

Redes de Computadores

TRABALHO Nº3, PL64

Ana Margarida Sousa Pimenta, A100830

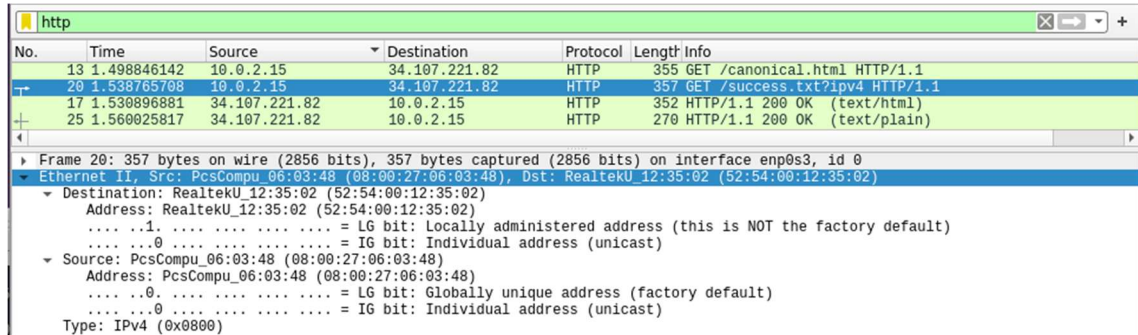
Miguel Tomás Antunes Pinto, A100815

Pedro Miguel Costa Azevedo, A100557

Captura e análise de Tramas Ethernet

1. Anote os endereços MAC de origem e de destino da trama capturada. Identifique a que sistemas se referem. Justifique.

O endereço MAC de origem é exibido no campo "Source" e o endereço MAC de destino é exibido no campo "Destination" pelos valores inseridos entre aspas e separados por dois pontos.



No.	Time	Source	Destination	Protocol	Length	Info
13	1.498846142	10.0.2.15	34.107.221.82	HTTP	355	GET /canonical.html HTTP/1.1
20	1.538765708	10.0.2.15	34.107.221.82	HTTP	357	GET /success.txt?ipv4 HTTP/1.1
17	1.530896881	34.107.221.82	10.0.2.15	HTTP	352	HTTP/1.1 200 OK (text/html)
25	1.560025817	34.107.221.82	10.0.2.15	HTTP	270	HTTP/1.1 200 OK (text/plain)

Frame 20: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_06:03:48 (08:00:27:06:03:48), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
Address: RealtekU_12:35:02 (52:54:00:12:35:02)
.....1. = LG bit: Locally administered address (this is NOT the factory default)
.....0 = IG bit: Individual address (unicast)
Source: PcsCompu_06:03:48 (08:00:27:06:03:48)
Address: PcsCompu_06:03:48 (08:00:27:06:03:48)
.....0 = LG bit: Globally unique address (factory default)
.....0 = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)

Através deste print é possível comprovar que o nosso computador é a source da trama, enquanto que o destino é o servidor que acedemos a partir do link disponibilizado no enunciado.

2. Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?

O valor do campo hexadecimal é 0x0800 e representa o protocolo de IPV4 (visível na imagem utilizada na pergunta anterior).

3. Quantos bytes são usados no encapsulamento protocolar, i.e. desde o início da trama até ao início dos dados do nível aplicacional (Application Data Protocol: http-over-tls, no caso de HTTPS)? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar.

////////////////////

A seguir responda às seguintes perguntas, baseado no conteúdo da trama Ethernet que contém o primeiro byte da resposta HTTP proveniente do servidor.

4. Qual é o endereço Ethernet da fonte? A que sistema de rede corresponde? Justifique.

O endereço de ethernet da fonte é 08:00:27:06:03:48(MAC origem) e é interface do nosso computador. Isso pode ser verificado através da análise da trama capturada, que apresenta o endereço MAC de origem na camada de enlace de dados, que é atribuído à interface de rede do dispositivo que enviou a trama. Nesse caso, o endereço Ethernet de origem identifica o adaptador de rede do computador que enviou a requisição HTTP para o servidor.

5. Qual é o endereço MAC do destino? A que sistema (host) corresponde?

O MAC de destino é 52:54:00:12:35:02 (destination da imagem da pergunta 1) e corresponde ao default gateway da rede local. Devido ao fato de o servidor não estar localizado na rede local, ele não pode ser acessado diretamente por nós. Por isso, as tramas serão trocadas entre o nosso computador e o gateway padrão, em vez de serem enviadas diretamente para o servidor.

6. Atendendo ao conceito de encapsulamento protocolar, identifique os vários protocolos contidos na trama recebida. Justifique, indicando em que campos dos cabeçalhos capturados se baseou.

A trama recebida contém diversos protocolos encapsulados em camadas sendo estes a Ethernet, o IPv4 e TCP. Para identificar esses protocolos, analisamos os cabeçalhos dos pacotes em cada camada, que contém informações sobre endereços, tipos de protocolo, portas de origem e destino, e números de sequência.

Protocolo ARP

1. (a) Abra uma consola no PC onde efetuou o ping. Observe o conteúdo da tabela ARP com o comando arp -a.

```
root@n1:/tmp/pycore.38495/n1.conf# arp
Address          HWtype  HWaddress      Flags Mask    Iface
192.168.0.1      ether   00:00:00:aa:00:00  C             eth0
root@n1:/tmp/pycore.38495/n1.conf#
```

No que toca à sua interpretação, na coluna Address verificamos o endereço físico correspondente ao endereço IP de um dispositivo na rede local. O HWtype diz nos o tipo de protocolo usado na camada física. Já o HWaddress indica o endereço MAC. O Flags informa do tipo do registo que está a

ser alocado em memória. Sendo que o tipo que obtemos é C, o que nos indica que este tipo foi obtido pelo protocolo ARP. A coluna Mask diz nos a máscara de subrede. Por último, a lface dá-nos a interface da rede, que é neste caso eth0.

(b) Indique, justificando, qual o equipamento da intranet em causa que poderá apresentar a maior tabela ARP em termos de número de entradas.

O equipamento da intranet em causa que poderá apresentar a maior tabela ARP é o router pois este precisa de armazenar informações ARP para todos os dispositivos conectados à rede local e para todos os dispositivos conectados remotamente.

2. (a) Qual é o valor hexadecimal dos endereços MAC origem e destino? Como interpreta e justifica o endereço destino usado?

O endereço de destino utilizado é o de broadcast, ff:ff:ff:ff:ff:ff. A mensagem de broadcast é enviada para todos os dispositivos numa rede, sem destinatário específico. Permite enviar informações para múltiplos dispositivos simultaneamente, mas pode sobrecarregar a rede se usada em excesso. (FALTA VER O ENDEREÇO MAC)

(b) Qual o valor hexadecimal do campo Tipo da trama Ethernet? O que indica?

O valor é 0x0806 e indica nos que se trata de um protocolo ARP.

(c) Observando a mensagem ARP, como pode saber que se trata efetivamente de um pedido ARP? Refira duas formas distintas de obter essa informação.

Para confirmar que se trata de um pedido ARP podemos verificar o valor do opcode, se este for 1 confirma-se que é de facto uma solicitação. Caso esse valor seja 2, nesse caso, trata-se de uma resposta. Outro modo de verificar se é ou não pedido é verificando o endereço MAC de destino (Target MAC Address). Se se tratar de um pedido, este campo estará preenchido a zeros.

(d) Explícite, em linguagem comum, que tipo de pedido ou pergunta é feita pelo host de origem à rede?

A mensagem "Who has 192.168.64.1? Tell 192.168.64.3" é enviada por um dispositivo para encontrar o endereço MAC de outro dispositivo que se encontra na mesma rede. Quando um dispositivo encontra o endereço IP solicitado este responde com um ARP Reply que contém o endereço MAC correspondente. O objetivo consiste em atualizar as tabelas ARP nos dispositivos da rede local, permitindo a comunicação

usando endereços MAC. O Wireshark é uma ferramenta para capturar e analisar essas mensagens.

3. Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.

(a) Qual o valor do campo ARP opcode? O que especifica?

O valor do campo opcode é "reply (2)", o que significa que se trata de um ARP reply.

(b) Em que posição da mensagem ARP está a resposta ao pedido ARP efetuado?

Encontra-se no campo Sender MAC Address.

(c) Identifique a que sistemas correspondem os endereços MAC de origem e de destino da trama em causa, recorrendo aos comandos ifconfig, netstat -rn e arp executados no PC selecionado.

////////////////////////////////////

(d) Justifique o modo de comunicação (unicast vs. broadcast) usado no envio da resposta ARP (ARP Reply).

A resposta ARP é enviada por unicast sendo especificamente direcionada para o dispositivo que fez a solicitação ARP original. A vantagem do unicast comparativamente ao broadcast reside no facto de que se economiza largura de banda e processamento na rede o que, por sua vez, promove a eficiência.

4. Verifique se o ping feito ao segundo PC originou pacotes ARP. Justifique a situação observada.

Sim, o segundo ping origina pacotes ARP, pois através do Wireshark verifica-se que a solicitação é enviada para obter esse endereço, se for bem-sucedida, o dispositivo receberá uma resposta ARP.

5. Identifique na mensagem ARP os campos que permitem definir o tipo e o tamanho dos endereços das camadas de rede e de ligação lógica que se pretendem mapear. Justifique os valores apresentados nesses campos.

Os comandos que identificam o tipo são o Hardware Type e o Protocol Type, já os que identificam o tamanho Hardware Size e o Protocol Size.

O Hardware Type indica o tipo de hardware utilizado na camada de ligação lógica, verificando-se neste caso o Ethernet. Cada tipo de hardware tem um valor numérico único atribuído a ele, no caso do Ethernet esse valor é 1. O Protocol Type indica o tipo de protocolo utilizado, sendo no nosso caso o IPv4, sendo o seu valor correspondente 0x0800. O campo Hardware Size indica o tamanho do endereço da camada de ligação lógica em bytes, sendo que no nosso caso o tamanho é 6 bytes. Por fim, o Protocol Size indica o tamanho do endereço da camada de rede em bytes, dado que o protocolo é IPv4 o seu tamanho é 4 bytes.

6. Na situação em que efetua um ping a um PC não local à sua sub-rede, esboce um diagrama em que indique claramente, e de forma cronológica, todas as mensagens ARP e ICMP trocadas, até à recepção da resposta ICMP do sistema destino (represente apenas os nós intervenientes). Assuma que todas as tabelas ARP se encontram inicialmente vazias.

3	1.190971462	00:00:00_aa:00:01	Broadcast	ARP	42	Who has 192.168.64.1? Tell 192.168.64.3
4	1.191317187	00:00:00_aa:00:07	00:00:00_aa:00:01	ARP	42	192.168.64.1 is at 00:00:00_aa:00:07
5	1.191329247	192.168.64.3	192.168.192.3	ICMP	98	Echo (ping) request id=0x001b, seq=1/256, ttl=64 (reply in 6)
6	1.191834443	192.168.192.3	192.168.64.3	ICMP	98	Echo (ping) reply id=0x001b, seq=1/256, ttl=62 (request in...)

```
vcmd
root@n1:/tmp/pycore.35207/n1.conf# ping 192.168.192.3
PING 192.168.192.3 (192.168.192.3) 56(84) bytes of data.
64 bytes from 192.168.192.3: icmp_seq=1 ttl=62 time=0.882 ms
^C
--- 192.168.192.3 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.882/0.882/0.882/0.000 ms
root@n1:/tmp/pycore.35207/n1.conf#
```

Domínios de colisão

1. Através da opção tcpdump, verifique e compare como flui o tráfego nas diversas interfaces dos vários dispositivos no departamento A (LAN comutada) e no departamento B (LAN partilhada) quando é gerado tráfego intra-departamento (por exemplo, através do comando ping). Que conclui? Comente os resultados obtidos quanto à utilização de hubs e switches no contexto de controlar ou dividir domínios de colisão. Documente as suas observações e conclusões com base no tráfego observado/capturado.

No departamento A, devido à utilização de um switch é nos possível afirmar que, de facto, a rede é comutada. Dado isto, podemos visualizar que o computador com IP 192.168.192.3, não captura as tramas enviadas pelo computador de IP 192.168.64.3, por sua vez são capturadas outras tramas que, no entanto, não se relacionam com o ping que executamos.

```

vcmd
root@n1:/tmp/pycore.35207/n1.conf# ping 192.168.192.3
PING 192.168.192.3 (192.168.192.3) 56(84) bytes of data.
64 bytes from 192.168.192.3: icmp_seq=1 ttl=62 time=0.737 ms
64 bytes from 192.168.192.3: icmp_seq=2 ttl=62 time=0.142 ms
64 bytes from 192.168.192.3: icmp_seq=3 ttl=62 time=0.132 ms
64 bytes from 192.168.192.3: icmp_seq=4 ttl=62 time=0.198 ms
^C
--- 192.168.192.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3079ms
rtt min/avg/max/mdev = 0.132/0.302/0.737/0.252 ms
root@n1:/tmp/pycore.35207/n1.conf#

```

```

vcmd
root@n1:/tmp/pycore.35207/n1.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C21:57:14.458615 IP6 fe80::200:ff:feaa:2 > ip6-allrouters: ICMP6, router solicitation, length 16
21:57:14.458663 IP6 fe80::200:ff:feaa:0 > ip6-allrouters: ICMP6, router solicitation, length 16
21:57:15.053877 IP 192.168.64.1 > 224.0.0.5: OSPFv2, Hello, length 44
21:57:17.054831 IP 192.168.64.1 > 224.0.0.5: OSPFv2, Hello, length 44

4 packets captured
4 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.35207/n1.conf#

```

Já no departamento B, uma vez que a rede é partilhada devido ao uso de um hub, pelo que é possível ver as tramas enviadas pelo computador de IP 192.168.192.3.

```

vcmd
root@n10:/tmp/pycore.35207/n10.conf# ping 192.168.64.3
PING 192.168.64.3 (192.168.64.3) 56(84) bytes of data.
64 bytes from 192.168.64.3: icmp_seq=1 ttl=62 time=0.793 ms
64 bytes from 192.168.64.3: icmp_seq=2 ttl=62 time=0.345 ms
64 bytes from 192.168.64.3: icmp_seq=3 ttl=62 time=0.343 ms
64 bytes from 192.168.64.3: icmp_seq=4 ttl=62 time=0.231 ms
^C
--- 192.168.64.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3054ms
rtt min/avg/max/mdev = 0.231/0.428/0.793/0.215 ms
root@n10:/tmp/pycore.35207/n10.conf#

```

```

vcmd
root@n10:/tmp/pycore.35207/n10.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C22:01:05.134551 IP 192.168.192.1 > 224.0.0.5: OSPFv2, Hello, length 44
22:01:07.134936 IP 192.168.192.1 > 224.0.0.5: OSPFv2, Hello, length 44
22:01:08.574925 IP6 fe80::24cd:15ff:fe67:8597.mdnss > ff02::fb.mdnss: 0 [9q] PTR (QM)? _nfs_tcp.local. PTR (QM)? _ipp_tcp.local. PTR (QM)? _ipps_tcp.local. PTR (QM)? _ftp_tcp.local. PTR (QM)? _webdav_tcp.local. PTR (QM)? _webdavs_tcp.local. PTR (QM)? _sftp_ssh_tcp.local. PTR (QM)? _smb_tcp.local. PTR (QM)? _afpov_ertcp_tcp.local. (141)
22:01:06.182925 IP6 fe80::200:ff:feaa:a > ff02::5: OSPFv3, Hello, length 36
22:01:06.252033 IP 192.168.192.1 > 224.0.0.5: OSPFv2, Hello, length 44

5 packets captured
5 packets received by filter
0 packets dropped by kernel
root@n10:/tmp/pycore.35207/n10.conf#

```

2. Construa manualmente a tabela de comutação do switch do Departamento A, atribuindo números de porta à sua escolha.