Universidade Federal do Vale do São Francisco – UNIVASF
Curso: Engenharia da Computação
Disciplina: Redes de Computadores I **Data de entrega:** 11/11/08
Professor: Leonardo Barreto Campos **Valor:** 1,0

Projeto - III[1]

Nesse projeto, o aluno investigará o protocolo ARP e IP. É importante que o aluno possua embasamento nesses protocolos e conhecimento das RFCs 826 (ftp://ftp.rfc-editor.org/in-notes/std/std37.txt) e RFC 791 (http://www.ietf.org/rfc/rfc0791.txt?number=791) que referem-se aos protcolos ARP e IP respectivamente.
O projeto consiste em analisar o tráfego de pacotes com auxílio da ferramenta Wireshark (http://www.wireshark.org/docs/wsug_html_chunked/index.html) e responder as perguntas gradativamente. Dessa forma, siga extritamente as orientações relacionadas abaixo e bom trabalho.

Cache do ARP

- Lembre-se que o protocolo ARP tipicamente mantem um cache com pares de tradução (endereços IP para Ethernet) em seu computador. O comando *arp* (tanto no MSDOS e Linux/Unix) é usado para visualizar e manipular o contéudo desse cache. Visto que o comando *arp* e o protocolo ARP tem o mesmo nome, eles são facilmente motivo de confusão. Mas coloque em sua cabeça que eles são diferentes – o comando *arp* é usado para visualizar e manipular o conteúdo do Cache do ARP. Enquanto que o protocolo ARP define o formato e propósito das mensagens enviadas e recebidas, e define as ações sobre o recebimento e transmissão de mensagens.
- Inicialmente vamos dar uma olhada no conteúdo do cache do ARP em seu computador. Linux/Unix: O executável do comando *arp* pode ser encontrado em vários lugares, as localizações mais populares são /sbin/arp (parao linux) e /usr/etc/arp (para variações do Unix). O comando *arp* sem argumentos irá mostrar o conteúdo do cache do ARP em seu computador.

Questão 1: Rode o comando arp, capture a tela de saída e coloque como Anexo I do projeto.

Questão 2: Qual é a significado de cada valor da coluna?

Enviando e recebendo mensagens ARP

- A fim de observar seu computador enviando e recebendo mensagens ARP, nós precisamos limpar o cache do ARP. Caso isso não seja realizado, seu computador não enviará uma mensagem ARP na rede para encontrar a tradução dos endereços IP-Ethernet.
- Linux/Unix: O comando *arp -d ** irá limpar o cache do ARP. Para rodar esse comando você precisa ter privilégios de root.

[1] Laboratório adaptado do site http://wps.aw.com/wps/media/objects/2567/2629599/Ethereal_Ethernet_ARP.pdf

Questão 3: Rode o comando *arp -d *,* imprima novamente a tabela ARP, capture a tela de saída e coloque como Anexo II do projeto.

Observando o ARP em ação

- Certifique que o cache do ARP está limpo como descrito anteriormente.
  Em seguida, certifique-se que o cache do seu browser está vazio(Para fazer isso no Mozilla, selecione Ferramentas → Opções → Avançado → Rede → Armazenamento offline → Limpar agora. No Internet Explorer, selecione, Ferramentas → Opções da Internet → Excluir Arquivos);
- Inicialize o sniffer Wireshark (velho e bom Ethereal);
- Entre com a seguinte URL em seu browser
  http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-lab-file3.html
- Pare a captura de pacotes no Wireshark. Nós não estamos interessados no IP ou protocolos de alto nível, dessa forma, altere a janela do Wireshark (listing of captured packets) para que a ferramente mostre informações somente sobre protocolos inferiores ao IP. Para que o Wireshark faça isso, selecione *Analyze* → *Enable Protocols*. Então desmarque o caixa do IP e selecione OK.

Questão 4: Selecione o primeiro quadro que contenha uma requisição ARP e mostre a tela do Wireshark.

Visualizando e imprimindo detalhes do quadro

- Para responder as questões a seguir, você necessitará olhar os detalhes dentro do quadro (janelas intermediárias e mais abaixo da ferramenta);
- Selecione o quadro Ethernet que contém a primeira requisição ARP. Expanda as informações contidas no quadro.

Questão 5: Após expandir as informações, capture a tela e mostre os detalhes do quadro ARP Request.

Questão 6: Quais são os valores hexadecimais para endereços de fonte e destino em cada quadro Ethernet contído na mensagem de requisição ARP?

Questão 7: Pegue o valor hexadecimal dos dois bytes do **campo tipo** do quadro. O que significa todos os bits do campo flag valerem 1?

Questão 8: A mensagem ARP contém o endereço IP do emissor?

- Em seguida, identifique o quadro ARP reply que foi enviado na resposta da requisição ARP (ARP Request), expanda as informações do quadro e responda as questões a seguir:

Questão 9: Após expandir as informações do ARP reply, capture a tela e mostre os detalhes desse quadro.

Questão 10: Quais são os valores hexadecimais para endereços de fonte e destino em cada quadro Ethernet contído no ARP reply?

Questão 11: Qual é o valor do campo opcode no qual a parte do quadro Ethernet contém a carga útil do ARP em que uma resposta ARP é feita?