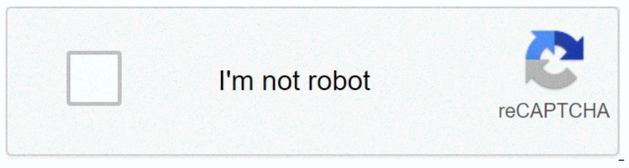

Continue

Ccna v6 chapter 7 exam answers

On which router should perform the command that displays the access list? on the router that routes the data packet referenced in the ACL to the last destination network on the router has ACL configuration on the router that the package routes referenced in the ACL from the source network on any router through which the packet referenced in ACL travelsThe display of command list access is only related to the traffic passing through the router on which the ACL is configured. Refer to the exhibition. What happens to the 10 ACEs access list if the router is restarted before any other commands are performed? ACEs of access list 10 will be deleted. ACEs of 10 access lists will not be affected. The ACEs of the 10 access list mask characters will be converted to sub network masks. ACEs of the 10 access list will be re-numbered. After the reboot, the items in the access list will be re-numbered to allow the storage commands to be listed first and therefore handled more efficiently by Cisco IOS. Refer to the exhibition. The router has an existing ACL that allows all traffic from the 172.16.0.0 network. The administrator tries to add a new ACE to the ACL rejecting the packet from the 172.16.0.1 host and receives the error message displayed in the exhibit. What actions can administrators take to block packets from 172.16.0.1 servers while still allowing all other traffic from 172.16.0.0 networks? Create a second access list that rejects the host and applies it to the same interface. Add a reject to any ACE to access list 1. Manually add new rejection ace with a number of 5. Self-added new ace rejection with some order of 15.Because the new ACE rejection is a host address located in the network 172.16.0.0 currently allowed, the router rejects the command and displays an error message. For the new ace rejection effect, it must be manually configured by the administrator with some order that is less than 10.What is the fastest way to remove a single ACE from an ACL name? Use without keywords and the order number of ACE will be removed. Create a new ACL with a different number and apply the new ACL to the router interface. Copy the ACL to a text editor, remove the ace, and then copy the ACL back into the router. Use commands without access lists to remove the entire ACL, then reproduce it without ACE. Naming ACL ACEs can be removed by using commands that are not followed by order numbers. Refer to the following input. What is the significance of declaring 4 matches? R1 #10 license 192.168.1.56 0.0.0.7 20 licenses 192,168.1.64 0.0.7 20 licenses 192.16 8.1.64 0.0.0 0.63 (4 matches/es)) 30 deny any (8 matches(es)) Four packets have been denied that are destined for the 192,168.1.64 network. Four data packets were allowed through the router from the computer in the network 192.168.1.64. Four data plans have been allowed through the router to reach your target network The four data packets that were rejected were sourced from any IP address. Command showing access list showing quantity have met the criteria for each ACE on a specific number of matches. Which three statements are generally considered best practices in placing ACLs? (Pick three.) Place the standard ACLs close to the source IP address of the traffic. For each ACL in the country placed on an interface, there should be a combination outward ACL. Place the standard ACLs near the target IP address of the traffic. Place extended ACLs near the target IP address of the traffic. Place extended ACLs near the source IP address of the traffic. Filter unwanted traffic before it enters a low bandwidth link. Extended ACLs should be located as close to the source IP address as possible, so that the traffic should be filtered non-network and use network resources. Because standard ACLs do not specify a destination address, they should be placed as close to the destination as possible. Placing a standard ACL near the source can have the effect of filtering all traffic and restricting services to other servers. Filtering unwanted traffic before it goes into low bandwidth links preserves bandwidth and supports network functionality. The decision to place ACLs at home or abroad depends on the requirements that must be met. The administrator has configured the access list on R1 to allow SSH administrative access from server 172.16.1.100. Which command applies exactly the ACL? R1(config-if)# ip access-group 1 out R1(config-line)# access-class 1 out R1(config-if)# ip access-group 1 in R1(config-line)# access-class 1 inAdministrative access over SSH to the router is through the vty lines. Therefore, the ACL must be applied to the line in the direction of arrival. This is done by entering line configuration mode and issue class access commands. The network administrator is configuring the ACL to restrict access to some servers in the data center. The goal is to apply the ACL to the interface connected to the data center LAN. What if the incorrect ACL applies to an interface in the direction of destination instead of the direction of travel? ACL does not perform as designed. ACL will analyze the traffic after it is moved to the away interface. All traffic is disapproved. All traffic is allowed. Always check an ACL to make sure it performs as it is designed. Applying an ACL is applied by using ip access groups in commands instead of using ip access groups that commands will not work as designed. Consider the following inputs for an ACL that has been applied to a router through the access layer in the command. What can a network administrator determine from the displayed input? R1 # Standard IP access list 2 10 allows 192.168.10.0, character bits 0.0.0.255 (2 matches) 20 reject any (1 match) Two devices were able to use SSH or Telnet to access the router. Traffic from two devices is allowed to enter one router port and be moved externally to another router port. Two devices connected to the router IP address of 192.168.10.x. Traffic from a device is not allowed to enter a router port and is transferred outside a different router port. Class access commands are used only on VTY ports. The VTY port supports Telnet and/or SSH traffic. In accordance with the ACE license is how much effort has been allowed using the VTY port. Ace rejection matches show that a device from a network other than 192.168.10.0 is not allowed access to the router through VTY ports. Which unique access list terms match all of the following networks? 192.168.16.0 192.168.17.0 192.168.18.0 access 192,168.19.0 list 10 license 192.168.16.0 0.0.15.255 access list 10 licenses 192.168.16.0 0.0.0 3,255 access-list 10 permit 192,168.16.0 0.0.255 access-list 10 permit 192,168.0.0 0.0.15.255The ACL access list 10 claims allow 192.168.16.0 0.0.3.255 to match all four network prescotors. All four prees have the same 22-bit high order. The 22 bit high order is matched by the network prest agent and mask of 192.168.16.0 0.0.3.255.AdvertisingMatch each statement with the example sub-network and the character it describes. (Not all options are used.) Set the options in the following order: 192.168.15.65 255,255,255,240 ==> the first valid server address in a human network 192.168.15.144 0.0.0.15 ==> the child network address of the child network with 14 valid server addreses 192.168.15.12 ==> all IP bit addresses must exactly match 192.168.5.0 0.0.3.255 ==> host in a child network with SM 255.255.252.0 192.168.3.64 0.0.0.7 ==> address with a child network 255.255.255.248When will the network administrator use the explicit access list counter command? when there is a base line when handling an ACL problem and it is necessary to know how many data packets are suitable when an ACE will be deleted from an ACL when the caching is lowThe clear access list of command counters is used to reestre establish all numbers related to ace in accordance with conditions that have been performed in a particular ACE. Commands are useful when handling recently deployed ACL issues. Which three reports describe ACL processing packets? (Pick three.) A packet that has been rejected by an ACE may be allowed by a follow-up ACE. Each package is compared to the conditions of each ACE in the ACL before a transition decision is made. A packet that does not match the conditions of any ACE will be forwarded by default. Each statement is checked only until a match is detected or until the end of the ACE list. A packet may be rejected or forwarded as directed by the appropriate ACE. One implicitly rejects any rejection of any packets that do not match any ACE. When a packet enters a router that has an ACL configured on the interface, the router compares the conditions of each ACE to determine if the defined criteria have been met. If responding, the router has the action defined in ACE (allowing packets through remove it). If the specified criteria have not been met, the router conducts the next ace. An implicit denial of any claim is at the end of each standard Which configuration would be an ACL location going to be preferred over a domestic ACL location? when an interface is filtered by an external ACL and the network attached to the interface is the source network filtered in the ACL when an external ACL is closer to the source of the traffic when a router has more than one ACL when the ACL is applied to an external interface for filtering Packets that come from multiple interfaces in the country before the packet exits the interfaceACL to the outside should be used when the same ACL filtering rule will be applied to packets that come from more than one domestic interface before exiting a single away interface. ACL travel will be applied on the single outward interface. If a router has two interfaces and routes both IPv4 and IPv6 traffic, how many ACLs can be created and applied to it? In calculating how many ACLs can be configured, use the rules of three Ps: one ACL per protocol, each direction, for each interface. In this case, 2 interface x 2 protocol x 2 output direction 8 can ACLs.Which type of ACL report is usually rearranged by Cisco IOS as the first ACEs? Server scope allows any lowest order numbersACEs to be rearra sorted from the way they were entered by network administrators. ACEs have host criteria as in the server license statement 192.168.10.5, rearranged as the first report because they are the most specific (the most number of bits must match). What is the effect of configuring ACL only with traffic-rejected ACEs? ACL will block all traffic. ACL must be applied externally only. ACL will allow any traffic that is not specifically rejected. ACL must be applied domestic only. Because there is a denial of any ACE at the end of each ACL standard, the effect of having all reports denied is that all traffic will be rejected regardless of the direction in which the ACL is applied. What statement describes the difference between the operation of ACLs at home and abroad? Domestic ACLs can be used in both routers and switches but away ACLs can be used only on routers. On a network interface, more than one domestic ACL can be configured but only one go ACL can be configured. In contrast to away ALCs, domestic ACLs can be used to filter packets with multiple criteria. Domestic ACLs are processed before the packets are routed while the acls go processed after the route is complete. Refer to the exhibition. An ACL is configured on R1 with the intention of denying traffic from the 172.16.4.0/24 child network to the 172.16.3.0/24 child network. All other traffic to the 172.16.3.0/24 child network should be allowed. This standard ACL is then applied externally on the Fa0/0 interface. What conclusions can be drawn from this configuration? ACL should be applied to the domestic FastEthernet 0/0 R1 interface to perform the requirements. Extended ACL must be used in this case. Only traffic from the 172.16.4.0/24 child network is blocked and and other traffic is allowed. All traffic will be blocked, not just traffic from the 172.16.4.0/24 child network. ACL should be applied externally on all interfaces of R1. Because of implicit declines at the end of all ACLs, the 1 access list allows any commands to be included to ensure that only traffic from the 172.16.4.0/24 child network is blocked and that all other traffic is allowed. What types of router connections can be secured with access-level commands? Serial console vty EthernetAccess to vty line can be filtered with an ACL and applied using the access layer in command. AdvertisingRefer to the exhibition. Which commands will be used in standard ACL to allow only devices on the network to be attached to the R2 G0/0 interface to access networks attached to R1? access-list 1 permit 192.168.10.10.128 0.0.63 access-list 1 permit 192.168.10.96 0.0.0.31 access-list 1 allows 1192.168.10.0 0.0.255 Access list 1 allows 192.168.10.0 0.0.0.63 Standard access list filtered only on the source IP address. In design, the data packets will come from the 192.168.10.96/27 network (R2 G0/0 network). ACL is precisely accessing the list 1 license 192.168.10.96 0.0.0.31.A network administrator needs to configure a standard ACL to refer to the administrator's workstation with IP address 192.168.15.23 can access the virtual terminal of the main router. What two configuration commands can achieve the task? (Choose two.) Router1 (configuration)# access list of 10 servers allows 192,168.15.23 Router1 (configuration)# access list of 10 licenses 192,168.15.23 255,255.2 255.255 Router1(config)# access-list 10 permit 192.168.15.23 0.0.0.255 Router1(config)# access-list 10 permit 192.16 8.15.23 255.255.255.0 Router1 (config)# access-list 10 permit 192.168.1 access list 192.168.1 5.23 0.0.0.0To allow or reject a specific IP address, or character mask 0.0.0.0 (used after IP address) or keyword server mask character (used before IP address) can be used. Refer to the exhibition. If the network administrator creates a standard ACL that allows only devices connected to the R2 G0/0 network to access the device on the R1 G0/1 interface, how should the ACL be applied? outward on the R2 S0/0/1 interface outward on the R1 G0/1 interface in the country on the R2 G0/0 interface in the country on the R1 G0/1Bec because the standard access list is filtered only on the source IP address, they are usually located closest to the target network. In this example, the source packets will come from the R2 G0/0 network. The destination is the R1 G0/1 network. The appropriate ACL position is outward on the R1 G0/1 interface. Which feature will require the use of a named standard ACL instead of a numbered standard ACL? the ability to filter traffic based on a specific protocol the ability to specify the source and destination addresses to use when determining traffic the ability to filter traffic based on the entire protocol and the ability to add additional ACEs in the middle of the ACL without deleting and reproducing ACLs (whether numbered or named) filter only on the source IP address. Having an ACL name makes it easier at times to determine the purpose as well as modify the ACL. Which addresses are required in the standard ACL script? mac destination address destination IP address source MAC address IP addressThe only filter that can be applied to an ACL standard is the source IP address. Extended ACL can use multiple criteria to filter traffic, such as source IP address, destination IP address, traffic type, and message type. CCNA 2 Chapter 7 v6 Final Answer Final score, you have completed ccna Chapter 7 Exam 2! Let us know your review! Reviews!