

# Proxy de CMS WebRTC de la configuración sobre la autopista

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Pasos para la configuración](#)

[Verificación](#)

[Troubleshooting](#)

[El cliente de WebRTC conecta solamente ningunos media \(debidos HELAR el error\)](#)

[El cliente de WebRTC no consigue se une a la opción de llamada](#)

## Introducción

Este documento describe los pasos para configurar y para resolver problemas Cisco que resuelve el servidor (CMS) WebRTC sobre la autopista.

## Prerrequisitos

### Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Autopista X8.9.2 y arriba
- Servidor 2.1.4 de CMS y arriba
- [traducción de Dirección de Red \(NAT\)](#)
- Traversal usando las retransmisiones alrededor de NAT (VUELTA)
- Utilidades del Traversal de la sesión para el (STUN) NAT
- Domain Name System (DNS)

Prerrequisitos de configuración:

- El móvil y el Acceso Remoto (MRA) se deben habilitar y configurar ya en la autopista, [hacen clic aquí](#) para las guías MRA
- WebBridge (WB) configurado y habilitado en CMS, [hace clic aquí](#) para la guía de configuración
- DÉ VUELTA a la clave de la opción instalada en la autopista-e
- Puerto TCP 443 abierto en el Firewall de Internet público en el IP Address público Autopista-e
- El puerto 3478 (peticiones TCP y UDP de la VUELTA) se abrió en el Firewall de Internet

- público en el IP Address público Autopista-e
- El puerto 3478 (peticiones TCP y UDP de la VUELTA) se abrió en el Firewall de CMS en el IP Address privado Autopista-e (si usted utiliza el NIC dual en la autopista-e)
- Expedientes del externo DNS para el FQDN del WebBridge, resolvable a la dirección IP del público-revestimiento Autopista-e
- Los DN internos registran WB FQDN resolvable a la dirección IP del servidor de CMS
- La reflexión NAT permitida en el firewall externo para el IP Address público Autopista-e, [hace clic aquí](#) por ejemplo la configuración

Nota: Los pares de la autopista que se utiliza para los servicios del invitado del Jabber no se pueden utilizar para los servicios de representación de CMS WebRTC.

## Componentes Utilizados

Este documento no se restringe a las versiones de software y hardware específicas, no obstante los requisitos de la versión mínima de software deben ser cumplidos.

- Interfaz de programación de aplicaciones (API) de CMS
- Cartero (cliente API)
- Autopista
- Servidor de 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 su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

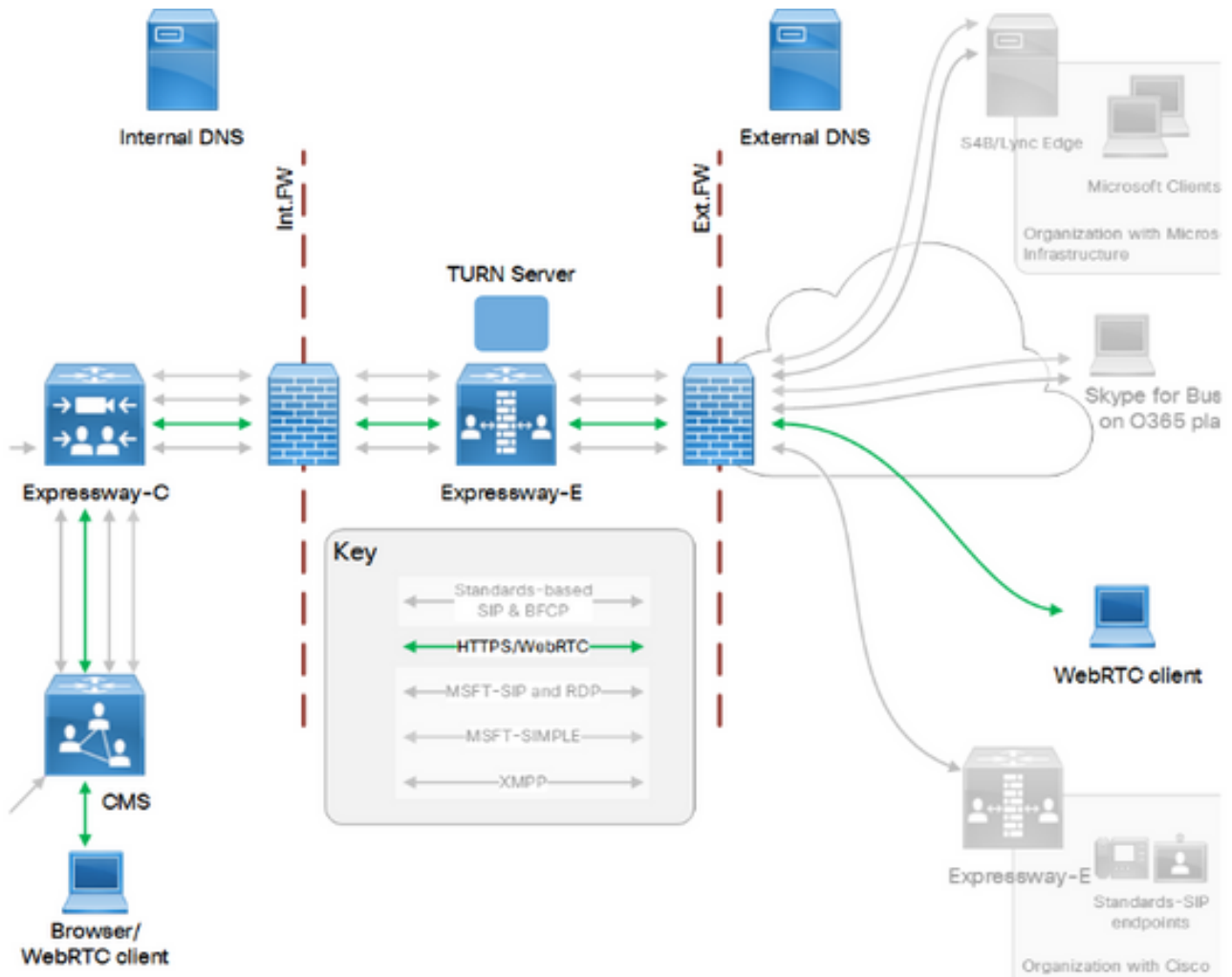
## Antecedentes

El Soporte de proxy de WebRTC se ha agregado a la autopista de la versión X8.9.2, que permite a los usuarios fuera del local para hojear a Cisco que resuelve el Bridge de la red del servidor.

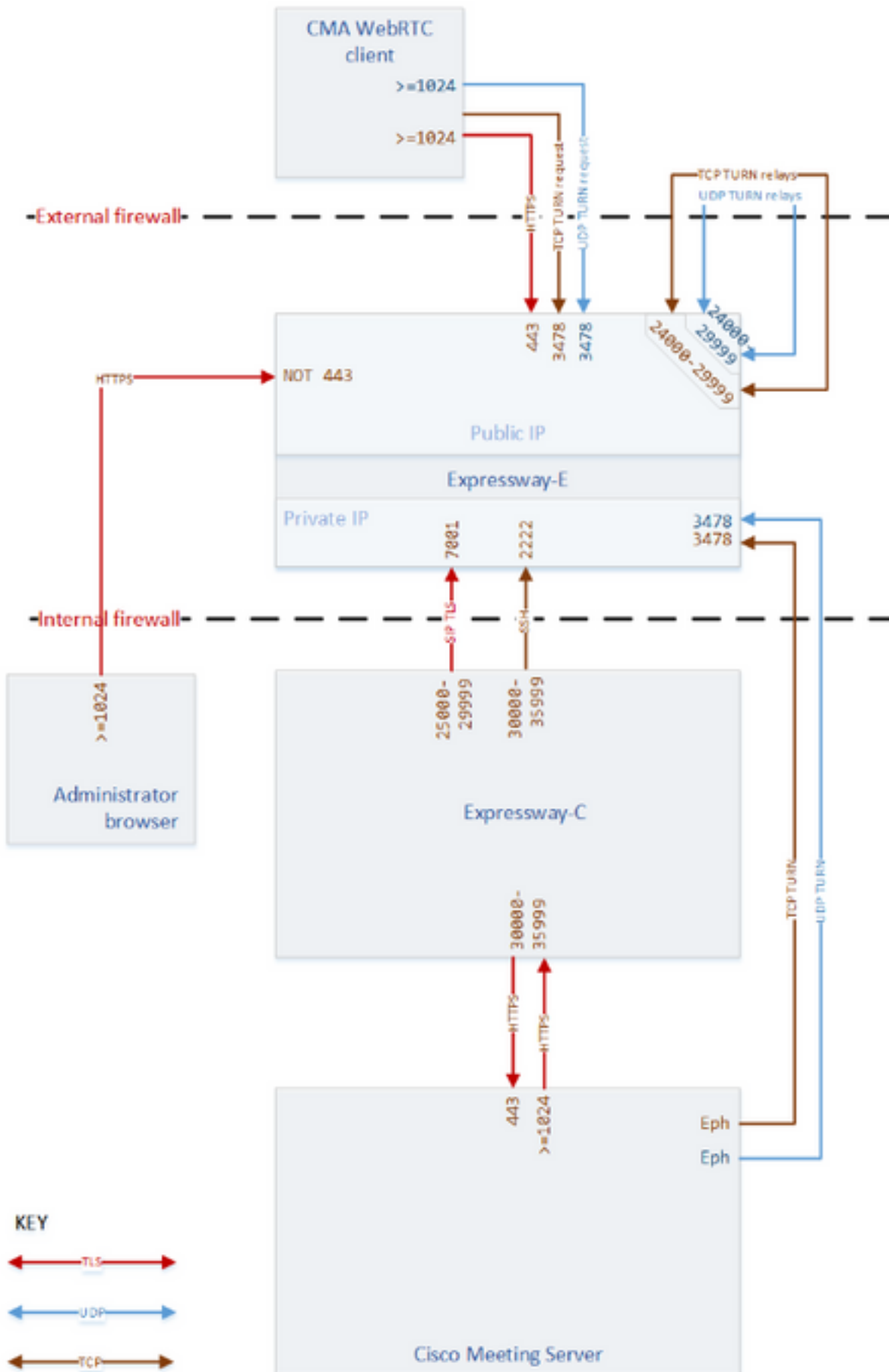
Los clientes externos y los invitados pueden manejar o unirse a los espacios sin la necesidad de cualquier software con excepción de un buscador admitido. [Haga clic aquí](#) para una lista de buscadores admitidos.

## Configurar

### Diagrama de la red



La imagen siguiente proporciona un ejemplo de las conexiones fluye de Web Proxy (Proxy Web) para CMS WebRTC:



Nota: Usted debe configurar su firewall externo para permitir la reflexión NAT para el IP address público de la autopista-e (de los Firewall los paquetes de la desconfianza típicamente que tienen el mismo IP address de la fuente y del destino).

## Pasos para la configuración

Paso 1. Integre el WB de CMS sobre la autopista-C.

a. Navegue a la **configuración > comunicación unificada > Cisco que resuelve el servidor**

b. Habilite el **servidor de la reunión Web Proxy (Proxy Web)**

c. Ingrese el FQDN del WB en el campo del **cliente URI de la cuenta del invitado**

d. Haga clic en la **salvaguardia**

e. Agregue el FQDN del WB sobre el certificado de servidor de la autopista-e como nombre alternativo sujeto (SAN), [haga clic aquí](#) para la guía del certificado de la autopista.

Nota: **El cliente URI de la cuenta de invitado** debe estar según lo configurado en el servidor WebAdmin (interfaz GUI de CMS de la red) sin el prefijo de **https://**.

The screenshot shows the Cisco Meeting Server configuration page. The navigation tabs at the top are Status, System, Configuration (selected), Applications, Users, and Maintenance. The main heading is 'Cisco Meeting Server'. Below it, there's a sub-heading 'Meeting Server configuration'. Under this, there's a section for 'Meeting Server Web Proxy' with a dropdown menu set to 'Enable' and an information icon. Below that, the 'Guest account client URI' field is highlighted with a red border and contains the text 'webbridge.alero.aca'. At the bottom left, there is a 'Save' button.

Paso 2. Habilite GIRAN la autopista-e y agregan el credencial de autenticación a la base de datos de autenticación local.

a. Navegue a la **configuración > al Traversal > a la VUELTA**

b. Habilite los servicios de la VUELTA, de **apagado a encendido**

c. Seleccione las **credenciales del cliente de la VUELTA de la configuración en la base de datos local** y agregue las credenciales (el nombre de usuario y contraseña)

Nota: Si usted tiene un cluster de la autopista-e y son todas que se utilizarán como servidores de la VUELTA, después asegure para habilitarlo en todos los Nodos.

Paso 3. Cambie el puerto de la administración de la autopista-e (opcional).

a. Navegue al **sistema > a la administración**

b. Bajo **configuración del servidor Web**, cambie el **puerto del administrador de la Web a 445** de las opciones del descenso-abajo, después seleccione la **salvaguardia**

c. Relance los pasos **3a a 3b** en toda la autopista-e usada para los servicios de representación de WebRTC

Nota: Cisco recomienda la administración que se cambie el puerto porque el uso 443 de los clientes de WebRTC. Si el navegador de WebRTC intenta al puerto de acceso 80, la autopista-e reorienta la conexión a 443.

Paso 4. Agregue la autopista-e como servidores de la VUELTA para el traversal de los media NAT sobre el servidor de CMS.

a. Descargue y instale al cartero

de; <https://chrome.google.com/webstore/detail/postman/fhbjgbiflinjbdgggehcdcbncdddomop?hl=en>

b. Ingrese el acceso URL API en la barra de dirección, por ejemplo; [https://<Callbridge\\_fqdn>:445/api/v1/<entity>](https://<Callbridge_fqdn>:445/api/v1/<entity>)

c. Envíe un POSTE con [https://<Callbridge\\_fqdn>:445/api/v1/turnservers](https://<Callbridge_fqdn>:445/api/v1/turnservers), después de que usted agregue estos campos en el cuerpo:

- **serverAddress:** (IP Address privado de la autopista)
- **clientAddress:** (IP Address público de la autopista)
- **tipo:** (autopista)
- nombre de usuario: (como está configurado en el paso **2c**)
- **contraseña:** (como está configurado en el paso **2c**)
- **tcpPortNumberOverride:** 3478

d. Relance el paso **4c** para que cada servidor de la autopista-e sea utilizado para la VUELTA

Las imágenes siguientes proporcionan los ejemplos de los pasos basados en la configuración:

The screenshot shows the Postman interface for a POST request. The URL is `https://core1.cluster.alero.aca:445/api/v1/turnServers`. The request body is set to `x-www-form-urlencoded` and contains the following data:

Key	Value
<input checked="" type="checkbox"/> serverAddress	10.48.36.248
<input checked="" type="checkbox"/> clientAddress	175.6.7.8
<input checked="" type="checkbox"/> type	expressway
<input checked="" type="checkbox"/> username	expturncreds
<input checked="" type="checkbox"/> password	cisco
<input checked="" type="checkbox"/> tcpPortNumberOverride	3478

POST  Params

Authorization Headers (2) **Body** Pre-request Script Tests

form-data  x-www-form-urlencoded  raw  binary

Key	Value
<input checked="" type="checkbox"/> serverAddress	10.48.79.129
<input checked="" type="checkbox"/> clientAddress	175.6.7.9
<input checked="" type="checkbox"/> type	expressway
<input checked="" type="checkbox"/> username	expturncreds
<input checked="" type="checkbox"/> password	cisco
<input checked="" type="checkbox"/> tcpPortNumberOverride	3478

## Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Paso 1. En la autopista-C, control que el WB está integrado correctamente.

a. Navegue a la **configuración > comunicación unificada > Cisco que resuelve el servidor**, y usted 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  ⓘ

Guest account client URI  ⓘ

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

b. Navegue a la **configuración > comunicación unificada > HTTP permiten la lista > las reglas automáticamente agregadas**, control que esto 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 que encuentre el WB en los Nodos descubiertos porque las reglas son simplemente tener en cuenta el proxy del tráfico HTTPS al WB, y no necesariamente para la comunicación unificada.

c. Marque que el túnel del Secure Shell (SSH) para el WB FQDN se ha empleado la autopista-C a

la autopista-e y que es activo. Navegue **estatus de los túneles a SSH del estatus > de las Comunicaciones unificadas > de las Comunicaciones unificadas**, usted debe ver que el FQDN del WB y de la blanco debe ser la autopista-e:

Target	Domain	Status	Peer
vcs-e.alero.local	webbridge.alero.aca	Active	10.48.36.247
vcs-e.alero.local	alero.lab	Active	10.48.36.247
vcs-e.alero.local	alero.local	Active	10.48.36.247
vcs-e2.alero.local	alero.lab	Active	10.48.36.247
vcs-e2.alero.local	webbridge.alero.aca	Active	10.48.36.247
vcs-e2.alero.local	alero.local	Active	10.48.36.247

Paso 2. Verifique que el servidor de la VUELTA se haya agregado al servidor de CMS.

a. En el WebUI, si usted utiliza un solo servidor de la autopista, navegue a los **registros > a los registros de acontecimientos**, la salida muestra el dirección IP del servidor de la VUELTA, como en el ejemplo:

```
2017-04-15 09:37:26.864 Info TURN server 7: starting up "10.48.36.248" (configured object 6508065f-298f-4146-8697-4b7087279de3)
```

b. Si usted utiliza los servidores múltiples de la VUELTA de la autopista, envíe una **petición get** con un cliente API con este comando:

```
https://<Callbridge_IP>:445/api/v1/turnservers
```

Nota: Este comando puede también ser utilizado si usted tiene un solo servidor de la VUELTA de la autopista.

La salida, en el caso de los servidores múltiples de la VUELTA de la autopista, es similar a ésta en este ejemplo:

```
<?xml version="1.0"?>
<turnServers total="2">
  <turnServer id="20efbd08-c08d-4893-8f7e-698d1c8ca7f9">
    <serverAddress>10.48.79.129</serverAddress>
    <clientAddress>175.6.7.9</clientAddress>
  </turnServer>
  <turnServer id="61ae465d-fe30-440e-b20a-8f75e8fb9b85">
    <serverAddress>10.48.36.248</serverAddress>
    <clientAddress>175.6.7.8</clientAddress>
  </turnServer>
</turnServers>
```

c. En el WebAdmin, navegue a **https://<Callbridge\_FQDN>:445/turn\_debug.html**

La salida visualiza el Round-Trip Time (RTT) asociado a cada servidor de la VUELTA. Esta información es importante para la selección CB del mejor servidor de la VUELTA utilizar.

Solo servidor de la VUELTA de la autopista del ejemplo:

```
Configured TURN / Edge servers: 1
eef94a2b-3bfa-40f7-b83c-ece8df424e15: 10.48.36.248:3478 (turn=1, edge=0, acano=0)
```

```
10.48.36.5 TURN chooser, local port number 56425
```



```
eef94a2b-3bfa-40f7-b83c-ece8df424e15 (10.48.36.248:3478), results: 1
0: server address 10.48.36.248:3478, reachable for 156s, mapped address 10.48.36.5:56425,
RTT 44ms
best : eef94a2b-3bfa-40f7-b83c-ece8df424e15, server address 10.48.36.248:3478, reachable for
156s, mapped address 10.48.36.5:56425, RTT 44ms
best (not msEdge): eef94a2b-3bfa-40f7-b83c-ece8df424e15, server address 10.48.36.248:3478,
reachable for 156s, mapped address 10.48.36.5:56425, RTT 44ms
no best result (msEdge) returned
```

### Ejemplo de los servidores múltiples de la VUELTA de la autopista:

```
Configured TURN / Edge servers: 2
eef94a2b-3bfa-40f7-b83c-ece8df424e15: 10.48.36.248:3478 (turn=1,edge=0,acano=0)
7eecf3eb-49f2-4963-bf67-2bac98355ca1: 10.48.79.129:3478 (turn=1,edge=0,acano=0)

10.48.36.5 TURN chooser, local port number 56425
eef94a2b-3bfa-40f7-b83c-ece8df424e15 (10.48.36.248:3478), results: 1
0: server address 10.48.36.248:3478, reachable for 283s, mapped address 10.48.36.5:56425,
RTT 52ms
7eecf3eb-49f2-4963-bf67-2bac98355ca1 (10.48.79.129:3478), results: 1
0: server address 10.48.79.129:3478, reachable for 64s, mapped address 10.48.36.5:56425, RTT
64ms
best : eef94a2b-3bfa-40f7-b83c-ece8df424e15, server address 10.48.36.248:3478, reachable for
283s, mapped address 10.48.36.5:56425, RTT 52ms
best (not msEdge): eef94a2b-3bfa-40f7-b83c-ece8df424e15, server address 10.48.36.248:3478,
reachable for 283s, mapped address 10.48.36.5:56425, RTT 52ms
no best result (msEdge) returned
```

Paso 3. A la hora de una llamada viva que se haga con el uso del cliente de WebRTC, usted puede ver el estatus de la retransmisión de los media de la VUELTA en la autopista. Navegue al uso de la retransmisión del estatus > de la VUELTA, después seleccione la visión.

## Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración, algunos problemas de WebRTC y fallas posibles típicos.

Los registros para las conexiones WB y el seguimiento DNS se pueden habilitar en el WebAdmin del servidor de CMS:

a. Conecte con el **WebAdmin**

b. Navegue a los **registros > detalló el seguimiento**

c. Habilite el **seguimiento de la conexión en Bridge de la red** y el **seguimiento DNS** para la duración deseada:

The screenshot shows two configuration panels. The top panel is titled "Web Bridge connection tracing" and shows "Web Bridge connection tracing status" as "Enabled for 8 minutes, 37 seconds longer". Below this are five buttons: "Enable for 1 minute", "Enable for 10 minutes", "Enable for 30 minutes", "Enable for 24 hours", and "Disable". The bottom panel is titled "DNS tracing" and shows "DNS logging status" as "Enabled for 8 minutes, 41 seconds longer". Below this are five buttons: "Enable for 1 minute", "Enable for 10 minutes", "Enable for 30 minutes", "Enable for 24 hours", and "Disable".

El registro de debug de la consola de Chrome y de Firefox se puede utilizar para resolver problemas los errores de la conexión cliente de WebRTC, tales como problemas con los media y

la Conectividad al WB. Esto se puede hacer visible con el uso de la combinación **Ctrl+Shift+C.** del teclado.

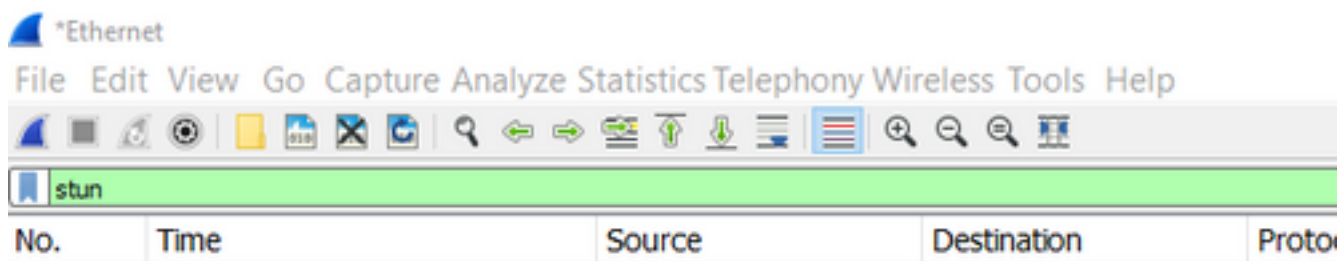
En Chrome, utilice **chrome://webrtc-internals/** o **alrededor: webrtc** en Firefox, en una lengüeta separada a la hora de una llamada viva para visualizar los diagnósticos avanzados, que es útil para resolver problemas de los media con WebRTC.

La captura de paquetes de Wireshark en el cliente de WebRTC también proporciona una cierta información útil sobre la retransmisión de los media con el servidor de la VUELTA.

## El cliente de WebRTC conecta solamente ningunos media (debidos HELAR el error)

Comience el Wireshark cuando usted intenta a una llamada y cuando ocurre el error, para la captura.

Filtre las trazas con **aturden**, ven el ejemplo:



En las trazas de Wireshark, usted ve que el cliente envía **afecta un aparato la petición** con las credenciales configuradas, al servidor de la VUELTA 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 contesta con **afecta un aparato el 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
```

O

```
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
```

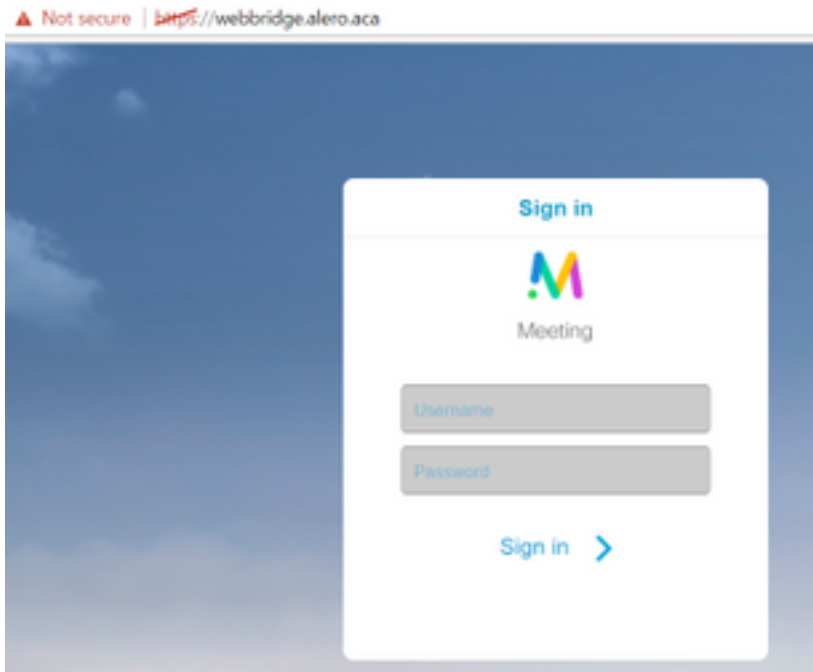
En los registros de CMS, el mensaje del registro abajo se muestra:

```
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
```

Solución:

Marque las credenciales de la VUELTA configuradas en el servidor de CMS y asegúrese de que hace juego eso configurada en la base de datos de autenticación local de la autopista-e.

El cliente de WebRTC no consigue se une a la opción de llamada



En el **estatus de Callbridge >** se visualiza la página **general**, esto:

```
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
```

Solución:

- Asegúrese de que el Callbridge pueda resolver el WB FQDN al IP Address interno (el Callbridge no debe resolver esto a la dirección IP Autopista-e)
- Vacie el caché DNS en el Callbridge, vía el comando line interface(cli), con el **rubor dns del comando**
- Asegúrese de que el WB confíe en el certificado de servidor de Callbridge (no el emisor)