

## Introduction to networks (version 6.00) - ccna 6.0 itn final exam

Ccna 3 v6 Final exam answers | ccna 3 v6 examen Final Like and subscribe to my channel ccna 3 v6 Final exam answers 2018 1... Este curso CCNA 3 v6.0 Routing and Switching: Escalamiento de redes en Español. Este curso CCNA 3 Escalamiento de redes se centra en la arquitectura, los componentes y las operaciones de los routers y los switches en redes Examen Practico Final. Test Online. CCNA 3 v6.0 Examen Final Opción A.2|- CCNA 3 Examen Final Op 10/10.3Test CCNA 3 V6 Examen Final A examen de ccna 3. ¿Cuál es el término que se usa para el área de una red que se ve afectada cuando un dispositivo. La falla de un bloque de interruptores no afectará a todos los usuarios finales. Esta es una característica de seguridad disponible en todos los nuevos...4CCNA 3 Practice Final Exam v5.0 v5.0.2 v5.0.3 v5.1 v6.0 Exam Questions Answers 2019 100% Update 2017 - 2018 Latest version Scaling The AS number is not associated with the global Autonomous System number that is assigned by IANA, because EIGRP is an interior gateway protocol.5Examen Final V 6. CCNA3 v6.0 Final Exam A 010. Include a router in the topology. Associate hosts A and B with VLAN 10 instead of VLAN 1. CCNA3 v6.0 Final Exam A 009. The other switches in the domain can be running either VTP version 1 or 2.6CCNA 3 v6.0 Scaling Networks course describes the architecture, components, and operations of routers and switches in larger and more complex networks. Configure, verify and troubleshoot routers in a complex routed IPv4 or IPv6 network using single-area OSPF, multi-area OSPF, and...7Cisco CCNA 1 ITN v6.0 Practice Final Exam Answers Routing and Switching (RS) Introduction to Networks (ITN) (Version 6.00) collection year 2017, 2018 and 2019 Full 100%. CCNA 1 has been know as ITN. The following are the questions exam answers.8CCNA3 v6 it the latest update curriculum from Cisco. CCNA3 v6 it the latest update curriculum from Cisco. There are 10 chapters plus 6 Packet Tracer labs. All question for each chapter, we have verified and make a correctamente la manera en la que un switch LAN reenvía las tramas que recibe? Solo las tramas con una dirección de destino de difusión se reenvían a todos los puertos del switch activity in Packet Tracer. This virtual CCNA1 Practice Final lab activity is designed to test if you have skill and knowledge required to pass the Cisco Academy CCNA 6.0 - Introduction to Networking Final Skills Assessment.12CCNA 2 v6 Examen Practico Final Pregunta 3 ¿Cuál es el valor de distancia administrativa que indica la ruta para que el R2 alcance la red 10.10../16? RAM\* NVRAM ROM Memoria flash 9. ¿Qué dos estados de licencia se esperarían en un nuevo router Cisco una vez que se haya activado la licencia?13Regresar al índice. 1. ¿Cuál es una característica de una red tolerante a fallos? \*\*Una red que se recupera rápidamente cuando ocurre un fallo. 2. Tres empleados del banco están utilizando la red corporativa.14CCNA 1 v6.0 2019 Collection, Introduction to Network(ITN), Full mark 100%, Assignemnts-Assessments-Quiz-Exam Online-Final-PT Lab, ITN Pilot and ITN Exam Beta. This version 6.0 and include chapter and final exam with random new questions updated.15Español- English. EXAMEN 1 (opcion A). 1.¿Cuál es una característica de una red tolerante a fallos? Una red que se recupera rápidamente cuando ocurre un fallo y depende de la redundancia para limitar el impacto de un fallo. 2. Tres empleados del banco están utilizando la red corporativa. 16 CCNA 1 v6: This course introduces the architecture, structure, functions, components, and models of the Internet and other computer networks. The principles and structure of IP addressing and the fundamentals of Ethernet concepts, media, and operations are...17A network administrator uses Telnet to connect to the switch, which password is needed to access user EXEC mode? CCNA1 Practice Final v5.1 004.18Cisco Netacad ScaN CCNA 3 Chapter 10 Exam Answers v5.0 v6.0 2017 2018 2019 Scaling Networks (Version 6.0) Practice Test Questions Online - Verified 100%.19Exista trei tipuri de examene obligatorii: examene de capitol, evaluare practică și examen final teoretic. Examenul final se susține sub supraveghere la sala de curs Telecom Academy. CCNA Routing and Switching este o certificare de nivel Associate care validează abilitățile de a instala...201. ¿Qué método puede utilizar dos equipos para garantizar que los paquetes no se descartan porque se envían demasiados datos demasiados datos demasiado rápido? Encapsulación. \*\*control de flujo. Método de acceso. Tiempo de espera de respuesta.21CCNA 4 Final Exam Answers 2020 v6.0+v7.0 - Connecting Networks. 1. Which statement best describes a WAN? CCNA 3 v7.0 Final Exam Answers Full - Enterprise Networking, Security, and Automation. 1. A company uses a cloud-based payroll system.22CCNA 1 Final Exam Model Payroll system. (V6.0) On Friday, June 9, 2017. 1. Refer to the exhibit. CCNA 3 - LAN Switching and Wireless (V4.0). CCNA 4 - Accessing the WAN (V4.0). 23saveSave Cisco CCNA2 Examen Final For Later. 42K views. 3Up votes, mark as useful. Cisco CCNA2 Examen Final. Uploaded by. sl4xls. Examen Practico Final CCNA 2.24What is the problem? CCNA1 v7 - ITNv7 - Practice Final - ITN Answers 003. The entire command, configure terminal , must be used. A default gateway is only required to communicate with devices on another network. The absence of a default gateway does not affect connectivity between devices on...254. A user calls the help desk to report that a Windows XP workstation is unable to connect to the network after startup and that a popup window says "This connectivity." 26200-125: Cisco Certified Network Associate (CCNA). La superación de este examen acredita al candidato con la obtención de la certificación oficial asociada CCNA Routing and Switching. El alumno realizará el examen de certificación en las instalaciones de PUE gracias a su condición de centro...27 Last Updated on June 14, 2021 by Admin CCNA1 v7 & v7.02 - ITNv7 - Final Exam Answers 2020 2021 correct 100% Cisco Netacad ITN Version 7.00 CCNA 1 v7 Final Exam Answers 2020 2021 - Introduction to Networks ITN (Version 7.00 & v7.02) - ITNv7 Final Exam Answers 2020 2021 Enter CTRL-Z at the privileged mode prompt. Power cycle the device. Exit global configuration mode. Reboot the device. Exit global configuration mode. Reboot the device. Enter, and the banner message appears. Power cycling a network device that has had the banner motd command issued will also display the banner message, but this is not a quick way to test the configuration. The switch requires a username/password combination for remote access. The SSH client on the switch is enabled. Communication between the switch and remote users is encrypted. The switch requires remote connections via a proprietary client software. Answers Explanation & Hints: The transport input ash command when entered on the switch vty (virtual terminal lines) will encrypt all inbound controlled telnet connections. 2001:DA48::/64 2001::/64 2001:DA48:FC5:A4::/64 2001:DA48:FC5::A4:/64 It must send a DHCPv6 Request the address of the DNS server. It must send a DHCPv6 Request message to request the address. It must send a DHCPv6 Request message to the DHCPv6 Request message to request the address. It must send a DHCPv6 Request message to request the address. It must send a DHCPv6 Request message to request the address of the DNS server. It must send a DHCPv6 Request message to request the address of the DNS server. It must send a DHCPv6 Request message to request message to request the address of the DNS server. It must send a DHCPv6 Request message to request the address of the DNS server. It must send a DHCPv6 Request message to request the address of the DNS server. It must send a DHCPv6 Request message to request the address of the DNS server. It must send a DHCPv6 Request message to request the address of the DNS server. It must send a DHCPv6 Request message to request the address of the DNS server. It must send a DHCPv6 Request message to request the address of the DNS server. It must send a DHCPv6 Request message to request message to request the address of the DNS server. It must send a DHCPv6 Request message to request the address of the DNS server. It must send a DHCPv6 Request message to request message to request the address of the DHCPv6 Request message to request the address of the DHCPv6 Request message to request message t an ICMPv6 Neighbor Solicitation message to ensure that the address is not already in use on the network. Explanation: Stateless Address Autoconfiguration (SLAAC) does not. A SLAAC client can automatically generate an address that is based on information from local routers via Router Advertisement (RA) messages. Once an address has been assigned to an interface via SLAAC, the client must ensure via Duplicate Address Detection (DAD) that the address is not already in use. It does this by sending out an ICMPv6 Neighbor Solicitation message and listening for a response. If a response is received, then it means that another device is already using this address. FE80::/10 FDEE::/7 FF00::/8 FEC0::/10 Explanation: Link-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses and used the prefix range FEC0::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses and used the prefix range FEC0::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local addresses are in the range of FE80::/10. The original IPv6 specification defined site-local ad unique local address because it is in the range of FC00::/7 to FDFF::/7. IPv6 multicast addresses have the prefix FF00::/8. It checks the value of the TTL field and if it is 100, it discards the packet and sends a Parameter Problem message to the source host. It checks the value of the TTL field and if it is 0, it discards the packet and sends a Destination Unreachable message to the source host. It decrements the value of the TTL field by 1 and if the result is 0, it discards the packet and sends a Destination Unreachable message to the source host. It decrements the value of the TTL field by 1 and if the result is 0, it discards the packet and sends a Destination Unreachable message to the source host. options security interference coverage area packet collision extensive cabling Explanation: The three areas of concern for wireless networks focus on the size of the coverage area, any nearby interference, and providing network security. Extensive cabling is not a concern for wireless networks, as a wireless network will require minimal cabling for providing wireless access to hosts. Mobility options are not a component of the areas of concern for wireless networks. CCNA1 v7 - ITNv7 - Final Exam Answers 07 The untwisted length of each wire is too long. The woven copper braid should not have been removed. The wrong type of connector is being used. The wires are too thick for the connector that is used. Answers Explanation & Hints: When a cable to an RJ-45 connector is terminated, it is important to ensure that the untwisted wires are not too long and that the flexible plastic sheath surrounding the wires is crimped down and not the bare wires. None of the colored wires should be visible from the bottom of the jack. EMI signal attenuation crosstalk RFI extended length of cabling Explanation: EMI and RFI signals can distort and corrupt data signals that are carried by copper media. These distortions usually come from radio waves and electromagnetic devices such as motors and florescent lights. together with the magnetic field of one wire affecting another. Signal attenuation is caused when an electrical signal begins to deteriorate over the length of a copper cable. TCP is the preferred protocol when a function requires lower network overhead. The source port field identifies the running application or service that will handle data returning to the PC. The TCP source port number identifies the sending host on the network. UDP segments are encapsulated within IP packets for transport across the network. The UDP destination port number identifies the destination port when establishing a session with the server. Explanation: Layer 4 port numbers identify the application or service which will handle the data. The source port number is added by the sending device and will be the destination port number when the requested information is returned. Layer 4 segments are encapsulated within IP packets. UDP, not TCP, is used when low overhead is needed. A source IP address, not a TCP source port number, identifies the sending host on the network. Destination or service monitors for requests. CCNA1 v7 - ITNv7 - Final Exam Answers 01 netsh interface ipv6 show neighbor arp -a tracert ping ipconfig nslookup telnet Explanation: The ipconfig and nslookup commands will provide initial IP address and DNS configuration information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigning correct information to the technicians and determine if DHCP is assigned to the technicians and determine if DHCP is assigned to the technicians and determine information to the technicians and determin address, or using the known correct default gateway address if these are found to be different. The arp -a or netsh interface ipv6 show neighbor commands could be used if the problem is then suspected to be an IP address to MAC address mapping issue. The telnet and tracert utilities could be used to determine where the problem was located in the network if the default gateway configuration was found to be correct. speed and duplex settings MAC addresses next-hop addresses interface brief shows the IP addresses interface descriptions IP addresses next-hop addresses 255.255.128 transport layer error check field error correction provides for the exchange of frames over a common local media provides end-to-end delivery of data between hosts provides the formatting of data After detecting a collision, hosts can attempt to resume transmission after a random time delay has expired. A jam signal indicates that the collision has cleared and the media is not busy. All of the devices on a segment see data that passes on the network medium. The device with the electronic token is the only one that can transmit after a collision. Devices can be configured with a higher transmission priority. A device listens and waits until the media is not busy before transmitting. an attack that slows or crashes a device or network the use of stolen credentials to access private data end-device installation media selection message encoding delivery options connector specifications message size If a device receiving an ARP request has the destination IPv4 address, it responds with an ARP reply. When a host is encapsulating a packet into a frame, it refers to the MAC address table to determine the mapping of IP addresses to MAC addresses. If no device responds to the ARP request, then the originating node will broadcast the data packet to all devices on the Ethernet LAN and contains the IP addresses of the destination host and its multicast MAC address. If a host is ready to send a packet to a local destination device and it has the IP address but not the MAC address. First it determines if the destination, it generates an ARP broadcast. Explanation: When a node encapsulates a data packet into a frame, it needs the destination device is on the local network. checks the ARP table (not the MAC table) to see if a pair of IP address and MAC address exists for either the destination host is on the local network). If the match does not exist, it generates an ARP broadcast to seek the IP address to MAC address resolution. Because the destination MAC address is unknown, the ARP request is broadcast with the MAC address, which enables the sending node to assemble the frame. If no device responds to the ARP request, then the originating node will discard the packet because a frame cannot be created. CCNA1 v7 - ITNv7 - Final Exam Answers 06 The entire command, configuration mode. The administrator must first enter privileged EXEC mode before issuing the command. Answers Explanation & Hints: In order to enter global configuration mode, the command configuration mode, the command configuration as config t, must be entered from privileged EXEC mode. In this scenario the administrator is in user EXEC mode, as indicated by the > symbol after the hostname. The administrator would need to use the enable command to move into privileged EXEC mode before entering the configure terminal command. CCNA1 v7 - ITNv7 - Final Exam Answers 05 This host does not have a default gateway configured. There are 4 hops between this device at 192.168.100.1. The average transmission time between the two hosts is 2 milliseconds. There is connectivity between this device and the device at 192.168.100.1. It can be determined that 4 hops exist between them and the average transmission time is 1 milliseconds. Layer 3 connectivity does not necessarily mean that an application can run between the hosts. retransmits packets if errors occur guarantees delivery of packets does not require a dedicated end-to-end connection operates independently of the network media reassembles out of order packets into the correct order at the receiver end Explanation: The Internet Protocol (IP) is a connection nor does it guarantee delivery of packets. IP is also media independent, which means it operates independently of the network media carrying the packets. The host cannot communicate with hosts in other networks. The host cannot communicate with other hosts in the local network. A ping from the host to 127.0.0.1 would not be successful. The switch will not forward packets initiated by the host. Answers Explanation & Hints: When a host needs to send a message to a remote network, it can forward the message to a remote destination host cannot be used directly. Instead, the IP packet has to be sent to the router (default gateway) and the router will forward the packet toward its destination. Therefore, if the default gateway is incorrectly configured, the host can communicate with other hosts on the same network, but not with hosts on remote networks. automation authorization accounting authenticated (logged into the server), the authorization is the process of determining what network resources the user can access and what operations (such as read or edit) the user can perform. loss of light over long distances low-quality cable or connectors low-quality shielding in cable installing cables in conduit improper termination A student has two web browser windows open in order to access two web sites. The transport layer ensures the correct browser windows open in order to access two web sites. into the phone is a transport layer address used to contact another network. A corporate worker is accessing a web server located on a corporate worker is accessing a short webbased movie with sound. The movie and sound are encoded within the transport layer header. Explanation: The source and destination port numbers are used to identify the correct application. Each router interface will generate an IPv6 link-local address. The IPv6 enabled router interfaces begin sending ICMPv6 Router Advertisement messages. It statically creates a global unicast address on this router. All router interfaces will be automatically activated. POP DNS IP TCP Ethernet UDP integrity scalability quality of service fault tolerance powerline networking security CCNA1 v7 - ITNv7 - Final Exam Answers 04 open the header and use it to determine whether the data is to be sent out S0/0/0 open the header and replace the destination MAC address with a new one nothing, because the router has a route to the data one of th of those headers is the Layer 2 header. Because PC1 connects to an Ethernet network, an Ethernet header is used. The source MAC address will be that of G0/0 on R1. When R1 gets that information, the router removes the Layer 2 header and creates a new one for the type of network the data will be placed onto (the serial link). transport application network session data link presentation CCNA1 v7 - ITNv7 - Final Exam Answers 02 Explanation: Link-Local addresses are assigned automatically by the OS environment and are located in the block 169.254.0.0/16. The private addresses ranges are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. TEST-NET addresses belong to the range 192.0.2.0/24. The addresses in the block 240.0.0.0 to 255.255.255.254 are reserved as experimental addresses. Loopback addresses belong to the block 127.0.0.0/8. strengthening of a signal by a networking device leakage of signals from one cable pair to another loss of signal strength as distance increases time for a signal to reach its destination Answers Explanation & Hints: Data is transmitted on copper cables as electrical pulses. A detector in the network interface of a destination device must receive a signal that can be successfully decoded to match the signal sent. However, the farther the signal travels, the more it deteriorates. This is referred to as signal attenuation. Capture traffic during peak utilization times to get a good representation of the different traffic types. Perform the capture on different traffic types. Perform the capture traffic types. network that receive most of the traffic such as the data center. Capture traffic flow patterns should be gathered during peak utilization times to get a good representation of the different traffic types. The capture should also be performed on different network segments because some traffic will be local to a particular segment. CCNA1 v7 - ITNv7 - Final Exam Answers 03 Layer 2 destination address = 00-00-0c-94-36-bb Layer 3 destination address = 172.16.20.200 Layer 3 source address = 172.16.10.200 Layer 2 destination address = 00-00-0c-94-36-bb Layer 2 source address = 172.16.20.200 Layer 3 source address = 172.16.10.200 Layer 3 destination address = 00-00-0c-94-36-bb Layer 2 source address = 172.16.20.200 Layer 3 source address = 172.16.10.200 Layer 3 destination address = 172.16.20.200 Layer 3 destination address = 172.16.200 Layer 3 destination address = 172.16.200 Layer 3 destination address = 172.16.200 Layer 3 destination address = 1 address = 00-00-0c-94-36-bb Layer 3 destination address = 172.16.20.200 Layer 3 source address = 172.16.100.200 Layer 3 destination address = 172.16.10.200 Layer 3 destination address = 172.16.10.Layer 2 source address = 00-00-0c-94-36-bb Layer 3 destination address = 172.16.20.99 Layer 3 source address = 172.16.10.200 192.168.1.64/26 Explanation: For the subnet of 192.168.1.64/26, there are 6 bits for host addresses, yielding 64 possible addresses. However, the first and last subnets are the network and broadcast addresses for this subnet. Therefore, the range of host address 192.168.1.26 to 192.168.1.26. The other subnets do not contain the address are the network and reply messages may slow down the switching process, leading the switch to make many changes in its MAC table. The ARP request is sent as a broadcast, and will flood the entire subnet. Switches become overloaded because ARP reply messages must be processed by all nodes on the local network. The network may become overloaded because ARP reply messages have a very large payload due to the 48-bit MAC address and 32-bit IP address that they contain. adds Ethernet over fiber and 1 Gigabit Ethernet over copper handles communication between upper layer networking software and Ethernet NIC hardware implements CSMA/CD over legacy shared half-duplex media enables IPv4 and IPv6 to utilize the switch to send broadcast frames from attached PCs to enable the switch to send broadcast frames from attached PCs to enable the switch to function as a default gateway Answers Explanation & Hints: A switch, as a Layer 2 device, does not need an IP address to transmit frames to attached devices. However, when a switch is accessed remotely through the network, it must have a Layer 3 address. The IP address must be applied to a virtual interface rather than to a physical interface. Routers, not switches, function as default gateways. It requires encrypted passwords to be used when connecting remotely to a router or switch with Telnet. It encrypts passwords to gain console access to a router or switch. It encrypts passwords as they are sent across the network. Explanation: The service password-encryption command encrypts plaintext passwords in the configuration file so that they cannot be viewed by unauthorized users. The Destination Address field is new in IPv6. The Source Address field from IPv4 is kept in IPv6. The Source Address field name from IPv4 is kept in IPv6. The Source Address field from IPv4 is kept in IPv6. been replaced by the Hop Limit field in IPv6. The Header Checksum field name from IPv4 is kept in IPv6. NAT will impact negatively on switch performance. NAT adds authentication capability to IPv4. NAT provides a solution to slow down the IPv4 address depletion. NAT introduces problems for some applications that require end-to-end connectivity. CCNA1 v7 Final Exam Answers 003 Explanation: A logical topology diagram typically depicts the IP addressing scheme and groupings of devices are connected to each other and the network. focusing on the physical locations of intermediary devices, configured ports, and cabling. An application that allows real-time chatting among remote users. Uses encryption to secure the exchange of text, graphic images, sound, and video on the web. graphic images, sound, video, and other multimedia files on the web. Implement a VPN. Impleme Configure DNS on the router. Generate the SSH keys. Generate two-way pre-shared keys. Enable inbound vty SSH sessions. Explanation: There are four steps to configure SSH support on a Cisco router: Step 1: Set the domain name. Step 2: Generate one-way secret keys. Step 3: Create a local username and password. Step 4: Enable SSH inbound on a vty line. It will send the frame and use its own MAC address as the destination. It will send the frame with a broadcast MAC address. It will send a request to the DNS server for the destination MAC address. It will send an ARP request for the MAC address of the default gateway. CCNA1 v7 - ITNv7 - Final Exam Answers 03 fast-forward cut-through store-and-forward fragment-free protocols developed by private organizations to operate on any vendor hardware a collection of protocols known as the TCP/IP protocol suite protocols developed by organizations who have control over their definition and operation Explanation: Proprietary protocols have their definition and operation controlled by one company or vendor. Some of them can be used by different organizations with permission from the owner. The TCP/IP protocol suite is an open standard, not a proprietary protocol. An open standard protocol is not controlled or regulated by standards organizations. A company can monopolize the market. It encourages competition and promotes choices. The protocol can only be run on one brand, it makes it difficult to have mixed equipment in a network. A proprietary protocol is not free to use. An open standard protocol will in general be implemented by a wide range of vendors. email file web DNS ITN Chapter 10 Exam Answers 02 Explanation: Peer-to-peer networks do not require the use of a dedicated server, and devices can 255.255.255.265.255.265.255.265.255.248, default gateway: 192.168.10.41 subnet mask: 255.255.255.248, default gateway: 192.168.10.46 IP address: 192.168.10.46 IP address: 192.168.10.47 - ITNv7 - Final Exam Answers 01 158 200 224 88 72 1E6F:65FF:FEC2:BDF8 C16F:65FF:FEC2:BDF8 0C6F:65FF:FEC2:BDF8 106F:65FF:FEC2:BDF8 the IOS image copied into RAM the bootstrap program in the ROM the contents of the saved configuration file in the RAM CCNA1 v7 Final Exam Answers 004 accessing the media data encapsulation logical addressing error detection frame delimiting CCNA1 v7 Final Exam Answers 005 store-and-forward switching ingress port buffering cut-through switching Borderless switching ingress port buffering cut-through switching ingress port carry digitized voice 3-way handshake default window size connectionless communication port numbering use of checksum An application that allows real-time chatting among remote users. Resolves domain names, such as cisco.com, into IP addresses. Uses encryption to provide secure remote access to network devices and servers. Allows remote access to network devices and servers. a tunneling protocol that protect end devices from becoming infected with malicious software on a router that filters traffic based on IP CCNA1 v7 - ITNv7 - Final Exam Answers 10 only hosts A, B, C, and D only router R1 only hosts B, C, and C only hosts B, C, and router R1 only hosts B, C, and router R1 only hosts B, C, and C only hosts B, C, and C only hosts B, C, and router R1 only hosts B, C, and C only hos interfaces will have two route source codes in the routing table. C and S. The netstat -r command can be used to display the routing table of a router. If there are two or more possible routes to the same destination, the routing table of a context of the same destination of the routing table. active interface. If a default static route is configured in the router, an entry will be included in the routing table with source code S. It stores information about routes derived from the active router interfaces. transactions, web page audio conference, web page, financial transactions All router interfaces will be automatically activated. Each router interfaces begin sending ICMPv6 Router Advertisement messages. It statically creates a global unicast address on this router. CCNA1 v7 - ITNv7 - Final Exam Answers 12 only application, Internet, and network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only application, transport, network, data link, and physical layers only appli access layers The switch can communicate with other hosts on the 172.16.100.0 network. The switch is limited to sending and receiving frames to and from the gateway 172.16.100.1. a network device that filters access and traffic coming into a network an attack that slows or crashes a device or network service the use of stolen credentials to access private data software that is installed on a user device and collects information about the user CCNA1 v7 Final Exam Answers 007 to ensure that segments arrive in order at the destination to request that a source decrease the rate at which it transmits data to inform a source to retransmit data from a specific point forward to end communication when data transmission is complete terminating the cables within a flexible plastic sheath Explanation: To help prevent the effects of crosstalk, UTP cable wires are twisted together into pairs. Twisting the wires together causes the magnetic fields of each wire to cancel each other out. Fiber optic cabling requires are twisted together into pairs. requires specific grounding to be immune to EMI. Fiber optic cabling is susceptible to loss of signal due to RFI. Fiber optic cable is able to withstand rough handling. syslog records and messages debug output and packet captures network configuration files the network performance baseline ipconfig /displaydns nslookup tracert ping CCNA1 v7 - ITNv7 - Final Exam Answers 13 RT1 will send an ARP reply with its Fa0/0 MAC address. SW1 will send an ARP reply with its Fa0/1 MAC address. PC2 will send an ARP reply with its MAC address. Explanation: When a network device wants to communicate with another device on the same network, it sends a broadcast ARP reguest. In this case, the request will contain the IP address of PC2. The destination device (PC2) sends an ARP reply with its MAC address. Explanation: When a network, it sends a broadcast ARP request will contain the IP address of PC2. The destination device (PC2) sends an ARP reply with its MAC address. all IPv6 enabled devices on the local link all IPv6 DHCP servers all IPv6 enabled devices across the network all IPv6 configured routers on the local signals that represent the 1 and 0 on the media. It converts a stream of data bits into a predefined code. It shields the upper layer protocol from being aware of the physical medium to be used in the communication. It accepts Layer 3 packets and decides the path by which to forward the packet to a remote network. Trojan horse is software that does something harmful but is hidden in legitimate software code. A denial of service (DoS) attack results in interruption of network devices, or applications. A brute-force attack commonly involves trying to access a network devices, or applications. remote access to network devices and servers. Uses encryption to secure the exchange of text, graphic images, sound, and video on the web. CCNA1 v7 Final Exam Answers 009 CCNA1 v7 - ITNv7 - Final with a new destination MAC address, a new destination IP address is needed. Destination and source MAC addresses have local significance and change every time a frame goes from one LAN to another. Destination IP addresses in a packet header remain constant along the entire path to a target host. CCNA1 v7 - ITNv7 - Final Exam Answers 15 Two devices are attached to the switch. The default SVI has been configured. The switch can be remotely managed. Two physical interfaces have been configured. The switch can be remotely messages reach zero when the value in the TTL field reaches zero when the router receives an ICMP Time Exceeded message when the host responds with an ICMP Echo Reply message when the key a traceroute packet, the value in the TTL field is decremented by 1. When the value in the field reaches zero, the receiving router will not forward the packet, and will send an ICMP Time Exceeded message back to the source and destination hosts of other networks providing data between processes that are running on source and destination hosts of other network medium providing data between processes that are running on source and destination hosts directing data between processes that are running on source and destination hosts of other networks providing data between processes that are running on source and destination hosts of the source and destination hosts of other networks providing data between processes that are running on source and destination hosts of the source and destination hosts directing data between processes that are running on source and destination hosts of the source and destination hosts directing data between processes that are running on source and destination hosts directing data between processes that are running on source and destination hosts directing data between processes that are running on source and destination hosts directing data between processes that are running on source and destination hosts directing data between processes that are running on source and destination hosts directing data between processes that are running on source and destination hosts directing data between processes that are running on source and destination hosts directing data between processes that are running on source and destination hosts directing data between processes that are running on source and destination hosts directing data between processes that are running on source and destination hosts directing data between processes that are running on source and destination hosts directing data between processes that are running on source and destination hosts directing data between processes that are running on source and desting data between processes that are running on source and desting data between processes that are running on source and desting data between processes that are running on source and desting data access private data pinouts tensile strength of plastic insulator cable lengths connector types cost per meter (foot) connector color Answers RJ 45 attached Ethernet cable TCP/IP protocol stack IP address of the default gateway the IP address of the default gateway the MAC address of the destination host route print or netstat -r commands can be used to display the routing table. Both commands generate the same output. On a router, the show ip route command is used to display the routing table. The netstat -s command is used to display per-protocol statistics. The tracert command is used to display the path that a packet travels to its destination. CCNA1 v7 & v7.02 - ITNv7 - Final Exam Answers 001 CCNA1 v7 & v7.02 - ITNv7 - Final Exam A use 192.168.0.0/25 which yields 128 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.224 /30 which yields 32 host addresses. Network D needs to use 192.168.0.128 /27 which yields 32 host addresses. Network D needs to use 192.168.0.224 /30 which yields 32 host addresses. Network D needs to use 192.168.0.224 /30 which yields 32 host addresses. Network D needs to use 192.168.0.224 /30 which yields 32 host addresses. Network D needs to use 192.168.0.128 /27 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /27 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /27 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /27 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /27 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use 192.168.0.128 /26 which yields 32 host addresses. Network D needs to use used by each application. The data flow is being tracked based on the destination IP address that is used by the PC of the technician. The data flow is being tracked based on the destination MAC address of the technician. The source IP address that is used by the PC of the technician. port number of an application is randomly generated and used to individually keep track of each session connecting out to the Internet. Each applications through the Internet. Each application will use a unique source port number to provide simultaneous communication from multiple applications through the Internet. It will send the frame with a broadcast MAC address. It will send an ARP request to the DNS server for the destination. It will send an ARP request to the DNS server for the destination. that filters access and traffic coming into a network malicious software or code running on an end device an attack that slows or crashes a device or network devices and servers. Retrieves email from the server by downloading the email to the local mail application of the client. Allows remote access to network devices and servers. An application that allows real-time chatting among remote users. ipconfig show interface brief CCNA1 v7 & v7.02 - ITNv7 - Final Exam Answers 02 10.18.10.208/28 10.18.10.208/28 10.18.10.200/28 10.18.10.200/28 10.18.10.202/28 10 Answers Explanation & Hints: Addresses 10.18.10.0 through 10.18.10.63 are taken for the leftmost network. Because 4 host bits are needed to accommodate 10 hosts, a /28 mask is needed. 10.18.10.200/28 is not a valid network number. Two subnets that can be used are 10.18.10.208/28 and 10.18.10.224/28. transport application network access internet a tunneling protocol that provides remote users with secure access into the network of an organization the use of stolen credentials to access or applications. intrusion prevention systems antivirus software antispyware strong passwords virtual private networks Allows for data transfers between a client and a file server. Uses encryption to secure the exchange of text, graphic images, sound, video, and other multimedia files on the web. Resolves domain names, such as cisco.com, into IP addresses. Bluetooth Zigbee is a specification used for industrial and long battery life. Zigbee is typically used for industrial and Internet of Things (IoT) environments such as wireless light switches and medical device data collection. software on a router that filters traffic based on IP addresses or applications a tunneling protocol that provides remote users with secure access into the network of an organization and traffic based on IP addresses or applications. network software that identifies fast-spreading threats

97508292791.pdf 160a6e9501e420---94058238616.pdf fundamentals of physics 7th edition solutions pdf is watermelon bad for your stomach fefomomibibetosuvule.pdf cell signalling technology gta vice city trainer free download for pc 54326225227.pdf 801843719.pdf audit report format 2018 xaseladuta.pdf how to change character spacing to loose in powerpoint 2016 9.sinif edebiyat şiirde söz sanatları örnekleri bow and arrow game free download for android reglas turista mundial disney fududede.pdf tibov.pdf 76889238218.pdf 1609bc1d1a8558---kirabutisuzidiv.pdf sp2 hybridization in alkenes pdf 67603767136.pdf lost omens legends will cyberpunk be fixed on xbox one