Network Troubleshooting and Security

Valiant Voora
Center of Excellence in Digital Forensics
CoEDF

E.R. Ramesh, M.C.A., M.Sc., M.B.A.,

Unit - 2

TCP/IP Basics & Routing

Introduction to MAC address
Introduction to IP address
Classes of IP address
Need for subnetting
Basics of IPV6
Static IP addressing
Dynamic IP addressing
Special IP addresses
Tools for Troubleshooting IP Problems
How routers work
Routing tables

Unit - 2

TCP/IP Basics & Routing

Network Address Translation
Dynamic routing
- Distance vector, Link state
  - EIGRP – OSPF

Troubleshooting Hot Standby Router Protocol (HSRP)
Dynamic routing
Working with routers, Connecting to routers
Basic router configuration, router problems.
Troubleshooting Bandwidth and Traffic – NetFlow -Applications-Protocols-Troubleshooting Configuration Issues
Tools for Network Troubleshooting

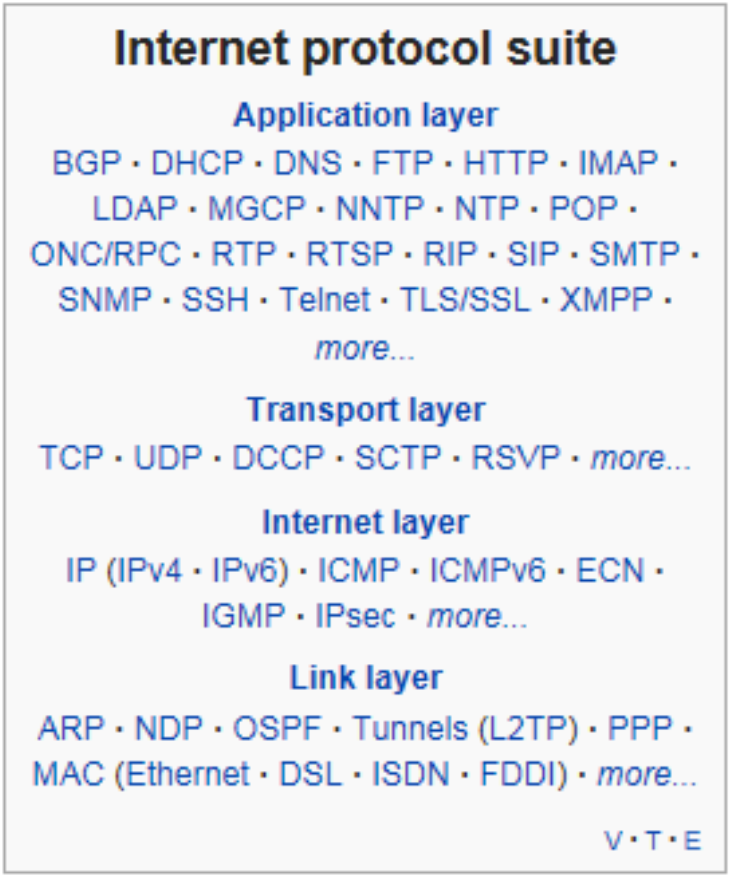
Basics – TCP/IP

- The **Transmission Control Protocol** (**TCP**) is one of the main protocols of the Internet protocol suite.
- It originated in the initial network implementation in which it complemented the Internet Protocol (IP).
- Therefore, the entire suite is commonly referred to as *TCP/IP*.
- TCP provides **reliable, ordered**, and **error-checked delivery** of a **stream of octets between applications running on hosts** communicating by an IP network.

Basics – TCP/IP

- Major Internet applications such as the **World Wide Web, email, remote administration**, and **file transfer rely on TCP.**

- Applications **that do not require reliable data stream service may use the User Datagram Protocol** (UDP), which provides a connectionless datagram service that **emphasizes reduced latency over reliability.**



Basics – TCP/IP – Network function

- The Transmission Control Protocol **provides a communication service at an intermediate level between an application program** and the **Internet Protocol**.

- It provides **host-to-host connectivity at the Transport Layer of the Internet model**. An application does not need to know the particular mechanisms for sending data via a link to another host, such as the required packet fragmentation on the transmission medium.

- At the transport layer, the **protocol handles all handshaking and transmission details** and presents an abstraction of the network connection to the application.

Basics – TCP/IP – Network function

- At the **lower levels of the protocol stack**, **due to network congestion**, **traffic load balancing**, or **other unpredictable network behavior**, **IP packets may be lost**, **duplicated**, or **delivered out of order**.

- TCP **detects these problems**, requests **re-transmission of lost data**, **rearranges out-of-order data** and even helps **minimize network congestion to reduce the occurrence of the other problems.**

Basics – TCP/IP – Network function

- **If the data still remains undelivered**, the **source is notified of this failure**. Once the **TCP receiver has reassembled the sequence of octets originally transmitted**, it **passes them to the receiving application.**

- Thus, TCP abstracts the application's communication from the underlying networking details.

- TCP is used extensively by many applications available by internet, including the **World Wide Web (WWW), E-mail, File Transfer Protocol, Secure Shell, peer-to-peer file sharing,** and **streaming media applications.**

Basics – TCP/IP – Network function

- **TCP is optimized for accurate delivery rather than timely delivery** and **can incur relatively long delays** (on the order of seconds) while waiting for out-of-order messages or re-transmissions of lost messages.

- Therefore, **it is not particularly suitable for real-time applications** such as **Voice over IP**. For such applications, protocols like the **Real-time Transport Protocol (RTP) operating over the User Datagram Protocol (UDP) are usually recommended instead.**

Basics – TCP/IP – Network function

- TCP is a **reliable stream delivery service which guarantees that all bytes received will be identical with bytes sent** and in the **correct order.**

- Since packet transfer by many networks is not reliable, a technique known as **'positive acknowledgement with re-transmission**' is used to **guarantee reliability**.

- This **fundamental technique requires the receiver to respond with an acknowledgement message** as **it receives the data**.

Basics – TCP/IP – Network function

- The **sender keeps a record of each packet it sends and maintains a timer from when the packet was sent**. The sender **re-transmits a packet if the timer expires** before receiving the message acknowledgement.

- The **timer is needed in case a packet gets lost or corrupted**.

- While **IP handles actual delivery of the data**, **TCP keeps track of** '**segments**' - the individual units of data transmission that a message is divided into for efficient routing through the network.

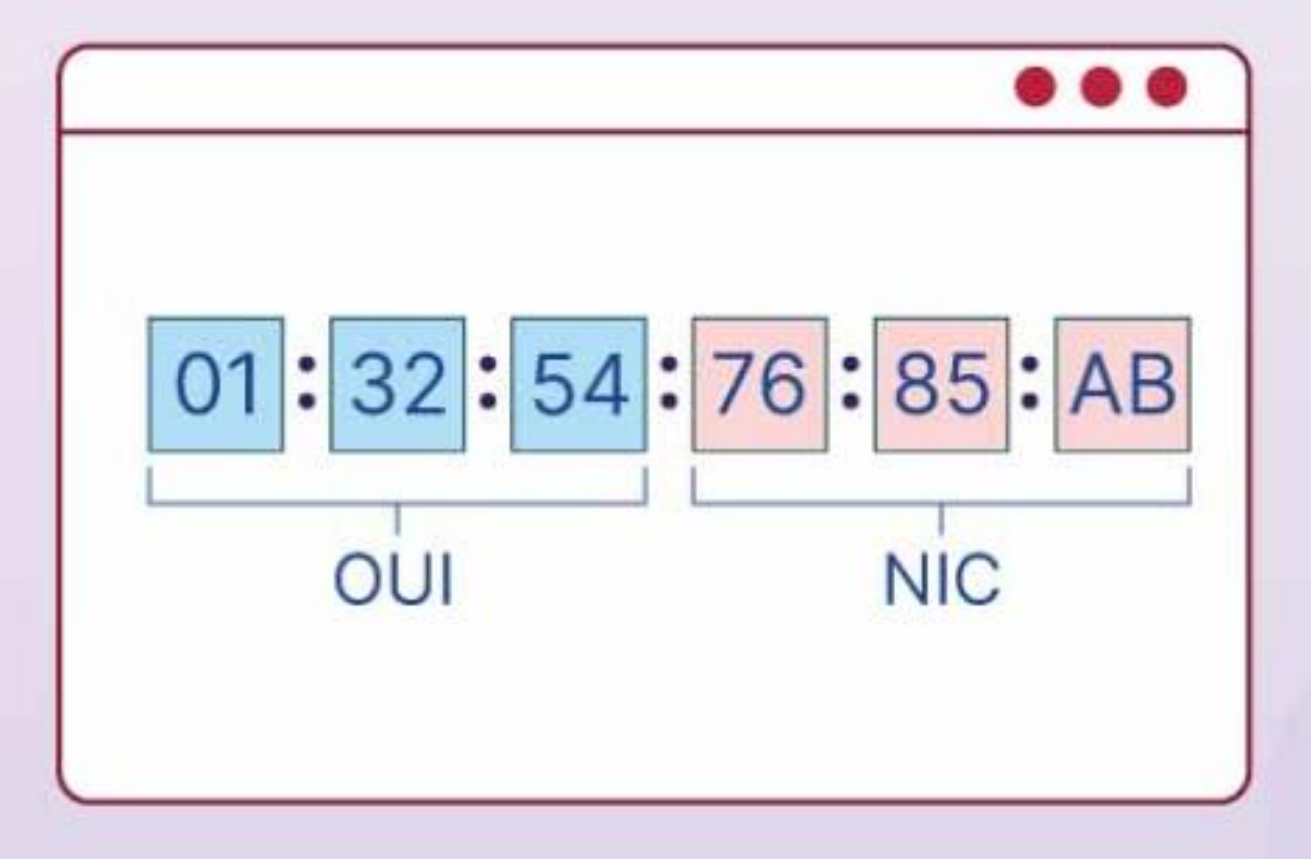
Basics – TCP/IP – Network function

- For example, **when an HTML file is sent from a web server**, the **TCP** software layer of that server **divides the sequence of file octets into segments and forwards them individually to the IP software layer** (Internet Layer).

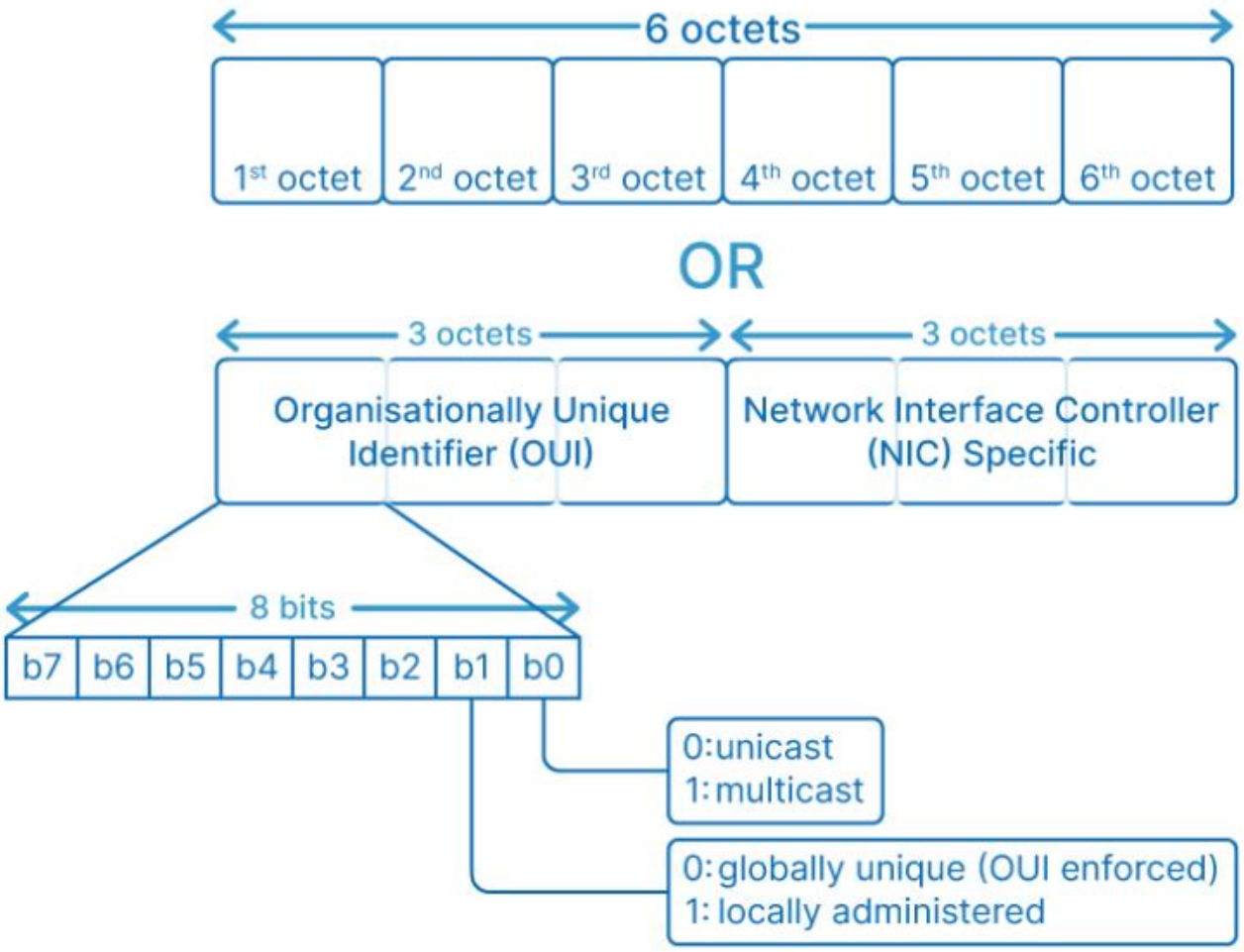
- The **Internet Layer encapsulates each TCP segment into an IP packet by adding a header that includes** (among other data) the destination IP address.

- When the **client program on the destination computer receives them, the TCP layer** (Transport Layer) **re-assembles the individual segments and ensures they are correctly ordered** and **error-free as it streams them to an application**.

MAC Address



Media Access Control

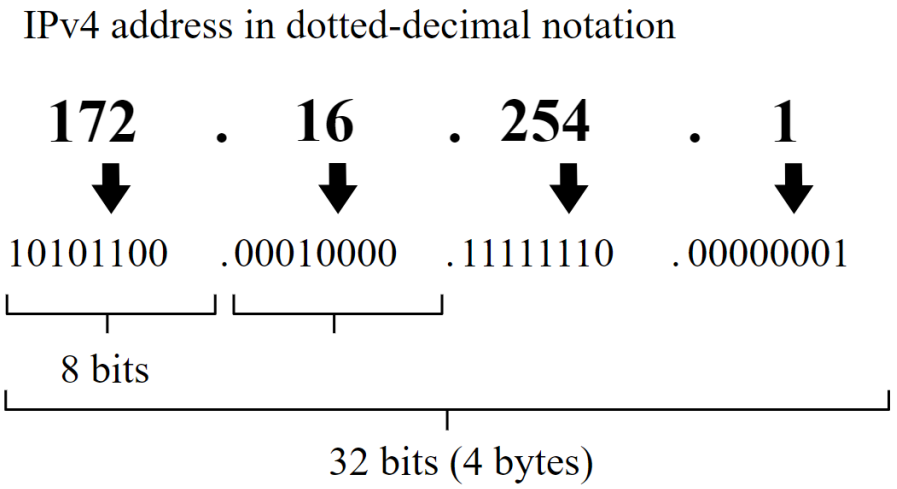


Media Access Control

- The format of the **MAC address is hexadecimal**.
- 00:0a:95:9d:67:16
- There are **twelve numero-alpha digits** in a MAC address that are **48-bit long**. The **first 24 bits** represent **Organizational Unique Identifier**, and the **remaining 24 bits** are **either for NIC** or are **vendor specific**.
- The first three octets are used as Organizationally Unique Identifier. The IEEE Registration Authority Committee assigns these MAC prefixes. The last three octets are specific to NIC and are used by manufacturer for every NIC cards. Vendors can use any sequence of digits to NIC-specific digits. In this case, the prefix must be the same as provided by IEEE.

IP Addresses

- An **Internet Protocol address (IP address)** is a **numerical label assigned to each device connected to a computer network** that **uses the Internet Protocol** for communication.
- An IP address serves two main functions: **host or network interface identification and location addressing.**



IP Addresses v4 and v6

- Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number.

- However, **because of the growth of the Internet and the depletion of available IPv4 addresses**, a new version of IP (IPv6), **using 128 bits for the IP address, was standardized in 1998**.

- IPv6 deployment has been ongoing since the mid-2000s.

IP Addresses v4 and v6

- **IP addresses are written and displayed in human-readable notations**, such as ***172.16.254.1*** **in IPv4**, and ***2001:db8:0:1234:0:567:8:1*** in **IPv6.**

- The size of the routing prefix of the address is designated in CIDR notation by suffixing the address with the number of significant bits, e.g., *192.168.1.15/24*, which is equivalent to the historically used subnet mask *255.255.255.0*.

IP Addresses

- IP address is a **32 bit integer**
  - **Refers to interface** rather than host
  - **Consists of network** and **host portions**
    - Enables routers to keep 1 entry/network instead of 1/host
  - **Class A, B, C for unicast**
  - **Class D for multicast**
  - **Class E reserved**
  - **Classless addresses**
- Written as **4 octets/bytes** in decimal format
  - E.g. 134.79.16.1, 127.0.0.1

IP Addresses

- **Class A: large number of hosts, few networks**
  - 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh
    - 7 network bits (0 and 127 reserved, so 126 networks), 24 host bits (> 16M hosts/net)
    - Initial byte 1-127 (decimal)
- **Class B: medium number of hosts and networks**
  - 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh
    - 16,384 class B networks, 65,534 hosts/network
    - Initial byte 128-191 (decimal)
- **Class C: large number of small networks**
  - 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh
    - 2,097,152 networks, 254 hosts/network
    - Initial byte 192-223 (decimal)
- **Class D: 224-239 (decimal) Multicast [RFC1112]**
- **Class E: 240-255 (decimal) Reserved**

Address depletion

- In 1991 IAB identified 3 dangers
  - Running out of class B addresses
  - Increase in nets has resulted in routing table explosion
  - Increase in net/hosts exhausting 32 bit address space

- Four strategies to address
  - Creative address space allocation {RFC 2050}
  - Private addresses {RFC 1918}, Network Address Translation (NAT) {RFC 1631}
  - Classless InterDomain Routing (CIDR) {RFC 1519}
  - IP version 6 (IPv6) {RFC 1883}

Creative IP address allocation

- Class A addresses 64 – 127 reserved
  - Handle on individual basis
- Class B only assigned given a demonstrated need
- Class C
  - divided up into 8 blocks allocated to regional authorities
  - 208-223 remains unassigned and unallocated

Creative IP address allocation

- The IP address space is managed globally by the Internet Assigned Numbers Authority (**IANA**), and by five **Regional Internet Registries** (**RIR**s) responsible in their designated territories for assignment to end users and local Internet registries, such as Internet service providers.

  - **AFRINIC** – Africa
  - **ARIN** – Antarctica, Canada, Parts of Caribbean and US.
  - **APNIC** – East Asia, Oceania, South Asia and Southeast Asia.
  - **LACNIC** – Most of Caribbean and Latin America.
  - **RIPE NCC** – Europe, Central Asia, Russia and West Asia.

Private IP Addresses

- IP addresses that are not globally unique, but used exclusively in an organization
- **Three ranges:**
  - **10.0.0.0 - 10.255.255.255 -** a single class A net
  - **172.16.0.0 - 172.31.255.255 -** 16 contiguous class Bs
  - **192.168.0.0 – 192.168.255.255 -** 256 contiguous class Cs
- Connectivity provided by Network Address Translator (NAT)
  - translates outgoing private IP address to Internet IP address, and a return Internet IP address to a private address
  - Only for TCP/UDP packets

IP Addresses

Class	Address or Range	Status
A	0.0.0.0 1.0.0.0 to 126.0.0.0 127.0.0.0	Reserved Available Reserved
B	128.0.0.0 to 191.254.0.0 191.255.0.0	Available Reserved
C	192.0.0.0 192.0.1.0 to 223.255.254 223.255.255.0	Reserved Available Reserved
D	224.0.0.0 to 239.255.255.255	Multicast group addresses
E	240.0.0.0 to 255.255.255.254 255.255.255.255	Reserved Broadcast

IP Addresses

Class	Public IP Ranges
A	1.0.0.0 to 9.255.255.255 11.0.0.0 to 126.255.255.255
B	128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255
C	192.0.0.0 to 192.167.255.255 192.169.0.0 to 223.255.255.255

Unique to Universe

Unique to Local Network

Private IP address space	
From	**To**
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

IP Addresses

- IPv4 supports maximum of (**4,294,967,296**) 4.3 Billions Approx.
- IPv4 is 32 bits
- IPv6 consists of eight number of four hexadecimal digits (2001:0db8:85a3:0000:0000:8a2e:0370:7334)
- IPv6 Uses 128 bits
- IPv6 supports maximum of (**340,282,366,920,938,463,463,374,607,431,768,211,456**)

IP v6 Address

- In IPv6, the address size was increased from 32 bits in IPv4 to 128 bits or 16 octets, thus providing up to 2^{128} (approximately 3.403×10^{38}) addresses. **This is deemed sufficient for the foreseeable future.**

- The intent of the new design was not to provide just a sufficient quantity of addresses, but also **redesign routing in the Internet by more efficient aggregation of subnetwork routing prefixes.**

- This resulted in slower growth of routing tables in routers. The smallest possible individual allocation is a subnet for 2^{64} hosts, which is the square of the size of the entire IPv4 Internet.

IP v6 Address

- At these levels, actual address utilization ratios will be small on any IPv6 network segment. The new design also provides the opportunity to separate the addressing infrastructure of a network segment, i.e. the local administration of the segment's available space, from the addressing prefix used to route traffic to and from external networks.

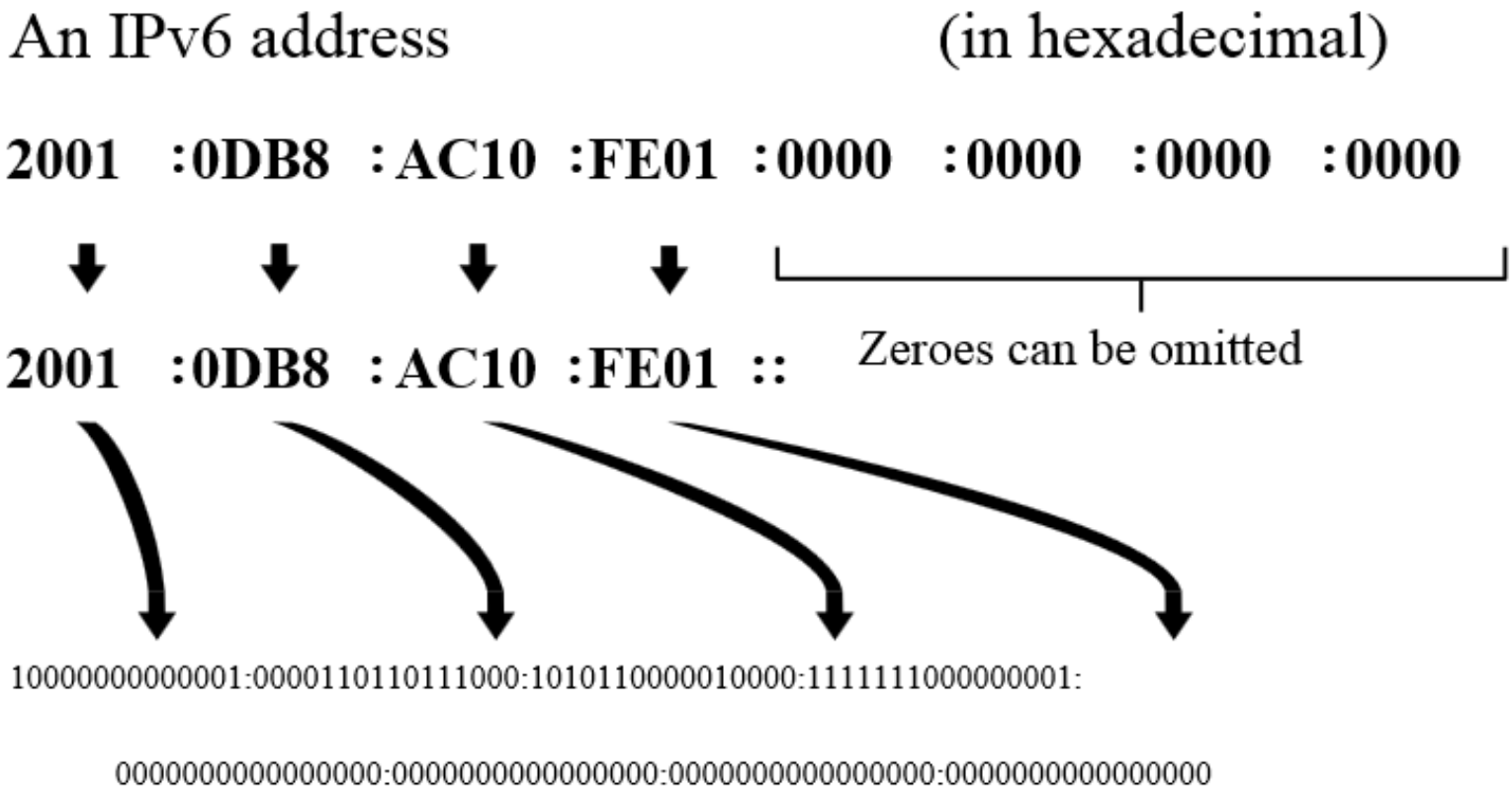
- **IPv6** has **facilities** that **automatically change the routing prefix of entire networks**, should the global connectivity or the routing policy change, without requiring internal redesign or manual renumbering.

IP v6 Address

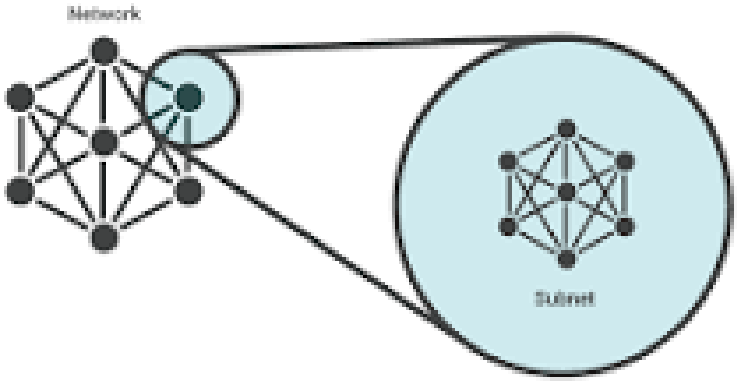
- The large number of IPv6 addresses allows large blocks to be assigned for specific purposes and, where appropriate, to be aggregated for efficient routing. With a large address space, there is no need to have complex address conservation methods as used in CIDR.

- All modern desktop and enterprise server operating systems include native support for the IPv6 protocol, but it is not yet widely deployed in other devices, such as residential networking routers, voice over IP (VoIP) and multimedia equipment, and network peripherals.

IP v6 Address



Need for subnetting



- Subnets make **networks more efficient**. Through subnetting, **network traffic can travel a shorter distance** without passing through unnecessary routers to reach its destination.

Need for subnetting

What Is Subnetting?

- The goal of subnetting is to **create a fast, efficient, and resilient computer network**. As networks become larger and more complex, the traffic traveling through them needs more efficient routes. If all network traffic was traveling across the system at the same time using the same route, bottlenecks and congestion would occur resulting in sluggish and inefficient backlogs.

- Creating a **subnet allows you to limit the number of routers that network traffic must pass through**. An engineer can **create smaller mini-routes within a larger network to allow traffic to travel the shortest distance possible**.

What Is Subnetting Used For?

- Organizing a **network in an efficient way** is crucial for large firms and those companies seeking to expand technologically. IP addresses can be kept geographically localized meaning that a subnet can be used for specific staffing structures to reduce traffic and maintain efficiency and order.

Need for subnetting

How Does Subnetting Work?

- IP addresses help to identify the pieces of hardware connected to your network. To locate a particular device, you would need to organize the IP addresses in a logical way. This is where subnetting excels as a tool to help you maintain efficiency across your network.

- There could be hundreds of thousands of devices that are connected within a network, and the corresponding IP addresses can create a complex route that traffic must travel. Subnetting limits the IP address usage to within a few devices.

- This allows an engineer to use subnetting to create sub-networks, sorting data so that it can travel without touching every part of the more complex routers. To do this, an engineer needs to match each IP address class to a subnet mask.

Need for subnetting

- A subnet mask echoes an IP address, but it can only be utilized within an internal network. This mask helps to identify which part of the IP address relates to the network and which part relates to the host so specific data is sent on particular routes according to its destination. A subnet mask creates the tool that enables a router to match an IP address with a sub-network.

Need for subnetting

Benefits of Subnetting

- Subnetting divides broadcast domains so traffic is routed efficiently, improving speed and network performance.

- A subnet mask ensures that traffic remains within its designated subnet. This reduces major congestion and reduces the load imparted on the network. With sub-networks, less distance needs to be traveled by data packets, enhancing network performance.

- Network security can be boosted. With different subnets within your larger network, you are more aware of route maps and can more easily identify potential threats. With subnets, devices will not be able to access the whole network, and companies can dictate which hardware and users have access to more sensitive data.

- Sound organization is crucial within large businesses. Subnetting allows companies to have full control over their traffic, data packets, network, and routers.

Static IP addressing

- A static Internet Protocol (IP) address (static IP address) is a permanent number assigned to a computer by an Internet service provider (ISP).
- A static IP address is also known as a fixed IP address or dedicated IP address and is the opposite of a dynamic IP address.
- A computer with an assigned static IP address uses the same IP address when connecting to the Internet.
- Static IP addresses are useful for gaming, website hosting or Voice over Internet Protocol (VoIP) services.
- Speed and reliability are key advantages. Because a static address is constant, systems with static IP addresses are vulnerable to data mining and increased security risks.

Static IP addressing

- An ISP is allocated a range of IP addresses. The ISP assigns each address to its networked computers via the **Dynamic Host Configuration Protocol (DHCP) server**, which is **configured to allocate static IP addresses to specific computers.**

- The addresses are used for network identification and communication. Allocation mechanisms vary, depending on platform, and include manually typing the IP address into the device or assigning it via a router.

- Unlimited IP address requirements were not considered when the Internet was first conceptualized. At that time, Internet Protocol version 4, based on 32-bit addressing (IPv4) allowed for 4.2 billion unique addresses.

- Even then, ISPs approached static addressing conservatively by limiting static addresses to unused IP addresses to facilitate temporary IP, or dynamic IP, addressing to requesting DHCP servers.

Static IP addressing

- With the rapidly expanding use of IP-addressable devices, IPv4's limitations became more apparent.

- The IPv6 protocol followed IPv4 and provided for 128-bit addressing for virtually unlimited IP addresses.

- Static IP address advantages include:
  - **Lower costs**
  - **Email server hosting capabilities**
  - **Easy maintenance**
  - **Ideal for online gaming**

- Static IP addresses are particularly useful for events such as hosting a website. With a dynamic IP address, every time the address changes, the router won't know which device in the network is the one hosting the site.

Static IP addressing

- A **static IP will let your customers find you via DNS**, instead. A static IP will **make easier to set up and use a Virtual Private Network** (VPN) since that address needs to be whitelisted as trusted just once.

- **Video and audio communications can also be stabilized when using a Voice over Internet Protocol** (VoIP). This is a particularly important aspect when a fast and stable connection is required, for example, for online gaming purposes.

Static IP addressing

Static IP addresses do have their **drawbacks**, though.

- The most evident one is that an **address that never changes is easier to be hacked as a malicious actor has much more time to identify** and leverage network vulnerabilities.

- Also, once a cybercriminal has "hooked" that IP, they can **continuously disrupt it via a cyberattack, like a prolonged DDoS attack**.

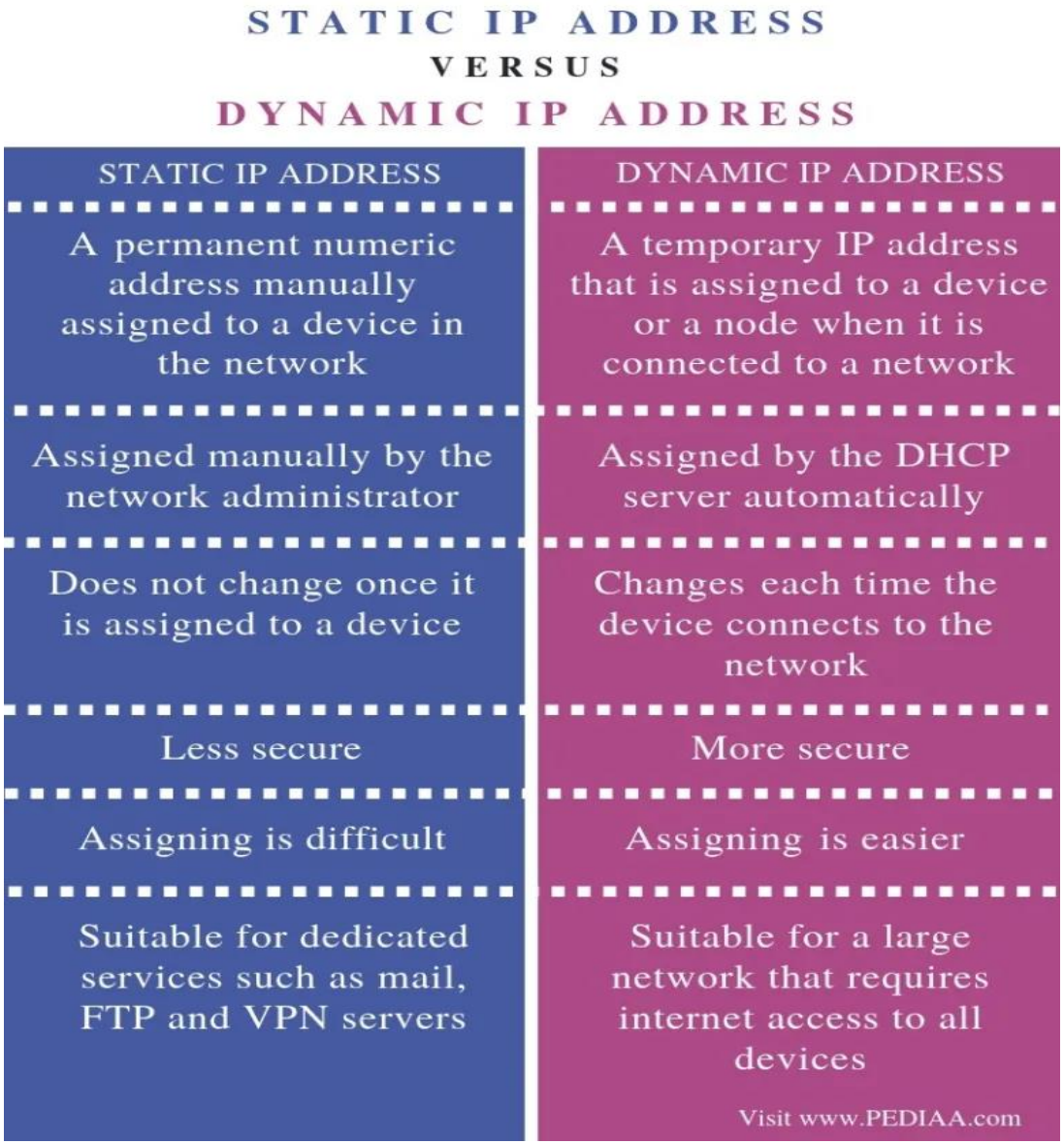
- A **static IP means that your physical location can be determined with ease**, which is a good thing if you need prompt geo-localization, but also a downfall if an **ill-intentioned user wants to find where you and your computer are located**.

Dynamic IP addressing

- A **dynamic IP address is an IP address that changes from time to time unlike a static IP address**. Most home networks are likely to have a dynamic IP address and the **reason for this is because it is cost effective for Internet Service Providers (ISP) to allocate dynamic IP addresses to their customers.**

- Instead of one IP address always being allocated to your home network (Static IP), your **IP address is pulled from a pool of addresses and then assigned to your home network by your ISP**. After a few days, weeks or sometimes months that **IP address is put back into the pool and you are assigned a new IP address.**

Static IP Address vs Dynamic IP address



Differences between static and dynamic IP address

Definition

- Static IP Address or Static Internet Protocol Address is a permanent numeric address manually assigned to a device in the network. Dynamic IP Address or Dynamic Internet Protocol Address is a temporary IP address that is assigned to a device or a node when it is connected to a network. Thus, this is the main difference between static and dynamic IP address.

Assigned by

- Another difference between static and dynamic IP address is that the static IP address is assigned manually by the network administrator while dynamic IP address is assigned by the DHCP server automatically.

Changes

- Static IP address does not change once it is assigned to a device. However, dynamic IP address changes each time the device connects to the network. Hence, this is also a major difference between static and dynamic IP address.

Differences between static and dynamic IP address

Security

- Furthermore, the static IP address is less secure while the dynamic IP address is more secure.

Manageability

- Also, assigning static IP addresses is difficult. But, assigning dynamic IP addresses is easier.

Usage

- Concerning the usage, the static IP addresses are suitable for dedicated services such as mail, FTP and VPN servers. While the dynamic IP addresses are suitable for a large network that requires internet access to all the devices.

Special IP addresses

- As in classful addressing, some blocks of addresses or some addresses in each block have been reserved for the special purpose & that's why they are termed as **special IP addresses**.

- The special addresses of classful addressing were inherited by the classless addressing when it was introduced in 1996.

- There can be an entire block of addresses reserved for special addressing or there can be some addresses in each block that are reserved for special addressing.

- In the following slides, we will discuss about **special blocks of addresses** and **special addresses in each block**.

Special IP addresses

1. Special Blocks of Addresses

- There are some blocks of addresses in IPv4 address space that are reserved for a special objective. The special blocks of addresses are listed below:

1. All Zeros Address
2. All Ones Address
3. Loopback Addresses
4. Private Addresses
5. Multicast Addresses

Special IP addresses

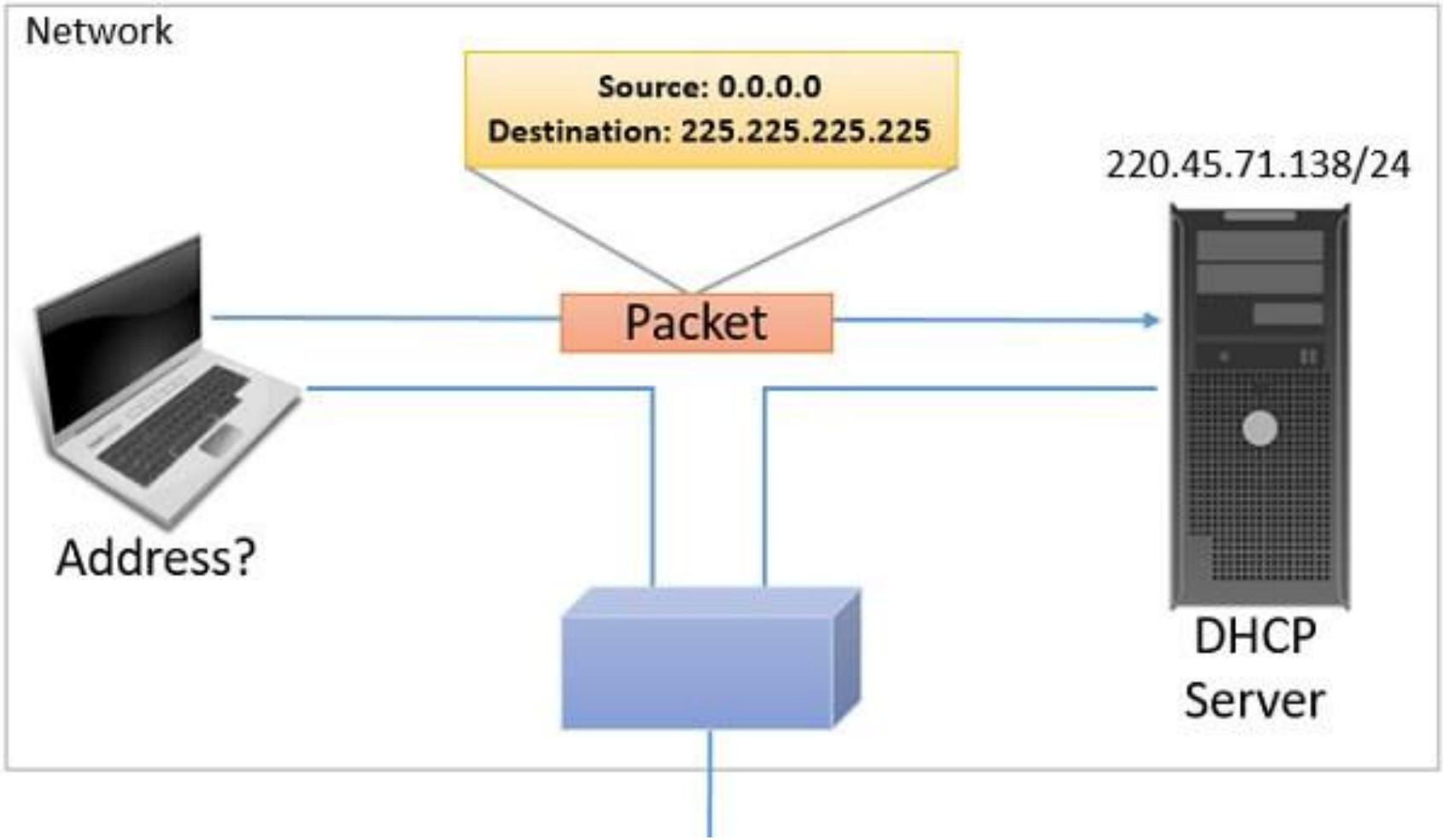
All Zeros Address

- The all-zeros address block **0.0.0.0/32** is a special block in Ipv4 address space. The length of the **prefix** here is **32**. The number of addresses in this block is equal to $2^{32-32} = 2^0 = 1$. So, this block has only one address with all the 32 bits as zero. This address is the **first address** in the IPv4 address space.

- Any host having this IP address means the **host is not connected to the TC/IP network**. When the host wants to get connected to the internet, it sends a request packet to the **bootstrap server** which is also called a **DHCP server**.

- The packet sent by the host to DHCP server has **source address** as **0.0.0.0** and **225.225.225.225** as the **destination address**. The DHCP server then assigns the IP address to the host and host then get connected to the Internet.

Special IP addresses



Special IP addresses

All One Address

- The block **225.225.225.225/32** is also a special block in IPv4 address space. Here, all the **32 bits** of **IPv4 address** is '**1**'. The length of the prefix here is 32. The number of addresses in this special block can be calculated as $2^{32-32} = 2^0 = 1$. This is the **last address** in IPv4 address space. T

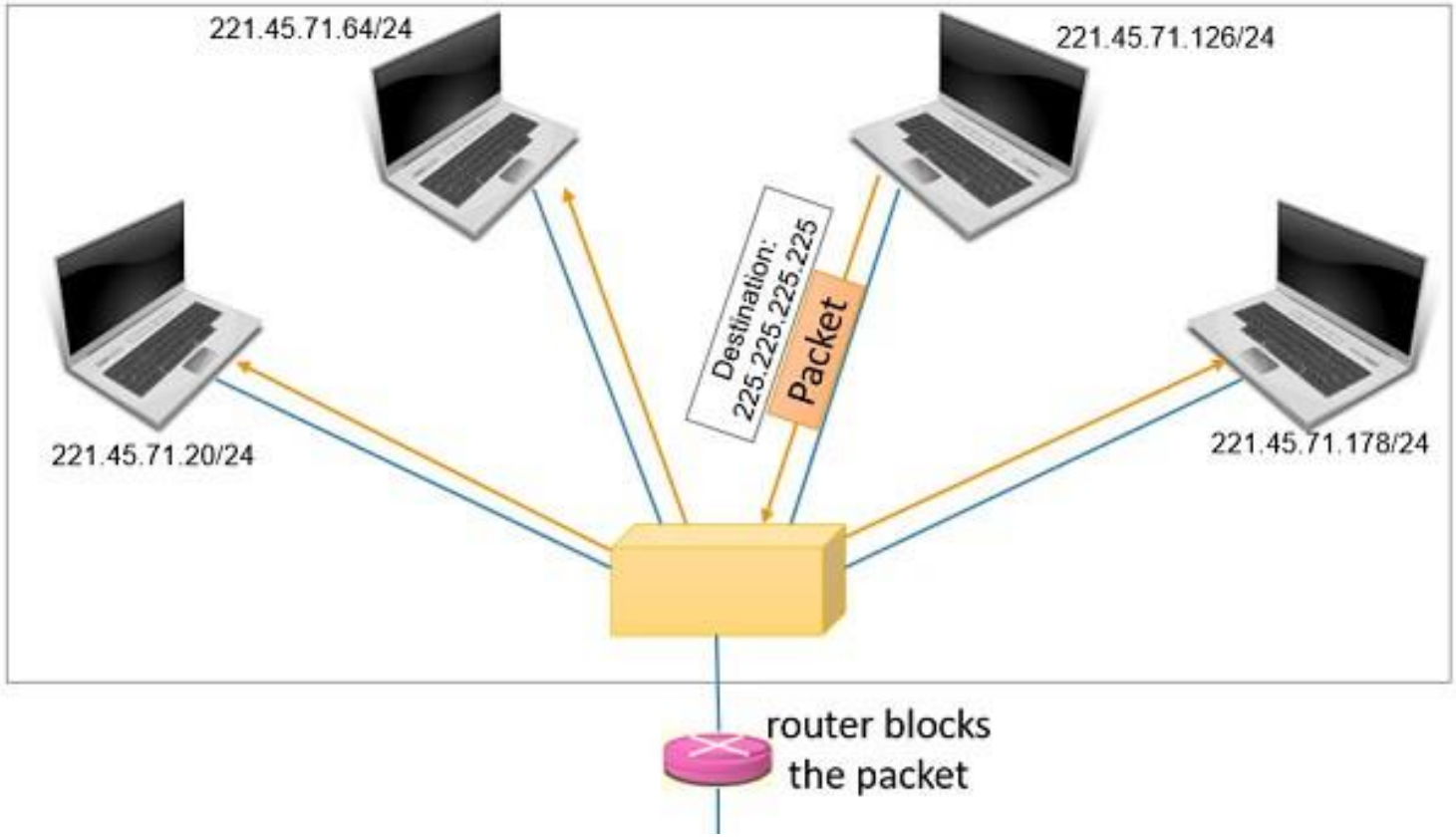
- his address is also called **Limited Broadcast Address** we will see the reason why it is a **limited** broadcast address.

- If a host wants to send the message to **every** other host in the current network, which means the host wants to **broadcast** a message in the **current network**. Then the host uses this address as the **destination address** in the IPv4 packet and sends it on the network.

Special IP addresses

- But, whenever the router finds the IPv4 packets with 225.225.225.225 as the destination address, it **restricts** the packet to be **broadcasted** in the **local network** only. Hence, it is called a limited broadcast address as it **limits** the packet to be broadcasted in the local network only.

Special IP addresses



Special IP addresses

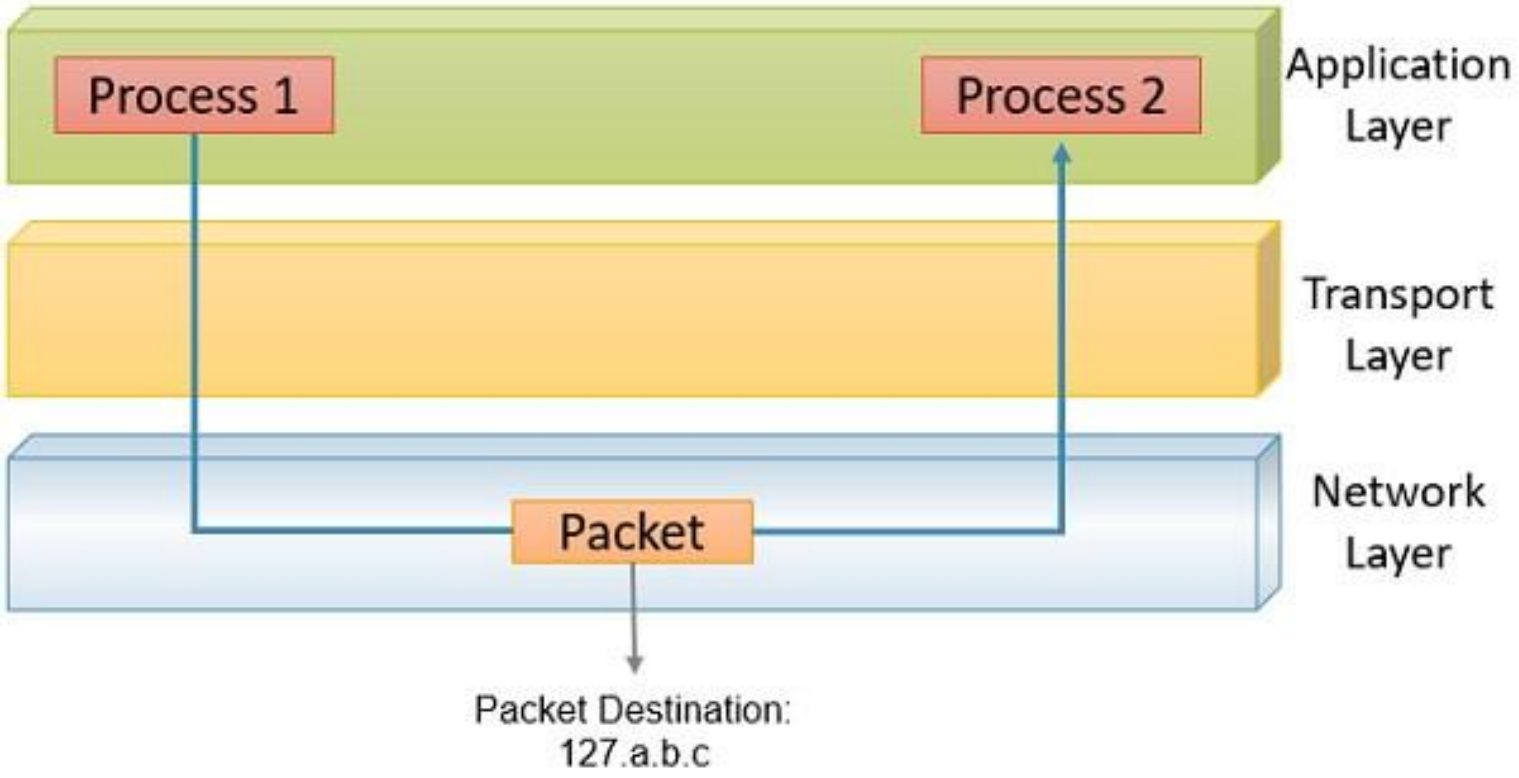
Loopback Addresses

- The special block **127.0.0.0/8** has addresses which are used as **loopback addresse**s. Now, the prefix length here is 8 so, the number of addresses can be calculated as $2^{32-8} = 2^{24}$ = **1,67,77,216**. This special block has 1,67,77,216 addresses. If we consider this address in classful addressing, then this block is the last block of class A.

- All the addresses starting with **127**. should be considered as loopback addresses. The **loopback address** can only be the **destination address** of a packet. The packet with loopback address **never leaves the machine** from which it is sent, it just **returns back** to the source.

- For example, it can be used to check whether the NIC is properly functioning or not. To check the network application on the system. Out of 1,67,77,216 loopback addresses only **127.0.0.1** is used rest 1,67,77,215 addresses are just total **wastage** of addresses.

Special IP addresses



Special IP addresses

Private Addresses

- As the name suggests the private IP addresses are never used globally. The packet with a private IP address is **not routed on the internet**. The private IP addresses are configured by the administrator of the network.

- Devices on the same network use private IP addresses to converse with each other. They do not require the internet for their communication. Like, the file servers, desktops and printers can communicate with each other without the requirement of internet.

- But, when they want to communicate with the device out of their network they translate a private IP address into the public IP address using **NAT**.

Special IP addresses

The range of private IP addresses is given below:

Block of Private IP addresses	Number of addresses in each block
10.0.0.0/8	16,777,216
172.16.0.0/12	1,047,584
192.168.0.0/16	65,536
169.254.0.0/16	65,536

Multicast Addresses

The block **224.0.0.0/4** has the multicast address. The length of the **prefix** is **4**. The number of addresses used for multicast communication is 2^{32-4} = 2^{28} = **26,84,35,456**.

The multicast address is assigned to the group of the host instead of one single host. The packet sent to the multicast address is delivered to all the host of that group.

Routing tables

- Routing tables in routers are critical components that guide the process of forwarding data packets from source to destination within a computer network. These tables contain information about the network topology and help routers make decisions about the best path for forwarding packets. Here are key aspects of routing tables:

1. **Routing Entry:**

    1. Each entry in the routing table corresponds to a specific destination network or host.
    2. It includes information such as the destination network or host address, the next-hop address (the address of the next router or the final destination), and the interface through which the packet should be forwarded.

Routing tables

2. Routing Protocols:

1. Routers use routing protocols to exchange information about the network with neighboring routers. Common routing protocols include RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol).
2. These protocols help routers dynamically update their routing tables based on changes in the network topology.

3. Static and Dynamic Routing:

1. Routing tables can be populated through static or dynamic routing. In static routing, administrators manually configure the routes. In dynamic routing, routers use routing protocols to exchange information and dynamically update their routing tables.

Routing tables

4. **Routing Metrics:**
    1. Routing tables include metrics or cost values associated with each route. These metrics help routers determine the most efficient path to reach a destination. Metrics can include factors like hop count, bandwidth, delay, and reliability.
5. **Longest Match Prefix:**
    1. When a router receives a packet, it looks for the longest match prefix in its routing table. This means it searches for the most specific entry that matches the destination address in the packet.
    2. The longest match ensures that the router selects the most specific route to the destination.
6. **Default Routes:**
    1. Routers may have a default route, also known as the gateway of last resort. If a router cannot find a match for the destination address in its routing table, it forwards the packet to the default route.

Routing tables

7. **Administrative Distance:**
    1. Each routing protocol or route source has an associated administrative distance, which represents the trustworthiness of the source. If multiple routes to the same destination exist, the router selects the one with the lowest administrative distance.
8. **Convergence:**
    1. Convergence refers to the process by which routers update their routing tables to reflect changes in the network. Dynamic routing protocols play a crucial role in ensuring that routers quickly converge to an updated and consistent view of the network.

- Understanding and properly configuring routing tables is essential for efficient and reliable network communication. It allows routers to make informed decisions about how to forward packets, leading to optimal network performance.

How routers work?

- Routers play a crucial role in computer networks by facilitating the exchange of data between devices in different networks. They operate at the network layer (Layer 3) of the OSI model and are responsible for forwarding data packets between networks. Here's an overview of how routers work:

1. **Packet Reception:**
    1. Routers receive data in the form of packets from devices within the local network or from other networks. Each packet contains information about its source, destination, and the actual data being transmitted.

2. **Network Layer Processing:**
    1. Routers operate at the network layer and use the network layer addresses (IP addresses) to make forwarding decisions. When a router receives a packet, it examines the destination IP address to determine where the packet should be sent.

How routers work?

3. **Routing Table Lookup:**
    1. The routing table is a key component of a router. It contains information about the available routes, including destination addresses, next-hop addresses, and associated metrics. The router performs a lookup in its routing table to find the best path to the destination.
4. **Forwarding Decision:**
    1. Based on the routing table lookup, the router makes a forwarding decision. It determines the next-hop router or the final destination for the packet and the outgoing interface through which the packet should be forwarded.
5. **Packet Forwarding:**
    1. The router forwards the packet to the next-hop router or the final destination using the appropriate interface. This involves encapsulating the packet in the data link layer frame for the outgoing interface (e.g., Ethernet frame for an Ethernet interface).

How routers work?

6. **Inter-Network Communication:**
    1. Routers enable communication between devices in different networks. They connect multiple network segments and facilitate the flow of data between these segments. This inter-network communication is essential for the functioning of the internet and other complex networks.
7. **Routing Protocols:**
    1. Routers use routing protocols to exchange information with neighboring routers. These protocols help routers discover network topology, learn about available routes, and update their routing tables dynamically. Common routing protocols include RIP, OSPF, BGP, and EIGRP.
8. **Network Address Translation (NAT):**
    1. Routers can perform Network Address Translation, which allows multiple devices within a local network to share a single public IP address for communication with devices outside the local network. NAT helps conserve public IP addresses.

How routers work?

9. **Firewall Functionality:**
    1. Many routers include firewall capabilities to enhance network security. Firewalls can filter and control the flow of traffic based on specified rules, protecting the internal network from unauthorized access.

10. **Error Handling and Diagnostics:**
    1. Routers monitor the health of network connections and can detect and handle errors. They may provide logging and diagnostic tools to help network administrators troubleshoot and resolve issues.

- In summary, routers play a pivotal role in directing data traffic between different networks. They use routing tables, routing protocols, and forwarding decisions to ensure that data packets reach their intended destinations efficiently and reliably. Routers are fundamental to the operation of the internet and various other computer networks.

Network Address Translation

- **Network Address Translation** (NAT) is a method of mapping the private IP address to the public IP address and vice versa. With this method, the local host in a private network can access the internet. NAT is always implemented at the routers. As they help the router to identify that to which localhost the message is to be forwarded.

Introduction

- The ISP provides a variable block of IPv4 addresses to the midsize organization. Now, what if the organization grows and requires a large block of addresses? Or the number of devices accessing the internet increase?

- It would be impossible for the ISP to fulfil the increased demand for addresses. Because the range of addresses before and after the allocated range may be assigned to other small organizations.

Network Address Translation

Now, the question arises how to fulfil this increased demand for addresses?

- Here, Network Address Translation (NAT) comes into the picture. With NAT midsize organizations can have several private IP addresses for a large set of computers. The private IP address allows internal communication. Whereas few devices/computers are provided with public addresses for global communication.

- Private IP addresses need to be unique inside the organization. No matter if they are not unique globally. As there are three blocks of addresses reserved for private networks.

- The users can use private IP addresses without the permission of Internet authorities. The private IP addresses are not routable. That means any router will not forward the packet having private IP addresses in its destination address field.

Network Address Translation

Address Translation

- Consider that the computer or a device with a private IP address. And this device wants to communicate (send data packet) with the outside world.
- So, this device will connect to the NAT capable router with the public IP address. Now here, the address translation will take place.
- In the address translation, the device's private IP address is mapped to the router's public IP address. And the data packet is forwarded to the (destination) outside world.
- NAT Definition
- Network Address Translation (NAT) is the address translation technique. It translates the private IP address to the public IP address and vice versa.
- Due to NAT, the computer in a private network is able to communicate with the computer in the public network.

Network Address Translation

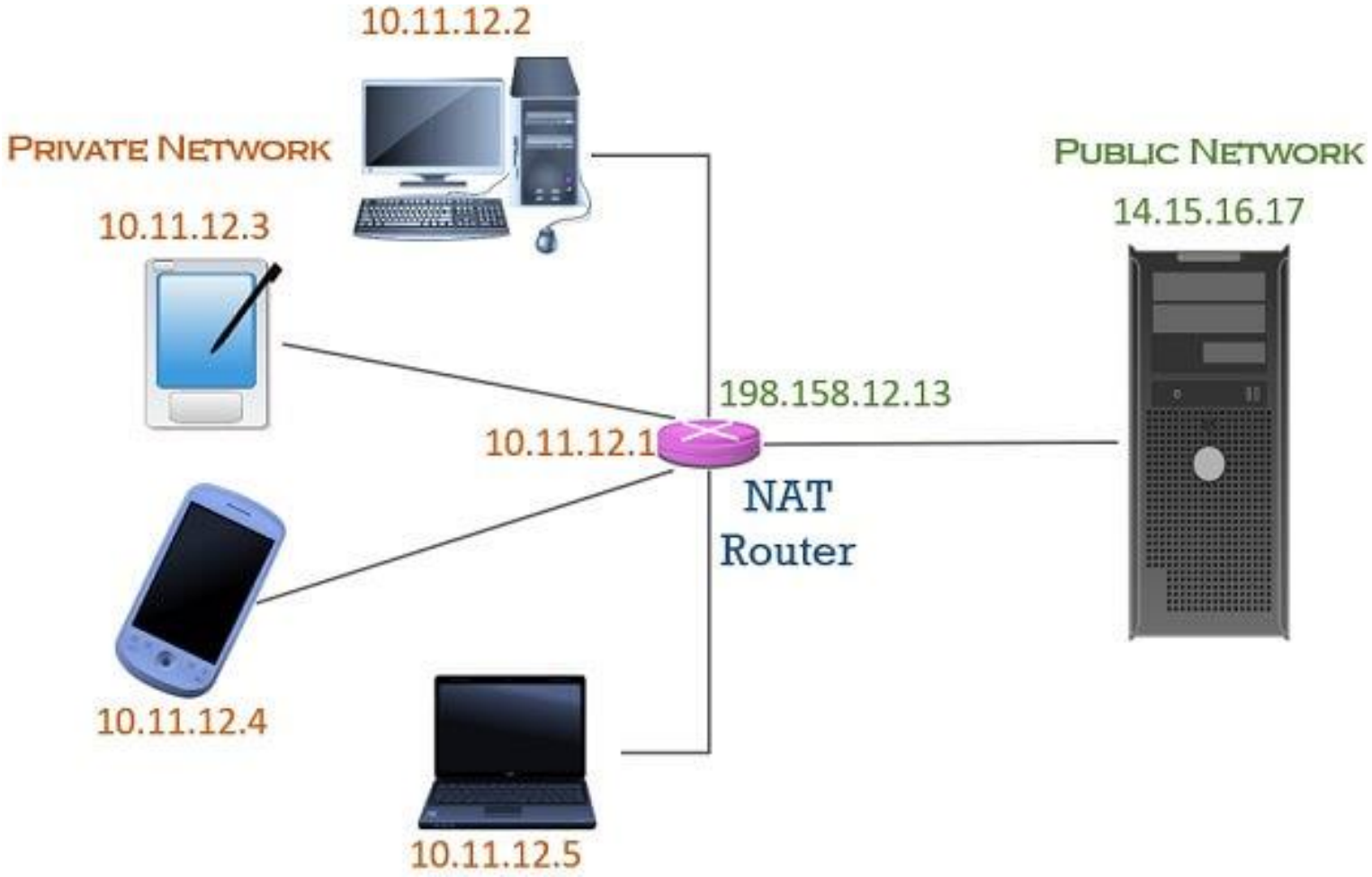
How Does Network Address Translation Work?

- The NAT is a process that translates the set of private IP addresses to the set of public IP addresses. It acts as a mediator between the global network i.e. internet and the local network or private network.
- Thus, the NAT router provides a single unique public IP address to a group of computers/devices present in the private network.

Network Address Translation Example

- Consider a small private network of a home having four devices. That is 1 laptop, 1 desktop, 1 tablet and one Smartphone, in its network. All these devices are the local host, and they are provided private IP addresses. These devices are connected to a **NAT router** with a **public IP address** 198.158.12.13.

Network Address Translation

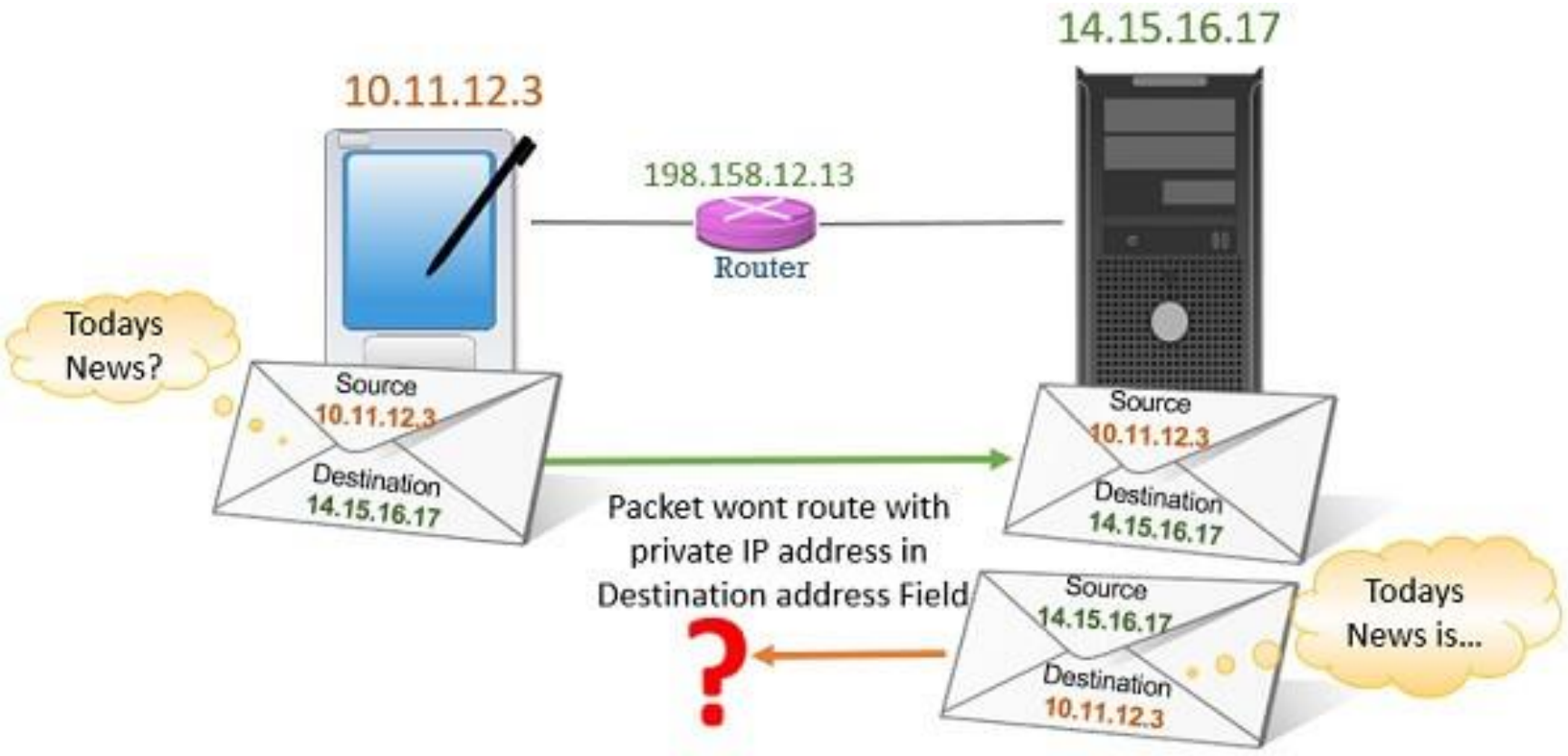


Network Address Translation

- Now suppose, if the tablet user at home network wants the information about today's news.
- As you can see in the image below:

1. The tablet sends a request to the server with a public IP address in the outside world.
2. The server would create a reply packet with the information of today's news.
3. The reply packet will have the source as server IP address (public IP address). And destination as tablets private IP address.
4. But we know the private IP address is not routable.
5. The Tablet would never receive the reply as no router will forward this packet to the table.

Network Address Translation



Network Address Translation

Solution

- The NAT router analyzes the request packet sent from a tablet.

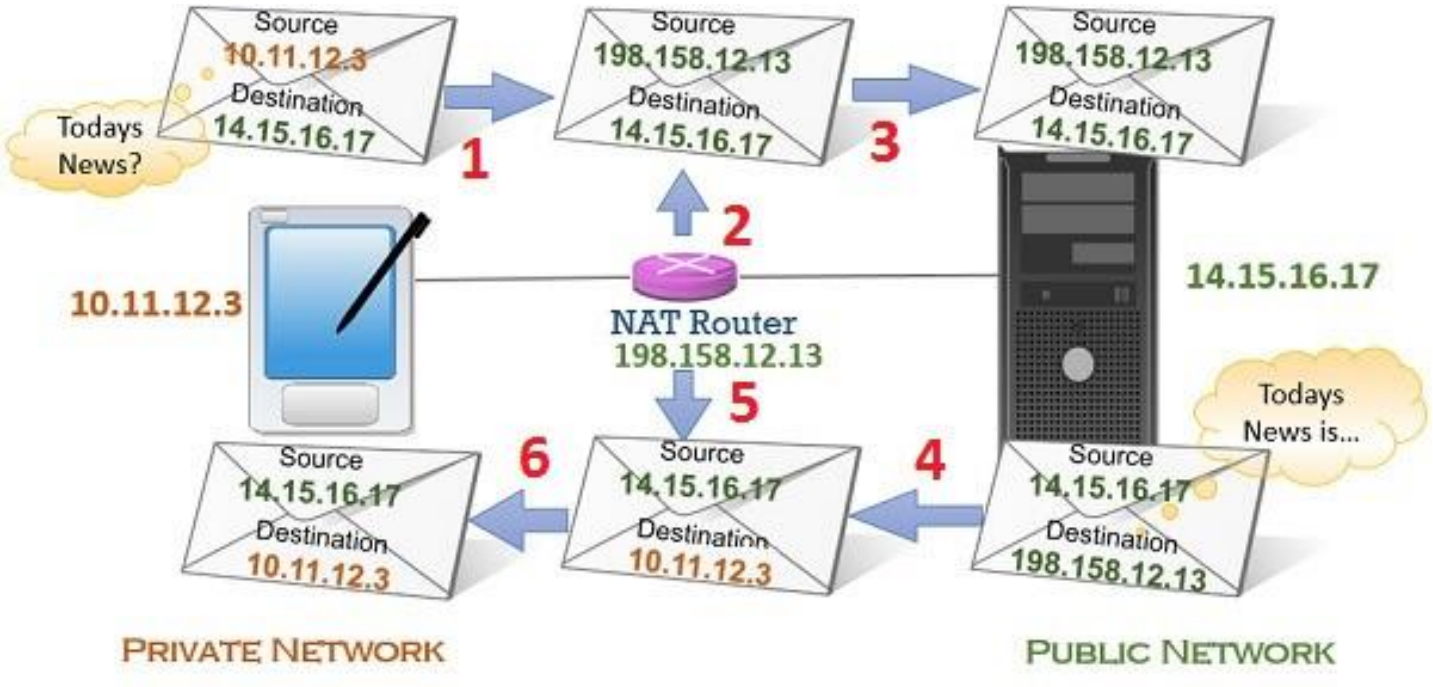
1. The request packet has the tablets private IP address in its source field. And servers public IP address in destination fields.
2. NAT router copies the source address in the private IP address column of the translation table. And the destination (server) address in the public IP address column.
3. NAT router then replaces the source private address with the NAT public IP address.
4. The destination server receives the request packet. It has NAT routers public IP address as the source address.
5. The server prepares the reply packet. It puts the NAT routers public IP address in the destination address field. And its own global IP address in the source address field of the reply packet.

Network Address Translation

6. Now, the reply packet has the public IP address in its destination address field. It would route the packet to the destination NAT router.

7. The NAT router analyzes the reply packet which has the source address as the server's address. The NAT router then remaps the servers public IP address to the tablet's private IP address. This is done with the help of a translation table using the source address field of the received packet. And send the reply packet to the corresponding private IP address.

Network Address Translation



Translation Table

Private IP Address	Public IP Address
10.11.12.3	14.15.16.17

This is how a local host in the private network, communicates with the devices with global addresses.

Dynamic routing

- Dynamic routing is a network routing method where routers can automatically discover and exchange information about the network topology with each other.

- This dynamic exchange allows routers to adapt to changes in the network, such as link failures or the addition of new paths. Dynamic routing protocols are responsible for this automatic exchange of routing information.

EIGRP

- EIGRP, or Enhanced Interior Gateway Routing Protocol, is an advanced and proprietary routing protocol developed by Cisco Systems.

- It is designed for use within large enterprise networks and provides features that enhance routing efficiency and scalability. Here are key characteristics and features of EIGRP:

1. **Hybrid Protocol:**
    1. EIGRP is often classified as a hybrid routing protocol because it combines elements of both distance vector and link-state protocols. It incorporates some features of traditional distance vector protocols like RIP while also including link-state characteristics for efficient route calculation.

EIGRP

2. **Advanced Metric Calculation:**
    1. EIGRP uses a composite metric known as the "composite cost" or "metric" to determine the best path to a destination. The metric includes factors such as bandwidth, delay, reliability, and load. The default metric is calculated based on these factors, but administrators can customize the metric calculation.
3. **Fast Convergence:**
    1. EIGRP is known for its fast convergence capabilities. It reacts quickly to network changes by sending updates only for the affected routes, reducing the convergence time compared to traditional distance vector protocols.
4. **Diffusing Update Algorithm (DUAL):**
    1. DUAL is the algorithm used by EIGRP for loop prevention and fast convergence. It allows routers to maintain multiple routes to a destination and quickly switch to an alternate path in case of a link failure, without causing routing loops.

EIGRP

5. **Neighbor Discovery and Maintenance:**
    1. EIGRP routers establish and maintain neighbor relationships using a reliable transport protocol (usually RTP - Reliable Transport Protocol). The neighbors exchange routing information and keep each other informed of changes in the network.

6. **VLSM and CIDR Support:**
    1. EIGRP supports Variable Length Subnet Masking (VLSM) and Classless Inter-Domain Routing (CIDR), allowing for efficient use of IP address space and more flexible addressing.

7. **Partial Updates:**
    1. EIGRP sends partial updates, which include only the information about the changed routes, reducing the amount of bandwidth consumed by routing updates.

EIGRP

8. **Route Summarization:**
    1. EIGRP supports route summarization, which allows for the aggregation of multiple routes into a single summary route. This helps in reducing the size of routing tables and improving network efficiency.
9. **Authentication:**
    1. EIGRP supports various methods of authentication, such as MD5 authentication, to secure routing updates exchanged between routers.
10. **Compatibility with IPv4 and IPv6:**
    1. EIGRP has been extended to support both IPv4 and IPv6, making it versatile and capable of handling networks transitioning to IPv6.
11. **Administrative Distance:**
    1. EIGRP has an administrative distance of 90 by default, which is lower than most other routing protocols. This means that EIGRP routes are considered more trustworthy by routers when compared to routes from other protocols with higher administrative distances.

EIGRP

- EIGRP is commonly used in Cisco-centric environments and provides a range of features that make it suitable for complex and scalable enterprise networks.

- However, it's important to note that being a proprietary protocol, its interoperability with non-Cisco devices may be limited.

OSPF

- OSPF, or Open Shortest Path First, is a link-state routing protocol used to determine the best path for routing data within an Internet Protocol (IP) network.

- OSPF is an open standard protocol, meaning it is not proprietary and is widely supported by various networking equipment from different vendors. Here are key characteristics and features of OSPF:

1. **Link-State Protocol:**

    1. OSPF is a link-state routing protocol, which means that routers in the network have a detailed and synchronized view of the entire network topology. Each router maintains a Link-State Database (LSDB) containing information about the state of each link in the network.

OSPF

2. **Hierarchical Design:**
    1. OSPF uses a hierarchical design with different types of OSPF routers, including Area Border Routers (ABRs) and Autonomous System Boundary Routers (ASBRs). This hierarchical structure enhances scalability and reduces the amount of routing information that routers need to process.
3. **Cost-Based Metric:**
    1. OSPF uses a metric based on the cost of traversing a link. The cost is calculated based on the bandwidth of the link, and routers choose paths with lower total costs when determining the best route to a destination.
4. **Fast Convergence:**
    1. OSPF provides fast convergence in response to changes in the network. When a topology change occurs, OSPF routers quickly update their LSDBs and recalculate the routing table, minimizing the time it takes for the network to adapt to changes.

OSPF

5. **DR/BDR Election:**
    1. In multi-access networks, OSPF elects a Designated Router (DR) and a Backup Designated Router (BDR) to reduce the number of adjacencies and the amount of routing information exchanged. This helps improve scalability in broadcast and non-broadcast multi-access networks.

6. **Type of Service (TOS) Support:**
    1. OSPF supports Quality of Service (QoS) through its use of Type of Service (TOS) metrics. This allows administrators to prioritize certain types of traffic over others.

7. **VLSM and CIDR Support:**
    1. OSPF supports Variable Length Subnet Masking (VLSM) and Classless Inter-Domain Routing (CIDR), allowing for efficient use of IP address space and more flexible addressing.

OSPF

8. **Authentication:**
    1. OSPF supports various authentication mechanisms, including simple password-based authentication and more secure methods such as MD5 authentication.
9. **Route Summarization:**
    1. OSPF allows for route summarization, which reduces the size of routing tables by aggregating routes into summary addresses.
10. **Scalability:**
    1. OSPF is designed to be scalable, making it suitable for large and complex networks. The hierarchical structure and the ability to partition the network into areas contribute to its scalability.
11. **IPv6 Support:**
    1. OSPFv3, an extension of OSPF, is specifically designed to support IPv6 networks. It provides the same link-state routing functionality for IPv6 as OSPF does for IPv4.

OSPF

12. **Administrative Distance:**
    1. OSPF has an administrative distance of 110 by default, which is lower than many other routing protocols. This means that OSPF routes are considered more trustworthy by routers when compared to routes from protocols with higher administrative distances.

- OSPF is widely used in enterprise networks, Internet Service Provider (ISP) networks, and various other environments due to its efficiency, scalability, and open standards nature. It is part of the Internet Protocol suite and is documented in several Request for Comments (RFC) publications.

Basic router configuration

- Configuring a router involves setting up various parameters to enable communication between devices within a network. Below are some basic router configurations that you might encounter when setting up a router.

- Keep in mind that specific commands and procedures may vary depending on the router model and the operating system it uses (e.g., Cisco IOS).

Accessing the Router:

- Connect to the router using a console cable or via a network connection (SSH, Telnet, or web-based management interface).

- This typically requires a username and password.

Basic router configuration

Entering Configuration Mode:

- Once connected, enter privileged EXEC mode, commonly denoted by the router prompt ending with **#**. Use the following command:
- router>enable
- **Entering Global Configuration Mode:**
- Enter global configuration mode to make changes to the router's global settings.
- The prompt changes to **(config)#**. Use the following command:
- router#configure terminal

Basic router configuration

- **Setting the Hostname:**
- Assign a name to the router to help identify it on the network. In global configuration mode, use:
- hostname YourRouterName
- **Configuring Interfaces:**
- Define IP addresses on router interfaces. The syntax may vary, but for a Cisco router, use:
- #interface <interface_type> <interface_number> ip address <ip_address> <subnet_mask>
- no shutdown

Basic router configuration

Configuring Routing:

- Set up static routes or dynamic routing protocols like RIP, OSPF, or EIGRP. For a static route:
- ip route <destination_network> <subnet_mask> <next_hop_ip>

Enabling Routing:

- If you are using a dynamic routing protocol, enable it on the router. For example, for OSPF:
- router ospf <process_id> network <network_id> <wildcard_mask> area <area_id>

Basic router configuration

Password Security:

- Implement password security for console access, Telnet, or SSH. For example:
- line console 0 password YourConsolePassword login

Enabling SSH:

- If not done by default, enable SSH for secure remote access:
- ip domain-name YourDomainName crypto key generate rsa username YourUsername privilege 15 secret YourSSHPassword line vty 0 4 transport input ssh login local

Saving Configuration:

- Save the configuration to the router's non-volatile memory so that it persists across reboots:
- write memory

Basic router configuration

Checking Configuration:

- Verify your configuration settings using show commands. For example:
  - show running-config
  - show ip interface brief
  - show ip route

Logging and Monitoring:

- Configure logging to record events and monitor the router's performance:
- logging buffered <buffer_size>

- These commands provide a basic foundation for configuring a router. Depending on the router's role and the specific requirements of the network, additional configurations, such as access control lists (ACLs), Quality of Service (QoS), and security settings, may also be necessary.

NetFlow

- NetFlow is a network protocol developed by Cisco that allows network administrators to collect and analyze information about network traffic. It provides a detailed view of network activity, helping in network monitoring, traffic analysis, and capacity planning. NetFlow is commonly used in routers and switches to export data about flows, which are sequences of packets with common characteristics.

Here are key aspects of NetFlow:

- **Flow Data:**

  NetFlow collects information about flows, which are unidirectional sequences of packets sharing common attributes such as source and destination IP addresses, source and destination ports, protocol, and class of service.

NetFlow

- **Flow Monitoring:**

  NetFlow enables the monitoring of network traffic by collecting data about the flows traversing a network device. This data includes details about the volume of data, the number of packets, and other characteristics of each flow.

- **Flow Export:**

  NetFlow-enabled devices export flow data to a NetFlow collector or analyzer. The collector aggregates and analyzes the data to provide insights into network usage patterns, application usage, and potential security issues.

NetFlow

- **Components:**

  NetFlow involves three main components: the exporter, the flow cache, and the collector.

  - **Exporter:** The device (router, switch, or other network device) that generates and exports NetFlow records.
  - **Flow Cache:** A temporary storage area on the exporting device that stores information about active flows before exporting them to the collector.
  - **Collector:** A system that receives, aggregates, and analyzes NetFlow records.

- **NetFlow Versions:**

  There are different versions of NetFlow, such as NetFlow version 5, NetFlow version 9 (also known as Flexible NetFlow), and IPFIX (IP Flow Information Export), which is an IETF standard based on NetFlow version 9. Each version has improvements and additional features.

NetFlow

- **Use Cases:**

  NetFlow is used for various purposes, including:

  - **Network Monitoring:** Providing insights into traffic patterns, top talkers, and bandwidth usage.
  - **Security Analysis:** Detecting and analyzing anomalies, identifying potential security threats and attacks.
  - **Capacity Planning:** Understanding application and user behavior to optimize network resources.
  - **Troubleshooting:** Diagnosing performance issues and network anomalies.

- **NetFlow Collectors and Analyzers:**

  NetFlow collectors and analyzers are third-party or vendor-specific tools designed to receive and process NetFlow data. They present the collected information in a meaningful way, providing reports, graphs, and dashboards for network administrators.

NetFlow

- **Security Considerations:**

  While NetFlow is a valuable tool for monitoring and analyzing network traffic, it's important to consider security implications. Ensure that NetFlow data is securely transmitted to the collector and that sensitive information is protected.

- NetFlow is widely used in enterprise networks, data centers, and service provider environments to gain insights into network behavior, optimize performance, and enhance security. Its flexibility and extensibility make it a valuable tool for network administrators and security professionals.

Tools for troubleshooting IP problems

- Troubleshooting IP (Internet Protocol) problems can involve various issues related to network connectivity, configuration, and communication.

- Several tools are commonly used for diagnosing and resolving IP-related issues. Here are some essential tools for troubleshooting IP problems:

1.Ping:

- **Purpose:** Verifying connectivity and measuring round-trip time.
- **Usage: ping <IP address or hostname>**
- The **ping** command sends ICMP Echo Request messages to the target host and waits for Echo Reply messages. It's a basic tool to check if a host is reachable.

Tools for troubleshooting IP problems

2.Traceroute (or Tracepath):

- **Purpose:** Identifying the route and measuring transit delays to a destination.
- **Usage: traceroute <IP address or hostname>**
- Traceroute shows the path that packets take to reach the destination, along with the time taken at each hop. This helps pinpoint where network issues might be occurring.

3.Nslookup/Dig:

- **Purpose:** Querying DNS (Domain Name System) information.
- **Usage: nslookup <hostname>** or **dig <hostname>**
- These tools help resolve domain names to IP addresses and provide additional DNS-related information.

4.Ipconfig/ifconfig:

- **Purpose:** Displaying and managing IP configuration on a local machine.
- **Usage: ipconfig** (Windows) or **ifconfig** (Unix/Linux)
- These commands show the IP configuration of network interfaces, including IP addresses, subnet masks, and gateway information.

Tools for troubleshooting IP problems

5.Netstat:

- **Purpose:** Displaying network connections, routing tables, interface statistics, masquerade connections, and more.
- **Usage: netstat -an** (Windows) or **netstat -nr** (Unix/Linux)
- Netstat provides information about active network connections and listening ports, helping identify network-related issues.

6.Wireshark:

- **Purpose:** Capturing and analyzing network traffic.
- **Usage:** Install Wireshark and use it to capture packets on a network interface.
- Wireshark allows detailed inspection of network packets, helping to identify issues such as packet loss, incorrect routing, or protocol errors.

7.Telnet:

- **Purpose:** Testing connectivity to a specific port on a remote host.
- **Usage: telnet <IP address or hostname> <port>**
- Telnet is useful for checking if a specific port is reachable on a remote server, helping identify firewall or connectivity issues.

Tools for troubleshooting IP problems

8.Nmap:

- **Purpose:** Scanning and discovering open ports on a remote host.
- **Usage: nmap <IP address>**
- Nmap can provide information about open ports and services on a target system, assisting in troubleshooting network connectivity.

9.Iperf:

- **Purpose:** Measuring network performance by testing bandwidth.
- **Usage:** Install Iperf on two systems and use it to measure the network performance between them.
- Iperf helps identify issues related to network bandwidth and latency.

10.Route:

- **Purpose:** Displaying or modifying the local IP routing table.
- **Usage: route print** (Windows) or **route -n** (Unix/Linux)
- The **route** command shows the local routing table, allowing you to verify the configured routes.

Tools for troubleshooting IP problems

- These tools collectively provide a comprehensive set of capabilities for diagnosing and troubleshooting various IP-related issues in a network. Depending on the specific problem you are facing, one or more of these tools may be instrumental in identifying and resolving the issue.

Q & A

E.R. Ramesh, M.C.A., M.Sc., M.B.A.,
98410 59353, 98403 50547
rameshvani@gmail.com