Continue

Picture this: you're attending a CCNA interview and being asked questions like, How do you configure a router? or What steps would you take to secure a network? Stepping into the world of CCNA interviews can feel like navigating a maze, but with the proper preparation, you can find your way with ease. Our blog on Top 73 CCNA Interview Questions and Answers is your ultimate guide to mastering the interview process. With our carefully curated list of CCNA Interview Questions, you'll be ready to tackle any challenge that comes your way. This blog is designed to help you understand the core concepts and provide clear, concise answers. Let's dive in and land your dream job! Table of Contents 1) CCNA Interview Questions and Answers for Beginners 2) CCNA Interview Questions and Answers for Intermediates 3) Advanced and Scenario-based CCNA Interview Questions and Answers 4) Conclusion CCNA Interview Questions and Answers for Beginners Here is a list of the top 20 CCNA Interview Questions along with their answers: 1) What is a MAC Address? Answer: A Media Access Control (MAC) address is a unique identifier assigned to a Network Interface Card (NIC) by the manufacturer. It is a 48-bit hexadecimal value used for communication at the data link layer of the Open Systems Interconnection (OSI) OSI model. 2) What is the Difference Between a Switch and a hub? Answer: A Hub, operating at the physical layer of the Open Systems Interconnection (OSI) model, broadcasts data to all connected devices. Conversely, a Switch functions at the data link layer, establishing dedicated connections for more efficient and secure communication. 3) Define the Concept of a Subnet Mask? Answer: A subnet mask is a 32-bit value used to determine the network and host portions of an IP address. It is applied to an IP address to identify the network ID and host ID within that network. 4) What is the Purpose of Address Resolution Protocol (ARP)? Answer: ARP maps an IP address to a MAC address on a local network. It allows devices to discover and communicate with each other at the data link layer using MAC addresses. 5) What is a Default Gateway? Answer: The default gateway is the IP address of the router or layer 3 switch that connects a local network to external networks. It is used to forward traffic destined for networks outside the local subnet. 6) What is a VLAN? Answer: VLAN is the acronym for Virtual Local Area Network, which is a logical grouping of devices on a network, regardless of their physical location. It allows for network segmentation and isolation, enhancing security and Network Management. 7) What is the Purpose of a Domain Name System (DNS)? Answer: DNS is used to translate human-readable domain names (e.g., www.example.com) into IP addresses. It enables users to access resources on the internet using domain names instead of remembering IP addresses. Understanding DNS is essential for the CCNA syllabus. 8) What is a Router? Answer: A Router is a network device that connects multiple networks and directs traffic between them based on IP addresses. It operates at the network layer of the OSI model. 9) What is the Difference Between TCP and UDP? Answer: Transmission Control Protocol (TCP) provides reliable, connection-oriented communication with error-checking and flow control. User Datagram Protocol (UDP) provides faster, connectionless communication without error-checking or flow control. 10) What is the Purpose of Dynamic Host Configuration Protocol (DHCP)? Answer: DHCP is used to automatically assign IP addresses, subnet masks, default gateways, and other network configuration parameters to devices on a network. It helps eliminate the need for manual IP configuration. 11) What is a Loopback Address? Answer: A loopback address is a special IP address used to test network connectivity on the local device. Packets sent to the loopback address are not transmitted on the network. This ensures that the devices network interface is functioning correctly without involving external networks. 12) What is the Difference Between a Static and Dynamic Routing Protocol? Answer: A Network Administrator manually configures network routes in static routing. On the other hand, dynamic routing protocols allow routers to exchange routing information and automatically adjust routing tables based on network changes. 13) What is ICMP? Answer: Internet Control Message Protocol (ICMP) is a network protocol used for diagnostics and error reporting in IP networks. It includes functions such as ping (to test network connectivity) and traceroute (to trace the path of packets across a network). 14) What is a Broadcast Domain? Answer: A broadcast domain is a logical division of a network in which all devices receive broadcast messages. Devices within the same broadcast domain can directly communicate with each other using MAC addresses. This concept is crucial for the network engineer job description. 15) What is the Purpose of Network Address Translation (NAT)? Answer: NAT is used to translate private IP addresses to public IP addresses for communication over the internet. It allows multiple devices to share a single public IP address and provides an added layer of security. 16) What is the Difference Between Half-duplex and Full-duplex Communication? Answer: Data can be transmitted in both directions but not simultaneously in half-duplex communication. Only one device can send data at a time. On the other hand, in full-duplex communication, data can be transmitted simultaneously in both directions, allowing for faster communication. 17) What is the Spanning Tree Protocol (STP)? Answer: STP is a network protocol that prevents loops in a switched network by creating a loop-free logical topology. It determines the best path for traffic and disables redundant paths to avoid network loops. 18) What is the Purpose of the Access Control List (ACL)? Answer: ACLs control network traffic by filtering packets based on specified criteria. They permit or deny traffic based on source/destination IP addresses, protocols, ports, or other criteria. 19) What is a Default Route? Answer: A default route is a routing entry used when no specific route exists in the routing table for a particular destination. It directs packets to the default gateway for further routing. 20) What is the Purpose of VLAN Trunking? Answer: Virtual Local Area Network (VLAN) Trunking allows multiple VLANs to be carried over a single physical link between switches. Start your journey to becoming a Cisco Certified Network Associate with our CCNA Training! 21) What is Latency? Answer: Latency is used to describe the delay of time between when a network device receives a data frame and when the network device resends this data frame on another network segment. 22) What Causes Network Congestion? Answers: Network congestion occurs when an excessive number of users attempt to utilise a shared bandwidth simultaneously. This phenomenon mostly occurs in larger networks that lack the efficient practice of network segmentation. 23) Explain how Cut-through LAN Switching Works? Answers: In Cut-through LAN switching, upon receiving a data frame, the router quickly forwards it to the next network segment after analysing the destination address without delay. 24) Explain the Advantage of Using Switches? Answer: Utilising a Switch offers a more efficient data transmission method in comparison to broadcasting data across all ports. Switches transform the incoming signal into a frame. This is followed by accessing and decoding the destination address and finally directing the frame to the corresponding port. 25) What do Data Packets Consist of? Sample Answer: Within a Data Packet, many components are available, including details about the sender, information regarding the recipient, and the actual data being transmitted. Additionally, each Data Packet is tagged with a numeric identification number, which not only defines its sequential order but also defines it as a specific packet number. 26) What are the Different Types of Passwords Used in Securing a CISCO Router? Sample Answer: There are five distinct password types available, including enable secret, virtual terminal, console, and auxiliary. 27) Define Data Packets? Answer: A Data Packet serves as a compact data unit bundled for transmission across a network. Also known as Network Layer Packages, they play a crucial role in the operation of the IP protocol as they sum up networking information within each packet. Data Packets contain a wealth of critical information, including email messages, web data, and Voice-over-IP (VoIP) calls. This knowledge supports effective management of various network topologies, including ring network topology. Each Data Packet has a unique numeric identification number that not only defines its order but also assigns it a unique packet number. 28) Define MTU? Answer: The Maximum Transmission Unit (MTU) is the largest frame or packet size a network device can handle, typically set at 1500 bytes by default, matching the Ethernet standard. In data transmission, Transmission Control Panel (TCP) uses the MTU to determine the maximum packet size for efficient communication. CCNA Interview Questions and Answers for Intermediate Interviews for CCNA job roles within the Information Technology (IT) field will mandatorily assess your knowledge and understanding of technical terms and concepts across various difficulty levels, including those related to CCNA Router Configuration Commands Guide. Lets look at the top CCNA Interview Questions. 29) What is the Difference Between a hub, a Switch and a Router? Explain Their Respective Functions in a Network? Answer: A Hub is a simple networking device that connects multiple devices in a network, but it operates at the physical layer (Layer 1) and does not perform any intelligent data forwarding. A Switch operates at the data link layer (Layer 2) and forwards data within a local network based on MAC addresses. A Router operates at the network layer (Layer 3) and forwards data between different networks based on IP addresses. 30) What is the Purpose of Subnetting, and how Does it Help in Network Design and Addressing? Answer: Subnetting allows the division of a large network into smaller subnetworks, known as subnets. It helps in network design and addressing by: a) Efficiently utilising IP address space. b) Enhancing network performance by reducing network traffic. c) Improving Network Security by creating isolated subnets. d) Facilitating Network Management and troubleshooting. 31) Explain the Process of IP Address Allocation in IPv4. What are the Different IP Address Classes, and how are They Used? Answer: In IPv4, IP addresses are allocated based on different address classes: a) Class A addresses have the first octet reserved for network identification and can support a large number of hosts. b) Class B addresses allocate the first two octets for network identification and are suitable for medium-sized networks. c) Class C addresses allocate the first three octets for network identification and are typically used for small networks. d) Class D addresses are reserved for multicast addresses. e) Class E addresses are reserved for experimental purposes. Sign up for our Cisco Meraki Training and master the latest in cloud-managed networks boost your professional growth and confidence! 32) What is the OSI model? Describe the Seven Layers and Their Functions? Answer: The Open Systems Interconnection (OSI) model is a conceptual framework that standardises network protocols. Its seven layers and their functions are as: a) Physical Layer: Deals with the physical transmission of data over the network. b) Data link Layer: Provides error-free data transmission between adjacent devices. c) Network Layer: Handles logical addressing and routing of data between networks. d) Transport Layer: Ensures reliable data delivery and manages end-to-end communication. e) Session Layer: Establishes and maintains communication sessions between applications. f) Presentation Layer: Formats and encrypts data for proper representation and security. g) Application Layer: Provides network services to applications and end-users. 33) What is VLAN Pruning, and how Does it Work? Answer: VLAN Pruning is a technique used to optimise VLAN traffic within a network. It prevents unnecessary broadcast traffic from being forwarded to switches that do not have any ports belonging to the respective VLAN. VLAN Pruning operates by allowing the VLAN information to be shared among Switches through VLAN Trunking Protocol (VTP). When a Switch receives a broadcast, it checks the VLAN membership of the port and prunes any VLANs that are not active on the receiving switch, thus reducing unnecessary broadcast traffic. 34) What is the Purpose of a DHCP Relay Agent? Answer: A Dynamic Host Configuration Protocol (DHCP) relay agent is used to forward DHCP messages between DHCP clients and DHCP servers located on different networks. When a DHCP client sends a DHCP Discover message, the relay agent intercepts the broadcast, encapsulates it in a unicast packet, and forwards it to the DHCP server. The DHCP relay agent helps extend the reach of DHCP servers and allows clients in different network segments to obtain IP configuration information dynamically. 35) What is the Purpose of VLANs? How Do They Enhance Network Segmentation and Security? Answer: VLANs divide a single physical network into multiple logical networks, enhancing network segmentation and security by permitting the following: a) Isolating network traffic, limiting broadcasts, and improving network performance. b) Providing logical grouping of devices regardless of their physical location. c) Enabling easier Network Management and scalability. d) Enhancing Network Security by controlling access between VLANs and implementing VLAN-based policies. 36) What is the Difference Between Static NAT and Dynamic NAT? Answer: Static NAT and Dynamic NAT are both methods of translating private IP addresses to public IP addresses for communication with external networks. The main difference between them is as follows: a) Static NAT: It maps a private IP address to an available public IP address from a one-to-one basis. It provides a direct and fixed translation between private and public IP addresses. b) Dynamic NAT: It maps a private IP address to an available public IP address from a pool of addresses. The mapping is performed dynamically as needed, allowing multiple private addresses to share a limited number of public IP addresses. 37) Describe the Different NAT Types and Their Functionalities? Answer: NAT is a process that translates private IP addresses to public IP addresses and vice versa. Different types of NAT include Static NAT, Dynamic NAT, and Port Address Translation (PAT). Static NAT maps one private IP address to one public IP address, dynamic NAT maps multiple private IP addresses to a pool of public IP addresses, and PAT maps multiple private IP addresses to a single public IP address using different ports. 38) What are Some Common WAN Technologies Used for Interconnecting Remote Locations? Answer: Common WAN technologies include the following: a) Leased lines: Dedicated point-to-point connections provided by service providers. b) Multi-Protocol Label Switching (MPLS): A protocol for efficient data forwarding in WANs. c) Point-to-Point Protocol (PPP): A protocol for establishing a direct connection between two endpoints. d) Virtual Private Network (VPN): Provides secure remote access over public networks. 39) What is the Difference Between a Static IP Address and a Dynamic IP Address? When Would you use Each Type? Answer: A static IP address is manually assigned and remains constant, ideal for servers and critical infrastructure. In contrast, a dynamic IP address is automatically assigned by a DHCP server and can change over time, commonly used for client devices like computers and smartphones 40) What is a MAC Address, and how is it Different From an IP Address? Answer: A MAC address is a unique identifier assigned to a network interface card (NIC). It is a hardware-based address and operates at the OSI models data link layer. MAC addresses are represented as a combination of six hexadecimal pairs, separated by colons or hyphens. Unlike IP addresses, MAC addresses are assigned by the manufacturer and are typically permanent. 41) Explain the Concept of VLAN Tagging and its Significance in a Network? Answer: VLAN tagging is a method used to identify and differentiate VLAN traffic. It involves adding additional information, known as a VLAN tag or VLAN header, to Ethernet frames. VLAN tagging is significant because it enables the switch to distinguish between different VLANs and ensures that traffic is delivered to the appropriate VLAN members, even when multiple VLANs share the same physical network infrastructure. 42) What is the Purpose of a Subnet Mask, and how is it Used in IP Addressing? Answer: A subnet mask is a 32-bit value used to divide an IP address into a network portion and a host portion. It helps determine which part of an IP address represents the network and which part represents the host. By comparing the subnet mask with an IP address, devices can identify the network to which the IP address belongs and determine if the destination IP address is on the local network or a remote network. 43) What is Open Shortest Path First (OSPF), and how Does it Work? Answer: OSPF is a link-state routing protocol used to determine the best path for routing IP packets within a network. It operates by exchanging Link-State Advertisements (LSAs) among routers to build a complete map of the network topology. OSPF routers exchange information about their connected links, including their state, cost, and bandwidth. With this information, OSPF calculates the shortest path to each network destination using Dijkstra's algorithm. The OSPF routing table is then built based on this calculation, allowing routers to make informed routing decisions and efficiently adapt to changes in the network topology. 44) Explain the Concept of VPN and its Benefits? Answer: A Virtual Private Network (VPN) is a secure and encrypted connection between two points. It allows users or branch offices to connect to a private network over a public network, such as the internet. It creates a virtual tunnel between the user/device and the private network, ensuring that data transmitted over the connection remains secure and private. The benefits of VPN include: a) VPNs use encryption protocols to protect data from interception and unauthorised access. b) VPNs enable users to securely access network resources from anywhere, providing flexibility and mobility. c) VPNs eliminate the need for dedicated leased lines, as they utilise existing internet connections, resulting in cost savings. d) VPNs mask the user's IP address, making it difficult for others to track their online activities. e) VPNs can bypass geographic restrictions, allowing users to access region-restricted content or services. 45) How Does DHCP Work? Answer: DHCP is a network protocol used to automatically assign IP addresses and network configuration parameters to devices on a network. Its working is to simplify network administration and eliminate the need for manual IP address configuration. DHCP works by using a DHCP server to lease IP addresses to client devices, along with other network configuration details such as subnet mask, default gateway, and DNS server addresses. 46) What is the Purpose of the Spanning Tree Protocol (STP) in Switching? How Does it Prevent Network Loops? Answer: STP is a protocol that prevents network loops in Ethernet networks by ensuring only one active path exists between devices. It elects a root bridge and determines the shortest path to it, blocking redundant paths to avoid broadcast storms and network instability. 47) What is the Purpose of VLAN Trunking and how Does it Work? Answer: VLAN Trunking enables multiple VLANs to be transmitted over a single physical link between switches, allowing devices on different switches to communicate as if on the same VLAN. It tags Ethernet frames with VLAN IDs using protocols like IEEE 802.1Q, ensuring switches can identify and forward traffic to the correct VLANs. 48) Explain the Three Sources of Signal Degradation on a Data Link? Answer: The three sources of signal degradation on a data link are attenuation, interference, and distortion. Attenuation is a result of the resistance within the medium. Interference is due to external noise introduced into the medium. Distortion occurs because of the many characteristics of the medium, which react differently to various frequency components of the signal. Learn how to design, configure, and troubleshoot complex networks join our ONS3 Training now! Advanced and Scenario-based CCNA Interview Questions and Answers Understanding how to approach and solve practical networking scenarios will demonstrate your problem-solving skills and knowledge in real-world networking situations. Here is a list of some CCNA Interview Questions and answers at an advanced level: 49) You are Troubleshooting a Network Connectivity Issue Between two Hosts on the Same Subnet. What Steps Would you Take to Identify and Resolve the Problem? Answer: In this scenario, it is better to start by verifying the physical connection and ensuring that both hosts are on the same subnet with the correct IP configurations. It is important to check if there are any firewall rules or access control lists blocking the traffic. Additionally, tools like ping, traceroute, and ARP can be used to diagnose and isolate the issue. 50) A User Reports That They are Unable to Access a Specific Website From Their Computer. What Could be the Possible Causes, and how Would you Troubleshoot the Issue? Answer: There could be several causes for this issue. It could be a DNS problem, a network connectivity issue, or a firewall restriction. To troubleshoot, you must check the DNS settings on the user's computer and ensure that it can resolve the website's domain name. Then, you must verify the network connectivity by pinging the website's IP address. If necessary, you must also check the firewall settings to ensure that it isn't blocking the traffic. 51) You Have Been Asked to Configure a new VLAN on a Switch. What Steps Would you Take to Create and Implement the VLAN? Answer: To create and implement a new VLAN, the following steps must performed: a) Access the Switch's configuration mode b) Create the VLAN using the appropriate command c) Assign the VLAN to the desired switch ports using the interface configuration mode d) Verify the VLAN configuration using show commands 52) A Company Wants to Implement a Redundant Network Design for High Availability. How Would you set up Redundant Links Between Switches and Prevent Network Loops? Answer: To set up redundant links between switches and prevent network loops, a protocol like STP must be used. STP allows for automatic detection and disables redundant paths, ensuring that there is only one active path at any given time. By configuring STP on the switches, it will calculate the shortest path to the root bridge and block any redundant paths, thereby preventing network loops. 53) A Remote Employee is Unable to Establish a VPN Connection to the Corporate Network. How Would you Troubleshoot the Issue? Answer: To troubleshoot the VPN connection issue, one must take steps like the following: a) Verify the remote employee's internet connectivity and ensure they can reach the VPN server b) Check the VPN client configuration on the employee's computer and ensure the correct settings are entered c) Verify the VPN server configuration, including IPsec or SSL settings, and ensure the correct ports are open on firewalls d) Check for any Network Address Translation (NAT) or firewall rules that may be blocking the VPN traffic e) Analyse VPN logs for any error messages or indications of connectivity issues 55) A Network Switch has Experienced a Power Outage and has Rebooted. However, Some Devices Connected to the Switch are Unable to Obtain an IP Address. How Would you Troubleshoot This DHCP Issue? Answer: To troubleshoot the DHCP issue, one must Perform the following operations: a) Verify that the DHCP service is running on the server and check for any error messages b) Confirm that the DHCP scope and address pool are properly configured with available IP addresses c) Check if the switch ports connecting the affected devices are configured as access ports in the appropriate VLAN and are not in a shutdown state 56) A User Complains About Slow Network Performance. What Steps Would you Take to Troubleshoot and Resolve the Issue? Answer: In this scenario, it is important to check the network configuration and bandwidth usage. One must also investigate for any network congestion, faulty cables, or switches. Additionally, the network traffic must be analysed using network monitoring tools to identify bottlenecks or abnormal behaviour. 57) A Network Device is Continuously Rebooting. What Could be the Possible Causes, and how Would you Address the Issue? Answer: Possible causes for continuous rebooting could include power supply issues, hardware failures, or software bugs. To address the issue, you must first check the power source and ensure it is stable. Then, inspect the device for any loose connections or faulty components. One must update the device's firmware or replace any faulty hardware if necessary. 58) A Company is Planning to Implement a Wireless Network. What Factors Would you Consider in Designing a Secure and Efficient Wireless Network? Answer: When designing a secure and efficient wireless network, factors to consider include the following: a) Network coverage and signal strength b) Security protocols and encryption methods c) Access control mechanisms d) Interference from neighbouring wireless networks and non-Wi-Fi devices e) Scalability and capacity planning for multiple devices f) Network segmentation and VLAN configurations g) Physical placement and deployment of access points 59) A Network Administrator Wants to Implement Quality of Service (QoS) to Prioritise VoIP Traffic on the Network. How Would you Configure and Implement QoS? Answer: To prioritise VoIP traffic using QoS, you must: a) Identify the VoIP traffic by assigning it a specific Differentiated Services Code Point (DSCP) value. b) Configure QoS policies on network devices (routers, switches) to classify and mark the VoIP traffic using the DSCP value. c) Implement traffic shaping or prioritisation mechanisms based on the marked VoIP traffic to ensure it receives preferential treatment across the network. 60) A Network Device is not Receiving an IP Address From the DHCP Server. How Would you Troubleshoot and Resolve This DHCP Issue? Answer: To troubleshoot and resolve the DHCP issue, one must opt for the following strategies: a) Verify the physical connectivity between the device and the network. b) Check if the DHCP server is running and has available IP addresses in its pool. c) Inspect the DHCP configuration on the server and ensure it is properly configured with the correct scopes and options. d) Verify that the device is configured to obtain an IP address automatically (DHCP client) and does not have any conflicting static IP configuration 61) A Network Switch is Exhibiting High CPU Utilisation. What Could be the Possible Causes, and how Would you Mitigate the Issue? Answer: High CPU utilisation on a Switch could be caused by high network traffic, excessive broadcast/multicast traffic, spanning-tree recalculations, or software bugs. One must identify the root cause using monitoring tools or logging features on the switch to mitigate the issue. Then, take steps like optimising network configurations, implementing traffic filters, upgrading switch firmware, or redistributing network load to alleviate the CPU load. 62) A Network Administrator Wants to Provide Secure Remote Access to the Internal Network. How Would you Implement This Using VPN Technology? Answer: To provide secure remote access to the internal network using VPN technology, one must do the following: a) Set up a VPN server, such as Cisco AnyConnect or OpenVPN, on the network. c) Configure the appropriate authentication and encryption protocols to establish a secure connection. c) Define user access policies and assign user credentials for authentication. d) Ensure firewall rules allow VPN traffic to reach the internal network. e) Educate and guide remote users on how to configure and connect to the VPN server using VPN client software. 63) A Network Administrator Wants to Segment the Network to Enhance Security. How Would you Implement Network Segmentation Using VLANs? Answer: To implement network segmentation using VLANs, you must perform the following: a) Identify the logical grouping of devices and determine the VLANs required. b) Configure VLANs on Switches and assign specific switch ports to each VLAN. c) Enable VLAN Trunking between Switches to carry multiple VLANs. d) Implement VLAN Access Control Lists (VACLs) or firewall rules to restrict inter-VLAN communication as needed. e) Verify connectivity and test the segmentation by ensuring devices in different VLANs cannot communicate by default. 64) A Company Plans to Upgrade its Network Infrastructure to Support Faster Network Speeds. How Would you Upgrade the Network From Fast Ethernet to Gigabit Ethernet? Answer: To upgrade the network from Fast Ethernet to Gigabit Ethernet, one must opt for the following: a) Replace the existing Fast Ethernet switches and network interfaces with Gigabit Ethernet switches and compatible network cards. b) Update the cabling infrastructure to support Gigabit Ethernet, c) Reconfigure the network devices with appropriate VLANs, IP addressing, and QoS settings. d) Perform thorough testing to ensure proper connectivity and performance after the upgrade. Join our CCNP Collaboration Training to stay updated with the latest collaboration technologies and best practices. 65) A Company Plans to Implement a Wireless Network with Multiple Access Points. How Would you Configure Seamless Roaming for Wireless Clients? Answer: Here's how to configure seamless roaming for wireless clients: a) Ensure all access points are configured with the same wireless network name (SSID) and security settings. b) Enable a common authentication method (e.g., WPA2-Enterprise with 802.1X) to allow clients to authenticate against a centralised authentication server. c) Configure the access points to use the same channel and non-overlapping frequency bands to minimise interference. d) Adjust the signal coverage and power levels of the access points to provide sufficient overlap for seamless client handoffs between access points. 66) A Network Administrator suspects a network device may have a faulty NIC. How would you verify and troubleshoot the issue? Answer: To verify and troubleshoot a NIC issue, one must do the following: a) Test the suspected NIC by connecting it to a different device or connecting a known working NIC to the device. b) Verify the NIC drivers and firmware are up to date. c) Check for any physical damage or loose connections on the NIC. d) Monitor the device's network traffic and error logs for any indications of NIC-related issues. Note: If necessary, replace the NIC with a known working one and retest the connectivity. 67) A Network Administrator Wants to Monitor Network Traffic and Analyse Performance. How Would you set up Network Monitoring and performance analysis, one must perform the following: a) Deploy network monitoring tools such as Wireshark, SolarWinds, or PRTG to capture and analyse network traffic. b) Configure network devices (routers, switches) to export NetFlow or SNMP data to the monitoring tools. c) Set up monitoring thresholds and alerts for network devices, bandwidth utilisation, latency, and other performance metrics. d) Implement packet capturing and analysis on specific network segments or devices to troubleshoot issues or detect anomalies. 68) How would you configure link aggregation using EtherChannel? Answer: To configure link aggregation using EtherChannel, you must do the following: a) Identify the switch ports that need to be aggregated. b) Configure the same parameters (such as speed and duplex mode) on each of the ports. c) Create an EtherChannel group and assign the desired protocol. d) Enable the EtherChannel on the switch ports and ensure they are part of the same link aggregation for increased bandwidth and redundancy. 69) How Would you Configure Inter-VLAN Routing Using a Layer 3 Switch? Answer: To configure inter-VLAN routing using a Layer 3 switch you have to do the following: a) The VLANs must be created on the Layer 3 switch. b) Assign the VLAN interfaces (SVIs) with IP addresses, one for each VLAN. c) Enable routing on the Layer 3 switch. d) Configure Access Control Lists (VACLs) or implement firewall rules to control traffic between VLANs. e) Ensure that the devices on each VLAN have their default gateway set to the IP address of the corresponding VLAN interface on the Layer 3 switch. 70) Define CDP and Its Functions? Answer: Cisco Discovery Protocol (CDP) stands as a pivotal Layer 2 networking protocol in the world of Cisco devices. It operates in a media-independent and network-independent manner, providing an invaluable service by allowing the discovery of Cisco devices across a network. It plays a crucial role in the efficient management of Cisco devices by not only locating them but also assisting in their configuration. This protocol paves the way for systems to gain insights into one another through various network-layer protocols. Some of its important functions include the following: a) Collecting information: CDP serves as an information gatherer aboutneighbouring devices that are directly connected to it and improves network visibility. b) Identifying adjacent Cisco Devices: It excels in pinpointing adjacent Cisco devices in the network and their specific properties. c) Detail extraction: CDP goes beyond basic discovery by extracting a wealth of information, including port numbers, IP addresses, router and switch models, interface specifics, iOS version details, and device ID-hostnames. This comprehensive data helps in configuration and monitoring. d) Inventory management: One of its key roles is simplifying the task of maintaining an up-to-date list of Cisco network devices. This not only ensures accuracy but also streamlines Network Management. e) Sharing vital data: CDP doesn't just keep insights to itself; it actively shares crucial information about other directly connected Cisco equipment. This includes data like the operating system version and IP addresses, which further enhance network intelligence and help in efficient resource allocation. Learn to design, install, and support networks for organisations by signing up for our CCNA Certification now! 71) What is Routing? Answer: Routing involves identifying the optimal path for data to travel from its source to its destination. This task is performed by a device called a router, which operates at the network layer. 72) What is BootP? Answer: BootP, short for Boot Program, is a protocol primarily used to boot diskless workstations connected to a network. Additionally, a diskless workstation can use BootP to ascertain its IP address and the IP address of the server PC. 73) What is PoE? Answer: Power over Ethernet (PoE) is a technology that enables network cables to transmit electrical power, allowing devices such as IP cameras and wireless access points to receive both data and power through a single cable. This simplifies installation and eliminates the need for separate power sources. Conclusion With these top CCNA Interview Questions and Answers, youre now equipped to tackle your interview with confidence and clarity. Dive deep into these questions, understand the concepts, and be ready to impress your interviewer. Best of luck on your journey to becoming a certified networking professional! Level up your networking skills with Cisco Packet Tracer Course - sign up now! It's important to prepare for an interview in order to improve your chances of getting the job. Researching questions beforehand can help you give better answers during the interview. Most interviews will include questions about your personality, qualifications, experience and how well you would fit the job. In this article, we review examples of various cisco voice engineer interview questions and sample answers to some of the most common questions.Use this templateor download as PDF Common Cisco Voice Engineer Interview QuestionsWhat experience do you have with Cisco Voice products?Cisco Voice Engineers are responsible for designing, implementing, and troubleshooting Cisco voice and unified communications products. Therefore, it is important for the interviewer to know what experience the candidate has with these products.Example: I have experience with a variety of Cisco Voice products, including Cisco Unified Communications Manager (CUCM), Cisco Unity Connection, and Cisco IP Phones. I have also worked with voice VoIP platforms such as Asterisk and FreeSWITCH. In addition, I have experience with a number of voice codecs, including G.711, G.729, G.722, and Opus.What Cisco Voice products are you familiar with?The interviewer is trying to gauge the applicant's Cisco Voice products and how they might be able to apply them in a real-world setting. This question is important because it allows the interviewer to get a better sense of the engineer's skill set and whether they would be a good fit for the position.Example: I am familiar with a variety of Cisco Voice products, including the Cisco Unified Communications Manager (CUCM), Cisco Unity Connection, and Cisco IP Phones. I have also worked with a number of other voice products from other vendors, including Avaya, Nortel, and Siemens.How would you configure a Cisco Voice product?The interviewer is trying to gauge the interviewee's technical expertise with Cisco Voice products. It is important for the interviewer to know if the interviewee is able to configure Cisco Voice products because this is an essential skill for the position.Example: There is no one-size-fits-all answer to this question, as the configuration of a Cisco Voice product will vary depending on the specific product and the specific needs of the customer. However, some tips on how to configure a Cisco Voice product include understanding the customer's voice requirements, understanding the various Cisco Voice products available, and having a good working knowledge of Cisco IOS.What troubleshooting steps would you take like if a Cisco Voice product was not working properly?One of the key responsibilities of a Cisco Voice Engineer is to troubleshoot issues with Cisco Voice products. This question allows the interviewer to gauge the engineer's knowledge and experience in troubleshooting Cisco Voice products. It is important to be able to identify the root cause of the issue and take the necessary steps to resolve it.Example: There are a few troubleshooting steps that can be taken when a Cisco Voice product is not working properly. First, check the power and connectivity to the device. Next, check the configuration of the device to ensure that it is correct. Finally, check the logs of the device to see if there are any error messages that can help identify the problem.What is your experience with VoIP?The interviewer is asking about your Cisco Voice Engineer's experience with VoIP because it is an important technology for many businesses. VoIP can save businesses money on their phone bills, and it can also provide features that traditional phone systems cannot. A Cisco Voice Engineer with a good understanding of how VoIP works and how to troubleshoot common problems.Example: I have worked with VoIP for over 5 years now. I have experience with a variety of VoIP platforms and protocols, including SIP, H.323, and MGCP. I have also worked with a variety of VoIP hardware, including Cisco IP Phones, Asterisk PBXs, and VoIP gateways. I have a good understanding of the various issues that can impact VoIP quality, such as jitter, latency, and packet loss. I am also familiar with the various methods that can be used to troubleshoot VoIP problems.What is your experience with SIP?The interviewer is asking about the Cisco Voice Engineer's experience with SIP because they will need to be able to work with SIP-based VoIP systems.Example: I have worked with SIP for about 2 years now. I have experience setting up and configuring SIP Trunks, as well as troubleshooting any issues that may arise. I am also familiar with the various SIP-related protocols, such as RTP, SRTP, and SDP.What is your experience with H.323?Cisco Voice Engineer is responsible for configuring, deploying, and troubleshooting Cisco VoIP systems. H.323 is a standard for VoIP systems that allows for interoperability between different vendors' systems. It is important for the interviewer to know the candidate's level of experience with H.323 in order to gauge their ability to configure and troubleshoot Cisco VoIP systems.Example: I have worked with H.323 for over 5 years now and have a good understanding of how it works. I have also implemented it in a few customer networks.What is your experience with QoS?An interviewer would ask "What is your experience with QoS?" to a Cisco Voice Engineer to find out if the engineer has experience working with Quality of Service, which is a networking technique used to manage network traffic in managed effectively. QoS is important because it helps to ensure that voice and video traffic is given priority over other types of traffic, such as data traffic, to help ensure that calls are clear and video is not choppy.Example: I have worked with QoS in both Cisco IOS and NX-OS. I am familiar with the MQC and Modular QoS CLI. I have configured QoS for various types of traffic, including VoIP, video, and data. I have also troubleshoot QoS issues.What is your experience with NAT?NAT is important for a Cisco Voice Engineer because it allows them to control how traffic is routed through a network. By understanding NAT, a Voice Engineer can optimise traffic flow and reduce congestion.Example: I have experience with NAT in Cisco routers. I am familiar with the various types of NAT (static, dynamic, PAT, etc) and how to configure them. I have also worked with NAT in other devices, such as SonicWALL firewall and Linux iptables.What is your experience with firewall configuration?When configuring a firewall, it is important to consider the types of traffic that will be passing through the firewall. Cisco Voice Engineers are familiar with the types of traffic that are typically used in voice communication and can configure the firewall to allow this traffic while still protecting the network.Example: I have experience with firewall configuration and I am familiar with the different types of firewalls available. I know how to configure a firewall to allow specific traffic through and how to block specific traffic. I am also familiar with the different types of attacks that can be used against a firewall and how to protect against them.What is your experience with call routing?The interviewer is asking about the Cisco Voice Engineer's experience with call routing because it is an important function of the job. The engineer must be able to route calls correctly in order to ensure that the callers are able to reach the intended recipient. This includes being able to troubleshoot any problems that may occur with the call routing system.Example: I have worked with call routing for a few years now and have experience with both on-premises and cloud-based solutions. I am familiar with various call routing algorithms and can troubleshoot issues related to call routing. I also have experience troubleshooting call routing issues and can often quickly identify and resolve problems.What is your experience with call admission control?Cisco Voice Engineer is responsible for designing, implementing, and troubleshooting Cisco VoIP systems. Call admission control is an important part of VoIP systems, as it helps to ensure that only high-quality calls are completed or admitted to the network, and that call quality is maintained by avoiding over-utilization of resources. Asking about an applicant's experience with call admission control helps to gauge their knowledge and expertise in designing and managing VoIP systems.Example: I have experience with call admission control in a Cisco VoIP environment. I have configured and implemented call admission control on Cisco routers and switches. I have also troubleshoot call admission control issues in a VoIP network.What is your experience with dial plans?There are a few reasons why an interviewer might ask a Cisco Voice Engineer about their experience with dial plans. First, the interviewer wants to know if the engineer has the necessary skills to configure and troubleshoot dial plans. Second, the interviewer wants to know if the engineer understands the various options available when configuring a dial plan, and how to select the best option for a given situation. Finally, the interviewer wants to know if the engineer is familiar with the common problems that can occur with dial plans, and how to troubleshoot them.Example: I have worked with dial plans for a few years now and have experience with both Cisco and Asterisk systems. I am familiar with the various components of a dial plan, such as route patterns, translation patterns, and voice gateways. I also have experience troubleshooting issues with dial plans, such as call routing problems and audio quality issues.What is your experience with voice mail integration?There are a few reasons why an interviewer would ask this question to a Cisco Voice Engineer. Firstly, voice mail integration is an important part of any VoIP system. It allows users to access their voicemail messages from any phone, and it can also be used to route calls to voicemail if the user is unavailable. Secondly, voice mail integration can be used to improve customer service. By being able to quickly and easily access voicemail messages, customers can get the information they need without having to wait on hold or speak to a customer service representative. Finally, voice mail integration can help to reduce costs. By routing calls to voicemail when the user is unavailable, businesses can avoid having to pay for long-distance or international call charges.Example: I have experience with voice mail integration in a few different environments. I have integrated Cisco Unity Connection with Cisco Unified Communications Manager (CUCM), as well as other third-party PBX systems. I have also written custom scripts to integrate voice mail systems with CRM applications.What is your experience with unified communications?Cisco Voice Engineer should have a good understanding of unified communications in order to be able to properly install and configure Cisco voice products. Unified communications is important because it allows businesses to communicate more effectively and efficiently. It can also help reduce costs by eliminating the need for multiple communication tools.Example: I have been working with unified communications for about 5 years now. I have experience with a variety of UC platforms, including Cisco, Avaya, and Microsoft. I have also worked with a number of different voice IP protocols, such as SIP, H.323, and MGCP. In my current role, I am responsible for designing, implementing, and troubleshooting UC solutions for our customers.What other Cisco products are you familiar with?There are many reasons an interviewer might ask this question. One possibility is that they want to gauge the candidate's familiarity with Cisco products. It can help the interviewer determine whether the candidate is a good fit for the position. If the candidate is not familiar with other Cisco products, it may be difficult for them to troubleshoot issues that arise.Example: I am familiar with a number of Cisco products, including the Cisco Unified Communications Manager (CUCM), the Cisco Unity Connection (CUC) voicemail system, the Cisco IP Phone portfolio, and the Cisco Telepresence line of products. In addition, I have experience with a number of other Cisco products such as the Cisco ASA firewall, the Cisco VPN concentrator, and the Cisco switch line. CCNA (Cisco Certified Network Associate) is a certification that proves your ability to understand, use, and manage Cisco networks. The CCNA certification provides you with the skills necessary for optimizing and administering Cisco networking resources in an organization. With this credential, you can move on to higher-level certifications such as the MCSA or MCDBA.Obtaining CCNA certification improves your knowledge base and enhances your job prospects.In this complete interview preparation guide, weve handpicked the top 50 CCNA interview questions along with detailed answers to help you ace your interview. Whether youre a fresher or an experienced candidate, this curated list covers the most frequently asked questions to boost your confidence.Let's begin with CCNA Interview Questions for Freshers in technology.CCNA Interview Questions and Answers for Freshers1. Name any two ports of Switches.Answer Port: An access point is a kind of connection on a machine or connected to a switch that is VLAN aware without requiring it to support VLAN tagging.Combo Port: These ports are used to connect devices to the switch. Switches are connected to a port that is called a combo port. The ports can be assigned to multiple destinations of devices. A device connected to a port is called a combo port. These ports can be assigned to multiple destinations of devices. A device combination is a group of one or more devices used to transmit or receive data. In other words, a combo port can be a single interface with two front ends, such as an RJ45 connector and an SFP module connector (also called MiniGBIC).2. What are three possible ways of data transmission in CCNA?Simplex Mode: Simplex mode is sort of a unidirectional within the communication is one-way. Only 1 of the 2 devices will send and the other will receive.Half-Duplex Mode: Every station or device can both transmit and receive information but not at the same time, however, it is not at the identical time. once the device transmits Half.Full-Duplex Mode: Each station will broadcast and receive information at an identical time in full-duplex mode, however, it is not at the identical time. once the device transmits data.The link's capability with signals traveling within the different directions in full-duplex mode.Either the connection or the receiver must have two physically independent transmission routes.On the other hand, capacitance is divided by signals moving in both directions.For more details please refer to the Transmission Modes in Computer Networks article.3. Differentiate between half-duplex and full-duplex.Simplex, Half-Duplex, and Full-Duplex) article. Name different IPX access lists.There are three IPX Access lists:Standard Access list: The access list is created using the source IP address. These ACLs allow or deny the whole protocol suite. They do not differentiate between the IP traffic such as TCP, UDP, HTTPS, etc. By using digits 1-99 or 1300-1999, the router will understand it as a standard ACL and set the address as the source IP address should be allowed or denied.Extended Access-list: It is a type of Access-list that is mainly used as it can differentiate IP traffic. The whole traffic will not be permitted or denied like in the standard access list. ACL uses both source and destination IP addresses and also port numbers to distinguish IP traffic. In this type of ACL, we can also mention which IP traffic should be allowed or denied. Those use range of numbers 100-199 and 2000-2699.Reflexive Access list: Reflexive Access-list can be defined as an access list that allows only the responses of the packets on sessions created within the network from the outside network.For more details please refer to the Access-Lists (ACL) article.4. What do you mean by 100BaseFX?100BASE-FX is another variation of the 100Base standard, however, here it works on optical fiber.For more details please refer to the Fast and Gigabit Ethernet article.5. Name the LAN Switching method that is mostly used in CISCO Catalyst 5000?The store-and-forward switching technique is used by the CISCO Catalyst 5000 and therefore it stores the entire frame to its buffers and performs a CRC (Cyclic Redundancy Check) before deciding whether or not to transmit this information frame.For more details please refer to the Message switching techniques article.6. Name different memories that are used in CISCO routers.The different memories that are used in Cisco routers are given below:Flash MemoryRAM (Random Access Memory)ROM (Read Only Memory)NVRAM (Non-Volatile Random Access Memory)For more details please refer to the different memories of the different memories that are used in Cisco routers are given below:Flash MemoryRAM (Random Access Memory)ROM (Read Only Memory)NVRAM (Non-volatile RAM) is a type of memory that retains its contents when power is turned off.7. What is the difference between tracert and traceroute?Traceroute is a feature or a utility that records the route (explicit passage PCs at each bounce) through a web between your PC and a predetermined objective PC and the Tracert tracking is a quick scan that shows a bit of tracking information of any network or device that can be obtained in a package from a PC or gadget.For more details please refer to the Difference between Ping and Traceroute article8. What do you mean by DLCI?DLCI (Data Link Connection Identifier) is the quantity of a personal or switched virtual circuit in a frame relay network, situated within the frame header, the DLCI field identifies that logical circuit the data travels over, and each DLCI includes a committed information rate (CIR) associated with it.For more details please refer to the Frame relay article. What do you mean by DLCI?DLCI (Data Link Connection Identifier) is the name router command that is used to display RAM content and NVRAM Content.To Show, the components of NVRAM or point to the arrangement file assigned to the CONFIG_FILE variable, we use the show startup-config command.For more details please refer to the Cisco Router basic commands article.10. Define Frame relay?Frame relay is a technology that provides fast and reliable data transmission in Internet networks. It is a standards-based networking technology that provides a path for data packets from one point on the network to another.For more details please refer to the How does Frame Relay work article.11. Difference between User mode and Privileged mode in Cisco?User mode is only for viewing router configurations and Privileged mode is for viewing all router configurations and also allows editing some basic configurations.12. What is EIGRP?Mention some metrics of the EIGRP Protocol.EIGRP determines the path value from metrics. EIGRP Messages - Hello, Update, Question, Answer and Confirm.For more details please refer to the Cisco devices please refer to the EIGRP fundamentals article.13 . What is CDP(Cisco Discovery Protocol)? Write its functions.Cisco Discovery Protocol (CDP) is a network discovery tool that helps network administrators and technicians identify nearby Cisco devices, especially those with a low-transparency protocol.For more details please refer to the Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) article.14. Difference between a broadcast domain and a collision domain?Broadcast domain: Broadcast domain refers to the transmission of information over a wide area, such as television or radio broadcasting. The collision domain consists of two or more objects that come into contact with each other frequently.For more details please refer to the Collision Domain and Broadcast Domain in the Computer Network article.15. What do you mean by route poisoning?Route poisoning is a way to control a router from transmitting packets through a path that has become weak within computer networks via route poisoning is a path that has become weak within networks. Distance-vector routing protocols in computer networks use route poisoning to show that when router routes that a route to a node has become invalid.For more details please refer to the Route Poisoning and Count to infinity problem article.16. How many types of passwords can be used in CISCO routers?There are three types of passwords that can be used in CISCO routers.These are console passwords: These are used to protect data stored in the router. They are used to log into the router and control access to the router's operation.User passwords: These are used to assign permissions to users and to control the overall operation of the router.Password attributes: They are used to set a password limit, on specify the amount of time a password must be used before it is automatically changed.For more details please refer to the Different Types of Passwords used in Securing Cisco Router article.17. Write the difference between public IP and private IP addresses.IP.A public IP address that identifies you on the Internet so that all the information you send can find you back.A private IP address is used inside a private network to securely connect to other devices in the same network. Each device on the same network has a unique IP address.For more details please refer to the Private and Public IP article.18. Explain PoE.Power over Ethernet (PoE) is a measure that allows Ethernet cables to simultaneously transfer data and power using a single network cable. This permits system integration and network installers to establish powered appliances in places that lack electrical circuitry. In addition, PoE stops the cost of installing extra electrical wiring, requiring professional electrical installers to assure that strict conduit regulations are followed. PoE technology transmits 10/100/1000 Mbps of data and 15W, 30W, 60W, and up to 90W of power budget to appliances over Cat5e, Cat6, and Cat6a. Cat7 and Cat8 Ethernet cables for the highest distance of 100m.For more details please refer to the Power Over Ethernet (POE) article.19. What is Round Trip Time?RTT is also known as round-trip time is a crucial tool in defining the working condition of a network. It is the time between a request and the response to any kind of server on the internet. A round-trip time is measured in milliseconds. RTT can be examined and determined by pinging a specific address. It refers to the time taken by a network request to reach the initial source.For more details please refer to the RTT(Round Trip Time) article.20. What is IPv6? What are its scopes?The DHCP scope is a valid range of IP addresses that are known for assignment or lease to client computers on an individual subnet. In a DHCP server, a scope is configured to determine the address pool of IPs that the server can provide to DHCP clients. DHCP Scopes define the IP addresses that are provided to the clients. They should be determined and activated before DHCP clients use the DHCP server for its dynamic IP configuration. Users can configure as many scopes on a DHCP server as needed in the network environment.For more details please refer to the What is DHCP (Dynamic Host Configuration Protocol) (DHCP) article.21. what is NVRAM?NVRAM (Non-volatile random-access memory) is a computer memory that can keep data when power is off. The memory chips has been turned off. NVRAM is a part of the larger type of non-volatile memory (NVM), which contains storage-class memory based on NAND flash. Flash memory chips are slow to read to and write than RAM chips, making them slow to read. NVRAM specifically refers to the contents that it works.For more details please refer to the What is Non-Volatile Random Access Memory (NVRAM)? article.22. What is the Service Password Encryption Command on CISCO Router?Switch? Answer: Service Password Encryption (Configure-Network Password Encryption Command on CISCO Router/Switch? Switch? It is to encrypt all passwords on your router so that they cannot be easily assumed from your running configuration. This command uses very weak encryption because the router has to decrypt the password very quickly for it to work.For more details please refer to the Different Types of Passwords used in Securing Cisco Router article.23. Explain different cable types?There are commonly two types of cables in networking, described below.Coaxial cable:-A coaxial cable is a kind of copper cable specially made with a metal guard and other parts arranged to stop signal interference. It is mainly used by cable TV firms to connect their satellite antenna installations to customer homes and businesses. It is also sometimes used by telephone companies to secure central offices to telephone poles near customers. Some homes and offices use coaxial cable, too, but its general use as an Ethernet connectivity medium in companies and data centers has been replaced by the deployment of twisted pair cabling.Twisted pair:-Twisted pair Ethernet is an Ethernet computer network that uses twisted pairs of insulated copper wires for the physical layer of the network to transmit of the network, which is connected to the data link layer. Twisted pair cable wires are turned around each other to reduce obstacles from other twisted pairs in the cable. Two twisted wires help in reducing crosstalk that can disrupt signals and increase electromagnetic induction, which has a typical speed of around 100m.For more details please refer to the Types of Ethernet Cable article.24. What is the port number of DNS and Telnet?The Port number of DNS is 53, and the Port number of Telnet is 23 and the Port number of DNS is 53.For more details please refer to the Various TCP and UDP ports article.25. Which service uses both TCP and UDP?The Domain Name System (DNS) uses the TCP and UDP protocols for some communications and is ideal for quick transfers and is suitable for large response messages.For more details please refer to the Various TCP and UDP ports article.26. What is the port number of SMTP and POP3?The port number of SMTP is 25 and the port number of SMTP is 25 and POP3 is 110.For more details please refer to the Difference between SMTP and POP3 article.27. What is CRC? Which layer does CRC work on?CRC stands for Cyclic Redundancy Check. It is a checksum algorithm used to detect errors in digital data streams transmitted between two or more computers. The layer where CRC works depends on the type of data being checked and how it needs to be processed by the system. In most cases, CRC is applied at the lower layer of an OSI model stack (OSI Reference Model).For more details please refer to the Cyclic Redundancy Check article.28. Which one is reliable TCP or UDP? and why?TCP is reliable because it guarantees the delivery of

data to the destination router. The delivery of data to the destination can not be secured in UDP.For more details please refer to the Various TCP and UDP ports article.29. What is the port number of FTP (data) and FTP?The Port number of FTP (data) is 20 and the Port number of FTP is 21.For more details please refer to the File Transfer Protocol (FTP) article.30. Which layer provides the logical addressing that routers will use for path determination?The Network layer provides logical addressing, typically IP addressing and routing.For more details please refer to the Network Layer Services- Packetizing, Routing, and Forwarding article.31. DNS uses which protocol? Why?The Domain Name System (DNS) uses Transmission Control Protocol (TCP) for zone transfers and User Datagram Protocol (UDP) for name queries.UDP exchanges fewer data than TCP.For more details please refer to the Why does DNS use UDP and not TCP article.32. Differentiate between forwarding lookup and reverse lookup in DNS?Forward DNS and reverse DNS lookups are two different methods of accessing the Internet. The forward area is the DNS zone where the hostname is stored in the IP address relationship. Reverse DNS is the query method for determining the domain name associated with an IP address.For more details please refer to the How to Implement Reverse DNS Look Up Cache? article.33. What is Split Horizon Cisco?A split horizon is developed to stop routing loops. Routing loops happen when a loop is created between two or more routers. For example, Router 1 has a network path to 192.168.1.0 via Router 2. Router 2 has a path to the same network, but it is back via Router 1. Therefore, Router 1 sends packets for 192.168.1.0 to Router 2, which then transmits the packets back to Router 1. This looping continues until the TTL (Time to Live) on the packet expires.For more details please refer to the Route Poisoning and Count to infinity problem in the Routing article.34. Why is RIP known as Distance Vector?The Routing Information Protocol (RIP) is the oldest distance-vector routing protocol that uses the hop count as a routing metric. RIP stops routing loops by executing a limit on the number of hops authorized in a path from source to destination. The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support. RIP executes the split horizon, route poisoning, and hold-down means to prevent the wrong routing information from being propagated. In RIPv1 routers broadcast updates with their routing table every 30 seconds. In the early deployments, routing tables were short enough that the traffic was not important. As networks grew in size, however, it became obvious there could be a huge traffic burst every 30 seconds, even if the routers had been initialized at random times.For more details please refer to the Routing Information Protocol (RIP) article.35. What is the administrative distance of RIP?By default, OSPF has a default management level of 110 and RIP has a default management level of 120.For more details please refer to the Routing Information Protocol (RIP) article.36. What is the limit of hop count in RIP?The limit of hop count in RIP is 15. Networks with a hop count of 16 or more are unreachable.For more details please refer to the Routing Information Protocol (RIP) article.37. How is RIP select the best path to the remote network?The main function of the router is to determine the best way to send packets. To determine the best route, a router searches its router table to find a network address similar to the destination IP address of the package.For more details please refer to the Routing Information Protocol (RIP) article.38. What are the differences between RIPv1 and RIPv2?RIPv1 uses a standard route. Occasional updates do not have subnet information and no support for VLSM. This limitation makes it impossible to have subnets of different sizes within the same network category. In other words, all subnets in the network class should be the same size. There is also no router authentication support, which makes RIP vulnerable to various attacks. RIPv2 is a vector distance route protocol defined in RFC 1723. As a phaseless protocol, it means, it included a subnet mask and network addresses in its router updates.For more details please refer to the Differences between RIPv1 and RIPv2 article.39. What is pinhole congestion?In computer networking, the router makes decisions regarding the way a packet will travel, based on the number of hops it carries to reach the destination and if it had 2 other ways to get there, it will only send it via the shortest path, regardless of the connection speed. This is known as pinhole congestion.For more details please refer to the Congestion Control in Computer Networks article.40. What is a passive interface in RIP?Router (config-router) # passive-interface serial0 / 0/0. Sets the interface as idle, meaning that route updates will not be sent to this interface. NOTE: In RIP, the passive-interface command will prevent the inter-face from sending route updates but will allow the visual interface to receive updates.For more details please refer to the Passive-Interface Command Behavior in RIP, EIGRP & OSPF article.CCNA Interview Questions and Answers for Experienced41. Explain the loop avoidance mechanism in RIP.The following methods are used to avoid Routing Loops in RIP:The maximum hop count mechanism can be used to block Routing Loops. Vector distance protocols use the TTL (Lifetime) value in the IP data header to avoid loops.Split horizontal is the setting of the route that stops the route from being advertised back to where it came from.Route Poisoning is another way to avoid loops. If the router finds that one of its connected routes has failed, the router will be toxic to the route by providing endless metrics to it.For more details please refer to the Routing Loop and How to Avoid Routing Loop article.42. Why EIGRP is called hybrid protocol?EIGRP does not transfer all data to the Routing table when changes are made, but will only transfer changes made since the Routing table was last updated. EIGRP does not send its routing table periodically, but will only send routing data in the event of a real change. This behavior is highly compliant with link-state routing regulations, so EIGRP is considered a hybrid protocol.For more details please refer to the EIGRP fundamentals article.43. What is meant by active and passive states in EIGRP?Active State: Routes where a follower route fails and no follower routes are likely to move to a functional state forcing EIGRP to submit query packages and reconnect.Passive State: The route is in a passive state where the route has a route to follow, and no failures have occurred so far.For more details please refer to the EIGRP fundamentals article.44. What does stuck-in-active mean?EIGRP is a reliable protocol and for each question the route you send to its neighbors you must get a response within 3 minutes. If the router does not get an answer to ALL its pending questions it will set the stage for SIA (STUCK INACTIVE) and kill the nearest neighbor.45. What is the EIGRP Feasibility Condition?The Feasibility condition states that the route will not be accepted if the Reported Range exceeds the best possible Route range. Or it means another way from a router's point of view: the path to the network will not be accepted if my neighbor's cost exceeds my cost.For more details please refer to the EIGRP Cost Calculation article.46. Explain what will happen if the packet is not acknowledged?If a packet is not acknowledged by the network, it means that the data was successfully delivered to its destination but no response was received from either end. As long as both ends are aware of each other and have been configured correctly, there should be no reason for the receiving node to do anything further with this packet. Data may still be flowing through this connection because acknowledgments take the time or because some intermediate nodes might be buffering packets before forwarding them on. However, if at any point in time you notice your traffic slowing down noticeably or becoming completely unavailable due to an excessive number of lost packets (especially during high-traffic times), then it's likely that something has gone wrong and you'll need to investigate what caused it.For more details please refer to the Stop and Wait for protocol, and its problems, and solutions article.47. Explain Null Zero in EIGRP?It is a visual interface used to ensure that routes enter the RIB, the tracks must have the next-hop to get into the RIB. If a packet arrives on a device with a route to Null 0 and is not elsewhere, it will dispose of it as the ACL would. Think of it as a visible interaction when the packets die well.For more details please refer to the article EIGRP fundamentals48. What is the EIGRP stub routing feature?The EIGRP stub routing feature allows the network administrator to prevent queries from being sent to a remote device. In addition to a simple hub and spoke network, where the remote device is connected to a single distribution device, the remote device can have a dual home on two or more distribution devices.49. Difference between LSA & LSU in OSPF?Link State Update (LSU) packs are OSPF Type 4. packs. Each LSA contains route, metrics, and topology information to define part of the OSPF network. The local router advertises the LSA inside the LSU package to its neighbors.50. What is Route Redistribution in computer networks?The use of a routing protocol to broadcast routes that are known by some other means, such as by another routing protocol, static routes, or directly connected routes, is called redistribution. While operating a single routing protocol throughout your whole IP internetwork is desirable, multi-protocol routing is common for a number of reasons, such as enterprise unions, multiple departments controlled by multiple network administrators, and multi-vendor environments. Running other routing protocols is usually part of a network design. In any case, having a multiple protocol environment makes redistribution a need.ConclusionCCNA certification offers deep knowledge and understanding of networking concepts which is very important to improve your networking skills. CCNA helps people in getting the desired job in topmost IT companies. If you're wondering "What are the basic questions for CCNA interview?", this article is the perfect guide for you. This article provides Freshers and Experienced candidates with the top 50 CCNA Interview Questions that are likely to get asked in their next CCNA Interview, along with the answers.To learn about CCNA certification from scratch, head over to CCNA Tutorial.

Common ccna interview questions. Vca vol exam questions and answers. Ccna v7 final exam answers 2021. Ccna 1 module 7. Ccna voice interview questions and answers. Ccna voice.

data to the destination router. The delivery of data to the destination can not be secured in UDP.For more details please refer to the Various TCP and UDP ports article.29. What is the port number of FTP (data) and FTP?The Port number of FTP (data) is 20 and the Port number of FTP is 21.For more details please refer to the File Transfer Protocol (FTP) article.30. Which layer provides the logical addressing that routers will use for path determination?The Network layer provides logical addressing, typically IP addressing and routing.For more details please refer to the Network Layer Services- Packetizing, Routing, and Forwarding article.31. DNS uses which protocol? Why?The Domain Name System (DNS) uses Transmission Control Protocol (TCP) for zone transfers and User Datagram Protocol (UDP) for name queries.UDP exchanges fewer data than TCP.For more details please refer to the Why does DNS use UDP and not TCP article.32. Differentiate between forwarding lookup and reverse lookup in DNS?Forward DNS and reverse DNS lookups are two different methods of accessing the Internet. The forward area is the DNS zone where the hostname is stored in the IP address relationship. Reverse DNS is the query method for determining the domain name associated with an IP address.For more details please refer to the How to Implement Reverse DNS Look Up Cache? article.33. What is Split Horizon Cisco?A split horizon is developed to stop routing loops. Routing loops happen when a loop is created between two or more routers. For example, Router 1 has a network path to 192.168.1.0 via Router 2. Router 2 has a path to the same network, but it is back via Router 1. Therefore, Router 1 sends packets for 192.168.1.0 to Router 2, which then transmits the packets back to Router 1. This looping continues until the TTL (Time to Live) on the packet expires.For more details please refer to the Route Poisoning and Count to infinity problem in the Routing article.34. Why is RIP known as Distance Vector?The Routing Information Protocol (RIP) is the oldest distance-vector routing protocol that uses the hop count as a routing metric. RIP stops routing loops by executing a limit on the number of hops authorized in a path from source to destination. The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support. RIP executes the split horizon, route poisoning, and hold-down means to prevent the wrong routing information from being propagated. In RIPv1 routers broadcast updates with their routing table every 30 seconds. In the early deployments, routing tables were short enough that the traffic was not important. As networks grew in size, however, it became obvious there could be a huge traffic burst every 30 seconds, even if the routers had been initialized at random times.For more details please refer to the Routing Information Protocol (RIP) article.35. What is the administrative distance of RIP?By default, OSPF has a default management level of 110 and RIP has a default management level of 120.For more details please refer to the Routing Information Protocol (RIP) article.36. What is the limit of hop count in RIP?The limit of hop count in RIP is 15. Networks with a hop count of 16 or more are unreachable.For more details please refer to the Routing Information Protocol (RIP) article.37. How is RIP select the best path to the remote network?The main function of the router is to determine the best way to send packets. To determine the best route, a router searches its router table to find a network address similar to the destination IP address of the package.For more details please refer to the Routing Information Protocol (RIP) article.38. What are the differences between RIPv1 and RIPv2?RIPv1 uses a standard route. Occasional updates do not have subnet information and no support for VLSM. This limitation makes it impossible to have subnets of different sizes within the same network category. In other words, all subnets in the network class should be the same size. There is also no router authentication support, which makes RIP vulnerable to various attacks. RIPv2 is a vector distance route protocol defined in RFC 1723. As a phaseless protocol, it means, it included a subnet mask and network addresses in its router updates.For more details please refer to the Differences between RIPv1 and RIPv2 article.39. What is pinhole congestion?In computer networking, the router makes decisions regarding the way a packet will travel, based on the number of hops it carries to reach the destination and if it had 2 other ways to get there, it will only send it via the shortest path, regardless of the connection speed. This is known as pinhole congestion.For more details please refer to the Congestion Control in Computer Networks article.40. What is a passive interface in RIP?Router (config-router) # passive-interface serial0 / 0/0. Sets the interface as idle, meaning that route updates will not be sent to this interface. NOTE: In RIP, the passive-interface command will prevent the inter-face from sending route updates but will allow the visual interface to receive updates.For more details please refer to the Passive-Interface Command Behavior in RIP, EIGRP & OSPF article.CCNA Interview Questions and Answers for Experienced41. Explain the loop avoidance mechanism in RIP.The following methods are used to avoid Routing Loops in RIP:The maximum hop count mechanism can be used to block Routing Loops. Vector distance protocols use the TTL (Lifetime) value in the IP data header to avoid loops.Split horizontal is the setting of the route that stops the route from being advertised back to where it came from.Route Poisoning is another way to avoid loops. If the router finds that one of its connected routes has failed, the router will be toxic to the route by providing endless metrics to it.For more details please refer to the Routing Loop and How to Avoid Routing Loop article.42. Why EIGRP is called hybrid protocol?EIGRP does not transfer all data to the Routing table when changes are made, but will only transfer changes made since the Routing table was last updated. EIGRP does not send its routing table periodically, but will only send routing data in the event of a real change. This behavior is highly compliant with link-state routing regulations, so EIGRP is considered a hybrid protocol.For more details please refer to the EIGRP fundamentals article.43. What is meant by active and passive states in EIGRP?Active State: Routes where a follower route fails and no follower routes are likely to move to a functional state forcing EIGRP to submit query packages and reconnect.Passive State: The route is in a passive state where the route has a route to follow, and no failures have occurred so far.For more details please refer to the EIGRP fundamentals article.44. What does stuck-in-active mean?EIGRP is a reliable protocol and for each question the route you send to its neighbors you must get a response within 3 minutes. If the router does not get an answer to ALL its pending questions it will set the stage for SIA (STUCK INACTIVE) and kill the nearest neighbor.45. What is the EIGRP Feasibility Condition?The Feasibility condition states that the route will not be accepted if the Reported Range exceeds the best possible Route range. Or it means another way from a router's point of view: the path to the network will not be accepted if my neighbor's cost exceeds my cost.For more details please refer to the EIGRP Cost Calculation article.46. Explain what will happen if the packet is not acknowledged?If a packet is not acknowledged by the network, it means that the data was successfully delivered to its destination but no response was received from either end. As long as both ends are aware of each other and have been configured correctly, there should be no reason for the receiving node to do anything further with this packet. Data may still be flowing through this connection because acknowledgments take the time or because some intermediate nodes might be buffering packets before forwarding them on. However, if at any point in time you notice your traffic slowing down noticeably or becoming completely unavailable due to an excessive number of lost packets (especially during high-traffic times), then it's likely that something has gone wrong and you'll need to investigate what caused it.For more details please refer to the Stop and Wait for protocol, and its problems, and solutions article.47. Explain Null Zero in EIGRP?It is a visual interface used to ensure that routes enter the RIB, the tracks must have the next-hop to get into the RIB. If a packet arrives on a device with a route to Null 0 and is not elsewhere, it will dispose of it as the ACL would. Think of it as a visible interaction when the packets die well.For more details please refer to the article EIGRP fundamentals48. What is the EIGRP stub routing feature?The EIGRP stub routing feature allows the network administrator to prevent queries from being sent to a remote device. In addition to a simple hub and spoke network, where the remote device is connected to a single distribution device, the remote device can have a dual home on two or more distribution devices.49. Difference between LSA & LSU in OSPF?Link State Update (LSU) packs are OSPF Type 4. packs. Each LSA contains route, metrics, and topology information to define part of the OSPF network. The local router advertises the LSA inside the LSU package to its neighbors.50. What is Route Redistribution in computer networks?The use of a routing protocol to broadcast routes that are known by some other means, such as by another routing protocol, static routes, or directly connected routes, is called redistribution. While operating a single routing protocol throughout your whole IP internetwork is desirable, multi-protocol routing is common for a number of reasons, such as enterprise unions, multiple departments controlled by multiple network administrators, and multi-vendor environments. Running other routing protocols is usually part of a network design. In any case, having a multiple protocol environment makes redistribution a need.ConclusionCCNA certification offers deep knowledge and understanding of networking concepts which is very important to improve your networking skills. CCNA helps people in getting the desired job in topmost IT companies. If you're wondering "What are the basic questions for CCNA interview?", this article is the perfect guide for you. This article provides Freshers and Experienced candidates with the top 50 CCNA Interview Questions that are likely to get asked in their next CCNA Interview, along with the answers.To learn about CCNA certification from scratch, head over to CCNA Tutorial.