Decifre o córrego RTP para a análise da perda de pacotes em Wireshark para atendimentos da Voz e do vídeo

Índice

Introdução

Este documento descreve o processo de como decifrar o tempo real que flui o córrego (RTP) para a análise da perda de pacotes em Wireshark para atendimentos da Voz e do vídeo. Você pode usar filtros de Wireshark a fim analisar as capturas de pacote de informação simultâneas tomadas ou perto da fonte e do destino de um atendimento. Isto é útil quando você deve pesquisar defeitos edições do áudio e de qualidade de vídeo quando as perdas da rede estão suspeitadas.

Problema

Este exemplo usa este fluxo de chamadas:

Telefone IP A (siteA central) > 2960 Switch > WAN Router do Roteador> (instalação central) > IPWAN > WAN Router (local B) > Roteador> 2960 > telefone IP B

Nesta encenação, o problema encontrado é que o vídeo chama o resultado do telefone IP A ao telefone IP B na qualidade de vídeo ruim da instalação central A à instalação de filial B onde a central tem a boa qualidade mas o lado do ramo tem edições.

Veja os pacotes perdidos receptor nas estatísticas de fluência do telefone IP do ramo:

Solução

A qualidade ruim é considerada somente no lado do ramo e porque a instalação central vê uma boa imagem, olha como o córrego da central à instalação de filial parece ser pacotes perdedores sobre a rede.

```
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
```

As capturas de pacote de informação são tomadas na central e ramificam WAN Router e WAN deixa cair estes pacotes. Focalize no córrego RTP do telefone IP central (192.168.10.146) para ramificar o telefone IP (192.168.207.231). Este córrego falta pacotes no WAN Router do ramo se WAN deixa cair os pacotes no córrego do WAN Router central para ramificar WAN Router. Use as opções de filtro no wireshark isolar o problema:

1. Abra a captação no wireshark.

2. Use o && ip.dst==192.168.207.231 do filtro ip.src==192.168.10.146. Isto filtra para fora todos os córregos UDP do telefone IP central para ramificar telefone IP.

3. Execute a análise na captação do lado do ramo somente mas note-o deve executar estas etapas para a captação central também.

4. Neste tiro de tela, o córrego UDP é filtrado entre a fonte e os endereços IP de destino e contém dois córregos UDP (diferenciados pelos números de porta UDP). Este é um atendimento video tão lá é dois córregos: áudio e vídeo. Neste exemplo, os dois córregos são:

   Córrego 1: Porta de origem UDP: 20560, porta do destino: 20800

   Córrego 2: Porta de origem UDP: 20561, porta do destino: 20801

5. Selecione um pacote de um dos córregos e clicar com o botão direito o pacote.

6. Seleto **descodifique como…** e datilografe o **RTP**.

7. O clique **aceita** e **aprova** a fim descodificar o córrego como o RTP.

   Você é deixado com o um córrego descodificado como o RTP e o outro como o UDP undecoded.

8. Selecione um pacote do córrego undecoded e descodifique-o como o RTP. Isto descodifica o áudio e os fluxos de vídeo no RTP.

   Nota: O fluxo de áudio está no formato do codec de G.722 e o tipo de payload Dynamic-RTP-97 indica o córrego do vídeo RTP.

   O problema é agora somente com qualidade de vídeo. Focalize no córrego do vídeo RTP e use os números de porta UDP para que este córrego filtre para fora outros córregos.

9. Veja o número de porta selecionando um dos pacotes que indica a informação de porta UDP na placa inferior na utilidade de Wireshark. No tiro de tela precedente, um dos pacotes do fluxo de vídeo é selecionado e você pode ver a porta de Src (20568) e informações da porta de Dst (as 20808) na placa inferior.

   Dica: Use este filtro: (ip.src==192.168.10.146 && ip.dst==192.168.207.231) && (eq 20568 udp.port e eq 20808 udp.port). Você verá somente o córrego do vídeo RTP mostrado neste tiro de tela.

   Nota: Escreva para baixo os primeiros e últimos números de sequência RTP para este córrego.

   O primeiro número de sequência RTP é 45514 o último é 50449 para o córrego video para fora filtrado RTP.

10. Certifique-se de que o primeiro e os últimos pacotes do número de sequência RTP estam presente no exemplo ambos os captures.for, a central e as captações do ramo) e notam que o SSRC para o o córrego seria o mesmo em ambas as captações.
11. Refine o filtro para combinar somente os pacotes entre os primeiros e os últimos córregos RTP.

    Os números de sequência são usados para refinar o córrego caso que as captações não foram tomadas simultaneamente, mas com pequeno retardo entre eles.

    Nota: É possível que a instalação de filial pôde ligar alguns números de sequência após 45514.

12. Selecione um começo e termine o número de sequência. Estes pacotes estam presente nas captações e refinam o filtro para indicar somente aqueles pacotes entre o começo e os números de sequência da extremidade RTP. O filtro para este é:

    ```
    (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 )
    ```

    Quando as captações são tomadas simultaneamente, nenhum pacote está faltado no início ou termina em ambas as captações. Se você vê que uma das captações não inclui algum no início dos pacotes/extremidade, use o primeiro número de sequência ou o último número de sequência na captação faltada em ambos os pacotes para refinar o filtro para ambas as captações. Observe os pacotes que capturaram em ambos os pontos entre os mesmos números de sequência (escala do número de sequência RTP).

    Quando você aplica o filtro, você vê este na instalação central e na instalação de filial:

Instalação central:

Instalação de filial:

Note o contagem de pacote de informação filtrado na placa inferior na utilidade de Wireshark em ambas as captações. A contagem indicada indica o número de pacotes que combinam os critérios desejados do filtro.

A instalação central tem 4,936 pacotes que combinam os critérios desejados do filtro entre o começo (45514) e terminam (50449) números de sequência RTP quando na instalação de filial houver somente 4,737 pacotes. Isto indica uma perda de 199 pacotes. Note que estes 199 pacotes combinam “Rcvr perderam a contagem dos pacotes” de 199 que foi considerada nas estatísticas de fluência do telefone IP do lado do ramo mostrado no início deste documento.

Isto confirma que todos os pacotes perdidos Rcvr eram realmente perdas da rede deixadas cair através de WAN. Isto é como o ponto da perda de pacotes na rede é isolado quando as edições do áudio/qualidade de vídeo forem seguradas que envolvem gotas suspeitadas da rede.