# Technical Skills

## 1. Can you explain the OSI model and why it is important in networking? Follow-up: Can you describe the function of each layer?

The OSI model is a representation of a layered stack of technologies in networking. It gives us a common language and a structure to base our discussions and troubleshooting on.

**Layer 1** is the physical layer; the media communications will use to transfer information. **Layer 2** is the Data Link Layer, which is further subdivided into the logical and MAC layer. Important in switching and NICs, essentially, this layer uses MAC addresses to communicate on Ethernet networks. **Layer 3** is the Network layer, the layer the internet works on by using IP addresses and routing. **Layer 4** is the Transport layer, most commonly, TCP and UDP ports allow for a multiplexing of traffic across different services on network hosts. Layer 5-7 are more commonly wrapped up in the TCP/IP model as one layer; however, **Layer 5** is the Session layer where session management takes place. **Layer 6**, Presentation is about formatting the data. **Layer 7**, Application, identifies what the end user is interfacing within production.

2. What’s the difference between a router and a switch? Follow-up: How would you determine which one to use in a given scenario?

A router operates at layer 3 by using IP address and routing tables to forward packets, whereas a switch operates at layer 2 by using MAC addresses and CAM tables to forward frames.

Routers are used for two common functions: at network edges in dividing LANs and the internet and separating subnets where different business departments live.

Switches are used to connect endpoints to a network. They also allow for further segmentation using VLANs. Layer 3 switches are modern switches that are sophisticated enough to operate at both layers 2 and 3, giving the switch routing capabilities.

## 3. How would you troubleshoot a network connection issue where a user is

## unable to access a particular website but can access others?

I start by identifying the scope of the issue. In this scenario, the scope seems to be pointed at the problem being isolated to this individual website. However, we need to rule out any user errors to start with. I would confirm the FQDN was typed correctly and include the proper use of HTTPS vs HTTP. With this ruled out, I would determine if there is a proxy server, host-based, or network firewall that could be blocking this particular website or category.

I would further test theories by connecting to this website from different ISPs to ensure it isn’t isolated to an individual transport network. A possible solution is to reroute traffic to this domain out of a secondary ISP.

Another theory I would test relies on the ownership and operations of the website. It is possible that changes to the IP address have not propagated to DNS servers across the internet and internal servers. A possible solution here is to flush DNS cache, update DNS records, and use alternate DNS providers.

The last theory I would investigate is the status of the service. For example, Downdetector could be reporting the service is unavailable in the area. After this, it may be time to discuss and investigate any SLA’s involved with the service.

## 4. What are some common networking protocols you’ve worked with

## (e.g., TCP/IP, HTTP, DNS)? Can you explain how they work?

TCP/IP is the most common as it is used across LANs and the internet. HTTP/s and DNS, being the most used on this stack, operate at the application layer of the TCP/IP model. HTTP (80) and HTTPS (443) are the protocols that web browsers use to communicate with web servers, HTTPS being the secure method. This protocol uses URLs to make connections with servers and resources on the servers through a number of methods such as GET, PUSH, PULL, and DELETE, among others.

DNS, the domain name service, allows web users to query servers based on user friendly and memorable names. DNS servers allow for this by storing publicly accessible records of IP addresses matched to IP and IPv6 addresses. Numerous DNS record types exist. For example, A (IP), AAAA (IPv6), NS, and TXT.

Other network protocols I’m familiar with are routing protocols such as OSPF and BGP. These protocols allow for dynamic routing updates through peering of network intermediary devices. Numerous others such as SFTP, SSH, DHCP, NTP, SMTP, are common.

## 5. How do you configure a static IP address on a device?

This depends on the device; however, commonly on end-user devices, such as a Windows client, the NIC can be configured through the Network and Sharing Center on the Control panel. I prefer (Win + R) combo to open Run and to type ncpa.cpl to use the network connections applet.

Each OS will have a unique way to achieve this using the GUI. It can often be achieved faster through the CLI, but the syntax will differ.

## 6. What is DHCP, and how does it work?

Dynamic Host Configuration Protocol uses a server/client architecture. Once a client is set to use DHCP, it sends out a broadcast to request an address and DNS information to any DHCP servers on the broadcast domain. If a server is not found, the client will automatically assign itself an APIPA, which can only be used for communications on that segment.

DHCP uses Discovery, Offer, Request, and Accept messages, DORA for short.

## 7. How would you troubleshoot DNS issues if a user cannot access a website

## by domain name but can do so by IP address?

Calling back to question 1, I can further elaborate that since the website is reachable via IP address, it can be determined the scope of the issue is a DNS issue. We need to find the root of the DNS issue by investigating the misconfigured DNS server record, cache, or host file. It is possible the domain was mistyped at the client or server. It’s also possible, a DNS filter could be inhibiting the resolution of the domain.

## 8. Explain the difference between IPv4 and IPv6. Why is IPv6 becoming more

## important?

IPv6 is important due to the proliferation of networking devices. As the number grows, the supply of available IP addresses is being consumed. IPv6 gives us a vastly higher number of available addresses. It is worth noting, this problem has been alleviated using NAT. This has led to a slower transition to IPv6. However, IPv6 has some built-in advantages such as IPsec.

## 9. Can you explain what subnetting is and why it’s important? How do you

## subnet a network?

Subnetting lets us manage our network and address space in a more granular way. It allows for segmenting networks by resource or department and is of benefit to security and traffic optimization. It also allows for a more efficient use of address space for larger networks.

## 10. What is a VLAN, and how do you configure one on a switch?

A virtual local area network supports the goals of segmentation and optimization through subnetting. For example, we want to separate network traffic based on functional departments or logical groups of resources. Perhaps though, there is a mix of departmental personnel on the floor. The finance personnel’s IT can be isolated on a switch through different VLANs. The switch port where these devices are connected is tagged for the appropriate VLAN, and trunks can be configured for cross-switch communications.

## 11. What is NAT, and how is it used in a typical home or office network setup?

Calling back to question 8, NAT was created to alleviate the supply of addresses. Each home or office is given a public IP as part of their internet service. The router will then typically have built-in DHCP, where it serves private network addresses to the home office. Each local device will be assigned a private address, and the router will use a NAT table to keep track of the connections made outbound by mapping private IP, port, and public IP.

## 12. How would you secure a Wi-Fi network in a corporate environment?

The corporate wireless network should be separate from any access given to guests -- a guest network should be created for this purpose. The corporate wireless network will need WPA2 or WPA3 security so only authorized users can connect, and the wireless transmissions are encrypted. Further, authentication and authorization can be achieved through using RADIUS and domain servers such as Active Directory.

13. What is the difference between TCP and UDP? When would you choose one over the other?

TCP ensures reliable communication through a secure handshake and acknowledgments of transmission, which are very important for applications where the integrity and security of data are important, e.g., banking and e-commerce.

UDP is of great use in media streaming, where any lag in receiving the data causes the experience of jitter and buffering. While TCP accounts for lost packets, UDP is real-time and time-sensitive--it’s too late to recover any lost packets, and doing so will not benefit the experience. UDP creates less overhead to optimize the use of the bandwidth to support this.

## 14. How would you approach configuring a VPN for remote employees?

Remote employees will use remote access VPN technology. Thus, a client will be installed and configured to connect to the VPN server, whether it be a firewall or a dedicated VPN concentrator. It will likely be using SSL, but IPsec is also an option. L2TP is also available natively in Windows.

Information such as the public IP of the VPN server, what modes and versions of IKEv2 are required in the configuration, and any authenticating information. It’s much easier to use SSL, but performance may suffer in comparison to IPsec. Newer protocols such as WireGuard are worth noting as performance may be improved, and security flaws in SSL libraries are worth avoiding.

# Problem-Solving and Troubleshooting

## 15. A user reports that their connection is slow. How would you go about

## diagnosing and fixing the problem?

We must keep network baselines and service agreements in mind. Is it peak traffic hours? What bandwidth is supported by the ISP, the internal network intermediary devices, or server resources? The context will help greatly as we must identify anomalies and any bottlenecks.

We can explore numerous theories, but we should narrow the scope by identifying the service or workflow the end user is using. A possible solution to explore is quality of service for the application or protocol, or we may need to limit the use of less necessary services, such as non-business-related services. The business could've outgrown the network as a new workload was implemented, creating congestion. Ultimately, it may be time to upgrade equipment.

## 16. You notice that a particular subnet has been experiencing consistent

## packet loss. What steps would you take to investigate and resolve the issue?

Potentially, the loss could be at any line card upstream from the point at which we are seeing the loss. First, I would identify the scope of the issue. Is it all traffic or a particular flow? What commonalities can be found about the affected flows? This could give me an idea of where the traffic is coming from and help narrow down an area in the network. Tools such as ping and pathping or traceroute could show dropped packets.

Narrowing the scope is crucial--this can be done by investigating from a halfway point in the network and working inwards or outwards based on findings. Looking at network card metrics along the route could show collisions and signify a malfunctioning NIC.

Dropped packets could also be due to network congestion, as intermediary devices may have full buffers. Recognizing a congested network and applying QoS may also be necessary.

## 17. Explain how you would handle a situation where a critical server goes

## down in a remote environment, and you are unable to access the office

## physically.

Depending on the incident response plan and procedures, we may have technical contacts, such as contractors or internal employees for outages like this. If the server is completely unreachable, it could be due to power failure, which becomes obvious with eyes on the premises. If monitoring solutions are still accessible, what information can be gleaned? Perhaps it showed failed contact with UPSs or other network devices. Short of a technical contact onsite and all attempts to connect via management protocols, it may be time to contract local resources, given that the location is so remote that traveling there myself is out of the question.

## 18. How do you monitor network performance and health? Which tools or

## methods would you use to track bandwidth, latency, and packet loss?

SNMP allows for monitoring network devices and metrics. Traps can be set to alert of congestion, CPU, storage, and memory use. Solutions that utilize SNMP and aggregate these metrics can show historical data to show trends and anomalies. SD-WAN can probe hosts found on local networks and on the internet to show latency and loss, giving metrics in real-time. Reports can often be generated as part of cloud subscriptions.

Remote Work & Soft Skills

## 19. As a remote engineer, how do you ensure effective communication with

## team members who are spread across different time zones?

A higher level of flexibility may be necessary for more extreme time zone differences. Pacific time, being four hours behind Eastern, communications will likely be scheduled in the latter half of the workday for EST employees. Scheduling tools will account for time zones making it easier for coordinating availability.

## 20. Can you describe a time when you had to work independently on a

## network issue? How did you manage your time and resources to resolve it?

I’ve troubleshot many networking issues. A common one was loss of network connectivity. These situations required identifying the scope of the issue to rule out the ISP or internal resources. Identifying the scope is of utmost importance as it steers the investigation. An accurate assessment will determine a timely solution, as we can begin activating the necessary resources to implement solutions. For example, the solution may be the ISP’s responsibility.

Managing long-term issues requires understanding the impact of the issue. Greater impact will require a more urgent response and reprioritizing resources and time. Workarounds can potentially alleviate the impact and require less urgency. It would be necessary to ensure alignment with the expectations of senior management.

## 21. How do you stay motivated and organized while working remotely

## without direct supervision?

My home office is clean and tidy. My work ethic aligns with my ambition to be successful and provide for my family. I keep active, energetic and healthy by incorporating a standing desk and under the desk walking pad.

## 22. How do you handle a situation where you need to collaborate on a

## network issue with a team but are facing connectivity problems (either due to

## remote tools or network issues).

I would first identify if the problem was local to me or involving the service or tool. Given that it was a service or tool, it would be a good procedure to have alternatives to fall back on. If local to me, it may be an internet outage and would require finding a secondary location to operate. This could be thought of as a personal business continuity plan.