uni-bh	CENTRO UNIVERSITÁRIO DE BELO HORIZONTE

Curso: Ciência Computação **Disciplina: Redes de Computadores** **Professor: Wagner José Rodrigues**

Objetivo: Conceitos sobre analisador de Protocolos e uso do sniffer wireshark

Atividade 1: Detalhando o ping com o uso do wireshark
Leitura indicada sobre endereço MAC e protocolo ARP: Kurose páginas 348 a 353

1) Inicie a captura do wireshark
2) Efetue o ping para o gateway padrão e pare a captura
3) Utilizando o resultado obtido no wireshark, pede-se:

a. Verifique as informações contidas no protocolo ARP (address resolution protocol – protocolo de resolução de endereços). Identifique as camadas e protocolos e em que camada temos um endereço de broadcast

b. Filtre os pacotes referentes ao serviço ping

c. Identifique as camadas apresentadas.

d. Verifique o tempo necessário para a recepção de todos os pacotes.

e. Identifique os endereços IP (Internet Protocol) e MAC (media access control: controle de acesso ao meio) da sua máquina e do gateway. Em que camadas os mesmos são descritos?

d) Inicie uma nova captura e efetue o seguinte ping: 201.7.176.59

f. Pare a captura. Perceba que a estrutura dos pacotes ICMP continua a mesma. A que máquinas se referem os endereços IP e MAC de origem e destino?

g. Digite o comando que deve ser digitado no prompt DOS para efetuar um ping com 10 pacotes com o envio de 50 bytes de dados cada.

Atividade 2 → Filtrando informações no Wireshark

1) Inicie a captura no WireShark.
2) Inicie um navegador
3) Solicite a abertura de uma página qualquer na internet, aguarde a recepção da mesma e pare a captura no wireshark.
4) Efetue as seguintes filtragens. Anote a informação que deve constar no campo Filter.

DICA: verifique informações constantes no ícone ”Display Filter”.

a) Somente pacotes TCP com exceção dos HTTP
b) Somente pacotes UDP com exceção dos DNS
c) Somente pacotes que contenham o endereço IP de um servidor acessado.
d) Somente pacotes que contenham o endereço físico (MAC) da sua máquina
e) Todos os pacotes com informação TCP usando a porta 80. A que serviço esta porta se refere?
f) Todos os pacotes com informação UDP usando a porta 53. A que serviço se refere esta porta?
g) Todos os pacotes com exceção dos protocolos HTTP e DNS