

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RN DISCIPLINA: REDES DE COMPUTADORES PROFESSOR: TADEU FERREIRA TÉCNICO EM INFORMÁTICA

Ethereal Lab: Ethernet e ARP

Neste laboratório investigaremos a camada de enlace usando o padrão Ethernet e o protocolo ARP. Como referência usaremos o livro: *"Redes de computadores: uma abordagem top down"* 3a. Edição de James F. Kurose especificamente o capítulo 5 deste livro.

É importante lembrar que não trabalharemos com informações acima da camada de enlace, portanto para esta laboratório consideraremos apenas os endereços físicos ou endereços MAC.

Neste laboratório usaremos a ferramenta Wireshark, esta ferramenta nos possibilita ver o conteúdo de cada quadro de dados que passa pela placa de rede do computador. Você pode obter o wireshark a partir do site oficial: <u>http://www.wireshark.org/</u>

Capturando e Analisando pacotes Ethernet

Vamos inicialmente capturar alguns quadros Ethernet para analisar. Para capturar os pacotes siga as instruções:

- Tenha certeza que o cache do seu browser está vazio. Isso garante que nossas requisições vão necessariamente ser feitas ao servidor de destino, e não serão respondidas pela cache local. (No firefox faça Ferramentas → Limpar histórico Recente, No IE8 faça Segurança → Apagar histórico de navegação → Marque a opção Arquivos Temporários de Internet → clique em delete)
- Abra o Wireshark
- Clique no botão "List Available Capture Interfaces" à esquerda.
- Inicie a captura clicando em START na placa de rede conectada à rede
- Use o browser para acessar a URL: http://dietinf.ifrn.edu.br/doku.php
- Pare o capturador de pacotes Wireshark clicando no botão Stop Running Live Capture você deve ter uma tela como a mostrada abaixo

⊗ 🛇 🛇 (Untitled) - Wireshark				
File Edit View Go Capture Analyze Statistics Telephony Tools Help				
🗟 🍇 🎕 😂 🖆 🔛 🗶 C 😑 I Q 🧅 🔶 🍝 두 📘 🔲 I Q Q Q 🕅 🚳 🔹				
Filter:			▼ Express	sion Clear Apply
No Time	Source	Destination	Protocol	Info
298 26.091	218 200.137.2.1	10 10.20.2.109	тср	http > 53249 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
299 26.091	242 10.20.2.109	200.137.2.110	ТСР	53249 > http [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=
300 26.091	313 10.20.2.109	200.137.2.110	HTTP	GET /doku.php HTTP/1.1
301 26.093	189 200.137.2.1	10 10.20.2.109	TCP	http > 53249 [ACK] Seq=1 Ack=822 Win=7488 Len=0 TS
302 26.151	779 65.55.64.25	4 10.20.2.109	HTTP	HTTP/1.1 200 OK
303 20.151	830 10.20.2.109			50890 > nttp [ALK] Seq=34/5 ACK=258/ W1N=999 Len=0
305 26,188	189 10.20.2.109	200.137.2.110	ТСР	53249 > http [ACK] Seg=822 Ack=1449 Win=8768 Len=0
306 26.190	449 200.137.2.1	10 10.20.2.109	ТСР	[TCP segment of a reassembled PDU]
<pre>+ Frame 300 (887 bytes on wire, 887 bytes captured) + Ethernet II, Src: Intel_ae:f6:39 (00:18:de:ae:f6:39), Dst: Intel_76:4a:40 (00:0e:0c:76:4a:40) + Internet Protocol, Src: 10.20.2.109 (10.20.2.109), Dst: 200.137.2.110 (200.137.2.110) + Transmission Control Protocol, Src Port: 53249 (53249), Dst Port: http (80), Seq: 1, Ack: 1, Len: 821</pre>				
- Hypertext Transfer Protocol				
+ GET / doku.pnp HTP/1.1\r\n				
User-Agent: Mozilla/5.0 (X11; U; Linux i686; pt-BR; v:1.9.2.3) Gecko/20100423 Ubuntu/10.04 (lucid) Firefox/3. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n				
Accept-Encoding: gzip.deflate\r\n				
0040 46 02 47 0050 48 54 54 0060 64 69 65 0070 2e 62 72 0080 20 4d 6f 0090 31 3b 20 0080 20 4d 6f 0090 31 3b 20 0080 32 2e 33	45 54 20 2f 64 50 2f 31 2e 31 74 69 6e 66 2e 0d 0a 55 73 65 7a 69 6c 6c 61 55 3b 20 4c 69 74 2d 42 52 3b 29 20 47 65 63	6f 6b 75 2e 70 68 70 0d 0a 48 6f 73 74 3a 69 66 72 6e 2e 65 64 72 2d 41 67 65 6e 74 2d 41 67 65 68 74 2f 35 2e 30 20 28 58 6e 75 78 20 92 38 38 20 72 76 3a 31 20 32 39 6b 6f 2f 32 30 31 30	20 F.GET , 20 HTTP/1 75 dietin 3a .brU 31 Mozil 36 1; U; I 2e ; pt-BF 30 2.3) G	/d oku.php .1Host: f. ifrn.edu se r-Agent: la /5.0 (X1 Li nux i686 R; rv:1.9. ec ko/20100
O Hypertext Transfer Protocol (http), 821 bytes Packets: 778 Displayed: 778 Profile: Default				

O protocolo ARP

O protocolo ARP é utilizado para descobrir ou resolver o Endereço MAC a partir de um endereço IP conhecido.

Use o comando *arp* para ver os valores atuais da sua cache de ARP. Ao executar o comando *arp* você deve obter uma resposta como essa:

```
#arp
```

```
EndereçoTipoHWEndereçoHWFlagsMáscaraIface192.168.2.4ether00:21:8d:01:5d:b5Ceth0
```

- 1. O que significa cada campo?
- 2. Quantas entradas há na sua tabela? Compare suas entradas com as do computador vizinho, são as mesmas entradas? Por quê?

Voltando ao Wireshark, use o campo *filter* para buscar um pacote arp. Para isso escreva *arp* no campo *Filter* e clique em *Apply*. O wireshark irá mostrar apenas os pacotes do tipo ARP.

- 3. Observe no painel central o quadro EthernetII. O que significa o campo Destination Address? Qual o valor dele? Por que este valor?
- 4. No painel central selecione Adress Resolution Protocol. O que significam os campos: Sender Mac Address, Sender IP Address, Target MAC Address e Target IP Address?
- 5. Há dois tipos de pacote ARP, um é uma requisição (request) mandada em broadcast e outro a resposta(reply) mandada em unicast. Identifique em sua captura os dois tipos de pacote, quais campos são diferentes nos campos do ARP?