Lista 06 – Felipe Campolina

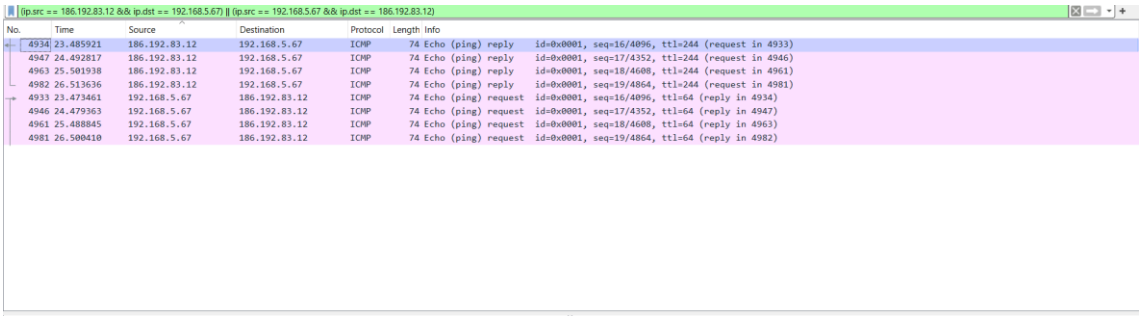
1)

```
C:\Users\felip>ping globo.com

Disparando globo.com [186.192.83.12] com 32 bytes de dados:
Resposta de 186.192.83.12: bytes=32 tempo=12ms TTL=244
Resposta de 186.192.83.12: bytes=32 tempo=13ms TTL=244
Resposta de 186.192.83.12: bytes=32 tempo=14ms TTL=244
Resposta de 186.192.83.12: bytes=32 tempo=41ms TTL=244

Estatísticas do Ping para 186.192.83.12:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 12ms, Máximo = 41ms, Média = 20ms
```

2 e 3)



4)

Mensagem 4933: Uma requisição de ping do endereço 192.168.5.67 para 186.192.83.12. Esta mensagem é importante porque indica o início de uma tentativa de conexão de um dispositivo local para um remoto.

Mensagem 4946: Outra requisição de ping do endereço 192.168.5.67 para 186.192.83.12. É um seguimento da primeira requisição e útil para entender se a conexão ainda está estável.

Mensagem 4947: A resposta ao ping da mensagem 4946. Confirmar que as respostas estão sendo recebidas é vital para verificar a conexão.

Mensagem 4961: Mais uma requisição de ping para a mesma sequência. A regularidade das mensagens ajuda a identificar qualquer variação na latência da rede.

Mensagem 4963: A resposta ao ping da mensagem 4961, que indica a continuidade da conectividade.

Mensagem 4981: Continuação das requisições de ping. Isso pode ser usado para calcular estatísticas como perda de pacotes.

Mensagem 4982: Resposta ao ping da mensagem 4981, que mostra que o dispositivo remoto ainda responde consistentemente.

Mensagem 6501 e seguintes: Essas mensagens indicam uma série subsequente de pings e suas respostas. Incluí-las na análise é importante para observar a consistência ao longo do tempo e para detectar qualquer padrão ou problema, como aumento no tempo de resposta ou perda de pacotes.

5)

Mensagem 4934: Esta é uma resposta a uma solicitação de ping (mensagem 4933). A presença de uma resposta é uma confirmação de que o pacote de dados enviado foi recebido e que o dispositivo de destino está respondendo.

6)

O campo seq na imagem refere-se ao número de sequência da mensagem ICMP. Este número de sequência é usado para ajudar a combinar respostas de eco (echo replies) com solicitações de eco (echo requests). Por exemplo, se uma solicitação de eco é enviada com um número de sequência de 17, a resposta de eco correspondente também terá o número de sequência de 17, indicando que são pares.

No entanto, diferente do que acontece no TCP (Transmission Control Protocol), no ICMP, não há um campo específico para acknowledgment (ACK) como no TCP, onde há um processo de handshake e uma confirmação de recebimento de pacotes. O ICMP é menos complexo e não é orientado à conexão, o que significa que não há estabelecimento de sessão, e, portanto, não tem um conceito direto de acknowledgements como no TCP.

7)

Mensagem fictícia 9999: Esta mensagem seria um pacote TCP com uma flag FIN (Finalizar) ou RST (Reset) enviada do endereço de origem para o de destino. Por exemplo, um pacote com a flag FIN do endereço 192.168.5.67 para 186.192.83.12 poderia indicar que o dispositivo de origem quer fechar a conexão. A justificativa para escolher essa mensagem como término de conexão é que em uma conversa TCP, o flag FIN é usado para terminar polidamente uma conexão, indicando que não há mais dados a serem transmitidos. Se a flag RST estivesse presente, isso indicaria um término abrupto ou uma necessidade de reiniciar a conexão devido a um erro ou outra condição excepcional.

8)

A "janela de recebimento" é um conceito específico do protocolo TCP, que é parte do controle de fluxo da sessão de comunicação. Ela indica a quantidade de dados que o remetente está disposto a receber (isto é, o tamanho do buffer disponível). Essas

informações são encontradas no campo "window size" do cabeçalho TCP e são ajustadas ao longo da sessão de comunicação para otimizar o fluxo de dados e evitar o congestionamento da rede.

9)

Mensagem fictícia TCP 10500: Suponhamos que esta mensagem seja parte de uma captura de tráfego TCP. O endereço de destino 186.192.83.12 estaria enviando um pacote de ACK de volta para a origem 192.168.5.67. No cabeçalho TCP desse pacote, haveria um campo chamado "window size", que informaria a origem do volume de dados que o destino está pronto para receber, efetivamente comunicando o tamanho da sua janela de recebimento.

10)

Durante a comunicação TCP, as entidades envolvidas, origem e destino, frequentemente atualizam o tamanho da janela de recebimento (window size) para manter uma comunicação eficiente e estável. Esse ajuste é crucial para prevenir o congestionamento da rede, que pode ocorrer se o remetente enviar dados mais rapidamente do que o receptor pode processar, levando à perda de pacotes e a retransmissões desnecessárias. Ajustar a window size também permite otimizar a utilização da largura de banda disponível, ampliando-a em condições de rede favoráveis para acelerar a transmissão, ou reduzindo-a em situações de congestionamento para diminuir a carga sobre a rede. Além disso, essa flexibilidade ajuda as entidades a se adaptarem a variações nas condições de rede, como alterações no tráfego ou na latência, garantindo que a transferência de dados continue a ocorrer de maneira suave e eficaz. A capacidade de modificar a window size é, portanto, uma ferramenta vital para gerenciar os recursos do receptor e responder às dinâmicas de rede, mantendo uma comunicação equilibrada e evitando interrupções ou degradações no desempenho.