...1...
Internet Architecture and Network Layer

Learning Outcomes...

- ❑ Identify role of ISP and ICANN.
- ❑ Compare IPv4 and IPv6.
- ❑ Configure Subnets in network.
- ❑ Interpret role of ARP and RARP.

1.0 INTRODUCTION

- The internet is a global network of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices, enabling the sharing of information and resources worldwide.
- The Internet (or internet) is the global system of interconnected computer networks that uses the Internet protocol suite to communicate between networks and devices.
- The internet is a network of networks that consists of private, public, academic, business and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies.
- The internet architecture describes the structure and protocols that make the global internet function. It doesn’t concern itself with individual networks but looks at how all networks interact to form the internet.
- Its focus is on the global system of interconnected computer networks and the protocols they use to communicate such as TCP/IP.
- The internet architecture is built on a layered model, where each layer provides services to the layer above it.
- This layered approach allows for modularity and flexibility, enabling different technologies and protocols to be used at each layer.
- The internet architecture is often described using the 5-layer or 7-layer models, with the network layer being a key component.
    - **5-Layer Model (TCP/IP Model or Internet Model):** The layers of TCP/IP model includes: 5. Application Layer, 4. Transport Layer, 3. Network Layer, 2. Data-link Layer, 1. Physical Layer. The Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today.
    - **7-Layer Model (OSI (Open Systems Interconnection Reference Model):** Layers of the OSI model includes: 7. Application layer, 6. Presentation layer and 5. Session layer 4. Transport layer, 3. Network layer, 2. Data link layer and 1. Physical layer.
- The network layer, also known as the internet layer, is responsible for routing data packets between different networks. It uses logical addressing (IP addresses) to identify devices and networks.

- The internet is a global network of interconnected computers, servers, and devices that communicate using standardized protocols like TCP/IP (Transmission Control Protocol/Internet Protocol).
- Internet Architecture refers to the structure and design of the interconnected networks on the Internet, which allows routers to route packets based on the destination network. The Internet architecture, which is also sometimes called the TCP/IP architecture.
- Internet's architectural model is organized in a stack of protocols composed of five distinct layers namely, Application layer, Transport layer, Network layer, Data-link layer and Physical layer.

1.1 STRUCTURE OF INTERNET

- The Internet is a global network that connects millions of computers and devices worldwide. It enables communication, information sharing, and various online services such as browsing websites, sending emails, social media and so on.
- The Internet works using a combination of protocols like TCP/IP, which ensure data is transmitted efficiently between devices.
- The internet, sometimes simply called the net, is a worldwide system of interconnected computer networks and electronic devices that communicate with each other using an established set of protocols.
- An Internet is a combination or collection of networks. Fig. 1.1 shows structure of Internet. A protocol needs to define its domain of operation, the messages exchanged, communication between routers, and interaction with protocols in other domains.
- The Internet has changed from a tree like structure, with a single backbone, to a multi-backbone structure run by different private corporations today.
- The Internet today is made of a huge number of networks and routers that connect them. A single protocol is not sufficient to provide routing for the entire internet because of scalability and administrative problems.

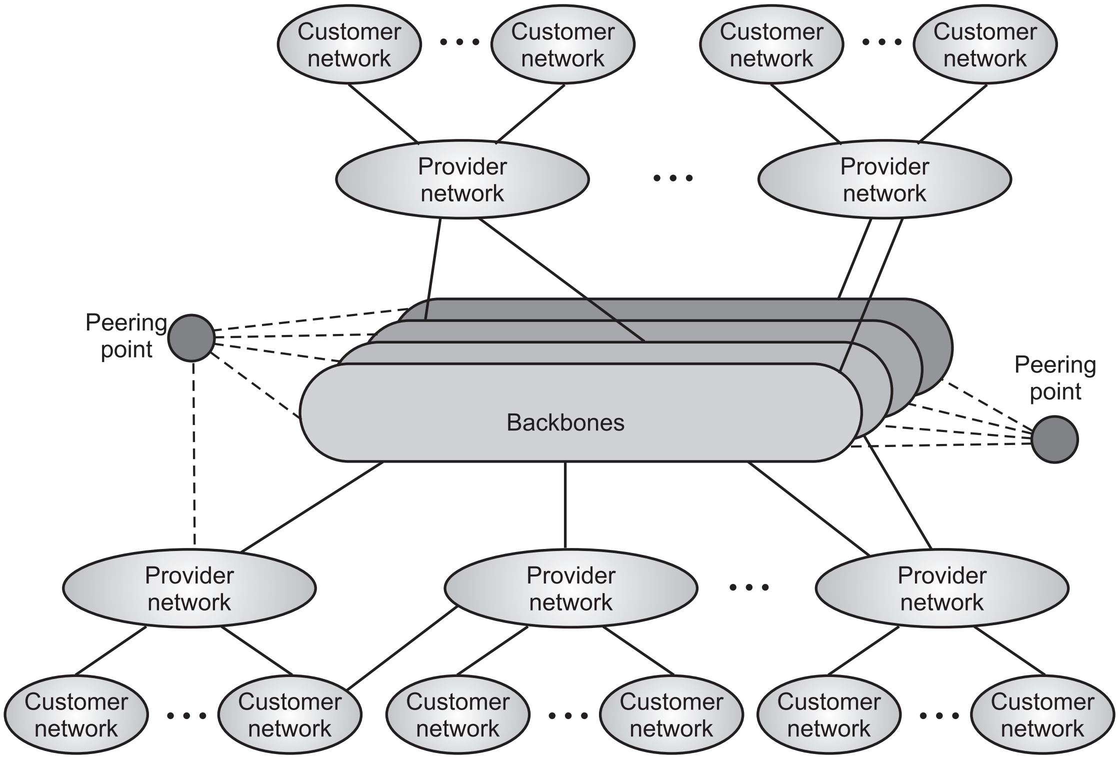


Fig. 1.1: Structure of Internet

- Hierarchical routing means considering each ISP as an Autonomous System (AS). Each AS can run a routing protocol that meets its needs, but the global Internet runs a global protocol to glue all ASs together.

- An Autonomous System (AS) is a group of networks and routers under the authority of a single administration.
- The routing protocol run in each AS is referred to as intra-AS routing protocol, intra-domain routing protocol or Interior Gateway Protocol (IGP).
- The global routing protocol is referred to as inter-AS routing protocol, inter-domain routing protocol or Exterior Gateway Protocol (EGP).
- Each AS is given an autonomous number (ASN) by the ICANN which is a 16-bit unsigned integer that uniquely defines an AS.

1.1.1 Architecture of Internet

- The Internet is a global network of computers connected. It allows people all over the world to communicate, share information, and access a huge amount of data.
- Internet is a world-wide global system of interconnected computer networks. The word 'Internet' is derived from two words namely, interconnection and networks. It is also referred to as 'Net'.
- Internet is a global network links thousands of computers at universities, research institutions, government agencies, business and houses throughout the world.
- Internet is a worldwide system of computer networks, i.e. a network of networks, which allows the participants (users) to share information.
- Fig. 1.2 shows architecture of Internet. A user/client can connect to the Internet using connection like telephone lines (DSL) which connecting to the ISP.

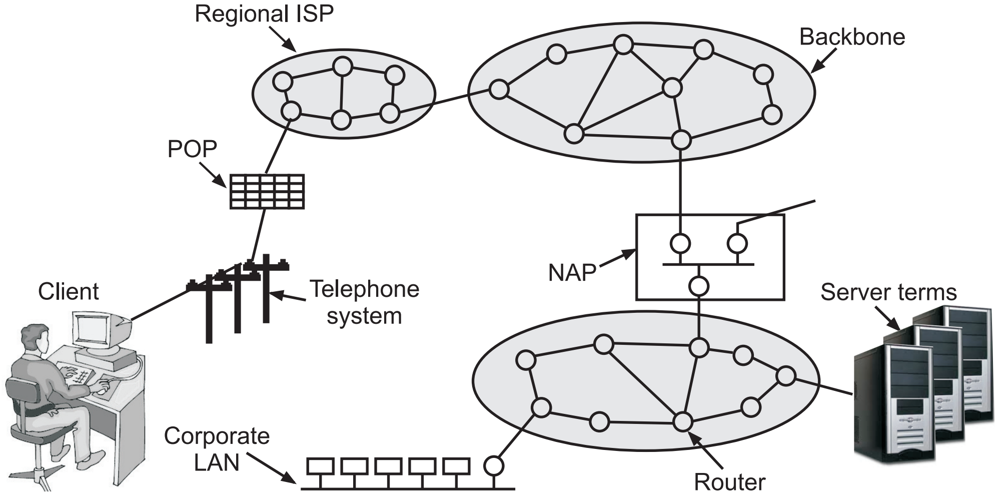


Fig. 1.2: Architecture of Internet

- The Internet is a truly global network that is joined by wired and wireless (e.g., satellite) networks of many ISPs (e.g., AT&T, British Telecom, Verizon).
- With its enormity and complexity, numerous routers on the Internet move IP packets between corporate networks and ISP networks, and between ISP networks.
- Depending on the geographical location of communicating hosts, IP packets have to pass through several ISP networks to reach their destinations.
- For the packet delivery across networks, ISPs have to work together, although they also have to compete with each other to attract more individual and corporate clients to their Internet access service.
- Today's Internet consists of a richly interconnected set of networks, mostly operated by Internet Service Providers (ISPs) exist mainly to provide service to “consumers” (i.e., individuals with computers in their homes.
- Backbones are large networks owned by communication companies such as BSNL and Airtel. Backbones and provider networks are also called Internet Service Providers (ISPs).

- An ISP network is composed of one or more Point-of-Presence (or POPs) as customer gateways to the Internet.
- The large ISP owns a number of POPs, each of which is literally a large structure (e.g. building) with its own internal high-speed LAN. Each POP houses different types of routers,
- A Network Access Point (NAP) is a crucial part of the internet's architecture / infrastructure, acting as a physical location where multiple internet service providers (ISPs) interconnect their networks to exchange data.
- NAP enabling efficient data exchange and connectivity between different internet service providers. ISP networks are coupled together for IP packets to travel across them to reach destinations.
- ISPs interconnect each other through designated access locations called Internet Exchange Points (IXPs) or through peering (See Fig. 1.2).
- The IXP or Internet Service Exchanges, also known as a Network Access Point (NAP) for a historical reason, is itself a high-speed LAN running on such speed standard as 10 Gigabit Ethernet installed in a building and becomes a junction point of participating ISP networks.
- The router constructs and maintains a routing table that enables decision-making regarding the delivery path of IP packets across an internet.
- An Internet Service Provider (ISP) is a company that provides individuals and organizations access to the Internet. The types of ISPs are explained below:
  - **National ISPs** operate within a specific country but may cover the entire nation. They offer a wide range of services and have extensive networks throughout the country, targeting both urban and rural areas. 'National ISPs provide regional/local ISPs with access to the Internet in exchange for contracted service fees.
  - **Regional ISPs** provide services within a specific region of a country, such as a state. They may focus on specific communities or areas, offering tailored services that meet local demand.
  - **Local ISPs** operate within a small area, such as a city or town (like municipal ISPs). They often provide personalized customer service and may offer unique plans that cater to the local population's needs.
- The local and regional ISPs provide Internet access to individual and business clients in a relatively limited geographical area by forwarding their IP packets to national ISPs' backbone networks.

How the Internet Works?

- The Internet is a technology that is considered to be a global system of interconnected computer networks.
- The internet is a global network of interconnected computers that communicate using standardized protocols like TCP/IP, enabling data transfer through packets routed by devices like routers and switches.
- The process of transferring information over the internet from one device to another relies on packet switching.
- Every device attempting to access the internet is initially linked either physically through cables or wirelessly.
- For instance, a computer can establish a physical connection to a modem using an Ethernet cable or connect wirelessly through Wi-Fi or Bluetooth signals.
- Data is transmitted across the internet in small units called "packets". Computers connected to the internet means that the systems are connected to computers' worldwide network. Therefore, each machine/device has its own or unique address.
- Each computer/device connected to the internet is also assigned a unique IP address that enables the device to be recognized. IP addresses are used to identify devices on the internet.
- Addresses of the internet are in the form "kkk.kkk.kkk.kkk," where each "kkk" ranges from 0-256. This structure of the internet address is known as an IP address (Internet Protocol).

- Fig. 1.3 describes the connection between two computers using the internet. Both systems have unique IP addresses. However, the internet is a unique object between both systems.

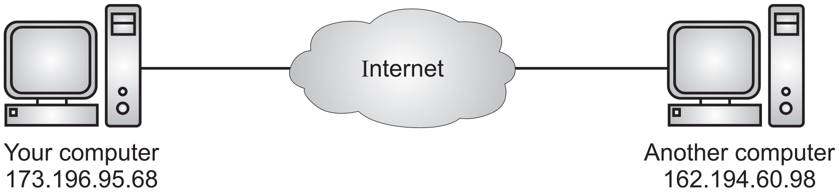


Fig. 1.3: Computer Connection via Internet

Components of Internet:

1. **Networks:** The internet is essentially a "network of networks," where smaller computer networks are interconnected globally.
2. **Devices:**
   - **Clients:** These are user devices like computers, smartphones, or tablets that access the internet.
   - **Servers:** Servers store websites, applications, and data. They respond to client requests by sending relevant data.
3. **Infrastructure:** Connections are established via physical cables (fiber optics, Ethernet), wireless signals (Wi-Fi, radio waves), and satellites.

- Following are the two versions of the Internet Protocol (IP) are in common uses in the Internet today:
  1. An **Internet Protocol version 4 (IPv4) address** is a 32-bits address that uniquely and universally defines the connection of a host or a router to the Internet.
  2. The growth of the Internet and the depletion of available IPv4 addresses, a new version of IP, **Internet Protocol version 6 (IPv6)**, using 128-bits for the IP address, was developed in 1995.
- The Internet is used on a vast level, and it is impossible to imagine our world without the Internet. Not only for personal use, organizations and government sectors are also connected to the internet and are providing us services.

1.1.2 Intranet

- An intranet is a private, secure network used by organizations to facilitate internal communication and information sharing among employees/members.
- Intranet is very efficient and reliable network system for any organization. Intranet is the system in which multiple PCs are connected to each other. PCs in intranet are not available to the world outside the intranet.
- Usually, each organization has its own Intranet network and members/employees of that organization can access the computers in their intranet.
- Intranet is defined as, private network of computers within an organization with its own server and firewall.
- Each computer in Intranet is also identified by an IP Address which is unique among the computers in that Intranet.
- An intranet operates similarly to the internet but is restricted to authorized users within the organization, ensuring data security.

Characteristics of an Intranet:

1. **Security:** An intranet incorporates security features such as user authentication, encryption and access controls to secure data/information and the company's strategic information.
2. **Remote Access:** Allows authenticated users to connect to the intranet remotely.

3. **Effective for Internal Communication:** An intranet is a dedicated private network to disseminate information within the organization.
4. **Collaboration Tools:** Intranets specifically designed to perform collaborative work like project management systems, shared workspaces, and collaborative document editing.
5. **Scalability:** Intranets are scalable to meet the changing needs of an organization.

How does the Intranet Work?

- The working of an Intranet depends on different components attached to its network. It works on client-server-based architecture.
- Fig. 1.4 shows working of Intranet. The components of Intranet are:
  1. **Client:** PCs (Personal Computers) users of an organization; these can consider as employees of the company who send requests to the server.
  2. **Server:** It is a kind of powerful computer which receives requests from multiple uses connected with the intranet. It processes multiple requests stores organizations' data and makes a central repository of files and documents to disseminate amongst users as and when required.
  3. **Firewall:** It is a security device which protects the intranet from unauthorized users.
  4. **Internet:** It is a global network which connects intranet from the global world.

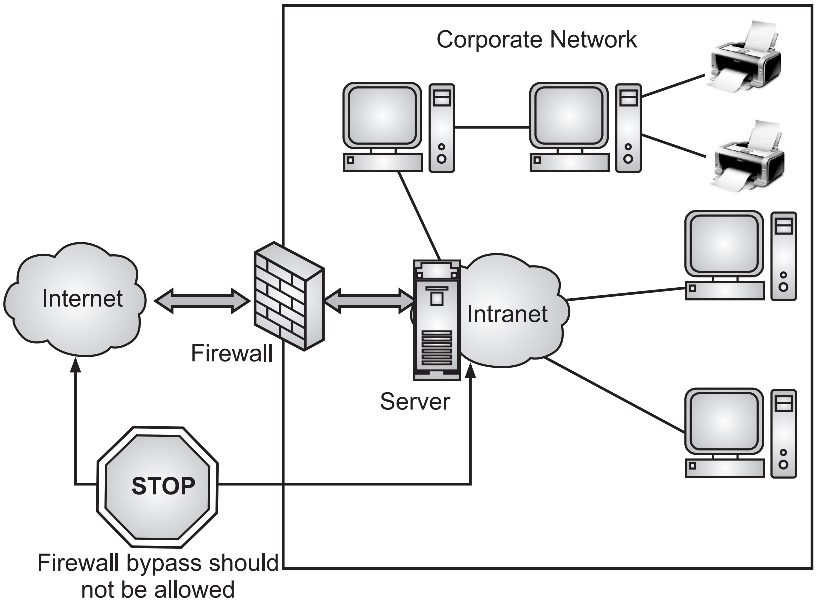


Fig. 1.4: Structure of Intranet

Benefits of Intranet:

1. **Improved Security**: Intranet provides a secure platform for sharing sensitive information. It protects sensitive organizational data from external threats. The information shared on intranet can only be accessed within an organization, therefore there is almost no chance of being theft.
2. **Collaboration:** Information is distributed among the employees as according to requirement and it can be accessed by the authorized users, resulting in enhanced teamwork.
3. **Enhanced Productivity**: Data is available at every time and can be accessed using company workstation. This helps the employees work faster.
4. **Improving Efficiency:** By providing a central location for employees to access the resources they need, intranets can help improve efficiency and productivity within an organization.
5. **Communication:** Intranet offers easy and cheap communication within an organization. Employees can communicate using chat, e-mail or blogs.
6. **Cost Savings:** Intranets can help reduce costs by eliminating the need for printed materials, such as documents and forms, and by streamlining processes that were previously done manually.

Disadvantages of Intranet:

1. **Limited Accessibility:** Because intranets are only accessible to the organization's employees, they may not be suitable for sharing information with external stakeholders, such as customers or partners.
2. **Dependence on Technology:** Intranets rely on technology, such as servers and network infrastructure, to function. If these technologies fail or experience problems, it could disrupt access to the Intranet.
3. **Maintenance and Management:** Intranets require ongoing maintenance and management to ensure that they are functioning correctly and that the content and resources on the Intranet are up-to-date. This can require a dedicated team of IT professionals or additional resources.
4. **High Cost for Smaller Organizations:** Implementing and maintaining an intranet can be expensive, particularly for smaller organizations.

Internet vs. Intranet

- Internet is a worldwide/global system of interconnected computer networks. An intranet serves as a private secure network used by organizations to facilitate internal operations.
- Following table differentiate between Intranet and Internet:

Sr. No.	Feature	Intranet	Internet
1.	Accessibility	Private (restricted to authorized users).	Public (accessible to anyone).
2.	What is?	A private network, within an Enterprise or Organization.	Worldwide/global system of connected networks.
3.	Purpose	Internal communication.	Global information sharing.
4.	Security	Highly secure (Firewalls, VPNs).	Less secure.
5.	User-base	Limited to organization members.	Open to all.
6.	Network	Localized Network.	Worldwide Network.
7.	Expensive	More expensive.	Less expensive.
8.	Content type	Organization-specific resources.	Diverse global content.
9.	Reliability	More reliability.	Less reliability.

1.1.3 Internet Service Provider (ISP) and its Role

- An Internet Service Provider (ISP) refers to an organization that offers various services to enable users to access and use the internet.
- ISPs can be privately owned, community-owned, commercial, or non-profit organizations.
- They offer common services, such as internet access, web hosting, internet transit, e-mail services, proxy servers, colocation, domain name registrations, and more.
- ISPs act as the gateway to the internet, enabling users to browse websites, stream videos, send emails, and perform other online activities.
- The main purpose of an ISP is to global connectivity of the Internet with high performance.

1.1.3.1 Role of Internet Service Provider (ISP)

- An ISP (internet service provider) is a company that provides individuals and organizations access to the internet and other related services.
- Internet Service Providers (ISPs) play a critical role in enabling individuals and organizations to access the internet and related services.
- They act as intermediaries between users and the global internet infrastructure, ensuring reliable connectivity and data transmission.

- A user can connect to the Internet either by dialing into an ISP's computer or by directly connecting to the ISP.
- ISPs are companies that provide users with internet connectivity. They operate the infrastructure, including the cables and routers needed to connect users to the global network.

Primary Roles of ISPs:

1. **Internet Access Provider:**
   - o ISPs offer internet connectivity through various technologies, including cable, DSL, fiber optic, satellite, and wireless networks.
   - o They provide bandwidth and speed options based on user needs, ensuring seamless access to online resources.
2. **Routing Data Traffic:**
   - o ISPs manage the routing of data packets between user devices and destination servers using IP addresses.
   - o They ensure efficient data transmission by determining the best path for packets across the network infrastructure.
3. **IP Address Allocation**:
   - o ISPs assign unique IP addresses to devices connected to their network, enabling identification and communication over the internet.
4. **Domain Name System (DNS) Services**:
   - o ISPs facilitate DNS operations, translating domain names (e.g., www.example.com) into numerical IP addresses for easier navigation.
5. **Network Management**:
   - o They maintain the physical infrastructure (routers, switches, servers) required for internet connectivity.
   - o Larger ISPs connect to backbone networks to ensure global reach and reliable service delivery.
6. **Web Hosting and Domain Registration**:
   - o Many ISPs offer services like hosting websites and registering domain names for businesses or individuals.
7. **Email Services**:
   - o ISPs often provide email accounts as part of their subscription packages.
8. **Security Features**:
   - o Some ISPs offer security solutions such as firewalls, antivirus software, and protection against cyber threats.

1.1.3.2 Working of ISP

- Fig. 1.5 shows how ISP works. Whether, to access the internet, reliable internet connection is needed.
- The devices like smartphone, laptop, IoT devices at home - everything needs to have an internet connection, which is provided by none other than ISPs.

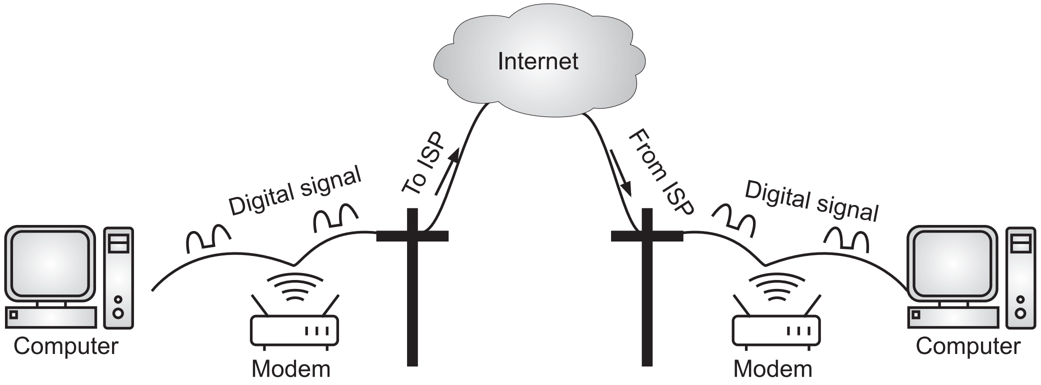


Fig. 1.5: Role of ISPs

- Following are some important factors to consider when choosing the right ISP:
  1. **Speed:** Ensure the ISP offers the bandwidth needed for the activities (e.g., streaming, gaming).
  2. **Coverage:** Availability in the area, especially in rural or remote regions.
  3. **Cost:** Pricing plans and any additional fees for installation or equipment.
  4. **Reliability:** Consistent connection with minimal downtime.
  5. **Customer Support**: Availability and quality of technical support.
- ISPs are categorized into tiers based on their network reach:

  Tier 1 ISPs: Own extensive physical networks with global reach; they form the backbone of internet infrastructure.

  Tier 2 ISPs: Connect regional or national customers by purchasing access from Tier 1 providers.

  Tier 3 ISPs: Focus on local markets by using higher-tier networks for connectivity.
- Worldwide example of ISPs includes:
  1. **United States:** Xfinity, Spectrum, Verizon, AT&T and CenturyLink.
  2. **India:** Jio, Airtel, BSNL, ACT Fibernet.
  3. **Europe:** BT (UK), Deutsche Telekom (Germany), Orange (France).
  4. **Global Satellite Providers:** Starlink, HughesNet, Viasat.

1.1.3.3 Types of ISP Internet Connection Providers

- Following are the different types of ISPs providers with connections available today:

Dial-Up Internet Connection Providers:

- A dial-up connection is one of the most common types of Internet connection offered by ISPs. The dial-up connection uses a telephone line to connect the computer to the Internet.
- In order to access using such a connection, a hardware device known as a modem is needed. A modem acts as an interface between the computer and a telephone line.
- A communication program instructs the modem to place a telephone call to a specific phone number provided by an ISP, establish a connection and then connect the computer to the Internet.

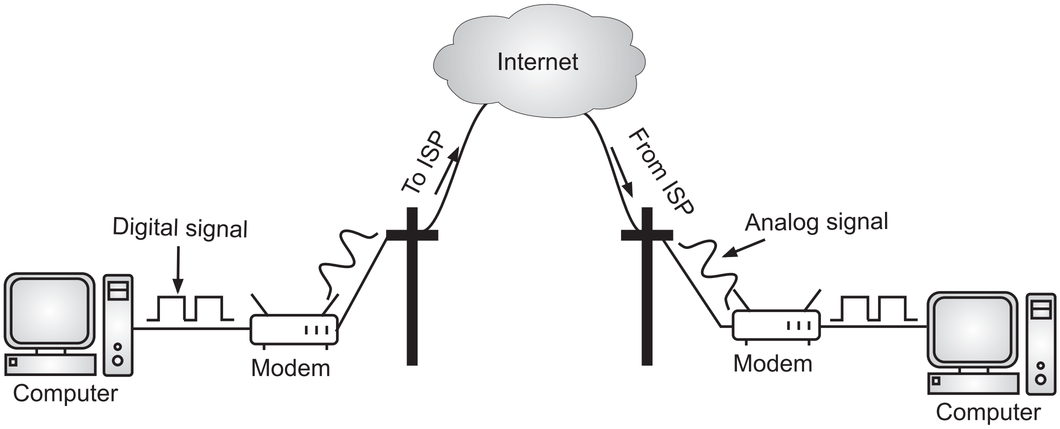


Fig. 1.6: Dial-up Connection using ISP

- The dial-up connection uses either the SLIP (Serial Line Internet Protocol) or PPP (Point to Point Protocol) protocols. However, most of the dial up connections are PPP protocol.

  Advantages of Dial-up Internet Connection Providers:
  1. It is the inexpensive in form of Internet access.
  2. It is fast enough to read information and download small files.
  3. Hardware cost in establishing such a connection is minimum.
  4. It is easy to set up and most widely available many ISPs provide this type of service.

Disadvantages of Dial-up Internet Connection Providers:

1. Using dial-up connection, cannot use the Internet and receive phone calls simultaneously.
2. It is the slowest connection available, especially when multiple users on the network need to access the Internet.
3. Dial-up connection has very slow means 56 kbps is the maximum internet speed.

DSL Internet Connection Providers:

- DSL (Digital Subscriber Line) which has emerged as a new Internet access technology that has brought high connection speeds to home users and business organizations.
- DSL is one of the most common forms of broadband connection as it provides fast Internet access over ordinary telephone lines.
- Fig. 1.7 shows DSL connection, enables internet connection through a telephone line. The services are widely available because houses are wired for phone connections already. It's provided by traditional phone companies (ISPs).
- The DSL technology leverages extra signals that telephone signals don't use. It utilizes a DSL router to connect to a telephone jack through a phone cable.
- These capabilities enable the users to use the internet even when using their telephones or the telephone is ringing.
- The telephone company uses a Digital Subscriber Line Access Multiplexer (DSLAM) at its end office so that multiple DSL users can be connected to the high-speed backbone network.
- DSL filters are used on customer premises with non-DSL connections. DSL uses analog sinusoidal carrier waves for data transmission. The waves are modulated and demodulated at the customer premises with DSL modems.

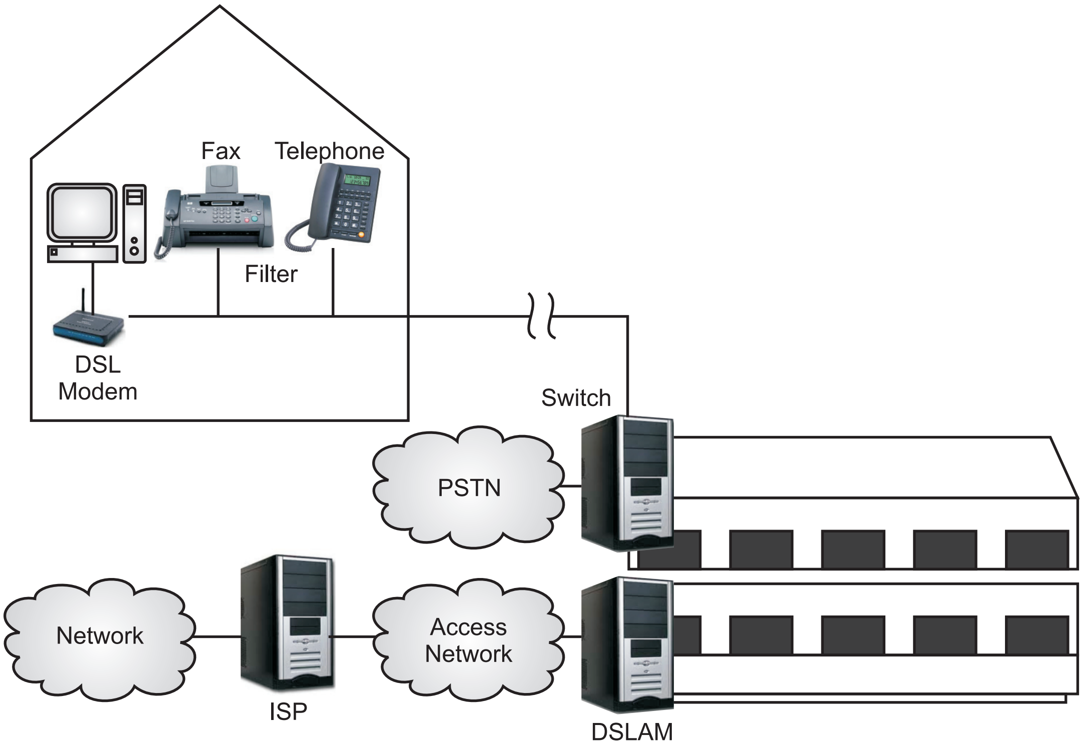


Fig. 1.7: DSL (Digital Subscriber Line) Connection

- ADSL (Asymmetric DSL) is the most popular and widely used high speed broadband connection that allows digital information to be sent at a very high speed over ordinary phone lines.
- DSL uses higher frequency bands for transmission of data in the range of 25 KHz to 1.5MHz. Voice transmission occurs at less than 4 KHz. So, data transmission occurs simultaneously with voice transmission.

Advantages of DSL Internet Connection Providers:

1. DSL is faster than ISDN and dial-up connection.
2. It allows us to use a telephone and Internet simultaneously.
3. DSL provides a consistent and stable internet speed.

Disadvantages of DSL Internet Connection Providers:

1. DSL has availability only in limited areas.
2. It is expensive in terms of setup and equipment costs.

Broadband Internet Connection Providers (ISDN):

- ISDN connection provides better speeds and higher quality than traditional connections like a dial-up connection
- ISDN (Integrated Services Digital Network) also establishes a connection to the ISP over a phone line when required.
- ISDN establishes the connection using the phone lines which carry digital signals instead of analog signals.
- Fig. 1.8 shows accessing internet using ISDN connection. It uses following components:
  - **Modem** is a device that modulates and demodulates signals for encoding and decoding digital data transmitted over a telephone line or cable system.
  - **Router** is a device that routes data from a local network to the internet and vice versa, often includes Wi-Fi capabilities.
  - The **ISP (Internet Service Provider)** is the company that provides internet access to customers.

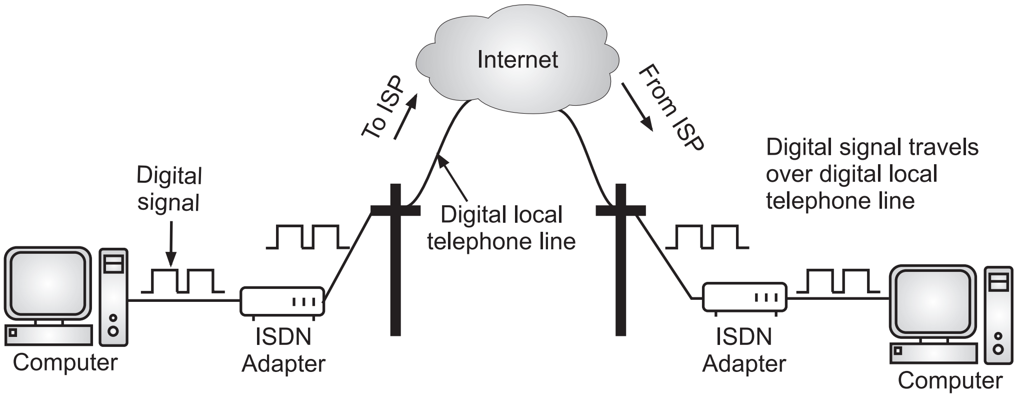

Internet
To ISP
From ISP
Digital signal travels over digital local telephone line
Digital signal
Digital local telephone line
Computer
ISDN Adapter
ISDN Adapter
Computer

Fig. 1.8: ISDN Connection

Advantages of ISDN Internet Connection Providers:

1. ISDN provides faster data transfer rates than traditional dial-up (maximum speed is upto 128 Kbps).
2. It establishes connections faster than dial-up modems.
3. ISDN is reliable because it offers a stable and consistent connection.
4. It handles voice, video, and data simultaneously.

Disadvantages of ISDN Internet Connection Providers:

1. ISDN is difficult to set up and troubleshoot.
2. It is expensive as compared to dial-up connection as per minute charges can make it costly when a lot of Internet access is required.
3. It has limited expendability/scalability (suitable for accessing the Internet in a LAN provided a limited number of computers (2 to 6) are attached to it and depending upon the usage).

Cable TV Internet Connection Providers:

- Fig. 1.9 shows that how internet is accessed using Cable TV connection.

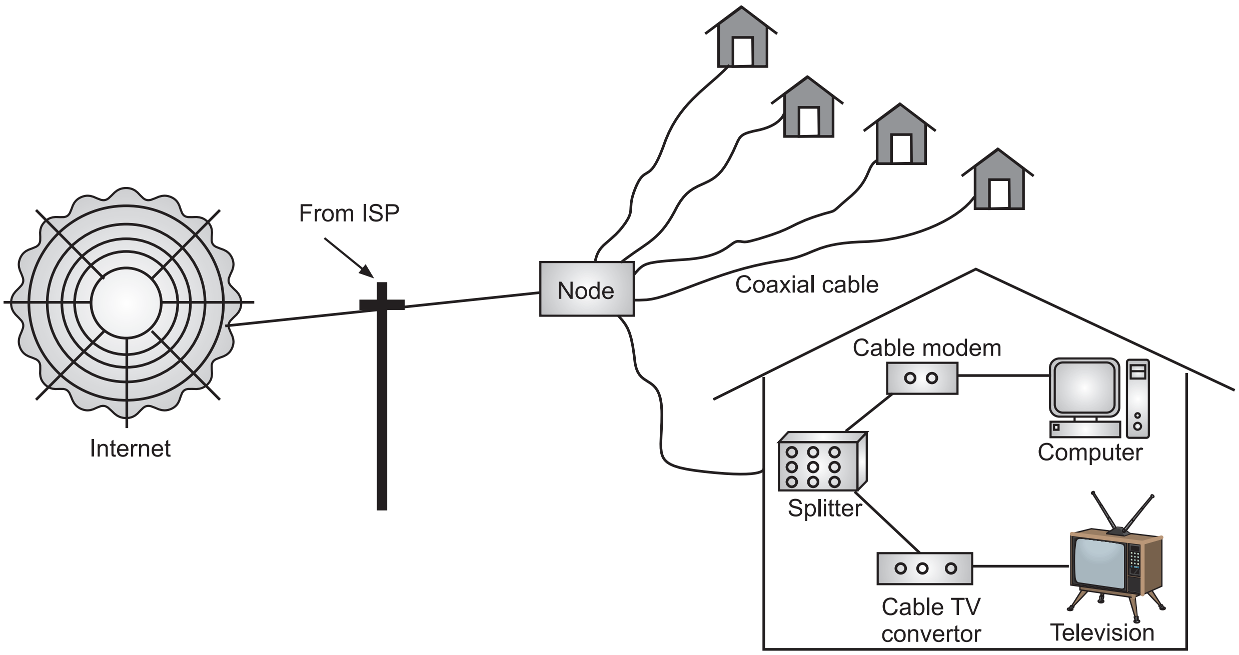


Fig. 1.9: Cable TV Connection

- Cable TV Internet connection is provided through Cable TV lines. It uses coaxial cable which is capable of transferring data at much higher speed (ranges from 256 Kbps to 1 Mbps) than common telephone line.
- Cable TV companies generally offer broadband cable services. Broadband cables use coaxial cables, which deliver cable TV to homes.
- The Internet service providers also offer internet services that are reliable and fast to help to perform a variety of operations at home or office.
- Cable TV uses a cable modem used to access this service, provided by the cable operator.
- The Cable modem comprises of two connections namely, one for internet service and other for Cable TV signals.
- Since Cable TV internet connections share a set amount of bandwidth with a group of customers, therefore, data transfer rate also depends on number of customers using the internet at the same time.

Advantages of Cable TV Internet Connection Providers:

1. In Cable TV the data transfer speed is very fast.
2. Cable TV provides continuous and instantaneous connectivity i.e. connection is always ON.

Disadvantages of Cable TV Internet Connection Providers:

1. Its initial cost may be high.
2. As the connection may be shared by multiple customers this may slow down the connection to the Internet during peak time.
3. Only available in areas with Cable TV connections.

Satellite Internet Connection Providers:

- Satellite Internet connection offers high speed connection to the internet. Satellite internet providers utilize geostationary satellites for data transmission between the internet and users.
- Satellite Internet connection is the most expensive alternative for getting a high-speed connection to the Internet.
- Satellite connection speeds range from 512k to 2.0 Mbps. Several companies, such as HughesNet, Viasat, and Starlink, offer satellite internet services.
- Fig. 1.10 shows how internet is accessed using satellite internet connection.

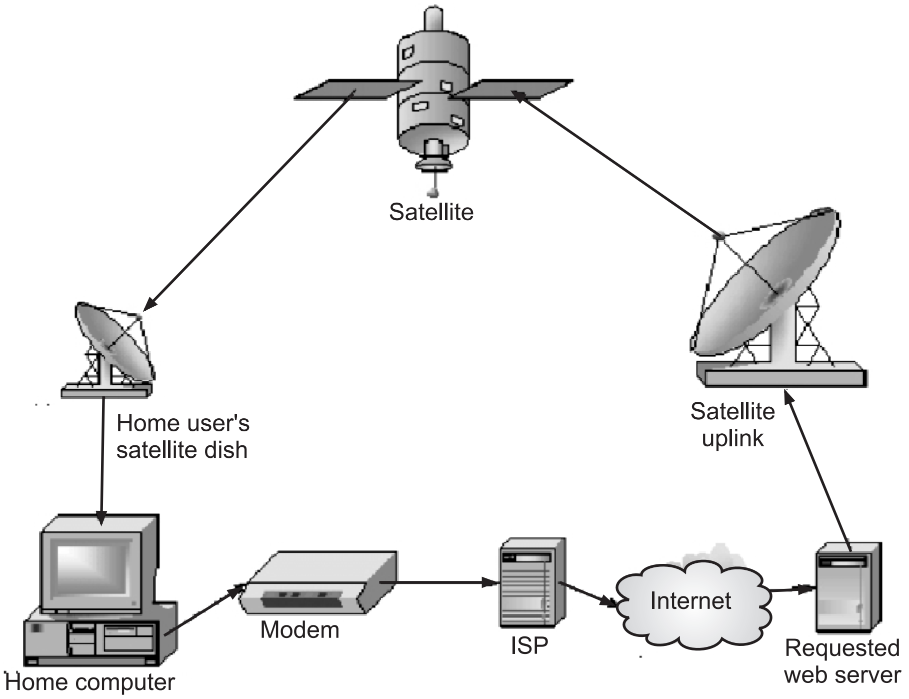


Fig. 1.10: Satellite Connection

Advantages of Satellite Internet Connection Providers:

1. Satellite internet connection has global coverage and can provide internet access almost anywhere.
2. Once properly set up, satellite internet provides a stable and consistent connection.
3. Satellite networks can be scaled easily, allowing for upgrades in service or the addition of more users without significant changes to local infrastructure.
4. Satellite internet connection is especially useful for organizations and individuals who need internet access while traveling, such as in remote areas, on ships, planes etc.

Disadvantages of Satellite Internet Connection Providers:

1. It is more expensive to set up than other high-speed Internet connections.
2. The speed can be severely impacted by weather conditions.
3. It can constantly be disturbed by limited bandwidth.

Wireless Internet Connection Providers:

- With the recent advancement in wireless technology, the high-speed Internet access is not limited to the desktop but it is now accessible on laptops, PDA's, mobiles also.
- Wireless Internet is the broadband Internet connection that use the radio frequency bands to connect to the Internet instead of using a telephone line or a cable network.
- Wireless Internet Connection makes use of radio frequency bands to connect to the internet and offers a very high speed (more than 10 Mbps).
- The wireless internet connection can be obtained by either WiFi or Bluetooth.
  - The ISP provider also offers Wi-Fi connections. Multiple users can access Wi-Fi connectivity with ease and flexibility. Wi Fi wireless technology is based on IEEE 802.11 standards that allows the Smartphone, PDA or computer to access the Internet through a wireless connection. It uses radio signals to send and receive data between your enabled device and the WAP (Wireless Access Point). Wi-Fi connections bring benefits such as mobility, flexibility and scalability, enabling numerous devices to connect concurrently.

- Bluetooth wireless technology makes use of short-wavelength radio waves and helps to create personal area network (PAN).

Advantages of Wireless Internet Connection Providers:

1. It provides greater mobility and covers a very long distance.
2. It is an extremely fast connection.

Disadvantages of Wireless Internet Connection Providers:

1. It has limited availability Wi-Fi or Bluetooth connection is usually available in public areas like airports, railways stations etc.
2. Slower in speed and limited range for connectivity.

Mobile Hotspot Internet Connection:

- Using a mobile hotspot, we can create a mobile hotspot by using your smartphone's data connection to connect the laptop to the Internet and this process is called "tethering."

1.1.4 Internet Corporation for Assigned Names and Numbers (ICANN)

- The Internet Corporation for Assigned Names and Numbers (ICANN) is a global non-profit organization. It manages and coordinates certain key elements of the internet. It was set up in 1998.
- ICANN plays a crucial role in maintaining the stability, security, and interoperability of the internet. It oversees the domain name system (DNS). DNS is the naming system used to identify websites and resources on the internet.
- Some of the major functions/roles of ICANN include the following:
  1. Managing and coordinating the domain name system (DNS) includes the assignment of domain names and the operation of the root server system.
  2. Allocating IP addresses and managing the global internet protocol address space.
  3. Setting technical standards and protocols for the internet's operation and ensuring their implementation.
  4. Accrediting and regulating domain name registrars and registries.
  5. Facilitating the introduction of new top-level domains (TLDs). Managing the process of their delegation.
  6. Ensuring that domain names and IP addresses are unique and accessible globally.
- The advisory bodies of ICANN include the following:
  1. **Governmental Advisory Committee (GAC):** Comprises representatives from national governments. Advises ICANN on public policy matters related to the internet.
  2. **Generic Names Supporting Organization (GNSO):** Represents the interests of non-country-code top-level domain registries, registrars, businesses, and individual internet users. It develops and recommends policies on generic TLDs.
  3. **Country Code Names Supporting Organization (ccNSO):** Represents country code and top-level domain managers. It helps develop policies specific to country code TLDs.
  4. **At-Large Advisory Committee (ALAC):** Represents the interests of individual Internet users and provides input on policy development.
  5. **Security and Stability Advisory Committee (SSAC):** Advises ICANN on matters related to the security and stability of the DNS and the internet infrastructure.

1.2 IPv4 AND IPv6 [S-22, W-22, S-23, W-23, W-24]

- The Internet Protocol (IP) is a protocol or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.
- Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place.

- Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.
- Once the packets arrive at their destination, they are handled differently depending on which transport protocol is used in combination with IP. The most common transport protocols are TCP and UDP.
- The Internet Protocol is responsible for addressing host interfaces, encapsulating data into datagrams, (including fragmentation and reassembly) and routing datagrams from a source host interface to a destination host interface across one or more IP networks. For these purposes, the Internet Protocol defines the format of packets and provides an addressing system.
- Internet Protocol is connectionless and unreliable protocol. It ensures no guarantee of successfully transmission of data.
- In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.
- Fig. 1.11 shows the position of IP in TCP/IP Protocol suite.

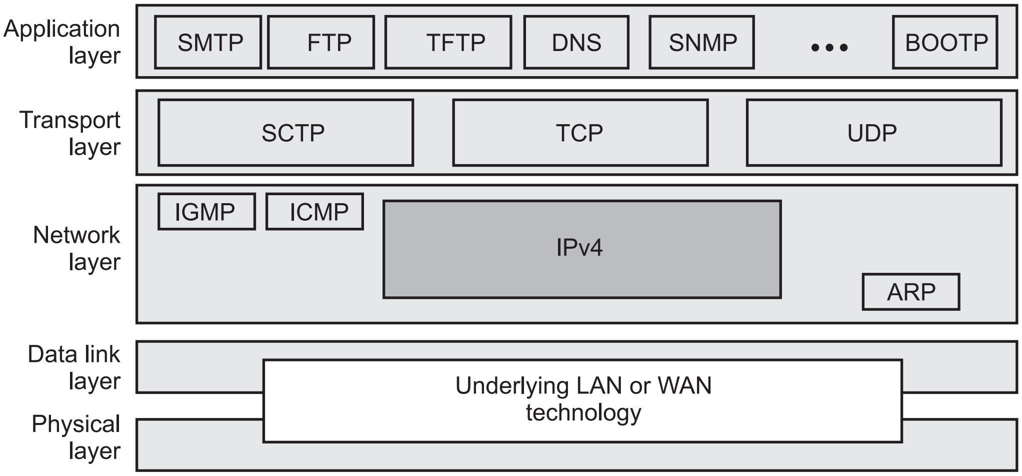


Fig. 1.11: Position of IP in TCP/IP Protocol Suite

- The Internet Protocol is a set of rules that allows our computers to communicate via the Internet. IPv4 and IPv6 are the two versions of the Internet Protocol (IP) are in common uses in the Internet today.
- IPv4 is a major protocol in the TCIP/IP suite. IPv4 addresses provide a way to uniquely identify the hosts in a network. IPv4 uses 32-bit logical addresses. IPv6 provides 128-bit IP addresses.

1.2.1 IPv4 Header Format [S-23, S-24, W-24]

- Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed.
- Packets in the network (internet) layer are called datagrams. The IP datagram format is shown in Fig. 1.12.
- A datagram is a variable-length packet consisting of two parts namely, header and data. The header is 20 to 60 bytes in length and contains information essential to routing and delivery.

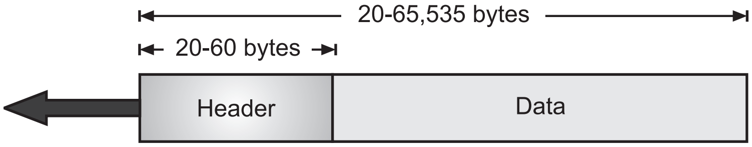


Fig. 1.12: IP Datagram

IPv4 Header Format:

- A 20-byte header contains almost 13 multipurpose fields, which hold specific related object information such as application, data type and source/destination addresses.

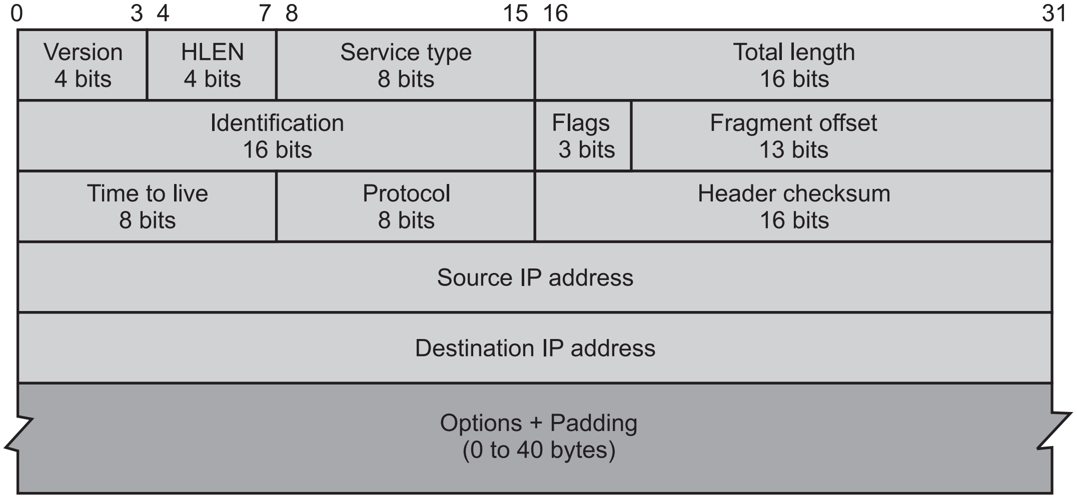


Fig. 1.13: IPv4 Header Format

- IP header format contains following fields:

1. **Version:** This contains the Internet header format and uses only four packet header bits. This 4-bit field defines the version of the IP protocol. Currently the version is 4. However, version 6 (or IPv6) may totally replace version 4 in the future. This field tells the IP software running in the processing machine that the datagram has the format of version 4.
2. **Header Length (HLEN):** This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable, (between 20 and 60 bytes). When there are no options, the header length is 20 bytes and the value of this field is 5 (5 × 4 = 20). When the option field is at its maximum size, the value of this field is 15 (15 × 4 = 60).
3. **Type Of Service (TOS):** This provides network service parameters. The TOS field is composed of a 3-bit precedence field (which is ignored today), 4 TOS bits and an unused bit that must be 0. The 4 TOS bits are:
   - 1000: Minimize delay.
   - 0100: Maximize throughput.
   - 0010: Maximize reliability.
   - 0001: Minimize monetary cost.
   - 0000: Normal service.
4. **Total Length:** This contains combined data and header length. This is a 16-bit field that defines the total length (header plus data) of the IP datagram in bytes. The header length can be found by multiplying the value in the HLEN field by four.

   Length of Data = Total Length – Header Length
5. **Identification:** This 16-bit field contains a specific number for primary data identification. Uniquely identify the datagram. Usually, it is increased by 1 each time a datagram is sent. All fragments of a datagram contain the same identification value. This allows the destination host to determine which fragment belongs to which datagram.
6. **Flags:** This router fragment activity is controlled by following three flags:

Sr. No.	Flag	Description
1.	0	Reserved, must be zero.
2.	DF (Do not Fragment)	0 means allow fragmentation; 1 means do not allow fragmentation.
3.	MF (More Fragments)	0 means that this is the last fragment of the datagram; 1 means that additional fragments will follow.

7. **Fragmentation OFFset:** This is a fragment identification via offset value. This is used to aid the reassembly of the full datagram. The value in this field contains the number of 64-bit segments (header bytes are not counted) contained in earlier fragments. If this is the first (or only) fragment, this field contains a value of zero.
8. **Time To Live (TTL):** This contains the total number of routers allowing packet pass-through. The time-to-live field or TTL, sets an upper limit on the number of routers through which a datagram can pass. It limits the lifetime of the datagram. It is initialized by the sender to some value, (often 32 or 64) and decremented by one by every router that handles the datagram. When this field reaches 0, the datagram is thrown away, and the sender is notified with an ICMP message. This prevents packets from getting caught in routing loops forever.
9. **Protocol:** This 8-bit field contains header transport packet information. This 8-bit field defines the higher-level protocol that uses the services of the IP layer. An IP datagram can encapsulate data from several higher level protocols such as TCP, UDP, ICMP, and IGMP. This field specifies the final destination protocol to which the IP datagram should be delivered. In other words, since the IP protocol multiplexes and de-multiplexes data from different higher-level protocols, the value of this field helps in the de-multiplexing process when the datagram arrives at its final destination.

Protocol	Description
0	Reserved.
1	Internet Control Message Protocol (ICMP).
2	Internet Group Management Protocol (IGMP).
3	Gateway-to-Gateway Protocol (GGP).
4	IP (IP encapsulation).
5	Stream.
6	Transmission Control Protocol (TCP).
8	Exterior Gateway Protocol (EGP).
9	Private Interior Routing Protocol.
17	User Datagram Protocol (UDP).
41	IP Version 6 (IPv6).
50	Encap Security Payload for IPv6 (ESP).
51	Authentication Header for IPv6 (AH).
89	Open Shortest Path First.

10. **Header Checksum:** It checks and monitors communication errors. The header checksum is calculated over the IP header only. It does not cover any data that follows the header. ICMP, IGMP, UDP, and TCP all have a checksum in their own headers to cover their header and data. To compute the IP checksum for an outgoing datagram, the value of the checksum field is first set to 0. Then the 16-bit one's complement sum of the header is calculated (i.e., the entire header is considered a sequence of 16-bit words). The 16-bit one's complement of this sum is stored in the checksum field. When an IP datagram is received, the 16-bit one's complement sum of the header is calculated. Since the receiver's calculated checksum contains the checksum stored by the sender, the receiver's checksum is all one bits if nothing in the header was modified. If the result is not all one bits (a checksum error), IP discards the received datagram. No error message is generated. It is up to the higher layers to somehow detect the missing datagram and retransmit.

11. **Source Address:** It stores source IP address. This 32-bit field defines the IP address of the source. This field must remain unchanged during the time the IP datagram travels from the source host to the destination host.
12. **Destination Address:** It stores destination IP address. This 32-bit field defines the IP address of the destination. This field must remain unchanged during the time the IP datagram travels from the source host to the destination host.
13. **Options:** This is the last packet header field and is used for additional information. When it is used, the header length is greater than 32 bits.

1.2.2 IPv6 Header Format [S-22, W-22, S-23, W-23, S-24, W-24]

- Internet Protocol version 6 is a new addressing protocol designed to incorporate all the possible requirements of future Internet known to us as Internet version 2. This protocol as its predecessor IPv4.
- IP version 6 (IPv6) is the latest version of IP. IP enables numerous nodes on different networks to interoperate seamlessly.
- IP version 4 (IPv4) is currently used in intranets and private networks, as well as the Internet. IPv6 is the successor to IPv4, and is based for the most part on IPv4.
- IPv4 has been widely deployed and used to network the Internet today. With the rapid growth of the Internet, enhancements to IPv4 are needed to support the influx of new subscribers, Internet-enabled devices, and applications. IPv6 is designed to enable the global expansion of the Internet.
- IPv6 builds upon the functionality of IPv4, providing improvements to addressing, configuration and maintenance, and security.
- IPv6 packet headers contain many of the fields found in IPv4 packet headers; some of these fields have been modified from IPv4.
- Pv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header.
- The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.

IPv6 Fixed Header:

- Fig. 1.14 shows the 8 fields that are available in the 40-byte IPv6 header.

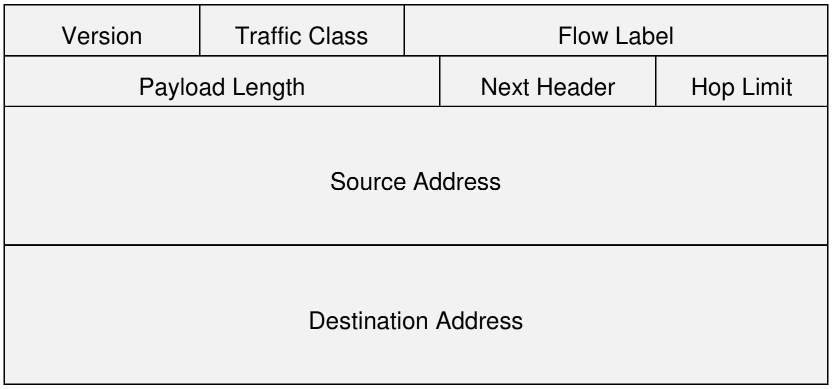


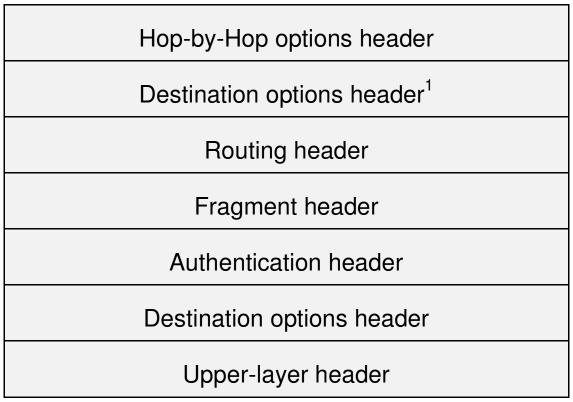
Fig. 1.14: IPv6 Packet Headers

- IPv6 fixed header is 40 bytes long and contains the following information.
  1. **Version (4-bits):** It represents the version of Internet Protocol, i.e. 0110.
  2. **Traffic Class (8-bits):** These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).

3. **Flow Label (20-bits):** This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.
4. **Payload Length (16-bits):** This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
5. **Next Header (8-bits):** This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4s.
6. **Hop Limit (8-bits):** This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.
7. **Source Address (128-bits):** This field indicates the address of originator of the packet.
8. **Destination Address (128-bits):** This field provides the address of intended recipient of the packet.

IPv6 Extension Headers: **[S-23, S-24]**

- In IPv6, extension headers are used to encode optional Internet-layer information. Extension headers are placed between the IPv6 header and the upper layer header in a packet.
- Extension headers are chained together using the next header field in the IPv6 header. The next header field indicates to the router which extension header to expect next.
- If there are no more extension headers, the next header field indicates the upper layer header (TCP header, User Datagram Protocol [UDP] header, ICMPv6 header, an encapsulated IP packet, or other items).
- The sequence of Extension Headers should be:


Hop-by-Hop options header
Destination options header[1]
Routing header
Fragment header
Authentication header
Destination options header
Upper-layer header

- These headers:
  1. should be processed by First and subsequent destinations.
  2. should be processed by Final Destination.
- Extension Headers are arranged one after another in a linked list manner, as depicted in Fig. 1.15.

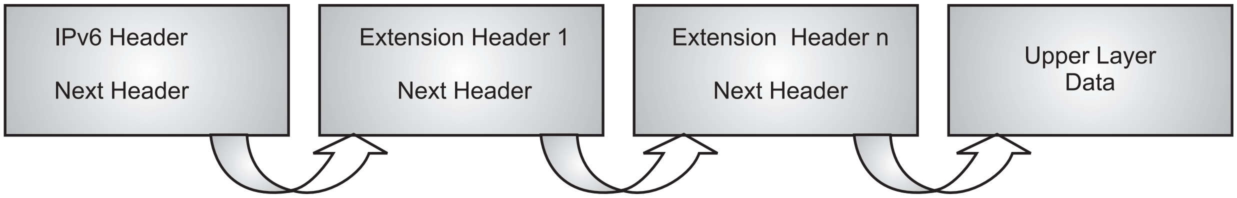


Fig. 1.15: Extension Headers Connected Format

Difference between IPv4 and IPv6:

- IPv4 has an address length of 32-bit represented in decimal format. IPv6 has a 128-bit address length represented in hexadecimal format. There are a lot more benefits of using IPv6 over IPv4. That are:
  - IPv6 has a large range of addresses.
  - It provides auto-configuration so it is easier to manage and cheaper than IPv4.
  - It provides end-to-end transparency of users due to the possibility of direct addressing.
  - It has improved security structures like IPSEC is built-in with key features.
  - It provides mobility of addresses with inter-operability with embedded networking devices.
  - It delivers flexibility and scalability features with a large range of addresses.
- Following table illustrates the difference between IPv4 and IPv6: **[S-22, W-23, S-24]**

Parameters	IPv4	IPv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon (:).
Classes	IPv4 has five different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask (means that IPv4 converts IP addresses into a subnet of different sizes)).	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	IPv6 is multicasting, which provides efficient network operations.

Contd...

Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets.
Use in Industry	Many companies have historically used and continue to use IPv4, including major tech companies like Apple, Microsoft, and Google, as well as other organizations like Ford Motor Company and AT&T.	These addresses are used by Comcast, Reliance Jio, T-Mobile USA, Sky broadband, Claro, Softbank, Orange, SK telecom, Cox communication, Kabel Deutschland and many more.

1.3 SUBNET AND SUBNET ADDRESSING

- A subnet, or subnetwork, is a logical subdivision of an IP network. Subnetting is the process of dividing a larger network into smaller, more manageable segments, each with its own unique range of IP addresses.
- A subnet (subnetwork) is a smaller network within a larger network. It helps organize and manage IP addresses more efficiently.
- Subnet Addressing (or Subnetting) is the process of dividing an IP network into smaller subnetworks by borrowing bits from the host portion of an IP address.

Concept of IP Address and IP Addressing: **[S-22, S-23, W-23, S-24]**

- IP addressing is the method used to identify hosts and network devices. The number of hosts connected to the internet continues to grow and the IP addressing scheme has been adapted over time to cope this growth.
- In this topic, we study IP addressing in detail with IPv4 address. The IPv4 addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the internet.
- An IP address is an address used to uniquely identify a device on an IP network. An IP address is a numerical (32 bits) representation that uniquely identifies a specific interface on the network.
- A 32-bit IP address actually consists of following two parts:
  1. **Network ID (or Network Address):** Identifies the network on which a host computer can be found.
  2. **Host ID (or Host Address):** Identifies a specific device on the network indicated by the network ID.

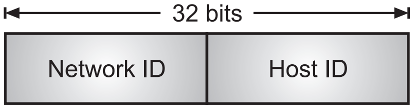


Fig. 1.16 (a): Parts of an IP Address

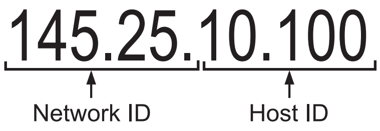


Fig. 1.16 (b): Example of an IP Address

Address Space:

- A protocol like IPv4 that defines addresses has an address space.
- An address space is the total number of addresses used by the protocol. If a protocol uses N bits to define an address, the address space is 2N because each bit can have two different values (0 or 1) and N bits can have 2N values.
- IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4 billion).

- Theoretically, if there were no restrictions, more than 4 billion devices could be connected to the Internet.
- In classful addressing the addressing space is divided into five classes as shown in Fig. 1.17.
- In the Fig. 1.17, we can see that Class A covers half of the address space, Class B covers 1/4 of the whole address space, Class C covers 1/8 address space and Classes D and E cover 1/16 of the address space.

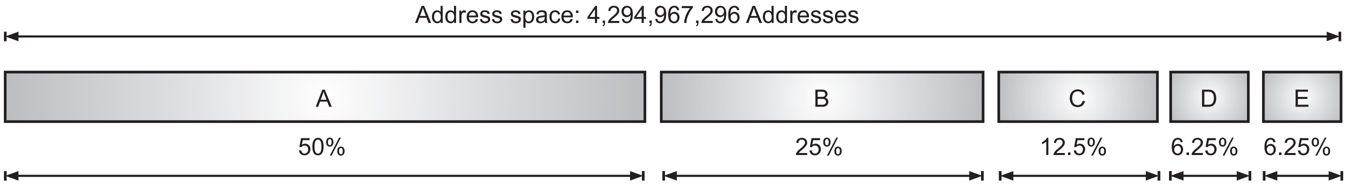


Fig. 1.17: Occupation of the Address Space in Classful Addressing

- Following table shows the number of addresses in each class:

Sr. No.	Class	Number of Addresses
1.	A	2^{31} = 2,147,483,648
2.	B	2^{30} = 1,073,741,824
3.	C	2^{29} = 536,870,912
4.	D	2^{28} = 268,435,456
5.	E	2^{28} = 268,435,456

Notations:

- There are three common notations to show an IPv4 address namely, binary notation (base 2), dotted-decimal notation (base 256), and hexadecimal notation (base 16).
- Fig. 1.18 shows all the three notations for IPv4 address.
- The notations for IP address are explained below:

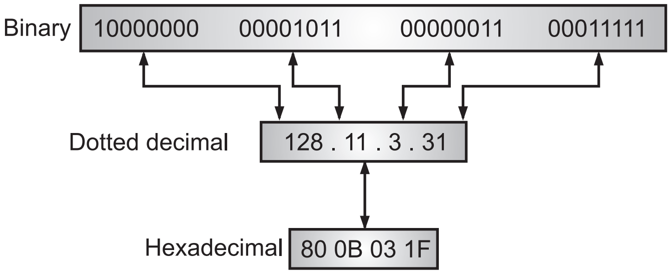


Fig. 1.18: Three Notations of IPv4 Addressing

1. **Binary Notation (Base 2):** Binary notation is the format that systems on the network use to process the address. In binary notation the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So, it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address. An example of binary notation is 01110101.10010101.00011101.11101010.
2. **Hexadecimal Notation (Base 16):** We sometimes see an IPv4 address in hexadecimal notation. Each hexadecimal digit is equivalent to four bits. This means that a 32-bits address has 8 hexadecimal digits. This notation is often used in network programming. An example of hexadecimal notation of an IPv4 address is C0.A8.01.64.
3. **Dotted-decimal Notation (Base 256):** To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the

bytes. Dotted-decimal notation is the format that is typically used for displaying the IP address in a human-readable format. An example of dotted-decimal notation is 192.168.1.100.

Classful Addressing: **[S-22, S-23, W-23, W-24]**

- As address is of the form (Net ID, Host ID), where Net ID identifies the network and Host ID identifies the host on the network. This addressing scheme is also referred to as the classful addressing scheme that is self-identifying.
- IP addresses, when started a few decades ago, used the concept of classes. This architecture is called classful addressing.
- Three types of classful addresses are Class A, Class B and Class C. IP addresses previously had one of the first three forms shown in Fig. 1.19 as per the original addressing scheme.
- Classful addressing, the address space is divided into five classes A, B, C, D, and E. IP addresses, when started a few decades ago, used the concept of classes. This architecture is called Classful addressing.
- In class A, the network length is 8 bits, but since the first bit, which is 0, defines the class, we can have only seven bits as the network identifier. This means there are only 27 = 128 networks in the world that can have a class A address.
- In class B, the network length is 16 bits, but since the first two bits, which are (10)2, define the class, we can have only 14 bits as the network identifier. This means there are only 214= 16384 networks in the world that can have a class B address.
- All addresses that start with (110)2, belong to class C. In class C, the network length is 24 bits, but since three bits define the class, we can have only 21 bits as the network identifier. This means there are 221= 2,097,152 networks in the world that can have a class C address.
- Class D is not divided into NetworkID and HostID. It is used for multicast addresses. All addresses that start with 1 1 1 1 in binary belong to class E. As in Class D, Class E is not divided into NetworkID and HostID and is used as reserve.
- In classful addressing, an IP address in classes A, B, and C is divided into NetworkID and HostID. These parts are of varying lengths, depending on the class of the address. Fig. 1.19 shows the Netid and Hostid bytes.

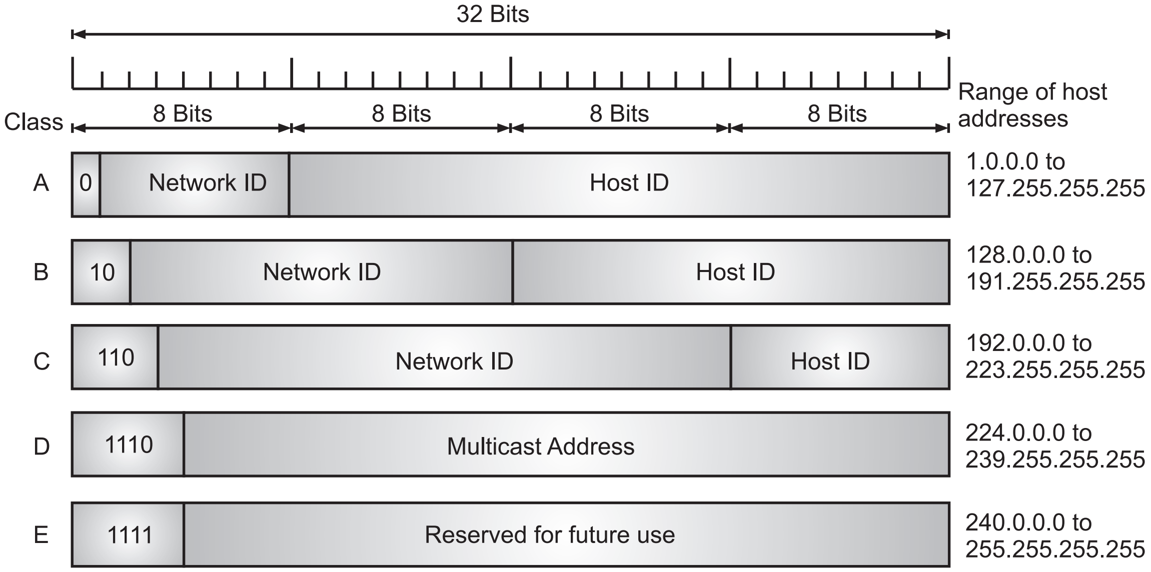
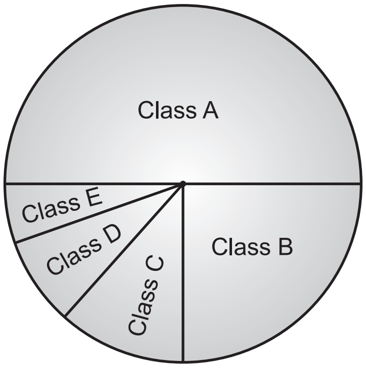


Fig. 1.19: Classful Addressing

- In classful addressing, the address space is divided into five classes A, B, C, D, and E as shown in Fig. 1.20. Each class in classful addressing, occupies some part of the whole address space. Fig. 1.20 shows the class occupation of the address space.



Class A: 2^{31} = 2,147,483,648 addresses, 50%

Class B: 2^{30} = 1,073,741,824 addresses, 25%

Class C: 2^{29} = 536,870,912 addresses, 12.5%

Class D: 2^{28} = 268,435,456 addresses, 6.25%

Class E: 2^{28} = 268,435,456 addresses, 6.25%

Fig. 1.20: Occupation of the Address Space

IP Address Classifications

Class	Bits in NetworkID	Number of Networks	Bits in HostID	Number of Hosts/Network	Address Range	Subnet Mask
A	8	126	24	4,000,000	1.0.0.0 to 126.255.255.255	255.0.0.0
B	16	16,384	16	65,536	128.0.0.0 to 191.255.255.255	255.255.0.0
C	24	2,000,000	8	65,536	192.0.0.0 to 223.255.255.255	255.255.255.0
D	0	0	28	268,400,000	224.0.0.0 to 239.255.255.255	
E	Class E addresses are reserved for future use (and Class D are usually used for testing only).					

1. Class A Addressing: [S-22, W-23]

- The first bit of the first octet is always set to zero. The highest order bit of the network byte is always 0.
- So that the first octet ranges from 1 – 127.

    00000001 – 01111111
    1 – 127
- The class A address only include IP starting from 1.x.x.x to 126.x.x.x. The IP range 127.x.x.x is reserved for loop back IP addresses.
- The default subnet mask for class A IP address is 255.0.0.0. This means it can have 126 networks (27-2) and 16777214 hosts (224-2).
- Class A IP address format is thus: 0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH.
- First byte specifies the network portion (8 bits). Remaining bytes specify the host portion (24 bits).
- Network values of 0 and 127 are reserved. This class is used for large addressing networks.
- There are 126 class A networks. There are more than 16 million host values for each class A network.

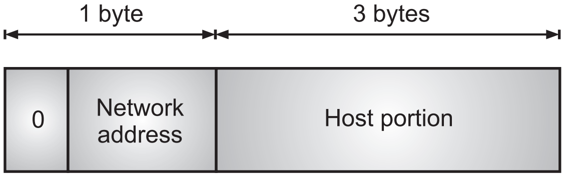


Fig. 1.21: Class A Addressing

2. Class B Addressing: [S-22, W-23]

- Here the first two bits in the first two bits is set to zero. The highest order bits 6 and 7 of the network portion are 10.

    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.

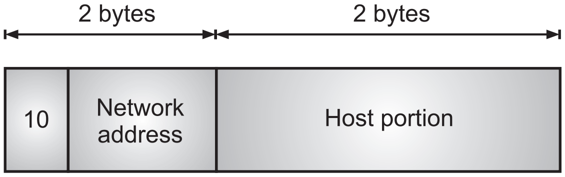


Fig. 1.22: Class B Addressing

- The first two bytes specify the network portion (16 bits). The last two bytes specify the host portion (16 bits).
- This class is used for medium sized addressing networks. There are more than 16 thousand class B networks. There are 65 thousand nodes in each class B network.

3. **Class C Addressing:** [S-22, W-23]

- The first octet of this class has its first 3 bits set to 110. The highest order bits 5, 6 and 7 of the network portion are 110.

11000000 – 11011111

192 – 123

- 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 (221) Network addresses and 254 (28-2) Host addresses.
- Class C IP address format is: 110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH.

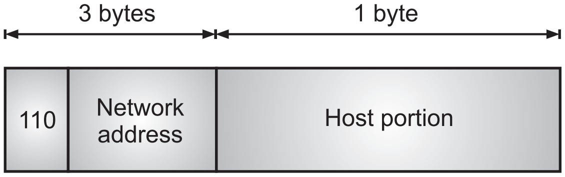


Fig. 1.23: Class C Addressing

- The first three bytes specify the network portion (24 bits). The last byte specifies the host portion (8 bits). This class is used for addressing small sized networks.
- There are more than 2 million class C networks. There are 254 nodes in each class C network.

4. **Class D Addressing:** [S-22, W-23]

- The first four bits of the first octet in class D IP address are set to 1110.

11100000 – 11101111

224 – 239

- Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting.

1110
Multicast address

Fig. 1.24: Class D Addressing

- In multicasting data is not intended for a particular host, but multiple ones. That is why there is no need to extract host address from the class D IP addresses.
- The Class D does not have any subnet mask. Class D address defines a group-ID and used for multicasting.
- Internet authorities have designated some multicast addresses to specific groups.

5. **Class E Addressing:** [S-22, W-23]

1111
Reserved for future use

Fig. 1.25: Class E Addressing

- The class E IP addresses are reserved for experimental purpose only for R&D or study.
- IP addresses in the class E ranges from 240.0.0.0 to 255.255.255.254.
- This class too is not equipped with any subnet mask. Fig. 1.25 shows address format of class E addressing.

Concept of Network Address:

- A network address, is particularly important because it is used in routing a packet to its destination network.

- The routers in the Internet normally use an algorithm to extract the network address from the destination address of a packet. To do this, we need a network mask.
- A network mask (or a default mask) in classful addressing is a 32-bit number with n leftmost bits all set to 1s and (32 − n) rightmost bits all set to 0s.
- The three default masks in classful addressing are shown in Fig. 1.26 (a). To extract the network address from the destination, address of a packet, a router uses the AND operation.
- When the destination address (or any address in the block) is ANDed with the default mask, the result is the network address as shown in Fig. 1.26 (b).

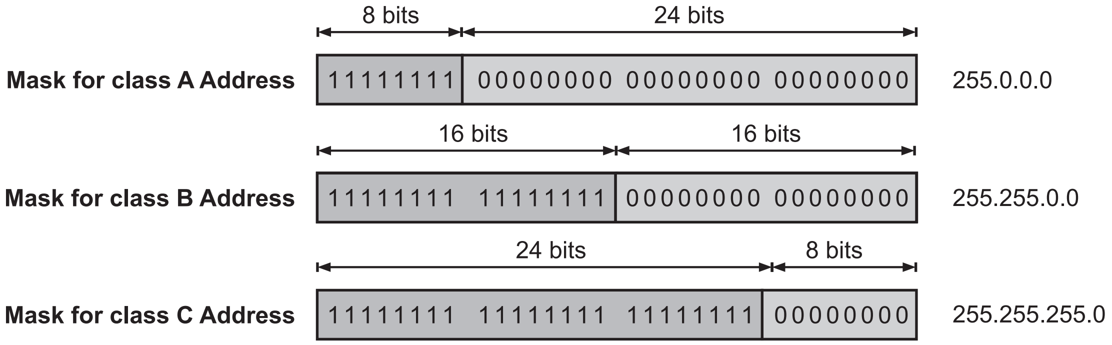


Fig. 1.26 (a): Network Mask

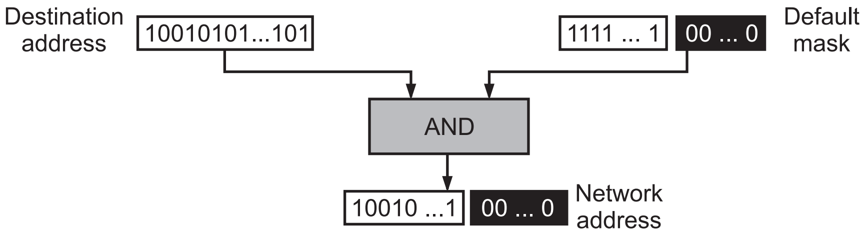


Fig. 1.26 (b): Finding a Network Address using the Default Mask

Subnetting:

- A subnet is a logical division of an IP network, allowing a larger network to be split into smaller, more manageable segments, each with its own unique IP address range, which improves network efficiency and security.
- Subnetting is the process of creating these subnets, and subnet addressing involves assigning IP addresses and subnet masks to these subnets.
- Subnetting is a method for partitioning/dividing a classful IP network into smaller subnetworks (subnets).
- The process of subnetting involves dividing a network up into smaller networks called subnets or sub networks.
- A subnet is a logical partition of an IP network into multiple, smaller network segments. Each of these subnets has its own specific address.
- To create these additional sub networks, we use a subnet mask. The subnet mask simply determines which portion of the IP address belongs to the host. The subnet address is created by dividing the host address into network address and host address.
- Subnetting provides the network administrator with several benefits, including extra flexibility, more efficient use of network address and the capability to contain broadcast traffic.
- To allow a single network address to span multiple physical networks is called subnet addressing or subnet routing or subnetting.

- Subnetting enables the network administrator to further divide the host part of the address into two or more subnets. In this case, a part of the host address is reserved to identify the particular subnet.
- Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you will only be able to use one network from your Class A, B, or C network, which is unrealistic.
- Each data link on a network must have a unique network ID, with every node on that link being a member of the same network. If you break a major network (Class A, B, or C) into smaller subnetworks, it allows you to create a network of interconnecting subnetworks.
- Each data link on this network would then have a unique network/sunetwork ID. Any device, or gateway, connecting n networks/subnetworks has n distinct IP addresses, one for each network/subnetwork that is interconnects.
- To subnet a network, extend the natural mask using some of the bits from the host ID portion of the address to create a subnetwork ID. For example, given a Class C network of 204.15.5.0 which has a natural maks of 255.255.255.0. you can create subnets in the following manner:

```
204.15.5.0          11001100.00001111.00000101.00000000
255.255.255.224     11111111.11111111.11111111.11100000
                    --------------------------(sub)--------
```

- By extending the mask to be 255.255.255.224, you have taken three bits (seen above as "sub") from the original host portion of the address and used them to make subnets. With these three bits, it is possible to create eight subnets.
- With the remaining five host ID bits. each subnet can have up to 32 host addresses, 30 of which can actually be assigned to a device since host ids of zeros or all ones are not allowed (it is very important to remember this).
- So, with this in mind, the following subnets have been created.

204.15.5.0	255.255.255.224	host address range 1 to 30
204.15.5.32	255.255.255.224	host address range 33 to 62
204.15.5.64	255.255.255.224	host address range 65 to 94
204.15.5.96	255.255.255.224	host address range 96 to 126
204.15.5.128	255.255.255.224	host address range 129 to 158
204.15.5.160	255.255.255.224	host address range 161 to 190
204.15.5.192	255.255.255.224	host address range 193 to 222
204.15.5.224	255.255.255.224	host address range 225 to 254

- Using the network subnetting scheme above, which allows for eight subnets, the network might appear as shown in Fig. 1.27.

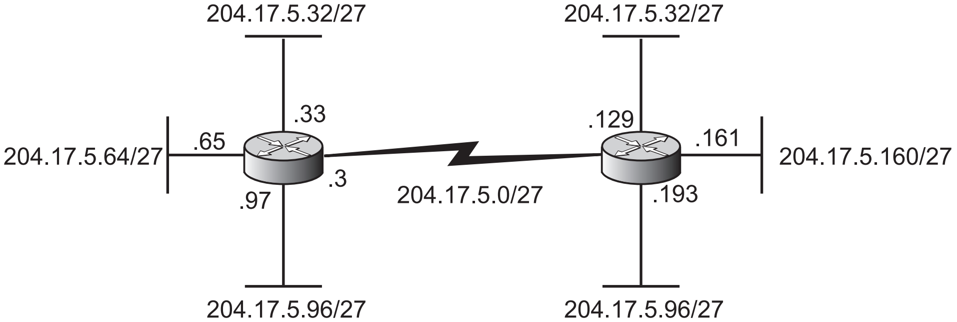


Fig. 1.27

- Fig. 1.28 shows a network using class B addresses before subnetting. In this example we have just one network with almost 216 hosts. The whole network is connected, through one single connection, to one of the routers in the Internet.

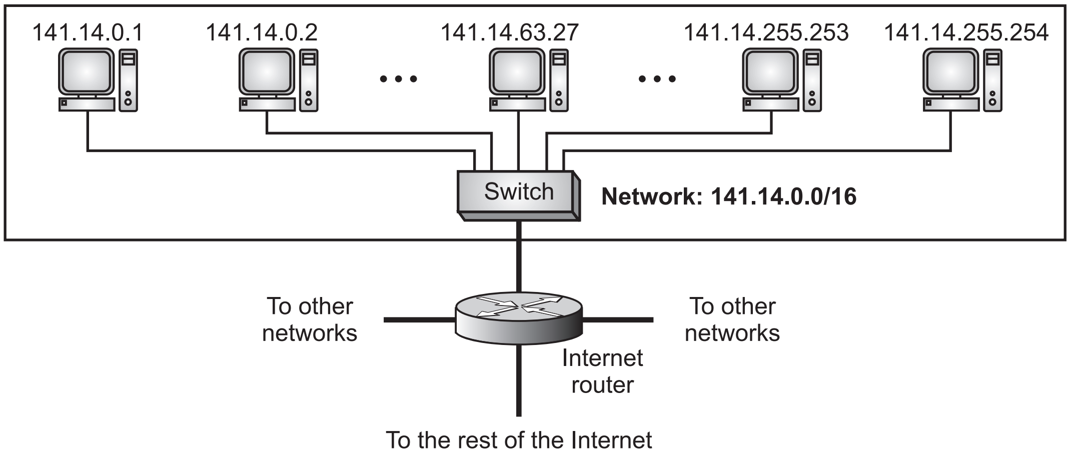


Fig. 1.28

- Fig. 1.29 shows the same network in Fig. 1.28 after subnetting. The whole network is still connected to the Internet through the same router. However, the network has used a private router to divide the network into four subnetworks.

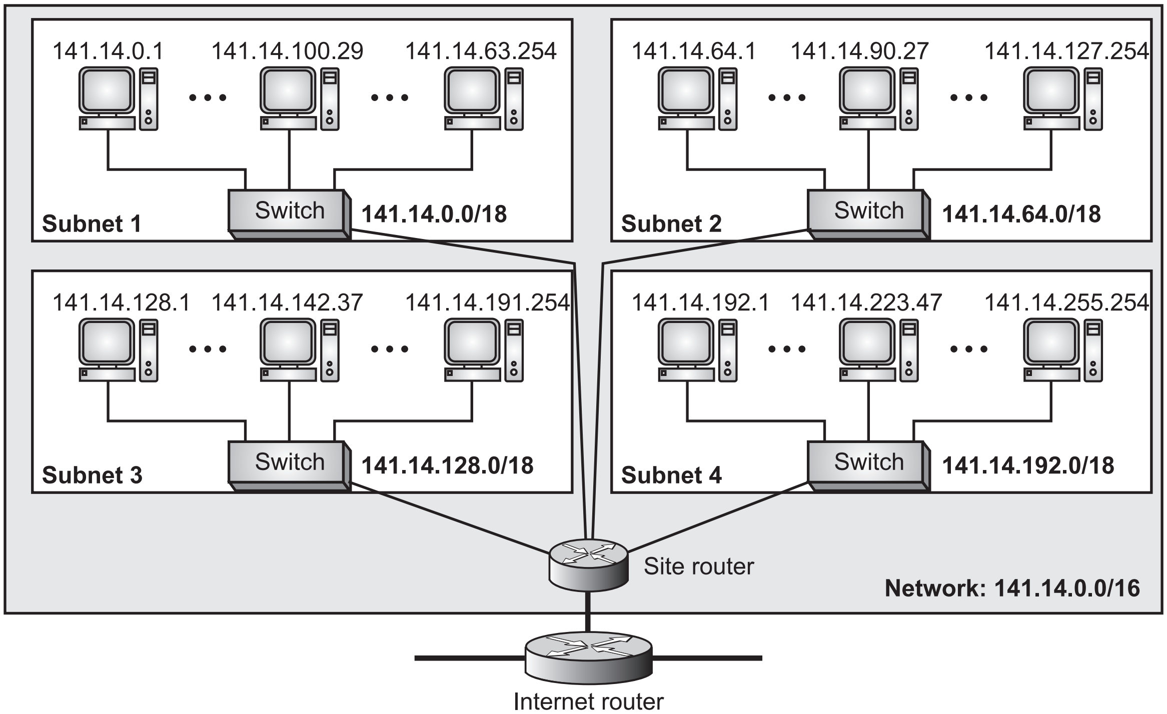


Fig. 1.29

Benefits of Subnetting:

1. **Efficient IP Address Usage:** Subnetting can help to make more efficient use of IP addresses.
2. **Improved Network Performance:** Subnetting can improve network performance by reducing network traffic and improving routing efficiency.
3. **Enhanced Security:** Subnetting can enhance security by isolating traffic between different parts of the network.
4. **Easier Network Management:** Subnetting can make it easier to manage and troubleshoot networks.

Examples:

Example 1: Assume a company has three offices Central, East, and West. The Central office is connected to the East and West offices via private, point-to-point WAN lines. The company is granted a block of 64 addresses with the beginning address 70.12.100.128/26. The management has decided to allocate 32 addresses for the Central office and divides the rest of addresses between the two other offices.

1. The number of addresses are assigned as follows:

   Central office $N_c = 32$ East office $N_e = 16$ West office $N_w = 16$

2. We can find the prefix length for each subnetwork:

   $n_c = n + \log_2(64/32) = 27$ $n_e = n + \log_2 (64/16) = 28$ $n_w = n + \log_2(64/16) = 28$

Solution:

Fig. 1.30 shows the configuration designed by the management. The Central office uses addresses 70.12.100.128/27 to 70.12.100.159/27. The company has used three of these addresses for the routers and has reserved the last address in the subblock. The East office uses the addresses 70.12.100.160/28 to 70.12.100.175/28. One of these addresses is used for the router and the company has reserved the last address in the subblock. The West office uses the addresses 70.12.100.160/28 to 70.12.100.175/28. One of these addresses is used for the router and the company has reserved the last address in the subblock. The company uses no address for the point-to-point connections in WANs.

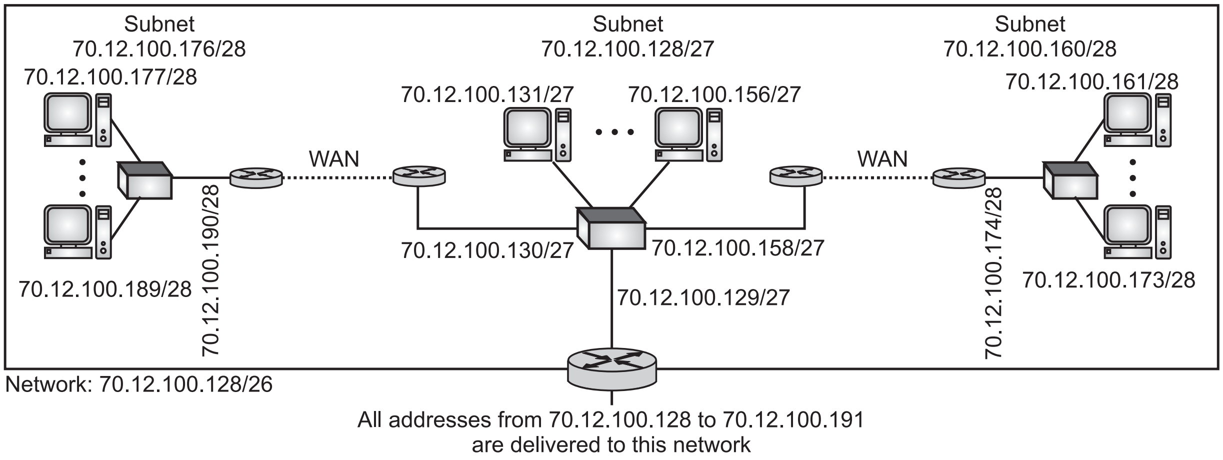


Fig. 1.30

Example 2: An organization is granted the block 130.34.12.64/26. The organization needs four subnetworks, each with an equal number of hosts. Design the subnetworks and find the information about each network.

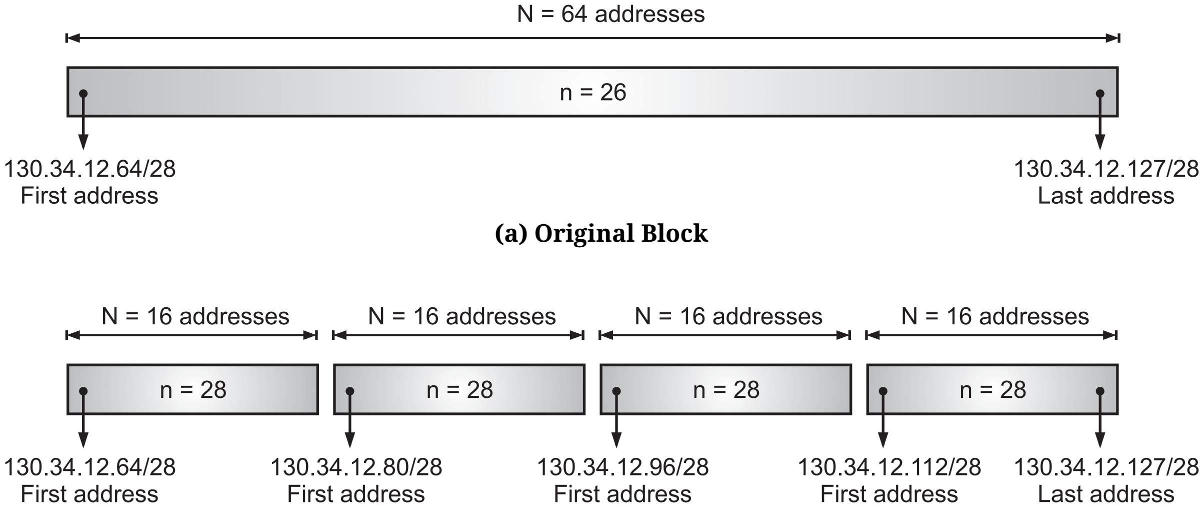
Solution:

The number of addresses for the whole network can be found as $N = 2^{32-26} = 64$. The first adddress in the network is 130.34.12.64/26 and the last address is 130.34.12.127/26. We now design the subnetworks:

1. We grant 16 addresses for each subnetwork to meet the first requirment (64/16 is a power of 2).
2. The subnetwork mask for each subnetwork is:

   $n_1 = n_2 = n_3 = n_4 = n + \log_2 (N/N_i) = 26 + \log_2 4 = 28$

3. We grant 16 address to each subnet starting from the first available address. Fig. 1.31 shows the subblock for each subnet. Note that the starting address in each subnetwork is divisible by the number of address in the subnetwork.



(a) Original Block

(b) Sbublocks

Fig. 1.31

1.4 ADDRESS MASKING AND SUPERNETTING

- Address Masking and Supernetting are techniques used in networking to manage IP addresses efficiently.

1.4.1 Address Masking

- Address masking commonly referred to as subnet masking. It involves using a subnet mask to divide an IP address into the network portion and the host portion.
- This process is crucial for subnetting, which allows a larger network to be divided into smaller sub-networks.
- A subnet mask is a 32-bit number (for IPv4) that determines which part of an IP address belongs to the network and which part to the host.

1.4.1.1 Concept of Masking

- A mask used to determine what subnet an IP address belongs to. A process that extracts the address of the physical network from an IP address is called Masking.
- If we done the subnetting, then masking extracts the subnetwork address from an IP address. It may at first seem to be odd that IP address classes are assigned in this way.
- After all, there are not any private networks that have 16 million hosts on them, so it makes little sense even to have Class A addresses. However, it's possible to subdivide IP addresses even further by creating subnets on them.
- A subnet is simply a subdivision of a network address that can be used to represent one LAN on an internetwork or the network of one of an ISP's clients.
- Thus, a large ISP might have a Class A address registered to it and it might farm out pieces of the address to its clients in the form of subnets.
- In many cases, a large ISP's clients are smaller ISPs, which in turn supply addresses to their own clients.
- A subnet allows the flow of network traffic between hosts to be segregated based on a network configuration.

- A subnet mask (or number) is used to determine the number of bits used for the subnet and host portions of the address. The mask is a 32-bit value that uses one-bits for the network and subnet portions and zero-bits for the host portion.
- A subnet mask is typically represented in dotted decimal notation, such as 255.255.255.0, or in CIDR notation, such as /24.

1.4.1.2 Subnet Masks [S-22]

- IP networks can be divided into smaller networks called subnetworks (or subnets). The suhnets are created through the use of subnet masks.
- The subset mask identifies which hits in the IP address are to be used to represent the network subnet portion of an IP address.
- The network mask is used when a network is not subnetted.
- When we divide a network to several subnetworks, we need to create a subnetwork mask (or subnet mask) for each subnetwork.
- Fig. 1.32 shows a subnetwork has subnetid and hostid.

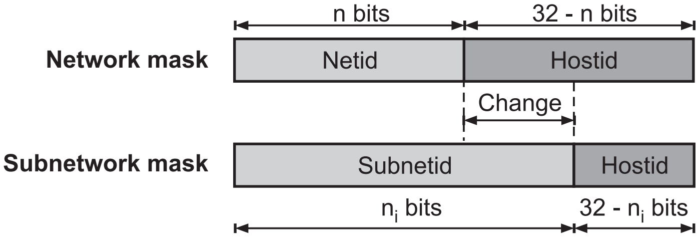


Fig. 1.32: Network Mask and Subnetwork Mask

- Subnets are created by borrowing bits from the host portion of the IP address as shown in Fig. 1.33.
- The network portion of the IP address and the new sub-net bits are used to define the new subnet. Routers use this information to properly forward data packets to the proper subnet.
- Subnetting is the process of breaking down a main class A, B, or C network into subnets for routing purposes.
- A subnet mask is the same basic thing as a netmask with the only difference being that we are breaking a larger organizational network into smaller parts, and each smaller section will use a different set of address numbers.

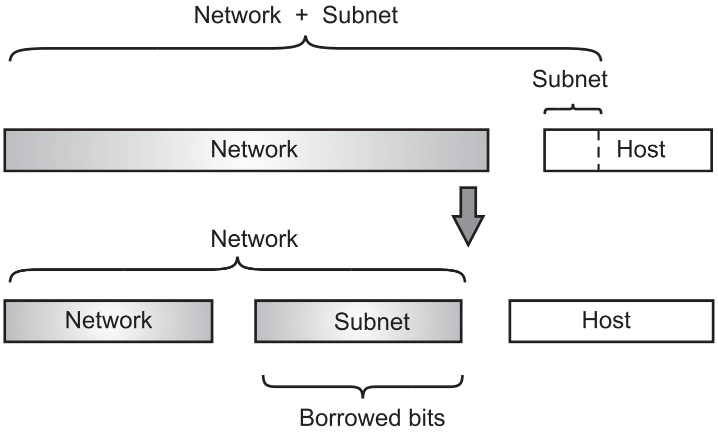


Fig. 1.33: Borrowing Bits from the Host to Create Subnets

- This will allow network packets to be routed between subnetworks. When doing subnetting, the number of bits in the subnet mask determine the number of available subnets.
- Two to the power of the number of bits minus two is the number of available subnets. When setting up subnets the following must be determined:
  - Number of segments, and
  - Hosts per segment.
- Subnetting provides the following advantages:
  - **Network Traffic Isolation:** There is less network traffic on each subnet.
  - **Simplified Administration:** Networks may be managed independently.
  - **Improved Security:** Subnets can isolate internal networks so they are not visible from external networks.

- A 14-bit subnet mask on a class B network only allows 2 node addresses for WAN links. A routing algorithm like OSPF (Open Shortest Path First) must be used for this approach.
- These protocols allow the Variable Length Subnet Masks (VLSM). RIP (Routing Information Protocol) and IGRP (Interior Gateway Routing Protocol) don't support this. Subnet mask information must be transmitted on the update packets for dynamic routing protocols for this to work.
- The router subnet mask is different than the WAN interface subnet mask. One network ID is required by each of:
  - Subnet,
  - WAN connection.
- One host ID is required by each of:
  - Each NIC on each host.
  - Each router interfaces.
- Types of subnet masks:
  - **Default:** Fits into a Class A, B, or C network category.
  - **Custom:** Used to break a default network such as a Class A, B, or C network into subnets.

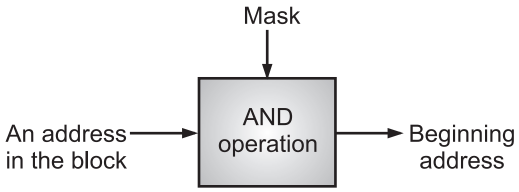


Fig. 1.34 (a): Masking Concept

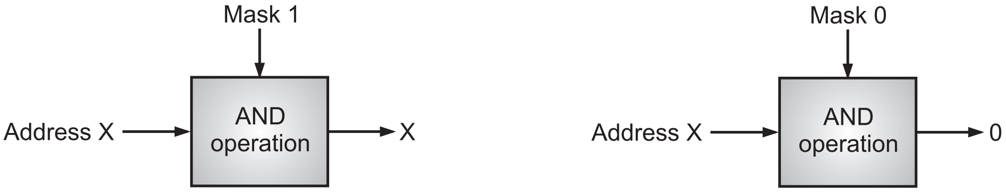
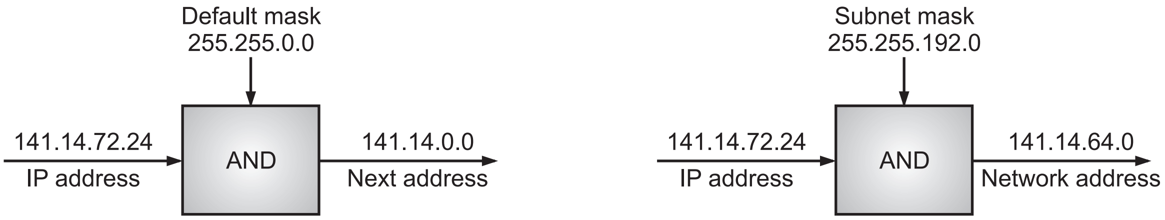


Fig. 1.34 (b): AND Operation

Default Masks

Class	Mask in Binary	Mask in dotted-decimal
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0



(a) Without Subnetting **(b) With Subnetting**

Fig. 1.35: Default Mask and Subnet Mask

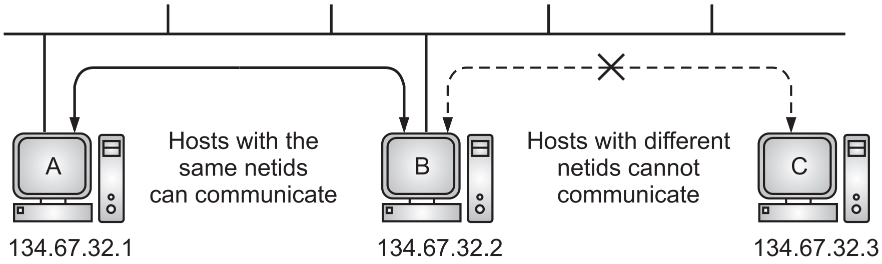


Fig. 1.36: Host Communication on a Local Network

- A subnet is defined by applying a bitmask, the subnetmask, to the IP address. If a bit is on the mask, the equivalent bit in the address is interpreted as a network bit.
- If the bit in the mask is off, the bit belongs to the host part of the address. The subnet is only known locally. To the rest of the Internet, the address is still interpreted as a standard IP address.

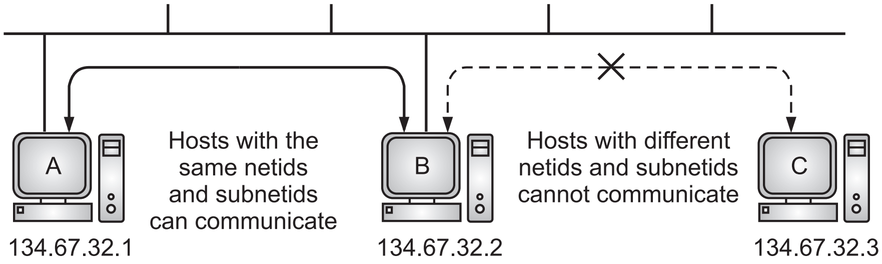


Fig. 1.37: Host Communication with Subnetting

- In following example explains how to find subnet masks and subnets.
- **Problem Statement**: Let's say you have an IP address of **192.168.1.10** and you want to create a subnet mask that allows for **30 hosts** in your subnet.

Step 1: Determine the Number of Hosts:

- First, calculate how many bits you need for the hosts. The formula to find the number of hosts is:

  Number of hosts = $2^n–2$

  Where n is the number of bits for the host part. The "-2" accounts for the network and broadcast addresses.

  For 30 hosts: $2^n – 2 \geq 30$

  Testing values: For n = 5

  $2^5–2=30$ (this works)

Step 2: Determine the Number of Subnet Bits:

- Next, we need to determine how many bits will be used for the network part of the address. Since an IPv4 address is 32 bits in total, you subtract the host bits from 32:

  Network bits=32–n=32–5=27

Step 3: Construct the Subnet Mask:

- Now, you convert the network bits to a subnet mask. A subnet mask uses 1s for the network part and 0s for the host part. For our example:

  27 bits for the network: 11111111.11111111.11111111.11111110

  This translates to decimal as: 255.255.255.254

Step 4: Verify the Subnet:

- Now you can verify the subnet:

  Subnet Mask: 255.255.255.254

  CIDR Notation: /27

1.4.2 Supernetting

- Supernetting is the process of combining multiple networks into a single, larger network. This technique is used to aggregate routing information, making it easier to manage and route traffic across networks.
- Supernetting, also called Classless Inter-Domain Routing (CIDR), is a way to aggregate multiple Internet addresses of the same class.
- Classful means that the IP addresses and subnets are within the same network. The problem with classful addressing is that there is a lot of unused IP address space.
- For example, a class A IP network has more than 16 million possible host addresses. A Class B network has more than 65,000 host addresses, but the fact is that only a limited number of Class A and B address space has been allocated for Internet use.
- However, the size of a class C block with a maximum number of 256 addresses may not satisfy the needs of an organization. Even a mid-size organization may need more addresses.
- One solution is supernetting. In supernetting, an organization can combine several class C blocks to create a larger range of addresses.
- In other words, several networks are combined to create a supernetwork. By doing this, an organization can apply for a set of class C blocks instead of just one.
- For example, an organization that needs 1000 addresses can be granted four class C blocks.
- The organization can then use these addresses in one supernetwork as shown in Fig. 1.38. When we group two or more classful networks together, they are called supernets.
- The technique supernetting was proposed in 1992 to eliminate the class boundaries and to make available the unused IP address space.
- Supernetting allows multiple networks to be specified by one subnet mask. In other words, the class boundary could be overcome.

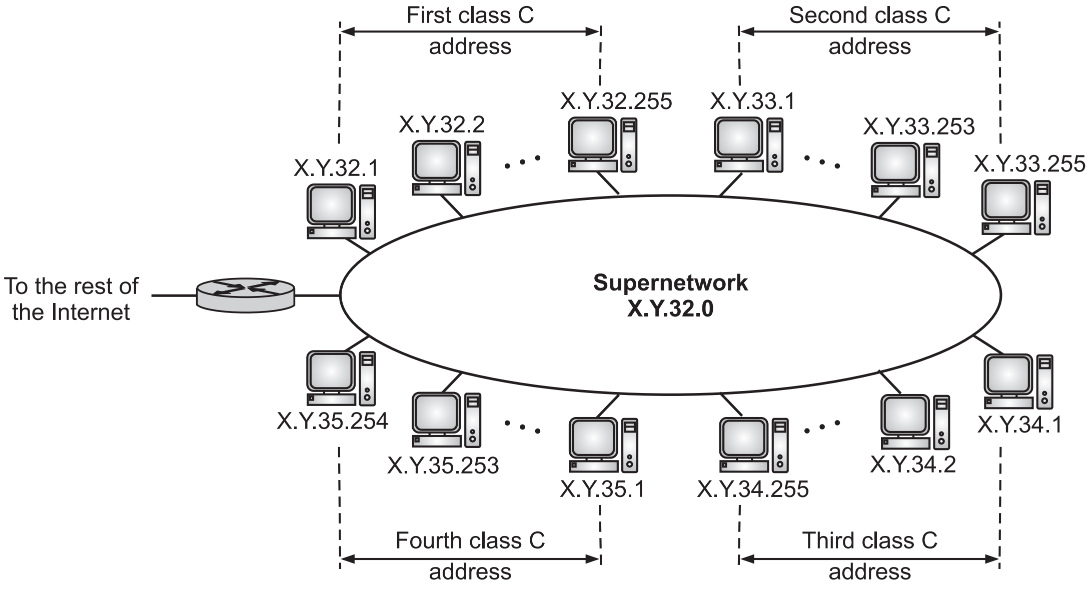


Fig. 1.38: A Supernetwork

- Supernetting required a simpler way to indicate the subnet mask. The technique developed is called Classless Inter-Domain Routing (CIDR). CIDR notation specifies the number of bits set to a 1 that make up the subnet mask. **[S-23]**
- For example, the Class C size subnet mask 255.255.255.0 is listed in CIDR notation as /24. This indicates the 24 bits are set to a 1. A Class B size subnet is written as /16, and a Class A subnet is written as /8. CIDR can also be used to represent subnets that identify only part of the octet bits in an IP address. For example, a subnet mask of 255.255.192.0 is written in CIDR as /18.

- The /18 comes from the 18 bits that are set to a 1 as shown below:

255	255	192	0
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 0 0 0 0 0 0	0 0 0 0 0 0 0 0

- CIDR notation truncates the subnet mask to what is known as "slash" notation. In this example, the network would be identified as 131.107.0.0/16.

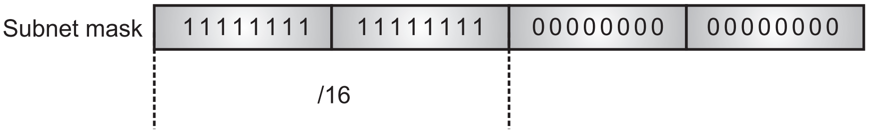


Fig. 1.39

- The "/16" value refers to the fact that the first 16 bits in the subnet mask are all set to values of binary 1.

1.4.2.1 Supernet Mask

- A supernet mask is the reverse of a subnet mask. A subnet mask for class C has more 1s than the default mask for this class. A supernet mask for class C has less 1s than the default mask for this class.
- When an organization or firm is granted one block of addresses (class A, B, or C), the first address in the block and the mask define the block (the range of addresses). We always know this range of addresses since the mask is always known (default mask).
- When an organization or firm divides its block into subnets, the first address in the sub-block and the subnet mask completely define the subblock (the range of addresses). In this case, however, the first address alone is not enough, we must have the subnet mask.
- Similarly, when an organization or firm combines several blocks into a superblock, we need to know the first address in the block and the supernet mask. Here also, the first address alone cannot define the range; we need a supernet mask to find how many blocks are combined to make a superblock.
- In subnetting, we need the first address of the subnet and the subnet mask to define the range of addresses. In supernetting, we need the first address of the supernet and the supernet mask to define the range of addresses.
- Fig. 1.40 shows the difference between a subnet mask and a supernet mask. A subnet mask that divides a block into eight subblocks has three more is (2^3 = 8) than the default mask while a supemet mask that combines eight blocks into one superblock has three less 1s than the default mask.

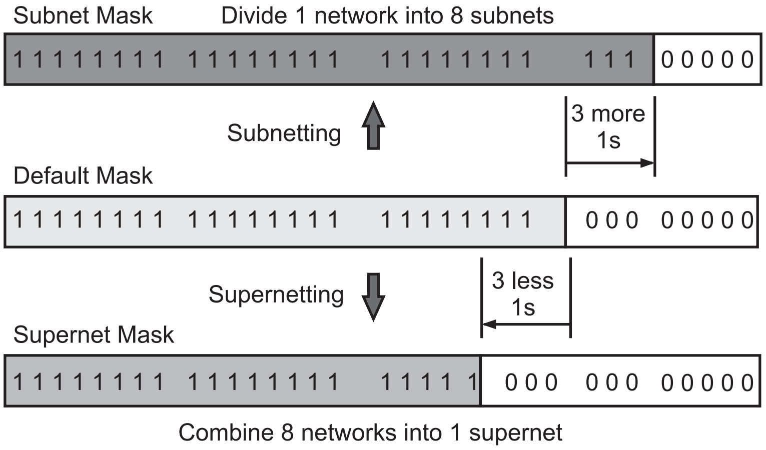


Fig. 1.40: Comparison of Subnet, Default and Supernet Masks

1.5 ADDRESS MAPPING

- Address Mapping in networking refers to the process of translating one type of address to another so devices can communicate efficiently across networks.
- An internet is made of a combination of physical networks connected together by internetworking devices like routers.
- A packet starting from a source host may pass through several different physical networks before finally reaching the destination host.
- The hosts and routers are recognized at the network level by their logical addresses. A logical address is an internetwork address.

- It is called a logical address because it is usually implemented in software. Every protocol that deals with interconnecting networks requires logical addresses.
- The logical addresses in the TCP/IP protocol suite are called IP addresses and are 32 bits long. However, packets pass through physical networks to reach these hosts and routers.
- At the physical level, the hosts and routers are recognized by their physical addresses. A physical address is a local address.
- It is called a physical address because it is usually (but not always) implemented in hardware. Examples of physical addresses are 48-bit MAC addresses in the Ethernet protocol, which are imprinted on the NIC installed in the host or router.
- The delivery of a packet to a host or a router requires two levels of addressing: logical and physical. We need to be able to map a logical address to its corresponding physical address and vice versa.
- These can be done using either static mapping or dynamic mapping.

  1. **Static Mapping:**
     - Static mapping means creating a table that associates a logical address with a physical address.
     - This table is stored in each machine on the network. Each machine that knows, for example, the IP address of another machine but not its physical address can look it up in the table.
  2. **Dynamic Mapping:**
     - In dynamic mapping, each time a machine knows the logical address of another machine, it can use a protocol to find the physical address.
     - Two protocols have been designed to perform dynamic mapping namely, Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP). ARP maps a logical address to a physical address; RARP maps a physical address to a logical address.
- Address mapping refers to the process of translating between different types of addresses used in networking, such as logical addresses (IP addresses) and physical addresses (MAC addresses).

1.5.1 Address Resolution Protocol (ARP)

- ARP stands for Address Resolution Protocol. ARP is used to convert the logical address i.e. IP address into physical address i.e. MAC address
- ARP is a protocol that maps IP addresses to MAC addresses on a local network. When a device wants to send data to another device on the same network, but only knows the IP address, it uses ARP to find the corresponding MAC address.
- Address Resolution Protocol (ARP) is a protocol or procedure that connects an ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN).
- This mapping procedure is important because the lengths of the IP and MAC addresses differ, and a translation is needed so that the systems can recognize one another.
- The most used IP today is IP version 4 (IPv4). An IP address is 32 bits long. However, MAC addresses are 48 bits long. ARP translates the 32-bit address to 48 and vice versa.
- There is a networking model known as the Open Systems Interconnection (OSI) model. First developed in the late 1970s, the OSI model uses layers to give IT teams a visualization of what is going on with a particular networking system.
- This can be helpful in determining which layer affects which application, device, or software installed on the network, and further, which IT or engineering professional is responsible for managing that layer.
- The MAC address is also known as the data link layer, which establishes and terminates a connection between two physically connected devices so that data transfer can take place.
- The IP address is also referred to as the network layer or the layer responsible for forwarding packets of data through different routers. ARP works between these layers.

- Fig. 1.41 shows the position of the ARP in the TCP/IP protocol suite. ARP accepts a logical address from the IP protocol, maps the address to the corresponding physical address and pass it to the data link layer.

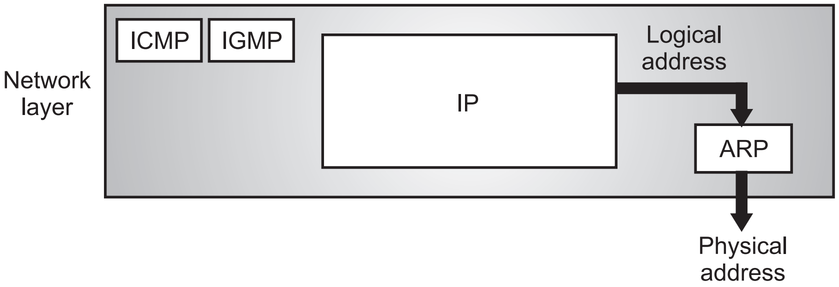
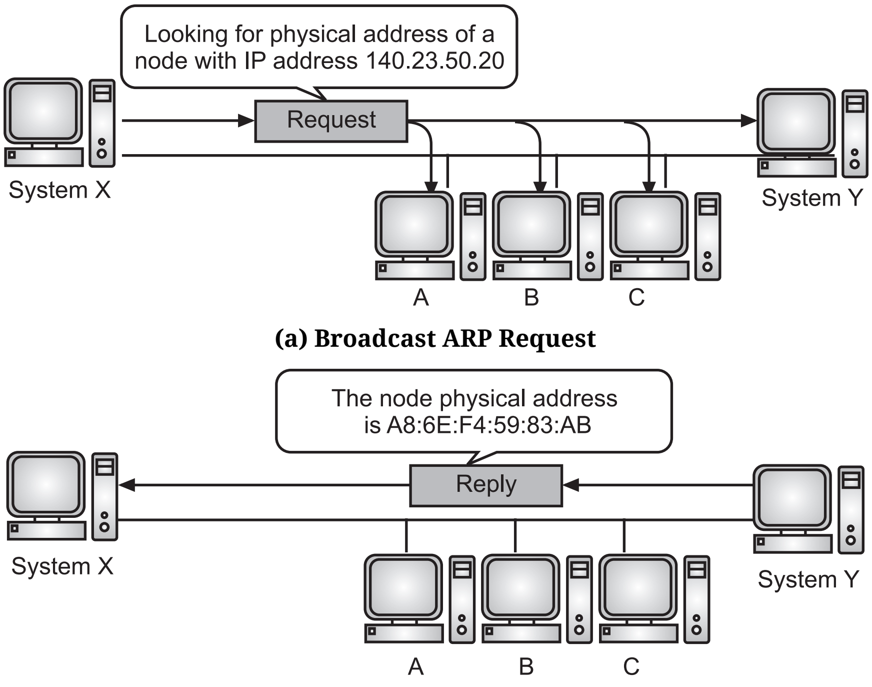


Fig. 1.41: Position of ARP in TCP/IP Protocol Suite

1.5.1.1 Mapping Logical to Physical Addresses

- ARP is a protocol that enables a device to discover the MAC address of another device on the network by knowing its IP address.
- For instance, when a computer needs to send a packet to another computer within the local area network (LAN), it must determine the MAC address of the destination computer to encapsulate the packet into a frame.
- To accomplish this, ARP broadcasts a request message containing its IP and MAC addresses along with the destination IP address.
- The device that possesses the IP address then responds with an ARP reply message containing its MAC address.
- The sender updates its ARP table with this entry. After that, it proceeds to transmit the frame to reach the intended destination.
- Fig. 1.42 shows the working of ARP.


Looking for physical address of a node with IP address 140.23.50.20
Request
System X
System Y
A
B
C

(a) Broadcast ARP Request

The node physical address is A8:6E:F4:59:83:AB
Reply
System X
System Y
A
B
C

(b) Unicast ARP Reply

Fig. 1.42: Working of ARP

- The sender first checks its ARP table to determine if it already has an entry for the destination IP address. If there is an entry, it uses the corresponding MAC address to send the frame. If there is no entry, it moves on to the next step.

- The sender then broadcasts an ARP request message to all devices on the network. This message contains the sender's IP and MAC addresses as well as the destination IP address.
- The device that has the matching IP address receives the ARP request message. After that, that device responds with an ARP reply message. This reply contains its IP and MAC addresses.
- Once the ARP reply message is received by the sender, it then updates its ARP table with the new entry. Further, it utilizes the destination MAC address to send the frame.

1.5.1.2 Working of ARP

- When a device wants to send data to another device on the same network, it first checks its ARP cache to see if it already knows the MAC address of the destination IP address.
- If the MAC address is not in the cache, the device sends an ARP request broadcast to all devices on the network, asking which device has the target IP address.
- The device with the target IP address responds with its MAC address.
- The requesting device then stores the IP-to-MAC mapping in its ARP cache for future use and uses the MAC address to transmit the data.

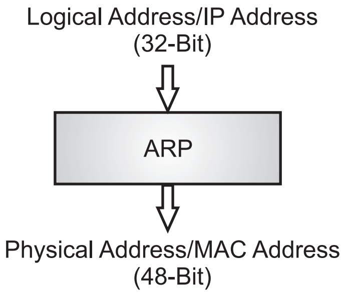
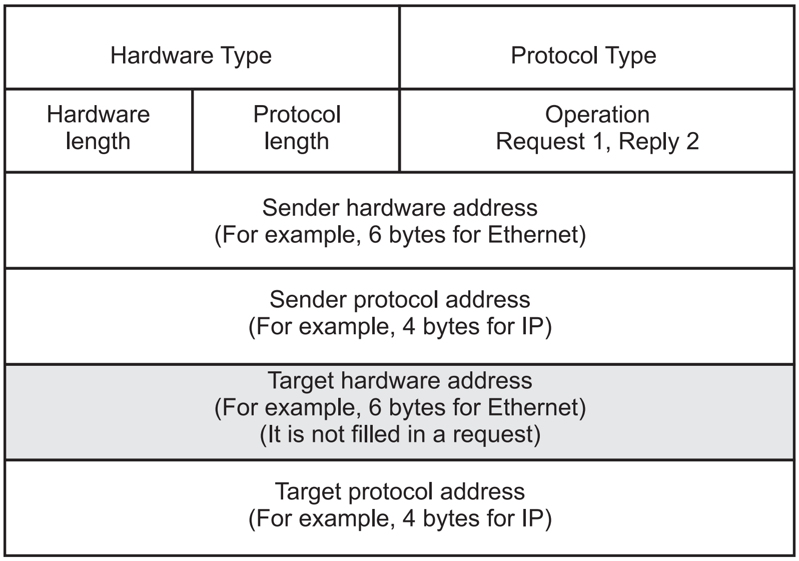


Fig. 1.43

1.5.1.3 ARP Packet Format

- The ARP uses a basic message format that contains either address resolution request or address resolution response.
- The ARP message size depends on the address size of the link layer and the network layer. The message header describes the network type used at each layer and the address size of each layer.
- The message header is complete with the help of the operation code, which is 1 for request and 2 for the response. The payload of the packet has four addresses, these are:
  - o Hardware address of the sender hosts.
  - o Protocol address of the sender hosts.
  - o Hardware address of the receiver hosts.
  - o Protocol address of the receiver hosts.
- The Packet format of the Address Resolution Protocol is shown in the Fig 1.44.



<table>
<tr><td colspan="2">Hardware Type</td><td>Protocol Type</td></tr>
<tr><td>Hardware length</td><td>Protocol length</td><td>Operation
Request 1, Reply 2</td></tr>
<tr><td colspan="3">Sender hardware address
(For example, 6 bytes for Ethernet)</td></tr>
<tr><td colspan="3">Sender protocol address
(For example, 4 bytes for IP)</td></tr>
<tr><td colspan="3">Target hardware address
(For example, 6 bytes for Ethernet)
(It is not filled in a request)</td></tr>
<tr><td colspan="3">Target protocol address
(For example, 4 bytes for IP)</td></tr>
</table>

Fig. 1.44: ARP Packet format

- Fig. 1.44 shows the format of an ARP packet. The fields are as follows:
  - o **Hardware Type:** This is a 16-bit field defining the type of the network on which. ARP is running. Each LAN has been assigned an integer based on its type. For example, Ethernet is given the type 1. ARP can be used on any physical network.

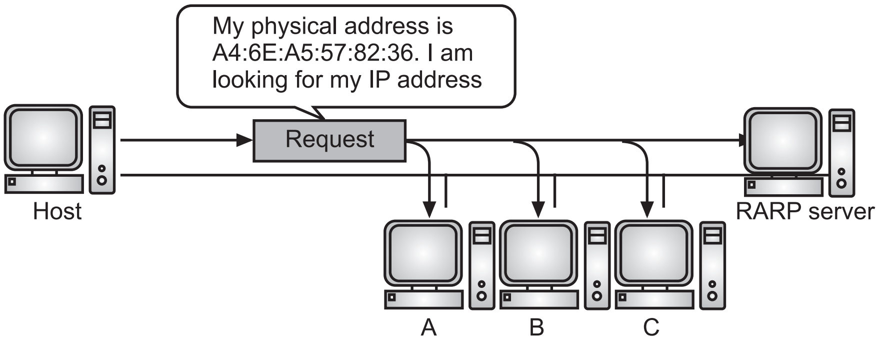
- **Protocol Type:** This is a 16-bit field defining the protocol. For example, the value of this field for the IPv4 protocol is 080016. ARP can be used with any higher-level protocol.
- **Hardware length:** This is an 8-bit field defining the length of the physical address in bytes. For example, for Ethernet the value is 6.
- **Protocol length:** This is an 8-bit field defining the length of the logical address in bytes. For example, for the IPv4 protocol the value is 4.
- **Operation:** This is a 16-bit field defining the type of packet. Two packet types are defined: ARP request (1), ARP reply (2).
- **Sender hardware address:** This is a variable-length field defining the physical address of the sender. For example, for Ethernet this field is 6 bytes long.
- **Sender protocol address:** This is a variable-length field defining the logical (for example, IP) address of the sender. For the IP protocol, this field is 4 bytes long.
- **Target hardware address:** This is a variable-length field defining the physical address of the target. For example, for Ethernet this field is 6 bytes long. For an ARP request message, this field is all 0s because the sender does not know the physical address of the target.
- **Target protocol address:** This is a variable-length field defining the logical (for example, IP) address of the target. For the IPv4 protocol, this field is 4 bytes long.

1.5.2 Reverse Address Resolution Protocol (RARP)

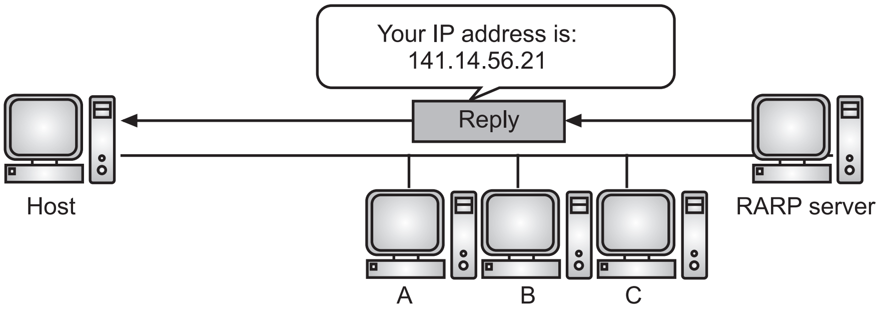
- Reverse Address Resolution Protocol (RARP) is used to map a device's physical (MAC) address to its logical (IP) address, allowing diskless or newly connected devices to obtain an IP address from an RARP server.
- RARP is a protocol that maps MAC addresses to IP addresses, allowing a device to determine its IP address from its MAC address.

1.5.2.1 Mapping Physical to Logical Addresses

- Reverse Address Resolution Protocol (RARP) is a network-specific standard protocol. It is described in RFC 903. Some network hosts, such as a diskless workstation, do not know their own IP address when they are booted.
- To determine their own IP address, they use a mechanism similar to ARP, but now the hardware address of the host is the known parameter, and the IP address is the queried parameter.
- RARP serves the opposite purpose of ARP. It allows a device to determine its IP address when it knows only its MAC address. Reverse Address Resolution Protocol or RARP Operates at layer 2 (data link layer) of the OSI model.
- The reverse address resolution is performed the same way as the ARP address resolution. Fig. 1.45 shows working of RARP.


My physical address is A4:6E:A5:57:82:36. I am looking for my IP address
Request
Host
RARP server
A
B
C

(a) RARP Request is Broadcast



(b) RARP Reply is Unicast

Fig. 1.45: Working of RARP

- The device broadcasts a request message using RARP, including its MAC address and asking for an IP address from an RARP server.
- The RARP server that has an entry matching the MAC address receives the request message. After that, it sends back a reply message containing the IP address.
- The device receives the reply message from the RARP server. It then configures itself with the given IP address.
- Depending on the configuration settings, the device may also choose to cache, or it can also delete the RARP after some time working.

1.5.2.2 Working of RARP

- A device sends a broadcast request containing its MAC address to an RARP server.
- The RARP server, which maintains a table mapping MAC addresses to IP addresses, responds with the corresponding IP address.
- The device then uses this IP address to communicate on the network.

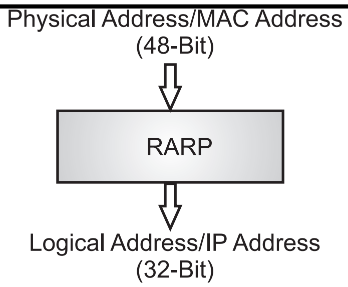


Fig. 1.46

1.5.2.3 RARP Packet Format

- Fig. 1.47 shows Packet Format of RARP.

Hardware Type		Protocol Type
Hardware Address length	Protocol Address length	Opcode
Sender hardware address		
Source protocol address		
Destination hardware address		
Destination protocol address		

Fig. 1.47: The RARP Packet Format (which is the same as the ARTP packet format)

- Similar to ARP, RARP packets have fields such as hardware type, protocol type, hardware address length, protocol address length, operation code, sender hardware address, sender protocol address, target hardware address, and target protocol address.
- RARP messages are encapsulated within Ethernet frames or other link-layer protocols when transmitted over the network.
- Each field in the RARP packet helps the server determine which machine requests an IP and ensures the correct IP is returned.

Difference between ARP and RARP:

Sr. No.	Parameters	ARP (Address Resolution Protocol)	RARP (Reverse Address Resolution Protocol)
1.	Purpose	Resolves IP addresses to MAC addresses.	Resolves MAC addresses to IP addresses.
2.	Functionality	Maps IP addresses to MAC addresses for communication.	Maps MAC addresses to IP addresses for address assignment.
3.	Usage	Used by devices to find the MAC address of a device with a known IP address.	Used by diskless or IP-less devices to determine their IP address.
4.	Message Type	ARP Request and ARP Reply messages.	RARP Request and RARP Reply messages.
5.	Resolution Process	Device sends ARP Request to find the MAC address associated with a known IP address.	Device sends RARP Request to find the IP address associated with a known MAC address.
6.	Request Type	Broadcast message requesting the MAC address for a specific IP address.	Broadcast message requesting the IP address for a specific MAC address.
7.	Response Type	Unicast message providing the MAC address corresponding to the requested IP address.	Unicast message providing the IP address corresponding to the requested MAC address.
8.	Packet Format	ARP packets have fields for hardware type, protocol type, hardware address length, protocol address length, operation code, sender hardware address, sender protocol address, target hardware address, and target protocol address.	RARP packets have similar fields as ARP packets.
9.	Usage Status	Widely used in modern networks.	Largely replaced by DHCP (Dynamic Host Configuration Protocol) for IP address assignment.
10.	Encapsulation	ARP messages are encapsulated within Ethernet frames or other suitable link-layer protocols.	RARP messages are encapsulated within Ethernet frames or other link-layer protocols.
11.	Common Use Case	Resolving IP addresses to MAC addresses in Ethernet-based networks.	Assigning IP addresses to diskless workstations or devices without statically configured IP addresses.

Practice Questions

1. What is IP address?
2. What is address space?
3. Compare and Contrast IPv4 and IPv6. Find examples of companies who are currently using IPv6. What are some of the benefits of using IPv6 over IPv4.
4. What is IP?
5. Explain classful IP addressing in detail.
6. Define the terms: IP address and IP.
7. Describe classless IP addressing in detail.
8. Compare IPv4 and IPv6.
9. With the help of diagram describe protocol format of IP.
10. Explain role of ISP and ICANN.
11. Explain ARP packet format.
12. Explain working of ARP an RARP.
13. Find the subnetwork address for the following:

Sr. No.	IP Address	Mask
1.	141.181.14.16	255.255.225.0
2.	200.34.22.156	255.255.255.240
3.	125.35.12.57	255.255.0.0

MSBTE Questions with Answers

Summer 2023

1. Draw and label sketch of IPv4 packet format. **[2 M]**

Ans. Refer to Section 1.2.1.

2. List any two extension headers of IPv6 protocol. **[2 M]**

Ans. Refer to Section 1.2.2.

3. State the importance of IPv6 over IPv4. **[2 M]**

Ans. Refer to Section 1.2.

4. Explain classful addressing mechanism of IPv4. **[4 M]**

Ans. Refer to Page 1.23.

5. Find out the error, if any in the following IPv4 addresses:

(i) 111.56.054.78 (ii) 222.34.7.8.20

(iii) 75.45.301.14 (iv) 11100101.23.14.67. **[4 M]**

Ans. Refer to Page 1.23.

6. Draw and explain IPv6 packet format. **[4 M]**

Ans. Refer to Section 1.2.2.

7. Explain the process of transition from IPv4 to IPv6. **[6 M]**

Ans. Refer to Section 1.2.

8. For the IP address given below, find the range of addresses in the following blocks:

(i) 123.56.77.32/29 (ii) 200.17.21.128/27

(iii) 17.34.16.0/23 (iv) 180.34.64.64/30. **[6 M]**

Ans. Refer to Page 1.21.

Winter 2023

1. Differentiate between IPv4 and IPv6 on the basis of length and security. **[2 M]**

Ans. Refer to Page. 1.20.

2. State the need of IPv6. **[2 M]**

Ans. Refer to Section 1.2.

3. Describe packet format of IPv6. **[4 M]**

Ans. Refer to Section 1.2.2.

4. From below list, explain any two different transition method from IPv4 to IPv6: (i) Dual stack (ii) Tunneling (iii) Header translation. **[4 M]**

Ans. Refer to Section 1.2.

5. For the IP addresses given below:

(1) Identify the classes to which the IP address belongs to

(2) Identify network address section

(3) Identify host address section

(4) Calculate number of hosts that can be assigned with each network

(i) 122.34.45.133

(ii) 12.12.12.12

(iii) 192.10.233.26. **[6 M]**

Ans. Refer to Page 1.23.

Summer 2024

1. State the difference between IPv4 and IPv6, (any two). **[2 M]**

Ans. Refer to Page 1.20.

2. Draw IPv6 packet format. **[2 M]**

Ans. Refer to Section 1.2.2.

3. Explain IPv4 addressing format with its classes. **[4 M]**

Ans. Refer to Section 1.2.1.

4. Explain different transition methods of IPv4 to IPv6. **[6 M]**

Ans. Refer to Section 1.2.

5. For the given IP address below:

(1) Identify the class to which the IP address belong

(2) Identify host address

(3) Identify network address

(4) Calculate the number of host that can be assigned with each network. IP addresses are:

(i) 121.33.43.131 (ii) 15.15.15.15

(iii) 198.22.5.36 (iv) 126.120.10.80. **[6 M]**

Ans. Refer to Page 1.23.

Winter 2024

1. State any two advantages of IPv6 Protocol over IPv4 Protocol. **[2 M]**

Ans. Refer to Section 1.2.

2. Enlist any four extension headers of IPv6. **[2 M]**

Ans. Refer to Page 1.19.

3. State any two limitations of IPv4 Protocol. **[2 M]**

Ans. Refer to Section 1.2.

4. Draw a neat labelled sketch of IPv4 Header format. Also explain (i) Service type (ii) Identification (iii) Flag (iv) Header checksum fields of it. **[4 M]**

Ans. Refer to Section 1.2.1.

5. A block of IP address is granted to a small organization. From this block of address one address is 205.16.37.39/28. Find

(i) First address of the block (ii) Last address of the block

(iii) Subnet Mask (iv) No. of Hosts. **[4 M]**

Ans. Refer to Page 1.35.

6. Draw a neat labelled sketch of IPv6 header format and explain all the fields of IPv6 header. **[6 M]**

Ans. Refer to Section 1.2.2.

7. For the following IP address given below: (i) 208.34.54.12 (ii) 238.34.2.1 (iii) 114.34.2.8 (iv) 129.14.6.8

(1) Identify the classes of IP address.

(2) Identify Network address section of each.

(3) Identify Host address section of each.

(4) Calculate number of Hosts that can be assigned with each network. **[6 M]**

Ans. Refer to Page 1.21.

❖❖❖