UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
DEPARTAMENTO DE INFORMÁTICA APLICADA
INF01154 - Redes de Computadores N

Nível de Enlace

1 Exercícios do Wireshark – ICMP

1. Abra o arquivo do laboratório de wireshark Ethernet ARP do Kurose, disponível na página da disciplina (*Cap6_Wireshark_Ethernet_ARP_v7.0.pdf*). **Execute todos os exercícios de forma online**.

2 Exercícios adicionais

1. Leia o help do ping (ping –h ou "$man ping") e efetue os seguintes testes com a ajuda do sniffer:
    a. Fazer um ping com 6 requisições de echo, tamanho do pacote de 300 bytes, TTL de 79. Mostre o comando utilizado e prove que funcionou através de uma imagem. Na imagem, mostre que o TTL funcionou e que o tamanho do pacote funcionou.
    b. Fazer um ping forçando a não fragmentação do pacote (-f no Windows ou "-M do" no linux) e tamanho do pacote de 1500 bytes (tamanho máximo dos dados no Ethernet). Verificar qual o máximo tamanho do pacote que funciona. Explique.
    c. Qual a mensagem (pacote de dados) enviados num comando de ping? Sugestão: analise com o sniffer o pacote ICMP.

2. Utilizar um sniffer de redes para analisar o funcionamento do ping. Capturar o ping de sua máquina para um vizinho, preencha na tabela linha a linha a sequência de comandos de um ping, explicando cada linha (mostrando o endereço nível 2 (MAC) e nível 3 (IP) envolvido em cada linha). Também deve ser considerado o protocolo ARP, além do ICMP. Pode-se utilizar a simbologia MAC_A (MAC da máquina A), MAC_B (MAC da máquina B) e MAC-R (MAC do roteador), por exemplo. Da mesma forma, pode-se utilizar IP_A, IP_B, etc. Quando não existirem pacotes no nível, basta deixar sem preenchimento.

   PS: O protocolo ARP deve aparecer na tabela.

Protocolo	End. MAC	End. IP	Descrição
Ex: arq request	Ex: Mac_x -> …		blá
Ex: icmp request	Ex: Mac_x -> Mac_y	Ex: IPx->IPy	

3. Repetir a tabela acima, porém fazendo ping para uma subrede diferente (usando nome em vez de IP para forçar resolução DNS). O protocolo ARP deve aparecer na tabela (sugestão: encadear comandos: "sudo arp –d IPROTEADOR ; ping www.xxx" OU "sudo arp –d IPROTEADOR && ping www.xxx"). Sugestão de filtro: arp or icmp or dns. Incluir a chamada ao DNS na tabela.

4. Faça, obrigatoriamente com apoio do sniffer, uma análise completa de um pacote Ethernet (todos os pacotes vão ser Ethernet). Liste todos os valores dos campos encontrados no cabeçalho do pacote Ethernet. Comparar teoria (campos da definição do protocolo) e prática (wireshark) para todos campos.


Hey
What's your address? 7:05 PM
173.168.15.10 7:05 PM
No man. Your local address. 7:05 PM
127.0.0.1 7:06 PM
Oh you geeky nerd!!!
I mean your physical address.
11:46 PM
29:01:38:62:31:58 11:47 PM
11:47 PM
Message