AnyConnect Optimal Gateway-Auswahlhilfe

Inhalt

[Einführung](#)
[Wie wirkt OGS?](#)
[OGS-Cache](#)
[Standortbestimmung](#)
[Fehlerszenarien](#)
[Wenn die Verbindung zum Gateway unterbrochen wird](#)
[Wiederaufnahme nach Suspendierung](#)
[TCP Delayed ACK Window Size (verzögertes ACK-Fenster): Falsches Gateway](#)
[Typisches Benutzerbeispiel](#)
[Fehlerbehebung bei OGS](#)
[Schritt 1: Löschen Sie den OGS-Cache, um eine Neubewertung zu erzwingen.](#)
[Schritt 2: Erfassen der Serverproben während des Verbindungsversuchs](#)
[Schritt 3: Überprüfen des vom OGS ausgewählten Gateways](#)
[Schritt 4: Validieren der von AnyConnect ausgeführten OGS-Berechnungen](#)
[Analyse](#)
[Fragen und Antworten](#)

Einführung

In diesem Dokument wird beschrieben, wie Probleme mit der Optimal Gateway Selection (OGS) behoben werden. OGS ist eine Funktion, mit der ermittelt werden kann, welches Gateway die niedrigste Round Trip Time (RTT) aufweist und mit diesem Gateway verbunden werden kann. Man kann die OGS-Funktion verwenden, um die Latenz für Internetdatenverkehr ohne Benutzereingriff zu minimieren. Mit OGS identifiziert und wählt der Cisco AnyConnect Secure Mobility Client (AnyConnect) das sichere Gateway, das am besten für die Verbindung oder Neuverbindung geeignet ist. OGS beginnt bei der ersten Verbindung oder bei einer Neuverbindung mindestens vier Stunden nach der vorherigen Trennung. Weitere Informationen finden Sie im Administratorhandbuch.

> **Tipp**: OGS funktioniert am besten mit dem neuesten AnyConnect-Client und der ASA-Software Version 9.1(3)* oder höher.

Wie wirkt OGS?

Eine einfache ICMP-Anfrage (Internet Control Message Protocol) funktioniert nicht, da viele Firewalls der Cisco Adaptive Security Appliance (ASA) so konfiguriert sind, dass sie ICMP-Pakete blockieren, um eine Erkennung zu verhindern. Stattdessen sendet der Client drei HTTP/443-Anforderungen an jedes Headend, das in einer **Zusammenführung** aller Profile angezeigt wird. Diese HTTP-Tests werden in den Protokollen als OGS-Pings bezeichnet, aber wie bereits erläutert, handelt es sich nicht um ICMP-Pings. Um sicherzustellen, dass eine (Re-)Verbindung nicht zu lange dauert, wählt OGS standardmäßig das vorherige Gateway aus, wenn es innerhalb

von sieben Sekunden keine OGS-Ping-Ergebnisse erhält. (Suchen Sie im Protokoll nach **OGS-Ping-Ergebnissen**.)

> **Hinweis**: AnyConnect sollte eine HTTP-Anfrage an 443 senden, da die Antwort selbst wichtig ist, keine erfolgreiche Antwort. Leider sendet das Fix für die Proxy-Verarbeitung alle Anfragen als HTTPS. Siehe Cisco Bug ID CSCtg38672 - OGS sollte mit HTTP-Anfragen pingen.

> **Hinweis**: Wenn im Cache keine Headends vorhanden sind, sendet AnyConnect zunächst eine HTTP-Anfrage, um festzustellen, ob ein Authentifizierungsproxy vorhanden ist und ob die Anforderung verarbeitet werden kann. Erst nach dieser ersten Anforderung beginnt der OGS Ping, um den Server zu testen.

- OGS bestimmt den Benutzerstandort anhand der Netzwerkinformationen, z. B. dem DNS-Suffix (Domain Name System) und der IP-Adresse des DNS-Servers. Die RTT-Ergebnisse werden zusammen mit diesem Speicherort im OGS-Cache gespeichert.

- Die Einträge der OGS-Standorte werden 14 Tage lang zwischengespeichert. Die Cisco Bug-ID CSCtk66531 wurde gespeichert, um diese Einstellungen benutzerdefinierbar zu machen.

- OGS wird von diesem Ort erst 14 Tage nach dem ersten Zwischenspeichern des Standorteintrags wieder ausgeführt. Während dieser Zeit werden der zwischengespeicherte Eintrag und die für diesen Speicherort bestimmten RTTs verwendet. Das bedeutet, dass AnyConnect beim erneuten Start kein OGS mehr ausführt. Stattdessen wird die optimale Gateway-Reihenfolge im Cache für diesen Standort verwendet. Im Diagnostic AnyConnect Reporting Tool (DART)-Protokoll wird folgende Meldung angezeigt:

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

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

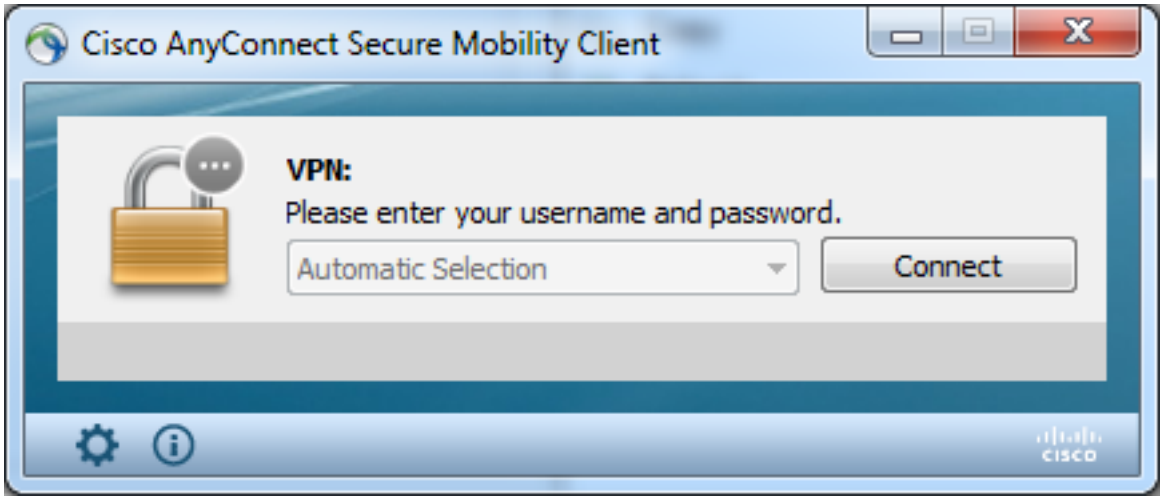
- RTT wird durch einen TCP-Austausch mit dem SSL-Port (Secure Sockets Layer) des Kabelmodems bestimmt, mit dem der Benutzer versuchen wird, eine Verbindung herzustellen, wie vom Hosteintrag im AnyConnect-Profil angegeben.

  Hinweis: Im Gegensatz zum HTTP-Ping, der einen einfachen HTTP-Beitrag ausführt und dann das RTT und das Ergebnis anzeigt, sind OGS-Berechnungen etwas komplizierter. AnyConnect sendet drei Tests für jeden Server und berechnet die Verzögerung zwischen dem gesendeten HTTP-SYN und dem FIN/ACK für jede dieser Tests. Anschließend wird der niedrigste Deltas verwendet, um die Server zu vergleichen und ihre Auswahl zu treffen. Obwohl HTTP-Pings also ein recht guter Hinweis darauf sind, welcher Server von AnyConnect ausgewählt wird, sind sie möglicherweise nicht unbedingt richtig. Weitere

Informationen hierzu finden Sie im restlichen Dokument.

- Derzeit führt OGS die Prüfungen nur aus, wenn der Benutzer aus einem Suspendiermodus kommt und der Schwellenwert überschritten wurde. OGS stellt keine Verbindung zu einer anderen ASA her, wenn die ASA, mit der der Benutzer verbunden ist, abstürzt oder nicht mehr verfügbar ist. OGS kontaktiert nur die primären Server im Profil, um den optimalen Server zu ermitteln.

- Wenn das OGS-Clientprofil heruntergeladen wurde und der Benutzer den AnyConnect-Client neu startet, wird die Option zur Auswahl anderer Profile wie folgt deaktiviert:



Selbst wenn der Benutzercomputer über mehrere andere Profile verfügt, können diese erst ausgewählt werden, wenn OGS deaktiviert ist.

OGS-Cache

Nach Abschluss der Berechnung werden die Ergebnisse in der Datei **preferences_global** gespeichert. Es gab Probleme damit, dass diese Daten zuvor nicht in der Datei gespeichert wurden.

Weitere Informationen finden Sie unter Cisco Bug ID CSCtj84626.

Standortbestimmung

Die OGS-Zwischenspeicherung funktioniert auf einer Kombination der DNS-Domäne und der einzelnen DNS-Server-IP-Adressen. Es funktioniert wie folgt:

- Standort A verfügt über eine DNS-Domäne von **locationa.com** und zwei DNS-Server-IP-Adressen - **ip1** und **ip2**. Jede Domäne/IP-Kombination erstellt einen Cacheschlüssel, der auf einen OGS-Cache-Eintrag zeigt. Beispiel: **locationa.com|ip1 -> ogscache1locationa.com|ip2 -> ogscache1**
- Wenn AnyConnect dann eine Verbindung zu einem physisch unterschiedlichen Netzwerk herstellt, wird die gleiche Erstellung von Domänen-/IP-Kombinationen erstellt und mit der zwischengespeicherten Liste abgeglichen. Wenn überhaupt Übereinstimmungen vorhanden sind, wird dieser OGS-Cache-Wert verwendet, und der Client wird weiterhin als an **Standort A** vorhanden angesehen.

Fehlerszenarien

Im Folgenden sind einige Fehlerszenarien aufgeführt, mit denen Benutzer konfrontiert werden können:

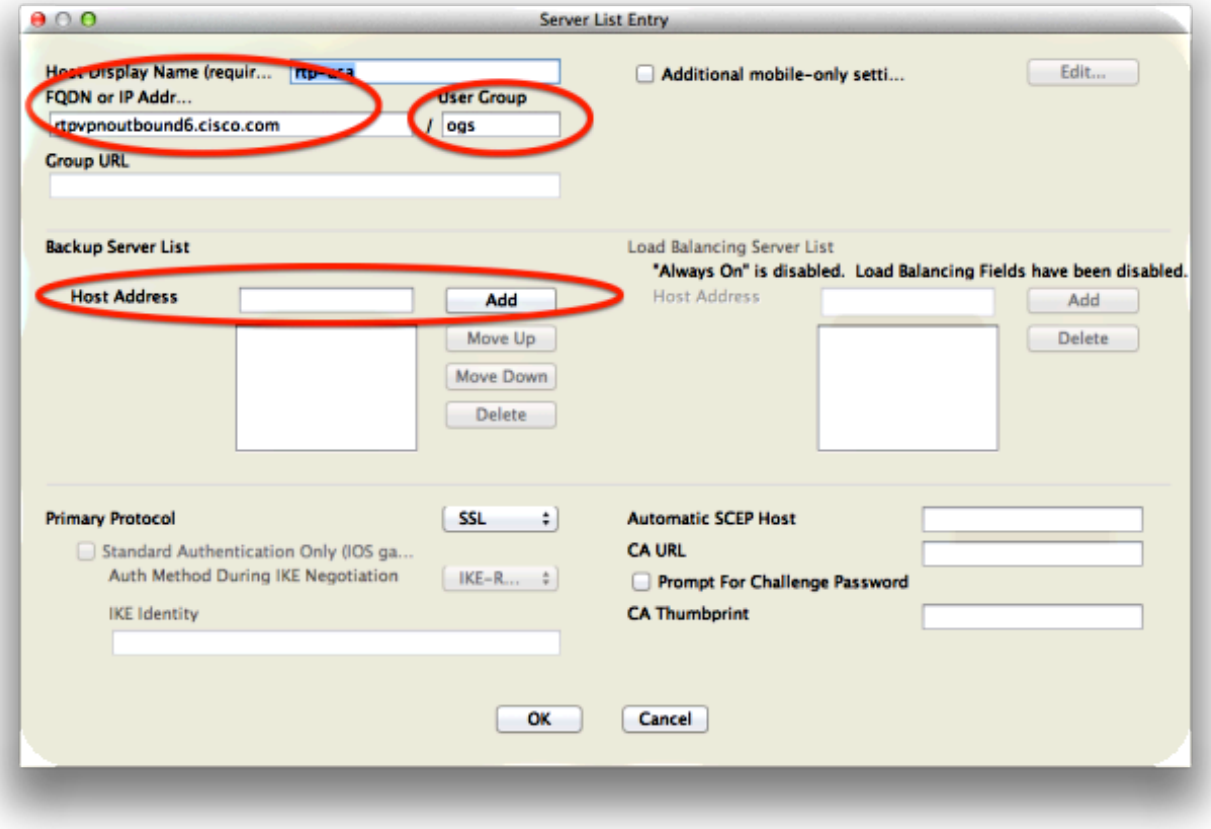
Wenn die Verbindung zum Gateway unterbrochen wird

Wenn bei Verwendung von OGS die Verbindung mit dem Gateway, mit dem die Benutzer verbunden sind, unterbrochen wird, stellt AnyConnect eine Verbindung zu den Servern in der **Sicherungsserverlisteundnicht** zum nächsten OGS-Host. Die Reihenfolge der Vorgänge ist wie folgt:

1. OGS kontaktiert nur die primären Server, um den optimalen Server zu ermitteln.

2. Nach der Bestimmung ist der Verbindungsalgorithmus wie folgt:
   Versuchen Sie, eine Verbindung zum optimalen Server herzustellen.Falls dies fehlschlägt, versuchen Sie die Liste der Backup-Server des optimalen Servers.Falls dies fehlschlägt, versuchen Sie jeden Server, der in der OGS-Auswahlliste verbleibt, geordnet nach den Auswahlergebnissen.

   Hinweis: Wenn der Administrator die Liste der Backup-Server konfiguriert, erlaubt der aktuelle Profil-Editor dem Administrator nur die Eingabe des FQDN (Fully Qualified Domain Name) für den Backup-Server, jedoch nicht der Benutzergruppe, wie dies für den primären Server möglich ist:



   Die Cisco Bug-ID CSCud84778 wurde eingegeben, um dies zu korrigieren. Die vollständige URL muss jedoch im Hostadressfeld für den Sicherungsserver eingegeben werden. Sie sollte wie folgt funktionieren: **https://*<ip-address>*/usergroup**.

Wiederaufnahme nach Suspendierung

Damit OGS nach einem Neustart ausgeführt werden kann, muss bei AnyConnect eine Verbindung hergestellt worden sein, wenn der Computer in den Ruhemodus versetzt wurde. OGS nach einer Wiederaufnahme wird nur ausgeführt, wenn die Netzwerkumgebung getestet wurde, um zu bestätigen, dass Netzwerkverbindungen verfügbar sind. Dieser Test umfasst einen DNS-Verbindungsuntertest.

Wenn der DNS-Server jedoch Anfragen vom Typ A mit einer IP-Adresse im Abfragefeld verwirft, anstatt mit "name not found" zu antworten (der häufigere Fall, der immer während der Tests auftritt), dann wird die Cisco Bug-ID CSCti20768 "DNS-Abfrage vom Typ A für IP-Adresse, sollte PTR sein, um Zeitüberschreitung zu vermeiden" gilt.

TCP Delayed ACK Window Size (verzögertes ACK-Fenster): Falsches Gateway

Wenn ASA-Versionen vor Version 9.1(3) verwendet werden, zeigen die Captures auf dem Client eine anhaltende Verzögerung im SSL-Handshake an. Es wird festgestellt, dass der Client seinen ClientHello sendet, und dann sendet die ASA seinen ServerHello. Darauf folgen normalerweise eine Zertifikatsmeldung (optionale Zertifikatsanforderung) und die ServerHelloDone-Nachricht. Die Anomalie hat zwei Aspekte:

1. Die ASA sendet die Zertifikatsmeldung nicht sofort nach dem ServerHello. Die Größe des Client-Fensters beträgt 64.860 Byte, was mehr als genug ist, um die gesamte Antwort von der ASA zu speichern.

2. Der Client speichert den ServerHello nicht sofort, sodass die ASA den ServerHello nach ca. 120 ms erneut überträgt. An diesem Punkt ruft der Client die Daten auf. Anschließend wird die Zertifikatsmeldung gesendet. Es ist fast so, als würde der Client auf weitere Daten warten.

Dies geschieht aufgrund der Interaktion zwischen TCP slow-start und TCP Delayed-ACK. Vor der ASA-Version 9.1(3) verwendet die ASA eine Zeitüberschreitungsgröße von 1, während der Windows-Client einen Wert für die verzögerte ACK von 2 verwendet. Das bedeutet, dass die ASA nur ein Datenpaket sendet, bis es ein ACK empfängt. Das bedeutet aber auch, dass der Client erst dann ein ACK sendet, wenn er zwei Datenpakete empfängt. Die ASA meldet das Zeitlimit nach 120 ms ab und überträgt den ServerHello erneut, woraufhin der Client die Daten und die Verbindung aufruft. Dieses Verhalten wurde durch die Cisco Bug-ID CSCug98113 geändert, sodass die ASA standardmäßig eine Fenstergröße für langsamen Start statt 1 verwendet.

Dies kann sich auf die OGS-Berechnung auswirken, wenn:

- Verschiedene Gateways führen verschiedene ASA-Versionen aus.
- Clients haben unterschiedliche verzögerte ACK-Fenstergrößen.

In solchen Situationen könnte die Verzögerung, die durch das verzögerte ACK eingeführt wird, ausreichen, um den Client zur Auswahl der falschen ASA zu bewegen. Unterscheidet sich dieser Wert zwischen dem Client und der ASA, können weiterhin Probleme auftreten. In solchen Situationen besteht die Problemumgehung darin, die Fenstergröße für verzögerte Bestätigungen anzupassen.

Windows

1. Starten Sie den **Registrierungs-Editor**.

2. Geben Sie die GUID der Schnittstelle an, auf der Sie die verzögerte ACK deaktivieren

möchten. Navigieren Sie dazu zu an:
HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows NT > CurrentVersion > NetworkCards > (number).
Schauen Sie sich jede Nummer an, die unter Netzwerkkarten aufgeführt ist. Auf der rechten Seite sollte die Beschreibung die Schnittstelle (z. B. Intel(R) Wireless WiFi Link 5100AGN) auflisten, und der ServiceName sollte die entsprechende GUID auflisten.

3. Suchen Sie diesen Registrierungsunterschlüssel und klicken Sie anschließend darauf:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<Interface GUID>
4. Zeigen Sie im Menü Bearbeiten auf Neu, und klicken Sie dann auf **DWORD-Wert**.
5. Nennen Sie den neuen Wert **TcpAckFrequency**, und weisen Sie ihm den Wert **1** zu.
6. Schließen Sie den Registrierungseditor.
7. Starten Sie Windows neu, damit diese Änderung wirksam wird.

Hinweis: Cisco Bug ID CSCum19065 wurde abgelegt, um TCP-Tuning-Parameter auf der ASA zu konfigurieren.

Typisches Benutzerbeispiel

Der häufigste Anwendungsfall ist, wenn ein Benutzer zu Hause OGS zum ersten Mal ausführt, die DNS-Einstellungen und das OGS-Ping die Ergebnisse im Cache aufzeichnet (standardmäßig ein Timeout von 14 Tagen). Wenn der Benutzer am nächsten Abend nach Hause zurückkehrt, erkennt OGS die gleichen DNS-Einstellungen, findet sie im Cache und überspringt den OGS-Ping-Test. Später, wenn der Benutzer zu einem Hotel oder Restaurant geht, das Internetdienste anbietet, erkennt OGS verschiedene DNS-Einstellungen, führt die OGS-Ping-Tests aus, wählt das beste Gateway aus und zeichnet die Ergebnisse im Cache auf.

Die Verarbeitung ist identisch, wenn sie aus einem temporären oder Ruhezustand wiederhergestellt wird, wenn die OGS- und die AnyConnect-Resume-Einstellungen dies zulassen.

Fehlerbehebung bei OGS

Schritt 1: Löschen Sie den OGS-Cache, um eine Neubewertung zu erzwingen.

Um den OGS-Cache zu löschen und das RTT für verfügbare Gateways neu zu bewerten, löschen Sie einfach die Datei Global AnyConnect Preferences (Globale AnyConnect-Voreinstellungen) vom PC. Der Speicherort der Datei variiert je nach Betriebssystem:

- Windows Vista und 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..
```

Schritt 2: Erfassen der Serverproben während des Verbindungsversuchs

1. Starten Sie Wireshark auf dem Testcomputer.

2. Starten Sie einen Verbindungsversuch auf AnyConnect.

3. Beenden Sie die Wireshark-Erfassung, sobald die Verbindung abgeschlossen ist. **Tipp**: Da die Erfassung nur zum Testen von OGS verwendet wird, empfiehlt es sich, die Erfassung zu beenden, sobald AnyConnect ein Gateway auswählt. Es ist am besten, keinen vollständigen Verbindungsversuch durchzuführen, da dies die Paketerfassung Cloud-fähig machen kann.

Schritt 3: Überprüfen des vom OGS ausgewählten Gateways

Gehen Sie wie folgt vor, um zu überprüfen, warum OGS ein bestimmtes Gateway ausgewählt hat:

1. Initiieren Sie eine neue Verbindung.

2. Führen Sie AnyConnect DART aus:
   Starten Sie **AnyConnect**, und klicken Sie auf **Erweitert**.Klicken Sie auf **Diagnose**.Klicken Sie auf **Weiter**.Klicken Sie auf **Weiter**.
3. Überprüfen Sie die DART-Ergebnisse aus der neu erstellten Datei **DartBundle_XXXX_XXXX.zip** auf dem Desktop.
   Navigieren Sie zu **Cisco AnyConnect Secure Mobility Client > AnyConnect.txt**.

   Beachten Sie, wann die OGS-Tests für einen bestimmten Server aus diesem DART-Protokoll gestartet wurden:

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

   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

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

   In der Regel sollten sie ungefähr zur gleichen Zeit sein, aber bei umfangreichen Aufnahmen hilft der Zeitstempel, die Pakete einzugrenzen, welche die HTTP-Sonden sind und welche die eigentlichen Verbindungsversuche sind.

Sobald AnyConnect drei Sonden an den Server sendet, wird diese Nachricht mit den Ergebnissen für jede der Sonden generiert:

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

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 ist wichtig, diese drei Werte zu beachten, da sie mit den Erfassungsergebnissen übereinstimmen müssen.

Achten Sie auf die Meldung "*** OGS Selection Results***" (Ergebnisse der OGS-Auswahl**), um den ausgewerteten RTT anzuzeigen, und ob der letzte Verbindungsversuch das Ergebnis eines zwischengespeicherten RTT oder einer neuen Berechnung war.

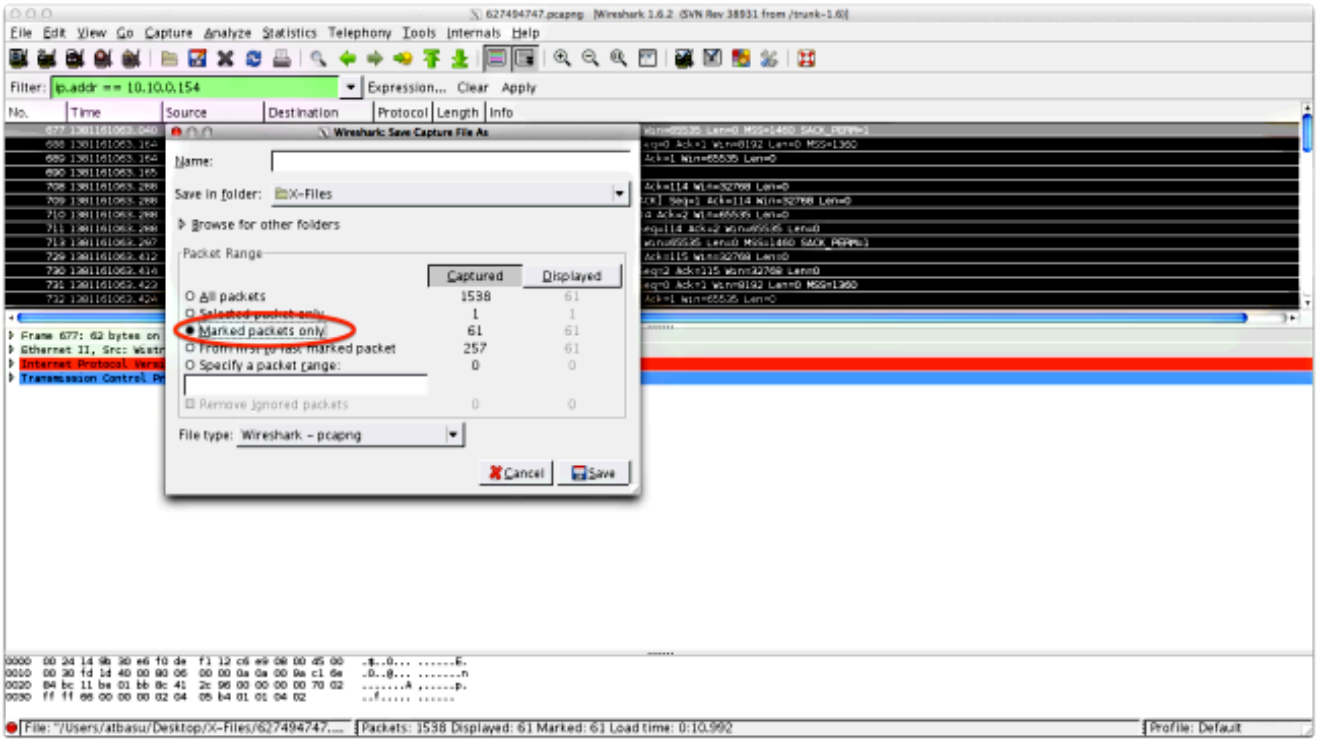
Hier ein Beispiel:

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

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.

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

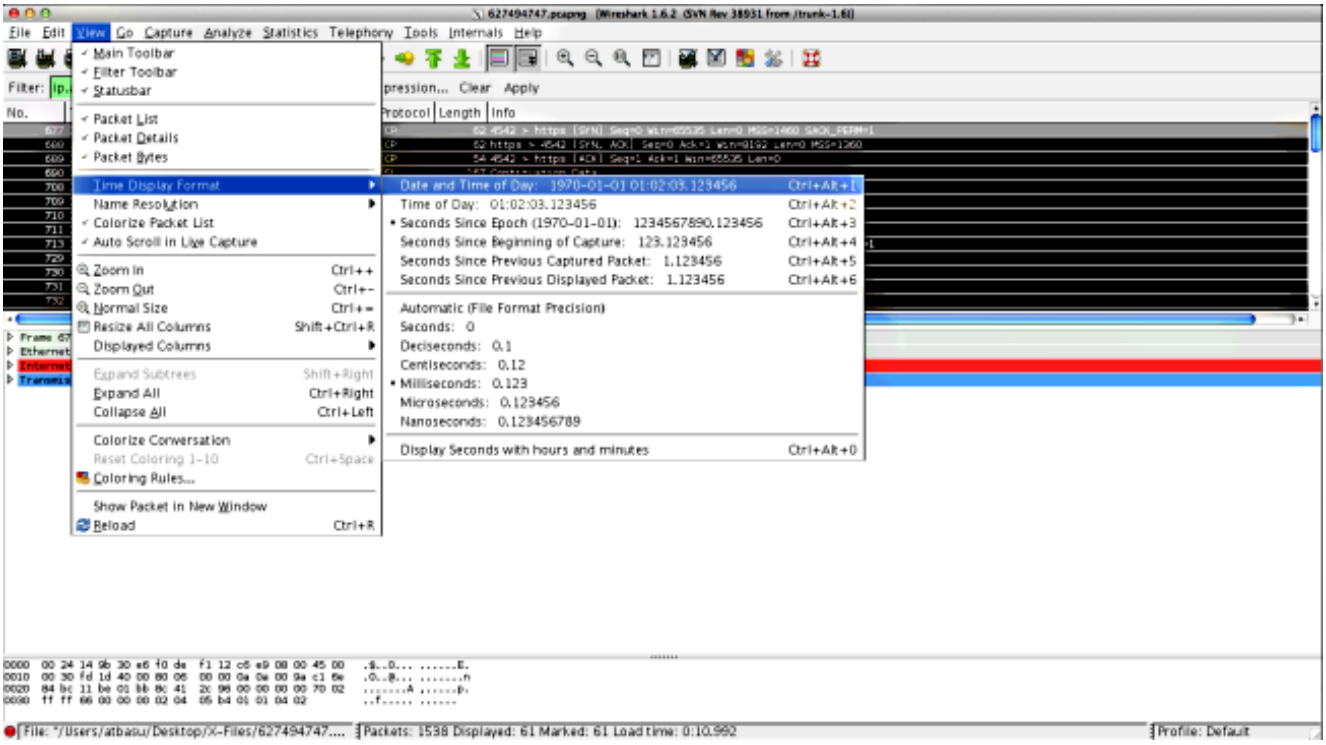
Schritt 4: Validieren der von AnyConnect ausgeführten OGS-Berechnungen

Überprüfen Sie die Erfassung auf die TCP/SSL-Tests, die zur Berechnung von RTT verwendet werden. Erfahren Sie, wie lange die HTTPS-Anforderung eine einzelne TCP-Verbindung übernimmt. Jede Anfrage sollte eine andere TCP-Verbindung verwenden. Öffnen Sie dazu die Erfassung in Wireshark, und wiederholen Sie die folgenden Schritte für jeden der Server:

1. Verwenden Sie den Filter **ip.addr**, um die an die einzelnen Server gesendeten Pakete in ihrer eigenen Erfassung zu isolieren. Navigieren Sie dazu zu **Bearbeiten**, und wählen Sie **Alle angezeigten Pakete markieren aus**. Navigieren Sie dann zu **Datei > Speichern unter**, wählen Sie die **Option Nur markierte Pakete** aus, und klicken Sie auf **Speichern**:

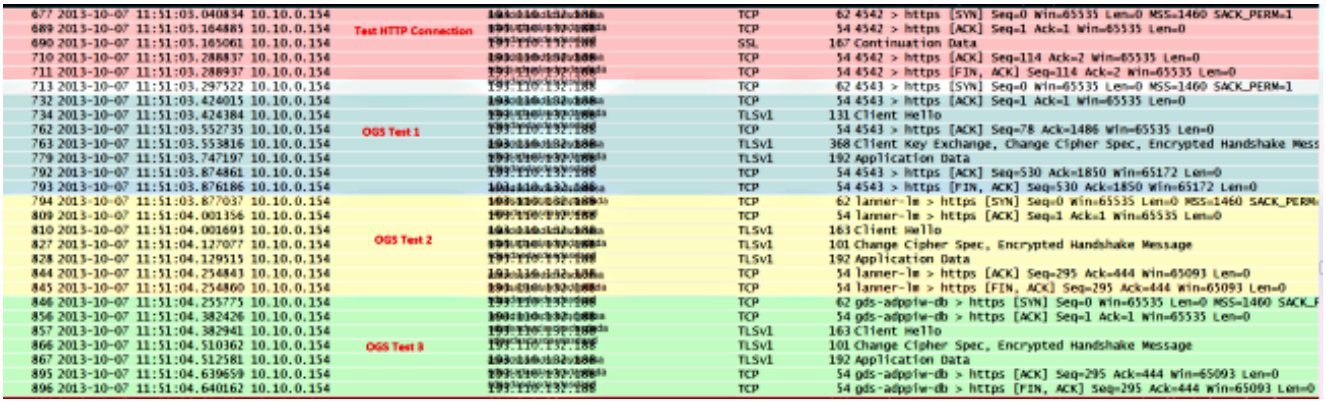


2. Navigieren Sie in dieser neuen Erfassung zu **Ansicht > Anzeigeformat > Datum und Uhrzeit**:

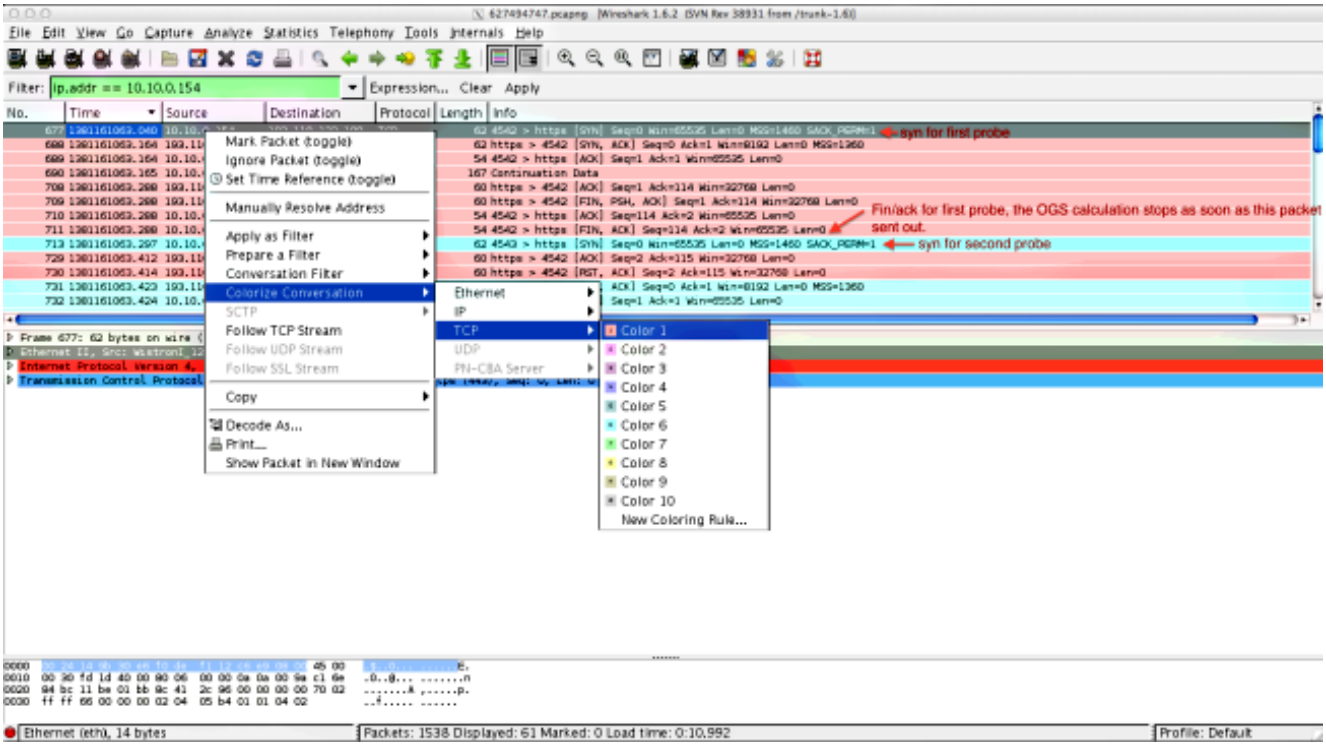


3. Identifizieren Sie das erste HTTP-SYN-Paket in dieser Erfassung, das gesendet wurde, als die OGS-Anfrage basierend auf den in Schritt 3.3.2 identifizierten DART-Protokollen gesendet wurde. Es ist wichtig zu beachten, dass die erste HTTP-Anforderung für den ersten Server keine Serverprobe ist. Die erste Anfrage für eine Serverabfrage lässt sich leicht

verwechseln, sodass die Werte komplett von denen abweichen, die OGS meldet. Dieses Problem wird hier hervorgehoben:

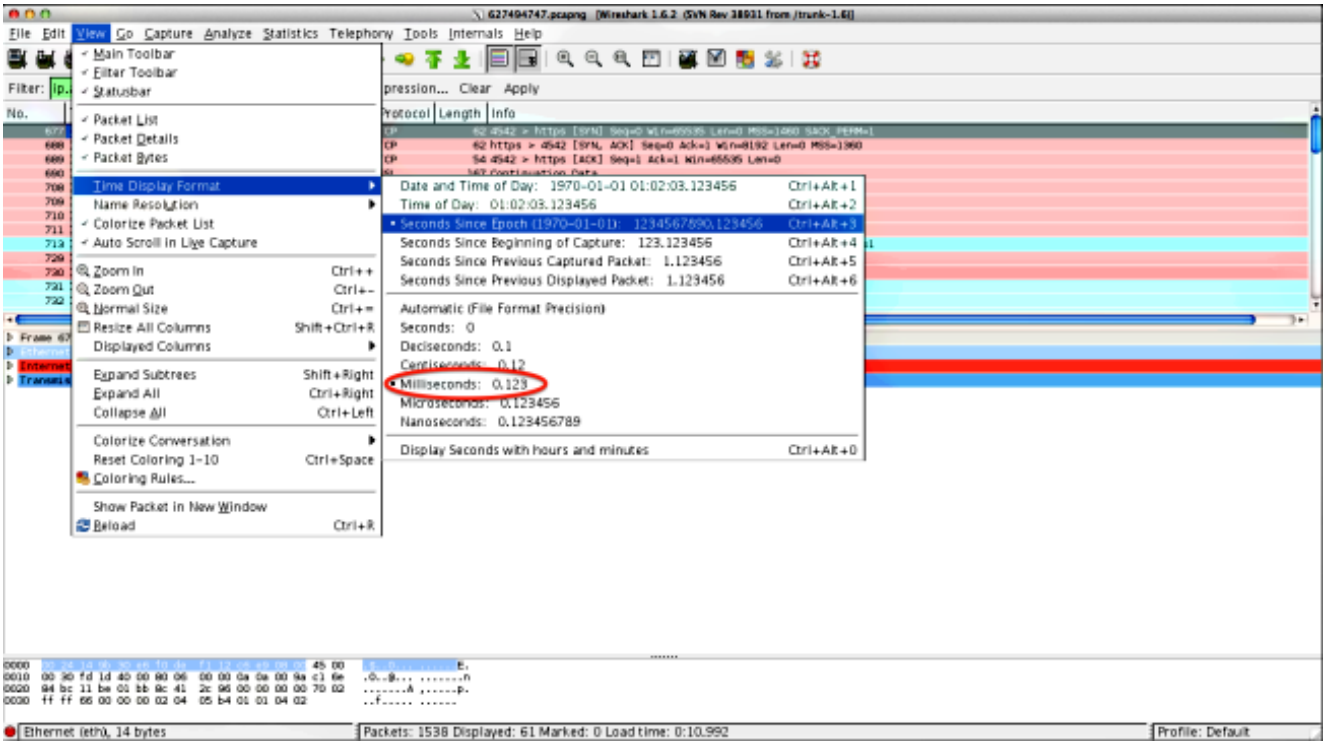


4. Um die einzelnen Sonden einfacher zu identifizieren, klicken Sie mit der rechten Maustaste auf das **HTTP-SYN** für die erste Anfrage, und wählen Sie dann **Colorize Conversation** (**Gesprächsverbindung** wie hier gezeigt) aus:



Wiederholen Sie diesen Vorgang für die SYNs aller Proben. Wie im vorherigen Bild gezeigt, werden die ersten beiden Sonden in verschiedenen Farben dargestellt. Der Vorteil der Einfärbung der TCP-Gespräche besteht darin, dass Neuübertragungen oder andere derartige Eigenschaften pro Anfrage leicht identifiziert werden können.

5. Um die Zeitanzeige zu ändern, gehen Sie zu **Ansicht > Zeitanzeigeformat > Sekunden seit Epoche**:



Wählen Sie **Millisekunden aus**, da dies die Genauigkeit ist, die OGS verwendet.

6. Berechnen Sie die Zeitdifferenz zwischen dem HTTP-SYN und dem FIN/ACK, wie im Diagramm von Schritt 4 gezeigt. Wiederholen Sie diesen Vorgang für jede der drei Prüfungen, und vergleichen Sie die Werte mit denen in den DART-Protokollen in Schritt 3.3.3.

Analyse

Wenn nach der Analyse der Erfassung die ermittelten RTT-Werte berechnet und mit den Werten in den DART-Protokollen verglichen werden und alles übereinstimmt, aber es scheint, als ob das falsche Gateway ausgewählt wird, dann liegt dies an einem von zwei Problemen:

- Es liegt ein Problem am Headend vor. Wenn dies der Fall ist, kann es zu viele Neuübertragungen von einem bestimmten Headend oder von anderen derartigen merkwürdigen Ereignissen in den Proben geben. Eine genauere Analyse des Austauschs ist erforderlich.

- Es besteht ein Problem mit dem Internetdienstanbieter (ISP). In diesem Fall kann es zu Fragmentierung oder großen Verzögerungen für ein bestimmtes Headend kommen.

Fragen und Antworten

Frage: Funktioniert OGS mit Lastenausgleich?

A: Ja. OGS kennt nur den Cluster-Masternamen und verwendet diesen, um das nächstgelegene Headend zu beurteilen.

Frage: Funktioniert OGS mit den im Browser definierten Proxy-Einstellungen?

Antwort: OGS unterstützt keine Auto Proxy- oder Proxy Auto Config (PAC)-Dateien, sondern einen fest codierten Proxyserver. Daher wird der OGS-Vorgang nicht ausgeführt. Die entsprechende Protokollmeldung lautet: "**OGS wird nicht ausgeführt, da die automatische Proxy-Erkennung konfiguriert ist**."