AnyConnect最佳網關選擇故障排除指南

目錄

簡介 OGS如何工作? OGS快取 位置確定 故障方案 網關連線丟失時 暫停後繼續 TCP Delayed-ACK Window Size選擇不正確的網關 典型使用者示例 OGS故障排除 步驟1.清除OGS快取以強制重新評估 步驟2.在連線嘗試期間捕獲伺服器探測器 步驟3.檢驗OGS選擇的網關 步驟4.驗證AnyConnect運行的OGS計算 分析 問答

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<u>《管理員指南》</u>。

提示:OGS最適用於最新的AnyConnect客戶端和ASA軟體版本9.1(3)*或<u>更高</u>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 <u>CSCtg38672</u> -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:

• 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:

S Cisco	AnyCor	nect Secure Mobility Client	
	-0	VPN: Please enter your username and password.	
		Automatic Selection	Connect
0	i		altalta cisco

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:

ctpvpnoutbound6.cisco Group URL	o.com	logs		
Backup Server List Host Address		Add	Load Balancing Server List "Always On" is disabled. I Host Address	oad Balancing Fields have been disab
		Move Up Move Down Delete		Delete
Primary Protocol Standard Authen Auth Method Du IKE Identity	tication Only (IOS ga rring IKE Negotiation	SSL +	Automatic SCEP Host CA URL Prompt For Challenge Pas CA Thumbprint	sword

思科錯誤ID <u>CSCud84778</u> 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 <u>CSCti20768</u> 「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<u>TCP slow-start</u>和<u>TCP delayed-ACK</u>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。
- 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\Interface s\<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 <u>CSCum19065</u> 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

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。
- 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。
- 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)。
- . 檢查在案頭上新建立的DartBundle_XXXX_XXX.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:

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)

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
Туре	:	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:

C C C X 627494747.pcapeg Wireshart	1.6.2 (SVN Rev 38931 from /trunk-1.6)
Elle Eux Yew Co Capture Analyze Statistics releptony Tools Internals Balb	m 🖬 🕅 🎫 🖗 😚
Filter In addr 10 100 154	
No. Time Source Destination Protocol Landh Info	7
677 1201161063.040 0 O Versionalitori Protocol Cengui Into	Von-63535 Lan-0 MSS-0460 SACK_PERM-1
666 1301161063, 164	ege0 Adx=1 W1rm=0192 Lar=0 M55=1360
600 1301101005.144 Marrie:	With Stores Parket
Add 1381161063, 208 Save in folder: TX-Files	Ack=114 W1#-52768 Len=0 281 Segs) Ack=114 W1#-52768 Len=0
7[0] 191161033 298	a Ackuz Witweesses Lenuc
713 1361161068 268 P growte for other folders	egulla Actual Monatodo Lenut Actual5535 Lenut Mosilado SACK ASPRO
729 1391161062 412 799 320141062 434	AckellS Mine22769 Lene0
224 1201161059-422	egrő Ackr3 Vonrelsz Lenrő MSSr1360
732 1301161063.434 O All packets 1538 61	Ack=1 bin=55536 Lan=0
A Grane 677: 62 bates as Marked packets only 61 61	2000
Ethernet 11, Src: Water O From more go last marked packet 257 61	
Internet Protocol Versi O Specify a packet gange: O	
E Remark Internet each str. 0 0	
In Hermove Janored packets 0 0	
File type: Wireshark – pcapng 💌	
Receil Receil	
Cancer Wave	
00000 00 24 14 9k 30 e6 10 de f1 12 c6 e9 08 00 45 00 .t.0	
0020 84 bc 11 be 01 bb 8c 41 2c 96 00 00 00 07 02	
0030 11 11 85 00 00 02 04 05 14 01 01 04 02	
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:

		_	X 627494747.pcaprg (Wireshark 1.6.2 (SVN Rev 38931 fro	om /trunk-1.6()	
<u>Eile E</u> dit	View Go Capture Analyze Statistics Te	lephor	w Iools Internals Help		
SK 64 6	- Main Toolbar		🛶 🐐 🛓 🔲 🗐 ାର୍ ପ୍ର୍ୟ 🗹 🗃 🛣 🐿 🕵 🐒	: #	
Filter: In.	< Eilter Toolbar		pression Clear Apply		
No	- gratospan	_	Pressional Length Info		
140.	✓ Packet List		(P 62.4542 > https: [Sth] Secret Vice#5535 Lanet MSS-1	460 SACK PERM	1
660	< Packet Details		(P 52 https: > 4542 [SrN, AOK] Seg=0 Ack+1 Won+9192 1	an-0 MSS-1260	
609 690	 Packet gytes 		CP 54-4542 > https://doil.seq=1.4ck=1.Win=65525.Len=0 SI NET Contraction Cata)	
700	Time Display Format	•	Date and Time of Day: 1970-01-01 01:02:03.123456	Orl+AR+L	
709	Name Resolution	•	Time of Day: 01:02:03.123456	Ctrl+Ak+2	
711	< Colorize Packet List		 Seconds Since Epoch (1970–01–01): 1234567890.123456 Seconds Since Replacing of Continues, 123, 1234567890. 	Ctrl+AR+3	
713	 Auto Scroll In Lige Capture 		Seconds Since Deginning of Capture: 123.123456 Seconds Since Previous Captured Packet: 1.123456	Orl+AR+9	
730	© Zoom in Ct	r1++	Seconds Since Previous Displayed Packet: 1.123456	Ctrl+At+6	
731	Q Zoom Qut O	rl+-			
•	R Besize All Columns Skills C	1+=	Automatic (File Format Precision)		
> Frame 67	Displayed Columns Shirt+C	11+1	Deciserands: 0.1		
P Ethernet			Centiseconds: 0.12		
Transmis	Expand Subtrees Shift+	right	Milliseconds: 0.123		
	Expand All Ctri+	ugnt Lieft	Microseconds: 0.123456		
	compre gri		Nanoseconds: 0.128456789		
	Colorize Conversation	•	Display Seconds with hours and minutes	Ctrl+Ak+0	
	Reset Coloring 1–10 Ctrl+3	pace			
	Coloring Pales				
	Show Packet in New Window				
	Eeload C	TI+R			
0000 00 24	14 96 30 e5 f0 de f1 12 c5 e9 08 00 45 00		.0E.		
0020 84 bc	11 be 01 be 80 41 20 96 00 00 00 00 70 02				
0000 11 11	66 00 00 00 02 04 06 04 01 04 02				
Elle: */11	isers (ath polit Desitten (%_Files /627494747	3 Par	kate: 1538 Displayed: 61 Marked: 61 Load time: 0:10 990		Drofile: 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:

6689 2013-10-07 11:31:03.164881 10.10.0.134 Tet HTTP Connection 99400000000000000000000000000000000000	677 2013-10-07 11:51:03.040834 1	0.10.0.154		193:019:010:010:000	TCP	62 4542 > https [SVN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
6690 2013-10-07 11:31:03.103061 10:10.0.0.134 19*1790*199/199 58. 10* Continuation Data 710 2013-10-07 11:31:03.28837 10:10.0.0.134 19*1790*199/199 TCP 34.4542 https: [F1N, 4KX] Seq-114 Ack-2 win-65335 Len-0 711 2013-10-07 11:31:03.29837 10:10.0.0.134 19*1790*199/199 TCP 54.4542 https: [F1N, 4KX] Seq-114 Ack-2 win-65335 Len-0 732 2013-10-07 11:31:03.297325 10:10.0.134 19*1790*199/199 TCP 54.4543 https: [ArX] Seq-114 Ack-2 win-65335 Len-0 732 2013-10-07 11:51:03.747167 10:10.0.154 19*1790*199/199 TCP 54.4543 https: [ArX] Seq-124 Ack-1 win-65335 Len-0 732 2013-10-07 11:51:03.747107 10:10.0.154 19*1799*199/19*1786 TCP 54.4543 https: [ArX] Seq-350 Ack-1456 win-65335 Len-0 733 2013-10-07 11:51:03.747107 10:10.0.154 19*1999/19*1786 TCP 54.4543 https: [ArX] Seq-550 Ack-1456 win-65172 Len-0 793 2013-10-07 11:51:03.876168 10:10.0.154 19*1999/19*19*19*19*19*19*19*19*19*19*19*19*19*1	689 2013-10-07 11:51:03.164885 1	0.10.0.154	Fast HTTP Connection	101/010/032/0881s	TCP	54 4542 > https [ACK] Seg=1 Ack=1 Win=65535 Len=0
712 2013-10-07 113:103,288837 10.100,0.134 1000000000000000000000000000000000000	690 2013-10-07 11:51:03.165061 1	0.10.0.154		191110.112.108	SSL	167 Continuation Data
711 2013-10-07 711:51:03, 288937 10.10, 0.154 793 400199370001 712 2013-10-07 711:51:03, 297321 01.00, 0.154 193 400199370001 TCP 54 454 > https: [F1N, ACK] Seq-11 Ack-2 win-05333 Lem-0 732 2013-10-07 711:51:03, 2424013 10.10, 0.154 193 4001993000000 TCP 54 454 > https: [ACK] Seq-1 Ack-1 win-65335 Lem-0 732 2013-10-07 711:51:03, 242410 10.10, 0.154 193 400199300000 TCP 54 454 > https: [ACK] Seq-78 Ack-1466 win-65335 Lem-0 761 2013-10-07 711:51:03, 27310 10.10, 0.154 193 400199300000 TCP 54 454 > https: [ACK] Seq-78 Ack-1466 win-65335 Lem-0 761 2013-10-07 711:51:03, 274107 10.10, 0.154 193 400199300000000000 TCP 54 454 > https: [ACK] Seq-78 Ack-1466 win-65372 Lem-0 792 2013-10-07 711:51:03, 276168 10.10, 0.154 193 4000000000000000000000000000000000000	710 2013-10-07 11:51:03.288837 1	0.10.0.154		1930110/152/1884	TCP	54 4542 > https [ACK] Seg=114 Ack=2 Win=65535 Len=0
712 2013-10-07 113 103, 29732 10.10, 0.134 Y917Y071997198 TCP 62 454 > https Status Seq-0 win-d5335 Lem-0 SACK_PERM-1 732 2013-10-07 113 103, 42431 https 10.10, 0.134 1994294997198 TCP 64 454 > https fXXI Seq-1 Ack-1 Win-d5335 Lem-0 742 2013-10-07 113 103, 42431 https 10.10, 0.134 19942949971985 TCP 54 454 > https fXXI Seq-146 win-d5335 Lem-0 763 2013-10-07 113 103, 553316 10, 10, 0.154 19942949971886 TCP 54 454 > https fXXI Seq-28 Ack-1468 win-d5335 Lem-0 763 2013-10-07 113 103, 747107 10.10, 0.154 199429499701886 TCP 54 454 > https fXXI Seq-30 Ack-1850 win-65172 Lem-0 792 2013-10-07 113 103, 747107 10.10, 0.154 199429499701897188 TCP 54 454 > https fXXI Seq-30 Ack-1850 win-65172 Lem-0 792 2013-10-07 113 103, 876168 10.10, 0.154 1994294997019971888 TCP 54 454 > https fXXI Seq-30 Ack-1850 win-65172 Lem-0 794 2013-10-07 113 104, 127077 10.10, 0.154 199429499797019971888 TCP 54 454 > https fXXI Seq-30 Ack-1450 Win-65172 Lem-0 802 2013-10-07 113 104, 127077 10.10, 0.134	711 2013-10-07 11:51:03.288937 1	0.10.0.154		1993-1110-1197-1108-11	TCP	54 4542 > https (FIN, ACK) Seg=114 Ack=2 Win=65535 Len=0
732 2013-10-07 11:51:03,424015 10.10,0.154 10.10,0.154 734 2013-10-07 11:51:03,424015 10.10,0.154 11.11:03,15235 11.11:01:01:01:01:01:01:01:01:01:01:01:01:0	713 2013-10-07 11:51:03.297522 1	0.10.0.154		193111011321188	TCP	62 4543 > https [SYN] Seg=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
734 2013-10-07 11:51:03, 42484 10.10, 0.154 994-1964*99/1984* TLSVL 131 Cfent Hello 762 2013-10-07 11:51:03, 552735 10:10, 0.154 993-1964*99/1984* TCP 54 4543 https: [AcX] Seq-78 Ack=1486 Win=65335 Len=0 779 2013-10-07 11:51:03, 572361 10:10, 0.154 1993-1964*99/1986* TLSVL 388 Cfient Key Exchange, Change Cipher Spec, Encrypted Handshake Mess 792 2013-10-07 11:51:03, 874861 10:10, 0.154 1993-1964*99/1986* TLSVL 192 Application Data 792 2013-10-07 11:51:03, 874861 10:10, 0.154 1993-1964*99/1986* TCP 54 4543 > https: [ArX] Seq-530 Ack=1850 Wine55172 Len=0 794 2013-10-07 11:51:03, 876186 10:10, 0.154 1993-1964*99/1986* TCP 54 4543 > https: [ArX] Seq-530 Ack=1450 Wine5172 Len=0 794 2013-10-07 11:51:04, 20135 Lino 10:80-106*0125 Len=0 562 2013-10-67 794 2013-10-07 11:51:04, 20135 Lino 1993-1996*99/1986* TCP 54 4543 > https: [ArX] Seq-530 Ack=1450 Wine5535 Len=0 802 2013-10-07 11:51:04, 20277 10:10, 0.154 1993-1996*99/1986* TCP 54 1amer-1e > https: [ArX] Seq-26 Ack=1 Wine5535 Len=0 822 2013-10-07 11:51:04, 20277 10:10, 0.154 1994-1996*99/1986* TCP 54 1amer-1e > https: [ArX] Seq-26 Ack=1 Wine5093 Len=0 <td>732 2013-10-07 11:51:03.424015 1</td> <td>0.10.0.154</td> <td></td> <td>1930210/28201884</td> <td>TCP</td> <td>54 4543 > https [ACK] Seg=1 Ack=1 Win=65535 Len=0</td>	732 2013-10-07 11:51:03.424015 1	0.10.0.154		1930210/28201884	TCP	54 4543 > https [ACK] Seg=1 Ack=1 Win=65535 Len=0
762 2013-10-07 11:51:03.55233 10.10.0.154 993717971991788 TCP 54 454 > https: [ACK] Seq-78 Ack-1466 win-6533 Len-0 763 2013-10-07 11:51:03.55316 10.10.0.154 994496494949484 TLSVI 386 CTient Key Exchange, Change CTaher Spec, Encrypted Handshake Mes 792 2013-10-07 11:51:03.747197 10.10.0.154 994496494949484 TLSVI 192 20p1(attien Data 792 2013-10-07 11:51:03.874616 10.10.0.154 99449649494949484 TCP 54 4543 > https: [TXN, Seq-530 Ack=1850 win-65172 Len-0 794 2013-10-07 11:51:03.876166 10.10.0.154 109449649494966 TCP 54 4543 > https: [TXN, Seq-530 Ack=1850 win-65172 Len-0 794 2013-10-07 11:51:04.01156 10.10.0.154 10944964949696 TCP 54 4543 > https: [ACK] Seq-28 Ack=140 SACK_PER 800 2013-10-07 11:51:04.0120155 10.10.0.154 109491969976997696 TCP 54 1amer-1e > https: [ACK] Seq-28 Ack=1 win-65535 Len-0 842 2013-10-07 11:51:04.127077 10.10.0.154 10949196499769976997696 TLSVI 183 CTient Heal De 822 2013-10-07 11:51:04.127077 10.10.0.154 1094964964964966 TLSVI 183 CTient Heal De 185 CTient Heal De 185 CTient Heal De 185 CTient Heal De <td>734 2013-10-07 11:51:03.424384 1</td> <td>0.10.0.154</td> <td></td> <td>199/110/1197/11884s</td> <td>TLSv1</td> <td>131 Client Hello</td>	734 2013-10-07 11:51:03.424384 1	0.10.0.154		199/110/1197/11884s	TLSv1	131 Client Hello
763 2013-10-07 11:51:03.53316 10:10.0.154 10:40:40:40:40:40:40:40:40:40:40:40:40:40	762 2013-10-07 11:51:03.552735 1	0.10.0.154	OGS Test 1	1997110.137.188	TCP	54 4543 > https [ACK] Seq=78 Ack=1486 Win=65535 Len=0
779 2013-10-07 11:51:03,747197 10.10.0.0.154 199400000000000000000000000000000000000	763 2013-10-07 11:51:03.553816 1	0.10.0.154		1930230/05820188+	TLSv1	368 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mes
792 2013-10-07 11:51:03,874861 10:10.0.154 19971797/1988 TCP 54 454 > https: [AKX] Saq-530 Ack.4850 win-65172 Len=0 793 2013-10-07 11:51:03,87033 10:10.0.154 100:100:000 TCP 54 454 > https: [TN:, ACX] Saq-530 Ack.4850 win-65172 Len=0 794 2013-10-07 11:51:03,87033 10:10.0.154 100:100:000 TCP 54 1amer-1e > https: [STN] Saq-530 Ack.1850 win-65153 Len=0 MSS-1460 MACK_PERM 809 2013-10-07 11:51:04,00156 10:10.0.154 100:100:0156 TCP 54 1amer-1e > https: [ACK] Saq-530 Ack.1 win-65535 Len=0 810 2013-10-07 11:51:04,00156 10:0.0.154 100:010:010:010:010 10:0.0.154 100:010:000 822 2013-10-07 11:51:04,001691 10:10.0.154 100:010:000 11:51:04 10:02:000 822 2013-10-07 11:51:04,212077 10:10.0.0154 100:010:000 11:51:04 10:02:000 844 2013-10-07 11:51:04,224401 10:10.0.0154 10:00:000 11:51:04 10:02:000 844 2013-10-07 11:51:04:324040 10:10:0.0154 10:00:010:0.0154 10:00:010:0.0154 10:00:010:0.0154 844 2013-10-07 11:51:04:3240 10:0.0.0154 10:00:010:000 10:00:010:0.0154 <t< td=""><td>779 2013-10-07 11:51:03.747197 1</td><td>0.10.0.154</td><td></td><td>2931/2261/2321/28841</td><td>TLSV1</td><td>192 Application Data</td></t<>	779 2013-10-07 11:51:03.747197 1	0.10.0.154		2931/2261/2321/28841	TLSV1	192 Application Data
793 2013-10-07 11:51:03.876168 10.10.0.154 100.10.054 794 2013-10-07 11:51:03.87031 10.00.154 100.10.054 809 2013-10-07 11:51:04.20155 10.00.154 100.10.054 809 2013-10-07 11:51:04.20155 10.00.154 100.10.054 809 2013-10-07 11:51:04.20155 10.10.0.154 100.10.054 810 2013-10-07 11:51:04.20155 10.10.0.154 100.10.0.154 827 2013-10-07 11:51:04.20207 10.10.0.154 100.10.0.154 847 2013-10-07 11:51:04.22707 10.10.0.154 100.10.0.154 847 2013-10-07 11:51:04.224841 10.10.0.134 005 Tert 2 848 2013-10-07 11:51:04.224841 10.10.0.134 100.0134 844 2013-10-07 11:51:04.234841 10.10.0.134 100.0134 842 2013-10-07 11:51:04.234841 10.10.0.134 100.003440000000000000000000000000000000	792 2013-10-07 11:51:03.874861 1	0.10.0.154		199719971379188	TCP	54 4543 > https [ACK] Seq=530 Ack=1850 win=65172 Len=0
794 2013-10-07 11:51:03.877037 10:10.0.554 100% state and stat	793 2013-10-07 11:51:03.876186 1	0.10.0.154		103+10+132+588+	TCP	54 4543 > https [FIN, ACK] Seq=530 Ack=1850 Win=65172 Len=0
800 2013-10-07 11:51:04.00135 10:0.0.154 100:01356 10:0.0.154 100:01356 10:0.0.154 10:0.0.154 810 2013-10-07 11:51:04.001356 10:0.0.154 10:0.10.0.154 10:0.10.0.154 10:0.10.0.154 10:0.10.0.154 10:0.10.0.154 10:0.0.154 10:0.0.154 <td>794 2013-10-07 11:51:03.877037 1</td> <td>0.10.0.154</td> <td></td> <td>103-120-082-289-1-</td> <td>TCP</td> <td>62 lanner-lm > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM</td>	794 2013-10-07 11:51:03.877037 1	0.10.0.154		103-120-082-289-1-	TCP	62 lanner-lm > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
810 2013-10-07 11:51:04.200310 0.05 Tent 2 104 coldadation with weather weat	809 2013-10-07 11:51:04.001356 1	0.10.0.154		1001110012320188	TCP	54 lanner-le > https [ACK] Seg=1 Ack=1 Win=65535 Len=0
827 2013-10-07 11:51:04.127077 10:10.03.134 OPS Test 2 100 Champe Cipher Spec, Encrypted Handshake Message 828 2013-10-07 11:51:04.127077 10:10.00.0134 1997199/1997199 11:51:04 122 Application Data 844 2013-10-07 11:51:04.225410 10:0.00.0134 1997199/1997199 11:51:04 122 Application Data 844 2013-10-07 11:51:04.255410 10:0.00.0134 1997199/1997199 10:0.00.0100.0100.0134 1997199/1997199 846 2013-10-07 11:51:04.255775 10:10.0.0154 1997199/1997199 TCP 54 Jammer-1m > https [FIN, ACX] Seq-29 Ack-444 Win-65093 Lem-0 846 2013-10-07 11:51:04.255775 10:10.0.0154 1997199/1997199 TCP 64 pds-adppiw-db > https [SIN] Seq-0 Win-65535 Lem-0 WSS-1460 SACK_ 857 2013-10-07 11:51:04.252775 10:10.0.0.154 1997199/1997199 TLSVL 10:0.1000.0154 1997199/1997199 866 2013-10-07 11:51:04.252775 10:10.0.0.154 1997199/1997199 TLSVL 10:0.1000.0154 1997199/1997199/1997199 866 2013-10-07 11:51:04.252775 10:10.0.0.154 1997199/1997199/1997199/1997199/1998 TLSVL 10:0.1000.0154<	810 2013-10-07 11:51:04.001693 1	0.10.0.154		193:019:010:02:038a	TLSv1	163 Client Hello
828 2013-10-07 113:104.129313 10.10.0.134 1997/1997/1996 TLSVL 192 Application Data 844 2013-10-07 113:104.219313 10.10.0.134 484343434344444 FCP 54 lammer-lm > https [CKS] Seq=295 Ack=444 win=65093 Len=0 845 2013-10-07 11:31:04.254560 10.10.0.154 19944344484444 FCP 54 lammer-lm > https [CKS] Seq=295 Ack=444 win=65093 Len=0 846 2013-10-07 11:31:04.254560 10.10.0.154 199443444844 FCP 54 lammer-lm > https [SKN] Seq=0 win=65353 Len=0 846 2013-10-07 11:31:04.254560 10.10.0.154 1994494494646 FCP 64 particle partin particle particle particle partin particle particle	827 2013-10-07 11:51:04.127077 1	0.10.0.154	OGS Test 2	\$99/636/632/2884×	TLSv1	101 Change Cipher Spec, Encrypted Handshake Message
844 2013-10-07 11:51:04,234441 10:10:0.0.134 100:10:00:104 100:1	828 2013-10-07 11:51:04.129515 1	0.10.0.154		T977T97797797798	TLSv1	192 Application Data
845 2013-10-07 11:51:04,255775 10:10:0.154 89% addedbables TCP 54 lammer-lm > https [FIN, ACK] Seq-295 Ack-444 win-65093 Lem-0 846 2013-10-07 11:51:04,352456 00:10:0.0.154 1999 1199 1999 1996 TCP 62 gds-adppiw-db > https [SIN] Seq=0 win-65535 Lem-0 WSS-1640 SACKE 856 2013-10-07 11:51:04,332452 10:10:0.154 1999 1199 1999 1996 TCP 54 gds-adppiw-db > https [SIN] Seq=0 win-65535 Lem-0 WSS-1640 SACKE 857 2013-10-07 11:51:04,332451 10:10:0.154 1999 1199 1199 1199 1199 1199 TCP 54 gds-adppiw-db > https [SIN] Seq=205 Ack-444 win-65033 Lem-0 867 2013-10-07 11:51:04,312451 10:10:0.154 1999 1199 1199 1199 1199 1199 1199 119	844 2013-10-07 11:51:04.254843 1	0.10.0.154		193okkiekidukiekiekiekiekiekiekiekiekiekiekiekiekiek	TCP	54 lanner-lm > https [ACK] Seg=295 Ack=444 Win=65093 Len=0
846 2013-10-07 11:51:04,253775 10:10:0,0.154 1994*P109*1996# TCP 62 pds-adpriv=cb > https:[5:W] Seq=0 win=65335 Len=0 MSS=1460 SACL. 856 2013-10-07 11:51:04,35245 10:10:0.0.154 1994*P109*1998*1886 TCP 54 pds-adpriv=cb > https:[5:W] Seq=0 win=65535 Len=0 MSS=1460 SACL. 857 2013-10-07 11:51:04,35245 10:10:0.0.154 1994*P109*199*188* TCS 163 Client: He11o 866 2013-10-07 11:51:04,35245 10:10:0.154 1995*P109*199*188* TLSVI 101 Change Cipher Spec, Encrypted Handshake Message 867 2013-10-07 11:51:04,51:258 TLSVI 101 Change Cipher Spec, Encrypted Handshake Message 895 2013-10-07 11:51:04,51:258 TLSVI 192 Application Data 895 2013-10-07 11:51:04,51:258 TLSVI 192 Application Data 895 2013-10-07 11:51:04,51:258 TLSVI 192 Application Data 895 2013-10-07 11:51:04,61:05:01:0.0.0.554 1994:090:930:088* TCP 54 pd5-adppiw-db > https: [ACK] Seq=205 Ack=444 win=65093 Len=0 895 2013-10-07 11:51:04,61:05:01:0.0.0.554 1994:090:930:088* TCP 54 pd5-adppiw-db > https: [ACK] Seq=205 Ack=444 win=65093 Len=0	845 2013-10-07 11:51:04.254860 1	0.10.0.154		190x0100x132x10884x	TCP	54 lanner-lm > https [FIN, ACK] Seg=295 Ack=444 Win=65093 Len=0
856 2013-10-07 11:51:04.382426 10:10.0.0.154 100410000504080 TCP 54 pds-adpplw-db > https [ACK] Seq=1 Ack=1 win=65535 Len=0 857 2013-10-07 11:51:04.382941 10:10.0.154 10051000100010 TLSVI 163 CTient HeTI0 866 2013-10-07 11:51:04.510365 10:0.0.154 1005100100010 TLSVI 101 Change Cipher Spec, Encrypted Handshake Message 867 2013-10-07 11:51:04.510365 10:0.0.154 1005100100010 10:0.154 867 2013-10-07 11:51:04.510565 10:0.0.154 10:0.154 10:0.154 867 2013-10-07 11:51:04.630659 10:0.0.154 10:0.154 10:0.154 895 2013-10-07 11:51:04.630659 10:0.0.154 10:0.154 10:0.154 895 2013-10-07 11:51:04.630659 10:0.0.154 10:0.154 10:0.154 895 2013-10-07 11:51:04.640165 10:0.0.154 10:0.154 10:0.154	846 2013-10-07 11:51:04.255775 1	0.10.0.154		299722012321208	TCP	62 gds-adppiw-db > https [SVN] Seq=0 win=65535 Len=0 MSS=1460 SACK_
857 2013-10-07 11:51:04, 332941 10.10, 0.154 1991*190*199188* TLSVI 163 Citent mello 866 2013-10-07 11:51:04, 512581 10.10, 0.154 1991*190*1997*188* TLSVI 101 Change Cipher Spec, Encrypted Handshake Message 867 2013-10-07 11:51:04, 512581 10.10, 0.154 1991*190*1997*188* TLSVI 192 Application Data 895 2013-10-07 11:51:04, 512581 10.10, 0.154 1991*099*1930*188* TCP 54 pd5-adppiv=db > https Ack=444 wine5093 Len=0 895 2013-10-07 11:51:04, 610565 10.10, 0.154 1991*09*199*199*199*189* TCP 54 pd5-adppiv=db > https Ack=444 wine5093 Len=0	856 2013-10-07 11:51:04.382426 1	0.10.0.154		1001110:132:088=	TCP	54 gds-adpp1w-db > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
866 2013-10-07 11:51:04.510362 10.10.0.154 DOS Text 3 1997110/19971586 TLSv1 101 Change Cipher Spec, Encrypted Handshake Message 867 2013-10-07 11:51:04.512581 10.10.0.154 14900140018086 TLSv1 192 AppTication Data 895 2013-10-07 11:51:04.630550 100.0.0.154 199914001939/1886 TCP 54 pdf-adppIweb https [ACK] Seq=205 Ack=444 wine55093 Len=0 896 2013-10-07 11:51:04.640162 10.10.0.154 199311001393/1886 TCP 54 pdf-adppIweb > https [ACK] Seq=205 Ack=444 wine55093 Len=0	857 2013-10-07 11:51:04.382941 1	0.10.0.154		199:199:199:1988da	TLSv1	163 Client Hello
867 2013-10-07 11:51:04.512581 10.10.0.154 199x1990:99x19888 TCP 54 gds-adppiw-db > https:[ACK] Seq=295 Ack=444 win=65093 Len=0 895 2013-10-07 11:51:04.640165 10.10.0.154 199x1990:99x19888 TCP 54 gds-adppiw-db > https:[T1N, ACK] Seq=295 Ack=444 win=65093 Len=0	866 2013-10-07 11:51:04.510362 1	0.10.0.154	OGS Test 8	193.110.132.188	TLSv1	101 Change Cipher Spec, Encrypted Handshake Message
895 2013-10-07 11:51:04.639659 10.10.0.154 1995/0109/0586 ¹⁰ TCP 54 gds-adpp/w-db > https: [ACK] Seq=295 Ack=444 wine65093 Len=0 896 2013-10-07 11:51:04.640162 10.10.0.154 1995/0109/159/1886 TCP 54 gds-adpp/w-db > https: [VIN, ACK] Seq=295 Ack=444 wine65093 Len=0	867 2013-10-07 11:51:04.512581 1	0.10.0.154		19302390058202884	TLSv1	192 Application Data
895 2013-10-07 11:51:04.640162 10.10.0.154	895 2013-10-07 11:51:04.639659 1	0.10.0.154		193-114-0-1232-1288-0	TCP	54 gds-adpp1w-db > https [ACK] Seq=295 Ack=444 Win=65093 Len=0
	896 2013-10-07 11:51:04.640162 1	0.10.0.154		193.110.132.188	TCP	54 gds-adpp1w-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:

000	S 627494747.pcapng [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]	
Elle Edit View Go Capture Analyze Statistics Telepho	ny Iools Internals Help	
雙聲聲聲覺覺 = 23 X 23 = 4, 4 4	• 🗢 🐺 🛓 🔲 🖼 I Q, Q, Q, 🗹 I 🐺 🕅 ங 🐇 I 😫	
Filter: ip.addr == 10.10.0.154 - 6	pression Clear Apply	
No. Time • Source Destination	Protocol Length Info	
677 1361161063.040 30.10.0 354 355 116 555 105	62 4542 > https: [Shh] Segr0 Winn65525 Lanno MSSn1460 SACK_PGRMm1 deavon for first pr	abe
688 1381161063.364 193.10 Mark Packet (toggle)	62 https > 4542 [SYN, ACK] Seqn0 Ackn1 WinnB192 Lenn0 MSSn1360	
599 1391161053, 164 10.10. Ignore Packet (toggle)	54 4542 > https://ACK Segn1 Ackr1 Winn05525 Lenn0 167 Continuation Data	
708 1381161063.288 193.11 Set Time Reference (togg	e) 60 https > 4542 [ACK] Segr1 Ack=114 Win=32768 Len=0	
709 1381161063, 288 193, 11 Manually Resolve Addres:	60 https > 4542 (FIN, PSH, AOK) Segri Ack+114 Min+22768 Len+0 Fin/ack for first pro	be, the OGS calculation stops as soon as this packet
710 1361161063, 269 10.10.	54 4542 > https://ACK Septil4 Ackn2 WintCOSD Lento 54 4542 > https://EIN. ACK] Septil4 Ackn2 WintCOSDS Lento	
713 1301161003.297 10.10. Apply as filter	62 4540 > https: [Shk] Seq=0 Win=65525 Lan=0 MSS=1460 SACK_PERM=1 🛶 Syn for Sec	ond probe
729 1301161063, 412 193, 10 Prepare a Filter	60 https > 4542 (AOK) Seq=2 Ack=115 Win=32768 Len=0	and the second
730 1301161063, 414 193, 10 Conversation Filter	60 https > 4542 (RST, ACK) Seq=0 Ack=1 Win=0192 Lan=0 MSS=1360 ACK Seq=0 Ack=1 Win=0192 Lan=0 MSS=1360	
732 1301161063.424 10.10. Colorize Conversation	Seg=1 Ack=1 Win=005035 Len=0	
-C SCIP))+
Frame 677: 62 bytes on size (Follow TCP Stream Sollow UCD Stream)	ICP Color 1	
Ethernet EL, Src: statroni 12 Follow UCP Stream b Internet Protocol Manian de Follow UCP Stream	DDP P Color 2	
Transmission Control Protocol Policy SSL Stream	spe (sear), seq: 0, Left; 0 & Color 3	
Сору	Color 4	
51 Decede At	Color 5	
- Print	Color Z	
Show Packat in New Wind	ew Color 8	
STOR FROM BING	Color 9	
	Color D	
	New Coloring Bula	
	THE SECOND STREET	
0000 00 24 14 06 00 46 10 46 11 12 46 49 09 00 45 00 1	uter and the second sec	
0020 94 bc 11 be 01 bb 9c 41 2c 96 00 00 00 00 70 02		
0000 ff ff 66 00 00 02 04 05 b4 01 01 04 02f		
Ethernet (eth), 14 bytes	kets: 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:

	0 0 0 0 0 27494747.pcaping (Winshark 1.6.2 (SVN Rev 38011 from /trank-1.6))						
Elle Edit View Go Capture Analyze Statistics Telephony Tools Internals Help							
EX 84 8	< Main Toolbar						
	Eilter Toolbar		-				
Filter: ip.	 Statusbar 	pression Clear Apply	_				
No.	< Packet List	Yotocol Length Info	â				
677	< Packet Details	CP 62 4542 > https://srnil.seguel.wtr=49555.ter=0.H58=1440.540X.HEMAL					
689	< Packet Bytes	CP 52 0100 × 4042 5010 4001 5000 40043 Minetics Letter Society	М				
690	Time Director Factoriat	6 MR Continuation Pate					
708	Line Doplay Format	Time of Darie (10/2)/2 1/3/458 Critical 2/3/458 Critical 2/3/458	П				
710	< Colorize Packet List	Strends Since (1970-01-01)-1124567200 (22456 October 2	П				
711	< Auto Scroll in Live Capture	Seconds Since Reginning of Capture: 123.123455 Ctrl+Ak+4 u					
729		Seconds Since Previous Captured Packet: 1,123456 Ctrl+Ak+5	П				
720	Q Zoom In Ctri	** Seconds Since Previous Displayed Packet: 1.123456 Ctrl+AR+6	H				
732	Q 200m Qut Ctr	Automatic (File Forent Perdicion)	ų,				
•	E Pariza All Columns Shift A Cr	Standard (
D Frame 67	Displayed Columns Smith Col	Decomos o					
> Enternet	Dipages Columns	Certiseneds: 0.12					
P Transmis	Expand Subtrees Shift+R	Milliseconds: 0.123					
	Expand All COVI+R	Microseconds: 0.123456					
	Collapse gli Ctri+	Nanoseconds: 0.123456789					
	Colorize Conversation	Display Seconds with hours and minutes Chrl+At+0					
	Reset Coloring 1–10 Ctrl+Sp	ce					
	Scoloring Rules						
	Show Packet in New Window						
	Beload Ctr	+2					
0000	· · · · · · · · · · · · · · · · · · ·		-				
0010 00 34	0 fd 1d 40 00 80 06 00 00 0a 0a 00 9a c1 6e	.9					
0020 94 bs 0030 ff ff	c 11 be 01 bb 9c 41 2c 96 00 00 00 00 70 02 f 66 00 00 00 02 04 05 b4 01 01 04 02	······································					
Etherne	t (eth), 14 bytes	Packets: 1538 Displayed: 61 Marked: 0 Load time: 0:10.992 Profile: Default	12				

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

o

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。」