AnyConnect最佳的网关选择排除故障指南

目录

简介

本文描述如何排除故障与最佳的网关选择(OGS)的问题。OGS是能使用为了确定的功能哪个网关有和连接到该网关的最低的往返时间(RTT)。一能使用OGS功能为了最小化互联网数据流的延迟，不用用户干涉。使用巩固网关为连接或重新连接是最佳的OGS， Cisco AnyConnect安全移动客户端(AnyConnect)识别并且选择。OGS开始在第一个连接或在重新连接在上一个断开以后的至少四个小时。更多信息可以在管理员指南找到。

> **提示**：OGS工作最佳与最新的AnyConnect客户端和ASA软件版本9.1(3) *或以后。

OGS如何工作？

简单互联网控制消息协议(ICMP) **ping请求不**工作，因为许多思科可适应安全工具(ASA)防火墙配置阻塞ICMP数据包为了防止发现。反而，客户端发送三HTTP/443请求对在所有配置文件**合并**出现的每头端。这些HTTP探测器被称为OGS在日志ping，但是，如前所述，他们不是ICMP Ping。为了保证a (关于)连接不采取太长， OGS选择上一个网关默认情况下，如果在七秒以内不收到任何OGS ping结果。(请寻找**OGS ping导致**日志。)

> **注意**：AnyConnect应该发送HTTP请求到443，因为答复是重要，不是一成功的答复。不幸地，代理处理的修正发送所有请求作为HTTPS。请参阅Cisco Bug ID CSCtg38672 - OGS应该ping与HTTP请求。

> **注意**：如果没有头端在缓存， AnyConnect首先发送一个HTTP请求为了确定是否有认证代理

，并且是否能处理请求。是在此初始请求之后开始OGS ping为了探查服务器。

- OGS确定根据网络信息的用户位置，例如域名系统(DNS)后缀和DNS服务器IP地址。RTT结果，与此位置一起，在OGS缓存存储。

- OGS位置条目被缓存14天。归档Cisco Bug ID CSCtk66531使这些设置用户可配置的。

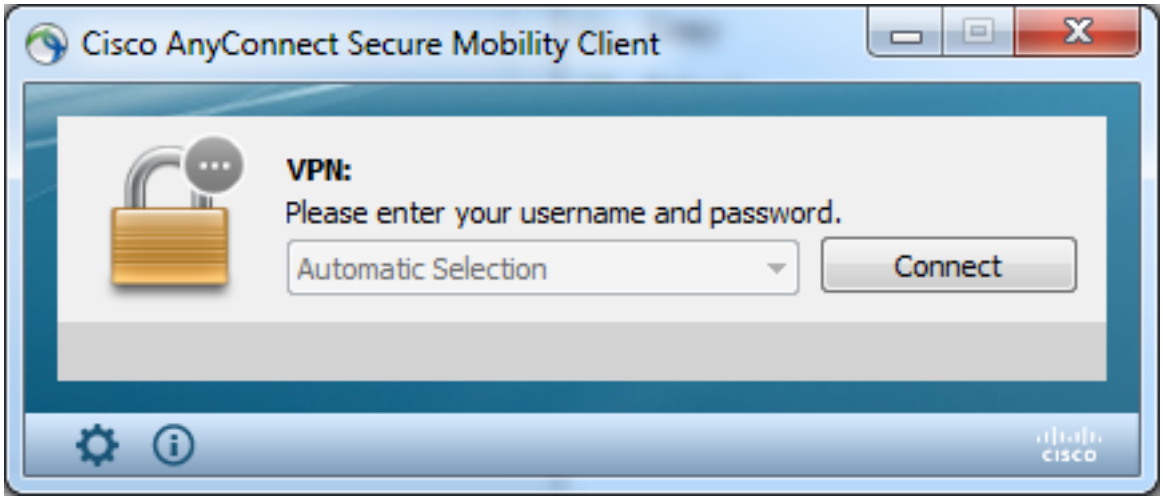
- 14天，在首先缓存后， OGS从此位置再没有运行直到位置条目。在此时间，它使用缓存的条目和RTT确定该位置。这意味着，当AnyConnect再时开始，再次不表演OGS;反而，它在缓存使用最佳的网关命令该位置。在诊断AnyConnect报告工具(箭)日志，此消息被看到：

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

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

- RTT确定与对用户将设法连接如指定由在AnyConnect配置文件的主机条目网关的安全套接字协议层(SSL)端口的TCP交换。

  注意： 不同于HTTP PING，执行一简单HTTP发表物然后显示RTT和结果， OGS计算是轻微更加复杂的。AnyConnect发送每个服务器的三台探测器，并且计算派出的HTTP SYN和FIN/ACK之间的延迟这些探测器中的每一台的。它然后使用Delta的最低为了比较服务器和做其选择。因此，即使HTTP ping是哪个服务器的一个相当好的征兆AnyConnect将选择，他们也许不一定相符。有关于此的更多信息在本文的其余。
- 目前， OGS只进行检查用户是否从挂起出来，并且阈值被超出了。如果ASA用户连接对失败或变得不可用， OGS不连接对不同的ASA。OGS联系在配置文件的仅主服务器为了确定最佳一个。

- 一旦OGS客户端配置文件下载，当用户重新启动AnyConnect客户端，中的选项其他配置文件变灰如显示此处：



即使用户计算机有多个其他配置文件他们不能选择任何一个，直到OGS disbaled。

OGS缓存

一旦计算完成，结果在**preferences_global**文件存储。有与在文件以前不存储的此数据的问题。

参考的Cisco Bug ID CSCtj84626欲了解更详细的信息。

位置确定

OGS高速缓冲存储在DNS域和各自的DNS服务器IP地址的组合工作。它工作如下：

- 位置A有**locationa.com**一个DNS域和两个DNS服务器IP地址- **ip1**和**ip2**。每个domain/IP组合创建缓存密钥对OGS缓存条目的该点。例如： **locationa.com|ip1 - > ogscache1locationa.com|ip2 - > ogscache1**
- 如果AnyConnect然后连接对物理的不同的网络， domain/IP组合同一积累根据被缓存的列表创建并且核对。如果有任何匹配，使用该OGS缓存值，并且客户端仍然认为在**位置A。**

故障情景

这是用户也许遇到的一些故障情景：

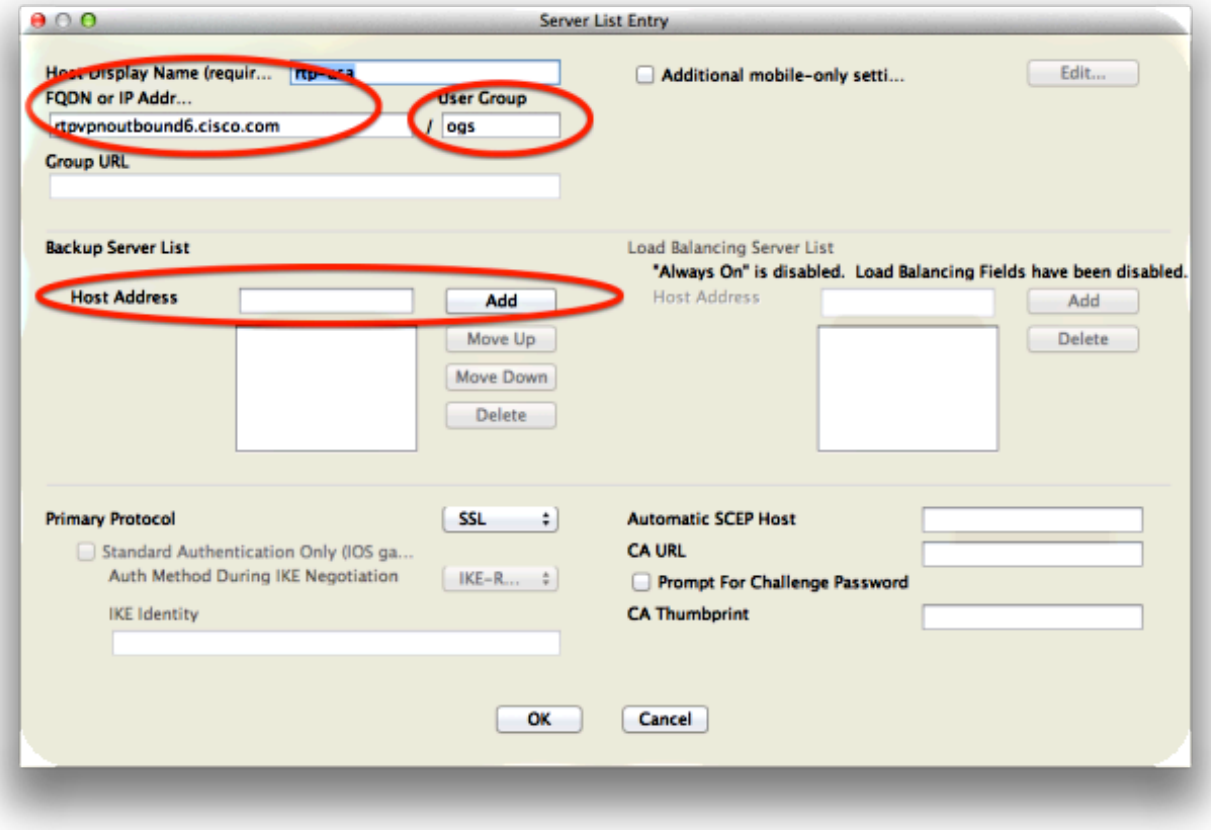
当对网关的连接丢失

当使用时OGS，如果对用户连接的网关的连接丢失，然后AnyConnect连接到在**备份服务器listandnot的**服务器到下台OGS主机。运算顺序如下：

1. OGS联系仅主服务器为了确定最佳一个。

2. 一旦确定，连接算法是：
   尝试连接到最佳的服务器。如果那发生故障，请尝试最佳的服务器的备份服务器列表。如果那发生故障，请尝试在OGS选择列表保持的每个服务器，定购由其选择发生。

   注意：当管理员配置备份服务器列表时，当前配置文件编辑器只允许管理员输入备份服务器的完全合格的域名(FQDN)，但是不是用户组象为主服务器可能的：



归档Cisco Bug ID CSCud84778为了更正此，但是在备份服务器的主机地址字段必须输入完整URL，并且应该工作：**https://*<ip-address>*/*usergroup***。

在挂起以后的恢复

为了OGS能运行，在恢复， AnyConnect一定有已建立连接后，当计算机放置休眠。OGS，在恢复只执行后，在网络环境测验发生后，被认为确认网络连通性是可用的。此测验包括subtest DNS的连接。

然而，如果DNS服务器丢包在查询字段键入A请求用一个IP地址，与应答与“没找到的名称” (更加普通的案件，总是遇到在测验期间)，然后Cisco Bug ID CSCti20768 “类型A的DNS查询相对IP地址的，应该是避免超时的PTR”应用。

TCP延迟ACK窗口大小选择不正确网关

当早于版本9.1(3)使用时ASA版本，在客户端的捕获显示SSL握手的不变延迟。什么被注意是客户端发送其ClientHello，然后ASA发送其ServerHello。这由身份验证消息(可选证书请求)和ServerHelloDone消息通常跟随。异常情况是二倍的：

1. ASA不在ServerHello以后立即发送身份验证消息。客户端窗口大小是64,860个字节，足够是保持从ASA的整个答复。

2. 客户端不立即ACK ServerHello，因此ASA在~120ms以后重新传输ServerHello，到时客户端ACK数据。然后身份验证消息发送。它几乎是，好象客户端等待更多数据。

这发生由于TCP缓慢启动和TCP延迟ACK之间的交互作用。在ASA版本9.1(3)之前， ASA使用缓慢启动窗口大小1，而Windows客户端使用延迟ACK值为2。这意味着ASA只发送一个数据包，直到获得ACK，但是也意味着客户端不发送ACK，直到收到两个数据包。ASA时代，在120ms和重新传输ServerHello后，在后客户端ACK数据和连接继续。 此行为由Cisco Bug ID CSCug98113更改默认

情况下，以便ASA使用一个缓慢的Start窗口大小2而不是1。

这能影响OGS计算，当：

- 不同的网关运行不同的ASA版本。
- 客户端有不同的延迟ACK窗口大小。

在这些情况下，延迟ACK介绍的延迟能是满足造成客户端选择错误的ASA。 如果此值有所不同在客户端和ASA之间，可能仍然有问题。在这些情况下，应急方案是调节延迟的确认窗口大小。

Windows

1. 开始**登记编辑**。
2. 识别您要禁用延迟ACK接口的GUID。为了执行此，请导航对：
   HKEY_LOCAL_MACHINE>SOFTWARE> Microsoft >视窗NT > CurrentVersion > NetworkCards > (编号)。
   查看每个编号列出在NetworkCards下。在右边，说明应该列出接口(例如，英特尔(R)无线WiFi林克5100AGN)和Servicename应该列出对应的GUID。
3. 找出然后单击此注册子键：
   HKEY_LOCAL_MACHINE \系统\ Currentcontrolset \服务\ Tcpip \参数\接口\ <interface GUID>
4. 在Edit菜单，对新的点，然后单击**DWORD值**。
5. 给出新的值**TcpAckFrequency**，并且赋予它值为**1**。
6. 离开登记编辑。
7. 重新启动此更改的Windows能生效。

   注意：在ASA归档Cisco Bug ID CSCum19065使TCP调整参数成为可配置。

普通用户示例

常见用途事例是，当用户第一次时在家运行OGS，它记录DNS设置，并且OGS ping缓存导致(默认为14天超时)。当用户第二天晚上时归还主页， OGS检测同样DNS设置，在缓存查找它，并且未参加OGS ping测试。以后，当用户去提供网络服务的旅馆或餐馆时， OGS在缓存检测不同的DNS设置，运行OGS ping测试，选择最好的网关，并且记录结果。

处理是相同的，当从中止或冬眠的状态时恢复，如果OGS和AnyConnect恢复设置允许它。

排除故障OGS

步骤1.清除OGS缓存为了强制再估价

为了清除OGS缓存并且复评可用的网关的RTT，删除从PC的全局AnyConnect首选文件。文件的位置变化基于操作系统(OS) ：

- Windows比斯塔和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..`

步骤2.在连接尝试期间，捕获服务器探测器

1. 开始在测验计算机的Wireshark。

2. 开始在AnyConnect的连接尝试。

3. 一旦连接完成，请终止Wireshark捕获。 **提示**：因为捕获只用于为了测试OGS，终止捕获是最佳的，当AnyConnect选择网关。因为那能覆盖数据包捕获，不通过完整连接尝试是最佳的。

步骤3.验证OGS选择的网关

为了验证OGS为什么选择一个特定的网关，请完成这些步骤：

1. 首次新连接。

2. 运行AnyConnect箭：
   启动**AnyConnect**，并且点击**先进**。点击**诊断**。单击 **Next**。单击 **Next**。
3. 检查在桌面的新建立的**文件**找到的箭结果。
   导航对**Cisco AnyConnect安全移动客户端> AnyConnect.txt**。

   注释OGS探测器为从此箭日志的一个特定服务器开始的时间：

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

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

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

   通常他们应该大概在同时是，但是，万一捕获大，数据包是HTTP探测器的时间戳帮助缩小，并且哪个是实际连接尝试。

   一旦AnyConnect发送三台探测器到服务器，此消息生成与其中每一台的结果探测器：

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

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 )

**************************************** 因为他们必须匹配捕获结果，注意这三个值是重要的。
```

寻找包含“*** OGS选择结果***”为了发现已评估RTT的消息，并且，如果最最近的连接尝试是被缓存的RTT或新核算的结果。

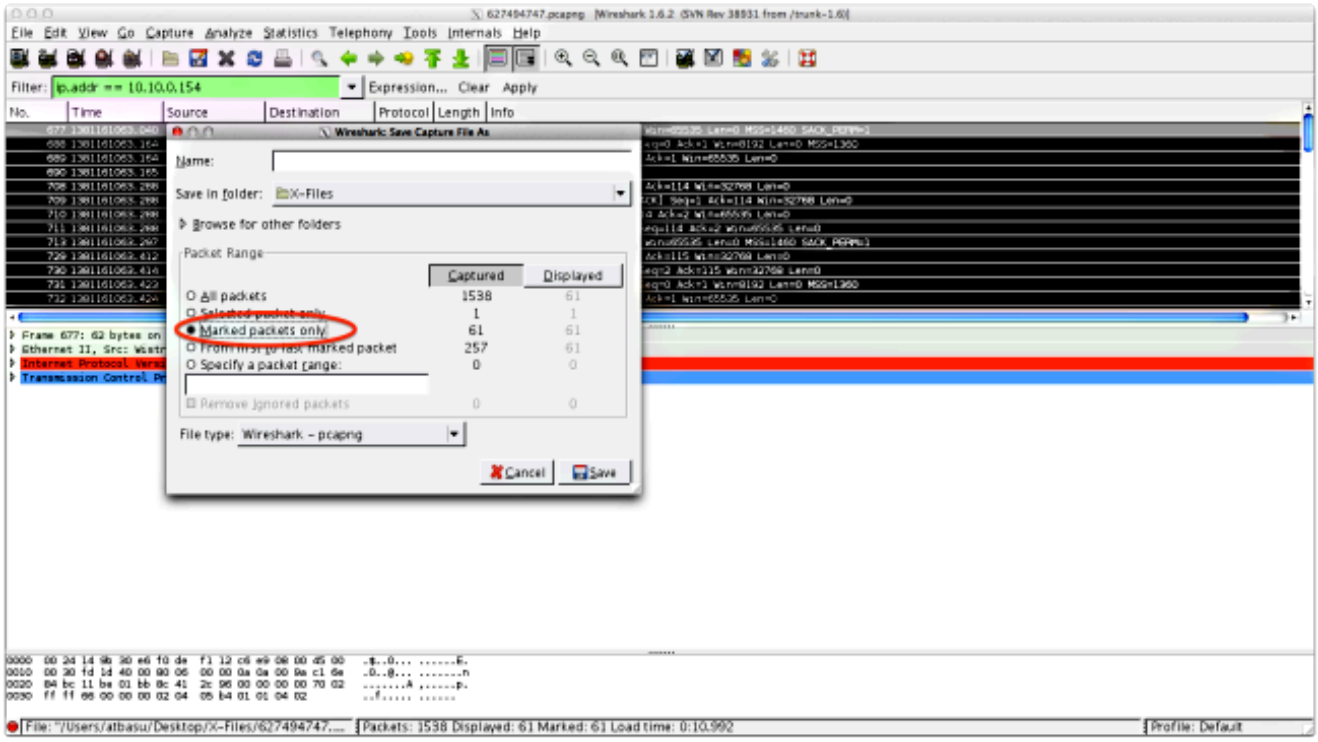
示例如下： **

```
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.

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

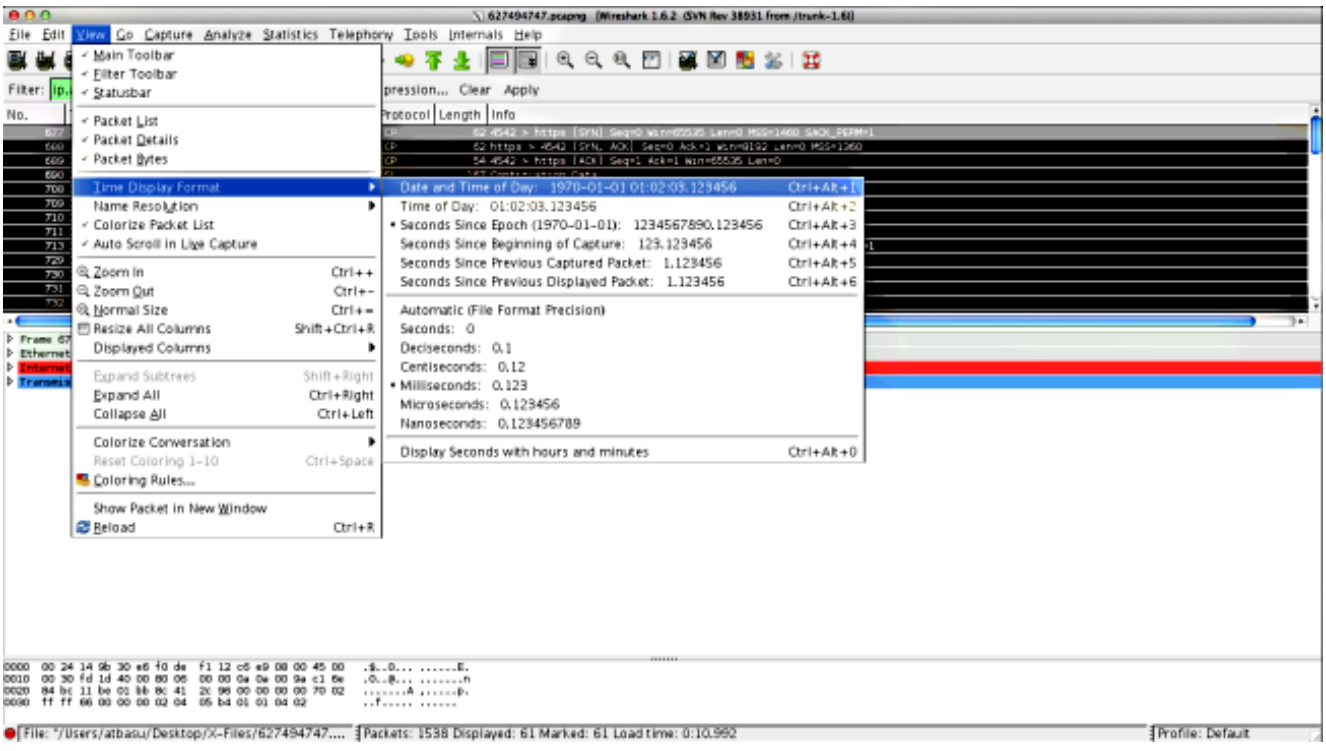
步骤4.验证AnyConnect负责的OGS计算

检查用于的TCP/SSL探测器的捕获为了计算RTT。请参阅HTTPS请求多久接收单个TCP连接。每探测器请求应该使用一不同的TCP连接。为了执行此，请打开在Wireshark的捕获，并且重复其中每一个的这些步骤服务器：

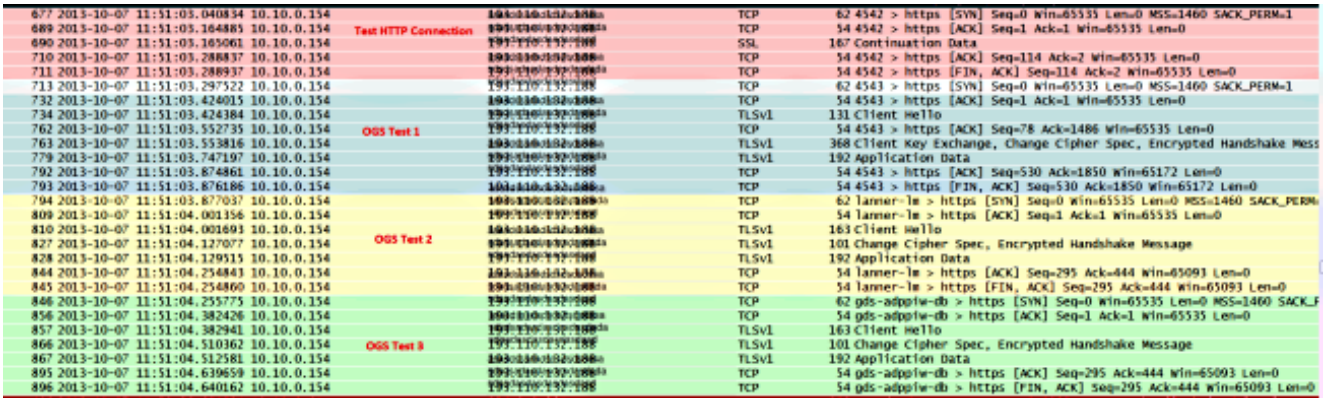
1. 请使用**ip.addr过滤器**为了离析发送的数据包其中每一个服务器到他们自己的捕获。为了执行此，导航编辑和选择MarkAll**显示数据包。然后请**导航对File > Save As**，选择**Markedpackets**唯一选择**，并且单击“Save”：



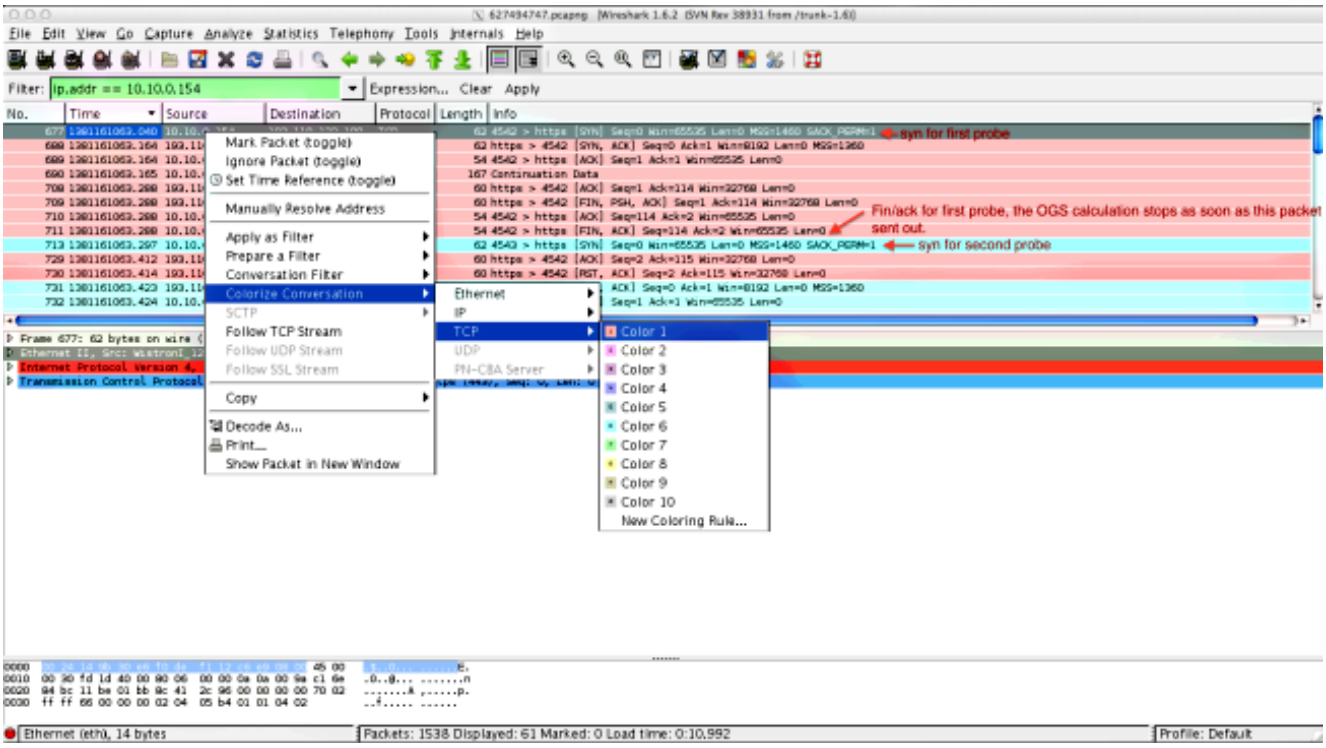
2. 在这中新的捕获，导航**查看>时间显示格式>伊达市和每日定时**：



3. 识别在发送的此捕获的第一HTTP SYN数据包，当OGS探测器在步骤3.3.2被发送了根据箭日志如识别。请记住，对于第一个服务器，第一个HTTP请求不是服务器探测器。弄错第一请求为服务器探测器和因而到达在值完全不同与是容易的什么OGS报告。此问题突出显示得此处：

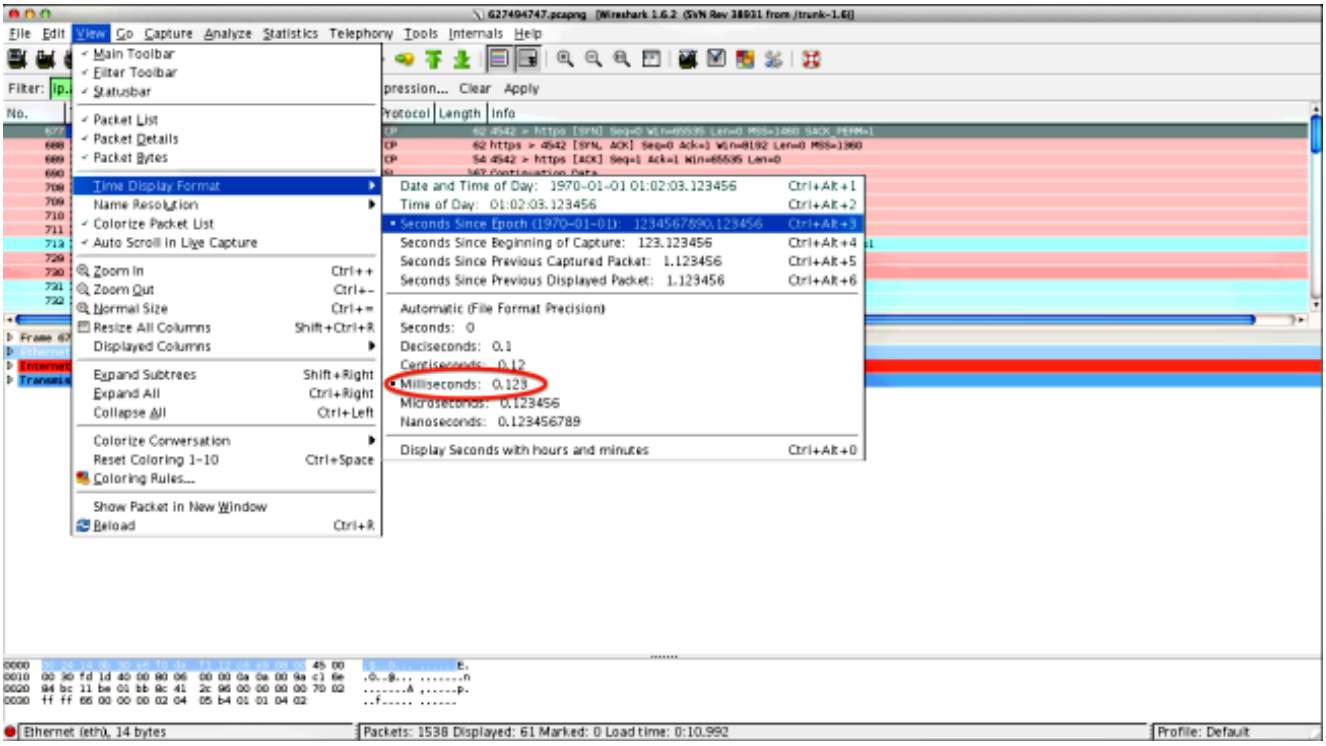


4. 为了更加容易地识别其中每一台探测器，请用鼠标右键单击第一台探测器的**HTTP SYN**，然后选择**Colorize会话**如显示此处：



重复SYN的此进程在所有探测器。如前一个镜像所显示，前两台探测器表示用不同的颜色。colorizing TCP会话优点是容易察觉重新传输或其他这样怪异每台探测器。

5. 为了更改时间显示，请导航**查看>时间显示格式>秒钟从世纪**：



选择**毫秒**，因为那是OGS使用的级别精确度。

6. 计算HTTP SYN和FIN/ACK之间的时差，如步骤4.重复所显示图表三台探测器中的每一台的此进程，并且比较值对在箭登录步骤显示的那些3.3.3。

分析

如果，在分析捕获确定的RTT值计算并且与在箭日志看到的值比较，并且后发现一切配合，但是仍然似乎类似错误的网关选择，则归结于两问题之一：

- 有在头端的一个问题。如果这是实际情形，也许有从一特定的头端的许多重新传输，或者在探测器看到的所有其他这样怪异。交换的一更加接近的分析要求。

- 有与互联网服务提供商的一问题。如果这是实际情形，也许有为一特定的头端或大延迟看到的分段。

Q&A

问： OGS与负载平衡一起使用？

回答: 可以。OGS的只知道为了判断最近的头端集群主控名称和用途。

问：OGS与在浏览器定义的代理设置一起使用？

回答:OGS不支持自动代理或代理自动设定(PAC)文件，但是支持一个硬编码代理服务器。同样地，OGS操作不发生。 相关日志消息是：“**OGS不会执行，因为自动代理检测配置**”。