AnyConnect最佳網關選擇故障排除指南

目錄

簡介

本文說明如何解決最佳閘道選擇(OGS)問題。OGS是一種功能，可用來確定哪個網關的來回時間(RTT)最短，並連線到該網關。您可以使用OGS功能來最小化網際網路流量的延遲，而無需使用者干預。藉助OGS，Cisco AnyConnect安全移動客戶端(AnyConnect)可以識別並選擇最適合連線或重新連線的安全網關。OGS在第一次連線時或在上一次斷開連線後至少四小時重新連線時開始。有關詳細資訊，請參閱《管理員指南》。

> **提示：**OGS最適用於最新的AnyConnect客戶端和ASA軟體版本9.1(3)*或更高版本。

OGS如何工作？

簡單網際網路控制訊息通訊協定(ICMP)**ping**要求無法運作，因為許多思科調適型安全裝置(ASA)防火牆設定為封鎖ICMP封包以阻止探索。相反，客戶端向所有配置檔案合併中顯示的每個頭端傳送三個HTTP/443請求。這些HTTP探測器在日誌中稱為OGS ping，但如前所述，它們不是ICMP ping。為了確保（重新）連線不會花費太長的時間，如果OGS在七秒內未收到任何OGS ping結果，則預設情況下會選擇上一個網關。(在日誌**中查詢OGS** ping結果。)

> **附註**：AnyConnect應向443傳送HTTP請求，因為響應本身很重要，而不是成功的響應。很遺憾，代理處理的修復程式以HTTPS形式傳送所有請求。請參閱思科錯誤ID CSCtg38672 - OGS應使用HTTP請求執行ping。

> **附註**：如果快取中沒有前端，則AnyConnect首先傳送一個HTTP請求，以確定是否存在身份驗

證代理，以及是否可以處理該請求。只有在此初始請求之後，它才會開始OGS ping以探測伺服器。

- OGS根據網路資訊(如域名系統(DNS)字尾和DNS伺服器IP地址)確定使用者位置。RTT結果連同此位置儲存在OGS快取中。

- OGS位置條目將快取14天。Cisco錯誤ID CSCtk66531 失敗，無法使使用者配置這些設定。

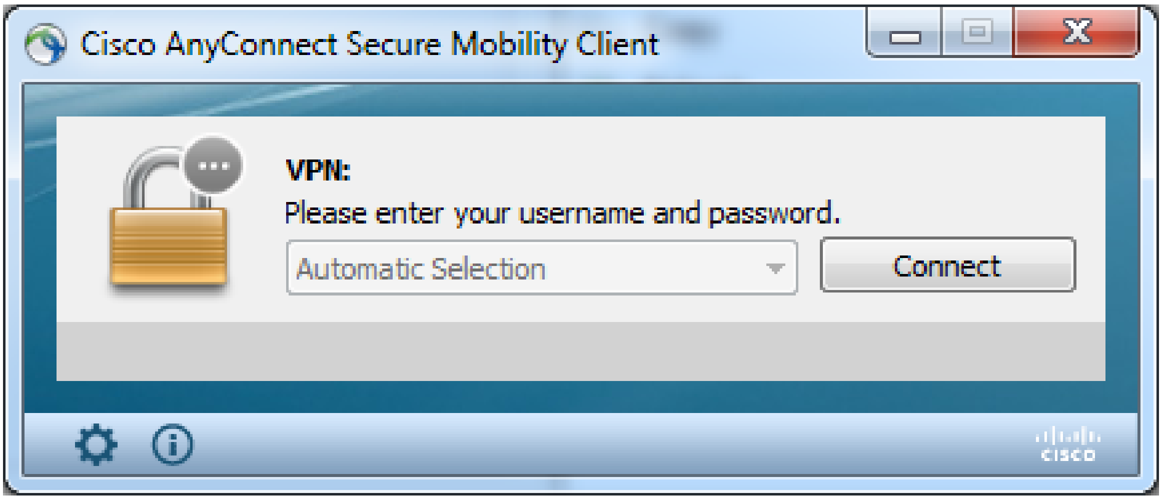
- 在首次快取位置條目14天後，才會從此位置再次運行OGS。在此期間，它會使用快取條目和為該位置確定的RTT。這表示當AnyConnect再次啟動時，它將不再執行OGS;相反，它在該位置的快取中使用最佳網關順序。在Diagnostic AnyConnect Reporting Tool(DART)日誌中，出現以下消息：

```
******************************************
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.

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

- 根據AnyConnect配置檔案中的主機條目指定，RTT通過到使用者將嘗試連線的網關的安全套接字層(SSL)埠的TCP交換來確定。

  注意：與HTTP-ping不同，HTTP-ping執行簡單的HTTP post，然後顯示RTT和結果，OGS計算稍微複雜一些。AnyConnect為每個伺服器傳送三個探測器，並計算其發出的HTTP SYN和每個探測器的FIN/ACK之間的延遲。然後，它使用最低的增量來比較伺服器並進行選擇。因此，即使HTTP-ping很好地指示AnyConnect將選擇哪個伺服器，它們也可能不一定符合。在本文檔的其餘部分中有關於此的詳細資訊。
- 目前，OGS僅在使用者退出暫停且已超過閾值時運行檢查。如果使用者所連線的ASA崩潰或變為不可用，則OGS不會連線到其他ASA。OGS僅聯絡配置檔案中的主要伺服器，以確定最佳伺服器。

- 下載OGS客戶端配置檔案後，當使用者重新啟動AnyConnect客戶端時，選擇其他配置檔案的選項將呈灰色顯示，如下所示：



VPN:
Please enter your username and password.

即使使用者電腦有多個其他配置檔案，在禁用OGS之前，他們也不能選擇其中的任何配置檔案。

OGS快取

計算完成後，結果將儲存在**preferences_global**檔案中。在此之前，此資料未儲存在檔案中時出現問題。

如需更多詳細資訊，請參閱Cisco錯誤ID CSCtj84626。

位置確定

OGS快取工作在DNS域和單個DNS伺服器IP地址的組合上。它的工作方式如下：

- 位置A有一個DNS域**locationa.com**，以及兩個DNS伺服器IP地址 — **ip1**和**ip2**。每個域/IP組合都會建立一個指向OGS快取條目的快取金鑰。例如： **locationa.com|ip1 -> ogscache1locationa.com|ip2 -> ogscache1**
- 如果AnyConnect隨後連線到物理上不同的網路，則會建立相同的域/IP組合集合，並根據快取清單進行檢查。如果有任何匹配，則使用OGS快取值，且客戶端仍被視為位**置A**。

故障方案

以下是使用者可能會遇到的一些失敗案例：

網關連線丟失時

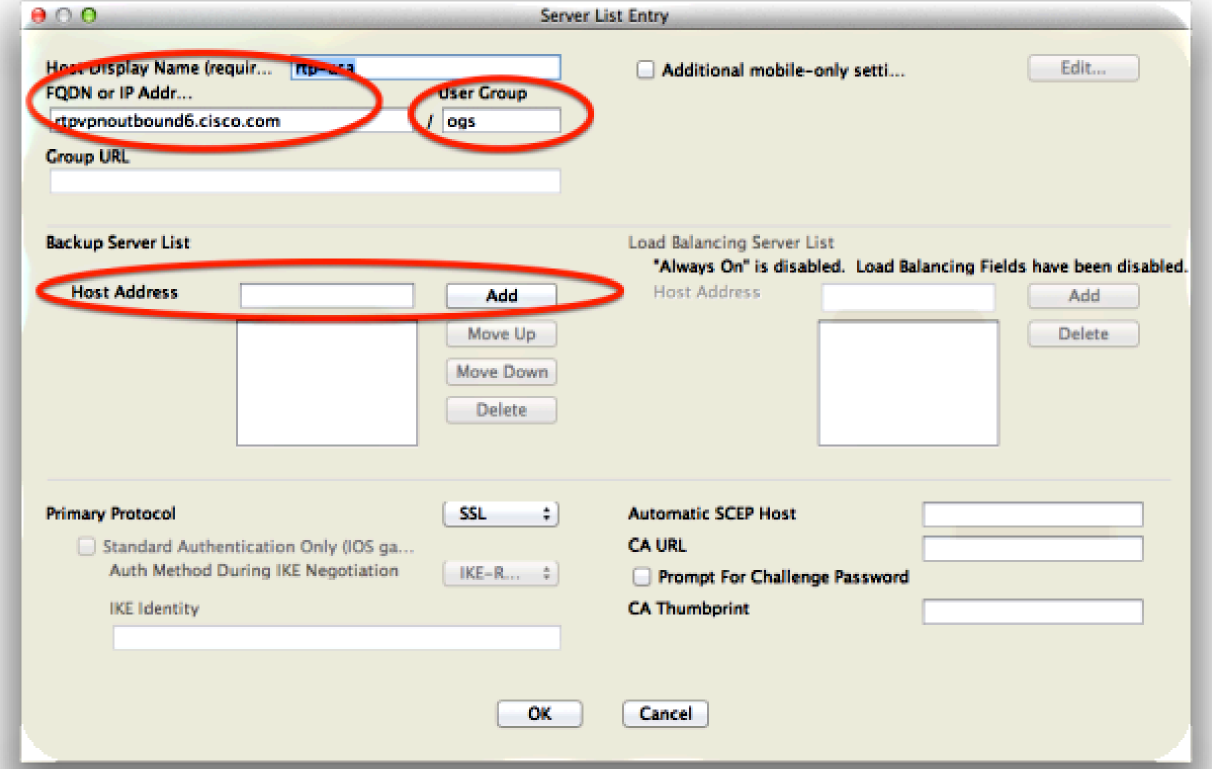
使用OGS時，如果與使用者所連線的網關的連線丟失，則AnyConnect會連線到 **備份伺服器清單和不** 到下一台OGS主機。操作順序如下：

1. OGS僅聯絡主伺服器以確定最佳伺服器。

2. 一旦確定，連線演算法為：
   嘗試連線到最佳伺服器。如果失敗，請嘗試最佳伺服器的備份伺服器清單。如果失敗，則嘗試保留在OGS選擇清單中的每台伺服器，按其選擇結果排序。

   附註：管理員配置備份伺服器清單時，當前配置檔案編輯器僅允許管理員輸入備份伺服器的完

全限定域名(FQDN)，而不允許為主伺服器輸入可能的使用者組：


Server List Entry

Host Display Name (requir... rtp-asa

FQDN or IP Addr... rtpvpnoutbound6.cisco.com / User Group ogs

Group URL

Backup Server List

Host Address

Primary Protocol SSL

□ Standard Authentication Only (IOS ga...

Auth Method During IKE Negotiation IKE-R...

IKE Identity

Load Balancing Server List

"Always On" is disabled. Load Balancing Fields have been disabled.

Automatic SCEP Host

CA URL

□ Prompt For Challenge Password

CA Thumbprint

思科錯誤ID CSCud84778 已歸檔以便更正此問題，但必須在備份伺服器的主機地址欄位中輸入完整的URL，它應該可以正常工作：**https://<*ip-address*>/usergroup**。

暫停後繼續

為了在恢復後運行OGS，AnyConnect必須在電腦進入睡眠狀態時建立連線。恢復之後的OGS僅在網路環境測試發生之後執行，用於確認網路連線是否可用。此測試包括DNS連線子測試。

但是，如果DNS伺服器捨棄在查詢欄位中含有IP位址的A型要求，而不是使用「找不到名稱」回覆（更常見的情況，在測試過程中總是發生），則思科錯誤ID CSCti20768 「IP地址的A型DNS查詢應使用PTR以避免超時」應用。

TCP Delayed-ACK Window Size選擇不正確的網關

使用低於版本9.1(3)的ASA版本時，客戶端上的捕獲顯示SSL握手中的持續延遲。注意的是，客戶端傳送其ClientHello，然後ASA傳送其ServerHello。這通常後跟一則Certificate消息（可選的Certificate Request）和ServerHelloDone消息。這種異常現象有兩方面：

1. ASA不會在ServerHello之後立即傳送證書消息。客戶端視窗大小為64,860位元組，足以容納來自ASA的整個響應。

2. 客戶端不會立即確認ServerHello，因此ASA會在大約120毫秒後重新傳輸ServerHello，此時客戶端將確認資料。然後會傳送證書消息。這幾乎就像是客戶端等待更多資料一樣。

發生這種情況的原因是TCP slow-start和TCP delayed-ACK之間的互動。在ASA 9.1(3)版之前，ASA使用的慢啟動視窗大小為1，而Windows客戶端使用的延遲ACK值為2。這意味著ASA僅傳送一個資料包，直到獲得ACK，但也意味著客戶端在收到兩個資料包之前不傳送ACK。ASA在120毫秒後超時並重新傳輸ServerHello，然後客戶端確認資料和連線繼續。此行為已由Cisco錯誤ID

CSCug98113更改，因此ASA預設使用慢啟動視窗大小2，而不是1。

在以下情況下，這可能會影響OGS計算：

- 不同的網關運行不同的ASA版本。
- 客戶端具有不同的延遲ACK視窗大小。

在這種情況下，延遲ACK引入的延遲可能足以導致客戶端選擇錯誤的ASA。如果此值在客戶端和ASA之間不同，則仍可能存在問題。在這種情況下，解決方法是調整「延遲確認」視窗大小。

Windows

1. 啟動註冊**表編輯器**。
2. 標識要在其上禁用延遲ACK的介面的GUID。為此，請導航 到：
   HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > WindowsNT > CurrentVersion > NetworkCards >（編號）。
   檢視「NetworkCards（網絡卡）」下列出的每個號碼。在右側，說明應列出介面(例如，Intel(R)Wireless WiFi Link 5100AGN),ServiceName應列出相應的GUID。
3. 找到並按一下此登錄檔子項：
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<介面GUID>
4. 在「編輯」選單上，指向「新建」，然後按一下「**DWORD值」**。
5. 將新值命名為**TcpAckFrequency**，並為其指定值**1**。
6. 退出登錄檔編輯器。
7. 重新啟動Windows以使此更改生效。

   附註：思科錯誤ID CSCum19065 已失敗，因此無法在ASA上配置TCP調整引數。

典型使用者示例

最常見的使用案例是當在家中的使用者第一次運行OGS時，它會記錄DNS設定，並且OGS ping結果在快取中（預設為14天超時）。 當使用者第二天晚上回到家時，OGS檢測到相同的DNS設定，在快取中找到它，並跳過OGS ping測試。之後，當使用者前往提供網際網路服務的酒店或餐廳時，OGS會檢測不同的DNS設定，運行OGS ping測試，選擇最佳網關，並將結果記錄在快取中。

如果OGS和AnyConnect恢復設定允許，當從掛起或休眠狀態恢復時，處理過程將完全相同。

OGS故障排除

步驟1.清除OGS快取以強制重新評估

為了清除OGS快取並重新評估可用網關的RTT，只需從PC中刪除Global AnyConnect Preferences檔案。檔案的位置因作業系統(OS)而異：

- Windows Vista和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..
```

步驟2.在連線嘗試期間捕獲伺服器探測器

1. 在測試電腦上啟動Wireshark。

2. 在AnyConnect上啟動連線嘗試。

3. 連線完成後停止Wireshark捕獲。 **提示：**由於捕獲僅用於測試OGS，因此最好在AnyConnect選擇網關時立即停止捕獲。最好不要進行完整的連線嘗試，因為這可能使資料包捕獲變雲。

步驟3.檢驗OGS選擇的網關

為了驗證OGS選擇特定網關的原因，請完成以下步驟：

1. 啟動新連線。

2. 運行AnyConnect DART:
   啟動**AnyConnect**，然後按一下**Advanced**。按一下「**Diagnostics**」。按「**Next**」（下一步）。按「**Next**」（下一步）。
3. 檢查在案頭上新建立的**DartBundle_XXXX_XXXX.zip**檔案中找到的DART結果。
   導覽至**Cisco AnyConnect Secure Mobility Client > AnyConnect.txt**。

   請注意從此DART日誌中啟動特定伺服器的OGS探測的時間：

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

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

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

通常，它們應該大致在同一時間，但在捕獲量較大時，時間戳有助於縮小哪些資料包是HTTP探測器和哪些資料包是實際連線嘗試的範圍。

AnyConnect向伺服器傳送三個探測後，將生成以下消息，其中包含每個探測的結果：

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

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 )

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

必須注意這三個值，因為它們必須與捕獲結果相匹配。

檢視包含「*** OGS Selection Results***」的消息以檢視評估的RTT，以及最近一次連線嘗試是快取RTT還是新計算的結果。

以下是範例：

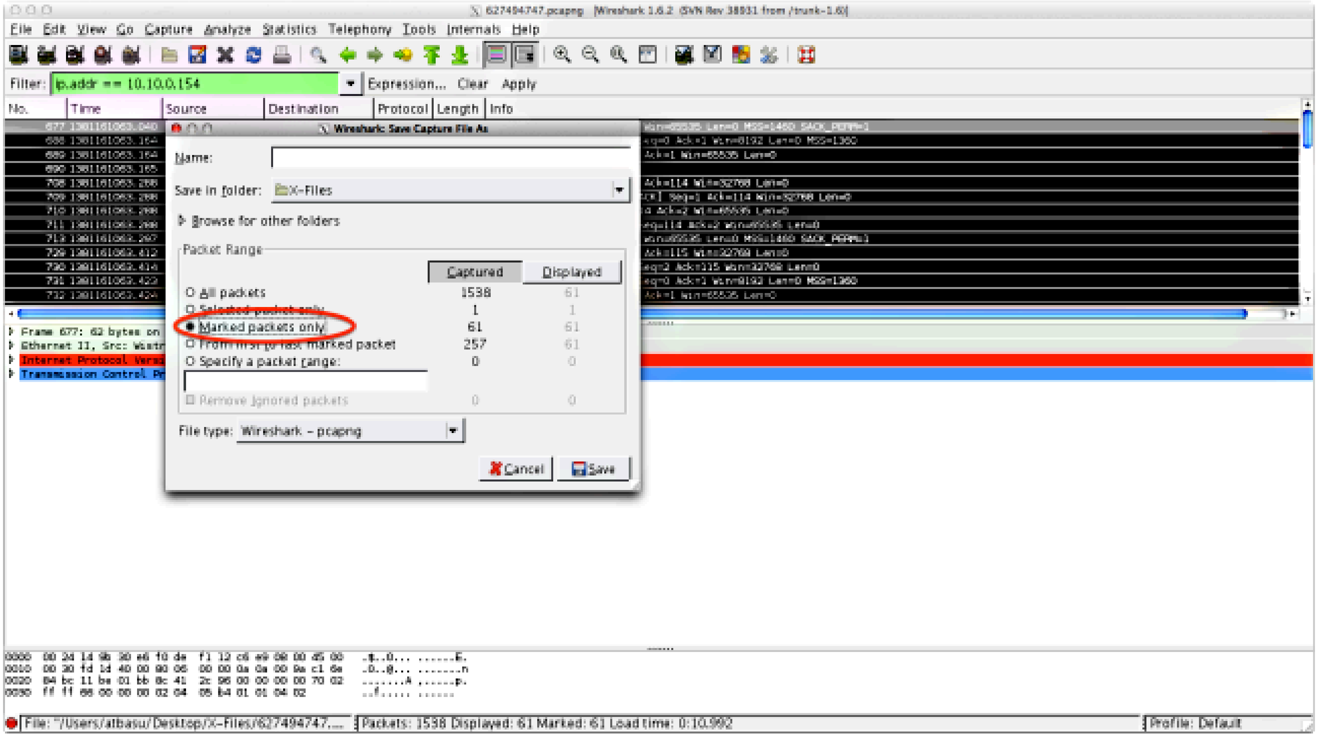
```
******************************************

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.

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

步驟4.驗證AnyConnect運行的OGS計算

檢查用於計算RTT的TCP/SSL探測的捕獲。檢視HTTPS請求佔用單個TCP連線的時間。每個探測請求都應使用不同的TCP連線。為此，請在Wireshark中開啟捕獲，然後對每個伺服器重複以下步驟：

1. 使用**ip.addr**過濾器可以將傳送到每個伺服器的資料包隔離到其自己的捕獲中。為此，請導航至**編輯**，然後選擇**標籤所有顯示的資料包**。然後導覽至**File > Save As**，選擇**Marked packets**

only選項，然後按一下**Save**:



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
Wireshark: Save Capture File As
Browse for other folders
Cancel
Save

Filter: ip.addr == 10.10.0.154

Name:

Save in folder: X-Files

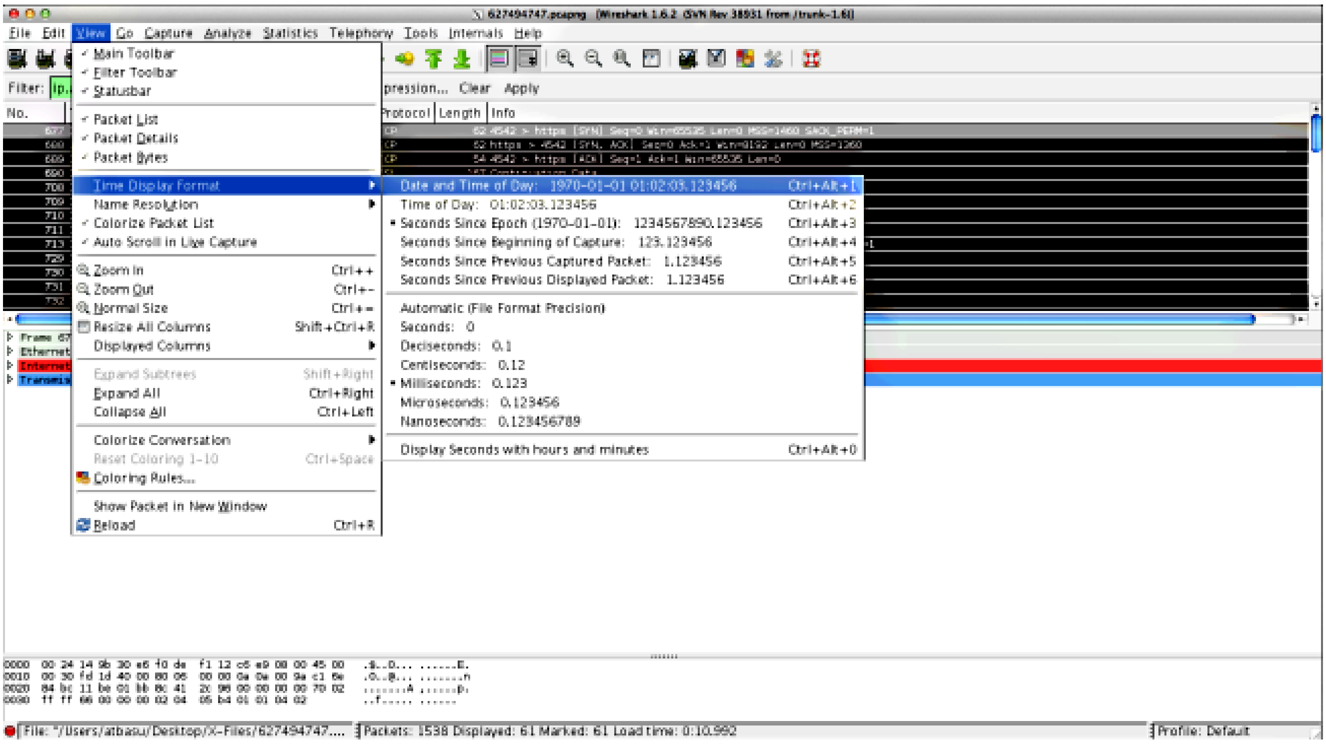
Packet Range

	Captured	Displayed
○ All packets	1538	61
○ Selected packet only	1	1
● Marked packets only	61	61
○ From first to last marked packet	257	61
○ Specify a packet range:	0	0
□ Remove Ignored packets	0	0

File type: Wireshark - pcapng

File: "/Users/atbasu/Desktop/X-Files/627494747.... Packets: 1538 Displayed: 61 Marked: 61 Load time: 0:10.992 Profile: Default

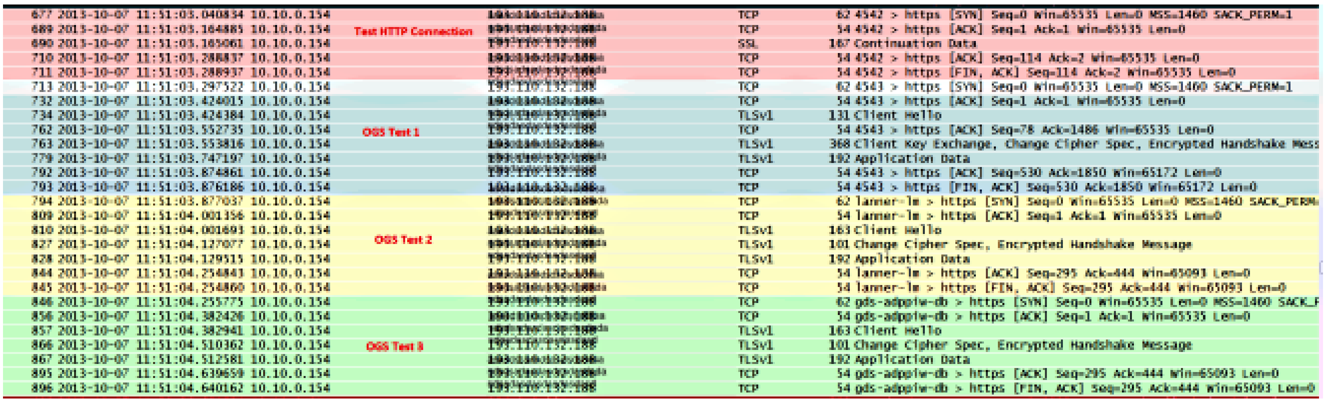
2. 在此新捕獲中，導航到**檢視>時間顯示格式>日期和時間**:



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
✓ Main Toolbar
✓ Filter Toolbar
✓ Statusbar
✓ Packet List
✓ Packet Details
✓ Packet Bytes
Time Display Format
Name Resolution
✓ Colorize Packet List
✓ Auto Scroll in Live Capture
Zoom In Ctrl++
Zoom Out Ctrl+-
Normal Size Ctrl+=
Resize All Columns Shift+Ctrl+R
Displayed Columns
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Conversation
Reset Coloring 1-10 Ctrl+Space
Coloring Rules...
Show Packet in New Window
Reload Ctrl+R
Date and Time of Day: 1970-01-01 01:02:03.123456 Ctrl+Alt+1
Time of Day: 01:02:03.123456 Ctrl+Alt+2
• Seconds Since Epoch (1970-01-01): 1234567890.123456 Ctrl+Alt+3
Seconds Since Beginning of Capture: 123.123456 Ctrl+Alt+4
Seconds Since Previous Captured Packet: 1.123456 Ctrl+Alt+5
Seconds Since Previous Displayed Packet: 1.123456 Ctrl+Alt+6
Automatic (File Format Precision)
Seconds: 0
Deciseconds: 0.1
Centiseconds: 0.12
• Milliseconds: 0.123
Microseconds: 0.123456
Nanoseconds: 0.123456789
Display Seconds with hours and minutes Ctrl+Alt+0

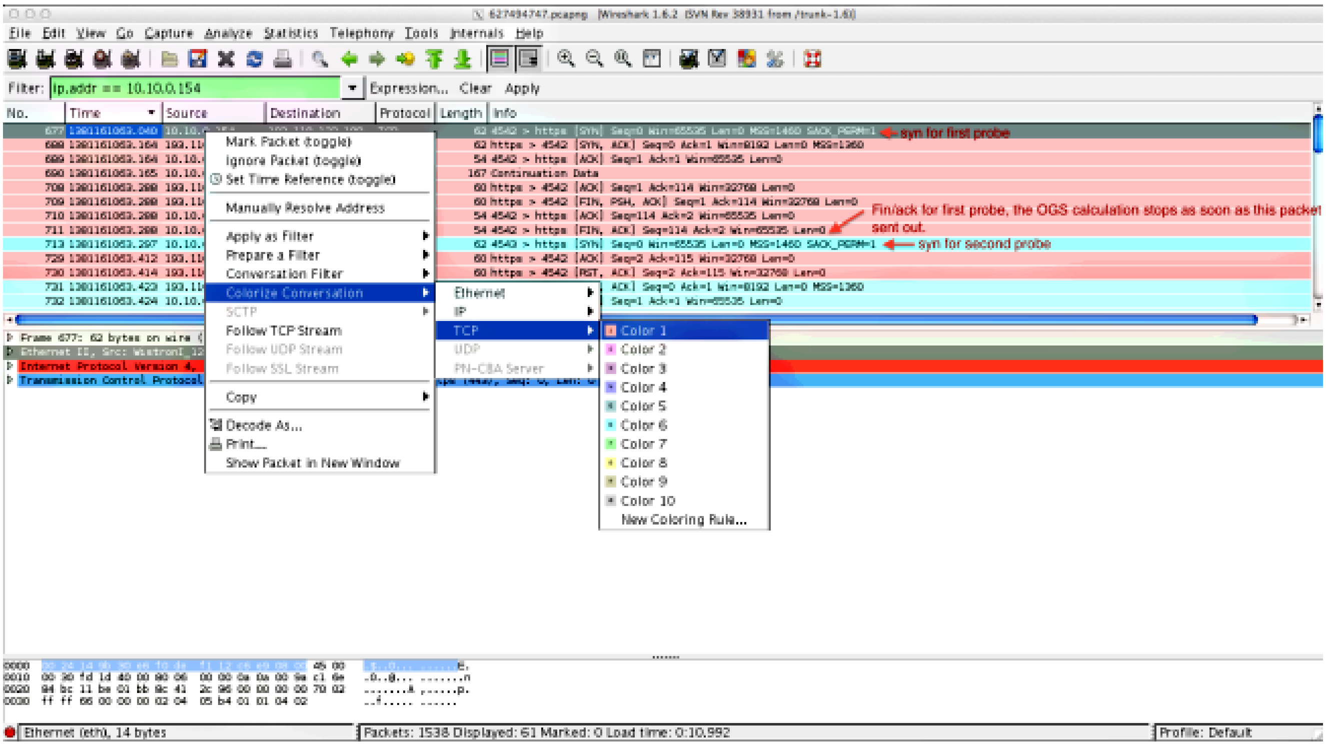
File: "/Users/atbasu/Desktop/X-Files/627494747.... Packets: 1538 Displayed: 61 Marked: 61 Load time: 0:10.992 Profile: Default

3. 根據步驟3.3.2中識別的DART日誌確定在傳送OGS探測時傳送的捕獲中的第一個HTTP SYN資料包。必須記住，對於第一個伺服器，第一個HTTP請求不是伺服器探測。很容易錯誤地發出第一個伺服器探測請求，因此得到的值與OGS報告的值完全不同。此處突出顯示了此問題：



```
677 2013-10-07 11:51:03.040834 10.10.0.154  193.110.132.188  TCP     62 4542 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
689 2013-10-07 11:51:03.164885 10.10.0.154  193.110.132.188  TCP     54 4542 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
690 2013-10-07 11:51:03.165061 10.10.0.154  193.110.132.188  SSL    167 Continuation Data
710 2013-10-07 11:51:03.288837 10.10.0.154  193.110.132.188  TCP     54 4542 > https [ACK] Seq=114 Ack=2 Win=65535 Len=0
711 2013-10-07 11:51:03.288937 10.10.0.154  193.110.132.188  TCP     54 4542 > https [FIN, ACK] Seq=114 Ack=2 Win=65535 Len=0
713 2013-10-07 11:51:03.297522 10.10.0.154  193.110.132.188  TCP     62 4543 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
732 2013-10-07 11:51:03.424015 10.10.0.154  193.110.132.188  TCP     54 4543 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
734 2013-10-07 11:51:03.424384 10.10.0.154  193.110.132.188  TLSv1  131 Client Hello
762 2013-10-07 11:51:03.552735 10.10.0.154  193.110.132.188  TCP     54 4543 > https [ACK] Seq=78 Ack=1486 Win=65535 Len=0
763 2013-10-07 11:51:03.553816 10.10.0.154  193.110.132.188  TLSv1  368 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess
779 2013-10-07 11:51:03.747197 10.10.0.154  193.110.132.188  TLSv1  192 Application Data
792 2013-10-07 11:51:03.874861 10.10.0.154  193.110.132.188  TCP     54 4543 > https [ACK] Seq=530 Ack=1850 Win=65172 Len=0
793 2013-10-07 11:51:03.876186 10.10.0.154  193.110.132.188  TCP     54 4543 > https [FIN, ACK] Seq=530 Ack=1850 Win=65172 Len=0
794 2013-10-07 11:51:03.877037 10.10.0.154  193.110.132.188  TCP     62 lanner-lm > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=
809 2013-10-07 11:51:04.001356 10.10.0.154  193.110.132.188  TCP     54 lanner-lm > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
810 2013-10-07 11:51:04.001693 10.10.0.154  193.110.132.188  TLSv1  163 Client Hello
827 2013-10-07 11:51:04.127077 10.10.0.154  193.110.132.188  TLSv1  101 Change Cipher Spec, Encrypted Handshake Message
828 2013-10-07 11:51:04.129515 10.10.0.154  193.110.132.188  TLSv1  192 Application Data
844 2013-10-07 11:51:04.254841 10.10.0.154  193.110.132.188  TCP     54 lanner-lm > https [ACK] Seq=295 Ack=444 Win=65093 Len=0
845 2013-10-07 11:51:04.254860 10.10.0.154  193.110.132.188  TCP     54 lanner-lm > https [FIN, ACK] Seq=295 Ack=444 Win=65093 Len=0
846 2013-10-07 11:51:04.255775 10.10.0.154  193.110.132.188  TCP     62 gds-adppiw-db > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_F
856 2013-10-07 11:51:04.382426 10.10.0.154  193.110.132.188  TCP     54 gds-adppiw-db > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
857 2013-10-07 11:51:04.382941 10.10.0.154  193.110.132.188  TLSv1  163 Client Hello
866 2013-10-07 11:51:04.510362 10.10.0.154  193.110.132.188  TLSv1  101 Change Cipher Spec, Encrypted Handshake Message
867 2013-10-07 11:51:04.512581 10.10.0.154  193.110.132.188  TLSv1  192 Application Data
895 2013-10-07 11:51:04.639659 10.10.0.154  193.110.132.188  TCP     54 gds-adppiw-db > https [ACK] Seq=295 Ack=444 Win=65093 Len=0
896 2013-10-07 11:51:04.640162 10.10.0.154  193.110.132.188  TCP     54 gds-adppiw-db > https [FIN, ACK] Seq=295 Ack=444 Win=65093 Len=0
```

4. 為了更輕鬆地識別每個探測器，請按一下右鍵第一個探測器的**HTTP SYN**，然後選擇**Colorize Conversation**，如下所示：



Filter: ip.addr == 10.10.0.154

```
677 1381161063.040 10.10.0.154                      62 4542 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
688 1381161063.164 193.11                           62 https > 4542 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1360
689 1381161063.164 10.10.                           54 4542 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
690 1381161063.165 10.10.                          167 Continuation Data
708 1381161063.288 193.11                           60 https > 4542 [ACK] Seq=1 Ack=114 Win=32768 Len=0
709 1381161063.288 193.11                           60 https > 4542 [FIN, PSH, ACK] Seq=1 Ack=114 Win=32768 Len=0
710 1381161063.288 10.10.                           54 4542 > https [ACK] Seq=114 Ack=2 Win=65535 Len=0
711 1381161063.288 10.10.                           54 4542 > https [FIN, ACK] Seq=114 Ack=2 Win=65535 Len=0
713 1381161063.297 10.10.                           62 4543 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
729 1381161063.412 193.11                           60 https > 4542 [ACK] Seq=2 Ack=115 Win=32768 Len=0
730 1381161063.414 193.11                           60 https > 4542 [RST, ACK] Seq=2 Ack=115 Win=32768 Len=0
731 1381161063.423 193.11                                  ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1360
732 1381161063.424 10.10.                                  Seq=1 Ack=1 Win=65535 Len=0
```

syn for first probe

Fin/ack for first probe, the OGS calculation stops as soon as this packet sent out.

syn for second probe

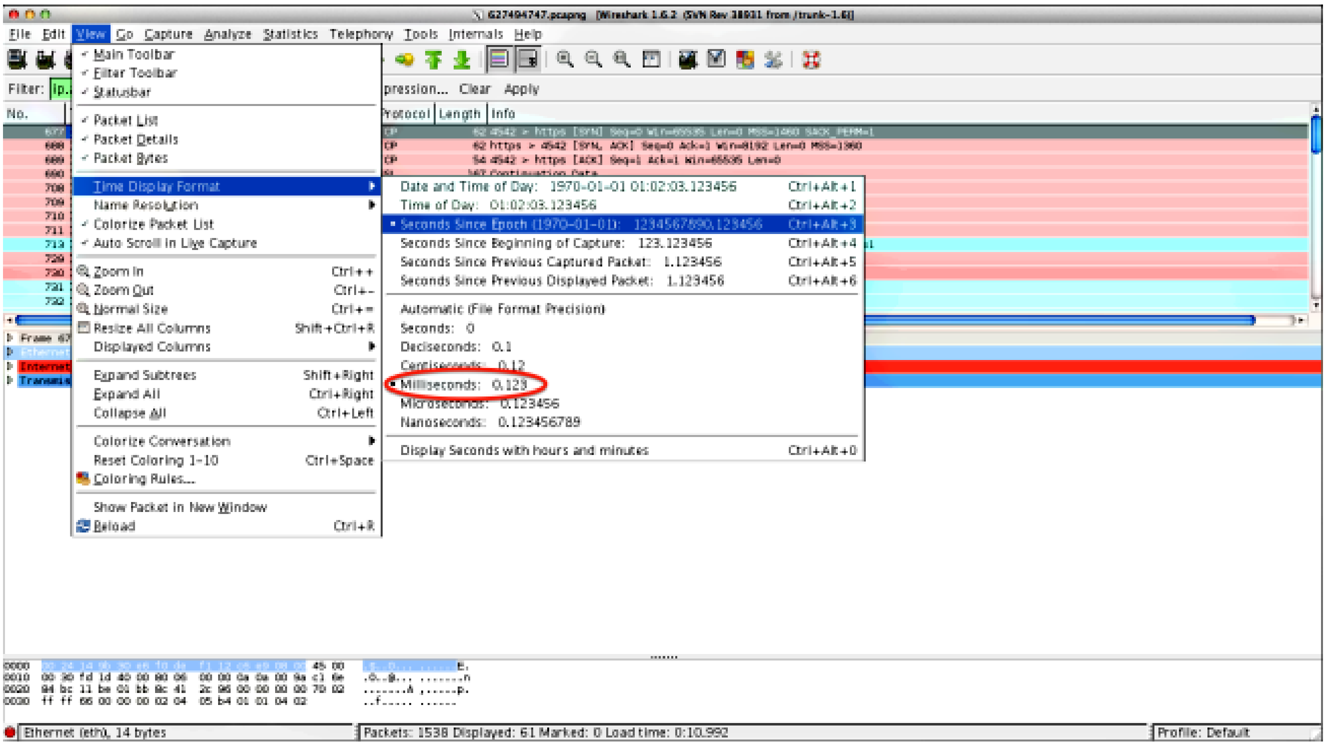
```
Frame 677: 62 bytes on wire (
Ethernet II, Src: Wistronl_12
Internet Protocol Version 4,
Transmission Control Protocol
```

```
0000  00 24 14 0b 90 e6 f0 de  f1 12 c6 e9 08 00 45 00   .$......  ......E.
0010  00 30 fd 1d 40 00 80 06  00 00 0a 0a 00 9a c1 6e   .0..@...  .......n
0020  84 bc 11 be 01 bb 8c 41  2c 96 00 00 00 00 70 02   .......A  ,.....p.
0030  ff ff 66 00 00 00 02 04  05 b4 01 01 04 02         ..f.....  ......
```

Ethernet (eth), 14 bytes | Packets: 1538 Displayed: 61 Marked: 0 Load time: 0:10.992 | Profile: Default

對所有探測器上的SYN重複此過程。如上圖所示，前兩個探測器以不同的顏色表示。對TCP會話進行著色處理的優點是易於發現每個探測點的重新傳輸或其他此類異常。

5. 要更改時間顯示，請導航到**檢視>時間顯示格式>自紀元以來的秒數**:


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Main Toolbar
Filter Toolbar
Statusbar
Packet List
Packet Details
Packet Bytes
Time Display Format
Name Resolution
Colorize Packet List
Auto Scroll in Live Capture
Zoom In Ctrl++
Zoom Out Ctrl+-
Normal Size Ctrl+=
Resize All Columns Shift+Ctrl+R
Displayed Columns
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Conversation
Reset Coloring 1-10 Ctrl+Space
Coloring Rules...
Show Packet in New Window
Reload Ctrl+R
Date and Time of Day: 1970-01-01 01:02:03.123456 Ctrl+Alt+1
Time of Day: 01:02:03.123456 Ctrl+Alt+2
Seconds Since Epoch (1970-01-01): 1234567890.123456 Ctrl+Alt+3
Seconds Since Beginning of Capture: 123.123456 Ctrl+Alt+4
Seconds Since Previous Captured Packet: 1.123456 Ctrl+Alt+5
Seconds Since Previous Displayed Packet: 1.123456 Ctrl+Alt+6
Automatic (File Format Precision)
Seconds: 0
Deciseconds: 0.1
Centiseconds: 0.12
Milliseconds: 0.123
Microseconds: 0.123456
Nanoseconds: 0.123456789
Display Seconds with hours and minutes Ctrl+Alt+0
Packets: 1538 Displayed: 61 Marked: 0 Load time: 0:10.992
Profile: Default

選擇**Milliseconds**，因為這是OGS使用的精度級別。

6. 計算HTTP SYN和FIN/ACK之間的時間差，如步驟4的圖中所示。對三個探測器中的每個探測器重複此過程，並將這些值與步驟3.3.3中的DART日誌中所示的值進行比較。

分析

如果在捕獲分析之後計算出確定的RTT值，並將其與DART日誌中顯示的值進行比較，發現所有內容都匹配，但似乎仍然選擇了錯誤的網關，則這是由兩個問題之一造成的：

- 頭端出現問題。如果是這種情況，則可能存在來自某個特定頭端的過多重傳，或者探針中發現的任何其他此類異常。需要對這種交換進行更深入的分析。
- Internet服務提供商(ISP)出現問題。 如果是這種情況，可能會出現特定頭端的分段或大量延遲。

問答

問：OGS是否適用於負載均衡？

答：是。OGS只知道集群主名稱，並使用該名稱來判斷最近的頭端。

Q:OGS是否適用於瀏覽器中定義的代理設定？

A:OGS不支援自動代理或代理自動配置(PAC)檔案，但支援硬編碼的代理伺服器。因此，不會執行OGS操作。相關日誌消息為：「由於配置了自動代理檢測，**將不執行**OGS。」