**Engenharia de Computação**

**Laboratório de Redes de Computadores I**

**Aula Prática 11 – Protocolos IP e ICMP**

**Objetivo:** Utilizando o programa *sniffer Wireshark*, verificar as características e funcionalidades dos protocolos ICMP e do IP.

**Descrição:**

Reveja os vídeos:

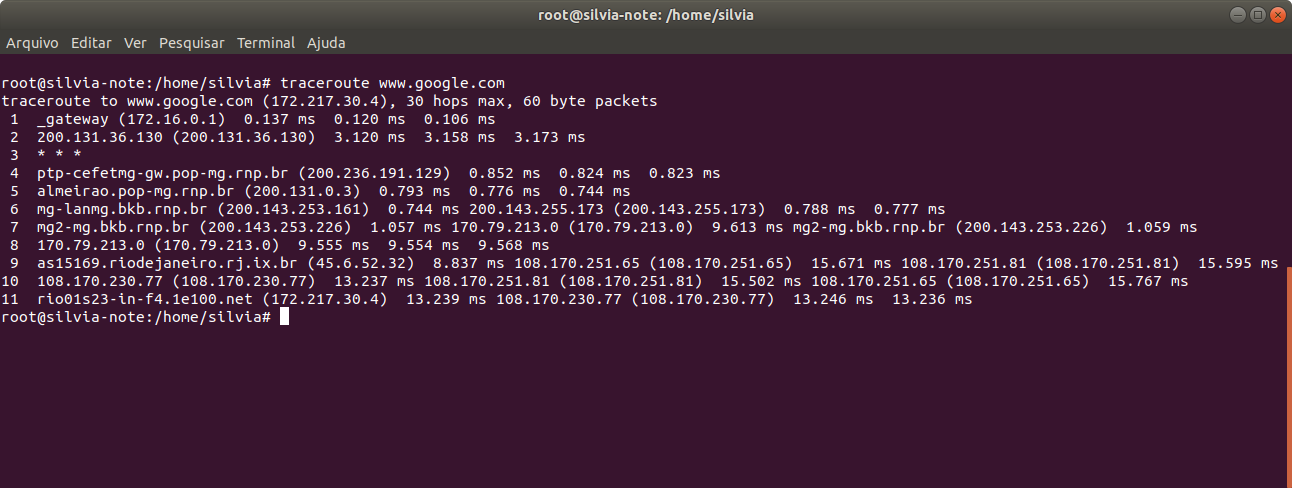
1) <https://www.youtube.com/watch?v=q9O59Tl9-pA>

2) <https://www.youtube.com/watch?v=y9Vx5l-th9Y&list=PLxvyNgS1BGn6V3vxq-5X1qQnWvgsfs3pU&index=7>

3) <https://www.youtube.com/watch?v=5OtebbSnwoM&list=PLxvyNgS1BGn6V3vxq-5X1qQnWvgsfs3pU&index=8>

Estudaremos o protocolo IP através do resultado de capturas feitas quando o comando **traceroute** (Linux/Unix) é executado. Este comando indica os saltos, roteadores, pelos quais o datagrama IP passou até atingir o destino.

Por exemplo, veja a tela abaixo contendo todos os passos para chegar ao servidor web do Google.



O programa *traceroute* envia datagramas de diferentes tamanhos para um destino X. No exemplo acima, o destino foi [www.google.com](http://www.google.com/). Para montar a rota, o *traceroute* envia um datagrama, com o campo TTL, *time-to-live*, igual a 1, depois outro com o TTL igual a 2, depois igual a 3 e assim por diante, até conseguir atingir o destino. Quando um roteador recebe um datagrama, ele subtrai do TTL menos uma unidade. No caso do TTL ficar com o valor zero, este roteador envia à origem uma mensagem ICMP, indicando que o tempo de vida do pacote expirou. Como consequência deste comportamento, o datagrama com o TTL 1 irá fazer com que o primeiro roteador da rota já retorne a mensagem ICMP de TTL expirado (type 11 – TTL-exceeded). O datagrama com o TTL=2 irá fazer com que o segundo roteador da rota retorne a mensagem ICMP de TTL expirado e assim por diante. A partir das mensagens ICMP recebidas, a origem conhecerá as identidades dos roteadores entre ela e o destino.

Faça login no Linux, inicie o Wireshark e a captura de pacotes. Numa tela de sistema, execute os comandos:

**sudo traceroute -I www.google.com 56**

**sudo traceroute -I www.google.com 2000**

**sudo traceroute -I www.google.com 3500**

Depois de aparecer os resultados, pare a captura.

1. Selecione a primeira mensagem de eco ICMP enviado pelo seu computador e expanda a parte do protocolo IP, na tela intermediária. Responda:
   1. Qual é o endereço IP do seu computador, origem (**Src**)? E do destino (**Dst**)?

172.16.127.255

172..217.28.228

* 1. Qual é o protocolo da camada superior ao IP (abaixo na lista da tela intermediária)?

ICMP

* 1. Quantos bytes tem o cabeçalho (**Header lenght**)? Quantos bytes tem o *payload* (parte de dados) do datagrama IP (Procure por **Total lenght** para fazer este cálculo)? Como você encontrou este valor?

20 Bytes. 36 Bytes. Total lenght - header lenght.

* 1. Este datagrama foi fragmentado (**fragment offset**)? Como você verificou esta informação?

Sim. pois há mais de um pacote ICMP em sequência para o mesmo IP.

1. Coloque a coluna de endereço de origem em ordem crescente, clicando no título **Source**. Selecione a primeira mensagem de eco ICMP (pacote com TTL=1) gerada pela sua máquina e expanda a parte do protocolo IP, na tela intermediária. Observe os valores dos campos. Na primeira tela, vá clicando nas requisições de eco ICMP subsequentes enviadas pelo seu computador. Responda:
2. O que há de diferente em cada requisição enviada?

O ttl vai aumentado, o número de identificação e checksum mudaram.

1. Qual é o padrão seguido pelo campo de identificação (**Identification**)?

0xaaf

1. Encontre a série de mensagens ICMP de resposta do tipo **Time-to-live exceeded** (primeiras mensagens da lista) enviadas pelo roteador mais próximo ao computador de origem.
2. Clique na primeira mensagem. Qual o valor do campo de identificação (**Identification**) e do campo **Time-to-live**?

0x0fdc, 64.

1. Verifique estes valores nas demais mensagens deste tipo (linhas subsequentes). Estes valores são alterados?

Sim.

1. Coloque a coluna **No.** em ordem crescente. Durante a captura, os datagramas IP foram definidos para terem tamanho de 56 bytes, de 2000 e depois de 3500 bytes. Responda.
2. Encontre a mensagem que foi a primeira mensagem configurada com o valor de 2000 bytes. Esta mensagem foi fragmentada? Qual campo confirma esta informação?

Sim. Pois o total lenght passou para 520, diferente da primeira solicitação.

1. Em quantos datagramas a mensagem foi fragmentada (**IP Fragments**)? Quais são os tamanhos dos datagramas IP?

3. 520

1. Encontre a mensagem que foi a primeira mensagem configurada com o valor de 3500 bytes. Em quantos datagramas a mensagem foi fragmentada? Quais são os tamanhos dos datagramas IP?

540. 3

5) Envie suas respostas pelo SIGAA.