

Curso: **Bacharel em Sistemas de Informação**

Professor: **Paulo Cezar de Oliveira**

Disciplina: **Rede de Computadores**

Aluno(a): _____

Turma: _____

Data de entrega: 10/03/2016

Observações:

- **LEIA ATENTAMENTE AS INSTRUÇÕES E O ENUNCIADO ANTES DE INICIAR O EXERCÍCIO.**
- Deve ser entregue por email (paulocezard@spei.br) e em dupla até o término da aula de hoje.
- As respostas descritivas devem ser enviadas no formato .doc, docx ou odt.
 - o No **assunto do email** coloque a **turma e o período**.
- Não se esqueça de identificar a atividade com nome e turma.
 - o No **nome do arquivo** coloque o **primeiro nome de cada envolvido**
- As respostas copiadas não serão consideradas, tanto de quem copiou quanto de quem forneceu o original.
- Não será aceito atraso na entrega do trabalho.

2ª Lista de Exercícios

Laboratório baseado em exercício proposto por Kurose no livro texto da disciplina. (Wireshark_ICMP_Sept_15_2009.pdf)

1. Objetivo

- Explorar aspectos dos protocolos ICMP e ARP;
- As mensagens ICMP geradas pelo programa Ping;
- O formato e conteúdo de uma mensagem ICMP;
- As mensagens de requisição e resposta do protocolo ARP.

2. ARP, ICMP e Ping

O programa Ping é uma ferramenta simples que permite verificar se um host está na rede ou não.

Seu funcionamento consiste no envio de pacotes (ICMP – Internet Control Message Protocol) para o endereço IP de destino; quando o alvo está ativo, o programa Ping no host de destino responde enviando um pacote de volta para o host de origem.

Com o mesmo tráfego gerado, vamos investigar o protocolo ARP (Address Resolution Protocol), usado para mapear o endereço IP e o endereço físico (MAC) da interface associada ao endereço IP de interesse. Esse endereço físico é usado para preencher o campo 'Destino' na camada de enlace.

3. Orientações

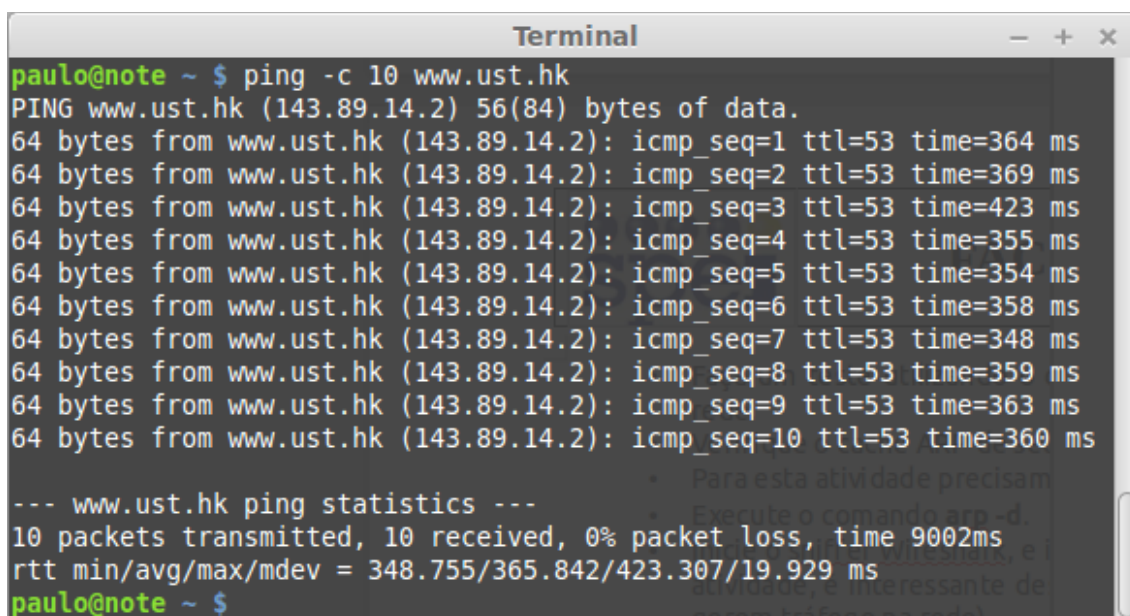
- Faça um print de cada tela do exercício identificado o que significam.
- O ideal é que essa atividade seja feita na rede cabeada.
- Para facilitar a atividade, é interessante desativar quaisquer outros aplicativos que gerem tráfego na rede.
- Desmarque a opção "use promiscuous mode.." do wireshark.
- Para aplicar um filtro no Wireshark, basta clicar com campo **Filter** na parte superior, digitar o protocolo ou endereço IP (ou qualquer outra expressão que necessitar) e em seguida clicar em **Aply**. Para limpar o filtro clique em **Clear**.

4. Atividades

- Faça um teste utilizando o comando PING para um endereço IP da rede.
- *Faça um print dessa tela.*
- Verifique o cache ARP de seu computador com o comando **arp -a**.
- *Faça um print dessa tela.*
- Para esta atividade precisamos limpar o cache do arp. Execute o comando **arp -d**.
- Inicie o sniffer Wireshark, e inicie captura de pacotes.
- Execute o comando `ping -n 10 www.ust.hk` (servidor Web em Hong Kong - University of Science and Technology). O argumento "-n 10" indica que 10 mensagens de Ping devem ser enviadas.
- Quando o programa Ping terminar, pare a captura de pacotes no Wireshark.

A - No final do experimento, seu terminal deve ficar semelhante ao da Figura 1.

1. *Faça um print dessa tela*, cole em um arquivo e em seguida, faça uma análise das informações que constam ali. (Número de pacotes enviados, tempo de resposta, TTL (o que significa?), total de bytes enviado por mensagem, time, perdas, etc...)



```
Terminal
paulo@note ~ $ ping -c 10 www.ust.hk
PING www.ust.hk (143.89.14.2) 56(84) bytes of data.
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=1 ttl=53 time=364 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=2 ttl=53 time=369 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=3 ttl=53 time=423 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=4 ttl=53 time=355 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=5 ttl=53 time=354 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=6 ttl=53 time=358 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=7 ttl=53 time=348 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=8 ttl=53 time=359 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=9 ttl=53 time=363 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=10 ttl=53 time=360 ms

--- www.ust.hk ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9002ms
rtt min/avg/max/mdev = 348.755/365.842/423.307/19.929 ms
paulo@note ~ $
```

Figura 1: Comando PING

B - A figura 2 apresenta uma imagem da saída no Wireshark, depois que o filtro "icmp" foi aplicado.

No Campo 1 Constam os pacotes capturados e os seus respectivos protocolos, no campo 2 estão as informações de cada pacote individualmente, para visualizar essas informações, basta escolher um pacote no campo 1 e clicar sobre ele. No campo 3 são os dados que cada pacote carrega.

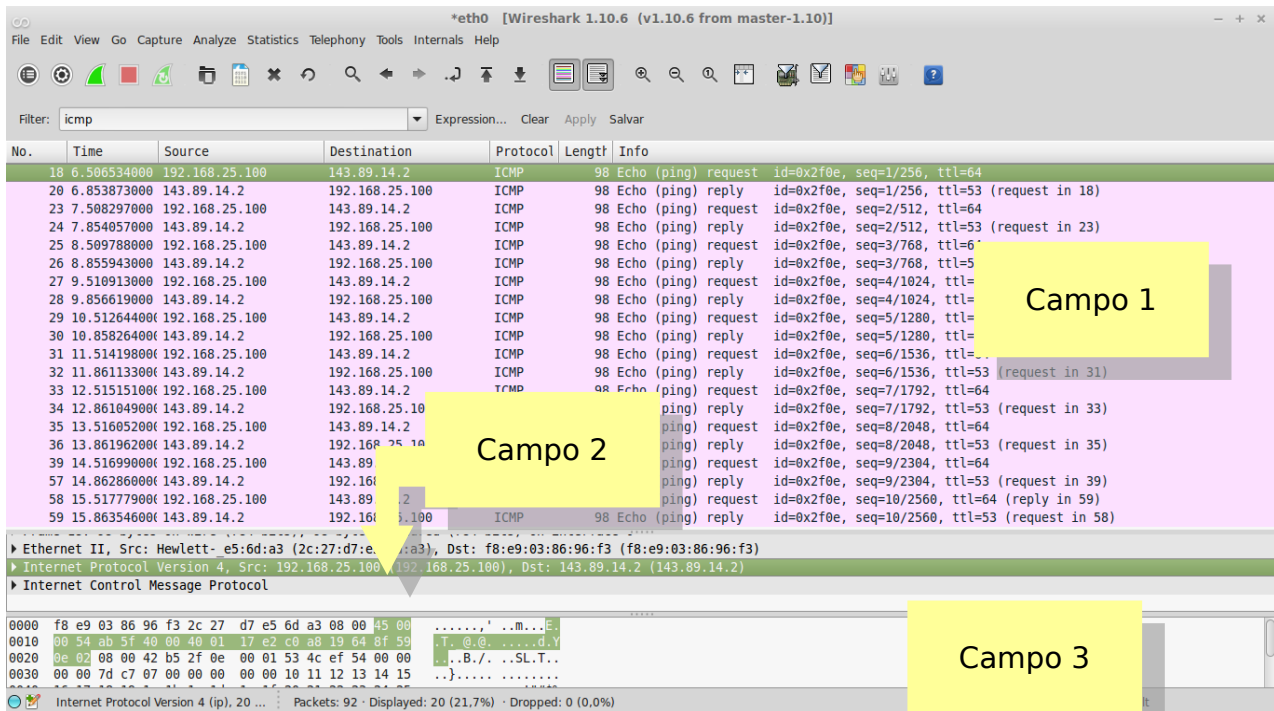


Figura 2: Pacotes ICMP no Wireshark

1. Faça um print da tela de seu experimento e em seguida faça uma análise das informações constantes ali.
2. Quantos protocolos você pode identificar?
3. Cite pelo menos 5 protocolos e seus significados.

C - Filtre somente o protocolo o protocolo ARP. *Faça um print da tela.*

1. Explique o endereço MAC de destino no cabeçalho Ethernet.
2. Quais os endereços MAC de origem e destino no cabeçalho Ethernet?
3. Quais os endereços IP associados aos MACs?
4. O que significa a expressão "who has" e "Tell" no wireshark?

D - Filtre somente o protocolo ICMP. *Faça um print da tela.*

1. Quantos pacotes ICMP trafegaram na rede?
2. O TTL no Wireshark é o mesmo do prompt de comando? Os valores variam no Wireshark? Porque?
3. Qual a diferença de request e replay?
4. Qual é o IP de origem?
5. Qual é o IP de destino?
6. Quais os protocolos utilizados para enviar o frame?
7. Qual é o tipo de encapsulamento do frame?
8. Qual é a versão do protocolo IP?
9. Qual o tamanho do campo Data?
10. O que significa o campo Data?
11. Qual é o tipo, código, checksum, identificador, e o número de sequência do ICMP?

12. Qual o IP do seu computador e qual o IP de do site acessado?
13. Identifique o protocolo IP e descreva as informações do cabeçalho conforme a figura 3.
14. Identifique o protocolo TCP e descreva as informações do cabeçalho conforme a figura 4:

0	4	8	15	16	32
Versão	Tamanho Cabeçalho	Tipo Serviço (TOS)	Tamanho Total (bytes)		
Identificação			Flag	Offset de Fragmentação	
Tempo de Vida (TTL)		Protocolo	Checksum		
Endereço IP Origem					
Endereço IP Destino					
Opções					
Dados					

Figura 3 – Cabeçalho do protocolo IP

0		15 16						32			
Número Porta Origem						Número Porta Destino					
Número Sequenciação											
ACKNOWLEDMENT											
Tamanho do Cabeçalho		Reservado		U R G	A C K	P S H	R S S	S Y N	F I N	Tamanho da Janela de Transmissão	
Checksum						Ponteiro Urgente					
Opções											
Dados											

Figura 4 – Cabeçalho do protocolo TCP