解密包丢失分析的RTP数据流在语音和视频呼叫的Wireshark

目录

简介

本文描述进程如何解密包丢失分析的实时流(RTP)数据流在语音和视频呼叫的Wireshark。您能使用Wireshark过滤器为了分析同时数据包捕获被采取在或接近呼叫的源和目的。这是有用的，当您必须排除故障音频和视频质量问题时，当网络损耗怀疑时。

问题

此示例使用此呼叫流：

IP电话A (中央siteA) > 2960 switch> Router> WAN路由器(中心站点) > IPWAN > WAN路由器(站点B) > Router> 2960 > IP电话B

在此方案中，遇到的问题是从IP电话A的视频呼叫对IP电话B导致坏视频质量从中心站点A到中央有优良品质的分支站点B，但是分组侧有问题。

请参阅在分组IP电话的流统计信息的接收方丢失的数据包：

解决方案

Bad质量在分组侧仅被看到，并且，因为中心站点看到一好镜像，看起来象从中央的数据流到分支站点似乎丢失在网络的数据包。

```
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
```

数据包捕获在中央印制厂被采取，并且分组WAN路由器和广域网丢弃这些数据包。在RTP数据流的重点从分支的中央IP电话(192.168.10.146) IP电话(192.168.207.231)。如果广域网从中央WAN路由器丢弃在数据流的数据包分支WAN路由器，此数据流未命中在分组WAN路由器的数据包。 请使用过滤器选项在wireshark隔离问题：

1. 打开在wireshark的捕获。

2. 请使用过滤器ip.src==192.168.10.146 && ip.dst==192.168.207.231。这过滤从中央IP电话的所有UDP数据流分支IP电话。

3. 只执行在分组侧捕获的分析，但是注释您必须执行中央捕获的这些步骤。

4. 在此屏幕画面， UDP数据流被过滤在来源和目的地IP地址之间并且包含两UDP数据流(区分由UDP端口号)。这是视频呼叫那么那里是两数据流：音频和视频。在本例中，两数据流是：

   数据流1 ：UDP源端口：20560，目的地端口：20800

   数据流2 ：UDP源端口：20561，目的地端口：20801

5. 选择从其中一的一数据包数据流并且用鼠标右键单击数据包。

6. 选择**解码作为…**并且键入**RTP**。

7. 单击**接受**并且**好**为了解码数据流作为RTP。

   您留下与作为RTP解码的一数据流和其他作为undecoded UDP。

8. 选择从undecoded数据流的一数据包并且解码它作为RTP。这解码音频和视频流到RTP。

   注意： 音频流在G.722编码格式，并且Dynamic-RTP-97有效载荷类型指示视频RTP数据流。

   问题当前仅是视频质量。着重视频RTP数据流并且请使用UDP端口号此数据流过滤其他数据流。

9. 通过选择显示关于底下窗格的UDP端口信息在Wireshark工具的其中一查看端口号数据包。在上一个屏幕画面，其中一从视频流的数据包选择，并且您能看到Src波尔特(20568)和关于底下窗格的Dst端口(20808)信息。

   提示：请使用此过滤器： (ip.src==192.168.10.146 && ip.dst==192.168.207.231) && (udp.port eq 20568和udp.port eq 20808)。您只将看到在此屏幕画面显示的视频RTP数据流。

   注意：写下此的第一个和最后RTP序号数据流。

第一个RTP序号是45514为时是50449过滤的视频RTP数据流的。

10. 确保第一，并且最后RTP序号数据包是存在两个captures.for示例，中央和分组捕获)和注意到，数据流的SSRC是相同的在两个捕获。
11. 完善过滤器匹配在第一和为时RTP数据流之间的仅数据包。

    序号用于完善数据流，万一捕获未同时被采取，但是与他们之间的轻微的延迟。

    注意：很可能，分支站点也许在45514以后启动一些序号。

12. 选择开始并且结束序号。这些数据包是存在捕获并且完善过滤器显示在开始和结尾RTP序号之间的仅那些数据包。此的过滤器是：

    ```
    (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 )
    ```

    当捕获同时被采取时，数据包在两个捕获起初没有未命中也不结束。如果看到一个捕获不包括一些数据包起初/末端，请使用第一个序号或最后序号在两数据包未命中的捕获完善两个的过滤器捕获。观察捕获在同样序号的数据包(RTP序号范围)之间的两个点。

    当您应用过滤器时，您在中心站点和分支站点看到此：

    中心站点：

    分支站点：

    注释已过滤数据包计数在Wireshark工具的底下窗格在两个捕获。**显示的**计数指示匹配希望的过滤器标准的数据包数量。

    中心站点有匹配在开始的4,936数据包(45514)之间的希望的过滤器标准并且结束(50449个)RTP序号，当在分支站点只有4,737数据包时。这指示199数据包损耗。 注意这199数据包匹配在本文的开始显示的分组侧IP电话流统计信息被看到的“Rcvr丢失数据包”计数199。

    这确认所有Rcvr丢失的数据包实际上是在广域网间丢弃的网络损耗。这是问题的在网络的包丢失如何隔离，当被处理介入怀疑的网络丢包时的音频/视频质量问题。