AWS Cloud Support Engineer Interview Questions:-

###basics Linux fundamentals

like system calls , strace , linux manage memory, shared memory, kernel using, boot process, DNS resolving ( how to resolve name to IP or what happen when you vist amazon.com), basics commands

###network basics like TCP/IP model,

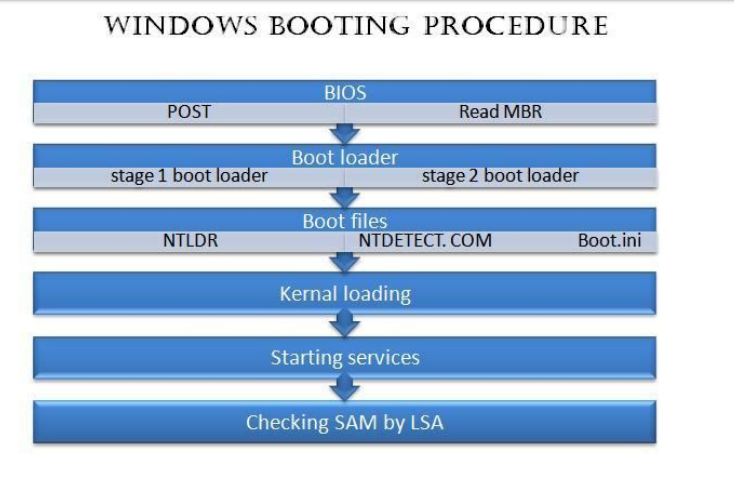
###tcpdump,

###tcp 3 ways hand check,

### ping ,telnet, , network basics like TCP/IP model tcpdump tcp 3 ways hand check ping telnet and most network fundamentals

###What do you know about AWS tools? Do you use it?

##Windows Booting Process?



a) POST - POST stands for Power On Self Test. POST checks all the hardware devices connected to a computer like RAM, hard disk etc

and make sure that the system can run smoothly with those hardware devices. If the POST is a failure the system halts with a beep sound.

b) Now BIOS checks the boot priority. We can set the boot priority as CD drive, hard disk or floppy drive.

c) MBR - The next duty of BIOS is to read the MBR. MBR stands for Master Boot Record and its the first sector on a hard disk. MBR

contains the partition table and boot loader.

Functions of Boot loader

Now BIOS has passed the control to boot loader and boot loader is a small program which loads kernel to computers memory. Actually

there are two stages of boot loaders, stage 1 boot loader and stage 2 boot loader. MBR contains the stage 1 boot loader and stage 1 boot loader is a link to the stage 2 boot loader. The stage 2 boot loader resides in the boot partition and it loads the kernel to memory.

Boot files and functions

Several steps like POST, boot files loading, MBR reading, Kernel initialization etc are

happening during the booting procedure of a Windows machine.

There are three boot files in a Windows operating system and they are NTLDR, NTDETECT.COM and Boot.ini. The boot files are found in

the active partition of hard disk and its normally C drive in a Windows machine.

NTLDR - NTLDR stands for NT Loader and its the second stage bootloader. The path of NTLDR is C:\Windows\i386\NTLDR.

Boot.ini - Boot.ini contains the configuration files of NTLDR. When the operating system is loaded we cannot pass any arguments to

kernal, so those arguments are passed through boot.ini. You can edit boot.ini by opening through notepad. The path of Boot.ini is

C:\boot.ini.

NTDETECT.COM - This file detect hardware's and passes information to NTLDR. Using the collected information the NTLDR creates a

hardware key and this key is used to detect hardware's. A new hardware key is generated after each reboot of the operating system and that's why system asks to reboot after installation of a new hardware. The hardware keys created by NTLDR can be found in Windows registry at

HKEY\_LOCAL\_MACHINE -> HARDWARES.

Kernel and its functions

After executing the functions of boot files the control is passed to Kernel. ntoskrnal.exe is the kernel file in a Windows machine and its path

is C:\Windows\system 32\ntoskrnal.exe. Kernel acts as a layer between software and hardware. The library file hal.dll

(C;\Windows\system32\hal.dll) helps Kernel to interact with hardware's. HAL stands for Hardware Abstraction Layer and this hal.dll file is machine specific. Now the drivers for hardware's are loaded from the file C:\Windows\system32\config\system and the Kernel is loaded to primary memory.

Services and log in procedure

When kernel is loaded in the primary memory services for each process is started and the registry entry for those services can be found at HKEY\_LOCAL\_MACHINE - System - Current control set - Services.

Winlogon.exe (C:\Windows\system32\winlogon.exe) is the last

service started during this process. Winlogon.exe starts the log in procedures of windows machine. It first calls the library file msgina.dll

(C:\Windows\system32\msgina.dll). MSGINA stands for Microsoft Graphics Identification and Authentication and it provides the log in

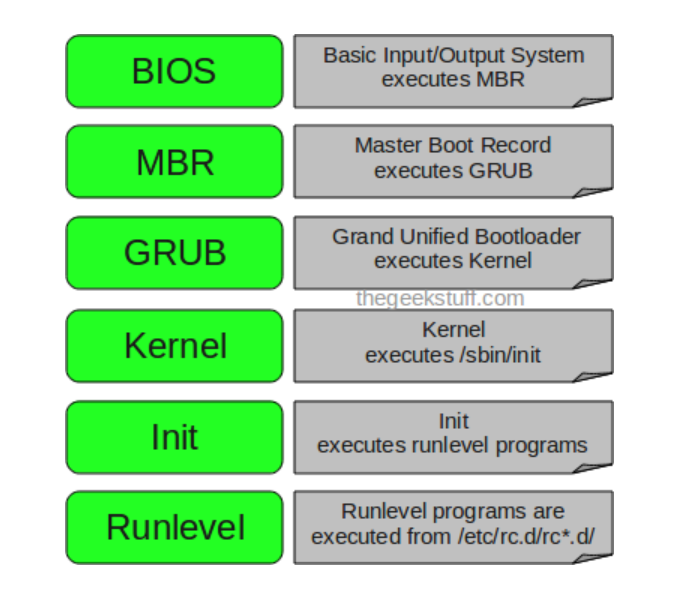
window. Now msginal.dll passes the control to LSA (Local Security Authority), it verifies the username and password from the SAM file.

SAM (Security Accounts Manager) contains the information about all users created in a Windows operating system.

Now the booting procedure is over and we have reached the desktop of Windows operating system.

### Linux booting Process?

https://www.thegeekstuff.com/2011/02/linux-boot-process/



##Windows BSOD error troubleshooting?

##Moderate level Pattern printing coding question.

##DNS? Subnet qs with numerical type ? DHCP? Routers?Switches?Gateways?

##Virtual Memory?Thrashing?

##Networking, troubleshooting, operating system

##main questions on linux and networking

##LINUX commands and have a brief knowledge of all OSI layers.

<https://maker.pro/linux/tutorial/basic-linux-commands-for-beginners>

Linux : how to kill a process , what does ls -l or -a do

Kill pid

Ls -l or -a (https://linoxide.com/linux-command/20-ls-command-linux/)

##windows : what does task manager do and whats on it --- check process, monitor performance

##TCP VS UDP

|  |  |
| --- | --- |
| **TRANSMISSION CONTROL PROTOCOL (TCP)** | **USER DATAGRAM PROTOCOL (UDP)** |
| TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data. | UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission. |
| TCP is reliable as it guarantees delivery of data to the destination router. | The delivery of data to the destination cannot be guaranteed in UDP. |
| TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data. | UDP has only the basic error checking mechanism using checksums. |
| Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver. | There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer. |
| TCP is comparatively slower than UDP. | UDP is faster, simpler and more efficient than TCP. |
| Retransmission of lost packets is possible in TCP, but not in UDP. | There is no retransmission of lost packets in User Datagram Protocol (UDP). |
| TCP has a (20-80) bytes variable length header. | UDP has a 8 bytes fixed length header. |
| TCP is heavy-weight. | UDP is lightweight. |
|  |  |
| TCP doesn’t supports Broadcasting. | UDP supports Broadcasting. |
| TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet. | UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP. |

##OSI model

##Tell me about AWS what do you know

##Behavior : have you ever had a problem and how did you solve it

#####

1. What command checks for running processes?

Ps -aux | less

Ps - u username (specific user process)

Ps -U root -u root -N/--deselect ( all processes except for root user)

2. What is TCP and UDP?

TCP - Transmission control protocol ( slow, but reliable, retransmission, data packets sent in sequence)

UDP - User datagram protocol (fast, used for multicast or broadcast, not reliable, used for DNS, gaming stream)

3. You said that in TCP, connection is established, how is this done?

Prerequisites for establishing a valid TCP connection: Both endpoints must already have a unique IP address (IPv4 or IPv6) and have assigned and enabled the desired port for data transfer. The IP address serves as an identifier, whereas the port allows the operating system to assign connections to the specific client and server applications

#####

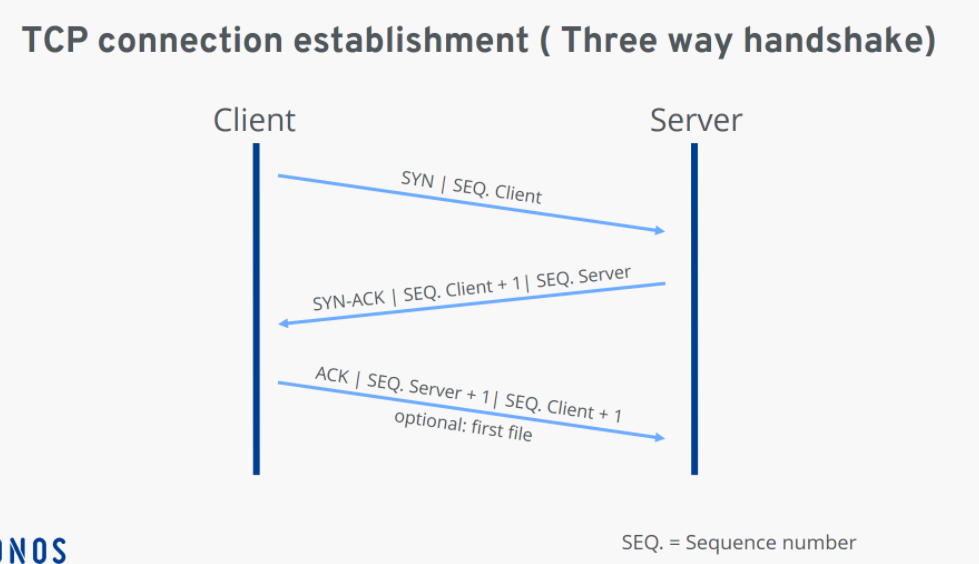
### TCH 3-way handshake

The actual process for establishing a connection with the TCP protocol is as follows:

First, the requesting client sends the server a SYN packet or segment (SYN stands for synchronize) with a unique, random number. This number ensures full transmission in the correct order (without duplicates).

If the server has received the segment, it agrees to the connection by returning a SYN-ACK packet (ACK stands for acknowledgment) including the client's sequence number plus 1. It also transmits its own sequence number to the client.

Finally, the client acknowledges the receipt of the SYN-ACK segment by sending its own ACK packet, which in this case contains the server's sequence number plus 1. At the same time, the client can already begin transferring data to the server.



4. What command shows the hops between two networks?

Traceroute(linux) / Tracert (windows)

5. How does traceroute command obtain these hops?

Before running a traceroute command, you should understand a network mechanism called “time to live” (TTL). TTL limits how long data can “live” in an IP network. Every packet of data is assigned a TTL value. Every time a data packet reaches a hop, the TTL value is decreased by one.

Another key element to understand is “round-trip time” (RTT). Traceroute ensures each hop on the way to a destination device drops a packet and sends back an ICMP error message. This means traceroute can measure the duration of time between when the data is sent and when the ICMP message is received back for each hop—giving you the RTT value for each hop.

6. What is MTU?

Maximum transmission unit -- max size of data you can sent on your connections. People may experience loss of data package when setting large MTU

7. What command checks for open ports?

ss -to display all TCP and UDP open ports

ss -tl ( -t tcp port -l list)

Ss -lu ( u for udp)

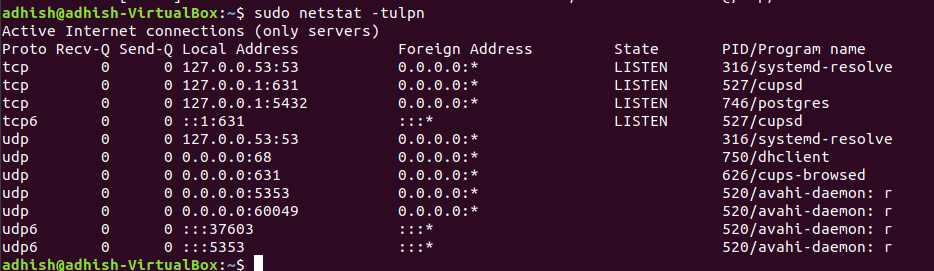
netstat -- all ports in linux

lsof - i (network command to check open ports)

lsof -i tcp ( all tcp connections)

lsof -i udp (all udp connections)

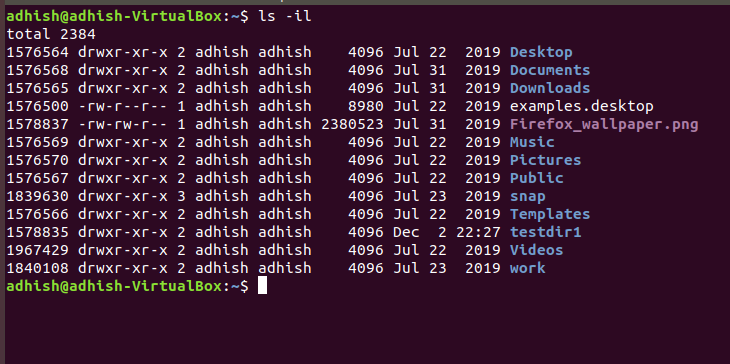
nestat -tulpn (tcp,udp, listening server pockets,process number,don’t resolve names, service running on specific port)



8. What does the inode command do?

inode(index node) command -it stores information about all regular file/directory.

Use ls -li or stats filename or stats /etc/pwd



9. How do you edit the file descriptor?

# sysctl -w fs.file-max=100000

10. How do you open files of a specific process?

(https://www.thegeekstuff.com/2012/08/lsof-command-examples/)

11. What command checks the routing table in Linux?

# Ip route list

# netstat -rn

# sudo route -n

12. Which directory are log files stored?

# /var/log

13. Which directory are third party software stored?

# /usr/opt

14. What is DNS?

#Domain name system -- it is used to translate domain name to ip addresses

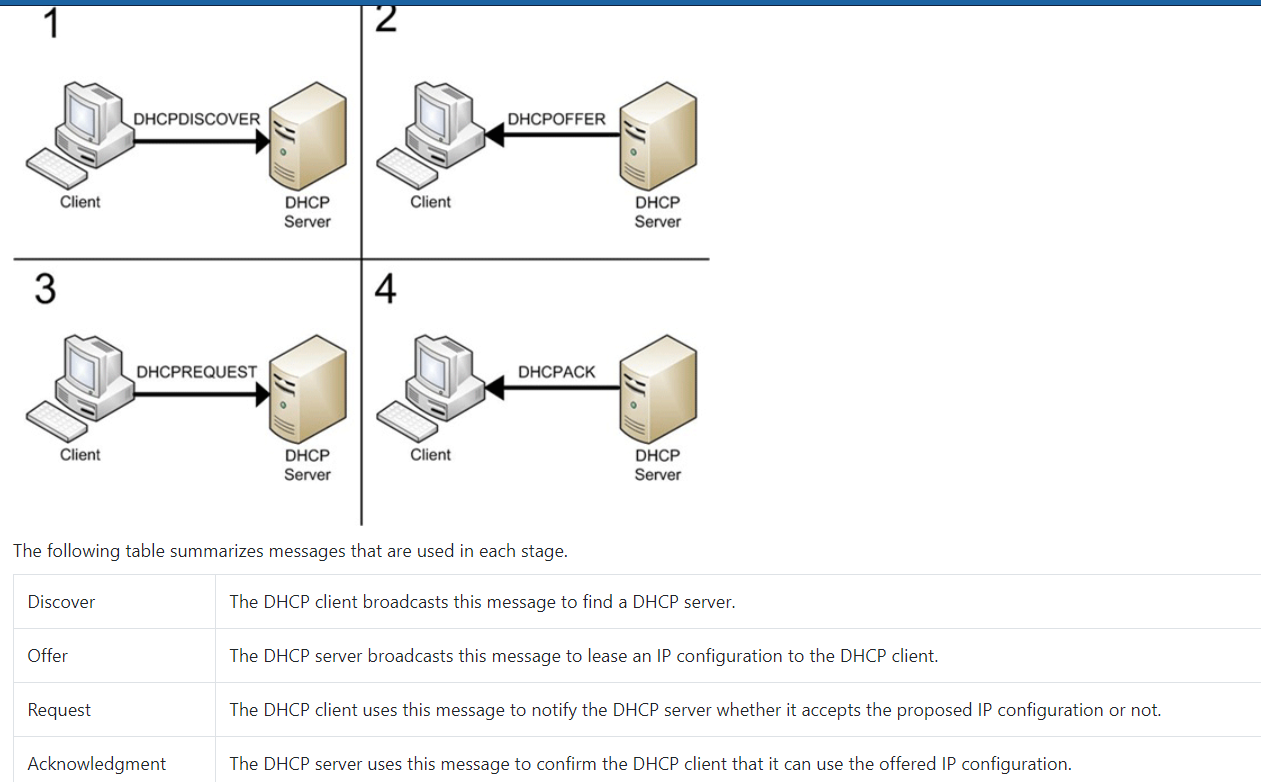
15. Tell me about the DNS process. (The entire technical process)

# https://www.cloudflare.com/learning/dns/what-is-dns/

16. What is DHCP.

# Dynamic Host configuration protocol -- It automatically applies IP addresses to the devices on the network

17. Tell me about the DHCP process. (The entire technical process)



18. Tell me examples of TCP.

# Web, SMTP, telnet, FTP

19. Tell me examples of UDP.

(or :- what is the difference about UDP and TCP, what kind of application base on UDP

what is FTP? what kind of application it used for?)

# media streaming, game streaming ,DNS Query, tunneling/VPN

20. What command checks port connection?

# telnet servername port ( only for TCP)

# netstat -an

# lsof -i:<port number>

##Virtual memory

##How ip address are allocated

using DHCP

##Osi layers

##What is virtual memory?

##Difference between process and thread?

Process is a program in execution while thread is a segment of process. Process can have multiple threads

##Difference between buffer and cache?

##buffer is a temp storage area which usually in memory block which are used to place data before transferring from input or / output device. Cache is a fast memory which is place between cpu and memory. It is used for holding frequently access data page or query.

##Ways to swap without using temporary variable

##where are the USB drivers installed in Linux. --- > libusb ??

##Describe DHCP DORA, Entire OSI stack, In depth DNS and DHCP, Wireshark process, ARP, HTTP etc.

Address resolution protocol (ARP):- it actually translates logical ip addresses to physical address(MAC address)

###I have a planned incoming DDoS attack against a network, what measures would you put in place to mitigate this? Why would you put these measures in place, what is the benefit vs cost?

###1. PC is not booting up, what may be the possible reasons?

###2. You are browsing two different things on the same browser how it will be defined which packets of data have to be sent where?

Using different port for per tab.

####

OS concepts:

Paging (memory management scheme in OS)

TLB (translation lookaside buffer -- memory cache that is used to reduce the time taken to access use memory location),

Deadlocks,

Virtual Memory,

Virtualization,

Memory Management

BSOD,

Mac troubleshooting,

Process management,

Hardware troubleshooting,

Network Adapter troubleshooting,

NIC troubleshooting,

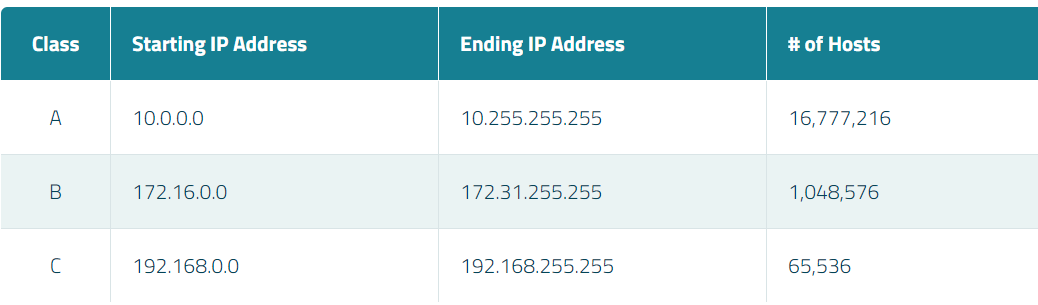
RAID troubleshooting etc. (chkdsk -f (disk error and fix) & chkdsk -r (disk error and bad sector and fix))

###Public/private ip, static/dynamic ip what are they, differences.

Public IP - accessible all over the internet

Private IP -- accessible to only specific IP address. Usually in enterprise/Corp

The following IP address block for private ip



Static/dynamic IP -- Static IP address does not change. Dynamic IP address can change over the time

###Tcp handshake? How to disconnect?

###What is a virtual memory?

If someone comes to you with a slow computer what do you do? -check task manager, antivirus, disk fragmentation.

Bluescreen, causes etc.

What is on device manager?

###Linux commands: list directory, change directory, check permission?

###ports used by various protocols

<https://packetlife.net/media/library/23/common-ports.pdf>

###ping and tracerouter mechanism

###slow connection troubleshooting

###What is Active Directory?

###Difference between static and dynamic routing

Dynamic routing uses BGP,RIP and EIGRP protocol

###A client in Germany is trying to access a server in London, but his connection is running slow. You are in Dublin. How do you diagnose his issue?

###1. common ports 2. active directory 3. IPsec 4. DHCP 5. DNS

#####Database :

Knowing the SQL Queries

Knowing about joins,subqueries,constraints etc.

Basic database troubleshooting (Like Can’t login, Can’t connect to the database)

Basic RDMS concept (they can refer tutorial point for the same DBMS topic)

######

Networking :

###Difference between router, switch.

###What is a Broadcast Domain?

A broadcast domain is a logical part or division of a computer network. In a broadcast domain, all the nodes can be reached via broadcast at the datalink layer. Broadcast domains are located within a network or multi-network segment. Multi-network segments require a bridge, such as the networking device. A broadcast domain member can also be any device or computer that is directly connected to the same switch or repeater. Networking devices, such as routers, are used to separate the boundaries of broadcast domains.

· Subnetting

###MSS/MTU

MSS( Max segment size) is OSI layer 4 data size (1460 bytes)

MTU(Max transfer unit) is OSI layer 3 data size (1500 bytes)

MSS = MTU - 40(IP header 20bytes + 20 bytes TCP header)

###OSI model with complete details and protocols on each layer.

###Flow/error control

· What is a firewall, why do you need it?

· OSI Model

######

OS :

-OS boot process (Win/Linux)

- Memory management ;Memory pages; Buffer and Caches, Basic commands

------------------------------

- My net isn't working, how do i troubleshoot?

- My net speed is slow, i need you to troubleshoot

- Whats ptr entry in DNS.

-Explain DNS, DHCP, Memory management to your grand father.

-Have you dealt with a bad customer?

-Any decisions that you regret?

basic linux system administration questions

Difference between Raid2 or RAID5, mdadm. Raid and logical volume.

LP Questions

https://www.rooftopslushie.com/request/Amazon-Leadership-Principles-Interview-Questions-149

####Windows, Linux and network troubleshooting, internet basics-blues screen, slow network, http error codes etc

####If a server failed to do a nightly backup, what could be a reason for that?

Answer : May be due to failure or mis-configuration of NTP Server. (Check in google)

###basics of networking questions.

###Basics of network troubleshooting and a few questions on clustering.

They are basically checking our knowledge on troubleshooting issues and customer service. Computer network related questions are asked.

###Linux server troubleshooting steps .

###Explain IPsec briefly.

###What are problems you found with AWS

###How to deal with an angry customer.

###How to handle problems like CPU is 100% occupied or the computer is slow what are the possible problems?

####Basic Networking questions:

What is the difference between Bandwidth, Delay and Latency?

What is MTU, Window Size, Segment (MSS)?

Describe 3-way handshake.

A scenario question about prefix-match and route summarization

A scenario question about Stateful/Stateless firewall.

A scenario question about packet flow in NAT

How DNS work

How DHCP work

What is BGP and describe the states - Idle, Connect, Active, Opensent, Openconfirm, Established.

Tell me a time you went out of your way to do something amazing for a client.

Do you have any question for me?

###what is Active Directory and why would anyone use it?

###importance of time in a Windows domain

###what is sysprep, sysvol, BSoD, DHCP, DNS, DFSR, WINS, Global Catalog,

###Describe built-in tools to troubleshoot network issues.

###Some best security practices and a scenario on a company under DoS attack and you choose best answers or suggest any additional answer.

###Questions related to NAT, DNS, EIGRP. He even asked Linux based questions like what ##commands will you use to find the disk space,

<https://www.cyberciti.biz/faq/linux-check-disk-space-command/>

##What is the difference between range and xrange in python.

##HTTP codes.

1XX -- informational

2XX -- success

3XX -- Redirection

4XX --- Client Error

5XX -- Server Error

(<https://www.restapitutorial.com/httpstatuscodes.html> )

##basic networks,Linux commands and operating systems.

Hypervisor, VmWare, windows troubleshooting (blue screen of death), DNS, DHCP, what happens when we type www.amazon.com, linux commands (basics since I told Im good in windows), what will you do when you type a website and website isn't coming (how do you troubleshoot?), Active directories in Windows Server, how would you handle a customer who complains that all his data has been lost and no when theres no back up?, difference between cloud and traditional services, what would you improve in AWS? how would you design your web application on AWS? He told next would be onsite if I was selected, but sadly I didnt get selected.

##Debugging skills on a webpage nor being found.

####Linux based rounds where they ask you lot on commands

###Basic networking stuff with http, dns in particular.

##operating systems questions were difficult

##Linux server troubleshooting steps

What is DNS?

##Steps for resolving www.amazon.com

##What is DHCP?

##Explain IPsec briefly

What are problems you found with AWS?

Technical -

questions about DNS, DHCP process, TCP/UDP, entire stack and functions of each layer, Active directory, web servers, linux configurations, object oriented programming concepts.

Some behavioral skills were also tested by giving some situations.

Behavioral -

Be ready to tell stories about your past work experience and projects to all the behavioral questions. They write down everything you say so be good at it. Leadership qualities are stressed the most. Handling conflicts, handling failures, misjudgement etc are some of the situations. Think over before you start answering. Also prepare for questions like why do you want to work with amazon? what do you want to do?

Explain DNS

What is DHCP

#####

1. What happens when you type amazon.com in the browser? ( was asked two times by different interviewers)

2. Phone interview was pleasant and the questions were troubleshooting issues

3. Database administration interview

4. Behavioral questions are pretty straight forward and the interviewers would like to know the experience of you in situations like challenging project/task. be prepared to what you have to answer.

5. Dont leave out to revise on the simple points such as common ports, DBA questions etc.

6. What and how the load value is calculated which is displayed when you give the command "uptime"?

#####

Mostly on my past experience and routing protocol related questions.

In what order are group policies applied in Active Directory?

TCP/ IP Stack, DNS, DHCP, IP routing, troubleshooting scenarios

Troubleshoot a user's connection problems.

know the basics of networking like TCP, UDP, routing protocols, and also how to troubleshoot a network. Know how ping and traceroute work etc.

On the behavioral side, just be yourself. Show them that you can handle difficult situations, and give examples. While giving examples, don't say "we did", talk about what "you" did. Use "I" a lot.

###Why Amazon

###Online Assessment :-

Online assessment covers IP/TCP, Subneting, Troubleshooting, Private/Public IPs, Routing, Linux Commands like iostat,vmstat, crontab, free, proc/meminfo etc.

Phone Interview: Is 1.1.1.1 routable? What are private IPs ( Ranges)? Are the private IPs submask Classless and Classful? How will you troubleshoot slow website? What linux command to check open ports?

###Most of the questions were based on Linux commands to test the network and IP address range.

###DNS, Basic linux commands, Leadership principles and please go through all the interview questions from glassdoor, they were really helpful.

###Linux -- How do you troubleshoot a Server? and other following questions based on that.

Linux commands

"I have forgotten my password, how will you help me?"

###Behavioral : Focus solely on Amazon 14 Principles and relate

###iIf you type example.com and it doesn't open. What would you do?

###What happens when you press the power button on your PC?

###HTTP codes 404, 403, 200

###1. Difference between DNS and IP?

### 2. Private IP vs Public IP?

###3. Cloud v Vitualization

###4. How to handle problems like CPU is 100% occupied or the computer is slow what are the possible problems?

###What is Linux boot up process?

###Why do you want to come and work at Amazon?

###Databases Concepts

###Networking Concepts

###Amazon Leadership Principles

###A client in Germany is trying to access a server in London, but his connection is running slow. You are in Dublin. How do you diagnose his issue?

###How do you find out what your IP Address is?

###Network troubleshooting commands

###Preemptive Multithreading What is nslookup?

###What is fstab?

###Docker basic commands and working.

###2.Differences between chef-solo and chef-zero.

###3.Git Basics

###4. Grep, nslookup, commands

###5. poymorphism,encapsulation and abstraction

###Windows administration. Windows and linux commands. DNS resolution in detail.

###Make sure you know the OSI model and dns very well.

###what the different between HTTP and HTTPS? and why HTTPS more secure?