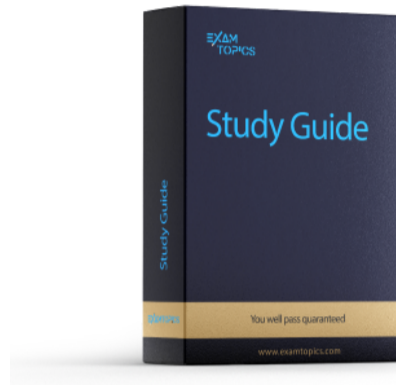


Prepare for your 200-301 exam with additional products



Study Guide

1969 PDF Pages

\$19.99

Buy Now

[Custom View Settings](#)

Question #500

Topic 1

What are two benefits of FHRPs? (Choose two.)

- A. They allow encrypted traffic
- B. They prevent loops in the Layer 2 network.
- C. They are able to bundle multiple ports to increase bandwidth
- D. They enable automatic failover of the default gateway
- E. They allow multiple devices to serve as a single virtual gateway for clients in the network

Correct Answer: *DE*

 **papibarbu** 8 months, 2 weeks ago

yes my man
upvoted 3 times

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 11 months, 1 week 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 8 times

 **Nawaf1** Highly Voted 11 months, 1 week ago

so now I need to memorize mac addresses!!?
this is absurd
upvoted 5 times

 **guisam** Most Recent 9 months, 1 week ago

<https://www.fingerinthenet.com/fhrp-introduction/>
upvoted 1 times

 **Customexit** 11 months 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 2 times

 **Garfieldcat** 11 months, 1 week ago

Selected Answer: B

I can remember this time I retry this question
upvoted 1 times

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 (63%)

B (37%)

 **RougePotatoe** Highly Voted 10 months, 3 weeks 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 7 times

 **bikila123** 1 month ago

The question is about multi vendor which means its not a cisco proprietary. but not how vrrp works ! correct me if am wrong
upvoted 1 times


 **rogi2023** Highly Voted 4 months, 3 weeks ago

Selected Answer: B

If I hit this question I will go for "B" - multivendor, just keep it simply
upvoted 5 times

 **shumps** Most Recent 18 hours, 34 minutes ago

its not cisco proprietary so B more relevant, D all FHRP do that's their main reason
upvoted 1 times

 **Yinxs** 3 weeks, 5 days ago

Selected Answer: B

It is a bad question. But the keyword is multivendor, and Cisco has some extra features like VRRP Object Tracking Integration. Maybe it is not specific to a security feature, but Cisco indeed have some enhancement based on standard VRRP.
For answer D: the issue is the word "member", member of router or member of the new subnet, I don't know.
upvoted 1 times

 **shefo1** 3 months ago

Selected Answer: D

chatGPT answer

The correct answer is D. To enable normal operations to continue after a member failure without requiring a change in a host ARP cache.

VRRP (Virtual Router Redundancy Protocol) is a standardized protocol that provides a way to create a virtual gateway IP address in a multivendor environment. It allows multiple routers to work together, sharing the same virtual IP address as the default gateway for hosts on a subnet.

When a new subnet is configured in a multivendor environment, implementing VRRP provides redundancy and fault tolerance for the default gateway. If one router fails, another router within the VRRP group can take over the virtual IP address seamlessly, ensuring that hosts can still communicate without any disruption. This capability allows normal operations to continue after a member failure without requiring a change in a host ARP (Address Resolution Protocol) cache.

upvoted 1 times

 **Isuzu** 3 months, 1 week 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** 4 months, 2 weeks ago

I think the second part is because CDP is not enabled to work by default when VRRP is used
upvoted 1 times

🗨️ 👤 **andresugiharto** 6 months 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** 7 months ago

D for 100%

upvoted 2 times

🗨️ 👤 **Anas_Ahmad** 8 months, 2 weeks 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** 10 months ago

Selected Answer: D

VRRP does not provide additional security features for Cisco devices.

When VRRP is implemented the virtual mac-address 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** 11 months, 1 week ago

Selected Answer: B

answer b

upvoted 1 times

🗨️ 👤 **RougePotatoe** 10 months, 3 weeks 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 5 times



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%)

  **mda2h** 1 month, 3 weeks ago


Selected Answer: B

- A. Wrong, it's DHCP that allows the auto discovery of (virtual) gateways, not VRRP
 - C. Wrong, no weighting scheme is used between the gateways in the VRRP group. Active-passive scheme only
 - D. Wrong, with VRRP users do not detect failure. If one GW fails, another one seamlessly takes up the role
- upvoted 2 times

  **Chopaka** 2 months, 2 weeks ago

Why not C? Like I don't see a reason to provide a virtual ip adres to de endusers....

upvoted 2 times

  **Chopaka** 2 months, 2 weeks ago

Why not C?

upvoted 2 times

  **ismail23** 4 months, 1 week ago

Selected Answer: B

B is right

upvoted 1 times

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

Community vote distribution

B (100%)

  **[Removed]** 2 months, 3 weeks ago

Selected Answer: B

Given answer is correct

upvoted 1 times

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 11 months, 3 weeks 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 12 times

 **zez** Most Recent 4 months, 1 week 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

 **dropspablo** 1 month, 2 weeks ago

Answer correct is "D".

VMAC

VRRP = 0000.5E00.01XX (XX = GROUP ID)

HSRP V1 = 0000.0C07.ACXX (XX = GROUP ID)

HSRP V2 = 0000.0C9F.FXXX (XXX = GROUP ID)

GLBP = 0007.B400.XXYY (XX = GROUP ID) (YY = AVF ID)

D. 00:00:0c:07:ac:0e (group 14 = "e" in hexadecimal)
upvoted 1 times

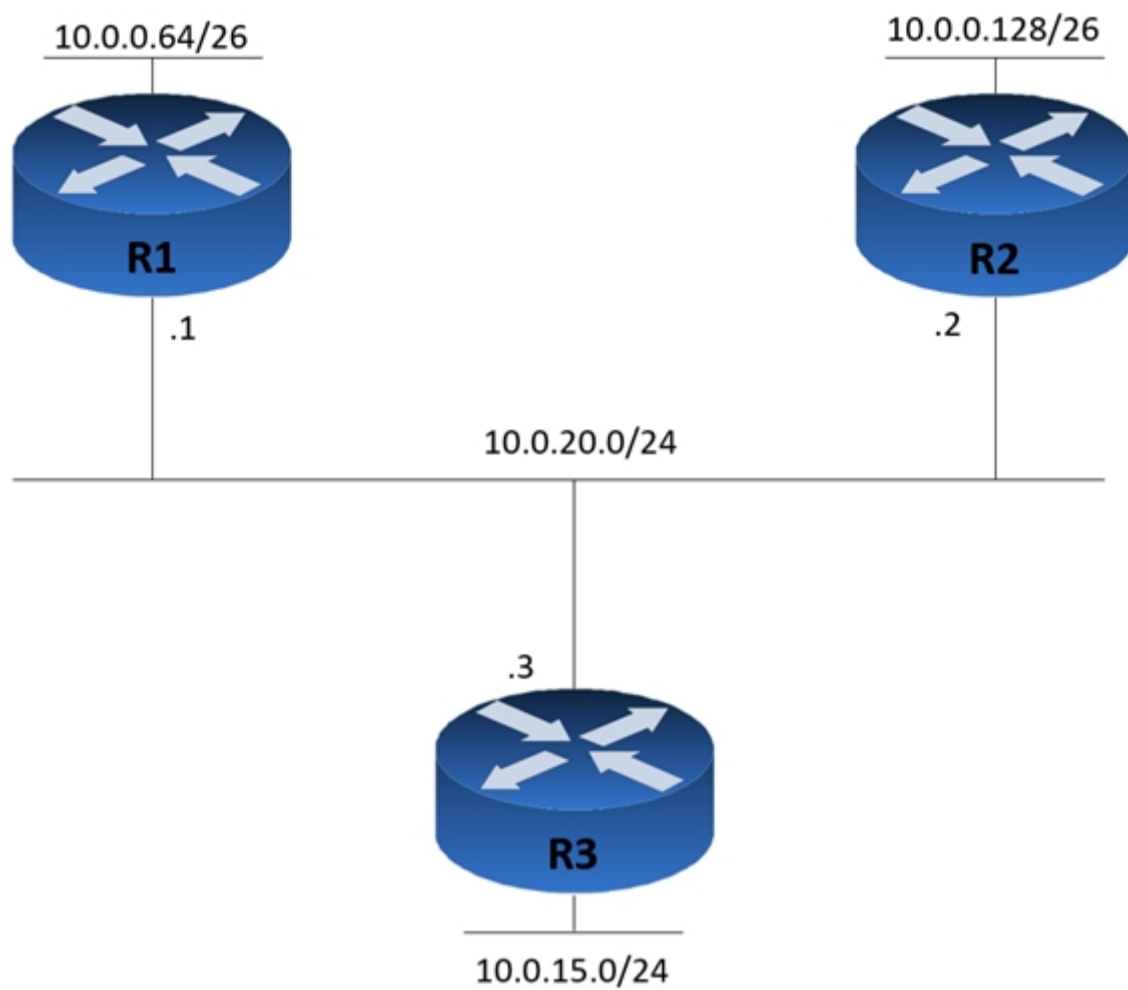
 **Hope_12** 4 months, 1 week ago

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 2 times



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).

jayjhaekim 3 months, 2 weeks 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 10 months ago

Why is A not the correct answer? - Can anyone help
 upvoted 3 times

Surves 9 months, 4 weeks ago

Because the destination network is 10.0.15.0/24 and not 10.0.0.64
 upvoted 3 times

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.

Community vote distribution

D (92%)

8%

 **RougePotatoe** Highly Voted 10 months, 3 weeks ago

Selected Answer: D


D is the only one that makes any sense yet I hate it.
upvoted 12 times

 **melmiosis** 10 months, 2 weeks ago

i know the feeling. im glad im close at least to ending this bs hehe
upvoted 6 times

 **joseangelatm** Highly Voted 8 months, 2 weeks ago

No metric election?
upvoted 5 times

 **xbololi** 2 months, 1 week ago

This selection is the last resort... It is almost impossible to have this kind of case... But thanks to cisco we need to know this sh.t
upvoted 2 times

 **wakaish** Most Recent 21 hours, 16 minutes ago


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

Administrative distance takes precedence over factors like the age of the route or the MAC address of the next hop. It is used to prioritize routes when there are multiple paths to the same destination, allowing the router to select the most appropriate route based on administrative distance values

upvoted 1 times

 **john1247** 3 months, 2 weeks ago

Why is B not the right answer?
upvoted 1 times

 **Sdiego** 7 months, 3 weeks ago

Selected Answer: A

A is correct
upvoted 1 times

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

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, 8 months ago

Correct Answer. Source:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/xr-16-6/sla-xr-16-6-book/sla-udp-jitter.html>
upvoted 14 times

 **Ali526** 2 years, 7 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 19 times

 **Stonetales987** 1 year, 10 months ago

Control F "measure" :)

upvoted 6 times

 **zaid** 2 years, 6 months ago

Right :)

upvoted 2 times

 **Samuelpn96** 2 years 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 8 months, 1 week 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 7 times

 **Liquid_May** Most Recent 3 weeks, 4 days ago

Is this required for the 200-301 exam? I don't remember seeing this topic covered on my netacad online course. Thanks

upvoted 1 times

 **Sam7007** 2 months ago

The correct answer is B. EEM (Embedded Event Manager).

IP SLA (Internet Protocol Service Level Agreement) is a feature in Cisco IOS that allows network administrators to measure various network performance metrics. To measure UDP jitter using IP SLA, the EEM feature is required. EEM provides the necessary scripting capabilities to configure and monitor IP SLA operations, including the measurement of UDP jitter.


LLDP (Link Layer Discovery Protocol), CDP (Cisco Discovery Protocol), and NTP (Network Time Protocol) are not directly related to measuring UDP jitter using IP SLA. LLDP and CDP are network discovery protocols, while NTP is used for time synchronization in network devices.

upvoted 2 times

 **GigaGremlin** 11 months, 1 week ago

Selected Answer: C

OK,... so measurement need some time... ;-)
upvoted 2 times

 **ptfish** 1 year, 2 months 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, 4 months ago

D, NTP is the right protocol
upvoted 2 times

 **msae26** 1 year, 4 months 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, 3 months ago

I thought jitter is related to QOS (gold profile)
upvoted 2 times

 **vadiminski** 2 years, 4 months ago

Jitter has something to do with time, NTP synchronizes time, thus NTP the most likely
upvoted 4 times

 **chr** 2 years, 4 months 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, 4 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.
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** 9 months ago

it's a dynamic nat address pool
upvoted 2 times

 **Goh0503** 12 months ago

Answer is C
<https://www.practicalnetworking.net/stand-alone/cisco-nat-configurations-ios-router/>
upvoted 1 times

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** 5 months ago

A is correct
upvoted 2 times

  **Nnandes** 1 year, 4 months ago

Nat pool, A is correct
upvoted 4 times

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, 7 months ago

Packet tracer supports "transport input all", does not support "transport input telnet ssh".
upvoted 13 times

  **Dante_Dan** 1 year, 8 months ago

Actual routers and switches accept the "transport input telnet ssh" command.
Also, this is stated in the official cert guide.
upvoted 8 times

  **VictorCisco** 5 months, 3 weeks ago

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

```
SW4(config-line)#
```

upvoted 1 times

  **raydel92** Highly Voted 1 year, 9 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

  **Techpro30** Most Recent 1 month, 2 weeks ago

```
Router(config-line)#transport input ssh
```

% Invalid input detected at '^' marker.

```
Router(config-line)#transport input all
Router(config-line)#
```

upvoted 1 times

  **XuniLrve4** 2 months, 3 weeks ago

Packet Tracer is simply just good enough to learn most material, and not meant to replicate all commands of Cisco hardware, hence this situation is definitely an example!
upvoted 1 times

  **Nnandes** 1 year, 4 months ago

```
transport input telnet ssh
```

upvoted 2 times

  **sdokmak** 2 years, 2 months ago



what about privilege level 15?
upvoted 3 times

  **sdokmak** 2 years, 2 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, 5 months ago

A is true of course, but these questions are mindboggling, in terms of logic...the answer presumes that we have not configured neither ssh nor telnet, unlike the question...poor
upvoted 6 times

  **youtri** 2 years, 5 months ago



i think the question says that ssh is configured and what is the next step to configure Telnet

upvoted 4 times

  **aliwqa777** 2 years, 5 months ago

A is correct

upvoted 2 times

  **youtri** 2 years, 5 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, 5 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

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, 7 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, 9 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, 6 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 6 months, 2 weeks 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** 9 months, 1 week ago

THE (DHCP#) DEFAULT-ROUTER IS MISSING FROM THE EXHIBIT
upvoted 1 times

 **Nnandes** 1 year, 4 months ago

D. Configure the default gateway
upvoted 1 times

 **Nicocisco** 1 year, 6 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, 5 months ago



Correct, you can't input a subnet mask in CIDR notation as shown in this question.
upvoted 1 times

 **uevenasdf** 2 years, 8 months ago

D is more right but arguably A could be right too
upvoted 2 times

  **RougePotatoe** 10 months, 3 weeks 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 2 times

  **Cpynch** 1 year, 7 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, 8 months ago

Didn't know we had routers in 1198 lol
upvoted 40 times

  **wirlernenman** 2 years, 7 months ago

What a catch 😄
upvoted 13 times


  **Samuelpn96** Highly Voted 2 years 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, 4 months ago

I think A is correct, the address is removed from the pool.
upvoted 2 times

  **Nnandes** 1 year, 4 months ago

A. The address is removed from the pool until the conflict is resolved.
upvoted 1 times



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, 8 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

  **Taloo** 2 years, 7 months ago

Wrong, the pool parameter displays the DHCP pool available. The binding parameter lists addresses leased (binding) to clients
upvoted 19 times

  **dave1992** 1 year, 9 months ago

wrong. reread the question. you are confusing a lot of people
upvoted 1 times

  **no_blink404** Most Recent 2 months, 3 weeks ago

Show ip DHCP binding
upvoted 1 times

  **g_mindset** 1 year 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, 4 months ago



show ip dhcp binding is the right answer
upvoted 2 times

  **ProgSnob** 1 year, 9 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, 10 months ago

key word "Have been assigned" DHCP binding shows you exactly that
upvoted 4 times

  **krey** 1 year, 11 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** 2 years, 2 months ago

Answer is correct
upvoted 3 times



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



  **sasquatchshrimp** Highly Voted 1 year, 1 month 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 6 times



  **sasquatchshrimp** 1 year, 1 month ago
world, not work
upvoted 1 times

  **g_mindset** Most Recent 1 year ago
Selected Answer: A
A it is!
upvoted 1 times

  **Nebulise** 1 year, 8 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** 2 years ago
Is recursive search an authoritative source?
upvoted 1 times

  **kmb192006** 1 year, 12 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, 12 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

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, 9 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 14 times
```

 **Garfieldcat** Most Recent 11 months, 1 week 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, 11 months ago

i don't understand this question, can someone put it in simple words please?
upvoted 3 times

 **kadamske** 1 year, 11 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 8 times
```


 **raydel92** 1 year, 9 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 5 times

 **raydel92** 1 year, 9 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, 11 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, 11 months ago

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



upvoted 9 times

  **Shoeboxx** Most Recent  5 months ago

Selected Answer: A

100% A.

upvoted 1 times

  **ctoklu** 1 year, 2 months ago

A-Correct

B-Should be the DNS...

upvoted 1 times

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

  **Sim_James_27** Highly Voted 1 year, 9 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 6 times

  **kyleptt** 3 months, 1 week ago

thanks for this !

upvoted 1 times

  **Mozah** Highly Voted 1 year, 9 months ago

nslookup can support "D".

D and E are correct

upvoted 5 times

  **shakyak** Most Recent 1 year, 10 months ago

Can some one justify E?

upvoted 1 times

  **cocoto4** 1 year, 10 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 9 times

  **Dante_Dan** 1 year, 8 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 11 times

  **bootloader_jack** 2 years ago

is D correct?

upvoted 1 times

  **DaBest** 1 year, 11 months ago

D + E are correct

upvoted 2 times

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, 10 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 28 times
```

 **gewe** Most Recent 7 months ago

just test it in PT... answer is D
upvoted 1 times

 **cormorant** 9 months 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** 10 months, 3 weeks 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** 1 year, 2 months ago

the command is telling me "Address is determined by setup command" And dhcp is working fine in network
upvoted 1 times

 **AWSEMA** 1 year, 2 months 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, 10 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, 10 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, 12 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** 2 years ago

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

upvoted 1 times

  **Cisna** 1 year, 12 months ago

show ip int brief wont show you DHCP infor

upvoted 4 times

  **Nicocisco** 1 year, 6 months ago

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

upvoted 2 times

  **xdxp23** 2 years, 1 month 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

  **AlexPIh** 2 years, 1 month 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** 2 years, 2 months ago

what about B?

upvoted 1 times

  **bwg** 2 years, 3 months ago


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

upvoted 2 times

  **kadamske** 1 year, 11 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, 12 months ago

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

upvoted 4 times

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, 4 months ago

A good way to memorize: Ernie Always Cries Even When Noone Is Dying
upvoted 16 times

 **dipanjana1990** 1 year, 1 month ago

how about "(E)VERY (A)WESOME (C)ISCO (E)NGINEER (W)ILL (N)EED (I)CE-CREAM (D)AILY" !!!
upvoted 13 times

 **ProgSnob** 1 year, 9 months ago

I use my own mnemonic devices but whatever works for a person is what matters.
upvoted 1 times

 **Liuka_92** 1 year, 3 months ago

it helped me
upvoted 2 times

 **Belinda** 1 year, 6 months ago

Thanks
upvoted 1 times

 **lordnano** Highly Voted 2 years, 6 months ago

B is not correct since the question talks about "logging trap debug".
C is the right answers:

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

 **Tarek70** Most Recent 3 months ago

0 emergency
1 alert
2 critical
3 error
4 warning
5 notification
6 information
7 debugging
upvoted 1 times


 **Tera_911** 1 year, 4 months ago

One more mnemonic - Every Awesome Cisco Engineer Will Need IceCream Daily
upvoted 8 times

 **LingLingW** 1 year, 8 months ago

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

upvoted 5 times

  **promaster** 2 years, 3 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, 4 months 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, 6 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, 9 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, 6 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



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, 7 months ago

Every Awesome Cisco Engineer Will Need Icecream Daily (L0-7)
upvoted 65 times

  **frejus** 2 years, 6 months ago

that's awesome thanks you
upvoted 9 times

  **S_10** Highly Voted 2 years, 1 month 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, 6 months ago

The answer is Emergency, Alert, and Critical but alert is not an option.
upvoted 6 times

  **SasithCCNA** 2 years, 6 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 25 times

  **kyleptt** 1 month, 2 weeks ago

I need to verify this I am thinking if you send logging trap 3 I think this means 4,5,6& 7 will be logged to the machine.
upvoted 1 times

  **SasithCCNA** 2 years, 6 months ago

Oops sorry what you have said is correct my bad . I didn't clearly read your answer.
upvoted 6 times

DRAG DROP -

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

Select and Place:

Answer Area

- FTP
- SMTP
- SNMP
- SSH
- TFTP
- VoIP

Connection Oriented

Connectionless

Correct Answer:

Answer Area

- FTP
- SMTP
- SNMP
- SSH
- TFTP
- VoIP

Connection Oriented

FTP

SMTP

SSH

Connectionless

SNMP

TFTP

VoIP

- 🗨️ **vadiminski** Highly Voted 👍 2 years, 4 months ago
 Correct answer, they ask which use TCP and which UDP
 upvoted 11 times
- 🗨️ **martialstriker09** Most Recent 🕒 1 year, 2 months ago
 TCP vs UDP lol
 upvoted 2 times

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:

⌘ An SNMP manager

⌘ An SNMP agent

⌘ 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, 11 months ago

be aware. If you are using SNMP, it will change all configs to those devices. answer B is right.
upvoted 6 times

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 `ip address dhcp`.

Note: The command `ip helper-address` enables a router to become a DHCP Relay Agent.

  **akhuseyinoglu** Highly Voted 3 years, 4 months ago

Correct Answer : A
upvoted 21 times

  **TeeltUp** 3 years, 4 months 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** 3 years, 2 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** 3 years, 1 month 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 configured before ip address dhcp to be able to configured.
upvoted 3 times

  **jjkcoins** 3 years, 1 month 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, 3 months 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** 3 years, 2 months ago

Agree, this is the answer that makes more sense
upvoted 2 times

  **kyleptt** Most Recent 1 month, 2 weeks ago

Definitely A but need to read this well lol
upvoted 1 times

  **Rob2000** 1 year, 11 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, 9 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, 9 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, 10 months ago

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

upvoted 4 times

 **boghota** 2 years, 10 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, 10 months ago

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

upvoted 5 times

 **altiit** 2 years, 10 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, 10 months ago

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

upvoted 2 times

  **GodUsopp** 2 years, 10 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, 11 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, 11 months ago

Correct answer is A straight from the cisco site.

upvoted 2 times

  **kimi7** 2 years, 11 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, 11 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, 11 months ago

Correct answer is indeed A

upvoted 3 times

  **Ebenezer** 2 years, 11 months ago

This answer is wrong. The correct answer is A.

upvoted 2 times

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, 5 months ago

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

A is correct

upvoted 7 times

  **no_blink404** Most Recent  2 months, 3 weeks ago

A is correct

upvoted 1 times

  **dicksonpwc** 2 years 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

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 3 years, 1 month 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 18 times

 **Isuzu** 3 months, 1 week ago

Best way to remember the answer... thank you

upvoted 3 times

 **mutlumesut** Most Recent 10 months, 2 weeks ago

why c is not correct?

upvoted 1 times

 **cormorant** 10 months, 2 weeks 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, 3 months ago

Selected Answer: BD

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

upvoted 4 times

 **Adaya** 2 years, 2 months ago

E almost catch me

upvoted 4 times

 **m_magdi** 2 years, 5 months ago

E why not

upvoted 2 times

 **ajajajaj** 2 years, 5 months ago

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

upvoted 3 times

 **LTTAM** 2 years, 8 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** 2 years ago

Your right, in fact. Is important read the question with patient 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 questions ready

upvoted 3 times

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, 11 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 22 times

  **Scipions** Highly Voted 2 years, 4 months ago

mannaggia al netacad

upvoted 11 times

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

  **IxlJustinIxI** Highly Voted 2 years, 4 months 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 27 times

  **BooleanPizza** 2 years ago

Every Awesome Cisco Engineer Will Need Ice Cream Daily :)
 upvoted 23 times

  **Alvaro13** 1 year, 1 month ago

From Jeremy It Lab
 upvoted 8 times

  **chr** Highly Voted 2 years, 4 months 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 5 months, 3 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, 6 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** 2 years, 1 month ago

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

  **Ahhmedd** 3 years, 2 months ago

WY not C
 upvoted 3 times

  **Chipapo** 3 years, 1 month ago

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

🗨️ 👤 **frejus** 2 years, 6 months ago

lol funny

upvoted 1 times

🗨️ 👤 **SasithCCNA** 2 years, 5 months ago

is it though

upvoted 1 times

🗨️ 👤 **Samuelpn96** 2 years ago

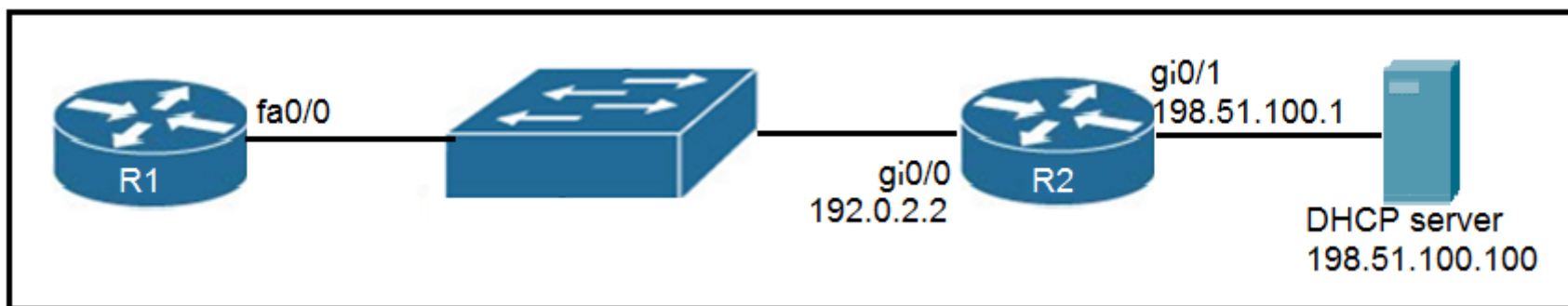
But aren't Extended ACLs filtering in a router a layer 4 operation?

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



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, 7 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 inside interface, ip helper-address 192.168.100.100 (dhcp server). Answers are B and C.

upvoted 26 times

kyleptt Most Recent 6 days, 15 hours ago

Is it that you can only have one helper address ?

upvoted 1 times

kyleptt 6 days, 15 hours ago

I will lab this up and see

upvoted 1 times

BettoAtzeni 1 month, 2 weeks ago

BC are correct

With these configurations in place:

1. R1, connected to the switch, will send out a DHCP request on its Fa0/0 interface.
2. R2's Gi0/0 interface, acting as a DHCP relay-agent, will receive the DHCP request.
3. R2 will forward the DHCP request to the DHCP server at IP address 198.51.100.100 (connected to R2's Gi0/1 interface).
4. The DHCP server will process the request and offer an IP address to R1.
5. R2 will relay the DHCP offer back to R1 through its Gi0/0 interface.
6. R1 will accept the DHCP offer and configure its Fa0/0 interface with the offered IP address.

In summary, by configuring R2's Gi0/0 interface as a DHCP relay-agent using the ip helper-address command, we allow R1 to obtain its IP configuration from the DHCP server connected to R2. This way, the DHCP request can traverse the network from the client (R1) to the DHCP server (198.51.100.100) and back without requiring any manual IP configuration on R1.

upvoted 2 times

cormorant 9 months, 2 weeks 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 4 months, 2 weeks 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, 3 months 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, 9 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, 8 months ago

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

upvoted 2 times

🗨️ 👤 **Zerotime0** 2 years, 7 months ago

I think thats it.

upvoted 1 times

🗨️ 👤 **Zerotime0** 2 years, 7 months ago

Nevermind bc correct

upvoted 3 times

🗨️ 👤 **sinear** 2 years, 8 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, 5 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, 8 months ago

Don't agree. CE are correct.

upvoted 4 times

🗨️ 👤 **ROBZY90** 2 years, 4 months 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** 2 years, 2 months ago

This is what I was looking for

upvoted 3 times

🗨️ 👤 **Ali526** 2 years, 8 months ago

Sorry. BC correct.

upvoted 9 times

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, 11 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 5 months, 3 weeks 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** 6 months, 2 weeks ago

Is this CCNA question?

upvoted 4 times

 **[Removed]** 2 months, 3 weeks ago

Yes, it's part of CCNA 200-301

upvoted 2 times

 **Taku2023** 5 months ago

this is Quality of Service

upvoted 3 times

 **DARKK** 1 year, 3 months 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, 9 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, 11 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, 3 months ago

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

upvoted 2 times


```
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, 8 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 44 times

 **pianetaperez** 2 years, 7 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** 10 months, 3 weeks 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** 3 months, 3 weeks 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 2 times

 **velrisan** 2 years, 3 months 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, 8 months ago

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

upvoted 12 times

 **oooMooo** 2 years, 4 months ago

The traffic is outgoing.

upvoted 2 times

 **raul_kapone** Most Recent 1 week, 1 day ago

Selected Answer: D

I'm absolutely sure that the answer is D.

With NAT the Inside Lobal is translated to the Inside Global.

Where the term "Inside" refers the physical location of our host (PC,server).

upvoted 1 times

 **Liquid_May** 3 weeks, 4 days ago

Selected Answer: D

The question asks about the source IP address after the NAT translation occurred. Assuming that the packet is leaving the private network and going to the internet, option D seems correct.

upvoted 1 times

 **Osas5** 1 month, 1 week ago

for me i will go with option C reason is outside Local is the Source address after NAT which can be viewed from the source PC inside Global is viewed from destination pc

upvoted 1 times

🗳️ **[Removed]** 2 months, 3 weeks ago

Selected Answer: D

D is correct. 172.23.104.4 is the source IP.

upvoted 2 times

🗳️ **Isuzu** 3 months, 1 week 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** 3 months, 2 weeks ago

D is the correct answer

upvoted 1 times

🗳️ **FALARASTA** 4 months, 2 weeks 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** 5 months, 1 week ago

D is the correct answer

upvoted 1 times

🗳️ **RougePotatoe** 10 months, 3 weeks 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** 10 months, 3 weeks ago

Selected Answer: D

The Answer is D

upvoted 1 times

🗳️ **re_roy** 10 months, 3 weeks ago

Answer is D

upvoted 1 times

🗳️ **GigaGremlin** 11 months, 1 week ago

Selected Answer: D

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

upvoted 1 times

🗳️ **Murphy2022** 11 months, 2 weeks 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** 10 months, 3 weeks 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** 1 year, 2 months 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** 1 year, 2 months ago

Correct is D
upvoted 1 times

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, 4 months ago

A is the right answer
upvoted 18 times

 **Eric852** Highly Voted 1 year, 5 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 10 times

 **dropspablo** Most Recent 3 months, 3 weeks 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 3 times

 **dropspablo** 3 months, 3 weeks 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** 3 months, 3 weeks 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 2 times

 **rogi2023** 4 months, 3 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** 5 months, 1 week 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** 6 months, 3 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 2 times

🗨️ **badboyrobinson** 9 months ago

Selected Answer: A

Going with A because notice level is not a biggie

upvoted 2 times

🗨️ **cormorant** 10 months, 2 weeks ago

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

upvoted 2 times

🗨️ **medamine2022** 1 year, 2 months ago

Selected Answer: A

a because the notice level for max reason reboot the device

upvoted 1 times

🗨️ **AudreyLin** 1 year, 6 months ago

Selected Answer: A

A is true

upvoted 1 times

🗨️ **yonten007** 1 year, 8 months ago

Selected Answer: A

A is the right answer

upvoted 2 times

🗨️ **ayoubenn** 1 year, 11 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, 4 months 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 7 times

🗨️ **oooMoo** 2 years, 4 months 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, 11 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, 11 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, 11 months ago

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

upvoted 1 times

DRAG DROP -

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

Select and Place:

Answer Area

- resolves web URLs to IP addresses
- assigns a default gateway to a client
- holds the TCP/IP settings to be distributed to the clients
- stores a list of IP addresses mapped to names
- assigns IP addresses to enabled clients

DHCP Server

DNS Server

Correct Answer:

Answer Area

- resolves web URLs to IP addresses
- assigns a default gateway to a client
- holds the TCP/IP settings to be distributed to the clients
- stores a list of IP addresses mapped to names
- assigns IP addresses to enabled clients

DHCP Server

assigns a default gateway to a client

holds the TCP/IP settings to be distributed to the clients

assigns IP addresses to enabled clients

DNS Server

resolves web URLs to IP addresses

stores a list of IP addresses mapped to names

ayd33n Highly Voted 3 years, 1 month 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 1 year, 2 months 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

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 3 years 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 27 times

 **Zerotime0** 2 years, 8 months ago

Agreed

upvoted 3 times

 **knister** Highly Voted 3 years, 2 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 7 times

 **SanchezEldorado** 3 years, 2 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 9 months ago

AUTHEnication and ip of ntp server. end of story

upvoted 1 times

 **WINDSON** 1 year, 2 months 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, 9 months ago

funny thing is that neither in Wendell Odom, nor on Netacad was mentioned NTP Authentication lol

upvoted 5 times

 **UnbornD9** 4 months, 4 weeks ago

I'm so tired of this f***** questions about something that IS NOT in the OFFICIAL CERT GUIDE...

upvoted 4 times

  **devildog** 2 years, 11 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** 3 years, 1 month ago

I think b and c are more correct. Authentication is not a must
upvoted 6 times

  **Mountie** 3 years, 2 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** 3 years, 2 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** 3 years, 3 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  2 years 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

  **Imadolfo2019** Highly Voted  2 years, 5 months ago

D is a answer...

upvoted 7 times

  **DARKK** Most Recent  1 year, 3 months ago

Selected Answer: D

Poor wording but it is D.

upvoted 2 times

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** Highly Voted 8 months 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 8 times

 **splashy** 8 months ago

255.255.255.253 must be ...252 ... typo

upvoted 3 times

 **NICE_ANSWERS** 3 months, 1 week ago

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

upvoted 1 times

 **Request7108** Most Recent 8 months, 2 weeks 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** 11 months, 1 week ago

Answer is D

<https://study-ccna.com/dynamic-nat/>

upvoted 2 times

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, 4 months ago

Selected Answer: C

HSRP uses Active/standby
VRRP uses Master/Backup
upvoted 17 times

 **Raisul** Most Recent 4 months, 2 weeks 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** 4 months, 2 weeks ago

Duplicate question.
upvoted 1 times

 **SamuelSami** 1 year 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 224.0.0.252.
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, 4 months ago

HSRP= Hot STANDBY Routing Protocol
upvoted 3 times

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

 **klosinski** Highly Voted 2 years, 11 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, 10 months ago

thanks

upvoted 3 times

 **Ebenezer** Highly Voted 2 years, 11 months ago

The right answer is FTP.

upvoted 7 times

 **Thaier** Most Recent 1 month, 2 weeks ago

Selected Answer: C

Answer is C

copy function in routers:

https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/cmdrefs/copy.htm

upvoted 1 times

 **LilGhost_404** 1 year, 7 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, 9 months ago

Selected Answer: D

D Correct

upvoted 1 times

 **AlexPlh** 2 years, 2 months ago

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

upvoted 2 times

 **lxJustinlx** 2 years, 3 months 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, 8 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, 11 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, 8 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, 11 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, 11 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 11 months, 3 weeks ago

Inside/Outside = Location of the host
Local/Global = Perspective
upvoted 2 times

 **Technique31** 1 year, 9 months ago

Selected Answer: C

C Correct

upvoted 4 times

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 `show ntp status` 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, 10 months ago

show ntp associations
for configured server
upvoted 7 times

 **Hodicek** Highly Voted 1 year, 10 months ago

NTP=CLOCK
upvoted 5 times

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 `overload` 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 `overload` keyword is shown below:

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

 **kaus33k** Highly Voted 1 year, 11 months ago

Overload is the answer that enables the PAT.
upvoted 8 times

 **kyleptt** Most Recent 2 weeks, 3 days ago

I think Pool can be used in this instance you can pool 1 address to many in the pool to be translated.
upvoted 1 times

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.

 **MoHTimo** 1 month, 1 week ago

I don't know why but I hate QoS part the most from all topics
upvoted 1 times


 **[Removed]** 2 months, 3 weeks ago

Selected Answer: C

to support IP services --> IP SLA (IP SERVICE Level Agreement) is an easy way to remember this. Basically the answer is in the question.
upvoted 1 times

 **aaaaaaaaakkk** 1 year, 2 months ago

just tell what is the ccna real exam is it ccnp or harder
upvoted 3 times

 **Mozah** 1 year, 7 months ago

Yes, correct answer is C
upvoted 4 times

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, 7 months ago

answer should be LLQ Low Latency Queueing
upvoted 25 times

 **lucky1559** Highly Voted 2 years ago

Some questions are tricky. They ask for prioritization method not queuing method, thus it leaves us with round-robin and expedited-forwarding.

So correct answer is expedited forwarding.
upvoted 13 times

 **Jackie_Manuas12** 1 year, 5 months ago

<They ask for prioritization method not queuing 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 5 months, 3 weeks 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** 6 months, 3 weeks 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** 1 year, 1 month ago

9tut.com shows the correct answer as Low Latency Queueing

upvoted 1 times

 **DARKK** 1 year, 3 months ago

Selected Answer: C

C is certainly correct here.

upvoted 2 times

 **Jeanromeo1** 1 year, 3 months 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, 4 months ago

correct answer is LOWER-LATENCY QUEUEING.

upvoted 2 times

 **bodybod** 1 year, 6 months ago

Selected Answer: C

easy easy easy
upvoted 1 times

🗨️ **gachocop3** 1 year, 6 months ago
the right answer is C
upvoted 1 times

🗨️ **juani85** 1 year, 6 months ago
Selected Answer: C
so good answer
upvoted 1 times

🗨️ **Nagib** 1 year, 7 months ago
answer should be c. low latency queueing
upvoted 1 times

🗨️ **Cisna** 1 year, 12 months ago
Right answer is C
upvoted 1 times

🗨️ **bootloader_jack** 1 year, 12 months ago
what do you mean by "prioritization method" ? be clear cisco.
upvoted 2 times

🗨️ **zaguy** 2 years 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** 2 years 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** 2 years, 3 months ago
I thought it was C...
upvoted 2 times

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

zombi1101 Highly Voted 4 months, 1 week 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 5 times

[Removed] Most Recent 4 months, 1 week ago

NO UFRONT PAYMENT!!

GET CERTIFIED.
 100%PASS GUARANTEED.

WhatsApp +1(409)223 7790

1. COMPTIA (network+ security+)
- 2: GMAT,GRE exams
- 3: IAPP Certifications (CIPP/E CIPM, CIPT)
- 4: ISACA certifications (CISA,CISM/ CRISC)
- 5: EC-COUNCIL Certification (CEH , CCISO)
- 6: PMI (PMP/CAPM/ACP/PBA ,RMP)
- 7: IMA (CMA certification)
- 8: CIA,IFRS, CERTIFICATIONS
- 9: ACCA,CFA,ICAEW certifications

10: ISO certification

11 PASS CISSP EXAM

12. APICS CERTIFICATIONS, CSCP, CPIM, CLTD

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

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, 7 months ago

answer should be
B. to provide fair queuing for buffered flows
traffic shaping is not necessarily doing limitation of bandwidth
upvoted 16 times

 **ZayaB** Highly Voted 2 years, 6 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 9 times

 **kyleptt** Most Recent 1 week ago

Selected Answer: B
Shaping affect the que
upvoted 1 times

 **Cynthia2023** 1 month, 2 weeks ago

Selected Answer: D
The purpose of traffic shaping is to control the rate of data transmission for a specific flow or type of traffic. It allows network administrators to limit the bandwidth that a flow can consume, preventing it from exceeding a certain rate and helping to manage network congestion and ensure fair distribution of resources. Traffic shaping can be used to control the flow of data over slower links, prioritize critical traffic, and prevent certain flows from overwhelming the network.
upvoted 1 times

 **[Removed]** 2 months, 3 weeks ago

Selected Answer: D
Answer D
upvoted 2 times

 **Shun5566** 3 months, 2 weeks ago

Selected Answer: B
I think is B
upvoted 1 times

 **Anas_Ahmad** 8 months, 3 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** 1 year 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** 3 months, 1 week ago

It says fair queuing over there tho
upvoted 1 times

  **SOAPGUY** 1 year, 4 months ago

Selected Answer: D



D IS THE PURPOSE, B IS THE METHOD.
upvoted 5 times

  **tumajay** 6 days, 15 hours ago

reverse is the case. B is the purpose, D is d method. traffic shaping is used to provide fair queuing by limiting bandwidth
upvoted 1 times

  **Smaritz** 1 year, 5 months ago

Seems to me it should be B
upvoted 2 times

  **siki1984** 1 year, 5 months ago

B is correct answer

Traffic shaping regulates and smooths out the packet flow by imposing a maximum traffic rate for each port's egress queue. Packets that exceed the threshold are placed in the queue and are retransmitted later. This process is similar to traffic policing; however, the packets are not dropped. Because packets are buffered, traffic shaping minimizes packet loss (based on the queue length), which provides a better traffic behavior for TCP traffic

chrome-

extension://oemndcbldboiebfnladdacbfmadadm/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 2 times

  **ismatdmour** 1 year, 5 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, 7 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, 7 months ago


Selected Answer: D

From Official 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, 8 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, 10 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, 11 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 article 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, 11 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

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, 4 months ago

A is the correct, pelati
upvoted 12 times

  **[Removed]** Most Recent 2 months, 3 weeks ago

Selected Answer: A

A is correct
upvoted 1 times



  **Ciscoman021** 5 months, 3 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 2 times



  **cormorant** 10 months, 1 week ago

always associate TFTP with ISO images and firmware upgrades
upvoted 2 times

  **sakisg** 1 year, 2 months ago

Selected Answer: A

a is correct
upvoted 1 times

  **Sajomon** 1 year, 3 months 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, 5 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, 7 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, 7 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, 8 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, 7 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, 7 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, 8 months ago

Selected Answer: A

I like A better

upvoted 1 times

  **Rockrl** 1 year, 8 months ago

Selected Answer: A

The correct answer is A

upvoted 2 times

  **shakyak** 1 year, 9 months ago

Selected Answer: A

A is the answer

upvoted 2 times

  **Shamwedge** 1 year, 9 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, 9 months ago



a is correct

upvoted 1 times

  **Bibby** 1 year, 9 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, 9 months ago

please change admin true option here A not D

upvoted 1 times

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, 7 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  5 months, 3 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** 6 months, 3 weeks ago

A is a DNS client.

B is a DHCP client

upvoted 1 times

Where does the configuration reside when a helper address is configured to 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, 9 months ago

It's a helper so closest to the client.
upvoted 6 times



  **Yinx** Most Recent 3 weeks, 4 days ago

Selected Answer: B

Because client send DHCP request packet to the helper by broadcast, so client and helper must be in the same subnet, they are very close. By contrast, helper router forward the request to the DHCP server by unicast, which is routable. So the DHCP server can be far away to the helper.
upvoted 1 times


  **justajoke** 2 months ago

Why do they word the questions this way? I know the answer, the hard part is figuring out what the hell the question is.
upvoted 1 times

  **Etidic** 10 months, 3 weeks ago

Selected Answer: B

The answer is B
upvoted 3 times

  **gaber** 1 year, 8 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 4 times

  **bwg** 2 years, 3 months ago

Can someone explain it?
upvoted 2 times

  **Sten111** 2 years, 2 months ago

This explains it pretty well
<https://www.ciscopress.com/articles/article.asp?p=330807&seqNum=9>
upvoted 3 times

  **dave1992** 1 year, 11 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** 10 months, 3 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 2 times

  **FALARASTA** 4 months, 2 weeks ago

There is no need to configure two routers along the way as dhcp helpers because the one closest to the client changes the broadcast to a unicast request automatically

upvoted 3 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*

  **Gauain** 2 months, 3 weeks ago

CORRECT

upvoted 1 times

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 2 years, 1 month ago

Way to remember: Emma Always Crying Even When Nobody Is Dying
upvoted 22 times

 **Renelis** Highly Voted 2 years, 2 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 8 months, 3 weeks ago

total freaking :-D
upvoted 1 times

 **hojusigol** 1 year, 7 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

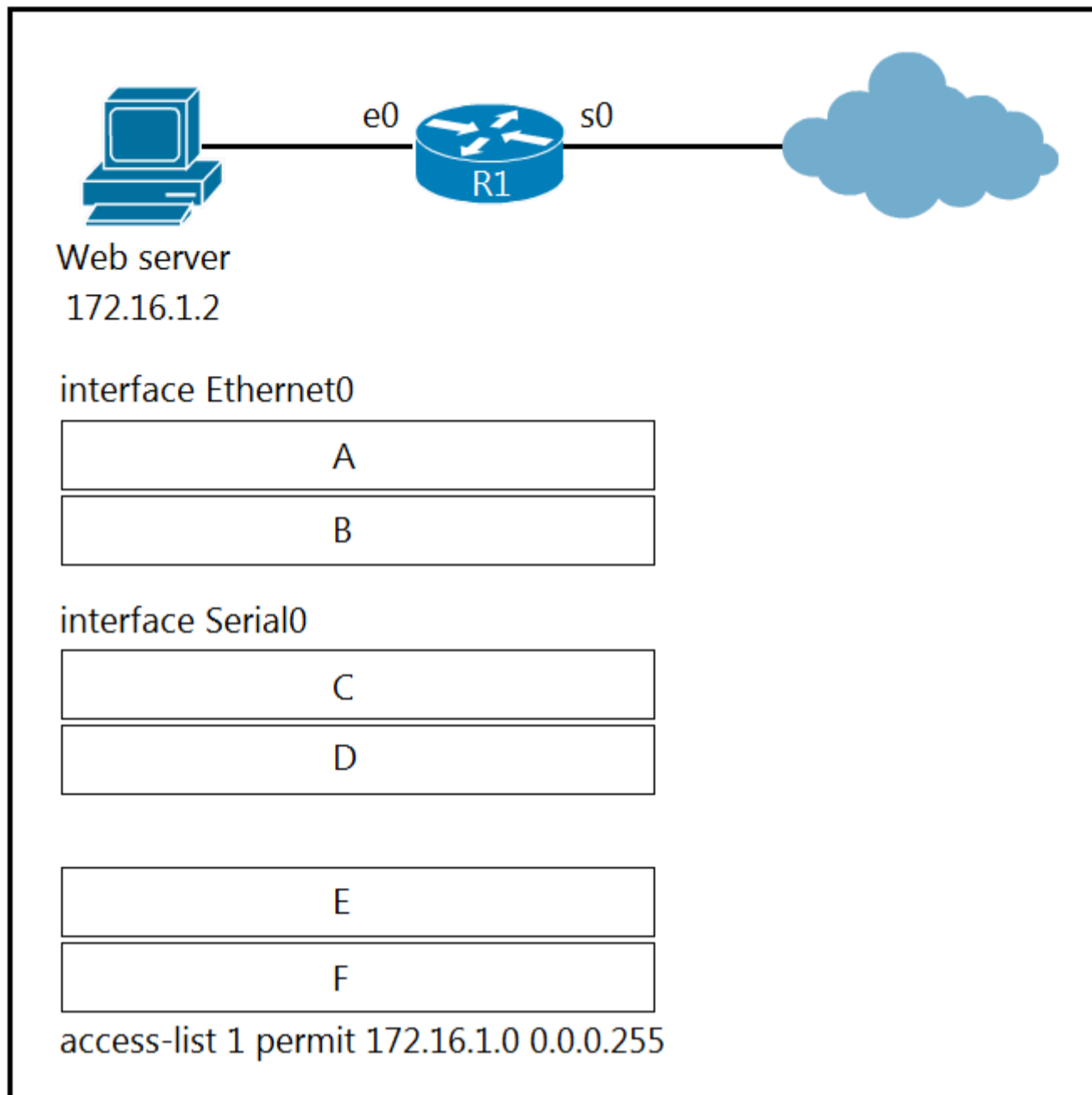
 **rgg** 1 year, 10 months ago

Another way to remember: every awesome Cisco engineer will need icecream daily
upvoted 5 times

 **joanb2s** 8 months, 3 weeks ago

total freaking
upvoted 1 times

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 right.

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 2 years ago

Why PAT? The question asks for a static nat operation, WHY PAT?
upvoted 11 times

 **Shamwedge** Highly Voted 1 year, 9 months ago

I hate these type of questions. You don't always have to do things in these exact orders...
upvoted 9 times

 **Dante_Dan** 1 year, 8 months ago

In this particular case, you do have to do it in order.
upvoted 2 times

 **Danu22** 1 year, 5 months ago

What source do you have for this claim? Because I also don't believe that the order particularly matters here.
upvoted 3 times

 **iGlitch** Most Recent 1 year, 4 months ago

The last two lines, you don't have to place them in this order this is a BS question.
upvoted 4 times

 **Netclick** 2 years, 2 months ago

It binds the inside local address and local port to the specified inside global address and global port.
upvoted 3 times

 **Orkhann** 2 years, 3 months ago

what "ip nat inside source static tcp ..." command do? Any explanation please?
upvoted 3 times

 **CiscoTerminator** 2 years, 1 month 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

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 2 years ago


Q at the end = queuing protocol = congestion management
upvoted 43 times

 **YetiPatty** 2 months, 3 weeks ago

Qongestion Management
upvoted 2 times

 **Isuzu** 3 months, 1 week ago

Nice Hint
upvoted 1 times

 **Smaritz** 1 year, 6 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, 10 months ago

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

 **nebolala1** Highly Voted 1 year, 10 months ago

what the f**** is that mean???
upvoted 15 times

 **LOST40** 1 year, 6 months ago

PQ-Priority queues
upvoted 2 times

 **raydel92** Most Recent 1 year, 9 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 4 times

 **dave1992** 1 year, 11 months ago

Class based weighted fair queueing and PQ?
upvoted 2 times

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

 **gaber** Highly Voted 1 year, 8 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/congston_mgmt_oview.html

enjoy

upvoted 6 times

 **zaguy** Highly Voted 2 years 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/congston_mgmt_oview.html

upvoted 5 times

 **Da_Costa** Most Recent 3 months ago

With Priority Queueing (PQ), traffic is classified into high, medium, normal, and low priority queues. The high priority traffic is serviced first, then medium priority traffic, followed by normal and low priority traffic. -> Therefore we can assign higher priority for voice traffic. Therefore PQ is the right answer

upvoted 1 times

 **dave1992** 1 year, 11 months ago

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

upvoted 1 times

 **appleness123** 2 years 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** 2 years ago

Yes, correct

upvoted 2 times

 **StingVN** 3 months, 4 weeks ago

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

upvoted 1 times

 **[Removed]** 2 months, 3 weeks ago


No, no, no it's not correct. It's ABSOLUTELY corect lol ;-)

upvoted 1 times

 **BooleanPizza** 2 years ago


Explanation?

upvoted 1 times

 **aosroyal** 1 year, 5 months ago



yes, correct

upvoted 4 times

  **Rothus** 1 year, 4 months ago

Yes, correct

upvoted 3 times

  **coolapple** 1 year, 4 months ago

Yes, definitely correct

upvoted 3 times

  **Dutch012** 6 months, 1 week ago

Yes, correct

upvoted 1 times

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, 9 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 14 times

 **gaber** 1 year, 8 months ago

yes, dhcp address assignment is just dhcp assigning addresses.
C is best here imo

upvoted 1 times

 **shakyak** 1 year, 9 months ago

This is the correct answer

upvoted 1 times

 **firstblood** Highly Voted 2 years ago

A is correct. Static IP should be excluded from the DHCP pool.

upvoted 8 times

 **Request7108** 8 months, 2 weeks 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 2 times

 **hker** 2 years 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 4 months, 3 weeks ago

B for me

upvoted 1 times

 **couragek** 7 months, 1 week ago

COULOOKPS

C

upvoted 1 times

 **Ciscoman021** 7 months, 2 weeks 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** 8 months, 2 weeks 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** 1 year, 1 month ago

Selected Answer: C

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

upvoted 1 times

🗨️ **Sajomon** 1 year, 3 months 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, 5 months 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, 7 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, 8 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, 3 months ago

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

upvoted 2 times

🗨️ **pjvillareal** 1 year, 9 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, 9 months ago

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

upvoted 1 times

🗨️ **Shamwedge** 1 year, 9 months ago

DHCP address assignment must be there way of saying DHCP reservation

upvoted 1 times

🗨️ **yasuke** 1 year, 12 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** 2 years 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** 2 years ago

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

upvoted 2 times

  **CiscoTerminator** 2 years 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** 2 years 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. DHCP OFFER
- B. DHCP relay agent
- C. DHCP server
- D. DHCP DISCOVER

Correct Answer: B

  **Stonetales987** Highly Voted  1 year, 10 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 8 times

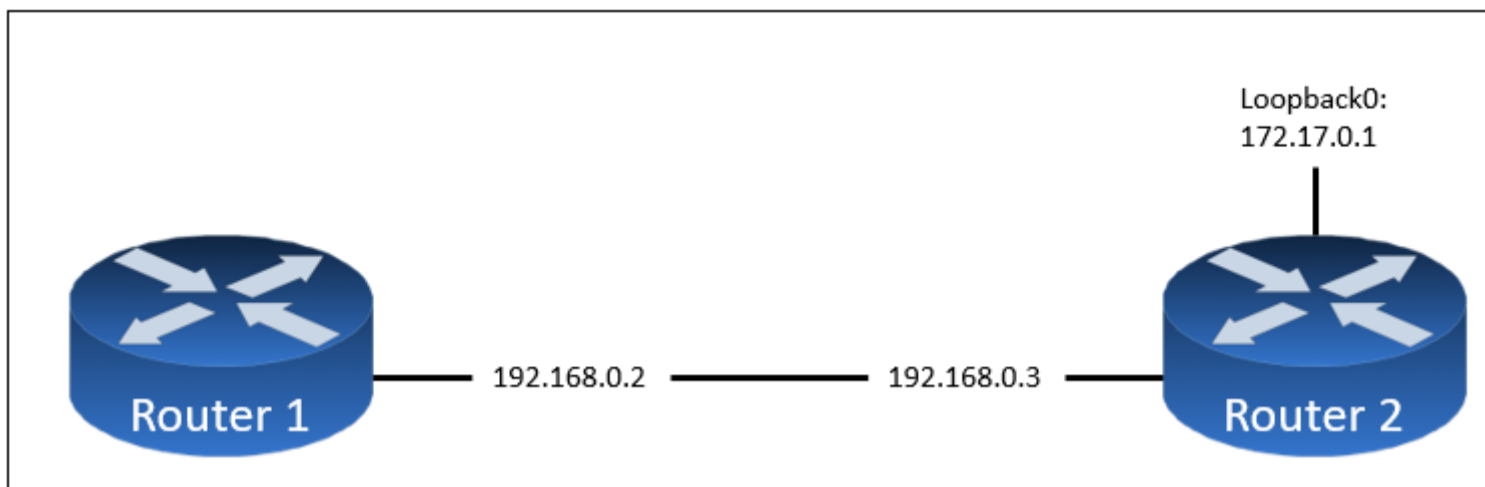
  **Redoxon** Most Recent  1 month, 4 weeks ago

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

The DHCP relay agent is a network device, such as a router or switch, that operates at the network layer (Layer 3) of the OSI model. Its purpose is to receive DHCP client messages broadcasted on one network segment and then forward them to a DHCP server on a different network segment. Similarly, it receives DHCP server messages and relays them back to the DHCP client.

By using a DHCP relay agent, DHCP messages can traverse multiple network segments, allowing DHCP clients to obtain IP addresses and other configuration information from DHCP servers located on different networks.

upvoted 1 times



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, 11 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 10 times

DaBest (Highly Voted) 1 year, 11 months ago

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

upvoted 5 times

Customexit 11 months, 2 weeks 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 5 times

dave1992 1 year, 11 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 stratum level it learns from its NTP server, so that the stratum level increases the more hops away from the original clock source.

upvoted 10 times

  **kennybb** 1 year, 2 months ago

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

  **GangsterDady** 1 year, 11 months ago

m also wondering
upvoted 1 times

  **Redoxon** Most Recent 1 month, 4 weeks ago

The command "ntp master" configures a router to act as an NTP server and provides its own time source. The number after "ntp master" represents the stratum level. In this case, "4" indicates that the router will be considered a stratum 4 NTP server. Stratum levels range from 1 to 15, where lower numbers indicate higher stratum levels and more accurate time sources.

By configuring Router 2 with "ntp master 4," it will operate as an NTP server without relying on external time sources, using its internal clock as the time reference.

upvoted 2 times

  **Priyamano** 1 year, 2 months ago

D is ok
upvoted 1 times

  **Hodicek** 1 year, 9 months ago

i server is client , so 2nd should to be master
upvoted 1 times



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

  **TechLover** 2 months, 4 weeks ago

Correct answer is A.
upvoted 1 times

  **Adaya** 1 year, 10 months ago

A is the correct answer
upvoted 3 times

  **ascsaca** 2 years ago

C correct
upvoted 1 times

  **ProgSnob** 1 year, 10 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 14 times

  **Rydaz** 4 months ago

any paid advice?
upvoted 2 times

  **Myname1277** 2 years ago

TFTP does not require authentication while FTP requires authentication so A is correct
upvoted 15 times



  **dave1992** 1 year, 11 months ago

You have to re read the question.
upvoted 2 times

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, 7 months ago

Selected Answer: C

C is correct
upvoted 2 times

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 2 years ago


Correct Answer therefore : B. SW1# config t SW1(config)#ntp master SW1(config)#ntp server192.168.1.1
upvoted 18 times

 **Sim_James_27** 1 year, 9 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, 10 months ago

i hate that question
upvoted 18 times

 **bikila123** 1 month ago

please watch jeremys it lab on youtube you will like this trust me
upvoted 1 times

 **Elmasquentona963** Most Recent 5 days, 5 hours ago

Selected Answer: B

The correct explanation would be:

SW(config)# ntp server 192.168.1.1

Makes the SW1 a client to the primary server reachable with an IP address of 192.168.1.1

SW1(config)# ntp master

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.

- The key is the following statement "SW1 act as an NTP server".
 - It implies issue an "ntp master" configuration command obligatory.
 - So, answer is B
- upvoted 1 times

 **PlsLetMePass** 1 month, 1 week ago

Selected Answer: C

Option B, SW1# config t SW1(config)#ntp master SW1(config)#ntp server 192.168.1.1, is not the correct answer because it configures the switch to be the primary NTP server. This means that the switch will be responsible for synchronizing the time of all other devices in the network.

In the case of the question, the switch is configured to act as a backup NTP server. This means that the switch will only provide NTP services if the upstream NTP server becomes unavailable.

If the switch is configured as the primary NTP server, it will not be able to act as a backup NTP server. This is because the switch will be too busy synchronizing the time of all other devices in the network.

Therefore, the correct configuration is to use the ntp backup and ntp server commands. These commands will configure the switch to act as a backup NTP server, and they will also specify the IP address of the upstream NTP server.

If the upstream NTP server becomes unavailable, the switch will start providing NTP services to the network using its own internal clock.
upvoted 1 times

 **MDK94** 1 year, 2 months 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 12 times

 **gachocop3** 1 year, 6 months ago

answer is B

upvoted 2 times

 **Nebulise** 1 year, 7 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 5 times

 **taiyi078** 1 year, 7 months ago

Selected Answer: B

Answer B

upvoted 1 times

 **ksave** 1 year, 7 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 3 times

 **Vinarino** 1 year, 8 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, 8 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=271918E500000005olcsuBTZcAlAy9u9O1OINPqAoEAbAQAABQAAAIKYCAGAcAAAAAAAK0iAgA=

B

upvoted 1 times

 **gaber** 1 year, 8 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, 9 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, 9 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, 9 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, 10 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, 10 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, 11 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-ntp.html#assnmodes>

upvoted 1 times

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, 3 months ago


Selected Answer: B

B for sure. "...for the *router* to pass *DHCPDISCOVER* messages on to the server"
upvoted 2 times

 **Kvothe24** 1 year, 4 months 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, 4 months 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, 4 months 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, 5 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 centrized location in the enterprise network
upvoted 1 times

 **NORLI** 1 year, 4 months 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, 6 months ago

the answer is B


upvoted 1 times

 **LilGhost_404** 1 year, 7 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, 7 months ago

Selected Answer: B

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

upvoted 1 times

 **awashenko** 1 year, 7 months ago

Selected Answer: B

A relay agent is needed. Answer is B
upvoted 1 times

🗨️ **Mozah** 1 year, 7 months ago

Selected Answer: B

I think B
upvoted 1 times

🗨️ **Ravan** 1 year, 7 months ago

Selected Answer: B

A relay agent (ip-helper)
upvoted 1 times

🗨️ **Cho1571** 1 year, 8 months ago

Ha! the answer is B
upvoted 1 times

🗨️ **daanderud** 1 year, 8 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, 8 months ago

Selected Answer: B

I think good answer B
upvoted 1 times

🗨️ **RJM** 1 year, 8 months ago

Selected Answer: B

Relay agent passes routed DHCP discover packets.
upvoted 3 times

🗨️ **gaber** 1 year, 8 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, 4 months 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

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

- A. alert
- B. critical
- C. notice
- D. debug

Correct Answer: D

  **hp2wx** Highly Voted 1 year, 2 months ago

Every good Cisco engineer will need intercourse daily :0
upvoted 10 times

  **Vinarino** Highly Voted 1 year, 8 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** 1 year, 2 months ago

0 EMERGENCY
upvoted 2 times

  **Da_Costa** Most Recent 3 months ago



Every awesome Cisco engineer need icecream daily from 0-7
upvoted 1 times

  **Vikramaditya_J** 1 month, 1 week ago

Small correction: Every awesome Cisco Engineer "Will" Need Icecream Daily (Level 0-7). Don't forget "Will" i.e., Warning. :-)
upvoted 1 times

  **arenjenkins** 10 months, 3 weeks ago

fck this questiion
upvoted 6 times

  **ptfish** 1 year, 2 months 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, 3 months ago

Emma Always Cries Even When Nobody Is Dying
upvoted 5 times

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

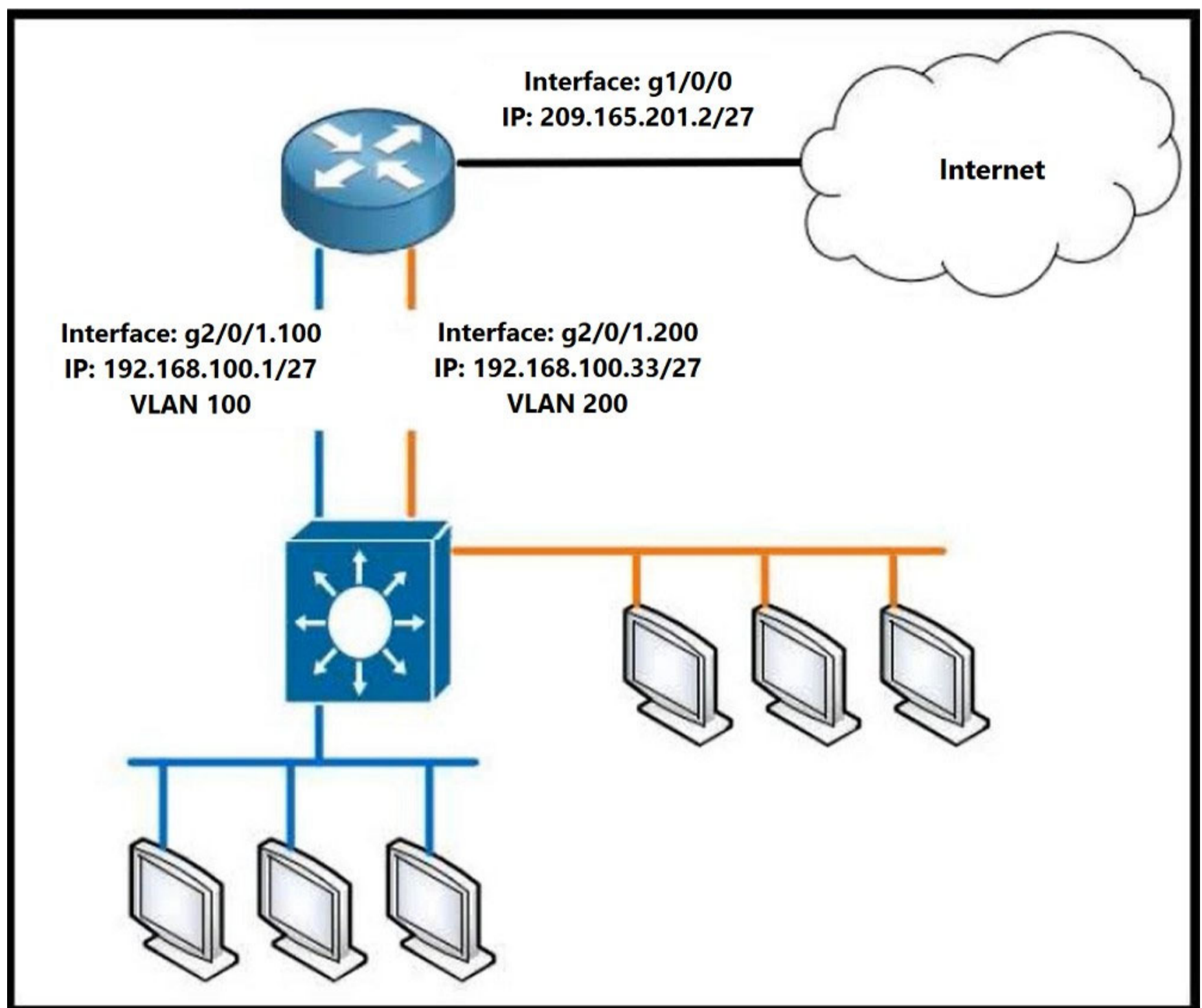
Which two statements about NTP operations are true? (Choose two.)

- 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  1 year, 2 months ago
NTP use UDP port 123.
upvoted 6 times

  **[Removed]** Most Recent  2 months, 1 week ago
Selected Answer: AB
A. NTP uses UDP over IP.
B. Cisco routers can act as both NTP authoritative servers and NTP clients.
upvoted 2 times



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 1 year, 1 month ago

just looking the IP address and subnet mask of the access list, you can find the right answer
upvoted 14 times

rogi2023 6 months ago

another broke question with bad wording/syntax on routers intf..but agree with AndreMD
upvoted 2 times

fransCISCO 7 months, 2 weeks ago

yes its A
upvoted 1 times

  **splashy** Highly Voted  12 months 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 8 times


```

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 12 months 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 1 year ago

Selected Answer: AC

A and C

only encrypted and crypto key not yet generated

upvoted 7 times

 **kyleptt** Most Recent 1 week ago

Selected Answer: AC

C & A must have RSA generated and transport input ssh

upvoted 1 times

 **Liquid_May** 3 weeks, 3 days ago

Selected Answer: AC

The ip ssh version 2 command is optional. The crypto key generate rsa 1024 is required for ssh connections. The transport input ssh command specifies that you only want to connect to the router via ssh, this way you can't connect to the router via Telnet, which doesn't support encrypted connections. Therefore, A and C.

Search for Set Up an IOS Router or Switch as SSH Client in this site:
<https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html>
upvoted 1 times

  **Shabeth** 2 months ago

Selected Answer: AC

A and C
upvoted 1 times


  **ahmadawni** 2 months ago

Selected Answer: AC

although "crypto key generate rsa" command enables SSH on the device, however the "transport input" command must be entered because 'The transport command defines which protocols can be used to connect to a line. The default protocol is none, which means that no incoming connections are allowed.'
upvoted 1 times

  **DMc** 4 months, 3 weeks 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** 11 months, 3 weeks 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** 11 months, 4 weeks ago

Selected Answer: AC

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

  **rogi2023** 6 months ago

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

  **sasquatchshrimp** 1 year, 1 month 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

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 1 year, 2 months 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 6 times

 **dropspablo** Most Recent 3 months, 2 weeks 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** 10 months, 3 weeks ago

Can anyone confirm that snmp-server user command is only available to SNMPv3?

upvoted 1 times

 **jonathan126** 4 months, 3 weeks 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-snmv3.pdf>

SNMPv2c use community string.

upvoted 4 times

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 1 year, 1 month 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 11 times

🗨️ **Elmasquentona963** Most Recent 5 days, 5 hours ago

Selected Answer: C

ntp master <stratum-level> global configuration command is the correct way to set the stratum value.
upvoted 1 times

🗨️ **sijan** 6 months, 1 week ago

C should be correct
upvoted 2 times

🗨️ **oatmealturkey** 6 months, 4 weeks ago

Selected Answer: C

It cannot be D because stratum is not a valid command.
upvoted 3 times

🗨️ **iampogiian** 9 months ago

Letter C ang sagot
upvoted 2 times

🗨️ **Aiman_Abdullah** 11 months 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** 12 months ago

Selected Answer: C

explained below
upvoted 4 times

🗨️ **beskardrip** 1 year, 2 months 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** 9 months, 3 weeks ago

Its not d, because the access list 10 is standar and cannot configure ports on this
upvoted 4 times

🗨️ **RougePotatoo** 10 months, 3 weeks ago

D has the command NTP stratum 2 (not a real command) it is suppose to be ntp master 2
upvoted 6 times

  **MDK94** 1 year, 2 months 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** 1 year, 2 months 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** 1 year, 2 months 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** 1 year, 2 months 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** 1 year, 2 months 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** 1 year, 2 months ago

Good Catch !
upvoted 3 times

  **BOFA** 1 year, 1 month 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, 3 months ago

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

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](https://en.wikipedia.org/wiki/File_Transfer_Protocol#:~:text=The%20File%20Transfer%20Protocol%20(FTP,the%20client%20and%20the%20server)

 **Liquid_May** 3 weeks, 3 days ago

I know that B is correct. However, C also seems correct since FTP supports encryption. Can someone, explain why is C not correct?
upvoted 2 times


 **Elmasquentona963** 4 days, 5 hours ago

Source: CCNA 200-301 Official Cert Guide, Volume 2
Table 12-3 Common Methods to Copy Files Outside a Router
Method Method - Encrypted?
TFTP - No
FTP - No
SCP - Yes

Source:

[https://en.wikipedia.org/wiki/File_Transfer_Protocol#:~:text=The%20File%20Transfer%20Protocol%20\(FTP,the%20client%20and%20the%20server](https://en.wikipedia.org/wiki/File_Transfer_Protocol#:~:text=The%20File%20Transfer%20Protocol%20(FTP,the%20client%20and%20the%20server)

FTP uses unencrypted connections, leaving both the data you transfer and your credentials exposed to eavesdropping attacks.
upvoted 1 times

 **StingVN** 3 months, 4 weeks 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 2 times

 **StingVN** 3 months, 4 weeks 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** 8 months, 1 week ago

B is correct
upvoted 3 times

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/>

 **kyleptt** 1 week ago

DRH - Domain , RSA key and Hostname
upvoted 1 times

 **[Removed]** 2 months, 1 week ago

Selected Answer: C

C. ip domain-name domain
You'll get an error if you don't set the ip domain-name
upvoted 1 times


 **StevenYung** 2 months, 2 weeks ago

Selected Answer: C

"before entering the command to generate the RSA key"
upvoted 1 times

 **Mccn** 7 months, 2 weeks 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** 7 months, 3 weeks ago

Selected Answer: D

The question "to generate the RSA key"
upvoted 1 times

 **Dutch012** 6 months, 3 weeks ago

"before entering the command to generate the RSA key"
upvoted 2 times

 **ratu68** 1 year, 2 months ago

Selected Answer: C

C is absolutely correct
upvoted 4 times

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, 4 months 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 16 times

 **[Removed]** Most Recent  2 months, 2 weeks ago

Selected Answer: D

Given answer is correct.
upvoted 1 times

 **shefo1** 3 months, 1 week ago

Selected Answer: D

of couse D is right
upvoted 3 times

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,-Example%3A&text=Forwards%20UPD%20broadcasts%2C%20including%20BOOTP%20and%20DHCP.&text=The%20address%20argument%20can%20be,to%20respond%20to%20DHCP%20requests

Example%


3A&text=Forwards%20UPD%20broadcasts%2C%20including%20BOOTP%20and%20DHCP.&text=The%20address%20argument%20can%20be,to%20respond

%20to%20DHCP%20requests

 **Yannik123** 5 months, 1 week ago

Selected Answer: D

The DHCP relay agent is an IP Helper address on a Cisco device
upvoted 2 times

 **Goena** 8 months, 2 weeks ago

Selected Answer: D

D is correct
upvoted 3 times

```
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 10 months, 3 weeks 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

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

 **RODCCN** 2 months, 1 week ago

Selected Answer: D

<https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5584-configure-system-time-settings-on-a-switch-through-the-comma.html>

upvoted 2 times

 **[Removed]** 2 months, 1 week ago

Selected Answer: D

clock set is correct

upvoted 1 times

 **Goena** 8 months, 2 weeks ago

Selected Answer: D

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

upvoted 3 times

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

 **[Removed]** 2 months, 1 week ago

Selected Answer: A

Given answer is correct

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

upvoted 1 times

 **Yannik123** 5 months, 2 weeks ago

Selected Answer: A

A is right I tested it in Packte Tracer.

upvoted 3 times

What prevents a workstation from receiving a DHCP address?

- A. STP
- B. VTP
- C. 802.1Q
- D. DTP

Correct Answer: C

  **Ghugs** Highly Voted 11 months, 2 weeks 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 7 times

  **splashy** 11 months ago

Thx for sharing i guess it's A then
upvoted 1 times

  **splashy** 11 months 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 3 times

  **fransCISCO** 10 months, 1 week 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

  **rijstraket** Highly Voted 7 months, 2 weeks 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 5 times

  **dropspablo** 1 month, 1 week ago

That is, by using PortFast it is possible to mitigate the problem caused by the STP transition time and ensure that workstations obtain IP addresses via DHCP without significant delays.
upvoted 1 times

  **RODCCN** Most Recent 2 months, 1 week ago

Selected Answer: C

Ok, how about C? If the port is in access mode, on vlan X and DHCP on vlan Y, and there's no dhcp relay configured, it'll prevent the computer to get IP.
upvoted 1 times

  **Da_Costa** 2 months, 2 weeks ago

Selected Answer: A

STP will prevent a workstation from receiving a dhcp message
upvoted 2 times

  **Da_Costa** 3 months ago

STP is the best option because when the port is blocked the client will not receive a dhcp address hence apipa will be used
upvoted 1 times

  **rogi2023** 4 months, 3 weeks ago



Selected Answer: A

in such questions the best practise is to exclude the wrong asnwrs 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 4 times

  **Secsoft** 3 weeks ago

sorry but I removed STP too thinking it as the stuffs related to port convergence
upvoted 1 times

  **rogi2023** 6 months ago

this is a very stupid question, I hope not to see such garbage on the exam especially for ccna level.
upvoted 2 times

  **mohdhafizuddinesa** 10 months, 1 week ago

You will not have IP from trunk port
upvoted 1 times

  **splashy** 11 months, 3 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** 11 months, 2 weeks ago

Dot1q ist VLAN tagging not authentication
upvoted 2 times

  **splashy** 11 months ago

Correct i got it mixed up with 802.1X... doh
upvoted 1 times

  **ShadyAbdekmalek** 11 months, 3 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**  11 months, 4 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 8 times


  **harveyDai** **Highly Voted**  1 year ago

I thought TFTP is only for File transferring.
upvoted 6 times

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

 **YetiPatty** 2 months, 3 weeks ago

Selected Answer: D

forgot to attach my vote lol
upvoted 2 times

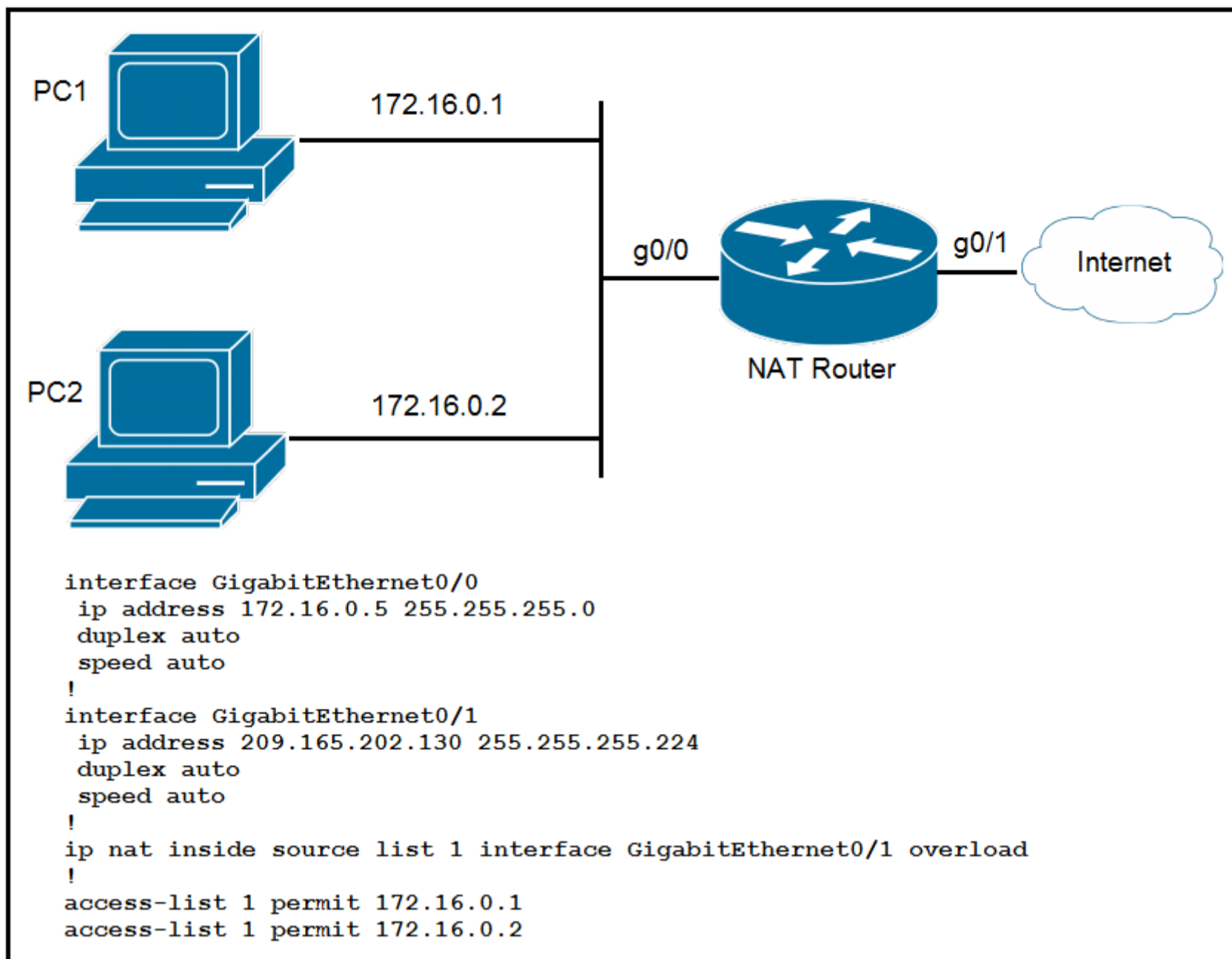
 **YetiPatty** 2 months, 3 weeks ago

Answer is correct:

Chatgpt: Marking is a QoS technique where a value is modified or added to a specific field in the packet header to indicate the class or priority of the packet. This marking can be used to differentiate and prioritize different types of traffic based on their specific requirements.

For example, in IP-based networks, the Differentiated Services Code Point (DSCP) field in the IP header can be modified to set the class of service for a packet. By changing the value of the DSCP field, the packet is marked with a specific priority or class, allowing routers and switches along the network path to apply appropriate QoS policies and forwarding behaviors.

Marking is crucial in QoS implementation as it enables network devices to identify and treat packets differently based on their class of service, ensuring that higher-priority traffic, such as voice or real-time applications, receives preferential treatment and appropriate QoS handling.
upvoted 2 times



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 7 months, 1 week ago

Selected Answer: B

Why is it not B?

upvoted 5 times

mda2h 2 months ago

Because after specifying the access list you either put:
 - The public IP address your packet source address will be natted to
 - or the outside interface (the public facing one)

Setting G0/0 is wrong cause it's the inside interface.

upvoted 2 times

e072f83 Most Recent 1 week, 6 days ago

Selected Answer: D

B= WRONG

D= the correct answer!!

upvoted 1 times

ds0321 2 weeks, 6 days ago

Selected Answer: B

is it B

upvoted 1 times

🗨️ 👤 **ds0321** 2 weeks, 6 days ago

my bad it is D
upvoted 1 times

🗨️ 👤 **[Removed]** 2 months, 1 week ago

Selected Answer: D

D. Add either the ip nat {inside|outside} command under both interfaces
ip nat inside and outside are missing on the interfaces
upvoted 2 times

🗨️ 👤 **4aynick** 4 months, 3 weeks ago

Selected Answer: D

100% D is correct
upvoted 3 times

🗨️ 👤 **rogi2023** 4 months, 3 weeks ago

Selected Answer: D

Only inside/outside on the interfaces is missing. and it is a must.
upvoted 3 times

🗨️ 👤 **Goena** 6 months, 3 weeks 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** 11 months, 1 week 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 4 times


```

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 9 months, 1 week 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 9 times

 **StingVN** 3 months, 4 weeks ago

agree yo

upvoted 1 times

 **Eallam** Most Recent 3 months ago

all answers are wrong , the protocol is written at the end not before the destination so it should be c abut C is also missing the transport protocol before the source ,
access-list 100 udp source destination eq 65

upvoted 3 times

 **Cynthia2023** 1 month ago

the protocol written immediately after the source IP address is because it's the source port

upvoted 1 times

 **enzo86** 5 months ago

Selected Answer: D

dhcp is udp and iphelper in f0/1 interface LAN

upvoted 3 times

 **RougePotatoe** 10 months, 3 weeks 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** 11 months, 1 week 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** 11 months, 1 week 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** 11 months, 2 weeks ago

Selected Answer: D

*I mean DHCP uses UDP port 67

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

upvoted 3 times

🗄️ 👤 **creaguy** 11 months, 2 weeks ago

Selected Answer: D

DHCP uses TCP port 67

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

upvoted 1 times

🗄️ 👤 **JonasWolfxin** 11 months, 3 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** 11 months, 4 weeks ago

Selected Answer: A

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

upvoted 1 times

🗄️ 👤 **splashy** 12 months 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** 12 months ago

Selected Answer: D

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

upvoted 2 times

🗄️ 👤 **joondale** 1 year 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** 1 year 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** 1 year ago

Selected Answer: B

IS B the answer?

upvoted 1 times

 **melmiosis** 10 months, 1 week 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:

show snmp chassis	displays information about the SNMP recipient
show snmp community	displays the IP address of the remote SNMP device
show snmp engineID	displays the SNMP security model in use
show snmp group	displays the SNMP access string
show snmp host	displays the SNMP server serial number

Correct Answer:

show snmp chassis	show snmp host
show snmp community	show snmp engineID
show snmp engineID	show snmp group
show snmp group	show snmp community
show snmp host	show snmp chassis

 **Reyliem** Highly Voted 12 months 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 7 times

 **no_blink404** Most Recent 2 months, 3 weeks ago

show snmp chassis: displays the snmp server serial number
show snmp community: displays the snmp access string
show snmp engineID: displays the IP address of the remote snmp device
show snmp group: displays the snmp security model in use
show snmp host: displays information about the snmp recipient

Sources:

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
& ChatGPT

upvoted 2 times

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 7 months, 1 week 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 initially) 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 14 times

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

  **Dutch012** Highly Voted 6 months, 3 weeks 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 7 times

  **Elmasquentona963** Most Recent 2 days, 11 hours ago

Selected Answer: A

Both tools (Policy and Shaping) attempt to keep the bit rate (bandwidth) at or below a specified speed, but by using two different actions:


- Policers: Discard or re-mark packets.
- Shapers: Delay packets by hold them in a queue.

So, I think the difference goes with the fact of in which interfaces must be enabled (Policy or Shaping). In that case, according to the statement of the question, the solution is to with improve the customer experience. Therefore the answer should be "A".

Why?

- Policers are enabled on an interface, in either direction.
- Shapers are enabled on an interface for egress (outgoing packets).

upvoted 1 times

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: A

A. policing

upvoted 1 times

  **dropspablo** 3 months, 2 weeks ago

Selected Answer: A

A. policing

upvoted 1 times

  **andresugiharto** 5 months, 4 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 3 times

  **JJY888** 6 months, 3 weeks ago

Selected Answer: A

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

upvoted 2 times

  **rijstraket** 7 months, 2 weeks 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 (Committed 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** 7 months, 2 weeks 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** 8 months, 3 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 3 times

🗄️ 👤 **yong08321** 9 months ago

Selected Answer: D

It's D shaping whenever there is bandwidth

upvoted 2 times

🗄️ 👤 **Panda_man** 9 months ago

Selected Answer: D

It's D shaping whenever there is bandwidth

upvoted 1 times

🗄️ 👤 **SemStrond** 10 months, 1 week 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

DRAG DROP -

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

Select and Place:

cloud-based weighted fair queueing	categorizes packets based on the value of a traffic descriptor
classification	guarantees minimum bandwidth to specific traffic classes when an interface is congested
congestion	prevents congestion by reducing the flow of outbound traffic
policing	outcome of overutilization
shaping	uses defined criteria to limit the transmission of one or more classes of traffic

Correct Answer:

cloud-based weighted fair queueing	classification
classification	policing
congestion	shaping
policing	congestion
shaping	cloud-based weighted fair queueing

gewe Highly Voted 7 months ago
 from top to bottom:
 classification
 class based weighted fair queueing
 shaping
 congestion
 policing
 upvoted 23 times

dropspablo 3 months, 2 weeks ago
 Correct
 upvoted 1 times

bisiyemo1 4 months, 2 weeks ago
 This is very correct
 upvoted 1 times

RougePotatoo Highly Voted 10 months, 3 weeks 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 19 times

  **EthanhuntMI6** 8 months, 3 weeks ago

I think 5 should be policing not shaping.
upvoted 9 times

  **jonathan126** 4 months, 3 weeks ago



But with shaping, congestion is still there, shaping just put the traffic into a queue, so it cannot prevent congestion
upvoted 2 times

  **Cynthia2023** Most Recent 1 month ago

1. **classification**: Categorizes packets based on the value of a traffic descriptor.
 2. **class-based weighted fair queueing**: Guarantees minimum bandwidth to specific traffic classes when an interface is congested.
 3. **shaping**: Prevents congestion by reducing the flow of outbound traffic.
 4. **congestion**: Outcome of overutilization.
 5. **policing**: Uses defined criteria to limit the transmission of one or more classes of traffic.
- upvoted 1 times

  **splashy** 11 months, 3 weeks ago

bandwidth = policing + shaping
limit transmission = by putting in a que
upvoted 2 times

  **Anon1216** 12 months ago

Shouldn't cloud-based wighted fair queueing and policing be swapped?
upvoted 11 times

  **Lance789** 11 months 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** 10 months, 4 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 7 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

DRAG DROP -

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

Select and Place:

event correlation and aggregation	The administrator can manually intervene at the source of the fault.
fault detection	The network management system launches a preconfigured script to restore functionality.
fault diagnosis and isolation	The system groups alarms from related issues.
problem resolution	The system identifies performance degradation or service interruption.
restoration of service	The system reports on the source of the issue.

Correct Answer:

event correlation and aggregation	problem resolution
fault detection	restoration of service
fault diagnosis and isolation	event correlation and aggregation
problem resolution	fault detection
restoration of service	fault diagnosis and isolation

Tamirkadosh Highly Voted 11 months, 1 week ago
wth is that bro
upvoted 31 times

EthanhuntMI6 Highly Voted 9 months, 1 week ago
No idea what this is, but not expecting anything great from cisco.
upvoted 10 times

no_blink404 Most Recent 2 months, 3 weeks ago
Here is what I think:

event correlation: The system groups alarms
fault detection: the system identifies performance degradation
fault diagnosis and isolation: the system reports on the source
problem resolution: the administrator can manually intervene
restoration of service: the network management system launches
upvoted 2 times

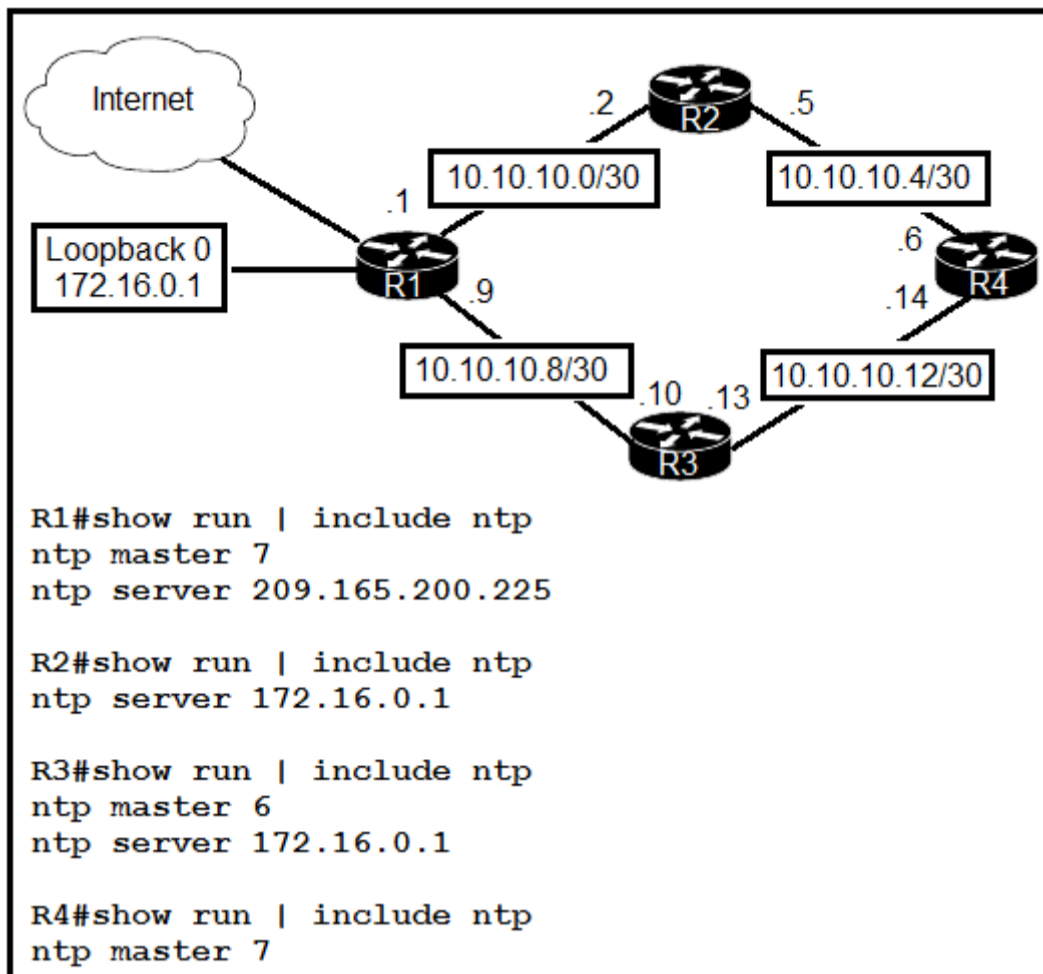
mda2h 1 month, 3 weeks ago
Figured out the same thing
Up this!
upvoted 2 times

gewe 7 months ago

just a basic understanding how SNMP works. thank you very very much. / now I know everything
upvoted 3 times

  **EthanhuntMI6** 8 months, 3 weeks ago

I think 'problem resolution' and 'fault diagnosis and isolation' need to be swapped.
upvoted 9 times



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

RougePotatoe Highly Voted 10 months, 3 weeks ago

Selected Answer: D

Pretty sure you have to have the NTP server configured before you can be a client
upvoted 5 times

[Removed] Most Recent 2 months, 2 weeks ago

Selected Answer: D

D. R1, R2, and R3
upvoted 1 times

dropspablo 3 months, 2 weeks ago

Selected Answer: D

Correct
upvoted 1 times

Swiz005 5 months ago

Selected Answer: A

Isn't this A?
upvoted 1 times

dropspablo 3 weeks, 3 days ago

Answer correct is "D". The R3 has the config "NTP master 6" configured with stratum 6, and the R1 "NTP master 7" (stratum 7 "greater than 6"), however the stratum that is taken into account in R3 would be that of the remote source captured by the R1 as a client of the ip 209.165.200.225, and not its ntp master 7 configuration, and normally these clock sources are reliable with stratum 1 (NIST), which would result in a stratum 2 for R1 and stratum 3 for R3. Just in case R1 loses access to this remote clock source, its config "ntp master 7" with stratum 7 would be triggered, and it would send a stratum 8 to R3, then R3 with config "ntp master 6" would be triggered for having a smaller stratum, making it its own server. But in this case R3 is a client, synchronized with a remote clock from R1 and with a supposed stratum 3 (NIST stratum 1 - R1 stratum 2 - R3 stratum 3).

upvoted 1 times

dropspablo 3 weeks, 3 days ago

But in this case R3 is a client, synchronized with a remote clock from R1 and with a supposed stratum 3 (NIST stratum 1 - R1 stratum 2 - R3 stratum 3).

upvoted 1 times

```
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 12 months ago

Selected Answer: D

There are no static entries?
There also is no outside interface defined?
So D
upvoted 12 times

 **creaguy** Highly Voted 11 months, 2 weeks ago


Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xr-16/nat-xr-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 6 times

 **Anas_Ahmad** Most Recent 9 months ago

Selected Answer: D

D is correct
upvoted 2 times

 **rijstraket** 9 months, 1 week ago

Selected Answer: D

The outside interface isn't defined, so D.
upvoted 3 times

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

 **RougePotatoe** Highly Voted 10 months 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 5 times

 **dorf05** Most Recent 2 months ago

correct answer; C
upvoted 2 times

 **RODCCN** 2 months, 1 week ago

Selected Answer: D

"The facility to which the message refers (for example, SNMP, SYS, and so forth). A facility can be a hardware device, a protocol, or a module of the system software. It denotes the source or the cause of the system message."

<https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.html>
upvoted 1 times

 **JuanluRea** 2 months, 3 weeks ago

Selected Answer: D

https://success.trendmicro.com/dcx/s/solution/TP000086250?language=en_US
upvoted 1 times

 **deluxeccna** 4 months, 4 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

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:

provides local control for network segments using a client-server scheme

uses authoritative servers for record keeping

maintains an address pool

associates hostnames to IP address

offers domain name server configuration

reduces the administrative burden for onboarding end users

assigns IP addresses to local hosts for a configurable lease time

function

function

function

function

Correct Answer:

provides local control for network segments using a client-server scheme

uses authoritative servers for record keeping

maintains an address pool

associates hostnames to IP address

offers domain name server configuration

reduces the administrative burden for onboarding end users

assigns IP addresses to local hosts for a configurable lease time

maintains an address pool

provides local control for network segments using a client-server scheme

reduces the administrative burden for onboarding end users

assigns IP addresses to local hosts for a configurable lease time

 **GigaGremlin** Highly Voted 11 months, 1 week ago

Yes,... I agree...
* Provides local control for network segments...
is wrong
Should be this one
* offers DNS config
upvoted 20 times

 **DUMPladore** Highly Voted 7 months, 4 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 10 times

 **dropspablo** 3 months, 2 weeks ago

I agree
upvoted 1 times

 **dropspablo** 3 months, 2 weeks 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 2 times

 **dropspablo** Most Recent 3 months, 2 weeks 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** 10 months ago

Does anyone even know what they are referring to when they say provides local control to network segments?

upvoted 4 times

  **perri88** 3 months ago

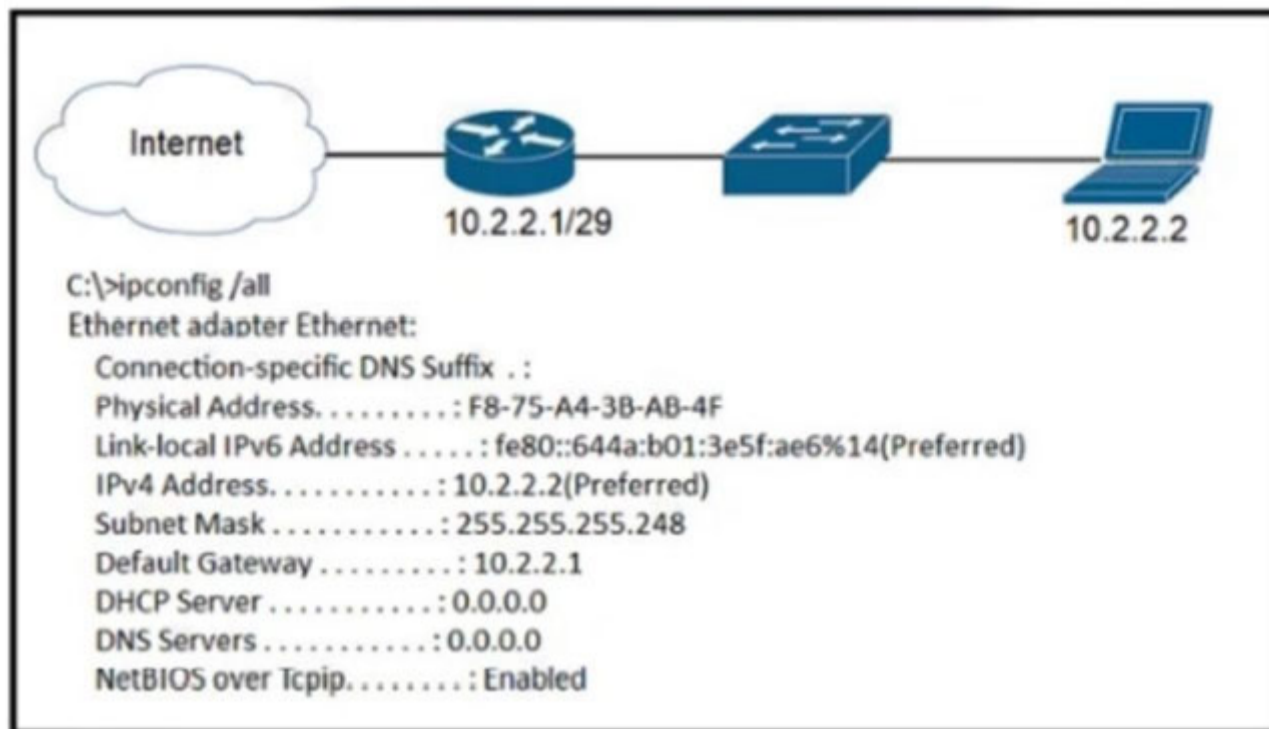
no idea

upvoted 1 times

  **EliasM** 11 months, 1 week ago

Why not offers domain names server configuration?

upvoted 6 times



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 3 months, 4 weeks ago

Selected Answer: B

connect internet. of course it should be DNS server. easy peasy.
upvoted 2 times

papinski 6 months, 2 weeks ago

Wish all questions were as easy as this
upvoted 2 times

gewe 7 months 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 9 months, 3 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 11 months, 2 weeks ago

Selected Answer: B

.....Duh !
upvoted 3 times

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** 11 months ago

some websites said the answer is LLQ. I think the answer should be policing, but 'which queueing method' made me confused jeez
upvoted 2 times

 **splashy** 11 months, 2 weeks 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 definitely not a Queuing method/algo, it's a congestion avoidance tool.

upvoted 4 times

 **RougePotatoe** 10 months, 3 weeks 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

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

  **supervictor** 1 month, 2 weeks ago

D. Marking

The other options, shaping, policing, and classification, do not directly change the ToS field in the IPv4 packet header.

upvoted 1 times

  **xyzboy** 3 months, 1 week ago

the answer is correct

upvoted 1 times

  **RougePotatoe** 10 months, 3 weeks 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** 10 months, 3 weeks 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 IP precedence 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](https://linuxreviews.org/Type_of_Service_(ToS)_and_DSCP_Values)

upvoted 2 times

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

  **[Removed]** 2 months, 1 week ago

Selected Answer: D

D. Uses two separate connections for control and data traffic
Ports 20 and 21
upvoted 1 times

  **papibarbu** 8 months, 1 week ago

port 20 and 21 OK
upvoted 4 times

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**  10 months, 3 weeks 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 6 times

  **tawanda_belkis** **Most Recent**  5 months, 1 week ago

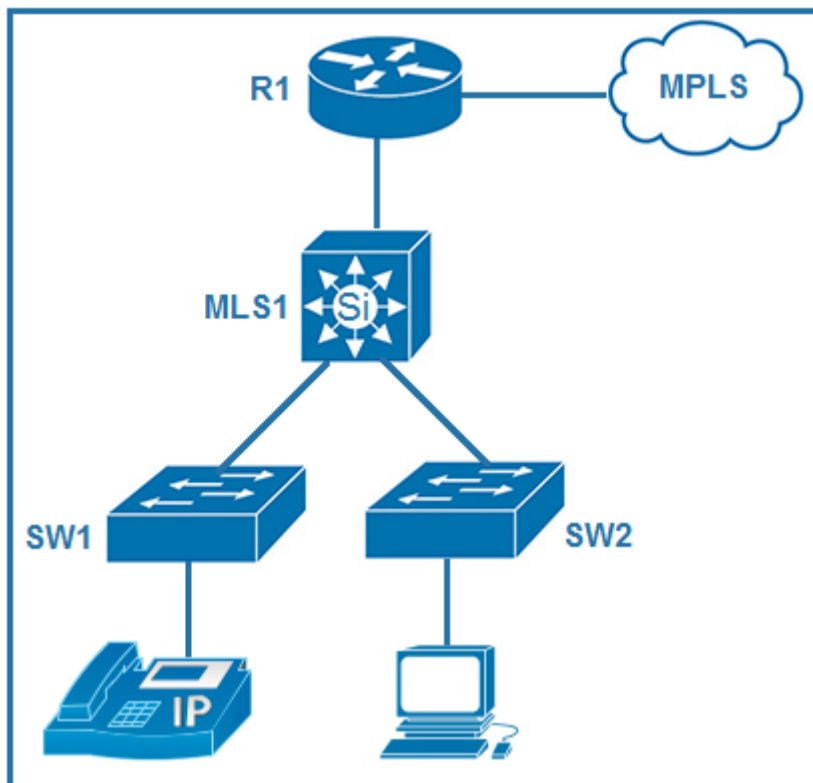
uses block numbers to identify and mitigate data transfer errors
upvoted 1 times

  **Yannik123** 5 months, 1 week 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 2 times



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.

 **no_blink404** 3 months, 1 week ago

I am pretty sure all/most of the traffic marking should be done on the lower layers ie access layer. Answer A seems correct.
upvoted 1 times

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

 **RougePotatoo** Highly Voted 10 months, 3 weeks 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 6 times

 **Elmasquentona963** Most Recent 2 days, 7 hours ago

Selected Answer: C

A Prioritization Strategy for Data, Voice and Video:
<omitted>
4. Put voice in a separate queue from video so that the policing function applies separately to each.
<omitted>

Source: CCNA 200-301 Official Cert Guide, Volume 2 (pg. 245)
upvoted 1 times

 **Yinx** 3 weeks, 3 days ago

Selected Answer: C

The foundation of Qos is classificaiton.
upvoted 1 times

 **Liquid_May** 3 weeks, 3 days ago

Selected Answer: B

I would go with B, as RougePotatoo stated, voice traffic can only function with a 1% packet loss or less, so it makes sense to avoid packet loss. Besides that, since video and voice traffic are both traffic types that can't afford delays or packet loss, I don't see how differentiating them would help regarding voice traffic.
upvoted 2 times

 **mda2h** 1 month, 3 weeks ago

Selected Answer: B

I'll go with B, since the question only talks about voice. Besides, if why stop at differentiate voice and video, why not data traffic as well?
upvoted 1 times

 **Mark_j_k90** 1 month, 3 weeks ago

Selected Answer: C

it's C! If you differentiate voice and video like Voice Platinum and Video Gold, you don't need to reduce packet loss, because a small amount of loss is tolerable.
upvoted 2 times

 **Olebogeng_G** 2 months, 2 weeks ago

It's C. Packet loss is tolerable.
upvoted 2 times

 **Bingchengchen236** 3 months ago

I choose C, because for voice traffic, usually UDP is used at transport layer, and a little bit packet doesn't matter
upvoted 4 times

 **bisiyemo1** 4 months, 2 weeks ago

Selected Answer: B

B is very very correct.
upvoted 1 times

🗨️ **Naghini** 8 months 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** 8 months, 1 week 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.

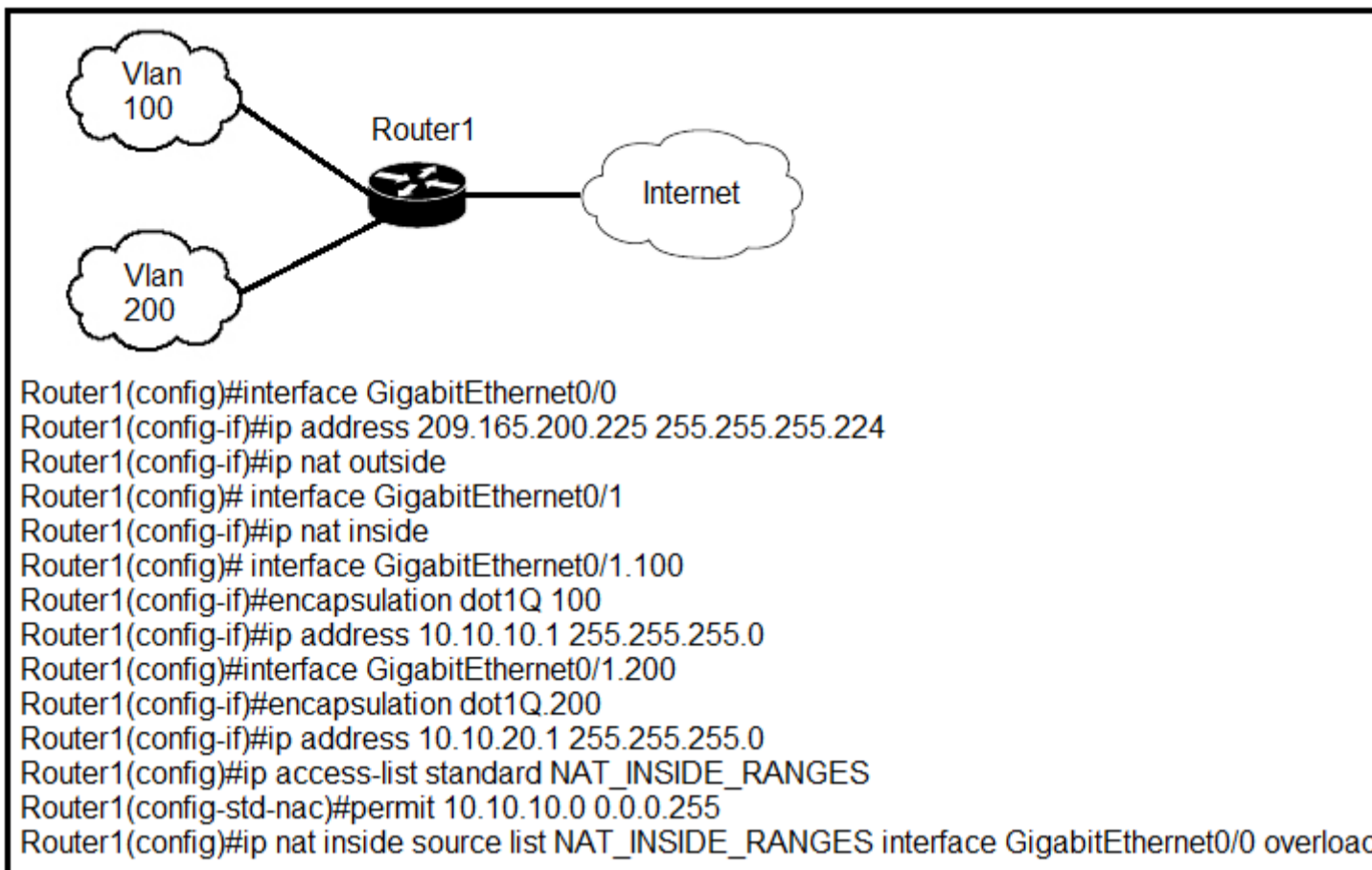
upvoted 4 times

🗨️ **kynnor** 5 months ago

- A. WRED - Weighted Random Early Detection packet dropping on Congestion Avoidance mechanism
- B. FIFO - First In first Out

- *C. PQ - Priority Queue*
- D. WFQ - Weight Fair Queue

upvoted 2 times



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

RougePotatoo Highly Voted 10 months, 2 weeks 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 12 times

Yannik123 Most Recent 5 months, 1 week ago

Selected Answer: D

D is the correct answer. You only need to read the given config in the picture.

upvoted 3 times

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

  **cormorant** Highly Voted 10 months, 2 weeks ago

something i know- PIN
something i have - the mobile
upvoted 5 times

  **Dunedrifter** 2 months, 2 weeks ago

And something I am completes the multi factor authentication requirements. In this case, it's the first two.
upvoted 2 times

  **Dunedrifter** 2 months, 2 weeks ago

Something I am means biometric authentication. (Fingerprint, Retina scan)
upvoted 2 times

  **ac89l** Most Recent 4 months, 1 week ago

how is this CCNA ?
upvoted 2 times

  **creaguy** 11 months, 2 weeks ago

Basically, the authenticator will require you to put a password on you phone.
upvoted 2 times

  **dipanjana1990** 1 year, 1 month 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** 10 months 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, 4 months 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, 11 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, 11 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** 10 months, 2 weeks ago

Not very realistic as you would need someone who knows the admin password to type it to employees' phones from time to time. Not very scalable, might work for small businesses though.

upvoted 2 times

🗨️ 👤 **Nicocisco** 1 year, 6 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 2 times

Which device performs stateful inspection of traffic?

- A. switch
- B. firewall
- C. access point
- D. wireless controller

Correct Answer: B

  **dicksonpwc** Highly Voted 2 years 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 11 times

  **LLAMBRA** Highly Voted 2 years, 1 month 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 6 times

  **Mark_j_k90** 1 month, 3 weeks ago

Ips is included in the new-generation firewall. You should know that! So your answer is right (B) but your explanation is not!



upvoted 1 times

  **DUMPladore** Most Recent 7 months, 4 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

  **juann** 1 year, 2 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 3 times

  **Mark_j_k90** 1 month, 3 weeks ago

you have to check every single question and answer they give you. 60% of the answer they give you is wrong!

upvoted 1 times

  **juann** 1 year, 2 months ago

They put the c as correct but I have doubts.

upvoted 1 times

  **aaaaaaaakkk** 1 year, 2 months ago



but the answer is b

upvoted 2 times

  **ROBZY90** 2 years, 4 months ago

Stateful refers to the device reading the config from top to bottom

upvoted 4 times

  **Ali526** 2 years, 8 months ago

B is correct.

upvoted 2 times

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, 8 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, 4 months 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** 1 year, 3 months 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 addresses and the switch ports associated with them...
upvoted 5 times

 **Ali526** Highly Voted 2 years, 8 months ago

C is correct (99%). For remaining 1%, please check by Friday.
upvoted 8 times

 **syslil** 2 years, 2 months ago

@ali526 you liar
upvoted 5 times

 **Acai** 2 years, 4 months ago

You lied to us Ali lol
upvoted 8 times

 **lucky1559** Most Recent 2 years 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 5 times

 **dicksonpwc** 2 years 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** 2 years, 1 month ago

C is correct... but isn't the syntax something like..."switchport port-security mac-address sticky" ?
upvoted 3 times

 **D0nkey_h0t** 1 year, 3 months ago

it's not a command written there, it's the action you are supposed to take
upvoted 2 times

 **EL_Touffiko** 2 years, 1 month ago

B is not correct because of the word "automatically"
upvoted 6 times

```
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

 **TheLorenz** Highly Voted 1 year, 6 months ago

Answer is C. You need to configure enable secret command in order to connect to telnet
upvoted 5 times

 **IFBBPROSALCEDO** Most Recent 2 months, 1 week ago

To allow administrators to authenticate directly to enable privilege mode via Telnet using a local username and password, the correct additional configuration is:

```
B. R1(config)#username admin privilege 15 secret p@ss1234
R1(config)#line vty 0 4
R1(config-line)#login local
```

Explanation:

Option B provides the correct configuration for enabling Telnet access with local authentication. Here's a breakdown of the commands:

R1(config)#username admin privilege 15 secret p@ss1234: This command creates a local username "admin" with privilege level 15 and sets the password as "p@ss1234". The privilege level 15 grants administrative access to the user.

R1(config)#line vty 0 4: This command enters the configuration mode for the virtual terminal lines (vty) from 0 to 4, which are used for Telnet access.

R1(config-line)#login local: This command enables local authentication for Telnet access on the vty lines, meaning the switch will use the locally configured username and password for authentication.

upvoted 1 times

 **[Removed]** 2 months, 1 week ago

Selected Answer: B

```
B.
R1(config)#username admin privilege 15 secret p@ss1234
R1(config-if)#line vty 0 4
R1(config-line)#login local
```

upvoted 1 times

 **Ciscoman021** 5 months, 3 weeks ago

Selected Answer: B

B is right
upvoted 2 times

 **alejandrol2** 9 months, 3 weeks ago

Answer A
Its the unique that enable telnet (transport input telnet)
upvoted 2 times


 **ike110** 7 months ago

Telnet is enabled by default, so no need to enable it again
upvoted 4 times

 **Etidic** 10 months, 3 weeks ago

Selected Answer: B

The answer is B
upvoted 1 times

  **Garfieldcat** 11 months, 1 week 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** 11 months, 1 week ago

Selected Answer: B

...authenticate directly to enable privilege mode via Telnet using a local username and password
upvoted 2 times

  **guynetwork** 1 year ago


Selected Answer: B

"authenticate directly"
upvoted 2 times

  **sasquatchshrimp** 1 year, 1 month 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, 4 months ago

Selected Answer: B

Level 15 is exec mode :)
upvoted 2 times

  **DatBroNZ** 1 year, 6 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

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 2 years 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, 11 months ago

Bad question I think.

upvoted 8 times

  **cormorant** Most Recent 9 months, 3 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

  **aaaaaaaaakkk** 1 year, 2 months 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** 2 years ago

Does this question have a typo?

upvoted 6 times

  **jeroenptrs93** 1 year, 9 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 6 times

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 Vioalton 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 2 years 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 30 times

 **nakres64** Highly Voted 2 years, 7 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

 **[Removed]** Most Recent 2 months, 2 weeks ago

Selected Answer: AE

Given answers are correct :

- A. The security violation counter dose not increment
 - E. The interface drops traffic from unknown MAC address
- upvoted 1 times

 **dropspablo** 3 months, 2 weeks 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** 11 months, 1 week ago

Answer A and E

<https://study-ccna.com/cisco-port-security-violation-configuration/>

upvoted 1 times

 **Mafix** 1 year, 6 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, 10 months ago

PROTECT MODE : B-C-D ARE NOT CORRECT ANSWERS 100%
upvoted 1 times

  **Jimmy** 2 years, 6 months ago

http://cisco.num.edu.mn/CCNA_R&S2/course/module2/2.2.4.4/2.2.4.4.html
upvoted 5 times

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, 7 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 31 times

  **Ethiopsis** Highly Voted 2 years, 6 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 15 times

  **StingVN** Most Recent 3 months, 4 weeks 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 2 times

  **kynnor** 5 months 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** 6 months, 2 weeks ago

Guys, it's asking about technology not protocol, I would go with C.

upvoted 1 times

  **[Removed]** 1 year, 2 months ago

Selected Answer: D

Make sense

upvoted 1 times

  **LilGhost_404** 1 year, 7 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, 7 months ago

Selected Answer: D


D SNMPV3


upvoted 2 times


  **Cho1571** 1 year, 8 months ago


Selected Answer: D


I picked D
upvoted 1 times


🗉  **RichyES** 1 year, 8 months ago
SNMPv3 so D is correct
upvoted 1 times


🗉  **Nebulise** 1 year, 9 months ago
Selected Answer: D
C is not correct
upvoted 1 times


🗉  **Hodicek** 1 year, 9 months ago
snmpv3
upvoted 1 times

🗉  **babaKazoo** 1 year, 9 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, 9 months ago
Protocol Vs Technology?
upvoted 1 times

🗉  **Hodicek** 1 year, 10 months ago
AGREE WITH SNMPv3
upvoted 1 times

🗉  **bootloader_jack** 1 year, 11 months ago
It says "device monitoring". So the answers is D
upvoted 3 times

🗉  **dicksonpwc** 2 years 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

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 Address Aging : Disabled
Maximum MAC Addresses : 3
Total MAC Addresses : 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, 8 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 8 times

 **Sal34** Most Recent 1 year, 3 months ago

Selected Answer: AC


The answer is 100% a and c
upvoted 2 times

 **Hodicek** 1 year, 9 months ago

aging time is 5 minutes
sticky is automatically 2 MACs
upvoted 3 times

 **Hodicek** 1 year, 10 months ago

B-D-E ARE INCORRECT ANSWERS FOR SURE
upvoted 2 times

 **sp123** 1 year, 11 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, 11 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** 2 years, 1 month ago

I have a question - does the statically configured mac address also disappear after 5 mins of inactivity or just the two dynamically learned?



upvoted 2 times

  **DaBest** 1 year, 11 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, 4 months 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** 2 years, 1 month 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, 6 months ago

C state that it learned two MACs dynamically . Output showed Sticky MAC addresses : 2



upvoted 3 times

  **ttomer** 2 years, 7 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, 4 months ago

1) Configured means the 1 mac address that was statically configured

2) Sticky means the 2 dynamically learnt

upvoted 11 times

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, 5 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, 3 months 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, 6 months ago

This is horribly dated info. All modern sources will tell you that "shutdown" also generates a syslog message.
 upvoted 13 times

 **RougePotatoo** 10 months 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


 **davidmdl85** Most Recent 1 month, 2 weeks ago

The documentation is confusing, some of them says shutdown mode sends logs and snmp traps (official cert book from wendell odom book 2 chap 6 page 115) and other sites says the opposite like cisco catalyst configuration
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-10/configuration_guide/sec/b_1610_sec_9500_cg/b_1610_sec_9500_cg_chapter_0101010.html
 upvoted 1 times

 **[Removed]** 2 months, 1 week ago

Selected Answer: B

B. One secure MAC address is manually configured on the interface.
 Configured MAC addresses : 1
 upvoted 1 times

 **gachocop3** 1 year, 6 months ago

isn't A also correct because SNMP trap and Syslog message are generated in shutdown mode?
 upvoted 4 times

 **babaKazoo** 1 year, 8 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 3 times

🗨️ 👤 **sgashashf** 1 year, 6 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, 11 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, 4 months ago

Answer B is correct.

Restrict mode is the only one that generates syslog violation.

upvoted 2 times

🗨️ 👤 **Subit123** 2 years, 3 months 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, 3 months ago

yea the answer is both a and b. it should show select 2 answers.

upvoted 2 times

🗨️ 👤 **Sal34** 1 year, 3 months ago

After reading C3L4H1R's post. I think the answer is a.

upvoted 1 times

🗨️ 👤 **mrsiafu** 2 years, 4 months ago

this question is all over the place...

upvoted 3 times

🗨️ 👤 **MM_9** 2 years, 8 months ago

B is correct but also A?

upvoted 2 times

🗨️ 👤 **GHH** 1 year, 10 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, 7 months ago

I think A is also correct, (if there is a valid SNMP configuration)

upvoted 2 times

🗨️ 👤 **FloridaMan88** 2 years, 7 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** 2 years 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, 9 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 further investigation is needed; may be this is different among various IOS versions.

upvoted 1 times


```
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, 11 months ago

After Dynamic ARP Inspection is applied, by default the interface becomes untrusted.
upvoted 12 times

 **BooleanPizza** Highly Voted 2 years ago

Answer is correct, also to make this port trusted you need to add the 'ip arp inspection trust' command on int fa0/1
upvoted 9 times

 **LTTAM** Most Recent 2 years, 8 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, 10 months ago

"31 Days Before Your CCNA 200-301 Exam"

Page 192.

upvoted 6 times

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: `λI am a normal user. My username/password is user_tom/learnforeverλ€`
- ☞ Authorization: `λuser_tom can access LearnCCNA server via HTTP and FTPλ€`
- ☞ Accounting: `λuser_tom accessed LearnCCNA server for 2 hoursλ€. This user only uses λshowλ€ commands.`

 **dave1992** Highly Voted 1 year, 11 months ago

Authentication =who?
 Authorization= what are they allowed to do?
 Account= what did they do ?
 upvoted 12 times

 **ac89l** 4 months, 1 week 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 2 times

 **lilbaby2** Highly Voted 2 years, 11 months ago

Any type of authentication conversation means verifying "identity"
 upvoted 6 times

 **StingVN** Most Recent 3 months, 4 weeks 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

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 3 years, 2 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, 11 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 8 times

 **StingVN** Most Recent 3 months, 4 weeks 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

 **DUMPlodore** 7 months, 4 weeks ago

Selected Answer: BC

B. ASCII

C. hexadecimal

upvoted 2 times

DRAG DROP -

Drag and drop the AAA functions from the left onto the correct AAA services on the right.

Select and Place:

Answer Area

controls the actions that a user can perform	Authentication
provides analytical information for the network administrator	
records user activities	
restricts the services that are available to a user	Authorization
verifies the password associated with a user	
identifies the user	Accounting

Correct Answer:

Answer Area

controls the actions that a user can perform	Authentication
provides analytical information for the network administrator	verifies the password associated with a user
records user activities	identifies the user
restricts the services that are available to a user	Authorization
verifies the password associated with a user	controls the actions that a user can perform
identifies the user	restricts the services that are available to a user
	Accounting
	provides analytical information for the network administrator
	records user activities

 **distortion** Highly Voted  2 years, 2 months ago

This correct
upvoted 10 times

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, 6 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** 4 months, 1 week ago

what is dtp traffic?

upvoted 1 times

 **DoBronx** Highly Voted 10 months, 3 weeks ago

Selected Answer: CD

never use the default vlan and shut it down.

upvoted 5 times

 **StingVN** Most Recent 3 months, 4 weeks 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 2 times

 **cormorant** 10 months, 2 weeks ago

how i miss those questions from 2 years ago. the ccna used to be much easier back then

upvoted 1 times

 **DaBest** 1 year, 11 months ago

and i thought vlan 99 is the cisco faivourit for vlan management guess i was wrong ~_~

upvoted 2 times

 **Acai** 2 years, 4 months ago


I think they might be referring to a Black Hole Vlan as Maxiturne said.

upvoted 2 times

 **Nhan** 2 years, 6 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, 7 months ago

I assume Vlan 99 in the answer is a VLAN that is not used in production.

upvoted 2 times

 **uevenasdf** 2 years, 11 months ago

C,D - I think it's good practice to change the vlan and shut it down.

upvoted 2 times

🗨️ 👤 **Goldsmate** 3 years 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

🗨️ 👤 **Maxiturne** 3 years 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 number you want
upvoted 4 times

🗨️ 👤 **I_Ninja** 3 years ago

putting them in access mode and assigning them to an unused vlan is one of the steps to mitigate vlan hopping attacks
upvoted 12 times

🗨️ 👤 **SanchezEldorado** 3 years 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, 7 months ago

all ports are by default in Vlan 1, that is why putting them in another vlan protect the port, not being so easy to guess it
upvoted 2 times

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 "The webpage that opens reports that it was safe") so we believed it should be called a "user awareness" program. Therefore the best answer here should be "user awareness". This is the definition of "User awareness" from CCNA 200-301

Official Cert Guide Book:

"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."

Note: Physical access control means infrastructure locations, such as network closets and data centers, should remain securely locked.

 **Daimen** Highly Voted 3 years, 3 months ago

The correct answer is A.

D is a type of attack not a program

upvoted 16 times

 **myusername66** Highly Voted 3 years, 4 months ago

Correct Answer: D

upvoted 8 times

 **cant_stop_studying** 2 years, 6 months ago

The question asked for the type of security program, not type of attack. Correct Answer is A.

upvoted 7 times

 **CJ32** 3 years, 2 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 6 times

 **DUMPIedore** Most Recent 7 months, 4 weeks ago

Selected Answer: A

The correct answer is A.


upvoted 2 times

 **creaguy** 11 months, 2 weeks 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 4 times

 **Smaritz** 1 year, 5 months ago

Almost chose Social Engineering, but A is correct

upvoted 2 times

 **Shamwedge** 1 year, 9 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, 11 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, 12 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** 3 years, 2 months ago

This was worded oddly too and i admit i answered it wrong too, A is correct

upvoted 4 times

  **Cheban** 3 years, 2 months ago

The correct answer is A

upvoted 2 times

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

web policy	Layer 2 Security Mechanisms
Passthrough	
WPA+WPA2	Layer 3 Security Mechanisms (for WLAN)
802.1X	

Correct Answer:

Answer Area

web policy	Layer 2 Security Mechanisms
Passthrough	
WPA+WPA2	Layer 3 Security Mechanisms (for WLAN)
802.1X	

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 etc

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, 5 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, 5 months 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 4 times

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, 9 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 10 times


 **dropspablo** Most Recent 3 months, 2 weeks 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 2 times

 **StingVN** 3 months, 4 weeks 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, 4 months ago

SMH on wanting to talk to the main CPU.. I guess after all the other choices, x marks the spot!
upvoted 3 times

 **karemAbdullah** 2 years, 11 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, 11 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** 3 years, 1 month ago

any official link to elaborate the answer ?

upvoted 2 times

 **DannySprings** 3 years, 1 month ago

<https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109669-secure-wlc.html#t4>

upvoted 6 times

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 3 years, 2 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 22 times

  **johnny1234** Highly Voted 3 years, 3 months ago

Definition of multi-factor- something you know + sth you have

upvoted 7 times

  **Dataset** Most Recent 2 years, 2 months ago

"multifactor" is the magic word

Regards

upvoted 2 times

  **Boomhower** 2 years, 12 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 3 times

  **dave369** 3 years, 3 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, 3 months ago

Actually B C and D are all correct

upvoted 4 times

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 3 years, 1 month 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 30 times

 **mustafa007** Highly Voted 3 years ago

IOU2(config)#crypto key generate rsa

% Please define a domain-name first.

IOU2(config)#

upvoted 23 times

 **[Removed]** Most Recent 2 months, 2 weeks ago

You'll get this message if you try to generate an RSA key and don't define a domain name first :

SW1(config)#crypto key generate rsa general-keys modulus 1024

% Please define a domain-name first.

upvoted 1 times

 **[Removed]** 2 months, 2 weeks ago

Selected Answer: C

Assign a DNS domain name

ip domain name example-ccna.com

upvoted 1 times

 **all4one** 3 months, 2 weeks ago

Selected Answer: C

C is correct.

upvoted 1 times

 **StingVN** 3 months, 4 weeks 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 2 times

 **dropspablo** 3 months, 2 weeks ago

by chatgpt

upvoted 1 times

 **DUMPlodore** 7 months, 4 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

🗨️ 👤 **sassasasadsccadsca** 8 months 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 2 times

🗨️ 👤 **cormorant** 10 months, 2 weeks 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 2 times

🗨️ 👤 **Liuka_92** 1 year, 2 months ago

Use this trick to remember easy: DRUL

D: domain name R: rsa key U: username L: line vty

upvoted 5 times

🗨️ 👤 **Crazy** 2 years, 11 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, 4 months 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** 3 years, 1 month ago

I am guessing the "DNS domain name" is referring to step 4 below.

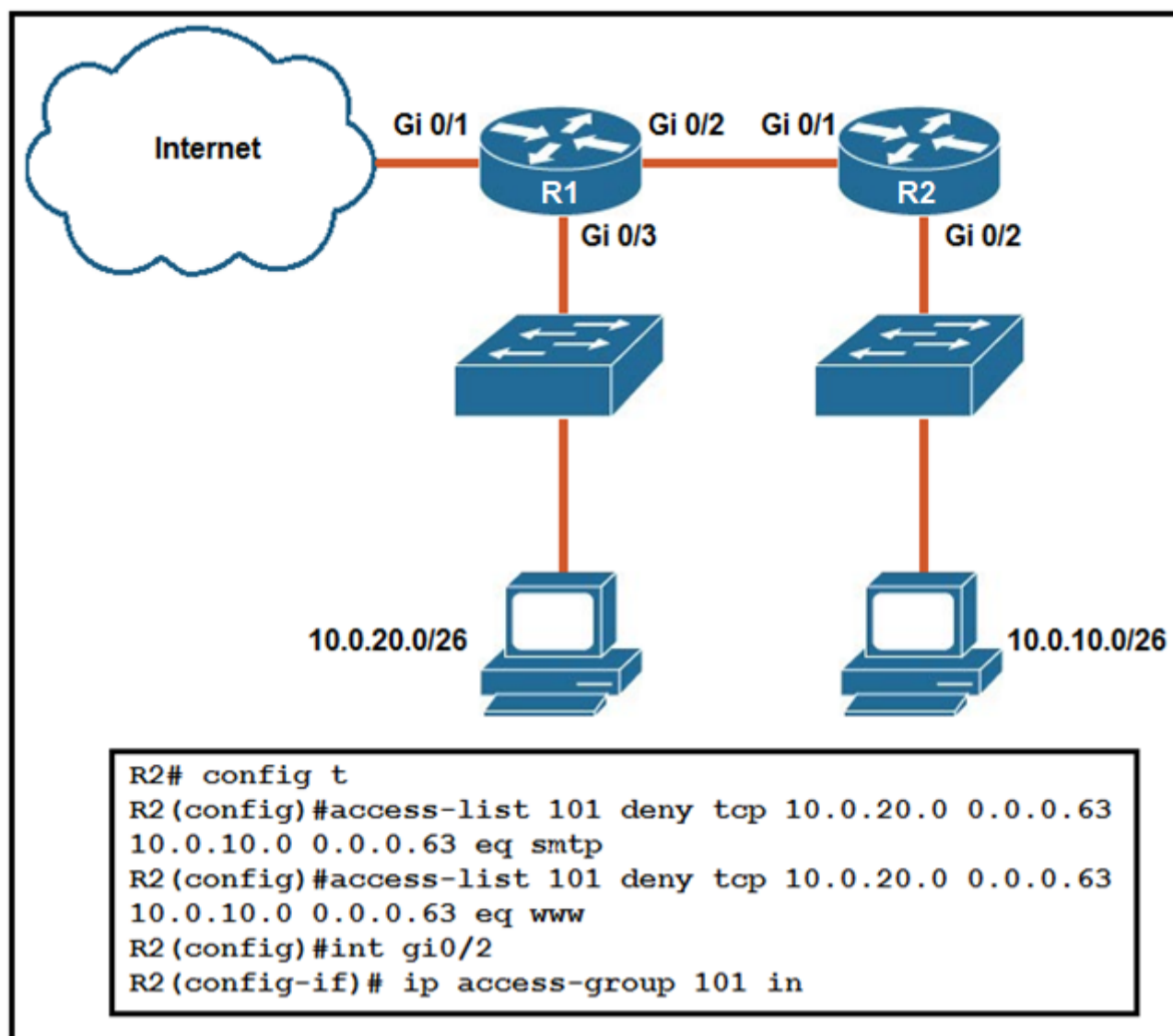
Configuring a Device for SSH Version 2 Using a Hostname and Domain Name

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 11 times



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 `permit ip any any` statement at the end of ACL 101 for allowed traffic.
- B. Add a `permit ip any any` 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, 8 months ago

Edit: forget, answer is OK. I misread.
upvoted 8 times

Njavwa Most Recent 5 months, 2 weeks 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 12 months ago

Selected Answer: AD

Can't be E because an extended access list needs to be closest to source
upvoted 2 times

[Removed] 1 year, 2 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 1 year, 2 months 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 2 times

🗨️ **guille_teleco** 1 year, 4 months 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, 5 months 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, 7 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, 8 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, 9 months ago

I think A, C are correct
upvoted 1 times

🗨️ **dave1992** 1 year, 9 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, 7 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, 11 months ago

I think A, C are correct
upvoted 2 times

🗨️ **Robin999** 2 years, 6 months ago

Correct Answers
upvoted 3 times

🗨️ **sinear** 2 years, 8 months ago

Wrong. Should be D E.
Extended should be moved close to the source of traffic, so here interface Gi0/2 on R2.

And ip should be swapped.

upvoted 4 times

  **Tintin_06** 2 years, 5 months 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** 11 months, 1 week ago

AES (key length:128, 192, 256 bytes. block> 128 bytes) is for WPA2
RC4 is for wep

upvoted 2 times

  **alexiro** 3 years, 1 month 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 4 times

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, 7 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 62 times

 **vadiminski** 2 years, 4 months ago

Absolutely correct
 upvoted 2 times

 **dave1992** 1 year, 11 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, 3 months ago

Yeah but DHCP snooping needs to be configured for DAI to work.
 upvoted 3 times

 **cybernett** Highly Voted 2 years, 6 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 3 months, 2 weeks 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 2 times

🗨️ 👤 **jorgenn** 1 year, 3 months 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, 4 months 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, 5 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, 6 months ago

the correct answer should be: the 1st and 4th are correct but the 2nd and 3rd should be swapped.

upvoted 6 times

🗨️ 👤 **sinear** 2 years, 8 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, 7 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 10 times

🗨️ 👤 **LTTAM** 2 years, 8 months ago

@sinear... that link actually gives the wrong answer.

The solution posted here is correct.

upvoted 1 times

🗨️ 👤 **JamesDean_Youldiots** 2 years, 3 months 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, 7 months ago

technically dhcp snooping mitigates man in the middle attacks!

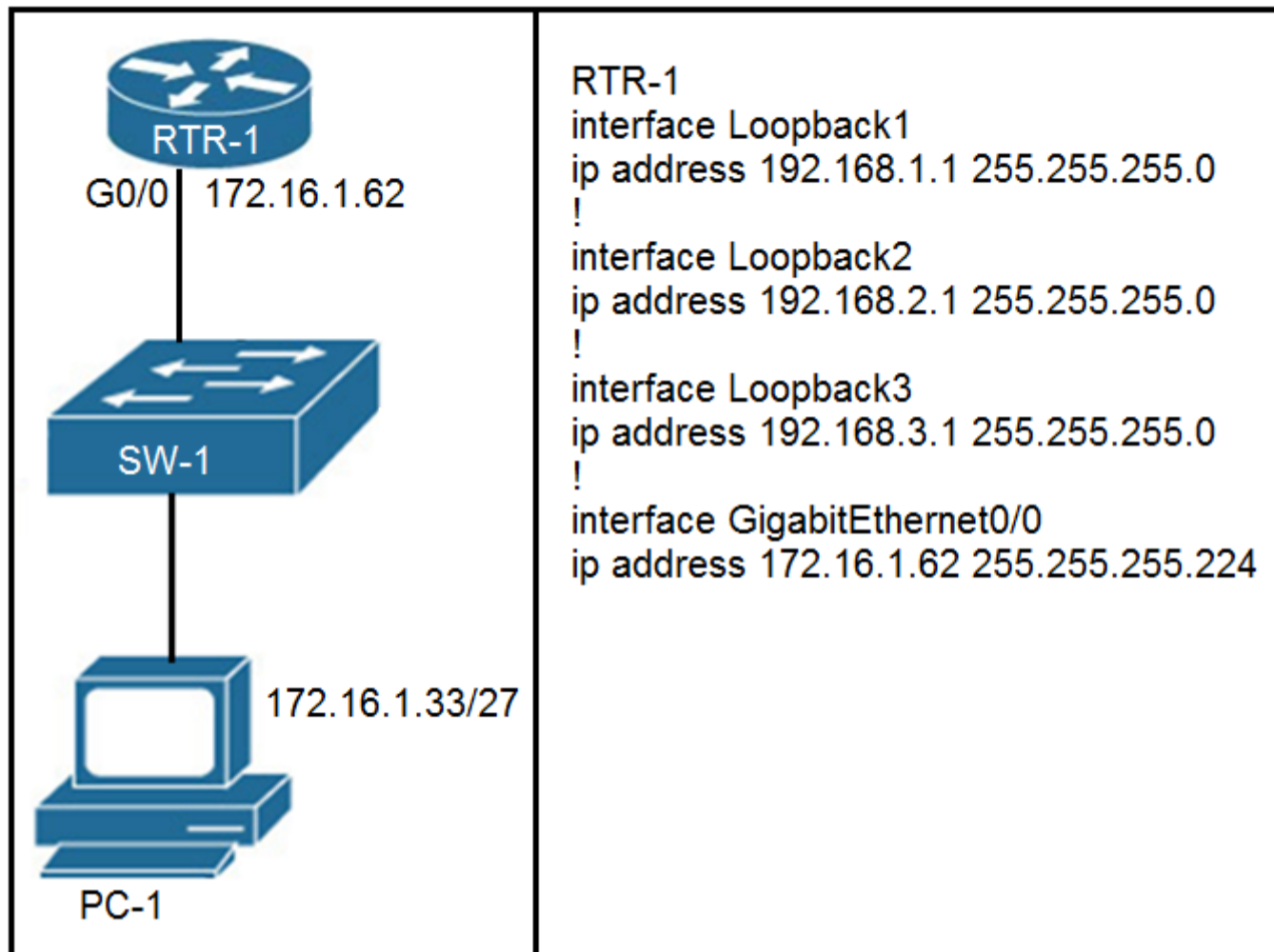
upvoted 1 times

🗨️ 👤 **Zerotime0** 2 years, 7 months ago

Thats what i chose

upvoted 1 times

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, 7 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 20 times

  **iGlitch** Highly Voted 1 year, 4 months 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 12 times

  **joeylam** 9 months, 1 week 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

  **Da_Costa** Most Recent 2 months, 2 weeks ago

B is correct because port 22 is ssh

upvoted 2 times

  **liviuml** 5 months 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** 3 months, 2 weeks 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 2 times

  **cormorant** 9 months 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** 1 year, 2 months ago

answer is A

upvoted 1 times

  **Hodicek** 1 year, 9 months ago


NO SORRY 1 FOR SSH AND OTHER FOR TELNET SO B IS CORRECT

upvoted 1 times

  **Hodicek** 1 year, 9 months ago

B - D ARE THE SAME AM I CORRECT?

upvoted 1 times

  **shakyak** 1 year, 9 months ago

No check the port number

upvoted 2 times

  **Belinda** 1 year, 6 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, 11 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, 7 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 vty lines.

upvoted 1 times

  **sgashashf** 1 year, 6 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, 4 months ago



whats the different between apply the ACL on the interface and on the vty line..

upvoted 2 times

  **Sten111** 2 years, 2 months ago



Question specifies any RTR1 interface

upvoted 2 times

  **ddino** 2 years, 5 months 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, 5 months 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** 2 years, 1 month 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 5 times

  **cortib** 1 year, 12 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, 7 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, 6 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, 7 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

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 broad, 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, 7 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 19 times

 **dave1992** Highly Voted 1 year, 11 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 14 times

 **GangsterDady** 1 year, 10 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, 8 months ago

So high means top of the access list not high in sequence number(making D an answer)?

upvoted 1 times

 **ds0321** Most Recent 4 weeks ago

Selected Answer: BE

options BE

upvoted 1 times

 **Cynthia2023** 1 month, 2 weeks ago

Selected Answer: BE

A can't be correct. and If a permit statement in the access list is too broad and matches more packets than intended, all incoming packets may be allowed, even though an ACL is applied to the interface.

upvoted 1 times

 **RODCCN** 1 month, 3 weeks ago

Selected Answer: AE

"The behavior for access-class when the specified access list is empty (or does not exist) has changed over time. In some (quite early) versions of IOS the default behavior was followed and all traffic was denied. In most versions of IOS (in its various flavors) has been that an empty (or non-existent) access list results in all traffic being permitted."

Link: <https://community.cisco.com/t5/routing/empty-access-list/td-p/630883>

upvoted 1 times

 **xbololi** 2 months, 1 week ago

Selected Answer: AE

"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."

<https://community.cisco.com/t5/routing/apply-empty-acl-what-happens/td-p/740473#:~:text=If%20you%20use%20ip%20access,empty%20ACL%20would%20deny%20traffic.>

upvoted 1 times

🗨️ **[Removed]** 2 months, 2 weeks ago

Selected Answer: BE

Answers B and E
upvoted 1 times

🗨️ **Dunedrifter** 2 months, 2 weeks ago

Selected Answer: BE

Not A. An empty ACL contains an explicit deny statement at the end. It will drop all traffic.
upvoted 1 times

🗨️ **Peter_panda** 5 months ago

Selected Answer: AE

<https://community.cisco.com/t5/routing/apply-empty-acl-what-happens/td-p/740473>
upvoted 1 times

🗨️ **krzysiew** 5 months, 2 weeks ago

a) ACL is empty - if acl is empty its mean all traffic is deny
upvoted 1 times

🗨️ **krzysiew** 5 months, 2 weeks ago

B and E
upvoted 1 times

🗨️ **Ciscoman021** 5 months, 3 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

🗨️ **DUMPladore** 7 months, 4 weeks ago

Selected Answer: BE

I go for BE
upvoted 1 times

🗨️ **Etidic** 10 months, 3 weeks ago

Selected Answer: BE

A and E are correct
upvoted 1 times

🗨️ **ptfish** 1 year, 1 month 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, 4 months 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, 8 months ago

A & E are correct answer
upvoted 1 times

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

 **dropspablo** 3 weeks, 2 days ago

Answer A is correct.

From what I understand, the letter "B" seems right, but it is "wrong", because even using the "service password-encryption" command, the "enable password" or "username password" settings are configured in "clear text", but only in shown in the running-config with an encryption weak (type 7).

The main purpose of the "service password-encryption" command is to prevent passwords from being displayed in plain text in the device configuration, protecting them from casual viewing (by an unauthorized user).

upvoted 1 times

 **ROCCN** 1 month, 3 weeks ago

Selected Answer: A

All passwords configured on an IOS device, with the exception of the passwords configured with enable secret password, are stored in clear-text in the device configuration file. This means that all that attacker needs to do to find out the passwords is to run the show running-config command.

LINK: <https://geek-university.com/service-password-encryption-command/>

upvoted 1 times

 **krzysiew** 5 months, 2 weeks ago

i think the answar is B

upvoted 1 times

 **sovafal192** 1 year, 7 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** 11 months, 2 weeks ago

the service does only encrypt existing passwords therefor the admin is still able to configure unencrypted password

upvoted 1 times

 **dropspablo** 3 weeks, 2 days ago

I tested it on Packet Tracert and with the "service password-encryption" command enabled, the passwords in "clear-text" will be encrypted, both the current ones and those configured afterwards. But answer A is correct.

upvoted 1 times

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 3 years, 1 month 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, 4 months 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 11 times

 **Cynthia2023** Most Recent 1 month ago

Selected Answer: A

bad wording though.

SAE (Simultaneous Authentication of Equals) is not a method of encryption itself; rather, it's an authentication method used in WPA3 (Wi-Fi Protected Access 3) to establish a secure connection between a wireless client and an access point.

SAE addresses the security vulnerabilities of traditional pre-shared keys (PSKs) used in WPA and WPA2. Instead of relying solely on a static passphrase, SAE uses a more robust and secure key exchange process to prevent various types of attacks, including offline dictionary attacks and brute-force attacks.

The actual encryption method used in WPA3 is typically AES (Advanced Encryption Standard), which provides the encryption and confidentiality of data transmitted over the network.


To clarify, SAE enhances the authentication process to protect against attacks on the initial key exchange, while AES provides the encryption of the data itself.

upvoted 1 times

 **dorf05** 2 months ago

answer; D


upvoted 1 times

 **Eallam** 2 months, 1 week ago

Selected Answer: D


AES is the right Answer here, the question is CLEARLY asking about Traffic, not about the Authentication method, SAE is used for securing Authentication, while the traffic itself is secured by AES

upvoted 1 times

 **Eallam** 2 months, 1 week ago

SAE is for key exchange, the question here asks about traffic, AES is used for traffic encryption D is the Answer

upvoted 1 times

 **Ciscoman021** 5 months, 3 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** 8 months, 2 weeks ago

Selected Answer: A

WPA3 uses simultaneous authentication of equals (SAE) encryption



upvoted 1 times

  **AWSEMA** 1 year, 2 months 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, 9 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, 4 months ago

Nse SAE

upvoted 4 times

  **mrsiafu** 2 years, 4 months 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, 4 months ago



Definitely not in the OCG

upvoted 3 times

  **UmbertoReed** 1 year, 11 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, 10 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

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, 8 months ago

Selected Answer: C

The correct answer should be C.
upvoted 5 times

 **anchiling** Most Recent 23 hours, 9 minutes ago

why not access point?
upvoted 1 times

 **RODCCN** 1 month, 3 weeks ago

Selected Answer: C

In a typical network configuration, you configure all switch ports connected to host ports as untrusted and configure all switch ports connected to switches as trusted. With this configuration, all ARP packets entering the network from a given switch bypass the security check. No other validation is needed at any other place in the VLAN or in the network. You configure the trust setting by using the ip arp inspection trust interface configuration command.


LINK: <https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/www.cisco.com/content/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/dynarp.html.xml>

upvoted 1 times

 **AWSEMA** 1 year, 1 month ago

Selected Answer: C

ROUTER !!!
upvoted 1 times

 **ratu68** 1 year, 2 months ago


Selected Answer: C

Has to be a network device to be trusted.

Answer is C
upvoted 4 times

 **AWSEMA** 1 year, 2 months ago

router
upvoted 1 times

 **snrov** 1 year, 5 months ago

Selected Answer: C

I swear it is C
upvoted 3 times

 **ismatdmour** 1 year, 5 months ago

Selected Answer: C

Definitely 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, 8 months ago

Selected Answer: C

definitely its C

upvoted 3 times



  **Cho1571** 1 year, 8 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, 8 months ago

Selected Answer: C



trusting static assigned address

upvoted 1 times

  **RichyES** 1 year, 8 months ago

C is the answer

upvoted 1 times

  **gaber** 1 year, 8 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, 8 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

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, 4 months 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 34 times

 **Jong12** 1 year, 11 months ago


SW2 and SW3 has the same configuration how can C be right and B not?
upvoted 1 times

 **Pkard** 1 year, 10 months ago


SW2 uses "password" and SW3 uses "secret".
I didn't see it at first either
upvoted 3 times

 **Pkard** 1 year, 10 months ago

"password" is stored as plain text and does not meet the requirements of the question
upvoted 2 times

 **dave1992** 1 year, 11 months ago

both are correct. its the same answer
upvoted 1 times

 **Belinda** 1 year, 6 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 5 months, 2 weeks ago

Selected Answer: C

Answer C is correct

upvoted 1 times

  **Adaya** 2 years, 2 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  2 years 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, 3 months ago



so true

upvoted 2 times

  **aosroyal** 1 year, 5 months ago

this does not help at all

upvoted 5 times

  **aosroyal** 1 year, 5 months ago

this does not help at all

upvoted 4 times

  **RODCCN** Most Recent  1 month, 3 weeks ago

Selected Answer: A

Untrusted Ports: ARP packets received on untrusted ports are subject to DAI inspection. DAI checks each ARP packet against the binding table to verify the source IP-MAC binding. If a packet fails the check, it is considered potentially malicious, and DAI can take actions to mitigate the threat.

upvoted 1 times

  **sasquatchshrimp** 1 year, 1 month 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 2 times

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 3 years, 1 month 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.

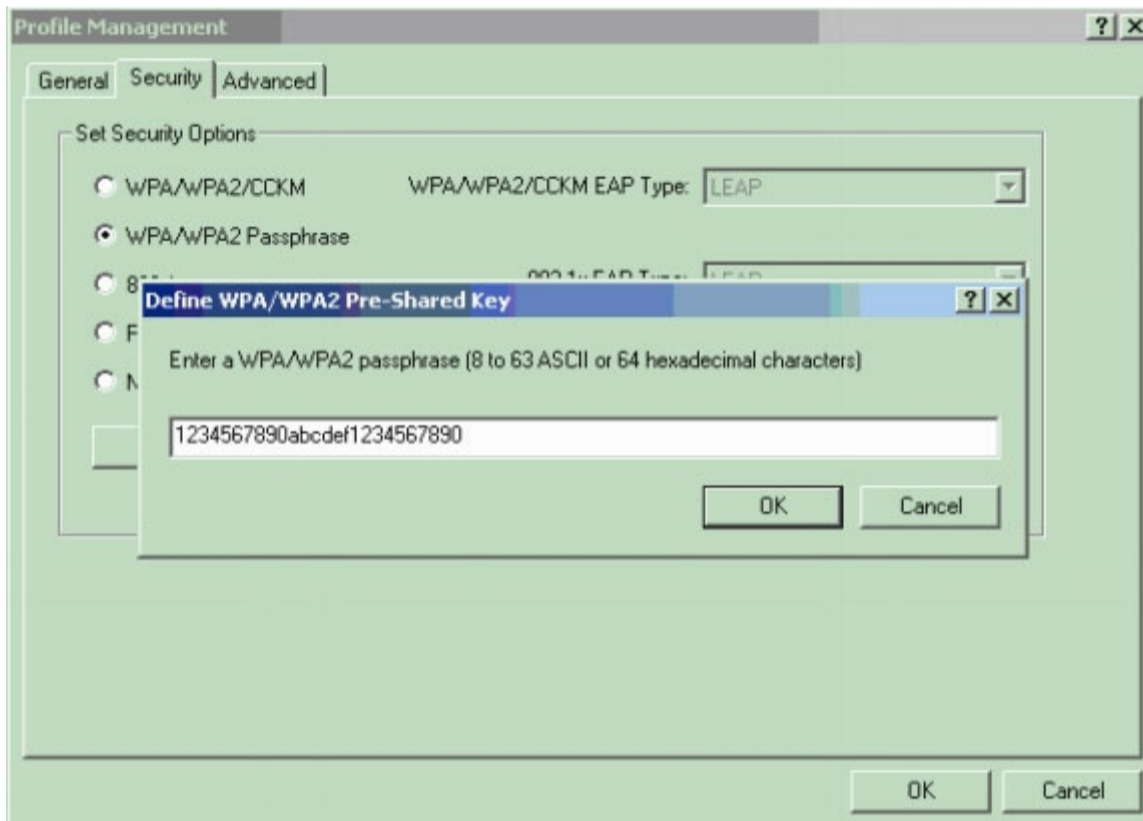
upvoted 10 times

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, 5 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 9 times

RougePotatoe 10 months, 2 weeks ago

Here is a link that supports this comment.

upvoted 2 times

RougePotatoe 10 months, 2 weeks ago

<https://www.cwnp.com/forums/posts?postNum=299964>

upvoted 3 times

Aleksoo Most Recent 6 days, 19 hours ago

This is from Boson CourseWare: WPA2, which implements the 802.11i wireless standard, was developed to address the security vulnerabilities in the WPA standard. One enhancement over WPA included in WPA2 is the encryption algorithm. Advanced Encryption System (AES) is a stronger encryption algorithm than the RC4 algorithm used by both WEP and WPA. AES uses a 128-bit block cipher to encrypt data and a security key of 128, 192, or 256 bits.

upvoted 1 times



RODCCN 1 month, 3 weeks ago

Selected Answer: A

WPA2 mandates the use of a new protocol, counter mode with cipher-block chaining message authentication protocol (CCMP). CCMP uses the AES block cipher, replacing the RC4 cipher used in wired equivalent privacy (WEP) and temporal key integrity protocol (TKIP). A block cipher processes data in blocks, while a streaming cipher like rivest cipher 4 (RC4) processes data bit by bit, in a serial stream. The encryption method is commonly referred to as CCMP/AES. AES uses a 128-bit key and encrypts data in 128-bit blocks. CCMP/AES uses several enhancements, including temporal keys (TK), packet numbers (PN), nonce [number or bit string used only once], upper layer encryption, and additional authentication data (AAD).

LINK: <https://www.controleng.com/articles/wireless-security-ieee-802-11-and-cmp-aes/>

upvoted 1 times

  **[Removed]** 2 months, 1 week ago

Selected Answer: A

A. AES-128

upvoted 1 times

  **ac89l** 4 months ago

Selected Answer: A

A is correct

upvoted 1 times

  **AWSEMA** 1 year, 1 month ago

Selected Answer: A

A ==>>>> AES-128 is used.



upvoted 4 times

  **lock12333** 1 year, 3 months ago

Selected Answer: C

cccccccccccccccccccccccccccccccccccc



upvoted 1 times

  **iGlitch** 1 year, 3 months ago

Selected Answer: A

AES-128 is used.



upvoted 2 times

  **Pkard** 1 year, 9 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, 11 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

upvoted 1 times

  **DaBest** 1 year, 11 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"

based 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

upvoted 2 times

  **Pkard** 1 year, 9 months ago

Right, it's still 128-bit encryption

upvoted 2 times

  **DaBest** 1 year, 11 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](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

upvoted 2 times

  **Joe_Q** 2 years, 5 months 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, 6 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

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

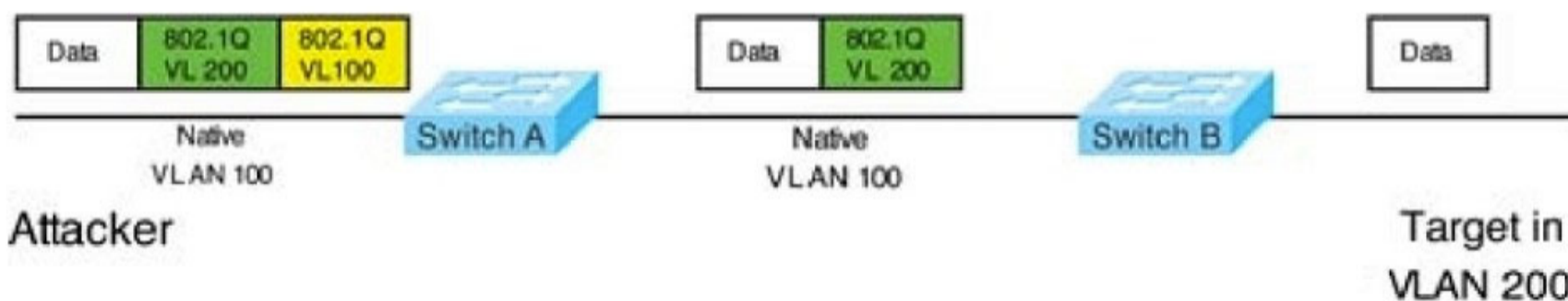
Configure BPDU guard.	802.1q double tagging
Configure dynamic ARP inspection.	ARP spoofing
Configure root guard.	unwanted superior BPDUs
Configure VACL.	unwanted BPDUs on PortFast-enabled interfaces

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 100 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.

configure BPDU guard: unwanted BPDUs on PortFast-enabled interfaces
Configure dynamic ARP inspection: ARP spoofing
Configure root guard: unwanted superior BPDUs
Configure VACL: 802.1q double tagging
upvoted 1 times

 **Paulo231** 2 months, 3 weeks ago
Mabuhay
upvoted 1 times

 **juneq888** 5 days, 11 hours ago
mini miss u! mini miss u!
upvoted 1 times

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, 7 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 21 times

 **salami** 1 year, 11 months ago

quite right, but service password encryption does weak encryption, it doesnt store them as hashed values

upvoted 2 times

 **RODCCN** Most Recent 1 month, 3 weeks ago

Selected Answer: C

The first method of encryption that Cisco provides is through the command service password-encryption. This command obscures all clear-text passwords in the configuration using a Vigenere cipher. You enable this feature from global configuration mode.

Router#config terminal

Router(config)#service password-encryption

LINK: <https://www.oreilly.com/library/view/hardening-cisco-routers/0596001665/ch04.html>

upvoted 1 times

 **Etidic** 10 months, 3 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.

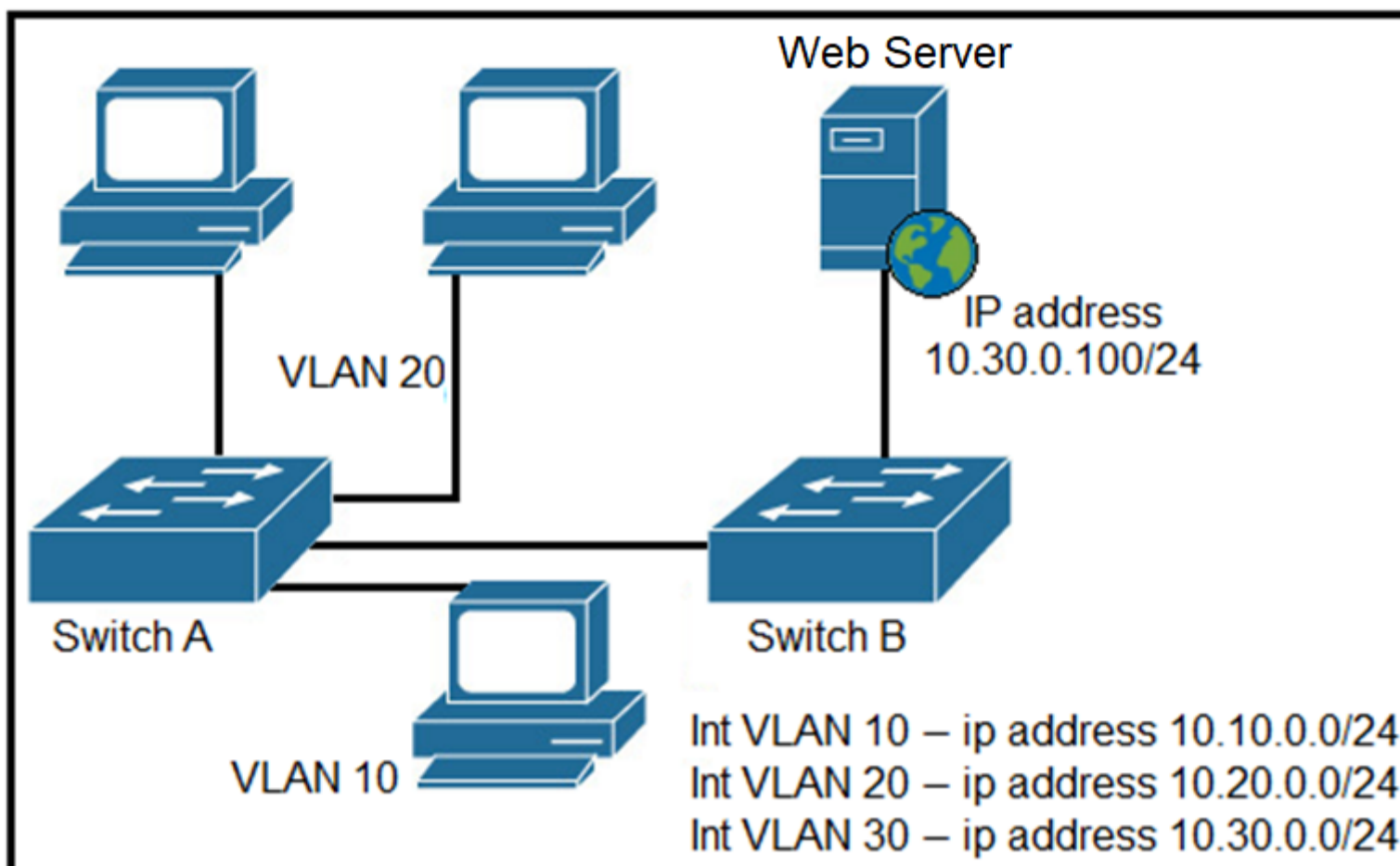
upvoted 4 times

 **BieLey** 11 months, 2 weeks ago

Selected Answer: C

Keyword = Prevent passwords

upvoted 2 times



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, 7 months ago

Sorry, D is correct, but not the best way to address this.
upvoted 18 times

Belinda 1 year, 6 months ago

Thanks
upvoted 1 times


ZayaB Highly Voted 2 years, 6 months ago

I agree with you Ali526. Not a good way to implement this ACL.
upvoted 5 times

  **dave1992** Most Recent 1 year, 9 months ago



if were blocking all traffic in vlan 20. would the acl include .20 and not .30???

upvoted 3 times

  **Aleks123** 1 year, 8 months ago

Hey Dave I believe its a typo your right!

upvoted 3 times

  **bitree** 1 year, 4 months 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

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 11 months, 3 weeks ago

stupid question
upvoted 17 times

  **Scipions** Highly Voted 2 years, 4 months ago

qwerty, admin, 12345678
upvoted 11 times

  **Bash2111** Most Recent 1 year, 3 months ago

A and E is correct
upvoted 2 times

  **VictorCisco** 5 months, 3 weeks 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 2 times

  **Vinarino** 1 year, 8 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, 4 months 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, 5 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 4 times

  **Ali526** 2 years, 8 months ago

A is correct. E assumes that administrator know the compromised computer. How is that going to happen?
upvoted 3 times

  **sinear** 2 years, 8 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

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, 9 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 10 times

 **Nicocisco** 1 year, 6 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** 10 months, 2 weeks 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, 6 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 5 months, 3 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, 9 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** 1 year, 2 months ago

confirmed according to what?

upvoted 1 times

 **Hodicek** 1 year, 9 months ago

A IS CORRECT ANSWER

upvoted 2 times

 **XBfoundX** 2 years, 8 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 default 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, 8 months ago

Isnt it easy here that all others except A , gave options about outside networks?

upvoted 1 times

 **Mhatz** 2 years, 10 months ago

I thought answer is D.

upvoted 3 times

  **illuded03jolted** 1 year, 3 months ago

private address "allows communicating across public network boundaries"??? Stop smoking funny stuff bruuh!
upvoted 2 times

  **WikiLips** 2 years, 10 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, 4 months 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

  **RODCCN** Most Recent  1 month, 3 weeks ago

Selected Answer: C

Dynamic ARP Inspection (DAI) is a security feature used to protect against ARP (Address Resolution Protocol) spoofing attacks in a local network. ARP is used to map IP addresses to MAC addresses in a network. In an ARP spoofing attack, an attacker sends fake ARP messages to associate a different MAC address with an IP address, leading to network disruption or interception of traffic.
upvoted 1 times

  **Bash2111** 1 year, 3 months ago

An ARP spoofing, also known as ARP poisoning, is a Man in the Middle (MitM) attack
upvoted 1 times

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, 5 months ago

The answer is D



A:- this is used for site to site VPN

upvoted 9 times

  **Rramos37** Most Recent 1 year, 11 months ago

Yes, D

upvoted 2 times

  **Alsaheer** 2 years, 4 months ago

D is correct

upvoted 3 times

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, 9 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 8 times

 **Eyan** Highly Voted 1 year, 12 months ago

checked and it is correct answers DE
upvoted 7 times

 **RODCCN** Most Recent 1 month, 3 weeks ago

Selected Answer: DE

Port-based authentication = 802.1x (RADIUS/TACACS+) - IEEE 802.1X port-based authentication is configured on a device to prevent unauthorized devices (supplicants) from gaining access to the network. The device can combine the function of a router, switch, and access point, depending on the fixed configuration or installed modules. The switch functions are provided by either built-in switch ports or a plug-in module with switch ports. This feature supports both access ports and trunk ports.

LINK: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/x3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

upvoted 1 times

 **raydel92** 1 year, 9 months ago

Selected Answer: DE

This might help:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/x3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html

upvoted 3 times

```

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 2 years, 2 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, 11 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

 **Shabeth** Most Recent 2 months, 1 week ago

Selected Answer: D

D is correct
upvoted 1 times


 **rmartin3444** 6 months ago

Shouldn't the wild card mask end in .127?
upvoted 3 times

 **splashy** 11 months, 4 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, 5 months 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, 9 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, 10 months ago

Why B is not correct?
upvoted 3 times

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

 **highfivejohn** Highly Voted 11 months ago

Selected Answer: C

C is best answer, had the question included the port err-disabled then D
upvoted 8 times

 **[Removed]** Most Recent 2 months, 1 week ago

Selected Answer: C

C. switchport port-security violation restrict
"restrict" will increment the security-violation count and forward an SNMP trap
upvoted 1 times

 **AlvinSK0814** 10 months 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 2 times

 **RougePotatoe** 10 months ago

The question didn't say anything about the port being shut down what makes you so sure it's D?
upvoted 6 times

 **creaguy** 11 months, 2 weeks 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** 10 months, 1 week 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 reenble it by entering the shutdown and no shut down interface configuration commands. This is the default mode.

upvoted 4 times

 **swampfartz** 1 year, 5 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, 11 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, 6 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, 11 months ago

C is correct, only Restrict will send a syslog/SNMP by default

upvoted 3 times

  **Chupacabro** 1 year, 8 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

  **RODCCN** 1 month, 3 weeks ago

Selected Answer: C

VLAN Hopping is an attack where the attacker is able to send traffic from one VLAN into another, one of the attacks is the "Double Tagging".
To prevent a Double Tagging attack, keep the native VLAN of all trunk ports different from user VLANs.



LINK: <https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation>

upvoted 1 times

  **dorf05** 2 months ago

Correct answer: B.... When using VACL

upvoted 2 times

  **Gauain** 2 months, 2 weeks ago

howwwwwwwww

upvoted 1 times

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, 3 months 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 16 times

 **raydel92** Highly Voted 1 year, 9 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 6 times

 **RODCCN** Most Recent 1 month, 3 weeks ago


Selected Answer: D

A switch maintains DHCP snooping information in its DHCP snooping binding table. The DHCP snooping binding table is a dynamic database that the switch uses to keep track of DHCP bindings between IP addresses and MAC addresses on the network.

When DHCP snooping is enabled on a switch, the switch monitors DHCP traffic between DHCP clients (devices that request IP addresses) and DHCP servers (devices that assign IP addresses). It examines the DHCP packets and extracts information such as the source MAC address, IP address, VLAN, and lease time.

The DHCP snooping binding table is then populated with these DHCP bindings, associating MAC addresses with IP addresses and the corresponding VLANs. This information helps the switch in forwarding DHCP traffic correctly to ensure that DHCP clients receive their assigned IP addresses and that unauthorized DHCP servers are blocked.

upvoted 1 times

 **cormorant** 9 months, 1 week 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, 11 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** 2 years ago

D is correct.

<https://community.fs.com/blog/what-is-dhcp-snooping-and-how-it-works.html>

upvoted 3 times

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 2 years 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 18 times

 **RODCCN** Most Recent 1 month, 3 weeks ago

Selected Answer: D

The command crypto key generate rsa modulus 1024 is used to generate an RSA (Rivest-Shamir-Adleman) key pair with a modulus of 1024 bits on a networking device, such as a router or a switch. The RSA key pair consists of a public key and a private key.

RSA Key Pair:

Public Key: The public key is used for encryption and is distributed to other devices in the network. It is used by other devices to encrypt data that can only be decrypted by the private key holder.

Private Key: The private key is used for decryption and is kept secure on the device that generated the key pair. It is used to decrypt data that was encrypted using the corresponding public key.

Purpose and Usage:

The generated RSA key pair is primarily used for securing communication and ensuring the integrity and confidentiality of data in network devices.

upvoted 1 times

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, 5 months ago

ASCII and Hex

upvoted 9 times

```

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, 11 months ago

there is no ssh entry in the table. I did not understand the answer.
upvoted 19 times

 **dropspablo** 3 weeks, 2 days ago

Remember: Among the keywords "eq ssh" does not exist, only "eq telnet". to configure ssh in the ACL we must use only its port number "eq 22".
Answer correct is A.
upvoted 2 times

 **kadamske** 1 year, 11 months ago

Me neither
upvoted 4 times

 **kokoyul** Highly Voted 1 year, 11 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 15 times

 **testsssssss** 1 year, 7 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 6 times

 **Dxpod** Most Recent 1 month ago

Selected Answer: A

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)
upvoted 1 times

 **Stevens0103** 1 month, 3 weeks ago

Selected Answer: A

By default, VTY lines allow remote access to a router without any restrictions, which can pose a security risk. However, by configuring and applying an access control list (ACL) to the VTY lines, you can control which IP addresses or networks are allowed or denied access to the router via Telnet or SSH. So, the ACL itself is a way of securing vty access, be it telnet or ssh. Since 'eq ssh' isn't a valid parameter, the answer should be A.
upvoted 2 times

 **Paulo231** 2 months, 3 weeks ago

Keyword SSH access: "live vty 0 15" configuration

upvoted 1 times

 **Da_Costa** 3 months ago


The key point is securing vty access

upvoted 1 times

 **ac89l** 4 months ago

another horrible question

upvoted 3 times

 **Njavwa** 5 months, 2 weeks 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 2 times

 **Yaqub009** 7 months, 1 week 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

 **RODCCN** 1 month, 3 weeks ago

You right, my friend. This is the list of port numbers to names that can be used:

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current Assigned Numbers RFC to find a reference to these protocols. You can find port numbers corresponding to these protocols by typing a ? in the place of a port number.

bgp
chargen
cmd
daytime
discard
domain
echo
exec
finger
ftp
ftp-data
gopher
hostname
ident
irc
klogin
kshell
login
lpd
nntp
pim-auto-rp
pop2
pop3
smtp
sunrpc
tacacs
talk
telnet
time
uucp
whois
www

LINK: https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-0/addr_serv/command/reference/ir40asrbook_chapter1.html

upvoted 1 times

 **splashy** 11 months 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** 11 months, 2 weeks 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** 11 months, 3 weeks ago


pay attention to 'securing'
upvoted 2 times

  **Amonzon** 1 year, 1 month ago

See the exhibit the TELNET is configured it is just missing SSH. Correct answer is D
upvoted 3 times

  **GohanF2** 1 year, 1 month 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** 1 year, 2 months 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 10 times

  **WINDSON** 1 year, 2 months ago

Answer A has been already in the configured in the list before. So how can use choose answer A ?
upvoted 4 times

  **DARKK** 1 year, 4 months ago

"Which access list *Entry* ..."

A lot of people misunderstood this question, securing mean you should Add ssh 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

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, 9 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

  **Cynthia2023** Most Recent 1 month, 4 weeks ago

<https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/datasheet-c78-742434.html> TFTP isn't used for WLC management connections.
upvoted 1 times

  **cortib** 1 year, 12 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

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 👍 2 years 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, 4 months 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, 7 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, 7 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 2 times

🗨️ 👤 **DaBest** 1 year, 11 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

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, 9 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 9 times

  **Cynthia2023** Most Recent 1 month ago

Selected Answer: B

DHCP snooping is a security feature in networking that helps prevent unauthorized or malicious DHCP servers from distributing incorrect IP addresses or configurations to network clients. One of its functions is to rate-limit certain DHCP traffic to protect against potential DHCP-based attacks. This helps ensure the integrity and security of the DHCP process within the network.

upvoted 1 times

  **Shabeth** 2 months, 1 week ago

Selected Answer: B

B.

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.

upvoted 1 times

  **[Removed]** 2 months, 1 week ago

Selected Answer: B

B. rate-limits certain traffic

upvoted 1 times

  **VictorCisco** 5 months, 3 weeks 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 denial 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 2 times

  **leoel** 8 months, 4 weeks ago

Selected Answer: B

answer is B

upvoted 2 times

  **SONG0092** 1 year, 5 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 4 times

  **sovafal192** 1 year, 7 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, 12 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** 2 years 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 3 times

🗨️ 👤 **Samuelpn96** 2 years ago

I think the answer is D (provides DDoS mitigation). One of the attacks that it prevents is DHCP Starvation attack, which is a denial 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 4 times

🗨️ 👤 **ccna_goat** 11 months ago

DHCP helps prevent man-in-the-middle attacks, not DDoS
upvoted 2 times

🗨️ 👤 **kadamske** 1 year, 11 months ago

The answer is not D because that is "DDOS" Distributed Denial Of Service, it is difference from just DOS
upvoted 5 times

🗨️ 👤 **Samuelpn96** 1 year, 11 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

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:

configure terminal	first
enable	second
enable secret \$hf!@4fs	third
exit	fourth
line vty 0 4	
service password-encryption	

Correct Answer:

configure terminal	enable
enable	configure terminal
enable secret \$hf!@4fs	enable secret \$hf!@4fs
exit	exit
line vty 0 4	
service password-encryption	

sasquatchshrimp (Highly Voted) 1 year, 1 month ago

No one:
Cisco: A guy is doing something, what are the exact steps and order?
upvoted 22 times

kamlo 9 months, 2 weeks ago

Hahahaha ggggggggggold :D
upvoted 2 times

CozTurk (Highly Voted) 1 year, 11 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

Shabeth (Most Recent) 2 months, 1 week ago

answers are correct
upvoted 1 times

iGlitch 1 year, 3 months ago


TRICKY, but the answers are correct.

upvoted 3 times

  **DARKK** 1 year, 4 months ago

Unless the user database includes user name and pwd , Enable secret is correct.

upvoted 1 times

  **aosroyal** 1 year, 5 months ago

bad qn

upvoted 4 times

  **SONG00992** 1 year, 5 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, 7 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** 10 months, 2 weeks ago

Incorrect, if you configure privilege level 15 it gets them directly to the user exec status.

upvoted 1 times

  **cdp_neighbor** 8 months, 4 weeks ago

Nope, unless you've configured "aaa authorization exec"

upvoted 1 times

  **awashenko** 1 year, 8 months ago

Enable, Config T, Enable Secret, Exit.


Service Password-Encryption encrypts plain text.

upvoted 4 times

  **Cho1571** 1 year, 8 months ago



you need the 4 steps plus the enable secret right before exit (and exit is optional)

upvoted 1 times

  **Hodicek** 1 year, 9 months ago

ENABLE - CONF T - ENABLE SECRET - EXIT

upvoted 4 times

  **Lala4eva** 1 year, 10 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** 2 years ago

Here we are talking bout encrypted password for enable mode so it should be enable secret command.

upvoted 5 times

  **WHTM** 2 years ago

'local user database has already been configured'

Correct answer

upvoted 1 times

  **stanibarb** 1 year, 11 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** 2 years ago

this doesn't seem correct

upvoted 2 times

  **django1001** 2 years 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

  **DARKK** Highly Voted 1 year, 4 months ago

Facilities is the key word here, as it is solely Physical, the other options can be breached via the network as well.
upvoted 7 times

  **nickname_fordiscussions** Highly Voted 1 year, 5 months ago

A B and D smh
upvoted 5 times

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 1 year, 1 month ago

Leave it to cisco to use terminology that engineers of many years have never heard or used... smh
upvoted 15 times

 **Phonon** Highly Voted 8 months, 2 weeks 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 9 times

 **StingVN** Most Recent 3 months, 3 weeks ago

Selected Answer: D

should be D
upvoted 1 times

 **4aynick** 5 months, 1 week ago

no CCNA scope
upvoted 1 times

 **[Removed]** 2 months, 2 weeks ago

Yes, this question is a CCNA 200-301 one
upvoted 1 times

 **nathnotnut** 6 months, 2 weeks ago

black hole lang ni enigma alam ko e
upvoted 2 times

 **Garfieldcat** 11 months, 1 week 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** 1 year, 1 month ago

unused so goes directly to Black hole.
upvoted 1 times

 **AWSEMA** 1 year, 2 months 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, 7 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

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, 9 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 20 times

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, 8 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 " multicast ability and security"

upvoted 16 times


 **dicksonpwc** Highly Voted 2 years 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 7 times

 **gaber** 1 year, 8 months ago

<https://kb.juniper.net/InfoCenter/index?page=content&id=KB19372>


upvoted 1 times

 **StingVN** Most Recent 3 months, 3 weeks ago

Selected Answer: D

D is the correct answer

upvoted 1 times

 **Ciscoman021** 5 months, 3 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** 8 months, 2 weeks 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, 4 months ago

This video gives a good explanation

<https://www.youtube.com/watch?v=ytAqv7qHGyU>

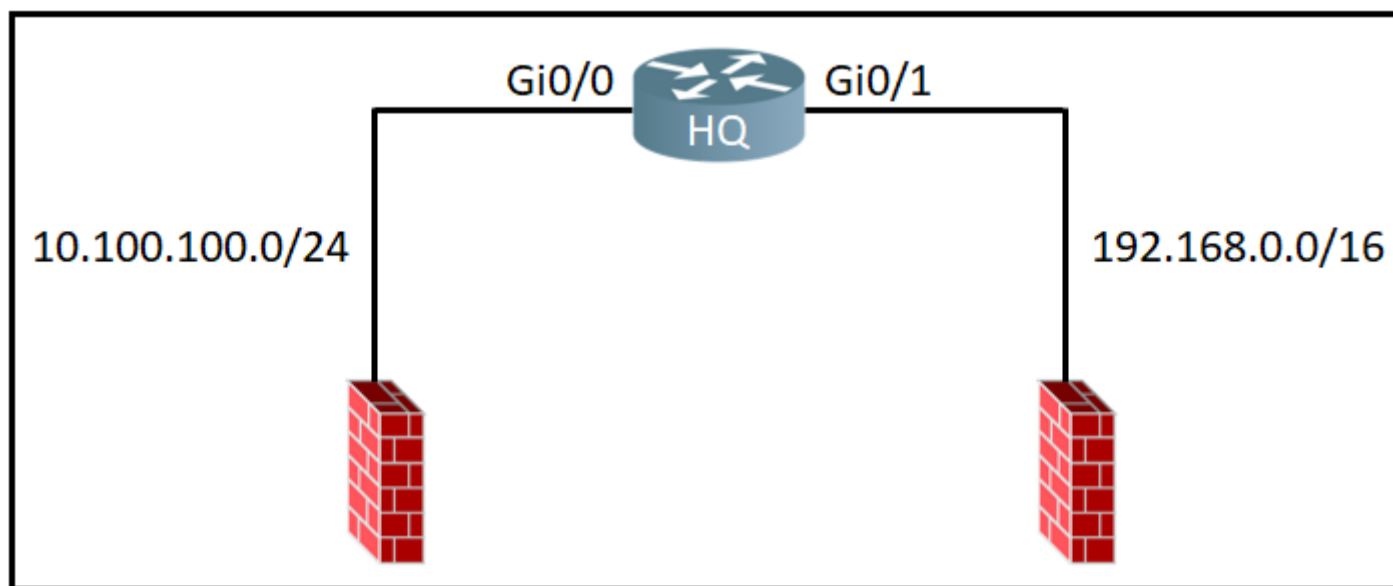
TL:DR: GRE supports multicast but does not offer encryption. Therefore, use GRE over IPsec for encryption

upvoted 4 times

 **Mhatz** 2 years, 10 months ago

Reference please

upvoted 2 times



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, 4 months ago

A is correct, standard is 1-99 or 1300-1999
upvoted 13 times

RODCCN Most Recent 1 month, 3 weeks ago

Selected Answer: A

Standard ACLs: Standard ACLs are used to filter traffic based on the source IP address only. They are identified by numbers from 1 to 99 and 1300 to 1999.

Extended ACLs: Extended ACLs allow filtering based on various criteria such as source and destination IP addresses, TCP/UDP ports, protocols, etc. They are identified by numbers from 100 to 199 and 2000 to 2699.

upvoted 1 times

[Removed] 2 months, 1 week ago

Selected Answer: A

A. ip access-list standard 99 permit 10.100.100.0 0.0.0.255 deny 192.168.0.0 0.0.255.255

0.0.0.255 = /24

0.0.255.255 = /16

upvoted 1 times

deluxeccna 5 months ago

Selected Answer: A

Answer is A

upvoted 3 times

GigaGremlin 11 months, 1 week ago

Selected Answer: B

Because of the /16

upvoted 1 times

fransCISCO 7 months, 2 weeks ago

it is A look at the wildcard

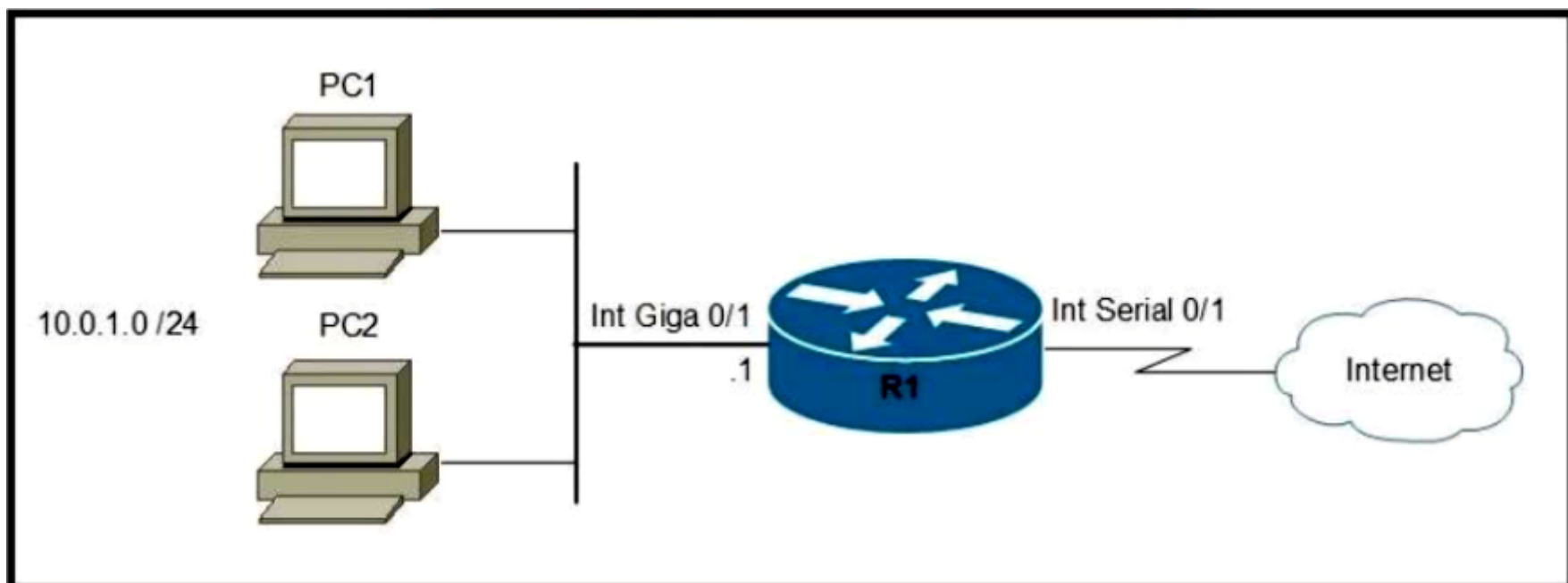
upvoted 4 times

Networknovice 1 year, 4 months 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.omniseccu.com/cisco-certified-network-associate-ccna/standard-access-control-lists.php#:~:text=Standard%20Access%20Control%20Lists%20\(ACLs\)%20are%20the%20oldest%20type%20of,access%20lists%22%20IOS%20comm and.](https://www.omniseccu.com/cisco-certified-network-associate-ccna/standard-access-control-lists.php#:~:text=Standard%20Access%20Control%20Lists%20(ACLs)%20are%20the%20oldest%20type%20of,access%20lists%22%20IOS%20comm and.)

upvoted 3 times



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

mantest Highly Voted 1 year, 3 months 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 5 times

Yinxs Most Recent 3 weeks, 2 days ago

Selected Answer: BC

A is a uncomplete command.However B and C are complete commands that can achieve this goal.
 upvoted 1 times

Vikramaditya_J 1 month, 1 week ago

Selected Answer: AC

Option B, "username cisco password 0 cisco," is incorrect because it creates a local user account with a password, but it does not enable remote access. Insead option A "ip ssh pubkey-chain" command is used to configure the SSH public key authentication method on a Cisco device. It allows users to authenticate using their public keys instead of passwords, enhancing security and convenience.
 upvoted 1 times

Eallam 2 months, 1 week ago

Selected Answer: AC

A and C , the username command is very bad
 upvoted 2 times

StingVN 3 months, 3 weeks 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 2 times

  **DARKK** 1 year, 3 months ago



Why not SSH? A

upvoted 1 times

  **Murphy2022** 11 months, 2 weeks ago

because that command doesn't exist inside CLI

upvoted 1 times

  **guisam** 9 months, 1 week ago



<https://networklessons.com/uncategorized/ssh-public-key-authentication-cisco-ios>

upvoted 1 times

  **Networknovice** 1 year, 4 months 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, 3 months 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** 11 months, 3 weeks ago

Great link!

upvoted 1 times

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.

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: D

Answer D is correct
upvoted 1 times

  **no_blink404** 2 months, 3 weeks ago

Correct answer is D. By default the traffic from RADIUS is not encrypted.
upvoted 1 times



  **StingVN** 3 months, 3 weeks 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, 3 months 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, 4 months 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 3 times

  **iGlitch** 1 year, 3 months ago

OK, but why it's missing confidentiality tho?
upvoted 1 times

  **martialstriker09** 1 year, 2 months 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 6 times

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 11 months 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 15 times

  **splashy** Highly Voted 10 months, 1 week 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 6 times

  **VictorCisco** 5 months, 3 weeks ago

Password can't prevent from PHYSICAL access to a port as well :)

upvoted 4 times

  **Yinx** Most Recent 3 weeks, 2 days ago

Selected Answer: B

A is not access control.

upvoted 1 times

  **Cynthia2023** 1 month ago

Selected Answer: A

Configuring a password for the console port is related to device access security, not physical access control.

upvoted 1 times

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: A

A - Other answers are not Physical access control

upvoted 1 times

  **4bed5ff** 2 months, 3 weeks ago

Selected Answer: A

"Video surveillance serves two primary purposes. Real-time CCTV monitoring as a detection control may allow a smaller number of security personnel to monitor a much larger area than could be effectively monitored directly. This allows a security force of the same size to secure a much larger area or to secure a smaller area in more detail or with fewer people."

Cisco CCNA in 60 Days - Paul Browning (under section heading "Physical Security")

upvoted 2 times

  **dropspablo** 3 months, 1 week 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** 3 months, 3 weeks 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 3 times

  **jonathan126** 4 months, 3 weeks ago

A - physical access control (detective control)

B - Authentication (AAA)

C - Availability (CIA)
D - Authentication (AAA)

upvoted 1 times

🗨️ 👤 **Ciscoman021** 5 months, 1 week 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** 6 months, 2 weeks ago

physical access control is the key to this answer.

upvoted 2 times

🗨️ 👤 **hamish88** 7 months, 1 week 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

🗨️ 👤 **Garfieldcat** 11 months, 2 weeks ago

if B is the answer, why D isn't ? Therefore, I opt A

upvoted 1 times

🗨️ 👤 **splashy** 10 months, 1 week ago

enable passwords don't require physical access to the device to be used

upvoted 2 times

🗨️ 👤 **BieLey** 11 months, 2 weeks 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** 11 months, 3 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** 1 year, 1 month 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 several websites mention cameras as physical access control tool. At least they help to restrict Access right?

upvoted 3 times

🗨️ 👤 **MDK94** 1 year, 2 months 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

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, 3 months 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 7 times

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

🗄️ **Phonon** Highly Voted 8 months, 2 weeks 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 6 times

🗄️ **RODCCN** Most Recent 1 month, 3 weeks ago

Selected Answer: B

enable secret priv4t3p4ss: This command sets the password for privileged EXEC mode, also known as the enable password. The password is "priv4t3p4ss."

line con 0 password p4ssw0rd1 login: This command sets the user EXEC password for console access. The password is "p4ssw0rd1." The "login" keyword ensures that the password is required when accessing the console.

line vty 0 15 password s3cr3t2 login: This command sets the user EXEC password for Telnet access. The password is "s3cr3t2." The "login" keyword ensures that the password is required when accessing the router through Telnet.

upvoted 1 times

🗄️ **[Removed]** 2 months, 2 weeks ago

Selected Answer: B

```
B.
enable secret priv4t3p4ss
line con 0
password p4ssw0rd1
login
line vty 0 15
password s3cr3t2
login
```

upvoted 1 times

🗄️ **StingVN** 3 months, 3 weeks 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 2 times

🗳️ 👤 **Anas_Ahmad** 8 months, 3 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 3 times

🗳️ 👤 **michael1001** 9 months, 1 week ago

Selected Answer: B

is B, please update answer
upvoted 4 times

🗳️ 👤 **[Removed]** 2 months, 2 weeks ago

It is.
upvoted 1 times

🗳️ 👤 **RougePotatoe** 10 months, 2 weeks 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** 10 months, 2 weeks ago

I see I missed up. login is complete command.
upvoted 1 times

🗳️ 👤 **Etidic** 10 months, 3 weeks ago

Selected Answer: B

the answer is B
upvoted 3 times

🗳️ 👤 **dick3311** 11 months ago

Selected Answer: D

I go for D
<https://study-ccna.com/cisco-privilege-levels/>
upvoted 2 times

🗳️ 👤 **mda2h** 1 month, 3 weeks ago

False! For enable, the keyword is level not privilege!
upvoted 1 times

🗳️ 👤 **Garfieldcat** 11 months, 1 week ago

Isn't exec level of enable sec password 15 by default ?
upvoted 4 times

🗳️ 👤 **GigaGremlin** 11 months, 1 week ago

Selected Answer: B

IMHO,...
no extra privilege 15 needed and for Password protection,
you're already 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** 11 months, 2 weeks ago

Selected Answer: D

D is correct because priv 15 is the priv for exec
upvoted 1 times

🗳️ 👤 **Garfieldcat** 11 months, 2 weeks 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** 11 months, 2 weeks ago

privilege 15 is the exec privilege
upvoted 1 times

🗳️ 👤 **creaguy** 11 months, 3 weeks ago

Selected Answer: B



enable secret priv4t3p4ss
!
line con 0


```
password p4ssword1
login
!
line vty 0 15
password s3cr3t2
login
upvoted 3 times
```


  **ShadyAbdekmalek** 11 months, 3 weeks ago

Selected Answer: B

D is wrong
I go for B
upvoted 2 times

  **BieLey** 11 months, 2 weeks ago

Why is it wrong when it asks for privileged?
upvoted 1 times

  **EliasM** 10 months, 4 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

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	

 **THEKRYPTONIAN** Highly Voted 1 year, 1 month ago

1.#switchport mode access
 2.#switchport port-security
 3.#switchport port-security maximum 2
 4.#switch port-security sticky
 upvoted 48 times

 **mda2h** 1 month, 3 weeks ago
 Agreed! Default behavior is Shutdown mode. No need to specify it
 upvoted 1 times

 **fransCISCO** 7 months, 2 weeks ago
 so this is the correct answer and sequence?? pls answer guys
 upvoted 2 times

🗨️ 👤 **abdelkader163** 2 weeks, 6 days ago

yes this is the correct order :))

upvoted 1 times

🗨️ 👤 **HeinyHo** Highly Voted 👍 12 months 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 12 times

🗨️ 👤 **dropspablo** Most Recent 🕒 3 months, 1 week 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 3 times

🗨️ 👤 **krzysiew** 5 months, 2 weeks ago

I checked packet tracet

- 1.#switchport mode access
- 2.#switchport port-security
- 3.#switch port-security sticky
- 4.#switchport port-security maximum 2

upvoted 5 times

🗨️ 👤 **gc999** 6 months 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** 7 months, 1 week 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** 7 months ago

"violation shutdown". is the default mode, so not needed unless another mode was set earlier

upvoted 3 times

🗨️ 👤 **Dutch012** 6 months, 1 week ago

right, it is not needed but it completes what the question is asking for

upvoted 1 times

🗨️ 👤 **kalidergr** 8 months, 3 weeks 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** 11 months, 1 week ago

don t understand, why shutdown..?

upvoted 1 times

🗨️ 👤 **clivebarker86** 11 months, 1 week ago

don t understand, why shutdown..?

upvoted 1 times

🗨️ 👤 **splashy** 11 months, 3 weeks 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** 1 year, 1 month 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** 1 year, 2 months 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, 3 months 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, 3 months 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** 1 year, 1 month ago

to permanently add the mac , need to save the configuration, otherwise reload will restore the configuration with no sticky mac
upvoted 4 times

🗨️ 👤 **MikeNY85** 1 year, 3 months ago

IT SAID TWO "RANDOM" MAC ADDS....WHICH MEANS "STICKY"
upvoted 2 times

🗨️ 👤 **NORLI** 1 year, 4 months ago

SO WHAT IS THE DIFFERENCE BETWEEN SWITCHPORT SECURITY AND SWITCHPORT 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, 4 months ago

I think since it's dynamically, it should be "switchport port-security mac-address sticky"
upvoted 1 times

🗨️ 👤 **DARKK** 1 year, 4 months ago

Nothing explicitly says it is dynamically.
upvoted 2 times

🗨️ 👤 **melmiosis** 10 months, 1 week ago

when we say RANDOM, it means DEFINETLY NOT STATIC...
What about STATIC is so "random"???

upvoted 3 times

🗨️ 👤 **purenuker** 8 months ago

Yeah , this is the most dumbest question of all times which Cisco asks ... I dont understand ..
upvoted 2 times

🗨️ 👤 **Peter_panda** 7 months, 2 weeks 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** 6 months, 2 weeks ago

totally agree
upvoted 1 times


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** 3 months, 3 weeks 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, 4 months 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

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

- It enables the device to allow user- or group-based access.
- It leverages a RADIUS server to grant user access to a reverse Telnet session.
- It records the amount of time for which a user accesses the network on a remote server.
- It restricts the CLI commands that a user can perform.
- It uses TACACS+ to log the configuration commands entered by a network administrator.
- It verifies the user and password before granting access to the device.

Accounting

Authorization

Correct Answer:

Answer Area

- It enables the device to allow user- or group-based access.
- It leverages a RADIUS server to grant user access to a reverse Telnet session.
- It records the amount of time for which a user accesses the network on a remote server.
- It restricts the CLI commands that a user can perform.
- It uses TACACS+ to log the configuration commands entered by a network administrator.
- It verifies the user and password before granting access to the device.

Accounting

It records the amount of time for which a user accesses the network on a remote server.

It uses TACACS+ to log the configuration commands entered by a network administrator.

Authorization

It leverages a RADIUS server to grant user access to a reverse Telnet session.

It restricts the CLI commands that a user can perform.

EliasM Highly Voted 11 months, 1 week 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 14 times

RougePotatoe 10 months, 2 weeks 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 5 times

  **jonathan126** 4 months, 3 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 4 times

  **studying_1** 4 months, 1 week ago

I agree

upvoted 3 times

  **enzo86** Highly Voted  5 months, 1 week 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 10 times

Layer 2 **Layer 3** **AAA Servers**

Layer 2 Security ⁶ WPA+WPA2

MAC Filtering⁹

Fast Transition

Fast Transition Adaptive

Over the DS

Reassociation Timeout 20 Seconds

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption AES TKIP CCMP256 GCMP128 GCMP256

OSSEN Policy

Authentication Key Management ¹⁹

802.1X Enable

CCKM Enable

PSK Enable

FT 802.1X Enable

FT PSK Enable

SUITEB-1X Enable

SUITEB192-1X Enable

WPA gtk-randomize State Disable

¹⁴

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 5 months 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 2 times

clivebarker86 11 months 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 11 months, 1 week 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, 3 months 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 4 times

 **iGlitch** 1 year, 3 months ago

This feature was NOT mentioned in the OCG 😊, but by now you should know how cisco exams work.

upvoted 7 times

The screenshot shows the configuration for Layer 2 Security. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. The 'Security Type' is set to 'Enterprise'. 'MAC Filtering' is disabled. Under 'WPA+WPA2 Parameters', 'WPA Policy' is disabled, 'WPA2 Policy' is checked, and 'WPA2 Encryption' is set to 'CCMP128(AES)'. 'Fast Transition' is set to 'Disable' and 'Protected Management Frame' (PMF) is set to 'Disabled'. Under 'Authentication Key Management', '802.1X-SHA1' is checked and 'Enable'.

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, 4 months 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 3 months, 3 weeks 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 3 times

Phonon 8 months, 2 weeks 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** 10 months, 3 weeks ago

Selected Answer: C

The answer is C
upvoted 2 times

🗄️ 👤 **Etidic** 10 months, 3 weeks ago

The answer is C
upvoted 2 times

🗄️ 👤 **creaguy** 11 months, 3 weeks 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** 11 months, 2 weeks ago

WPA and AKM must be configured, while PKM is optional. 802.11r still works with PKM being disabled.
upvoted 1 times

🗄️ 👤 **Murphy2022** 11 months, 1 week ago

i was tired read W as R
upvoted 2 times

🗄️ 👤 **JUveNTino** 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

🗄️ 👤 **dulceordog** 1 year, 1 month ago

'B' is correct
to configure 802.11w feature for optional and mandatory, you must have WPA and AKM configured. The RNS (Robust Secure Network) IE must be enabled with an AES Cipher.
To configure 802.11w as mandatory, you must enable PMF AKM in addition to WPA AKM
upvoted 1 times

🗄️ 👤 **iGlitch** 1 year, 3 months 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, 4 months 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** 10 months, 3 weeks ago

Restrictions for 802.11w • 802.11w cannot be applied on an open WLAN, WEP-encrypted WLAN, or a TKIP-encrypted WLAN. • The WLAN on which 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** 1 year, 2 months 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** 1 year, 2 months ago

"Required" is not an obligation here...
upvoted 1 times

🗄️ 👤 **Netox7** 1 year, 4 months 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


Which encryption method is used by WPA3?

- A. TKIP
- B. AES
- C. SAE
- D. PSK

Correct Answer: C

-  **Garfieldcat** Highly Voted 11 months, 1 week ago
SAE is refer to authentication. encryption method should be B -AES
upvoted 12 times
-  **EliasM** 11 months ago
Garfield is right. Check page 662 of OCG.
upvoted 3 times
-  **Techpro30** Most Recent 3 weeks, 2 days ago
Thought Id add my AI 2 cents.....Simultaneous Authentication of Equals (SAE) is a security protocol that protects wireless networks. SAE is a key exchange protocol used in WPA3, which enables devices to securely establish a shared secret key for encrypting wireless communications
upvoted 1 times
-  **Secsoft** 1 month ago
Which encryption method is used by WPA3?
A. TKIP
B. AES
C. SAE
D. PSK
ChatGPT
The encryption method used by WPA3 is:




C. SAE (Simultaneous Authentication of Equals)

WPA3 uses the SAE (Simultaneous Authentication of Equals) protocol for key exchange and encryption. This protocol is based on the Elliptic Curve Diffie-Hellman (ECDH) key exchange and provides stronger security compared to the older WPA and WPA2 protocols. It ensures forward secrecy, protecting the confidentiality of data even if an attacker captures encrypted traffic and later gains access to the network's pre-shared key.
The answer is correct. please don't confuse people.
upvoted 1 times
-  **StingVN** 3 months, 3 weeks 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-PSK) 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 3 times
-  **krzysiew** 5 months, 2 weeks ago
i think
WPA3 - SAE
WPA3 Enterprise AES (WPA3 Enterprise, by default, uses a 128-bit AES-CCMP)
upvoted 1 times
-  **krzysiew** 5 months, 2 weeks ago
WPA3-Personal SAE authentication metod
WPA3 Enterprise AES (by default, uses a 128-bit AES-CCMP) cryptographic metod
upvoted 1 times
-  **Zortex** 6 months 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** 8 months, 2 weeks 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** 10 months, 3 weeks ago

Selected Answer: B

The answer is B

upvoted 4 times

 **sjorwen** 11 months 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** 3 months, 3 weeks 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 2 times

 **SVN05** 7 months, 1 week 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

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

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: B

Given answer is correct.

B. Authentication verifies the identity of a person accessing a network, and authorization determines what resource a user can access.
upvoted 1 times

  **studying_1** 3 months, 2 weeks ago

Selected Answer: B



Answer is correct

upvoted 1 times

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** 3 months, 3 weeks ago

where is the hostname?

upvoted 1 times

  **StingVN** 3 months, 3 weeks 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 2 times

Which type of 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

 **RODCCN** 1 month, 3 weeks ago

Selected Answer: A

A SYN flood is a type of network attack that overwhelms the target server by sending a large number of SYN packets (the first step in establishing a TCP connection) to a specific port, without completing the connection handshake. This flood of half-open TCP connections consumes the server's resources, leading to a denial-of-service (DoS) condition, as the server becomes unable to handle legitimate connection requests.

upvoted 1 times

 **Eminn** 7 months, 3 weeks 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.](https://www.netscout.com/what-is-ddos/syn-flood-attacks#:~:text=A%20TCP%20SYN%20flood%20DDoS,into%20a%20half%2Dopen%20state)

upvoted 2 times

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

 **Phonon** Highly Voted 8 months, 2 weeks 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 8 times

 **Request7108** Highly Voted 8 months, 2 weeks 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/xs-3s/sec-pki-xe-3s-book/sec-cfg-auth-rev-cert.html

upvoted 7 times

 **Stichy007** Most Recent 6 months, 2 weeks ago

Selected Answer: CD

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xs-16/sec-pki-xe-16-book/sec-deploy-rsa-pki.html

upvoted 3 times

 **michael1001** 9 months, 1 week ago

Selected Answer: BD

Should be B and D

upvoted 4 times

 **battlefate** 9 months ago

agreed.

upvoted 2 times

DRAG DROP -

Drag and drop the descriptions of AAA services from the left onto the corresponding services on the right.

Select and Place:

<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">allows the user to change to enable mode</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">limits the user's access permissions</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">log session statistics</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">records user commands</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">secures access to routers</div> <div style="border: 1px solid black; padding: 2px;">validates user credentials</div>	<div style="border: 2px solid yellow; padding: 5px; margin-bottom: 10px;"> Accounting <div style="border: 1px solid black; height: 20px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; height: 20px;"></div> </div> <div style="border: 2px solid yellow; padding: 5px; margin-bottom: 10px;"> Authentication <div style="border: 1px solid black; height: 20px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; height: 20px;"></div> </div> <div style="border: 2px solid yellow; padding: 5px;"> Authorization <div style="border: 1px solid black; height: 20px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; height: 20px;"></div> </div>
---	--

Correct Answer:

<div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">allows the user to change to enable mode</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">limits the user's access permissions</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">log session statistics</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">records user commands</div> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">secures access to routers</div> <div style="border: 1px solid black; padding: 2px;">validates user credentials</div>	<div style="border: 2px solid yellow; padding: 5px; margin-bottom: 10px;"> Accounting <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">log session statistics</div> <div style="border: 1px solid black; padding: 2px;">records user commands</div> </div> <div style="border: 2px solid yellow; padding: 5px; margin-bottom: 10px;"> Authentication <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">validates user credentials</div> <div style="border: 1px solid black; padding: 2px;">secures access to routers</div> </div> <div style="border: 2px solid yellow; padding: 5px;"> Authorization <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">limits the user's access permissions</div> <div style="border: 1px solid black; padding: 2px;">allows the user to change to enable mode</div> </div>
---	--

no_blink404 2 months, 3 weeks ago

Provided answer is correct
upvoted 2 times

LeonardoMeCabrio 3 months, 1 week ago

Given answers are correct.
upvoted 2 times

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 11 months, 2 weeks 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 13 times

 **highfivejohn** Highly Voted 11 months ago

Selected Answer: D

Why would I need to run "aaa new-model" if the scenario indicated RADIUS was already present? D

upvoted 6 times

 **[Removed]** Most Recent 2 months, 2 weeks ago

Again...a question that has nothing to do with CCNA 200-301...

upvoted 3 times

 **4aynick** 3 months, 1 week ago

Need create new authentication group for console.

`aaa authentication login CONSOLE local`

After map it to console line

`line console 0`

`login authentication CONSOLE`

upvoted 1 times

 **4aynick** 3 months, 1 week ago

I don't find correct answer

upvoted 1 times

 **krzysiew** 5 months, 2 weeks ago

Selected Answer: A

`aaa new-model` `line con 0` `password plaintextpassword` `privilege level 15`

upvoted 1 times

 **oatmealturkey** 7 months 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 4 times

 **usamahrakib001** 7 months, 3 weeks 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 4 times

 **SemStrond** 10 months, 1 week ago

Selected Answer: D

D is the correct answer

upvoted 4 times

Which wireless security protocol relies on Perfect Forward Secrecy?

- A. WEP
- B. WPA2
- C. WPA
- D. WPA3

Correct Answer: A



  **Etidic** Highly Voted 10 months, 3 weeks ago

Selected Answer: D

The answer is D
upvoted 7 times

  **gamdimu** Most Recent 1 month, 3 weeks ago

WPA3 is the correct answer
upvoted 1 times

  **Gauain** 2 months, 2 weeks ago

Answer is D.
upvoted 1 times


  **studying_1** 4 months, 1 week ago

Selected Answer: D

The answer is D
upvoted 1 times

  **RAJ_1920** 5 months ago

@examtopics please fix
upvoted 1 times

  **krzysiew** 5 months, 2 weeks ago

Selected Answer: D

WPA3 networks include perfect forward secrecy.
upvoted 1 times

  **michael1001** 9 months, 1 week ago

Selected Answer: D

D - please fix
upvoted 3 times

  **clivebarker86** 11 months ago

PFS its a WPA3 feature
upvoted 1 times

  **GigaGremlin** 11 months, 1 week 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** 11 months, 3 weeks ago

Selected Answer: D

WPA3 networks include PFS
upvoted 1 times

  **ShadyAbdekmalek** 11 months, 3 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 2 times

  **ShadyAbdekmalek** 11 months, 3 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** 11 months, 4 weeks ago

PFS is used in WPA3

upvoted 1 times

  **splashy** 11 months, 4 weeks ago

Selected Answer: D

<https://blog.compass-security.com/2019/07/from-open-wi-fi-to-wpa3/>

upvoted 2 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

  **[Removed]** 2 months, 1 week ago

Selected Answer: C

C. It is when a new network vulnerability is discovered before a fix is available.

upvoted 2 times

  **ac89l** 4 months ago

Selected Answer: C

Agree, answer is C

upvoted 4 times

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 11 months, 1 week 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** Highly Voted 9 months ago

Bad question, playing with english....

"doubling the modulus size from 1024"... why not just say "change the modulus size to 2048"...

upvoted 5 times

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

 **RougePotatoo** Highly Voted 10 months, 2 weeks ago

my distain for cisco grows
upvoted 22 times

 **splashy** Highly Voted 11 months, 3 weeks 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 9 times

 **Cynthia2023** Most Recent 1 month ago

Selected Answer: BE

The correct answers are (E) unique user knowledge and (B) soft tokens.

Explanation:

Single sign-on (SSO) is not an example of multifactor authentication. SSO allows users to access multiple applications with a single set of credentials.

Passwords that expire are a security policy that enforces regular password changes, but this is not an example of multifactor authentication on its own.

Soft tokens are a form of multifactor authentication. They are typically software-based applications that generate one-time passwords or time-based codes for users to use along with their regular passwords.

Shared password responsibility is not an example of multifactor authentication. It refers to the practice of distributing account credentials among multiple people, which is generally not recommended for security reasons.

upvoted 2 times

 **saifeddinezekri** 1 month, 3 weeks ago

Multifactor authentication (MFA) is a security mechanism that requires users to provide two or more different forms of identification before gaining access to a system or service. These factors typically fall into three categories: something you know (like a password), something you have (like a smartphone), and something you are (like a fingerprint).

upvoted 2 times

 **Shabeth** 2 months, 1 week ago

Selected Answer: BE

B & E

Types of Authentication Factors

MFA generally refers to five types of authentication factors which are expressed as:

Knowledge: Something the user knows, like username, password, or a PIN.

Possession: Something the user has, like a safety token.

Heritage: Something the user is, which can be demonstrated with fingerprint, retina verification, or voice recognition.

Place: Based on the user's physical position.

Time: A time-based window of opportunity to authenticate like OTP.

upvoted 3 times

 **Chichi69** 2 months, 3 weeks ago

Answer is BE

upvoted 1 times

 **Friday_Night** 3 months, 3 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** 5 months ago

From someone who's taken and passed the Sec+ exam, its def BE.

upvoted 3 times

  **Ciscoman021** 5 months, 1 week 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 3 times

  **Zortex** 6 months 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** 6 months, 2 weeks 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** 7 months, 3 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** 9 months ago

Selected Answer: BC

Agreed with @splasy 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 3 times

  **RougePotatoe** 10 months, 2 weeks 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** 10 months, 3 weeks ago

why not E

upvoted 2 times

  **mrgreat** 1 year ago

Selected Answer: AB

C is incorrect, A and B are corret

upvoted 1 times

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

🗨️ 👤 **perri88** 3 months ago

this cannot be a real question.
upvoted 2 times

🗨️ 👤 **mellos** 9 months, 3 weeks ago

No entiendo esta pregunta
upvoted 3 times

🗨️ 👤 **[Removed]** 2 months, 2 weeks ago

Me either

A mi tampoco
upvoted 1 times

🗨️ 👤 **Request7108** 8 months, 2 weeks ago

Agreed. This is a very confusing question.
upvoted 2 times

🗨️ 👤 **[Removed]** 2 months, 2 weeks ago

Yes it really is!
upvoted 1 times

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

🗨️ 👤 **RODCCN** 1 month, 3 weeks ago

Selected Answer: A

<https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html>
upvoted 1 times

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

🗨️ 👤 **Shabeth** 2 months, 1 week ago

Selected Answer: A

A.
WPA
-Uses TKIP (temporal key integrity protocol) for encryption
TKIP adds the following features using legacy hardware and underlying WEP encryption
MIC
Timestamp
Sender's mac add
Tkip sequence counter
Key mixing algorithm
Longer initializing vector
Short term replacement for WEP
-Released in 2003 and Replaced in 2004
upvoted 1 times

🗨️ 👤 **[Removed]** 3 months, 1 week ago

Selected Answer: A

From the OCG, pg 662, Table 28-2:
"Encryption and MIC with TKIP?"
WPA: Yes
WPA2: No
WPA3: No
upvoted 2 times

🗨️ 👤 **beerbiceps1** 5 months, 2 weeks 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** 8 months, 2 weeks ago

Could be A or C.
Bad question. WPA can use both TKIP/MIC and Pre-Shared Key
upvoted 4 times

🗨️ 👤 **battlefate** 9 months 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 2 times

🗨️ 👤 **mis779548** 8 months, 2 weeks ago

and you the same
upvoted 1 times

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 10 months 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 6 times

  **Yinx** Most Recent 3 weeks, 2 days ago

Selected Answer: DE

E is about physical security.

upvoted 1 times

  **Shun5566** 3 months, 2 weeks ago

Selected Answer: AD

Agree alejandro

upvoted 1 times

  **bisiyemo1** 4 months, 4 weeks ago

Selected Answer: AD

A and D is the correct answers

upvoted 1 times

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  9 months, 3 weeks ago

Selected Answer: A

And Aes for encryption
upvoted 10 times

  **SVN05** 7 months, 1 week ago

Agreed.
upvoted 2 times

  **Cynthia2023** Most Recent  2 months, 2 weeks ago

Selected Answer: A

(A). It uses SAE (Simultaneous Authentication of Equals) for authentication. WPA3 replaces the pre-shared key (PSK) authentication method used in WPA2 with SAE, which provides stronger protection against offline dictionary and brute-force attacks. SAE allows users to securely authenticate with the network without revealing their passwords and protects against various authentication-related vulnerabilities.
upvoted 2 times



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 6 months, 1 week 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 13 times

  **Wes_60** 5 months, 2 weeks ago

You ain't kidding.
upvoted 1 times

  **shaney67** Most Recent 5 days, 1 hour ago

Would A not be IDS? as in Detection not Prevention?
upvoted 1 times

  **perri88** 3 months ago

from chatgpt:
To provide a more accurate answer, a function of a Next-Generation IPS is:
A. Correlates user activity with network events.

Next-Generation IPS systems often have the ability to correlate user activity with network events. By monitoring and analyzing network traffic, they can associate specific network events with the user or device responsible for generating them. This correlation helps in identifying potential security incidents, pinpointing the source of malicious activities, and assisting in forensic investigations. This user-based visibility allows security teams to better understand the context and intent behind network events, enabling more effective incident response and threat mitigation.
upvoted 2 times

  **no_blink404** 3 months, 1 week ago

Selected Answer: A

A is the correct answer
upvoted 1 times

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:

It supports local, PPP, RADIUS, and TACACS+ options	Accounting
It tracks the services that a user is using.	
It records the amount of network resources consumed by the user.	Authentication
It assigns per-user attributes.	
It permits and denies login attempts.	

Correct Answer:

It supports local, PPP, RADIUS, and TACACS+ options	Accounting It records the amount of network resources consumed by the user. It tracks the services that a user is using.
It tracks the services that a user is using.	Authentication It permits and denies login attempts. It supports local, PPP, RADIUS, and TACACS+ options
It records the amount of network resources consumed by the user.	
It assigns per-user attributes.	
It permits and denies login attempts.	

RougePotatoe Highly Voted 9 months, 4 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

no_blink404 Most Recent 2 months, 3 weeks ago

The provided answer looks correct. Per user attributes would be called as CoA (Change of Authorization).

upvoted 2 times

Request7108 8 months, 2 weeks 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

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

RougePotatoo (Highly Voted) 10 months, 2 weeks 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 27 times

EthanhuntMI6 (Highly Voted) 9 months, 1 week ago

This is probably the most stupidest question you can ask for a certification exam. Great job cisco, never fails to disappoint us.
upvoted 17 times

Cynthia2023 (Most Recent) 1 month ago

1. ****security policy****: Document that outlines an organization's security goals and practices and the roles and responsibilities of the organization's personnel.

2. ****security standard****: Tactical document that sets out specific tasks and methods to maintain security.
3. ****education****: User-awareness learning level that focuses on learning about topics and practices beyond what is typically required by the user's job.
4. ****awareness****: User-awareness learning level that focuses on security practices that all employees must understand and enforce.
5. ****training****: User-awareness learning level that focuses on teaching employees how to perform tasks specifically required by their jobs.
upvoted 2 times

🗨️ 👤 **no_blink404** 2 months, 3 weeks ago
Awareness: practices beyond what is typically required by the user's job
Education: practices that all employees must understand and enforce
Security policy: document that outlines an organisation's security goals
Security standard: tactical document that sets out specific tasks
Training: how to perform tasks specifically required by their jobs.
upvoted 3 times

🗨️ 👤 **XuniLrve4** 2 months, 3 weeks ago
Awareness and education is definitely swapped making answer incorrect. This I remember well from JeremyIT material and Boson exsim.
upvoted 1 times

🗨️ 👤 **XuniLrve4** 2 months, 3 weeks ago
Awareness and education is definitely swapped making anser incorrect. This I remember well from JeremyIT material and Boson exsim.
upvoted 1 times

🗨️ 👤 **deluxeccna** 4 months, 3 weeks ago
Such a stupid question. Looks more like a Cambridge English test
upvoted 6 times

🗨️ 👤 **BI1024** 11 months ago
Awariness and education should be replaced in the answer no?
upvoted 7 times

🗨️ 👤 **EliasM** 10 months, 4 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** 7 months, 4 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 3 times

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 9 months, 1 week 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 7 times

  **RODCCN** Most Recent 1 month, 3 weeks ago

Selected Answer: A

Because the default number of secure addresses is one and the default violation action is to shut down the port, configure the maximum number of secure MAC addresses on the port before you enable port security on a trunk.

LINK: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port_sec.html

upvoted 1 times

  **Shabeth** 2 months, 1 week ago

Selected Answer: A

A.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port_sec.html

upvoted 2 times

  **[Removed]** 2 months, 1 week ago

Selected Answer: A

A. It places the port in the err-disabled state if it learns more than one MAC address.

upvoted 1 times

  **Vikramaditya_J** 4 months, 2 weeks 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** 6 months 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** 9 months, 1 week ago

Selected Answer: A

Labbed it (quickly) in packet tracer, answer is A

upvoted 2 times

  **alejandro12** 9 months, 3 weeks ago

A, dont have sense, the objctive of trunk is learns more than one MAC address.

Should be C

upvoted 2 times

Which device separates networks by security domains?

- A. intrusion protection system
- B. firewall
- C. wireless controller
- D. access point

Correct Answer: B

 **Paul889** 2 months ago

Is this CCNA a question?
upvoted 1 times

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


 **RODCCN** 1 month, 3 weeks ago

Selected Answer: A

To prevent VLAN hopping attacks, you should use the switchport mode trunk command to manually configure your trunk ports, and use the switchport nonegotiate command to disable the dynamic trunking protocol.

LINK: <https://www.linkedin.com/advice/0/what-security-risks-challenges-vlan-trunking#:~:text=To%20prevent%20VLAN%20hopping%20attacks,disable%20the%20dynamic%20trunking%20protocol.>

upvoted 1 times

 **Etidic** 10 months, 3 weeks ago

Selected Answer: A

A is the correct answer
upvoted 3 times

 **xbololi** 2 months, 2 weeks ago

wow thank you sir.
upvoted 1 times

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** 5 months, 2 weeks 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** 7 months, 2 weeks 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

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**  9 months, 1 week ago

Selected Answer: D

Authentication Header (AH)
Encapsulating Security Payload (ESP)
upvoted 18 times

 **RODCCN** **Most Recent**  1 month, 3 weeks ago

Selected Answer: D

When a site-to-site VPN is configured, IPsec tunnel mode with ESP (Encapsulating Security Payload) provides encapsulation and encryption of the entire original IP packet. In this mode, the entire IP packet, including the original IP header and payload, is encapsulated within a new IP packet with a new IP header added by the VPN gateway. The original packet is encrypted, ensuring confidentiality, and the new IP header allows the encrypted packet to be routed over the public internet securely to the other VPN gateway, where it is decrypted and forwarded to its final destination.

upvoted 1 times

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** Highly Voted 6 months, 1 week ago


Selected Answer: A

A is the correct answer. Line vty can go only with access-class, not with access-group!
upvoted 8 times

 **[Removed]** Most Recent 2 months, 1 week ago

Selected Answer: A


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
upvoted 2 times

 **Dutch012** 6 months, 2 weeks ago

It should be access-group 120 like answer D not like A
upvoted 1 times

 **icecool2019** 11 months ago

The answer should be C
upvoted 2 times

 **EliasM** 10 months, 4 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 7 times

 **Request7108** 8 months, 2 weeks ago

No, this is for SSH access so it will be port 22
upvoted 1 times

 **RougePotatoe** 10 months, 2 weeks ago

Standard access range is 1-99 so it can't be C.
upvoted 5 times

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?](https://www.ciscopress.com/articles/article.asp?p=2995354&seqNum=2#:~:text=A%20controller%2C%20or%20SDN%20controller,the%20devices'%20distributed%20control%20plane)

[p=2995354&seqNum=2#:~:text=A%20controller%2C%20or%20SDN%20controller,the%20devices'%20distributed%20control%20plane](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 11 months ago

control plane, create routing table
upvoted 16 times

 **TinKode** 10 months ago

And data plane makes routing decisions based on control plane routing table.
upvoted 3 times

 **Sant11** Most Recent 2 weeks, 4 days ago

Selected Answer: C

In the context of an SDN architecture, the function that is primarily centralized on a controller is indeed:

C. Makes a routing decision

While it's true that SDN controllers can have an impact on the overall IP routing table, the centralization of routing decisions is a more accurate and fundamental representation of the controller's role in an SDN environment.

Option A ("Creates the IP routing table") involves the process of populating the routing table with routes and their associated information. While an SDN controller can influence routing decisions by programming forwarding rules in network devices, the creation of the IP routing table typically involves the management of routing protocols, which might still be distributed across the network devices.

So, while both options A and C have connections to the controller's role in SDN, option C is a more direct and specific representation of how SDN controllers primarily centralize routing decisions.

upvoted 2 times

 **iamomiema** 2 weeks, 5 days ago

the answer should be A!, The control plane is responsible for creating a routing table which then be used by the data plane to know where to forward a packet (makes a routing decision)
upvoted 1 times

 **ds0321** 3 weeks ago

Selected Answer: A

the answer is A
upvoted 1 times

 **Liquid_May** 3 weeks, 2 days ago

Selected Answer: A

In the 31 Days Before CCNA Guide on page 813 the following is stated: "The data plane is responsible for forwarding data as quickly as possible. To do so, it relies on tables built by the control plane".

In the same page it is stated that one of the functions of the data plane is performing IP routing table lookups.

Based on that, I would say that making a routing decision, would be a data plane function and to create the IP routing table would be a control plane function.

upvoted 1 times

 **enzo86** 7 months, 1 week 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 3 times

🗨️ **danny43213** 7 months, 2 weeks ago

one of the functions of a data plane is matching the destination IP address IP address to the routing table i.e routing decision but the table is in the control plane therefore I go with A.

upvoted 2 times

🗨️ **michael1001** 9 months, 1 week 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 2 times

🗨️ **RougePotatoe** 9 months, 4 weeks ago

Question 760 is a similar question and its answer was make routing decisions

upvoted 2 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

The screenshot shows a configuration page with tabs for General, Security, QoS, Policy-Mapping, and Advanced. Under the Security tab, there are sub-tabs for Layer 2, Layer 3, and AAA Servers. The Layer 2 Security dropdown is set to 'WPA+WPA2'. Below it, 'MAC Filtering' is unchecked. The 'Fast Transition' section has 'Fast Transition' unchecked. The 'Protected Management Frame' section has 'PMF' set to 'Disabled'. The 'WPA+WPA2 Parameters' section has 'WPA Policy' and 'WPA2 Policy' unchecked, and 'WPA2 Encryption' with 'AES' and 'TKIP' both unchecked. The 'Authentication Key Management' section has '802.1X', 'CCKM', and 'PSK' all set to 'Enable'.

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 11 months, 1 week 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 7 times

perri88 Most Recent 3 months ago

To provide the highest encryption and authentication using domain credentials from LDAP, the engineer must take the following two steps:

- C. Select WPA+WPA2 on Layer 2 Security.
- D. Select 802.1X from under Authentication Key Management.

Explanation:



Select WPA+WPA2 on Layer 2 Security: This step ensures the use of Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) protocols for securing the wireless network. WPA and WPA2 provide robust encryption and authentication mechanisms to protect network communications. By selecting WPA+WPA2, the network supports both protocols, allowing compatibility with a wide range of client devices.

upvoted 2 times

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

  **no_blink404** 2 months, 2 weeks ago

Selected Answer: D

D is correct
upvoted 1 times

  **StingVN** 3 months, 3 weeks 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** 5 months, 2 weeks 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** 7 months, 2 weeks 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** 11 months, 1 week 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

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:

DHCP snooping	rogue server that spoofs IP configuration
Dynamic ARP Inspection	cache poisoning
IP Source Guard	flood attacks
storm control	rogue clients on the network

Correct Answer:

DHCP snooping	IP Source Guard
Dynamic ARP Inspection	DHCP snooping
IP Source Guard	storm control
storm control	Dynamic ARP Inspection

 **Anon1216** Highly Voted 12 months 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 37 times

 **splashy** Highly Voted 11 months, 4 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 20 times

 **no_blink404** Most Recent 2 months, 2 weeks ago

Typical Cisco question, I asked ChatGPT and this was the answer:

DHCP Snooping - Rogue clients on the network

Dynamic ARP Inspection - Rogue server that spoofs IP config

IP Source Guard - Cache poisoning

Storm Control - Flood attacks

upvoted 2 times

 **RougePotatoe** 10 months, 2 weeks 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 3 times

 **Acidscars** 1 month, 4 weeks ago

I think you are correct. People are getting hung up on the "Rogue Server" and "spoofing IP configuration". It's extremely vague. Is it spoofing it's own IP configuration (IP Source Guard) or is it a DHCP server sending out spoofed DHCP packets (DHCP Snooping)? Spoofing IP Configuration would be a very odd way of saying sending out fake DHCP. So I think it would be IP source guard. Another terribly worded Cisco question.

upvoted 1 times

 **lolungos** 2 months, 3 weeks ago

The previous answers are correct, you did have the correct documentation but by cisco the best practices is to set DHCP snooping and trust just the dhcp server port meaning you don't need to validate anything else that way with the IP Source Guard. And you can have more than one rogue client on several ports, that's what you need to validate.

upvoted 2 times

  **RougePotatoe** 10 months, 2 weeks 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** 10 months, 2 weeks 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?

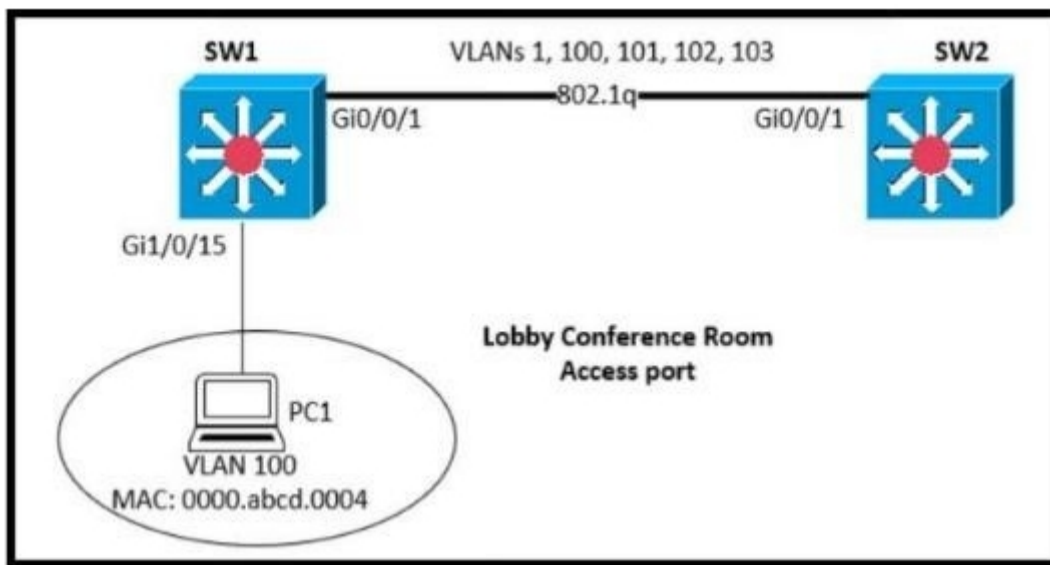
upvoted 1 times

  **RougePotatoe** 10 months, 2 weeks 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/xs-3s/asr903/sec-storm-control-xe-3s-asr903-book.html#:~:text=Storm control prevents traffic on,traffic on the Layer2 interfaces.

upvoted 1 times



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

🗨️ 👤 **Gotcha** 2 weeks, 4 days ago

Selected Answer: C

Dear Friends.

The only configuration that I can do is de C option. I tested with Packet Tracer, and these are the lines:

```
Switch(config-if)#switchport port-security mac-address 0000.abcd.0004
Port-security not enabled on interface FastEthernet0/15.
Switch(config-if)#vlan 100
```

I could see that the command "switchport port-security switchport port-security" does not exist.

This is the option in Packet Trace to "switchport port-security" command :

```
Switch(config-if)#switchport port-security ?
aging Port-security aging commands
mac-address Secure mac address
maximum Max secure addresses
violation Security violation mode
upvoted 1 times
```

🗨️ 👤 **Eallam** 2 months, 1 week ago

Selected Answer: A

no command is called switchport secure-mac
upvoted 1 times

🗨️ 👤 **sekvenca** 2 months, 2 weeks ago

A can't be right !
It doesn't specify either the MAC address nor does it specify to use sticky,
So you just set up port security but no MAC address is gonna be picked up !
D
upvoted 1 times

🗨️ 👤 **4aynick** 4 months, 2 weeks ago

correct answer - A
upvoted 2 times

🗨️ 👤 **DaimonANCC** 5 months, 1 week ago

chatgpt wrote the right question C
upvoted 1 times

```

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(config-if)# switchport mode trunk

Correct Answer: CD

 **joondale** Highly Voted 11 months, 3 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 20 times

 **oatmealturkey** 7 months, 1 week 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 7 times

 **EthanhuntMI6** 9 months, 1 week 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 3 times

 **Etidic** 10 months, 3 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 is added to the LINE VTY 0 4/5 15 interface.

I hope this helps!

upvoted 2 times

  **IAmAlwaysWrongOnExamtopics** 9 months, 1 week ago

we need enable secret to go into privilege exec mode

upvoted 3 times

  **splashy** 11 months, 3 weeks ago

Tested, very good catch! I've never been aware of this (because we always use an enable secret...)

upvoted 3 times

  **dropspablo** Most Recent 3 months ago

Selected Answer: AC

SSH test on PT without the enable secret below and it really shows that you can't access:

Cisco Packet Tracer PC Command Line 1.0

```
C:\>ssh -l pablo 10.0.32.2
```

Password: xxx

```
SW3>
```

```
SW3>enable
```

```
% No password set.
```

```
SW3>
```

upvoted 1 times

  **dropspablo** 3 months ago

I tested with telnet and it's the same thing:

```
C:\>telnet 10.0.32.2
```

```
Trying 10.0.32.2 ...Open
```

User Access Verification

Username: pablo

Password:

```
SW3>en
```

```
% No password set.
```

```
SW3>
```

upvoted 1 times

  **dropspablo** 3 months ago

In fact, it is possible to access it, but only in user mode SW3> and execute some commands (show, ping, ssh...). However, in the privileged SW3# podo for "remote access", a password of "Enable" would be required, "even if it has not been configured", unlike access via console.

upvoted 1 times

  **StingVN** 3 months, 3 weeks 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

  **perri88** 3 months ago

wrong, try it on packet tracer. you need the "enable secrete" to access enable mode remotely. and the crypto keys were already created, check the exhibit last command.

upvoted 2 times

  **ccna_exam** 4 months 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** 4 months 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 2 times

 **rogi2023** 6 months 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** 6 months, 3 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** 7 months 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

 **mohdhafizuddinesa** 9 months 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** 9 months, 1 week ago

Selected Answer: BC

Answer is B and C, answer well explained by Etidic

upvoted 2 times

 **Etidic** 10 months, 3 weeks ago

Selected Answer: BC

the correct answer is B and C

upvoted 1 times

 **splashy** 11 months, 3 weeks 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** 10 months, 1 week 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 privileged switch# directly, and not switch>

you need to have an "enable secret blabla" command entered or the user will not be able to enter privileged 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** 11 months, 3 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** 11 months, 3 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** 12 months 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** 12 months ago

Answer is wrong, can see in the exhibit that a crypto key has already been generated.

Answer is: B C

upvoted 2 times

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 12 months 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 11 times

 **creaguy** 11 months, 3 weeks 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** 6 months 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** 11 months, 2 weeks ago

Always apply the answer with the least privileges. So protect.

upvoted 4 times

 **VicM** Most Recent 4 months 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%E2%80%93%20When%20a%20violation%20occurs,sent%20when%20this%20violation%20occurs.>

upvoted 1 times

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 9 months, 4 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 12 times

 **hamish88** 4 months, 4 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 5 times

 **Acidscars** 1 month, 4 weeks ago

Agreed, since they are not part of your domain and you couldn't use group policy to push it out, so this could be very laborious. Also, would you even have access or permission to touch third party contractor computers? If these are NSA contractors, thats a hard no to both. C would definitely solve the problem, but is not the proper answer. It's B. Use a public certificate that any computer will trust.

upvoted 1 times

 **rogi2023** 5 months, 4 weeks ago

Perhaps you are not allowed to install on contractor devices, so reading carefully answer "B" makes sense..

upvoted 2 times

 **MartiFia** Most Recent 1 month, 1 week ago

Is this even CCNA?

upvoted 2 times

 **Shabeth** 2 months, 1 week ago

Selected Answer: B

B.

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215621-tls-ssl-certificates-in-ise.html>

upvoted 2 times

 **perri88** 3 months ago

Selected Answer: B

The certificate error experienced by contractors suggests that their devices do not trust the certificate presented by the Cisco ISE for the guest portal. To resolve this, a trusted certificate needs to be installed on the Cisco ISE, which is signed by a trusted third-party certificate authority (CA). This ensures that when contractors connect to the guest portal, their devices recognize the certificate as valid and trusted.

Option A, installing an internal CA signed certificate on the Cisco ISE, would only address certificate errors for devices within the same organization that have the internal CA's root certificate installed as a trusted root. It would not resolve certificate errors for external contractors' devices.

Options C and D involve installing certificates on the contractor devices. However, this would require distributing and configuring certificates on each contractor device individually, which may not be practical or feasible in this scenario.

upvoted 2 times

 **dropspablo** 3 months ago

Selected Answer: C

We can deduce that the EAP-TLS wireless authentication method is used, which requires a server and client certificate. Because the contracting client got a certificate error, but the employee clients did not. This eliminates the problem of the certificate on the ISE server, both in an EAP-TLS

and in a PEAP (which uses a certificate only on the server, not on the client). In this case, (to be continued...)

upvoted 1 times

  **dropspablo** 3 months ago

(continuation) In this case, then it would be an EAP-TLS, and the PKI could be public that are issued by a CA of a trusted third party company (Verisign, Let's Encrypt, DigiCert...) and these have native recognition on client devices. However, as there was an error only for contracting customers, it is likely to be a private PKI, which are issued by a private Certificate Authority (CA), trusted only internally, as this requires a process there is more during authentication, which is the installation of an internal PKI CA in the clients' devices, and it may have been this process that was missing in the contracting clients, during the authentication process, causing an error. So I believe, correct me if I'm wrong, answer C (Install an internal CA signed certificate on the contractor devices).

upvoted 1 times

  **ac89l** 4 months 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** 4 months, 3 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** 5 months 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

  **crisip** 9 months, 2 weeks ago

Selected Answer: D

i would say D

upvoted 1 times

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

 **michael1001** Highly Voted 9 months, 1 week ago

Selected Answer: BD

it's B and D, please fix.
upvoted 7 times

 **[Removed]** 2 months, 2 weeks ago

They never fix anything. So many answers are wrong...
upvoted 2 times

 **Xavi01** Highly Voted 1 year ago

Selected Answer: BD

The correct answers are B/D. WPA2 & WPA3.

CCMP was certainly not around when WEP was established.
upvoted 6 times


 **mda2h** Most Recent 1 month, 3 weeks ago

Why not E. WPA ?
upvoted 1 times

 **[Removed]** 2 months, 2 weeks ago

Selected Answer: BD

Answers B and D
upvoted 1 times

 **perri88** 3 months ago

Selected Answer: BD

CCMP is an encryption protocol based on the Advanced Encryption Standard (AES) algorithm. It provides both encryption and data integrity by combining the Counter Mode (CTR) for encryption and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for data integrity.

WPA3 (Wi-Fi Protected Access 3) and WPA2 (Wi-Fi Protected Access 2) are the latest and most commonly used wireless security standards. Both WPA3 and WPA2 support the use of CCMP as the encryption and integrity protocol for securing wireless communications.

On the other hand, WEP (Wired Equivalent Privacy) is an older and weaker security standard that uses the RC4 encryption algorithm, not CCMP. WEP has been found to have significant security vulnerabilities and is no longer recommended for use.

upvoted 1 times

 **Kerrera** 3 months, 1 week ago

Selected Answer: CD


WPA3 --> GCMP, source: page 662 CCNA 200-301 Official Cert Guide, Volume 1, Wendell Odom
upvoted 1 times

 **Kerrera** 3 months, 1 week ago

Sorry I was wrong, The question CCMP or GCMP has nothing to do with this matter
upvoted 1 times

 **Kerrera** 3 months, 1 week ago

WPA3 --> GCMP, source: page 662 CCNA 200-301 Official Cert Guide, Volume 1, Wendell Odom
upvoted 1 times

 **Ciscoman021** 5 months, 2 weeks 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** 5 months, 3 weeks ago

B/D, WEP uses TKIP

upvoted 1 times

  **gewe** 7 months 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** 11 months, 1 week ago

Agreed. WEP is an old technology.

upvoted 3 times

  **creaguy** 11 months, 2 weeks 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** 1 year ago

I think this should be WPA2 & WPA3 i could be wrong so feel free to correct :).

upvoted 3 times

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

🗨️ 👤 **Amr_001** 1 week, 1 day ago

official cert guide vol1, page 662 :

s. WPA3 leverages

stronger encryption by AES with the Galois/Counter Mode Protocol (GCMP). It also uses Protected Management Frames (PMF) to secure important 802.11 management frames between APs and clients, to prevent malicious activity that might spoof or tamper with a BSS's operation.

upvoted 2 times

🗨️ 👤 **Vikramaditya_J** 1 month, 1 week ago

Selected Answer: C

C. CCMP256: CCMP256 stands for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol using a 256-bit encryption key. It is the encryption cipher used in WPA3-Personal for enhanced security.

upvoted 1 times

🗨️ 👤 **Shabeth** 2 months, 1 week ago

Selected Answer: A

its A

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/wlan_security.html

upvoted 2 times

🗨️ 👤 **no_blink404** 2 months, 2 weeks ago

Hard question. I think the keyword 'must' infers the minimum requirement.

ChatGPT says its C.

upvoted 1 times

🗨️ 👤 **perri88** 3 months ago

Selected Answer: B

Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)

<https://www.wi-fi.org/discover-wi-fi/security>

upvoted 2 times

🗨️ 👤 **dropspablo** 3 months ago

Selected Answer: A

That elliptic curve got me, but I believe it's this:

WPA2 uses CCMP-128 security level with AES-128 cipher suite plus CBC-MAC cipher (personal or enterprise mode).

WPA3 also uses CCMP-128 security level with AES-128 cipher suite plus CBC-MAC cipher (personal or enterprise mode);

(or) GCMP-128 security level with AES-128 cipher suite plus GMAC cipher (enterprise mode);

(or) GCMP-192 security level (called Suite B) with AES-256 cipher suite plus GMAC cipher (enterprise mode).

In the case the question asked for the AES cipher (not the security level which is also 128 bits), CCMP-128 in this case refers to the 128 bit AES cipher.

According to RFC 5430, this confusion between cipher and elliptic curve security level is common, which represents the set of encryption ciphers plus the integrity cipher (AES Encryption + MIC CBC-MAC / or MIC GMAC).

upvoted 1 times

🗨️ 👤 **dropspablo** 3 months ago



The 128-bit security level corresponds to an elliptic curve size of 256 bits and AES-128; it also makes use of SHA-256 [SHS]. The 192-bit security level corresponds to an elliptic curve size of 384 bits and AES-256; it also makes use of SHA-384 [SHS].

Note: Some people refer to the two security levels based on the AES key size that is employed instead of the overall security provided by the combination of Suite B algorithms. At the 128-bit security level, an AES key size of 128 bits is used, which does not lead to any confusion.

However, at the 192-bit security level, an AES key size of 256 bits is used, which sometimes leads to an expectation of more security than is offered by the combination of Suite B algorithms.

<https://datatracker.ietf.org/doc/html/rfc5430#:~:text=The%20128%2Dbit,Suite%20B%0A%20%20%20algorithms.>

upvoted 1 times

  **StingVN** 3 months, 3 weeks 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** 5 months, 2 weeks ago

Selected Answer: A

WPA3-Personal use CCMP-128 and AES-128

upvoted 1 times

  **michael1001** 9 months, 1 week ago

Selected Answer: A

CCMP128 is mandatory for WPA3:

https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

upvoted 4 times

  **B11024** 11 months 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** 11 months ago

CCMP is not WPA2?

upvoted 1 times

  **dosu01** 9 months, 2 weeks 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 2 times

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

  **Hari2512** 3 months, 1 week ago

QUESTION 76

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

upvoted 2 times

  **papibarbu** 8 months ago

Yes C is Correct

upvoted 2 times

  **Tylosh** 12 months ago

Selected Answer: C

C is correct !

upvoted 2 times

  **Xavi01** 1 year ago

Selected Answer: C

<https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKPREA4/vlan1-and-vlan-hopping-attack>

upvoted 2 times

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  10 months, 1 week 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 10 times

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 3 years, 1 month 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 8 times

🗨️ **Hodicek** Most Recent 1 year, 9 months ago

GIVEN ANSWE IS CORRECT
upvoted 3 times

🗨️ **Alsaheer** 2 years, 4 months ago

D is correct
upvoted 4 times

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, 9 months ago


exam technique: without any prior knowledge, u can rule out two of the options just because they criticize CISCO's product
upvoted 73 times

 **JamesDean_Youldiots** 2 years, 3 months 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 18 times

 **Ethiopis** 2 years, 6 months ago


hahaha... good one.
upvoted 5 times

 **YoniEth** 1 year, 11 months ago

obviously
upvoted 2 times

 **chomjosh** Highly Voted 3 years, 1 month 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, 5 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 2 years 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, 6 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, 9 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** 3 years, 1 month 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, 9 months ago

controller <-> Application = northbound
controller <-> Devices = southbound

upvoted 14 times

 **dicksonpwc** Highly Voted 2 years ago

A is correct.

Explanation

A northbound interface is defined as the connection between the controller and applications

upvoted 6 times

 **SamuelSami** Most Recent 1 year 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** Highly Voted 1 year, 11 months ago

the correct Answer is A (allows configuration and monitoring of the network from one centralized point)

upvoted 7 times

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, 9 months ago

B: It has the most cisco product hype
upvoted 19 times

  **ismatdmour** Highly Voted  1 year, 5 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 13 times

  **Vinarino** Most Recent  1 year, 8 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, 4 months 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 5 times

  **Alsaheer** 2 years, 4 months ago

B is correct

upvoted 2 times

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

focused on network	Controller-Based Networking
focused on devices	
user input is a configuration	
user input is a policy	Traditional Networking
uses allow list security model	
uses block list security model	

Correct Answer:

Answer Area

focused on network	Controller-Based Networking
focused on devices	
user input is a configuration	
user input is a policy	Traditional Networking
uses allow list security model	
uses block list security model	

cormorant Highly Voted 10 months, 2 weeks ago

in short:
 traditional networking: bad
 controller-based networking: good
 upvoted 13 times

RougePotatoe Highly Voted 10 months, 2 weeks ago

Anyone have any idea on what they are referring to regarding the allow list and block list?
 upvoted 5 times

dropspablo 3 months ago

I believe that in traditional networks we focus more on blocks when creating ACLs. Unlike Software Defined Networks such as ACI (Application Policy Infrastructure Controller (APIC)) which focuses more on Permission Policies or SDA networks (DNA-Center controller) which also focuses on Permissions but with SGT, as these networks are Intent Based Networks (IBN) leaving the blocks and the rest to the Artificial Intelligence to do.
 upvoted 3 times

  **Request7108** 8 months, 2 weeks 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

  **espanrews** 3 months, 3 weeks 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** 3 months, 2 weeks 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

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, 9 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 44 times

 **nathnotnut** 6 months, 2 weeks ago

tell us that you're a reliable source without telling us you're a reliable source :))

upvoted 2 times

 **cdewet** Highly Voted 2 years, 9 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, 5 months ago

Selected Answer: AB

in C NICs are not part of VMs. Virtual switches of VMs are what connect virtual NICs of VMs to physical network (say a router). C is incorrect. Virtualization is not having the netgear or part of it in the Internet (This is cloud IaaS) but to have the physical server shared by multiple virtualized servers. However, we can have virtualized 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, 8 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, 8 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** 2 years, 2 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, 8 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 . A and B as previously stated. careful reading is key.

upvoted 5 times


 **bestboy120** 2 years, 8 months ago

Read the whole answer "The environment must be configured with one hypervisor that serves solely as a network manager to monitor SNMP traffic."

just because there is a word "hyperhivisor" itd doesnt mean its this

U dont need to configured anything with menager to monitor SNMP traffic

upvoted 4 times

 **Whippy29** 2 years, 11 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, 12 months ago



The correct answers are B and E. You can not talk about virtualization without talking about hypervisors.

upvoted 3 times

  **omsh** 3 years ago

yes the answer is BE

upvoted 3 times

  **ozy** 3 years ago

Correct answer BE

upvoted 3 times

  **dave1992** 1 year, 11 months ago

hypervisor manages the NIC, RAM, and CPU. not the software. E is not the answer.

upvoted 2 times

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 11 months, 3 weeks 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 14 times

  **dicksonpwc** Highly Voted 2 years 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 8 times

  **Ciscoman021** Most Recent 5 months, 3 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** 8 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 1 times

  **karels94** 11 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 1 times

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, 6 months ago

Funny how many questions are about the advantages of a DNA Center over a traditional network ^^ Good marketing Cisco upvoted 19 times

 **dicksonpwc** Highly Voted 2 years 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 5 times

 **Taloo** Most Recent 2 years, 6 months ago

I think it's C because Controller-based decouple control plane, not data plane upvoted 2 times

 **lordnano** 2 years, 6 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, 4 months ago

t'ha detto tutto lui

upvoted 2 times

 **studying_1** 3 months, 2 weeks ago

hai ragione, lol non parlo bene italiano e spagnolo, ma capisco poco, non c'è problema, parlo solo francese e inglese

upvoted 2 times

 **[Removed]** 2 months, 2 weeks ago

Are you French?

upvoted 1 times

 **XBfoundX** 2 years, 8 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

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, 10 months ago

Could literally say any of those answers
upvoted 12 times

  **yewastedmytime** 2 years, 9 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

  **[Removed]** Most Recent 2 months, 1 week ago


Selected Answer: BC

B. reduced operational costs
C. faster changes with more reliable results
upvoted 1 times

  **Request7108** 8 months, 2 weeks 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 2 times

  **splashy** 11 months, 4 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 4 times

  **Tylosh** 12 months 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** 1 year, 1 month 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, 5 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** 3 years, 1 month ago

How does it reduce operational cost ?
upvoted 3 times

  **chomjosh** 3 years, 1 month ago

Multiple processes are carried out from simple automation, delivering results in a timely and cost effective manner. Operational cost is therefore reduced.

upvoted 11 times

  **chomjosh** 3 years, 1 month 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

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 3 years, 1 month ago

JSON, XML = REST API

YAML = Ansible

upvoted 20 times

 **lordnano** 2 years, 6 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, 10 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 6 times

 **Ciscoman021** Most Recent 5 months, 3 weeks 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, 6 months ago

Here is the broken link: [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-](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)

[x/rest_cfg/2_1_x/b_Cisco_APIC_REST_API_Configuration_Guide/b_Cisco_APIC_REST_API_Configuration_Guide_chapter_01.html](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** 3 years, 2 months ago

Reference link is broken...

upvoted 1 times

 **ponder** 3 years, 2 months ago

<https://community.cisco.com/t5/nso-developer-hub-documents/rest-api-basics/ta-p/3635342>

upvoted 1 times

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 3 years, 1 month 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 13 times

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:

name: value

JSON can use arrays. Array values must be of type string, number, object, array, boolean or null. For example:

```
{
  name: "John",
  age: 30,
  cars: [ "Ford", "BMW", "Fiat" ]
}
```

JSON can have empty object like taskId: {}

 **i_am_confused** Highly Voted 1 year, 2 months ago


Answer is C. JSON uses { [: ,
JSON does NOT use - ;
upvoted 7 times

 **distortion** Highly Voted 2 years, 2 months ago


The layout is not great. But watch out for the : after the "response": part. and a , after each line.
upvoted 7 times

 **RODCCN** Most Recent 1 month, 2 weeks ago

C: <https://developer.mozilla.org/en-US/docs/Learn/JavaScript/Objects/JSON>
upvoted 1 times

 **dave1992** 1 year, 9 months ago

If you had a hard time. Look at the end between the " ____" it should be a colon. Not a - ;
upvoted 2 times

 **mrsiafu** 2 years, 4 months ago

This is a terrible representation... the layout that is

upvoted 4 times

DRAG DROP -

Drag and drop the descriptions from the left onto the configuration-management technologies on the right.

Select and Place:

Answer Area

- fundamental configuration elements are stored in a manifest
- uses TCP port 10002 for configuration push jobs
- uses Ruby for fundamental configuration elements
- uses SSH for remote device communication
- uses TCP 8140 for communication
- uses YAML for fundamental configuration elements

Ansible

Chef

Puppet

Correct Answer:

Answer Area

- fundamental configuration elements are stored in a manifest
- uses TCP port 10002 for configuration push jobs
- uses Ruby for fundamental configuration elements
- uses SSH for remote device communication
- uses TCP 8140 for communication
- uses YAML for fundamental configuration elements

Ansible

uses SSH for remote device communication

uses YAML for fundamental configuration elements

Chef

uses TCP port 10002 for configuration push jobs

uses Ruby for fundamental configuration elements

Puppet

fundamental configuration elements are stored in a manifest

uses TCP 8140 for communication

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

Embedded Ruby

(ERB) templates to create custom Puppet language files, offering a declarative-paradigm programming approach.

A Puppet piece of code is called a manifest, and is a file with .pp extension.

  **ostralo** Highly Voted 2 years, 3 months ago

I studied CCNA at Cisco Netacad... these things were not in the course...

No port information...

upvoted 25 times

  **mhayek** 10 months, 2 weeks ago

it actually is netacad in automation chapter in CCNA3

upvoted 2 times

  **[Removed]** 2 months, 2 weeks ago

It is in CCNA 3 chapter 14.5 but they don't talk about the ports nor SSH for Ansible

upvoted 1 times

  **ttomer** Highly Voted 2 years, 7 months ago

Both Chef and Puppet uses Ruby...

upvoted 21 times

  **dropspablo** Most Recent 3 months ago

(Answer is correct)

In summary, please remember the following important facts about Chef:

+ Use "pull" model (nodes are dynamically updated with the configurations that are present in the server)

+ Use TCP port 10002 (default command port) for configuration push jobs

+ Use Ruby for device configuration

+ Files needed for operation: Recipe, Cookbook...

<https://www.9tut.com/chef-tutorial>

upvoted 1 times

  **dropspablo** 3 months ago

We also made a comparison list of Ansible, Puppet and Chef automation tool here:


https://www.9tut.com/images/ccna_self_study/Ansible_Puppet_Chef/Ansible_Puppet_Chef_compare.jpg

upvoted 2 times

  **esandrews** 3 months, 3 weeks ago

It was difficult to find port numbers. When you search for them, these dump exam questions come up as primary reference, so go imagine what's the point

upvoted 1 times

  **KisDezso** 7 months, 3 weeks ago


This is some CCNP ENARSI questions

upvoted 1 times

  **Garfieldcat** 11 months, 1 week ago

both Chef and Puppet are ruby based

upvoted 1 times

  **kijken** 1 year, 7 months ago

It was in the course of pluralsight for CCNA, but I think this is a crap question that is not about Cisco networking. And besides of that, in real world you go with 1 of them, no point knowing all details of all 3

upvoted 3 times

  **awashenko** 1 year, 8 months ago

Could be one of the questions they're thinking about adding and it doesnt actually count towards your score. This is not in my CCNA academy course.

upvoted 1 times

  **JeffDidntKillHimself** 1 year, 9 months ago

haha pp extension

upvoted 6 times

  **oooMoo** 2 years, 4 months ago

Anisble

SSH

YAML

Chef

TCP 10002


Ruby

Puppet

manifest configurations

TCP 8140

upvoted 20 times

 **mrsiafu** 2 years, 4 months ago

you won't find this stuff in the official cert guide...

upvoted 14 times

Question #724

Topic 1

Which two capabilities of Cisco DNA Center make it more extensible as compared to traditional campus device management? (Choose two.)

- A. REST APIs that allow for external applications to interact natively
- B. adapters that support all families of Cisco IOS software
- C. SDKs that support interaction with third-party network equipment
- D. modular design that is upgradable as needed
- E. customized versions for small, medium, and large enterprises

Correct Answer: AC

Cisco DNA Center offers 360-degree extensibility through four distinct types of platform capabilities:

⇒ Intent-based APIs leverage the controller and enable business and IT applications to deliver intent to the network and to reap network analytics and insights for

IT and business innovation.

⇒ Process adapters, built on integration APIs, allow integration with other IT and network systems to streamline IT operations and processes.

⇒ Domain adapters, built on integration APIs, allow integration with other infrastructure domains such as data center, WAN, and security to deliver a consistent intent-based infrastructure across the entire IT environment.

⇒ SDKs allow management to be extended to third-party vendor's network devices to offer support for diverse environments.

Reference:

<https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-cent-platf-aag-cte-en.html>

 **Networknovice** Highly Voted 1 year, 4 months ago

SDN=Software-Defined Networking. Its in the name "software."

API's= Application Programming Interface. = software

REST API's = isn't a specific API but a set of rules for API's

SDKs= Software Development Kits

Enabling software to allow for external applications defiantly makes it more "extensible" (able to be extended). The traditional device management seemed to really want to keep things proprietary, or at least attempt a push in that direction. It appears now that Cisco knows it needs to adapt and allow for 3rd party devices/applications so that it can remain competitive.

upvoted 5 times

DRAG DROP -

Drag and drop the descriptions of device management from the left onto the types of device management on the right.

Select and Place:

implements changes via an SSH terminal	Cisco DNA Center Device Management [] [] []
manages device configurations on a per-device basis	
monitors the cloud for software updates	
security is managed near the perimeter of the network with firewalls, VPNs, and IPS	
uses CLI templates to apply a consistent configuration to multiple devices at an individual location	
uses NetFlow to analyze potential security threats throughout the network and take appropriate action on that traffic	
	Traditional Device Management [] [] []

Correct Answer:

implements changes via an SSH terminal	Cisco DNA Center Device Management monitors the cloud for software updates uses CLI templates to apply a consistent configuration to multiple devices at an individual location uses NetFlow to analyze potential security threats throughout the network and take appropriate action on that traffic
manages device configurations on a per-device basis	
monitors the cloud for software updates	
security is managed near the perimeter of the network with firewalls, VPNs, and IPS	
uses CLI templates to apply a consistent configuration to multiple devices at an individual location	
uses NetFlow to analyze potential security threats throughout the network and take appropriate action on that traffic	
	Traditional Device Management implements changes via an SSH terminal manages device configurations on a per-device basis security is managed near the perimeter of the network with firewalls, VPNs, and IPS

Dutch012 Highly Voted 6 months, 2 weeks ago
 Doing things nicely and easily = DNA
 upvoted 8 times

What software-defined architecture plane assists network devices with making packet-forwarding decisions by providing Layer 2 reachability and Layer 3 routing information?

- A. management plane
- B. control plane
- C. data plane
- D. policy plane

Correct Answer: B

  **IxlJustinlxl** Highly Voted 2 years, 3 months ago

The control plane is the part of a network that controls how data is forwarded, while the data plane controls the actual forwarding process. Making packet forwarding decisions is 'how data is forwarded'.

ANSWER = B

upvoted 15 times

  **Irios2799** Most Recent 6 months, 2 weeks ago


Selected Answer: B

Pls correct me if i'm wrong.

The control plane PROVIDE the layer 2 reachability and layer 3 routing information to assist the forwarding decisions in the data plane. It doesn't mean that the control plane MAKE the forwarding decision, only provide the tables and databases to data plane.



Thanks!

upvoted 2 times

  **jossyda** 1 year, 3 months ago



palabra clave... Asiste.

upvoted 3 times

  **DaBest** 1 year, 11 months ago

anyone knows what is the role of management plane?

upvoted 1 times

  **priya17** 1 year, 10 months ago

the device is configured and monitored in management plane

upvoted 5 times

  **dave1992** 1 year, 11 months ago

it manages

upvoted 6 times

  **nakres64** 2 years, 7 months ago

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/SDN/SDN.html

upvoted 4 times

What are two benefits of controller-based networking compared to traditional networking? (Choose two.)

- A. controller-based increases network bandwidth usage, while traditional lightens the load on the network
- B. controller-based reduces network configuration complexity, while traditional increases the potential for errors
- C. controller-based allows for fewer network failures, while traditional increases failure rates
- D. controller-based provides centralization of key IT functions, while traditional requires distributed management functions
- E. controller-based inflates software costs, while traditional decreases individual licensing costs


Correct Answer: BD

  **ITstudent123** Highly Voted 2 years, 10 months ago

- C. controller-based allows for fewer network failures, while traditional increases failure rates
- D. controller-based provides centralization of key IT functions, while traditional requires distributed management functions

Regarding the controller-based network, A and E are not benefits.
I don't know if C is true, but B and D are.

So B and D
upvoted 5 times

  **ITstudent123** 2 years, 10 months ago

Regarding the controller-based network, A and E are not benefits.
I don't know if C is true, but B and D are.

So B and D
upvoted 2 times

  **kadamske** 1 year, 11 months ago

C is not true, none of them can reduce a network failures.
upvoted 2 times

  **Zerotime0** 2 years, 8 months ago

Agreed we don't know if a team of techs are dumb or not. So C is out.
upvoted 4 times

  **cormorant** Most Recent 9 months ago

reduces network complexity and centralised key IT functions. end of story
upvoted 1 times

  **ProgSnob** 1 year, 9 months ago

C would make sense because it reduces the possibility for human error to cause an outage but B is more obvious and it also includes the issue with errors in the answer.
upvoted 1 times

  **LuisTon** 2 years, 1 month ago

Guys, Cisco itself has shared some numbers that show that a Controller-Based network does help your network to have fewer network errors throughout the time.
upvoted 3 times

  **ismatdmour** 1 year, 5 months ago

Controller based can have fewer network errors than traditional networking while configuration. Answer C takes about network failures and not configuration errors which should not increase or decrease with the use of controllers.
upvoted 1 times

Which type of API allows SDN controllers to dynamically make changes to the network?

- A. northbound API
- B. REST API
- C. SOAP API
- D. southbound API

Correct Answer: D

  **boghota** Highly Voted 2 years, 9 months ago

Are there CCNA 200-301 Topics that haven't been covered with these questions?
upvoted 13 times

  **martco** Highly Voted 2 years, 7 months ago



Answer is D

Cisco overview doc for SDN here: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/SDN/SDN.html

however I recommend everyone to spend 40 mins watching any of the (non-vendor specific) fundamentals of SDN/Openflow vids on YT...my personal rec is David Mahler's stuff

(fact is nowadays if you don't know some SDN basics you just won't be getting jobs anymore!!)

upvoted 10 times

  **DaBest** 1 year, 11 months ago

here is a link for David vid:

https://www.youtube.com/watch?v=DiChnu_PAzA

upvoted 4 times

  **cormorant** Most Recent 9 months ago

Southbound APIs facilitate control over the network and enable the SDN Controller to DYNAMICALLY MAKE CHANGES according to real-time demands and needs.

upvoted 2 times

DRAG DROP -

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

Select and Place:

accounting

tracks activity

authentication

updates session attributes

authorization

verifies access rights

CoA

verifies identity

Correct Answer:

accounting

accounting

authentication

CoA

authorization

authentication

CoA

authorization

recosmith12 Highly Voted 1 year ago
authentication and authorization are backwards
upvoted 28 times

perri88 3 months ago
agreed
upvoted 2 times

splashy 11 months, 4 weeks ago
Yup should be
accounting
coa
authorization
authentication
upvoted 20 times

mrgreat 12 months ago
Correct
upvoted 5 times

[Removed] Most Recent 2 months, 2 weeks ago
Answers are :

1 -accounting
2 - CoA
3 - authorization
4 - authentication
upvoted 2 times

Yannik123 4 months, 3 weeks ago

@examtopics please correct the answer it should be:

accounting

CoA

authorization

authentication

upvoted 3 times

  **ahmt** 6 months, 4 weeks ago

accounting

coa

authorization

authentication

upvoted 2 times

  **AlexFordly** 10 months, 2 weeks ago

accounting

coa

authorization

authentication

upvoted 2 times

Which option about JSON is true -

- A. uses predefined tags or angle brackets () to delimit markup text
- B. used to describe structured data that includes arrays
- C. used for storing information
- D. similar to HTML, it is more verbose than XML

Correct Answer: B

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:

```
{  
  "name": "Mark"  
}
```

JSON can use arrays. Array values must be of type string, number, object, array, boolean or null..

For example:

```
{  
  "name": "John",  
  "age": 30,  
  "cars": [ "Ford", "BMW", "Fiat" ]  
}
```

 **hamish88** 7 months, 2 weeks ago


As per my understanding, Json is a data storage/transfer method. So it doesn't describe anything. I will go with option C.
upvoted 1 times

 **oatmealturkey** 6 months, 3 weeks ago

That is not quite accurate. JSON is a data serialization language so as a language it describes things by definition. Read the Official Certification Guide Vol. 1 & 2 by Wendall Odom, trust me it will help. Page 419: "To describe the data structures, the data serialization languages include special characters and conventions that communicate ideas about list variables, dictionary variables, and other more complex data structures."
upvoted 2 times

 **g_mindset** 1 year ago

Trick question but would go with DESCRIBES DATA, considering the key/value pair structure. B is correct.
upvoted 1 times

 **YoniEth** 1 year, 10 months ago

It also used to store objects which is unordered type. Store information sums it up.
upvoted 2 times

 **DARKK** 1 year, 3 months ago

So would C be the right answer?
upvoted 1 times

Which option best describes an API?

- A. a contract that describes how various components communicate and exchange data with each other
- B. an architectural style (versus a protocol) for designing applications
- C. a stateless client-server model
- D. request a certain type of data by specifying the URL path that models the data

Correct Answer: A

 **Suhib** Highly Voted 2 years ago

A contract?!!! weird way to describe it!
upvoted 11 times


 **pythonshadow** Highly Voted 2 years ago

An API is a set of definitions and protocols for building and integrating application software. It's sometimes referred to as a contract between an information provider and an information user—establishing the content required from the consumer (the call) and the content required by the producer (the response).
<https://www.redhat.com/en/topics/api/what-is-a-rest-api>
upvoted 9 times

 **Shabeth** Most Recent 2 months, 2 weeks ago

Selected Answer: A

answer is A
upvoted 1 times


 **cormorant** 9 months, 2 weeks ago

Which option best describes an API? a contract that describes

thank God there are sites like this on the internet to prepare us for the real thing
upvoted 4 times

 **ar2** 1 year, 4 months ago

a stateless client-server model
upvoted 3 times

 **ar2** 1 year, 3 months ago

my mistake this is a rest api
upvoted 1 times


 **ismatdmour** 1 year, 5 months ago

Selected Answer: A

D sounds ok also, but A is more general (more correct). APIs may or may not use URLs. REST API use URI (http) which is common.
upvoted 1 times

 **BraveBadger** 1 year, 4 months ago

Nah, D is completely wrong, you can't just make up whatever URL you want to get the data you want, which is what I think D implies. The api is crafted in a way that the URL's are specific to the functionality.
upvoted 1 times

 **kijken** 1 year, 7 months ago

Sounds more like D, any thoughts anyone?
upvoted 2 times

 **Raman1996** 1 year, 7 months ago


you should study harder bro
upvoted 5 times

 **RainyPT** 1 year, 6 months ago



Been building API's for years now and honestly got confused too.
upvoted 2 times

 **ratboy5757** 11 months, 3 weeks ago

bro you're using dumps maybe u should too
upvoted 4 times

 **raydel92** 1 year, 9 months ago

Would this help?
<https://dzone.com/articles/designing-rest-api-what-is-contract-first>
upvoted 1 times

  **Ed12345** 1 year, 11 months ago

Correct answer is - a stateless client-server model
upvoted 2 times

  **jahinchains** 1 year, 4 months ago

that is rest api
upvoted 2 times

DRAG DROP -


Drag and drop the characteristics of a cloud environment from the left onto the correct examples on the right.


Select and Place:

multitenancy	One or more clients can be hosted with the same physical or virtual infrastructure
on-demand	Resources can be added and removed as needed to support current workload and tasks
resiliency	Tasks can be migrated to different physical locations to increase efficiency or reduce cost.
scalability	Resources are dedicated only when necessary instead of on a permanent
workload movement	Tasks and data residing on a failed server can be seamlessly migrated to other physical resources.

Correct Answer:

multitenancy	multitenancy
on-demand	scalability
resiliency	workload movement
scalability	on-demand
workload movement	resiliency

 **shakyak** Highly Voted 1 year, 9 months ago
 multitenant->One or more
 Scalability->add and remove if needed
 Workload Movement->migrate
 on-demand->dedicated if needed
 Resiliency->Failure seamless recovery
 upvoted 22 times

 **DaBest** Most Recent 1 year, 11 months ago
 In cloud computing, multitenancy means that multiple customers of a cloud vendor are using the same computing resources. Despite the fact that they share resources, cloud customers aren't aware of each other, and their data is kept totally separate. Multitenancy is a crucial component of cloud computing; without it, cloud services would be far less practical. Multitenant architecture is a feature in many types of public cloud computing, including IaaS, PaaS, SaaS, containers, and serverless computing.

<https://www.cloudflare.com/learning/cloud/what-is-multitenancy/>
upvoted 2 times

 **BooleanPizza** 2 years ago

"Resources can be added or removed as needed to support current workloads and tasks" is actually elasticity, but close enough I guess.
upvoted 2 times

 **vadiminski** 2 years, 4 months ago

I believe the answer is correct, can't give a reliable source though
upvoted 2 times

Question #733

Topic 1

Which of the following is the JSON encoding of a dictionary or hash?

A. {key: value}

B. [key, value]

C. {key, value}

D. (key: value)

Correct Answer: A

 **Sten111** Highly Voted 2 years, 2 months ago

Here are the actual answers

<https://itexamanswers.net/question/which-of-the-following-is-the-json-encoding-of-a-dictionary-or-hash>

upvoted 10 times

 **Micah7** Highly Voted 2 years, 3 months ago

You can still tell the answer based on the symbols used- The 3 here below:

```
:  
{  
,
```

The: is always in the middle as well.....

upvoted 6 times

 **Nebulise** 1 year, 7 months ago

I hope Micah here isn't short for Micah Bell

upvoted 4 times

 **Hari2512** Most Recent 3 months, 1 week ago

Which of the following is the JSON encoding of a dictionary or hash?


A. {"key": "value"}

upvoted 1 times

 **sasquatchshrimp** 1 year, 1 month ago

this question lets me know that I am a network master.

upvoted 4 times

 **Nvoid** 1 year, 8 months ago

Hey fix the encoding on the site! use url encoding, unicode, or ascii come on now!

upvoted 3 times

 **Hodicek** 1 year, 9 months ago

A. {"key": "value"}

upvoted 5 times

 **Erconte98** 2 years, 3 months ago

re-established the question because after the download it is hidden

upvoted 1 times

Which role does a hypervisor provide for each virtual machine in server virtualization?

- A. infrastructure-as-a-service
- B. Software-as-a-service
- C. control and distribution of physical resources
- D. services as a hardware controller

Correct Answer: C


  **DaBest** Highly Voted 1 year, 11 months ago

Answer is correct. The hypervisor creates and manages virtual machines on a host computer and allocates physical system resources to them.
upvoted 9 times

  **[Removed]** Most Recent 2 months, 1 week ago

Selected Answer: C

C. control and distribution of physical resources
That's correct, physical resources such as CPU, RAM, NIC, storage..
upvoted 1 times

  **dave1992** 1 year, 11 months ago

i think D is also correct. i manages or controls the CPU, RAM and NIC hardware.
upvoted 3 times

  **Request7108** 8 months, 2 weeks ago

It is correct but it's not the best answer. It is more than simply a hardware controller.
upvoted 2 times

What is the function of a server?

- A. It transmits packets between hosts in the same broadcast domain.
- B. It provides shared applications to end users.
- C. It routes traffic between Layer 3 devices.
- D. It reates security zones between trusted and untrusted networks.

Correct Answer: B

Which CRUD operation modifies an existing table or view?

- A. read
- B. update
- C. replace
- D. create

Correct Answer: B

  **tchekdy** Highly Voted 2 years, 6 months ago

Create (SQL INSERT) : POST - Used to support the creation of a child resource, but can also modify the underlying state of a system.

Read (SQL SELECT) : GET - Retrieve a representation of a resource, but with additional semantics available.

Update (SQL UPDATE) : PUT - Update a resource using a full representation. Can also be used to create a resource. The full representation requirement is a large caveat, see the following.

Update (again) : PATCH - Update a resource using a partial representation.

Delete (SQL DELETE) : DELETE - Delete a resource. This is the best matched mapping.

upvoted 13 times

  **Nhan** Highly Voted 2 years, 6 months ago

Create, read, update and delete, there is an existing table, which it's already create so the crud will update it

upvoted 5 times

  **Cyberops** Most Recent 1 year, 3 months ago

Selected Answer: B

modifies is the keyword

upvoted 3 times

In software-defined architectures, which plane is distributed and responsible for traffic forwarding?

- A. management plane
- B. policy plane
- C. data plane
- D. control plane

Correct Answer: C

  **Nicocisco** Highly Voted 1 year, 6 months ago

Selected Answer: C

Yeah C because in software-defined architectures, control plane is centralised, and data plane still distributed.

data plane forward traffic.

upvoted 8 times

  **[Removed]** Most Recent 2 months, 1 week ago

Selected Answer: C

C. data plane

upvoted 1 times

  **yuz1227** 6 months, 1 week ago

Selected Answer: C

data plane aka forwarding plane

upvoted 2 times

Refer to the exhibit. Which type of configuration is represented in the output?

```
cisco_ospf_vrf {"R1 default":  
  ensure => 'present',  
  auto_cost => '100',  
}
```

- A. Ansible
- B. JSON
- C. Chef
- D. Puppet

Correct Answer: D

Reference:

<https://forge.puppet.com/modules/puppetlabs/ciscopuppet/1.0.0>

 **wondaah** Highly Voted 6 months, 1 week ago

Puppet => arrows, easiest way to remember
upvoted 17 times

Which configuration management mechanism uses TCP port 22 by default when communicating with managed nodes?

- A. Ansible
- B. Python
- C. Puppet
- D. Chef

Correct Answer: A

  **ZayaB** Highly Voted 2 years, 6 months ago

Ansible:


- uses SSH (port 22) for remote device communication
- uses YAML for fundamental configuration

Chef:

- uses TCP port 10002 for configuration push jobs
- uses Ruby for fundamental configuration elements



Puppet:

- uses TCP 8140 for communication
 - fundamental configuration elements are stored in a manifest
- upvoted 46 times

  **Hodicek** 1 year, 9 months ago

excellent

upvoted 4 times

  **martco** Highly Voted 2 years, 7 months ago

Answer A

sneaky question because you could make use of SSH universally in device configuration scenarios....but the keyword terminology here is "managed nodes" which is part of the Ansible architecture description....A is the most correct

upvoted 6 times

  **DavidCisco** Most Recent 4 months, 2 weeks ago

Selected Answer: A

<https://www.ansible.com/overview/how-ansible-works>

upvoted 2 times

What does an SDN controller use as a communication protocol to relay forwarding changes to a southbound API?

- A. Java
- B. REST
- C. OpenFlow
- D. XML

Correct Answer: C

 **Aleks123** Highly Voted 1 year, 8 months ago

How Do SDN Southbound APIs Work?

Southbound APIs facilitate control over the network and enable the SDN Controller to dynamically make changes according to real-time demands and needs.

OpenFlow, which was developed by the Open Networking Foundation (ONF), is the first and probably most well-known southbound interface. OpenFlow defines the way the SDN Controller should interact with the forwarding plane to make adjustments to the network, so it can better adapt to changing business requirements. With OpenFlow, entries can be added and removed to the internal flow-table of switches and routers to make the network more responsive to real-time traffic demands.

upvoted 17 times

What uses HTTP messages to transfer data to applications residing on different hosts?

- A. OpenStack
- B. OpFlex
- C. REST
- D. OpenFlow

Correct Answer: C

 **dicksonpwc** Highly Voted 2 years ago

C is correct.

Explanation:

A RESTful API is an architectural style for an application program interface (API) that uses HTTP requests to access and use data. That data can be used to GET, PUT, POST and DELETE data types, which refers to the reading, updating, creating and deleting of operations concerning resources.

<https://searcharchitecture.techtarget.com/definition/RESTful-API>

upvoted 8 times

 **Dante_Dan** Most Recent 1 year, 7 months ago

Selected Answer: C

REST (Representational State Transfer) describes a type of API that allows applications to sit on different hosts, using HTTP messages to transfer data over the API.

upvoted 3 times

Which JSON data type is an unordered set of attribute-value pairs?

- A. string
- B. array
- C. Boolean
- D. object

Correct Answer: D

 **MikD4016** Highly Voted 11 months, 3 weeks ago

JSON Object :

An object is an unordered set of name/value pairs. An object begins with { (left brace) and ends with } (right brace). Each name is followed by : (colon) and the name/value pairs are separated by , (comma).

JSON Array :

An array is an ordered collection of values. An array begins with [(left bracket) and ends with] (right bracket). Values are separated by , (comma).
upvoted 11 times

 **dave1992** Most Recent 1 year, 9 months ago

Key:Value Pair: Each and every colon identifies one key:value pair, with the key before the colon and the value after the colon.

■ Key: Text, inside double quotes, before the colon, used as the name that references a value.

424 CCNA 200-301 Official Cert Guide, Volume 2

■ Value: The item after the colon that represents the value of the key, which can be

■ Text: Listed in double quotes.


■ Numeric: Listed without quotes.

■ Array: A special value (more details later).

■ Object: A special value (more details later)

■ Multiple Pairs: When listing multiple key:value pairs, separate the pairs with a comma at the end of each pair (except the last pair)

upvoted 4 times

 **sp3nc3** 1 year, 10 months ago

D is correct

In JSON, they take on these forms:

An object is an unordered set of name/value pairs. An object begins with {left brace and ends with }right brace. Each name is followed by :colon and the name/value pairs are separated by ,comma.

<https://www.json.org/json-en.html>

upvoted 4 times

 **dicksonpwc** 2 years ago

D is correct.

Explanation:


JSON (JavaScript Object Notation) is an open standard file format and data interchange format that uses human-readable text to store and transmit data objects consisting of attribute–value pairs and arrays (or other serializable values).

upvoted 1 times

 **Insidious_Intent** 2 years ago

How is this not an array?

upvoted 2 times

 **iGlitch** 1 year, 3 months ago

I thought it was the array at first, but the question states that it's an "Attribute-value pair" and the array in JSON looks like this { "Key":["Value", "Value", "Value"]} }

upvoted 1 times

 **Myname1277** 2 years ago

Arrays are ordered I guess

upvoted 2 times

 **digimaniac** 2 years ago

agree, should be array

upvoted 2 times

 **BooleanPizza** 2 years ago

Because an array is an ordered list of elements.
upvoted 2 times

Question #743

Topic 1

Which protocol is used in Software Defined Access (SDA) to provide a tunnel between two edge nodes in different fabrics?

- A. Generic Router Encapsulation (GRE)
- B. Virtual Local Area Network (VLAN)
- C. Virtual Extensible LAN (VXLAN)
- D. Point-to-Point Protocol (PPP)

Correct Answer: C

 **Dibilli** Highly Voted 2 years, 1 month ago

OMG. why CCNA contains such a question???
upvoted 9 times

 **Gandzasar** 2 years ago

I don't know
upvoted 3 times

 **DaBest** 1 year, 11 months ago

i agree, it should have been question number 404 instead of 403 ~_~"
upvoted 2 times

 **BooleanPizza** 2 years ago

Because SDA is part of the exam objectives. Also the CCNA changed alot in the last couple of years, it's no longer CCNA R&S, it includes stuff from the old CCNA Security, Wireless, etc
upvoted 2 times

 **Cynthia2023** Most Recent 1 month, 4 weeks ago

VXLAN is a network encapsulation technique used in modern data center environments and Software Defined Networking (SDN) architectures, including SDA. It is designed to enable scalable and flexible network virtualization by encapsulating Layer 2 Ethernet frames in UDP (User Datagram Protocol) packets.

In SDA, VXLAN is employed to create an overlay network that can span across different fabrics and provide connectivity between edge nodes in a scalable and efficient manner. VXLAN helps overcome the limitations of traditional VLAN-based networks and allows for more dynamic and automated provisioning of network services in a software-defined environment.

upvoted 1 times

 **rictorres333** 1 year ago

Selected Answer: C


Chapter 17, Vol2
upvoted 1 times

 **dicksonpwc** 2 years ago

C is correct
Explanation:

The SD(Cisco® Software-Defined Access)-Access fabric uses the VXLAN data plane to provide transport of the full original Layer 2 frame and additionally uses LISP as the control plane to resolve endpoint-to-location (EID-to-RLOC) mappings. The SD-Access fabric replaces sixteen (16) of the reserved bits in the VXLAN header to transport up to 64,000 SGTs using a modified VXLAN-GPO (sometimes called VXLAN-GBP) format described in <https://tools.ietf.org/html/draft-smith-vxlan-group-policy-04>.

upvoted 4 times

 **gaber** 1 year, 8 months ago

It's that simple.
upvoted 2 times

Which plane is centralized by an SDN controller?

- A. management-plane
- B. data-plane
- C. services-plane
- D. control-plane

Correct Answer: D

  **Hodicek** Highly Voted 1 year, 9 months ago

D IS CORRECT ANSWER

upvoted 6 times

  **wondaah** Most Recent 6 months, 1 week ago

Selected Answer: D

D is correct

upvoted 2 times

  **cormorant** 9 months ago

Which plane is centralized by an SDN CONTROLLER?!

the CONTROL plane

upvoted 3 times

  **Bobrock** 1 year, 10 months ago

Control plane is centralized. = B is correct

upvoted 2 times

  **dicksonpwc** 2 years ago

B is correct. SDN Architecture The SDN control plane is centralized while the data plane is distributed. The centralized nature of the control plane makes the network flexible and enhances flow forward decision-making. The SDN controller resides in the control plane of an SDN architecture that can be programmed externally.

upvoted 4 times

  **dave1992** 1 year, 9 months ago

so you mean D then ?

upvoted 4 times

Where is the interface between the control plane and data plane within the software-defined architecture?

- A. application layer and the management layer
- B. application layer and the infrastructure layer
- C. control layer and the application layer
- D. control layer and the infrastructure layer

Correct Answer: D

  **kijken** Highly Voted 1 year, 7 months ago

Data plane is infrastructure layer
Control plane is Control layer
upvoted 22 times

  **cormorant** Highly Voted 9 months ago

so the question is just asking to translate control plane and data plane into SDA language?!
upvoted 6 times

Why would a network administrator choose to implement automation in a network environment?

- A. To simplify the process of maintaining a consistent configuration state across all devices
- B. To centralize device information storage
- C. To implement centralized user account management
- D. To deploy the management plane separately from the rest of the network

Correct Answer: A

  **Paul1111** 2 weeks ago

Correct
upvoted 1 times

Which two events occur automatically when a device is added to Cisco DNA Center? (Choose two.)

- A. The device is placed into the Managed state.
- B. The device is placed into the Unmanaged state.
- C. The device is assigned to the Local site.
- D. The device is assigned to the Global site.
- E. The device is placed into the Provisioned state.

Correct Answer: AD

🗨️ 👤 **Wong93** Highly Voted 2 years ago

Device in Global Site: When you successfully add, import, or discover a device, Cisco DNA Center places the device in the Managed state and assigns it to the Global site by default.

So I believe the answer is A and D.
upvoted 26 times

🗨️ 👤 **cortib** 1 year, 12 months ago

agree. source:
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-0-x/b_dnac_ug_1_0/b_dnac_ug_1_0_chapter_01110.html
upvoted 5 times

🗨️ 👤 **Pkard** 1 year, 9 months ago

also agree, here is the relevant section from Cortib's link:

"Device in Global Site—When you successfully add, import, or discover a device, DNA Center places the device in the Managed state and assigns it to the Global site by default. Even if you have defined Syslog and SNMP server settings for the Global site, DNA Center does not change the Syslog and SNMP server settings on the device."
upvoted 1 times

🗨️ 👤 **cormorant** Most Recent 9 months, 2 weeks ago

global site and managed site.
a device added to cisco dna's centre is akin to someone being hired at a company. the new employee needs to be managed and globalised to integrate
upvoted 2 times

🗨️ 👤 **Aboed** 1 year, 8 months ago

Selected Answer: AD

Device in Global Site—When you successfully add, import, or discover a device, DNA Center places the device in the Managed state and assigns it to the Global site by default. Even if you have defined Syslog and SNMP server settings for the Global site, DNA Center does not change the Syslog and SNMP server settings on the device.
upvoted 2 times

🗨️ 👤 **Hodicek** 1 year, 9 months ago

A- D R CORRECT ANSWERS
upvoted 1 times

🗨️ 👤 **Samuelpn96** 1 year, 11 months ago

In the section "What Should I Know Before I Start" it says that on a succesful discovery, the devices are placed in managed state. It shows a picture of the global inventory with added devices in managed state.

https://www.cisco.com/c/dam/en_us/training-events/product-training/dnac-13/DNAC13_AddingDevicesByUsingDiscovery.pdf

So, for me the answer is Managed and Global.
upvoted 4 times

🗨️ 👤 **Toob93** 1 year, 11 months ago

A,d correct
upvoted 4 times

Which two components are needed to create an Ansible script that configures a VLAN on a switch? (Choose two.)

- A. playbook
- B. recipe
- C. model
- D. cookbook
- E. task

Correct Answer: AE


  **sovafal192** Highly Voted  1 year, 7 months ago

Selected Answer: AE


Ansible works with playbooks, which contains tasks.
upvoted 13 times

  **AWSEMA** Most Recent  1 year, 2 months ago

Inventory. The "inventory" is a configuration file where you define the host information. ...
Playbooks. In most cases – especially in enterprise environments – you should use Ansible playbooks. ...
Plays. Playbooks contain plays. ...
Tasks. ...
Roles. ...
Handlers. ...
Templates. ...
Variables.
upvoted 2 times

  **Liuka_92** 1 year, 2 months ago

answer B and D:
Chef works with cookbooks, which contains recipe.
upvoted 2 times

  **Paulo231** 2 months, 3 weeks ago

That's bs
upvoted 1 times

  **SVN05** 7 months ago

Your explanation about Chef is spot on but you misunderstood the question. Read again. It stated components required for Ansible not Chef.
upvoted 3 times

  **JonasWolfxin** 1 year, 1 month ago

stupid guy
upvoted 6 times

  **battery1979** 1 year, 2 months ago

The question asked about Ansible.
upvoted 2 times

In software-defined architecture, which plane handles switching for traffic through a Cisco router?

- A. control
- B. data
- C. management
- D. application

Correct Answer: B

  **EthanhuntMI6** 9 months ago

How & why?

upvoted 4 times

  **Yaqub009** 7 months ago

<https://blog.ip-space.net/2013/08/management-control-and-data-planes-in.html>

Management Plane - For configuration device. CLI or GUI. Some protocol uses here: SSH, Telnet, SNMP, TFTP, SFTP, HTTPS. For example, you config router with Management plane on CLI.

Control Plane - This is brain of device. This plane MAKE A DECISION. STP, ARP, OSPF, EIGRP, BGP used this plane for ROUTING.

Data Plane - Called also Forwarding Plane. It's uses for Packet FORWARDING.

Generalization:

You config device Management Plane.

Device learn ROUTING path with Control Plane, and write it Routing Information Base (RIB) and Forwarding Information Base (FIB).

Data Plane use FIB for FORWARDING.

upvoted 1 times

  **kennie0** 3 months, 3 weeks ago

just answer the question and stop beating around the bush

upvoted 2 times

What are two southbound APIs? (Choose two.)

- A. Thrift
- B. DSC
- C. CORBA
- D. NETCONF
- E. OpenFlow

Correct Answer: DE

OpenFlow is a well-known southbound API. OpenFlow defines the way the SDN Controller should interact with the forwarding plane to make adjustments to the network, so it can better adapt to changing business requirements.

The Network Configuration Protocol (NetConf) uses Extensible Markup Language (XML) to install, manipulate and delete configuration to network devices.

Other southbound APIs are:

• onePK: a Cisco proprietary SBI to inspect or modify the network element configuration without hardware upgrades.

• OpFlex: an open-standard, distributed control system. It send summary policy to network elements.

 alexiro Highly Voted 3 years, 1 month ago

Chapter 16. Introduction to Controller-Based Networking CCNA v10 2
SBI interface

the second major section gives three sample architectures that happen to show three separate SBIs, specifically:
OpenFlow (from the ONF; www.opennetworking.org)
OpFlex (from Cisco; used with ACI)
CLI (Telnet/SSH) and SNMP (used with Cisco APIC-EM)
CLI (Telnet/SSH) and SNMP, and NETCONF (used with Cisco Software-Defined Access)
upvoted 8 times

 StingVN Most Recent 3 months, 3 weeks ago

Selected Answer: DE

The two southbound APIs commonly used in networking are:

D. NETCONF: NETCONF (Network Configuration Protocol) is a standardized protocol used for managing network devices. It provides mechanisms to retrieve, configure, and manage network devices using XML-based data encoding and remote procedure calls.

E. OpenFlow: OpenFlow is a protocol that enables communication between the control plane and the forwarding plane of a software-defined network (SDN). It allows for centralized control and programmability of network switches and routers.

Therefore, the correct answers are D. NETCONF and E. OpenFlow.

upvoted 1 times

What makes Cisco DNA Center different from traditional network management applications and their management of networks?

- A. Its modular design allows the implementation of different versions to meet the specific needs of an organization.
- B. It only supports auto-discovery of network elements in a greenfield deployment.
- C. It omits support high availability of management functions when operating in cluster mode.
- D. It abstracts policy from the actual device configuration.

Correct Answer: D

  **welju** Highly Voted 3 years, 2 months ago

A if we are being asked about benefits of deployment
D if we are being asked about device management
upvoted 38 times

  **khalid86** Highly Voted 2 years, 11 months ago

D is correct.

Automation: Using controllers and open APIs, Cisco DNA simplifies network management through abstraction and centralized policy enforcement that allows IT to focus on business intent and consistently apply configurations to improve service and keep operations consistently secure from the core to the edge.

<https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-06-digital-nw-architect-faq-cte-en.html>
upvoted 7 times

  **hamish88** Most Recent 7 months, 2 weeks ago

I guess A is not wrong but a fact that is possible in both management types, however, D is the real difference between these two designs.
upvoted 1 times

  **splashy** 11 months, 4 weeks ago

Selected Answer: D

The primary characteristic and difference is still the separation of control and data plane:

How is the policy abstract or abstracted from the device configuration?

-It is separated from the device configuration. It is implemented on a higher, centralized level.
-It is configured (mostly) in a GUI, which is a different way of interfacing than on the devices themselves.

A is aiming more for qualities like for example scalability. And the way the sentence is worded would imply that traditional networking is not scalable (or very limited) to the needs of an organization.



upvoted 4 times

  **ismatdmour** 1 year, 5 months ago

Selected Answer: A

CISCO DNA Center abstracts policy, correct. However, it does abstract (summarise) policy from the intent (from top) and not from the actual devices configuration. The abstracted policy is down enforced to actual devices (not vice versa). Hence D violates actual intention of DNA/SDN networks. A is correct. It is one goal of SDNs and Centralized controllers.

upvoted 1 times

  **xped2** 1 year, 6 months ago

Correct Answer: B

A. DNA is single pane of glass. The answer says modular but after that the answer is too vague.

B. Auto-discovery only in greenfield, brownfield you have to manually add the device. Traditional Management requires manual adding too (this is the difference)

C. Cluster is for HA

D. The Cisco DNA controller translates abstract expression of policy into actual device configuration. Not the other way around, as D suggests.

Reference Link: <https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2/iwan/quick-start/iwan-app-quick-start-2-2/workflows.pdf>

upvoted 1 times

  **Vinarino** 1 year, 8 months ago

WHAT IS DIFFERENT - between old & new is being asked...

Not Benefits - Not Device Management

upvoted 1 times

  **Vinarino** 1 year, 8 months ago

Automation is STEP 4 in a GREENFIELD deployment

See: ==> Cisco DNA Center SD-Access LAN Automation Deployment Guide <==

upvoted 1 times

  **Vinarino** 1 year, 8 months ago

Greenfield deployment refers to the installation of an IT system where previously there was none.

==> Cisco DNA Center SD-Access LAN Automation Deployment Guide <==

In four main steps, the Cisco LAN automation workflow helps enterprise IT administrators prepare, plan, and automate greenfield networks:

Step 1

Plan: Understand the different roles in the LAN automation domain. Plan the site and IP pool and understand the prerequisites for seed devices.

Step 2

Design: Design and build global sites. Configure global network services and site-level network services. Configure global device credentials.

Design the global IP address pool and assign the LAN automation pool.

Step 3

Discover: Discover seed devices.

Step 4

Provision: Start and stop LAN automation:

A: Start LAN automation: Push the temporary configuration to seed devices, discover devices, upgrade the image, and push the initial configuration to discovered devices.

B: Stop LAN automation: Convert all point-to-point links to Layer 3.

upvoted 1 times

  **dicksonpwc** 2 years ago



D is correct.

Explanation:

AI endpoint analytics

Implementation of DPI and other methods to identify endpoint clients upon accessing the network. Then uses AI/ML to place them into logical groups so that policies can be assigned based on the endpoint requirements.

upvoted 1 times

  **ostralo** 2 years, 3 months ago

Because Cisco DNA center is using intent-based Network, so I believe option D "It abstracts policy from the actual device configuration." is incorrect

it should be it abstracts policy from intents...

upvoted 3 times

  **anonymous1966** 2 years, 6 months ago

The question asks basically to compare DNA with PI and the answer is de SDA capability. So, I agree with "D"

upvoted 3 times

  **devildog** 2 years, 11 months ago

Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task. The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity—greatly facilitating remote office setups.

upvoted 2 times

  **Ebenezer** 2 years, 11 months ago


You don't have to fret. D is the correct answer.

upvoted 4 times

  **Sheikh_Shams** 3 years, 1 month ago

I am confuse about A and D but I think A is correct.from my research.

upvoted 3 times

  **naw** 3 years, 2 months ago

Without enough first-hand experience using DNA center, I can only assume that there is a very specific version range of firmware and hardware permitted. While some different versions may be usable together, the broad statement of "...allows someone to implement different versions..." would require a lot of clarification.



Additionally, the user/access/QoS policy/ies can be configured, and maintained somewhere other than on the specific piece of equipment. The various wireless APs don't have to make the decision about denying connectivity, or shaping traffic. This is a big point of debate, because air-time is finite, but LAN bandwidth is effectively infinite by comparison, so it can make a lot of sense to do a lot of this work on the AP... depending on your specific implementation.

upvoted 3 times

  **dave369** 3 years, 3 months ago

After a lot of research, I can't find anything that supports "D" as the answer.

upvoted 4 times

  **mikexb** 3 years, 2 months ago

i mean, isn't the defining characteristic of the DNA center functionality that it moves the control plane away from the local devices? Since policy is implemented at the control plane level, and the control plane no longer resides at the device, this suggests D is true.

I'm having a hard time finding why A is wrong though...
upvoted 5 times

Question #752

Topic 1

Which API is used in controller-based architectures to interact with edge devices?

- A. southbound
- B. overlay
- C. northbound
- D. underlay

Correct Answer: A

  **vadiminski** Highly Voted  2 years, 4 months ago

overlay: the virtual network
underlay: the physical network
nothbound: interacts with the server
the given answer is correct
upvoted 35 times

  **sdokmak** 2 years, 2 months ago

Good summary
upvoted 7 times

  **dicksonpwc** Most Recent  2 years ago

Northbound APIs do not interact with end devices.
A is correct. As the southbound interface is the connection between the controller and the physical networking hardware.
upvoted 3 times

DRAG DROP -

Drag and drop the statements about networking from the left onto the corresponding networking types on the right.

Select and Place:

Answer Area

- This type allows better control over how networks work and how networks are configured.
- This type enables networks to integrate with applications through APIs.
- New devices are configured using the physical infrastructure.
- This type provisions resources from a centralized location.
- This type requires a distributed control plane.

Controller-Based Networking

Traditional Networking

Correct Answer:

Answer Area

- This type allows better control over how networks work and how networks are configured.
- This type enables networks to integrate with applications through APIs.
- New devices are configured using the physical infrastructure.
- This type provisions resources from a centralized location.
- This type requires a distributed control plane.

Controller-Based Networking

This type allows better control over how networks work and how networks are configured.

This type enables networks to integrate with applications through APIs.

This type provisions resources from a centralized location.

Traditional Networking

New devices are configured using the physical infrastructure.

This type requires a distributed control plane.

VictorCisco 5 months, 2 weeks ago

just to be honest, ANY NEW device configured via physical infrastructure firstly, no matter where it will be used.
upvoted 1 times

RougePotatoe 10 months ago

I think
New devices are configured using the physical infrastructure
this type enables networks to integrate with applications through APIs
this type provisions resources from a centralized location

this type allows better control over how networks work and how networks are configured
this type requires a distributed control plane

Traditional requires the user to manually setup the AP where as controller based you could have the WLC just configure the AP for you.
Traditional configuration methods also allow you to have more control over each AP. Feel free to prove me wrong.
upvoted 2 times

  **dropspablo** 3 months ago

This is not about Wireless LAN Controllers (WLC), it is referring to SDN Automation when referring to "Controller-Based Network". And Traditional Networks would be just a network without SDN controller (OpenDayLight, APIC, APIC-Enterprise, DNA Center...). In traditional managers such as Cisco Prime Infrastructure (PI) and Cisco DNA Center management (with Controller DNA Center) there is a Plug-and-play feature that automatically installs the device when connecting the cable and powering on (I don't know which ones devices). A traditional network without even a CISCO PI manager would not have this capability. I believe that's why.

upvoted 2 times

```
1 [  
2  { "switch": "3750", "port": e2 },  
3  { "router": "2951", "port": e20 },  
4  { "switch": "3750", "port": e23 },  
5 ]
```

Refer to the exhibit. What is represented beginning with line 1 and ending with line 5?

- A. object
- B. value
- C. key
- D. array

Correct Answer: A

 **splashy** Highly Voted 1 year ago

Selected Answer: D

Netacad Mod 3 14.2.6

These are some of the characteristics of JSON:

It uses a hierarchical structure and contains nested values.

It uses braces { } to hold objects and square brackets [] hold arrays.

Its data is written as key/value pairs.

upvoted 9 times

 **Timbul** Highly Voted 8 months, 3 weeks ago

The answer is array. Please fix

upvoted 5 times

 **Vikramaditya_J** Most Recent 1 month, 1 week ago

Selected Answer: D

No second thought. It's a JSON array. In JSON, an array is an ordered list of values enclosed in square brackets ([]). Each value within the array can be of any valid JSON data type, such as objects, strings, numbers, or other arrays. In this case, the JSON code represents an array containing three objects, each containing key-value pairs.

Each line in the JSON code represents an element (object) within the array. Each object contains key-value pairs, such as "switch": "3750", "port": "e2" in line 2, "router": "2951", "port": "e20" in line 3, and so on.


upvoted 1 times

 **perri88** 3 months ago

Selected Answer: D

an array of objects

upvoted 1 times

 **4aynick** 3 months, 3 weeks ago

It is array of objects

correct D

<https://medium.com/@angela.amarapala/difference-between-arrays-and-json-objects-fa1c8598f9f1>

upvoted 1 times

 **4aynick** 3 months, 3 weeks ago

it is array of objects

Correct D

upvoted 1 times

 **Shansab** 9 months ago

Selected Answer: D

Array is correct

upvoted 4 times

 **michael1001** 9 months, 1 week ago

Selected Answer: D



It is array, please fix.

upvoted 2 times

 **Yunus_Empire** 9 months, 2 weeks ago

Selected Answer: D

Array is Right
upvoted 2 times

  **Etidic** 10 months, 3 weeks ago

Selected Answer: D

the answer is D
upvoted 2 times

  **rictorres333** 1 year ago

Selected Answer: D

Array is correct.
upvoted 3 times

  **Paszak** 1 year, 2 months ago

Array of objects
upvoted 2 times

Question #755

Topic 1

Which CRUD operation corresponds to the HTTP GET method?

- A. create
- B. read
- C. delete
- D. update

Correct Answer: B

Reference:

<https://hub.packtpub.com/crud-operations-rest/>

  **Nickname53796**  1 year, 3 months ago

Selected Answer: B

Create action is POST,
Read action are GET, HEAD and OPTIONS,
Update actions are PUT and PATCH,
Delete action is DELETE.

Good job on not picking the same answer, A, as the original braindump from 2021
upvoted 11 times

What differentiates device management enabled by Cisco DNA Center from traditional campus device management?

- A. CLI-oriented device
- B. centralized
- C. device-by-device hands-on
- D. per-device

Correct Answer: B

 **hp2wx** 1 year, 1 month ago

Selected Answer: B

Selected answer is correct. When using Cisco DNA Center to manage network device, device management is centralized and is managed from the DNA center GUI. Using DNA Center allows for us to have a more centralized management of network infrastructure as configuration changes can be applied to an many devices at once when these changes are done through DNA Center
upvoted 4 times

DRAG DROP -

Drag and drop the statements about networking from the left onto the corresponding networking types on the right.

Select and Place:

Answer Area

This type deploys a consistent configuration across multiple devices.	Controller-Based Networking <div style="background-color: #FFFF00; height: 20px; width: 100%; margin-bottom: 5px;"></div> <div style="background-color: #FFFF00; height: 20px; width: 100%;"></div>
A distributed control plane is needed.	
This type requires a distributed management plane.	Traditional Networking <div style="background-color: #FFFF00; height: 20px; width: 100%; margin-bottom: 5px;"></div> <div style="background-color: #FFFF00; height: 20px; width: 100%;"></div>
Southbound APIs are used to apply configurations.	
Northbound APIs interact with end devices.	

Correct Answer:

Answer Area

This type deploys a consistent configuration across multiple devices.	Controller-Based Networking <div style="background-color: #ADD8E6; padding: 5px; margin-bottom: 5px;">This type deploys a consistent configuration across multiple devices.</div> <div style="background-color: #ADD8E6; padding: 5px;">This type requires a distributed management plane.</div>
A distributed control plane is needed.	
This type requires a distributed management plane.	Traditional Networking <div style="background-color: #ADD8E6; padding: 5px; margin-bottom: 5px;">A distributed control plane is needed.</div> <div style="background-color: #ADD8E6; padding: 5px;">Northbound APIs interact with end devices.</div>
Southbound APIs are used to apply configurations.	
Northbound APIs interact with end devices.	

splashy Highly Voted 1 year ago

CBN
 Deploys a consistent config multiple devices
 Southbound API's to apply configs

TN:
 distributed control plane
 distributed management plane

northbound API is not towards end devices and not in traditional networking.
 upvoted 56 times

evil3xx Highly Voted 11 months, 3 weeks ago

Controller-based Networking :
 – This type deploys a consistent configuration across multiple devices.
 – Southbound APIs are used to apply configurations.
 Traditional Networking :
 – A distributed control plane is needed.
 – This type requires a distributed management plane.
 upvoted 25 times

paolino555 Most Recent 2 months, 1 week ago

Northbound API not interact with end devices.

upvoted 1 times

  **Anas_Ahmad** 8 months, 2 weeks ago

Northbound APIs do not interact with end devices. They allow the SND controller to interact with applications on the application plane.

upvoted 4 times

Question #758

Topic 1

Which two REST API status-code classes represent errors? (Choose two.)

A. 1XX

B. 2XX

C. 3XX

D. 4XX

E. 5XX

Correct Answer: DE

  **[Removed]** 2 months, 2 weeks ago

This is out of scope CCNA 200-301

upvoted 2 times

  **TechLover** 2 months, 2 weeks ago

1xx-informational, the request was received.

2xx-Successful, request successfully received.

3xx-Redirection, further action need to be taken.

4xx-Client error, syntax error.

5xx-Server error, server failed.

upvoted 3 times

  **Ciscoman021** 5 months, 2 weeks ago

Selected Answer: DE

D and E

upvoted 3 times

  **splashy** 11 months, 4 weeks ago


<https://www.django-rest-framework.org/api-guide/status-codes/#:~:text=Status%20Codes%20%20Informational%20-%201xx%20This%20class,Error%20-%205xx%20...%206%20Helper%20functions%20>

upvoted 3 times

How do servers connect to the network in a virtual environment?

- A. a cable connected to a physical switch on the network
- B. wireless to an access point that is physically connected to the network
- C. a virtual switch that links to an access point that is physically connected to the network
- D. a software switch on a hypervisor that is physically connected to the network

Correct Answer: D

 **Dunedrifter** 2 months, 2 weeks ago

Selected Answer: D

D is correct. That's how you configure a virtual network in vmware esxi and connect them with physical cisco core switches.
upvoted 2 times

 **dropspablo** 3 months ago

Selected Answer: D


If I'm not mistaken:
Letter C is wrong: "a virtual switch that links to an access point that is physically connected to the network" - (An "access point" is an AP, Wi-Fi wireless network device).
Correct answer is the letter D: "a software switch on a hypervisor that is physically connected to the network". - (The software switch on the hypervisor allows communication between the virtual machines and the physical network).
upvoted 1 times

 **dropspablo** 3 months ago

Open vSwitch (virtual switch) can operate both as a "software-based" network switch running within a virtual machine (VM) hypervisor...

https://en.wikipedia.org/wiki/Open_vSwitch#:~:text=both%20as%20a-,software%2Dbased,-network%20switch%20running

upvoted 1 times


 **StingVN** 3 months, 3 weeks ago

Selected Answer: C

Agree with C, virtual switch.
upvoted 1 times

 **M365Certy** 9 months, 1 week ago

I think this is supposed to be virtual switch
upvoted 1 times

 **Phonon** 8 months, 2 weeks ago

D is still most correct (keyword hypervisor) but you are right, it should be virtual switch.
upvoted 4 times

What is the function of the controller in a software-defined network?

- A. forwarding packets
- B. multicast replication at the hardware level
- C. making routing decisions
- D. fragmenting and reassembling packets

Correct Answer: C

 **Liquid_May** 3 weeks, 2 days ago

I don't think C is very correct, forwarding data should be a function of the data plane, however among the given options I think it is the most correct.

upvoted 1 times

 **HM01** 2 months, 3 weeks ago

What is the function of the controller in a software-defined network?

- A. forwarding packets
- B. multicast replication at the hardware level
- C. setting packet-handling policies
- D. fragmenting and reassembling packets

WHAT WILL BE ANSWER FOR THIS ONE GUYS?

upvoted 1 times

 **Dhruv3390** 8 months, 1 week ago

An SDN controller is an application in a software-defined networking (SDN) architecture that manages flow control for improved network management and application performance. The SDN controller platform typically runs on a server and uses protocols to tell switches where to send packets.

upvoted 2 times

 **michael1001** 9 months, 1 week ago

Selected Answer: C

C is correct - Several articles on the purpose of an SDN controller confirms that the controller becomes the control plane. The purpose of the control plane is to "control" how data is forwarded then let the data plane perform the rest.

upvoted 2 times

 **RougePotatoe** 10 months ago

Hold up now. There was another question like this before and the answer was build routing table but now the best answer is make routing decisions?

upvoted 3 times

 **RougePotatoe** 9 months, 4 weeks ago

The other question is 697

upvoted 2 times

 **Yunus_Empire** 9 months, 2 weeks ago

Two Other Questions i Found them same i think 791 match some other question

upvoted 1 times

DRAG DROP -

Drag and drop the HTTP methods used with REST-based APIs from the left onto the descriptions on the right.

Select and Place:

DELETE	creates a resource and returns its URI in the response header
GET	creates or replaces a previously modified resource using information in the request body
POST	removes a resource
PATCH	retrieves a list of a resource's URIs
PUT	updates a resource using instructions included in the request body

Correct Answer:

DELETE	POST
GET	PATCH
POST	DELETE
PATCH	GET
PUT	PUT

GigaGremlin Highly Voted 11 months, 1 week ago

IMHO it should be like this:

- Post
- Put
- Delete
- Get
- Patch

upvoted 18 times

splashy Highly Voted 11 months, 4 weeks ago

I agree with rictorres

- GET: retrieve data
- POST: create data
- PUT: fully update (i.e. replace) an existing record
- PATCH: update part of an existing record
- DELETE: delete records

<https://rapidapi.com/blog/put-vs-patch/>

upvoted 13 times

TechLover Most Recent 2 months, 2 weeks ago

- Anytime you see:
- Put- Update/replace
- Patch- Update/modify

upvoted 2 times

rictorres333 1 year ago

It can be error between PATCH and PUT

GET: retrieve data
POST: create data
PUT: fully update (i.e. replace) an existing record
PATCH: update part of an existing record
DELETE: delete records
upvoted 6 times

Question #762

Topic 1

What is a function of a southbound API?

- A. Use orchestration to provision a virtual server configuration from a web server
- B. Automate configuration changes between a server and a switching fabric
- C. Manage flow control between an SDN controller and a switching fabric
- D. Facilitate the information exchange between an SDN controller and application

Correct Answer: C

 **Yunus_Empire** Highly Voted 9 months, 2 weeks ago

30 More Question To Go!!!
upvoted 8 times

 **[Removed]** 2 months, 1 week ago

30?? There are 1138 questions in total
upvoted 1 times

 **john1247** 7 months, 1 week ago

now it is time PM22:20 i'm tired
upvoted 2 times

 **braeiv123** 6 months, 1 week ago

fml, you're missing a 0 now
upvoted 6 times

 **shaney67** Most Recent 1 month ago

What is a function of a southbound API?

- A. Use orchestration to provision a virtual server configuration from a web server
- B. Automate configuration changes between a server and a switching fabric
- C. Manage flow control between an SDN controller and a switching fabric
- D. Facilitate the information exchange between an SDN controller and application

ChatGPT

B. Automate configuration changes between a server and a switching fabric

A southbound API is responsible for facilitating communication and automation between the controller (or management plane) and the network devices (switches, routers, etc.) in a software-defined networking (SDN) environment. It allows the controller to automate configuration changes and manage the behavior of the network devices based on the higher-level instructions and policies provided by the controller.

upvoted 1 times

Which script paradigm does Puppet use?

- A. recipes and cookbooks
- B. playbooks and roles
- C. strings and marionettes
- D. manifests and modules

Correct Answer: D

  **creaguy** Highly Voted 11 months, 2 weeks ago

It's C. strings and marionettes.....LOL !
upvoted 9 times

  **mrgreat** 11 months, 1 week ago

It's D. Read this one son: <https://www.guru99.com/puppet-tutorial.html>
Four types of Puppet building blocks are

Resources
Classes
Manifest
Modules

upvoted 2 times

  **DoBronx** 10 months, 3 weeks ago

master of puppets im pulling your strings
upvoted 9 times

  **[Removed]** Most Recent 2 months, 2 weeks ago

Selected Answer: D

D. manifests and modules
upvoted 1 times

  **Zepar** 3 months, 3 weeks ago

This is what ChatGPT says:

Puppet uses the paradigm of manifests and modules. Manifests in Puppet are files written in Puppet's domain-specific language (DSL) called Puppet Language. These manifests describe the desired configuration state of a system by defining resources, attributes, and relationships between them. Resources can include files, packages, services, users, groups, and more.

Modules in Puppet are a way to organize and encapsulate related manifests and associated files. Modules provide a means of grouping and reusing Puppet code, making it easier to manage and maintain configurations across multiple systems. Each module typically focuses on a specific aspect of system configuration.

By writing manifests and organizing them into modules, Puppet users can define the desired state of their systems and let Puppet handle the task of bringing the systems into that state. Puppet's agent periodically applies the manifests and modules, ensuring that the systems remain in the desired configuration state.

Therefore, the correct answer is D. manifests and modules

upvoted 1 times

  **esandrews** 3 months, 3 weeks ago

Master of Puppets, I'm pulling your strings...
upvoted 2 times

  **Panda_man** 10 months ago

Selected Answer: D

D is correct
upvoted 4 times

Which set of methods is supported with the REST API?

- A. GET, PUT, ERASE, CHANGE
- B. GET, POST, MOD, ERASE
- C. GET, PUT, POST, DELETE
- D. GET, POST, ERASE, CHANGE

Correct Answer: C

 **Vlad_Is_Love_ua** 11 months, 3 weeks ago

<https://restfulapi.net/http-methods/>

Table of Contents

HTTP GET

HTTP POST

HTTP PUT

HTTP DELETE

HTTP PATCH

upvoted 4 times

Which technology is appropriate for communication between an SDN controller and applications running over the network?

- A. Southbound API
- B. REST API
- C. NETCONF
- D. OpenFlow

Correct Answer: D

 **splashy** Highly Voted 1 year ago

Selected Answer: B

"communication between an SDN controller AND applications" -> northbound

-<https://www.econfigs.com/ccna-7-7-c-northbound-and-southbound-apis/>

-ccna mod 3 13.4.4 Traditional & SDN Architectures

Does this imply that

Netconf & Openflow = Southbound

And would this make "B" the most correct answer?

upvoted 15 times

 **ccna_goat** 11 months, 3 weeks ago

use northbound (REST API) in communication between your applications and controller.

use southbound (OpenFlow, OpFlex, RESTCONF, NETCONF) in communication between controller and network devices.

B is correct answer indeed.

upvoted 5 times

 **Vikramaditya_J** Most Recent 1 month, 1 week ago

Selected Answer: B

Did anyone notice the question? It mentions - SDN controller "end" applications, not SDN controller "and" applications. I think it could be a typo. But I'm still confused.

upvoted 1 times

 **dorf05** 1 month, 4 weeks ago

D: OpenFlow specifies the communication between the control plane and the data plane. It implements one of the first standards in SDN enabling the SDN controller to interact directly with the forwarding nodes – switches and routers – in a network.

upvoted 1 times

 **korek_team** 8 months ago

Selected Answer: B

use northbound =REST API

Southbound=Netconf & Openflow

upvoted 3 times

 **michael1001** 9 months, 1 week ago

Selected Answer: B

Answer is B, please fix.


upvoted 3 times

 **cristip** 9 months, 2 weeks ago

Selected Answer: B

REST API is the only one here in northbound

upvoted 3 times

 **BieLey** 11 months, 2 weeks ago

Selected Answer: B

All other options are Southbound

upvoted 4 times

DRAG DROP -

Drag and drop each characteristic of device-management technologies from the left onto the deployment type on the right.

Select and Place:

orchestrates background device configuration

provides greater flexibility for custom and non-standard configurations

relies on per-device management

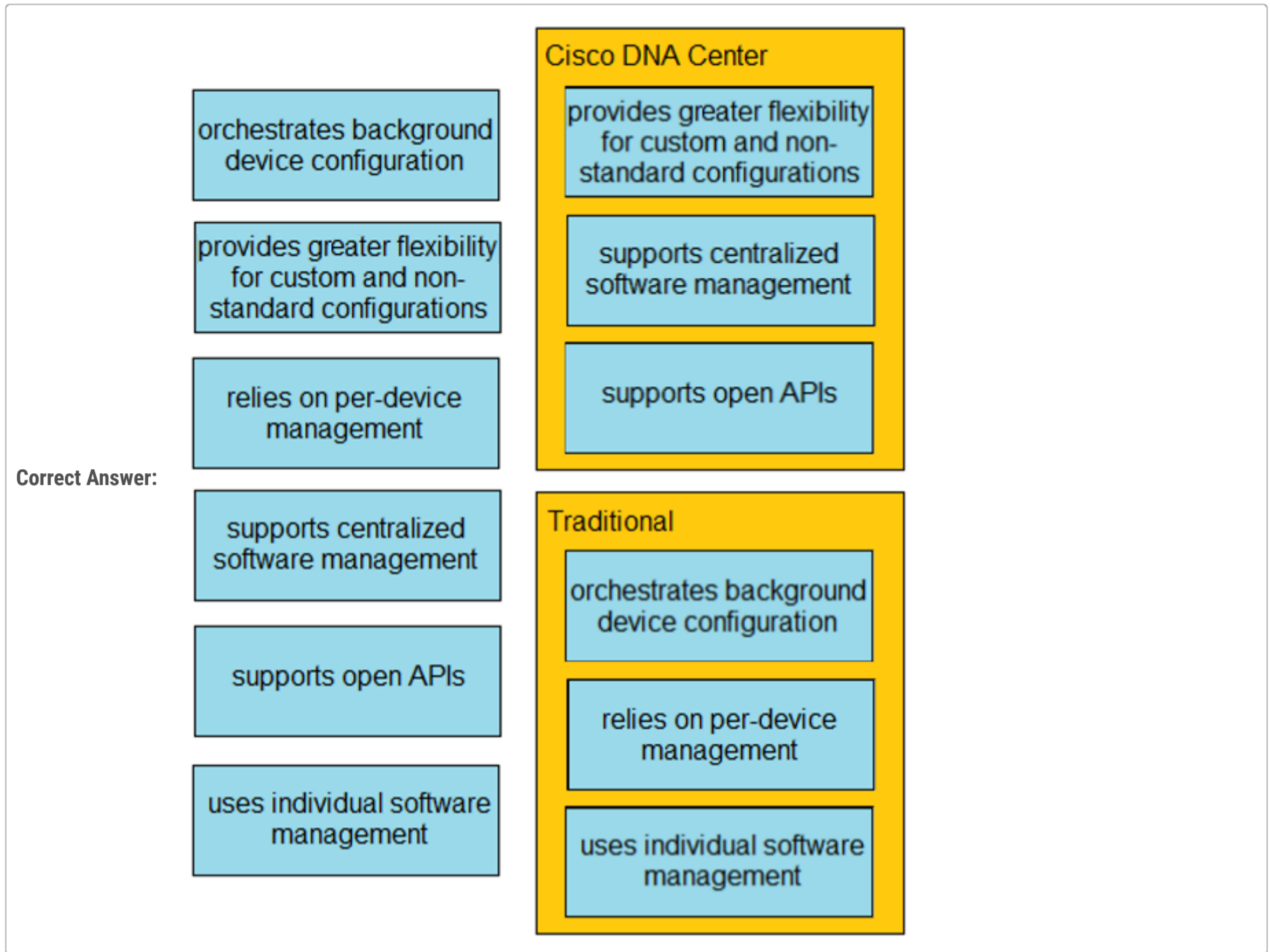
supports centralized software management

supports open APIs

uses individual software management

Cisco DNA Center

Traditional



Garfieldcat Highly Voted 11 months, 1 week ago

I think orchestra background device configuration is not true to Tradition network
upvoted 17 times

EliasM 10 months, 4 weeks ago

I believe that Orchestration and support for custom and non-standard configs should be swapped.
upvoted 13 times

Cynthia2023 Most Recent 1 month, 4 weeks ago

Belong to Cisco DNA Center (Software-Defined Networking Solution):

Orchestrates background device configuration, streamlining the process of applying changes to multiple devices simultaneously and reducing manual configuration efforts.

Provides greater flexibility for custom and non-standard configurations, allowing network administrators to tailor settings to specific requirements without being limited by rigid configurations.

Supports centralized software management, enabling the deployment and updates of software across the network from a single, unified interface.
upvoted 1 times

Cynthia2023 1 month, 4 weeks ago

Belong to Traditional (Legacy Networking):

Relies on per-device management, necessitating manual configuration adjustments for each network device individually.

Uses individual software management, requiring separate installations and updates for software on each device, potentially leading to longer deployment times.

May have limited support for open APIs, making it challenging to integrate with third-party applications and limiting automation possibilities compared to more modern solutions like Cisco DNA Center
upvoted 1 times

paolino555 2 months, 1 week ago



Should be:

Cisco DNA
Orchestrates
Provides greater flexibility
Support centralized

Traditional:
relies on per-device
support open API (Openflow es)
uses individual software management
upvoted 2 times

  **dropspablo** 1 month, 1 week ago

Support API is SDN (DNA Center with NBI)
upvoted 1 times

  **HM01** 2 months, 3 weeks ago

The feature of orchestrating background device configuration is specific to Cisco DNA Center. Cisco DNA Center is a network management and automation platform that provides centralized control, automation, and analytics for network infrastructure.

With Cisco DNA Center, administrators can automate the configuration and provisioning of network devices in the background. This includes tasks such as deploying configurations, pushing software updates,

Providing greater flexibility for a custom and non-standard configuration is a feature that is more commonly associated with traditional network configuration approaches rather than Cisco DNA Center.

In traditional network configuration, administrators have more flexibility and control over customizing and implementing non-standard configurations. They can manually configure network devices using command-line interfaces (CLIs) or device-specific configuration interfaces. This allows them to

upvoted 3 times

  **dropspablo** 1 month, 1 week ago

I gree!

Cisco DNA Center

- orchestrates the configuration of background device.
- supports management centralized software.
- supports open APIs.

Traditional

- provides greater flexibility for settings custom and non-standard.
- depends on management per device.
- use software management individual.

upvoted 3 times

  **Dhruv3390** 8 months, 1 week ago

Network orchestration is an approach to managing and automating interactions between networks, people, devices, domains, applications, and systems within an infrastructure. This helps service providers deliver secure and quick services to their customers.

So it is true for Tradition network

upvoted 1 times

  **Dhruv3390** 8 months, 1 week ago

Even most of SDN bound with configuration policies, so it is not flexible

upvoted 2 times

What is the function of `off-the-shelf` switches in a controller-based network?

- A. setting packet-handling policies
- B. forwarding packets
- C. providing a central view of the deployed network
- D. making routing decisions

Correct Answer: B

  **dropspablo** 2 months, 4 weeks ago


Selected Answer: B

In SDN's purest form, the controller has all the intelligence: Switches are dumb, commercial off-the-shelf (COTS) devices that are managed by the controllers.

Therefore we can deduce "off-the-shelf" switches are only used to forward packets.

https://quizlet.com/761289670/6-automation-virtualization-cloud-sdn-dna_14548715_2023_01_05_20_24-flash-cards/



upvoted 2 times

  **hamish88** 5 months, 1 week ago

The answer is B,

A is wrong as. The controller is responsible for setting packet-handling policies, making routing decisions, and providing a central view of the deployed network.

upvoted 3 times

  **zamkljo** 5 months, 2 weeks ago

A

Control Plane: All activities that are necessary to perform data plane activities but do not involve end-user data packets

Making routing tables

Setting packet handling policies (e.g., security)

Base station beacons announcing availability of services

upvoted 1 times

  **wondaah** 6 months, 1 week ago

Selected Answer: B

just trying to confuse you with controller based network. Doesn't matter

upvoted 1 times

  **Goena** 7 months ago

Selected Answer: A


Correct answer is A

upvoted 2 times

  **EthanhuntMI6** 9 months ago

Shouldn't the correct answer be D. Please let me know if it's wrong.

upvoted 1 times

  **guisam** 9 months, 1 week ago

<https://dictionary.cambridge.org/dictionary/english/off-the-shelf>

upvoted 1 times

  **aeris_ai** 1 year ago

Newbie here, got answer A from other dumps, can anyone clarify?

Please and thank you.

upvoted 2 times

  **Murphy2022** 11 months, 2 weeks ago

off-the-shelf as in: is running on the basic config.

upvoted 3 times

  **Tdawg1968** 4 months, 1 week ago

That makes sense

upvoted 1 times

Which REST method updates an object in the Cisco DNA Center Intent API?

- A. CHANGE
- B. UPDATE
- C. POST
- D. PUT

Correct Answer: D

 **Zepar** Highly Voted 3 months, 3 weeks ago

The REST method that is typically used to update an object in the Cisco DNA Center Intent API is D. PUT.

In RESTful APIs, different HTTP methods are used to perform different actions on resources. The PUT method is commonly used to update an existing resource or replace it entirely with a new representation.

When using the Cisco DNA Center Intent API to update an object, you would typically send an HTTP request with the PUT method to the appropriate endpoint, providing the updated representation of the object in the request body. This allows you to modify the attributes or properties of the object and persist those changes in the system.

Therefore, the correct answer is D. PUT
upvoted 5 times

 **Cynthia2023** Most Recent 1 month, 3 weeks ago

Selected Answer: D

RESTful APIs (Application Programming Interfaces) use HTTP as the communication protocol for exchanging data between clients and servers.
upvoted 1 times

 **[Removed]** 2 months, 2 weeks ago

Selected Answer: D

D. PUT
upvoted 1 times

 **EngrRex** 11 months, 3 weeks ago

Selected Answer: B

I think the answer here is UPDATE, since PUT is under HTTP
upvoted 1 times

 **Bonesaw** 11 months, 3 weeks ago

Negative, it is still PUT

<https://developer.cisco.com/docs/dna-center/#!cisco-dna-center-platform-overview/intent-api-northbound>
upvoted 7 times

```
{
  "SW1" : ["Ten-GigabitEthernet0/0", "Ten-GigabitEthernet0/1"],
  "SW2" : ["Ten-GigabitEthernet0/0", "Ten-GigabitEthernet0/1"],
  "SW3" : ["Ten-GigabitEthernet0/0", "Ten-GigabitEthernet0/1"],
  "SW4" : ["Ten-GigabitEthernet0/0", "Ten-GigabitEthernet0/1"]
}
```

Refer to the exhibit. How many JSON objects are represented?

- A. 1
- B. 2
- C. 3
- D. 4

Correct Answer: D

 **rictorres333** Highly Voted 12 months ago

Selected Answer: A

By definition a object structure is {}, i think A is correct.

upvoted 9 times

 **splashy** Highly Voted 11 months, 4 weeks ago

Selected Answer: A

{object}


[array]

upvoted 7 times

 **Vikramaditya_J** Most Recent 4 months, 3 weeks ago

A JSON object is surrounded by curly brackets, { and }, and contains a comma-separated list of name/value pairs. So, apparently it's A.


upvoted 1 times

 **JJY888** 6 months, 2 weeks ago

Selected Answer: A

Make sure you catch the upper left and upper right corners.

upvoted 1 times

 **Phonon** 8 months, 2 weeks ago

Selected Answer: A

Anything in {} is an object.

therefore

1

upvoted 3 times

 **melmiosis** 10 months, 1 week ago


An object consisting of an array of objects?

upvoted 1 times

 **creaguy** 11 months, 2 weeks ago

If I understand this correctly it would be 1 object and 4 arrays shown correct ?

upvoted 4 times

 **HeinyHo** 12 months ago

Selected Answer: A



I think A, D would be too easy. {} is an object so 1

upvoted 1 times

Which definition describes JWT in regard to REST API security?

- A. an encrypted JSON token that is used for authentication
- B. an encrypted JSON token that is used for authorization
- C. an encoded JSON token that is used to securely exchange information
- D. an encoded JSON token that is used for authentication

Correct Answer: C

  **dropspablo** 2 months, 4 weeks ago

JWT, which stands for JSON Web Token, is a technique defined in RFC 7519 for remote authentication between two parties. It is one of the most used ways to authenticate users in RESTful APIs.

What is JSON Web Token?

JWT (JSON Web Token) is an industry standard RCT 7519 method for performing two-party authentication via a signed token that authenticates a web request. This token is a Base64 code that stores JSON objects with the data that allow authentication of the request.

<https://www.devmedia.com.br/como-o-jwt-funciona/40265>

upvoted 1 times

  **dropspablo** 2 months, 4 weeks ago

I believe answer D, because "This token is a Base64 code that stores JSON objects with the data that allow authentication of the request."

upvoted 1 times

  **espannews** 3 months, 3 weeks ago


C and D are correct. -this ciscodump is a wonderful journey

upvoted 1 times

  **espannews** 3 months, 3 weeks ago

this is what my AI friend says on this matter: Both statements are correct. JWTs are used to securely transmit information between parties as a JSON object . This information can include authentication and authorization data, allowing the recipient to verify the identity of the sender and determine what resources they have access to . So while JWTs can be used for securely exchanging information, they are primarily used for authentication and authorization purposes.

upvoted 1 times

  **Ciscoman021** 5 months, 2 weeks ago

Selected Answer: D

JWT (JSON Web Token) is an encoded JSON token that is commonly used in REST API security for authentication and authorization. Therefore, the correct answer is D - "an encoded JSON token that is used for authentication".

upvoted 4 times

  **Zortex** 6 months ago

D. an encoded JSON token that is used for authentication

JSON Web Tokens (JWT) is an open standard for securely transmitting information between parties as a JSON object. In the context of REST API security, JWT is typically used for authentication purposes. It is a compact, URL-safe means of representing claims to be transferred between two parties.

When a user authenticates with a REST API, the server generates a JWT token that contains user information, such as the user ID and access privileges. The token is then sent to the client, typically in the form of an HTTP header, and is included in subsequent requests to the API.

The server then validates the token to ensure that it was issued by a trusted authority and that it has not been tampered with. If the token is valid, the server grants access to the requested resources. If the token is invalid or has expired, the server denies access to the resources.

Therefore, the correct definition of JWT in regard to REST API security is that it is an encoded JSON token that is used for authentication.

upvoted 3 times

  **danny43213** 7 months, 2 weeks ago

JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON

upvoted 2 times

  **mrgreat** 11 months, 3 weeks ago

Check this: <https://www.examttopics.com/discussions/cisco/view/79793-exam-350-401-topic-1-question-427-discussion/#:~:text=Which%20definition%20describes%20JWT%20in,that%20is%20used%20for%20authentication>

upvoted 1 times

  **splashy** 11 months, 4 weeks ago

Selected Answer: D

<https://www.rfc-editor.org/rfc/rfc7519#ref-JWS>

https://en.wikipedia.org/wiki/JSON_Web_Token#Use

<https://medium.com/emblatech/secure-your-spring-restful-apis-with-jwt-a-real-world-example-bfdd2679db5f>
upvoted 2 times

  **splashy** 11 months, 3 weeks ago

And a week later...

It's encoded

It exchanges more info then just authentication

<https://jwt.io/introduction/>

It's probably C :)

upvoted 2 times

  **oatmealturkey** 7 months, 1 week ago

I still think the answer is D. JWT provides authentication, but technically it does not in itself provide security to the information that is being exchanged, because without HTTPS (TLS), the information can still be intercepted and the JWT can be stolen. But please correct me if I'm wrong!

upvoted 3 times

```
1 [
2   { "switch": "3750", "port": e2 },
3   { "router": "2951", "port": e20 }.
4   { "switch": "3750", "port": e23 }
5 ]
```

Refer to the exhibit. What is identified by the word `switch` within line 2 of the JSON Schema?

- A. array
- B. value
- C. object
- D. key

Correct Answer: *D*

🗄️ 👤 **Customexit** Highly Voted 👍 10 months, 2 weeks ago

Selected Answer: D

Key-value pairs have a colon between them as in "key" : "value".

<https://www.digitalocean.com/community/tutorials/an-introduction-to-json>
upvoted 5 times

🗄️ 👤 **[Removed]** Most Recent 🕒 2 months, 1 week ago

Selected Answer: D

D. key
"key": "value"
upvoted 1 times

🗄️ 👤 **Phonon** 8 months, 2 weeks ago

Selected Answer: D

Here is an example of a key-value pair in JSON:

```
{"name": "John"}
```

In this example, "name" is the key and "John" is the value. The value is a string, and it is associated with the key "name".

Here is another example of a key-value pair in JSON:

```
{"age": 30}
```

In this example, "age" is the key and 30 is the value. The value is a number, and it is associated with the key "age".
upvoted 4 times

🗄️ 👤 **Sunnyip** 9 months ago

Selected Answer: D

The formula {"key": "value"}
upvoted 3 times

🗄️ 👤 **cormorant** 10 months, 2 weeks ago

json follows the formula {"key": "value"} pair. note that it's also an array of values []
upvoted 4 times

🗄️ 👤 **arenjenkins** 10 months, 3 weeks ago

Selected Answer: B

it's b
upvoted 4 times

🗄️ 👤 **GigaGremlin** 11 months, 1 week ago



A name/value pair consists of a field name (in double quotes), followed by a colon, followed by a value:
"name": "Mark"
upvoted 1 times

```
{ "Employee's name": "Arthur" }
```

Refer to the exhibit. Which type of JSON data is shown?

- A. boolean
- B. array
- C. key
- D. object

Correct Answer: *D*

  **Paul1111** 2 weeks ago

Correct

upvoted 1 times

DRAG DROP -

Drag and drop the characteristics from the left onto the technology types on the right.

Select and Place:

This type of technology provides automation across multiple technologies and domains.	Configuration Management
This type of technology enables consistent configuration of infrastructure resources.	
Puppet is used for this type of technology.	Orchestration
Ansible is used for this type of technology.	

Correct Answer:

This type of technology provides automation across multiple technologies and domains.	Configuration Management
This type of technology enables consistent configuration of infrastructure resources.	Puppet is used for this type of technology.
Puppet is used for this type of technology.	Orchestration
Ansible is used for this type of technology.	This type of technology provides automation across multiple technologies and domains.
	Ansible is used for this type of technology.

usamhtrakib001 Highly Voted 10 months, 3 weeks ago

puppet uses (agent) on both sides and pull model that's why specific. Ansible use push model and (agent less) so can be used in multiple technologies
upvoted 10 times

dropspablo 2 months, 4 weeks ago

I concur with your statement. The given answer is correct. Just adding:
"Ansible can be used with any configuration management system you have. Ansible can be used with other deployment systems, or scripts you might already have. You could also just use Ansible for everything. But either way, it's an AMAZING driver that probably has a great place in your environment whatever you are doing. Even if you have a lot of legacy IT automation that you feel you can't get out from under, give Ansible a try for orchestration. As Atlassian points out, we can play nicely with others ."

<https://www.ansible.com/blog/orchestration-you-keep-using-that-word#:~:text=tasks%20increasingly%20trivial.-,Ansible,-can%20be%20used>
upvoted 1 times

dropspablo 2 months, 4 weeks ago

How Ansible can even automate sending chat messages and do just about anything. Puppet works with a focus on Infrastructure.

<https://www.puppet.com/why-puppet/use-cases/continuous-configuration-automation#:~:text=State%20of%20Infrastructure%20at%20Scale>
upvoted 1 times

MDubYa913 Most Recent 2 months, 2 weeks ago

I really don't think this is going to be on the CCNA test.
upvoted 3 times

  **[Removed]** 2 months, 2 weeks ago

Me either
upvoted 1 times

  **perri88** 3 months ago

answer is correct
upvoted 2 times

  **VicM** 4 months ago

<https://intellipaat.com/blog/what-is-puppet/?US#:~:text=Puppet%20definition,%2C%20configuring%2C%20and%20managing%20servers.>
<https://www.openlogic.com/blog/overview-ansible-architectures-and-orchestrations#:~:text=Ansible%20is%20an%20open%20source%20orchestration%20engine%20that%20automates%20cloud,and%20many%20other%20IT%20needs.>

upvoted 1 times

  **JJY888** 4 months, 1 week ago

I think ChatPT is right about this. I also backed it up with GOOGLE.
<https://www.puppet.com/why-puppet/use-cases/continuous-configuration-automation>
<https://www.edureka.co/blog/what-is-ansible/#:~:text=Ansible%20is%20an%20open%20source,multi%2Dtier%20IT%20application%20environments.>

ChatGPT:

These statements can be categorized as follows:

Configuration management:

Puppet is used for this type of technology.

Ansible is used for this type of technology.

Orchestration:

This type of technology provides automation across multiple technologies and domains.

This type of technology enables consistent configuration of infrastructure resources.


Therefore, the statements about Puppet and Ansible fall under configuration management, while the statements about automation across multiple technologies and consistent configuration of infrastructure resources fall under orchestration.

upvoted 1 times

Which communication interaction takes place when a southbound API is used?

- A. between the SDN controller and PCs on the network
- B. between the SDN controller and switches and routers on the network
- C. between the SDN controller and services and applications on the network
- D. between network applications and switches and routers on the network

Correct Answer: B

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: B

Yes, between the SDN controller at the control plane and the data plane (routers and switches).

upvoted 1 times

  **Zepar** 3 months, 3 weeks ago

The communication interaction that takes place when a southbound API is used is
B. between the SDN controller and switches and routers on the network.

In a software-defined networking (SDN) architecture, the control plane is centralized in an SDN controller, which manages and controls the behavior of network devices such as switches and routers. The southbound API is the interface through which the SDN controller communicates with these network devices.

When using the southbound API, the SDN controller sends instructions and configuration commands to the switches and routers in the network. These instructions can include actions like modifying forwarding tables, setting up flow rules, configuring quality of service (QoS) parameters, and more.

The switches and routers, acting as the data plane, receive and process the instructions from the controller, implementing the desired network behavior. They forward traffic based on the rules and configurations received from the controller.

Therefore, the correct answer is B. between the SDN controller and switches and routers on the network.

upvoted 2 times

  **kennie0** 3 months, 3 weeks ago

PC is a device too so why not A?

upvoted 1 times

What are two characteristics of a public cloud implementation? (Choose two.)

- A. It is owned and maintained by one party, but it is shared among multiple organizations
- B. It enables an organization to fully customize how it deploys network resources
- C. It provides services that are accessed over the Internet
- D. It is a data center on the public Internet that maintains cloud services for only one company
- E. It supports network resources from a centralized third-party provider and privately-owned virtual resources

Correct Answer: AC

 **Sant11** 2 weeks, 4 days ago

Selected Answer: AC

A & C are correct. E refers to a hybrid cloud
upvoted 2 times

 **dropspablo** 2 months, 4 weeks ago

Wrong answer. I believe that the correct one is C and E, they are clearer. This site below has got some questions right. About the letter A she is half right, but her statement about sharing with other organizations is not very clear, maybe if it were users she could be more correct, about the public cloud characteristic, the letter A is badly worded.

<https://itexamanswers.net/question/what-are-two-characteristics-of-a-public-cloud-implementation-choose-two>
upvoted 1 times

 **dropspablo** 3 weeks, 1 day ago


I think the letter E is correct, as the public cloud started to be offered first by Amazon, and then by Google and Microsoft "third-party provider". And for example, Google Driver (Software as a Service), everything we store in it is seen as our property "privately-owned virtual resources".
upvoted 1 times

 **ananinamia** 2 weeks, 2 days ago

You should be a thinker
upvoted 1 times

 **Bingchengchen236** 3 months ago

The answer AC is correct I think, for E, it is not saying that the resources is offered by a third-party provided, what it emphasizes is the public cloud can 'support' a third party ..., that is not the case in most public cloud I think.
upvoted 1 times

 **Naghini** 7 months, 2 weeks ago

Selected Answer: CE

Public cloud is a type of computing where resources are offered by a third-party provider via the internet. (<https://cloud.google.com/learn/what-is-public-cloud>)
C & E are correct.
upvoted 4 times

DRAG DROP -

Drag and drop the descriptions from the left on to the correct configuration-management technologies on the right.

Select and Place:

fundamental configuration elements are stored in a manifest

uses TCP port 10002 for configuration push jobs

uses Ruby for fundamental configuration elements

uses SSH for remote device communication

uses TCP 8140 for communication

uses YAML for fundamental configuration elements

Ansible

Chef

Puppet

Correct Answer:

- fundamental configuration elements are stored in a manifest
- uses TCP port 10002 for configuration push jobs
- uses Ruby for fundamental configuration elements
- uses SSH for remote device communication
- uses TCP 8140 for communication
- uses YAML for fundamental configuration elements

Ansible

- uses SSH for remote device communication
- uses YAML for fundamental configuration elements

Chef

- uses TCP port 10002 for configuration push jobs
- uses Ruby for fundamental configuration elements

Puppet

- fundamental configuration elements are stored in a manifest
- uses TCP 8140 for communication


 **RODCCN** 1 month, 2 weeks ago

ANSIBLE:
Uses SSH
Uses YAML

CHEF:
Uses Ruby
Uses TCP 10002

PUPPET:
Fundamental configuration stored in a manifest
Uses TCP 8140

LINK: <https://ipcisco.com/lesson/ansible-vs-puppet-vs-chef/>
upvoted 1 times

 **Shabeth** 2 months, 2 weeks ago

answers are correct
upvoted 1 times

DRAG DROP -

Drag and drop the REST API call methods for HTTP from the left onto the actions they perform on the right. Not all methods are used.

Select and Place:

DELETE

GET

POST

PUT

PATCH

creates a resource on the server

reads data from the server

removes a resource from the server

updates an entry in the database

Correct Answer:

DELETE

GET

POST

PUT

PATCH

POST

GET

DELETE

PUT

 **splashy** Highly Voted 11 months, 4 weeks ago


POST
GET
DELETE
PATCH

Wouldn't "patch" be the "safer" option, since you are just updating one thing in a database and not the complete database? Put could wipe the entries you are not modifying?

<https://rapidapi.com/blog/put-vs-patch/>

Feel free to correct me if i got it wrong.

upvoted 19 times

 **HM01** 2 months, 3 weeks ago

PUT is commonly used for completely replacing an entry, while PATCH is often used for making partial updates to an existing entry in a database.

I guess PUT will be more suitable here.

upvoted 3 times

  **splashy** 11 months, 3 weeks ago

<https://community.cisco.com/t5/networking-knowledge-base/cisco-dna-center-platform-api/ta-p/4105156>

<https://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/restapi/restapi/RESTAPIintro.html#97727>

IOS XE Rest API & Cisco DNA center only use "PUT" and don't use "PATCH" (or so it seems)

I had to look it up for a previous similar question but in relation to Cisco DNA center only.

This question only mentions Rest API call methods for HTTP period, not in the use context of Cisco DNA.

upvoted 6 times

  **RODCCN** 1 month, 2 weeks ago

Links:

<https://www.edureka.co/blog/what-is-rest-api/>

<https://www.techtarget.com/searcharchitecture/tip/The-5-essential-HTTP-methods-in-RESTful-API-development>

upvoted 1 times

  **MikD4016** Most Recent 11 months, 3 weeks ago

PUT

The single-resource equivalent of POST is PUT, which updates a resource by replacing its content entirely. As a RESTful API HTTP method, PUT is the most common way to update resource information.

It's possible to create a resource with a PUT method, but this approach carries the risk of creating resources by accident, as noted above. If PUT is applied to a collection of resources, the entire resource collection gets replaced, which usually isn't the intention.

PATCH

PATCH is another HTTP method used to update resources. As opposed to replacing resources, like the PUT method does, PATCH only modifies resource contents. As a general rule, these modifications should be expressed in a standard format like JSON or XML.

Much like in PUT, it's poor practice to specifically apply PATCH methods to a whole resource collection -- that is, unless you truly intend to update every resource it contains.

upvoted 4 times

DRAG DROP -

Drag and drop the REST principles from the left onto their definitions on the right.

Select and Place:

cacheable	divides architecture components into the consumers and producers of a service
client-server	divides the architecture into a hierarchy of levels
layered system	enables the client to reuse a previous response for subsequent equivalent requests
stateless	operates without any stored session information on the server
uniform interface	simplifies the communication between components, regardless of the architecture supporting them

Correct Answer:

cacheable	layered system
client-server	cacheable
layered system	uniform interface
stateless	stateless
uniform interface	client-server

splashy Highly Voted 1 year ago

The provided answers don't make any sense at all it's:
 client server
 layered
 cachable
 stateless
 uniform interface
 upvoted 93 times

JJY888 Highly Voted 6 months, 2 weeks ago

Wow, are the admins trying to make people fail? If you don't know the answer then leave it blank.
https://www.google.com/search?q=rest+api+principles+cacheable&rlz=1C1GCEA_enUS1017US1017&sxsrf=AJOqlzWo8u4i9OSbtB2SW9haUXcF9rheQA%3A1677544877980&ei=rU39Y6aqO9C3qtsP2NybqA4&ved=0ahUKEwjmtK_U_bb9AhXQm2oFHVjuBuUQ4dUDCBA&uact=5&oq=rest+api+principles+cacheable&gs_lcp=Cgxn3Mtd2l6LXNlcnAQAzIFCCEQoAEyBQghEKABMgsIIRAWEB4Q8QQHToKCAAQRxDWBBCwAzoHCAAQsAMQQzoFCAAQgAQ6BggAEBYQHjoJCAAQFhAeEPeeOgUIABCGAzoFCCEQqwI6CAghEBYQHhAdSgQIQRgAUlciWOSmYlkoaAFwAXgAgAF7iAGiB5IBAzguMpgBAKABAcgBCsABAQ&scient=gs-wiz-serp
 client server
 layered
 cachable
 stateless
 uniform interface
 upvoted 8 times

ac891 Most Recent 4 months ago

This is my 4th time renewing my CCNA, And I have never ever same across this kind of questions ! What the hell is happening !?

upvoted 4 times

  **[Removed]** 2 months, 2 weeks ago

I think they mix things up and i'm pretty sure this won't be in the CCNA 200-301. Maybe this is CCNP or other Cisco exam, i don't know but not CCNA 200-301.

upvoted 2 times

  **esandrews** 3 months, 3 weeks ago

CCNA is getting dated and losing value, that's why they're filling it up now with all this absurd amount of cutting-edge mumbojumbo

upvoted 3 times

DRAG DROP -

Drag and drop the Ansible terms from the left onto the right.

Select and Place:

control node	collection of actions to perform on target devices, expressed in YAML format
inventory	device with Ansible installed that manages target devices
managed node	network device, without Ansible installed, upon which commands can be executed
module	specific action to be performed on one or more target devices
playbook	unit of Python code to be executed
task	Ansible file that defines the target devices upon which commands and tasks can be executed

Correct Answer:

control node	playbook
inventory	managed node
managed node	control node
module	task
playbook	module
task	inventory

 splashy Highly Voted 1 year ago

- playbook
- control node
- managed
- task
- module
- inventory

control node has ansible installed managed does not

<https://opensource.com/resources/what-ansible#:~:text=The%20control%20node%20is%20a%20computer%20that%20runs,any%20device%20being%20managed%20by%20the%20control%20node.>

<https://www.tecmint.com/install-and-configure-an-ansible-control-node/>
upvoted 44 times

  **dropspablo** 2 months, 4 weeks ago

I agree and adding about python:

"Modules can be written in any language capable of returning JSON, although most Ansible modules (except for Windows PowerShell) are written in Python using the Ansible API (this eases the development of new modules)."

<https://opensource.com/article/19/3/developing-ansible-modules#:~:text=are%20written%20in-,Python,-using%20the%20Ansible>
upvoted 1 times

  **Bfgran18** Most Recent 4 weeks ago

playbook
control node
managed
task
module
inventory
<https://www.maquinasvirtuales.eu/ansible-conceptos-basicos/>
upvoted 1 times

  **Shri_Fcb10** 3 months, 3 weeks ago

do they even ask this time of questions in CCNA?
upvoted 2 times

  **JJY888** 4 months, 1 week ago

Control node: device with Ansible installed that manages target devices
Inventory: Ansible file that defines the target devices upon which commands and tasks can be executed
Managed node: target device(s) that Ansible manages
Module: unit of Python code to be executed
Playbook: collection of actions to perform on target devices, expressed in YAML format
Task: specific action to be performed on one or more target devices
upvoted 1 times

```

{
  "Test_Questions" : [
    "Automation",
    "Configuration",
  ],
  "Test_Exam_Level" : [
    "CCNA",
    "CCNP",
  ],
  "Test_Response" : [
    "Correct",
    "Incorrect",
  ],
}

```

Refer to the exhibit. How many objects keys, and JSON list values are present?

- A. Three objects, two keys, and three JSON list values
- B. Three objects, three keys, and two JSON list values
- C. One object, three keys, and three JSON list values
- D. One object, three keys, and two JSON list values

Correct Answer: B

 **rictorres333** Highly Voted 1 year ago

Selected Answer: C

What is in a JSON object?

A JSON object contains zero, one, or more key-value pairs, also called properties. The object is surrounded by curly braces {}. Every key-value pair is separated by a comma. The order of the key-value pair is irrelevant.

What is JSON key?

A JSON object contains zero, one, or more key-value pairs, also called properties. The object is surrounded by curly braces {}. Every key-value pair is separated by a comma. The order of the key-value pair is irrelevant. A key-value pair consists of a key and a value, separated by a colon (:)

What is JSON list?

Array Datatype in JSON

Similar to other programming languages, a JSON Array is a list of items surrounded in square brackets ([]). Each item in the array is separated by a comma. The array index begins with 0. The square brackets [...] are used to declare JSON array. JSON array are ordered list of values.

In question:

{ } = 1
 : = 3
 [] = 3

Correct is C.

upvoted 17 times

 **Shansab** Highly Voted 9 months ago

Selected Answer: C

it is clear only one object.

upvoted 6 times

 **esandrews** Most Recent 3 months, 3 weeks ago

Not a single correct answer at this point.

upvoted 1 times

 **enzo86** 5 months, 1 week ago

Selected Answer: C

C is correct

upvoted 2 times

🗨️ **JJY888** 6 months, 2 weeks ago

Selected Answer: C

List values are arrays separated by []
upvoted 2 times

🗨️ **RaselAhmedIT** 6 months, 3 weeks ago

I'm still confused, what will be the correct answer?
upvoted 2 times

🗨️ **mzu_sk8** 10 months ago

Selected Answer: C

clearly one object
upvoted 2 times

🗨️ **BI1024** 11 months ago

Selected Answer: C

Only one object indicated by the {} with 3 keys indicated by the : and 3 list values indicated by the []
upvoted 5 times

🗨️ **arenjenkins** 11 months, 2 weeks ago

Selected Answer: C

One object
upvoted 4 times

🗨️ **shubhambala** 1 year ago

Selected Answer: C

C is the answer boys & gals
upvoted 6 times

🗨️ **g_mindset** 1 year ago

Selected Answer: C

3 list values there
upvoted 3 times

🗨️ **splashy** 1 year ago

Selected Answer: D

"JSON objects are wrapped in curly braces. Inside the object, we can list any number of key-value pairs, separated by commas:"

<https://atacomsian.com/blog/what-is-json>

upvoted 2 times

🗨️ **4aynick** 3 months, 3 weeks ago

from your logic must be 6 list value
upvoted 1 times

🗨️ **splashy** 11 months, 3 weeks ago

Got to go with g_mindset & rictorres,
I misinterpreted list values, they are actually the arrays so 1 3 3

So it's C
upvoted 5 times

Which two primary drivers support the need for network automation? (Choose two.)

- A. Increasing reliance on self-diagnostic and self-healing
- B. Eliminating training needs
- C. Policy-driven provisioning of resources
- D. Reducing hardware footprint
- E. Providing a single entry point for resource provisioning

Correct Answer: CE

 **RougePotatoe** Highly Voted 10 months, 2 weeks ago

Anyone know why A isn't an answer? From my knowledge there been a significant push for automatic fault detection and repair.
upvoted 6 times

 **dropspablo** 2 months, 4 weeks ago

I believe that despite the importance that self-diagnosis and self-healing resources have been having, they are not the main points. The key points for the need for automation would be a centralized point for provisioning settings and the provisioning of them by policies and smart features.

According to this site that has been hitting some, the answer is correct:

<https://itexamanswers.net/question/which-two-primary-drivers-support-the-need-for-network-automation-choose-two>

upvoted 2 times

 **abdelkader163** Most Recent 3 weeks ago

Selected Answer: AC

Increasing reliance on self-diagnostic and self-healing
Policy-derived provisioning of resources

upvoted 1 times

 **shaney67** 1 month ago

A. Increasing reliance on self-diagnostic and self-healing
C. Policy-driven provisioning of resources

The two primary drivers that support the need for network automation are:

A. Increasing reliance on self-diagnostic and self-healing: As networks become more complex, the ability to automatically diagnose issues and initiate self-healing processes becomes crucial for maintaining network stability and reducing downtime.

C. Policy-driven provisioning of resources: Network automation enables organizations to define policies for resource provisioning and configuration. This helps ensure consistent and standardized configurations across the network, reducing the risk of errors and misconfigurations.


The other options (B, D, and E) are not typically considered primary drivers for network automation.

upvoted 1 times

 **dropspablo** 2 months, 4 weeks ago

"Providing a single entry point for resource provisioning" I believe refers to the need to have a single centralized point for managing and configuring resources on a network.

upvoted 1 times

 **alfuga** 3 months, 1 week ago

I think that the DE option focuses on virtualization and not on network management by automation

upvoted 1 times

 **sbnpj** 5 months, 3 weeks ago

I think A,C, and E are correct answers, if I have to choose two I would go with C and E.

upvoted 2 times

 **cormorant** 10 months, 2 weeks ago

Which two primary drivers support the need for network automation? (Choose two.)

Policy-driven provisioning of resources & Providing a single entry point for resource provisioning. no arguing. let's just accept that network automation is meant for policy-driven provisioning and providing a single point of entry for provisioning. what matters is to pass the test, not to dispute cisco's idealised worldview

upvoted 4 times

 **RougePotatoe** 10 months ago

You do realize the answers aren't provided by cisco correct?

upvoted 4 times

  **Anas_Ahmad** 8 months, 3 weeks ago

do you think thta answer provided by Cisco?

upvoted 2 times

Question #782

Topic 1

What is an expected outcome when network management automation is deployed?

- A. A distributed management plane must be used.
- B. Complexity increases when new device configurations are added.
- C. Custom applications are needed to configure network devices.
- D. Software upgrades are performed from a central controller.

Correct Answer: D



  **shaney67** 1 month ago

D. Software upgrades are performed from a central controller.

An expected outcome when network management automation is deployed is that software upgrades can be performed from a central controller. Automation allows for centralized control over network devices, which can include the ability to schedule and execute software updates across the network from a single point of control. This can lead to more efficient and consistent software management across the network.

The other options do not accurately describe expected outcomes of network management automation.

upvoted 1 times



  **dropspablo** 2 months, 4 weeks ago

Cisco DNA Center Deployment using "SWIM"

"Software Image Management (SWIM) manages software upgrades and controls the consistency of image versions across your network."

<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/dnac-swim-deployment-guide.html#:~:text=devices%20with%20SWIM.-,Cisco%20DNA%20Center,-is%20designed%20for>

upvoted 1 times

  **Phonon** 8 months, 2 weeks ago

D. Software upgrades are performed from a central controller.

Network management automation is the use of software tools and techniques to automate the process of managing and configuring network devices. Some expected outcomes when network management automation is deployed include:

Improved efficiency and accuracy: Network management automation can help to reduce the time and effort required to manage and configure network devices, as well as reduce the risk of errors.

Enhanced security: Network management automation can help to ensure that devices are configured correctly and consistently, which can help to reduce the risk of security vulnerabilities.

Improved visibility and control: Network management automation can provide a centralised view of the network and enable administrators to manage and configure devices from a central location.

Simplified software upgrades: Network management automation can enable software upgrades to be performed from a central controller, rather than having to be performed manually on each device.

In summary, an expected outcome when network management automation is deployed is that software upgrades are performed from a central controller.

upvoted 3 times


```
{  
  "Routers": ["R1", "R2", "R3"],  
  "Switches": ["SW1", "SW2", "SW3"]  
}
```

Refer to the exhibit. What is represented by `R1` and `SW1` within the JSON output?



- A. object
- B. value
- C. key
- D. array

Correct Answer: B

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: B

B is correct, it's a value
upvoted 1 times

  **4aynick** 3 months, 1 week ago

It is value in array, which variable type is string.
Answer is correct 🍷
upvoted 2 times

DRAG DROP -

Drag and drop the statements about networking from the left onto the corresponding networking types on the right.

Select and Place:

Maintenance costs are higher than with other networking options.	Traditional Networking
This type provides a centralized view of the network.	
This type implements changes individually at each device.	Controller-Based Networking
This type leverages controllers to handle network management.	

Correct Answer:

Maintenance costs are higher than with other networking options.	Traditional Networking
This type provides a centralized view of the network.	
This type implements changes individually at each device.	Controller-Based Networking
This type leverages controllers to handle network management.	

JJY888 4 months, 1 week ago

I believe the answer is correct BUT controller-based networks will cost more. Just saying.
upvoted 3 times

ananiamia 2 weeks, 2 days ago

Time or money is the cost for you?
upvoted 1 times

perri88 3 months ago

it depends on the size of your network
upvoted 2 times

Which HTTP status code is returned after a successful REST API request?

- A. 200
- B. 301
- C. 404
- D. 500

Correct Answer: A

 **Phonon** Highly Voted 8 months, 2 weeks ago

Selected Answer: A

A. 200

In HTTP (Hypertext Transfer Protocol), status codes are used to indicate the outcome of a request. When a client (such as a web browser) makes a request to a server (such as a web server), the server responds with a status code and a message.

A successful REST API request typically returns a status code of 200 (OK). This indicates that the request was successful and that the server was able to process it and provide a response.

Here are some other common HTTP status codes:

301 (Moved Permanently): This status code indicates that the requested resource has been permanently moved to a new location.

404 (Not Found): This status code indicates that the requested resource could not be found.

500 (Internal Server Error): This status code indicates that an error occurred on the server while processing the request.

In summary, the HTTP status code returned after a successful REST API request is 200 (OK).

https://en.wikipedia.org/wiki/List_of_HTTP_status_codes

upvoted 5 times

 **4aynick** Most Recent 3 months, 3 weeks ago


Client Error - 4xx

The 4xx class of status code is intended for cases in which the client seems to have erred. Except when responding to a HEAD request, the server SHOULD include an entity containing an explanation of the error situation, and whether it is a temporary or permanent condition.

Server Error - 5xx

Response status codes beginning with the digit "5" indicate cases in which the server is aware that it has erred or is incapable of performing the request. Except when responding to a HEAD request, the server SHOULD include an entity containing an explanation of the error situation, and whether it is a temporary or permanent condition.

upvoted 1 times

 **4aynick** 3 months, 3 weeks ago

Informational - 1xx

This class of status code indicates a provisional response. There are no 1xx status codes used in REST framework by default.

Successful - 2xx

This class of status code indicates that the client's request was successfully received, understood, and accepted.

Redirection - 3xx

This class of status code indicates that further action needs to be taken by the user agent in order to fulfill the request.

upvoted 1 times

With REST API, which standard HTTP header tells a server which media type is expected by the client?

- A. Accept-Encoding: gzip, deflate
- B. Accept-Patch: text/example; charset=utf-8
- C. Content-Type: application/json; charset=utf-8
- D. Accept: application/json

Correct Answer: D

 **guynetwork** Highly Voted 1 year ago

this is not ccna question
upvoted 9 times

 **splashy** Highly Voted 1 year ago

Did not see this pop up anywhere in the ccna course on netacad.
upvoted 8 times

 **[Removed]** 2 months, 2 weeks ago

I didn't either
upvoted 1 times

 **Cynthia2023** Most Recent 1 month, 4 weeks ago

Selected Answer: D

Accept and Content-type are both headers sent from a client(browser say) to a service.
Accept header is a way for a client to specify the media type of the response content it is expecting and Content-type is a way to specify the media type of request being sent from the client to the server.
upvoted 1 times

 **dropspablo** 2 months, 4 weeks ago

Selected Answer: D

Using liviuml link:

Content-Type: application/json
(Content-Type: Determines what kind of representation is desired on the server-side).

Accept: application/json
(Accept: Determines what kind of representation is desired on the client-side).

<https://restfulapi.net/content-negotiation/#:~:text=desired%20on%20the-,client%2Dside,-%2C%20an%20HTTP%20header>
upvoted 2 times

 **perri88** 3 months ago

Selected Answer: C


open your chrome inspector and check the headers of any js file. you will see
Content-Type:
application/javascript; charset=utf-8
upvoted 1 times

 **liviuml** 5 months ago

The answer is D
<https://restfulapi.net/content-negotiation/>
upvoted 3 times

 **StevenYung** 2 months, 1 week ago

The answer is D
upvoted 1 times

 **zamkljo** 5 months, 2 weeks ago

Accept Header tells the API that it is expecting the response in the specified media type e.g. application/json or application/xml.
Accept: application/json

And Content-Type tells the API about the media type of the request being sent in the request body e.g. application/json.
Content-Type: application/json
upvoted 1 times

 **rijstraket** 7 months, 1 week ago

Selected Answer: D

The Accept header always indicates what kind of response from the server a client can accept. Content-type is about the content of the current request or response, depending on which kind of HTTP message it is applied.


upvoted 1 times

  **Panda_man** 10 months ago

Selected Answer: C

Media type is content type meaning it's C

upvoted 1 times

  **splashy** 11 months, 4 weeks ago

Selected Answer: D

Started reading and have to agree with D now, it's about what the client sends to the server to tell to the server what content type it can understand and expects.

The Accept request HTTP header indicates which content types, expressed as MIME types, the client is able to understand.

The Content-Type representation header is used to indicate the original media type of the resource (prior to any content encoding applied for sending).

In responses, a Content-Type header provides the client with the actual content type of the returned content.

upvoted 1 times



  **g_mindset** 1 year ago

Selected Answer: C

The answer is C.

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Type>

upvoted 1 times

  **Phonon** 8 months, 2 weeks ago

Seconded

upvoted 1 times

```

{
  "aaaUser": {
    "attributes": {
      "pwd": "password1",
      "firstName": "Abraham",
      "lastName": "Lincoln",
      "phone": "5555551212",
      "email": "test@cisco.com"
    },
    "children": [(
      "aaaUserDomain": {
        "attributes": {
          "name": "ExampleCisco"
        },
        "children": [{
          "aaaUserRole": {
            "attributes": {
              "name": "admin"
            }
          }
        ]
      }
    )]
  }
}

```

Refer to the exhibit. How many objects are present in the given JSON-encoded data?

- A. One
- B. Four
- C. Seven
- D. Nine

Correct Answer: C

 **splashy** Highly Voted 11 months, 4 weeks ago

Selected Answer: D

8 times { because they made an error and put one (which should be a { *facepalm*
 9 times }
 upvoted 15 times

 **g_mindset** Highly Voted 1 year ago

Selected Answer: D

The answer is 9.

Simply count all the opening or closing curly brackets that represent the start or closing of an object value. NOTE: there's an error on that exhibit, the opening bracket in the array is supposed to be an opening bracket.

upvoted 9 times

 **shaney67** Most Recent 1 month ago

C. Seven

The given JSON-encoded data contains seven objects. Each object is enclosed within curly braces {}. The objects present are:

Outermost object: "aaaUser"
 Attributes object within "aaaUser"
 Children array within "aaaUser"
 Object within children array: "aaaUserDomain"
 Attributes object within "aaaUserDomain"
 Children array within "aaaUserDomain"
 Object within children array: "aaaUserRole"

So, there are a total of seven objects in the provided JSON-encoded data.

upvoted 1 times

🗨️ **perri88** 3 months ago

I say 8

upvoted 2 times

🗨️ **Chichi69** 3 months ago

The answer is seven

upvoted 2 times

🗨️ **jonathan126** 4 months, 3 weeks ago

```
{
  "aaaUser": {
    "attributes": {
      "pwd": "password!",
      "firstName": "Abraham",
      "lastName": "Lincoln",
      "phone": "5555551212",
      "email": "test@cisco.com"
    },
    "children": [
      {
        "aaaUserDomain": {
          "attributes": {
            "name": "ExampleCisco"
          },
          "children": [
            {
              "aaaUserRole": {
                "attributes": {
                  "name": "admin"
                }
              }
            }
          ]
        }
      }
    ]
  }
}
```

upvoted 3 times

🗨️ **Njavwa** 5 months ago

i think this includes nested objects, i'm still counting 8

upvoted 1 times

🗨️ **Panda_man** 10 months ago

Selected Answer: D

Count curly brackets - it's 9 of them so it's D

upvoted 3 times

🗨️ **ShadyAbdekmalek** 11 months, 3 weeks ago

Selected Answer: A

One object including sub objects

upvoted 1 times

🗨️ **rictorres333** 12 months ago

.... it can be NINE counting object inside of Arrays... :)

upvoted 1 times

🗨️ **rictorres333** 12 months ago

Selected Answer: A

[] means ARRAY structure.

It left us two first { that means nestedobject. I think ONE.

upvoted 2 times

🗨️ **harveyDai** 1 year ago

I don't understand why is 7

upvoted 2 times

What is the purpose of the Cisco DNA Center controller?

- A. to securely manage and deploy network devices
- B. to scan a network and generate a Layer 2 network diagram
- C. to secure physical access to a data center
- D. to provide Layer 3 services to autonomous access points

Correct Answer: A

Cisco DNA Center is a powerful network controller and management dashboard for secure access to networks and applications. It lets you take charge of your network, optimize your Cisco investment, and lower your IT spending.



Reference:



<https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-so-cte-en.html>

What is the function of the controller in a software-defined network?

- A. forwarding packets
- B. multicast replication at the hardware level
- C. setting packet-handling policies
- D. fragmenting and reassembling packets

Correct Answer: C

  **korek_team** 6 months, 2 weeks ago
answer is correct
upvoted 2 times


  **Yunus_Empire** 9 months, 2 weeks ago
Given answer is correct 🙌
upvoted 2 times



```
Device# configure terminal
Device(config)# netconf ssh acl 1
Device(config)# netconf lock-time 100
Device(config)# netconf max-sessions 1
Device(config)# netconf ma-message 10
```


Refer to the exhibit. A network engineer must configure NETCONF. After creating the configuration, the engineer gets output from the command show line but not from show running-config. Which command completes the configuration?


- A. Device(config)# netconf lock-time 500
- B. Device(config)# netconf max-message 1000
- C. Device(config)# no netconf ssh acl 1
- D. Device(config)# netconf max-sessions 100

Correct Answer: B

 **Sein** Highly Voted 7 months, 2 weeks ago
Since when it's in ccna scope...
upvoted 13 times


 **[Removed]** 2 months, 2 weeks ago
Exactly. It's NOT in CCNA 200-301...
upvoted 1 times


 **Dutch012** Highly Voted 6 months, 2 weeks ago
For god sake Cisco !!
upvoted 6 times

 **shaney67** Most Recent 1 month ago
C. Device(config)# no netconf ssh acl 1

The command "Device(config)# no netconf ssh acl 1" would complete the configuration. It removes the previously configured NETCONF SSH access control list (ACL) with index 1. This might be necessary if the access control list is causing issues with the NETCONF configuration and preventing the correct behavior of the "show running-config" command.


By removing the ACL configuration, the "show running-config" command should be able to display the entire running configuration without being affected by the ACL restrictions.
upvoted 1 times


 **Tdawg1968** 4 months, 1 week ago
Perhaps because there is a typo in the command? Missing the x
upvoted 1 times


 **StefanOT2** 8 months, 1 week ago
Selected Answer: B

Max-Message give a max KB value for the output. The running-config is obviously too big to fit into the output. So I am pretty sure it is B.

Cisco documentation says
netconf max-message size
(Optional) Specifies the maximum size, in kilobytes (KB), for the messages received in a NETCONF session.
The valid range is 1 to 2147483. The default value is infinite.
To set the maximum size to infinite, use the no netconf max-message command.
upvoted 3 times

 **dropspablo** 2 months, 3 weeks ago
So, if you configured "Device(config)# netconf max-message 10" with a maximum message size of 10KB, it's possible that this is limiting the amount of information returned by the show running-config command. This might explain why you can see the output from the show line command, which is probably shorter, but not from the show running-config command.
upvoted 1 times

 **dropspablo** 2 months, 3 weeks ago
I agree
upvoted 1 times

 **Phonon** 8 months, 2 weeks ago
Selected Answer: B

I think its answered correctly:

https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/ntw-servs/b-network-services/m_netconf-sshv2.html
upvoted 2 times

Question #791

Topic 1

Which statement identifies the functionality of virtual machines?

- A. Virtualized servers run most efficiently when they are physically connected to a switch that is separate from the hypervisor
- B. The hypervisor can virtualize physical components including CPU, memory, and storage
- C. Each hypervisor can support a single virtual machine and a single software switch
- D. The hypervisor communicates on Layer 3 without the need for additional resources

Correct Answer: B

  **MED095** Highly Voted 7 months, 3 weeks ago

if you reach here that means u probably completed all 791 questions. i appreciate your dedication and i wish u all the best in your exam. good luck mate :)

upvoted 24 times

  **[Removed]** 2 months, 2 weeks ago

Thank you! Good luck! I've been studying for the past 15 months (netacad, questions, book..) and i still don't feel like i'm ready. This really takes time and patience!!

upvoted 2 times

  **Dutch012** 6 months, 1 week ago

love you <3

upvoted 4 times

  **[Removed]** Most Recent 2 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

  **LeonardoMeCabrio** 3 months, 1 week ago

Stay strong!! And good luck!!

upvoted 2 times

  **Temansky** 7 months, 1 week ago

Got through 2 times lol

Good luck guys!

upvoted 4 times

Which network plane is centralized and manages routing decisions?

- A. management plane
- B. data plane
- C. policy plane
- D. control plane

Correct Answer: D

 **espan** 3 months, 3 weeks ago

Incomplete questions for an incomplete quest
upvoted 1 times

What is a benefit of using private IPv4 addressing?

- A. Multiple companies can use the same addresses without conflicts.
- B. Direct connectivity is provided to internal hosts from outside an enterprise network.
- C. Communication to the internet is reachable without the use of NAT.
- D. All external hosts are provided with secure communication to the internet.

Correct Answer: A

```
MacOs$ ifconfig
```

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=400<CHANNEL_IO>
ether f0:18:98:64:60:32
inet6 fe80::492:c09f:57cf:8c36%en0 prefixlen 64 secured scopeid 0x6
inet 10.8.138.14 netmask 0xffffe000 broadcast 10.8.159.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
```

Refer to the exhibit. A network engineer must provide configured IP addressing details to investigate a firewall rule issue. Which subnet and mask identify what is configured on the en0 interface?

- A. 10.8.0.0/16
- B. 10.8.64.0/18
- C. 10.8.128.0/19
- D. 10.8.138.0/24

Correct Answer: C

 **gewe** Highly Voted 7 months ago

ff - 1111 1111 - 255
eo - 1110 0000 - 224
00 - 0000 0000 - 0
upvoted 16 times

 **all4one** Most Recent 3 months, 2 weeks ago

You can cross-check the answer using the ip of 10.8.138.14 and broadcast domain 10.8.159.255
In a /19 means you increment by 32 for each network.
The network and new network is 10.8.128.0 - 10.8.160.0. So, the broadcast is correct.
upvoted 2 times

 **dropspablo** 2 months, 3 weeks ago

Correct
upvoted 1 times

What are two characteristics of a small office / home office connection environment? (Choose two.)

- A. It requires 10Gb ports on all uplinks.
- B. It supports between 1 and 50 users.
- C. It supports between 50 and 100 users.
- D. A router port connects to a broadband connection.
- E. It requires a core, distribution, and access layer architecture.

Correct Answer: *BD*

  **supvictor** 1 month, 2 weeks ago

B. It supports between 1 and 50 users: SOHO environments are typically designed to serve a small number of users, ranging from a single user (a home office) up to around 50 users in a small office setup.

D. A router port connects to a broadband connection: In SOHO environments, a common setup involves a router connecting to a broadband internet connection, such as DSL, cable, or fiber, to provide internet access to the connected devices in the home or office.

upvoted 1 times

Which element of a virtualization solution manages virtualized services and enables connections between virtualized services and external interfaces?

- A. software
- B. network functionality
- C. virtual machine
- D. hardware

Correct Answer: C

  **oatmealturkey** Highly Voted 7 months ago

Selected Answer: A

"Virtualization software - A hypervisor provides management for virtualized services. It enables connections between virtual services and external interfaces."

<https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-virtualization.html#~how-it-works>

upvoted 7 times

  **JJY888** Most Recent 4 months, 1 week ago

sbnpj: I'm sorry my friend but ChatGPT is often wrong because Ciscs's wording combined with extra correct answers throws it off.

upvoted 1 times

  **JJY888** 4 months, 1 week ago

Selected Answer: A

I personally work with virtualization and this is a crap question. It is either A or D. But A has my vote by a long shot.

upvoted 3 times

  **rogi2023** 5 months, 3 weeks ago

Selected Answer: A

agree with oatmealturkey "Virtualization software - A hypervisor provides management for virtualized services. It enables connections between virtual services and external interfaces."



upvoted 1 times

  **sbnpj** 5 months, 3 weeks ago

As per Chatgpt

The correct answer to the question is B. Network functionality, which refers to the virtualized network components responsible for managing and directing traffic between virtualized services and external interfaces. This includes elements such as virtual switches, routers, firewalls, and load balancers.

upvoted 2 times

  **dropspablo** 2 months, 3 weeks ago

"Network functionality" has a very broad and far-reaching meaning, so it will always be chosen, but this is not the answer cisco wants. Try removing the letter B and you will see that the letter A. Software will be perfectly chosen!

upvoted 1 times

  **gewe** 7 months ago

A hypervisor provides management for virtualized services. It enables connections between virtual services and external interfaces. It should include platform management, a virtualization layer, a programmable API, and a health monitoring system

It seems to be A

upvoted 1 times

Which group of channels in the 802.11b/g/n/ac/ax 2.4 GHz frequency bands are nonoverlapping channels?

- A. channels 1, 5, and 10
- B. channels 1, 6, and 11
- C. channels 1, 5, and 11
- D. channels 1, 6, and 10

Correct Answer: *B*

What is a function of Layer 3 switches?

- A. They route traffic between devices in different VLANs.
- B. They transmit broadcast traffic when operating in Layer 3 mode exclusively.
- C. They move frames between endpoints limited to IP addresses.
- D. They forward Ethernet frames between VLANs using only MAC addresses,


Correct Answer: C

  **Bugatti** Highly Voted 7 months ago



Went through these questions 3 times... taking the exam next week :)
upvoted 9 times

  **Trains** 3 months ago

Must've passed because there wasn't a response to the "how'd it go" questions lol. Looks like the key to success is by going through it at least 3 times
upvoted 5 times

  **kennie0** 3 months, 3 weeks ago

how was your exam?
upvoted 2 times

  **Wes_60** 5 months, 2 weeks ago

How did it go?
upvoted 2 times

  **oatmealturkey** Highly Voted 7 months ago

Selected Answer: A

They route traffic between devices in different VLANs.
upvoted 6 times



  **AndreaGambera** Most Recent 3 weeks, 4 days ago

Selected Answer: U

A is correct !
upvoted 1 times


  **john1247** 3 months ago

300 problems left, but I can't see the end. When will it be over.1138/798
upvoted 2 times

  **JJY888** 6 months, 2 weeks ago

Selected Answer: A

https://documentation.meraki.com/MS/Layer_3_Switching/Layer_3_vs_Layer_2_Switching#:~:text=Since%20VLANs%20exist%20in%20their,functions%20in%20addition%20to%20switching.
upvoted 1 times

  **Dutch012** 6 months, 2 weeks ago

Selected Answer: B

Same as router
upvoted 1 times

  **Dutch012** 6 months, 2 weeks ago

I meant A Dammit!!!
upvoted 2 times

  **gewe** 7 months ago

A and C seems both correct
upvoted 1 times

  **oatmealturkey** 6 months, 3 weeks ago

"They move frames between endpoints limited to IP addresses" is strange wording and makes me think it is wrong. Endpoints are not limited to IP addresses, they have MAC addresses as well. And like a router, Layer 3 switches do not only use IP address. They inspect the destination MAC address to determine if it is on the same or a different subnet, if different subnet they strip frame and re-encapsulate etc., if same subnet they forward to destination endpoint. Based on MAC address. And actually if you just focus on the word "frames" and take it very literally, that is the Layer 2 PDU so IP addresses aren't involved.

upvoted 4 times

DRAG DROP

Drag and drop the RF terms from the left onto the corresponding statements on the right.

absorption	measure of the minimum power required to decode a radio signal without excessive errors
noise floor	measure of the total unwanted signals at the receiver
reflection	deviation from the propagation path that occurs when a signal encounters an obstacle
receiver sensitivity	reduction of energy in a signal as it travels away from the access point and encounters free space or obstacles
signal-to-noise ratio	relative power of the desired radio signal to unwanted signals at the receiver

Correct Answer:

absorption	signal-to-noise ratio
noise floor	noise floor
reflection	receiver sensitivity
receiver sensitivity	reflection
signal-to-noise ratio	absorption

ike110 Highly Voted 7 months ago
should't it be as follows?

receiver sensitivity
noise floor
reflection
absorption
signal-to-noise ratio
upvoted 26 times

dropspablo 2 months, 3 weeks ago
I agree, adding:

Signal-to-Noise Ratio (SNR) and Noise Floor
[https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_\(SNR\)_and_Wireless_Signal_Strength](https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_(SNR)_and_Wireless_Signal_Strength)

Receiver Sensitivity
<https://support.huawei.com/enterprise/br/doc/EDOC1000077015/bc2e25db/receiver-sensitivity>
upvoted 1 times

dropspablo 2 months, 3 weeks ago
Absorption e Reflection:

<https://www.mdpi.com/1424-8220/20/18/5121#:~:text=media%20%5B15%5D%3A-,Absorption,-%3A%20change%20of%20the>

<https://www.cambiumnetworks.com/blog/when-it-comes-to-wi-fi-coverage-green-is-not-always-a-good-color/>
upvoted 1 times

Irios2799 6 months, 2 weeks ago

You're right, the answer provided is terribly wrong...

upvoted 4 times

  **dropspablo** Most Recent 3 weeks, 1 day ago

unwanted signal = noise

upvoted 1 times

  **Friday_Night** 3 months, 3 weeks ago

they should just let the people answer these questions instead of them answering wrong

upvoted 3 times

  **JJY888** 4 months, 1 week ago

Comon sense is not that common.

receiver sensitivity

noise floor

reflection

absorption



signal-to-noise ratio

upvoted 1 times

  **beerbiceps1** 5 months, 2 weeks ago

the drag and drop answers are mostly wrong. Please do your research before taking the exam.

upvoted 2 times

  **JJY888** 6 months, 2 weeks ago

Based on simple Google searches:

receiver sensitivity

noise floor

reflection

absorption

signal-to-noise ratio

upvoted 3 times

  **gewe** 7 months ago

that's right lke110

upvoted 3 times

Which cable type must be used to interconnect one switch using 1000 BASE-SX GBIC modules and another switch using 1000 BASE-SX SFP modules?

- A. LC to SC
- B. SC to SC
- C. LC to LC
- D. SC to ST

Correct Answer: D

 **JJY888** Highly Voted 6 months, 2 weeks ago

Selected Answer: A

SFP is LC:

all SFP and SFP+ optics require LC connectors so the question becomes when you need single mode fiber or multi mode fiber but the connector type is clear. SC square connectors are too big to fit in a SFP or SFP+.

GBIC is SC:

GBIC is commonly used with Gigabit Ethernet and Fibre Channel. But its applications are not limited to these two types. There is also Fast Ethernet (FE) GBIC, BIDI GBIC, CWDM GBIC, DWDM GBIC, etc. Generally, GBIC is with the SC connector. Jan 14, 2015


The question is really about connector types. My answers were Googled.

upvoted 11 times

 **Da_Costa** Most Recent 3 months ago

LC SC is the correct answer


upvoted 1 times

 **RidzV** 6 months, 1 week ago

Selected Answer: A

Agree with below explanation from JJY888


upvoted 1 times

 **DavidCisco** 6 months, 3 weeks ago

Selected Answer: A

1000 BASE-SX GBIC is SC and 1000 BASE-SX SFP is LC

upvoted 1 times

 **DavidCisco** 6 months, 3 weeks ago

Can someone explain why this is the answer?

upvoted 1 times

 **wondaah** 6 months, 1 week ago

Because GBIC is old and still uses SC. SFP are smaller and cannot fit SC connectors therefore they use LC

upvoted 1 times

DRAG DROP

Drag and drop the virtualization concepts from the left onto the matching statements on the right.

guest operating system	An operating system instance that is decoupled from the server hardware.
host operating system	Each core can run more than one process simultaneously.
hypervisor	Runs on a physical server, manages, and allocates the physical resources.
multithreading	The software that manages the basic functions of the physical hardware.
virtual machine	The software that manages the basic functions of the vital machine.

Correct Answer:

guest operating system	virtual machine
host operating system	multithreading
hypervisor	host operating system
multithreading	guest operating system
virtual machine	hypervisor

gewe Highly Voted 7 months ago

1. virtual machine
 2. multithreading
 3. hypervisor
 4. host OS
 5. guest OS
- upvoted 19 times

JJY888 Highly Voted 6 months, 2 weeks ago

1. virtual machine
 2. multithreading
 3. hypervisor
 4. host OS
 5. guest OS
- upvoted 5 times

Nwanna1 Most Recent 2 weeks ago

1. Host Operating system (Virtual machine is not an Operating system)
 2. Multithreading
 3. Hypervisor
 4. Virtual Machine (Asked for software not operating system)
 5. Guest Operating system
- upvoted 1 times

What is a benefit of a point-to-point leased line?

- A. low cost
- B. full-mesh capability
- C. simplicity of configuration
- D. flexibility of design

Correct Answer: C

 **Da_Costa** 3 months ago

Point-to-point leased line simplifies the configuration as the circuit is available on a permanent basis and does not require a connection to be set up before traffic is passed. It does not require to define a permanent virtual circuit (PVC) in the configuration either ...C is correct
upvoted 3 times

Why is TCP desired over UDP for applications that require extensive error checking, such as HTTPS?

- A. UDP uses sequencing data for packets to arrive in order, and TCP offers the capability to receive packets in random order.
- B. UDP uses flow control mechanisms for the delivery of packets, and TCP uses congestion control for efficient packet delivery.
- C. UDP reliably guarantees delivery of all packets, and TCP drops packets under heavy load.
- D. UDP operates without acknowledgments, and TCP sends an acknowledgment for every packet received.

Correct Answer: A


 **Mshamel** Highly Voted 7 months ago

Selected Answer: D

The answer is D.
upvoted 7 times

 **exsiaino** Most Recent 1 week ago

correct answer is D.
upvoted 1 times

 **Yinx** 3 weeks, 2 days ago

Selected Answer: D

Obviously, A is wrong.
upvoted 1 times

 **Da_Costa** 2 months, 1 week ago

Selected Answer: D

Going through the answers I think the right choice is D
upvoted 1 times


 **jaya9233** 2 months, 3 weeks ago

a is incorrect
upvoted 2 times

 **yuz1227** 6 months, 1 week ago


Selected Answer: D

correct answer is D.
upvoted 2 times

 **JJY888** 6 months, 2 weeks ago

Selected Answer: D

UDP does not use sequence numbers or windowing, so there is no need for a three-way handshake to set initial values. If a device using UDP becomes swamped by an excessive number of datagrams, it will simply drop those that it cannot process
upvoted 1 times

 **DavidCisco** 6 months, 3 weeks ago

Selected Answer: D

The answer is D, Answer A is upside down
upvoted 3 times

 **gewe** 7 months ago

UDP operates without acknowledgments, and TCP sends an acknowledgment for every packet received.
upvoted 4 times

Which component controls and distributes physical resources for each virtual machine?

- A. hypervisor
- B. OS
- C. CPU
- D. physical enclosure

Correct Answer: A

What is the role of nonoverlapping channels in a wireless environment?

- A. to increase bandwidth
- B. to stabilize the RF environment
- C. to allow for channel bonding
- D. to reduce interference

Correct Answer: B

🗨️ **MorpheusX** Highly Voted 2 months ago

Why do I even pay money for the question catalogue if so many questions are answered incorrectly? You still learn the wrong things if you don't pay attention. That sucks!!!

upvoted 5 times

🗨️ **Gus1987** 1 month, 2 weeks ago

thats happend to me, with a group buy a cersthero exam and i must to check idk how many question wrong

upvoted 1 times

🗨️ **[Removed]** Most Recent 2 months, 2 weeks ago

Selected Answer: D

Answer D is correct

upvoted 1 times

🗨️ **Shaolinta** 3 months, 2 weeks ago

Selected Answer: D

The correct answer is:

D. to reduce interference

The role of nonoverlapping channels in a wireless environment is to reduce interference between wireless devices. In wireless networks, such as Wi-Fi networks, different devices transmit data wirelessly using specific frequency bands. These frequency bands are divided into channels, which act as virtual pathways for data transmission.

When multiple wireless devices operate in close proximity and use overlapping channels, there is a potential for interference. Interference occurs when devices in overlapping channels transmit signals simultaneously, leading to signal degradation and reduced performance.

Nonoverlapping channels are spaced far enough apart to minimize interference between adjacent channels. By assigning wireless devices to nonoverlapping channels, network administrators can reduce interference and improve overall network performance. This allows devices operating on different channels to transmit data without significantly overlapping with adjacent channels.

Therefore, the primary role of nonoverlapping channels in a wireless environment is to reduce interference, enhancing the stability and reliability of wireless communication.

upvoted 1 times

🗨️ **Shaolinta** 3 months, 2 weeks ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

🗨️ **JJY888** 6 months, 2 weeks ago

Selected Answer: D

Considering the 2.4 GHz band is only 100 MHz wide, the 11 channels of 20 MHz overlap with one another. This is what causes the interference on your network and a lag in your WiFi's performance. Certain channels yield better WiFi performance than others because they are non-overlapping.

<https://www.minim.com/blog/wifi-channels-explained#:~:text=Considering%20the%202.4%20GHz%20band,because%20they%20are%20non%20overlapping.>

upvoted 3 times

🗨️ **Dutch012** 6 months, 2 weeks ago

D boys!!

upvoted 2 times

🗨️ **Peter_panda** 6 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 4 times

🗨️ 👤 **Rynurr** 6 months, 4 weeks ago

Selected Answer: D

IMO ' to reduce interference ' is correct answer
upvoted 4 times

🗨️ 👤 **ike110** 6 months, 4 weeks ago

" to reduce interference" would make sense too I presume
upvoted 3 times

Question #806

Topic 1

What are two advantages of implementing a controller-based architecture instead of traditional network architecture? (Choose two.)

- A. It allows for seamless connectivity to virtual machines.
- B. It increases security against denial-of-service attacks.
- C. It supports complex and high-scale IP addressing schemes.
- D. It enables configuration task automation.
- E. It provides increased scalability and management options.

Correct Answer: DE



What is the purpose of the service-set identifier?

- A. It identifies the wireless network to which an application must connect.
- B. It identifies the wired network to which a network device is connected.
- C. It identifies the wired network to which a user device is connected.
- D. It identifies a wireless network for a mobile device to connect.

Correct Answer: B

- 🗨️ **purenuker** Highly Voted 6 months, 3 weeks ago
So many incorrect answers here .. Is this what I paid for ?
upvoted 18 times
- 🗨️ **Dutch012** 6 months, 2 weeks ago
it is bad but at least we have a discussion section.
upvoted 6 times
- 🗨️ **AndreaGambera** Most Recent 3 weeks, 4 days ago
Selected Answer: D
D is correct !
upvoted 1 times
- 🗨️ **Vyncy** 3 months ago
Isn't A correct answer ? Device doesn't have to be mobile to be able to connect to wifi (for example desktop pc with wifi card)
upvoted 2 times
- 🗨️ **mrmanistheman** 4 months, 1 week ago
Selected Answer: D
The admins need to sort this out, would be useless without the knowlegable folk in the discussion section.
Correct answer is D.
upvoted 1 times
- 🗨️ **Njavwa** 5 months ago
wired networks do not have SSIDs
SSIDs are for Wi-Fi
upvoted 2 times
- 🗨️ **DaimonANCC** 5 months, 1 week ago
Selected Answer: D
Correct, the service-set identifier (SSID) is a unique identifier for a wireless local area network (WLAN). It is used to identify the wireless network to which a mobile device, such as a laptop or smartphone, can connect.
upvoted 2 times
- 🗨️ **JJY888** 6 months, 2 weeks ago
The problem is B, C, and D are correct. Maybe to question is which one does NOT.
upvoted 1 times
- 🗨️ **Peter_panda** 6 months, 3 weeks ago
How they establish the correct answer ?!
upvoted 2 times
- 🗨️ **wondaah** 6 months, 1 week ago
they throw dice
upvoted 2 times
- 🗨️ **lucantonelli93** 6 months, 4 weeks ago
Selected Answer: D
it's D the correct answer
upvoted 3 times
- 🗨️ **Rynurr** 6 months, 4 weeks ago
Selected Answer: D
definitely "D"
'It identifies a wireless network for a mobile device to connect'



upvoted 3 times

  **ike110** 6 months, 4 weeks ago

Selected Answer: D

The answer should be D

upvoted 4 times

  **ike110** 6 months, 4 weeks ago

SSID - The abbreviation stands for service set identifier

upvoted 1 times

  **SamSerious365** 6 months, 4 weeks ago

Wrong, D should be the correct answer.

upvoted 3 times

Question #808

Topic 1

Which is a fact related to FTP?

- A. It always operates without user authentication.
- B. It uses block numbers to identify and mitigate data-transfer errors.
- C. It uses two separate connections for control and data traffic.
- D. It relies on the well-known UDP port 69.

Correct Answer: C

  **learntstuff** 1 month, 4 weeks ago

Selected Answer: C

First paragraph in this link,

<https://learn.microsoft.com/en-us/connectors/ftp/>

upvoted 1 times

  **learntstuff** 1 month, 4 weeks ago

Answer is correct

upvoted 1 times

How do UTP and STP cables compare?

- A. UTP cables provide faster and more reliable data transfer rates and STP cables are slower and less reliable.
- B. STP cables are shielded and protect against electromagnetic interference and UTP lacks the same protection against electromagnetic interference.
- C. STP cables are cheaper to procure and easier to install and UTP cables are more expensive and harder to install.
- D. UTP cables are less prone to crosstalk and interference and STP cables are more prone to crosstalk and interference.

Correct Answer: B

  **nitti47** 3 months ago

STP means shield twisted pair easy B is the answer
upvoted 2 times

  **[Removed]** 2 months, 2 weeks ago

Yes, Shielded Twisted Pair
upvoted 1 times

  **kncappy** 3 months ago

B. Shielded cables (STP) are used to reduce electromagnetic and radio frequency interference. Unshielded cables (UTP) are cheaper and easier to install.
upvoted 2 times

  **krzysiew** 5 months, 2 weeks ago



Selected Answer: B

definitely
upvoted 2 times

What are two disadvantages of a full-mesh topology? (Choose two.)

- A. It requires complex configuration.
- B. It needs a high MTU between sites.
- C. It works only with BGP between sites.
- D. It has a high implementation cost.
- E. It must have point-to-point communication.

Correct Answer: AD

  **sam225555** 2 months ago

Selected Answer: AD

correct
upvoted 1 times

DRAG DROP

Drag and drop the wireless standards from the left onto the number of nonoverlapping channels they support on the right.

802.11a	J Non-Overlapping Channels
802.11b	
802.11g	
802.11n 2.4 GHz	2J Non-Overlapping Channels
802.11n 5 Ghz	

Correct Answer:

802.11a	J Non-Overlapping Channels
802.11b	
802.11g	
802.11n 2.4 GHz	2J Non-Overlapping Channels
802.11n 5 Ghz	

iMo7ed Highly Voted 4 months ago

3 Non-Overlapping Channels:

- 802.11b
- 802.11g
- 802.11n (2.4 GHz)

23 Non-Overlapping Channels:

- 802.11a
- 802.11n (5 GHz)

upvoted 9 times

51007 2 months, 1 week ago

thank you

upvoted 1 times

perri88 3 months ago

correct

upvoted 2 times

Peter_panda Highly Voted 6 months, 2 weeks ago

Probably the choices are 3, respectively 23 (not J and 2J). 2.4GHz networks have 3 non overlapping channels, 5GHz networks have 23

upvoted 7 times

 **Peter_panda** 6 months, 2 weeks ago


So the answers are: b, g, n@2.4G, respectively a, n@5G

upvoted 11 times

 **MorpheusX** Most Recent 2 months ago

Why do I even pay money for the question catalogue if so many questions are answered incorrectly? You still learn the wrong things if you don't pay attention. That sucks!!!

upvoted 1 times

 **[Removed]** 2 months, 2 weeks ago

802.11a : 5 GHz

802.11b : 2.4 GHz

802.11g : 2.4 GHz

802.11n : both 2.4 GHz and 5 GHz

802.11b has 3 Non-Overlapping Channels

802.11g has 3 Non-Overlapping Channels

802.11n - 2.4Ghz has 3 Non-Overlapping Channels

802.11a has 23 Non-Overlapping Channels

802.11n - 5Ghz has 23 Non-Overlapping Channels

upvoted 1 times

Question #812

Topic 1

Which technology allows for multiple operating systems to be run on a single host computer?

- A. virtual routing and forwarding
- B. virtual device contexts
- C. network port ID virtualization
- D. server virtualization

Correct Answer: D

Question #813

Topic 1

Why would an administrator choose to implement an automated network management solution?


- A. to reduce operational costs
- B. to support simpler password policies
- C. to enable "box by box" configuration and deployment
- D. to limit recurrent management costs

Correct Answer: A

What is a function of the core and distribution layers in a collapsed-core architecture?

- A. The router can support HSRP for Layer 2 redundancy in an IPv6 network.
- B. The core and distribution layers are deployed on two different devices to enable failover.
- C. The router operates on a single device or a redundant pair.
- D. The router must use IPv4 and IPv6 addresses at Layer 3.


Correct Answer: C

 **dropspablo** 2 months, 3 weeks ago

Selected Answer: C

C is correct, the CORE and Distribution layer are collapsed (unified) into one and using only one device (router, SW...). However, it usually uses two collapsed layer devices (pair) for redundancy or load distribution.


upvoted 1 times

 **Yannik123** 4 months ago

Selected Answer: C

I think C is the correct answer.

upvoted 1 times

 **VictorCisco** 5 months, 2 weeks ago

Selected Answer: B

collapsed-core architecture is at least 2 devices - one for distribution layer, one for core layer.

upvoted 2 times

 **Lokylax** 4 months, 1 week ago

That's wrong. A collapsed core architecture takes the normal three-tier hierarchical network and collapses it into a two-tier network. In a two-tier network, the function of the switches in the core layer and distribution layer are "collapsed" into a combined core and distribution layer on a single switch.

upvoted 3 times

 **Dutch012** 6 months, 1 week ago

I guess B is better

upvoted 3 times

What must be considered before deploying virtual machines?

- A. resource limitations, such as the number of CPU cores and the amount of memory
- B. support for physical peripherals, such as monitors, keyboards, and mice
- C. whether to leverage VSM to map multiple virtual processors to two or more virtual machines
- D. location of the virtual machines within the data center environment

Correct Answer: A

What are two facts that differentiate optical-fiber cabling from copper cabling? (Choose two.)

- A. It is less expensive when purchasing patch cables.
- B. It carries electrical current further distances for PoE devices.
- C. It provides greater throughput options.
- D. It has a greater sensitivity to changes in temperature and moisture.
- E. It carries signals for longer distances.

Correct Answer: CE

  **mjalal2023** 1 month ago

Selected Answer: AC

A and C

upvoted 1 times

  **juneq888** 3 days, 7 hours ago

No, not A. Fiber is more expensive than copper cable.

upvoted 1 times

  **kncappy** 3 months ago

Selected Answer: CE

A. It is less expensive when purchasing patch cables. - No, fiber is more expensive

B. It carries electrical current further distances for PoE devices. - No, fiber cables transmit data via light

C. It provides greater throughput options. - Yes, copper ethernet cables can transfer data around 300 Mbps while fiber can transfer data up to 10Gbps

D. It has a greater sensitivity to changes in temperature and moisture. - No, fiber cables have more pressure resistance and are less susceptible to EMI

E. It carries signals for longer distances. - Yes, copper cables can carry signals for 330 feet/100m while fiber can carry 1000 feet for multi-mode and up to 25 miles for single-mode

upvoted 4 times

  **mjalal2023** 1 month ago

Optical Fiber and Signal!!

They are not related, Fiber uses Lights not the Signal, So E is Incorrect!

upvoted 1 times

What are two behaviors of a point-to-point WAN topology? (Choose two.)

- A. It leverages a dedicated connection.
- B. It provides direct connections between each router in the topology.
- C. It delivers redundancy between the central office and branch offices.
- D. It uses a single router to route traffic between sites.
- E. It connects remote networks through a single line.

Correct Answer: BD

 **Techpro30** 1 month, 3 weeks ago

Selected Answer: AE

Its A, E

upvoted 2 times

 **MorpheusX** 2 months ago

Why do I even pay money for the question catalogue if so many questions are answered incorrectly? You still learn the wrong things if you don't pay attention. That sucks!!!

upvoted 2 times

 **Simon_1103** 4 months, 3 weeks ago

Selected Answer: AE


A point-to-point WAN topology uses a dedicated line or circuit to connect two network devices, such as routers or switches, over a long distance. This dedicated connection is typically established by a service provider and provides a direct link between the two devices, with no intermediary network devices in between. This topology is often used to connect remote sites or branch offices to a central office or data center, and can be used for various WAN technologies such as T1/E1 lines, leased lines, or MPLS circuits.

Option B is incorrect because a point-to-point topology only provides a direct connection between the two devices at each end of the link, not between each router in the topology.

Option C is incorrect because point-to-point topologies typically do not provide redundancy between sites, as there is only one dedicated line or circuit connecting the two devices.

Option D is incorrect because point-to-point topologies require two routers or devices, one at each end of the dedicated line or circuit, to route traffic between the sites.

upvoted 3 times

 **JJY888** 6 months, 2 weeks ago

Selected Answer: AE

<https://ipccisco.com/wan-topology-types/#:~:text=Point%2Dto%2DPoint%20is%20the,distance%20between%20the%20two%20sites.>

upvoted 2 times

 **Titan_intel** 6 months, 2 weeks ago

I am not sure about this one.


upvoted 1 times

 **Peter_panda** 6 months, 2 weeks ago

Selected Answer: AE

I would say A and E, anyway I'm not sure

upvoted 3 times

 **Dutch012** 6 months, 2 weeks ago

Same as you, I just followed my logic

upvoted 1 times

What is a link-local all-nodes IPv6 multicast address?


- A. ff02:0:0:0:0:0:0:1
- B. 2004:33c:94d9:431e:255::
- C. fffe:034:0dd:45d6:789e::
- D. fe80:4433:034:0dd::2

Correct Answer: A

 **j1mlawton** Highly Voted 7 months ago

Selected Answer: A

An IPv6 multicast address for well-known link-local messages would start with "FF02"
upvoted 7 times

 **ike110** 6 months, 4 weeks ago

Correct. IPv6 multicast addresses can be used for link-local LAN communications or they can be scoped for site-specific communications or even global use. An IPv6 multicast address for well-known link-local messages would start with "FF02" and you may recognize that FF02::1 is the all-nodes link-local multicast group address.
upvoted 2 times

 **[Removed]** Most Recent 2 months, 1 week ago

Selected Answer: A

A. ff02:0:0:0:0:0:0:1
ff02 is all-nodes
upvoted 1 times

 **Mshamel** 7 months ago

Selected Answer: D

the correct answer is D.
upvoted 2 times

 **studying_1** 4 months, 1 week ago

ff02::2 is all routers not all nodes, answer is A
upvoted 2 times

 **rogi2023** 5 months, 3 weeks ago

you are wrong: the key is " all-nodes" so therefore multicast and answer A
upvoted 2 times

 **Dutch012** 6 months, 2 weeks ago

it is asking about link-local multicast address, A is right
upvoted 2 times

Which is a reason to implement IPv4 private addressing?

- A. Comply with PCI regulations.
- B. Reduce the size of the forwarding table on network routers.
- C. Reduce the risk of a network security breach.
- D. Comply with local law.

Correct Answer: C

  **shaney67** 1 month ago

B. Reduce the size of the forwarding table on network routers.

Implementing IPv4 private addressing, also known as Network Address Translation (NAT), can help reduce the size of the forwarding table on network routers. NAT allows multiple devices within a private network to share a single public IP address for communication with external networks. This conserves public IP addresses and reduces the size of the routing table, as routers only need to manage the translation of private IP addresses to the single public IP address.

upvoted 1 times

Which signal frequency appears 60 times per minute?

- A. 1 Hz signal
- B. 1 GHz signal
- C. 60 Hz signal
- D. 60 GHz signal

Correct Answer: A

🗳️ 👤 **joefahim** 1 week ago

Hertz (Hz) is a unit of frequency, and a 60 Hz signal oscillates or cycles 60 times per second. A signal with a frequency of 60 times per minute is equivalent to a 1 Hz signal.

Answer is A

upvoted 1 times

🗳️ 👤 **Cynthia2023** 1 month, 2 weeks ago

Selected Answer: A

A is correct. Frequency is the number of cycles or oscillations of a signal that occur in one second.

upvoted 1 times

🗳️ 👤 **dropspablo** 2 months, 3 weeks ago

Selected Answer: A

A 1 Hz signal means that one cycle or oscillation occurs per second. So in one minute there would be 60 cycles as there are 60 seconds in one minute. So the correct answer is indeed A. 1 Hz signal, which would be 60 cycles per minute.

upvoted 2 times

🗳️ 👤 **lolungos** 2 months, 4 weeks ago

Selected Answer: C

60hz - 60 times per second

upvoted 1 times

🗳️ 👤 **xbololi** 2 months, 1 week ago

Please re read the question.

upvoted 1 times

🗳️ 👤 **lolungos** 3 months, 2 weeks ago

Selected Answer: C

1 hz is equal 1 cicle per SECOND

upvoted 1 times

🗳️ 👤 **StingVN** 3 months, 3 weeks ago

Selected Answer: C

The correct answer is C. 60 Hz signal.

A signal frequency that appears 60 times per minute is a 60 Hz signal. The unit "Hz" (hertz) represents the number of cycles or oscillations per second. In this case, a signal with a frequency of 60 Hz means it completes 60 cycles or oscillations in one second.

Since there are 60 seconds in a minute, a 60 Hz signal will complete 60 cycles per second multiplied by 60 seconds, resulting in a total of 3,600 cycles or oscillations per minute.

To summarize, a signal frequency that appears 60 times per minute is a 60 Hz signal.

upvoted 1 times

🗳️ 👤 **Friday_Night** 3 months, 3 weeks ago

1Hz=1 cycle/sec

60Hz=60cycles/sec --> this is too much question is about per minute.. you got confused sir

upvoted 3 times

🗳️ 👤 **jonathan126** 4 months, 3 weeks ago

The correct answer is A. x Hz means x cycles in one second. 1 Hz = 1 cycle in one second.

upvoted 1 times

🗳️ 👤 **RAJ_1920** 5 months ago

Guys answer is A, as 1hz is ONE cycle per second. It will only occur 60 times in 1 minutes as it has 60 seconds in it.

upvoted 2 times

🗄️ 👤 **Ciscoman021** 5 months, 4 weeks ago

Selected Answer: A

A signal frequency that appears 60 times per minute is equivalent to a frequency of 1 Hz, where "Hz" stands for Hertz, a unit of frequency defined as one cycle per second.

upvoted 2 times

🗄️ 👤 **kapel21** 6 months, 1 week ago

C. 60 Hz signal appears 60 times per minute.

Hertz (Hz) is the unit of frequency, which measures the number of cycles of a wave that occur in one second. Therefore, 1 Hz means that one cycle of a wave occurs in one second.

Since there are 60 seconds in a minute, if a signal has a frequency of 60 Hz, it means that there are 60 cycles of the wave in one second, and hence there will be $60 \times 1 = 60$ cycles or appearances of the signal in one minute.

Option A (1 Hz signal) appears only once per second, Option B (1 GHz signal) appears one billion times per second, and Option D (60 GHz signal) appears 60 billion times per second, which are much higher frequencies than the frequency required to appear 60 times per minute.

upvoted 1 times

🗄️ 👤 **Zortex** 6 months, 1 week ago

Selected Answer: C

Frequency is defined as the number of cycles of a periodic waveform that occur in one second. In this case, we are given the number of occurrences per minute, which is 60. To convert this to frequency, we divide 60 by 60 (the number of seconds in a minute) to get 1 cycle per second or 1 Hz.

Therefore, options A and B are incorrect since they do not match the given frequency of 60 occurrences per minute. Option D is also incorrect because 60 GHz is an extremely high frequency used in some wireless communication systems and is not related to the given frequency of 60 occurrences per minute.

upvoted 1 times

🗄️ 👤 **ike110** 6 months, 4 weeks ago

Selected Answer: A

correct

upvoted 2 times

Question #821

Topic 1

What is a function of spine-and-leaf architecture?

- A. offers predictable latency of the traffic path between end devices
- B. mitigates oversubscription by adding a layer of leaf switches
- C. exclusively sends multicast traffic between servers that are directly connected to the spine
- D. limits payload size of traffic within the leaf layer

Correct Answer: A

🗄️ 👤 **VarDav** 4 weeks ago

Selected Answer: A

A seems like the more text book answer than B

upvoted 1 times

What is a function of an endpoint?

- A. It passes unicast communication between hosts in a network.
- B. It transmits broadcast traffic between devices in the same VLAN.
- C. It provides security between trusted and untrusted sections of the network.
- D. It is used directly by an individual user to access network services.

Correct Answer: D

🗨️ 👤 **JJY888** 6 months, 2 weeks ago

Selected Answer: D

An endpoint is a remote computing device that communicates back and forth with a network to which it is connected. Examples of endpoints include: Desktops. Laptops. Smartphones.

upvoted 4 times

What is a function of MAC address learning?

- A. It is disabled by default on all interfaces connected to trunks.
- B. It increases security on the management VLAN.
- C. It is enabled by default on all VLANs and interfaces.
- D. It increases the potential for MAC address flooding.

Correct Answer: C

🗨️ 👤 **gewe** **Highly Voted** 👍 7 months ago

great construct question.. its really function that is enables

upvoted 6 times

🗨️ 👤 **VictorCisco** 5 months, 2 weeks ago

Yeah! What is the main purpose of a cisco switch?

It's GREEN!

upvoted 7 times

Which IPv6 address range is suitable for anycast addresses for distributed services such as DHCP or DNS?

- A. FF00:1/12
- B. 2001:db8:0234:ca3e::1/128
- C. FE80::1/10
- D. 2002:db84:3f30:ca84:be76:2/64

Correct Answer: B

  **Cynthia2023** 1 month, 2 weeks ago

Selected Answer: B

The key characteristic of anycast addresses is that they are assigned to multiple interfaces (nodes) in different locations. However, these anycast addresses are regular global unicast addresses, and there is no special reserved range specifically for anycast use.

upvoted 2 times

  **rogi2023** 5 months, 4 weeks ago

Selected Answer: B

A-valid multicast IPv6 address
 B-valid single IPv6 address
 C-valid IPv6 link local address
 D-not valid IPv6 address - not long enough :-)
 therefore the correct answer is B

upvoted 4 times

  **rogi2023** 5 months, 3 weeks ago

B is not a range, but at least it is valid global host IPv6 address - so could be also anycast address...but it is a tricky (shit) question.

upvoted 6 times

What is a similarity between OM3 and OM4 fiber optic cable?

- A. Both have a 62.5 micron core diameter.
- B. Both have a 100 micron core diameter.
- C. Both have a 50 micron core diameter.
- D. Both have a 9 micron core diameter.

Correct Answer: C

  **Dutch012**  6 months, 2 weeks ago

again, Cisco is an ass



upvoted 13 times

  **kncappy**  3 months ago

Selected Answer: C

In terms of core sizes, OM1 and OM2 have a core of 62.5 microns while OM3, OM4, and OM5 have a core of 50 microns

upvoted 1 times

  **JJY888** 6 months, 2 weeks ago

Selected Answer: C

OM3 vs OM4: Similarities

They have the same fiber core size 50/125 and the termination of the connectors is the same. Additionally, both of them are designed for use with 850-nm VCSELs (vertical-cavity surface-emitting lasers) and have aqua sheaths.Sep 1, 2015

upvoted 3 times

Which device segregates a network into separate zones that have their own security policies?

- A. IPS
- B. switch
- C. access point
- D. firewall

Correct Answer: D

What is the primary purpose of private address space?

- A. limit the number of nodes reachable via the Internet
- B. simplify the addressing in the network
- C. conserve globally unique address space
- D. reduce network complexity

Correct Answer: C

 **Calinserban** 1 month, 1 week ago

Should be A, private is referring at ipv4 and globally unique is referring at ipv6
upvoted 2 times

What is a characteristic of a collapsed-core network topology?

- A. It enables all workstations in a SOHO environment to connect on a single switch with internet access.
- B. It enables the core and access layers to connect to one logical distribution device over an EtherChannel.
- C. It allows wireless devices to connect directly to the core layer, which enables faster data transmission.
- D. It allows the core and distribution layers to run as a single combined layer.

Correct Answer: D

 **shaney67** 1 month ago

B. It enables the core and access layers to connect to one logical distribution device over an EtherChannel.

In a collapsed-core network topology, the core and access layers connect to one logical distribution device (usually a switch or a set of switches) over an EtherChannel or aggregated link. This design simplifies the network architecture by reducing the number of layers and devices required, which is often suitable for small to medium-sized networks. It's a way to collapse the traditional hierarchical three-layer network design into fewer layers, making management and configuration simpler.

upvoted 1 times

A technician receives a report of network slowness and the issue has been isolated to the interface FastEthernet0/13. What is the root cause of the issue?


FastEthernet0/13 is up, line protocol is up
Hardware is Fast Ethernet, address is 0001.4d27.66cd (bia 0001.4d27.66cd)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 250/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set

Keepalive not set -
Auto-duplex (Full) Auto Speed (100), 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 18:52:43, output 00:00:01, output hang never
Last clearing of "show interface" counters never

Queueing strategy: fifo -
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 12000 bits/sec, 6 packets/sec
5 minute output rate 24000 bits/sec, 6 packets/sec
14488019 packets input, 2434163609 bytes
Received 345348 broadcasts, 0 runts, 0 giants, 0 throttles
261028 input errors, 259429 CRC, 1599 frame, 0 overrun, 0 ignored
0 watchdog, 84207 multicast
0 input packets with dribble condition detected
19658279 packets output, 3529106068 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

- A. local buffer overload
- B. err-disabled port on the far end
- C. physical errors
- D. duplicate IP addressing

Correct Answer: C

  **kncappy** 2 months, 3 weeks ago

Selected Answer: C

A high number of CRCs typically result from collisions but can also indicate a physical issue (cabling, bad interface/NIC)
upvoted 4 times

  **Yannik123** 4 months ago

Selected Answer: C

Look on CRC
upvoted 2 times

  **HSong** 4 months, 2 weeks ago

reliability 250/255,
upvoted 1 times

What occurs when overlapping Wi-Fi channels are implemented?

- A. Users experience poor wireless network performance.
- B. Wireless devices are unable to distinguish between different SSIDs.
- C. The wireless network becomes vulnerable to unauthorized access.
- D. Network communications are open to eavesdropping.

Correct Answer: A

 **VarDav** 4 weeks ago

Selected Answer: A

Answer is correct

upvoted 1 times

```

Router1#show interface ethernet 1
Ethernet1 is up, line protocol is up
  Hardware is Lance, address is 0010.7b36.1be8 (bia 0010.7b36.1be8)
  Internet address is 10.100.48.240/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 1/75/1/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: random early detection(RED)
  Output queue :0/40 (size/max)
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    7558065 packets input, 783768942 bytes, 1 no buffer
    Received 8280963 broadcasts, 0 runts, 0 giants, 1 throttles
    15 input errors, 14278 CRC, 0 frame, 0 overrun, 3 ignored
    0 input packets with dribble condition detected
    798092 packets output, 50280266 bytes, 0 underruns
    0 output errors, 15000 collisions, 0 interface resets
    0 babbles, 0 late collision, 179 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out

```

Refer to the exhibit. An administrator received a call from a branch office regarding poor application performance hosted at the headquarters. Ethernet 1 is connected between Router1 and the LAN switch. What identifies the issue?

- A. The MTU is not set to the default value.
- B. There is a duplex mismatch.
- C. The QoS policy is dropping traffic.
- D. The link is over utilized.

Correct Answer: C

 **ike110** Highly Voted 6 months, 4 weeks ago

Isn't the duplex mismatch a better option due to high # of collisions?
upvoted 7 times

 **oatmealturkey** Highly Voted 6 months, 3 weeks ago

Selected Answer: B

C is clearly incorrect because if that were the case we would see output drops and there are zero output drops.
upvoted 6 times

 **[Removed]** Most Recent 2 months, 1 week ago

Selected Answer: B

B. There is a duplex mismatch.
15000 collisions in the output
upvoted 1 times

 **JJY888** 4 months, 1 week ago

Selected Answer: B

The output shows that there are 15000 collisions on the interface, indicating a duplex mismatch issue between Router1 and the switch. Therefore, the correct answer is B.
upvoted 5 times

 **Ruddypotech** 4 months, 3 weeks ago


Hardware in Lance: La operacion normal de este tipo de hardware es Half Duplex.
El contador 179 deferred se incrementa cuando hay interrupcion en el envio de data porque el otro extremo esta full duplex y hay mismatch en la

negociacion.
upvoted 1 times

 **DavidCisco** 6 months, 2 weeks ago

Selected Answer: D

The interface registers a lot of traffic, it is the only one that makes sense
upvoted 2 times

 **Rynurr** 6 months, 4 weeks ago

Selected Answer: B

'There is a duplex mismatch. ' sounds better for me, so "B".
upvoted 3 times

Question #832

Topic 1

DRAG DROP

Drag and drop the cloud-computing components from the left onto the correct descriptions on the right.

broad network access	The consumer can choose when to start or stop using the service.
measured service	The provider can bill the consumer in accordance with the level of usage.
on-demand self-service	The provider allocates CPU, memory, and disk from its shared compute resources to multiple customers.
rapid elasticity	The resource pool can expand quickly to meet demand.
resource pooling	The service is available from many types of devices and networks.

Correct Answer:

broad network access	on-demand self-service
measured service	measured service
on-demand self-service	resource pooling
rapid elasticity	rapid elasticity
resource pooling	broad network access

 **beerbisceps1** **Highly Voted**  5 months, 2 weeks ago

The answer given is correct
upvoted 8 times

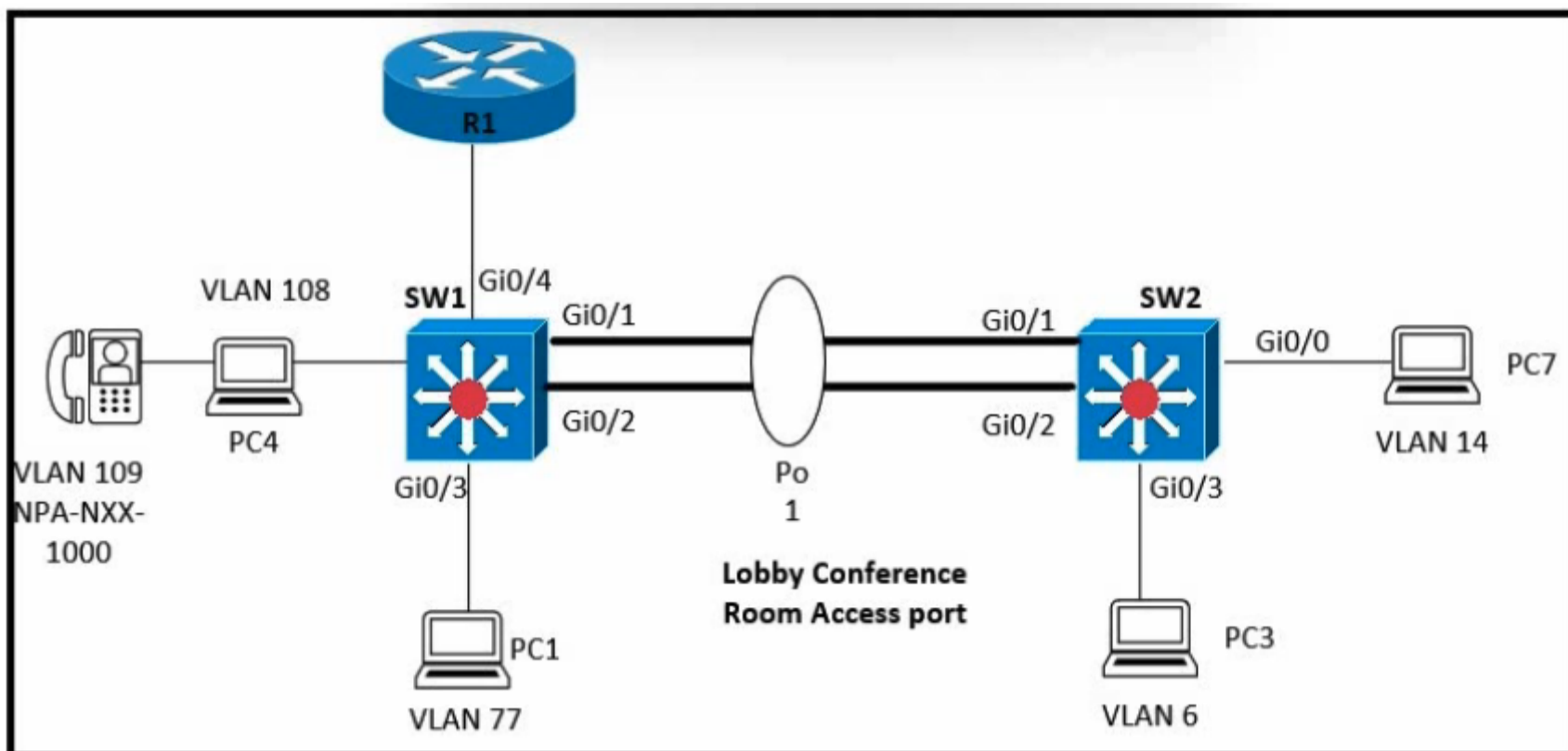
 **perri88** **Most Recent**  3 months ago

correct
upvoted 3 times

What is the functionality of the Cisco DNA Center?

- A. IP address pool distribution scheduler
- B. data center network policy controller
- C. console server that permits secure access to all network devices
- D. software-defined controller for automation of devices and services

Correct Answer: D



Refer to the exhibit. Which configuration enables an EtherChannel to form dynamically between SW1 and SW2 by using an industry-standard protocol, and to support full IP connectivity between all PCs?

```

A. SW1#
interface Gi0/1
switchport
switchport mode access
channel-group 1 mode active
!
interface Gi0/2
switchport
switchport mode access
channel-group 1 mode active

SW2#
interface Gi0/1
switchport
switchport mode access
channel-group 1 mode desirable
!
interface Gi0/2
switchport
switchport mode access
channel-group 1 mode desirable

B. SW1#
interface Gi0/1
switchport
switchport mode trunk
channel-group 1 mode on
!
interface Gi0/2
switchport
switchport mode trunk
channel-group 1 mode auto

SW2#
interface Gi0/1
switchport

```

```
switchport mode trunk
channel-group 1 mode auto
!
interface Gi0/2
switchport
switchport mode trunk
channel-group 1 mode on
interface port-channel 1
switchport
switchport mode trunk
```

```
C. SW1#
interface Gi0/1
switchport
switchport mode trunk
channel-group 1 mode active
!
interface Gi0/2
switchport
switchport mode trunk
channel-group 1 mode active
```

```
SW2#
interface Gi0/1
switchport
switchport mode trunk
channel-group 1 mode passive
!
interface Gi0/2
switchport
switchport mode trunk
channel-group 1 mode passive
```

```
D. SW1#
interface Gi0/1
switchport
switchport mode trunk
channel-group 1 mode auto
!
interface Gi0/2
switchport
switchport mode trunk
channel-group 1 mode auto
```

```
SW2#
interface Gi0/1
switchport
switchport mode trunk
channel-group 1 mode desirable
!
interface Gi0/2
switchport
switchport mode trunk
channel-group 1 mode desirable
```

Correct Answer: C

Correct answer line c. PAGP is the standard protocol uses mode:
on --- on
desirable/auto -- desirable

LACP is not standard uses:
on --- on
passive/active -- active

The question is asking the standard protocol
upvoted 4 times

  **hamish88** 4 months, 4 weeks ago

The correct answer is C. LACP is the industrial standard protocol for EtherChannel.
upvoted 5 times



Question #835

Topic 1

Which functionality is provided by the console connection on a Cisco WLC?



- A. HTTP-based GUI connectivity
- B. secure in-band connectivity for device administration
- C. out-of-band management
- D. unencrypted in-band connectivity for file transfers

Correct Answer: C

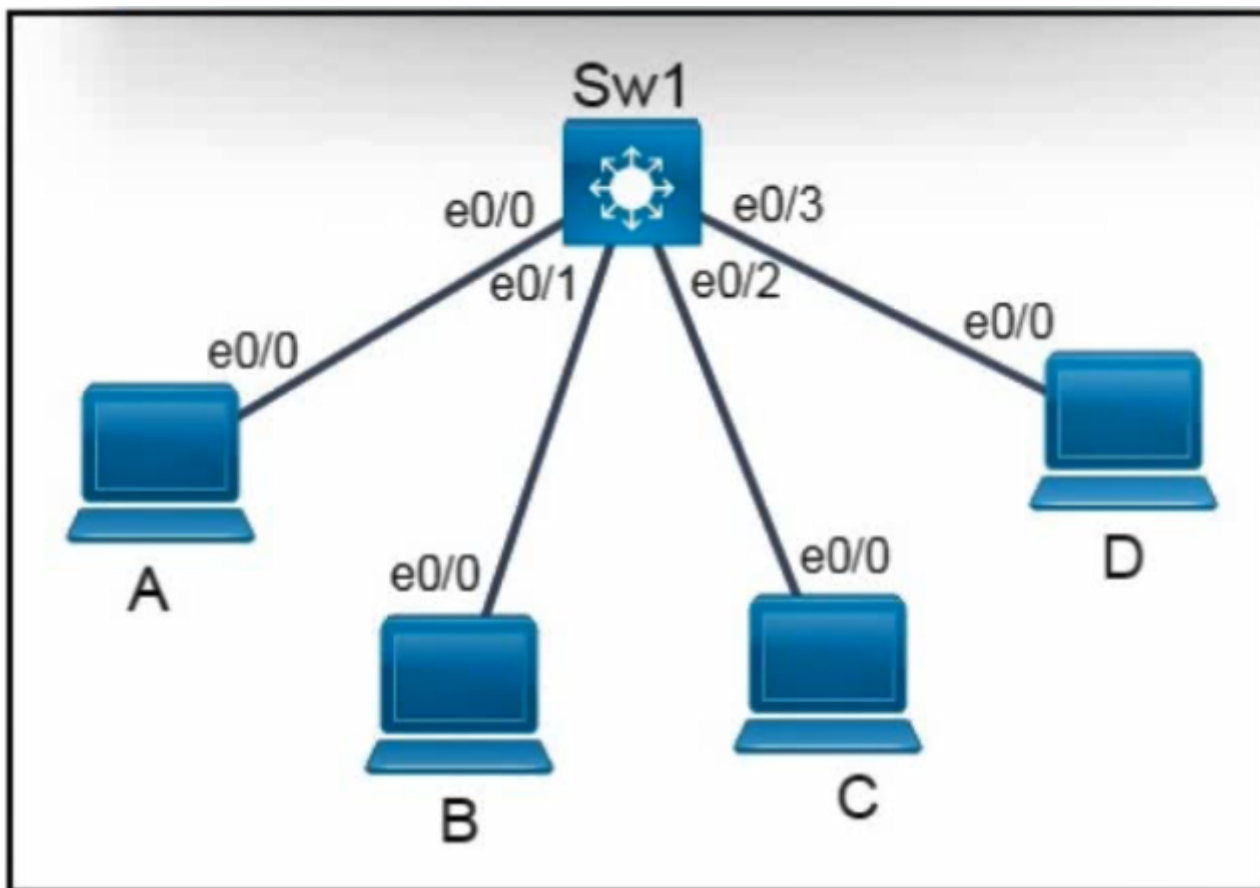
  **Ciscoman021** 5 months, 2 weeks ago

Selected Answer: C

The console connection on a Cisco Wireless LAN Controller (WLC) provides out-of-band management functionality. Therefore, the correct answer is C - "out-of-band management"
upvoted 3 times

  **ike110** 6 months, 4 weeks ago

CIMC port is used for out-of-band management, but not Console
upvoted 3 times



Refer to the exhibit. Host A switch interface is configured in VLAN 2. Host D sends a unicast packet destined for the IP address of host A.

```
Sw1#show mac-address table
Mac Address Table
```

Vlan	Mac Address	Type	Ports
2	000c.859c.bb7b	DYNAMIC	e0/1
3	000c.859c.bb7b	DYNAMIC	e0/1
2	0010.11dc.3e91	DYNAMIC	e0/2
3	0010.11dc.3e91	DYNAMIC	e0/2
2	0043.29d9.c045	DYNAMIC	e0/3

Sw1#

What does the switch do when it receives the frame from host D?

- A. It floods the frame out of every ports except the source port.
- B. It creates a broadcast storm.
- C. It shuts down the source port and places it in err-disable mode.
- D. It drops the frame from the MAC table of the switch.

Correct Answer: A

The screenshot shows the Cisco WLAN configuration page for a profile named 'lantest'. The interface includes a navigation menu at the top with options like MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK, and Home. The main content area is titled 'WLANs > Edit 'lantest'' and has tabs for General, Security, QoS, Policy-Mapping, and Advanced. The 'General' tab is active, showing the following configuration details:

- Profile Name: lantest
- Type: WLAN
- SSID: lantest
- Status: Enabled
- Security Policies: [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
- Radio Policy: All
- Interface/Interface Group(G): guest
- Multicast Vlan Feature: Enabled
- Broadcast SSID: Enabled
- NAS-ID: none

Refer to the exhibit. A Cisco engineer creates a new WLAN called lantest. Which two actions must be performed so that only high-speed 2.4-GHz clients connect? (Choose two.)

- A. Enable the Status option.
- B. Set the Radio Policy option to 802.11g Only.
- C. Set the Radio Policy option to 802.11a Only.
- D. Set the Interface/Interface Group(G) to an interface other than guest.
- E. Enable the Broadcast SSID option.

Correct Answer: AE

oatmealturkey Highly Voted 6 months, 4 weeks ago

Selected Answer: AB

Answers are A (you have to enable the WLAN for it become operational) and B
upvoted 6 times

StingVN Most Recent 3 months, 3 weeks ago

Selected Answer: BD

B and D
upvoted 1 times

VictorCisco 5 months, 2 weeks ago

Selected Answer: AB

A. enable the WLAN
B. 802.1g broadband 2.4-GHz
upvoted 3 times

Rynurr 6 months, 4 weeks ago

Selected Answer: BE

Shouldn't be "BE" cause 802.1g only supports 2.4-GHz?
upvoted 2 times

oatmealturkey 6 months, 3 weeks ago

Enable SSID Broadcast is not one of the two choices. With SSID broadcast disabled, the effect is that clients will need to know the SSID information in order to connect to the WLAN, so basically it "hides" the SSID from clients that don't know about it already. It's not relevant to

this question.
upvoted 3 times

🗨️ 👤 **Rynurr** 6 months, 3 weeks ago

You are right, AB is correct.
Status check box is MUST to enable this WLAN
upvoted 1 times

Question #838

Topic 1

How does Rapid PVST+ create a fast loop-free network topology?

- A. It uses multiple active paths between end stations.
- B. It requires multiple links between core switches.
- C. It maps multiple VLANs into the same spanning-tree instance.
- D. It generates one spanning-tree instance for each VLAN.

Correct Answer: D

🗨️ 👤 **Ciscoman021** 5 months ago

Selected Answer: D

Rapid PVST+ creates a fast loop-free network topology by generating one spanning-tree instance for each VLAN, which is option D.
upvoted 2 times

🗨️ 👤 **Dutch012** 6 months, 2 weeks ago

isn't supposed to take more time if the answer was D ?
upvoted 2 times

Question #839

Topic 1

Which two functions does a WLC perform in the lightweight access-point architecture that an AP performs independently in an autonomous architecture? (Choose two.)

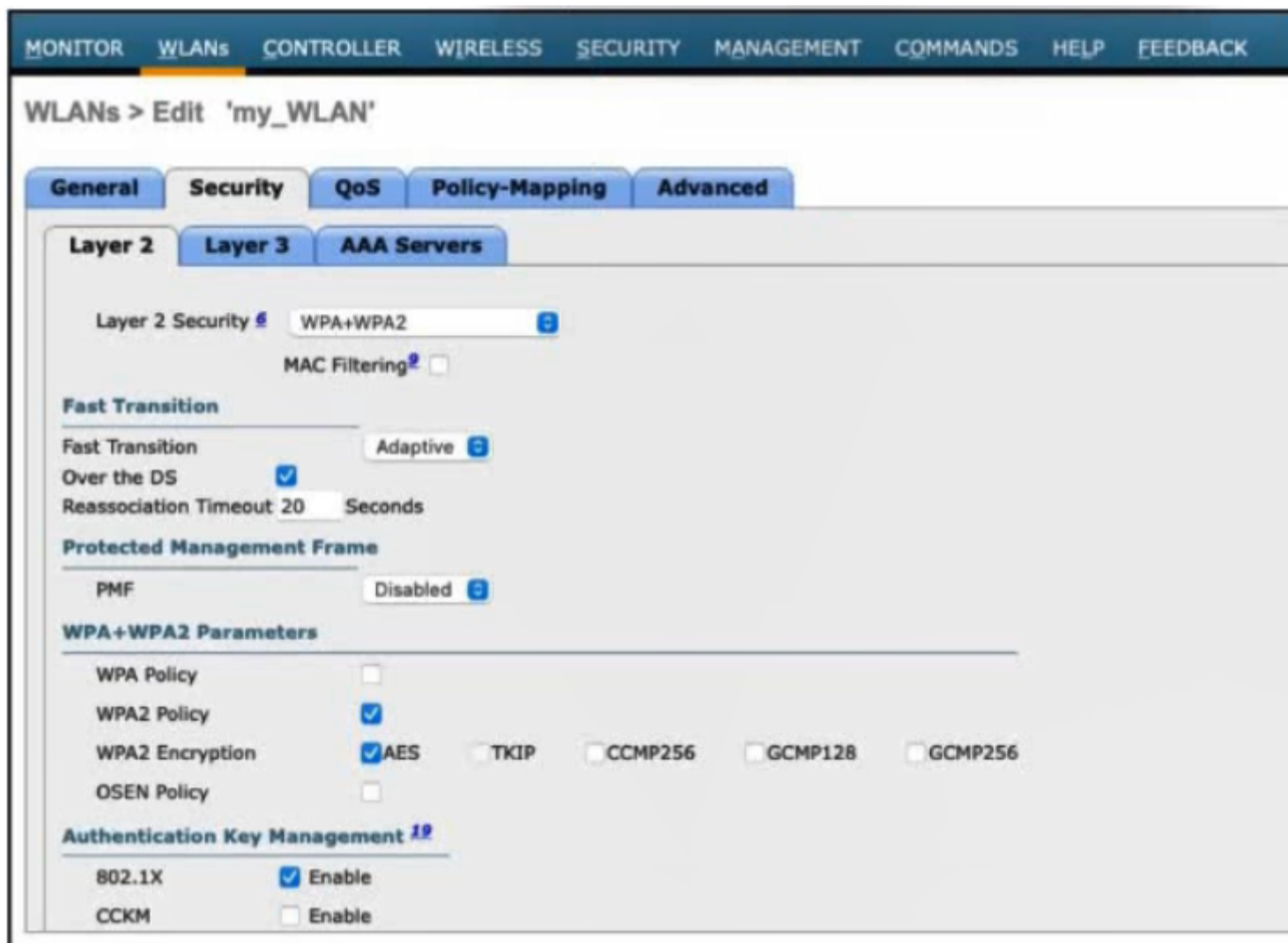
- A. managing RF channels, including transmission power
- B. handling the association, authentication, and roaming of wireless clients
- C. sending and processing beacon frames
- D. encrypting and decrypting traffic that uses the WAP protocol family
- E. preventing collisions between wireless clients on the same RF channel

Correct Answer: AB

🗨️ 👤 **studying_1** 4 months, 1 week ago

Selected Answer: AB

the answer is correct, WLC handles RF management, Security/ QOS management, client authentication, client association/ roaming management
upvoted 3 times



Refer to the exhibit. A network engineer is configuring a wireless LAN with Web Passthrough Layer 3 Web Policy. Which action must the engineer take to complete the configuration?

- A. Set the Layer 2 Security to 802.1X.
- B. Enable TKIP and CCMP256 WPA2 Encryption.
- C. Enable the WPA Policy.
- D. Set the Layer 2 Security to None.

Correct Answer: C

ike110 Highly Voted 6 months, 4 weeks ago

Selected Answer: D

Navigate to WLAN > Edit > Security > Layer2, and select None for Layer 2 Security:

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116879-configure-wlc-00.html>

upvoted 11 times

dropspablo 2 months, 3 weeks ago

Latest link: https://www.cisco.com/c/en/us/td/docs/switches/lan/Denali_16-1/ConfigExamples_Technotes/Techzone_Articles/Example_and_Technotes_Denali_16_1_1/Example_and_Technotes_Denali_16_1_1_chapter_011011.html

.html

upvoted 1 times

Rynurr Most Recent 6 months, 4 weeks ago

Selected Answer: D

"D" should be correct answer

upvoted 4 times

A network administrator plans an update to the Wi-Fi networks in multiple branch offices. Each location is configured with an SSID called "Office". The administrator wants every user who connects to the SSID at any location to have the same access level. What must be set the same on each network to meet the requirement?

- A. radio policy
- B. profile name
- C. NAS-ID configuration
- D. security policies

Correct Answer: C

 **oatmealturkey** Highly Voted 6 months, 4 weeks ago

Never heard of NAS-ID until now :O
upvoted 13 times


 **Stevens0103** Most Recent 1 month, 1 week ago

Selected Answer: B

The question was about setting the same access level for users connecting to the "Office" SSID at different locations. The NAS-ID is a way to classify users into different groups or policies on a RADIUS server based on attributes sent by the NAS, but it doesn't inherently ensure the same access level for all users connecting to the "Office" SSID across multiple locations.

A profile name in a Wi-Fi network context typically refers to a configuration profile that defines various settings for a specific SSID, including security settings, authentication methods, access policies, and other network parameters. By ensuring that the profile name is consistent across all branch offices, the administrator is effectively making sure that users connecting to the "Office" SSID will have the same access level and experience, regardless of their physical location.

upvoted 1 times

 **no_blink404** 2 months, 2 weeks ago

Selected Answer: D


Going with D, since NAS-ID configuration is not purely to do with WIFI.

NAS-ID is used to notify the source of a RADIUS access request, which enables the RADIUS server to choose a policy for that request.

upvoted 1 times

 **jonathan126** 4 months, 3 weeks ago

why B is not the answer? As long as they have the same profile name, they are under the same instance, so the access should be the same?
upvoted 1 times

 **Ciscoman021** 5 months, 3 weeks ago

Selected Answer: D

D. security policies must be set the same on each network to meet the requirement of providing every user who connects to the SSID at any location with the same access level. Security policies define the level of access granted to users on the network, including authentication, encryption, and authorization rules. By ensuring that the same security policies are applied to the SSID at all locations, the administrator can ensure that users have the same level of access, regardless of which branch office they are connecting from.

Radio policies (A) control the radio settings of the Wi-Fi network, such as channel, power, and data rates. Profile name (B) refers to the name assigned to a specific network configuration profile. NAS-ID configuration (C) is a setting used in RADIUS authentication, which is not directly related to Wi-Fi network access levels.

upvoted 1 times

 **Titan_intel** 6 months, 2 weeks ago

Not sure if the answer is C or D...
upvoted 1 times

 **JBlacc** 6 months, 2 weeks ago

Selected Answer: C

Network access server identifier (NAS-ID) is used to notify the source of a RADIUS access request, which enables the RADIUS server to choose a policy for that request. You can configure one on each WLAN profile, VLAN interface, or access point group. The NAS-ID is sent to the RADIUS server by the controller through an authentication request to classify users to different groups. This enables the RADIUS server to send a customized authentication response.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-8/config-guide/b_wl_17_8_cg/m_nas-id.pdf

upvoted 1 times

 **ike110** 6 months, 4 weeks ago

Selected Answer: D

D is the only answer that makes sense
upvoted 4 times



Refer to the exhibit. The P2P Blocking Action option is disabled on the WLC. The security team has a new requirement for each client to retain their assigned IP addressing as the clients move between locations in the campus network. Which action completes this configuration?

- A. Enable the Static IP Tunneling option.
- B. Disable the Coverage Hole Detection option.
- C. Set the P2P Blocking Action option to Forward-UpStream.
- D. Check the DHCP Addr. Assignment check box.

Correct Answer: C

ike110 Highly Voted 6 months, 4 weeks ago

Selected Answer: A

Static IP Tunneling - allows clients to travel between different WLC on the network and retain connectivity even if the static ip is in a different subnet.

<https://mrnciew.com/2013/03/25/static-ip-clients-mobility/>
upvoted 8 times

Stevens0103 Most Recent 1 month, 1 week ago

Selected Answer: A

"At times you may want to configure static IP addresses for wireless clients. When these wireless clients move about in a network, they could try associating with other controllers. If the clients try to associate with a controller that does not support the same subnet as the static IP, the clients fail to connect to the network. You can now enable dynamic tunneling of clients with static IP addresses."

"Dynamic anchoring of static IP clients with static IP addresses can be associated with other controllers where the client's subnet is supported by tunneling the traffic to another controller in the same mobility group. This feature enables you to configure your WLAN so that the network is serviced even though the clients use static IP addresses."

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010011000.html
upvoted 1 times

Stevens0103 1 month, 1 week ago

Configuring Dynamic Anchoring of Static IP Clients (GUI)
Procedure
Step 1
Choose WLANs to open the WLANs page.

Step 2
Click the ID number of the WLAN on which you want to enable dynamic anchoring of IP clients. The WLANs > Edit page is displayed.

Step 3
Choose the Advanced tab to open the WLANs > Edit (Advanced) page.


Step 4

Enable dynamic anchoring of static IP clients by selecting the "Static IP Tunneling" check box.

Step 5

Click Apply to commit your changes.

upvoted 1 times

 **Ciscoman021** 5 months, 1 week ago

Selected Answer: D

The option that completes this configuration is D. Check the DHCP Addr. Assignment check box.


By checking the DHCP Addr. Assignment check box, the WLC will retain the assigned IP address for each client as they move between locations in the campus network. This is because the WLC will act as a DHCP server and assign the same IP address to the client each time they connect to the network, based on the client's MAC address.

Enabling the Static IP Tunneling option (option A) creates a virtual private network (VPN) between two WLCs or between a WLC and another device such as a router, but it does not address the requirement of retaining the assigned IP addressing for clients as they move between locations.

Disabling the Coverage Hole Detection option (option B) is not related to the requirement of retaining the assigned IP addressing for clients.

Setting the P2P Blocking Action option to Forward-UpStream (option C) allows clients to communicate with each other directly, but it does not address the requirement of retaining the assigned IP addressing for clients as they move between locations.

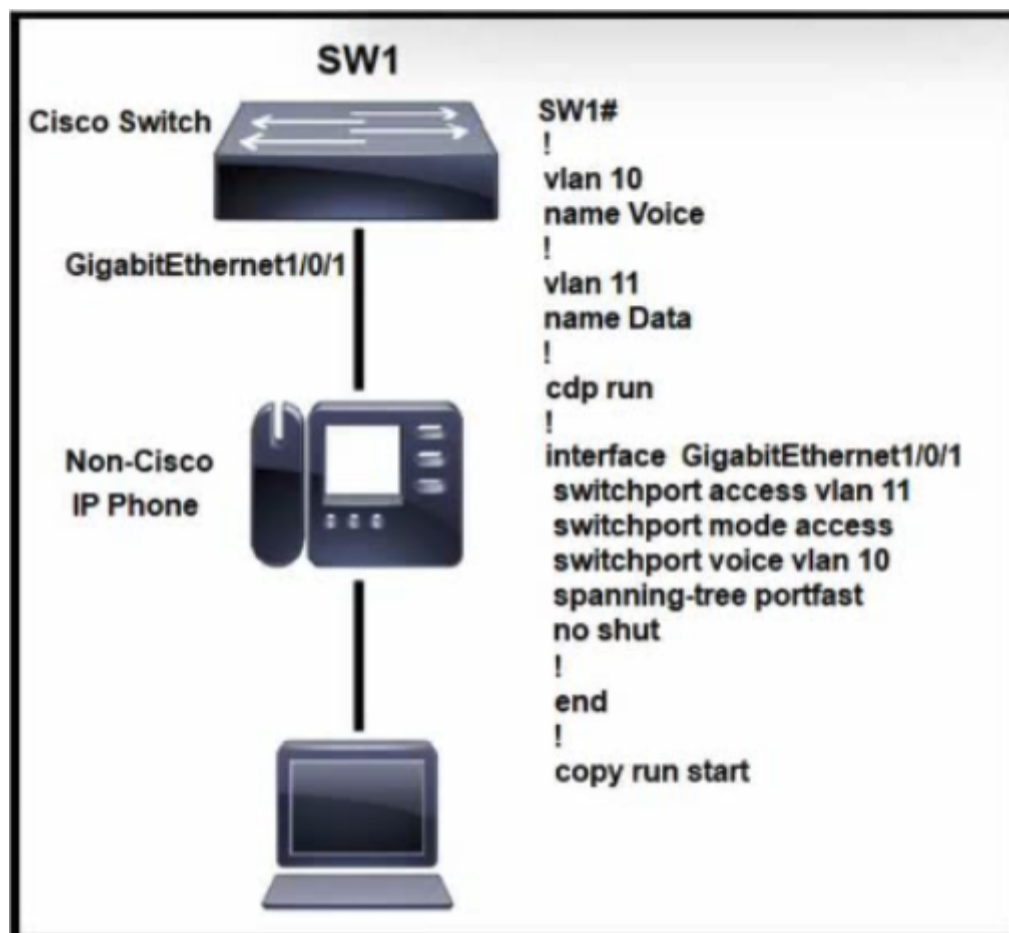
upvoted 2 times

 **JJY888** 6 months, 2 weeks ago

Selected Answer: A

<https://mrnciew.com/2013/03/25/static-ip-clients-mobility/>

upvoted 2 times



Refer to the exhibit. A multivendor network exists and the company is implementing VoIP over the network for the first time. Which configuration is needed to implement the neighbor discovery protocol on the interface and allow it to remain off for the remaining interfaces?

- A. SW1(config)#lldp run -
SW1(config)#interface gigabitethernet1/0/1
SW1(config-if)#lldp enable
- B. SW1(config)#no cdp run -
SW1(config)#interface gigabitethernet1/0/1

SW1(config-if)#lldp transmit -
SW1(config-if)#lldp receive
- C. SW1(contig)#lldp enable -
SW1(config)#interface gigabitethernet1/0/1
SW1(config-if)#lldp run
- D. SW1(config)#no cdp enable -
SW1(config)#interface gigabitethernet1/0/1
SW1(config-if)#cdp run

Correct Answer: B

no_blink404 2 months, 2 weeks ago

Selected Answer: B

Answer is B.

Can't be answer A since 'lldp enable' isn't a legitimate command.

upvoted 2 times

dropspablo 2 months, 3 weeks ago

Selected Answer: B

B is correct because the commands "SW1(config-if)#lldp transmit -

SW1(config-if)#lldp receive" enable LLDP directly on the specific interface, without needing the command "SW1(config)#lldp run" which would also work, as it enables LLDP on all interfaces.

CDP is enabled on all interfaces with the command "(config)#cdp run" and we disable or enable it only on a specific interface with "(config-if)#cdp enable" or "(config-if)#no cdp enable", but in LLDP the "lldp enable" command does not exist, because we have more options like defining "transmit" and "receive" on the interface, while CDP can only enable or disable a CDP interface with "cdp enable", that's why LLDP has more options. Correct me if I'm wrong on any point!

upvoted 2 times

perri88 3 months ago

it doesn't say it's a cisco switch, it's a 3rd party vendor. so.

The commands "lldp transmit" and "lldp receive" are used to enable or disable the transmission and reception of LLDP (Link Layer Discovery Protocol) packets on a network device.

To effectively use these commands, the LLDP feature must be enabled on the device. The specific command to enable LLDP may vary depending on the operating system or platform. However, a common command is "lldp run" or "lldp enable" to globally enable LLDP on the device.

So, to use "lldp transmit" and "lldp receive" commands, it is generally necessary to have "lldp run" or a similar command enabled on the device. This ensures that LLDP is actively running, allowing the device to transmit and receive LLDP packets and participate in the LLDP discovery process with neighboring devices.

upvoted 1 times

  **JuanluRea** 3 months ago

Selected Answer: A

<https://www.comparitech.com/net-admin/cisco-discovery-protocol/#:~:text=Can%20CDP%20and%20LLDP%20coexist,to%20interoperate%20with%20other%20vendors.>

Can CDP and LLDP coexist?

Yes. CDP and LLDP can coexist, or be used at the same time, especially if your network environment is made up of devices from different vendors. The majority of Cisco devices will also support LLDP, as this allows them to interoperate with other vendors. However, in those devices, LLDP is off by default.



I think A is correct because LLDP will not work without "lldp run" command.

upvoted 1 times

  **dropspablo** 2 months, 3 weeks ago

Command "lldp enable" does not exist!

upvoted 2 times

  **pikos1** 3 months, 3 weeks ago

In "B" answer is missing "lldp run" command.... without that command lldp will not work

upvoted 3 times

  **MassNasty1** 3 months, 3 weeks ago

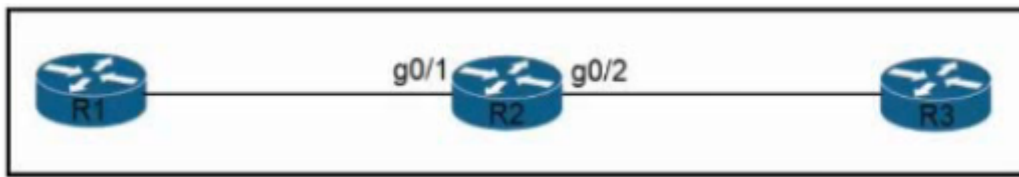
B should be correct. CDP is a Cisco's Proprietary Layer 2 Neighbor Discovery Protocol; it should be disabled in the global configuration mode and would not work in a multivendor environment. LLDP is the vendor neutral, IEEE 802.1AB standard protocol for Layer 2 Neighbor Discovery that Cisco switches generally support. CDP is enabled by default on Cisco Switches and must be disabled globally. Answer B is correct.

upvoted 1 times

  **ac89l** 4 months ago

can anyone confirm this?

upvoted 1 times



Refer to the exhibit. Routers R1, R2, and R3 use a protocol to identify the neighbors' IP addresses, hardware platforms, and software versions. A network engineer must configure R2 to avoid sharing any neighbor information with R3, and maintain its relationship with R1. What action meets this requirement?

- A. Configure the `no lldp receive` command on g0/1.
- B. Configure the `no cdp run` command globally.
- C. Configure the `no cdp enable` command on g0/2.
- D. Configure the `no lldp run` command globally.

Correct Answer: D

- purenuker** Highly Voted 6 months, 2 weeks ago
 Examtopics , please correct your answers , we are paying our money to receive false answers !!!!! And may be somebody will be dropped off the exam because of your answers !!!!!!!
 upvoted 31 times
- beerbisceps1** 5 months, 2 weeks ago
 I agree!!!!
 upvoted 4 times
- davidmdl85** Most Recent 1 month ago
 Because they dont specify and we're doing a cisco exam, ill assume that all the routers are cisco, so the answer is C and not A
 upvoted 1 times
- Brocolee** 1 month, 3 weeks ago
 Can anyone explain why not A? Does the questions referring to Cisco environment or multi-vendor network somewhere? What did I miss?
 upvoted 1 times
- omikun** 4 months, 2 weeks ago
 Admin .please correct your answers.
 there are lot of answer need to be corrected.
 We are not paying for getting the false information.
 It will destroy someone's career.
 upvoted 4 times
- zamkljo** 5 months, 2 weeks ago
Selected Answer: C
 C. Configure the `no cdp enable` command on g0/2
 upvoted 2 times
- Ciscoman021** 5 months, 4 weeks ago
Selected Answer: C
 my answer is C. please update the correct answer examtopic.
 upvoted 2 times
- tal10** 6 months, 3 weeks ago
Selected Answer: C
 We need a relationship with router 1
 upvoted 2 times
- Rynurr** 6 months, 4 weeks ago
Selected Answer: C
 "C" is the correct answer, casue we still need maintain a relationship with R1
 upvoted 4 times
- gewe** 7 months ago
 my choice is C also
 upvoted 1 times

  **oatmealturkey** 7 months ago

Selected Answer: C

Configuring no lldp run, assuming the routers are using LLDP, will mean that R1 and R2 don't maintain a relationship, so that answer is incorrect. C is the correct answer

upvoted 2 times

Question #845

Topic 1

SIP-based Call Admission Control must be configured in the Cisco WLC GUI. SIP call-snooping ports are configured. Which two actions must be completed next? (Choose two.)

- A. Set the QoS level to silver or greater for voice traffic.
- B. Configure two different QoS roles for data and voice traffic.
- C. Enable Media Session Snooping on the WLAN.
- D. Set the QoS level to platinum for voice traffic.
- E. Enable traffic shaping for the LAN interface of the WLC.



Correct Answer: BD

  **oatmealturkey** **Highly Voted**  7 months ago

Selected Answer: CD

B is incorrect, we already set the QoS level to platinum for voice traffic and for this question nothing needs to be done for data traffic. The correct answers are C and D, the question literally references the call-snooping ports but you still have to enable snooping

upvoted 11 times

  **4bed5ff** 2 months, 3 weeks ago

Agreed: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/wireless_quality_of_service.html#:~:text=Ensure%20that%20you%20have%20enabled%20call%20snooping%20for%20the%20WLAN

upvoted 2 times

  **[Removed]** **Most Recent**  2 months, 2 weeks ago

One more not CCNA 200-301 related question...

upvoted 3 times

```

Cat9300-1# show interface g1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 321 (VLAN0321)
Administrative Native VLAN tagging: enabled
Trunking VLANs Enabled: 100,200,300
Pruning VLANs Enabled: 2-1001

```

Refer to the exhibit. A network administrator configures an interface on a new switch so that it connects to interface Gi1/0/1 on switch Cat9300-1. Which configuration must be applied to the new interface?

- A. switchport mode trunk
switchport trunk native vlan 321
switchport trunk allowed vlan 100,200,300
- B. switchport mode dynamic desirable
switchport trunk native vlan 321
switchport trunk allowed vian 100,200,300
- C. switchport trunk encapsulation dot1q
switchport trunk native vlan 321
switchport trunk allowed vlan 100-300
- D. switchport nonegotiate
switchport access vlan 321
switchport trunk allowed vlan except 2-1001

Correct Answer: B

 **oatmealturkey** Highly Voted 7 months ago

Selected Answer: A

Why B? The switch port in the exhibit was configured with "switchport mode trunk", as can be seen by Administrative Mode: trunk. So why not do same configuration on the new switch? Also I believe Cisco recommends statically configuring trunks and not using DTP for security reasons
upvoted 13 times

 **AndreaGambera** Most Recent 2 weeks, 6 days ago

A is Correct !!! 100%


upvoted 1 times

 **NetworkGeek00** 1 month, 1 week ago

Selected Answer: A

A is the correct one

upvoted 1 times

 **dropspablo** 2 months, 3 weeks ago

Selected Answer: A

I choose the letter A. The trunk negotiation is enabled, however as we have "Switchport Mode Trunk", static mode configured, for best practices I believe that keeping the trunk statically on the other side would be more adequate and consistent. For example, a technician could disable negotiation on the static side by mistake (with "switchport nonegotiate") and the other side with dynamic negotiation would lose trunk mode negotiation. Therefore, I believe that static mode would be better with static mode (On/On) or dynamic mode with dynamic (Desirable/Auto) would also be best.

upvoted 1 times

 **nzjobhunt** 4 months, 2 weeks ago



A is correct

upvoted 1 times

 **Peter_panda** 4 months, 3 weeks ago

A and B are both correct. Negotiation of trunking is on, so the trunk will form for trunk, dynamic auto or dynamic desirable option set on the other end of the link. Anyway, I would probably choose answer B at the exam (but I hope that the question at the exam is more clear)

upvoted 1 times

  **Ciscoman021** 5 months, 4 weeks ago

Selected Answer: A

Administrative Mode: Trunk


Operational Mode: Trunk

it means interface Gi1/0/1 is Trunk without any protocols.

why Dynamic Desirable?

A is right.

upvoted 2 times

  **Rynurr** 6 months, 4 weeks ago

Selected Answer: A

Should be "A", other options doesn't make sense.

upvoted 3 times

Question #847

Topic 1

Which command enables HTTP access to the Cisco WLC?

- A. config network telnet enable
- B. config network secureweb enable
- C. config certificate generate webadmin
- D. config network webmode enable

Correct Answer: D

  **dropspablo** 2 months, 3 weeks ago

Answer D correct.

Interesting ChatGPT response:

B. config network secureweb enable

This command enables secure web access (HTTPS) to the Cisco WLC. By default, the WLC only allows HTTPS access for added security. However, if you specifically want to enable unsecured HTTP access, you can use the following command:

D. config network webmode enable

Importantly, using unsecured HTTP access is generally not recommended due to security risks. It is advisable to use HTTPS whenever possible to ensure data confidentiality and integrity.

upvoted 1 times

  **huykg009** 4 months, 4 weeks ago

Selected Answer: D

D is correct:

have configuration AP 1852I and this command is correct.

upvoted 1 times

  **Goena** 6 months, 2 weeks ago

Selected Answer: D

D is correct:

To access GUI over browser, webmode must be enable on WLC. By default it is disabled. You can enable it with below command on CLI:

config network webmode enable

upvoted 4 times

Which port state processes BPDUs, but does not forward packets or update the address database in Rapid PVST+?

- A. blocking
- B. learning
- C. listening
- D. disabled

Correct Answer: A

 **Mariachi** Highly Voted 5 months, 3 weeks ago

Selected Answer: B

out of available options ... Learning seems to be the most correct.

Blocking state is not available with RPVST+.

upvoted 9 times

 **dropspablo** 1 month, 1 week ago

I agree. Regarding the learning and blocking states, both process BPDUs, but do not update the MAC address table and do not forward packets. The key issue is that rapid-pvst does not use the blocking state (old STP), but DISCARDIND STATE, as it does not have this option, it only remains the letter B. "learning".

upvoted 1 times

 **purenuker** Highly Voted 6 months, 2 weeks ago

<https://www.ii.pwr.edu.pl/~kano/course/module4/4.2.3.1/4.2.3.1.html>

"RSTP does not have a blocking port state. RSTP defines port states as discarding, learning, or forwarding."

WTF !?!?!

upvoted 7 times

 **Stevens0103** Most Recent 1 month, 1 week ago

Selected Answer: A

Configuring Rapid PVST+

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n1_1/Cisco_n5k_layer2_config_gd_rel_503_N1_1_chapter9.html#con_1241802

Blocking State

A LAN port in the blocking state does not participate in frame forwarding.

A LAN port in the blocking state performs as follows:

Discards frames received from the attached segment.

Discards frames switched from another port for forwarding.

Does not incorporate the end station location into its address database. (There is no learning on a blocking LAN port, so there is no address database update.)

Receives BPDUs and directs them to the system module.

Receives, processes, and transmits BPDUs received from the system module.

Receives and responds to network management messages.

upvoted 3 times

 **ahmadawni** 1 month, 3 weeks ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n1_1/Cisco_n5k_layer2_config_gd_rel_503_N1_1_chapter9.html#con_1241757:~:text=Port%20States-,Rapid%20PVST%2B%20Port%20State%20Overview,-Propagation%20delays%20can

upvoted 1 times

 **Shabeth** 2 months, 2 weeks ago

Selected Answer: B

B. Blocking

upvoted 1 times


  **Shabeth** 2 months, 2 weeks ago

i meant A. Blocking
upvoted 1 times

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: B

B - Learning
upvoted 1 times

  **no_blink404** 2 months, 2 weeks ago

Selected Answer: A

The answer is A. Do not be misled. Read the official Cisco documentation:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n1_1/Cisco_n5k_layer2_config_gd_rel_503_N1_1_chapter9.html

upvoted 2 times

  **[Removed]** 2 months, 2 weeks ago

No i can't be A since Blocking is not a RSTP state. The three RSTP states are : Discarding, Learning and Forwarding
upvoted 2 times

  **perri88** 3 months ago

Selected Answer: B

"RSTP does not have a blocking port state. RSTP defines port states as discarding, learning, or forwarding."

upvoted 3 times

  **DMc** 3 months, 2 weeks ago

A - 100% as per Cisco

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n1_1/Cisco_n5k_layer2_config_gd_rel_503_N1_1_chapter9.html

Blocking State

A LAN port in the blocking state does not participate in frame forwarding.

A LAN port in the blocking state performs as follows:

Discards frames received from the attached segment.

Discards frames switched from another port for forwarding.

Does not incorporate the end station location into its address database. (There is no learning on a blocking LAN port, so there is no address database update.)

Receives BPDUs and directs them to the system module.

Receives, processes, and transmits BPDUs received from the system module.

Receives and responds to network management messages.

upvoted 4 times

  **Shri_Fcb10** 3 months, 3 weeks ago

Seems like A and B both are right, correct me if I a wrong.

https://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli_rel_4_1/Cisco_Nexus_5000_Series_Switch_CLI_Software_Configuration_Guide_chapter11.pdf

Read out page 12 on the above PDF

upvoted 1 times

  **Friday_Night** 3 months, 3 weeks ago

I'll go for listening.....C

it's not blocking because it processes BPDUs but cannot update the address database

so it can't be learning either.

upvoted 1 times

  **MassNastty1** 3 months, 3 weeks ago

Uhhhh, Rapid PVST+ definitely has a blocking port state, which doesn't forward anything it receives or update the address database....

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/521_n1_1/b_Nexus_5000_Layer2_Config_521N1.html#con_1205207

The answer is blocking state.

upvoted 1 times

  **[Removed]** 2 months, 2 weeks ago

No it doesn't. In RSTP the Disabled, Blocking and Listening states (STP) are merged into the Discarding state.

upvoted 1 times

  **VicM** 4 months ago

C: listening

upvoted 1 times

  **studying_1** 3 months, 2 weeks ago

it's rapid pvst+, there isn't a listening state, only discarding, learning & forwarding

upvoted 3 times

🗨️ 👤 **omikun** 4 months, 2 weeks ago

The port state that processes BPDUs, but does not forward packets or update the address database in Rapid PVST+ is:

C. Listening

The Listening state is the first state in the Rapid PVST+ port states, where a port listens for BPDUs from the root bridge and prepares to move to the Learning state. During this state, the switch processes BPDUs to determine the location and identity of the root bridge, but does not forward packets or update the address database. Once the Listening state expires, the port moves to the Learning state.

upvoted 2 times

🗨️ 👤 **studying_1** 3 months, 2 weeks ago

it's rapid pvst+, there isn't a listening state, only discarding, learning & forwarding

upvoted 2 times

🗨️ 👤 **Njavwa** 5 months ago

RSTP does not have a blocking port state. RSTP defines port states as discarding, learning, or forwarding.

im thinking this can be error with the phrasing, in the discarding state the port discards all BPDU,

in the learning mode it will receive BPDU and also processes them as to prepares to send them to the system module and also ncorporates the end station location into its address database.

forwarding shouldn't even cross your mind on this question

upvoted 1 times

🗨️ 👤 **krzysiew** 5 months, 2 weeks ago

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/b_Cisco_Nexus_5000_Series_NX-OS/Cisco_Nexus_5000_Series_NX-OS__chapter9.pdf

upvoted 1 times

🗨️ 👤 **krzysiew** 5 months, 2 weeks ago

Selected Answer: A

difference between Blocking <-> Learning

Blocking State:

Does not incorporate the end station location into its address database. (There is no learning on a blocking LAN port, so there is no address database update.)

upvoted 2 times

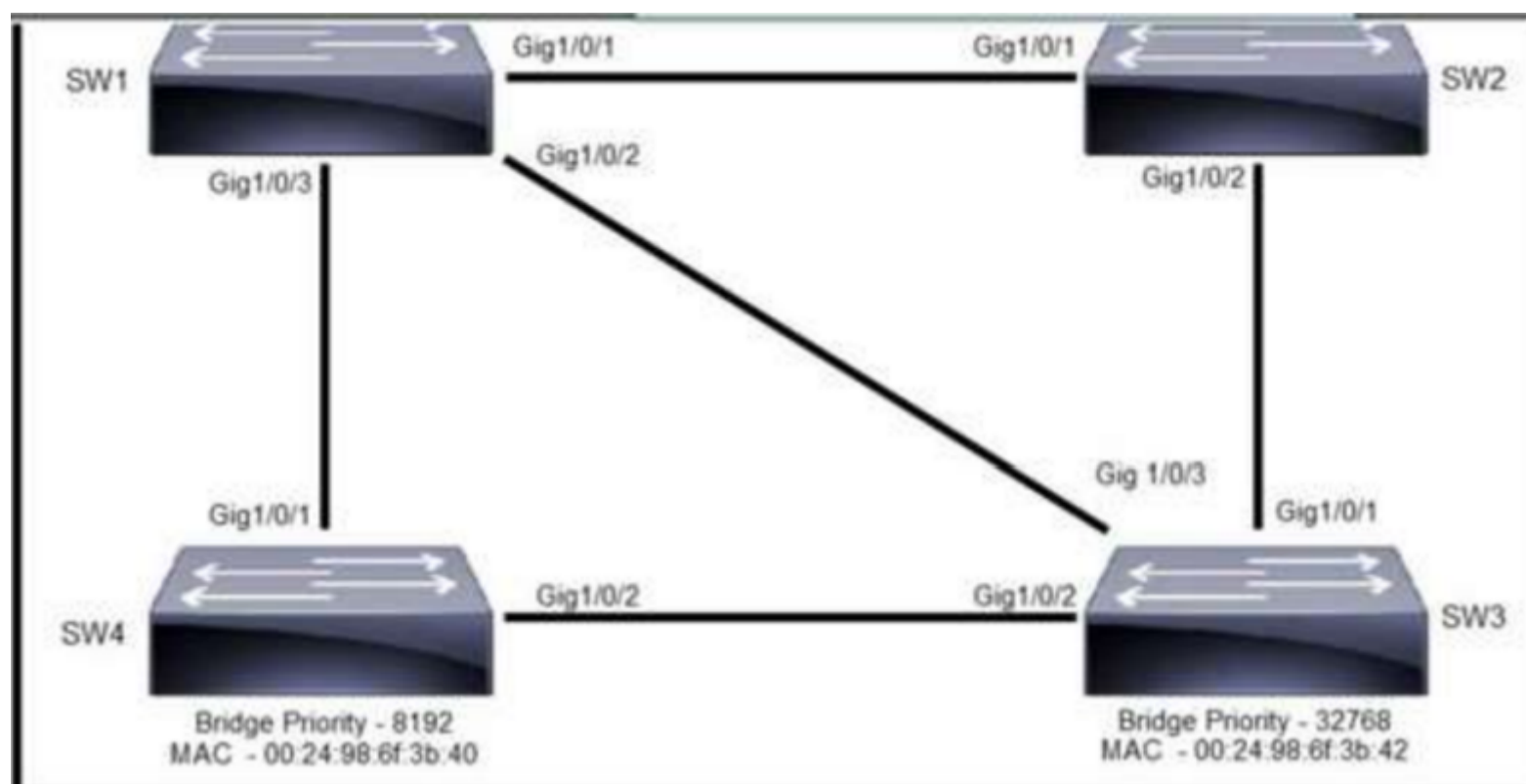
Question #849

Topic 1

A switch is forwarding a frame out of all interfaces except the interface that received the frame. What is the technical term for this process?

- A. ARP
- B. CDP
- C. flooding
- D. multicast

Correct Answer: C



Refer to the exhibit. Rapid PVST+ mode is on the same VLAN on each switch. Which switch becomes the root bridge and why?

- A. SW4, because its priority is highest and its MAC address is lower
- B. SW1, because its priority is the lowest and its MAC address is higher
- C. SW2, because its MAC address is the highest
- D. SW3, because its priority is the highest

Correct Answer: C

oatmealturkey (Highly Voted) 7 months ago

This diagram is cut off at the top, right? The given answer is wrong because a switch does not become the root bridge by having the highest MAC address. First criterion is the switch with the lowest priority will become the root bridge, but if all switches have the same priority then the switch with the lowest MAC will become the root bridge
upvoted 20 times

tal10 (Highly Voted) 6 months, 3 weeks ago

WRONG ANSWER
upvoted 7 times

mda2h (Most Recent) 1 month, 2 weeks ago

Selected Answer: A

Tricky question! Do not confuse highest priority with highest priority value!
A high STP priority = the lowest priority value in the BID.
upvoted 2 times

dropspablo 1 month, 1 week ago

It's true, now I understand!
upvoted 1 times

Shri_Fcb10 1 month, 3 weeks ago

Man I regret paying for this website
upvoted 2 times

perri88 3 months ago

Selected Answer: B

in STP the criteria with lowest(1.priority then 2.MAC address) wins
upvoted 2 times


Friday_Night 3 months, 3 weeks ago

in STP the criteria with lowest(1.priority then 2.MAC address) wins
SW1 and SW2 has no details though...
upvoted 3 times

sany11 4 months, 3 weeks ago

Switch 4 is the ANSWER!



upvoted 2 times

  **Simon_1103** 5 months, 1 week ago

Selected Answer: A

A. SW4, because its priority is highest and its MAC address is lower

upvoted 3 times

  **zamljo** 5 months, 2 weeks ago

Selected Answer: B

Lowest priority then lowest MAC

upvoted 2 times

  **kapel21** 6 months, 1 week ago

To determine which switch becomes the root bridge in a Rapid PVST+ network, the switch with the lowest bridge ID is selected as the root bridge. The bridge ID is a combination of the priority value and the switch MAC address. The priority value is a 4-bit value that can be set in increments of 4096, with the default value being 32768.

In the exhibit, the switch priority values are not explicitly shown, so we must assume that the default value of 32768 is being used. The bridge ID of each switch is:

SW1: Priority 32768, MAC address 001c.c4b6.4f80, Bridge ID 32768.001c.c4b6.4f80

SW2: Priority 32768, MAC address 001c.c4d6.b680, Bridge ID 32768.001c.c4d6.b680

SW3: Priority 32768, MAC address 001c.c4b6.e300, Bridge ID 32768.001c.c4b6.e300

SW4: Priority 4096, MAC address 000e.0c6f.9c00, Bridge ID 4096.000e.0c6f.9c00

Since SW4 has the lowest bridge ID, it becomes the root bridge.

Therefore, the correct answer is A. SW4, because its priority is the highest and its MAC address is lower.

upvoted 5 times

Which EtherChannel mode must be configured when using LAG on a WLC?

- A. on
- B. passive
- C. active
- D. auto

Correct Answer: A

 **Jcrazybaby** 6 days, 21 hours ago

Answer is C
upvoted 1 times

 **VarDav** 3 weeks, 6 days ago

Selected Answer: A

'mode on' is required
upvoted 1 times

 **shaney67** 1 month ago

C. active

When configuring Link Aggregation Groups (LAG) on a Wireless LAN Controller (WLC), the "active" mode should be used for the EtherChannel. This mode is also known as "LACP active mode" (Link Aggregation Control Protocol active mode). LACP is a protocol used to dynamically negotiate and manage the creation of Link Aggregation Groups.

In an active LACP configuration, the WLC actively initiates the negotiation process and forms an EtherChannel with the connected switch. This helps ensure that the configuration is consistent on both ends of the link.

Options A, B, and D are not the recommended modes for configuring LAG with LACP on a WLC.
upvoted 2 times

 **krzysiew** 5 months, 2 weeks ago

Selected Answer: A

LAG requires the EtherChannel to be configured for 'mode on' on both the controller and the Catalyst switch.
upvoted 4 times


DRAG DROP


Drag and drop the VLAN port modes from the left onto the descriptions on the right.

dynamic access	allows the port to belong to one VLAN when manually configured
private	allows the port to be assigned automatically to one VLAN
static access	allows the port to belong to one or more VLANs
trunk	allows the port to support a single VLAN across a service-provider network
tunnel	allows the port to communicate with others within the same community VLAN

Correct Answer:

dynamic access	static access
private	dynamic access
static access	trunk
trunk	tunnel
tunnel	private

 **mda2h** 1 month, 2 weeks ago
correct
upvoted 1 times

 **Shabeth** 2 months, 2 weeks ago
answers are correct
upvoted 1 times

Which switch concept is used to create separate broadcast domains?

- A. STP
- B. VTP
- C. VLAN
- D. CSMA/CD

Correct Answer: C

How must a switch interface be configured when an AP is in FlexConnect mode?

- A. access port
- B. EtherChannel
- C. PoE port
- D. trunk port

Correct Answer: A

🗨️ **Kerrera** 2 months, 1 week ago

Selected Answer: D

It is useful for double connection, wired and wireless, for example Chromecast, one vlan for cable and another for wifi, allowed as a trunk in the switch

upvoted 1 times

🗨️ **fmaquino** 3 months, 1 week ago

Selected Answer: D

Trunk port

upvoted 1 times

🗨️ **lolungos** 3 months, 2 weeks ago

Selected Answer: D

Trunk. Since it puts the traffict directly on the switch in flexconnect mode it and it supports multiple vlans it needs to put it on the proper vlan.

Source - I'm a CWNP

upvoted 3 times

🗨️ **ac89l** 4 months ago

Selected Answer: D

D

according to chatGPT

upvoted 1 times

🗨️ **fmaquino** 4 months ago

Selected Answer: D

Should be D

upvoted 1 times

🗨️ **Lokylax** 4 months ago

Not sure this is the good answer as an autonomous AP needs a trunk port.

In this cisco documentation the FlexConnect AP is connected to a trunk port : https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html#18116

upvoted 2 times

🗨️ **learntstuff** 1 month, 4 weeks ago

If you follow this link and read right above the config section. It will say you can use a switch port OR a trunk port. they say they just happen to use a trunk port in that config. so technically both switch and trunk are correct.

upvoted 1 times

What are two features of PortFast? (Choose two.)

- A. Convergence is fast after a link failure.
- B. STP loops are mitigated for uplinks to other switches.
- C. Ports transition directly from the blocking state to the forwarding state.
- D. Ports operate normally without receiving BPDUs.
- E. Ports that connect to the backbone automatically detect indirect link failures.

Correct Answer: BC

  **dropspablo** 3 weeks ago

Selected Answer: AD

Letter D is correct. Ports with PortFast DO NOT operate normally when receiving BPDUs. "They operate normally WITHOUT receiving BPDUs". If the port receive any STP BPDU, it will revert to normal/regular mode and participate in listening and learning states. (letter A and D is correct).
https://www.arubanetworks.com/techdocs/ArubaOS_80_Web_Help/Content/ArubaFrameStyles/Network_Parameters/Portfast%20and%20BPDU%20Guard.htm#:~:text=If%20the%20port%20receives%20any%20STP%20BPDU%2C%20it%20moves%20back%20to%20normal/regular%20mode%20and%20will%20participate%20in%20the%20listening%20and%20learning%20states.

upvoted 1 times

  **dropspablo** 3 weeks ago

Letter C is wrong because I believe that when a port is in blocking state it is probably participating in the STP topology, thus receiving BPDUs, in this case as seen in the link, the PortFst feature is disabled when receiving BPDUs, so letter C is wrong. I also believe that in some questions you mention that with PortFast enabled on the interfaces, loops and storms can occur, but if I am right, this would only happen if all the other ports in the STP topology would also have PortFast enabled, in this case as there would be none BPDU on the network, so just in this case STP would not be enabled (keeping PortFast), just then loops and broadcast storms would occur.

upvoted 1 times

  **Da_Costa** 3 weeks, 5 days ago

Selected Answer: BC

No more explanation

upvoted 1 times

  **davidmdl85** 1 month ago

A and C should be correct

<https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKQwEAO/advanced-stp-features-portfast-bpdu-guard-and-bpdu-filter>

upvoted 1 times

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

  **no_blink404** 2 months, 2 weeks ago

You CAN receive a BPDU on a portfast interface, that's why you usually enable BPDU guard with PortFast. For that reason A & C are the best answers

upvoted 1 times

  **perri88** 3 months ago

Selected Answer: CD

C AND D

upvoted 1 times

  **ac89l** 4 months ago

Selected Answer: AD

D- correct. source:

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

upvoted 2 times

  **[Removed]** 2 months, 2 weeks ago

D is not correct.

"Even though PortFast is enabled, the interface will still listen for BPDUs. Unexpected BPDUs might be accidental, or part of an unauthorized attempt to add a switch to the network." (Cisco NetAcad)

upvoted 1 times

  **ac89l** 4 months, 1 week ago

The discussion is about ACD

A -IMHO is correct

C- There is no Blocking state in portfast (misleading answer)

D- correct. source:

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

upvoted 1 times

  **jonathan126** 4 months, 3 weeks ago

Selected Answer: CD

A - uplinkfast

B - loop guard

C - portfast

D - portfast (port is connected to end device, so no BPDU from the end device to the port)

E - backbonefast

Answers: C and D

upvoted 2 times

  **ac89l** 4 months, 1 week ago

Why C is correct ? there is no Blocking State in PortFast.

upvoted 1 times


  **chuckwu7777** 3 months, 3 weeks ago

When the switch powers up, or when a device is connected to a port, the port enters the spanning tree listening state. When the Forward Delay timer expires, the port enters the learning state. When the Forward Delay timer expires a second time, the port is transitioned to the forwarding or blocking state.

When you enable PortFast on a switch or trunk port, the port is immediately transitioned to the spanning tree forwarding state.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp_enha.html#wp1046787

upvoted 1 times

  **zamkljo** 5 months, 2 weeks ago

Selected Answer: AC

A,C are the answers.

upvoted 3 times



  **Dutch012** 6 months, 1 week ago

Selected Answer: CD

regarding D: "PortFast-configured interfaces do not receive BPDUs. If a PortFast-configured interface receives a BPDU, an invalid configuration exists."

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

upvoted 2 times

  **Dutch012** 6 months, 1 week ago

regarding D: "PortFast-configured interfaces do not receive BPDUs. If a PortFast-configured interface receives a BPDU, an invalid configuration exists."

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

upvoted 1 times

  **perri88** 3 months ago

PORTS OPERATE NORMALLY WITHOUT RECEIVING BPDUS" THAT'S CORRECT, BECAUSE WHEN THEY DO RECEIVE BPDU THEY DON'T OPERATE NORMALLY AND YOU WILL SEE ERRORS

upvoted 1 times

  **dropspablo** 3 weeks ago

Correcting, the letter D is correct, as if the port receives any STP BPDU, it will revert to normal/regular mode and participate in listening and learning states. (letter A and D is correct).

-----//-----

https://www.arubanetworks.com/techdocs/ArubaOS_80_Web_Help/Content/ArubaFrameStyles/Network_Parameters/Portfast%20and%20BPDUGuard.htm#:~:text=If%20the%20port%20receives%20any%20STP%20BPDU%2C%20it%20moves%20back%20to%20normal/regular%20mode%20and%20will%20participate%20in%20the%20listening%20and%20learning%20states.

upvoted 1 times

  **dropspablo** 2 months, 3 weeks ago

But PortFast's two features are being asked. I believe that the letter D is not a resource.

upvoted 1 times

  **dropspablo** 3 weeks ago

Disregard my answer. I believe letter A and D is correct!



upvoted 1 times

  **Brianhealey136** 6 months, 3 weeks ago



Selected Answer: AC

This is A, and C

upvoted 1 times

  **ukguy** 6 months, 3 weeks ago

AC right answers
upvoted 1 times

  **Rynurr** 6 months, 4 weeks ago

Selected Answer: AC

I agree with oatmealturkey. Should be "AC"
upvoted 2 times

  **oatmealturkey** 7 months ago

Selected Answer: AC

PortFast does not mitigate loops, that is not its function or purpose. In fact if you configure PortFast on a trunk port/uplink port, you are at greater risk of loops which is why it is only supposed to be configured on access ports
upvoted 3 times

Question #856

Topic 1

What is the root port in STP?

- A. It is the port with the highest priority toward the root bridge.
- B. It is the port on the root switch that leads to the designated port on another switch.
- C. It is the port that is elected only when the root bridge has precisely one port on a single LAN segment.
- D. It is the port on a switch with the lowest cost to reach the root bridge.

Correct Answer: D

  **[Removed]** 2 months, 1 week ago

Selected Answer: D

D. It is the port on a switch with the lowest cost to reach the root bridge.
upvoted 1 times

  **fmaquino** 4 months ago

Selected Answer: D

D is correct
upvoted 3 times

Question #857

Topic 1

When a switch receives a frame from an unknown source MAC address, which action does the switch take with the frame?

- A. It sends the frame to ports within the CAM table identified with an unknown source MAC address.
- B. It floods the frame out all interfaces, including the interface it was received on.
- C. It associates the source MAC address with the LAN port on which it was received and saves it to the MAC address table.
- D. It attempts to send the frame back to the source to ensure that the source MAC address is still available for transmissions.

Correct Answer: C

When the LAG configuration is updated on a Cisco WLC, which additional task must be performed when changes are complete?

- A. Reboot the WLC.
- B. Flush all MAC addresses from the WLC.
- C. Re-enable the WLC interfaces.
- D. Re-associate the WLC with the access point.

Correct Answer: A

 **dropspablo** 2 months, 3 weeks ago

Selected Answer: A

When you enable LAG or make any changes to the LAG configuration, you must immediately reboot the controller.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/config-guide/b_cg82/b_cg82_chapter_010101011.html#:~:text=When%20you%20enable%20LAG%20or%20make%20any%20changes%20to%20the%20LAG%20configuration%2C%20you%20must%20immediately%20reboot%20the%20controller.


upvoted 1 times

 **LeonardoMeCabrio** 3 months, 1 week ago

Selected Answer: A

A is the correct answer

upvoted 1 times

 **krzysiew** 5 months, 2 weeks ago

Selected Answer: A

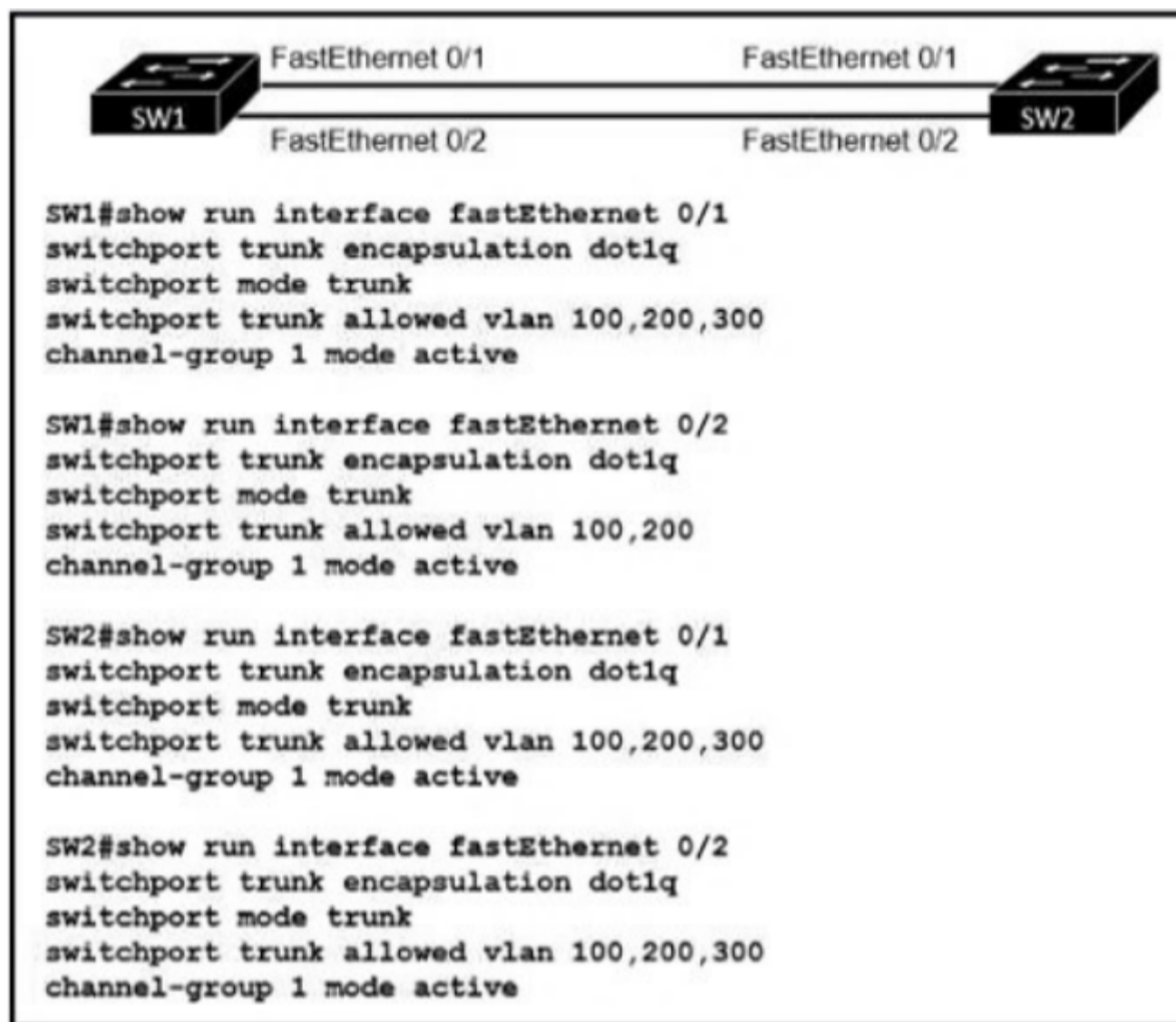
When you enable LAG or make any changes to the LAG configuration, you must immediately reboot the controller.

upvoted 4 times

 **VictorCisco** 5 months, 2 weeks ago

is it really needed to reboot WLC?

upvoted 1 times



Refer to the exhibit. An engineer is building a new Layer 2 LACP EtherChannel between SW1 and SW2, and they executed the given show commands to verify the work. Which additional task must be performed so that the switches successfully bundle the second member in the LACP port-channel?

- A. Configure the switchport trunk allowed vlan 300 command on SW1 port-channel 1.
- B. Configure the switchport trunk allowed vlan add 300 command on interface Fa0/2 on SW2.
- C. Configure the switchport trunk allowed vlan add 300 command on SW1 port-channel 1.
- D. Configure the switchport trunk allowed vlan 300 command on interface Fa0/2 on SW1.

Correct Answer: D

oatmealturkey Highly Voted 7 months ago

Selected Answer: C

Wrong, if we do switchport trunk allowed vlan 300 that replaces the previous allowed vlans so they are no longer allowed. You have to "add" vlan 300

upvoted 9 times

molly_zheng Most Recent 4 months ago

Selected Answer: C

C is correct

upvoted 2 times

ac89l 4 months ago

Selected Answer: C

You always update the information within the Portchannel information..

upvoted 2 times

Rynurr 6 months, 4 weeks ago

Selected Answer: C



I agree with oatmealturkey, so "C" is the correct answer.

upvoted 2 times

gewe 7 months ago

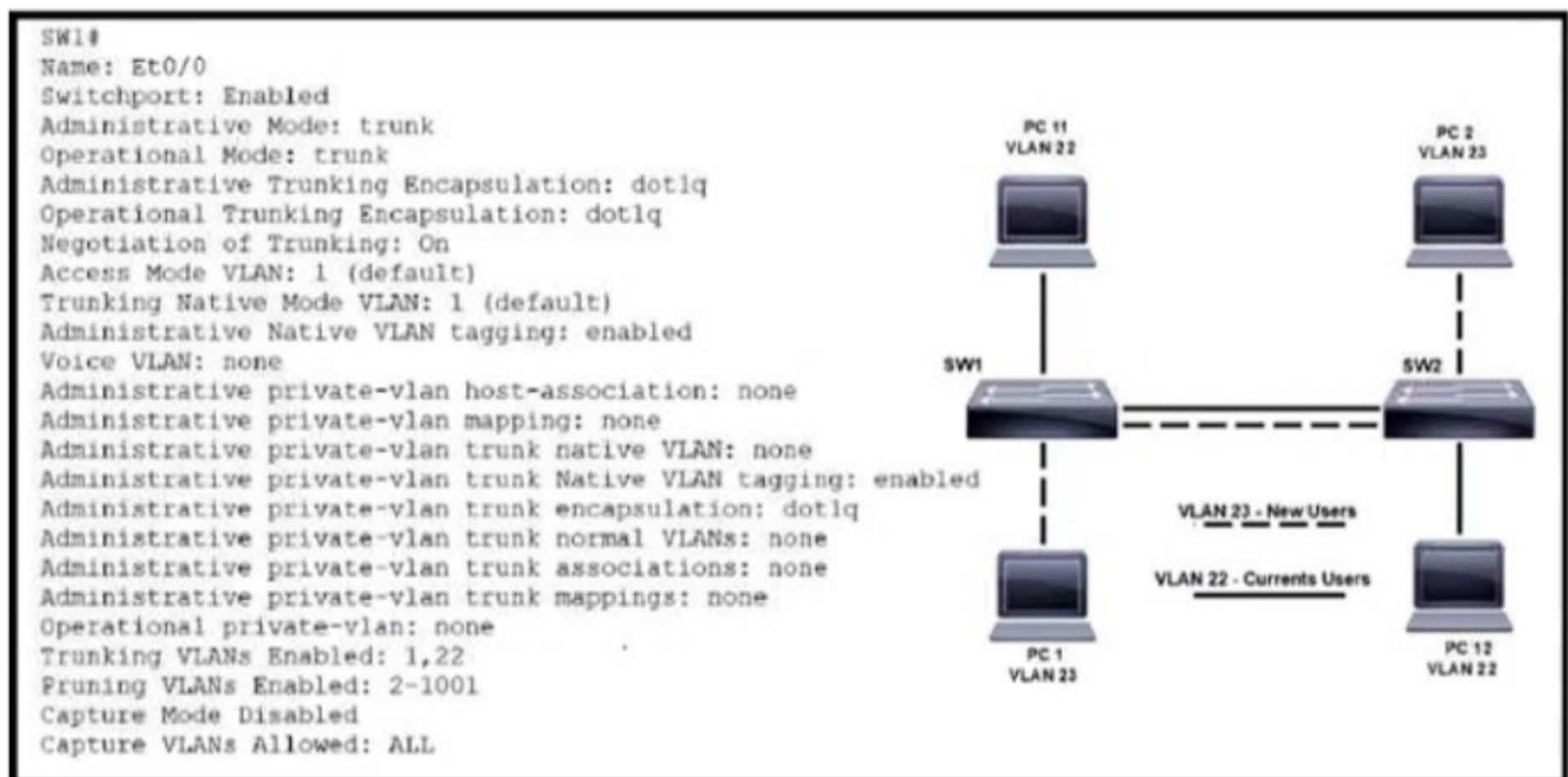
I was thinking about option B, but it is on SW2 which is configured correctly, so in this case we can add vlan 300 to po1, which makes C best choice

upvoted 3 times

  **yuz1227** 6 months, 1 week ago

You always update the information within the Portchannel information..

upvoted 5 times



Refer to the exhibit. VLAN 23 is being implemented between SW1 and SW2. The command show interface ethernet0/0 switchport has been issued on SW1. Ethernet0/0 on SW1 is the uplink to SW2. Which command when entered on the uplink interface allows PC 1 and PC 2 to communicate without impact to the communication between PC 11 and PC 12?

- A. switchport trunk allowed vlan 2-1001
- B. switchport trunk allowed vlan 23
- C. switchport trunk allowed vian add 23
- D. switchport trunk allowed vian 22-23

Correct Answer: A

gewe Highly Voted 7 months ago

I would go with option C..
correct me if I m not right
upvoted 12 times

krzysiew 5 months, 2 weeks ago

if vian = vlan you are right
upvoted 2 times

oatmealturkey 7 months ago

you are right
upvoted 5 times

Yinx Most Recent 3 weeks, 2 days ago

Selected Answer: A

2-1001 includes 22,23
upvoted 1 times

no_blink404 2 months, 2 weeks ago

Selected Answer: C

Answer is C, we need to 'add' vlan 23 to the already existing 1 & 22 vlan trunk. All the other answers will overwrite the allowed vlan range.
upvoted 1 times


dropspablo 2 months, 3 weeks ago

Selected Answer: A

The command syntax in the C (vian) response is wrong. The letter A command is correct, because vlan 2-1001 ignores default vlans 1 and default vlans 1002-1005, which seems more correct to me when using the trunk tags. Correct me if I'm wrong.
upvoted 1 times

  **dropspablo** 1 month, 1 week ago


Correction, the letter C must be correct, "vian" looks like misprint only (disregard my previous answer)
upvoted 1 times

  **Zepar** 3 months, 3 weeks ago

Looks like an Eye test exam.
upvoted 3 times

  **AndreaGambera** 2 weeks, 6 days ago

I agree
upvoted 1 times

  **Shabeth** 2 months, 2 weeks ago

yes! LOL, id still go with C
upvoted 1 times

  **Tdawg1968** 4 months, 1 week ago

If it's not C because of an i instead of l, that is just purely devious!
upvoted 1 times

  **bisiyemo1** 4 months, 3 weeks ago


Selected Answer: C

C is very correct
upvoted 2 times

  **liviuml** 5 months ago



Selected Answer: A

Correct answer A.
B will remove vlan 22.
C & D have "vian" instead of "vlan" - syntax isnot correct.
Regards,
upvoted 3 times

  **rogi2023** 5 months, 3 weeks ago

Selected Answer: C

C. switchport trunk allowed vian add 23
upvoted 3 times

  **RidzV** 6 months, 1 week ago

Selected Answer: C


We need to add vlan 23. Given answer doesn't make any sense.
upvoted 2 times

  **meszdenn** 6 months, 1 week ago

Correct me if i am wrong, but the two bottom answers have an "i" instead of "l" in vlan so they do not work. The above two answers "set" the allowed vlans, they do not "add" them.


In order to make sure that the communication on VLAN22 is not ruined by the new configuration, the only available option is allowing vlan 2-1001 or am i wrong? IF it was adding vlan 23 then i would agree, but i dont see an add..

upvoted 3 times

  **Rynurr** 6 months, 4 weeks ago

Selected Answer: C

Should be "C", cause we need to add VLAN 23
upvoted 3 times

  **lucantonelli93** 6 months, 4 weeks ago

It's C
upvoted 3 times

  **j1mlawton** 7 months ago

Selected Answer: D

Got to be D?
upvoted 1 times

  **j1mlawton** 7 months ago

CCCCC
upvoted 4 times

A network engineer starts to implement a new wireless LAN by configuring the authentication server and creating the dynamic interface. What must be performed next to complete the basic configuration?

- A. Create the new WLAN and bind the dynamic interface to it.
- B. Configure high availability and redundancy for the access points.
- C. Enable Telnet and RADIUS access on the management interface.
- D. Install the management interface and add the management IP.

Correct Answer: D

  **Simon_1103** Highly Voted 6 months, 2 weeks ago

Selected Answer: A

The correct answer is A because after configuring the authentication server and creating the dynamic interface, the next step in configuring a new WLAN is to create the WLAN and bind the dynamic interface to it. This will allow the wireless clients to connect to the WLAN and authenticate using the configured authentication server. Configuring high availability and redundancy for the access points, enabling Telnet and RADIUS access on the management interface, and installing the management interface and adding the management IP are all important steps in configuring a wireless LAN, but they come after creating the WLAN and binding the dynamic interface to it.

upvoted 9 times

  **oatmealturkey** Highly Voted 7 months ago

Selected Answer: A

The management interface is not "installed" and it is mandatory to statically configure it at setup, so at this point in the process that has already happened so D is incorrect. A is the correct answer, it is the next thing you do after configuring a dynamic interface.



upvoted 8 times

  **sbnpj** Most Recent 5 months, 3 weeks ago

Selected Answer: A

agree A is the correct Answer

upvoted 2 times

  **Rynurr** 6 months, 4 weeks ago

Selected Answer: A

"A" is the correct answer

upvoted 2 times

General	Security	OoS	Policy-Mapping	Advanced
Off Channel Scanning Defer				
Scan Defer Priority	0 1 2 3 4 5 6 7			
	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>			
Scan Defer Time(msecs)	100			
FlexConnect				
FlexConnect Local Switching ²	<input type="checkbox"/> Enabled			
FlexConnect Local Auth ¹²	<input type="checkbox"/> Enabled			
Learn Client IP Address ⁵	<input checked="" type="checkbox"/> Enabled			
Vlan based Central Switching ¹³	<input type="checkbox"/> Enabled			
Central DHCP Processing	<input type="checkbox"/> Enabled			
Override DNS	<input type="checkbox"/> Enabled			
NAT-PAT	<input type="checkbox"/> Enabled			
Central Assoc	<input type="checkbox"/> Enabled			
Lync				
Lync Server	Disabled			
Local Client Profiling				
HTTP Profiling <input type="checkbox"/>				
DHCP Profiling <input type="checkbox"/>				
HTTP Profiling <input type="checkbox"/>				
PMIP				
PMIP Mobility Type <input type="checkbox"/>				
PMIP NAI Type Hexadecimal				
PMIP Profile None				
PMIP Realm				
Universal AP Admin Support				
Universal AP admin <input type="checkbox"/>				
11v BSS Transition Support				
BSS Transition <input type="checkbox"/>				
Disassociation Imminent <input checked="" type="checkbox"/>				
Disassociation Timer (o to 3000 TBTT) 200				
Optimized Roaming Disassociation Timer (0 to 40 TBTT) 40				

Refer to the exhibit. An architect is managing a wireless network with APs from several branch offices connecting to the WLC in the data center. There is a new requirement for a single WLAN to process the client data traffic without sending it to the WLC. Which action must be taken to complete the request?

- A. Enable local HTTP profiling.
- B. Enable FlexConnect Local Switching.
- C. Enable local DHCP Profiling.
- D. Enable Disassociation Imminent.

Correct Answer: B

 **dropspablo** 2 months, 3 weeks ago

Resposta B parece correta!

"When a FlexConnect access point can reach the controller (referred to as the connected mode), the controller assists in client authentication. When a FlexConnect access point cannot access the controller, the access point enters the standalone mode (local authentication) and authenticates clients by itself."

...

"In the Advanced tab, select the FlexConnect Local Switching check box to enable local switching for the WLAN."

[https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-](https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html#21265:~:text=tab%2C%20select%20the-,FlexConnect%20Local%20Switching,-check%20box%20to)


[2/configuration/guide/cg/cg_flexconnect.html#21265:~:text=tab%2C%20select%20the-,FlexConnect%20Local%20Switching,-check%20box%20to](https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html#21265:~:text=tab%2C%20select%20the-,FlexConnect%20Local%20Switching,-check%20box%20to)
upvoted 1 times

 **perri88** 3 months ago

Selected Answer: B

By enabling FlexConnect Local Switching, the client data traffic is directly forwarded at the AP, reducing latency and bandwidth consumption. The AP in FlexConnect mode acts as a local switch, providing connectivity and forwarding traffic within the branch office without the need to send the traffic back to the WLC.

upvoted 1 times

 **Ciscoman021** 5 months, 3 weeks ago

Selected Answer: B

The action that must be taken to complete the request of processing client data traffic without sending it to the WLC is to enable FlexConnect Local Switching.

FlexConnect Local Switching (also known as "local switching" or "central switching") is a feature of Cisco wireless networks that allows for client traffic to be switched locally at the access point (AP) rather than being sent to the wireless LAN controller (WLC) for processing. This can improve network performance and reduce the load on the WLC.

upvoted 2 times

 **Dutch012** 6 months, 1 week ago

correct

upvoted 2 times

What must be considered for a locally switched FlexConnect AP if the VLANs that are used by the AP and client access are different?

- A. The APs must be connected to the switch with multiple links in LAG mode.
- B. The native VLAN must match the management VLAN of the AP.
- C. The switch port mode must be set to trunk.
- D. IEEE 802.1Q trunking must be disabled on the switch port.

Correct Answer: C

Which command configures the Cisco WLC to prevent a serial session with the WLC CLI from being automatically logged out?

- A. config sessions maxsessions 0
- B. config serial timeout 9600
- C. config serial timeout 0
- D. config sessions timeout 0

Correct Answer: D

  **oatmealturkey** Highly Voted 7 months ago



Selected Answer: C

Wrong, config sessions timeout 0 is for Telnet/SSH sessions
upvoted 6 times

  **dorf05** Most Recent 1 month, 3 weeks ago

Selected Answer: C



serial indicate directly connected while session is for remote connection.
upvoted 1 times

  **Toto86** 2 months, 2 weeks ago

Selected Answer: C



If you enter config serial timeout 0, serial sessions never time out.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/configuration-guide/b_cg81/b_cg81_chapter_011.html
upvoted 1 times



  **Yannik123** 4 months ago

Selected Answer: C

C is right. @examtopics please correct the answer
upvoted 3 times

  **Rydaz** 4 months, 1 week ago

If you set the serial timeout value to 0, serial sessions never time out.
answer is C
upvoted 1 times

  **HSong** 4 months, 2 weeks ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_011.html
upvoted 2 times



  **Njavwa** 5 months ago

If you configure a session-timeout of 0, it means 86400 seconds for 802.1X (EAP), and it disables the session-timeout for all other security types
upvoted 1 times

  **JJY888** 6 months, 2 weeks ago

Selected Answer: C

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/configuration-guide/b_cg81/b_cg81_chapter_011.html
upvoted 3 times

  **Rynurr** 6 months, 4 weeks ago

Selected Answer: C

Definitely "C".
'If you enter config serial timeout 0, serial sessions never time out.'
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/configuration-guide/b_cg81/b_cg81_chapter_011.html
upvoted 3 times

A Cisco engineer at a new branch office is configuring a wireless network with access points that connect to a controller that is based at corporate headquarters. Wireless client traffic must terminate at the branch office and access-point survivability is required in the event of a WAN outage. Which access point mode must be selected?

- A. Lightweight with local switching disabled
- B. FlexConnect with local switching enabled
- C. OfficeExtend with high availability disabled
- D. Local with AP fallback enabled

Correct Answer: B

 **Cynthia2023** 2 months, 3 weeks ago

Selected Answer: B

FlexConnect is a feature in Cisco wireless networks that allows access points to operate in a distributed manner, providing local switching capabilities at the branch office. In this mode, the access points can continue to serve wireless clients even if the WAN connection to the controller at the corporate headquarters is lost.

upvoted 2 times

What is an advantage of using auto mode versus static mode for power allocation when an access point is connected to a PoE switch port?

- A. Power policing is enabled at the same time.
- B. The default level is used for the access point.
- C. All four pairs of the cable are used.
- D. It detects the device is a powered device.

Correct Answer: D

 **Nwanna1** 3 days, 4 hours ago

The switch supports these PoE modes: auto – The switch automatically detects if the connected device requires power. If the switch discovers a powered device connected to the port and if the switch has enough power, it grants power, updates the power budget, turns on power to the port on a first-come, first-served basis, and updates the LEDs... static – The switch pre-allocates power to the port (even when no powered device is connected) and guarantees that power will be available for the port. Reference:

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_011010.html

upvoted 1 times

 **Nwanna1** 3 days, 4 hours ago

The switch supports these PoE modes:

auto – The switch automatically detects if the connected device requires power. If the switch discovers a powered device connected to the port and if the switch has enough power, it grants power, updates the power budget, turns on power to the port on a first-come, first-served basis, and updates the LEDs...

static – The switch pre-allocates power to the port (even when no powered device is connected) and guarantees that power will be available for the port.

Reference:

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_011010.html

upvoted 1 times

 **paolino555** 1 week, 2 days ago

chat gpt:

D. It detects the device is a powered device.

When you use auto mode for power allocation in a Power over Ethernet (PoE) switch port, the switch automatically detects the connected device and allocates the appropriate amount of power required for that device. This is known as "autonegotiation" or "auto-detection." This feature has the advantage of ensuring that the connected device receives the exact amount of power it needs, preventing over- or under-powering.

In contrast, static mode would require you to manually configure the power settings for the port, which can be less efficient and might not provide the optimal power allocation for the specific device connected to the port.


Option D highlights the advantage of auto mode in terms of automatically detecting the device as a powered device and allocating power accordingly.

upvoted 1 times

 **Secsoft** 2 weeks, 3 days ago

I will go with D. If the switch detects the powered device then only it turns the power on whereas in static mode the power is always available irrespective of the type of devices connected to it.

upvoted 1 times

 **Shabeth** 2 months, 2 weeks ago

Selected Answer: B

its B for me

upvoted 2 times

 **[Removed]** 2 months, 2 weeks ago

I'd say answer D

auto—The switch automatically detects if the connected device requires power. If the switch discovers a powered device connected to the port and if the switch has enough power, it grants power, updates the power budget, turns on power to the port on a first-come, first-served basis, and updates the LEDs.



upvoted 2 times

 **dropspablo** 2 months, 2 weeks ago

Selected Answer: B

Answer D is wrong because only the mode "NEVER disables powered device detection and never powers the PoE port" (according to the link). Both in static mode and in Auto they detect if the device is a powered device, but static also ensures power load to the port when there are many PoE devices, which is the advantage of static mode (high priority interface). Both Static and Auto if you do not specify the maximum power, the device will pre-allocate the maximum value. Now the advantage of "Auto" mode would be that it is enabled by default on all ports, meeting the plug-and-play requirement. I believe correct Answer letra B!

[https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/16-11/configuration_guide/int_hw/b_1611_int_and_hw_9400_cg/configuring_poe.html#:~:text=the%20default%20configuration-,\(auto%20mode\)%20works%20well%2C%20providing%20plug%2Dand%2Dplay%20operation.,-No%20further%20configuration](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/16-11/configuration_guide/int_hw/b_1611_int_and_hw_9400_cg/configuring_poe.html#:~:text=the%20default%20configuration-,(auto%20mode)%20works%20well%2C%20providing%20plug%2Dand%2Dplay%20operation.,-No%20further%20configuration)
upvoted 2 times

  **HSong** 4 months, 2 weeks ago

Selected Answer: B

It is B.

upvoted 1 times

  **Pandaren** 6 months ago

B:"Use the auto setting on any PoE port. The auto mode is the default setting."

upvoted 4 times

The screenshot shows the Cisco configuration interface for a Local Net User. The 'Security' menu is expanded to 'Local Net Users'. The configuration fields are as follows:

Field	Value
User Name	NA-User
Password
Confirm Password
Guest User	<input checked="" type="checkbox"/>
Lifetime (seconds)	86400
Guest User Role	<input type="checkbox"/>
WLAN Profile	Any WLAN
Description	For NA WLAN Auth

Refer to the exhibit. Wireless LAN access must be set up to force all clients from the NA WLAN to authenticate against the local database. The WLAN is configured for local EAP authentication. The time that users access the network must not be limited. Which action completes this configuration?

- A. Check the Guest User Role check box.
- B. Uncheck the Guest User check box.
- C. Set the Lifetime (seconds) value to 0.
- D. Clear the Lifetime (seconds) value.

Correct Answer: C

xbololi Highly Voted 2 months, 1 week ago

I'm studying more than 6 months for ccna... When i started to work on dumps i think i saw cisco wireless device more than switch and router in total...

upvoted 5 times

Shri_Fcb10 1 month, 3 weeks ago

that is so true

upvoted 1 times

Tdawg1968 Most Recent 4 months, 1 week ago

I agree with B to force all clients to authenticate.

upvoted 1 times

liviuml 5 months ago

Selected Answer: B

Lifetime valid range is 60 to 2,592,000 seconds, default is 86,400 seconds.

For unlimited time Guest User has to be unchecked,

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-6/configuration-guide/b_cg76/b_cg76_chapter_0101100.pdf

Regards

upvoted 4 times

Njavwa 5 months ago

when you uncheck the guest box will you still have guests ? if yes then its the answer if we wont have guests after unchecking then the correct answer should be setting the timer to 0

upvoted 1 times

bisiyemo1 5 months, 2 weeks ago

Selected Answer: C

C is correct



upvoted 1 times

Ciscoman021 5 months, 2 weeks ago

Selected Answer: B

To configure the wireless LAN access to force all clients to authenticate against the local database using local EAP authentication and allow access at any time, you need to uncheck the Guest User check box. This ensures that all users are required to authenticate against the local database, and not just guests.

upvoted 1 times


  **JJY888** 6 months, 2 weeks ago

Selected Answer: C

<https://community.cisco.com/t5/wireless/guest-user-account-lifetime/td-p/2552337>



https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/wireless/controller/8-1/configuration-guide/b_cg81/b_cg81_chapter_011.html.xml

upvoted 4 times

  **papinski** 6 months, 2 weeks ago

Running with this.

upvoted 1 times

  **Rynurr** 6 months, 4 weeks ago

Selected Answer: B

Should be "B"

upvoted 2 times

  **oatmealturkey** 7 months ago

Selected Answer: B

Wrong, uncheck Guest User box and the Lifetime will go away.

A. Check the Guest User Role check box.

B. Uncheck the Guest User check box.

C. Set the Lifetime (seconds) value to 0.

D. Clear the Lifetime (seconds) value.

upvoted 3 times

DRAG DROP

Drag and drop the wireless architecture benefits from the left onto the architecture types on the right.

Appropriate for a small-business environment.	Split-MAC
Work is divided between the access point and the controller.	
The access points transmit beacon frames.	
Supports per device configuration and management.	Autonomous
Uses the CAPWAP tunneling protocol.	

Correct Answer:

Appropriate for a small-business environment.	Split-MAC
Work is divided between the access point and the controller.	
Uses the CAPWAP tunneling protocol.	
The access points transmit beacon frames.	Autonomous
Supports per device configuration and management.	
Uses the CAPWAP tunneling protocol.	

no_blink404 2 months, 2 weeks ago

The answer looks correct. The LWAPP AP handles the transmission of beacon frames.
 Source: <https://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/TechArch.html#wp999574>
 upvoted 3 times

perri88 3 months ago

Beacon frames are transmitted periodically, they serve to announce the presence of a wireless LAN and to synchronise the members of the service set. Beacon frames are transmitted by the access point (AP) in an infrastructure basic service set (BSS). In IBSS network beacon generation is distributed among the stations.
 upvoted 1 times

🗨️ 👤 **ac89l** 4 months ago

I think it is correct.
Can anyone confirm this?
upvoted 1 times

🗨️ 👤 **studying_1** 4 months ago

yes, answer is correct
upvoted 3 times

Question #869

Topic 1

What is a specification for SSIDs?

- A. They must include one number and one letter.
- B. They are a Cisco proprietary security feature.
- C. They are case sensitive.
- D. They define the VLAN on a switch.

Correct Answer: C

🗨️ 👤 **[Removed]** 2 months, 2 weeks ago

Selected Answer: C

C is correct, they are case sensitive.
upvoted 1 times

🗨️ 👤 **LeonardoMeCabrio** 3 months, 1 week ago

Selected Answer: C

C is correct
upvoted 2 times

🗨️ 👤 **ac89l** 4 months ago

Selected Answer: D

Should be D, based on elimination.
upvoted 1 times

🗨️ 👤 **studying_1** 4 months ago

no, C is correct
upvoted 5 times

🗨️ 👤 **ac89l** 4 months ago

you're right .. my bad
upvoted 1 times

What is a reason to configure a trunk port that connects to a WLC distribution port?

- A. Provide redundancy if there is a link failure for out-of-band management.
- B. Allow multiple VLANs to be used in the data path.
- C. Permit multiple VLANs to provide out-of-band management.
- D. Eliminate redundancy with a link failure in the data path.

Correct Answer: B

  **studying_1** 3 months, 2 weeks ago

Selected Answer: B

answer is correct, distribution port is connected to the wired network(distribution system) and used for data traffic, and usually it's trunk which allows multiple vlans

upvoted 3 times

DRAG DROP

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

Answer Area

access point	manages access points
virtual interface	provides Wi-Fi devices with a connection to a wired network
dynamic interface	used for out-of-band management
service port	used for guest authentication
wireless LAN controller	applied to the WLAN for wireless client communication

Answer Area

Correct Answer:

access point	wireless LAN controller
virtual interface	access point
dynamic interface	service port
service port	dynamic interface
wireless LAN controller	virtual interface

gewe Highly Voted 7 months ago

I would swap virtual/dynamic interfaces.
upvoted 9 times

LeonardoMcCabrio 2 months, 2 weeks ago

Agree with that also
upvoted 1 times

perri88 3 months ago

agreed
upvoted 1 times

Rynurr 6 months, 4 weeks ago

I agree with that
upvoted 3 times

gewe Highly Voted 7 months ago

The WLC has a virtual interface that it uses for mobility management. This includes DHCP relay, guest web authentication, VPN termination, and some other features.
upvoted 7 times

no_blink404 Most Recent 2 months, 2 weeks ago

wireless lan controller
access point
service port
virtual interface
dynamic interface



source: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/m_configuring_virtual_interfaces.pdf
upvoted 2 times

  **Shun5566** 3 months, 1 week ago

wireless LAN controller
access point service port
virtual interface
dynamic interface
upvoted 1 times

  **Shun5566** 3 months, 1 week ago

wireless LAN controller
access point
service port
virtual interface
dynamic interface
upvoted 2 times

  **JJY888** 6 months, 2 weeks ago

Swap virtual and dynamic.

<https://networklessons.com/cisco/ccna-200-301/cisco-wireless-lan-controller-wlc-basic-configuration#:~:text=Virtual%20Gateway%20IP%20Address%3A%20The,the%20WLC%20and%20wireless%20clients.>
upvoted 2 times

  **krzysiew** 5 months, 2 weeks ago

I agree
upvoted 2 times

The screenshot shows the Cisco WLC configuration interface for a WLAN profile named 'TEST_PROFILE'. The 'Security' tab is active, showing the following settings:

- Profile Name: TEST_PROFILE
- Type: WLAN
- SSID: CISCO_TEST
- Status: Enabled
- Security Policies: [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
- Radio Policy: All
- Interface/Interface Group(G): management
- Multicast Vlan Feature: Enabled
- Broadcast SSID: Enabled
- NAS-ID: Cisco_42:0e:44

Refer to the exhibit. A Cisco WLC administrator is creating a new wireless network with enhanced SSID security. The new network must operate at 2.4 Ghz with 54 Mbps of throughput. Which set of tasks must the administrator perform to complete the configuration?

- A. Uncheck the Broadcast SSID check box and set the Radio Policy to 802.11a/g only.
- B. Check the Broadcast SSID check box and set the Radio Policy to 802.11g only.
- C. Uncheck the Broadcast SSID check box and set the Radio Policy to 802.11g only.
- D. Check the Broadcast SSID check box and set the Radio Policy to 802.11a only.

Correct Answer: A

Rynurr Highly Voted 6 months, 4 weeks ago

Selected Answer: C

Should be "C".

802.11g uses 2.4GHz and throughput up to 54 Mbit/s.

"enhanced SSID security" = hiding SSID, so we must uncheck Broadcast SSID option

upvoted 9 times

[Removed] Most Recent 2 months, 2 weeks ago

Selected Answer: C

C. Uncheck the Broadcast SSID check box and set the Radio Policy to 802.11g only.

(enhanced SSID security) (must operate at 2.4 Ghz)

upvoted 1 times

jonathan126 4 months, 3 weeks ago

Based on Cisco's article, disabling SSID broadcast provides some security, so answer C should be correct.

"This article guides you on how to successfully disable SSID broadcast on your access point for added security"

<https://www.cisco.com/c/en/us/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5177-disable-ssid-broadcast-on-a-wireless-access-point.html>

upvoted 1 times

Njavwa 4 months, 4 weeks ago

Selected Answer: C

both 802.1a/g have a maximum data rate of 54Mbps, unfortunately only 802.1g provides for 2.4, 802.1a provides for 5Ghz

upvoted 2 times

Simon_1103 5 months, 1 week ago


Selected Answer: C

Option C is correct:(Answer from ChatGPT)

Unchecking the Broadcast SSID check box will hide the network name (SSID) from being broadcasted to wireless clients. Setting the Radio Policy to 802.11g only will allow the network to operate at 2.4 GHz with 54 Mbps of throughput. Option A is incorrect because setting the Radio Policy to 802.11a/g only will enable both 2.4 GHz and 5 GHz bands, which may not be necessary for the requirements given.

Option B is incorrect because checking the Broadcast SSID check box will broadcast the network name, which could potentially make it easier for attackers to target the network.

Option D is incorrect because setting the Radio Policy to 802.11a only will disable the 2.4 GHz band, which is required for the requirements given.
upvoted 3 times

  **Spike111** 5 months, 1 week ago

Selected Answer: B

as hiding your SSID does not provide complete security, and other methods such as encryption and a strong password should also be used¹. In practice, hiding the SSID makes no difference whatsoever to the security of your network². Therefore, it is recommended that you do not hide your SSID also any hacker with a simple network sniffing tool can find out your SSID in seconds, even if you are not broadcasting it.

upvoted 1 times

  **espanrews** 3 months, 3 weeks ago

OK it makes no difference to a hacker, but it might help to hide it from other kind of criminals, and we have to choose an answer. I go with C, it looks more secure (except for hackers).



upvoted 2 times

  **purenuker** 6 months, 1 week ago

Selected Answer: C

802.11a operating frequency is 5GHz - it is not correct answer

upvoted 3 times

  **ike110** 6 months, 4 weeks ago

Selected Answer: C

The answer is C

upvoted 3 times

  **lucantonelli93** 6 months, 4 weeks ago


Selected Answer: B

For me, the correct answer is the b.

https://it.wikipedia.org/wiki/IEEE_802.11

It uses the same frequencies as the 802.11b standard i.e. the 2.4 GHz band and provides a theoretical speed of 54 Mb/s which in reality translates into a net speed of 24.7 Mb/s, similar to that of the 802.11a standard .

upvoted 1 times

  **krzysiew** 5 months, 2 weeks ago

but we must enhance ssid security that why we uncheck broadcast SSID

upvoted 2 times

  **oatmealturkey** 7 months ago

Selected Answer: C

802.11a is 5 Ghz and we want 2.4 only ("must" operate at 2.4) so A is incorrect.

upvoted 3 times

Which switching feature removes unused MAC addresses from the MAC address table, which allows new MAC addresses to be added?

- A. MAC address aging
- B. MAC move
- C. MAC address auto purge
- D. dynamic MAC address learning

Correct Answer: A

🗨️ 👤 **[Removed]** 2 months, 2 weeks ago

Selected Answer: A

Given answer is correct

A. MAC address aging

upvoted 1 times

🗨️ 👤 **StingVN** 3 months, 3 weeks ago

Selected Answer: A

A. MAC address aging

MAC address aging is a switching feature that removes unused MAC addresses from the MAC address table after a certain period of inactivity. This frees up space in the MAC address table, allowing new MAC addresses to be added when new devices are connected to the network. The aging time determines how long a MAC address can remain in the table without any activity before it is considered unused and eligible for removal. This feature helps optimize the usage of MAC address table resources in a switch.

upvoted 4 times

🗨️ 👤 **studying_1** 3 months, 2 weeks ago

Yes, by default it's 5 minutes

upvoted 3 times

WLANs > Edit 'CCNA'

General | **Security** | **QoS** | **Policy-Mapping** | **Advanced**

Allow AAA Override Enabled

Coverage Hole Detection Enabled

Enable Session Timeout Session Timeout (secs)

Aironet IE Enabled

Diagnostic Channel [18](#) Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

P2P Blocking Action Disabled

Client Exclusion [3](#) Enabled Timeout Value (secs)

Maximum Allowed Clients [8](#)

Static IP Tunneling [11](#) Enabled

Wi-Fi Direct Clients Policy Disabled

Maximum Allowed Clients Per AP Radio

Clear HotSpot Configuration Enabled

Client user idle timeout(15-100000)

Client user idle threshold (0-10000000) Bytes

DHCP

DHCP Server Override

DHCP Addr. Assignment Required

OEAP

Split Tunnel Enabled

Management Frame Protection (MFP)

MFP Client Protection [4](#) Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

NAC State None

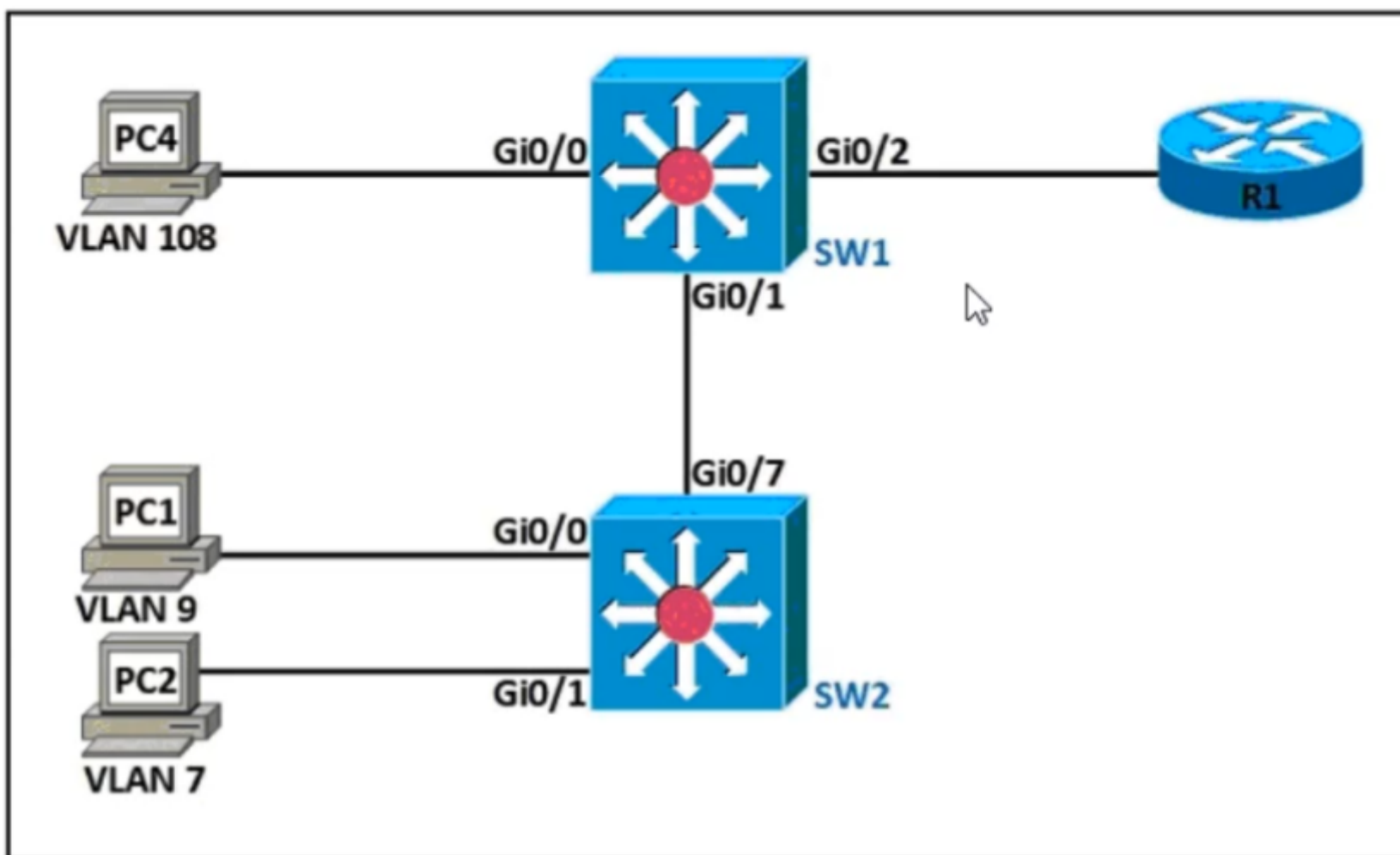
Load Balancing and Band Select

Client Load Balancing

Refer to the exhibit. A network engineer configures the CCNA WLAN so that clients must reauthenticate hourly and to limit the number of simultaneous connections to the WLAN to 10. Which two actions complete this configuration? (Choose two.)

- A. Enable the Wi-Fi Direct Clients Policy option
- B. Enable the Enable Session Timeout option and set the value to 3600.
- C. Enable the Client Exclusion option and set the value to 3600.
- D. Set the Maximum Allowed Clients value to 10.
- E. Set the Maximum Allowed Clients Per AP Radio value to 10.

Correct Answer: BD



Refer to the exhibit. The SW1 and SW2 Gi0/0 ports have been preconfigured. An engineer is given these requirements:

- Allow all PCs to communicate with each other at Layer 3.
- Configure untagged traffic to use VLAN 5.
- Disable VLAN 1 from being used.

Which configuration set meets these requirements?

A. SW1#

```
interface Gi0/1
switchport mode trunk
switchport trunk allowed vlan 5,7,9,108
switchport trunk native vlan 5
```

```
interface Gi0/2
switchport mode trunk
switchport trunk allowed vlan 5,7,9,108
```

SW2#

```
interface Gi0/1
switchport mode access
switchport access vlan 7
```

```
interface Gi0/7
switchport mode trunk
switchport trunk allowed vlan 7,9,108
```

B. SW1#

```
interface Gi0/1
switchport mode trunk
switchport trunk allowed vlan 5,7,9,108
switchport trunk native vlan 5
```

```
interface Gi0/2
switchport mode access
switchport trunk allowed vlan 7,9,108
```

```
SW2#  
interface Gi0/1  
switchport mode access  
no switchport access vlan 1  
switchport access vlan 7
```

```
interface Gi0/7  
switchport mode trunk  
switchport trunk allowed vlan 7,9,108  
switchport trunk native vlan 5
```

```
C. SW#1 -  
interface Gi0/1  
switchport mode trunk  
switchport trunk allowed vlan 5,7,9,108  
switchport trunk native vlan 5
```

```
interface Gi0/2  
switchport mode trunk  
switchport trunk allowed vlan 5,7,9,108
```

```
SW2#  
interface Gi0/1  
switchport mode access  
switchport access vlan 7
```

```
interface Gi0/7  
switchport mode trunk  
switchport trunk allowed vlan 5,7,9,108  
switchport trunk native vlan 5
```

```
D. SW1#  
interface Gi0/1  
switchport mode trunk  
switchport trunk allowed vian 5,7,9,108
```

```
interface Gi0/2  
switchport mode trunk  
switchport trunk allowed vlan 7,9,108
```

```
SW2#  
interface Gi0/1  
switchport mode trunk  
switchport trunk allowed vlan 7
```

```
interface Gi0/7  
switchport mode trunk  
switchport trunk allowed vlan 5,7,9,108
```

Correct Answer: C

 **dropspablo** 2 months, 2 weeks ago

Selected Answer: C

Letter A - Two mismatch (between SW1 and SW2): Native Vlan and Vlan Allowed.

Letter B - A mismatch (between SW1 and SW2): Vlan Allowed.

Letter C - Working, best option!

Letter D - Native Vlan 5 not configured. (*wrong command vian)

upvoted 3 times

🗨️ 👤 **JJY888** 4 months, 1 week ago

Scratch my comment from the record, please.
upvoted 1 times

🗨️ 👤 **JJY888** 4 months, 1 week ago

Selected Answer: B

It can't be C. Option B is the only answer with the PC on SW1 connected as an access port.
upvoted 4 times

🗨️ 👤 **[Removed]** 2 months, 2 weeks ago

Yes, it can be C
upvoted 2 times

🗨️ 👤 **LeonardoMeCabrio** 3 months, 1 week ago

B cannot be correct. A configuration for access port at vlan 1 exists.
upvoted 2 times

🗨️ 👤 **Channaveera** 5 months, 4 weeks ago

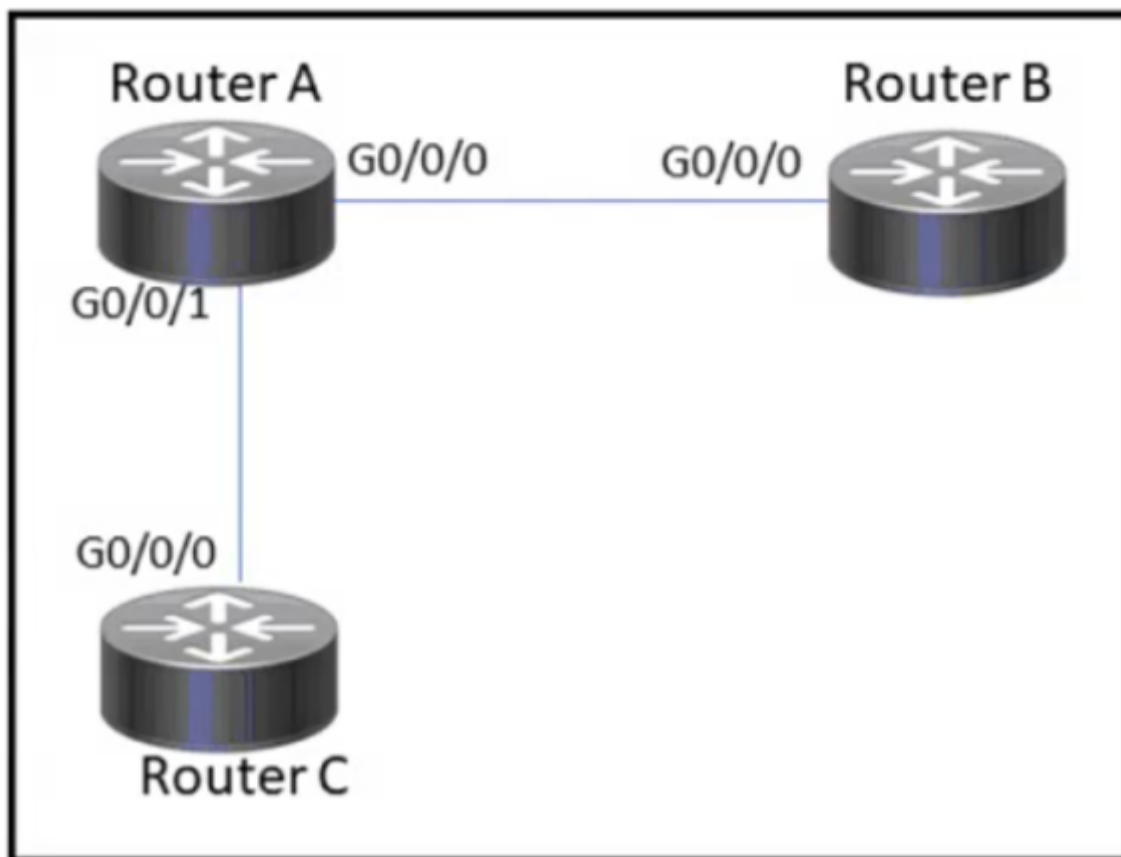
Why SW1 is Trunk.
Switch to router port is enabled Trunk only for router on stick.

```
interface Gi0/2
switchport mode trunk
switchport trunk allowed vlan 5,7,9,108
```

upvoted 1 times

🗨️ 👤 **fra130186** 2 months, 3 weeks ago

Allow all PCs to communicate with each other at Layer 3, that's y
upvoted 1 times



Refer to the exhibit. How must router A be configured so that it only sends Cisco Discovery Protocol information to router C?

A. #config t

```
Router A (config)#no cdp run -
Router A (config)#interface gi0/0/1
```

```
Router A (config-if)#cdp enable -
```

B. #config t

```
Router A (config)#cdp run -
Router A (config)#interface gi0/0/0
Router A (config-if)#no cdp enable
```

C. #config t -

```
Router A (config)#cdp run -
Router A (config)#interface gi0/0/1
```

```
Router A (config-if)#cdp enable -
```

D. #config t

```
Router A (config)#cdp run -
Router A (config)#interface gi0/0/0
Router A (config-if)#cdp enable
```

Correct Answer: A

Rynurr Highly Voted 6 months, 4 weeks ago

Selected Answer: B

"B" is the correct answer.
interface gi0/0/0
Router A (config-if)#no cdp enable
upvoted 9 times

gewe Highly Voted 7 months ago

B seems correct as cdp is enabled by default
upvoted 8 times

  **dorf05** Most Recent 1 week, 6 days ago

Selected Answer: A

CDP stands for Cisco Discovery Protocol, which is a proprietary Layer 2 protocol that runs on Cisco devices to discover and share information about neighboring devices¹. CDP is enabled by default on all supported interfaces, except for Frame Relay multipoint subinterfaces¹.

To disable CDP globally on a Cisco device, you can use the command `no cdp run` in global configuration mode². This will stop the device from sending and receiving CDP packets on all interfaces.

To enable CDP on a specific interface, you can use the command `cdp enable` in interface configuration mode³. This will override the global configuration and allow the interface to send and receive CDP packets.

For example, if you want to disable CDP globally on a switch and enable it only on interface FastEthernet 2/12, you can use the following commands:

```
Switch(config)# no cdp run
Switch(config)# interface FastEthernet 2/12
Switch(config-if)# cdp enable
```

upvoted 1 times

  **ds0321** 3 weeks, 1 day ago

Selected Answer: B

it is B

<https://www.cisco.com/c/en/us/support/docs/network-management/discovery-protocol-cdp/43485-cdponios43485.html>

upvoted 1 times

  **bauga** 3 weeks, 2 days ago

Selected Answer: A

the answer is A

upvoted 2 times

  **Cynthia2023** 1 month ago

Selected Answer: B

CDP must be globally enabled first.

upvoted 1 times

  **Cynthia2023** 1 month ago



If CDP is disabled globally on the device, you won't be able to enable it on specific interfaces. When CDP is globally disabled, the device stops sending or receiving CDP packets altogether, so you won't be able to enable it on a per-interface basis.

upvoted 2 times

  **Shri_Fcb10** 1 month, 3 weeks ago

should it not be `cdp run` instead of `cdp enable`, enable keyword used with LLDP if I am not wrong

upvoted 1 times

  **sam225555** 2 months ago

Selected Answer: B

B" is the correct answer.

upvoted 1 times

  **fmaquino** 2 months ago

Selected Answer: B

B seems the correct answer

upvoted 1 times

  **fmaquino** 3 months, 1 week ago

Selected Answer: B

B seems correct



upvoted 1 times

  **MassNastty1** 3 months, 3 weeks ago

100% B is the correct answer.

https://www.cisco.com/c/en/us/td/docs/optical/cpt/r9_5/command/reference/cpt95_cr/cpt95_cr_chapter_0

upvoted 1 times

  **saoETo** 5 months, 1 week ago

Selected Answer: B

```
Router(config)# no cdp run
Router(config)# end
Router# show cdp
% CDP is not enabled
```

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# cdp enable
% Cannot enable CDP on this interface, since CDP is not running
Router(config-if)#
```

https://www.cisco.com/c/en/us/td/docs/optical/cpt/r9_5/command/reference/cpt95_cr/cpt95_cr_chapter_01101.pdf
upvoted 2 times

  **rogi2023** 5 months, 3 weeks ago

Selected Answer: A



Answer A is correct. You can enable cdp either globally with "cdp run" on all interfaces or just per intf basis with cmd "cdp enable" directly on intf. To fulfill the requirements in the question = A is correct.

upvoted 5 times

  **perri88** 3 months ago

"cdp enable" command on any interface. Disabling CDP globally means that CDP is disabled for all interfaces on the device, and it will not be possible to enable CDP on a specific interface.

upvoted 1 times

  **beamage** 3 months, 2 weeks ago

wrong!!!!

upvoted 1 times

  **Channaveera** 5 months, 4 weeks ago

I agree with gewe B is the answer



upvoted 1 times

  **DavidCisco** 6 months, 1 week ago

Selected Answer: B

CDP must be enable in conf global because of this it is enable in all interfaces so you must disable in interface g0/0/0 to router B

upvoted 1 times

  **JJY888** 6 months, 2 weeks ago

Selected Answer: B


It's can't be A because :

```
R3(config)#no cdp run
R3(config)#inter
R3(config)#interface g0/1
R3(config-if)#cd
R3(config-if)#cdp en
R3(config-if)#cdp enable
R3(config-if)#exi
R3(config-if)#exit
R3(config)#exi
R3(config)#exit
R3#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
R3#sh
R3#show cd
R3#show cdp inter
R3#show cdp interface
% CDP is not enabled
I did this on packet tracer myself
```


upvoted 3 times

  **Dutch012** 6 months, 2 weeks ago

Selected Answer: A

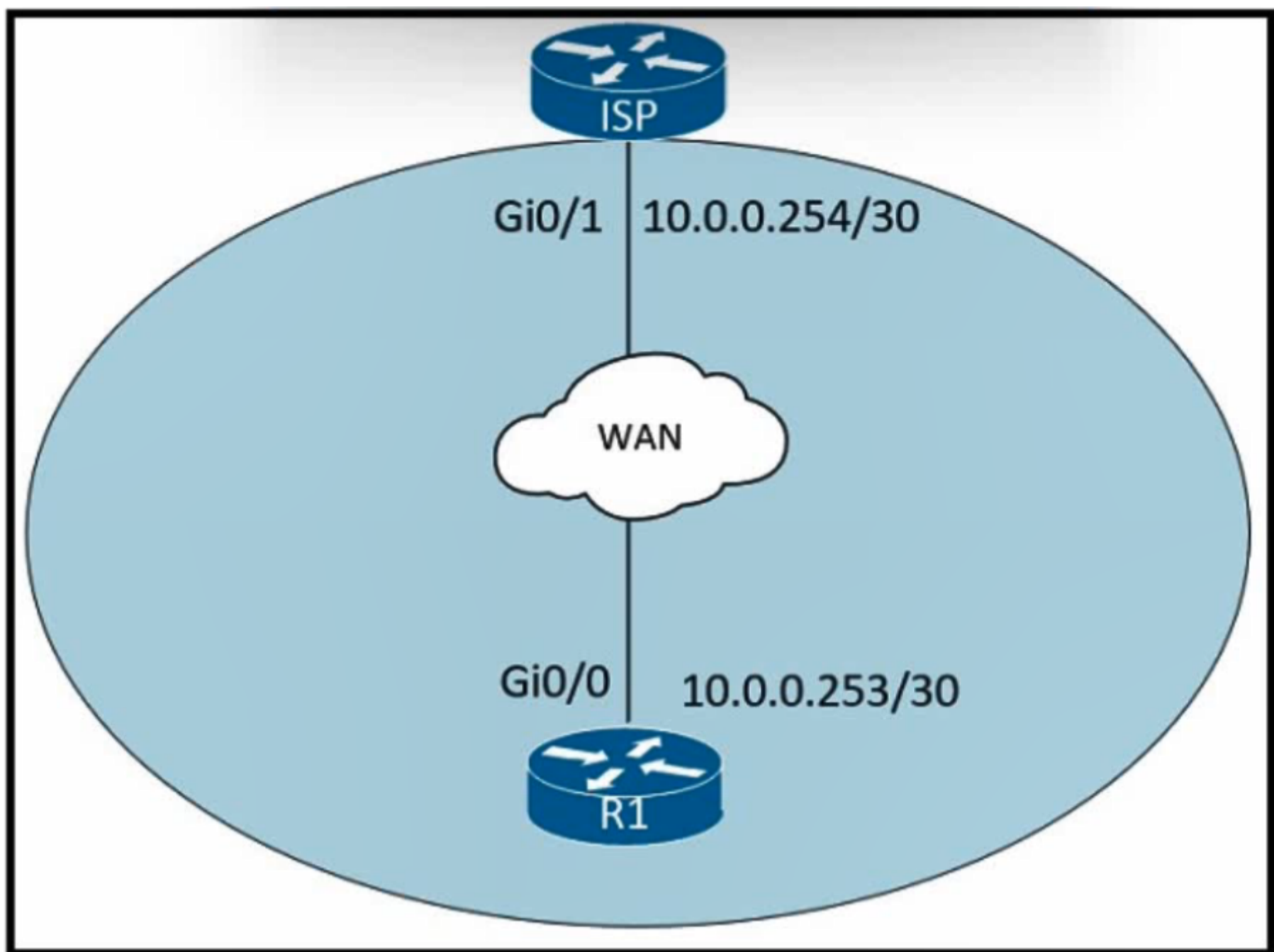
We should only enable it on gi0/0/1 which is connected to Router C, so all other ports should be disabled.

upvoted 3 times

  **perri88** 3 months ago

"cdp enable" command on any interface. Disabling CDP globally means that CDP is disabled for all interfaces on the device, and it will not be possible to enable CDP on a specific interface.

upvoted 1 times



Refer to the exhibit. An administrator must turn off the Cisco Discovery Protocol on the port configured with address last usable address in the 10.0.0.0/30 subnet. Which command set meets the requirement?

- A. interface gi0/1
no cdp enable
- B. interface gi0/0
no cdp run
- C. interface gi0/0
no cdp advertise-v2
- D. interface gi0/1
clear cdp table

Correct Answer: B

gewe Highly Voted 7 months ago

thats correct.
answer is A
upvoted 9 times

purenuker Highly Voted 6 months, 1 week ago

So stupid question - last usable address of 10.0.0.0/30 is 10.0.0.2/30 ...
upvoted 7 times

VictorCisco 5 months, 2 weeks ago

even more stupid as offer to configure ISP router 🤔 Who allows it to him??? 🤔 🤔
upvoted 4 times

deluxeccna 5 months ago

Maybe he works for the ISP



upvoted 1 times

  **MassNastty1** Most Recent 3 months, 3 weeks ago

A is correct, source:

https://www.cisco.com/c/en/us/td/docs/optical/cpt/r9_5/command/reference/cpt95_cr/cpt95_cr_chapter_0

upvoted 1 times

  **bisiyemo1** 5 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

  **bisiyemo1** 6 months, 1 week ago

Selected Answer: A

Please Examtopics, the correct answer is A.

This your current updated questions need a review.

upvoted 4 times



  **DavidCisco** 6 months, 1 week ago

Selected Answer: A

global - no cdp run

interface - no cdp enable

upvoted 4 times

  **Rynurr** 6 months, 4 weeks ago

Selected Answer: A

Last usable address is 10.0.0.254, so "A" is the only answer.

upvoted 1 times

  **lucantonelli93** 6 months, 4 weeks ago

It's A , please correct

upvoted 2 times

  **ahmt** 7 months ago

Selected Answer: A

Answer is A

upvoted 4 times

  **oatmealturkey** 7 months ago

Selected Answer: A

Answer is A, .254 is last usable address and no cdp run is not a valid interface command so it can't be B anyway. [no] cdp run is a global command.

The valid config-if command is no cdp enable

upvoted 5 times

  **j1mlawton** 7 months ago

Selected Answer: A

Last useable address it can only be the highest IP out of the 2?

upvoted 3 times

Which WLC port connects to a switch to pass normal access-point traffic?

- A. redundancy
- B. service
- C. console
- D. distribution system

Correct Answer: D

 **shaney67** 3 weeks ago

The correct answer is B. service.

In a Wireless LAN Controller (WLC) setup, the service port is the one that connects to a switch to pass normal access-point traffic. This port is responsible for handling the communication between the access points and the WLC, allowing the access points to send and receive data to and from the wired network.

The other options are as follows:

A. redundancy: This port is used for communication between redundant WLCs for failover and backup purposes.

C. console: This port is typically used for out-of-band management and configuration of the WLC.

D. distribution system: This term is often used in the context of the wireless network itself, referring to the infrastructure that connects the access points and provides wireless coverage. It's not specifically related to the port on the WLC that connects to a switch.

So, the correct choice for the port that connects to a switch to pass normal access-point traffic is B. service.

upvoted 2 times

 **Amr_001** 5 days, 15 hours ago

Distribution system port: Used for all normal AP and management traffic; usually connects to a switch port in 802.1Q trunk mode from official cert guide

upvoted 1 times

 **MartiFia** 1 week, 1 day ago

This is answer from ChatGPT which is not correct.

The service port can be used management purposes, primarily for out-of-band management. However, AP management traffic is not possible across the service port.

A distribution system port connects the controller to a neighbor switch and serves as the data path between these two devices.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-6/configuration-guide/b_cg76/b_cg76_chapter_011010.html#ID106

upvoted 1 times

Which default condition must be considered when an encrypted mobility tunnel is used between two Cisco WLCs?

- A. The tunnel uses the IPsec protocol for encapsulation.
- B. Control and data traffic encryption are enabled.
- C. The tunnel uses the EoIP protocol to transmit data traffic.
- D. TCP port 443 and UDP 21 are used.

Correct Answer: D

 **oatmealturkey** Highly Voted 7 months ago

Selected Answer: B

D is incorrect. The controller uses UDP port 16667 to send data traffic. EoIP is not used to send data traffic across an encrypted mobility tunnel. Data traffic is encrypted in an encrypted mobility tunnel and control traffic is always encrypted, so the answer is B.

<https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107188-mobility-groups-faq.pdf>

upvoted 5 times

 **dropspablo** Most Recent 1 month ago

Correct answer is "B".

"The Encrypted Mobility Tunnel feature should be enabled on all the mobility peers in the network to have the tunnel created. The default state is set to disabled."

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/encrypted_mobility_tunnel.html#info-encrypted-mobility-tunnel:~:text=The%20Encrypted%20Mobility%20Tunnel%20feature%20should%20be%20enabled%20on%20all%20the%20mobility%20peers%20in%20the%20network%20to%20have%20the%20tunnel%20created.%20The%20default%20state%20is%20set%20to%20disabled.

upvoted 1 times

 **Secsoft** 1 month, 3 weeks ago

Almost every answers of wireless network are incorrect. Where is the admin?

upvoted 1 times

 **4bed5ff** 2 months, 2 weeks ago

Selected Answer: B

Confirming oatmealturkey's answer: <https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107188-mobility-groups-faq.html#:~:text=If%20encrypted%20mobility,send%20the%20data%20traffic>


upvoted 2 times

 **JJY888** 6 months, 2 weeks ago

Selected Answer: B

<https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107188-mobility-groups-faq.pdf>

upvoted 1 times

 **Rynurr** 6 months, 4 weeks ago

Selected Answer: B

I agree with oatmealturkey. Only answer "B" makes sense.

upvoted 2 times

The screenshot shows the 'Advanced' configuration page with the following settings:

- Allow AAA Override: Enabled
- Coverage Hole Detection: Enabled
- Enable Session Timeout:
- Aironet IE: Enabled
- Diagnostic Channel: Enabled
- Override Interface ACL: IPv4: None, IPv6: None
- Layer2 Acl: None
- URL ACL: None
- P2P Blocking Action: Disabled
- Client Exclusion: Enabled, Timeout Value (secs): 180
- Maximum Allowed Clients: 0
- Static IP Tunneling: Enabled
- Wi-Fi Direct Clients Policy: Disabled
- Maximum Allowed Clients Per AP Radio: 200
- DHCP: DHCP Server: Override, DHCP Addr. Assignment: Required
- Management Frame Protection (MFP): MFP Client Protection: Optional
- OTIM Period (In beacon intervals): 802.11a/n (1 - 255): 1, 802.11b/g/n (1 - 255): 1
- NAC: NAC State: None
- Load Balancing and Band Select: Client Load Balancing: , Client Band Select:

Refer to the exhibit. After a recent internal security audit, the network administrator decided to block all P2P-capable devices from the selected SSID. Which configuration setting must the administrator apply?

- A. Set the Wi-Fi Direct Client Policy to Not-Allow.
- B. Select a correctly configured Layer 2 ACL.
- C. Set the MFP Client Protection to Required.
- D. Set the P2P Block Action to Drop.

Correct Answer: A

Ciscoman021 (Highly Voted) 5 months, 3 weeks ago

Selected Answer: D

To block all P2P-capable devices from the selected SSID, the network administrator should set the P2P Block Action to "Drop".

P2P (Peer-to-Peer) traffic is often used by file sharing applications and other unauthorized software, which can pose a security risk to the network. By setting the P2P Block Action to "Drop", the network administrator can prevent P2P traffic from being transmitted over the selected SSID.

The other configuration settings listed are not directly related to blocking P2P traffic. Wi-Fi Direct Client Policy, for example, is used to control Wi-Fi Direct clients, while MFP (Management Frame Protection) Client Protection helps prevent forged management frames. A Layer 2 ACL (Access Control List) can be used to control access to network resources based on MAC addresses, IP addresses, and other criteria, but it is not specifically designed to block P2P traffic.

upvoted 6 times

spazzix (Most Recent) 3 weeks, 2 days ago

P2P block action only stops p2p traffic, not client association onto the WLAN.

Wi-Fi Direct Client Policy actually prevents the device from connecting to the WLAN.

If the question read: "...block all P2P traffic on the selected SSID." then D would be correct

But by definition, D is only relevant if P2P devices are actually on the WLAN.

upvoted 1 times

mda2h 1 month, 2 weeks ago

Selected Answer: D

Not sure about the full extent of Wi-Fi Direct capabilities but CISCO seems to want you to answer D

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-5/configuration-guide/b_cg75/b_cg75_chapter_01001011.pdf

upvoted 1 times



pikos1 3 months, 3 weeks ago



It is really CCNA question?



upvoted 3 times

[Removed] 2 months, 2 weeks ago

No, it is not
upvoted 1 times

  **studying_1** 3 months, 1 week ago
yes, these are real CCNA questions, study all the questions
upvoted 2 times



  **[Removed]** 2 months, 2 weeks ago
No, this is not a CCNA 200-301 question
upvoted 1 times



  **LekkiDee** 4 months ago
The correct answer is A. Set the Wi-Fi Direct Client Policy to Not-Allow.
If you read the question properly, they are asking how you can block all P2P-capable devices from the selected SSID. What they are saying is to prevent the devices from connecting to the SSID. In the responses below, It appears you are talking about blocking the peers from communicating via P2P.

see this link or read the shorter snippet further below.

https://content.cisco.com/content.sjs?uri=/searchable/chapter/content/en/us/td/docs/wireless/controller/7-5/configuration-guide/b_cg75/b_cg75_chapter_01000000.html.xml#:~:text=Click%20the%20Advanced%20tab.&text=From%20the%20Wi%2DFi%20Direct,to%20associate%20with%20the%20WLAN

upvoted 4 times

  **Ciscoman021** 6 months ago
Selected Answer: D
Disabled—Disables peer-to-peer blocking and bridges traffic locally within the controller whenever possible. This is the default value.
upvoted 1 times

  **AaronRow** 6 months, 1 week ago
Selected Answer: D
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-5/configuration-guide/b_cg75/b_cg75_chapter_01001011.pdf
upvoted 2 times

What is the primary purpose of a console port on a Cisco WLC?

- A. in-band management via an asynchronous transport
- B. in-band management via an IP transport
- C. out-of-band management via an asynchronous transport
- D. out-of-band management via an IP transport

Correct Answer: D

  **beerbiceps1** Highly Voted 5 months, 1 week ago

I paid to learn wrong info
upvoted 18 times

  **XuniLrve4** 2 months, 2 weeks ago

Well if it makes you feel any better, I have used several dumps from various sites (paid) and they all have wrong answers, but those questions we learn very well from searching material etc... and actually helps retain the material. At least here there are people who are willing and able to contribute.
upvoted 5 times

  **Ciscoman021** Highly Voted 5 months, 3 weeks ago

Selected Answer: C

The correct answer is C.

The console port on a Cisco Wireless LAN Controller (WLC) is used for out-of-band management via an asynchronous transport. The console port provides a direct, physical connection to the WLC and can be used for initial configuration, troubleshooting, and recovery in case of network connectivity issues.

In contrast, in-band management refers to the management of the WLC using the same network infrastructure that is used for user traffic. This is typically done via an IP transport, such as SSH or HTTPS, and allows administrators to manage the WLC remotely.

Therefore, options A and B are incorrect as they refer to in-band management methods. Option D is also incorrect as it refers to out-of-band management via an IP transport, which is not typically done using the console port.

upvoted 7 times

  **Cynthia2023** Most Recent 1 month ago

An asynchronous transport in networking refers to a communication method where data is transmitted and received in an asynchronous manner. In this context, the console port on a Cisco Wireless LAN Controller (WLC) is used for out-of-band management via an asynchronous transport, meaning that data is sent and received without a synchronized clock signal.

In simpler terms, "asynchronous" in networking means that data is sent and received without a fixed time interval or specific synchronization. This is commonly used in scenarios like console access to network devices, where the data is transmitted at the sender's pace and doesn't require a constant clock signal for synchronization. This makes it suitable for scenarios where there might be varying delays between transmissions.

upvoted 1 times

  **Toto86** 2 months, 2 weeks ago

Selected Answer: C

The correct answer ist C.

Console port: Used for out-of-band management, system recovery, and initial boot functions; asynchronous connection to a terminal emulator

Source: CCNA 200-301 Official Cert Guide, Volume 1 page 672

upvoted 3 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: C

The correct answer is "C"

upvoted 4 times

  **oatmealturkey** 7 months ago

Selected Answer: C

Console Port Connections

The controller has both EIA/TIA-232 asynchronous (RJ-45) and USB 5-pin mini Type B, 2.0 compliant serial console ports. The default parameters for the console ports are 9600 baud, 8 data bits, 1 stop bit, and no parity. The console ports do not support hardware flow control.

<https://www.cisco.com/c/en/us/td/docs/wireless/controller/5500/install/guide/ctrl5500.html>

upvoted 3 times

Which port type does a lightweight AP use to connect to the wired network when it is configured in local mode?

- A. EtherChannel
- B. access
- C. LAG
- D. trunk

Correct Answer: A

  **gewe** Highly Voted 6 months, 4 weeks ago

B , since in local mode all traffic goes tunnelled to WLC
upvoted 7 times

  **Rynurr** Highly Voted 6 months, 3 weeks ago

Selected Answer: B

Definitely "B"
upvoted 5 times

  **Da_Costa** Most Recent 3 weeks, 1 day ago

The autonomous AP must be connected in trunk mode in order to carry multiple VLANs,
upvoted 1 times

  **Da_Costa** 3 weeks, 1 day ago



Selected Answer: D

Truk is the right answer
upvoted 1 times

  **mrmanistheman** 4 months, 1 week ago

Selected Answer: B

The correct answer is B
upvoted 1 times

  **Ciscoman021** 5 months, 3 weeks ago

Selected Answer: B

When a lightweight AP is configured in local mode, it typically uses an "access" port to connect to the wired network.

An access port is a type of port on a network switch that is configured to carry traffic for only one VLAN. In this mode, the AP is essentially treated as a client device on the network, and it connects to a single VLAN on the switch. This allows the AP to receive configuration information and other management traffic from the controller, as well as to forward wireless traffic to the wired network.

upvoted 4 times

  **lucantonelli93** 6 months, 4 weeks ago

It's B , please correct
upvoted 5 times

  **oatmealturkey** 7 months ago

Selected Answer: B

While the Cisco WLCs always connect to 802.1Q trunks, Cisco lightweight APs do not understand VLAN tagging and must only be connected to the access ports of the neighbor switch.

<https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/69719-wlc-lwap-config.html>

Thanks to CAPWAP data tunnel between the LAP and the WLC, the LAP does not need to know anything about VLANs.


<https://study-ccna.com/lightweight-access-point-configuration/>

upvoted 4 times

Which step immediately follows receipt of the EAP success message when session resumption is disabled for an EAP-TLS connection?


- A. PMKID caching
- B. four-way handshake
- C. 802.1X authentication
- D. EAPOL-key frame

Correct Answer: C

 **lolungos** 2 months, 3 weeks ago

Selected Answer: D

This question is messed up. After the EAP Success on a EAP-TLS scenario you start the 4-way handshake which is made by 4 EAPOL-KEY frames... Knowing cisco I would go D, but as usual more than one answer may apply
upvoted 1 times

 **Ciscoman021** 5 months, 3 weeks ago

Selected Answer: C

When session resumption is disabled for an EAP-TLS connection, the step that immediately follows the receipt of the EAP success message is the 802.1X authentication. After the EAP success message is received, the authentication server sends an EAP success message to the supplicant indicating that the authentication was successful, and then the supplicant sends an EAPOL-logoff message to the authenticator to terminate the session.

After the session is terminated, the supplicant must re-authenticate the next time it tries to connect to the network. Therefore, the next step in the process is to initiate a new 802.1X authentication exchange between the supplicant and the authenticator, starting with the EAPOL-start frame.

Option C, 802.1X authentication, is the correct answer.

upvoted 2 times

 **loco_desk** 6 months, 1 week ago

When session resumption is disabled for an EAP-TLS connection, the step that immediately follows the receipt of the EAP success message is the generation of the Pairwise Master Key (PMK) and the initiation of the four-way handshake. Therefore, the correct answer is B. four-way handshake.
upvoted 3 times

 **Stichy007** 6 months, 3 weeks ago

answer is definitely D, smh

upvoted 2 times

 **Rynurr** 6 months, 3 weeks ago

Selected Answer: D

Yeah, "D" looks like correct answer

upvoted 2 times

 **gewe** 6 months, 4 weeks ago

you are right oatmeal turkey its DDDD

upvoted 3 times

 **oatmealturkey** 7 months ago

Selected Answer: D

802.1X is performed by EAP-TLS authentication, 802.1X is not a "step" so C is incorrect. According to this source, what follows the EAP Success message is a series of four EAPOL-Key frames known as the EAPOL-Key exchange:

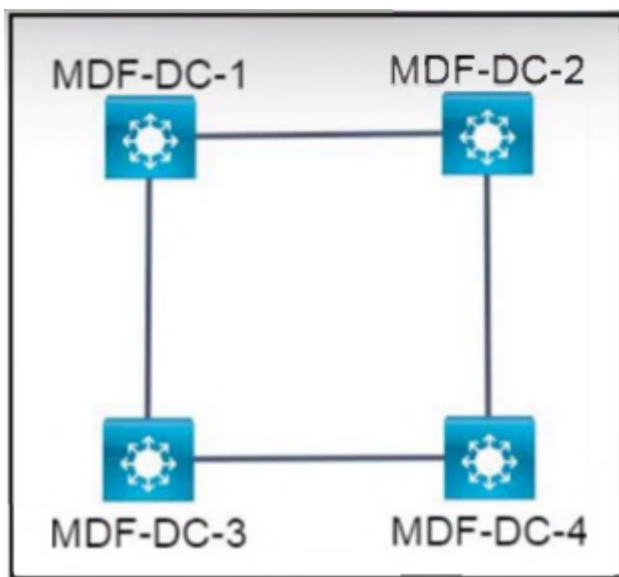
<https://www.securew2.com/blog/802-1x-eap-tls-authentication-flow-explained>

upvoted 3 times

 **jonathan126** 4 months, 3 weeks ago

according to your source, EAPOL-key frame is transferred during the four-way handshake process. The EAPOL-key frame is not a step, but the EAPOL-key frame exchange could be a step. So I think C and D are also incorrect, leaving option B the correct answer.

upvoted 3 times



Refer to the exhibit. All interfaces are in the same VLAN. All switches are configured with the default STP priorities. During the STP elections, which switch becomes the root bridge?

- A. MDF-DC-1: 08:E0:43:42:70:13
- B. MDF-DC-2: 08:0E:18:22:05:97
- C. MDF-DC-4: 08:E0:19:A1:B3:19
- D. MDF-DC-3: 08:0E:18:1A:3C:9D

Correct Answer: D

[Removed] 2 months, 2 weeks ago

Selected Answer: D

D. MDF-DC-3: 08:0E:18:1A:3C:9D

upvoted 2 times

Yannik123 4 months ago

Selected Answer: D

Given answer is right.

upvoted 3 times

purenuker 6 months, 1 week ago

Selected Answer: B

08:E0:43:42:70:13 - 400
 08:0E:18:22:05:97 - 164
 08:E0:19:A1:B3:19 - 610
 08:0E:18:1A:3C:9D - 283

Am I wrong ?

And if I am not - how it is possible "D" to be the correct answer ?!

upvoted 3 times

VarDav 3 weeks, 6 days ago

22 in hex is 34 in decimal

upvoted 1 times

rogi2023 5 months, 2 weeks ago

how did you calculate those numbers? In this scenario the lowest MAC wins - so look at the 4.th byte..in option B - 22 and in option D - 1A. 1A<22 so therefore D is correct.

upvoted 9 times

Balbes 1 month ago

1A = 26.

upvoted 1 times

Midus 6 months, 3 weeks ago

Correct : The default value is 32768, and the lowest number is preferred. In the case of a tie, the switch with the lowest MAC address will be selected.

upvoted 3 times

What are two port types used by a Cisco WLC for out-of-band management? (Choose two.)

- A. service
- B. console
- C. management
- D. distribution system
- E. redundant

Correct Answer: AB

🗨️ 👤 **[Removed]** 2 months, 2 weeks ago

Selected Answer: AD

Answers A and D

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/ports_and_interfaces.html

Controllers have two types of ports:

Distribution system ports

Service port

upvoted 1 times

🗨️ 👤 **no_blink404** 2 months, 2 weeks ago

Selected Answer: AB

Going with A & B.

In-band: connecting to a router via telnet or SSH. This implies that you have IP reachability to the device.

Out-of-band: no IP reachability to the device. This implies that you need to either physically connect a console cable to the device in order to access it or connect to the device via a terminal server. The terminal server in turn has a console cable connected to the router.

<https://learningnetwork.cisco.com/s/question/0D53i00000Kt4Q9CAJ/what-is-outofband-management-in-simple-words>

upvoted 3 times

🗨️ 👤 **HM01** 2 months, 3 weeks ago

Selected Answer: AB

CORRECT

upvoted 1 times

🗨️ 👤 **john1247** 3 months ago

Selected Answer: AC

i think A and C correct.

upvoted 1 times

What is a reason to implement LAG on a Cisco WLC?

- A. Allow for stateful failover between WLCs.
- B. Increase security by encrypting management frames.
- C. Increase the available throughput on the link.
- D. Enable the connected switch ports to use different Layer 2 configurations.

Correct Answer: A

 **oatmealturkey** Highly Voted  7 months ago

Selected Answer: C

A is incorrect, a LAG is configured on a single WLC's distribution system ports which are connected to a multilayer switch, not to another WLC. It increases available bandwidth between the wired and wireless networks.

The redundancy port of a WLC is for connecting to the redundancy port of another WLC for high availability deployment designs. There is only one redundancy port on a WLC, so LAG is unrelated to that.


upvoted 11 times

 **mrmanistheman** Most Recent  4 months, 1 week ago

Selected Answer: C

Most definitely C, to increase throughput.

upvoted 2 times

 **Ciscoman021** 5 months, 3 weeks ago

Selected Answer: C

The reason to implement LAG (Link Aggregation Group) on a Cisco WLC (Wireless LAN Controller) would be C. Increase the available throughput on the link.

LAG combines multiple physical links into a single logical link, increasing the available bandwidth and improving network performance. By using LAG, multiple links can be used simultaneously to transmit and receive data, which allows the WLC to provide higher throughput than a single link could provide. This is especially important in high-density WLAN environments where there are many wireless clients connecting to the network and generating a large amount of traffic.

upvoted 3 times

 **DINVIS** 6 months, 3 weeks ago

its definitely C

upvoted 1 times

 **Rynurr** 6 months, 3 weeks ago

Selected Answer: C

"Increase the available throughput on the link."
for sure

upvoted 1 times

 **lucantonelli93** 6 months, 4 weeks ago

Selected Answer: C


It's C , please correct the answer

upvoted 2 times

 **lucantonelli93** 6 months, 4 weeks ago

It's C , please correct the answer

upvoted 1 times

 **drewsped** 6 months, 4 weeks ago

Selected Answer: C

Ccccccc

upvoted 1 times

 **gewe** 6 months, 4 weeks ago

C for sure

upvoted 2 times

A wireless access point is needed and must meet these requirements:

- “zero-touch” deployed and managed by a WLC
- process only real-time MAC functionality
- used in a split-MAC architecture

Which access point type must be used?

- A. mesh
- B. autonomous
- C. lightweight
- D. cloud-based

Correct Answer: C

  **UAE7** 6 months, 3 weeks ago

answer is correct

<https://www.cisco.com/c/en/us/support/docs/wireless/aironet-1200-series/70278-lap-faq.html>

upvoted 3 times

Which interface is used for out-of-band management on a WLC?

- A. management
- B. virtual
- C. dynamic
- D. service port

Correct Answer: D

 **shaney67** 3 weeks ago

The interface used for out-of-band management on a Wireless LAN Controller (WLC) is:

A. management

Explanation:

The management interface on a WLC is specifically designed for out-of-band management purposes. It's used to access the controller's management functions, configure settings, monitor performance, and perform various administrative tasks.

The other options:


B. virtual: The virtual interface is typically used to represent a logical interface, such as a VLAN interface, within the context of the controller. It's not primarily used for direct out-of-band management.

C. dynamic: "Dynamic" isn't a specific type of interface on a WLC, and it doesn't relate to out-of-band management.

D. service port: The service port on a WLC is used for normal access-point traffic, not for out-of-band management.

In summary, the correct interface used for out-of-band management on a WLC is the A. management interface.

upvoted 1 times

 **Goena** 6 months, 2 weeks ago

Selected Answer: D

Out of band is service-port interface

In band is management interface



upvoted 4 times



```
SW2
vtp domain cisco
vtp mode transparent
vtp password ciscotest
interface fastethernet0/1
  description connection to sw1
  switchport mode trunk
  switchport trunk encapsulation dot1q
```

Refer to the exhibit. How does SW2 interact with other switches in this VTP domain?

- A. It transmits and processes VTP updates from any VTP clients on the network on its trunk ports.
- B. It processes VTP updates from any VTP clients on the network on its access ports.
- C. It receives updates from all VTP servers and forwards all locally configured VLANs out all trunk ports.
- D. It forwards only the VTP advertisements that it receives on its trunk ports.

Correct Answer: D

  **[Removed]** 2 months, 1 week ago
VTP is not part of CCNA 200-301
upvoted 1 times

  **VictorCisco** 5 months, 2 weeks ago
If a switch make advertisements only via trunk ports??
upvoted 1 times

  **RidzV** 6 months, 1 week ago

Selected Answer: D

Each switch can use one of four different VTP modes:



VTP client mode – a switch using this mode can't change its VLAN configuration. That means that a VTP client switch cannot create or delete VLANs. However, received VTP updates are processed and forwarded.

VTP server mode – a switch using this mode can create and delete VLANs. A VTP server switch will propagate VLAN changes. This is the default mode for Cisco switches.

VTP transparent mode – a switch using this mode doesn't share its VLAN database, but it forwards received VTP advertisements. You can create and delete VLANs on a VTP transparent switch, but these changes will not be sent to other switches.

VTP mode off – similar to VTP transparent mode, with a difference that a switch using this mode will not forward received VTP updates. This command is supported only in VTP V3.

upvoted 4 times

  **UAE7** 6 months, 3 weeks ago
answer is correct
<https://study-ccna.com/vtp-modes/>
upvoted 1 times

A network engineer is upgrading a small data center to host several new applications, including server backups that are expected to account for up to 90% of the bandwidth during peak times. The data center connects to the MPLS network provider via a primary circuit and a secondary circuit. How does the engineer inexpensively update the data center to avoid saturation of the primary circuit by traffic associated with the backups?

- A. Assign traffic from the backup servers to a dedicated switch.
- B. Place the backup servers in a dedicated VLAN.
- C. Advertise a more specific route for the backup traffic via the secondary circuit.
- D. Configure a dedicated circuit for the backup traffic.

Correct Answer: C

 **aynur_ganbarova** 1 month, 3 weeks ago

The correct answer is B. Place the backup servers in a dedicated VLAN.


Placing the backup servers in a dedicated VLAN allows for the segregation and control of the backup traffic within the data center. This solution helps prevent saturation of the primary circuit by dedicating a specific VLAN for the backup traffic and allowing bandwidth management, traffic isolation, and the implementation of Quality of Service (QoS) policies.

upvoted 1 times

 **[Removed]** 2 months, 2 weeks ago

This is not CCNA 200-301

upvoted 1 times

 **StingVN** 3 months, 3 weeks ago

Selected Answer: C

To inexpensively update the data center and avoid saturation of the primary circuit by traffic associated with the backups, the network engineer can implement the following solution:

C. Advertise a more specific route for the backup traffic via the secondary circuit.

By advertising a more specific route for the backup traffic via the secondary circuit, the engineer can ensure that the backup traffic is directed through the secondary circuit instead of overwhelming the primary circuit. This can be achieved by configuring the routing protocols or static routes to prioritize the secondary circuit for the backup traffic.


This approach allows the engineer to leverage the existing infrastructure and circuits without the need for additional dedicated equipment or circuits, making it a cost-effective solution. It effectively separates the backup traffic from other data center traffic and ensures efficient utilization of the available network resources.

upvoted 3 times

 **MassNastty1** 3 months, 3 weeks ago

Answer C is correct since it is the most inexpensive option with it being a simple, IP route specification. Everything else is either more time consuming or requires more overhead costs.

upvoted 1 times

 **Yannik123** 4 months ago

I think that all the given answers could be correct. Can anyone explain?

upvoted 1 times


```

R1
interface GigabitEthernet0/1
 ip address 192.168.12.1 255.255.255.128
 no shutdown
router ospf 1
 network 192.168.12.1 0.0.0.0 area 1

R2
interface GigabitEthernet0/1
 ip address 192.168.12.2 255.255.255.128
 no shutdown

```

Refer to the exhibit. A network engineer started to configure two directly-connected routers as shown. Which command sequence must the engineer configure on R2 so that the two routers become OSPF neighbors?

- A. interface GigabitEthernet0/1
ip ospf 1 area 1
- B. router ospf 1
network 192.168.12.1 0.0.0.0 area 1
- C. interface GigabitEthernet0/1
ip ospf 1 area 0
- D. router ospf 1
network 192.168.12.0 0.0.0.127 area 0

Correct Answer: D

 **gewe** Highly Voted 7 months ago

wrong answer as area is 0...
answer A is correct
upvoted 11 times

 **proshant06** 2 months ago


Why area 0 is wrong. Would u plz explain?
upvoted 1 times

 **MadKisa** 2 months ago

Areas must match
upvoted 1 times

 **MassNastty1** Most Recent 3 months, 3 weeks ago

A and C are literally contain incorrect syntax commands. The correct syntax is Router OSPF (Priority Number), followed by Network (IP Address) (Wildcard Mask) (Area ID). The answer D indicates that this is a point to multipoint connection but the exhibit shows that it is a point to point network. Therefore, B seems to be the correct answer. The wildcard subnet mask must be the same for the two routers to establish a neighbor adjacency.
upvoted 1 times

 **MassNastty1** 3 months, 3 weeks ago

Also, the exhibit output shows that OSPF was configured globally, not via Interface configuration.
upvoted 1 times

 **studying_1** 3 months, 2 weeks ago

you can configure ospf on the interface, and the area shown in the exhibit is 1, the command is (ip ospf process-id area area number) A is correct
B can't be correct, because ospf uses a wild mask so in B it represents a host ip address, which is not the same as the interface's.
upvoted 3 times

 **Swiz005** 5 months ago

Selected Answer: A

Ignore my earlier comment. OSPF can be enabled on an interface, so the correct answer is A
upvoted 1 times

 **perri88** 3 months ago

why not B?
upvoted 1 times

  **eldritchone** 2 months, 1 week ago

B is incorrect because the network statement uses the wildcard mask 0.0.0.0 which as a normal mask is 255.255.255.255.

A mask of 255.255.255.255 specifies a single ip address, and the ip address in the command is not the ip address of R2's G0/1 interface.

upvoted 1 times

  **Swiz005** 5 months ago

Selected Answer: B

Definitely B

upvoted 3 times

  **eldritchone** 2 months, 1 week ago

B is incorrect because the network statement uses the wildcard mask 0.0.0.0 which as a normal mask is 255.255.255.255.

A mask of 255.255.255.255 specifies a single ip address, and the ip address in the command is not the ip address of R2's G0/1 interface.

upvoted 1 times

  **Ciscoman021** 5 months, 2 weeks ago

Selected Answer: A

A is correct.

upvoted 2 times

  **VictorCisco** 5 months, 2 weeks ago

Selected Answer: A

it is possible to enable OSPF on an interface.

Ip address is already configured. So it is just needed to put the interfece in the same area as the neighbor.

A is correct.

upvoted 1 times

  **mustdoit** 6 months ago

Selected Answer: A

B isn't correct, they won't become neighbors.

Not even to mention C and D which use different area.

A is the only answer that establishes neighbor relationship.

upvoted 2 times

  **perri88** 3 months ago

why B isn't correct?

upvoted 1 times

  **DavidCisco** 6 months, 1 week ago

Selected Answer: A

To configure ospf in the interface

ip ospf process-id area area-id



so A is correct

upvoted 3 times

  **rogi2023** 5 months, 2 weeks ago



I agree, answer A is the only which makes sense, BUT the question is IF this cmd also enables the ospf proces. without ospf routing protocol enabled it won't work. But i just dig to deep..Definitely the A answer is the one which has no errors.

upvoted 1 times

  **rogi2023** 5 months, 2 weeks ago

My BAD, the cmd itself on interface will also start the ospf proces. I just tried in GNS3. :-)

upvoted 1 times



  **papinski** 6 months, 2 weeks ago

Selected Answer: B

Definitely not D

B includes the network

upvoted 3 times


  **janekk** 6 months, 2 weeks ago

Not B (correct A)

bad ip addr:

network 192.168.12.1 0.0.0.0 area 1

upvoted 9 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: B

Must be in same area 1, so "B".

A and C doesn't make sense

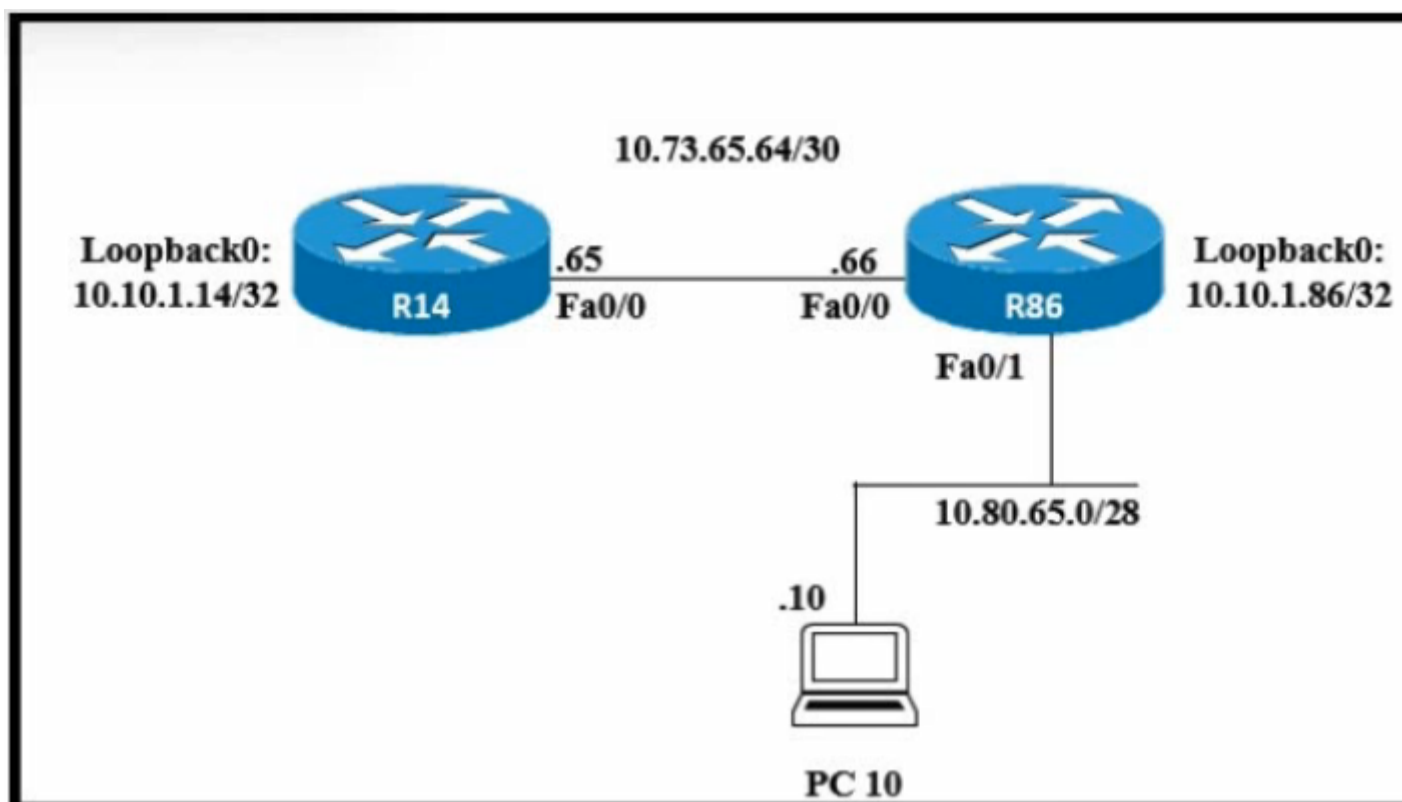
upvoted 1 times

```
R1# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
default
       U - per-user static route, o - ODR
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O    10.0.1.3/32 [110/100] via 10.0.1.100, 00:39:08, Serial0
C    10.0.1.0/24 is directly connected, Serial0
O    10.0.1.5/32 [110/5] via 10.0.1.50, 00:39:08, Gigabit Ethernet 0/0
D    10.0.1.4/32 [110/10] via 10.0.1.4, 00:39:08, Gigabit Ethernet 0/0
```

Refer to the exhibit. What does route 10.0.1.3/32 represent in the routing table?

- A. all hosts in the 10.0.1.0 subnet
- B. a single destination address
- C. the source 10.0.1.100
- D. the 10.0.0.0 network

Correct Answer: B



Refer to the exhibit. Router R14 is in the process of being configured. Which configuration must be used to establish a host route to a PC 10?

- A. `ip route 10.80.65.10 255.255.255.254 10.80.65.1`
- B. `ip route 10.80.65.10 255.255.255.255 10.73.65.66`
- C. `ip route 10.73.65.66 0.0.0.255 10.80.65.10`
- D. `ip route 10.73.65.66 255.0.0.0 10.80.65.10`

Correct Answer: D

Vikramaditya_J Highly Voted 4 months, 2 weeks ago

Selected Answer: B

A host route always uses /32 (=255.255.255.255) subnet mask and it's syntax is:

`ip route <destination-ip-address> 255.255.255.255 <next-hop-ip-address>`

For example, to create a host route for the host with IP address 192.168.1.100 with a next-hop router IP address of 10.1.1.1, the following command can be used:

`ip route 192.168.1.100 255.255.255.255 10.1.1.1`

upvoted 5 times

[Removed] Most Recent 2 months, 2 weeks ago

Selected Answer: B

B is correct - To reach host 10.80.65.10 (a host route must be a /32 so 255.255.255.255), you send traffic to the next hop which is 10.73.65.66

upvoted 1 times

Da_Costa 2 months, 4 weeks ago

I fear for this answer, I don't know

upvoted 1 times

kennie0 3 months, 3 weeks ago

i cant believe I pay for these answers picked by the owner of this site

upvoted 2 times

learntstuff 1 month, 4 weeks ago

stop complaining and research the answer. we all know some of the answers are wrong

upvoted 1 times

Tdawg1968 4 months ago

B - Route to host/Mask through first hop IP

upvoted 2 times

RidzV 6 months, 1 week ago

Selected Answer: B

No brainier. Route for specific Destination address should have mask of 255.255.255.255

upvoted 2 times

🗨️ **bisiyemo1** 6 months, 1 week ago

Selected Answer: B

It is B please.
upvoted 1 times

🗨️ **papinski** 6 months, 2 weeks ago

Selected Answer: B

First hop is .66
upvoted 1 times

🗨️ **tal10** 6 months, 3 weeks ago

Selected Answer: B

b is the correct answer
upvoted 1 times

🗨️ **Rynurr** 6 months, 3 weeks ago

Selected Answer: B

"B" is the correct answer
upvoted 1 times

🗨️ **lucantonelli93** 6 months, 4 weeks ago

Selected Answer: B

It's B ! Please correct this answer
upvoted 1 times

🗨️ **lucantonelli93** 6 months, 4 weeks ago

It's B ! Please correct this answer
upvoted 1 times

🗨️ **drewsped** 6 months, 4 weeks ago

Bbbbbbb

Answers for recent batch of questions are dub
upvoted 2 times

🗨️ **j1mlawton** 7 months ago

Selected Answer: B

BBBBBB
upvoted 2 times

🗨️ **ahmt** 7 months ago

Selected Answer: B

B is correct
ip route 10.80.65.10 255.255.255.255 10.73.65.66
upvoted 3 times

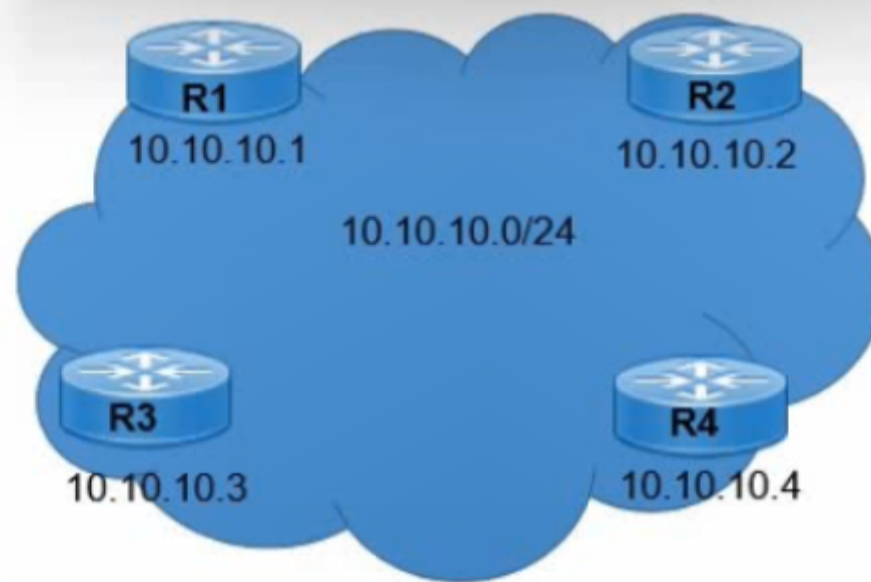
🗨️ **oatmealturkey** 7 months ago

Selected Answer: B

How on Earth did you get D
upvoted 3 times

🗨️ **gewe** 7 months ago

B is correct
upvoted 4 times



```
R1# show ip route
C    1.0.0.0/8 is directly connected, Loopback0
C    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O    10.10.10.3/32 [110/100] via 10.10.10.3, 00:39:08, GigabitEthernet0/3
C    10.10.10.0/24 is directly connected, GigabitEthernet0/0
O    10.10.10.2/32 [110/5] via 10.10.10.2, 00:39:08, GigabitEthernet0/2
R    10.10.10.4/32 [120/10] via 10.10.10.4, 00:39:08, GigabitEthernet0/4
```

Refer to the exhibit. Which next-hop IP address has the least desirable metric when sourced from R1?

- A. 10.10.10.4
- B. 10.10.10.5
- C. 10.10.10.3
- D. 10.10.10.2

Correct Answer: B

oatmealturkey Highly Voted 7 months ago

Selected Answer: C

10.10.10.5 is not even in the topology diagram or shown as a next hop in the routing table at all so how can it be B???

upvoted 12 times

Rynurr Highly Voted 6 months, 3 weeks ago

Selected Answer: C

Yeah "C".
the least desirable metric = highest metric in OSPF

upvoted 7 times

blue91235 3 months, 3 weeks ago

For the ospf only , or in general ?

upvoted 2 times

dropspablo Most Recent 2 months, 2 weeks ago

Selected Answer: A

(I choose the letter A because RIP hops metric is less desirable than OSPF cost metric.)

"When a single routing protocol learns multiple routes to the same subnet, the metric tells it which route is best. However, when two different routing protocols learn routes to the same subnet, because each routing protocol's metric is based on different information, IOS cannot compare the metrics. For example, OSPF might learn a route to subnet 10.1.1.0 with metric 101, and EIGRP might learn a route to 10.1.1.0 with metric 2,195,416, but the EIGRP-learned route might be the better route—or it might not. There is simply no basis for comparison between the two metrics.

When IOS must choose between routes learned using different routing protocols, IOS uses a concept called administrative distance. (OCG v1 Chapter 19: Understanding OSPF Concepts)"

upvoted 2 times

Friday_Night 3 months, 3 weeks ago

it's a lot better if these so called "experts" don't put an answer at all. let the community decide the best answer. I'm assuming the questions are from cisco but the answers are not

upvoted 2 times

🗨️ 👤 **Rydaz** 4 months ago

why not A? because its RIP AD of 120 so it's the highest, wich means least desirable. ?

upvoted 3 times

🗨️ 👤 **Njavwa** 4 months, 4 weeks ago

Selected Answer: C

$[110/100] = 100 = AD$, $100 = \text{metric}$

the more we think about it the more it doesn't make much sense.

least should be the one with the highest Metric... all we wanted was to much a normal revision with less debate its so unfortunate that ITEXAMS completes things

upvoted 1 times

🗨️ 👤 **Njavwa** 4 months, 4 weeks ago

$110 = AD$

$100 = \text{metric}$

upvoted 1 times

🗨️ 👤 **Dutch012** 6 months, 1 week ago

Selected Answer: D

Its D, D's metric is 5 which is the least desirable

upvoted 6 times

🗨️ 👤 **hamish88** 5 months, 1 week ago

You made my day. :) The lower the number, the better

upvoted 2 times

🗨️ 👤 **Peter_panda** 6 months, 1 week ago

Could be A. It does not say anywhere that we are referring only to OSPF learned routes, but only with OSPF routes we can compare metrics. The RIP route is the least desirable overall (higher AD), but its metric cannot be compared with anything (there are no other RIP routes).

upvoted 3 times

🗨️ 👤 **rogi2023** 5 months, 2 weeks ago

I agree, very stupid "cisco" kind question. I red the question again and again to find the solution key. The RIP route 120/10 is for sure the worst with 10hops..but I just play dum and assume they wanna know the highest # after "/" so I would go with answer "C". I hope not to see this question with these wording on exam.

upvoted 2 times

🗨️ 👤 **Stichy007** 6 months, 3 weeks ago

Selected Answer: C

lols this is hilarious, ans is c

upvoted 2 times

🗨️ 👤 **lucantonelli93** 6 months, 4 weeks ago

Selected Answer: C

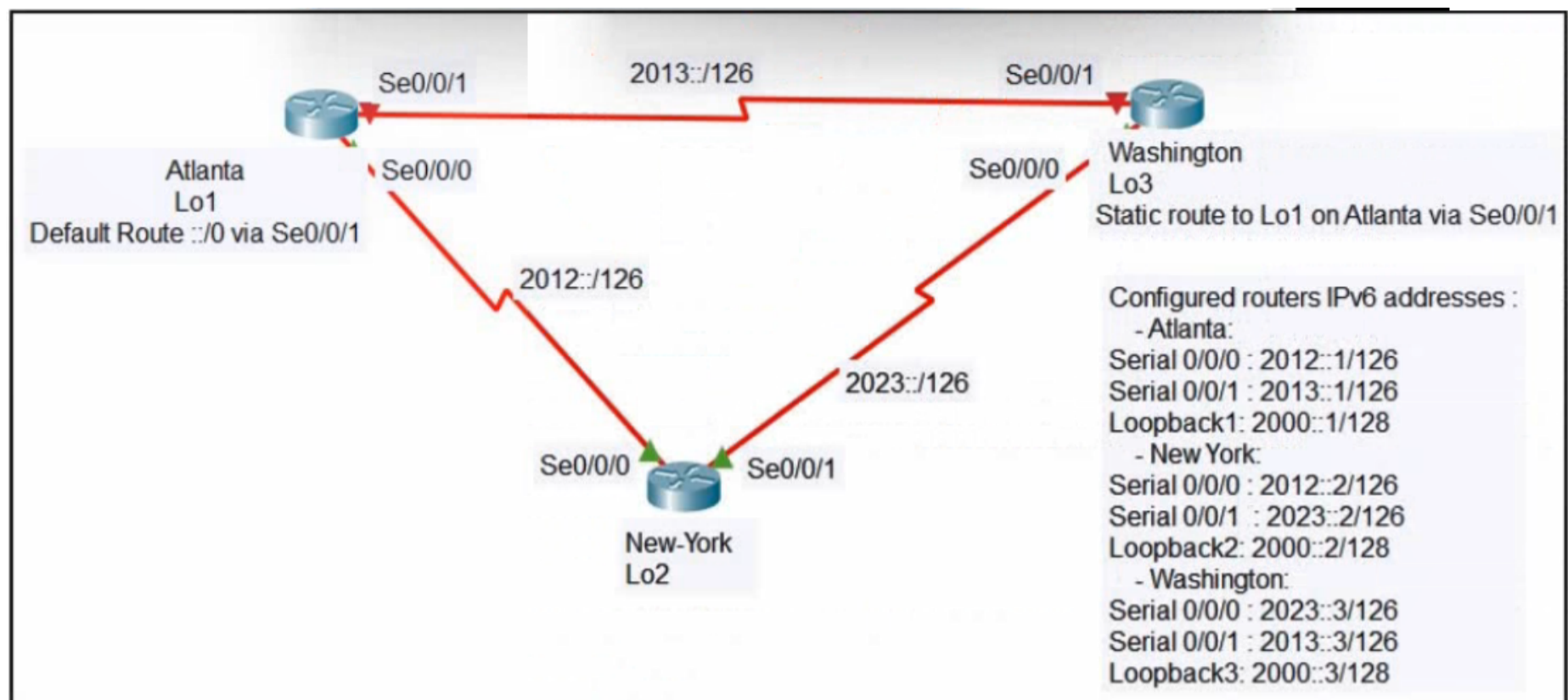
It's C the answer , please correct

upvoted 2 times

🗨️ 👤 **gewe** 6 months, 4 weeks ago

option C has highest metric.

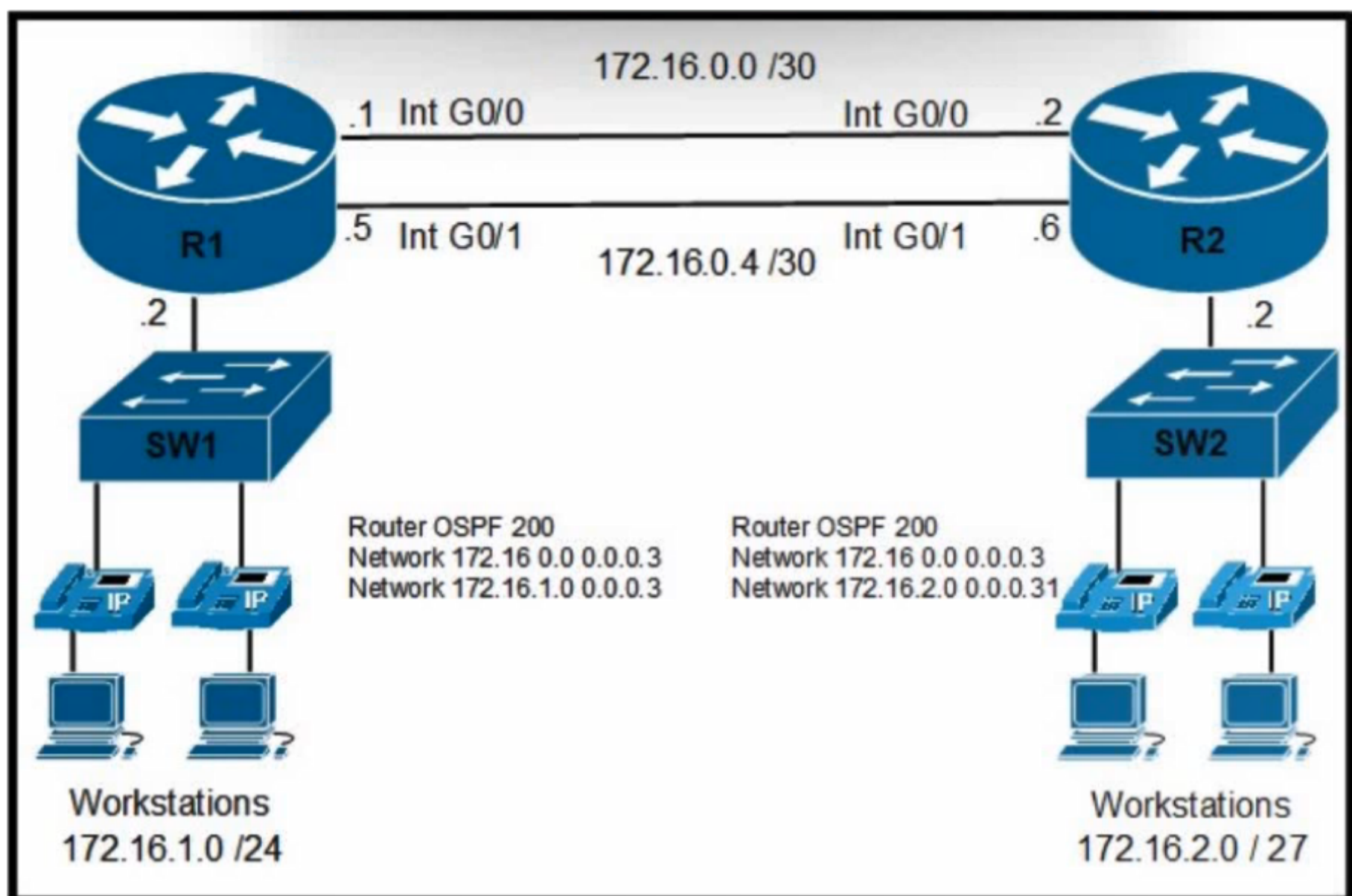
upvoted 2 times



Refer to the exhibit. The New York router must be configured so that traffic to 2000::1 is sent primarily via the Atlanta site, with a secondary path via Washington that has an administrative distance of 2. Which two commands must be configured on the New York router? (Choose two.)

- A. ipv6 route 2000::1/128 2012::1
- B. ipv6 route 2000::1/128 2012::1 5
- C. ipv6 route 2000::1/128 2012::2
- D. ipv6 route 2000::1/128 2023::2 5
- E. ipv6 route 2000::1/128 2023::3 2

Correct Answer: AE



Refer to the exhibit. The primary route across Gi0/0 is configured on both routers. A secondary route must be configured to establish connectivity between the workstation networks. Which command set must be configured to complete this task?

A. R1 -
`ip route 172.16.2.0 255.255.255.248 172.16.0.5 110`

R2 -
`ip route 172.16.1.0 255.255.255.0 172.16.0.6 110`

B. R1 -
`ip route 172.16.2.0 255.255.255.240 172.16.0.2 113`

R2 -
`ip route 172.16.1.0 255.255.255.0 172.16.0.1 114`

C. R1 -
`ip route 172.16.2.0 255.255.255.224 172.16.0.6 111`

R2 -
`ip route 172.16.1.0 255.255.255.0 172.16.0.5 112`


D. R1 -
`ip route 172.16.2.0 255.255.255.240 172.16.0.5 89`

R2 -
`ip route 172.16.1.0 255.255.255.0 172.16.0.6 89`

Correct Answer: C


Danthemann 1 month ago

Honestly you only have to remember dinner masks here for the answer of /24 and /27
 upvoted 1 times

 **enzo86** 5 months, 1 week ago

c 100%

upvoted 3 times

 **wondaah** 6 months, 1 week ago

Selected Answer: C

Answer is C: only one with the correct subnetmask

upvoted 4 times

DRAG DROP

```



Router1#show ip route
Gateway of last resort is 10.10.11.2 to network 0.0.0.0
 209.165.200.0/27 is subnetted, 1 subnets
 B    209.165.200.224 [20/0] via 10.10.12.2, 03:22:14
 209.165.201.0/27 is subnetted, 1 subnets
 B    209.165.201.0 [20/0] via 10.10.12.2, 02:26:33
 209.165.202.0/27 is subnetted, 1 subnets
 B    209.165.202.128 [20/0] via 10.10.12.2, 02:26:03
 10.0.0.0/8 is variably subnetted, 10 subnets, 4 masks
 O    10.10.13.0/25 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
 O    10.10.13.128/28 [110/2] via 10.10.10.5, 00:00:12, GigabitEthernet0/1
 O    10.10.13.144/28 [110/2] via 10.10.10.9, 00:01:57, GigabitEthernet0/2
 O    10.10.13.160/29 [110/2] via 10.10.10.5, 00:00:12, GigabitEthernet0/1
 O    10.10.13.208/29 [110/2] via 10.10.10.13, 00:01:57, GigabitEthernet0/3
 S*  0.0.0.0/0 [1/0] via 10.10.11.2
    
```



Refer to the exhibit. Drag and drop the destination IPs from the left onto the paths to reach those destinations on the right.

1.1.1.1	Router2
10.10.13.126	Router3
10.10.13.129	Router5
10.10.13.150	Internet cloud
10.10.13.209	Router4
209.165.200.30	MPLS cloud



Correct Answer:



1.1.1.1	10.10.13.126
10.10.13.126	10.10.13.129
10.10.13.129	10.10.13.209
10.10.13.150	1.1.1.1
10.10.13.209	10.10.13.150
209.165.200.30	209.165.200.30



  **mda2h** 1 month, 2 weeks ago
correct
upvoted 1 times

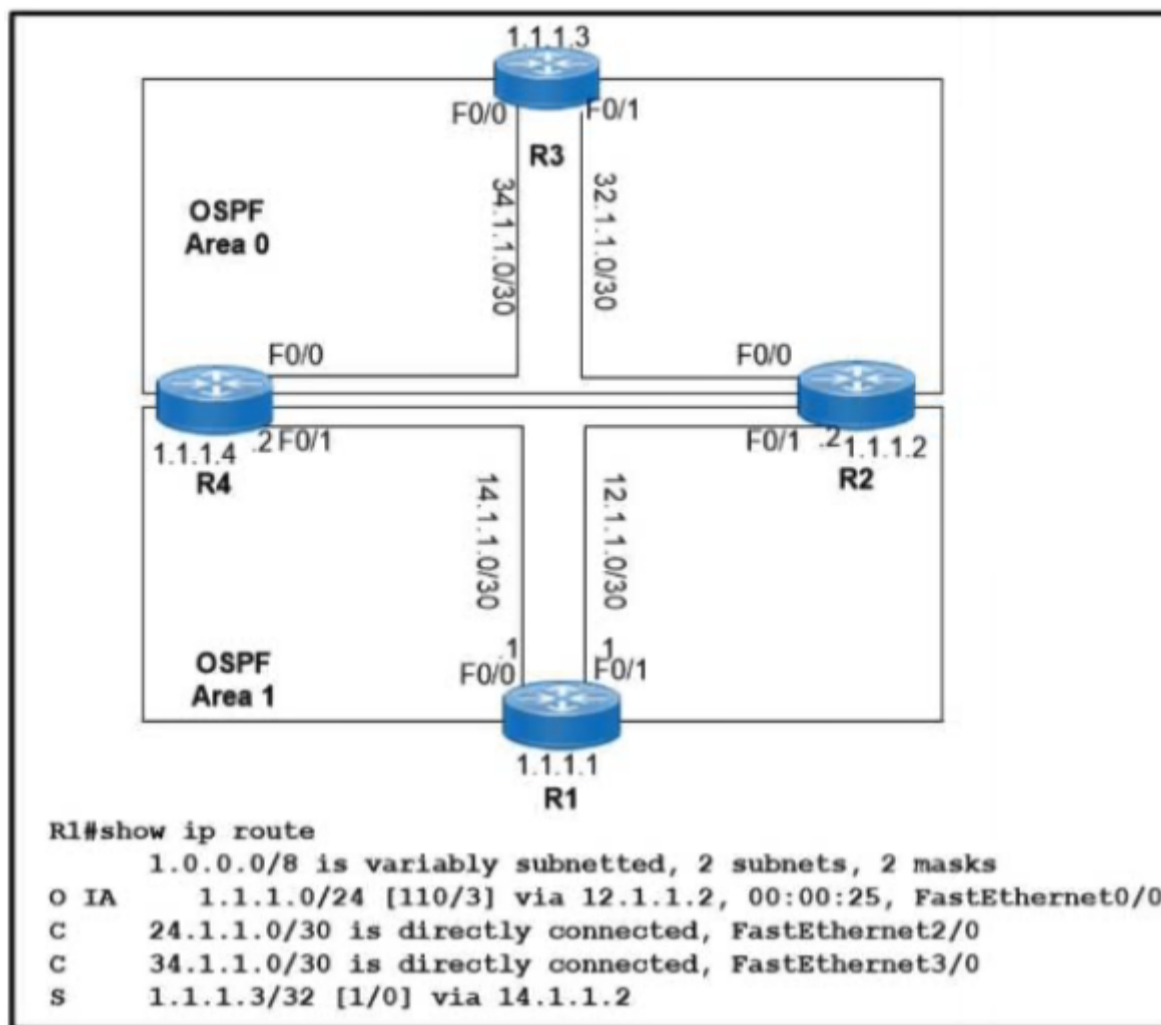
  **enzo86** 5 months, 1 week ago
IS CORRECT .
upvoted 2 times

  **Dutch012** 6 months, 2 weeks ago
The answers are correct
upvoted 3 times

  **rogi2023** 5 months, 2 weeks ago
Not really. The route to 209.165.200.30 would go through Internet again, check out the routing table. The parent network C-class netw is subnetted with one subnet mask/27 and therefore is written 209.165.200.0/27 but actually the netw which leads to MPLS cloud is 209.165.200.224/27. I hope not to see such errors on the exam.
upvoted 12 times

  **mda2h** 1 month, 2 weeks ago
Valid point!
upvoted 1 times

  **perri88** 3 months ago
good point
upvoted 1 times



Refer to the exhibit. Which two values does router R1 use to determine the best path to reach destinations in network 1.0.0.0/8? (Choose two.)

- A. lowest cost to reach the next hop
- B. highest administrative distance
- C. lowest metric
- D. highest metric
- E. longest prefix match

Correct Answer: BC

oatmealturkey Highly Voted 7 months ago

Highest administrative distance is never used to select the best route, we want lowest administrative distance.
upvoted 12 times

Luinus Highly Voted 6 months, 1 week ago

Selected Answer: CE

I remember this question in my exam the answer is C and E
upvoted 9 times

ac89l Most Recent 4 months, 1 week ago

Why not A ?
upvoted 3 times

[Removed] 2 months, 1 week ago

I would say A too. OSPF uses cost as a metric
upvoted 1 times

spazzix 3 weeks, 2 days ago

It's the classic CCNA gotcha: take something correct and add an incorrect element.

Lowest cost would be a great answer for an OSPF environment, but lowest cost to the *next hop* doesn't help us; the total cost for the route could be bad.

upvoted 1 times

mda2h 1 month, 2 weeks ago

Same question, why not A?
For me lowest cost refers to both AD and metric ...

upvoted 1 times

🗨️ 👤 **ViKing300** 5 months ago

Selected Answer: AE

i think is A and E
upvoted 3 times

🗨️ 👤 **hamish88** 4 months, 4 weeks ago

Distance to the next hop is not of any importance to us.
upvoted 2 times

🗨️ 👤 **JJY888** 6 months, 1 week ago

Selected Answer: CE

I can't believe they chose the highest administrative distance. SMH.
upvoted 5 times

🗨️ 👤 **tal10** 6 months, 3 weeks ago

Selected Answer: CE

lowest metric and best prefix
upvoted 4 times

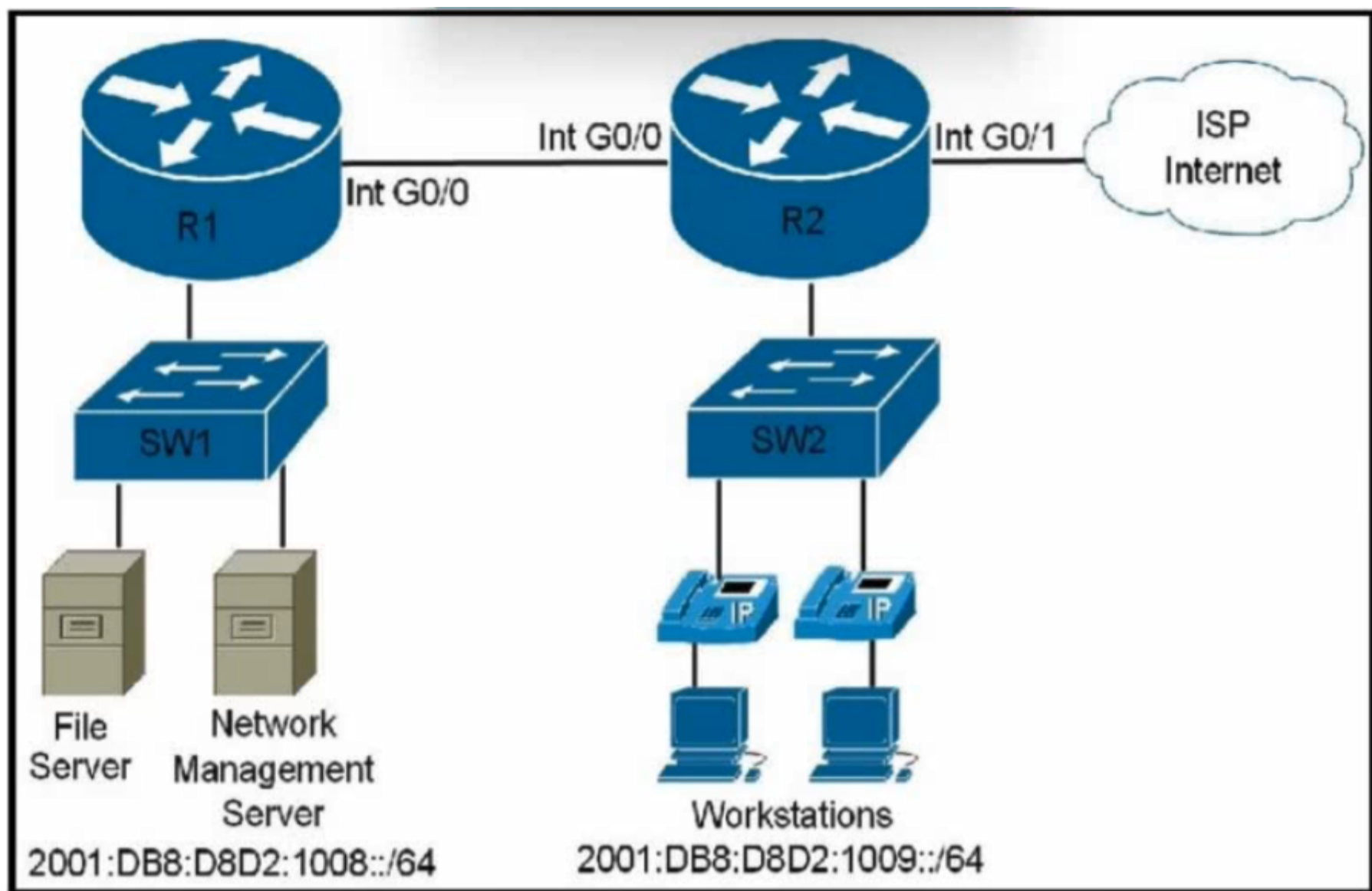
🗨️ 👤 **Rynurr** 6 months, 3 weeks ago

Selected Answer: CE

IMO should be "CE"
upvoted 3 times

🗨️ 👤 **gewe** 6 months, 4 weeks ago

lowest metric, lowest AD that's it
upvoted 2 times



Refer to the exhibit. A public IPv6 address must be configured for internet access. Which command must be configured on the R2 WAN interface to the service provider?

- A. ipv6 address fe80::/10
- B. ipv6 address 2001:db8:433:37:7710:ffff:ffff:ffff/64 anycast
- C. ipv6 address 2001:db8:123:45::4/64
- D. ipv6 address fe80::260:3EFF:FE11:6770 link-local

Correct Answer: C

wondaah Highly Voted 6 months, 1 week ago

no brainer if you got this far :)
upvoted 5 times

mezanmi Most Recent 6 months, 1 week ago

Only one syntax is correct.
upvoted 2 times

DRAG DROP

```

Router1#show ip route
Gateway of last resort is 10.10.11.2 to network 0.0.0.0

 209.165.200.0/27 is subnetted, 1 subnets
B   209.165.200.224 [20/0] via 10.10.12.2, 06:08:59
 209.165.201.0/27 is subnetted, 1 subnets
B   209.165.201.0 [20/0] via 10.10.12.2, 05:13:18
 209.165.202.0/27 is subnetted, 1 subnets
B   209.165.202.128 [20/0] via 10.10.12.2, 05:12:48
10.0.0.0/8 is variably subnetted, 9 subnets, 4 masks
C   10.10.10.0/28 is directly connected, GigabitEthernet0/0
C   10.10.11.0/30 is directly connected, FastEthernet2/0
C   10.10.12.0/30 is directly connected, GigabitEthernet0/1
O   10.10.13.0/25 [110/2] via 10.10.10.1, 00:00:03, GigabitEthernet0/0
O   10.10.13.128/28 [110/2] via 10.10.10.1, 00:00:03, GigabitEthernet0/0
O   10.10.13.144/28 [110/2] via 10.10.10.1, 00:00:03, GigabitEthernet0/0
O   10.10.13.160/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O   10.10.13.208/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O   10.10.13.252/30 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
S*  0.0.0.0/0 [1/0] via 10.10.11.2
    
```

Refer to the exhibit. Drag and drop the subnet masks from the left onto the corresponding subnets on the right. Not all subnet masks are used.

255.255.248.0	10.10.13.0
255.255.255.128	10.10.13.128
255.255.255.224	10.10.13.160
255.255.255.240	10.10.13.252
255.255.255.248	
255.255.255.252	

Correct Answer:

255.255.248.0	255.255.255.252
255.255.255.128	255.255.255.224
255.255.255.224	255.255.255.248
255.255.255.240	255.255.255.128
255.255.255.248	
255.255.255.252	

  **gewe** Highly Voted 6 months, 4 weeks ago



255.255.255.128
255.255.255.240
255.255.255.248
255.255.255.252
upvoted 44 times

  **Simon_1103** Highly Voted 6 months, 1 week ago

10.10.13.0 --> 255.255.255.128
10.10.13.128 --> 255.255.255.240
10.10.13.160 --> 255.255.255.248
10.10.13.252 --> 255.255.255.252
upvoted 10 times

  **Tdawg1968** Most Recent 4 months ago


Yikes!
upvoted 2 times

  **Njavwa** 4 months, 4 weeks ago

10.10.13.0 does not even have an answer listed
upvoted 1 times

  **[Removed]** 2 months, 2 weeks ago

Yes, 10.10.13.0/25
upvoted 1 times

  **rogi2023** 5 months, 2 weeks ago



I am just wondering, if someone would just memorize the answers provided by authors/admins of the page if they would successfully pass the exam. Here are just too many errors.
upvoted 5 times

  **[Removed]** 2 months, 2 weeks ago

No, they wouldn't :-)
upvoted 1 times

  **Peter_panda** 4 months, 4 weeks ago

under 50%... :-)
upvoted 2 times

  **rogi2023** 5 months, 2 weeks ago

So please, at least fix those ones which all commented as errors. PLEASE.
upvoted 1 times

  **JJY888** 6 months, 1 week ago

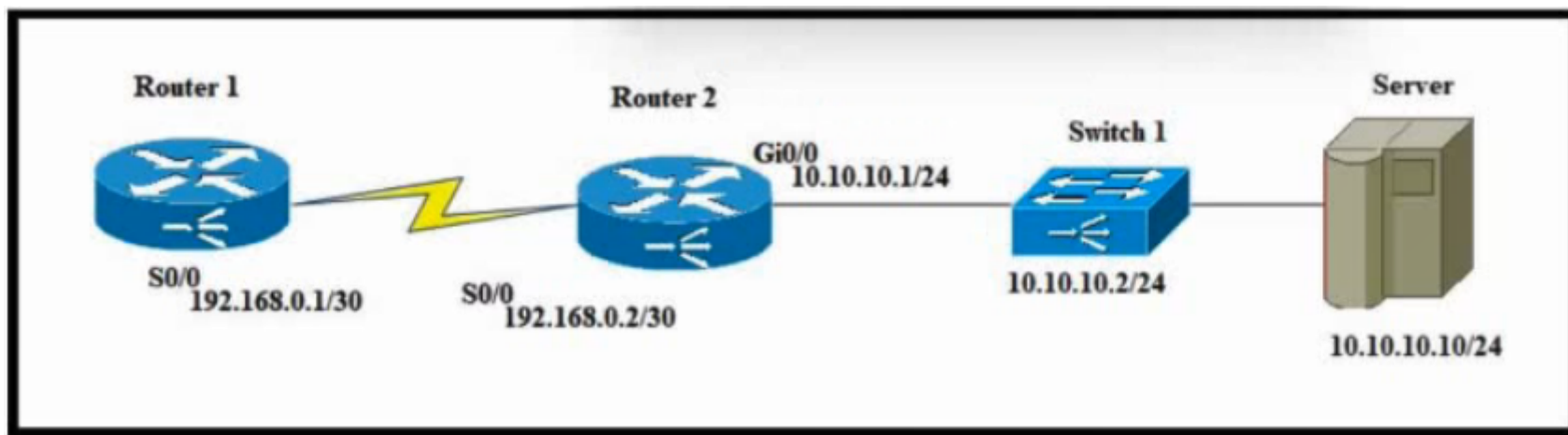
Why are the answers listed backwards? Please correct.
upvoted 3 times

  **[Removed]** 2 months, 2 weeks ago

It's even worse that the answers listed backwards. 255.255.255.240 is not even there.
10.10.13.128 --> 255.255.255.240
upvoted 1 times

  **[Removed]** 2 months, 2 weeks ago

than***
upvoted 1 times



Refer to the exhibit. A network engineer must configure router R1 with a host route to the server. Which command must the engineer configure?

- A. R1(config)#ip route 10.10.10.10 255.255.255.255 192.168.0.2
- B. R1(config)#ip route 10.10.10.0 255.255.255.0 192.168.0.2
- C. R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.2
- D. R1(config)#ip route 192.168.0.2 255.255.255.255 10.10.10.10

Correct Answer: A

[Removed] 2 months, 1 week ago

Selected Answer: A

A. R1(config)#ip route 10.10.10.10 255.255.255.255 192.168.0.2 - is the right answer
upvoted 1 times

Swiz005 5 months ago

What's the difference between route A and D?
upvoted 1 times

[Removed] 2 months, 1 week ago

The first address must be the destination.
To reach host 10.10.10.10 you send the traffic to the next hop (Router 2 in this case) 192.168.0.2
upvoted 1 times

studying_1 4 months, 1 week ago

A is the correct answer, D is wrong, the 2 ip addresses should be swapped
upvoted 2 times



Refer to the exhibit. IPv6 is being implemented within the enterprise. The command `ipv6 unicast-routing` is configured. Interface Gig0/0 on R1 must be configured to provide a dynamic assignment using the assigned IPv6 block. Which command accomplishes this task?

- A. `ipv6 address 2001:DB8:FFFF:FCF3::64 link-local`
- B. `ipv6 address 2001:DB8:FFFF:FCF3::1/64`
- C. `ipv6 address 2001:DB8:FFFF:FCF3::64 eui-64`
- D. `ipv6 address autoconfig 2001:DB8:FFFF:FCF2::/64`

Correct Answer: C

[Removed] 2 months, 1 week ago

Selected Answer: C

Answer C is correct
upvoted 1 times

Kasapin 5 months ago

Selected Answer: C

I think it's a typo in C, it should be `::/64`, it's missing `/`.
upvoted 4 times

zamkljo 5 months, 2 weeks ago

Selected Answer: C

The correct answer : C
upvoted 3 times

lucantonelli93 6 months, 3 weeks ago

Selected Answer: B

The correct answer it's B.
upvoted 2 times

gewe 7 months ago

B is correct
in C there is missing `///`
upvoted 1 times

oatmealturkey 7 months ago

It's a typo. B is not correct because it is a static assignment.
upvoted 8 times

studying_1 4 months, 1 week ago

i agree with oatmealturkey, it should be dynamic, C is correct
upvoted 4 times

Dutch012 6 months, 1 week ago

that's my opinion too!
upvoted 4 times

```
R1# show ip route | begin gateway
Gateway of last resort is 209.165.200.246 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 209.165.200.246, Serial0/1/0
is directly connected, Serial0/1/0
    172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
S   172.16.0.0/24 [1/0] via 207.165.200.250, Serial0/0/0
O   172.16.0.128/25 [110/32445] via 207.165.200.254, 00:00:23, Serial0/0/1
D   172.16.0.192/29 [90/3184439] via 207.165.200.254, 00:00:25, Serial0/0/1
    207.165.200.0/24 is variably subnetted, 4 subnets, 2 masks
C   207.165.200.248/30 is directly connected, Serial0/0/0
L   207.165.200.249/32 is directly connected, Serial0/0/0
C   207.165.200.252/30 is directly connected, Serial0/0/1
L   207.165.200.253/32 is directly connected, Serial0/0/1
```

Refer to the exhibit. With which metric does router R1 learn the route to host 172.16.0.202?

- A. 90
- B. 110
- C. 32445
- D. 3184439

Correct Answer: C

☒  **Stichy007** Highly Voted 6 months, 3 weeks ago

Selected Answer: C

C is correct, 172.16.0.202 would not be in the subnet for D
upvoted 7 times

☒  **[Removed]** Most Recent 2 months, 2 weeks ago

Selected Answer: C

Answer C is correct
upvoted 1 times

☒  **studying_1** 4 months, 1 week ago

Selected Answer: C

C is correct
upvoted 2 times

☒  **tal10** 6 months, 3 weeks ago

Selected Answer: D

i think the correct answer is d because it has the longest prefix
upvoted 2 times

☒  **yuz1227** 6 months, 1 week ago

it can't be because 172.16.0.202 is not in that segment (172.16.0.192/29):

Network: 172.16.0.192/29

Broadcast: 172.16.0.199

HostMin: 172.16.0.193

HostMax: 172.16.0.198

upvoted 7 times

☒  **4bed5ff** 2 months, 2 weeks ago

But if 172.16.0.2 is in segment 172.16.0.128:

Network: 172.16.0.128/25

Broadcast: 172.16.0.255

HostMin: 172.16.0.129

HostMax: 172.16.0.254

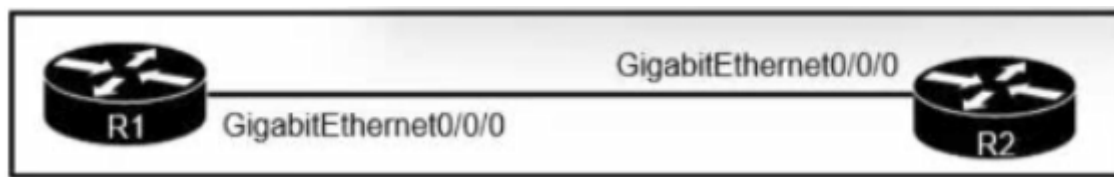
Doesn't this overlap with 172.16.0.192/29 at some point?

upvoted 1 times

☒  **andrizo** 1 week, 6 days ago

Not in the .192 range.

upvoted 1 times



Refer to the exhibit. A network engineer must configure the link with these requirements:

- Consume as few IP addresses as possible.
- Leave at least two additional useable IP addresses for future growth.

Which set of configurations must be applied?

- A. R1(config-if)#ip address 10.10.10.1 255.255.255.252
R2(config-if)#ip address 10.10.10.2 255.255.255.252
- B. R1(config-if)#ip address 10.10.10.1 255.255.255.240
R2(config-if)#ip address 10.10.10.12 255.255.255.240
- C. R1(config-if)#ip address 10.10.10.1 255.255.255.248
R2(config-if)#ip address 10.10.10.4 255.255.255.248
- D. R1(config-if)#ip address 10.10.10.1 255.255.255.0
R2(config-if)#ip address 10.10.10.5 255.255.255.0

Correct Answer: A

ahmt Highly Voted 7 months ago

Selected Answer: C

C is correct. 252(/30) ip subnet have only 2 usable ip address. 248(/29) ip subnet have 6 usable ip address.
upvoted 10 times

oatmealturkey Highly Voted 7 months ago

Selected Answer: C

A is incorrect, it does not leave any usable addresses. C is correct
upvoted 7 times

Vikramaditya_J Most Recent 1 month, 2 weeks ago

Selected Answer: C

We have to configure the link which will need 2 IP addresses, 1 for each port on each Router. We also need 2 spare IPs for future growth, so overall we need 4 usable IP addresses. If we consider using the /30 (255.255.255.252) mask, it will give us $2^2 (=4)$ i.e., total 4 IPs and 2 usable IPs, which doesn't fulfil the given requirements. So, we can consider using the next /29 (255.255.255.248) mask, which gives us $2^3 (=8)$ i.e., total 8 IP address and 6 usable IP addresses, which perfectly fulfil the given requirements.
upvoted 1 times

[Removed] 2 months, 2 weeks ago

Selected Answer: C

C. R1(config-if)#ip address 10.10.10.1 255.255.255.248
R2(config-if)#ip address 10.10.10.4 255.255.255.248

This will give you 6 usable ip addresses which is enough for the 4 ip addresses required and will only waste 2 ip addresses.
upvoted 1 times

4aynick 3 months, 3 weeks ago

all is correct except A
upvoted 1 times

studying_1 3 months, 2 weeks ago

No, it says "Consume as few IP addresses as possible." so only C is correct
upvoted 3 times


Inaaya_45 4 months ago

Why not B? wouldn't that leave 14 usable addresses?
upvoted 1 times

studying_1 3 months, 2 weeks ago

right, but it requires two additional addresses, and we need to consume as few ip addresses as possible,

upvoted 2 times

  **Vikramaditya_J** 4 months, 1 week ago

Selected Answer: C

As per the exhibit, there's a requirement to configure the link and also keep 2 spare IP addresses for future use. So, calculate like this:

2 IPs for Network ID and broadcast IP for whatever subnet we use.


2 IPs for connected interfaces on each router i.e. 1 for R1 gi0/0/0 and 1 for R2 gi0/0/0.

2 IPs reserved for future use.

In this way, we need atleast 6 IPs here and the subnet that can provide a closest value in terms of total required IPs is /29 (255.255.255.248). The /29 subnet provides a total of 8 IPs addresses per subnet and out of that 6 are host usable IPs.

So, for given subnet 10.10.10.X/29 we can have IP range from 10.10.10.0 - 10.10.10.7. Where 10.10.10.0 will be network ID and 10.10.10.7 will be broadcast IP. Rest 10.10.10.1 - 10.10.10.6 can be used to assign to any hosts of links.

upvoted 1 times

  **Ciscoman021** 5 months, 4 weeks ago

Selected Answer: C

With a /30 subnet mask, you can have a total of 4 IP addresses, 2 of which can be used for hosts. The reason for this is that the /30 subnet mask has 30 bits set to 1, leaving 2 bits for host addresses.

With a /29 subnet mask, you can have a total of 8 IP addresses, 6 of which can be used for hosts. The reason for this is that the /29 subnet mask has 29 bits set to 1, leaving 3 bits for host addresses.

upvoted 3 times

  **mhayek** 6 months, 1 week ago

A is correct. A 30-bit subnet mask allows for four IPv4 addresses: two host addresses, one all-zeros network, and one all-ones broadcast address. A point-to-point link can only have two host addresses. There is no real need to have the broadcast and all-zeros addresses with point-to-point links. Even A 31-bit subnet mask allows for exactly two host addresses, and eliminates the broadcast and all-zeros addresses, thus it conserves the use of IP addresses to the minimum for point-to-point links.



upvoted 1 times

  **bisiyemo1** 6 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

  **JJY888** 6 months, 1 week ago

Selected Answer: C

2 additional!!

upvoted 2 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: C

Definitely "C" is the correct answer

upvoted 3 times

  **j1mlawton** 7 months ago

Selected Answer: C

Is it not .248? .252 would not leave any free ip addresses

upvoted 2 times

  **gewe** 7 months ago

C is correct

upvoted 4 times

DRAG DROP

-

Drag and drop the device behaviors from the left onto the matching HSRP state on the right.

has heard from the neighbor device and is receiving hello packets	Active
is forwarding packets	Learn
is ready to forward packets if the device that is currently forwarding packets fails	Listen
is transmitting and receiving hello packets	Speak
is waiting to hear from the neighbor device	Standby

Correct Answer:

has heard from the neighbor device and is receiving hello packets	is forwarding packets
is forwarding packets	is waiting to hear from the neighbor device
is ready to forward packets if the device that is currently forwarding packets fails	is transmitting and receiving hello packets
is transmitting and receiving hello packets	has heard from the neighbor device and is receiving hello packets
is waiting to hear from the neighbor device	is ready to forward packets if the device that is currently forwarding packets fails

 **gewe** Highly Voted 7 months ago

from top to bottom::

Is forwarding packets

has heard from neighbor device, receiving hello packets

is waiting to hear from neighbor device

is transmiting and receiving hello packets

is ready to forward packets if active device fail

pls correct me if I m not right

upvoted 17 times

 **Stevens0103** 1 month, 1 week ago

active: is forwarding packets

learn: is waiting to hear from the neighbor device

listen: has heard from athe neighbor device and is receiving hello packets

speak: is transmitting and receiving hello packets

standby: is ready to forward packets if the device that is currently forwarding packets fails

<https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/10583-62.html#topic13>

upvoted 4 times

 **dropspablo** 1 month ago

I agree, very good link. Just a tip, unlike STP where the status "LISTEN" comes before "LEARN", in HSRP the status first enters "LEARN" and then comes "LISTEN", although they have different meanings if you pay attention to the order can help!

upvoted 1 times

  **gewe** Highly Voted 6 months, 4 weeks ago

Active – This is the state of the device that is actively forwarding traffic.

Init or Disabled – This is the state of a device that is not yet ready or able to participate in HSRP.

Learn – This is the state of a device that has not yet determined the virtual IP address and has not yet seen a hello message from an active device.

Listen – This is the state of a device that is receiving hello messages.

Speak – This is the state of a device that is sending and receiving hello messages.

Standby – This is the state of a device that is prepared to take over the traffic forwarding duties from the active device.

<https://www.pearsonitcertification.com/articles/article.aspx?p=2141271>

upvoted 6 times

  **[Removed]** Most Recent 2 months, 2 weeks ago

HSRP State Description

Learn The router has not determined the virtual IP address and has not yet seen a hello message from the active router. In this state, the router waits to hear from the active router.

Listen The router knows the virtual IP address, but the router is neither the active router nor the standby router. It listens for hello messages from those routers.

Speak The router sends periodic hello messages and actively participates in the election of the active and/or standby router.

Standby The router is a candidate to become the next active router and sends periodic hello messages.

Active The router won the election.

upvoted 1 times

  **[Removed]** 2 months, 2 weeks ago

Active : is forwarding packets

Learn : is waiting to hear from the neighbor device

Listen : has heard from the neighbor device and is receiving hello packets

Speak : is transmitting and receiving hello packets

Standby: is ready to forward packets if the device that is currently forwarding packets fails

upvoted 1 times

  **MassNasty1** 3 months, 3 weeks ago

Active - Forwarding Packets



Listen - Heard Neighbor Device and is Receiving Hello Messages

Learn - Waiting to Receive Hello Messages

Speak - Receiving and Transmitting Hello Messages

Standby - Ready to Take Over Active Router Role if Current Active Router Fails

upvoted 2 times

  **mustdoit** 6 months, 1 week ago

Listen and speak need to swap positions.

Listen - has heard...

Speak - is transmitting and receiving...

Everything else is correct.

upvoted 5 times

  **j1mlawton** 7 months ago

I'd go with the following

- Is transmitting...

- Has heard...

- Is waiting...

- Is forwarding...

- Is ready...

upvoted 3 times



Refer to the exhibit. A static route must be configured on R86 to forward traffic for the 172.16.34.0/29 network, which resides on R14. Which command must be used to fulfill the request?

- A. ip route 10.73.65.65 255.255.255.248 172.16.34.0
- B. ip route 172.16.34.0 255.255.255.248 10.73.65.65
- C. ip route 172.16.34.0 0.0.0.7 10.73.65.64
- D. ip route 172.16.34.0 255.255.224.0 10.73.65.66

Correct Answer: D

ahmt Highly Voted 7 months ago

Selected Answer: B

B is correct. 172.16.34.0/29 subnet mask is 255.255.255.248, next hop is interface on R14(10.73.65.65).
upvoted 5 times

papibarbu Most Recent 2 months, 3 weeks ago

The answer is B
Let's be serious Exam topic how the R86 can send traffic on its own IP the .66 to join the network behind the R14
upvoted 1 times

Shaolinta 3 months ago

Selected Answer: B

e l'interfaccia corretta
upvoted 1 times

Tdawg1968 4 months ago

The answer selected would really confuse someone trying to learn subnet masks.
upvoted 2 times

ac89l 4 months, 1 week ago

I'm loosing trust with this website ...
upvoted 2 times

HSong 4 months, 2 weeks ago

Selected Answer: B

D? silly mistake.
upvoted 1 times

Ciscoman021 5 months, 4 weeks ago

Selected Answer: B

simple question but false answer.
upvoted 3 times

bisiyemo1 6 months, 1 week ago

Selected Answer: B

B is correct
upvoted 2 times

Stichy007 6 months, 3 weeks ago

Selected Answer: B

am i a joke to these people, obvious answer is B
upvoted 4 times

tal10 6 months, 3 weeks ago

Selected Answer: B

definitive B
upvoted 2 times

tal10 6 months, 3 weeks ago

Selected Answer: B

the correct answer


upvoted 2 times

 **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: B

It's B the correct answer

upvoted 3 times

 **Rynurr** 6 months, 3 weeks ago

Selected Answer: B

"B" is the correct answer

upvoted 3 times

 **oatmealturkey** 7 months ago

Selected Answer: B

Check the subnet mask on D, it is obviously wrong

upvoted 2 times

 **j1mlawton** 7 months ago

Selected Answer: B

Next hop is interface on R14

upvoted 3 times

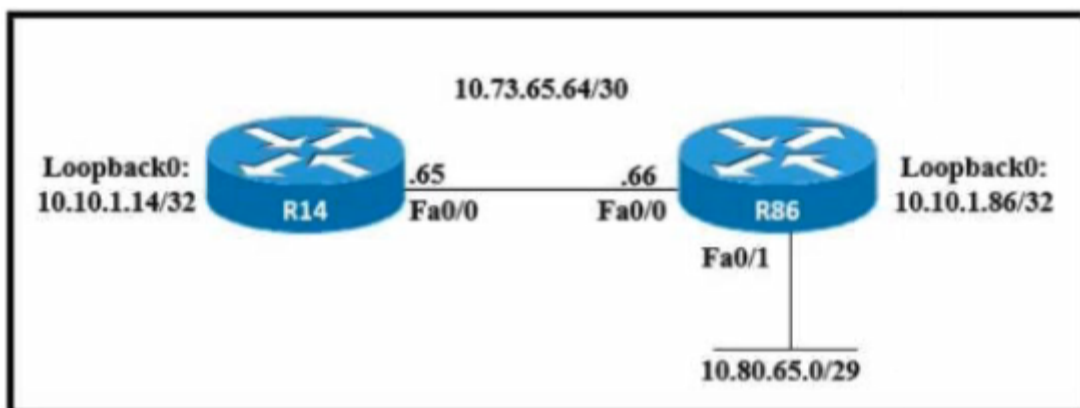
 **gewe** 7 months ago

B is correct

upvoted 3 times

Question #907

Topic 1



Refer to the exhibit. An engineer must configure a floating static route on an external EIGRP network. The destination subnet is the /29 on the LAN interface of R86. Which command must be executed on R14?

- A. ip route 10.80.65.0 255.255.248.0 10.73.65.66 1
- B. ip route 10.80.65.0 255.255.255.240 fa0/1 89
- C. ip route 10.80.65.0 255.255.255.248 10.73.65.66 171
- D. ip route 10.73.65.66 0.0.0.224 10.80.65.0 255

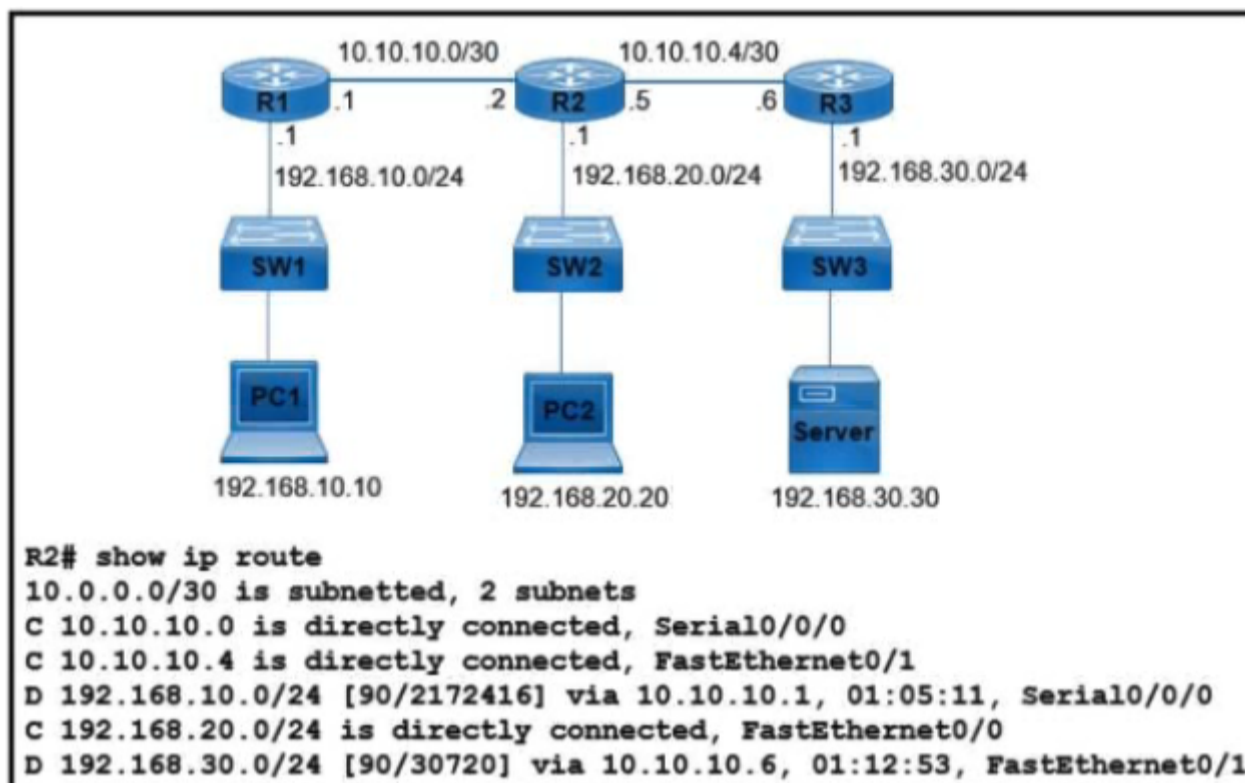
Correct Answer: C

 **SVN05** Highly Voted 6 months, 3 weeks ago

Selected Answer: C

External EIGRP has an AD of 170 unlike Regular EIGRP that has an AD of 90. So by putting 171 makes it a floating static route.

upvoted 9 times



Refer to the exhibit. What is the next-hop IP address for R2 so that PC2 reaches the application server via EIGRP?

- A. 192.168.30.1
- B. 10.10.10.6
- C. 10.10.10.5
- D. 192.168.20.1

Correct Answer: B

[Removed] 2 months, 2 weeks ago

Selected Answer: B

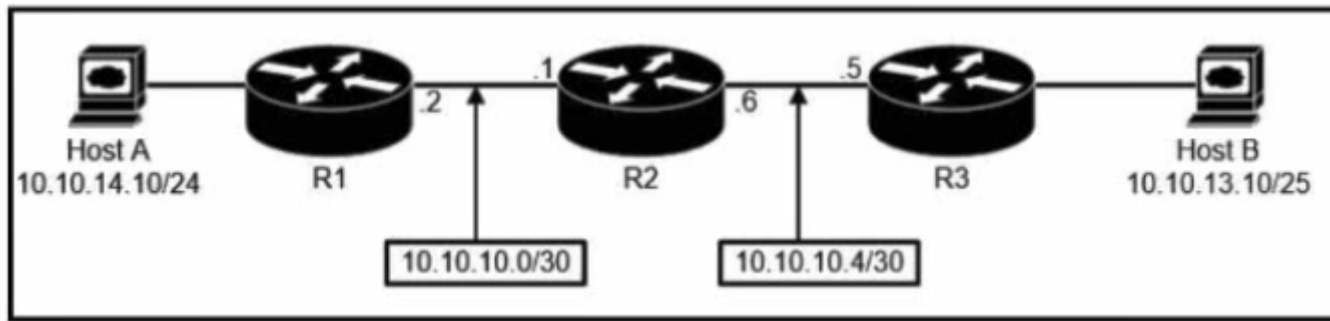
Answer B is correct
upvoted 1 times

studying_1 3 months, 2 weeks ago

Selected Answer: B

Answer is correct, 192.168.30.0/24 via 10.10.10.6
upvoted 2 times

DRAG DROP



- ip route 10.10.13.0 255.255.255.128 10.10.10.1
- ip route 10.10.13.0 255.255.255.128 10.10.10.5
- ip route 10.10.13.10 255.255.255.255 10.10.10.1
- ip route 10.10.14.0 255.255.255.0 10.10.10.2
- ip route 10.10.14.0 255.255.255.0 10.10.10.6
- ip route 10.10.14.10 255.255.255.255 10.10.10.6

R1

R2

R3

Correct Answer:

- ip route 10.10.13.0 255.255.255.128 10.10.10.1
- ip route 10.10.13.0 255.255.255.128 10.10.10.5
- ip route 10.10.13.10 255.255.255.255 10.10.10.1
- ip route 10.10.14.0 255.255.255.0 10.10.10.2
- ip route 10.10.14.0 255.255.255.0 10.10.10.6
- ip route 10.10.14.10 255.255.255.255 10.10.10.6

R1

ip route 10.10.14.0 255.255.255.0 10.10.10.2

R2

ip route 10.10.13.0 255.255.255.128 10.10.10.5

ip route 10.10.13.10 255.255.255.255 10.10.10.1

R3

ip route 10.10.14.10 255.255.255.255 10.10.10.6



Simon_1103 (Highly Voted) 6 months, 1 week ago
 R1 - ip route 10.10.13.0 255.255.255.128 10.10.10.1
 R2 - ip route 10.10.13.0 255.255.255.128 10.10.10.5
 R2 - ip route 10.10.14.0 255.255.255.0 10.10.10.2
 R3- ip route 10.10.14.0 255.255.255.0 10.10.10.6
 upvoted 24 times

Shabeth 2 months, 2 weeks ago
 correct
 upvoted 1 times

rogi2023 5 months, 2 weeks ago
 this is all correct. Wondaah has mistyped the subnet masks, otherwise also the next-hop -IPs correct.
 upvoted 1 times

  **kat1969** Most Recent 3 weeks, 6 days ago



I hate the fact that this material has so many of the answers coded wrongly!
upvoted 1 times

  **wondaah** 6 months, 1 week ago


cant answer with these answers, all wrong
upvoted 4 times

  **UAE7** 6 months, 3 weeks ago

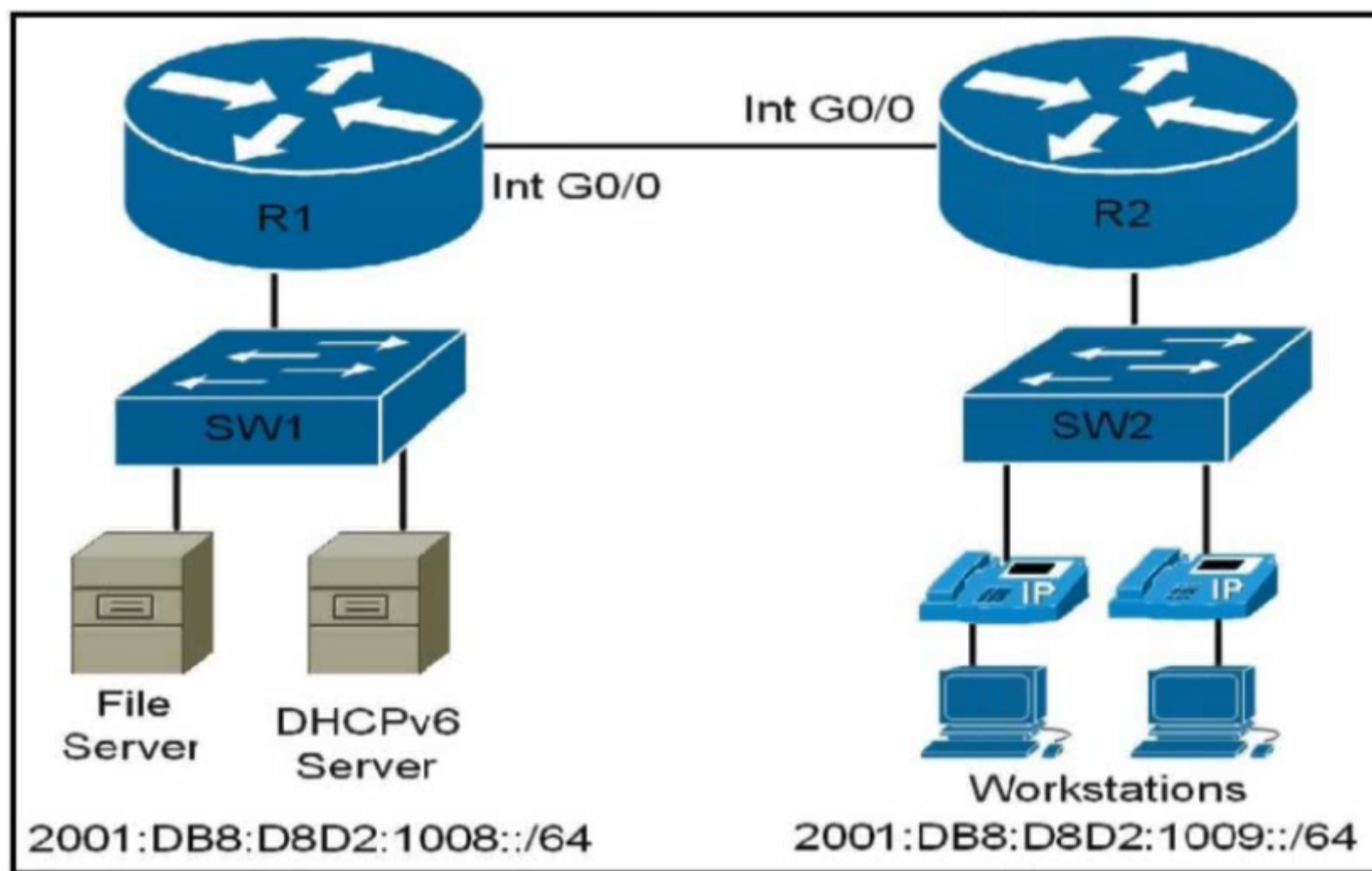
R1 - ip route 10.10.13.0 255.255.255.128 10.10.10.1
R2 - ip route 10.10.13.0 255.255.255.128 10.10.10.5
R2 - ip route 10.10.14.10 255.255.255.128 10.10.10.2
R3- ip route 10.10.14.10 255.255.255.128 10.10.10.6
upvoted 4 times

  **First93** 6 months, 2 weeks ago

I think the subnet mask of r3 and second r2 IP route is 255.255.255.0.
upvoted 2 times

  **ike110** 6 months, 3 weeks ago

incorrect answers
upvoted 1 times



Refer to the exhibit. An IPv6 address must be obtained automatically on the LAN interface on R1. Which command must be implemented to accomplish the task?

- A. ipv6 address autocontig
- B. ipv6 address dhcp
- C. ipv6 address fe80::/10
- D. ipv6 address 2001:db8:d8d2:1008:4332:45:0570::/64

Correct Answer: C

Dutch012 Highly Voted 6 months, 2 weeks ago

Selected Answer: A

Just use ipv6 address autocontig guys, it's safer.
upvoted 9 times

DavidCisco Highly Voted 5 months, 2 weeks ago

Selected Answer: B

"ipv6 address autoconfig": The interface should only obtain its configuration using RAs and the stateless address autoconfiguration (SLAAC). With ipv6 address autoconfig, a router will not attempt to contact DHCPv6.

"ipv6 address dhcp": DHCPv6 does not have an option to advertise a default gateway, and the default gateway still has to be discovered through RAs. It will depend on DHCPv6 to discover its address and prefix, and on RAs to discover its gateway.
So if the DHCPv6 is in the same LAN that the R1 LAN interface is the best option.

B is the best correct answer

<https://community.cisco.com/t5/ipv6/ipv6-address-autoconfig-vs-ipv6-address-dhcp/td-p/2710597>

upvoted 5 times

Techpro30 Most Recent 2 weeks, 6 days ago

I believe its B for the exam, although in reality, like Dutch said, its safer/better:

There are a few reasons why you might not want to use DHCP for IPv6 addresses.

DHCP is a stateful protocol, which means that it requires a DHCP server to maintain a database of IP addresses and their corresponding lease information. This can be a burden on the DHCP server, especially in large networks.

DHCP is not as secure as SLAAC. When a device uses DHCP, it sends its MAC address to the DHCP server, which can be used to track the device.
DHCP can be more complex to configure than SLAAC.

upvoted 1 times

🗨️ **TechLover** 2 months, 2 weeks ago

B is correct
upvoted 1 times

🗨️ **perri88** 3 months ago

Selected Answer: B

it's says obtain, not auto generate. I go with B
upvoted 4 times

🗨️ **gulu73** 3 months, 2 weeks ago

Selected Answer: A

Configuring the Stateless DHCPv6 Client
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. ipv6 address autoconfig [default]
5. end

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-16/dhcp-xe-16-book/ip6-dhcp-stateless-auto.html
upvoted 3 times

🗨️ **Friday_Night** 3 months, 2 weeks ago

I wanted to answer with A but then I saw there is a DHCP server, it's like implicitly telling me to use it and I think this is a scenario based question... so I'll go for B (why use autoconfig if there is a DHCP server?)

upvoted 3 times

🗨️ **MassNastty1** 3 months, 3 weeks ago

B. is not a valid command. This is from the cisco site:

Configuring the Stateless DHCPv6 Client
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. ipv6 address autoconfig [default]
5. end

Source: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-16/dhcp-xe-16-book/ip6-dhcp-stateless-auto.html
upvoted 1 times

🗨️ **Vyncy** 3 months, 1 week ago

It most certainly is valid command
upvoted 3 times

🗨️ **Vikramaditya_J** 4 months, 3 weeks ago

Selected Answer: A

The option C configures a link local IPv6 address (that ranges between FE80::10 and FEB0::10) which isn't correct because when you enable IPv6 on an interface then the device will automatically create a link-local address. The ipv6 address autoconfig command causes the device to perform IPv6 stateless address auto-configuration to discover prefixes on the link and then to add the EUI-64 based addresses to the interface.

upvoted 1 times

🗨️ **Matalongo** 4 months, 4 weeks ago

A. ipv6 address autocontig
upvoted 1 times

🗨️ **bisiyemo1** 6 months, 1 week ago

Selected Answer: B

B is correct
upvoted 2 times

🗨️ **mageknight** 6 months, 3 weeks ago

The dhcp server isn't in the same subnet than the wan interface of the router, so by default it can't receive configuration from the dhcp server. It should be A for me...

upvoted 1 times

🗨️ **mageknight** 6 months, 3 weeks ago

sorry it is for LAN so it should be B

upvoted 1 times

🗨️ **mageknight** 6 months, 3 weeks ago

depend if it is stateless or statefull dhcp server

upvoted 1 times

🗨️ **SVN05** 6 months, 3 weeks ago

Selected Answer: A

Are you guys sure about Ipv6 address dhcp as i search on google only ip address dhcp appears(for IPv4) however for ipv6 address autoconfig is aviable for IPv6 and as gewe explained. Im going with A. Answer C is a link local address where its used within a subnet,not routable however the network that is presented to us is using global unicast addressing scheme(2001:DB8) thus answer C makes no sense.

upvoted 3 times

🗨️ **rogi2023** 5 months, 2 weeks ago

B is correct. this si from GNS3:

```
R2(config-if)#ipv6 address d
```

```
R2(config-if)#ipv6 address dhcp ?
```

```
rapid-commit Enable Rapid-Commit
```

```
<cr>
```

upvoted 1 times

🗨️ **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: B

For me , the correct answer is B

upvoted 2 times

🗨️ **Rynurr** 6 months, 3 weeks ago

Selected Answer: B

IMO should be "B"

upvoted 3 times

🗨️ **gewe** 6 months, 4 weeks ago

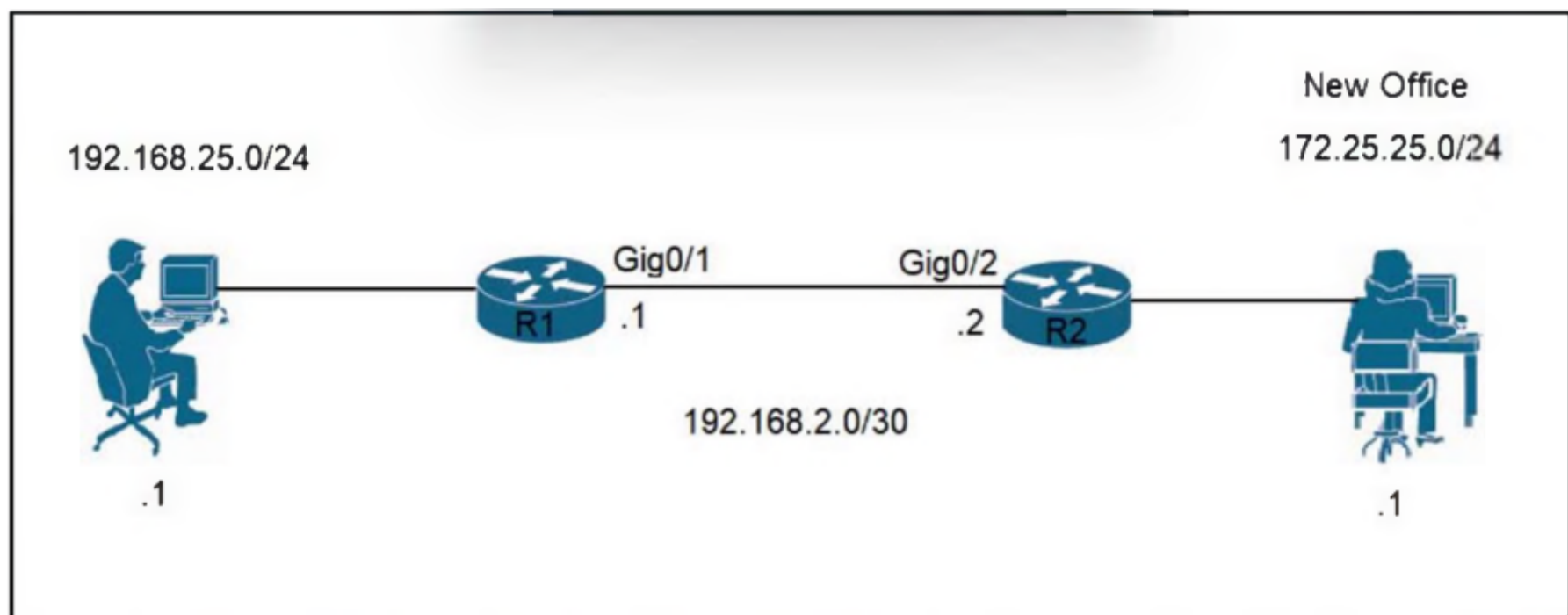
ipv6 address autoconfig - Enables the interface to automatically obtain an IPv6 address using router advertisement information and the EUI-64 identifier. The no form of this command disables address auto-configuration. A maximum of 15 autoconfigured addresses are supported.

upvoted 2 times

🗨️ **gewe** 6 months, 4 weeks ago

what about option A?

upvoted 1 times



Refer to the exhibit. A network engineer is updating the configuration on router R1 to connect a new branch office to the company network. R2 has been configured correctly. Which command must the engineer configure so that devices at the new site communicate with the main office?

- A. `ip route 172.25.25.1 255.255.255.255 g0/2`
- B. `ip route 172.25.25.0 255.255.255.0 192.168.2.2`
- C. `ip route 172.25.25.0 255.255.255.0 192.168.2.1`
- D. `ip route 172.25.25.1 255.255.255.255 g0/1`

Correct Answer: B

papinski Highly Voted 6 months, 2 weeks ago

Selected Answer: B

Oh wow! A right answer!
upvoted 5 times

wondaah 6 months, 1 week ago

i wouldnt say its right, because the question says what command to communicate with the main office. implying that you have to enter the command on r2 and route the network to r1
upvoted 1 times

lolungos 3 months, 1 week ago

"R2 has been correctly configured" + "updating configuration in R1"
+ remember that the route needs to know how to go back to it's original site to have communication
upvoted 1 times

Dutch012 6 months, 1 week ago

but all the destinations in the ip route command are 172.25.25.0, so the route to the new site, the question is written in a wrong way
upvoted 5 times

[Removed] Most Recent 2 months, 2 weeks ago

Selected Answer: B

B - `ip route 172.25.25.0 255.255.255.0 192.168.2.2`
upvoted 2 times

shiv3003 4 months, 4 weeks ago

The question itself is wrong!
upvoted 1 times

Lokylax 4 months, 1 week ago

The question is not wrong. It reads R2 is configured correctly. If you don't add the route on R1 the traffic sent from new office will never return.
upvoted 1 times

hamish88 4 months, 4 weeks ago

B is correct. As it is said a network engineer is updating the configuration on router R1.
upvoted 2 times

  **Swiz005** 5 months ago

Selected Answer: C

I believe the gateway for the network is 192.168.2.1 and not 192.168.2.2?
upvoted 1 times

  **kat1969** 3 weeks, 6 days ago

Usually you point either to the physical outbound interface or to the next hop neighbor address.
upvoted 1 times

  **wondaah** 6 months, 1 week ago

Selected Answer: C

Question says to route to the main office and not the new office
upvoted 1 times

  **VictorCisco** 5 months, 2 weeks ago

Actually , it is said that devices at the new site should be able to communicate with the main office. So we need a route to a new site on the R1.
upvoted 3 times

A network engineer must migrate a router loopback interface to the IPv6 address space. If the current IPv4 address of the interface is 10.54.73.1/32, and the engineer configures IPv6 address 0:0:0:0:ffff:a36:4901, which prefix length must be used?

- A. /64
- B. /96
- C. /124
- D. /128

Correct Answer: B

 **gewe** Highly Voted 7 months ago

i would go with D
upvoted 10 times

 **SVN05** Highly Voted 6 months, 3 weeks ago

Selected Answer: D

/128(for IPv6) is the equivalent to /32(for IPv4). Both are host subnets.
upvoted 7 times

 **[Removed]** Most Recent 2 months, 2 weeks ago

Selected Answer: D

D. /128
/128 (Ipv6) is the equivalent to /32 for IPv4
upvoted 1 times

 **Yannik123** 3 months, 4 weeks ago

Selected Answer: D

D is correct an /32 Ipv4 subnet mask is an /128 Ipv6 subnet mask
upvoted 4 times

 **mrmanistheman** 4 months, 1 week ago


Selected Answer: D

Correct answer is D, half these answers are incorrect 😂
upvoted 2 times

 **Vikramaditya_J** 4 months, 2 weeks ago

Selected Answer: D

It should be D. The equivalent subnet mask in IPv6 for an IPv4 /32 subnet mask is /128 and here're sample loopback interface config steps:
configure terminal
interface loopback 0
ipv6 address 2001:db8::1/128
no shutdown
exit
show interface loopback 0
upvoted 1 times

 **JJY888** 6 months, 1 week ago

Selected Answer: D

I think loopback interfaces are configured at /32 for IPv4 and /128 for IPv6.
upvoted 2 times

 **Dutch012** 6 months, 2 weeks ago

D boys
upvoted 1 times

 **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: D

The correct answers is D
upvoted 2 times

A Cisco engineer notices that two OSPF neighbors are connected using a crossover Ethernet cable. The neighbors are taking too long to become fully adjacent. Which command must be issued under the interface configuration on each router to reduce the time required for the adjacency to reach the FULL state?

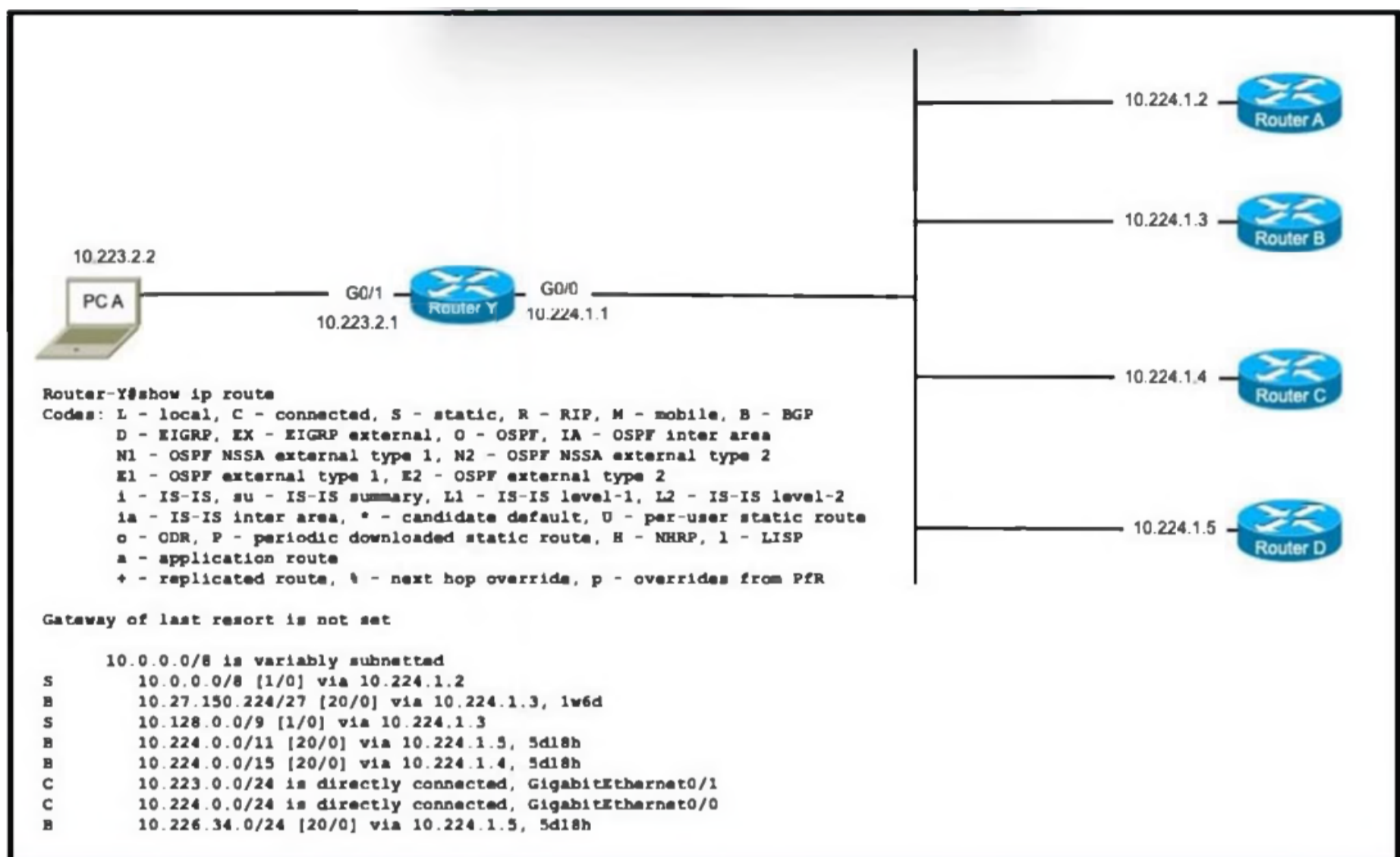
- A. ip ospf dead-interval 40
- B. ip ospf network broadcast
- C. ip ospf priority 0
- D. ip ospf network point-to-point

Correct Answer: D

  **rogi2023** Highly Voted  5 months, 2 weeks ago

Selected Answer: D

D is correct answer. Because of ethernet (CSMA/CD) - With this cmd, we will avoid DR/BDR election.
upvoted 5 times



Refer to the exhibit. PC A is communicating with another device at IP address 10.227.225.255. Through which router does router Y route the traffic?

- A. router A
- B. router B
- C. router C
- D. router D

Correct Answer: A

oatmealturkey Highly Voted 7 months ago

Selected Answer: D

Correct answer is D. Look for the longest match in the routing table.
upvoted 10 times

shaney67 Most Recent 1 month, 2 weeks ago

Trying to work out why it couldn't be switch C
would the /15 not take precedence as it is the longest? and is in the range
10.226.0.1 - 10.227.255.254
upvoted 3 times

FutureCiscoEngineer 1 week, 5 days ago

Check again for the range, it starts from 10.224.0.1 not from 10.226.0.1.
upvoted 2 times

Vikramaditya_J 1 month, 2 weeks ago

Selected Answer: A

The given destination IP address "10.227.225.255" falls and only available in the network "10.0.0.0/8", which goes via Router A with address 10.224.1.2.

Let's see the IP ranges of all the given routes:

10.0.0.0/8 = 10.0.0.0 - 10.255.255.255 (Given destination IP "10.227.225.255" falls in this range)

10.128.0.0/9 = 10.128.0.0 - 10.191.255.255

10.224.0.0/11 = 10.224.0.0 - 10.255.255.255

10.224.0.0/15 = 10.224.0.0 - 10.225.255.255

Remaining last 3 subnets are out of picture here:

10.223.0.0/24

10.224.0.0/24
10.226.34.0/24
upvoted 4 times

🗨️ 👤 **AtousaF** 1 month ago

I assume 10.227.225.255 is part of this range : 10.224.0.0/11 = 10.224.0.0 - 10.255.255.255! so D is correct.
upvoted 1 times

🗨️ 👤 **Tdawg1968** 4 months ago

Makes sense. /11 gives a block of 32. So we are working in the 2nd octet. 224 is the starting network address of that block which would cover up to 256. That would include 227.
upvoted 4 times

🗨️ 👤 **DavidCisco** 5 months, 1 week ago

Selected Answer: D

Comprobado, la respuesta correcta es la D, subnetear mirando las /
upvoted 2 times

🗨️ 👤 **VictorCisco** 5 months, 2 weeks ago

Selected Answer: B

only B is correct answer.
10.128.0.0/9
Usable Host IP Range: 10.128.0.1 - 10.255.255.254
it is contain the offered address
upvoted 1 times

🗨️ 👤 **studying_1** 4 months, 1 week ago

reread the question, the destination ip address is 10.227.225.255, D is correct
upvoted 2 times

🗨️ 👤 **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: D

The correct answer it's D
upvoted 1 times

🗨️ 👤 **Midus** 6 months, 3 weeks ago

10.226.34.0/24 mismatch 10.227 .. correct is 10.224.0.0/15 or no?
upvoted 2 times

🗨️ 👤 **SVN05** 6 months, 3 weeks ago

Can someone please explain in detail how do we go about this question? Thank you all.
upvoted 3 times

🗨️ 👤 **mageknight** 6 months, 3 weeks ago

ip add 10.227.225.255 take place in the /11 subnet so the next hop is 10.224.1.5 = router D
upvoted 2 times

🗨️ 👤 **SVN05** 6 months, 3 weeks ago

Thanks mageknight. I understand the process of how it routes but how do you calculate such a big subnet??!!
upvoted 1 times

🗨️ 👤 **Stichy007** 6 months, 3 weeks ago

you need to understand how to calculate subnets, with a /11 its in the second octet and each subnet is separated by 32. /9 = 128, /10 = 64, /11=32 . therefore 227 would be in that range.
upvoted 2 times

🗨️ 👤 **Rynurr** 6 months, 3 weeks ago

Selected Answer: D

I agree, correct answer is "D"
upvoted 3 times

🗨️ 👤 **gewe** 6 months, 4 weeks ago

that's right, correct answer is D.
upvoted 4 times

Gateway of last resort is 172.16.2.2 to network 0.0.0.0

```

10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
  10.10.100.0/26 is directly connected, GigabitEthernet0/0/6
C   10.10.10.0/24 is directly connected, GigabitEthernet0/0/0
L   10.10.10.3/32 is directly connected, GigabitEthernet0/0/0
  172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S   172.16.1.33/32 is directly connected, GigabitEthernet0/0/1
C   172.16.2.0/23 is directly connected, GigabitEthernet0/0/1
L   172.16.2.1/32 is directly connected, GigabitEthernet0/0/1
S*  0.0.0.0/0 [1/0] via 172.16.2.2

```

Refer to the exhibit. A packet sourced from 10.10.10.32 is destined for the Internet. What is the administrative distance for the destination route?

- A. 0
- B. 1
- C. 2
- D. 32

Correct Answer: B

 **JJY888** Highly Voted 6 months, 1 week ago

Selected Answer: B

This makes me angry at Cisco. Why try and trick people!? Look at the word SOURCED not destined. Then you realize that it's the default internet address of 0.0.0.0. STATIC administrative distance is 1.

upvoted 12 times

 **[Removed]** 2 months, 2 weeks ago

Because they want you to fail so you'll take the exam several times and they'll make more money...

upvoted 2 times

 **kat1969** 3 weeks, 6 days ago

I completely agree! 'Psychometric exams' are not learning re-enforcement! They are set up to confound.

upvoted 1 times

 **SVN05** Highly Voted 6 months, 3 weeks ago

Selected Answer: B

For this exam, all you have to understand is 0.0.0.0 means the internet. The first portion of the sentence is to throw you off balance. Just focus on the second portion of the question and you'll see that the AD is stated clearly 1.

upvoted 5 times

 **andrizo** Most Recent 1 week, 6 days ago

Selected Answer: B

C is directly connected, which is 1.

upvoted 1 times

 **Friday_Night** 3 months, 2 weeks ago

172.16.2.2 is a subnet of 172.16.2.0/23 right? which is directly connected so admin distance is 0. what am I missing here?

upvoted 1 times

 **Simon_1103** 5 months, 1 week ago

Selected Answer: B

The administrative distance for the destination route is 1 because the gateway of last resort is configured with an administrative distance of 1 (indicated by the [1/0] in the routing table output) and the destination route for the Internet (0.0.0.0/0) is learned via that gateway. Therefore, the correct answer is B. 1.

upvoted 1 times

 **Irios2799** 6 months, 2 weeks ago

The host 10.10.10.32 belongs to subnet 10.10.10.0/24 and the subnet is directly connected.

The AD should be 0.

upvoted 3 times

🗨️ 👤 **Irios2799** 6 months, 2 weeks ago

Sorry i don't read well the question, the packet is destined to internet, that's the trick, the answer is B.

upvoted 2 times

🗨️ 👤 **Dutch012** 6 months, 2 weeks ago

Selected Answer: B

"destined for the Internet" means it going through the gateway last resort which is a static route.

AD of static route is 1

upvoted 4 times

🗨️ 👤 **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: A

The correct answers it's A

<https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/15986-admin-distance.html>

upvoted 2 times

🗨️ 👤 **mageknight** 6 months, 3 weeks ago

"A packet ... is destined for the Internet." it could be 200.123.25.41 so it isn't directly connected but match with 0.0.0.0 the static route with AD = 1

upvoted 2 times

🗨️ 👤 **Rynurr** 6 months, 3 weeks ago

Selected Answer: A

Directly connected interface = AD 0, so "A" is the correct answer.

upvoted 3 times

🗨️ 👤 **j1mlawton** 7 months ago

Selected Answer: A

Isn't it AD of 0 for directly connected routes and 1 for static?

upvoted 4 times

```
GigabitEthernet1 is up, line protocol is up
Hardware is CSR vNIC, address is 5000.0004.0000 (bia 5000.0004.0000)
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full Duplex, 1000Mbps, link type is auto, media type is RJ45
```

Refer to the exhibit. Which format matches the Modified EUI-64 IPv6 interface address for the network 2001:db8::/64?

- A. 2001:db8::5000:00ff:fe04:0000/64
- B. 2001:db8::4332:5800:41ff:fe06:/64
- C. 2001:db8::5000:0004:5678:0090/64
- D. 2001:db8::5200:00ff:fe04:0000/64

Correct Answer: C

 **oatmealturkey** Highly Voted 7 months ago

Selected Answer: D

A is also incorrect because the 7th bit of the MAC address was not flipped/set to 1. D is the correct answer.
upvoted 10 times

 **Vikramaditya_J** Highly Voted 4 months, 3 weeks ago

Selected Answer: D

Given MAC = 50 00 00 04 00 00
To make it EUI-64 IPv6, insert FFE0 in the middle of the MAC, so it will become: 50 00 00 FF E0 00 00
After this, "5" in binary will be written as "0101" and "0" in binary as "0000" OR we can say "50" in binary can be written as 01010"0"0. Now, flip the 7th bit, so it will become "010100"1"0" and now this "010100"1"0" can again be written in decimal as "52" after flipping the 7th bit. So, finally it will become: 52 00 00 FF E0 00 00
And our EUI-64 IPv6 will be: 2001:db8::5200:00FF:FE04:0000 /64
upvoted 7 times

 **bilatuba** Most Recent 1 month, 2 weeks ago

Selected Answer: D


A is incorrect. It doesn't invert the 7th bit.
upvoted 1 times

 **Mark_j_k90** 2 months ago

Why you give us this incorrect answer? The answer is D 'cause the eui-64 was flipped from 0 to 1, making the address look like 5200! Please, stop putting this wrong answer. Let the community choose. Apparently we know things better than your imaginary experts.
upvoted 2 times

 **blue91235** 5 months, 1 week ago

Why A is not correct ? the first address block 5000 its same in the question and answer can somebody explain why D is the answer ?
upvoted 1 times

 **JJY888** 6 months, 1 week ago


Selected Answer: D

This answer was GUESSED I guess. :-/
upvoted 2 times

 **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: D

The correct answers it's D
upvoted 1 times

 **SVN05** 6 months, 3 weeks ago

Anybody can mention which address you used from the table to implement the eui 64 calculations?
upvoted 2 times

 **studying_1** 3 months, 2 weeks ago

5000.0004.0000, then add right in the middle fffe = 5000.00ff.fe04.0000, then invert the 7th bit, = 5200.00ff.fe04.0000
upvoted 1 times

 **ike110** 6 months, 3 weeks ago

Selected Answer: D

D is the only one that makes sense
upvoted 2 times

  **j1mlawton** 7 months ago

Selected Answer: A

..FF FE
upvoted 5 times

  **j1mlawton** 6 months, 4 weeks ago

D is correct
upvoted 3 times



Question #917

Topic 1

What is the benefit of using FHRP?

- A. reduced ARP traffic on the network
- B. balancing traffic across multiple gateways in proportion to their loads
- C. higher degree of availability
- D. reduced management overhead on network routers

Correct Answer: C

  **Bhrino** 3 months, 1 week ago


Selected Answer: C

b is correct bc fhrp just offers more redundancy there for more availability
upvoted 1 times



  **Dutch012** 6 months, 2 weeks ago

Selected Answer: C

correct
upvoted 2 times

  **seapimp** 6 months, 2 weeks ago

imo B makes sense
upvoted 2 times




  **xbololi** 2 months, 2 weeks ago



it actually does but... FHRP is for backup not for splitting the workload. So if you enable FHRP for three routers unless the primary one goes down the other two wont get any part at the routing.
upvoted 1 times




Why is a first-hop redundancy protocol implemented?



- A. to enable multiple switches to operate as a single unit
- B. to provide load-sharing for a multilink segment
- C. to prevent loops in a network
- D. to protect against default gateway failures



Correct Answer: C



  **ike110** Highly Voted  6 months, 3 weeks ago
Who sets the answers? Do they do it incorrectly to test us? :)
upvoted 5 times



  **Stichy007** 6 months, 3 weeks ago
i want to know that too.
upvoted 4 times



  **AndreaGambera** Most Recent  2 weeks, 1 day ago
Selected Answer: D
D is correct!
upvoted 1 times



  **LeonardoMeCabrio** 3 months, 1 week ago
Selected Answer: D
DDDDDDD
upvoted 2 times



  **ccnk** 3 months, 3 weeks ago
Selected Answer: D
DDDDDDDDDDDDDD
upvoted 2 times



  **mrmanistheman** 4 months, 1 week ago
Selected Answer: D
D is correct, another wrong answer!
upvoted 2 times



  **Dutch012** 6 months, 2 weeks ago
Selected Answer: D
D correct
upvoted 3 times

  **Stichy007** 6 months, 3 weeks ago
Selected Answer: D
definitely D
upvoted 4 times

  **lucantonelli93** 6 months, 3 weeks ago
Selected Answer: D
The correct answers it's D
upvoted 3 times

  **lucantonelli93** 6 months, 3 weeks ago
The correct answers it's D
upvoted 2 times

  **SVN05** 6 months, 3 weeks ago
Selected Answer: D
Definitely D
upvoted 1 times

  **Rynurr** 6 months, 3 weeks ago
Selected Answer: D

"D" is the correct answer
upvoted 2 times

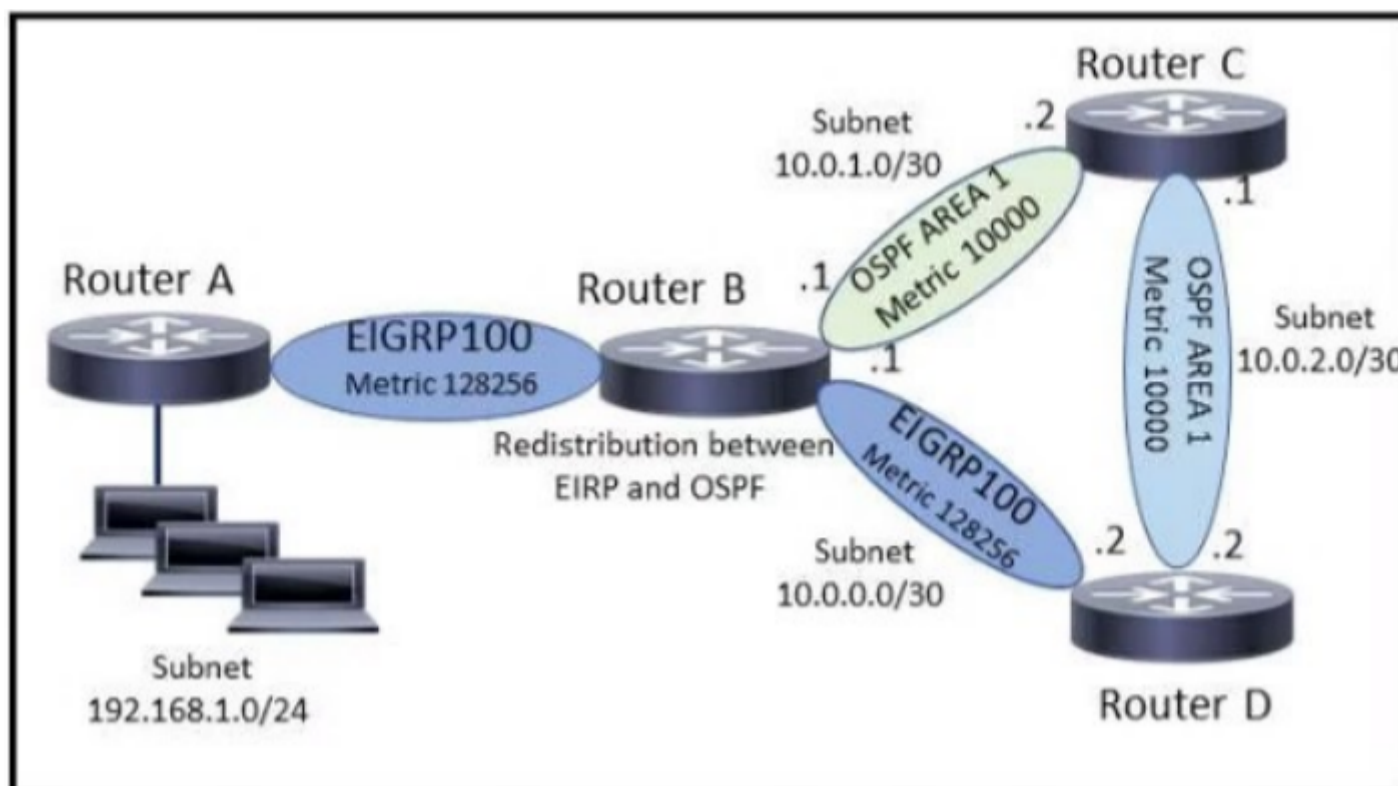
  **gewe** 6 months, 4 weeks ago

D definitely is correct
upvoted 3 times

  **oatmealturkey** 7 months ago

Selected Answer: D

FHRPs protect against default gateway failures.
upvoted 4 times



Refer to the exhibit. A network engineer executes the show ip route command on router D. What is the next hop to network 192.168.1.0/24 and why?

- A. The next hop is 10.0.2.1 because it uses distance vector routing.
- B. The next hop is 10.0.0.1 because it has a higher metric.
- C. The next hop is 10.0.2.1 because it is a link-state routing protocol.
- D. The next hop is 10.0.0.1 because it has a better administrative distance.

Correct Answer: D

mustdoit (Highly Voted) 6 months, 1 week ago

Selected Answer: C

Answer should be C. Redistributed EIGRP which is same as external EIGRP has AD of 170. Correct me if I'm wrong
upvoted 5 times

dropspablo (Most Recent) 1 month ago

Selected Answer: D

I agree with JuanluRea, see Router-B caption "Redistribution between EIRP and OSPF" and AS100 is the same, redistribution is for OSPF only. It would then be "AD 90" (not 170), answer D is correct!
upvoted 2 times

JuanluRea 2 months, 1 week ago

Selected Answer: D

There isn't redistribution Eigrp - Eigrp, only Eigrp - OSPF. The Eigrp has a AS 100 always. It's internal Eigrp, no external
upvoted 4 times

fra130186 2 months, 3 weeks ago

the redistribution is on the router B, so D is correct
upvoted 3 times

perri88 3 months ago

it's not clear why yet
upvoted 1 times

kat1969 3 weeks, 6 days ago

Because we see EIGRP100 on both sides of Router B, EIGRP is forwarding routes to Subnet 10.0.0.0/30. We also have a redistribution from EIGRP into OSPF happening then subnet on Router 2 (a distraction) and advertising routes to subnet 10.0.1.0/30 and then subnet 10.0.2.0/30. So the EIGRP to EIGRP route exchange has the lower AD (AD 90) because it is in the same AS (AS100). Ergo the OSPF route will not be considered. I hope this helps?
upvoted 2 times

Mariachi 5 months, 3 weeks ago

Selected Answer: C

EIGRP is not running on LAN side of the router, so it's going to be redistributed, so it's external EIGRP route ... so the AD is 170 vs 110 via the OSPF route.

upvoted 4 times

  **dropspablo** 1 month ago

EIGRP is running on the LAN side of Router-A, it just doesn't show up. Otherwise, OSPF and EIGRP would have no route to reach the final destination.

upvoted 1 times

What is a similarity between global and unique local IPv6 addresses?

- A. They use the same process for subnetting.
- B. They are part of the multicast IPv6 group type.
- C. They are routable on the global internet.
- D. They are allocated by the same organization.

Correct Answer: A

 **Peter_panda** Highly Voted 6 months ago

Selected Answer: A

Unique local addresses are NOT assigned by an organization.

https://en.wikipedia.org/wiki/Unique_local_address

A unique local address (ULA) is an Internet Protocol version 6 (IPv6) address in the address range fc00::/7.[1] Its purpose in IPv6 is somewhat analogous to IPv4 private network addressing, but with significant differences. Unique local addresses may be used freely, without centralized registration, inside a single site or organization or spanning a limited number of sites or organizations. They are routable only within the scope of such private networks, but not in the global IPv6 Internet.

upvoted 6 times

 **4Lucky711** Most Recent 1 month, 2 weeks ago

Selected Answer: A

I think A is correct.


upvoted 1 times

 **mrmanistheman** 4 months, 1 week ago

Selected Answer: A

Correct answer is A

upvoted 2 times

 **zamkljo** 5 months, 2 weeks ago

Selected Answer: A

They are NOT allocated by the same organization.

upvoted 1 times

 **rogi2023** 5 months, 2 weeks ago

Selected Answer: A

Peter_panda explained it perfect - the answer is A just to raise the % for A !!!


upvoted 1 times

 **purenuker** 5 months, 3 weeks ago

Selected Answer: A

Peter_panda explained it perfect - the answer is A

upvoted 2 times

 **JJY888** 6 months, 1 week ago

Selected Answer: A

1 is globally routable and the other is unique to the organization. One comes from the ISP and the other is generated privately. Both use the same subnet. /64, /128. etc.

upvoted 4 times

 **Dutch012** 6 months, 2 weeks ago

D is wrong in global unicast first 3 hexets are allocated via ISP, not like unique local.

the answer is A, both use the 4th hexet for subnetting.

upvoted 2 times

 **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: D

The correct answer it's D for me

upvoted 1 times

 **Rynurr** 6 months, 3 weeks ago

Selected Answer: D

Yeah, looks like "D" is the correct answer.

upvoted 2 times

 **j1mlawton** 7 months ago

Selected Answer: D

Think D is maybe the better answer

upvoted 2 times

Question #921

Topic 1

An engineer must configure the IPv6 address 2001:0db8:0000:0000:0700:0003:400F:572B on the serial0/0 interface of the HQ router and wants to compress it for easier configuration. Which command must be issued on the router interface?

- A. ipv6 address 2001:db8::700:3:400F:572B
- B. ipv6 address 2001:db8:0::700:3:4F:572B
- C. ipv6 address 2001::db8:0000::700:3:400F:572B
- D. ipv6 address 2001:0db8::7:3:4F:572B

Correct Answer: A

Gateway of last resort is 172.16.2.2 to network 0.0.0.0

```

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.10.10.0/24 is directly connected, GigabitEthernet0/0/0
L    10.10.10.3/32 is directly connected, GigabitEthernet0/0/0
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S    172.16.1.33/32 is directly connected, GigabitEthernet0/0/1
C    172.16.2.0/23 is directly connected, GigabitEthernet0/0/1
L    172.16.2.1/32 is directly connected, GigabitEthernet0/0/1
S*  0.0.0.0/0 [1/0] via 172.16.2.2

```

Refer to the exhibit. A packet that is sourced from 172.16.3.254 is destined for the IP address of GigabitEthernet0/0/0. What is the subnet mask of the destination route?

- A. 0.0.0.0
- B. 255.255.254.0
- C. 255.255.255.0
- D. 255.255.255.255

Correct Answer: C

 **j1mlawton** Highly Voted 7 months ago

Selected Answer: D

If we're looking for the destination subnet mask then I go for D 255.255.255.255
upvoted 6 times

 **dropspablo** Most Recent 1 month ago

Selected Answer: C


Closed mask /32 is not the "connected" subnet (just a "local" host), in this case the interface g0/0/0 has the following configuration: (config-if)# ip add 10.10.10.3 255.255.255.0. Do not get confused, because in the "#show ip route" output, the "Local" ip address (L) will always be shown with a closed mask (255.255.255.255), but the "Connected" network (C) will show the subnet. If asked which host mask would be /32, but the subnet mask is /24.

upvoted 1 times

 **dropspablo** 1 month ago

We don't know if the destination route points to the subnet or the host, but even if the route pointed directly to the host (/32), that's just the configuration, /32 is not considered a subnet, just a local host. If 10.10.10.3 /32 were a subnet then what would its broadcast address be?

upvoted 1 times

 **paolino555** 2 months ago

Selected Answer: D

"for the IP address of GigabitEthernet0/0/0"
upvoted 2 times

 **[Removed]** 2 months, 2 weeks ago

Selected Answer: D

Answer D - IP address of GigabitEthernet0/0/0 is a /32
upvoted 1 times

 **Olebogeng_G** 2 months, 3 weeks ago

When you look at the routing table, code C stands for connected network, the network that the interface is connected to. Code L refers to the IP address of the interface that the network is connected to. If the IP address of the interface connected to network 10.10.10.0 is 10.10.10.3, then the subnet of that interface must be /32. So D.

upvoted 3 times

 **shiv3003** 4 months, 2 weeks ago

Selected Answer: D

mask of the destination ip adr
upvoted 1 times

🗨️ 👤 **kynnor** 5 months ago

I think the correct Answer is D.
Routing use the LONGEST MATCH PREFIX Algorithm

<https://networklessons.com/cisco/ccna-200-301/longest-prefix-match-routing>
in this case /32 is longer than /24
upvoted 1 times

🗨️ 👤 **rogi2023** 5 months, 2 weeks ago

Selected Answer: C

It's a bit tricky question. Asume this scenario: You wanna remotely ssh/telnet to that router interface IP. On that router the cmd "sh ip route" shows what in the exhibit, not saying anything how was the netw 10.10.10.0/24 advertised. Starting with IOS 15 (i guess) the output shows also the local intf IP's as JJY888 explained.

I disagree with ike110, because any valid unicast host IP is a /32 address. So therefore they are asking for the /24 subnet from the RT. and the key phrase is "what is the subnet mask of the destination route"

Of course I might be wrong, if the /32 route for the intf was advertised .. So for me the C - correct answer.

upvoted 3 times

🗨️ 👤 **dropspablo** 1 month ago

I gree

upvoted 1 times

🗨️ 👤 **JJY888** 6 months, 1 week ago

Selected Answer: D

This help me clear this up:

A connected route represents the network address. It uses the actual subnet prefix (mask). A local route represents the host address. It always uses the subnet prefix /32. Dec 20, 2021

Connected Routes and Local Routes Explained

ComputerNetworkingNotes

<https://www.computernetworkingnotes.com> > connected-

Connected = Network Address

Local = Address of the interface

So the questing is what is the interface subnet mask?

upvoted 3 times

🗨️ 👤 **ike110** 6 months, 3 weeks ago

Selected Answer: D

The key phrase here is "destined for the IP address of GigabitEthernet0/0/0", which is the ip of the interface and this host. - /32

upvoted 4 times

🗨️ 👤 **SVN05** 6 months, 3 weeks ago

Can someone help to further explain why the answer is C or D for that matter. Thank you.

upvoted 4 times

🗨️ 👤 **mageknight** 6 months, 3 weeks ago

C 10.10.10.0/24 refer to the subnet which is connected to L (local) 10.10.10.3/32. the /32 refer exclusively/exactly to this host and this host is the destination mapped with g0/0/0 interface, so the mask is 255.255.255.255. Sorry for my english...

upvoted 6 times

🗨️ 👤 **zamkljo** 5 months, 2 weeks ago

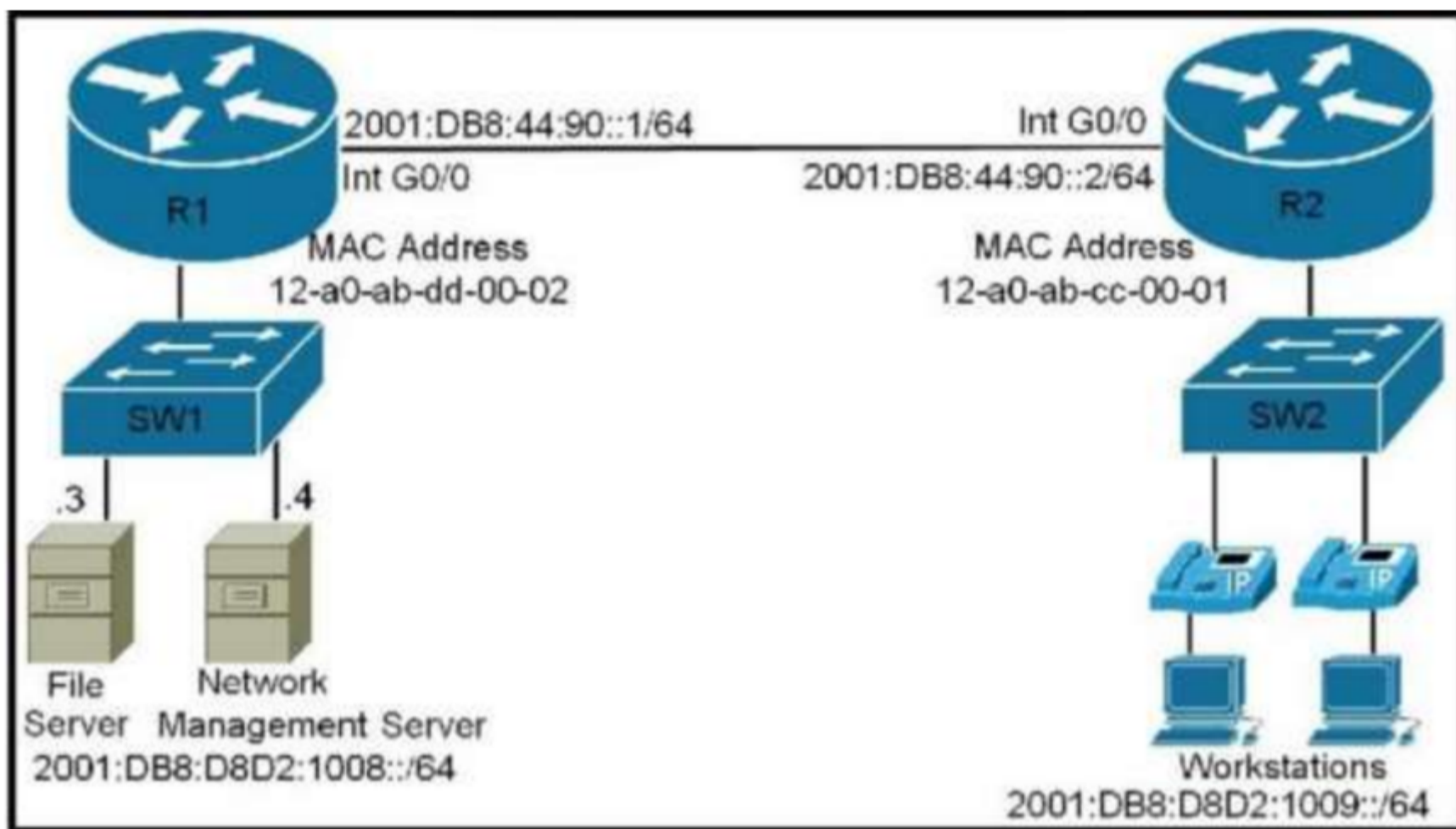
Agree but it would've been better if they made it clear that looking got "Host Route" or "Network Route". That "destination route" still is confusing.

upvoted 3 times

🗨️ 👤 **SVN05** 6 months, 3 weeks ago

Thank you so much.

upvoted 2 times



Refer to the exhibit. The IPv6 address for the LAN segment on router R2 must be configured using the EUI-64 format. Which address must be used?

- A. ipv6 address 2001:DB8:D8D2:1009:10A0:ABFF:FECC:1 eui-64
- B. ipv6 address 2001:DB8:D8D2:1009:1230:ABFF:FECC:1 eui-64
- C. ipv6 address 2001:DB8:D8D2:1009:4331:89FF:FF23:9 eui-64
- D. ipv6 address 2001:DB8:D8D2:1009:12A0:AB34:FFCC:1 eui-64

Correct Answer: B

  **oatmealturkey** Highly Voted 7 months ago

Selected Answer: A

Answer is A. Where did 1230 come from (nowhere) vs. where did 10A0 come from (EUI-64)
upvoted 9 times

  **sdmejia01** Highly Voted 6 months, 4 weeks ago

Correct answer is A. If you change the 7th bit of the Router's MAC Address, you would get 10A0 instead of 12A0.
upvoted 6 times



  **omikun** Most Recent 4 months, 2 weeks ago

answer A:
result from EUI-64 calculator
<https://eui64-calc.princelle.org/>
upvoted 1 times

  **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: A

The correct answers it's A
upvoted 1 times

  **SVN05** 6 months, 3 weeks ago

Can someone explain this question further in detail. Thanks.
upvoted 2 times

  **Stichy007** 6 months, 3 weeks ago

after inserting fffe in the middle of the mac-address you need to flip the 7th bit which would change 0001 0010 (12) to 0001 0000 (10) therefore
answer is A
upvoted 6 times

R7#

172.22.0.0/24 is subnetted, 1 subnets

D 172.22.49.0 [90/284160] via 10.81.22.2, 04:55:53, FastEthernet0/0

10.0.0.0/8 is variably subnetted, 26 subnets, 5 masks

D EX 10.10.10.10/32 [170/35840] via 10.3.5.1, 04:55:55, FastEthernet0/1

D 10.9.1.0/30 [90/33280] via 10.3.5.1, 04:55:56, FastEthernet0/1

B 10.111.99.0/24 [20/0] via 10.6.25.2, 03:58:52

D 10.14.3.0/30 [90/30720] via 10.3.5.1, 04:55:58, FastEthernet0/1

C 10.9.4.0/30 is directly connected, FastEthernet1/0

B 10.100.100.0/24 [20/0] via 10.6.25.2, 03:58:53

D 10.0.1.0/30 [90/30720] via 10.3.5.1, 04:55:58, FastEthernet0/1

D EX 10.10.10.70/32 [170/161280] via 10.3.5.1, 04:55:57, FastEthernet0/1

B 10.90.0.0/16 [200/0] via 0.0.0.0, 03:57:59, Null0

D EX 10.90.1.0/24 [170/158720] via 10.3.5.1, 04:55:57, FastEthernet0/1

D EX 10.90.2.0/24 [170/158720] via 10.3.5.1, 04:55:57, FastEthernet0/1

D 10.90.3.0/29 [90/161280] via 10.3.5.1, 02:46:03, FastEthernet0/1

D EX 10.90.3.0/24 [170/158720] via 10.3.5.1, 02:46:04, FastEthernet0/1

D EX 10.90.4.0/24 [170/158720] via 10.3.5.1, 04:55:59, FastEthernet0/1

D EX 10.90.5.0/24 [170/158720] via 10.3.5.1, 04:55:59, FastEthernet0/1

B* 0.0.0.0/0 [20/0] via 10.6.25.2, 02:22:38

Refer to the exhibit. According to the output, which parameter set is validated using the routing table of R7?

- A. R7 is missing a gateway of last resort.
R7 is receiving routes that were redistributed in EIGRP.
R7 will forward traffic destined to 10.90.8.0/24.
- B. R7 has a gateway of last resort available.
R7 is receiving routes that were redistributed from BGP.
R7 will drop traffic destined to 10.90.8.0/24.
- C. R7 is missing a gateway of last resort.
R7 is receiving routes that were redistributed from BGP.
R7 will forward traffic destined to 10.90.8.0/24.
- D. R7 has a gateway of last resort available.
R7 is receiving routes that were redistributed in EIGRP.
R7 will drop traffic destined to 10.90.8.0/24.

Correct Answer: B

 **sdmejia01** Highly Voted 6 months, 4 weeks ago

Selected Answer: D

I think D is the best answer, however, I don't think the router would drop packets to 10.90.8.0/24, it would just send the packets out the gateway of last resort. Correct me if I am wrong please.

upvoted 7 times


 **Peter_panda** 6 months ago

Router will "send" packets destined for 10.90.8.0/24 to Null0, so basically will drop that destination and not forward those packets

upvoted 5 times

 **kynnor** 5 months ago

Null0 mean summary on that router
upvoted 3 times

  **Stevens0103** 1 month, 1 week ago

The route "10.90.0.0/16" is a summarized address range. And the "Null0" interface essentially means that any traffic destined for that route will be discarded by the router itself.
upvoted 2 times

  **oatmealturkey** Highly Voted 7 months ago

Selected Answer: D

D EX = redistributed in EIGRP. We don't know for sure from what source these routes were redistributed.
upvoted 5 times

  **Toto86** Most Recent 2 months, 2 weeks ago


Selected Answer: B

The router has only a BGP default gateway and 10.90.8.0/24 is a privat address. The router should drop the traffic.
upvoted 2 times

  **ac89l** 4 months ago

Selected Answer: D

Answer is D.
Now move on.....
upvoted 1 times

  **rogi2023** 5 months, 2 weeks ago

Selected Answer: D


missing gateway is wrong - therefore A/C - out
B- is wrong because "R7 is receiving routes that were redistributed from BGP." REDISTRIBUTED FROM ?? BGP is the only Internet routing protocol and redistribution work for routing protocol in automous systems like EIGRP/RIP/OSPF
upvoted 3 times

  **kat1969** 3 weeks, 6 days ago

and the designation 'D EX' indicates an external route redistributed into EIGRP from another external source (routing instance or protocol).
upvoted 1 times


  **kynnor** 5 months ago

I Agree that the answer is D,
small correction for the comment :
BGP is not only internet routing protocol.
It's ROUTING PROTOCOL. BGP has private AS# : 64512 to 65535
upvoted 1 times

  **Stichy007** 6 months, 3 weeks ago

Selected Answer: D

ans is D
upvoted 1 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: D

"D" is correct
upvoted 2 times

Question #925

Topic 1

Which type of IPv4 address type helps to conserve the globally unique address classes?

- A. loopback
- B. multicast
- C. private
- D. public

Correct Answer: C

What are two purposes of HSRP? (Choose two.)

- A. It provides a mechanism for diskless clients to autoconfigure their IP parameters during boot.
- B. It improves network availability by providing redundant gateways.
- C. It groups two or more routers to operate as one virtual router.
- D. It passes configuration information to hosts in a TCP/IP network.
- E. It helps hosts on the network to reach remote subnets without a default gateway.

Correct Answer: BC

 **DantheMann** 1 month ago

Not sure about this one. I though grouping together was VRRP? would be be and D
upvoted 1 times

What are two benefits for using private IPv4 addressing? (Choose two.)

- A. They allow for Internet access from IoT devices.
- B. They alleviate the shortage of public IPv4 addresses.
- C. They provide a layer of security from internet threats.
- D. They supply redundancy in the case of failure.
- E. They offer Internet connectivity to endpoints on private networks.

Correct Answer: BC

 **Shabeth** 2 months, 2 weeks ago

correct
upvoted 1 times

DRAG DROP

```

Router2#show ip route
Gateway of last resort is 10.10.10.13 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
C 10.10.10.8/30 is directly connected, FastEthernet0/3
C 10.10.10.12/30 is directly connected, FastEthernet0/4
C 10.10.10.0/30 is directly connected, FastEthernet0/1
O 10.10.13.0/25 [110/6576] via 10.10.10.9, 00:01:38, FastEthernet0/3
  [110/6576] via 10.10.10.5, 00:01:38, FastEthernet0/2
  [110/6576] via 10.10.10.1, 00:01:38, FastEthernet0/1
C 10.10.10.4/30 is directly connected, FastEthernet0/2
O 10.10.13.144/28 [110/110] via 10.10.10.9, 00:01:39, FastEthernet0/3
  [110/110] via 10.10.10.5, 00:01:39, FastEthernet0/2
  [110/110] via 10.10.10.1, 00:01:38, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 10.10.10.13
    
```

Refer to the exhibit. OSPF is running between site A and site B. Drag and drop the destination IPs from the left onto the network segments used to reach the destination on the right.

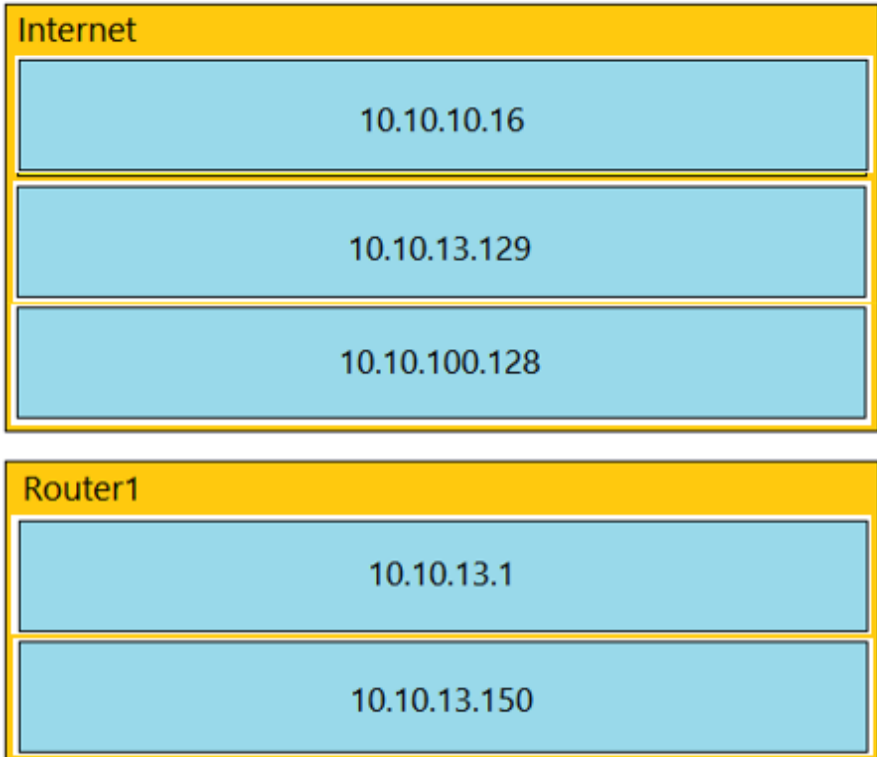
- 10.10.10.16
- 10.10.13.1
- 10.10.13.129
- 10.10.13.150
- 10.10.100.128

Internet

Router1

Correct Answer:

- 10.10.10.16
- 10.10.13.1
- 10.10.13.129
- 10.10.13.150
- 10.10.100.128



Dutch012 Highly Voted 6 months, 2 weeks ago
the answers are correct
upvoted 8 times

Shabeth Most Recent 2 months, 2 weeks ago
given answers are correct
upvoted 1 times

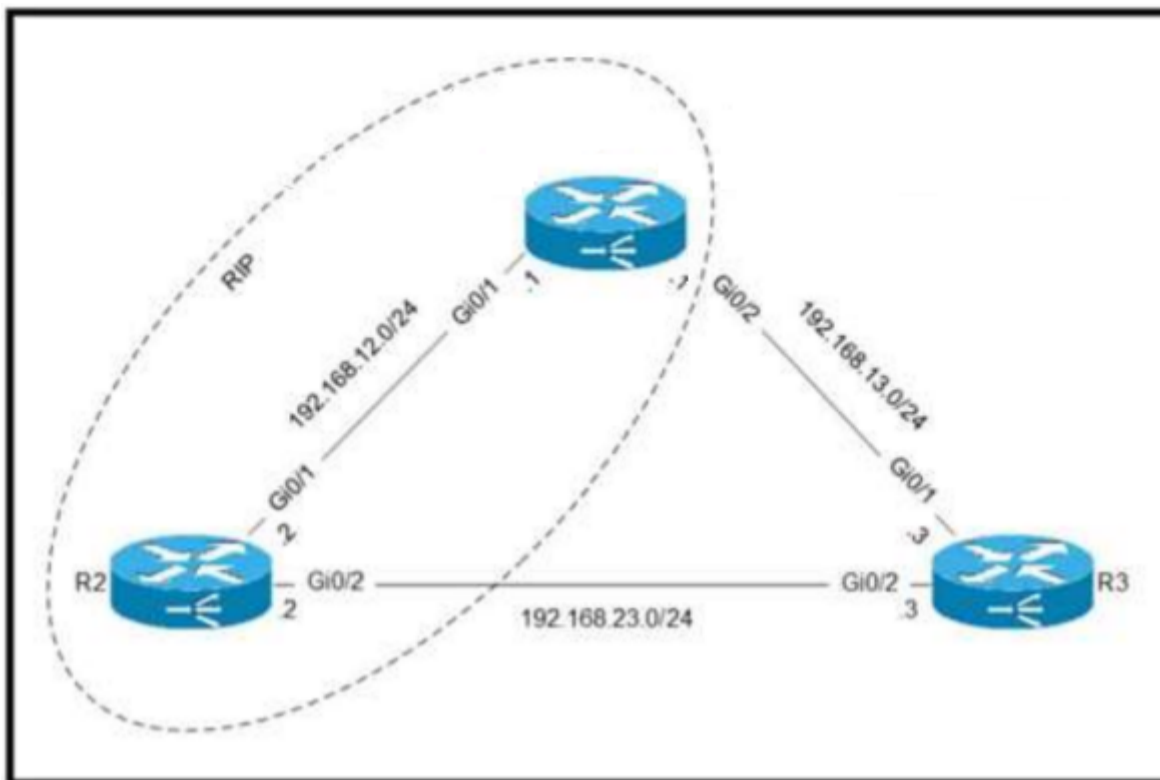
[Removed] 3 months, 3 weeks ago
It should be:
Internet
10.10.10.16
10.10.100.128

Router1
10.10.13.1
10.10.13.129
10.10.13.150
upvoted 2 times

Yannik123 3 months, 3 weeks ago
No given answers are correct the 10.10.13.129 is not included in the:
Network 10.10.13.0/25
First IP 10.10.13.1
Last IP 10.10.13.126
Broadcast 10.10.13.127

neither in the

Network 10.10.13.144/28
First IP 10.10.13.145
Last IP 10.10.13.158
Broadcast10.10.13.159
upvoted 1 times



Refer to the exhibit. Routers R1 and R2 are configured with RIP as the dynamic routing protocol. A network engineer must configure R1 with a floating static route to service as a backup route to network 192.168.23. which command must the engineer configure on R1?

- A. ip route 192.168.23.0 255.255.255.0 192.168.13.3 100
- B. ip route 192.168.23.0 255.255.255.255 192.168.13.3 121
- C. ip route 192.168.23.0 255.255.255.0 192.168.13.3 121
- D. ip route 192.168.23.0 255.255.255.0 192.168.13.3

Correct Answer: C

RidzV Highly Voted 6 months, 1 week ago

Selected Answer: C

Floating route must have AD greater than primary route via RIP which has AD of 120.
upvoted 8 times

When deploying a new network that includes both Cisco and third-party network devices, which redundancy protocol avoids the interruption of network traffic if the default gateway router fails?

- A. VRRP
- B. FHRP
- C. GLBP
- D. HSRP

Correct Answer: A

  **UAE7** Highly Voted  6 months, 3 weeks ago

VRRP, Virtual Router Redundancy Protocol, is a vendor-neutral redundancy protocol that groups a cluster of physical routers (two or more routers) to produce a new single virtual router.

upvoted 7 times

  **douglasbr26** Most Recent  6 months, 1 week ago

The correct would not be D

Hot Standby Router Protocol (HSRP) is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway. Version 1 of the protocol was described in RFC 2281 in 1998. Version 2 of the protocol includes improvements and supports IPv6

upvoted 1 times

  **Yannik123** 3 months, 3 weeks ago

No because it is a third party device included you can't take HSRP you must take VRRP

upvoted 1 times

What are two benefits of private IPv4 addressing? (Choose two.)

- A. propagates routing information to WAN links
- B. provides unlimited address ranges
- C. reuses addresses at multiple sites
- D. conserves globally unique address space
- E. provides external internet network connectivity

Correct Answer: CD

Which Cisco proprietary protocol ensures traffic recovers immediately, transparently, and automatically when edge devices or access circuits fail?

- A. FHRP
- B. VRRP
- C. HSRP
- D. SLB

Correct Answer: C

 **Cynthia2023** 1 month, 4 weeks ago

SLB (Server Load Balancing) is not a Cisco proprietary protocol. SLB is a generic networking technique used to distribute incoming network traffic across multiple servers, and it is not tied to any specific vendor.

upvoted 1 times

 **[Removed]** 2 months, 2 weeks ago

Selected Answer: C

Answer C is correct

upvoted 2 times

 **rlkc** 2 months, 2 weeks ago

Selected Answer: C

C is correct.

upvoted 2 times

 **rlkc** 2 months, 2 weeks ago

To administrator: Please delete the above comment and answer. Thanks.

upvoted 1 times

 **StingVN** 3 months, 1 week ago

Selected Answer: D

The Cisco proprietary protocol that ensures traffic recovers immediately, transparently, and automatically when edge devices or access circuits fail is option D. SLB (Server Load Balancing).

SLB is a feature within Cisco devices that allows for the distribution of incoming network traffic across multiple servers to improve performance and reliability. While SLB primarily focuses on load balancing server traffic, it can also help in recovering traffic when edge devices or access circuits fail.

Options A (FHRP), B (VRRP), and C (HSRP) are First Hop Redundancy Protocols (FHRPs) used for providing redundancy and high availability for the default gateway in a local network. They are not specifically designed to handle traffic recovery when edge devices or access circuits fail.

Therefore, the correct answer is option D. SLB.

upvoted 1 times

 **[Removed]** 2 months, 2 weeks ago

The correct answer is C.

<https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234->

[hsrpguidetochttps://www.examtopycs.com/discussions/cisco/view/111566-exam-200-301-topic-1-question-932-discussion/#.html](https://www.examtopycs.com/discussions/cisco/view/111566-exam-200-301-topic-1-question-932-discussion/#.html)

upvoted 2 times

 **XuniLrve4** 2 months, 2 weeks ago

Wrong...(HSRP) Background and Operations

One way to achieve near-100 percent network uptime is to use HSRP, which provides network redundancy for IP networks, and ensures that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits.


upvoted 2 times

Entry #	
1	192.168.10.0 255.255.254.0
2	192.168.10.0 255.255.255.192
3	192.168.10.0 255.255.0.0
4	192.168.10.0 255.255.224.0

Refer to the exhibit. Which entry is the longest prefix match for host IP address 192.168.10.5?

- A. 1
- B. 2
- C. 3
- D. 4

Correct Answer: B

 **MoHTimo** 1 month, 1 week ago
if all the questions in the exam like this
upvoted 2 times

```

R1# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
Gateway of last resort is not set
C    172.16.0.0/16 is directly connected, Loopback0
     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O    172.16.1.3/32 [110/100] via 10.0.1.100, 00:39:08, Serial0
O    172.16.1.9/32 [110/5] via 172.16.1.50, 00:43:01, Gigabit Ethernet 0/0
D    172.16.1.4/30 [90/7445] via 172.16.9.5, 00:39:08, Gigabit Ethernet 0/0
     [90/7445] via 172.16.4.4, 00:39:08, Gigabit Ethernet 0/4

```

Refer to the exhibit. How does router R1 handle traffic to 172.16.1.4 /30 subnet?

- A. It sends all traffic over the path via 172.16.9.5 using 172.16.4.4 as a backup.
- B. It sends all traffic over the path via 10.0.1.100.
- C. It sends all traffic over the path via 172.16.4.4.
- D. It load-balances traffic over 172.16.9.5 and 172.16.4.4

Correct Answer: D

Which two IPv6 addresses are used to provide connectivity between two routers on a shared link? (Choose two.)

- A. FF02::0001:FF00:0000/104
- B. ff06:bb43:cc13:dd16:1bb:ff14:7545:234d
- C. 2002::512:1204b:1111::1/64
- D. 2001:701:104b:1111::1/64
- E. ::ffff:10.14.101.1/96

Correct Answer: CD

 **oatmealturkey** Highly Voted 7 months ago

Selected Answer: DE

C is incorrect, it contains 2 double colons so not a valid address. ::ffff:10.14.101.1/96 is a valid IPv4-mapped IPv6 address, google it.
upvoted 7 times

 **JJY888** Highly Voted 4 months ago

Selected Answer: AD

The two IPv6 addresses that are used to provide connectivity between two routers on a shared link are:

- A. FF02::0001:FF00:0000/104
- D. 2001:701:104b:1111::1/64

A. FF02::0001:FF00:0000/104 is the multicast address used for the solicited-node multicast address. This address is used to communicate with a specific IPv6 address on a shared link. When a device needs to send an IPv6 packet to a specific device, it first sends a Neighbor Solicitation message to the solicited-node multicast address for the destination IPv6 address. The router receiving this message responds with a Neighbor Advertisement message containing its MAC address.

D. 2001:701:104b:1111::1/64 is a link-local address that is automatically assigned to the interface of the router on the shared link. Link-local addresses are used to communicate with other devices on the same link and are not routable. This address is used by the routers to communicate with each other on the shared link.

upvoted 6 times

 **Cynthia2023** Most Recent 1 month ago

Selected Answer: AD

A. FF02::0001:FF00:0000/104: This multicast address is used for IPv6 Neighbor Discovery's "Solicited-Node Multicast" group.

D. 2001:701:104b:1111::1/64: This is an IPv6 unicast address. While it can be used for connectivity between two routers on a shared link, it's not a multicast address specifically designed for Neighbor Discovery like the address in option A. However, it can still be used for routing and communication between routers on the shared link.

E. is an IPv4-mapped IPv6 address, which is used to represent IPv4 addresses in an IPv6 format, but it's not specifically used for router-to-router connectivity on a shared link. They are specifically used for communication between IPv6-only and IPv4 systems during the transition period from IPv4 to IPv6.

upvoted 2 times

 **Stevens0103** 1 month, 1 week ago

IPv4-mapped IPv6 addresses are of the form ::FFFF:a.b.c.d, where a.b.c.d represents the IPv4 address. These addresses are primarily used for applications and systems that need to communicate with IPv4 devices over an IPv6 network. When an IPv6-only system communicates with an IPv4 system using an IPv4-mapped IPv6 address, the IPv6 network can encapsulate the IPv6 packets within IPv4 packets, allowing the communication to traverse IPv4 networks.

Therefore, IPv4-mapped IPv6 addresses are not designed to provide connectivity between two routers on a shared link. They are specifically used for communication between IPv6-only and IPv4 systems during the transition period from IPv4 to IPv6.

For direct communication and connectivity between two routers on a shared link, you should use standard IPv6 unicast addresses. Unicast addresses are used for point-to-point communication between individual devices, including routers. These addresses follow the standard IPv6 address format and are routable on the IPv6 network.

upvoted 3 times

 **Shabeth** 2 months, 2 weeks ago

Selected Answer: AD

A and D



upvoted 1 times

 **perri88** 3 months ago

the IPv6 address "::ffff:10.14.101.1/96" is a valid representation of an IPv6 address with an embedded IPv4 address. This format is known as IPv4-mapped IPv6 address.

In this case, "::ffff:10.14.101.1" represents the IPv4 address "10.14.101.1" embedded within an IPv6 address. The "::ffff:" prefix indicates that the following part of the address is an IPv4 address. The "/96" suffix indicates the network prefix length, specifying that the first 96 bits represent the network portion of the address.

upvoted 1 times

  **perri88** 3 months ago

Selected Answer: DE

the IPv6 address "::ffff:10.14.101.1/96" is a valid representation of an IPv6 address with an embedded IPv4 address. This format is known as IPv4-mapped IPv6 address.

In this case, "::ffff:10.14.101.1" represents the IPv4 address "10.14.101.1" embedded within an IPv6 address. The "::ffff:" prefix indicates that the following part of the address is an IPv4 address. The "/96" suffix indicates the network prefix length, specifying that the first 96 bits represent the network portion of the address.

upvoted 1 times

  **hamish88** 4 months, 4 weeks ago

What's the problem with A and B?

upvoted 1 times

  **ViKing300** 5 months ago

it is A and D guyz look the dots on the E option



upvoted 1 times

  **bisiyemo1** 6 months, 1 week ago

Selected Answer: DE

I didn't notice the double colon appears twice. C is absolutely wrong

upvoted 2 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: DE

I agree with oatmealturkey. At first i didnt notice 2double colons.

upvoted 1 times

DRAG DROP

```
R1# show ip route | begin gateway
Gateway of last resort is not set
  172.16.0.0/16 is variably subnetted, 5 subnets, 5 masks
O   172.16.2.128/25 [110/3184437] via 207.165.200.250, 00:00:25, Serial0/0/0
O   172.16.3.64/27 [110/3184437] via 207.165.200.250, 00:00:25, Serial0/0/0
O   172.16.3.128/28 [110/3184437] via 207.165.200.250, 00:00:25, Serial0/0/0
O   172.16.3.192/29 [110/3184437] via 207.165.200.250, 00:00:25, Serial0/0/0
O   172.16.4.0/23 [110/3184437] via 207.165.200.250, 00:00:25, Serial0/0/0
  207.165.200.0/24 is variably subnetted, 4 subnets, 2 masks
C   207.165.200.248/30 is directly connected, Serial0/0/0
L   207.165.200.249/32 is directly connected, Serial0/0/0
C   207.165.200.252/30 is directly connected, Serial0/0/1
L   207.165.200.253/32 is directly connected, Serial0/0/1
```

Refer to the exhibit. Drag and drop the learned prefixes from the left onto the subnet masks on the right.

172.16.3.128	255.255.254.0
172.16.3.64	255.255.255.128
172.16.2.128	255.255.255.224
172.16.3.192	255.255.255.240
172.16.4.0	255.255.255.248

Correct Answer:

172.16.3.128	172.16.4.0
172.16.3.64	172.16.2.128
172.16.2.128	172.16.3.64
172.16.3.192	172.16.3.128
172.16.4.0	172.16.3.192

UAE7 Highly Voted 6 months, 3 weeks ago
 answers are correct
 upvoted 8 times

 **StingVN** Highly Voted 3 months ago

172.16.3.128 – 255.255.255.240

172.16.3.64 – 255.255.255.224

172.16.2.128 – 255.255.255.128

172.16.3.192 – 255.255.255.248

172.16.4.0 – 255.255.254.0

upvoted 5 times

Question #937

Topic 1

```
Router1#show ip route
Gateway of last resort is not set
 209.165.200.0/27 is subnetted, 1 subnets
B    209.165.200.224 [20/0] via 10.10.12.2, 00:09:57
 10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C    10.10.10.0/28 is directly connected, GigabitEthernet0/0
C    10.10.11.0/30 is directly connected, FastEthernet2/0
O    10.10.13.0/24 [110/2] via 10.10.10.1, 00:08:34, GigabitEthernet0/0
C    10.10.12.0/30 is directly connected, GigabitEthernet0/1
```

Refer to the exhibit. Which action is taken by the router when a packet is sourced from 10.10.10.2 and destined for 10.10.10.16?

- A. It floods packets to all learned next hops.
- B. It uses a route that is similar to the destination address.
- C. It queues the packets waiting for the route to be learned.
- D. It discards the packets.

Correct Answer: D

 **enzo86** Highly Voted 5 months, 1 week ago

correct. is D.

upvoted 5 times

 **RidzV** Highly Voted 6 months, 1 week ago

Selected Answer: D

Answer is correct.

10.10.10.16 is not in the defined subnet range i.e. 10.10.10.0/28 and since default gateway is not set, packets to the undefined destination address will be dropped.

upvoted 5 times

 **[Removed]** Most Recent 2 months, 1 week ago

Selected Answer: D

D. It discards the packets.

There's no route to the destination so it discards the packets.

upvoted 1 times

 **ac89l** 4 months ago

Selected Answer: B

This is broadcast address, and it will be routed to closest route matching the subnet.

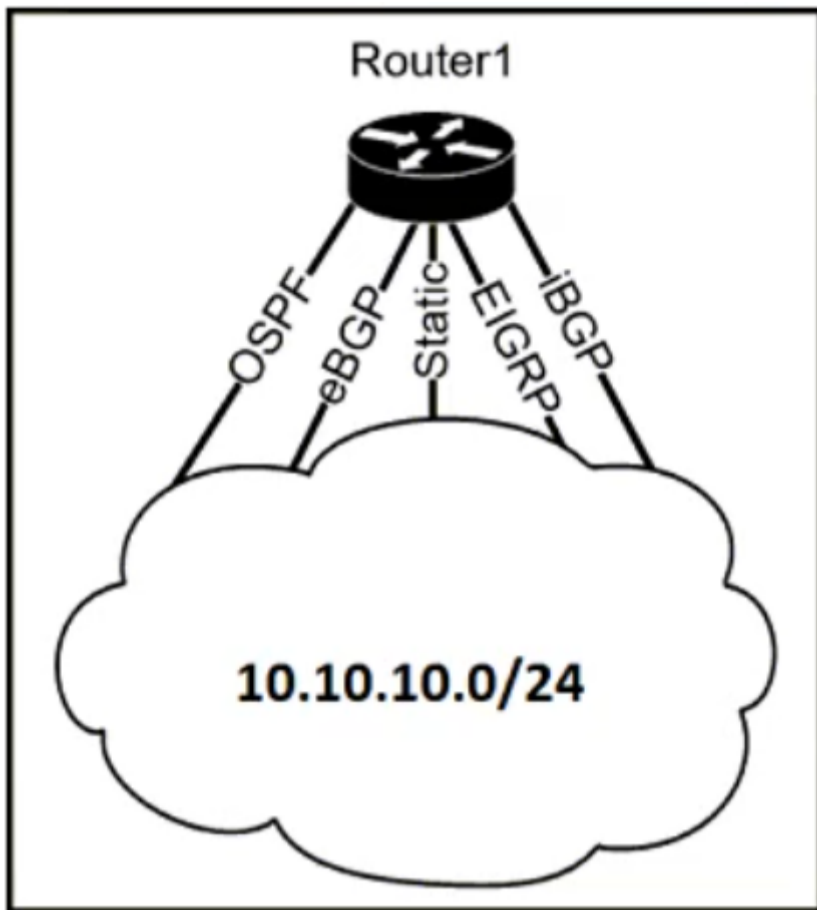
upvoted 1 times

 **ac89l** 4 months ago

my bad, the answer is D

upvoted 1 times

DRAG DROP



Refer to the exhibit. The Router1 routing table has multiple methods to reach 10.10.10.0/24 as shown. The default Administrative Distance is used. Drag and drop the network conditions from the left onto the routing methods that Router1 uses on the right.

- All protocols are up.
- OSPF and eBGP are down.
- The static route and eBGP are down.
- The static route and EIGRP are down.
- The static route and OSPF are down.

eBGP

EIGRP

Static

Correct Answer:

- All protocols are up.
- OSPF and eBGP are down.
- The static route and eBGP are down.
- The static route and EIGRP are down.
- The static route and OSPF are down.

- eBGP**
 - The static route and EIGRP are down.
 - The static route and OSPF are down.
- EIGRP**
 - The static route and eBGP are down.
- Static**
 - All protocols are up.
 - OSPF and eBGP are down.

Dutch012 Highly Voted 6 months, 2 weeks ago

The answers are correct
upvoted 9 times

JJY888 Highly Voted 6 months, 1 week ago

Directly connected interface 0
Static route 1
Dynamic Mobile Network Routing (DMNR) 3
EIGRP summary route 5
External BGP 20
EIGRP internal route 90
IGRP 100
Open Shortest Path First (OSPF) 110
Intermediate System to Intermediate System (IS-IS) 115
Routing Information Protocol (RIP) 120
Exterior Gateway Protocol (EGP) 140
ODR 160
EIGRP external route 170
Internal BGP 200
Next Hop Resolution Protocol (NHRP) 250[6]
Default static route learned via DHCP 254[citation needed]
Unknown and unused 255[b]
upvoted 7 times

DavidCisco Most Recent 5 months, 1 week ago

<https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/15986-admin-distance.html>
upvoted 1 times

Stichy007 6 months, 3 weeks ago

Its basically asking what would happen based on the routing methods used. so if and interface is using ebgp all other routing options will be down.
upvoted 2 times

gewe 7 months ago

can someone tell me what is right answer for this. I think I lost in this question
upvoted 4 times

Peter_panda 6 months ago

Very annoying question.
It should be translated as "Static route will be used if: all protocols are up and/or eBGP&EIGRP&OSPF are down (but not the static route)" and the same for the routing protocols (BGP learned route will be used if: static route is down... and so on)
upvoted 10 times


mageknight 6 months, 3 weeks ago

me too
upvoted 4 times

An engineer must configure a core router with a floating static default route to the backup router at 10.200.0.2. Which command meets the requirements?

- A. ip route 0.0.0.0 0.0.0.0 10.200.0.2 1
- B. ip route 0.0.0.0 0.0.0.0 10.200.0.2 10
- C. ip route 0.0.0.0 0.0.0.0 10.200.0.2
- D. ip route 0.0.0.0 0.0.0.0 10.200.0.2 floating

Correct Answer: B

 **Yannik123** 3 months, 3 weeks ago

Selected Answer: B

Floating static default route must have a higher AD so B is the only correct answer.
upvoted 2 times

 **douglasbr26** 6 months, 1 week ago

The correct answer would be "A" static route cost is 1
upvoted 2 times

 **imigr** 6 months ago

the question is for a floating static default route (backup), therefore "B" is correct with route cost 10
upvoted 6 times

```
CPE# show run | include ip route
ip route 0.0.0.0 0.0.0.0 203.0.113.1 21

CPE# show ip route 203.0.113.1
Routing entry for 203.0.113.0/30
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via Ethernet0/1
    Route metric is 0, traffic share count is 1

CPE# ping 203.0.113.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

CPE# show ip route
Gateway of last resort is 198.51.100.1 to network 0.0.0.0
B*   0.0.0.0/0 [20/0] via 198.51.100.1, 00:02:07
     198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks
C     198.51.100.0/30 is directly connected, Ethernet0/0
L     198.51.100.2/32 is directly connected, Ethernet0/0
     203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C     203.0.113.0/30 is directly connected, Ethernet0/1
L     203.0.113.2/32 is directly connected, Ethernet0/1
```

Refer to the exhibit. After configuring a new static route on the CPE, the engineer entered this series of commands to verify that the new configuration is operating normally. When is the static default route installed into the routing table?

- A. when a route to 203.0.113.1 is learned via BGP
- B. when 203.0.113.1 is no longer reachable as a next hop
- C. when the default route learned over external BGP becomes invalid
- D. when the default route learned over external BGP changes its next hop

Correct Answer: C

 **Kerrera** 2 months ago

Selected Answer: C

Floating static route BGP back up, AD=21
upvoted 1 times

 **ananiamia** 2 weeks, 4 days ago

twentyOne?
upvoted 1 times

```

R_1# show ip route
.....
D 192.168.20.0/26 [90/24513456] via 10.10.10.1
R 192.168.20.0/24 [120/5] via 10.10.10.2
O 192.168.0.0/19 [110/219414] via 10.10.10.13
B 192.168.0.0/16 is variably subnetted, 4 subnets, 4 masks
D 192.168.20.0/27 [90/4123710] via 10.10.10.12
D 192.168.20.0/25 [90/14464211] via 10.10.10.11
S. 0.0.0.0/0 [1/0] via 10.10.10.14

```

Refer to the exhibit. Packets are flowing from 192.168.10.1 to the destination at IP address 192.168.20.75. Which next hop will the router select for the packet?

- A. 10.10.10.1
- B. 10.10.10.11
- C. 10.10.10.12
- D. 10.10.10.14

Correct Answer: B

 **AndreaGambera** 2 weeks, 6 days ago

B is Correct !
upvoted 1 times

 **MadKisa** 2 months ago

Selected Answer: B

Answer is correct
upvoted 1 times

 **[Removed]** 2 months, 2 weeks ago

Selected Answer: B

Answer B is correct
upvoted 1 times

 **yousfs1212** 2 months, 2 weeks ago

Selected Answer: C

The router will select 10.10.10.12 as the next hop for the packet.

The routing table shows that there are four routes to the destination subnet 192.168.20.0/24. The first three routes are for more specific subnets of 192.168.20.0/26, 192.168.20.0/27, and 192.168.20.0/25. When there are multiple routes to the same destination subnet, the router will select the route with the longest prefix match. In this case, the route with the longest prefix match is 192.168.20.0/27, which has a prefix length of 27. The next hop for this route is 10.10.10.12.

The fourth route in the routing table is for the default route, which is used when the destination IP address does not match any of the other routes in the table. The default route has a prefix length of 0, which means that it matches any destination IP address. The next hop for the default route is 10.10.10.14.

Since the destination IP address in this case matches the route with the longest prefix match (192.168.20.0/27), the router will select the next hop for that route, which is 10.10.10.12.

upvoted 1 times

 **kat1969** 3 weeks, 6 days ago

The 192.168.20.0/27 match indicates that the subnet is subnet 20.0 not subnet 20.64, ergo an address of 192.168.20.75 would not be in the subnet for that prefix.

upvoted 1 times

 **Stevens0103** 1 month, 1 week ago

This is for you:
<https://www.cisco.com/en/US/docs/security/pix/pix50/configuration/guide/subnets.html>

upvoted 1 times

 **MadKisa** 2 months, 1 week ago

/27 left u with 30 usable addresses and u need to reach 192.168.20.75, so answer B is correct

upvoted 1 times

🗨️ **Friday_Night** 3 months, 2 weeks ago

the longest matching prefix is not infallible guys....don't be too excited to answer C
upvoted 2 times

🗨️ **Leethy** 5 months ago

Selected Answer: C

To determine the next hop for the packet from 192.168.10.1 to the destination IP address 192.168.20.75, we need to find the most specific matching route in the routing table. Let's analyze the given routing table:

192.168.20.0/26 (90/24513456) via 10.10.10.1
192.168.20.0/24 (120/5) via 10.10.10.2
192.168.20.0/27 (90/4123710) via 10.10.10.12
192.168.20.0/25 (90/14464211) via 10.10.10.11
0.0.0.0/0 (1/0) via 10.10.10.14

The destination IP address 192.168.20.75 falls within the following subnets:

192.168.20.0/26
192.168.20.0/24
192.168.20.0/27
192.168.20.0/25

Among these, the most specific match (with the longest prefix) is the /27 subnet (3rd entry). Thus, the router will select the next hop 10.10.10.12 for the packet. The correct answer is:

C. 10.10.10.12
upvoted 2 times

🗨️ **[Removed]** 2 months, 2 weeks ago

/27 means 5 bits in the host portion. $2^5 = 32$ (-2) = 30 assignable IP addresses so the range will be 192.168.20.1 to 192.168.20.30. The question says : to the destination at IP address 192.168.20.75 therefore it can't be C
upvoted 1 times

🗨️ **Stevens0103** 1 month, 1 week ago

This is for you:

<https://www.cisco.com/en/US/docs/security/pix/pix50/configuration/guide/subnets.html>

upvoted 1 times

🗨️ **HM01** 2 months, 3 weeks ago

Bro 192.168.20.75 is not in the range of /27.

In a /27 subnet, there are 32 IP addresses in total. However, the first address (192.168.20.0) is the network address, and the last address (192.168.20.31) is the broadcast address. Therefore, these two addresses are not usable for host assignment.

B is correct

upvoted 2 times

🗨️ **hamish88** 4 months, 3 weeks ago

Come on now. The highest IP address that can fall in the 192.168.20.0/27 range is 192.168.20.30. The answer B is correct.

upvoted 6 times

🗨️ **kennie0** 3 months, 3 weeks ago

you didnt justify your answer. She did, however.

upvoted 1 times

🗨️ **MadKisa** 2 months ago

What is there to justify it's basic knowledge

upvoted 1 times

🗨️ **Brocolee** 2 months, 1 week ago

Hamish88 wrote: "... The highest IP address that can fall in the 192.168.20.0/27 range is 192.168.20.30."

What do you mean by hamish88 didn't justify the answer? He literally explained that the highest useable IP address range in the /27 block is 192.168.20.30.

Can you even read? read again.

upvoted 1 times

🗨️ **douglasbr26** 6 months, 1 week ago

the correct answer


upvoted 4 times

A router received three destination prefixes: 10.0.0.0/8, 10.0.0.0/16, and 10.0.0.0/24. When the show ip route command is executed, which output does it return?


- A. Gateway of last resort is 172.16.1.1 to network 0.0.0.0
 - o E2 10.0.0.0/8 [110/5] via 192.168.1.1, 0:01:00, Ethernet0
 - o E2 10.0.0.0/16[110/5] via 192.168.2.1, 0:01:00, Ethernet1
 - o E2 10.0.0.0/24[110/5] via 192.168.3.1, 0:01:00, Ethernet2
- B. Gateway of last resort is 172.16.1.1 to network 0.0.0.0
 - o E2 10.0.0.0/8 [110/5] via 192.168.1.1, 0:01:00, Ethernet0
- C. Gateway of last resort is 172.16.1.1 to network 0.0.0.0
 - o E2 10.0.0.0/24[110/5] via 192.168.3.1, 0:01:00, Ethernet2
- D. Gateway of last resort is 172.16.1.1 to network 0.0.0.0
 - o E2 10.0.0.0/16[110/5] via 192.168.2.1, 0:01:00, Ethernet1
 - o E2 10.0.0.0/24[110/5] via 192.168.3.1, 0:01:00, Ethernet2


Correct Answer: A

 **shiv3003** Highly Voted 4 months, 3 weeks ago
wait what??
upvoted 6 times


 **ac89l** 4 months, 1 week ago
exactly ...
upvoted 4 times


 **ac89l** Highly Voted 4 months ago
WTH i paid for ??
upvoted 5 times


 **MadKisa** 2 months ago
This answer is actually correct, these are all different subnets
upvoted 2 times


 **Nwanna1** Most Recent 1 day, 2 hours ago
Explanation
For the purpose of installing routes in the routing table, the router considers different prefix lengths as different destinations. That is why multiple routes from the same and/or different routing protocols are installed in the routing table. Tie breaker is longest match rule, that selects the route with the longest subnet mask (prefix length) from among routes already in the routing table.

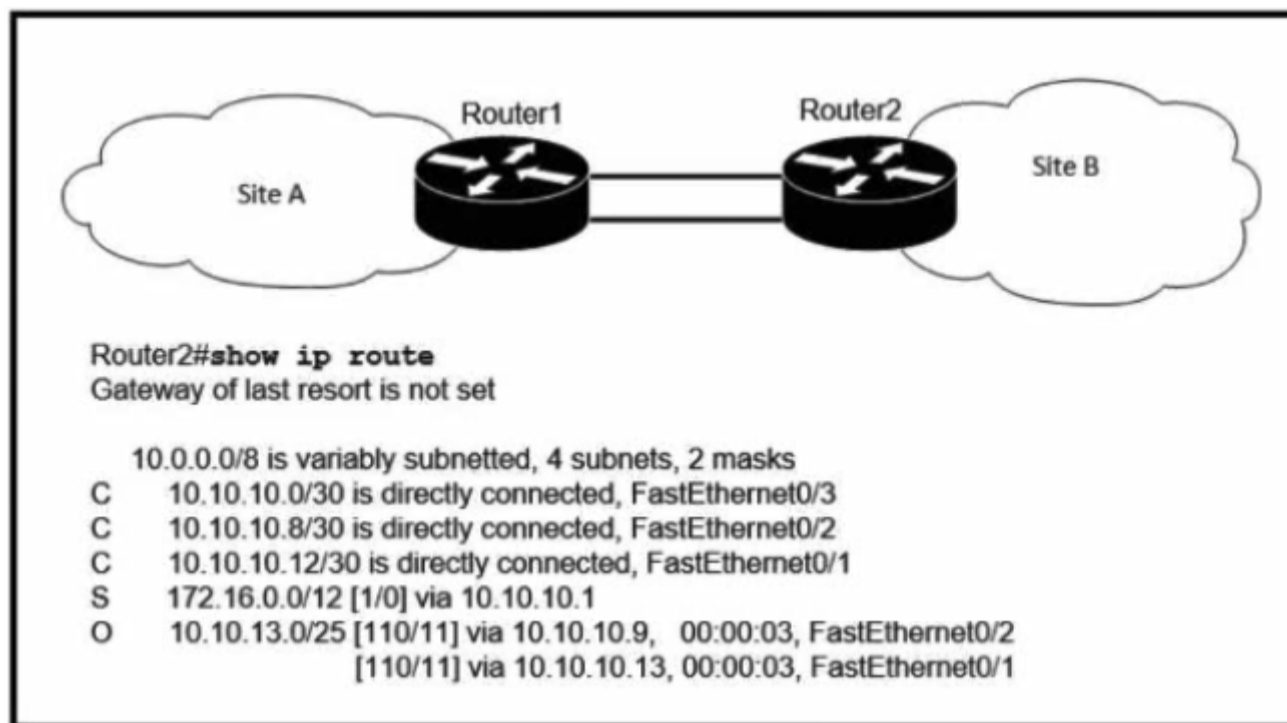
Reference: <https://www.cisconetsolutions.com/introduction-to-routing-protocols/>
so A is correct
upvoted 1 times

 **MadKisa** 2 months ago
Selected Answer: A
Answer is correct
upvoted 2 times

 **Yannik123** 3 months, 3 weeks ago
Can someone explain. At first i thought answer A is right because every präfix have his own next hop interface but also answer B could be possible, because the /16 and /24 subnets are included in the /8 subnet?
upvoted 2 times

 **studying_1** 3 months, 2 weeks ago
it will add all three, because they're different destination. the prefix is different, all get added in this case, correct answer is A
upvoted 4 times

 **studying_1** 3 months, 2 weeks ago
right, it could be B, i take what i said earlier back lol je ne connais pas la reponse maintenant lol
upvoted 2 times



Refer to the exhibit. User traffic originating within site B is failing to reach an application hosted on IP address 192.168.0.10, which is located within site A. What is determined by the routing table?

- A. The traffic is blocked by an implicit deny in an ACL on router2.
- B. The lack of a default route prevents delivery of the traffic.
- C. The traffic to 192.168.0.10 requires a static route to be configured in router1.
- D. The default gateway for site B is configured incorrectly.

Correct Answer: D

oatmealturkey Highly Voted 7 months ago

Selected Answer: B

There is no route in the routing table that matches the destination and there is no default route in the routing table for packets whose destination don't match any of the routes, so the answer is B. You can't determine anything about how a default gateway has been configured by looking at a routing table, default route/gateway of last resort is a different concept than default gateway.

upvoted 13 times

purenuker Highly Voted 5 months, 2 weeks ago

One of the dumbest questions with the dumbest answers ...

upvoted 5 times

_mva Most Recent 1 month, 1 week ago

Default gateways are only used when routing isn't enabled. B is correct.

upvoted 1 times

Vikramaditya_J 1 month, 1 week ago

Selected Answer: B

As the option D says "The default gateway for site B is configured incorrectly." but there's no any default gateway configured on Router B. Therefore, the statement in option D is not correct. In this scenario, only option B is the most accurate option.

upvoted 1 times

yuz1227 6 months, 1 week ago

Selected Answer: B

Yup.. definetly B.. Correct answer is B

upvoted 2 times

Rynurr 6 months, 3 weeks ago

Selected Answer: B

Definitely "B"

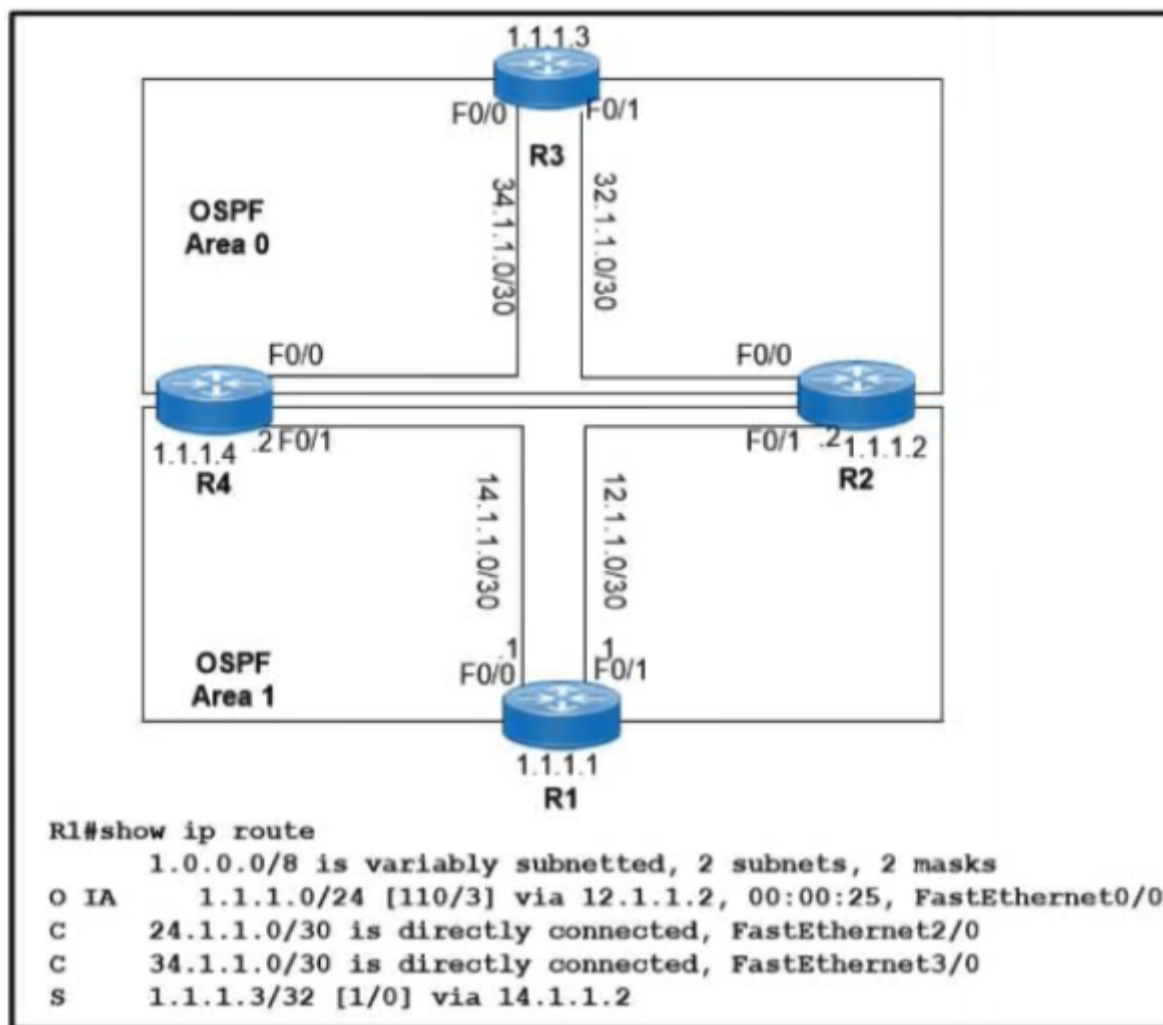
upvoted 3 times

sdmejia01 6 months, 4 weeks ago

Selected Answer: B

Correct answer is B. oatmealturkey is right.

upvoted 4 times



Refer to the exhibit. Which two values does router R1 use to identify valid routes for the R3 loopback address 1.1.1.3/32? (Choose two.)

- A. lowest cost to reach the next hop
- B. highest administrative distance
- C. lowest metric
- D. highest metric
- E. lowest administrative distance

Correct Answer: CE

andrizo 2 weeks, 2 days ago

Selected Answer: CE

Cost is accounted in metric. The format is (AD/metric).
upvoted 1 times

dropspablo 2 months, 2 weeks ago

Selected Answer: CE

1 - longer mask.
2 - lowest AD.
3 - Lowest metric.

In the static route the default metric is always 0 (zero), and from what I understand it cannot be changed. That's why, in two static routes to the same subnet destination, the static route is usually chosen among the dynamic protocols, as it always has a metric of 0 (having the adjustment option available for Administrative Distance only, but predominant).

Letter A is wrong because the final route decision would be based on the metric that calculates the value up to the network destination (lowest), and not just the cost of the next hop. Also, the expression Cost usually refers to OSPF metric, but even in OSPF the decision of the predominant route is made by the sum of all costs to the final destination, resulting in the value of its metric, the decision is never taken based on the cost of the next hop only. Please correct me if I'm wrong!

upvoted 4 times

jonathan126 4 months, 3 weeks ago

Not sure.. If the question is asking which route the router should choose, then it would be by the longest prefix.

If the question is asking what values the router base on to put the route into the routing table, then it would be C and E. Option A seems to be a sub-set of option C.

upvoted 1 times

DINVIS 5 months ago

lowest cost and lowest administrative distance is the right answer
A&E

upvoted 2 times

  **hamish88** 4 months, 3 weeks ago



Did you mean C and E?

upvoted 2 times

  **studying_1** 4 months, 1 week ago

yes, C & E

upvoted 3 times

  **Leethy** 5 months, 1 week ago

Selected Answer: AE

The two values that router R1 uses to identify valid routes for the R3 loopback address 1.1.1.3/32 are:

A. Lowest cost to reach the next hop: Router R1 will look for the route with the lowest cost to reach the next hop, as determined by the routing protocol being used. This is typically the metric or cost associated with the path to the next hop.

E. Lowest administrative distance: If there are multiple routes with the same cost, router R1 will use the administrative distance to determine the best path. The administrative distance is a value assigned to each routing protocol that indicates the reliability of the routing information. A lower administrative distance indicates a more reliable source of routing information.

Therefore, options A and E are the correct answers.

upvoted 2 times

  **blue91235** 5 months, 1 week ago

shouldn't it be A and E ?

upvoted 2 times

  **beerbiceps1** 5 months, 1 week ago



shouldn't it be AE? Please correct me if i am wrong.

upvoted 3 times

What is the role of community strings in SNMP operations?

- A. It translates alphanumeric MIB output values to numeric values.
- B. It passes the Active Directory username and password that are required for device access.
- C. It serves as a sequence tag on SNMP traffic messages.
- D. It serves as a password to protect access to MIB objects.

Correct Answer: D

  **JJY888** 6 months, 1 week ago

Selected Answer: D

<https://www.dnsstuff.com/snmp-community-string#what-is-an-snmp-community-string>
upvoted 2 times

  **UAE7** 6 months, 3 weeks ago

answer is correct

The "SNMP community string" is like a user ID or password that allows access to a router's or other device's statistics (MIB objects)
upvoted 2 times

  **gewe** 6 months, 4 weeks ago

@ carloshmg here <https://www.examtopics.com/>
upvoted 1 times

  **carloshmg_90** 7 months ago

@gewe

Hello,
all good?
where do you find these questions that they published yesterday?
upvoted 1 times

  **gewe** 7 months ago

sorry. answer is correct
upvoted 1 times

  **carloshmg_90** 7 months ago

@gewe

Hello,
all good?
where do you find these questions that they published yesterday?
upvoted 1 times

  **gewe** 7 months ago

B sound better
upvoted 1 times

Which syslog severity level is considered the most severe and results in the system being considered unusable?

- A. Error
- B. Emergency
- C. Alert
- D. Critical

Correct Answer: B

  **Ciscoman021** 5 months, 1 week ago

Selected Answer: B

Syslog is a standard for logging messages and events on network devices. It uses severity levels to indicate the severity of the message or event being logged. The syslog severity levels range from 0 (Emergency) to 7 (Debug).

Among these severity levels, Emergency (severity level 0) is considered the most severe. Messages logged at this level indicate a catastrophic system failure or complete system shutdown, and the system is considered unusable. This severity level should be reserved for only the most severe and critical events that require immediate attention.

Therefore, the syslog severity level that is considered the most severe and results in the system being considered unusable is Emergency (severity level 0).

upvoted 3 times

  **UAE7** 6 months, 3 weeks ago

Level 0 is the most severe syslog level. Level 0 indicates an emergency, rendering the system unusable.

upvoted 3 times

The clients and DHCP server reside on different subnets. Which command must be used to forward requests and replies between clients on the 10.10.0.1/24 subnet and the DHCP server at 192.168.10.1?

- A. ip route 192.168.10.1
- B. ip dhcp address 192.168.10.1
- C. ip default-gateway 192.168.10.1
- D. ip helper-address 192.168.10.1

Correct Answer: D

  **[Removed]** 2 months, 1 week ago

Selected Answer: D

D. ip helper-address 192.168.10.1

upvoted 1 times

  **JJY888** 6 months, 1 week ago

Selected Answer: D

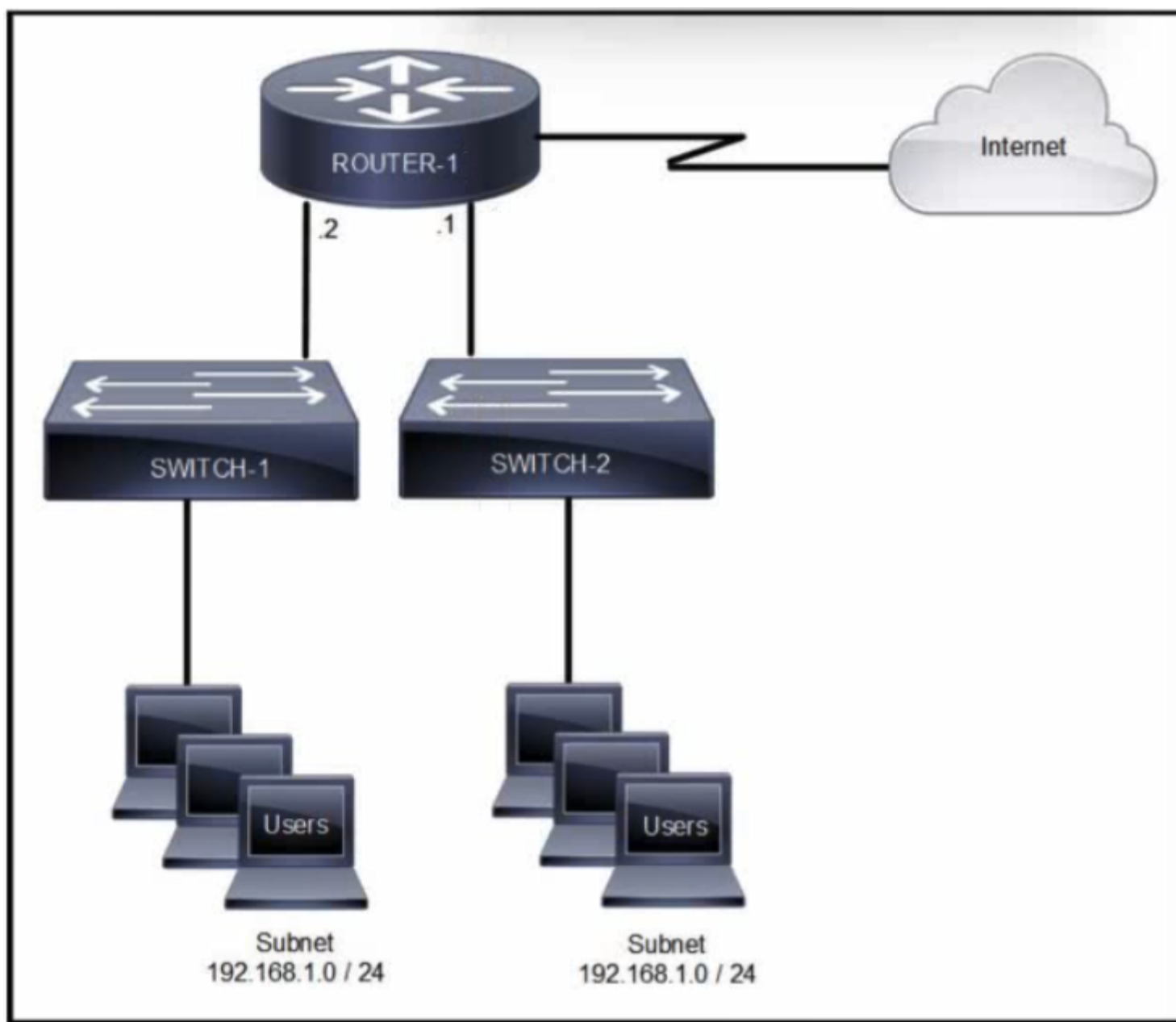
This question is not clear but easy if you know the material.

upvoted 3 times

  **UAE7** 6 months, 3 weeks ago

The 'ip helper-address' command tells the interface to forward the incoming DHCP message to the configured DHCP server

upvoted 4 times



Refer to the exhibit. Which command set configures ROUTER-1 to allow Internet access for users on the 192.168.1.0/24 subnet while using 209.165.202.129 for Port Address Translation?

A. `ip nat pool CCNA 192.168.0.0 192.168.1.255 netmask 255.255.255.0`

```
access-list 10 permit 192.168.0.0 0.0.0.255
ip nat inside source list 10 pool CCNA overload
```

B. `ip nat pool CCNA 209.165.202.129 209.165.202.129 netmask 255.255.255.255`

```
access-list 10 permit 192.168.1.0 255.255.255.0
ip nat inside source list 10 pool CCNA overload
```

C. `ip nat pool CCNA 192.168.0.0 192.168.1.255 netmask 255.255.255.0`

```
access-list 10 permit 192.168.0.0 255.255.255.0
ip nat inside source list 10 pool CCNA overload
```

D. `ip nat pool CCNA 209.165.202.129 209.165.202.129 netmask 255.255.255.255`

```
access-list 10 permit 192.168.1.0 0.0.0.255
ip nat inside source list 10 pool CCNA overload
```

Correct Answer: A

oatmealturkey Highly Voted 7 months ago

Selected Answer: D

NAT policies perform address translation by translating internal IP addresses to the addresses in a NAT pool.
upvoted 7 times

Rynurr Highly Voted 6 months, 3 weeks ago

Selected Answer: D

Only "D" got the right ACL defined.
upvoted 6 times

  **purenuker** Most Recent 5 months, 2 weeks ago

This question is a total mess - 2 same subnets on different router ports - impossible !
How can answer 'A' be correct when it defines such a dumb range - 192.168.ZERO.0 - 192.168.ONE.0 with netmask for 255 addresses !?!
Examtopics - I will never pay you again !
upvoted 3 times

  **studying_1** 3 months, 2 weeks ago

no, please don't say that, it's an awesome site, the help all of us,
upvoted 1 times

  **studying_1** 3 months, 2 weeks ago

typo they* not the
upvoted 1 times

  **VictorCisco** 5 months, 2 weeks ago

Actually, refer to the exhibit, there are 2!!! INTERFACES ON THE ROUTER, configured with the same subnet address range. So, who can do it?? go one and try!

There is no correct answer.
upvoted 3 times

  **Stichy007** 6 months, 2 weeks ago

Selected Answer: D

D for sure
upvoted 2 times

  **sdmejia01** 6 months, 4 weeks ago

Selected Answer: D

The correct answer is D. The Pool indicates the public addresses you will use to go out the internet. The access list includes the private subnet you will be NATing.
upvoted 3 times

Which IP header field is changed by a Cisco device when QoS marking is enabled?

- A. ECN
- B. Header Checksum
- C. Type of Service
- D. DSCP

Correct Answer: B

  **Rynurr** Highly Voted 6 months, 3 weeks ago

Selected Answer: C

C. Type of Service
For sure
upvoted 8 times

  **Sant11** Most Recent 4 weeks, 1 day ago


Selected Answer: D

Ethernet (802.1Q, 802.1p) -> Class of Service (CoS)
802.11 (Wi-Fi) -> Wi-Fi Traffic Identifier (TID)
MPLS -> Experimental (EXP)
IPv4 e IPv6 -> IP Precedence (IPP)
IPv4 e IPv6 -> Differentiated Services Code Point (DSCP)
upvoted 3 times

  **raptuz** 1 month ago

Selected Answer: D

the RFC 2474 replaced the IPv4 TOS and IP precedence fields with the DS field
https://en.wikipedia.org/wiki/Differentiated_services#Background
upvoted 1 times

  **dropspablo** 2 months, 2 weeks ago

Selected Answer: C

Correct answer letter C (Type of Service), field responsible for marking.

"DSCP services can be constructed by setting the bits in an IP header field (RFC 2474)"

<https://datatracker.ietf.org/doc/html/rfc2474#:~:text=combination%20of%3A%0A%0A%20%20%20%2D-,setting%20bits%20in%20an%20IP%20hea,der%20field,-at%20network%20boundaries>

My conclusion: the field in the IP header would be the Type of Service (ToS) and in IPv6 the Traffic Class in which the marking would occur. Both are 8 bits long and can be tagged with the old 3-bit IPP method (RFC 791) or the modern 6-bit DSCP method (RFC 2474) + ECN (RFC 3168). That is, the DSCP does not represent a field, but a service configuration in the Type of Service (ToS) field in the IPv4 header, or in the Traffic Class field for IPv6.

upvoted 2 times

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: C

Answer C is correct.
IPv4 and IPv6 specify an 8-bit field in their packet headers to mark packets. Both IPv4 and IPv6 support an 8-bit field for marking: the Type of Service (ToS) field for IPv4 and the Traffic Class field for IPv6.
Source : Cisco Netacad
upvoted 1 times

  **no_blink404** 2 months, 2 weeks ago

Selected Answer: D

I think it is DSCP.

https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/qos/cgr1000_Book/qos_mark_cgr1000.pdf

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/16-6/configuration_guide/qos/b_166_qos_9400_cg/b_166_qos_9400_cg_chapter_01.html#concept_ww3_gcb_p1b

upvoted 1 times

  **Dunedrifter** 2 months, 3 weeks ago

Selected Answer: D

cisco netacad says the answer is DSCP. Go for D.

upvoted 1 times

  **Alizadeh** 4 months ago

Selected Answer: D

The Differentiated Services Code Point (DSCP) is a field in the IP header that is used for Quality of Service (QoS) marking. It allows for traffic to be classified into different categories, which can then be used to manage and control traffic flow on the network. This classification and marking is used as a basis for providing different levels of service to different types of traffic.

upvoted 2 times

  **JJY888** 4 months ago

Selected Answer: D

The DSCP field in the IP header is a 6-bit field that is used to specify the priority level of a packet. When QoS marking is enabled on a Cisco device, the device can change the value of the DSCP field in the IP header to mark packets with the appropriate priority level.

C. Type of Service (ToS) is a field in the IP header that was used to specify the priority level of a packet before the introduction of DSCP. QoS marking using DSCP replaces the ToS field with the DSCP field.


upvoted 3 times

  **shiv3003** 4 months, 2 weeks ago

Selected Answer: D

i go for D

upvoted 3 times

  **Dutch012** 6 months, 2 weeks ago

Type of service includes (DSCP + ECN) ECN does not always change or be supported, the only thing that is always used with QOS, and is changing in this field is DSCP so, I would rather go with DSCP than the Type of service.

upvoted 2 times

  **Dutch012** 6 months, 2 weeks ago

the plan is changed, went with C.

upvoted 1 times

  **Stichy007** 6 months, 2 weeks ago

Selected Answer: C

ans is C

upvoted 2 times

  **sdmejia01** 6 months, 4 weeks ago

I think both Type of Service and DSCP are correct answers. Both are in the IP header, right? Correct me if I am wrong please.

upvoted 1 times

  **sdmejia01** 6 months, 4 weeks ago

Sorry I would go with answer C. The IPv4 Header has a 1 byte field called Type of Service, and DSCP lives inside that byte, that's why I think the best answer is C.

upvoted 8 times

DRAG DROP

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

agent	collection of uniquely identifiable objects whose state can be interrogated over SNMP
managed device	network node-controlled by SNMP
MIB	system that runs monitoring applications and controls network nodes
NMS	SNMP component that captures and translates device and network data

Correct Answer:

agent	MIB
managed device	NMS
MIB	managed device
NMS	agent

gewe Highly Voted 6 months, 4 weeks ago
 MIB
 Managed device
 NMS
 Agent
 upvoted 22 times

sdmejia01 Highly Voted 6 months, 4 weeks ago
 I agree with gewe. the right order is:
 MIB
 Managed Device
 NMS
 Agent
 upvoted 6 times

JJY888 Most Recent 4 months ago
 MIB
 Managed device
 NMS
 Agent
 upvoted 2 times

Which DSCP per-hop forwarding behavior is divided into subclasses based on drop probability?

- A. expedited
- B. default
- C. assured
- D. class-selector

Correct Answer: A

  **oatmealturkey** Highly Voted 7 months ago

Selected Answer: C

Assured forwarding, look it up
upvoted 9 times

  **Rynurr** Highly Voted 6 months, 3 weeks ago

Selected Answer: C

Definitely "C"
<https://docs.oracle.com/cd/E19253-01/816-4554/ipqos-intro-10/index.html>
upvoted 5 times

  **shaney67** Most Recent 1 month, 1 week ago

The DSCP (Differentiated Services Code Point) per-hop forwarding behavior that is divided into subclasses based on drop probability is the Assured Forwarding (AF) behavior. The AF behavior allows network administrators to assign packets into one of four classes (AF1, AF2, AF3, and AF4), and within each class, packets are further divided into three drop precedence levels: low drop probability (1), medium drop probability (2), and high drop probability (3).

upvoted 1 times

  **Vikramaditya_J** 4 months, 1 week ago

Selected Answer: C

The DSCP per-hop forwarding behavior that is divided into subclasses based on drop probability is the Assured Forwarding (AF) behavior. The AF behavior is divided into 4 subclasses (AF1, AF2, AF3, and AF4), each with 3 drop probabilities. Each forwarding class provides 3 drop precedences, which allow different levels of drop probability to be assigned to packets with different DSCP values.

3

. Therefore, the AF behavior is used to provide a differentiated quality of service for network traffic by dividing it into subclasses based on drop probability.

upvoted 1 times

  **gewe** 6 months, 4 weeks ago

AF is right

upvoted 3 times

What are two features of the DHCP relay agent? (Choose two.)

- A. assigns DNS locally and then forwards request to DHCP server
- B. minimizes the necessary number of DHCP servers
- C. permits one IP helper command under an individual Layer 3 interface
- D. is configured under the Layer 3 interface of a router on the client subnet
- E. allows only MAC-to-IP reservations to determine the local subnet of a client

Correct Answer: AB

 **oatmealturkey** Highly Voted 7 months ago

Selected Answer: BD

The DHCP relay agent itself does not assign anything locally or otherwise DNS or otherwise, so A is incorrect. It does minimize the number of DHCP servers because it means we don't need a DHCP server on every subnet, so B is correct. You actually can configure more than one IP helper command under an individual Layer 3 interface, so C is incorrect and D is correct.

upvoted 15 times

 **shaney67** Most Recent 1 month, 1 week ago

I would guess C,D however B could also be correct?

upvoted 1 times

 **shaney67** 1 month, 1 week ago

The DHCP relay agent is typically configured under the Layer 3 interface of a router on the client subnet.

To clarify, when you configure a DHCP relay agent on a router, you associate it with the Layer 3 interface that is connected to the client subnet. This router interface is responsible for receiving DHCP broadcast requests from clients on that subnet and forwarding those requests to the DHCP server, which is typically located in a different subnet.

upvoted 1 times

 **shaney67** 1 month, 1 week ago

relay agent allows you to configure only one IP helper (also known as IP helper-address) command under an individual Layer 3 interface. The IP helper-address command is used to specify the IP address of the DHCP server or other services that are available on a different subnet.

upvoted 1 times

 **shaney67** 1 month, 1 week ago

A DHCP relay agent can help minimize the necessary number of DHCP servers in a network. In scenarios where multiple subnets exist and clients in those subnets need IP configuration from a central DHCP server, using a DHCP relay agent can reduce the need for deploying DHCP servers in every subnet.

upvoted 1 times

 **dropspablo** 2 months, 2 weeks ago

Letter C is wrong because in only 1 (one) interface of the L3 device (router, L3 switch) we can configure more than 1 (one) "ip help-address" command Example: (config-if)#ip helper-address 10.10. 10.51 - (config-if)#ip helper-address 10.10.10.52 (on the same interface). From what I understand, this is pretty common to get redundancy between DHCP servers for workstation, although it has some implications.

<https://community.cisco.com/t5/other-network-architecture-subjects/ip-helper-address-with-two-dhcp-server/td-p/260792>

upvoted 1 times

 **jonathan126** 4 months, 3 weeks ago

The feature describes the subject matter, while the benefit is the elaboration based on the feature.


Option B seems to be a benefit rather than a feature

Option C does not say we can only configure one IP helper command, so it is kinda correct, it is also a feature

Option D is a feature.

I would choose C and D. Correct me if I'm wrong.

upvoted 1 times

 **Ciscoman021** 5 months, 2 weeks ago

Selected Answer: BD

B and D

upvoted 2 times

 **VictorCisco** 5 months, 2 weeks ago

Okay, while B and D seems correct. Why not C?

upvoted 1 times

 **Rynurr** 6 months, 3 weeks ago

Selected Answer: BD

I agree with oatmealturkey.
"BD" is the correct answer.
upvoted 2 times

  **Jacques1982** 6 months, 3 weeks ago

Selected Answer: BD

B and D for sure
upvoted 2 times

A DHCP pool has been created with the name CONTROL. The pool uses the next to last usable IP address as the default gateway for the DHCP clients. The server is located at 172.16.32.15. What is the next step in the process for clients on the 192.168.52.0/24 subnet to reach the DHCP server?

- A. ip helper-address 172.16.32.15
- B. ip default-gateway 192.168.52.253
- C. ip forward-protocol udp 137
- D. ip default-network 192.168.52.253

Correct Answer: B

 **oatmealturkey** Highly Voted 7 months ago

Selected Answer: A

The question states that the pool has been created and that it uses the next to last usable IP address as the default gateway for the DHCP clients. So that already implies that B is not the answer. But just to confirm once and for all, 192.168.52.253 is NOT the last usable address, that would be 192.168.52.254. The answer is A because we need to configure a helper address since the DHCP server is on a different subnet.

upvoted 12 times

 **Jacques1982** 6 months, 3 weeks ago

I agree with your answer being A. The default gateway is the next to last so that would be .253. They already state that the default gateway has been set up so you would need a helper address.

upvoted 2 times

 **Zepar** Highly Voted 3 months, 3 weeks ago

To be honest the admin should stop answering the questions and let people decide. so many incorrect answers.

upvoted 6 times

 **Friday_Night** Most Recent 3 months, 2 weeks ago

a DHCP pool consists of usable IP addresses right? But in this question it states that the entire pool is for default gateway use? ("The pool uses the next to last usable IP address as the default gateway for the DHCP clients") I don't get this part...

upvoted 1 times

 **Bhrino** 3 months, 3 weeks ago

Selected Answer: A

need to configure a DHCP Relay agent next to use it so I'd set a

upvoted 1 times

 **DavidCisco** 5 months, 1 week ago

Selected Answer: A

To reach the DHCP server (Para que lleguen) no esta preguntando como se crea el pool si no que hay que hacer para que lleguen a el, osea la A

upvoted 2 times

 **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: A


The correct answer is A

upvoted 2 times

 **lucantonelli93** 6 months, 3 weeks ago

The correct answer is A

upvoted 1 times

 **Rynurr** 6 months, 3 weeks ago

Selected Answer: A

I agree with oatmealturkey. Only "A" makes sense.

upvoted 2 times

 **Jacques1982** 6 months, 3 weeks ago

Difficult question.

So it could be either A or B. I would say A because of you need the hosts on subnet 192.168.52.0 to get a DHCP address from the server. So you would need the ip-helper address.

but...

it says that the subnet of 192 needs to "reach" which doesn't mean it requests the IP but just reach it.. therefore a default gateway of .253 (which is the second to last on that subnet, .254 is the last usable)

upvoted 3 times

  **VictorCisco** 5 months, 2 weeks ago

not difficult but stupid. Another one. What is the next step in the process for clients...
of course on client devices we need to put in dhcp helper command...

of course , on the real exam I would answer A. But the question is dump..

upvoted 2 times

  **Stichy007** 6 months, 3 weeks ago

i agree, next to last is the key term which is more .253, question is worded poorly

upvoted 3 times

Question #954

Topic 1

Which two transport layer protocols carry syslog messages? (Choose two.)

- A. IP
- B. RTP
- C. TCP
- D. UDP
- E. ARP

Correct Answer: CD

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: CD

Given answers are correct - Transport layer protocols are TCP and UDP


upvoted 2 times

  **dropspablo** 2 months, 2 weeks ago

Syslog is transported over UDP 514 or TCP 6514.

<https://blog.invgate.com/what-is-syslog#:~:text=How%20is%20Syslog-,transported,-%3F>

upvoted 2 times

  **Zepar** 3 months, 3 weeks ago

Correct

upvoted 3 times

Question #955

Topic 1

What is the purpose of classifying network traffic in QoS?

- A. configures traffic-matching rules on network devices
- B. services traffic according to its class
- C. identifies the type of traffic that will receive a particular treatment
- D. writes the class identifier of a packet to a dedicated field in the packet header

Correct Answer: C

  **Zepar** 3 months, 3 weeks ago

Correct

upvoted 1 times

DRAG DROP

Drag and drop the Qos features from the left onto the corresponding statements on the right.

classification	applies a specific action to packets whenever the maximum rate of packets is exceeded
marking	set the ToS value to associate a packet with a QoS group
policing	reduces traffic congestion by holding packets and distributing them when the available bandwidth allows
queuing	the overall process of using specific criteria to differentiate traffic into categories

Correct Answer:

classification	queuing
marking	marking
policing	classification
queuing	policing

j1mlawton Highly Voted 7 months ago

I think
 - Policing
 - Marking
 - Queuing
 - Classification
 upvoted 44 times

Shabeth 2 months, 2 weeks ago

this is correct
 upvoted 2 times

bisiyemo1 4 months, 3 weeks ago

Correct
 upvoted 2 times

Dutch012 6 months, 2 weeks ago

I agree with j1mlawton
 upvoted 3 times

valekky Most Recent 2 months, 4 weeks ago

This is misleading. I am totally disappointed. We paid for this.
 upvoted 1 times

Tdawg1968 3 months, 4 weeks ago

I agree. I'm disappointed that the answers they have been chosen past 800 (where we pay to see more) have been the least accurate. I was feeling pretty good with the first set of questions, but now I'm feeling confused and second guessing everything when I see these questions. Then I see everyone is feeling the same. Not good...
 upvoted 4 times

[Removed] 2 months, 2 weeks ago

You even have to pay after question 560 now
 upvoted 1 times

 **JJY888** 4 months ago

What is the purpose of classifying network traffic in QoS?

- A. configures traffic-matching rules on network devices
- B. services traffic according to its class
- C. identifies the type of traffic that will receive a particular treatment
- D. writes the class identifier of a packet to a dedicated field in the packet header

upvoted 1 times

 **yousfs1212** 2 months, 2 weeks ago

Of course C is right!




upvoted 1 times

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
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 R3?

- 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 FastEthernet0/1
ip helper-address 10.0.1.1
!
access-list 100 permit udp host 10.0.1.1 eq 67 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: B

-  **Dutch012** Highly Voted 6 months, 2 weeks ago
Why we should care about ACL? it is not applied on the F 0/1 interface
so logically B and D are right
what do you think guys?
upvoted 7 times
-  **ac89l** 4 months ago
i agree
corrupted question
upvoted 2 times
-  **Bhrino** Highly Voted 3 months, 3 weeks ago

Selected Answer: B

I believe that b and d could work so this has 2 correct answers because you could the name or port number
upvoted 5 times

  **[Removed]** Most Recent 2 months, 2 weeks ago

Selected Answer: B

Answer B
upvoted 1 times

  **krzysiew** 5 months, 1 week ago

Selected Answer: D

here is a similar question
<https://www.examttopics.com/discussions/cisco/view/82007-exam-200-301-topic-1-question-582-discussion/>
upvoted 2 times

  **Goena** 6 months ago

DHCP uses UDP port 67
upvoted 2 times

DRAG DROP

Drag and drop the steps in a standard DNS lookup operation from the left into the order on the right.

An endpoint submits a request for the IP address of a domain name.	Step 1
The DNS submits a request to the domain DNS server.	Step 2
The DNS receives a reply from the domain DNS server.	Step 3
The DNS responds to the endpoint.	Step 4
The DNS submits a request to a root DNS server.	Step 5

Correct Answer:

An endpoint submits a request for the IP address of a domain name.	An endpoint submits a request for the IP address of a domain name.
The DNS submits a request to the domain DNS server.	The DNS submits a request to a root DNS server.
The DNS receives a reply from the domain DNS server.	The DNS submits a request to the domain DNS server.
The DNS responds to the endpoint.	The DNS receives a reply from the domain DNS server.
The DNS submits a request to a root DNS server.	The DNS responds to the endpoint.

 **RidzV** Highly Voted 6 months, 1 week ago

Answer is correct.

The 8 steps in a DNS lookup:

1. A user types 'example.com' into a web browser and the query travels into the Internet and is received by a DNS recursive resolver.
 2. The resolver then queries a DNS root nameserver (.).
 3. The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD.
 4. The resolver then makes a request to the .com TLD.
 5. The TLD server then responds with the IP address of the domain's nameserver, example.com.
 6. Lastly, the recursive resolver sends a query to the domain's nameserver.
 7. The IP address for example.com is then returned to the resolver from the nameserver.
 8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially.
- Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser is able to make the request for the web page:
9. The browser makes a HTTP request to the IP address.
 10. The server at that IP returns the webpage to be rendered in the browser (step 10).

upvoted 12 times

 **[Removed]** Most Recent 2 months, 1 week ago

Given answers are correct.

upvoted 1 times

Which two features introduced in SNMPv2 provide the ability to retrieve large amounts of data in one request and acknowledge a trap using PDUs?
(Choose two.)

- A. Get
- B. GetNext
- C. Set
- D. GetBulk
- E. Inform

Correct Answer: DE

 **mageknight** Highly Voted 6 months, 3 weeks ago

SNMPv2 introduced two features that provide the ability to retrieve large amounts of data in one request and acknowledge a trap using PDUs. These features are:

GetBulkRequest: This feature allows a management station to retrieve a large amount of data in one request, reducing the number of requests needed to retrieve the same information. The GetBulkRequest PDU specifies a starting OID and a maximum number of variables to be returned in a single response.

InformRequest: This feature is used to acknowledge receipt of a trap message from an agent. The InformRequest PDU is similar to the trap PDU, but it includes a request identifier, which allows the management station to match the acknowledgment with the original trap. The InformRequest also requires an acknowledgment from the receiving device, which provides greater reliability in trap delivery.

upvoted 10 times

 **dropspablo** 2 months, 2 weeks ago

I agree!

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/command/nm-snmp-cr-book/nm-snmp-cr-s1.html#wp3859164626:~:text=snmp%20get-,snmp%20get%2Dbulk,snmp%20get%2Dnext,-snmp%20ifmib%20ifalias>

upvoted 1 times

 **Bhrino** Most Recent 3 months, 3 weeks ago

Selected Answer: DE

in order to retrieve Large amounts of data as stated in the question in regards to SNMP v2 is Get bulk message which is just a better version of Get next which is just used to gather information

The Inform Request feature is just used as an acknowledgment of trap messages

upvoted 3 times

 **lolungos** 2 months, 3 weeks ago

So... B and D then...

upvoted 1 times

 **dropspablo** 2 months, 2 weeks ago

D. GetBulk

E. Inform

upvoted 1 times

DRAG DROP

-

Drag and drop the DNS commands from the left onto their effects on the right.

ip domain-lookup	adds an entry to the host table
ip domain-name	completes the FQDN of the DNS server
ip host switch_1 192.168.0.1	displays address-mapping information
ip name-server	enables host-to-IP-address translation
show hosts	specifies the IP address of the DNS server

Correct Answer:

ip domain-lookup	ip host switch_1 192.168.0.1
ip domain-name	ip domain-name
ip host switch_1 192.168.0.1	show hosts
ip name-server	ip domain-lookup
show hosts	ip name-server

 **sdmejia01** Highly Voted 6 months, 3 weeks ago

The answer is correct.
upvoted 13 times

What is the purpose of configuring different levels of syslog for different devices on the network?

- A. to set the severity of syslog messages from each device
- B. to control the number of syslog messages from different devices that are stored locally
- C. to identify the source from which each syslog message originated
- D. to rate-limit messages for different severity levels from each device

Correct Answer: A

 **NetworkGeek00** 1 month, 1 week ago

Selected Answer: A

A is correct
upvoted 1 times

 **Secsoft** 1 month, 3 weeks ago

Why not B?
upvoted 1 times

 **Dunedrifter** 2 months, 3 weeks ago

Selected Answer: A

Correct answer is A
upvoted 1 times

 **Ciscoman021** 5 months, 2 weeks ago

Selected Answer: A

The purpose of configuring different levels of syslog for different devices on the network is to set the severity of syslog messages from each device.
upvoted 1 times

 **dos2** 6 months, 1 week ago

Selected Answer: A

A correct, D means rate-limit
upvoted 2 times


 **oatmealturkey** 6 months, 3 weeks ago

Configuring different levels of Syslog is a different thing than configuring rate-limiting of Syslog messages.

Rate-limiting: <https://www.oreilly.com/library/view/cisco-ios-cookbook/0596527225/ch18s15.html>

Configuring logging levels: https://www.grandmetric.com/knowledge-base/design_and_configure/syslog-configure-syslog-server-logging-cisco/

Please correct me if I'm wrong.
upvoted 2 times


 **Rynurr** 6 months, 3 weeks ago

Selected Answer: D

The correct answer is "D"
upvoted 3 times

 **oatmealturkey** 6 months, 3 weeks ago

Why D?
upvoted 1 times


 **sdmejia01** 6 months, 3 weeks ago

I would go with D.
upvoted 1 times

 **oatmealturkey** 6 months, 3 weeks ago

It is C. You are thinking of the default gateway, we need the DHCP server address which is 192.168.20.2. The exhibit with the long output is meant to throw us off, just look at the topology diagram and it is there. If we only needed 192.168.10.2 for DHCP for VLAN 10, then we would not need an IP helper address.

upvoted 11 times

 **[Removed]** 2 months, 2 weeks ago

True. I didn't even look at the output, only at the topology to be honest.

upvoted 2 times

Question #963

Topic 1

DRAG DROP

Drag and drop the DNS lookup commands from the left onto the functions on the right.

ip dns server	enables DNS lookup on an individual interface
ip domain list	enables the DNS server on the device
ip domain lookup source-interface	identifies a DNS server to provide lookup services
ip domain name	specifies a sequence of domain names
ip host	specifies the default domain to append to unqualified host names
ip name-server	statically maps an IP address to a hostname

Correct Answer:

ip dns server	ip domain lookup source-interface
ip domain list	ip dns server
ip domain lookup source-interface	ip name-server
ip domain name	ip domain list
ip host	ip domain name
ip name-server	ip host

 **sdmejia01** Highly Voted 6 months, 3 weeks ago

The answers are correct!

upvoted 11 times

Refer to the exhibit. Which minimum configuration items are needed to enable Secure Shell version 2 access to R15?

A. Router(config)#hostname R15 -
R15(config)#ip domain-name cisco.com
R15(config)#crypto key generate rsa general-keys modulus 1024

R15(config)#ip ssh version 2 -

R15(config-line)#line vty 0 15 -
R15(config-line)# transport input ssh

B. Router(config)#crypto key generate rsa general-keys modulus 1024

Router(config)#ip ssh version 2 -
Router(config-line)#line vty 0 15
Router(config-line)# transport input ssh
Router(config)#ip ssh logging events
R15(config)#ip ssh stricthostkeycheck

C. Router(config)#hostname R15 -
R15(config)#crypto key generate rsa general-keys modulus 1024

R15(config-line)#line vty 0 15 -
R15(config-line)# transport input ssh
R15(config)#ip ssh source-interface Fa0/0
R15(config)#ip ssh stricthostkeycheck

D. Router(config)#ip domain-name cisco.com
Router(config)#crypto key generate rsa general-keys modulus 1024

Router(contig)#ip ssh version 2 -
Router(config-line)#line vty 0 15
Router(config-line)# transport input all
Router(config)#ip ssh logging events

Correct Answer: A

  **sdmejia01** Highly Voted 6 months, 3 weeks ago

I think answer is A. You need to set a hostname, a domain name and then the crypto key to enable SSH.
upvoted 8 times

  **AboZouz** 4 months, 4 weeks ago

Host name router already exist in the config !!!
upvoted 1 times

  **[Removed]** 2 months, 2 weeks ago

No, "Router" is the default name
upvoted 1 times

  **jonathan126** 4 months, 3 weeks ago

The hostname Router is default. A hostname must first be configured in order to generate the key.
upvoted 5 times

  **[Removed]** Most Recent 2 months, 2 weeks ago

Selected Answer: A



A is correct
upvoted 1 times

  **YetiPatty** 2 months, 3 weeks ago

Selected Answer: A

just remember the acronym DRUL

upvoted 1 times

  **Bhrino** 3 months, 3 weeks ago

Selected Answer: A

A is the only option that adds a hostname and ip domain name server before generating RSA key making A correct!

upvoted 2 times

  **krzysiew** 5 months, 1 week ago

Selected Answer: A

i agree

upvoted 3 times

```
hostname CPE
service password-encryption

ip domain name ccna.cisco.com
ip name-server 198.51.100.210

crypto key generate rsa modulus 1024

username admin privilege 15 secret s0m3s3cr3t

line vty 0 4
transport input ssh
login local
```

Refer to the exhibit. An engineer executed the script and added commands that were not necessary for SSH and now must remove the commands. Which two commands must be executed to correct the configuration? (Choose two.)

- A. no ip name-server 198.51.100.210
- B. no login local
- C. no service password-encryption
- D. no ip domain name ccna.cisco.com
- E. no hostname CPE

Correct Answer: AB

  **oatmealturkey** Highly Voted 7 months ago

Selected Answer: AC

Login local is required to implement SSH in this case because we are not using AAA authentication. But password service-encryption is not needed because all it does is encrypt any plaintext passwords displayed in the running configuration. It has nothing to do with SSH. For example, you can configure a plaintext password for Telnet access, do service password-encryption to scramble it in the running config, but then when you Telnet into the device, sniff the packet and see that the password is still in plaintext.

upvoted 11 times

  **ahmt** Highly Voted 7 months ago

Selected Answer: AC

SSH Configuration:
hostname CPE
ip domain name ccna.cisco.com
crypto key generate rsa modulus 1024
username admin privilege 15 secret s0m3s3cr3t
line vty 0 4
transport input ssh
login local

upvoted 8 times

  **MJBM** Most Recent 3 months, 2 weeks ago

According to Packet tracer the login local is not required but if you do not have the login local then you need the enable password/secret to access the privilege mode. Correct me if I'm wrong.

upvoted 1 times

  **Bhrino** 3 months, 3 weeks ago

Selected Answer: AC

you need b to use the user name and pass word the answer is A and C

upvoted 2 times

  **bisiyemo1** 6 months, 1 week ago

Selected Answer: AC



AC is correct

upvoted 2 times

  **JJY888** 6 months, 1 week ago

Selected Answer: AC

You will know if you've been studying other material which I strongly suggest.
upvoted 2 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: AC

I agree, should be "AC"
upvoted 2 times

  **sdmejia01** 6 months, 3 weeks ago

Selected Answer: AC

oatmealturkey is right. The answers are AC.
upvoted 2 times

Which two actions are taken as the result of traffic policing? (Choose two.)

- A. bursting
- B. dropping
- C. remarking
- D. fragmentation
- E. buffering

Correct Answer: AE

 **oatmealturkey** Highly Voted 7 months ago

Selected Answer: BC

Traffic policing does not cause bursting at all, in fact it imposes a ceiling so it limits it if anything. Traffic policing enforcement causes packets to be either dropped or re-marked.

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

upvoted 14 times

 **Ciscoboy** Most Recent 1 month ago

Selected Answer: BC

Remarking and dropping

upvoted 1 times

 **shaney67** 1 month, 1 week ago

Two actions that are taken as a result of traffic policing:

Dropping or Discarding Excess Traffic: When traffic policing is enforced and the incoming traffic rate exceeds the allowed rate (defined by a specified threshold), the excess traffic is dropped or discarded. This action helps in maintaining network quality of service (QoS) and prevents congestion caused by an excessive influx of traffic.

Remark or Re-mark Traffic: When traffic policing is applied, the excess traffic can also be remarked or re-marked with a lower priority or a specific Differentiated Services Code Point (DSCP) value. This remarking helps ensure that the exceeded traffic is treated with a lower priority in subsequent stages of the network, allowing for better resource allocation and management.

These actions collectively help in managing network congestion, prioritizing traffic, and ensuring that network resources are utilized efficiently.

upvoted 1 times

 **NetworkGeek00** 1 month, 1 week ago

Selected Answer: BC

B and C correct


upvoted 1 times

 **Ciscoman021** 6 months ago

Selected Answer: BC

Traffic policing propagates bursts. When the traffic rate reaches the configured maximum rate, excess traffic is dropped (or remarked). The result is an output rate that appears as a saw-tooth with crests and troughs. In contrast to policing, traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time. The result of traffic shaping is a smoothed packet output rate.

upvoted 4 times

 **Rynurr** 6 months, 3 weeks ago

Selected Answer: BC

"BC" are correct

upvoted 3 times

 **sdmejia01** 6 months, 3 weeks ago

Selected Answer: BC

B and C are the correct answers!!

upvoted 4 times

 **gewe** 7 months ago

AB is correct

upvoted 1 times

Which two server types support domain name to IP address resolution? (Choose two.)

- A. authoritative
- B. web
- C. file transfer
- D. resolver
- E. ESX host

Correct Answer: *BD*

  **oatmealturkey** Highly Voted 7 months ago

Selected Answer: AD

Web server is not for DNS! This source explains why resolver & authoritative are the correct answers:

<https://www.cloudns.net/wiki/article/202/#:~:text=Authoritative%20DNS%20nameservers%20provide%20answers,etc%20for%20a%20domain%20name.>

upvoted 11 times

  **Ciscoboy** Most Recent 1 month ago

Selected Answer: AD

paid for wrong information

upvoted 1 times



  **shaney67** 1 month, 1 week ago

The two server types that support domain name to IP address resolution are:

Domain Name System (DNS) Servers: DNS servers are specialized servers responsible for translating human-readable domain names (like www.example.com) into IP addresses that computers use to identify each other on a network. DNS servers maintain a database of domain name to IP address mappings, allowing users to access websites and services using easy-to-remember domain names.

Dynamic Host Configuration Protocol (DHCP) Servers: While DHCP servers are primarily responsible for assigning IP addresses to devices on a network, they can also provide domain name resolution information to those devices. When a device connects to a network and obtains an IP address from a DHCP server, it can also receive DNS server information from the DHCP server. This DNS information allows the device to perform domain name to IP address resolution using the DNS server's capabilities.

upvoted 1 times

  **RidzV** 6 months, 1 week ago

Selected Answer: AD

What is DNS resolver?



DNS Resolvers are responsible for providing the correct IP address of a domain name to the requesting host. For example, if you make a request from your web browser and there is no information on your computer about this domain name (it is not cached), your computer will send the request to DNS resolvers. The resolver will then try to find the name servers, that are responsible for this domain name and contain the necessary records. These name servers are called authoritative.

What is authoritative name server?

Authoritative DNS nameservers provide answers to DNS resolvers with the correct IP addresses and records. These name servers contain the DNS zone with all information, like the IP address of the server, the responsible mail servers, etc for a domain name.

Both servers work hand in hand - resolvers ask the authoritative name servers. They cannot be used for different purposes - e.g. authoritative name server cannot be used as DNS resolver or vice versa.

upvoted 2 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: AD

Definitely "AD"

upvoted 3 times

What is a purpose of traffic shaping?

- A. It enables policy-based routing.
- B. It enables dynamic flow identification.
- C. It provides best-effort service.
- D. It limits bandwidth usage.

Correct Answer: D

  **Ciscoman021** Highly Voted  5 months, 2 weeks ago

Selected Answer: D

The purpose of traffic shaping is to limit the bandwidth usage of certain types of network traffic in order to prevent congestion and ensure that critical applications receive the necessary network resources.

Traffic shaping is typically used to enforce Quality of Service (QoS) policies that prioritize certain types of network traffic, such as voice and video traffic, over other less critical traffic. By limiting the bandwidth usage of non-critical traffic, traffic shaping can help prevent network congestion and ensure that the available bandwidth is allocated in a way that meets the organization's priorities.

Therefore, the correct answer is option D: it limits bandwidth usage.

upvoted 5 times

  **shaney67** Most Recent  1 month, 1 week ago

Bandwidth Allocation: Traffic shaping allows administrators to allocate specific amounts of bandwidth to different types of network traffic. This ensures that critical applications or services receive the necessary bandwidth while preventing any single application from hogging all available resources.



upvoted 1 times

  **[Removed]** 2 months, 2 weeks ago

Selected Answer: D

D. It limits bandwidth usage


upvoted 1 times

  **Mariachi** 5 months, 3 weeks ago

Selected Answer: C

just because the other answers are wrong ...

upvoted 1 times

  **Bhrino** 3 months, 4 weeks ago


no for example if someone pays for a certain bandwidth traffic shaping can limit their usage to what they pay for


upvoted 1 times


An engineering team asks an implementer to configure syslog for warning conditions and error conditions. Which command does the implementer configure to achieve the desired result?


- A. logging trap 5
- B. logging trap 2
- C. logging trap 3
- D. logging trap 4


Correct Answer: D


 **ac89l** Highly Voted 4 months, 1 week ago
0Every 1Awesome 2Cisco 3Engineer 4Will 5Need 6Icecream 7Daily
upvoted 9 times

 **learntstuff** Most Recent 1 month, 3 weeks ago
D. Doing the command with a 4 should return logs for 0-4.
Doing it with a 3 should return logs for 0-3
upvoted 2 times

 **MadKisa** 2 months ago
Selected Answer: D
Correct
upvoted 1 times

 **[Removed]** 2 months, 2 weeks ago
Selected Answer: D
Answer D
upvoted 1 times

 **Dunedrifter** 2 months, 3 weeks ago
Selected Answer: D
D is correct
upvoted 1 times

 **HM01** 2 months, 3 weeks ago
Selected Answer: C
C. logging trap 3

Explanation:

The logging trap command is used to set the severity level for syslog messages that will be sent to the syslog server. The severity levels range from 0 to 7, with 0 being the most severe and 7 being the least severe.

In this scenario, the engineering team wants to configure syslog to capture warning conditions and error conditions. The severity level for warning messages is 4 (warning) and for error messages is 3 (error).

Therefore, by using the command logging trap 3, the implementer will configure syslog to capture and send error messages to the syslog server.
upvoted 1 times


 **Mariachi** 5 months, 3 weeks ago
Selected Answer: D
D is correct !

Table 3 Message Logging Level Keywords

Level	Keyword	Description
0	LOG_EMERG	System unstable emergencies
1	LOG_ALERT	Immediate action needed alerts
2	LOG_CRIT	Critical errors
3	LOG_ERR	Error conditions
4	LOG_WARNING	Warning conditions
5	LOG_NOTICE	Normal but significant events
6	LOG_INFO	Informational messages
7	LOG_DEBUG	Debugging messages

2
Critical conditions
LOG_CRIT
errors
3
Error conditions
LOG_ERR
warnings
4
Warning conditions
LOG_WARNING
notifications
5
Normal but significant condition
LOG_NOTICE
informational
6
Informational messages only
LOG_INFO
debugging
7
Debugging messages
LOG_DEBUG
upvoted 2 times

  **rogi2023** 5 months, 2 weeks ago

0- Every - emergency
1-Awesome - alert
2-cisco - critical
3-engineer - error
4-will - warning
5-need - notification
6-ice - informational
7-daily - debug
upvoted 6 times

DRAG DROP

Drag and drop the attack-mitigation techniques from the left onto the types of attack that they mitigate on the right.

Answer Area

Configure the 802.1x authentication protocol	802.1q double-tagging VLAN-hopping attack
Configure the DHCP snooping feature	MAC flooding attack
Configure the native VLAN with a nondefault VLAN	man-in-the-middle spoofing attack
Disable Dynamic Trunking Protocol – switch-spoofing VLAN-hopping attack	switch-spoofing VLAN-hopping attack

Answer Area

Correct Answer:

Configure the 802.1x authentication protocol	Configure the native VLAN with a nondefault VLAN
Configure the DHCP snooping feature	Configure the DHCP snooping feature
Configure the native VLAN with a nondefault VLAN	Configure the 802.1x authentication protocol
Disable Dynamic Trunking Protocol – switch-spoofing VLAN-hopping attack	Disable Dynamic Trunking Protocol – switch-spoofing VLAN-hopping attack

oatmealturkey Highly Voted 7 months ago

MAC flooding attack ----> Configure 802.1x
MITM spoofing attack (read: rogue DHCP server) -----> Configure DHCP snooping
upvoted 26 times

JJY888 Highly Voted 6 months, 1 week ago

I think the answers are corect.
upvoted 7 times

Shabeth 2 months, 2 weeks ago

i agree, the answers are correct
upvoted 1 times

no_blink404 Most Recent 2 months, 2 weeks ago

Provided answer is correct.
<https://www.securew2.com/blog/preventing-man-in-the-middle-mitm-attacks-the-ultimate-guide>
upvoted 1 times

MassNastty1 3 months, 3 weeks ago

oatmeal turkey is correct:

MITM Attacks - DHCP Snooping

MAC Flooding - 802.1X Authentication

802.1Q Double Tagged VLAN Hopping Attacks - Change Native VLAN To non-default VLAN

Switch Spoofing VLAN Hopping - Disable DTP (Set Switchport to Nonnegotiate)

upvoted 5 times

MassNastty1 3 months, 3 weeks ago



i mean incorrect lol

upvoted 2 times

Which WLC management connection type is vulnerable to man-in-the-middle attacks?



- A. console
- B. Telnet
- C. SSH
- D. HTTPS

Correct Answer: B

  **no_blink404** 3 months, 1 week ago


Selected Answer: B

No encryption would mean more chance of eavesdropping on the connection. Correct answer is B
upvoted 1 times

  **RidzV** 6 months, 1 week ago

Selected Answer: B

No encryption, more vulnerabilities
upvoted 2 times

  **Goena** 6 months, 2 weeks ago

Selected Answer: B

Telnet:
<https://itexamanswers.net/question/which-wlc-management-connection-type-is-vulnerable-to-man-in-the-middle-attacks>
upvoted 2 times

```
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 global configuration 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

Which type of encryption does WPA1 use for data protection?

- A. PEAP
- B. TKIP
- C. AES
- D. EAP

Correct Answer: C

  **gewe** Highly Voted 7 months ago

TKIP is correct
upvoted 10 times

  **Bhrino** Most Recent 3 months, 3 weeks ago

Selected Answer: B



WPA 2 and 3 use AES counter...
upvoted 3 times

  **Ciscoman021** 5 months, 3 weeks ago

Selected Answer: B

WPA1 (Wi-Fi Protected Access 1) uses TKIP (Temporal Key Integrity Protocol) encryption for data protection. TKIP is an encryption protocol that was designed to provide stronger security than the previous WEP (Wired Equivalent Privacy) encryption standard, which was known to have vulnerabilities. TKIP uses a combination of encryption techniques, including a per-packet key mixing function, to provide data confidentiality and integrity. However, TKIP is now considered insecure and has been replaced by AES (Advanced Encryption Standard) in modern Wi-Fi security protocols such as WPA2 and WPA3.

upvoted 4 times



  **DINVIS** 6 months, 2 weeks ago

TKIP is the right answer!
upvoted 2 times

  **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: B

The correct answer it's B
upvoted 2 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: B

TKIP indeed
upvoted 3 times

  **oatmealturkey** 7 months ago

Selected Answer: B

AES was not introduced until WPA2, it is not part of WPA1.
https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
upvoted 4 times


```
access-list 10 permit 10.0.0.0 0.0.0.255

interface Serial0

ip access-list 10 in
```

Refer to the exhibit. A network administrator must permit traffic from the 10.10.0.0/24 subnet to the WAN on interface Serial0. What is the effect of the configuration as the administrator applies the command?

- A. The router accepts all incoming traffic to Serial0 with the last octet of the source IP set to 0.
- B. The permit command fails and returns an error code.
- C. The router fails to apply the access list to the interface.
- D. The sourced traffic from IP range 10.0.0.0 - 10.0.0.255 is allowed on Serial0.

Correct Answer: B

  **oatmealturkey** Highly Voted 6 months, 4 weeks ago

Selected Answer: C

The permit command does not fail, it is syntactically correct even though the ACL would not work as intended because it would not allow traffic from the 10.10.0.0/24 subnet. The answer is C because ip access-list 10 in is not a valid command and is rejected. The correct command would be ip access-group 10 in.

upvoted 20 times

  **seapimp** Highly Voted 6 months, 2 weeks ago

Answer is B. ip access-list is not a valid command. ip access-group is required

upvoted 5 times

  **mutlumesut** Most Recent 1 month ago

Spoto says "D" is answer for this question, which one is true? :))))))

upvoted 1 times

  **mutlumesut** 1 month ago

Spoto says the answer is "D" for this question :))))))

upvoted 1 times

  **Shabeth** 2 months, 2 weeks ago

Selected Answer: C

C is correct



upvoted 1 times

  **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: C

The correct answer it's C

upvoted 1 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: C

Yeah i agree, 'C' is the correct answer.

upvoted 1 times

  **Jacques1982** 6 months, 3 weeks ago

Selected Answer: C

It would apply the access list but no traffic will be permitted as the applied IP is incorrect
upvoted 2 times

 **sdmejia01** 6 months, 3 weeks ago

Selected Answer: C

The correct answer is C. The router will fail to apply the ACL to the Serial interface because it doesn't use the right syntax. The right interface subcommand is: ip access-group 10 in. Also it would not work as intended because it includes the wrong subnet. Please fix answer.
upvoted 4 times

Question #975

Topic 1

DRAG DROP

-

Drag and drop the statements about AAA services from the left to the corresponding AAA services on the right. Not all options are used.

It grants access to network assets, such as FTP servers.	Authentication
It restricts the CLI commands that a user is able to perform.	
It performs user validation via TACACS+.	Authorization
It records the duration of each connection.	
It supports User Access Reporting.	
It verifies "who you are".	

Correct Answer:

It grants access to network assets, such as FTP servers.	Authentication It performs user validation via TACACS+. It verifies "who you are".
It restricts the CLI commands that a user is able to perform.	
It performs user validation via TACACS+.	Authorization It grants access to network assets, such as FTP servers. It restricts the CLI commands that a user is able to perform.
It records the duration of each connection.	
It supports User Access Reporting.	
It verifies "who you are".	

 **sdmejia01** **Highly Voted** 6 months, 3 weeks ago

Answers are correct
upvoted 10 times

 **VictorCisco** **Most Recent** 5 months, 2 weeks ago

FTP server just need authentication (or free access). Is there authorization ?
upvoted 1 times

A network engineer must configure an access list on a new Cisco IOS router. The access list must deny HTTP traffic to network 10.125.128.32/27 from the 192.168.240.0/20 network, but it must allow the 192.168.240.0/20 network to reach the rest of the 10.0.0.0/8 network. Which configuration must the engineer apply?

- A. ip access-list extended deny_outbound
10 permit ip 192.168.240.0 255.255.240.0 10.0.0.0 255.0.0.0
20 deny tcp 192.168.240.0 255.255.240.0 10.125.128.32 255.255.255.224 eq 443
30 permit ip any any
- B. ip access-list extended deny_outbound
10 deny tcp 192.168.240.0 0.0.15.255 10.125.128.32 0.0.0.31 eq 80
20 permit ip 192.168.240.0 0.0.15.255 10.0.0.0 0.255.255.255
30 deny ip any any log
- C. ip access-list extended deny_outbound
10 deny tcp 10.125.128.32 255.255.255.224 192.168.240.0 255.255.240.0 eq 443
20 deny tcp 192.168.240.0 255.255.240.0 10.125.128.32 255.255.255.224 eq 443
30 permit ip 192.168.240.0 255.255.240.0 10.0.0.0 255.0.0.0
- D. ip access-list extended deny_outbound
10 deny tcp 192.168.240.0 0.0.15.255 any eq 80
20 deny tcp 192.168.240.0 0.0.15.255 10.125.128.32 0.0.0.31 eq 80
30 permit ip 192.168.240.0 0.0.15.255 10.0.0.0 0.255.255.255

Correct Answer: B

 **sdmejia01** Highly Voted 6 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 9 times

 **[Removed]** Most Recent 2 months, 1 week ago

Selected Answer: B

B.

ip access-list extended deny_outbound

10 deny tcp 192.168.240.0 0.0.15.255 10.125.128.32 0.0.0.31 eq 80

20 permit ip 192.168.240.0 0.0.15.255 10.0.0.0 0.255.255.255

30 deny ip any any log

upvoted 1 times

What is the definition of backdoor malware?

- A. malicious code that is installed onto a computer to allow access by an unauthorized user
- B. malicious program that is used to launch other malicious programs
- C. malicious code that infects a user machine and then uses that machine to send spam
- D. malicious code with the main purpose of downloading other malicious code

Correct Answer: C

  **oatmealturkey** Highly Voted 7 months ago

Selected Answer: A

Wrong, the correct answer is A.
[https://en.wikipedia.org/wiki/Backdoor_\(computing\)](https://en.wikipedia.org/wiki/Backdoor_(computing))
upvoted 13 times

  **Vikramaditya_J** Most Recent 4 months, 3 weeks ago

Selected Answer: A

Backdoor malware is a type of Trojan that allows attackers to gain remote access to a system by negating normal authentication procedures. Backdoor attacks let attackers gain control of system resources, perform network reconnaissance, and install different types of malwares. Backdoors can be installed in both software and hardware. There have been many high-profile backdoor attacks in recent years, including the SolarWinds attack in 2020, which was suspected to be carried out by nation-state actors. Backdoor attacks can be prevented by using strong passwords, keeping software up to date, and using security software. BTW, any type of malware can potentially be used to send spam.
upvoted 4 times

  **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: A

It's A
upvoted 3 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: A

Indeed, "A" is the correct answer.
upvoted 3 times

What does WPA3 provide in wireless networking?

- A. backward compatibility with WPA and WPA2
- B. safeguards against brute force attacks with SAE
- C. increased security and requirement of a complex configuration
- D. optional Protected Management Frame negotiation

Correct Answer: B

  **sdmejia01** Highly Voted 6 months, 3 weeks ago

Selected Answer: B

Correct answer is B. <https://www.swascan.com/wi-fi-security/>
upvoted 6 times

Which global command encrypts all passwords in the running configuration?

- A. service password-encryption
- B. enable password-encryption
- C. enable secret
- D. password-encrypt

Correct Answer: A

 **sdmejia01** Highly Voted 6 months, 3 weeks ago

Selected Answer: A

Correct answer is A. <https://community.cisco.com/t5/other-network-architecture-subjects/service-password-encryption-command/td-p/269324>
upvoted 6 times

```

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#ip domain-name CC-Net.com
R1(config)#enable secret Passfornewuser
R1(config)#line vty 0 15
R1(config-line)#transport input ssh
R1(config-line)#login local

```

Refer to the exhibit. A network administrator is configuring a router for user access via SSH. The service-password encryption command has been issued. The configuration must meet these requirements:

- Create the username as CCUser.
- Create the password as NA!2\$cc.
- Encrypt the user password.

What must be configured to meet the requirements?

- A. username CCUser privilege 10 password NA!2\$cc
- B. username CCUser privilege 15 password NA!2\$cc
enable secret 0 NA!2\$cc
- C. username CCUser secret NA!2Sce
- D. username CCUser password NA!2\$cc
enable password level 5 NA!2\$cc

Correct Answer: C

 **dropspablo** 2 months, 1 week ago

A request was made to encrypt the password, but both the "#password" and "#secret" commands fulfill this request, since the "#service password-encryption" command is enabled. The difference is that other commands include privilege (authorization) levels, and this was not requested. Letter C is correct, as it meets all requirements, without exaggeration. The encryption service in this case is just to confuse.

upvoted 1 times

 **JJY888** 4 months ago

Selected Answer: C

To create the username as CCUser, create the password as NA!2\$cc, and encrypt the user password, option C is the correct configuration.

Option A only creates the user and sets a plain-text password. Option B sets a privileged level password for enable mode, but it does not create the user or encrypt the password. Option D creates the user and sets a plain-text password but does not encrypt the password. Option C creates the user, sets an encrypted password, and meets all the specified requirements.

upvoted 3 times

 **The_dark_knight** 3 months, 1 week ago

But there is the service-password encryption command is issued so why we need secret if in case need more security but they didn't say about that

upvoted 1 times

 **itemba36** 4 months, 3 weeks ago

C is wrong, because NA!2Sce is not the right password.


I think A is right. Although this user password NA!2\$cc is not encrypted in Answer A, the service-password encryption command will encrypt it.

upvoted 4 times

 **Shabeth** 2 months, 2 weeks ago

I agree, ill go with A too

upvoted 1 times

 **rogi2023** 5 months, 2 weeks ago

Selected Answer: A

Another tricky question with bad wording - IMHO

First lets agree that C is not a typo and therefore it's wrong answer.

trying to find MIN/MAX solution I go with A. - What do you think ?

I hope not to see such Q on exam.

upvoted 1 times

  **[Removed]** 2 months, 2 weeks ago

I think it's a typo

upvoted 1 times

  **sdmejia01** 6 months, 3 weeks ago

Selected Answer: C

C is correct. The requirements don't ask for privilege access and the secret password is already set.

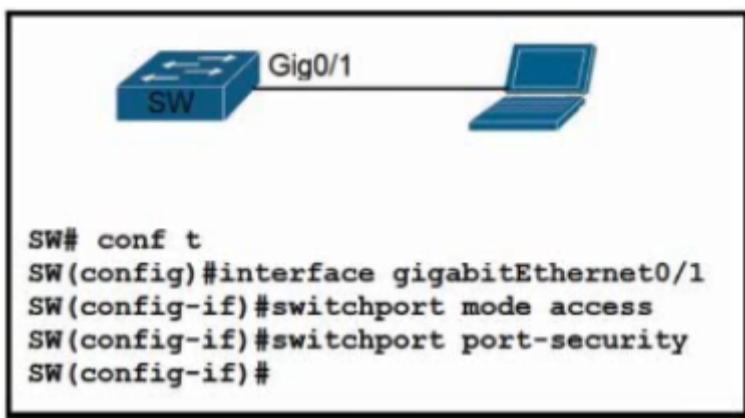
upvoted 3 times

  **mageknight** 6 months, 3 weeks ago

Create the password as NA!2\$cc.

it is a different password in answer C

upvoted 1 times



Refer to the exhibit. A network engineer started to configure port security on a new switch. These requirements must be met:

- MAC addresses must be learned dynamically.
- Log messages must be generated without disabling the interface when unwanted traffic is seen.

Which two commands must be configured to complete this task? (Choose two.)

- A. SW(config-if)#switchport port-security violation restrict
- B. SW(config-if)#switchport port-security mac-address 0010.7B84.45E6
- C. SW(config-if)#switchport port-security maximum 2
- D. SW(config-if)#switchport port-security violation shutdown
- E. SW(config-if)#switchport port-security mac-address sticky

Correct Answer: BC

Yaqub009 Highly Voted 6 months, 3 weeks ago

Selected Answer: AE

1. MAC addresses must be learned dynamically :
 E. SW(config-if)#switchport port-security mac-address sticky because,
 --sticky command automatically learns the MAC address of the computer connected to SW.
 2. Log messages must be generated without disabling the interface when unwanted traffic is seen:
 --A. SW(config-if)#switchport port-security violation restrict.
 So, correct answers are A and E.

B is incorrect, because this MAC is not dynamically learned
 C is incorrect, because they don't say that there can have max 2 MAC addresses
 D is incorrect, because Shutdown mode is disable the interface.
 upvoted 27 times

rogi2023 5 months, 2 weeks ago

This is correct inclusive detailed explanation :-) AE
 upvoted 7 times

bisiyemo1 Highly Voted 6 months, 1 week ago

Selected Answer: AE

A and E
 upvoted 5 times

learntstuff Most Recent 1 month ago

Selected Answer: AE

every time I do this question I add the 2 MAC addresses in there and it does not state it.
 upvoted 1 times

[Removed] 2 months, 2 weeks ago

Selected Answer: AE

A and E are correct
 upvoted 1 times

Shabeth 2 months, 2 weeks ago

Selected Answer: AE

A and E

upvoted 2 times

  **Dunedrifter** 2 months, 3 weeks ago

Selected Answer: AE

AE correct



upvoted 2 times

  **Zepar** 3 months, 3 weeks ago

Selected Answer: AE

A and E is the Correct Answer



upvoted 2 times

  **JJY888** 6 months, 1 week ago

Selected Answer: AE

Sticky is dynamically learned Mac and restrict means logged.

upvoted 3 times

  **Dutch012** 6 months, 2 weeks ago

Selected Answer: AC

Mac address(es), it means the maximum should be 2 or more, by default maximum is 1



upvoted 3 times

  **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: AE

The correct answers it's AE

upvoted 5 times

  **Rynurr** 6 months, 3 weeks ago

Selected Answer: AE

Definitely "AE"

upvoted 3 times

  **Jacques1982** 6 months, 3 weeks ago

Selected Answer: AE

A and E for sure

upvoted 3 times

  **ukguy** 6 months, 3 weeks ago

AE are correct answers

upvoted 4 times

  **gewe** 6 months, 4 weeks ago

MAC addresses - which make option C correct. and yes restrict won't shut down port, but will generate syslog msg



upvoted 3 times

  **j1mlawton** 7 months ago

Selected Answer: AC

I think A,C for this one. Restrict wont shut down the port and will generate counters

upvoted 5 times

  **ac89l** 4 months, 1 week ago

Who the hell asked for maximum 2 ?

should be AE

upvoted 2 times

Which type of security program is violated when a group of employees enters a building using the ID badge of only one person?

- A. intrusion detection
- B. network authorization
- C. physical access control
- D. user awareness

Correct Answer: C

 **Cynthia2023** 1 month ago

Selected Answer: C

Given Answer is correct.
upvoted 1 times

 **Yannik123** 1 month, 2 weeks ago

Selected Answer: C

Given Answer is correct.
upvoted 1 times

What are two protocols within the IPsec suite? (Choose two.)

- A. 3DES
- B. AES
- C. ESP
- D. TLS
- E. AH

Correct Answer: CE

 **mageknight** **Highly Voted**  6 months, 3 weeks ago

IPsec (Internet Protocol Security) is a suite of protocols used for securing internet protocol (IP) communications. The two protocols within the IPsec suite are:

Authentication Header (AH): AH provides data authentication and integrity protection for IP packets, but does not provide encryption. AH calculates a hash value over the IP packet and some additional data, and places the result in a new header that is added to the packet.

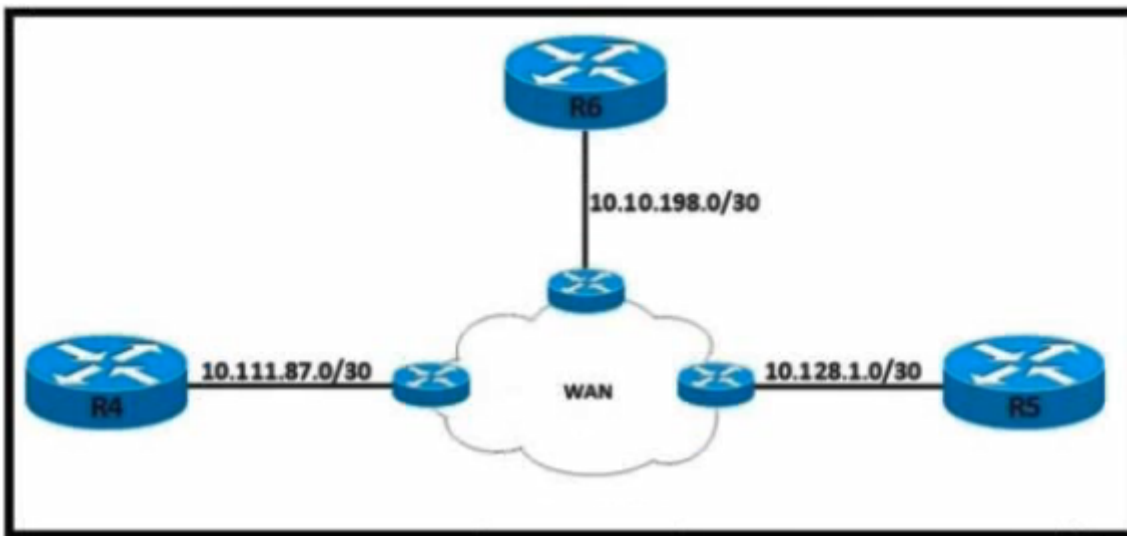
Encapsulating Security Payload (ESP): ESP provides both encryption and data authentication for IP packets. ESP encrypts the original IP packet and places it inside a new packet, along with a new ESP header that provides data authentication and integrity protection.

Both AH and ESP protocols can be used alone or in combination to provide secure communication between two network devices. AH and ESP are often used in conjunction with the Internet Key Exchange (IKE) protocol, which is used to negotiate and establish security associations (SAs) between devices.

upvoted 8 times

 **sdmejia01** **Most Recent**  6 months, 3 weeks ago

Answers are correct. <https://www.ibm.com/docs/en/i/7.1?topic=concepts-ip-security-protocols>
upvoted 4 times



Refer to the exhibit. Local access for R4 must be established and these requirements must be met:

- Only Telnet access is allowed.
- The enable password must be stored securely.
- The enable password must be applied in plain text.
- Full access to R4 must be permitted upon successful login.

Which configuration script meets the requirements?

```
A. !
conf t
!
username test1 password testpass1
enable secret level 15 0 Test123
!
line vty 0 15
login local
transport input telnet
```


```
B. !
config t
!
username test1 password testpass1
enable password level 15 0 Test123
!
line vty 0 15
login local
transport input all
```

```
C. !
config t
!
username test1 password testpass1
enable password level 1 7 Test123
!
line vty 0 15
accounting exec default
transport input all
```

```
D. !
config t
!
username test1 password testpass1
enable secret level 1 0 Test123
!
line vty 0 15
```

login authentication
password Test123
transport input telnet

Correct Answer: A

  **mda2h** 1 month, 1 week ago

Selected Answer: A


Possible solutions are A and D.
D has login authentication => tells switch to use aaa to authenticate => wrong cause we cant local access
Thus A is correct
upvoted 1 times

  **Friday_Night** 3 months, 2 weeks ago



how is enable secret command be plain text?
upvoted 2 times

  **XuniLrve4** 2 months, 2 weeks ago

They are asking when configure it enters as plain text and is encrypted when shown in running-config
upvoted 1 times

  **perri88** 3 months ago

only cisco knows
upvoted 4 times

  **4aynick** 3 months, 3 weeks ago

correct
upvoted 2 times

  **ac89l** 4 months ago

Can anyone validate this please?
upvoted 1 times

  **XuniLrve4** 2 months, 2 weeks ago

There are only two options firstly that only permit telnet alone A,D, and the only other option is "D" and it has plain text password w no encryption. Hope this helps.
upvoted 2 times

What is a characteristic of RSA?

- A. It uses preshared keys for encryption.
- B. It is an asymmetric encryption algorithm.
- C. It is a symmetric decryption algorithm.
- D. It requires both sides to have identical keys for encryption.

Correct Answer: D

 **NetworkGeek00** 1 month, 1 week ago


Selected Answer: B

B is correct
upvoted 1 times

 **sam225555** 2 months, 1 week ago

Selected Answer: B

The correct answer it's B
upvoted 1 times

 **Ciscoman021** 5 months, 3 weeks ago

Selected Answer: B


RSA (Rivest-Shamir-Adleman) is an asymmetric encryption algorithm, which is a type of public-key cryptography. In asymmetric encryption, a public key is used for encryption, and a private key is used for decryption. The two keys are mathematically related, but it is computationally infeasible to derive the private key from the public key.

Option B, "It is an asymmetric encryption algorithm", is therefore the correct answer.
upvoted 3 times

 **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: B

The correct answer it's B
upvoted 2 times

 **Rynurr** 6 months, 3 weeks ago

Selected Answer: B

Yeah "B" is the correct answer
upvoted 1 times

 **mageknight** 6 months, 3 weeks ago

Asymmetric Encryption: RSA is an asymmetric encryption algorithm, which means that it uses a different key for encryption and decryption.
upvoted 3 times

 **oatmealturkey** 7 months ago

Selected Answer: B

Answer is B - RSA is an asymmetric encryption algorithm.
<https://study-ccna.com/cisco-cryptography-symmetric-vs-asymmetric-encryption/>
upvoted 4 times

What are two differences between WPA2 and WPA3 wireless security? (Choose two.)

- A. WPA2 uses 192-bit key encryption, and WPA3 requires 256-bit key encryption.
- B. WPA3 uses AES for stronger protection than WPA2, which uses SAE.
- C. WPA2 uses 128-bit key encryption, and WPA3 supports 128-bit and 192-bit key encryption.
- D. WPA3 uses SAE for stronger protection than WPA2, which uses AES.
- E. WPA3 uses AES for stronger protection than WPA2, which uses TKIP.

Correct Answer: CD

  **mageknight** Highly Voted 6 months, 3 weeks ago

WPA2 uses 128-bit key encryption with AES, while WPA3 supports 128-bit and 192-bit key encryption with AES and the new SAE protocol for key establishment.

upvoted 8 times

  **Stevens0103** Most Recent 1 month, 1 week ago

Selected Answer: CD

<https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/wpa3-dep-guide-og.html#:~:text=WPA3%20is%20the%20third%20and,purpose%20of%20standardizing%20wireless%20security.>

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/67134-wpa2-config.html>

upvoted 1 times

  **LeonardoMeCabrio** 2 months, 2 weeks ago

Selected Answer: C

CD CD CD



upvoted 1 times

  **Zepar** 3 months, 3 weeks ago

Selected Answer: CD

C and D is correct

upvoted 1 times

  **Leethy** 5 months, 1 week ago

Selected Answer: AD

A. WPA2 uses 192-bit key encryption, and WPA3 requires 256-bit key encryption.

D. WPA3 uses SAE for stronger protection than WPA2, which uses AES.



upvoted 1 times

  **ac89l** 4 months, 1 week ago

CD

WPA3 supports 128 and 192



upvoted 1 times

  **Rydaz** 4 months, 1 week ago

WPA2 uses 128

correct answer is C and D

upvoted 2 times

  **Rydaz** 4 months, 1 week ago

guaranty with a warranty on top

upvoted 1 times

What is an enhancement implemented in WPA3?

- A. applies 802.1x authentication and AES-128 encryption
- B. employs PKI and RADIUS to identify access points
- C. uses TKIP and per-packet keying
- D. defends against deauthentication and disassociation attacks

Correct Answer: D

 **Goena** 6 months, 2 weeks ago

Selected Answer: D

D is correct:

Additionally, WPA3 personal and enterprise connections requires PMF (Protected Management Frame) negotiation mandatorily. PMF provides an additional layer of protection from de-authentication and disassociation attacks.

upvoted 3 times

Which action must be taken when password protection is implemented?

- A. Use less than eight characters in length when passwords are complex.
- B. Include special characters and make passwords as long as allowed.
- C. Share passwords with senior IT management to ensure proper oversight.
- D. Store passwords as contacts on a mobile device with single-factor authentication.

Correct Answer: B

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.

It assigns per-user attributes.	Authentication
It reaches the CLI commands that a user is able to perform.	
It permits and derives login attempts.	Authorization
It records the amount of network resources consumed by the user.	
It supports local, PPP, RADIUS, and TACACS+ options.	
It tracks the services that a user is using.	

Correct Answer:

It assigns per-user attributes.	Authentication
It reaches the CLI commands that a user is able to perform.	
It permits and derives login attempts.	Authorization
It records the amount of network resources consumed by the user.	
It supports local, PPP, RADIUS, and TACACS+ options.	
It tracks the services that a user is using.	

ac89l Highly Voted 4 months ago

IMO , Answers is correct
upvoted 7 times

studying_1 3 months, 2 weeks ago

I agree with you
upvoted 2 times

[Removed] 2 months, 2 weeks ago

Me too
upvoted 1 times

ananinamia 2 weeks, 3 days ago

mee to
upvoted 1 times

An engineer must configure R1 for a new user account. The account must meet these requirements:

- It must be configured in the local database.
- The username is engineer2.
- It must use the strongest password configurable.

Which command must the engineer configure on the router?

- A. R1(config)# username engineer2 privilege 1 password 7 test2021
- B. R1(config)# username engineer2 secret 4 \$1\$b1Ju\$kZbBS1Pyh4QzwXyZ
- C. R1(config)# username engineer2 algorithm-type scrypt secret test2021
- D. R1(config)# username engineer2 secret 5 password \$1\$b1Ju\$kZbBS1Pyh4QzwXyZ

Correct Answer: C

 **Yinx** 3 weeks ago

I tried all commands on GNS3 Cisco C3725 router, all are wrong.
upvoted 1 times

 **mcontento** 1 month, 1 week ago

A.
CAT9200(config)#username engineer2 privilege 1 password 7 test2021
Invalid encrypted password: test2021

B.
CAT9200(config)#username engineer2 secret 4 \$1\$b1Ju\$kZbBS1Pyh4QzwXyZ
ERROR: Type 4 passwords have been deprecated.
Migrate to a supported password type

C.
CAT9200(config)#username engineer2 algorithm-type scrypt secret test2021
CAT9200(config)#do show run | inc engineer2
username engineer2 secret 9 \$9\$2FTH4wYx6hzf1X\$1WVSI21bbXZ7JIP5v42YDvImoHd6DTHW5pcm4J0ly8A
CAT9200(config)#


D.
CAT9200(config)#username engineer2 secret 5 password \$1\$b1Ju\$kZbBS1Pyh4QzwXyZ
% Ambiguous command: "username engineer2 secret 5 password \$1\$b1Ju\$kZbBS1Pyh4QzwXyZ"
CAT9200(config)#

The only option that runs is option C. I configured the user and pass, and when I did "show run", the password was encrypted.
upvoted 2 times

 **Eallam** 2 months, 1 week ago

Selected Answer: C

<https://www.linkedin.com/pulse/enable-secret-password-algorithms-md5-sha256-scrypt-michael-akintola>
upvoted 1 times

 **Toto86** 2 months, 1 week ago

Selected Answer: C

C is the strongest password, type 9 and SHA-256 algorithm.

CCNA 200-301 Official Cert Guide, Volume 2 page 93
<https://community.cisco.com/t5/networking-knowledge-base/understanding-the-differences-between-the-cisco-password-secret/ta-p/3163238>
upvoted 3 times

 **dropspablo** 2 months, 1 week ago

Selected Answer: C

As of bug CSCue95644 (which is a Cisco issue identifier), keyword 4 for specifying a SHA-256 encrypted secret string has been deprecated. This indicates that the use of that particular type of encryption algorithm is no longer recommended or supported by Cisco.

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/d1/sec-d1-cr-book/sec-cr-e1.html#:~:text=4%20keyword%20is-,deprecated,->

The syntax of the letter C is correct, only the password "test2021" would be weak, but as shown is just a "test" password, it will not be this password that the engineer will hand over to the user, without a crisis. However, setting the password with type 9 (SCRYPT) is the strongest that can be set, better than 5 and 8. The old type 4 is no longer recommended due to its fragility (bug CSCue95644).

upvoted 2 times

  **Dunedrifter** 2 months, 3 weeks ago

Selected Answer: B

B. R1(config)# username engineer2 secret 4 \$1\$b1Ju\$kZbBS1Pyh4QzwXyZ

This command creates a local user account named "engineer2" and sets the password as the given encrypted string "\$1\$b1Ju\$kZbBS1Pyh4QzwXyZ". The "secret" keyword is used to specify the encrypted password. The "4" indicates the encryption type, which in this case appears to be MD5.

Option A uses the "password" keyword, which indicates a simple, unencrypted password. Option C uses the "algorithm-type scrypt" which is not necessary for this scenario, and Option D is incorrect because it uses the wrong keyword ("password") instead of "secret" for specifying an encrypted password.

upvoted 1 times

  **perri88** 3 months ago

Selected Answer: B

The command starts with the "username" keyword, followed by the desired username, which in this case is "engineer". The "secret" keyword is used to specify the password. The number "5" following the secret keyword indicates the password encryption type, which is SHA256-based salted password hashing algorithm (scrypt) in this case. The password itself is specified after the encryption type.

Option B is the correct command because it specifies the use of the strongest password encryption method (scrypt) and provides a secure password. The provided password, "S1\$b1Ju\$kZbBS1Pyh4QzwXyZ", is a strong password that meets the requirement for a strong password.

upvoted 2 times

  **LeonardoMeCabrio** 3 months, 1 week ago

Selected Answer: B

B is correct, C uses a very common password and cannot be correct!!

upvoted 2 times

  **Zepar** 3 months, 3 weeks ago

Selected Answer: B

B seems to meet all those conditions.

upvoted 3 times


  **4aynick** 3 months, 3 weeks ago

if strongest password - answer D

if strongest store password - C

I dont understand what Cisco want

upvoted 1 times

  **Goena** 6 months, 2 weeks ago

Command: username engineer2 algorithm-type scrypt secret test2021 is not know in PT.

upvoted 1 times

  **mageknight** 6 months, 3 weeks ago

algorithm-type scrypt: This specifies the algorithm used for password hashing, which in this case is "scrypt". "scrypt" is a password-based key derivation function that is designed to be highly resistant to brute force attacks.

upvoted 3 times

Which two VPN technologies are recommended by Cisco for multiple branch offices and large-scale deployments? (Choose two.)

- A. GETVPN
- B. DMVPN
- C. site-to-site VPN
- D. clientless VPN
- E. IPsec remote access

Correct Answer: AB

  **mageknight** Highly Voted 6 months, 3 weeks ago

DMVPN and FlexVPN are more commonly recommended by Cisco for large-scale VPN deployments, GETVPN can be a viable alternative in certain situations where a tunnel-less VPN solution is desirable. Ultimately, the choice between these VPN technologies will depend on specific requirements and factors, such as the underlying network topology, transport technologies, and security policies
upvoted 5 times

  **perri88** Most Recent 3 months ago

Selected Answer: AB

A. GETVPN (Group Encrypted Transport VPN): GETVPN is a Cisco VPN technology that provides secure and scalable VPN connectivity for multiple branch offices and large-scale deployments. It uses a group-based encryption mechanism to encrypt traffic between sites, allowing for efficient and scalable encryption across the network. GETVPN is particularly suitable for deployments with high bandwidth requirements and complex routing environments.

B. DMVPN (Dynamic Multipoint VPN): DMVPN is another Cisco VPN technology designed for scalable and dynamic VPN deployments. It allows for the creation of secure overlay networks over public or private WAN connections. DMVPN provides efficient and scalable connectivity between multiple branch offices by using a combination of IPsec, GRE (Generic Routing Encapsulation), and NHRP (Next Hop Resolution Protocol). It simplifies the configuration and management of VPN connections, making it well-suited for large-scale deployments.
upvoted 1 times

  **JJY888** 4 months ago

Selected Answer: AB

Here we go again. Cisco will give you 3 correct answers and ask for the best 2 out of the 3. Cisco is not really concerned if you can implement or repair their technology only that you fail the test the first, maybe more, times around.

I think AB is correct. C is technically correct too.

https://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/enterprise-class-teleworker-ect-solution/prod_brochure0900aecd80582078.pdf

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/enterprise-class-teleworker-ect-solution/prod_brochure0900aecd80582078.pdf
upvoted 4 times

  **[Removed]** 2 months, 2 weeks ago

Exactly, they want you to take the test several times so they make money! If i fail at the first attempt, i'll never take it again though
upvoted 1 times

  **JJY888** 6 months, 1 week ago

Never heard of these SMH.
upvoted 3 times

DRAG DROP

Drag and drop the statements about AAA services from the left onto the corresponding AAA services on the right. Not all options are used.

It grants access to network assets, such as FTP servers.	Accounting
It limits the services available to a user.	
It performs user validation via TACACS+.	
It records the duration of each connection.	Authorization
It supports User Access Reporting.	
It verifies "who you are".	

Correct Answer:

It grants access to network assets, such as FTP servers.	Accounting
It limits the services available to a user.	It records the duration of each connection.
It performs user validation via TACACS+.	It supports User Access Reporting.
It records the duration of each connection.	Authorization
It supports User Access Reporting.	It performs user validation via TACACS+.
It verifies "who you are".	It verifies "who you are".

sdmejia01 Highly Voted 6 months, 3 weeks ago

The answer is wrong. It should be...
 Accounting: it records the duration of each connection and it supports user access reporting.
 Authorization: it limits the services available to a user and it grants access to network assets, such as FTP Servers.
 upvoted 28 times

Shabeth 2 months, 2 weeks ago

this is correct
 upvoted 1 times

RidzV Highly Voted 6 months, 1 week ago

Given answers for authorisation are actually for authentication.
 And the two skipped options will be correct for authorisation.
 upvoted 8 times

NetworkGeek00 Most Recent 1 month, 1 week ago

authorization answers are wrong. it should be
 limits services
 grant access
 upvoted 1 times

  **WilsonCeck** 2 months, 1 week ago

I think correct answers are:

ACCOUNTING: record duration of each connection / supports user access reporting

AUTHORIZATION: limits the services available to use / grants access to network assets, such as FTP Sservers

upvoted 3 times

  **kat1969** 4 weeks ago

They definitely got the answers coded wrong!Authorization is what grants access or limits services available to use.

upvoted 1 times

Question #993

Topic 1

What is a characteristic of RSA?

- A. It uses preshared keys for encryption.
- B. It is a public-key cryptosystem.
- C. It is a private-key encryption algorithm.
- D. It requires both sides to have identical keys.

Correct Answer: B

  **mageknight** Highly Voted  6 months, 3 weeks ago

RSA is a public-key cryptosystem. This means that it uses a pair of keys, one of which is kept private and the other of which is made public. The public key can be distributed to anyone who wants to send encrypted messages to the owner of the private key, while the private key is kept secret and is used by the owner to decrypt messages.

upvoted 10 times

Question #994

Topic 1

What is used as a solution for protecting an individual network endpoint from attack?

- A. antivirus software
- B. wireless controller
- C. router
- D. Cisco DNA Center

Correct Answer: A

Which security method is used to prevent man-in-the-middle attacks?

- A. authentication
- B. anti-replay
- C. authorization
- D. accounting

Correct Answer: B

  **mageknight** Highly Voted 6 months, 3 weeks ago

Anti-replay is a security method that is used to prevent man-in-the-middle attacks by ensuring that network packets are received and processed only once. This is typically accomplished by adding a unique identifier, called a sequence number or nonce, to each packet. The recipient of the packet keeps track of the sequence numbers that it has received and processes only packets that have not been received before. If a packet with a duplicate sequence number is received, it is discarded.

upvoted 6 times

  **purenuker** 5 months ago

But isn't this just how TCP functions in "normal way" - with seq and ack numbers ?

upvoted 1 times

  **lolungos** 3 months, 1 week ago

With TCP as a man in the middle you can request re-transmission

upvoted 1 times

  **Philipli308** Most Recent 1 month, 1 week ago

Selected Answer: A

Man-in-the-middle attack should be the person without authentication, they try to collect all the packet of network traffic by the software sniffer and reached the goal.

upvoted 1 times

  **Shabeth** 2 months, 2 weeks ago

Selected Answer: A

A. Authentication- MITM attacks can be prevented or detected by two means: authentication and tamper detection.

upvoted 1 times



  **perri88** 3 months ago

Selected Answer: A

Authentication is the security method used to prevent man-in-the-middle attacks. Man-in-the-middle attacks occur when an attacker intercepts and alters communication between two parties, without their knowledge. By authenticating the identities of the communicating parties, it becomes more difficult for an attacker to impersonate one of them and insert themselves into the communication.

Authentication methods can include passwords, digital certificates, biometric authentication, two-factor authentication (2FA), and other mechanisms that verify the identity of the communicating parties. By ensuring that the parties involved are who they claim to be, authentication helps protect against man-in-the-middle attacks and helps establish a secure and trusted communication channel.

upvoted 2 times

  **Leethy** 5 months, 1 week ago

Selected Answer: A

Option B: Anti-replay is a security method used to prevent an attacker from intercepting and replaying valid data, but it is not specifically used to prevent man-in-the-middle (MITM) attacks.

Anti-replay works by using sequence numbers or timestamps to ensure that each piece of data is unique and has not been intercepted and replayed by an attacker. While this can help prevent certain types of attacks, it is not a complete solution for preventing MITM attacks. Authentication, on the other hand, is specifically designed to prevent MITM attacks by verifying the identity of each party in a communication.

upvoted 4 times

Which cipher is supported for wireless encryption only with the WPA2 standard?

- A. RC4
- B. AES
- C. SHA
- D. AES256

Correct Answer: *B*

  **mda2h** 1 month, 1 week ago

Dafuq Cisco WPA3 standard uses AES as well ...
upvoted 1 times

```

CPE# show ip access-list Services
Extended IP access list Services
  10 permit tcp 10.0.0.0 0.255.255.255 any eq www
  20 permit tcp 10.0.0.0 0.255.255.255 any eq 443
  30 permit udp 10.0.0.0 0.255.255.255 host
198.51.100.11 eq domain
  40 deny ip any any log

```

Refer to the exhibit. This ACL is configured to allow client access only to HTTP, HTTPS, and DNS services via UDP. The new administrator wants to add TCP access to the ONS service. Which configuration updates the ACL efficiently?

- A. no ip access-list extended Services
ip access-list extended Services
30 permit tcp 10.0.0.0 0.255.255.255 host 198.51.100.11 eq domain
- B. ip access-list extended Services
35 permit tcp 10.0.0.0 0.255.255.255 host 198.51.100.11 eq domain
- C. ip access-list extended Services
permit tcp 10.0.0.0 0.255.255.255 host 198.51.100.11 eq domain
- D. no ip access-list extended Services
ip access-list extended Services
permit udp 10.0.0.0 0.255.255.255 any eq 53
permit tcp 10.0.0.0 0.255.255.255 host 198.51.100.11 eq domain deny ip any any log

Correct Answer: D

 **gewe** Highly Voted 6 months, 4 weeks ago

its said add so option B would be better
upvoted 10 times

 **Brocolee** 2 months ago

Just curious, It said "by gewe" which mean you are the contributor of this questions right? So who gave the answer above? you or admin? I find it strange since I saw few questions listed that you are the contributor only to find that you give different answer in the comment... I mean, I don't blame you if you change your answer after further research.
upvoted 1 times

 **oatmealturkey** 6 months, 3 weeks ago

And is most efficient
upvoted 3 times

 **[Removed]** Most Recent 2 months, 1 week ago

What is the ONS service??
upvoted 1 times

 **Shri_Fcb10** 1 month, 3 weeks ago

Its DNS, typo error. God knows when they will fix it
upvoted 1 times

 **Simon_1103** 4 months, 3 weeks ago

Selected Answer: B

Option A will delete the ACL completely and create a new one with only one entry, which is not efficient.

Option C is missing the line number and will insert the new entry at the beginning of the list, which may affect the order of other rules.

Option D allows access to both UDP and TCP DNS services and adds an unnecessary entry at the end that denies all other IP traffic. This option is not efficient and may cause issues.

Option B adds a new entry to the existing ACL with the appropriate line number and rule syntax, allowing TCP access to the ONS service while keeping the existing rules for HTTP, HTTPS, and DNS services. This option is the most efficient and effective way to update the ACL.

upvoted 4 times

🗨️ **rx78_2** 5 months, 3 weeks ago

Selected Answer: B

B is the correct answer.
D would deny HTTP as well as HTTPS connection
upvoted 4 times

🗨️ **Stichy007** 6 months, 2 weeks ago

Selected Answer: B

Answer is B. They really did a horrible job with some of these questions.
upvoted 4 times

🗨️ **lucantonelli93** 6 months, 3 weeks ago

Selected Answer: B

For me it's B
upvoted 1 times

🗨️ **Rynurr** 6 months, 3 weeks ago

Selected Answer: B

Should be "B"
upvoted 1 times

Question #998

Topic 1

Which WPA mode uses PSK authentication?

- A. Local
- B. Personal
- C. Enterprise
- D. Client

Correct Answer: B

🗨️ **Ciscoman021** **Highly Voted** 👍 5 months, 3 weeks ago

Selected Answer: B

The WPA mode that uses PSK (Pre-Shared Key) authentication is the Personal mode.

WPA (Wi-Fi Protected Access) is a security protocol used in wireless networks to protect the communication between devices. WPA has two modes of operation: Personal mode and Enterprise mode.

Personal mode, also known as WPA-PSK (Pre-Shared Key), uses a shared secret key (PSK) to authenticate wireless clients and encrypt network traffic. The PSK is a passphrase or password that is shared between the access point and wireless clients.

Enterprise mode, also known as WPA-EAP (Extensible Authentication Protocol), uses a RADIUS (Remote Authentication Dial-In User Service) server to authenticate wireless clients. Enterprise mode provides stronger security than Personal mode, but it requires more setup and infrastructure.

In summary, WPA-Personal mode uses PSK authentication, while WPA-Enterprise mode uses RADIUS server authentication.

upvoted 7 times

🗨️ **Goena** **Most Recent** 🕒 6 months, 2 weeks ago

Selected Answer: B

WPA2-PSK is also known as WPA2 Personal.
upvoted 2 times

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. interface FastEthernet0/0

```
ip address 10.122.49.1 255.255.255.252
```

```
ip access-group 110 in
```

```
ip access-list extended 110
```

```
permit tcp 10.139.58.0 0.0.0.15 host 10.122.49.1 eq 22
```

B. interface FastEthernet0/0

```
ip address 10.122.49.1 255.255.255.240
```

```
access-group 120 in
```

```
ip access-list extended 120
```

```
permit tcp 10.139.58.0 255.255.255.248 any eq 22
```

C. interface FastEthernet0/0

```
ip address 10.122.49.1 255.255.255.252
```

```
ip access-group 105 in
```

```
ip access-list standard 105
```

```
permit tcp 10.139.58.0 0.0.0.7 eq 22 host 10.122.49.1
```

D. interface FastEthernet0/0

```
ip address 10.122.49.1 255.255.255.248
```

```
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
```

Correct Answer: A

 **IFBBPROSALCEDO** 1 month ago

I agree!

upvoted 1 times

 **Cynthia2023** 1 month, 4 weeks ago

Selected Answer: A

permit tcp 10.139.58.0 0.0.0.15 host 10.122.49.1 eq 22
the only correct wild mask.

upvoted 3 times

 **LeonardoMeCabrio** 2 months, 2 weeks ago

Selected Answer: A

A is correct.

upvoted 1 times

 **studying_1** 3 months, 2 weeks ago

Selected Answer: A

Answer is correct, look at the wild mask in the access list, only correct one is in A

upvoted 2 times

 **Bhrino** 3 months, 4 weeks ago

Selected Answer: B

This could be wrong But I believe be because /28 is 240 and ssh port number is 22

upvoted 1 times

 **studying_1** 3 months, 2 weeks ago

the interface's ip address has nothing to do with the given subnet, we should look at the access-list not the configuration in the interface, it's totally different

upvoted 1 times

  **studying_1** 3 months, 2 weeks ago

it can't be B, the wild mas in the access list is wrong

upvoted 1 times

  **studying_1** 3 months, 2 weeks ago

wild mask* sorry typo

upvoted 1 times

Question #1000

Topic 1

To improve corporate security, an organization is planning to implement badge authentication to limit access to the data center. Which element of a security program is being deployed?

- A. user awareness
- B. user training
- C. physical access control
- D. vulnerability verification

Correct Answer: C

  **AndreaGambera** 3 weeks, 2 days ago

Correct

upvoted 1 times

  **Dunedrifter** 2 months, 3 weeks ago

Selected Answer: C

Correct

upvoted 1 times

  **studying_1** 3 months, 2 weeks ago

Selected Answer: C

Answer is correct

upvoted 1 times

DRAG DROP

Drag and drop the characteristics of northbound APIs from the left onto any position on the right. Not all characteristics are used.

supports automation	1
communicates between the SDN controller and the application plane	2
communicates between the SDN controller and the data plane	3
supports data sharing between systems	4
supports network virtualization protocols	
supports REST-based requirements	
uses OpenFlow to interface between the data and control planes	

Correct Answer:

supports automation	supports automation
communicates between the SDN controller and the application plane	communicates between the SDN controller and the application plane
communicates between the SDN controller and the data plane	
supports data sharing between systems	supports data sharing between systems
supports network virtualization protocols	
supports REST-based requirements	supports REST-based requirements
uses OpenFlow to interface between the data and control planes	

sdmejia01 Highly Voted 6 months, 3 weeks ago
 Answers are correct!
 upvoted 18 times

ogame Highly Voted 2 months ago
 Answer:
 + supports automation
 + communicates between the SDN controller and the application plane
 + supports network virtualization protocols
 + supports REST-based requirements
 upvoted 6 times

Stevens0103 1 month, 1 week ago
<https://www.webwerks.in/blogs/southbound-vs-northbound-sdn-what-are-differences>

upvoted 1 times

 **Cynthia2023** Most Recent 1 month, 2 weeks ago

Southbound APIs: Focus on data sharing between the SDN controller and the network devices for configuration and control of the network infrastructure.

Northbound APIs: Focus on providing a standardized interface for applications and higher-level management systems to interact with the SDN controller.

upvoted 3 times

Question #1002

Topic 1

Which benefit does Cisco DNA Center provide over traditional campus management?

- A. Cisco DNA Center automates HTTPS for secure web access, and traditional campus management uses HTTP.
- B. Cisco DNA Center leverages SNMPv3 for encrypted management, and traditional campus management uses SNMPv2.
- C. Cisco DNA Center leverages APIs, and traditional campus management requires manual data gathering.
- D. Cisco DNA Center automates SSH access for encrypted entry, and SSH is absent from traditional campus management.

Correct Answer: C

 **[Removed]** 2 months, 1 week ago

Selected Answer: C

C. Cisco DNA Center leverages APIs, and traditional campus management requires manual data gathering.

upvoted 1 times

 **Ciscoman021** 5 months, 2 weeks ago

Selected Answer: C

Cisco DNA Center provides the benefit of leveraging APIs (Application Programming Interfaces) over traditional campus management which requires manual data gathering.

upvoted 3 times

 **Goena** 7 months ago

Selected Answer: C

Answer C is correct

upvoted 4 times