

Configuración de WebRTC de CMS o proxy de aplicación web sobre Expressway

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuration Steps](#)

[Paso 1. Integrar CMS WB en Expressway-C](#)

[Paso 2. Habilite la activación de Expressway-E y agregue la credencial de autenticación a la base de datos de autenticación local](#)

[Paso 3. Cambiar el puerto de administración de Expressway-E](#)

[Paso 4. Agregue Expressway-E como TURN Server\(s\) para NAT Traversal de medios en el servidor CMS](#)

[Verificación](#)

[Paso 1. En Expressway-C, comprobar que WB esté integrado correctamente](#)

[Paso 2. Verifique que se ha agregado el servidor TURN al servidor CMS](#)

[Paso 3. Verificación del uso de TURN Relay durante una llamada en curso](#)

[Troubleshoot](#)

[Se conecta el cliente WebRTC externo, pero no hay medios \(debido a una falla de ICE\)](#)

[El cliente WebRTC externo no recibe la opción para unirse a la llamada](#)

[El cliente WebRTC externo se atasca \(en la carga de medios\) al conectarse a cospace y, a continuación, se redirige a la página inicial de WB](#)

[El cliente WebRTC externo no se puede unir a cospace y recibe una advertencia \(no se puede conectar: vuelva a intentarlo más tarde\)](#)

[Información Relacionada](#)

Introducción

En este documento se describen los pasos para configurar y solucionar problemas en WebRTC de Cisco Meeting Server (CMS) mediante Expressway.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Expressway X12.6.1 y posterior (x12.6.1 y posterior solo pueden funcionar con CMS 2.9.2 o posterior debido a cambios en el comportamiento de EXP TURN)
- Servidor CMS 2.9.3 y posteriores
- traducción de Dirección de Red (NAT)
- Traversal mediante relés (GIRO) alrededor de NAT
- Utilidades transversales de sesión (STUN) para NAT
- Sistema de nombres de dominio (DNS)

Requisitos previos de configuración:

- La configuración básica de acceso móvil y remoto (MRA) (zona transversal de UC, túneles SSH) ya debe estar habilitada y configurada en Expressway. [Haga clic aquí](#) para obtener guías de MRA.
- Para CMS 2.9.x - WebBridge (WB), XMPP y CallBridge configurados y habilitados en CMS, consulte la [guía de configuración](#)
- Activar tecla opción instalado en el Expressway-E.
- Puerto TCP 443 abierto en el servidor de seguridad de la Internet pública a dirección de (dirección) del Expressway-E.
- TCP y UDP puerto 3478 (las solicitudes de activación) abrir en Firewall de internet pública a dirección de (dirección) del Expressway-E.
 - TCP 3478 solo se necesita si 'turnservers' en la API de CMS tiene tcpPortNumberOverride establecido en 3478.
- El puerto UDP 3478 (solicitudes TURN) se abrió en el firewall desde CMS a la dirección IP privada de Expressway-E (si utiliza Dual-NIC en Expressway-E).
 - CMS 2.9.2 y versiones anteriores envían solicitudes vinculantes al Exp E, mientras que 2.9.3 envía solicitudes de asignación
- Registros de DNS externo para la URL de unión para webbridge, que se pueden resolver en la dirección IP de acceso público de Expressway-E.
- Registro DNS interno para URL de conexión que se puede resolver en la dirección IP del servidor de webbridge.
- Si ejecuta X12.5.2 o una versión anterior, asegúrese de que se permita la reflexión NAT en el firewall externo para la dirección IP pública de Expressway-E. [Haga clic aquí](#) para ver un ejemplo de configuración. A partir de X12.5.3, esto ya no es necesario para un Expressway independiente.
- Al utilizar el puerto 443 para TURN, aún necesita abrir el puerto UDP 3478 para medios en el firewall externo.

Precaución: cuando el puerto TCP 443 está habilitado, Expressway ya no puede responder en el puerto TCP 3478.

Nota: el par de Expressway que se utiliza para los servicios Jabber Guest no se puede utilizar para los servicios de proxy CMS WebRTC.

Nota: Si va a actualizar a la versión 3.0 o posterior desde versiones anteriores, consulte [Guía para una actualización sin problemas desde Cisco Meeting Server 2.9 a la 3.0 \(y versiones posteriores\)](#)

Componentes Utilizados

Este documento no se limita a versiones específicas de software y hardware; sin embargo, deben cumplirse los requisitos mínimos de versión de software.

- CMS Application Program Interface (API)
- Expressway
- Servidor CMS

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La compatibilidad con proxy de WebRTC se ha agregado a Expressway desde la versión X8.9.2, que permite a los usuarios externos navegar a un puente web de Cisco Meeting Server.

Cientes externos y los invitados pueden administrar o unirse a espacios sin la necesidad de cualquier software que no sea un explorador compatible. [Haga clic aquí para obtener una lista de los exploradores compatibles.](#)

A partir del 5 de febrero de 2021, estos son los navegadores compatibles con CMS 3.1.1:

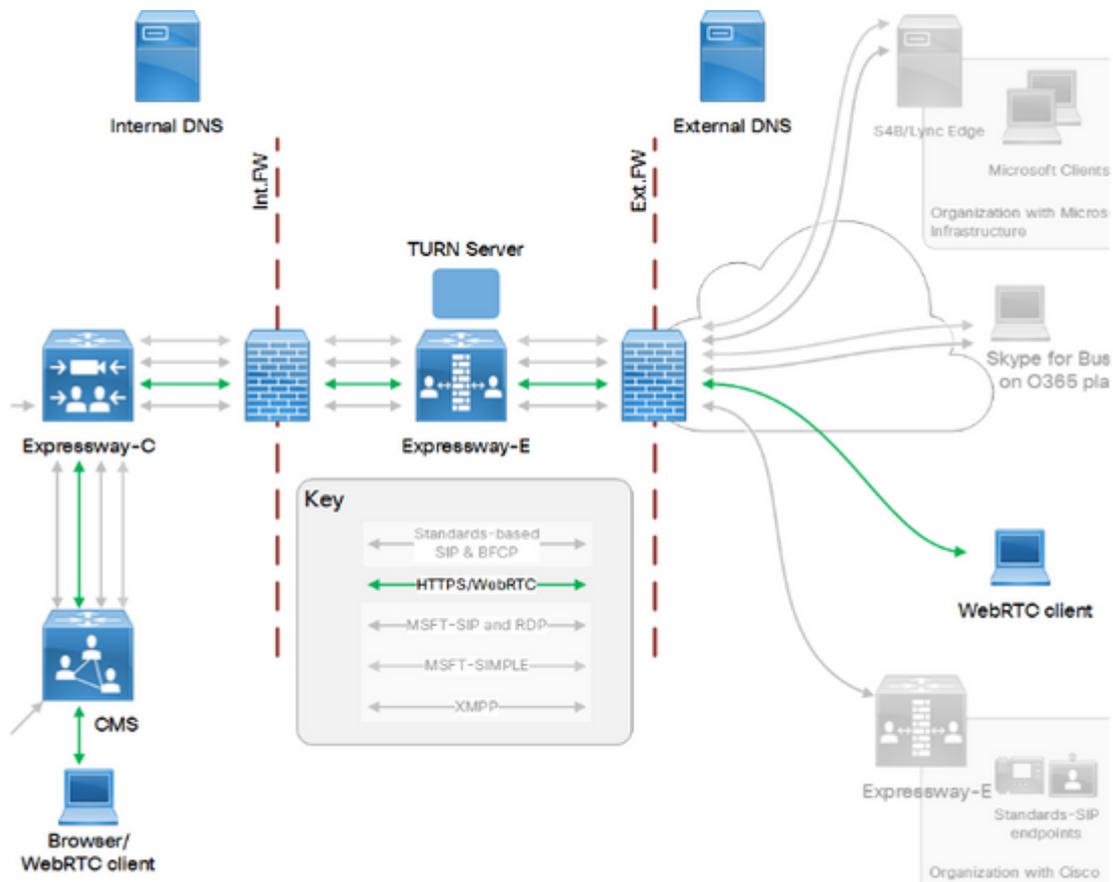
Browsers	Versions
Google Chrome (Windows, macOS and Android)	88
Mozilla Firefox (Windows)	82
Chromium-based Microsoft Edge (Windows)	88
Apple Safari for macOS	13.x and 14.0
Apple Safari for iOS	iOS versions: 13.x and 14.0
Yandex (Windows)	20.8 and 20.11

Note: Web app is not supported on the legacy Microsoft Edge.

Note: Web app is not supported on virtual machines (VMs) running these supported browsers.

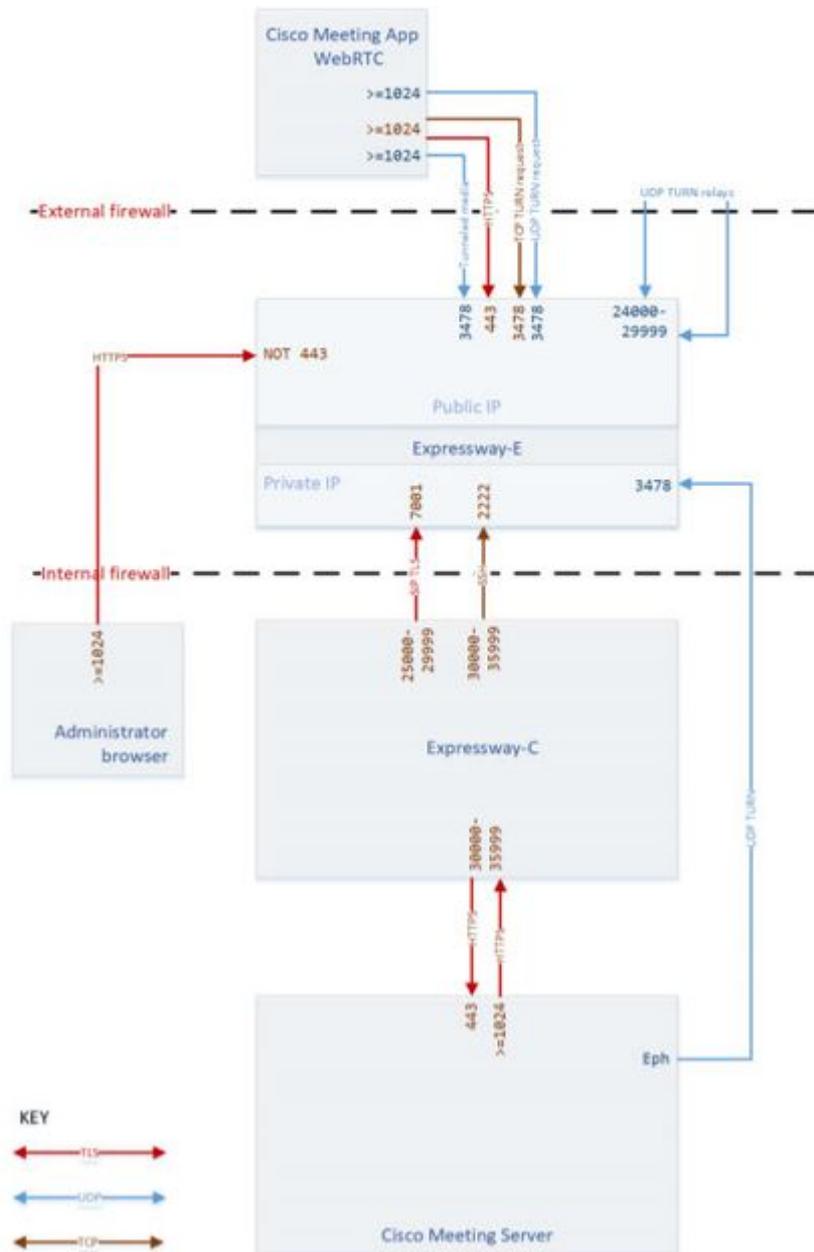
Configurar

Diagrama de la red



Esta imagen proporciona un ejemplo del flujo de conexiones de Web Proxy para CMS WebRTC: (de la [guía de configuración de Uso de puertos IP exp.](#))

Web Proxy for Cisco Meeting Server Connections



Nota: al ejecutar X12.5.2 o una versión anterior, debe configurar su firewall externo para permitir la reflexión NAT para la dirección IP pública y Expressway-E (los firewalls suelen desconfiar de los paquetes que tienen la misma dirección IP de origen y de destino). A partir de X12.5.3, esto ya no es necesario para un Expressway independiente.

Configuration Steps

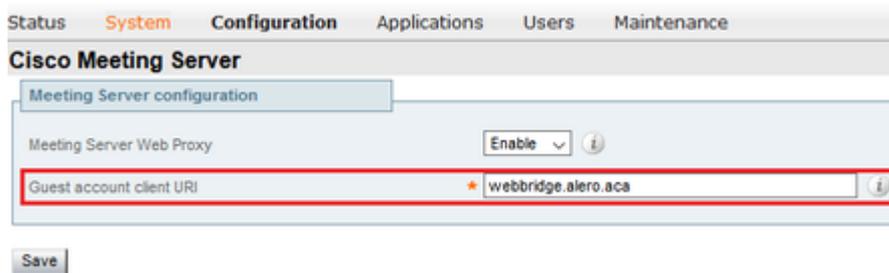
Paso 1. Integrar CMS WB en Expressway-C

- Vaya a **Configuration > Unified Communication > Cisco Meeting Server**.
- Habilite el **proxy web de Meeting Server**.

c. Introduzca la URL de unión en el campo **URI de cliente de cuenta de invitado**.

d. Click **Save**.

e. Agregue la URL de unión a CMS en el certificado de servidor de Expressway-E como un nombre alternativo de sujeto (SAN). Consulte la [Guía de implementación de creación y uso de certificados de Cisco VCS](#).



Paso 2. Habilite la activación de Expressway-E y agregue la credencial de autenticación a la base de datos de autenticación local

a. Vaya a **Configuration > Traversal > TURN**.

b. Habilite **TURN services**, de **off** a **on**.

c. Elija **Configure TURN client credentials on local database** y agregue las credenciales (nombre de usuario y contraseña).

Nota: Si tiene un clúster de Expressway-Es y todos se van a utilizar como servidores TURN, asegúrese de habilitarlo en todos los nodos. Debe configurar dos instancias turnServer independientes a través de la API y señalarlas a cada uno de los servidores de Expressway-E en el clúster (según el proceso de configuración que se muestra en el paso 4, que muestra el proceso para un servidor de Expressway-E; la configuración del segundo turnServer sería similar, solo usando las direcciones IP respectivas y las credenciales de activación para el otro servidor de Expressway-E).

Nota: Puede utilizar un equilibrador de carga de red delante de las autopistas para el tráfico TCP/HTTPS, pero los medios de activación deben pasar del cliente al servidor de activación de IP pública. Los medios de activación no deben pasar a través del equilibrador de carga de red

Paso 3. Cambiar el puerto de administración de Expressway-E

Este paso es necesario ya que las conexiones webrtc entran en TCP 443, pero Exp 12.7 introdujo una nueva Interfaz de administración dedicada (DMI) que se puede utilizar para 443.

a. Vaya a **System > Administration**.

b. En **Configuración del servidor Web**, cambie el **puerto del administrador Web** a **445** en las opciones desplegadas y, a continuación, haga clic en **Guardar**.

c. Repita los pasos 3a a 3b en todos los Expressway-E utilizados para los servicios de proxy WebRTC.

Nota: Cisco recomienda cambiar el puerto de administración porque los clientes WebRTC utilizan 443. Si el navegador WebRTC intenta 80 de puerto de acceso, el Expressway-E redirige la conexión a

Paso 4. Agregue Expressway-E como TURN Server(s) para NAT Traversal de medios en el servidor CMS

En CMS 2.9.x en adelante, utilice el menú **Configuration** > **API** para agregar servidores de turno:

- serverAddress: (dirección IP privada de Expressway)
- clientAddress: (dirección IP pública de Expressway)
- tipo: (expressway)
- nombre de usuario: (como se ha configurado en el paso 2c)
- contraseña: (según la configuración del paso 2c)
- tcpPortNumberOverride: 3478

d. Repita el paso 4c para cada servidor de Expressway-E que se utiliza para activar

Esta imagen proporciona un ejemplo de los pasos de configuración:

Field	Value	Present
serverAddress	Address CB reaches out to using 3478 UDP	present
clientAddress	Address Client (web app or WebRTC) uses for TURN	present
username	username that was configured in step 2c	present
password	password that was configured in step 2c	present
useShortTermCredentials	false	present
sharedSecret		
type	expressway	present
numRegistrations	0	present
tcpPortNumberOverride	3478	present
callBridge		Choose
callBridgeGroup		Choose

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Paso 1. En Expressway-C, comprobar que WB esté integrado correctamente

a. Vaya a **Configuration** > **Unified Communication** > **Cisco Meeting Server**. Debe ver la dirección IP del WB:

Status **System** Configuration Applications Users Maintenance

Cisco Meeting Server You are here: [C](#)

Meeting Server configuration

Meeting Server Web Proxy Enable

Guest account client URI *

Guest account client URI resolved to the following targets	
Name	Address
webbridge.alero.aca	10.48.36.5

b. Vaya a **Configuration > Unified Communication > HTTP allow list > Automatically added rules**. Compruebe que se ha agregado a las reglas:

Meeting Server web bridges	https	443	Prefix	/	GET, POST, PUT, HEAD, DELETE
Meeting Server web bridges	wss	443	Prefix	/	GET, POST, PUT, HEAD, DELETE

Nota: no se espera encontrar el WB en los nodos Detectados porque las reglas son simplemente para permitir el proxy del tráfico HTTPS al WB, y no necesariamente para la comunicación unificada.

c. Compruebe que el túnel de Secure Shell (SSH) para el FQDN de WB se ha generado en Expressway-C para Expressway-E y que está activo. Vaya a **Estado > Unified Communications > Unified Communications SSH tunnels status**. Debe ver el FQDN del WB y el destino debe ser Expressway-E.

Status System Configuration Applications Users Maintenance

Unified Communications SSH tunnels status You are here: [Status](#) > [Unified Com](#)

Target	Domain	Status
vcs-e.alero.local	webbridge.alero.aca	Active
vcs-e.alero.local	alero.lab	Active
vcs-e.alero.local	alero.local	Active
vcs-e2.alero.local	alero.lab	Active
vcs-e2.alero.local	webbridge.alero.aca	Active
vcs-e2.alero.local	alero.local	Active

Paso 2. Verifique que se ha agregado el servidor TURN al servidor CMS

En el menú CMS API, busque los servidores de turno, y haga clic en cada uno. Dentro de cada objeto, hay un enlace para verificar el estado:

Related objects: [/api/v1/turnServers](#)
[/api/v1/turnServers/266cb509-71fb-4ecc-b600-b93d07d886ff/status](#)

Table view XML view

Object configuration	
serverAddress	10.0.0.36
clientAddress	175.12.5.1
numRegistrations	0
username	cmsturn
useShortTermCredentials	false
type	expressway
tcpPortNumberOverride	3478

La salida muestra información que incluye el tiempo de ida y vuelta (RTT) en milisegundos (Ms) había asociado el servidor de activación. Esta información es importante para la selección de CB de que use el servidor de Active mejor.

Paso 3. Verificación del uso de TURN Relay durante una llamada en curso

En el momento en que se realiza una llamada en directo con el uso del cliente WebRTC, puede ver el estado de activación de retransmisión de medios en Expressway. Navegue hasta **Estado > Uso de retransmisión de activación**, luego elija **ver**.

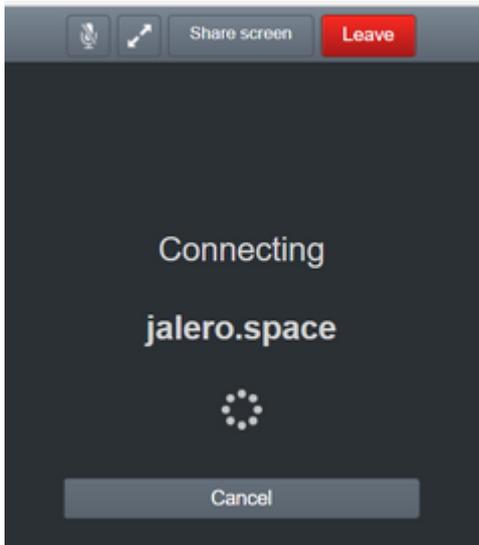
Troubleshoot

Herramientas útiles:

- Archivo HAR de los navegadores ([Cómo generar un archivo HAR en Chrome o Firefox](#))
- Volcado interno de WebRTC desde el explorador - chrome://webrtc-internals o edge://webrtc-internals - Crear volcado tan pronto como se intente Unir.
- Los registros de la consola del navegador también pueden ser útiles.
- Captura de Wireshark del cliente, Exp E, Exp C y CMS.
- Los debugs de Exp E network.http.trafficserver ayudan con la resolución de problemas de websocket.

Se conecta el cliente WebRTC externo, pero no hay medios (debido a una falla de ICE)

En este escenario, el cliente RTC puede resolver el ID de llamada en jalero.space, pero cuando ingresa su nombre y selecciona **Unirse a llamada**, el cliente muestra **Conectando**, como se muestra en esta imagen:



Después de unos 30 segundos, se redirige a la página WB inicial.

Para resolver problemas, complete estos pasos:

- Wireshark de inicio en el cliente de RTC al intentar una llamada y cuando se produce el error, detener la captura.
- Cuando se produce el problema, compruebe los registros de eventos CMS:

Navegue hasta **Registros > Registros de eventos** en CMS WebAdmin.

- Filtre los rastros de Wireshark con stun. Observe este ejemplo:



En las trazas Wireshark, verá que el cliente envía asignar solicitud con las credenciales configuradas, en el servidor de Expressway-E activar en el puerto 3478:

```
1329    2017-04-15 10:26:42.108282    10.55.157.229    10.48.36.248    STUN    186
    Allocate Request UDP user: expturncreds realm: TANDBERG with nonce
```

El servidor responde con **asignar Error**:

```
1363    2017-04-15 10:26:42.214119    10.48.36.248    10.55.157.229    STUN    254
    Allocate Error Response user: expturncreds with nonce realm: TANDBERG UDP error-code: 431
    (*Unknown error code*) Integrity Check Failure
```

or

```
3965    2017-04-15 10:34:54.277477    10.48.36.248    10.55.157.229    STUN    218
    Allocate Error Response user: expturncreds with nonce realm: TANDBERG UDP error-code: 401
    (Unauthorized) Unauthorized
```

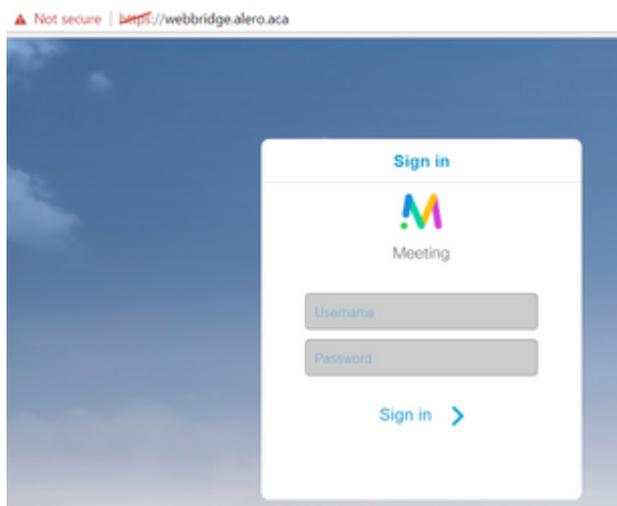
En los registros de CMS, se muestra este mensaje de registro:

```
2017-04-15 10:34:56.536 Warning call 7: ICE failure 4 (unauthorized - check credentials)
```

Solución:

Verifique las credenciales de activación configuradas en el CMS y asegúrese de que coincidan con la que está configurada en la base de datos de autenticación local de Expressway-E.

El cliente WebRTC externo no recibe la opción para unirse a la llamada



En la Callbridge estado > **General página**, se muestra:

```
2017-04-15 12:09:06.647 Web bridge connection to "webbridge.alero.aca" failed (DNS failure)
2017-04-15 12:10:11.634 Warning web bridge link 2: name resolution for "webbridge.alero.aca" fa
2017-04-15 11:55:50.835 Info failed to establish connection to web bridge link 2 (unknown error
```

Solución:

- Asegúrese de que Callbridge puede resolver la URL de unión al FQDN de webbridge (Callbridge no debe resolver esto en la dirección IP de Expressway-E).
- Vaciar la memoria caché de DNS en Callbridge, a través de la interfaz de línea de comandos (CLI), con el comando **dns flush**.
- Asegúrese de que el WB confía en el certificado del servidor Callbridge (no en el emisor).

El cliente WebRTC externo se atasca (en la carga de medios) al conectarse a cospace y, a continuación, se redirige a la página inicial de WB

Solución:

- Asegúrese de que CMS puede resolver el registro SRV _xmpp-client en la red interna para el dominio CB y asegúrese de que las conexiones WebRTC funcionen internamente.

- Recopile una captura de Wireshark en el cliente y un registro de diagnóstico que incluya tcpdump en Expressway-E mientras intenta conectarse con el cliente externo:

Navegue hasta **Mantenimiento > Diagnóstico > Registro de diagnóstico** y asegúrese de que **Tomar tcpdump durante el registro** esté marcado, como se muestra en esta imagen, antes de seleccionar **Iniciar nuevo registro**:

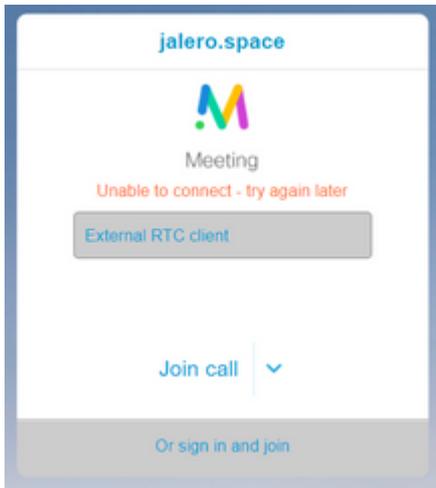


Nota: asegúrese de que la captura de Wireshark en el dispositivo del cliente y el registro en Expressway-E se inician antes de reproducir la llamada que falla. Cuando se ha reproducido la llamada de un fallo, detenga y descargue el inicio de sesión en el Expressway-E y la captura en el cliente.

- Extraiga/descomprima el paquete de registro descargado de Expressway-E y abra el archivo .pcap tomado en la interfaz pública.
- Filtrar en ambas capturas de paquetes con stun:
 - A continuación, busque la solicitud de enlace del cliente externo a la dirección IP pública de Expressway-E, haga clic con el botón secundario y seleccione **Seguir > Secuencia UDP**.
 - Por lo general, el puerto de destino de la solicitud de enlace del cliente estaría en el rango de 24000-29999, que es el rango de puertos de transmisiones TURN en Expressway-E.
- Si no se recibe ninguna respuesta a las solicitudes de enlace en el lado del cliente, compruebe la captura de Expressway-E si llegan las solicitudes.
- Si llegan las solicitudes y el Expressway-E es la respuesta al cliente, compruebe si el firewall externo permite que el tráfico UDP saliente.
- Si las solicitudes no llegan, verifique el FW para asegurarse de que el rango de puertos previamente listado no esté bloqueado.
- Si Expressway-E se implementa con un controlador de interfaz de red dual (DUAL-NIC) con el modo NAT estático habilitado y es X12.5.2 o anterior, asegúrese de que la reflexión NAT sea compatible y esté configurada en el firmware externo. A partir de X12.5.3 esto ya no es necesario para un Expressway independiente.

El cliente WebRTC externo no se puede unir a cospace y recibe una advertencia (no se puede conectar: vuelva a intentarlo más tarde)

En este escenario, el cliente RTC puede resolver el ID de llamada en jalero.space, pero cuando ingresa su nombre y selecciona **Unirse a llamada**, la advertencia **No se puede conectar - vuelva a intentarlo más tarde** se muestra inmediatamente:



Solución:

Asegúrese de que CMS, en la red interna, consigue solucionar siempre la _xmpp cliente registro SRV para el dominio CB.

Información Relacionada

- [Guía de uso del puerto de VCS/Expressway IP](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).