Chapter Three

Network Layer Addressing

What is the Internet?

- It is a "network of networks”
- Up until the early 1990s, the Internet was largely populated by academic, government, and industrial researchers
- the WWW (World Wide Web) changed all that and brought millions of new, non-academic users to the net
- Uses TCP/IP protocols and packet switching

How the Internet Works?

- the major backbone operators, companies like **AT&T** and **Sprint**, operate large international backbone networks,
  - with thousands of routers connected by high-bandwidth fiber optics
- Large corporations and hosting services that run server farms connect directly to the backbone
- To allow packets to hop between backbones, all the major backbones connect at the **NAPs** (Network Access Points)
- **NAP** is a room full of routers, at least one per backbone
- A LAN in the room connects all the routers
- The two core protocols are **TCP (**Transmission Control Protocol) and **IP** (the Internet Protocol)

IP versions and Addressing

- Each TCP/IP host is identified by a logical IP address
- A unique IP address is required for each host and network component that communicates using TCP/IP
- Each IP address includes a network ID and a host ID
- We have two versions of IP, IPv4 and IPv6
- IPv4 address is 32 bits long,
- IPv6 address is 128 bits long

IPv4

- IPv4 (simply IP from now on) address consists of 32 bits of information
- These bits are divided into four sections, referred to as *octets* or bytes
- You can depict an IP address using one of three methods:
  - Dotted-decimal, as in 172.16.30.56
  - Binary, as in 10101100.00010000.00011110.00111000
  - Hexadecimal, as in 82 39 1E 38

- **Classifying IP Addresses**
  - There are five different address classes: A, B, C, D, and E.
  - The first three classes A through C, each use a different size for the network ID and host ID portion of the address
  - Class D is for special type of address called a **Multicast Address**
  - Class E is an **experimental** address class that isn't used.
  - The 32-bit IP address is a structured or hierarchical address
  - In this scheme, a part of the address is designated as the network address, and the other part is designated as either the subnet and host or just the node address
  - The first four bits of the IP address are used to determine into which class a particular address fits

- If the first bit is a **zero (0)**, the address is Class A address.
- If the first two bits are **10**, the address is a Class B address.
- If the first three bits are **110**, the address is a Class C address.
- If the first four bits are **1110**, the address is a Class D address.
- If the first four bits are **1111**, the address is a Class E address
- **Class A Addresses**
  - the first octet is the network ID, and the remaining three octets are the host ID
  - only 126 Class A networks can exist in the entire Internet
  - each Class A network can accommodate more than 16 million hosts
  - Only about 40 Class A addresses are actually assigned to companies or organizations
  - The rest are
    - either reserved for use by IANA (Internet Assigned Numbers Authority) or
    - are assigned to organizations that manage IP assignments for geographic regions such as Europe, Asia, and Latin America

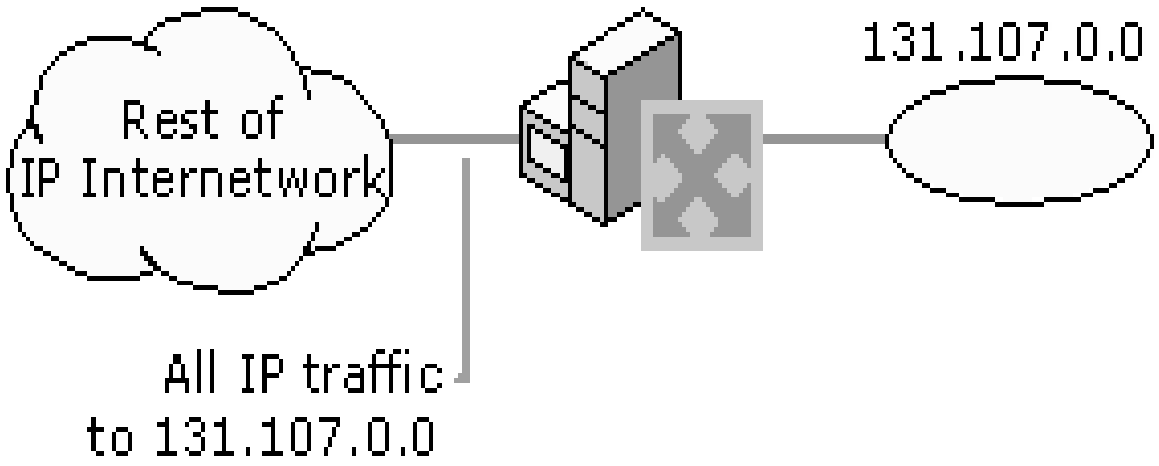
- **Class B addresses**
  - the first two octets of the IP address are used as the network ID, and the second two octets are used as the host ID
  - a total of 16, 384 Class B network can exist
  - Each Class B address can accommodate more than 65,000 hosts
  - **Problem**: careless assignment of Class B addresses can lead to a large percentage of the available host addresses being wasted on organizations that don't need them
- **Class C addresses**
  - the first three octets are used for network ID, and the fourth octet is used for the host ID
  - each Class C network can accommodate only 254 hosts
  - allow for more than 2 million networks
  - **Problem**: networks are too small

- The following table summarizes the details of each address class

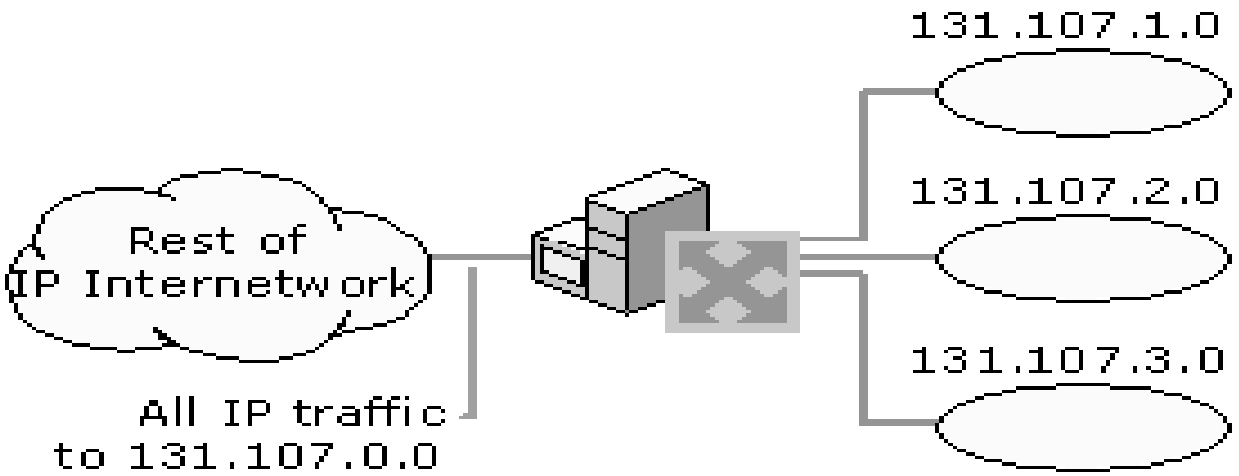
Class	Address Number Range	Starting Bits	Length of Network ID	Number of Networks	Host
A	1 – 126.x.y.z	0	8	126	16,777,214
B	128 – 191.x.y.z	10	16	16, 384	65,534
C	192 – 223.x.y.z	110	24	2,097,152	254

- **Subnets and Subnet Masks**
  - **Subnetting** is the process of creating networks that aren't limited to the scales provided by Class A, B, C IP addresses
  - **Subnetting** is used to create smaller broadcast domains and to better utilize the bits in the host ID.
  - With subnetting, you can create networks with more realistic host limits
  - Subnetting provides a more flexible way to designate which portion of an IP address represents the network ID and which portion represents the host ID.
  - Subnetting lets you select an arbitrary number of bits to use for the network ID

- Two reasons compel people to use subnetting
  - to allocate the limited IP address space more efficiently
  - performance reasons – networks are segmented into smaller broadcast domains
- A **subnet** is a network that falls within a Class A, B, or C network
- Subnets are created by using one or more of the Class A, B, or C host bits to extend the network ID
- subnets can have network IDs of any length
- The router is aware of the separate sub-netted network IDs and will route IP packets to the appropriate subnet



Network 131.107.0.0 before subnetting



Network 131.107.0.0 after subnetting

- **Subnet Masks**
  - A 32-bit number which is used to inform the router which portion of the host ID should be used for the subnet network ID
  - The bits of the subnet mask are defined as:
    - All bits that correspond to the network ID are set to 1.
    - All bits that correspond to the host ID are set to 0
  - Each host on a TCP/IP network requires a subnet mask even on a single-segment network
  - A default subnet mask is based on the IP address classes
  - the default subnet masks are
    - Class A – 255.0.0.0
    - Class B – 255.255.0.0
    - Class C – 255.255.255.0

- To determine the network ID of an IP address, the router must have both the IP address and the subnet mask.
- The router then performs a bitwise operation called a Logical AND on the IP address in order to extract the network ID
- **For example**, here's how the network address is extracted from an IP address using the 20-bit subnet mask from the previous example:

	144	28	16	17
IP address:	10010000	00011100	00100000	00001001
Subnet mask:	11111111	11111111	11110000	00000000
Network ID:	10010000	00011100	00100000	00000000
	144	28	16	0

- Thus, the network ID for this subnet is **144.28.16.0**

- **Network Prefix**
  - is a shorthand notation that is used to indicate how many bits of an IP address represent the network ID
  - is indicated with a ***slash*** immediately after the IP address, followed by the number of network ID bits to use
  - For example, the IP address 144.28.16.17 with the subnet mask 255.255.240.0 can be represented as ***144.28.16.17/20***
  - Network prefix notation is also called **Classless Inter-Domain Routing** notation, or just **CIDR** for short

- The table lists the default subnet masks using the network prefix notation for the subnet mask

Address Class	Bits for Subnet Mask	Network Prefix
Class A	11111111 00000000 00000000 00000000	/8
Class B	11111111 11111111 00000000 00000000	/16
Class C	11111111 11111111 11111111 00000000	/24

- Since all hosts on the same network must be using the same network ID, the ID must be defined by the same subnet mask
- For example, 157.55.0.0/16 is not the same network ID as 157.55.0.0/24.
  - The network ID 157.55.0.0/16 implies a range of valid host IP addresses from 157.55.0.1 to 157.55.255.254.
  - The network ID 157.55.0.0/24 implies a range of valid host IP addresses from 157.55.0.1 to 157.55.0.254.

- A few additional restrictions that are placed on subnet masks are:
  - The minimum number of network ID bits is **eight**.
  - The maximum number of network ID bits is **30**.
  - Because the network ID is always composed of consecutive bits set to 1, only **nine** values are possible for each octet of a subnet mask (including 0).

- **Subnetting Example**
  - Suppose we are using 255.255.240.0 as a subnet mask and 172.16.0.0 as a Network address (172.16.0.0/20)
  - answer five simple questions:
    1. How many subnets does the subnet mask produce?
    2. How many valid hosts per subnet?
    3. What are the valid subnets?
    4. What are the valid hosts in each subnet?
    5. What is the broadcast address of each subnet?
  - How many subnets?
    - $2^x - 2$, where X is the amount of masked bits, or the 1s
    - In this example, . there are $2^4 = 16$ subnets

- How many hosts per subnet?
  - $2^x - 2$, where X is the amount of unmasked bits, or the 0s
  - In this example, there are $2^{12} - 2 =$ 4094 hosts per subnet
- What are the valid subnets?
  - 256 – subnet mask = base number.
  - For example, 256 – 240 = 16, 32, 48, … 224
- What are the valid hosts?
  - Valid hosts are the numbers between the subnets, minus all 0s and all 1s
- What is the broadcast address for each subnet?
  - Broadcast address is all host bits turned on, which is the number immediately after the last host number.

Valid subnet	**First Valid host**	**Last Valid host**	**Broadcast**
16	16.1	31.254	31.255
32	32.1	47.254	47.255

- **Public and Private Addresses**
  - there are two types of addresses employed on the Internet, ***public addresses and private addresses***
  - **Public Addresses**
    - Public addresses are assigned by **InterNIC** (Internet Network Information Center)
    - consist of class-based network IDs or blocks of CIDR-based addresses (called CIDR blocks) that are guaranteed to be globally unique to the Internet
  - ***Private Address***
    - An IP address in the private address space is never assigned as a public address
    - IP addresses within the private address space are known as private addresses

Reserved addresses

- some blocks of IPv4 addresses have a special usage
- These include :
  - 0.0.0.0/8, which is reserved for self-identification.
    - A common address in this block is 0.0.0.0, which is sometimes used when a host boots and does not yet know its IPv4 address.
  - 127.0.0.0/8, which is reserved for loopback addresses.
    - Each host implementing IPv4 must have a loopback interface (that is not attached to a datalink layer).
    - By convention, IPv4 address 127.0.0.1 is assigned to this interface.
    - This allows processes running on a host to use TCP/IP to contact other processes running on the same host.
    - This can be very useful for testing purposes.

- 169.254.0.0/16 is used for link-local addresses
  - Some hosts use an address in this block when they are connected to a network that does not allocate addresses as expected.
- 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16
  - are reserved for private networks that are not directly attached to the Internet.
  - These addresses are often called private addresses

- **10.0.0.0/8**
  - is a class A network ID
  - allows the following range of valid IP addresses: 10.0.0.1 to 10.255.255.254
  - has 24 host bits that can be used for any subnetting scheme within the private organization
- **172.16.0.0/12**
  - interpreted either
    - as a block of 16 class B network IDs or
    - as a 20-bit assignable address space (20 host bits) which can be used for any subnetting scheme within the private organization.
  - allows the following range of valid IP addresses: 172.16.0.1 to 172.31.255.254.

- **192.168.0.0/16**
  - interpreted
    - » either as a block of 256 class C network IDs
    - » or as a 16-bit assignable address space (16 host bits), which can be used for any subnetting scheme within the private organization
  - allows the following range of valid IP addresses: 192.168.0.1 to 192.168.255.254
- Traffic to destination private addresses are not reachable on the Internet.
- Internet traffic from a host that has a private address must
  - either send its requests to an application layer gateway (such as a proxy server), which has a valid public address,
  - or have its private address translated into a valid public address by a network address translator (NAT) before it is sent on the Internet

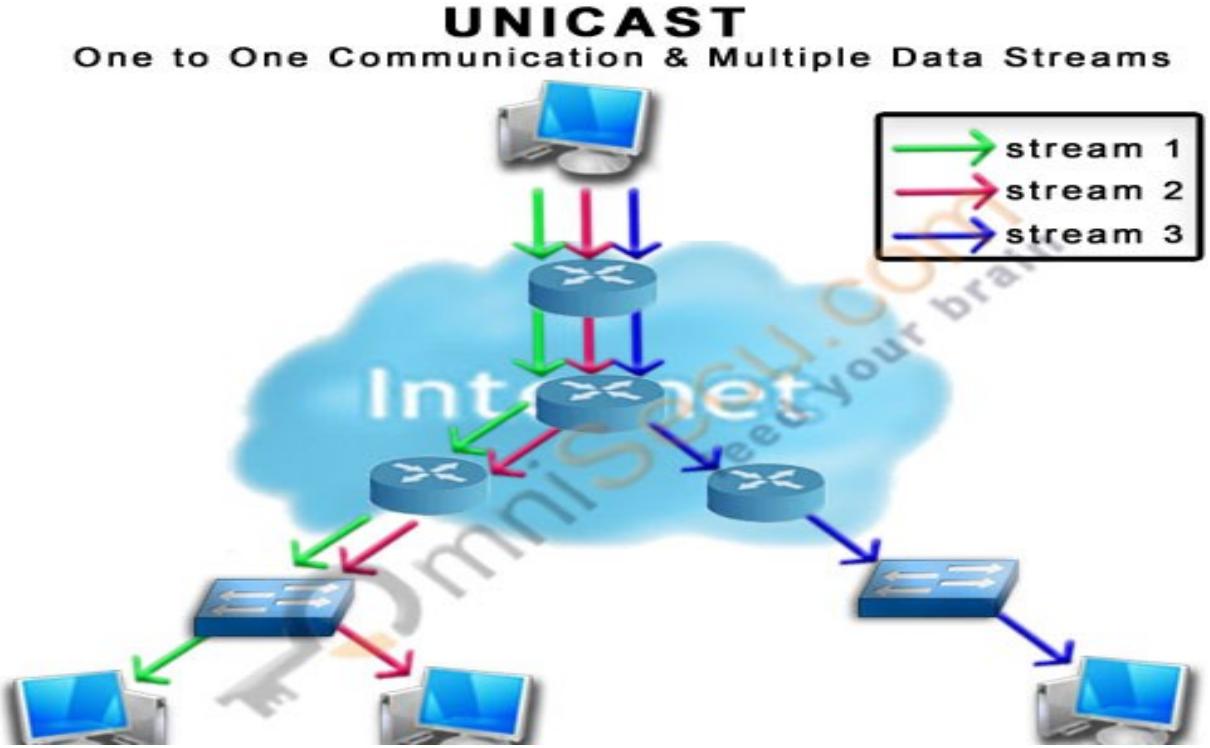
IP Version 6 (IPv6)

- is the successor of IP version 4
- All IPv6 addresses are 128 bits wide.
- This implies that there are 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456(3.4×10^{38}) different IPv6 addresses.
- As the surface of the Earth is about 510,072,000 km^2, this implies that there are about 6.67 × 10 IPv6 addresses per square meter on Earth.
  - Compared to IPv4, which offers only 8 addresses per square kilometer,
- IPv6 supports ***unicast***, ***multicast*** and ***anycast*** addresses.
- As with IPv4, an IPv6 ***unicast*** address is used to identify one datalink-layer interface on a host.
- If a host has several datalink layer interfaces (e.g. an Ethernet interface and a WiFi interface), then it needs several IPv6 addresses.

Types of Communication in IPv6

- the types of network communication in IPv4 are Unicast, Multicast and Broadcast.
- There is no broadcast in IPv6.
- The types of network communication in IPv6 are **Unicast, Multicast and Anycast.**
- **Unicast**
  - is a type of communication where data is sent from one computer to another computer.
  - is a one-to-one type of network communication.
  - Different data streams are generated for each Unicast connection.
  - This type of communication is the option when clients need different data from network server.

- In Unicast type of communication, there is only one sender, and only one receiver.
- Example
  - Browsing a website. (Webserver is the sender and your computer is the receiver.)
  - Downloading a file from a FTP Server. (FTP Server is the sender and your computer is the receiver.)



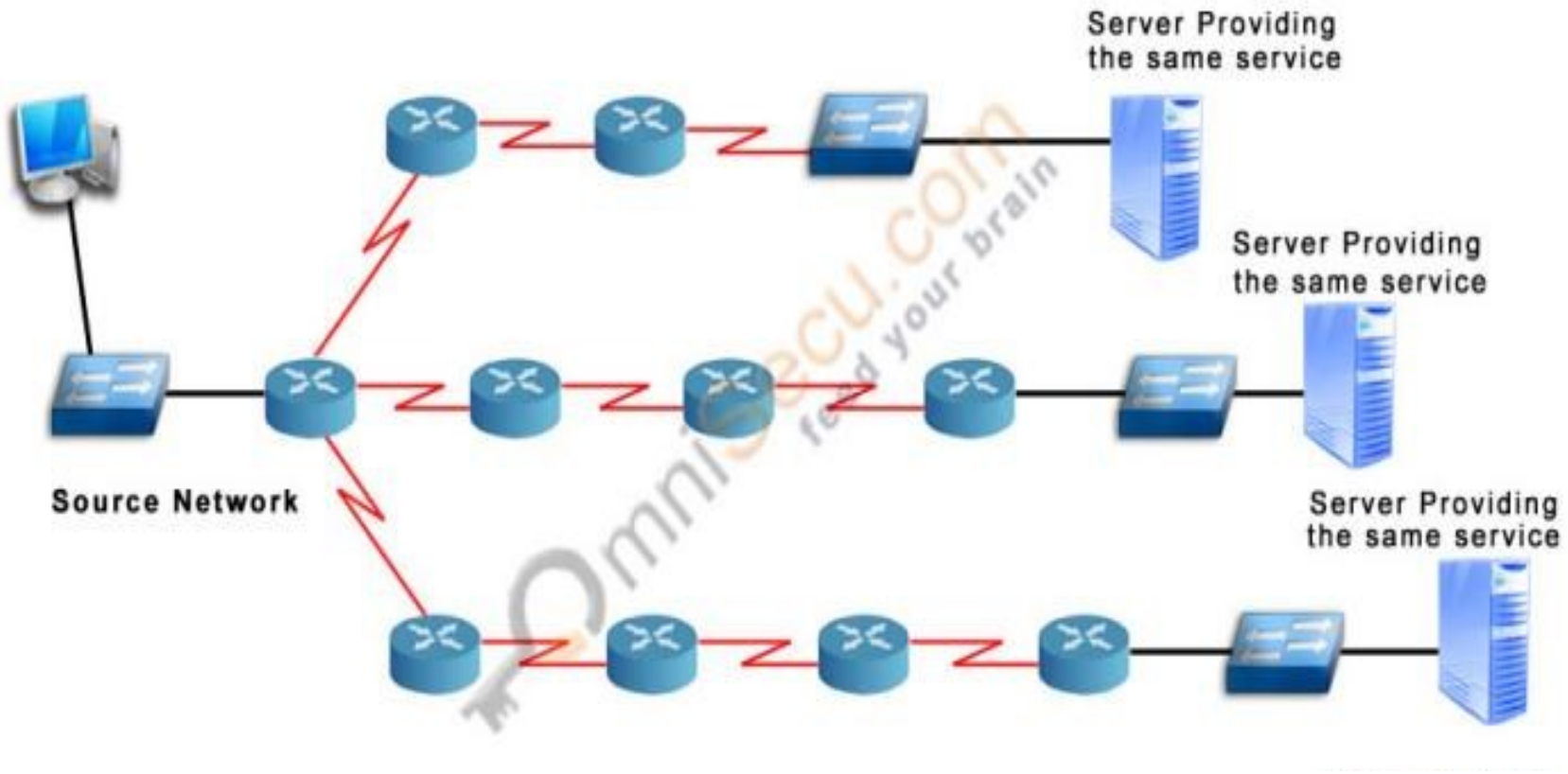
- Unicast Addresses
  - Global = 2000::/3
    - Is globally unique in the Internet
    - These are equivalent to IPv4 public addresses
    - Are globally routable addresses on IPv6 Internet.
    - The first 3 bits 001 are going to be the same for all global unicast addresses
    - Example:
      - 2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b
  - Link-local = FE80::/10
    - Can be used only on the local network link
    - Are not valid nor recognized outside the enterprise
    - Has the following format
      - Fe80::interface-ID/10
    - Example: fe80::23a1:b152
  - Unique Local = FD00::/8
    - Equivalent to 10.0.0.0/8

- **Multicast**
  - is a type of communication where multicast traffic addressed for a group of devices on the network.
  - IPv6 multicast traffic are sent to a group and only members of that group receive the Multicast traffic.
  - Devices which are interested in a particular Multicast traffic must join to that Multicast group to receive the traffic.
  - In Multicast, the sender transmit only one copy of data and it is delivered to many devices (Not all devices as in IPv4 Broadcast) who are interested in that traffic.
  - when multiple clients require same data at the same instance (for example, online TV) we can use multicast instead of unicast.
  - The multicast server generate only one stream of data and that stream is replicated to different devices, who are interested in that data traffic.

– Multicast type of network communication can save precious network bandwidth and also network device processor utilization.

- Multicast Addresses
  - Come from the FF00::/8 range
  - One of the multicast addresses is ff02::1
  - This address represents All-nodes multicast address
  - It is similar to the IPv4 broadcast address

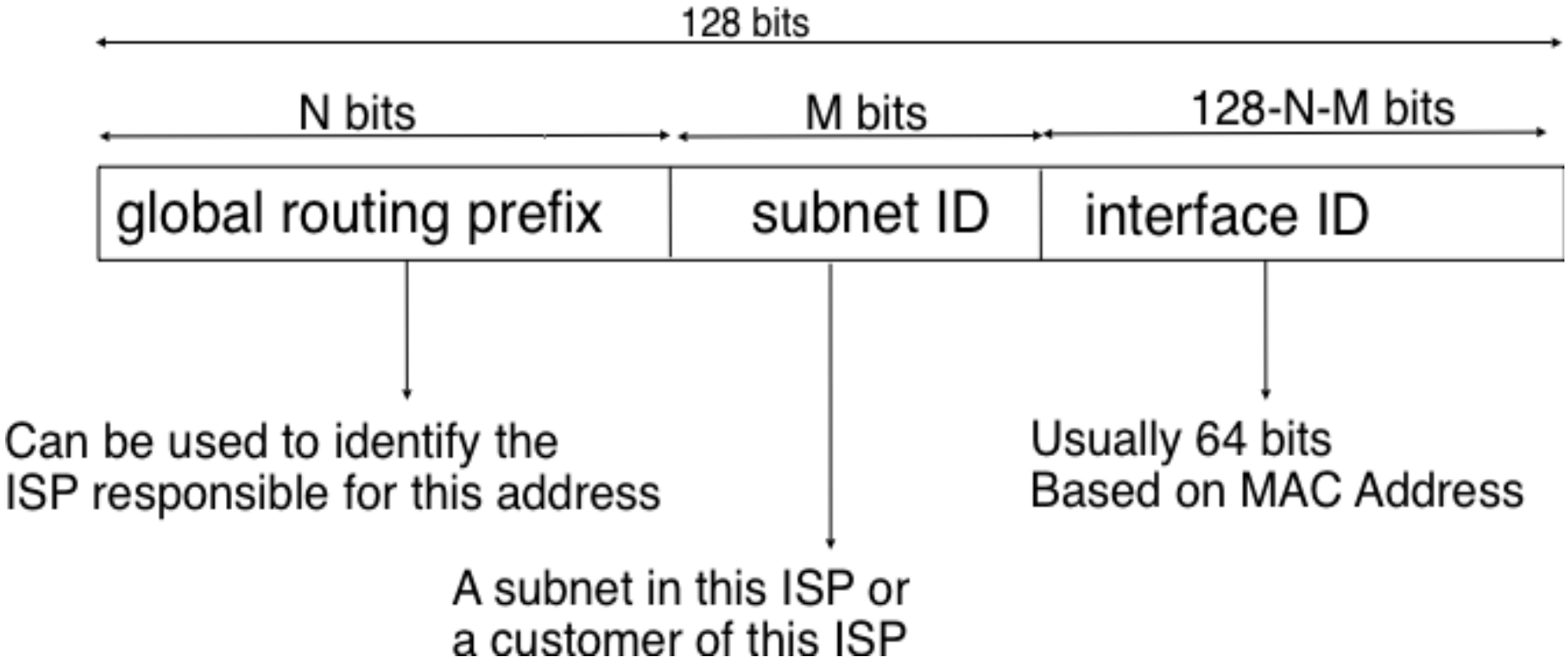
- **Anycast**
  - IPv6 datagrams from a source are routed to the nearest device (in terms of routing distance) from a group servers which provide the same service.
  - Every nodes which provide the same service are configured with same Anycast destination address.



- IPv6 Anycast network communication can identify the near node from a group of server nodes, which provides the same service and avail the service from the near server.

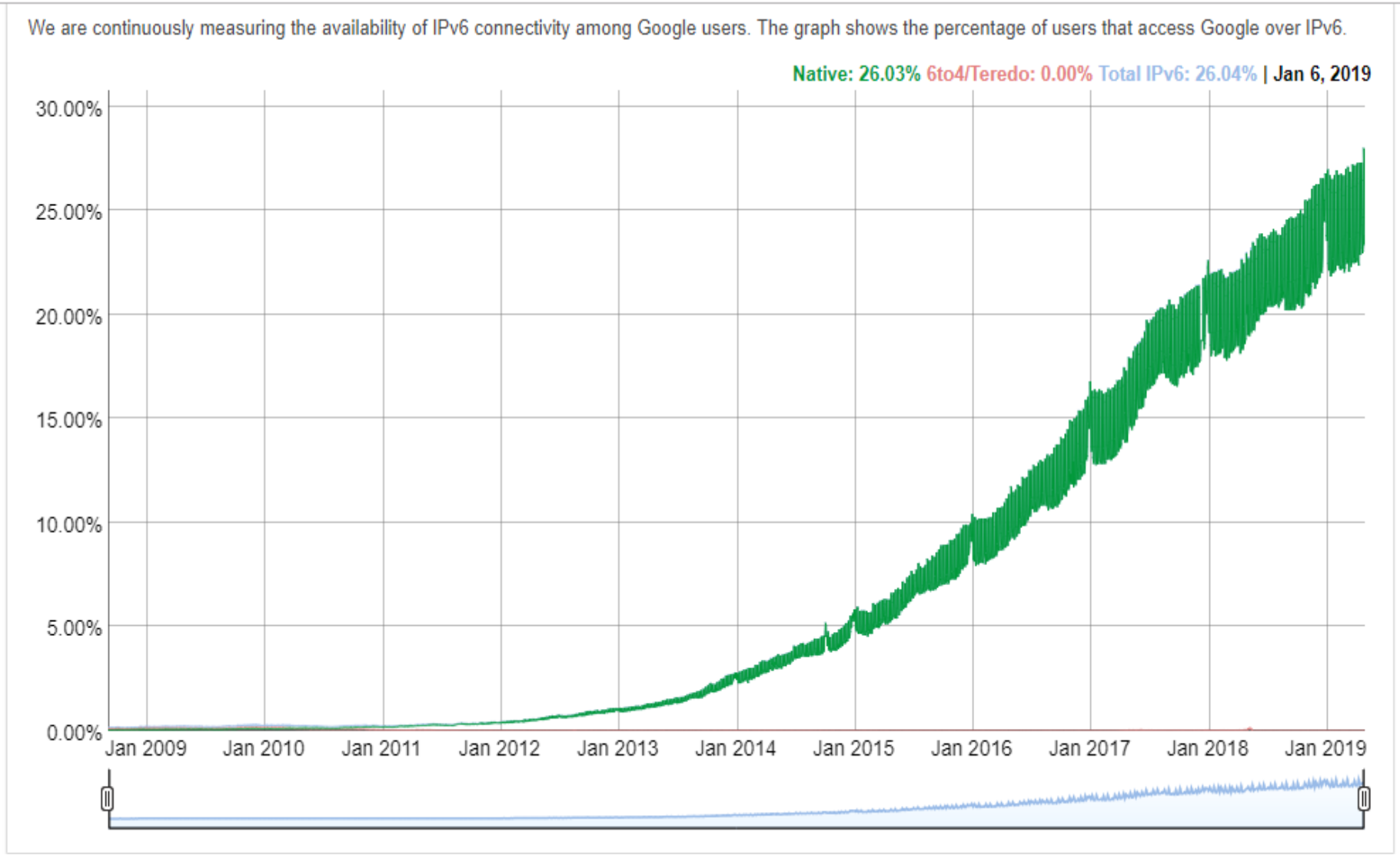
- An IPv6 unicast address is composed of three parts :
  1. A **global routing** prefix that is assigned to the Internet Service Provider that owns this block of addresses
  2. A **subnet identifier** that identifies a customer of the ISP
  3. An **interface identifier** that identifies a particular interface on an end-system
- interface identifiers are always **64 bits** wide.
  - This implies that while there are 2^{128} different IPv6 addresses, they must be grouped in 2^{64} subnets.
- The preferred format for writing IPv6 addresses is ***x:x:x:x:x:x:x:x***,
  - where the ***x*** 's are hexadecimal digits representing the eight 16-bit parts of the address.

- In general, an IPv6 unicast address is structured as shown in the figure below.



- Examples of IPv6 addresses :
  - abcd:ef01:2345:6789:abcd:ef01:2345:6789
  - 2001:db8:0:0:8:800:200c:417a
  - fe80:0:0:0:219:e3ff:fed7:1204
- IPv6 addresses often contain a long sequence of bits set to 0.
- In this case, a compact notation has been defined.
  - **::** is used to indicate one or more groups of 16 bits blocks containing only bits set to 0.
- For example,
  - 2001:db8:0:0:8:800:200c:417a is represented as 2001:db8::8:800:200c:417a
  - ff01:0:0:0:0:0:0:101 is represented as ff01::101
  - 0:0:0:0:0:0:0:1 is represented as ::1
  - 0:0:0:0:0:0:0:0 is represented as ::

- An IPv6 prefix can be represented as **address/length**, where ***length*** is the length of the prefix in bits.
- For example, the three notations below correspond to the same IPv6 prefix :
  - 2001:0db8:0000:cd30:0000:0000:0000:0000/60
  - 2001:0db8::cd30:0:0:0:0/60
  - 2001:0db8:0:cd30::/60



- **IPv6 Adoption**

RANK	IPV6%	COUNTRY
1	63.6%	India
2	51.1%	Saint Barthelemy
3	46.4%	United States
4	44.6%	Belgium
5	40.4%	Germany
6	37.5%	Viet Nam
7	37.4%	Malaysia
8	35.8%	Greece
9	31.2%	Taiwan
10	29.6%	Japan

- IPv6 Adoption By Country (The top 10 countries)

Some Network Services

- **Directory Service**
  - is simply the software system that stores, organizes and provides access to information in a directory
  - is a shared information infrastructure for locating, managing, administering, and organizing common items and network resources
  - is an important component of a NOS
  - Some of the examples of a directory service are:
    - LDAP (lightweight Directory Access Protocol) is a directory service in Unix operating system.
    - Active Directory: a directory service in Windows 2000 Server and later versions

- **Name Service**
  - maps the names of network resources to their respective network addresses
  - DNS and WINS (Windows Internet Name Service) is two examples of name services
  - **Domain Name System (DNS)**
    - is a hierarchical distributed database and an associated set of protocols that define
      - A mechanism for querying and updating the database
      - A mechanism for replicating the information in the database among servers
      - A schema of the database
    - contains various types of data including host names and domain names
    - The names in a DNS database form a hierarchical tree structure called the domain name space

- Domain names consist of individual labels separated by dots. For example: mydomain.microsoft.com
- A Fully Qualified Domain Name (FQDN)
  - is the complete domain name for a specific computer, or host, on the Internet
  - consists of two parts: the hostname and the domain name.
  - For example, an FQDN for a hypothetical mail server might be **mymail.somecollege.edu**. The hostname is **mymail**, and the host is located within the domain **somecollege.edu.**

- **Dynamic Host Configuration Protocol (DHCP)**
  - an open, industry standard, frees network administrators from having to configure all of the computers manually
  - assigns an IP address to a machine from the pool of available IP addresses

- The four steps to assign an IP address dynamically
  - The DHCP client asks for an IP address (DHCP Discover)
  - The DHCP server offers an address (DHCP Offer)
  - accepts the offer and requests the address (DHCP Request)
  - officially assigned the address (DHCP Acknowledge)
- the DHCP server places an administrator-defined time limit on the address assignment, called a **lease**