Custom View Settings

Question #501 *Topic 1*

What is the MAC address used with VRRP as a virtual address?

A. 00-05-42-38-53-31

B. 00-00-5E-00-01-0a

C. 00-00-0C-07-AD-89

D. 00-07-C0-70-AB-01

Correct Answer: *B*

Community vote distribution

B (100%)

Goh0503 Highly Voted 8 months ago

Answer B
000.5E00.01xx is VRRP virtual MAC
0000.0c07.acxx is HSRP virtual MAC
0007.b400.xxyy is GLBP virtual MAC

upvoted 7 times

guisam Most Recent 6 months ago

https://www.fingerinthenet.com/fhrp-introduction/

upvoted 1 times

Customexit 7 months, 3 weeks ago

I guess V = 5 (vrrp)
G rhymes with b (glbp)
and uhh, h and o spells ho and that's funny (h0, hsrp)
i honestly haven't memorized any more than that..

upvoted 1 times

Garfieldcat 7 months, 3 weeks ago

Selected Answer: B

I can remember this time I retry this question

upvoted 1 times

Nawaf1 8 months ago

so now I need to memorize mac addresses!!?
this is absurd

upvoted 3 times

Question #502 *Topic 1*

Why would VRRP be implemented when configuring a new subnet in a multivendor environment?

A. when a gateway protocol is required that supports more than two Cisco devices for redundancy

B. to interoperate normally with all vendors and provide additional security features for Cisco devices

C. to ensure that the spanning-tree forwarding path to the gateway is loop-free

D. to enable normal operations to continue after a member failure without requiring a change in a host ARP cache

Correct Answer: *B*

VRRP is the industry standards based FHRP similar to Cisco's HSRP but is supported by multiple vendors.

Community vote distribution

D (69%) B (31%)

RougePotatoe Highly Voted 7 months, 1 week ago

Selected Answer: D

I can only confirm the first half of B to be true unable to find anything on how VRRP provides security. So I picked D as D is 100% how VRRP works.

upvoted 5 times

lsuzu Most Recent 2 days, 17 hours ago

Selected Answer: D

Option A is incorrect. VRRP can support more than two Cisco devices for redundancy, but it can also support devices from other vendors.
Option B is incorrect. VRRP does not provide any additional security features for Cisco devices.
Option C is incorrect. Spanning tree is responsible for preventing loops in the Layer 2 network. VRRP is responsible for providing redundancy for Layer 3 networks.

upvoted 1 times

FALARASTA 1 month ago

I think the second part is because CDP is not enabled to work by deafult when VRRP is used

upvoted 1 times

rogi2023 1 month, 2 weeks ago

Selected Answer: B

If I hit this question I will go for "B" - multivendor, just keep it simlpy

upvoted 3 times

andresugiharto 2 months, 3 weeks ago

VRRP support "authentication", but not sure if the correct answer is B
https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/addr_serv/configuration/guide/ic40crs1book_chapter10.html

upvoted 1 times

gewe 3 months, 3 weeks ago

D for 100%

upvoted 2 times

Anas_Ahmad 5 months, 1 week ago

Selected Answer: D

host does not need to make an arp request to learn another mac-address for the gateway.

upvoted 1 times

sssssse 6 months, 3 weeks ago

Selected Answer: D

VRRP does not provide additonal security features for Cisco devices.
When VRRP is implemented the virtual mac-addres of the VRRP group remains the same so the host does not need to make an arp request to learn another mac-address for the gateway. D is the right answer

upvoted 2 times

Garfieldcat 7 months, 3 weeks ago

Selected Answer: B

answer b

upvoted 1 times

RougePotatoe 7 months, 1 week ago

First part of the claim is true but i'm not sure about the second part. I can't find anything on how VRRP offer additional security features for cisco devices.

upvoted 3 times

Question #503 *Topic 1*

Why implement VRRP?

A. To hand over to end users the autodiscovery of virtual gateways

B. To provide end users with a virtual gateway in a multivendor network

C. To leverage a weighting scheme to provide uninterrupted service

D. To detect link failures without the overhead of Bidirectional Forwarding Detection

Correct Answer: *B*

Community vote distribution

B (100%)

ismail23 4 weeks, 1 day ago

Selected Answer: B

B is right

upvoted 1 times

Question #504 *Topic 1*

Which type of address is shared by routers in a HSRP implementation and used by hosts on the subnet as their default gateway address?

A. multicast address

B. virtual IP address

C. loopback IP address

D. broadcast address

Correct Answer: *B*

Question #505 *Topic 1*

By default, which virtual MAC address does HSRP group 14 use?

A. 00:05:5e:19:0c:14

B. 00:05:0c:07:ac:14

C. 04:15:26:73:3c:0e

D. 00:00:0c:07:ac:0e

Correct Answer: *D*

MikD4016 Highly Voted 8 months, 1 week ago

As you know that HSRP uses this virtual MAC address, 0000.0C07.ACxy, where xy is the HSRP group number in hexadecimal.

so your HSRP group no is 14 which is in a decimal format so we need to change it into hexadecimal

14 = 0000 1110 binary

0000 1110 = 0e hex

so by this process, for HSRP Group 14 the Mac address will be : 00:00:0c:07ac:0e

upvoted 9 times

zezc Most Recent 1 month ago

A. 00:05:5e:19:0c:14.

HSRP (Hot Standby Router Protocol) is a protocol that allows multiple routers to work together to present the appearance of a single virtual router to the hosts on a LAN. When a group is configured for HSRP, the routers within the group communicate with each other to determine which router should be the active (forwarding) router and which router should be the standby (backup) router.

Each HSRP group is assigned a virtual MAC address that is shared by the active and standby routers in the group. The virtual MAC address is used as the source MAC address for all HSRP-related packets, and it is used by the hosts on the LAN to address packets to the HSRP virtual router.

The default virtual MAC address for HSRP group 14 is 00:05:5e:19:0c:14. Therefore, option A is the correct answer. Option B is the default virtual MAC address for HSRP group 7, option C is not a valid MAC address format, and option D is the default MAC address for VMware virtual NICs.

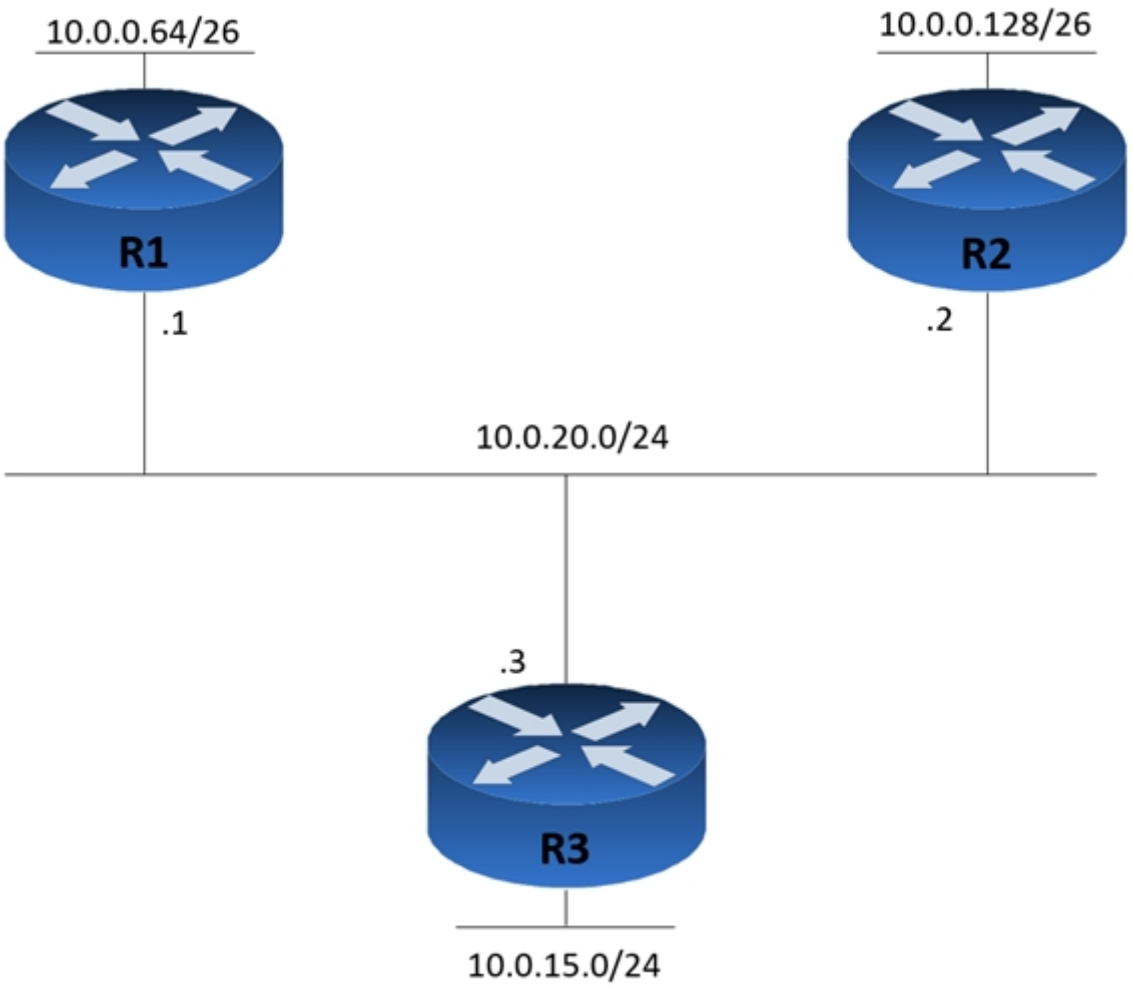
upvoted 1 times

Hope_12 1 month ago

I think you can get the answer on with below:
000.5E00.01xx is VRRP virtual MAC
0000.0c07.acxx is HSRP virtual MAC

upvoted 1 times

Question #506 *Topic 1*



Refer to the exhibit. Router R1 is added to the network and configured with the 10.0.0.64/26 and 10.0.20.0/26 subnets. However, traffic destined for the LAN on
R3 is not accessible. Which command when executed on R1 defines a static route to reach the R3 LAN?

A. ip route 10.0.0.64 255.255.255.192 10.0.20.3

B. ip route 10.0.15.0 255.255.255.0 10.0.20.1

C. ip route 10.0.15.0 255.255.255.192 10.0.20.1

D. ip route 10.0.15.0 255.255.255.0 10.0.20.3

Correct Answer: *D*
We need to specify the destination network (10.0.15.0/24) and the next hop IP of the router to get to that network (10.0.20.3).

jayjihaekim 1 week, 2 days ago
Static Routing: ip route <Destination IP> <Subnet-mask> {interface address }
10.0.15.0 24 = 255.255.255.0 10.0.20.3
upvoted 1 times

Swiz005 6 months, 3 weeks ago
Why is A not the correct answer? - Can anyone help
upvoted 3 times

Surves 6 months, 2 weeks ago
Because the destination network is 10.0.15.0/24 and not 10.0.0.64
upvoted 3 times

Question #507 *Topic 1*

A router has two static routes to the same destination network under the same OSPF process. How does the router forward packets to the destination if the net- hop devices are different?

A. The router chooses the route with the oldest age.

B. The router chooses the next hop with the lowest IP address.

C. The router chooses the next hop with the lowest MAC address.

D. The router load-balances traffic over all routes to the destination.

Correct Answer: *D*
Load balancing is a standard functionality of Cisco IOS Software that is available across all router platforms. It is inherent to the forwarding process in the router, and it enables a router to use multiple paths to a destination when it forwards packets. The number of paths used is limited by the number of entries that the routing protocol puts in the routing table. Four entries is the default in Cisco IOS Software for IP routing protocols except for BGP. BGP has a default of one entry.

RougePotatoe Highly Voted 7 months, 1 week ago

Selected Answer: D

D is the only one that makes any sense yet I hate it.

upvoted 9 times

melmiosis 7 months, 1 week ago

i know the feeling. im glad im close at least to ending this bs hehe

upvoted 5 times

john1247 Most Recent 3 days, 18 hours ago

Why is B not the right answer?

upvoted 1 times

Sdiego 4 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

joseangelatm 5 months, 1 week ago

No metric election?

upvoted 3 times

Question #508 *Topic 1*

What does the implementation of a first-hop redundancy protocol protect against on a network?

A. default gateway failure

B. BGP neighbor flapping

C. spanning-tree loops

D. root-bridge loss

Correct Answer: *A*

Question #509 *Topic 1*

Which feature or protocol is required for an IP SLA to measure UDP jitter?

A. LLDP

B. EEM

C. CDP

D. NTP

Correct Answer: *D*

LTTAM Highly Voted 2 years, 4 months ago

Correct Answer. Source:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/xe-16-6/sla-xe-16-6-book/sla-udp-jitter.html

upvoted 13 times

Ali526 2 years, 4 months ago

The problem with such links, specially from Cisco, is that you have to read a whole book to get an answer, and that is if you are lucky. Thanks anyway.

upvoted 15 times

Stonetales987 1 year, 6 months ago

Control F "measure" :)

upvoted 4 times

zaid 2 years, 3 months ago

Right :)

upvoted 2 times

Samuelpn96 1 year, 9 months ago

Time synchronization, such as that provided by the Network Time Protocol (NTP), is required between the source and the target device to provide accurate one-way delay (latency) measurements.

This part in his link proves that NTP is the right answer here.
Thanks for the link,

upvoted 4 times

Phonon Highly Voted 5 months ago

Selected Answer: D

D. NTP (Network Time Protocol)

IP SLA (Internet Protocol Service Level Agreement) is a feature in Cisco IOS that allows administrators to measure and monitor network performance. One of the types of performance measurements that can be performed using IP SLA is UDP jitter, which is a measure of the variability in the delay of UDP packets.

To measure UDP jitter using IP SLA, the NTP (Network Time Protocol) feature must be enabled on the device. NTP is used to synchronize the device's clock with a reference time source, which is necessary to accurately measure the delay of UDP packets. Without NTP, the device's clock may drift over time, leading to inaccurate jitter measurements.

Therefore, the correct answer is D. NTP.

upvoted 6 times

GigaGremlin Most Recent 8 months ago

Selected Answer: C

OK,... so measurement need some time... ;-)

upvoted 2 times

ptfish 10 months, 3 weeks ago

Selected Answer: D

The keyword is "UDP". Both LLDP and CDP are Layer 2 neighbor discovery protocols.
EEM = Embedded Event Manager.

So the answer is D.

upvoted 4 times

Nnandes 1 year ago

D, NTP is the right protocol

upvoted 2 times

msae26 1 year, 1 month ago

Correct Answer: NTP
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book/sla_udp_jitter.html

upvoted 1 times

jehangt3 2 years ago

I thought jitter is related to QOS (gold profile)

upvoted 2 times

vadiminski 2 years ago

Jitter has somthing to do with time, NTP synchronizes time, thus NTP the most likely

upvoted 4 times

chr 2 years ago

Interesting blog post on IP SLA that is worth skimming over..
https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKN0EAO/ip-sla-fundamentals
Does not mention NTP, though this is the correct answer as LTTAM and oooMooo have pointed out.

upvoted 2 times

oooMooo 2 years, 1 month ago

Time synchronization, such as that provided by the Network Time Protocol (NTP), is required between the source and the target device to provide accurate one-way delay (latency) measurements.

upvoted 4 times

Question #510 *Topic 1*

Refer to the exhibit. Which feature is enabled by this configuration?

```
R1(config)#ip nat pool cisco 10.1.1.0 10.1.1.50 255.255.255.0
```

A. static NAT translation

B. a DHCP pool

C. a dynamic NAT address pool

D. PAT

Correct Answer: *C*

cormorant 5 months, 3 weeks ago

it's a dynamic nat address pool

upvoted 2 times

Goh0503 8 months, 2 weeks ago

Answer is C

https://www.practicalnetworking.net/stand-alone/cisco-nat-configurations-ios-router/

upvoted 1 times

Question #511 *Topic 1*

Which NAT term is defined as a group of addresses available for NAT use?

A. NAT pool

B. dynamic NAT

C. static NAT

D. one-way NAT

Correct Answer: *A*

Lulu03 1 month, 3 weeks ago

A is correct

upvoted 2 times

Nnandes 1 year ago

Nat pool, A is correct

upvoted 4 times

Question #512 *Topic 1*

Which command can you enter to allow Telnet to be supported in addition to SSH?

A. transport input telnet ssh

B. transport input telnet

C. no transport input telnet

D. privilege level 15

Correct Answer: *A*

pianetaperez Highly Voted 2 years, 3 months ago

Packet tracer supports "transport input all", does not support "transport input telnet ssh".

upvoted 11 times

Dante_Dan 1 year, 5 months ago

Actual routers and switches accept the "transport input telnet ssh" command.

Also, this is stated in the official cert guide.

upvoted 4 times

VictorCisco 2 months, 1 week ago

SW4(config-line)#transport input ssh telnet
^
% Invalid input detected at '^' marker.

SW4(config-line)#

upvoted 1 times

raydel92 Highly Voted 1 year, 6 months ago

Selected Answer: A

If you set transport input telnet, it will override any previous config. So, in real device you should set transport input telnet ssh, if you want both. In Packet Tracer this is not allowed, instead it is transport input all.

upvoted 6 times

Nnandes Most Recent 1 year ago

transport input telnet ssh

upvoted 2 times

sdokmak 1 year, 11 months ago

what about privilege level 15?

upvoted 3 times

sdokmak 1 year, 11 months ago

nevermind this gives you access to enable mode straight away, probably not the answer they're looking for.

upvoted 3 times

SUKABLED 2 years, 1 month ago

A is true of course, but these questions are mindboggling, in terms of logicality....the answer presumes that we have not configured neither ssh nor telnet, unlike the question...poor

upvoted 6 times

youtri 2 years, 1 month ago

i thnk the question says that ssh is configured and what is the next step to confugure Telnet

upvoted 4 times

aliwqa777 2 years, 2 months ago

A is correct

upvoted 2 times

youtri 2 years, 2 months ago

i think is not correct because packet tracer doesn t support this command
the correct i think is B

upvoted 2 times

1234Rob5678 2 years, 2 months ago

A is correct. Question is asking for Telnet AND SSH, B would only allow Telnet, also packet tracer does not support ALL functions of live equipment.

upvoted 7 times

Question #513 *Topic 1*

Refer to the exhibit. After you apply the given configuration to a router, the DHCP clients behind the device cannot communicate with hosts outside of their subnet.
Which action is most likely to correct the problem?

```
ip dhcp pool test
    network 192.168.10.0 /27
    domain-name cisco.com
    dns-server 172.16.1.1 172.16.2.1
    netbios-name-server 172.16.1.10 172.16.2.10
```

A. Configure the dns server on the same subnet as the clients

B. Activate the dhcp pool

C. Correct the subnet mask

D. Configure the default gateway

Correct Answer: *D*

xsp Highly Voted 2 years, 3 months ago

Answer is correct, since question is "Which action is most likely to correct the problem?"
Means that the given set of command is missing something.

Since when we are configuring a DHCP server on a router:

conf t
service dhcp
ip dhcp pool <pool name>
network <network address of the pool>
default-router <ip address of the interface facing the hosts, or ip adress of the interface facing downstream clients>
dns-server <ip address of dns-server>
exit

upvoted 13 times

Randman 1 year, 5 months ago

Is not configuring the default gate this command?:
SW1(config)# ip default-gateway 192.168.10.1

upvoted 1 times

Nicocisco 1 year, 3 months ago

This is to configure it directly on the equipment. We want the DHCP server to send the information to it.

upvoted 2 times

nathnotnut Most Recent 3 months ago

why not C? i am a beginner, but I also know that you should put the "subnet mask" not the "/27", wouldnt it become and error?

upvoted 1 times

cormorant 6 months ago

THE (DHCP#) DEFAULT-ROUTER IS MISSING FROM THE EXHIBIT

upvoted 1 times

Nnandes 1 year ago

D. Configure the default gateway

upvoted 1 times

Nicocisco 1 year, 3 months ago

I know the answer is D, but we can't put de mask for network in CIDR right?

upvoted 2 times

Danu22 1 year, 1 month ago

Correct, you can't input a subnet mask in CIDR notation as shown in this question.

upvoted 1 times

uevenasdf 2 years, 4 months ago

D is more right but arguably A could be right too

upvoted 2 times

RougePotatoe 7 months, 1 week ago

The DNS sever does not need to be on the same subnet as your clients. You can double check this by going into your network settings and adjusting DNS to 1.1.1.1 or 8.8.8.8. You can check the before and after results with ipconfig /all in command prompt. Typically your default DNS server on your local network is your default gateway on SOHO routers but your SOHO router will send that DNS query up to the ISP and typically one of their DNS servers will answer your DNS query. Remember your router is typically getting DHCP information from the ISP as well.

upvoted 1 times

Cpynch 1 year, 4 months ago

It's possible, but without more information you'd have to make an assumption whereas, with D there is clearly a default gateway missing.

upvoted 1 times

Question #514 *Topic 1*

Refer to the exhibit. Which rule does the DHCP server use when there is an IP address conflict?

```
Router#  show ip dhcp conflict
IP address      Detection method    Detection time
172.16.1.32     Ping                Feb 16 1998 12:28 PM
172.16.1.64     Gratuitous ARP      Feb 23 1198 08:12 AM
```

A. The address is removed from the pool until the conflict is resolved.

B. The address remains in the pool until the conflict is resolved.

C. Only the IP detected by Gratuitous ARP is removed from the pool.

D. Only the IP detected by Ping is removed from the pool.

E. The IP will be shown, even after the conflict is resolved.

Correct Answer: *A*

An address conflict occurs when two hosts use the same IP address. During address assignment, DHCP checks for conflicts using ping and gratuitous ARP. If a conflict is detected, the address is removed from the pool. The address will not be assigned until the administrator resolves the conflict.

uevenasdf Highly Voted 2 years, 4 months ago

Didn't know we had routers in 1198 lol

upvoted 35 times

wirlernenman 2 years, 3 months ago

What a catch 😅

upvoted 13 times

Samuelpn96 Highly Voted 1 year, 9 months ago

When the DHCP server detects there is a conflict of an IP address before or right after it is assigned to a client, it will automatically remove the IP address from the DHCP pool and move it to the DHCP conflict table. The IP address in question will remain there until an administrator sees and clears the DHCP conflict table.

https://www.firewall.cx/cisco-technical-knowledgebase/cisco-switches/1063-cisco-switch-router-dhcp-server-conflicts.html

upvoted 14 times

Nnandes Most Recent 1 year ago

I think A is correct, the address is removed from the pool.

upvoted 2 times

Nnandes 1 year ago

A. The address is removed from the pool until the conflict is resolved.

upvoted 1 times

Question #515 *Topic 1*

Which command can you enter to determine the addresses that have been assigned on a DHCP Server?

A. Show ip DHCP database.

B. Show ip DHCP pool.

C. Show ip DHCP binding.

D. Show ip DHCP server statistic.

Correct Answer: *C*

wannaknow Highly Voted 2 years, 4 months ago

Seems Correct answer is B
Switch#sh ip dhcp ?
binding DHCP address bindings
conflict DHCP address conflicts
pool DHCP pools information
relay Miscellaneous DHCP relay information
snooping DHCP snooping
Switch#

upvoted 7 times

Talloo 2 years, 3 months ago

Wrong, the pool parameter displays the DHCP pool available. The binding parameter lists addresses leased (binding) to clients

upvoted 16 times

dave1992 1 year, 6 months ago

wrong. reread the question. you are confusing a lot of people

upvoted 1 times

g_mindset Most Recent 9 months ago

Selected Answer: C

Router#show ip dhcp binding - Displays a list of all bindings created.

https://www.ciscopress.com/articles/article.asp?p=1574301&seqNum=6

upvoted 3 times

Nnandes 1 year ago

show ip dhcp binding is the right answer

upvoted 2 times

ProgSnob 1 year, 6 months ago

Binding gives you the actual addresses leased. Pool just gives the statistics regarding what is configured and will only tell you the number of addresses leased, not the actual address.

upvoted 4 times

joseph267 1 year, 6 months ago

key word "Have been assigned" DHCP binding shows you exactly that

upvoted 4 times

krey 1 year, 8 months ago

i Think Its B.
it was stated IP addresses assigned on DHCP server.
If its assigned by DHCP server that could be C.

upvoted 1 times

Adaya 1 year, 11 months ago

Answer is correct

upvoted 3 times

Question #516 *Topic 1*

What is the authoritative source for an address lookup?

A. a recursive DNS search

B. the operating system cache

C. the ISP local cache

D. the browser cache

Correct Answer: *A*

g_mindset 9 months ago

Selected Answer: A

A it is!

upvoted 1 times

sasquatchshrimp 10 months, 1 week ago

In DNS, "authoritative" basically means, who can be trusted to own and know the dns entries for the specified item. In this item, its asking for an authoritative source, which has to be a server. DNS entries that are cached can be wrong, old/outdated. So Caches are ruled out. Now, this is a terrible question, but a basically, a recursive dns query is a packet that goes out to the big work dns networks and "walks the tree" to find an authoritative dns server for the website you are looking for. https://www.cloudflare.com/learning/dns/what-is-recursive-dns/

upvoted 4 times

sasquatchshrimp 10 months, 1 week ago

world, not work

upvoted 1 times

Nebulise 1 year, 5 months ago

Helpful article explaining why answer is A:
https://umbrella.cisco.com/blog/what-is-the-difference-between-authoritative-and-recursive-dns-nameservers

upvoted 2 times

bootloader_jack 1 year, 8 months ago

Is recursive search an authoritative source?

upvoted 1 times

kmb192006 1 year, 8 months ago

B,C,D are CACHE from the authoritative server when happens. ISP (DNS server) runs recursive search (root server -> TLD server -> authoritative server) to get correct name resolution and cache the result. Browser requests name solution from ISP and cache the result

upvoted 4 times

cortib 1 year, 8 months ago

that's tricky, i guess the key is in the word source. The other answer are cached, so they will come from a first DNS lookup and that is the Source.

upvoted 1 times

Question #517 *Topic 1*

Which command is used to verify the DHCP relay agent address that has been set up on your Cisco IOS router?

A. show ip interface brief

B. show ip dhcp bindings

C. show ip route

D. show ip interface

E. show interface

F. show ip dhcp pool

Correct Answer: *D*

raydel92 Highly Voted 1 year, 6 months ago

Selected Answer: D

With that command you can see if the helper address (dhcp relay) is configured.

Router1#sh ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 10.0.0.1/30
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is 192.168.4.2

upvoted 12 times

Garfieldcat Most Recent 7 months, 3 weeks ago

since interface id is not unknown, I think the command need to be interface"s". Missing "s" in string "show ip interface" is invalid too..

upvoted 1 times

DaBest 1 year, 8 months ago

i don't understand this question, can someone put it in simple words please?

upvoted 3 times

kadamske 1 year, 8 months ago

DHCP relay agent means: a router interface is getting its ip address automatically through dhcp, this normally happens between two connected router. After a Dhcp server has already been configured in the network, you'll issue this command on the router's interface "ip address dhcp"
Router1#sh ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 10.0.0.1/30
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is 192.168.4.2

Router2(config)#interface gigabitEthernet 0/0
Router2(config-if)#ip address dhcp
Router2(config-if)#no shutdown

Router2#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 10.0.0.2/30
Broadcast address is 255.255.255.255
Address determined by DHCP
MTU is 1500 bytes
Helper address is not set

upvoted 6 times

raydel92 1 year, 6 months ago

It is not like this kadamske, DHCP relay is when you configure the Helper address on a router interface. That router is not the DHCP server, but can inform the devices on the network about the IP of the DHCP server.
When a device does not know the IP address of a DHCP server, it broadcast a DHCPDISCOVER, and routers do not retransmit broadcast, so if the DHCP server is beyond the network, the device will not find it. Instead with the helper address, it can transmit a unicast packet directly to the DHCP server.
Right answer still D, because you can see the helper address with that command.

upvoted 4 times

raydel92 1 year, 6 months ago

It is more that they retransmit the broadcast DHCPDISCOVER, as a unicast to the IP indicated by the Helper address. Hope it can help.

upvoted 2 times

kadamske 1 year, 8 months ago

And the only way to verify that is with the command " Show ip interface xx

upvoted 3 times

Question #518 *Topic 1*

Which type of information resides on a DHCP server?

A. a list of the available IP addresses in a pool

B. a list of public IP addresses and their corresponding names

C. usernames and passwords for the end users in a domain

D. a list of statically assigned MAC addresses

Correct Answer: *A*

DaBest Highly Voted 1 year, 8 months ago

obviously thats a list of the available IP addresses in a pool..

upvoted 9 times

Shoeboxx Most Recent 1 month, 3 weeks ago

Selected Answer: A

100% A.

upvoted 1 times

ctoklu 11 months, 2 weeks ago

A-Correct
B-Should be the DNS...

upvoted 1 times

Question #519 *Topic 1*

What are two roles of Domain Name Services (DNS)? (Choose two.)

A. builds a flat structure of DNS names for more efficient IP operations

B. encrypts network Traffic as it travels across a WAN by default

C. improves security by protecting IP addresses under Fully Qualified Domain Names (FQDNs)

D. enables applications to identify resources by name instead of IP address

E. allows a single host name to be shared across more than one IP address

Correct Answer: *DE*

Mozah Highly Voted 1 year, 5 months ago
nslookup can support "D".
D and E are correct
upvoted 5 times

Sim_James_27 Most Recent 1 year, 6 months ago
E is correct-having multiple ips assigned to one host, can do dns load balancing (like round robin), mostly i have used this terminology on SQL clusters and File share clusters
upvoted 4 times

shakyak 1 year, 7 months ago
Can some one justify E?
upvoted 1 times

Dante_Dan 1 year, 4 months ago
You can check it yourself :)
Go to a command prompt and type: nslookup examtopics.com
You will see something like this:

Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: examtopics.com
Addresses: 2606:4700:3032::6815:bb7
2606:4700:3034::ac43:a6ef
172.67.166.239
104.21.11.183

As you can see, more than one IP addresses (even an IPv6 address) are included under the same domain name
upvoted 7 times

cocoto4 1 year, 6 months ago
Say you have 3 servers hosting a webpage at webpage.com, so instead of the user typing 1.1.1.1, 1.1.1.2 or 1.1.1.3 to get to the server with the least load you can load balance this via the hostname. Also if you need to change the ip addresses users can still use the same name(webpage.com)
upvoted 8 times

bootloader_jack 1 year, 8 months ago
is D correct?
upvoted 1 times

DaBest 1 year, 8 months ago
D + E are correct
upvoted 2 times

Question #520 *Topic 1*

Which Cisco IOS command will indicate that interface GigabitEthernet 0/0 is configured via DHCP?

A. show ip interface GigabitEthernet 0/0 dhcp

B. show interface GigabitEthernet 0/0

C. show ip interface dhcp

D. show ip interface GigabitEthernet 0/0

E. show ip interface GigabitEthernet 0/0 brief

Correct Answer: *D*

joseph267 Highly Voted 1 year, 6 months ago

stop confusing people the answer is correct

R2#show ip int gi0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
Internet address is 10.1.0.2/24
Broadcast address is 255.255.255.255
Address determined by DHCP
MTU is 1500 bytes

upvoted 27 times

gewe Most Recent 3 months, 3 weeks ago

just test it in PT... answer is D

upvoted 1 times

cormorant 5 months, 3 weeks ago

let me guess. both d and e are correct but d is cisco's best practice so it's more correct

upvoted 1 times

RougePotatoe 7 months, 1 week ago

Selected Answer: D

Yes "show ip int brief" will show if address is configured manually but so can "show ip interface g0/0".

upvoted 1 times

MrUnknown 11 months ago

the command is telling me "Address is determined by setup command" And dhcp is working fine in network

upvoted 1 times

AWSEMA 11 months, 1 week ago

Selected Answer: D

Router#sh ip int g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 10.0.0.11/24
Broadcast address is 255.255.255.255
Address determined by DHCP
MTU is 1500 bytes

upvoted 1 times

dicksonpwc 1 year, 7 months ago

Correct Answer should be E
i have done a test and test result as below

We have a small network consisting of a router and a DHCP server. We want to configure the interface Gi0/0 on the router as a DHCP client. This is how this is done:
R1(config)#int Gi0/0
R1(config-if)#ip address dhcp
We can verify that the Gi0/0 interface has indeed got its IP address from the DHCP server by running the show ip int brief command:

R1#show ip int brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 192.168.0.1 YES DHCP up up
GigabitEthernet0/1 unassigned YES unset administratively down down
The DHCP keyword in the method column indicates that the IP information were obtained by the DHCP server.

upvoted 2 times

Hodicek 1 year, 6 months ago

E router will not accept br at the end of the command, so this command is totally wrong , the given answer by examtopics is correct , i checked it on my lab on packet tracer

upvoted 3 times

kmb192006 1 year, 8 months ago

I don't know why people say no one is correct...Instead Answer D is working for me in PT. With "show ip interface <interface>" the output shows the IP address is either determined by DHCP or setup command (manually):

R2#show ip int brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 10.1.0.2 YES DHCP up up
GigabitEthernet0/0/1 10.2.0.1 YES manual up down
GigabitEthernet0/0/2 unassigned YES unset administratively down down
Vlan1 unassigned YES unset administratively down down

R2#show ip int gi0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
Internet address is 10.1.0.2/24
Broadcast address is 255.255.255.255
Address determined by DHCP
MTU is 1500 bytes
...

R2#show ip int gi0/0/1
GigabitEthernet0/0/1 is up, line protocol is down (disabled)
Internet address is 10.2.0.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
...

upvoted 4 times

lucky1559 1 year, 9 months ago

There is no correct answer on this one (should be: show ip interface brief).

upvoted 1 times

Cisna 1 year, 8 months ago

show ip int brief wont show you DHCP infor

upvoted 4 times

Nicocisco 1 year, 3 months ago

Yes but we don't have the option show ip interface brief. so D is good

upvoted 2 times

xdxp23 1 year, 9 months ago

D because "show ip interface" show's all of the settings that are IP specific. You can see in the example code they provide on the website below that ip helper address is listed under the "show ip interface" command.

https://www.ciscopress.com/articles/article.asp?p=1829350

upvoted 2 times

AlexPlh 1 year, 10 months ago

no one.
sh ip interface brif will show you
Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0 unassigned YES DHCP up up

upvoted 4 times

bunblake 1 year, 10 months ago

what about B?

upvoted 1 times

bwg 2 years ago

What's the difference between "show interface" and "show ip interface"?

upvoted 2 times

kadamske 1 year, 8 months ago

The best way to verify is to try them in packet tracer and see the big difference

upvoted 2 times

Cisna 1 year, 8 months ago

Basically both give the same details only that show ip int will give more details that show int

upvoted 4 times

Question #521 *Topic 1*

What will happen if you configure the logging trap debug command on a router?

A. It causes the router to send messages with lower severity levels to the syslog server

B. It causes the router to send all messages with the severity levels Warning, Error, Critical, and Emergency to the syslog server

C. It causes the router to send all messages to the syslog server

D. It causes the router to stop sending all messages to the syslog server

Correct Answer: *C*

vadiminski Highly Voted 2 years, 1 month ago

A good way to memorize: Ernie Always Cries Even When Noone Is Dying

upvoted 16 times

dipanjana1990 10 months, 1 week ago

how about "(E)VERY (A)WESOME (C)ISCO (E)NGINEER (W)ILL (N)EED (I)CE-CREAM (D)AILY" !!!

upvoted 10 times

ProgSnob 1 year, 6 months ago

I use my own mnemonic devices but whatever works for a person is what matters.

upvoted 1 times

Liuka_92 1 year ago

it helped me

upvoted 2 times

Belinda 1 year, 3 months ago

Thanks

upvoted 1 times

lordnano Highly Voted 2 years, 2 months ago

B is not correct since the question talks about "logging trap debug".
C is the right anwers:
The comment of wirlerneman is right, but not really useful without the source and the details:
"
When a level is specified in the logging trap level command, the router is configured to send messages with lower severity levels as well. For example, the logging trap warning command configures the router to send all messages with the severity warning, error, critical, and emergency. [this is Important]
Similarly, the logging trap debug command causes the router to send all messages to the syslog server. Exercise caution while enabling the debug level. Because the debug process is assigned a high CPU priority, using it in a busy network can cause the router to crash.
"
https://www.ciscopress.com/articles/article.asp?p=426638&seqNum=3

upvoted 11 times

Tera_911 Most Recent 1 year, 1 month ago

One more mnemonic - Every Awesome Cisco Engineer Will Need IceCream Daily

upvoted 7 times

LingLingW 1 year, 5 months ago

Level
0 - Emergency
1 - Alert
2 - Critical
3- Error
4 - Warning
5 - Notification
6 - Informational
7 - Debugging

upvoted 5 times

promaster 1 year, 11 months ago

logging trap debug command causes the router to send all messages to the syslog server. Exercise caution while enabling the debug level. Because the debug process is assigned a high CPU priority, using it in a busy network can cause the router to crash..... fr cisco press
https://www.ciscopress.com/articles/article.asp?p=426638&seqNum=3

upvoted 1 times

mrsiafu 2 years, 1 month ago

System Message Logging
https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.html#wp1054426

upvoted 2 times

Tonking 2 years, 3 months ago

The Correct answer is B - The logging trap warning command configures the router to send all messages with the severity warning, error, critical, and emergency

upvoted 2 times

pagamar 1 year, 5 months ago

No B: Alarm severity is missing in the list, plus Notifications and Informational. The right answer should be C (all messages).

upvoted 1 times

wirlernenman 2 years, 3 months ago

For example, the logging trap warning command configures the router to send all messages with the severity warning, error, critical, and emergency. Similarly, the logging trap debug command causes the router to send all messages to the syslog server. Exercise caution while enabling the debug level.

upvoted 2 times

Question #522 *Topic 1*

A network administrator enters the following command on a router: logging trap 3. What are three message types that will be sent to the Syslog server? (Choose three.)

A. informational

B. emergency

C. warning

D. critical

E. debug

F. error

Correct Answer: *BDF*

martco Highly Voted 2 years, 3 months ago
Every Awesome Cisco Engineer Will Need Icecream Daily (L0-7)
upvoted 61 times

frejus 2 years, 2 months ago
that's awesome thanks you
upvoted 8 times

S_10 Highly Voted 1 year, 10 months ago
BEST WAY TO REMEMBER TRAP MESSAGE
Every means Emergency
Awesome means Alert
Cisco means Critical
Engineer means Error
Will means Warning
Need Notice (Notification)
Ice-Cream means Informational
Daily Debugging
upvoted 29 times

Techno_Head Most Recent 2 years, 3 months ago
The answer is Emergency, Alert, and Critical but alert is not an option.
upvoted 5 times

SasithCCNA 2 years, 3 months ago
no ,

SNMP Trap messages classify as follows,
level 7 - Debug
level 6 - Informational
level 5 - Notifications
level 4 - Warnings
level 3 - Errors
level 2 - Critical
level 1 - Alerts
level 0 - Emergencies

The questions tells 'logging trap 3' command is entered by the network administrator which means all messages from 0 to 3(include 3) will be logged. So emergencies, alerts ,critical and error messages are logged. In the question only 3 answers are asked so BDF is correct.
upvoted 24 times

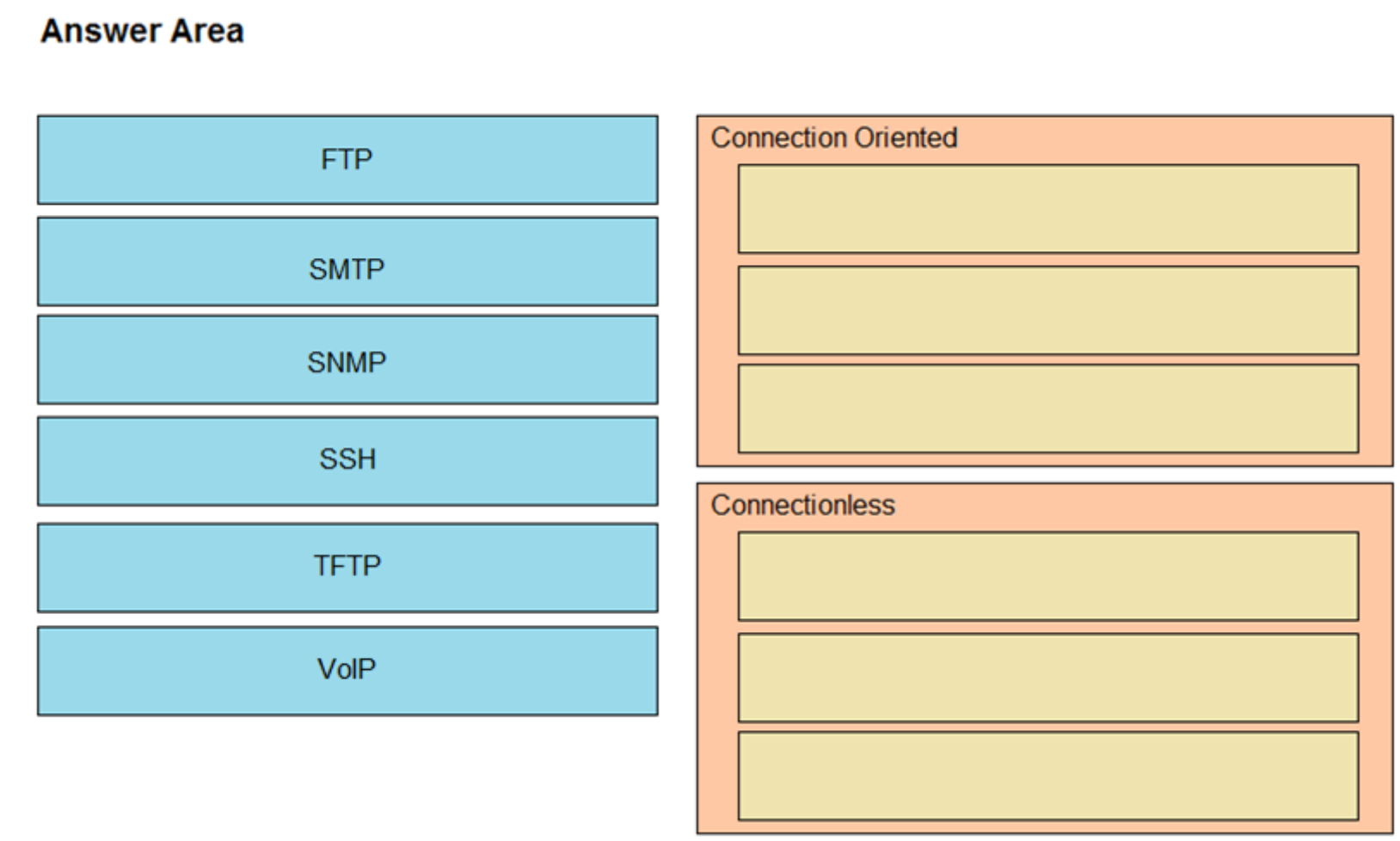
SasithCCNA 2 years, 3 months ago
Oops sorry what you have said is correct my bad . I didn't clearly read your answer.
upvoted 5 times

Question #523 *Topic 1*

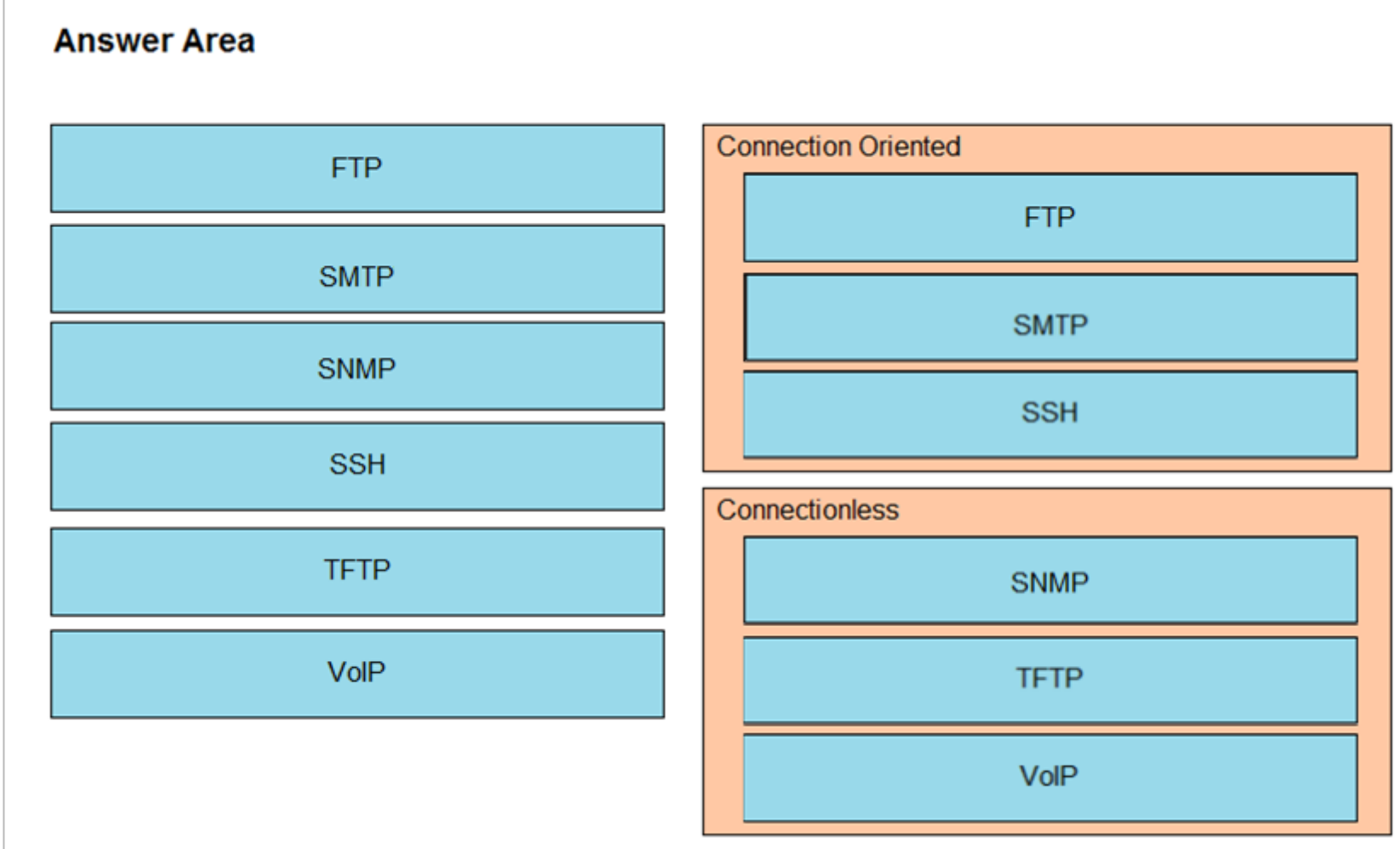
DRAG DROP -

Drag and drop the network protocols from the left onto the correct transport services on the right.

Select and Place:



Correct Answer:



vadiminski Highly Voted 2 years, 1 month ago

Correct answer, they ask which use TCP and which UDP

upvoted 9 times

martialstriker09 Most Recent 11 months, 2 weeks ago

TCP vs UDP lol

upvoted 2 times

Question #524 *Topic 1*

A network engineer must back up 20 network router configurations globally within a customer environment. Which protocol allows the engineer to perform this function using the Cisco IOS MIB?

A. ARP

B. SNMP

C. SMTP

D. CDP

Correct Answer: *B*
SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.
The SNMP framework has three parts:
ɹ€¢ An SNMP manager
ɹ€¢ An SNMP agent
ɹ€¢ A Management Information Base (MIB)
The Management Information Base (MIB) is a virtual information storage area for network management information, which consists of collections of managed objects.
With SNMP, the network administrator can send commands to multiple routers to do the backup.

omgrain Highly Voted 2 years, 8 months ago
be aware. If you are using SNMP, it will change all configs to those devices. answer B is right.
upvoted 6 times

Question #525 *Topic 1*

Which command enables a router to become a DHCP client?

A. ip address dhcp

B. ip dhcp client

C. ip helper-address

D. ip dhcp pool

Correct Answer: *A*
If we want to get an IP address from the DHCP server on a Cisco device, we can use the command ג€ip address dhcpג€.
Note: The command ג€ip helper-addressג€ enables a router to become a DHCP Relay Agent.

akhuseyinoglu Highly Voted 3 years ago
Correct Answer : A
upvoted 20 times

TeeItUp 3 years ago
Correct Answer: B
"You must configure the ip dhcp client commands before entering the ip address dhcp command on an interface to ensure that the DHCPDISCOVER messages that are generated contain the correct option values."
upvoted 5 times

SanchezEldorado 2 years, 11 months ago
I was really confused for a bit, but the answer is A. The snippet in the previous comment is only part of the statement. You ONLY need to configure "ip dhcp client" commands before "ip add dhcp" IF you want them to be enabled right away. It doesn't mean that you actually NEED to use "ip DHCP client" commands. In otherwords, you don't NEED option values to enable DHCP on the interface.

"The ip dhcp client commands are checked only when an IP address is acquired from DHCP. If any of the ip dhcp client commands are entered after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from DHCP. This means that the new configuration will take effect only after either the ip address dhcp command or the release dhcp and renew dhcpEXECcommandshave been configured."

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/12-4/dhcp-12-4-book/config-dhcp-client.html
upvoted 5 times

Mountie 2 years, 10 months ago
Before You Begin
You must configure the ip dhcp client commands before entering the ip address dhcp command on an interface to ensure that the DHCPDISCOVER messages that are generated contain the correct option values. The ip dhcp client commands are checked only when an IP address is acquired from DHCP. If any of the ip dhcp client commands are entered after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from DHCP. This means that the new configuration will take effect only after either the ip address dhcp command or the release dhcp and renew dhcpEXECcommandshave been configured.
according to your link, ip dhcp client must be confugured before ip address dhcp to be able to configured.
upvoted 3 times

jjkcoins 2 years, 10 months ago
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/12-4/dhcp-12-4-book/config-dhcp-client.html
upvoted 1 times

Daimen Highly Voted 3 years ago
A is the right answer. ip dhcp address makes the router become a dhcp client. ip dhcp client is needed to enable some parameters which makes the router(dhcp client) function properly.
upvoted 12 times

knister 2 years, 11 months ago
Agree, this is the answer that makes more sense
upvoted 2 times

Rob2000 Most Recent 1 year, 8 months ago
Correct Answer: A
The command that makes the client send DCHP REQUEST to get an IP address from a DHCP server is "ip address dhcp", so it is the one that enables DHCP on an interface. .
"ip dhcp client" defines parameters used by the client to ask the address, for example the client id,hostname, lease time among others.
It is good practice to define the client parameters before the client requests the address.
upvoted 1 times

GrigTech 2 years, 5 months ago

Before You Begin
You must configure the ip dhcp client commands before entering the ip address dhcp command on an interface to ensure that the DHCPDISCOVER messages that are generated contain the correct option values. The ip dhcp client commands are checked only when an IP address is acquired from DHCP. If any of the ip dhcp client commands are entered after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from DHCP. This means that the new configuration will take effect only after either the ip address dhcp command or the release dhcp and renew dhcpEXECcommandshave been configured.

upvoted 1 times

icca17 2 years, 6 months ago

Correct is A!
Configuring the DHCP Client

Cisco devices running Cisco software include the Dynamic Host Configuration Protocol (DHCP) server and relay agent software, which are enabled by default. Your device can act as both the DHCP client and the DHCP server. Use the ip address dhcp command to obtain IP address information for the configured interface.
SUMMARY STEPS
1. enable
2. configure terminal
3. interface type number
4. ip address dhcp
5. end
6. debug dhcp detail
7. debug ip dhcp server packets

upvoted 2 times

DavidL 2 years, 6 months ago

Answer A. In packet tracer it has no ip dhcp client command.

upvoted 4 times

boghota 2 years, 6 months ago

I can confirm this. ISR4331 Router in Cisco Packet Tracer shows:

Router(config)#ip dhcp ?
excluded-address Prevent DHCP from assigning certain addresses
pool Configure DHCP address pools
relay DHCP relay agent parameters

Router(config)#int g0/0/0
Router(config-if)#ip ?
access-group Specify access control for packets
address Set the IP address of an interface
authentication authentication subcommands
flow NetFlow Related commands
hello-interval Configures IP-EIGRP hello interval
helper-address Specify a destination address for UDP broadcasts
mtu Set IP Maximum Transmission Unit
nat NAT interface commands
ospf OSPF interface commands
proxy-arp Enable proxy ARP
split-horizon Perform split horizon
summary-address Perform address summarization

Router(config-if)#ip address ?
A.B.C.D IP address
dhcp IP Address negotiated via DHCP

Router(config-if)#ip address dhcp ?
<cr>

upvoted 4 times

JimGrayham 2 years, 6 months ago

A. ip address dhcp. CCNA 200-301: Official Cert Guide Vol. 1 P.197 Chapter 6: Configuring Basic Switch Management.

upvoted 4 times

altiit 2 years, 7 months ago

Correct Answer is A, Use the ip address dhcp command to obtain IP address information for the configured interface.
ip dhcp client client-id {interface-name| ascii string| hex string}

ip dhcp client class-id {string| hex string}

ip dhcp client lease days [hours][minutes]

ip dhcp client hostname host-name

[no] ip dhcp client request option-name

ip address dhcp

Note: There is no command ip dhcp client without client-ID, class-ID, Hostname, request and lease.

upvoted 3 times

diamcle 2 years, 7 months ago

ip address dhcp is for Cisco IOS Release 15M&T
ip dhcp client is for Cisco IOS Release 12.4
So, I thinh the question needs to be more specific.

upvoted 2 times

GodUsopp 2 years, 7 months ago

IP DHCP CLIENT is not a full command it has many options such as
(config-if)# ip dhcp client class-id my-class-id
or
(config-if)# ip dhcp client lease 2
or
(config-if)# ip dhcp client hostname router1
or
(config-if)# no ip dhcp client request tftp-server-address

these are examples of the full commands for the ip dhcp client and all of them are optional commands.
Source
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/12-4/dhcp-12-4-book/config-dhcp-client.html

upvoted 3 times

Saske16 2 years, 7 months ago

correct answer is B, remember A is not wrong but for cisco some answers are more correct than others. A is right but B is more right as you have to configure the ip dhcp client commands before entering ip address dhcp

upvoted 1 times

devildog 2 years, 7 months ago

Correct answer is A straight from the cisco site.

upvoted 2 times

kimi7 2 years, 8 months ago

from the cisco page https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/12-4/dhcp-12-4-book/config-dhcp-client.html

On the DHCP server, the configuration is as follows:

ip dhcp pool 1
network 10.1.1.0 255.255.255.0
lease 1 6

On the DHCP client, the configuration is as follows on interface E2:

interface Ethernet2
ip address dhcp
so how A is not the right answer i dont know...al the other options are set with
ip address client...something
but just to enable it to take ip its
ip address dhcp

upvoted 2 times

karemAbdullah 2 years, 8 months ago

to configure the interface Gi0/0 on the router as a DHCP client. This is how this is done:

R1(config)#int Gi0/0
R1(config-if)#ip address dhcp

A is the correct answer

upvoted 2 times

KingKeelo1 2 years, 8 months ago

Correct answer is indeed A

upvoted 3 times

Ebenezer 2 years, 8 months ago

This answer is wrong. The correct answer is A.

upvoted 2 times

SharonANita 2 years, 8 months ago

ip address ---A

upvoted 2 times

Question #526 *Topic 1*

Which function does an SNMP agent perform?

A. It sends information about MIB variables in response to requests from the NMS

B. It manages routing between Layer 3 devices in a network

C. It coordinates user authentication between a network device and a TACACS+ or RADIUS server

D. It requests information from remote network nodes about catastrophic system events

Correct Answer: *A*

hippyjm Highly Voted 2 years, 1 month ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-16/snmp-xe-16-book/nm-snmp-cfg-snmp-support.html

A is correct

upvoted 7 times

dicksonpwc Most Recent 1 year, 9 months ago

This document discusses how to enable an SNMP agent on a Cisco device and how to control the sending of SNMP notifications from the agent. For information about using SNMP management systems, see the appropriate documentation for your network management system (NMS) application.

upvoted 2 times

Question #527 *Topic 1*

What are two roles of the Dynamic Host Configuration Protocol (DHCP)? (Choose two.)

A. The DHCP server assigns IP addresses without requiring the client to renew them.

B. The DHCP server leases client IP addresses dynamically.

C. The DHCP client is able to request up to four DNS server addresses.

D. The DHCP server offers the ability to exclude specific IP addresses from a pool of IP addresses.

E. The DHCP client maintains a pool of IP addresses it is able to assign.

Correct Answer: *BD*

chomjosh Highly Voted 2 years, 10 months ago

Tricky question. Note DHCP is administered at the "Server" level. The word "client" in the other options was deliberate to mislead. DHCP server requires clients to renew IP except it is tied to MAC, hence option A is out.
BD is correct.

upvoted 15 times

Isuzu 2 days, 15 hours ago

Best way to remember the answer... thank you

upvoted 1 times

mutlumesut Most Recent 7 months ago

why c is not correct?

upvoted 1 times

cormorant 7 months ago

if 'e' said, 'the dhcp server maintains a pool of IPs it is able to assign', that would also be correct

upvoted 3 times

DARKK 1 year ago

Selected Answer: BD

B & D are correct. E says CLIENT, Don't get tricked.

upvoted 4 times

Adaya 1 year, 11 months ago

E almost catch me

upvoted 4 times

m_magdi 2 years, 1 month ago

E why not

upvoted 2 times

ajajajaj 2 years, 1 month ago

If it's DHCP server, it could be correct...

upvoted 3 times

LTTAM 2 years, 4 months ago

BD is correct. Love how they throw in DHCP server and DHCP client. If you don't catch these minor misplacement of words, one can easily get this question wrong.

upvoted 4 times

velrisan 1 year, 9 months ago

Your right, in fact. Is important read the question with pacient and the options too. The answer is B and D. Is a easy question with a easy answer. But sometime we feels with so much confidence and believe we have this quiestions ready

upvoted 3 times

Question #528 *Topic 1*

Which command must be entered when a device is configured as an NTP server?

A. ntp peer

B. ntp master

C. ntp authenticate

D. ntp server

Correct Answer: *B*

sabaheta Highly Voted 2 years, 8 months ago

- ntp master {stratum-level}: NTP server mode—the device acts only as an NTP server, and not as an NTP client. The device gets its time information from the internal clock on the device.
- ntp server {address | hostname}: NTP client/server mode—the device acts as both client and server. First, it acts as an NTP client, to synchronize time with a server. Once synchronized, the device can then act as an NTP server, to supply time to other NTP clients.

reference : Wendell Odom CCNA vol 2
Correct answer : B
upvoted 18 times

Scipions Highly Voted 2 years, 1 month ago

mannaggia al netacad
upvoted 11 times

Question #529 *Topic 1*

What event has occurred if a router sends a notice level message to a syslog server?

A. A certificate has expired

B. An interface line has changed status

C. A TCP connection has been torn down

D. An ICMP connection has been built

Correct Answer: *B*

IxlJustinlxl Highly Voted 2 years ago

0 Emergencies System shutting down due to missing fan tray
1 Alerts Temperature limit exceeded
2 Critical Memory allocation failures
3 Errors Interface Up/Down messages
4 Warnings Configuration file written to server, via SNMP request
5 Notifications Line protocol Up/Down
6 Information Access-list violation logging
7 Debugging Debug messages
ANSWER = B
upvoted 24 times

BooleanPizza 1 year, 9 months ago

Every Awesome Cisco Engineer Will Need Ice Cream Daily :)
upvoted 21 times

Alvaro13 10 months, 1 week ago

From Jeremy It Lab
upvoted 7 times

chr Highly Voted 2 years ago

When an interface goes down a log message is generated including the following "#LINEPROTO-5-UPDOWN".
5 is the severity level. Severity 5 is classed as "notification"
Odum book 2 pages 176-177
upvoted 8 times

Ciscoman021 Most Recent 2 months, 2 weeks ago

Selected Answer: B

If a router sends a notice level message to a syslog server, it typically indicates that an interface line has changed status. the correct answer is B.
upvoted 1 times

xX_CCNA_Xx 1 year, 2 months ago

here is another good one

Eernie Always Cry Even When No-one Is Dying (:

0 Emergency
1 Alert
2 Critical
3 Errors
4 Warning
5 Notification
6 Information
7 Debugging
upvoted 2 times

Angel75 1 year, 10 months ago

Notice... means Notification I suppose (level 5)
upvoted 4 times

Ahhmedd 2 years, 10 months ago

WY not C
upvoted 3 times

Chipapo 2 years, 10 months ago

The router doesn't even operate at later 4
upvoted 13 times

frejus 2 years, 2 months ago

lol funny

upvoted 1 times

SasithCCNA 2 years, 2 months ago

is it though

upvoted 1 times

Samuelpn96 1 year, 9 months ago

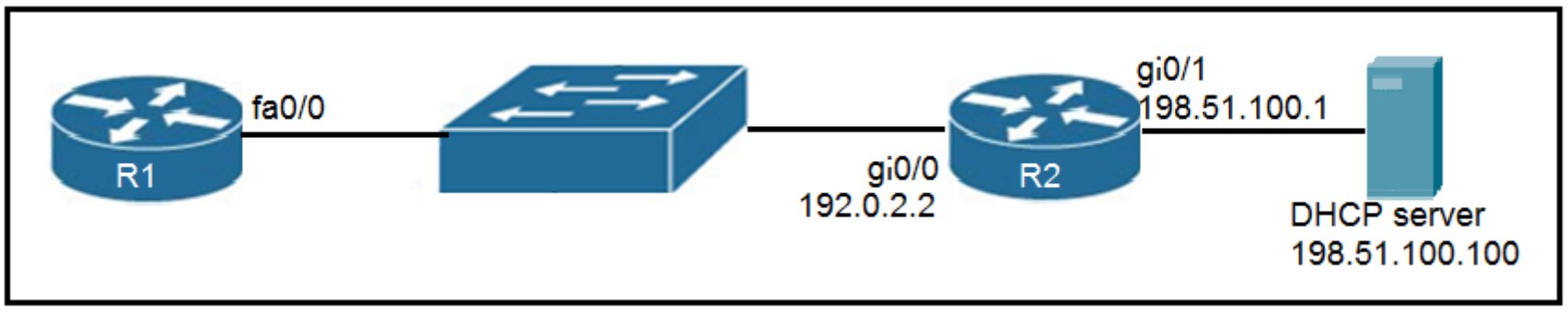
But aren't Extended ACLs filtering in a router a layer 4 operation?

Guidelines and Restrictions for Using Layer 4 Operators in ACLs
https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book/acl.html

But the answer is B anyway.

upvoted 1 times

Question #530 *Topic 1*



Refer to the exhibit. An engineer deploys a topology in which R1 obtains its IP configuration from DHCP. If the switch and DHCP server configurations are complete and correct, which two sets of commands must be configured on R1 and R2 to complete the task? (Choose two.)

A. R1(config)# interface fa0/0 R1(config-if)# ip helper-address 198.51.100.100

B. R2(config)# interface gi0/0 R2(config-if)# ip helper-address 198.51.100.100

C. R1(config)# interface fa0/0 R1(config-if)# ip address dhcp R1(config-if)# no shutdown

D. R2(config)# interface gi0/0 R2(config-if)# ip address dhcp

E. R1(config)# interface fa0/0 R1(config-if)# ip helper-address 192.0.2.2

Correct Answer: *BC*

ZayaB Highly Voted 2 years, 3 months ago

Note that DHCP server is behind R2 and R1 needs IP via DHCP. Therefore, R2 needs to be a relay agent. On R1 interface, ip address dhcp and R2 inside interface, ip helper-address 192.168.100.100 (dhcp server). Answers are B and C.

upvoted 24 times

cormorant Most Recent 6 months ago

the ip helper-address cmd must point to the ip of the dhcp server. oftentimes, it's a router. but here, it's an actual server!

upvoted 1 times

FALARASTA 1 month ago

Configuring DHCP relay agents
We configure a DHCP relay agent only on the interface that is directly connected to a local subnet or a client.

https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-dhcp-relay-agent-on-cisco-routers.html

upvoted 1 times

SVN05 1 year ago

I think ZayaB mistaken for the ip helper-address command. It suppose to be "ip helper-address 198.51.100.100" on R2 Gi 0/0 and "ip address dhcp" on R1 Fa 0/0

upvoted 2 times

Hodicek 1 year, 6 months ago

act r1 as PC and add dhcp helper command to r2 and ip should be the dhcp server

upvoted 1 times

sinear 2 years, 4 months ago

It should be B and D, with in D "R1" instead of "R2".

upvoted 2 times

Zerotime0 2 years, 4 months ago

I think thats it.

upvoted 1 times

Zerotime0 2 years, 4 months ago

Nevermind bc correct

upvoted 3 times

sinear 2 years, 4 months ago

I think there is an error in the answers.
Refer to same question 413 on https://pupuweb.com/ccna-200-301-actual-exam-question-answer-dumps-5/2/ : it is correct there
Instead of having
I think here they put an error in the answer (confusion between R1 and R2 in the proposal with "ip dhcp address".

upvoted 1 times

Aval0n1 2 years, 2 months ago

There is no need of DHCP relay if gi0/0 R2 have assigned dhcp address. So B and C are correct

upvoted 2 times

Ali526 2 years, 5 months ago

Don't agree. CE are correct.

upvoted 4 times

ROBZY90 2 years, 1 month ago

BC Is correct, you must configure relay-agent on the router closest to the client (Not on the client). Bit of a tricky question to be honest

upvoted 10 times

sdokmak 1 year, 11 months ago

This is what I was looking for

upvoted 3 times

Ali526 2 years, 4 months ago

Sorry. BC correct.

upvoted 9 times

Question #531 *Topic 1*

Which two actions are performed by the Weighted Random Early Detection mechanism? (Choose two.)

A. It supports protocol discovery.

B. It guarantees the delivery of high-priority packets.

C. It can identify different flows with a high level of granularity.

D. It can mitigate congestion by preventing the queue from filling up.

E. It drops lower-priority packets before it drops higher-priority packets.

Correct Answer: *DE*
Weighted Random Early Detection (WRED) is just a congestion avoidance mechanism. WRED drops packets selectively based on IP precedence. Edge routers assign IP precedences to packets as they enter the network. When a packet arrives, the following events occur:
1. The average queue size is calculated.
2. If the average is less than the minimum queue threshold, the arriving packet is queued.
3. If the average is between the minimum queue threshold for that type of traffic and the maximum threshold for the interface, the packet is either dropped or queued, depending on the packet drop probability for that type of traffic.
4. If the average queue size is greater than the maximum threshold, the packet is dropped.
WRED reduces the chances of tail drop (when the queue is full, the packet is dropped) by selectively dropping packets when the output interface begins to show signs of congestion (thus it can mitigate congestion by preventing the queue from filling up). By dropping some packets early rather than waiting until the queue is full, WRED avoids dropping large numbers of packets at once and minimizes the chances of global synchronization. Thus, WRED allows the transmission line to be used fully at all times.
WRED generally drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, the higher the priority of a packet, the higher the probability that the packet will be delivered.
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conavd/configuration/15-mt/qos-conavd-15-mt-book/qos-conavd-cfg-wred.html

poovnair Highly Voted 2 years, 8 months ago
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conavd/configuration/xe-16/qos-conavd-xe-16-book/qos-conavd-cfg-wred.html
DE
upvoted 8 times

Ciscoman021 Most Recent 2 months, 1 week ago
Selected Answer: DE
The two actions performed by the Weighted Random Early Detection (WRED) mechanism are:

D. It can mitigate congestion by preventing the queue from filling up.
E. It drops lower-priority packets before it drops higher-priority packets.
upvoted 1 times

ricky1802 3 months, 1 week ago
Is this CCNA question?
upvoted 3 times

Taku2023 1 month, 3 weeks ago
this is Quality of Service
upvoted 2 times

DARKK 1 year ago
Selected Answer: DE
D & E are correct. WREN does NOT guarantees the delivery of high-priority packets, B is just flat out Wrong.
upvoted 1 times

cdewet 2 years, 6 months ago
I also think the answer is DE.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conavd/configuration/xe-16/qos-conavd-xe-16-book/qos-conavd-time-wred.html
"WRED is a congestion avoidance mechanism. WRED combines the capabilities of the Random Early Detection (RED) algorithm with the IP precedence feature to provide for preferential traffic handling of higher priority packets. WRED can selectively discard lower priority traffic when the interface begins to get congested and provide differentiated performance characteristics for different classes of service."
upvoted 2 times

Ebenezer 2 years, 8 months ago

This answer is wrong. The answer should be B and D. WRED guarantees the delivery of high priority packets and it ensures there is no congestion. If there are no high priority packets and congestion, there will be no need for QoS.

upvoted 1 times

SVN05 1 year ago

Ebenezer. Your right however the question stats actions performed thus D and E are higher priority answers compared to B.

upvoted 2 times

Question #532 *Topic 1*

```
R2#show ip nat translations
Pro  Inside global      Inside local     Outside local      Outside global
tcp  172.23.104.3:43268 10.4.4.4:43268   172.23.103.10:23   172.23.103.10:23
tcp  172.23.104.4:45507 10.4.4.5:45507   172.23.103.10:80   172.23.103.10:80
```

Refer to the exhibit. An engineer configured NAT translations and has verified that the configuration is correct. Which IP address is the source IP after the NAT has taken place?

A. 10.4.4.4

B. 10.4.4.5

C. 172.23.103.10

D. 172.23.104.4

Correct Answer: *C*

LTTAM Highly Voted 2 years, 4 months ago

The answer should be D. According to Cisco, the Inside Global would be considered the source address after NAT has taken place.

Source - https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/4606-8.html

upvoted 42 times

pianetaperez 2 years, 3 months ago

If the communication is originated by the external host, the answer is C. The router applies a Destination NAT, not a Source NAT.

upvoted 2 times

RougePotatoe 7 months, 1 week ago

Even if you were right there were no translation done. Notice Outside local and Outside global had no translation performed.

upvoted 2 times

Friday_Night 2 weeks, 2 days ago

correct me if im wrong but the inside router does not detect the private IP address (inside global address)of a received packet right? they can only see public IP address (outside global) used. that's why the inside/outside global is always the same

upvoted 1 times

velrisan 2 years ago

D is correct answer. Why? Because this: When the NAT router receives a packet on its inside interface with a source address of 10.10.10.1, the source address is translated to 171.16.68.5. This also means that when the NAT router receives a packet on its outside interface with a destination address of 171.16.68.5, the destination address is translated to 10.10.10.1.
Source is the sama source provide by LTTAM there you will see why the correct is the "D" and below of the link is present a small example about outside

upvoted 3 times

sinear Highly Voted 2 years, 4 months ago

Hard to answer that question without knowing what kind of paqet we are talking about, incoming or outgoing ?

upvoted 11 times

oooMooo 2 years, 1 month ago

The traffic is outgoing.

upvoted 2 times

Isuzu Most Recent 2 days, 14 hours ago

Selected Answer: C

Maybe this question wanted to ask “which IP address is the source IP at the receiving side?” as there are two correct answers for inside local IP address (10.4.4.4 & 10.4.4.5) so they cannot be the correct answer.

upvoted 1 times

Da_Costa 1 week, 1 day ago

D is the correct answer

upvoted 1 times

FALARASTA 1 month ago

Selected Answer: D

I believe this is the same as address after direct traslation from inside local. Simply your companys pubic ip address. then it is the inside global D

upvoted 1 times

Matalongo 1 month, 3 weeks ago

D is the correct answer
upvoted 1 times

RougePotatoe 7 months, 1 week ago

Selected Answer: D

In case anyone is confused. Notice how there is no NAT or PAT done on the outside network.
Inside = Company network
Outside = External network

Global = Public
Local = Private
upvoted 2 times

Etidic 7 months, 2 weeks ago

Selected Answer: D

The Answer is D
upvoted 1 times

re__roy 7 months, 2 weeks ago

Answer is D
upvoted 1 times

GigaGremlin 8 months ago

Selected Answer: D

Which IP address is the source IP after the NAT has taken place?
upvoted 1 times

Murphy2022 8 months ago

Selected Answer: C

I've rebuild this with static nat inside of packet tracer. When the packet arrives at the router and is converted with nat the source IP matches the inside global address.
upvoted 1 times

RougePotatoe 7 months, 1 week ago

C is incorrect. Notice how there was no NAT performed on the outside ip address. The Outside local and outside global is the same thus no NAT or PAT was performed.
upvoted 1 times

TA77 11 months, 1 week ago

Selected Answer: D

Answer is D.

Inside Local: The IP address of the host from the perspective of the inside network. (The actual IP address of the host).

Inside Global: The IP address of the host from the prospective of the outside network. (The public IP address configured on the router. Which is the IP address of the host after NAT took place).

Outside local: The IP address of the destination from the prospective of the inside network.

Outside Global: The IP address of the destination from the prospective of the outside network.

For the last two, unless the 'Destination Nat' is configured, they will be the same. 'Destination Nat' is outside the scope of CCNA.
upvoted 1 times

Liuka_92 11 months, 2 weeks ago

Correct is D
upvoted 1 times

iGlitch 1 year ago

Selected Answer: D

Source IP is another word for 'Inside global IP'.
upvoted 1 times

PoBratsky 1 year ago

Selected Answer: D

D is correct
upvoted 1 times

BraveBadger 1 year, 1 month ago

Selected Answer: C

I'm going with C because to me "after the NAT has taken place" means the packet is leaving the router, and it's source IP would be the outside global. But as others have said it depends on if the packet is coming in or going out.
upvoted 4 times

MDK94 11 months, 1 week ago

After the packet leaves the router its IP address would be the Inside global address, not the outside global address, meaning its D

upvoted 2 times

battery1979 11 months, 1 week ago

That was my take on it as well.

upvoted 1 times

ismatdmour 1 year, 2 months ago

Selected Answer: D

D is correct. The question is asking what happened to the source IP after NAT. Keyword is "source IP" which tells us that the question is about outgoing traffic translation (where the inside local is changed to inside global). Hence D. If the question asked about what happened to "destination IP" then the talk will be about incoming traffic where the destination ip of inside global will be translated to inside local (source ip is kept unchanged of outside global"). In this other case, C will be the correct answer. One more note on this question is that all addresses are private; i.e NAT is translating private to private addresses, which can be needed in certain cases.

upvoted 2 times

Question #533 *Topic 1*

If a notice-level message is sent to a syslog server, which event has occurred?

A. A network device has restarted.

B. A debug operation is running.

C. A routing instance has flapped.

D. An ARP inspection has failed.

Correct Answer: *C*
Usually no action is required when a route flaps so it generates the notification syslog level message (level 5).

Artengineer Highly Voted 3 years ago
A is the right answer
upvoted 17 times

Eric852 Highly Voted 1 year, 2 months ago
Selected Answer: C
C is the correct answer.
A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. C states that it's A routing instance, which means it only happens to a single subject. Flapping does not mean the interface going up and down multiple times in very short period, I don't know where that definition came from, it means the instance went through a down-up cycle(s). The whole device restarted is much worse than a single instance flapped, all the config that's not in the start-up config can be wiped out.
upvoted 8 times

dropspablo Most Recent 1 week, 4 days ago
Selected Answer: C
Routing instance refers to the OSPF process, as in EIGRP or BGP they use Autonomous System (AS), which are similar to OSPF areas.
Below, a deliberate failure was created in the OSPF adjacency with hello mishmash, with this we can see that we received logging messages level 5 Notice, referring to the failure in the routing instance of Process 10.
R3(config-if)#ip ospf hello-interval 20
%OSPF-5-ADJCHG: Process 10, Nbr 10.23.0.2 on GigabitEthernet0/1 from FULL to DOWN, Neighbor Down: Dead timer expired.
%OSPF-5-ADJCHG: Process 10, Nbr 10.23.0.2 on GigabitEthernet0/1 from FULL to DOWN, Neighbor Down: Interface down or detached.
upvoted 1 times

dropspablo 1 week, 4 days ago
And even, instead of changing the hello-interval, we turn off this interface, also we receive the message:
%OSPF-5-ADJCHG: Process 10, Nbr 10.23.0.2 on GigabitEthernet0/1 from FULL to DOWN, Neighbor Down: Interface down or detached.
(Process 10 routing instance failed.)
So answer C is correct, as this level 5 message (notice) can be forwarded to the Syslog server via SNMP.
upvoted 1 times

dropspablo 1 week, 4 days ago
But this is a tricky question, because also when we restart a network device, the devices connected to it publish a notice-level message (level 5) that can be forwarded to the Syslog Server via SNMP:
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down.
However, this message indicates an interruption in the connectivity of the interface, and we cannot say with this message alone that a network device has been restarted, there are also other reasons for this message, such as cable disconnection or port turned off.
And in the exercise it is questioned what “occurred” only with “notice-level message”, and not what could have happened.
And when an OSPF process fails (routing instance adjacency down) - we know with 100% certainty what “occurred”, a routing instance has flapped.
upvoted 1 times

rogi2023 1 month, 2 weeks ago
Selected Answer: C
I believe they wait for answer C, and I believe the C is correct. I vote for C to rise the % of C.
upvoted 1 times

Peter_panda 2 months ago
Selected Answer: C
I would say C, e.g. an adjacency change generates a notification level (5) message.
%OSPF-5-ADJCHG: Process 1, Nbr 192.168.12.2 on FastEthernet0/0 from LOADING to FULL, Loading Done
https://networklessons.com/ospf/troubleshooting-ospf-neighbor-adjacency
upvoted 2 times

oatmealturkey 3 months, 2 weeks ago
Selected Answer: A

This is an old source but still from Cisco, and it says "The Notice level displays interface up or down transitions and system restart messages."
https://www.ciscopress.com/articles/article.asp?p=426638&seqNum=3
upvoted 1 times

badboyrobinson 5 months, 2 weeks ago

Selected Answer: A

Going with A because notice level is not a biggie
upvoted 2 times

cormorant 7 months ago

notice level means the router is flapping. it's all that matters to pass to test
upvoted 2 times

medamine2022 10 months, 3 weeks ago

Selected Answer: A

a because the notice level for max reason reboot the device
upvoted 1 times

AudreyLin 1 year, 2 months ago

Selected Answer: A

A is true
upvoted 1 times

yonten007 1 year, 4 months ago

Selected Answer: A

A is the right answer
upvoted 2 times

ayoubenn 1 year, 7 months ago

Interface up or down transitions and system restart messages, displayed at the notifications level: this message is only for information.
upvoted 1 times

imo90s 2 years, 1 month ago

Answer is A. (A router restart is not a big deal)
Router flapping would be level 3 (as it means that interface(s) are going up down multiple times in very short period)
upvoted 6 times

oooMooo 2 years, 1 month ago

Error messages about software or hardware malfunctions, displayed at levels warnings through emergencies: these types of messages mean that the functionality of the access point is affected.

Output from the debug commands, displayed at the debugging level: debug commands are typically used only by the Technical Assistance Center (TAC).

Interface up or down transitions and system restart messages, displayed at the notifications level: this message is only for information; access point functionality is not affected.

Reload requests and low-process stack messages, displayed at the informational level: this message is only for information; access point functionality is not affected.
upvoted 2 times

devildog 2 years, 7 months ago

From Cisco documentation:

Error Message %ASA-5-336010 EIGRP-<ddb_name> tableid as_id: Neighbor address (%interface) is event_msg: msg
Explanation Neighbor Change. A neighbor went up or down.

Recommended Action Check to see why the link on the neighbor is going down or is flapping. This may be a sign of a problem, or a problem may occur because of this.
upvoted 3 times

Clxxcv420 2 years, 8 months ago

https://www.cisco.com/en/US/docs/security/asa/asa80/system/message/logmsgs.pdf

It's not a ARP inspection, it on level 3 generates... I think the answer is A.
upvoted 2 times

Dileesh 2 years, 8 months ago

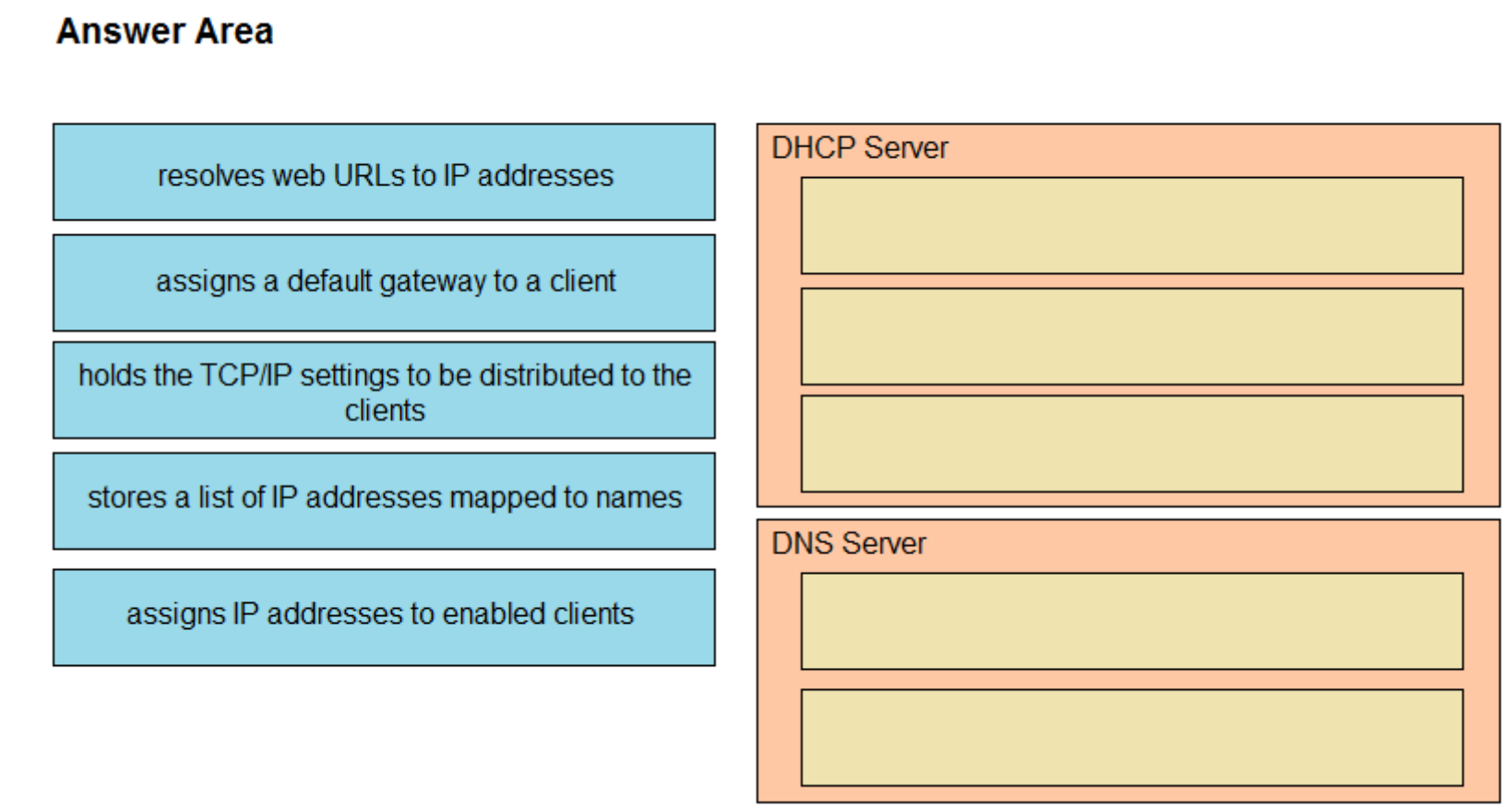
Usually no action is required when a route flaps so it generates the notification syslog level message (level 5).
upvoted 1 times

Question #534 *Topic 1*

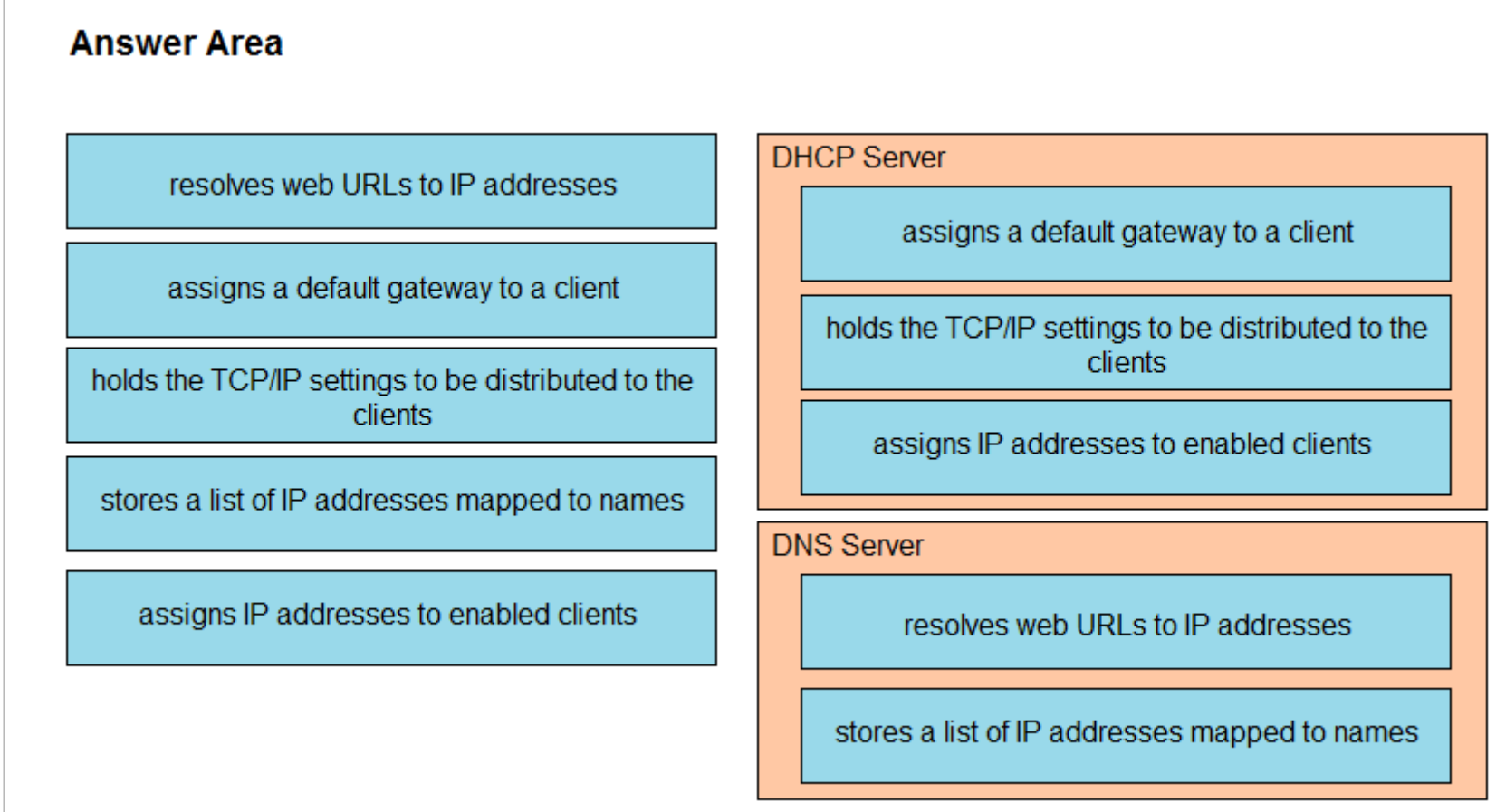
DRAG DROP -

Drag and drop the functions from the left onto the correct network components on the right.

Select and Place:



Correct Answer:



ayd33n Highly Voted 2 years, 10 months ago

DHCP:
Assigns a Default Gateway to a client
Holds TCP/IP Settings to be distributed to the clients
Assigns IP addresses to enabled clients

DNS:
Resolves web URLs to IP addresses
Stores a list of IP addresses mapped to names

upvoted 9 times

martialstriker09 Most Recent 11 months, 2 weeks ago

Answered this pretty easily. Immediately knew that DNS - translates IP addresses to names. didn't even bother thinking about the DHCP options lol

upvoted 2 times

Question #535 *Topic 1*

Which two tasks must be performed to configure NTP to a trusted server in client mode on a single network device? (Choose two.)

A. Enable NTP authentication.

B. Verify the time zone.

C. Specify the IP address of the NTP server.

D. Set the NTP server private key.

E. Disable NTP broadcasts.

Correct Answer: *AC*
To configure authentication, perform this task in privileged mode:
Step 1: Configure an authentication key pair for NTP and specify whether the key will be trusted or untrusted.
Step 2: Set the IP address of the NTP server and the public key.
Step 3: Enable NTP client mode.
Step 4: Enable NTP authentication.
Step 5: Verify the NTP configuration.
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/ntp.html

toto74500 Highly Voted 2 years, 9 months ago
Step 1: Configure an authentication key pair for NTP and specify whether the key will be trusted or untrusted.
Step 2: Set the IP address of the NTP server and the public key.
Step 3: Enable NTP client mode.
Step 4: Enable NTP authentication.
Step 5: Verify the NTP configuration.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/ntp.html
Note: A trusted NTP server may or may not require a secret key so it is not a “must” in this question.

I think answer is more Enable NTP Authentication + Specify the Ip address of the NTP server
upvoted 26 times

Zerotime0 2 years, 5 months ago
Agreed
upvoted 3 times

knister Highly Voted 2 years, 11 months ago
A and C in this case. The key of the question is in "trusted". You need to configure authentication as in here
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/ntp.html#wp1019984
upvoted 6 times

SanchezEldorado 2 years, 11 months ago
The article you referenced is 13 years old and doesn't seem to apply anymore. A and C are correct, but I believe you ALSO need to specify the "Trusted-Key". Is that the same as the "Private key"? If so, then D is also correct. Here's a more up to date configuration link that shows the commands:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swadmin.html#47087
upvoted 3 times

cormorant Most Recent 5 months, 3 weeks ago
AUTHEnication and ip of ntp server. end of story
upvoted 1 times

WINDSON 11 months, 3 weeks ago
Config NTP server IP & config time zone is must. But answer b is verify time zone but not config..... NTP authentication is not a must..... who can provide accurate explanation ?
upvoted 2 times

reagan_donald 1 year, 5 months ago
funny thing is that neither in Wendell Odom, nor on Netacad was mentioned NTP Authentication lol
upvoted 5 times

UnbornD9 1 month, 2 weeks ago
I'm so tired of this f****** questions about something that IS NOT in the OFFICIAL CERT GUIDE...
upvoted 2 times

devildog 2 years, 7 months ago

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/ntp.html#wp1019854

upvoted 1 times

Chipapo 2 years, 10 months ago

I think b and c are more correct. Authentication is not a must

upvoted 6 times

Mountie 2 years, 10 months ago

Time zone should be set before setting NTP server as the clock source. Time Zone is used to identified the offset of summer time that's used in specific areas.

upvoted 3 times

lazy2z 2 years, 11 months ago

The question required to configure client mode, i think NTP server "private key" should not be valid. It should be "public key"
Reference - https://www.cisco.com/en/US/products/hw/switches/ps679/products_configuration_guide_chapter09186a008007d785.html#14543

upvoted 2 times

rjthefool 2 years, 11 months ago

Why wouldn't I enable NTP authentication before setting the NTP server private key

upvoted 2 times

Question #536 *Topic 1*

What is the primary purpose of a First Hop Redundancy Protocol?

A. It allows directly connected neighbors to share configuration information

B. It reduces routing failures by allowing Layer 3 load balancing between OSPF neighbors that have the same link metric

C. It allows a router to use bridge priorities to create multiple loop-free paths to a single destination

D. It reduces routing failures by allowing more than one router to represent itself as the default gateway of a network

Correct Answer: *D*

dicksonpwc Highly Voted 1 year, 9 months ago

D is correct answer.
Explanation:
A first hop redundancy protocol (FHRP) is a computer networking protocol which is designed to protect the default gateway used on a subnetwork by allowing two or more routers to provide backup for that address; in the event of failure of an active router, the backup router will take over.

upvoted 9 times

lmadolfo2019 Highly Voted 2 years, 2 months ago

D is a answer...

upvoted 7 times

DARKK Most Recent 1 year ago

Selected Answer: D

Poor wording but it is D.

upvoted 2 times

Question #537 *Topic 1*

An engineer is configuring NAT to translate the source subnet of 10.10.0.0/24 to any one of three addresses: 192.168.3.1, 192.168.3.2, or 192.168.3.3. Which configuration should be used?

A. enable configure terminal ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30 access-list 1 permit 10.10.0.0 0.0.0.255 ip nat outside destination list 1 pool mypool interface g1/1 ip nat inside interface g1/2 ip nat outside

B. enable configure terminal ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30 access-list 1 permit 10.10.0.0 0.0.0.254 ip nat inside source list 1 pool mypool interface g1/1 ip nat inside interface g1/2 ip nat outside

C. enable configure terminal ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30 route map permit 10.10.0.0 255.255.255.0 ip nat outside destination list 1 pool mypool interface g1/1 ip nat inside interface g1/2 ip nat outside

D. enable configure terminal ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30 access-list 1 permit 10.10.0.0 0.0.0.255 ip nat inside source list 1 pool mypool interface g1/1 ip nat inside interface g1/2 ip nat outside

Correct Answer: *D*

splashy 4 months, 3 weeks ago

Selected Answer: D

D is the least incorrect, but still very not correct lol:

prefix length 30 = 255.255.255.253 = 4-2 hosts = 2 hosts

It actually "works" in PT but you have the broadcast address in your range which is no bueno.

Prefix should be /29

upvoted 4 times

splashy 4 months, 3 weeks ago

255.255.255.253 must be ...252 ... typo

upvoted 2 times

NICE_ANSWERS 2 days, 15 hours ago

Why must the prefix length be 29 to make the configuration fully correct? And why is /30 not advisable?

upvoted 1 times

Request7108 5 months, 1 week ago

I didn't see it at first but B is wrong because the wildcard written ends in .254 which is a valid mask but not a valid wildcard

upvoted 1 times

Goh0503 8 months ago

Answer is D
https://study-ccna.com/dynamic-nat/

upvoted 2 times

Question #538 *Topic 1*

When the active router in an HSRP group fails, which router assumes the role and forwards packets?

A. forwarding

B. listening

C. standby

D. backup

Correct Answer: *C*

Cyberops Highly Voted 1 year ago

Selected Answer: C

HSRP uses Active/stanby
VRRP uses Master/Backup

upvoted 16 times

Raisul Most Recent 1 month ago

When the active router in an HSRP group fails, what router assumes the role and forwards packets?
A. listening
B. backup
C. forwarding
D. standby **

upvoted 1 times

Raisul 1 month ago

Duplicate question.

upvoted 1 times

SamuelSami 8 months, 3 weeks ago

HSRP is a Cisco proprietary protocol. VRRP is an open standard protocol. HSRP is an application layer protocol. VRRP is a network layer protocol. HSRP version 1 uses UDP port number 1985 and multicast address 224.0.
Virtual Router Redundancy Protocol (VRRP) is a network management protocol that is used to increase the availability of default gateway servicing hosts on the same subnet. VRRP improves the reliability and performance of the host network by enabling a virtual router to act as the default gateway for that network.
What is the VRRP protocol used for?
The Virtual Router Redundancy Protocol (VRRP) eliminates the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router (a VPN 3000 Series Concentrator cluster) to one of the VPN Concentrators on a LAN.

upvoted 3 times

Networknovice 1 year ago

HSRP= Hot STANDBY Routing Protocol

upvoted 3 times

Question #539 *Topic 1*

What protocol allows an engineer to back up 20 network router configurations globally while using the copy function?

A. TCP

B. SMTP

C. FTP

D. SNMP

Correct Answer: *D*

klosinskil Highly Voted 2 years, 7 months ago

D
https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/15217-copy-configs-snmp.html
upvoted 10 times

pastele111 2 years, 7 months ago

thanks
upvoted 3 times

Ebenezer Highly Voted 2 years, 8 months ago

The right answer is FTP.
upvoted 6 times

LilGhost_404 Most Recent 1 year, 3 months ago

Selected Answer: D
The real answer is the D, to clarify. It will use SNMP to send a copy command to all the switches, and the copy command will use TFTP to send the config to the TFTP Server.
upvoted 1 times

Technique31 1 year, 6 months ago

Selected Answer: D
D Correct
upvoted 1 times

AlexPlh 1 year, 10 months ago

https://linuxkings.com/2020/02/08/how-to-backup-and-restore-cisco-router-data-with-ftp-server/
upvoted 2 times

IxlJustinlxl 2 years ago

Answer is D

SNMP works in conjunction with TFTP to backup configuration files. This is accomplished by downloading a current copy of your router's configuration file to a TFTP server via SNMP.
upvoted 4 times

Raooff 2 years, 5 months ago

D is good
Generally you can use requests "get" to get information and "set" to make configurations, with any application using SNMP
upvoted 2 times

nj1999 2 years, 8 months ago

Process of elimination on this one too.
TCP, SMTP, and SNMP don't have a 'copy' function only FTP.
SMTP can only GET and SET
upvoted 4 times

sinear 2 years, 4 months ago

You confuse FFTP and SMTP. SMTP is a mail protocol, not a file transfer protocol. TFTP indeed only supports get and set
upvoted 4 times

pastele111 2 years, 8 months ago

its confusing, SNMP takes readings from network devices and communication with MIB but....all data is usually stored as a file, so... maybe answer C) more correct here while use a 'copy' command to FTP server??
upvoted 2 times

Question #540 *Topic 1*

Which type of address is the public IP address of a NAT device?

A. outside global

B. outside local

C. inside global

D. inside local

E. outside public

F. inside public

Correct Answer: *C*

NAT use four types of addresses:

☞ Inside local address - The IP address assigned to a host on the inside network. The address is usually not an IP address assigned by the Internet Network

Information Center (InterNIC) or service provider. This address is likely to be an RFC 1918 private address.

☞ Inside global address - A legitimate IP address assigned by the InterNIC or service provider that represents one or more inside local IP addresses to the outside world.

☞ Outside local address - The IP address of an outside host as it is known to the hosts on the inside network.

☞ Outside global address - The IP address assigned to a host on the outside network. The owner of the host assigns this address.

DaBest Highly Voted 1 year, 8 months ago

c- inside global is the correct answer, the question ask what the address is called after NAT has happened

upvoted 7 times

Customexit Most Recent 8 months, 1 week ago

Inside/Outside = Location of the host
Local/Global = Perspective

upvoted 2 times

Technique31 1 year, 6 months ago

Selected Answer: C

C Correct

upvoted 4 times

Question #541 *Topic 1*

Which two pieces of information can you determine from the output of the show ntp status command? (Choose two.)

A. whether the NTP peer is statically configured

B. the IP address of the peer to which the clock is synchronized

C. the configured NTP servers

D. whether the clock is synchronized

E. the NTP version number of the peer

Correct Answer: *BD*

Below is the output of the ג€show ntp statusג€ command. From this output we learn that R1 has a stratum of 10 and it is getting clock from 10.1.2.1.

```
R1#show ntp status
Clock is synchronized, stratum 10, reference is 10.1.2.1
nominal freq is 250.0000 Hz, actual freq is 249.9987 Hz, precision is 2**18
reference time is D5E492E9.98ACB4CF (13:00:25.596 CST Wed Sep 18 2013)
clock offset is 15.4356 msec, root delay is 52.17 msec
root dispersion is 67.61 msec, peer dispersion is 28.12 msec
```

GangsterDady Highly Voted 1 year, 7 months ago

show ntp associations
for configured server

upvoted 6 times

Hodicek Most Recent 1 year, 6 months ago

NTP=CLOCK

upvoted 4 times

Question #542 *Topic 1*

Which keyword in a NAT configuration enables the use of one outside IP address for multiple inside hosts?

A. source

B. static

C. pool

D. overload

Correct Answer: *D*

By adding the keyword ג€overloadג€ at the end of a NAT statement, NAT becomes PAT (Port Address Translation). This is also a kind of dynamic NAT that maps multiple private IP addresses to a single public IP address (many-to-one) by using different ports. Static NAT and Dynamic NAT both require a one-to-one mapping from the inside local to the inside global address. By using PAT, you can have thousands of users connect to the Internet using only one real global IP address. PAT is the technology that helps us not run out of public IP address on the Internet. This is the most popular type of NAT.

An example of using ג€overloadג€ keyword is shown below:

R1(config)# ip nat inside source list 1 interface ethernet1 overload

kaus33k Highly Voted 1 year, 7 months ago

Overload is the answer that enables the PAT.

upvoted 8 times

Question #543 *Topic 1*

Which feature or protocol determines whether the QOS on the network is sufficient to support IP services?

A. LLDP

B. CDP

C. IP SLA

D. EEM

Correct Answer: *C*
IP SLA allows an IT professional to collect information about network performance in real time. Therefore it helps determine whether the QoS on the network is sufficient for IP services or not.
Cisco IOS Embedded Event Manager (EEM) is a powerful and flexible subsystem that provides real-time network event detection and onboard automation. It gives you the ability to adapt the behavior of your network devices to align with your business needs.

aaaaaaaaakkk 11 months, 1 week ago
just tell what is the ccna real exam is it ccnp or harder
upvoted 3 times

Mozah 1 year, 4 months ago
Yes, correct answer is C
upvoted 4 times

Question #544 *Topic 1*

In QoS, which prioritization method is appropriate for interactive voice and video?

A. traffic policing

B. round-robin scheduling

C. low-latency queuing

D. expedited forwarding

Correct Answer: *C*
Low Latency Queuing (LLQ) is the preferred queuing policy for VoIP audio. Given the stringent delay/jitter sensitive requirements of voice and video and the need to synchronize audio and video for CUVA, priority (LLQ) queuing is the recommended for all video traffic as well. Note that, for video, priority bandwidth is generally fudged up by 20% to account for the overhead.

luciomagi Highly Voted 2 years, 4 months ago
answer should be LLQ Low Latency Queueing
upvoted 25 times

lucky1559 Highly Voted 1 year, 9 months ago
Some questions are tricky. They ask for prioritization method not queueing method, thus it leaves us with round-robin and expedited-forwarding.

So correct answer is expedited forwarding.
upvoted 11 times

Jackie_Manuas12 1 year, 2 months ago
<They ask for prioritization method not queueing method>

Huh?
Please see -> Prioritization methods collectively can be called "queuing methods," "output queuing," or "fancy queuing."
https://www.ccexpert.us/traffic-shaping-3/choosing-a-traffic-prioritization-method.html
upvoted 4 times

Ciscoman021 Most Recent 2 months, 1 week ago
Selected Answer: C
Low-latency queuing (LLQ) is a congestion management technique that provides strict priority queuing for voice and video traffic, allowing these applications to be processed with minimal delay and jitter. LLQ is designed to ensure that voice and video traffic is sent through the network as quickly as possible, while still allowing other types of traffic to be transmitted when there is available bandwidth.
upvoted 1 times

oatmealturkey 3 months, 1 week ago
Selected Answer: C
I generally go by the OCG and it makes clear that LLQ is for prioritization--see page 243 of Vol. 2
upvoted 1 times

doomboticon 10 months ago
9tut.com shows the correct answer as Low Latency Queueing
upvoted 1 times

DARKK 1 year ago
Selected Answer: C
C is certainly correct here.
upvoted 2 times

Jeanromeo1 1 year ago
Selected Answer: C
Queuing
Low Latency Queuing (LLQ) is the preferred queuing policy for VoIP audio. Given the stringent delay/jitter sensitive requirements of TP and the need to synchronize audio and video for CUVA, priority (LLQ) queuing is the recommended for all video traffic as well. Note that, for video, priority bandwidth is generally fudged up by 20% to account for the overhead.
upvoted 2 times

msomali 1 year, 1 month ago
correct answer is LOWER-LATENCY QUEUEING.
upvoted 2 times

bodybod 1 year, 2 months ago

Selected Answer: C

easy easy easy

upvoted 1 times

gachocop3 1 year, 2 months ago

the right answer is C

upvoted 1 times

juani85 1 year, 2 months ago

Selected Answer: C

so good answer

upvoted 1 times

Nagib 1 year, 3 months ago

answer should be c. low latency queueing

upvoted 1 times

Cisna 1 year, 8 months ago

Right answer is C

upvoted 1 times

bootloader_jack 1 year, 8 months ago

what do you mean by "prioritization method" ? be clear cisco.

upvoted 2 times

zaguy 1 year, 9 months ago

In most cases, one Low Latency class is sufficient for all bounded delay traffic. In some cases, it might be necessary to define more than one Low Latency class. For this reason, Low Latency classes are assigned one out of five priority levels (not including the Expedited Forwarding class, see Low Latency versus DiffServ).
Low Latency versus DiffServ
Low Latency classes are different from DiffServ classes in that they do not receive type of service (TOS) markings. Not all packets are marked as Low Latency. Preferential treatment is guaranteed only while the packets are passing through the QoS gateway.

The exception to this rule is the Expedited Forwarding DiffServ class. A DiffServ class defined as an Expedited Forwarding class automatically becomes a Low Latency class of highest priority. Such a class receives the conditions afforded it by its DiffServ marking both in QoS and on the network.
https://sc1.checkpoint.com/documents/R77.10/CP_R77.10_QoS_WebAdminGuide/14869.htm#o15056

upvoted 1 times

dicksonpwc 1 year, 9 months ago

I think the correct answer should be C.
Explanation:
Low Latency Queuing
LLQ adds strict priority to the CBWFQ and allows delay sensitive data (Voice and Video) to be dequeued and sent before lower priority packets. This practice gives delay sensitive data preferential treatment over other traffic. To direct traffic to the LLQ, use the priority command for the class after the named class within a policy map is specified. Any class of traffic can be attached to a service policy, which uses priority scheduling, and that traffic can be prioritized over other class traffic.

upvoted 1 times

Dataset 1 year, 12 months ago

I thought it was C...

upvoted 2 times

Question #545 *Topic 1*

DRAG DROP -

Drag and drop the SNMP components from the left onto the descriptions on the right.

Select and Place:

Answer Area

MIB	collection of variables that can be monitored
SNMP agent	unsolicited message
SNMP manager	responds to status requests and requests for information about a device
SNMP trap	resides on an NMS

Correct Answer:

Answer Area

MIB	MIB
SNMP agent	SNMP trap
SNMP manager	SNMP agent
SNMP trap	SNMP manager

[Removed] 1 month ago

Book for online proctor exam and we'll remotely take the exam for you. Pay us after confirmation of PASSED results
ITTCA.org

WhatsApp +1(409)223 7790

upvoted 2 times

zombi1101 1 month ago

MIB - collection of variables that can be monitored
SNMP Agent - responds to status requests and requests for information about a device
SNMP Manager - resides on an NMS
SNMP Trap - unsolicited message

upvoted 2 times

Question #546 *Topic 1*

What is the purpose of traffic shaping?

A. to be a marking mechanism that identifies different flows

B. to provide fair queuing for buffered flows

C. to mitigate delays over slow links

D. to limit the bandwidth that a flow can use

Correct Answer: *D*
The primary reasons you would use traffic shaping are to control access to available bandwidth, to ensure that traffic conforms to the policies established for it, and to regulate the flow of traffic in order to avoid congestion that can occur when the sent traffic exceeds the access speed of its remote, target interface.

luciomagi Highly Voted 2 years, 4 months ago
answer should be
B. to provide fair queuing for buffered flows
traffic shaping is not necessarily doing limitation of bandwidth
upvoted 14 times

ZayaB Highly Voted 2 years, 3 months ago
Answer D seems correct. Explanation: Traffic shaping is a bandwidth control technique. It is used on computer networks and delays some or all datagrams. Traffic shaping is created to comply with a specified traffic profile. Traffic shaping maximizes or guarantees performance, boosts latency. It can also increase available bandwidth for certain kinds of packets. Application-based traffic shaping is the most common form of traffic shaping.
upvoted 7 times

Shun5566 Most Recent 5 days, 17 hours ago
Selected Answer: B
I think is B
upvoted 1 times

Anas_Ahmad 5 months, 2 weeks ago
Selected Answer: B
Traffic shaping retains excess packets in a queue and then schedules the excess for later
transmission over increments of time
upvoted 2 times

DixieNormus 9 months ago
From the link that two people have posted even though they believe the answer is B:
Using traffic shaping, you can control access to available bandwidth, ensure that traffic conforms to the policies established for it, and regulate the flow of traffic in order to avoid congestion that can occur when the egress traffic exceeds the access speed of its remote, target interface. For example, you can control access to the bandwidth when policy dictates that the rate of a given interface should not, on average, exceed a certain rate
even though the access rate exceeds the speed.
From this I am gathering that the answer is D.
Also note that "fair queuing" is not the same as "queuing", just because you see the word queue does not mean that it is "fair queuing".
upvoted 2 times

NICE_ANSWERS 2 days, 14 hours ago
It says fair queuing over there tho
upvoted 1 times

SOAPGUY 1 year ago
Selected Answer: D
D IS THE PURPOSE, B IS THE METHOD.
upvoted 5 times

Smaritz 1 year, 2 months ago
Seems to me it should be B
upvoted 1 times

siki1984 1 year, 2 months ago
B is correct answer

Traffic shapingregulatesandsmoothsoutthepacketflowby imposinga maximumtraffic rateforeachport'segressqueue.Packetsthatexceedthethresholdareplacedin thequeueandaretransmittedlater. Thisprocessis similarto traffic policing;however, thepacketsarenotdropped.Becausepacketsarebuffered,trafficshapingminimizespacketloss(basedon

thequeuelength),whichprovidesa bettertraffic behaviorforTCPtraffic

chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/qos/7x/b_3k_QoS_Config_7x/b_3k_QoS_Config_7x_chapter_0100.pdf

upvoted 1 times

ismatdmour 1 year, 2 months ago

Selected Answer: D

Ans. is D: "to limit the bandwidth that a flow can use". Shaping is applied to flows that receive preferential treatment using LLQ. However, LLQs may result in flows which utilizes more BW than the committed BW over the link (e.g. to ISP). At the other side (ISP) packets can be dropped due to exceeding BW limits (Policing). Hence, to avoid packets dropping by policers at the other end we limit BW from the exit side (Shaping). Of course, shaping results in other less prioritised flows getting higher BW, so some tend to choose B. However, this is not the intention of Shaping as we could have applied fair queuing from the beginning.

upvoted 1 times

Ay10 1 year, 3 months ago

Traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time. So B

upvoted 1 times

Dante_Dan 1 year, 4 months ago

Selected Answer: D

From Offical Cert Guide Book #2

(Imagine this scenario) You have a 1 Gbps link from a router into a Service Provider, but a 200 Mbps CIR for traffic to another site. The Service Provider has told you that it always discards incoming traffic that exceeds the CIR. The solution? Use a shaper to slow down the traffic, in this case to a 200 Mbps shaping rate.
That scenario, shaping before sending data to a Service Provider that is policing, is one of the typical uses of a shaper...".

upvoted 2 times

gaber 1 year, 5 months ago

looks like bandwidth limiting is just a tool of traffic shaping according to cisco:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/qos/7x/b_3k_QoS_Config_7x/b_3k_QoS_Config_7x_chapter_0100.pdf

plus answer d is just too negative, answer is b

upvoted 1 times

Lala4eva 1 year, 6 months ago

According to F5.com Traffic shaping enables organizations to increase network performance by controlling the amount of data that flows into and out of the network. Therefore making D the correct answer. Please check out my source. https://www.f5.com/services/resources/glossary/traffic-shaping

upvoted 3 times

UmbertoReed 1 year, 8 months ago

Originally I thought it was B, but I have never read a resource that describes shaping as a "fair queuing" tool, at least at the CCNA level.

This articule from Cisco seems to confirm that D is correct: https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html

"This document clarifies the functional differences between shaping and policing, both of which limit the output rate."

upvoted 3 times

kadamske 1 year, 8 months ago

According to the cisco documentation from the link you provided, B should be the correct answer because it is mentioned that it buffers the flows and nothing like bandwidth was mentioned

upvoted 1 times

MarcoT95 1 year, 8 months ago

The primary reasons you would use traffic shaping are to control access to available bandwidth, to ensure that traffic conforms to the policies established for it, and to regulate the flow of traffic in order to avoid congestion that can occur when the sent traffic exceeds the access speed of its remote, target interface.

D is correct

upvoted 4 times

DonnerKomet 1 year, 9 months ago

I think D is correct, cause B is more related to QUEUEING.

upvoted 4 times

dicksonpwc 1 year, 9 months ago

i think the B is the correct

Traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time.

upvoted 3 times

Question #547 *Topic 1*

What is a function of TFTP in network operations?

A. transfers IOS images from a server to a router for firmware upgrades

B. transfers a backup configuration file from a server to a switch using a username and password

C. transfers configuration files from a server to a router on a congested link

D. transfers files between file systems on a router

Correct Answer: *A*

dontone_ma_piu_pelato Highly Voted 2 years, 1 month ago

A is the correct, pelati

upvoted 11 times

Ciscoman021 Most Recent 2 months, 2 weeks ago

Selected Answer: A

TFTP (Trivial File Transfer Protocol) is a simple file transfer protocol that is often used for transferring small files between network devices. One of the primary functions of TFTP in network operations is to transfer IOS (Internetwork Operating System) images from a TFTP server to a router for firmware upgrades. Therefore, option A is the correct answer.

upvoted 1 times

cormorant 7 months ago

always associate TFTP with ISO images and firmware upgrades

upvoted 2 times

sakisg 11 months ago

Selected Answer: A

a is correct

upvoted 1 times

Sajomon 1 year ago

Selected Answer: A

Trivial File Transfer Protocol (TFTP) is a network protocol used to transfer files between hosts in a TCP/IP network.

upvoted 1 times

ismatdmour 1 year, 2 months ago

Selected Answer: A

D is incorrect as no need for TFTP internally (IOS handles that, I believe, using commands such as "copy"). TFTP can be used to transfer conf. files but the statement is incorrect because TFTP needs no user./pass. authentication. Using TFTP (UDP based) over a congested link means that files cannot be transferred reliably (C incorrect). Finally, A is correct and is the reason TFTP is mostly used (Firmware upgrade) whereby the admin have the IOS image on one device and uses TFTP to load the image to all other devices quickly.

upvoted 3 times

reagan_donald 1 year, 4 months ago

Selected Answer: A

Router OS does not need TFTP inside its own operating system to transfer files between file systems....A is correct

upvoted 4 times

awashenko 1 year, 4 months ago

Selected Answer: D

I like A and D here but I think D is the more correct answer in terms of the CCNA.

upvoted 1 times

babaKazoo 1 year, 4 months ago

A. is wrong because TFTP can transfer things like configuration files but not firmware updates.

D. Is correct.

upvoted 1 times

aike92 1 year, 4 months ago

A is correct.

Your logic is justifiable, but TFTP is not secure like FTP so for security purposes we use it for Trivial things, sorta like Telnet
So for the means of "Network operations" it wouldn't be used for transferring all types or just any types of files

upvoted 1 times

Nebulise 1 year, 4 months ago

Wrong. The main reason i use TFTP on routers/switches at work is to copy IOS files to upgrade the switch/router.

upvoted 5 times

Cho1571 1 year, 4 months ago

Selected Answer: A

I like A better

upvoted 1 times

Rockrl 1 year, 5 months ago

Selected Answer: A

The correct answer is A

upvoted 2 times

shakyak 1 year, 6 months ago

Selected Answer: A

A is the answer

upvoted 2 times

Shamwedge 1 year, 6 months ago

I think it's D. It says "network operations" and to me, that implies a more generalized function that exists outside of the Router/Switch environment. In a basic "network operation," you would use TFTP to transfer files.

upvoted 3 times

Hodicek 1 year, 6 months ago

a is correct

upvoted 1 times

Bibby 1 year, 6 months ago

TFTP requires a TFTP client and a TFTP server. It can be used to transfer files, but routers cannot be configured as fully functional TFTP servers.

upvoted 2 times

Alibaba 1 year, 6 months ago

please change admin true option here A not D

upvoted 1 times

oflu61 1 year, 6 months ago

its D bcs u can also send different files in tftp

upvoted 1 times

Question #548 *Topic 1*

What is a DHCP client?

A. a workstation that requests a domain name associated with its IP address

B. a host that is configured to request an IP address automatically

C. a server that dynamically assigns IP addresses to hosts.

D. a router that statically assigns IP addresses to hosts.

Correct Answer: *B*

Armoonbear Highly Voted 1 year, 4 months ago

Selected Answer: B

Keyword is DHCP "CLIENT".

The "CLIENT" (Meaning a computer or device on the network) requests IP address information from the DHCP "SERVER"

upvoted 9 times

Ciscoman021 Most Recent 2 months, 2 weeks ago

Selected Answer: B

B. A DHCP client is a host, such as a computer or network device, that is configured to obtain an IP address automatically from a DHCP (Dynamic Host Configuration Protocol) server. When a DHCP client is connected to a network, it sends a broadcast request for an IP address to the DHCP server. The DHCP server then assigns an available IP address to the client and also provides other configuration information such as the subnet mask, default gateway, and DNS server addresses. This allows the client to communicate on the network without requiring manual IP address configuration.

upvoted 2 times

Dutch012 3 months, 1 week ago

A is a DNS client.
B is a DHCP client

upvoted 1 times

Question #549 *Topic 1*

Where does the configuration reside when a helper address is configured lo support DHCP?

A. on the router closest to the server

B. on the router closest to the client

C. on every router along the path

D. on the switch trunk interface

Correct Answer: *B*

shakyak Highly Voted 1 year, 6 months ago
It's a helper so closest to the client.
upvoted 5 times

Etidic Most Recent 7 months, 2 weeks ago
Selected Answer: B
The answer is B
upvoted 1 times

gaber 1 year, 5 months ago
a router, being a device that communicates with other networks, the client-being the source generating the request, and the server being the dhcp server on the destination lan. the router with the helper-address configured(which is on the local network) will turn the broadcast traffic into unicast traffic, after which any device it hits will see it as unicast, not needing any further configuration.

thus, we're looking at B

https://networkengineering.stackexchange.com/questions/41376/how-ip-helper-address-works

https://community.cisco.com/t5/routing/forwarding-udp-broadcast-traffic/td-p/595108

https://community.cisco.com/t5/switching/broadcast-traffic-on-router/td-p/751300
upvoted 3 times

bwg 2 years ago
Can someone explain it?
upvoted 2 times

Sten111 1 year, 11 months ago
This explains it pretty well
https://www.ciscopress.com/articles/article.asp?p=330807&seqNum=9
upvoted 3 times

dave1992 1 year, 7 months ago
I can explain,
By default routers don't forward broadcast traffic so the ip helper config will need to be applied on every interface towards the client. This means if you have 2 routers between a DHCP server and a client, the helper config will need to be on BOTH routers. C is actually the correct answer, B works for 1 scenario, C works for all scenarios
upvoted 9 times

Etidic 7 months, 2 weeks ago
B is the correct answer in all scenarios.
You only need to configure ip helper address on the closet router to the client.
Then you would need to make sure that an ip route exists between the dhcp server and that router that is acting as a dhcp helper
upvoted 1 times

FALARASTA 1 month ago
There is no need to configure two routers along the way as dhcp helpers because the one closest to the client chnages the broadcast to a unicast request automatically
upvoted 2 times

Question #550 *Topic 1*

What facilitates a Telnet connection between devices by entering the device name?

A. SNMP

B. DNS lookup

C. syslog

D. NTP

Correct Answer: *B*

Question #551 *Topic 1*

When deploying syslog, which severity level logs informational messages?

A. 0

B. 2

C. 4

D. 6

Correct Answer: *D*
Reference:
https://en.wikipedia.org/wiki/Syslog

Suleee Highly Voted 1 year, 9 months ago
Way to remember: Emma Always Crying Even When Nobody Is Dying
upvoted 19 times

Renelis Highly Voted 1 year, 11 months ago
severity-level

Number of the desired severity level at which messages should be logged. Messages at or numerically lower than the specified level are logged. Severity levels are as follows:

0 —emergency: System unusable
1 —alert: Immediate action needed
2 —critical: Critical condition—default level
3 —error: Error condition
4 —warning: Warning condition
5 —notification: Normal but significant condition
6 —informational: Informational message only
7 —debugging: Appears during debugging only
upvoted 12 times

joanb2s Most Recent 5 months, 1 week ago
total freaking :-D
upvoted 1 times

hojusigol 1 year, 3 months ago
Every means Emergency

Awesome means Alert

Cisco means Critical

Engineer means Error

Will means Warning

Need Notice (Notification)

Ice-Cream means Informational

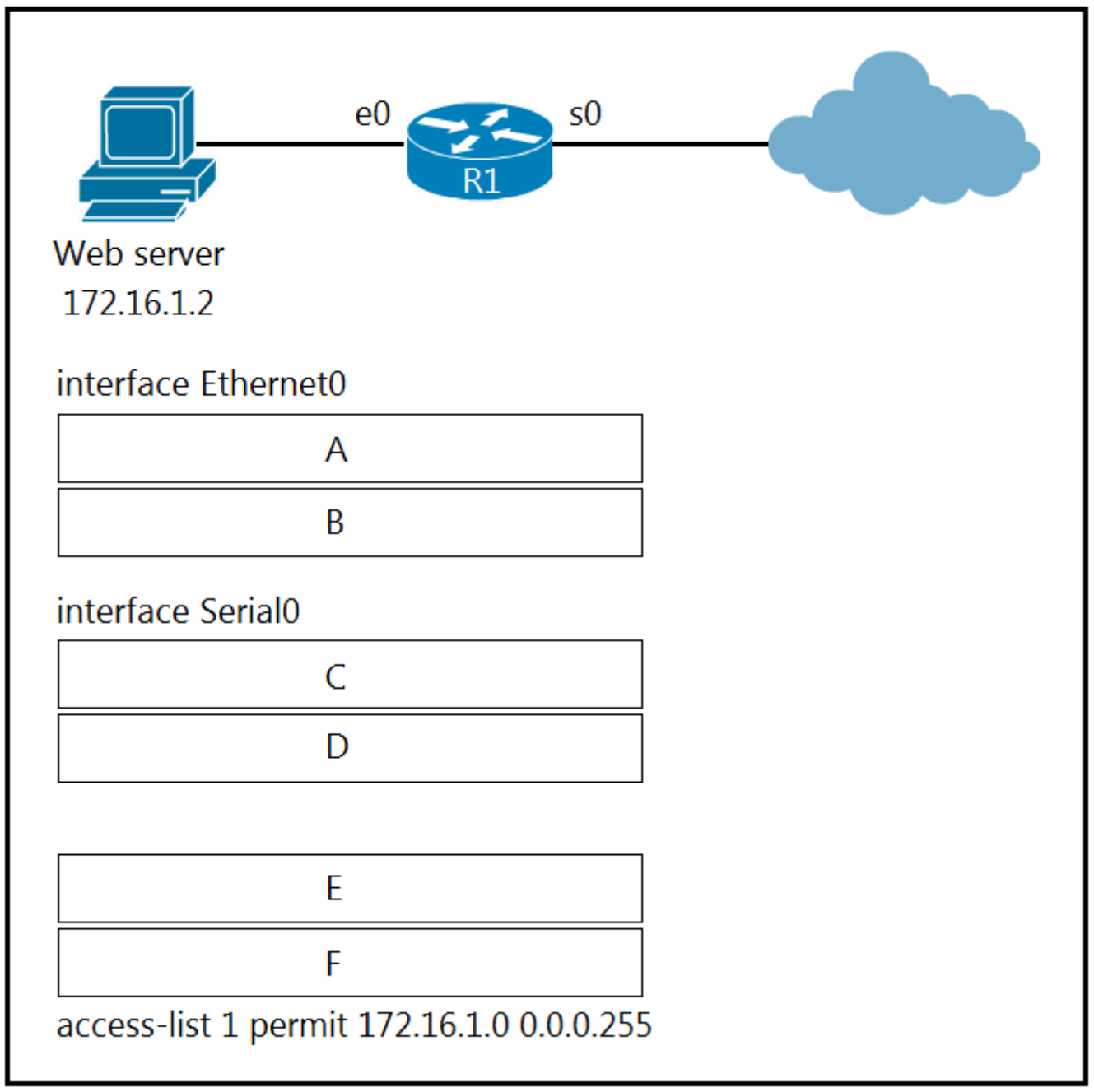
Daily Debugging
upvoted 5 times

rgg 1 year, 7 months ago
Another way to remember: every awesome Cisco engineer will need icecream daily
upvoted 5 times

joanb2s 5 months, 1 week ago
total freaking
upvoted 1 times

Question #552 *Topic 1*

DRAG DROP -



Refer to the exhibit. An engineer is configuring the router to provide static NAT for the webserver. Drag and drop the configuration commands from the left onto the letters that correspond to its position in the configuration on the fight.

Select and Place:

ip address 172.16.1.1 255.255.255.0	position A
ip address 45.83.2.214 255.255.255.240	position B
ip nat inside	position C
ip nat inside source list 1 interface s0 overload	position D
ip nat inside source static tcp 172.16.1.2 80 45.83.2.214 80 extendable	position E
ip nat outside	position F

Correct Answer:

ip address 172.16.1.1 255.255.255.0	ip address 172.16.1.1 255.255.255.0
ip address 45.83.2.214 255.255.255.240	ip nat inside
ip nat inside	ip address 45.83.2.214 255.255.255.240
ip nat inside source list 1 interface s0 overload	ip nat outside
ip nat inside source static tcp 172.16.1.2 80 45.83.2.214 80 extendable	ip nat inside source static tcp 172.16.1.2 80 45.83.2.214 80 extendable
ip nat outside	ip nat inside source list 1 interface s0 overload

DonnerKomet Highly Voted 1 year, 9 months ago
Why PAT? The question asks for a static nat operation, WHY PAT?
upvoted 8 times

Shamwedge Highly Voted 1 year, 6 months ago
I hate these type of questions. You don't always have to do things in these exact orders....
upvoted 7 times

Dante_Dan 1 year, 5 months ago
In this particular case, you do have to do it in order.
upvoted 1 times

Danu22 1 year, 1 month ago
What source do you have for this claim? Because I also don't believe that the order particularly matters here.
upvoted 1 times

iGlitch Most Recent 1 year, 1 month ago
The last two lines, you don't have to place them in this order this is a BS question.
upvoted 2 times

Netclick 1 year, 10 months ago
It binds the inside local address and local port to the specified inside global address and global port.
upvoted 3 times

Orkhann 1 year, 11 months ago
what "ip nat inside source static tcp ..." command do? Any explanation please?
upvoted 3 times

CiscoTerminator 1 year, 10 months ago
it statically maps the inside LAN IP of the server to the outside Public IP and port that people can access over the Internet
upvoted 7 times

Question #553 *Topic 1*

Which two QoS tools provide congestion management? (Choose two.)

A. CBWFQ

B. FRTS

C. CAR

D. PBR

E. PQ

Correct Answer: *AE*

BooleanPizza Highly Voted 1 year, 9 months ago
Q at the end = qeueing protocol = congestion management
upvoted 38 times

Isuzu 16 hours, 58 minutes ago
Nice Hint
upvoted 1 times

Smaritz 1 year, 3 months ago
It seems that sometimes it is just that simple, and that some previous questions have made us look for something more complex LOL
upvoted 2 times

Stonetales987 1 year, 6 months ago
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conmgt/configuration/xe-3s/qos-conmgt-xe-3s-book/qos-conmgt-oview.html
upvoted 1 times

nebolala1 Highly Voted 1 year, 7 months ago
what the f**** is that mean???
upvoted 14 times

LOST40 1 year, 3 months ago
PQ-Priority queues
upvoted 2 times

raydel92 Most Recent 1 year, 6 months ago
Selected Answer: AE
Common Cisco IOS-based congestion management tools include CBWFQ and LLQ algorithms. LLQ brings strict priority queuing (PQ) to CBWFQ.
Source: CCNAv7: Enterprise Networking, Security, and Automation, chapter 9
upvoted 3 times

dave1992 1 year, 7 months ago
Class based weighted fair queueing and PQ?
upvoted 2 times

Question #554 *Topic 1*

Which QoS tool is used to optimize voice traffic on a network that is primarily intended for data traffic?

A. WRED

B. FIFO

C. WFQ

D. PQ

Correct Answer: *D*

zaguy Highly Voted 1 year, 9 months ago

Given Answer : PQ

Deciding Which Queueing Policy to Use

•PQ guarantees strict priority in that it ensures that one type of traffic will be sent, possibly at the expense of all others.
Strict PQ allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues are dequeued.

https://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/12_2sr/qos_12_2sr_book/congstion_mgmt_oview.html

upvoted 5 times

gaber Highly Voted 1 year, 5 months ago

"Many popular QoS techniques that serve data traffic very well, such as WFQ and RED, are ineffective for voice applications."

"FIFO (first-in, first-out). FIFO entails no concept of priority or classes of traffic. With FIFO, transmission of packets out the interface occurs in the order the packets arrive"

thus D

https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html

https://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/12_2sr/qos_12_2sr_book/congstion_mgmt_oview.html

enjoy

upvoted 5 times

dave1992 Most Recent 1 year, 7 months ago

Anyone studying the book that can point PQ out in book 2?

upvoted 1 times

appleness123 1 year, 8 months ago

PQ almost always refers to voice as per https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01110.html

upvoted 2 times

Gandzasar 1 year, 9 months ago

Yes, correct

upvoted 2 times

StingVN 2 weeks, 5 days ago

idk but everybody say this is correct then i'm also think it should be correct. lol

upvoted 1 times

BooleanPizza 1 year, 9 months ago

Explanation?

upvoted 1 times

aosroyal 1 year, 2 months ago

yes, correct

upvoted 4 times

Rothus 1 year, 1 month ago

Yes, correct

upvoted 3 times

coolapple 1 year ago

Yes, definitely correct

upvoted 3 times

Dutch012 2 months, 4 weeks ago

Yes, correct

upvoted 1 times

Question #555 *Topic 1*

An engineer is installing a new wireless printer with a static IP address on the Wi-Fi network. Which feature must be enabled and configured to prevent connection issues with the printer?

A. client exclusion

B. DHCP address assignment

C. passive client

D. static IP tunneling

Correct Answer: *C*
Passive clients are wireless devices, such as scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information when they associate with an access point. As a result, when passive clients are used, the controller never knows the IP address unless they use the DHCP.
Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/m_configuring_passive_clients.html

raydel92 Highly Voted 1 year, 6 months ago

Selected Answer: C
Passive clients are wireless devices, such as scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information when they associate with an access point. As a result, when passive clients are used, the controller never knows the IP address unless they use the DHCP.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/m_configuring_passive_clients.html
upvoted 13 times

gaber 1 year, 5 months ago
yes, dhcp address assignment is just dhcp assigning addresses.
C is best here imo
upvoted 1 times

shakyak 1 year, 6 months ago
This is the correct answer
upvoted 1 times

firstblood Highly Voted 1 year, 9 months ago
A is correct. Static IP should be excluded from the DHCP pool.
upvoted 7 times

Request7108 5 months, 1 week ago
Client exclusion on a WLC is the timeout forced on a client with repeated failures. While you are correct about needing to prevent the static IP from being used in the pool, this question is not about that
upvoted 1 times

hker 1 year, 9 months ago
Most of the wireless LAN infrastructure provide DHCP and prohibit connections from clients with static IP. So excluding the IP address of the printer may not help, as the network will refuse the Wi-Fi association from the printer with static IP.
upvoted 2 times

shiv3003 Most Recent 1 month, 1 week ago
B for me
upvoted 1 times

couragek 4 months ago
COULOOKPS
C
upvoted 1 times

Ciscoman021 4 months, 1 week ago

Selected Answer: C
Passive clients are wireless devices, such as scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information when they associate with an access point. As a result, when passive clients are used, the controller never knows the IP address unless they use the DHCP.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-6/configuration-guide/b_cg76/b_cg76_chapter_01100000.html

upvoted 1 times

Request7108 5 months, 1 week ago

Selected Answer: C

Correct answer is C and here is a short explanation of why:
A) Client exclusion is a timeout forced on devices that repeatedly fail to connect
B) There is an option to force DHCP address assignment for devices on a WLAN but this would prevent the device with a static IP from connecting
C) Passive client enabled for devices that are quiet like those with static IPs
D) Static IP tunneling is for passing a device with a static address over a mobility tunnel to another WLC that does not have the device's subnet in its interface ranges or groups.

upvoted 1 times

AWSEMA 10 months, 1 week ago

Selected Answer: C

google is ur friend hhhh btw "C" is the correct answer

upvoted 1 times

Sajomon 1 year ago

Selected Answer: B

Passive clients are wireless devices, such as scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information when they associate with an access point. As a result, when passive clients are used, the controller never knows the IP address unless they use the DHCP.

upvoted 1 times

chalaka 1 year, 1 month ago

B (DHCP address assignment) is correct because DHCP Address Allocation Mechanism (or assignment) is the mechanism (Manual Allocation) we're going to use to Provide an IP address to a client manually.

upvoted 1 times

awashenko 1 year, 4 months ago

Selected Answer: C

I also think the answer is C. The questions states that the printer is being assigned an address statically so why would we need to have DHCP address assignment?

upvoted 2 times

Cho1571 1 year, 4 months ago

Selected Answer: B

Isn't a DHCP reservation a 'DHCP address assignment'

It is a poor wording but the same thing

upvoted 1 times

DARKK 1 year ago

A static IP is NOT the same as a DHCP Reservation. C seems better here.

upvoted 2 times

pjvillareal 1 year, 5 months ago

Can anyone explain to me why letter C is not the correct answer here? It should be C, passive client feature, based on this Cisco link:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/m_configuring_passive_clients.html

DHCP address assignment is just the DHCP DORA process, not DHCP exclude feature. Client exclusion is yet another feature not related to DHCP excluding feature.

upvoted 1 times

pjvillareal 1 year, 5 months ago

I meant DHCP reservation on the last paragraph, not exluding..

upvoted 1 times

Shamwedge 1 year, 6 months ago

DHCP address assignment must be there way of saying DHCP reservation

upvoted 1 times

yasuke 1 year, 8 months ago

For enhanced security, we recommend that you require all clients to obtain their IP addresses from a DHCP server. To enforce this requirement, you can configure all WLANs with a DHCP Addr. Assignment Required setting, which disallows client static IP addresses. If DHCP Addr. Assignment Required is selected, clients must obtain an IP address via DHCP. Any client with a static IP address is not allowed on the network. The controller monitors DHCP traffic because it acts as a DHCP proxy for the clients.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01001001.html

upvoted 3 times

zaguy 1 year, 9 months ago

DHCP Reservation should be an option here, but it isnt provided. Similar questions mention excluded addresses, particularly with reference to the subnet gateway. Badly worded, so in context of the options provided "client exclusion" seems to be the best choice.

upvoted 4 times

hker 1 year, 9 months ago

I agree with the answer provided: B. DHCP address assignment

upvoted 2 times

CiscoTerminator 1 year, 9 months ago

and why would one enable "DHCP Address Assignment" when question is saying a static IP is being configured - answer definitely wrong.

upvoted 4 times

hker 1 year, 9 months ago

DHCP Address Assignment will assign a specific IP address to the DHCP clients with a specific MAC. e.g. always assign the IP address 192.168.111.222 for the client with MAC address 00:DD:11:BB:22:CC, when the request comes from 192.168.111.0/24. It's a feature of a DHCP server.

upvoted 4 times

Question #556 *Topic 1*

When a client and server are not on the same physical network, which device is used to forward requests and replies between client and server for DHCP?

A. DHCPOFFER

B. DHCP relay agent

C. DHCP server

D. DHCPDISCOVER

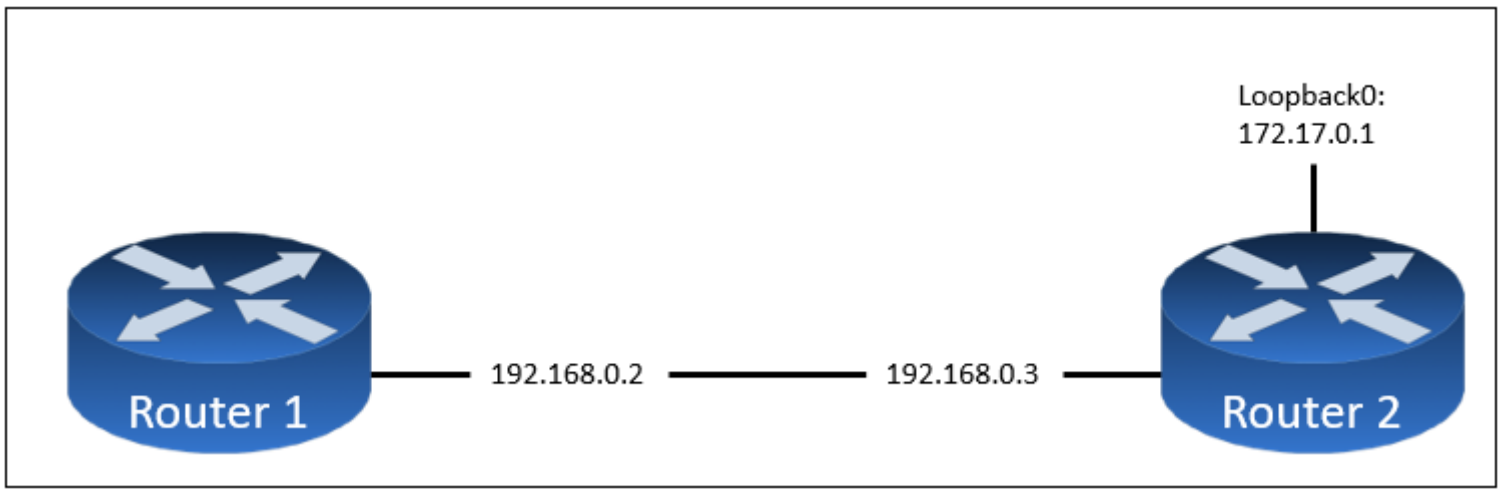
Correct Answer: *B*

Stonetales987 Highly Voted 1 year, 6 months ago

B is correct. A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/dhcp-relay-agent.html#GUID-9E110360-34EA-40BB-9314-2AFABD7F2FDA

upvoted 7 times

Question #557 *Topic 1*



Refer to the exhibit. The ntp server 192.168.0.3 command has been configured on router 1 to make it an NTP client of router 2. Which command must be configured on router 2 so that it operates in server-only mode and relies only on its internal clock?

A. Router2(config)#ntp server 172.17.0.1

B. Router2(config)#ntp server 192.168.0.2

C. Router2(config)#ntp passive

D. Router2(config)#ntp master 4

Correct Answer: *D*

dave1992 Highly Voted 1 year, 7 months ago

■ ntp master {stratum-level}: NTP server mode—the device acts only as an NTP server, and not as an NTP client. The device gets its time information from the internal clock on the device.
■ ntp server {address | hostname}: NTP client/server mode—the device acts as both client and server. First, it acts as an NTP client, to synchronize time with a server. Once syn- chronized, the device can then act as an NTP server, to supply time to other NTP clients.

upvoted 9 times

Priyamano Most Recent 11 months, 1 week ago

D is ok

upvoted 1 times

Hodicek 1 year, 6 months ago

i server is client , so 2nd should to be master

upvoted 1 times

DaBest 1 year, 8 months ago

I think D is correct (ntp master 4) but whats the 4 means?

upvoted 4 times

dave1992 1 year, 7 months ago

The lower the stratum level, the more accurate the reference clock is considered to be. An NTP server that uses its internal hardware or external reference clock sets its own stratum level. Then, an NTP client adds 1 to the stra- tum level it learns from its NTP server, so that the stratum level increases the more hops away from the original clock source.

upvoted 8 times

Customexit 8 months, 1 week ago

To expand on this for anyone in the future.

The 4 is the stratum level. You do not need to specify the stratum level, you can simply enter the command R1(config)#ntp master

Without specifying the stratum level, the default stratum is 8.

Example:
(no prior NTP configurations were done)
R1(config)#ntp master
R1(config)#do show ntp associations

address ref clock st when poll reach delay offset disp
*~127.127.1.1 .LOCL. 7 3 64 3 0.00 0.00 0.01
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1#show ntp status
Clock is synchronized, stratum 8

(I have omitted any irrelevant gibberish from these commands btw)
127.127.1.1 is the loopback address (note: not a loopback 'interface')

Now if you did
R1(config)#ntp master 4
R1(config)#do show ntp ass

address ref clock st when poll reach delay offset disp
*~127.127.1.1 .LOCL. 3 5 64 3 0.00 0.00 0.01

R1(config)#do show ntp status
Clock is synchronized, stratum 4

upvoted 4 times

kennybb 11 months ago

is it ntp level?
max is 1>2>3>4

upvoted 1 times

GangsterDady 1 year, 7 months ago

m also wondering

upvoted 1 times

Question #558 *Topic 1*

Which protocol requires authentication to transfer a backup configuration file from a router to a remote server?

A. FTP

B. SMTP

C. TFTP

D. DTP

Correct Answer: *A*

Adaya 1 year, 7 months ago

A is the correct answer

upvoted 3 times

ascsaca 1 year, 9 months ago

C correct

upvoted 1 times

ProgSnob 1 year, 6 months ago

Some free advice from someone who has been taking these exams for 15 years. They always give wrong answer options that they expect people to select due to overlooking one word in the question. Read the questions more than once.

upvoted 13 times

Rydaz 3 weeks, 5 days ago

any paid advice?

upvoted 1 times

Myname1277 1 year, 9 months ago

TFTP does not require authentication while FTP requires authentication so A is correct

upvoted 14 times

dave1992 1 year, 7 months ago

You have to re read the question.

upvoted 1 times

Question #559 *Topic 1*

Which condition must be met before an NMS handles an SNMP trap from an agent?

A. The NMS must receive the same trap from two different SNMP agents to verify that it is reliable.

B. The NMS must receive a trap and an inform message from the SNMP agent within a configured interval.

C. The NMS software must be loaded with the MIB associated with the trap.

D. The NMS must be configured on the same router as the SNMP agent.

Correct Answer: *C*

Mozah 1 year, 4 months ago

Selected Answer: C

C is correct

upvoted 2 times

Question #560 *Topic 1*

An engineer is configuring switch SW1 to act as an NTP server when all upstream NTP server connectivity fails. Which configuration must be used?

A. SW1# config t SW1(config)#ntp peer 192.168.1.1 SW1(config)#ntp access-group peer accesslist1

B. SW1# config t SW1(config)#ntp master SW1(config)#ntp server192.168.1.1

C. SW1# config t SW1(config)#ntp backup SW1(config)#ntp server192.168.1.1

D. SW1# config t SW1(config)#ntp server192.168.1.1 SW1(config)#ntp access-group peer accesslist1

Correct Answer: *B*
ntp server192.168.1.1 makes the SW1 a client to the primary server reachable with an IP address of 192.168.1.1
NTP server makes SW1 a server and uses its own internal clock to provide the time when the connectivity to the primary server 192.168.1.1 fails.

zaguy Highly Voted 1 year, 8 months ago
Correct Answer therefore : B. SW1# config t SW1(config)#ntp master SW1(config)#ntp server192.168.1.1
upvoted 17 times

Sim_James_27 1 year, 6 months ago
A is right, If a particular device is configured as an NTP peer it means that it will peer with another system and accept the time from that system
upvoted 1 times

nebolala1 Highly Voted 1 year, 7 months ago
i hate that question
upvoted 15 times

MDK94 Most Recent 11 months, 1 week ago
Correct me if I'm wrong but I think it's B because:

The "NTP Master" command sets this device (SW1) as an NTP server, the second command "NTP server 192.168.1.1" synchronises this device to 192.168.1.1's time. if the upstream connectivity to 192.168.1.1 is lost, this device will continue to act as a NTP server for the rest of the hosts in the network.
upvoted 8 times

gachocop3 1 year, 3 months ago
answer is B
upvoted 2 times

Nebulise 1 year, 4 months ago
It's worth noting that A and C aren't even valid commands for NTP in IOS. so you can at least rule those bad boi's out.
upvoted 4 times

taiyi078 1 year, 4 months ago
Selected Answer: B
Answer B
upvoted 1 times

ksave 1 year, 4 months ago
Selected Answer: B
ntp server192.168.1.1 makes the SW1 a client to the primary server reachable with an ip add 192.168.1.1
NTP server makes SW1 a server and uses its own internal clock to provide the time when the connectivity to the primary server 192.168.1.1 fails.
upvoted 2 times

Vinarino 1 year, 4 months ago
"all upstream NTP server connectivity fails." On SW1 (not yet an NTP server), 1. Where is the access-list? 2. How does this client obtain it? 3. Do switches typically utilize ACLs? - As a novice, I'd pick B
upvoted 3 times

gaber 1 year, 5 months ago
ntp master = Configures the device as an authoritative NTP
server.

(this is for when you are doodling with the configuration on the switch after the thing fails)

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_2/nx-os/system_management/configuration/guide/sm_nx_os_cli/sm_3ntp.pdf?bcsi-ac-4d57fec82d0c41f9=271918E500000005olcsuBTZcAIAy9u9O1OlNPqAoEAbAQAABQAAAIKYCAGAcAAAAAAAAK0iAgA=

B

upvoted 1 times

gaber 1 year, 5 months ago

sorry that comment kind of sucks, but check this out:

"A peer configured alone takes on the role of a server and should be used as backup"

so a switch configured with the peer command makes it not a server, so there's your answer; B once again

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/sw/4_0/system_management/configuration/guide/n1000v_sys_manage/system_6ntp.pdf#:~:text=NTP%20Peers%20NTP%20allows%20you%20to%20create%20a,maintains%20the%20right%20time%20even%20if%20its%20NTP

upvoted 1 times

Yeeheet 1 year, 6 months ago

Selected Answer: A

You can create NTP peer relationships to designate the time-serving hosts that you want your network device to consider synchronizing with and to keep accurate time if a server failure occurs.

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/system-management/guide/b_Cisco_Nexus_7000_Series_NX-OS_System_Management_Configuration_Guide-RI/configuring_ntp.html

upvoted 2 times

Pkard 1 year, 6 months ago

The answer is A base on the link posted by oflu61. Here is the relevant passage to make life easier: "A peer that is configured alone takes on the role of a server and should be used as a backup. If you have two servers, you can configure several devices to point to one server and the remaining devices to point to the other server. You can then configure a peer association between these two servers to create a more reliable NTP configuration."

upvoted 1 times

Holko18 1 year, 6 months ago

Selected Answer: B

From official Cisco 200-301 guide:

1. Establish an association with the NTP servers per the ntp server command.
2. Establish an association with your internal clock using the ntp master stratum command.
3. Set the stratum level of the internal clock (per the ntp master {stratum-level} command) to a higher (worse) stratum level than the Internet-based NTP servers .
4. Synchronize with the best (lowest) known time source, which will be one of the Internet NTP servers in this scenario

I think answer is B.

upvoted 3 times

oflu61 1 year, 6 months ago

i think is A :
High Availability -> "You can configure NTP peers to provide redundancy in case an NTP server fails."

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/system-management/b-cisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x/b-cisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x_chapter_0101.html

upvoted 1 times

sp3nc3 1 year, 7 months ago

the correct answer is A. The symmetric active mode is used between NTP devices to synchronize with each other, it's used as a backup mechanism when they are unable to reach the (external) NTP server.

upvoted 1 times

DaBest 1 year, 8 months ago

I think answer is A :
Symmetric active/passive mode is intended for configurations where a group of low stratum peers operate as mutual backups for each other. A peer is configured in symmetric active mode by using the peer command and specifying the DNS name or address of the other peer. The other peer is also configured in symmetric active mode in this way.

Note: If the other peer is not specifically configured in this way, a symmetric passive association is activated upon arrival of a symmetric active message. Since an intruder can impersonate a symmetric active peer and inject false time values, symmetric mode should always be authenticated.

https://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html#assnmodes

upvoted 1 times

TetsuRuger 1 year, 9 months ago

How come D is correct??
Can somebody tell me the reason??

upvoted 1 times

Sipan 1 year, 9 months ago

B is the correct answer

upvoted 4 times

Question #561 *Topic 1*

A network administrator must enable DHCP services between two sites. What must be configured for the router to pass DHCPDISCOVER messages on to the server?

A. DHCP Binding

B. a DHCP Relay Agent

C. DHCP Snooping

D. a DHCP Pool

Correct Answer: *B*

DARKK 1 year ago

Selected Answer: B

B for sure. "...for the *router* to pass *DHCPDISCOVER* messages on to the server"

upvoted 1 times

Kvothe24 1 year, 1 month ago

Selected Answer: B

In my opinion, answer is: B. Because they ask what is needed "to pass DHCPDISCOVER messages" and this is the role of a DHCP Relay Agent.

upvoted 3 times

chalaka 1 year, 1 month ago

tricky question, they didn't mention that the networks are in different areas, so they are connected via the same router (fe0/0 and fe0/1 for example), therefore the answer is: D. a DHCP Pool

upvoted 4 times

dfvanloon 1 year, 1 month ago

Copied from GP:
At first glance it does appear this way, however, this is only because we are assuming that a helper address (DHCP relay agent) isn't already configured. Since the question doesn't explicitly state anything about any "default" configurations then we can't assume that a DHCP relay agent hasn't already been configured. The question just says what MUST be configured (out of the options that are provided in the answers).

With that being said, if a DHCP relay agent has already been configured then the only thing you ABSOLUTELY need at this point is the DHCP pool. This is because, if the DHCP server has a scope or pool configured for a particular network, then the server will respond; otherwise, it will NOT respond. So, without a DHCP pool it wouldn't matter if you had the DHCP relay agent configured because the DHCP server would never respond. Thus, you MUST have the pool configured in order for DHCP to work correctly. DHCP pool is the better answer.

upvoted 4 times

ismatdmour 1 year, 2 months ago

Selected Answer: B

Router need to be configured as Relay agent. In this case it will receive the broadcast discover message and forward it as unicast to the configured dhcp which exists in another subnet probably in a centrlized location in the enterprise network

upvoted 1 times

NORLI 1 year, 1 month ago

B is wrong because the question did not ask if they were in different network. you only need to configure a router as a relay agent if the dhcp server and the workstation are in different network using the the ip-helper address command. The question say dhcp discover which means it is only clients in the dhcp pool that will get the discovery message so D is the correct answer.

upvoted 1 times

gachocop3 1 year, 3 months ago

the answer is B

upvoted 1 times

LilGhost_404 1 year, 3 months ago

Selected Answer: B

https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5567-configure-dynamic-host-configuration-protocol-dhcp-relay-set.html

upvoted 1 times

Cpynch 1 year, 4 months ago

Selected Answer: B

Relay agents are required to pass broadcast messages off of the broadcast domain.

upvoted 1 times

awashenko 1 year, 4 months ago

Selected Answer: B

A relay agent is needed. Answer is B

upvoted 1 times

Mozah 1 year, 4 months ago

Selected Answer: B

I think B

upvoted 1 times

Ravan 1 year, 4 months ago

Selected Answer: B

A relay agent (ip-helper)

upvoted 1 times

Cho1571 1 year, 4 months ago

Ha! the answer is B

upvoted 1 times

daanderud 1 year, 5 months ago

Selected Answer: B

Answer is wrong. Relay agent is need for allow all DHCP packets to pass between subnets.

upvoted 1 times

juani85 1 year, 5 months ago

Selected Answer: B

I think good answer B

upvoted 1 times

RJM 1 year, 5 months ago

Selected Answer: B

Relay agent passes routed DHCP discover packets.

upvoted 3 times

gaber 1 year, 5 months ago

I'm inclined to agree with this. It says "to pass", you don't need a pool to pass these packets, as the pool is located on the server. Routers don't automatically forward the packets so it needs a dhcp relay agent to find the server at the other site.

B

upvoted 1 times

chalaka 1 year, 1 month ago

tricky question, they didn't mention that the networks are in different areas, so they are connected via the same router (fe0/0 and fe0/1 for example), therefore the answer is: D. a DHCP Pool

upvoted 1 times

Question #562 *Topic 1*

Which level of severity must be set to get informational syslogs?

A. alert

B. critical

C. notice

D. debug

Correct Answer: *D*

Vinarino Highly Voted 1 year, 5 months ago

Syslog uses the User Datagram Protocol (UDP), port 514

SEVERITY LEVEL
** SEVERITY IN EVENT = Default SMS setting for Syslog Security option.
This setting will send all events to remote Syslog system
1 ALERT
2 CRITICAL
3 ERROR
4 WARNING
5 NOTICE
6 INFORMATIONAL (7 Debug [lower] will include ALL Informational messages)
7 DEBUG

upvoted 9 times

Liuka_92 11 months, 2 weeks ago

0 EMERGENCY

upvoted 2 times

hp2wx Highly Voted 10 months, 3 weeks ago

Every good Cisco engineer will need intercourse daily :0

upvoted 6 times

arenjenkins Most Recent 7 months, 2 weeks ago

fck this questiion

upvoted 5 times

ptfish 10 months, 3 weeks ago

Selected Answer: D

The informational level is lower than the notice level. So only debug level can get those information. Answer D is correct.

upvoted 2 times

redivivo 1 year ago

Emma Always Cries Even When Nobody Is Dying

upvoted 4 times

Question #563 *Topic 1*

On workstations running Microsoft Windows, which protocol provides the default gateway for the device?

A. STP

B. DHCP

C. SNMP

D. DNS

Correct Answer: *B*

Question #564 *Topic 1*

Which two statements about NTP operations are true? (Choose two.)

A. NTP uses UDP over IP.

B. Cisco routers can act as both NTP authoritative servers and NTP clients.

C. Cisco routers can act only as NTP servers.

D. Cisco routers can act only as NTP clients.

E. NTP uses TCP over IP.

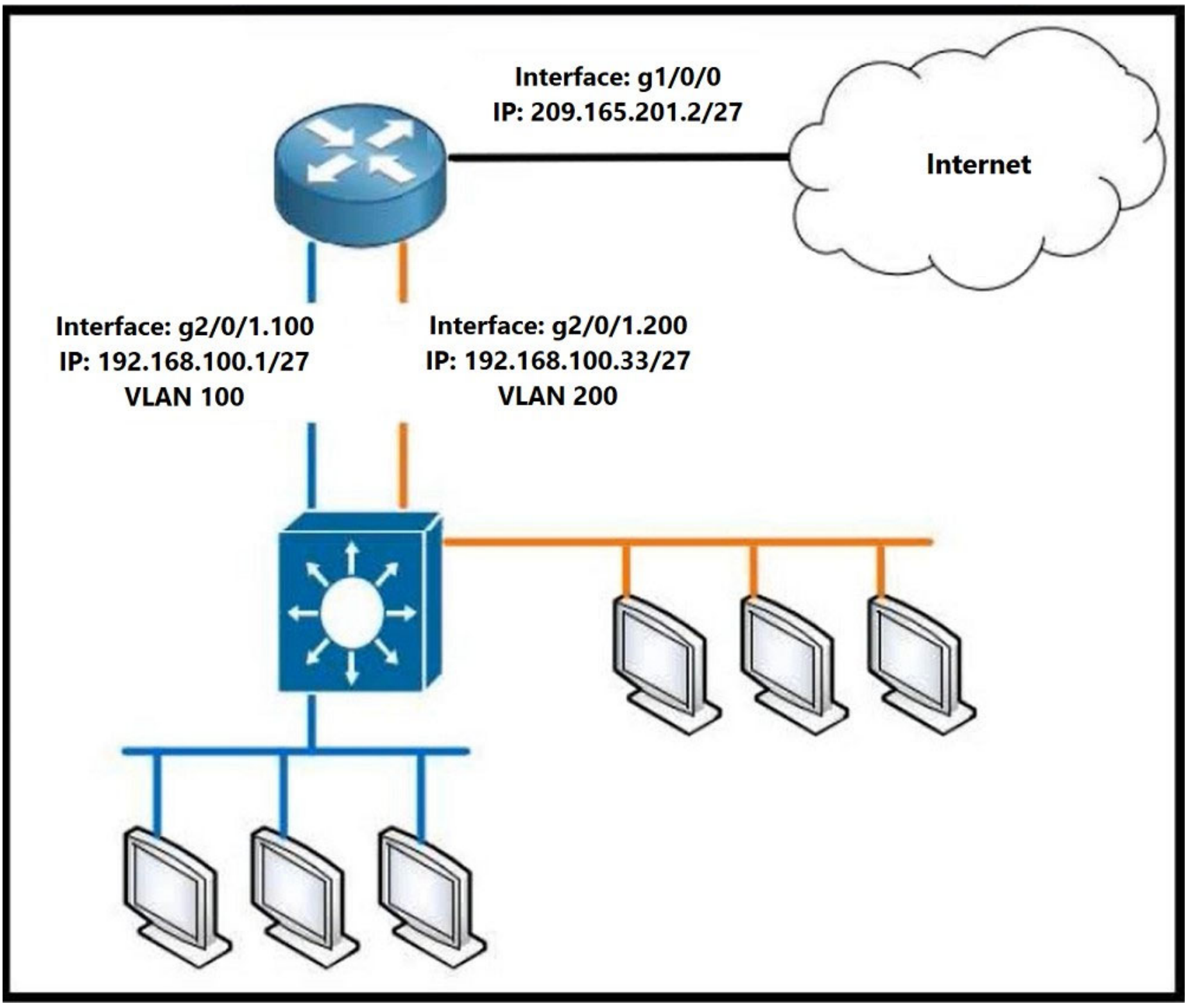
Correct Answer: *AB*

kebkim Highly Voted 11 months ago

NTP use UDP port 123.

upvoted 5 times

Question #565 *Topic 1*



Refer to the exhibit. Which configuration must be applied to the router that configures PAT to translate all addresses in VLAN 200 while allowing devices on VLAN
100 to use their own IP addresses?

A. Router1(config)#access-list 99 permit 192.168.100.32 0.0.0.31 Router1(config)#ip nat inside source list 99 interface gi1/0/0 overload Router1(config)#interface gi2/0/1.200 Router1(config)#ip nat inside Router1(config)#interface gi1/0/0 Router1(config)#ip nat outside

B. Router1(config)#access-list 99 permit 192.168.100.0 0.0.0.255 Router1(config)#ip nat inside source list 99 interface gi1/0/0 overload Router1(config)#interface gi2/0/1.200 Router1(config)#ip nat inside Router1(config)#interface gi1/0/0 Router1(config)#ip nat outside

C. Router1(config)#access-list 99 permit 209.165.201.2 255.255.255.255 Router1(config)#ip nat inside source list 99 interface gi1/0/0 overload Router1(config)#interface gi2/0/1.200 Router1(config)#ip nat inside Router1(config)#interface gi1/0/0 Router1(config)#ip nat outside

D. Router1(config)#access- list 99 permit 209.165.201.2 0.0.0.0 Router1(config)#ip nat inside source list 99 interface gi1/0/0 overload Router1(config)#interface gi2/0/1.200 Router1(config)#ip nat inside Router1(config)#interface gi1/0/0 Router1(config)#ip nat outside

Correct Answer: *A*

AndreMD Highly Voted 10 months ago
just looking the IP address and subnet mask of the access list, you can find the right answer
upvoted 12 times

rogi2023 2 months, 3 weeks ago
another broke question with bad wording/syntax on routers intf..but agree with AndreMD
upvoted 1 times

fransCISCO 4 months, 1 week ago

yes its A

upvoted 1 times

splashy Highly Voted 8 months, 2 weeks ago

This config is so broke it hurts my head, OR multiple clients from vlan 200 will be able to send traffic outside, OR 1 client from vlan 100. Either way there will be clients with outside connectivity issues.

upvoted 7 times

Question #566 *Topic 1*

```
R1#show run
Building configuration...
!
hostname R1
!
username CNAC password 0 cona123
!
ip domain-name CNAC.com
!
interface GigabitEthernet0/0/0
 ip address 192.168.1.10 255.255.255.0
 duplex auto
 speed auto
!
line vty 0 15
 login local

R1#show crypto key mypubkey rsa

R1#show ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
```

Refer to the exhibit. Which two commands must be added to update the configuration of router R1 so that it accepts only encrypted connections? (Choose two.)

A. transport input ssh

B. username CNAC secret R!41!3705926@

C. crypto key generate rsa 1024

D. line vty 0 4

E. ip ssh version 2

Correct Answer: *CE*

splashy Highly Voted 8 months, 2 weeks ago

Selected Answer: AC

The default setting on switch/router to accept remote access is telnet.

Crypto key is not yet generated.

"...configuration of router R1 so that it accepts ONLY encrypted connections..."

So A + C

upvoted 7 times

guynetwork Highly Voted 9 months ago

Selected Answer: AC

A and C
only encrypted and crypto key not yet generated

upvoted 7 times

DMc Most Recent 1 month, 1 week ago

Given answer of C & E is correct.
Given answer C & E is probably correct but A & C is good too. Go with C/E because you need C/E first (for encryption) then you do need A for remote access, so focus on “encryption” in the question.
https://ipwithease.com/how-to-configure-ssh-version-2-on-cisco-router/

upvoted 1 times

creaguy 8 months, 1 week ago

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/15-s/sec-usr-ssh-15-s-book/sec-secure-shell-v2.html#:~:text=the%20default%20host.-,Configuring%20a%20Device%20for%20SSH%20Version%202%20Using%20RSA%20Key%20Pairs,-SUMMARY%20STEPS

upvoted 1 times

king_oat 8 months, 2 weeks ago

Selected Answer: AC

A and C
telnet ssh and crypto key not yet created
upvoted 3 times

rogi2023 2 months, 3 weeks ago

and the cmd "crypto key generate rsa 1024" enables the ssh ver2 by default
upvoted 2 times

sasquatchshrimp 10 months, 1 week ago

Selected Answer: AD

https://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/1100-cisco-routers-ssh-support-configuration-rsa-key-generation.html
upvoted 1 times

Question #567 *Topic 1*

Which command implies the use of SNMPv3?

A. snmp-server user

B. snmp-server host

C. snmp-server enable traps

D. snmp-server community

Correct Answer: *A*

Reference:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/15-e/snmp-15-e-book.pdf

ptfish Highly Voted 10 months, 3 weeks ago

Adds a new user to an SNMPv3 group and configures a plain
text password for the user.
Example:
Device(config)# snmp-server user user1 group1
v3 auth md5 password123 priv passwd123654
upvoted 5 times

dropspablo Most Recent 1 week, 1 day ago

Selected Answer: A

"Device(config)# snmp-server user user1 group1 v3 auth md5 password123 priv des passwd123654"

(Added a new user named "user1" to the SNMPv3 group "group1". User is configured for authentication (auth) using MD5 hashing algorithm with password "password123". In addition, user also has privacy (priv) enabled using the DES encryption algorithm with the privacy password "passwd123654".)

There are several authentication and privacy algorithms available for SNMPv3, such as MD5, SHA, DES, AES, and others.
upvoted 1 times

RougePotatoe 7 months, 1 week ago

Can anyone confirm that snmp-server user command is only avaliable to SNMPv3?
upvoted 1 times

jonathan126 1 month, 1 week ago

"SNMPv3 is a security model in which an authentication strategy is set up for a user and the group in which the user resides".
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/5700/snmp-xe-3se-5700-book/nm-snmp-snmpv3.pdf

SNMPv2c use community string.
upvoted 3 times

Question #568 *Topic 1*

R1 as an NTP server must have:
- NTP authentication enabled
- NTP packets sourced from Interface loopback 0
- NTP stratum 2
- NTP packets only permitted to client IP 209.165.200.225

How should R1 be configured?

A. ntp authenticate ntp authentication-key 2 sha1 CISCO123 ntp source Loopback0 ntp access-group server-only 10 ntp master 2 ! access-list 10 permit udp host 209.165.200.225 any eq 123

B. ntp authenticate ntp authentication-key 2 md5 CISCO123 ntp interface Loopback0 ntp access-group server-only 10 ntp stratum 2 ! access-list 10 permit 209.165.200.225

C. ntp authenticate ntp authentication-key 2 md5 CISCO123 ntp source Loopback0 ntp access-group server-only 10 ntp master 2 ! access-list 10 permit 209.165.200.225

D. ntp authenticate ntp authentication-key 2 md5 CISCO123 ntp source Loopback0 ntp access-group server-only 10 ntp stratum 2 ! access-list 10 permit udp host 209.165.200.225 any eq 123

Correct Answer: *D*

splashy Highly Voted 10 months, 1 week ago
C seems correct, its an acl question.
10 is standard acl number so A and D are wrong cause they are extended acls.
NTP Master 2 makes the router an ntp server with stratum lvl 2.
upvoted 10 times

sijan Most Recent 2 months, 4 weeks ago
C should be correct
upvoted 2 times

oatmealturkey 3 months, 2 weeks ago
Selected Answer: C
It cannot be D because stratum is not a valid command.
upvoted 2 times

iampogiian 5 months, 2 weeks ago
Letter C ang sagot
upvoted 2 times

Aiman_Abdullah 7 months, 3 weeks ago
try to login to any router, i think we cannot insert any stratum 2 , only master 2 can. and for ntp access-group server-only 10,, i should serve-only 10.. anyway Answer is C. agree with MDK94
upvoted 3 times

splashy 8 months, 2 weeks ago
Selected Answer: C
explained below
upvoted 4 times

beskardrip 11 months, 1 week ago
Selected Answer: D
Pretty sure its D because it says Only NTP packets are allowed and on the access list command on D it specifies only allow traffic on port 123.
upvoted 1 times

alejandro12 6 months, 2 weeks ago
Its not d, because the access list 10 is standar and cannot configure ports on this
upvoted 4 times

RougePotatoe 7 months, 1 week ago
D has the command NTP stratum 2 (not a real command) it is suppose to be ntp master 2
upvoted 6 times

MDK94 11 months, 1 week ago
Note ntp access-group serve-only is the correct command not server-only, but its incorrect on every answer so it shouldn't matter.

Source: https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/system_management/command/reference/yr40crs_chapter10.html#wp1797670550:~:text=Allows%20only%20time%20requests.

A. Incorrect because sha1 isn't used for NTP authentication, must be MD5
ntp authenticate
ntp authentication-key 2 sha1 CISCO123
ntp source Loopback0
ntp access-group server-only 10
ntp master 2
access-list 10 permit udp host 209.165.200.225 any eq 123
upvoted 3 times

MDK94 11 months, 1 week ago

B. Incorrect because it isn't using the NTP source command (uses ntp interface Loopback0) instead
ntp authenticate
ntp authentication-key 2 md5 CISCO123
ntp interface Loopback0
ntp access-group server-only 10
ntp stratum 2
access-list 10 permit 209.165.200.225
upvoted 3 times

MDK94 11 months, 1 week ago

Both C and D are correct answers in my opinion, the only difference is that the access-list is more granular for D, meaning C is probably the best option.

C.
ntp authenticate
ntp authentication-key 2 md5 CISCO123
ntp source Loopback0
ntp access-group server-only 10
ntp master 2
access-list 10 permit 209.165.200.225

D.
ntp authenticate
ntp authentication-key 2 md5 CISCO123
ntp source Loopback0
ntp access-group server-only 10
ntp stratum 2
access-list 10 permit udp host 209.165.200.225 any eq 123
upvoted 3 times

MDK94 11 months, 1 week ago

Granularity of the ACL shouldn't be required as the acl is being applied to "serve-only" aka only allow time requests

Source: https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/system_management/command/reference/yr40crs_chapter10.html#wp1797670550:~:text=Allows%20only%20time%20requests.
upvoted 2 times

MDK94 11 months, 1 week ago

I just realised, its 100% C because the access-list 10 is a standard access-list, meaning that specifying the protocol (udp) and destination address as any with the eq port number wouldn't be allowed.

C is the correct answer 100%
upvoted 6 times

ratu68 11 months ago

Good Catch !
upvoted 3 times

BOFA 10 months, 1 week ago

you got a point but there is something pops up on my mind the acl command is using standard numbered acl which ranges between 1 to 99 and as i studied the standard use only source ip so correct me if im wrong
upvoted 1 times

iGlitch 1 year ago

I thought the question is about NTP, but it's NOT.
upvoted 1 times

Question #569 *Topic 1*

What is a capability of FTP in network management operations?

A. offers proprietary support at the session layer when transferring data

B. uses separate control and data connections to move files between server and client

C. encrypts data before sending between data resources

D. devices are directly connected and use UDP to pass file information

Correct Answer: *B*
Reference:
https://en.wikipedia.org/wiki/File_Transfer_Protocol#:~:text=The%20File%20Transfer%20Protocol%20(FTP,the%20client%20and%20the%20server

StingVN 2 weeks, 5 days ago

Selected Answer: B

The File Transfer Protocol (FTP) is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture using separate control and data connections between the client and the server.

upvoted 1 times

StingVN 2 weeks, 5 days ago

The File Transfer Protocol (FTP) is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture using separate control and data connections between the client and the server.

upvoted 1 times

papibarbu 5 months ago

B is correct

upvoted 2 times

Question #570 *Topic 1*

A network engineer is configuring a switch so that it is remotely reachable via SSH. The engineer has already configured the host name on the router. Which additional command must the engineer configure before entering the command to generate the RSA key?

A. password password

B. ip ssh authentication-retries 2

C. ip domain-name domain

D. crypto key generate rsa modulus 1024

Correct Answer: *C*
Reference:
https://www.letsconfig.com/how-to-configure-ssh-on-cisco-ios-devices/

Mccn 4 months, 1 week ago
We have configured hostname and domain-name because they are needed to generate RSA key. We have configured hostname as IOS and domain-name
upvoted 1 times

Sdiego 4 months, 2 weeks ago
Selected Answer: D
The question "to generate the RSA key"
upvoted 1 times

Dutch012 3 months, 1 week ago
"before entering the command to generate the RSA key"
upvoted 1 times

ratu68 11 months ago
Selected Answer: C
C is absolutely correct
upvoted 3 times

Question #571 *Topic 1*

Which QoS traffic handling technique retains excess packets in a queue and reschedules these packets for later transmission when the configured maximum bandwidth has been surpassed?

A. traffic policing

B. weighted random early detection

C. traffic prioritization

D. traffic shaping

Correct Answer: *D*
Reference:
https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html

Networknovice Highly Voted 1 year ago
Policing drops or remarks traffic that exceeds limits, but shaping regulates the traffic back to a defined rate by delaying or queuing the traffic.
upvoted 13 times

Question #572 *Topic 1*

Which command must be entered to configure a DHCP relay?

A. ip dhcp relay

B. ip dhcp pool

C. ip address dhcp

D. ip helper-address

Correct Answer: *D*
Reference:
https://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htdhcpre.html#:~:text=ip%20helper%2Daddress%20address,-Example%
3A&text=Forwards%20UPD%20broadcasts%2C%20including%20BOOTP%20and%20DHCP.&text=The%20address%20argument%20can%20be,to%20respond
%20to%20DHCP%20requests

Yannik123 2 months ago

Selected Answer: D

The DHCP relay agent is an IP Helper address on a Cisco device

upvoted 1 times

Goena 5 months ago

Selected Answer: D

D is correct

upvoted 2 times

Question #573 *Topic 1*

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
1
DHCP snooping is operational on following VLANs:
1
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is disabled
circuit-id default format: vlan-mod-port
remote-id: aabb.cc00.6500 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface Trusted Allow option Rate limit (pps)
```

```
Switch#show ip dhcp snooping statistics detail
Packets Processed by DHCP Snooping = 34
Packets Dropped Because
IDB not known = 0
Queue full = 0
Interface is in errdisabled = 0
Received on untrusted ports = 32
Nonzero giaddr = 0
Source mac not equal to chaddr = 0
No binding entry = 0
Insertion of opt82 fail = 0
Unknown packet = 0
Interface Down = 0
Unknown output interface = 0
Misdirected Packets = 0
Packets with Invalid Size = 0
Packets with Invalid Option = 0
```

Refer to the exhibit. The DHCP server and clients are connected to the same switch. What is the next step to complete the DHCP configuration to allow clients on
VLAN 1 to receive addresses from the DHCP server?

A. Configure the ip dhcp snooping trust command on the interface that is connected to the DHCP client.

B. Configure ip dhcp relay information option command on the interface that is connected to the DHCP server.

C. Configure ip dhcp snooping trust command on the interface that is connected to the DHCP server.

D. Configure the ip dhcp information option command on the interface that is connected to the DHCP client.

Correct Answer: *C*

RougePotatoe Highly Voted 7 months, 1 week ago

Selected Answer: C

If a Layer 2 LAN port is connected to a DHCP server, configure the port as trusted by entering the ip dhcp snooping trust interface configuration command.
https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/snoodhcp.html#wp1073367

upvoted 5 times

Question #574 *Topic 1*

A network analyst is tasked with configuring the date and time on a router using EXEC mode. The date must be set to January 1, 2020 and the time must be set to
12:00 am. Which command should be used?

A. clock timezone

B. clock summer-time date

C. clock summer-time recurring

D. clock set

Correct Answer: *D*

Goena 5 months ago

Selected Answer: D

D is correct: clock set hh:mm:ss day month year

upvoted 2 times

Question #576 *Topic 1*

Which command creates a static NAT binding for a PC address of 10.1.1.1 to the public routable address 209.165.200.225 assigned to the PC?

A. R1(config)#ip nat inside source static 10.1.1.1 209.165.200.225

B. R1(config)#ip nat outside source static 209.165.200.225 10.1.1.1

C. R1(config)#ip nat inside source static 209.165.200.225 10.1.1.1

D. R1(config)#ip nat outside source static 10.1.1.1 209.165.200.225

Correct Answer: *A*

Yannik123 2 months, 1 week ago

Selected Answer: A

A is right I tested it in Packte Tracer.

upvoted 2 times

Question #577 *Topic 1*

What prevents a workstation from receiving a DHCP address?

A. STP

B. VTP

C. 802.1Q

D. DTP

Correct Answer: *C*

Ghugs Highly Voted 8 months ago

I think its STP, specifically portfast. I found this one the cisco white pages, under the DHCP troubleshooting section.
"...verify that the port has STP portfast enabled and trunking/channeling disabled. The default configuration is STP portfast disabled and trunking/channeling auto, if applicable. For the 2900XL/3500XL/2950/3550 switches, STP portfast is the only required configuration. These configuration changes resolve the most common DHCP client issues that occur with an initial installation of a Catalyst switch."

from https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html#anc72

upvoted 6 times

splashy 7 months, 3 weeks ago

Thx for sharing i guess it's A then

upvoted 1 times

splashy 7 months, 3 weeks ago

Still undecided on this one really... STP ok but you will eventually get a DHCP address. I can however find a lot of issues with vlans not getting a dhcp address (because of various reasons from wrong tagging, not having a dhcp server on the vlan, not having a helper address when the dhcp server is on a different vlan, adding vlans without adding a dhcp pool for the vlan, ...)

upvoted 2 times

fransCISCO 7 months ago

HEY SPLASHY, YOURE MY IDOL,YOU HAVE MANY COMMENTS IN SOME QUESTIONS. I HAVE SOMETHING FOR YOU. WHATS YOUR EMAIL SO THAT I CAN CONTACT YOU

upvoted 2 times

rogi2023 Most Recent 1 month, 2 weeks ago

Selected Answer: A

in such questions the best practise is to exclude the wrong asnwers first.
VTP - says how to spread out VLANs across the network between sw - this one is out.
DTP - says how to create a working trunk. btw on trunk int you won't get an dhcp - ip, so this one out as well.
802.1q - says how to tag VLAN-id in trunk - so also this one is out.
so just with exclusions the last option is STP, which after reading the explanatory comments make sense. So A is definitely correct.

upvoted 3 times

rogi2023 2 months, 3 weeks ago

this is a very stupid question, I hope not to see such garbage on the exam especially for ccna level.

upvoted 2 times

rijstraket 4 months ago

Selected Answer: A

The time it takes to get to the Forwarding state might be too long for a client's DHCP process (which starts after the interface on the client becomes 'up'). Using Spanning-Tree PortFast can mitigate this exact issue. So yes, STP can prevent workstations from getting an IP-adress using DHCP.

upvoted 4 times

mohdhafizudddinesa 6 months, 3 weeks ago

You will not have IP from trunk port

upvoted 1 times

splashy 8 months, 2 weeks ago

Selected Answer: C

STP can't prevent you from getting an DHCP address, it prevents infinite loops of traffic by blocking ports, not by blocking traffic from going to every client on the subnet.

If you cannot authenticate yourself on the network however, you will not be able to send a DHCP request and get an offer.

upvoted 3 times

Murphy2022 8 months ago

Dot1q ist VLAN tagging not authentication
upvoted 2 times

splashy 7 months, 3 weeks ago
Correct i got it mixed up with 802.1X... doh
upvoted 1 times

ShadyAbdekmalek 8 months, 2 weeks ago
Selected Answer: A
Answer is A : STP
At is also same as Question 108 which has the correct answer
upvoted 1 times

Question #578 *Topic 1*

What is a feature of TFTP?

A. offers anonymous user login ability

B. uses two separate connections for control and data traffic

C. relies on the well-known TCP port 20 to transmit data

D. provides secure data transfer

Correct Answer: *A*

nicombe Highly Voted 8 months, 2 weeks ago
B: TFTP uses Port 69...heh
C: FTP uses TCP Ports 20 & 21
D: Neither FTP nor TFTP provide secure data transfer on their own
A: TFTP does not support authentication. Maybe no login ability at all offers anonymity..?
upvoted 6 times

harveyDai Highly Voted 9 months ago
I thought TFTP is only for File transferring.
upvoted 5 times

Question #579 *Topic 1*

Which QoS forwarding per-hop behavior changes a specific value in a packet header to set the class of service for the packet?

A. shaping

B. classification

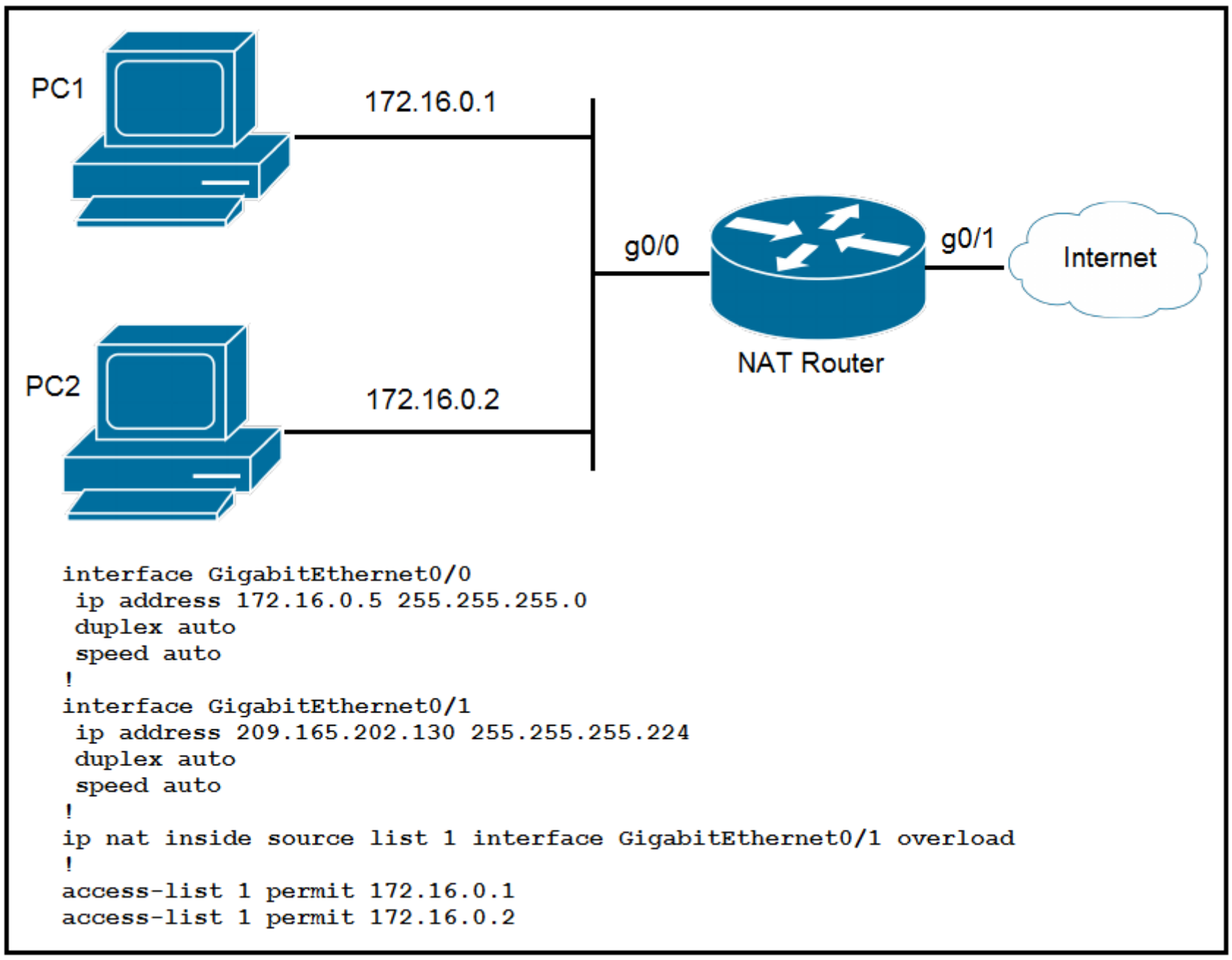
C. policing

D. marking

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #580 *Topic 1*



Refer to the exhibit. How should the configuration be updated to allow PC1 and PC2 access to the Internet?

A. Modify the configured number of the second access list

B. Change the ip nat inside source command to use interface GigabitEthernet0/0

C. Remove the overload keyword from the ip nat inside source command

D. Add either the ip nat {inside|outside} command under both interfaces

Correct Answer: *D*

j1mlawton Highly Voted 3 months, 3 weeks ago

Selected Answer: B

Why is it not B?

upvoted 5 times

4aynick Most Recent 1 month, 1 week ago

Selected Answer: D

100% D is correct

upvoted 1 times

rogi2023 1 month, 2 weeks ago

Selected Answer: D

Only inside/outside on the interfaces is missing. and it is a must.

upvoted 2 times

Goena 3 months, 1 week ago

Selected Answer: D

Answer D is correct:
ip nat inside source list INSIDE-NET pool SHARED-IP (g0/1)overload (in this case G0/1).
Only inside/outside on the interfaces is missing.

upvoted 3 times

Question #581 *Topic 1*

What is the purpose of the ip address dhcp command?

A. to configure an interface as a DHCP relay

B. to configure an interface as a DHCP client

C. to configure an interface as a DHCP helper

D. to configure an interface as a DHCP server

Correct Answer: *B*

Goh0503 8 months ago

Answer B
This command enables the DHCP client on the interface and removes all manually-configured addresses on the interface.

https://www.cisco.com/c/en/us/td/docs/routers/nfvis/switch_command/b-nfvis-switch-command-reference/ip_addressing_commands.pdf

upvoted 3 times

Question #582 *Topic 1*

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker
!
ip cef
!
interface FastEthernet0/0
description WAN_INTERFACE
ip address 10.0.1.2 255.255.255.252
ip access-group 100 in
!
interface FastEthernet0/1
description LAN_INTERFACE
ip address 10.148.2.1 255.255.255.0
duplex auto
speed auto
!
ip forward-protocol nd
!
access-list 100 permit eigrp any any
access-list 100 permit icmp any any
access-list 100 permit tcp 10.149.3.0 0.0.0.255 host 10.0.1.2 eq 22
access-list 100 permit tcp any any eq 80
access-list 100 permit tcp any any eq 443
access-list 100 deny ip any any log
```

Refer to the exhibit. Which configuration enables DHCP addressing for hosts connected to interface FastEthernet0/1 on router R4?

A. interface FastEthernet0/1 ip helper-address 10.0.1.1 ! access-list 100 permit tcp host 10.0.1.1 eq 67 host 10.148.2.1

B. interface FastEthernet0/0 ip helper-address 10.0.1.1 ! access-list 100 permit udp host 10.0.1.1 eq bootps host 10.148.2.1

C. interface FastEthernet0/0 ip helper-address 10.0.1.1 ! access-list 100 permit host 10.0.1.1 host 10.148.2.1 eq bootps

D. interface FastEthernet0/1 ip helper-address 10.0.1.1 ! access-list 100 permit udp host 10.0.1.1 eq bootps host 10.148.2.1

Correct Answer: *A*

rijstraket Highly Voted 5 months, 4 weeks ago

Selected Answer: D

B and C configure fa0/0, so those are incorrect. Bootps uses UDP so A is also incorrect. D is correct, but the answer has a flaw: As they use a non rearrangeable ACL the ACE would be added at the bottom, below the deny rule (rendering the newly added rule useless).

upvoted 7 times

StingVN 2 weeks, 5 days ago

agree yo

upvoted 1 times

enzo86 Most Recent 1 month, 3 weeks ago

Selected Answer: D

dhcp is udp and iphelper in f0/1 interface LAN

upvoted 2 times

RougePotatoe 7 months, 1 week ago

Selected Answer: D

As port 67 and bootps is kind of similar in the sense that it doesn't really give you a huge differentiating factor notice the transport protocols. Bootps and DHCP both are listed as UDP 67.

upvoted 3 times

Garfieldcat 7 months, 3 weeks ago

why only permit specific host instead of network ? the question is asking the config to allow source hosts of the subnet.

upvoted 3 times

Goh0503 8 months ago

Answer D
First = need to be configured On Fa 0/1 as the host is this Interface per the Question requirement

Second =DHCP uses UDP port 67

https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#:~:text=The%20DHCP%20employs%20a%20connectionless,is%20used%20by%20the%20client.

upvoted 3 times

creaguy 8 months, 1 week ago

Selected Answer: D

*I mean DHCP uses UDP port 67

https://www.sysnettechsolutions.com/en/what-is-bootp/

upvoted 3 times

creaguy 8 months, 1 week ago

Selected Answer: D

DHCP uses TCP port 67

https://www.sysnettechsolutions.com/en/what-is-bootp/

upvoted 1 times

JonasWolfxin 8 months, 2 weeks ago

Selected Answer: D

answer: D; BOOTP is implemented using the User Datagram Protocol (UDP) for transport protocol, port number 67 is used by the (DHCP) server for receiving client-requests and port number 68 is used by the client for receiving (DHCP) server responses. BOOTP operates only on IPv4 networks.

upvoted 3 times

king_oat 8 months, 2 weeks ago

Selected Answer: A

A is correct. Can assign TCP to port 67 (DHCP)

upvoted 1 times

splashy 8 months, 2 weeks ago

Selected Answer: D

"for hosts connected to interface FastEthernet0/1"
not B &C
DHCP is UDP port 67
D is correct

upvoted 2 times

HeinyHo 8 months, 3 weeks ago

Selected Answer: D

LAN is Fa 0/1 and DHCP is UDP so it's D

upvoted 2 times

joondale 8 months, 3 weeks ago

ip helper-address must be configured on FastEthernet0/1 right? because it is the interface closest to the clients. So B and C are already eliminated from the choices. And DHCP uses UDP so D is the answer i think. Pls correct me if im wrong

upvoted 4 times

rictorres333 8 months, 3 weeks ago

Selected Answer: B

TCP 67 is bootp but DHCP is UDP bootp.
Is TCP or UDP used for DHCP?
The DHCP employs a connectionless service model, using the User Datagram Protocol (UDP). It is implemented with two UDP port numbers for its operations which are the same as for the bootstrap protocol (BOOTP).

B is correct.

upvoted 1 times

shubhambala 8 months, 3 weeks ago

Selected Answer: B

IS B the answer?

upvoted 1 times

melmiosis 7 months ago

no... the question clearly asks what configuration is to be applied to f0/1... B & C configs are to be applied on f0/0. idk how many people are missing this. '

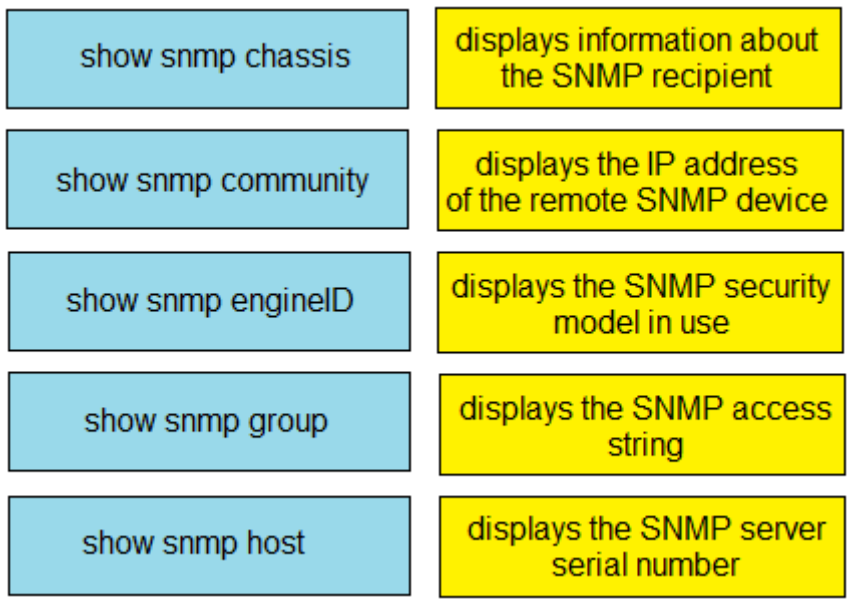
upvoted 1 times

Question #583 *Topic 1*

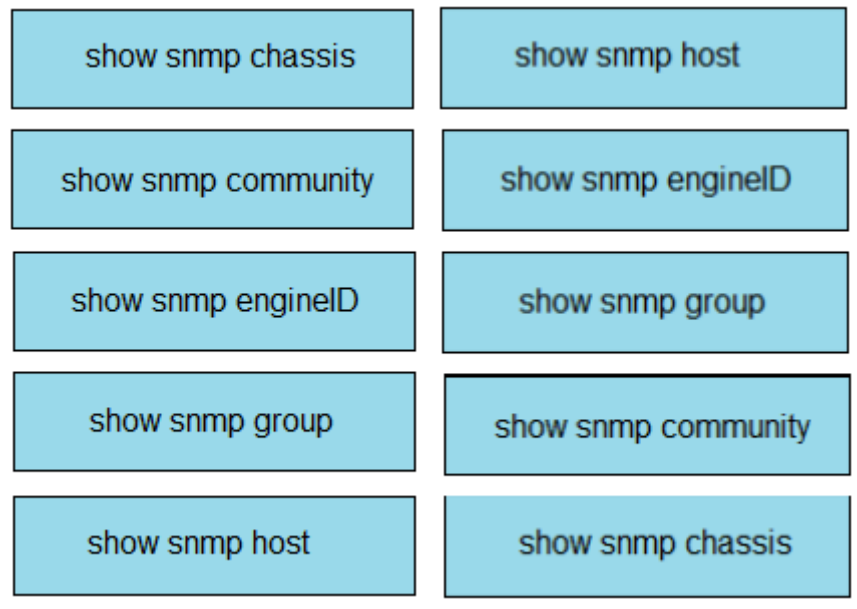
DRAG DROP -

Drag and drop the SNMP manager and agent identifier commands from the left onto the functions on the right.

Select and Place:



Correct Answer:



Reylien Highly Voted 8 months, 3 weeks ago

Answer is correct

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/command/snmp-xe-3se-3850-cr-book/snmp-xe-3se-3850-cr-book_chapter_0110.html

upvoted 5 times

Question #584 *Topic 1*

An engineer is configuring SSH version 2 exclusively on the R1 router. What is the minimum configuration required to permit remote management using the cryptographic protocol?

A. hostname R1 service password-encryption crypto key generate rsa general-keys modulus 1024 username cisco privilege 15 password 0 cisco123 ip ssh version 2 line vty 0 15 transport input ssh login local

B. hostname R1 ip domain name cisco crypto key generate rsa general-keys modulus 1024 username cisco privilege 15 password 0 cisco123 ip ssh version 2 line vty 0 15 transport input ssh login local

C. hostname R1 crypto key generate rsa general-keys modulus 1024 username cisco privilege 15 password 0 cisco123 ip ssh version 2 line vty 0 15 transport input ssh login local

D. hostname R1 ip domain name cisco crypto key generate rsa general-keys modulus 1024 username cisco privilege 15 password 0 cisco123 ip ssh version 2 line vty 0 15 transport input all login local

Correct Answer: *B*

SVN05 Highly Voted 3 months, 4 weeks ago

Selected Answer: B

So before generating a RSA key, always remember you'll need a hostname and ip domain name. Then only you can create a RSA key(yes password isn't a requirement initally) which leaves us with answer B and answer D.

Moving on, the question asks to permit remote management(vty lines basically) using a cryptographic protocol thus we don't want to allow anyone in right? so we set a boundary to only allow what we want and that is SSH(cause by default telnet is included if we use transport input all) so that leaves us with answer B.

upvoted 8 times

Question #585 *Topic 1*

Which per-hop traffic-control feature does an ISP implement to mitigate the potential negative effects of a customer exceeding its committed bandwidth?

A. policing

B. queuing

C. marking

D. shaping

Correct Answer: *A*

dropspablo 1 week, 1 day ago

Selected Answer: A

A. policing

upvoted 1 times

andresugiharto 2 months, 2 weeks ago

Answer: A

Shapping: Outgoing traffic only
Policing: In and Out traffic.
https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html

upvoted 2 times

Dutch012 3 months, 1 week ago

Selected Answer: A

Remember that
The customer Router does the shaping (cares and saves your traffic in a queue if you surpass the configured rate), but ISP Router does the policing (it drops your packets and doesn't care or save your traffic in a queue if you surpass the configured rate)

upvoted 3 times

JJY888 3 months, 1 week ago

Selected Answer: A

https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html

upvoted 1 times

rijstraket 4 months ago

Selected Answer: A

Example: Your ISP sold you a fibre connection with a traffic contract and a guaranteed bandwidth of 10 Mbit, the fibre interface however is capable of sending 100 Mbit per second. Most ISPs will configure policing to drop all traffic above 10 Mbit so that you can't get more bandwidth than what you are paying for. It's also possible that they shape it down to 10 Mbit but shaping means they have to buffer data while policing means they can just throw it away. The 10 Mbit that we pay for is called the CIR (Commited Information Rate).

Policing would be the most logical answer, as ISP's usually don't take care of your traffic as you would within your own network. If you really need to get that traffic through, fix it on your own equipment (instead of depending on the provider) so that it all fits properly within the bandwidth you pay for.

upvoted 2 times

ashraf8 4 months, 1 week ago

Selected Answer: D

From Wikipedia: "In communications, traffic policing is the process of monitoring network traffic for compliance with a traffic contract and taking steps to enforce that contract. Traffic sources which are aware of a traffic contract may apply traffic shaping to ensure their output stays within the contract and is thus not discarded. Traffic exceeding a traffic contract may be discarded immediately, marked as non-compliant, or left as-is, depending on administrative policy and the characteristics of the excess traffic."

upvoted 1 times

EthanhuntMI6 5 months, 2 weeks ago

Selected Answer: A

Most ISPs will configure policing to drop all traffic above 10 Mbit so that you can't get more bandwidth than what you are paying for. It's also possible that they shape it down to 10 Mbit but shaping means they have to buffer data while policing means they can just throw it away.

https://networklessons.com/quality-of-service/qos-traffic-shaping-explained

upvoted 2 times

yong08321 5 months, 3 weeks ago

Selected Answer: D

It's D shaping whenever there is bandwidth

upvoted 2 times

Panda_man 5 months, 3 weeks ago

Selected Answer: D

It's D shaping whenever there is bandwidth

upvoted 1 times

SemStrond 7 months ago

Selected Answer: D

Why isnt it D?
Shapping Traffic shaping (or packet shaping) is a technique of limiting the bandwidth that can be consumed by certain applications to ensure high performance for critical applications.

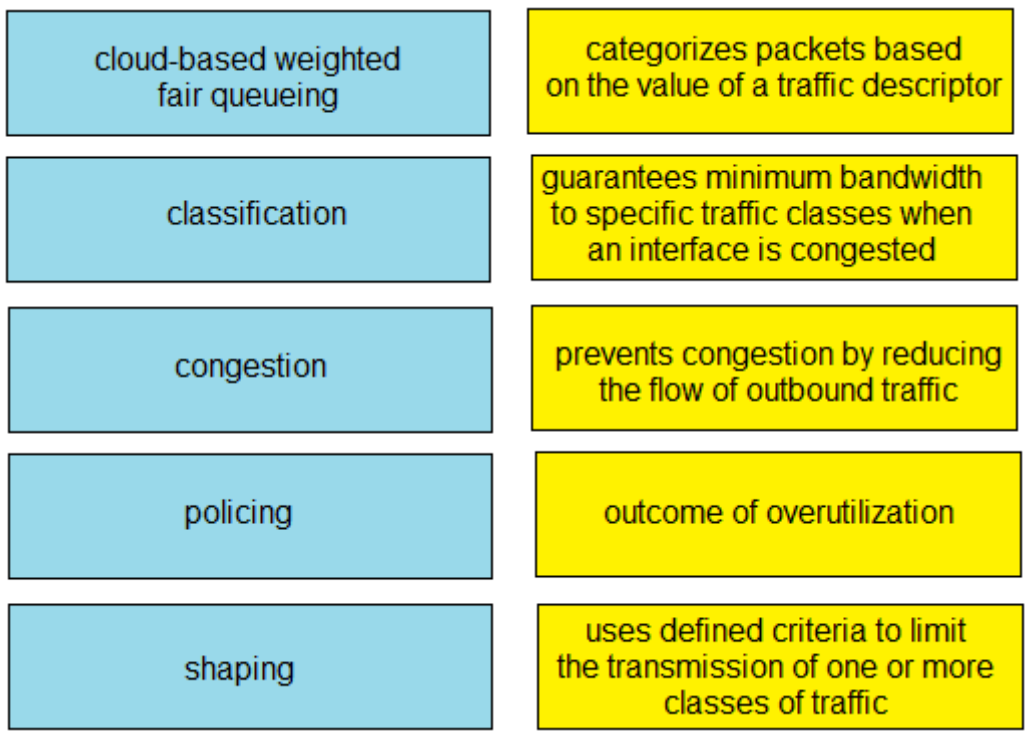
upvoted 2 times

Question #586 *Topic 1*

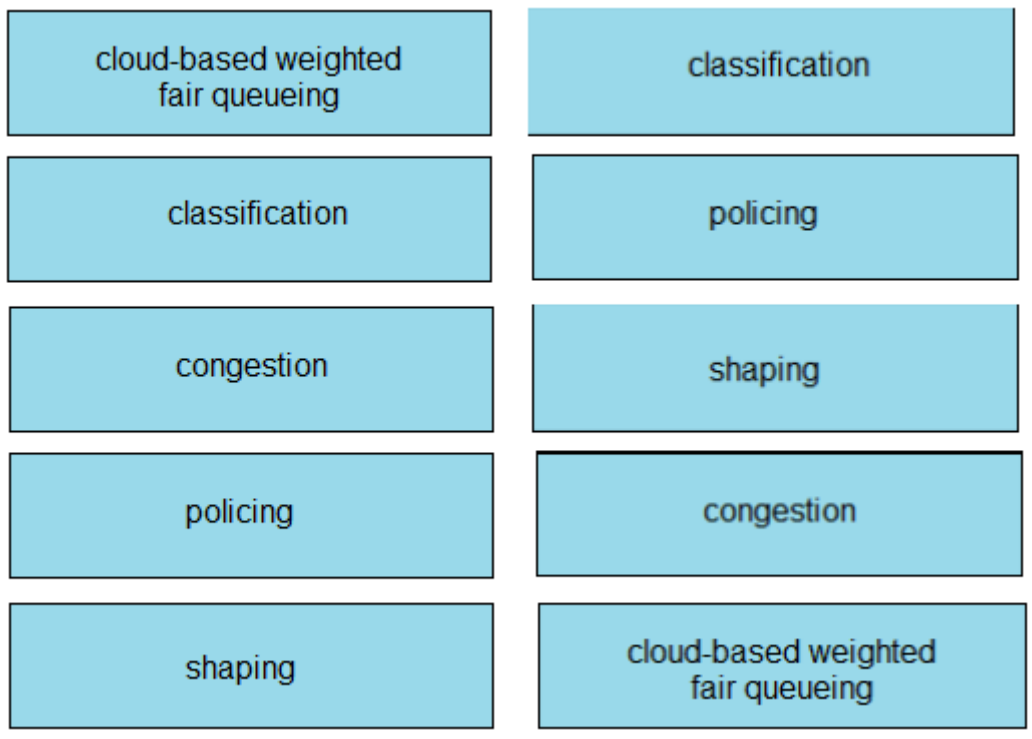
DRAG DROP -

Drag and drop the QoS terms from the left onto the descriptions on the right.

Select and Place:



Correct Answer:



RougePotatoe Highly Voted 7 months, 1 week ago

1.classification
2.cloud based weighted fair queueing = "to guarantee a minimum amount of bandwidth to each class" OCG vol 2 ch11
3.policing = Discard messages
4.congestion
5.shaping = que traffic for non priority packets

My distain of Cisco grows everyday.

upvoted 14 times

EthanhuntMI6 5 months, 2 weeks ago

I think 5 should be policing not shaping.

upvoted 7 times

jonathan126 1 month, 1 week ago

But with shaping, congestion is still there, shaping just put the traffic into a queue, so it cannot prevent congestion

upvoted 1 times

Anon1216 Highly Voted 8 months, 2 weeks ago

Shouldn't cloud-based wighted fair queueing and policing be swapped?

upvoted 11 times

Lance789 7 months, 3 weeks ago

Class-based weighted fair queueing (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces.

https://www.cisco.com/en/US/docs/ios/12_0t/12_0t5/feature/guide/cbwfq.html#wp17641

I think the answers given are correct
upvoted 3 times

EliasM 7 months, 2 weeks ago
I do not believe that "Policing" guarantees traffic bandwidth. Its used by ISP to avoid oversuscription. It drops traffic or remarks it, i dont think its intended to guarantee anything. Correct me if im wrong, but i agree with Anon.
upvoted 6 times

gewe Most Recent 3 months, 3 weeks ago
from top to bottom:
classification
class based weighted fair queueing
shaping
congestion
policing
upvoted 10 times

dropspablo 1 week, 1 day ago
Correct
upvoted 1 times

bisiyemo1 1 month ago
This is very correct
upvoted 1 times

splashy 8 months, 2 weeks ago
bandwidth = policing + shaping
limit transmission = by putting in a que
upvoted 2 times

Question #587 *Topic 1*

Which remote access protocol provides unsecured remote CLI access?

A. console

B. Telnet

C. SSH

D. Bash

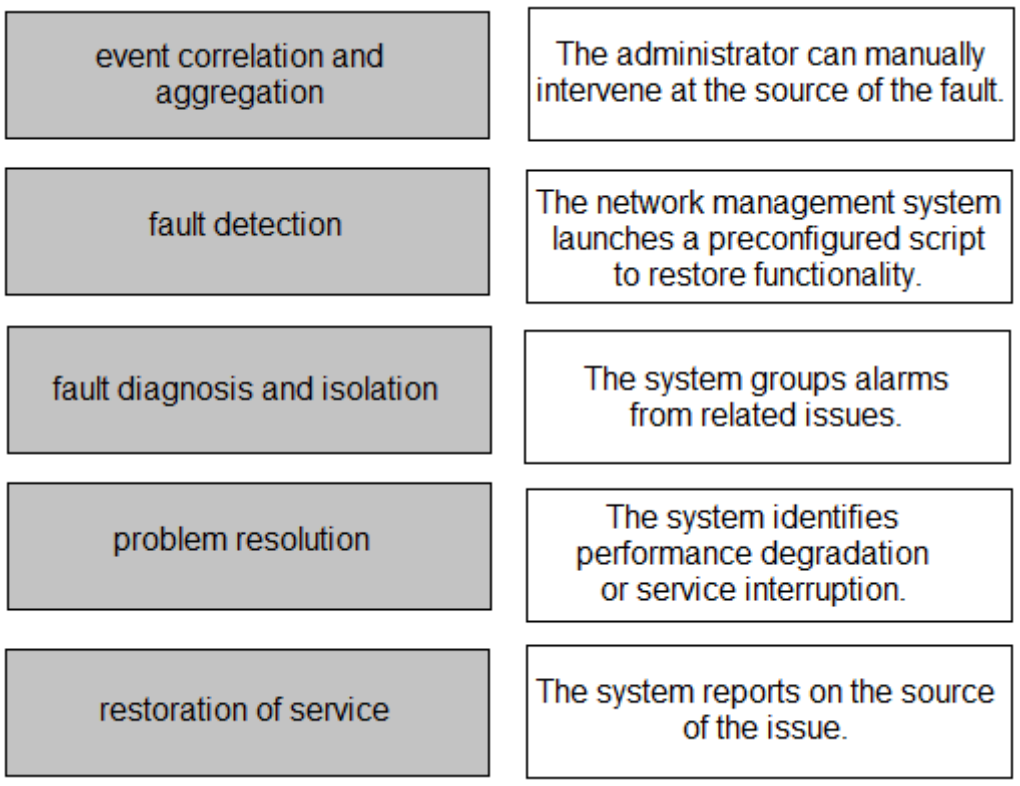
Correct Answer: *B*

Question #588 *Topic 1*

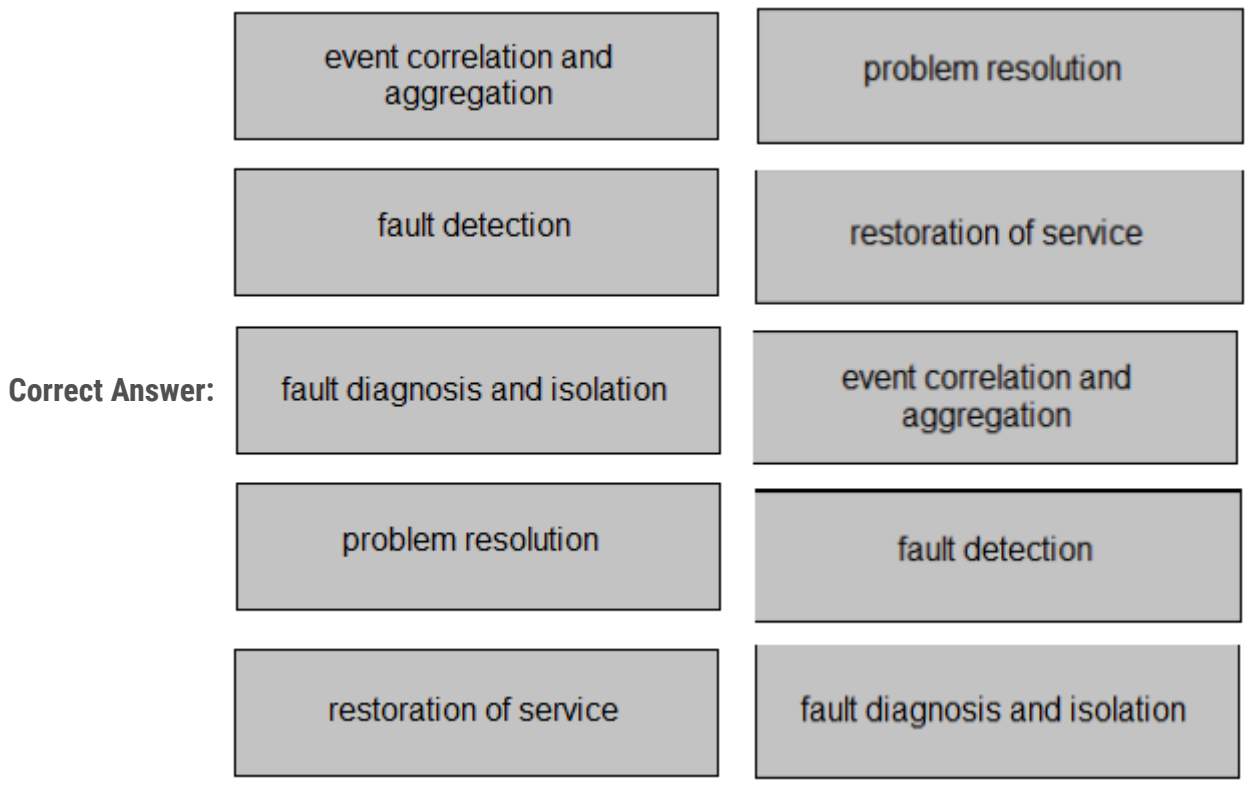
DRAG DROP -

Drag and drop the functions of SNMP fault-management from the left onto the definitions on the right.

Select and Place:



Correct Answer:



Tamirkadosh Highly Voted 8 months ago

wth is that bro

upvoted 24 times

EthanhuntMI6 Highly Voted 6 months ago

No idea what this is, but not expecting anything great from cisco.

upvoted 7 times

gewe Most Recent 3 months, 3 weeks ago

just a basic understanding how SNMP works. thank you very very much. / now I know everything

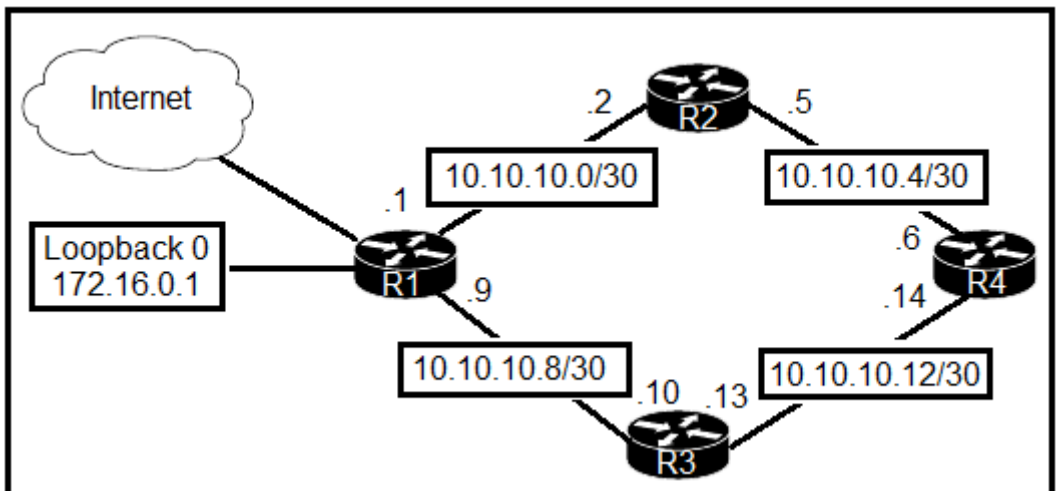
upvoted 3 times

EthanhuntMI6 5 months, 2 weeks ago

I think 'problem resolution' and 'fault diagnosis and isolation' need to be swapped.

upvoted 5 times

Question #589 *Topic 1*




```
R1#show run | include ntp
ntp master 7
ntp server 209.165.200.225

R2#show run | include ntp
ntp server 172.16.0.1

R3#show run | include ntp
ntp master 6
ntp server 172.16.0.1

R4#show run | include ntp
ntp master 7
```

Refer to the exhibit. Which router or router group are NTP clients?

A. R1

B. R2 and R3

C. R1, R3, and R4

D. R1, R2, and R3

Correct Answer: *D*

dropspablo 1 week, 1 day ago

Selected Answer: D

Correct

upvoted 1 times

Swiz005 1 month, 3 weeks ago

Selected Answer: A

Isn't this A?

upvoted 1 times

RougePotatoe 7 months, 1 week ago

Selected Answer: D

Pretty sure you have to have the NTP server configured before you can be a client

upvoted 4 times

Question #590 *Topic 1*

```
CPE1# show protocols e0/1
Ethernet0/1 is up, line protocol is up
  Internet address is 10.0.12.2/24

CPE1# show ip access-list LAN
Standard IP access list LAN
   10 permit 10.0.12.0, wildcard bits 0.0.0.255

CPE1# show ip nat translations

CPE1# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
Inside interfaces:
   Ethernet0/1
Hits: 0 Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
- - Inside Source
[Id: 1] access-list LAN pool NATPOOL refcount 0
   pool NATPOOL: netmask 255.255.255.0
     start 198.51.100.11 end 198.51.100.20
     type generic, total addresses 10, allocated 0 (0%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Refer to the exhibit. What is the next step to complete the implementation for the partial NAT configuration shown?

A. Modify the access list for the internal network on e0/1.

B. Reconfigure the static NAT entries that overlap the NAT pool.

C. Apply the ACL to the pool configuration.

D. Configure the NAT outside interface.

Correct Answer: *B*

splashy Highly Voted 8 months, 2 weeks ago

Selected Answer: D

There are no static entries?
There also is no outside interface defined?
So D

upvoted 10 times

creaguy Highly Voted 8 months, 1 week ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-16/nat-xe-16-book/iadnat-addr-consv.html#:~:text=ip%20nat%20pool%20net%2D208%20172.31.233.208%20172.31.233.223,inside%0A!%0Aaccess%2Dlist%201%20permit%2010.114.11.0%200.0.0.255

upvoted 5 times

Anas_Ahmad Most Recent 5 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

rijstraket 5 months, 4 weeks ago

Selected Answer: D

The outside interface isn't defined, so D.

upvoted 2 times

Question #591 *Topic 1*

What is a syslog facility?

A. host that is configured for the system to send log messages

B. password that authenticates a Network Management System to receive log messages

C. group of log messages associated with the configured severity level

D. set of values that represent the processes that can generate a log message

Correct Answer: *D*

deluxeccna 1 month, 2 weeks ago

Selected Answer: C

The correct answer is C.

A syslog facility is a group of log messages that are associated with a particular configured severity level. Syslog facilities are used to categorize log messages so that they can be filtered and managed more easily. The severity level of a log message determines how important the message is and how it should be handled.

Option A is incorrect because it describes a syslog host, which is a device that is configured to receive and store syslog messages from other devices.

Option B is incorrect because it describes a password used to authenticate a Network Management System (NMS) to receive log messages, which is not related to syslog facilities.

Option D is incorrect because it describes the syslog process, which is a set of values that represent the processes that can generate a log message, but it is not the same as a syslog facility.

upvoted 1 times

RougePotatoe 6 months, 3 weeks ago

Selected Answer: D

The Facility value is a way of determining which process of the machine created the message.
https://success.trendmicro.com/solution/TP000086250-What-are-Syslog-Facilities-and-Levels

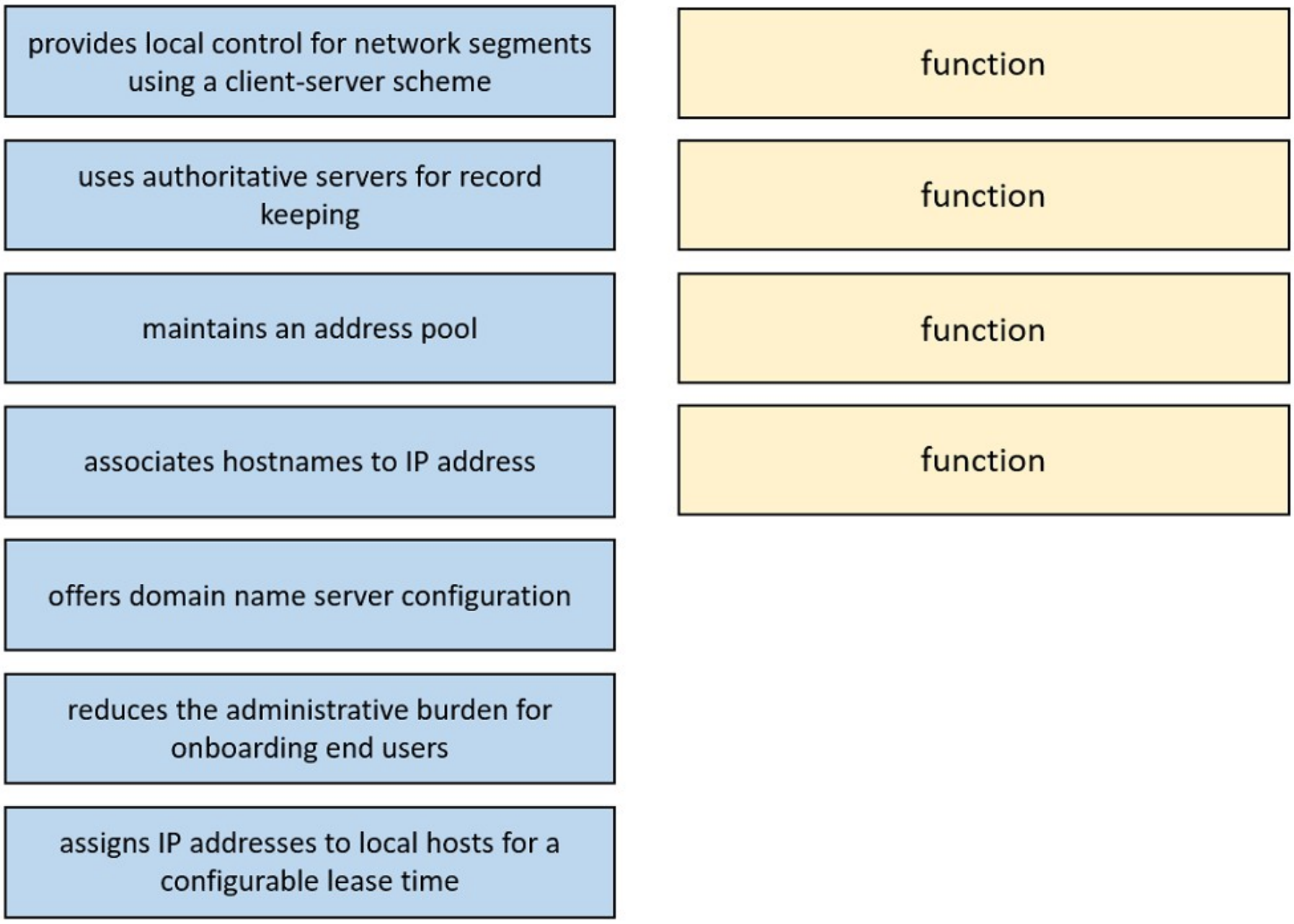
upvoted 4 times

Question #592 *Topic 1*

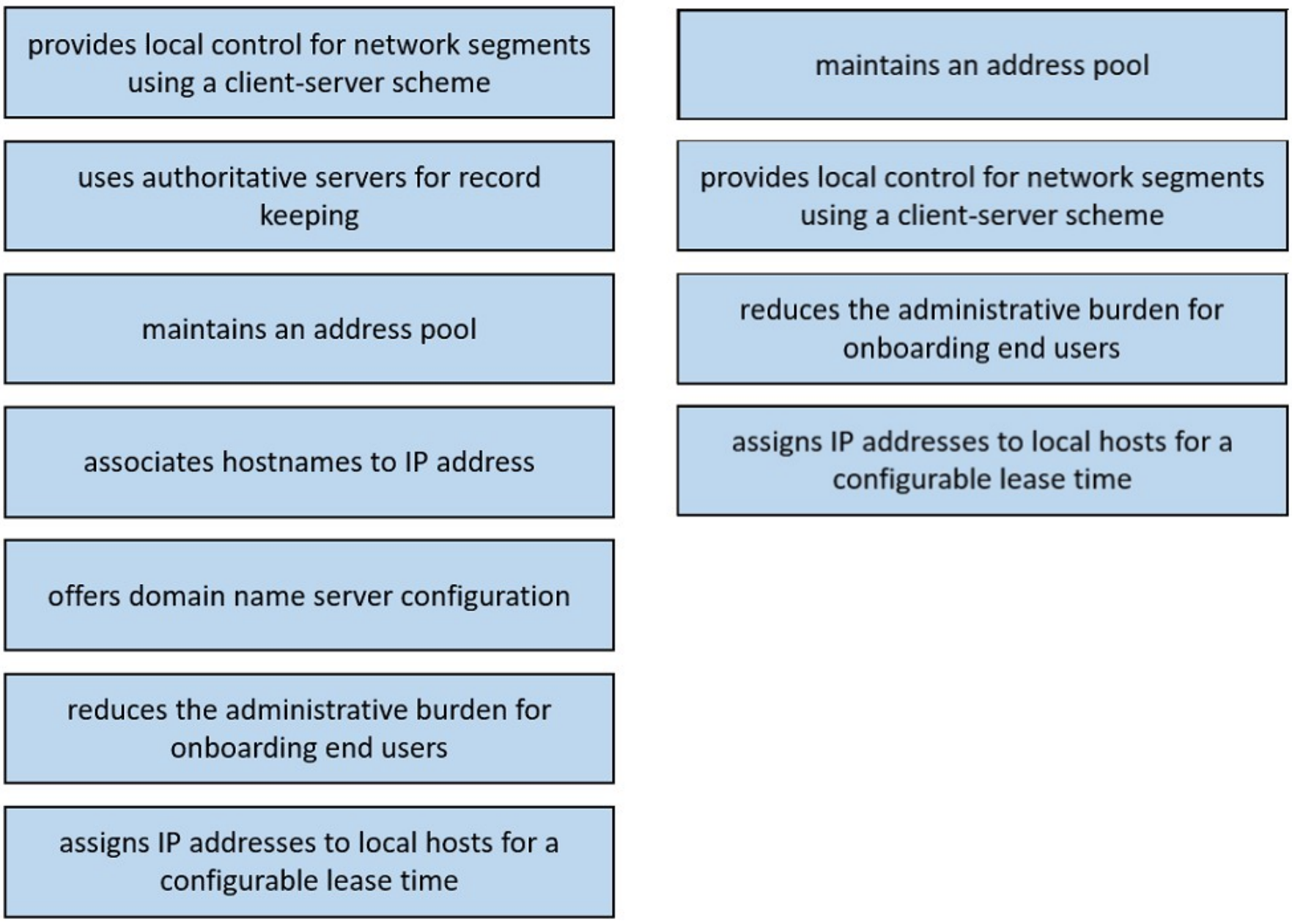
DRAG DROP -

Drag and drop the functions of DHCP from the left onto any of the positions on the right. Not all functions are used.

Select and Place:



Correct Answer:



GigaGremlin Highly Voted 8 months ago

Yes,... I agree...
* Provides local control for network segments...
is wrong
Should be this one
* offers DNS config

upvoted 14 times

DUMPledore Highly Voted 4 months, 2 weeks ago

Maintains an address pool
Offers domain name server configuration
Reduces the administrative burden for onboarding end users
Assigns IP addresses to local hosts for a configurable lease time

upvoted 6 times

dropspablo 1 week ago

I agree

upvoted 1 times

dropspablo 1 week ago

In factidit, I believe it is:
- provides local control for network segments using a client-server scheme.
- maintains an address pool.
- reduces the administrative burden for onboarding end users.
- assigns IP addresses to local hosts for a configurable lease time.

- Offers domain name server configuration.
(...assigning a DNS server is optional, but not necessarily a primary function of using DHCP.)

https://community.cisco.com/t5/network-management/ccna-question-function-of-dhcp/m-p/4475431#M141997

upvoted 1 times

dropspablo Most Recent 1 week ago

Actually the given answers are correct:
- provides local control for network segments using a client-server scheme.
- maintains an address pool.
- reduces the administrative burden for onboarding end users.
- assigns IP addresses to local hosts for a configurable lease time.
wrong
- use authoritative servers for record keeping.

(From what I've seen, after trying to figure it out, although DHCP is used to dynamically assign network settings, it's not common to refer to a DHCP server as an authoritative server for registration. Is more common to use this nomenclature, in view of CCNA, for DNS servers - such as the NS that hosts the domain name, and NTP server (master role), correct me if I'm wrong.
- Offers domain name server configuration.
(...assigning a DNS server is optional, but not necessarily a primary function of using DHCP.)
https://community.cisco.com/t5/network-management/ccna-question-function-of-dhcp/m-p/4475431#M141997

upvoted 1 times

RougePotatoe 6 months, 3 weeks ago

Does anyone even know what they are referring to when they say provides local control to network segments?

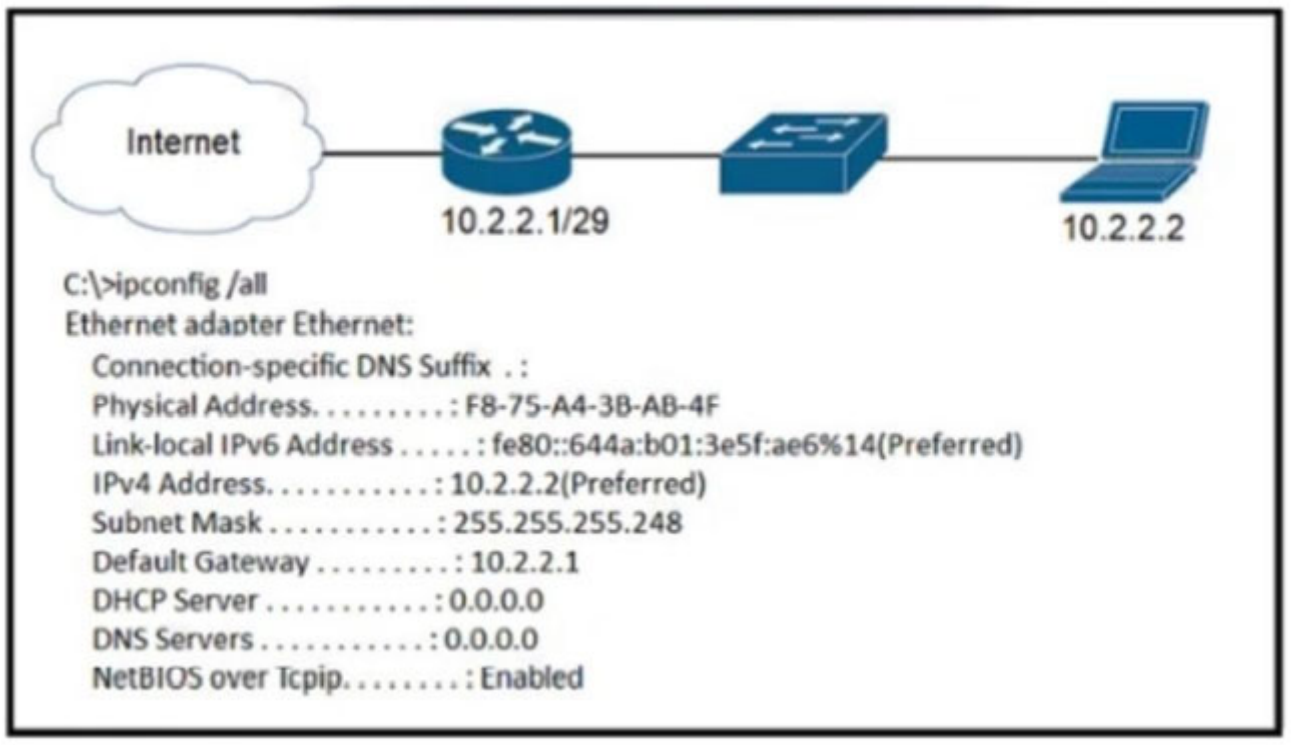
upvoted 2 times

EliasM 8 months ago

Why not offers domain names server configuration?

upvoted 5 times

Question #593 *Topic 1*



Refer to the exhibit. A newly configured PC fails to connect to the internet by using TCP port 80 to www.cisco.com. Which setting must be modified for the connection to work?

A. Subnet Mask

B. DNS Servers

C. Default Gateway

D. DHCP Servers

Correct Answer: *B*

StingVN 2 weeks, 5 days ago

Selected Answer: B

connect internet. of course it should be DNS server. easy peasy.

upvoted 1 times

papinski 3 months ago

Wish all questions were as easy as this

upvoted 1 times

gewe 3 months, 3 weeks ago

bit tricky... you have to really really careful with choosing correct answer. don't be so fast with choosing questions as I m . I did mistake of course when I have seen no DHCP. but yeah BBB is correct

upvoted 1 times

alejandro12 6 months, 2 weeks ago

b is correct

If you see, there is a configuration on pc, there you can configure the dns servers; no dhcp servers

upvoted 2 times

creaguy 8 months, 1 week ago

Selected Answer: B

.....Duh !

upvoted 2 times

Question #594 *Topic 1*

Which QoS queuing method discards or marks packets that exceed the desired bit rate of traffic flow?

A. CBWFQ

B. policing

C. LLQ

D. shaping

Correct Answer: *B*
Use the police command to mark a packet with different quality of service (QoS) values based on conformance to the service-level agreement.
Traffic policing allows you to control the maximum rate of traffic transmitted or received on an interface.
Reference:
https://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/12_2sr/qos_12_2sr_book/traffic_policing.html

KoreaSpurs 7 months, 3 weeks ago
some websites said the answer is LLQ. I think the answer should be policing, but 'which queueing method' made me confused jeez
upvoted 1 times

splashy 8 months, 1 week ago
Selected Answer: B
This one made me read the entire QOS chapter again (netacad module 3 chapter 9), because of the way the question is asked...

"discards or (re)marks packets" -> definitely policing

But it never buffers.

So for me based on what you see in ccna it's defnitely not a Queuing method/algo, it's a congestion avoidance tool.
upvoted 1 times

RougePotatoe 7 months, 1 week ago
CBWFQ can be configured to mark or drop specific traffic but it isn't on be default.
https://www.cisco.com/en/US/docs/ios/12_0t/12_0t5/feature/guide/cbwfq.html#:~:text=CBWFQ%20allows%20you%20to%20specify,case%20with%20flow%2Dbased%20WFQ.

LLQ doesn't seem to mark anything, IE record it, so the answer is probably CBWFQ even though you have to configure it?
https://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/12_2sr/qos_12_2sr_book/llq_for_ipsec.html
upvoted 1 times

Question #595 *Topic 1*

Which QoS per-hop behavior changes the value of the ToS field in the IPv4 packet header?

A. Shaping

B. Policing

C. Classification

D. Marking

Correct Answer: *D*

RougePotatoe 7 months, 1 week ago

It seems like this is correct? I don't see how this is CCNA level...
https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html#anc22

upvoted 1 times

RougePotatoe 7 months, 1 week ago

Yes it is correct.
Marking is a method that you use to modify the QoS fields of the incoming and outgoing packets. The QoS fields that you can mark are IPprecedence and differentiated services code point (DSCP) in Layer 3. The QoS group is a label local to the system to which you can assign intermediate marking values. You can use the QoS group label to determine the egress scheduling.
DSCP is the equivalent to ToS but it interprets the field differently.
https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/101x/configuration/qos/cisco-nexus-9000-nx-os-quality-of-service-configuration-guide-101x/m-configuring-marking.pdf
https://linuxreviews.org/Type_of_Service_(ToS)_and_DSCP_Values

upvoted 2 times

Question #596 *Topic 1*

What is the function of FTP?

A. Always operated without user connection validation

B. Uses block number to identify and mitigate data-transfer errors

C. Relies on the well-known UDO port 69 for data transfer

D. Uses two separate connections for control and data traffic

Correct Answer: *D*

papibarbu 4 months, 3 weeks ago

port 20 and 21 OK

upvoted 3 times

Question #597 *Topic 1*

How does TFTP operate in a network?

A. Provides secure data transfer

B. Relies on the well-known TCP port 20 to transmit data

C. Uses block numbers to identify and mitigate data-transfer errors

D. Requires two separate connections for control and data traffic

Correct Answer: *C*

RougePotatoe Highly Voted 7 months, 1 week ago

Selected Answer: C

Seems correct as a,b,d makes no sense.

Block Number : The Block Number field on Data Packets starts with one and then increase sequentially by one for each new packets. This type of numbering allows TFTP applications to identify between new DATA packets and duplicates.
https://www.omnisecu.com/tcpip/tftp-data-packet.php#:~:text=Block%20Number%20%3A%20The%20Block%20Number,from%200%20to%20512%20bytes.

upvoted 5 times

tawanda_belkis Most Recent 1 month, 4 weeks ago

uses block numbers to identify and mitigate data transfer errors

upvoted 1 times

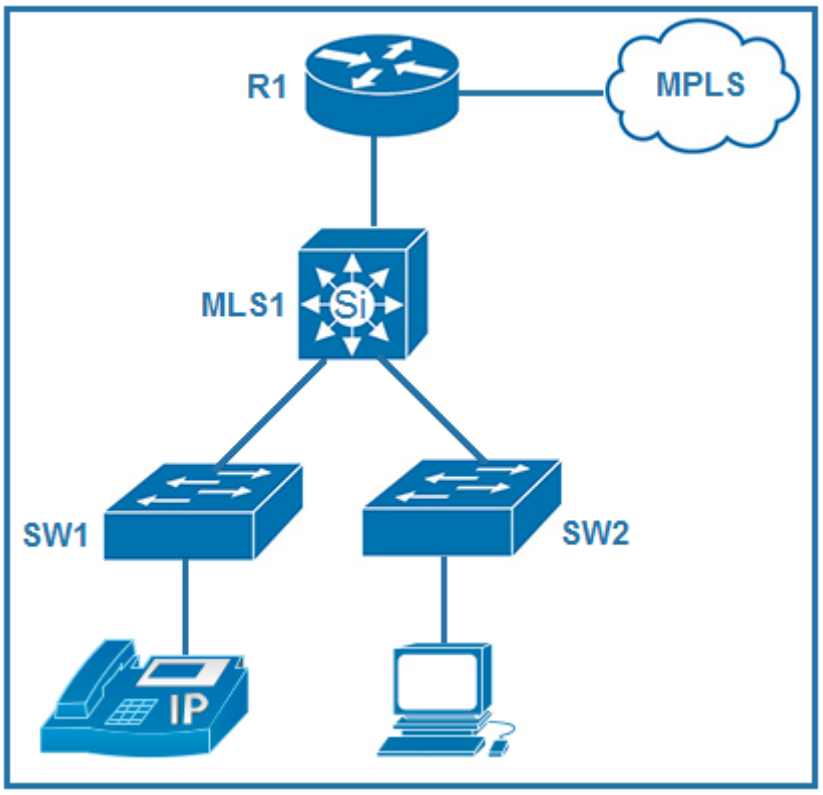
Yannik123 1 month, 4 weeks ago

Selected Answer: C

The answers A, B and D are features of FTP not TFPT so answer C is the only correct one.

upvoted 1 times

Question #598 *Topic 1*



Refer to the exhibit. Which plan must be implemented to ensure optimal QoS marking practices on this network?

A. Trust the IP phone markings on SW1 and mark traffic entering SW2 at SW2

B. As traffic traverses MLS1 remark the traffic, but trust all markings at the access layer

C. Remark traffic as it traverses R1 and trust all markings at the access layer.

D. As traffic enters from the access layer on SW1 and SW2, trust all traffic markings.

Correct Answer: *A*
Tell the switch to trust CoS markings from a Cisco IP phone on the access port. Cisco IP phones use 802.1q tags, these .1q tags contain the CoS value, to mark voice traffic at layer 2. When it's forwarded upstream, the DSCP value is trusted (on the uplink port) and unchanged, but the .1q tag (and with it the CoS value) is stripped off by the upstream switch when received over the trunk.

Currently there are no comments in this discussion, be the first to comment!

Question #599 *Topic 1*

How does QoS optimize voice traffic?

A. by reducing bandwidth usage

B. by reducing packet loss

C. by differentiating voice and video traffic

D. by increasing jitter

Correct Answer: *C*

RougePotatoe Highly Voted 7 months, 1 week ago

Selected Answer: B

Key guidelines are
Delay one way: 150ms or less
Jitter: 30ms or less
Loss: 1% or less

From the official cert guide vol 2 Ch11.

upvoted 5 times

bisiyemo1 Most Recent 1 month ago

Selected Answer: B

B is very very correct.

upvoted 1 times

Naghini 4 months, 3 weeks ago

Selected Answer: B

I think B is correct.

upvoted 1 times

Question #600 *Topic 1*

Which QoS tool can you use to optimize voice traffic on a network that is primarily intended for data traffic?

A. WRED

B. FIFO

C. PQ

D. WFQ

Correct Answer: *C*

Phonon 5 months ago

Selected Answer: C

C)Priority Queuing (PQ).

PQ allows you to assign a higher priority to voice traffic, which ensures that voice packets are transmitted before data packets. This helps to minimize delays and jitter in the transmission of voice traffic, which can improve the overall quality of the call. Other QoS tools, such as Weighted Fair Queuing (WFQ) and Weighted Random Early Detection (WRED), can also be used to optimize voice traffic, but PQ is generally the most effective option for this purpose.

upvoted 3 times

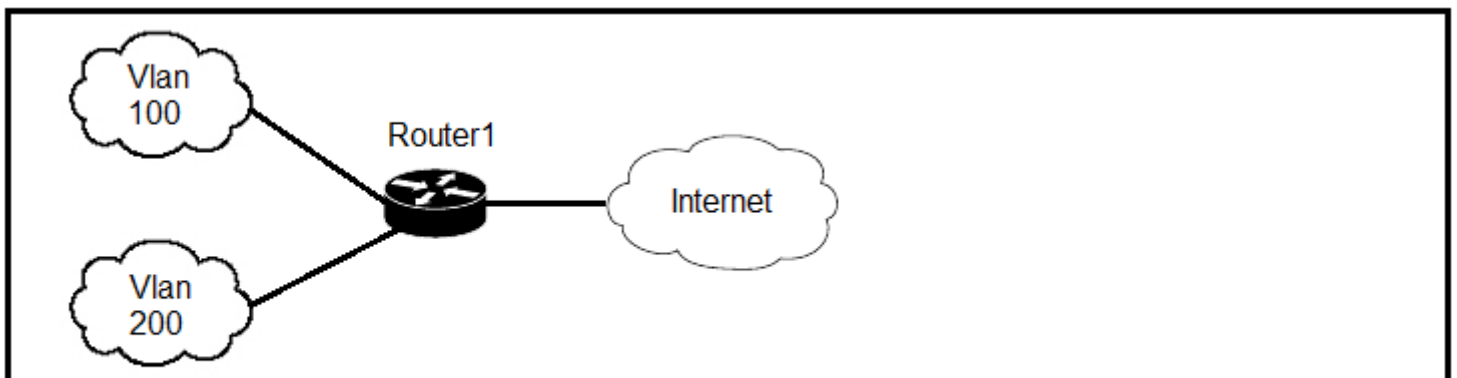
kynnor 1 month, 3 weeks ago

A. WRED - Weighted Random Early Detection
packet droping on Congestion Avoidance mechanism
B. FIFO - First In firt Out

C. PQ - Priorty Queue
D. WFQ - Weight Fair Queue

upvoted 2 times

Question #601 *Topic 1*




```
Router1(config)#interface GigabitEthernet0/0
Router1(config-if)#ip address 209.165.200.225 255.255.255.224
Router1(config-if)#ip nat outside
Router1(config)# interface GigabitEthernet0/1
Router1(config-if)#ip nat inside
Router1(config)# interface GigabitEthernet0/1.100
Router1(config-if)#encapsulation dot1Q 100
Router1(config-if)#ip address 10.10.10.1 255.255.255.0
Router1(config)#interface GigabitEthernet0/1.200
Router1(config-if)#encapsulation dot1Q.200
Router1(config-if)#ip address 10.10.20.1 255.255.255.0
Router1(config)#ip access-list standard NAT_INSIDE_RANGES
Router1(config-std-nac)#permit 10.10.10.0 0.0.0.255
Router1(config)#ip nat inside source list NAT_INSIDE_RANGES interface GigabitEthernet0/0 overload
```

Refer to the exhibit. Users on existing VLAN 100 can reach sites on the Internet. Which action must the administrator take to establish connectivity to the Internet for users in VLAN 200?

A. Define a NAT pool on the router.

B. Configure the ip nat outside command on another interface for VLAN 200

C. Configure static NAT translations for VLAN 200.

D. Update the NAT_INSIDE_RANGES ACL.

Correct Answer: *D*

RougePotatoe Highly Voted 7 months, 1 week ago

Selected Answer: D

D is correct answer because of the following command: "ip nat inside source list NAT_INSIDE_RANGES interfaces G0/0 Overload".
This command essentially tells the router all ip addresses specified from the access list "NAT_INSIDE_RANGES" will be translated via port address translation (PAT) using the ip address of G0/0.
By reconfiguring the ACL to include the 200 vlan it will provide the easiest way to get VLAN 200 access to the internet.

upvoted 10 times

Yannik123 Most Recent 1 month, 3 weeks ago

Selected Answer: D

D is the correct answer. You only need to read the given config in the picture.

upvoted 2 times

Question #602 *Topic 1*

An organization secures its network with multi-factor authentication using an authenticator app on employee smartphones. How is the application secured in the case of a user's smartphone being lost or stolen?

A. The application requires the user to enter a PIN before it provides the second factor

B. The application requires an administrator password to reactivate after a configured interval

C. The application verifies that the user is in a specific location before it provides the second factor

D. The application challenges a user by requiring an administrator password to reactivate when the smartphone is rebooted

Correct Answer: *A*

ac89l 1 month ago
how is this CCNA ?
upvoted 2 times

cormorant 7 months ago
something i know- PIN
something i have - the mobile
upvoted 3 times

creaguy 8 months, 1 week ago
Basically, the authenticator will require you to put a password on you phone.
upvoted 2 times

dipanjana1990 10 months, 1 week ago
That's what happens in GooglePay where you first enter a PIN and after entering the app, and before making the transaction you have to provide the password as a second factor.
upvoted 1 times

RougePotatoe 6 months, 3 weeks ago
That is not MFA. PIN is something you know Password is also something you know. For it to be multi-factor you must have more than 1 factor. In this case you have only demonstrated the use of 1 factor. The 3 categories are something you know, something you have, and something you are. Something you have is like an authentication app or device. Something you are is biometric such as finger printing.
upvoted 3 times

BraveBadger 1 year, 1 month ago
Definitely A, the user is not likely to know the admin pass and a location is not a secure factor, but a pin is a typical factor that a user would know/have.
upvoted 1 times

Rob2000 1 year, 7 months ago
Must be: A
Because B asks for (Administrator Password) which I'm not sure if in this case will be different from: "User Password" and what's more important than that is that B, doesn't mention anything about the "second-factor Authentication"
upvoted 2 times

perrilos 1 year, 8 months ago
Personally, I think the answer is 'B' due to the question stating "how is the application secure after the smartphone is stolen or lost?" The Answer (A) given here does not answer this question.
upvoted 1 times

RougePotatoe 7 months, 1 week ago
Not very realistic as you would need someone who knows the admin password to type it it to employees' phones from time to time. Not very scalable, might work for small businesses though.
upvoted 1 times

Nicocisco 1 year, 3 months ago
If the admin password is entered and the phone is stolen before the time interval ends, it is not secure for that time interval
upvoted 1 times

Question #603 *Topic 1*

Which device performs stateful inspection of traffic?

A. switch

B. firewall

C. access point

D. wireless controller

Correct Answer: *B*

dicksonpwc Highly Voted 1 year, 9 months ago

B is correct.
Explanation:
Stateful inspection, also known as dynamic packet filtering, is a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.

upvoted 10 times

LLAMBRA Highly Voted 1 year, 10 months ago

There are two devices that inspect traffic are the IPS and the Firewall.
In the answer options the IPS does not appear, but the firewall does.
The correct answer is the firewall (B)

upvoted 5 times

DUMPledore Most Recent 4 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

juann 11 months ago

Which device tracks the state of active connections in order to make a decision to forward a packet through?

A. wireless access point
B. firewall
C. wireless LAN controller
D. Router

Correct Answer: C

could you solve this please?

upvoted 2 times

juann 11 months ago

They put the c as correct but I have doubts.

upvoted 1 times

aaaaaaaakkk 10 months, 3 weeks ago

but the answer is b

upvoted 2 times

ROBZY90 2 years, 1 month ago

Stateful refers to the device reading the config from top to bottom

upvoted 4 times

Ali526 2 years, 5 months ago

B is correct.

upvoted 2 times

Question #604 *Topic 1*

A network administrator enabled port security on a switch interface connected to a printer. What is the next configuration action in order to allow the port to learn the MAC address of the printer and insert it into the table automatically?

A. enable dynamic MAC address learning

B. implement static MAC addressing

C. enable sticky MAC addressing

D. implement auto MAC address learning

Correct Answer: *C*

sinear Highly Voted 2 years, 4 months ago

Actually, why couldn't it be B as well ? The mac address does not need to be sticky, it can also be just "dynamic". Sticky adds the learned mac into the running config, what simple dynamic doesn't, but that doesn't prevent the mac to be learned too if it was just "dynamic".

Edit: I think the reason is that we don't have to "enable" dynamic. It is automatically enabled when do run switchport port-security.

upvoted 9 times

imo90s 2 years, 1 month ago

dynamic mac address learning is for associating IPs and MAC addresses of devices in the CAM. It has nothing to do with security. I

upvoted 3 times

D0nkey_h0t 11 months, 3 weeks ago

could you please tell us where have you seen ip addresses in MAC Adress Table? before your comment i believed that MAC Adress Table, which is stored in CAM as you mentioned, contains only MAC adresses and the switch ports associated with them...

upvoted 5 times

Ali526 Highly Voted 2 years, 5 months ago

C is correct (99%). For remaining 1%, please check by Friday.

upvoted 8 times

syslil 1 year, 11 months ago

@ali526 you lier

upvoted 5 times

Acai 2 years ago

You lied to us Ali lol

upvoted 8 times

lucky1559 Most Recent 1 year, 9 months ago

Sticky mode learns MAC automaticaly and saves them to address table AND running config (to save them to startup so they wont be forgotten) while Dymamic mode saves only to address table. But both learns MACs dynamically. Thus both A and C are correct.

upvoted 4 times

dicksonpwc 1 year, 9 months ago

C is correct.
Explanation:
You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling sticky learning. To enable sticky learning, enter the switchport port-security mac-address sticky command

upvoted 2 times

Angel75 1 year, 10 months ago

C is correct... but isn't the syntax something like..."switchport port-security mac-address sticky" ?

upvoted 3 times

D0nkey_h0t 11 months, 3 weeks ago

it's not a command written there, it's the action you are supposed to take

upvoted 2 times

El_Touffiko 1 year, 10 months ago

B is not correct because of the word "automatically"

upvoted 5 times

Question #605 *Topic 1*

```
Switch(config)#hostname R1
R1(config)#interface FastEthernet0/1
R1(config-if)#no switchport
R1(config-if)#ip address 10.100.20.42 255.255.255.0
R1(config-if)#line vty 0 4
R1(config-line)#login
```

Refer to the exhibit. An engineer booted a new switch and applied this configuration via the console port. Which additional configuration must be applied to allow administrators to authenticate directly to enable privilege mode via Telnet using a local username and password?

A. R1(config)#username admin R1(config-if)#line vty 0 4 R1(config-line)#password p@ss1234 R1(config-line)#transport input telnet

B. R1(config)#username admin privilege 15 secret p@ss1234 R1(config-if)#line vty 0 4 R1(config-line)#login local

C. R1(config)#username admin secret p@ss1234 R1(config-if)#line vty 0 4 R1(config-line)#login local R1(config)#enable secret p@ss1234

D. R1(config)#username admin R1(config-if)#line vty 0 4 R1(config-line)#password p@ss1234

Correct Answer: *B*

Ciscoman021 2 months, 2 weeks ago

Selected Answer: B

B is right

upvoted 2 times

alejandro12 6 months, 2 weeks ago

Answer A
Its the unique that enable telnet (transport input telnet)

upvoted 2 times

ike110 3 months, 3 weeks ago

Telnet is enabled by default, so no need to enable it again

upvoted 4 times

Etidic 7 months, 2 weeks ago

Selected Answer: B

The answer is B

upvoted 1 times

Garfieldcat 7 months, 4 weeks ago

question request a privilege execution and password but have not mentioned sec password.
why need to use key word sec instead of password

upvoted 1 times

GigaGremlin 8 months ago

Selected Answer: B

....authenticate directly to enable privilege mode via Telnet using a local username and password

upvoted 2 times

guynetwork 9 months ago

Selected Answer: B

"authenticate directly"

upvoted 2 times

sasquatchshrimp 10 months, 1 week ago

Selected Answer: C

My guess is C
https://community.cisco.com/t5/other-network-architecture/how-do-i-set-telnet-password/td-p/42975

upvoted 2 times

Wilasky 1 year, 1 month ago

Selected Answer: B

Level 15 is exec mode :)

upvoted 1 times

DatBroNZ 1 year, 2 months ago

Selected Answer: B

B is correct.

Level 15 is Privileged Exec Mode, which is what the question is asking about.

upvoted 3 times

TheLorenz 1 year, 2 months ago

Answer is C. You need to configure enable secret command in order to connect to telnet

upvoted 4 times

Question #606 *Topic 1*

Which effect does the aaa new-model configuration command have?

A. It enables AAA services on the device.

B. It configures the device to connect to a RADIUS server for AAA.

C. It associates a RADIUS server to the group.

D. It configures a local user on the device.

Correct Answer: *A*

Samuelpn96 Highly Voted 1 year, 9 months ago

Enabling AAA
To enable AAA, you need to configure the aaa new-model command in global configuration.

https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html

upvoted 13 times

bootloader_jack Highly Voted 1 year, 8 months ago

Bad question I think.

upvoted 7 times

cormorant Most Recent 6 months, 2 weeks ago

Which effete does the aaa new-model configuration command have?

It enables AAA services on the device

the new-model configuration is all about enabling AAA on the device. nothing else

upvoted 1 times

aaaaaaaakkk 11 months, 1 week ago

Configuring AAA on IOS for general administrative access entails four basic steps:
Enable the "new model" of AAA.
Configure the server(s) to be used for AAA (e.g. TACACS+ servers).
Define authentication and authorization method lists.
Enforce AAA authentication on the relevant lines (e.g. console and VTY lines).

upvoted 1 times

kekmaster 1 year, 8 months ago

Does this question have a typo?

upvoted 6 times

jeroenptrs93 1 year, 5 months ago

Effete derives from Latin effetus, meaning "no longer fruitful," and for a brief time in English it was used to describe an animal no longer capable of producing offspring.
Seems like it ;)

upvoted 5 times

Question #607 *Topic 1*

Refer to the exhibit. Which two events occur on the interface, if packets from an unknown Source address arrive after the interface learns the maximum number of secure MAC address? (Choose two.)

```
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Protect
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 4
Total MAC Addresses : 3
Configured MAC Addresses: 1
Sticky MAC Addresses : 2
Last Source Address:Vlan : 0001:0fAA.33BB:1
Security Vioaltion Count : 0
```

A. The security violation counter dose not increment

B. The port LED turns off

C. The interface is error-disabled

D. A syslog message is generated

E. The interface drops traffic from unknown MAC address

Correct Answer: *AE*

BooleanPizza Highly Voted 1 year, 9 months ago

protect—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.

restrict—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the SecurityViolation counter to increment.

shutdown—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

upvoted 28 times

nakres64 Highly Voted 2 years, 4 months ago

correct
Protect – When a violation occurs in this mode, the switchport will permit traffic from known MAC addresses to continue sending traffic while dropping traffic from unknown MAC addresses. When using this mode, no notification message is sent when this violation occurs.

upvoted 9 times

dropspablo Most Recent 6 days, 10 hours ago

Correct Answer A e E.
With protect mode, the only action the switch takes for a frame that violates the port security rules is to discard the frame. The switch does not change the port to an errdisabled state, does not generate messages, and does not even increment the violations counter (Official Cert Guide, V2 pg350).

upvoted 1 times

Goh0503 8 months ago

Answer A and E
https://study-ccna.com/cisco-port-security-violation-configuration/

upvoted 1 times

Mafix 1 year, 3 months ago

Shutdown – After violation, the switchport will be taken out of service and placed in the err-disabled state. The switchport will remain in this state until manually removed.

Protect – After violation, the switchport will permit traffic from known MAC addresses to continue sending traffic while dropping traffic from unknown MAC addresses. When using this mode, no notification message is sent when this violation occurs.

Restrict – After violation occurs, the switchport will permit traffic from known MAC addresses to continue sending traffic while dropping traffic from unknown MAC addresses. However, unlike the protect violation type, a message is also sent indicating that a violation has occurred.

upvoted 3 times

Hodicek 1 year, 6 months ago

PROTECT MODE : B-C-D ARE NOT CORRECT ANSWERS 100%

upvoted 1 times

Jimmy 2 years, 3 months ago

http://cisco.num.edu.mn/CCNA_R&S2/course/module2/2.2.4.4/2.2.4.4.html

upvoted 5 times

Question #608 *Topic 1*

Which technology must be implemented to configure network device monitoring with the highest security?

A. IP SLA

B. syslog

C. NetFlow

D. SNMPv3

Correct Answer: *D*

martco Highly Voted 2 years, 3 months ago

"..device monitoring....highest security"
Netflow although related to security generally is just a data collection protocol whereas the whole point of SNMPv3 is that it's hardened

answer here should be D

upvoted 29 times

Ethiopis Highly Voted 2 years, 3 months ago

Netflow is of course a tremendous security tool. However, at the CCNA level SNMP is used for monitoring. SNMPv3 is the most secured of all.

upvoted 14 times

StingVN Most Recent 2 weeks, 4 days ago

Selected Answer: D

D. SNMPv3

SNMPv3 (Simple Network Management Protocol version 3) is the technology that should be implemented to configure network device monitoring with the highest security. SNMPv3 provides authentication, encryption, and access control, making it the most secure version of SNMP. It allows for secure and encrypted communication between network devices and network management systems, ensuring the confidentiality and integrity of the monitoring data.

upvoted 1 times

kynnor 1 month, 3 weeks ago

From chatGPT :

SNMPv3 (Simple Network Management Protocol version 3) is primarily used for network device management and monitoring. It provides authentication, authorization, and encryption mechanisms to secure SNMP messages. SNMPv3 authentication is based on a shared secret key or digital certificates, while encryption is provided by the use of the Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), or Advanced Encryption Standard (AES).

NetFlow, on the other hand, is a protocol used for network traffic analysis and monitoring. It captures and exports flow data, which includes information about the source and destination IP addresses, ports, protocols, and other metadata. NetFlow doesn't provide authentication or encryption mechanisms on its own, but it can be used in conjunction with other security technologies like VPNs and firewalls to enhance network security.

upvoted 1 times

Dutch012 3 months, 1 week ago

Guys, it's asking about technology not protocol, I would go with C.

upvoted 1 times

[Removed] 11 months ago

Selected Answer: D

Make sense

upvoted 1 times

LilGhost_404 1 year, 3 months ago

Selected Answer: D

SNMPv3 is for device monitoring, Netflow is a flow traffic monitor not a device monitor, your switch's RAM could be at 95% and you wont know that with netflow,

upvoted 2 times

AvroMax 1 year, 3 months ago

Selected Answer: D

D SNMPV3

upvoted 2 times

Cho1571 1 year, 4 months ago

Selected Answer: D

I picked D
upvoted 1 times

RichyES 1 year, 5 months ago
SNMPv3 so D is correct
upvoted 1 times

Nebulise 1 year, 6 months ago
Selected Answer: D
C is not correct
upvoted 1 times

Hodicek 1 year, 6 months ago
snmpv3
upvoted 1 times

babaKazoo 1 year, 6 months ago
Selected Answer: D
Most secure is the key here SNMPv3 is the most secure, so D.
upvoted 1 times

Carter_Milk 1 year, 6 months ago
Protocol Vs Technology?
upvoted 1 times

Hodicek 1 year, 6 months ago
AGREE WITH SNMPv3
upvoted 1 times

bootloader_jack 1 year, 8 months ago
It says "device monitoring". So the answers is D
upvoted 3 times

dicksonpwc 1 year, 9 months ago
NetFlow statistics are useful for several applications. Among the top advantages of using NetFlow are:

Network Monitoring, Network Planning and Security Analysis
Answer should be C
upvoted 1 times

Question #609 *Topic 1*

Refer to the exhibit. Which two statements about the interface that generated the output are true? (Choose two.)

```
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Protect
Aging Time : 5 mins
Aging Type : Inactivity
SecureStatic Addres Aging : Disabled
Maximum MAC Addresses : 3
Total MAC Addreses : 3
Configured MAC Addresses : 1
Sticky MAC Addresses : 2
Last Source Address : Vlan  : 0001.0fAA.33BB:1
Security Violation Count : 0
```

A. learned MAC addresses are deleted after five minutes of inactivity

B. the interface is error-disabled if packets arrive from a new unknown source address

C. it has dynamically learned two secure MAC addresses

D. it has dynamically learned three secure MAC addresses

E. the security violation counter increments if packets arrive from a new unknown source address

Correct Answer: *AC*

Chupacabro Highly Voted 1 year, 5 months ago

B - wrong. only shuts int when violation mode is "shutdown"
D - wrong. dynamically learned only 2 MACADD using sticky command
E - wrong. only increments on "restrict" and "shutdown" violation mode

Answer - A, C

upvoted 7 times

Sal34 Most Recent 1 year ago

Selected Answer: AC

The answer is 100% a and c

upvoted 1 times

Hodicek 1 year, 6 months ago

aging time is 5 minutes
sticky is automatically 2 MACs

upvoted 3 times

Hodicek 1 year, 6 months ago

B-D-E ARE INCORRECT ANSWERS FOR SURE

upvoted 2 times

sp123 1 year, 8 months ago

There really isn't a good second answer here. Technically sticky mac addresses are considered static. That being said, I guess the provided answers are the best choices anyways.

From the Official Cert Guide:

Example 6-4 proves the point. It shows two commands about interface F0/2 from the port security example shown in Figure 6-2 and Example 6-1. In that example, port security was configured on F0/2 with sticky learning, so from a literal sense, the switch learned a MAC address off that port (0200.2222.2222). However, the show mac address-table dynamic command does not list the address and port because IOS considers that MAC table entry to be a static entry. The show mac address-table secure command does list the address and port.

upvoted 2 times

dave1992 1 year, 7 months ago

You're misunderstanding the text. Sticky mac learning works by DYNAMICALLY learning the MAC address traffic is received on the port, the book is saying that the show MAC address table dynamic command doesn't list it because it's configured on port security. The MAC address can be seen if you type in the "show MAC address table secure command"

Sticky MAC addresses NOT static. They ARE dynamic.
upvoted 3 times

syanev 1 year, 10 months ago
I have a question - does the statically configured mac address also diappear after 5 mins of inactivity or just the two dynamically learned?
upvoted 2 times

DaBest 1 year, 8 months ago
it dose only if you use the STATIC commend like this:
"switchport port-security aging static time 5 type inactivity"
upvoted 1 times

Sicko 2 years, 1 month ago
https://community.cisco.com/t5/switching/what-exactly-does-mac-address-sticky-do/td-p/857804

Given Answers are correct.

Sticky MAC ADRESS means that when you reload the Switch the Switch stills save the mac address that was learned DYNAMICALLY.
upvoted 2 times

CiscoTerminator 1 year, 10 months ago
that is not TRUE entirely - if you don't copy run start after the switch has learnt the MACs, and reboot the switch - it will not save them and wont be available after reload.
upvoted 4 times

Kareemelkh 2 years, 3 months ago
C state that it learned two MACs dynamically . Output showed Sticky MAC addresses : 2
upvoted 3 times

ttomer 2 years, 3 months ago
How did it learned DYNAMICALLY? 2 Sticky MACs and 1 configured...
Therefore I conclude they weren't dynamically learned, am I wrong?
upvoted 2 times

imo90s 2 years, 1 month ago
1) Configured means the 1 mac address that was statically configured
2) Sticky means the 2 dynamically learnt
upvoted 11 times

Question #610 *Topic 1*

Refer to the exhibit. Which statement about the interface that generated the output is true?

```
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address : Vlan : 0001.0fAA.33BB:1
Security Violation Count   : 0
```

A. A syslog message is generated when a violation occurs.

B. One secure MAC address is manually configured on the interface.

C. One secure MAC address is dynamically learned on the interface.

D. Five secure MAC addresses are dynamically learned on the interface.

Correct Answer: *B*

C3L4H1R Highly Voted 2 years, 2 months ago

A is incorrect, it does not send syslog message, read this:
http://cisco.num.edu.mn/CCNA_R&S2/course/module2/2.2.4.4/2.2.4.4.html

upvoted 7 times

Sal34 1 year ago

The answer is b. It increases the violation counter in the shutdown state and does not send a syslog message. Thanks, C3L4H1R.

upvoted 2 times

sgashashf 1 year, 3 months ago

This is horribly dated info. All modern sources will tell you that "shutdown" also generates a syslog message.

upvoted 12 times

RougePotatoe 6 months, 3 weeks ago

To back up his claim the following is from the cert guide: "If Example 6-7 had used the restrict violation mode instead of protect, the port status would have also remained in a secure-up state; however, IOS would show some indication of port security activity, such as an accurate incrementing violation counter, as well as syslog messages."

upvoted 2 times

gachocop3 Most Recent 1 year, 2 months ago

isn't A also correct because SNMP trap and Syslog message are generated in shutdown mode?

upvoted 4 times

babaKazoo 1 year, 4 months ago

B is correct.

Why A is wrong for this question:
It is true that when a Shutdown happens it is logged and incremented but in this example the max MAC address limit has not been reached. So the next violation of an unknown MAC address will simply be learned without causing a shutdown.

upvoted 2 times

sgashashf 1 year, 3 months ago

Your logic is flawed. The question doesn't ask what will happen when a new MAC is detected, it asks what will happen when a violation occurs, which implies a 6th MAC is detected. The question is just wrong.

upvoted 8 times

dave1992 1 year, 7 months ago

B is correct, restrict increments the violation counter, and shutdown sends a trap notification to the SNMP manager

upvoted 2 times

imo90s 2 years, 1 month ago

Answer B is correct.
Restrict mode is the only one that generates syslog violation.

upvoted 2 times

Subit123 2 years ago

Restrict: The offending frame is dropped and an SNMP trap and a Syslog message are generated. The security violation causes the violation counter to increment.

Shutdown: The offending frame is dropped. The interface is placed in an error-disabled state and an SNMP trap and a Syslog message are generated.

upvoted 11 times

Sal34 1 year ago

yea the answer is both a and b. it should show select 2 answers.

upvoted 2 times

Sal34 1 year ago

After reading C3L4H1R's post. I think the answer is a.

upvoted 1 times

mrsiafu 2 years, 1 month ago

this question is all over the place...

upvoted 3 times

MM_9 2 years, 4 months ago

B is correct but also A?

upvoted 2 times

GHH 1 year, 6 months ago

They are both correct but something my cisco teacher told me is often on the exam there are multiple correct answers, but you have to choose the one "best" answer. This can mean the most specific correct answer or the most relevant correct answer, etc. In this case I think you chose the one most relevant. So my guess is that because most of the answers are referring to the MAC addresses learned on the interface, B is the better answer.

upvoted 4 times

nakres64 2 years, 4 months ago

I think A is also correct, (if there is a valid SNMP configuration)

upvoted 2 times

FloridaMan88 2 years, 3 months ago

A is correct, but only AFTER all the allowed MAC addresses are learned. As of "now" in the print out only 1 of 5 MAC addresses are learned/ configured, so no violation yet.

upvoted 4 times

hema5tho 1 year, 9 months ago

That doesn't change the duality of the question. A) says when a violation occurs.
And a violation would be 6 Mac addresses under that interface, doesn't matter how many MAC's are there now.

upvoted 4 times

pagamar 1 year, 5 months ago

Agree with hema5tho. A is also correct, as far as I know, despite the CCNA course says Shutdown violation mode does not generate a Syslog message (one error out of many?). But forther investigation is needed; may be this is different among various IOS versions.

upvoted 1 times

Question #611 *Topic 1*

```
ip arp inspection vlan 2
interface fastethernet 0/1
        switchport mode access
        switchport access vlan 2
```

Refer to the exhibit. What is the effect of this configuration?

A. The switch port remains administratively down until the interface is connected to another switch.

B. Dynamic ARP Inspection is disabled because the ARP ACL is missing.

C. The switch port interface trust state becomes untrusted.

D. The switch port remains down until it is configured to trust or untrust incoming packets.

Correct Answer: *C*
Dynamic ARP inspection (DAI) is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks. After enabling DAI, all ports become untrusted ports.

Ebenezer Highly Voted 2 years, 8 months ago
After Dynamic ARP Inspection is applied, by default the interface becomes untrusted.
upvoted 12 times

BooleanPizza Highly Voted 1 year, 9 months ago
Answer is correct, also to make this port trusted you need to add the 'ip arp inpection trust' command on int fa0/1
upvoted 9 times

LTTAM Most Recent 2 years, 5 months ago
Answer is correct. As per Cisco documentation.... " In a typical network configuration for DAI, all ports connected to host ports are configured as untrusted..."

Source: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html
upvoted 3 times

GreatDane 2 years, 7 months ago
"31 Days Before Your CCNA 200-301 Exam"

Page 192.
upvoted 5 times

Question #612 *Topic 1*

What is the difference between AAA authentication and authorization?

A. Authentication identifies and verifies a user who is attempting to access a system, and authorization controls the tasks the user performs.

B. Authentication controls the system processes a user accesses, and authorization logs the activities the user initiates.

C. Authentication verifies a username and password, and authorization handles the communication between the authentication agent and the user database.

D. Authentication identifies a user who is attempting to access a system, and authorization validates the user's password.

Correct Answer: *A*
AAA stands for Authentication, Authorization and Accounting.
☞ Authentication: Specify who you are (usually via login username & password)
☞ Authorization: Specify what actions you can do, what resource you can access
☞ Accounting: Monitor what you do, how long you do it (can be used for billing and auditing)
An example of AAA is shown below:
☞ Authentication: ג€I am a normal user. My username/password is user_tom/learnforeverג€
☞ Authorization: ג€user_tom can access LearnCCNA server via HTTP and FTPג€
☞ Accounting: ג€user_tom accessed LearnCCNA server for 2 hoursג€. This user only uses ג€showג€ commands.

dave1992 Highly Voted 1 year, 7 months ago
Authentication =who?
Authorization= what are they allowed to do?
Account= what did they do ?
upvoted 9 times

ac89l 1 month ago
I like people who are able to simplify things to others :)
Einstein said “If you can't explain it to a six year old, you don't understand it yourself.”
upvoted 1 times

lilbaby2 Highly Voted 2 years, 7 months ago
Any type of authentication conversation means verifying "identity"
upvoted 6 times

StingVN Most Recent 2 weeks, 4 days ago
Selected Answer: A
The correct answer is A. Authentication and authorization are two distinct processes in computer security:

Authentication: This process verifies the identity of a user or entity attempting to access a system or resource. It typically involves presenting credentials such as a username and password, digital certificates, or biometric information. The goal is to ensure that the user is who they claim to be.

Authorization: Once authentication is successful, authorization determines what actions or tasks the authenticated user is allowed to perform. It involves checking the user's privileges and permissions to access specific resources, perform certain operations, or execute particular commands. The goal is to control and limit the actions that a user can take within the system based on their authenticated identity.

So, authentication is about verifying the user's identity, while authorization is about controlling the user's access and actions within the system.
upvoted 1 times

Question #613 *Topic 1*

When configuring a WLAN with WPA2 PSK in the Cisco Wireless LAN Controller GUI, which two formats are available to select? (Choose two.)

A. decimal

B. ASCII

C. hexadecimal

D. binary

E. base64

Correct Answer: *BC*
Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/multi-preshared-key.pdf

SanchezEldorado Highly Voted 2 years, 11 months ago
The reference link in the answer doesn't go anywhere. Here's the correct link:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/config-guide/b_cg82/b_cg82_chapter_01010011.pdf
upvoted 16 times

poovnair Highly Voted 2 years, 8 months ago
If you chose PSK in Step 7, choose ASCII or HEX from the PSK Format drop-down list and then enter a preshared key in the blank text box. WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters. The PSK parameter is a set-only parameter. The value set for the PSK key is not visible to the user for security reasons. For example, if you selected HEX as the key format when setting the PSK key, and later when you view the parameters of this WLAN, the value shown is the default value. The default is ASCII
upvoted 7 times

StingVN Most Recent 2 weeks, 4 days ago
Selected Answer: BC
Both ASCII and hexadecimal formats are commonly used for entering the pre-shared key when configuring a WLAN with WPA2 PSK. These formats allow for easy input and representation of the key in a human-readable form. The other options (decimal, binary, base64) are not typically used for entering pre-shared keys in this context.
upvoted 1 times

DUMPledore 4 months, 2 weeks ago
Selected Answer: BC
B. ASCII
C. hexadecimal
upvoted 2 times

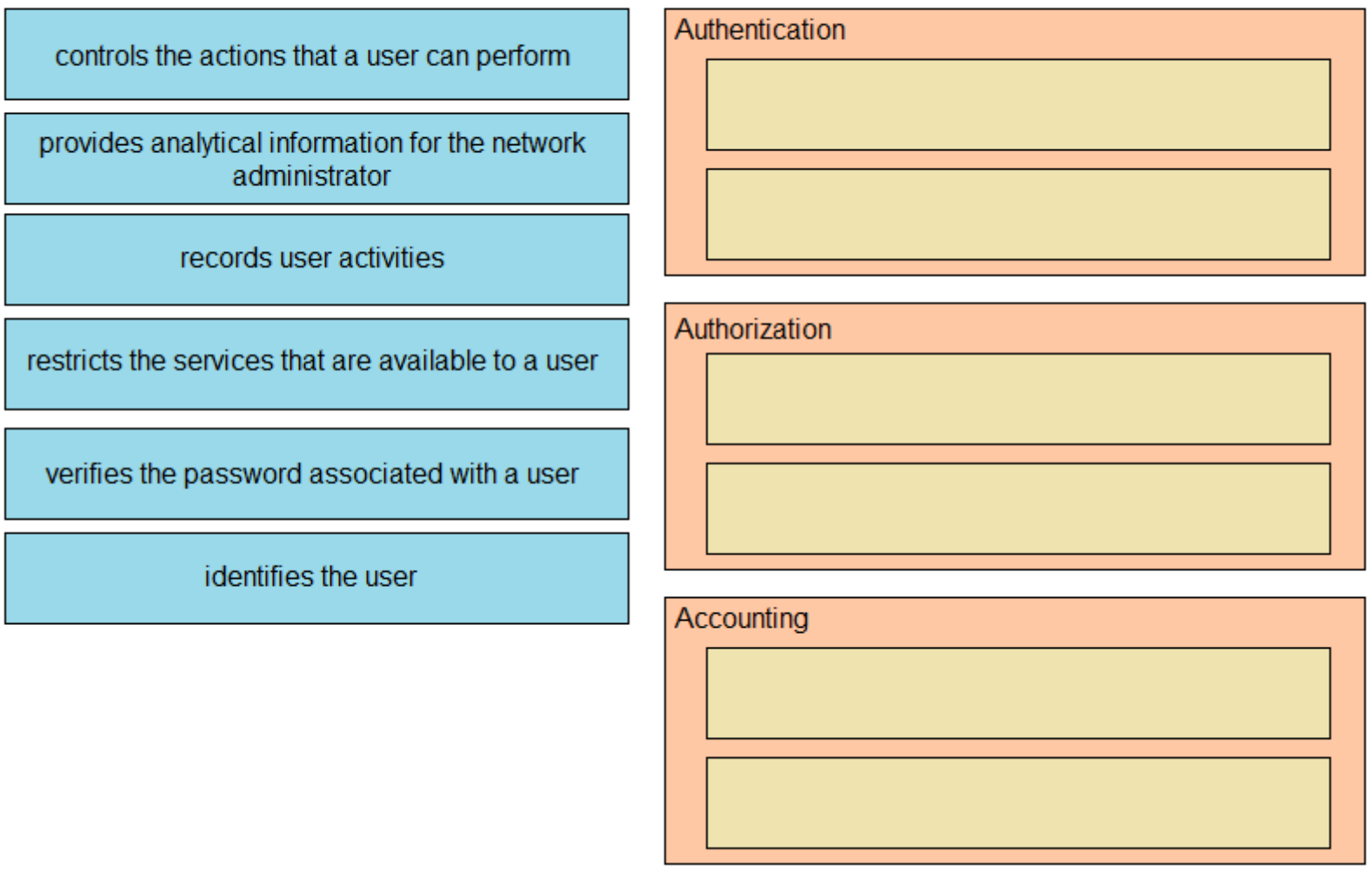
Question #614 *Topic 1*

DRAG DROP -

Drag and drop the AAA functions from the left onto the correct AAA services on the right.

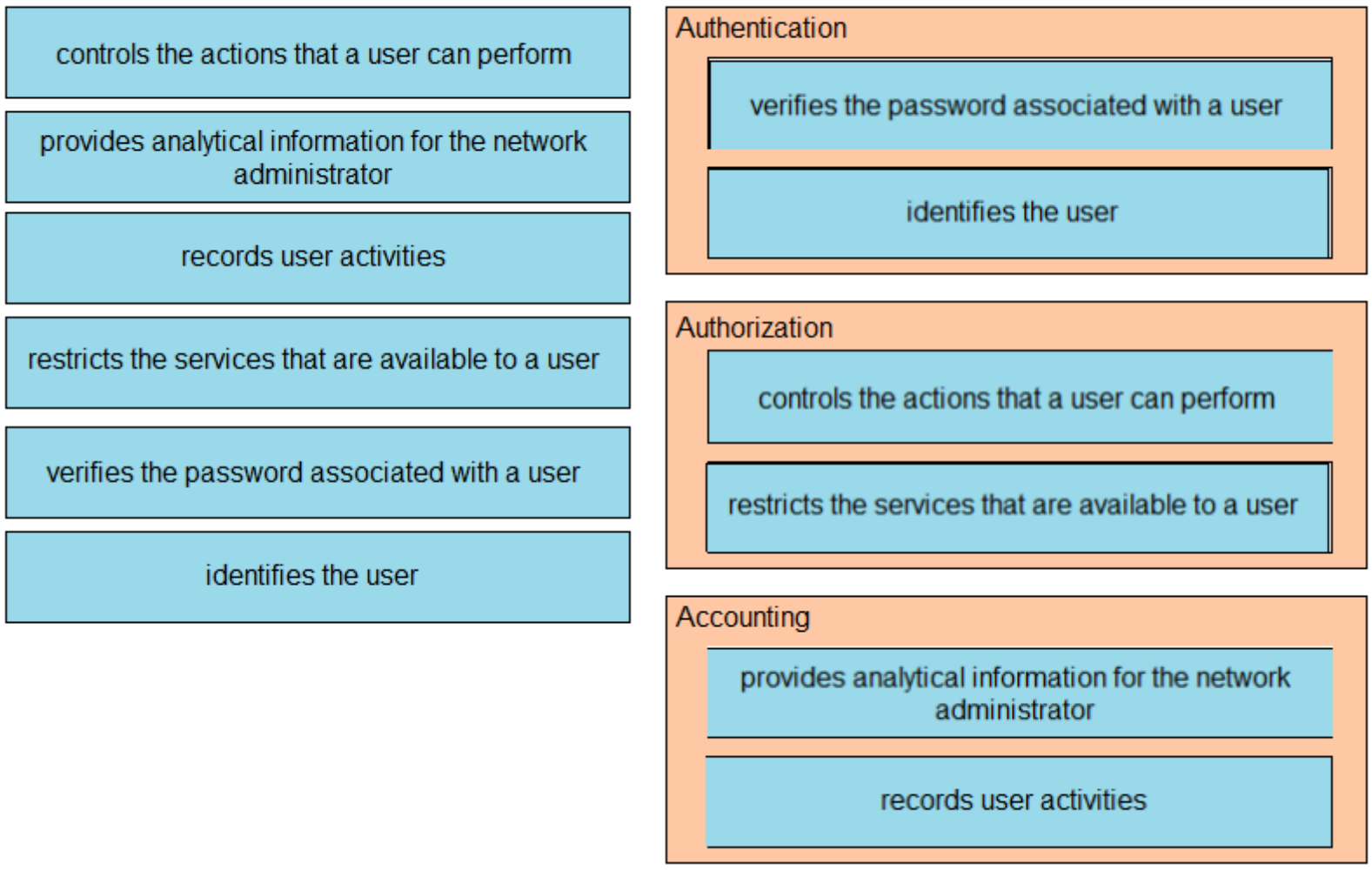
Select and Place:

Answer Area



Correct Answer:

Answer Area



distortion Highly Voted 1 year, 11 months ago

This correct

upvoted 10 times

Question #615 *Topic 1*

An engineer is asked to protect unused ports that are configured in the default VLAN on a switch. Which two steps will fulfill the request? (Choose two.)

A. Configure the ports as trunk ports.

B. Enable the Cisco Discovery Protocol.

C. Configure the port type as access and place in VLAN 99.

D. Administratively shut down the ports.

E. Configure the ports in an EtherChannel.

Correct Answer: *CD*

ZayaB Highly Voted 2 years, 3 months ago

The answer is trying to say is that put the ports into access vlan so that it does not get dtp traffic and put it under an unused vlan that is not in the network, for this example is 99...this is the best practice. Answers C & D is correct.

upvoted 10 times

ac89l 1 month ago

what is dtp traffic?

upvoted 1 times

StingVN Most Recent 2 weeks, 4 days ago

Selected Answer: CD

C. Configuring the port type as access and placing the unused ports in a specific VLAN (such as VLAN 99) ensures that any connected devices will not have access to the default VLAN, thereby protecting it.

D. Administratively shutting down the unused ports completely disables them, preventing any traffic from passing through and enhancing security.

The other options are not directly related to protecting unused ports in the default VLAN:
A. Configuring the ports as trunk ports is used for carrying multiple VLANs across a single link.
B. Enabling the Cisco Discovery Protocol (CDP) is a network protocol used by Cisco devices for discovering and sharing information about neighboring devices.
E. Configuring the ports in an EtherChannel is a technique for bundling multiple physical links into a logical link for increased bandwidth and redundancy.

upvoted 1 times

cormorant 7 months ago

how i miss those questions from 2 years ago. the ccna used to be much easier back then

upvoted 1 times

DoBronx 7 months, 1 week ago

Selected Answer: CD

never use the default vlan and shut it down.

upvoted 4 times

DaBest 1 year, 8 months ago

and i thought vlan 99 is the cisco faivourit for vlan management guess i was wrong ~_~

upvoted 2 times

Acai 2 years ago

I think they might be referring to a Black Hole Vlan as Maxiturne said.

upvoted 2 times

Nhan 2 years, 3 months ago

All port are in vlan 1 by default which everyone known. There for put in ina vlan 99 no body know what is that vlan for, also shit down it is one of the best practice

upvoted 2 times

GA24 2 years, 4 months ago

I assume Vlan 99 in the answer is a VLAN that is not used in production.

upvoted 2 times

uevenasdf 2 years, 8 months ago

C,D - I think it's good practice to change the vlan and shut it down.

upvoted 2 times

Goldsmate 2 years, 9 months ago

I don't understand how configuring the port as an access port and putting it in Vlan 99 (c), protects the port. I chose A and D as my answers.

upvoted 2 times

I_Ninja 2 years, 9 months ago

putting them in access mode and assigning them to an unused vlan is one of the steps to mitigate vlan hopping attacks

upvoted 11 times

Maxiturne 2 years, 9 months ago

The answer C is not complete but the idea is to put the port in access mode in a "blackhole vlan" read an unused vlan without any "issue". Vlan 99 is not a special vlan available on switches for this application, you can use any vlan nummer you want

upvoted 3 times

SanchezEldorado 2 years, 9 months ago

Additionally, setting up a Trunk port would not protect the port. An attacker could simply setup a switch with a trunk to access the rest of the network.

upvoted 3 times

laurvy36 1 year, 4 months ago

all ports are by default in Vlan 1, that is why puting them in another vlan protect the port, not beeing so easy to guest it

upvoted 1 times

Question #616 *Topic 1*

An email user has been lured into clicking a link in an email sent by their company's security organization. The webpage that opens reports that it was safe, but the link may have contained malicious code.
Which type of security program is in place?

A. user awareness

B. brute force attack

C. physical access control

D. social engineering attack

Correct Answer: *A*
This is a training program which simulates an attack, not a real attack (as it says ɹ€The webpage that opens reports that it was safeɹ€) so we believed it should be called a ɹ€user awarenessɹ€ program. Therefore the best answer here should be ɹ€user awarenessɹ€. This is the definition of ɹ€User awarenessɹ€ from CCNA 200-301
Offical Cert Guide Book:
ɹ€User awareness: All users should be made aware of the need for data confidentiality to protect corporate information, as well as their own credentials and personal information. They should also be made aware of potential threats, schemes to mislead, and proper procedures to report security incidents. ɹ€
Note: Physical access control means infrastructure locations, such as network closets and data centers, should remain securely locked.

Daimen Highly Voted 3 years ago
The correct answer is A.
D is a type of attack not a program
upvoted 15 times

myusername66 Highly Voted 3 years ago
Correct Answer: D
upvoted 8 times

CJ32 2 years, 11 months ago
This is a phishing scheme if anything. The security "program" in place is User Awareness. Granted, it's not good awareness, but it is up to the user to protect themselves against the attack.
upvoted 5 times

cant_stop_studying 2 years, 3 months ago
The question asked for the type of security program, not type of attack. Correct Answer is A.
upvoted 5 times

DUMPledore Most Recent 4 months, 2 weeks ago
Selected Answer: A
The correct answer is A.
upvoted 1 times

creaguy 8 months, 1 week ago
Selected Answer: A
My company send phishing emails on purpose. If you click on the link. They make you take a security awareness training :)
upvoted 3 times

Smaritz 1 year, 2 months ago
Almost chose Social Engineering, but A is correct
upvoted 1 times

Shamwedge 1 year, 6 months ago
To me, they don't specify the email was sent by a program, like KnowBe4, in the question. They made it seem like it was sent by a person, so to me that's why I chose Social Engineering. If it was sent by a program, then yes User Awareness is the correct answer.
upvoted 1 times

dave1992 1 year, 7 months ago
If the email was sent by the employees company, but it was a trick, this a USER AWARENESS program. pretty messed up for the security company to send an email with malicious code LOL. A is the correct answer.
upvoted 1 times

02092020 2 years, 8 months ago

It took me a while to understand that de webpage reports: "it was safe, but the link could have contained malicious code."
So the user was informed that the link could contain malicious code -> Answer A.

upvoted 5 times

Krausmiester 2 years, 11 months ago

This was worded oddly too and i admit i answered it wrong too, A is correct

upvoted 4 times

Cheban 2 years, 11 months ago

The correct answer is A

upvoted 2 times

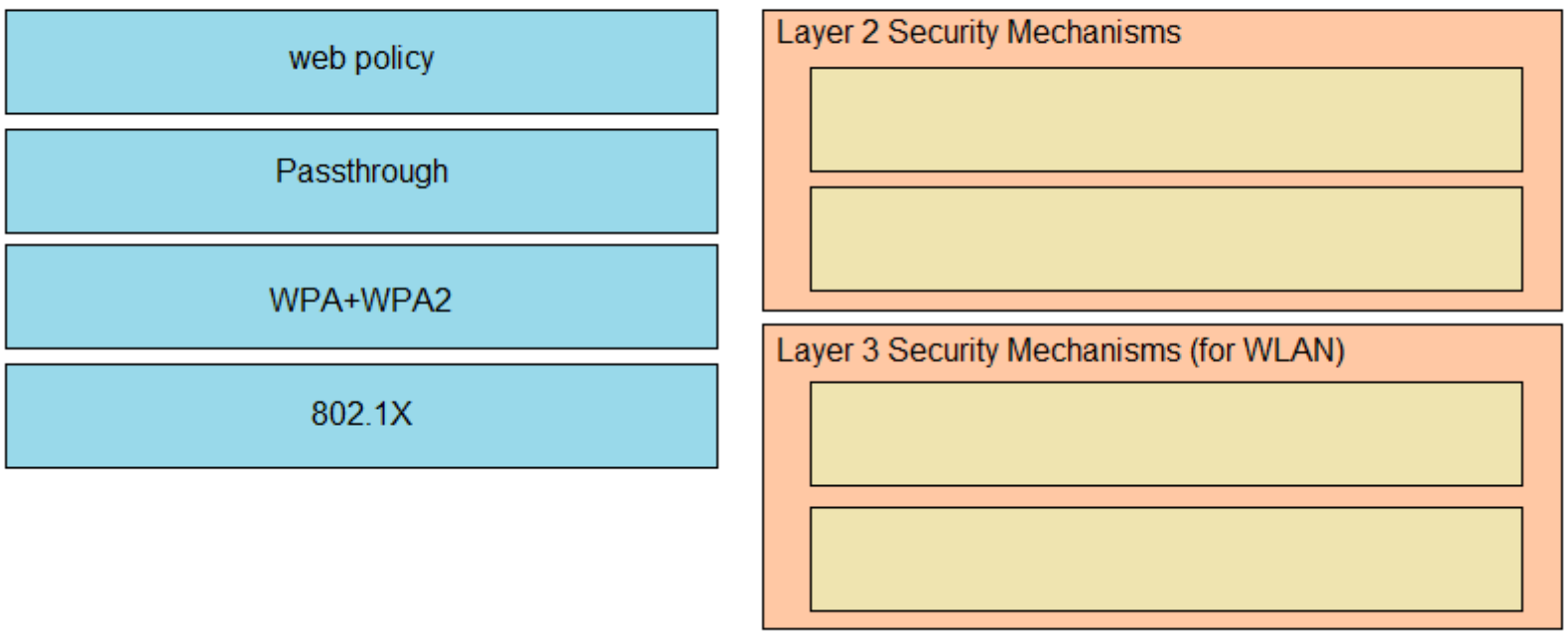
Question #617 *Topic 1*

DRAG DROP -

Drag and drop the Cisco Wireless LAN Controller security settings from the left onto the correct security mechanism categories on the right.

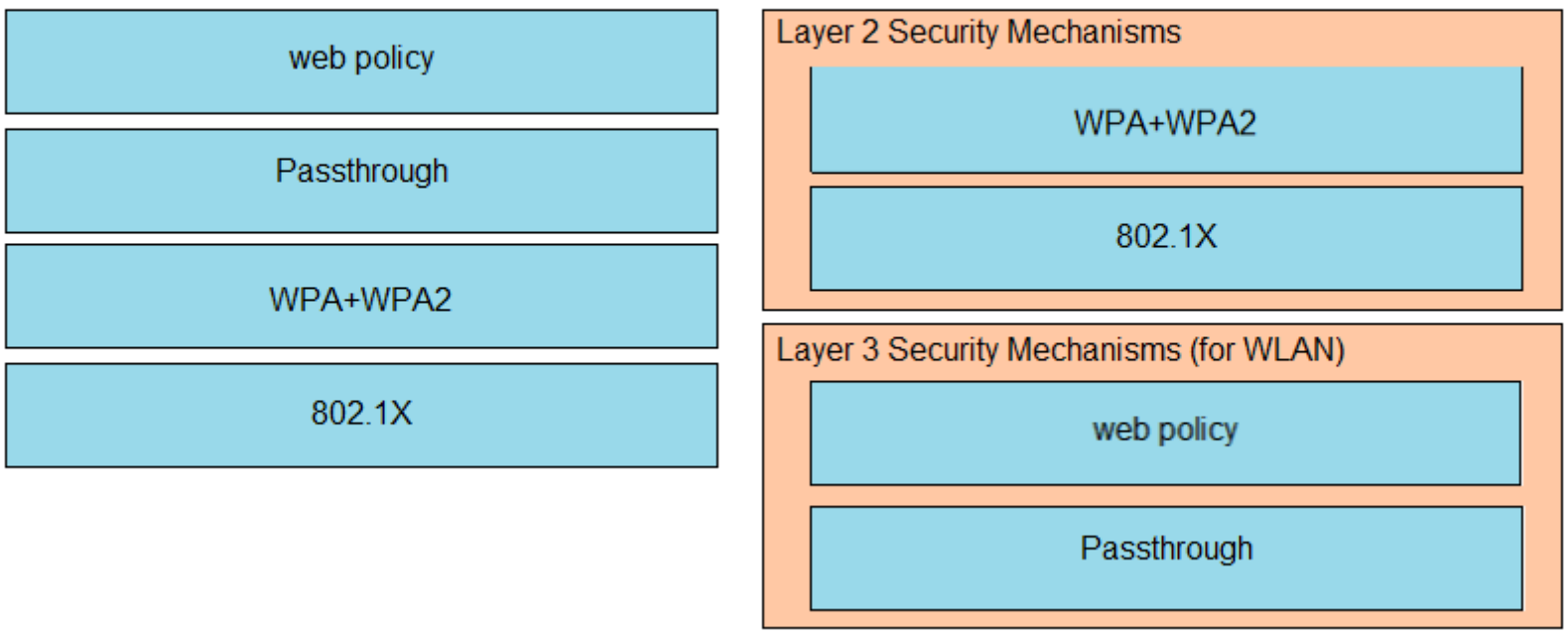
Select and Place:

Answer Area



Correct Answer:

Answer Area



Layer 2 Security Mechanism includes WPA+WPA2, 802.1X, Static WEP, CKIP while Layer 3 Security Mechanisms (for WLAN) includes IPSec, VPN Pass-

Through, Web Passthrough ג€¦

Reference:

https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/106082-wlc-compatibility-matrix.html

Jackie_Manuas12 1 year, 2 months ago

https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/106082-wlc-compatibility-matrix.html

upvoted 4 times

Tintin_06 2 years, 1 month ago

WPA1 2 or 3 are security certifications.
It does set the standards for wireless L2 operations, but it is not a protocol.

https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

(802.11 is hard...)

upvoted 3 times

Question #618 *Topic 1*

Which feature on the Cisco Wireless LAN Controller when enabled restricts management access from specific networks?

A. TACACS

B. CPU ACL

C. Flex ACL

D. RADIUS

Correct Answer: *B*
Whenever you want to control which devices can talk to the main CPU, a CPU ACL is used.
Note: CPU ACLs only filter traffic towards the CPU, and not any traffic exiting or generated by the CPU.
Reference:
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109669-secure-wlc.html

reagan_donald Highly Voted 1 year, 5 months ago
I don't remember if this was even explained in Wendell Odom? But i a sure i have not met this topic on Netacad.....
upvoted 9 times

dropspablo Most Recent 5 days, 2 hours ago
Selected Answer: B
ACLs can only be applied to dynamic interfaces. In WLC firmware version 4.0, there are CPU ACLs that can filter traffic destined for the management interface. (You can only configure CPU ACLs via GUI or CLI).
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71978-acl-wlc.html
upvoted 1 times

StingVN 2 weeks, 4 days ago
Selected Answer: C
C. Flex ACL (Access Control List)

Explanation:
Flex ACL, also known as FlexConnect Access Control List, is a feature on the Cisco Wireless LAN Controller that allows for the enforcement of access control policies for management access to the controller from specific networks. By configuring Flex ACL, you can define rules that determine which networks are allowed or denied access to manage the controller.

The other options are not directly related to restricting management access from specific networks:
A. TACACS (Terminal Access Controller Access Control System) is a security protocol used for centralized authentication, authorization, and accounting (AAA) services.
B. CPU ACL (Central Processing Unit Access Control List) is a feature that allows you to apply access control policies to control traffic destined for the CPU of a network device.
D. RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized authentication, authorization, and accounting for remote access and network services.
upvoted 1 times

mrsiafu 2 years, 1 month ago
SMH on wanting to talk to the main CPU.. I guess after all the other choices, x marks the spot!
upvoted 2 times

karemAbdullah 2 years, 8 months ago
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71978-acl-wlc.html
upvoted 2 times

phu 2 years, 8 months ago
For any traffic to the CPU, for example, management protocols such as SNMP, HTTPS, SSH, Telnet, or network services protocols such as Radius or DHCP, use a “CPU ACL”
upvoted 2 times

Mountie 2 years, 10 months ago
any official link to elaborate the answer ?
upvoted 2 times

DannySprings 2 years, 10 months ago
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109669-secure-wlc.html#t4
upvoted 5 times

Question #619 *Topic 1*

Which set of actions satisfy the requirement for multifactor authentication?

A. The user enters a user name and password, and then re-enters the credentials on a second screen.

B. The user swipes a key fob, then clicks through an email link.

C. The user enters a user name and password, and then clicks a notification in an authentication app on a mobile device.

D. The user enters a PIN into an RSA token, and then enters the displayed RSA key on a login screen.

Correct Answer: *C*
This is an example of how two-factor authentication (2FA) works:
1. The user logs in to the website or service with their username and password.
2. The password is validated by an authentication server and, if correct, the user becomes eligible for the second factor.
3. The authentication server sends a unique code to the user's second-factor method (such as a smartphone app).
4. The user confirms their identity by providing the additional authentication for their second-factor method.

welju Highly Voted 2 years, 11 months ago
multi factor can be 2 of the 3
1. something you know - password, pin
2. something you have - card, badge
3. something you are - retina, voice, facial recognition
upvoted 21 times

johnny1234 Highly Voted 2 years, 11 months ago
Definition of multi-factor- something you know + sth you have
upvoted 6 times

Dataset Most Recent 1 year, 11 months ago
"multifactor" is the magic word
Regards
upvoted 1 times

Boomhower 2 years, 8 months ago
C is correct.
a and d are pretty much the same. As for B, when have you ever seen a link as a multifactor authentication method.
upvoted 2 times

dave369 2 years, 11 months ago
I agree with Zanna. I suspect that the original question must have asked "Which set of actions *does not* satisfy the requirement for multifactor authentication"
upvoted 4 times

Zanna 3 years ago
Actually B C and D are all correct
upvoted 4 times

Question #620 *Topic 1*

Which configuration is needed to generate an RSA key for SSH on a router?

A. Configure VTY access.

B. Configure the version of SSH.

C. Assign a DNS domain name.

D. Create a user with a password.

Correct Answer: *C*

alexiro Highly Voted 2 years, 9 months ago

two conditions must be met before SSH can operate normally on a Cisco IOS switch

The Cisco IOS image used must be a k9(crypto) image in order to support SSH. ""!--- Step 2: Configure the DNS domain of the router.

upvoted 29 times

mustafa007 Highly Voted 2 years, 9 months ago

IOU2(config)#crypto key generate rsa

% Please define a domain-name first.
IOU2(config)#

upvoted 21 times

all4one Most Recent 6 days, 19 hours ago

Selected Answer: C

C is correct.

upvoted 1 times

StingVN 2 weeks, 4 days ago

Selected Answer: B

B. Configure the version of SSH.

Explanation:
To generate an RSA key for SSH on a router, you need to configure the version of SSH. This involves specifying the desired version of SSH to be used on the router, such as SSH version 1 or SSH version 2. The specific commands to configure the SSH version may vary depending on the router's operating system.

The other options are not directly related to generating an RSA key for SSH:
A. Configuring VTY (Virtual Terminal) access is unrelated to generating an RSA key for SSH. VTY access controls remote management access to a router using protocols such as Telnet or SSH.
C. Assigning a DNS domain name is not directly related to generating an RSA key for SSH. DNS (Domain Name System) is used for domain name resolution and mapping domain names to IP addresses.
D. Creating a user with a password is unrelated to generating an RSA key for SSH. User creation and password assignment are part of configuring user authentication and authorization on a router, but not specifically related to SSH key generation.

upvoted 1 times

dropspablo 5 days, 2 hours ago

by chatgpt

upvoted 1 times

DUMPledore 4 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

sassasasasdccadsca 4 months, 3 weeks ago

- The Cisco IOS image used must be a k9 (crypto) image to support SSH.
- the hostname must be different from the default one
- define domain-name of the DNS

upvoted 1 times

cormorant 7 months ago

little things like this convince me that the only way to pass the CCNA is to do a bunch of brain dumps prior to taking it

upvoted 1 times

Liuka_92 11 months, 2 weeks ago

Use this trick to remember easy: DRUL
D: domain name R: rsa key U: username L: line vty

upvoted 5 times

Crazey 2 years, 8 months ago

B. Configure VTY access.

Tested on Packet Tracer + also shown on Cbt nuggets CCNA course

The ip ssh rsa keypair-name command enables an SSH connection using the Rivest, Shamir, and Adleman (RSA) keys that you have configured.

Previously, SSH was linked to the first RSA keys that were generated (that is, SSH was enabled when the first RSA key pair was generated). This behavior still exists, but by using the ip ssh rsa keypair-name command, you can overcome this behavior.

If you configure the ip ssh rsa keypair-name command with a key pair name, SSH is enabled if the key pair exists or SSH will be enabled if the key pair is generated later.

If you use this command to enable SSH, you are not forced to configure a hostname and a domain name, which was required in SSH Version 1 of the Cisco software.

Ref: https://www.cisco.com/c/en/us/td/docs/routers/asr920/configuration/guide/sec-usr-ssh/sec-usr-ssh-xe-3-13s-asr-920-book/m_sec-secure-shell-v2.html#GUID-B3B3CEE9-5113-4B40-B070-C21F82C8779C

upvoted 1 times

Acai 2 years ago

Bro you said all of that yet it has nothing on why B is the answer. You only mention that there's a way around C....

upvoted 3 times

ataraxium 2 years, 9 months ago

I am guessing the "DNS domain name" is referring to step 4 below.

Configuring a Device for SSH Version 2 Using a Hostname and Domain Name
SUMMARY STEPS
1. enable

2. configure terminal

3. hostname name

4. ip domain-name name

5. crypto key generate rsa

6. ip ssh [time-out seconds | authentication-retries integer]

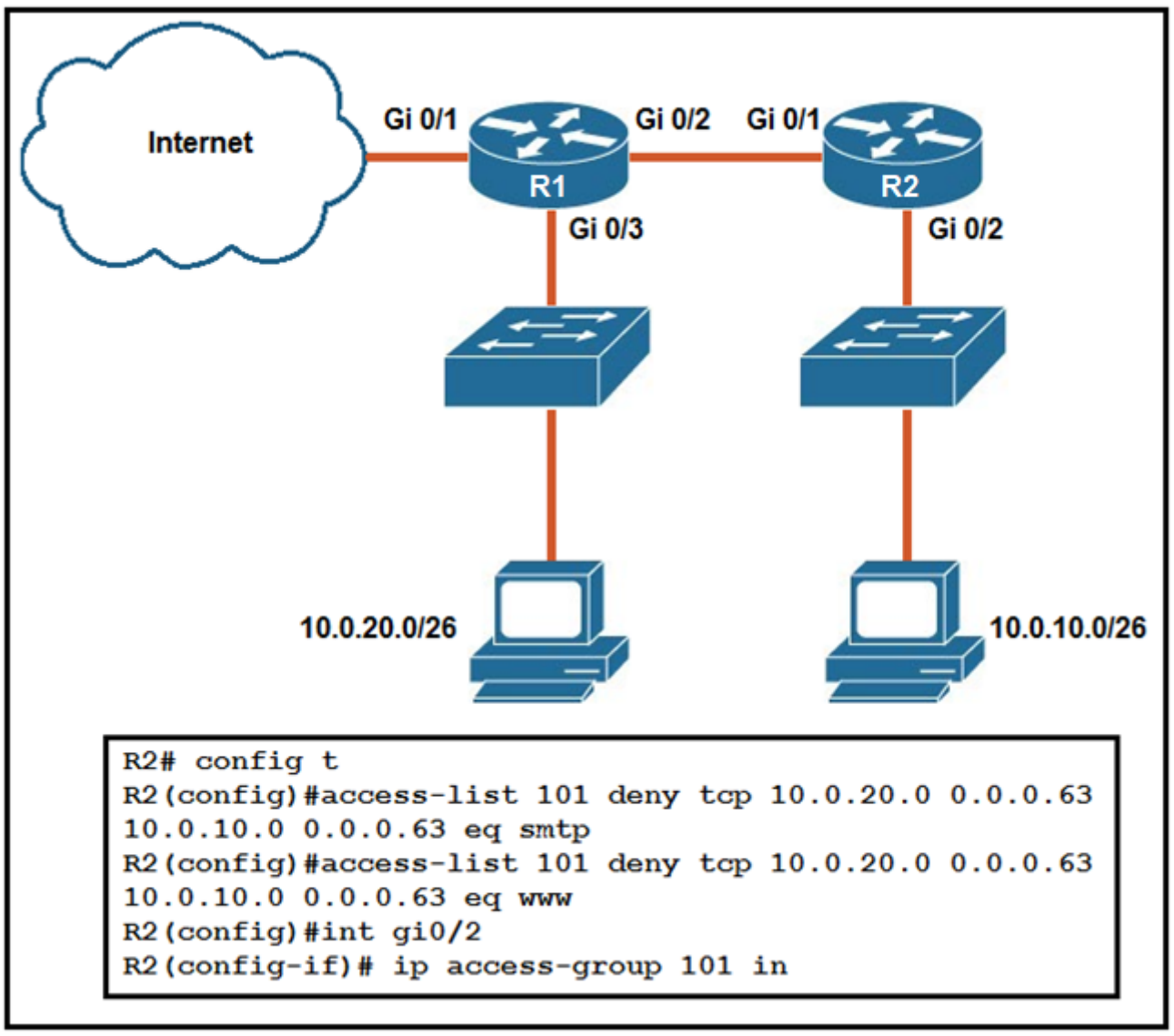
7. ip ssh version [1 | 2]

8. exit

From: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/15-s/sec-usr-ssh-15-s-book/sec-secure-shell-v2.html

upvoted 10 times

Question #621 *Topic 1*



Refer to the exhibit. An extended ACL has been configured and applied to router R2. The configuration failed to work as intended.
Which two changes stop outbound traffic on TCP ports 25 and 80 to 10.0.20.0/26 from the 10.0.10.0/26 subnet while still allowing all other traffic? (Choose two.)

A. Add a ג€permit ip any anyג€ statement at the end of ACL 101 for allowed traffic.

B. Add a ג€permit ip any anyג€ statement to the beginning of ACL 101 for allowed traffic.

C. The ACL must be moved to the Gi0/1 interface outbound on R2.

D. The source and destination IPs must be swapped in ACL 101.

E. The ACL must be configured the Gi0/2 interface inbound on R1.

Correct Answer: *AD*

sinear Highly Voted 2 years, 4 months ago
Edit: forget, answer is OK. I misread.
upvoted 8 times

Njavwa Most Recent 2 months, 1 week ago
extended ACL close to source
source IP if applied to R2 is 10.0.10.0
destination 10.0.20.0
all configs has to do with the R2 two int
upvoted 1 times

splashy 8 months, 2 weeks ago
Selected Answer: AD
Can't be E because an extended access list needs to be closest to source
upvoted 2 times

[Removed] 11 months ago
Selected Answer: AD
Ae is wrong..... Extended closest to the source.... The blocked traffic doesn't need to travel the entire network to THEN get blocked.
upvoted 1 times

AWSEMA 11 months, 2 weeks ago
deny tcp 10.0.10.0 0.0.0.63 10.0.20.0 0.0.0.63 eq 25
deny tcp 10.0.10.0 0.0.0.63 10.0.20.0 0.0.0.63 eq 80

permit ip any any
upvoted 1 times

guille_teleco 1 year ago
A and D are the correct, all the configuration is applied on R2. R1 has nothing to do on this question.
upvoted 1 times

Terra_Nova 1 year, 1 month ago
Selected Answer: AD
A and D are correct

All ACLs have a implicit deny at the end which blocks all traffic so we need to add a permit to allow that traffic through

The Source and destinations then need swapped.
Using packet tracer the source has to be first...

R1(config)#access-list 101 deny tcp ?
A.B.C.D Source address
any Any source host
host A single source host

and then the destination-

R1(config)#access-list 101 deny tcp 10.0.10.0 0.0.0.63 ?
A.B.C.D Destination address
any Any destination host
eq Match only packets on a given port number
gt Match only packets with a greater port number
host A single destination host
lt Match only packets with a lower port number
neq Match only packets not on a given port number
range Match only packets in the range of port numbers
upvoted 1 times

LilGhost_404 1 year, 3 months ago
Selected Answer: AE
it should be A and E, moving the acl to the router 1 port 2, does the same like in the router router 2 port 2, important is the allow command at the end of the acl or the implicit deny kicks in
upvoted 1 times

gaber 1 year, 5 months ago
without the permit statement, it'll just deny those things and do nothing else

for acls, you enter the source first and then the dest:

source_address_argument
[port_argument] dest_address_argument
[port_argument]

indicated answers are good
upvoted 2 times

Mursal99 1 year, 5 months ago
I think A, C are correct
upvoted 1 times

dave1992 1 year, 6 months ago
I THINK its DE because D should be moved closest to the source for extended, and because we are denying traffic, it auto permits all the rest of the traffic, leaving us with needing to swap the dest and source around to make the question true.
upvoted 1 times

laurvy36 1 year, 4 months ago
the acces list is already configured inbound, so that results that is configured on g0/2 being in this manner close to source
upvoted 1 times

Ed12345 1 year, 7 months ago
I think A, C are correct
upvoted 2 times

Robin999 2 years, 3 months ago
Correct Answers
upvoted 3 times

sinear 2 years, 4 months ago
Wrong. Should be D E.
Extended should be moved close to the source of trafic, so here interface Gi0/2 on R2.

And ip should be swapped.
upvoted 4 times

Tintin_06 2 years, 1 month ago
"If you intend to filter
a packet, filtering closer to the packet's source means that the packet takes up less bandwidth in the network, which seems to be more efficient—and it is. Therefore, Cisco suggests locating extended ACLs as close to the source as possible.
However, the second point seems to contradict the first point, at least for standard ACLs, to locate them close to the destination. Why? Well, because standard ACLs look only at the source IP address, they tend to filter more than you want filtered when placed close to the source."
upvoted 2 times

Question #622 *Topic 1*

An engineer must configure a WLAN using the strongest encryption type for WPA2-PSK. Which cipher fulfills the configuration requirement?

A. WEP

B. AES

C. RC4

D. TKIP

Correct Answer: *B*
Many routers provide WPA2-PSK (TKIP), WPA2-PSK (AES), and WPA2-PSK (TKIP/AES) as options. TKIP is actually an older encryption protocol introduced with
WPA to replace the very-insecure WEP encryption at the time. TKIP is actually quite similar to WEP encryption. TKIP is no longer considered secure, and is now deprecated. In other words, you shouldn't be using it.
AES is a more secure encryption protocol introduced with WPA2 and it is currently the strongest encryption type for WPA2-PSK/.

cormorant 8 months ago
AES (key length:128, 192, 256 bytes. block> 128 bytes) is for WPA2
RC4 is for wep
upvoted 1 times

alexiro 2 years, 9 months ago
WPA2-PSK (AES): This is the most secure option. It uses WPA2, the latest Wi-Fi encryption standard, and the latest AES encryption protocol. You should be using this option. On some devices, you'll just see the option "WPA2" or "WPA2-PSK." If you do, it will probably just use AES, as that's a common-sense choice.
https://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/
upvoted 3 times

Question #623 *Topic 1*

DRAG DROP -

Drag and drop the attack-mitigation techniques from the left onto the types of attack that they mitigate on the right.

Select and Place:

Answer Area

configure 802.1x authenticate	802.1q double-tagging VLAN-hopping attack
configure DHCP snooping	MAC flooding attack
configure the native VLAN with a nondefault VLAN ID	man-in-the-middle spoofing attack
disable DTP	switch-spoofing VLAN-hopping attack

Answer Area

Correct Answer:

configure 802.1x authenticate	configure the native VLAN with a nondefault VLAN ID
configure DHCP snooping	configure DHCP snooping
configure the native VLAN with a nondefault VLAN ID	configure 802.1x authenticate
disable DTP	disable DTP

martco Highly Voted 2 years, 3 months ago

change the default vlan id => prevents double tagging
configure 802.1x authenticate => prevents MAC flooding
enable DHCP Snooping => prevents MITM
disable DTP => prevents switch spoofing

upvoted 54 times

vadiminski 2 years ago

Absolutely correct

upvoted 1 times

dave1992 1 year, 7 months ago

wrong. DHCP snooping stops Rogue servers. Dynamic Arp inspection stops MITM attacks. 802.1x is to authenticate users and they dont get access until they authenticate.

upvoted 2 times

iGlitch 1 year ago

Yeah but DHCP snooping needs to be configured for DAI to work.

upvoted 2 times

cybernett Highly Voted 2 years, 2 months ago

Check the source
https://www.interserver.net/tips/kb/mac-flooding-prevent/
Mac flooding is overcome by 802.1X
MITM attack is overcome by DHCP Snooping
Please correct the answers @Admin

upvoted 7 times

dropspablo Most Recent 4 days, 2 hours ago

I think the original answer is correct.
Despite the confusion that 802.1x and DHCP Snooping can mitigate MiTM, however 802.1x is generally considered the strongest and recommended feature for this attack as it provides TRUE individual authentication.
https://garykongcybersecurity.medium.com/insecure-802-1x-port-based-authentication-using-eap-md5-c2b298bfc3ab
And about MAC Flooding attack, the best way to mitigate it is with port-security, or with DHCP Snooping feature activated, limiting the reception rate, with commands:
ip dhcp snooping limit rate 10
#ip arp inspection limit rate 8
and about "802.1q double-tagging VLAN-hopping." If you use the default native Vlan 1 and the network is using the native vlan for another vlan,

and there is traffic from native vlans (without tags) through the trunk ports, and the default native vlan would mistakenly receive this traffic from another native vlan (not default) used on the network.

upvoted 1 times

jorgenn 1 year ago

Implementing IEEE 802.1X suites will allow packet filtering rules to be installed explicitly by an AAA server based on dynamically learned information about clients, including the MAC address. These are the methods often used to prevent the MAC Flooding attack.

upvoted 2 times

kentsing 1 year ago

https://www.interserver.net/tips/kb/mac-flooding-prevent/
How to prevent the MAC Flooding Attack?
We can prevent the MAC Flooding attack with various methods. The following are some of these methods.
1) Port Security
2) Authentication with AAA server
3) Security measures to prevent ARP Spoofing or IP Spoofing
4) Implement IEEE 802.1X suites
2nd & 3rd answer should be swapped, Mac flooding should be prevented by 802.1x implementation

upvoted 2 times

msomali 1 year, 2 months ago

DHCP Snooping and 80.1x Authenticate are placed in the wrong Attacks, Need to be replaces, Admin Please change the Answers

Refer to the links below for further understandings.
https://www.interserver.net/tips/kb/mac-flooding-prevent/?__cf_chl_tk=HBU0WjmLQLFAbu4i57fVpxtcHbOHnpJti.oipqw.CyU-1649211364-0-gaNycGzNCJE

http://solidsystemsllc.com/prevent-man-in-the-middle-attacks/
https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

upvoted 3 times

Gere 2 years, 3 months ago

the correct answer should be: the 1st and 4th are correct but the 2nd and 3rd should be swapped.

upvoted 5 times

sinear 2 years, 4 months ago

Not correct. Right answer is https://itexamanswers.net/question/drag-and-drop-the-attack-mitigation-techniques-from-the-left-onto-the-types-of-attack-that-they-mitigate-on-the-right

upvoted 5 times

Ali526 2 years, 4 months ago

The first and the 4th are correct. 2nd and 3rd answers are wrong and need to be switched. Instead of reading answers on another exam web site, I prefer reading about the topic on sites that actually describe the issue.

upvoted 9 times

LTTAM 2 years, 4 months ago

@sinear... that link actually gives the wrong answer.

The solution posted here is correct.

upvoted 1 times

JamesDean_Youldiots 2 years ago

The answer posted to the website is wrong. 802.1x is for MAC flooding, and DHCP snooping is for MITM attacks. I just googled them both individually. Plus, that's what two other braindumps that I'm studying have as their correct answer, including the link that sinear posted.

upvoted 2 times

Littleowl 2 years, 4 months ago

technically dhcp snooping mitigates man in the middle attacks!

upvoted 1 times

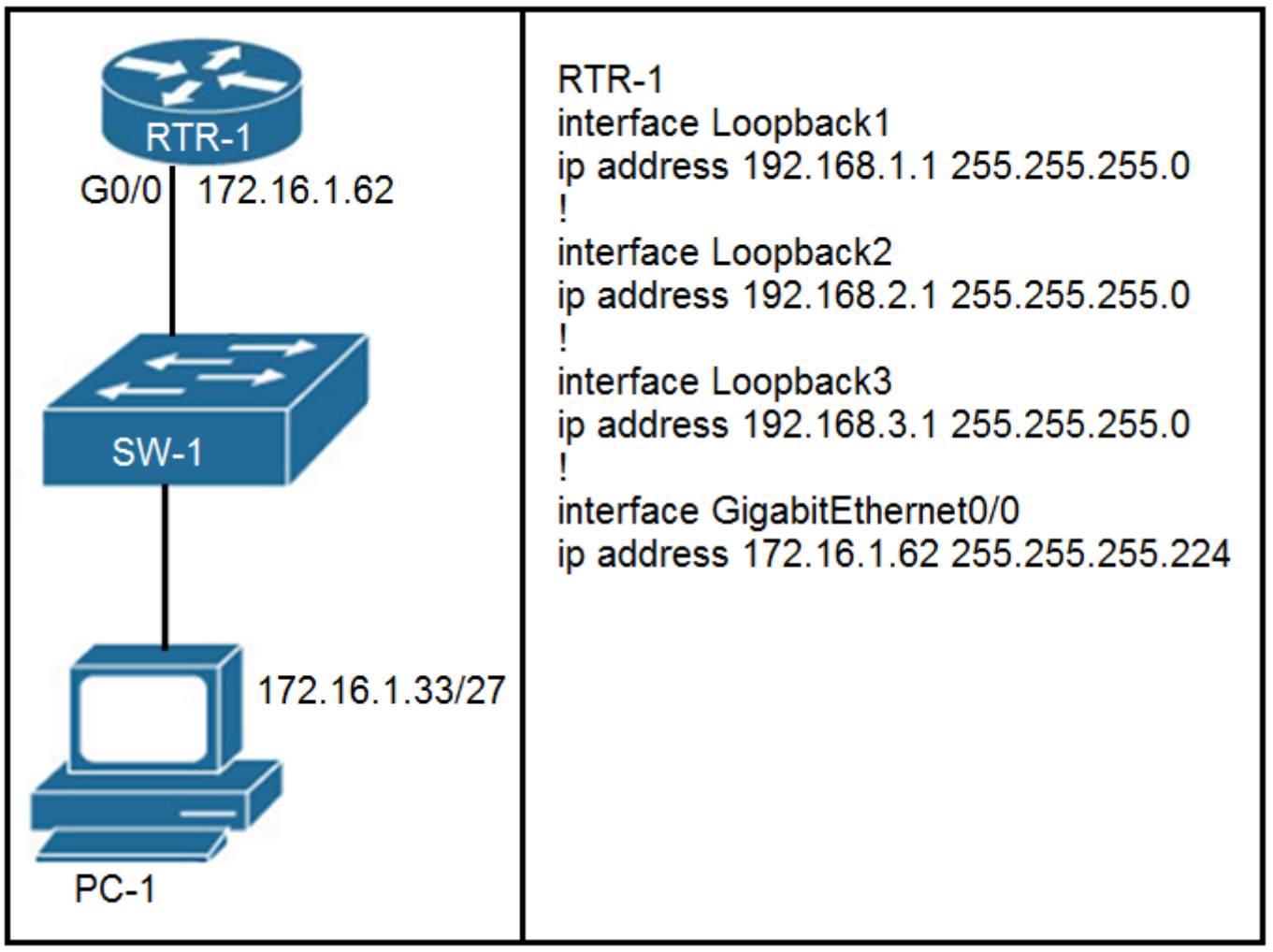
Zerotime0 2 years, 4 months ago

Thats what i chose

upvoted 1 times

Question #624 *Topic 1*

Refer to the exhibit. Which configuration for RTR-1 denies SSH access from PC-1 to any RTR-1 interface and allows all other traffic?



A.

```
access-list 100 deny tcp host 172.16.1.33 any eq 22
access-list 100 permit ip any any

interface GigabitEthernet0/0
ip access-group 100 in
```

B.

```
access-list 100 deny tcp host 172.16.1.33 any eq 22
access-list 100 permit ip any any

line vty 0 15
access-class 100 in
```

C.

```
access-list 100 deny tcp host 172.16.1.33 any eq 23
access-list 100 permit ip any any

interface GigabitEthernet0/0
ip access-group 100 in
```

D.

```
access-list 100 deny tcp host 172.16.1.33 any eq 23
access-list 100 permit ip any any

line vty 0 15
access-class 100 in
```

Correct Answer: *B*

nakres64 Highly Voted 2 years, 4 months ago

access-group [in|out] is used to tie an access-list to an interface.
access-class [in|out] is used to tie an access-list to vty lines.

So in case you want to prevent incoming network traffic on port 80 through Ethernet 0/0 you use
int E0/0
ip access-group 123 in

In case you want to allow only your PC from accessing the VTY via telnet/SSH use
line vty 0 4
ip access-class 1 in

upvoted 19 times

iGlitch Highly Voted 1 year, 1 month ago

A and B both are correct, BUT if you choose g0/0 interface then PC1 still be able to SSH using RTR-1 loopback interfaces, So you should implement that ACL on VTY lines to prevent SSH connections thro any interface.

upvoted 11 times

joeylam 5 months, 4 weeks ago

I guess the SSH connection to the loopback will be blocked at G0/0 of RTR1 before it reach the loopback address?

upvoted 3 times

liviuml Most Recent 1 month, 3 weeks ago

Answer A.
Both A and B have same result. Tested in PT.
My answer is based on the fact that extended ACL should be applied closest to the source.
If ACL is applied to vty the pachets will cross G0/0 to reach virtual terminal.
Usually vty are secured with standard ACL, lines with extended ACL.
The practice result of A and B are the same.
I think is more abotu best practice. Regards,
Read: https://www.computernetworkingnotes.com/ccna-study-guide/how-to-secure-vty-access-to-the-router.html

upvoted 2 times

dropspablo 4 days, 1 hour ago

Perhaps the router would be vulnerable with an ACL on the interface, as another host could access the VTY lines from other interfaces (if it has one), without ACLs. I believe it would be better to place the ACLs directly on the VTY lines, to ensure security.

upvoted 1 times

cormorant 5 months, 3 weeks ago

the part that trips you up: denies SSH access from PC-1 to any RTR-1 interface. option a indicates a single interface, which goes against te statement "to any RTR-1 interface". therefore you should aim for live vty 0 15. thus you should rule out a

upvoted 1 times

Computerguy 11 months ago

answer is A

upvoted 1 times

Hodicek 1 year, 6 months ago

NO SORRY 1 FOR SSH AND OTHER FOR TELNET SO B IS CORRECT

upvoted 1 times

Hodicek 1 year, 6 months ago

B - D ARE THE SAME AM I CORRECT?

upvoted 1 times

shakyak 1 year, 6 months ago

No check the port number

upvoted 2 times

Belinda 1 year, 3 months ago

Hello! B and D are not the same. B is eq 22 which means SSH while D is eq 23 means TELNET. Port 22 is for SSH while port 23 is for TELNET. SSH data transmission is encrypted while TELNET data transmission is in plain where anyone can read it.

upvoted 5 times

dave1992 1 year, 7 months ago

A is correct because the question is asking for 1 host. not a whole network. we are denying traffic to the router. we dont need any complex config. its simply answer A.

upvoted 2 times

Cpynch 1 year, 4 months ago

A will block SSH traffic for anything on any other interface of the router as well I believe.

It specifically asks to block SSH to RTR-1 interface, AKA the vyt lines.

upvoted 1 times

sgashashf 1 year, 3 months ago

Close. A will block PC1 from being able to SSH into anything on the other side of the router. Our goal is to ensure PC1 can't SSH into RTR-1, not to stop it from SSHing into any devices beyond.

upvoted 3 times

Ray12345 2 years ago

whats the different between apply the ACL on the interface and on the vty line..

upvoted 2 times

Sten111 1 year, 11 months ago

Question specifies any RTR1 interface
upvoted 2 times

ddino 2 years, 1 month ago
A is the answer unless you are planning to allow everyone else to ssh to your router
upvoted 2 times

Joe_Q 2 years, 1 month ago
If the ACL is applied to the G0/0 interface it completely denies SSH traffic to the network as a whole. In this case, you just what to deny SSH traffic to the router's VTY ports. Therefore, question A is not correct. I know poorly worded question. Some of these questions do not prove if you know the content, it just proves that you are able to pick out "Key" words in a timely manner.
upvoted 11 times

onmils2 1 year, 9 months ago
Answer A doesn't deny ssh for the whole network only for host 172.16.1.33, it's in the command that it only block this IP.
upvoted 4 times

cortib 1 year, 8 months ago
only from the host to any. ACL structure = access-list "number" deny/permit host "sourceip" (source port) "destination ip" "destination port"
In this case source address is pc1, destination any, so ssh connection qill be blocked from pc1 to all the network
upvoted 1 times

Cpynch 1 year, 4 months ago
Correct. All SSH traffic stops at gi0/0 with A, even SSH packets that are headed to elsewhere on any other interface of the router. So, if another router was connect to another interface on RTR-1, and you wanted to SSH to that router, traffic would not flow past gi0/0 for anything, on any network from that specific host.
upvoted 1 times

Nhan 2 years, 3 months ago
For this question we are looking at denying ssh which is port 22, and because it is line very so it's is using access class so given answer is correct
upvoted 4 times

xsp 2 years, 3 months ago
for interface, add ip access-group <access list number> in/out
for vty, access-class <access list number> in/out
upvoted 3 times

Question #625 *Topic 1*

While examining excessive traffic on the network, it is noted that all incoming packets on an interface appear to be allowed even though an IPv4 ACL is applied to the interface. Which two misconfigurations cause this behavior? (Choose two.)

A. The ACL is empty

B. A matching permit statement is too broadly defined

C. The packets fail to match any permit statement

D. A matching deny statement is too high in the access list

E. A matching permit statement is too high in the access list

Correct Answer: *BE*
Traffic might be permitted if the permit statement is too braid, meaning that you are allowing more traffic than what is specifically needed, or if the matching permit statement is placed ahead of the deny traffic. Routers will look at traffic and compare it to the ACL and once a match is found, the router acts accordingly to that rule.

kijken Highly Voted 1 year, 4 months ago
NOT A:
I see alot say A, but A has a hidden deny any on the end of the list as has every access list.
upvoted 13 times

dave1992 Highly Voted 1 year, 7 months ago
A. not even sure what that means.
B. is the answer because its too specific meaning its allowing everthing it shouldnt
C. not the answer because if it was failing to match, then traffic would be getting denied
D. not the answer because traffic would be getting denied.
E. is the answer because it wouldnt matter how many deny commands if you are permitting it first at the top of the ACL
upvoted 12 times

GangsterDady 1 year, 7 months ago
option A states that ACL IS EMPTY. But the fact is that acl can never be empty because of deny statement at the end which is by default.
upvoted 6 times

Chupacabro 1 year, 5 months ago
So high means top of the access list not high in sequence number(making D an answer)?
upvoted 1 times

Peter_panda Most Recent 1 month, 3 weeks ago
Selected Answer: AE
https://community.cisco.com/t5/routing/apply-empty-acl-what-happens/td-p/740473
upvoted 1 times

krzysiew 2 months, 1 week ago
a) ACL is empty - if acl is empty its mean all traffic is deny
upvoted 1 times

krzysiew 2 months, 1 week ago
B and E
upvoted 1 times

Ciscoman021 2 months, 2 weeks ago
Selected Answer: AE
the correct answers are options A and E. Option B is incorrect because a broadly defined permit statement would allow traffic that matches the statement, but it would not cause all traffic to be allowed. Option C is incorrect because if the packets fail to match any permit statement in the ACL, they should be denied by default, unless there is an explicit permit any statement at the end of the ACL. Option D is also incorrect because if a matching deny statement is too high in the access list, it would block the traffic, rather than allowing it.
upvoted 2 times

DUMPledore 4 months, 2 weeks ago
Selected Answer: BE
I go for BE
upvoted 1 times

Etidic 7 months, 2 weeks ago
Selected Answer: BE

A and E are correct
upvoted 1 times

ptfish 10 months, 3 weeks ago
A is wrong. Because the empty acl will cause all traffic to be denied. but the question says that all incoming packets on the interface appear to be allowed even with the IPv4 ACL applied.
upvoted 1 times

Danilodelacruzjr 1 year ago
(X) A. If the packet fails to match any permit statements than every packet will be blocked because of the implicit deny on every ACL.
(X)B. because of the implicit deny, there will always be packets that will be blocked not unless the permit statement is permit any any.
(correct) C. this can be the answer if the broad permit statement is permit any any.
(correct) D. the implicit deny will always be at the end of an ACL with the exception of an empty ACL. the implicit deny only applies if there is 1 or more line in the ACL (except permit any any statement).
(X) E. there should always be a single permit statement in the ACL because the implicit deny will block all traffic without a permit statement.
upvoted 2 times

RichyES 1 year, 5 months ago
A & E are correct answer
upvoted 1 times

hema5tho 1 year, 9 months ago
B and E was my election. Why not A? Cause ACL's have an implicit deny from the moment you create them. By definition they can't be empty.
upvoted 6 times

Alvinlongks 1 year, 9 months ago
I think A is not a good choice given that even if the ACL is empty and no other conditions arematch, the router rejects the packet because of an implicit deny all clause.
upvoted 4 times

aung_hein_kyaw 1 year, 11 months ago
i think question says ipv4 acl applied to the interface .if acl is empty,how do u match access-group " name or number" in interface .
upvoted 1 times

Sten111 1 year, 11 months ago
I agree with A and E but i'm not convinced with the arguments discounting B here.

If I wanted to configure an ALC to allow only traffic from 192.168.1.0/24 and messed up the wildcard mask e.g.

access-list 1 permit 192.168.0.0 0.0.255.255 (Would allow all traffic from 192.168.x.x)

Then that is a misconfiguration and would allow my entire network, if contained within 192.168.0.0/16.

This is a matching permit statement that is too broadly defined caused by a misconfiguration.

This is a bad question and it looks to me like there are three correct answers here.
upvoted 1 times

Micah7 2 years ago
Raymond9 makes a valid point. More here on this: https://community.cisco.com/t5/routing/apply-empty-acl-what-happens/td-p/740473
upvoted 1 times

Sicko 2 years, 1 month ago
https://community.cisco.com/t5/routing/apply-empty-acl-what-happens/td-p/740473

"The statement that an ACL always has an implicit deny any at the bottom has one exception. And that exception is when the ACL is empty. If you use ip access-group to apply an ACL and that ACL has no statements then all traffic is permitted."

Ans: A&E
upvoted 7 times

Question #626 *Topic 1*

The service password-encryption command is entered on a router. What is the effect of this configuration?

A. restricts unauthorized users from viewing clear-text passwords in the running configuration

B. prevents network administrators from configuring clear-text passwords

C. protects the VLAN database from unauthorized PC connections on the switch

D. encrypts the password exchange when a VPN tunnel is established

Correct Answer: *A*

krzysiew 2 months, 1 week ago

i think the answar is B

upvoted 1 times

sovafal192 1 year, 4 months ago

Selected Answer: A

I was flapping between A and B but, this cleared for me:
"If the service password-encryption command is set, the encrypted form of the password you create is displayed when the more nvram:startup-config command is entered. "

upvoted 2 times

Murphy2022 8 months, 1 week ago

the service does only encrypt existing passwords therefor the admin is still able to configure unencrypted password

upvoted 1 times

Question #627 *Topic 1*

Which WPA3 enhancement protects against hackers viewing traffic on the Wi-Fi network?

A. SAE encryption

B. TKIP encryption

C. scrambled encryption key

D. AES encryption

Correct Answer: *A*

alexiro Highly Voted 2 years, 9 months ago

The third version of a Wi-Fi Alliance standard introduced in 2018 that requires pre-shared key or 802.1x authentication, GCMP, SAE, and forward secrecy.

Simultaneous Authentication of Equals (SAE)
A strong authentication method used in WPA3 to authenticate wireless clients and APs and to prevent dictionary attacks for discovering pre-shared keys.

upvoted 17 times

DARKK Highly Voted 1 year ago

This is a bad question because AES Is technically correct, SAE is the handshake mechanism WPA 3 uses, it protects against offline dictionary attacks, and by the way the question is worded it's probably A, but D is correct as the actual encryption is AES for WPA 2 AND WPA 3. Thus AES is what is protecting all the data, but SAE is an enhancement WPA 3 has over WPA.

upvoted 9 times

Ciscoman021 Most Recent 2 months, 2 weeks ago

Selected Answer: A

The WPA3 enhancement that protects against hackers viewing traffic on the Wi-Fi network is SAE (Simultaneous Authentication of Equals) encryption. SAE is a secure key establishment protocol that provides stronger protection against password guessing attacks and offline dictionary attacks compared to the previous WPA2-Personal (PSK) protocol. SAE uses the Dragonfly key exchange method and provides forward secrecy, which means that if an attacker obtains the Wi-Fi network password, they cannot decrypt previously captured traffic. Therefore, option A is the correct answer.

upvoted 1 times

Anas_Ahmad 5 months ago

Selected Answer: A

WPA3 uses simultaneous authentication of equals (SAE) encryption

upvoted 1 times

AWSEMA 11 months, 1 week ago

Selected Answer: A

WPA3 uses simultaneous authentication of equals (SAE) encryption and allows only WiFi devices that support WPA3 to join the virtual access point (VAP).

upvoted 2 times

xped2 1 year, 6 months ago

AES in general can be used by WPA3 to prevent the viewing of traffic, SAE only protects authentication

Though, AES isn't new to WPA3, but SAE is. "Simultaneous authentication of equals"
It results in a more secure initial key exchange while in personal mode, replaces WPS, and mitigates vulnerabilities posed by weak PSKs.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/16-12/config-guide/b_wl_16_12_cg/wpa3.html

upvoted 5 times

Nse_Sa 2 years, 1 month ago

Nse SAE

upvoted 4 times

mrsiafu 2 years, 1 month ago

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-2/config-guide/b_wl_17_2_cg/wi_fi_protected_access_3.html

upvoted 2 times

mrsiafu 2 years, 1 month ago

Definitely not in the OCG

upvoted 3 times

UmbertoReed 1 year, 8 months ago

There's a brief mention on page 663 of the first volume. It's the last page of chapter 28.

upvoted 1 times

ProgSnob 1 year, 6 months ago

I confirmed this. When things are mentioned briefly it's harder to remember those very few words as compared to something like OSPF which we spend a lot of time focusing on. My advice to mrsiafu and others is to take handwritten notes. Go through each chapter at least twice. First time do a read through and then go back a second time and outline the important things and things you know you might forget. This way, when you do a review you can focus on what you need instead of doing a full read-through of the chapter again and again.

upvoted 7 times

Question #628 *Topic 1*

Refer to the exhibit. If the network environment is operating normally, which type of device must be connected to interface fastethernet 0/1?

```
ip arp inspection vlan 2-10
interface fastethernet 0/1
        ip arp inspection trust
```

A. DHCP client

B. access point

C. router

D. PC

Correct Answer: *C*

shebo Highly Voted 1 year, 5 months ago

Selected Answer: C

The correct answer should be C.

upvoted 5 times

AWSEMA Most Recent 9 months, 3 weeks ago

Selected Answer: C

ROUTER !!!

upvoted 1 times

ratu68 11 months ago

Selected Answer: C

Has to be a network device to be trusted.

Answer is C

upvoted 4 times

AWSEMA 11 months, 1 week ago

router

upvoted 1 times

snrov 1 year, 1 month ago

Selected Answer: C

I swear it is C

upvoted 3 times

ismatdmour 1 year, 2 months ago

Selected Answer: C

Definitly the router. Routers are networki devices that are under Administrative control. Hence, they are configured Trusted in DAI and DHCP Snooping

upvoted 3 times

SparkySM 1 year, 4 months ago

Selected Answer: C

definitely its C

upvoted 3 times

Cho1571 1 year, 4 months ago

Selected Answer: C

Looks like the answer is C since the port is trusted.
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html

upvoted 2 times

valipuiu 1 year, 4 months ago

Selected Answer: C

trusting static assigned address

upvoted 1 times

RichyES 1 year, 5 months ago

C is the answer

upvoted 1 times

gaber 1 year, 5 months ago

ip arp inspection trust = dhcp
no ip arp inspection trust = no dhcp

thus: A

https://www.cisco.com/c/en/us/td/docs/wireless/asr_900/feature/guides/dynarp.html#:~:text=Table%C2%A01%20Default%20Dynamic%20ARP%20Inspection%20Configuration%20%20,ACLs%20are%20defined.%20%203%20more%20rows%20

upvoted 1 times

babaKazoo 1 year, 4 months ago

A. Is a DHCP client which is a deceptive way of saying a PC, if it was a DHCP server then yes it would be correct.

upvoted 6 times

Question #629 *Topic 1*

Refer to the exhibit. An administrator configures four switches for local authentication using passwords that are stored as a cryptographic hash. The four switches must also support SSH access for administrators to manage the network infrastructure. Which switch is configured correctly to meet these requirements?

```
SW1(config-line) #line vty 0 15
SW1(config-line) #no login local
SW1(config-line) #password cisco

SW2(config) #username admin1 password abcd1234
SW2(config) #username admin2 password abcd1234
SW2(config-line) #line vty 0 15
SW2(config-line) #login local

SW3(config) #username admin1 secret abcd1234
SW3(config) #username admin2 secret abcd1234
SW3(config-line) #line vty 0 15
SW3(config-line) #login local

SW4(config) #username admin1 secret abcd1234
SW4(config) #username admin2 secret abcd1234
SW4(config-line) #line console 0
SW4(config-line) #login local
```

A. SW1

B. SW2

C. SW3

D. SW4

Correct Answer: *C*

vadiminski Highly Voted 2 years ago

Keyword local authentication: "login local" configuration
Keyword cryptographic hash: "secret" configuration
Keyword SSH access: "live vty 0 15" configuration
--> Answer C is correct
upvoted 30 times

Jong12 1 year, 7 months ago

SW2 and SW3 has the same configuration how can C be right and B not?
upvoted 1 times

Pkard 1 year, 7 months ago

SW2 uses "password" and SW3 uses "secret".
I didn't see it at first either
upvoted 2 times

Pkard 1 year, 7 months ago

"password" is stored as plain text and does not meet the requirements of the question
upvoted 2 times

dave1992 1 year, 7 months ago

both are correct. its the same answer
upvoted 1 times

Belinda 1 year, 3 months ago

Hello! B and C are not the same. At the privilege mode when you put in two commands, enable password and enable secret then the enable secret override the enable password since the enable secret is encrypted while the enable password is not. The main aim is to encrypt the password/key to prevent hackers from hacking it.
upvoted 2 times

krzysiew Most Recent 2 months, 1 week ago

Selected Answer: C

Answer C is correct
upvoted 1 times

Adaya 1 year, 11 months ago
Thank vadiminski
upvoted 3 times

Question #630 *Topic 1*

```
ip arp inspection vlan 5-10
interface fastethernet 0/1
   switchport mode access
   switchport access vlan 5
```

Refer to the exhibit. What is the effect of this configuration?

A. The switch discards all ingress ARP traffic with invalid MAC-to-IP address bindings.

B. All ARP packets are dropped by the switch.

C. Egress traffic is passed only if the destination is a DHCP server.

D. All ingress and egress traffic is dropped because the interface is untrusted.

Correct Answer: *A*
Dynamic ARP inspection is an ingress security feature; it does not perform any egress checking.

dicksonpwc Highly Voted 1 year, 9 months ago
Dynamic ARP Inspection (DAI) is a security feature that validates Address Resolution Protocol (ARP) packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address bindings.
upvoted 6 times

redivivo 1 year ago
so true
upvoted 2 times

aosroyal 1 year, 1 month ago
this does not help at all
upvoted 4 times

aosroyal 1 year, 1 month ago
this does not help at all
upvoted 4 times

sasquatchshrimp Most Recent 10 months ago
Selected Answer: A
https://documentation.meraki.com/MS/Other_Topics/Dynamic_ARP_Inspection#:~:text=Whitelisting%20Blocked%20Entries-,Overview,switch%20to%20validate%20ARP%20packets.
upvoted 1 times

Question #631 *Topic 1*

When a site-to-site VPN is used, which protocol is responsible for the transport of user data?

A. IPsec

B. IKEv1

C. MD5

D. IKEv2

Correct Answer: *A*
A site-to-site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. A site-to-site
VPN means that two sites create a VPN tunnel by encrypting and sending data between two devices. One set of rules for creating a site-to-site VPN is defined by
IPsec.

alexiro Highly Voted 2 years, 9 months ago

IPsec The term referring to the IP Security protocols, which is an architecture for providing encryption and authentication services, usually when creating VPN services through an IP network
Site-to-site IPSec VPNs offer scalability as a benefit. This is because each remote office only needs an Internet connection to create a VPN tunnel back to the main office.

upvoted 9 times

Question #632 *Topic 1*

Which type of wireless encryption is used for WPA2 in preshared key mode?

A. AES-128

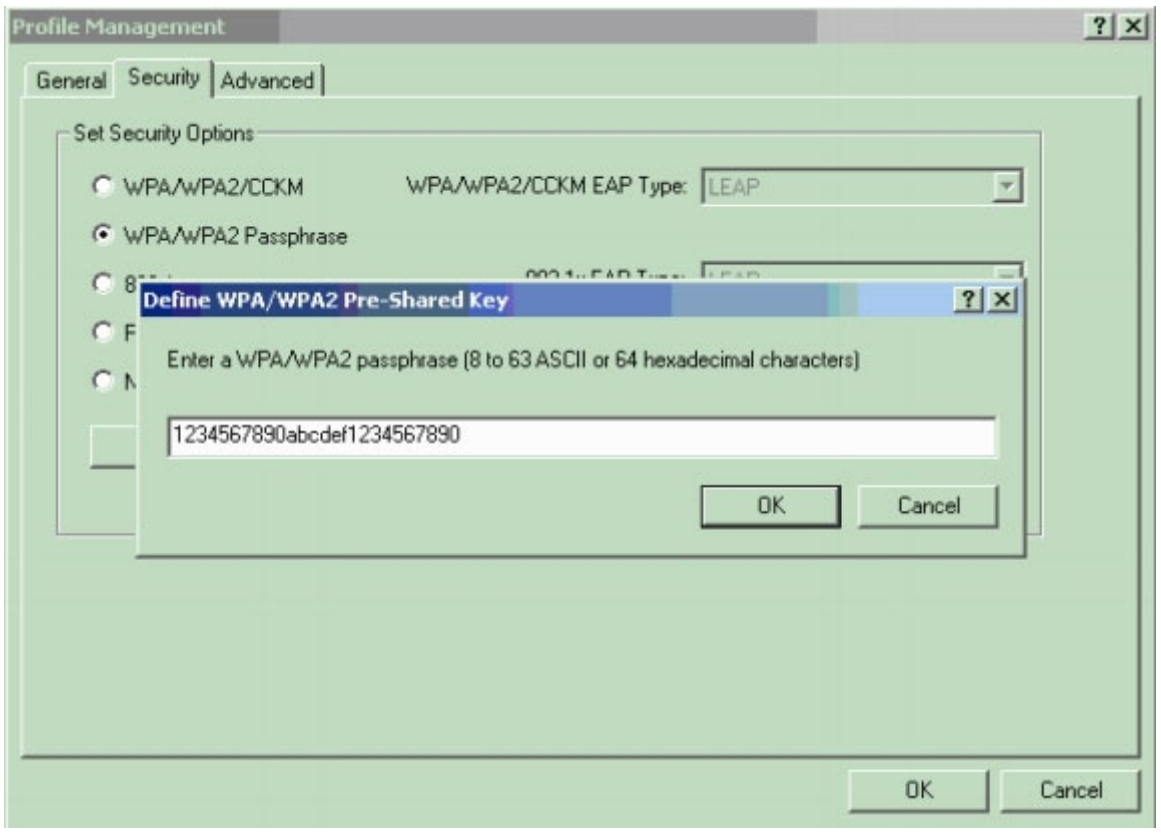
B. TKIP with RC4

C. AES-256

D. RC4

Correct Answer: *C*

We can see in this picture we have to type 64 hexadecimal characters (256 bit) for the WPA2 passphrase so we can deduce the encryption is AES-256, not AES-
128.



Reference:

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/67134-wpa2-config.html

Rakeshch Highly Voted 2 years, 2 months ago

WPA2 aes is always 128 bit key for both psk and enterprise. The number of characters from passphrase dont have anything to do with the key length.
It is not even possible to select the key length.
Always 128.

upvoted 8 times

RougePotatoe 7 months, 1 week ago

Here is a link that supports this comment.

upvoted 2 times

RougePotatoe 7 months, 1 week ago

https://www.cwnp.com/forums/posts?postNum=299964

upvoted 3 times

ac89l Most Recent 3 weeks, 3 days ago

Selected Answer: A

A is correct

upvoted 1 times

AWSEMA 10 months, 1 week ago

Selected Answer: A

A ====> AES-128 is used.

upvoted 4 times

lock12333 11 months, 3 weeks ago

Selected Answer: C

ccccccccccccccccccccccccccc

upvoted 1 times

iGlitch 1 year ago

Selected Answer: A

AES-128 is used.

upvoted 2 times

Pkard 1 year, 5 months ago

I agree with AES-128. The shared key may be 256 bits long but the encryption is 128 bits.

https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#:~:text=Each%20wireless%20network%20device%20encrypts,to%2063%20printable%20ASCII%20characters.

upvoted 1 times

DaBest 1 year, 8 months ago

this is the same link the website answer used.
AES-128bit Black on white

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/67134-wpa2-config.html#:~:text=AES%20Counter%20Mode%20is%20a%20block%20cipher%20that%20encrypts%20128-bit%20blocks%20of%20data%20at%20a%20time%20with%20a%20128-bit%20encryption%20key.

upvoted 1 times

DaBest 1 year, 8 months ago

Notice! i found this link and now im confused.. anyone know whats the meaning of this?
"Each wireless network device encrypts the network traffic by deriving its 128-bit encryption key from a 256-bit shared key"
baised on that, i wonder what should be the answer...

https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#:~:text=Each%20wireless%20network%20device%20encrypts%20the%20network%20traffic%20by%20deriving%20its%20128-bit%20encryption%20key%20from%20a%20256-bit%20shared%20key

upvoted 2 times

Pkard 1 year, 5 months ago

Right, it's still 128-bit encryption

upvoted 2 times

DaBest 1 year, 8 months ago

The Answer should be AES-128 bit!
cisco says that themselves on their website

https://www.cisco.com/assets/sol/sb/isa500_emulator/help/guide/ae1217496.html#:~:text=Encryption%3A%20Choose%20the%20encryption%20type%3A%2064%20bits%20(10%20hex%20digits)%2C%2064%20bits%20(5%20ASCII)%2C%20128%20bits%20(26%20hex%20digits)%2C%20or%20128%20bits%20(13%20ASCII).%20The%20default%20is%2064%20bits%20(10%20hex%20digits).%20The%20larger%20size%20keys%20provide%20stronger%20encryption%2C%20thus%20making%20the%20key%20more%20difficult%20to%20crack.

upvoted 2 times

Joe_Q 2 years, 1 month ago

WPA 2 implements the National Institute of Standards and Technology (NIST)-recommended Advanced Encryption Standard (AES) encryption algorithm with the use of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES Counter Mode is a block cipher that encrypts 128-bit blocks of data at a time with a 128-bit encryption key. The CCMP algorithm produces a message integrity code (MIC) that provides data origin authentication and data integrity for the wireless frame.

upvoted 4 times

joaofcoantunes 2 years, 2 months ago

WPA2 Support only AES-CCMP (CCNA 200-301 Official Cert Guide, Volume 1 - Page 662). (AES-Counter Mode CBC-MAC Protocol) The encryption algorithm used in the 802.11i security protocol. It uses the AES block cipher, but restricts the key length to 128 bits.
So I think its correct A - AS128

upvoted 3 times

Question #633 *Topic 1*

DRAG DROP -

Drag and drop the threat-mitigation techniques from the left onto the types of threat or attack they mitigate on the right.

Select and Place:

Answer Area

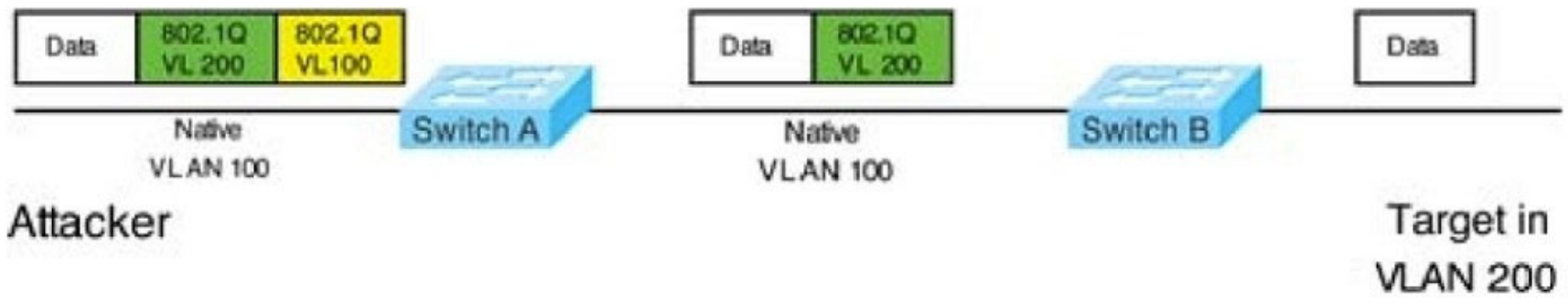
Configure BPDU guard.	802.1q double tagging
Configure dynamic ARP inspection.	ARP spoofing
Configure root guard.	unwanted superior BPDUs
Configure VACL.	unwanted BPDUs on PortFast-enabled interfaces

Correct Answer:

Answer Area

Configure BPDU guard.	Configure VACL.
Configure dynamic ARP inspection.	Configure dynamic ARP inspection.
Configure root guard.	Configure root guard.
Configure VACL.	Configure BPDU guard.

Double-Tagging attack:



In this attack, the attacking computer generates frames with two 802.1Q tags. The first tag matches the native VLAN of the trunk port (VLAN 10 in this case), and the second matches the VLAN of a host it wants to attack (VLAN 20).

When the packet from the attacker reaches Switch A, Switch A only sees the first VLAN 10 and it matches with its native VLAN 10 so this VLAN tag is removed.

Switch A forwards the frame out all links with the same native VLAN 10. Switch B receives the frame with an tag of VLAN 20 so it removes this tag and forwards out to the Victim computer.

Note: This attack only works if the trunk (between two switches) has the same native VLAN as the attacker.

To mitigate this type of attack, you can use VLAN access control lists (VACLs, which applies to all traffic within a VLAN. We can use VACL to drop attacker traffic to specific victims/servers) or implement Private VLANs.

ARP attack (like ARP poisoning/spoofing) is a type of attack in which a malicious actor sends falsified ARP messages over a local area network as ARP allows a gratuitous reply from a host even if an ARP request was not received. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. This is an attack based on ARP which is at Layer 2. Dynamic ARP inspection (DAI) is a security feature that validates ARP packets in a network which can be used to mitigate this type of attack.

Question #634 *Topic 1*

Which command prevents passwords from being stored in the configuration as plain text on a router or switch?

A. enable secret

B. enable password

C. service password-encryption

D. username cisco password encrypt

Correct Answer: *C*

nakres64 Highly Voted 2 years, 4 months ago

correct
enable password <string> - Sets the enable password, and stores that password in plaintext in the config.

enable secret <string> - Sets the enable password, and stores that password as an md5 hash in the config.

service password-encryption - For any passwords in the config that are stored in plaintext, this command changes them to be stored as hashed values instead.

upvoted 20 times

salami 1 year, 7 months ago

quite right, but service password encryption does weak encryption, it doesnt store them as hashed values

upvoted 2 times

Etidic Most Recent 7 months, 2 weeks ago

Selected Answer: C

The correct answer is C.

Enable secret <string> only encrypts the password used to enter privileged exec mode. Other passwords like line vty 0 4 password etc will have their passwords visible in the running configuration.

upvoted 3 times

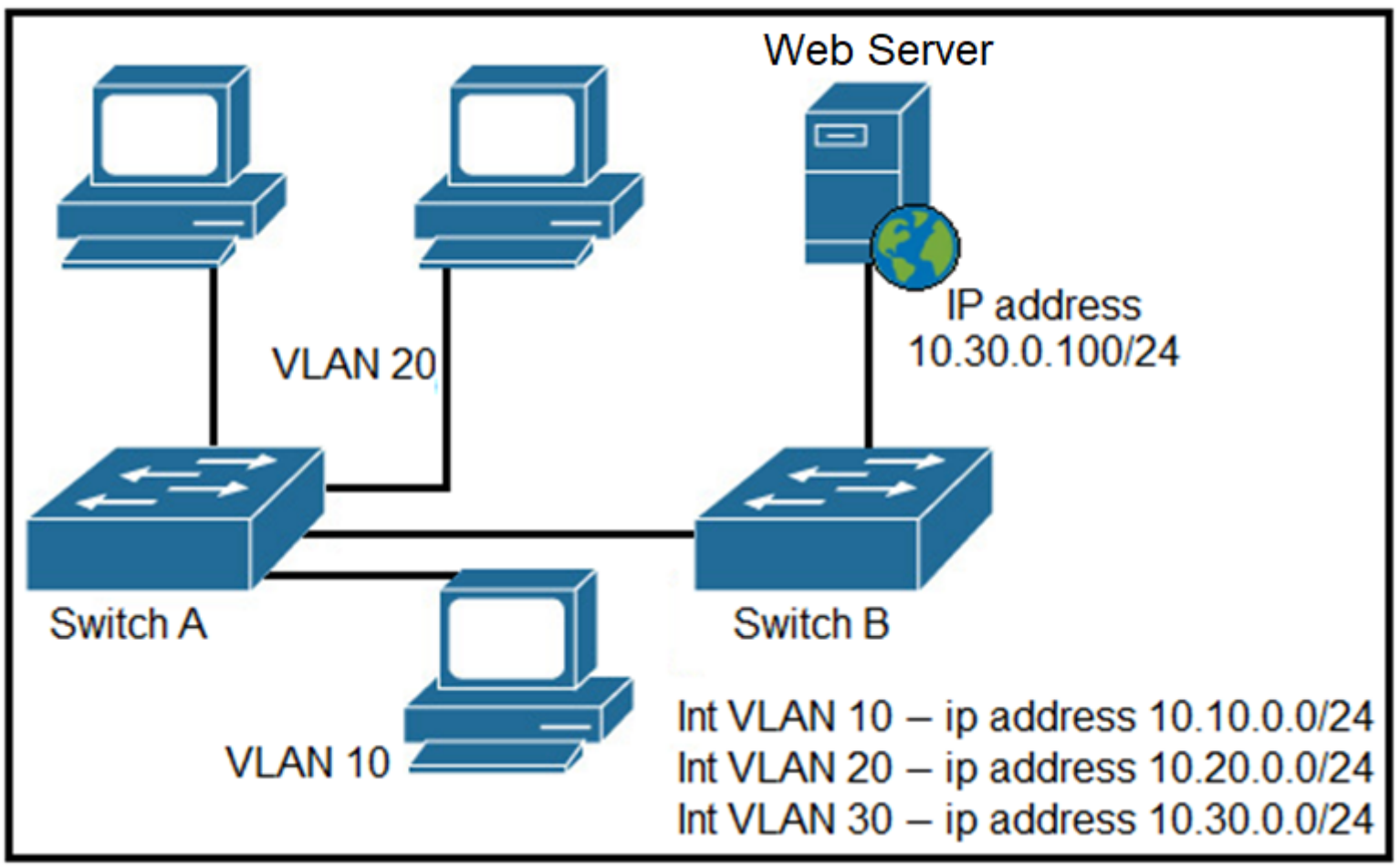
BieLey 8 months, 1 week ago

Selected Answer: C

Keyword = Prevent passwords

upvoted 1 times

Question #635 *Topic 1*



Refer to the exhibit. A network engineer must block access for all computers on VLAN 20 to the web server via HTTP. All other computers must be able to access the web server. Which configuration when applied to switch A accomplishes the task?

A.
```
config t
ip access-list extended wwwblock
permit ip any any
deny tcp any host 10.30.0.100 eq 80
int vlan 20
ip access-group wwwblock in
```

B.
```
config t
ip access-list extended wwwblock
permit ip any any
deny tcp any host 10.30.0.100 eq 80
int vlan 30
ip access-group wwwblock in
```

C.
```
config t
ip access-list extended wwwblock
deny tcp any host 10.30.0.100 eq 80
int vlan 10
ip access-group wwwblock in
```

D.
```
config t
ip access-list extended wwwblock
deny tcp any host 10.30.0.100 eq 80
permit ip any any
int vlan 20
ip access-group wwwblock in
```

Correct Answer: *D*

Ali526 Highly Voted 2 years, 4 months ago
Sorry, D is correct, but not the best way to address this.
upvoted 18 times

Belinda 1 year, 3 months ago
Thanks
upvoted 1 times

ZayaB Highly Voted 2 years, 3 months ago
I agree with you Ali526. Not a good way to implement this ACL.
upvoted 5 times

dave1992 Most Recent 1 year, 6 months ago

if were blocking all traffic in vlan 20. would the acl include .20 and not .30???

upvoted 3 times

Aleks123 1 year, 5 months ago

Hey Dave I believe its a typo your right!

upvoted 3 times

bitree 1 year, 1 month ago

you could specify the source addressed with the specific range instead of 'any' but it's not necessary since only vlan 20 is off that interface. 'any' suffices. It is not a typo because the .30 is where the destination address is.

upvoted 2 times

Question #636 *Topic 1*

In which two ways does a password manager reduce the chance of a hacker stealing a user's password? (Choose two.)

A. It encourages users to create stronger passwords

B. It uses an internal firewall to protect the password repository from unauthorized access

C. It stores the password repository on the local workstation with built-in antivirus and anti-malware functionality

D. It automatically provides a second authentication factor that is unknown to the original user

E. It protects against keystroke logging on a compromised device or web site

Correct Answer: *AE*

ccna_goat Highly Voted 8 months, 1 week ago
stupid question
upvoted 14 times

Scipions Highly Voted 2 years, 1 month ago
qwerty, admin, 12345678
upvoted 10 times

Bash2111 Most Recent 1 year ago
A and E is correct
upvoted 1 times

VictorCisco 2 months, 1 week ago
A is definitely not correct. The question is "reduce the chance of a hacker STEALING (not login! not guesing)". It doesn't matter how strong password is to steal it. if you can steal "qwerty" you can steal "JHGJHBHBndfjdn$%%%kdfmke282828"!
upvoted 1 times

Vinarino 1 year, 4 months ago
1-Something you have (CAC-card, Token [RandomKeygen]) + 2-Something you know (PIN / PWD) + 3-Something you are (Username / (Bio) - Retina-scan or Fingerprint = Multifactor.
Typically tools (processes) in a compromised anything will NOT continue to function = A&D
upvoted 2 times

ROBZY90 2 years, 1 month ago
E is correct as you can generally copy and paste pwds from a password manager and thus this prevents against keystroke logging
upvoted 3 times

Rakeshch 2 years, 2 months ago
Correct A E
E Assumes that the Admin doesn't know there is a compromised device on network. If there is one it will prevent it from logging keyboard presses and stealing the password
upvoted 3 times

Ali526 2 years, 5 months ago
A is correct. E assumes that administrator know the compromised computer. How is that going to happen?
upvoted 2 times

sinear 2 years, 4 months ago
The "compromised" device here is is the web site on which the user has to log. So he knows which one it is of course (since it is under his supervision). By preventing keystroke logging, he protects against pwd thefts.
upvoted 1 times

Question #637 *Topic 1*

Which goal is achieved by the implementation of private IPv4 addressing on a network?

A. provides an added level of protection against Internet exposure

B. provides a reduction in size of the forwarding table on network routers

C. allows communication across the Internet to other private networks

D. allows servers and workstations to communicate across public network boundaries

Correct Answer: *A*

Niko9988 Highly Voted 2 years, 6 months ago

the question is indeed strange. in CCNA courser it was mentioned several time that NAT is not considered as a security means. So, i would answer like - the goal of using IPv4 private range is to optimize the network address usage

upvoted 8 times

Nicocisco 1 year, 3 months ago

Yes but thanks to private IPs, it is possible to create networks that are "disconnected" from the Internet and therefore have protection. It's the fact that NAT brings security because private IPs can go out on the internet that is false

upvoted 1 times

RougePotatoe 7 months, 1 week ago

The point Niko was making is that Cisco explicitly said NAT is not meant to be a security feature thus contradicting this answer and the logical separation it creates from the public network.

upvoted 1 times

cybernett Highly Voted 2 years, 3 months ago

By default private ip address cannot communicate across internet hence C is wrong,you will need NAT. So A is correct

upvoted 7 times

Ciscoman021 Most Recent 2 months, 2 weeks ago

Selected Answer: A

The goal achieved by the implementation of private IPv4 addressing on a network is:

A. provides an added level of protection against Internet exposure.

Private IPv4 addresses are reserved for use within private networks, and they are not routable on the Internet. By using private IPv4 addresses, organizations can create their own internal networks that are isolated from the public Internet, providing an added level of protection against external attacks and Internet exposure.

upvoted 1 times

shakyak 1 year, 6 months ago

I just confirmed the correct answer is "provides a reduction in size of the forwarding table on network routers"

upvoted 4 times

JonasWolfxin 10 months, 3 weeks ago

confirmed according to what?

upvoted 1 times

Hodicek 1 year, 6 months ago

A IS CORRECT ANSWER

upvoted 2 times

XBfoundX 2 years, 5 months ago

B cannot be the answer because even if I have a private enviroment I can still have a lots of private networks, By defualt we are using just a Default Route for going through Internet, if we have huge companies to be administrated maybe we can talk about BGP.

Basically I can still have a lot of different Networks an example is a Data Center lots of devices in different private networks

upvoted 1 times

Zerotime0 2 years, 5 months ago

Isnt it easy here that all others except A , gave options about outside networks?

upvoted 1 times

Mhatz 2 years, 7 months ago

I thought answer is D.

upvoted 3 times

illuded03jolted 11 months, 4 weeks ago

private address "allows communicating across public network boundaries"??? Stop smoking funny stuff bruuh!

upvoted 2 times

WikiLips 2 years, 6 months ago

private IPv4 addressing across public network boundaries?

upvoted 5 times

Question #638 *Topic 1*

Which type of attack is mitigated by dynamic ARP inspection?

A. DDoS

B. malware

C. man-in-the-middle

D. worm

Correct Answer: *C*

vadiminski Highly Voted 2 years ago

worm and malware are clearly wrong. you could assume that DDOS is correct, but it is not the primary reason of ARP poisoning. Hence, the given answer is correct

upvoted 11 times

Bash2111 Most Recent 1 year ago

An ARP spoofing, also known as ARP poisoning, is a Man in the Middle (MitM) attack

upvoted 1 times

Question #639 *Topic 1*

What is a function of a remote access VPN?

A. establishes a secure tunnel between two branch sites

B. uses cryptographic tunneling to protect the privacy of data for multiple users simultaneously

C. used exclusively when a user is connected to a company's internal network

D. allows the users to access company internal network resources through a secure tunnel

Correct Answer: *D*

msomali Highly Voted 1 year, 2 months ago

The answer is D
A:- this is used for site to site VPN

upvoted 8 times

Rramos37 Most Recent 1 year, 8 months ago

Yes, D

upvoted 2 times

Alsaher 2 years, 1 month ago

D is correct

upvoted 3 times

Question #640 *Topic 1*

What are two recommendations for protecting network ports from being exploited when located in an office space outside of an IT closet? (Choose two.)

A. enable the PortFast feature on ports

B. configure static ARP entries

C. configure ports to a fixed speed

D. implement port-based authentication

E. shut down unused ports

Correct Answer: *DE*

ProgSnob Highly Voted 1 year, 6 months ago

I was thinking static ARP entries would also prevent ports from being exploited but I guess the other two are actually better choices.

upvoted 7 times

Eyan Highly Voted 1 year, 8 months ago

checked and it is correct answers DE

upvoted 5 times

raydel92 Most Recent 1 year, 6 months ago

Selected Answer: DE

This might help:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

upvoted 2 times

Question #641 *Topic 1*

```
interface GigabitEthernet0/1
ip address 192.168.1.2 255.255.255.0
ip access-group 2699 in
!
access-list 2699 deny icmp any 10.10.1.0 0.0.0.255 echo
access-list 2699 deny ip any 10.20.1.0 0.0.0.255
access-list 2699 permit ip any 10.10.1.0 0.0.0.255
access-list 2699 permit tcp any 10.20.1.0 0.0.0.127 eq 22
```

Refer to the exhibit. A network administrator must permit SSH access to remotely manage routers in a network. The operations team resides on the 10.20.1.0/25 network. Which command will accomplish this task?

A. access-list 2699 permit udp 10.20.1.0 0.0.0.255

B. no access-list 2699 deny tcp any 10.20.1.0 0.0.0.127 eq 22

C. access-list 2699 permit tcp any 10.20.1.0 0.0.0.255 eq 22

D. no access-list 2699 deny ip any 10.20.1.0 0.0.0.255

Correct Answer: *D*

Already a statement is there in last to allow SSH Traffic for network 10.20.1.0 0.0.0.127, but Second statement says deny ip any 10.20.1.0 0.0.0.255, so how it will work once it is denied. So the right answer is remove the --- no access-list 2699 deny ip any 10.20.1.0 0.0.0.255.

distortion Highly Voted 1 year, 11 months ago

Answer is correct. The first encountered rule applies. The first rule is a deny so it never gets to the permit.

upvoted 11 times

dave1992 Highly Voted 1 year, 7 months ago

remember on ACLs that the rules apply in order. so it will never matter if you have the right config at the bottom if the one at the top is not allowing it.

upvoted 5 times

rmartin3444 Most Recent 2 months, 3 weeks ago

Shouldn't the wild card mask end in .127?

upvoted 2 times

splashy 8 months, 2 weeks ago

Are there different "rules" for the 2000-2699 range? According to Netacad (current course) and the latest packet tracer the "no access-list" command (in 0-200 range standard + extended) always deletes the whole ACL no matter if you specify an ACE after the command? This would nuke the ACL making tcp traffic for Operations possible but also all other traffic? B would give the same result?

In the current IOS you can also enter the acl subconfig for numbered ACL's like you can for named and delete ACE's by their sequence number which is the preferred and recommended way to do it.

upvoted 1 times

pagamar 1 year, 1 month ago

Sorry guys, but removing an ACE of a numbered ACL does not remove the entire ACL??? Of course, this will allow the SSH to pass, but I think it was not the goal of the command!

upvoted 2 times

Hodicek 1 year, 6 months ago

DELETE DENY FOR THIS LINE: access-list 2699 deny ip any 10.20.1.0 0.0.0.255
SO COMMAND IS: no access-list 2699 deny ip any 10.20.1.0 0.0.0.255 CAN SOLVE THE ISSUE , WHILE 22 PORT IS ALREADY ENABLED IN THE LAST COMMAND IN THE TABLE, NO NEED TO ADD IT AGAIN.

upvoted 2 times

rgg 1 year, 7 months ago

Why B is not correct?

upvoted 3 times

Question #642 *Topic 1*

A port security violation has occurred on a switch port due to the maximum MAC address count being exceeded. Which command must be configured to increment the security-violation count and forward an SNMP trap?

A. switchport port-security violation access

B. switchport port-security violation protect

C. switchport port-security violation restrict

D. switchport port-security violation shutdown

Correct Answer: *C*
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.html

AlvinSK0814 6 months, 3 weeks ago
Answer should be D

restrict—When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

shutdown—The interface is error-disabled when a violation occurs, and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.
upvoted 1 times

RougePotatoe 6 months, 2 weeks ago
The question didn't say anything about the port being shut down what makes you so sure it's D?
upvoted 6 times

highfivejohn 7 months, 2 weeks ago
Selected Answer: C
C is best answer, had the question included the port err-disabled then D
upvoted 4 times

creaguy 8 months ago
Selected Answer: D
Directly from the pdf provided reference.

When configuring port security violation modes, note the following information:
• protect—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
• restrict—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the SecurityViolation counter to increment.
• shutdown—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
upvoted 2 times

splashy 7 months ago
copy pasted directly out of provided link

•Restrict—A port security violation restricts data, causes the SecurityViolation counter to increment, and causes an SNMP Notification to be generated. The rate at which SNMP traps are generated can be controlled by the snmp-server enable traps port-security trap-rate command. The default value ("0") causes an SNMP trap to be generated for every security violation.

•Shutdown—A port security violation causes the interface to shut down immediately. When a secure port is in the error-disabled state, you can bring it out of this state by entering the errdisable recovery cause psecure-violation global configuration command or you can manually reenable it by entering the shutdown and no shut down interface configuration commands. This is the default mode.
upvoted 4 times

swampfartz 1 year, 2 months ago
The question never states that they want the port shutdown as well. Therefore the best answer it C.
upvoted 4 times

dave1992 1 year, 7 months ago
Protect - drops the packet with unknown src address until you remove a secure mac address to drop below the max value. no trap is sent.
Restrict- same but violation increments and TRAP sent to SNMP manager.
shutdown- puts interface in error disabled and sends a trap to the manager

upvoted 4 times

sgashashf 1 year, 3 months ago

When a port configured for "shutdown" experiences a violation, it sends an syslog message, sets the violation count to 1, then error disables. These questions are flat out wrong.

upvoted 1 times

DaBest 1 year, 8 months ago

C is correct, only Restrict will send a syslog/SNMP by default

upvoted 3 times

Chupacabro 1 year, 5 months ago

"Regarding the two correct answers, a port in port security restrict does cause the switch to issue log messages for a violating frame, send SNMP traps about that same event (if SNMP is configured), and increment the counter of violating frames." - CCNA 200-301 Vol. 2 by W. Odom

So I assume that D is also an answer(only based on the book) as it also sends syslog and SNMP (if configured). But I guess it's a matter of specificity of perks unlocked, so also C for me.

upvoted 3 times

Question #643 *Topic 1*

What is a practice that protects a network from VLAN hopping attacks?

A. Enable dynamic ARP inspection

B. Configure an ACL to prevent traffic from changing VLANs

C. Change native VLAN to an unused VLAN ID

D. Implement port security on internet-facing VLANs

Correct Answer: *C*

Question #644 *Topic 1*

Where does a switch maintain DHCP snooping information?

A. In the CAM table

B. In the frame forwarding database

C. In the MAC address table

D. In the binding database

Correct Answer: *D*

Networknovice Highly Voted 1 year ago

Keep in mind a CAM table, and a MAC table are the same thing! Therefore, since they are each listed, you can eliminate both as potential answers. One way to remember is that CAM is MAC spelled backward.

upvoted 14 times

raydel92 Highly Voted 1 year, 6 months ago

Selected Answer: D

A DHCP table is built that includes the source MAC address of a device on an untrusted port and the IP address assigned by the DHCP server to that device. The MAC address and IP address are bound together. Therefore, this table is called the DHCP snooping binding table.

Source: CCNAv7: Switching, Routing, and Wireless Essentials, chapter 11.3.2

upvoted 5 times

cormorant Most Recent 5 months, 4 weeks ago

the cam and mac table are the same thing. there is no such thing as a frame forwarding databse. this leaves only d- binding database

upvoted 3 times

dave1992 1 year, 7 months ago

Dynamic Arp Inspection inspects DHCP traffic and tracks the IP address to the mac Address, so if invalid traffic comes with spoofed IP, its dropped because its not in the table. (DHCP snooping has to be enabled first)

upvoted 1 times

BooleanPizza 1 year, 9 months ago

D is correct.
https://community.fs.com/blog/what-is-dhcp-snooping-and-how-it-works.html

upvoted 2 times

Question #645 *Topic 1*

A network administrator must configure SSH for remote access to router R1. The requirement is to use a public and private key pair to encrypt management traffic to and from the connecting client. Which configuration, when applied, meets the requirements?

A. R1#enable R1#configure terminal R1(config)#ip domain-name cisco.com R1(config)#crypto key generate ec keysize 1024

B. R1#enable R1#configure terminal R1(config)#ip domain-name cisco.com R1(config)#crypto key generate ec keysize 2048

C. R1#enable R1#configure terminal R1(config)#ip domain-name cisco.com R1(config)#crypto key encrypt rsa name myKey

D. R1#enable R1#configure terminal R1(config)#ip domain-name cisco.com R1(config)#crypto key generate rsa modulus 1024

Correct Answer: *D*

dicksonpwc Highly Voted 1 year, 9 months ago

crypto key generate rsa [general-keys | usage-keys | signature | encryption] [label key-label] [exportable] [modulus modulus-size] [storage devicename :] [redundancy] [on devicename :]

modulus modulus-size

By default, the modulus of a certification authority (CA) key is 1024 bits. The recommended modulus for a CA key is 2048 bits. The range of a CA key modulus is from 350 to 4096 bits. As the default key is 1024 bits. So that the answer D is correct

upvoted 17 times

Question #646 *Topic 1*

When a WLAN with WPA2 PSK is configured in the Wireless LAN Controller GUI, which format is supported?

A. decimal

B. ASCII

C. unicode

D. base64

Correct Answer: *B*

Smaritz Highly Voted 1 year, 2 months ago

ASCII and Hex

upvoted 7 times

Question #647 *Topic 1*

```
access-list 101 permit ospf any any
 access-list 101 permit tcp any any eq 179
 access-list 101 permit tcp any eq 179 any
 access-list 101 permit gre any any
 access-list 101 permit esp any any

access-list 101 deny ospf any any
 access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet
 access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq 500
 access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq 4500
 access-list 101 deny ip any any log

interface Ethernet0/0
  ip address 10.1.1.25 255.255.255.0
  ip access-group 101 in
```

Refer to the exhibit. A network administrator has been tasked with securing VTY access to a router. Which access-list entry accomplishes this task?

A. access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet

B. access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq scp

C. access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq https

D. access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq ssh

Correct Answer: *D*

bootloader_jack Highly Voted 1 year, 8 months ago

there is no ssh entry in the table. I did not understand the answer.

upvoted 18 times

kadamske 1 year, 8 months ago

Me neither

upvoted 4 times

kokoyul Highly Voted 1 year, 8 months ago

"A network administrator has been tasked with securing VTY access to a router".
You need to secure VTY access and add SSH too, not just Telnet.

upvoted 14 times

testsssssssss 1 year, 4 months ago

"Which access-list entry accomplishes this task" = Which of the lines does secure it.
Telnet is trash, but is the only one configured on this access list.

upvoted 5 times

ac89l Most Recent 3 weeks, 3 days ago

another horrible question

upvoted 2 times

Njavwa 2 months, 1 week ago

some of these questions are not clear, the ideal is to look for pain points, like secure, UDP, TCP etc
from what is given there is no config for SSH that is explicitly defined

upvoted 1 times

Yaqub009 3 months, 3 weeks ago

Selected Answer: A

Router(config)#access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq ?
<0-65535> Port number
ftp File Transfer Protocol (21)
pop3 Post Office Protocol v3 (110)
smtp Simple Mail Transport Protocol (25)
telnet Telnet (23)
www World Wide Web (HTTP, 80)

D. access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq ssh - incorrect.
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq 22 - correct

Only A is correct command.

upvoted 2 times

splashy 7 months, 3 weeks ago

Switch(config)#access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq ?
<0-65535> Port number
ftp File Transfer Protocol (21)
pop3 Post Office Protocol v3 (110)
smtp Simple Mail Transport Protocol (25)
telnet Telnet (23)
www World Wide Web (HTTP, 80)

Can't get "eq ssh" in Packet Tracer only "eq 22" don't have any real cisco gear to test on atm.

upvoted 5 times

BieLey 8 months, 1 week ago

Selected Answer: D

Telnet is not secure
SSH = secure

Don't think you need to look at the exhibit, that will just confuse everything.

upvoted 5 times

evil3xx 8 months, 2 weeks ago

pay attention to 'securing'

upvoted 1 times

Amonzon 10 months, 1 week ago

See the exhibit the TELNET is configured it is just missing SSH. Correct answer is D

upvoted 3 times

GohanF2 10 months, 1 week ago

I assume as the access list for allowing telnet connection is already setup , we just need to add the access list for securing the ssh connection as well and thats why the answer is D

upvoted 1 times

MDK94 11 months, 1 week ago

I really hope Cisco don't think that the answer is actually D as well because EQ SSH isn't a real command entry option, for SSH you need to use the port number 22. Tested on both my own real hardware and in packet tracer, both show the same thing: https://ibb.co/6yr5z0s

Answer is 100% A

The question is asking "Which access-list entry accomplishes this task" I make that out to mean, "Out of the entries in the access-list, which is securing the vty lines", NOT "Which command do you need to add to make the vty lines secure".

upvoted 9 times

WINDSON 11 months, 2 weeks ago

Answer A has been already in the configured in the list before. So how can use choose answer A ?

upvoted 3 times

DARKK 1 year ago

“Which access list *Entry* …”
A lot of people misunderstood this question, securing mean you should Add shh to the ACL, the entry that would accomplish it is one of the answers, it doesn’t refer to the existing entries as none of those secure access. It’s really easy if you don’t overthink it. It doesn’t specify “previous or following entries” so it likely refers to the an entry you would add to the ACL.

upvoted 4 times

pagamar 1 year, 1 month ago

Hi guys, two things.
First, the ACL is applied inbound, but 10.1.1.x (source) is the address of the interface, so??? This is one of the many defects of the exhibit (i.e. OSPF permit, then deny...)!
Second, the "telnet" ACE is "partially securing" the VTY access, since it defines the only networks allowed to use the protocol.
Or not? :-) So, I agree (bleah!) with "A".

upvoted 2 times

igl00 1 year, 2 months ago

1. "securing VTY access to a router" doesn't rally mean SECURE access, but a way of communicating with the router.
2.Question says Referr to the exibit, meaning answer should come from the exibit.
3. Although D will be a correct answer, it is not in the exibit, and answer A will satisfy all requirements. Question could have been worded better.

upvoted 2 times

Irv23 1 year, 3 months ago

I can see why people are confused about this question. When they ask, which access-list entry accomplishes this task, the entries they are mentioning are the 4 answers below the question, not the exhibit. Also, when they say, refer to the exhibit I think they mean which Answer will need to be added in the Exhibit to secure VTY access to a router. So an ssh entry is required in the table. Hopefully this helps.

upvoted 6 times

LilGhost_404 1 year, 3 months ago

Selected Answer: A

the answer is A, the question is clear, "Which access-list entry accomplishes this task" telnet isnt in the entrys.
your can only activate telnet or only ssh or both to acces and configure a switch.
you dont need telnet + ssh. your could have one of them or both.
upvoted 1 times

LilGhost_404 1 year, 3 months ago
sorry for the typo, SSH is not in the entrys...
upvoted 1 times

Question #648 *Topic 1*

Which two protocols must be disabled to increase security for management connections to a Wireless LAN Controller? (Choose two.)

A. HTTPS

B. SSH

C. HTTP

D. Telnet

E. TFTP

Correct Answer: *CD*

dave1992 Highly Voted 1 year, 5 months ago
HTTP and Telnet both are unsecure. That's why we have HTTPS and SSH. TFTP isn't used for WLC topics. Only simple file transferring unencrypted.
upvoted 8 times

cortib Most Recent 1 year, 8 months ago
correct.
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109669-secure-wlc.html#T8
upvoted 4 times

Question #649 *Topic 1*

Which security program element involves installing badge readers on data-center doors to allow workers to enter and exit based on their job roles?

A. physical access control

B. biometrics

C. role-based access control

D. multifactor authentication

Correct Answer: *A*

dicksonpwc Highly Voted 1 year, 9 months ago

Physical access control systems (PACS) are a type of physical security designed to restrict or allow access to a certain area or building. ... Physical access control examples of credentials include fobs and key card entry systems, encrypted badges, mobile credentials, PIN codes and passwords.

upvoted 8 times

DARKK Most Recent 1 year ago

This is definitely physical security, used to enforce role based access. So it's a weird question, but since the bottom line is restricting physical access

upvoted 1 times

hojusigol 1 year, 3 months ago

look like role-based BUT the door is 'physically' blocking you so that you cannot access. so it is PACS. the point is the 'door'

upvoted 1 times

LilGhost_404 1 year, 3 months ago

Selected Answer: A

A is more accurate, if someone already passed inside, it doesnt matter wich role he has, the person is already on the datacenter room.

upvoted 1 times

DaBest 1 year, 8 months ago

i thought "role-based access control" was more accurate, but i guess the answer is "Physical access control" for some reason..

upvoted 3 times

Question #650 *Topic 1*

Which function is performed by DHCP snooping?

A. listens to multicast traffic for packet forwarding

B. rate-limits certain traffic

C. propagates VLAN information between switches

D. provides DDoS mitigation

Correct Answer: *B*

raydel92 Highly Voted 1 year, 6 months ago

Selected Answer: B

Use the following steps to enable DHCP snooping:

Step 1. Enable DHCP snooping by using the "ip dhcp snooping" global configuration command.
Step 2. On trusted ports, use the "ip dhcp snooping trust" interface configuration command.
Step 3. Limit the number of DHCP discovery messages that can be received per second on untrusted ports by using the "ip dhcp snooping limit rate (rate in secs)" interface configuration command.
Step 4. Enable DHCP snooping by VLAN, or by a range of VLANs, by using the "ip dhcp snooping vlan (vlan or vlan range)" global configuration command.

upvoted 6 times

VictorCisco Most Recent 2 months, 1 week ago

Selected Answer: D

The answer is D (provides DDoS mitigation). One of the attacks that it prevents is DHCP Starvation attack, which is a dynial of service.

Definitely not B.
Read carefully "rate-limit certain TRAFFIC !" it is not the same as limit the number of DHCP discovery messages!
rate-limit kinda ~ speed-limit. Definitely not that DHCP does.

upvoted 1 times

leooel 5 months, 2 weeks ago

Selected Answer: B

answer is B

upvoted 1 times

SONG00992 1 year, 2 months ago

Rate-limits DHCP traffic from trusted and untrusted sources.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/snoodhcp.pdf

upvoted 3 times

sovafal192 1 year, 4 months ago

Selected Answer: B

I go with B, bc:
In DHCP process you ave:
DHCP discover -> broadcast
DHCP Offer -> unicast
DHCP acknowledgement -> unicast
so we can sort out A, because there is no multicast packet in the DHCP procedure.
C and D are also bad, but because they are not in sight with dhcp...

upvoted 1 times

Eyan 1 year, 8 months ago

answer is correct, another function for that it determines which DHCP messages are valid

I checked that and found its on Cisco 200-105 exam

upvoted 1 times

CiscoTerminator 1 year, 9 months ago

Answer B is correct: https://community.cisco.com/t5/switching/ip-dhcp-snooping-limit-rate-command/td-p/1203764 . There is actually a command just for this rate limiting feature on both trusted and untrusted interfaces.

upvoted 2 times

Samuelpn96 1 year, 9 months ago

I think the answer is D (provides DDoS mitigation). One of the attacks that it prevents is DHCP Starvation attack, which is a dynial of service.

Common Attacks Prevented by DHCP Snooping

DHCP Spoofing Attack
DHCP spoofing occurs when an attacker attempts to respond to DHCP requests and trying to list itself (spoof) as the default gateway or DNS server, hence, initiating a man in the middle attack. With that, it is possible that they can intercept traffic from users before forwarding to the real gateway or perform DoS by flooding the real DHCP server with requests to choke IP address resources.

DHCP Starvation Attack
DHCP starvation attack commonly targets network DHCP servers, in a bid to flood the authorized DHCP server with DHCP REQUEST messages using spoofed source MAC addresses. The DHCP server will respond to all requests, not knowing this is a DHCP starvation attack, by assigning available IP addresses, resulting in the depletion of DHCP pool.

https://community.fs.com/blog/what-is-dhcp-snooping-and-how-it-works.html
upvoted 3 times

ccna_goat 7 months, 3 weeks ago

DHCP helps prevent man-in-the-middle attacks, not DDoS
upvoted 2 times

kadamske 1 year, 8 months ago

The answer is not D because that is "DDOS" Distributed Denial Of Service, it is difference from just DOS
upvoted 4 times

Samuelpn96 1 year, 8 months ago

A denial-of-service (DoS) attack floods a server with traffic, making a website or resource unavailable. A distributed denial-of-service (DDoS) attack is a DoS attack that uses multiple computers or machines to flood a targeted resource. Both types of attacks overload a server or web application with the goal of interrupting services.

The principal difference between a DoS and a DDoS is that the former is a system-on-system attack, while the latter involves several systems attacking a single system.

https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos

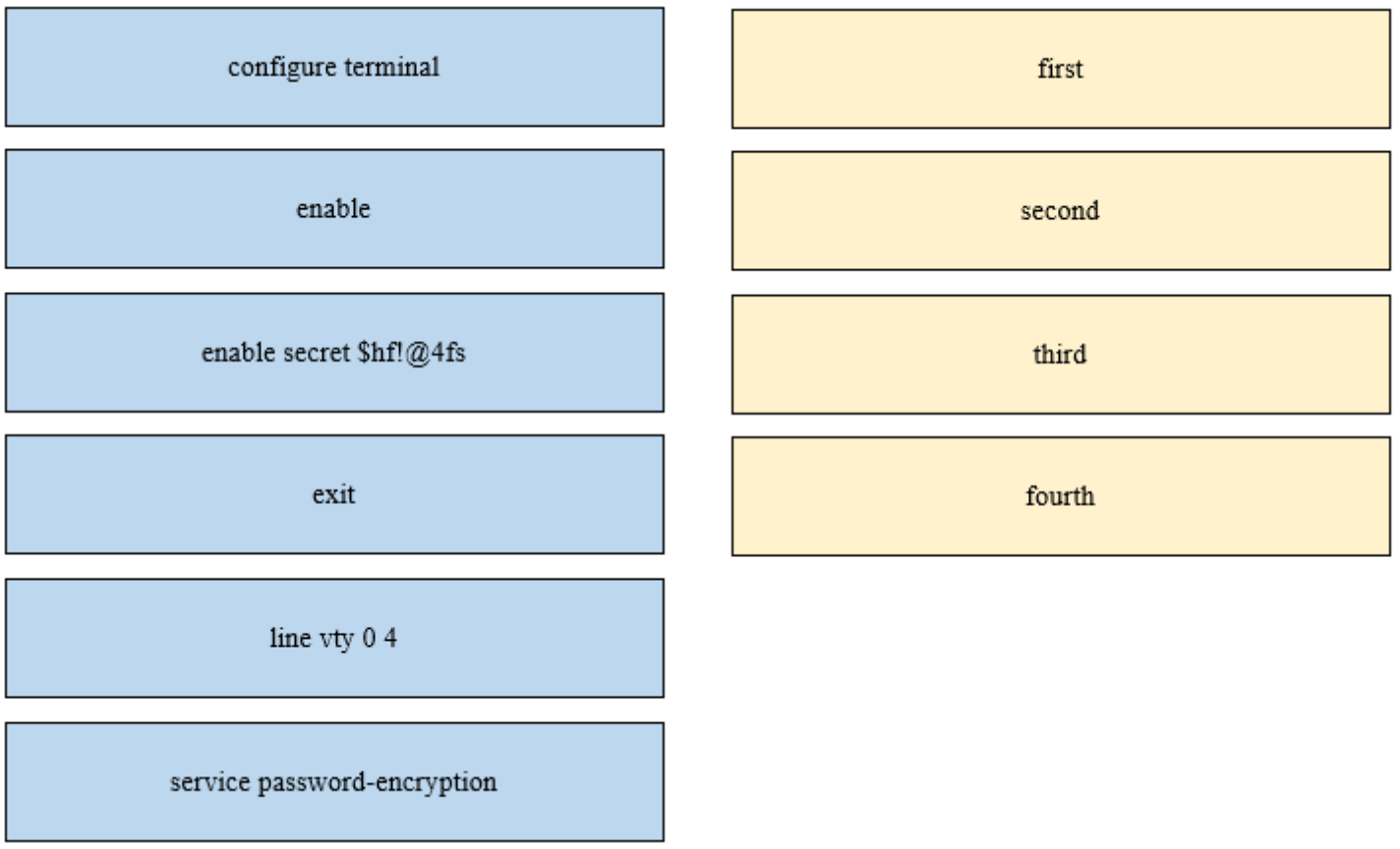
From what I understand, a DDOS still is a Denial of Service, but originated from multiple sources.
upvoted 2 times

Question #651 *Topic 1*

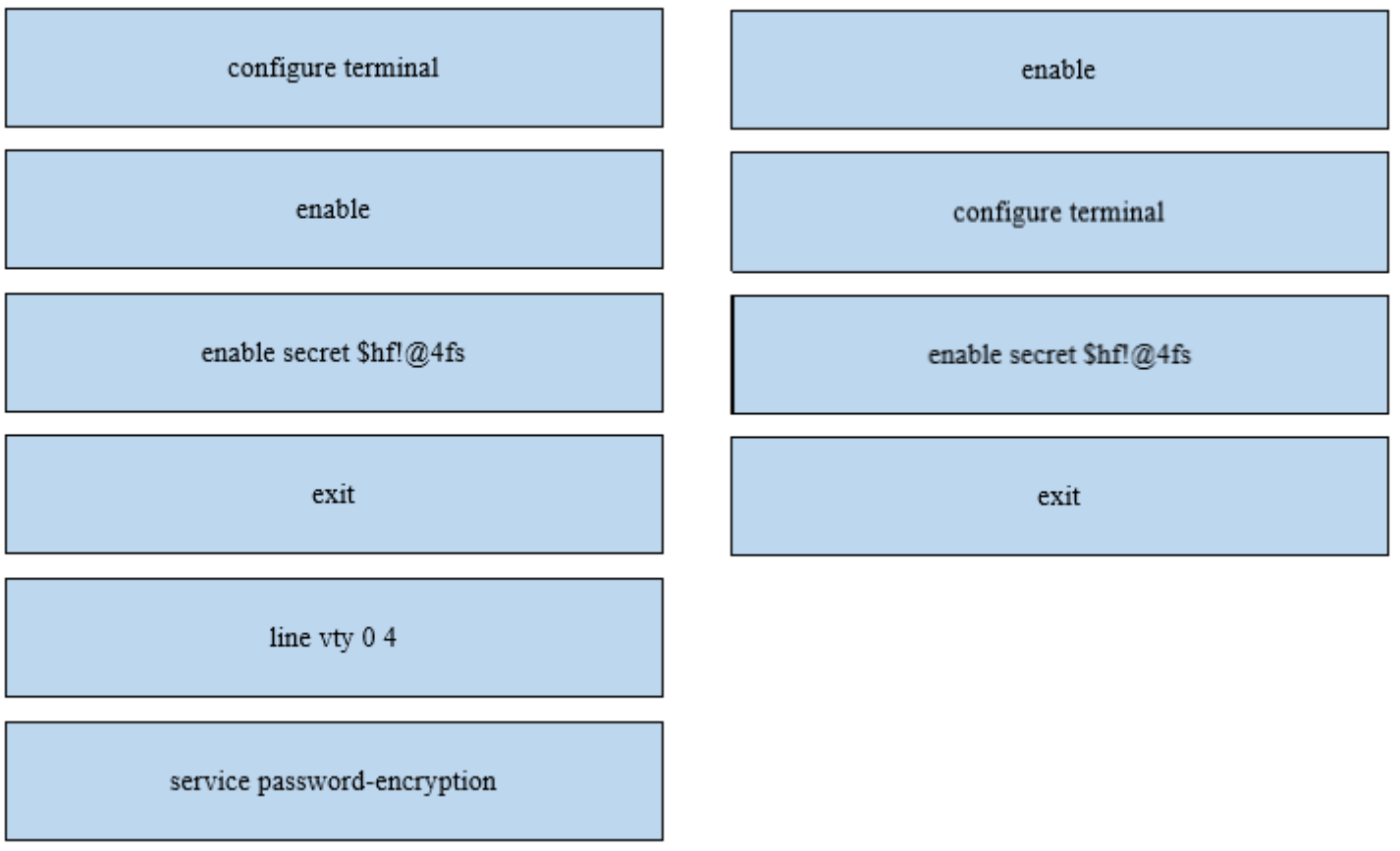
DRAG DROP -

An engineer is configuring an encrypted password for the enable command on a router where the local user database has already been configured. Drag and drop the configuration commands from the left into the correct sequence on the right. Not all commands are used.

Select and Place:



Correct Answer:



sasquatchshrimp Highly Voted 10 months ago

No one:
Cisco: A guy is doing something, what are the exact steps and order?

upvoted 18 times

kamlo 6 months, 1 week ago

Hahahaha ggggggggold :D

upvoted 1 times

CozTurk Highly Voted 1 year, 8 months ago

Very poorly worded question. Is the aim to configure an encrypted PW or to make sure passwords aren't stored in clear text. Answer could very well be the enable secret Fucking SMFH Cisco

upvoted 16 times

iGlitch Most Recent 1 year ago

TRICKY, but the answers are correct.

upvoted 2 times

DARKK 1 year ago

Unless the user database includes user name and pwd , Enable secret is correct.
upvoted 1 times

aosroyal 1 year, 1 month ago
bad qn
upvoted 3 times

SONG00992 1 year, 2 months ago
enable password - it will enables a password that based on a clear text, unlike,

enable secret - it will enables a password and password encryption that based on the md5 hashing algorithm. This is is a most recommended command to supply while enabling a password to any cisco network devices.

https://community.cisco.com/t5/network-security/enable-password-and-enable-secret/td-p/1931118
upvoted 1 times

Shamwedge 1 year, 3 months ago
The local user account only gets you access to the router, you still need a seperate password for the enable command. Answer is enable secret
upvoted 1 times

RougePotatoe 7 months, 1 week ago
Incorrect, if you configure privilege level 15 it gets them directly to the user exec status.
upvoted 1 times

cdp_neighbor 5 months, 2 weeks ago
Nope, unless you've configured "aaa authorization exec"
upvoted 1 times

awashenko 1 year, 4 months ago
Enable, Config T, Enable Secret, Exit.

Service Password-Encryption encrypts plain text.
upvoted 4 times

Cho1571 1 year, 4 months ago
you need the 4 steps plus the enable secret right before exit (and exit is optional)
upvoted 1 times

Hodicek 1 year, 6 months ago
ENABLE - CONF T - ENABLE SECRET ..... - EXIT
upvoted 4 times

Lala4eva 1 year, 6 months ago
According to the CCNA Routing and Switching Portable Command Guide (Pg. 99, 237-238) book it shows the following:

Password Encryption:
R1(Config)#: service password-encryption
R1(Config)#: enable password cisco
R1(Config)#: line console 0
R1(Config)#: password cisco
R1(Config)#: no service password-encryption
upvoted 1 times

lucky1559 1 year, 9 months ago
Here we are talking bout encrypted password for enable mode so it should be enable secret command.
upvoted 5 times

WHTM 1 year, 9 months ago
'local user database has already been configured"
Correct answer
upvoted 1 times

stanibarb 1 year, 8 months ago
answer yourself if the local user database include encrypted password for the enable command, which is the primary task here
upvoted 4 times

kay123 1 year, 9 months ago
this doesn't seem correct
upvoted 2 times

django1001 1 year, 9 months ago
Doesn't seem correct... it should be enable secret instead of service password encryption.
upvoted 13 times

Question #652 *Topic 1*

Which protocol is used for secure remote CLI access?

A. Telnet

B. HTTP

C. HTTPS

D. SSH

Correct Answer: *D*

Question #653 *Topic 1*

Which implementation provides the strongest encryption combination for the wireless environment?

A. WEP

B. WPA + TKIP

C. WPA + AES

D. WPA2 + AES

Correct Answer: *D*

Question #654 *Topic 1*

What does physical access control regulate?

A. access to networking equipment and facilities

B. access to servers to prevent malicious activity

C. access to specific networks based on business function

D. access to computer networks and file systems

Correct Answer: *A*

nickname_fordiscussions Highly Voted 1 year, 1 month ago

A B and D smh

upvoted 5 times

DARKK Highly Voted 1 year ago

Facilities is the key word here, as it is solely Physical, the other options can be breached via the network as well.

upvoted 5 times

Question #655 *Topic 1*

A network engineer is asked to configure VLANS 2, 3, and 4 for a new implementation. Some ports must be assigned to the new VLANS with unused ports remaining. Which action should be taken for the unused ports?

A. configure in a nondefault native VLAN

B. configure ports in the native VLAN

C. configure ports in a black hole VLAN

D. configure ports as access ports

Correct Answer: *C*

sasquatchshrimp Highly Voted 10 months ago

Leave it to cisco to use terminology that engineers of many years have never heard or used... smh

upvoted 13 times

Phonon Highly Voted 5 months ago

Selected Answer: C

A black hole VLAN is a virtual LAN that is configured on a network switch, but it is not connected to any device or port. Traffic that is sent to a port in a black hole VLAN is discarded, effectively "sinking" into a "black hole." Black hole VLANs are sometimes used as a security measure to isolate or quarantine certain ports or devices, or to prevent unauthorized access or traffic on a network.

upvoted 5 times

StingVN Most Recent 2 weeks, 3 days ago

Selected Answer: D

should be D

upvoted 1 times

4aynick 1 month, 4 weeks ago

no CCNA scope

upvoted 1 times

nathnotnut 3 months, 1 week ago

black hole lang ni enigma alam ko e

upvoted 2 times

Garfieldcat 7 months, 4 weeks ago

so...answer A :configure in "non-default native VLAN" has the same meaning as blackhole vlan except omitting one more step to shut it down

upvoted 1 times

dhrubo113 10 months, 2 weeks ago

unused so goes directly to Black hole.

upvoted 1 times

AWSEMA 11 months, 1 week ago

Selected Answer: C

Some administrators take unused ports a step further by creating a black hole VLAN. This is a VLAN that's local to this switch only, has no layer 3 switch virtual interface (SVI) configured for it, and isn't allowed to traverse an uplink trunk port

upvoted 1 times

onikafei 1 year, 3 months ago

Selected Answer: C

C is correct!

A black hole is a vlan that is unused where you put unused ports in or hosts that you dont want to be on the network.

upvoted 4 times

Question #656 *Topic 1*

When a WPA2-PSK WLAN is configured in the Wireless LAN Controller, what is the minimum number of characters that is required in ASCII format?

A. 6

B. 8

C. 12

D. 18

Correct Answer: *B*

Futchihoore Highly Voted 2 years, 6 months ago

WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01010001.html

upvoted 19 times

Question #657 *Topic 1*

What mechanism carries multicast traffic between remote sites and supports encryption?

A. ISATAP

B. IPsec over ISATAP

C. GRE

D. GRE over IPsec

Correct Answer: *D*

Raooff Highly Voted 2 years, 5 months ago

CCNA security course
Ipsec dosent support multicast, that is why GRE used with VPN, and as long as the GRE is not totally secure, the whole GRE. Encapsulation can be encapsulated in ipsec header so nlw we have both " mulitcast ability and security"

upvoted 15 times

dicksonpwc Highly Voted 1 year, 9 months ago

D is correct.
Explanation:
IPsec cannot encapsulate multicast, broadcast, or non-IP packets, and GRE cannot authenticate and encrypt packets. Based on the same principle, these applications encapsulate packets as IP packets using GRE and then transmit the packets over IPsec tunnels

upvoted 6 times

gaber 1 year, 5 months ago

https://kb.juniper.net/InfoCenter/index?page=content&id=KB19372

upvoted 1 times

StingVN Most Recent 2 weeks, 3 days ago

Selected Answer: D

D is the correct answer

upvoted 1 times

Ciscoman021 2 months, 2 weeks ago

Selected Answer: D

The mechanism that carries multicast traffic between remote sites and supports encryption is D) GRE over IPsec.

upvoted 1 times

Phonon 5 months ago

Selected Answer: D

IPsec over GRE (Generic Routing Encapsulation) is a mechanism that can be used to carry multicast traffic between remote sites and supports encryption. It combines the functionality of both IPsec and GRE to provide secure and efficient communication between sites. With IPsec over GRE, the multicast traffic is encapsulated inside a GRE tunnel, and the tunnel is then protected using IPsec encryption. This allows the multicast traffic to be securely transmitted over the public internet or other untrusted networks.

upvoted 1 times

vadiminski 2 years ago

This video gives a good explanation
https://www.youtube.com/watch?v=ytAqv7qHGyU
TL:DR: GRE supports multicast but does not offer encryption. Therefore, use GRE over IPsec for encryption

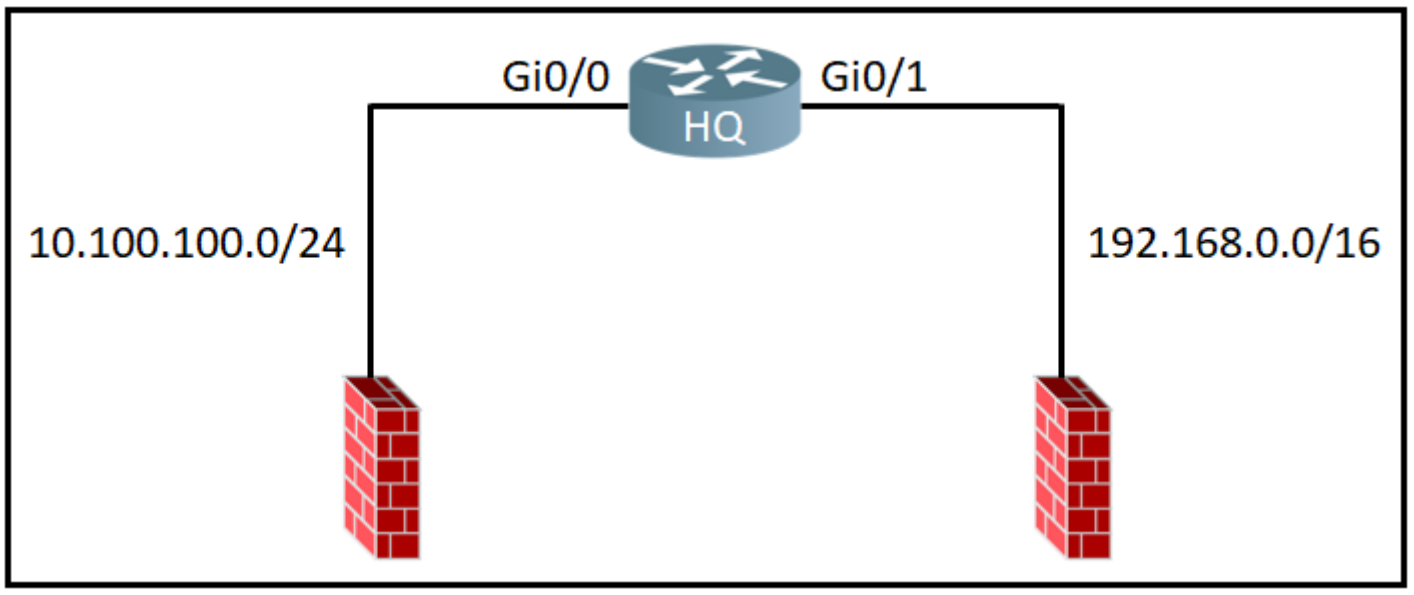
upvoted 3 times

Mhatz 2 years, 7 months ago

Reference please

upvoted 2 times

Question #658 *Topic 1*



Refer to the exhibit. An access-list is required to permit traffic from any host on interface Gi0/0 and deny traffic from interface Gi0/1. Which access list must be applied?

A. ip access-list standard 99 permit 10.100.100.0 0.0.0.255 deny 192.168.0.0 0.0.255.255

B. ip access-list standard 99 permit 10.100.100.0 0.0.0.255 deny 192.168.0.0 0.255.255.255

C. ip access-list standard 199 permit 10.100.100.0 0.0.0.255 deny 192.168.0.0 0.255.255.255

D. ip access-list standard 199 permit 10.100.100.0 0.0.0.255 deny 192.168.0.0 0.0.255.255

Correct Answer: *A*

DARKK Highly Voted 1 year ago
A is correct, standard is 1-99 or 1300-1999
upvoted 11 times

deluxeccna Most Recent 1 month, 3 weeks ago
Selected Answer: A
Answer is A
upvoted 2 times

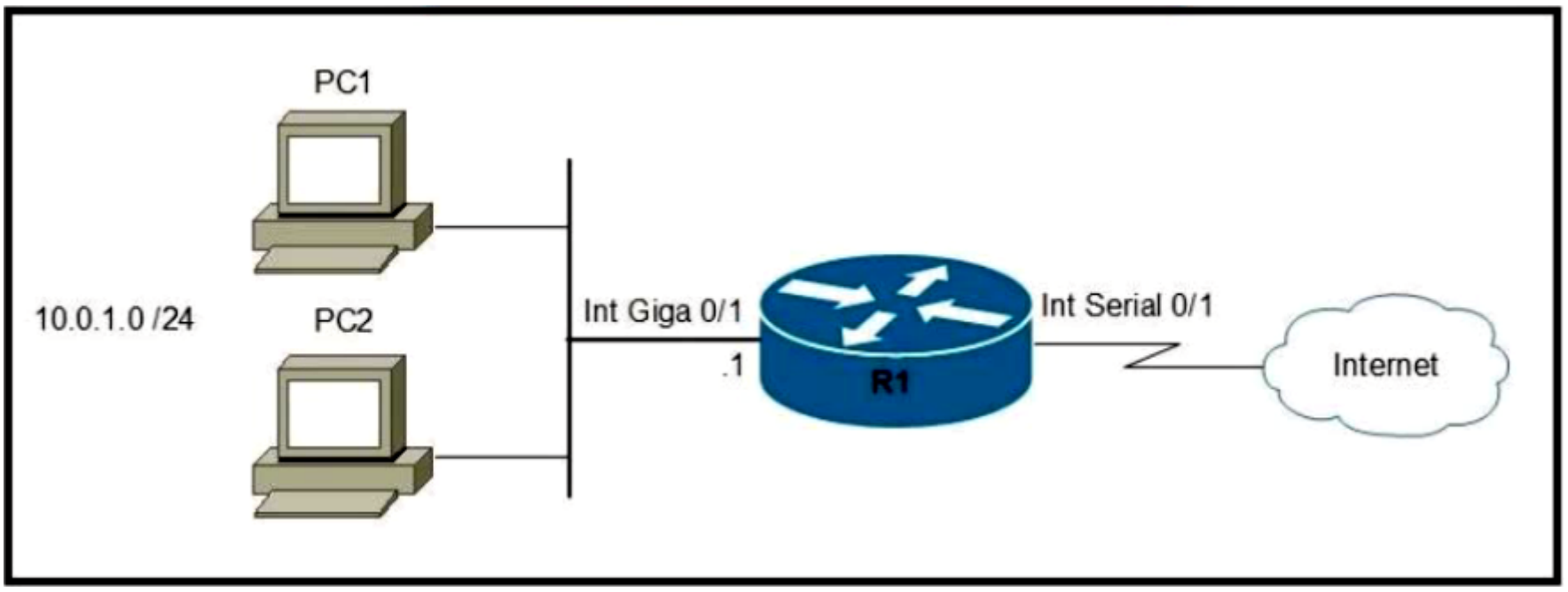
GigaGremlin 8 months ago
Selected Answer: B
Because of the /16
upvoted 1 times

fransCISCO 4 months, 1 week ago
it is A look at the wildcard
upvoted 3 times

Networknovice 1 year ago
It is not choice D because for Standard Access Control Lists, Access list number must be between 1–99 or 1300–1999. Choice D's access list number was not within this range.

https://www.omnisecu.com/cisco-certified-network-associate-ccna/standard-access-control-lists.php#:~:text=Standard%20Access%20Control%20Lists%20(ACLs)%20are%20the%20oldest%20type%20of,access%2Dlists%22%20IOS%20command.
upvoted 3 times

Question #659 *Topic 1*



Refer to the exhibit. Which two commands must be configured on router R1 to enable the router to accept secure remote-access connections? (Choose two.)

A. ip ssh pubkey-chain

B. username cisco password 0 cisco

C. crypto key generate rsa

D. transport input telnet

E. login console

Correct Answer: *BC*

StingVN 2 weeks, 3 days ago

Selected Answer: AC

The correct answers are:

A. ip ssh pubkey-chain
C. crypto key generate rsa

These two commands are required to enable secure remote-access connections on router R1.

Option A (ip ssh pubkey-chain) enables SSH connections using public key authentication, which is a more secure method compared to password-based authentication.

Option C (crypto key generate rsa) generates an RSA key pair that is used for encryption and authentication purposes when establishing secure connections, such as SSH.

The other options are not directly related to enabling secure remote-access connections:

B. username cisco password 0 cisco - This command creates a local user account with the username "cisco" and a plaintext password. However, it does not enable secure remote-access connections.

D. transport input telnet - This command allows telnet access to the router, but telnet is not a secure protocol.

E. login console - This command enables console line authentication, but it is not specific to remote-access connections or providing security for them.

upvoted 1 times

DARKK 1 year ago

Why not SSH? A

upvoted 1 times

Murphy2022 8 months ago

because that command doesn't exist inside CLI

upvoted 1 times

guisam 5 months, 4 weeks ago

https://networklessons.com/uncategorized/ssh-public-key-authentication-cisco-ios

upvoted 1 times

mantest 1 year ago

Ans is correct. Watch the below given video for the reference - https://www.oreilly.com/content/how-do-i-configure-a-cisco-router-for-secure-remote-access-using-ssh/

upvoted 4 times

Networknovice 1 year ago

Regarding answer B, can passwords have spaces?? wouldn't the password be "0 cisco"?? Correct me if I'm wrong, but aren't spaces disallowed as a password requirement?

upvoted 2 times

iGlitch 1 year ago

This is a document by NSA, I found it really helpful:

https://media.defense.gov/2022/Feb/17/2002940795/-1/-1/1/CSI_CISCO_PASSWORD_TYPES_BEST_PRACTICES_20220217.PDF

upvoted 4 times

splashy 8 months, 1 week ago

Great link!

upvoted 1 times

Question #660 *Topic 1*

Which service is missing when RADIUS is selected to provide management access to the WLC?

A. authorization

B. authentication

C. accounting

D. confidentiality

Correct Answer: *D*
Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.
With RADIUS only the password is encrypted while the other information such as username, accounting information, etc are not encrypted.
Encryption is "the process of converting information or data into a code, especially to prevent unauthorized access". So since RADIUS only encrypts the passwords, there is no confidentiality.

StingVN 2 weeks, 3 days ago

Selected Answer: C
C. Accounting

When RADIUS is used to provide management access to a Wireless LAN Controller (WLC), the service that is missing is accounting. RADIUS primarily handles authentication and authorization for network access. Authentication verifies the identity of the user or device, while authorization determines the level of access granted to the authenticated entity. However, accounting, which involves tracking and recording of network resource usage, is not typically provided by RADIUS in the context of management access to a WLC.
upvoted 1 times

iGlitch 1 year ago
Unlike TACACS+, RADIUS by itself provides no encryption of all traffic. It protects only a small part of the traffic, notably the passwords.
upvoted 2 times

Networknovice 1 year ago
Answer is correct.

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.

https://en.wikipedia.org/wiki/RADIUS#:~:text=Remote%20Authentication%20Dial%2DIn%20User,and%20use%20a%20network%20service.
upvoted 2 times

iGlitch 1 year ago
OK, but why it's missing confidentiality tho?
upvoted 1 times

martialstriker09 11 months, 2 weeks ago
Confidentiality means "the state of keeping or being kept secret or private". With RADIUS only the password is encrypted while the other information such as username, accounting information, etc are not encrypted. Encryption is "the process of converting information or data into a code, especially to prevent unauthorized access". So since RADIUS only encrypts the passwords, that means its the confidentiality is missing
upvoted 5 times

Question #661 *Topic 1*

Which action implements physical access control as part of the security program of an organization?

A. setting up IP cameras to monitor key infrastructure

B. configuring a password for the console port

C. backing up syslogs at a remote location

D. configuring enable passwords on network devices

Correct Answer: *B*

highfivejohn Highly Voted 7 months, 2 weeks ago

Selected Answer: A

A is the only answer that lists a 'Physical' measure to counter-act 'Physical' security vulnerabilities. Make all the passwords you want on all your console ports, but if someone who shouldn't have access gets to one your 'Physical' security has already failed.

upvoted 11 times

dropspablo Most Recent 2 days, 6 hours ago

Selected Answer: A

Physical access control: Infrastructure locations, such as network
closets and data centers, should remain securely locked. Badge access to sensitive locations is a scalable solution, offering an audit trail of identities and timestamps when access is granted. Administrators can control access on a granular basis and quickly remove access when an employee is dismissed. (Official-Cert-Guide-Volume-2)

upvoted 1 times

Zers 2 weeks, 2 days ago

Are these question makers high? What do they even mean by physical security?
Physical security means we need to stop access to anyone unauthorized to the server, how is a password helping in that?

upvoted 2 times

jonathan126 1 month, 2 weeks ago

A - physical access control (detective control)
B - Authentication (AAA)
C - Availability (CIA)
D - Authentication (AAA)

upvoted 1 times

Ciscoman021 1 month, 4 weeks ago

Selected Answer: B

B. Configuring a password for the console port implements physical access control as part of the security program of an organization. This is because the console port is a physical port on a network device that provides direct access to the device's configuration and management interfaces. By setting up a password for the console port, only authorized personnel can physically access the device and make changes to its configuration, which helps prevent unauthorized access and potential security breaches.

Option A involves monitoring infrastructure through IP cameras, which falls under the category of physical security but does not necessarily provide access control. Option C involves backing up logs at a remote location, which is important for auditing and incident response, but does not directly relate to physical access control. Option D involves configuring enable passwords on network devices, which provides logical access control rather than physical access control.

upvoted 2 times

QBangash 3 months ago

physical access control is the key to this answer.

upvoted 2 times

hamish88 4 months ago

As per my understanding, it should be A.

Physical access control: Infrastructure locations, such as network closets and data centers, should remain securely locked. Administrators should control physical access and quickly remove access when an employee is dismissed.

Az controlling access is part of this section I would go with A. Moreover:

https://www.cisco.com/c/dam/global/hr_hr/assets/images/Cisco_rjesenja_za_zastitu_objekata_i_imovine_-_Alper_Erdal.pdf

https://www.cisco.com/c/dam/global/hr_hr/assets/ciscoconnect/2013/pdfs/Cisco_Physical_Security_solutions_Radenko_Citakovic.pdf

upvoted 1 times

splashy 7 months ago

Selected Answer: B

When you have physical access to a console port, a camera won't tap you on the shoulder and prevent you from accessing it, a console password however will.
upvoted 4 times

VictorCisco 2 months, 1 week ago
Password can't prevent from PHYSICAL access to a port as well :)
upvoted 1 times

Garfieldcat 8 months ago
if B is the answer, why D isn't ? Therefore, I opt A
upvoted 1 times

splashy 7 months ago
enable passwords don't require physical access to the device to be used
upvoted 2 times

BieLey 8 months, 1 week ago
Selected Answer: B
Personal credentials: Most PACS require a user to have identifying credentials to enter a facility or access data. Physical access control examples of credentials include fobs and key card entry systems, encrypted badges, mobile credentials, PIN codes and passwords. Personal credentials tell the system who is trying to gain entry.
- https://www.openpath.com/blog-post/physical-access-control
upvoted 2 times

king_oat 8 months, 2 weeks ago
Selected Answer: B
A. Monitors access, does not restrict. (Wrong)
B. You need to physically there at the console port, but last defense is the password. (Correct).
upvoted 2 times

Flips95 9 months, 3 weeks ago
Selected Answer: A
Physical access control systems (PACS) are a type of physical security designed to restrict or allow access to a certain area or building.
answer A does not really restrict access...but serveral websites mention cameras as physical access control tool. At least they help to restrict Access right?
upvoted 3 times

MDK94 11 months, 1 week ago
Lets think about this:

A and B are the only two options that make sense, A is commonly part of a business security program as is B.

The feeling I have with B is that if the password for the console port is needed then the attacker already has "Physical access" to the device, hence why I'm going with A.

I've tried to find information about this to clear up this question, and tbh I cannot get a clear answer, it seems the lines between IP cameras / CCTV and Physical Access Control is very blurred.
upvoted 2 times

IT_MP7 11 months, 2 weeks ago
Usually IP cameras are only a part of a security access control. To enter a data centre (e.g.) you have to pass several blocks, like video CC, guards, gates, biometrics, only then, you can get to a network device.
Answer A is correct
upvoted 1 times

Manu__ 12 months ago
Selected Answer: B
agree with Networknovice
upvoted 1 times

iGlitch 1 year ago
Selected Answer: C
The correct answer is C.

IP cameras are a part of monitoring (It will NOT prevent physical access to the equipment).
Passwords will prevent from gaining access to the CLI (It will NOT prevent physical access to the equipment).
Backing up data to a remote server will prevent physical access because the server is outside the building and maybe in another geographical area.
upvoted 1 times

Networknovice 1 year ago
Selected Answer: B
from NIST,
physical access control system: An electronic system that controls the ability of people or vehicles to enter a protected area by means of authentication and authorization at access control points.
https://csrc.nist.gov/glossary/term/physical_access_control_system

A camera is only a deterrent, kinda like a well-lit parking lot... It does not physically stop someone. A password provides Authentication which challenges the user for a response before allowing the user to access to the network.

upvoted 2 times

Question #662 *Topic 1*

Which field within the access-request packet is encrypted by RADIUS?

A. authorized services

B. password

C. authenticator

D. username

Correct Answer: *B*

Reference:

https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

iGlitch Highly Voted 1 year ago

Selected Answer: B

RADIUS by itself provides no encryption of all traffic. It protects only a small part of the traffic, notably the passwords.

upvoted 5 times

Question #663 *Topic 1*

A Cisco engineer is configuring a factory-default router with these three passwords:

☞ The user EXEC password for console access is p4ssw0rd1.

☞ The user EXEC password for Telnet access is s3cr3t2.

☞ The password for privileged EXEC mode is priv4t3p4ss.

Which command sequence must the engineer configure?

A. enable secret priv4t3p4ss ! line con 0 password p4ssw0rd1 ! line vty 0 15 password s3cr3t2

B. enable secret priv4t3p4ss ! line con 0 password p4ssw0rd1 login ! line vty 0 15 password s3cr3t2 login

C. enable secret priv4t3p4ss ! line con 0 password login p4ssw0rd1 ! line vty 0 15 password login s3cr3t2 login

D. enable secret privilege 15 priv4t3p4ss ! line con 0 password p4ssw0rd1 login ! line vty 0 15 password s3cr3t2 login

Correct Answer: *D*

StingVN 2 weeks, 3 days ago

Selected Answer: B

B. enable secret priv4t3p4ss ! line con 0 password p4ssw0rd1 login ! line vty 0 15 password s3cr3t2 login

Option B is the correct command sequence to configure the passwords for the given scenario. Here's the breakdown:

"enable secret priv4t3p4ss" sets the privileged EXEC mode password.
"line con 0" indicates the console line configuration.
"password p4ssw0rd1" sets the password for console access.
"login" enables login authentication on the console line.
"line vty 0 15" indicates the virtual terminal lines configuration.
"password s3cr3t2" sets the password for Telnet access.
"login" enables login authentication on the virtual terminal lines.
This command sequence correctly sets the specified passwords for console and Telnet access, as well as enables login authentication for both.

upvoted 1 times

Phonon 5 months ago

Selected Answer: B

The correct command sequence is:

enable secret priv4t3p4ss
line con 0 password p4ssw0rd1 login
line vty 0 15 password s3cr3t2 login

This will configure the password for privileged EXEC mode as "priv4t3p4ss", the user EXEC password for console access as "p4ssw0rd1", and the user EXEC password for Telnet access as "s3cr3t2". The "login" keyword is used to enable password authentication for the console and Telnet access.

upvoted 4 times

Anas_Ahmad 5 months, 2 weeks ago

Selected Answer: B

Router(config)#enable secret ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies an ENCRYPTED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
level Set exec level password

upvoted 2 times

michael1001 6 months ago

Selected Answer: B

is B, please update answer

upvoted 3 times

RougePotatoe 7 months, 1 week ago

Selected Answer: A

B,C,D's login command is messed up. The command is login local. Which are incomplete on all the options.

upvoted 2 times

RougePotatoe 7 months, 1 week ago

I see I missed up. login is complete command.

upvoted 1 times

Etidic 7 months, 1 week ago

Selected Answer: B

the answer is B

upvoted 3 times

dick3311 7 months, 2 weeks ago

Selected Answer: D

I go for D
https://study-ccna.com/cisco-privilege-levels/

upvoted 2 times

Garfieldcat 7 months, 4 weeks ago

Isn't exec level of enable sec password 15 by default ?

upvoted 4 times

GigaGremlin 8 months ago

Selected Answer: B

IMHO,...
no extra privilege 15 needed and for Password protection,
you're allready using secret (MD5) instead of Password.
To enter privileged EXEC mode, just enter the "enable" command and Password
Answer D simply set the encrypted Password "privilege 15 priv4t3p4ss"

upvoted 3 times

Murphy2022 8 months ago

Selected Answer: D

D is correct because priv 15 is the priv for exec

upvoted 1 times

Garfieldcat 8 months ago

what's the function of the phase : "privilege 15" in the command ? I go for B too. Indeed, I don't understand ..

upvoted 2 times

Murphy2022 8 months ago

privilege 15 is the exec privilege

upvoted 1 times

creaguy 8 months, 1 week ago

Selected Answer: B

enable secret priv4t3p4ss
!
line con 0
password p4ssword1
login
!
line vty 0 15
password s3cr3t2
login

upvoted 3 times

ShadyAbdekmalek 8 months, 2 weeks ago

Selected Answer: B

D is wrong
I go for B

upvoted 2 times

BieLey 8 months, 1 week ago

Why is it wrong when it asks for privileged?

upvoted 1 times

EliasM 7 months, 2 weeks ago

syntax for enable secret is:

enable secret [level level] { [0] unencrypted-password | encryption-type encrypted-password}

Theres no privilege keyword, only level.

upvoted 9 times

Question #665 *Topic 1*

DRAG DROP -

An engineer is tasked to configure a switch with port security to ensure devices that forward unicasts, multicasts, and broadcasts are unable to flood the port. The port must be configured to permit only two random MAC addresses at a time. Drag and drop the required configuration commands from the left onto the sequence on the right. Not all commands are used.

Select and Place:

Answer Area

switchport mode access	1
switchport port-security	2
switchport port-security mac-address 0060.3EDD.77AB	3
switchport port-security mac-address 00D0.D3ED.622A	4

switchport port-security mac-address sticky

switchport port-security maximum 2

switchport port-security violation shutdown

Correct Answer:

Answer Area

switchport mode access	switchport port-security
switchport port-security	switchport port-security mac-address sticky
switchport port-security mac-address 0060.3EDD.77AB	switchport port-security maximum 2
switchport port-security mac-address 00D0.D3ED.622A	switchport port-security violation shutdown

switchport port-security mac-address sticky

switchport port-security maximum 2

switchport port-security violation shutdown

THEKYPTONIAN Highly Voted 10 months, 1 week ago

1.#switchport mode access
2.#switchport port-security
3.#switchport port-security maximum 2
4.#switch port-security sticky

upvoted 33 times

fransCISCO 4 months ago

so this is the correct answer and sequence?? pls answer guys

upvoted 2 times

HeinyHo Highly Voted 8 months, 2 weeks ago

It says: only two random MAC addresses at a time, not the first two macs. So the sticky command is incorrect, as are the static MACs, leaving only 4 options

upvoted 11 times

dropspablo Most Recent 2 days ago

1.switchport mode access
2.switchport port-security
3.switchport port-security maximum 2
4.switchport port-security violation shutdown

"Dynamic secure MAC addresses" are typically used when the host(s) connecting to a specific switchport is constantly changing, and the intention is to limit the port to only be used by a specific number of hosts at once. https://www.ciscopress.com/articles/article.asp?p=1722561
Adding: By default, Cisco IOS sets the aging time (aging time) of port security table entry to 0 (zero), which means that the entry will be removed immediately when a device disconnects. Therefore, by disconnecting the MAC device currently connected to the port, you can immediately connect another device without causing a violation.

upvoted 1 times

krzysiew 2 months, 1 week ago

I checked packet tracert
1.#switchport mode access
2.#switchport port-security
3.#switch port-security sticky
4.#switchport port-security maximum 2

upvoted 3 times

gc999 2 months, 2 weeks ago

I think "shutdown" is incorrect as it will cause the first two devices cannot use as well. It said we should "permit" them to use.

upvoted 1 times

SVN05 3 months, 3 weeks ago

Agreed with Peter_panda & HeinyHo. I've seen a few places mentioning that port security was usually configured on access ports(including pkt labs and other sites that explain how to implement port security concept for ccna) so my answer as follows.

1.switchport mode access
2.switchport port-security
3.switchport port-security maximum 2
4.switchport port-security violation shutdown

Based on my experience with going over alot of questions here, Cisco takes everything literally so if the question says permit only two random MAC addresses at a time indicates it can be always changed to something else. Sticky will be a permanent mark on the MAC table thus not allowing any other device to associate with it.

upvoted 3 times

ike110 3 months, 3 weeks ago

"violation shutdown". is the default mode, so not needed unless another mode was set earlier

upvoted 2 times

Dutch012 2 months, 4 weeks ago

right, it is not needed but it completes what the question is asking for

upvoted 1 times

kalidergr 5 months, 1 week ago

Port security will only work on access ports. Therefore, in order to enable port security, the user must first make the port an access port.
Source: https://cowbell.insure/blog/port-security-2/

upvoted 1 times

clivebarker86 7 months, 3 weeks ago

don t understand, why shutdown..?

upvoted 1 times

clivebarker86 7 months, 3 weeks ago

don t understand, why shutdown..?

upvoted 1 times

splashy 8 months, 1 week ago

switchport mode access command is essential

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int f0/1
Switch(config-if)#switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.

Shutdown is default setting so no need to specify

upvoted 6 times

GohanF2 10 months, 1 week ago

The answers are correct. sticky is not an option . Due that it will saved the first 2 MAC addresses to the running configuration. IF any other device " randomly" connects to the same port then the connection will be refused till we cleared the sticky mac addresses

upvoted 4 times

WINDSON 11 months, 2 weeks ago

answer is wrong , no need "shutdown". it is default state. instead you need to add sticky to learn random mac address

upvoted 2 times

Nickname53796 1 year ago

I will say that the default behavior of port security is to shutdown the port for violations. So why would we need to type that command?

But it makes more sense in this context than sticky.

upvoted 3 times

MikeNY85 1 year ago

SORRY ANSWER IS CORRECT. STICKY WILL MAKE THE PORT STICK TO ONLY TWO MAC ADDS "PERMANENTLY" SO ANSWER IS CORRECT!

upvoted 2 times

RexChen 10 months, 3 weeks ago

to permantently add the mac , need to save the configuration, otherwise reload will restore the configuration with no sticky mac

upvoted 3 times

MikeNY85 1 year ago

IT SAID TWO "RANDOM" MAC ADDS.....WHICH MEANS "STICKY"

upvoted 2 times

NORLI 1 year, 1 month ago

SO WHAT IS THE DIFFERENCE BETWEEN SWITCHPORT SECURITY AND SWITHPORT SECURITY SHUTDOWN? PLUS THE QUESTION SAYS RANDOM ISN'T THAT THE FUNCTION OF MAC ADDRESS STICKY SO THE THE PORT WILL DYNAMICALLY LEARN THE MAC ADDRESS

upvoted 3 times

MikeNY85 1 year ago

I think since it's dynamically, it should be "switchport port-security mac-address sticky"

upvoted 1 times

DARKK 1 year ago

Nothing explicitly says it is dynamically.

upvoted 2 times

melmiosis 6 months, 4 weeks ago

when we say RANDOM, it means DEFINETLY NOT STATIC...
What about STATIC is so "random"???

upvoted 3 times

purenuker 4 months, 3 weeks ago

Yeah , this is the most dumbest question of all times which Cisco asks ... I dont understand ..

upvoted 2 times

Peter_panda 4 months ago

It says “to permit only two random MAC addresses at a time”. So, if one MAC address expires, the switch can learn another MAC address. If sticky is used, only the first 2 macs are learned and are switch does not forget them until the next reboot. So, sticky is not a good answer here.

upvoted 5 times

Dutch012 3 months, 1 week ago

totally agree

upvoted 1 times

Question #666 *Topic 1*

What is a function of Opportunistic Wireless Encryption in an environment?

A. provide authentication

B. protect traffic on open networks

C. offer compression

D. increase security by using a WEP connection

Correct Answer: *B*
Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/16-12/config-guide/b_wl_16_12_cg/wpa3.html

StingVN 2 weeks, 3 days ago

Selected Answer: B

B. Protect traffic on open networks.

The function of Opportunistic Wireless Encryption (OWE) in an environment is to protect traffic on open networks. Open networks, such as public Wi-Fi hotspots, do not typically have encryption enabled by default, making them vulnerable to eavesdropping and data interception. OWE provides a mechanism to encrypt wireless communication on these open networks, adding a layer of security to protect the transmitted data. It helps ensure the confidentiality and integrity of the network traffic, even in the absence of a pre-shared key or a separate authentication mechanism.

upvoted 1 times

MikeNY85 1 year ago

The use of OWE enhances wireless network security for deployments where Open or shared PSK based networks are deployed.
Answer is correct.

upvoted 4 times

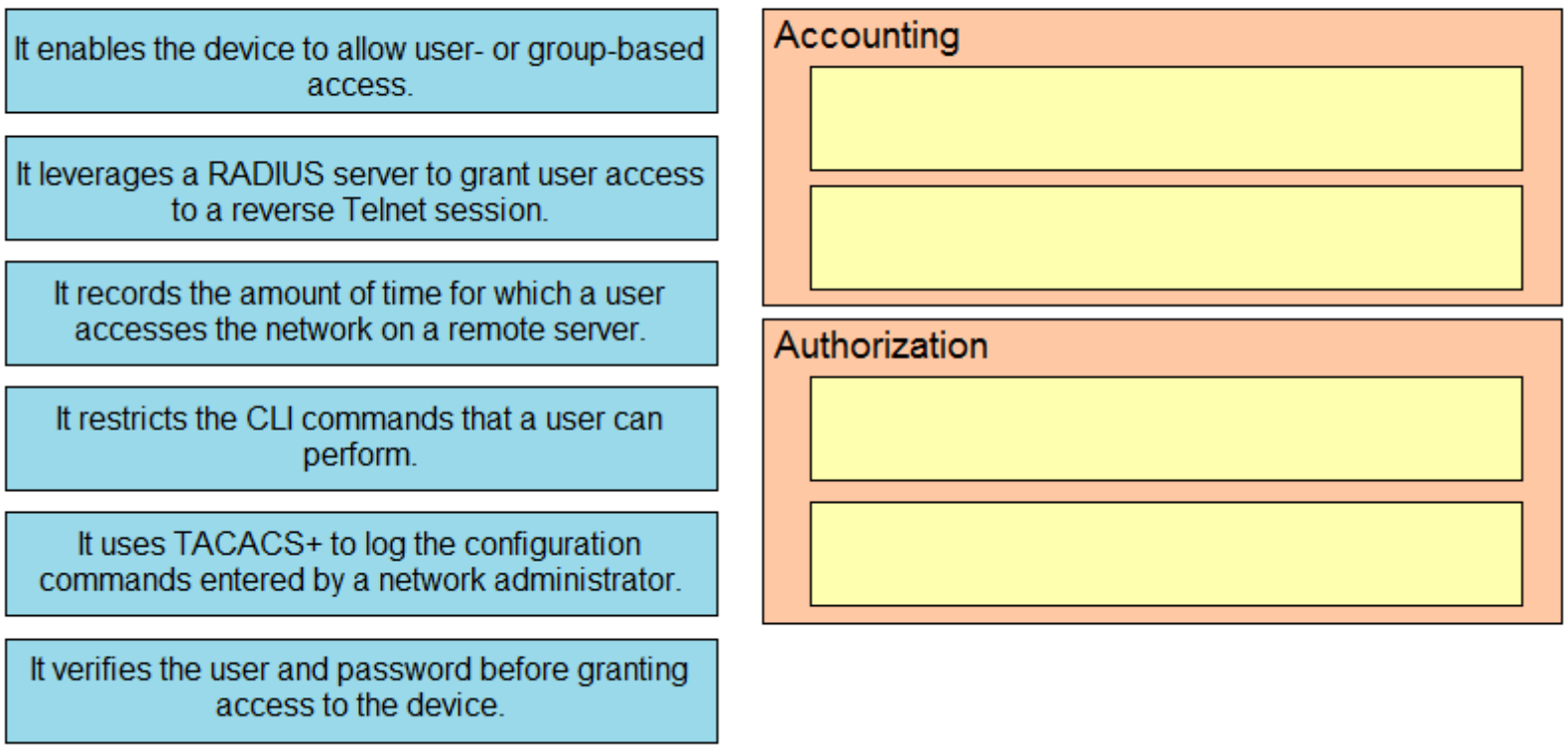
Question #667 *Topic 1*

DRAG DROP -

Drag and drop the AAA features from the left onto the corresponding AAA security services on the right. Not all options are used.

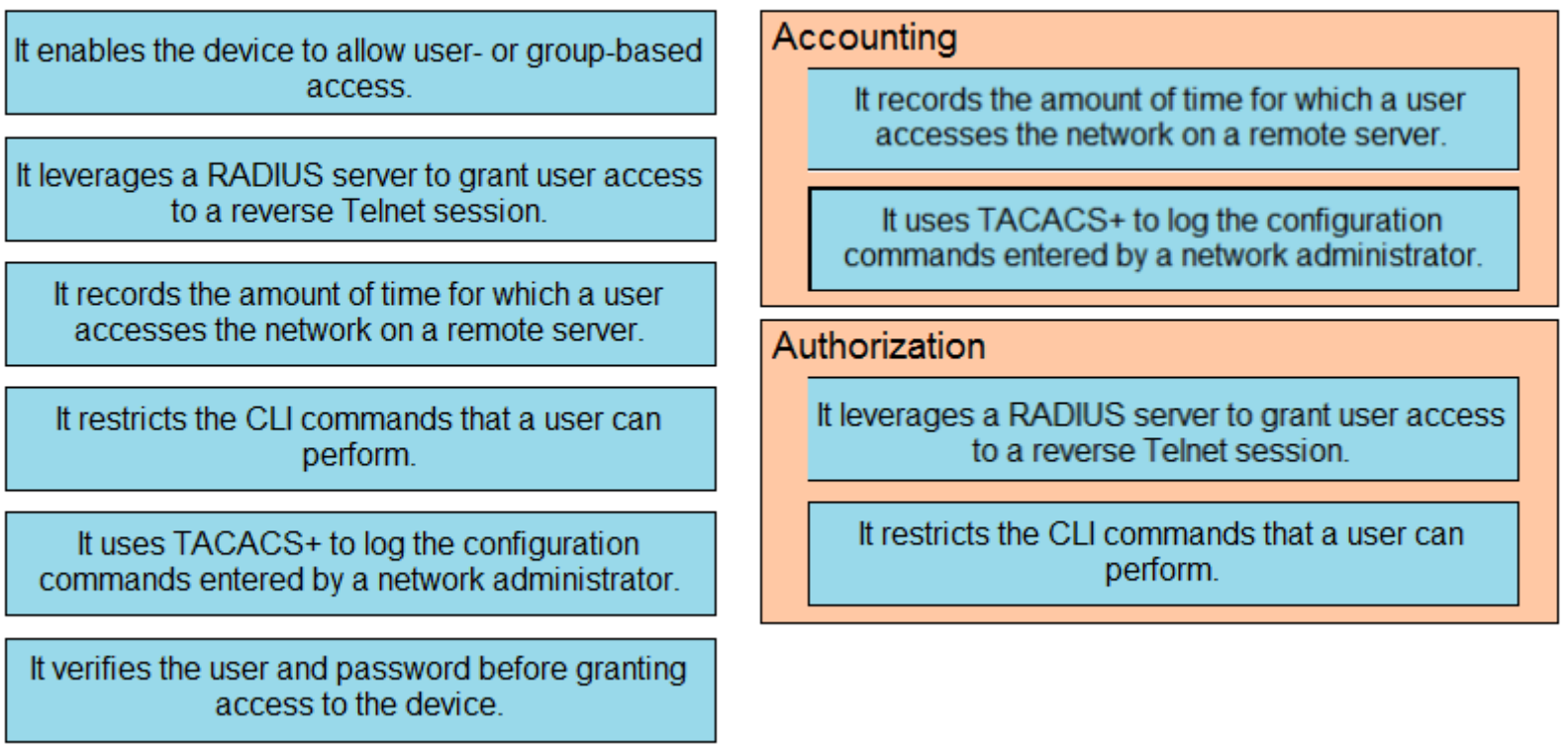
Select and Place:

Answer Area



Correct Answer:

Answer Area



EliasM Highly Voted 8 months ago

I think the RADIUS options refers more to Authentication. Please correct me if im wrong, but i think that in Authorization the RADIUS option is incorrect, and instead it should be "Enables the device for user or group based access".

upvoted 11 times

RougePotatoe 7 months, 1 week ago

Authorization controls access to resources
authentication controls identity verification
accounting records

Reverse telnet allows you to telnet to a device then from that device connect to the console of another device. Below is a quick snippet highlighting most of what you'll need to know about it.
https://community.cisco.com/t5/switching/reverse-telnet/td-p/2159217

Based on what reserve telnet is I would have to say the listed answer is correct.

upvoted 3 times

jonathan126 1 month, 2 weeks ago

Based on your information, reverse telnet is a method to access a device, another method could be to access a device via console cable, which does not seem to be authorization control.

Authorization controls limit the access of a user. A user group can be granted to multiple users and these users will be limited to the access granted to the group. This is more related to authorization.
The answer should be user/group based access and restrict CLI command for authorization

upvoted 3 times

studying_1 1 month ago

I agree

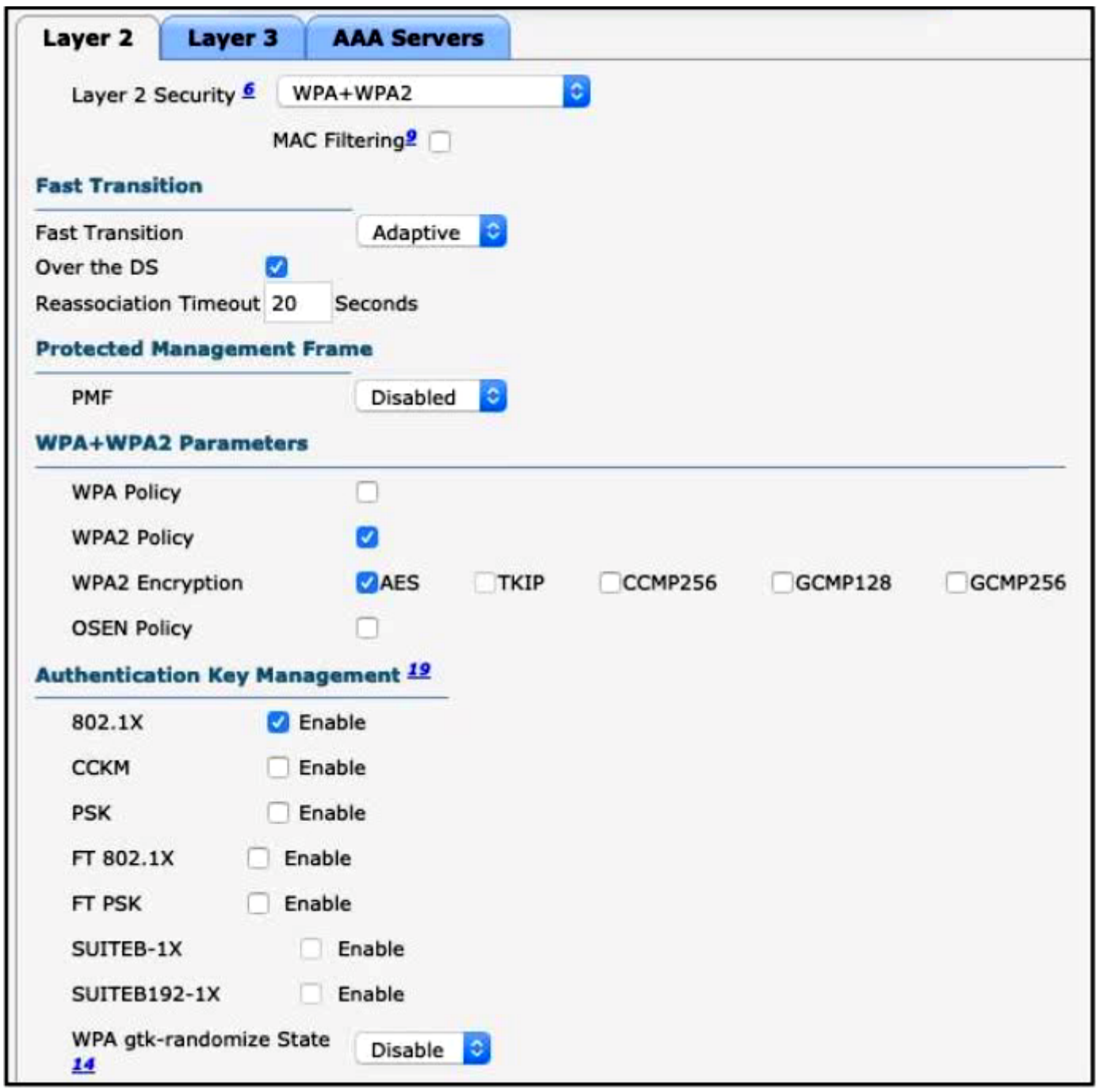
upvoted 1 times

enzo86 Highly Voted 2 months ago

It is incorrect in authorization, it should be:
it enables the device to allow user or group based access
it restricts the cli commands that a user can perform

upvoted 5 times

Question #668 *Topic 1*



Refer to the exhibit. Clients on the WLAN are required to use 802.11r. What action must be taken to meet the requirement?

A. Under Protected Management Frames, set the PMF option to Required.

B. Enable CCKM under Authentication Key Management.

C. Set the Fast Transition option and the WPA gtk-randomize State to disable.

D. Set the Fast Transition option to Enable and enable FT 802.1X under Authentication Key Management.

Correct Answer: *D*

liviuml 1 month, 3 weeks ago

Selected Answer: D

D is correct.
Search for "Configuring 802.11r Fast Transition (GUI)" in following page:
https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/80211r-ft/b-80211r-dg.html#task_2C619E3A576D474F80D6CB4BA8B4DBA6
Regards,

upvoted 1 times

clivebarker86 7 months, 3 weeks ago

c'era una domanda simile che parlava dello stesso protocollo, ma tra le 2 risposte psk o 802.1x veniva scelta PSK

upvoted 1 times

Garfieldcat 7 months, 4 weeks ago

Does it imply that fast transition is usually applied in Enterprise mode if activation of 802.1x is required?

upvoted 1 times

iGlitch 1 year ago

Selected Answer: D

IEEE 802.11r-2008 or fast BSS transition
And this may explain why D is correct:
https://blogs.cisco.com/networking/what-is-802-11r-why-is-this-important

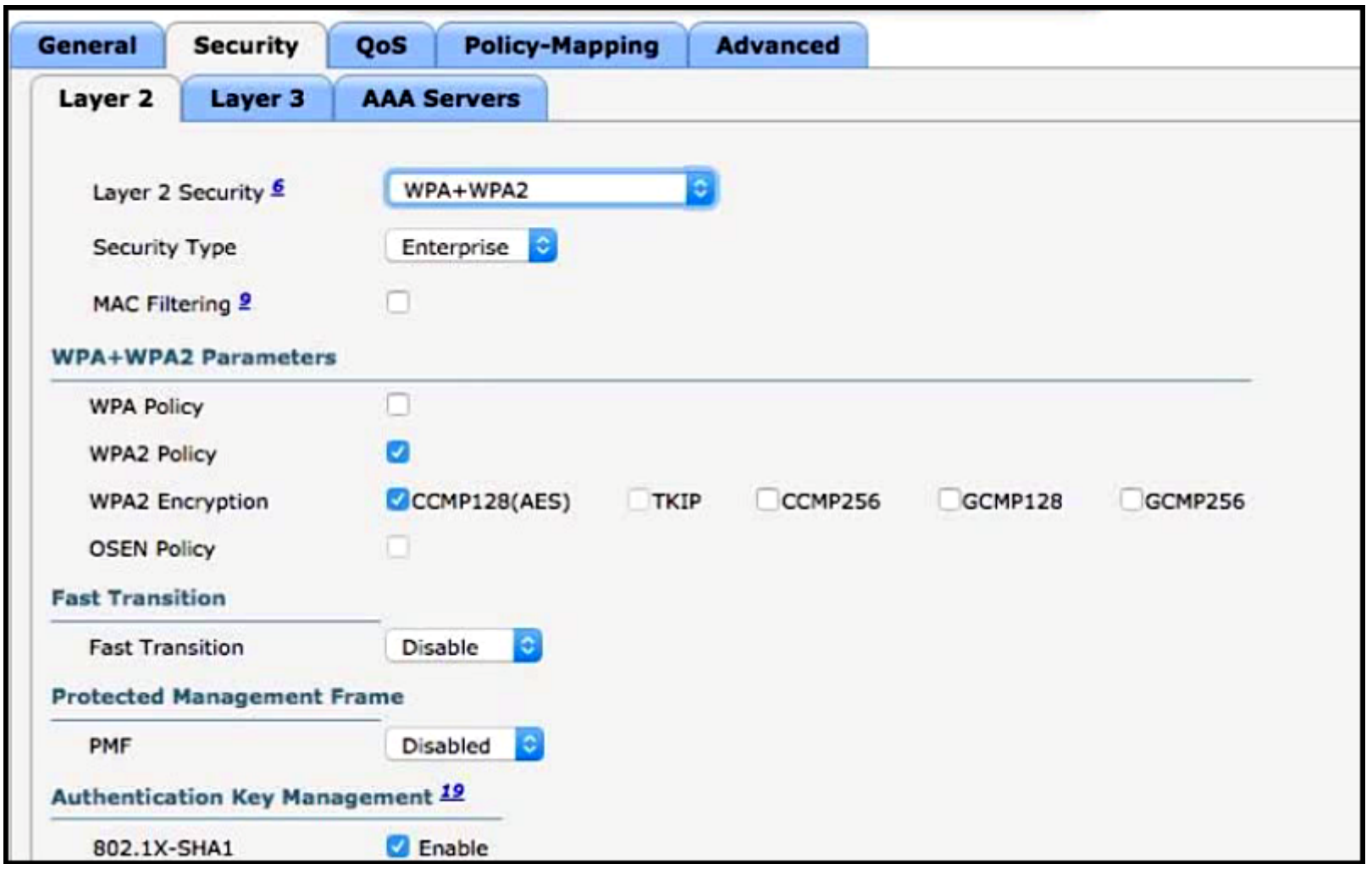
upvoted 3 times

iGlitch 1 year ago

This feature was NOT mentioned in the OCG 😉, but by now you should know how cisco exams work.

upvoted 5 times

Question #669 *Topic 1*



Refer to the exhibit. What must be configured to enable 802.11w on the WLAN?

A. Set Fast Transition to Enabled.

B. Enable WPA Policy.

C. Set PMF to Required.

D. Enable MAC Filtering.

Correct Answer: *B*
Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/5700/software/release/3se/wlan/configuration_guide/b_wlan_3se_5700_cg/b_wlan_3se_5700_cg_chapter_01000.pdf

BraveBadger Highly Voted 1 year, 1 month ago

Selected Answer: C

IEEE 802.11w is the Protected Management Frames standard. I think the correct answer is C.

upvoted 6 times

StingVN Most Recent 2 weeks, 3 days ago

Selected Answer: C

C. Set PMF to Required.

To enable 802.11w (also known as Protected Management Frames or PMF) on the WLAN, the action that must be taken is to set PMF to Required.

PMF is a security feature in Wi-Fi networks that provides protection for management frames, such as association and disassociation frames, against various attacks. By setting PMF to Required, all clients connecting to the WLAN will be required to support and use PMF for enhanced security. This ensures that management frames exchanged between the access point and clients are protected from potential tampering or exploitation.

Options A, B, and D do not specifically relate to enabling 802.11w (PMF) on the WLAN.

upvoted 1 times

Phonon 5 months ago

Selected Answer: C

IEEE 802.11w is an amendment to the IEEE 802.11 standard that defines enhancements to the security of wireless local area networks (WLANs). It specifies the use of Protected Management Frames (PMFs), which provide an additional layer of security for management frames that are used to control the operation of a WLAN. This includes management frames such as Beacon frames, which are used to advertise the presence of a WLAN, and Association Request frames, which are used to initiate the connection process between a client device and an access point. 802.11w aims to prevent certain types of attacks, such as man-in-the-middle attacks, which can be used to intercept and modify management frames in order to disrupt the operation of a WLAN.

upvoted 3 times

Etidic 7 months, 2 weeks ago

Selected Answer: C

The answer is C

upvoted 2 times

Etidic 7 months, 2 weeks ago

The answer is C

upvoted 2 times

creaguy 8 months, 1 week ago

Selected Answer: C

https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/17-1/config-guide/ewc_cg_17_11/802_11w.html#:~:text=Step%C2%A04,the%20following%20fields%3A

upvoted 3 times

Murphy2022 8 months, 1 week ago

WPA and AKM must be configured, while PKM is optional. 802.11r still works with PKM being disabled.

upvoted 1 times

Murphy2022 8 months ago

i was tired read W as R

upvoted 2 times

JUveNTino 10 months, 2 weeks ago

Selected Answer: C

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212576-configure-802-11w-management-frame-prote.html

upvoted 4 times

dulceordog 10 months, 3 weeks ago

'B' is correct
to configure802.11w feature for optional and mandatory, you must have WPA and AKM configured.The RNS (RobustSecureNetwork)IE must be enabledwith an AES Cipher.
To configure802.11w as mandatory, you must enable PMF AKM in additionto WPA AKM

upvoted 1 times

iGlitch 1 year ago

Selected Answer: C

Wiki:
"IEEE 802.11w-2009 is an approved amendment to the IEEE 802.11 standard to increase the security of its management frames".

C is the correct answer.

upvoted 2 times

chalaka 1 year, 1 month ago

Selected Answer: B

B is correct, before set PMP to required, WPA and AKM must be configured.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/5700/software/release/3se/wlan/configuration_guide/b_wlan_3se_5700_cg/b_wlan_3se_5700_cg_chapter_01000.pdf
(Page 3, Before You Begin,
WPA and AKM must be configured.)

upvoted 1 times

Etidic 7 months, 2 weeks ago

Restrictions for 802.11w • 802.11w cannot be applied on an open WLAN, WEP-encrypted WLAN, or a TKIP-encrypted WLAN. • The WLANonwhich 802.11w is configured must have either WPA2-PSK or WPA2-802.1x security configured.

Since WPA2 is enabled in the GUI then WPA may or may not be selected.
The answer is C

upvoted 1 times

ctoklu 11 months, 2 weeks ago

correct
and to me, follow up text saying "To configure 802.11w as mandatory, you must enable PMF AKM in addition to WPA AKM" covers also Optional selection for PMF

upvoted 1 times

ctoklu 11 months, 2 weeks ago

"Required" is not an obligation here...

upvoted 1 times

Netox7 1 year, 1 month ago

Selected Answer: C

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212576-configure-802-11w-management-frame-prote.html

upvoted 4 times

Question #670 *Topic 1*

Which encryption method is used by WPA3?

A. TKIP

B. AES

C. SAE

D. PSK

Correct Answer: *C*

Garfieldcat Highly Voted 7 months, 4 weeks ago

SAE is refer to authentication. encryption method should be B -AES

upvoted 11 times

EliasM 7 months, 3 weeks ago

Garfield is right. Check page 662 of OCG.

upvoted 3 times

StingVN Most Recent 2 weeks, 3 days ago

Selected Answer: B

B. AES

WPA3 (Wi-Fi Protected Access 3) primarily uses the Advanced Encryption Standard (AES) encryption method. AES is a strong and widely adopted encryption algorithm that provides secure and robust encryption for wireless communication. WPA3 improves the security of Wi-Fi networks by incorporating stronger encryption protocols, and AES is the recommended encryption algorithm for ensuring data confidentiality in WPA3.

TKIP (Temporal Key Integrity Protocol) was used in the earlier WPA and WPA2 security standards but is not used in WPA3 due to its known security vulnerabilities.

SAE (Simultaneous Authentication of Equals) is the authentication method used in WPA3-Personal (WPA3-PKS) mode, but it is not the encryption method.

PSK (Pre-Shared Key) refers to a method of authentication rather than encryption and is commonly used in WPA2-Personal mode.

upvoted 1 times

krzysiew 2 months, 1 week ago

i think
WPA3 - SAE
WPA3 Enterprise AES (WPA3 Enterprise, by default, uses a 128-bit AES-CCMP)

upvoted 1 times

krzysiew 2 months, 1 week ago

WPA3-Personal SAE authentication metod
WPA3 Enterprise AES (by default, uses a 128-bit AES-CCMP) cryptographic metod

upvoted 1 times

Zortex 2 months, 3 weeks ago

WPA3 (Wi-Fi Protected Access 3) uses the Simultaneous Authentication of Equals (SAE) algorithm, also known as Dragonfly, as its encryption method. SAE is a secure key exchange protocol that is resistant to offline dictionary attacks and protects against attacks on weaker passwords. This algorithm provides better security and protection against various types of attacks, such as brute-force and dictionary attacks, compared to the previous WPA2 standard which used the Pre-Shared Key (PSK) method.

upvoted 1 times

Phonon 5 months ago

Selected Answer: B

WPA3 uses SAE (Simultaneous Authentication of Equals), which is a secure key exchange protocol that provides forward secrecy. It is also known as Dragonfly Key Exchange or Opportunistic Wireless Encryption (OWE). WPA3 also uses AES (Advanced Encryption Standard) for encryption of data.

B is the encryption type, that's the question. NOT authentication type.

upvoted 4 times

Etidic 7 months, 2 weeks ago

Selected Answer: B

The answer is B

upvoted 4 times

sjorwen 7 months, 2 weeks ago

When using WPA3 only, the access point will transmit in the beacon the capability to only accept STA using WPA3 SAE. When using transition mode, the access point will broadcast in the beacon capabilities to accept STA using both WPA2 and WPA3. In this configuration, STA that do not support WPA3 can still connect to the SSID.

So SAE is correct!

upvoted 1 times

Question #671 *Topic 1*

Which type of traffic is sent with pure IPsec?

A. multicast traffic from a server at one site to hosts at another location

B. broadcast packets from a switch that is attempting to locate a MAC address at one of several remote sites

C. unicast messages from a host at a remote site to a server at headquarters

D. spanning-tree updates between switches that are at two different sites

Correct Answer: *C*

StingVN 2 weeks, 3 days ago

Selected Answer: C

C. Unicast messages from a host at a remote site to a server at headquarters.

Pure IPsec is typically used to secure unicast traffic between two endpoints. Unicast traffic refers to one-to-one communication between a specific sender and receiver. In this case, it would involve unicast messages from a host at a remote site to a server at headquarters.

IPsec is a protocol suite used to provide secure communication over IP networks. It can be used to encrypt and authenticate IP packets, ensuring the confidentiality, integrity, and authenticity of the transmitted data. While IPsec can also support multicast and broadcast traffic, the term "pure IPsec" generally refers to the use of IPsec in a point-to-point unicast communication scenario.

upvoted 1 times

SVN05 3 months, 3 weeks ago

Selected Answer: C

Just my input here. Multicast traffic is not related with IPsec at all. It is associated with GRE thus option A is out. Furthermore, IPSec is only passes unicast traffic. Not multicast and broadcast thus option B is out which leaves us with either C or D. I'll go with C as it stated the word unicast. Good enough for me.

upvoted 1 times

Question #672 *Topic 1*

How does authentication differ from authorization?

A. Authentication is used to record what resource a user accesses, and authorization is used to determine what resources a user can access.

B. Authentication verifies the identity of a person accessing a network, and authorization determines what resource a user can access.

C. Authentication is used to determine what resources a user is allowed to access, and authorization is used to track what equipment is allowed access to the network.

D. Authentication is used to verify a person's identity, and authorization is used to create syslog messages for logins.

Correct Answer: *B*

studying_1 6 days, 14 hours ago

Selected Answer: B

Answer is correct

upvoted 1 times

Question #673 *Topic 1*

An engineer has configured the domain name, user name, and password on the local router. What is the next step to complete the configuration for a Secure Shell access RSA key?

A. crypto key import rsa pem

B. crypto key generate rsa

C. crypto key zeroize rsa

D. crypto key pubkey-chain rsa

Correct Answer: *B*

4aynick 1 week, 5 days ago

where is the hostname?

upvoted 1 times

StingVN 2 weeks, 3 days ago

Selected Answer: B

B. crypto key generate rsa

The next step to complete the configuration for a Secure Shell (SSH) access RSA key on the local router is to use the "crypto key generate rsa" command. This command generates an RSA key pair that will be used for SSH encryption and authentication purposes.

After running this command, the router will prompt for the key modulus size (usually 1024 or 2048 bits) and will generate the RSA key pair. The generated RSA public key will be used for SSH server authentication, and the private key will be stored on the router for secure SSH communication.

Options A, C, and D are not the correct commands for generating an RSA key pair for SSH access on a router.

upvoted 1 times

Question #674 *Topic 1*

Which type if network attack overwhelms the target server by sending multiple packets to a port until the half-open TCP resources of the target are exhausted?

A. SYN flood

B. reflection

C. teardrop

D. amplification

Correct Answer: *A*

Eminn 4 months, 1 week ago

Selected Answer: A

https://www.netscout.com/what-is-ddos/syn-flood-attacks#:~:text=A%20TCP%20SYN%20flood%20DDoS,into%20a%20half%2Dopen%20state.

upvoted 1 times

Question #675 *Topic 1*

Which two components comprise part of a PKI? (Choose two.)

A. preshared key that authenticates connections

B. one or more CRLs

C. RSA token

D. CA that grants certificates

E. clear-text password that authenticates connections

Correct Answer: *CD*

Stichy007 3 months ago

Selected Answer: CD

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-16/sec-pki-xe-16-book/sec-deploy-rsa-pki.html

upvoted 1 times

Phonon 5 months ago

Selected Answer: BD

B) CRL (Certificate Revocation List) is a list of digital certificates that have been revoked by the issuing CA before their expiration date.

D) CA (Certificate Authority) is a trusted entity that grants digital certificates to organizations or individuals, which can be used to establish secure connections and exchange data securely

Both are the integral parts of Public Key Infrastructure (PKI)

upvoted 4 times

Request7108 5 months, 1 week ago

Selected Answer: BD

A) A PSK has nothing to do with PKIs
B) A CRL informs devices when a certificate is revoked/withdrawn
C) RSA token has nothing to do with PKIs
D) A certificate authority is center of the flow of trust
E) I have no idea what they're meaning here but maybe this is just another PSK reference

B and D are clear answers. More reading here:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-3s/sec-pki-xe-3s-book/sec-cfg-auth-rev-cert.html

upvoted 4 times

michael1001 6 months ago

Selected Answer: BD

Should be B and D

upvoted 3 times

battlefate 5 months, 3 weeks ago

agreed.

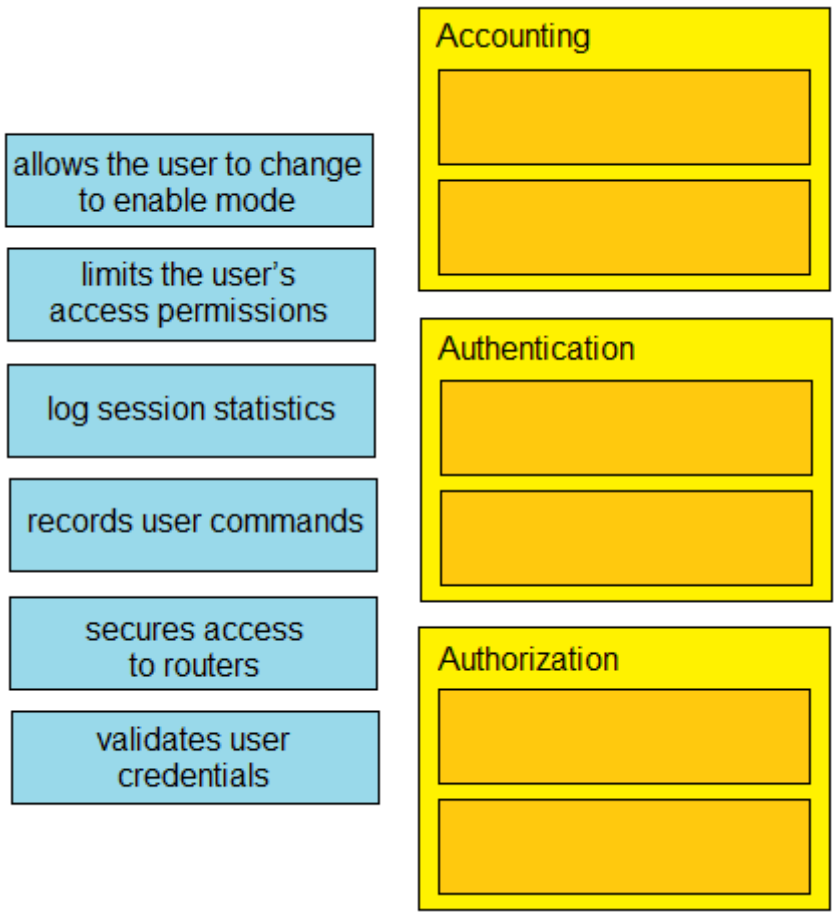
upvoted 1 times

Question #676 *Topic 1*

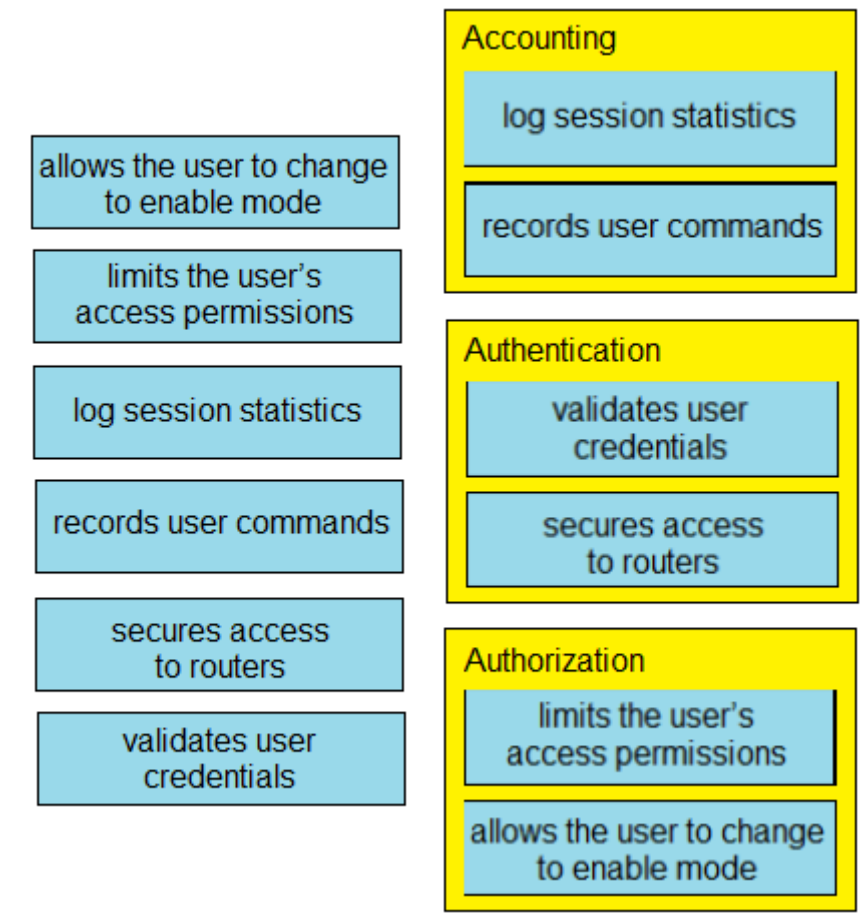
DRAG DROP -

Drag and drop the descriptions of AAA services from the left onto the corresponding services on the right.

Select and Place:



Correct Answer:



LeonardoMeCabrio 11 hours, 46 minutes ago

Given answers are correct.

upvoted 1 times

Question #677 *Topic 1*

After a recent security breach and a RADIUS failure, an engineer must secure the console port of each enterprise router with a local username and password.
Which configuration must the engineer apply to accomplish this task?

A. aaa new-model line con 0 password plaintextpassword privilege level 15

B. aaa new-model aaa authorization exec default local aaa authentication login default radius username localuser privilege 15 secret plaintextpassword

C. username localuser secret plaintextpassword line con 0 no login local privilege level 15

D. username localuser secret plaintextpassword line con 0 login authentication default privilege level 15

Correct Answer: *A*

splashy Highly Voted 8 months, 1 week ago

Selected Answer: D

I could be wrong but...

A.Only password no local username

B."aaa auth login default radius" doesn't work in Packet Tracer, "aaa auth login default group radius" works.

C."no login local" is the opposite of what we want.

D.The only downside i see with this is that i think you need to implement on each device separately,
but since there was a security breach and a Radius failure, i think we are stuck with this option anyway?

So D?

upvoted 10 times

highfivejohn Highly Voted 7 months, 2 weeks ago

Selected Answer: D

Why would I need to run "aaa new-model" if the scenario indicated RADIUS was already present? D

upvoted 5 times

krzysiew Most Recent 2 months, 1 week ago

Selected Answer: A

aaa new-model line con 0 password plaintextpassword privilege level 15

upvoted 1 times

oatmealturkey 3 months, 3 weeks ago

Selected Answer: B

A is incorrect because it does not specify a username which is required by the question. C is obviously incorrect too.

D is actually incorrect as well, because "login authentication default" only works when AAA has been enabled ("aaa new-model"). I tried configuring D in PT and was not able to Telnet.

Although in B, "aaa auth login default radius" is not a valid command, when I configured B in PT I was still able to Telnet, so it only needs the other commands in the sequence to be valid in order to work. B is the answer.

upvoted 3 times

usamahrakib001 4 months, 1 week ago

Login local command would be used only if aaa new model is disabled, but when aaa new model is enabled you should use "login authentication default" which is enabled by default when aaa new model is enabled.

upvoted 3 times

SemStrond 7 months ago

Selected Answer: D

D is the correct answer

upvoted 4 times

Question #678 *Topic 1*

Which wireless security protocol relies on Perfect Forward Secrecy?

A. WEP

B. WPA2

C. WPA

D. WPA3

Correct Answer: *A*

Etidic Highly Voted 7 months, 2 weeks ago

Selected Answer: D

The answer is D

upvoted 5 times

studying_1 Most Recent 1 month ago

Selected Answer: D

The answer is D

upvoted 1 times

RAJ_1920 1 month, 3 weeks ago

@examtopics please fix

upvoted 1 times

krzysiew 2 months, 1 week ago

Selected Answer: D

WPA3 networks include perfect forward secrecy.

upvoted 1 times

michael1001 6 months ago

Selected Answer: D

D - please fix

upvoted 3 times

clivebarker86 7 months, 3 weeks ago

PFS its a WPA3 feature

upvoted 1 times

GigaGremlin 7 months, 4 weeks ago

Selected Answer: D

If you're still using WEP for your Wifi, you definitive have to have a Perfect Secrecy and not just for forward...

upvoted 2 times

king_oat 8 months, 2 weeks ago

Selected Answer: D

WPA3 networks include PFS

upvoted 1 times

ShadyAbdekmalek 8 months, 2 weeks ago

Selected Answer: D

WPA3 (Wi-Fi Protected Access 3) is the newest wireless security protocol designed to encrypt data using a frequent and automatic encryption type called Perfect Forward Secrecy.

upvoted 1 times

ShadyAbdekmalek 8 months, 2 weeks ago

Selected Answer: C

WPA3 (Wi-Fi Protected Access 3) is the newest wireless security protocol designed to encrypt data using a frequent and automatic encryption type called Perfect Forward Secrecy.

upvoted 1 times

nicombe 8 months, 2 weeks ago

PFS is used in WPA3

upvoted 1 times

splashy 8 months, 2 weeks ago

Selected Answer: D

https://blog.compass-security.com/2019/07/from-open-wi-fi-to-wpa3/

upvoted 1 times

Question #679 *Topic 1*

What is a zero-day exploit?

A. It is when the network is saturated with malicious traffic that overloads resources and bandwidth.

B. It is when an attacker inserts malicious code into a SQL server.

C. It is when a new network vulnerability is discovered before a fix is available.

D. It is when the perpetrator inserts itself in a conversation between two parties and captures or alters data.

Correct Answer: *C*

ac89l 3 weeks, 3 days ago

Selected Answer: C

Agree, answer is C

upvoted 2 times

Question #680 *Topic 1*

A network engineer is replacing the switches that belong to a managed-services client with new Cisco Catalyst switches. The new switches will be configured for updated security standards including replacing.
Telnet services with encrypted connections and doubling the modulus size from 1024. Which two commands must the engineer configure on the new switches?
(Choose two.)

A. transport input ssh

B. transport input all

C. crypto key generate rsa modulus 2048

D. crypto key generate rsa general-keys modulus 1024

E. crypto key generate rsa usage-keys

Correct Answer: *AC*

Goh0503 Highly Voted 7 months, 4 weeks ago

Answer A and C

Question requirement
A Telnet services with encrypted connections === >A transport input ssh
C doubling the modulus size from 1024. ===> C. crypto key generate rsa modulus 2048

upvoted 7 times

battlefate Most Recent 5 months, 3 weeks ago

Bad question, playing with english....
"doubling the modulus size from 1024"... why not just say "change the modulus size to 2048"...

upvoted 3 times

Question #681 *Topic 1*

What are two examples of multifactor authentication? (Choose two.)

A. single sign-on

B. soft tokens

C. passwords that expire

D. shared password repository

E. unique user knowledge

Correct Answer: *BC*

RougePotatoe Highly Voted 7 months, 1 week ago

my distain for cisco grows

upvoted 15 times

splashy Highly Voted 8 months, 1 week ago

Selected Answer: BC

Single sign-on allows users to access multiple applications, websites, resources with one set of login credentials.
It is not a part of a MFA, it actually needs MFA to be secured.

A soft (or hard) token can be a part of a MFA
A password that expires can be a part of a MFA

upvoted 8 times

Friday_Night Most Recent 2 weeks ago

ccna 200-301 is just the beginning of this network industry. why do they do this? the question is ok but the choices..... :((

upvoted 1 times

Sleezyglizzy 1 month, 3 weeks ago

From someone who's taken and passed the Sec+ exam, its def BE.

upvoted 3 times

Ciscoman021 1 month, 4 weeks ago

Selected Answer: BE

Soft tokens: Soft tokens are software applications that generate one-time passwords (OTP) that are used as a second factor of authentication. Users typically install the soft token application on their smartphone or other mobile device, and use it in conjunction with a username and password to access a system or application.
Unique user knowledge: Unique user knowledge refers to information that only the user knows, such as the answer to a security question or a personal identification number (PIN). This is an example of a second factor of authentication that is used in conjunction with a username and password to verify the user's identity.

upvoted 2 times

Zortex 2 months, 2 weeks ago

Selected Answer: BE

B. Soft tokens: A soft token is a type of authentication method that generates a one-time password (OTP) that can be used for a single login session. Soft tokens are typically generated using a mobile app or software on a computer, and require something the user has (their device) and something they know (their password) to authenticate.

E. Unique user knowledge: Unique user knowledge is a form of authentication that requires the user to answer questions or provide information that only they should know. For example, a security question that only the user would know the answer to, such as "What is your mother's maiden name?" or "What was the name of your first pet?".

Single sign-on (A), passwords that expire (C), and shared password repositories (D) are not examples of multifactor authentication, as they only rely on one factor (something the user knows, such as a password) for authentication.

upvoted 1 times

JJY888 3 months, 1 week ago

Selected Answer: BC

B is something you have. C is an example of something that you know. E is just a definition and not an example. BC. Cisco is not being fair with this question.

upvoted 2 times

Sdiego 4 months, 2 weeks ago

Selected Answer: BE

E refers to: Your favourite team or something like that something you know- that is the second factor

upvoted 4 times

battlefate 5 months, 3 weeks ago

Selected Answer: BC

Agreed with @splashy that BC is correct answer.
B. A soft (or hard) token can be a part of a MFA
C. A password that expires (OTP) can be a part of a MFA

upvoted 2 times

RougePotatoe 7 months, 1 week ago

Selected Answer: BE

For something to be considered multifactor authentication you have to have more than 1 factor. Typically a factor falls into one of 3 categories something you know, something you have, and something you are (biometric). Technically non of the answers here are considered MFA as they only list 1 step for each answer. If you have to pick two to make a MFA the most common is password and token thing google authenticator. Thus the answer should be B (randomized pin) and E (password).

upvoted 6 times

DoBronx 7 months, 1 week ago

why not E

upvoted 2 times

mrgreat 8 months, 3 weeks ago

Selected Answer: AB

C is incorrect, A and B are corret

upvoted 1 times

Question #682 *Topic 1*

Which characteristic differentiates the concept of authentication from authorization and accounting?

A. consumption-based billing

B. identity verification

C. user-activity logging

D. service limitations

Correct Answer: *B*

mellos 6 months, 2 weeks ago

No entiendo esta pregunta

upvoted 2 times

Request7108 5 months, 1 week ago

Agreed. This is a very confusing question.

upvoted 1 times

Question #683 *Topic 1*

What is a function of Cisco Advanced Malware Protection for a Next-Generation IPS?

A. inspecting specific files and file types for malware

B. authorizing potentially compromised wireless traffic

C. authenticating end users

D. URL filtering

Correct Answer: *A*

Question #684 *Topic 1*

What is a feature of WPA?

A. TKIP/MIC encryption

B. small Wi-Fi application

C. preshared key

D. 802.1x authentication

Correct Answer: *A*

KingJPugh 1 day, 7 hours ago

Selected Answer: A

From the OCG, pg 662, Table 28-2:
"Encryption and MIC with TKIP?"
WPA: Yes
WPA2: No
WPA3: No

upvoted 1 times

beerbisceps1 2 months ago

going with A
https://www.arubanetworks.com/techdocs/Instant_40_Mobile/Advanced/Content/UG_files/Authentication/UnderstandingEncryption.htm#:~:text=WPA%20uses%20TKIP%20and%20WPA2%20uses%20the%20AES%20algorithm.

upvoted 1 times

Phonon 5 months ago

Could be A or C.
Bad question. WPA can use both TKIP/MIC and Pre-Shared Key

upvoted 4 times

battlefate 5 months, 3 weeks ago

I can't find any suitable answer to this question.
A, C and D can be used as one of the security feature with WEP, WPA, WPA2
B is just not related to the question.

upvoted 1 times

mis779548 5 months, 1 week ago

and you the same

upvoted 1 times

Question #685 *Topic 1*

Which two practices are recommended for an acceptable security posture in a network? (Choose two.)

A. Use a cryptographic keychain to authenticate to network devices.

B. Place internal email and file servers in a designated DMZ.

C. Back up device configurations to encrypted USB drives for secure retrieval.

D. Disable unused or unnecessary ports, interfaces, and services.

E. Maintain network equipment in a secure location.

Correct Answer: *DE*

alejandro12 Highly Voted 6 months, 3 weeks ago

A,D
Use a cryptographic keychain to authenticate to network devices is correct, think Maintain network equipment in a secure location should be for physical not for security posture
upvoted 5 times

Shun5566 Most Recent 1 week, 1 day ago

Selected Answer: AD

Agree alejandro
upvoted 1 times

bisiyemo1 1 month, 2 weeks ago

Selected Answer: AD

A and D is the correct answers
upvoted 1 times

Question #686 *Topic 1*

How does WPA3 improve security?

A. It uses SAE for authentication.

B. It uses RC4 for encryption.

C. It uses TKIP for encryption.

D. It uses a 4-way handshake for authentication.

Correct Answer: *A*

Surves Highly Voted 6 months, 1 week ago

Selected Answer: A

And Aes for encryption
upvoted 8 times

SVN05 3 months, 3 weeks ago

Agreed.
upvoted 1 times

Question #687 *Topic 1*

What is a function of a Next-Generation IPS?

A. correlates user activity with network events

B. serves as a controller within a controller-based network

C. integrates with a RADIUS server to enforce Layer 2 device authentication rules

D. makes forwarding decisions based on learned MAC addresses

Correct Answer: *A*

Dutch012 Highly Voted 2 months, 4 weeks ago

What the hell is that Cisco!?, I am probably going to get royally as.s fu.cked if these type of questions in the exam

upvoted 9 times

Wes_60 2 months ago

You ain't kidding.

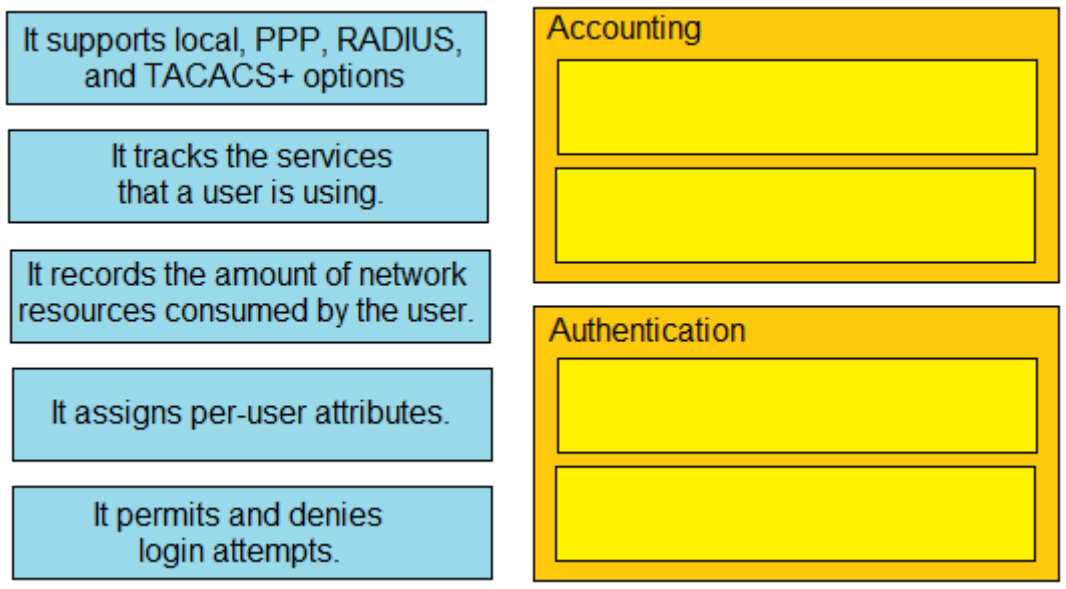
upvoted 1 times

Question #688 *Topic 1*

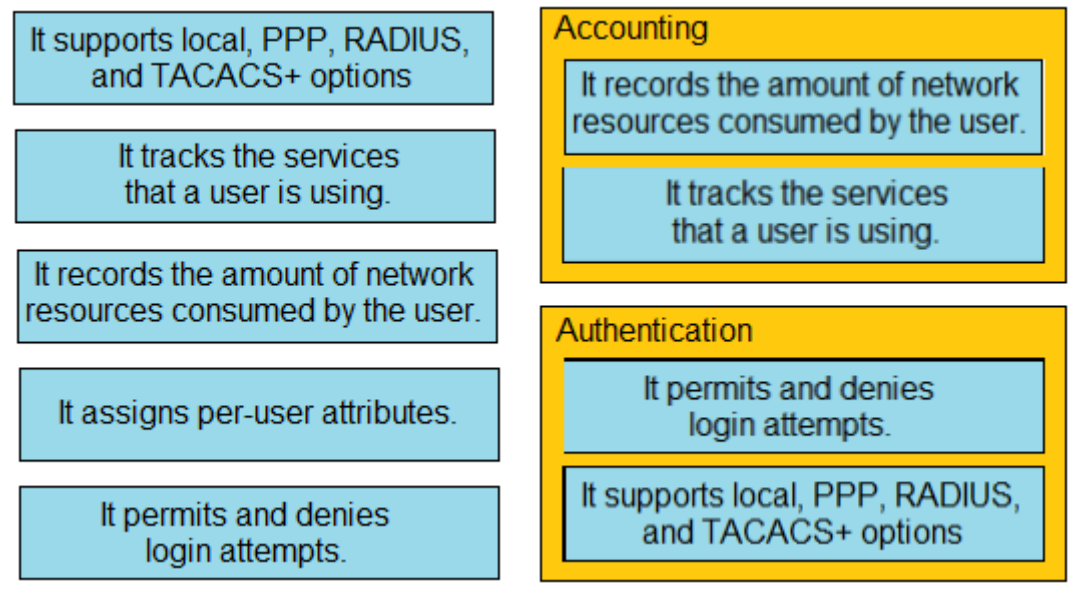
DRAG DROP -

Drag and drop the statements about AAA from the left onto the corresponding AAA services on the right. Not all options are used.

Select and Place:



Correct Answer:



RougePotatoe Highly Voted 6 months, 2 weeks ago

Per user attributes sounds like authorization. As each user could be configured to have different authorizations to different software and applications.

upvoted 6 times

Request7108 Most Recent 5 months, 1 week ago

In the AAA environment I run, there are attributes returned in the authorization profile. These are called Cisco AV pairs, which stands for "attribute values"
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215525-use-radius-for-device-administration-wit.html

upvoted 2 times

Question #689 *Topic 1*

DRAG DROP -

Drag and drop the elements of a security program from the left onto the corresponding descriptions on the right.

Select and Place:

awareness	document that outlines an organization's security goals and practices and the roles and responsibilities of the organization's personnel
education	tactical document that sets out specific tasks and methods to maintain security
security policy	user-awareness learning level that focuses on learning about topics and practices beyond what is typically required by the user's job
security standard	user-awareness learning level that focuses on security practices that all employees must understand and enforce
training	user-awareness learning level that focuses on teaching employees how to perform tasks specifically required by their jobs

Correct Answer:

awareness	security policy
education	security standard
security policy	awareness
security standard	education
training	training

RougePotatoe Highly Voted 7 months, 1 week ago

security policy
security standard
education
awareness
training

It fits better takes it or leave it. The nuances is too blurry I wish cisco went out of business.

upvoted 20 times

EthanhuntMI6 Highly Voted 5 months, 4 weeks ago

This is probably the most stupidest question you can ask for a certification exam. Great job cisco, never fails to disappoint us.

upvoted 13 times

deluxeccna Most Recent 1 month, 2 weeks ago

Such a stupid question. Looks more like a Cambridge English test

upvoted 3 times

BI1024 7 months, 3 weeks ago

Awarness and education should be replaced in the answer no?

upvoted 6 times

EliasM 7 months, 2 weeks ago

I believe so, but i dont know for sure...

upvoted 2 times

Question #690 *Topic 1*

Which IPsec transport mode encrypts the IP header and the payload?

A. pipe

B. transport

C. control

D. tunnel

Correct Answer: *D*

Goena 4 months, 2 weeks ago

Selected Answer: D

IPsec is used in tunnel mode or transport mode. Security gateways use tunnel mode because they can provide point-to-point IPsec tunnels. ESP tunnel mode encrypts the entire packet, including the original packet headers.

upvoted 2 times

Question #691 *Topic 1*

What is the default port-security behavior on a trunk link?

A. It places the port in the err-disabled state if it learns more than one MAC address.

B. It causes a network loop when a violation occurs.

C. It disables the native VLAN configuration as soon as port security is enabled.

D. It places the port in the err-disabled state after 10 MAC addresses are statically configured.

Correct Answer: *A*

rijstraket Highly Voted 5 months, 4 weeks ago

Selected Answer: A

When you enable port security on a switch, by default only one MAC address can be learned. To allow more than one MAC address on a switch port simultaneously, use the command:port-security maximum <max-number>.

upvoted 6 times

Vikramaditya_J Most Recent 1 month ago

Selected Answer: B

It's a vague question. None of the options present a correct answer, but A looks somewhat closer. Here's why:
A trunk port does not place the port in the err-disabled state if it learns more than one MAC address, as port security is not supported on trunk ports. Therefore, it is not possible for a trunk port to trigger the err-disabled state due to port security violations. However, it is possible to configure port security on a trunk port to restrict the number of MAC addresses allowed on a specific VLAN.

upvoted 1 times

rogi2023 2 months, 3 weeks ago

I think, portsecurity is NOT enabled on trunk intf, you have to change it to access mode first. To me it is another stupid question.

upvoted 1 times

michael1001 5 months, 4 weeks ago

Selected Answer: A

Labbed it (quickly) in packet tracer, answer is A

upvoted 2 times

alejandro12 6 months, 2 weeks ago

A, dont have sense, the objetive of trunk is learns more than one MAC address.
Should be C

upvoted 2 times

Question #692 *Topic 1*

Which device separates networks by security domains?

A. intrusion protection system

B. firewall

C. wireless controller

D. access point

Correct Answer: *B*

Question #693 *Topic 1*

How are VLAN hopping attacks mitigated?

A. manually implement trunk ports and disable DTP

B. configure extended VLANs

C. activate all ports and place in the default VLAN

D. enable dynamic ARP inspection

Correct Answer: *A*

Etidic 7 months, 2 weeks ago

Selected Answer: A

A is the correct answer

upvoted 3 times

Question #694 *Topic 1*

Which enhancements were implemented as part of WPA3?

A. Forward secrecy and SAE in personal mode for secure initial key exchange

B. 802.1x authentication and AES-128 encryption

C. AES-64 in personal mode and AES-128 in enterprise mode

D. TKIP encryption improving WEP and per-packet keying

Correct Answer: *A*

Ciscoman021 2 months ago

Selected Answer: A

Forward security and SAE in personal mode for secure initial key exchange were implemented as part of WPA3.

upvoted 1 times

Smaritz 4 months ago

A: This new system, called Wi-Fi Device Provisioning Protocol (DPP), works by transmitting how to gain access to the system without transmitting a password into the air. With DPP, users use QR codes or NFC tags to let devices onto the network. By snapping a picture or receiving a radio signal from the router, a device can be authenticated to the network without sacrificing security.

upvoted 1 times

Question #695 *Topic 1*

When a site-to-site VPN is configured which IPsec mode provides encapsulation and encryption of the entire original IP packet?

A. IPsec transport mode with AH

B. IPsec tunnel mode with AH

C. IPsec transport mode with ESP

D. IPsec tunnel mode with ESP

Correct Answer: *D*

michael1001 Highly Voted 5 months, 4 weeks ago

Selected Answer: D

Authentication Header (AH)
Encapsulating Security Payload (ESP)

upvoted 12 times

Question #696 *Topic 1*

An engineer is configuring remote access to a router from IP subnet 10.139.58.0/28. The domain name, crypto keys, and SSH have been configured. Which configuration enables the traffic on the destination router?

A. line vty 0 15 access-class 120 in ! ip access-list extended 120 permit tcp 10.139.58.0 0.0.0.15 any eq 22

B. interface FastEthernet0/0 ip address 10.122.49.1 255.255.255.252 ip access-group 10 in ! ip access-list standard 10 permit udp 10.139.58.0 0.0.0.7 host 10.122.49.1 eq 22

C. interface FastEthernet0/0 ip address 10.122.49.1 255.255.255.252 ip access-group 110 in ! ip access-list standard 110 permit tcp 10.139.58.0 0.0.0.15 eq 22 host 10.122.49.1

D. line vty 0 15 access-group 120 in ! ip access-list extended 120 permit tcp 10.139.58.0 0.0.0.15 any eq 22

Correct Answer: *A*

ricky1802 3 months ago

Selected Answer: A

A is the correct answer. Line vty can go only with access-class, not with access-group!

upvoted 4 times

Dutch012 3 months, 1 week ago

It should be access-group 120 like answer D not like A

upvoted 1 times

icecool2019 7 months, 3 weeks ago

The answer should be C

upvoted 2 times

RougePotatoe 7 months, 1 week ago

Standard access range is 1-99 so it can't be C.

upvoted 4 times

EliasM 7 months, 2 weeks ago

I disagree. In C you are allowing source port 22. Clients will never use port 22 as source port when connecting to a ssh device. They will use a randomly generate port, usually between the 49k-65k port range. The only options that correctly configured the ACL are A and D, but only A uses the correct command for VTY lines which is access-class. So correct answer is A.

upvoted 6 times

Request7108 5 months, 1 week ago

No, this is for SSH access so it will be port 22

upvoted 1 times

Question #697 *Topic 1*

In an SDN architecture, which function of a network node is centralized on a controller?

A. Creates the IP routing table

B. Discards a message due filtering

C. Makes a routing decision

D. Provides protocol access for remote access devices

Correct Answer: *C*
A controller, or SDN controller, centralizes the control of the networking devices. The degree of control, and the type of control, varies widely. For instance, the controller can perform all control plane functions (such as making routing decisions) replacing the devices' distributed control plane.
Reference:
https://www.ciscopress.com/articles/article.asp?p=2995354&seqNum=2#:~:text=A%20controller%2C%20or%20SDN%20controller,the%20devices'%20distributed%20control%20plane

clivebarker86 Highly Voted 7 months, 3 weeks ago
control plane, create routing table
upvoted 11 times

TinKode 6 months, 3 weeks ago
And data plane makes routing decisions based on control plane routing table.
upvoted 3 times

enzo86 Most Recent 4 months ago
the answer is A The term control plane refers to any action that controls the data plane. Most of these actions have to do with creating the tables used by the data plane, tables such as the IP routing table, an IP Address Resolution Protocol (ARP) table, a switch MAC address table, and so on.
upvoted 1 times

danny43213 4 months ago
one of the functions of a data plane is matching the destination IP address IP address to the routing table i.e routing decission but the table is in the control plane therfore I go with A.
upvoted 2 times

michael1001 5 months, 4 weeks ago
Selected Answer: C
C is correct - Several articles on the purpose of an SDN controller confirms that the controller becomes the control plane exists in the middle of the management and data plane.
upvoted 1 times

RougePotatoe 6 months, 2 weeks ago
Question 760 is a similar question and its answer was make routing decisions
upvoted 1 times

Question #698 *Topic 1*

Which management security process is invoked when a user logs in to a network device using their username and password?

A. authentication

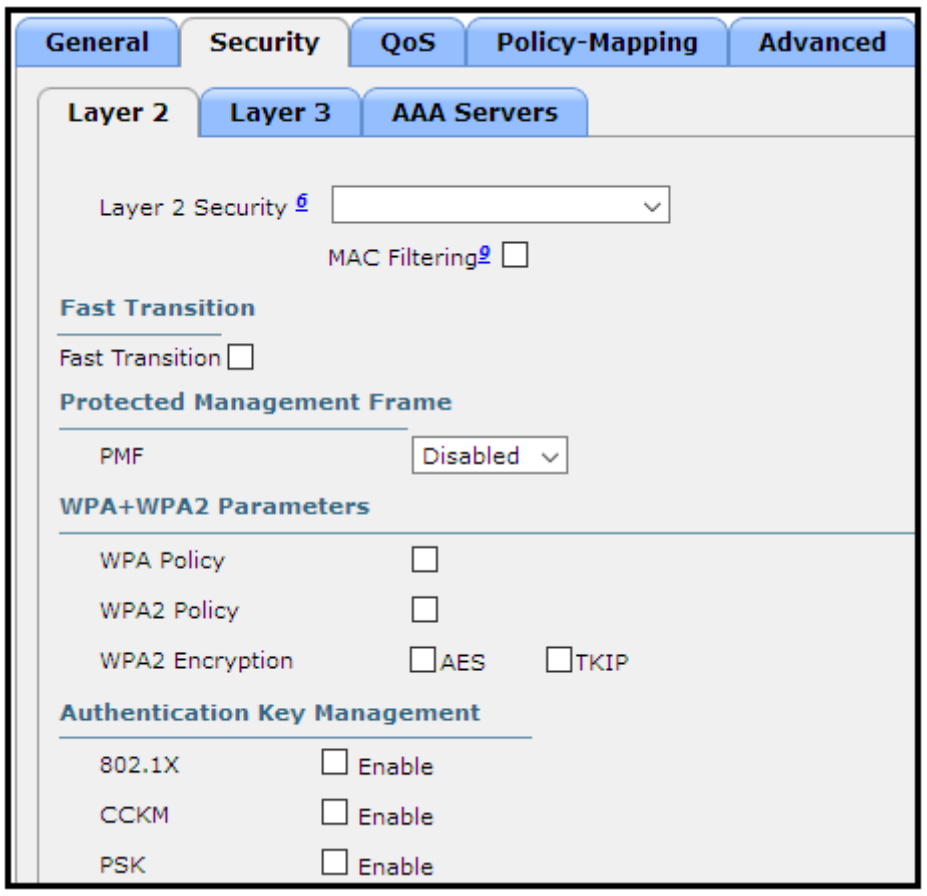
B. auditing

C. accounting

D. authorization

Correct Answer: *A*

Question #699 *Topic 1*



Refer to the exhibit. What are the two steps an engineer must take to provide the highest encryption and authentication using domain credentials from LDAP?
(Choose two.)

A. Select PSK under Authentication Key Management.

B. Select Static-WEP + 802.1X on Layer 2 Security.

C. Select WPA+WPA2 on Layer 2 Security.

D. Select 802.1X from under Authentication Key Management.

E. Select WPA Policy with TKIP Encryption.

Correct Answer: *CD*

Goh0503 Highly Voted 7 months, 4 weeks ago

Answer is C and D
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/211277-WLC-with-LDAP-Authentication-Configurati.html#:~:text=Step%206.%20Set%20the%20L2%20security%20method%20to%20WPA2%20%2B%20802.1x%20and%20set%20L3%20security%20to%20noneas%20shown%20in%20the%20image.

upvoted 5 times

Question #700 *Topic 1*

Which enhancement is implemented in WPA3?

A. employs PKI to identify access points

B. applies 802.1x authentication

C. uses TKIP

D. protects against brute force attacks

Correct Answer: *D*

StingVN 2 weeks, 3 days ago

Selected Answer: A

The enhancement implemented in WPA3 (Wi-Fi Protected Access 3) is that it employs PKI (Public Key Infrastructure) to identify access points.

A. Employs PKI to identify access points.

In WPA3, the use of PKI allows for more secure identification and authentication of access points. It helps ensure that the client devices are connecting to legitimate and trusted access points, reducing the risk of connecting to rogue or malicious networks.

Therefore, option A is the correct enhancement implemented in WPA3.

upvoted 1 times

Ciscoman021 2 months ago

Selected Answer: D

The correct answer is D. WPA3 (Wi-Fi Protected Access 3) implements an enhancement to protect against brute-force attacks.

upvoted 1 times

Smaritz 4 months ago

Answer is D: Home users are expected to use the WPA3 Personal form, which relies on passphrase-based authentication. This form offers a familiar user experience but a vastly superior level of protection against brute force cracking thanks to Simultaneous Authentication of Equals (SAE).

https://www.netspotapp.com/blog/wifi-security/what-is-wpa3.html

upvoted 1 times

Goh0503 7 months, 4 weeks ago

Selected Answer: D

Answer D
https://blogs.cisco.com/networking/wpa3-bringing-robust-security-for-wi-fi-networks#:~:text=Protection%20against%20brute%20force%20%E2%80%9Cdictionary%E2%80%9D%20attacks%20and%20passive%20attacks.

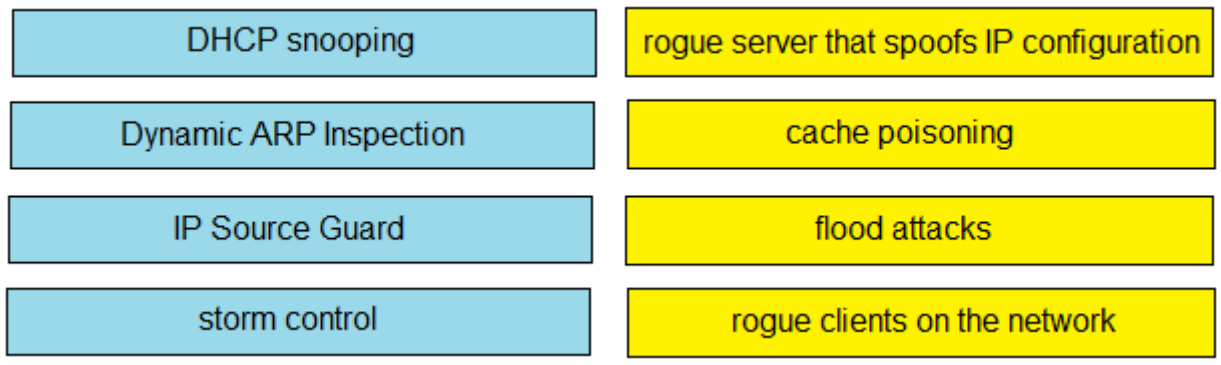
upvoted 4 times

Question #701 *Topic 1*

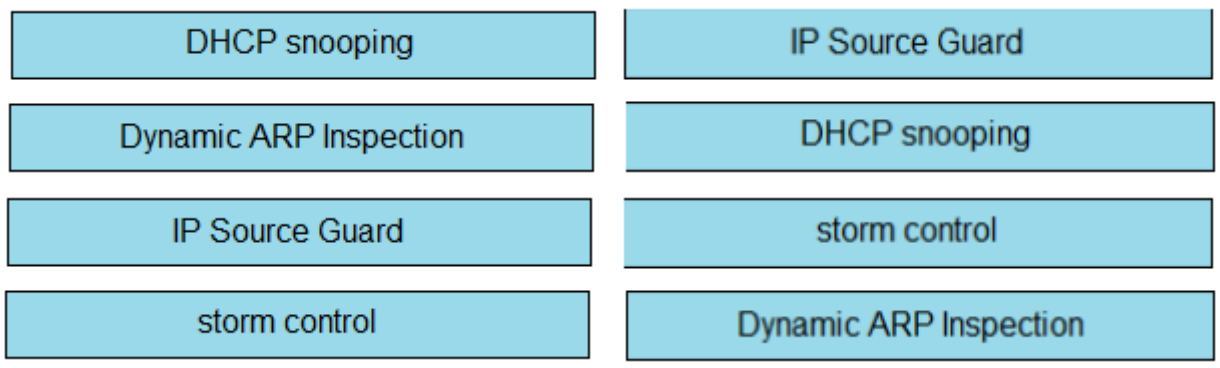
DRAG DROP -

Drag and drop the Cisco IOS attack mitigation features from the left onto the types of network attack they mitigate on the right.

Select and Place:



Correct Answer:



Anon1216 Highly Voted 8 months, 2 weeks ago

Correct me if I'm wrong, but this answer doesn't look right to me at all. Shouldn't it be:

DHCP Snooping - Rogue server, Dynamic ARP Inspection - Cache poisoning, IP Source Guard - rogue clients, storm control - flood attacks

upvoted 26 times

splashy Highly Voted 8 months, 2 weeks ago

I agree with Anon

DHCP Snooping - Rogue server that spoofs ip config (rogue DHCP server)
Dynamic ARP Inspection - Cache poisoning (ARP cache poisoning)
storm control - flood attacks
IP Source Guard - rogue clients (IP source guard is configured separated but uses the dhcp snooping bindings table to detect a malicious IP/MAC combo)

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_0110110.html#d351221e533a1635

upvoted 16 times

RougePotatoe Most Recent 7 months, 1 week ago

Answer should be, see use case and explanation of what each does below:
IP source guard
Dynamic Arp inspection
Storm control
DHCP snooping

upvoted 2 times

RougePotatoe 7 months, 1 week ago

You can use IP source guard to prevent traffic attacks if a host tries to use the IP address of its neighbor and you can enable IP source guard when DHCP snooping is enabled on an untrusted interface....It filters traffic based on the DHCP snooping binding database and on manually configured IP source bindings...IPSG for static hosts allows IPSG to work without DHCP.

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_0110110.html#:~:text=You can use IP source,enabled on an untrusted interface.

upvoted 1 times

RougePotatoe 7 months, 1 week ago

A server will typically be statically configured. In other words typically configured to not receive an ip address from the DHCP server. DHCP snooping would only be aware of the DHCP assigned ip addresses so that is why we need something that can work with manually configured (static) ip addresses. This brings up the question as to why they would have a server on an untrusted port, as ip source guard only can be configured on untrusted ports. The alternative question is, if the rogue server is connected to another port (not the same one as the original it is trying to spoof) why would they have IPSG configured on the other untrusted ports?

upvoted 1 times

RougePotatoe 7 months, 1 week ago

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. Storm control is applicable for physical interfaces and is used to restrict the unicast, broadcast and multicast ingress traffic on the Layer2 interfaces.

https://www.cisco.com/c/dam/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/asr903/sec-storm-control-xe-3s-asr903-book.html#:~:text=Storm control prevents traffic on,traffic on the Layer2 interfaces.

upvoted 1 times

RougePotatoe 7 months, 1 week ago

Dynamic ARP Inspection (DAI) is a security feature that validates Address Resolution Protocol (ARP) packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address bindings

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html#96862

upvoted 1 times

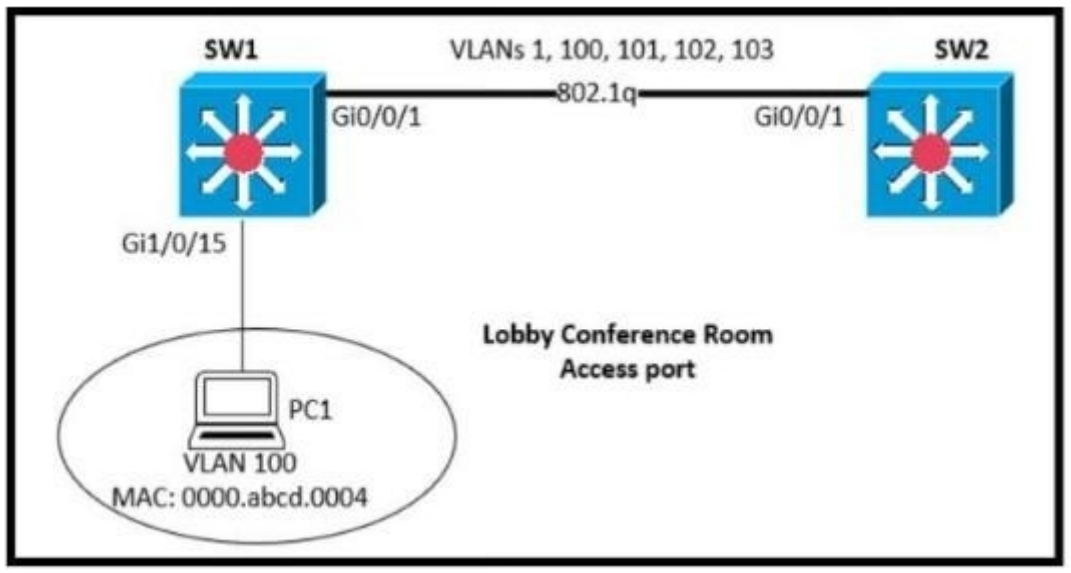
RougePotatoe 7 months, 1 week ago

The DHCP snooping feature determines whether traffic sources are trusted or untrusted. An untrusted source may initiate traffic attacks or other hostile actions. To prevent such attacks, the DHCP snooping feature filters messages and rate-limits traffic from untrusted sources.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/snoodhcp.pdf

upvoted 1 times

Question #702 *Topic 1*



SW1 supports connectivity for a lobby conference room and must be secured. The engineer must limit the connectivity from PC1 to the SW1 and SW2 network.

The MAC addresses allowed must be limited to two. Which configuration secures the conference room connectivity?

A. interface gi1/0/15 switchport port-security switchport port-security maximum 2

B. interface gi1/0/15 switchport port-security switchport port-security mac-address 0000.abcd.0004vlan 100

C. interface gi1/0/15 switchport port-security mac-address 0000.abcd.0004 vlan 100

D. interface gi1/0/15 switchport port-security mac-address 0000.abcd.0004 vlan 100 interface switchport secure-mac limit 2

Correct Answer: *A*

4aynick 1 month, 1 week ago

correct answer - A

upvoted 2 times

DaimonANCC 1 month, 4 weeks ago

chatgpt wrote the right question C

upvoted 1 times

Question #703 *Topic 1*

```
SW1#show run
Building configuration...
!
hostname SW1
!
ip domain-name CCNA-test
!
username CCNA privilege 1 password 0 cisco123
!
interface FastEthernet0/1
 switchport access vlan 10
!
interface Vlan10
 ip address 192.168.1.2 255.255.255.0
!
line vty 0 4
 login local
 transport input telnet
line vty 5 15
 login local
 transport input telnet

SW1#show crypto key mypubkey rsa
% Key pair was generated at: 0:1:23 UTC Mar 1 2020
Key name: SW1.CCNA-test
```

Refer to the exhibit. An engineer is updating the management access configuration of switch SW1 to allow secured, encrypted remote configuration. Which two commands or command sequences must the engineer apply to the switch? (Choose two.)

A. SW1(config)#enable secret ccnaTest123

B. SW1(config)#username NEW secret R3mote123

C. SW1(config)#line vty 0 15 SW1(config-line)#transport input ssh

D. SW1(config)# crypto key generate rsa

E. SW1(config)# interface f0/1 SW1(confif-if)# switchport mode trunk

Correct Answer: *CD*

joondale Highly Voted 8 months, 2 weeks ago

Selected Answer: AC

Going with A and C. There is a username and password configured already. Configuring enable secret is a must when using SSH otherwise you cannot enter to enabled mode. Try it in packet tracer. Pls correct me if im wrong

upvoted 18 times

oatmealturkey 4 months ago

Yep you are right! I tried it in PT.

First I did B and C on the switch. Then went on the PC and although I successfully connected to the switch via SSH, it did not allow me to enter into privileged EXEC mode because of the missing enable secret command.

So I went back to the switch and removed B, then did A. Went back to the PC to connect via SSH, connected with no problem, and was then able to enter into privileged EXEC mode and thus configure the switch remotely which is what the question requires.

Thanks all!

upvoted 5 times

EthanhuntMI6 5 months, 4 weeks ago

Level 0 – Zero-level access only allows five commands- logout, enable, disable, help and exit.

Level 1 – User-level access allows you to enter in User Exec mode that provides very limited read-only access to the router.

Level 15 – Privilege level access allows you to enter in Privileged Exec mode and provides complete control over the router.

upvoted 1 times

Etidic 7 months, 2 weeks ago

the username and password already configured as you see is a PRIVILEGE 1 level credential which is why it is necessary to create another username and secret to enable privilege exec mode access. You do not necessarily need to add the command enable secret <string> to access the privileged exec mode via telnet/ssh. the username and secret command should be adequate when the LOGIN LOCAL command in added to the LINE VTY 0 4/5 15 interface.

I hope this helps!
upvoted 2 times

IAmAlwaysWrongOnExamtopics 5 months, 4 weeks ago
we need enable secret to go into privilege exec mode
upvoted 3 times

splashy 8 months, 1 week ago
Tested, very good catch! I've never been aware of this (because we always use an enable secret...)
upvoted 2 times

StingVN Most Recent 2 weeks, 2 days ago
Selected Answer: BD
B. SW1(config)#username NEW secret R3mote123
This command creates a new username (NEW) with a password (R3mote123) for authentication when accessing the switch remotely.

D. SW1(config)#crypto key generate rsa
This command generates an RSA key pair used for secure SSH communication. The RSA key pair is necessary for encrypting the remote management traffic.

Therefore, options B and D are the commands or command sequences that the engineer must apply to the switch to enable secured, encrypted remote configuration.
upvoted 1 times

ccna_exam 2 weeks, 5 days ago
The correct answers are:

A. SW1(config)#enable secret ccnaTest123
C. SW1(config)#line vty 0 15 SW1(config-line)#transport input ssh

The enable secret command sets the password for the privileged EXEC mode. The transport input ssh command configures the switch to accept only SSH connections on the virtual terminal lines (VTYs).

The other options are incorrect.

Option B, username NEW secret R3mote123, creates a new username and password for remote access, but it does not secure the connection.

Option D, crypto key generate rsa, generates an RSA key pair for SSH authentication, but it does not configure the switch to accept SSH connections.

Option E, interface f0/1 switchport mode trunk, configures interface f0/1 as a trunk port, but it does not affect remote access.
upvoted 1 times

ccna_exam 2 weeks, 5 days ago
The correct answers are:

C. SW1(config)#line vty 0 15 SW1(config-line)#transport input ssh
D. SW1(config)# crypto key generate rsa
These commands will enable SSH on the switch and generate an RSA key pair, which is required for SSH authentication.

The other commands are not necessary for enabling SSH on the switch. The command in option A sets the enable password, which is used for local login to the switch. The command in option B creates a new user account with the username "NEW" and the password "R3mote123". The command in option E configures interface f0/1 as a trunk port.
upvoted 1 times

rogi2023 2 months, 3 weeks ago
Selected Answer: AC
I agree with joondale. Although the username is just privilege Level1, but in this level 1 the enable cmd is accessible so therefore "Configuring enable secret is a must when using SSH otherwise you cannot enter to enabled mode." Therefore answers are A and C.
upvoted 1 times

Yaqub009 3 months, 2 weeks ago
Selected Answer: AC
In the exhibit,
1.Hostname changed
2.Domain-name configured
3.Username and Password configured (B had been configured,no longer needed)
4.crypto key also configured (D had been configured, D no longer needed)

B D wrong, A C True.
upvoted 2 times

Yaqub009 3 months, 3 weeks ago
Selected Answer: AC
Wrongs:
B.Username is given on exhibit.

D.Key is also generated. Attention to the end of the exhibition
E.Fa0/1 is access port

Corrects:
A.We must set password to ENABLE mode for ssh config
C.Only TELNET config on exhibit. We must config "transport input ssh" command.
upvoted 1 times

mohdhafizudddinesa 5 months, 3 weeks ago

B is wrong since in the answer option only create a normal user access and not privilege user

https://study-ccna.com/cisco-privilege-levels/#:~:text=It%20is%20important%20to%20secure,the%20devices%20from%20unauthorized%20access.
upvoted 1 times

michael1001 5 months, 4 weeks ago

Selected Answer: BC

Answer is B and C, answer well explained by Etidic
upvoted 2 times

Etidic 7 months, 2 weeks ago

Selected Answer: BC

the correct answer is B and C
upvoted 1 times

splashy 8 months, 1 week ago

Selected Answer: AC

Tested in PT
C:\>ssh -l kek 192.168.1.2

Password:

S1>enable
% No password set.
upvoted 2 times

splashy 7 months ago

To make things clear...

If there is no "username blabla privilege 15 password/secret blabla" entered
which would make the user log in to priviledged switch# directly, and not switch>

you need to have an "enable secret blabla" command entered or the user will not be able to enter priviledged mode and be stuck in switch>
not being able to get to switch#

Don't take my word for it try it yourself in PT.
upvoted 3 times

king_oat 8 months, 2 weeks ago

Selected Answer: BC

Answer is wrong, can see in the exhibit that a crypto key has already been generated.
Answer is: B C
upvoted 2 times

ShadyAbdekmalek 8 months, 2 weeks ago

Selected Answer: BC

B. SW1(config)#username NEW secret R3mote123
C. SW1(config)#line vty 0 15 SW1(config-line)#transport input ssh
upvoted 3 times

Anon1216 8 months, 2 weeks ago

Selected Answer: BC

Answer is wrong, can see in the exhibit that a crypto key has already been generated.
Answer is: B C
upvoted 4 times

Anon1216 8 months, 2 weeks ago

Answer is wrong, can see in the exhibit that a crypto key has already been generated.
Answer is: B C
upvoted 2 times

Question #704 *Topic 1*

Which port security violation mode allows from valid MAC addresses to pass but blocks traffic from invalid MAC addresses?

A. restrict

B. shutdown

C. protect

D. shutdown VLAN

Correct Answer: *C*

Tylosh Highly Voted 8 months, 2 weeks ago

I don't think it's a good question , because “protect” and “restrict” also allows traffic from passing with a valid

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port_sec.pdf

upvoted 10 times

creaguy 8 months, 1 week ago

When configuring port security violation modes, note the following information:
• protect—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
• restrict—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the SecurityViolation counter to increment.
• shutdown—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

upvoted 1 times

rogi2023 2 months, 3 weeks ago

restrict also sends a SNMP trap. Tylosh is right both ""protect” and “restrict” also allows traffic from passing with a valid MAC... but as Bieley says: "Always apply the answer with the least privileges. So protect."

upvoted 1 times

BieLey 8 months, 1 week ago

Always apply the answer with the least privileges. So protect.

upvoted 2 times

VicM Most Recent 2 weeks, 6 days ago

Protect – When a violation occurs in this mode, the switchport will permit traffic from known MAC addresses to continue sending traffic while dropping traffic from unknown MAC addresses. When using this mode, no notification message is sent when this violation occurs.
https://www.pluralsight.com/blog/it-ops/switchport-security-concepts#:~:text=Protect%20%E2%80%93%20When%20a%20violation%20occurs,sent%20when%20this%20violation%20occurs.

upvoted 1 times

Question #705 *Topic 1*

A customer wants to provide wireless access to contractors using a guest portal on Cisco ISE. The portal is also used by employees. A solution is implemented, but contractors receive a certificate error when they attempt to access the portal. Employees can access the portal without any errors. Which change must be implemented to allow the contractors and employees to access the portal?

A. Install an Internal CA signed certificate on the Cisco ISE.

B. Install a trusted third-party certificate on the Cisco ISE.

C. Install an internal CA signed certificate on the contractor devices.

D. Install a trusted third-party certificate on the contractor devices.

Correct Answer: *B*
Reference:
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/200295-Install-a-3rd-party-CA-certificate-in-IS.html

RougePotatoe Highly Voted 6 months, 2 weeks ago

Selected Answer: C

Supplied reference seemed like a lazy copy and paste without verifying it was relevant or not.
Since employees can access the portal it indicates that this is an issue strictly on the contractors' devices and not on the ISE. Assuming this ISE is not meant to be access by anyone but the contractors and employees internally signed certificate should be added on contractors' devices to allow trust. No need for 3rd party because its meant to verify a website such as amazon is who they say they are. See link below.

https://www.ssl2buy.com/wiki/self-signed-certificate-vs-trusted-ca-signed-certificate

upvoted 10 times

hamish88 1 month, 2 weeks ago

Do you want to install an internal CA-signed certificate on 1000 contractor devices? Isn't it easier and more practical to install a trusted third-party certificate on the Cisco ISE? It also works for everyone.

upvoted 1 times

rogi2023 2 months, 2 weeks ago

Perhaps you are not allowed to install on contractor devices, so reading carefully answer "B" makes sense..

upvoted 2 times

ac89l Most Recent 3 weeks, 3 days ago

Selected Answer: B

It is recommended to use the Company Internal CA for Admin and EAP certificates, and a publicly-signed certificate for Guest/Sponsor/Hotspot/etc portals. The reason is that if a user or guest comes onto the network and the ISE portal uses a privately-signed certificate for the Guest Portal, they get certificate errors or potentially have their browser block them from the portal page. To avoid all that, use a publicly-signed certificate for Portal use to ensure a better user experience
Source: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215621-tls-ssl-certificates-in-ise.html

upvoted 2 times

huykg009 1 month, 2 weeks ago

Selected Answer: B

Why everybody chose C, the Correct is B
here is the link: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215621-tls-ssl-certificates-in-ise.html

upvoted 1 times

liviuml 1 month, 3 weeks ago

Selected Answer: B

Answer B.
I was thinking about B or C but after studies Sico recommendation I vote for B.
Search for Guest or Portal certificate in following link:
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215621-tls-ssl-certificates-in-ise.html
Regards,

upvoted 1 times

cristip 6 months ago

Selected Answer: D

i would say D

upvoted 1 times

Question #706 *Topic 1*

Which two wireless security standards use counter mode cipher block chaining Message Authentication Code Protocol for encryption and data integrity? (Choose two.)

A. Wi-Fi 6

B. WPA3

C. WEP

D. WPA2

E. WPA

Correct Answer: *BC*

Xavi01 Highly Voted 9 months ago

Selected Answer: BD

The correct answers are B/D. WPA2 & WPA3.

CCMP was certainly not around when WEP was established.

upvoted 5 times

michael1001 Highly Voted 5 months, 4 weeks ago

Selected Answer: BD

it's B and D, please fix.

upvoted 5 times

Ciscoman021 Most Recent 2 months, 1 week ago

Selected Answer: BD

The two wireless security standards that use counter mode cipher block chaining Message Authentication Code Protocol (CCMP) for encryption and data integrity are:

B. WPA3
D. WPA2

upvoted 1 times

sbnpj 2 months, 2 weeks ago

B/D, WEP uses TKIP

upvoted 1 times

gewe 3 months, 3 weeks ago

cbc-mac is used in wpa2
gcmp is used in wpa3

I would rather go only with WPA2...
but I m not for 100%sure

upvoted 1 times

kostka 8 months ago

Agreed. WEP is an old technology.

upvoted 2 times

creaguy 8 months, 1 week ago

Selected Answer: BD

C is wrong. It's WPA2

https://learningnetwork.cisco.com/s/question/0D53i00000Ksnr2CAB/wep-wpa-wpa2-tkip-aes-ccmp-eap#:~:text=WPA2%2C%20aka%20802.11i,help%20fast%20roaming.

upvoted 4 times

splashy 9 months ago

I think this should be WPA2 & WPA3 i could be wrong so feel free to correct :).

upvoted 1 times

Question #707 *Topic 1*

A network engineer is implementing a corporate SSID for WPA3-Personal security with a PSK. Which encryption cipher must be configured?

A. CCMP128

B. GCMP256

C. CCMP256

D. GCMP128

Correct Answer: *A*

StingVN 2 weeks, 2 days ago

Selected Answer: C

When implementing a corporate SSID for WPA3-Personal security with a PSK (Pre-Shared Key), the encryption cipher that must be configured is:

C. CCMP256

CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) is the encryption protocol used in WPA3, and the "256" refers to the key length. CCMP256 utilizes AES-256 (Advanced Encryption Standard with a key length of 256 bits) for stronger encryption and security.

Therefore, option C, CCMP256, is the correct encryption cipher that should be configured for a corporate SSID implementing WPA3-Personal security with a PSK.

upvoted 1 times

Ciscoman021 2 months ago

Selected Answer: A

WPA3-Personal use CCMP-128 and AES-128

upvoted 1 times

michael1001 5 months, 4 weeks ago

Selected Answer: A

CCMP128 is mandatory for WPA3:
https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

upvoted 3 times

Bl1024 7 months, 3 weeks ago

Answer is correct regarding WPA3-personal:
WPA3 mandates the adoption of Protected Management Frames, which help guard against eavesdropping and forging. It also standardizes the 128-bit cryptographic suite and disallows obsolete security protocols. WPA3-Enterprise has optional 192-bit security encryption and a 48-bit IV for heightened protection of sensitive corporate, financial and governmental data. WPA3-Personal uses CCMP-128 and AES-128.
https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

upvoted 1 times

clivebarker86 7 months, 3 weeks ago

CCMP is not WPA2?

upvoted 1 times

dosu01 6 months ago

Yes, but even WPA3 use it
GCMP256 is used for WPA3-Enterprise with 192-bit mode
https://www.wi-fi.org/discover-wi-fi/security

upvoted 1 times

Question #708 *Topic 1*

What is a practice that protects a network from VLAN hopping attacks?

A. Implement port security on internet-facing VLANs

B. Enable dynamic ARP inspection

C. Assign all access ports to VLANs other than the native VLAN

D. Configure an ACL to prevent traffic from changing VLANs

Correct Answer: *C*

papibarbu 4 months, 2 weeks ago
Yes C is Correct
upvoted 1 times

Tylosh 8 months, 2 weeks ago
Selected Answer: C
C is correct !
upvoted 1 times

Xavi01 9 months ago
Selected Answer: C
https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKPREA4/vlan1-and-vlan-hopping-attack
upvoted 1 times

Question #709 *Topic 1*

An administrator must use the password complexity not manufacturer-name command to prevent users from adding `Cisco` as a password.
Which command must be issued before this command?

A. login authentication my-auth-list

B. service password-encryption

C. password complexity enable

D. confreg 0x2142

Correct Answer: *C*

skeah Highly Voted 6 months, 4 weeks ago
It's C and the minimum length of with password complexity enable is 8.
https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5563-configure-password-settings-on-a-switch-through-the-command.html
upvoted 5 times

Question #710 *Topic 1*

An organization has decided to start using cloud-provided services. Which cloud service allows the organization to install its own operating system on a virtual machine?

A. platform-as-a-service

B. network-as-a-service

C. software-as-a-service

D. infrastructure-as-a-service

Correct Answer: *D*
Below are the 3 cloud supporting services cloud providers provide to customer:
☞ SaaS (Software as a Service): SaaS uses the web to deliver applications that are managed by a third-party vendor and whose interface is accessed on the clients' side. Most SaaS applications can be run directly from a web browser without any downloads or installations required, although some require plugins.
☞ PaaS (Platform as a Service): are used for applications, and other development, while providing cloud components to software. What developers gain with
PaaS is a framework they can build upon to develop or customize applications. PaaS makes the development, testing, and deployment of applications quick, simple, and cost-effective. With this technology, enterprise operations, or a third-party provider, can manage OSes, virtualization, servers, storage, networking, and the PaaS software itself. Developers, however, manage the applications.
☞ IaaS (Infrastructure as a Service): self-service models for accessing, monitoring, and managing remote datacenter infrastructures, such as compute (virtualized or bare metal), storage, networking, and networking services (e.g. firewalls). Instead of having to purchase hardware outright, users can purchase IaaS based on consumption, similar to electricity or other utility billing.
In general, IaaS provides hardware so that an organization can install their own operating system.

alexiro Highly Voted 2 years, 9 months ago
create a fault tolerant colocation site as a cloud provider, you would be searching for an Infrastructure as a Service provider. This would allow

you to install your own operation system and applications
upvoted 7 times

Hodicek Most Recent 1 year, 6 months ago
GIVEN ANSWE IS CORRECT
upvoted 2 times

Alsaher 2 years, 1 month ago
D is correct
upvoted 3 times

Question #711 *Topic 1*

How do traditional campus device management and Cisco DNA Center device management differ in regards to deployment?

A. Traditional campus device management allows a network to scale more quickly than with Cisco DNA Center device management.

B. Cisco DNA Center device management can deploy a network more quickly than traditional campus device management.

C. Cisco DNA Center device management can be implemented at a lower cost than most traditional campus device management options.

D. Traditional campus device management schemes can typically deploy patches and updates more quickly than Cisco DNA Center device management.

Correct Answer: *B*

Raymond9 Highly Voted 2 years, 6 months ago
exam technique: without any prior knowledge, u can rule out two of the options just because they criticize CISCO's product
upvoted 70 times

JamesDean_Youldiots 2 years ago
As someone with ZERO experience trying to break into the industry, I totally used that logic on a few of the questions, and even picked the answer that seemed like it praised CISCO the most. I took the exam after using PASS4SURE as a study guide. That bullshit application cost me hundreds of dollars to license, months of wasted time learning irrelevant questions, and another $300 wasted on the failed exam that i was completely unprepared for. i'm so bitter about spending months studying obsolete information. It has 455 questions and NONE of them are even RELEVANT to the CCNA. Unlike this braindump, which is a word for word copy of the exam questions. I'm definitely gonna pass this time around and you all are going to also!
upvoted 16 times

Ethiopis 2 years, 3 months ago
hahaha... good one.
upvoted 4 times

YoniEth 1 year, 7 months ago
obviously
upvoted 1 times

chomjosh Highly Voted 2 years, 9 months ago
Key word in question: "in regards to deployment". I find this strategy useful when questions have what looks like more than one correct answer in the options. An understanding of the question context helps to select the most appropriate answer.
B is therefore correct.
upvoted 7 times

Smaritz 1 year, 2 months ago
Yes it takes some time to read carefully and understand which aspect of something they are asking about
upvoted 1 times

dicksonpwc Most Recent 1 year, 9 months ago
Answer B is correct.
automation: Software Image Management (SWIM)

Manages software upgrades and controls the consistency of image versions and configurations across your network.

Speeds and simplifies the deployment of new software images and patches. Pre-and post-checks help prevent adverse effects from an upgrade.

Automation: Plug and Play (PnP)

Zero-touch provisioning for new device installation. Allows off-the-shelf Cisco devices to be provisioned simply by connecting to the network.

Enables deployment of new devices in minutes and without onsite support visits. Eliminates repetitive tasks and staging.
upvoted 3 times

anonymous1966 2 years, 2 months ago
Just to help, from the official book:
"Cisco hopes to continue to update Cisco DNA Center's traditional network management features to be equivalent compared to Cisco PI, to the point at which DNA Center could replace PI.In terms of intent and strategy, Cisco focuses their development of Cisco DNA Center features toward simplifying the work done by enterprises, with resulting reduced costs and much faster deployment of changes. Cisco DNA Center features help make initial installation easier, simplify the work to implement features that traditionally have challenging configuration, and use tools to help you notice issues more quickly. Some of the features unique to Cisco DNA Center include"
upvoted 2 times

Niko9988 2 years, 6 months ago
i doubt that DNA may speed up the INITIAL network deploymen. Normally it will take even more time because of the controller rollout. But the maintenance cost would be definetelly lower than using a traditional way of working.

So, i would vote for answer C.
upvoted 3 times

KyleP 2 years, 10 months ago
It can apply configs quickly making deployment faster.
upvoted 3 times

Question #712 *Topic 1*

Which purpose does a northbound API serve in a controller-based networking architecture?

A. facilitates communication between the controller and the applications

B. reports device errors to a controller

C. generates statistics for network hardware and traffic

D. communicates between the controller and the physical network hardware

Correct Answer: *A*

shakyak Highly Voted 1 year, 5 months ago
controller <->Application = northbound
controller<-> Devices = southbound
upvoted 11 times

dicksonpwc Highly Voted 1 year, 9 months ago
A is correct.
Explanation
A northbound interface is defined as the connection between the controller and applications
upvoted 6 times

SamuelSami Most Recent 8 months, 3 weeks ago
application programming interface
A northbound interface is an application programming interface (API) or protocol that allows a lower-level network component to communicate with a higher-level or more central component, while -- conversely -- a southbound interface allows a higher-level component to send commands to lower-level network components.
The purpose of northbound API
Northbound APIs are the link between the applications and the SDN controller. The applications can tell the network what they need (data, storage, bandwidth, and so on) and the network can deliver those resources, or communicate what it has
upvoted 2 times

Question #713 *Topic 1*

What benefit does controller-based networking provide versus traditional networking?

A. allows configuration and monitoring of the network from one centralized point

B. provides an added layer of security to protect from DDoS attacks

C. combines control and data plane functionality on a single device to minimize latency

D. moves from a two-tier to a three-tier network architecture to provide maximum redundancy

Correct Answer: *A*

DaBest 1 year, 8 months ago
the correct Answer is A (allows configuration and monitoring of the network from one centralized point)
upvoted 4 times

Question #714 *Topic 1*

What is an advantage of Cisco DNA Center versus traditional campus device management?

A. It is designed primarily to provide network assurance.

B. It supports numerous extensibility options, including cross-domain adapters and third-party SDKs.

C. It supports high availability for management functions when operating in cluster mode.

D. It enables easy autodiscovery of network elements in a brownfield deployment.

Correct Answer: *B*

Shamwedge Highly Voted 1 year, 6 months ago

B: It has the most cisco product hype

upvoted 16 times

ismatdmour Highly Voted 1 year, 2 months ago

Selected Answer: B

Careful. Such a question carries almost all correct with one or more words in 3 of them makes them incorrect. A is correct, DNA center assures networking by monitoring and other tools, however, it is not the "primary" objective (Automation and programmability is the primary objective. C is correct, but to provide high availability to data plane forwarding not to management functions. D is correct, but for "Green field" deployment rather in brownfield deployment. B is the only correct after all.

upvoted 11 times

Vinarino Most Recent 1 year, 4 months ago

B = thumbs up

(May 2018) Brownfield development is a term commonly used in the information technology industry to describe problem spaces needing the development and deployment of new software systems in the immediate presence of existing (legacy) software applications/systems.

GREENFIELD ==> via Cisco (Planning System Installation?)

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/UC8-5-1/ipt_system_inst_upg/planti.html

upvoted 1 times

NetAdmin950 2 years, 1 month ago

Answer is correct, Validate here :

https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-cent-plat-sol-over-cte-en.html

upvoted 3 times

Alsaher 2 years, 1 month ago

B is correct

upvoted 2 times

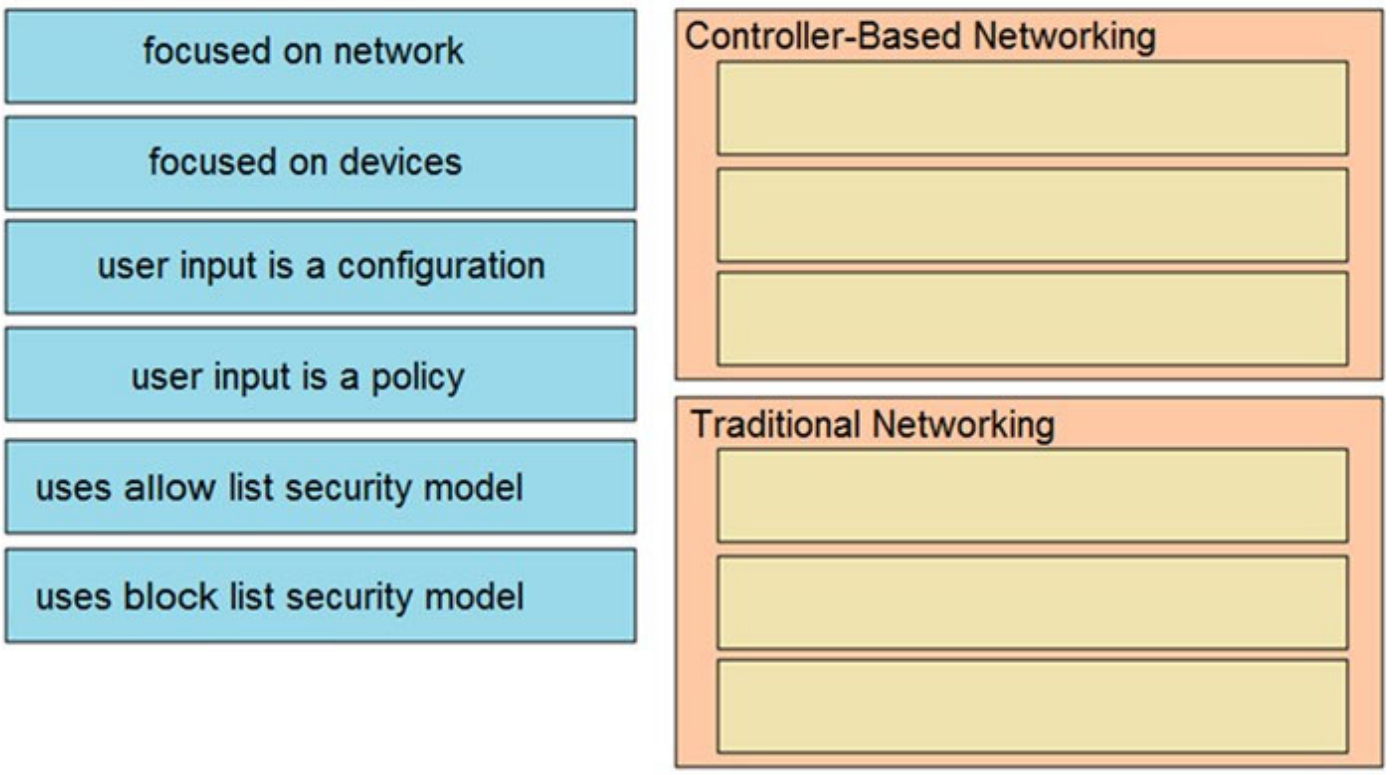
Question #715 *Topic 1*

DRAG DROP -

Drag and drop the characteristics of networking from the left onto the correct networking types on the right.

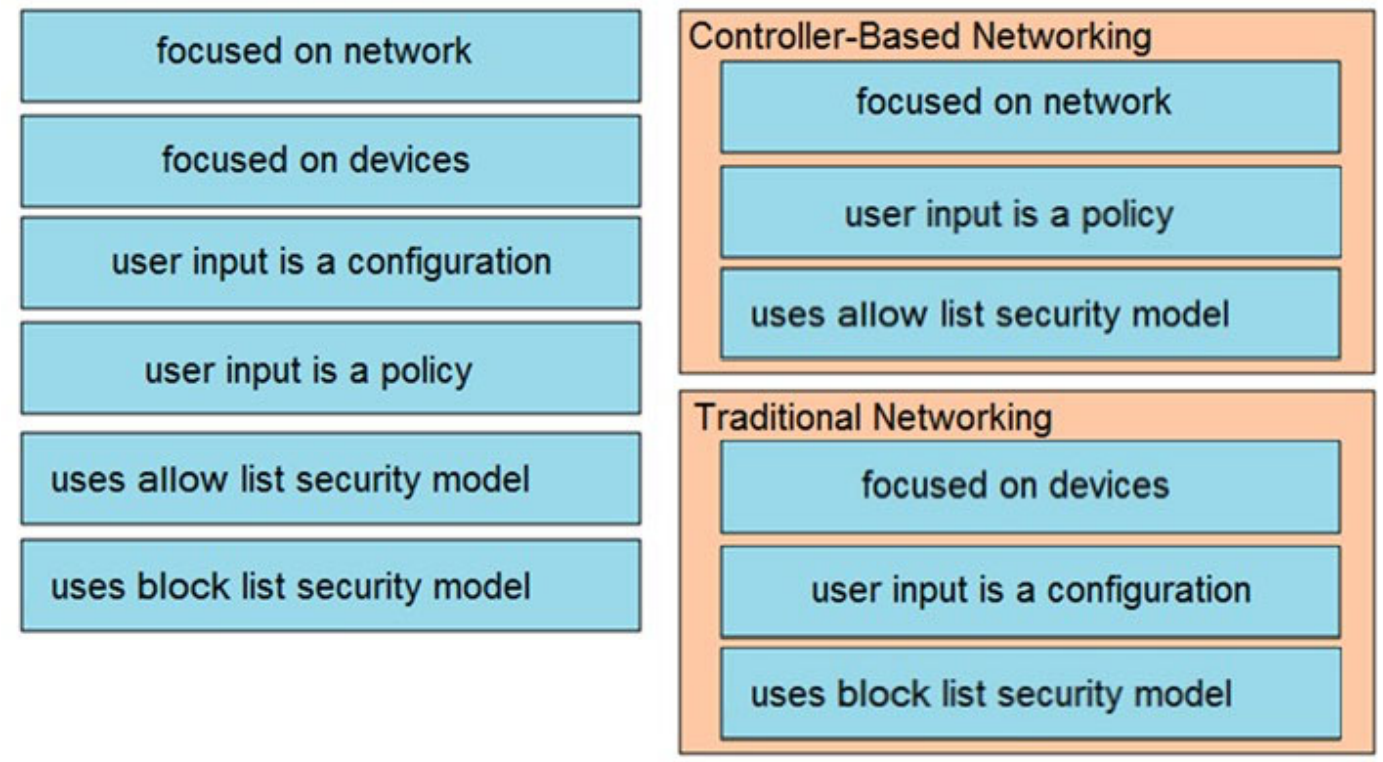
Select and Place:

Answer Area



Correct Answer:

Answer Area



cormorant Highly Voted 7 months ago

in short:
traditional networking: bad
controller-based networking: good

upvoted 8 times

RougePotatoe Most Recent 7 months, 1 week ago

Anyone have any idea on what they are referring to regarding the allow list and block list?

upvoted 4 times

Request7108 5 months, 1 week ago

Zero based trust is the new "way" and instead of starting where everything is allowed unless denied, zero trust starts with everything blocked and everything you want to allow has to be enabled.

upvoted 1 times

espandrews 2 weeks, 1 day ago

Isn't denying everything by default as traditional configuration ACLs have worked? I don't see any difference, so I'll call marketing bs.

upvoted 1 times

lolungos 1 week ago

Actually no, if you don't apply and ACL everything is open an available to pass (on cisco devices) and from default you don't have any ACLs created on the device, so default deployment is wide open to pass any traffic.

upvoted 2 times

Question #716 *Topic 1*

What are two fundamentals of virtualization? (Choose two.)

A. It allows logical network devices to move traffic between virtual machines and the rest of the physical network.

B. It allows multiple operating systems and applications to run independently on one physical server.

C. It allows a physical router to directly connect NICs from each virtual machine into the network.

D. It requires that some servers, virtual machines, and network gear reside on the Internet.

E. The environment must be configured with one hypervisor that serves solely as a network manager to monitor SNMP traffic.

Correct Answer: *AB*

Abdulaziz Highly Voted 2 years, 6 months ago

I am a VMware certified professional and the correct answer is A and B
Explanation:
A- Each virtualization solution have virtual switches (logical network), these virtual switches allows virtual machines to communicate on the network. We also assign vlan tag on these switches or make them trunk.
B) The main purpose of Server Virtualization is to run many VMs on the same physical server

upvoted 39 times

nathnotnut 3 months, 1 week ago

tell us that you're a reliable source without telling us you're a reliable source :))

upvoted 1 times

cdewet Highly Voted 2 years, 6 months ago

I do not agree that E is an option. Yes, a virtual environment cannot function without a hypervisor, but it's function is not to act solely as a network manager to monitor SNMP traffic.
Correct answer is AB

upvoted 34 times

ismatdmour Most Recent 1 year, 2 months ago

Selected Answer: AB

in C NICs are not part of VMs. Virtual switches of VMs are what connect vitrual NICs of VMs to physical network (say a router). C is incorrect. Virtulization is not having the netgear or part of it in the Internet (This is cloud IaaS) but to have the physical server shared by mutiple virtulized servers. However, we can have virtulized netgear in the Cloud. D is incorrect. Hypervisor manages physical server hardware (not software like SNMP). E is incorrect. A and B are answers.

upvoted 1 times

Vinarino 1 year, 4 months ago

Ya don't mandate a physical net, nor SNMP in virtual environment...
SNMP can be fully configured on an ESXi hypervisor through the ESX CLI. The commands vary between different versions of ESXi. To gather more valuable and accurate data from your virtual environment, it's highly recommended you have VMware Tools installed on each VM.

upvoted 1 times

Vinarino 1 year, 5 months ago

A classified forensic net has 1 physical connection to RDP in. Thus, to communication / move data to/from physical networks can be moot, plus a security breach.
SNMP makes no typical common sense, thus probably correct

upvoted 1 times

promaster 1 year, 11 months ago

AB are true and therefore correct, E is not true because the hypervisor is not about using SNMP.

upvoted 2 times

Zerotime0 2 years, 5 months ago

Right tricky one,for someone who memorized answers to questions and mainly remembers hypervisor=virtualization. Here in E it mentions but limits to “solely” .rule it out . Aand B as previously stated.careful reading is key.

upvoted 5 times

bestboy120 2 years, 5 months ago

Read the whole answear "The environment must be configured with one hypervisor that serves solely as a network manager to monitor SNMP traffic."
just becouse there is a word "hyperhivsor" itd doesnt mean its this
U dont need to configured anything with menager to monitor SNMP traffic

upvoted 4 times

Whippy29 2 years, 8 months ago

How could A not be correct, think about Hyper-V and others, logical switches between VM's which can also interface with physical network

upvoted 4 times

Ebenezer 2 years, 8 months ago

The correct answers are B and E. You can not talk about virtualization without talking about hypervisors.

upvoted 3 times

omsh 2 years, 9 months ago

yes the answer is BE

upvoted 3 times

ozy 2 years, 9 months ago

Correct answer BE

upvoted 3 times

dave1992 1 year, 7 months ago

hypervisor manages the NIC, RAM, and CPU. not the software. E is not the answer.

upvoted 2 times

Question #717 *Topic 1*

How does Cisco DNA Center gather data from the network?

A. Devices use the call-home protocol to periodically send data to the controller

B. Devices establish an IPsec tunnel to exchange data with the controller

C. The Cisco CLI Analyzer tool gathers data from each licensed network device and streams it to the controller

D. Network devices use different services like SNMP, syslog, and streaming telemetry to send data to the controller

Correct Answer: *D*

ccna_goat Highly Voted 8 months, 1 week ago

how am i supposed to know that? not mentioned in any course and even in OCG. all i can do here is wild guess.

upvoted 11 times

dicksonpwc Highly Voted 1 year, 9 months ago

D is correct.

Explanation:

Local Network Telemetry: Cisco DNA Center collects data from several different sources and protocols on the local network, including the following: traceroute; syslog; NetFlow; Authentication, Authorization, and Accounting (AAA); routers; Dynamic Host Configuration Protocol (DHCP); Telnet; wireless devices; Command-Line Interface (CLI); Object IDs (OIDs); IP SLA; DNS; ping; Simple Network Management Protocol (SNMP); IP Address Management (IPAM); MIB; Cisco Connected Mobile Experiences (CMX); and AppDynamics ®. The great breadth and depth of data collection allows Cisco DNA Center to give a clearer picture of the state of the network, clients, and applications. This data is kept on the Cisco DNA Center appliance locally (at your location) and is available for a period of 14 days. Local Network Telemetry is not transported to any other server nor is it sent to the cloud.

https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-faq-cte-en.html

upvoted 7 times

Ciscoman021 Most Recent 2 months, 2 weeks ago

Selected Answer: D

D. Network devices use different services like SNMP, syslog, and streaming telemetry to send data to the controller.

Cisco DNA Center uses various methods to gather data from the network devices, such as SNMP, syslog, and streaming telemetry. These protocols allow the devices to send data to the controller in real-time or at regular intervals, providing comprehensive visibility into the network. The data collected by Cisco DNA Center is then analyzed and used for network management, troubleshooting, and optimization.

upvoted 1 times

papibarbu 4 months, 2 weeks ago

D is correct. Explanation: Local Network Telemetry: Cisco DNA Center collects data from several different sources and protocols on the local network, including the following: traceroute; syslog; NetFlow; Authentication, Authorization, and Accounting (AAA); routers; Dynamic Host Configuration Protocol (DHCP); Telnet; wireless devices; Command-Line Interface (CLI); Object IDs (OIDs); IP SLA; DNS; ping; Simple Network Management Protocol (SNMP); IP Address Management (IPAM); MIB; Cisco Connected Mobile Experiences (CMX); and AppDynamics ®. The great breadth and depth of data collection allows Cisco DNA Center to give a clearer picture of the state of the network, clients, and applications. This data is kept on the Cisco DNA Center appliance locally (at your location) and is available for a period of 14 days. Local Network Telemetry is not transported to any other server nor is it sent to the cloud. https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-faq-cte-en.html

upvoted 1 times

karels94 7 months, 2 weeks ago

D is correct.

Explanation:

Local Network Telemetry: Cisco DNA Center collects data from several different sources and protocols on the local network, including the following: traceroute; syslog; NetFlow; Authentication, Authorization, and Accounting (AAA); routers; Dynamic Host Configuration Protocol (DHCP); Telnet; wireless devices; Command-Line Interface (CLI); Object IDs (OIDs); IP SLA; DNS; ping; Simple Network Management Protocol (SNMP); IP Address Management (IPAM); MIB; Cisco Connected Mobile Experiences (CMX); and AppDynamics ®. The great breadth and depth of data collection allows Cisco DNA Center to give a clearer picture of the state of the network, clients, and applications. This data is kept on the Cisco DNA Center appliance locally (at your location) and is available for a period of 14 days. Local Network Telemetry is not transported to any other server nor is it sent to the cloud.

https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-faq-cte-en.html

upvoted 1 times

Question #718 *Topic 1*

Which statement compares traditional networks and controller-based networks?

A. Only controller-based networks decouple the control plane and the data plane.

B. Traditional and controller-based networks abstract policies from device configurations.

C. Only traditional networks natively support centralized management.

D. Only traditional networks offer a centralized control plane.

Correct Answer: *A*
Most traditional devices use a distributed architecture, in which each control plane is resided in a networking device. Therefore, they need to communicate with each other via messages to work correctly.
In contrast to distributed architecture, centralized (or controller-based) architectures centralizes the control of networking devices into one device, called SDN controller.

LeGrosMatou Highly Voted 2 years, 3 months ago
Funny how many questions are about the advantages of a DNA Centrer over a traditional network ^^ Good marketing Cisco
upvoted 18 times

dicksonpwc Most Recent 1 year, 9 months ago
A is correct.
Explanation:
In traditional network architecture, the control plane and data plane are integrated. Any changes to the system are dependent upon configuring physical network devices, the protocols, and software they support. You can perform only limited changes to the overall system as the network devices bottleneck logical network traffic flows. Devices function autonomously and offer limited logical awareness toward the wider network.

In contrast, SDN decouples the Control Plane from the Data Plane and centrally integrates the network logic at the controller level. A controller separated between the two Planes logically centralizes the network intelligence such that users can choose which programmable features to move from network devices onto the application server or controller.

https://www.bmc.com/blogs/software-defined-networking/#
upvoted 4 times

Talloo 2 years, 3 months ago
I think it's C because Controller-based decouple control plane, not data plane
upvoted 2 times

lordnano 2 years, 2 months ago
Please reread answer C. Centralized Management is definitely not a strength of traditional networks...
And Controller-based decouple control plane and data plane from a single device. So A is the only one that makes sense.
upvoted 4 times

il_pelato_di_casalbruciato 2 years, 1 month ago
t'ha detto tutto lui
upvoted 2 times

studying_1 1 week, 2 days ago
hai ragione, lol non parlo bene italiano e espagnolo, ma capisco poco,non c'e problema, parlo solo francese e inglese
upvoted 1 times

XBfoundX 2 years, 5 months ago
The only one that is correct is the A. Because only a Controller Based Network have The Data Plane and Control Plane that are separated from a unique "brain entity".
upvoted 3 times

Question #719 *Topic 1*

What are two benefits of network automation? (Choose two.)

A. reduced hardware footprint

B. reduced operational costs

C. faster changes with more reliable results

D. fewer network failures

E. increased network security

Correct Answer: *BC*

dcouch Highly Voted 2 years, 7 months ago

Could literally say any of those answers

upvoted 11 times

yewastedmytime 2 years, 6 months ago

Several of those answers are right, but not the 'most-right', A is not correct though. Automation doesn't reduce your hardware footprint at all, if anything it does quite the opposite.

upvoted 5 times

Request7108 Most Recent 5 months, 1 week ago

Selected Answer: BC

B and C seem to have the most Cisco Kool-Aid poured into them, although E is definitely up there for me as well.

upvoted 1 times

splashy 8 months, 2 weeks ago

Selected Answer: BC

https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/network-automation-strategy-wp.html#BenefitsofNetworkAutomation

Security is a higher level of automation and falls under "security automation" and a ssuch is not one of the primary benefits of network automation. Faster, cheaper and more reliable deployment are your first candidates.

upvoted 3 times

Tylosh 8 months, 2 weeks ago

Selected Answer: CE

I think misconfiguration is one of the biggest downside of traditional network , so automation did increase the security of network

upvoted 2 times

sasquatchshrimp 10 months ago

Selected Answer: CE

Going with C and E, a common security issue is misconfiguration, if you are using network automation, the chances of misconfiguration drops, thus increasing security by avoid security misconfigurations.

upvoted 1 times

ismatdmour 1 year, 2 months ago

Selected Answer: BC

Ans. is B: op. cost is reduced due to automation of configuration, IOS update and group deployment of policies
Ans.2 is C: You can auto configure new device(s) based on their type/function which is more reliable than human configuration which is prone to errors.
D. is incorrect, the network devices and interconnections remain prone to failures. Automation ensure error free configuration/policy deployment/...etc and not that devices have less failures.
E. Security in traditional networks or controller networks is dependent on security configuration (either configured per device or automated).

upvoted 2 times

KyleP 2 years, 10 months ago

How does it reduce operational cost ?

upvoted 3 times

chomjosh 2 years, 10 months ago

Multiple processes are carried out from simple automation, delivering results in a timely and cost effective manner. Operational cost is therefore reduced.

upvoted 9 times

chomjosh 2 years, 10 months ago

Multiple processes is carried out from simple automation, delivering results in a timely and cost effective manner. Operational cost is therefore reduced.

upvoted 9 times

Question #720 *Topic 1*

Which two encoding methods are supported by REST APIs? (Choose two.)

A. SGML

B. YAML

C. XML

D. JSON

E. EBCDIC

Correct Answer: *CD*
The Application Policy Infrastructure Controller (APIC) REST API is a programmatic interface that uses REST architecture. The API accepts and returns HTTP
(not enabled by default) or HTTPS messages that contain JavaScript Object Notation (JSON) or Extensible Markup Language (XML) documents.
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/rest_cfg/2_1_x/b_Cisco_APIC_REST_API_Configuration_Guide/b_Cisco_APIC_REST_API_Configuration_Guide_chapter_01.html

ataraxium Highly Voted 2 years, 9 months ago
JSON, XML = REST API
YAML = Ansible
upvoted 18 times

lordnano 2 years, 2 months ago
YAML is used in Ansible but you wouldn't say "= Ansible".
Actually the whole question is strange as also boghota shoed. It underlines a bit Ciscos conservative network background.
upvoted 1 times

boghota Highly Voted 2 years, 6 months ago
"Unlike SOAP-based web services, there is no "official" standard for RESTful web APIs. This is because REST is an architectural style, while SOAP is a protocol. REST is not a standard in itself, but RESTful implementations make use of standards, such as HTTP, URI, JSON, and XML." - Wikipedia

REST = REpresentational State Transfer (it can use XML, JSON and some other but JSON is the most popular choice)
SOAP = Simple Object Access Protocol (uses XML for all messages)
API = Application Programming Interface

https://www.soapui.org/learn/api/soap-vs-rest-api/
https://en.wikipedia.org/wiki/Representational_state_transfer
upvoted 5 times

Ciscoman021 Most Recent 2 months, 1 week ago
Selected Answer: CD
The two encoding methods that are supported by REST APIs are:

C. XML
D. JSON
upvoted 1 times

ZayaB 2 years, 3 months ago
Here is the broken link: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/rest_cfg/2_1_x/b_Cisco_APIC_REST_API_Configuration_Guide/b_Cisco_APIC_REST_API_Configuration_Guide_chapter_01.html
upvoted 3 times

mikexb 2 years, 11 months ago
Reference link is broken...
upvoted 1 times

ponder 2 years, 11 months ago
https://community.cisco.com/t5/nso-developer-hub-documents/rest-api-basics/ta-p/3635342
upvoted 1 times

Question #721 *Topic 1*

What are two characteristics of a controller-based network? (Choose two.)

A. It uses Telnet to report system issues.

B. The administrator can make configuration updates from the CLI.

C. It uses northbound and southbound APIs to communicate between architectural layers.

D. It decentralizes the control plane, which allows each device to make its own forwarding decisions.

E. It moves the control plane to a central point.

Correct Answer: *CE*

alexiro Highly Voted 2 years, 9 months ago

controller-based networking A style of building computer networks that use a controller that centralizes some features and provides application programming interfaces (APIs) that allow for software interactions between applications and the controller (northbound APIs) and between the controller and the network devices (southbound APIs).

centralized control plane An approach to architecting network protocols and products that places the control plane functions into a centralized function rather than distributing the function across the networking devices.

upvoted 11 times

Question #722 *Topic 1*

Which output displays a JSON data representation?

A.

```
{
  "response": {
  "taskId": {};
  "url": "string"
  };
  "version": "string"
}
```

B.

```
{
  "response"- {
  "taskId"- {},
  "url"- "string"
  },
  "version"- "string"
}
```

C.

```
{
  "response": {
  "taskId": {},
  "url": "string"
  },
  "version": "string"
}
```

D.

```
{
  "response", {
  "taskId", {};
  "url", "string"
  };
  "version", "string"
}
```

Correct Answer: *C*

JSON data is written as name/value pairs.

A name/value pair consists of a field name (in double quotes), followed by a colon, followed by a value:

ג€nameג:€ג€Markג€

JSON can use arrays. Array values must be of type string, number, object, array, boolean or null. For example:

{

ג€nameג:€ג€Johnג€,

ג€age30:€ג,

ג€carsג€:[ג€Fordג ,€ג€BMWג ,€ג€Fiatג€]

}

JSON can have empty object like ג€taskIdג€:{}

distortion Highly Voted 1 year, 11 months ago

The layout is not great. But watch out for the : after the "response": part. and a , after each line.

upvoted 7 times

i_am_confused Highly Voted 11 months, 3 weeks ago

Answer is C. JSON uses { [: ,
JSON does NOT use - ;

upvoted 6 times

dave1992 Most Recent 1 year, 5 months ago

If you had a hard time. Look at the end between the " ___" it should be a colon. Not a - ;

upvoted 1 times

mrsiafu 2 years, 1 month ago

This is a terrible representation... the layout that is

upvoted 3 times

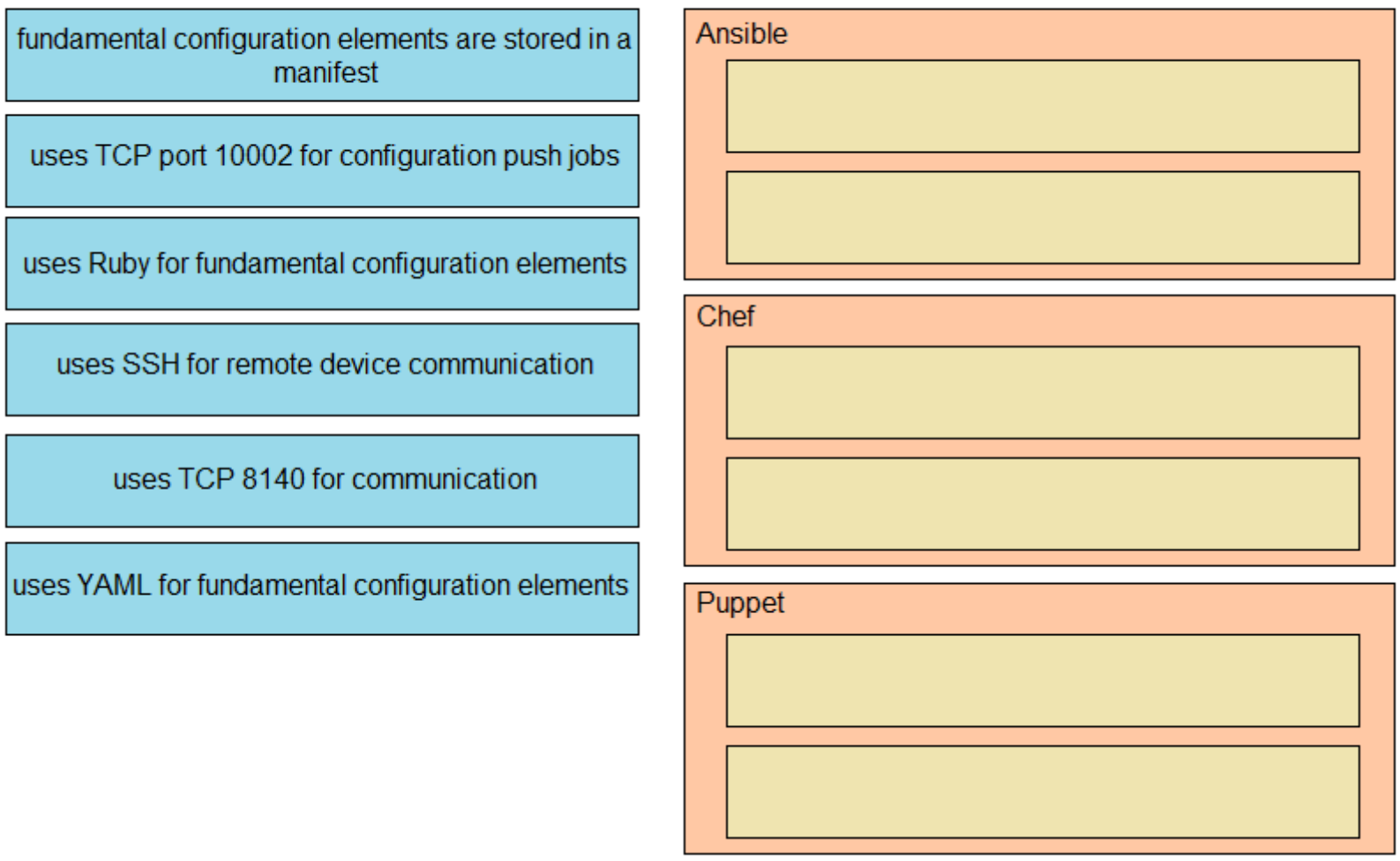
Question #723 *Topic 1*

DRAG DROP -

Drag and drop the descriptions from the left onto the configuration-management technologies on the right.

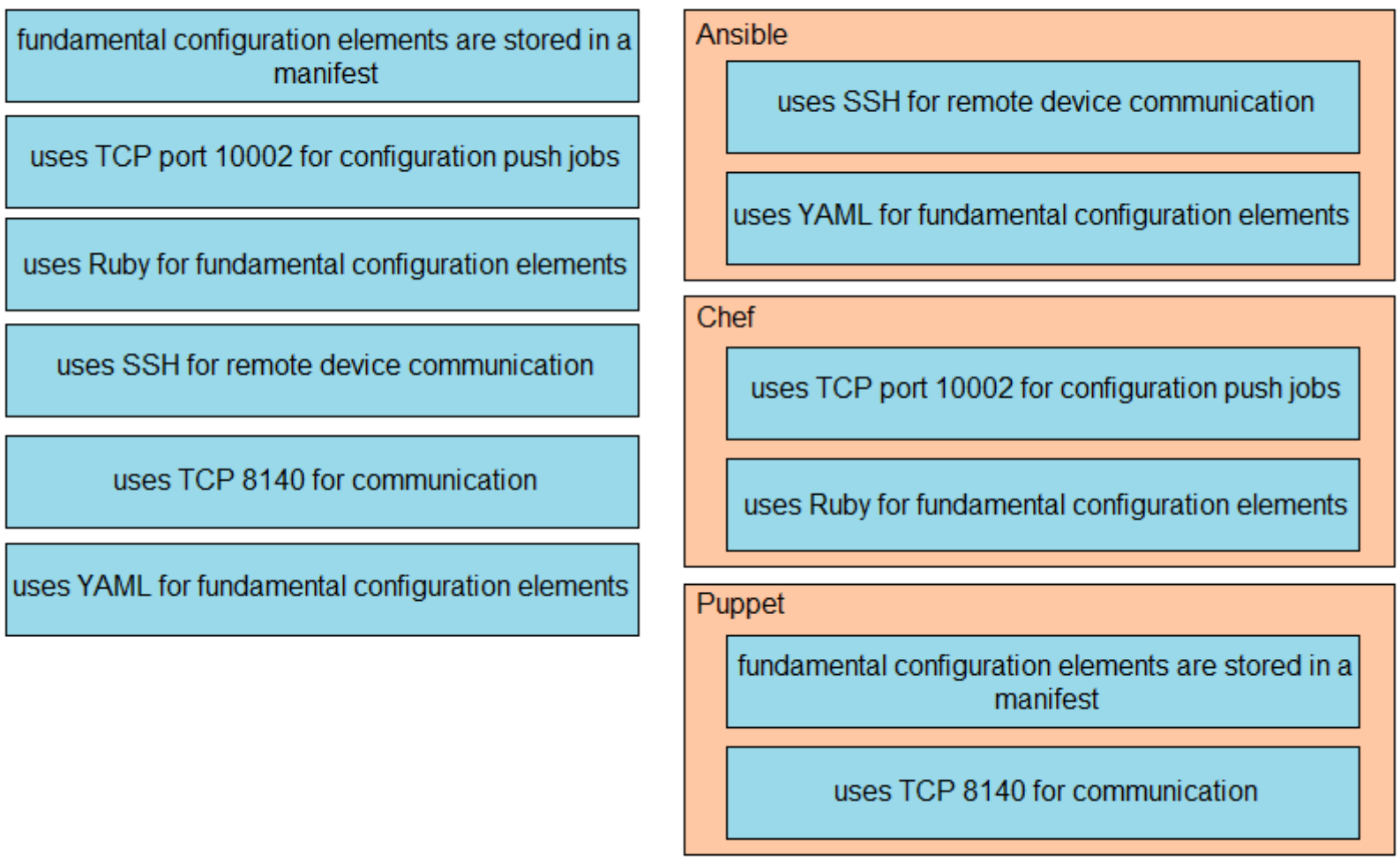
Select and Place:

Answer Area



Correct Answer:

Answer Area



The focus of Ansible is to be streamlined and fast, and to require no node agent installation. Thus, Ansible performs all functions over SSH.

Ansible is built on

Python, in contrast to the Ruby foundation of Puppet and Chef.

TCP port 10002 is the command port. It may be configured in the Chef Push Jobs configuration file . This port allows Chef Push Jobs clients to communicate with the Chef Push Jobs server.

Puppet is an open-source configuration management solution, which is built with Ruby and offers custom Domain Specific Language (DSL) and