Déchiffrez le flot de RTP pour l'analyse de perte de paquets dans Wireshark pour la Voix et les appels vidéos

Contenu

Introduction

Ce document décrit le processus de la façon déchiffrer le flot de transmission en continu (RTP) pour l'analyse de perte de paquets dans Wireshark pour la Voix et les appels vidéos. Vous pouvez utiliser des filtres de Wireshark afin d'analyser les captures simultanées de paquet prises ou près derrière la source et derrière la destination d'appel. C'est utile quand vous devez dépanner les questions de qualité audios et vidéoes quand des pertes de réseau sont suspectées.

Problème

Cet exemple utilise cet écoulement d'appel :

Commutateur 2960 > routeur > routeur WAN du téléphone IP A (siteA central) > (lieu d'exploitation principal) > IPWAN > routeur WAN (site B) > routeur > 2960 > téléphone IP B

Dans ce scénario, le problème rencontré est que les appels vidéos du téléphone IP A au téléphone IP B résultent de la mauvaise qualité vidéo du lieu d'exploitation principal A à la filiale B où le central a la bonne qualité mais le côté de branchement a des questions.

Voyez les paquets perdus par récepteur en statistiques coulantes du téléphone IP de branchement :

Solution

La mauvaise qualité est vue seulement du côté de branchement et parce que le lieu d'exploitation principal voit une bonne image, elle ressemble au flot du central à la filiale semble être les paquets perdants au-dessus du réseau.

```
IP addressing scheme
Central IP phone: 192.168.10.146
Central Gateway: 192.168.10.253
Central WAN router: 192.168.10.254
```

```
Branch WAN router: 192.168.206.210
Branch Gateway: 192.168.206.253
Branch IP phone: 192.168.207.231
```

Les captures de paquet sont prises sur le central et s'embranchent routeur WAN et le WAN relâche ces paquets. Concentrez sur le flot de RTP du téléphone IP central (192.168.10.146) pour s'embrancher le téléphone IP (192.168.207.231). Ce flot manque des paquets sur le routeur WAN de branchement si le WAN relâche les paquets sur le flot du routeur WAN central pour s'embrancher routeur WAN. Utilisez les options de filtre dans le wireshark d'isoler le problème :

1. Ouvrez la capture dans le wireshark.

2. Utilisez le && ip.dst==192.168.207.231 du filtre ip.src==192.168.10.146. Ceci filtre tous les flots d'UDP de téléphone IP central pour s'embrancher téléphone IP.

3. Exécutez l'analyse sur la capture de côté de branchement seulement mais notez-vous doit exécuter ces étapes pour la capture centrale aussi bien.

4. Dans ce tir d'écran, le flot d'UDP est filtré entre la source et les adresses IP de destination et contient deux flots d'UDP (différenciés par les numéros de port UDP). C'est un appel vidéo tellement là sont deux flots : audio et vidéo. Dans cet exemple, les deux flots sont :

   Flot 1 : Port de source d'UDP : 20560, destination port : 20800

   Flot 2 : Port de source d'UDP : 20561, destination port : 20801

5. Sélectionnez un paquet d'un des flots et cliquez avec le bouton droit le paquet.

6. Choisi **décodez en tant que…** et tapez le **RTP**.

7. Le clic **reçoivent** et **approuvent** afin de décoder le flot comme RTP.

   Vous êtes laissé avec un flot décodé comme RTP et l'autre en tant qu'UDP undecoded.

8. Sélectionnez un paquet du flot undecoded et décodez-le comme RTP. Ceci décode l'audio et les flux vidéos dans le RTP.

   Remarque: Le flux audio est dans G.722 le format de codecs et le type de la charge utile Dynamic-RTP-97 indique le flot visuel de RTP.

   Le problème est maintenant seulement avec la qualité vidéo. Concentrez sur le flot visuel de RTP et utilisez les numéros de port UDP pour que ce flot filtre d'autres flots.

9. Visualisez le numéro de port en sélectionnant un des paquets qui affiche les informations de port UDP sur le volet inférieur dans l'utilitaire de Wireshark. Dans le tir d'écran précédent, un des paquets du flux vidéo est sélectionné et vous pouvez voir le port de Src (20568) et informations de port de Dst (les 20808) sur le volet inférieur.

   Conseil : Utilisez ce filtre : (ip.src==192.168.10.146 && ip.dst==192.168.207.231) && (eq 20568 udp.port et eq 20808 udp.port). Vous verrez seulement le flot visuel de RTP affiché dans ce tir d'écran.

   Remarque: Notez les premiers et derniers numéros de séquence de RTP pour ce flot.

   Le premier numéro de séquence de RTP est 45514 le bout est 50449 pour filtré le flot visuel de RTP.

10. Assurez-vous que le premier et les derniers paquets de numéro de séquence de RTP sont présents dans l'exemple les deux captures.for, le central et les captures de branchement) et notent que le SSRC pour le le flot serait identique sur les les deux les captures.
11. Affinez le filtre pour apparier seulement les paquets entre le premier et les derniers flots de RTP.

    Les numéros de séquence sont utilisés pour affiner le flot au cas où les captures n'étaient pas prises simultanément, mais avec le léger retard entre eux.

    Remarque: Il est possible que la filiale pourrait mettre en marche quelques numéros de séquence après 45514.

12. Sélectionnez un début et finissez le numéro de séquence. Ces paquets sont présents dans les captures et affinent le filtre pour afficher seulement ces paquets entre le début et les numéros de séquence de RTP de fin. Le filtre pour ceci est :

    ```
    (ip.src==192.168.10.146 && ip.dst==192.168.207.231) && (udp.port eq 20568
    and udp.port eq 20808) && ( rtp.seq>=44514 && rtp.seq<=50449 )
    ```

    Quand des captures sont simultanément prises, aucun paquet n'est manqué au début ou finit sur les deux captures. Si vous voyez qu'une des captures n'inclut pas quelques paquets au start/end, utilisez le premier numéro de séquence ou le dernier numéro de séquence dans la capture manquée en les deux paquets pour affiner le filtre pour chacun des deux les captures. Observez les paquets qui les ont capturé aux deux points entre les mêmes numéros de séquence (plage de numéro de séquence de RTP).

    Quand vous appliquez le filtre, vous voyez ceci au lieu d'exploitation principal et à la filiale :

    Lieu d'exploitation principal :

Filiale :

Notez le compte filtré de paquet au volet inférieur sur l'utilitaire de Wireshark sur les deux captures. Le compte affiché indique le nombre de paquets appariant les critères désirés de filtre.

Le lieu d'exploitation principal a 4,936 paquets qui apparient les critères désirés de filtre entre le début (45514) et finissent (50449) numéros de séquence de RTP tandis qu'à la filiale il y a seulement 4,737 paquets. Ceci indique une perte de 199 paquets. Notez que ces 199 paquets apparient « Rcvr le compte ont perdu paquets » de 199 qui a été vu en statistiques coulantes du téléphone IP de côté de branchement affiché au début de ce document.

Ceci confirme que tous les paquets perdus par Rcvr étaient réellement des pertes de réseau lâchées à travers le WAN. C'est comment le point de perte de paquets dans le réseau est isolé tandis que des questions d'audio/qualité vidéo sont traitées impliquant des baisses suspectées de réseau.