Cisco ccna networking for beginners pdf

1996-2014 ©, Amazon.com, Inc. or its affiliates ×1996-2014©CSS Error, Amazon.com, Inc. Alternatively, its affiliates understand basic cisco networking concepts for recognizing various networking devices such as hubs, switches, routers, and so on. Configure various networking scenarios/devices using Cisco packet tracker simulationSigning a small network and solving it HTTP (Web Server) + Configuration of DNS servers in Cisco Packet Tracker (File Transfer Protocol) Cisco Packet Tracking Configuration in DHCP (Dynamic Host Configuration Protocol) Server) Cis The server of theco packet tracking server Cisco packet tracker (simple mail delivery protocol) requires only basic knowledge of how the computer works on the server, before networking knowledge is not requiredneting equipment knowledge or experience is also a Cisco CCNA networking basics for beginners: welcome to get started is not necessary. This course is designed for beginners who want to enter the world of computer networks. Beginners will learn how to transfer and receive data from a computer network and how to understand the basics of how a small computer network is created. People who are not familiar with computer networks and want to understand how computer networks actually work can also enjoy this process. This course introduces a variety of concepts, practice activities, and simulations to help build learners' skills and understanding of computer networking. Learn about basic networking concepts, different networking devices such as hubs, switches, routers, and more, and how to use packet tracking simulation to configure different networking scenarios and apply IP addressing schemes. After all, you will be able to build a small network and troubleshooting. No previous networking knowledge is required. In this course, you will have the following:1: Understanding basic networking concepts2. Recognizes a variety of networking devices, including hubs, switches, and routers. Use Cisco Packet Tracker Simulation4 to create different networking scenarios. Applies ip addressing scheme55. How to build a small network and solve the problem6. Configure web server (HTTP) + DNS servers in cisco packet trackers with OSI layer View7. Configure the File Transfer Protocol (FTP) server in Cisco Packet Tracker 8. Dynamic Host Configuration Protocol (DHCP) server configuration in Cisco Packet Tracker9. The configuration of email/SMTP (Simple Mail Delivery Protocol) servers in Cisco packet tracking is for anyone who wants to learn basic Cisco networking knowledge and who wants to start preparing for the Cisco CCNA exam who pursues careers such as IT help desk engineers, network engineers, network/system administrators, etc. This course introduces instructors in this area00:3403:14[1]00:30 and overview of the roadmap and computer networking15:22Network protocols and communications16:11Sy computer applications Various networking devices07:55Netwalking media (wired and wireless)06:41 Preparing straight and cross cables with clamping tools:0908:2804:00 Cisco packets tracking:38spick 2-PC connection Cisco packet tracker 09:38[1]:12Build small network and troubleshooting000:08 Cisco packet tracking12:57 Cisco Packet Tracer 10:19 CISCO Packet Tracer10:19 CISco Packet Tracer on CISco Packet Tracer Server (Dynamic Host Configuration Protocol) Cisco Packet Trace Server on server (Dynamic Host Configuration Protocol) Cisco 013:44 Configuration of CISCO Packets/SMTPP Servers on servers Sunil Soni certies Cisco NetAcad instructors and faculty at engineering colleges to drive interdisciply research and innovation in technology and science. He earned a PhD in computer science in computer networking. He has extensive educational experience in computer science. His research includes deep learning, machine learning, computer networks, and open source technologies. Online exams that support remote certification exams are downloaded at a glance, read infographics (PDF-1.1 MB) study-ccna.com welcome to the website, a free CCNA tutorial site that closely follows the Cisco CCNA curriculum. This site is designed to pass the CCNA exam (200-301), but it can also be used as a reference site for all networking-related networking. Here you will find all the materials you need to study for the CCNA exam. On the left, you'll see a list of articles. Articles on this site are divided into chapters. The first few chapters explain some basic networking terms and devices. The chapters then go a little deeper. You can start reading articles from scratch or find specific articles that interest you. So, what are you waiting for? Select the topic on the left and start learning! We wish you luck! CCNA (Cisco Certified Network Associates) is a popular certification for computer network engineers provided by a company called Cisco Systems. Valid for all types of engineers, including entry-level network engineers, network administrators, network support engineers, and network specialists. It helps you familiarize yourself with a wide range of networking concepts, such as the OSI model, IP addressing, network security, and more. It is estimated that more than one million CCNA certificates have been awarded since it was first launched in 1998. CCNA means Cisco Authorized Network Associates. CCNA certificates cover a wide range of networking concepts and CCNA fundamentals. This helps candidates prepare for the latest network technologies that are more likely to study and work with CCNA fundamentals. Some of the CCNA basics covered in CCNA authentication include: OSI model IP covering WLAN and VLAN network security and management (with ACLs) router/routing protocol (EIGRP, OSPF and RIP) IP Troubleshoot network device security issues Note: Cisco authentication is valid for only 3 years. When the certification expires, the certificate holder must take the CCNA certification exam again. Why do I need to be CCNA certified? Certificates validate the ability of experts to understand, operate, configure, and troubleshoot medium-level transitions and routed networks. It also includes verifying and implementing connections through remote sites using the WAN. It teaches candidates how to create a point-to-point network and teaches them how to meet user requirements by determining the network topology given to how it routes protocols to connect the network and explains how to establish a connection with a remote network that explains how to configure the network address. Certificate holders can install, configure, and operate LAN and WAN services for small network CCNA certificates, which are prerequisites for many other Cisco certifications, such as CCNA security, CCNA wireless, CCNA voice, and more. It's easy to follow the available research materials. Types of CCNA certificationsSafe CCNA. Cisco offers five levels of network certification: entry, associate, professional, professional and architect. Cisco Certified Network Associates (200-301 CCNA) The new certification program covers a wide range of basics for your IT career. As mentioned earlier in this CCNA tutorial, the validity of a CCNA certificate lasts for three years. Exam Exam Fee 200-301 CCNA ExperienceNetwork Technician 120 minutes 50-60 minutes (prices may vary in other countries) In addition to this certification, the new certification process registered by CCNA is detailed by CCNA Cloud CCNA Collaborative CCNA Switching and Routing CCNA Security CCNA Service Provider CCNA Data Center CCNA. CCNA-certified candidates can also prepare for the exam with the help of CCNA Boot Camp. To successfully complete the entire CCNA course with the test, topics such as TCP/IP and OSI models, subnets, IPv6, network address translation (NAT), and wireless access must be thoroughly followed. The CCNA course covers network default installation, operations, configuration, and the underlying IPv4 and IPv6 networks. CCNA networking courses also include network access, IP connectivity, IP services, network security fundamentals, automation, and programmability. The new changes to the current CCNA exam, along with HSRP, DTP, and Ethereum Advanced Troubleshooting Technology Network Design, meet certification eligibility criteria and do not require a degree. However, some employers prefer CCNA basic level programming knowledge internet local area network internet local area network consists of computers. If you interconnect computers within restricted areas such as offices, residences, labs, and so on, this regional network includes WAN, WLAN, LAN, SAN, and so on. Of these wands, LAN and WLAN are the most popular ones. In this guide to ccna research, learn how you can use these network systems to build a local area network. What is a network to understand the need for networking? A network is defined as two or more independent devices or computers connected to resource sharing (such as printers and CDs) sharing, file exchange, or electronic communication allowances. For example, computers on a network can be connected via telephone lines, cables, satellites, radio waves, or infrared beams. There are two common types of networks: local area network (LAN) wide area network (WAN) to know the difference between LAN and WAN in the OSI reference model, layer 3, that is, the network layer is involved in networking. This layer is responsible for packet forwarding, routing through intermediate routers, and recognizing and forwarding local host domain messages to the transport layer (tier 4). The network works by connecting computers and peripherals using two devices, including routing and switches. If two devices or computers are connected to the same link, no network layer is required. Learn more about the types of computer network Internet work devices used on a network You need a variety of Internet work devices for your Internet connection. Some of the common devices used to build the Internet include: NIC: The network interface card or NIC has a circuit board installed on the workstation printed on it. Indicates the physical connection between the workstation and the network cable. NiCs operate in the physical layer of the OSI model, but are also considered data link layer devices. Part of the NIC is to facilitate information between workstations and networks. It also controls the transmission of data to the wire hub: the hub amplifies the signal and then transmits it back to help extend the length of the network cable system. They are basically multiport backsydes and they don't care about the data at all. The hub connects the workstation and sends the transfer to all connected workstations. Bridges: As your network grows, it often becomes difficult to handle. To manage these growing networks, they are often divided into smaller LANs. These small LANS are connected to each other through a bridge. This reduces traffic consumption on the network, but it can also monitor packets as they move between segments. Track mac addresses associated with various ports. Switch: The switch is used for bridge options. It is becoming a simpler and more intelligent way to connect networks than bridges. Information can be transferred to specific workstations. The switch allows each workstation to transmit information over a network independently of the other workstations. It's like a modern phone line with multiple private conversations happening at once. Routers: The purpose of using routers is to pass data to the target device along the most efficient and cost-effective path. Because it operates on network tier 3, it communicates through an IP address rather than a physical (MAC) address. Routers connect two or more different networks together, such as internet protocol networks. Routers can connect different network types such as Ethernet, FDDI, and token rings. Broouters: A combination of routers and bridges. Brouter serves as a filter to convert some data to the local network and redirect unknown data to other networks. Modem: A device that converts a computer-generated digital signal into an analog signal that travels through a telephone line. TCP/IP, which understands the TCP/IP layer, means transport control protocol/Internet protocol. Decide how your computer connects to the Internet and how data is transferred between computers. TCP: You are responsible for subdividing data into small packets before transferring data from the network. It can also be re-assembled when the packet arrives. Internet Protocol (IP): Responsible for resolving, transmitting, and receiving data packets over the Internet. The image below shows the TCP/IP model connected to the OSI layer. Understanding the TCP/IP Internet Layer Understanding the TCP/IP Internet Layer Understanding the TCP/IP Internet Layer, and performing a simple example. If you enter something in the address bar, the request is processed as a server. The server responds back to us with a request. On the Internet, this communication is possible due to the TCP/IP protocol. Messages are sent and received in small packages. The Internet layer of the TCP/IP reference model is responsible for transferring data between the source and target computers. This layer contains two activities that transfer data to the network interface layer, so how does this happen? The Internet layer packs data into data packets called IP datagrams. It consists of the source and destination IP addresses. In addition, the IP datagram header field consists of information such as version, header length, service type, datagram length, and length of residence. At the network layer, you can observe network protocols such as ARP, IP, ICMP, IGMP, and so on. Datagrams are sent over the network using these protocols. They each resemble the same few features. Internet Protocol (IP) is responsible for IP addressing, routing, and fragmentation and re-scription of packets. Decide how messages are routed on the network. Similarly, there is an ICMP protocol. Responsible for diagnostic and reporting errors caused by the failure of delivery of IP packets. The IGMP protocol is responsible for the management of ip multicast groups. An ARP or address resolution protocol is responsible for resolving Internet-layer addresses to the network interface layer. Such as hardware address. RARP is used for computers with low disks to determine ip addresses using a network. The image below shows the format of the IP address. Understanding the TCP/IP transport layer The transport layer is also called the host-to-host transport layer. You are responsible for providing session and datagram communication services to the application layer. The main protocols in the transport layer are the User Datagram Protocol (UDP) and the Transport Control Protocol (TCP). TCP is responsible for sequencing and approving sent packets. It also performs recovery of packets lost during transmission. Packet delivery via TCP is safer and more guaranteed. Other protocols in the same category are FTP, HTTP, SMTP, POP, IMAP, and so on. UDP is used when the amount of data to be transferred is small. Packet delivery is not guaranteed. UDP is used for VoIP, video conferencing, ping, etc. Network segmentationNetwork segmentation suggests splitting the network into smaller networks. It helps to split the traffic load and improve the speed of the internet. Network segmentation can be achieved by implementing a demilitarized zone (DMZ) and a gateway between a network or system with different security requirements in the following ways: Use Internet Protocol Security (IPsec) to implement server and domain isolation. Implement storage-based segmentation and filtering using techniques such as logical unit number (LUN) masking and encryption. If network segmentation is important, improve security to protect against malicious cyberattacks that can compromise network usability by implementing DSD-evaluated cross-domain solutions if necessary - improving security. Network Isolation To detect and respond to unknown intrusions of network problems - provides a quick way to isolate compromised devices from the rest of the network in the in the time of intrusion. Reduce congestion - You can allow additional hosts on the LAN by partitioning the LAN to reduce the number of hosts per network by adding extended network-routers to expand the network. VLAN SegmentationVLAN allows administrators to partition the network. Segmentation is based on factors such as project teams, features, or applications, regardless of the physical location of the user or device. A group of devices connected to a VLAN works as if it were on its own independent network, even if it shared a common infrastructure with other VLAN's. KLANs are used for data links or internet layers, whereas subnets are used for the network/IP layer. Devices within a VLAN can talk to each other without a Layer-3 switch or router. Popular devices used for partitioning are switches, routers, legs, etc. SubnetingSubnets is more concerned about IP addresses. Subnetting is primarily hardware-based, unlike software-based CLNs. A subnet is a group of IP addresses. If the routing device belongs, you can reach the address without using it. The same subnet. In this CCNA tutorial, you will learn some of the things you need to do to properly configure access audit logs that require proper access to a secure network segment ACL or Access list as you perform network segment segmentation - packets, devices, users, applications, and protocols continue to monitor incoming and outgoing traffic security policies based on user identities or applications. It does not allow card holder data to be terminated to other network segments outside the PCI DSS range that are not based on ports, IP addresses, and protocols. Packet delivery process Until now, we have seen different protocols, segmentation, various communication layers, etc. Now let's look at how packets are delivered over the network. The process of passing data from one host to another depends on whether the sending and receiving hosts are in the same domain. Packets can be delivered in two ways, when the packet receiving and transmitting device destined for the remote system from another network is connected to the same broadcast domain, it is possible to exchange data using a switch and a MAC address. However, if the sending and receiving devices are connected to a different broadcast domain, you must use an IP address and router. Layer 2 Packet Delivery Is simple for IP packets within a single LAN segment. Assume host A wants to send packets to hostB. First, the MAC address mapping for host B must have an IP address. In Tier 2, packets are sent to the MAC address to the source and destination addresses. If there is no mapping, Host A sends an ARP request (broadcast to the LAN segment) for the MAC address of the IP address. Host B responds with an ARP reply that accepts the request and represents the MAC address. Segment packet routing packets are headed for systems on the same local network. The send node resolves the packet in the following ways: The number of nodes on the target node is placed in the MAC header destination address field. The node number of the transport node is placed in the MAC header source address field, where the full IPX address of the target node is placed in the IPX header destination address field. The full IPX address of the transport node is placed in the IPX header destination address field. Layer 3 Packet Delivery Requires several steps to deliver IP packets over a routed network. For example, if Host A wants to send a packet to host B, host A sends the packet to the default gateway (the default gateway router). To send packets to the router, Host A must know the Mac address of the router Host A sends an ARP request requesting the Mac address of the router. Broadcast from the local network. The default gateway router accepts ARP requests for MAC addresses. Respond back to the A host with the Mac address on the primary router. You now know the MAC address of the host Arouter. You can send IP packets with the destination address of host B. Packets destined for Host B sent to the primary router by Host A have the following information, and the source IP information of the source Mac address information at the destination Mac address will receive an ARP request from the host A Now Host B from the host A Now Host B to receive an ARP request from the primary gateway router for the host B Mac address when the router receives the packet: Host B responds again with a response indicating the MAC address associated with the ARP reply. The primary router now sends packets to host B segment packet routing, and packet routing occurs when two nodes in different network segments perform in the following way: In the first packet, the MAC header places the target number 20 on the router and in its own source field 01. For IPX headers, place the destination numbers 02, the source fields AA, and 01. While in the second packet, the MAC header places the target number as 02 on the router and the source to 21 on the router. For IPX headers, place the destination numbers 02 and source fields as AA and 01. Wireless regional network network wireless technology was first introduced in the 90s. Used to connect the device to the LAN. Technically, it is called the 802.11 protocol. WLAN or Wireless Local NetworksWLAN is wireless network communication over a short distance using wireless or infrared signals. WLAN is being sold under the Wi-Fi brand name. All components that connect to a WLAN are considered stations and fall into one of two categories. Access Point (AP): The AP transmits and receives radio frequency signals to a device that can receive transmitted signals. Typically, these devices are routers. Clients: Can consist of a variety of devices, such as workstations, laptops, IP phones, desktop computers, and more. All workstations that can be connected to each other are called basic service sets (BSS). Examples of WLAN include WLAN adapter access point (AP) station adapter WLAN switch WLAN router security server cables, connectors, and so on. Unlike CSMA/CD used in Ethernet LANs, the type of WLAN infrastructure peer-to-peer bridge wireless distributed system is the main difference between WLAN and LAN (collision detection and carrier detection multiple access). WLANS USE COLLISION AVOIDANCE AND CARRIER DETECTION MULTIPLE ACCESS (CSMA/CA) TECHNOLOGIES. The WLAN use the Ready to Send (RTS) protocol and the Send Clear (CTS) protocol to avoid conflicts. WLAN uses a different frame format than the one used by wired Ethernet LANs. The WLAN requires additional information in the layer 2 header of the frame. WLAN Critical ComponentsWLAN relies very heavily on these components for effective wireless communication, radio frequency The WLAN Standard ITU-R Local FCC Wireless 802.11 Standard and Wi-Fi Protocol Wi-Fi Alliance range from am radio bands in this one-to-one radio frequency transmission radio range. Radio frequencies are emitted into the air by antennas that generate radio waves. The following factors are radio frequency transmission, absorption - when radio waves protrude from object reflections - when radio waves attack uneven surface scattering - when absorbed by WLAN standards and WLAN standards to establish certification, some tissues have moved forward. The organization has set up a regulatory body to control the use of the RF band. New transmissions, modulations, and frequencies are approved by all regulatory ies of the WLAN service before they are used or implemented. These regulators include the Federal Communications Commission (FCC) for the U.S. European Communications Standards Institute (ETSI) for Europe, which has other authority to define standards for these wireless technologies. This includes the Institute of Electrical and Electronic Engineers (IEEE) International Telecommunication Union (ITU) ITU-R Local FCC WirelessITU (International Telecommunication Union) coordinating spectrum allocation and regulation between all regulatory ies in each country. No license is required to operate wireless equipment in an unauthorized frequency band. For example, the 2.4 gigahertz band is used not only for wireless LANs, but also for Bluetooth devices, microwave ovens and portable mobile phones. The WiFi protocol and the 802.11 standard IEEE 802.11 WLAN use a media access control protocol called collision avoidance and carrier detection multiple access (CSMA/CA) to allow wireless interconnectivity of access points on IEEE 802.11 networks through wireless deployment systems. The Electrical and Electronic Engineers Laboratory (IEEE) 802 standard consists of a family of networking standards that cover the physical layer specifications of technology from Ethernet to wireless. IEEE 802.11 uses ethernet protocols and CSMA/CA for route sharing. The IEEE has defined various specifications (shown in the table) for WLAN services. For example, 802.11g is applied to a wireless LAN. Used to transmit at short distances of up to 54 Mbps in the 2.4 GHz band. Similarly, it can have an extension of 802.11b that applies to wireless LANS and provides 11 Mbps transmission (replaced by 5.5, 2, and 1 Mbps) in the 2.4 GHz band. Use only direct sequence spread spectrum (DSSS). The table below shows the various Wi-Fi protocols and data rates. The Wi-Fi AllianceWi-Fi Alliance provides certification to ensure interoperability between 802.11 products from a variety of vendors. This certification includes early adoption of pending IEEE drafts, such as the IEEE draft, which covers three IEEE 802.11 RF technologies and security. WLAN Security Network Security This is an important issue in the WLAN. As a precautionary measure, random wireless clients should generally be banned from joining the WLAN. WLAN is vulnerable to these various security threats, unauthorized access MAC and IP spoofing session hijack dos (denial of service) attacks in CCNA tutorials, we will learn about the techniques used to secure WLAN from vulnerabilities, WEP (Wired Equivalent Privacy): WEP is used to combat security threats. Provides security to the WLAN by encrypting messages sent from the air. Only listeners with the correct encryption key can decrypt the information. However, it is considered a weak security standard and WPA is a better option in comparison. WPA/WPA2 (WI-FI PROTECTED ACCESS): Introduces the Time Key Integrity Protocol (TKIP) into Wi-Fi to further strengthen security standards. TKIP is regularly renewed and can't be stolen. It also improves data integrity by using stronger hash mechanisms. Wireless Intrusion Prevention System / Intrusion Detection System: A device that monitors the wireless spectrum for the presence of unauthorized access points. There are three deployment models for WIPS, AP (Access Point) does some of the time, ap (access point) has a dedicated WIPS feature built into it by alternating them with regular network connection functions. Therefore, during the implementation of a WLAN, wips and network connectivity functions can be performed at all times of wips deployed through dedicated sensors, and access point placement can have more impact on throughput than standard. The efficiency of a WLAN can be affected by three factors: the location of the topology distance access point. In this CCNA tutorial for beginners you will know how WLAN can be implemented in two ways, ad hoc mode: in this mode, you can connect directly without the need for an access point. This setting is better for small offices (or home offices). The only downside is that security is weak in these modes. Infrastructure mode: In this mode, clients can connect through an access point. Infrastructure mode is categorized into two modes: Basic Service Set (BSS): BSS provides the basic building blocks for the 802.11 wireless LAN. BSS consists of a computer group and one access point (AP) that connects to a wired LAN. There are two types of BSS, independent BSS, and infrastructure BSS. All BSSes have an ID called BSSID. (Mac address of the access point providing the BSS service). Extended Service Set (ESS): The connected BSS set. ESS allows mobile users to roam anywhere, especially within an area where multiple access points (AP) are applied. Each ESS has an ID called SSID. WLAN Topology BSA: The physical area of radio frequency (RF) coverage provided by the access point in BSS. It depends on the RF generated by the deformation caused by the access point power output. Rf. Physical environments that affect remote devices cannot communicate directly, only through access points. The AP begins sending beacons that advertise the characteristics of BSS, such as supported modulation methods, channels, and protocols. ESA: If a single cell doesn't provide enough coverage, you can add cells to expand coverage. This is called ESA. 10-15% redundancy is recommended for wireless voice networks and 15-20% redundancy when remote users roam without losing their RF connection. Data rate: The rate at which data is transmitted is the rate at which information is transmitted between electronic devices. Measured in Mbps. Data rate movement can occur on a per-transport basis. Configure access points: Wireless access points can be configured through a command-line interface or browser GUI. The functionality of an access point typically allows you to adjust parameters such as which radios can be activated, which frequencies are provided, and which IEEE standards to use in that RF. Step 2) Implement wireless as a single access point and a single client without wireless security step 3) Verify that the wireless client has received a DHCP IP address. You can connect to a local wired primary router and browse to the external Internet. Step 4) WPA/WPA2 to help keep your wireless network safe. TroubleshootingWLAN can cause some configuration issues, such as configuring incompatible security methods that configure defined SSID on clients that do not match the access point. Split your environment into wired networks versus wireless networks, and split your wireless network into configuration and RF issues to determine the proper operation of your existing wired infrastructure and related services to ensure that other hosts connected to your existing Ethernet can update your DHCP address and reach the Internet to verify your configuration and eliminate the possibility of RF problems. Co-finds the access point and wireless client together. Always start the wireless client in open authentication and make sure there are metal obstacles when you establish a connection. Lan allows network-enabled printers, network-connected storage, and Wi-Fi devices to connect to each other. If you connect networks across different geographic regions, you can use a wide area network (WAN). In this CCNA tutorial for beginners, we will see how computers from different networks communicate with each other. Router A Routers The device used to connect the network from the LAN. Connect at least two networks and pass packets. According to the information in the packet headers and routing tables, the router connects the network. The primary device required for the operation of the Internet and other complex networks. Routers are categorized into two statics: the administrator manually sets up and configures a routing table to specify each route. Dynamic: You can automatically search for routes. Examine information from other routers. Based on this, you can make packet-by-packet decisions about how to send data over the network. Binary digit BasicComputer over the Internet communicates over an IP address. Each device on the network is identified by a unique IP address. These IP addresses use binary numbers that are converted to decimal places. We'll see this later, first see some basic binary spot classes. Binary numbers include numbers 1,1,0,0,1,1. However, how this number is used to communicate between routing and networks. Let's start with a few basic binary lessons. In binary arithmetic, all binary values consist of 8 bits of 1 or 0. If the bit is 1, it is considered active, and if it is 0, it is not active. How do I calculate binaries? You're familiar with decimal locations like 10, 100, 1000, 10,000, and so on. That's only 10 to power. Binary values work in a similar way, but use base as 2 instead of the default 10. For example, 20, 21, 22, 23, ... 26. The value of the bit rises from left to right. To do this, 1,2,4,.... You will receive a value such as 64. See the table below. Now because you are well aware of the value of each bit of byte. The next step is to understand how these numbers are converted to binaries such as 01101110. Each number 1 in the binary number represents two forces, and each 0 represents 0. In the table above, you can see that bits with values 64, 32, 8, 4, and 2 are turned on and represented by binary 1. Therefore, for binary values in Table 01101110, add the number 64+32+8+4+2 to get the number 110. Important factors for configuring a network address IP address Network configuration must first understand how IP addresses work. The IP address is Internet Protocol. It is primarily responsible for packet routing over packet switching networks. An IP address consists of 32 binary bits that can be divided into the network portion and the host portion. 32 binary bits are divided into four octets (1 octet = 8 bits). Each octet is converted to a decimal point and separated by a period (point). An IP address consists of two segments. Network ID- The network ID identifies the network on which the computer has a host ID- 32 bits is divided into four octets (1 octet = 8 bits) that identify the computer on that network. The values for each octet range from 0 to 255 decimal points. The right most bit of the octet holds a value of 20 and gradually increases to 27 For example, if you have an IP address of 10.10.16.1, the following addresses are first subdivided into the following octets: The values for each octet range from 0 to 255 decimal points. Now you can convert it to binary format. 00001010.000010.0000100100.0001000.00010000.000000000.0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 IP address classIP address classes are categorized into different types: Internet Communication Class B 128-191 Internet Communication Class B 128-191 Internet Communication Class C 192-223 Internet Communication Class D 224-239 Multi-casting Class E 240-254 For internet communication classes reserved for research and experimentation, the type of Internet address that can communicate from internet to Internet, The range of personal addresses that can be communicated on a per-Internet level, and the range of personal addresses of internet addresses. Class Category Class Class A 10.0.0.0 – 10.255.255.255 Class B 172.16.0.0 - 172 .31.255.255 Class C 192-223 - 192.168.255.255 Multiple organizations of subnets and subnet masks may be required. To do this, you need to set up a network with more than 1,000 hosts in multiple buildings. This array can be made by splitting the network into subdivisions known as subnets. Network size is affected, and network classes that apply to network numbers that receive the IP addressing schema that you use for network performance can be negatively affected by crashes and the resulting traffic load. That subnet masking can be a useful strategy. Apply a subnet mask to the IP address and split the IP address into two parts, dividing it into extended network addresses and host addresses. Subnet masks help you pinpoint where the endpoints of a subnet are located if they are provided within that subnet. Classes have different default subnet masks, and Class A-255.0.0.0 Class B-255.255.0 Class C- 255.255.255.0 Router Security protects routers from unauthorized access, tampering, and eavesdropping. For these usage technologies, the highly secure connection point threat defense path Point Threat Defense VPN with guest traffic: Route user traffic directly to the Internet to guests and return corporate traffic to headquarters. This ensures that guest traffic does not pose a threat to the corporate environment. Access to the public cloud: Only the selected type of traffic can use the local Internet route. A variety of security software, such as firewalls, can provide protection against unauthorized network access. Full direct Internet access: All traffic is routed to the Internet using a local route. This protects enterprise-class threats from enterprise-class threats. VPN solutions protect different types of WAN designs (public, private, wired, wireless, etc.) and the data they perform. Data can be divided into two categories from the rest of the data in the transfer data that is secured through the following technologies: Encryption (origin authentication, hiding topology, etc.) compliance standards (HIPAA, PCI DSS, Sabane Oxley) compliance summary: CCNA full form or CCNA abbreviation is Cisco A network-connected Internet local area network is a network of computers that interconnect computers within a restricted area. WAN, LAN, and WLAN are the most popular Internet local area networks according to the OSI reference model, tier 3, that is, network layer 3 is involved in networking layer 3, which is involved in packet delivery, routing through intermediate routers, and recognizing and delivering local host domain messages to the transmission layer (tier 4). For some of the common devices used to build a network, the NIC hub bridge switch router TCP is responsible for decomposing data into small packets before being transmitted from the network. The TCP/IP reference model at the Internet tier does two things, and it is safer to transfer data through TCP to the network interface layer that routes data to the correct targetpackit delivery, and UDP is used when the amount of data being transmitted is small. Packet delivery is not guaranteed. Network segmentation can be delivered in two ways by combining splitting the network into smaller network VLAN subdivision subnets, packets destined for remote systems from other networks destined for the system of the same local network WLAN is a wireless or infrared signal connecting to the WLAN all components connecting to the WLAN through wireless network communication at a short distance is considered a station and belongs to one of two categories. WLAN uses CSMA/CA technology technology that allows routers to connect two networks and pass packets between routers, and IP addresses are internet protocols that are critical to switching packets, using CSMA/CA technology technology that allows routers to implement wired equivalent privacy (WPA/WI-FI protected access) wireless intrusion prevention system/intrusion detection system WLAN in two ways. The IP address consists of two segments that communicate over the Internet personal range of IP addresses, download the very secure connection download PDF CCNA interview question and answer page 2 PDF 1, what is classified as a secure router from unauthorized access and eavesdropping using branch threat defense VPN? Routing is the process of finding a path that data can pass from source to target. Routing occurs on a device called a router, which is a network-layer device. 2) What is the purpose of the data link? The task of the data link layer is to ensure that messages are sent to the correct device. Another feature of this layer is the frame. 3) What are the main advantages of using the switch? When a switch receives a signal, it frames it from the bit of that signal. This process allows you to gain access, read the destination address, and pass the frame to that port. This is a very efficient means of data transfer instead of broadcasting from any port. 4) When does network congestion occur? Network congestion occurs when there are too many users. You want to use the same bandwidth. This is especially true for large networks that do not rely on network segmentation.5) What is a window into networking terminology? The window indicates the number of segments that can be sent from the source to the target before sending the approval back. 6) Do bridges split the network into smaller sections? Not really. What bridges actually do is filter using large networks without changing the size of the network. 7) What LAN switching methods are being used in CISCO Catalyst 5000? The CISCO Catalyst 5000 use storage and forward switching methods. Stores the entire frame in a buffer, performs a CRC check, and decides whether to pass that data frame. 8) What is the role of the LLC lower tier? The LLC lower tier means logical link control. You can provide optional services to application developers. One option is to use stop/start code to provide flow control to the network layer. The LLC may also provide error correction. 9) How is RIP different from IGRP? RIP relies on the number of hops to determine the best route to the network. IGRP, on the other hand, considers a number of factors before deciding on the best path to take, such as bandwidth, reliability, MTU, and hops. 10) What are the other memories used by CISCO routers? Other memories used by CISCO routers include - NVRAM stores startup configuration files. - DRAM stores the running configuration file. - Flash Memory - Stores Cisco IOS. 11) What is BootP? BootP is a protocol used to boot diskless workstations that are connected to a network. It is short for boot programs. Diskless workstations also use BootP to determine their own IP address and that of the server PC. 12) What are the features of the application layer in networking? The application layer supports the communication components of the application and provides network services to application processes that exceed the OSI reference model specification. It also synchronizes applications on the server and client. 13) When using a CISCO router, such as looking at system information, connecting to a remote device, and checking the status of the router, differentiating the user mode from the privileged mode user mode is used for normal tasks. Privileged mode, on the other hand, includes all the options available in user mode and many more. You can use this mode to create configurations on your router, including testing and debugging. 14) What is 100BaseFX? Ethernet with fiber optic cable as the main transmission medium. 100 means a data rate of 100 Mbps. 15) Differentiate the entire duplex from the semi-duplex. In a completely double, both the transmitting device and the receiving device can communicate at the same time, that is, both can be transmitted and received at the same time. In the case of a half-weight, the device cannot receive it during transmission. Anti. 16) What is an MTU? MTU means maximum transfer device. The maximum packet size that can be sent to a line of data without the need for fragmentation. 17) How does cut-through LAN switching work? Cut-through LAN switching sends the router back immediately as soon as it receives the data frame, reads the destination address, and passes it to the next network segment. 18) What is the waiting time? Latency is a time delay that network devices measure from when they receive data frames to when they are sent back to other network segments. 19) Utilizing RIP, what are the limits when it comes to the number of hops? The maximum limit is a 15-hop count. Something higher than 15 indicates that you are considered unable to connect to the network. 20) What is a frame relay? Frame relays are WAN protocols that provide connection-oriented communication by creating and maintaining virtual circuits. It has a high-performance rating and works on data links and physical layers. 21) How do I configure my Cisco router to route IPX? The initial thing to do is to enable IPX routing using the IPX routing command. Each interface used in the IPX network is then configured with a network number and encapsulation method. 22) What are the other IPX access lists? There are two types of IPX Access List 1: Standard.2. Extension.Standard Access List can only filter source or destination IP addresses. The extended access list use source and destination IP addresses, ports, sockets, and protocols when filtering the network. 23) Explain the benefits of VLAN. VLAN allows you to create conflict domains in groups other than physical locations. With VLAN, you can set up your network in a variety of ways, including features, hardware types, protocols, and more. This is a huge advantage when compared to traditional LANs, where conflict domains are always connected to physical locations. 24) What is a subnet? Subnetting is the process of creating a smaller network from a large parent network. As part of the network, each subnet is assigned several additional parameters or identifiers to represent subnet numbers. 25) What are the advantages of tiered models in the networking industry? Tiered networks offer many benefits. Administrators can change one layer without having to change another layer. Encourage specialization to help the network industry evolve faster. Layered models also help administrators solve problems more efficiently. 26) Why do UDP leases prefer to be compared to TCP? This is because UDP is unreliable and out of order. Virtual circuitry and recognition cannot be established. 27) What are some standards supported by the presentation layer? The presentation layer supports many standards, so make sure your data is displayed correctly. This includes PICT, TIFF, and JPEG for graphics, MIDI, MPEG, and graphics. For video/audio only. 28) What is the easiest way to configure the router remotely? If you need to configure your router remotely, the most convenient way is to use a Cisco auto-installation procedure. However, the router must connect to a WAN or LAN through one of the interfaces. 29) What does the show protocol show? - Routing protocol configured on the router. - The address assigned to each interface. - Encapsulation method configured for each interface. 30) How do you describe the IP address? There are three possible ways to do this: using dotted points. Example: 192.168.0.1 - Uses binary. Example: 1000000010.00111111.0110010.01110011 using Hexadecimal. For example: 82 1E 10 A1 31) How do I go to privileged mode? How do I switch back to user mode? To access privileged mode, type Activate command at the prompt. To return to user mode, type the command Deactivate. 32) What is HDLC? HDLC means a high level of data link control protocol. It is a courtesy protocol of CISCO. A basic encapsulation that operates within a CISCO router. 33) How do I create internet work? InternetWorks is created when the network connects using a router. Specifically, the network administrator assigns logical addresses to all networks that connect to the router. 34) What is bandwidth? Bandwidth is the transfer capacity of a medium. A measure of the volume that a transmission channel can handle, measured in Kbps. 35) How does holddown work? The hold removes the link from the update message to prevent it from restoring the aborted link. Use triggered updates to reset the hold timer. 36) What is a packet? Packets are the result of data encapsulation. These are data that is lapping up according to different protocols in the OSI layer. Packets are also called datagrams. 37) What is the segment? A segment is a section of a data stream that comes from the parent OSI layer and is ready to be transferred towards the network. Segments are logical units of the transport layer. 38) Provides some benefits of LAN switching. - Allow full dual data transfer and reception - Media Speed Adaptation - Easy and efficient migration 39) What is path addiction? Path poisoning is the process of inserting a table entry in 16 into a path that makes it impossible to connect. This technique is used to avoid problems caused by inconsistent updates in the path. 40) How do I find a valid host on a subnet? The best way to move on this is to use equation 256 minus the subnet mask. Hosts that are considered valid are hosts that can be found between subnets. 41) What is DLCI? DLCI or data link connection identifiers are typically assigned by the frame relay service provider to uniquely identify each virtual circuit that exists on the network. 42) Provides an overview of the conversion steps for data encapsulation. At the reference point of the data transmitter, The end user is converted to a segment. The segment is then passed to another layer and converted into packets or datagrams. These packets are then converted into frames before being forwarded to the network interface. Finally, the frame is converted to bits before the actual data transfer. 43) What other types of passwords are used to secure CISCO routers? There are five types of passwords that you can actually use. This allows you to use secrets, virtual terminals, consoles, and assistive features. 44) Why is network segmentation good when managing large networks? For network management, subdividing a network makes network traffic easier and ensures that all users always have high bandwidth. This translates into better performance, especially in growing networks. 45) What can be accessed from the identifying information of the CISCO router? The host name and interface. The host name is the name of the router. The interface is a fixed configuration that references the router port. 46) Distinguishing between a physical topology logical topology and a logical topology is a signal path through a physical topology. The physical topology is the actual layout of the network media. 47) What causes the triggered update to reset the router hold timer? This can happen if the hold timer has already expired or if the router has received a processing operation that is proportional to the number of links in the Internet operation. 48) What commands should I use to delete configuration data stored in NVRAM when configuring my router? A. Run -config B. Start clearing -config C. NVRAM D. Delete NVRAM Correct Answer: B. Start -config 49) See the command shown, which command should be used for branch routers before traffic sent to router next? Hostname: Branch Hostname: Remote PH# 123-6000, 123-6001 PH# 123-8000, 123-8001 SPID1: 32055512360001 SPID1: 32055512380001 SPID2: 32055512360002 SPID2: 32055512380002 ISDN switch-type basic ni username Remote password cisco interface bri0 IP address 10.1.1.1 255.255.255.0 encapsulation PPP PPP authentication chap ISDN spid1 41055512360001 ISDN spid2 41055512360002 dialer map IP 10.1.1.2 name Remote 1238001 dialer-list 1 protocol IP permit Correct Answer: (config-if)# dialer-group 1 50) When configuring a router utilizing both physical and logical interfaces, what factor must be considered in determining the OSPF router ID? The highest IP address of the physical interface. The lowest IP address of the logical interface. The intermediate IP address of the logical interface. The lowest IP address of the physical interface. The highest IP address of all interfaces. The highest IP address in the logical interface. The lowest IP address in the interface. Correct answer: A. The highest IP address of the physical interface. 51) What is the difference between switches, hubs and routers? The hub switch router hub has a single one. Domains and conflict domains. Coming from one port is sent to another port. A device that filters and forwards packets between LAN segments. The switch has a single broadcast domain and multiple conflict domains. It supports all packet protocols operating on data link layer 2 and tier 3 routers, and 3 routers are devices that transmit data packets along the network. 52) What is the size of the IP address? The size of the IP address is 32 bits for IPv4 and 128 bits for IPv6. 53) Do you mention what data packets make up? A data packet consists of the sender's information, the recipient's information, and the contained data. There is also a numeric identification number that defines the packet number and order. When data is sent over the network, that information is split into data packets. In short, data packets pass information about the messages sent and routing configurations. 54) What does DHCP mean? DHCP means dynamic host configuration protocol. DHCP automatically assigns IP addresses to specified workstation clients. You can also create static IPS on computers such as printers, servers, routers, and scanners. 55) Mention what BOOTP is? BOOTP is a computer networking protocol used by configuration servers to deploy IP addresses to network devices. 56) Can you explain why UDP prefers TCP over TCP? This is because UDP does not have a sequence and is not trusted. You can't create virtual circuits and recognition. 57) Specify the difference between dynamic IP and static IP address? Dynamically, IP addresses are provided by DHCP servers, and static IP addresses are provided manually. 58) Mention the scope for private IP? The range for private IP is Class A: 10.0.0.0. – 10.0.0.255 Class B: 172.16.0.0 – 172.31.0.0 Class C: 192.168.0.0 – 192.168.0.255 59) How many ways to access the router? Telnet (IP) AUX (Phone) Console (Cable) 60 What is EIGRP? EIGRP means an improved internal gateway routing protocol and is a routing protocol designed by Cisco Systems. Used for routers that share routes with other routers within the same autonomous system. Unlike other routers such as RIP, EIGRP only sends gradual updates, reducing the workload on the router and the amount of data it needs to transfer. 61) What is the coefficient of the EIGRP protocol? The EIGRP protocol consists of bandwidth load delay reliability MTU maximum transfer device 62) What does the clock speed do? Your watch can communicate properly with your router or DCE equipment. 63) Which command should I use to delete or remove configuration data stored in NVRAM? Start Erasing - Coding is the difference between TCP and UDP, which commands should I use if I want to delete configuration data stored in nvram 64) hats? Both TCP and UDP are protocols for transferring files over a computer network. Transport Control Protocol (TCP) User Datagram Protocol (UDP) A connection-oriented protocol. If the connection is lost during file transfer, the server will request the lost part. There is no corruption during message transfer while UDP sends messages based on connectionless protocols. When you send data, there is no guarantee that the messages sent will reach you without leakage, the messages are delivered in the order in which they are sent, and the data in TCP may not be in the same order as it is read into the stream. When one packet ends and another packet begins to be sent individually and arrives at the example of TCP, does the example on the World Wide Web, file transfer protocol, e-mail, UDP explain the difference between VOIP (voice over Internet protocol) TFTP (trivial file transfer protocol) 65) semi-duplex and full duplex? Full redundancy means that communication can occur in both directions at the same time, and half-weight means that communication can occur in one direction at a time. 66) What are the conversion steps for data encapsulation? The conversion phase of data encapsulation includes layers 1, 2, and 3 (applications/presentations/sessions): The user's alphanumeric input is converted to data layer 4 (transfer): The data is converted to a small segment layer 5 (network): Is there a data converted to a packet or datagram, and a network header converted to layer 6 (data link): If the datagram or packet is built into frame 7 layer (physical frame conversion), are there 6 stuck commands? Cntrl +Shift +F6 and X are the commands we provide if the router iOS is attached. 68) What is path addiction? Path poisoning is a technique that prevents a network from sending packets over an invalid path. 69) In the case of RIP, what path entries are assigned to the dead or wrong path? For RIP table entries, 16 hops die or are assigned to the wrong path and cannot be connected. Page 3 Details Last updated: 11 November 2020 Then a curated list of the top 80 CCNA (Cisco Certified Network Colleagues) courses for beginners and professionals. CCNA learning is essential for network engineers and ensures network installation, monitoring, and troubleshooting. This course covers concepts such as routing and switching, packet tracers, FHRP, security, subneting, and more. The best CCNA courses now you can see a list of 80 best CCNA courses that will help you become a certified network expert. There are many online CCNA courses on this list, some are free and some are paid for. FAQ⚡ can I get a printable certificate? Yes, you will receive a print certificate in many courses. In fact, some course providers can send certificates to the address they want, Ỿ eligible to sign up for a CCNA course? Most courses: Basic networking knowledge. Basic PC operating system navigation technology. All server knowledge is not obsessive, but understated. 💻 if I miss a class? All recorded and can be played later. ✔ I don't like the CCNA course I purchased? Most courses offer a 30-day return policy or have a 7? free trial. Most courses have forums where course authors can ask frequently answered questions. Author.