



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



## **CERTIFICATION TEST**

- [CertificationTest.net](https://CertificationTest.net) - Cheap & Quality Resources With Best Support

Which complication does a NAT introduce in SDP for a SIP call?

- A. Additional headers due to NAT encapsulation can cause the packet size to exceed the MTU.
- B. When the client is behind a NAT they may be unable to determine the appropriate offset due to time zones.
- C. The IP address specified in the connection data field may be an unrouteable internal address.
- D. The encryption keys advertised in the SDP are only valid for clients not behind a NAT.

**Suggested Answer:** C

Community vote distribution

C (100%)

🗳️ 👤 **veraiden** Highly Voted 👍 2 years, 2 months ago

Should be C: the problem is that if NAT enabled, some firewalls doesn't write the translated address into the SIP Signalling (fortinet for example has VIP feature that make it works).

upvoted 6 times

🗳️ 👤 **Collabinski** Most Recent 🕒 11 months, 1 week ago

Selected Answer: C

Cert Guide pg 182 -183

If a device were to try and route to the private IP address of another endpoint, the transmission would fail at the source router, because private IP addresses are not publicly routable

upvoted 1 times

🗳️ 👤 **ysrck** 1 year, 5 months ago

Selected Answer: C

Answer is C

upvoted 2 times

🗳️ 👤 **msully** 1 year, 6 months ago

Selected Answer: C

Answer is C

upvoted 2 times

🗳️ 👤 **chacthor** 1 year, 10 months ago

Selected Answer: C

Should be C

upvoted 3 times

🗳️ 👤 **rob79** 2 years, 2 months ago


This should be C

upvoted 3 times

A company already has a Cisco Unified Communications Manager for internal audio and video traffic, but it requires video communication with external partners and customers. It is important to ensure security for the deployment and the connectivity. What must be set up to enable this requirement?

- A. Cisco Unified Border Element and Cisco ASA Firewall
- B. Cisco Unified Border Element and Cisco Firepower Firewall
- C. Cisco Expressway-C and Cisco Expressway-E
- D. Cisco Expressway-C and Cisco Unified Border Element

**Suggested Answer:** C

 **Duke\_CT** 7 months, 2 weeks ago

To enable secure video communication with external partners and customers while ensuring security for the deployment and connectivity, the best option would be:

C. Cisco Expressway-C and Cisco Expressway-E

Cisco Expressway-C and Cisco Expressway-E together form the Cisco Expressway Series. They provide secure communication for remote and external users to connect with the internal Unified Communications Manager securely. Expressway-C is deployed inside the corporate network, while Expressway-E is deployed in the DMZ (Demilitarized Zone) to provide secure access for external users. This setup allows for secure traversal of firewalls and NAT (Network Address Translation) devices, ensuring both connectivity and security for external video communication.

upvoted 3 times

When an Expressway-E is configured for static NAT, which Session Description Protocol attribute is modified to reflect the NAT address?

- A. SDP b-line
- B. SIP record route
- C. SDP c-line
- D. SDP m-line

**Suggested Answer:** C

Community vote distribution

C (100%)

  **AKREM86** Highly Voted 2 years, 11 months ago

C is correct as c-line shows the connection information, Media IP address. So if it is natted it will be reflected there.  
upvoted 8 times



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

**Selected Answer: C**

With static NAT enabled on LAN2 of the Expressway-E, the c-line of the SIP INVITE has now been rewritten to c=IN IP4 64.100.0.10, and this means that when endpoint B sends outbound RTP media to endpoint A, this will be sent to IP address 64.100.0.10, the public NAT address of the NAT router, which is 1:1 NATed to the LAN2 IP address of the Expressway-E, 10.0.10.2. As RTP media from endpoint B arrives at the NAT router with a destination IP address of 64.100.0.10, the NAT router will forward these packets to the Expressway-E at 10.0.10.2 and two-way media is achieved.


[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X8-5/Cisco-Expressway-Basic-Configuration-Deployment-Guide-X8-5-2.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X8-5/Cisco-Expressway-Basic-Configuration-Deployment-Guide-X8-5-2.pdf)

upvoted 3 times

  **Simdude** 2 years, 12 months ago

it should be D

upvoted 1 times

  **iamnoone** 3 months, 1 week ago

No it shouldn't. B is correct.

upvoted 1 times

A company is installing Cisco Collaboration infrastructure and one of the requirements is that they must be able to communicate with many external parties that are using H.323 and SIP. Internally they want to register the endpoints only on SIP. Which functionality would describe the feature that needs to be enabled and where to achieve this?

- A. Interworking in Expressway-C
- B. Transcoding in Cisco Unified Communications Manager
- C. Transcoding in Expressway-C
- D. Interworking in Cisco Unified Communications Manager

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **ocero** 8 months, 3 weeks ago

Answer is Ajavascript:void(0)

upvoted 1 times

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

**Selected Answer: A**

By default, the Expressway acts as a SIP-H.323 and H.323-SIP gateway but only if at least one of the endpoints that are involved in the call is locally registered. You can change this setting so that the Expressway acts as a SIP-H.323 gateway regardless of whether the endpoints involved are locally registered. You also have the option to disable interworking completely.

The options for the H.323 <-> SIP interworking mode are:

- Off: The Expressway does not act as a SIP-H.323 gateway.
- Registered only: The Expressway acts as a SIP-H.323 gateway but only if at least one of the endpoints is locally registered.
- On: The Expressway acts as a SIP-H.323 gateway regardless of whether the endpoints are locally registered.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0-2/exwy\\_b\\_cisco-expressway-administrator-guide-x1402.pdf](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0-2/exwy_b_cisco-expressway-administrator-guide-x1402.pdf)

upvoted 3 times

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

**Selected Answer: A**

Answer is A

upvoted 2 times

🗳️ 👤 **msully** 2 years, 6 months ago

**Selected Answer: A**

Answer is A

upvoted 2 times

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

**Selected Answer: A**

Should be A

upvoted 2 times

🗳️ 👤 **tilo1988** 2 years, 11 months ago

change the correct answer to A please

upvoted 1 times

🗳️ 👤 **leigh1141** 3 years, 10 months ago

Interworking - interworking is required on expressway series to interwork h.323 to SIP calls. CUCM is SIP only and does not support H.323 calls.

Inteworking for B2B calls is always done at expressway level

upvoted 2 times

🗳️ 👤 **Mark03** 3 years, 10 months ago

Answer is A Interworking to convert between SIP and H323

upvoted 2 times

  **Abhishek1610** 3 years, 12 months ago

Correct answer is A. Interworking in Expressway-C

upvoted 1 times

  **mactian007** 4 years ago


Answer should be A

upvoted 3 times

  **khader09** 4 years, 2 months ago

B. Transcoding in Cisco Unified Communications Manager. Using g.711 codec internally and 729 externally.

upvoted 2 times

  **BangBang86** 4 years, 4 months ago

No transcoding is needed here, since there is no need to convert codecs, instead interworking from SIP to H.323 and vice-versa for the signaling.

upvoted 4 times

What is a key configuration requirement for Hybrid Message Service High Availability deployment with multiple IM and Presence clusters?

- A. You must have the Intercluster Sync Agent working across your IM and Presence clusters.
- B. You must have the Intercluster Lookup Service working across all of your IM and Presence clusters.
- C. Your IM and Presence Service clusters must have Multiple Device Messaging disabled.
- D. AXL service should be activated only on the publisher of each IM and Presence cluster.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **Collabinski** 11 months, 1 week ago

**Selected Answer: A**

- If you have multiple IM and Presence Service clusters, you must have the Intercluster Sync Agent (ICSA) working across them.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/spark/hybridservices/messageservice/cmgt\\_b\\_spark-hybrid-message-deployment-guide/cmgt\\_b\\_spark-hybrid-message-deployment-guide\\_chapter\\_01.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/messageservice/cmgt_b_spark-hybrid-message-deployment-guide/cmgt_b_spark-hybrid-message-deployment-guide_chapter_01.html)

upvoted 3 times

🗳️ 👤 **Ol\_Mykhailiuk** 1 year, 1 month ago

**Selected Answer: A**

The Cisco Sync Agent must be running on the database publisher node of each intercluster peer on the local and remote IM and Presence database publisher nodes.

upvoted 1 times

🗳️ 👤 **Mark03** 2 years, 10 months ago

A is correct

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/im\\_presence/configAdminGuide/11\\_5\\_1/cup0\\_b\\_config-and-admin-guide-1151su5/cup0\\_b\\_imp-system-configuration-1151su5\\_chapter\\_01100.pdf](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/11_5_1/cup0_b_config-and-admin-guide-1151su5/cup0_b_imp-system-configuration-1151su5_chapter_01100.pdf)

upvoted 4 times

Cisco Collaboration endpoints are exchanging encrypted signaling messages.  
What is one major complication in implementing NAT ALG for voice and video devices?

- A. Internal endpoints cannot use addresses from the private address space.
- B. The NAT ALG cannot inspect the contents of encrypted signaling messages.
- C. NAT ALG introduces jitter in the voice path.
- D. Source addresses cannot provide the destination addresses that remote endpoints should use for return packets.

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **rob79** Highly Voted 2 years, 2 months ago

NAT ALGs never work anyway.  
upvoted 9 times

🗳️ 👤 **Collabinski** Most Recent 11 months, 1 week ago

**Selected Answer: B**

Answer is B  
upvoted 1 times

🗳️ 👤 **msully** 1 year, 6 months ago

**Selected Answer: B**

Answer is B

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X14-0/basic\\_config/exwy\\_b\\_cisco-expressway-e-and-expressway-c-basic-configuration-deployment-guide-x14-0/exwy\\_m\\_advanced-networking-deployments.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0/basic_config/exwy_b_cisco-expressway-e-and-expressway-c-basic-configuration-deployment-guide-x14-0/exwy_m_advanced-networking-deployments.html)

upvoted 2 times

🗳️ 👤 **leigh1141** 2 years, 10 months ago

The NAT ALG cannot inspect the contents of encrypted signaling message -  
[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/srnd/collab11/collab11/security.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11/security.html)  
upvoted 2 times

🗳️ 👤 **Mark03** 2 years, 10 months ago

Answer is B - AKREM86 is right  
upvoted 1 times

🗳️ 👤 **AKREM86** 2 years, 11 months ago

Ref: [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/srnd/collab11/collab11/security.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11/security.html)  
upvoted 2 times

🗳️ 👤 **khader09** 3 years, 2 months ago

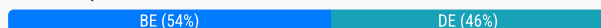
A NAT ALG is similar to a firewall ALG, but a NAT ALG actually changes (maps) the addresses and ports in the signaling messages. The NAT ALG cannot inspect the contents of encrypted signaling messages.  
upvoted 4 times

What are two reasons why port 8443 is unreachable from the Internet to the Expressway-E? (Choose two.)

- A. The MRA license is missing on the Expressway-E.
- B. The Unified Communications zone is down.
- C. Transform is not configured on Expressway-E.
- D. The SRV record for \_cisco-uds is misconfigured.
- E. The firewall is blocking the port.

**Suggested Answer:** BE

Community vote distribution



**somedudebob** Highly Voted 3 years, 1 month ago

Traffic is coming from the internet so can not be the cisco\_uds record, as it is created on the internal DNS only. Collab\_edge is the external DNS record. It has to be port blocked or traversal zone down  
upvoted 6 times

**BangBang86** Highly Voted 3 years, 4 months ago

Either port blocked, or the UC traversal zone is down.  
upvoted 6 times

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

Selected Answer: DE

D & E are correct. The links in the comments do not refer to UC Zone at all.  
upvoted 1 times

**cyberknock** 12 months ago

Selected Answer: DE

there is no unified communications zone, it is for sure DE, the \_cisco-uds record must be present  
upvoted 1 times

**preki10** 1 year ago

Selected Answer: DE

There is no "Unified Communications zone", B can't be right....cannot assume it refers to "Unified Communications traversal zone"  
upvoted 1 times

**TestingAAgain** 1 year, 6 months ago

Selected Answer: DE

Traffic coming through an MRA pair (C&E) DOES use the \_cisco-uds record to get from the C to CUCM. B is wrong because there is no unified Communications Zone (there is a UC Traversal zone, close, but different) in the expressway. Since the 8443 traffic is actually destined for CUCM, if the \_cisco-uds record is botched, it won't get there...and thus it will be unreachable.  
upvoted 3 times

**msully** 1 year, 6 months ago

Selected Answer: BE

B and E. Collab-edge is used for MRA, not UDS.  
upvoted 5 times

**chacthor** 1 year, 10 months ago

Selected Answer: BE

Should be BE  
upvoted 4 times

**rlcabrini** 2 years, 11 months ago

<https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/118798-technote-cucm-00.html#anc6>

Topic 1

B - The Unified Communications zone is down.

E - Firewall is blocking.

upvoted 4 times

  **Collabinski** 11 months, 2 weeks ago



Nothing in this link specifies anything about a "UC Zone". It does mention both the \_cisco-uds SRV and firewalls blocking ports,

upvoted 1 times

  **khader09** 3 years, 2 months ago

D and E are correct

upvoted 1 times

  **msully** 1 year, 10 months ago

Not D, cisco-uds is an internal srv, collab-edge is the external (internet facing) srv record

upvoted 2 times

Which media encryption mode can be configured on an Expressway zone?

- A. Advanced Encryption Standard
- B. IPsec
- C. Triple Data Encryption Standard
- D. force unencrypted

**Suggested Answer: D**

Community vote distribution

D (100%)

🗳️ 👤 **khader09** Highly Voted 🏆 3 years, 8 months ago

D. force unencrypted  
upvoted 7 times

🗳️ 👤 **aocstr** Most Recent ⌚ 11 months ago

**Selected Answer: D**

answer is D  
upvoted 3 times

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

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0-1/exwy\\_b\\_cisco-expressway-administrator-guide-x14-0-1/exwy\\_m\\_zones-and-neighbors.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0-1/exwy_b_cisco-expressway-administrator-guide-x14-0-1/exwy_m_zones-and-neighbors.html)  
upvoted 1 times

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

**Selected Answer: D**

The encryption mode options are:

- Force encrypted: All media to and from the zone/subzone must be encrypted. If the target system/endpoint is configured to not use encryption, then the call will be dropped.
  - Force unencrypted: All media must be unencrypted. If the target system/endpoint is configured to use encryption, then the call may be dropped; if it is configured to use Best effort then the call will fall back to unencrypted media.
  - Best effort: Use encryption if available, otherwise fall back to unencrypted media.
  - Auto: No specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on the target system/endpoint requests. This is the default behavior and is equivalent to how the Expressway operated before this feature was introduced.
- Encryption policy (any encryption setting other than Auto) is applied to a call by routing it through a back-to-back user agent (B2BUA) hosted on the Expressway.

upvoted 2 times

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

Should be D  
upvoted 1 times

🗳️ 👤 **Abhishek1610** 3 years, 6 months ago

Available modes are "Force encrypted, Force unencrypted, Auto and Best Effort"  
So the answer is option D - "Force unencrypted".  
upvoted 4 times

🗳️ 👤 **BangBang86** 3 years, 10 months ago

Available modes are "Force encrypted, Force unencrypted, Auto and Best Effort".  
upvoted 4 times

What is the purpose of a transform in the Expressway server?

- A. A transform has the function as a neighbor zone in the Expressway. It creates a connection with another server.
- B. A transform changes the audio codec when the call goes through the Expressway.
- C. A transform is used to route calls to a destination.
- D. A transform changes an alias that matches certain criteria into another alias.

**Suggested Answer:** D

*Community vote distribution*

D (100%)

  **Collabinski** 11 months, 1 week ago

**Selected Answer: D**

Pre-search transform configuration allows the destination alias (called address) in an incoming search request to be modified. The Expressway applies the transformation before any searches are sent to external zones.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X14-0/basic\\_config/exwy\\_b\\_cisco-expressway-e-and-expressway-c-basic-configuration-deployment-guide-x14-0/exwy\\_m\\_routing-configuration.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0/basic_config/exwy_b_cisco-expressway-e-and-expressway-c-basic-configuration-deployment-guide-x14-0/exwy_m_routing-configuration.html)

upvoted 2 times

  **cyberknock** 1 year ago

**Selected Answer: D**

D is true

upvoted 2 times

  **khader09** 3 years, 2 months ago

D is correct

upvoted 4 times

An organization with a domain name of example.com.

Which two SRV records are valid for a SIP and H.323 communication? (Choose two.)

- A. \_sips.\_tcp.example.com
- B. \_sips.\_udp.example.com
- C. \_h323ls.\_udp.example.com
- D. \_h323ls.\_tcp.example.com
- E. \_collab-edge.\_tls.example.com

**Suggested Answer: AC**

Community vote distribution

AC (100%)



  **Collabinski** 11 months, 1 week ago

**Selected Answer: AC**

The format of DNS SRV queries for sip (RFC 3263) and H.323 used by Expressway are:

- \_sips.\_tcp.<fully.qualified.domain>
- \_sip.\_tcp.<fully.qualified.domain>
- \_sip.\_udp.<fully.qualified.domain> - not recommended for video calls, only use for audio-only calls
- \_h323ls.\_udp.<fully.qualified.domain> - for UDP location (RAS) signaling, such as LRQ
- \_h323cs.\_tcp.<fully.qualified.domain> - for H.323 call signaling

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-6/exwy\\_b\\_cluster-creation-maintenance-deployment-guide/exwy\\_b\\_cluster-creation-maintenance-deployment-guide\\_chapter\\_01010.html#concept\\_F5323B1B7F8CED8A4ACEE5D70EC43C4B](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-6/exwy_b_cluster-creation-maintenance-deployment-guide/exwy_b_cluster-creation-maintenance-deployment-guide_chapter_01010.html#concept_F5323B1B7F8CED8A4ACEE5D70EC43C4B)  
upvoted 1 times

  **msully** 1 year, 6 months ago

**Selected Answer: AC**

A and C. Official cert guide page 204  
upvoted 1 times

  **chamba87** 2 years, 10 months ago

The format of DNS SRV queries for sip (RFC 3263) and H.323 used by Expressway are:

- \_sips.\_tcp.<fully.qualified.domain>
- \_sip.\_tcp.<fully.qualified.domain>
- \_sip.\_udp.<fully.qualified.domain> - not recommended for video calls, only use for audio-only calls
- \_h323ls.\_udp.<fully.qualified.domain> - for UDP location (RAS) signaling, such as LRQ
- \_h323cs.\_tcp.<fully.qualified.domain> - for H.323 call signaling

The format of DNS SRV queries for sip (RFC 3263) and H.323 typically used by an endpoint are:

- \_sips.\_tcp.<fully.qualified.domain>
- \_sip.\_tcp.<fully.qualified.domain>
- \_sip.\_udp.<fully.qualified.domain> - not recommended for video calls, only use for audio-only calls
- \_h323ls.\_udp.<fully.qualified.domain> - for UDP location (RAS) signaling, such as LRQ

\_h323cs.\_tcp.<fully.qualified.domain> - for H.323 call signaling

\_h323rs.\_udp.<fully.qualified.domain> - for H.323 registrations

upvoted 1 times

🗨️ 👤 **Mark03** 2 years, 10 months ago

That is correct, A & C

upvoted 1 times

🗨️ 👤 **khader09** 3 years, 2 months ago

A and C are correct

upvoted 3 times


What is the Cisco-recommended key length in bits for a Cisco Expressway certificate?

- A. 1024
- B. 2048
- C. 4096
- D. 8192

**Suggested Answer: C**

Community vote distribution

C (100%)


 **iamnoone** 3 months, 2 weeks ago

**Selected Answer: C**

It's not specified in the documentation, but it's common as a best practice to use 4096 nowadays.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X14-3/cert\\_creation\\_use/exwy\\_b\\_cisco-expressway-certificate-creation-and-use-deployment-guide-x14-3/exwy\\_m\\_generating-a-certificate-signing-request.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-3/cert_creation_use/exwy_b_cisco-expressway-certificate-creation-and-use-deployment-guide-x14-3/exwy_m_generating-a-certificate-signing-request.html)

upvoted 1 times

 **Collabinski** 11 months, 1 week ago

**Selected Answer: C**

Certificates with Key Length of 8192 Bits

SIP TLS zones may fail to become active if certificates use a key length of 8192 bits. We recommend using certificates with a key length of 4096 bits.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-5/exwy\\_b\\_certificate-creation-use-deployment-guide/exwy\\_b\\_certificate-creation-use-deployment-guide\\_chapter\\_01000.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-5/exwy_b_certificate-creation-use-deployment-guide/exwy_b_certificate-creation-use-deployment-guide_chapter_01000.html)

upvoted 1 times

 **Ol\_Mykhailiuk** 1 year, 1 month ago

**Selected Answer: C**

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-5/exwy\\_b\\_certificate-creation-use-deployment-guide/exwy\\_b\\_certificate-creation-use-deployment-guide\\_chapter\\_01000.html#:~:text=We%20recommend%20using%20certificates%20with%20a%20key%20length%20of%204096%20bits.](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-5/exwy_b_certificate-creation-use-deployment-guide/exwy_b_certificate-creation-use-deployment-guide_chapter_01000.html#:~:text=We%20recommend%20using%20certificates%20with%20a%20key%20length%20of%204096%20bits.)

SIP TLS zones may fail to become active if certificates use a key length of 8192 bits. We recommend using certificates with a key length of 4096 bits.

upvoted 1 times

 **leigh1141** 2 years, 10 months ago

Answer is D - [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X8-9/Cisco-Expressway-Certificate-Creation-and-Use-Deployment-Guide-X8-9.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X8-9/Cisco-Expressway-Certificate-Creation-and-Use-Deployment-Guide-X8-9.pdf)

upvoted 1 times

 **leigh1141** 2 years, 10 months ago

Typo in answer it's C - 4096

upvoted 2 times

 **khader09** 3 years, 2 months ago

recommend using

certificates with a key length of 4096 bits.

upvoted 3 times

`(\d{3}) (\d{3}) (\d{3}) (\d{3})`


Refer to the exhibit. Which two numbers match the regular expression? (Choose two.)

- A. d20d16d20d22
- B. 2091652010224
- C. 209165200225
- D. d209d165d200d224
- E. 209165200224

**Suggested Answer:** *CE*

Community vote distribution

CE (100%)

 **iamnoone** 3 months, 2 weeks ago

**Selected Answer:** CE

`\d`: This is a special sequence in regex that matches any digit (equivalent to `[0-9]`).

`{3}`: This is a quantifier that specifies exactly how many times the preceding element should be repeated. In this case, it means that exactly three digits should be matched.

`(\d{3})`: The parentheses around `\d{3}` create a capture group. This means that the matched sequence of three digits is stored as a group, which can be referenced later in the regex or in the code that uses the regex.

So, the entire regex `(\d{3})(\d{3})(\d{3})(\d{3})` matches a string that consists of four groups of exactly three digits each.

C&E contain 4 groups of 3 digits.

upvoted 1 times

 **Collabinski** 11 months, 1 week ago

**Selected Answer:** CE

The third use of backslash is for specifying generic character types. The following are always recognized:

`\d` any decimal digit

`\D` any character that is not a decimal digit

`\s` any whitespace character

`\S` any character that is not a whitespace character

`\w` any "word" character

`\W` any "non-word" character

`\d{8}`

matches exactly 8 digits. An opening curly bracket that appears in a position where a quantifier is not allowed, or one that does not match the syntax of a quantifier, is taken as a literal character.

upvoted 1 times

 **JamieF66** 2 years, 2 months ago

CE are correct

upvoted 2 times

A company has enabled ICE to optimize call flows and improve video quality between their Cisco Collaboration endpoints internally and externally. For which reason would you see activity on the TURN server when a call is established between two external endpoints?

- A. The video call is using encryption, which is not supported by ICE with CUCM 12.5
- B. ICE cannot reduce the packet loss on the link
- C. A STUN cannot punch holes in the firewall
- D. The video call is using 4K resolution, which is not supported by ICE with CUCM 12.5

**Suggested Answer: C**

Community vote distribution


C (100%)

 **virtu** Highly Voted 2 years, 10 months ago

The answer is C "Those addresses (A, B, and C) populate the SIP SDP offer and answer as ICE candidates, and after the signaling has gone through, both endpoints will have the remote party ICE candidate addresses. It is at that point that the endpoints do a connectivity check by sending STUN messages to one another in an attempt to punch transport holes in the firewalls in order to establish media connectivity between peers."


<https://www.cisco.com/c/en/us/td/docs/solutions/PA/ICE/icepa125.html>

upvoted 11 times

 **jagifoto** Most Recent 10 months ago

Answer is C. <https://www.cisco.com/c/en/us/td/docs/solutions/PA/ICE/icepa125.html>

upvoted 1 times


 **Collabinski** 11 months, 1 week ago

**Selected Answer: C**

Interactive Connectivity Establishment (ICE), defined in RFC 8445, is a protocol that combines STUN and TURN. Using ICE, endpoints can determine if there is direct connectivity between them and will then apply the STUN hole-punching techniques to keep the firewall ports opened, thus allowing for both inbound and outbound media traffic. If direct media connectivity cannot be achieved, the endpoints will fall back to the TURN server and will send their UDP traffic centrally instead of going peer-to-peer.

<https://www.cisco.com/c/en/us/td/docs/solutions/PA/ICE/icepa125.html>

upvoted 3 times

 **msully** 1 year, 6 months ago

**Selected Answer: C**

As virtu said, the answer is C

upvoted 1 times


Which role does Call Policy play when preventing toll fraud on Expressways?

- A. It controls which calls are allowed, which calls are rejected, and which calls are redirected to a different destination.
- B. It changes the calling and called number on a call.
- C. It changes the audio protocol used by a call through Expressways.
- D. It changes the audio codec used in a call through Expressways.

**Suggested Answer: A**

Community vote distribution

A (100%)

 **iamnoone** 3 months, 2 weeks ago

**Selected Answer: A**

Call Policy plays a key role in preventing toll fraud on Cisco Expressways by enabling administrators to define rules that determine how calls are handled based on their source and destination. Specifically, Call Policy allows the following actions:

- 1) Allowing calls: Permitting legitimate calls to proceed.
- 2) Rejecting calls: Blocking unauthorized or suspicious calls, such as those associated with toll fraud attempts.
- 3) Redirecting calls: Sending calls to a different destination if necessary.

<chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2025/pdf/BRKCOL-2116.pdf>  
upvoted 1 times

 **Collabinski** 11 months, 1 week ago

**Selected Answer: A**

You can set up rules to control which calls are allowed, which calls are rejected, and which calls are to be redirected to a different destination. These rules are known as Call Policy (or Administrator Policy).

If Call Policy is enabled and has been configured, each time a call is made the Expressway will execute the policy in order to decide, based on the source and destination of the call, whether to:

- Proxy the call to its original destination.
- Redirect the call to a different destination or set of destinations.
- Reject the call.

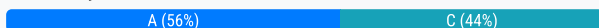
[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0/exwy\\_b\\_cisco-expressway-administrator-guide/exwy\\_m\\_dial-plan-and-call-processing.html#concept\\_8876F177CE697E827E6FD343D743CC1F](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0/exwy_b_cisco-expressway-administrator-guide/exwy_m_dial-plan-and-call-processing.html#concept_8876F177CE697E827E6FD343D743CC1F)  
upvoted 3 times

What happens to the encrypted signaling traffic of a collaboration device if you place it inside a firewall with private IP addresses and try to make a call over IP without any collaboration infrastructure?

- A. The signaling makes it back to the endpoint because the firewall is an application layer gateway and provides address translation.
- B. Encrypted IP traffic for collaboration devices always is trusted by the firewall.
- C. The signaling does not make it back to the endpoint because the firewall cannot inspect encrypted traffic.
- D. The signaling makes it back to the endpoint because the endpoint sent the private address to the external endpoint.

**Suggested Answer: A**

Community vote distribution



🗳️ **khader09** Highly Voted 3 years, 2 months ago

The signaling does not make it back to the endpoint because the firewall cannot inspect encrypted traffic.  
upvoted 8 times

🗳️ **TestingAAgain** Highly Voted 1 year, 6 months ago

**Selected Answer: A**

Don't like this question. However, the key to the question is that we're talking about signaling that is encrypted. That means TLS over TCP/IP. Since the station is initiating the connection to the outside via TCP/IP (with TLS on top), the signaling traffic will go through, and return traffic come back via the dynamic NAT from the firewall. Has nothing to do with the traffic being "always trusted" though. The media is a different story. Media exchange would fail as the device would not be reachable from the outside without additional collaboration infrastructure unless you are using some form of static NAT. So, the best answer here is A.  
upvoted 5 times

🗳️ **iulianm** 1 year, 5 months ago

A NAT ALG is similar to a firewall ALG, but a NAT ALG actually changes (maps) the addresses and ports in the signaling messages. The NAT ALG cannot inspect the contents of encrypted signaling messages. Answer C  
upvoted 1 times

🗳️ **daniepad** Most Recent 1 month ago

**Selected Answer: C**

C. The signaling does not make it back to the endpoint because the firewall cannot inspect encrypted traffic.  
Here's why:

When a collaboration device is behind a firewall with a private IP, it cannot be directly reached from the outside world unless NAT traversal or a specific collaboration infrastructure is in place.

If the signaling is encrypted (e.g., SIP over TLS), the firewall cannot inspect or modify the payload to help with NAT traversal.

This makes C the most technically accurate and complete explanation.  
upvoted 1 times

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

**Selected Answer: C**

If the signaling flows do not go through the firewall so that the firewall can inspect the signaling traffic, the RTP streams could be blocked because the firewall will not know which ports need to be opened to allow the RTP streams for a conversation.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/srnd/collab12/collab12/security.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12/security.html)

upvoted 2 times

🗳️ **cyberknock** 12 months ago

**Selected Answer: C**

Answer C, because firewall cannot inspect the encrypted traffic and is not able to rewrite ip addresses  
upvoted 2 times

🗳️ **BangBang86** 3 years, 4 months ago

The signaling does not make it back.  
upvoted 1 times

Which statement about scheduling Expressway backups is true?

- A. It is not supported on the application.
- B. It is allowed from the application CLI of the Expressway only.
- C. It is allowed from the application CLI and GUI of the Expressway.
- D. It is allowed from the application GUI of the Expressway only.

**Suggested Answer: A**

Community vote distribution

A (100%)

  **BangBang86** Highly Voted 3 years, 4 months ago

Scheduling backups is not supported in the Expressway code.  
upvoted 10 times

  **khader09** Highly Voted 3 years, 2 months ago

We cannot schedule backup  
upvoted 5 times



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

Selected Answer: A  
Scheduled backups are not supported for Cisco Expressways. This Community thread talks about how to automate outside of Cisco.

<https://community.cisco.com/t5/telepresence-and-video-infrastructure/how-to-automate-expressway-e-and-c-backups/m-p/4305067>  
upvoted 4 times

  **cyberknock** 1 year ago



Selected Answer: A  
Scheduling Backups will come in X15 next year. Correct anser A  
upvoted 1 times

  **kljw5** 1 year, 7 months ago

These answers are all incorrect or have been resolved in recent updates. Backups are available in the GUI. They save Call Details and Certificates. There are other new questions in this exam that are similar. Be sure to update with new admin guide information.  
upvoted 1 times

  **kljw5** 1 year, 7 months ago

I stand corrected. the question is about scheduling backups. "scheduling" is not a feature available.  
upvoted 1 times

  **chacthor** 1 year, 10 months ago

Should be A  
upvoted 2 times

Between which two DTMF relay methods does the Expressway support interworking? (Choose two.)

- A. unsolicited notify
- B. RFC 2833
- C. KPML
- D. passthrough
- E. H.245 user input indication

**Suggested Answer:** BE

Reference:

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/Cisco-Expressway-Administrator-Guide-X12-6.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/admin_guide/Cisco-Expressway-Administrator-Guide-X12-6.pdf)


Community vote distribution

BE (100%)

 **jonycakes** Highly Voted 2 years ago

B&E: When the Expressway is interworking a call between SIP and H.323, it also interworks the DTMF signaling, but only between RFC 2833 DTMF, and the H.245 user input indicators "dtmf" and "basicString".

Source: [https://jerome.pro:8443/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/Cisco-Expressway-Administrator-Guide-X12-5.pdf](https://jerome.pro:8443/c/dam/en/us/td/docs/voice_ip_comm/expressway/admin_guide/Cisco-Expressway-Administrator-Guide-X12-5.pdf)  
upvoted 5 times

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

**Selected Answer: BE**

Interworking DTMF signals

For SIP calls, the Expressway implements RFC 2833 for DTMF signaling in RTP payloads.

For H.323 calls, the Expressway implements H.245 UserInputIndication for DTMF signaling. dtmf is the only supported UserInputCapability. Expressway does not support any other H.245 user input capabilities (eg. basicString, generalString)

When the Expressway is interworking a call between SIP and H.323, it also interworks the DTMF signaling, but only between RFC 2833 DTMF, and the H.245 user input indicators "dtmf" and "basicString".

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0-2/exwy\\_b\\_cisco-expressway-administrator-guide-x1402.pdf](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0-2/exwy_b_cisco-expressway-administrator-guide-x1402.pdf)  
upvoted 2 times

What allows endpoints behind a NAT to discover the paths through which they will pass media?

- A. RTP
- B. TLS
- C. SNMP
- D. ICE

**Suggested Answer:** D

Reference:

<https://www.cisco.com/c/en/us/td/docs/solutions/PA/ICE/icepa125.html>

*Community vote distribution*

D (100%)


  **Collabinski** 11 months, 1 week ago

**Selected Answer: D**

ICE makes use of Traversal Using Relay NAT (TURN) and Session Traversal Utilities for NAT (STUN) to optimize the media path of MRA calls.


<https://www.cisco.com/c/en/us/td/docs/solutions/PA/ICE/icepa125.html>

upvoted 3 times

  **Tristam22** 9 months, 2 weeks ago

Where is Cisco 300-820 questions ? I don't see it here anymore. Only in discussions.

upvoted 4 times

  **NIPProject** 9 months, 2 weeks ago

Where is All Cisco dumps? I can't find them

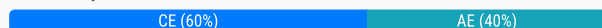
upvoted 3 times

Which two types of information does Cisco Expressway back up? (Choose two.)

- A. call records
- B. log files
- C. IP addresses
- D. current call states
- E. security certificates

**Suggested Answer:** CE

Community vote distribution



**jonycakes** Highly Voted 3 years, 1 month ago

What Gets Backed Up: A&E

The data saved to a backup file includes:

- Bootstrap key (from X8.11)
- System configuration settings
- Clustering configuration
- Local authentication data (but not Active Directory credentials for remotely managed accounts)
  - User account and password details
  - Server security certificate and private key
- Call detail records (if the CDR service on Expressway is enabled)

Source: [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/Cisco-Expressway-Administrator-Guide-X8-11-4.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/admin_guide/Cisco-Expressway-Administrator-Guide-X8-11-4.pdf)  
upvoted 8 times

**Collabinski** 1 year, 11 months ago

Definitely a loaded question. E. is a given, but for Call Records to work the CDR service on expressway need to be enabled and IP addresses are found in the System Config. I couldn't see why an admin would not enable CDR since it has many benefits, so I think I would choose A over C since it's pretty vague.

upvoted 1 times

**AAMM** 2 years, 7 months ago

then it should be A&C

upvoted 1 times

**Omitted** 2 years, 6 months ago

I think A & E make the most sense based on this document but IP addresses is rather ambiguous and could fall under system configuration settings...

upvoted 2 times

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

**Selected Answer: CE**

I just labbed this up as I was confused. call records are only backed up if selected. They are not backed up by default. Current call states are not backed up. Log files are not backed up. However IP Addresses are part of the configuration, as are the SSL certificates (both server and CA that have been loaded. The correct answers are C and E

upvoted 5 times

**Omitted** 2 years, 6 months ago

The question (here at least) isn't asking what is backed up by default though.

upvoted 1 times

**TestingAAgain** 2 years, 6 months ago

True it isn't. But you only get 2 answers and IP addresses and SSL certs are backed up by default. CDR isn't. Which two you gonna chose?

upvoted 2 times

**ingbioriznova** Most Recent 9 months, 3 weeks ago

It is C and E because according to this link the system configuration includes the IP address:[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0-1/exwy\\_b\\_cisco-expressway-administrator-guide-x14-0-1/exwy\\_m\\_maintenance.html#reference\\_34747E548B7AAE12D29DFD43A90B3A8D](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0-1/exwy_b_cisco-expressway-administrator-guide-x14-0-1/exwy_m_maintenance.html#reference_34747E548B7AAE12D29DFD43A90B3A8D)  
upvoted 2 times

🗨️ 👤 **sandman0409** 1 year, 3 months ago

**Selected Answer: AE**

think it should be A&E. Cisco didn't mention about IP addresses being backed up by Expressway servers.

Source: [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0-1/exwy\\_b\\_cisco-expressway-administrator-guide-x14-0-1/exwy\\_m\\_maintenance.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0-1/exwy_b_cisco-expressway-administrator-guide-x14-0-1/exwy_m_maintenance.html)  
upvoted 2 times

🗨️ 👤 **RafaKarz** 1 year, 4 months ago

Explanation:

The data saved to a backup file includes:

Bootstrap key (from X8.11)

System configuration settings

Clustering configuration

Local authentication data (but not Active Directory credentials for remotely managed accounts)

User account and password details

Server security certificate and private key

Call detail records (if the CDR service on Expressway is enabled)

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/Cisco-Expressway-Administrator-Guide-X8-11-4.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/admin_guide/Cisco-Expressway-Administrator-Guide-X8-11-4.pdf)  
upvoted 2 times

🗨️ 👤 **Collabinski** 1 year, 11 months ago

**Selected Answer: AE**

Tough question. I would probably choose A & E

upvoted 2 times

🗨️ 👤 **cyberknock** 1 year, 11 months ago

**Selected Answer: CE**

There are no call records, they are called Call Detail Records. C&E is the correct answer here.

upvoted 2 times

🗨️ 👤 **kc10boom** 3 years, 1 month ago

A and E.

upvoted 4 times



Which connection does the traversal zone configuration define?

- A. Expressway-E and Collaboration Endpoints
- B. Cisco UCS E-Series and Cisco UCM
- C. Cisco UC and Cisco Unified Presence Server
- D. Cisco Expressway-C and Cisco Expressway-E platforms

**Suggested Answer:** D

Reference:

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X8-11/Cisco-Expressway-Basic-Configuration-Deployment-Guide-X8-11-4.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X8-11/Cisco-Expressway-Basic-Configuration-Deployment-Guide-X8-11-4.pdf)



  **Duke\_CT** 7 months, 2 weeks ago

The traversal zone configuration defines the connection between:

D. Cisco Expressway-C and Cisco Expressway-E platforms.

Expressway-C and Expressway-E are components of the Cisco Expressway Series, used for secure communication for remote and external users to connect with the internal Unified Communications Manager (UCM) or other collaboration endpoints. The traversal zone configuration establishes a secure communication link between the Expressway-C and Expressway-E platforms, enabling external users to securely access internal communication resources.

upvoted 2 times

  **Duke\_CT** 7 months, 2 weeks ago

Which connection does the traversal zone configuration define?

- A. Expressway-E and Collaboration Endpoints
- B. Cisco UCS E-Series and Cisco UCM
- C. Cisco UC and Cisco Unified Presence Server
- D. Cisco Expressway-C and Cisco Expressway-E platforms

upvoted 1 times



Which protocol should be used to verify the connectivity for different media paths found during a call using ICE?

- A. STUN
- B. RTP
- C. SNMP
- D. TURN

**Suggested Answer: A**

Reference:

<https://www.cisco.com/c/en/us/td/docs/solutions/PA/ICE/icepa125.html>

  **Duke\_CT** 7 months, 2 weeks ago



ICE (Interactive Connectivity Establishment) is a technique used in communication protocols such as VoIP, video, and instant messaging to help establish connectivity between two parties. It's commonly used with protocols like SIP (Session Initiation Protocol) and WebRTC (Web Real-Time Communication).

To verify connectivity for different media paths found during a call using ICE, the protocol typically used is:

- A. STUN (Session Traversal Utilities for NAT)

STUN is used to discover the public IP address and port(s) assigned to a device by its NAT router. It helps in determining the network topology and the type of NAT being used, which is crucial for establishing peer-to-peer connections, especially in scenarios where one or both parties are behind NAT devices or firewalls.

upvoted 1 times

  **Duke\_CT** 7 months, 2 weeks ago

Which protocol should be used to verify the connectivity for different media paths found during a call using ICE?

- A. STUN
- B. RTP
- C. SNMP
- D. TURN

upvoted 1 times

Which SIP media encryption mode is applied by default for newly created zones in the Cisco Expressway?

- A. Off
- B. Best Effort
- C. Auto
- D. Force Encrypted

**Suggested Answer: C**

Community vote distribution

C (100%)

  **undertabler**  2 years, 10 months ago

**Selected Answer: C**

Answer C: Auto - no specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on the target system/endpoint requests. This is the default behavior and is equivalent to how the Expressway operated before this feature was introduced.  
upvoted 7 times

  **rob79**  3 years ago

This should be C "Auto"  
upvoted 5 times

  **ocero**  8 months, 3 weeks ago

Page 21.

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/Cisco-Expressway-Administrator-Guide-X8-10.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/admin_guide/Cisco-Expressway-Administrator-Guide-X8-10.pdf)

As the new media encryption mode is off by default, it is off for the CETls zones that are automatically created for MRA. These zones are not editable through the web interface. To use AES GCM media encryption with MRA.

Tricky question  
upvoted 1 times

  **Collabinski** 1 year, 11 months ago

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0-1/exwy\\_b\\_cisco-expressway-administrator-guide-x14-0-1/exwy\\_m\\_zones-and-neighbors.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0-1/exwy_b_cisco-expressway-administrator-guide-x14-0-1/exwy_m_zones-and-neighbors.html)  
upvoted 1 times

  **Collabinski** 1 year, 11 months ago

**Selected Answer: C**

The encryption mode options are:

- Force encrypted: All media to and from the zone/subzone must be encrypted. If the target system/endpoint is configured to not use encryption, then the call will be dropped.
  - Force unencrypted: All media must be unencrypted. If the target system/endpoint is configured to use encryption, then the call may be dropped; if it is configured to use Best effort then the call will fall back to unencrypted media.
  - Best effort: Use encryption if available, otherwise fall back to unencrypted media.
  - Auto: No specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on the target system/endpoint requests. This is the default behavior and is equivalent to how the Expressway operated before this feature was introduced.
- Encryption policy (any encryption setting other than Auto) is applied to a call by routing it through a back-to-back user agent (B2BUA) hosted on the Expressway.

upvoted 1 times

  **Collabinski** 1 year, 11 months ago

This has been verified on my local Expressway. Auto is the default  
upvoted 1 times

  **cyberknock** 2 years ago



**Selected Answer: C**

This is C for sure  
upvoted 1 times

  **preki10** 2 years ago

**Selected Answer: C**

Default: Auto  
upvoted 1 times

  **chacthor** 2 years, 10 months ago

Should be C  
upvoted 2 times



Cisco media traversal technology has enabled a secure environment where internal video endpoints call and receive calls from external video endpoints. How does the Expressway-C and Expressway-E communicate?

- A. Expressway-C establishes an outgoing request to Expressway-E, enabling the Expressway-E in the DMZ to notify the internal Expressway-C of an incoming call from an external endpoint.
- B. Internal endpoints are registered to Expressway-E in the DMZ. Expressway-C, which is also in the DMZ, will receive and make calls on behalf of Expressway- E because they are in the same network.
- C. Expressway-E establishes an outgoing request to Expressway-C, enabling the Expressway-C in the DMZ to notify the internal Expressway-E of an incoming call from an external endpoint.
- D. Internal endpoints are registered to Expressway-C in the DMZ. Expressway-E, which is also in the DMZ, will receive and make calls on behalf of Expressway- C because they are in the same network.

**Suggested Answer: A**

Reference:

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-5/exwy\\_b\\_mra-expressway-deployment-guide/exwy\\_b\\_mra-expressway-deployment-guide\\_chapter\\_00.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-5/exwy_b_mra-expressway-deployment-guide/exwy_b_mra-expressway-deployment-guide_chapter_00.html)

  **Duke\_CT** 7 months, 2 weeks ago

The correct answer is:

A. Expressway-C establishes an outgoing request to Expressway-E, enabling the Expressway-E in the DMZ to notify the internal Expressway-C of an incoming call from an external endpoint.

In a typical deployment scenario, Expressway-C, located within the corporate network, establishes an outgoing connection to Expressway-E, which is deployed in the DMZ. Expressway-E acts as the edge device and facilitates communication with external endpoints. When an external endpoint initiates a call, Expressway-E receives the call and notifies Expressway-C about the incoming call, allowing for secure communication between internal and external endpoints.

upvoted 2 times

Which dial plan component is configured in Expressway-C to route a call to the Cisco UCM?

- A. call routing
- B. traversal subzone
- C. call policy
- D. search rule

**Suggested Answer: D**

Community vote distribution

D (100%)

🗳️ 👤 **Collabinski** 11 months, 1 week ago

**Selected Answer: D**

D is correct

upvoted 1 times

🗳️ 👤 **Ol\_Mykhailiuk** 1 year, 1 month ago

**Selected Answer: D**

Search rules specify the range of telephone numbers / URIs to be handled by this neighbor Unified CM. They can also be used to transform URIs before they are sent to the neighbor

upvoted 2 times

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

**Selected Answer: D**

Answer is D. Reference: [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X8-1/Cisco-Expressway-SIP-Trunk-to-Unified-CM-Deployment-Guide-CUCM-8-9-and-X8-1.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X8-1/Cisco-Expressway-SIP-Trunk-to-Unified-CM-Deployment-Guide-CUCM-8-9-and-X8-1.pdf)

upvoted 2 times

🗳️ 👤 **msully** 1 year, 6 months ago

**Selected Answer: D**

Search rules

upvoted 1 times

🗳️ 👤 **chachor** 1 year, 10 months ago

Should be D

upvoted 2 times

🗳️ 👤 **tilo1988** 1 year, 11 months ago

Why administrator doesn't change it? It's D (search rule).

upvoted 4 times

🗳️ 👤 **chachor** 1 year, 10 months ago

He must be changing millions of answers from other exams

upvoted 1 times

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

Should Be "Search Rule"

upvoted 3 times

🗳️ 👤 **rob79** 2 years, 2 months ago

This should be D search rule.

upvoted 4 times

Which attribute in the SDP for a call is affected by the static NAT address configuration in an Expressway-E?

- A. connection
- B. name
- C. version
- D. bandwidth

**Suggested Answer: A**

Community vote distribution

A (100%)

  **rob79** Highly Voted 2 years ago

This should be A connection  
upvoted 9 times

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

**Selected Answer: A**

Tough question. You could almost be convinced it is B, but this doc mainly points to c= connection.



[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X8-5/Cisco-Expressway-Basic-Configuration-Deployment-Guide-X8-5-2.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X8-5/Cisco-Expressway-Basic-Configuration-Deployment-Guide-X8-5-2.pdf)

upvoted 1 times


  **cyberknock** 1 year ago

**Selected Answer: A**



the c= line - connection  
upvoted 2 times

  **chacthor** 1 year, 10 months ago



Should be A  
upvoted 1 times

  **tilo1988** 1 year, 11 months ago

the answer is A (connection), NOT B  
upvoted 4 times

  **tilo1988** 1 year, 11 months ago

c-line shows the connection information, Media IP address. So if it is natted it will be reflected there.  
upvoted 2 times

  **tilo1988** 1 year, 11 months ago

I think the answer is B. its attribute c-line=connection. There is no attribute "name"  
upvoted 3 times

Which describes what could be done on the Expressway-E to successfully route calls from Expressway-C on the internal network to the Internet?

- A. Application layer gateway could be enabled to bridge the media traffic.
- B. A static NAT route could be added to the firewall to bridge the two networks.
- C. The Expressway-E could be enabled for Dual-NIC capability.
- D. The Expressway-E could be enabled for interworking.

**Suggested Answer:** C

Community vote distribution

C (100%)

 **Collabinski** 11 months, 1 week ago

**Selected Answer: C**

Recommended: Dual NIC Static NAT Deployment The following example illustrates the recommended deployment. It shows the typical DMZ configuration where the internal and external firewalls cannot route directly to each other, and dual-NIC devices such as Expressway-E are required to validate and forward the traffic between the isolated subnets.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X14-0/basic\\_config/exwy\\_b\\_cisco-expressway-e-and-expressway-c-basic-configuration-deployment-guide-x14-0.pdf](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0/basic_config/exwy_b_cisco-expressway-e-and-expressway-c-basic-configuration-deployment-guide-x14-0.pdf)


upvoted 1 times

 **TestingAAgain** 1 year, 6 months ago

**Selected Answer: C**

C is the answer

upvoted 2 times

 **Mark03** 2 years, 10 months ago

C is correct, ask about Expressway and not firewall

upvoted 4 times

 **khader09** 3 years, 2 months ago

B. A static NAT route could be added to the firewall to bridge the two networks.

upvoted 1 times

 **somedudebob** 3 years, 1 month ago

But the question asks what could be done on the Expressway, B is a change to the firewall. I believe C is correct

upvoted 7 times

Edit transform

Configuration

Priority

1

i

Description

CCNPCollab

i

Pattern type

Regex

i

Pattern string

((^0-7))(\d{3,5})

i

Pattern behavior

Replace

i

Replace string

\1\2@ccnpcollab.com

i

State

Enabled

i

Save

Delete

Cancel

Refer to the exhibit. What is the result of a transformation applied to alias 88514?

- A. 98851@ccnpcollab.com
- B. 88513@ccnpcollab.com
- C. 88514@ccnpcollab.com
- D. 88515@ccnpcollab.com

**Suggested Answer: C**

Community vote distribution

C (100%)

**BangBang86** Highly Voted 3 years, 4 months ago

The answer should be 88514@ccnpcollab.com, since the regex considers anything after digit 8 (excludes 1-7), leaves the rest intact, and replaces the domain. So in short terms, it simply adds the domain after the DN.

upvoted 5 times

**chamba87** Highly Voted 2 years, 10 months ago

Answer is C i tested in the check pattern tool on a EXP-E

upvoted 5 times

**Collabinski** Most Recent 10 months, 3 weeks ago

Side note. All of the aliases in the answers are a match to this Transform, so if it's specified in the question any other answer it would be correct.

Verified on Expressway

upvoted 1 times

**Collabinski** 11 months, 1 week ago

**Selected Answer: C**

I tested this on my Expressway-C and the alias match was 88514.

upvoted 1 times

**msully** 1 year, 6 months ago

**Selected Answer: C**

[1-7] excludes 1-7 and replaces the domain with ccnpcollab.com. C is correct

upvoted 2 times



**chactor** 1 year, 10 months ago

Should be C

upvoted 2 times

**Simdude** 2 years, 12 months ago

88514@ccnpcollab.com is correct  
upvoted 1 times

  **khader09** 3 years, 2 months ago  
C. 88514@ccnpcollab.com  
upvoted 4 times

When configuring a Cisco Expressway solution and need to design the dial plan with various rules for URIs and numbers coming through the device. To do so, it is important that some dial plan rules are applied in a certain order. When configuring the transform section, you must know the range of the priorities.

Which range is correct?

- A. any number in the drop-down menu
- B. any number in the dialog box
- C. any number between 1-128
- D. any number between 1-65534

**Suggested Answer: D**

Community vote distribution

D (100%)

🗳️ 👤 **khader09** Highly Voted 🏆 3 years, 2 months ago

D. any number between 1-65534

upvoted 5 times

🗳️ 👤 **Collabinski** Most Recent ⌚ 11 months, 1 week ago

**Selected Answer: D**

Up to 100 pre-search transforms can be configured. Each transform must have a unique priority number between 1 and 65534.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0/exwy\\_b\\_cisco-expressway-administrator-guide/exwy\\_m\\_dial-plan-and-call-processing.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0/exwy_b_cisco-expressway-administrator-guide/exwy_m_dial-plan-and-call-processing.html)

upvoted 1 times

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

**Selected Answer: D**

D is the answer

upvoted 3 times

🗳️ 👤 **Mark03** 2 years, 10 months ago

Answer is D

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/Cisco-Expressway-Administrator-Guide-X8-6.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/admin_guide/Cisco-Expressway-Administrator-Guide-X8-6.pdf)

upvoted 4 times

Which zone is required on a B2B deployment between Expressway-C and Expressway-E?

- A. traversal zone
- B. DNS zone
- C. default zone
- D. neighbor zone

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗲️ 👤 **Collabinski** 11 months, 1 week ago

**Selected Answer: A**

A is correct

upvoted 1 times

🗲️ 👤 **TestingAAgain** 1 year, 6 months ago

**Selected Answer: A**

A Traversal Zone

upvoted 3 times

🗲️ 👤 **khader09** 3 years, 2 months ago

A. traversal zone

upvoted 4 times

Which mode should be used when Call Policy is configured on Expressways?

- A. extended CPL
- B. local CPL, policy service, and off
- C. on
- D. remote CPL

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **BangBang86** Highly Voted 3 years, 4 months ago

The possible modes are "local CPL, policy service, or off"  
upvoted 7 times

🗳️ 👤 **khader09** Highly Voted 3 years, 2 months ago

B. local CPL, policy service, and off  
upvoted 7 times

🗳️ 👤 **Collabinski** Most Recent 11 months, 1 week ago

**Selected Answer: B**

B is correct  
upvoted 1 times

🗳️ 👤 **Ol\_Mykhailiuk** 1 year, 1 month ago

**Selected Answer: B**

The Call Policy mode controls from where the Expressway obtains its Call Policy configuration. The options are:

- Local CPL: uses locally-defined Call Policy.
- Policy service: uses an external policy service.
- Off: Call Policy is not in use.

upvoted 3 times

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

**Selected Answer: B**

should be B  
upvoted 1 times

🗳️ 👤 **Omitted** 1 year, 6 months ago

**Selected Answer: B**

Haven't taken the test but this question needs to be rephrased if these are the options.  
upvoted 1 times

🗳️ 👤 **msully** 1 year, 6 months ago

**Selected Answer: B**

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/Cisco-Expressway-Administrator-Guide-X12-5-1.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/admin_guide/Cisco-Expressway-Administrator-Guide-X12-5-1.pdf)

Page 168

upvoted 1 times

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

Everyone on here is wrong.. Let's read the question again, words are important on a cisco exam. "Which mode should be used when Call Policy is configured on Expressways?" not which modes are available, but which one should be used when it's configured on the expressway. This means it's a local and per the guide that is "On" which is the answer they have here.

page 170

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/Cisco-Expressway-Administrator-Guide-X12-5-1.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/admin_guide/Cisco-Expressway-Administrator-Guide-X12-5-1.pdf)

upvoted 3 times

🗨️ 👤 **kljw5** 1 year, 7 months ago

Being that there are 3 answers on the admin guide that can be selected. "ON" is not one of them. Correct answer should be local CPL, policy service, and off.

upvoted 1 times

🗨️ 👤 **Omitted** 1 year, 6 months ago

The correct answer should be "local CPL" or "policy service" with the wording of the question. That isn't an option. I would not say "on" as that isn't a call policy mode.

upvoted 1 times

🗨️ 👤 **chacthor** 1 year, 10 months ago

**Selected Answer: B**

Should be B

upvoted 1 times

🗨️ 👤 **chacthor** 1 year, 10 months ago

Should be B

upvoted 1 times

🗨️ 👤 **tilo1988** 1 year, 11 months ago

@Administrator: please change the correct Answer to B! It's known for 1 Year and 5 months.

upvoted 2 times

🗨️ 👤 **chumleyex** 1 year, 9 months ago

But B is wrong and they have the answer correct. Would you have all 3 modes active to turn this feature on? No you wouldn't.

upvoted 1 times

🗨️ 👤 **Mark03** 2 years, 10 months ago

B is the correct answer. There is no such a thing as "mode ON" for Policy Services

upvoted 4 times

🗨️ 👤 **AKREM86** 2 years, 11 months ago

B is correct.

Reference:

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/Cisco-Expressway-Administrator-Guide-X12-5-1.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/admin_guide/Cisco-Expressway-Administrator-Guide-X12-5-1.pdf)

Page 168

upvoted 5 times

When designing the call control on a Cisco Expressway Core, which is the sequence of dial plan functions?

- A. transforms, CPL, user policy, search rules
- B. search rules, zones, local zones
- C. DNS zone, local zone, search rules
- D. search rules, transforms

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **khader09** Highly Voted 3 years, 2 months ago

A. transforms, CPL, user policy, search rules  
upvoted 5 times

🗳️ 👤 **Simdude** 2 years, 12 months ago

what is user policy ?  
upvoted 3 times

🗳️ 👤 **virtu** 2 years, 11 months ago

Find Me service  
upvoted 4 times

🗳️ 👤 **Collabinski** Most Recent 11 months, 1 week ago

Selected Answer: A

he pre-search transform function allows you to modify the alias in an incoming search request. The transformation is applied by the Expressway before any Call Policy (CPL) or User Policy is applied, and before any searches take place.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0/exwy\\_b\\_cisco-expressway-administrator-guide/exwy\\_m\\_dial-plan-and-call-processing.html#reference\\_18DBC558E34532EB78E9603EF988C3AB](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0/exwy_b_cisco-expressway-administrator-guide/exwy_m_dial-plan-and-call-processing.html#reference_18DBC558E34532EB78E9603EF988C3AB)

upvoted 2 times

🗳️ 👤 **chacthor** 1 year, 10 months ago

Should be A  
upvoted 1 times

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

Selected Answer: A

Proof in the comments below.  
upvoted 2 times

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

A is the Answer...  
<https://ccieme.wordpress.com/2016/11/07/14-4-cisco-vcs-dial-plan-components/>  
upvoted 3 times

🗳️ 👤 **chamba87** 2 years, 10 months ago

A is correct.  
<https://www.youtube.com/watch?v=XGV29NxHoVk>  
upvoted 2 times

🗳️ 👤 **Abhishek1610** 3 years ago

Correct answer is A  
upvoted 2 times

🗳️ 👤 **BangBang86** 3 years, 4 months ago

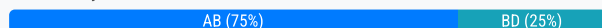
The right order is transforms, then CPL, and lastly Search Rules.  
upvoted 2 times

Which two items are configured when deploying a B2B collaboration solution? (Choose two.)

- A. SIP trunk between Cisco Unified Communications Manager and Cisco Expressway-C
- B. search rules in Cisco Expressway-E
- C. SIP trunk between Cisco Unified Communications Manager and Cisco Expressway-E
- D. traversal client on a Cisco Expressway-E
- E. DNS zone on a Cisco Expressway-C

**Suggested Answer: AB**

Community vote distribution



**leigh1141** Highly Voted 3 years, 10 months ago

A and B  
upvoted 8 times

**khader09** Highly Voted 4 years, 2 months ago

A & B are correct  
upvoted 5 times

**sgtalex77** Most Recent 6 months, 4 weeks ago

A & B

<https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/213864-configure-business-to-business-audio-and.html>

upvoted 1 times

**Collabinski** 1 year, 11 months ago

<https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/213864-configure-business-to-business-audio-and.html#anc14>

upvoted 1 times

**Collabinski** 1 year, 11 months ago

**Selected Answer: AB**

Step 1. SIP trunk between CUCM and Expressway-C

After CUCM discovery is done by Expressway-C, Neighboring zone(s) are automatically configured for each node, and the transport protocol is discovered.

When the CUCM cluster is configured in mixed mode there is one zone for Transmission Control Protocol (TCP) for non-secure traffic with destination port 5060 and 1 zone for TLS (Transport Layer Security ) for secure traffic with destination port 5061. These ports can not be changed.

The two zones are used for all edge calls to and from the edge endpoints.

Inbound calls from the edge endpoints take the route of these auto-added zones and hence target TCP 5060 or TLS 5061 on CUCM.

Step 4. Configure dialplan

a.Transform and/or Search Rules on Expressway-C and E

From Expressway Administration page, navigate to Configuration > Dial Plan > Transforms y Configuration > Dial Plan > Transform or Search Rules

upvoted 3 times

**Babas09** 2 years, 5 months ago

Transversal Client is only expressway C.

The good answers are AB

upvoted 2 times

**TestingAAgain** 2 years, 6 months ago

**Selected Answer: BD**

But what if there is no CUCM in the mix? You might have endpoints directly registered to the C, or to a TMS. You'd definately need search rules (B), but a B2B also requires a traversal zone, which means you'd need a traversal client on the E (answer D). And you'd have to have this even if you were using a CUCM (or not). So I think the answers here are B and D

upvoted 1 times

**RosadeColores** 2 years, 2 months ago

On Expressway-E you would need in that case a traversal server, not a client.  
upvoted 4 times

Which step is taken when configuring a Cisco Expressway solution?

- A. Configure the Expressway-E by using a non-traversal server zone.
- B. Enable static NAT on the Expressway-E only.
- C. Disable H.323 mode on the Expressway-E.
- D. Enable H.323 H.460.19 demultiplexing mode on the Expressway-C.

**Suggested Answer: B**

*Community vote distribution*

B (100%)

  **Collabinski** 11 months, 1 week ago

**Selected Answer: B**

The Expressway-E has both NICs enabled, and static NAT enabled on its outward-facing LAN interface. The Expressway-C inside the network is a traversal client of the Expressway-E in the DMZ.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X14-0/basic\\_config/exwy\\_b\\_cisco-expressway-e-and-expressway-c-basic-configuration-deployment-guide-x14-0/exwy\\_m\\_advanced-networking-deployments.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0/basic_config/exwy_b_cisco-expressway-e-and-expressway-c-basic-configuration-deployment-guide-x14-0/exwy_m_advanced-networking-deployments.html)

upvoted 2 times

  **leigh1141** 2 years, 10 months ago

B - Expressway E is to be natted only

upvoted 2 times

Configuration	
Rule name	* CCNP-Collab <i>i</i>
Description	CCNP-Collab <i>i</i>
Priority	* 1 <i>i</i>
Protocol	SIP <i>i</i>
Source	Local Zone <i>i</i>
Request must be authenticated	No <i>i</i>
Mode	Alias pattern match <i>i</i>
Pattern type	Regex <i>i</i>
Pattern string	* 1?3+5 <i>i</i>
Pattern behavior	Replace <i>i</i>
Replace string	135 <i>i</i>
On successful match	Stop <i>i</i>
Target	* Traversal Zone <i>i</i>
State	Enabled <i>i</i>

Refer to the exhibit. When configuring a search rule that routes calls to a zone, what occurs when 13358 is dialed?

- A. 13358 is replaced by 135, and then is sent to the local zone.
- B. 13358 is replaced by 135 and remains in the same zone.
- C. 13358 is replaced by 135, and then is sent to the traversal zone.
- D. 13358 is sent directly to the traversal zone.

**Suggested Answer: C**

Community vote distribution

D (100%)

**Collabinski** 11 months, 1 week ago

**Selected Answer: D**

Babasa09 is correct. I tested it on my Expressway and the match failed, so it would send it to the Traversal Zone. If you make the alias 1335 then there will be a successful match.

upvoted 1 times

**Babas09** 1 year, 5 months ago

Answer D

For the response to be C, regex should be 1?3+58

upvoted 3 times

**TestingAAgain** 1 year, 6 months ago

None of the answers are correct. I dropped this all into the expression tester on an expressway in my lap, and it says that the pattern doesn't match. So, it would not be sent to the target zone, because it didn't match the pattern. The expressway would then continue to process the next search rule.

upvoted 2 times

**kljw5** 1 year, 7 months ago

So am i to understand C is the correct answer then? as it will match 1335 then stop and replace the string with 135?? or is D correct as the 13358 as a whole string doesn't match?????

upvoted 1 times

🗨️ 👤 **undertabler** 1 year, 10 months ago

There is no match 13358 so this search rule will not be applied. I believe there is a typo.  
upvoted 2 times

🗨️ 👤 **tilo1988** 1 year, 11 months ago

Based on LINK for Regex: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2018/pdf/BRKCOL-2018.pdf>

\* 0 or more repetitions of previous character or expression

+ 1 or more repetitions of previous character or expression

? 0 or 1 repetitions of previous character or expression

Based on Website (<https://www.regextester.com/10544>) there are a few options which meets this Regex:

135, 1335, 13335, 1333335

1135, 11335, 113335, 11333335

no match for 13358: D is correct

upvoted 2 times

🗨️ 👤 **Krachowsky** 9 months ago

I think these are valid matches:

35,335,33335,33335 etc.

135,1335,13335,133335 etc.

Because there is no way to get more then one 1 at the beginning. "?" says that the character before the "?" must be there 0 or 1 times.

upvoted 1 times

🗨️ 👤 **ddrogi** 3 years, 1 month ago

This is all wrong it should be 1358 and send to traversal zone

upvoted 1 times

🗨️ 👤 **virtu** 2 years, 11 months ago

Hi, why you are saying that it should be 1358? picture has a replace behavior without any append or something like that

upvoted 2 times

🗨️ 👤 **Bazant** 1 year, 12 months ago

Because 13358 will not be matched by shown regex. 1335 will be matched.

upvoted 1 times

🗨️ 👤 **virtu** 2 years, 10 months ago

Yep, i check pattern, and it will work if matching alias will be 1335 without 8 in the end of string

upvoted 1 times

**Create transform** You are here: [Configuration](#) > [Dial plan](#) > [Transform](#) > **Create transform**

**Configuration**

Priority	<input type="text" value="5"/>	
Description	<input type="text" value="Convert Untitled CM supplied domain information to the Expressway SIP domain"/>	
Pattern type	<input type="text" value="Regex"/>	
Pattern string	<input type="text" value="(4\d{3})@exp-name.exp.domain *)?"/>	
Pattern behavior	<input type="text" value="Replace"/>	
Replace string	<input type="text" value="\1@exp.domain"/>	
State	<input type="text" value="Enabled"/>	

Refer to the exhibit. Which description of the transformation is true?

- A. It converts 4123@exp-name.exp.domain:<port> to 4123@exp.domain
- B. It changes all patterns that begin with 4123@exp-name.exp.domain:<port> to 1@exp.domain
- C. It changes 413@exp-name.exp.domain:<port> to 413@exp.domain
- D. It converts 4.3@exp-name.exp.domain:<port> to 1@exp.domain

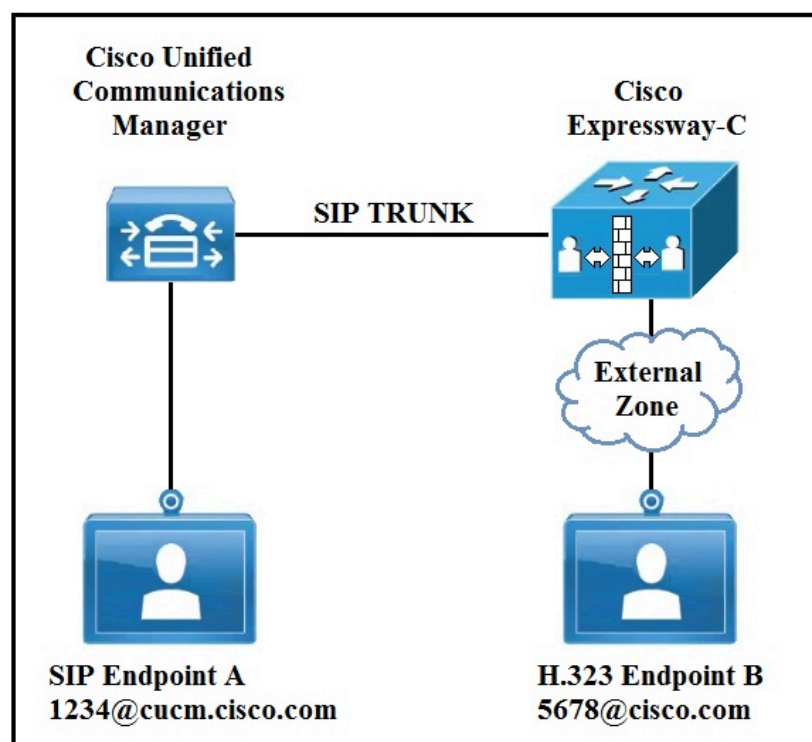
**Suggested Answer:** A

**khader09** Highly Voted 8 months, 2 weeks ago

A is correct, but the pattern string should be:

`(4\d{3})@exp-name.exp.domain(:.*)?`

upvoted 6 times



Refer to the exhibit. In an environment SIP devices are registered to CUCM and H.323 devices to VCS.

What would be required to enable these calls to setup correctly?

- A. Create a presearch transform.
- B. Change the domain of SIP endpoint A to cisco.com.
- C. Disable SIP in the external zone.
- D. Change the interworking mode to On.

**Suggested Answer: D**

Community vote distribution

D (100%)

**Collabinski** 11 months, 1 week ago

**Selected Answer: D**

D is correct

upvoted 2 times

Which step is required when configuring cloud and hybrid deployments for Cisco Jabber?

- A. Add the Jabber user to Cisco Unity Connection.
- B. Add the Jabber user to Expressway-E.
- C. Add the Jabber user to Expressway-C.
- D. Add Jabber Users to the Cisco Webex Administration Tool.

**Suggested Answer:** D

*Community vote distribution*

D (100%)

 **Collabinski** 11 months, 1 week ago

**Selected Answer: D**

D seems correct.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/jabber/12\\_6/cjab\\_b\\_cloud-and-hybrid-deployments-cisco-jabber-12-6/cjab\\_b\\_cloud-and-hybrid-deployments-cisco-jabber-12-6\\_chapter\\_0101.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/12_6/cjab_b_cloud-and-hybrid-deployments-cisco-jabber-12-6/cjab_b_cloud-and-hybrid-deployments-cisco-jabber-12-6_chapter_0101.html)

upvoted 1 times

Which two licenses are required for the B2B feature to work? (Choose two.)

- A. Traversal Server
- B. TURN Relays
- C. Rich Media Sessions
- D. Advanced Networking
- E. Device Provisioning

**Suggested Answer:** AC

Community vote distribution

AC (100%)


  **BangBang86** Highly Voted 3 years, 10 months ago

Traversal server and RMS. Any other is not needed. (Unless the calls needs Interworking, but that is not the case in this question).  
upvoted 13 times

  **Panda\_man** Most Recent 8 months, 2 weeks ago

Selected Answer: AC

A,C correct  
upvoted 1 times

  **Collabinski** 1 year, 5 months ago



Selected Answer: AC

- Rich Media Sessions: Determines the number of non-Unified Communications calls allowed on the Expressway (or Expressway cluster) at any one time. See the Call Types and Licensing section for more information.



- Traversal Server: Enables the Expressway to work as a firewall traversal server.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0/exwy\\_b\\_cisco-expressway-administrator-guide/exwy\\_m\\_managing-licensing.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0/exwy_b_cisco-expressway-administrator-guide/exwy_m_managing-licensing.html)

upvoted 2 times

  **iulianm** 1 year, 11 months ago

Room system and desktop system registration licenses: These licenses are required for all devices that register to Cisco Expressway-C. Devices that consume a registration license will not consume a Rich Media license when they are in a call with any other Cisco registered device, Cisco Infrastructure product (for example, Cisco Meeting Server), or calls in the Cisco Collaboration Cloud.  
upvoted 1 times

  **iulianm** 1 year, 11 months ago



Answer are BC  
upvoted 1 times

  **tilo1988** 2 years, 5 months ago

BangBang86 wrote correct Answer 1 year ago and have 7 votes. Why administrator doesnt change the corrcet Answer to A and C?  
upvoted 4 times

  **rob79** 2 years, 8 months ago

Shouldn't E be device registration?  
upvoted 1 times

  **Bazant** 2 years, 5 months ago

In the answer you have "Device Provisioning" not "Device Registration", so no this in NOT correct answer. The question asks what you need for B2B. No matter where the device is registered you need Traversal Server and RMS  
upvoted 1 times

An Expressway-E is configured using a single NIC with NAT.

How must the Expressway-C traversal client zone be configured to connect to the Expressway-E?

- A. TLS verify must be enabled.
- B. The zone profile must be set to default.
- C. The peer address must be the Expressway-E NAT address.
- D. The peer address must be the Expressway-E LAN 1 IP address.

**Suggested Answer: C**

*Community vote distribution*

C (100%)

  **Collabinski** 11 months, 1 week ago

**Selected Answer: C**

You must enter the FQDN of the Expressway-E, as it is seen from outside the network, as the peer address on the Expressway-C's secure traversal zone.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X14-0/basic\\_config/exwy\\_b\\_cisco-expressway-e-and-expressway-c-basic-configuration-deployment-guide-x14-0/exwy\\_m\\_advanced-networking-deployments.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0/basic_config/exwy_b_cisco-expressway-e-and-expressway-c-basic-configuration-deployment-guide-x14-0/exwy_m_advanced-networking-deployments.html)

upvoted 3 times

  **khader09** 3 years, 2 months ago

C is correct

upvoted 3 times


	Expressway-E
<b>Rule name</b>	Enter Block ISDN call for example
<b>Description</b>	Enter Block everything (including nonregistered endpoints)
<b>Priority</b>	Enter 41
<b>Protocol</b>	<i>Any</i>
<b>Source</b>	
<b>Request must be authenticated</b>	<i>No</i>
<b>Mode</b>	<i>Alias pattern match</i>
<b>Pattern type</b>	<i>Regex</i>
<b>Pattern string</b>	Enter (9\d+) (.*) (@example.com)
<b>Pattern behavior</b>	<i>Replace</i>
<b>Replace string</b>	Enter do-not-route-this-call for example
<b>On successful match</b>	<i>Stop</i>
<b>Target</b>	<i>TraversalZone</i>
<b>State</b>	<i>Enabled</i>

Refer to the exhibit. An ISDN gateway is registered to Expressway-C with a prefix of 9 and/or it has a neighbor zone specified that routes calls starting with a 9.


Which value should be entered into the "Source" field to prevent toll fraud regardless at origin of the call?

- A. Traversal Zone
- B. Any
- C. Neighbor Zone
- D. All

**Suggested Answer: D**

 **BangBang86** Highly Voted 3 years, 10 months ago

There is no such parameter "All". It must be set to "Any".  
upvoted 10 times

 **daniepad** Most Recent 1 week, 2 days ago

**Selected Answer: B**  
For me, any is more accurate as it also covers non-registered devices  
upvoted 1 times

 **Collabinski** 1 year, 5 months ago

Tough question. If the exam specifies "All Zones" then that is the answer.

• To minimize toll fraud risks, avoid using the "Any" wild card for the Source setting.

To provide extra security you can set the rule's Source option to All zones. This means that the query is only sent to the target zone if it originated from any configured zone or the Local Zone.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0/exwy\\_b\\_cisco-expressway-administrator-guide/exwy\\_m\\_dial-plan-and-call-processing.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0/exwy_b_cisco-expressway-administrator-guide/exwy_m_dial-plan-and-call-processing.html)  
upvoted 4 times

 **TestingAAgain** 2 years ago

From the expressway help file below. The difference between the two is that any also blocks unregistered devices. I go with ANY as the answer  
The sources of the requests for which this rule applies.

Any: locally registered devices, neighbor or traversal zones, and any non-registered devices.

All zones: locally registered devices plus neighbor or traversal zones.

upvoted 2 times

  **jonycakes** 2 years, 6 months ago

Answer B: The dropdown options for the Source field are -

\*Any

\*All zones

\*Local Zone

\*Named



Source: [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X8-8/Cisco-Expressway-Basic-Configuration-Deployment-Guide-X8-8.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X8-8/Cisco-Expressway-Basic-Configuration-Deployment-Guide-X8-8.pdf)

upvoted 4 times

  **chamba87** 3 years, 3 months ago

or maybe the answer make reference to any of the all 3 options above O\_o ?

upvoted 1 times

  **Bazant** 2 years, 5 months ago

No as possible choices at Expressway are:

Any: locally registered devices, neighbor or traversal zones, and any non-registered devices.

All zones: locally registered devices plus neighbor or traversal zones.

Local Zone: locally registered devices only.

Named: a specific zone or subzone.

No "Neighbor Zone" or "Traversal Zone" available, so the any possible correct answer is B "Any"

upvoted 1 times

  **aocstr** 11 months ago

this would not prevent toll fraud though, tricky question

upvoted 1 times

Expressway-C Traversal Zone:  
SIP: Failed to connect to 192.168.1.6:7001

Expressway-C Event Log shows the following:

2019-10-23T11:01:51.925-04:00 : Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="192.168.1.5" Src-port="27204" Dst-ip="192.168.1.6" Dst-port="7003" Detail="tlsv1 alert unknown ca" Protocol="TLS" Common-name="amer-expressway01.example.com" Level="1" UTCtime="2019-10-23 15:01:51.923"

Expressway-C server certificate shows the following decoded output:

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: sha256WithRSAEncryption


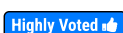
Issuer: O=Temporary CA fce4028e-92ba-4cbc-9e71-08b959888af4, OU=Temporary CA fce4028e-92ba-4cbc-9e71-08b959888af4, CN=Temporary CA fce4028e-92ba-4cbc-9e71-08b959888af4

Refer to the exhibit. An Expressway-C and Expressway-E are configured for B2B calling and the Expressway-E zone is set to TLS Verify. Currently, calls do not reach the Expressway-C. The Traversal Client zone on the Expressway-C for B2B reports the information in the exhibit for the Peer 1 address.

Which action resolves this error?

- A. Configure the Expressway-C Traversal Client zone Peer 1 address with the fully qualified domain name of the Expressway-E.
- B. Configure the Expressway-C Traversal Client zone transport protocol with TCP.
- C. Add a server certificate to the Expressway-C that is signed by a certificate authority.
- D. Add an intermediate certificate to the Expressway-C that is signed by a certificate authority.

**Suggested Answer: D**

 **chamba87**  2 years, 9 months ago

Yep i feel the same, the answer is C  
upvoted 5 times

 **iamnoone**  3 months, 2 weeks ago

**Selected Answer: D**  
Correct answer should be D.

There's no such a thing like a "temporary CA". An Issuer (CA) is an Issuer. It signs certificates. This is just the common name of the CA used to sign the certificate. It can be whatever.

In this case TLS fails as stated in the Event Log Detail because of "tlsv1 alert unknown ca". This means that the certificate presented for the TLS negotiation is not trusted by the Exp-C, because of the lack of an intermediate or root certificate that signed the specific certificate. (public or private)

So, either an intermediate is missing, or the root certificate of the CA in the trust store is not there.  
upvoted 1 times

 **Collabinski** 11 months, 1 week ago

If TLS verify mode is enabled, the neighbor system's FQDN or IP address, as specified in the Peer address field of the zone's configuration, is used to verify against the certificate holder's name in the X.509 certificate presented by that system. (The name must be in the SAN attribute of the certificate.) The certificate itself must also be valid and signed by a trusted certificate authority.  
So when certificates have been generated with peer or cluster FQDNs, ensure that the zone's Peer address fields are configured with FQDNs rather than IP addresses.

-[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X14-0-2/cert\\_creation\\_use/exwy\\_b\\_certificate-creation-and-use-deployment-guide-x1402/exwy\\_b\\_certificate-creation-use-deployment-guide\\_chapter\\_01000.html#concept\\_BFDB31BC4989A5EB232AF2A85AD1727E](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0-2/cert_creation_use/exwy_b_certificate-creation-and-use-deployment-guide-x1402/exwy_b_certificate-creation-use-deployment-guide_chapter_01000.html#concept_BFDB31BC4989A5EB232AF2A85AD1727E)  
upvoted 1 times

🗨️ 👤 **Collabinski** 11 months, 1 week ago

Tough question. Could be A or D.

Managing the Trusted CA Certificate List The Trusted CA certificate page (Maintenance > Security certificates > Trusted CA certificate) allows you to manage the list of certificates for the Certificate Authorities (CAs) trusted by this Expressway. When a TLS connection to Expressway mandates certificate verification, the certificate presented to the Expressway must be signed by a trusted CA in this list and there must be a full chain of trust (intermediate CAs) to the root CA.

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X8-9/Cisco-Expressway-Certificate-Creation-and-Use-Deployment-Guide-X8-9.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X8-9/Cisco-Expressway-Certificate-Creation-and-Use-Deployment-Guide-X8-9.pdf)

upvoted 1 times

🗨️ 👤 **Collabinski** 11 months, 2 weeks ago

SIP TLS Negotiation Failures on Neighbor and Traversal Zones

If TLS verify mode is enabled, the neighbor system's FQDN or IP address, as specified in the Peer address field of the zone's configuration, is used to verify against the certificate holder's name in the X.509 certificate presented by that system. (The name must be in the SAN attribute of the certificate.) The certificate itself must also be valid and signed by a trusted certificate authority.

So when certificates have been generated with peer or cluster FQDNs, ensure that the zone's Peer address fields are configured with FQDNs rather than IP addresses.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X14-0-2/cert\\_creation\\_use/exwy\\_b\\_certificate-creation-and-use-deployment-guide-x1402/exwy\\_b\\_certificate-creation-use-deployment-guide\\_chapter\\_01000.html#concept\\_BFDB31BC4989A5EB232AF2A85AD1727E](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0-2/cert_creation_use/exwy_b_certificate-creation-and-use-deployment-guide-x1402/exwy_b_certificate-creation-use-deployment-guide_chapter_01000.html#concept_BFDB31BC4989A5EB232AF2A85AD1727E)

upvoted 1 times

🗨️ 👤 **jonycakes** 2 years ago

Answer D: When a TLS connection to Expressway mandates certificate verification, the certificate presented to the Expressway must be signed by a trusted CA in this list and there must be a full chain of trust (intermediate CAs) to the root CA.

Source [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X8-9/Cisco-Expressway-Certificate-Creation-and-Use-Deployment-Guide-X8-9.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X8-9/Cisco-Expressway-Certificate-Creation-and-Use-Deployment-Guide-X8-9.pdf)

upvoted 2 times

🗨️ 👤 **Omitted** 1 year, 6 months ago

You can upload the server certificate with the full chain on it. The issue here seems to be the temporary cert. I think it is C

upvoted 2 times

🗨️ 👤 **khader09** 3 years, 2 months ago

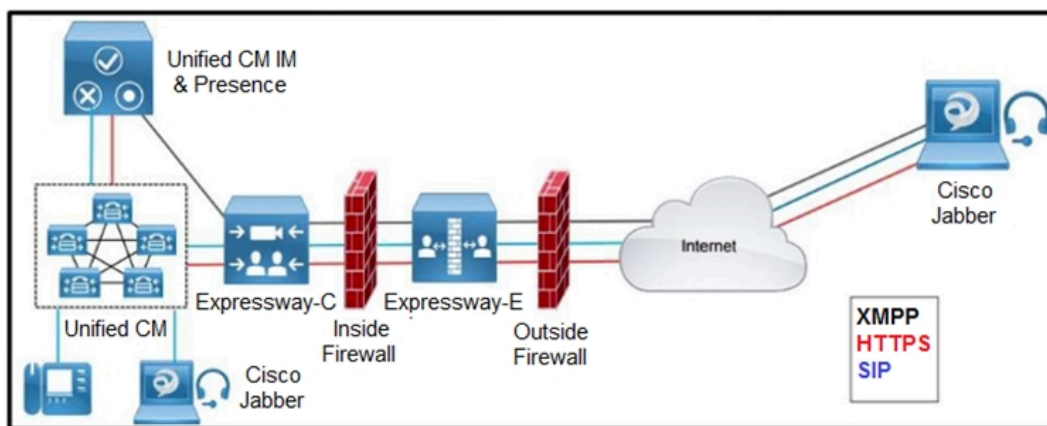
I feel answer is C

upvoted 2 times

🗨️ 👤 **BangBang86** 3 years, 4 months ago

The ExpC is using a temporary CA, and it needs a certificate signed by a CA (either private or public).

upvoted 4 times



Refer to the exhibit. Which inbound connection should an administrator configure on the outside firewall?

- A. Media: UDP 36000 to 36011
- B. XMPP: TCP 5222
- C. SIP: TCP 5061
- D. HTTPS (tunneled over SSH between C and E): TCP 2222

**Suggested Answer: C**

Reference:

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-5/Cisco-Expressway-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X12-5.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-5/Cisco-Expressway-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X12-5.pdf)

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

Both B and C are correct. Probably a multichoice question...

The external firewall must allow the following inbound connections to the Expressway-E:

SIP: TCP 5061

HTTPS: TCP 8443

XMPP: TCP 5222

Media: UDP 36002 to 59999

Source: Official Cert Guide

upvoted 9 times

**Krachowsky** 1 year, 3 months ago

That is wrong.

The SIP:TCP 5061 is not valid.

Only between Expressway-C and On-premises Infrastructure you need to open a SIP TCP Port. And the TCP Port is 5060, not 5061. Port 5061 is used for TLS.

Connections Between Off-premises Endpoints and the Expressway-E only needs to be opened for SIP:TLS 5061, not for SIP:TCP 5060.

Have a look at the reference tilo1988 mentioned in his comment.

So only B is correct.

upvoted 3 times

**JamieF66** Highly Voted 2 years, 8 months ago

Answer B.

SIP TLS 5061 and XMPP TCP 5222

upvoted 6 times

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

**Selected Answer: B**

This an MRA scenario (screenshot), this should be a multiple answer question. In which case B, C and D are all correct.

B) XMPP (IM and Presence)

C) SIP signaling

D) UDS (phonebook and provisioning)

These should be opened ports according to the Cisco documentation, in order to for connections between Off-premises Endpoints and the Expressway-E (Table 2):

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X15-0/ip-port/exwy\\_b\\_cisco-expressway-ip-port-usage-configuration-guide-x15/exwy\\_m\\_mobile-and-remote-access.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-0/ip-port/exwy_b_cisco-expressway-ip-port-usage-configuration-guide-x15/exwy_m_mobile-and-remote-access.html)

A. Media UDP 36000-36011 seems too short of a range for RTP flows. In the documentation it states 36000-59999 UDP.

upvoted 1 times


 **iamnoone** 3 months, 1 week ago

Pfff my bad, HTTPS is 443 or 8443 in this case.

Again B & C look possible answers, but since it's not a multiple answer question, only B anyways.

TLS is used for SIP. But on the firewall you would open TCP 5061 anyway. TLS run on top of that using certificates.

upvoted 1 times

 **jagifoto** 1 year, 4 months ago

B. XMPP: TCP 5222 this is the answer XMPP (IM and Presence)

Offpremises

endpoint

1024-65535 TCP ExpresswayE Public IP

5222

upvoted 2 times

 **TestingAAgain** 2 years ago

I agree the answers should be B & C. While tilo1988 points out that the protocol running on port 5061 is actually TLS, the question is what do you have to open on the FIREWALL. The access list requires you to open TCP port 5061, TCP Port 5022, TCP port 8433, and UDP36000 - 59999. TLS is actually a secure layer that runs on TOP of TCP/IP.

upvoted 3 times

 **aocstr** 11 months, 2 weeks ago

Technically TLS runs over TCP and option B is related to TCP, not TLS. I would choose XMPP, is a "closer" answer I'd say.

upvoted 1 times

 **kljw5** 2 years, 1 month ago

This answer almost got me. SIP is almost right but offnet SIP incoming should be SIP TLS not TCP so that's incorrect. Only valid answer provided is XMPP TCP 5222

upvoted 3 times

 **tilo1988** 2 years, 5 months ago

Based on following LINK and page 18(SIP Calls) + 29 (MRA Connections):

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-5/Cisco-Expressway-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X12-5.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-5/Cisco-Expressway-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X12-5.pdf)

SIP UDP: 5060

SIP TCP: 5060

SIP TLS: 5061

XMPP TCP: 5222

RTP/RTCP: 36000-59999

There could be ONLY one correct answer B (XMPP: TCP 5222)

upvoted 5 times

How does an administrator configure an Expressway to make sure an external caller cannot reach a specific internal address?

- A. block the call with a call policy rule in the Expressway-E
- B. add the specific URI in the firewall section of the Expressway and block it
- C. configure FAC for the destination alias on the Expressway
- D. add a search rule route all calls to the Cisco UCM

**Suggested Answer: C**


Reference:

[https://www.google.com/url?](https://www.google.com/url?sa=t&rc=t&q=&esrc=s&source=web&cd=&ved=2ahUKEwiW2dKTxpfvAhX87nMBHQw5CBoQFjABegQIAxAD&url=https%3A%2F%2Fcommunity.cisco.com%2Fkxiwq67737%2Fattachments%2Fkxiwq67737%2F4576-docs-colaboracao-voz-e-video%2F141%2F2%2Fipcor-fac.pdf&usg=AOvVaw32Q70oP4UYkubwFJlImAQ9)

[sa=t&rc=t&q=&esrc=s&source=web&cd=&ved=2ahUKEwiW2dKTxpfvAhX87nMBHQw5CBoQFjABegQIAxAD&url=https%3A%2F%2Fcommunity.cisco.com%2Fkxiwq67737%2Fattachments%2Fkxiwq67737%2F4576-docs-colaboracao-voz-e-video%2F141%2F2%2Fipcor-fac.pdf&usg=AOvVaw32Q70oP4UYkubwFJlImAQ9](https://www.google.com/url?sa=t&rc=t&q=&esrc=s&source=web&cd=&ved=2ahUKEwiW2dKTxpfvAhX87nMBHQw5CBoQFjABegQIAxAD&url=https%3A%2F%2Fcommunity.cisco.com%2Fkxiwq67737%2Fattachments%2Fkxiwq67737%2F4576-docs-colaboracao-voz-e-video%2F141%2F2%2Fipcor-fac.pdf&usg=AOvVaw32Q70oP4UYkubwFJlImAQ9)

Community vote distribution

A (100%)

 **TheBabu** 11 months, 3 weeks ago

**Selected Answer: A**

A is correct.

upvoted 1 times

 **Collabinski** 2 years, 5 months ago

From everything I've searched, FAC is a feature specific to CUCM, not expressway. Call Policy is the Expressway feature to control which calls are allowed, which calls are rejected, and which calls are to be redirected to a different destination.

<https://community.cisco.com/t5/unified-communications-infrastructure/block-unwanted-calls-on-cisco-expressway/td-p/4320919>

<https://community.cisco.com/t5/unified-communications-infrastructure/block-unwanted-calls-on-cisco-expressway/td-p/4320919>

upvoted 2 times

 **hake** 2 years, 6 months ago

This is the correct link to the Reference Document: <https://community.cisco.com/kxiwq67737/attachments/kxiwq67737/4576-docs-colaboracao-voz-e-video/141/2/lpcor-fac.pdf>


But I don't understand, why the correct answer should be C. For external calls the right answer should be A.

upvoted 1 times

 **TestingAAgain** 3 years ago

Should be A, and the link provided as a reference doesn't even work.

upvoted 2 times

 **tilo1988** 3 years, 5 months ago


Yes it is A, but why Administrator doesn't change it?

upvoted 1 times

 **veraiden** 3 years, 7 months ago

Should be A

upvoted 3 times

 **JamieF66** 3 years, 8 months ago

Answer A

upvoted 3 times

An engineer wants to configure a zone on the Expressway-E to receive communications from the Expressway-C in order to allow inbound and outbound calls.

How is the peer address configured on the Expressway-C when Expressway-E has only one NIC enabled and is using static NAT mode?

- A. Expressway-E DHCP
- B. Cisco UCM FQDN
- C. Cisco UCM DHCP
- D. Expressway-E FQDN


**Suggested Answer: D**

Reference:

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X8-11/Cisco-Expressway-Basic-Configuration-Deployment-Guide-X8-11-4.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X8-11/Cisco-Expressway-Basic-Configuration-Deployment-Guide-X8-11-4.pdf)

*Community vote distribution*

D (100%)

 **Panda\_man** 8 months, 2 weeks ago

**Selected Answer: D**

D is correct

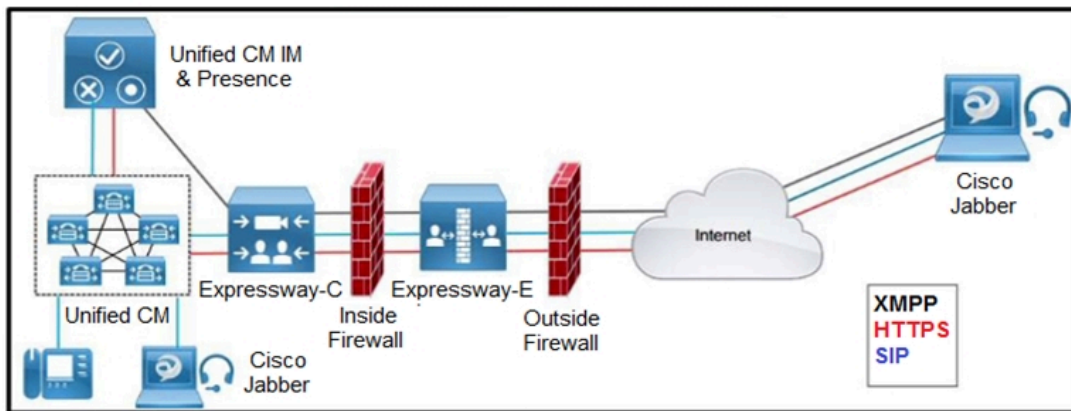
upvoted 1 times

 **Collabinski** 1 year, 5 months ago

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X8-11/Cisco-Expressway-Basic-Configuration-Deployment-Guide-X8-11-4.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X8-11/Cisco-Expressway-Basic-Configuration-Deployment-Guide-X8-11-4.pdf)

"You must enter the FQDN of the Expressway-E, as it is seen from outside the network, as the peer address on the Expressway-C's secure traversal zone. The reason for this is that in static NAT mode, the Expressway-E requests that incoming signaling and media traffic should be sent to its external FQDN, rather than its private name."

upvoted 2 times



Refer to the exhibit. Which two outbound connections should an administrator configure on the internal firewall? (Choose two.)

- A. XMPP: TCP 7400
- B. SIP: TCP 7001
- C. SIP TCP 5061
- D. Media: UDP 36012 to 59999
- E. HTTPS: TCP 8443

**Suggested Answer: AB**

Community vote distribution

AB (100%)

**undertabler** Highly Voted 1 year, 4 months ago

**Selected Answer: AB**

The internal firewall must allow the following outbound connections from the Expressway-C to the Expressway-E:

SIP: TCP 7001

Traversal media: UDP 2776 to 2777 (or 36000 to 36011 for large VM/appliance)

XMPP: TCP 7400

HTTPS (tunneled over SSH between C and E): TCP 2222

Source: Official Cert Guide

upvoted 5 times

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

**Selected Answer: AB**

Table 3. Connections Between Expressway-C and Expressway-E

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X15-0/ip-port/exwy\\_b\\_cisco-expressway-ip-port-usage-configuration-guide-x15/exwy\\_m\\_mobile-and-remote-access.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-0/ip-port/exwy_b_cisco-expressway-ip-port-usage-configuration-guide-x15/exwy_m_mobile-and-remote-access.html)

upvoted 1 times

**kljw5** 1 year, 1 month ago

I think this is a typo in the answers Correct answers should be SIP TLS 7001 and XMPP TCP 7400 HTTPS is not valid through internal firewall as most traffic is TLS not TCP so that rules out all the answers. This is a core question in which signaling protocol is allowed from C to E.

upvoted 2 times

**TestingAAgain** 1 year ago

Not a typo. The question is what do you configure on the FIREWALL. TLS is a secure layer that runs on top of TCP/IP. You have to open TCP ports on the firewall for TLS to flow through. If you look at table 16 on page 31 of the Cisco Expressway IP Port Usage for Firewall Traversal Deployment guide, you'll see 7001 and 7400 right there in the table for SIP and XMPP.

upvoted 6 times

**msully** 1 year ago

This is the correct answer

upvoted 1 times

  **tilo1988** 1 year, 5 months ago

page 29(MRA):

SIP TLS: 7001

XMPP TCP 7400

SSH 2222

RTP/RTCP 2776 - 2777

upvoted 1 times

The screenshot shows a firewall configuration window with the following sections:

- IP Configuration:**
  - IP protocol: IPv4
  - Use dual network interfaces: Yes
  - External LAN interface: LAN 1
  - IPv4 gateway: 192.168.108.1
- LAN 1 - Internal:**
  - IPv4 address: 192.168.114.18
  - IPv4 subnet mask: 255.255.255.0
  - IPv4 subnet range: 192.168.114.0 - 192.168.114.255
  - IPv4 static NAT mode: Off
  - Maximum transmission unit (MTU): 1500
- LAN 2 - External:**
  - IPv4 address: 192.168.108.2
  - IPv4 subnet mask: 255.255.255.0
  - IPv4 subnet range: 192.168.108.0 - 192.168.108.255
  - IPv4 static NAT mode: Off
  - Maximum transmission unit (MTU): 1500

A "Save" button is located at the bottom left of the configuration window.

Refer to the exhibit. The firewall has been configured from NAT 192.168.108.2 to 100.64.0.1. Which configuration changes are needed for an Expressway-E with dual network interfaces?

A.

External LAN interface: LAN 2  
 LAN 1 IPv4 static NAT mode: On  
 LAN 1 IPv4 static NAT address: 100.64.0.1  
 LAN 2 IPv4 static NAT mode: On  
 LAN 2 IPv4 static NAT address: 100.64.0.1

B.

External LAN interface: LAN 2  
 LAN 2 IPv4 static NAT mode: On  
 LAN 2 IPv4 static NAT address: 100.64.0.1

C.

External LAN interface: LAN 1  
 LAN 1 IPv4 static NAT mode: On  
 LAN 1 IPv4 static NAT address: 100.64.0.1

D.

External LAN interface: LAN 2  
 LAN 1 IPv4 static NAT mode: On  
 LAN 1 IPv4 static NAT address: 100.64.0.1

Suggested Answer: B

JamieF66 8 months, 2 weeks ago

B is correct

upvoted 3 times

An engineer is deploying an Expressway solution for the SIP domain Cisco.com. Which SRV record should be configured in the public DNS to support inbound B2B calls?

- A. \_collab-edge.\_tls.cisco.com
- B. \_cisco-uds.\_tcp.cisco.com
- C. \_sip.\_tcp.cisco.com
- D. \_cuplogin.\_tcp.cisco.com

**Suggested Answer:** C

Reference:

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2018/pdf/BRKCOL-2018.pdf>

  **jonycakes** 1 year ago

C is correct:

SIP B2B - Cisco SRV Records for business-to-business

\_sips.\_tcp.domain 5061 TLS

\_sip.\_tcp.domain 5060 TCP

\_sip.\_udp.domain 5060 UDP

upvoted 3 times

A call is sent by Cisco UCM to Expressway with a URI of 75080001@expc1a.pod8.test.lab. If (7508'i')@expc1a\pod8\test\lab.\* is the pattern string, what would be the replacement string of the transform in Expressway to re-write the call so that it becomes 75080001@conf.pod8.test.lab?

- A. \1@conf\pod8.test.lab.@"
- B. \1@conf\pod8\test\lab.\*"
- C. \1@conf.pod8\test\lab"
- D. \1@conf\pod8\test.lab.!"

**Suggested Answer: C**

Community vote distribution

C (100%)

🗳️ 👤 **OZtemp** 9 months ago

Shouldn't the answer be: \1@conf\pod8\test\lab instead of \1@conf.pod8\test\lab? Why isn't there a slash before the period beginning with pod8?

upvoted 2 times

🗳️ 👤 **Panda\_man** 1 year, 8 months ago

**Selected Answer: C**

C is correct

upvoted 2 times

🗳️ 👤 **TestingAAgain** 3 years ago

Actually, none of the answers are valid. I plugged this into the expression tester on my Expressway C in my lab, and the alias does not match the regex pattern.

upvoted 1 times

🗳️ 👤 **TestingAAgain** 3 years ago

The problem is the apostrophe pipe ( ' | ). The apostrophe isn't a valid character in REGEX, and the pipe specifies a logical OR. BUT, assuming the regex pattern was: (7508.\*)@expc1a\pod8\test\lab, then the answer would be C as verified by the expression tester. C doesn't work due to the unescaped period in the string, and the others add extra unwanted characters to the output.

upvoted 1 times

🗳️ 👤 **rob79** 3 years, 8 months ago

Shouldn't this be B?

upvoted 1 times

🗳️ 👤 **rob79** 3 years, 6 months ago

Sorry ignore this C is correct

upvoted 3 times

Transforms											
Priority	State	Description	Pattern	Type	Behavior	Replace					
<input type="checkbox"/> 1	✓ Enabled	Strip Domain from all calls	(.*)@(.*)	Regex	Replace	\1					
<input type="checkbox"/> 2	✓ Enabled	add pod1 local domain to all requests	(.*)	Regex	Replace	\1@pod1.local					

Search rules											
Priority	Rule name	Protocol	Source	Mode	Pattern type	Pattern string	Pattern behavior	On match	Target	SIP variant	Enabled
1	Route all Calls to Local Zone	Any	Any	Any alias				Continue	LocalZone	Any	✓

Search history				
Search type	Source	Destination	SIP variant	Status
SIP (INVITE)	jabberuser@pod1.local	sip:endpointc@pod1.local	Standards-based	Not found
SIP (INVITE)	jabberuser@pod1.local	sip:endpointb@pod1.local	Standards-based	Not found
SIP (INVITE)	jabberuser@pod1.local	sip:endpointa@pod1.local	Standards-based	Not found

Refer to the exhibit. Calls to locally registered endpoints are failing. At present, there are two endpoints registered locally to this Expressway. An H.323 endpoint with an alias of `EndpointA` is registered, and a SIP endpoint with an alias of `EndpointB@pod1.local` is also registered. How is this issue resolved?

- A. The dialplan must be redesigned to use the transforms to convert the alias into SIP URI format and then use separate search rules for each format that needs to be dialed within the local zone.
- B. The calls are failing because there are insufficient licenses. Additional licenses must be installed for the Expressway to route these calls.
- C. The current search rule does not match the call, so the search rule must be modified to include a SIP Variant of `Standards-Based`.
- D. Calling parties are placing calls with the wrong domain. End-users must be instructed not to use the pod1.local domain as that is owned by the local system. Calls to any other domain would work.

#### Suggested Answer: A

Community vote distribution

A (100%)

 Collabinski 11 months, 1 week ago

**Selected Answer: A**

Stripping @domain for dialing to H.323 numbers

SIP endpoints can only make calls in the form of URIs - for example name@domain. If the caller does not specify a domain when placing the call, the SIP endpoint automatically appends its own domain to the number that is dialed. So if you dial 123 from a SIP endpoint, the search will be placed for 123@domain. If the H.323 endpoint being dialed is registered as 123, the VCS will be unable to locate the alias 123@domain and the call will fail.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0/exwy\\_b\\_cisco-expressway-administrator-guide/exwy\\_m\\_dial-plan-and-call-processing.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0/exwy_b_cisco-expressway-administrator-guide/exwy_m_dial-plan-and-call-processing.html)

upvoted 2 times

```

tvcs: Event="System Configuration Changed" Detail="xConfiguration Bandwidth
Link 17 Pipe2 Name: " Level="1"
httpd[10591]: web: Event="System Configuration Changed" Detail="Create Zones
Zone 7 ZoneName: cms4.pod1.local" Src-ip="10.0.251.192" Src-port="50107"
User="admin" Level="1"
httpd[10591]: web: Event="System Configuration Changed" Detail="Create Zones
Zone 7 Type: Neighbor" Src-ip="10.0.251.192" Src-port="50107" User="admin"
Level="1"
httpd[10591]: web: Event="System Configuration Changed" Detail="Zones Zone 7
H323 Mode - changed from: On to: Off" Src-ip="10.0.251.192" Src-port="50107"
User="admin" Level="1"
httpd[10591]: web: Event="System Configuration Changed" Detail="Zones Zone 7
Neighbor SIP B2BUA Replaces Mode - changed from: Forward to: Terminate"
Src-ip="10.0.251.192" Src-port="50107" User="admin" Level="1"
httpd[10591]: web: Event="System Configuration Changed" Detail="Zones Zone 7
Neighbor Peer Address - changed from: to: cms4.pod1.local"
Src-ip="10.0.251.192" Src-port="50107" User="admin" Level="1"
tvcs: Event="System Configuration Changed" Detail="xConfiguration Zones Zone 7
H323 Mode: Off" Level="1"
tvcs: Event="System Configuration Changed" Detail="xConfiguration Zones Zone 7
Neighbor SIP B2BUA Replaces Mode: Terminate" Level="1"
tvcs: Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="cms4.pod1.local" Type="A and AAAA"
tvcs: Event="System Configuration Changed" Detail="xConfiguration Zones Zone 7
Neighbor Peer 1 Address: cms4.pod1.local" Level="1"
tvcs: Module="network.dns" Level="DEBUG": Detail="Could not resolve hostname"

```

Refer to the exhibit. A new neighbor zone is added for a new Cisco Meeting Server, but the zone is showing a SIP status of failed from the time the zone it was created. What should be done to resolve this issue?

- A. The search rule must be changed to continue on match
- B. The existing zone using ID 7 must be deleted
- C. More bandwidth must be added to the appropriate pipes
- D. The underlying DNS issue must be resolved

**Suggested Answer: D**

Community vote distribution

D (100%)

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

**Selected Answer: D**

Should be D, at the end it says "Could not resolve hostname"  
upvoted 6 times

 **Madc5** Highly Voted 2 years, 3 months ago

D is corect  
upvoted 5 times

 **Collabinski** Most Recent 11 months, 2 weeks ago

Looks like A to me.

<https://www.cisco.com/c/en/us/support/docs/unified-communications/spark/212475-troubleshooting-guide-for-cisco-spark-hy.html#anc18>

The general rule of thumb with Search rules is the more specific the Pattern string, the lower it can be placed in the Search rule priority list. Generally a DNS Zone is configured with a Pattern string that is going to catch anything that is not a local domain and send it to the Internet. Due to this, we recommend that you set that type of Search rule to a high priority so it's invoked last.

It seems like a Search Rule match would resolve the "underlying DNS issue"  
upvoted 2 times

 **TestingAAgain** 1 year, 6 months ago

**Selected Answer: D**

D is correct.

upvoted 1 times

Which two considerations must be made when using Expressway media traversal? (Choose two.)

- A. It is possible to NAT both Expressway-E interfaces
- B. The Unified Communications traversal zone should be used for MRA
- C. The Expressway-E must be put in a firewall DMZ segment
- D. Expressway Control is the traversal server installed in the DMZ
- E. Cisco UCM zone should be either traversal server or client

**Suggested Answer:** BC

Community vote distribution

BC (100%)

🗨️ 👤 **Panda\_man** 8 months, 2 weeks ago

**Selected Answer: BC**

BC correct

upvoted 1 times

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

**Selected Answer: BC**

• An Expressway-E located outside the firewall on the public network or in the DMZ, which acts as the firewall traversal server.

Unified Communications features such as Mobile and Remote Access or Jabber Guest, require a Unified Communications traversal zone connection between the Expressway-C and the Expressway-E. This involves:

- Installing suitable security certificates on the Expressway-C and the Expressway-E.
- Configuring a Unified Communications traversal zone between the Expressway-C and the Expressway-E.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0/exwy\\_b\\_cisco-expressway-administrator-guide/exwy\\_m\\_unified-communications.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0/exwy_b_cisco-expressway-administrator-guide/exwy_m_unified-communications.html)

upvoted 2 times

Jabber cannot log in via Mobile and Remote Access. You inspect Expressway-C logs and see this error message:

XCP\_JABBERD Detail="Unable to connect to host '%IP%', port 7400:(111) Connection refused"

Which is the cause of this issue?

- A. Rich Media Session licenses are not activated on Expressway-E.
- B. Expressway-E is listening on the wrong IP interface.
- C. The destination port for Expressway-E is set to 7400 instead of 8443 on the Expressway-C.
- D. The XCP Service is not activated on Expressway-E.

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **Abhishek1610** Highly Voted 👍 3 years ago

<https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/118798-technote-cucm-00.html#anc6>  
upvoted 7 times

🗳️ 👤 **Collabinski** Most Recent ⌚ 11 months, 1 week ago

**Selected Answer: B**

B is correct. kljw5 has the right explanation.  
upvoted 2 times

🗳️ 👤 **kljw5** 1 year, 7 months ago

Expressway-C Logs Show This Error: XCP\_JABBERD Detail="Unable to connect to host '%IP%', port 7400:(111) Connection refused"

If Expressway-E Network Interface Controller (NIC) is incorrectly configured, this can cause the Extensible Communications Platform (XCP) server to not be updated. If Expressway-E meets these criteria, then you will probably encounter this issue:

Uses a single NIC.

Advanced Networking Option Key is installed.

The Use Dual Network Interfaces option is set to Yes.

In order to correct this problem, change the Use Dual Network Interfaces option to No.

The reason this is a problem is because Expressway-E listens for the XCP session on the wrong network interface, which causes the connection to fail/timeout. Expressway-E listens on TCP port 7400 for the XCP session. You can verify this if you use the netstat command from the VCS as root.  
upvoted 3 times

🗳️ 👤 **Abhishek1610** 3 years ago

If Expressway-E Network Interface Controller (NIC) is incorrectly configured, this can cause the Extensible Communications Platform (XCP) server to not be updated.  
upvoted 1 times

🗳️ 👤 **khader09** 3 years, 2 months ago

B is correct

<https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/118798-technote-cucm-00.html#anc9>  
upvoted 2 times

Which configuration is required when implementing Mobile and Remote Access on Cisco Expressway?

- A. IPS
- B. SAML authentication
- C. Cisco Unified CM publisher address
- D. SSO

**Suggested Answer:** C

*Community vote distribution*

C (100%)

  **Collabinski** 11 months, 1 week ago

**Selected Answer: C**

Step 1

On the Expressway-C primary peer, go to Configuration > Unified Communications > Unified CM servers.

Step 2

Click New and add the following details for the publisher node:

- Unified CM publisher address—The server address of the publisher node.
- Username—User ID of an account that can access the server.
- Password—Password of the account that can access the server
- TLS verify mode (What about for basic MRA without ICE – is this recommended?)
- AEM GCM media encryption—Set to On to enable AEM GCM support. This field appears only if you
- Deployment—If you have configured multiple Deployments, select the appropriate deployment. Note that this field does not appear unless you have configured deployments.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-7/exwy\\_b\\_mra-deployment/exwy\\_m\\_basic-configuration.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-7/exwy_b_mra-deployment/exwy_m_basic-configuration.html)

upvoted 1 times

  **leigh1141** 2 years, 10 months ago

Unified CM configuration is required for MRA

upvoted 1 times

What is the purpose of using ICE for Mobile and Remote Access endpoints in the Cisco Collaboration infrastructure?

- A. ICE controls the bandwidth usage for Cisco Collaboration endpoints if the endpoints are located outside the company network.
- B. ICE enables Cisco Collaboration endpoints to determine if there is direct connectivity between them.
- C. ICE uses FAST updates to optimize the video quality in case of packet loss. This technology is available only from Cisco Unified CM version 11.5 and later.
- D. ICE enablement allows for the Cisco Collaboration endpoint to register through Expressway servers to Cisco Unified Communications Manager behind a firewall.

**Suggested Answer: B**

*Community vote distribution*

B (100%)

  **Collabinski** 11 months, 1 week ago

**Selected Answer: B**

Interactive Connectivity Establishment (ICE), defined in RFC 8445, is a protocol that combines STUN and TURN. Using ICE, endpoints can determine if there is direct connectivity between them and will then apply the STUN hole-punching techniques to keep the firewall ports opened, thus allowing for both inbound and outbound media traffic. If direct media connectivity cannot be achieved, the endpoints will fall back to the TURN server and will send their UDP traffic centrally instead of going peer-to-peer.

<https://www.cisco.com/c/en/us/td/docs/solutions/PA/ICE/icepa125.html>

upvoted 1 times

  **Ernisa** 10 months ago

Correct, except that ICE is not a protocol, it is a framework, a technique or a mechanism.

upvoted 1 times

  **Mark03** 2 years, 10 months ago

Answer is B

<https://www.cisco.com/c/en/us/td/docs/solutions/PA/ICE/icepa125.html>

upvoted 3 times

  **khader09** 3 years, 2 months ago

The following ICE-capable endpoints can send media directly to each other when they are MRA-registered and ICE passthrough is enabled:

upvoted 3 times

  **khader09** 3 years, 2 months ago

B is correct

upvoted 3 times

When deploying an Expressway Core and Expressway Edge cluster for mobile and remote access, which TLS verify subject name must be configured on the Expressway-E UC traversal zone?

- A. Webex CUSP Cluster Name
- B. Expressway-E Cluster Name
- C. Cisco Unified Communications Manager Publisher FQDN
- D. Expressway-C Cluster Name

**Suggested Answer: B**

Community vote distribution

D (100%)

🗳️ 👤 **BangBang86** Highly Voted 3 years, 4 months ago

This should be Expressway-C cluster FQDN.  
upvoted 6 times

🗳️ 👤 **Abhishek1610** Highly Voted 2 years, 12 months ago

The correct answer is D. Expressway-C Cluster Name  
upvoted 5 times

🗳️ 👤 **Collabinski** Most Recent 11 months, 1 week ago

**Selected Answer: D**

On Expressway-E enter the name to look for in the traversal client's certificate (must be in the Subject Alternative Name attribute). If there is a cluster of traversal clients, specify the cluster name here and ensure that it is included in each client's certificate.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-5/exwy\\_b\\_mra-expressway-deployment-guide/exwy\\_b\\_mra-expressway-deployment-guide\\_chapter\\_01000.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-5/exwy_b_mra-expressway-deployment-guide/exwy_b_mra-expressway-deployment-guide_chapter_01000.html)

upvoted 2 times

🗳️ 👤 **AKREM86** 1 year, 6 months ago

Answer is D.

Explanation: [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X8-8/Mobile-Remote-Access-via-Expressway-Deployment-Guide-X8-8.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X8-8/Mobile-Remote-Access-via-Expressway-Deployment-Guide-X8-8.pdf)

On Expressway E, Enter the name to look for in the traversal client's certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). If there is a cluster of traversal clients, specify the cluster name here and ensure that it is included in each client's certificate.

Traversal Client is EXP-C

upvoted 3 times

🗳️ 👤 **chacthor** 1 year, 10 months ago

Should be D

upvoted 2 times

🗳️ 👤 **tilo1988** 1 year, 11 months ago

@Adminiistrator: Change the correct answer to D! NOT B

upvoted 1 times

🗳️ 👤 **rob79** 2 years ago

D Expressway C is correct

upvoted 3 times

🗳️ 👤 **Simdude** 2 years, 12 months ago

D is the correct why would exp-e need to know its tls name

upvoted 3 times

🗳️ 👤 **ddrogi** 3 years, 1 month ago



D. Expressway-C FQDN

upvoted 5 times

  **khader09** 3 years, 2 months ago

B. Expressway-E Cluster Name

upvoted 2 times

  **Madc5** 2 years, 3 months ago

wrong answer

upvoted 3 times

```
Module="network.ldap" Level="INFO": Detail="Authentication credential found
in directory for identity: expresswayturn"

Module="developer.nomodule" Level="WARN"
CodeLocation="ppcmains/sip/sipproxy/
SipProxyAuthentication.cpp(686)" Method="SipProxyAuthentication::
checkDigestSAResponse" Thread="0x7a2485cb0700": calculated response does not
match supplied response,
calculatedResponse=769c8f488b71eebdf28b61ab1dc9f5e9,
response=319a0bb365dccf98c1bb7b3ce350f6cc

Event="Authentication Failed" Service="SIP" Src-ip="10.1.1.161"
Src-port="25713" Detail="Incorrect authentication credential for user"
Protocol="TLS" Method="OPTIONS" Level="1"
```

Refer to the exhibit. Mobile Cisco Jabber cannot register with on-premises Cisco Unified Communications Manager using Mobile and Remote Access. Some logs were captured on Expressway Edge.


Which action corrects this problem?

- A. Ensure that the peer address does not match the Common Name on certificate.
- B. Ensure that the \_cisco-uds SRV record has been configured.
- C. Ensure that the credential has been entered correctly.
- D. Ensure that the SIP domains are added on Expressway Core.

**Suggested Answer: C**

Community vote distribution

C (100%)

 **Collabinski** 11 months, 1 week ago

**Selected Answer: C**

When the password is incorrect, you see this in the Expressway-E logs:

```
Module="network.ldap" Level="INFO": Detail="Authentication credential found in directory for identity: traversal? Module="developer.nomodule"
Level="WARN" CodeLocation="ppcmains/sip/sipproxy/ SipProxyAuthentication.cpp(686)" Method="SipProxyAuthentication::
checkDigestSAResponse" Thread="0x7f2485cb0700": calculated response does not match supplied response,
calculatedResponse=769c8f488f71eebdf28b61ab1dc9f5e9, response=319a0bb365decf98c1bb7b3ce350f6ec Event="Authentication Failed"
Service="SIP" Src-ip="10.48.80.161" Src-port="25723" Detail="Incorrect authentication credential for user" Protocol="TLS" Method="OPTIONS"
Level="1"
```

<https://community.cisco.com/kxiwq67737/attachments/kxiwq67737/discussions-collaboration-apps/17264/1/117811-configure-vcs-00.pdf>  
upvoted 1 times

 **AKREM86** 1 year, 6 months ago

Correct Answer C: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2018/pdf/BRKCOL-2021.pdf>  
upvoted 1 times

 **khader09** 3 years, 2 months ago

When the password is incorrect, you see this in the Expressway-E logs:  
upvoted 1 times

 **kljw5** 1 year, 7 months ago

isn't that what it says "Incorrect authentication credential for user"??  
upvoted 2 times

Which two statements about Expressway media traversal are true? (Choose two.)

- A. Expressway Control is the traversal server installed in the DMZ.
- B. The Expressway Edge must be put in a firewall DMZ segment.
- C. Cisco Unified Communications Manager zone can be either traversal server or client.
- D. The Unified Communications traversal zone can be used for Mobile and Remote Access.
- E. Both Expressway Edge interfaces can be NATed.

**Suggested Answer:** BD

Community vote distribution

BD (100%)

  **chamba87** Highly Voted 2 years, 9 months ago

B & D are correct

upvoted 6 times

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

**Selected Answer:** BD

• An Expressway-E located outside the firewall on the public network or in the DMZ, which acts as the firewall traversal server.

Unified Communications features such as Mobile and Remote Access or Jabber Guest, require a Unified Communications traversal zone connection between the Expressway-C and the Expressway-E.



[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0/exwy\\_b\\_cisco-expressway-administrator-guide/exwy\\_m\\_unified-communications.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0/exwy_b_cisco-expressway-administrator-guide/exwy_m_unified-communications.html)

upvoted 1 times

  **leigh1141** 2 years, 10 months ago

D and E - Zone for MRA is always unfied coms and Expressway E must be deployed in the DMZ segment

upvoted 1 times

  **chacthor** 1 year, 10 months ago

It can't be E

upvoted 3 times

Which zone is required between Expressway-E and Expressway-C in Mobile and Remote Access deployments?

- A. Unified Communications traversal zone
- B. neighbor zone
- C. DNS zone
- D. traversal zone

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **Panda\_man** 8 months, 2 weeks ago

**Selected Answer: A**

A is correct

upvoted 1 times

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

Answer is A

Which type of traversal zone?

- If your deployment is for business to business calling, use a traversal zone.
- If your deployment is for mobile and remote access, use a Unified Communications traversal zone

upvoted 2 times

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

Unified Communications features such as Mobile and Remote Access or Jabber Guest, require a Unified Communications traversal zone connection between the Expressway-C and the Expressway-E.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0/exwy\\_b\\_cisco-expressway-administrator-guide/exwy\\_m\\_unified-communications.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0/exwy_b_cisco-expressway-administrator-guide/exwy_m_unified-communications.html)

upvoted 4 times

🗳️ 👤 **djs9nomad** 1 year, 6 months ago

Answer is D.

Traversal zone (client and server) between E and C.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0/exwy\\_b\\_cisco-expressway-administrator-guide/exwy\\_m\\_zones-and-neighbors.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0/exwy_b_cisco-expressway-administrator-guide/exwy_m_zones-and-neighbors.html)

upvoted 1 times

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

That's to set up a connection from Exp-C to Exp-E. A Unified Communications Traversal Zone is required for MRA to work.

upvoted 2 times


For a Mobile and Remote Access deployment, which server's certificate must include the Unified registration domain as a Subject Alternate Name?

- A. Expressway-C server certificate
- B. Cisco Unified Communications Manager server certificate
- C. Expressway-E server certificate
- D. Expressway-C and Expressway-E server certificate

**Suggested Answer:** C

Community vote distribution

C (100%)

 **khader09** Highly Voted 3 years, 2 months ago


The Expressway-E server certificate needs to include the following elements in its list of subject alternative names (SAN):

Unified CM registrations domains

XMPP federation domains

IM and Presence chat node aliases (federated group chat)

upvoted 9 times

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

**Selected Answer: C**

Expressway-E server certificate requirements

The Expressway-E server certificate must include the elements listed below in its list of subject alternative names (SAN). If the Expressway-E is also known by other FQDNs, all of the aliases must be included in the server certificate SAN.

- Unified CM registrations domains: all of the domains which are configured on the Expressway-C for Unified CM registrations. Required for secure communications between endpoint devices and Expressway-E.

The Unified CM registration domains used in the Expressway configuration and Expressway-E certificate, are used by Mobile and Remote Access clients to lookup the \_collab-edge DNS SRV record during service discovery. They enable MRA registrations on Unified CM, and are primarily for service discovery.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X14-0-2/cert\\_creation\\_use/exwy\\_b\\_certificate-creation-and-use-deployment-guide-x1402/exwy\\_b\\_certificate-creation-use-deployment-guide\\_chapter\\_011.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0-2/cert_creation_use/exwy_b_certificate-creation-and-use-deployment-guide-x1402/exwy_b_certificate-creation-use-deployment-guide_chapter_011.html)

upvoted 2 times

A Jabber user is being prompted to trust the Expressway-E certificate when using Mobile and Remote Access. The administrator has validated that the Expressway-E certificate is being trusted by the machine running the Jabber client. What else can be done to solve this problem?

- A. Create a new CSR with new information on the SAN field.
- B. Include Cisco Unified Communications Manager registration domain in the Expressway-E certificate as a SAN.
- C. Change the domain name.
- D. Change the FQDN of the Expressway.

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗨️ 👤 **Collabinski** 11 months, 1 week ago

**Selected Answer: B**

khader09s information is correct.

upvoted 1 times

🗨️ 👤 **Mark03** 2 years, 10 months ago

Answer is B:

<https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/118798-technote-cucm-00.html>

upvoted 3 times

🗨️ 👤 **khader09** 3 years, 2 months ago

The Unified CM registration domain used for the collab-edge record must be present within the SAN of the Expressway-E certificate. CSR tool in the Expressway server will give you the option to add the Unified CM registration domain as a SAN

upvoted 3 times

🗨️ 👤 **khader09** 3 years, 2 months ago

B is correct

upvoted 2 times

Which DNS record and port combination must be resolved externally for Mobile and Remote Access to be used?

- A. \_collab-edge on port 8443
- B. \_cisco-uds-edge on port 5061
- C. \_collab-edge on port 5061
- D. \_cisco-uds on port 8443

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **Collabinski** 11 months, 1 week ago

**Selected Answer: A**

Public DNS (External Domains)

The public, external DNS must be configured with \_collab-edge.\_tls.<domain> SRV records so that endpoints can discover the Expressway-Es to use for Mobile and Remote Access. You also need SIP service records for general deployment (not specifically for MRA).

Domain Service Protocol Priority Weight Port Target host

example.com collab-edge tls 10 10 8443 expe1.example.com

example.com collab-edge tls 10 10 8443 expe2.example.com

example.com sips tcp 10 10 5061 expe1.example.com

example.com sips tcp 10 10 5061 expe2.example.com

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X14-0/mra/exwy\\_b\\_mra-deployment-guide-14/exwy\\_m\\_requirements-for-mra.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0/mra/exwy_b_mra-deployment-guide-14/exwy_m_requirements-for-mra.html)

upvoted 1 times

 **leigh1141** 2 years, 10 months ago

A - 8443 is required from the public IP address of the expressway for collab-edge SRV records

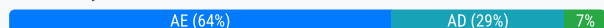
upvoted 3 times

Which two statements about Mobile and Remote Access certificate are true? (Choose two.)

- A. Expressway Core can use private CA signed certificate.
- B. You must upload the root certificates in the phone trust store.
- C. Expressway must generate certificate signing request.
- D. Expressway Edge must use public CA signed certificate.
- E. The Jabber client can work with public or private CA signed certificate.

**Suggested Answer: AE**

Community vote distribution



**TestingAAgain** Highly Voted 3 years ago

**Selected Answer: AE**

I meant to put A & E. Sorry.

upvoted 8 times

**BangBang86** Highly Voted 4 years, 10 months ago

Jabber works fine with a private CA, and the ExpC can use a private CA. Those should be the right answers.

upvoted 5 times

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

**Selected Answer: AE**

A. Expressway Core can use private CA signed certificate.

> Yes it can use a private CA signed cert. But the Exp-E needs to trust it. Is it best practice? I guess not. Bin there, done that.

B. You must upload the root certificates in the phone trust store.

> Nope

C. Expressway must generate certificate signing request.

> No, it doesn't have too (must not). I believe you can use a private key generated and provided by a CA, and upload it manually via SCP.

D. Expressway Edge must use public CA signed certificate.

> No it must not. Can work with a private CA signed cert.

E. The Jabber client can work with public or private CA signed certificate.

> Yes it can. It will prompt the user to trust the certificate presented, if the root or intermediate CA cert is not in the devices trust store. End of story.

So A&E correct answers.

upvoted 1 times

**ad5354f** 8 months, 1 week ago

I think Collabinski is right.

C and D are the answers I would prefer

A. Expressway Core can use private CA signed certificate – While technically possible, this is not recommended for MRA, as clients connecting via the Edge would not trust a private CA.

E. The Jabber client can work with public or private CA signed certificate – This is only partially true. The Jabber client can trust a private CA signed certificate if the root CA certificate is manually installed on the device, but for MRA via the Edge, a public CA is required for seamless operation.

upvoted 1 times

**Panda\_man** 1 year, 8 months ago

**Selected Answer: AD**

A and D

upvoted 2 times

**Testme1235** 2 years, 2 months ago

**Selected Answer: AE**

Which two statements about Mobile and Remote Access certificate are true? (Choose two.)



- A. Expressway Core can use private CA signed certificate.
- B. You must upload the root certificates in the phone trust store.
- C. Expressway must generate certificate signing request.
- D. Expressway Edge must use public CA signed certificate.
- E. The Jabber client can work with public or private CA signed certificate.

upvoted 1 times

  **Collabinski** 2 years, 5 months ago

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X8-9/Cisco-Expressway-Certificate-Creation-and-Use-Deployment-Guide-X8-9.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X8-9/Cisco-Expressway-Certificate-Creation-and-Use-Deployment-Guide-X8-9.pdf)

upvoted 1 times

  **jagifoto** 2 years, 4 months ago

Hi Collabinski , your answers are wrong.

upvoted 2 times

  **Collabinski** 2 years, 5 months ago

**Selected Answer: CD**

The only server that is really required to be signed by a public CA is the Expressway-E. This is the only server that clients will see the certificate from when signing in via MRA therefore using a public CA will ensure that users do not have to manually accept the certificate.

#### Certificate Generation Overview

X.509 certificates may be supplied from a third party, or may be generated by a certificate generator such as OpenSSL or a tool available in applications such as Microsoft Certification Authority. Third-party certificates supplied by recognized certificate authorities are recommended, although Expressway deployments in controlled or test environments can use internally generated certificates.

Certificate generation is usually a 3-stage process:

- Stage 1: generate a private key
- Stage 2: create a certificate request
- Stage 3: authorize and create the certificate

upvoted 2 times

  **Collabinski** 2 years, 5 months ago

I think C & D are correct.

<https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/213872-configure-and-troubleshoot-collaboration.html>

upvoted 2 times

  **ad5354f** 8 months, 1 week ago

i think , you're right.

upvoted 1 times

  **Collabinski** 2 years, 5 months ago

Whether the cert is public or private, it looks like you must generate a CSR in Expressway before uploading the file.

upvoted 1 times

  **aocstr** 1 year, 11 months ago

Not really, you can upload the certificate and private key generated by a CA without having to use CSR

upvoted 3 times

  **TestingAAgain** 3 years ago

**Selected Answer: AD**

I agree with the answers below. You can load a cert without a CSR as long as you also load the private key (you do this in clustering a lot), and you can use a private CA on the E as long as you're not going to have physical phones running through it.

upvoted 2 times

  **leigh1141** 4 years, 4 months ago

Answer is A and D. Expressway C can use a public/private. Expressway E must use a private

upvoted 3 times

  **tclpj** 4 years, 11 months ago

answer should be A and D. For C, I think the key work is "can" or "must"

upvoted 4 times

In a Mobile and Remote Access deployment, where must communications be encrypted with TLS?


- A. Cisco Expressway-E and endpoints outside the enterprise
- B. Cisco Expressway-C, Cisco Unified Communications Manager, and IM&P
- C. Cisco Expressway-C, Cisco Expressway-E, and Cisco Unified Communications Manager
- D. Cisco Expressway-C, Cisco Expressway-E, and endpoints outside the enterprise

**Suggested Answer: D**

Community vote distribution

D (75%)

A (25%)

  **FilipeM** Highly Voted 3 years ago

D is correct:

"All signaling between the Cisco Expressway-E and the external endpoints must be encrypted and depending on the endpoint software version, traffic must also be authenticated with certificates"

"The communication between the Cisco Expressway-C and the Cisco Expressway-E must always be encrypted and authenticated using server certificates from both servers"

upvoted 8 times

  **leigh1141** 2 years, 10 months ago

Agreed - answer would be D

upvoted 3 times

  **jagifoto** Most Recent 10 months ago

D. Cisco Expressway-C, Cisco Expressway-E, and endpoints outside the enterprise must be the answer.

upvoted 1 times

  **Collabinski** 11 months, 1 week ago

**Selected Answer: A**

Public DNS (External Domains)

The public, external DNS must be configured with \_collab-edge.\_tls.<domain> SRV records so that endpoints can discover the Expressway-Es to use for Mobile and Remote Access. You also need SIP service records for general deployment (not specifically for MRA).

Domain Service Protocol Priority Weight Port Target host

example.com collab-edge tls 10 10 8443 expe1.example.com



example.com collab-edge tls 10 10 8443 expe2.example.com

example.com sips tcp 10 10 5061 expe1.example.com

example.com sips tcp 10 10 5061 expe2.example.com

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X14-0/mra/exwy\\_b\\_mra-deployment-guide-14/exwy\\_m\\_requirements-for-mra.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0/mra/exwy_b_mra-deployment-guide-14/exwy_m_requirements-for-mra.html)

upvoted 1 times

  **iamnoone** 3 months, 2 weeks ago

The traversal zone (UCM or not) between the C&E must also be encrypted.

upvoted 1 times

  **itzme2nw** 1 year, 11 months ago

**Selected Answer: D**

It should be D

MRA requires secure communication between Expressway-C and Expressway-E, and between Expressway-E and external endpoints.

As per tech note

<https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/118798-technote-cucm-00.html>

upvoted 3 times


  **Abhishek1610** 3 years ago

Correct answer Option A.

MRA requires secure communication between Expressway-C and Expressway-E, and between Expressway-E and external endpoints

<https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/118798-technote-cucm-00.html#anc6>

upvoted 1 times

  **chamba87** 2 years, 9 months ago

then Aswer is D

upvoted 5 times

  **Mash11** 3 years, 1 month ago

Media encryption is enforced on the call legs between the Expressway-C and the Expressway-E, and between

the Expressway-E and endpoints located outside the enterprise.

upvoted 3 times

  **khader09** 3 years, 2 months ago

A is correct

upvoted 1 times

When determining why Mobile and Remote Access to Cisco TelePresence equipment does not work anymore for an organization. There are several administrators and configuration changes could have happened without anyone knowing. Internal communication seems to be working, but no external system can register or call anywhere. Gathering symptoms, you also discover that no internal systems can call out either. What is TraversalZone missing that causes this issue?

- A. link to the DefaultZone
- B. pipe to the DefaultZone
- C. SIP trunk to the DefaultZone
- D. route pattern to the DefaultZone

**Suggested Answer: C**

Community vote distribution

A (100%)

🗳️ 👤 **BangBang86** Highly Voted 3 years, 4 months ago

There is no way to set a SIP Trunk to the ExpC defaultZone, instead this is a possible missing "Link" to the defaultZone.  
upvoted 10 times

🗳️ 👤 **Collabinski** Most Recent 11 months, 1 week ago

Selected Answer: A

The Expressway comes preconfigured with the Default Zone and default links between it and the Traversal Subzone. You can also manage calls from unrecognized systems and endpoints by configuring the "links" and "pipes" associated with the Default Zone.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0-2/exwy\\_b\\_cisco-expressway-administrator-guide-x1402/exwy\\_m\\_zones-and-neighbors.html#reference\\_AB9714D9A58AB2411A667F451A8ED9A5](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0-2/exwy_b_cisco-expressway-administrator-guide-x1402/exwy_m_zones-and-neighbors.html#reference_AB9714D9A58AB2411A667F451A8ED9A5)  
upvoted 1 times

🗳️ 👤 **AKREM86** 1 year, 6 months ago

Correct Answer A. Link to DefaultZone  
Explanation here :

"Using Links and Pipes to Manage Access and Bandwidth

You can also manage calls from unrecognized systems and endpoints by configuring the "links" and "pipes" associated with the Default Zone. For example, you can delete the default links to prevent any incoming calls from unrecognized endpoints, or apply pipes to the default links to control the bandwidth consumed by incoming calls from unrecognized endpoints."

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/X14-0-2/exwy\\_b\\_cisco-expressway-administrator-guide-x1402/exwy\\_m\\_zones-and-neighbors.html#reference\\_AB9714D9A58AB2411A667F451A8ED9A5](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/admin_guide/X14-0-2/exwy_b_cisco-expressway-administrator-guide-x1402/exwy_m_zones-and-neighbors.html#reference_AB9714D9A58AB2411A667F451A8ED9A5)  
upvoted 1 times

🗳️ 👤 **Abhishek1610** 3 years ago

The correct answer is option "A" - link to the DefaultZone  
upvoted 3 times

🗳️ 👤 **khader09** 3 years, 2 months ago

route pattern to the DefaultZone  
upvoted 1 times

🗳️ 👤 **Madc5** 2 years, 3 months ago

is, wrong, can you explain your decision?  
upvoted 1 times

Which entry in the public (external) DNS is valid to configure DNS SRV records for a Cisco Mobile and Remote Access solution?

- A. \_cisco-uds.\_tcp.<domain>
- B. \_cisco-mra.\_tls.<domain>
- C. \_collab-edge.\_tls.<domain>
- D. \_cisco-expwy.\_tls.<domain>

**Suggested Answer: A**

Community vote distribution

C (100%)

Abhishek1610 Highly Voted 3 years ago

\_cisco-uds is used for CUCM  
\_collab-edge is used for MRA  
\_cuplogin is used for IM&P

Correct answer is option C. \_collab-edge.\_tls.<domain>  
upvoted 5 times

BangBang86 Highly Voted 3 years, 4 months ago

\_cisco-uds is used for internal communication, while \_collab-edge is used for external clients.  
upvoted 5 times

Collabinski Most Recent 11 months, 1 week ago

**Selected Answer: C**

Public DNS (External Domains) The public, external DNS must be configured with \_collab-edge.\_tls. SRV records so that endpoints can discover the Expressway-Es to use for Mobile and Remote Access.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-5/exwy\\_b\\_mra-expressway-deployment-guide/exwy\\_b\\_mra-expressway-deployment-guide\\_chapter\\_0100.pdf](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-5/exwy_b_mra-expressway-deployment-guide/exwy_b_mra-expressway-deployment-guide_chapter_0100.pdf)  
upvoted 1 times

khader09 3 years, 2 months ago

\_collab-edge.\_tls.<domain>  
upvoted 4 times

Prorod 3 years, 3 months ago

\_collab-edge.\_tls.<domain> is used for external resolution  
upvoted 3 times

```

2021-02-02T12:18:27.359-08:00 expc tvcs: UTime="2021-02-02 20:18:27,359" Module="network.sip" Level="INFO": Action="Sent" Local-ip="1
2021-02-02T12:18:27.360-08:00 expc tvcs: UTime="2021-02-02 20:18:27,359" Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="
SIPMSG:
|REGISTER sip:cucm.pod1.local SIP/2.0
Via: SIP/2.0/TCP 10.0.101.115:5060;egress-zone=CEtcpucmipod1local;branch=z9hG4bKaa525ee7842f3b408b2cbc882ff5866237642.8b46bf0f88eff29ef
Via: SIP/2.0/TLS 10.0.101.119:7002;egress-zone=UC;branch=z9hG4bK0822ed2041bc6f7a15d68e86ce58290b2465.967ceda2f6ae2c01deb5a118f58ab29e;
Via: SIP/2.0/TLS 10.0.132.202:54651;branch=z9hG4bK00006696;received=10.0.132.202;ingress-zone=CollaborationEdgeZone
Call-ID: 005056ae-48d5084e-000041c1-00004e3b@10.0.132.202
CSeq: 4351 REGISTER
Contact: <sip:6649132f-la5c-a445-9400-869c6960b0d9@10.0.101.115:5060;transport=tcp;orig-hostport=10.0.132.202:54651>;+sip.instance="<ur
From: <sip:2000@cucm.pod1.local>;tag=005056ae48d5085000002633-0000339d
To: <sip:2000@cucm.pod1.local>
Max-Forwards: 14
Route: <sip:cucm.pod1.local;transport=tcp;lr>
User-Agent: Cisco-CSF
Expires: 3600
Date: Tue, 02 Feb 2021 20:18:26 GMT
Supported: replaces,join,sdp-anat,norefersub,resource-priority,extended-refer,X-cisco-callinfo,X-cisco-serviceuri,X-cisco-escapecodes,}
P-Asserted-Identity: <sip:2000@cucm.pod1.local>
Reason: SIP ;cause=200;text="cisco-alarm:24 Name=CSFjabberuse ActiveLoad=Jabber_for_Windows-11.8.2.50390 InactiveLoad=Jabber_for_Windo
Session-ID: c0d0278100255000a0000dcf900d0000;remote=00000000000000000000000000000000
Content-Type: multipart/mixed;boundary=uniqueBoundary
Content-Length: 1271
2021-02-02T12:18:27.363-08:00 expc tvcs: UTime="2021-02-02 20:18:27,362" Module="network.sip" Level="INFO": Action="Received" Local-i
2021-02-02T12:18:27.363-08:00 expc tvcs: UTime="2021-02-02 20:18:27,363" Module="network.sip" Level="DEBUG": Action="Received" Local-
SIPMSG:
|SIP/2.0 405 Method Not Allowed
Via: SIP/2.0/TCP 10.0.101.115:5060;egress-zone=CEtcpucmipod1localrt=7002;ingress-zone=UCZone,SIP/2.0/TLS 10.0.132.202:54651;branch=z9hG
Call-ID: 005056ae-48d5084e-000041c1-00004e3b@10.0.132.202
CSeq: 4351 REGISTER
From: <sip:2000@cucm.pod1.local>;tag=005056ae48d5085000002633-0000339d
To: <sip:2000@cucm.pod1.local>;tag=220085250
Allow: INVITE,OPTIONS,INFO,BYE,CANCEL,ACK,PRACK,UPDATE,REFER,SUBSCRIBE,NOTIFY
Server: Cisco-CUCM12.5
Date: Tue, 02 Feb 2021 20:18:27 GMT
Warning: 399 cucm "SIP trunk disallows REGISTER"
Content-Length: 0

```

Refer to the exhibit. An engineer is deploying mobile and remote access in an environment that already had functioning Business to Business calling. Mobile and remote access SIP registrations are failing. To troubleshoot, SIP logs were collected. How is this issue resolved?

- A. Change the SIP profile on the SIP trunk for the Expressway-E to Standard SIP Profile for TelePresence Endpoint
- B. Change the Incoming Port in the SIP Trunk Security Profile for the Expressway-C to not match SIP line registrations
- C. Enable autoregistration for the appropriate DN range on the Cisco UCM servers running the CallManager service
- D. Write a custom normalization script since the vcs-interop normalization script does not allow registrations

**Suggested Answer: B**

Community vote distribution

B (100%)

 **Collabinski** 11 months, 1 week ago

**Selected Answer: B**

A diagnostic log from Expressway-C shows a SIP/2.0 405 Method Not Allowed message in response to the Registration request sent by the Jabber client. This is likely due to an existing Session Initiation Protocol (SIP) trunk between Expressway-C and CUCM using port 5060/5061. In order to correct this issue, change the SIP port on the SIP Trunk Security Profile that is applied to the existing SIP trunk configured in CUCM and the Expressway-C neighbor zone for CUCM to a different port such as 5065.

<https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/118798-technote-cucm-00.html#anc16>

upvoted 1 times

 **Ol\_Mykhailiuk** 1 year, 1 month ago

**Selected Answer: B**

In order to correct this issue, change the SIP port on the SIP Trunk Security Profile that is applied to the existing SIP trunk configured in CUCM and the Expressway-C neighbor zone for CUCM to a different port such as 5065.

upvoted 1 times

 **Omitted** 1 year, 6 months ago

**Selected Answer: B**

B is correct, this is a common issue. <https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/118798-technote-cucm-00.html#anc16>

upvoted 3 times

### Unified Communications status

Unified Communications (last updated: 14:11:51 PST)

Unified Communications status Enabled

Unified CM registrations Domain configured but no active zone connection

IM and Presence Service Domain configured but no active zone connection

XMPP Federation Not configured ([Configure a domain on Expressway-C](#))

Single Sign-On support Not configured (Enable on the [Unified Communications](#) page)

OAuth token with refresh Not configured (Enable on the [Unified Communications](#) page)

#### Activity

Unified CM calls: Current video	0
Unified CM calls: Current audio (SIP)	0
Current UCM/LDAP basic authenticated sessions	8
Total UCM/LDAP basic authenticated sessions	15
Total provisioning requests since last restart	21

#### Domains

Name	Services	Associated zones
<a href="#">pod1.local</a>	Unified CM registrations, IM and Presence Service	No associated zones

#### Servers

<a href="#">IM and Presence Service nodes</a>	1
<a href="#">Unified CM servers</a>	1
<a href="#">Unity Connection servers</a>	There are no <a href="#">Unity Connection servers</a> configured.

#### Zones

There are no Unified Communications traversal zones configured. [Configure a secure Unified Communications traversal zone connection between this Expressway-C and the Expressway-E](#)

```

xstatus zones zone 2
's Zones: /
Zone:
2:
  Bandwidth:
  ClusterUsage: "0"
  LocalUsage: "0"
  Name: "EXPE.pod1.local"
  Status: "Active"
  TraversalClient:
  Peer:
  SIP:
    Address: "10.0.101.119"
    Apparent: "10.0.101.115:27240"
    LastStatusChange: "2021-02-02 14:26:21"
    Port: "7001"
    ResourceUsage:
    NonTraversalCallsAvailable: "1500"
    ProtocolMode: "Both"
    RegistrationsAvailable: "0"
    ResourceUsageValid: "True"
  TURN:
    Port:
    Count: "0"
    Port: "3478"
    Ports:
    Count: "1"
  TURNRelaysAvailable: "1800"
  TraversalCallsAvailable: "300"
  Server: "TANDBERG/4137 (X12.5.3)"
  Status: "Active"
  Type: "TraversalClient"

```

Refer to the exhibit. Logins and failing via mobile and remote access. How is this resolved?

- A. Mobile and remote access login has not been enabled for the domain configured in the Expressway-C. The domain must be edited to allow Cisco UCM registrations.
- B. SIP is disabled on the Expressway-E. The SIP protocol must be enabled on the server.
- C. No Cisco UCM servers are configured in the Expressway-C. Servers must be added for CallManager and IM and Presence services.
- D. Although a traversal client zone exists, there is no Unified Communications traversal client zone. One must be created.

#### Suggested Answer: D

Community vote distribution

D (100%)

**Madc5** Highly Voted 2 years, 3 months ago

D is correct

upvoted 8 times

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

Selected Answer: D

Unified CM registrations and IM&P say the "domain is configured but no active zone connection. This link has the suggestion from the Mentor in the Community thread.

<https://community.cisco.com/t5/other-collaboration-subjects/cisco-vcs-mra-there-are-no-unified-communications-traversal/td-p/2693645>

upvoted 1 times

**Collabinski** 11 months, 3 weeks ago

While D could be correct. CUCM is not configured in the Exp-C here. Wouldn't that need to be resolved first before the UC Traversal Zone could work?

upvoted 1 times

**Collabinski** 11 months, 1 week ago

Disregard. I see the active IM&P and Unified CM servers under the Server section.

upvoted 1 times

**TestingAAgain** 1 year, 6 months ago

Selected Answer: D

D is correct. If you look at the bottom of the diagram, it shows a CUCM server configured and also states at the very bottom that the UC traversal zone is not configured

upvoted 3 times

**Alarms**

Alarm	Description
<input type="checkbox"/> Unified CM port conflict	There is a port conflict on Unified CM 10.0.101.111 between neighbor zone CUCM.pod1.local and Unified Communications (both are using port 5060)
Action	
The same port on Unified CM cannot be used for line side (Unified Communications) and SIP trunk traffic. Review the port configuration on Unified CM and reconfigure the <a href="#">Zone</a> if necessary	

Refer to the exhibit. Mobile and remote access is being added to an existing B2B deployment and is failing. When the administrator looks at the alarms on the

Expressway-C, the snippets are shown. Which configuration action should the administrator take to fix this issue?

- A. The listening port on the Expressway-C for SIP TCP must be changed to a value other than 5060
- B. The listening port on the Expressway-C for SIP TLS must be changed to a value other than 5061
- C. The listening port on the Cisco UCM for the Expressway-C SIP trunk must be changed to something other than 5060 or 5061
- D. The listening port on the Cisco UCM for the Expressway-C SIP trunk is set to something other than 5060 or 5061. It must be set to 5060 for insecure and 5061 for secure SIP

**Suggested Answer: C**

Community vote distribution

C (100%)

**Collabinski** 11 months, 1 week ago

**Selected Answer: C**

Also, this was mentioned in the doc.

† Unified CM can listen on 5061 for TCP SIP but we discourage it.

upvoted 1 times

**Collabinski** 11 months, 3 weeks ago

\* If you have MRA connections to the Unified CM, which are line-side connections to 5060/5061, then you should avoid using 5060/5061 as the listening port for any SIP trunks you create on that Unified CM.

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-5/Cisco-Expressway-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X12-5.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-5/Cisco-Expressway-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X12-5.pdf)

upvoted 1 times

**TestingAAgain** 1 year, 6 months ago

**Selected Answer: C**

Should be C

upvoted 2 times

**chacthor** 1 year, 10 months ago

Should be C

upvoted 2 times

**tilo1988** 1 year, 11 months ago

Page 131 on following LINK: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2018/pdf/BRKUCC-2801.pdf>

C is correct

upvoted 3 times

**Madc5** 2 years, 3 months ago

must be C

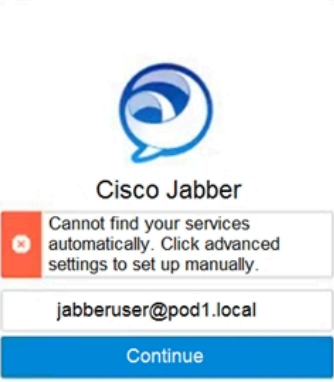
upvoted 4 times

**jonycakes** 2 years ago

You are correct sir, C is the answer:

Source: <https://video.cisco.com/video/5828524592001>

upvoted 2 times



```
Standard query 0x2b84 SRV _cisco-uds._tcp.pod1.local
Standard query response 0x2b84 No such name SRV _cisco-uds._tcp.pod1.local SOA ad.skype.local
Standard query 0x71d9 SRV _cuplogin._tcp.pod1.local
Standard query response 0x71d9 No such name SRV _cuplogin._tcp.pod1.local SOA ad.skype.local
Standard query 0x27bb SRV _collab-edge._tls.pod1.local
Standard query response 0x27bb No such name SRV _collab-edge._tls.pod1.local SOA ad.skype.local
Standard query 0xb09e SRV _collab-edge._tls.pod1.local
Standard query response 0xb09e No such name SRV _collab-edge._tls.pod1.local SOA ad.skype.local
Standard query 0xe2b5 A pod1.local
Standard query response 0xe2b5 A pod1.local SOA ad.skype.local
Standard query 0x687e A pod1
Standard query 0x687e A pod1
Standard query 0xa661 A loginp.webexconnect.com
Standard query response 0xa661 A loginp.webexconnect.com (NAME global-cas-c63.webexconnect.com )
Standard query 0xccba SRV _cisco-uds._tcp.pod1.local
Standard query response 0xccba No such name SRV _cisco-uds._tcp.pod1.local SOA ad.skype.local
Standard query 0x8530 SRV _cuplogin._tcp.pod1.local
Standard query response 0x8530 No such name SRV _cuplogin._tcp.pod1.local SOA ad.skype.local
Standard query 0xd02d SRV _collab-edge._tls.pod1.local
Standard query response 0xd02d No such name SRV _collab-edge._tls.pod1.local SOA ad.skype.local
Standard query 0x91d6 SRV _cisco-uds._tcp.pod1.local
Standard query response 0x91d6 No such name SRV _cisco-uds._tcp.pod1.local SOA ad.skype.local
Standard query 0x0648 SRV _cuplogin._tcp.pod1.local
Standard query response 0x0648 No such name SRV _cuplogin._tcp.pod1.local SOA ad.skype.local
Standard query 0xb4fa SRV _cisco-uds._tcp.pod1.local
Standard query response 0xb4fa No such name SRV _cisco-uds._tcp.pod1.local SOA ad.skype.local
Standard query 0x5299 SRV _cuplogin._tcp.pod1.local
Standard query response 0x5299 No such name SRV _cuplogin._tcp.pod1.local SOA ad.skype.local
```

Refer to the exhibit. The administrator attempted to log in, but Jabber clients cannot log in via mobile and remote access. How is this issue resolved?

- A. Skype for Business mode must be disabled on the DNS server because it conflicts with Jabber login requirements.
- B. The domain pod1.local must be deprovisioned from the Webex cloud for Jabber logins.
- C. A DNS SRV record must be created for \_collab-edge.\_tls.pod1.local that points to the Expressway-E.
- D. The username jabberuser@pod1.local is invalid. The user should instead sign-in simply as jabberuser.

**Suggested Answer: C**

Community vote distribution

C (100%)

 **Collabinski** 11 months, 1 week ago

**Selected Answer: C**

C is correct

upvoted 1 times

```

Module="network.tcp" Level="DEBUG": Dst-ip="10.0.101.119" Dst-port="7002" Detail="TCP Connecting"
Module="network.tcp" Level="DEBUG": Dst-ip="10.0.101.119" Dst-port="7002" Detail="TCP Connection Established"
Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.0.101.115" Src-port="27161" Dst-ip="10.0.101.119"
  Dst-port="7002" Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Common-name="10.0.101.119"

```

Valid from	Friday, October 18, 2019 ...
Valid to	Sunday, October 17, 202...
Subject	expe.pod1.local, Systems...
Public key	RSA (4096 Bits)
Public key parameters	05 00
Enhanced Key Usage	Server Authentication (1....
Subject Alternative Name	DNS Name=expe.pod1.local
Subject Key Identifier	c7b28ee75e675005198f9...

**Location**

Peer 1 address	10.0.101.119		SIP: Failed to connect to 10.0.101.119:7002 : TLS negotiation failure <a href="#">Check the certificates for the traversal connection</a>
Peer 2 address			
Peer 3 address			
Peer 4 address			
Peer 5 address			
Peer 6 address			

Refer to the exhibit showing logs from the Expressway-C, a copy of the Expressway-E certificate, and the UC traversal zone configuration for the Expressway-C.

An office administrator is deploying mobile and remote access and sees an issue with the UC traversal zone. The zone is showing `TLS negotiation failure`. What is causing this issue?

- A. The Expressway-E certificate includes the Expressway-C FQDN as a SAN entry
- B. The Expressway-C is missing the FQDN of Cisco UCM in the Common Name of its certificate
- C. In the UC Traversal Zone on the Expressway-C, the peer address is set to the IP of the Expressway-E, which is not a SAN entry in the Expressway-E certificate
- D. The Expressway-E does not have the FQDN of Cisco UCM listed as a SAN in its certificate

**Suggested Answer: D**

Community vote distribution

C (100%)

**Madc5** Highly Voted 2 years, 3 months ago

the correct answer is C

upvoted 15 times

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

**Selected Answer: C**

UC Traversal Zone Settings

Peer 1 address

Enter the FQDN of the Expressway-E.

Note that if you use an IP address (not recommended), that address must be present in the Expressway-E server certificate.

If you have configured Expressway-E with a dual NIC interface for MRA, enter the FQDN of Expressway-E's internal interface (not the IP address).

Expressway-C requires a local DNS record that points to the FQDN of the Expressway-E's internal LAN.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X14-0-1/mra/exwy\\_b\\_mra-deployment-guide-x1401/exwy\\_m\\_basic-configuration.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0-1/mra/exwy_b_mra-deployment-guide-x1401/exwy_m_basic-configuration.html)

upvoted 2 times

  **AKREM86** 1 year, 6 months ago

It should be C.

Explanation : "Enter the FQDN of the Expressway-E.

Note that if you use an IP address (not recommended), that address must be present in the Expressway-E server certificate."

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X14-0-1/mra/exwy\\_b\\_mra-deployment-guide-x1401/exwy\\_m\\_basic-configuration.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0-1/mra/exwy_b_mra-deployment-guide-x1401/exwy_m_basic-configuration.html)

upvoted 2 times

Which part of a hybrid cloud-based deployment with Cisco Webex Messenger Service is used for meeting capabilities?

- A. Cisco Unified CM is always used for meeting capabilities.
- B. Depending on the media flow, the Webex Meeting Center or local Cisco Unified CM meeting resources are used for meeting capabilities.
- C. Depending on the origin of the user, the Webex Meeting Center or local Cisco Unified Communications Manager meeting resources are used for meeting capabilities.
- D. Cisco Webex Meeting Center is always used for meeting capabilities.

**Suggested Answer: D**

Community vote distribution

D (100%)

🗳️ 👤 **BangBang86** Highly Voted 3 years, 4 months ago

The answer should be "Depending on the origin of the user, the Webex Meeting Center or local Cisco Unified Communications Manager meeting resources are used for meeting capabilities." since the source of the user is the most relevant.

upvoted 5 times

🗳️ 👤 **Collabinski** Most Recent 11 months, 1 week ago

**Selected Answer: D**

D is correct

upvoted 2 times

🗳️ 👤 **msully** 1 year, 6 months ago

**Selected Answer: D**

The following services are available in a hybrid cloud-based deployment that uses Webex Messenger service:

Contact Source—The Cisco Webex Messenger service provides contact resolution.

Presence—The Cisco Webex Messenger service allows users to publish their availability and subscribe to other users' availability.

Instant Messaging—The Cisco Webex Messenger service allows users to send and receive instant messages.

Audio—Place audio calls through desk phone devices or computers through Cisco Unified Communications Manager.

Video—Place video calls through Cisco Unified Communications Manager.

Conferencing—Cisco Webex Meetings Center provides hosted meeting capabilities.

Voicemail—Send and receive voice messages through Cisco Unity Connection.

upvoted 1 times

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

**Selected Answer: D**

should be D

upvoted 3 times

🗳️ 👤 **lycaba** 2 years, 1 month ago

**Selected Answer: D**

The answer is D.

upvoted 3 times

🗳️ 👤 **chamba87** 2 years, 10 months ago

The answer is D



upvoted 2 times

🗳️ 👤 **Mark03** 2 years, 10 months ago

Answer: D

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/jabber/12\\_8/cjab\\_b\\_planning-guide-cisco-jabber-128/cjab\\_b\\_planning-guide-cisco-jabber-128\\_chapter\\_010.html?bookSearch=true#CJAB\\_RF\\_H9B69A5D\\_00](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/12_8/cjab_b_planning-guide-cisco-jabber-128/cjab_b_planning-guide-cisco-jabber-128_chapter_010.html?bookSearch=true#CJAB_RF_H9B69A5D_00)

upvoted 3 times

  **virtu** 2 years, 10 months ago

Answer is D. Based on Conferencing—Cisco Webex Meetings Center provides hosted meeting capabilities.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/jabber/12\\_5/Planning\\_Guide/cjab\\_b\\_planning-guide-for-cisco-jabber-125/cjab\\_b\\_planning-guide-for-cisco-jabber-125\\_chapter\\_011.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/12_5/Planning_Guide/cjab_b_planning-guide-for-cisco-jabber-125/cjab_b_planning-guide-for-cisco-jabber-125_chapter_011.html)

See section Hybrid Cloud-Based Deployment with Cisco Webex Messenger Service

upvoted 3 times

Which step is required when configuring Cisco Webex Hybrid Message Service?

- A. Register Expressway-C Connector Hosts to the Cisco Webex Cloud.
- B. Register Expressway-C to Cisco Unified Communications Manager.
- C. Add Expressway-C and Cisco Unified CM to the Cisco Webex Cloud.
- D. Add Cisco Unity Connection to Expressway-E.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

  **Collabinski** 11 months, 1 week ago

**Selected Answer: A**

We recommend that the Expressway-C be dedicated to hosting connectors for Webex Hybrid Services. You can use the Expressway-C connector host for other purposes, but that can change the supported number of users.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/spark/hybridservices/messageservice/cmgt\\_b\\_spark-hybrid-message-deployment-guide/cmgt\\_b\\_spark-hybrid-message-deployment-guide\\_chapter\\_01.html#task\\_E4158047C66F3B4FA5353D2156F999DB](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/messageservice/cmgt_b_spark-hybrid-message-deployment-guide/cmgt_b_spark-hybrid-message-deployment-guide_chapter_01.html#task_E4158047C66F3B4FA5353D2156F999DB)

upvoted 1 times

  **khader09** 3 years, 2 months ago

A. Register Expressway-C Connector Hosts to the Cisco Webex Cloud.

upvoted 4 times

Which service is available in a cloud-based deployment using Cisco Webex Messenger?

- A. Presence
- B. Phone services
- C. Voicemail
- D. Call forward services

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **khader09** Highly Voted 3 years, 2 months ago

The following services are available in a cloud-based deployment using Webex Messenger:

Contact Source

Presence—

Instant Messaging—.

Conferencing

upvoted 5 times

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

**Selected Answer: A**

The following services are available in a cloud-based deployment using Webex Messenger:

-Contact Source

-Presence

-Instant Messaging

-Conferencing

Cert Guide pg 446

upvoted 1 times

Which statement about the Cisco Webex hybrid service is true?

- A. Expressway Connector is required for an on-premises Exchange server.
- B. Hybrid Message service works only with Jabber cloud deployment.
- C. Directory Connector is required for Azure AD.
- D. Directory Connector must be deployed for OBTP to work with on-premises video devices.

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **Collabinski** 11 months, 1 week ago

**Selected Answer: A**

The Cisco Webex Hybrid Calendar Service high-level architecture, depicted in Figure 3-1, enables an organization to integrate their corporate Microsoft Exchange calendar services with Webex through the Expressway-C Connector Host.

This is in the link Mark03 provided  
upvoted 1 times

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

**Selected Answer: A**

Should be A. Directory connector is not required for OBTP....the calendar connector is.  
upvoted 3 times

🗳️ 👤 **Mark03** 2 years, 10 months ago

Answer is A

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/spark/hybridservices/calendarservice/cmgt\\_b\\_deploy-spark-hybrid-calendar-service/cmgt\\_b\\_deploy-spark-hybrid-calendar-service\\_chapter\\_011.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/calendarservice/cmgt_b_deploy-spark-hybrid-calendar-service/cmgt_b_deploy-spark-hybrid-calendar-service_chapter_011.html)  
upvoted 2 times

🗳️ 👤 **Abhishek1610** 3 years ago

Correct option is A  
upvoted 2 times

🗳️ 👤 **khader09** 3 years, 2 months ago

A. Expressway Connector is required for an on-premises Exchange server.  
upvoted 2 times

🗳️ 👤 **BangBang86** 3 years, 4 months ago

Indeed Expressway Connector is required.  
upvoted 3 times

Which two statements about Cisco Webex Video Mesh Nodes are true? (Choose two.)

- A. When Expressway Core works with VMN clusters, Expressway Core decides which VMN is used for signaling/media connection.
- B. Cloud-registered devices choose a VMN cluster based on the lowest STUN round trip delay.
- C. The cascading traffic between VMN must bypass the firewall.
- D. When Cisco Unified Communications Manager works with multiple VMNs, Cisco Unified CM decides which VMN is used for signaling connection.
- E. A VMN can terminate a media connection while operating in maintenance mode.

**Suggested Answer: BD**

Community vote distribution

BD (100%)

 **Collabinski** 11 months, 1 week ago

**Selected Answer: BD**


Look at the SIP Dial-in Flow to VMN (scenario1), it eludes to CUCM making decisions.

<https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2019/pdf/BRKCOL-2073.pdf>

Local reachable VMN resources are tried first, in order of lowest SRT delay. When all local resources are exhausted, the participant connects to the cloud.

Cert Guide pg 426

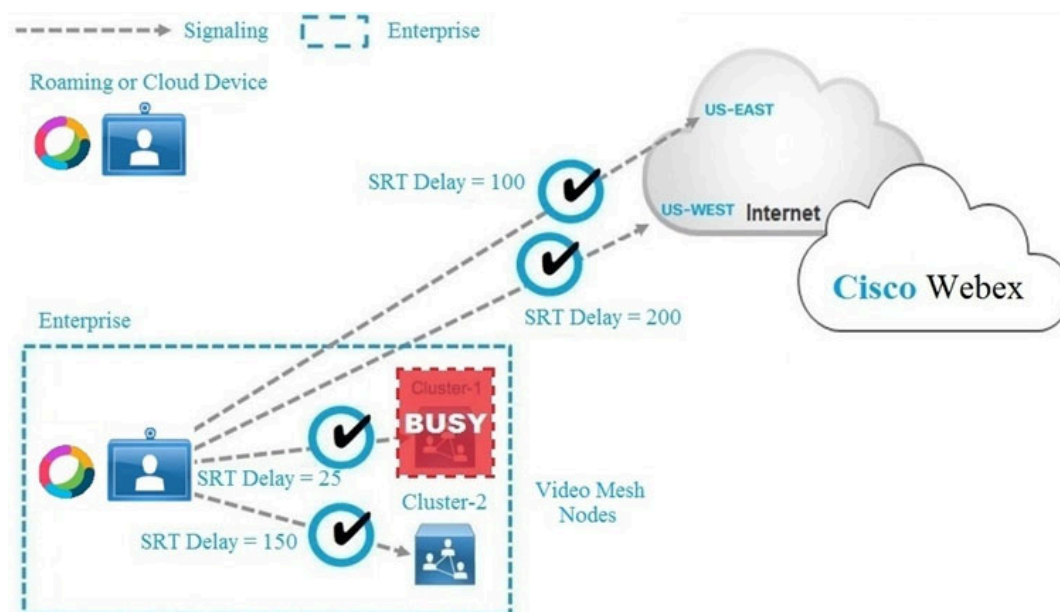
upvoted 1 times

 **tilo1988** 1 year, 11 months ago

D is correct because: In Unified CM, each SIP trunk can support up to 16 Video Mesh destinations (IP addresses). LINK:

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/wbxt/videomesh/cmgt\\_b\\_webex-video-mesh-deployment-guide/cmgt\\_b\\_hybrid-media-deployment-guide\\_chapter\\_011.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/videomesh/cmgt_b_webex-video-mesh-deployment-guide/cmgt_b_hybrid-media-deployment-guide_chapter_011.html)

upvoted 3 times



Refer to the exhibit. If the Webex Teams device cannot connect to Video Mesh Cluster-1 because it is busy, which media node does the Webex Teams device connect to next?

- A. Both Cloud Node US-EAST and US-WEST
- B. Video Mesh Cluster-2
- C. Cloud Node US-EAST
- D. Cloud Node US-WEST

**Suggested Answer: B**

Community vote distribution

B (100%)

**Collabinski** 11 months, 1 week ago

**Selected Answer: B**

Local reachable Video Mesh resources are tried first, in order of lowest SRT delay. When all local resources are exhausted, the participant connects to the cloud.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/wbxt/videomesh/cmgt\\_b\\_webex-video-mesh-deployment-guide/cmgt\\_b\\_hybrid-media-deployment-guide\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/videomesh/cmgt_b_webex-video-mesh-deployment-guide/cmgt_b_hybrid-media-deployment-guide_chapter_010.html)

upvoted 1 times

**Ol\_Mykhailiuk** 1 year ago

**Selected Answer: B**

Learned reachability information is provided to the Webex cloud every time a call is set up. This information allows the cloud to select the best resource (cluster or cloud), depending on the relative location of the client to available clusters and the type of call. If no resources are available in the preferred cluster, additional clusters are tested for availability based on SRT delay. A preferred cluster is chosen with the lowest SRT delay. Calls are served on premises from a secondary cluster when the primary cluster is busy. Local reachable Video Mesh resources are tried first, in order of lowest SRT delay. When all local resources are exhausted, the participant connects to the cloud.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/wbxt/videomesh/cmgt\\_b\\_webex-video-mesh-deployment-guide/cmgt\\_b\\_hybrid-media-deployment-guide\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/videomesh/cmgt_b_webex-video-mesh-deployment-guide/cmgt_b_hybrid-media-deployment-guide_chapter_010.html)

upvoted 1 times

**iulianm** 1 year, 5 months ago

I agree, B is right. Cluster 2 from on-premise has STUN Round-Trip Delay (SRT) lower than 250ms. In that case Cluster 2 will be selected. If Cluster 2 had for example SRT = 300 (>250) then cloud US-EAST will be chosen.

upvoted 2 times

🗨️ 👤 **chumleyex** 1 year, 9 months ago

I Agree, B is right.

Cloud Cluster Selection for Overflow Based on 250 ms or Higher STUN Round-Trip Delay

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/wbxt/videomesh/cmgt\\_b\\_webex-video-mesh-deployment-guide/cmgt\\_b\\_hybrid-media-deployment-guide\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/videomesh/cmgt_b_webex-video-mesh-deployment-guide/cmgt_b_hybrid-media-deployment-guide_chapter_010.html)

upvoted 1 times

🗨️ 👤 **undertabler** 1 year, 10 months ago

**Selected Answer: B**

The correct answer is B - Video Mesh Cluster-2. Local Webex Video Mesh resources are always tried first (unless the round-trip delay is not greater than 250 then the lower cloud resource would be used.) Source: Official Cert Guide

upvoted 3 times

🗨️ 👤 **chamba87** 2 years, 10 months ago

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/wbxt/videomesh/cmgt\\_b\\_webex-video-mesh-deployment-guide/cmgt\\_b\\_hybrid-media-deployment-guide\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/videomesh/cmgt_b_webex-video-mesh-deployment-guide/cmgt_b_hybrid-media-deployment-guide_chapter_010.html)

"Which cluster is used also depends on latency rather than just location. For example, a cloud cluster with lower STUN round-trip (SRT) delay than a Webex Video Mesh cluster may be a better candidate for the meeting. This logic prevents a user from landing on a geographically far cluster with a high SRT delay"

upvoted 2 times

🗨️ 👤 **tilo1988** 1 year, 11 months ago

the answer is C (US-EAST), correct?

upvoted 1 times

🗨️ 👤 **virtu** 2 years, 10 months ago

From my point of view, the answer will be C US-East based on the lowest SRT, because the question says The Webex Teams Endpoint, not SIP endpoint registered to CUCM. Based on the registration procedure, Webex Teams endpoint upon registration retrieves a list of nodes from Cloud, and make connectivity test to choose VMN based on the lowest SRT.

upvoted 2 times

🗨️ 👤 **khader09** 3 years, 2 months ago

A preferred cluster is chosen with the lowest SRT delay. Calls are served on premises from a secondary cluster when the primary cluster is busy. Local reachable Webex Video Mesh resources are tried first, in order of lowest SRT delay. When all local resources are exhausted, the participant connects to the cloud.

upvoted 2 times

A Cisco Webex Hybrid Video Mesh Node can be installed in the DMZ and on the internal network.

Which statement is true?

- A. Webex Cloud supports either a DMZ-based Mesh Node for security or an internal-based Mesh Node for media control only.
- B. Installing a Video Mesh Node in the DMZ requires you to open TCP and UDP port 4444 in your internal firewall for full clustering functionality.
- C. Installing a Video Mesh Node in the DMZ requires the external firewall to allow UDP traffic from ANY port to the address of the Video Mesh Nodes via port 5004.
- D. Using internal Video Mesh Node also works due to Mobile and Remote Access setup for Webex Teams clients. A DMZ node is added for extra security.

**Suggested Answer:** C

Community vote distribution

C (100%)

🗳️ 👤 **Collabinski** 11 months, 1 week ago

**Selected Answer: C**

Not recommended by Cisco, but C is correct.

DMZ-based deployment of the Video Mesh cluster is not recommended due to the following reasons:

- The external firewall will need to allow UDP traffic from ANY port to the address of the Video Mesh Nodes via port 5004, so that roaming Webex Teams endpoints can send media to the nodes. This is not a preferred approach.

<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.html>

upvoted 1 times

🗳️ 👤 **tilo1988** 1 year, 11 months ago

<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.html>

Answer is C

upvoted 2 times

🗳️ 👤 **chamba87** 2 years, 10 months ago

"The external firewall will need to allow UDP traffic from ANY port to the address of the Video Mesh Nodes via port 5004, so that roaming Webex Teams endpoints can send media to the nodes. This is not a preferred approach."

So yes, C is the correct answer

upvoted 3 times

🗳️ 👤 **leigh1141** 2 years, 10 months ago

Answer is C - It will use 5004 for traffic

upvoted 1 times

Where are voice calls handled in a Cisco Jabber hybrid cloud-based deployment with Cisco Webex Platform Service?

- A. Voice calls use Webex Calling platform for call control and use hybrid media nodes for local conferencing.
- B. Voice calls use local media nodes to keep traffic internal for internal traffic and use Webex Calling for external calls.
- C. Voice call use Cisco Unified Communications Manager for local calls and Webex Calling for external calls.
- D. Voice calls use local Cisco Unified Communications Manager for all calls.

**Suggested Answer:** D

*Community vote distribution*

D (100%)

 **Collabinski** 11 months, 1 week ago

**Selected Answer: D**

Configure Deskphone Control

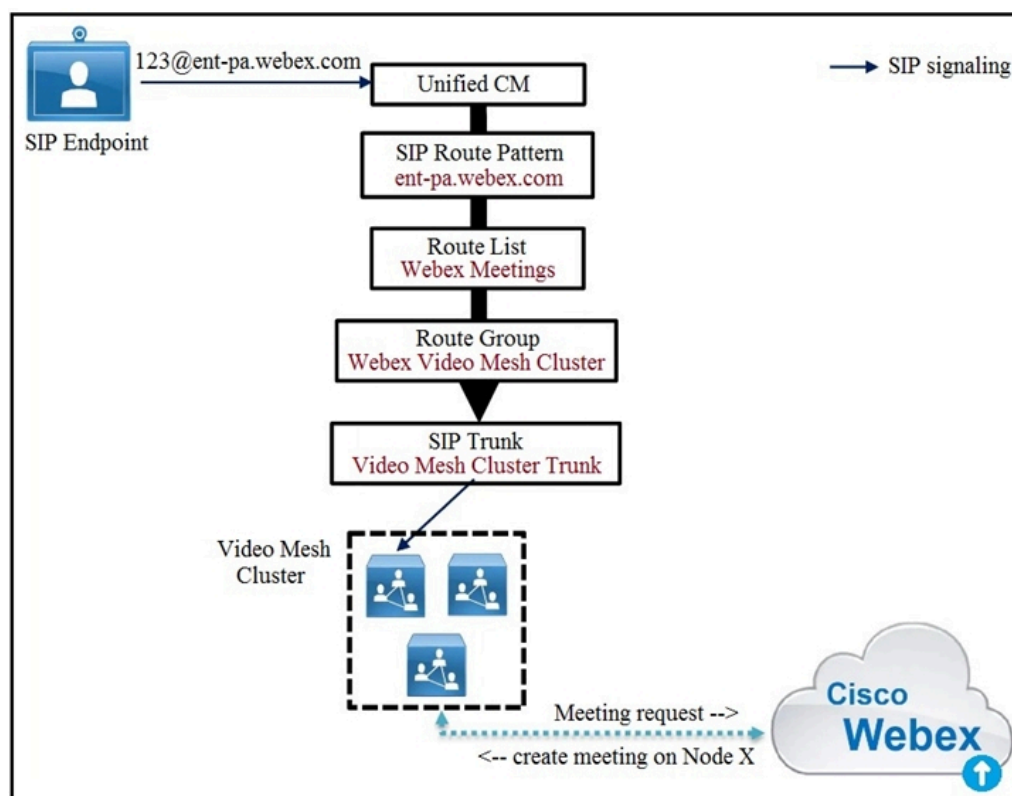
Prerequisites

The Cisco CTIManager service must be running in the Cisco Unified Communications Manager cluster.

- You cannot use this feature with devices that do not support CTI.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/jabber/12\\_5/DIGCloud/cjab\\_b\\_cloud-hybrid-deploy-125/cjab\\_b\\_cloud-hybrid-deploy-125\\_chapter\\_01001.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/12_5/DIGCloud/cjab_b_cloud-hybrid-deploy-125/cjab_b_cloud-hybrid-deploy-125_chapter_01001.html)

upvoted 2 times



Refer to the exhibit. Cisco Unified Communications Manager routes the call via the Webex Meetings route list and route group to the Video Mesh cluster Node#1 in the Video Mesh cluster is hosting the meeting and has reached full capacity, but other nodes in the cluster still have spare capacity.

What happens to the participant's call?

- A. Another node in the cluster is used and an intra-cluster cascade between the two Video Mesh nodes is formed.
- B. The call is queued.
- C. The call fails.
- D. Another node in the cluster is used and an intra-cluster cascade between Webex and the new Video Mesh node is formed.

**Suggested Answer: A**

Community vote distribution

A (100%)

**khader09** Highly Voted 3 years, 2 months ago

If the node hosting the meeting reaches full capacity, another node in the cluster will be used and an intra-cluster cascade will be formed. (The intra-cluster cascade routes from node to node, not via Webex.)

upvoted 12 times

**leigh1141** Highly Voted 2 years, 10 months ago

Answer is A > If the node hosting the meeting reaches full capacity, another node in the cluster will be used and an intra-cluster cascade will be formed.

<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/hms.html>

upvoted 6 times

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

Selected Answer: A

khader09 and leigh1141 have it correct. Answer is A



upvoted 2 times

**TestingAAgain** 1 year, 6 months ago

Selected Answer: A

answer is A

upvoted 3 times

  **BangBang86** 3 years, 4 months ago

The IntraCluster is not made against the cloud, instead it is handled locally to the cluster.

upvoted 2 times

  **Simdude** 3 years, 4 months ago

So answer is C ?

upvoted 1 times

  **khader09** 3 years, 2 months ago

answer is A

upvoted 4 times

An organization wants to enable a Cisco Webex connector to synchronize all employees automatically with Cisco Webex instead of using a manual list.

Where is the Webex Hybrid Directory Service configured?

- A. Install Cisco Directory Connector on a Microsoft Windows Domain server and configure the software and Webex Control Hub.
- B. Enable the directory service in Cisco Unified Communications Manager under Cisco Unified Serviceability and add the service in Webex Control Hub.
- C. Enable the directory service on Cisco Expressway Edge for Office 365 or Cisco Expressway Core for internal Active Directory and add the service in Webex Control Hub.
- D. Install the Cisco Express Connector and configure the device in Cisco Unified Communications Manager under Cisco Unified Serviceability and add the service in Webex Control Hub.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **Collabinski** 11 months, 1 week ago

<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/hybrid/12x/hybcvd/directory.html>

upvoted 1 times

🗳️ 👤 **Collabinski** 11 months, 1 week ago

**Selected Answer: A**

To deploy Webex Hybrid Directory Service in the PA for Webex Hybrid Services, we recommend the following:

- Ensure that the end-user account mail ID field in the Unified CM End User database contains the user's email address. Webex Teams users correlate to Cisco Unified CM end users by means of email addresses. With LDAP directory integration, the mail ID field for Unified CM end users is typically mapped from the mail field of the LDAP directory during synchronization.

- Install Cisco Directory Connector on a separate Windows server from the Active Directory Domain Service or Active Directory Lightweight Directory Services.

- Run a first synchronization after the Directory Connector installation finishes. Then configure full synchronization and incremental synchronization schedules to keep the Directory Connector (and in turn Webex) updated when resource and user information changes (resource or user update, deletion, or addition) within Microsoft Active Directory

upvoted 1 times

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

**Selected Answer: A**

Answer is A, but it's misleading as the server does NOT have to be a domain controller....just a member of the domain.

upvoted 2 times

🗳️ 👤 **Omitted** 1 year, 6 months ago

i think that is what was meant by domain server.

upvoted 1 times

🗳️ 👤 **Abhishek1610** 3 years ago

CDC is installed on Windows domain

upvoted 1 times

With QoS enabled, which two statements about the Cisco Webex Video Mesh Node signaling and media traffic are true? (Choose two.)

- A. From VMN to CUCM SIP endpoints, the source UDP ports from 52500 to 62999 is used for audio traffic.
- B. From VMN to Webex Teams clients, the source UDP port 5004 is used for video traffic.
- C. From Webex cloud to VMN, the source UDP port 9000 is used for audio traffic.
- D. From VMN to video endpoints, the destination UDP port 5004 is used for audio traffic.
- E. From VMN to Webex cloud, the destination UDP port 9000 is used for video traffic.

**Suggested Answer:** AB

  **Collabinski** 11 months, 1 week ago

Figure 2. Traffic Signatures for Video Mesh (Quality of Service Enabled) shows UDP 52500-62999 from SIP Endpoints to VMN and TCP/UDP 5004 from Webex Clients to VMN.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/wbxt/videomesh/cmgt\\_b\\_webex-video-mesh-deployment-guide/cmgt\\_b\\_hybrid-media-deployment-guide\\_chapter\\_010.html#reference\\_CAE1A60E80AE6EC7BF96DAE7980D792D](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/videomesh/cmgt_b_webex-video-mesh-deployment-guide/cmgt_b_hybrid-media-deployment-guide_chapter_010.html#reference_CAE1A60E80AE6EC7BF96DAE7980D792D)

upvoted 2 times

  **itzme2nw** 1 year, 11 months ago

A,B seems correct

Video Mesh Node Unified CM SIP endpoints 52500 to 62999 Unified CM SIP Profile EF Audio

Video Mesh Node Webex Teams application or endpoint 5004 52100 to 52299 AF41 Video

upvoted 2 times

  **chamba87** 2 years, 9 months ago

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/wbxt/videomesh/cmgt\\_b\\_webex-video-mesh-deployment-guide/cmgt\\_b\\_hybrid-media-deployment-guide\\_chapter\\_010.html#reference\\_CAE1A60E80AE6EC7BF96DAE7980D792D](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/videomesh/cmgt_b_webex-video-mesh-deployment-guide/cmgt_b_hybrid-media-deployment-guide_chapter_010.html#reference_CAE1A60E80AE6EC7BF96DAE7980D792D)

Looks like A and B are correct

upvoted 4 times

  **virtu** 2 years, 10 months ago

maybe A and D

upvoted 1 times

  **Collabinski** 11 months ago

Thought the same thing for a minute, but it is a vague answer.

upvoted 2 times

  **khader09** 3 years, 2 months ago

A and B

upvoted 2 times

What should be considered when using the Cisco Webex hybrid service?

- A. Directory Connector must be deployed for OBTP to work with on-premises video devices
- B. Directory Connector is required for Azure AD
- C. Hybrid Message service works only with Jabber cloud deployment
- D. Expressway Connector is required for an on-premises Exchange server

**Suggested Answer:** D

Community vote distribution

D (100%)

🗉 👤 **Dregtien** 8 months, 4 weeks ago

this question is already been asked : question 74

upvoted 1 times

🗉 👤 **Collabinski** 1 year, 5 months ago

Nothing in the documents provided mention anything about a Directory Connector required for Azure

upvoted 1 times

🗉 👤 **Collabinski** 1 year, 5 months ago

**Selected Answer: D**

D is correct

upvoted 2 times

🗉 👤 **TestingAAgain** 2 years ago

**Selected Answer: D**

Correct answer is D

upvoted 1 times

🗉 👤 **jonycakes** 2 years, 6 months ago

<Answer D>

Source: [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/spark/hybridServices/calendarService/cmgt\\_b\\_deploy-spark-hybrid-calendar-service/cmgt\\_b\\_deploy-spark-hybrid-calendar-service\\_chapter\\_011.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridServices/calendarService/cmgt_b_deploy-spark-hybrid-calendar-service/cmgt_b_deploy-spark-hybrid-calendar-service_chapter_011.html)

upvoted 2 times

🗉 👤 **Madc5** 2 years, 9 months ago

correct D

upvoted 3 times

When a Cisco Webex Video Mesh Node is configured for an organization, which process does the Webex Teams client use to discover the optimal bridging resource?

- A. the lowest STUN round-trip delay to each node and cloud
- B. a reachable Video Mesh Node and then overflows to the cloud, if needed
- C. the SIP delay header during call setup
- D. an HTTPS speed and latency test to each node and the cloud

**Suggested Answer:** B

Reference:

<https://www.cisco.com/c/en/us/solutions/collateral/unified-communications/spark-hybrid-services/datasheet-c78-738153.html>

Community vote distribution

B (100%)

🗳️ 👤 **FreeWill06** 1 year, 1 month ago

the question is about "discovering" not selecting, under this circumstances, I would say B is the correct answer.

upvoted 1 times

🗳️ 👤 **Omitted** 1 year, 6 months ago

**Selected Answer: B**

Tough because A isn't wrong but B is the better answer since lowest STUN RT isn't the only criteria.

upvoted 1 times

🗳️ 👤 **JCArias** 1 year, 7 months ago

B is correct, only selects cloud cluster if round-trip delay is higher than 250ms, but option A says the "lowest" which is not a rule always

upvoted 1 times

🗳️ 👤 **Pashat** 1 year, 11 months ago

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/wbxt/videomesh/cmgt\\_b\\_webex-video-mesh-deployment-guide/cmgt\\_b\\_hybrid-media-deployment-guide\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/videomesh/cmgt_b_webex-video-mesh-deployment-guide/cmgt_b_hybrid-media-deployment-guide_chapter_010.html)

looks like A to me. Document specifies low stun rtt

upvoted 2 times

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

Local reachable Video Mesh resources are tried first, in order of lowest SRT delay. When all local resources are exhausted, the participant connects to the cloud.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/wbxt/videomesh/cmgt\\_b\\_webex-video-mesh-deployment-guide/cmgt\\_b\\_hybrid-media-deployment-guide\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/videomesh/cmgt_b_webex-video-mesh-deployment-guide/cmgt_b_hybrid-media-deployment-guide_chapter_010.html)

upvoted 2 times