<https://www.naukri.com/code360/guided-paths/computer-networks/content/190928/offering/2433400>

**Introduction to Networkingfooter line**

The dictionary defines the word networking as "a group or system of interconnected people or things." Similarly, within the computer world, the term network means two or more connected computers which will share resources like data and applications, office machines, an online connection, or some combination.

The main task is to supply participants with one platform for exchanging data and sharing resources. This task is so essential that many aspects of lifestyle and therefore the times would be unimaginable without networks. Here's a real-life example: during a typical office, every workstation has its computer. Without a network of computers, it might be difficult for a team to figure on a project since there would be no commonplace to share or store digital documents and knowledge, and team members wouldn't be ready to share specific applications.

**Overview of Network Components**

The following list describes the network components depicted and, therefore, the functions they serve:

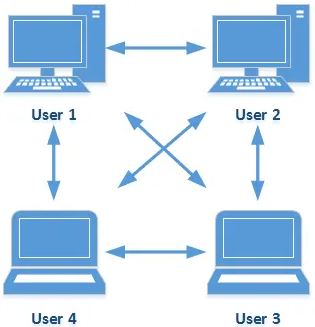
* **Client:** The term client defines the device an end-user uses to access a network. This device could be a workstation, laptop, smartphone with wireless capabilities, or a spread of other end-user terminal devices.
* **Server:** A server, because the name suggests, serves up resources to a network. These resources might include e-mail access provided by an e-mail server, sites provided by an internet server, or files available on a digital computer.

**Network Architecture**

A way to categorize networks is predicated on where network resources reside. An example of a client/server network may be a collection of PCs, all sharing files on a centralized server. However, if those PCs had their OS (OS) (for example, Microsoft Windows 8 or Mac OS X) configured for file sharing, they might share files from one another's hard drives. Such an appointment would be a peer-to-peer network because the peers (the PCs during this example) make resources available to other peers.

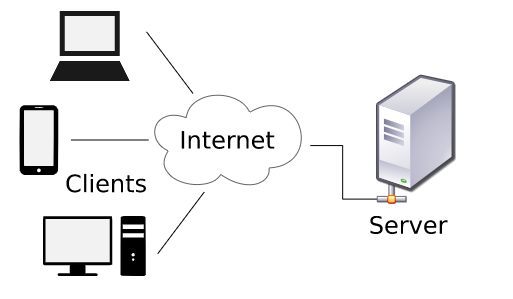
**Peer-to-Peer Networks**

Peer-to-peer networks allow interconnected devices (for example, PCs) to share their resources. Those resources might be, for instance, files or printers. As an example of a peer-to-peer network, consider below figure, where each peer can share files on their hard drives shared with the opposite peers within the network.



**Client-Server Networks**

Client/server may be a model of interaction during which a program sends an invitation to a different program and awaits a response. The requesting program is named a client; the answering program is called a server. Although the client/server model is often used between programs during a single computer, the term typically refers to a network. A client-server network may have quite one server, each dedicated to handling a selected function.



**Topologiesfooter line**

The configuration, or topology, of a network is vital to determining its performance. Topology is the way a network is arranged, including the physical or logical description of how links and nodes are found to relate to every other. It maps how different nodes on a network--including switches and routers--are placed and interconnected, as well as how data flows. Diagramming the locations of endpoints and repair requirements helps determine the most precise placement for every node to optimize traffic flows. A well-planned topology enhances the user experience and allows administrators to maximize performance while fulfilling business needs. When the proper topology is chosen for a business's needs, it's easier to locate faults, troubleshoot and fixes problems, and share resources across networks.

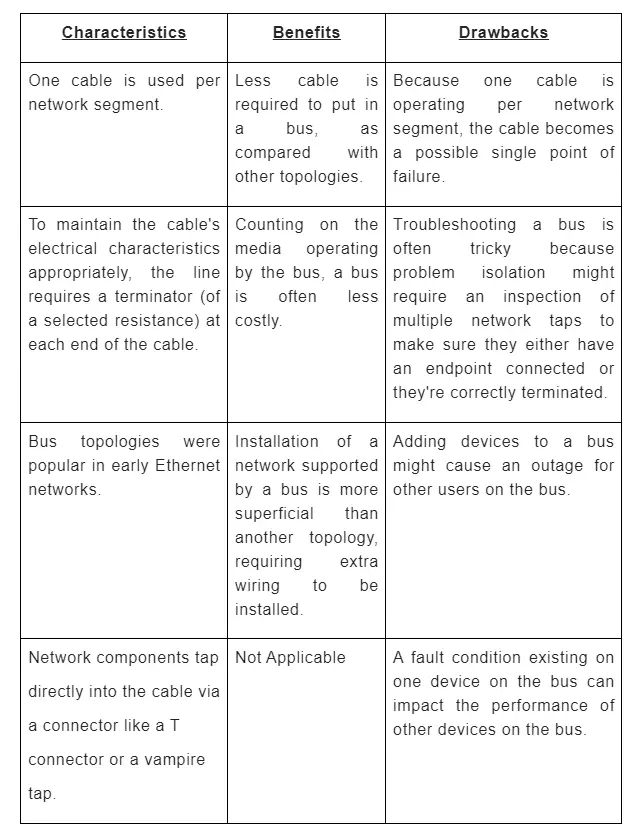
Type of Physical Topologies

The physical topology refers to the particular connections (wires, cables, etc.) of how the network is arranged. Setup, maintenance, and provisioning tasks require insight into the physical network. The subsequent are some of the physical topologies:

**Bus topology**

As depicted , it typically uses a single cable running throughout, requiring connectivity. Early Ethernet networks commonly relied on bus topologies.

Every device connected to this structure requires a network segment. One network segment may be a single collision domain, which suggests that each one device connected to the bus might attempt to gain access to the bus at an equivalent time, leading to a condition referred to as a collision. Table 1-1 identifies a number of characteristics, benefits, and disadvantages of the bus.



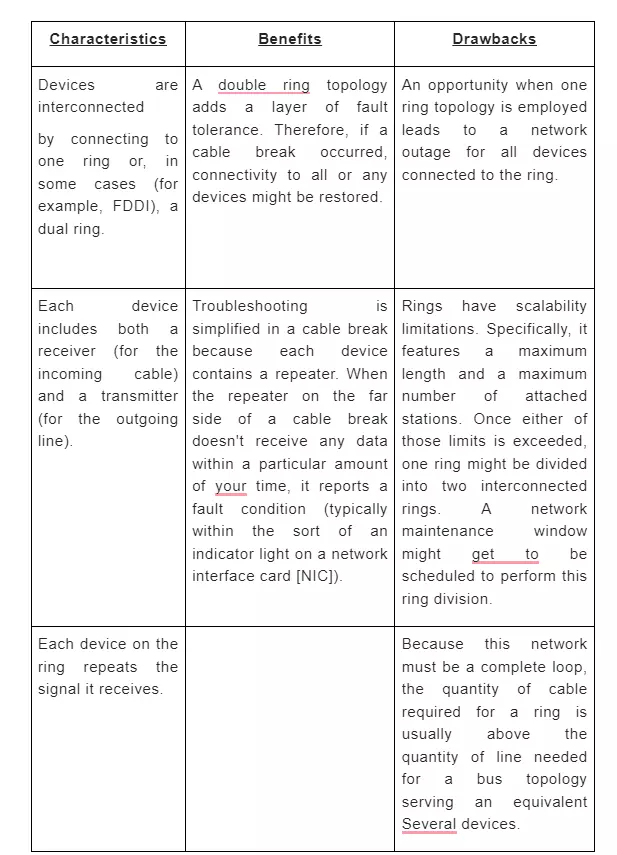
**Table 1**

**Ring topology**

Ring topology, where traffic flows circularly around a closed network loop (that is, a ring). Typically, this topology sends data, during a single direction, to every connected device successively until the intended destination receives the info. Token Ring networks typically relied on the same topology, although the ring may need been the topology, whereas physically, the topology was a star.

The method of transferring data within the ring structure is named token passing. A token may be a particular sequence of bits containing control information. Owning the ticket allows a network device to transfer data to the network. There's just one token in each network. The sending computer removes the token from the ring and sends the requested data within the circle. Each computer forwards the info until the packet finds the pc that matches the info address. The receiving computer then sends a message that the information has been received back to the sending computer. After verification, the sending computer creates a replacement token and releases it to the network.

Because this topology allows devices on the ring to require turns transmitting, contention for media access wasn't dragged because it was for a bus. If the crew was broken at any point, data would stop flowing. Table 2 identifies a number of the primary characteristics, benefits, and disadvantages of a hoop topology.

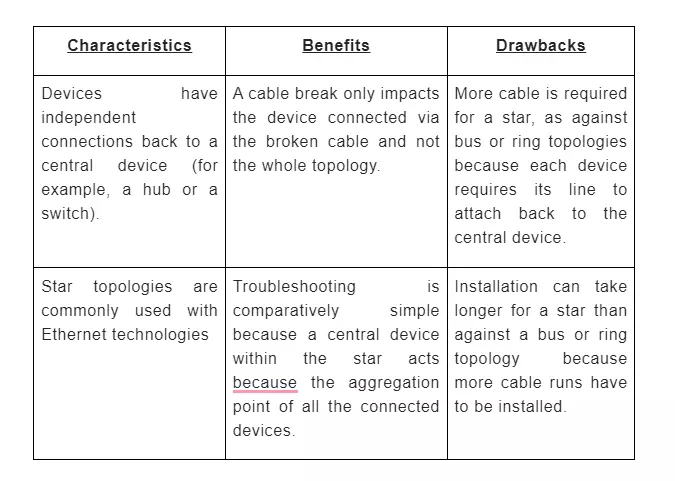


**Table 2**

**Star topology**

Star topology may be where each piece of a network is attached to a central node (often called a hub or switch). The attachment of those network pieces to the main component is visually represented during a form, almost like a star.

Computers aren't connected to at least one another in a star but are all connected to a central hub or switch. When a computer sends data to other computers on the network, it's sent along the cable to a central hub or control, determining which port it must send the info through for it to succeed in the right destination.



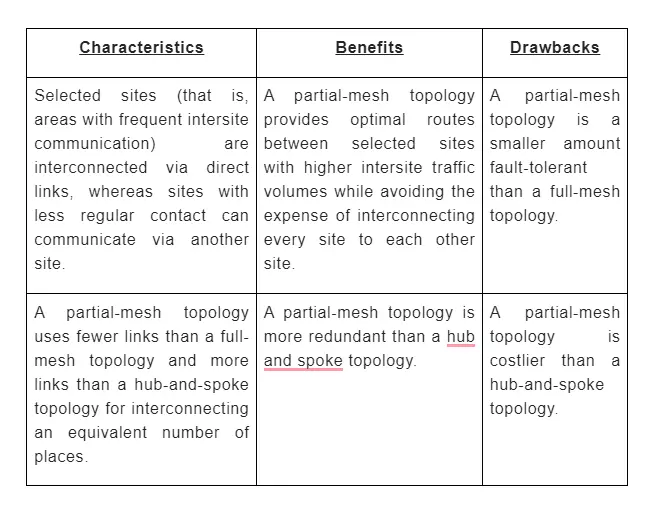
**Table 3**

**Mesh topology**

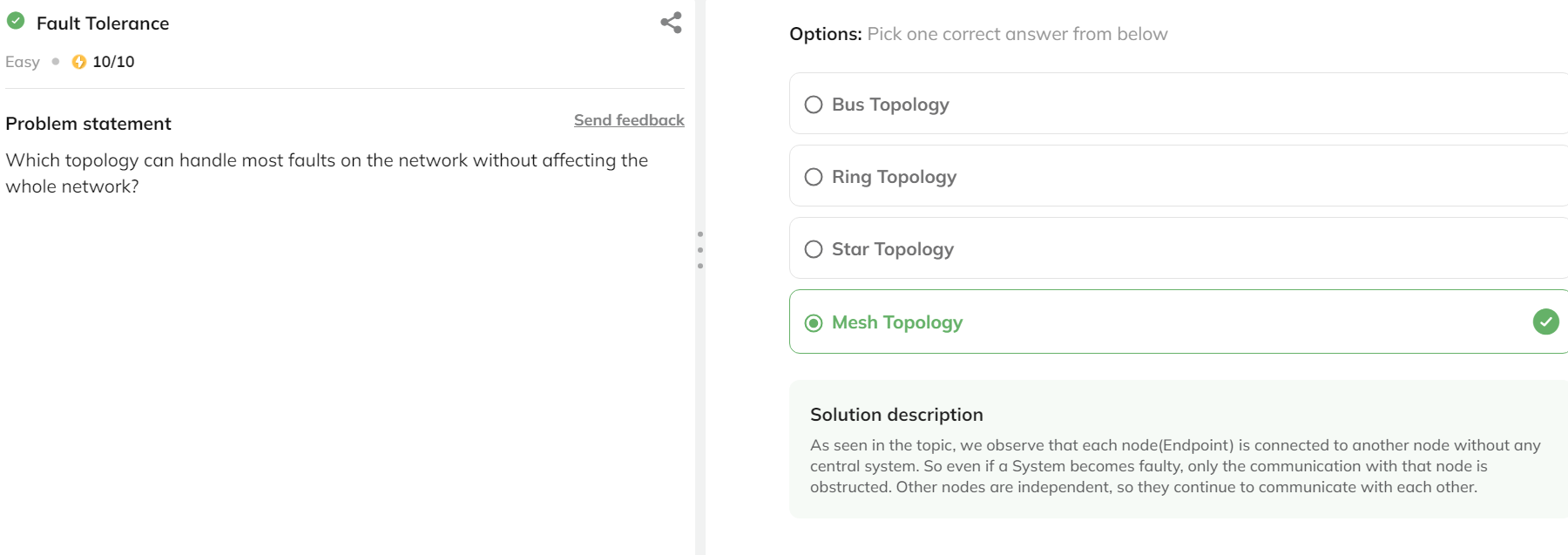
A mesh may be a network setup where each computer and network device is interconnected with each other. This topology setup allows for many transmissions to be distributed, albeit one among the connections goes down. It's a topology commonly used for wireless networks. Below may be a visual example of an accessible computer found out on a web employing a mesh.

Each computer not only sends its signals but also relays data from other computers. This sort of topology is costly as It's challenging to determine the connections of the mesh. During a mesh, every node features a point-to-point connection to the opposite node. The links within the mesh are often wired or wireless.

Mesh network topologies create multiple routes for information to travel among connected nodes. This approach increases the resilience of the network just in case of a node or connection failure. More extensive mesh networks may include multiple routers, switches, and other devices, which operate as nodes. A mesh network can consist of many wireless mesh nodes, which allows it to span an outsized area.

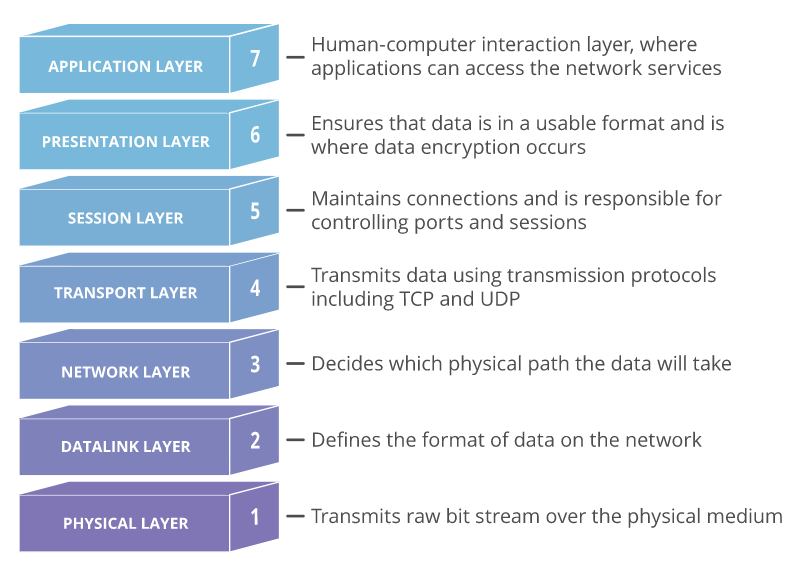


**Table 4**



## ****OSI Model****footer line

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the primary standard model for network interchanges, embraced by all significant PC and telecom organizations inside the 1980s. To raise and see how a particular innovation fits in, be that as it may, it assists with having a typical perspective against which different advancements from different merchants are frequently looked at. Understanding the OSI model additionally can help investigate organizations. One of the solitary standard methods of sorting the capacity of organization innovation is to state at what layer (or layers) of the OSI model that innovation works.



Presently we should take apart each layer and look at its job and usefulness to comprehend the OSI model and its utilization. Before beginning, different mental aides are accessible to help with remembering these layers in their appropriate request. A down-top (that is, beginning at the absolute bottom of the stack with Layer 1 and managing your high to Layer 7) acrostic is:

### ****The Physical Layer****

At this layer, double articulations (that is, a progression of 1s and 0s). A twofold word is framed from **bits**, where a touch might be a solitary one or one 0. At upper layers, nonetheless, pieces are gathered into what's alluded to as a convention information unit or an information administration unit.

It characterizes electrical and actual determinations for gadgets. The virtual layer depicts the association between an apparatus and a transmission medium, similar to a copper or optical link. This incorporates the format of pins, voltages, link particulars, centers, repeaters, network connectors, have transport connectors, and the sky is the limit from there. The principle capacities and administrations performed by the actual layer are:

* **The portrayal of Bits:**Data during this layer comprises a surge of pieces. The pieces should be encoded into signals for transmission. It characterizes the kind of encoding, i.e., how 0's and 1's are changed to flag.
* **Information Rate:**This layer characterizes the speed of transmission, the number of pieces each second.
* **Synchronization:**It manages the synchronization of the transmitter and recipient. The sender and recipient are synchronized at bit level.
* **Interface:**The actual layer characterizes the transmission interface among gadgets and, in this way, the transmission medium.
* **Line Configuration:** This layer interfaces gadgets with the medium: Point to Point setup and Multipoint arrangement.

### ****The Data Link Layer****

This layer cares about bundling information into **frames** and sends, transmitting organization, performing mistake identification/rectification, distinguishing network gadgets with a location, and taking care of stream control. These cycles are aggregately referenced as information interface control.

Layer 2 of the OSI model comprises of two sublayers: the **Media Access Control** (MAC) sublayer and, along these lines, the **Logical Link Control** (LLC) sublayer. The MAC sublayer controls gadget connection. The LLC sublayer manages tending to and multiplexing. Actual Addressing for network associations exists at the information connect layer. The primary capacities and administrations performed by this layer are:

* **Framing:** Frames are the floods of pieces from the organization layer into reasonable informationThe Data Link Layer does this division of stream of bits.
* **Physical Addressing:** The Data Link layer adds a header to the casing to characterize the exact location of the sender or beneficiary of the edge if the edges are to be disseminated to various frameworks on the organization.
* **Flow Control:** Error control is accomplished by adding a trailer at the highest point of the edge. Duplication of designs is moreover forestalled by utilizing this system. Connection Layers add an apparatus to stop the proliferation of borders.
* **Error Control:** Error control is achieved by adding a trailer at the end of the frame. Duplication of structures is also prevented by using this mechanism. Data Link Layers adds a means to avoid the recurrence of frames.
* **Access Control:** Protocols of this layer figure out which of the gadgets has authority over the connection at some random time when at least two devices are associated with an identical connection.

The information interface layer is selective from the contrary layers in that it's two sublayers of its own:

* **Media Access Control:**The MAC layer is obligated for moving information frames to and from one Network Interface Card (NIC) to an alternate across a common channel. This layer’s usefulness is made into the organization connectors, consolidating a chronic number that recognizes the dealer and connector.
* **Logical Link Control:**The Logical Link Control (LLC) sublayer explains the data connection; along these lines, it controls the synchronization, stream control, and slip checking elements of the information interface layer. This layer can deal with association arranged transmissions (dissimilar to the MAC sublayer beneath it), albeit this layer can likewise offer connectionless support.

### ****The Network Layer****

### 

This layer has two primary capacities. One is finishing sections into network **Packets** and reassembling them on the less than desirable end. The inverse is directing parcels by finding the most obvious way across an actual organization. This layer utilizes network addresses (commonly Internet Protocol addresses) to course parcels to an objective hub. The organization layer discovers the objective by using intelligent addresses, similar to IP (web convention). At this layer, switches are a fundamental part that will not work precisely in a real sense of course data where it should go between networks.

* The network layer breaks the more oversized parcels into little bundles.
* Association administrations are given, including network layer stream control, layer mistake control, and bundle succession control.
* **Logical Addressing** Sensible Addressing Physical Addressing carried out by the DL layer handles the issue of tending to locally. The Network layer adds a header to the parcel coming from the upper layer that additionally incorporates consistent addresses of the sender and, subsequently, the collector.
* **Routing** When free organizations or connections are associated with make internetworks/broad organization, the directing devices(router or switches) course the parcels to their last objective. This is frequently perhaps the most capacity of the network layer.

As the connection layer manages the conveyance of the bundles between two frameworks on an identical organization, the organization layer essentially guarantees that each pack gets from its starting place to a definitive objective. It likewise partitions the active messages into parcels and gathers approaching bundles into messages for more elevated levels. The steering issue in broadcast networks is direct; along these lines, the organization layer usually is slight or non-existent. On the off chance that two PCs (framework) are associated with a close connection, there's no requirement for an organization layer. In any case, for good measure, if two frameworks ate joined to various networks(relationships) with interfacing gadgets between the networks(links), then, at that point, there's a necessity for the organization layer to achieve the source-to-objective conveyance. Devices for this layer:

### ****The Transport Layer****

### 

This layer goes about as a line between the OSI model's upper and lower layers. It takes information moved inside the session layer and breaks it into **Segments** on the sending end. In particular, messages are taken from the upper (Layers 5–7) and are epitomized into pieces for transmission to the lower (Layers 1–3). Also, information streams from lower layers are decapsulated and shipped off Layer 5 (the meeting layer) or another upper layer, depending on the convention. It's obligated for reassembling the fragments on the less than desirable end, turning it back to information that the meeting layer will utilize.

* **Service Point Addressing:** Transport Layer header incorporates administration point address which is that the port location. This layer gets the message to the appropriate cycle on the pc, in contrast to Network Layer, which receives every bundle to the correct PC.
* **Division and Reassembling:**A message is parted into segments(that are communicable); each part contains a succession number, which empowers this layer to reassemble the message. The message is reassembled accurately upon landing in the objective and replaces bundles that were lost in transmission.
* **Association Control:**It incorporates two sorts:
  + Connectionless Transport Layer: Each fragment is viewed as an autonomous bundle and conveyed to the vehicle layer at the objective machine.
  + Association Oriented Transport Layer: The association is framed with the vehicle layer at the objective machine before conveying bundles.
* **Flow Control:** during this layer, stream control is performed end to complete rather than across one connection.
* **Error Control:** Error Control is performed end to wrap up during this layer to guarantee that the whole message shows up at the getting transport layer with no mistake. Blunder Correction is finished through retransmission.

### ****The Session Layer****

This layer tracks the exchanges between PCs, which likewise are called **Sessions**. This layer sets up, controls, and finishes the concourses among area and distant applications. The Session Layer permits clients on various machines to decide dynamic correspondence meetings between them. Its principal point is to characterize, keep up with and synchronize the cooperation between imparting frameworks. The meeting layer oversees and synchronizes the discussion between two separate applications. In the Session layer, floods of information are stamped and are sufficiently resynchronized so the closures of the messages aren't cut rashly, and information misfortune is kept away from.

* **Discourse Control:**This layer permits two frameworks to begin correspondence with each other fifty-fifty duplex or full-duplex.
* **Token Management:** This layer keeps two gatherings from endeavoring an identical essential activity at a comparable time.
* **Synchronization:** This layer permits a cycle to highlight designated spots, which are considered synchronization focuses on the stream of information. Model: If a framework sends a record of 800 pages, adding designated sites after every 50 pages are proposed. This guarantees that a fifty-page unit is effectively gotten and recognized. This is frequently gainful at the hour of the crash as though an accident occurs at pagination 110; there's no chance to retransmit one to100 pages.

### ****The Presentation Layer****

### 

The show layer is responsible for the arranging of information being traded and protecting that information with **encryption**. This layer fundamentally acts because of the interpreter of the organization. Another name of the show layer is that the Syntax layer. The principal objective of this layer is to require care of the sentence structure and semantics of the information traded between two conveying frameworks.

This layer takes care that the data is sent in such that the recipient will comprehend the information(data) and be prepared to utilize the information. Languages(syntax) are frequently unique between the two conveying frameworks. Under this condition, the show layer plays an undertaking as an interpreter. To frame it workable for PCs with various information portrayals to talk, the data designs to be traded are frequently characterized in a theoretical manner.

* **Interpretation:**Before being sent, the information inside the characters and numbers ought to be changed to bitstreams. The show layer is obligated for interoperability between encoding techniques as various PCs utilize diverse encoding strategies. It deciphers information between the configurations the organization requires and subsequently the arrangement of the pc.
* **Encryption:** It completes encryption at the transmitter and decoding at the collector.
* **Compression:** It does information squeezing to downsize the data transfer capacity of the information to be sent. The primary job of information pressure is proportional back to the measure of pieces to be sent. It’s significant in communicating interactive media like sound, video, text, and so on.

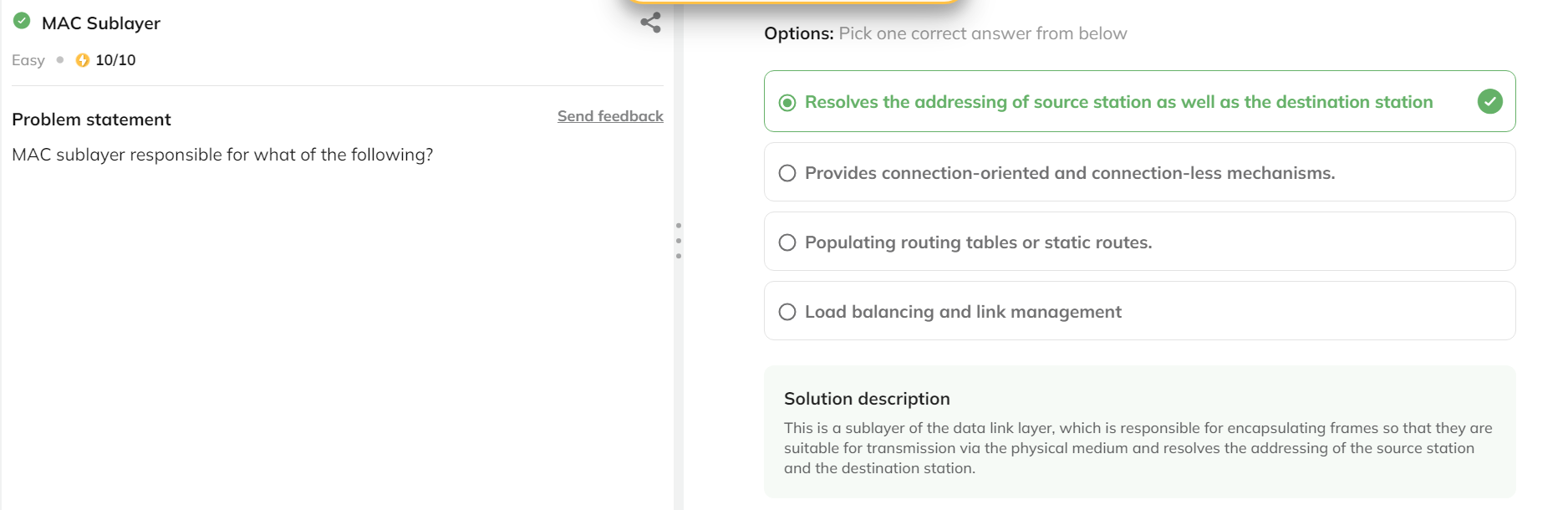
### ****The Application Layer****

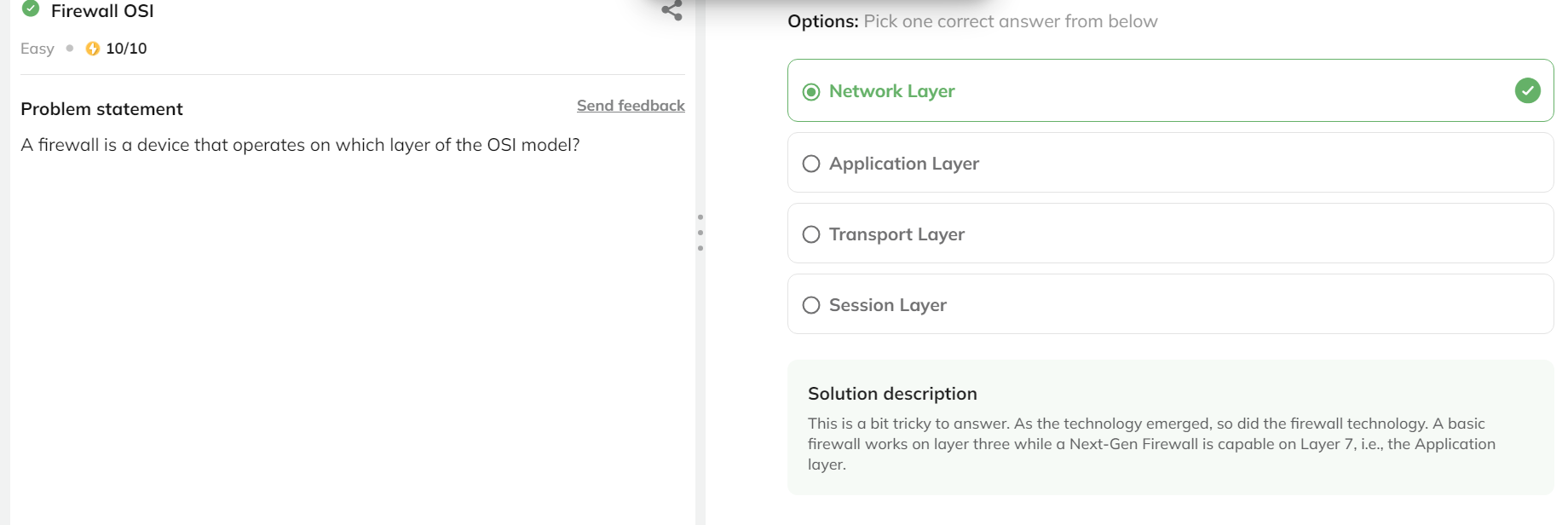
The application layer gives application administrations to a network. An essential and frequently misconstrued idea is that end-client applications (for instance, Microsoft Word) don't live at the machine layer. The machine layer upholds administrations utilized by end-client applications. For example, email is an application layer administration that dwells at the apparatus layer. In contrast, Microsoft Outlook (an illustration of an email customer) is an end-client application that doesn't live at the machine layer. Another capacity of the machine layer is promoting accessible administrations.

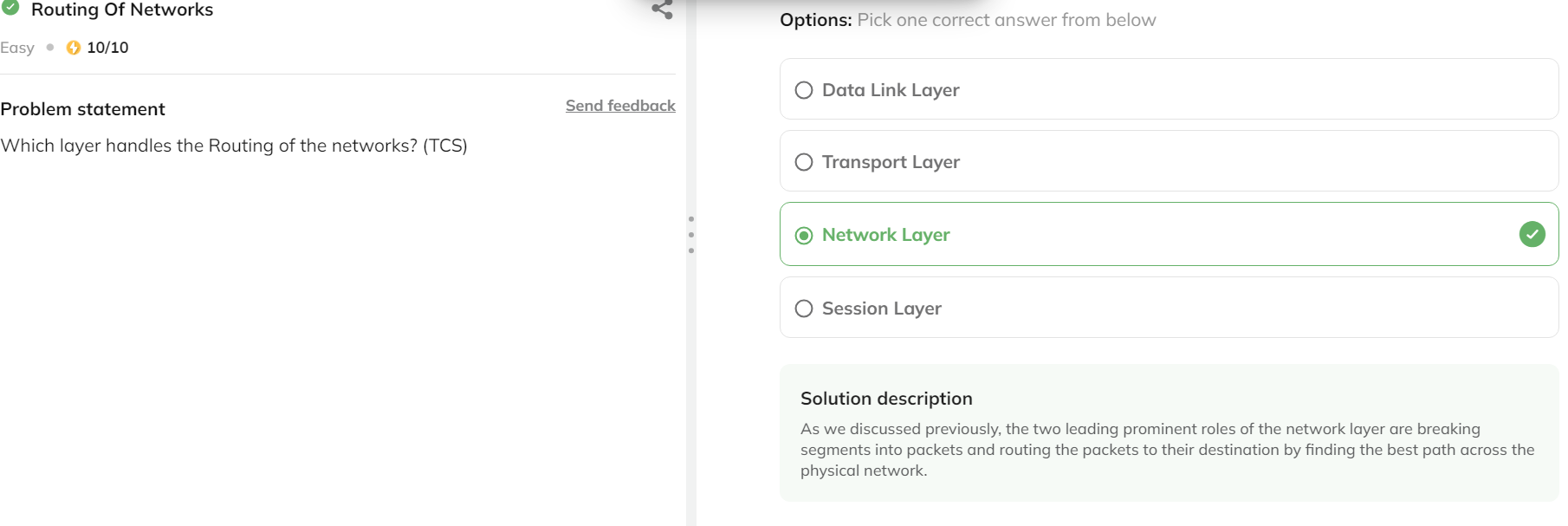
* **Mail Services:** This layer gives the plan to Email sending and capacity.
* **Organization Virtual Terminal:**It permits a client to go online to an unfamiliar host. The apparatus makes programming copying of a terminal at the far off have. The client's PC converses with the product terminal, which progressively chats with the host and the reverse way around. Then, at that point, the distant host trusts it's speaking with one among its terminals and permits the client to go on the web.
* **Index Services:**This layer gives admittance to worldwide data about different administrations.
* **File Transfer, Access, and Management (FTAM):** it's a run-of-the-mill component to get to records and oversees them. Clients can get to documents on a remote PC and watch them. They will likewise recover documents from an unfamiliar PC.

The accompanying portrays the elements of the machine layer in extra detail:

* Application administrations: tests of the apparatus administrations living at the machine layer incorporate document sharing and email.
* Administration ad: Some applications' administrations (for instance, some organized printers) occasionally send promotions, spreading the word about the stock of their administration for different gadgets on the organization. Different administrations, notwithstanding, register themselves and their administrations with a brought together index (for instance, Microsoft Active Directory), which might be questioned by other organization gadgets looking for such administrations. structures







## ****Interview Questions****footer line

Networking Basic

**Q1.** What is a node? (**Cisco**)

**Answer:** A node may be a point of connection within a network for systematic data transmission. A computer or printer, or other devices capable of sending and receiving data through a network is often called a node. Let's consider that there are two computers, two printers, and a server connected during a network; then we will say there are five nodes.

**Q2.** What exactly does one mean by a backbone network? (**Juniper**)

**Answer:** It is a network liable for assigning the info and, therefore, the route to different networks. Monitoring the channels, protocols, and bandwidth management is additionally the responsibility of a backbone network. It's due to this reason it's been named as a backbone network.

**Q3.** In data encapsulation, how each chunk knows about its destination? (**Cisco**)

**Answer:**Data encapsulation is an approach during which the info is split into smaller packets called chunks. All chunks have their source and destination address on them, which is how they reach their destination. It's necessary for network security that the chunk must contain its source address too.

**Q4.**What is the importance of the Physical Layer within the OSI model? (**Arista**)

**Answer:** Physical layer resembles the particular transfer of data from source to destination in bitstream – electrical impulse, light, or radio wave. In simple words, it accepts a frame from the info link layer and converts it into bits. It also receives bits from the physical medium and converts them into the structure.

**Q5.**What are the standards to see the network reliability? (**Dell**)

**Answer:**Network reliability means the power of the network to hold out the specified operation, like communication through a network. Network reliability plays a significant role in network functionality. The network monitoring systems and devices are the essential requirements for creating network reliability. The network monitoring system identifies the issues within the network while the network devices make sure that data should reach the excellent destination.

The following factors can measure the reliability of a network:

* **Downtime:** The downtime is defined because of the required time to recover.
* **Failure Frequency:** it's the frequency when it fails to figure the way it's intended.
* **Catastrophe:**It indicates that the network has been attacked by some unexpected event like fire or earthquake.

## Classful Addressingfooter line

Classful addressing may be a concept that divides the available address space of IPv4 into five classes, namely A, B, C, D & E. Nowadays, this idea has become obsolete and has been replaced with classless addressing. IP addresses, before 1993, use the classful addressing where classes have a hard and fast number of blocks and every block features a fixed number of hosts. Each of those classes features a valid range of IP addresses. Types D and E are reserved for multicast and experimental purposes, respectively. The order of bits within the first octet determine the classes of IP address.

**The IP Address**

IP (Internet Protocol) Address is the address of your network hardware. It helps in connecting your computer to other devices on your Network and everyone over the planet. An IPv4 address may be a 32-bit address. However, instead of writing out each bit value, the address is usually written in dotted-decimal notation. Consider the IP address of 10.1.2.3. This address is written in dotted-decimal notation. Notice that the IP address is split into four separate numbers, separated by periods. Each number represents one-fourth of the IP address. Specifically, each number represents an 8-bit portion of the 32 bits within the address. Because each of those four divisions of an IP address represents 8 bits, these divisions are called octets.

All devices connected to an online connection have a singular IP address, which suggests billions of IP addresses are required. An IP address has information about how to reach a selected host, especially outside the LAN. An IP address may be a 32-bit unique address having an address space of 2³². Generally, there are two notations during which IP address is written, dotted mathematical notation and hexadecimal notation. Addresses in IPv4 are 32-bits long. This enables for a maximum of 4,294,967,296 (2³²) unique addresses. Addresses in IPv6 are 128-bits, which allows for 3.4 x 10³⁸ (2¹²⁸) unique addresses.

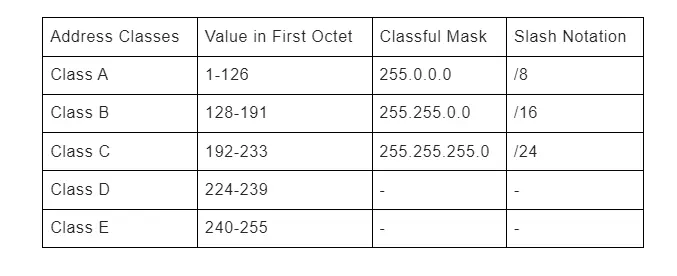
IPv4 address is split into two parts:

* **Network ID:** A network ID, within the world of Transmission Control Protocol/Internet Protocol or TCP/IP, is the portion of the TCP/IP address that identifies the Network for a given host, usually composed of three octets with dotted-decimal representation. The term "network ID" also can be applied in several ways to local network resources for user authentication. Still, the classic use of the time relates to the TCP/IP address itself, how that's wont to route information. Think of the Network ID because the suburb you reside in and therefore the Node ID your street therein suburb. You'll tell precisely where someone is if you've got their suburb and street name. In the same way, the Network ID tells us which Network a specific computer belongs to. Therefore the Node ID identifies that computer from all the remainder that reside within the same Network.
* **Host ID:**The Host ID is the portion of an IP address that uniquely identifies a number on a given TCP/IP network. You discover the host ID by logically NANDing the binary sort of the IP address with the binary some the subnet mask for the Network. The opposite part of an IP address is the network ID, which specifies the Network to which the host belongs.

When writing a network address, or an IP address for that matter, Who must provide more detail than simply a dotted-decimal representation of an IP address's 32 bits. For instance, just being told that a tool has an IP address of 10.1.2.3 doesn't tell you the Network on which the IP address resides. To understand the network address, you would like to understand the subnet mask, which might be written in dotted-decimal notation or Lukasiewicz notation (also referred to as slash notation ). Within the Example, where we have an IP address of 10.1.2.3 and an 8-bit subnet mask, the IP address might be written as 10.1.2.3 255.0.0.0 or 10.1.2.3 /8. Similarly, the network address might be written as 10.0.0.0 255.0.0.0 or 10.0.0.0 /8.

**Classes of Addresses**

Although an IP address (or a network address) needs subnet mask information to work out which bits represent the network portion of the lesson, there are default subnet masks with which you ought to be familiar. The default subnet mask for a given IP address is solely determined by the worth within the IP address's first octet.



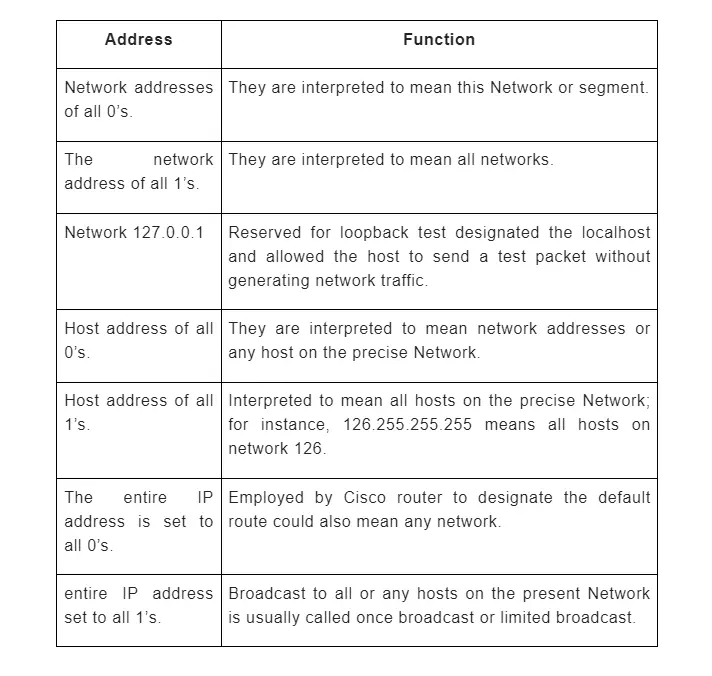
**Class A Addresses**

Class A addresses are for networks with a sizable amount of total hosts. Class A allows for 126 networks by using the primary octet for the Network ID. the primary bit is usually set and glued to zero during this octet. And next seven bits within the octet are ready to at least one, which then complete the network ID. The 24 bits within the remaining octets represent the host's ID, allowing 126 networks and approximately 17 million hosts per Network. Class A network number values begin at one and end at 127. the category A format is as follows:

**Network.Host.Host.Host**

Class A network addresses are 1 byte long, with the primary little bit of the byte reserved and the seven remaining bits available for manipulation or address. As a result, the theoretical maximum number of sophistication A networks which will be created is 128. Why well, each of the seven-bit positions can either be a zero or one, and a couple of to the facility of seven gives you 128. The designers of the IP address scheme said that the primary little bit of the quick bite during a Class A network address should be off, or 0. this suggests Class A address must be between zero and 127 within the first byte, inclusive.

To complicate matters further, the Network of all zeros addresses is resolved by designating the default route. Additionally, the route address 127, reserved for diagnostics, cannot be used either, which suggests that you can only use the numbers 1 to 126to designate class eight network addresses. this means the particular number of usable classes in network addresses is 128 - 2 or 126.



Each class address has three bytes for the host address of the machine this suggests there are 2²⁴ unique combinations and thus precisely that a lot of potential special hosting lessons for every class within the Network. Because host addresses with two partners of all zeros and ones are reserved, the particular maximum usable number of hosts for sophistication in-network is 2²⁴ - 2, which equals 16,777,214.

**Class B Addresses**

In a class be network addresses, the primary two bytes are assigned to the network Addresses, and therefore, the remaining 2 bytes are used for host addresses. The format is as follows:

**Network.Network.Host.Host**

With a network address being two Bytes, we are left with 2¹⁶ unique combinations, but the web designers decided that each Class B network address should start with digit one, then 0. This leaves 14-bit positions available to control so. Wicked 16,384 unique class be network addresses. during a Class B network, the RFC state that the primary bit on the primary bite should be turned on, but the second bit always must be turned off if we turn the opposite six bits on all of them on we'll find the range for the category be Network:

10000000 = 128

10111111 = 191

As you'll see, a category B network is defined when the preceding byte is configured from 128 to 191.

**Class C Addresses**

The first octet of sophistication C IP addresses has its first 3 bits set to 110. Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for sophistication C is 255.255.255.x. Class C network addresses were for little organizations and used 3bytes for the Network and 1 byte for node addresses. Class C gives 2097152 (2²¹) Network addresses and 254 (2⁸-2) Host addresses. Class C IP address format is:

**Network.Network.Network.Host**

In a class C network address, the primary three-bit positions are always the binary the calculation is as follows:

Three bytes, or 24 bits, minus three reserve positions, leave 21 positions. Hence, there are 2²¹, or 20,97,152 possible C Class networks. The RFC defines the primary 2 bits of the primary update as always turned on for sophisticated C networks, but the third bit will never get on. Here's the range for a category C network:

11000000 = 192

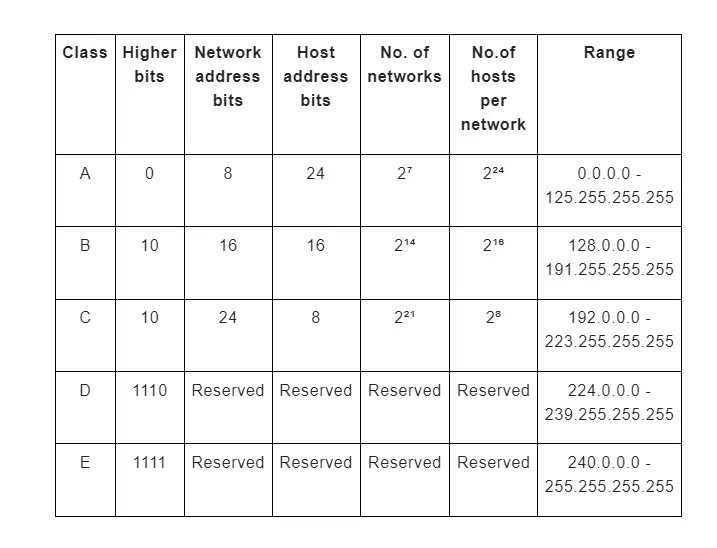
11011111 = 223

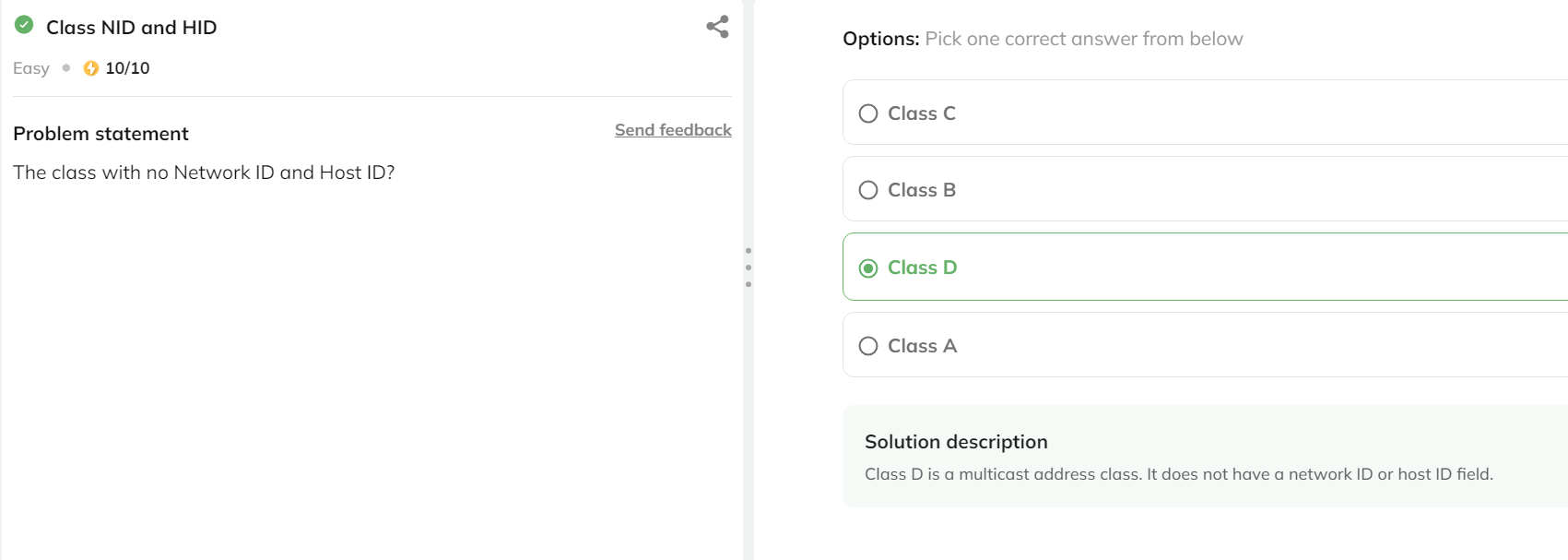
So if you see an IP address with a variety from 192 up to 223, you recognize it is a class C IP address. Each unique class C network has one byte to use for host addresses. This gets us to 2^8 or 256 minus the two reserved patterns for all zeros and ones for a complete of 254 available host addresses for every class C network. When deciding which network address class to use, you want to consider what percentage of local hosts there'll get on the Network and how many subnetworks will be within the organization. Therefore, if the organization is small and the Network will have fewer than 256 hosts, a category C address is perhaps sufficient. If the organization is large, then a category B or Class A address could be more appropriate.

**Class D and E Addresses**

Class D addresses are used for multicasting applications. Unlike the previous classes, this is often not used for "normal" networking operations. Class D addresses have their first three bits set to "1" and their fourth bit to "0". Class D addresses are 32-bit network addresses, meaning that each one of the values within the range of 224.0.0.0 – 239.255.255.255 are wont to identify multicast groups uniquely. There are no host addresses within the category D address space since all the hosts within a gaggle share the group's IP address for receiver purposes. Example for a category D IP address: **226.22.5.172.**

Class E networks are defined by having the primary four network address bits as 1. That encompasses addresses from 240.0.0.0 to 255.255.255.255. While this class is reserved, its usage was never defined. As a result, most network implementations discard these addresses as illegal or undefined. The exception is 255.255.255.255, which is employed as a broadcast address. For example, a category E IP address is **244.124.79.31.**





## ****Private IP Addresses****footer line

The local address of the home router is set to the default dedicated IP address number. This is usually the equivalent address of the opposite model from that manufacturer and is often seen in the manufacturer's documentation. Your public IP address is the IP address that someone at the other end of your Internet activity will see (if they bother to find it). This is the only reason it is called a public IP address. The web works similarly, except that it guides your activities (emails, answers to Google queries, etc.) and forwards the emails to your computer address. If there is no public IP address, there is nothing you can do. It is your pass to the Internet.

 In theory, your computer should have your unique IP address so that it only receives knowledge prepared for you. However, this is not how it works due to an important exception: computers on the network connect to the router and share an equivalent public IP address.

### ****Range of Private IP Address****

### 

The organization that distributes IP addresses to the earth reserves various IP addresses for personal networks. In your simple home network, the router is in the middle, the computer is wired or wirelessly connected to it, and these networks are clustered. Once an internet connection is established through your internet service provider, your router sends internet activity to any computer connected to your router, which is the basis of a network innovation called Network Address Translation. (NAT).

* NAT can be a process where your router changes your private IP address to a public IP address so that you can send your traffic across the network and track changes in the process.
* When this information is returned to your router, it will reverse the change from a valid IP address to a personal IP address and forward the traffic to your computer.

Your private address is only used for your router, your network, and you. The range of remote addresses on the web does not need to be in sync with the rest of the earth and therefore does not need to be in sync with the Internet. The private address range is generally used by one address. Network administrators who use these personal addresses have more subnet space and more addresses than those assigned. The private IP address does my job for your home network. A single network typically uses these address blocks. Even if your neighbor uses the same course, it will not cause a problem because that is your network, not yours. You see, these private addresses are called non-routable addresses. Networks on the web only route Internet activity to your public IP address, not your IP.

* Class A: 10.0.0.0 — 10.255.255.255
* Class B: 172.16.0.0 — 172.31.255.255
* Class C: 192.168.0.0 — 192.168.255.255

## ****Public IP Addresses****footer line

A public IP address is an IP address that can be accessed directly via the Web and assigned by your Internet Service Provider (ISP) to your network router. Your device also has a private IP; the IP remains hidden once it connects to the network through the router's public IP. Using a public IP address to connect to the Internet is like using a PO Box instead of providing your home address. It's a bit more secure but more noticeable. If the resource on your tenant is to be directly accessible from the network, it must have a public IP address. Depending on the type of resource, there may be other requirements. Certain types of resources in the lease are designed to be directly accessible from the Web and automatically include a public IP address. For example, NAT gateway or a general load balancer. What can now access other types of resources as long as they are configured? For example, the instance in your VCN.

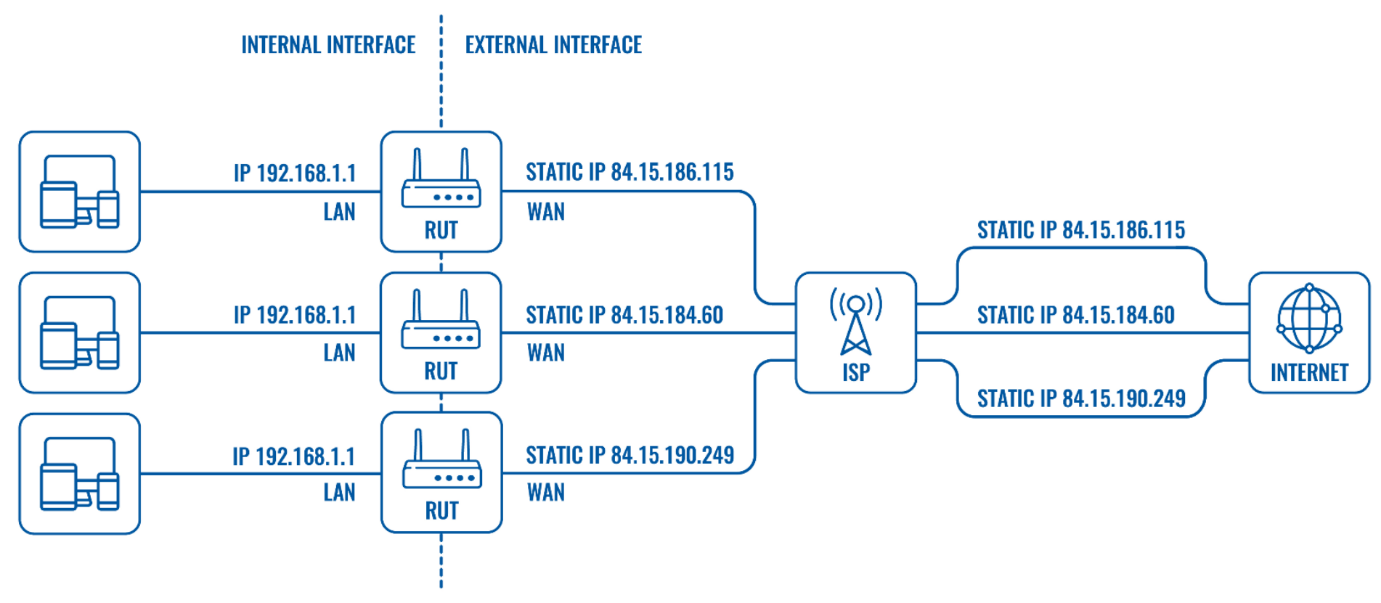
### ****Public IP Address****

The public (external) IP address is assigned to each device connected to the Web, and each IP address is unique. Therefore, it is impossible to have two devices with the same public IP address. This addressing scheme allows widgets to "search" and exchange information online. The user cannot control the (public) IP address assigned to the device. Since the device is connected to the network, the network service provider will transfer a public IP address to the machine as soon as possible. This usually doesn't seem right. Public IP addresses are generally static, dynamic, or shared.

### ****Static IP****

Public static is sometimes referred to as private, meaning that the IP address never changes and is linked to a user, device, server, or website. A web service provider provides unique and constant IP addresses for different routers (they never change for each device). In this case, the router performs the NAT process instead of the ISP, so when the router sends or receives data from a remote host on the Web, the ISP is "transparent."

Most users do not need a static IP address, but when external devices, websites, or users must remember their IP address for continued use, a static IP address is essential. For example, if you continuously need to access a tool remotely. Since the IP address never changes, you or other users only need to remember one IP address at any given time to be successful on the device.



### ****Shared IP****

### 

Shared IP in some cases, an ISP can assign a public IP address to a group of users and then use NAT to isolate their traffic. We all know that multiple devices (even websites) can share a public IP address. The ISP provides the customer with a private WAN IP address and then uses NAT to distinguish which host a particular packet should be directed to. However, shared IP has a massive disadvantage because the owner of the tool or website is no longer the only entity responsible for its IP address. For example, if one of the multiple users with the same IP address commits some cybercrime so that IP address is blocked, what will also block all users using that IP. You can find more information about Network Address Translation (NAT) here.

### ****Dynamic IP address****

A dynamic public network means that the IP address may change from time to time (for example, once you lose the connection and reconnect, the ISP may change the address periodically). We all know that in the case of a dynamic IP address, the ISP provides a private WAN IP address for the router and then "translates" it to a public IP address when connecting to a remote host on the Web. The most significant difference with a static IP address is that the dynamic IP provided by the ISP is not permanent. They will change when the router disconnects and reconnects, re-registers with the network operator, or in some cases, the ISP may periodically update the IP address. When it comes to remote access, dynamic IP complicates things because it is impossible to know the external IP address at any given time. Although the use of dynamic IP addresses for remote access is more complicated, it is not impossible; what can achieve it by using active DNS services (Service → Dynamic DNS). Naming services or DNS provide names for IP addresses (for example, www.google.com, www.facebook.com). Dynamic DNS will periodically rebind the IP address to the hostname. Therefore, when using dynamic DNS, you only need to remember the hostname to be successful on the selected device at any given time, although its IP address may change from time to time.

## ****Ping, DHCP Client Address****footer line

### ****DHCP Overview****

Statically assigning IP address information to individual networked devices is often time-consuming, error-prone, and lacking scalability. Rather than static IP address assignments, many corporate networks dynamically set IP address parameters to their devices. An early option for performing this automatic assignment of IP addresses was Bootstrap Protocol (BOOTP for short). However, the foremost popular approach for dynamic IP address assignment is Dynamic Host Configuration Protocol (DHCP). DHCP offers a more robust solution to IP address assignment than the answer provided by BOOTP. DHCP doesn't require a statically configured database of MAC address to IP address mappings. Also, DHCP features a wide variety of options beyond introductory IP address, subnet mask, and default gateway parameters. For instance, a DHCP server can educate a DHCP client about the IP address of a WINS server, or maybe an administrator-defined parameter (for example, the IP address of a TFTP server from which a configuration file might be downloaded). A protocol rendered obsolete by BOOTP and DHCP is Reverse Address Resolution Protocol (RARP).

### ****Ping Overview****

Ping may be a command-line utility available on virtually any OS with network connectivity that tests to ascertain if a networked device is reachable. The ping command sends an invitation over the network to a selected device. A successful ping leads to a response from the pc that was pinged back to the originating computer. A ping is employed to verify connectivity at an IP level to a second TCP/IP device. It does this by transmitting Internet Control Message Protocol (ICMP) Echo Request messages and waits for a return message. Unless modified, the ping command will send 4 requests by default in Windows. What percentage of responses get returned and the way long it takes for the round-trip provide essential information, such as:

* Bytes sent and received
* Packets sent, received, and lost
* Approximate round-trip time (in milliseconds)

The ping is initiated several times to check consistency within the connection. Here's what a successful ping request would return when connecting to a router. A Ping measures the time it takes for packets sent from the local host to a destination computer and back. The Ping tool measures and records the round-trip time of the package and any losses along the way. DomainTools' Ping service offers Ping information to display in a graphical and arranged manner available directly from the DomainTools website. This tool tests the essential connectivity of domains and IP addresses. Use this tool for troubleshooting purposes and to check response times.

## ****Subnetting****footer line

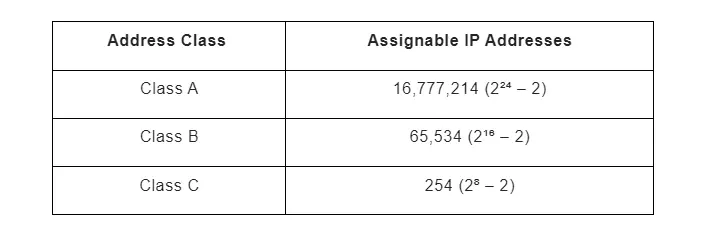
A  subnet or subnet can be a network within the network. Subnets make the web more efficient. Through subnetting, network traffic can be transmitted over a shorter distance without going through unnecessary routers to reach the destination successfully. Imagine that Alice mails a letter to Bob, who lives in a small town near her home. For Bob to receive the letter as soon as possible, it must be sent from Alice's post office to Bob's city post office, and then to Bob. If the letter were first sent to a post office a few miles away, it could take longer for Alice's letter to succeed Bob. Like mail, the network will be more efficient when the message is spread as directly as possible. When a network receives data packets from another web, it classifies and routes these data packets by subnet so that the data packets do not reach the destination through inefficient routes.

When the IP system was first introduced, it quickly became apparent that although it is now much easier to find the selected network, it is now also challenging to send the knowledge packet to the machine you want to be on the web. This becomes especially obvious when the network becomes large enough to support a business because network performance becomes more significant. Subnets help solve this problem by dividing the network into smaller parts, reducing congestion. The data packet is ready to flow to the destination and avoid human bottlenecks. For logical reasons (firewalls, etc.) or physical requirements (smaller broadcast domains, etc.), companies can use IP subnets to divide more extensive networks. In other words, routers use subnets to form routing options.

### ****The purpose of subnetting****

Consider the number of assignable IP addresses in the various IP address categories shown in Table 1. Remember that the host bits of an IP address cannot be all zeros (representing a network address) or all ones (representing a directed broadcast address). Therefore, the number of IP addresses that who can assign in a subnet is generally determined by the following formula, where h is the number of host bits during the subnet mask:

Number of IP addresses that can be assigned during the subnet = 2ʰ – 2,



Suppose you decide to use a class B private IP address (for example, 172.16.0.0/16) as your internal IP address. For performance reasons, you may not want to support up to 65,534 hosts in a single broadcast domain. Therefore, the best practice is to use this network address and subnet the network (thus expanding the number of network bits in the network subnet mask) to other subnets.

Calculate the number of subnets created

To determine the number of subnets created by adding bits to the classful mask, you can use the following formula, where s is the number of bits rendered:

Number of subnets made = 2ˢ

For example, Suppose you use a 28-bit subnet mask to subnet the 192.168.1.0 network, and you want to calculate the percentage of subnets created. First, determine the percentage of borrowed bits that you have acquired. Remember that the number of bits rendered is the number of bits that exceed the classful mask during the subnet mask. In this case, because the value of the leading octet in the network address is 192, you will conclude that this is usually a class C network. Also, as you may recall, a class C network has 24 bits in its subnet mask with class (that is, default). Because you now have a 28-bit subnet mask, the number of rendered bits is generally calculated as follows:

number of borrowed bits = bits in a custom subnet mask-bits in a classful subnet mask

 number Borrowed bits = 28 - 24 = 4

Now, if you only know you have four borrowed places, you will increase the install from 2 to 4 (2⁴, or 2 \* 2 \* 2 \* 2), which equals 16. Based on this calculation, you can conclude that dividing into 192.168.1.0/24 subnets with a 28-bit subnet mask results in 16 subnets.

Calculate the number of obtainable hosts

Suppose you want to calculate the number of available hosts IP addresses in one of the 192.168.1.0/28 subnets. First, you need to calculate the number of host bits in the subnet mask. Since it recognizes that the IPv4 address consists of 32 bits, it will subtract the number of bits in the subnet mask (28 in this example) from 32 to calculate the number of host bits:

host bits = 32-host bits Count the number of bits in the subnet mask

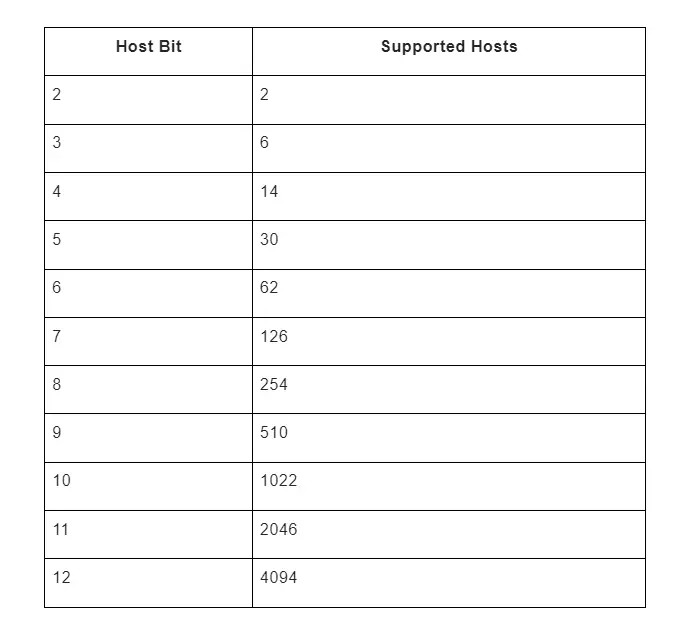
number of bits in the host = 32-28 = 4

Now you only know the number of host bits. You will apply it to the above formula, where h is the number of host bits in the subnet mask:

The number of IP addresses that can be allocated in the subnet = 2ʰ-2

The number of IP addresses that can be allocated in the subnet = 24-2 = 16-2 = 14

Through this calculation, you will conclude that 192,168.1.0 / 28 Each of these subnets has 14 available IP addresses.



### ****Figuring New IP Address Ranges****

Since you basically can figure the number of subnets made upheld a given number of acquired pieces, the ensuing coherent advance is to compute the IP address ranges making up those subnets. for instance, on the off chance that you took the 172.25.0.0/16 and subnetted it with a 24-bit subnet veil, the subsequent subnets would be as per the following:

172.25.0.0/24

172.25.1.0/24

172.25.2.0/24

...

172.25.255.0/24

Let’s consider how such a calculation is performed. Notice in the previous example that you count by 1 in the third octet to calculate the new networks. To determine in what octet you start counting and by want increment you count, a new term needs to be defined. The interesting octet is the octet containing the last 1 in the subnet mask.

Example:

A 27-bit subnet veil is applied to an organization address of 192.168.10.0/24. To compute the made subnets, you'll play out the ensuing advances:

1. The subnet cover (in parallel) is 11111111.11111111.11111111.11100000. The intriguing octet is the fourth octet on the grounds that the fourth octet contains the final remaining one inside the subnet.
2. The decimal worth of the fourth octet inside the subnet veil is 224 (11100000 in decimal). Along these lines, the square size is 32 (256 – 224 = 32).
3. The first subnet is 192.168.10.0/27 (the worth of the principal 192.168.10.0 organization with the acquired pieces [the initial three pieces inside the fourth octet] set to 0).
4. Tallying by 32 inside the intriguing octet (the fourth octet) permits you to ascertain the excess subnets:

192.168.10.0

192.168.10.32

192.168.10.64

192.168.10.96

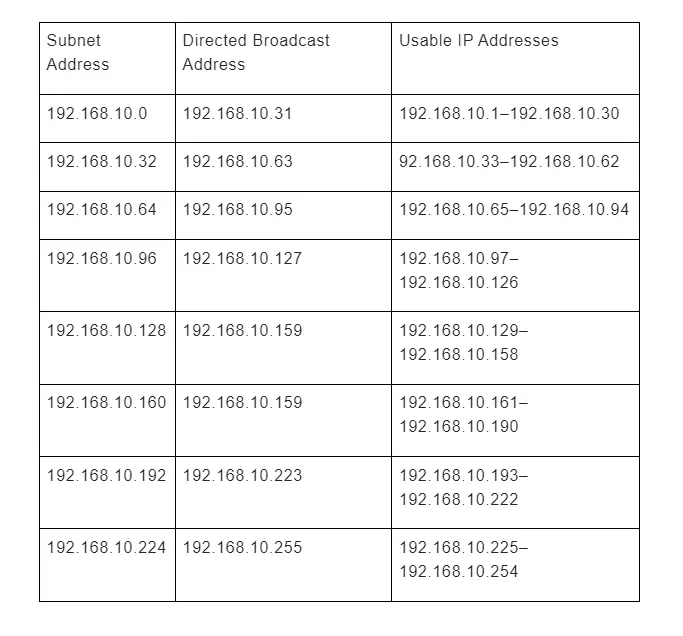
192.168.10.128

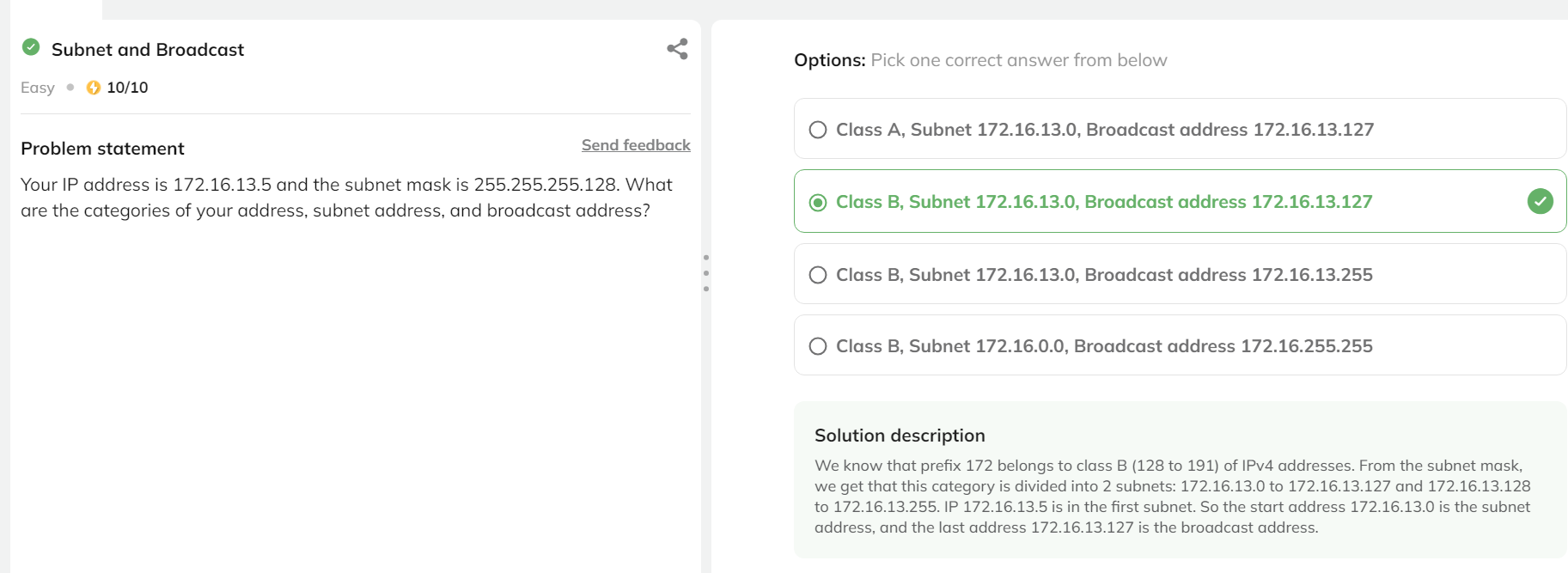
192.168.10.160

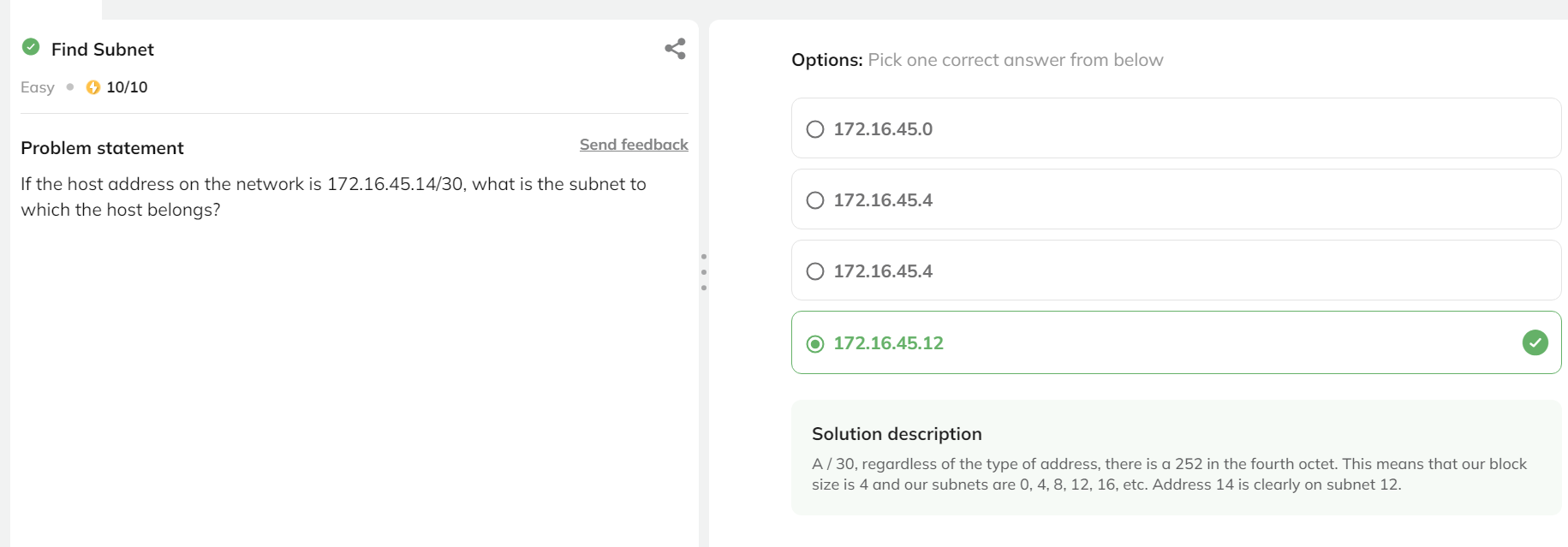
192.168.10.192

192.168.10.224

Since you know the subnets made from a classful organization given a subnet cover, an ensuing consistent advance is to work out the usable addresses inside those subnets. Review that you can't dole out an IP address to a device if all the host bits inside the IP address are set to 0 on the grounds that an IP address with all host bits set to 0 is that the location of the subnet itself. Also, you can't appoint an IP address to a device if all the host bits inside the IP address are set to 1 on the grounds that an IP address with all host bits set to 1 is the coordinated transmission address of a subnet. By barring the organization and coordinated transmission addresses from the 192.168.10.0/27 subnets (as recently determined), the usable addresses are displayed in Table 3 not really settled.







## ****Supernetting****footer line

Supernetting is to add a network to create a more extensive network (supernet or supernet). Let us consider the basic definition of an IP (network) address: it consists of a network part and a host ID. For subnetting, we "borrow" bits from the host ID to create a smaller network. In contrast, we extract bits from the network part for supernets to develop a more extensive network. Supernets are usually used to route advertisements. However, it has other uses, such as building access control lists (ACLs), combining multiple static routes into one, etc.

Supernetting is mainly used for route summarization, combining the routes of multiple networks with similar network prefixes into one routing entry. The routing entry points to an excellent network that spans all networks. This continuously significantly reduces the dimensionality of the routing table and the metric of routing updates exchanged by the routing protocol. Combine multiple IP network addresses into one IP address. Supernetting minimizes the number of routing table entries in CIDR, which also targets the internal network.

### ****The purpose of Supernetting****

The primary purpose of the supernet is to reduce the dimension of the routing table in the router. For example, instead of having eight separate routes (pointing to the equivalent next hop), a router can have an aggregate way of eight independent ways. This is usually important for the following reasons:

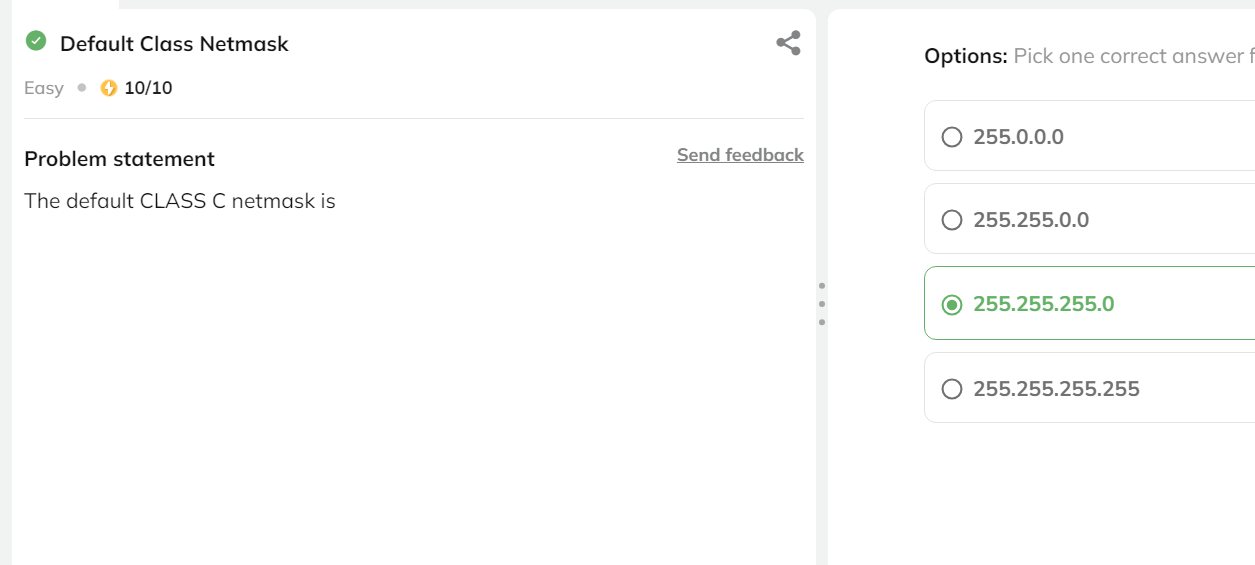
* It can save memory and processing resources on the routing device. They have little storage space for routing tables, and their throughput to view routing tables is also low.
* Provides network stability because fluctuations in a specific part of the network will not extend to all or any aspect of the web. That is, the changes are usually isolated.

In addition to the benefits of the routing table, it also helps prevent IP address depletion through classless inter-domain routing (CIDR). Basically, instead of distributing the Class B network to everyone who needs the equivalent of a Class C network, you can now use variable-length prefixes (like / 19, / 21, etc.) to add these Class C networks as efficiently as possible. Finally, you will use supernets to expand the number of addresses available on the network. For example, you would add four / 24 networks (each with 254 public IP addresses) to create a / 22 network (with 1022 available IP addresses).

### ****Rules of Supernetting****

Supernet rules are the same as subnetting. Super grids are counted in the order of 2, 2, 4, 8, 16, etc.; Once you create a supernet, you want to make sure it only covers what you want to add network, not less. Less is better, so avoid routing problems.

* Make sure the network is continuous (defined as "adjacent or together in order").
* Determine the number of networks to be added and make sure the number is two.
* The value of the leading non-public octet in the first (lowest) IP address block in the list of networks to be added is compared to the number of networks to be added (plus the order of 2). The value of the non-public leading octet must be A multiple of the number of networks to be aggregated. For example, 16 is a multiple of 8 but 8 is not a multiple of 16.

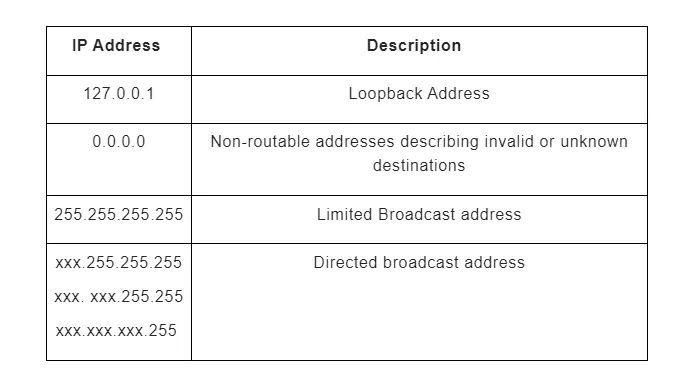


## Interview Questionsfooter line

IPV4 Addressing

**Q1.** What are the different particular IP addresses? **(Cisco)**

**Answer:** Below are multiple unique IP addresses and Their roles:



**Q2.** What is a private IP? What is the range set for  private IP? **(Dell)**

**Answer:**A dedicated IP address is a series of non-Internet IP addresses used on the internal network. Private IP addresses are provided by network devices (such as routers) through network address translation. The range for private IP addresses are:

Class A: 10.0.0.0 — 10.255.255.255

Class B: 172.16.0.0 — 172.31.255.255

Class C: 192.168.0.0 — 192.168.255.255

**Q3.** How is Public IP different from private IP? Can we access other networks Using their public IP? **(Cisco)**

**Answer:**Your private IP address exists in the specified remote IP address range reserved by the Internet Assigned Numbers Authority and should not appear on the Internet. There are millions of private networks globally, and all of these networks contain devices assigned personal IP addresses within these ranges. Yes, that is how the Internet works; we access other systems using their public IPs.

**Q4.**What is Ping utility? What protocol does ping work on and on which layer of the OSI model? **(Arista)**

**Answer:** Ping is a command-line utility used on almost any operating system with a network connection to test whether it can access networked devices. The ping command sends a request to a specific device over the network. A successful ping will cause the computer to ping the original computer to respond. Ping works using ICMP protocol and works on layer 3.

**Q5.**What is the Process of DHCP? How does it work?

**Answer:**Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automatically configure devices on an IP network, allowing them to use network services, such as DNS, NTP, and any communication protocol based on UDP or TCP. The DHCP server dynamically assigns IP addresses and other network configuration parameters to each device on the network to communicate with other IP networks.

The following factors can measure the reliability of a network:

* **Discover:**The client discovers DHCP
* **Offers:**The DHCP server provides a set of IPs for the client to choose any
* **Request:**The client selects an IP and asks for a DHCP confirmation
* **Acknowledgment:**The DHCP server sends a DHCP ACK execution confirmation to the client.

**Q6.**Your router has the following IP address on Ethernet0: 172.16.2.1/23. Which of the following can be a valid host ID on the LAN interface connected to the router? **(Wipro)**

**Answer:** 172.16.2.255. The IP address of the E0 interface router is 172.16.2.1/23, which is 255.255.254.0. This makes the block size of the third octet 2. The router interface is on subnet 2.0, and the broadcast address is 3.255 because the next subnet is 4.0. The valid host range is 2.1 to 3.254. The router is using the first valid host address in the content.

**Q7.**What is the maximum number of IP addresses assigned to a host on the local subnet using a subnet mask of 255.255.255.224?**(TCS)**

**Answer:** 30. A / 27 (255.255.255.224) has 3 bits on and 5 bits off. This provides eight subnets, each with 30 hosts. Is it essential to use this mask with class A, B, or C network addresses? Not at all. The number of host bits will never change.

**Q8.**How many subnets and hosts do the network address 172.16.0.0/19 provide? **(Infosys)**

**Answer:** 8 subnets, 8,190 hosts each. The CIDR address of /19 is 255.255.224.0. This is a Class B address, so it has only three subnet bits, but it provides 13 host bits or eight subnets, each with 8,190 hosts.