Contenu

Introduction

Ce document décrit comment dépanner des questions avec la sélection optimale de passerelle (OGS). OGS est une caractéristique qui peut être utilisée afin de déterminer quelle passerelle a la plus basse durée d'aller-retour (DURÉE DE TRANSMISSION) et se connecter à cette passerelle. On peut employer la caractéristique OGS afin de réduire la latence pour le trafic Internet sans intervention de l'utilisateur. Avec OGS, le Client à mobilité sécurisé Cisco AnyConnect (AnyConnect) l'identifie et sélectionne qui sécurisent la passerelle sont les meilleurs pour la connexion ou la reconnexion. OGS commence sur la première connexion ou sur une reconnexion au moins quatre heures après la déconnexion précédente. Plus d'informations peuvent être trouvées du guide d'administrateur.

> **Conseil** : OGS fonctionne meilleur avec le plus défunt client d'AnyConnect et la version de logiciel ASA 9.1(3) * ou plus tard.

Comment OGS fonctionne-t-il ?

Une requête ping simple de Protocole ICMP (Internet Control Message Protocol) ne fonctionne pas parce que beaucoup de Pare-feu de l'appliance de sécurité adaptable Cisco (ASA) sont configurés afin de bloquer des paquets d'ICMP pour empêcher la détection. Au lieu de cela, le client envoie trois demandes HTTP/443 à chaque headend qui apparaît dans une **fusion de** tous les profils. Ces sondes de HTTP désigné sous le nom des pings OGS dans les logs, mais, comme expliqué plus tôt, elles ne sont pas des pings d'ICMP. Afin de s'assurer que la connexion a (au sujet de) ne prend pas trop long, OGS sélectionne la passerelle précédente par défaut s'il ne

reçoit aucun résultat de ping OGS dans sept secondes. (Recherchez les **résultats de ping OGS** dans le log.)

> Remarque: AnyConnect devrait envoyer une demande de HTTP à 443, parce que la réponse elle-même est importante, pas une réponse réussie. Malheureusement, la difficulté pour la manipulation de proxy envoie toutes les demandes comme HTTPS. Voir l'ID de bogue Cisco CSCtg38672 - OGS devrait cingler avec des demandes de HTTP.

> Remarque: S'il n'y a aucun headends dans le cache, AnyConnect envoie d'abord une demande de HTTP afin de déterminer s'il y a un Seveur mandataire d'authentification, et s'il peut traiter la demande. C'est seulement après cette requête initiale qu'il commence les pings OGS afin de sonder le serveur.

- OGS détermine l'emplacement d'utilisateur basé sur l'information réseau, telle que le suffixe de Système de noms de domaine (DNS) et l'adresse IP de serveur DNS. Les résultats de DURÉE DE TRANSMISSION, avec cet emplacement, sont enregistrés dans le cache OGS.

- Des entrées d'emplacement OGS sont cachées pendant 14 jours. L'amélioration CSCtk66531 a été classée pour rendre ces configurations utilisateur-configurables.

- OGS n'est pas exécuté de nouveau de cet emplacement jusqu'à pendant 14 jours après que l'entrée d'emplacement est d'abord cachée. Pendant ce temps, il utilise l'entrée cachée et les durées de transmission déterminées pour cet emplacement. Ceci signifie que quand les reprendre d'AnyConnect, il n'exécute pas OGS de nouveau ; au lieu de cela, il utilise la commande optimale de passerelle dans le cache pour cet emplacement. Dans les logs diagnostiques d'outil de génération de rapports d'AnyConnect (DART), ce message est vu :

- La DURÉE DE TRANSMISSION est déterminée avec un échange de TCP au port de Secure Sockets Layer (SSL) de la passerelle à laquelle l'utilisateur essayera de se connecter comme spécifié par l'entrée de hôte dans le profil d'AnyConnect.

  Remarque: À la différence du HTTP-ping, qui fait un courrier simple de HTTP et puis affiche la DURÉE DE TRANSMISSION et le résultat, les calculs OGS sont légèrement plus compliqués. AnyConnect envoie trois sondes pour chaque serveur, et calcule le retard entre la synchronisation de HTTP qu'il envoie et le FIN/ACK pour chacune de ces sondes. Il emploie alors le plus bas des deltas afin de comparer les serveurs et faire sa sélection. Ainsi, quoique les HTTP-pings soient une indication assez bonne dont le serveur l'AnyConnect choisira, ils ne pourraient pas nécessairement compter. Il y a plus d'informations sur ceci dans le reste du document.
- Actuellement, OGS exécute seulement les contrôles si l'utilisateur sort d'un interrompre, et le seuil a été dépassé. OGS ne se connecte pas à une ASA différente si l'ASA l'utilisateur est connectée aux crash ou devient indisponible. OGS contacte seulement les serveurs primaires dans le profil afin de déterminer l'optimal.

- Une fois que le profil de client OGS est téléchargé, quand les restars d'utilisateur le client d'Anyconnect, l'option de sélectionner d'autres profils seront greyed comme affiché ici :

Même si l'ordinateur d'utilisateur a d'autres profils, ils ne pourront pas sélectionner l'un d'entre eux jusqu'à ce qu'OGS disbaled.

Cache OGS

Une fois que le calcul est de finition, les résultats sont enregistrés dans le fichier **preferences_global**. Il y a eu des questions avec ces données n'étant pas enregistré dans le fichier avant.

Référez-vous à l'ID de bogue Cisco CSCtj84626 pour plus de détails.

Détermination d'emplacement

La mise en cache OGS travaille à une combinaison du domaine de DN et des différentes adresses IP de serveur DNS. Cela fonctionne comme suit :

- Le Site A a un domaine de DN de **locationa.com**, et deux adresses IP de serveur DNS - **ip1** et **ip2**. Chaque combinaison domain/IP crée une clé de cache que les points à un OGS cachent l'entrée. Exemple : **locationa.com|ip1 - > ogscache1locationa.com|ip2 - > ogscache1**

- Si AnyConnect se connecte alors à un physique-différent réseau, le même habillage des combinaisons domain/IP est créé et vérifié contre la liste cachée. S'il y a des correspondances du tout, cette valeur de cache OGS est utilisée, et le client est encore considéré à l'**emplacement R.**

Scénarios de panne

Voici quelques scénarios de panne que les utilisateurs pourraient rencontrer :

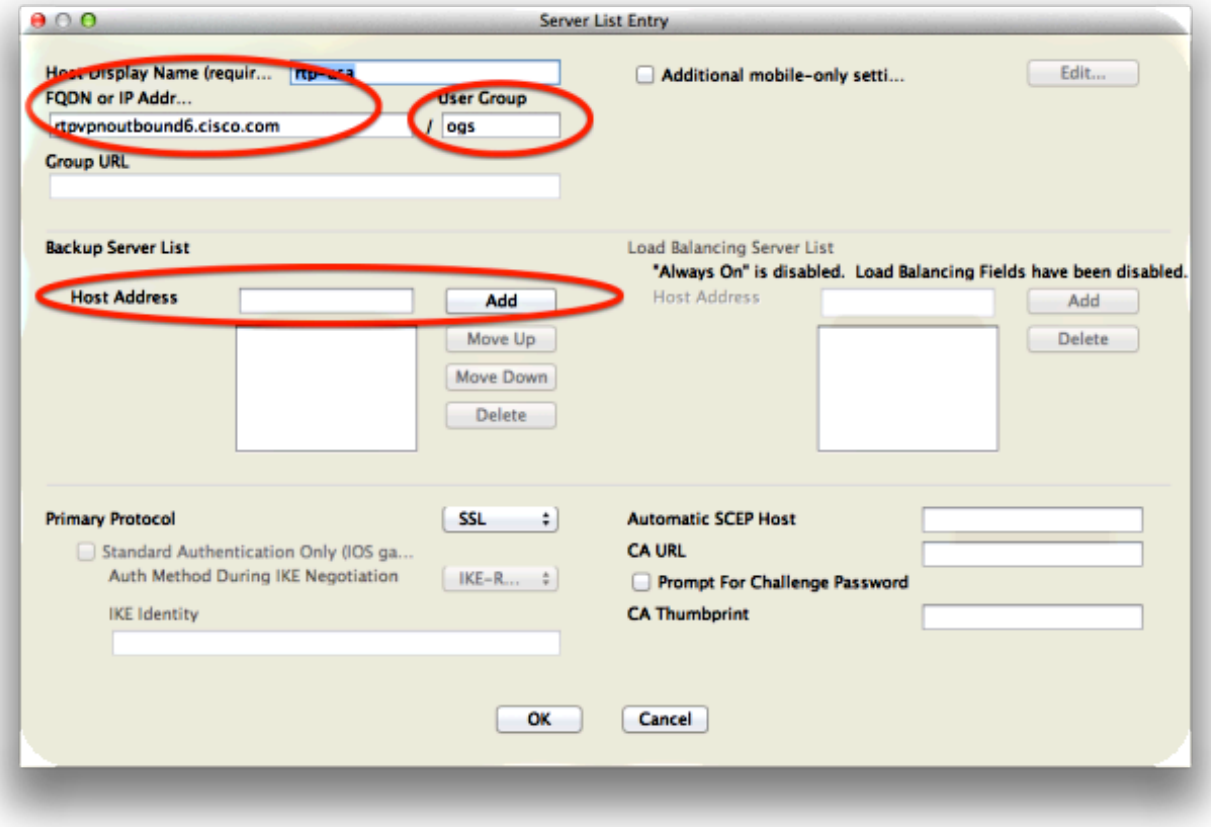
Quand la Connectivité à la passerelle est perdue

Quand OGS est utilisé, si la Connectivité à la passerelle à laquelle les utilisateurs sont connectés est perdue, alors AnyConnect se connecte aux serveurs dans la **liste de sauvegarde de serveur** et **pas au** prochain hôte OGS. La commande des exécutions est comme suit :

1. OGS contacte seulement les serveurs primaires afin de déterminer l'optimal.
2. Une fois que déterminé, l'algorithme de connexion est :

   Tentative de se connecter au serveur optimal.Si cela échoue, essayez la liste de sauvegarde du serveur du serveur optimal.Si cela échoue, jugez chaque serveur qui reste dans la liste de sélection OGS, commandé par sa sélection résulte.

   Remarque: Quand l'administrateur configure la liste de sauvegarde de serveur, l'éditeur en cours de profil laisse seulement l'administrateur pour écrire le nom de domaine complet (FQDN) pour le serveur de sauvegarde, mais pas l'user-group comme est possible au serveur primaire :



L'ID de bogue Cisco CSCud84778 a été classé afin de corriger ceci, mais l'URL complet doit être écrit dans le domaine de host address pour le serveur de sauvegarde, et il devrait fonctionner : **https://*<ip-address>/usergroup***.

Reprise après un interrompre

Pour qu'OGS s'exécute après qu'une reprise, AnyConnect doive avoir eu une connexion établie quand l'ordinateur a été mis pour dormir. OGS après qu'une reprise soit seulement exécutée après que le test d'environnement de réseau se produise, qui est censé pour confirmer cette connexion réseau est disponible. Ce test inclut une Connectivité de DN subtest. Cependant, si les baisses de serveur DNS tapent des demandes A avec une adresse IP dans le domaine de requête, par opposition à répondre avec le « nom non trouvé » (le cas plus commun, toujours produit pendant les tests), puis à l'ID de bogue Cisco CSCti20768 « requête DNS du type A pour l'adresse IP, devrait être le PTR pour éviter le délai d'attente » s'applique.

La taille de la fenêtre du TCP Retarder-ACK sélectionne la passerelle incorrecte

Quand les versions ASA avant la version 9.1(3) sont utilisation, les saisies sur le client affichent un retard persistant dans la prise de contact SSL. Ce qui est noté est que le client envoie son ClientHello, puis l'ASA envoie son ServerHello. Ceci est normalement suivi par un message de certificat (demande facultative de certificat) et le message de ServerHelloDone. L'anomalie est double :

1. L'ASA n'envoie pas immédiatement le message de certificat après le ServerHello. La taille de

la fenêtre de client est de 64,860 octets, qui est plus qu'assez pour tenir la réponse entière de l'ASA.

2. Le client ne fait pas ACK le ServerHello immédiatement, ainsi l'ASA retransmet le ServerHello après ~120ms, lequel au point le client Acks les données. Alors le message de certificat est envoyé. Il est presque comme si le client attend plus de données.

Ceci se produit en raison de l'interaction entre le lent-commencement et le TCP RETARDER-ACK de TCP. Avant la version 9.1(3) ASA, l'ASA utilise une taille de fenêtre de lent-commencement de 1, tandis que le client Windows utilise une valeur retarder-ACK de 2. Ceci signifie que l'ASA envoie seulement un paquet de données jusqu'à ce qu'elle obtienne un ACK, mais il signifie également que le client n'envoie pas un ACK jusqu'à ce qu'il reçoive deux paquets de données. Les temps ASA après que 120ms et retransmet le ServerHello, après quoi le client Acks les données et la connexion continue. Ce comportement a été changé par l'ID de bogue Cisco CSCug98113 de sorte que l'ASA utilise une taille de la fenêtre lente de début de 2 par défaut au lieu de 1.

Ceci peut affecter le calcul OGS quand :

- Les différentes passerelles exécutent différentes versions ASA.
- Les clients ont les différentes tailles de la fenêtre retarder-ACK.

Dans de telles situations, le retard introduit par le retarder-ACK a pu être suffisant pour faire sélectionner le client l'ASA fausse. Si cette valeur diffère entre le client et l'ASA, il pourrait encore y avoir des problèmes. Dans de telles situations, le contournement est d'ajuster la taille de la fenêtre retardée d'accusés de réception.

Windows

1. Commencez **Registry Editor**.

2. Identifiez le GUID de l'interface sur laquelle vous voulez désactiver le retarder-ACK. Afin de faire ceci, naviguez vers :
   HKEY_LOCAL_MACHINE > LOGICIEL > Microsoft > Windows NT > CurrentVersion > NetworkCards > (nombre).
   Regardez chaque nombre indiqué sous NetworkCards. Du côté droit, la description devrait répertorier l'interface (par exemple, Intel (R) lien Sans fil 5100AGN de WiFi) et le ServiceName devraient répertorier le GUID correspondant.

3. Localisez et puis cliquez sur cette sous-clé de registre :
   HKEY_LOCAL_MACHINE \ SYSTÈME \ CurrentControlSet \ services \ Tcpip \ paramètres \ interfaces \ <Interface GUID>

4. Sur le menu Edit, le point à nouveau, et cliquent sur alors la **valeur DWORD**.

5. Nommez la nouvelle valeur **TcpAckFrequency**, et assignez-lui une valeur de **1.**

6. Quittez Registry Editor.

7. Reprise Windows pour que cette modification la prenne effet.

   Remarque: La demande d'amélioration CSCum19065 a été classée de rendre le TCP

accordant des paramètres configurable sur l'ASA.

Exemple typique d'utilisateur

Le cas le plus d'usage courant est quand un utilisateur exécute à la maison OGS la première fois, il enregistre les configurations de DN et les résultats de ping OGS dans le cache (par défaut à un délai d'attente de 14-jour). Quand l'utilisateur renvoie à la maison la soirée suivante, OGS détecte les mêmes configurations de DN, les trouve dans le cache, et ignore le test de ping OGS. Plus tard, quand l'utilisateur va à un hôtel ou à un restaurant qui offre le service Internet, OGS détecte différentes configurations de DN, exécute les tests de ping OGS, sélectionne la meilleure passerelle, et enregistre les résultats dans le cache.

Le traitement est identique quand il reprend d'un état interrompu ou hiberné, si les configurations de reprise OGS et d'AnyConnect tiennent compte de lui.

Dépannez OGS

Étape 1. Effacez le cache OGS afin de forcer une réévaluation

Afin d'effacer les OGS cachent et réévaluent la DURÉE DE TRANSMISSION pour les passerelles disponibles, suppriment simplement les préférences globales d'AnyConnect classent du PC. L'emplacement du fichier varie basé sur le système d'exploitation (SYSTÈME D'EXPLOITATION) :

- Windows Vista et Windows 7
- Windows XP
- Mac OS X
- Linux

Étape 2. Capturez les sondes de serveur pendant la tentative de connexion

1. Début Wireshark sur la machine de test.
2. Commencez une tentative de connexion sur AnyConnect.
3. Arrêtez la capture Wireshark une fois que la connexion est complète.**Conseil** : Puisque la capture est seulement utilisée afin de tester OGS, il est le meilleur d'arrêter la capture dès qu'AnyConnect sélectionnera une passerelle. Il est le meilleur de ne pas passer par une tentative complète de connexion, parce que cela peut opacifier la capture de paquet.

Étape 3. Vérifiez la passerelle sélectionnée par OGS

Afin de vérifier pourquoi OGS a sélectionné une passerelle particulière, terminez-vous ces étapes :

1. Initiez une nouvelle connexion.
2. Exécutez le DART d'AnyConnect :

Lancement **AnyConnect**, et clic **avancé**.**Diagnostics de** clic.Cliquez sur **Next** (Suivant).Cliquez sur **Next** (Suivant).

3. Examinez les résultats de DART trouvés dans le **fichier** de création récente sur l'appareil de bureau.

   Naviguez vers le **Client à mobilité sécurisé Cisco AnyConnect > l'AnyConnect.txt**.

   Notez le temps où les sondes OGS ont commencé pour un serveur particulier de ce log de DART :

   Habituellement ils devraient être vers la même époque, mais au cas où les captures seraient grandes, le groupe date/heure aide à se rétrécir vers le bas que les paquets sont les sondes de HTTP et lesquels sont la tentative réelle de connexion.

   Une fois qu'AnyConnect envoie trois sondes au serveur, ce message est généré avec les résultats pour chacune des sondes :
   Il est important de prêter l'attention à ces trois valeurs, parce qu'ils doivent apparier les résultats de capture.

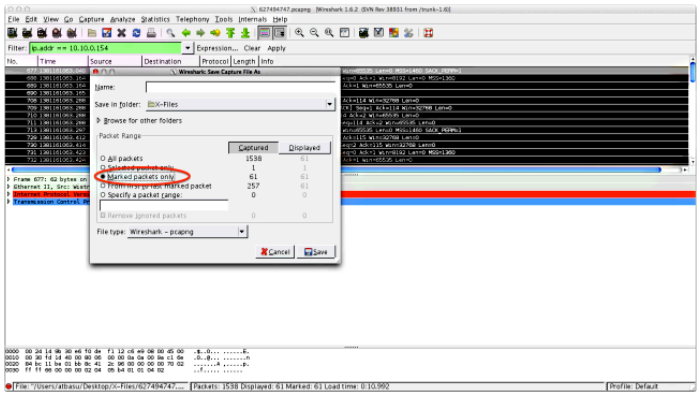
   Recherchez le message qui contient « le *** de résultats de sélection du *** OGS » afin de voir la DURÉE DE TRANSMISSION évaluée, et si la tentative la plus récente de connexion était le résultat d'une DURÉE DE TRANSMISSION cachée ou d'un nouveau calcul.

   Voici un exemple :

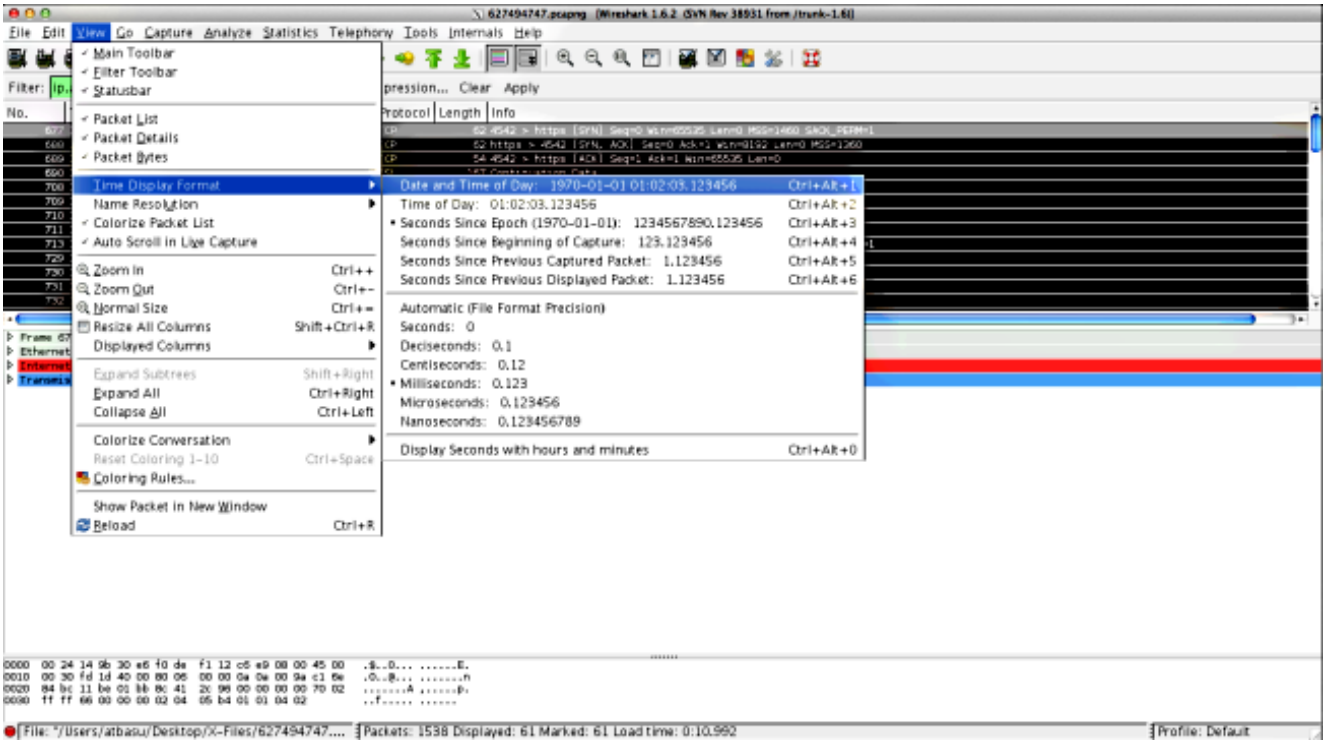
Étape 4. Validez les calculs OGS exécutés par AnyConnect

Examinez la capture pour assurer le TCP/SSL sonde utilisé afin de calculer la DURÉE DE TRANSMISSION. Voyez combien de temps la demande HTTPS assure une connexion TCP simple. Chaque demande de sonde devrait utiliser une connexion TCP différente. Afin de faire ceci, ouvrez la capture dans Wireshark, et répétez ces étapes pour chacun des serveurs :

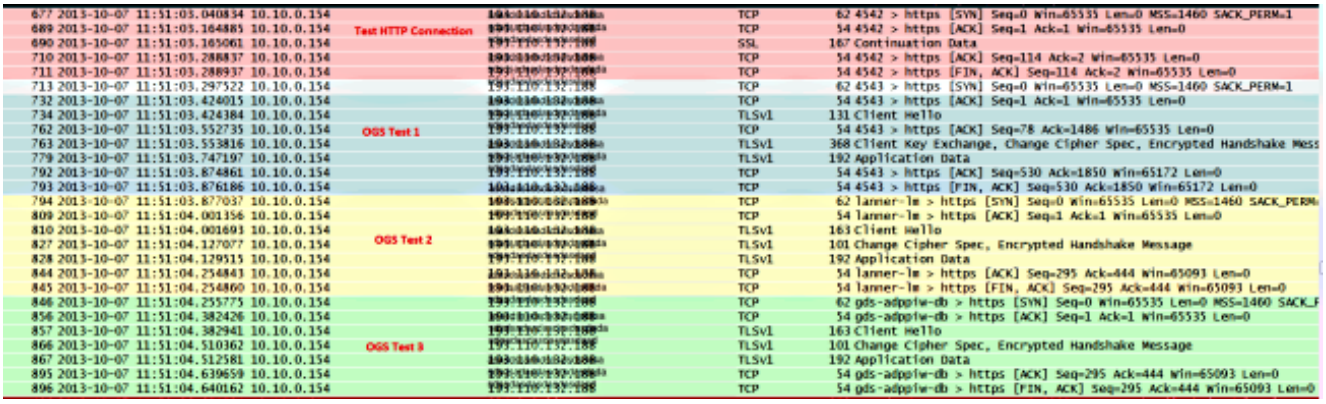
1. Utilisez le **filtre ip.addr** afin d'isoler les paquets envoyés à chacun des serveurs dans leur propre capture. Afin de faire ceci, naviguer pour éditer**,** et MarkAll choisi **a affiché des paquets.** Naviguez **alors** pour classer **> sauvegarde comme, sélectionner l'option de** Markedpackets **seulement**, et cliquer sur la sauvegarde **:**



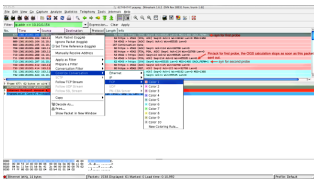
2. Dans cette nouvelle capture, naviguez **pour visualiser > format d'affichage de temps > date et heure** :



3. Identifiez le premier paquet de synchronisation de HTTP dans cette capture qui a été envoyée quand la sonde OGS a été envoyée basée sur les logs de DART comme identifié dans l'étape 3.3.2. Il est important de se souvenir que, pour le premier serveur, la première demande de HTTP n'est pas une sonde de serveur. Il est facile de confondre la première demande avec une sonde de serveur, et arrive ainsi aux valeurs complètement différentes de ce qu'OGS signale. Ce problème est mis en valeur ici :

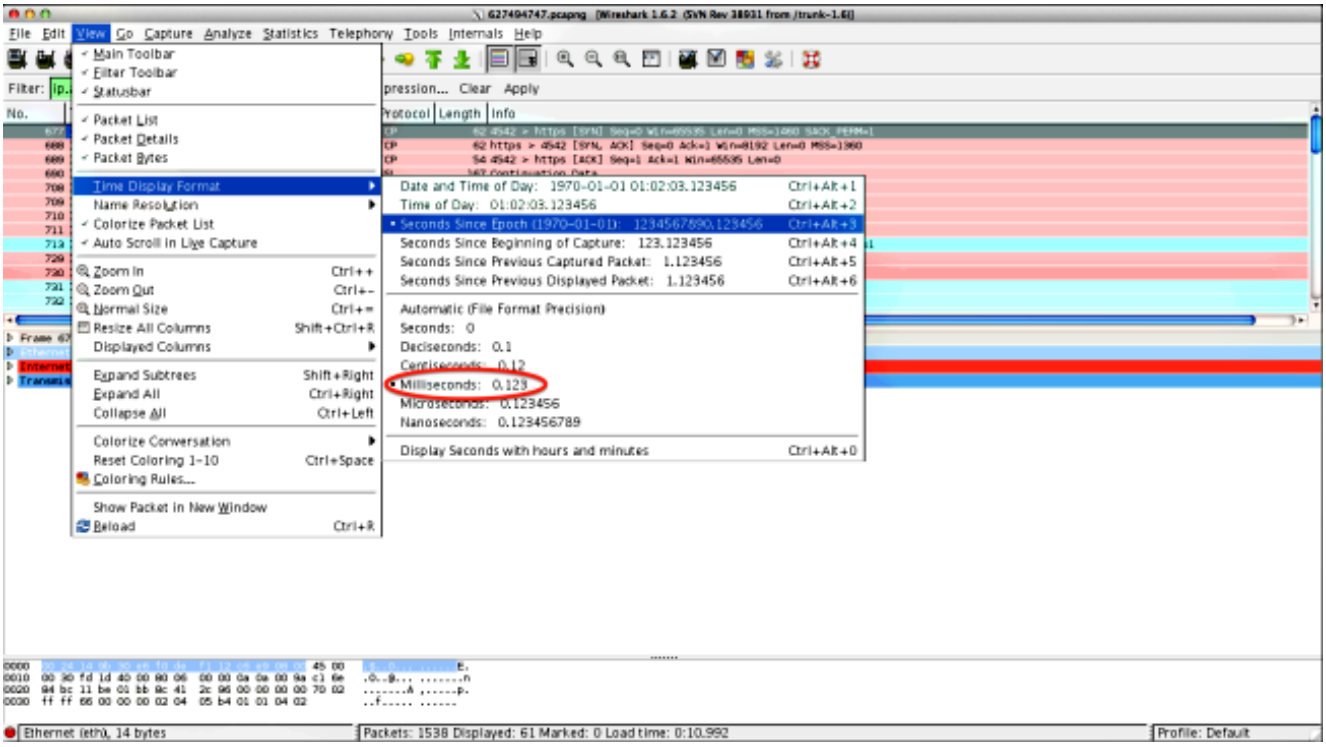


4. Afin d'identifier plus facilement chacune des sondes, cliquez avec le bouton droit la **synchronisation de HTTP** pour la première sonde, et puis sélectionnez la **conversation de Colorize** comme affiché ici :



Répétez ce processus pour les synchronisations sur toutes les sondes. Suivant les indications de l'image précédente, les deux premières sondes sont dépeintes dans différentes couleurs. L'avantage de colorizing les conversations de TCP est de repérer facilement des retransmissions ou d'autres telles singularités par sonde.

5. Afin de changer l'affichage de temps, naviguez **pour visualiser > format > secondes d'affichage de temps depuis l'époque** :



Sélectionnez les **millisecondes**, parce que c'est le niveau de la précision qu'OGS utilise.

6. Calculez la différence de temps entre la synchronisation de HTTP et le FIN/ACK, suivant les indications du diagramme de la répétition d'étape 4. ce processus pour chacune des trois sondes, et comparez les valeurs à ceux affichées dans l'étape 3.3.3 de logins de DART.

Analyse

Si après que l'analyse des captures, les valeurs déterminées de DURÉE DE TRANSMISSION soient calculées et comparées aux valeurs vues dans les logs de DART et tout s'avère pour s'assortir, mais il semble toujours comme la passerelle fausse est sélectionné, alors il est dû à un de deux problèmes :

- Il y a une question sur le headend. Si c'est le cas, il pourrait y avoir trop de retransmissions d'un headend particulier, ou toutes les autres telles singularités vues dans les sondes. Une analyse plus étroite de l'échange est exigée.

- Il y a un problème avec le fournisseur de services Internet (ISP). Si c'est le cas, il pourrait y avoir fragmentation ou grands retards vus pour un headend particulier.

Q&A

Q : OGS fonctionne-t-il avec l'Équilibrage de charge ?

A : Oui. OGS se rend seulement compte du nom de maître de batterie, et des utilisations qui afin de juger le headend le plus proche.

Q : OGS fonctionne-t-il avec les paramètres de proxy définis dans le navigateur ?

A : OGS ne prend en charge pas les fichiers automatiques automatiques de proxy ou de config de proxy (PAC), mais prend en charge un serveur proxy dur-codé. En soi, l'exécution OGS ne se produit pas. Le message de log approprié est : « **OGS ne sera pas exécuté parce que la détection automatique de proxy est configurée**. »