**Namal Institute Mianwali**

|  |  |
| --- | --- |
| Name | Muhammad Abrar Hussain |
| Registration No. | NIM-BSCS-2020-62 |
| Assignment No. | 08 |

# Computer Networks Laboratory Manual #8

**IP Addressing**

|  |  |  |  |
| --- | --- | --- | --- |
| **Course Title** | Computer Networks | **Course Number** | CS – 331 L |
| **Instructor** | Shahzad Arif  shahzad.arif@namal.edu.pk | **Lab Engineer** | Asad Majeed  [asad.majeed@namal.edu.pk](mailto:asad.majeed@namal.edu.pk) |

1. **Introduction:**

In this laboratory exercise, you shall learn the Network layer addressing, useful for routing.

1. **Objective:**

After completing this lab, the student will be able to

* + Identify and differentiate between different IP address classes.
  + To understand IP addressing schemes used in LANs.
  + To use subnetting to divide a large network into subnets
  + To understand NAT

1. **Methodology:**

To achieve this objective, will solve different problems related to IP addresses.

1. **Background – IP Addressing and the Local Area Network:**

With reference to Figure 1, network devices operate by implementing Layer 1,2, and 3 functionalities. A switch only implements Layers 1&2 whereas a router implements Layers 1,2&3, whereas the hosts/end devices generally implement all 7 layers.

For network configuration Internet Protocol (IP) requires IP addresses, in addition to the Layer 2 MAC addresses.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 7 | Application Layer |  | 4 | Application Layer |
| 6 | Presentation Layer |
| 5 | Session Layer |
| 4 | Transport Layer | 3 | Transport Layer |
| 3 | Network Layer | 2 | Network Layer |
| 2 | Data Link Layer | 1 | Link Layer (Physical Layer) |
| 1 | Physical Layer |
|  | ***OSI Model*** |  | ***IP Model*** |

*Figure 1: OSI vs IP model*

# Local Area Networks (LANs)

A local area network or "LAN" is a collection of devices that are physically connected to the same hub, switch, or group of interconnected switches. To function properly, LANs are configured so that any device can send a broadcast message that can be seen by all devices on the LAN. For this reason, LANs are often referred to as "broadcast domains".

The ability of each device to send broadcast messages to all devices on the LAN is important because when a device needs to initiate a communication session with another device on the LAN, the sending device usually only knows the logical Internet Protocol (IP) address of the intended target system. However, the way networks function, any message being sent must ultimately be directed not to the target system's logical IP address, but to an address that is built into the target computer's physical network interface known as the MAC address.

To obtain a MAC address for the target system, the sending computer must broadcast, the equivalent of “shouting out”, a message to all devices on the LAN asking the device that has been assigned the target IP address to reply with its built-in hardware MAC address. After the device assigned to that IP address responds to the sending system, the sending device then directs the communication message that it wants to send to the MAC address of the target system. This protocol that resolves the MAC address among LAN-based devices is called the Address Resolution Protocol or "ARP". As each device obtains IP address/MAC address pairs for devices on the LAN with which it has communicated, it caches the address values so that it does not need to send the same broadcast requests repeatedly.

In the past, if a device needed to determine an IP address for a known MAC address, it would use a protocol called Reverse ARP or "RARP", but that protocol is now rarely used and is considered obsolete.

Another characteristic of a LAN is that all devices on the LAN have the same value in the portion of their IP addresses that identify their network or subnet. By comparing the network-identifying portion of its IP address with that of the target device, the sending system knows whether the target device is on the same LAN.

# Routers

When a device in a Local Area Network needs to communicate with a device in another

LAN must send that traffic to a specialized device connected to the LAN called a “router” whose purpose is to find the best path for the message to take to arrive at the intended target device and to send the message along its way following that path.

To allow the billions of devices on the Internet to find each other, routers regularly need to communicate among themselves using protocols that enable them to share routing information so that, when a device needs to send a communication message to a target device, the routers work together to determine the best path for the message packet to use to arrive at the intended target device.

Each router port is configured with a specific routing protocol that is associated with that port's function. For example, a router port that connects to the Internet must learn how to efficiently route communication messages to destinations around the world. Protocols that facilitate this are called "gateway routing protocols" and have names such as the Border Gateway Protocol ("BGP") or Exterior Gateway Protocol ("EGP").

A router port that connects to an organization's internal networks must learn how the organization's network is configured to efficiently route traffic throughout the organization. Protocols that serve this purpose are called "interior routing protocols" and have names such as Enhanced Interior Gateway Routing Protocol ("EIGRP"), Interior

Gateway Routing Protocol ("IGRP"), Open Shortest Path First ("OSPF"), Routing Information Protocol I and II ("RIP"/"RIP II").

## Dynamic Host Configuration Protocol or "DHCP" servers

There are two ways to assign an IP address to a device joining the network:

* One method is to have the device’s administrator manually type in an unused IP address from the appropriate address range that he or she received from the network administrator into the device’s configuration.
* The other method is to configure each device so that when it connects to the network, it asks a specialized computer on the network running “DHCP server” software to assign it an IP address from the address range associated with the network.

The use of DHCP servers significantly reduces the amount of administrative effort associated with assigning, unassigning, and keeping track of IP addresses, and it is very rare these days for organizations not to use DHCP.

## Domain Name Service or “DNS” servers

Earlier, we had mentioned that a target device could be located by its IP address or by its device or “host” name. If a device needs to connect to a device, but only knows its name,

e.g.,  [www . namal .edu](http://www.uhcl.edu/) , it can ask a computer configured with Domain Name Service ("DNS") software to find the IP address of the intended target device by its host name.

Each DNS server holds information about the devices that are part of an organization’s network. It also keeps track of the addresses of specialty devices that the world needs to find, e.g., e-mail servers. The DNS server is not merely a standalone directory service. In cases where a sending device needs to find the address of a device that belongs to a different organization, the DNS will locate the appropriate DNS server anywhere on the Internet to give you the appropriate target device’s IP address information.

**What is Internet Protocol (IP) addressing?**

When devices communicate with each other over a local area network or “LAN” or across the internet, the message transmitted is ultimately directed to the target device’s network hardware address that is programmed into the device by the manufacturer. This hardware address known as the “MAC” address is physically encoded very much like an automobile’s VIN (Chassis Number) that includes information about the manufacturer and when the device was created along with a sequential number.

Unfortunately, MAC addresses do not help route communication messages outside of a small number of locally interconnected devices because they are randomly scattered around the world, i.e., a device with a MAC address of 10:20:30:40:50:60 could be in New York and another with a MAC address of 10:20:30:40:50:61 could be in Beijing.

To enable devices to find each other easily no matter where they are in the world, the creators of the Internet came up with a logical addressing scheme that made it much easier for devices to find each other, no matter where they were on the Internet. These logical, Internet Protocol, addresses are commonly referred to as “IP addresses”.

# The form and organization of IP addresses

*Note – for this discussion, we will be describing IPv4 addresses, a four-byte address format that has been in use for decades and continues to be used by a majority of Internet-connected organizations. The latest IP addressing scheme, IPv6, uses a six-byte address so that many more devices on the Internet can be addressed.*

Each IPv4 address is four bytes in length and is expressed in the form: “nnn.nnn.nnn.nnn”, where each “nnn” is a number from 0 through 255, the largest value of that can be expressed in eight binary bits. For example, the string 192.168.252.199 would be a syntactically correct expression of an IPv4 address.

Each IP address string is made up of two components:

* A network identifying component which is the leftmost part of the address, and
* A device-identifying component which is the rightmost part of the address

The network identifying component is used by network routing devices or “routers” to determine the best way to send a communication message to take it closer to its destination, the target device itself. The device-identifying component of the IP address is only of significance to the target device and any other devices sharing the same local area network (LAN).

The length of the network and device-identifying components may vary based on the number of devices that an organization needs to address, but the total number of bytes used for the address will always be four for IPv4 addresses.

# Classful Routing

Message routing devices or “routers” transfer messages from one organization to another using a highly structured method of IP addressing called “classful routing”, where IP address ranges are grouped into five classes. Because of its structured nature, routers using classful routing are far more efficient than other methods that will be described later in this discussion.

The following table describes the fundamental IP address network classes including how the addresses are defined, the number of device IP addresses the network class can support, and examples of the device IP address that would be included in the network. The last column in the table shows the first byte values for networks in each class that is set by convention.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **IP address network class** | **# of leftmost bytes that**  **identify the network** | **# of rightmost bytes that identify**  **devices within the network** | **Maximum # of IP addresses**  **supported by each**  **network in this class** | **Maximum # of Networks in a Class** | **Examples of IP addresses that would be on the same network in this class** | **IP addresses in this class have a first-byte value of:** | | Class A | 1 | 3 | 16,777,216 | **127** | **10**.1.7.242,  **10**.7.23.195 | 0 through 127 | | Class B | 2 | 2 | 65,535 | **16,384** | **172.16**.21.9,  **172.16**.47.18,  **172.16**.250.241 | 128 through 191 | | Class C | 3 | 1 | 256 | **2,097,152** | **192.168.45.**1,  **192.168.45.**25,  **192.168.45.**253 | 192 through 223 | | Class D |  |  |  |  |  |  | | Class E |  |  |  |  |  |  |   *Table 1: Classful IP addresses* |

*Notes:*

1. *The network-identifying component of each device IP address example is displayed in bold.*
2. *There are also class D addresses (first-byte value from 224 through 239) used for multi-casting, and class E addresses (first-byte value from 240 through 255) that are used for Internet Engineering Task Force (IETF) research -- internal testing. These two classes are not part of this discussion.*

# Classless Inter-Domain Routing (CIDR)

The number of class "A", "B" and "C" IP address ranges is severely limited, so when an organization obtains an IP address range, they usually obtain several class “C” ranges, or, if they are lucky, a class “B”. Obtaining a class “A” address range is highly unlikely.

If all we had was classful addressing and an organization obtained a class “B” IP address range, all the devices would need to be on the same local area network which could result in extremely poor performance and a lack of network design flexibility. Fortunately, the development of the Classless Inter-Domain Routing (CIDR) method of IP addressing, and routing allowed organizations to easily segregate any of their classful IP address ranges or “networks” into several sub-ranges or “subnets” using “subnet masks”.

*Note - For the remainder of this discussion, the term "network" will be used to refer to either a network or a subnet.*

# Subnet masks

Each Internet router that uses classful routing knows that any IP address starting with 0 through 127 is a class “A” address with a network-identifying component one byte in length. Any IP address beginning with 128 through 191 is a class “B” address, so the network identifying component is two bytes in length, etc.

But when an organization needs to break up it's class "A" or class “B” network into several class “C”- or other smaller-sized subnets, its routers cannot rely on the initial byte of the IP address to tell it anything about the length of the network identifying component of the subnetted address.

To provide the routers with this information when using classless routing, you must specify the length of the network identifying component of the subnet’s IP addresses using a “subnet mask”. The subnet mask for each subnet is formatted just like an IP address, i.e., “nnn.nnn.nnn.nnn”, but the meaning of the byte values is very different. In a subnet mask, all the bits from the left that are to be included in the network-identifying component of the IP address have a value of one, and all the bits from the right that identify the device within the range have a value of zero.

So, if you need to carve out a class “C”-sized subnet from a class “A” or class “B” network, you will specify a subnet mask with a decimal value of 255.255.255.0 or a binary value of 11111111 11111111 11111111 00000000.

With classless routing, you are not limited to subnet sizes based on the three fundamental class sizes. You may need to have a subnet with more than 254 devices or less. Some subnets only involve two devices, so creating a class “C”-sized subnet for that purpose would waste addresses. Fortunately, subnet masks provide enough flexibility to allow us to set the boundary between the IP address’ network identifying component and its device-identifying component at virtually any bit in the four-byte IP address string.

If an organization has obtained a class “B” network and needs to create a subnet within the network that can handle twice the number of device addresses as a traditional class “C” range, we could define a subnet that indicates we are using the first 23 bits of each IP address for our network identifying component and the last 9 bits to address up to 510 devices in the subnet (2 to the 9th power minus two reserved addresses). In this case, the subnet mask would have a decimal value of 255.255.254.0 or a binary value of 11111111 11111111 11111110 00000000.

If an organization has a class “B” or a class “C” network and needs to create a subnet that can handle half the number of devices as a traditional class “C” range, we could define a subnet that indicates we are using the first 25 bits of each IP address in the subnet for our network identifying component, and the last 7 bits to address up to 126 devices in the subnet (2 to the 7th power minus two reserved addresses). In this case, the subnet mask would have a decimal value of 255.255.255.128 or a binary value of 11111111 11111111 11111111 10000000.

# Routable address vs. Non-routable addresses

Were we to give every device in the world its unique IP address, we would have run out of addresses at the end of the 90s, the time of the world wide web (WWW) boom. So, the Internet Engineering Task Force (IETF) decided that, since most devices only need to be accessed within their organization and never need to be accessed remotely, they would reserve ranges of addresses that every organization can use for their internal device-to-internal device communication traffic. These addresses are called “non-routable” addresses (or “RFC 1918” addresses since the recommendation was the 1918th accepted through the IETF’s “Request for comment (RFC)” process).

The IP address ranges that are reserved by RFC 1918 are:

* 10.0.0.0 through 10.255.255.255 Class A Address, Subnet Mask: 255.0.0.0
* 172.16.0.0 through 172.31.255.255; Class B Address, Subnet Mask: 255.255.0.0
* 192.168.0.0 through 192.168.255.255; Class C Address, Subnet Mask: 255:255:255.0

Because all Internet-based routers are configured to ignore any message packet destined for an IP address in any of the above ranges, there is no concern about millions of organizations using the same numbers as other organizations to address their devices. However, routers that are used to exchange information among devices within an organization are configured to treat these IP addresses as any other IP routable address.

# CIDR notation – the easier way

Since many of us are not very efficient binary calculators, CIDR notation provides a simpler method of expressing the mask merely by indicating the network address (i.e., the first address in the IP address range) followed by a slash and the number of bits that are in the network identifying component of the IP address.

*Note – The sample ranges and maximum device counts have been adjusted to reflect the fact that IP addressing reserves the first address in the range to identify the network and the last address in the range to broadcast to all devices in the network, so they cannot be assigned to individual devices.*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | **Mask Expression** | **CIDR Notation** | **Sample IP Address** | **Max # of Devices** | | 255.255.255.0 | 192.168.64.0/24 | 192.168.64.1 – 192.168.64.254 | 254 | | 255.255.254.0 | 192.168.64.0/23 | 192.168.64.1 – 192.168.65.254 | 510 | | 255.255.252.0 | 192.168.64.0/22 | 192.168.64.1 – 192.168.67.254 | 1022 | | 255.255.248.0 | 192.168.64.0/21 | 192.168.64.1 – 192.168.71.254 | 2046 |   *Table 2: CIDR notation* |

**Can a device with a non-routable IP address ever receive a message from the Internet?**

Yes – but only if a mechanism called “Network Address Translation (NAT)” is set up on one of the routing devices. What NAT does is reserve an alias IP address for the device that is in a routable range. When a message arrives destined for the alias IP address, the router changes the destination IP address to the target device’s actual non-routable IP address before sending it to the target device.

When a device that has a non-routable address needs to send a communication message outbound to a device on the Internet, one of two NAT methods could be employed:

1. If the router is configured to perform “one-to-one address translation”, it will replace the sending device’s non-routable IP address in the outbound message with its associated routable IP address that has been configured in the router’s NAT table.
2. If the router is configured to perform many-to-one address translation, each sending device’s non-routable IP address will be replaced with the address of the router itself. In this case, since all exiting communication traffic from multiple sending devices will leave the campus with the same IP address and each is probably expecting a response, the router will need to know which response is supposed to go to which target internal device. To accomplish this, other data elements in the message header, such as the “session ID” are used to identify the appropriate internal device.

**IPv6**

IPv6 is the next generation of IP addressing. It has 128 bits to represent the address so theoretically it has 2128 IP addresses. IPv6 addresses are represented as eight groups of four hexadecimal digits each, separated by colons. The full representation may be shortened; for example, 2001:0db8:0000:0000:0000:8a2e:0370:7334 becomes 2001:db8::8a2e:370:7334.

1. **Tasks:**

**5.1. You have been given the IP address 192.10.0.0. You are required to do the following tasks:**

**Identify the class of given IP addresses:**

* This IP address from class c

**Write down the default subnet mask for the identified class:**

* 255.255.255.0

**Your task is to divide this given network into subnets and fill the table given below:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CIDR Notation of the first Network** | **Subnet Mask** | **Subnet Mask in binary** | **Number of Networks** | **Number of Hosts** |
| 192.168.0.0/24 | 255.255.255.0 | 11111111.11111111.11111111.00000000 | 1 | 254 |
| 192.168.0.0/25 | 255.255.255.128 | 11111111.11111111.11111111.10000000 | 2 | 126 |
| 192.168.0.0/26 | 255.255.255. 192 | 11111111.11111111.11111111.11000000 | 4 | 62 |
| 192.168.0.0/27 | 255.255.255.224 | 11111111.11111111.11111111.11100000 | 8 | 30 |
| 192.168.0.0/28 | 255.255.255.240 | 11111111.11111111.11111111.11110000 | 16 | 14 |

**5.2. If you have the following address 192.10.1.0/27. How many total bits are used to identify the network and how many total bits are used to identify the hosts? Also, write the subnet mask of the given address.**

* 27 bits will be used to identify the network.
* 5 bits will be used for identifying the host
* 255.255.255.224

**5.3. Can you subnet the 192.10.0.0/24 such that we have 30 networks and 4 hosts per network? If yes, then how.**

To get the number of 30 networks and 4 hosts on each network we will make the first five-bit of the last octet 1 and the next three will remain 0.

* Yes, we can subnet to 192.10.0.0/24, such that we have 30 networks and 4 hosts per network.
* Subnet mask >> 11111111.11111111.11111111.11111000
* CIDR Notation >> 192.10.0.0/29

**5.4. If you have the following address 192.23.10.0/28. Answer the following:**

* Subnet Mask: 255.255.255.240
* Number of Networks: 16
* Number of Hosts: 14

**Full Range of first three Networks:**

|  |  |
| --- | --- |
| **Start Range** | **End Range** |
| 192.23.10.0/28 | 192.23.10.15/28 |
| 192.23.10.16/28 | 192.23.10.31/28 |
| 192.23.10.32/28 | 192.23.10.47/28 |

**Usable Range of first three Networks:**

|  |  |  |
| --- | --- | --- |
| **192.23.10.0/28 (Network IP)** | **192.23.10.16/28**  **(Network IP)** | **192.23.10.32/28 (Network IP)** |
| * + - * 192.23.10.1/28 | * + - * 192.23.10.17/28 | * + - * 192.23.10.33/28 |
| * + - * 192.23.10.2/28 | * + - * 192.23.10.18/28 | * + - * 192.23.10.34/28 |
| * + - * 192.23.10.3/28 | * + - * 192.23.10.19/28 | * + - * 192.23.10.35/28 |
| * + - * 192.23.10.4/28 | * + - * 192.23.10.20/28 | * + - * 192.23.10.36/28 |
| * + - * 192.23.10.5/28 | * + - * 192.23.10.21/28 | * + - * 192.23.10.37/28 |
| * + - * 192.23.10.6/28 | * + - * 192.23.10.22/28 | * + - * 192.23.10.38/28 |
| * + - * 192.23.10.7/28 | * + - * 192.23.10.23/28 | * + - * 192.23.10.39/28 |
| * + - * 192.23.10.8/28 | * + - * 192.23.10.24/28 | * + - * 192.23.10.40/28 |
| * + - * 192.23.10.9/28 | * + - * 192.23.10.25/28 | * + - * 192.23.10.41/28 |
| * + - * 192.23.10.10/28 | * + - * 192.23.10.26/28 | * + - * 192.23.10.42/28 |
| * + - * 192.23.10.11/28 | * + - * 192.23.10.27/28 | * + - * 192.23.10.43/28 |
| * + - * 192.23.10.12/28 | * + - * 192.23.10.28/28 | * + - * 192.23.10.44/28 |
| * + - * 192.23.10.13/28 | * + - * 192.23.10.29/28 | * + - * 192.23.10.45/28 |
| * + - * 192.23.10.14/28 | * + - * 192.23.10.30/28 | * + - * 192.23.10.46/28 |

**Rubrics Sheet**

|  |  |  |
| --- | --- | --- |
| **Activities** | **Description** | **Marks** |
| **Task 1** | Student has performed the given task without any errors. | 2 |
| **Task 2** | Student has performed the given task without any errors | 1 |
| **Task 3** | Student has performed the given task without any errors | 1 |
| **Task 4** | Student has performed the given task without any errors | 1 |
| **Viva Voce** | Student can answer the questions regarding subnetting and the performed tasks. | 5 |