



- Expert Verified, Online, **Free**.



CERTIFICATION TEST

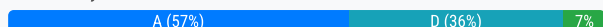
- CertificationTest.net - Cheap & Quality Resources With Best Support

On a branch office deployment, it has been noted that if the FlexConnect AP is in standalone mode and loses connection to the WLC, all clients are disconnected, and the SSID is no longer advertised. Considering that FlexConnect local switching is enabled, which setting is causing this behavior?

- A. ISE NAC is enabled
- B. 802.11r Fast Transition is enabled
- C. Client Exclusion is enabled
- D. FlexConnect Local Auth is disabled

Suggested Answer: D

Community vote distribution



kthekillerc Highly Voted 3 years, 8 months ago

The question stated the AP lost connection therefore all connected users would loose connectivity and have to reauthenticate. If Flexconnect Local Auth has been disabled this behavior would occur. The provided answer is correct.

upvoted 6 times

GnXxUbik Most Recent 1 month, 1 week ago

Selected Answer: D

Is this exam version 1.1 or 1.0?

upvoted 1 times

rrahim 4 months ago

Selected Answer: D

When a FlexConnect AP is in standalone mode (disconnected from the WLC), it can continue serving clients only if FlexConnect Local Authentication is enabled.

If Local Auth is disabled, the AP relies on the WLC for client authentication.

If the AP loses WLC connectivity, it cannot authenticate new clients or maintain existing client sessions, causing disconnections.

To fix this, enable FlexConnect Local Authentication under the WLAN configuration on the WLC.

upvoted 1 times

rrahim 4 months, 1 week ago

When FlexConnect Local Auth is disabled, the FlexConnect AP cannot authenticate clients locally if the connection to the Wireless LAN Controller (WLC) is lost. As a result, the AP stops advertising the SSID, and all clients are disconnected. Enabling FlexConnect Local Auth allows the AP to authenticate clients locally, ensuring that the SSID remains available and clients stay connected even when the WLC is unreachable.

upvoted 1 times

Nad_E 4 months, 1 week ago

Selected Answer: A

<https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/113606-byod-flexconnect-dg-000.html>

Note: RADIUS Network Admission Control (NAC) is not supported when the FlexConnect AP is in disconnected mode. Thus, if the FlexConnect AP is in standalone mode and loses connection to the WLC, all clients are disconnected, and the SSID is no longer advertised.

upvoted 1 times

Walid_Gaber 5 months, 3 weeks ago

Selected Answer: D

When FlexConnect Local Authentication is disabled, the AP relies on the WLC for client authentication. If the AP loses connection to the WLC, it cannot authenticate clients, and as a result:

The SSID is no longer advertised.

Clients are disconnected because the AP cannot perform authentication locally.

upvoted 1 times

🗄️ 👤 **Ocsicccnp** 9 months ago

Selected Answer: A

<https://www.cisco.com/c/en/us/support/docs/wireless/wireless-lan-controller-software/221229-configure-cwa-with-flexconnect-aps-on-a.html#:~:text=local%20switching%20mode.,Prerequisites,local%20authentication%20on%20the%20FlexAPs%20is%20not%20supported%20for%20this%20sOther%20Documents%20in>

upvoted 1 times

🗄️ 👤 **glaubersd** 1 year, 4 months ago

Hello,

I'm going to take my exam next month and I'm not sure about this question. Would it really be option A?

upvoted 1 times

🗄️ 👤 **qwertyEDCA** 1 year, 6 months ago

Selected Answer: A

Answer: A

Note: RADIUS Network Admission Control (NAC) is not supported when the FlexConnect AP is in disconnected mode. Thus, if the FlexConnect AP is in standalone mode and loses connection to the WLC, all clients are disconnected, and the SSID is no longer advertised.

source: most_ahdy - link:

<https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/113606-byod-flexconnect-dg-000.html>

upvoted 1 times

🗄️ 👤 **rrahim** 4 months, 1 week ago

The issue occurs because RADIUS NAC is not supported in standalone mode, and FlexConnect Local Auth is disabled. Enabling FlexConnect Local Auth ensures that the AP can authenticate clients locally, allowing the SSID to remain advertised and clients to stay connected even when the WLC is unreachable.

upvoted 1 times

🗄️ 👤 **[Removed]** 1 year, 5 months ago

Right straight from Cisco Site, A is 100% correct

upvoted 1 times

🗄️ 👤 **most_ahdy** 1 year, 10 months ago

<https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/113606-byod-flexconnect-dg-000.html>

I think it is A

upvoted 1 times

🗄️ 👤 **GoldLeader** 1 year, 11 months ago

Selected Answer: A

D is wrong because in standalone mode existing clients are not de-authenticated and the SSID remains up and locally switched. NAC enabled WLANs however REQUIRE a connection to the WLC. When the WLC connection is lost NAC enabled SSID must therefore become disabled and users deleted.

upvoted 3 times

🗄️ 👤 **anagy11** 1 year, 12 months ago

Selected Answer: D

I think D is the cause of the issue, as the WLC puts clients on the exclusion list because of multiple consecutive failed authentication attempts to the central authentication server, thus denying the client from the network.

upvoted 1 times

🗄️ 👤 **TJR72** 2 years, 2 months ago

Selected Answer: C

When FlexConnect local switching is enabled, the clients are associated directly with the FlexConnect AP. If the AP loses connection to the WLC, the clients should still be able to communicate with each other on the local network. However, if Client Exclusion is enabled and the AP cannot communicate with the WLC, it will remove all associated clients, and the SSID will no longer be advertised. This behavior can be changed by disabling Client Exclusion on the WLC.



upvoted 1 times

🗄️ 👤 **cvndani** 2 years, 9 months ago

Maybe B....

<https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/dam/en/us/td/docs/wireless/controller/technotes/80211r-ft/b-80211r-dg.html.xml>

upvoted 1 times

  **cvndani** 2 years, 9 months ago

Or D....assuming that the configuration are central switching and central authentication:

"authentication down, switch down—In this state, the WLAN disassociates existing clients and stops sending beacon and probe requests. This state is valid in both standalone mode and connected mode."

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/flexconnect.html

upvoted 2 times



  **Liselot** 2 years, 11 months ago

Selected Answer: A

MAC Filtering is not supported on FlexConnect access points in standalone mode. However, MAC Filtering is supported on FlexConnect access points in connected mode with local switching and central authentication. Also, Open SSID, MAC Filtering, and RADIUS NAC for a locally switched WLAN with FlexConnect access points is a valid configuration where MAC is checked by ISE.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-3/config-guide/b_cg83/flexconnect.html#:~:text=MAC%20Filtering%20is,checked%20by%20ISE.

upvoted 1 times


  **poy4242** 2 years, 11 months ago

Selected Answer: A

As per cisco documentation

All 802.11 authentication and association processing occurs regardless of which operational mode the AP is in. When in connected mode, the FlexConnect AP forwards all association/authentication information to the WLC. When in standalone mode, the AP cannot notify the WLC of such events, which is why WLANs that make use of central authentication/switching methods are unavailable.

upvoted 4 times

  **drel** 3 years, 11 months ago

Not D. Disabling local auth cannot disconnect already authenticated clients and cannot impact on broadcasting SSID

upvoted 3 times

  **Pawnstar** 3 years, 9 months ago

Well whats the answer then if it isn't D?

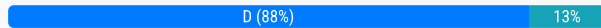
upvoted 3 times

An engineer must implement intrusion protection on the WLAN. The AP coverage is adequate and on-channel attacks are the primary concern. The building is historic, which makes adding APs difficult. Which AP mode and submode must be implemented?

- A. AP mode: local, AP submode: none
- B. AP mode: monitor, AP submode: WIPS
- C. AP mode: monitor, AP submode: none
- D. AP mode: local, AP submode: WIPS

Suggested Answer: D

Community vote distribution



🗳️ 👤 **55f2ace** 2 months, 1 week ago

Selected Answer: A

This is on the Guide Chapter 14.

aWIPS can work but is inefficient in this case, and attack detection may be slow. However, if you are primarily concerned about on-channel attacks (that is, incidents where attackers attempt to spoof your APs, act as relays, or perform other attacks while operating on the same channels as your active APs), then this mode is perfectly sufficient.

upvoted 1 times

🗳️ 👤 **GoldLeader** 11 months, 2 weeks ago

Selected Answer: D

Both B and D would enable Intrusion protection. However, D is the best answer because the question states that the building is historic and adding APs is difficult. Therefore you would not want to switch existing client serving local access points to monitor mode as this would create coverage holes not easily filled by adding coverage. D keeps the access point client serving as well as implementing intrusion protection.

upvoted 1 times

🗳️ 👤 **anagy11** 12 months ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **anagy11** 12 months ago

Wrong, D is the correct

upvoted 1 times

🗳️ 👤 **GnXxUbik** 6 days, 3 hours ago

B, because wips is only available in monitor mode

upvoted 1 times

🗳️ 👤 **Tonymopar** 1 year ago

B is correct

upvoted 1 times

🗳️ 👤 **Vlad_Is_Love_ua** 1 year, 1 month ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/wireless/technology/wips/deployment/guide/WiPS_deployment_guide.html

On-Channel vs. Off-Channel Scanning per WIPS Mode

The figure below explains the radio's behavior. When a radio is on its serving channel it is considered "on-channel", when the radio is scanning other channels, it is considered "off-channel".

An AP in local mode is mostly "on-channel", making it difficult to detect attackers "off-channel". A monitor mode AP is always "off-channel", but cannot server clients, the WSM module provides a great combination of both.

upvoted 3 times

  **Bergin_a** 1 year, 2 months ago

B is coreect

upvoted 2 times

  **Citizenx** 2 years, 1 month ago

correct, the on-channel says no need to scan other channels.

upvoted 3 times

  **kthekillerc** 2 years, 8 months ago

provided answer is correct

upvoted 3 times

An engineer is implementing a FlexConnect group for access points at a remote location using local switching but central DHCP. Which client feature becomes available only if this configuration is changed?

- A. multicast
- B. static IP
- C. fast roaming
- D. mDNS

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **[Removed]** 11 months, 4 weeks ago

Selected Answer: B

Answer is B

upvoted 4 times

🗳️ 👤 **GoldLeader** 1 year, 11 months ago

Selected Answer: B

DHCP is required when central DHCP is enabled. A client device is therefore not allowed to have a static non dhcp assigned IP. So B. Static IP feature becomes available if you disable central DHCP.

upvoted 2 times

🗳️ 👤 **Citizenx** 3 years, 1 month ago

Selected Answer: B

Agree with kthekillerc

upvoted 3 times

🗳️ 👤 **AleGil** 3 years, 2 months ago

D is the right answer: mDNS is not supported over local switching, you have to change the config to Central switching. Answer B cannot be true, because it's not related to clients.

upvoted 1 times

🗳️ 👤 **kthekillerc** 3 years, 8 months ago

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-7/configguide/b_cg87/flexconnect.html Provided answer is correct. After 3 failed attempts the static Ip is given.

upvoted 4 times

🗳️ 👤 **jemand3** 3 years, 1 month ago

This would be the better explanation: "For WLANs with local switching and central DHCP feature enabled, clients with static IP addresses are not allowed. Enabling central DHCP will internally enable DHCP required option." Provided answer is correct.

upvoted 4 times

🗳️ 👤 **fimka** 4 years, 5 months ago

There must be a config exhibit or something missing, as the options or the "right answer" make no sense or am I just reading it right..?

upvoted 2 times

🗳️ 👤 **fimka** 4 years, 5 months ago

Actually, after reviewing this, there is nothing missing. This is apparently just about local switching limitations. mDNS snooping is not available in local switching. Static IP might be indeed correct, if we also assume that central authentication is implemented, as in that case the "Learn Client IP Address" default should be disabled...

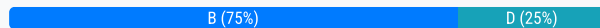
upvoted 2 times

A FlexConnect remote office deployment is using five 2702i APs indoors and two 1532i APs outdoors. When a code upgrade is performed and FlexConnect Smart AP Image Upgrade is leveraged, but no FlexConnect Master AP has been configured, how many image transfers between the WLC and APs will occur?

- A. 1
- B. 2
- C. 5
- D. 7

Suggested Answer: B

Community vote distribution



Skliffi Highly Voted 4 years, 7 months ago

Correct.

"A FlexConnect group can have one primary AP per AP model. If a primary AP is not selected manually, the AP that has the least MAC address value is automatically chosen as the primary AP for that model."

upvoted 8 times

Igur 4 years, 7 months ago

nevertheless the "B" is correct.

"A FlexConnect group can have one primary AP per AP model" So, one AP of each model will download the upgrade image. In this case total 2 image transfers will occur

upvoted 7 times

sjorwen Most Recent 11 months ago

Selected Answer: D

Without a Master AP configured, each AP will individually download the image from the WLC. Thus, the total number of image transfers between the WLC and the APs will be equal to the number of APs. so answer is 7

upvoted 1 times

GoldLeader 1 year, 11 months ago

Selected Answer: B

Answer B. is correct.

upvoted 1 times

kthekillerc 3 years, 8 months ago

provided answer is correct

upvoted 3 times

franc79 4 years ago

hi guys, did you pass the exam? can you give any more suggestion privately?

upvoted 3 times

Where is a Cisco OEAP enabled on a Cisco Catalyst 9800 Series Wireless Controller?

- A. RF Profile
- B. Flex Profile
- C. Policy Profile
- D. AP Join Profile

Suggested Answer: B

Reference:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/flexconnect.html

Community vote distribution

B (100%)

🗲️ 👤 **rrahim** 5 months, 1 week ago

Selected Answer: B

Step 1. Create a new Flex Profile. Go to Configuration > Tags & Profiles > Flex. select Add.

Step 2. Enter a Name and enable OEAP. Also, make sure the native VLAN ID is the one in the AP switchport.

upvoted 1 times

🗲️ 👤 **GoldLeader** 11 months, 2 weeks ago

Selected Answer: B

Answer B. is correct.

upvoted 2 times

🗲️ 👤 **Pawnstar** 2 years, 8 months ago

Configuration

Answer is correct.

1. In order to create a Flex profile, enable Office Extend AP and navigate to Configuration > Tags & Profiles > Flex.

upvoted 4 times

🗲️ 👤 **kthekillerc** 2 years, 8 months ago

provided answer is correct

upvoted 3 times

When configuring a Cisco WLC, which CLI command adds a VLAN with VLAN ID of 30 to a FlexConnect group named BranchA-FCG?

- A. config flexconnect BranchA-FCG vlan 30 add
- B. config flexconnect BranchA-FCG vlan add 30
- C. config flexconnect group BranchA-FCG vlan 30 add
- D. config flexconnect group BranchA-FCG vlan add 30

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **GoldLeader** 11 months, 2 weeks ago

Selected Answer: D

Answer D. is correct.

upvoted 1 times

🗳️ 👤 **Liselot** 1 year, 11 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/flexconnect_groups.html

upvoted 3 times

🗳️ 👤 **kthekillerc** 2 years, 7 months ago

Provided answer is correct

upvoted 3 times

🗳️ 👤 **Pawnstar** 2 years, 8 months ago

config flexconnect group group-name vlan add vlan-id.

Answer is correct.

upvoted 4 times

The image shows the Cisco FlexConnect configuration page with the following settings:

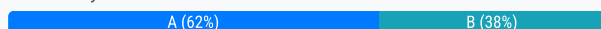
- General** tab is selected.
- Maximum Allowed Clients Per AP Radio: 200
- Clear HotSpot Configuration: ☐ Enabled
- Client user idle timeout(15-100000): ☐
- Client user idle threshold (0-10000000): 0 Bytes
- Radius NAI-Realm: ☐
- 11ac MU-MIMO: ☒
- Off Channel Scanning Defer**
 - Scan Defer Priority: 0 1 2 3 4 5 6 7
 - 0: ☐ 1: ☐ 2: ☐ 3: ☐ 4: ☒ 5: ☒ 6: ☒ 7: ☐
 - Scan Defer Time(msecs): 100
- FlexConnect**
 - FlexConnect Local Switching ²: ☐ Enabled
 - FlexConnect Local Auth ¹²: ☐ Enabled
 - Learn Client IP Address ⁵: ☒ Enabled

Refer to the exhibit. A customer has implemented Cisco FlexConnect deployments with different WLANs around the globe and is opening a new branch in a different location. The engineer's task is to execute all the wireless configuration and to suggest how to configure the switch ports for new APs. Which configuration must the switching team use on the switch port?

- A. trunk mode
- B. access mode
- C. single VLAN
- D. multiple VLAN

Suggested Answer: A

Community vote distribution



Fortinet Highly Voted 3 years, 4 months ago

answer should be B, there is no wlan being switch locally as shown in the picture by not checking flexconnect local switching
upvoted 9 times

CiscoTester1 Most Recent 1 year ago

Shouldn't it be A-Trunk mode because picture is showing WLAN's Flexconnect configuration page, While AP's Flexconnect Tab will have VLAN support option, Native VLAN and WLAN to VLAN Mapping
upvoted 1 times

raphim 1 year, 2 months ago

Selected Answer: A

Because the question contains "FlexConnect deployments with different WLANs" i would choose A
upvoted 2 times

Roomy 1 year, 2 months ago

Answer should be B- Access Mode
upvoted 1 times

GoldLeader 1 year, 5 months ago

Selected Answer: A

Answer A. Trunk Mode is the best answer. I think this question is trying to be tricky by showing the FlexConnect Local Switching enabled checkbox "unchecked". And while true if this was the only WLAN enabled an access port config would work. This however is not in keeping with the whole point of FlexConnect which is to do local switching in which case a trunk port is required.

upvoted 4 times

🗳️ 👤 **Vlad_Is_Love_ua** 1 year, 5 months ago

Selected Answer: A

if to listen to recommendations Cisco that is correct is - A. trunk.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/flexconnect.html#flex-vlans-acls:~:text=You%20can%20configure%20the,locally%20switched%20client%20traffic.

upvoted 1 times

🗳️ 👤 **simo_2020** 1 year, 8 months ago

Selected Answer: A

The answer should be (A):

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/flexconnect.html#:~:text=VLANs%20and%20ACLs,you%20,-can%20configure%20the

upvoted 2 times

🗳️ 👤 **JimDiGriz** 1 year, 9 months ago

ChatGPT says:

To configure switch ports for new APs in a FlexConnect deployment, the switching team should use the following configuration:

Configure the switch port as an access port and assign it to the appropriate VLAN.

Enable Power over Ethernet (PoE) on the switch port to provide power to the AP.

Enable PortFast on the switch port to speed up the process of moving the port to the forwarding state.

Configure the switch port as an edge port to prevent the port from participating in Spanning Tree Protocol (STP) convergence.

Configure the switch port with the appropriate Quality of Service (QoS) settings to ensure that traffic from the AP is given priority over other traffic.

For FlexConnect deployments, it is recommended to configure the switch port as an access port rather than a trunk port. This allows the AP to communicate directly with the FlexConnect controller without interference from other VLANs. Additionally, when configuring the switch port as an access port, ensure that the native VLAN on the switch port matches the VLAN assigned to the WLAN.

It is also important to configure the AP with the appropriate VLAN and SSID settings to ensure that it can communicate with the FlexConnect controller and provide wireless access to clients.

upvoted 2 times

🗳️ 👤 **itapase0314** 1 year, 11 months ago

Selected Answer: A

Access port works but Trunk port on configuration guide, as other SSIDs potentially requires local-switching.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html

upvoted 1 times

🗳️ 👤 **Caradum** 2 years, 5 months ago

Selected Answer: B

AP is in local mode. So no trunk port needed.

upvoted 3 times

🗳️ 👤 **Citizenx** 2 years, 7 months ago

not enabling local switching means the AP works like local mode AP en switch port remains an access port. All other wlan goes centrally through the capwap tunnel.

Answer=B

upvoted 2 times

🗳️ 👤 **rrahim** 5 months ago

yeah, so many people here don't understand the difference between WLAN and VLAN and don't even know what CAPWAP tunnel is.

upvoted 1 times

🗨️ 👤 **junjunpatotoy** 2 years, 10 months ago

Selected Answer: B

It should be an access port

upvoted 2 times

🗨️ 👤 **Guglielmino** 2 years, 9 months ago

"different WLANs" --> I think that the correct answer is trunk port

upvoted 2 times

🗨️ 👤 **Seba_o_s** 1 year, 1 month ago

But the WLAN is centrally so the VLAN would be at the WLC not local at the switch. The WLAN/VLAN assignment would be a mapping at AP group.

upvoted 1 times

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

Answer A is correct. The connecting switchports should be configured as trunk, not in access mode.

upvoted 1 times

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

provided answer is correct

upvoted 1 times

🗨️ 👤 **kashika_2** 3 years, 2 months ago

I would say A correct.

Picture shows how to configure one wlan, OEAP Flexconnect should be configured on the AP not the wlan.

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/215928-flexconnect-oeap-with-split-tunneling-co.html>

upvoted 3 times

A corporation is spread across different countries and uses MPLS to connect the offices. The senior management wants to utilize the wireless network for all the employees. To ensure strong connectivity and minimize delays, an engineer needs to control the amount of traffic that is traversing between the APs and the central WLC. Which configuration should be used to accomplish this goal?

- A. FlexConnect mode with central switching enabled
- B. FlexConnect mode with central authentication
- C. FlexConnect mode with OfficeExtend enabled
- D. FlexConnect mode with local authentication

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **GoldLeader** 11 months, 2 weeks ago

Selected Answer: D

Answer D. is correct.

upvoted 1 times

🗳️ 👤 **Vlad_Is_Love_ua** 11 months, 3 weeks ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/flexconnect.html#flexconnect-switching-modes~:text=Configuring%20FlexConnect,-FlexConnect%20Overview,-FlexConnect%20is%20a

upvoted 1 times

🗳️ 👤 **chomjosh** 2 years ago

FlexConnect mode with local authentication and local switching. Answer D implies this since central switching implementation would result in an increase in traffic traversing between the APs and WLC.

upvoted 2 times

🗳️ 👤 **malkana** 2 years, 4 months ago

Local authentication can only be enabled on the WLAN of a FlexConnect access point that is in local switching mode. Question says The senior management wants to utilize the wireless network for all the employees.

I reckon than FlexConnect mode with OfficeExtend enabled is the best option to choose

upvoted 2 times

🗳️ 👤 **chomjosh** 2 years ago

this is a typical Cisco question that attempts to draw away attention from the critical and important aspects you should be considering. The statement: "wants to utilize the wireless network for all employees" is completely irrelevant in this context as there is no mention of location(office or home). This is a mere deflection, so OfficeExtend option would not be a best answer, since there's that possibility that the Wireless usage all the employees in reference might just be at the office locations ONLY.

upvoted 3 times

🗳️ 👤 **Guglielmino** 2 years, 3 months ago

OfficeExtend make sense on Internet, but these employees are connected through MPLS

upvoted 3 times

🗳️ 👤 **Johnconnor2021** 10 months, 1 week ago

As Guglielmino says would make sense if it say Internet instead of MPLS. Moreover, it says the corporation has spread over several countries hence it's a central WLC so it's RELEVANT to consider OfficeExtend as an option. Hence, I disagree with chomjosh argument but since the question mentions MPLS what Guglielmino said must be considered. OfficeExtend is not a suitable option here because of that.

upvoted 1 times

🗳️ 👤 **Pawnstar** 2 years, 8 months ago

This answer is completely irrelevant. The question is asking how to minimise traffic between the AP and controller which is located over the WAN. Answer would be FlexConnect for local switching and local authentication.

Provided answer is correct.

upvoted 3 times

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

OEAP allows the control of what traffic goes back to the WLC by deciding what traffic will be split tunneled.

upvoted 1 times

🗨️ 👤 **kthekillerc** 2 years, 8 months ago

provided answer is correct.

upvoted 1 times

🗨️ 👤 **NightmareCreature** 2 years, 10 months ago

I think the answer here should be C

A Cisco OfficeExtend access point (Cisco OEAP) provides secure communications from a Cisco WLC to a Cisco AP at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. The user's experience at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security. Cisco OEAPs are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), enabling an entire group of computers to be represented by a single IP address. There is no limit to the number of Cisco OEAPs that you can deploy behind a NAT device.

upvoted 2 times

🗨️ 👤 **Johnconnor2021** 10 months, 1 week ago

you said yourself : (...) over the Internet (...) but the question says through MPLS which normally is more expensive. Hence, Local Auth is a more suitable option. If the question would have mentioned Internet then OfficeExtend would have more sense IMO.

upvoted 1 times

An engineer configures a Cisco Aironet 600 Series OfficeExtend AP for a user who works remotely. What is configured on the Cisco WLC to allow the user to print a printer on his home network?

- A. split tunneling
- B. SE-connect
- C. FlexConnect
- D. AP failover priority

Suggested Answer: A

Reference:

<https://www.cisco.com/c/en/us/support/docs/wireless/aironet-602-officeextend-access-point/117540-configure-splittunneloeap-00.html>

  **rrahim** 4 months, 1 week ago

Selected Answer: A

Why Not the Other Options?

B. SE-Connect ✖

SE-Connect (Spectrum Expert Connect) is used for wireless spectrum analysis and does not help with routing traffic between corporate and local networks.

C. FlexConnect ✖

FlexConnect is used in branch offices to allow APs to switch traffic locally when the WLC is unavailable.


OEAP does not use FlexConnect, as it operates in a fully tunneled mode by default.

D. AP Failover Priority ✖

AP Failover Priority determines which APs reconnect first to a WLC in case of a failure.

It does not control traffic flow between the corporate SSID and local home devices.

upvoted 1 times


  **rrahim** 4 months, 1 week ago

A Cisco Aironet 600 Series OfficeExtend AP (OEAP) is designed for remote users to securely extend corporate wireless connectivity to their home.

By default, an OEAP tunnels all traffic back to the corporate WLC using CAPWAP. This means that devices connected to the OEAP cannot communicate with local home network devices (such as a printer) unless Split Tunneling is enabled.

With Split Tunneling, the AP can be configured to send corporate traffic to the WLC while allowing local traffic (like printing) to stay within the home network.

upvoted 1 times

  **kthekillerc** 7 months, 2 weeks ago

Provided answer is correct

upvoted 4 times



An engineer must configure a Cisco WLC to support Cisco Aironet 600 Series OfficeExtend APs. Which two Layer 2 security options are supported in this environment? (Choose two.)

- A. Static WEP + 802.1X
- B. WPA+WPA2
- C. Static WEP
- D. CKIP
- E. 802.1X

Suggested Answer: BC

Community vote distribution

BE (100%)

  **rrahim** 4 months, 1 week ago

Selected Answer: BE

When configuring a Cisco Wireless LAN Controller (WLC) to support Cisco Aironet 600 Series OfficeExtend APs, the following Layer 2 security options are supported:

WPA+WPA2 (B):

WPA (Wi-Fi Protected Access) and WPA2 are robust security protocols that provide strong encryption and authentication. They are widely supported and recommended for securing wireless networks.

WPA2 uses AES encryption, which is more secure than WEP.

802.1X (E):

802.1X is an authentication framework that provides port-based network access control. It is often used in conjunction with WPA or WPA2 to authenticate users or devices before granting access to the network.

It works with EAP (Extensible Authentication Protocol) methods like EAP-TLS, EAP-PEAP, or EAP-FAST.

upvoted 1 times

  **rrahim** 4 months, 1 week ago

Why not the other options?

A. Static WEP + 802.1X:

Static WEP (Wired Equivalent Privacy) is an outdated and insecure encryption method. While 802.1X is secure, combining it with WEP is not recommended because WEP is vulnerable to attacks.

C. Static WEP:

Static WEP is not considered secure and is not recommended for modern wireless networks. It is easily cracked and does not meet current security standards.

D. CKIP:

CKIP (Cisco Key Integrity Protocol) is a proprietary encryption protocol used by Cisco, but it is not commonly used or supported in modern wireless deployments. It is not a standard Layer 2 security option for OfficeExtend APs.

Conclusion:

The two supported and recommended Layer 2 security options for Cisco Aironet 600 Series OfficeExtend APs are WPA+WPA2 and 802.1X.

upvoted 1 times

  **ahmie** 7 months, 2 weeks ago

For Layer 2 Security, the following options are supported for the 600 Series OfficeExtend Access Point:

None.

WPA+WPA2.

Static WEP.

802.1X (only for remote LANs) Figure 2. WLAN Layer 2 Security Settings.

Answer is correct!!!

upvoted 1 times

🗨️ 👤 **raphim** 8 months, 2 weeks ago

Selected Answer: BE

In the datasheet is WEP not listed but 802.1x and WPA/WPA2

I would choose B and E

upvoted 2 times

🗨️ 👤 **Pawnstar** 2 years, 8 months ago

Answer is correct.

For Layer 2 Security, only these options are supported for the Cisco Aironet 600 Series OEAP:

None

WPA+WPA2

Static WEP can also be used but not for .11n data rates.

upvoted 4 times

🗨️ 👤 **kthekillerc** 2 years, 8 months ago

provided answer is correct

upvoted 2 times

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

B,E correct.

Aironet 600 Datasheet:

Security

- 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA
- 802.1X
- Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP)

upvoted 2 times

🗨️ 👤 **Igur** 3 years, 7 months ago

nevertheless B+C are correct answers.

"When setting the security setting in the WLAN, there are specific elements that are not supported on the 600 series. For Layer 2 Security, only these options are supported for the Cisco Aironet 600 Series OEAP:

None

WPA+WPA2

Static WEP can also be used but not for .11n data rates."



<https://www.cisco.com/c/en/us/support/docs/wireless/aironet-600-series-officeextend-access-point/113003-office-extend-config-00.html#wlan-settings>

upvoted 11 times

An organization is supporting remote workers in different locations. In order to provide wireless network connectivity and services, OfficeExtend has been implemented. The wireless connectivity is working, but users report losing connectivity to their local network printers. Which solution must be used to address this issue?

- A. OEAP gateway override
- B. OEAP split tunnel
- C. WLAN static IP tunneling
- D. FlexConnect local switching

Suggested Answer: B

  **kthekillerc** Highly Voted 8 months, 4 weeks ago
provided answer is correct
upvoted 6 times

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

Selected Answer: B

OfficeExtend AP (OEAP) is used to provide secure corporate wireless connectivity to remote users working from home. By default, all traffic from an OEAP is tunneled back to the corporate WLC, meaning that local network devices (like home printers) are inaccessible.

To fix this, OEAP Split Tunnel must be enabled.

- ✓ OEAP Split Tunnel allows the AP to send corporate traffic to the WLC while keeping local traffic within the home network.
- ✓ This enables users to connect to both the corporate network and their local devices (like home printers).

upvoted 1 times

  **rrahim** 4 months, 1 week ago

A. OEAP Gateway Override ✗

This setting is used to override the default gateway configuration for the OEAP but does not control how traffic is split between corporate and local networks.

C. WLAN Static IP Tunneling ✗

This feature is not related to OfficeExtend or local printing issues.

It deals with static IP clients in tunneled WLANs, not split traffic handling.

D. FlexConnect Local Switching ✗

FlexConnect is used in branch offices, allowing APs to switch traffic locally only when disconnected from the WLC.

OEAP does not use FlexConnect; it relies on a dedicated CAPWAP tunnel.

upvoted 1 times

What is configured to use more than one port on the OEAP to extend the wired network?

- A. remote LAN ACL
- B. AAA override
- C. client load balancing
- D. remote LAN

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **rrahim** 4 months, 1 week ago

Selected Answer: D

The remote LAN feature on the Cisco OfficeExtend Access Point (OEAP) allows the use of more than one port to extend the wired network. This is particularly useful for remote workers who need to connect multiple wired devices (such as printers, desktop computers, or other peripherals) to their local network while also being connected to the corporate wireless network.

Remote LAN:

This feature enables the OEAP to provide wired connectivity to local devices through its Ethernet ports. It essentially extends the wired network at the remote site, allowing local devices to communicate with each other and access the corporate network securely.

upvoted 1 times

🗨️ 👤 **Vlad_Is_Love_ua** 11 months, 3 weeks ago

Selected Answer: D

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215681-configure-oeap-and-rlan-on-catalyst-9800.html#anc8:~:text=an%20OfficeExtend%20AP,Configure%20RLAN%20on%209800%20WLC,clients%20in%20RLAN%20is%20similar%20to%20the%20central%20Local%20EAP>

upvoted 2 times

🗨️ 👤 **kthekillerc** 2 years, 8 months ago

provided answer is correct

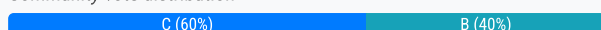
upvoted 2 times

An engineer must implement Cisco Identity-Based Networking Services at a remote site using ISE to dynamically assign groups of users to specific IP subnets. If the subnet assigned to a client is available at the remote site, then traffic must be offloaded locally, and subnets are unavailable at the remote site must be tunneled back to the WLC. Which feature meets these requirements?

- A. learn client IP address
- B. FlexConnect local authentication
- C. VLAN-based central switching
- D. central DHCP processing

Suggested Answer: C

Community vote distribution



Sorvahr Highly Voted 4 years, 2 months ago

Answer is correct.

B is about authentication, not about switching the traffic.

upvoted 6 times

rrahim Most Recent 4 months, 1 week ago

Selected Answer: C

To meet the requirements of dynamically assigning groups of users to specific IP subnets and ensuring that traffic is offloaded locally if the subnet is available at the remote site (or tunneled back to the WLC if the subnet is unavailable), the VLAN-based central switching feature is used.

VLAN-based central switching:

This feature allows the FlexConnect Access Point (AP) to determine whether to switch traffic locally or tunnel it back to the Wireless LAN Controller (WLC) based on the VLAN assigned to the client. If the VLAN (and corresponding subnet) is available at the remote site, traffic is switched locally. If the VLAN is not available, traffic is tunneled back to the WLC.

upvoted 1 times

rrahim 4 months, 1 week ago

Why not the other options?

A. Learn client IP address:

This feature allows the AP to learn the IP address of the client, but it does not determine whether traffic should be offloaded locally or tunneled back to the WLC.

B. FlexConnect local authentication:

This feature allows the AP to authenticate clients locally at the remote site, but it does not address the requirement of dynamically assigning subnets or offloading traffic based on subnet availability.

D. Central DHCP processing:

This feature involves the WLC handling DHCP requests for clients, but it does not determine whether traffic should be offloaded locally or tunneled back to the WLC based on subnet availability.

upvoted 1 times

Gumpy1 7 months, 1 week ago

Selected Answer: C

I do believe C is correct. This is about switching traffic. When a user is in the process of being authenticated he isn't switched to a different subnet UNTIL after he is authenticated, so I don't think option b is correct.

upvoted 1 times

Supersede 8 months, 4 weeks ago

Selected Answer: C

C

When a WLAN is locally switched in flex and a VLAN is configured on the AP side, the traffic is switched locally. When a VLAN is not defined in an AP, the VLAN drops the packet.

When VLAN-based central switching is enabled, the corresponding AP tunnels the traffic back to the controller. The controller then forwards the traffic to its corresponding VLAN.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/16-12/config-guide/b_wl_16_12_cg/flexconnect.html

upvoted 1 times

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

Selected Answer: B

FlexConnect local authentication is a feature that allows FlexConnect APs to authenticate clients locally and assign them IP addresses from a subnet that is available at the remote site. If the subnet assigned to the client is unavailable at the remote site, the traffic is tunneled back to the WLC.

upvoted 1 times

🗨️ 👤 **Roomy** 1 year, 2 months ago

B is correct

upvoted 1 times

🗨️ 👤 **GoldLeader** 1 year, 5 months ago

Selected Answer: C

C. is correct.

upvoted 1 times

🗨️ 👤 **JimDiGriz** 1 year, 8 months ago

Selected Answer: B

The correct answer is B. FlexConnect local authentication.

FlexConnect local authentication allows the WLC to offload authentication and authorization of clients to the local AP in FlexConnect mode. This means that the AP at the remote site can dynamically assign groups of users to specific IP subnets based on their authentication and authorization status, and then locally offload the traffic for those subnets. If a subnet is not available at the remote site, the AP can tunnel the traffic back to the WLC for central processing.

upvoted 1 times

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

provided answer is correct

upvoted 2 times

🗨️ 👤 **Mimimimimi** 2 years, 9 months ago

Adding source:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide/ch7_HREA.html#:~:text=FlexConnect%20VLAN%20Based%20Central%20Switching

upvoted 4 times

An engineer must configure Cisco OEAPs for three executives. As soon as the NAT address is configured on the management interface, it is noticed that the WLC is not responding for APs that are trying to associate to the internal IP management address. Which command should be used to reconcile this?

- A. config flexconnect office-extend nat-ip-only disable
- B. config network ap-discovery nap-ip-only enable
- C. config flexconnect office-extend nat-ip-only enable
- D. config network ap-discovery nat-ip-only disable

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **rrahim** 4 months, 1 week ago

Selected Answer: D

When configuring Cisco OfficeExtend APs (OEAPs), the NAT address is assigned to the management interface to allow remote APs to reach the WLC over the internet. However, once NAT is enabled, APs that were using the internal IP to associate fail to connect.

To fix this, you need to disable the setting that forces APs to use only the NAT IP for discovery:

✓ Running the command `config network ap-discovery nat-ip-only disable` allows both internal and external APs to discover the WLC using either the internal IP or the NAT IP.

upvoted 1 times

🗨️ 👤 **Vlad_Is_Love_ua** 11 months, 3 weeks ago

Selected Answer: D

`config network ap-discovery nat-ip-only {enable | disable}`

where

enable—Enables use of NAT IP only in Discovery response. This is the default. Use this command if all APs are outside of the NAT gateway.

disable—Enables use of both NAT IP and non-NAT IP in discovery response. Use this command if APs are on the inside and outside of the NAT gateway; for example, Local Mode and OfficeExtend APs on the same controller.

<https://community.cisco.com/t5/wireless/office-extend-ap-and-external-addresses/td-p/3742395>

upvoted 3 times

🗨️ 👤 **mikmon1** 1 year, 9 months ago

Selected Answer: D

D looks good

upvoted 2 times

An engineer is responsible for a wireless network for an enterprise. The enterprise has distributed offices around the globe, and all APs are configured in FlexConnect mode. The network must be configured to support 802.11r and CCKM. What needs to be implemented to accomplish this goal?

- A. Enable VLAN-based central switching.
- B. Enable FlexConnect local authentication.
- C. Enable FlexConnect local switching.
- D. Create FlexConnect groups.

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **rrahim** 4 months, 1 week ago

Selected Answer: D

When using FlexConnect mode, the APs can perform local switching and authentication without needing a constant connection to the WLC. However, fast roaming protocols like 802.11r (Fast Transition) and CCKM (Cisco Centralized Key Management) require additional configuration to work correctly.

- ✓ FlexConnect Groups allow APs to share security credentials and enable fast roaming between APs without needing to reauthenticate users.
 - ✓ This is required to support 802.11r and CCKM in FlexConnect mode.
- upvoted 1 times

🗳️ 👤 **Vlad_Is_Love_ua** 8 months ago

Selected Answer: D

FlexConnect with CCKM

Central Authentication is supported. This includes Local and Central data switching. The APs must be part of the same FlexConnect Group.

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html#anc9>

upvoted 1 times

🗳️ 👤 **Robesera** 1 year, 2 months ago

VLAN based switching is not relevant to the question.

11r is not supported with FlexConnect local auth.

Although local switching is supported for 11r, to use CCKM fast roaming with FlexConnect access points, you must configure FlexConnect Groups.

11r is only supported when all AP's are in the same Flex group.

Therefore, provided answer D is correct.

upvoted 2 times

A corporation has employees working from their homes. A wireless engineer must connect 1810 OEAP at remote teleworker locations. All configuration has been completed on the controller side, but the network readiness is pending. Which two configurations must be performed on the firewall to allow the AP to join the controller? (Choose two.)

- A. Block UDP ports 1812 and 1813 on the firewall.
- B. Enable NAT Address on the 5520 with an Internet-routable IP address.
- C. Configure a static IP on the OEAP 1810.
- D. Allow UDP ports 5246 and UDP port 5247 on the firewall.
- E. Allow UDP ports 12222 and 12223 on the firewall.

Suggested Answer: BD

Reference:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_Cisco_OfficeExtend_Access_Point_.pdf

Community vote distribution

BD (100%)

 **GnXxUbik** 6 days, 2 hours ago

Selected Answer: BD

copilot says B,D but gemini says D,E :)

upvoted 1 times

 **rrahim** 4 months, 2 weeks ago

Selected Answer: DE

D. Allow UDP ports 5246 and UDP port 5247 on the firewall.

These ports are used for communication between the OEAP and the WLC (Wireless LAN Controller). Allowing them ensures the OEAP can establish a connection to the controller.

E. Allow UDP ports 12222 and 12223 on the firewall.

These ports are also used for CAPWAP (Control and Provisioning of Wireless Access Points) communication between the OEAP and the WLC, enabling the AP to join the controller.

upvoted 1 times

 **GoldLeader** 11 months, 2 weeks ago

Selected Answer: BD

Going with B. and D. on this one but I agree with anagy11 comment that the wording "on the firewall" is confusing. D. and E. would be the only 2 answers that you make sense from that perspective but OEAP does not require ports 12222 and 12223 so E. makes no sense in that regard. Terrible question wording.

Corporate Firewall

The Wireless LAN Controller should be placed in DMZ and the corporate Firewall must allow CAPWAP Control and CAPWAP Data traffic through the Firewall to the Wireless LAN Controller. The general configuration on the firewall is to allow CAPWAP control and CAPWAP management port numbers through the firewall.

Note

The UDP 5246 and 5247 ports need to be opened on the firewall for communication between the Wireless LAN controller and the Cisco OfficeExtend Access Point 1810.

upvoted 1 times

 **anagy11** 12 months ago

Selected Answer: BD

Strange question wording...

"Which two configurations must be performed on the firewall to allow the AP to join the controller?"

on the firewall...

upvoted 2 times

🗨️ 👤 **qqqqqqqqqq123** 1 year, 7 months ago

B. Enable NAT Address on the 5520 with an Internet-routable IP address.

&

D. Allow UDP ports 5246 and UDP port 5247 on the firewall.

is correct <https://mrncciew.com/2013/03/12/how-does-oeap-work/>

upvoted 3 times

🗨️ 👤 **Henry_008** 1 year, 7 months ago

should be DE?

upvoted 2 times

🗨️ 👤 **PauBau** 1 year, 2 months ago

Agree, it is D and E.D.

Allow UDP ports 5246 and UDP port 5247 on the firewall: These are the default ports used by lightweight APs to communicate with the WLC for control and data traffic.

E. Allow UDP ports 12222 and 12223 on the firewall: These are the default ports used by CAPWAP for APs to communicate with the WLC.

upvoted 1 times


An enterprise has two WLANs configured on WLC. It is reported that when converting APs to FlexConnect mode, WLAN A works but WLAN B does not. When converting APs to local mode, WLAN B works, but WLAN A does not. Which action is needed to complete this configuration?

- A. Create a Cisco FlexConnect group with WLAN-VLAN mapping.
- B. Disable local switching on the WLANs.
- C. Map the AP group to the WLAN interface.
- D. Join the APs to a Cisco FlexConnect group.

Suggested Answer: A

Community vote distribution

A (100%)

 **rrahim** 4 months, 2 weeks ago

Selected Answer: A

In FlexConnect mode, WLANs must be properly mapped to VLANs at the branch office to function correctly. Creating a FlexConnect group and configuring WLAN-VLAN mapping ensures that the WLANs are correctly associated with the appropriate VLANs, allowing both WLANs to work in FlexConnect mode.

The other options are not the correct solutions:

B. Disable local switching on the WLANs: This would prevent WLANs from working in FlexConnect mode, which is not the desired outcome.

C. Map the AP group to the WLAN interface: This is not directly related to resolving the issue with FlexConnect mode.

D. Join the APs to a Cisco FlexConnect group: While this is necessary, it does not address the specific issue of WLAN-VLAN mapping required for WLAN B to work in FlexConnect mode.

upvoted 1 times

An engineer wants the wireless voice traffic class of service to be used to determine the queue order for packets received, and then have the differentiated services code point set to match when it is resent to another port on the switch. Which configuration is required in the network?

- A. Platinum QoS configured on the WLAN
- B. WMM set to required on the WLAN
- C. mls qos trust dscp configured on the controller switch port
- D. mls qos trust cos configured on the controller switch port

Suggested Answer: C

Community vote distribution

D (50%)

A (25%)

C (25%)

andit 2 years, 7 months ago

The Correct Answer is D.

"When you enter the mls qos trust cos command on a port, the switch uses the CoS marking on incoming packets in order to put the packet in the right queue. When the packet is resent, the switch makes the DSCP value correspond to the CoS."

See: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/voice-over-wireless-lan-vowlan/116056-technote-qos-00.html#anc3>
upvoted 8 times

Liselot 1 year, 11 months ago

I think andit's explanation is right
upvoted 1 times

somebodyfromtheinterwebz 1 year, 5 months ago

You gave the right surce, but the wrong answer:

"When you enter the mls qos trust dscp command on a port, (...) When the packet is resent on another port, the switch sets the CoS tag to match the DSCP so there is no conflict between the two values"

This is exactly what the questions asks.

The "mls qos trust cos" command, like you wrote just makes the DSCP value correspond to the CoS. But the case of the packet resenting to another port is not handled here.

upvoted 1 times

Mimimimimi 2 years, 3 months ago

Answer is C.

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/voice-over-wireless-lan-vowlan/116056-technote-qos-00.html#:~:text=When%20you%20enter,to%20the%20CoS.>

"Set to match" vs "correspond to"

upvoted 5 times

rrahim 4 months, 1 week ago

Selected Answer: D

In a wireless QoS deployment, voice traffic needs to be prioritized throughout the network. The Class of Service (CoS) values are assigned based on 802.1p (Layer 2 QoS), while Differentiated Services Code Point (DSCP) values are used for Layer 3 QoS.

✓ mls qos trust cos ensures that the switch trusts the CoS value assigned by the WLC and maps it to the appropriate DSCP value for end-to-end QoS.
upvoted 1 times

santoshkotla 5 months ago

Selected Answer: D

Concentrate on the wording. DSCP to correspond to CoS. Answer is D.
upvoted 1 times

[Removed] 8 months, 3 weeks ago

The engineer wants to use the wireless voice traffic class of service to determine the queue order for packets received. This means that Quality of Service (QoS) needs to be configured to prioritize voice traffic.

"cos" stands for Class of Service, which is typically used for Ethernet frames and not specifically designed for voice traffic prioritization.

In this case, the engineer wants to prioritize voice traffic using the wireless voice traffic class of service, which is better achieved by trusting the Differentiated Services Code Point (DSCP) value rather than the Class of Service (COS) value.

Therefore, option D is not the right configuration, and option C, "msl qos trust dscp configured on the controller switch port," is the correct configuration required in the network.

upvoted 1 times

🗳️ 👤 **Roomy** 9 months ago

D is correct - trust cos

upvoted 1 times

🗳️ 👤 **BrockHarbor** 10 months, 3 weeks ago

Selected Answer: D

Ignore the reference to DSCP upon resend. It is meant to throw you off and is irrelevant to what the question is asking.

The key ask here is to use the CoS to determine queue order for frames received on a switch.

upvoted 1 times

🗳️ 👤 **GoldLeader** 11 months, 2 weeks ago

Selected Answer: D

Answer D. I agree with andit explanation.

upvoted 1 times

🗳️ 👤 **Vlad_Is_Love_ua** 11 months, 3 weeks ago

Selected Answer: C

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/voice-over-wireless-lan-vowlan/116056-technote-qos-00.html#:~:text=When%20you%20enter,to%20the%20CoS.>

upvoted 1 times

🗳️ 👤 **kejvi** 1 year, 2 months ago

not msl qos.. but mls qos

upvoted 1 times

🗳️ 👤 **yrzy** 1 year, 3 months ago

Selected Answer: A

If WLAN QoS is default, the voice class of service will be rewritten to default on the controller.

Platinum QoS must be enabled to maintain class of service for received voice packets.

upvoted 1 times

🗳️ 👤 **twoplanker** 1 year, 7 months ago

Correct answer is D because the engineer was the voice traffic CLASS OF SERVICE to be used. So we're wanting to trust COS and have the switch then remark DSCP to match.

upvoted 1 times

🗳️ 👤 **HOT2012** 2 years, 7 months ago

C dscp

upvoted 2 times

🗳️ 👤 **kthekillerc** 2 years, 7 months ago

Provided answer is correct

upvoted 1 times

🗳️ 👤 **iamccie** 3 years, 3 months ago

Correct answer is D

upvoted 2 times

🗳️ 👤 **maro_moh** 3 years, 4 months ago

answer is D

upvoted 2 times

🗳️ 👤 **Net_Boy_RD** 3 years, 6 months ago

I think is A, because that commands are globally enable, not per port. And the answer talk about mark the traffic on the wireless, so the need to implement QoS on the wireless.

upvoted 1 times

When using a Cisco Catalyst 9800 Series Wireless Controller, which statement about AutoQoS is true?

- A. It has a set of predefined profiles that you cannot modify further
- B. It matches traffic and assigns each matched packet to QoS groups
- C. It automates deployment of wired QoS and makes wireless QoS implementation easier
- D. It allows the output policy map to put specific QoS queues into specific subgroups

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **74008cf** 2 weeks, 2 days ago

Selected Answer: C

Answer is C.

B is just a generic description about how QoS works, AutoQoS does much more.

upvoted 1 times

🗳️ 👤 **rrahim** 4 months, 1 week ago

Selected Answer: C

AutoQoS on the Cisco Catalyst 9800 Series Wireless Controller is designed to simplify the deployment of Quality of Service (QoS) across both wired and wireless networks. Here's why this statement is true:

Automates deployment of wired QoS:

AutoQoS automatically configures QoS settings on the wired network, ensuring that traffic is prioritized appropriately as it traverses the network.

Makes wireless QoS implementation easier:

AutoQoS also simplifies the configuration of wireless QoS by applying predefined QoS profiles and policies that align with best practices. This reduces the complexity of manually configuring QoS for wireless traffic.

Why not the other options?

A. It has a set of predefined profiles that you cannot modify further:

This is incorrect because AutoQoS does provide predefined profiles, but these profiles can be modified and customized as needed.

B. It matches traffic and assigns each matched packet to QoS groups:

While AutoQoS does involve traffic classification and prioritization, this statement is too specific and does not fully capture the broader purpose of AutoQoS, which is to automate and simplify QoS deployment.

upvoted 1 times

🗳️ 👤 **Vlad_Is_Love_ua** 7 months, 4 weeks ago

Selected Answer: B

Information About Auto QoS

Wireless Auto QoS automates deployment of wireless QoS features. It has a set of predefined profiles which can be further modified by the customer to prioritize different traffic flows. Auto-QoS matches traffic and assigns each matched packet to qos-groups. This allows the output policy map to put specific qos-groups into specific queues, including into the priority queue.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/16-12/config-guide/b_wl_16_12_cg/wireless-auto-qos.html

upvoted 2 times

🗳️ 👤 **Citizenx** 1 year, 7 months ago

Answer is correct

upvoted 2 times

🗳️ 👤 **kthekillerc** 2 years, 1 month ago

provided answer is correct

upvoted 1 times

🗳️ 👤 **skh** 2 years, 10 months ago

correct

Auto-QoS matches traffic and assigns each matched packet to qos-groups

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-2/config-guide/b_wl_17_2_cg/wireless_auto_qos.html

upvoted 4 times

A network engineer is deploying 8865 IP phones with wireless clients connected to them. In order to apply the appropriate QoS, the IP voice traffic needs to be distinguished from client data traffic. Which switch configuration feature must be enabled?

- A. Voice VLAN
- B. QBSS
- C. WME
- D. QoS routing

Suggested Answer: A

  **rrahim** 4 months, 1 week ago

Selected Answer: A

To distinguish IP voice traffic from client data traffic and apply the appropriate QoS, the Voice VLAN feature must be enabled on the switch. Here's why:

Voice VLAN:

This feature allows the switch to separate voice traffic (from devices like IP phones) from data traffic (from connected wireless clients). By assigning the IP phone to a dedicated Voice VLAN, the switch can prioritize voice traffic using QoS policies, ensuring high-quality voice communication.

How it works:

The IP phone is connected to the switch, and wireless clients may connect through the phone. The switch tags voice traffic with the Voice VLAN ID and applies QoS policies to prioritize it, while data traffic is handled separately.

upvoted 1 times

  **rrahim** 4 months, 2 weeks ago

Selected Answer: A

A Voice VLAN is specifically designed to separate voice traffic from data traffic on the network. By configuring a Voice VLAN, the switch can prioritize IP voice traffic (e.g., from the 8865 IP phones) and apply the appropriate QoS settings to ensure high-quality voice communication.

upvoted 1 times

  **kthekillerc** 7 months, 2 weeks ago

Provided answer is correct

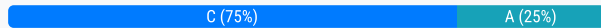
upvoted 4 times

A network engineer wants to implement QoS across the network that supports multiple VLANs. All the APs are connected to switch ports and are configured in local mode. Which trust model must be configured on the switch ports to which the APs are connected?

- A. CoS
- B. WMM UP
- C. DSCP
- D. IPP

Suggested Answer: C

Community vote distribution



🗳️ 👤 **rrahim** 4 months, 1 week ago

Selected Answer: C

When implementing QoS across a network that supports multiple VLANs and uses Cisco Access Points (APs) in local mode, the DSCP (Differentiated Services Code Point) trust model must be configured on the switch ports to which the APs are connected. Here's why:

DSCP Trust Model:

DSCP is a Layer 3 QoS marking that provides granular traffic classification and prioritization. When the switch ports trust DSCP, they honor the DSCP values in the IP headers of packets, ensuring consistent QoS treatment across the network. This is particularly important in a multi-VLAN environment where traffic from different VLANs may have different QoS requirements.

Local Mode APs:

In local mode, APs forward all traffic to the Wireless LAN Controller (WLC), which applies QoS policies based on DSCP markings. By configuring the switch ports to trust DSCP, the switch ensures that the QoS markings are preserved as traffic travels between the APs and the WLC.

upvoted 1 times

🗳️ 👤 **CiscoTester1** 1 year ago

Because Local mode on AP, APs will terminate CAPWAP tunnel and AP will use DSCP marking of CAPWAP tunnel and convert it to UP value for 802.11 frame using DSCP to UP mapping, so C DSCP is correct

upvoted 1 times

🗳️ 👤 **GoldLeader** 1 year, 5 months ago

Selected Answer: C

Cos markings only exist as a TAG within trunk packets. The question states that the access points are in local mode = access ports. There will therefore be no CoS markings on the packets between the access point and switch. Answer D. DSCP is correct as these markings are Layer3 and exist on both trunks and access ports.

upvoted 1 times

🗳️ 👤 **pioo1979** 1 year, 4 months ago

AP local mode != Local switching

AP local mode mean the AP build up a CAPWAP tunnel to the WLC :)

upvoted 1 times

🗳️ 👤 **Vlad_Is_Love_ua** 1 year, 5 months ago

Selected Answer: C

это dscp

upvoted 1 times

🗳️ 👤 **yrzy** 1 year, 9 months ago

Selected Answer: C

CAPWAP packets sent from local mode APs are UnTag packets.

upvoted 1 times

🗳️ 👤 **qqqqqqqqqq123** 2 years, 1 month ago

[https://www.cisco.com/c/en/us/support/docs/wireless-mobility/voice-over-wireless-lan-vowlan/116056-technote-qos-00.html#:~:text=Switchports%20connected%20to%20local%20mode%20access%20points%20\(APs\)%20and%20Hybrid%20Remote%20Edge%20Access%20Po](https://www.cisco.com/c/en/us/support/docs/wireless-mobility/voice-over-wireless-lan-vowlan/116056-technote-qos-00.html#:~:text=Switchports%20connected%20to%20local%20mode%20access%20points%20(APs)%20and%20Hybrid%20Remote%20Edge%20Access%20Po)

Answer is DSCP



upvoted 4 times

  **elmi4474** 2 years, 3 months ago

Selected Answer: A

When we use CoS, it is suppose to configure on trunk links and local switching. It makes sense with the option A.

upvoted 1 times

  **Citizenx** 2 years, 7 months ago

Agree with kthekillerc

upvoted 1 times

  **kthekillerc** 3 years ago

only option of trust mode is dscp

upvoted 2 times

  **kthekillerc** 3 years, 2 months ago

provided answer is correct. Switchports connected to local mode access points (APs) and Hybrid Remote Edge Access Point (H-REAP)/FlexConnect APs with no locally switching Wireless LANs (WLANs) should be access ports set with the mls qos trust dscp command. It could not be B as there is no such thing. 3 options for WMM are disabled, required, and allowed.

upvoted 4 times

  **Pawnstar** 3 years, 3 months ago

Answer is B.

upvoted 1 times

An enterprise started using WebEx as a virtual meeting solution. There is a concern that the existing wireless network will not be able to support the increased amount of traffic as a result of using WebEx. An engineer needs to remark the QoS value for this application to ensure high quality in meetings. What must be implemented to accomplish this task?

- A. QoS preferred call index
- B. UP to DSCP map
- C. AVC profiles
- D. WLAN quality of service profile

Suggested Answer: C

Reference:

<https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2018/pdf/BRKEWN-3003.pdf>


Community vote distribution

C (100%)

 **jncreator** Highly Voted 3 years ago

C is correct.

upvoted 7 times

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

Selected Answer: C

To ensure high-quality WebEx meetings on the wireless network, the engineer must implement AVC (Application Visibility and Control) profiles. Here's why:

AVC Profiles:

AVC allows the network to identify and classify specific applications, such as WebEx, and apply appropriate QoS policies to them. By creating an AVC profile for WebEx, the engineer can remark the QoS value (e.g., DSCP or UP) for WebEx traffic, ensuring it receives the necessary priority and bandwidth for high-quality performance.

How it works:

AVC uses deep packet inspection (DPI) to recognize application traffic. Once identified, the traffic can be marked with the appropriate QoS value and prioritized accordingly.

upvoted 1 times

 **Vlad_Is_Love_ua** 11 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

 **qqqqqqqqqq123** 1 year, 7 months ago

[https://www.cisco.com/c/en/us/support/docs/wireless-mobility/voice-over-wireless-lan-vowlan/116056-technote-qos-00.html#:~:text=Switchports%20connected%20to%20local%20mode%20access%20points%20\(APs\)%20and%20Hybrid%20Remote%20Edge%20Access%20Po](https://www.cisco.com/c/en/us/support/docs/wireless-mobility/voice-over-wireless-lan-vowlan/116056-technote-qos-00.html#:~:text=Switchports%20connected%20to%20local%20mode%20access%20points%20(APs)%20and%20Hybrid%20Remote%20Edge%20Access%20Po)

upvoted 1 times

 **qqqqqqqqqq123** 1 year, 7 months ago

posted in error.

upvoted 1 times

 **chomjosh** 2 years, 1 month ago

C correct

upvoted 1 times

 **Oscar14258** 2 years, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

🗨️ 👤 **HOT2012** 2 years, 7 months ago

Selected Answer: C

C correct

upvoted 1 times

🗨️ 👤 **Pawnstar** 2 years, 8 months ago

Correct answer is C.

upvoted 1 times

🗨️ 👤 **Solanki** 2 years, 8 months ago

C. Application Visibility & Control (AVC) allows: • Deep Packet Inspection in the wireless controller – allows application identification, remarking, rate limiting, and dropping of unwanted traffic.

upvoted 3 times

🗨️ 👤 **kthekillerc** 2 years, 8 months ago

For optimum performance, the network must recognize Webex traffic, mark it with a DSCP (Differentiated Services Code Point) value, and prioritize the flows as they traverse the network. Without proper protection, congestion can cause performance impacts to both Webex communication traffic on highly utilized enterprise networks. This congestion typically occurs at the WAN edge and Internet perimeter. Provided answer is correct.

upvoted 1 times

A corporation has a wireless network where all access points are configured in FlexConnect. The WLC has a Data WLAN and a VoWiFi WLAN implemented where centrally-switched SSID is configured for the APs. Which QoS configuration must be implemented for the wireless packets to maintain the marking across the wired and wireless network?


- A. Set QoS to Platinum.
- B. Enable CAC.
- C. Allow WMM.
- D. Trust DSCP.

Suggested Answer: D

Community vote distribution

D (50%)

A (50%)

 **rrahim** 4 months, 1 week ago

Selected Answer: D

In a FlexConnect deployment where access points (APs) are configured with centrally-switched SSIDs, the Trust DSCP QoS configuration must be implemented to maintain consistent QoS markings across the wired and wireless network. Here's why:


Trust DSCP:

DSCP (Differentiated Services Code Point) is a Layer 3 QoS marking that provides end-to-end traffic prioritization. By configuring the Wireless LAN Controller (WLC) and APs to trust DSCP, the QoS markings in the IP headers of packets are preserved as traffic traverses both the wired and wireless network. This ensures consistent QoS treatment for applications like voice (VoWiFi) and data.

Centrally-Switched SSIDs:

In centrally-switched mode, traffic from the APs is tunneled back to the WLC. Trusting DSCP ensures that the QoS markings are maintained as traffic passes through the WLC and into the wired network.

upvoted 1 times

 **obifunk** 6 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **GoldLeader** 1 year, 5 months ago

D. Trust DSCP. Question is not asking what markings will be applied but what will allow whatever marking there is to exist and be maintained throughout it's journey over both the wired and wireless infrastructure.

upvoted 3 times

 **yrzy** 1 year, 9 months ago

Selected Answer: A

If WLAN QoS is default (Silver), the class of service will be rewritten to Best Effort on the controller.

upvoted 1 times

 **kthekillerc** 3 years, 1 month ago

WMM is WiFi Multimedia Qos, the question was which feature provides for wireless and WIRED. Provided answer is correct and verified.

upvoted 4 times

 **santoshkotla** 2 years, 7 months ago

is D the answer?

upvoted 2 times

 **kthekillerc** 3 years, 2 months ago

Provided answer is correct

upvoted 2 times

 **Pawnstar** 3 years, 3 months ago

Answer should be C - Allow WMM.

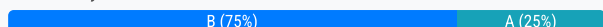
upvoted 3 times

A company is collecting the requirements for an on-premises event. During the event, a wireless client connected to a dedicated WLAN will run a video application that will need on average 391595179 bits per second to function properly. What is the QoS marking that needs to be applied to that WLAN?

- A. Platinum
- B. Gold
- C. Silver
- D. Bronze

Suggested Answer: B

Community vote distribution



rrahim 4 months, 1 week ago

Selected Answer: B

In Cisco Wireless QoS, different QoS profiles are used to prioritize traffic based on its requirements. The Gold QoS profile is recommended for video traffic, ensuring low latency and jitter while maintaining a good balance of network resources.

Why is Gold the Correct Choice?

The given bandwidth requirement is 391,595,179 bps (\approx 392 Mbps), which is typical for high-quality video applications.

Cisco QoS Profiles:

Platinum (Voice) – Highest priority, used for VoIP with very low latency.

Gold (Video) – Optimized for video applications, ensuring smooth playback and minimal buffering. ✓

Silver (Best Effort) – Default QoS, used for general web browsing and email.

Bronze (Background) – Lowest priority, used for non-critical data like bulk file transfers.

Since video streaming needs low latency but not as strict as voice, Gold QoS is the most appropriate choice.

upvoted 1 times

riktammenaars 8 months, 2 weeks ago

Selected Answer: B

From the official cisco study guide:

You will probably never use Gold unless you deploy a WLAN dedicated to video traffic.

upvoted 1 times

[Removed] 1 year, 5 months ago

Selected Answer: B

From the controller GUI itself.

Platinum (voice)

Gold (Video)

Silver (Best Effort)

Bronze (Background)

upvoted 2 times

GoldLeader 1 year, 11 months ago

Selected Answer: B

B. Gold, there is no bandwidth restriction on the default Gold profile.

upvoted 1 times

superwatermelon 2 years ago

Gold profile=Maximum DSCP Ceiling of 34. DSCP to WMM UP says Interactive Video DSCP=34, UP=5 and AC=Video AC_VI.

upvoted 1 times

JimDiGriz 2 years, 2 months ago

Selected Answer: A

To determine the appropriate QoS marking, we need to calculate the bandwidth required for the application in kilobits per second (kbps), and then map that value to the appropriate QoS class.

$391595179 \text{ bits per second} = 391595179 / 1000 \text{ kbps} = 391595.179 \text{ kbps}$

Based on Cisco's recommended QoS values, a bandwidth requirement of 391595.179 kbps corresponds to the Platinum QoS class. Therefore, the correct answer is A. Platinum.

upvoted 1 times

  **qqqqqqqqqq123** 2 years, 7 months ago

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/81831-qos-wlc-lap.html#:~:text=Gold/Video%E2%80%9494Supports%20high%2Dquality%20video%20applications.>

Gold is correct

upvoted 1 times

  **largestyle** 1 year, 6 months ago

This document is from 2008...

upvoted 1 times

  **kthekillerc** 3 years, 8 months ago

Provided answer is correct

upvoted 3 times

802.11a(5 GHz) > Media

Voice **Video** **Media**

Call Admission Control (CAC)

Admission Control (ACM) ☒ Enabled

CAC Method [4](#) Load Based ▾

Max RF Bandwidth (5-85) (%)

Reserved Roaming Bandwidth (0-25) (%)

Expedited bandwidth ☐

SIP CAC Support [3](#) ☐ Enabled

Per-Call SIP Bandwidth [2](#)

SIP Codec G.711 ▾

SIP Bandwidth (kbps)

SIP Voice Sample Interval (msecs)

Refer to the exhibit. Which two items must be supported on the VoWLAN phones to take full advantage of this WLAN configuration? (Choose two.)

- A. TSPEC
- B. SIFS
- C. 802.11e
- D. WMM
- E. APSD

Suggested Answer: CD

 **Sorvahr** Highly Voted 3 years, 8 months ago

Answer is correct
upvoted 5 times

 **most_ahdy** Most Recent 10 months, 1 week ago

The expedited bandwidth request feature enables CCXv5 clients to indicate the urgency of a WMM traffic specifications (TSPEC) request (for example, an e91 to the WLAN. When the controller receives this request, it attempts to facilitate the urgency of the call in any way possible without potentially altering the que other TSPEC calls that are in progress.

https://www.cisco.com/en/US/docs/wireless/controller/7.4/configuration/guides/system_management/config_system_management_chapter_010000.html

in the exhibit the Expedited bandwidth is not selected so TSPEC is not valid
upvoted 1 times

 **Citizenx** 2 years, 1 month ago

You must enable admission control (ACM) for CCXv4 clients that have WMM enabled.
The WMM standard is a subset of IEEE 802.11e.
C+D
upvoted 2 times

 **kthekillerc** 2 years, 8 months ago

Provided answer is correct
upvoted 1 times

 **friendsedu** 3 years, 3 months ago

I thing CD

The 802.11e, WMM, and Cisco Compatible Extension specifications help balance and prevent the overloading of a cell with audio streams. CAC determines whether there is enough channel capacity to start a call; if not, the phone can scan for another channel

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide/Chapter-9.html

upvoted 3 times

  **cisco_spo** 3 years, 6 months ago

I would argue TSPEC and 802.11e but it seems kind of redundant since TSPEC is defined in the 802.11e standard. That said WMM is not related to CAC and Power Save is not involved in the shown configuration and SIFS is definitely not a feature that needs to be supported. So going with Cisco's "the best answer" I'd say TSPEC and 802.11e.

upvoted 2 times

  **funkeymonkey** 3 years, 7 months ago

I would say the answer is A + D

upvoted 2 times

An engineer must use Cisco AVC on a Cisco WLC to prioritize Cisco IP cameras that use the wireless network. Which element do you configure in a rule?



- A. permit-ACL
- B. WMM required
- C. mark
- D. rate-limit

Suggested Answer: C

  **skh** Highly Voted 4 years, 4 months ago
ccorrect

AVC profile mapped to WLAN has a rule for MARK or DROP action.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/AVC_8point8_dg.html
upvoted 5 times

  **rrahim** Most Recent 4 months, 1 week ago
Selected Answer: C

To prioritize Cisco IP cameras using Cisco AVC (Application Visibility and Control) on a Cisco Wireless LAN Controller (WLC), the mark element is configured in a rule. Here's why:



Mark:

The mark action in an AVC rule allows you to apply a QoS marking (e.g., DSCP or UP) to the traffic that matches the rule. For Cisco IP cameras, you can create an AVC rule to identify the traffic and mark it with a high-priority QoS value (e.g., Platinum for video traffic). This ensures that the IP camera traffic is prioritized on the wireless network.

How it works:

AVC uses deep packet inspection (DPI) to identify specific applications or traffic types. Once the traffic is identified, the mark action applies the appropriate QoS marking to ensure proper prioritization.



upvoted 1 times

  **McMurphy** 7 months, 3 weeks ago
NBAR Supported Feature

NBAR as a feature can perform the following tasks:

1. Classification–Identification of Application/Protocol.
2. AVC–Provides visibility of classified traffic and also gives an option to control the same using Drop or Mark (DSCP) action.
3. NetFlow–Updating NBAR stats to NetFlow collector like Cisco Prime Assurance Manager (PAM).

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/AVC_8point8_dg.html
upvoted 1 times

  **kthekillerc** 3 years, 8 months ago
provided answer is correct
upvoted 2 times

An IT administrator is managing a wireless network in which most devices are Apple iOS. A QoS issue must be addressed on the WLANs. Which configuration must be performed?

- A. Enable Fastlane globally under Wireless > Access Points > Global Configuration.
- B. Create a new AVC Profile named AUTOQOS-AVC-PROFILE and apply to all WLANs.
- C. Enable Fastlane under each WLAN setting.
- D. Enable WMM TSPEC/TCLAS negotiation under Wireless > Advanced.



Suggested Answer: C

Reference:

https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/8-3/Optimizing_WiFi_Connectivity_and_Prioritizing_Business_Apps.pdf

Community vote distribution

A (100%)

  **masters777** 3 months, 1 week ago

Selected Answer: C

On 9800 Controller

tags/profiles->wlan->SSID->advanced tab->Fastlane

upvoted 1 times

  **rrahim** 4 months, 1 week ago

Selected Answer: C

For a wireless network with mostly Apple iOS devices, Fastlane is the recommended configuration to address QoS issues. Fastlane is a Cisco feature designed to optimize the performance of Apple devices on wireless networks by ensuring proper QoS handling. Here's why:

Fastlane:

Fastlane combines Wi-Fi Multimedia (WMM) and AVC (Application Visibility and Control) to prioritize traffic for Apple devices. It ensures that voice, video, and other real-time traffic from Apple devices receive the appropriate QoS treatment.

Configuration:

Fastlane must be enabled under each WLAN setting to ensure that the QoS policies are applied to the traffic on that WLAN. This ensures consistent performance for Apple iOS devices across the network.

Why not the other options?

A. Enable Fastlane globally under Wireless > Access Points > Global Configuration:

Fastlane is not enabled globally; it must be configured on a per-WLAN basis to ensure proper QoS handling for Apple devices.

upvoted 1 times

  **raphim** 8 months, 2 weeks ago



Selected Answer: A

You can only enable Fastlane per WLAN.

The Global Setting is just to reset Fastlane to its default parameters

--> Answer A

upvoted 1 times

  **TJR72** 1 year, 1 month ago



Selected Answer: A

Why enable each individual WLAN when you can enable it globally?

Enabling Fastlane globally under the WLC's Wireless > Access Points > Global Configuration settings allows Fastlane to be applied to all WLANs on the network.

While C is technically correct, the best answer is A.

upvoted 1 times



  **TJR72** 1 year, 1 month ago

Never mind, Fastlane can only be enabled on a per-WLAN basis,

https://www.cisco.com/c/dam/en/us/td/docs/wireless/access_point/9130ax/tech-notes/fastlane-faq.pdf

Correct answer is C

upvoted 6 times

  **Zatingke** 1 year, 5 months ago

Enable FT on WLAN automatically enable FT globally

upvoted 1 times

What is the Cisco recommended configuration for a Cisco switch port connected to an AP in local mode for optimal voice over WLAN performance with an 8821 wireless phone?

- A. switchport encapsulation dot1q switchport mode trunk mls qos trust device cisco-phone
- B. switchport mode access mls qos trust device cisco-phone
- C. switchport mode access mls qos trust cos
- D. switchport mode access mls qos trust dscp

Suggested Answer: C

Reference:

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/8821/english/Deployment/8821_wlandg.pdf

Community vote distribution

D (100%)

 **daeman**  2 years, 9 months ago

The question asks that the switch configuration should be for the AP not the WLC so...from the link provided:

Enable DSCP trust for Cisco Access Points

mls qos

!

interface X mls qos trust dscp

upvoted 8 times

 **rrahim**  4 months, 2 weeks ago


Selected Answer: C

C. switchport mode access mls qos trust cos

This configuration ensures that the switch port operates in access mode and trusts the Class of Service (CoS) values from the AP, which is critical for maintaining proper QoS for voice traffic.

D. switchport mode access mls qos trust dscp: While DSCP trust is important, CoS trust is specifically recommended for VoWLAN with Cisco 8821 phones.

upvoted 1 times

 **ForneyJR** 9 months, 4 weeks ago

Selected Answer: D

From the link provided, D is correct. On p. 40

Enable DSCP trust for Cisco Access Points

mls qos

interface X

mls qos trust dscp

upvoted 1 times

 **Vlad_Is_Love_ua** 1 year, 11 months ago

Selected Answer: D

Enable DSCP trust for Cisco Access Points

mls qos

!

interface X

mls qos trust dscp


upvoted 1 times

 **GoldLeader** 1 year, 11 months ago

Selected Answer: D

Answer D.

upvoted 1 times

 **SamGill** 2 years, 4 months ago

Selected Answer: D

For AP QoS on Switchport: DSCP is used
For Controller QoS on Switchport: CoS is used.
Because this asks for AP, the right answer is D
upvoted 3 times

🗲️ 👤 **itapase0314** 2 years, 5 months ago

Selected Answer: D

Cisco Cert guide says " DSCP is the preferred mothod of QoS trust"
upvoted 1 times

🗲️ 👤 **Axel315** 2 years, 6 months ago

Selected Answer: D

Enable DSCP trust for Cisco Access Points
upvoted 1 times

🗲️ 👤 **cvndani** 2 years, 9 months ago

Selected Answer: D

Answer D
upvoted 2 times

🗲️ 👤 **cvndani** 2 years, 9 months ago

Selected Answer: D

Answer D

Enable COS trust for Cisco Wireless LAN Controller
mls qos
!
interface X
mls qos trust cos
upvoted 2 times

🗲️ 👤 **junjunpatotoy** 2 years, 9 months ago

Answer D
upvoted 3 times

An engineer has configured Media Stream on the WLC and must guarantee at least 2 Mbps stream per user. Which RRC template should the engineer use?

- A. coarse
- B. medium
- C. low
- D. ordinary

Suggested Answer: B

Reference:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_0101010.html

Community vote distribution

B (100%)

 **rrahim** 4 months, 1 week ago

Selected Answer: B

When configuring Media Stream on a Cisco Wireless LAN Controller (WLC) to guarantee a minimum bandwidth of 2 Mbps per user, the medium RRC (Radio Resource Control) template should be used. Here's why:

RRC Templates:

RRC templates define how radio resources are allocated for Media Stream sessions. The medium template is designed to provide a balance between resource allocation and user capacity, making it suitable for guaranteeing a minimum of 2 Mbps per user.

Why Medium?:

The medium template ensures that sufficient bandwidth is reserved for Media Stream sessions while still allowing other users to access the network. It is the appropriate choice for applications requiring moderate bandwidth, such as video streaming.

upvoted 1 times

 **Vlad_Is_Love_ua** 7 months, 4 weeks ago

Selected Answer: B

From the Select from Predefined Templates drop-down list under Resource Reservation Control (RRC) Parameters, choose one of the following options to specify the details about the resource reservation control:

Very Coarse (below 300 kbps)

Coarse (below 500 kbps)


Ordinary (below 750 kbps)

Low (below 1 Mbps)

Medium (below 3 Mbps)

High (below 5 Mbps)

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_0101010.html#reference_6367D939CF0E4A0FBE224851D5
upvoted 3 times

 **Robesera** 1 year, 2 months ago

Provided answer is correct.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/configuration/guide/b_cg85/multicast_broadcast_setup.html#:~:text=From%20the%20Select%20from%20Predefined%20Templates%20drop%2Ddown%20list%20under%20
upvoted 2 times

Refer to the exhibit.

```
AL-CORE#show mls qos map cos-dscp
Cos-dscp map:
      cos:  1  2  3  4  5  6  7
      -----
      dscp:  8 16 24 32 45 48 56
```

Which COS to DSCP map must be modified to ensure that voice traffic is tagged correctly as it traverses the network?

- A. COS of 6 to DSCP 46
- B. COS of 3 to DSCP 26
- C. COS of 7 to DSCP 48
- D. COS of 5 to DSCP 46

Suggested Answer: D

Community vote distribution

D (100%)

 **Vlad_Is_Love_ua** 7 months, 3 weeks ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-7/config-guide/b_cg87/wireless_quality_of_service.html#qos-profiles
upvoted 3 times

 **Zatingke** 11 months, 2 weeks ago

45 looks weird
upvoted 1 times



Which QoS level is recommended for guest services?

- A. gold
- B. bronze
- C. platinum
- D. silver



Suggested Answer: B

Community vote distribution

D (100%)

  **tchase68w** Highly Voted 4 years, 6 months ago

According to the 300-430 Exam guide D is the correct answer
upvoted 6 times

  **Baio** 4 years, 6 months ago

but in the configuration guide of release 8.10 there is a different indication: Bronze/Background—Provides the lowest bandwidth for guest services.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/quality_of_service.html?bookSearch=true

upvoted 7 times

  **Pawnstar** Highly Voted 3 years, 9 months ago

The controller supports four QoS levels:

Platinum/Voice—Ensures a high quality of service for voice over wireless.

Gold/Video—Supports high-quality video applications.

Silver/Best Effort—Supports normal bandwidth for clients. This is the default setting.

Bronze/Background—Provides the lowest bandwidth for guest services.

Answer is B.

upvoted 5 times

  **Pawnstar** 3 years, 8 months ago

After reviewing the official cert guide I am now confused about what is the correct answer. According to the four precious metals information, it looks like Silver (Marking of 0) is used for Guest services.

I would now be inclined to go with answer D.

upvoted 2 times

  **John662266** Most Recent 3 weeks, 2 days ago

Selected Answer: B

The controller supports four QoS levels:

Platinum/Voice—Ensures a high quality of service for voice over wireless.

Gold/Video—Supports high-quality video applications.

Silver/Best Effort—Supports normal bandwidth for clients. ...

Bronze/Background—Provides the lowest bandwidth for guest services.

upvoted 1 times

  **derobert87** 7 months ago

Selected Answer: B

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/voice-over-wireless-lan-vowlan/116056-technote-qos-00.html#anc1>

I would go with Bronze for guests.

upvoted 2 times

🗄️ 👤 **Ocsicccnp** 11 months, 3 weeks ago

I think the provided answer is correct B

https://www.cisco.com/en/US/docs/wireless/controller/7.4/configuration/guides/system_management/config_system_management_chapter_01110.html#:

upvoted 1 times

🗄️ 👤 **Gumpy1** 1 year, 2 months ago

Selected Answer: D

Straight from Cisco on 9800 controller - silver/best effort https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-9/config-guide/b_wl_17_9_cg/m_wireless_qos_cg_vewlc1_from_17_3_1_onwards.html

upvoted 1 times

🗄️ 👤 **ahmie** 1 year, 7 months ago

Silver/Best Effort—Supports normal bandwidth for clients. This is the default setting. Bronze/Background—Provides the lowest bandwidth for guest services.

B is the correct answer

upvoted 1 times

🗄️ 👤 **itapase0314** 2 years, 5 months ago

Selected Answer: D

Current 300-430 cert guide says Silver is for "Hotspots/guest users".

upvoted 1 times

🗄️ 👤 **cvndani** 2 years, 9 months ago

I cursed for five days the 300-430 ENWLSI official course, in Ciso eReader (ENWLSI v1.1.22), page 51 says :

-Platinum (voice): Assures a high QoS for voice over wireless.

-Gold (video): Supports high-quality video applications.

-Silver (best effort): Supports normal bandwidth for clients.

-Bronze (background): Provides the lowest bandwidth for guest services.

upvoted 4 times

🗄️ 👤 **cvndani** 2 years, 9 months ago

Sorry, I did the course* :)

upvoted 1 times

🗄️ 👤 **cvndani** 2 years, 9 months ago

Bronze

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/quality_of_service.html

upvoted 1 times

🗄️ 👤 **Oscar14258** 3 years, 1 month ago

Selected Answer: D

According to the ENWLSI Guide D is the correct answer

upvoted 3 times

🗄️ 👤 **GameOver** 3 years, 4 months ago

QoS Profile Name Maximum DSCP Ceiling Use Case

Platinum 46 Most commonly used. Recommended

for most enterprise deployments.

Gold 34 Limited use.

Silver 0 Hotspots/guest

upvoted 3 times

🗄️ 👤 **kthekillerc** 3 years, 8 months ago

provided answer is correct

upvoted 1 times

🗄️ 👤 **Fenstar** 4 years, 2 months ago

not sure on this one the table in the book does state it should be D but the text following it states silver OR bronze. what Baio states is also true. So who knows. I would go for Silver since it's best effort and not scavenger

upvoted 1 times

🗄️ 👤 **skh** 4 years, 4 months ago

According to the 300-430 Exam guide D is the correct answer book Table 11-6 The Four QoS Profiles in AireOS Controllers Silver Hotspots/guest users.

upvoted 2 times

An engineer wants to configure WebEx to adjust the precedence and override the QoS profile on the WLAN. Which configuration is needed to complete this task?

- A. Change the WLAN reserved bandwidth for WebEx
- B. Create an AVC profile for WebEx
- C. Create an ACL for WebEx
- D. Change the AVC application WebEx-app-sharing to mark

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **GoldLeader** 11 months, 2 weeks ago

Selected Answer: B

There are four WebEx applications you can profile. "app-sharing, control, media, meeting" Therefore the best answer is B. Create a profile for WebEx to which you would add all 4 of these and set them to mark. Answer D. would only account for one of the 4.

upvoted 2 times

🗳️ 👤 **paFkoo** 2 years, 2 months ago

B, is correct, bcs. mark or drop are action (not profile) to be done over the AVC profile , and can not be profile by itself.

upvoted 1 times

🗳️ 👤 **Pawnstar** 2 years, 8 months ago

Provided answer is correct.

webex-app-sharing is for sharing traffic only (doesn't include webex-audio or webex-video) for streaming.

upvoted 2 times

🗳️ 👤 **kthekillerc** 2 years, 8 months ago

D is the correct answer, b is incomplete, the real answer for b should read as B) create the avc profile for webex marked with a lower dscp value. which wont achieve the solution the question asks for.

upvoted 4 times

🗳️ 👤 **Fortinet** 2 years, 10 months ago

B should be correct, creating a profile for webex is the solution

upvoted 2 times

🗳️ 👤 **iamccie** 3 years, 3 months ago

" D. Change the AVC application WebEx-app-sharing to mark" is the correct answer.

upvoted 3 times

🗳️ 👤 **skh** 3 years, 4 months ago

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7-5/AVC_dg7point5.html

upvoted 2 times

All APs are receiving multicast traffic, instead of only the APs that need it. What is the cause of this problem?

- A. The multicast group includes all APs
- B. The wrong multicast address was used
- C. The multicast group is assigned the wrong VLAN
- D. Multicast IGMP snooping is not enabled

Suggested Answer: D

🗨️ 👤 **rrahim** 4 months, 1 week ago

Selected Answer: D

When all APs are receiving multicast traffic instead of only the APs that need it, the issue is likely due to Multicast IGMP snooping not being enabled. Here's why:

IGMP Snooping:

IGMP (Internet Group Management Protocol) snooping is a feature that allows switches to listen to IGMP messages and forward multicast traffic only to the ports where it is needed. If IGMP snooping is not enabled, the switch will flood multicast traffic to all ports, including those connected to APs that do not need the traffic.

Why it's the cause:

Without IGMP snooping, the switch cannot determine which APs have clients interested in the multicast traffic. As a result, it sends the multicast traffic to all APs, causing unnecessary network congestion.

upvoted 1 times

🗨️ 👤 **rrahim** 4 months, 1 week ago

A. The multicast group includes all APs:

This is not a valid scenario because multicast groups are defined by IP addresses, not by APs. APs do not join multicast groups; clients do.

B. The wrong multicast address was used:

Using the wrong multicast address would result in the wrong clients receiving the traffic, but it would not cause all APs to receive the traffic.

C. The multicast group is assigned the wrong VLAN:

Assigning the multicast group to the wrong VLAN would prevent clients in the correct VLAN from receiving the traffic, but it would not cause all APs to receive the traffic.

upvoted 1 times

🗨️ 👤 **CiscoTester1** 1 year ago

Brothers, Answer is A, take a look below

"the controller snoops to learn which wirelessclients want to join which multicast groups on which APs. The multicast traffic will be forwardedto all APs over their CAPWAP tunnels via the CAPWAP multicast address. However, only theAPs hosting clients that are registered for the multicast group will transmit that traffic onto theWLAN. The other APs will not."

upvoted 1 times

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

When IGMP Snooping is enabled on the WLC, still all the APs will receive the multicast traffic:

The multicast traffic will be forwarded to all APs over their CAPWAP tunnels via the CAPWAP multicast address. However, only the APs hosting clients that are registered for the multicast group will transmit traffic onto the WLAN.

upvoted 3 times

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



Agree with iamccie

upvoted 1 times

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

provided answer is correct

upvoted 1 times

  **iamccie** 3 years, 9 months ago

Looks correct, when IGMP snooping is enabled, multicast traffic is sent only to the ports which sent IGMP joins. If IGMP snooping is disabled, then traffic is flooded to all the ports in that VLAN.

upvoted 4 times

What is the difference between PIM sparse mode and PIM dense mode?

- A. Sparse mode supports only one switch. Dense mode supports multiswitch networks.
- B. Sparse mode floods. Dense mode uses distribution trees.
- C. Sparse mode uses distribution trees. Dense mode floods.
- D. Sparse mode supports multiswitch networks. Dense mode supports only one switch.

Suggested Answer: C

Community vote distribution

C (100%)

🗲️ 👤 **Vlad_Is_Love_ua** 11 months, 3 weeks ago

Selected Answer: C

Sparse mode uses distribution trees. Dense mode floods.

upvoted 1 times

🗲️ 👤 **kthekillerc** 2 years, 8 months ago

provided answer is correct

upvoted 2 times

🗲️ 👤 **skh** 3 years, 4 months ago

Correct

In Dense mode packets are flooded to the entire network and then branches where there are no receivers are eliminated.

In Sparse mode packets branches distribution growth as new nodes join the multicast group.

<https://community.calix.com/s/article/Dense-Mode-Multicast-vs-Sparse-Mode-Multicast-1>

upvoted 4 times

🗲️ 👤 **Sorvahr** 3 years, 8 months ago

Answer is correct

upvoted 2 times

An engineer has been hired to implement a way for users to stream video content without having issues on the wireless network. To accomplish this goal, the engineer must set up a reliable way for a Media Stream to work between Cisco FlexConnect APs. Which feature must be enabled to guarantee delivery?



- A. Unicast Direct
- B. IGMP Direct
- C. Multicast Direct
- D. Multicast-to-Unicast Direct

Suggested Answer: C

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

Multicast Direct - Answer is C.

upvoted 13 times

  **Hugh_Jazz** Highly Voted 2 years ago

Correct answer should be C, the Multicast Direct feature. MD feature deals specifically with streams.

upvoted 6 times

  **Kyle9856** Most Recent 1 year, 3 months ago



Provided answer is correct

-By enabling 802.11n data rates and providing packet error correction, multicast-to-unicast capabilities of Cisco VideoStream enhance the reliability of delivering streaming video over Wi-Fi beyond best-effort features of traditional wireless networks.

[https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-](https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/VideoStream/b_Cisco_Unified_Wireless_Network_Solution_VideoStream_Deployment_Guide.html)

[1/VideoStream/b_Cisco_Unified_Wireless_Network_Solution_VideoStream_Deployment_Guide.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/VideoStream/b_Cisco_Unified_Wireless_Network_Solution_VideoStream_Deployment_Guide.html)

upvoted 2 times

  **Liselot** 11 months, 1 week ago

That is multicast-to-unicast mode.

Multicast-to-unicast Direct does not exist

upvoted 1 times

  **kthekillerc** 1 year, 8 months ago

Provided answer is correct

upvoted 1 times

  **kosminsmile** 1 year, 11 months ago

VideoStream

VideoStream provides efficient bandwidth utilization by removing the need to broadcast multicast packets to all WLANs on the AP regardless if there is a client joined to a multicast group. In order to get around this limitation, the AP has to send multicast traffic to the host using Unicast forwarding, only on the WLAN that the client is joined and at the data rate the client is joined at.

VideoStream can be enabled globally on the controller. The feature can also be enabled at the WLAN level, and provides more control to the administrator to identify specific video streams for Multicast Direct functionality.

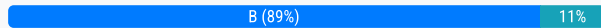
upvoted 4 times

A network engineer observes a spike in controller CPU overhead and overall network utilization after multicast is enabled on a controller with 500 APs. Which feature corrects the issue?

- A. controller IGMP snooping
- B. multicast AP multicast mode
- C. broadcast forwarding
- D. unicast AP multicast mode

Suggested Answer: B

Community vote distribution



Citizenx Highly Voted 2 years, 1 month ago

Selected Answer: B

With multicast-unicast, the wlc would have to make a copy for every packet before sending it to an AP. With lots of AP, that would give a nice spike in cpu.

By enabling multicast-multicast, now the wlc sends only 1 copy to a unique chosen multicast address and all APs joining that multicast address receive the packet.

upvoted 6 times

rrahim Most Recent 4 months, 1 week ago

Selected Answer: B

Unicast mode (D) sends individual copies of multicast packets to each AP.

This increases CPU load on the WLC, as it must handle 500 separate unicast transmissions instead of one efficient multicast stream.

Unicast is only useful when the network does not support multicast.

Key Takeaways:

- ✓ Multicast mode should be used if the network supports it, as it reduces CPU load and network overhead.
- ✓ Unicast mode should only be used if multicast is not supported on the network.
- ✓ Multicast AP Multicast Mode is the best choice in this scenario.

upvoted 1 times

DiegoECUIO 7 months, 3 weeks ago

Selected Answer: B

Multicast mode - In this mode, the controller sends multicast packets to a CAPWAP multicast group. This method reduces overhead on the controller processor and shifts the work of packet replication to your network, which is much more efficient than the unicast method.

When you use a different VLAN/Subnet for AP and WLC, Multicast routing is mandatory on the wired side to support forwarding the downlink CAPWAP Multicast packet from WLC to AP.

upvoted 1 times

Vlad_Is_Love_ua 1 year, 1 month ago

Selected Answer: B

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/81671-multicast-wlc-lap.html#anc4>

upvoted 1 times

JimDiGriz 1 year, 2 months ago

Selected Answer: D

D is a correct one

unicast AP multicast mode

To correct this issue, the engineer should enable the "Unicast AP Multicast Mode" feature. This feature allows multicast traffic to be converted to unicast traffic and forwarded only to the APs that have clients that are interested in the multicast stream, instead of flooding the multicast traffic to all APs. This helps to reduce network congestion and improve overall network performance.

Enabling "Multicast AP Multicast Mode" on the other hand, will cause the multicast traffic to be sent to all APs, increasing the network utilization and causing the controller CPU overhead to spike. This mode is not recommended in large wireless networks with many APs.

upvoted 1 times

🗨️ 👤 **Pawnstar** 2 years, 8 months ago

I take it back, the WLC should be configured for multicast-multicast mode. Provided answer is correct.
upvoted 2 times

🗨️ 👤 **kthekillerc** 2 years, 8 months ago

Correct answer should be D
upvoted 1 times

🗨️ 👤 **Pawnstar** 2 years, 9 months ago

answer is D.
upvoted 1 times

🗨️ 👤 **Fortinet** 2 years, 10 months ago

answer should be A
upvoted 1 times

🗨️ 👤 **Cyrillka** 2 years, 9 months ago

No B is correct

In Multicast-Unicast mode, each multicast packet is converted into a unicast packet and flooded to all the APs registered on that controller. Hence it is more CPU intensive and adds overhead on the controller.

upvoted 3 times

An engineer is configuring multicast for wireless for an all-company video meeting on a network using EIGRP and BGP within a single domain from a single source. Which type of multicast routing should be implemented?

- A. Protocol Independent Multicast Dense Mode
- B. Source Specific Multicast
- C. Multicast Source Discovery Protocol
- D. Protocol Independent Multicast Sparse Mode

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **s123** 9 months ago

Selected Answer: D

The question asks "type of routing" used, SSM consists of multiple protocols and uses PIM Sparse mode for routing

https://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_cfg_ssm.html

upvoted 1 times

🗳️ 👤 **Roomy** 10 months ago

The correct answer is B

upvoted 1 times

🗳️ 👤 **Citizenx** 2 years, 1 month ago

D is right.

Pim Sparse uses a distributed way to deliver multicast to the devices that asked for this traffic.

In Dense mode the multicast traffic will be flooded out to all devices in periodic time, causing lot of traffic overhead.

upvoted 2 times

🗳️ 👤 **kthekillerc** 2 years, 3 months ago

b is the correct answer

upvoted 1 times

🗳️ 👤 **Guglielmino** 2 years, 3 months ago

Why? It says "a single source", so we no need to use SSM...

upvoted 1 times

🗳️ 👤 **kthekillerc** 2 years, 6 months ago

Provided answer is correct

upvoted 1 times

🗳️ 👤 **powerslave666** 2 years, 6 months ago

B is answer correct

upvoted 1 times

🗳️ 👤 **Sorvahr** 3 years, 8 months ago

I think B is correct

PIM Source-Specific Multicast (PIM-SSM) builds trees that are rooted in just one source, offering a more secure and scalable model for a limited number of applications (mostly broadcasting of content). In SSM, an IP datagram is transmitted by a source S to an SSM destination address G, and receivers can receive this datagram by subscribing to channel (S,G). See informational RFC 3569.

upvoted 2 times

🗳️ 👤 **MoBenones** 3 years, 6 months ago

More info to support B is the answer:

<https://mrncciew.com/2012/12/28/multicast-deployment-types/>

upvoted 2 times

🗳️ 👤 **Robesera** 1 year, 8 months ago

SSM requires IGMP

[https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-2_2_e/multicast/configuration_guide/b_mc_1522e_3750x_3560x_cg/b_mc_3750x_3560x_chapter_010.html#:~:text=appropriate%20but%20requires,I(version%20%20support)



[2_2_e/multicast/configuration_guide/b_mc_1522e_3750x_3560x_cg/b_mc_3750x_3560x_chapter_010.html#:~:text=appropriate%20but%20requires,I\(version%20%20support](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-2_2_e/multicast/configuration_guide/b_mc_1522e_3750x_3560x_cg/b_mc_3750x_3560x_chapter_010.html#:~:text=appropriate%20but%20requires,I(version%20%20support)

upvoted 1 times

  **alexblue** 2 years ago

SSM is a type of PIM deployment. So answer is D

upvoted 1 times



  **Igur** 3 years, 7 months ago

seems to be the D is correct.

Protocol Independent Multicast–Sparse Mode (PIM–SM or PIM) is the routing protocol most suited to get multicast routing up and running within a single domain

<http://www.telfor.rs/telfor2002/radovi/2-19.pdf>

upvoted 5 times

  **Sorvahr** 3 years, 8 months ago

I think B is correct

upvoted 1 times

Which statement about the VideoStream/Multicast Direct feature is true?

- A. IP multicast traffic is reliable over WLAN by default as defined by the IEEE 802.11 wireless multicast delivery mechanism.
- B. Each VideoStream client acknowledges receiving a video IP multicast stream.
- C. It converts the unicast frame to a multicast frame over the air.
- D. It makes the delivery of the IP multicast stream less reliable over the air, but reliable over Ethernet.

Suggested Answer: B

Reference:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/configuration-guide/b_cg81/multicast_broadcast_setup.html



  **Sorvahr** 8 months, 2 weeks ago

Media Stream

The IEEE 802.11 wireless multicast delivery mechanism does not provide a reliable way to acknowledge lost or corrupted packets. As a result, if any multicast packet is lost in the air, it is not sent again which may cause an IP multicast stream unviewable.

The Media Stream (formerly VideoStream) feature makes the IP multicast stream delivery reliable over the air, by converting the multicast frame to a unicast frame over the air. Each Media Stream client acknowledges receiving a video IP multicast stream.

upvoted 4 times

  **Sorvahr** 8 months, 2 weeks ago

Answer is correct

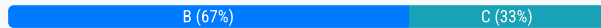
upvoted 3 times

Which configuration is applied to prevent the network from a Layer 2 flooding of multicast frames with a seamless transfer of multicast data to the client when roaming from one controller to another?

- A. Enable IGMPv3 on the central Layer 3 switch.
- B. Enable IGMP snooping on the WLC.
- C. Enable multicast mode on the WLC.
- D. Create multicast groups on the central Layer 3 switch.

Suggested Answer: B

Community vote distribution



🗳️ 👤 **[Removed]** 8 months, 2 weeks ago

Selected Answer: B

IGMP snooping is a Layer 2 protocol that prevents multicast flooding by forwarding multicast traffic only to those ports that have joined the multicast group. IGMP snooping can be enabled on wireless LAN controllers (WLCs) to prevent Layer 2 flooding of multicast frames when clients roam from one controller to another.

upvoted 1 times

🗳️ 👤 **Roomy** 10 months ago

Answer is C

upvoted 1 times

🗳️ 👤 **GoldLeader** 11 months, 2 weeks ago

Selected Answer: B

B. is correct. See link rph02533 provided in the section regarding IGMP enabled.

upvoted 1 times

🗳️ 👤 **JimDiGriz** 1 year, 2 months ago

Selected Answer: C

C. Enable multicast mode on the WLC.

to prevent the network from Layer 2 flooding of multicast frames and enable seamless transfer of multicast data to clients when roaming from one controller to another, the recommended configuration is to enable multicast mode on the WLC.

upvoted 1 times

🗳️ 👤 **rph02533** 1 year, 6 months ago

B is correct

https://www.cisco.com/en/US/docs/wireless/controller/7.4/configuration/guides/system_management/config_system_management_chapter_01011.html#:

upvoted 3 times

🗳️ 👤 **kthekillerc** 2 years, 7 months ago

Provided answer is correct

upvoted 3 times

An engineer is configuring multicast for two WLCs. The controllers are in different physical locations and each handles around 500 wireless clients. How should the CAPWAP multicast group address be assigned during configuration?

- A. Each WLC must be assigned a unique multicast group address.
- B. Each WLC management address must be in the same multicast group.
- C. Both WLCs must be assigned the same multicast group address.
- D. Each WLC management address must be in a different multicast group.

Suggested Answer: A

Community vote distribution

A (100%)

 **cskshiet** Highly Voted 3 years ago

I think it is A:

Choose Controller > General to configure AP multicast mode (multicast or unicast) & CAPWAP multicast group address(only for multicast mode). Use private multicast IP (239.0.0.0/8) for the group address, but avoid 239.0.0.x or 239.128.0.x as these overlap with the link local MAC addresses & flood out all switch ports. This group address cannot be used for any application in your network. If you have multiple controllers, configure different group address for different controllers.

<https://mrnciew.com/2012/11/17/configuring-multicast-on-wlc/>

upvoted 12 times

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

Selected Answer: A

When configuring multicast for two Wireless LAN Controllers (WLCs) in different physical locations, each WLC should be assigned a unique multicast group address. Here's why:

Unique Multicast Group Address:

Assigning a unique multicast group address to each WLC ensures that multicast traffic is localized to the specific WLC and its associated APs. This prevents unnecessary multicast traffic from being forwarded across the network to the other WLC, reducing network congestion and improving efficiency.

Why it's important:

If both WLCs use the same multicast group address, multicast traffic from one WLC could be forwarded to the other WLC's APs, even if those APs do not need the traffic. This would lead to inefficient use of network resources and increased overhead.

upvoted 1 times

 **kejvi** 10 months, 2 weeks ago

Selected Answer: A

yes, A

management address is UNICAST

upvoted 1 times

 **Vlad_Is_Love_ua** 11 months, 3 weeks ago

Selected Answer: A

You can use an address from the range 239.0.0.0 through 239.255.255.255, but avoid 239.0.0.x and 239.120.0.x. If you need to configure multiple controllers with multicast group addresses, make sure each one gets a unique address.

upvoted 2 times

 **Robesera** 1 year, 8 months ago

A seems right according to this.

<https://mrnciew.com/2012/11/17/configuring-multicast-on-wlc/#:~:text=If%20you%20have%20multiple%20controllers%2C%20configure%20different%20group%20address%20for%20different%20controllers.>

upvoted 2 times

🗨️ 👤 **alexblue** 2 years ago

It is also important that the multicast IP address be set to a different value on each WLC.

https://www.cisco.com/c/en/us/td/docs/wireless/technology/5760_deploy/CT5760_Controller_Deployment_Guide/Multicast_Configuration.pdf

upvoted 2 times

🗨️ 👤 **Citizenx** 2 years, 1 month ago

A should be right. WLC mngt address send 1 copy to an unique multicast address. You always need an unique addresses to avoid conflicts with other existing multicast addresses for example 224.0.0.13 All PIM Routers

upvoted 2 times

🗨️ 👤 **HOT2012** 2 years, 7 months ago

correct is A

upvoted 2 times

🗨️ 👤 **Pawnstar** 2 years, 8 months ago

The CAPWAP multicast group configured on the controllers should be different for different controllers.

upvoted 2 times

🗨️ 👤 **kthekillerc** 2 years, 8 months ago



Provided answer is correct

upvoted 2 times

A wireless network has been implemented to enable multicast video to be streamed reliably over the wireless link to the wireless users. After a client reports that the video is unable to stream, the administrator determines that the client is connecting at a data rate of 12 Mbps and is trying to stream to a valid multicast address on the network. Which two actions must be applied? (Choose two.)

- A. Turn off IGMP snooping for all the configured WLANs on the controller.
- B. Implement video-stream for the multicast video on the controller.
- C. Allow multicast-direct to work correctly and multicast-direct to be enabled globally.
- D. Change the WLAN QoS value to Bronze for the WLAN that multicast will be enabled.
- E. Allow RTSP to stream the video due to wireless multicast not using acknowledgements.

Suggested Answer: BC

  **rrahim** 4 months, 1 week ago

Selected Answer: BC

To resolve the issue of the client being unable to stream multicast video, the following actions must be taken:

B. Implement video-stream for the multicast video on the controller:

The video-stream feature on the Cisco Wireless LAN Controller (WLC) is specifically designed to optimize multicast video streaming. It ensures that multicast video traffic is handled efficiently and reliably over the wireless network.

C. Allow multicast-direct to work correctly and multicast-direct to be enabled globally:

Multicast-direct is a feature that converts multicast traffic into unicast traffic for clients connected to the AP. This ensures reliable delivery of multicast streams, as unicast traffic is acknowledged by the client, unlike multicast traffic, which is unacknowledged. Enabling multicast-direct globally ensures that all APs use this feature.

upvoted 2 times

  **kthekillerc** 1 year ago

Provided answer is correct

upvoted 4 times

Which two restrictions are in place with regards to configuring mDNS? (Choose two.)

- A. mDNS uses only UDP port 5436 as a destination port.
- B. mDNS cannot use UDP port 5353 as the destination port.
- C. mDNS is not supported on FlexConnect APs with a locally switched WLAN.
- D. Controller software must be newer than 7.0.6+.
- E. mDNS is not supported over IPv6.

Suggested Answer: CD

Community vote distribution

CE (100%)

 **shasxz**  3 years, 10 months ago

C E ARE CORRECT

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/multicast_broadcast_setup.html

Restrictions for Configuring Multicast DNS

mDNS over IPv6 is not supported.

mDNS snooping is not supported on access points in FlexConnect mode in a locally switched WLAN and mesh access points. For locally switched WLANs, all multicast traffic including mDNS is simply bridged between the local VLAN and the SSID.

upvoted 21 times

 **Profiteur** 3 years, 9 months ago


Agreed, we also have the first introduction on mDNS on the release 7.4; Support for the Multicast DNS (mDNS) protocol is introduced. Check older release if you need; <https://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn74.html>

upvoted 5 times

 **Sergey_1989**  4 years, 1 month ago

C and E

upvoted 8 times

 **Skliffi** 4 years, 1 month ago

mDNS use IPv6 as adressess, how it can not work with it

upvoted 5 times

 **rrahim**  4 months, 1 week ago

Selected Answer: CE

When configuring mDNS (Multicast DNS), the following restrictions apply:

C. mDNS is not supported on FlexConnect APs with a locally switched WLAN:

mDNS is not supported on FlexConnect APs when the WLAN is configured for local switching. This is because mDNS relies on centralized processing on the Wireless LAN Controller (WLC), and local switching bypasses the WLC.

E. mDNS is not supported over IPv6:

mDNS is designed to work with IPv4 and is not supported over IPv6. If the network uses IPv6, mDNS will not function.

upvoted 1 times


 **largestyle** 9 months ago

Cisco AireOS feature guide states mDNS first supported in 7.4.100, there is no reference to a version 7.0.6,

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/201007-AireOS-feature-list-per-release.html#toc-hld-408070459>.

IPv6 is now supported but this question may have been written years ago and no one's updated...

upvoted 1 times

 **ahmie** 1 year, 1 month ago

Bonjour protocol is an Apple service discovery protocol which locates devices and services on a local network with the use of multicast Domain Name System (mDNS) service records. The Bonjour protocol operates on service announcements and service queries. Each query or advertisement is sent

to the Bonjour multicast address ipv4 224.0.0.251 (ipv6 FF02::FB). This protocol uses mDNS on UDP port 5353.

<https://www.cisco.com/c/en/us/support/docs/wireless/wireless-lan-controller-software/210835-Troubleshooting-mDNS.html>

C & D are the best Answer

upvoted 1 times

🗲️ 👤 **Phuoc** 1 year, 6 months ago

C & D is correct.

mDNS gateway supports both IPv4 and IPv6 records and transports

<https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-3/deployment-guide/c9800-mDNS-technical-guide-rel-17-3.pdf>

upvoted 1 times

🗲️ 👤 **Tonymopar** 1 year, 7 months ago

C and E are better chooses

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-6/configuration-guide/b_cg76/b_cg76_chapter_01011.html

upvoted 1 times

🗲️ 👤 **Vlad_Is_Love_ua** 1 year, 7 months ago

Selected Answer: CE

Restrictions for Configuring Multicast DNS

mDNS over IPv6 is not supported.

mDNS snooping is not supported on access points in FlexConnect mode in a locally switched WLAN and mesh access points. For locally switched WLANs, all multicast traffic including mDNS is simply bridged between the local VLAN and the SSID.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-6/configuration-guide/b_cg76/b_cg76_chapter_01011.html

upvoted 1 times

🗲️ 👤 **largestyle** 1 year ago

As per the new 300-430 guide page 295 To configure an AireOS controller to participate in mDNS, navigate to CONTROLLER > mDNS > General and then check the box next to mDNS Global Snooping to enable it, as shown in Figure 12-16. For an IOS-XE controller, go to Configuration > Services > mDNS Gateway and select Transport. Then choose ipv4, ipv6, or both, and click Apply.

upvoted 1 times

🗲️ 👤 **Ahmed_Samy_Mohamed** 1 year, 8 months ago

Restrictions for Configuring Multicast DNS

mDNS over IPv6 is not supported.

upvoted 1 times

🗲️ 👤 **javierr50** 2 years, 1 month ago

Selected Answer: CE

C E

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-6/configuration-guide/b_cg76/b_cg76_chapter_01011.html

upvoted 2 times

🗲️ 👤 **Pawnstar** 3 years, 2 months ago

Answer is C and E.

Restrictions for Configuring Multicast DNS

mDNS over IPv6 is not supported.

mDNS snooping is not supported on access points in FlexConnect mode in a locally switched WLAN and mesh access points. For locally switched WLANs, all multicast traffic including mDNS is simply bridged between the local VLAN and the SSID.

upvoted 4 times

🗲️ 👤 **kthekillerc** 3 years, 2 months ago

Provided answer is correct

upvoted 1 times

🗲️ 👤 **Moomyao** 3 years, 11 months ago

C & D are correct

-IPv6 is supported (ruled out)

-mDNS use 5353 port (a & b are ruled out)

upvoted 3 times

A network engineer needs to configure multicast in the network. The implementation will use multiple multicast groups and PIM routers. Which address provides automatic discovery of the best RP for each multicast group?

- A. 224.0.0.13
- B. 224.0.0.14
- C. 224.0.1.39
- D. 224.0.1.40

Suggested Answer: D

Community vote distribution

D (50%)

A (50%)

🗳️ 👤 **Robesera** Highly Voted 1 year, 8 months ago

Correct.

[https://www.cisco.com/c/en/us/support/docs/ip/multicast/118405-config-rp-](https://www.cisco.com/c/en/us/support/docs/ip/multicast/118405-config-rp-00.html#:~:text=The%20RP%20Discovery%20Messages%20destined%20to%20224.0.1.40%20contain%20the%20best%20elected%20RP%2Dto%2Dgroup%20r)

00.html#:~:text=The%20RP%20Discovery%20Messages%20destined%20to%20224.0.1.40%20contain%20the%20best%20elected%20RP%2Dto%2Dgroup%20r
upvoted 6 times

🗳️ 👤 **rrahim** Most Recent 4 months, 2 weeks ago

Selected Answer: D

224.0.1.40 is the multicast group address used by Auto-RP (Automatic Rendezvous Point) to automatically discover and distribute RP information across the network. This simplifies the configuration of multicast networks with multiple multicast groups and PIM routers.

The other options are incorrect:

A. 224.0.0.13: This is used for PIMv2 Hello messages, not RP discovery.

B. 224.0.0.14: This is used for the RIP (Routing Information Protocol) version 2 multicast group.

C. 224.0.1.39: This is used for Cisco-RP-Announce messages in Auto-RP, but not for RP discovery itself.

upvoted 1 times

🗳️ 👤 **Far3** 5 months, 2 weeks ago

Selected Answer: D

Auto discovery so D is the correct one.

upvoted 1 times

🗳️ 👤 **Markus_Kruber** 10 months, 1 week ago

Selected Answer: D

According to https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xr-16-5/imc-pim-xr-16-5-book/imc-basic-cfg.html D and C should be correct

upvoted 1 times

🗳️ 👤 **AhcMez** 11 months, 1 week ago

Auto discovery so D is the correct one.

upvoted 1 times

🗳️ 👤 **TJR72** 1 year, 2 months ago

Selected Answer: A

The address that provides automatic discovery of the best RP (Rendezvous Point) for multiple multicast groups is the "Bootstrap Router (BSR)" address. The BSR address is a reserved multicast address (224.0.0.13) used by routers to exchange information about candidate RPs and multicast group-to-RP mappings in a multicast-enabled network

upvoted 1 times

A shopping center uses AireOS controllers with Cisco Wave 2 APs. A separate WLAN named Guest-012345678-WLAN is used for guest wireless clients.

Management needs location analytics to determine popular areas. CMX must track only associated clients. What must be selected on the CMX server settings?

- A. Exclude probing clients
- B. Duty Cycle Cutoff
- C. Enable Locally Administered MAC Filtering
- D. Enable Location MAC Filtering


Suggested Answer: A

Reference:

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_config/b_cg_cmx106/the_cisco_cmx_detect_and_locate_service.html#id_123333

Community vote distribution

A (100%)

 **rrahim** 4 months, 1 week ago

Selected Answer: A

To ensure that Cisco CMX (Connected Mobile Experiences) tracks only associated clients and not probing clients, the Exclude probing clients option must be selected on the CMX server settings. Here's why:

Exclude probing clients:

This setting ensures that CMX only tracks clients that are fully associated with the wireless network. Probing clients are devices that are scanning for available networks but are not yet connected. By excluding probing clients, CMX focuses on gathering location analytics for active users, providing more accurate data about popular areas in the shopping center.

upvoted 2 times

 **Vlad_Is_Love_ua** 11 months, 3 weeks ago

Selected Answer: A

. You can also ignore the non-associated clients by selecting Exclude Probing Only Clients.

upvoted 1 times

 **Tonymopar** 1 year ago

Answer could be B?

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_config/b_cg_cmx106/the_cisco_cmx_detect_and_locate_service.html#id_123333:~:text=From%20Cisco%20CMX,%3E%20Tracking%20window.

upvoted 1 times

 **Zatingke** 1 year, 5 months ago

Probing clients are not associated

upvoted 1 times

A wireless engineer needs to implement client tracking. Which method does the angle of arrival use to determine the location of a wireless device?

- A. received signal strength
- B. triangulation
- C. time distance of arrival
- D. angle of incidence

Suggested Answer: D

Reference:

<https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/WiFiLBS-DG/wifich2.html>

Community vote distribution

D (100%)

🗳️ 👤 **rrahim** 4 months, 1 week ago

Selected Answer: D

The angle of arrival (AoA) method determines the location of a wireless device based on the angle of incidence of the signal arriving at the access points (APs). Here's how it works:

Angle of Incidence:

The AoA method calculates the direction from which a client device's signal is received by measuring the angle at which the signal arrives at multiple APs. By combining the angles from at least two APs, the location of the client device can be determined using triangulation.

How it works:

Each AP measures the angle at which the client's signal is received. These angles are then used to calculate the intersection point, which represents the client's location.

upvoted 1 times

🗳️ 👤 **Vlad_Is_Love_ua** 11 months, 3 weeks ago

Selected Answer: D

D. angle of incidence

upvoted 1 times

🗳️ 👤 **kthekillerc** 2 years, 7 months ago

Provided answer is correct

upvoted 2 times

🗳️ 👤 **Pawnstar** 2 years, 8 months ago

Scratch my previous comment, D is the right answer according to Cisco - not wiki.

Angle of Arrival (AoA)

The Angle of Arrival (AoA) technique, sometimes referred to as Direction of Arrival (DoA), locates the mobile station by determining the angle of incidence at which signals arrive at the receiving sensor. Geometric relationships can then be used to estimate location from the intersection of two lines of bearing (LoBs) formed by a radial line to each receiving sensor, as illustrated in Figure 2-5. In a two-dimensional plane, at least two receiving sensors are required for location estimation with improved accuracy coming from at least three or more receiving sensors (triangulation).

upvoted 3 times

🗳️ 👤 **Pawnstar** 2 years, 8 months ago

I think the correct answer should be C.

https://en.m.wikipedia.org/wiki/Angle_of_arrival

upvoted 1 times

Which two steps are needed to complete integration of the MSE to Cisco Prime Infrastructure to track the location of clients/rogues on maps? (Choose two.)

- A. Synchronize access points with the MSE.
- B. Add the MSE to Cisco Prime Infrastructure using the CLI credentials.
- C. Add the MSE to Cisco Prime Infrastructure using the Cisco Prime Infrastructure communication credentials.
- D. Apply a valid license for Wireless Intrusion Prevention System.
- E. Apply a valid license for location tracking.

Suggested Answer: DE

Community vote distribution

BD (50%)

AC (50%)

 **daeman** Highly Voted 2 years, 9 months ago

C and E should be the answer.

[https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide_chapter_0100110.html#task_1153829)

[7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide_chapter_0100110.html#task_1153829](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide_chapter_0100110.html#task_1153829)

communication username configured for MSE.

[https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide_chapter_0100110.html#task_1153829)

[7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide_chapter_0100110.html#task_1153829](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide_chapter_0100110.html#task_1153829)

Licensing for Clients and Tags

You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points.

•Licenses for tags and clients are offered separately. (The clients license also includes tracking of rogue clients, rogue access points and wired clients).

upvoted 9 times

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

Selected Answer: CE

To successfully integrate Cisco Mobility Services Engine (MSE) with Cisco Prime Infrastructure (PI) for tracking client and rogue devices on maps, the following steps are required:

1. Adding the MSE to Cisco Prime Infrastructure

You need to use the correct Cisco Prime Infrastructure communication credentials to establish the connection.


(Option C is correct) because these credentials enable MSE and Prime to communicate properly.

2. Applying a Location Tracking License

MSE requires a valid location tracking license to provide client and rogue tracking functionality.

(Option E is correct) because without this license, MSE cannot track clients on maps in Prime Infrastructure.

upvoted 1 times

 **rrahim** 4 months, 1 week ago

Why Not the Other Options?

✗ A. Synchronize access points with the MSE

Not required for MSE integration; APs are already synced with the WLC, which provides data to MSE.

✗ B. Add the MSE to Cisco Prime Infrastructure using the CLI credentials

CLI credentials are not used for integration. PI needs the communication credentials instead.

✗ D. Apply a valid license for Wireless Intrusion Prevention System (WIPS)

WIPS is not required for location tracking. It is needed for wireless security monitoring, not client/rogue tracking.

upvoted 1 times

🗲️ 👤 **Far3** 5 months, 2 weeks ago

Selected Answer: CE

To integrate a Mobility Services Engine (MSE) with Cisco Prime Infrastructure for location tracking of clients and rogues, the following steps are critical:

Add the MSE to Cisco Prime Infrastructure using the communication credentials:

MSE needs to be added to Cisco Prime Infrastructure using the communication credentials configured on the MSE. This step establishes a connection between the two systems, enabling data exchange for location tracking.

Apply a valid license for location tracking:

A valid license for location services must be applied to the MSE to enable tracking of clients and rogues on maps in Cisco Prime Infrastructure. Without this license, location tracking features will not function.

upvoted 1 times

🗲️ 👤 **meromu7** 7 months, 1 week ago

Selected Answer: CE

C and E should be the answer

upvoted 1 times

🗲️ 👤 **Le91** 8 months ago

Selected Answer: CE

C and E should be the answer

upvoted 1 times

🗲️ 👤 **riktammenaars** 8 months, 1 week ago

Selected Answer: BE

"You also need to add the CMX from the Services > Mobility Services > Mobility Services Engines page, using the CMX IP address and the cmxadmin credentials. As mentioned earlier, Mobility Services Engine (MSE) used to be the name of the physical (or virtual) appliance on which the CMX services were deployed, and Cisco Prime Infrastructure still uses this name to refer to the CMX appliance."

upvoted 1 times

🗲️ 👤 **Seba_o_s** 1 year, 7 months ago

Selected Answer: BD

B and D

This link also mark A and D but in the explanation he makes option B and D very clear.

<https://www.exam-answer.com/stolen-laptop-location-wireless-settings>

upvoted 1 times

🗲️ 👤 **ahmie** 1 year, 7 months ago

Selected Answer: AC

I think A and C

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 8 months ago

C. Add the MSE to Cisco Prime Infrastructure using the Cisco Prime Infrastructure communication credentials.

E. Apply a valid license for location tracking.

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 8 months ago

The two steps that are needed to complete integration of the MSE to Cisco Prime Infrastructure to track the location of clients/rogues on maps are:

Add the MSE to Cisco Prime Infrastructure.

Apply a valid license for location tracking.

Therefore, the correct answers are B and E.

upvoted 1 times

🗲️ 👤 **cvndani** 2 years, 9 months ago

I think C and D

upvoted 1 times

An IT department receives a report of a stolen laptop and has information on the MAC address of the laptop. Which two settings must be set on the wireless infrastructure to determine its location? (Choose two.)

- A. Location History for Clients must be enabled on the MSE.
- B. Client location tracking must be enabled on the MSE.
- C. Location History for Visitors must be enabled on the MSE.
- D. Location History for Rogue APs & Rogue Clients must be enabled on the MSE.
- E. Tracking optimization must be enabled on the WLC.



Suggested Answer: AE

Community vote distribution

BE (50%)

AB (25%)

BD (25%)

  **rrahim** 4 months, 1 week ago

Selected Answer: AB

To determine the location of a stolen laptop using its MAC address, the following settings must be configured on the Mobility Services Engine (MSE):



A. Location History for Clients must be enabled on the MSE:

Enabling location history allows the MSE to store historical location data for clients. This is necessary to track the past locations of the stolen laptop.

B. Client location tracking must be enabled on the MSE:

Client location tracking must be enabled to allow the MSE to calculate and report the real-time and historical locations of wireless clients, including the stolen laptop.

upvoted 2 times

  **Gumpy1** 8 months, 3 weeks ago

Selected Answer: AB

A: Location History so you could see where they were

B: Client location tracking to see current

C: no, on Cisco instructions on setting this up, there isn't a "visitor" tracking option. Client tracking is for all clients

D: no, this is not a Rogue AP or Rogue client, appears to be employee or client (could be visitor)

E: no, tracking optimization is for RFID tags, and this laptop does not have an RFID tag

upvoted 1 times

  **Gumpy1** 8 months, 3 weeks ago

A & B

A-Location History for Clients - where it was

B-Client location tracking - for current tracking

Not C - it isn't a visitor, but even if it was it was still a client, it isn't listed as visitor location history in docs that I saw

Not D - this is not a Rogue AP or Rogue Client - it was an employee laptop

Not E - Tracking Optimization is for RFID tags - not laptops, laptops do not have RFID tags in them

Configuring MSE Tracking and History Parameters

[https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide_chapter_0100110.html#task_1153829)

[7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide_chapter_0100110.html#task_1153829](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide_chapter_0100110.html#task_1153829)

upvoted 1 times

  **Seba_o_s** 1 year, 1 month ago

Selected Answer: BD

B and D

This link also mark A and D but in the explanation he makes option B and D very clear.

<https://www.exam-answer.com/stolen-laptop-location-wireless-settings>

upvoted 1 times

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

- B. Client location tracking must be enabled on the MSE.
- D. Location History for Rogue APs & Rogue Clients must be enabled on the MSE.

The other options are not required to track the location of a stolen laptop:

- A. Location History for Clients is more commonly used for tracking the location history of wireless clients over time.
- C. Location History for Visitors is used to track the location of visitors to the network.
- E. Tracking optimization is not required for tracking the location of a stolen laptop.

upvoted 1 times

  **JimDiGriz** 1 year, 8 months ago

Selected Answer: BE

B. Client location tracking must be enabled on the MSE: This setting is necessary to track the location of the clients, including the stolen laptop, on the maps.

E. Tracking optimization must be enabled on the WLC: This setting ensures that the WLC optimizes the tracking process by sending only relevant information to the MSE, reducing network traffic.

upvoted 2 times

  **PauBau** 1 year, 8 months ago



I would go for A and B. You would see where a client currently is or where it has been seen last which would be relevant if it is now switched off but you still want to locate it.

C: as we could assume it is for a corporate client

D: , same as C

E: Tracking optimization is just for channels 1,6,11 on 2.4 GHz, so for 5GHz



upvoted 2 times

  **Liselot** 2 years, 5 months ago

To optimize the monitoring and location calculation of RFID tags, you can enable tracking optimization on up to four channels within the 2.4-GHz band of an 802.11b/g/n access point which tags are usually programmed to operate (such as channels 1, 6, and 11).



This won't help if the laptop is on 5 GHz

upvoted 1 times

  **Liselot** 2 years, 5 months ago

I would go for A & B, but not sure...

upvoted 2 times

  **rph02533** 2 years ago

A & B seems correct

To generate report and investigate further both - history and tracking parameters have to be configured prior the incident

https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/MSE_CMx/8_0_MSE_CAS/configuring_mse___system_settings_and_services.html

https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/MSE_CMx/8_0_MSE_CAS/monitoring_the_system_and___services.html#:~:text=client%20report%20results,Client%20Location,historical%20location

Note

upvoted 1 times

  **alexblue** 2 years, 6 months ago

We need to assume that "our" laptop was ON at the time it was stolen :-)

upvoted 1 times

  **Citizenx** 2 years, 7 months ago

A en E correct.

A- You want to see where in time your laptop has been seen on the map. (history view)

E- scanning only the channels you're using in your deployment gives you more precise location points on the map to see in time where your laptop is been seen.

upvoted 1 times

  **Kyle9856** 2 years, 9 months ago

With it being a stolen laptop, you want to know where both visitors and clients are, so with that logic, would it not be A and B so that you know where the locations of all that are on site area?

upvoted 1 times

🗨️ 👤 **kthekillerc** 2 years, 9 months ago

correction B and E typo sorry

upvoted 3 times

🗨️ 👤 **kthekillerc** 2 years, 10 months ago

Appears the correct answer should be A and C. Thoughts?

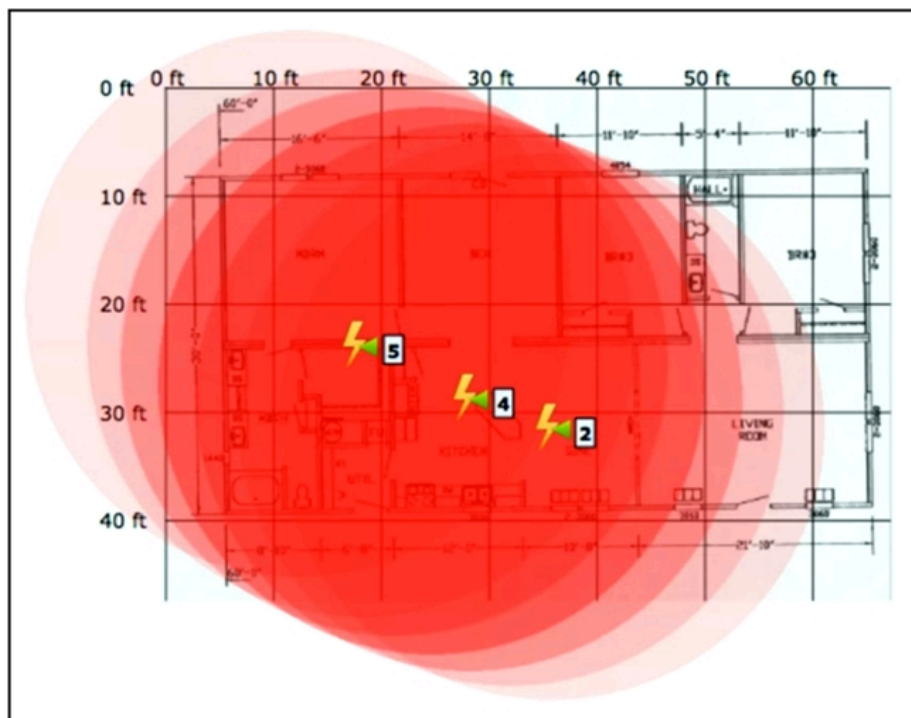
upvoted 1 times

🗨️ 👤 **JimDiGriz** 1 year, 8 months ago

Option A, Location History for Clients, is not directly related to determining the real-time location of a specific client, but it allows the IT department to view the location history of all clients.

Option C, Location History for Visitors, is used to track the location history of guests and not specific clients like the stolen laptop.

upvoted 1 times



Refer to the exhibit. An engineer needs to manage non-802.11 interference. What is observed in the output on PI?

- A. At least one strong interferer is impacting connectivity at this site.
- B. Several light interferers are collectively impacting connectivity at this site.
- C. The three individual clusters shown indicate poor AP placement.
- D. RF at this site is unable to provide adequate wireless performance.

Suggested Answer: C

Community vote distribution

B (100%)

GoldLeader 11 months, 2 weeks ago

Selected Answer: B

I'm going with B on this one.

upvoted 1 times

daeman 1 year, 9 months ago

Selected Answer: B

Although A is a possible answer, B is the best choice.

[https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide_chapter_01001.html)

[7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide_chapter_01001.html](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide_chapter_01001.html)

Show Zone of Impact—Displays the approximate interference impact area. The opacity of the circle denotes its severity. A solid red circle represents a very strong interferer that likely disrupts Wi-Fi communications, a light pink circle represents a weak interferer.

We can see an area where the circles overlap and create what is close to a solid red circle, however the fact that each lightning bolt has a number greater than 1 this makes B the best choice as they seem to want to put emphasis on the number of interferers rather than the severity.

upvoted 3 times

Citizenx 2 years, 1 month ago

I think B.

You see several light layers making a big red one in the middle combined, but if you check all the outer circles you see the same opacity upper left AP and lower right AP indicating low impact in color opacity.

upvoted 3 times

🗨️ 👤 **Mimimimi** 2 years, 6 months ago

Answer is B.

Lightning bolts display an RF interferer source.

The opacity of the circle displays the severity. If several light interferers overlap, the circles opacity becomes 'dark'. Look at the outlines of the circles, there are 5 light interferers and only 3 have been identified as uniques.

upvoted 3 times

🗨️ 👤 **kthekillerc** 2 years, 6 months ago

correction I believe the answer is B several light interferers

upvoted 2 times

🗨️ 👤 **andit** 2 years, 7 months ago

I am also for A or B. The lightning symbol stands for interferer. If its one strong or many weak its hard to say. But probably rather the many weak ones.

upvoted 3 times

🗨️ 👤 **kthekillerc** 2 years, 8 months ago

provided answer is correct

upvoted 1 times

🗨️ 👤 **Fortinet** 2 years, 10 months ago

It should be A, that lightning symbol represents interferences on PI

upvoted 1 times

After looking in the logs, an engineer notices that RRM keeps changing the channels for non-IEEE 802.11 interferers. After surveying the area, it has been decided that RRM should not change the channel. Which feature must be enabled to ignore non-802.11 interference?

- A. Avoid Cisco AP Load
- B. Avoid Non-802.11 Noise
- C. Avoid Persistent Non-WiFi Interference
- D. Avoid Foreign AP Interference

Suggested Answer: C

🗨️ **Cyrillka** Highly Voted 1 year, 9 months ago

Should be C correct

Check the Avoid Non-802.11a (802.11b) Noise check box to cause the controller's RRM algorithms to consider noise (non-802.11 traffic) in the channel when assigning channels to lightweight access points, or uncheck it to disable this feature. For example, RRM may have access points avoid channels with significant interference from nonaccess point sources, such as microwave ovens. The default value is selected.

Check the Avoid Persistent Non-WiFi Interference check box to configure the controller to stop ignoring persistent non-Wi-Fi interference in new channel calculation. The persistent non-Wi-Fi interference is considered during the metric calculation for channels.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-6/config-guide/b_cg86/radio_resource_management.html

upvoted 5 times

🗨️ **rrahim** Most Recent 4 months, 1 week ago

Selected Answer: C

To prevent Radio Resource Management (RRM) from changing channels due to non-802.11 interference, the Avoid Persistent Non-WiFi Interference feature must be enabled. Here's why:

Avoid Persistent Non-WiFi Interference:

This feature allows RRM to ignore non-802.11 interference (e.g., from microwaves, cordless phones, or Bluetooth devices) when making channel decisions. It ensures that RRM does not unnecessarily change channels in response to transient or persistent non-WiFi interference.

Why it's the solution:

If RRM keeps changing channels due to non-802.11 interference, it can disrupt network performance. Enabling this feature ensures that RRM focuses on optimizing channels based on WiFi-related factors rather than non-WiFi interference.

upvoted 1 times

🗨️ **twoplanker** 7 months ago

I actually got this question on my last exam verbatim and yes, the question is written incorrectly. It should be "disable" but either way, C is correct.

upvoted 2 times

🗨️ **alexblue** 1 year ago

the question is wrong...should be "disable", not "to enable"

We dont want to change channel due to interferences

upvoted 2 times

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

provided answer is correct https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/configure-guide/b_wi_16_10_cg/radio-resource-management.html

upvoted 1 times

🗨️ **anonymonkey** 1 year, 3 months ago

kthekillerc is correct but can be seen with the working link from Cyrillka.

upvoted 2 times

🗨️ **anonymonkey** 1 year, 3 months ago

ugh, it's actually unchecking this and checking C...tricky

<https://community.cisco.com/t5/wireless/non-wifi-interference/td-p/2444494>

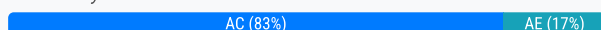
upvoted 4 times

Which two protocols are used to communicate between the Cisco MSE and the Cisco Prime Infrastructure network management software?
(Choose two.)

- A. HTTPS
- B. Telnet
- C. SOAP
- D. SSH
- E. NMSP

Suggested Answer: AE

Community vote distribution



Skliffi Highly Voted 4 years, 1 month ago
A&C

<https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/113344-cuwn-ppm.html#anc5>
upvoted 11 times

Sorvahr Highly Voted 4 years, 2 months ago
Correct answers are A & C
upvoted 8 times

MoBenones 4 years ago
Some extra info:
<https://mrncciew.files.wordpress.com/2014/09/nmsp-02.png>
upvoted 5 times

rrahim Most Recent 4 months, 1 week ago
Selected Answer: AC

The primary protocol for MSE management communication with Cisco Prime Infrastructure (or WCS/NCS) is SOAP/XML over HTTPS (TCP port 443). This is separate from NMSP (Network Mobility Services Protocol), which is used for real-time location tracking and other mobility services.
upvoted 1 times

robi1020 11 months ago
Selected Answer: AE

The two protocols used to communicate between the Cisco Mobility Services Engine (MSE) and the Cisco Prime Infrastructure network management software are:

- A. HTTPS
- E. NMSP (Network Mobility Service Protocol)

These protocols ensure secure and efficient communication between the MSE and Cisco Prime Infrastructure for managing the wireless network infrastructure.
upvoted 1 times

DiegoECUIO 1 year, 1 month ago
Selected Answer: AE
A&E are the right answer
upvoted 1 times

[Removed] 1 year, 2 months ago
HTTPS is used for secure communication between the MSE and Cisco Prime Infrastructure. NMSP is a Cisco-proprietary protocol that is used for managing wireless networks.

The other answer choices are not used for communication between the MSE and Cisco Prime Infrastructure:

Telnet is an insecure protocol that is not recommended for use in production environments.
SSH is a secure protocol that is used for remote access to devices.
SOAP is a web services protocol that is used for exchanging messages between applications.

upvoted 1 times

🗨️ 👤 **DiegoECUIO** 1 year, 1 month ago

NMSP is not SNMP, NMSP means Network Mobility Service Protocol and this protocolo is not used for management, is used for client information to the location engine MSE

upvoted 1 times

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

I checked on google bard and pasted above link. Google ai also said a&c.

upvoted 1 times

🗨️ 👤 **Heddy** 1 year, 5 months ago

<http://www.netprojnetworks.com/ccie-enterprise-wireless-v1-0-mobility-services-engine/>

upvoted 1 times

🗨️ 👤 **Heddy** 1 year, 5 months ago

that means A & C

upvoted 1 times

🗨️ 👤 **Vlad_Is_Love_ua** 1 year, 7 months ago

Selected Answer: AC

Choose one of the following transport types from the Transport Type drop-down list:

SOAP—Simple Object Access Protocol. Use SOAP to send notifications over HTTP/HTTPS and to be processed by web services on the destination. Specify whether to send notifications over HTTPS by selecting its corresponding check box. Enter the destination port number in the Port Number text box.

[https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-3/user/guide/bk_CiscoPrimeInfrastructure_3_3_0_UserGuide/bk_CiscoPrimeInfrastructure_3_3_0_UserGuide_chapter_0100110.html)

[3/user/guide/bk_CiscoPrimeInfrastructure_3_3_0_UserGuide/bk_CiscoPrimeInfrastructure_3_3_0_UserGuide_chapter_0100110.html](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-3/user/guide/bk_CiscoPrimeInfrastructure_3_3_0_UserGuide/bk_CiscoPrimeInfrastructure_3_3_0_UserGuide_chapter_0100110.html)

upvoted 2 times

🗨️ 👤 **Oscar14258** 2 years, 7 months ago

Selected Answer: AC

A&C are corrects

upvoted 4 times

🗨️ 👤 **kthekillerc** 2 years, 9 months ago

correct answer is a and c

upvoted 3 times

🗨️ 👤 **malkana** 2 years, 10 months ago

Selected Answer: AC

NMSP is used for communication between MSE and Controller not Prime.

upvoted 4 times

🗨️ 👤 **kthekillerc** 3 years, 1 month ago

Cisco Network Mobility Services Protocol (NMSP) is a secure two-way protocol that can be run over a connection-oriented (TLS) or HTTPS transport. The wireless infrastructure runs the NMSP server and Cisco Connected Mobile Experiences (Cisco CMX) acts as an NMSP client. Provided answer is correct.

upvoted 2 times

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

A&C correct.

upvoted 3 times

🗨️ 👤 **Ansar88** 3 years, 10 months ago

A&E Correct

[https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-3/user/guide/bk_CiscoPrimeInfrastructure_3_3_0_UserGuide/bk_CiscoPrimeInfrastructure_3_3_0_UserGuide_chapter_0100110.html)

[3/user/guide/bk_CiscoPrimeInfrastructure_3_3_0_UserGuide/bk_CiscoPrimeInfrastructure_3_3_0_UserGuide_chapter_0100110.html](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-3/user/guide/bk_CiscoPrimeInfrastructure_3_3_0_UserGuide/bk_CiscoPrimeInfrastructure_3_3_0_UserGuide_chapter_0100110.html)

upvoted 3 times

🗨️ 👤 **powerslave666** 3 years, 6 months ago

NMSP is for synchronize MSE and WLC.

A & C Correct

upvoted 2 times

  **powerslave666** 3 years ago

<https://mrncciew.files.wordpress.com/2014/09/nmsp-02.png>

See, A&C correct Answers

upvoted 3 times



An engineer must configure MSE to provide guests access using social media authentication. Which service does the engineer configure so that guests use Facebook credentials to authenticate?

- A. Social Connect
- B. Client Connect
- C. Visitor Connect
- D. Guest Connect

Suggested Answer: A


Community vote distribution

C (100%)

 **kthekillerc**  2 years, 10 months ago


Correction the answer is C, also another question on the exam that is not in this dump is what is the Facebook url redirect port and it is `http://mse>8084/fbwifi/forward`.

upvoted 9 times

 **Liselot** 2 years, 5 months ago

Thanks killer

upvoted 1 times



 **Coffee313**  3 years, 3 months ago

C is correct

[https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-](https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/CMX_Connect_Engage_Visitor_Connect/Guide/Cisco_CMX_Connect_Engage_Config_Guide_VC/Overview.html)

[0/CMX_Connect_Engage_Visitor_Connect/Guide/Cisco_CMX_Connect_Engage_Config_Guide_VC/Overview.html](https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/CMX_Connect_Engage_Visitor_Connect/Guide/Cisco_CMX_Connect_Engage_Config_Guide_VC/Overview.html)

upvoted 8 times

 **rrahim**  4 months, 1 week ago

Selected Answer: C

Visitor Connect:

This feature is part of the Cisco CMX Connect and Engage solution and provides a customizable guest access portal. It supports social authentication plug-ins (e.g., Facebook, LinkedIn, Google+) for guest onboarding, making it the correct choice for enabling social media authentication.

How it works:


Visitor Connect integrates with the MSE, WLC, and lightweight APs to provide a seamless guest access experience. Guests can log in using their social media accounts, and the system handles the authentication process.

Why not the other options?

A. Social Connect:

While this might sound like the correct option, the documentation confirms that Visitor Connect is the feature that supports social authentication plug-ins.

upvoted 1 times

 **Gumpy1** 7 months, 4 weeks ago

Selected Answer: C

Answer is C

In black in white from Cisco docs:

[https://www.cisco.com/c/en/us/td/docs/wireless/mse/7-](https://www.cisco.com/c/en/us/td/docs/wireless/mse/7-6/CMX_Dashboard/Guide/Cisco_CMX_Dashboard_Config_Guide/CMX_Dashboard_Visitor_Connect.pdf#:~:text=Cisco%20CMX%20Visitor%20Connect%20is%20)

[6/CMX_Dashboard/Guide/Cisco_CMX_Dashboard_Config_Guide/CMX_Dashboard_Visitor_Connect.pdf#:~:text=Cisco%20CMX%20Visitor%20Connect%20is%20](https://www.cisco.com/c/en/us/td/docs/wireless/mse/7-6/CMX_Dashboard/Guide/Cisco_CMX_Dashboard_Config_Guide/CMX_Dashboard_Visitor_Connect.pdf#:~:text=Cisco%20CMX%20Visitor%20Connect%20is%20)

upvoted 1 times

 **Vlad_Is_Love_ua** 1 year, 7 months ago

Selected Answer: C

Cisco CMX Visitor Connect is a guest access solution based on Mobility Services Engine (MSE), Cisco Wireless LAN Controller (WLC) and Lightweight Access points (AP). The Visitor Connect is an intuitive simple location aware guest captive portal, that enables you to create a custom on-boarding experience for your visitors. This is designed to provide best experience for both mobile and laptop users.

For splash pages, the Visitor Connect supports customization of:

Social authentication plug-in like Facebook, LinkedIn, and Google+

[https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-](https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/CMX_Connect_Engage_Visitor_Connect/Guide/Cisco_CMX_Connect_Engage_Config_Guide_VC/Overview.html)

[0/CMX_Connect_Engage_Visitor_Connect/Guide/Cisco_CMX_Connect_Engage_Config_Guide_VC/Overview.html](https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/CMX_Connect_Engage_Visitor_Connect/Guide/Cisco_CMX_Connect_Engage_Config_Guide_VC/Overview.html)

upvoted 1 times

🗨️ 👤 **Jason233** 1 year, 9 months ago

Selected Answer: C

CMX Visitor Connect

upvoted 1 times

🗨️ 👤 **Kyle9856** 2 years, 9 months ago

Selected Answer: C

Visitor Connect as Captive Portal

CMX Visitor Connect is an intuitive simple guest captive portal that allows easy onboarding of the guests. The Visitor Connect is location aware and serve different splash templates to different locations or zones.

•Social authentication plug-in like Facebook, LinkedIn, and Google+

[https://www.cisco.com/c/en/us/td/docs/wireless/mse/7-](https://www.cisco.com/c/en/us/td/docs/wireless/mse/7-6/CMX_Dashboard/Guide/Cisco_CMX_Dashboard_Config_Guide/CMX_Dashboard_Visitor_Connect.html)

[6/CMX_Dashboard/Guide/Cisco_CMX_Dashboard_Config_Guide/CMX_Dashboard_Visitor_Connect.html](https://www.cisco.com/c/en/us/td/docs/wireless/mse/7-6/CMX_Dashboard/Guide/Cisco_CMX_Dashboard_Config_Guide/CMX_Dashboard_Visitor_Connect.html)

upvoted 5 times

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

provided answer is correct

upvoted 2 times

🗨️ 👤 **Cyrillka** 3 years, 3 months ago

C is Correct

Configuring Facebook App for Visitor Connect



https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/CMX/CMX_Visitor.html

upvoted 4 times

A network engineer has been hired to perform a new MSE implementation on an existing network. The MSE must be installed in a different network than the Cisco WLC. Which configuration allows the devices to communicate over NMSP?

- A. Allow UDP/16113 port on the central switch.
- B. Allow TCP/16113 port on the firewall.
- C. Allow UDP/16666 port on the VPN router.
- D. Allow TCP/16666 port on the router.

Suggested Answer: B

  **rrahim** 4 months, 1 week ago

Selected Answer: B

For the Mobility Services Engine (MSE) and Cisco Wireless LAN Controller (WLC) to communicate over the Network Mobility Services Protocol (NMSP), the following configuration is required:

NMSP Communication:

NMSP uses TCP port 16113 for communication between the MSE and the WLC. If the MSE and WLC are in different networks, the firewall between them must allow traffic on this port.

Why TCP/16113?:



NMSP relies on TCP for reliable communication, and port 16113 is the default port used for this protocol. Allowing this port on the firewall ensures that the MSE and WLC can establish a connection and exchange data.

upvoted 1 times

  **Pawnstar** 8 months ago

NMSP operates on TCP/16113. Answer provided is correct

upvoted 3 times

  **kthekillerc** 8 months, 3 weeks ago

provided answer is correct

upvoted 2 times

  **Hugh_Jazz** 1 year ago

Answer is correct

upvoted 3 times


What is the default NMSP echo interval between Cisco MSE and a Wireless LAN Controller?

- A. 10 seconds
- B. 15 seconds
- C. 30 seconds
- D. 60 seconds

Suggested Answer: B

Reference:

https://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch4_CAS.html

  **rrahim** 4 months, 1 week ago

Selected Answer: B



The Network Mobility Services Protocol (NMSP) is used for communication between the Cisco Mobility Services Engine (MSE) and the Wireless LAN Controller (WLC) to exchange real-time location and telemetry data.

The default NMSP echo interval (heartbeat) between MSE and WLC is 15 seconds.

This interval ensures regular connectivity checks and maintains a stable connection between the devices.



(Option B is correct).

upvoted 1 times

  **kthekillerc** 8 months, 3 weeks ago

provided answer is correct

upvoted 2 times

  **Pawnstar** 9 months, 2 weeks ago

How frequently an echo request is sent from a MSE to a controller. The default value is 15 seconds.

Answer is correct.

upvoted 3 times

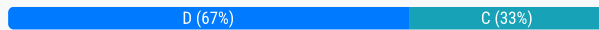
An engineer just added a new MSE to Cisco Prime Infrastructure and wants to synchronize the MSE with the Cisco 5520 WLC, located behind a firewall in a DMZ.

It is noticed that NMSP messages are failing between the two devices. Which traffic must be allowed on the firewall to ensure that the MSE and WLC are able to communicate using NMSP?

- A. TCP 1613
- B. UDP 16113
- C. UDP 1613
- D. TCP 16113

Suggested Answer: D

Community vote distribution



🗨️ 👤 **Seba_o_s** 7 months, 2 weeks ago

Selected Answer: D

TCP 16113

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/network-mobility-services-protocol.pdf

upvoted 1 times

🗨️ 👤 **Markus_Kruber** 10 months, 1 week ago

Selected Answer: D

"The TCP port (16113) that the controller and Cisco CMX communicate over must be open (not blocked) on any firewall that exists between the controller and the Cisco CMX for NMSP to function." https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/network-mobility-services-protocol.html => D is correct

upvoted 1 times

🗨️ 👤 **qqqqqqqqqq123** 1 year, 7 months ago

Selected Answer: C

Correct:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-4/config-guide/b_wl_17_4_cg/m_fastlocate.html#:~:text=Since%20data%20packets,available%20more%20frequently.

upvoted 1 times

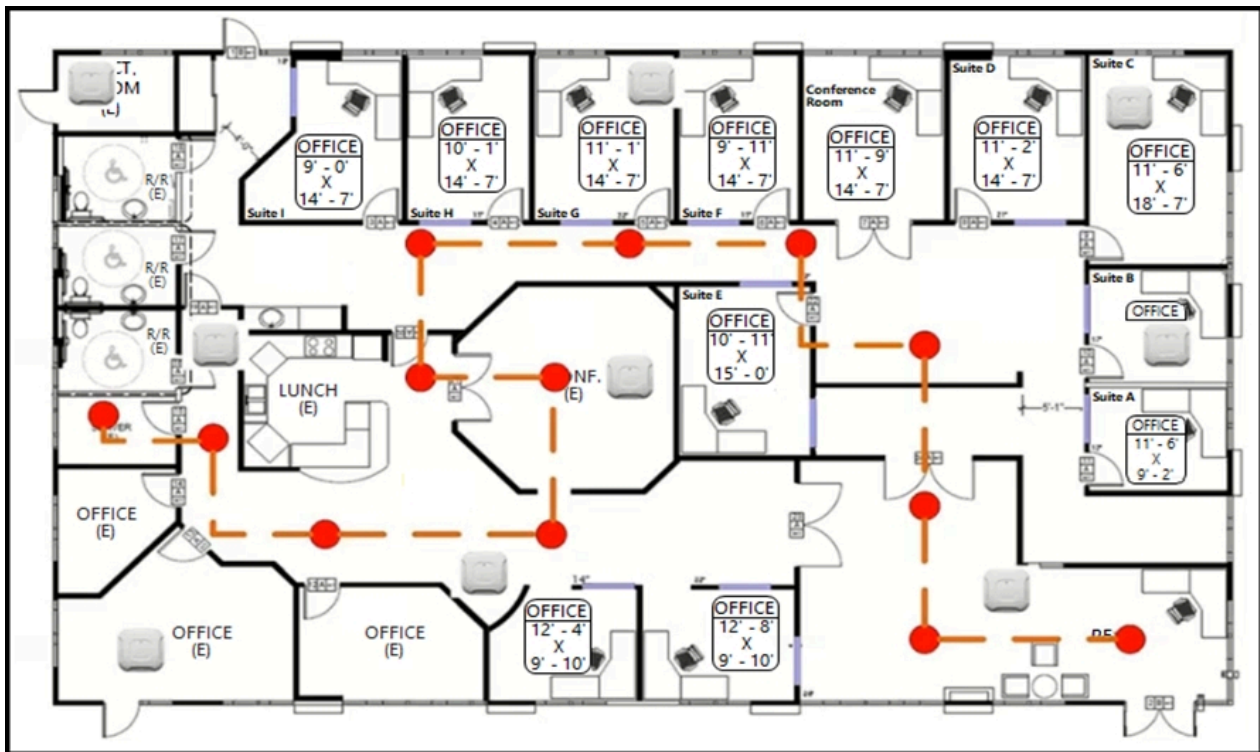
🗨️ 👤 **somebodyfromtheinterwebz** 1 year, 5 months ago

I dont think so, provided answer seems correct:

"The TCP port (16113) that the controller and Cisco CMX communicate over must be open (not blocked) on any firewall that exists between the controller and the Cisco CMX for NMSP to function"

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/network-mobility-services-protocol.pdf

upvoted 3 times



Refer to the exhibit. An engineer needs to configure location services in an office. The requirement is to use FastLocate and achieve higher locations refresh rates. Which location-based technique should be implemented?

- A. probe-based
- B. location patterning
- C. data packet-based
- D. angulation

Suggested Answer: C

Community vote distribution

C (100%)

DiegoECUIO 7 months, 3 weeks ago

Since data packets are more frequent than probe request packets, they can be aggregated better. FastLocate enables higher location refresh rates by collecting RSSI or location information through data packets received by the APs. Using these data packets, location-based services (LBS) updates are initiated by the network and are available more frequently.

upvoted 1 times

rph02533 1 year, 6 months ago

Selected Answer: C

Provided answer is correct

Since data packets are more frequent than probe request packets, they can be aggregated better. FastLocate enables higher location refresh rates by collecting RSSI or location information through data packets received by the APs. Using these data packets, location-based services (LBS) updates are initiated by the network and are available more frequently.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-2/config-guide/b_wl_17_2_cg/fastlocate_for_cisco_catalyst_series_access_points.pdf

upvoted 2 times

An engineer is managing a wireless network for a shopping center. The network includes a Cisco WLC, a Cisco MSE, and a Cisco Prime Infrastructure. What is required to use Cisco CMX Location Analytics?

- A. Enable tracking parameters in Cisco MSE.
- B. Enable Context Aware and CMX Browser Engage.
- C. Install Cisco Prime Infrastructure with floor maps.
- D. Set history parameters in Cisco MSE.

Suggested Answer: B

Community vote distribution

D (100%)

🗳️ 👤 **Ocsicccnp** 8 months, 4 weeks ago

Selected Answer: D

Note In order for the CMX analytics to access data from the MSE, you must set the history parameters on the MSE.

upvoted 1 times

🗳️ 👤 **draven76** 1 year, 10 months ago

Selected Answer: D

I think it's D: "In order for the CMX analytics to access data from the MSE, you must set the history parameters on the MSE."

https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/CMX_Analytics/Guide/CMX_Analytics_Guide/CMX_Getting_Started.html#56189

upvoted 3 times

🗳️ 👤 **somebodyfromtheinterwebz** 2 years, 5 months ago

I say C:

Prerequisites for Enabling CMX Analytics Service:

"CMX analytics requires both floor plans and coverage areas to be defined in the Prime Infrastructure in order for CMX analytics visualization and reporting to function"

https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/CMX_Analytics/Guide/CMX_Analytics_Guide.pdf

upvoted 1 times

🗳️ 👤 **Robesera** 2 years, 8 months ago

It wouldnt be B because CMX Browser Engage is not used for Location Analytics. Browser Engage allows organizations to customize the web browsing experience for mobile users in their venue by offering various context-aware value added services.

Correct answer should be D.

https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/CMX_Analytics/Guide/CMX_Analytics_Guide/CMX_Getting_Started.html#:~:text=7.9%20million%20points-,Note,-In%20order%20for

upvoted 3 times

🗳️ 👤 **twoplanker** 2 years, 7 months ago

This looks correct to me:

In order for the CMX analytics to access data from the MSE, you must set the history parameters on the MSE.

upvoted 3 times

🗳️ 👤 **Yod_Jjot** 2 years, 8 months ago

I think that C is correct.

Ref: <https://mrnciew.com/2016/06/10/cisco-cmx-10-2-part-2/>

upvoted 1 times

🗳️ 👤 **Robesera** 2 years, 8 months ago

I dont think it would be C since the question states that Prime is already installed

upvoted 2 times



An engineer configures a deployment to support:

- ⇒ Cisco CMX
- ⇒ licenses for at least 3000 APs
- ⇒ 6000 WIPS licenses

The Cisco vMSE appliance must be sized for this deployment. Which Cisco vMSE Release 8 option must the engineer deploy?

- A. Large vMSE
- B. Low-End vMSE
- C. Standard vMSE
- D. High-End vMSE

Suggested Answer: *D*

  **Yod_Jjot** 8 months, 3 weeks ago

D is correct

Refer to: https://www.cisco.com/c/en/us/products/collateral/wireless/mobility-services-engine/data_sheet_c07-473865.html

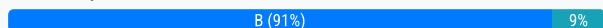
upvoted 2 times

A new MSE with wIPS service has been installed and no alarm information appears to be reaching the MSE from controllers. Which protocol must be allowed to reach the MSE from the controllers?

- A. SOAP/XML
- B. NMSP
- C. CAPWAP
- D. SNMP

Suggested Answer: A

Community vote distribution



Sorvahr Highly Voted 3 years, 8 months ago

B is correct. NMSP is used between CMX and WLC. CAPWAP is used between WLC and AP's.
upvoted 17 times

Skliffi Highly Voted 3 years, 7 months ago

B is correct
NMSP (Network Mobility Services Protocol) – The protocol used for communication between Wireless LAN Controllers and the Mobility Services Engine. In the case of a wIPS Deployment, this protocol provides a pathway for alarm information to be aggregated from controllers to the MSE and for wIPS configuration information to be pushed to the controller. This protocol is encrypted.
https://www.cisco.com/c/en/us/td/docs/wireless/technology/wips/deployment/guide/WiPS_deployment_guide.html#pgfId-80073
upvoted 11 times

qwertyEDCA Most Recent 6 months, 3 weeks ago

Selected Answer: B
B is the correct answer, find documentation through the link provided by e.g Skliffi.
- https://www.cisco.com/c/en/us/td/docs/wireless/technology/wips/deployment/guide/WiPS_deployment_guide.html
upvoted 1 times

[Removed] 8 months, 2 weeks ago

https://www.cisco.com/c/en/us/td/docs/wireless/technology/wips/deployment/guide/WiPS_deployment_guide.html#pgfId-80073

The documentation states that the MSE uses SNMP to receive wIPS alarm information from the controllers. The NMSP protocol is used for communication between controllers and the MSE, but it is not specifically used for wIPS alarms.

I am going with SNMP
upvoted 1 times

most_ahdy 10 months, 1 week ago

Network Mobility Services Protocol (NMSP)-The protocol handles communication between controllers and the mobility services engine. In an wIPS deployment, this protocol provides a pathway for alarm information to be aggregated from controllers and forwarded to the mobility services engine and for wIPS configuration information to be pushed to the controller. This protocol is encrypted.
upvoted 1 times

most_ahdy 10 months, 1 week ago

https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/5-2/wIPS/configuration/guide/msecg_wIPS/msecg_ch1_wIPS.html
upvoted 1 times

GoldLeader 11 months, 2 weeks ago

Selected Answer: B
Answer B. NMSP (Network Mobility Services Protocol) – The protocol used for communication between Wireless LAN Controllers and the Mobility Services Engine. In the case of a wIPS Deployment, this protocol provides a pathway for alarm information to be aggregated from controllers to the MSE.
upvoted 3 times

CHERIFNDIAYE 1 year ago

Selected Answer: B

NMSP is between WLAN and MSE.

SNMP is between Prime infrastructure and WLAN.

SOAP/XML is between Prime infrastructure and MSE.

CORRECT ANSWER IS B.

upvoted 2 times

  **Tonymopar** 1 year ago

Selected Answer: B

[https://www.cisco.com/c/en/us/td/docs/wireless/technology/wips/deployment/guide/WiPS_deployment_guide.html#pgfId-80073~:text=NMSP%20\(Network%20Mobility,protocol%20is%20encrypted.](https://www.cisco.com/c/en/us/td/docs/wireless/technology/wips/deployment/guide/WiPS_deployment_guide.html#pgfId-80073~:text=NMSP%20(Network%20Mobility,protocol%20is%20encrypted.)

upvoted 1 times

  **JimDiGriz** 1 year, 2 months ago

Selected Answer: D

NMSP (Network Mobility Services Protocol) is not used for wIPS (Wireless Intrusion Prevention System) alarms. NMSP is used to enable communication between the Cisco Mobility Services Engine (MSE) and Cisco wireless LAN controllers (WLCs) to support location-based services such as Cisco CMX (Connected Mobile Experiences). SNMP (Simple Network Management Protocol) is the protocol used to forward wIPS alarms from the WLC to the MSE.


upvoted 1 times

  **Jason233** 1 year, 3 months ago

Selected Answer: B

NMSP is used between CMX and WLC

upvoted 1 times

  **cvndani** 1 year, 9 months ago

Selected Answer: B

B is the correct answer

upvoted 3 times

  **kthekillerc** 2 years, 8 months ago

B is the correct answer

upvoted 5 times

  **Hugh_Jazz** 3 years ago

B is correct.

upvoted 7 times

  **maro_moh** 3 years, 4 months ago

B is correct.

upvoted 8 times

  **masaharu** 3 years, 10 months ago

I think C is correct.

upvoted 1 times

Which two statements about the requirements for a Cisco Hyperlocation deployment are true? (Choose two.)

- A. After enabling Cisco Hyperlocation on Cisco CMX, the APs and the wireless LAN controller must be restarted.
- B. NTP can be configured, but that is not recommended.
- C. The Cisco Hyperlocation feature must be enabled on the wireless LAN controller and Cisco CMX.
- D. The Cisco Hyperlocation feature must be enabled only on the wireless LAN controller.
- E. If the Cisco CMX server is a VM, a high-end VM is needed for Cisco Hyperlocation deployments.

Suggested Answer: AC

Community vote distribution

CE (100%)

 **Sorvahr** Highly Voted 3 years, 8 months ago

C and E

upvoted 18 times

 **Profiteur** 3 years, 3 months ago

Agreed; Sauce is here: <https://www.cisco.com/c/en/us/support/docs/wireless/connected-mobile-experiences/214757-cmx-location-limitations-and-hardware-re.html>


CMX limitations

The amount of data the CMX Location can handle heavily depends on the node size. Software limitations of Low, Standard and High end node can be found in the table below:

Limitations Low-end Standard High-end

Hyperlocation support No No Yes

upvoted 6 times

 **Citizenx** Highly Voted 2 years, 1 month ago

C+E are right.

A is wrong because only APs and the hyperlocation service on CMX must be restarted.

-NTP is very important

-HIGH end vm needed.

upvoted 6 times

 **[Removed]** Most Recent 8 months, 2 weeks ago

Selected Answer: CE

C. The Cisco Hyperlocation feature must be enabled on the wireless LAN controller and Cisco CMX.

E. If the Cisco CMX server is a VM, a high-end VM is needed for Cisco Hyperlocation deployments.

upvoted 1 times

 **GoldLeader** 11 months, 2 weeks ago

Selected Answer: CE

C. and E.

upvoted 2 times

 **Vlad_Is_Love_ua** 1 year, 1 month ago

After enabling Hyperlocation on Cisco CMX, you must restart the services:

Log in to the console or through SSH and use the `cmxctl stop` and `cmxctl start` command to stop and restart the services.

You can enter the `cmxctl status` command to check if the Hyperlocation service is running.

After enabling Hyperlocation on Cisco CMX, you must also restart the APs:

Use the Cisco Prime Infrastructure WLC GUI or WLC CLI to restart the APs.

You can also power cycle the APs from the switch.

upvoted 1 times

🗨️ 👤 **cvndani** 1 year, 9 months ago

In this guide indicates that VM High End is needed, but it does not say anything that the wifi controller and the AP's have to be restarted. So C and E are the correct answers.

<https://www.cisco.com/c/en/us/support/docs/wireless/connected-mobile-experiences/200907-configuring-and-troubleshooting-hyperloc.html>

upvoted 2 times

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

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_ap_4800_hyperlocation_deployment_guide.html

upvoted 1 times

🗨️ 👤 **Mimimimimi** 2 years, 6 months ago

I believe the answer is C&E. Following Skliffi's URL:

Wrong answers:

Answer A: CMX & AP's need a restart, not the WLC

B: Must always be configured.

D: It must be enabled on CMX AND WLC

C: Features must indeed be enabled on WLC & CMX

E: A high-end VM is required.

upvoted 3 times

🗨️ 👤 **kthekillerc** 2 years, 6 months ago

answers provided are correct and it is required to restart the devices see link https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/dam/en/us/td/docs/wireless/controller/technotes/8-8/b_ap_4800_hyperlocation_deployment_guide.html.xml

[uri=/searchable/chapter/content/dam/en/us/td/docs/wireless/controller/technotes/8-8/b_ap_4800_hyperlocation_deployment_guide.html.xml](https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/dam/en/us/td/docs/wireless/controller/technotes/8-8/b_ap_4800_hyperlocation_deployment_guide.html.xml)

upvoted 1 times

🗨️ 👤 **cvndani** 1 year, 9 months ago

It indicates that its necessary restart CMX service and AP's, not WLC....

upvoted 1 times

🗨️ 👤 **kthekillerc** 2 years, 8 months ago

Provided answer is correct

upvoted 2 times

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

Hard to find out 100% correct answers - no need to restart WLC after enabling hyperlocation

After enabling Hyperlocation on CMX it is also required to restart the APs.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_ap_4800_hyperlocation_deployment_guide.html#id_81964

upvoted 2 times

🗨️ 👤 **powerslave666** 3 years ago

It doesn't indicate restart:

The major steps involved in setting up a Hyperlocation system are:

1. Assemble the APs and mount them to the ceiling, recording the exact X, Y, height, and orientation of the devices.
2. Install Cisco WLC and connect the APs to Cisco WLC.
3. Enable the functions that are required, including Hyperlocation, in Cisco WLC.
4. Import Cisco WLC into Cisco PI.
5. Place the AP on the map in Cisco PI.
6. Save and export the map from Cisco PI to a local storage point.
7. Install Cisco CMX.
8. Configure and enable Hyperlocation.
9. Import the map from the local storage point.
10. Verify that the system is showing the clients correctly on the map and that the APs are placed and oriented correctly.

11. Complete Location Accuracy testing of static clients to determine the level of accuracy obtained.

By following these basic steps, a system can be up and running within one day, and the accuracy of the system can be gauged.

upvoted 1 times

An engineer is performing a Cisco Hyperlocation accuracy test and executes the `cmxloc start` command on Cisco CMX. Which two parameters are relevant?

(Choose two.)

- A. X, Y real location
- B. client description
- C. AP name
- D. client MAC address
- E. WLC IP address

Suggested Answer: AD

Community vote distribution

AD (100%)

🗲️ 👤 **Nyi19921992** Highly Voted 🍌 3 years, 6 months ago

Answer is correct

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_command/cmxcli106/cmxcli1051_chapter_010.html#wp9568417800

upvoted 7 times

🗲️ 👤 **rrahim** Most Recent 🕒 4 months, 1 week ago

Selected Answer: AD

A. X, Y real location: This parameter specifies the actual physical coordinates (real location) of the client device being tested. It is used to compare against the calculated location to determine accuracy.

D. client MAC address: This parameter identifies the specific client device being tracked for the location accuracy test. The MAC address is used to monitor and analyze the device's location data.

The other options (B, C, and E) are not directly relevant to the `cmxloc start` command for this specific test.

upvoted 1 times

🗲️ 👤 **Juancho386** 8 months ago

Selected Answer: AD

Provided answer is correct

upvoted 1 times

🗲️ 👤 **kthekillerc** 2 years, 7 months ago

Provided answer is correct

upvoted 3 times

Where is Cisco Hyperlocation enabled on a Cisco Catalyst 9800 Series Wireless Controller web interface?

- A. Policy Profile
- B. AP Join Profile
- C. Flex Profile
- D. RF Profile

Suggested Answer: B

Reference:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/cisco-hyperlocation.html

Community vote distribution

B (100%)

🗳️ 👤 **rrahim** 4 months, 1 week ago

Selected Answer: B

B. AP Join Profile

Cisco Hyperlocation is enabled under the AP Join Profile in the Configuration > Tags & Profiles > AP Join section of the web interface. This is where you configure settings such as enabling Hyperlocation, setting the detection threshold, trigger threshold, and reset threshold.

upvoted 1 times

🗳️ 👤 **Vlad_Is_Love_ua** 7 months, 3 weeks ago

Selected Answer: B

Configure Hyperlocation on the Cisco WLC (Cisco IOS XE)

To configure the Cisco Catalyst 9800 WLC for Hyperlocation, take the following steps:

Log in to the Cisco Catalyst 9800 WLC.

Navigate to Configuration > Tags & Profiles > AP Join.

At this point, either modify an existing profile or create a new one, if necessary.

In the Edit AP Join Profile page, choose AP and then Hyperlocation.

Check the Enable Hyperlocation check box.

Save or update the profile:

If this profile is new, click Save & Apply to Device.

If you are modifying an existing profile, click Update and Apply to Device.

Save the configuration.

upvoted 2 times

🗳️ 👤 **Vlad_Is_Love_ua** 7 months, 4 weeks ago

Selected Answer: B

Where is Cisco Hyperlocation enabled on a Cisco Catalyst 9800 Series Wireless Controller web interface?

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/cisco-hyperlocation.html#task_k2c_nps_xfb

upvoted 1 times

🗳️ 👤 **alexblue** 1 year, 6 months ago

the link says to restart the WLC only

upvoted 1 times

  **kthekillerc** 2 years, 1 month ago

prohttps://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/wireless/controller/9800/16-11/config-guide/b_wl_16_11_cg/cisco-hyperlocation.html.xml

vided answer is correct

upvoted 4 times

The Cisco Hyperlocation detection threshold is currently set to -50 dBm. After reviewing the wireless user location, discrepancies have been noticed. To improve the Cisco Hyperlocation accuracy, an engineer attempts to change the detection threshold to -100 dBm. However, the Cisco Catalyst 9800 Series Wireless

Controller does not allow this change to be applied. What actions should be taken to resolve this issue?

- A. Disable Cisco Hyperlocation, change the Cisco Hyperlocation detection threshold, and then enable it.
- B. Create a new profile on Cisco CMX with the new Cisco Hyperlocation detection range, and apply it on the WLAN.
- C. Place the APs to monitor mode, shutdown the radios, and then change the Cisco Hyperlocation detection threshold.
- D. Shutdown all radios on the controller, change the Cisco Hyperlocation detection range, and enable the radios again.

Suggested Answer: A

Community vote distribution

A (50%)

B (50%)

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

In your document https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-1/config-guide/b_wl_17_11_cg/cisco-hyperlocation.html:

"Restrictions on Cisco Hyperlocation

It is not possible to modify detection, trigger, and reset thresholds while Hyperlocation is in enabled state."

So the correct answer is A

upvoted 17 times

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

Selected Answer: A

A. Disable Cisco Hyperlocation, change the Cisco Hyperlocation detection threshold, and then enable it.

To change the Cisco Hyperlocation detection threshold on a Cisco Catalyst 9800 Series Wireless Controller, you must first disable Cisco Hyperlocation, make the necessary changes, and then re-enable it. This is because certain settings, like the detection threshold, cannot be modified while Hyperlocation is active.


upvoted 1 times

 **riktammenaars** 8 months ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-1/config-guide/b_wl_17_11_cg/cisco-hyperlocation.html#restrictions-on-hyperlocation

upvoted 1 times

 **Ocsiccnnp** 8 months, 4 weeks ago

Selected Answer: A

It is not possible to modify detection, trigger, and reset thresholds while Hyperlocation is in enabled state.

upvoted 1 times

 **JimDiGriz** 2 years, 2 months ago

Selected Answer: A

It is not possible to modify detection, trigger, and reset thresholds while Hyperlocation is in enabled state.

upvoted 2 times

 **kthekillerc** 3 years, 4 months ago

Selected Answer: B

Believe answer should be B

upvoted 2 times

 **anonymonkey** 3 years, 3 months ago

Think you were right the first time. https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-1/config-guide/b_wl_17_11_cg/cisco-hyperlocation.html

upvoted 4 times

 **kthekillerc** 3 years, 6 months ago

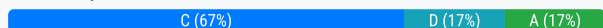
Provided answer is correct
upvoted 1 times

An engineer must track guest traffic flow using the WLAN infrastructure. Which Cisco CMX feature must be configured and used to accomplish this tracking?

- A. analytics
- B. connect and engage
- C. presence
- D. detect and locate

Suggested Answer: D

Community vote distribution



chomjosh Highly Voted 3 years, 1 month ago

C is correct answer
upvoted 6 times

rrahim Most Recent 4 months, 1 week ago

Selected Answer: C

The Presence Analytics Service in Cisco CMX is specifically designed to track and analyze user behavior, including guest traffic flow. It provides data on device presence, dwell time, and movement patterns, which are essential for understanding guest traffic on the WLAN infrastructure.

Explanation of the options:

A. analytics:

While the analytics feature provides detailed insights into traffic patterns, the Presence Analytics Service is more specific to tracking user presence and movement, which is ideal for guest traffic analysis.

upvoted 1 times

riktammenaars 8 months ago

Selected Answer: A

Presence was a lighter version for Location tracking -> now available through Location Analytics and feature is deprecated

upvoted 1 times

5db1f59 8 months, 3 weeks ago

Selected Answer: B

Answer is B:

Question says track guest traffic flow... not the guests location

upvoted 1 times

Gumpy1 1 year, 1 month ago

Selected Answer: D

D is correct...this says "track" not "study behavior". To study behavior would be C.

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmxcfg/b_cg_cmxcfg106/the_cisco_cmxcfg_presence_analytics_service.html

upvoted 1 times

DiegoECUIO 1 year, 7 months ago

D is correct because the answer is about tracking location and detect and locate is more suitable option

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-1/cmxcfg/CMX_Config_guide/CMX_Location.pdf

upvoted 1 times

yrzy 2 years, 3 months ago

Selected Answer: A

The Cisco Connected Mobile Experiences (Cisco CMX) Analytics service provides a set of data analytic tools for analyzing Wi-Fi device locations. The Analytics service helps organizations use the network as a data source to view visitors' behavior patterns and trends, which will in turn help businesses improve visitor experience and boost customer service.

upvoted 1 times

  **gabtown** 2 years, 9 months ago

Selected Answer: C

Answer is C. https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-4/cmx_config/b_cg_cmx104/the_cisco_cmx_presence_analytics_service.html#concept_7C141AE7189344CA8F9238F4A7ED1DFD
upvoted 4 times


  **Citizenx** 3 years, 1 month ago

Answer is correct.

The Cisco Connected Mobile Experiences (Cisco CMX) DETECT & LOCATE service enables you to view and track devices in your deployment.

Using the DETECT & LOCATE service, you can either view all the access points deployed in all the buildings of a campus or view the Access Points deployed on the individual floors of each building. You can also locate Wi-Fi tags, rogue APs, Wi-Fi interferers, and Bluetooth low energy (BLE) beacons.

upvoted 2 times

  **Citizenx** 3 years, 1 month ago

After reading more about this, i think it should be presence (c), and to be in detail: presence analytics:

it gives you info about visitors, passerby of visitors and peak hours. The detect and locate is more about tracking objects.

upvoted 5 times

  **HarryPotter69** 3 years, 3 months ago

I believe the answer to be Presence

Read the difference between Presence Analytics and Detect and Locate - Since I read the it to be related to traffic I say Presence

Presence Analytics

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-4/cmx_config/b_cg_cmx104/the_cisco_cmx_presence_analytics_service.html#concept_7C141AE7189344CA8F9238F4A7ED1DFD

vs

Detect and Locate

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-4/cmx_config/b_cg_cmx104/the_cisco_cmx_detect_and_locate_service.html
upvoted 3 times

  **ozone1864** 3 years, 6 months ago

@kthekillerc are you sure ? I think its C

upvoted 2 times

  **kthekillerc** 3 years, 7 months ago

Provided answer is correct. Detect and locate allows you to monitor guest traffic on the aps you enabled for flow tracking. The question said in the wlan infrastructure traffic flow monitoring what feature would be used.

upvoted 1 times

  **Hugh_Jazz** 4 years ago

Concur, C. Detect and Locate would only be for devices such as APs.

upvoted 3 times

  **cskshiet** 4 years ago

Correct answer is C:

The Cisco CMX Presence Analytics service is a comprehensive analytics and engagement platform that uses APs to detect visitor presence based on their mobile devices' Received Signal Strength Indication (RSSI). The AP detects these client mobile devices irrespective of the latter's wireless association state as long as they are within the specified signal range, and the wireless option is enabled on the mobile device (ability to detect devices wirelessly even if they are not connected to the network)

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-4/cmx_config/b_cg_cmx104/the_cisco_cmx_presence_analytics_service.html
upvoted 3 times

An engineer has successfully implemented 10 active RFID tags in an office environment. The tags are not visible when the location accuracy is tested on the Cisco CMX Detect and Locate window. Which setting on Cisco CMX allows the engineer to view the tags?

- A. Enable RFID tags in tracking options.
- B. Enable probing clients for active tags.
- C. Define an RFID group globally and add the tags.
- D. Enable hyperlocation services for RFID.

Suggested Answer: A

🗲️ 👤 **rrahim** 4 months, 1 week ago

Selected Answer: A

For Cisco CMX to detect and locate active RFID tags, you must enable RFID tracking in the tracking options.

Active RFID tags use Wi-Fi to transmit location beacons, which are picked up by the WLAN infrastructure.

By enabling RFID tags in tracking options, Cisco CMX will recognize and track these tags in the Detect and Locate window.

(Option A is correct).

Why Not the Other Options?

✗ B. Enable probing clients for active tags – Probing clients is for Wi-Fi devices sending probe requests, not active RFID tags.

upvoted 1 times

🗲️ 👤 **rph02533** 1 year ago

Provided answer is correct

refer: [https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-](https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_config/b_cg_cmx106/managing_cisco_cmx_system_settings.html#task_1167241:~:text=Only%20the%20elements%20selected%20here%20will%20be)

[6/cmx_config/b_cg_cmx106/managing_cisco_cmx_system_settings.html#task_1167241:~:text=Only%20the%20elements%20selected%20here%20will%20be](https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_config/b_cg_cmx106/managing_cisco_cmx_system_settings.html#task_1167241:~:text=Only%20the%20elements%20selected%20here%20will%20be)

upvoted 1 times

🗲️ 👤 **kthekillerc** 2 years, 2 months ago

Provided answer is correct

upvoted 4 times

An engineer completed the basic installation for two Cisco CMX servers and is in the process of configuring high availability, but it fails. Which two statements about the root of the issue are true? (Choose two.)

- A. The Cisco CMX instances are installed in the same subnet.
- B. The types of the primary and secondary Cisco CMX installations differ.
- C. The delay between the primary and secondary instance is 200 ms.
- D. The sizes of the primary and secondary Cisco CMX installations differ.
- E. Both Cisco CMX installations are virtual.

Suggested Answer: BD

 **Profiteur** Highly Voted 2 years, 3 months ago

Answer is correct: https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_config/b_cg_cmx106/managing_cisco_cmx_system_settings.html

Pre-requisites for HA

Both the primary and the secondary server should be of the same size and the same type (VM or physical appliance).

Both the primary and the secondary server should have the same Cisco CMX version.

Both the primary and the secondary server should be connected on the same subnet.

Both the primary and the secondary server should be connected on the same subnet if Layer 2 HA is required.

Both the primary and the secondary server should be IP connected with delay of less than 250ms if Layer 3 HA is used.


From Cisco CMX release 10.6.2, NTP server settings must be configured on both Primary and Secondary server instance before HA pairing starts. We recommend that you use the same NTP server on both Primary and Secondary. As a Cisco CMX admin you can also use a dedicated NTP for Primary and Secondary.

upvoted 6 times

 **Madhankg** Most Recent 11 months ago

Answer is correct

upvoted 3 times

 **Sorvahr** 2 years, 8 months ago

Answer is correct.

upvoted 3 times

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
2	0.003747	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
3	1.087479	10.48.39.214	10.48.71.21	UDP	130	9999 → 2003 Len=88
4	2.733577	10.48.39.214	10.48.71.21	UDP	130	9999 → 2003 Len=88
5	2.999859	10.48.39.251	10.48.71.21	UDP	178	9999 → 2003 Len=136
6	3.001227	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
7	4.355249	10.48.39.214	10.48.71.21	UDP	146	9999 → 2003 Len=104
8	5.999538	10.48.39.251	10.48.71.21	UDP	178	9999 → 2003 Len=136
9	6.000959	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
10	8.999418	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
11	9.000791	10.48.39.251	10.48.71.21	UDP	178	9999 → 2003 Len=136
12	9.262904	10.48.39.214	10.48.71.21	UDP	146	9999 → 2003 Len=104
13	10.894785	10.48.39.214	10.48.71.21	UDP	130	9999 → 2003 Len=88
14	11.995126	10.48.39.251	10.48.71.21	UDP	194	9999 → 2003 Len=152
15	11.999193	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
16	14.994902	10.48.39.251	10.48.71.21	UDP	178	9999 → 2003 Len=136
17	14.996368	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
18	17.994857	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
19	17.996231	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
20	18.102843	10.48.39.251	10.48.71.21	UDP	130	9999 → 2003 Len=88
21	21.098408	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
22	21.099952	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
23	24.098574	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
24	24.099804	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
25	27.098099	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
26	27.099839	10.48.39.251	10.48.71.21	UDP	130	9999 → 2003 Len=88
27	28.880307	10.48.39.164	10.48.71.21	UDP	146	9999 → 2003 Len=104
28	28.881569	10.48.39.214	10.48.71.21	CAPP	146	CAPP MD5 Encrypted
29	30.094237	10.48.39.251	10.48.71.21	UDP	178	9999 → 2003 Len=136
30	30.097812	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
31	30.513451	10.48.39.214	10.48.71.21	UDP	130	9999 → 2003 Len=88
32	30.515926	10.48.39.164	10.48.71.21	UDP	130	9999 → 2003 Len=88

> Frame 1: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
 > Ethernet II, Src: Ciscollc_2a:c4:a3 (00:06:f6:2a:c4:a3), Dst: Vmware_99:4e:19 (00:50:56:99:4e:19)
 > Internet Protocol Version 4, Src: 10.48.39.251, Dst: 10.48.71.21
 > User Datagram Protocol, Src Port: 9999 (9999), Dst Port: 2003 (2003)
 v Data (120 bytes)
 Data: ae 2f 44 f0 00 00 b4 5f ef 06 fd cb b7 6c 03 c7 ...
 [Length: 120]

Refer to the exhibit. The image shows a packet capture that was taken at the CLI of the Cisco CMX server. It shows UDP traffic from the WLC coming into the server. What does the capture prove?

- A. The Cisco CMX server receives NetFlow data from the WLC.
- B. The Cisco CMX server receives NMSP traffic from the WLC.
- C. The Cisco CMX server receives SNMP traffic from the WLC.
- D. The Cisco CMX server receives Angle-of-Arrival data from the WLC.

Suggested Answer: D

Nyi19921992 2 years, 6 months ago

Answer is correct

<https://www.cisco.com/c/en/us/support/docs/wireless/connected-mobile-experiences/200907-configuring-and-troubleshooting-hyperloc.html>
 upvoted 9 times

alexblue 1 year ago

16113 Network Mobility Services Protocol (NMSP)

2003 AoA (The AP encapsulates the AoA packet inside Capwap towards the WLC, therefore port 2003 has to be open between the WLC and CMX)

80 HTTP

443 HTTPS

Internet Control Message Protocol (ICMP)



161, 162 Simple Network Management Protocol (SNMP)

upvoted 6 times

A Cisco CMX 3375 appliance on the 10.6.1 version code counts duplicate client entries, which creates wrong location analytics. The issue is primarily from iOS clients with the private MAC address feature enabled. Enabling this feature requires an upgrade of the Cisco CMX 3375 appliance in a high availability pair to version 10.6.3. SCP transfers the Cisco CMX image, but the upgrade script run fails. Which configuration change resolves this issue?

- A. Upgrade the high availability pair to version 10.6.2 image first and then upgrade to version 10.6.3.
- B. Save configuration and use the upgrade script to upgrade the high availability pair without breaking the high availability.
- C. Break the high availability using the cmxha config disable command and upgrade the primary and secondary individually.
- D. Run root patch to first upgrade to version 10.6.2 and then migrate to version 10.6.3.

Suggested Answer: C

  **Ocsicccnp** 8 months, 4 weeks ago

Selected Answer: C

In CMX's current format you have to disable HA in order to perform an upgrade. In order to disable HA from the command line, run cmxha config disable from the primary CMX

upvoted 1 times

  **profu** 2 years ago

<https://www.cisco.com/c/en/us/support/docs/availability/high-availability/213664-configure-cmx-high-availability.html>

upvoted 1 times

  **Zatingke** 2 years, 5 months ago

Can't upgrade when HA is working

upvoted 1 times

An engineer has implemented advanced location services for a retail wireless deployment. The marketing department wants to collect user demographic information in exchange for guest WLAN access and to have a customized portal per location hosted by the provider. Which social connector must be tied into Cisco CMX to provide this service?

- A. Gmail
- B. Google+
- C. Facebook
- D. MySpace

Suggested Answer: C

🗨️ 👤 **DiegoECUIO** 7 months, 3 weeks ago

CMX only support Facebook connector, connector like goggle, gmail and myspace have not defined
upvoted 1 times

🗨️ 👤 **BrockHarbor** 10 months, 3 weeks ago

Probably FB

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cm_config/b_cg_cm106/the_cisco_cm_connect_and_engage_service.html#con_1132546
upvoted 1 times

🗨️ 👤 **Zatingke** 1 year, 5 months ago

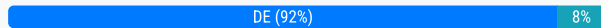
FB or G+?
upvoted 1 times

What are two considerations when deploying a Cisco Hyperlocation? (Choose two.)

- A. NTP configuration is available, but not recommended.
- B. The Cisco Hyperlocation feature must be enabled only on the wireless LAN controller.
- C. After enabling Cisco Hyperlocation on Cisco CMX, the APs and the wireless LAN controller must be restarted.
- D. The Cisco Hyperlocation feature must be enabled on the wireless LAN controller and Cisco CMX.
- E. If the Cisco CMX server is a VM, a high-end VM is needed for Cisco Hyperlocation deployments.

Suggested Answer: CD

Community vote distribution



daeman Highly Voted 2 years, 3 months ago

Selected Answer: DE

Should be D and E

upvoted 8 times

Gumpy1 Most Recent 7 months, 4 weeks ago

Selected Answer: DE

D and E.

Cisco doc look under Assumptions and Recommendations & Summary of the Installation and Setup Process:

https://www.cisco.com/c/en/us/td/docs/interfaces_modules/cmx/hyperlocation/quick_start/HyperlocationQuickStart.pdf

upvoted 1 times

shards 1 year, 4 months ago

Selected Answer: DE

Only CMX services and the APs need restarting. Not the WLC.

upvoted 1 times

itapase0314 1 year, 11 months ago

Selected Answer: DE

Should be D and E

upvoted 1 times

cvndani 2 years, 3 months ago

Selected Answer: CE

In this guide indicates that VM High End is needed, but it does not say anything that the wifi controller and the AP's have to be restarted.

<https://www.cisco.com/c/en/us/support/docs/wireless/connected-mobile-experiences/200907-configuring-and-troubleshooting-hyperloc.html>

upvoted 1 times

cvndani 2 years, 3 months ago

Sorry, D and E

upvoted 6 times



After installing and configuring Cisco CMX, an administrator must change the NTP server on the Cisco CMX server. Which action accomplishes this task?

- A. Manually edit /etc/ntp.conf using an XML editor before restarting the server by using service restart all services.
- B. Log in to the Cisco CMX CLI and issue set ntp server NTP IP where NTP IP is the IP of the NTP server.
- C. Manually edit /etc/ntp.conf as the admin user before restarting ntpd by using service ntpd restart.
- D. Log in to the Cisco CMX GUI as the administrator and type the IP address of the NTP server in System tab > Settings> TimeZone/NTP.

Suggested Answer: C

Reference:

<https://www.cisco.com/c/en/us/support/docs/wireless/connected-mobile-experiences/200906-Troubleshooting-CMX-connectivity-with-WL.pdf>

  **Yod_Jjot** 8 months, 3 weeks ago

C is correct

upvoted 4 times

A customer managing a large network has implemented location services. Due to heavy load, it is needed to load balance the data coming through NMSP from the WLCs. Load must be spread between multiple CMX servers to help optimize the data flow for Aps. Which configuration in CMX meets this requirement?

- A. `cmxctl config feature flags nmsplb.cmx-ap-grouping true`
 B. `cmxctl config feature flags nmsplb.cmxgrouping true`
 C. `cmxctl config feature flags nmsplb.cmx-loadbalance true`
 D. `cmxctl config feature flags nmsplb.cmx-rssi-distribute true`

Suggested Answer: B

Reference:

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_command/cmxcli106/cmxcli1051_chapter_010.html#wp7273815000

<https://www.cisco.com/c/en/us/support/docs/wireless/connected-mobile-experiences/214894-optimize-cmx-performance.html>

Community vote distribution

B (100%)

 rrahim 4 months, 1 week ago

Selected Answer: B

B. cmxctl config feature flags nmsplb.cmxgrouping true

The documentation specifies that enabling `nmsplb.cmxgrouping` allows for load balancing of NMSP traffic across multiple CMX servers. This configuration ensures that the data flow is optimized and the load is distributed evenly.

Explanation of the options:

A. cmxctl config feature flags nmsplb.cmx-ap-grouping true:

This is incorrect. This command is not related to load balancing NMSP traffic.

B. cmxctl config feature flags nmsplb.cmxgrouping true:

This is correct. Enabling `nmsplb.cmxgrouping` ensures that NMSP traffic is load balanced across multiple CMX servers.

C. cmxctl config feature flags nmsplb.cmx-loadbalance true:

This is incorrect. While it sounds relevant, the documentation specifies `nmsplb.cmxgrouping` as the correct feature flag for load balancing.

D. cmxctl config feature flags nmsplb.cmx-rssi-distribute true:

This is incorrect. This command is not related to load balancing NMSP traffic.

upvoted 1 times

 Vlad_Is_Love_ua 11 months, 1 week ago

Selected Answer: B

<https://www.cisco.com/c/en/us/support/docs/wireless/connected-mobile-experiences/214894-optimize-cmx->

[illegible]

An engineer needs to provision certificates on a Cisco Catalyst 9800 Series Wireless Controller. The customer uses a third-party CA server. Which protocol must be used between the controller and CA server to request and install certificates?

- A. SCEP
- B. TLS
- C. LDAP
- D. SSL

Suggested Answer: A

Reference:



<https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/trustpoints/b-configuring-trustpoints-on-cisco-catalyst-9800-series-controllers/c-workflow-to-configure-a-trustpoint-for-a-third-party-certificate-on-catalyst-9800.html>

  **rrahim** 4 months, 1 week ago

Selected Answer: A

To provision certificates on a Cisco Catalyst 9800 Series Wireless Controller using a third-party CA (Certificate Authority) server, the SCEP (Simple Certificate Enrollment Protocol) must be used. SCEP is a protocol specifically designed for certificate enrollment and allows the controller to request and install certificates from the CA server.

upvoted 1 times

  **Yod_Jjot** 8 months, 3 weeks ago

A is the correct answer:

There are many ways to enroll your trustpoint and receive a certificate from the CA. Depending on the configuration, you can:

Enroll the Trustpoint automatically.

The Catalyst 9800 controller supports automatic certificate enrollment protocols like Simple Certificate Enrollment Protocol (SCEP) and Enrollment over Secure Tunnel (EST) to forward and receive certificate requests generated on the controller to the CA.

Enroll the Trustpoint manually.

The Catalyst 9800 controller supports manual enrollment that uses the PKCS#12 Certificate Signing Request (CSR) mechanism to issue certificates for the controller. Subsequent to the CSR request, the signed certificate for the controller, together with the CA root certificate, are uploaded to the controller. Note that it is also possible to use OpenSSL or any other utility to generate the keys and the CSR.

upvoted 3 times

A corporation has recently implemented a BYOD policy at their HQ. Which two risks should the security director be concerned about? (Choose two.)

- A. network analyzers
- B. malware
- C. lost and stolen devices
- D. keyloggers
- E. unauthorized users

Suggested Answer: BC

Community vote distribution

BE (100%)

🗲️ 👤 **Le91** 8 months ago

Selected Answer: BC

B and C are the correct answers

upvoted 1 times

🗲️ 👤 **SrStew** 8 months, 1 week ago

I think it's b and c because BYOD you usually don't have MDM so if a lost or stolen device you wouldn't have any remote wipe or locking power.

upvoted 1 times

🗲️ 👤 **netwkguy99** 10 months, 1 week ago

Selected Answer: BE

Just thinking outside the box here but with a BYOD why would the organization care about lost/stolen devices, wouldn't it be unauthorized users that's more concerning?

Thinking it's malware and unauthorized users? B and E

upvoted 1 times

🗲️ 👤 **rrahim** 4 months, 4 weeks ago

Well if someone loses a device which already has a guest login and a weak password to login to\unlock that device then malware can be installed on that device

upvoted 1 times

🗲️ 👤 **kthekillerc** 3 years, 7 months ago

Provided answers are correct

upvoted 2 times

When implementing self-registration for guest/BYOD devices, what happens when an employee tries to connect four devices to the network at the same time?

- A. The last device is removed and the newly added device is updated as active device.
- B. The registration is allowed, but only one device is connected at any given time.
- C. All devices are allowed on the network simultaneously.
- D. Purge time dictates how long a device is registered to the portal.

Suggested Answer: B

Community vote distribution

C (100%)

🗳️ 👤 **Mimimimimi** Highly Voted 2 years, 8 months ago

A is correct, just poorly phrased.

As no specific configurations are specified, default is applied, agreed?

By default:

- 5 devices can be registered
 - 3 simultaneous logins
 - Oldest connection is disconnected (so the newly added is updated as active and last could be read as oldest.)
- upvoted 9 times

🗳️ 👤 **qwertyEDCA** 1 year, 6 months ago

Your right, A is correct.

Source: <https://community.cisco.com/t5/network-access-control/how-to-limit-number-of-devices-per-user-used-to-access-scure/td-p/2678865>
upvoted 1 times

🗳️ 👤 **techgirl321** Most Recent 3 months, 1 week ago

Selected Answer: D

D. D is the only answer that is 100% verifiable
upvoted 1 times

🗳️ 👤 **meromu7** 7 months, 3 weeks ago

Selected Answer: A

A is correct, just poorly phrase
upvoted 1 times

🗳️ 👤 **AhcMez** 1 year, 11 months ago

C is correct what ever the numbers of devices .
upvoted 1 times

🗳️ 👤 **GoldLeader** 1 year, 11 months ago

Selected Answer: C

Going with A. Employee can have all 4 registered at the same time but cannot have more than 3 connected at the same time by default.
upvoted 1 times

🗳️ 👤 **somebodyfromtheinterwebz** 2 years, 5 months ago

TO add the discussion, take a look at the screenshot in this forum:

<https://community.cisco.com/t5/network-access-control/how-to-limit-number-of-devices-per-user-used-to-access-scure/td-p/2678865>

Restrict employee to 5 devices (by default) but:

Maximum simultaneous logins: 3 (by default) and when guest exceeds limit: remove oldest connection.

I say A.

upvoted 2 times

🗳️ 👤 **Citizenx** 3 years, 1 month ago

B is right.

default registered devices is max 5, but the allowed login time has value [1-999] so C is false.

upvoted 3 times

  **alexblue** 3 years ago

but it says "login at the same time"...so answer is C, up to 5 allowed

upvoted 1 times

  **kthekillerc** 3 years, 3 months ago



correction correct answer is C up to 5 devices are allowed on at the same time.

upvoted 1 times

  **kthekillerc** 3 years, 8 months ago

Provided answer is correct



upvoted 1 times

  **Skiliffi** 4 years, 7 months ago

Not sure but mb C is correct. Consider guide linked below, by default there is no limits for simultaneous logins



<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-22/204463-Configure-Maximum-Concurrent-User-Session.html#anc24>

upvoted 3 times

  **cvndani** 2 years, 9 months ago

I tested on my ISE version 2.7, by default checkbox maximum simultaneous logins are 3 and checked, and disconnect the oldest connection, so the A answer is the correct.

upvoted 4 times

  **Igur** 4 years, 7 months ago

Just tested it in my lab. By creating as new guest type the default settings are: Maximum simultaneous logins = 3; Disconnect oldest connection = enable.

So, the A should be correct

upvoted 8 times

  **stardust82** 3 years, 11 months ago

But oldest is not the last one. Even if you can configure it. This is a typical cisco question which is hard to answer

upvoted 2 times

What is an important consideration when implementing a dual SSID design for BYOD?

- A. After using the provisioning SSID, an ACL that used to make the client switch SSIDs forces the user to associate and traverse the network by MAC filtering.
- B. If multiple WLCs are used, the WLAN IDs must be exact for the clients to be provisioned and traverse the network correctly.
- C. SSIDs for this setup must be configured with NAC State-RADIUS NAC for the clients to authenticate with Cisco ISE, or with NAC State-ISE NAC for Cisco ISE to associate the client.
- D. One SSID is for provisioning and the other SSID is for gaining access to the network. The use of an ACL should not be enforced to make the client connect to the REAL SSID after provisioning.

Suggested Answer: D

  **Skliffi** Highly Voted 4 years, 7 months ago

B is correct:

"When implementing BYOD solutions using more than one Wireless LAN Controller, WLAN IDs must be kept consistent. WLAN ID is used by ISE in determining which WLAN (SSID) clients are using to connect to the network. Ensuring each WLAN has the same WLAN ID on each WLC is essential for proper operation and security."

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_Wireless.html

upvoted 8 times

  **Pawnstar** 3 years, 8 months ago

The question doesn't mention more than one controller though?

upvoted 7 times

  **Sorvahr** Highly Voted 4 years, 8 months ago

Correct answer is B.

upvoted 5 times

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

Selected Answer: B

Option B ("If multiple WLCs are used, the WLAN IDs must be exact") is actually a valid statement in the context of a multi-WLC BYOD deployment.



Option D is also correct, as it highlights the two-SSID approach, which is a fundamental aspect of BYOD onboarding.

Thus, the best answer in a multi-WLC BYOD setup would be:

✓ B and D together.

Good job Cisco! FU



upvoted 1 times

  **Ocsicccnp** 8 months, 4 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

  **Ocsicccnp** 8 months, 4 weeks ago

Selected Answer: A

A

upvoted 1 times

  **[Removed]** 1 year, 8 months ago

B and C are not the correct considerations because:

Option B states that if multiple Wireless LAN Controllers (WLCs) are used, the WLAN IDs must be exact for the clients to be provisioned and traverse the network correctly. However, the consideration for implementing a dual SSID design for BYOD does not necessarily depend on the use of multiple WLCs.

Option C states that the SSIDs for this setup must be configured with specific NAC (Network Access Control) settings for the clients to authenticate with Cisco ISE (Identity Services Engine). While NAC may be a consideration in a BYOD implementation, it is not specifically related to the use of dual

SSIDs.

Going with D

upvoted 2 times

🗲️ 👤 **AhcMez** 1 year, 11 months ago

C is the correct one .

upvoted 1 times

🗲️ 👤 **kthekillerc** 3 years, 8 months ago

Provided answer is correct

upvoted 4 times

🗲️ 👤 **Giuspe** 3 years, 8 months ago

B is the right answer

upvoted 3 times

🗲️ 👤 **kosminsmile** 3 years, 11 months ago

Centralized Campus—Dual SSID Design

n this design there are two SSIDs: one provides enrollment/provisioning and the other provides secure network access. After connecting to the BYOD_Provisioning SSID and completing the enrollment and provisioning steps, the user connects to the BYOD_Employee SSID, which provides network access over a secure EAP-TLS connection.

upvoted 5 times

🗲️ 👤 **Pavs0490** 3 years, 9 months ago

"After the device is provisioned, it is assumed that the user will switch to the second SSID for regular network access. To prevent the user from staying connected to the provisioning SSID, an access list that provides only access to ISE, DHCP, and DNS must be enforced on the provisioning SSID."

upvoted 3 times

🗲️ 👤 **maro_moh** 4 years, 4 months ago

Correct answer is A

upvoted 1 times

Refer to the exhibit. A network administrator deploys the DHCP profiler service in two ISE servers: 10.3.10.101 and 10.3.10.102. All BYOD devices connecting to WLAN on VLAN63 have been incorrectly profiled and are assigned as unknown profiled endpoints. Which action efficiently rectifies the issue according to Cisco recommendations?

```
(Cisco WLC) >show dhcp proxy
DHCP ProxyBehaviour: enabled
!
interface Vlan63
ip address 10.10.63.252/22
description Dot1x_BYOD
no shutdown
!
```

- A. Nothing needed to be added on the Cisco WLC or VLAN interface. The ISE configuration must be fixed.
- B. Disable DHCP proxy on the Cisco WLC.
- C. Disable DHCP proxy on the Cisco WLC and run the ip helper-address command under the VLAN interface to point to DHCP and the two ISE servers.
- D. Keep DHCP proxy enabled on the Cisco WLC and define helper-address under the VLAN interface to point to the two ISE servers.

Suggested Answer: C

Community vote distribution

C (50%)

A (50%)

rrahim 4 months, 1 week ago

Selected Answer: C

C. Disable DHCP proxy on the Cisco WLC and run the ip helper-address command under the VLAN interface to point to DHCP and the two ISE servers.

The issue arises because the DHCP proxy feature on the Cisco WLC is intercepting DHCP requests, preventing them from reaching the ISE servers for profiling. To resolve this, the DHCP proxy must be disabled on the WLC, and the ip helper-address command must be configured on the VLAN interface to forward DHCP requests to both the DHCP server and the ISE servers.

upvoted 1 times

Le91 8 months ago

Selected Answer: C

C is correct.

upvoted 1 times

Ocsicccnp 8 months, 4 weeks ago

Selected Answer: C

C

upvoted 1 times

obifunk 1 year ago

Selected Answer: C

C is correct.

<https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456>

upvoted 2 times

Hhj1 2 years, 5 months ago

May be C

Layer 3 ,not same subnet ,may be use ip helper address is better....

<https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/110865-dhcp-wlc.html>

upvoted 1 times

Aaron_0801 2 years, 5 months ago

Selected Answer: A

Answer should be A

<https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/110865-dhcp-wlc.html#anc0>

upvoted 2 times

  **kthekillerc** 3 years, 8 months ago

Provided answer is correct

upvoted 3 times

An engineer must implement a BYOD policy with these requirements:

- ⇒ Onboarding unknown machines
- ⇒ Easily scalable
- ⇒ Low overhead on the wireless network

Which method satisfies these requirements?

- A. triple SSID
- B. single SSID
- C. open SSID
- D. dual SSID

Suggested Answer: B

🗨️ 👤 **rrahim** 4 months, 1 week ago

Selected Answer: B

A Single SSID BYOD solution is the best method to meet the given requirements:

Onboarding Unknown Machines:

With a single SSID, all devices connect to the same SSID, and unknown devices are redirected to a captive portal for onboarding. Users are guided through the onboarding process to install certificates or perform necessary authentication steps.

Easily Scalable:

Since there's only one SSID, network management is simplified.

Unlike dual SSID or triple SSID approaches, there's no need to manage multiple SSIDs for different device states.

Low Overhead on the Wireless Network:

Fewer SSIDs = less overhead on the wireless network.

Each additional SSID increases management traffic, beacons, and channel contention.

A single SSID approach minimizes unnecessary wireless overhead.

upvoted 1 times

🗨️ 👤 **kthekillerc** 7 months, 2 weeks ago

Provided answer is correct

upvoted 2 times

🗨️ 👤 **cskshiet** 1 year ago

B is correct, see:

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_Wireless.html

upvoted 4 times

A company has a single WLAN configured for 802.1x authentication with the QoS set to Silver. This WLAN supports all corporate and BYOD access. A decision has been made to allow users to install Cisco Jabber on their personal mobile devices. Users report poor voice quality when using Jabber. QoS is being applied only as best effort. What must be configured to ensure that the WLAN remains on the Silver class and to ensure Platinum class for Jabber?

- A. Configure QoS on the mobile devices that have Jabber installed.
- B. Enable Cisco Centralized Key Management on the WLAN so that the Jabber-enabled devices will connect.
- C. Configure the WLAN to broadcast on 5 GHz radios only and allow Jabber users to connect.
- D. Configure an AVC profile for the Jabber traffic and apply it to the WLAN.

Suggested Answer: D

  **rrahim** 4 months, 1 week ago



Selected Answer: D

Since the WLAN is set to Silver QoS, all traffic—including Cisco Jabber—is treated as best effort, leading to poor voice quality. To ensure Cisco Jabber receives Platinum QoS (voice priority) while keeping the WLAN at Silver, an Application Visibility and Control (AVC) profile must be used.

Application Visibility and Control (AVC) allows the controller to identify and classify Jabber traffic separately from other traffic on the WLAN. Applying an AVC profile with the correct DSCP marking (e.g., EF - Expedited Forwarding) ensures Jabber traffic is prioritized without changing the overall WLAN QoS class.

This method ensures voice traffic gets Platinum QoS while keeping all other traffic at Silver.

upvoted 1 times

  **Ocsicccnp** 8 months, 4 weeks ago

Selected Answer: D

d

upvoted 1 times

  **kthekillerc** 3 years, 8 months ago

Provided answer is correct

upvoted 2 times

An engineer is implementing profiling for BYOD devices using Cisco ISE. When using a distributed model, which persona must the engineer configure with the profiling service?

- A. Device Admin Node
- B. Primary Admin Node
- C. Monitor Node
- D. Policy Services Node

Suggested Answer: D

Community vote distribution

B (100%)

🗳️ 👤 **AhcMez** Highly Voted 1 year, 11 months ago

Selected Answer: B

B is the Good answer . we can not configure anything directly on the policy node , we need to make it on the primary node .
upvoted 5 times

🗳️ 👤 **rrahim** Most Recent 4 months, 1 week ago

Selected Answer: D

In a distributed Cisco ISE deployment, the Policy Services Node (PSN) is responsible for profiling and making policy decisions based on the collected device attributes.

Profiling service in ISE gathers device characteristics (e.g., MAC address, DHCP requests, HTTP headers) and classifies BYOD devices (e.g., iPhones, Androids, laptops).

PSNs handle RADIUS authentication, authorization, and profiling services in a distributed ISE model.

The profiling service must be enabled on the PSN that will process endpoint traffic.

upvoted 1 times

🗳️ 👤 **steffel1972** 4 months, 4 weeks ago

Selected Answer: D

D is the right answer
upvoted 1 times

🗳️ 👤 **GOfeni** 8 months ago

Selected Answer: D

Question is not clearly written in my opinion. Any configuration is indeed performed on a PAN, however, SERVICES can only be enabled on a PSN. Since the question is regarding the profiling service, it will be enabled on a PSN.
upvoted 2 times

🗳️ 👤 **Le91** 8 months ago

Selected Answer: D

D is the right answer
upvoted 1 times

🗳️ 👤 **Le91** 8 months ago

Selected Answer: D

Answer is D
upvoted 1 times

🗳️ 👤 **5db1f59** 8 months, 3 weeks ago

Selected Answer: D

Answer is D:

<https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456#toc-hld--942339322>

upvoted 1 times

🗳️ 👤 **Ocsiccnp** 9 months, 1 week ago

Selected Answer: D

Answer D

upvoted 1 times

  **Gumpy1** 1 year, 1 month ago

Selected Answer: B

You log into the Admin node and make the profile, the PSN-Policy Service Node carries out the directions received from the Admin Node.

upvoted 1 times

  **Gumpy1** 1 year, 1 month ago

I re-read the question (tricky-not clear to me)...It is actually D as written. You do the changes on the PAN, but on the PSN Persona, you click the tick box for policy service>enable profiling service. Here is an article to help.

<https://community.cisco.com/t5/security-knowledge-base/ise-profiling-design-guide/ta-p/3739456#toc-hld-55974052>

upvoted 2 times

  **kthekillerc** 3 years, 7 months ago

Provided answer is correct

upvoted 3 times

DRAG DROP -

The network management team in a large shopping center has detected numerous rogue APs from local coffee shops that are broadcasting SSIDs. All of these

SSIDs have names starting with ATC (for example, ATC302, ATC011, and ATC566). A wireless network engineer must appropriately classify these SSIDs using the Rogue Rules feature. Drag and drop the options from the left onto the categories in which they must be used on the right. Not all options are used.

Select and Place:

Answer Area

friendly	Type
malicious	
set substring-ssid to ATC	State
set SSID value to ATC	
external	Condition
internal	

Answer Area

Suggested Answer:

friendly	Type
malicious	friendly
set substring-ssid to ATC	State
set SSID value to ATC	external
external	Condition
internal	set SSID value to ATC

c9800 Highly Voted 2 years, 4 months ago

correct answer should be:

Type = External

State = Friendly

Condition = set substring-ssid

<https://community.cisco.com/t5/wireless/wildcard-or-regex-in-rogue-ap-rules/td-p/2620976>
upvoted 10 times

Lislot 1 year, 11 months ago

Thanks for the reference, c9800, but this reference shows:

Type: Friendly

State: External

Condition: set substring-ssid

upvoted 11 times

  **bombero**  2 years, 11 months ago



<https://mrnciew.files.wordpress.com/2013/06/rogue-ap-03.png>

upvoted 10 times

  **GoldLeader**  11 months, 2 weeks ago

Answer A. - SSID Wildcard—Requires that the rogue access point have a substring of the specific user-configured SSID. The controller searches the substring in the same occurrence pattern and returns a match if the substring is found in the whole string of an SSID.

upvoted 1 times

  **PauBau** 1 year, 2 months ago

Type: friendly

State: external

Condition: set substring-ssid to ATC (all start with ATC, so just sub-string)

upvoted 1 times

  **cvndani** 1 year, 9 months ago

Provided answer is correct.

upvoted 1 times

  **Coffee313** 2 years, 6 months ago

Why the condition is "set SSID" instead of "set substring-ssid"? I think that the condition should be different.

upvoted 1 times

  **kthekillerc** 2 years, 7 months ago

Provided answer is correct.

upvoted 1 times

  **Hugh_Jazz** 3 years ago

Correct mappings for top two are:

Type = External

State = Friendly

upvoted 1 times

What must be configured on ISE version 2.1 BYOD when using Single SSID?


- A. open authentication
- B. 802.1x
- C. no authentication
- D. WPA2

Suggested Answer: B

Community vote distribution

B (50%)

A (50%)

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

Provided answer is correct, the question is what is configured on ISE not the WLC where WPA2 is configured.
upvoted 6 times

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

Selected Answer: B

When using a Single SSID for BYOD (Bring Your Own Device) with Cisco ISE version 2.1, 802.1X authentication must be configured. This ensures that devices are properly authenticated and authorized before gaining access to the network, while also allowing for seamless onboarding and provisioning.

Explanation of the options:

A. open authentication:

This is incorrect. Open authentication is insecure and does not provide the necessary control for BYOD onboarding and network access.

B. 802.1x:

This is correct. 802.1X authentication is required for a Single SSID BYOD design to ensure secure authentication and authorization of devices.

upvoted 1 times

 **rrahim** 4 months, 2 weeks ago

Selected Answer: A

Open Authentication is typically used in the initial phase of a BYOD deployment with a Single SSID. It allows devices to connect to the network without requiring credentials initially, enabling them to onboard and register with the ISE server.

After the device is onboarded, more secure authentication methods (e.g., 802.1X or WPA2) can be enforced for subsequent connections.

Why not the others?

B. 802.1x: This is a secure authentication method but is not used in the initial phase of BYOD onboarding with a Single SSID.

C. No Authentication: This is not a valid configuration for BYOD deployments, as some form of authentication is required for security.

D. WPA2: This is a security protocol for Wi-Fi networks but is not used in the initial phase of BYOD onboarding with a Single SSID.

upvoted 1 times

 **raphim** 8 months, 2 weeks ago

Selected Answer: B

The question text want to know the config on ISE not on WLC - so it must be B

upvoted 1 times


 **CHERIFNDIAYE** 1 year ago

Selected Answer: A

the correct answer is A :



<https://community.cisco.com/t5/security-knowledge-base/ise-byod-dual-vs-single-ssid-onboarding/ta-p/3641422>

upvoted 1 times

  **cvndani** 1 year, 9 months ago

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216535-configure-single-ssid-wireless-byod-on-w.html>

upvoted 3 times

  **Giuspe** 2 years, 8 months ago


Answer is D

upvoted 1 times

A wireless engineer must implement a corporate wireless network for a large company in the most efficient way possible. The wireless network must support 32 VLANs for 300 employees in different departments. Which solution must the engineer choose?

- A. Configure a second WLC to support half of the APs in the deployment.
- B. Configure one single SSID and implement Cisco ISE for VLAN assignment according to different user roles.
- C. Configure different AP groups to support different VLANs, so that all of the WLANs can be broadcast on both radios.
- D. Configure 16 WLANs to be broadcast on the 2.4-GHz band and 16 WLANs to be broadcast on the 5.0-GHz band.

Suggested Answer: B

  **rrahim** 4 months, 2 weeks ago

Selected Answer: B

Single SSID with VLAN Assignment:

Using a single SSID simplifies the wireless network configuration and improves user experience. Employees can connect to the same SSID regardless of their department or role.

Cisco Identity Services Engine (ISE) can dynamically assign users to the appropriate VLAN based on their role, credentials, or other attributes (e.g., department, device type, or security posture). This eliminates the need to configure multiple SSIDs or AP groups for each VLAN.

Scalability and Manageability:

A single SSID reduces the complexity of managing multiple SSIDs and ensures consistent wireless coverage.

Cisco ISE provides centralized policy enforcement, making it easier to manage VLAN assignments and security policies for a large number of users.

Efficient Use of Wireless Resources:

Broadcasting fewer SSIDs reduces airtime overhead and improves wireless performance.

Dynamically assigning VLANs based on user roles ensures that employees are placed on the correct network segment without manual intervention.

upvoted 1 times

  **kthekillerc** 7 months, 2 weeks ago

Provided answer is correct

upvoted 3 times

Which feature on the Cisco Wireless LAN Controller must be present to support dynamic VLAN mapping?

- A. FlexConnect ACL
- B. VLAN name override
- C. CCKM/OKC
- D. AAA override

Suggested Answer: D




  **skh**  4 years, 4 months ago

D correct AAA override

[https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-](https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010010000.html)

[4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010010000.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010010000.html)



upvoted 5 times

  **rrahim**  4 months, 1 week ago

Selected Answer: D

To support dynamic VLAN mapping on a Cisco Wireless LAN Controller (WLC), the AAA override feature must be enabled. This feature allows the WLC to apply VLAN assignments dynamically based on the attributes (such as user roles or group memberships) received from the RADIUS server (e.g., Cisco ISE) during authentication.

upvoted 1 times

  **Ocsiccnnp** 8 months, 4 weeks ago

Selected Answer: D

From the Advance tab, enable the Allow AAA Override check box to override the WLC configuration when the RADIUS server returns the attributes needed to place the client on the proper VLAN as shown in the image:

upvoted 1 times

  **kthekillerc** 3 years, 8 months ago


Provided answer is correct

upvoted 4 times

Which three properties are used for client profiling of wireless clients? (Choose three.)

- A. HTTP user agent
- B. DHCP
- C. MAC OUI
- D. hostname
- E. OS version
- F. IP address

Suggested Answer: ABC

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

Answer is correct

upvoted 5 times

 **skh** Highly Voted 10 months, 4 weeks ago

Answer is correct

The user can configure these policies and enforce end-points with specified policies. The wireless clients will be profiled based on MAC OUI, DHCP, HTTP user agent (valid Internet is required for successful HTTP profiling). The WLC uses these attributes and predefined classification profiles to identify devices.

<https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7-5/NativeProfiling75.html>

upvoted 5 times

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

Selected Answer: ABC

A. HTTP user agent:

This is correct. The HTTP user agent string provides information about the device's browser and operating system, which is useful for profiling.

B. DHCP:

This is correct. DHCP options and requests can provide information about the device type, vendor, and other attributes.

C. MAC OUI:

This is correct. The MAC OUI (Organizationally Unique Identifier) identifies the manufacturer of the device, which is a key attribute for profiling.

D. hostname:

While the hostname can provide some information, it is not as reliable or specific as the other options for profiling.

E. OS version:

The OS version is useful for profiling but is typically derived from other attributes like the HTTP user agent or DHCP.

F. IP address:

The IP address is not used for profiling as it does not provide information about the device type or characteristics.

upvoted 1 times

Which command set configures a Cisco Catalyst 9800 Series Wireless Controller so that the client traffic enters the network at the AP switch port?

A.

```
config terminal
wireless profile policy [policy name]
local switching
end
```

B.

```
config terminal
wireless flexconnect policy [policy name]
local switching
end
```

C.

```
config terminal
wireless flexconnect policy [policy name]
no central switching
end
```

D.

```
config terminal
wireless profile policy [policy name]
no central switching
end
```

Suggested Answer: D

  **Sorvahr**  2 years, 2 months ago

Wrong. Correct answer is D




upvoted 12 times

  **iamccie**  1 year, 9 months ago

Agreed, the correct answer is D :

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213945-understand-flexconnect-on-9800-wireless.html>

upvoted 5 times

  **kthekillerc**  1 year ago



D is the suggested correct answer???

upvoted 3 times

  **kthekillerc** 1 year, 1 month ago

Provided answer is correct

upvoted 2 times

  **skh** 1 year, 10 months ago

Correct answer is D

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/flexconnect.html

upvoted 4 times

What is the default IEEE 802.1x AP authentication configuration on a Cisco Catalyst 9800 Series Wireless Controller?

- A. EAP-PEAP with 802.1x port authentication
- B. EAP-TLS with 802.1x port authentication
- C. EAP-FAST with CAPWAP DTLS + port authentication
- D. EAP-FAST with CAPWAP DTLS

Suggested Answer: C

Community vote distribution

D (82%)

C (18%)

🗳️ 👤 **Profiteur** Highly Voted 3 years, 9 months ago

Checked on our WLC 9800. The default AP Join Profile has EAP-FAST with CAPWAP DTLS> I would go with answer D
upvoted 14 times

🗳️ 👤 **Guglielmino** Highly Voted 2 years, 9 months ago

Selected Answer: D

I tested in lab; the answer is certainly D.
upvoted 6 times

🗳️ 👤 **rrahim** Most Recent 4 months, 1 week ago

Selected Answer: D

The default IEEE 802.1X AP authentication configuration on a Cisco Catalyst 9800 Series Wireless Controller uses EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling) with CAPWAP DTLS (Datagram Transport Layer Security). This provides secure authentication and encryption for communication between the AP and the controller.
upvoted 1 times

🗳️ 👤 **Gumpy1** 7 months, 4 weeks ago

Selected Answer: C

I am going with C
How can you not have port authentication using dot1x which points to a AAA Radius Server. Without having the configs set on the port- ours is global on the switch- how does a client get authenticated?
upvoted 1 times

🗳️ 👤 **Gumpy1** 7 months, 3 weeks ago

Ah, but it does say "on a 9800 controller", the port config would be on the switch. So I would then say D
upvoted 1 times

🗳️ 👤 **qwertyEDCA** 1 year ago

Selected Answer: D

Answer is D 100%
upvoted 1 times

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

The default IEEE 802.1x AP authentication configuration on a Cisco Catalyst 9800 Series Wireless Controller is EAP-PEAP with 802.1x port authentication, not EAP-FAST with CAPWAP DTLS.
upvoted 1 times

🗳️ 👤 **copa77** 1 year, 11 months ago

Selected Answer: C

Look at section - Verifying the Authentication Type makes it look like C
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-10/config-guide/b_wl_17_10_cg/m_data_dtls.pdf
upvoted 1 times

🗳️ 👤 **copa77** 1 year, 11 months ago

Look at section - Verifying the Authentication Type makes it look like C
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-10/config-guide/b_wl_17_10_cg/m_data_dtls.pdf
upvoted 1 times

🗨️ 👤 **Robesera** 2 years, 2 months ago

Just verified on the 9800, AP Join Profile. Correct answer is D, EAP-FAST with CAPWAP DTLS
upvoted 2 times

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

Selected Answer: D

The correct answer is D
upvoted 2 times

🗨️ 👤 **kthekillerc** 3 years ago

<https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/guide-c07-743627.html> Port authentication needs performed on the switch for Aps to work with 802.1x attached is the link and the config for your switchports.
upvoted 1 times

🗨️ 👤 **alexblue** 2 years, 6 months ago

I don't agree. It doesn't say anywhere that is mandatory. The opposite, it says it is very flexible and that it can be applied to a certain group of APs is desired.

I would go with D, even if someone or the exam correctors say NOT.

I have also applied for the Cisco learning course and labs and it is not mandatory
upvoted 1 times

🗨️ 👤 **MarMar912** 3 years ago

correct answer is "EAP-FAST with CAPWAP DTLS". I verified that in software 17.3.3.
upvoted 2 times

🗨️ 👤 **kthekillerc** 3 years, 1 month ago

Provided answer is correct
upvoted 1 times

🗨️ 👤 **Cyrillka** 3 years, 3 months ago

D is correct
default ap profile
upvoted 3 times

🗨️ 👤 **maro_moh** 3 years, 10 months ago

is it correct ???
upvoted 1 times

An engineer must implement rogue containment for an SSID. What is the maximum number of APs that should be used for containment?

- A. 1
- B. 2
- C. 3
- D. 4

Suggested Answer: D

Reference:

https://www.cisco.com/c/en/us/td/docs/wireless/technology/roguedetection_deploy/Rogue_Detection.html




  **skh**  3 years, 4 months ago

correct

An individual rogue device can be contained by 1 to 4 managed APs which work in conjunction to mitigate the threat temporarily.

<https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html>

upvoted 5 times

  **DiegoECUIO**  7 months, 3 weeks ago

An individual rogue device can be contained by 1 to 4 managed APs which work in conjunction to mitigate the threat temporarily.

upvoted 1 times

  **kthekillerc** 2 years, 7 months ago

Provided answer is correct

upvoted 2 times

An engineer is following the proper upgrade path to upgrade a Cisco AireOS WLC from version 7.3 to 8.9. Which two ACLs for Cisco CWA must be configured when upgrading from the specified codes? (Choose two.)

- A. Permit 0.0.0.0 0.0.0.0 any DNS any
- B. Permit 0.0.0.0 0.0.0.0 UDP DNS any
- C. Permit 0.0.0.0 0.0.0.0 UDP any DNS
- D. Permit any any any
- E. Permit 0.0.0.0 0.0.0.0 UDP any any

Suggested Answer: BC

Reference:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html>

Community vote distribution

CE (100%)

 **rrahim** 4 months, 2 weeks ago

Selected Answer: BC

- B. Permit 0.0.0.0 0.0.0.0 UDP DNS any
- C. Permit 0.0.0.0 0.0.0.0 UDP any DNS

Explanation:

Permit 0.0.0.0 0.0.0.0 UDP DNS any:

This ACL allows DNS traffic (UDP port 53) from any source to any destination. DNS is required for resolving hostnames during the CWA process.

Permit 0.0.0.0 0.0.0.0 UDP any DNS:

This ACL allows DNS traffic (UDP port 53) from any source to any destination. It ensures that DNS queries and responses are permitted, which is critical for CWA to function properly.

upvoted 1 times

 **rrahim** 4 months, 2 weeks ago

Why the Other Options Are Incorrect:

A. Permit 0.0.0.0 0.0.0.0 any DNS any:

This ACL is incorrect because it uses any instead of specifying UDP for DNS traffic. DNS uses UDP (and sometimes TCP), but this ACL is too broad and not specific enough.


D. Permit any any any:

This ACL is overly permissive and not recommended for CWA. It allows all traffic, which is not necessary and could pose a security risk.

E. Permit 0.0.0.0 0.0.0.0 UDP any any:

This ACL is too broad and not specific to DNS traffic. It allows all UDP traffic, which is not required for CWA and could lead to unnecessary traffic being permitted.

upvoted 1 times

 **Jason233** 1 year, 9 months ago

Selected Answer: CE

>permit 0.0.0.0 0.0.0.0 UDP any DNS

>permit 0.0.0.0 0.0.0.0 UDP any any

upvoted 1 times

  **Gumpy1** 7 months ago

I agree with Jason233, here is a power point slide that helps explain #47

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKEWN-2014.pdf>

upvoted 1 times



  **Jason233** 1 year, 9 months ago

Note: Earlier versions of WLC software such as 7.2 or 7.3 did not require you to specify Domain Name System (DNS), but later code versions require you to permit DNS traffic on that redirect ACL.

```
>permit 0.0.0.0 0.0.0.0 UDP any DNS
```

```
>permit 0.0.0.0 0.0.0.0 UDP any any
```

upvoted 1 times

  **cvndani** 2 years, 3 months ago

Provide answer is correct.

upvoted 2 times



CMX Facebook Wi-Fi allows access to the network before authentication. Which two elements are available? (Choose two.)

- A. Allow HTTP traffic only before authentication and block all the traffic.
- B. Allow all the traffic before authentication and intercept HTTPS only.
- C. Allow HTTPs traffic only before authentication and block all other traffic.
- D. Allow all the traffic before authentication and intercept HTTP only.
- E. Allow SNMP traffic only before authentication and block all the traffic.

Suggested Answer: CD

Reference:

https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/CMX_Connect_Engage_Visitor_Connect/Guide/Cisco_CMX_Connect_Engage_Config_Guide_VC/CMX_Facebook_Wi-Fi.html

  **masters777** 3 months, 1 week ago

Selected Answer: CD

see reference link: https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/CMX_Connect_Engage_Visitor_Connect/Guide/Cisco_CMX_Connect_Engage_Config_Guide_VC/CMX_Facebook_Wi-Fi.html

The following are the different options to choose for access before authentication:

Allow HTTPs traffic only before authentication and block all the traffic:

– To do this, click the sequence number whose Source Port or Dest Port has the value HTTPs. The Access Control Lists > Rules > Edit page appears and you can select Permit from the Action drop-down list and click Apply.

Allow all the traffic before authentication and intercept HTTP only.

– To intercept HTTP, click the sequence number whose Source Port or Dest Port has the value HTTP. The Access Control Lists > Rules > Edit page appears and you can select Deny from the Action drop-down list and click Apply.

upvoted 1 times

  **rrahim** 4 months, 2 weeks ago

Selected Answer: AD

A. Allow HTTP traffic only before authentication and block all the traffic.

D. Allow all the traffic before authentication and intercept HTTP only.

Explanation:

CMX Facebook Wi-Fi:

CMX Facebook Wi-Fi is a solution that allows users to access a wireless network by logging in via their Facebook credentials. Before authentication, limited access is provided to facilitate the login process.

Allow HTTP traffic only before authentication and block all the traffic:

This option allows users to access only HTTP traffic (unencrypted web traffic) before authentication. This is typically used to redirect users to the Facebook login page or a captive portal. All other traffic is blocked until authentication is completed.

Allow all the traffic before authentication and intercept HTTP only:

This option allows all traffic before authentication but intercepts HTTP traffic to redirect users to the Facebook login page or captive portal. This ensures that users can still access other services (e.g., DNS) while being redirected for authentication.



upvoted 1 times

  **rrahim** 4 months, 2 weeks ago

C. Allow HTTPS traffic only before authentication and block all other traffic:

Allowing only HTTPS traffic before authentication is not practical because the Facebook login page or captive portal typically uses HTTP for redirection.

upvoted 1 times

  **malkana** 10 months, 2 weeks ago

he following are the different options to choose for access before authentication:

Allow HTTPs traffic only before authentication and block all the traffic:

– To do this, click the sequence number whose Source Port or Dest Port has the value HTTPs. The Access Control Lists > Rules > Edit page appears and you can select Permit from the Action drop-down list and click Apply.

Allow all the traffic before authentication and intercept HTTP only.



– To intercept HTTP, click the sequence number whose Source Port or Dest Port has the value HTTP. The Access Control Lists > Rules > Edit page appears and you can select Deny from the Action drop-down list and click Apply.

upvoted 3 times

  **kthekillerc** 1 year, 1 month ago

Provided answer is correct

upvoted 2 times

  **drel** 1 year, 5 months ago

Correct

https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/www.cisco.com/content/en/us/td/docs/wireless/mse/8-0/CMX_Connect_Engage_Visitor_Connect/Guide/Cisco_CMX_Connect_Engage_Config_Guide_VC/CMX_Facebook_Wi-Fi.html.xml

upvoted 2 times

An engineer is implementing Cisco Identity-Based Networking on a Cisco AireOS controller. The engineer has two ACLs on the controller. The first ACL, named BASE_ACL, is applied to the corporate_clients interface on the WLC, which is used for all corporate clients. The second ACL, named HR_ACL, is referenced by ISE in the Human Resources group policy. What is the resulting ACL when a Human Resources user connects?

- A. HR_ACL appended with BASE_ACL
- B. HR_ACL only
- C. BASE_ACL appended with HR_ACL
- D. BASE_ACL only

Suggested Answer: B

  **rrahim** 4 months, 2 weeks ago

Selected Answer: B

B. HR_ACL only

Explanation:



Cisco Identity-Based Networking (IBN):

In Cisco IBN, Access Control Lists (ACLs) are used to enforce policies based on user roles or groups. When a user connects to the network, the ACL associated with their role or group is applied.

ACL Application:

The ACL referenced by Cisco ISE (Identity Services Engine) in the user's group policy takes precedence over any ACL applied to the interface. This means that when a Human Resources (HR) user connects, the HR_ACL (referenced by ISE) is applied, and the BASE_ACL (applied to the corporate_clients interface) is overridden.

upvoted 1 times

  **Pawnstar** 9 months, 2 weeks ago

Answer is correct.

upvoted 2 times

Branch wireless users report that they can no longer access services from head office but can access services locally at the site. New wireless users can associate to the wireless while the WAN is down. Which three elements (Cisco FlexConnect state, operation mode, and authentication method) are seen in this scenario? (Choose three.)

- A. authentication-local/switch-local
- B. WPA2 personal
- C. authentication-central/switch-central
- D. lightweight mode
- E. standalone mode
- F. WEB authentication

Suggested Answer: ABE

🗲️ 👤 **rrahim** 4 months, 1 week ago

Selected Answer: ABE

- ✓ A. authentication-local/switch-local → Since the WAN is down, authentication and traffic switching are happening locally.
 - ✓ B. WPA2 personal → WPA2-PSK (Personal) does not require centralized authentication, allowing new users to still connect.
 - ✓ E. standalone mode → When the WAN is down, FlexConnect operates in standalone mode, meaning the AP functions independently.
- upvoted 2 times

🗲️ 👤 **rrahim** 4 months, 2 weeks ago

Selected Answer: ADF

- A. authentication-local/switch-local
- D. lightweight mode
- F. WEB authentication

Explanation:

authentication-local/switch-local:

This indicates that the FlexConnect AP is configured to perform local authentication and switching. This allows wireless users to access local resources even when the WAN connection to the central controller is down.

lightweight mode:

The APs are operating in lightweight mode, meaning they are managed by a central wireless LAN controller (WLC). FlexConnect is a feature of lightweight APs that allows them to operate in a semi-autonomous manner when the WAN connection to the WLC is unavailable.

WEB authentication:

WEB authentication (captive portal) is often used in branch offices to authenticate users locally without requiring a connection to the central controller. This allows new users to associate with the wireless network even when the WAN is down.

upvoted 1 times

🗲️ 👤 **kthekillerc** 10 months, 2 weeks ago

provided answer is correct

upvoted 4 times

```
(Cisco Controller) >
(Cisco Controller) >*EAP Framework: Jan 21 23:55:43.569: eap_fast.c-EVENT: New context (EAP handle = c4000000)
*EAP Framework: Jan 21 23:55:43.569: eap_fast.c-EVENT: Allocated new EAP-FAST context (handle = 37000000)
*EAP Framework: Jan 21 23:55:43.569: eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle = c4000000)
*EAP Framework: Jan 21 23:55:43.569: eap_fast_auth.c-AUTH-EVENT: Received Identity
*EAP Framework: Jan 21 23:55:43.569: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV (436973636f0000000000000000000000)
*EAP Framework: Jan 21 23:55:43.569: eap_fast_auth.c-AUTH-EVENT: Sending Start
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle = c4000000)
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Start
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Ignoring unknown ext rec type: 10
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Ignoring unknown ext rec type: 11
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA proposed...
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: TLS_RSA_WITH_AES_128 proposed...
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: TLS_RSA_WITH_RC4_128 proposed...
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Proposed ciphersuite(s):
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 255
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 49188

*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 103
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 57
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT:      TLS_DHE_RSA_WITH_AES_128_CBC_SHA
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 22
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 61

*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT:      TLS_RSA_WITH_AES_128_CBC_SHA
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: Unknown ciphersuite 10
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: Unknown ciphersuite 49159
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: Unknown ciphersuite 49169
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT:      TLS_RSA_WITH_RC4_128_SHA
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: Unknown ciphersuite 4
*EAP Framework: Jan 21 23:55:43.592: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b)
*EAP Framework: Jan 21 23:55:43.592: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b
*EAP Framework: Jan 21 23:55:43.592: eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle = c4000000)
*EAP Framework: Jan 21 23:55:43.592: eap_fast_auth.c-AUTH-EVENT: Received ACK from peer
*EAP Framework: Jan 21 23:55:43.592: eap_fast.c-EVENT: Free context (EAP handle = c4000000)
```

Refer to the exhibit. An engineer deployed a Cisco WLC using local EAP. Users who are configured for EAP-PEAP cannot connect to the network. Based on the local EAP debug on the controller provided, why is the client unable to connect?

- A. The client is failing to accept certificate.
- B. The Cisco WLC is configured for the incorrect date.
- C. The Cisco WLC local EAP profile is misconfigured.
- D. The user is using invalid credentials.

Suggested Answer: A

Community vote distribution

C (86%)

14%

HOT2012 Highly Voted 3 years, 1 month ago

C correct

upvoted 7 times

Caradum Highly Voted 2 years, 5 months ago

Selected Answer: C

User is configured for PEAP authentication. WLC starts EAP-FAST context (Line 3). -> EAP Profile on the WLC needs to be corrected to use PEAP. So C should be correct.

upvoted 6 times

rrahim Most Recent 4 months, 2 weeks ago

Selected Answer: A

A. The client is failing to accept the certificate.

Explanation:

EAP-PEAP Authentication:

EAP-PEAP (Protected Extensible Authentication Protocol) relies on a server certificate to establish a secure TLS tunnel for authentication. If the client cannot validate or accept the server certificate, the authentication process will fail.

Debug Output Analysis:

The debug output shows the EAP-FAST process, but it does not indicate any issues with the EAP profile configuration or user credentials.

The absence of errors related to invalid credentials or misconfiguration suggests that the issue lies with the certificate exchange between the client and the server.

Common Causes for Certificate Issues:

The server certificate may be self-signed or issued by an untrusted Certificate Authority (CA), causing the client to reject it.

The client may not have the necessary root CA certificate installed to validate the server certificate.

The server certificate may be expired or have an incorrect Common Name (CN) or Subject Alternative Name (SAN).

upvoted 1 times

  **rrahim** 4 months, 2 weeks ago

Why the Other Options Are Incorrect:

B. The Cisco WLC is configured for the incorrect date:

While an incorrect date on the WLC could cause certificate validation issues, this scenario is less common and would typically affect all clients, not just those using EAP-PEAP.



C. The Cisco WLC local EAP profile is misconfigured:

The debug output does not indicate any misconfiguration in the EAP profile. If the profile were misconfigured, the debug logs would likely show errors related to the EAP method or parameters.

D. The user is using invalid credentials:

The debug output does not show any authentication failures related to invalid credentials. If the credentials were incorrect, the logs would indicate a failure during the authentication phase.

upvoted 1 times

  **Gumpy1** 7 months, 4 weeks ago

Selected Answer: A

I say answer provided is correct, A

The local Eap policy can include Eap-Fast and PEAP, but the debug output is barking about the ciphersuite. Using Local EAP the certificate has to be on the controller and the client. The controller offers its options, but the client has to accept one. See Cisco doc:

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215026-local-eap-authentication-on-catalyst-980.html#toc-hld-396697388>

upvoted 1 times

  **ahmedshahas** 1 year, 1 month ago

Correct C

upvoted 1 times

  **ahmedshahas** 1 year, 1 month ago

Can I get Oyeah?

upvoted 1 times

An engineer set up identity-based networking with ISE and configured AAA override on the WLAN. Which two attributes must be used to change the client behavior from the default settings? (Choose two.)

- A. DHCP timeout
- B. DNS server
- C. IPv6 ACL
- D. DSCP value
- E. multicast address

Suggested Answer: CD

 **cskshiet** Highly Voted 6 months, 4 weeks ago

Correct:

The AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.

AAA Override for IPv6 ACLs

In order to support centralized access control through a centralized AAA server such as the Cisco Identity Services Engine (ISE) or ACS, the IPv6 ACL can be provisioned on a per-client basis using AAA Override attributes. In order to use this feature, the IPv6 ACL must be configured on the controller and the WLAN must be configured with the AAA Override feature enabled. The actual named AAA attribute for an IPv6 ACL is Airespace-IPv6-ACL-Name, which is similar to the Airespace-ACL-Name attribute that is used for provisioning an IPv4-based ACL. The AAA attribute returned contents should be a string equal to the name of the IPv6 ACL as configured on the controller.

upvoted 10 times

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

Selected Answer: CD

IPv6 ACL:

ISE can dynamically assign an IPv6 Access Control List (ACL) to a client based on its identity or role. This allows for granular control over the traffic that the client is allowed to send or receive.

DSCP Value:

ISE can assign a Differentiated Services Code Point (DSCP) value to the client's traffic. This allows for prioritization or marking of the client's traffic based on its identity or role, which is useful for Quality of Service (QoS) policies.

upvoted 1 times

☒ **RADIUS Authentication Settings**

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret **Show**

Enable KeyWrap ☒ ⓘ

* Key Encryption Key **Show**

* Message Authenticator Code Key **Show**

Key Input Format ☐ ASCII ☒ HEXADECIMAL

CoA Port **Set To Default**

Refer to the exhibit. The security team has implemented ISE as an AAA solution for the wireless network. The wireless engineer notices that though clients are able to authenticate successfully, the ISE policies that are designed to place them on different interfaces are not working. Which configuration must be applied in the RADIUS Authentication Settings section from the ISE Network Device page?

- A. Disable KeyWrap.
- B. Use ASCII for the key input format.
- C. Change the CoA Port.
- D. Correct the shared secret.

Suggested Answer: C

Yod_Jjot 8 months, 1 week ago

Answer C is correct.

Port 1700 must be accessible for Cisco ISE
upvoted 3 times

kthekillerc 1 year, 7 months ago

Provided answer is correct
upvoted 4 times

An engineer is setting up a WLAN to work with a Cisco ISE as the AAA server. The company policy requires that all users be denied access to any resources until they pass the validation. Which component must be configured to achieve this stipulation?

- A. WPA2 passkey
- B. AAA override
- C. CPU ACL
- D. preauthentication ACL



Suggested Answer: B

  **Coffee313** Highly Voted 2 years, 9 months ago

I would say D is correct
upvoted 11 times

  **c9800** Highly Voted 2 years, 4 months ago

I think D is the correct answer
upvoted 6 times

  **GnXxUbik** Most Recent 3 weeks, 1 day ago

Selected Answer: D

D is correct
upvoted 1 times

  **rrahim** 4 months, 2 weeks ago

Selected Answer: D

Preauthentication ACL:

A preauthentication ACL (Access Control List) is used to restrict the resources that a client can access before they successfully authenticate. This ensures that users cannot access any network resources until they have passed the authentication process.

By configuring a preauthentication ACL, the engineer can enforce the company policy of denying access to all resources until the user is validated by the Cisco ISE (Identity Services Engine).

Why the Other Options Are Incorrect:

A. WPA2 passkey:

A WPA2 passkey is used for securing the wireless network with a pre-shared key (PSK). It does not control access to resources before or after authentication.

B. AAA override:

AAA override is used to dynamically assign VLANs or other attributes based on the user's role or identity after authentication. It does not restrict access before authentication.

C. CPU ACL:

A CPU ACL is used to control traffic destined for the CPU of the wireless LAN controller (WLC). It is not used to restrict user access to network resources before authentication.

upvoted 2 times

  **Ace_Pee** 1 year ago



I think only web auth supports preauth acls. So if its corp then i think AAA override as 802.1x/eap only allows EAP/auth traffic prio to being authenticated.

upvoted 3 times

  **kthekillerc** 2 years, 7 months ago

Provided answer is correct

upvoted 1 times

  **Cyrilka** 2 years, 9 months ago

D is correct

upvoted 6 times

A Cisco WLC has been added to the network and Cisco ISE as a network device, but authentication is failing. Which configuration within the network device configuration should be verified?

- A. SNMP RO community
- B. device interface credentials
- C. device ID
- D. shared secret

Suggested Answer: *D*

🗨️ 👤 **rrahim** 4 months, 2 weeks ago

Selected Answer: D

Shared Secret:

The shared secret is a key piece of configuration used for secure communication between the Cisco WLC and Cisco ISE. It must match on both devices for authentication to succeed.

If the shared secret is incorrect or mismatched, the WLC will not be able to authenticate with ISE, leading to authentication failures.

upvoted 1 times

🗨️ 👤 **Liselot** 11 months, 1 week ago



D is correct

upvoted 2 times

A user is trying to connect to a wireless network that is configured for WPA2-Enterprise security using a corporate laptop. The CA certificate for the authentication server has been installed on the Trusted Root Certification Authorities store on the laptop. The user has been prompted to enter the credentials multiple times, but the authentication has not succeeded. What is causing the issue?

- A. There is an IEEE invalid 802.1X authentication policy on the authentication server.
- B. The user Active Directory account is locked out after several failed attempts.
- C. There is an invalid 802.1X authentication policy on the authenticator.
- D. The laptop has not received a valid IP address from the wireless controller.

Suggested Answer: C

  **cisco_spo** Highly Voted 3 years, 6 months ago



This is a classic Cisco putting ambiguous questions that will have multiple right answers. The IP address response is incorrect and can be ruled out because DHCP occurs after a 802.1x authentication when the client is in the run state (assuming no WebAuth). That leaves an invalid authentication policy on the authenticator which it could be if they didn't define the AAA settings properly. It could be an account lockout as the user will not be notified if it's locked. The final option is an invalid authentication policy on the authentication server. All three of these could be right but I would choose the user account is locked because it says you are troubleshooting a user specific issue. The misconfigured authenticator or authentication server would have widespread problems affecting multiple users whereas the individual user account being locked would explain a user specific problem.

upvoted 21 times

  **Sorvahr** Highly Voted 3 years, 8 months ago

Wrong, correct answer is A



upvoted 9 times

  **claudio392** Most Recent 3 months, 1 week ago

Selected Answer: A

I suppose this answer

upvoted 1 times

  **rrahim** 4 months, 1 week ago

Selected Answer: B

The issue is likely caused by the user's Active Directory (AD) account being locked out after multiple failed authentication attempts. When a user enters incorrect credentials multiple times, many organizations have policies in place to lock the account temporarily or until an administrator unlocks it. This prevents unauthorized access but can also cause legitimate users to be locked out if they mistype their credentials.

upvoted 2 times

  **kthekillerc** 2 years, 7 months ago

Provided answer is correct

upvoted 1 times

  **Seba_o_s** 8 months ago

No, there indicate that "the authenticator", that mean the WLC, but the policy are configured in ISE or authentication server. Correct answer is A

upvoted 3 times

  **Pavs0490** 2 years, 9 months ago

I think it may be A.

"If the supplicant submits an invalid credential or is not allowed to access the network for policy reasons, the authentication server returns a RADIUS Access-Reject message with an encapsulated EAP-Failure message"

upvoted 3 times

A wireless engineer is configuring LWA using ISE. The customer is a startup company and requested the wireless users to authenticate against a directory, but LDAP is unavailable. Which solution should be proposed in order to have the same security and user experience?

- A. Use SAML.
- B. Use the internal database of the RADIUS server.
- C. Use a preshared key on the corporate WLAN.
- D. Use Novell eDirectory.

Suggested Answer: D

Community vote distribution

B (100%)

 **alexblue** Highly Voted 1 year ago

Answer should be B because if LDAP is unavaible, then cannot use Novell neither.

The following are valid with LDAP working:

You can choose any one of the following built-in schema types or create a custom schema:

Active Directory

Sun Directory Server

Novell eDirectory

You can click the arrow next to Schema to view the schema details.

If you edit the attributes of the predefined schema, Cisco ISE automatically creates a Custom schema.

upvoted 8 times

 **pan1234** Highly Voted 1 year, 7 months ago

it states ldap is unavailable..that includes novell

upvoted 6 times

 **twoplanker** Most Recent 7 months ago

Selected Answer: B

It's the internal database. Novell requires LDAP as well.

upvoted 2 times

 **joseph_climber** 1 year, 7 months ago

D


https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/m_extrnal_identity_store.html

upvoted 1 times

 **kthekillerc** 1 year, 7 months ago

Provided answer is correct

upvoted 1 times

 **Pawnstar** 1 year, 8 months ago

Answer is B

upvoted 3 times

 **cskshiet** 2 years ago

Should be B....ise has no integration with Novell.

upvoted 4 times

An engineer has implemented 802.1x authentication on the wireless network utilizing the internal database of a RADIUS server. Some clients reported that they are unable to connect. After troubleshooting, it is found that PEAP authentication is failing. A debug showed the server is sending an Access-Reject message.

Which action must be taken to resolve authentication?

- A. Use the user password that is configured on the server.
- B. Disable the server certificate to be validated on the client.
- C. Update the client certificate to match the user account.
- D. Replace the client certificates from the CA with the server certificate.

Suggested Answer: B

Community vote distribution

D (100%)

  **rrahim** 4 months, 2 weeks ago

Selected Answer: A

A. Use the user password that is configured on the server.

Explanation:

PEAP Authentication Failure:

PEAP (Protected Extensible Authentication Protocol) uses a server certificate to establish a secure TLS tunnel, but the actual user authentication is performed using credentials (username and password) stored in the RADIUS server's internal database.

If the RADIUS server sends an Access-Reject message, it indicates that the user credentials provided by the client do not match those configured on the server.

Root Cause:

The most common reason for an Access-Reject message during PEAP authentication is an incorrect username or password. The client may be providing credentials that do not match those stored in the RADIUS server's internal database.

Solution:

Ensure that the client is using the correct username and password as configured on the RADIUS server. This will resolve the authentication failure.
upvoted 2 times

  **GOfeni** 8 months ago

Selected Answer: A

PEAP is a Tunnel Method that only validates the Server certificate. Since the question mentions "the server is sending an Access-Reject message", it is understood the Server certificate has been validated successfully (therefore B is incorrect).

The question does not explicitly mention what Inner Method is being used, however it mentions the "internal database of a RADIUS server" is being used for Authentication, this means Username and Password are configured locally on the RADIUS server, since certificates are not supported with Internal Database (therefore C and D are incorrect).

In this case, some clients are using the wrong user password, and they need to use the password that have been configured on the server to solve the issue.

upvoted 2 times

  **[Removed]** 1 year, 8 months ago

Here is a quote from the Cisco documentation:

If PEAP authentication is failing and the server is sending an Access-Reject message, it is likely that the client certificate is not valid or does not match the user account. To resolve the issue, you can update the client certificate to match the user account. You can do this by using a certificate enrollment system or by manually installing the client certificate on the client device.

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 8 months ago

According to the Cisco documentation, the best solution to the problem is (C) Update the client certificate to match the user account.

upvoted 1 times

🗨️ 👤 **Ace_Pee** 2 years ago

RADIUS wont send an access reject if the certs are invalid if using PEAP mschapv2

upvoted 1 times

🗨️ 👤 **Zanjit500** 2 years ago

The server is not trusting the client, not the other way around.

Hence D.

upvoted 1 times

🗨️ 👤 **NoWiresIncluded** 2 years ago

Selected Answer: D



Disabling the Server Certificate check will work (B), but then you are not using PEAP, you are back to LEAP, and you have removed all the security benefits of that cert. You need to reload the server certificate onto the clients that are failing. Choice D.

upvoted 4 times

A customer wants to allow employees to easily onboard their personal devices to the wireless network. The visitors also must be able to connect to the same network without the need to engage with anyone from the reception desk. Which process must be configured on Cisco ISE to support this requirement?

- A. MAC authentication bypass
- B. native supplicant provisioning
- C. local web auth
- D. self-registration guest portal

Suggested Answer: D

  **rrahim** 4 months, 1 week ago

Selected Answer: D

To allow employees to easily onboard their personal devices and enable visitors to connect to the wireless network without assistance, the self-registration guest portal must be configured on Cisco ISE. This portal allows users to register their devices and gain network access without requiring intervention from IT or reception staff.

upvoted 1 times

  **DiegoECUIO** 7 months, 3 weeks ago

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216330-ise-self-registered-guest-portal-configu.html>

upvoted 1 times

A customer has a distributed wireless deployment model where the WLCs are located in the data centers. Because the file servers are located in the data center, the traffic from the corporate WLAN `Corp-401266017` must go through the controllers, where the guest WLAN `Guest-19283746` traffic must use the local Internet line installed in each office. Which configuration will accomplish this task?

- A. Disable Local Switching for the corporate and guest WLAN.
- B. Disable Local Switching for the corporate WLAN and enable it for the guest WLAN.
- C. Enable Local Switching for the corporate and guest WLAN.
- D. Enable Local Switching for the corporate WLAN and disable it for the guest WLAN.

Suggested Answer: D

Community vote distribution

B (100%)

cvndani **Highly Voted** 2 years, 3 months ago

Selected Answer: B

B is correct answer

upvoted 6 times

joand3512004 **Most Recent** 9 months, 1 week ago

Selected Answer: B

B is correct!

upvoted 1 times

DiegoECUIO 1 year, 1 month ago

D is correct, you wouldn't give access to corporate files to the guest users, only the corporate users need access

upvoted 1 times

NoWiresIncluded 1 year, 7 months ago

Selected Answer: B

B, you need the corporate to central switch through the WLC and the Guest to locally switch to the local router.

upvoted 4 times

daeman 2 years, 3 months ago

Selected Answer: B

B seems to meet the state requirement of sending Corp traffic to the data centers via the WLC and allowing guest traffic to traverse to the internet locally.

upvoted 4 times



A network engineer is implementing BYOD on a wireless network. Based on the customer requirements, a dual SSID approach must be taken. Which two advanced WLAN configurations must be performed? (Choose two.)

- A. Set NAC State to Radius NAC.
- B. Set Allow AAA Override to Enabled.
- C. Set DHCP Addr. Assignment to Required.
- D. Select DHCP Profiling.
- E. Select Enable Session Timeout.

Suggested Answer: AB

Community vote distribution

AB (100%)

  **rrahim** 4 months, 1 week ago

Selected Answer: BC

Set Allow AAA Override to Enabled:

AAA override allows the wireless LAN controller (WLC) to dynamically assign VLANs or other attributes based on the user's role or identity. This is essential for BYOD implementations, as it ensures that devices are placed on the correct network segment (e.g., corporate vs. guest) after authentication.

Set DHCP Addr. Assignment to Required:

DHCP address assignment is necessary to ensure that devices connecting to the BYOD SSID receive an IP address. This is critical for both corporate and guest devices to access network resources.

upvoted 2 times

  **rrahim** 4 months, 1 week ago

Why the Other Options Are Incorrect:

A. Set NAC State to Radius NAC:

NAC (Network Admission Control) is used for enforcing security policies, but it is not specifically required for a dual SSID BYOD implementation. It is more relevant for advanced security and compliance scenarios.

D. Select DHCP Profiling:

DHCP profiling is used to gather information about devices based on DHCP traffic, but it is not a mandatory configuration for a dual SSID BYOD setup. It is more relevant for device identification and profiling.

E. Select Enable Session Timeout:

Session timeout is used to limit the duration of a user's session, but it is not directly related to the dual SSID BYOD implementation. It is more relevant for managing session duration and resource usage.



upvoted 2 times

  **NoWiresIncluded** 7 months ago

Selected Answer: AB

A & B, you need to point the users to the ISE for onboarding

upvoted 2 times

  **cvndani** 1 year, 3 months ago

Provided answers are correct

upvoted 3 times

Which three characteristics of a rogue AP pose a high security risk? (Choose three.)

- A. open authentication
- B. high RSSI
- C. foreign SSID
- D. accepts clients
- E. low RSSI
- F. distant location

Suggested Answer: ACD

Community vote distribution

ABD (80%)


ACD (20%)

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

A,B & D is correct
upvoted 17 times

 **rix18** 2 years, 10 months ago

Could you post where are you find the B?
upvoted 1 times

 **casterJR** Most Recent 8 months, 1 week ago

A, B & D is correct - B (high RSSI-biggest threat) Means greater coverage and more users are likely to connect to it and also it means it might be closer or within the building.
upvoted 1 times

 **most_ahdy** 1 year, 4 months ago

https://www.cisco.com/c/dam/global/en_hk/assets/event/cisco_connect_2015/pdf/4-1.pdf
page 26
A, B,D
upvoted 1 times

 **GoldLeader** 1 year, 5 months ago

Selected Answer: ABD

I think B. High RSSI is a greater threat as that tells you the rouge AP is very near your network and possibly inside it. C. Foreign SSID would be less threatening as that means the rouge AP is not trying to fool or mislead anyone that the SSID is legitimate to your organization.
upvoted 2 times

 **NoWiresIncluded** 1 year, 7 months ago

Selected Answer: ABD

A - Open Authentication means that the clients will not go through security checks, including the clients authenticating the system.
B - High RSSI, it means that the Rogue is close enough for your clients to connect to it, it also may indicate that it is in your building and not a neighbor's AP
D - If your corporate clients are joining an unknown AP that is a big problem, especially if they don't realize it.
Not C - Foreign SSIDs are an indication that they are not your APs; if they use the same SSID that is a problem, as they are mimicking your network to entrap users.
Not E - low RSSI means that they are probably outside your building and clients may not even detect them or be able to join consistently
Not F - Distant location is the same as low RSSI, users might not even detect or be able to join
upvoted 3 times

 **Mimimimimi** 2 years ago

ABD.
A Rogue transmitting a similar SSID as the corporate is an indication for malicious intent. (Crossing away answer C).
Especially with open authentication and high RSSI (to cover a large area).

A foreign SSID is easier to distinguish and staff should not have a reason to try and connect to it.

Several containment triggers are:

High RSSI (depending on the configured minimum. Documentation uses example -45 dBm)

Using-my-SSID

upvoted 1 times

🗲️ 👤 **twoplanker** 2 years ago

Selected Answer: ACD

provided answer is correct

upvoted 2 times

🗲️ 👤 **cvndani** 2 years, 3 months ago

Selected Answer: ABD

I think A-B-D

upvoted 3 times

🗲️ 👤 **Liselot** 2 years, 5 months ago

A low RSSI would fall under the Rogue Detection Minimum RSSI field and thus kept undetected.

I would opt for A, D, E

upvoted 1 times

🗲️ 👤 **kthekillerc** 3 years, 1 month ago

provided answer is correct

upvoted 1 times

Which AP model of the Cisco Aironet Active Sensor is used with Cisco DNA Center?

- A. 1800s
- B. 3600e
- C. 3800s
- D. 4800i

Suggested Answer: A

Community vote distribution

A (100%)

  **rrahim** 4 months, 1 week ago

Selected Answer: A

The Cisco Aironet 1800s Active Sensor is specifically designed for Cisco DNA Assurance and works with Cisco DNA Center for wireless network monitoring and testing.

It acts as a client device to proactively test and report wireless network performance.

Used for real-time monitoring, troubleshooting, and assurance in a Cisco DNA Center deployment.

Supports tests like connectivity, authentication, roaming, and application performance to help diagnose network issues.

The other models listed (3600e, 3800s, 4800i) are standard APs but do not serve as dedicated active sensors for Cisco DNA Center.

upvoted 1 times

  **NoWiresIncluded** 7 months ago

Selected Answer: A

A is correct

upvoted 2 times

  **joseph_climber** 2 years, 1 month ago

correct

<https://www.cisco.com/c/en/us/products/collateral/wireless/access-points/guide-c07-744250.html>

upvoted 2 times

  **skh** 2 years, 10 months ago

correct

https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/deploy-guide/Cisco_1800S_Sensor_Deployment_Guide_133.pdf

upvoted 2 times

Which component must be integrated with Cisco DNA Center to display the location of a client that is experiencing connectivity issues?

- A. Cisco Hyperlocation Module
- B. Wireless Intrusion Prevention System
- C. Cisco Connected Mobile Experiences
- D. Cisco Mobility Services Engine

Suggested Answer: A

Community vote distribution

C (89%)

11%

 **Sorvahr** Highly Voted 4 years, 8 months ago

C is correct


upvoted 15 times

 **HOT2012** Highly Voted 3 years, 7 months ago

Selected Answer: C

c is correct one

upvoted 6 times

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

Selected Answer: C

Cisco Connected Mobile Experiences (CMX):

CMX is a location-based analytics and engagement platform that integrates with Cisco DNA Center. It provides real-time location tracking of wireless clients, enabling network administrators to pinpoint the location of devices experiencing connectivity issues.

CMX uses data from Cisco access points (APs) and other network elements to determine the physical location of clients within a wireless environment.

Why the Other Options Are Incorrect:

A. Cisco Hyperlocation Module:

The Cisco Hyperlocation Module is an add-on module for certain Cisco APs that enhances location accuracy. While it improves location tracking, it is not a standalone solution for displaying client locations in Cisco DNA Center. It works in conjunction with CMX.

upvoted 1 times

 **Le91** 8 months ago

Selected Answer: A

By integrating the Hyperlocation Module with Cisco DNA Center, you can enhance the visibility of client locations and improve troubleshooting capabilities for connectivity issues

upvoted 1 times

 **Gumpy1** 1 year, 1 month ago

Selected Answer: A

I do believe A is correct as stated. Although question is not worded very well.

In this Cisco doc, Cisco CMX (Cisco Connected Mobile Experiences) is NOT required for Cisco Hyperlocation,

https://www.cisco.com/c/en/us/td/docs/wireless/spaces/detect-and-locate/b-cisco-cle/m_hyperlocation.html (this cancels "c", because the question says "must")

but Hyperlocation is needed for accurate location of a device that is having trouble connecting to the wifi signal anyway. It is the component that must be integrated (either through CMX, Cisco Spaces, 9800 WLC.)

upvoted 1 times

 **casterJR** 1 year, 2 months ago

C is correct - Cisco DNA Center supports integration with both Cisco Connected Mobile Experiences (CMX) and Cisco Spaces for location services.

while Cisco Hyperlocation Module itself is not directly integrated with Cisco DNA Center, you can choose between CMX and Cisco Spaces for location

services, depending on your requirements and existing infrastructure

upvoted 1 times

🗨️ 👤 **DiegoECUIO** 1 year, 7 months ago

A is correct https://www.cisco.com/c/en/us/td/docs/wireless/spaces/detect-and-locate/b-cisco-cle/m_hyperlocation.html

upvoted 1 times

🗨️ 👤 **NoWiresIncluded** 2 years ago

This question is not good, MSE integrates with DNA so it can also be used along with CMX for location even though it is EOL... so it should be B & C

upvoted 1 times

🗨️ 👤 **copa77** 2 years, 5 months ago

Selected Answer: C

C is correct

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/2-2-3/b_cisco_dna_assurance_2_2_3_ug/b_cisco_dna_assurance_2_2_3_ug_chapter_010000.pdf

upvoted 2 times

🗨️ 👤 **NightmareCreature** 3 years, 10 months ago

C is for sure the correct answer:

Cisco Connected Mobile Experiences (CMX) is a smart Wi-Fi solution that uses the Cisco wireless infrastructure to provide location services and location analytics for consumers' mobile devices.

upvoted 3 times

The IT manager is asking the wireless team to get a report for all guest user associations during the past two weeks. In which two formats can Cisco Prime save this report? (Choose two.)

- A. CSV
- B. PDF
- C. XLS
- D. DOC
- E. plain text

Suggested Answer: AB

Reference:

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-2/user/guide/bk_CiscoPrimeInfrastructure_3_2_0_UserGuide/bk_CiscoPrimeInfrastructure_3_2_0_UserGuide_chapter_01010.html

Community vote distribution

AB (100%)

 **NoWiresIncluded** 7 months ago

Selected Answer: AB

I used to run reports all the time, CSV and PDF are the correct answers.
upvoted 2 times

 **Vlad_Is_Love_ua** 8 months, 1 week ago

Selected Answer: AB

The Analytics Dashboard provides reports that help you understand and monitor the behavior pattern of visitors within a particular venue.

The Analytics service's report facility also provides a more regular and manager-oriented set of information through parameterized templates to measure various trends and patterns that occur over time in a particular zone. You can create new reports and modify existing reports. You can schedule a report at a customized frequency, print reports, and download reports in PDF, Excel, or HTML formats. You can either choose to autogenerate or customize a report.

upvoted 1 times

 **Vlad_Is_Love_ua** 8 months, 1 week ago

The Analytics Dashboard provides reports that help you understand and monitor the behavior pattern of visitors within a particular venue.

The Analytics service's report facility also provides a more regular and manager-oriented set of information through parameterized templates to measure various trends and patterns that occur over time in a particular zone. You can create new reports and modify existing reports. You can schedule a report at a customized frequency, print reports, and download reports in PDF, Excel, or HTML formats. You can either choose to autogenerate or customize a report.

upvoted 1 times

 **kthekillerc** 2 years, 1 month ago

Provided answer is correct


upvoted 1 times

 **Igur** 3 years, 1 month ago

Correct. "You can also save reports in CSV or PDF format"

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-6/user/guide/bk_CiscoPrimeInfrastructure_3_6_0_UserGuide/bk_CiscoPrimeInfrastructure_3_6_0_UserGuide_chapter_010111.html

upvoted 4 times

 **Sorvahr** 3 years, 2 months ago

Answer is correct.

upvoted 3 times

A customer is experiencing performance issues with its wireless network and asks a wireless engineer to provide information about all sources of interference and their impacts to the wireless network over the past few days. Where can the requested information be accessed?

- A. CleanAir reports on Cisco Prime Infrastructure
- B. Performance reports on Cisco Prime Infrastructure
- C. Interference Devices reports on Cisco Wireless LAN Controller
- D. Air Quality reports on Cisco Wireless LAN Controller

Suggested Answer: A

Community vote distribution

A (50%)

D (50%)

🗳️ 👤 **rrahim** 4 months, 1 week ago

Selected Answer: A

The CleanAir reports on Cisco Prime Infrastructure (PI) provide detailed information about all sources of interference and their impacts on the wireless network. CleanAir technology identifies and categorizes interference sources, such as microwaves, cordless phones, and Bluetooth devices, and provides historical data on their effects on network performance.

upvoted 2 times

🗳️ 👤 **robi1020** 10 months, 2 weeks ago

Selected Answer: A

Correct

upvoted 1 times

🗳️ 👤 **raphim** 1 year, 2 months ago

Selected Answer: D

Answer D is correct

You also have "Air Quality Reports" on the Wireless Controller

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_cleanair.html

upvoted 1 times

🗳️ 👤 **JJBIG** 1 year, 2 months ago

Answer A

Step 1 Choose Wireless > 802.11a/n or 802.11b/g/n > CleanAir to open the 802.11a (or 802.11b) > CleanAir page.

Figure 14-1 802.11a (or 802.11b) > CleanAir

Step 2 Select the CleanAir check box to enable Cisco CleanAir functionality on the 802.11a/n or 802.11b/g/n network, or unselect it to prevent the controller from detecting spectrum interference. By default, the value is not selected.

Step 3 Select the Report Interferers check box to enable the Cisco CleanAir system to report any detected sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.

upvoted 1 times

🗳️ 👤 **Seba_o_s** 1 year, 2 months ago

From WLC you can not get history report. Right answer A

upvoted 1 times

🗳️ 👤 **rph02533** 2 years ago

correct

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-1/user/guide/pi_ug/rep.html#23577:~:text=No,CleanAir%20Reports,-The%20following%20table

upvoted 2 times

🗳️ 👤 **kthekillerc** 3 years ago

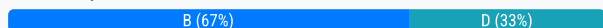
Provided answer is correct
upvoted 2 times

An engineer must provide a graphical report with summary grouped data of the total number of wireless clients on the network. Which Cisco Prime Infrastructure report provides the required data?

- A. Client Traffic Stream Metrics
- B. Client Summary
- C. Posture Status Count
- D. Mobility Client Summary

Suggested Answer: D

Community vote distribution



🗳️ **masters777** 3 months, 1 week ago

Selected Answer: B

Cisco Prime login -> Dashboard -> under network summary -> Client Summary
upvoted 1 times

🗳️ **rrahim** 4 months, 1 week ago

Selected Answer: B

Client Summary Report:

The Client Summary report in Cisco Prime Infrastructure provides a high-level overview of wireless clients connected to the network. It includes grouped data such as the total number of clients, client distribution by SSID, client distribution by AP, and other relevant metrics.

This report is ideal for generating graphical summaries of client activity and connectivity.

Why the Other Options Are Incorrect:

A. Client Traffic Stream Metrics:

This report focuses on detailed traffic metrics for individual clients, such as throughput, retries, and packet counts. It does not provide a summary of the total number of clients.

C. Posture Status Count:

This report is related to network access control (NAC) and provides information about the compliance status of clients (e.g., compliant, non-compliant). It does not provide a summary of the total number of wireless clients.

D. Mobility Client Summary:

This report is specific to mobility services and provides information about client roaming behavior. It does not provide a summary of the total number of clients on the network.

upvoted 1 times

🗳️ **most_ahdy** 10 months, 1 week ago

https://www.cisco.com/c/dam/en/us/td/docs/net_mgmt/prime/infrastructure/3-2/reference/reports_field_ref.xlsx

upvoted 2 times

🗳️ **GoldLeader** 11 months, 2 weeks ago

Selected Answer: D

D. is a graphical report that displays the total number of wireless clients on the network.

upvoted 1 times

🗳️ **Ace_Pee** 1 year ago

I say B as you need a mobility oracle (POS and EOS) in the network to use the report referenced in D.

upvoted 1 times

🗨️ 👤 **Vlad_Is_Love_ua** 1 year, 1 month ago

Selected Answer: B

[https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-9/user/guide/bk_CiscoPrimeInfrastructure_3_9_0_UserGuide/monitor_network_clients_and_users.html#con_1418185)

[9/user/guide/bk_CiscoPrimeInfrastructure_3_9_0_UserGuide/monitor_network_clients_and_users.html#con_1418185](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-9/user/guide/bk_CiscoPrimeInfrastructure_3_9_0_UserGuide/monitor_network_clients_and_users.html#con_1418185)

upvoted 2 times

🗨️ 👤 **TiredOfCertExams** 1 year, 1 month ago

Client Summary Dashboard has nice data, but is not a graphical report. It is a graphical dashboard. The question specifies what PI report provides the data. So in my opinion, D. Mobility Client Summary report is the correct choice.

upvoted 2 times

🗨️ 👤 **Vlad_Is_Love_ua** 1 year, 1 month ago

Client Summary Dashboard

The Client dashboard (Dashboard > Overview > Client Summary) page displays the client-related dashlets. These dashlets enable you to monitor the clients on the network. The data for graphs is also polled/updated periodically and stored in Cisco Prime Infrastructure database. On the other hand, most of the information in the Client Details page are polled directly from the controller/switch.

upvoted 1 times

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

Provided answer is correct

upvoted 2 times

🗨️ 👤 **cskshiet** 3 years ago

Correct.

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-0/user/guide/prime_infra_ug/rep.html

upvoted 3 times

An engineer is using Cisco Prime Infrastructure reporting to monitor the state of security on the WLAN. Which output is produced when the Adaptive wIPS Top 10 AP report is run?

- A. last 10 wIPS events from monitor mode APs
- B. last 10 wIPS events from sniffer mode APs
- C. last of 10 sniffer mode APs with the most wIPS events
- D. last of 10 monitor mode APs with the most wIPS events

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Mimimimimi** Highly Voted 👍 1 year, 8 months ago
Answer A is correct.

It is literally in the below source:

[https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/6-](https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/6-0/wIPS/configuration/guide/wipscg60/msecg_ch7_wIPS.html#:~:text=Adaptive%20wIPS%20Top%2010%20AP%E2%80%94Lists%20the%20last%2010%20events)

[0/wIPS/configuration/guide/wipscg60/msecg_ch7_wIPS.html#:~:text=Adaptive%20wIPS%20Top%2010%20AP%E2%80%94Lists%20the%20last%2010%20events](https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/6-0/wIPS/configuration/guide/wipscg60/msecg_ch7_wIPS.html#:~:text=Adaptive%20wIPS%20Top%2010%20AP%E2%80%94Lists%20the%20last%2010%20events)
upvoted 5 times

🗳️ 👤 **rrahim** Most Recent 🕒 4 months, 1 week ago

Selected Answer: A

The documentation states that the Adaptive wIPS Top 10 AP report lists the last 10 events reported for monitor access points. This means the report provides a summary of the most recent wIPS events detected by monitor mode APs.
upvoted 1 times

🗳️ 👤 **GoldLeader** 11 months, 2 weeks ago

Selected Answer: A

Adaptive wIPS Top 10 AP—Lists the last 10 events reported for monitor access points.
upvoted 1 times

🗳️ 👤 **Heddy** 11 months, 3 weeks ago

wips events are by monitor mode, so either A or D, now if you are Optimus Prime, what do you want to see the first last 10 bad events or the last 10 ppl that reporting bad events
upvoted 1 times

🗳️ 👤 **Vlad_Is_Love_ua** 1 year, 1 month ago

Selected Answer: A

Adaptive wIPS Top 10 AP—Lists the last 10 events reported for monitor access points.
https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/6-0/wIPS/configuration/guide/wipscg60/msecg_ch7_wIPS.html#:~:text=Adaptive%20wIPS
upvoted 3 times

🗳️ 👤 **Liselot** 1 year, 11 months ago

This report displays the top ten access points with the highest number of generated adaptive wIPS alarms.
upvoted 1 times

🗳️ 👤 **Liselot** 1 year, 11 months ago

Adaptive wIPS Top 10 AP—Lists the last 10 events reported for monitor access points.
upvoted 1 times

🗳️ 👤 **Caradum** 1 year, 11 months ago

https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/6-0/wIPS/configuration/guide/wipscg60/msecg_ch7_wIPS.html

"Adaptive wIPS Top 10 AP—Lists the last 10 events reported for monitor access points."

Correct Answer is D.

upvoted 3 times

  **anonymonkey** 2 years, 3 months ago

D

https://www.cisco.com/c/en/us/td/docs/wireless/technology/wips/deployment/guide/WiPS_deployment_guide.html#pgfld-43469

upvoted 2 times



  **Guglielmino** 2 years, 3 months ago

https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/6-0/wIPS/configuration/guide/wipscg60/msecg_ch7_wIPS.html

"•Adaptive wIPS Top 10 AP—Lists the last 10 events reported for monitor access points."

A is correct

upvoted 3 times

  **drel** 2 years, 11 months ago

Not about events.

Adaptive wIPS Top 10 APs - This report displays the top ten access points with the highest number of generated adaptive wIPS alarms.

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-0/user/guide/prime_infra_ug/rep.html

upvoted 3 times

Rogue Rule > Edit

Rule Name: Rule 1

Type: **Malicious**

Match Operation: ☒ Match All ☐ Match Any

Enable: ☒

Conditions

Minimum RSSI (-95 to -50): dBm

Time Duration (0-3600): secs.

User configured SSID

SSID	Actions
Admin	<input type="button" value="Add SSID"/> <input type="button" value="Remove"/>

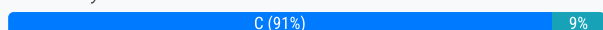
Client Count

Refer to the exhibit. An engineer tries to manage the rogues on the Cisco WLC. Based on the configuration, which AP is marked as malicious by the controller?

- A. rogue AP with SSID admin seen for 4000 seconds and heard at -70dBm
- B. rogue AP with SSID admin seen for 3000 seconds and heard at -60dBm
- C. rogue AP with SSID admin seen for 4000 seconds and heard at -60dBm
- D. rogue AP with SSID admin seen for 3000 seconds and heard at -70dBm

Suggested Answer: D

Community vote distribution



KalRona Highly Voted 3 years, 2 months ago

Answer C

Duration—Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the Time Duration text box. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.

Meaning the Rouge AP would need to have a stronger signal than -65db and seen longer than 3600 sec.

upvoted 5 times

casterJR Most Recent 8 months, 1 week ago

Correct answer is C.

upvoted 1 times

DiegoECUIO 1 year, 1 month ago

Selected Answer: D

D answer is correct

upvoted 1 times

kejvi 1 year, 4 months ago

Selected Answer: C

-60 > -65 and 4000 > 3600 Must be C

upvoted 2 times

GoldLeader 1 year, 5 months ago

Selected Answer: C

C. Meets both the time duration 4000 is greater than 3600, and RSSI -60 is greater than -65. All other answers fail to meet both requirements.

upvoted 1 times

🗨️ 👤 **NoWiresIncluded** 1 year, 7 months ago

Selected Answer: C

it has to be a minimum of -65, that means that -70 is too weak, and a minimum of 3600 seconds, so 3000 seconds is too short of a duration. So C.

upvoted 1 times

🗨️ 👤 **C4l4v3r4** 2 years, 3 months ago

Selected Answer: C

Duration - Requires that the rogue access point be detected for a minimum period of time (everything greater than that triggers the rule - 4000 is more than 3600).

RSSI - Requires that the rogue access point have a minimum RSSI value (everything greater than that triggers the rule - -60dBm is greater signal power than -65dBm)

upvoted 4 times

🗨️ 👤 **sgr4523** 2 years, 3 months ago

Selected Answer: C

No hesitation. Agree to KalRona, answer must be C

upvoted 2 times

🗨️ 👤 **alexblue** 2 years, 6 months ago

I checked 4 sites. One go for 4000s 70dbm and most go for 3000s 70dbm

Both are incorrect

MINIMUM DURATION, so a greater duration than 3600 is 4000s, so 3000s ruled out

MINIMUM RSSI, -60 is greater than -65, -65 is greater than -70 ... so -70 ruled out

CONCLUSION: -60db 4000s, and I dont care if even Cisco says opposite, as per its own definition for these parameters

upvoted 1 times

🗨️ 👤 **kthekillerc** 2 years, 10 months ago

correction answer is a

upvoted 1 times

🗨️ 👤 **kthekillerc** 3 years, 1 month ago

Provided answer is correct. 1) it has to be heard at -70 because the alert policy threshold is at -65 therefore it has to be higher than -65 to trigger an alert. The timer threshold is set at and up to 3600 seconds thus the alert trigger has to be 3000 as it would never poll the rogue for more than 3600.

In conclusion it has to be D and provided answer is correct.

upvoted 2 times

🗨️ 👤 **talosgt** 2 years, 9 months ago

-70dbm is lower my man...the answer is C

upvoted 7 times

🗨️ 👤 **drel** 3 years, 5 months ago

B is the right answer

upvoted 4 times

🗨️ 👤 **drel** 3 years, 5 months ago

Sorry, but C, because of time treshhold

upvoted 10 times

Which devices can be tracked with the Cisco Context Aware Services?

- A. wired and wireless devices
- B. wireless devices
- C. wired devices
- D. Cisco certified wireless devices

Suggested Answer: A

Reference:

<https://www.cisco.com/c/en/us/support/docs/wireless/context-aware-software/110836-cas-faq.html>

  **MoBenones** Highly Voted 1 year, 7 months ago

A is correct: <https://www.cisco.com/c/en/us/support/docs/wireless/context-aware-software/110836-cas-faq.html#:~:text=The%20Cisco%20Context%2DAware%20Services,Fi%20active%20RFID%20CCX%20tags>.

The Cisco Context-Aware Services allows you to track and locate IP enabled devices both wired and wireless with the Cisco Unified Wireless Network and Wired network. Wireless devices include Wi-Fi enabled client devices and Wi-Fi active RFID CCX tags.


upvoted 6 times

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

Selected Answer: A

Cisco Context Aware Services (CAS) can track both wired and wireless devices. This feature provides visibility into the location and movement of devices connected to the network, regardless of whether they are connected via wired or wireless infrastructure.

upvoted 1 times

  **kthekillerc** 7 months, 3 weeks ago

Provided answer is correct

upvoted 1 times

Which two events are outcomes of a successful RF jamming attack? (Choose two.)

- A. disruption of WLAN services
- B. unauthentication association
- C. deauthentication broadcast
- D. deauthentication multicast
- E. physical damage to AP hardware

Suggested Answer: *AE*

  **Fenstar** Highly Voted 3 years, 8 months ago

answer is correct



https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/7-4/wIPS_Configuration/Guide/7_4_MSE_wIPS/7_4_MSE_wIPS_appendix_01100.html
upvoted 5 times

  **robi1020** Most Recent 11 months, 1 week ago

[https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/7-](https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/7-4/wIPS_Configuration/Guide/7_4_MSE_wIPS/7_4_MSE_wIPS_appendix_01100.html#:~:text=the%20wireless%20environment.,Denial%20of%20Service%20at%20wIPS%20Solution)

[4/wIPS_Configuration/Guide/7_4_MSE_wIPS/7_4_MSE_wIPS_appendix_01100.html#:~:text=the%20wireless%20environment.,Denial%20of%20Service%20at%20wIPS%20Solution](https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/7-4/wIPS_Configuration/Guide/7_4_MSE_wIPS/7_4_MSE_wIPS_appendix_01100.html#:~:text=the%20wireless%20environment.,Denial%20of%20Service%20at%20wIPS%20Solution)

upvoted 2 times

  **kthekillerc** 3 years, 1 month ago

Provided answer is correct

upvoted 2 times

An engineer must create an account to log in to the CLI of an access point for troubleshooting. Which configuration on the WLC will accomplish this?

- A. Allow New Telnet Sessions
- B. ReadWrite User Access Mode
- C. SNMP V3 User
- D. Global Configuration Enable Password

Suggested Answer: *D*

🗲️ 👤 **rph02533** 1 year ago

correct

refer: [https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-](https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/m_configuring_global_credentials_for_access_points.html)

[4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/m_configuring_global_credentials_for_access_points.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/m_configuring_global_credentials_for_access_points.html)

upvoted 1 times

🗲️ 👤 **Pawnstar** 2 years, 3 months ago

Answer is correct.

upvoted 2 times

A multitenant building contains known wireless networks in most of the suites. Rogues must be classified in the WLC. How are the competing wireless APs classified?

- A. adhoc
- B. friendly
- C. malicious
- D. unclassified

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **NoWiresIncluded** 7 months ago

Selected Answer: B

B is correct, they must be classified (so D is out) and if they are known to be other tenants they are to be classified as friendly not malicious.
upvoted 2 times

🗨️ 👤 **rph02533** 1 year ago

correct

https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/consolidated_guide/b_consolidated_3850_3se_cg_chapter_01000101
upvoted 1 times

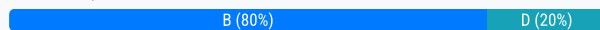
An enterprise has recently deployed a voice and video solution available to all employees using AireOS controllers. The employees must use this service over their laptops, but users report poor service when connected to the wireless network. The programs that consume bandwidth must be identified and restricted.

Which configuration on the WLAN aids in recognizing the traffic?

- A. NetFlow Monitor
- B. AVC Profile
- C. QoS Profile
- D. Application Visibility

Suggested Answer: D

Community vote distribution



rrahim 4 months, 1 week ago

Selected Answer: B

AVC (Application Visibility and Control) Profile:

AVC is a feature on Cisco wireless LAN controllers (WLCs) that provides visibility into the applications and protocols being used on the network. It allows administrators to identify bandwidth-consuming applications and enforce policies to restrict or prioritize specific types of traffic.

By enabling AVC, the enterprise can monitor and classify traffic based on applications (e.g., voice, video, web browsing) and take appropriate actions to optimize network performance.:

Application Visibility is a feature provided by AVC. However, it is not a standalone configuration option on the WLAN. It is part of the AVC profile.

upvoted 1 times

Ocsicccnp 8 months, 3 weeks ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/AVC_8point8_dg.html#pgfld-50560:~:text=Once%20Application%20Visibility%20is%20enabled%20on%20the%20specific%20WLAN

Once Application Visibility is enabled on the specific WLAN

upvoted 1 times

Gumpy1 1 year, 1 month ago

Selected Answer: D

D is correct....Application visibility is offered on AirOS, see article on how to configure it.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/AVC_8point8_dg.html#pgfld-50619

upvoted 1 times

raphim 1 year, 8 months ago

Selected Answer: B

On AireOS Controller you have to set up a "AVC Profile"

On IOS-XE Controller you have to enable "Application Visibility"

So the question says its an AirOS Controller - so B must be correct

upvoted 3 times

Zanjit500 2 years ago

Id say B & D. It's subjective dependent on how you interpret the question.

Typical Cisco BS question. I wonder whether they get the answers correct themselves.

upvoted 2 times

casperionx 1 year, 1 month ago

Its B, App Visibility is XE, AireOS is AVC Profile.

upvoted 1 times

  **NoWiresIncluded** 2 years ago

Selected Answer: B

B is correct, it states that the traffic must be restricted, therefore you need to implement an AVC profile on the SSID to do that, just turning on AV will show you the traffic, but not do anything about it. So not D.

upvoted 1 times

  **NoWiresIncluded** 2 years ago

I might modify my answer now that I re-read the question, it says what will help you identify the traffic, it doesn't say what will restrict it, which would be D.

upvoted 1 times

  **rph02533** 2 years, 6 months ago

B and D both seem correct.

i'd go with D

https://www.youtube.com/watch?v=VGSyLgf6boU&ab_channel=TravisBonfigli

Question is asking about configuration on WLAN.

Application visibility can be enabled under WLANs> Wlan ID >Qos menu

AVC profile is configured under Wireless>Application visibility and control menu

upvoted 1 times

Which customizable security report on Cisco Prime Infrastructure will show rogue APs detected since a point in time?

- A. Network Summary
- B. Rogue APs Events
- C. New Rogue APs
- D. Rogue APs Count Summary

Suggested Answer: C

Community vote distribution

B (67%)

C (33%)

 **raphim** 8 months, 2 weeks ago

Selected Answer: B

Because "New Rogue AP" Report is NOT Customizable as required in the question it must be answer B

[https://content.cisco.com/chapter.sjs?](https://content.cisco.com/chapter.sjs?uri=%2Fsearchable%2Fchapter%2Fwww.cisco.com%2Fcontent%2Fen%2Fus%2Ftd%2Fdocs%2Fnet_mgmt%2Fprime%2Finfrastructure%2F2-1%2Fuser%2Fguide%2Fpi_ug%2Freps.html.xml#23577)

[uri=%2Fsearchable%2Fchapter%2Fwww.cisco.com%2Fcontent%2Fen%2Fus%2Ftd%2Fdocs%2Fnet_mgmt%2Fprime%2Finfrastructure%2F2-1%2Fuser%2Fguide%2Fpi_ug%2Freps.html.xml#23577](https://content.cisco.com/chapter.sjs?uri=%2Fsearchable%2Fchapter%2Fwww.cisco.com%2Fcontent%2Fen%2Fus%2Ftd%2Fdocs%2Fnet_mgmt%2Fprime%2Finfrastructure%2F2-1%2Fuser%2Fguide%2Fpi_ug%2Freps.html.xml#23577)

upvoted 2 times

 **rrahim** 4 months, 1 week ago

You are correct that the "New Rogue APs" report is not customizable as required in the question. Based on the Cisco Prime Infrastructure documentation, the correct answer is:

B. Rogue APs Events


Explanation:

Rogue APs Events Report:

The Rogue APs Events report is customizable and provides detailed information about rogue AP events, including detection, classification, and mitigation actions. It allows administrators to filter and view rogue APs detected since a specific point in time.

This report is designed to help track and analyze rogue AP activity over a defined period, making it the most suitable option for the requirement.

upvoted 1 times

 **JJBIG** 9 months, 1 week ago

The following table describes the various Security reports that you can generate in Prime Infrastructure

New Rogue APs Customizable : No

Rogue AP Events Customizable : Yes


So it should be C

upvoted 1 times

 **JJBIG** 9 months, 1 week ago

florin_xpc's link is good, answer should be B, not C

upvoted 1 times

 **florin_xpc** 9 months, 2 weeks ago

B - correct answer

[https://content.cisco.com/chapter.sjs?](https://content.cisco.com/chapter.sjs?uri=%2Fsearchable%2Fchapter%2Fwww.cisco.com%2Fcontent%2Fen%2Fus%2Ftd%2Fdocs%2Fnet_mgmt%2Fprime%2Finfrastructure%2F2-1%2Fuser%2Fguide%2Fpi_ug%2Freps.html.xml#33117)

[uri=%2Fsearchable%2Fchapter%2Fwww.cisco.com%2Fcontent%2Fen%2Fus%2Ftd%2Fdocs%2Fnet_mgmt%2Fprime%2Finfrastructure%2F2-1%2Fuser%2Fguide%2Fpi_ug%2Freps.html.xml#33117](https://content.cisco.com/chapter.sjs?uri=%2Fsearchable%2Fchapter%2Fwww.cisco.com%2Fcontent%2Fen%2Fus%2Ftd%2Fdocs%2Fnet_mgmt%2Fprime%2Finfrastructure%2F2-1%2Fuser%2Fguide%2Fpi_ug%2Freps.html.xml#33117)

upvoted 1 times

 **AhcMez** 11 months ago

Selected Answer: B

Answer B

upvoted 2 times

🗨️ 👤 **Azer969** 1 year ago

I think that answer B

upvoted 1 times

🗨️ 👤 **NoWiresIncluded** 1 year ago

Selected Answer: C

C is correct

upvoted 2 times

🗨️ 👤 **rph02533** 1 year, 6 months ago

correct

[https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-0/user/guide/prime_infra_ug/rep.html#:~:text=This%20report%20displays%20all%20rogues%20detected%20for%20the%20first)

[0/user/guide/prime_infra_ug/rep.html#:~:text=This%20report%20displays%20all%20rogues%20detected%20for%20the%20first](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-0/user/guide/prime_infra_ug/rep.html#:~:text=This%20report%20displays%20all%20rogues%20detected%20for%20the%20first)

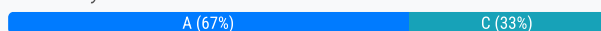
upvoted 1 times

After receiving an alert about a rogue AP, a network engineer logs into Cisco Prime Infrastructure and looks at the floor map where the AP that detected the rogue is located. The map is synchronized with a mobility services engine that determines that the rogue device is actually inside the campus. The engineer determines that the rogue is a security threat and decides to stop it from broadcasting inside the enterprise wireless network. What is the fastest way to disable the rogue?

- A. Go to the location where the rogue device is indicated to be and disable the power.
- B. Create an SSID similar to the rogue to disable clients from connecting to it.
- C. Update the status of the rogue in Cisco Prime Infrastructure to contained.
- D. Classify the rogue as malicious in Cisco Prime Infrastructure.

Suggested Answer: C

Community vote distribution



🗨️ 👤 **rrahim** 4 months, 1 week ago

Selected Answer: C

Containment in Cisco Prime Infrastructure:

Cisco Prime Infrastructure provides a feature to contain rogue APs. When a rogue AP is marked as "contained," the system uses nearby authorized access points (APs) to send deauthentication frames to clients connected to the rogue AP, effectively preventing it from operating within the enterprise wireless network.

This method is automated and does not require physical intervention or manual configuration of SSIDs.

upvoted 1 times

🗨️ 👤 **rrahim** 4 months, 1 week ago

Why the Other Options Are Incorrect:

A. Go to the location where the rogue device is indicated to be and disable the power:

While physically disabling the rogue AP is effective, it is not the fastest method. It requires locating the device and manually powering it off, which can be time-consuming.

B. Create an SSID similar to the rogue to disable clients from connecting to it:

Creating a similar SSID is not a reliable or efficient method to disable a rogue AP. It does not stop the rogue AP from broadcasting and may cause confusion for legitimate clients.

D. Classify the rogue as malicious in Cisco Prime Infrastructure:

Classifying the rogue as malicious helps identify it as a threat, but it does not automatically stop the rogue AP from broadcasting. Containment is the action that disables the rogue AP.

upvoted 1 times

🗨️ 👤 **MaxMusti** 11 months ago

Guys i strugglet there too you can jamm a AP over Contained on the Prime.

(Info will get pushed to the WLC)

After this he isnt working anymore and you can search him and power off

Search for Jamming cool feature but be careful



upvoted 1 times

🗨️ 👤 **Supersede** 1 year, 4 months ago

Selected Answer: A

A - seems the only way to DISABLE the rogue AP. Other options doesn't satisfy the requirement.

upvoted 1 times

  **peer1024** 1 year, 8 months ago

Selected Answer: A

"to stop if from broadcasting" - this ist not containment. containment means to send disassociation frames to clients. No power...no broadcasting !

upvoted 3 times

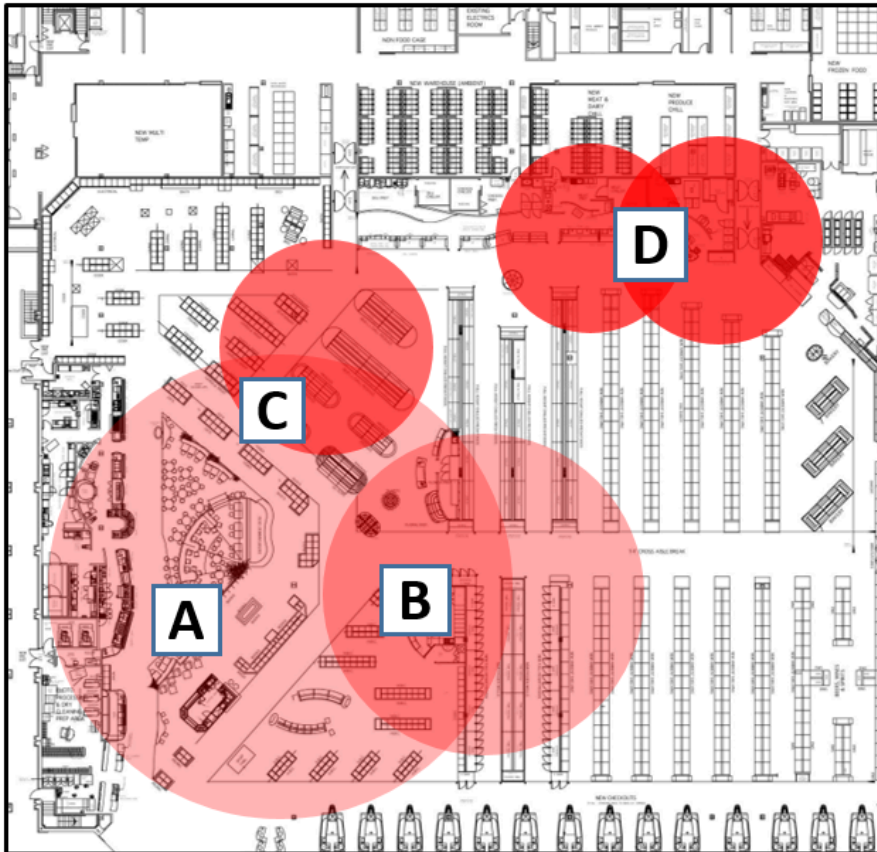
  **NoWiresIncluded** 2 years ago

Selected Answer: C

C is correct, fastest solution is to contain the AP, setting it to Malicious does not mean that it will be contained.

upvoted 2 times

Refer to the exhibit.



Which area indicates the greatest impact on the wireless network when viewing the Cisco CleanAir Zone of Impact map of interferers?

- A. A
- B. B
- C. C
- D. D

Suggested Answer: D

Reference:

<https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/112139-cleanair-own-guide-00.html>

Community vote distribution

D (100%)

 **raphim** 8 months, 2 weeks ago

Selected Answer: D

D is correct

"Zone of Impact is rendered as a circle around the detected device, and its opacity darkens with higher severity"

upvoted 1 times

A wireless network engineer must present a list of all rogue APs with a high severity score to senior management. Which report must be created in Cisco Prime Infrastructure to provide this information?

- A. Rogue AP Count Summary
- B. New Rogue APs
- C. Rogue AP Events
- D. Rogue APs

Suggested Answer: D

Community vote distribution

D (100%)

cvndani **Highly Voted** 2 years, 9 months ago

Selected Answer: D

D is the correct answer, tested on my PI 3.4
upvoted 6 times

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

Selected Answer: D

Rogue APs Report:

The Rogue APs report in Cisco Prime Infrastructure provides a detailed list of all detected rogue APs, including their severity scores. This report can be filtered to show only rogue APs with high severity scores, making it ideal for presenting to senior management.

The report includes information such as the rogue AP's MAC address, SSID, severity score, and detection time, which are critical for assessing the threat level.

upvoted 1 times

Le91 8 months ago

Selected Answer: D

To create a report in Cisco Prime Infrastructure to provide information about all rogue APs with high severity scores, you would typically use the "Rogue APs" report and customize it to filter for high severity scores.

upvoted 1 times

peer1024 2 years ago

Selected Answer: D

On Prime 3.10 the name is Rogue APs(Updated). It generates a list of rogue AP WITHOUT any time stap. Just a list.... I will stay with D

upvoted 2 times

An engineer must run a Client Traffic Stream Metrics report in Cisco Prime Infrastructure. Which task must be run before the report?

- A. scheduled report
- B. radio performance
- C. client status
- D. software

Suggested Answer: B

Reference:

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-0/user/guide/prime_infra_ug/rep.html

  **rrahim** 4 months, 1 week ago

Selected Answer: B

B. radio performance

Explanation:

Traffic Stream Metrics and Radio Performance Background Tasks:

According to the documentation, both the traffic stream metrics and radio performance background tasks must be running before generating the Client Traffic Stream Metrics report.

These tasks collect the necessary data about client traffic and radio performance, which are required to generate the report.

upvoted 1 times

  **BrockHarbor** 10 months, 3 weeks ago

B. Radio Performance

See Table 22-3

"Note The traffic stream metrics and radio performance background tasks must be running prior to generating this report."

https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/www.cisco.com/content/en/us/td/docs/net_mgmt/prime/infrastructure/2-1/user/guide/pi_ug/rep.html.xml

upvoted 1 times

What is the maximum time range that can be viewed on the Cisco DNA Center issues and alarms page?

- A. 3 hours
- B. 24 hours
- C. 3 days
- D. 7 days

Suggested Answer: D

🗲️ 👤 **Sorvahr** Highly Voted 1 year, 2 months ago

D is correct

upvoted 7 times

🗲️ 👤 **Skiffi** Highly Voted 1 year, 1 month ago

D - 7 days.

24 Hours drop-down list

Allows you to display information on the window based on the time range you select. Default is 24 Hours. Do the following:

From the 24 Hours drop-down list, choose a time range: 3 hours, 24 hours, or 7 days.

upvoted 7 times

🗲️ 👤 **iamccie** Most Recent 9 months, 2 weeks ago

Default is 24 hrs, but you can view them for upto 7 days. So D is the correct answer.

upvoted 4 times

A wireless engineer must configure access control on a WLC using a TACACS+ server for a company that is implementing centralized authentication on network devices. Which role value must be configured under the shell profile on the TACACS+ server for a user with read-only permissions?

- A. ADMIN
- B. MANAGEMENT
- C. MONITOR
- D. READ

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **Vlad_Is_Love_ua** 11 months, 1 week ago

Selected Answer: C

The minimum TACACS+ authorization level is MONITOR only, which is equivalent to read-only access in RADIUS. The maximum level is ALL, which authorizes an administrator with super-user privileges to execute configuration changes across the entire controller (both at the CLI and web interface)

upvoted 1 times

🗨️ 👤 **KalRona** 2 years, 8 months ago

C. MONITOR is correct

Usage: In order to grant the user read-only access, the <username> value must be set to monitor. In order to grant the user read-write access <https://www.cisco.com/c/en/us/support/docs/security/secure-access-control-system/115926-tacacs-radius-devices-00.html>

upvoted 3 times

🗨️ 👤 **KalRona** 2 years, 8 months ago

Edit:



Usage: In order to grant the user read-only access, the <username> value must be set to monitor. In order to grant the user read-write access, the <username> value must be set to admin.

upvoted 1 times

The CTO of an organization wants to ensure that all Android devices are placed into a separate VLAN on their wireless network. However, the CTO does not want to deploy ISE. Which feature must be implemented on the Cisco WLC?

- A. WLAN local policy
- B. RADIUS server overwrite interface
- C. AAA override
- D. custom AVC profile

Suggested Answer: A

  **rrahim** 4 months, 1 week ago

Selected Answer: A

WLAN Local Policy:

The WLAN local policy feature on the Cisco WLC allows you to define policies based on attributes such as device type (e.g., Android, Windows, smartphones, tablets) and assign specific actions, such as placing devices into a separate VLAN.

This feature does not require ISE and can be configured directly on the WLC. It uses attributes like device type (detected via DHCP or HTTP User-Agent) to apply policies dynamically.

Why the Other Options Are Incorrect:

B. RADIUS server overwrite interface:

This is not a valid feature on the Cisco WLC. The correct feature for dynamic VLAN assignment based on device type is WLAN local policy.


C. AAA override:

AAA override requires a RADIUS server to return VLAN assignments based on user or device attributes. While it can achieve the goal, it is not necessary in this case because the WLAN local policy feature can handle device-based VLAN assignment without ISE or a RADIUS server.

D. custom AVC profile:

AVC (Application Visibility and Control) profiles are used for monitoring and controlling application traffic but do not support dynamic VLAN assignment based on device type.

upvoted 2 times

  **Liselot** 11 months, 1 week ago

A is correct

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-5/configuration-guide/b_cg75/b_cg75_chapter_0111100.html#task_5531F3E9DFD847C08A2BD66DBCDB4194

upvoted 2 times

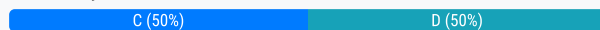
Event	5405 RADIUS Request dropped
Failure Reason	11036 The Message-Authenticator RADIUS attribute is invalid

Refer to the exhibit. A wireless engineer has integrated the wireless network with a RADIUS server. Although the configuration on the RADIUS is correct, users are reporting that they are unable to connect. During troubleshooting, the engineer notices that the authentication requests are being dropped. Which action will resolve the issue?

- A. Allow connectivity from the wireless controller to the IP of the RADIUS server.
- B. Provide a valid client username that has been configured on the RADIUS server.
- C. Configure the shared-secret keys on the controller and the RADIUS server.
- D. Authenticate the client using the same EAP type that has been set up on the RADIUS server.

Suggested Answer: C

Community vote distribution



cvndani Highly Voted 1 year, 3 months ago

C is correct

<https://community.cisco.com/t5/network-access-control/cisco-accs-11036-the-message-authenticator-radius-attribute-is/td-p/2054255>

upvoted 5 times

rrahim Most Recent 4 months, 1 week ago

Selected Answer: C

The issue indicated by Event 5405 and Failure Reason 11036 suggests that the Message-Authenticator attribute in the RADIUS request is invalid, which often points to a mismatch in the shared secret keys between the wireless controller and the RADIUS server.

To resolve this issue, the most appropriate action would be:

C. Configure the shared-secret keys on the controller and the RADIUS server.

Ensuring that the shared-secret keys match on both the wireless controller and the RADIUS server will help in properly authenticating the requests and resolving the issue

upvoted 1 times

NoWiresIncluded 7 months ago

Selected Answer: C

This is a shared secret mis-match

upvoted 1 times

kthekillerc 1 year, 10 months ago

provided answer is correct

upvoted 3 times

joseph_climber 2 years, 1 month ago

Selected Answer: D

Note

When CPU ACL is enabled, it is applicable to both wireless and wired traffic.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/access_control_lists.html

upvoted 1 times

What must be configured on the Global Configuration page of the WLC for an AP to use 802.1x to authenticate to the wired infrastructure?

- A. local access point credentials
- B. RADIUS shared secret
- C. TACACS server IP address
- D. supplicant credentials

Suggested Answer: B

Community vote distribution

D (100%)

 **daeman** Highly Voted 1 year, 3 months ago

Selected Answer: D

Incorrect should be D:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-6/configuration-guide/b_cg76/b_cg76_chapter_01101000.pdf

Choose Wireless > Access Points > Global Configuration to open the Global Configuration page. Under 802.1x Supplicant Credentials, select the 802.1x Authentication check box. In the Username text box, enter the username that is to be inherited by all access points that join the controller.
upvoted 7 times

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

Selected Answer: D

For an Access Point (AP) to use 802.1X to authenticate to the wired infrastructure, the supplicant credentials must be configured on the Global Configuration page of the Wireless LAN Controller (WLC).

The AP acts as a supplicant in this scenario, and it needs credentials (username and password) to authenticate itself to the wired network using the 802.1X protocol.

These credentials are typically configured on the WLC and are used by the AP to communicate with a RADIUS server for authentication.
upvoted 1 times

 **Vlad_Is_Love_ua** 8 months ago

Selected Answer: D

Configure the LAP

In this section, you are presented with the information to configure the LAP as a 802.1x supplicant.

If the AP is already joined to the WLC, go the Wireless tab and click on the AP, go the Credentials field and under the 802.1x Supplicant Credentials heading, check the Over-ride Global credentials check box in order to set the 802.1x username and password for this AP.
<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-fixed/107946-LAP-802-1x.html>
upvoted 1 times

 **segr4523** 1 year, 3 months ago

Selected Answer: D

RADIUS shared secret would mean the AP is the authenticator, which is not the case. The controller is the authenticator.

If we want to authenticate an AP to the wired network, we need to enable the dot1x supplicant on the AP and provide its authentication credentials
upvoted 4 times

For security purposes, an engineer enables CPU ACL and chooses an ACL on the Security > Access Control Lists > CPU Access Control Lists menu. Which kind of traffic does this change apply to as soon as the change is made?

- A. wireless traffic only
- B. wired traffic only
- C. VPN traffic
- D. wireless and wired traffic

Suggested Answer: A

Community vote distribution

D (100%)

🗳️ 👤 **Skliffi** Highly Voted 4 years, 3 months ago

D correct.

Note

When CPU ACL is enabled, it is applicable to both wireless and wired traffic.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/access_control_lists.html

upvoted 17 times

🗳️ 👤 **EvanABS** Highly Voted 4 years, 4 months ago

D is correct

upvoted 10 times

🗳️ 👤 **casterJR** Most Recent 8 months, 1 week ago

Correct answer is D

upvoted 1 times

🗳️ 👤 **Vlad_Is_Love_ua** 1 year, 5 months ago

Selected Answer: D

You have to decide which traffic you want to block/ permit for WLC CPU. Remember that when CPU ACL is enabled via GUI it apply for both wireless & wired traffic. If you want to conditionally apply this rule you can use CLI "config acl cpu <acl-name> {wired|wireless|both}"

upvoted 1 times

🗳️ 👤 **tuanalex** 3 years, 1 month ago

Selected Answer: D

D is correct

upvoted 4 times

🗳️ 👤 **Pawnstar** 3 years, 2 months ago

D is the correct answer.

upvoted 4 times

Refer to the exhibit. An engineer is creating an ACL to restrict some traffic to the WLC CPU. Which selection must be made from the direction drop-down list?

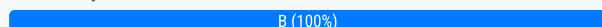
Access Control Lists > Rules > New

Sequence	<input type="text"/>
Source	<div>Any</div>
Destination	<div>Any</div>
Protocol	<div>Any</div>
DSCP	<div>Any</div>
Direction	<div>Any</div>
Action	<div>Any</div> <div>Inbound</div> <div>Outbound</div>

- A. It must be Inbound because traffic goes to the WLC.
- B. Packet direction has no significance; it is always Any.
- C. It must be Outbound because it is traffic that is generated from the WLC.
- D. To have the complete list of options, the CPU ACL must be created only by the CLI.

Suggested Answer: A

Community vote distribution



 Mimimimimi Highly Voted 1 year, 8 months ago

Does not matter which direction is selected. It will always be any for a CPU ACL.
Answer is B.

Source:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/bg_cg85/access_control_lists.html#:~:text=If%20you%20are%20planning%20to%20apply%20this%20ACL%20to%20the%20controller%20CPU%2C%20th
upvoted 12 times

 Den07 Highly Voted 3 years, 3 months ago

B should be the answer by looking at the configuration:

If the source and destination are any, the direction in which this ACL is applied can be any.

upvoted 8 times

 PicoOstrava Most Recent 8 months, 2 weeks ago

"For AireOS controllers using versions 6.0 and later, CPU ACLs are applicable for traffic originating both to and from the controller. Thus, when you're creating the ACLs and attaching them to the CPU, the ACL direction fields do not have any relevance." as per Official Cert Guide

upvoted 1 times

 Vlad_Is_Love_ua 11 months, 1 week ago

Selected Answer: B

If you are planning to apply this ACL to the controller CPU, the packet direction does not have any significance, it is always 'Any'.


https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/access_control_lists.html#ID2622:~:text=If%20you%20are%20planning%20to%20apply%20this%20ACL%20to%20the%20controller%20CPU%2C%20upvoted 2 times

 Guglielmino 2 years, 3 months ago

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71978-acl-wlc.html>

"Because this example uses any for the Source and Destination fields, you do not have to specify the direction. It can be left at its default value of any."

upvoted 1 times

  **anonymonkey** 2 years, 3 months ago

In this instance, the answer is any but not always as the second portion of option B states. per the source documentation referenced, this would only be any due to the source and destination being any making A the best choice.

upvoted 3 times

  **malkana** 2 years, 4 months ago

CPU ACLs only filter traffic towards the CPU, and not any traffic exiting or generated by the CPU.

Note: For the WLC 5500 series in versions 6.0 and later, the CPU ACL is applicable for traffic originated from the WLC as well. For the other WLC platforms, this behavior is implemented in versions 7.0 and later. Also, when creating CPU ACLs direction fields do not have any impact.

upvoted 1 times

  **kthekillerc** 2 years, 7 months ago



Provided answer is correct, the ACL on the WLC is to parse the incoming traffic to minimize WLC CPU.

upvoted 1 times

  **Pawnstar** 2 years, 8 months ago

The direction has no significance when it comes to CPU ACL's. B is the right answer.

upvoted 2 times

  **Vikiboy** 3 years, 3 months ago

Also, when creating CPU ACLs direction fields do not have any impact

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

upvoted 4 times

  **maro_moh** 3 years, 4 months ago

I think the correct answer is (B) because source and destination in the exhibit are Any

what do u think ??

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71978-acl-wlc.html>

upvoted 5 times

  **maro_moh** 3 years, 4 months ago

I think the correct answer is (B) because source and direction in the exhibit are Any

what do u think ??



<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71978-acl-wlc.html>

upvoted 4 times

An engineer must implement a CPU ACL that blocks web management traffic to the controller, but they also must allow guests to reach a Web Authentication Redirect page. To which IP address is guest client HTTPS traffic allowed for this to work?

- A. DNS server IP
- B. controller management IP
- C. virtual interface IP
- D. client interface IP

Suggested Answer: C

  **rrahim** 4 months, 1 week ago

Selected Answer: C

Virtual Interface IP:

The virtual interface IP address on the Cisco Wireless LAN Controller (WLC) is used for several purposes, including web authentication (e.g., guest access). When guests attempt to access the network, they are redirected to the web authentication page hosted on the virtual interface.

To allow guest clients to reach the Web Authentication Redirect page, HTTPS traffic must be permitted to the virtual interface IP address. This ensures that guests can complete the authentication process.

Why the Other Options Are Incorrect:

A. DNS server IP:

The DNS server IP is used for resolving domain names but is not directly involved in the web authentication process. It does not host the Web Authentication Redirect page.

B. controller management IP:

The controller management IP is used for managing the WLC (e.g., SSH, web GUI access). It is not used for guest web authentication.

D. client interface IP:

The client interface IP is used for client traffic but does not host the Web Authentication Redirect page. The virtual interface is specifically designed for this purpose.

upvoted 1 times

  **kthekillerc** 7 months, 3 weeks ago

provided answer is correct

upvoted 4 times

An engineer needs to configure an autonomous AP for 802.1x authentication. To achieve the highest security an authentication server is used for user authentication. During testing, the AP fails to pass the user authentication request to the authentication server. Which two details need to be configured on the AP to allow communication between the server and the AP? (Choose two.)

- A. username and password
- B. PAC encryption key
- C. RADIUS IP address
- D. shared secret
- E. group name

Suggested Answer: CD

🗲️ 👤 **GnXxUbik** 3 weeks ago

Selected Answer: CD

CD is correct

upvoted 1 times

🗲️ 👤 **rrahim** 4 months, 1 week ago

Selected Answer: CD

To allow communication between the autonomous AP and the RADIUS (authentication) server for 802.1X authentication, the following details must be configured on the AP:

C. RADIUS IP address: The AP needs to know the IP address of the RADIUS server to send authentication requests.

D. shared secret: The shared secret is a pre-shared key configured on both the AP and the RADIUS server to secure the communication between them. It ensures that the AP and the RADIUS server can trust each other.

upvoted 1 times

🗲️ 👤 **Le91** 8 months, 1 week ago

correct

upvoted 1 times

🗲️ 👤 **MaxMusti** 11 months ago

provided answer is correct

upvoted 1 times

A customer wants the APs in the CEO's office to have different usernames and passwords for administrative support than the other APs deployed throughout the facility. Which feature must be enabled on the WLC and APs to achieve this goal?

- A. local management users
- B. HTTPS access
- C. 802.1X supplicant credentials
- D. override global credentials

Suggested Answer: D

Community vote distribution

D (100%)

🗲️ 👤 **cskshiet** Highly Voted 1 year, 6 months ago

Correct answer is D:

You can set a global username, password, and enable password that all access points that are currently joined to the controller and any that join in the future inherit as they join the controller. If desired, you can override the global credentials and assign a unique username, password, and enable password for a specific access point.

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01101011.html
upvoted 8 times

🗲️ 👤 **joseph_climber** Highly Voted 1 year, 1 month ago

Selected Answer: D

You can set a global username, password, and enable password that all access points inherit as they join the controller including access points that are currently joined to the controller and any that join in the future. You can override the global credentials and assign a unique username, password, and enable password for a specific access point. The following are requirements enforced on the password:
upvoted 5 times

🗲️ 👤 **rrahim** Most Recent 4 months, 1 week ago

Selected Answer: D

To allow specific APs (such as those in the CEO's office) to have different usernames and passwords for administrative access than the other APs in the network, the override global credentials feature must be enabled on the Wireless LAN Controller (WLC) and the APs.

This feature allows you to configure unique administrative credentials for individual APs, overriding the global credentials that are applied to all APs by default.

It provides flexibility and enhanced security for sensitive areas like the CEO's office.
upvoted 1 times

🗲️ 👤 **kthekillerc** 10 months, 2 weeks ago

d is the correct answer
upvoted 3 times

🗲️ 👤 **kthekillerc** 1 year, 1 month ago

provided answer is correct
upvoted 1 times

An engineer configured a Cisco AireOS controller with two TACACS+ servers. The engineer notices that when the primary TACACS+ server fails, the WLC starts using the secondary server as expected, but the WLC does not use the primary server again until the secondary server fails or the controller is rebooted. Which cause of this issue is true?

- A. Fallback is enabled
- B. Fallback is disabled
- C. DNS query is disabled
- D. DNS query is enabled

Suggested Answer: B

  **Ocsicccnp** 9 months ago

Selected Answer: B

In off mode, the WLC supports failover only. In other words, fallback is disabled. When the primary RADIUS server goes down, the WLC will failover to the next

[https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/106258-radius-fbkftr-wlc-](https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/106258-radius-fbkftr-wlc-config.html#anc7:~:text=In%20off%20mode%2C%20the%20WLC%20supports%20failover%20only.%20In%20other%20words%2C%20fallback%20is%20disab)

[config.html#anc7:~:text=In%20off%20mode%2C%20the%20WLC%20supports%20failover%20only.%20In%20other%20words%2C%20fallback%20is%20disab](https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/106258-radius-fbkftr-wlc-config.html#anc7:~:text=In%20off%20mode%2C%20the%20WLC%20supports%20failover%20only.%20In%20other%20words%2C%20fallback%20is%20disab)
upvoted 1 times

  **rph02533** 2 years, 6 months ago

B correct



<https://community.cisco.com/t5/wireless/wlc-tacacs-fall-backfeature/td-p/3414217>

upvoted 2 times

  **kthekillerc** 3 years, 6 months ago

no there are 43 additional questions on the actual exam that are not on this site.

upvoted 2 times

  **miguelon** 3 years, 2 months ago

and where i can find the additional questions???

upvoted 1 times

  **ozone1864** 3 years, 7 months ago

Guys are these questions still valid ?

upvoted 1 times

  **MaxMusti** 11 months ago

Yes they are

upvoted 1 times

  **kthekillerc** 3 years, 7 months ago

provided answer is correct

upvoted 2 times

An engineer is implementing RADIUS to restrict administrative control to the network with the WLC management IP address of 192.168.1.10 and an AP subnet of 192.168.2.0/24. Which entry does the engineer define in the RADIUS server?

- A. administrative access defined on the WLC and the network range 192.168.2.0/255.255.254.0
- B. NAS entry of the virtual interface and the network range 192.168.2.0/255.255.255.0
- C. shared secret defined on the WLC and the network range 192.168.1.0/255.255.254.0
- D. WLC roles for commands and the network range 192.168.1.0/255.255.255.0

Suggested Answer: A

Community vote distribution

C (64%)

B (36%)

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

Selected Answer: C

I would say the correct answer should be C because the subnet given will cover both the mgmt interface and the AP range. Also the shared secret used on the WLC needs to be defined on the RADIUS.

upvoted 6 times

 **daeman** Highly Voted 2 years, 3 months ago

Selected Answer: B

The management IP of the WLC and the AP subnet must have be NAS entries on the RADIUS server in order for it to process the packet(s).

https://techhub.hp.com/eginfolib/networking/docs/switches/12500/5998-4885_security_cr/content/378521628.htm#:~:text=A%20RADIUS%20server%20identifies%20a,the%20server%20processes%20the%20packet.

upvoted 5 times

 **Robesera** 2 years, 2 months ago

Option B says NAS entry of the virtual interface. You need the mgmt IP in the RADIUS not the virtual interface IP

upvoted 5 times

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

Selected Answer: C

Evaluating Option C:

✓ "Shared secret defined on the WLC and the network range 192.168.1.0/255.255.254.0"

The shared secret between the WLC and RADIUS is required for authentication.

The subnet 192.168.1.0/23 (255.255.254.0) covers both 192.168.1.x (WLC) and 192.168.2.x (APs).

Since the APs communicate with the WLC for management and authentication, this subnet would allow both devices to be recognized within the same range.

□ This is indeed a correct and efficient approach, making Option C a strong contender.

upvoted 1 times

 **rrahim** 4 months, 1 week ago

Evaluating Option B:

□ "NAS entry of the virtual interface and the network range 192.168.2.0/255.255.255.0"

The NAS entry should be the virtual interface or management IP of the WLC.

However, limiting the subnet to only 192.168.2.0/24 means that it does not explicitly cover the WLC's management IP (192.168.1.10).

This might work for AP authentication but not necessarily for full WLC management authentication.

□ Potential Issue: If the WLC itself needs authentication via RADIUS, the WLC's management IP must be within the defined range.

Final Decision:

Given that Option C includes both the WLC management IP and AP subnet, as well as the required shared secret, it is indeed the best choice.

□ Final Answer: ✓ C. "Shared secret defined on the WLC and the network range 192.168.1.0/255.255.254.0"

upvoted 1 times

🗨️ 👤 **rrahim** 4 months, 2 weeks ago

Selected Answer: B

NAS (Network Access Server) Entry:

The NAS entry in the RADIUS server identifies the device (in this case, the WLC) that is acting as the gateway for RADIUS authentication.

The virtual interface IP address of the WLC is typically used for this purpose.

Network Range:

The AP subnet is 192.168.2.0/24, so the network range should be defined as 192.168.2.0/255.255.255.0 to match the AP subnet.

upvoted 1 times

🗨️ 👤 **[Removed]** 11 months, 2 weeks ago

Possible A?

says admin access to WLC (192.168.1.10) - ok

and network 192.168.2.0/255.255.254.0 - it includes 192.168.2.0 up to 3.0

upvoted 1 times

🗨️ 👤 **peer1024** 1 year, 2 months ago

Selected Answer: C

What do You need for RADIUS? shared secret and IP address OR IP address range! Using a IP address range is not the best design but it will work!

Keep in mind RADIUS need a "shared secret" nothing else. The given ip address range contains the WLC and all IPs.

upvoted 1 times

🗨️ 👤 **Zanjit500** 1 year, 6 months ago

Careful.

192.168.1.0 /23 (192.168.0.1 - 192.168.1.254)

192.168.2.0 /23 (192.168.2.1 - 192.168.3.254)

Neither covers both AP mgmt and WLC. I actually think the AP mgmt reference is a bum steer and irrelevant.

Closest is C though.

Another ridiculous illogical question with no logical answer. Well done Cisco, well done.

upvoted 5 times

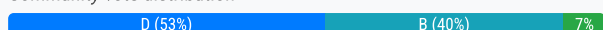
A customer requires wireless traffic from the branch to be routed through the firewall at corporate headquarters. A RADIUS server is in each branch location.

Which Cisco FlexConnect configuration must be used?

- A. central authentication and local switching
- B. central authentication and central switching
- C. local authentication and local switching
- D. local authentication and central switching

Suggested Answer: D

Community vote distribution



peer1024 Highly Voted 1 year, 6 months ago

Selected Answer: D

I can clearly say that I found the options on WLC 9800.

Within Policy Profile: Central Switching, Central Authentication, Central DHCP, Central Association. Each option can be set to on (enabled) or off (disabled)

The option to define a local RADIUS server or local users as well is within the flex profile.

The solution "local authentication and central switching" is possible on WLC 9800.

upvoted 6 times

rrahim Most Recent 4 months, 1 week ago

Selected Answer: D

Since the requirement is to route all wireless traffic through the HQ firewall, we need central switching (which sends all traffic to the HQ controller first).

✓ Local authentication (since RADIUS is at each branch).

✓ Central switching (to ensure traffic is sent to HQ).

□ Final Answer: □ D. Local authentication and central switching

upvoted 1 times

Bobydigital 7 months, 1 week ago

Selected Answer: C

Where is the information about where the WLC is located? If the WLC is in the cloud or another location but not in HQ? The traffic should go through the firewall to the HQ, the RADIUS is in the location.

Local auth/local switch

(C)

upvoted 1 times

peer1024 1 year, 2 months ago

Selected Answer: D

A RADIUS server is in each branch location. ----> local authentication

traffic through the firewall at corporate headquarters ----> central switching

Interesting thing is that the guys Gold Leader ignored the WLC 9800 and are still using AirOS. Is ths an AirOS or IOS XE related question?

upvoted 1 times

GoldLeader 1 year, 5 months ago

Selected Answer: B

B. - Not D. because:

Local authentication can only be enabled on the WLAN of a FlexConnect access point that is in local switching mode.

upvoted 4 times

  **BrockHarbor** 1 year, 4 months ago

I believe you are correct. The valid functional states are

Central auth/central switch

Central auth/local switch


Local auth/local switch

Auth Local/switch central is not a valid state

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/flexconnect.html#ID42

<https://wlanlessonslearned.wordpress.com/tag/flexconnect/>

upvoted 2 times

  **Zanjit500** 1 year, 6 months ago

Another ambiguous question with subjective answers.

I suspect they are looking for D.

If you were to overthink it though, you could argue that local auth + local switching would cause traffic to go over the WAN and presumably hit the main HQ firewall. But maybe traffic exiting the WLC centrally also goes via a FW. Who knows?

The Flexgroup is however the right place to configure your choice of local AAA servers,

upvoted 2 times


  **yrzy** 1 year, 9 months ago

Selected Answer: D

D is correct

config ap flexconnect radius auth set {primary | secondary} <ip_address> <auth_port> <secret> <Cisco_AP>

upvoted 1 times

  **rph02533** 2 years ago

Selected Answer: B

B is correct

There is NO local authentication/central switching in flexconnect state

refer : [https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-](https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/flexconnect.html#:~:text=192.168.201.226%20255.255.255.229%0Aend%0A!,-Configuring%20the%20Controller%20for%20FlexConnect,-You%20can%20configure)

[guide/b_cg810/flexconnect.html#:~:text=192.168.201.226%20255.255.255.229%0Aend%0A!,-Configuring%20the%20Controller%20for%20FlexConnect,-You%20can%20configure](https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/flexconnect.html#:~:text=192.168.201.226%20255.255.255.229%0Aend%0A!,-Configuring%20the%20Controller%20for%20FlexConnect,-You%20can%20configure)

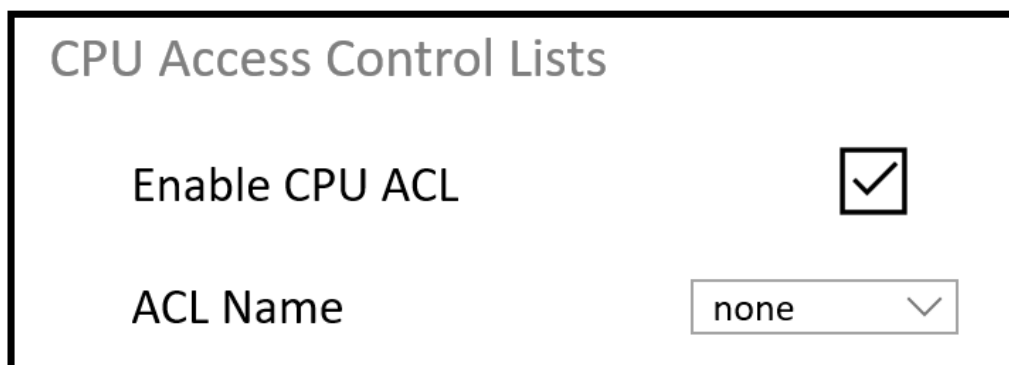
upvoted 2 times

  **yrzy** 1 year, 9 months ago

Table 1. WLANs "Example"

upvoted 1 times

Refer to the exhibit.



CPU Access Control Lists

Enable CPU ACL ☒

ACL Name none

An engineer must restrict some subnets to have access to the WLC. When the CPU ACL function is enabled, no ACLs in the drop-down list are seen. What is the cause of the problem?

- A. The ACL does not have a rule that is specified to the Management interface.
- B. No ACLs have been created under the Access Control List tab.
- C. When the ACL is created, it must be specified that it is a CPU ACL.
- D. This configuration must be performed through the CLI and not through the web GUI.

Suggested Answer: B

Community vote distribution

B (50%)

A (50%)

  **largestyle** 8 months ago

See <https://rscciew.wordpress.com/page/2/>

upvoted 1 times

  **raphim** 8 months, 2 weeks ago

Selected Answer: B

The only thing you have to do is create a ACL, "Enable CPU ACL" and select the ACL.



So B is correct

upvoted 2 times

  **Zanjit500** 1 year ago

B is correct. Tested on AireOS. If you dont have any ACLs created, then none will appear when enabling CPU ACL. Dont involve management interfaces and access to the WLC itself.


upvoted 2 times

  **TJR72** 1 year, 1 month ago

Selected Answer: A

When the CPU ACL function is enabled on the WLC, only the ACLs that have a rule specified for the Management interface will appear in the drop-down list. The Management interface is used for WLC management traffic, and if an ACL is not associated with it, it will not be available to be used as a CPU ACL. Therefore, the engineer needs to ensure that the ACL has a rule specified for the Management interface in order to be able to select it as a CPU ACL.

upvoted 2 times

  **rph02533** 1 year, 6 months ago

provided answer is correct

upvoted 1 times

An engineer configures the wireless LAN controller to perform 802.1x user authentication. Which configuration must be enabled to ensure that client devices can connect to the wireless, even when WLC cannot communicate with the RADIUS?

- A. pre-authentication
- B. local EAP
- C. authentication caching
- D. Cisco Centralized Key Management

Suggested Answer: B

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

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally on the controller. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, so it removes dependence on an external authentication server.

Reference: <http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/100590-ldap-eapfast-config.html>
upvoted 9 times

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

Selected Answer: B

When the WLC cannot communicate with the RADIUS server, it needs an alternative method to authenticate users. Local EAP allows the WLC to act as an authentication server and handle 802.1x authentication itself, without relying on an external RADIUS server.

Local EAP is a backup authentication method that provides authentication services when the external RADIUS server is unreachable. The WLC maintains a local user database or certificate-based authentication, allowing clients to authenticate without needing RADIUS.
upvoted 1 times



  **kthekillerc** 1 year ago

Provided answer is correct
upvoted 1 times

An IT team is growing quickly and needs a solution for management device access. The solution must authenticate users from an external repository instead of the current local on the WLC, and it must also identify the user and determine what level of access users should have. Which protocol do you recommend to achieve these goals?

- A. network policy server
- B. RADIUS
- C. TACACS+
- D. LDAP

Suggested Answer: C

  **rrahim** 4 months, 1 week ago

Selected Answer: C

TACACS+ (Terminal Access Controller Access-Control System Plus):

TACACS+ is specifically designed for device administration and provides detailed authorization and accounting capabilities.

It authenticates users against an external repository and can determine the level of access (authorization) based on user roles.

It is ideal for managing access to network devices, such as WLCs, and supports granular control over commands and permissions.

Why not the other options?

A. Network Policy Server (NPS):

NPS is a Microsoft implementation of RADIUS and is primarily used for network access control, not device administration.



B. RADIUS (Remote Authentication Dial-In User Service):

RADIUS is more suited for network access authentication (e.g., wireless or VPN) and lacks the granular authorization capabilities of TACACS+.

D. LDAP (Lightweight Directory Access Protocol):

LDAP is used for directory services and user authentication but does not provide the same level of granular authorization for device access as TACACS+.

upvoted 1 times

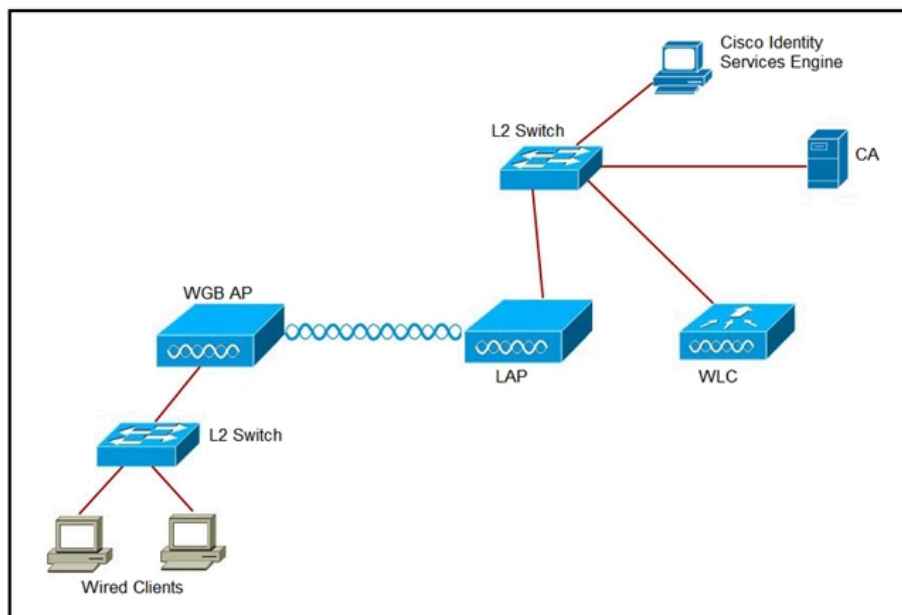
  **Liselot** 11 months, 1 week ago

C for sure!

upvoted 3 times

Refer to the exhibit. An engineer must connect a fork lift via a WGB to a wireless network and must authenticate the WGB certificate against the RADIUS server.

Which three steps are required for this configuration? (Choose three.)



- A. Configure the certificate, WLAN, and radio interface on WGB.
- B. Configure the certificate on the WLC.
- C. Configure WLAN to authenticate using ISE.
- D. Configure the access point with the root certificate from ISE.
- E. Configure WGB as a network device in ISE.
- F. Configure a policy on ISE to allow devices to connect that validate the certificate.

Suggested Answer: CDE

Community vote distribution

ACF (100%)

segr4523 Highly Voted 1 year, 3 months ago

Selected Answer: ACF

Worst question I saw on this exam....

I agree with daeman.

Explanations :

- A. Configure the certificate, WLAN, and radio interface on WGB. --> That's true
- B. Configure the certificate on the WLC. --> Nope, the WLC is the authenticator, it is neither authenticated or needs to authenticate anything
- C. Configure WLAN to authenticate using ISE. --> True, on the controller the SSID to which the WGB will connect must be configured, and broadcasted by the LAP
- D. Configure the access point with the root certificate from ISE. --> If they are talking about the WGB access point, then that's true, the root certificate that signed ISE certificate needs to be installed in the WGB AP
- E. Configure WGB as a network device in ISE. --> That's surely wrong. The WGB is not the authenticator in the dot1x process. It is the client. The controller is the authenticator.
- F. Configure a policy on ISE to allow devices to connect that validate the certificate. --> As I understand it, in some ways, that's true. We need to create an authentication/authorization policy on ISE so that the WGB AP will be authenticated by ISE based on the its certificate.

upvoted 8 times

rrahim Most Recent 4 months, 1 week ago

Selected Answer: ACF

A Workgroup Bridge (WGB) allows a non-wireless-capable device (like a forklift scanner or computer) to connect to a Wi-Fi network by acting as a client. Since the authentication must be performed using certificates and RADIUS (ISE), the following steps are required: