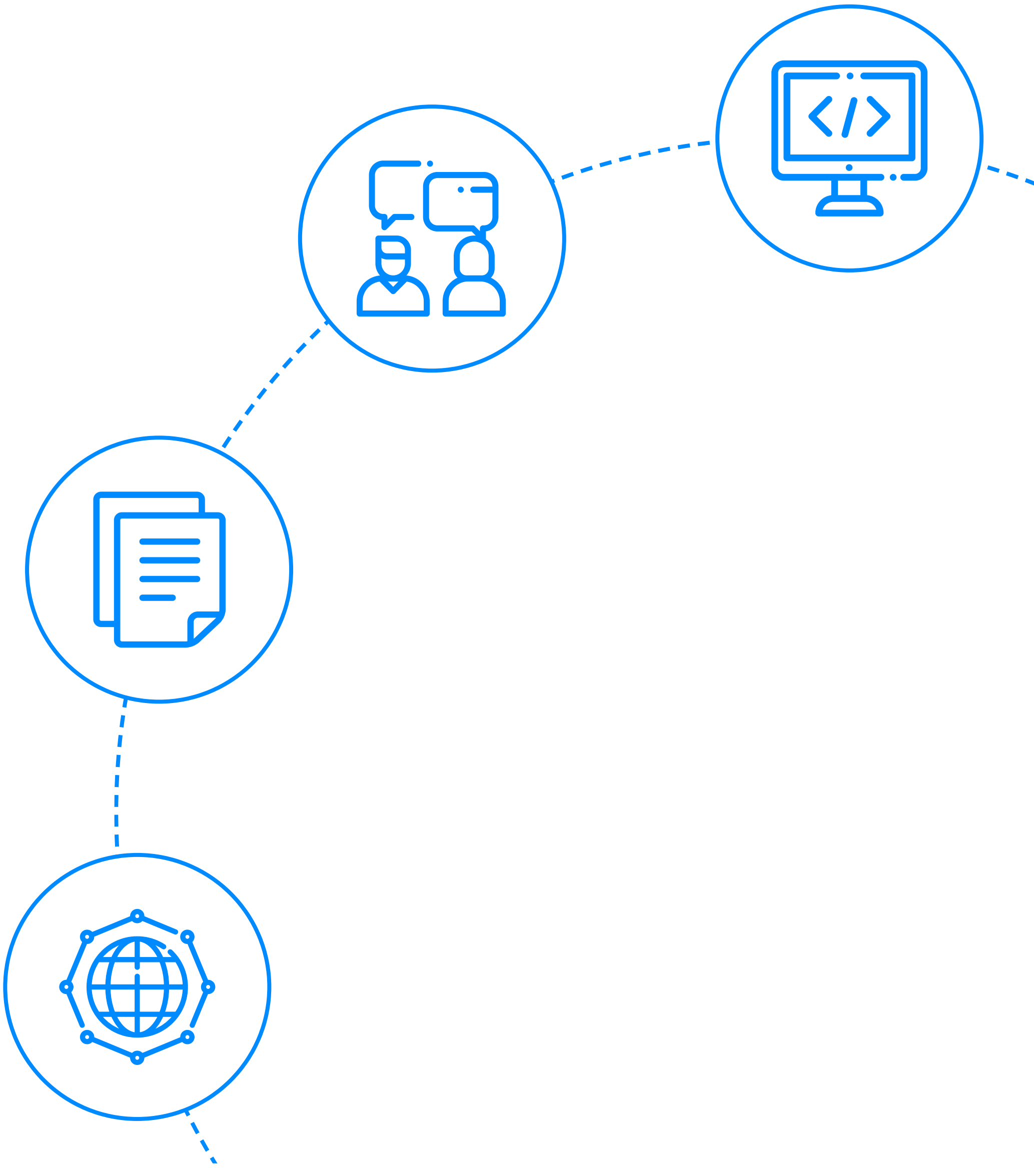
InterviewBit

Network Security Interview Questions



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

Contents

Network Security Interview Questions for Freshers

Network Security Interview Questions for Experienced

Let's get Started

Network security is the process of protecting your computer from unauthorized access and unauthorized activities. Network security is a complex topic, and there are many different ways to protect your network.

There are two main types of network security: **physical** and **virtual**.

- Physical security is the process of physically protecting your network from unauthorized access.
- Virtual security is the process of protecting your network from unauthorized activities such as malicious software and hackers.

Both physical and virtual security can be implemented in different ways, and it is essential to choose the right approach for your organization.

The most common approach is to use locks on your computer or network ports to prevent unauthorized access. In addition, you can also use software such as antivirus software to protect your network from malicious software.

The Role of network security includes the following:

1. Scanning the network for viruses, Trojans, and other malicious software.
2. Creating new rules to protect against malware infections.
3. Monitoring the network for suspicious activity such as suspicious email attachments or suspicious website behaviour.
4. Keeping up-to-date with best practices in network security such as best practices in firewall configuration and anti-virus scanning.

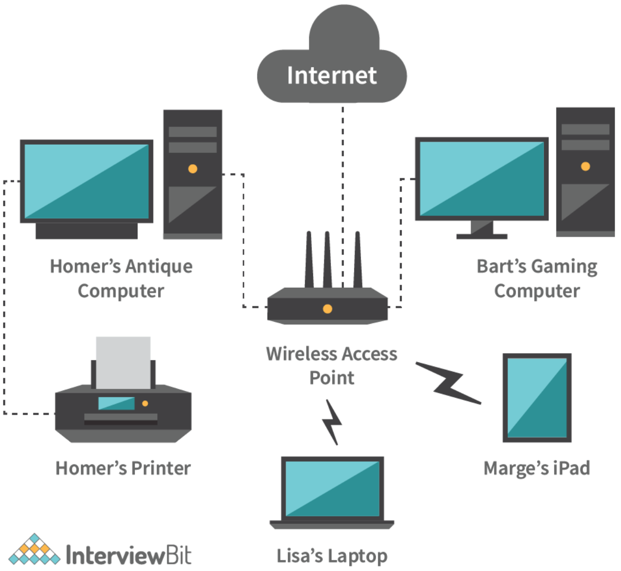
There are also other ways to protect your network besides physical security. For example, you can use virtual security to protect your network from unauthorized activities such as malicious software and hackers.

In this article, we'll answer the most common interview questions about network security. There are many different types of network security jobs, and the variety only increases as new and ever-changing threats emerge. You might want to choose a speciality like information security or network security, but the truth is that almost any job market requires you to know a little bit about digital defence in order to succeed. Fortunately, there are a number of good resources available to help you prepare for an interview by learning more about what you'll be working on. Below we've compiled some of our top resources for preparing for network security interviews.

Network Security Interview Questions for Freshers

1. What is a network?

A **network** is a set of interconnected computers and other devices that allows information to flow between them. This is the process of connecting these devices and allowing them to communicate with each other. One of the most important aspects of networking is the ability to share data. The Internet is a huge network that allows people to share information and communicate with each other. By sharing data, people can access information more efficiently and get it faster. Another important aspect of networking is security. Networking is a risky activity because there are many unknowns that can happen. For example, if someone hacks into your computer, you could lose all of your data. If someone steals your identity, you could be in trouble.



2. What is a protocol?

A protocol is a set of rules that govern how two or more parties interact with each other. It is a way of specifying how data should be exchanged between two or more parties. Protocols are often used to control the flow of data, such as when sending emails or transferring files.

The most common type of protocol is the HTTP protocol, which defines how to exchange data between a web server and a web browser. HTTP is used by many websites to transfer data such as images, videos, and text.

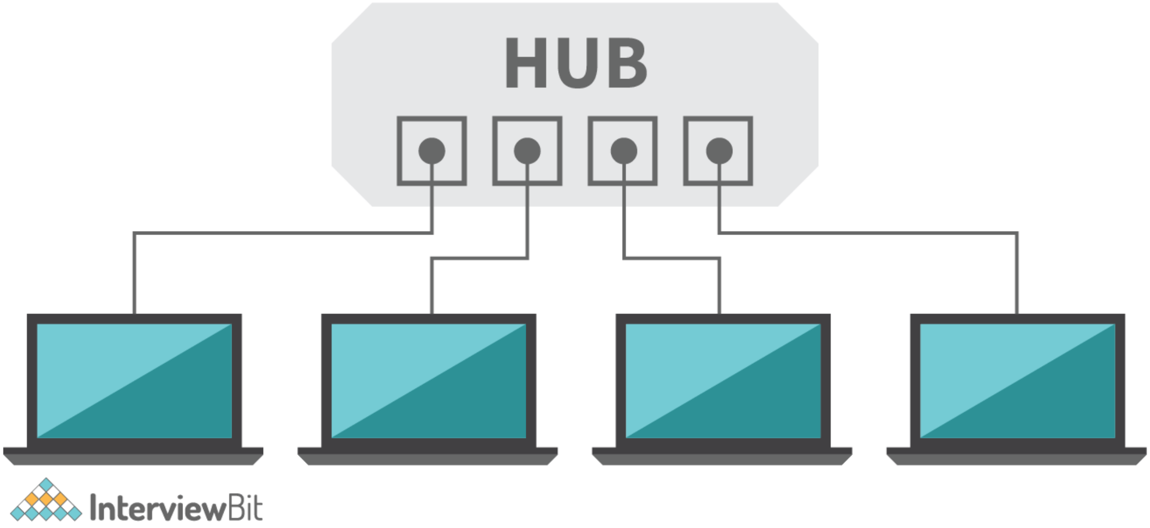
3. What is pipelining?

Pipelining is a method of software development that involves writing and testing multiple versions of a software program at the same time. The process is similar to parallel processing, but it works on a more granular scale. Instead of writing one program, you write multiple programs that can run in parallel. The result is that you can write a new version of the program in just a few hours instead of weeks or months.

When you use pipelining, you write multiple versions of your software program at the same time. Each version is tested and developed separately. When all the programs are completed, the final version is run all at once.

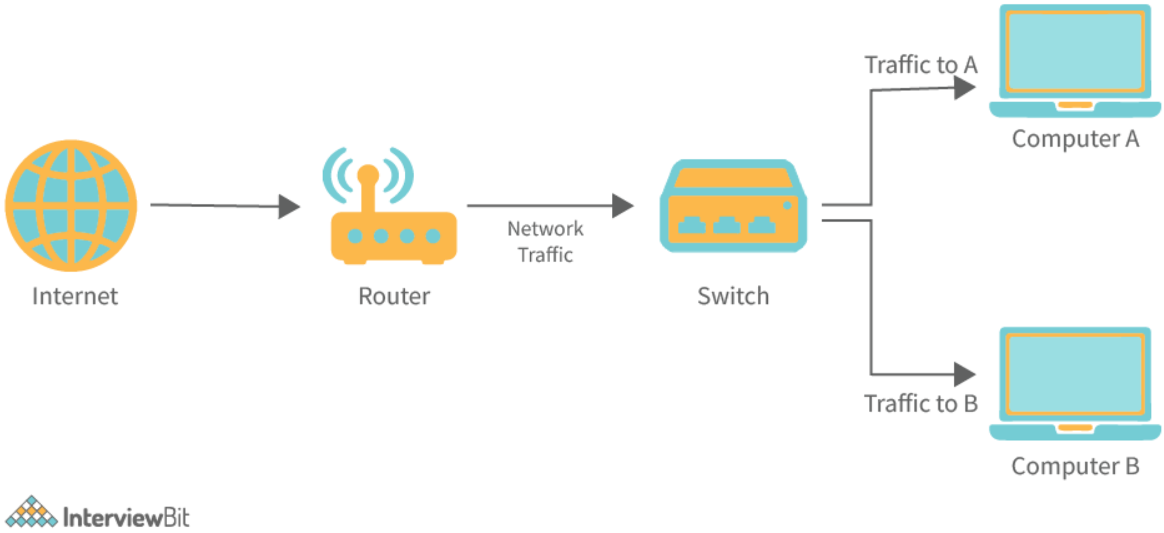
4. What is the hub in networking?

Hubs are nodes in a network that is responsible for connecting other nodes. Hubs are often the first point of contact for new nodes, and they are also the first point of entry for external resources, such as software updates and customer service.



5. What is a switch in networking?

Network devices (especially switches) that connect devices in a local area network (LAN) and pass data between them. A switch forwards data packets between devices connected to the same port, but not between ports on different devices or to other networks. A router, in contrast, forwards data packets between networks. A switch sends only to the device it is intended for (another switch, a router, or a user's computers).



6. What is simplex in networking?

In a Simplex operation, a single signal is transmitted and continuously goes in the same direction. The transmitter and receiver operate on the same frequency. When two stations transmit to each other on the same frequency at the same time, the mode is known as half-duplex (not simultaneous). Half-duplex, however, is commonly known as Simplex (not simultaneous).

Sometimes, at high and microwave wireless frequencies, simplex or half-duplex mode will not be adequate for providing enough range for communications. To increase the effectiveness of the range, wireless repeaters are employed. There are several different frequencies that the incoming signal might be than the outgoing signal, thus preventing the transmitted signal from overwhelming the repeater receiver. Repeaters, strategically positioned at significant locations with wide line-of-sight coverage areas, may greatly enhance the range of a wireless communications system.

7. What are the factors that affect the performance of the network?

The performance of a network is dependent on a number of factors, including the quality of the hardware, the speed of the internet connection, and the amount of traffic that is being transferred. The speed of the internet connection is important because it affects how quickly data can be transferred. A high-speed connection can transfer data at a much higher rate than a low-speed connection.

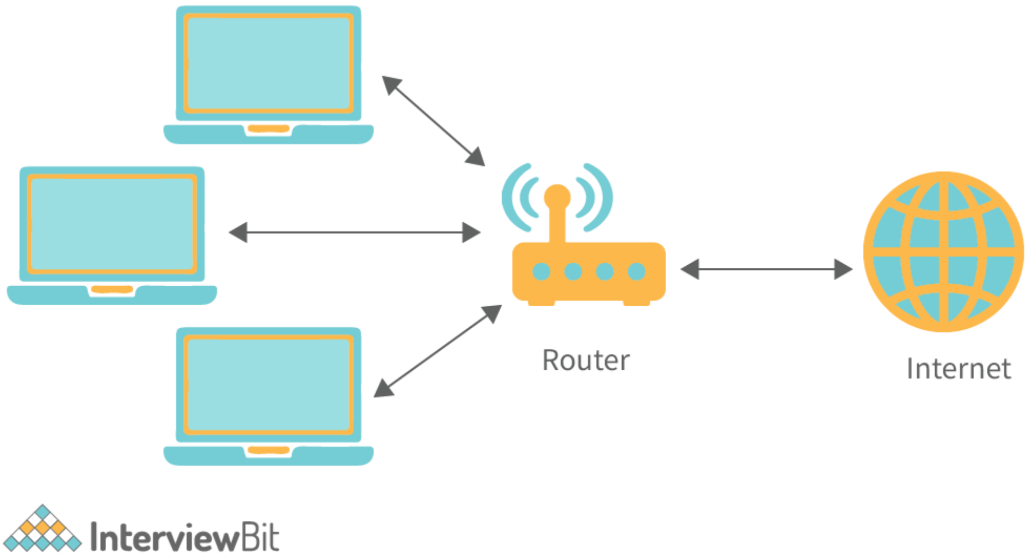
The quality of the hardware also affects the performance of a network. Poorly-made hardware can cause problems with connectivity and performance. Finally, traffic can affect the performance of a network. If too much traffic is being transferred over a network, it can slow down the performance of the network. So, if you want to improve your network's performance, you should make sure that all of your equipment is up to date and that you are using the best possible internet connection.

8. What is LAN in networking?

Personal computers and workstations may share data, tools, and programs via a local area network. A switch or series of switches interconnects network devices so that computers and workstations may share data, tools, and programs. Private addressing is used in conjunction with the TCP/IP protocol to establish a local area network. A router connects the local area network to the wider internet.

The amount of data that can be transmitted at any given moment is limited by the number of computers connected, which means that the hardware (such as hubs, network adapters, and Ethernet cables) must be inexpensive and fast (i.e., hubs, network adapters, and Ethernet cables). Due to their small size, LANs (which are privately owned) cannot be used for much beyond an office building, home, hospital, school, etc. To build and maintain a LAN, twisted-pair cables and coaxial cables are typically used. The distance covered is also limited, so noise and error are minimized.

In the early days of LANs, data rates usually ranged from 4 to 16 Mbps. Today, 100 Mbps and 1000 Mbps speeds are more common. Because of the short path between computers in a LAN, the delay is very short. A LAN may be connected with up to thousands of PCs, even if wired connections are the primary means of communication. A LAN may include both wired and wireless connections to provide greater speed and security. A LAN can be more stable and have fewer congestion issues than a typical network. For example, in a single room where several Counter-Strike players are playing (without internet access).

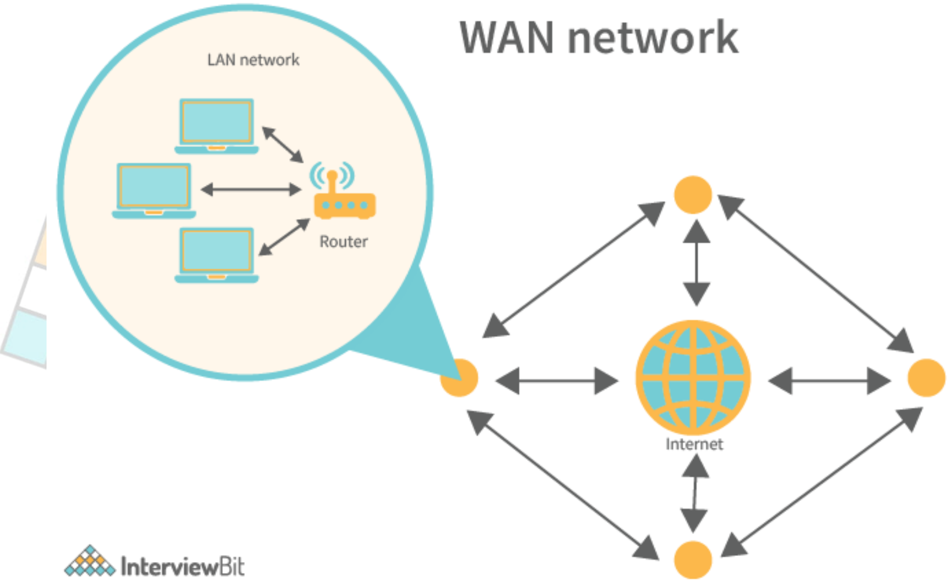


9. What is WAN in networking?

WANs, also known as wide area networks, connect LANs over telephone lines and radio waves to form computer networks that cover a large area, even though they might be confined to a single country or state. Enterprises, governmental agencies, and other organizations may connect to WANs. WANs are fast and costly to operate.

WANs are difficult to design and maintain, with switched WAN and point-to-point WAN being the two types. A WAN is less fault-tolerant and has more congestion in the network than a MAN. Telephone lines or satellite links are used for communication. WANs are prone to long-distance noise and errors.

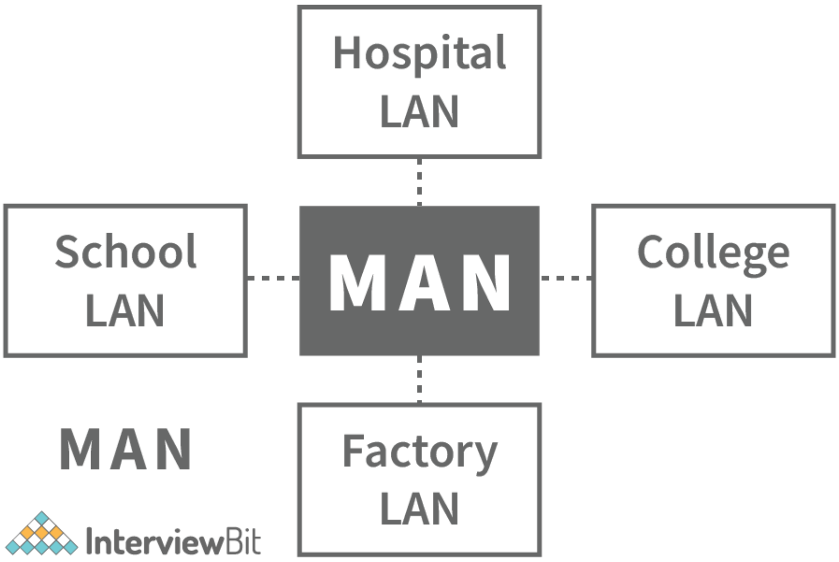
WAN data rates are slower than LAN data rates, because of the increased distance and increased number of servers and terminals involved, plus slower speeds. WAN speeds range from Kbps to Mbps, whereas LAN speeds typically range from Mbps to Gigabits per second (Gbps). The biggest obstacle is the propagation delay. Devices are utilised for WAN transmission in addition to Optic wires, microwave emissions, and satellites. Switched WANs include Asynchronous Transfer Mode (ATM) networks and Point-to-Point WANs, which connect a home computer to the Internet via a telephone line.



10. What is MAN in networking?

Compared to a WAN, a MAN connects different computers that are in two or more cities, but are physically separated. It is used to provide high-speed connections. It is large in geographic scope and may function as an ISP (internet service provider). MAN connections range from Mbps. It is difficult to establish and maintain a MAN network due to its complexity.

MANs are less reliable and more congested. They are costly and may or may not be controlled by a single organisation. Data transfers through MANs are fast but there is a low amount of data. Modems and wire/cable are used for transmission of data. A MAN is a portion of a telephone company network that provides a DSL line to a customer or a city's cable TV network.



11. What is the internet?

Almost everyone uses the internet as their most important resource and tool. Internet connects millions of computers, webpages, websites, and servers. We may communicate with our loved ones via email, photos, videos, and messages via the internet. We may also share and get information online via the internet. When we have a device that is connected to the internet, we can use all of our applications, websites, social media apps, and more services. Sending and receiving information on the internet has become very fast in recent years.

12. What is an intranet?

An intranet is a sort of closed network. It is used by a variety of firms and is accessible only by its employees. Intranets are networks that allow PCs from several corporations to communicate with each other. An intranet is a private network that allows access only by its members and employees. Many corporations and companies have their very own intranet networks, which are accessible to only their employees and clients. Because an intranet is a closed network, it does not pass information to the outside world and protects your data.

13. What is Access control in networking?

Access control is the process of restricting access to systems, resources, or information. A set of rules determine who may access what aspects of a system, what materials may be used, and who may enter a computing environment. It is a fundamental security concept that protects an organisation from danger.

Access control is the process of restricting access to systems, resources, or information. A set of rules determine who may access what aspects of a system, what materials may be used, and who may enter a computing environment. It is a fundamental security concept that protects an organisation from danger.

14. What is Application security in networking?

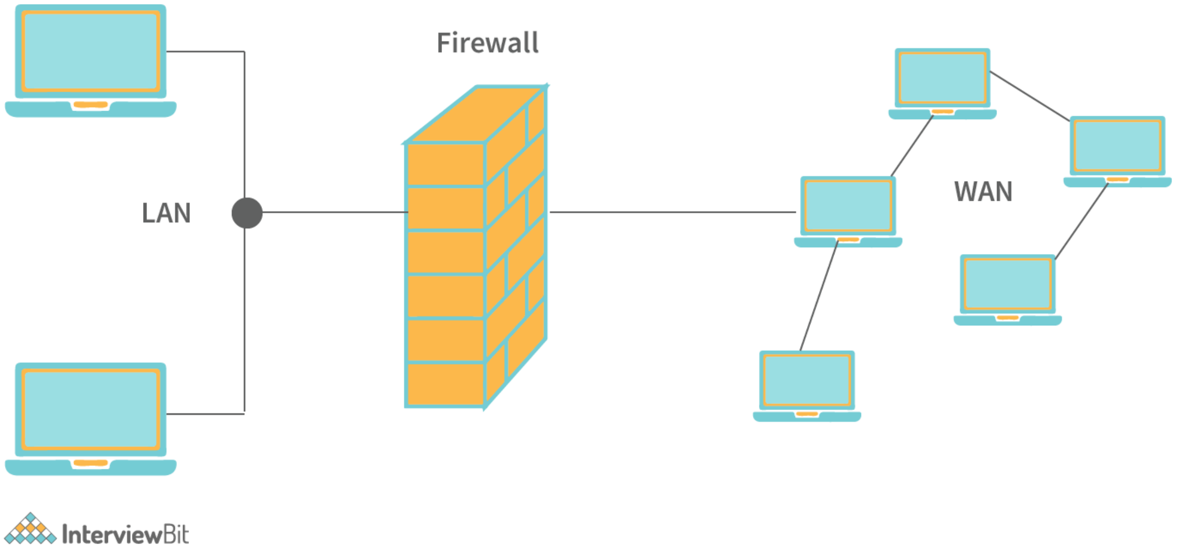
An application security program identifies, repairs, and eliminates vulnerabilities in applications within an organisation. Application security is all about finding, dealing with, and fixing vulnerabilities in applications. Application vulnerabilities that match with CWEs are identified and fixed. A weakness in the application is discovered and prevented from being exploited in the future.

15. What is Firewalls in networking?

A firewall monitors all incoming and outgoing traffic and matches a set of security rules to determine whether to accept, reject, or drop a packet.

When a rule is matched, an action is performed on the network traffic. For example, a firewall table might match network traffic against a rule specifying that employees from the HR department are forbidden from accessing data from a code server, and another rule may specify that system administrators are permitted to access both HR and technical data. A firewall can be designed to suit the organisation's security and efficiency needs by combining rules.

A firewall operates in two phases. It blocks both outgoing and incoming network connections. On the one hand, a firewall allows outgoing connections from a server. In this case, outgoing connections are permitted from a firewall's perspective. On the other hand, it is always best to set a firewall rule to block outgoing connections. This is because doing so will improve security and prevent unwanted communication. As mentioned above, ICMP messages are the most common type of incoming traffic. They have a source IP address and a destination IP address. Port numbers are also included in TCP and UDP communications. In the case of incoming ICMP packets, the type of message is used as opposed to a port number.



16. What is Network segmentation?

A subnet can be created by dividing a network into multiple segments or subnets, each of which acts as a separate little network. Controlled traffic flow between subnets is possible by using this architectural technique. In addition to improving monitoring, boosting performance, localizing technology problems, and most importantly, enhancing security, segmentation is employed by businesses.

Network security personnel have an effective tool in preventing important assets, such as customers' personal information, corporate financial records and important intellectual property, from being exploited by malicious outsiders or curious insiders by means of network segmentation. These assets are frequently located in hybrid and multi-cloud environments, which have to be protected against hacking attempts. To know the security impact of segmentation, it is crucial to comprehend the nature of trust among network security.

17. What is Virtual Private Network?

A virtual private network (VPN) is a secure connection over an unsecure network, such as the internet. A VPN service creates a safe and encrypted connection across an insecure network like the internet. A VPN connects a private network with a public network like the internet to extend the network. The term "virtual private network" implies that the network is accessible by users sitting in the remote area. It uses tunneling protocols to create a secure connection.

Consider a scenario where a bank's corporate office is located in Washington, USA and uses a local network of 100 computers. Mumbai and Tokyo branch offices are used to connect with the head office using a leased line, a costly and time-consuming process. Using VPN, we can eradicate this challenge in a powerful way.

18. What is Web Security?

The security of a network or computer system is concerned with protecting it from damage or theft of software, hardware, or data. Computer systems are protected from misdirection or disruption of their services.

Website protection is known as web security and also includes cloud protection and web application security. It defends cloud services and web-based applications, respectively. A virtual private network (VPN) is also safeguarded.

To operate any business that uses computers, web security is critical. If a website is compromised or hackers can manipulate your software or systems, your website—and even your entire network—can be halted, resulting in business disruptions.

19. What is Wireless security?

Wireless networks provide several advantages to users, but they are really complicated to operate. Data packets travelling through wires provide users with the assurance that data sent through wire will unlikely be overheard by eavesdroppers.

We should focus on the following areas to ensure a secure wireless connection: Identifying the endpoint of the wireless network and the end users, protecting wireless data packets from middlemen, ensuring wireless data packets are intact, and keeping the wireless data packets anonymous.

All 802.11 wireless devices communicate with one another, regardless of their manufacturers. Whenever all wireless devices conform to the same standards, there is no problem. However, some rogue devices may be a danger to wireless security, as they may intercept our confidential data or cause the network to go down.

20. What is Mobile device security?

Mobile security protects the infrastructure, software, and strategy behind mobile devices that travel with users. Mobile devices, including smartphones, tablets, and laptops, must be protected from cyberattacks. Mobile devices are becoming more popular than their stationary counterparts, so they are becoming bigger targets for hackers.

As more workers and consumers use mobile devices for internet browsing, mobile devices have become an integral part of their daily lives. Mobile devices have evolved from desktop-only internet browsers to being the preferred method of browsing the internet. Laptop-toting travellers are now the exception rather than the norm. Browsing on mobile devices has become the primary form of internet usage, and mobile web traffic has overtaken desktop internet usage.

Mobile devices pose a greater danger to corporate security than stationary computers do. Mobile devices are more vulnerable than stationary computers to both physical and virtual attacks. Since mobile devices are mobile and can be used anywhere, they are more susceptible to theft and loss than stationary devices. Besides the physical and virtual threats posed by third-party applications and Wi-Fi hotspots, administrators must be on the lookout for the possibility of man-in-the-middle attacks. With mobile devices, users can root them, install any app, and lose them physically.

Mobile devices pose a significant threat to data integrity, for which corporations have to invest a lot more in strategies. Even with the expense, it's a critical component of cybersecurity.

Network Security Interview Questions for Experienced

21. Explain the basic working of network security?

A network security measures and procedures, hardware and software solutions, and set of rules and standards for network access and security. The phrase describes all the approaches to safeguarding a network and its data from intrusions and other dangers.

Network security involves blocking access to computer programs and networks, identifying and eliminating viruses, protecting data through encryption, and monitoring traffic.

An effective network security plan safeguards client data, keeps shared information secure, and ensures reliable network access and performance. It reduces overhead expenses and safeguards organisations from costly data breaches or other security incidents. Companies must protect themselves from cyberthreats by ensuring legitimate access to systems, applications, and data.

22. What is Intrusion Prevention System in network security?

An intrusion protection system (IPS) is a network security device (either hardware or software) that monitors a network for illegal activity and blocks, blocks, or drops it if it occurs, in addition to reporting it.

An IDS, which merely detects malicious activity without taking action, is more advanced than an intrusion prevention system (IPS). A next-generation firewall (NGFW) or unified threat management (UTM) solution may include an intrusion prevention system (IPS). Strong enough to examine a large volume of traffic without slowing down network performance, they are amongst the most common network security solutions.

23. What is network encryption?

SSL (also known as transport layer security [TLS]) is the standard network protection technology used to symbolise a secure connection in a user's internet browser (the padlock). Network data protection standards SSL (secure sockets layer) and Layer 2 VPN (virtue layer VPN) have become common worldwide thanks to their recognisable sign. They are utilised by many businesses that desire to ensure their safety and security as well as their internal networks, backbone networks, and virtual private networks (VPNs).

Network-level data encryption is a fairly blunt weapon at the low level. Information flowing over the network is almost completely oblivious to the value of the data, and this context is almost always set to protect everything. Even when the “protect everything” strategy is used, network traffic patterns can provide valuable information to potential attackers.

Network data encryption is only part of a complete data security strategy. An organisation must also consider the risks associated with data generation and consumption to ensure the best possible result. Driving on the freeway at high speed is much easier than in a parking lot or private garage!

24. What are the benefits of a firewall?

- A firewall must monitor all data moving through a network to ensure it is not infected with malicious code. It monitors every packet and determines whether it contains any dangerous content. If it does, it blocks it immediately.
- A Trojan is harmful to a user because it hides on a computer and monitors everything you do. It may see everything you do on your computer, including your personal information. When your computer behaves strangely, it is probably because it is being controlled by a Trojan. A firewall will block Trojans immediately once they enter your system.
- Computer hackers on the internet look for vulnerable computers in order to carry out illegal acts. When they find such computers, they will begin to execute harmful applications such as computer viruses. There may also be unknown individuals looking for open internet connections, such as the neighbours. In order to prevent these incidents, it is critical to be protected by a firewall security system.
- A firewall can block certain hosts and services from accessing the system in order to prevent hackers from exploiting them. The best course of action is to block these hosts from accessing the system. If a user feels that they need protection from these types of unwanted access, this access policy may be enforced.
- Privacy is one of the primary concerns of an online user. Hackers look for details about the user's privacy in order to learn about it. A firewall, for example, can block many of the services offered by a website such as the domain name service and the finger. As a result, hackers are unable to obtain user information. Firewalls may also block DNS information, preventing the attacker from obtaining the website's name and IP address.

25. What is a Proxy firewall?

A proxy firewall protects network resources by filtering packets at the application layer, rather than the network or transport layers. However, applications may slow down and functionality may be affected by using one.

Traditional firewalls do not focus on decrypting traffic or inspecting application protocol traffic. As a result, only a small portion of the threat landscape is covered by IPSs or antivirus solutions.

Proxy servers act as a conduit between two networks, providing an intermediary between computers and servers on the internet so that secure data may be passed back and forth. A proxy server blocks, filters, archives, and manages requests from devices in order to protect networks from cyberterrorism and unauthorised access. It decides which traffic is permitted and denied and detects signs of a cyberthreat or malware intrusion.

26. What is a UTM firewall?

A single device within your network provides multiple security functions and services. With UTM, your network users are protected with a variety of security functions, including antivirus, content filtering, email and web blocking, and anti-spam, to name a few.

Bringing together all of an organisation's IT security services into one device may simplify the protection of the network. It is possible to monitor all dangers and security-related activity with a single pane of glass through your business. You get comprehensive, simplified access to all aspects of your security or wireless framework with this approach.

27. Explain Stateful Inspection?

Stateful inspection also known as dynamic packet filtering is a firewall technology that monitors the state of active connections and allows network packets through the firewall based on this information. In contrast to stateless inspection, stateful inspection is well suited to static packet filtering and can also support UDP and similar protocols. However, it can also handle TCP and other protocols like it.

Check Point Software Technologies (CPST) developed the technique for stateful firewall technology in the early 1990s to overcome the limitations of stateless firewall technology. Since then, stateful firewall technology has become a prevalent industry standard and is one of the most popular firewall technologies in use today.

28. Why does an Active FTP not work with network firewalls?

A firewall is established by typing a port number (or a range of port numbers) and an incoming or outgoing direction of traffic (active or passive FTP) into the rules. These two types of traffic require two different rules. A firewall must have two different rules for active FTP in order to allow these two kinds of traffic. The initiator in a push is external, whereas the initiator in a pull is internal. Active FTP is a unique application of ftp that requires different configurations.

29. What is a DDoS attack?

An internet traffic flood is used to prevent users from accessing connected online services and sites in a DDoS Attack. DDoS attacks are often motivated by a range of reasons, including hacktivists seeking to damage a company's servers for fun or to demonstrate cyber vulnerabilities, as well as individuals who are annoyed by a company's services. A competitor may disrupt or shut down another business's online operations to steal business away or to obtain money through extortion. A hostageware or ransomware infection on their servers may be forced them to pay a large financial sum to have the damage repaired.

A financially motivated distributed denial-of-service attack is one in which a competitor disrupts or shuts down another business's online operations to steal business away in the meanwhile. Even the largest multinational corporations are not immune to being "DDoS'ed", rising DDoS attacks. An enormous attack occurred in February 2020 on Amazon Web Services (AWS), which toppled an earlier attack on GitHub two years before. DDoS attacks can lead to a drop in legitimate traffic, loss of business, and reputation damage.

30. What is Ransomware?

A ransomware threat encodes data, usually encrypting it, until the victim pays a ransom to the attacker. In many situations, the ransom demand comes with an expiration date. If the victim doesn’t pay in time, the data is irretrievable or the ransom is increased, the demand is fulfilled. Ransomware attacks are common these days. Businesses all over North America and Europe are victims of ransomware.

Cybercriminals target consumers and enterprises of all stripes. In addition to the FBI, several government agencies, including the No More Ransom Project, recommend avoiding paying the ransom to avoid encouraging the ransomware cycle. Furthermore, half of those who pay the ransom will likely be targeted again by ransomware, especially if the infection is not removed from the system.

31. What is Malware?

A malicious software is a harmful computer program that hackers use to wreak destruction and gain access to sensitive information. Microsoft defines malware as any software that damages a single computer, server, or computer network. It refers to software rather than the manner in which it was developed. Because malware is employed for a particular purpose rather than a specific technology or tactic, it is distinguished by its functionality rather than its origin.

All instances of malware are also instances of viruses, but not every instance of malware is an instance of a virus (because viruses are just one type of malware).

32. What is Spyware?

Spyware is a kind of malware that enters your computer or mobile device and gathers information about you, including the sites you visit, the stuff you download, your username and password, payment information, and email correspondence. It's no surprise that spyware is sneaky. It sneaks into your computer without your permission or knowledge and joins your operating system. You may even agree to the terms of a seemingly legitimate program without reading the fine print, in which case spyware may be installed on your computer. Despite the various methods spyware can utilise to infiltrate your computer, the method of operation is always the same—it runs quietly in the background, staying secret, gathering data or monitoring your activity in order to inflict harm on your machine or your activities. Even if you discover its undesirable presence on your machine, Spyware does not have an easy uninstall feature.

33. What is Adware?

Adware is a type of malware that displays unwanted advertisements on your computer or mobile device. Adware is commonly installed on computers and mobile devices without the user's knowledge. When users try to install legitimate applications, adware is often activated. Some pop-up windows display advertisements without collecting data or infecting your computer, but some pop-up windows are designed to target you with customised adverts. It is possible for adware to direct you to malicious websites and infected pages via advert links, putting you at risk of computer viruses.

34. What is Phishing?

Some pop-up windows display advertisements without collecting data or infecting your computer, but some pop-up windows are designed to target you with customised adverts. It is possible for adware to direct you to malicious websites and infected pages via advert links, putting you at risk of computer viruses. A phishing email is sent to trick the victim into giving up sensitive information, such as credit card numbers and logins. This type of cybercrime is common, and everyone should be aware of it. It is accomplished through email. Malware can also be installed on a victim's machine in a phishing attack.

35. What is the use of a VPN?

A VPN service can increase your online security, anonymity, and freedom, all without having to sacrifice any of them. It's a straightforward and quick method of doing so. When using the internet, your device constantly sends data to other sites in order to exchange information. A VPN creates a secure tunnel between your device (e.g. mobile or laptop) and the web. Using a VPN, you may send data across a secure, encrypted connection to an external server: the VPN server. From there, your information will be delivered to its destination on the web. Securing your data and hiding your online identity are just a few of the advantages of rerouting your internet traffic through a VPN server.

36. What is traceroute?

By using tools for network diagnostics, known as traceroute, administrators can trace the path data packets take from their source to their destination, thus finding connectivity problems. On a Windows machine, tracert is the command; on Linux and Mac, it is traceroute. Traceroute and tracert both function similarly; they trace the route data takes from one location in a network to a specific IP server. Traceroute records the name and IP address of each intermediate device that a data packet must traverse in order to reach its destination. It then provides the round-trip time (RTT) and the device name. You can use traceroute to determine where a problem is occurring, but it alone can't tell you if there is one. To help you determine if there is a problem, ping can be used. Imagine that you're trying to visit a website and pages take a long time to load. If you use traceroute to determine where the longest delays are occurring, you can determine where the problem is.

37. What is Port Scanning?

A port scan is a method for discovering which ports are open on a machine or network. To test whether someone is at home before knocking on the door, you could port scan the system or network. It reveals which ports are open and accepting information, as well as shows if firewalls are installed between the source and target. Fingerprinting is the term used to describe this technique. As a result, it can also be an ideal reconnaissance tool for attackers seeking to discover a network's weakest point of entry. It is also used to test network security and the firewall's strength. Port scanning is a standard technique employed by hackers to discover open doors or weak spots in a network. A port scan attack may help cyber criminals discover available ports and determine whether they are sending or receiving data. It may also reveal whether security systems like firewalls are being used by a company. When hackers contact a port, the response they receive determines whether the port is being used and whether potential vulnerabilities exist. A business may also scan ports using this technique and analyze the response for potential vulnerabilities. They may then employ tools like IP scanner, network scanner (Nmap), and Netcat to ensure the security of their network and systems.

38. What is port blocking within LAN?

An Internet Service Provider (ISP) blocks Internet traffic by using the port number and transfer protocol. Blocking certain types of ports within a local area network is known as port blocking. Blocking ports on plug-and-play devices such as USB flash drives, removable devices, CD/DVD/CD-ROM, floppy, and mobile devices like smartphones is among the reasons for port blocking.

Suppose your network has DHCP service enabled. When a user connects their laptop to your device, they can obtain your IP address from the DHCP and gain access to your network resources. This is why you should turn on port security if you can to prevent ports from conflicting with MAC addresses and allowing anonymous users to obtain an IP address.

39. What is a Botnet?

A botnet is a group of computers that has been taken over by a bot, or a robot-controlled computer network. Multi-layered computer schemes are often used to infiltrate and assemble a botnet. Massive data theft, server crashes, and malware distribution are just a few of the automated tasks that bots are capable of completing.

A botnet is a group of infected devices used to scam other users or cause disruptions without the victims’ consent. The “what is a botnet attack and how does it work?” query is appropriate here. To assist you in understanding how botnets are created and employed, we'll demonstrate how they're made.

40. What is secure remote access?

A secure remote access process or solution may include security procedures such as VPN, multifactor authentication, and endpoint protection, among others. It is designed to keep crooks away from an organisation's digital assets and safeguard sensitive information. Remote access may be protected via VPN, multifactor authentication, or endpoint protection.

Today's IT environment, which is facing a rapidly changing threat landscape and the growing number of remote workers as a result of the Covid pandemic, demands secure remote access. In order to succeed, users must be educated, strong cybersecurity policies must be implemented, and best security hygiene practices must be developed.

Conclusion

Network security is the protection of information and data in a network. It is the protection of data that is stored on a computer or network server from unauthorized access, modification, or theft. Network security is an important part of protecting your organization's data and systems. It can help to prevent cyber attacks and protect critical infrastructure from damage.

In order to be successful in a security interview, you need to have a solid understanding of the basics of security. This includes understanding the basic concepts and principles of security, including how to secure your network and how to protect your data. You also need to know what types of threats you face, how you can detect and prevent them, and how you can protect yourself from them. In addition, you should also understand what types of vulnerabilities are present in your system and how they can be exploited.

For example, if you have a lot of sensitive data stored on your computer or network, this might make it easier for hackers to gain access to your system. In this case, it is important that you understand the risks and benefits of different types of systems.

Finally, it is important that you know how to perform various tasks on your system and how they can be performed safely. This includes setting up network settings (for example, firewall rules), configuring services (for example, web browser or file transfer programs), managing devices (for example, computers or printers), and managing user accounts (for example, logging into social media accounts).

Important Interview Resources

- https://www.interviewbit.com/blog/security-engineer-salary/
- https://www.interviewbit.com/blog/cyber-security-projects/
- https://www.interviewbit.com/blog/network-architecture/
- https://www.interviewbit.com/cyber-security-interview-questions/
- https://www.interviewbit.com/computer-network-mcq/
- https://www.interviewbit.com/technical-interview-questions/

Links to More Interview Questions

- C Interview Questions
- Web Api Interview Questions
- Cpp Interview Questions
- Machine Learning Interview Questions
- Css Interview Questions
- Django Interview Questions
- Operating System Interview Questions
- Git Interview Questions
- Dbms Interview Questions
- Pl Sql Interview Questions
- Ansible Interview Questions
- Php Interview Questions
- Hibernate Interview Questions
- Oops Interview Questions
- Docker Interview Questions
- Laravel Interview Questions
- Dot Net Interview Questions
- React Native Interview Questions
- Java 8 Interview Questions
- Spring Boot Interview Questions
- Tableau Interview Questions
- Java Interview Questions
- C Sharp Interview Questions
- Node Js Interview Questions
- Devops Interview Questions
- Mysql Interview Questions
- Asp Net Interview Questions
- Kubernetes Interview Questions
- Aws Interview Questions
- Mongodb Interview Questions
- Power Bi Interview Questions
- Linux Interview Questions
- Jenkins Interview Questions