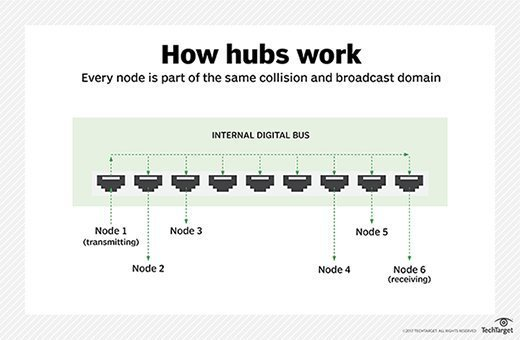
**LEVEL TWO ASSESSMENT DevOps TRAINING**

1. **Describe Hub, Switch and Router**

Hub

This splits the network connection into multiple computers.It is a networking device that enables multiple devices or connections to connect to a single network. It has a lot of ports in it and a computer which intends to be connected to the network is plugged into one of these ports. When a data frame arrives at a port, it broadcasts it to every port without considering its particular destination or not.. It is an unintelligent hardware device. It passes along data or traffic received from one computer to the other computers in the network.Hubs are basic devices and has no need for an IP Address. According to Jessica Scarpati of SearchNetworking, they are called “dumb switches”.

Apart from security and privacy issues as regards all ports receiving the traffic from one computer, there is also the issue of the collision domain which can cause network performance problems.



There are two types of hubs;

|  |  |
| --- | --- |
| Active Hub | Passive Hub |
| It is a hub with its own power supply | It collects power supply from the active hub and wiring from nodes. |
| It can clean, improve and relay the signal along with the network | They relay signals into network without cleaning and boosting them |
| It works as a repeater as well as a wiring center | It does not work as a repeater |
| It can be used as an extension for two or more nodes | It can’t be used to extend the distance between nodes. |

Switch

A switch is a hardware device that centralizes communications among various linked devices in one local area network(LAN).A switch is a data link layer networking device which connects devices in a network and is used to send and receive packet data over the network.

Like a hub, a switch also has many ports, to which computers are plugged in. However, when a data frame arrives at any port of a network switch, it examines the destination address, records it and sends the frame to the corresponding device(s). Thus, it supports both unicast and multicast communications. Most devices connect to the switch using ethernet cables They can also operate at the network layer--Layer 3 where routing occurs.

There are two main types of switches

1. Unmanaged Switches; It has little brain power as everything is automatic.
2. Managed switches; This allows you to make changes to the settings of the switch and make changes. It is scalable which entitles network room to grow.

Router.

It is the most intelligent of the three hardware devices. It is a networking device designed specifically to understand, manipulate and direct traffic. It has a user interface so where to direct the traffic can be told to the router. It connects multiple switches and their respective networks and forms a bigger network. These networks may be in a single location or across multiple locations. It also allows networked devices and multiple users access the internet. The wouter works as a dispatcher, directing and choosing the most efficient route for data packets to travel across a network and protects information from security threats.

**2. What is the OSI Model**

A reference model that allows for specification of standard of communication. It is a model with seven layers that the computer systems use to communicate over a network and describe the functions of a networking system. It was the first standard model for network communications when it was first conceived around the early 1980s until the modern internet turned to a different modern. The Open Systems Interconnection helps to visualise and communicate how networks operate and helps isolate and troubleshoot networking problems. OSI divides the whole task into seven smaller tasks and each layer takes one. In some ways the OSI model is the universal language of computer networking.

**3. Explain the different types of OSI Models**

Each of the seven layers are self-contained and each layer can perform its tasks independently. The layers give a visual description of what is going on in a particular networking system.

7. Application Layer

6. Presentation

5.Session

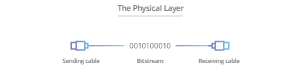
4.Transport

3.Network

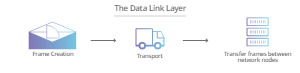
2.Data Link

1.Physical layer

1. Physical Layer; This represents the electrical and physical representation of the system. The lowest layer of the OSI model is concerned with transmitting raw, unstructured data over the physical medium. The physical equipment in this layer is what is involved in the data transfer such as the cables and switches. This is the layer where the data is converted into bits stream, a string of 1s and 0s. At this layer, physical resources such as network hubs, repeaters, modem e.t.c can be found.



1. Data Link; The second layer of the OSI model takes packets from the network layer and breaks them into smaller pieces called frames. It is responsible for flow control and error control in intra network communication. It provides node-to-node transfer where data is packaged into frames. This layer has its own two sublayers; Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.



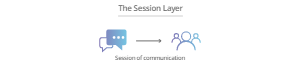
1. Network layer; It is responsible for facilitating data transfer between two different networks. If two devices communicating are on the same network, then the network layer is unnecessary. The network layer has two main functions; One is breaking up segments into smaller units called network packets and reassembling the packets on the receiving device. Two, it also finds the best physical path for the data(packets) to reach its destination, this is called routing. The network layer uses network addresses(usually Internet Protocol address(IP) to route packets to destination nodes.



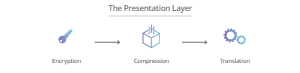
1. Transport layer; This is responsible for end-to-end communication between the two devices. It manages the delivery and error checking of data packets. It takes data from the session layer and breaks into segments before transferring to the network layer. It is responsible for reassembling the segments into data that the network layer can consume. It is also responsible for flow control(providing an optimal speed transmission so data can be sent at a rate that matches the connection speed of the receiving device) and error control(ensuring data received is complete and correct and if not requesting a retransmission). The TCP is a perfect example of the transport layer.



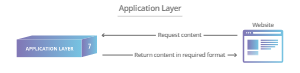
1. Session layer; This controls the conversations between different computers. It creates communication channels called sessions, between devices. It opens and closes the sessions. The time between when the session is opened and when it is closed is called the session. Sessions are created when computers need to speak to each other. The session layer ensures the sessions remain open and functional while data is being transferred, and closes them when communication ends. The session layer also sets checkpoints during a data transfer and if the session is interrupted, devices can resume data transfer from the last checkpoint.



1. Presentation layer; This layer prepares data for both the application layer and the session layer. It defines how two devices should encode, encrypt and compress data so it is received correctly on the other end.Two communicating devices communicating may be using different encoding methods which makes this layer responsible for translating incoming data into a syntax that the application layer of the receiving device can understand. It is also responsible for compressing data it receives from the application layer before delivering it to the session layer.



1. Application Layer; This is the layer at the top. This is the layer end users interact with. It receives information directly from users and displays incoming data to the user. Applications themselves do not reside at the application layer rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user. Examples of application protocols include HTTP, SMTP(Simple Mail Transfer Protocol) and DNS(Domain Name System) e.t.c.



**4. What do you mean by TCP/IP Model?**

This is a concise version of the OSI model. It stands for Transmission Control Protocol and Internet Protocol. This helps to determine how a specific computer should be connected to the internet and how data should be transmitted. It also creates virtual networks when multiple computers are connected together. This model also allows for communication over large distances. It is also a very highly reliable model.

The TCP/IP model has four layers;

1. Application layer; which is at the top, allows access to network resources.
2. Transport layer; which provides reliable process to process message delivery and error delivery.
3. Internet layer; this layer moves packets from source to destination and provides internet working.
4. Network Interface; this layer is responsible for transmission of data between two device on the same network.

**5. What do you mean by HTTP, TCP and UDP.**

HTTP; This is located at layer 7 of the OSI model. HTTP is often called the protocol of the Internet, because most Internet traffic is based on HTTP. When a user requests a Web resource, it is requested using HTTP. It is called the HyperText Transfer Protocol. HTTP contains specific instructions on how to read and process this data once it arrives. Before data is sent from one node on the Internet to another, it gets wrapped in information detailing the nature of the request being sent, or the response to said request. When you type a URL into your web browser, you are sending an HTTP request to a web server. That server will then respond, again using the formatting of HTTP. HTTP describes what the data in the stream contains.

TCP; This is located at layer 4 of the OSI model. TCP manages the data stream. Whenever packets of data are sent or received there are hosts of information that goes along with it. TCP is what adds the information to the data.TCP's job is to ensure that all data sent in a stream moves from Point A to Point B intactly and in correct order. Protocols like TCP tell the destination computer which application should receive said data. TCP in particular sacrifices raw speed to ensure reliability in the data being transmitted.

UDP; This is also a form of protocol like TCP. It is a datagram oriented protocol. It sacrifices accuracy for speed.It is used for broadcast and multicast type of network connection. it does not guarantee the delivery of the transport layer segments, it doesn’t check to see if the segments were received by the destination. It is unreliable unlike the TCP.

**6. What is a firewall?**

According to CISCO; A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. It establishes a barrier between your internal network and incoming traffic from external sources like the internet, in order to block malicious traffic like viruses and hackers. . Firewalls guard traffic at a computer’s entry point, called ports, which is where information is exchanged with external devices. Firewalls can either be software or hardware

There are various types of firewalls;

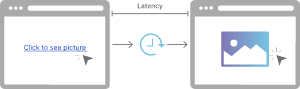
1. Proxy firewall
2. Stateful inspection firewall
3. Unified threat management firewall
4. Next generation Firewall
5. Threat focused firewall
6. Virtual firewall

**7. Explain DNS**

DNS is the short form of Domain Name Server is a server that translates URL and web addresses to their corresponding IP addresses and allows browsers to load internet resources. According to Cloudflare, it is the phonebook of the internet. DNS eliminates the need for humans to memorise IP addresses. The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device. The request made by the computer to find an IP address is made to the recursive domain server while the authoritative domain servers are usually the ones with the IP addresses that are being searched for.

**8. Define Latency**

Latency is a measure of delay. Latency is the time that passes between a user’s action and the resulting response to the action. In networking terms as the total round trip time it takes for a data packet to travel. It is often measured in milliseconds.



“Although data on the Internet travels at the speed of light, the effects of distance and delays caused by internet infrastructure equipment mean that latency can never be eliminated completely. It can and should, however, be minimized” (Cloudfare)

**9. Define Caching**

A cache is a high-speed data storage layer which stores a subset of data, typically temporary in nature. Caching is the process of storing copies of files in a cache, or temporary storage location, so that they can be accessed more quickly. When we visit a web page for the first time, it takes a while to load and most of the content that appeared on the browser is cached, saving it on the device’s hard drive so the next time we visit that page, it loads faster as most of the content was already saved. If one clears her browser cache, the saved content deletes and when visiting the page again, the page loads anew.

E.g Web browsers cache HTML files, JavaScript, and images in order to load websites more quickly, while DNS servers cache DNS records for faster lookups and CDN servers cache content to reduce latency.

**10. Explain Wireless Access Point**

Wireless Access Point (WAP), allows wireless devices to connect to the network with no cable.It is a networking hardware device that allows other wireless devices to connect to a wired network. It can also be a configured node on a Local Area Network.

There are four standards of WAP;

1. 802.11 A, very good standard but then flopped. It is not compatible with any of the other standards
2. 802.11 B, 11mb per second.
3. 802.11 G, 54mb per second. A lot more stable B and G wireless cards are compatible.
4. 802.11N there was a pre N before the standard N arrived. The pre N device would have problems because it was more of a draft. It allows for a much larger area. A lot faster, at least two times faster than g. It allows for real time video and voice communication. B, G and N are compatible with each other.