InterviewBit

Troubleshooting Interview Questions

To view the live version of the page, click here.

Contents

Troubleshooting Interview Questions for Freshers

Troubleshooting Interview Questions for Experienced

Troubleshooting Interview Questions for Experienced

(.....Continued)

19. An ADSL (Asymmetric Digital Subscriber Line) router connects a PC to the internet. The DNS server IP address is specified on the ADSL router. Is it necessary to configure the DNS server IP address on the computer to access the internet?

20. How would you resolve DNS issues?

21. A customer requests your assistance in determining why a piece of software or utility fails to load or loads with an error. So, how would you help?

22. Can one recover data from a dead PC?

23. Under what circumstances can you not convert a basic disc to a dynamic disc?

24. Discuss the best Network Troubleshooting Practices.

25. What are upper layer faults and how do you rectify them?

26. How to troubleshoot IP related problems?

27. How to troubleshoot local connectivity issues?

28. What does the term "disc error" mean, and how would you respond if you received this message?

29. Explain differential backup vs incremental backup.

30. Why is it important to test your computer's RAM? How can you do it?

31. A consumer claims that their Windows restarts at random intervals. What are your thoughts on this, and how would you solve the problem?

Let's get Started

Introduction

It is a popular notion that if you do not encounter any hurdles or problems in your efforts to keep your business running well, something is wrong. That is how issues in the workplace are unavoidable.

Today's businesses are increasingly reliant on IT techniques. Unfortunately, many firms do not devote enough attention to IT issues that may have an impact on their business processes and security. Taking a few simple steps can assist solve a range of problems while also reducing risks, downtime, and troubleshooting.

What is Troubleshooting?

The process of discovering, planning, and resolving a problem, error, or fault in the software, computer system or any other device is known as troubleshooting. When a computer or software becomes faulty, unresponsive, or behaves abnormally, it can be repaired and restored. Troubleshooting is used to keep a system or software in the desired state, particularly when it encounters or exhibits a problem. It is a methodical strategy that is carried out in one or more phases, depending on the problem's complexity. Identifying the problem is usually the first stage, followed by devising a solution to address the issue and finally putting that solution into action. However, there may be multiple causes for the problem, necessitating a more involved treatment.

Troubleshooting Interview Questions for Freshers

1. Mention some common networking issues.

Some common networking issues are:

- **Problem with the cable**: The cable that connects two devices can become defective, shorter, or physically damaged.
- **Connectivity Issue**: The port or interface to which the device is attached or configured may be physically down or malfunctioning, preventing communication between the source and destination hosts.
- **Incorrect configurations**: Network faults and service disruptions can occur as a result of incorrect configuration, IP looping, routing problems, and other configuration difficulties.
- **Software Issue**: The transmission of IP data packets between the source and destination is disrupted due to software compatibility difficulties and version mismatches.
- **Traffic overload**: When a network (or a portion of a network) or a network node is overburdened with data, this is known as network congestion. Every network has a limit on the amount of data it can manage. This capacity establishes a limit on how much bandwidth and traffic your network can handle before performance suffers.
- **Network IP problems**: The source will be unable to reach the target IP over the network due to poor configuration of IP addresses, subnet masks, and routing IP to the next hop.

2. Define the Network Troubleshooting Procedure.

The combined measurements and processes used to discover, diagnose, and address problems in a computer network are referred to as network troubleshooting. It's a logical procedure used by network engineers to address network issues and increase network performance.

Before you begin troubleshooting any problem, you should have a clear grasp of what the issue is, how it arose, who it affects, and how long it has been present. You'll have a far higher chance of addressing the problem quickly if you acquire the proper facts and clarify the problem, rather than wasting time on useless fixes. To assist diagnose and fixing the issue, you can always start troubleshooting with these simple network troubleshooting procedures.

- **Hardware Inspection**: To begin, inspect the hardware that is installed on a computer, server, laptop, or other similar devices to ensure that it is connected, switched on, and operational. Sometimes the issue is as simple as a loose cord, a router that has shut down, or an unplugged cord; in these circumstances, network troubleshooting is unnecessary. Other basic methods for debugging network hardware can be followed.
  Perhaps turning the gadget on and off or leaving it off for sixty seconds will cure the problem. Cycling at a high intensity is also a good way to do so.
- **Ipconfig:** Ipconfig can be used to display TCP/IP network configuration values, discard a device's current IP and DHCP settings, and refresh a device's DHCP settings. Type ipconfig into the terminal from the command prompt. You may get your default gateway and IP address, but if it starts with 169, it won't get a genuine IP address. In some circumstances, using "ipconfig/renew" to request a new one would solve the problem. If you acquire your IP address through an ethernet cable, the problem is with the router rather than the network.
- **Ping and Tracert:** The "ping" command lets you send a signal to another device, which, if it is operational, will respond with a response to the sender. The "ping" command employs a "echo request," which is a component of the ICMP (Internet Control Message Protocol). When you ping a device, you're sending out an echo request, and you'll get an echo back if the device is active or online. Tracert command displays all of a packet's steps on its way to its destination.
  If the IP address is correct without ethernet, the issue is most likely between your router and the internet. This is the moment to use ping to check if larger servers can connect to your router. If this is unable to connect to your router, there may be an issue. Tracert, which bounces between your router and server's DNS, can also be used to track the problem. We can pinpoint the exact site of the issue, and if the error occurs early, the issue may be with your local network.
- **DNS Check:** Use nslookup command to see if the server you're using has any issues. The nslookup command retrieves DNS records for a domain name or an IP address. Remember that DNS servers contain IP addresses and domain names, therefore the nslookup command allows you to query DNS records for information. If you see terms like "timed out," "service failure," "refused," or "network is unreachable" on your screen, the issue is with the DNS rather than your network. To find the precise IP address(es) associated with a domain name, use the nslookup command. There is a DNS problem if this utility is unable to resolve this information. Along with simple lookup, the nslookup tool can query specific DNS servers to discover if there is a problem with the host's default DNS

3. What is the difference between a Router, a Switch, and a Hub?

- **Hub (layer 1 Device):**
  - Hubs, also known as repeaters, are network devices that operate on layer 1 (the physical layer) to connect network devices for communication.
  - A hub is a basic and inexpensive networking device that connects a group of computers to a single network. When a hub receives a data packet (an Ethernet frame) at one of its ports, it broadcasts (repeats) the packet to all of its ports, which includes all other network devices. When two network devices on the same network try to send packets at the same time, a collision occurs.
  - Hub is a network monitoring tool. They're also employed to give connectivity in businesses. It can be used to create a device that can be accessed from anywhere on the network.

- **Switch (layer 2 Device):**
  - Switches are network devices that communicate at the OSI model's layer 2 (data link layer)
    Switches are also known as intelligent hubs. A device in a network that filters and forwards packets between LAN segments is a switch. Switches work at the data connection layer (layer 2) of the OSI Reference Model, as well as the network layer occasionally (layer 3).
  - It enables multiple connections of many devices in the same network, as well as port and VLAN security settings administration.
  - Switch is often used to connect numerous nodes in local area networks. A switch, like a bridge, uses the same forwarding or filtering logic on each port. When a network host or switch sends a message to another network host or switch, the switch receives the frames and decodes them to read the message's physical (MAC) address component. A switch divides a LAN into numerous collision zones, each with its own broadband connection, allowing the LAN's bandwidth to be significantly increased.

- **Router (Layer 3 Device):**
  - Routers are network devices that operate at the OSI Layer 3 level of communication. Because layer-3 protocols have access to logical addresses(IP addresses), routers can send data across networks . Routers are sometimes known as Layer-3 switches.
  - Router is a data packet forwarding network device. A router connects at least two networks, typically two LANs or WANs, or a LAN and its ISPs network and determines how to send each data packet based on its current network status. Its main goal is to use adaptive and non-adaptive routing to

4. What is netstat utility?

This command is commonly used for incoming and outgoing connections, routing tables, port listening, and use statistics. The netstat command creates graphs that illustrate network and protocol statistics. In table format, you can see the status of TCP and UDP endpoints, as well as routing table and interface information. For example, while checking the status of a host's listening port or seeing whether remote hosts are connected to a local host on a given port, the netstat command is used. The netstat utility can also be used to detect whether services on a host are associated with specific active ports.

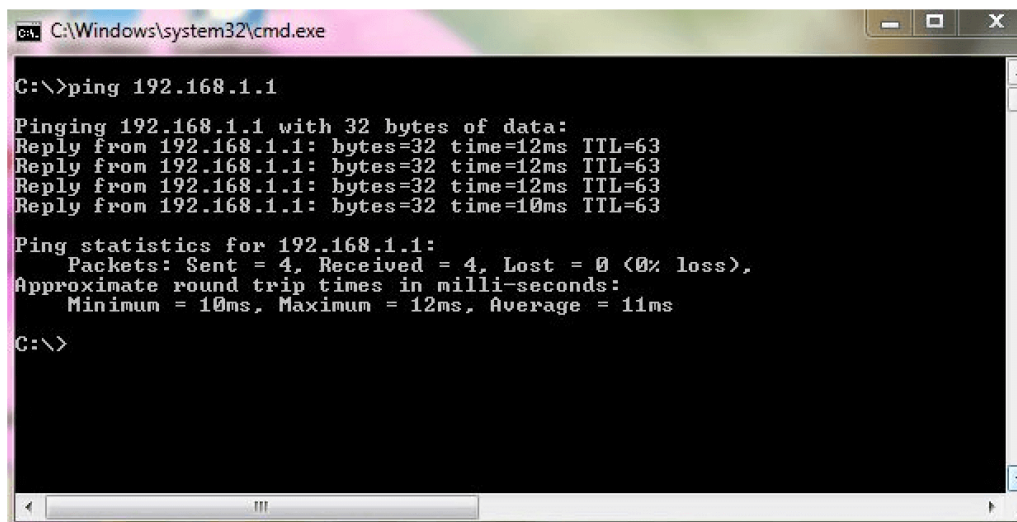## 5. What exactly is a Domain? What is the difference between a Workgroup and a Domain?

A domain is a type of computer network in which all user accounts, computers, printers, and other security principles are registered with a central database that is located on one or more domain controller clusters. A workgroup, on the other hand, is a peer-to-peer LAN that allows computers to share files and printers. Computers and other networking devices can all be part of a domain or workgroup. Each arrangement, however, has a different method of managing network resources.

The primary distinction between a domain and a workgroup is that in a domain, network managers utilise servers to govern all computers on the domain, but in a workgroup, no computer has control over another. Furthermore, devices in a domain can be connected to many local networks, whereas in a workgroup, all devices are part of the same LAN or subnet.

6. What do you know about Ping?

A Ping is a tool for determining whether or not an IP address is connected to another TCP/IP computer. It's a piece of computer network administration software that checks a host's reach on an Internet Protocol network. It's compatible with almost any operating system that has networking capabilities, as well as the majority of embedded network administration applications.

The PING utility validates reachability to the remote end's destination host using IP ICMP echo request and echoes reply messages. The reception of related echo Reply messages, as well as round-trip times, are displayed. The most used TCP/IP command for troubleshooting connectivity, reachability, and name resolution is ping. It contains two messages: the first is whether the data packet is capable of sending and receiving messages from the destination IP address, and the second is the process' RTT time (RTT means round trip time and is calculated in milliseconds).

7. What do you know about the protocol analyzer?

A Protocol analyzer is a sophisticated tool for locating network problems. It is the software that intercepts and records the flow of data packets between the source and the destination. For example, if the system is slow, it can check for latency difficulties and other networking issues, which will aid in the diagnosis of the main cause.

8. What do you understand about Safe Mode?

OS settings or other system issues might cause some program faults. Safe Mode is a troubleshooting environment available in both Windows and Mac operating systems. Safe Mode disables non-essential applications and processes, allowing you to isolate problems more easily. Whenever your system is in Safe Mode, run the troublesome software and try to reproduce the issue you were experiencing while it was in regular mode. If you don't experience the same issue in safe mode, it's likely that the problem is exacerbated by your operating system or another software rather than the application you're debugging.

9. Name three steps you'd take to troubleshoot a problem with an FTP server.

The three steps you'd take to troubleshoot a problem with an FTP server are:

* Ping can be used to test basic connectivity. The "ping" command uses a "echo request," which is an ICMP component (Internet Control Message Protocol). When you ping a device, you're making an echo request, and if the device is active or online, you'll get an echo back.
* Use Nmap to see if the ports are open (20 and 21). The Nmap hosted security tool can assist you in determining the effectiveness of your firewall and security settings. Ports are numbered addresses for network communication on current operating systems. By default, different types of services use distinct ports. Because port configuration might pose a security risk, knowing which ports are open and which are blocked is crucial.
* Check to see if the server's traffic is being restricted by a firewall.

10. A computer that is linked to switch port 23. The switch has figured out the PC's mac address. The port is now closed. Will the mac address be retained by the switch?

The mac-address will not be retained by the switch. A database is maintained in the switch where the mac address is stored. When the port is turned off, the mac address is removed from the switch's mac-address database.

11. To troubleshoot CPU performance issues, an administrator tries to run esxtop by enabling SSH and using putty, but no output is produced. What is the best way to solve this problem?

Press f and place an asterisk next to each field that should be displayed in ESXTOP to display output.

Esxtop displays status information for the physical server running an ESX Server. It displays CPU and memory use for each physical processor, as well as disc and network bandwidth for each network and disc device connected to the ESX Server system.

12. When debugging a VM's CPU performance difficulties, which counters will be used to indicate CPU contention?

The ESXTOP tool is used to evaluate the memory, CPU, and network utilisation of an ESXi host. It's an excellent tool for VMware admins to employ when dealing with performance concerns. To set up ESXTOP, you'll need the vSphere Client, as well as putty and SSH sessions. CPU performance is measured using the counters percent RDY, percent MLMTD, and percent CSTP.

13. Assume a virtual machine is turned off abruptly. To troubleshoot the issue, which VM log files should be considered?

If this occurs, an administrator should investigate the problem by looking at the vmware.log and hostd.log log files. Vmare.log log files keeps track of virtual machine and ESX host activity and the agent that manages and configures the ESXi host and its virtual machines is described in the hostd.log log files.

## 14. How would you prevent and troubleshoot internet browser crashes and freezes?

Several troubleshooting tips are recommended by Google, Mozilla, and Microsoft to assist you to figure out why your Internet browser fails.

- Mozilla, Google, and Microsoft distribute updates for their browsers Firefox, Chrome, and Internet Explorer regularly. These upgrades correct issues while also improving browser stability and security. Therefore, older versions should be updated from time to time.
- Add-ons make your online experience better, but incompatible add-ons may crash your browser. It's tough to know which of your add-ons is creating issues if you have a lot of them. All add-ons are momentarily disabled when you run your browser in safe mode. If your browser doesn't crash in safe mode, one of your add-ons is likely to blame. To discover the conflicting add-on, disable all one at a time.
- Malware might crash your browser at any time or when you access specific websites. Malware can reroute your Internet searches or perhaps even take full control of your browser. To scan for malware on your computer, Microsoft suggests using the Microsoft Security Scanner and antivirus.
- Reset the browser to its default state if all other troubleshooting methods have failed.

15. What is BIOS?

One of the most prevalent applications of Flash memory is for your computer's basic input/output system, sometimes known as the BIOS. When a computer is turned on, the BIOS allows it to do specific tasks right away. The BIOS' primary function is to control the early phases of a computer's starting process, guaranteeing that the operating system is loaded appropriately into memory. BIOS is vital to the functioning of most computers today, and understanding it can help you troubleshoot problems with your machine.
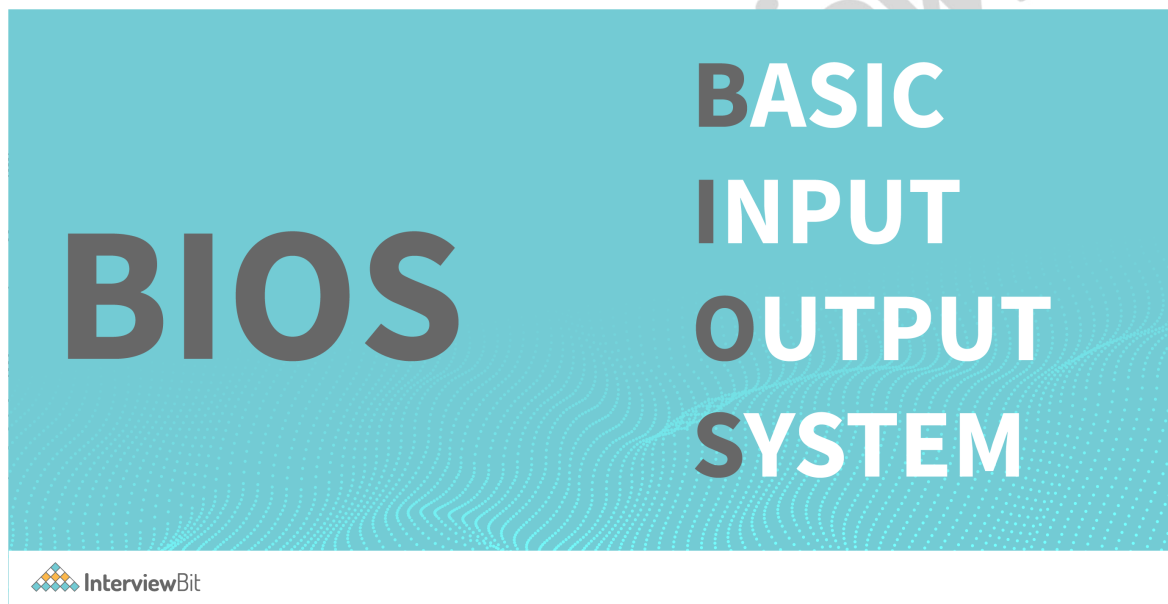
- The Power On Self Test is the first thing the BIOS does once you turn on your computer. The BIOS examines the computer's hardware at the POST to ensure that it can complete the startup procedure. When a POST is successfully finished, the system normally emits a beep. However, if the attempt fails, the system usually produces a sequence of beeps. The quantity, duration, and pattern of such sounds can help you figure out why the test failed.
- After the POST, the BIOS tries to load the operating system using a program called a bootstrap loader, which is made to look for any available operating systems and load them into memory if one is discovered. At this stage, the BIOS drivers are also loaded. These are programs that allow the computer to control hardware devices simply.
- In addition to computer security, the BIOS can play a role. The boot process can be password-protected in most BIOS software versions, which means you must provide a password before any BIOS action can take place. Because the BIOS performs nearly all of its duties during startup, the entire computer is effectively password-protected. Resetting a forgotten BIOS password, on the other hand, can be time-consuming and need access to some of the computer's highly sensitive components.
- The BIOS software is usually stored on a Read-Only Memory (ROM) or a flash memory chip connected to the motherboard of your computer. Because the BIOS software is the first to take control of the system when you switch it on, the position of the BIOS program on the chip is critical. Your computer's CPU would just not know where to find the BIOS if it wasn't constantly in the same position on the same chip, and the boot process would fail.

16. What should you do if you can't download a critical file because it's too large?

The issue of a file being too large for a USB drive can be solved quite easily by changing the file system of the detachable drive from FAT32 to a more current system, such as exFAT or NTFS.

Before you begin, examine the USB drive you're about to change for any vital files you own, and if it does, copy them to a separate location (such as the PC or a different removable drive). This is important since changing a drive's file system will wipe all of its contents. If you're unsure, go with exFAT: it has better support from non-Windows device manufacturers, so if you wish to use the USB drive with either a Mac or Linux computer, possibilities are they'll be able to open the contents without any additional adjusting. If you plan to use the drives with older Windows PCs, such as Windows XP, choose NFTS instead of exFAT because exFAT is a newer format that the older computer may not recognise.
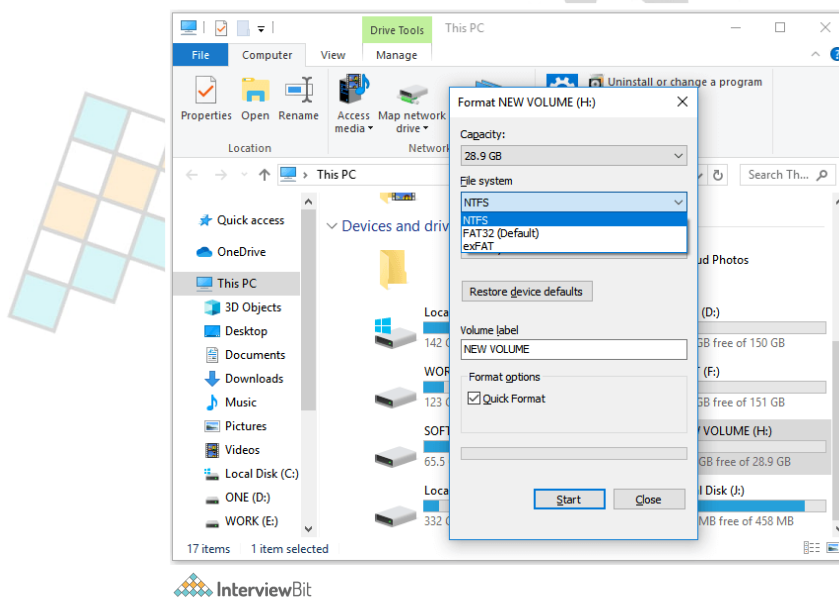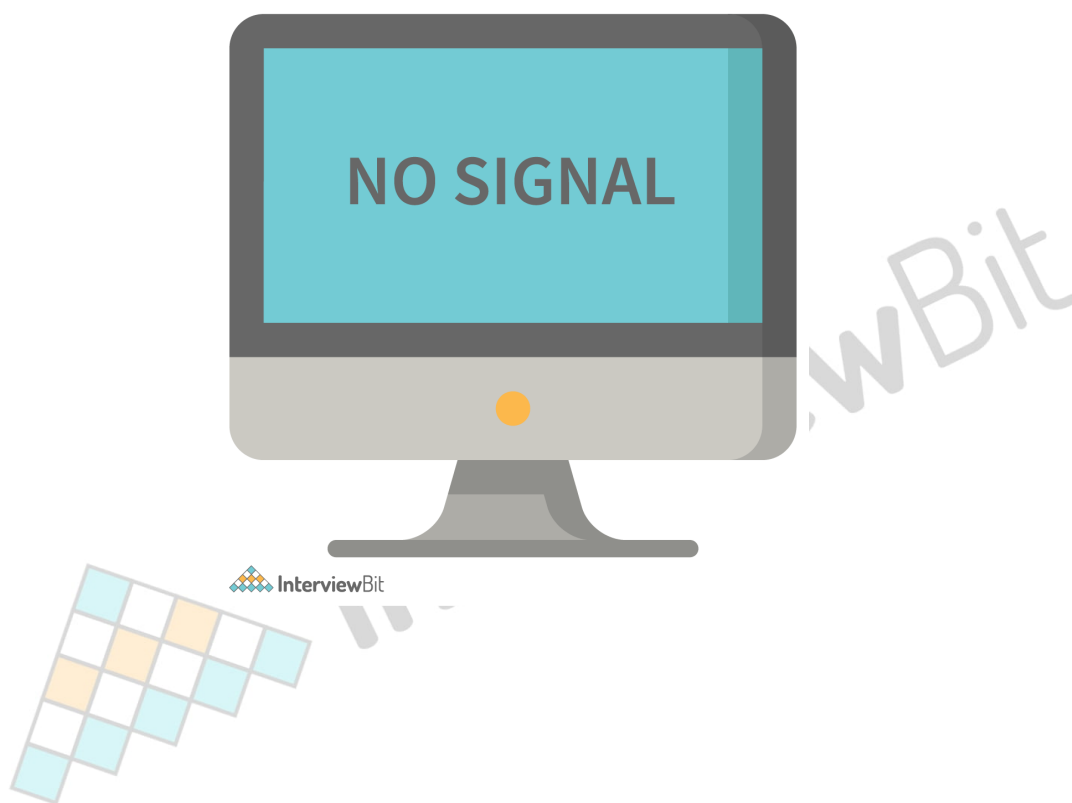

Troubleshooting Interview Questions for Experienced

17. How would you fix the 'No Signal Input' error on your screen?

The most common fixes for the the 'No Signal Input' error on your screen are:

- **Power and Cabling Issues:** This may seem self-evident, but the solution could be as simple as double-checking all electrical connections and ensuring the input device is turned on. Make sure your video monitor cable or HDMI cable is securely attached to the PC or other input device as well as the display. If you're using a desktop tower computer, ensure it's turned on. Some PCs feature cooling fans that spin and create noise even when the computer is not turned on. Check that the power light is on and that the monitor and computer are both connected to a power supply. If you ever discover that your monitor isn't turning on properly, this is a superb method to employ. Examine the state of your power cord. This display problem can be caused by a faulty power cord or power strip. When working with a frayed or damaged power cord, use caution.

- **Source of Input is Incorrect:** Make sure the correct input source is selected if your monitor has multiple input channels. If you're using a video output or HDMI cable to connect to a PC, make sure the monitor input is set to the correct source, such as HDMI or Video. You can normally accomplish this by pushing the menu button until you find the input button on the monitor's main menu or control panel, then selecting the input button to cycle through the settings until you obtain the correct video signal.

- **Setting the Monitor Resolution:** If the monitor display resolutions are out of sync with the input signal, some external display monitors will display no image and an error message. The monitor may display a "no input signal" message if your PC video card or graphics card is set to a display resolution higher than the monitor's native display resolution. To find out what your monitor's maximum and native resolutions are, look at its specifications. If you're not sure and have a Windows PC, consider starting it in safe mode, which has a lower display resolution.

- **Problems with Graphics Cards:** If you're using a graphics card that can be swapped out, check sure it's firmly seated in its slot. Before removing an internal graphics card, make sure all cables are disconnected and the device is turned off. A display device may produce an error message due to a faulty video card or an incompatible video card driver. When a computer is turned on, never remove the cover.

- **Experiment using a different cable or a computer:** A damaged video cable is also likely to be the source of the monitor's lack of signal. If the problem persists, try connecting your monitor and PC with a fresh cable. If not, the problem is due to a problem with your video cable. If the problem persists, try connecting your monitor to a different computer. If your monitor still displays the same image, it's possible that the monitor is the source of the

18. **An organisation's administrator is unable to telnet to a router that is located 10 hops away from the admin PC. What tool can be used to locate the point where the connection is lost? Explain more about the command.**

The admin can use the traceroute command-line tool to inspect the location where packets are being dropped on the router.

Traceroute is a command-line tool used in real-time network troubleshooting to determine the path data packets traverse across the internet to their destination addresses. When you visit a website, the traffic must pass through multiple intermediaries before it reaches the website. The traffic passes through your local router, the routers of your Internet service provider, and onto larger networks, among other things.

Traceroute shows us the path that visitors take to get to the website. It also shows the length of time that each halt takes. If you're experiencing trouble accessing a website that appears to be operational, there could be a problem somewhere along the path between your computer and the website's servers. Traceroute would reveal the source of the issue.

In more technical terms, traceroute uses the ICMP protocol to deliver a series of packets (the same protocol used for the ping command.) The time-to-live (also known as TTL, or hop limit) of the first packet is 1, the second packet is 2, and so on. The TTL is reduced by one each time a packet is forwarded to a new router. The packet is deleted when it reaches 0 and the router delivers an error message. Traceroute ensures that each router in the path discards a packet and responds by forwarding packets in this manner.

19. **An ADSL (Asymmetric Digital Subscriber Line) router connects a PC to the internet. The DNS server IP address is specified on the ADSL router. Is it necessary to configure the DNS server IP address on the computer to access the internet?**

It is necessary to configure the DNS server IP address on the machine. Take the case of a person who wants to visit a website. When a user starts a browser and types the website's URL name, a DNS resolution is required, in which the URL name is submitted to a DNS server. The PC must start the DNS request, which necessitates the configuration of the DNS server IP address on the PC. The DNS request will fail if the PC does not recognise the DNS server IP address, and internet access will be lost.

20. How would you resolve DNS issues?

Following are some ways to resolve DNS issues:

- **Check your cords and connections**: If you're using wired connections, double-check that everything is correctly plugged in. If you're using a wireless network, ensure sure it's turned on and connected. Check to see if your router is turned on and working.
- **Rule out ISP problems**: Make sure you're not having problems with your Internet service provider by attempting to link with another device. If you can directly connect to your ISP without going through the router, do so.
- **Reboot your router**: Turn it back on after a minute and wait till the indicator lights cease blinking before attempting to connect.
- **Scan for malware**: In some situations, a virus could be preventing you from accessing the internet. In this instance, you may have more pressing concerns to address before addressing IP connectivity.
- **Examine your TCP/IP settings**: These options control how your computer interacts with others. You could have recently updated these settings and attempted to manually enter them. Find "Manage network connections" in your computer's networking or control panel. Locate and tap on both IPv6 and IPv4 "Properties" under "Local Area Connections," "Properties." Make sure "Obtain an IP address automatically" and "Obtain DNS servers address automatically" are both checked.
- **Clean out your DNS cache**: Your computer's DNS cache is where it saves networking information from previous visits and efforts to connect to online sites. The cache can get corrupted as a result of incorrect data. Type ipconfig /flushdns into the command prompt to flush, or clear, this cache. The DNS cache will now have to update the DNS information the next time you visit a website.
- **Obtain a new domain name**: Is your website address functional but taking you to an unfamiliar site? It's most possible that you neglected to renew the domain name.
  If necessary, update and reinstall the network adapter driver: When was the last time you updated your drivers? This may be causing problems, especially if you've upgraded your PC's hardware since purchasing it. You can fix DNS problems by manually searching for network device driver updates and updating them.
- **Switch to Google's public DNS servers**: Google's servers are usually more dependable and may be utilised without going via your ISP. You can change your DNS servers to Google's by altering the following properties in your Internet Protocol Version 4 (TCP/IPv4).

21. A customer requests your assistance in determining why a piece of software or utility fails to load or loads with an error. So, how would you help?

Below are some of the things that you would need to check to troubleshoot the software program:

- Check to see if the program's or utility's developer has any fixes or updates available. In some circumstances, the software program will need to be updated to work properly on the computer.
- When one executes the software or utility, one must ensure all other programs are closed. If the software runs successfully after all other programs have been closed, there may be conflicts with other programs.
- After the program is installed, ensure the computer is rebooted at least once. Some programs require a restart of the computer after installation to function properly.
- Check that the date on the computer is correct. Software may rely on the date in various circumstances, and if the date is wrongly specified, it can cause problems.
- If the aforementioned suggestions fail to solve your problems, reinstall the program or utility.
- Your operating system may be the source of your software problem in some circumstances. For this, basic operating system troubleshooting steps must be followed.

22. Can one recover data from a dead PC?

Method 1: The system isn't always completely dead. Sometimes, it simply won't start because of faulty or damaged system files, malware attacks, software problems, or missing DLLs. In such instances, the BIOS utility built into the system can be used to retrieve data. Follow the instructions below:

- Connect the dead system to a USB drive (made with the Windows Media Creation Tool).
- Turn on your computer, press the F12 boot key to access the boot menu, and select the USB installation media.
- You will then be taken to the Automatic Repair setup.
- It will say that the Automatic Repair failed to repair your computer, so select Advanced options.
- Click Troubleshoot->Advanced options-> Command Prompt.
- The window for the Command Prompt appears. Hit Enter after typing notepad.exe.
- Select File > Open from the File menu in Notepad.
- Select This PC from the drop-down menu, then go to the files and folders you want to recover.
- To access them, change the file type to the 'ALL FILES' from txt.
- Select the external disc from the Send to the menu by right-clicking on the chosen file.

If the data is stored on the c: drive, however, this procedure may fail. With the new Windows installation, the c: disc will be formatted permanently.

Method 2:

If your system won't start and you're worried about the loss of data, you can use the dead PC's hard disc as an external drive and follow the steps below:

- Remove the hard disc from the affected computer and attach it to a functional computer. To utilise it as a hard drive, use a hard drive connector such as a SATA to USB converter or an external Hard Drive Enclosure. Connect the hard drive to the PC using an appropriate connector if the PC supports PATA/IDE 3.0.
- Open Disk Management by right-clicking (or long-pressing) the Start button and selecting disk management.
- Assign a drive letter to the hard disc if the system recognises it but shows it as RAW.

Method 3:

When your system fails to boot and you attempt to repair it, you run the risk of losing vital data. To avoid data loss, use reliable data recovery software to recover your important system files, photographs, videos, and documents. These programs provide a bootable recovery disc feature that enables you to recover data from crashed, corrupted, formatted or non-bootable computers.

23. Under what circumstances can you not convert a basic disc to a dynamic disc?

Dynamic discs are logical discs that can use several hard drives in the computer to provide disc redundancy, mirroring, and improved performance and reliability. Dynamic discs are a type of volume management that permits volumes on one or more physical discs to have noncontiguous extents.

It is not possible to transform every standard hard disc into a dynamic disc. Removable media, such as ZIP and Jaz discs, for example, cannot be transformed into dynamic discs. The explanation for this is straightforward. A dynamic disc is a storage device that can span many drives. The volume would be broken if it spanned a detachable disc and the disc was eliminated from the system.

If the basic disc is on a laptop computer, it cannot be turned into a dynamic disc. This can be due to a variety of factors. You ought not to be running Windows Server 2003 on a laptop in the first place. Second, the majority of laptops have only one hard drive. Dynamic discs would provide no benefit to a system with a single hard drive. Third, when a laptop has multiple hard drives, one of them is frequently located in a docking station. A dynamic disc volume that encompassed the device's internal hard drive, as well as the docking station's hard drive would indeed be damaged if you removed your laptop from the docking station.

Clustered servers are the third case in which a basic disc cannot be transformed into a dynamic disc. The final criteria about basic drives that cannot be transformed are that any hard disc with a sector size bigger than 512 bytes can't be converted (albeit this is unlikely). Cluster sizes larger than 512 bytes are possible, but not sectors.

24. Discuss the best Network Troubleshooting Practices.

It is also crucial to have some best practices in place to make troubleshooting as speedy and painless as possible. Following these best network troubleshooting practices as you strive to resolve network issues will help speed up the process and minimise superfluous or repeating efforts.

- **Gather facts about network and network problems**: To provide the greatest help to your end consumers, you must first determine what the issue is. Collect enough information from the people who are having network problems as well as the network itself to be able to duplicate or diagnose the problem. Take cautious not to confuse symptoms with the core cause, as what appears to be a problem may be a symptom of a greater problem.
- **Logs can be customised**: Make sure your event and security logs are set up to provide you with the information you need to troubleshoot and analyse the root cause. Each log should provide a clear explanation of the items or events being tracked, as well as the date and time, as well as information about the report's source (MAC or IP address).
- **Examine security and access**: Check that no access or security concerns have arisen by ensuring that all access permissions are as they should be and that no one has tampered with a sensitive section of the network they weren't meant to. Check that any firewalls, antivirus, and malware software are up to date and that no security concerns are interfering with your users' ability to operate.
- **Adhere to an escalation protocol**: There's nothing more irritating than going to the IT help desk and getting routed to someone else, who then directs you to someone else, who then refers you to someone else, and so on. Establish a clear escalation system that identifies who is responsible for certain concerns, as well as the last person in the chain who can be contacted for assistance. All of your end customers should know who to contact if they have a problem, so they don't waste time talking to five different people who can't help them.
- **Using monitoring tools**: Manual troubleshooting is possible, however, it can take a long time if you go through each step. It might be stressful to try to locate the problem, let alone remedy it when you have a slew of individuals banging on your office door or sending you frantic emails. It's best to employ monitoring tools in commercial and corporate circumstances to ensure you're obtaining all of the relevant network information and aren't missing anything crucial, not to mention avoiding exposing the firm to excessive danger.

SolarWinds® Network Performance Monitor (NPM) is my preferred monitoring software . It's a well-designed application with capabilities that help you debug network issues quickly and thoroughly. NetPath network path analysis, which shows your network topology and performance pathways, and PerfStack, which enables you to compare multiple performance measures against each other as well as historical data, are two more NPM capabilities. You can use these tools to see which performance issues are linked and troubleshoot the root cause more quickly.

25. What are upper layer faults and how do you rectify them?

If you still can't find a solution after examining physical connectivity, local connectivity, IP connectivity, and routing issues, the fault could be in the transport and application layer protocol.
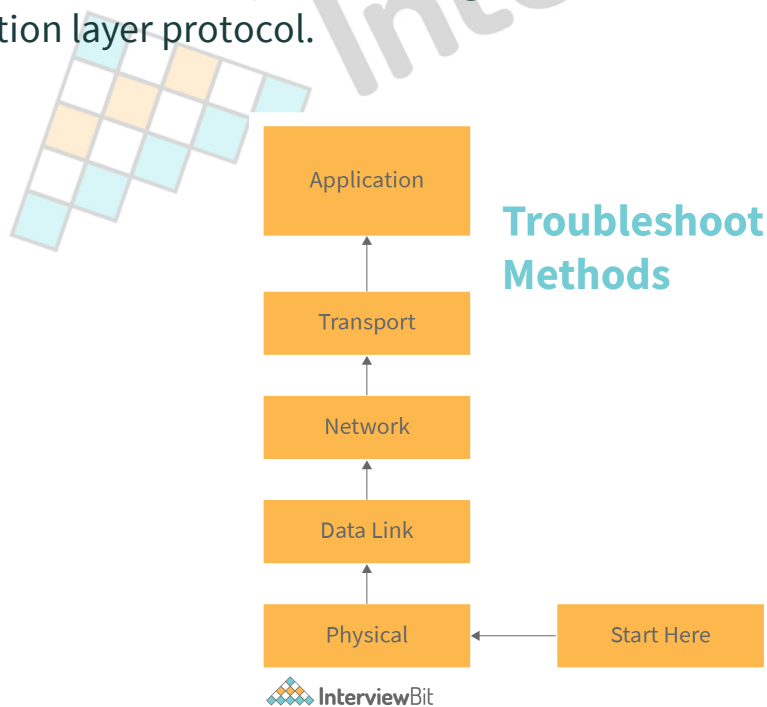
A defect can occur for a variety of reasons:

- The data connection has been lost.
- Incoming and outgoing traffic is blocked by a packet filter or firewall.
- On the server, a specific service is unavailable.
- Between the client and the server host, there could be an authentication and access issue.
- Issues with software incompatibility or mismatches between the source and destination hosts.

26. How to troubleshoot IP related problems?

If we cannot reach the destination IP address and cannot identify a route to the next-hop at any point in the network using the TCP/IP protocol suite, we will utilise the PING and TRACEROUTE tools to diagnose the cause and location of the problem.

The following are some general steps to troubleshoot IP-related network issues:

- To begin, identify the pair of devices between the source and destination hosts that are experiencing connectivity issues.
- The failure could be due to a physical connectivity issue once you've located the devices using the tools. As a result, examine all of the physical connections along the path.
- If you work in a LAN network, there may be a problem with the LAN connectivity as well. As a result, double-check your LAN connections. The local port may be broken or unavailable, preventing the source from communicating with the destination IP.
- A router connectivity issue when travelling through numerous channels to reach the destination could be one of the causes of the error. As a result, verify that the router is appropriately defined at each intermediate hop.
- Examine the configuration options.

27. How to troubleshoot local connectivity issues?

If you discover that there is a problem with LAN connectivity on a huge level, you should take the following actions to identify the root cause and resolve it:

- Ping the destination IP if the destination and source have the same subnet mask.
- Otherwise, ping the router's gateway IP address if the destination is on a different subnet mask.
- If both pings fail, first verify the configuration settings to see if the subnet mask and route to be taken to reach the target are properly defined in the routing table.
- Check if your source host can ping another hop in the LAN network other than the destination host or route to that once you've completed the configuration section and verified everything to be in order.
- There could be a variety of reasons why you are unable to ping another device. It could also be a setup problem, a physical connectivity problem, or a problem with repetitious IP address entry.

28. What does the term "disc error" mean, and how would you respond if you received this message?

When the computer BIOS cannot detect a bootable operating system on any of the storage devices included in the notebook computer's boot path, the Non-System Disk Error or Disk Error message appears.

Here are a few approaches that may be useful, and any of them may be the answer to your problem.

Method 1: Examine all non-bootable storage media.

First and foremost, make a list of all non-bootable storage devices connected to the computer and remove or detach them. When you connect many devices to a computer, the system may have trouble determining which device has the OS loaded, which can result in an error like this. As a result, disconnect all non-bootable external devices.

Method 2: Check the IDE (Integrated Drive Electronics) or SATA (Serial Advanced Technology Attachment)cable on the HDD.

If your hard disk's IDE or SATA cable is damaged or improperly attached, the system may be unable to read the disc, resulting in the "non-system disc error." If the cable is damaged or malfunctioning, simply reconnect it properly or purchase a new one.

If the HDD cable is in good shape and securely attached, but the error remains, it's possible that the HDD on which Windows was installed is not set as the primary disc in BIOS.

Method 3: If necessary, change the boot order.

Access the BIOS/UEFI environment on your PC and make sure the hard disc drive you're trying to boot from is in the correct boot order settings, which should be at the very top of the boot order list. To alter the boot order, follow these steps:

- While the computer is restarting, press the key required to enter the BIOS or UEFI setup screen (usually Esc, F2, F8, F10).
- Select the Boot tab in BIOS with the arrow keys on the keyboard and give the system drive the boot priority, which should be set at the top.
- The mouse pointer can be used to specify the boot sequence in UEFI.
- The BIOS/UEFI setup utility should be saved and exited. The computer will reboot with the new settings in place.

Method 4: Reinstall the hard drive.

Another option for resolving this issue is to remove and reinstall the hard disc.

Steps:

- Remove the power cable/charger from the PC and turn it off.
- Then the battery should be removed (for laptops).
- Disconnect the hard drive from the computer.
- After blowing out the dust, clean the hard disc using a dry rag.
- Reconnect it to your computer.
- Return the battery to its original position.
- Connect the charger or power cable.
- Restart the computer.

Method 5: Access hard drive and recover data from the hard disk without OS.

Except for external influences, you must accept the fact that something went wrong with the hard disc drive's boot files, which may have gotten damaged or corrupted, and that fixing the HDD's boot sector, master boot record (), and boot configuration data (BCD) must take effect.

- Make a bootable Disk.
- Proceed by booting from the bootable USB.
- Recover data from a non-booting hard drive.

29. Explain differential backup vs incremental backup.

The fundamental distinction between incremental and differential backups is that incremental backups save space and time by simply saving modified data. Incremental backups, on the other hand, are not as effective as differential backups. Let's discuss Full Backups before diving into the distinctions between Incremental and Differential backups. A full backup is the launching point in both incremental and differential backup schemes in their most basic form. Of course, a complete backup backs up all the information on a partition or disc by copying all data-containing disc sectors to the backup image file.

An incremental backup is a copy of any data that has changed since the last backup. As a result, if you make a full backup of your system on Sunday, an incremental backup on Monday will only transfer and save data that has changed or been added since Sunday. On Tuesday, an incremental backup will only deal with data that has changed since Monday's incremental backup, and so on. The differential backup, unlike an incremental backup, only backs up data that has changed since the last full backup.

The difference between incremental backup and differential backup is given in the table below:

Particulars	Incremental backup	Differential backup
Description	Backs up all data that has changed since the previous backup, such as since the last complete or incremental backup.	All data that has changed since the last full backup is backed up.
Storage space	It demands less amount of storage space.	This backup requires less storage than a full backup, but more than incremental backups.
Data recovery	Data recovery might take a long time and be difficult.	Data recovery takes less time.
Backup	Taking a backup is quicker.	This backup is faster than a full backup, but not as fast as an incremental backup.
Bandwith range	It has a lower bandwidth range.	It uses less bandwidth than a full backup, but more than incremental recovery.

Daily, a differential backup approach backs up files that have changed since the previous full backup. Because less data is stored up, they are much faster than complete backups. In contrast to differential backups, incremental backups copy files that have changed after the last backup of whatever type, which can be a complete or incremental backup. The fewer data that needs to be backed up when incremental backups are conducted, the shorter the time between backups.

One of the advantages of differential backup over incremental backup is that you just need the most recent full backup and differential backup to recover data, which speeds up the process. However, until the next full backup, the amount of space needed by backed up data will increase with each differential backup.

Among the three strategies: full, differential, and incremental, incremental is the one that saves the most space. Even though the incremental backups offer more versatility and granularity (duration between backups), they have a tradition of taking longer to restore because they should be built from the most recent full backup and all successive incremental backups.

30. Why is it important to test your computer's RAM? How can you do it?

The working memory of your computer is its random access memory (RAM). The operating system and programs on your computer are constantly writing and retrieving data from RAM. When you open a web page such as this one, for example, your web browser saves it in RAM as you read it. When you start a PC game, it loads data from a slower storage system (such as a hard disc or solid-state drive) into considerably faster RAM.

If your computer's RAM is defective, you may experience issues. When your computer goes to read the RAM, it will consider various data than it saved to RAM. Software crashes, system freezing, blue screens of death (BSODs), file corruption, and other issues can result as a result of this. These programs work by writing data to every sector of your computer's RAM and then recovering it back in a sequential manner. If the utility returns a different result, it means your RAM is bad.

The finest RAM testing software necessitates booting into a separate bootable system. This gets Windows (or some other operating system) out of the way and gives the tool complete access to your RAM at a low level. You can run tools from within Windows, such as HCI Design's MemTest, but they aren't as trustworthy.

- Launch the Windows Memory Diagnostics program. A RAM testing tool is included with Windows. It comes preinstalled on Windows 10, Windows 11, Windows 7, and all other recent Windows versions.
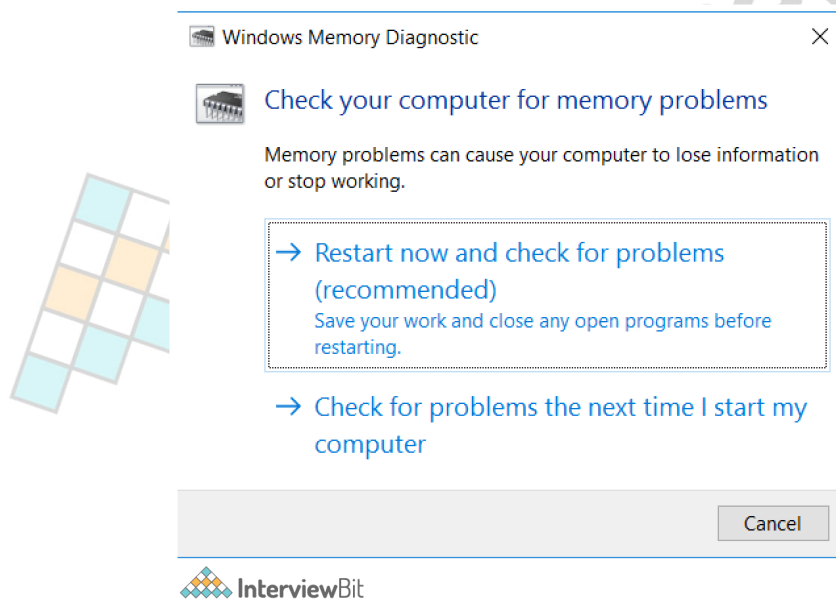
- You can install and use MemTest86 if you need a more capable testing tool. It runs a larger range of tests and may uncover issues that the Windows test would miss. If you want to try something else, MemTest86+ is a free and open-source program. Both of these programs are self-contained and bootable. You can copy a USB image from MemTest86 to a USB disc. To make a bootable USB drive, simply run the EXE file provided with the download as well as provide a spare USB drive. Restart your computer once you've made bootable media and instruct it to boot from the USB device where you copied the memory test tool.

31. A consumer claims that their Windows restarts at random intervals. What are your thoughts on this, and how would you solve the problem?

If your Windows machine restarts without warning, consider the troubleshooting methods below for assistance in addressing the issue.

Software issues: Microsoft intended Windows to automatically reboot when issues, such as a blue screen of death, occur since the release of Windows XP. Although this feature is useful for random failures, it makes troubleshooting and repair more complex. The procedures to disable and enable this function in Windows XP, Vista, 7, 8, and 10 are listed below.

- Right-click My Computer on the desktop. Open File Explorer in Windows 8 or 10 and right-click This PC in the left navigation pane.
- In the pop-up menu, choose the Properties option.
- Select the Advanced tab or the Advanced system settings link in the System Properties box.
- Click on The settings option under Startup and Recovery on the Advanced tab.
- Disable the Automatically restart check box in the Startup and Recovery window.
- Click the OK button.

Hardware issues: If you've previously attempted to introduce a new hardware device, make sure it's not the source of your problems. By looking for problems in Device Manager, you can make sure you're not having any hardware conflicts. If you've just installed new hardware drivers, you might want to go back to an older version. If the unexpected reboots persist despite updating drivers and removing any newly attached hardware, the computer memory is bad. Finally, improperly installed hardware devices in the computer can result in random reboots. Ensure that all cables and expansion cards are correctly connected to the computer.

Computer viruses: These viruses usually cause the computer to reset every 5, 10, 15, or 30 minutes after it has booted. If you suspect your computer is infected, make sure you have an antivirus program installed and that your virus scanner definitions are updated.

Overheating: Most computers today are intended to shut down or reboot automatically if the processor, video card, or other components become too hot. Examine the rear of the computer to see if the fan on the power supply is operating. A temperature gun can be used to determine how hot the computer's hardware devices or integrated circuits are.

Issues with the Operating System: If your computer continues to reboot after completing the steps above, you're most likely dealing with a problem with the Microsoft Windows operating system. When the computer starts to boot up, restart it and enter BIOS setup. Allow the machine to sit idle for several minutes after you've loaded the BIOS setup.

If the system doesn't reboot after resting in BIOS and you've exhausted all of the above options, try enabling a restore point in Windows from before the problem began. If enabling a previous restore point fails, or if no restore points are available, you will most probably have to reinstall Microsoft Windows.

Conclusion:

We are optimistic that this article on troubleshooting interview questions has improved your knowledge of troubleshooting and related concepts. If you have a good grip on all of the questions offered here, you will be able to comfortably crack any relevant interview.

Useful Resources:

- Networking Interview Questions and Answers
- OS Interview Questions
- Computer Network MCQ With Answers

Links to More Interview Questions

C Interview Questions

Php Interview Questions

C Sharp Interview Questions

Web Api Interview Questions

Hibernate Interview Questions

Node Js Interview Questions

Cpp Interview Questions

Oops Interview Questions

Devops Interview Questions

Machine Learning Interview Questions

Docker Interview Questions

Mysql Interview Questions

Css Interview Questions

Laravel Interview Questions

Asp Net Interview Questions

Django Interview Questions

Dot Net Interview Questions

Kubernetes Interview Questions

Operating System Interview Questions

React Native Interview Questions

Aws Interview Questions

Git Interview Questions

Java 8 Interview Questions

Mongodb Interview Questions

Dbms Interview Questions

Spring Boot Interview Questions

Power Bi Interview Questions

Pl Sql Interview Questions

Tableau Interview Questions

Linux Interview Questions

Ansible Interview Questions

Java Interview Questions

Jenkins Interview Questions