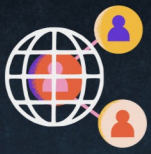


Networking Short notes

FOR DEVOPS ENGINEERS

TRAIN WITH SHUBHAM

Networking Short Notes

Basics of Networking

Networking plays a crucial role in the world of DevOps, where the focus is on automating software development, testing, and deployment processes. As a DevOps engineer, having a strong understanding of networking is essential for several reasons:

- Infrastructure Design: One of the core responsibilities of a DevOps engineer is to design and implement infrastructure that supports software development and deployment. This includes setting up networks, configuring routers and firewalls, and ensuring that servers and other devices are properly connected. Understanding networking protocols and infrastructure design principles is essential for designing an efficient and scalable infrastructure.
- Application Deployment: DevOps engineers are responsible for deploying applications to production environments. This involves setting up and configuring servers, load balancers, and other network components to ensure that the application runs smoothly and reliably. Understanding networking principles is essential for configuring network components and resolving network-related issues that may arise during application deployment.
- Automation: DevOps is all about automating processes to improve efficiency and reduce errors. Networking automation tools, such as Ansible and Puppet, are used to automate the configuration of network devices and ensure that they are properly configured and maintained. A good understanding of networking protocols and automation tools is essential for automating network-related tasks.

- Monitoring: DevOps engineers are responsible for monitoring and maintaining the infrastructure and applications they manage. This includes monitoring network traffic, identifying bottlenecks and performance issues, and troubleshooting network-related problems. Understanding networking protocols and tools is essential for identifying and resolving network issues in a timely manner.

The OSI Model

The OSI model is a conceptual framework for understanding how data is transmitted across a network, and it consists of seven layers: physical, data link, network, transport, session, presentation, and application.

Functions of Layers

Physical Layer :

- Physical characteristics of interfaces and media
- Representation of bits.
- Data rate
- Synchronization of bits
- Line configuration (point-to-point or multi-point)
- Transmission Mode
- Physical Topology

Data Link Layer :

- Framing
- Physical addressing
- Error control
- Flow control
- Access control

Network Layer :

- Routing
- Congestion control
- Billing

Transport Layer :

- Service Point addressing
- Segmentation and reassembly
- Flow control
- Error control

Functions of Layers

Session Layer :

- Dialog control
- Synchronization

Presentation Layer :

- Data encoding
- Encryption
- Compression

Application Layer :

- File Transfer
- Mail services
- Directory services

TCP/IP Reference Model

TCP/IP stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols used to interconnect network devices on the internet.

TCP/IP is also used as a communications protocol in a private computer network (an intranet or extranet).

The IP Protocol

At the network layer, the Internet can be viewed as a collection of subnet-works or Autonomous systems that are connected together. The network layer protocol that used for Internet is Internet Protocol (IP).

Its job is to provide a best-efforts way to transport datagrams from source to destination, without regard to whether or not these machines are on the same network or not these are other networks in between them. Communication in the Internet works as follows.

Each datagram is transmitted, after getting from Transport layer, through the Internet, possibly being fragmented into smaller units as it goes. When all pieces finally get to the destination machine, they are reassembled by the network layer into the original datagram.

Note:

Datagram
Packets in IP layer are called Datagrams. A Datagram is a variable length packet(upto 65,536 bytes) consisting of two parts : Header and Data. The header can be from 20 to 60 bytes and contains information essential to routing and delivery.

Version
The first field defines the version number of the IP. The current version is 4(IPv4),with binary value 0100.

Header length
(HLEN) The HLEN field defines the length of the header in multiples of four bytes .The four bits can represent a number between 0 to 15,which,when multiplied by 4,gives a maximum of 60 bytes.

Service Type.
The service type field defines how datagram should be handled. It includes bits that define the priority of the datagram. It also contains bits that specify the type of service the sender desires such as the level of throughput, reliability, and delay.

Total Length
The total length field defines the total length of the IP datagram. It is a two-byte field (16 bits) and can define up to 65,535 bytes.

Identification
The identification field is used in fragmentation. A datagram, when passing through different networks, may be divided into fragments to match the network frame size. When this happens, each fragment is identified with a sequence number in this field.

Flags
The bits in the flags field deal with fragmentation (the datagram can or can not be fragmented; can be first, middle, or last fragment; etc.).

Fragmentation offset
The fragmentation offset is a pointer that shows the offset of the data in the original datagram (if it is fragmented).

Protocol
The protocol field defines which upper-layer protocol data are encapsulated in datagram (TCP, UDP, ICMP etc.).

Time to live

The time to live field defines the number of hops a datagram can travel before it is discarded. The source host, when it creates the datagram, sets this field to an initial value. Then, as the datagram travels through the Internet, router by router, each router decrements this value by 1. If this value becomes 0 before the datagram reaches its final destination, the datagram is discarded. This prevents a datagram from going back and forth forever between routers.

Header Checksum

This is a 16-bit field used to check the integrity of the header, not the rest of the packet.

Source address

The source address field is a four-byte (32-bit) Internet address. It identifies the original source of the datagram.

Destination address

The destination address field is a four-byte (32-bit) Internet address. It identifies the final destination of the datagram.

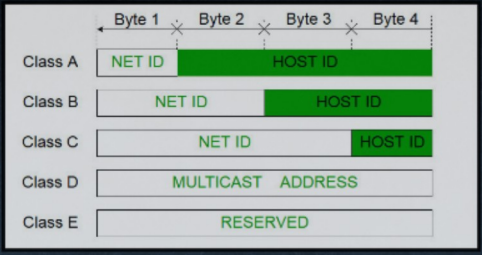
Options

The options field gives more functionality to IP datagram. It can carry fields that control routing, timing, management, and alignment.

ADDRESSING

In addition to the physical address the internet requires an additional addressing convention : an address that identifies the connection of a host to its network. Each Internet address consists of 4 bytes defining three fields : class type,netid,and hosted. These parts are varying lengths depending on the class of the address

CLASSES



There are currently five different classes:
They are Class A, Class B, Class C, Class D, Class E

Class A : This can accommodate more hosts since 3 bytes are reserved for HOSTID. Class A will begin with 0 .

Class B : This will start with 10 and Host id will have 2 bytes length.

Class C : This will start with 110 and Hostid will have 1 byte length.

Class D: This will start with 1110 . This is reserved for Multicast addresses.

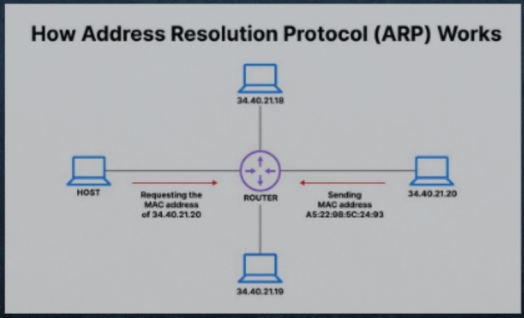
Class E : This is reserved for feature use and will start with 1111 .

Protocols

Address resolution protocol (ARP)

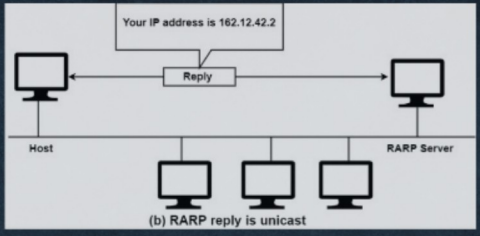
The address resolution Protocol associates an ip address with physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address usually imprinted on the network interface card.(NIC)

Anytime a host or a router needs to find the physical address of another host on its network, it formats an ARP query packet that includes the IP address and broadcast it over the network. Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes its internet address and sends back its physical address. The host both to its cache memory and to the datagram header, then sends the datagram on its way.



Reverse Address resolution protocol(RARP)

The RARP allows a host to discover its internet address when it knows only its physical address. The question here is ,why do we need RARP? A host is supposed to have its internet address stored on its hard disk ! RARP works much like ARP. The host wishing to retrieve its internet address broadcasts an RARP query packet that contains its physical address to every host on its physical network. A server on the network recognizes the RARP packet and returns the host's internet address.



(b) RARP reply is unicast

Internet Control Message Protocol (ICMP)

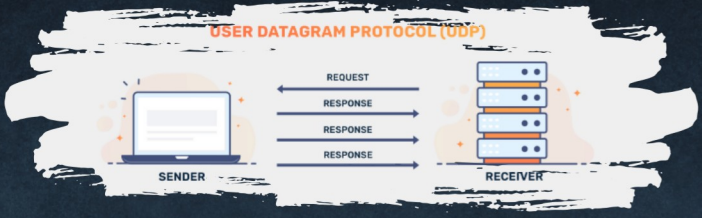
The Internet control message protocol is a mechanism used by hosts and routers to send notification of datagram problems back to the sender. IP is an unreliable and connectionless protocol.

ICMP allows IP to inform a sender if a datagram is undeliverable. A datagram travels from router to router until it reaches one that can deliver it to its final destination.

If a router is unable to route or deliver the datagram because of unusual conditions or due to congestion, ICMP allows it to inform the original source.

ICMP uses echo test/reply to test whether a destination is reachable and responding. It also handles both control and error message, but its sole function is ti\o report problems, not correction them. A datagram carries only source and destination address. For this reason ICMP can send message only to the source, not to an intermediate router.

User Datagram Protocol (UDP)



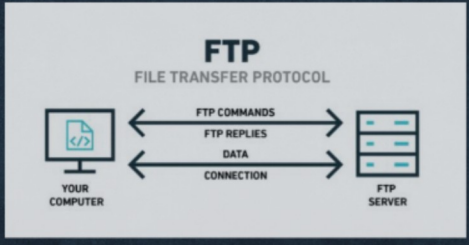
The user datagram protocol (UDP) is the simpler of the two standard TCP/IP transport protocols.
It is an end-to-end transport level protocol that adds only port addresses, check sum error control, and length information to the data from the upper layer. The packet produced by the UDP is called a user datagram .

- Source port address. The source port address is the address of the application program that has created the message.
- Destination port address. The destination port address is the address of the application program that will receive the message.
- Total length. The total length field defines the total length of the user datagram in bytes.
- Check sum. The check sum is a 16-bit field used in error detection.

FTP (File Transfer Protocol)

FTP (File Transfer Protocol) is a network protocol for transmitting files between computers over Transmission Control Protocol/Internet Protocol (TCP/IP) connections. Within the TCP/IP suite, FTP is considered an application layer protocol.

In an FTP transaction, the end user's computer is typically called the local host. The second computer involved in FTP is a remote host, which is usually a server. Both computers need to be connected via a network and configured properly to transfer files via FTP. Servers must be set up to run FTP services, and the client must have FTP software installed to access these services.



FTP is a standard network protocol that can enable expansive file transfer capabilities across IP networks. Without FTP, file and data transfer can be managed with other mechanisms -- such as email or an HTTP web service -- but those other options lack the clarity of focus, precision and control that FTP enables.

Networking Topologies

Two main types of network topologies in computer networks are
1) Physical topology
2) Logical topology

The physical arrangement of the computer wires and other network components makes up this form of network.

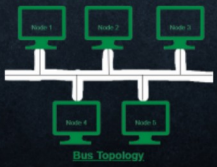
Logical topology: Logical topology provides information on the physical architecture of a network.

There are various Physical Topologies, including:

- Bus Topology
- Ring Topology
- Star Topology
- Tree Topology
- Mesh Topology
- Hybrid Topology

Bus Topology

A single cable links all of the included components in a bus topology. The primary wire serves as the network's spine. The computer server is one of the computers in the network. A linear bus design is one that has two ends.

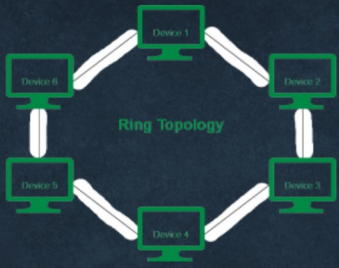


Bus Topology

Ring Topology

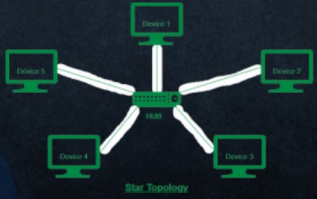
Every device in a ring network has precisely two neighbouring devices for transmission purposes. It is known as a ring topology because its creation resembles a band. Every machine in this structure is linked to another. The last component is merged with the first one in this case.

To transmit information from one machine to another, this topology employs tokens. In this topology, all messages travel in the same direction through a ring.



Star Topology

All machines in the star architecture are linked together by a hub. This connection is referred to as a centre node, and it connects all other nodes. It is most commonly used on LAN networks because it is cheap and simple to set up.



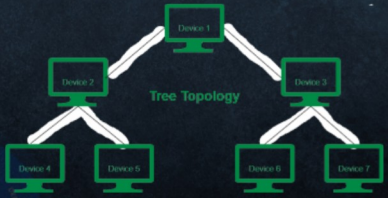
Mesh Topology

The mesh architecture has a distinct network design in which every computer on the network communicates with every other computer. It establishes a P2P (point-to-point) link between all network devices. It provides a high degree of redundancy, so even if one network cable breaks, data can still reach its target via an alternate route.

Mesh Topology

Tree Topology

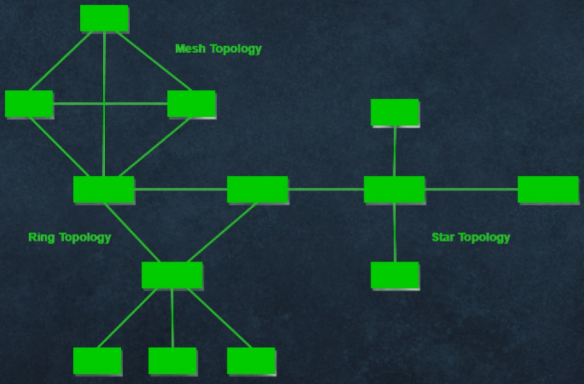
Tree structures have a base node that connects all other nodes to create a hierarchy. As a result, it is also referred to as hierarchy geometry. This topology is known as a Star Bus topology because it combines several star topologies into a single bus. Tree topology is a popular network topology that is comparable to bus and star topologies.



Hybrid Topology

A hybrid topology is one that incorporates two or more networks. As you can see in the above design, the resulting network does not follow any of the conventional topologies.

For example, as shown in the above image, Star and P2P topology are used in a workplace in one section. When two distinct fundamental network topologies are linked, a hybrid topology is always formed.



CIDR Notation

Classless inter-domain routing (CIDR) is a collection of Internet Protocol (IP) protocols used to generate unique IDs for networks and individual devices. IP identifiers enable specific information packets to be sent to specific machines. Technicians found it challenging to monitor and identify IP addresses shortly after the introduction of CIDR, so a notation system was created to make the process more efficient and standardised.

The capacity to group blocks of addresses into a singular routing network is a distinguishing feature of CIDR, and the prefix standard used to understand IP numbers enables this. The first portion of the bit sequence that forms the binary encoding of an IP address is shared by CIDR blocks, and blocks are marked using the same decimal-dot CIDR notation scheme that is used for IPv4 addresses.

For example, 10.10.1.16/32 is a 32-bit address prefix, which is the maximum amount of bits permitted in IPv4. Addresses with the same prefix and amount of bits always pertain to the same block. Furthermore, the length of the prefix distinguishes bigger groups from smaller blocks. Short prefixes enable more addresses, whereas long suffixes designate tiny chunks.

The updated IPv6 protocol also uses CIDR notation, and the grammar is the same. The only change is that IPv6 names can be up to 128 bits long, as opposed to the 32-bit limit of IPv4. Despite the fact that IPv6 names can be up to 128 bits long, subnets on MAC layer networks always use 64-bit host IDs.

CIDR Conversion Table

IPv4 CIDR IP/CIDR	to last IP address	Mask	Hosts (*)	Class
a.b.c.d/32	+0.0.0.0	255.255.255.255	1	1/256 C
a.b.c.d/31	+0.0.0.1	255.255.255.254	2	1/258 C
a.b.c.d/30	+0.0.0.3	255.255.255.252	4	1/64 C
a.b.c.d/29	+0.0.0.7	255.255.255.248	8	1/32 C
a.b.c.d/28	+0.0.0.15	255.255.255.240	16	1/16 C

How CIDR makes subnetting easier

By designating a portion of the host identifier, a specific subnet mask is formed, and bigger subnets are produced by moving more bits from the host identity to the subnet mask. A network's ultimate subnet is marked in binary with all ones. The ultimate subnet is 255.255.255.255 when written in CIDR dot-decimal format.

Prior to CIDR, subnet masks with all zeros (255.255.255.0) and subnet masks with all ones (255.255.255.255) could not be used because they could be mistaken with network IDs, but CIDR-compliant equipment distinguishes between the two using CIDR notation's prefixes and suffixes.

MAC Address

1. The MAC address is the physical address that individually recognises each device on a network. To interact between two networked devices, we need two addresses: an IP address and a MAC identifier. It is given to each NIC (Network Interface Card) capable of connecting to the internet.

2. Media Access Control is an abbreviation for Media Access Control. It is also known as Physical Address, Hardware Address, or BIA. (Burned In Address).

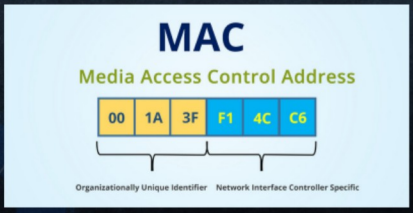
3. It has a worldwide unique MAC address, which means that no two machines with the same MAC address can coexist. It is displayed in hexadecimal notation on each gadget.

4. It has 12 numbers and 48 bits, with the first 24 bits used for the OUI (Organization Unique Identifier) and the remaining 24 bits used for NIC/vendor-specific information.

5. It works at the data link layer of the OSI architecture.

6. It is provided by the device's manufacturer and is embedded in the device's NIC, which should not be altered.

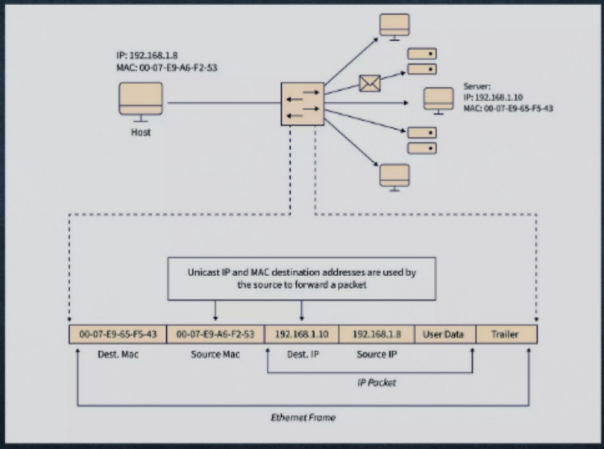
7. The ARP algorithm is used to link a logical identity with a physical or MAC address.



Types of MAC Address

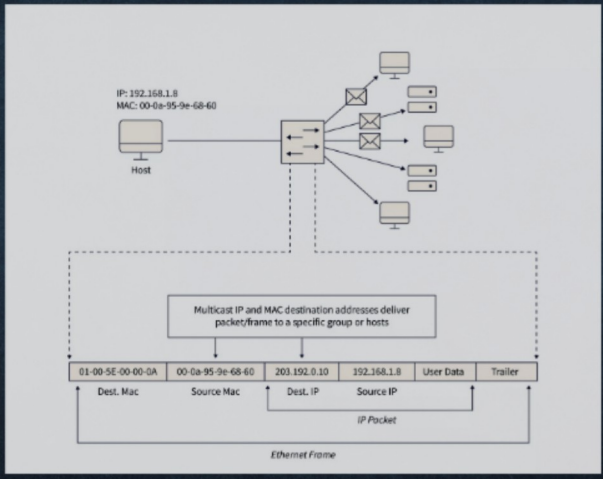
Unicast MAC Address

The Unicast MAC address of a network NIC identifies it. A Unicast addressed packet is only received by the interface going to a specific NIC. If the LSB (least significant bit) of the first octet of an address is set to zero, the message is only meant to reach one recipient NIC. The MAC address of the originating computer is always unicast.



Multicast MAC Address

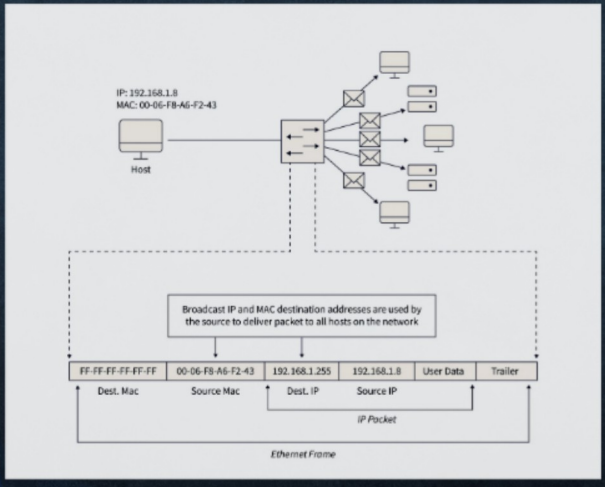
Using multicast addresses, the source device can transmit a data packet to a large number of other devices or NICs. In a Layer-2 (Ethernet) Multicast address, the first three characters of the first octet, or the LSB (least significant bit), are set to one and designated for multicast addresses. The leftover 24 bits are used by the device that wishes to communicate data in a group.



Broadcast MAC Address

It's a graphical depiction of all networked gadgets. Broadcast frames are Ethernet frames that comprise one number in each of the destination address's bits (FF-FF-FF-FF-FF), also known as broadcast addresses.

These bits hold all of the designated broadcast addresses. All machines on that LAN section will receive packets with the MAC identifier FF-FF-FF-FF-FF-FF-FF. As a result, if a parent device needs to send data to every device on the network, the broadcast address can be used as the target MAC address.



All about DNS

The DNS is a database of domain name and IP address information that enables computers to locate the correct IP address for a hostname URL input into it. When we attempt to visit a website, we usually type its domain name into the web browser, such as trainwithshubham.com, ip.com, or bharat.com. Web browsers, on the other hand, require the precise IP addresses in order to access information for the website. The DNS is responsible for converting domain names to IP addresses so that data can be loaded from the website's host.

Websites may have multiple IP numbers relating to a single domain name. Large sites, such as Google, will have people accessing a computer from all over the globe. Even if the site name entered in the browser is the same, the server that a computer in Singapore attempts to access will most likely be distinct from the one that a computer in Toronto tries to reach. DNS caching comes into play here.

How Does DNS Work?

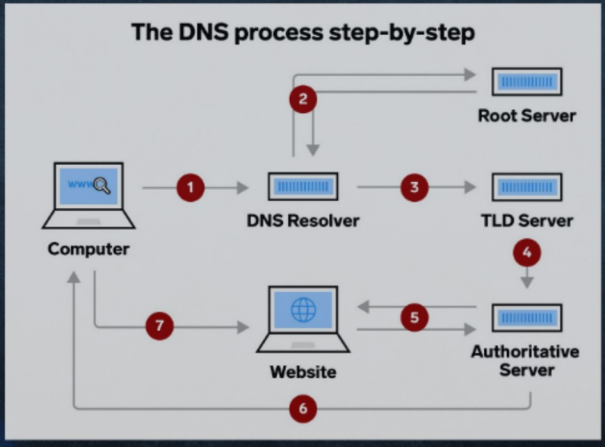
The DNS is in charge of transforming the domain, also known as the website or web page name, to the IP address. A DNS query is the act of inputting the domain name, and DNS resolve is the process of locating the associated IP address.

DNS inquiries are classified into three types: recursive queries, incremental queries, and non-recursive queries.

- Recursive queries are those that require a DNS server to reply with the desired resource record. If an entry cannot be located, an error notice must be displayed to the DNS client.

- Iterative queries are those in which the DNS client requests an answer from numerous DNS servers until the best response is discovered, or until an error or timeout happens. If the DNS server cannot discover a match for the query, it will forward the request to a DNS server authorised for a lower level of the domain namespace. The DNS client then queries this reference address, and the procedure is repeated with additional DNS servers.

- Non-recursive requests are those that are handled by a DNS resolver when the requested resource is accessible, either because the server is authoritative or because the resource is already in cache.



DHCP (Dynamic Host Configuration Protocol)

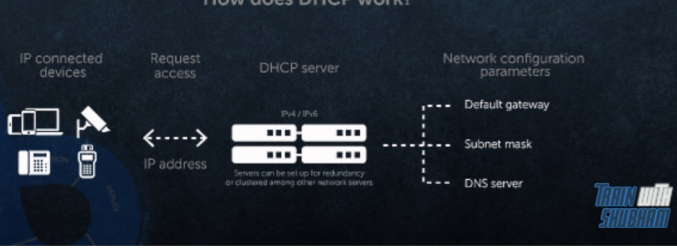
Dynamic Host Configuration Protocol (DHCP) is a network administration protocol that assigns an IP address to any device or component on a network so that they can interact using IP. (Internet Protocol). These settings are automated and managed collectively by DHCP. There is no need to explicitly give IP addresses to new devices. As a result, no user setup is required to join to a DHCP-based network.

DHCP can be used on both local networks and big corporate networks. Most routers and networking devices use DHCP as the default mechanism. RFC (Request for opinions) 2131 is another name for DHCP.

How does DHCP work?

DHCP operates at the application layer of the TCP/IP protocol stack, randomly assigning IP addresses to DHCP clients/nodes and allocating TCP/IP setup information to DHCP clients. Subnet mask information, default gateway information, IP identities, and domain name system identifiers are all examples of information.

DHCP is a client-server system in which servers handle a collection of distinct IP addresses as well as client setup factors and distribute addresses from those address pools.



Why should you use DHCP?

To reach the network and its services, each device on a TCP/IP-based network must have a unique unicast IP address. IP addresses for new computers or computers relocated from one subnet to another must be manually setup without DHCP; IP addresses for computers withdrawn from the network must be manually reclaimed.

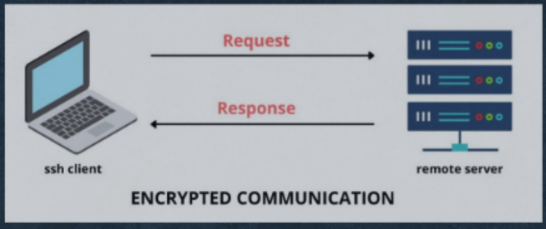
This complete procedure is automated and handled centrally by DHCP. When a DHCP-enabled client connects to the network, the DHCP server keeps a collection of IP numbers and leases one to it. Because IP addresses are dynamic (leased) rather than immutable (assigned forever), addresses that are no longer in use are immediately returned to the pool for reallocation.

In the shape of a lease offer, the network administrator creates DHCP servers that keep TCP/IP configuration information and provide address setup to DHCP-enabled clients. The setup information is saved in a directory by the DHCP server, which includes:

- Valid TCP/IP setup values for all network consumers.
- Valid IP numbers are kept in a database for client distribution, as are excluded addresses.
- IP numbers that have been reserved for specific DHCP customers. This enables a single IP address to be assigned to a single DHCP customer in a uniform manner.
- The lease term, or the amount of time the IP address can be used before requiring a licence renewal.

SSH (Secure Shell or Secure Socket Shell)

- SSH is a protocol for safely accessing distant computers via command line interaction.
- It uses port number 22 by default.
- SSH is the most commonly used method for connecting to distant Linux and Unix-like systems.
- Historically, telnet was used to reach distant computer command line interfaces, but due to security concerns, telnet has become obsolete, and ssh is now used instead of telnet.



- Secure communication encrypts conversation with a public key over an unsecure route and uses a powerful password verification. It is used to supplant unprotected remote login protocols like Telnet, rlogin, rsh, and others, as well as unsafe file transmission protocols like FTP.

- Its security features are extensively used by network managers for remote management of systems and apps.

- The SSH protocol safeguards the network against assaults such as DNS spoofing, IP source routing, and IP faking.

The architecture of SSH Protocol

The SSH architecture is made-up of three well-separated layers. These layers are:

1. **Transport Layer**
2. **User-authentication layer**
3. **Connection Layer**

Since the SSH protocol architecture is open, it offers great freedom and makes it possible to use SSH for a variety of other reasons in addition to just a private shell. The transport layer is analogous to the transport layer protection in the design. (TLS). The user-login layer can be used with custom authentication techniques, and the connection layer provides for the multiplexing of numerous secondary sessions into a single SSH link.

Transport Layer

The transport layer is the protocol suite's upper component. This layer manages the charge of managing initial key exchange, server identification, encryption, compression, and integrity checking for SSH-2. It serves as an interface for transmitting and getting plaintext messages of up to 32, 768 bytes in size.

User authentication Layer

The user authentication layer, as the name implies, is in charge of client identification and offers a variety of authentication techniques. Because authentication is done on the client side, when a login alert appears, it is generally for an SSH client rather than a server, and the server reacts to these authentications.

The User authentication layer contains several authentication techniques, including:

Password: Password verification is a simple method of identification. It has the option to alter the password for simple entry. However, it is not used by all apps.

Public-key: The public-key authentication method is built on public keys and allows DSA, ECDSA, or RSA keypairs.

keyboard-interactive: In this case, the server transmits a prompt for the user to input information, and the client responds with the user's keyed-in answers. It is used to authenticate users with a one-time passcode or OTP.

GSSAPI: In this technique, authentication is done by external methods such as Kerberos 5 or NTLM, which provide SSH connections with single sign-on functionality.

Connection Layer

The link layer specifies the routes through which SSH services are delivered. It specifies the terms channel, channel request, and worldwide request. One SSH link can handle multiple channels at the same time and transmit data in both ways. In the link layer, channel requests are used to send out-of-band channel-specific data, such as the changed dimensions of a terminal window or the departure code of a server-side process. The following are the typical link layer channel types:

- **Shell:** It is used for desktop interfaces, SFTP, and exec commands.
- **Direct-TCPIP:** This protocol is used to forward client-to-server communications.
- **Forwarded-TCPIP**: It is used for redirected server-to-client communications.

SCP (Secure Copy Protocol)

The safe Copy Protocol, abbreviated "SCP," aids in the safe transmission of computer data from a local to a remote host. It is comparable to the File Transfer Protocol "FTP," but it also includes protection and authentication.

The SCP operates on Port 22, and some believe it is a hybrid of the BSD RCP and the SSH protocol.

The RCP protocol is used to transmit files, and the SSH protocol offers authentication and encryption, so SCP is a hybrid of these two protocols.

Because the data being transmitted stays private, the SCP can be used to effectively prevent packet sniffers from extracting valuable information from data packets.

The SCP can also benefit from using SSH because it allows the inclusion of permissions and timestamps for the file that needs to be uploaded.

CP vs SCP

SCP will be easy to grasp if you've used the "cp command" on your local Linux computer. To execute a copy action, both commands must have a source and target file-system address. The primary distinction here is that the SCP needs one or both places to be on a remote system.

For example, the following copy instruction could be used:

copy /main/shub/pictures/picture.png /main/shub/archive/picture*.png*
This command would commence a copy process that would transfer all files in the directory pictures in user shub's main directory with names beginning with picture.png" into the directory "archive" in the "main" directory.

The SCP instruction can be used to accomplish the same operation:

scp /main/shub/pictures/picture.png john@myhost.com:/main/shub/archive*

As shown above, when using the SCP command with the login name shub, those same files would be uploaded to the server myhost.com into the remote directory */main/shub/archive*. The SCP will let the uploading process initiate only if the user "shub" provides his remote password.

A remote location could also be specified as a source if one needs to download the files. For instance,

scp shub@myhost.com:/main/shub/archive/picture.png /main/shub/downloads*

on myhost.com with the name starting with "picture and ending in .png," into the local directory /main/shub/downloads.

The SCP Command Syntax

Before going into the explanation of how the SCP command works, let's take a look at its basic syntax:
scp [-32658BCpqrv] [-c cipher] [-F ssh_config] [-i identity_file]

[-l limit] [-o ssh_option] [-P port] [-S program]

[[user@]SRC_host:]file1 ... [[user@]DEST_host:]file2

- [-c cipher]

This option selects and uses the cipher to encrypt the data transfer. It is passed to the SSH session directly.

- [-F ssh_config]

With this option, an alternative per-user configuration file would be specified for the SSH. It is sent to SSH directly.

- [-i dentity_file]

It chooses the file which provides the identity (key) for RSA authentication. It is passed to the SSH directly.

- [-I limit]

This option can be used to limit the bandwidth, which is in Kbps.

- [-o ssh_option]

It can be applied to pass options to SSH using the same format as of the ssh_config. It is helpful to specify the options which have no separate SCP command-line flag.

- -P port:

This option states the port needed to connect to, on the remote host. Keep in mind that this option has a capital “P”; small “p” is used for other tasks

- -p:

It is used to preserve access times, modification times, and modes from the original file.

- -q:

It can be applied to disable the progress meter.

- -r:

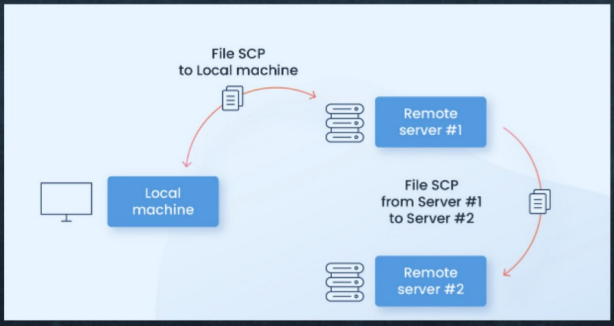
It can be used to copy the entire directories recursively.

- -S program:

It specifies the name of the program that is used for the encrypted connection. It is essential for the program to understand the SSH options.

- -v:

This is the verbose mode which forces SCP and SSH to show the debugging messages about the progress. It can be useful for troubleshooting connection, authentication, and configuration issues.



cURL (Client URL)

Client URL (pronounced "curl") is a command line utility that allows data to be exchanged between a device and a website via a terminal. A user provides a server URL (the place where they want to make a request) and the data they want to transmit to that server URL using this command line interface (CLI).

The cURL function makes use of the client-side URL transfer tool libcURL. Many various transmission methods are supported by this software, including HTTPS, SMTP, and FTP. When making queries, you can also include cookies, establish proxies, and add login details.

curl is powered by libcurl, a portable client-side URL transfer library. You can use it directly on the command line or include it in a script. The most common use cases for curl are:

- Downloading files from the internet
- Endpoint testing
- Debugging
- Error logging

Basics: How to Use curl

curl [option] [url]

Options will direct curl to perform certain actions on the URL listed. The URL gives curl the path to the server it should perform the action on. You can list one URL, several URLs, or parts of a URL, depending on the nature of your option.

Listing more than one URL:
curl -O http://url1.com/file1.html -O http://url2.com/file2.html

Listing different parts of a URL:
http://example.{page1,page2,page3}.html

cURL Protocols and Formats

cURL utilises the HTTP interface by default. cURL can also use the following protocols and formats:

FTP - File Transfer Protocol.

The File send Protocol (FTP) is a protocol used to send data from a server to a client. Use this protocol in conjunction with cURL to send items like this:

cURL -T [chosen-file] "ftp://[target-destination]"

cURL is an excellent substitute for a normal FTP client.

Simple Mail Transfer Protocol

For transmitting messages to an SMTP server, use the Simple Mail Transfer Protocol (SMTP). This info includes the content you're transmitting, as well as the sender and recipient. It appears as follows:

cURL smtp://[smtp-sever] --mail-from [sender] --mail-rcpt \ [receiver] --upload-file [mail-content-file]

Dictionary Network Protocol (DICT)
The Dictionary Network Protocol (DICT) allows you to access dictionaries by running the following command with

cURL: cURL "dict://dict.org/d:hello"

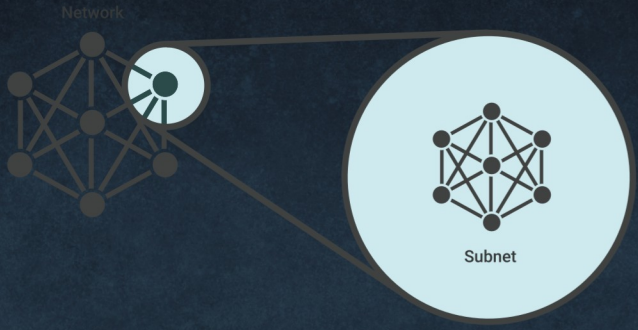
This command returns a result with the dictionary selected and the definition of "hello" from the dictionary.

Make cURL work for you.
cURL is a command-line utility that enables you to request and send data over a URL using various protocols. It gives you flexibility and control of URLs on the terminal.

Using cURL on the terminal is simple, but may not be intuitive to use by every user. By providing the URL and the options needed, you can request and download data from URLs, transfer data to URLs, and more.

What is a subnet

A subnet or subnetwork is a smaller network inside a large network. Subnetting makes network routing much more efficient.

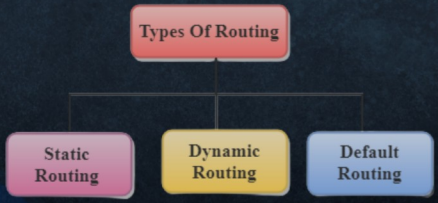


Subnetting occurs when a larger network is split into smaller networks to keep security. As a result, lesser networks are easier to maintain. For example, if we examine a class A address, the potential number of hosts for each network is 224. It is clear that maintaining such a large number of hosts is challenging, but it is much simpler to maintain if we split the network into tiny sections.

Subnet itself is a huge chapter to study and gain some experience with it, if you want to more then refer to some blogs and articles for in-depth subnetting

Routing

- A router is a mechanism that selects a way for data to be transferred from source to target. A router is a unique instrument that performs routing.
- A router operates at the network layer of the OSI model and at the internet layer of the TCP/IP model.
- A router is a networking device that sends packets using information from the packet header and routing table.
- Routing methods are used to route messages. The routing method is nothing more than software that determines the best route for packet transmission.
- The metric is used by routing algorithms to find the optimal route for packet delivery. The metric is the unit of measurement used by the routing algorithm to determine the best route to the target, such as step count, bandwidth, latency, present traffic on the channel, and so on.
- The routing algorithm creates and manages the routing table for the route selection procedure.



Static Routing

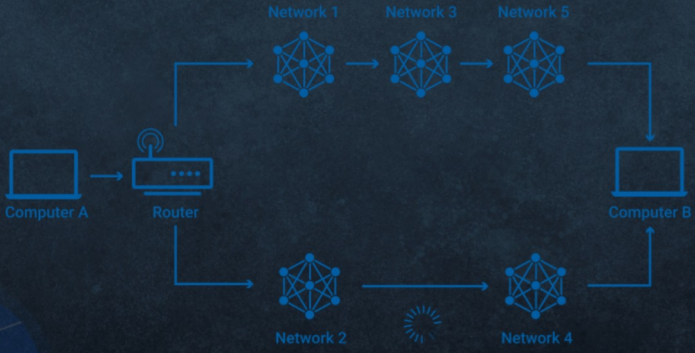
- Nonadaptive Routing is another name for static routing.
- It is a method in which an administrator physically enters paths into a routing database.
- The packets for the target can be sent by a Router along the path specified by the user.
- This method does not make routing choices based on network condition or topology.

Default Routing

- Default Routing is a routing method in which a router is set to deliver all messages to the same hop device, regardless of whether it belongs to a specific network or not. A packet is sent to the device for which default routing is set.
- Default When networks have a singular departure point, routing is used.
- It is also helpful when a large number of communication networks must send data to the same HP device.
- When a particular route is stated in the routing table, the router will take that route instead of the usual route. When a particular route is not listed in the routing table, the default route is used.

Dynamic Routing

- It is also referred to as Adaptive Routing.
- It is a method in which a router creates a new path in the routing table for each packet in reaction to changes in the network's state or topology.
- Dynamic protocols are used to find novel paths to the target.
- RIP and OSPF are the protocols used in Dynamic Routing to find novel paths.
- If any path fails, an automatic adjustment will be made to get to the location.



What are routing algorithms?

Routing algorithms are programs that execute various routing schemes. They operate by allocating a cost number to each connection, which is computed using various network data. Every router attempts to send the data packet to the next best connection at the lowest possible cost.

Here are some examples of algorithms.

- Distance Vector Routing

The Distance Vector Routing algorithm needs all routers to communicate with one another on a regular basis about the best way information they have discovered. Each router transmits information about the current overall cost estimate to all known locations.

Every router in the network eventually finds the optimal path information for all potential locations.

- Link State Routing

Every router in the network finds all other routers in the network when using Link State Routing. A router uses this information to build a map of the entire network and then determines the quickest path for any data packet.

Thank you Dosto

TRAIN WITH SHUBHAM