

# R-Pi

**Team Emertxe**



# IoT Protocols

IPv4



# IPv4

## Introduction



- works at the network layer of the OSI model and at the Internet layer of the TCP/IP model
- has the responsibility of identifying hosts based upon their logical addresses
- To route data among them over the underlying network
- uses 32-bit logical address, to identify the host

# Packet Structure



# IPv4

## Packet Structure



- IPv4 being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets
- IPv4 packet encapsulates data unit received from above layer and add to its own header information

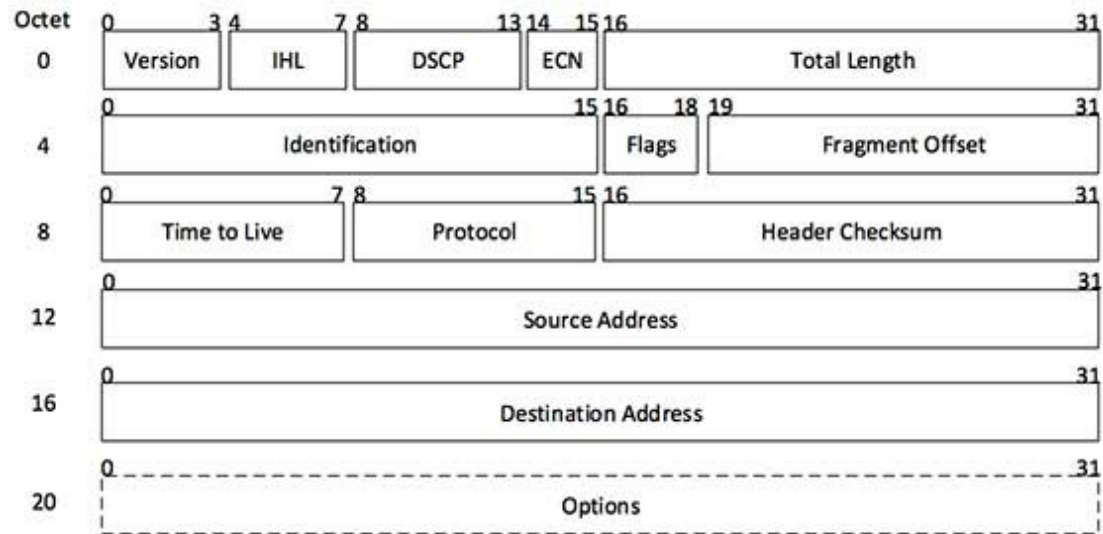


(IP Encapsulation)

# IPv4

## Packet Structure

- The encapsulated data is referred to as IP Payload
- IPv4 header contains all the necessary information to deliver the packet at the other end



[Image: IP Header]

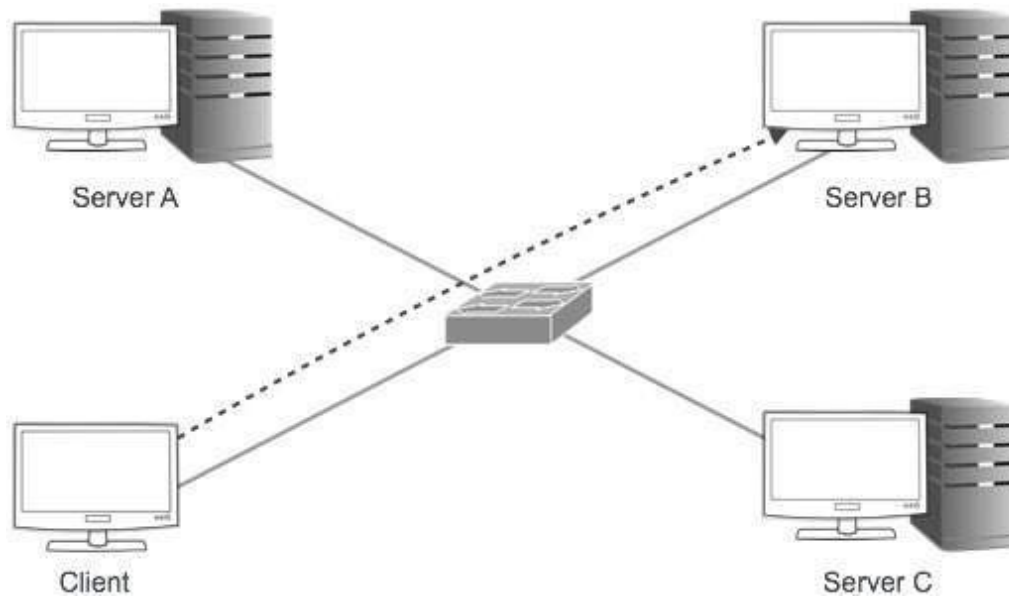
# Addressing Modes



# IPv4

## Unicast Addressing Mode

- In this mode, data is sent only to one destined host
- The Destination Address field contains 32- bit IP address of the destination host
- Here the client sends data to the targeted server

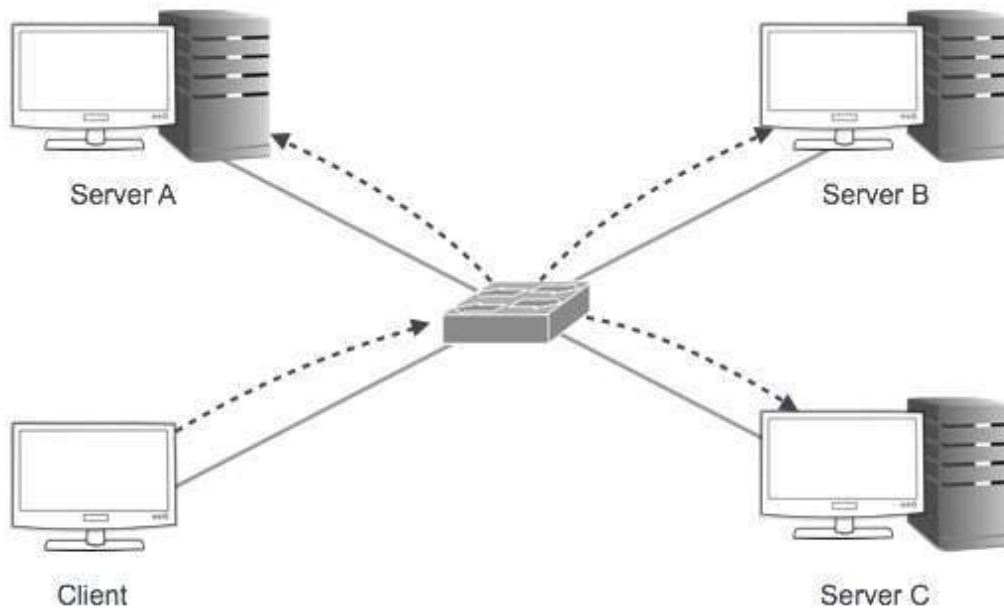




# IPv4

## Broadcast Addressing Mode

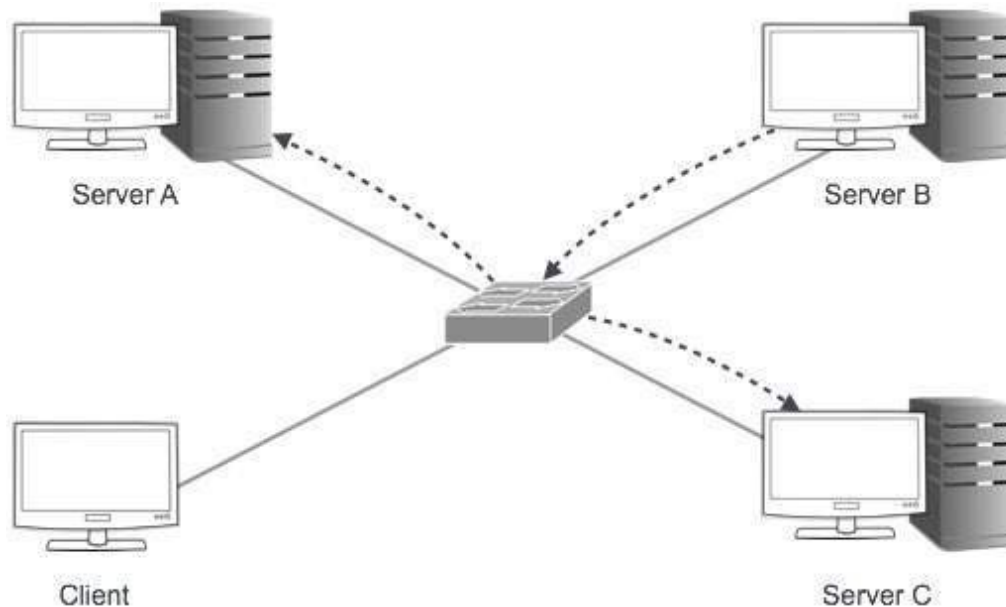
- In this mode, the packet is addressed to all the hosts in a network segment
- The Destination Address field contains a special broadcast address, i.e. 255.255.255.255
- When a host sees this packet on the network, it is bound to process it
- Here the client sends a packet, which is entertained by all the Servers



# IPv4

## Multicast Addressing Mode

- This mode is a mix of the previous two modes, i.e. the packet sent is neither destined to a single host nor all the hosts on the segment
- In this packet, the Destination Address contains a special address which starts with 224.x.x.x and can be entertained by more than one host



# IPv4

## Hierarchical Addressing Scheme

- IPv4 uses hierarchical addressing scheme
- An IP address, which is 32-bits in length, is divided into two or three parts as depicted



- A single IP address can contain information about the network and its sub-network and ultimately the host
- This scheme enables the IP Address to be hierarchical where a network can have many sub-networks which in turn can have many hosts

# IPv4

## Subnet Mask

- The 32-bit IP address contains information about the host and its network
- routers use Subnet Mask, which is as long as the size of the network address in the IP address
- Subnet Mask is also 32 bits long, If the IP address in binary is ANDed with its Subnet Mask, the result yields the Network address
- For example, say the IP Address is 192.168.1.152 and the Subnet Mask is 255.255.255.0 then

IP	192.168.1.152	11000000	10101000	00000001	10011000	ANDed
Mask	255.255.255.0	11111111	11111111	11111111	00000000	
Network	192.168.1.0	11000000	10101000	00000001	00000000	Result

- It can be identified now that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network

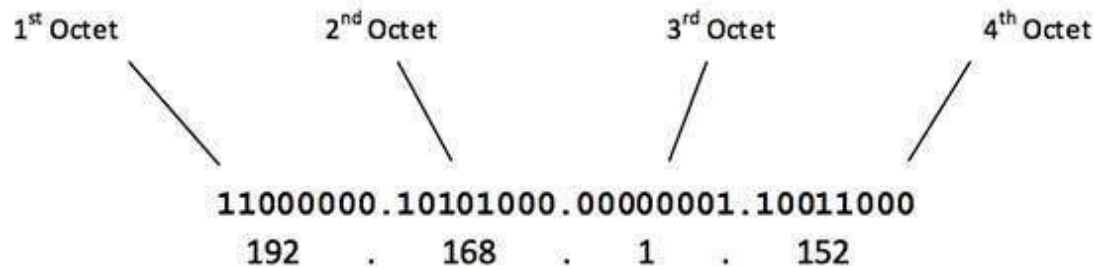
# Address Classes



# IPv4

## Introduction

- Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses.
- All the five classes are identified by the first octet of IP Address
- The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address



- The number of networks and the number of hosts per class can be derived by this formula

Number of networks =  $2^{\text{network\_bits}}$

Number of Hosts/Network =  $2^{\text{host\_bits}} - 2$

# IPv4

## Class A

- The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 - 127, i.e

00000001 - 01111111  
1 - 127

- Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only.
- The IP range 127.x.x.x is reserved for loopback IP addresses
- The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks ( $2^7-2$ ) and 16777214 hosts ( $2^{24}-2$ )
- Class A IP address format is thus: 0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

# IPv4

## Class B

- An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e

10000000 – 10111111  
128 – 191

- Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x
- Class B has 16384 (214) Network addresses and 65534 (216-2) Host addresses
- Class B IP address format is: 10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH



# IPv4

## Class C

- The first octet of Class C IP address has its first 3 bits set to 110, that is

**110**00000 - **110**11111  
192 - 223

- Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x
- Class C gives 2097152 ( $2^{21}$ ) Network addresses and 254 ( $2^8-2$ ) Host addresses.
- Class C IP address format is: 110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

# IPv4

## Class D

- Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of:

**1110**0000 - **1110**1111  
224 - 239

- Class D has IP address range from 224.0.0.0 to 239.255.255.255
- Class D is reserved for Multicasting
- In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask

# IPv4

## Class E



- This IP Class is reserved for experimental purposes only for R&D or Study.
- IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254.
- Like Class D, this class too is not equipped with any subnet mask.

# Subnetting



# IPv4

## Introduction



- Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network.
- Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.
- CIDR or Classless Inter Domain Routing provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet.
- By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

# Ipv4: Subnets

## Class A



- In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e.  $2^{24} - 2$  Hosts per Network).
- To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly.
- For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets ( $2^1 = 2$ ) with  $(2^{23} - 2)$  8388606 Hosts per Subnet.
- The Subnet mask is changed accordingly to reflect subnetting.

# Ipv4: Subnets

## Class B

- By default, using Classful Networking, 14 bits are used as Network bits providing  $(2^{14})$  16384 Networks and  $(2^{16}-2)$  65534 Hosts.
- Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits.

# Ipv4: Subnets

## Class C

- Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network



Reserved Addresses



# IPv4

## Private IP Addresses

- Every class of IP, (A, B & C) has some addresses reserved as Private IP addresses.
- These IPs can be used within a network, campus, company and are private to it.
- These addresses cannot be routed on the Internet, so packets containing these private addresses are dropped by the Routers.

Class A IP Range	Subnet Mask
10.0.0.0 – 10.255.255.255	255.0.0.0
172.16.0.0 – 172.31.255.255	255.240.0.0
192.168.0.0 – 192.168.255.255	255.255.0.0

- In order to communicate with the outside world, these IP addresses must have to be translated to some public IP addresses using NAT process, or Web Proxy server can be used.
- The sole purpose to create a separate range of private addresses is to control assignment of already-limited IPv4 address pool.
- By using a private address range within LAN, the requirement of IPv4 addresses has globally decreased significantly.
- It has also helped delaying the IPv4 address exhaustion.

# IPv4

## Private IP Addresses

- IP class, while using private address range, can be chosen as per the size and requirement of the organization.
- Larger organizations may choose class A private IP address range where smaller organizations may opt for class C.
- These IP addresses can be further sub-netted and assigned to departments within an organization.

# IPv4

## Loopback IP Addresses

- The IP address range 127.0.0.0 - 127.255.255.255 is reserved for loopback, i.e. a Host's self-address, also known as localhost address.
- This loopback IP address is managed entirely by and within the operating system.
- Loopback addresses, enable the Server and Client processes on a single system to communicate with each other.
- When a process creates a packet with destination address as loopback address, the operating system loops it back to itself without having any interference of NIC.
- Data sent on loopback is forwarded by the operating system to a virtual network interface within operating system.
- This address is mostly used for testing purposes like client-server architecture on a single machine.
- Other than that, if a host machine can successfully ping 127.0.0.1 or any IP from loopback range, implies that the TCP/IP software stack on the machine is successfully loaded and working.

# IPv4

## Link-local Addresses



- In case a host is not able to acquire an IP address from the DHCP server and it has not been assigned any IP address manually, the host can assign itself an IP address from a range of reserved Link-local addresses.
- Link local address ranges from 169.254.0.0 - 169.254.255.255
- Assume a network segment where all systems are configured to acquire IP addresses from a DHCP server connected to the same network segment.
- If the DHCP server is not available, no host on the segment will be able to communicate to any other.
- In absence of DHCP server, every host machine randomly chooses an IP address from the above mentioned range and then checks to ascertain by means of ARP, if some other host also has not configured itself with the same IP address.
- Once all hosts are using link local addresses of same range, they can communicate with each other.
- These IP addresses cannot help system to communicate when they do not belong to the same physical or logical segment.
- These IPs are also not routable.

# Packet Flow in Network



# IPv4

## Packet Flow in Network

- All the hosts in IPv4 environment are assigned unique logical IP addresses.
- When a host wants to send some data to another host on the network, it needs the physical (MAC) address of the destination host.
- To get the MAC address, the host broadcasts ARP message and asks to give the MAC address whoever is the owner of destination IP address.
- All the hosts on that segment receive the ARP packet, but only the host having its IP matching with the one in the ARP message, replies with its MAC address.
- Once the sender receives the MAC address of the receiving station, data is sent on the physical media.

# IPv4

## Packet Flow in Network

- To understand the packet flow, we must first understand the following components:
  - MAC Address
  - Address Resolution Protocol
  - Proxy Server
  - Dynamic Host Control Protocol
  - Domain Name System
  - Network Address Translation



# Ipv4: Packet Flow in Network

## Step-1:Acquiring an IP Address (DHCP)

- When the user's PC boots up, it searches for a DHCP server to acquire an IP address.
- For the same, the PC sends a DHCPDISCOVER broadcast which is received by one or more DHCP servers on the subnet and they all respond with DHCPOFFER which includes all the necessary details such as IP, subnet, Gateway, DNS, etc.
- The PC sends DHCPREQUEST packet in order to request the offered IP address.
- Finally, the DHCP sends DHCPACK packet to tell the PC that it can keep the IP for some given amount of time that is known as IP lease.
- Alternatively, a PC can be assigned an IP address manually without taking any help from DHCP server.
- When a PC is well configured with IP address details, it can communicate other computers all over the IP enabled network.

# Ipv4: Packet Flow in Network

## Step: 2 – DNS Query



- When a user opens a web browser and types `www.emertxe.com` which is a domain name and a PC does not understand how to communicate with the server using domain names, then the PC sends a DNS query out on the network in order to obtain the IP address pertaining to the domain name.
- The pre-configured DNS server responds to the query with IP address of the domain name specified.

# Ipv4: Packet Flow in Network

## Step: 3 – ARP Request



- The PC finds that the destination IP address does not belong to his own IP address range and it has to forward the request to the Gateway.
- The Gateway in this scenario can be a router or a Proxy Server.
- Though the Gateway's IP address is known to the client machine but computers do not exchange data on IP addresses, rather they need the machine's hardware address which is Layer-2 factory coded MAC address.
- To obtain the MAC address of the Gateway, the client PC broadcasts an ARP request saying "Who owns this IP address?" The Gateway in response to the ARP query sends its MAC address.
- Upon receiving the MAC address, the PC sends the packets to the Gateway.
- An IP packet has both source and destination addresses and it connects the host with a remote host logically, whereas MAC addresses help systems on a single network segment to transfer actual data.
- It is important that source and destination MAC addresses change as they travel across the Internet (segment by segment) but source and destination IP addresses never change.

THANK YOU