

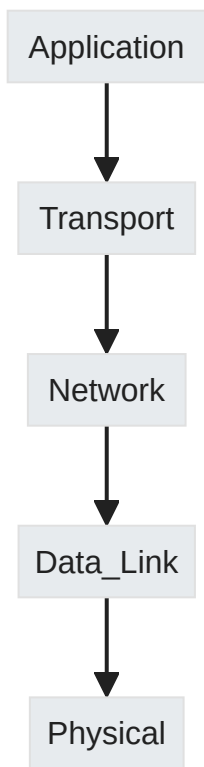
Network Layer Protocols and IP Addressing

1 Network Layer Protocols and IP Addressing

1.1 Network Layer Protocols

- Referred to as the IP layer, includes protocols like ICMP and IPX in addition to IP.
 - **ICMP (Internet Control Message Protocol):** A protocol for sending alerts about network issues like unavailable services or unreachable devices.
 - **IPX (Internetwork Packet Exchange):** An old protocol for sending data across Novell NetWare(Software) networks, now largely Outdated.
 - **IP (Internet Protocol):** The main protocol for sending data packets across the internet using unique addresses.

1.1.1 TCP/IP Model Layers



1.1.2 Protocols Overview


- **IP (Internet Protocol):** known as logical address since it's changed due to multiple reasons
 - **IPv4:** Standard internet protocol with 32-bit addresses.
 - **IPv6:** Newer version with 128-bit addresses for increased address space.

1.1.3 Data Encapsulation

Data transfer involves encapsulating data at each layer with specific headers.

Layer	PDU Name	Header Added
Application	Data	None
Transport	Segment	TCP/UDP
Network	Packet	IP

Layer	PDU Name	Header Added
Data Link	Frame	Ethernet

 Encapsulation wraps data with necessary protocol information before transmission across a network.

1.1.4 IPv4 Packet Format

Version	Header Length	Type of Service	Total Length	
Identification			Flags	Fragment Offset
TTL	Protocol		Header Checksum	
Source IP Address				
Destination IP Address				
Options				Padding

Component	Size (Bits)	Description
Version	4	Indicates the IP version (IPv4) or (IPv6).
Header Length	4	Specifies the header size in 32-bit words. Minimum value is 5 (indicating 20 bytes) without options.
Type of Service	8	Used for Quality of Service (QoS); directs routers to handle the packet with a certain level of precedence.
Total Length	16	The entire packet size, including header and data, in bytes. Maximum size is 65,535 bytes.
Identification	16	A unique identifier for fragmented packets to aid in reassembly at the destination.
Flags	3	Control flags related to fragmentation (e.g., whether a packet can be fragmented).
Fragment Offset	13	Indicates where in the original data this fragment belongs; used during reassembly of

Component	Size (Bits)	Description
		fragmented packets ; to help the receiver assemble the fragments.
Time to Live (TTL)	8	Limits the packet's lifespan; decrements on each router hop and discards if it reaches zero to prevent looping.
Protocol	8	Identifies the protocol of the encapsulated data (e.g., TCP, UDP). 1 : ICMP 2 : IGMP 6 : TCP 17 : UDP
Header Checksum	16	A checksum used for error-checking the header only; recalculated at each hop.
Source IP Address	32	The IP address of the originating host sending the packet.
Destination IP Address	32	The intended recipient's IP address for this packet.
Options	Variable	Optional parameters for additional features; rarely used and not included in minimum header length calculation.
Padding	<i>Variable</i>	<i>Used to ensure that the header's length is a multiple of 32 bits; filled with zeros.</i>

- **Flags & Fragment Offset:** Used during packet fragmentation and reassembly to ensure packets are properly reconstructed.
- The Flags field is 3 bits long
 1. **Reserved Fragment (bit):** Always set to 0; not used.
 2. **Don't Fragment (DF) bit:** If 1, the packet can't be split; if 0, it can be.
 3. **More Fragments (MF) bit:** If 1, more packet pieces are coming; if 0, this is the last or only piece.



TTL prevents infinite loops by discarding packets after they pass through a certain number of routers.

Default is 255

1.2 Introduction to IPv4 Addresses

IP Address —Identifies→ Node on Network —Used For→ Data Forwarding

An IP address uniquely identifies a node on a network and is used to forward data packets.

1.2.1 Address Notation & Range

- **IPv4:** 32 bits long in dotted decimal notation (e.g., 192.168.10.14).
- **Range:** 0.0.0.0 to 255.255.255.255 .
- Conversion between decimal and binary systems
- 192

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	0	0	0	0	0	0

1.2.2 IP Address Structure

- **Network part:** Identifies the network.
- **Host part:** Identifies hosts within that network.



Network **mask/subnet mask**: distinguishes between these two parts.

1.2.2.1 Example of Structure and Notation

Example

IP address: 192.168.10.1

Network mask: 255.255.255.0 or /24 notation.

Network part is: 192.168.10.0

Host part is: 0.0.0.255

1.2.3 Classification of Addresses (IPv4)

Class	Leading Bits	Address Range	Default Mask	Purpose
A	0xxx...	0.0.0.0– 127.255.255.255	/8	Large networks
B	10xx...	128.0.0.0– 191.255.255.255	/16	Medium networks
C	110x...	192.0.0.0– 223.255.255.	/24	Small networks

Calculation

A:

1	0	0	0	0	0	0	0
128	0	0	0	0	0	0	0

$$0 - 128 - > 127$$

Calculation

Same idea for B , C same as A but with more leading 1's

🌐 Classes D (224.x.x.x–239.x.x.x) for multicast and E (240.x.x.x–254.x.x.x) for research are not typically assigned to hosts.

Multicast address: is used to implement one-to-multiple message transmission.

1.2.4 IP Address Types

- **Network address/network ID:** identifies a network.
- **Broadcast address:** a special address used to send data to all hosts on a network ; last address of the network ID.
- **Available addresses:** IP addresses that can be allocated to device interfaces on a network ; address after network ID till Broadcast address.

Number of available addresses: $2^n - 2$ (n is the number of bits in the host part).
-2 for broadcast and network id.

1.2.4.1 IP Address Calculation

What are the network address, broadcast address, and number of available addresses of class B address 172.16.10.1/16?

☰ Example

Network ID: 172.16.0.0


Broadcast address: 172.16.255.255

Number of available addresses: $2^{16} - 2 = 65534$


Range of available addresses:

172.16.0.1 – 172.16.255.254

1.2.5 Private vs Public IPs

 **Private IP Addresses**

- Class A: 10.0.0.0 – 10.255.255.255
- Class B: 172.16.0.0 – 172.31.255.255
- Class C: 192.168.0.0–192.168.255.255

 **Public IP Addresses**

Allocated by IANA, unique across the Internet.

Private IPs require **NAT** to communicate with public networks.

1.2.5.1 Special IPv4 Addresses

Use Case	Address	Function
Broadcast	255.255.255.255	Used to send a message to all devices on the local network.
Any Network	0.0.0.0	Represents an unspecified host or the default network; used as a source address for devices seeking to obtain an IP assignment.
Loopback	127.0.0.0/8	Used by a host to send traffic to itself for testing or inter-process communication.
Link-local	169.254.0.0/24	Automatically assigned to a device for local communications when no external DHCP server is available.

1.2.6 IPv4 vs IPv6 Comparison

Feature	IPv4	IPv6
Length	32 bits	128 bits
Address Types	Unicast, Broadcast, Multicast	Unicast, Multicast, Anycast
Characteristics		
Address Availability	Limited number of addresses	Virtually unlimited number of addresses
Packet Header Design	Not as efficiently designed	Simplified packet header for more efficient routing
Network Dependency	ARP dependency can cause flooding	Automatic address allocation reduces dependencies

1.3 Subnetting

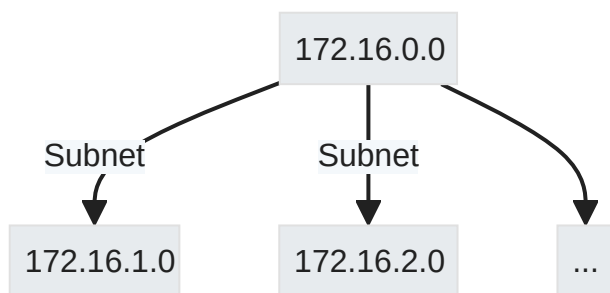
Why Subnetting?

Reduces broadcast domains, increases network efficiency, and improves IP address usage.

- **technique:**
 - **VLSM (Variable Length Subnet Masking):** A technique that allows network administrators to divide an IP address space into subnets of different sizes, optimizing the use of IP addresses based on the varying needs of each subnet.
 - **FLSM (Fixed Length Subnet Masking):** A subnetting approach where all subnets are created equal in size, using a consistent subnet mask, which can lead to inefficient use of IP addresses if subnets have widely differing numbers of hosts.

1.3.1 Class B Address Example

Example 172.16.0.0 to subnets each subnet support 200 user



Subnet	Network ID	Network Broadcast	Available Address
Subnet 1	172.16.1.0	172.16.1.255	$2^8 - 2 = 254$
Subnet 2	172.16.2.0	172.16.2.255	$2^8 - 2 = 254$
Subnet X	172.16.X.0	172.16.X.255	$2^8 - 2 = 254$

Tip

- Take bits from the host part to create a subnet.
- Use Variable Length Subnet Mask (VLSM) for efficiency.

1.4 ICMP (Internet Control Message Protocol)

Role & Uses:

- Helper protocol used alongside IP.
- Handles error messages and Functioning info.

ICMP Types:

Type	Code	Description
0	0	Echo Reply
3	0-3	Destination Unreachable
5	0	Redirect
8	0	Echo Request

Warning

ICMP can be exploited for network attacks; thus, it should be properly secured.

ICMP Redirect messages are sent by routers to tell a computer to use a more direct route for sending data to its destination, improving network efficiency.

Ping uses ICMP (**Echo Request and Echo Reply**) to test if a computer can communicate with another on the network, measuring how long it takes for messages to go back and forth.

ICMP is a protocol (**Tracert**) that helps identify network issues by sending error messages, like "Destination Unreachable," when data can't reach its intended target. The Tracert tool uses ICMP to map the route data takes to its destination by sending packets with increasing TTL values until the packets reach their endpoint, returning timing information at each hop.

1.5 IPv4 Address Configuration & Basic Application

Configuration Steps:

1. Enter Interface View:

```
M↓ Markdown ↕
1 [Huawei] interface <interface-type> <interface-number>
```

2. Assign IP Address:

```
M↓ Markdown ↕
```

```
1 [Huawei-GigabitEthernet0/0/1] ip address <ip-address> {  
  <mask> | <mask-length> }
```

mask: specifies a subnet mask. The value is in dotted decimal notation.
mask-length: specifies a mask length. The value is an integer ranging from 0 to 32.

1.5.1 Logical vs Physical Interfaces:

Physical interfaces are Physical ports on devices whereas logical interfaces like VLANIF or Loopback are virtual and always up.

A device deletes data not meant for its IP if it's routed through Loopback interface.

1.5.2 Network IP Address Planning

Objectives:

- **Uniqueness:** Each device on the network must have a distinct IP address to avoid conflicts.
- **Continuity:** The range of IP addresses should be contiguous to simplify routing and network management.
- **Scalability:** The plan should accommodate future growth without major changes to the existing structure.
- **Easy Management:** The address scheme should be logical and structured to make administration tasks straightforward.
- **High Utilization:** Efficient use of assigned IP spaces to minimize waste and maximize the available address pool.