# Guía óptima del Troubleshooting de la selección de gateway de AnyConnect

## Contenido

[Introducción](#)
[¿Cómo OGS trabaja?](#)
[Caché OGS](#)
[Determinación de la ubicación](#)
[Escenarios de falla](#)
[Cuando la Conectividad al gateway se pierde](#)
[Curriculum vitae después de un suspender](#)
[El tamaño de la ventana TCP Retrasar-ACK selecciona el gateway incorrecto](#)
[Ejemplo del usuario típico](#)
[Troubleshooting OGS](#)
[Paso 1. Borre el caché OGS para forzar una nueva evaluación](#)
[Paso 2. Capture las sondas del servidor durante el intento de conexión](#)
[Paso 3. Verifique el gateway seleccionado por OGS](#)
[Paso 4. Valide los cálculos OGS ejecutados por AnyConnect](#)
[Análisis](#)
[Q&A](#)

## Introducción

Este documento describe cómo resolver problemas los problemas con la selección de gateway óptima (OGS). OGS es una característica que se puede utilizar para determinar qué gateway tiene el Round Trip Time más bajo (RTT) y conectar con ese gateway. Uno puede utilizar la característica OGS para minimizar el tiempo de espera para el tráfico de Internet sin la intervención del usuario. Con OGS, el Cliente de movilidad Cisco AnyConnect Secure (AnyConnect) identifica y selecciona que aseguren el gateway sean los mejores para la conexión o la reconexión. OGS comienza sobre la primera conexión o sobre una reconexión por lo menos cuatro horas después de la desconexión anterior. Más información se puede encontrar en la guía de administrador.

> **Tip**: OGS trabaja mejor con el último cliente de AnyConnect y la versión de software ASA 9.1(3) * o más adelante.

## ¿Cómo OGS trabaja?

**Un pedido de ping** simple del Internet Control Message Protocol (ICMP) no trabaja porque muchos Firewall adaptantes del dispositivo de seguridad de Cisco (ASA) se configuran para bloquear los paquetes icmp para prevenir la detección. En lugar, el cliente envía tres peticiones HTTP/443 a cada headend que aparece en una **fusión de** todos los perfiles. Se refieren estas sondas HTTP mientras que OGS hace ping en los registros, pero, según lo explicado anterior, él

no es ping de ICMP. Para asegurarse de que la conexión a (con referencia a) no dure demasiado, OGS selecciona el gateway anterior por abandono si no recibe ninguna resultados del ping OGS en el plazo de siete segundos. (Busque los **resultados del ping OGS** en el registro.)

> **Note**: AnyConnect debe enviar un pedido de HTTP a 443, porque la respuesta sí mismo es importante, no una respuesta acertada. Desafortunadamente, el arreglo para la dirección del proxy envía todas las peticiones como HTTPS. Vea el Id. de bug Cisco CSCtg38672 - OGS debe hacer ping con los pedidos de HTTP.

> **Note**: Si no hay headends en el caché, AnyConnect primero envía un pedido de HTTP para determinar si hay un Proxy de autenticación, y si puede manejar la petición. Es sólo después de esta Solicitud inicial que comienza los ping OGS para sondar el servidor.

- OGS determina la ubicación del usuario basada en la información de red, tal como el sufijo del Domain Name System (DNS) y el IP Address del servidor DNS. Los resultados RTT, junto con esta ubicación, se salvan en el caché OGS.
- Las entradas de la ubicación OGS se ocultan por 14 días. El Id. de bug Cisco CSCtk66531 fue clasifiado para hacer éstos las configuraciones utilizador configurables.
- OGS no se ejecuta otra vez de esta ubicación hasta 14 días después de que la entrada de la ubicación primero se oculta. Durante este tiempo, utiliza entrada almacenada en caché y los RTT determinados para esa ubicación. Esto significa que cuando AnyConnect comienza otra vez, no realiza OGS otra vez; en lugar, utiliza la orden óptima del gateway en el caché para esa ubicación. En los registros de diagnóstico de la herramienta de informe de AnyConnect (DARDO), se considera este mensaje:

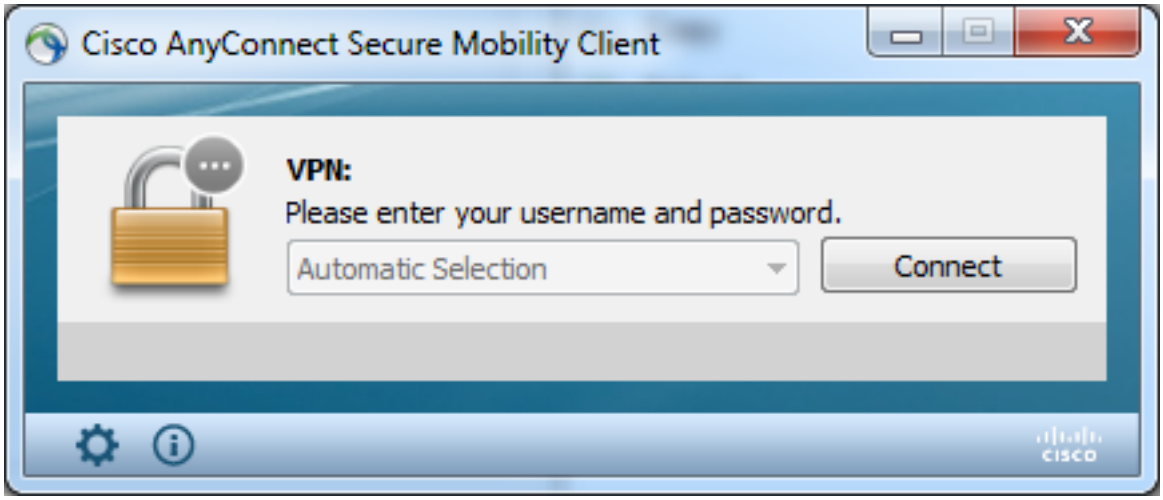
```
****************************************
Date : 10/04/2013
Time : 14:00:44
Type : Information
Source : acvpnui

Description : Function: ClientIfcBase::startAHS
File: .\ClientIfcBase.cpp
Line: 2785
OGS was already performed, previous selection will be used.

****************************************
```

- El RTT se determina con un intercambio TCP al puerto de la capa de socketes seguros (SSL) del gateway con el cual el usuario intentará conectar según lo especificado por la entrada de host en el perfil de AnyConnect.

> **Note**: A diferencia del HTTP-ping, que hace un poste simple HTTP y después visualiza el RTT y el resultado, los cómputos OGS son levemente más complicados. AnyConnect envía tres sondas para cada servidor, y calcula el retardo entre el HTTP SYN que envía y el FIN/ACK para cada uno de estas sondas. Entonces utiliza el más bajo de los deltas para comparar los servidores y hacer su selección. Así pues, aunque los HTTP-ping son una indicación bastante buena cuyo el servidor el AnyConnect elegirá, puede ser que no marquen necesariamente. Hay más información sobre esto en el resto del documento.

- Actualmente, OGS funciona con solamente los controles si el usuario sale de un suspender, y se ha excedido el umbral. OGS no conecta con un diverso ASA si el ASA el usuario está conectado con las caídas o llega a ser inasequible. OGS entra en contacto solamente a los servidores primarios en el perfil para determinar el óptimo.

- Una vez que se descarga el perfil del cliente OGS, cuando el usuario recomienza al cliente de AnyConnect, la opción para seleccionar otros perfiles será grayed hacia fuera como se muestra aquí:




  Incluso si la máquina del usuario tiene múltiplo otros perfiles no podrán seleccionar ningunos de ellos hasta que OGS disbaled.

### Caché OGS

Una vez que se acaba el cálculo, los resultados se salvan en el archivo **preferences_global**. Ha habido problemas con estos datos que no eran salvados en el archivo antes.

Refiera al Id. de bug Cisco CSCtj84626 para más detalles.

### Determinación de la ubicación

OGS que oculta los trabajos sobre una combinación del dominio DNS y de los dirección IP del servidor de los DN individuales. Trabaja como sigue:

- La ubicación A tiene un dominio DNS de **locationa.com**, y dos IP Addresses del servidor DNS - **ip1** e **ip2**. Cada combinación domain/IP crea una clave del caché esas puntas a una entrada de caché OGS. Por ejemplo: **locationa.com|ip1 - > ogscache1locationa.com|ip2 - > ogscache1**
- Si AnyConnect entonces conecta con una red físico-diferente, la misma acumulación de las combinaciones domain/IP se crea y se marca contra la lista ocultada. Si hay algunas coincidencias en absoluto, se utiliza ese valor del caché OGS, y todavía consideran al cliente estar en la **ubicación A.**

## Escenarios de falla

Aquí están algunos escenarios de falla que los usuarios pudieron encontrar:

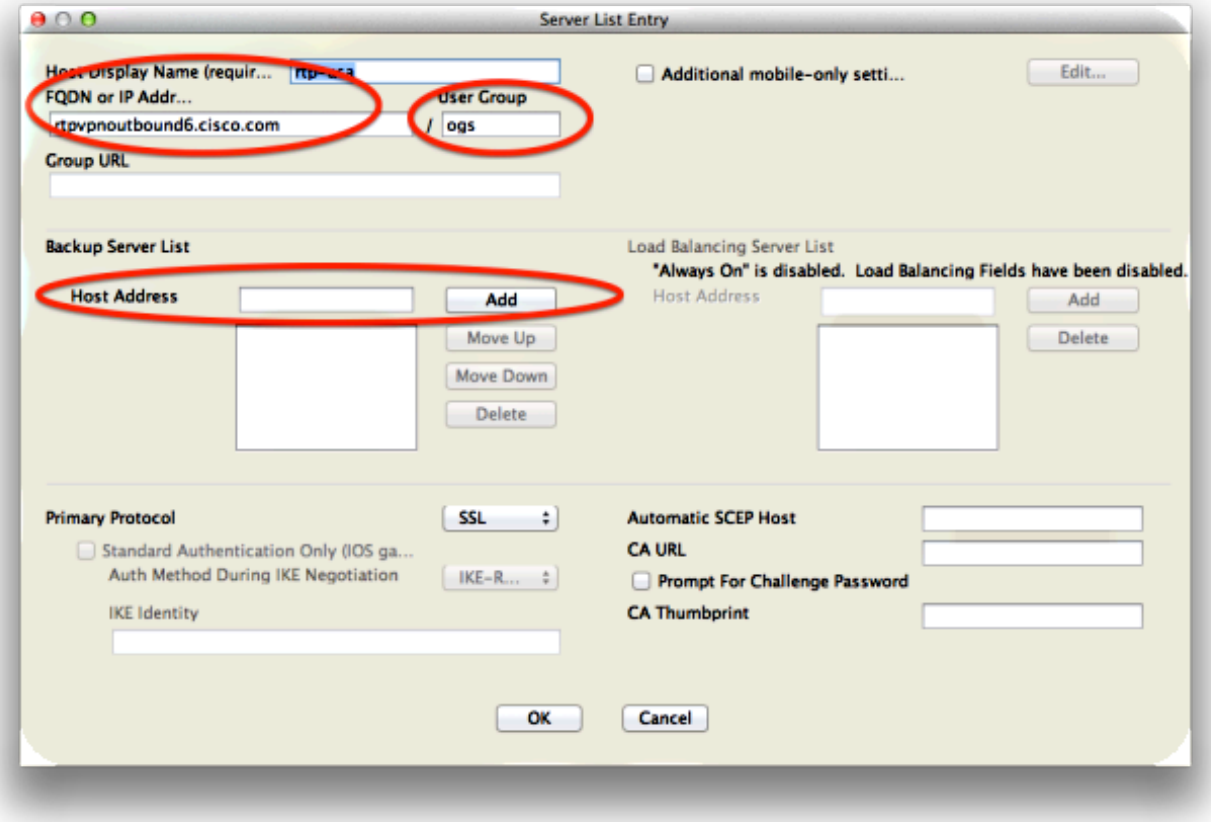
## Cuando la Conectividad al gateway se pierde

Cuando se utiliza OGS, si la Conectividad al gateway con el cual los usuarios están conectados se pierde, después AnyConnect conecta con los servidores en el **listandnot del servidor de backup** con el host siguiente OGS. La orden de funcionamiento es como sigue:

1. OGS entra en contacto solamente a los servidores primarios para determinar el óptimo.

2. Una vez que está determinado, el algoritmo de la conexión es:
   Tentativa de conectar con el servidor óptimo.Si eso falla, intente la lista del servidor de backup del servidor óptimo.Si eso falla, intente cada servidor que permanezca en la lista de la selección OGS, pedido por su selección resulta.

   **Note**: Cuando el administrador configura la lista del servidor de backup, el editor actual del perfil permite solamente que el administrador ingrese el Nombre de dominio totalmente calificado (FQDN) (FQDN) para el servidor de backup, pero no el grupo de usuarios como es posible para el servidor primario:




   El Id. de bug Cisco CSCud84778 se ha clasifiado para corregir esto, pero el URL completo se debe ingresar en el campo de la dirección de host para el servidor de backup, y debe trabajar: **https://*<ip-address>/usergroup***.

## Curriculum vitae después de un suspender

Para que OGS se ejecute después de que un curriculum vitae, AnyConnect deba haber tenido una conexión establecida cuando la máquina fue puesta para dormir. OGS después de que un curriculum vitae se realice solamente después de que ocurra la prueba del entorno de red, que se significa para confirmar que la conectividad de red está disponible. Esta prueba incluye una Conectividad DNS más subtest.

Sin embargo, si los descensos del servidor DNS teclean las peticiones A con una dirección IP en el campo de la interrogación, en comparación con la contestación con el “nombre no encontrado” (el caso más común, encontrado siempre durante las pruebas), después el Id. de bug Cisco CSCti20768 “interrogación DNS del tipo A para la dirección IP, debe estar la PTR para evitar el descanso” se aplica.

## El tamaño de la ventana TCP Retrasar-ACK selecciona el gateway incorrecto

Cuando las Versiones de ASA que la versión 9.1(3) se utilizan anterior, las capturas en el cliente muestran un retardo persistente en el contacto SSL. Se nota qué es que el cliente envía su ClientHello, después el ASA envía su ServerHello. Esto es seguida normalmente por un mensaje del certificado (pedido de certificado opcional) y el mensaje de ServerHelloDone. La anomalía es doble:

1. El ASA no envía inmediatamente el mensaje del certificado después del ServerHello. El tamaño de la ventana del cliente es 64,860 bytes, que es más que suficiente llevar a cabo la respuesta entera del ASA.

2. El cliente no hace ACK el ServerHello inmediatamente, así que el ASA retransmite el ServerHello después de ~120ms, momento en el cual el cliente ACK los datos. Entonces el mensaje del certificado se envía. Casi está como si el cliente espera más datos.

Esto sucede debido a la interacción entre el lento-principio y TCP RETRASAR-ACK TCP. Antes de la Versión de ASA 9.1(3), el ASA utiliza un tamaño de la ventana del lento-principio de 1, mientras que el cliente de Windows utiliza un valor retrasar-ACK de 2. Esto significa que el ASA envía solamente un paquete de datos hasta que consiga un ACK, pero también significa que el cliente no envía un ACK hasta que reciba dos paquetes de datos. Los tiempos ASA hacia fuera después de que 120ms y retransmite el ServerHello, después de lo cual el cliente ACK los datos y la conexión continúa. Este comportamiento fue cambiado por el Id. de bug Cisco CSCug98113 de modo que el ASA utilice un tamaño de la ventana lento del comienzo de 2 por abandono en vez de 1.

Esto puede afectar el cálculo OGS cuando:

- Diversos gatewayes funcionan con diversas Versiones de ASA.
- Los clientes tienen diversos tamaños de la ventana retrasar-ACK.

En tales situaciones, el retardo introducido por el retrasar-ACK podía ser suficiente hacer al cliente seleccionar el ASA incorrecto. Si este valor diferencia entre el cliente y el ASA, podría todavía haber problemas. En tales situaciones, la solución alternativa es ajustar el tamaño de la ventana retrasado de los acuses de recibo.

**Windows:**

1. Comience el **Editor de registro**.

2. Identifique el GUID de la interfaz en la cual usted quiere inhabilitar el retrasar-ACK. Para hacer esto, navegue a:
   **HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows NT > CurrentVersion > NetworkCards > (número).**
   Mire cada número enumerado bajo NetworkCards. En el Lado derecho, la descripción debe enumerar la interfaz (por ejemplo, Intel (R) link inalámbrico 5100AGN de WiFi) y el ServiceName deben enumerar el GUID correspondiente.

3. Localice y después haga clic este subkey del registro:
   **HKEY_LOCAL_MACHINE \ SISTEMA \ CurrentControlSet \ servicios \ Tcpip \ parámetros **

**interfaces \ <Interface GUID>**

4. En el menú Edición, la punta a nuevo, y entonces hace clic el **valor DWORD**.
5. Nombre el nuevo valor **TcpAckFrequency**, y asígnele un valor de **1.**
6. Salga el Editor de registro.
7. Recomience Windows para que este cambio tome el efecto.

**Note**: El Id. de bug Cisco CSCum19065 se ha clasifiado para hacer los Parámetros de ajuste TCP configurables en el ASA.

# Ejemplo del usuario típico

El caso más de uso común es cuando un usuario en casa ejecuta OGS la primera vez, él registra las configuraciones DNS y los resultados del ping OGS en el caché (valores por defecto a un descanso del 14-día). Cuando el usuario vuelve a casa la tarde próxima, OGS detecta las mismas configuraciones DNS, las encuentra en el caché, y salta la prueba de ping OGS. Más adelante, cuando el usuario va a un hotel o a un restaurante que ofrezca el servicio de Internet, OGS detecta diversas configuraciones DNS, funciona con las pruebas de ping OGS, selecciona el mejor gateway, y registra los resultados en el caché.

El proceso es idéntico cuando reanuda de un estado suspendido o hibernado, si las configuraciones del curriculum vitae OGS y de AnyConnect permiten él.

# Troubleshooting OGS

## Paso 1. Borre el caché OGS para forzar una nueva evaluación

Para borrar los OGS ocultan y evalúan de nuevo el RTT para los gatewayes disponibles, borran simplemente las preferencias globales de AnyConnect clasifían del PC. La ubicación del archivo varía basado en el operating system (OS):

- Windows Vista y Windows 7

```
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\preferences_global.xml
Note: in older client versions it used to be stored in C:\ProgramData\Cisco\Cisco
AnyConnect VPN Client
```

- Windows XP

```
C:\Documents and Settings\AllUsers\Application Data\Cisco\Cisco AnyConnect VPN
Client\preferences_global.xml
```

- Mac OS X

```
/opt/cisco/anyconnect/.anyconnect_global
Note: with older versions of the client it used to be /opt/cisco/vpn..
```

- Linux

```
/opt/cisco/anyconnect/.anyconnect_global
Note: with older versions of the client it used to be /opt/cisco/vpn..
```

## Paso 2. Capture las sondas del servidor durante el intento de conexión

1. Comience Wireshark en la máquina de la prueba.

2. Comience un intento de conexión en AnyConnect.

3. Pare la captura de Wireshark una vez que la conexión es completa. **Tip**: Puesto que la captura se utiliza solamente para probar OGS, es el mejor parar la captura tan pronto como AnyConnect seleccione un gateway. Es el mejor no pasar con un intento de conexión completo, porque ése puede nublarse a la captura de paquetes.

## Paso 3. Verifique el gateway seleccionado por OGS

Para verificar porqué OGS seleccionó un gateway determinado, complete estos pasos:

1. Inicie una nueva conexión.

2. Ejecute el DARDO de AnyConnect:
   Inicie **AnyConnect**, y haga clic **avanzado**.Haga clic los **diagnósticos**.Haga clic en Next (Siguiente).Haga clic en Next (Siguiente).
3. Examine los resultados del DARDO encontrados en el **archivo** creado recientemente en el escritorio.
   Navegue al **Cliente de movilidad Cisco AnyConnect Secure > a AnyConnect.txt**.

   Observe el tiempo que las sondas OGS comenzaron para un servidor determinado de este registro del DARDO:

```
****************************************

Date : 10/04/2013
Time : 14:21:27
Type : Information
Source : acvpnui

Description : Function: CHeadendSelection::CSelectionThread::Run
File: .\AHS\HeadendSelection.cpp
Line: 928
OGS starting thread named gw2.cisco.com

****************************************
```

   Generalmente deben estar aproximadamente al mismo tiempo, pero en caso de que las capturas sean grandes, las ayudas del sello de fecha/hora se estrechan abajo que los paquetes son las sondas HTTP y cuáles son los intentos de conexión reales.

   Una vez que AnyConnect envía tres sondas al servidor, este mensaje se genera con los resultados para cada uno de las sondas:

```
****************************************

Date : 10/04/2013
Time : 14:31:37
```

```
Type : Information
Source : acvpnui

Description : Function: CHeadendSelection::CSelectionThread::logThreadPingResults
File: .\AHS\HeadendSelection.cpp
Line: 1137
OGS ping results for gw2.cisco.com: (219 218 132 )

****************************************
```

Es importante prestar la atención a estos tres valores, porque deben hacer juego los resultados de la captura.

Busque el mensaje que contiene “el *** de los resultados de la selección del *** OGS” para considerar el RTT evaluado, y si el intento de conexión más reciente era el resultado de un RTT ocultado o de un nuevo cálculo.

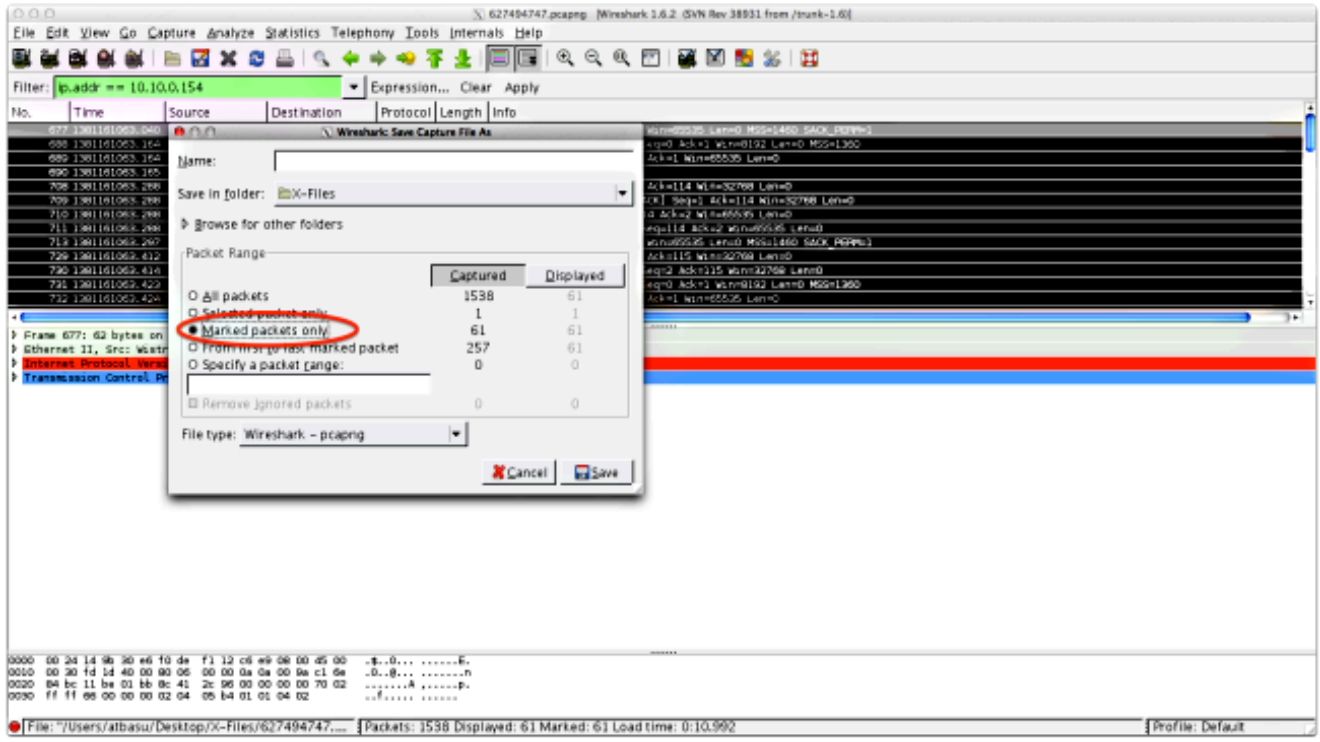
Aquí tiene un ejemplo:

```
****************************************

Date        : 10/04/2013
Time        : 12:29:38
Type        : Information
Source      : vpnui

Description : Function: CHeadendSelection::logPingResults
File: .\AHS\HeadendSelection.cpp
Line: 589
*** OGS Selection Results ***
OGS performed for connection attempt. Last server: 'gw2.cisco.com'

Results obtained from OGS cache. No ping tests were performed.

Server Address     RTT (ms)
gw1.cisco.com     302
gw2.cisco.com     132 <========= As seen, 132 was the lowest delay
of the three probes from the previous DART log
gw3.cisco.com     506
gw4.cisco.com     877


Selected 'gw2.cisco.com' as the optimal server.

****************************************
```

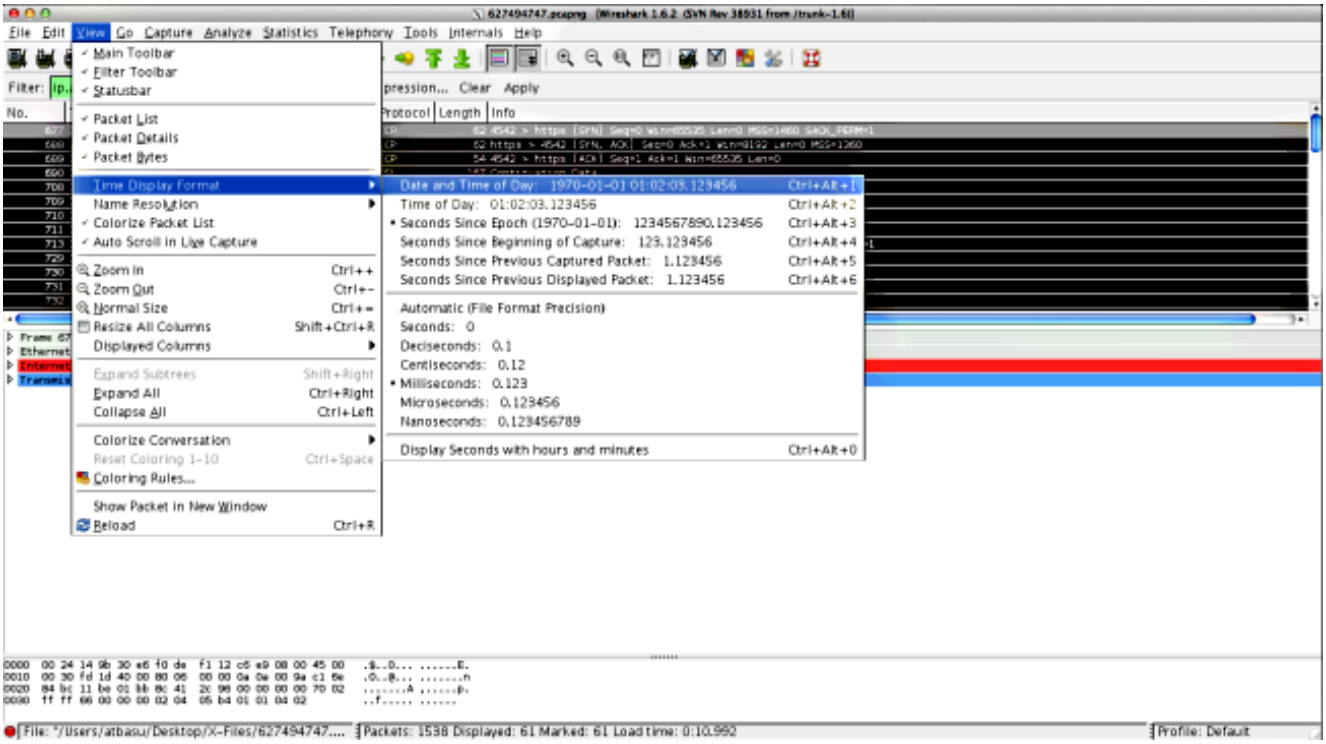
## Paso 4. Valide los cálculos OGS ejecutados por AnyConnect

Examine la captura para saber si hay el TCP/SSL sonda utilizado para calcular el RTT. Vea cuánto tiempo la petición HTTPS asume el control una sola conexión TCP. Cada petición de la sonda debe utilizar una diversa conexión TCP. Para hacer esto, abra la captura en Wireshark, y relance estos pasos para cada uno de los servidores:

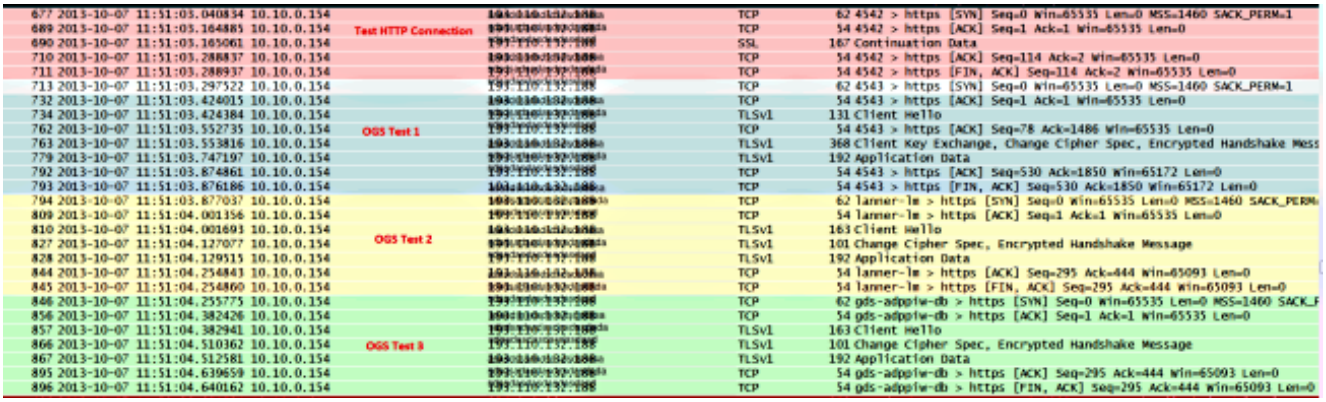
1. Utilice el **filtro ip.addr** para aislar los paquetes enviados a cada uno de los servidores en su propia captura. Para hacer esto, navegar para editar**,** y MarkAll selecto **visualizó los paquetes. Después** navegue al File (Archivo) **>** Save as (Guardar como)**, seleccione la opción de** Markedpackets **solamente**, y haga clic la salvaguardia**:**



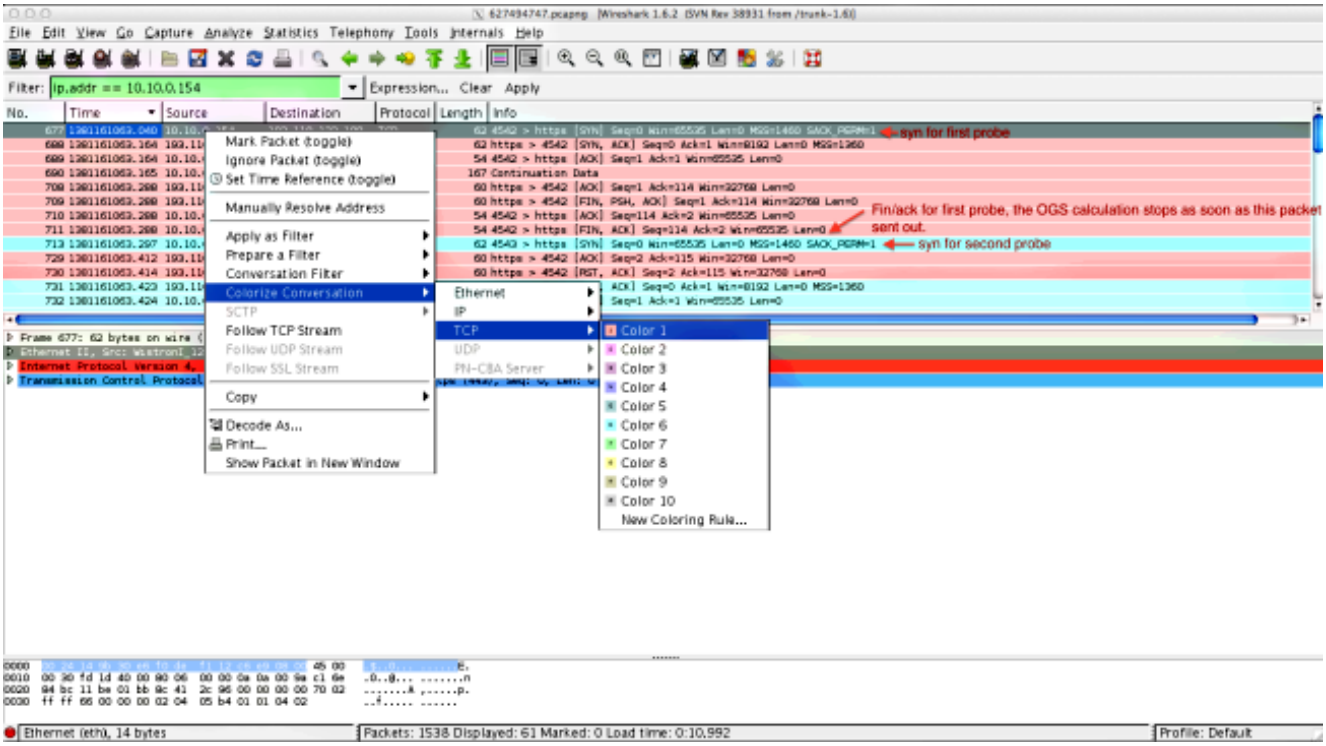

2. En esta nueva captura, navegue **para ver > formato de visualización > fecha y Time Of Day del tiempo**:




3. Identifique el primer paquete SYN HTTP en esta captura que fue enviada cuando la sonda OGS fue enviada basada en los registros del DARDO según lo identificado en el paso 3.3.2. Es importante recordar que, para el primer servidor, el primer pedido de HTTP no es una sonda del servidor. Es fácil confundir la primera petición desde una sonda del servidor, y llega así los valores totalmente diferentes de qué OGS señala. Este problema se resalta aquí:

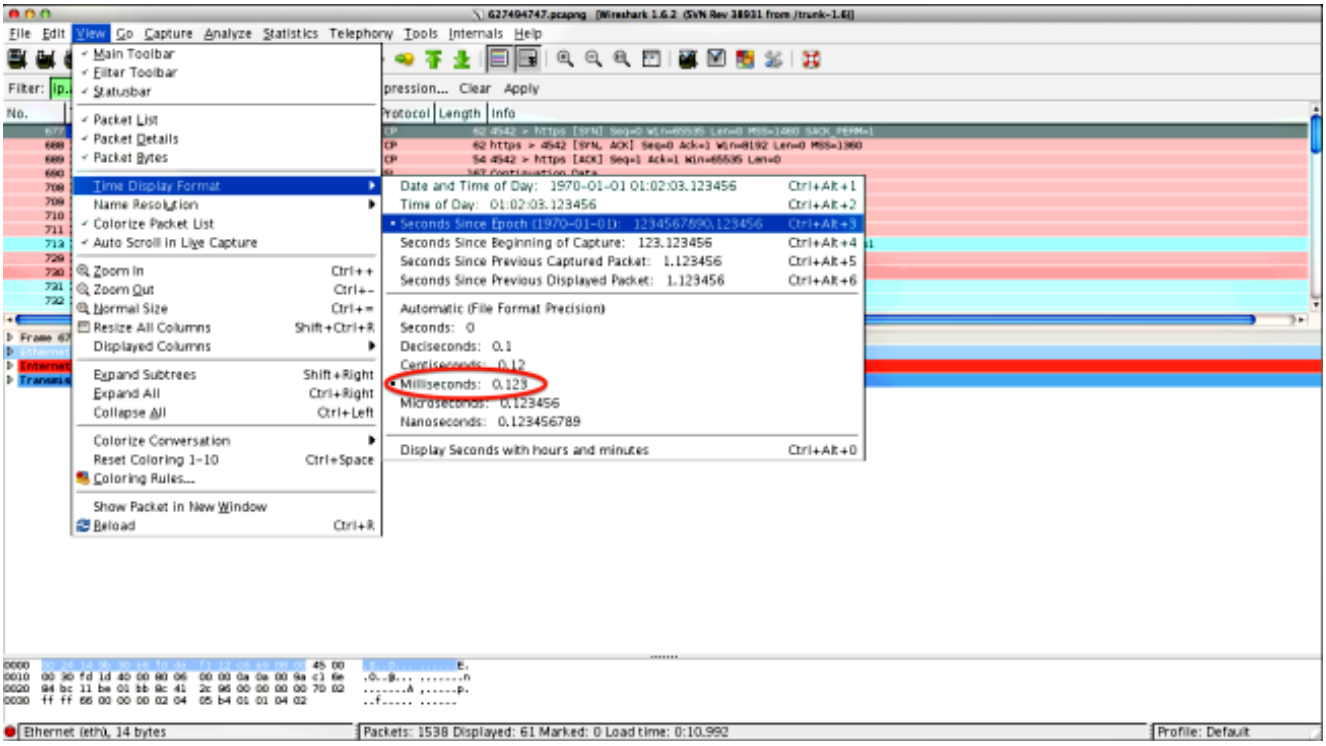



4. Para identificar más fácilmente cada uno de las sondas, haga clic con el botón derecho del ratón el **HTTP SYN** para la primera sonda, y después seleccione la **conversación de Colorize** como se muestra aquí:




Relance este proceso para los SYN en todas las sondas. Tal y como se muestra en de la imagen anterior, las primeras dos sondas se representan en diversos colores. La ventaja de colorizing las conversaciones TCP es manchar fácilmente las retransmisiones u otras tales singularidades por la sonda.

5. Para cambiar la visualización del tiempo, navegue **para ver > formato de visualización > los segundos del tiempo desde el epoch**:




Seleccione los **milisegundos**, porque ése es el nivel de precisión que OGS utiliza.

6. Calcule la diferencia de tiempo entre el HTTP SYN y el FIN/ACK, tal y como se muestra en del diagrama de la repetición del paso 4. este proceso para cada uno de las tres sondas, y compare los valores a ésos mostrados en el DARDO abre una sesión el paso 3.3.3.

### Análisis

Si después de que el análisis de las capturas los valores determinados RTT se calcule y se compare a los valores considerados en los registros del DARDO y todo se encuentra para corresponder con para arriba, pero todavía parece como el gateway incorrecto se está seleccionando, después es debido a uno de dos problemas:

- Hay un problema en el headend. Si éste es el caso, pudo haber demasiadas retransmisiones a partir de un headend del detalle, o cualquier otra tal singularidad vista en las sondas. Un análisis más cercano del intercambio se requiere.

- Hay un problema con el Proveedor de servicios de Internet (ISP). Si éste es el caso, pudo haber fragmentación o retardos grandes vistos para un headend del detalle.

## Q&A

**A:** ¿OGS trabaja con el balanceo de carga?

**R:** Yes. OGS es solamente consciente del nombre del master del cluster, y de las aplicaciones que para juzgar el headend más cercano.

**A:** ¿OGS trabaja con las configuraciones de representación definidas en el navegador?

**R:** OGS no soporta los archivos autos autos del proxy o de los Config del proxy (PAC), pero

soporta un servidor proxy codificado por hardware. Como tal, la operación OGS no ocurre. El mensaje del registro relevante es: “**OGS no será realizado porque se configura la detección automática del proxy**.”