



## Tarefa

### Objetivo

Faça um relatório contendo os resultados dos exercícios abaixo. Para cada exercício, a interpretação dos resultados deve estar descrita.

### Exercícios

#### 1. Uso do comando *ping*:

- Teste o comando e verifique que tipo de opções podem ser utilizadas. Dê o comando *man ping* para ver as opções.
- Use o comando *ping* para uma máquina ao lado da sua e para outra fora da rede. Comente o resultado.
- Utilizando o *ping* com a variação do TTL do pacote trace a rota de um pacote da sua origem ao destino, verificando os roteadores intermediários.

#### 2. Uso do *traceroute* ou *tracpath*:

- Tente usar o comando *traceroute* ou *tracpath*. Caso você receba uma mensagem de erro, dê o comando: *sudo apt-get install traceroute* Ao pedir a senha de *root*, informe *labredes*.
- Utilizando o comando *traceroute* identifique o caminho que é utilizado para alcançar:
  - a) A máquina do seu lado
  - b) Uma máquina dentro da PUC, como [www.pucrs.br](http://www.pucrs.br) por exemplo.
  - c) Uma máquina de fora da PUC, como [www.google.com](http://www.google.com) por exemplo.

Comente os resultados.

#### 3. Consulte as características da placa de rede utilizando o comando *ifconfig*.

- a) A máscara utilizada identifica sub-redes? Se sim, quantas sub-redes existem para o endereço? Quantos *hosts* por sub-redes existem?
- b) Qual é o endereço de rede do endereço IP da máquina?
- c) Qual é o endereço de *broadcast* do endereço IP da máquina?

#### 4. Mostre e explique a tabela de roteamento da máquina (comando *netstat -r* ou *route -n*). Comente cada linha da tabela informando para que ela serve.

## 5. Uso do *Wireshark*:

Utilize o programa *Wireshark* e monitore o tráfego da rede. O *Wireshark* deve rodar como *root*, então abra um terminal, e digite:

```
sudo wireshark
```

Uma senha será pedida, informe a senha *labredes*.

Para capturar o tráfego da rede, entre na opção *Capture -> Interfaces* e selecione a opção *Start* na interface eth1 ou eth0, a que aparecer com o endereço 10.32.X.X ao lado.

Para parar a captura dos pacotes, vá em *Capture -> Interface* e selecione a opção *Stop*.

Analise o cabeçalho dos protocolos Ethernet, IP e ARP.

- Consulte a tabela arp da máquina (arp -a)
- Rode o *Wireshark* (filtre pacotes ARP)
- Dê um *ping* para a máquina ao lado.
- Pare o *Wireshark*.
- Consulte a tabela arp novamente.
- Analise os pacotes capturados pelo *Wireshark*.
- O que foi observado?
- É possível identificar como o ARP funciona?
- Qual é o formato do cabeçalho do Protocolo ARP?

## 6. Uso do *Wireshark* + *traceroute*:

Rode o *Wireshark* e capture o tráfego gerado pelo comando *traceroute*. Analisando o tráfego gerado, descreva como o *traceroute* é implementado. Qual protocolo ele utiliza?

## 7. Uso do *Wireshark* + *ping*:

- Use o comando *ping* e varie o tamanho do pacote a ser enviado. Monitore o tráfego para analisar as mensagens geradas e as informações de fragmentação contidas no pacote IP. Descreva como ocorreu o processo de fragmentação analisando os cabeçalhos dos datagramas IP. Quais campos foram usados na fragmentação?

8. O que são RFCs? Qual o nome, número e data do último RFC existente atualmente? (Procure em: [www.ietf.org](http://www.ietf.org)).

## Resultados e Entrega

O relatório poderá ser entregue individualmente ou em dupla.

**Entrega dia 16/03**