Roll.No. : K017	Name: Sneha Darbarwar
Sem/Year : 3rd/2nd	Batch: CSE Cybersecurity
Date of Experiment : 3-9-24	Date of Submission: 29-9-24
Grade --	

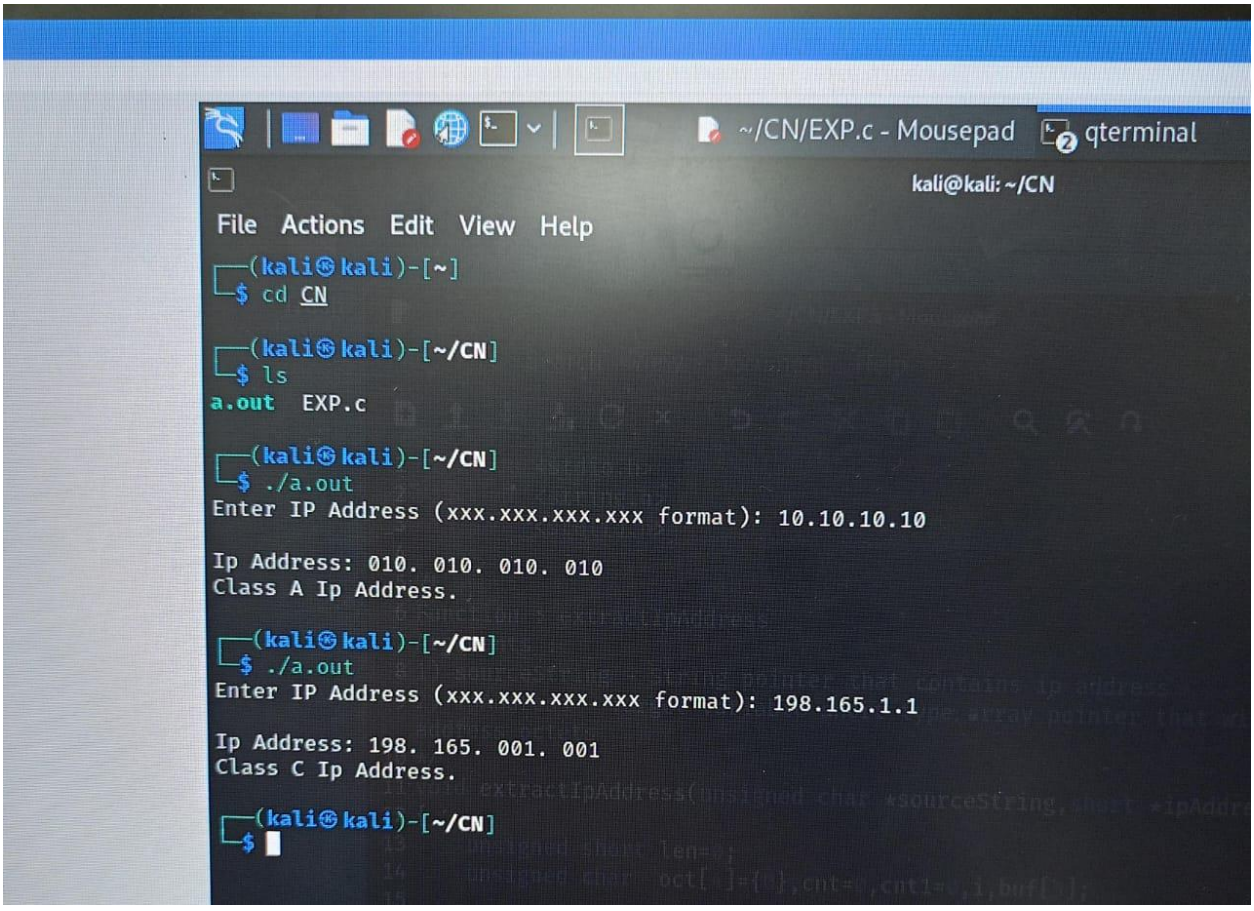
CODE:

```
#include <stdio.h>
#include <string.h>

/*
Function : extractIpAddress
Arguments :
1) sourceString - String pointer that contains ip address
2) ipAddress - Target variable short type array pointer that will store ip address octets
*/
void extractIpAddress(unsigned char *sourceString,short *ipAddress)
{
   unsigned short len=0;
   unsigned char  oct[4]={0},cnt=0,cnt1=0,i,buf[5];

   len=strlen(sourceString);
   for(i=0;i<len;i++)
   {
      if(sourceString[i]!='.'){
         buf[cnt++] =sourceString[i];
      }
      if(sourceString[i]=='.' || i==len-1){
         buf[cnt]='\0';
         cnt=0;
```

```
            oct[cnt1++]=atoi(buf);
        }
    }
    ipAddress[0]=oct[0];
    ipAddress[1]=oct[1];
    ipAddress[2]=oct[2];
    ipAddress[3]=oct[3];
}

int main()
{
    unsigned char ip[20]={0};
    short ipAddress[4];

    printf("Enter IP Address (xxx.xxx.xxx.xxx format): ");
    scanf("%s",ip);

    extractIpAddress(ip,&ipAddress[0]);

    printf("\nIp Address: %03d. %03d. %03d.
%03d\n",ipAddress[0],ipAddress[1],ipAddress[2],ipAddress[3]);

    if(ipAddress[0]>=0 && ipAddress[0]<=127)
        printf("Class A Ip Address.\n");
    if(ipAddress[0]>127 && ipAddress[0]<191)
        printf("Class B Ip Address.\n");
    if(ipAddress[0]>191 && ipAddress[0]<224)
        printf("Class C Ip Address.\n");
    if(ipAddress[0]>224 && ipAddress[0]<=239)
```

```
        printf("Class D Ip Address.\n");
    if(ipAddress[0]>239)
        printf("Class E Ip Address.\n");

    return 0;
}
```

OUTPUT:



QUESTION AND ANSWERS:

1. Identify the reasons for adoption of IPV6 address format.

1. Exhaustion of IPv4 Addresses

- Limited Address Space: IPv4 uses a 32-bit address space, which allows for approximately 4.3 billion unique IP addresses. However, with the explosion of internet-connected devices (smartphones, IoT, etc.), the available IPv4 addresses have been largely exhausted.
- IPv6's Larger Address Space: IPv6 uses a 128-bit address, providing 3.4 x 10^38 addresses. This massive address pool can accommodate the growing number of devices and new internet services well into the future.

2. Improved Routing Efficiency

- Hierarchical Addressing: IPv6 supports more efficient hierarchical addressing and routing structures, reducing the size of routing tables and improving the overall efficiency of internet routing.
- Simplified Headers: IPv6 headers are simpler compared to IPv4, which streamlines packet processing by routers, leading to faster data transmission and lower overhead in network routing.

3. Enhanced Security

- Built-in IPsec Support: Unlike IPv4, which offers IPsec (Internet Protocol Security) as an optional feature, IPv6 includes IPsec as a mandatory feature. This provides built-in encryption and authentication at the network layer, improving overall security.
- End-to-End Encryption: With IPv6, it's easier to maintain end-to-end encryption and authentication, as the larger address space allows for direct addressing without relying on Network Address Translation (NAT).

4. Elimination of NAT (Network Address Translation)

- Direct Addressing: In IPv4, the lack of available addresses led to widespread use of NAT, where a single public IP address is shared among multiple devices. NAT introduces complexities, limits the direct connectivity between devices, and can slow down communication.
- IPv6's Abundant Addressing: IPv6 eliminates the need for NAT, allowing every device to have a globally unique IP address. This simplifies network management and enables easier peer-to-peer communication without intermediary devices.

5. Support for Auto-Configuration

- Stateless Address Autoconfiguration (SLAAC): IPv6 supports SLAAC, which allows devices to automatically generate their own IP addresses when they connect to a network,

without the need for a DHCP server. This simplifies network configuration, especially in large networks or for mobile devices.
- Plug-and-Play Functionality: Devices can automatically configure their network settings and communicate with other devices, reducing manual configuration and improving network scalability

2. What is routable IP address and non-routable IP address? Give examples of each.

A routable IP address is an IP address that can be accessed and routed over the public internet. These addresses are globally unique, and traffic intended for these addresses can travel across multiple networks, including the internet, as they are part of the global routing system.

Characteristics:

- Globally Unique: Routable IP addresses are assigned by regional internet registries (RIRs) to ensure that no two devices on the internet share the same address.
- Publicly Accessible: Devices with routable IP addresses can be accessed from any other device on the internet, assuming no firewalls or security restrictions are in place.
- Requires Allocation by ISP: When you connect to the internet, your Internet Service Provider (ISP) assigns you a routable IP address for communication with the public internet.

Examples of Routable IP Addresses:

- IPv4:
  - 8.8.8.8 (Google's public DNS server)
  - 172.217.16.142 (An example IP address of Google's website)
- IPv6:
  - 2001:4860:4860::8888 (Google's public DNS server IPv6 address)

Usage:

- Web Servers: Public-facing servers (like websites) need routable IP addresses so they can be accessed globally.
- Email Servers: Similarly, email servers require routable IPs to send and receive emails from other mail servers.

Non-Routable IP Address:

A non-routable IP address, also called a private IP address, is an IP address that cannot be routed over the public internet. These addresses are typically used within private networks, such as homes, offices, or businesses. Devices using non-routable IP addresses communicate within their

local network, and any traffic destined for the internet needs to go through a device performing Network Address Translation (NAT).

Characteristics:

- Private Use: Non-routable addresses are reserved for use within private networks (e.g., home or office LANs).
- Not Globally Unique: Devices in different private networks can have the same private IP address since they are isolated from each other.
- Requires NAT: Devices with private IP addresses must use NAT to communicate with devices on the public internet. The router or gateway with a public (routable) IP address translates between the private and public IPs.

Examples of Non-Routable (Private) IP Address Ranges:

(These ranges are defined by RFC 1918 for IPv4 and RFC 4193 for IPv6.)

- IPv4 Private Address Ranges:
  - 10.0.0.0 – 10.255.255.255 (10.0.0.0/8)
  - 172.16.0.0 – 172.31.255.255 (172.16.0.0/12)
  - 192.168.0.0 – 192.168.255.255 (192.168.0.0/16)

  For example:

  - 192.168.1.1 (common default IP address for home routers)
  - 10.0.0.5 (used within a large office network)
- IPv6 Private Address Range:
  - Unique Local Addresses (ULAs): fc00::/7

  Example:

  - fc00:abcd:1234::1

Usage:

- Home Networks: Most home networks use non-routable IP addresses (like 192.168.1.x), and the router manages communication with the public internet using NAT.
- Corporate Networks: Large companies use private IP ranges (like 10.x.x.x) for internal communication, and devices inside the corporate network use a gateway with a routable IP to access external services.

Key Differences Between Routable and Non-Routable IP Addresses:

Aspect	Routable IP Address	Non-Routable IP Address
Global Access	Accessible over the public internet	Not accessible over the public internet
Uniqueness	Globally unique	Can be reused in different private networks
Usage	For public servers, internet-facing services	For private networks (LANs)

.

Communication with Internet	Direct communication with the internet	Requires NAT for internet communication
IP Range Examples	8.8.8.8, 2001:4860:4860::8888	192.168.1.x, 10.x.x.x, fc00::/7

In summary, routable IP addresses are used for devices that need to communicate over the public internet, while non-routable IP addresses are used within local networks and require NAT to access the wider internet

3. What is Loopback IP? What is the significance of Loop

Loopback IP Address

A loopback IP address is a special IP address used by a host to test network functionality and communicate with itself. It allows for testing internal network interfaces without involving the physical network interface or external networks.

- IPv4 Loopback Address: The loopback IP range in IPv4 is 127.0.0.0 to 127.255.255.255, with 127.0.0.1 being the most commonly used address.
- IPv6 Loopback Address: The loopback address in IPv6 is represented as ::1.

Purpose of Loopback IP:

- The loopback address is used for self-communication. When a packet is sent to this address, it is returned to the same device, bypassing the network interface hardware.

Significance of the Loopback Address

1. Network Testing and Diagnostics:
    - The loopback address is primarily used to test whether the TCP/IP stack (software component responsible for handling networking) on a host is working correctly. By sending a packet to 127.0.0.1 (or ::1 in IPv6), the host can verify that the network software is functioning without needing a physical network connection.
    - A common command used to test the loopback address is ping 127.0.0.1 (or ping ::1 for IPv6). This command checks if the system's networking stack is operational.
2. Software and Service Testing:
    - Many networked applications use the loopback address for testing purposes. For example, a web server running on a local machine can be accessed via http://127.0.0.1 or http://localhost, allowing the developer to test it without exposing it to external users.
    - Developers use the loopback interface to ensure that local services (e.g., databases, web applications) are running as expected.
3. Isolating Traffic:
    - The loopback address is isolated from any physical network. Any traffic sent to the loopback address does not leave the host. This makes it useful for testing network services without involving external network hardware or risking exposure to external networks.
4. Efficiency in Local Communication:
    - When a program needs to communicate with another process on the same machine, it can use the loopback address to avoid the overhead of routing the traffic through the network interface card (NIC) and the physical network. This is faster and reduces the chances of network congestion.
5. Avoiding IP Address Conflicts:
    - The loopback IP address is reserved, meaning it cannot be assigned to any physical device or host on the network. This prevents conflicts, ensuring that any traffic directed at a loopback address will always be handled locally.
6. Localhost Alias:
    - The loopback address is typically mapped to the hostname "localhost". This alias is used by many networked services and applications to reference the local machine. For instance, typing ping localhost will resolve to 127.0.0.1 or ::1.
7. Routing Purposes:
    - In routing, the loopback address can be used to simplify route advertisement and testing. For example, routers can use loopback interfaces for routing protocols like BGP or OSPF to identify themselves using a stable IP address that remains the same regardless of which physical interface is active.

Key Differences between Loopback and Other IP Addresses

Aspect	Loopback IP Address	Routable/Non-Routable IP Address
Purpose	Self-communication, testing, diagnostics	Communication within and outside of local networks
Routing	Does not leave the host	Routed across the network
Examples	IPv4: 127.0.0.1, IPv6: ::1	IPv4: 192.168.1.1 (private), 8.8.8.8 (public)
Usage	Internal testing, running local services	Device-to-device communication within a network

Conclusion

The loopback IP address is a crucial tool for testing and diagnosing local networking capabilities on a device without involving external network hardware. It plays a significant role in software development, service testing, and ensuring that the internal networking stack is functioning properly.