

Laboratório nº 4

Wireshark

Objetivos

Neste laboratório serão realizadas as seguintes tarefas:

- Aprender a utilizar o *Wireshark* para analisar pacotes na rede;
- Recordar o significado *Portos tcp* e *IPs* de origem e destino;
- Analisar os dados pelas diferentes camadas de rede;
- Analisar os pacotes numa ligação *Telnet* ao terminal virtual do router;
- Perceber a comunicação e equivalência entre endereços físicos *MAC* e lógicos *IP*;
- Analisar a conectividade entre computadores *intraLAN* e *interLAN* usando o simulador.

Parte 1

1. Análise do tráfego de rede - ICMP

O *Wireshark* é um software analisador de protocolos ou uma aplicação (*packet sniffer*) usado para identificar e resolver possíveis problemas de rede (*network troubleshooting*), análise e desenvolvimento de protocolos, etc.

Conforme os fluxos de dados circulam na rede, o *Wireshark* captura a informação (*PDU*), decodifica e analisa seu conteúdo de acordo com as *RFCs* apropriadas ou outras especificações.

Neste laboratório, vamos utilizar o *Wireshark* para capturar informação para posterior análise, a Figura 1 apresenta a interface de programa.

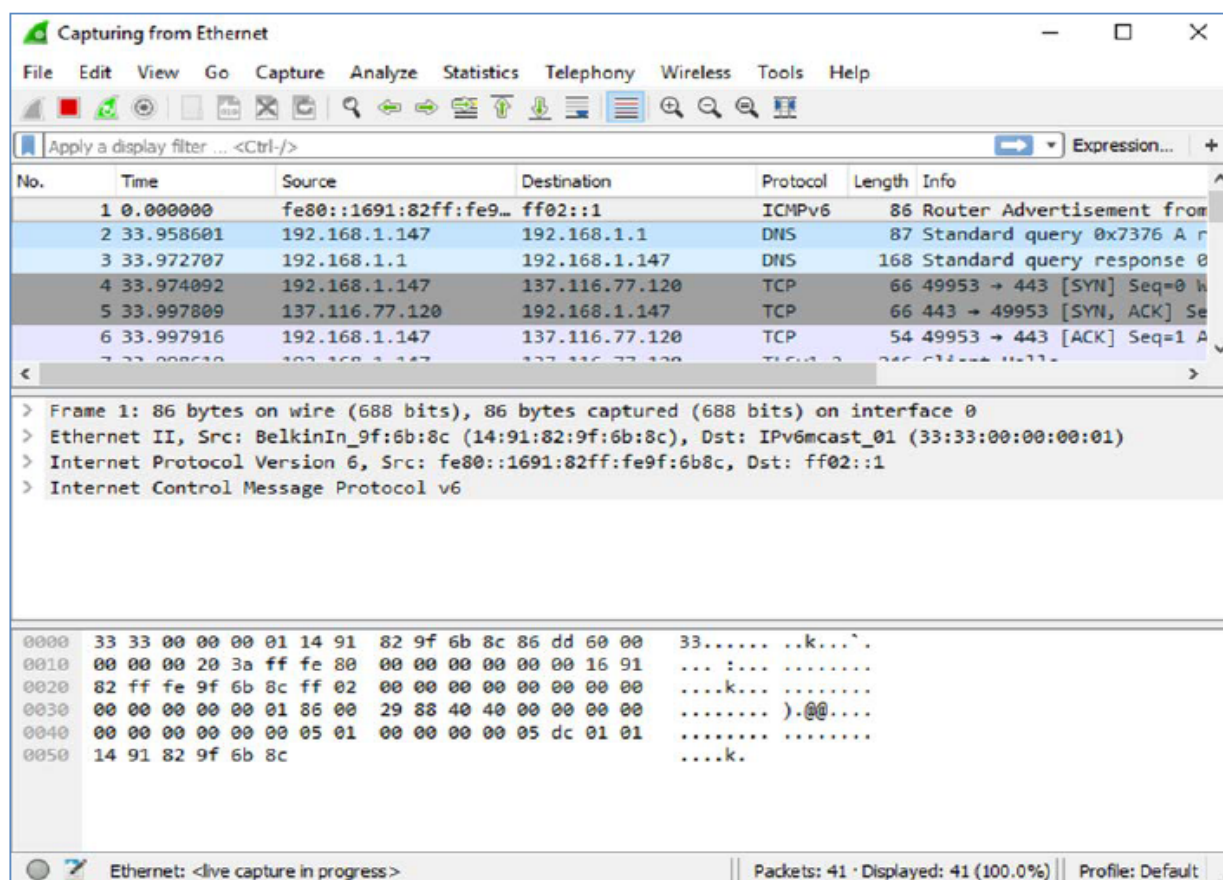


Figura 1 - Interface do Wireshark

Nota: Neste ponto o docente deve mostrar as funcionalidades básicas de captura e análise do software

Exercício 1 - Neste exercício vamos simplesmente capturar informação da rede para verificar o bom funcionamento do *Wireshark*.

- 1) O Wireshark deve ser executado em modo administrador
- 2) Deve seleccionar a interface de rede Ethernet

Estando a funcionar correctamente, deve ver a informação a ser capturada, caso contrário resolva para prosseguir.

Captura dos pacotes ICMP na rede local

Neste exercicio vamos capturar informação da rede, neste caso os pacotes ICMP (ping) entre o seu PC e o default-gateway. Posteriormente analisar e comparar os endereços físicos MAC e os endereços lógicos IP na comunicação.

Exercício 2 - Anote o endereço físico MAC, endereço IP e o endereço IP do default-gateway

MAC: _____
IP: _____
Gateway: _____

Exercício 3 - Captura da informação de rede do ICMP

1. Abra a janela da linha de comandos e prepare o ping para o default-gateway
2. Inicie o *Wireshark* para a captura de pacotes na rede
3. De volta à linha de comando execute o ping ao default-gateway
4. Após o ping terminar, termine a captura do *wireshark*

Exercício 4 - Análise da informação de rede capturada

1. Aplique um filtro no Wireshark para se visualizar apenas os pacotes referentes ao ICMP, como mostra a Figura 2

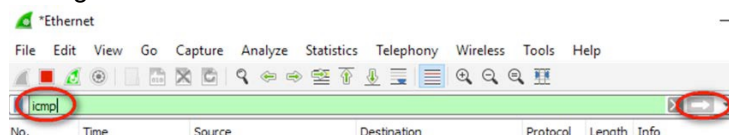


Figura 2 - Filtro icmp

2. Deve ver apenas os pacotes relativos ao ICMP, o ICMP request e o ICMP reply
Consegue visualizar? _____
3. Selecciona o primeiro ICMP com IP origem na sua máquina e IP destino ao default-gateway. Na secção intermedia do Wireshark analise:

IP origem: _____
IP destino: _____
MAC origem: _____
MAC destino: _____

Confira se o endereço MAC origem corresponde ao da sua maquina. _____
Confira se o endereço MAC destino corresponde ao do router. _____

Como foi obtido o MAC destino pelo seu PC? _____


Captura dos pacotes ICMP fora rede local

Neste exercicio vamos capturar informação da rede, neste caso os pacotes ICMP (ping) entre o seu PC e o site www.cisco.com. Posteriormente analisar e comparar os endereços físicos MAC e os endereços lógicos IP na comunicação.

Exercício 5 - Captura da informação de rede do ICMP

1. Abra a janela da linha de comandos e prepare o ping para www.cisco.com
2. Inicie o *Wireshark* para a captura de pacotes na rede
3. De volta à linha de comando execute o ping para www.cisco.com
4. Após o ping terminar, termine a captura do *wireshark*

Exercício 6 - Análise da informação de rede capturada


1. Aplique um filtro no Wireshark para se visualizar apenas os pacotes referentes ao ICMP, como mostra a Figura 2.
2. Deve ver apenas os pacotes relativos ao ICMP, o ICMP request e o ICMP reply
Consegue visualizar? 
3. Seleccione o primeiro ICMP com IP origem na sua máquina e IP destino ao site www.cisco.com. Na secção intermedia do Wireshark analise:

IP origem:  _____.


IP destino:  _____

MAC origem:  _____

MAC destino  _____

Confira se o endereço MAC origem corresponde ao da sua maquina.  _____

Confira se o endereço MAC destino corresponde ao do site www.cisco.com:. _____

Como foi obtido o MAC destino pelo seu PC?  _____

Nota: Porque razão o Wireshark mostra o MAC destino o da interface do router (*default-gateway*)?



2. Análise do tráfego de rede – HTTP, DNS

Nesta etapa vamos capturar a informação do tráfego de rede relativo a um pedido a uma página *web*. Vamos observar os diversos protocolos envolvidos, como o *http* e o *dns*.

Exercício 7 - Captura de pacotes pelo Wireshark

1. Inicie a captura com o Wireshark
2. Inicie a captura de pacotes no *Wireshark* e utilizando o internet explorer navegue até <http://www.york.ac.uk/teaching/cws/www/webpage1.html>. O docente ajudá-lo-á nesta parte.
3. Confirme que o Wireshark conseguiu capturar pacotes. Pare o wireshark.

Exercício 8 - Identifique quais os pacotes relacionados com a navegação feita ao site. Para isso coloque no *wireshark* filtro **http**. Depois escolha um pacote e verifique os portos usados. Com essa informação altere o filtro para: **tcp.port eq 80 and tcp.port eq 53** (pode ter de alterar estes portos consoante aqueles que está a utilizar).

Quais são os protocolos utilizados? _____

Exercício 9 - Altere o filtro para **dns**. Procure os pacotes referentes ao site <http://www.york.ac.uk/>. Pacote Query e Response.

Construa o pacote Query referente ao protocolo *DNS*, Figura 3

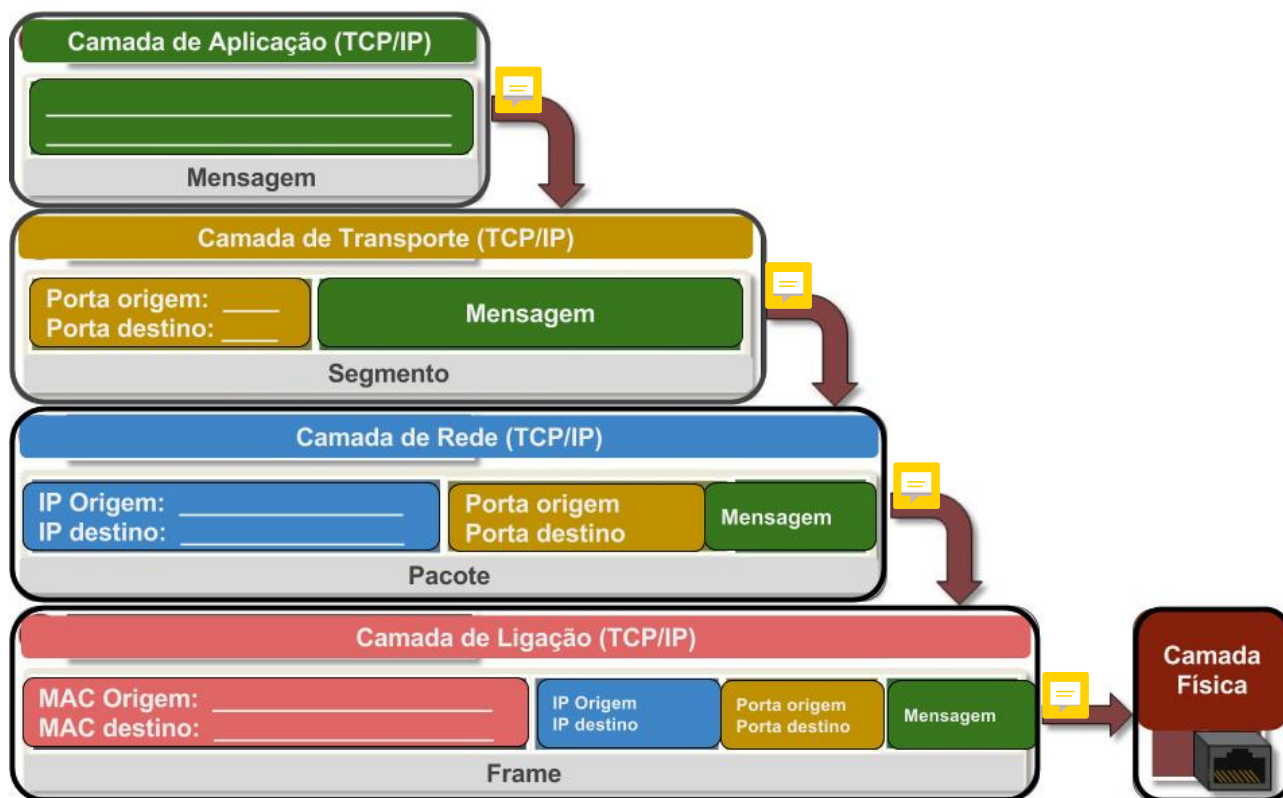


Figura 3 - Modelo de rede em camadas

Construa o pacote Response referente ao protocolo DNS, Figura 4

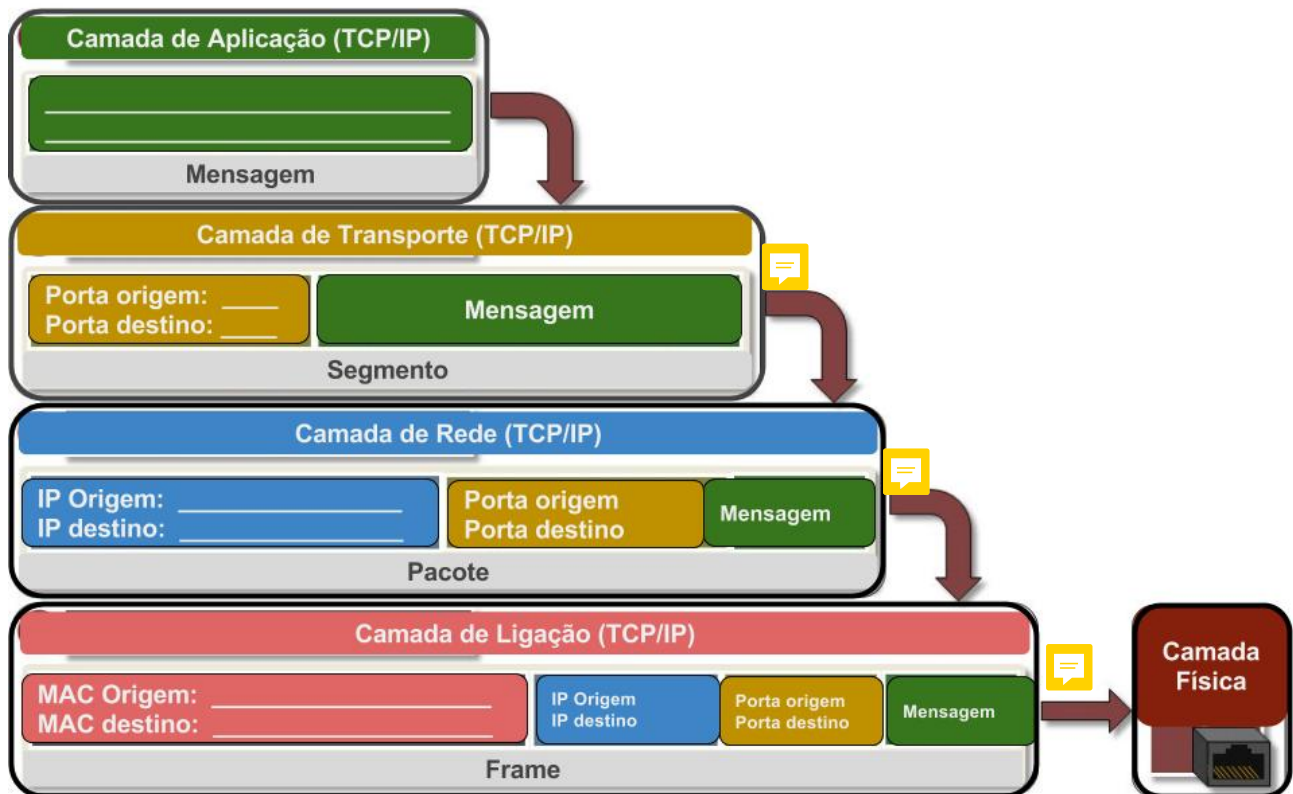


Figura 4 - Modelo de rede em camadas

Qual o IP do site www.york.ac.uk?

Exercício 10 - Volte a colocar o filtro **tcp.port eq 80 and tcp.port eq 53233** (pode ter de alterar estes portos consoante aqueles que está a utilizar).

Exercício 11 - Selecione o primeiro pacote **GET**. Preencha a mensagem deste pacote, nomeadamente:

- request

- a codificação

Exercício 12 - Selecione o segundo pacote **HTTP 200 OK**. Preencha os dados do pacote, Figura 5

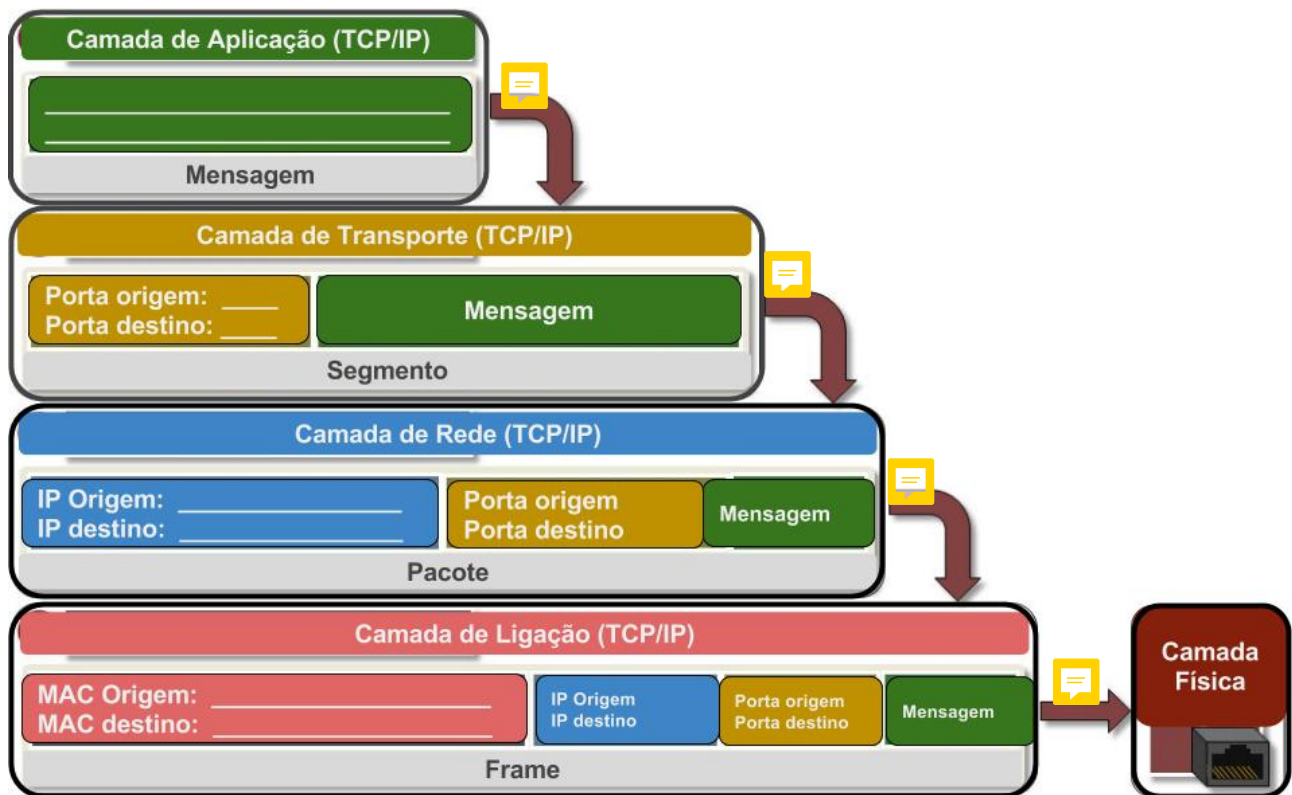


Figura 5 - Modelo de rede em camadas

Consegue visualizar o conteúdo do site através da captura no Wireshark? Onde?

Exercício 13 - Inicie uma nova captura de pacotes no Wireshark e utilizando o internet explorer navegue até <https://www.york.ac.uk/teaching/cws/wws/webpage1.html>.

Consegue visualizar o conteúdo do site através da captura no Wireshark? _____

Explique o porquê _____

Parte 2

3. Análise da comunicação no simulador

O ponto anterior foi utilizado um analisador de protocolos, foi importante na aprendizagem e entendimento das comunicações de rede. Neste exemplo, vamos realizar um cenário de teste que permita consolidar a relação entre endereços físicos *MAC* e endereços lógicos *IPs* no processo de comunicação.

A figura seguinte representa um exemplo possível da topologia de rede da *ESTG* com ligação ao exterior (*internet*). Implemente apenas o cenário das duas *LANs* (*LRSC* e *LCA*) interligados ao router *R1* para testes.

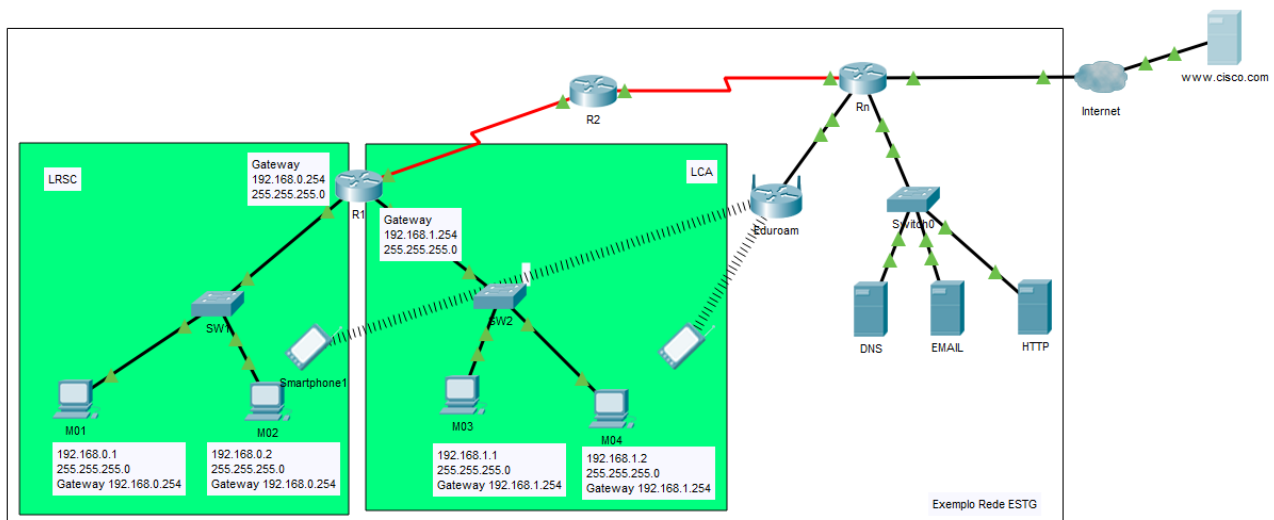


Figura 6 - Interligação de redes com um Router.

Após a configuração do cenário e com conectividade entre todos os *PCs*, iremos analisar o endereçamento *IP* e a sua relação com os endereços físicos (*MAC*).

A **tabela de ARP (Address Resolution Protocol)** existe em todos os *PCs* e faz o mapeamento entre endereços físicos (*MAC*) e endereços *IPs*.

Exercício 14 - Comunicação dentro da mesma rede local:

- Na linha de comandos de *M01* faça o comando **arp -d**
O que faz este comando?







- Faça **ping** de *M01* para *M02*. Na linha de comando faça **arp -a**, o que observa?





- Mude para o **modo simulação** e repita o processo de comunicação entre M01 e M02. Neste modo de simulação o cenário fica parado no tempo para ser possível analisar a informação existente nos pacotes.
- Clique no pacote de ICMP existente no desenho ou no *Simulation Panel*.
- Observe a *tab "Outbound PDU Details"* e preencha a Tabela 1.

Tabela 1 - Análise dos endereços IPs e físicos MAC

IP Origem	IP Destino
	
MAC Destino	MAC Origem
	





Exercício 15 - Comunicação entre PCs em redes diferentes:

- Na linha de comandos de M01 faça **arp -a**
- Faça **ping** de M01 para M03. Na linha de comando faça **arp -a**, o que observa?


- Tem alguma informação sobre o endereço MAC ou endereço IP do PC M03?


- Mude para o **modo simulação** e repita o processo de comunicação entre M01 e M03. Neste modo de simulação o cenário fica parado no tempo para ser possível analisar a informação existente nos pacotes.
- Clique no pacote de ICMP existente no desenho ou no *Simulation Panel*.
- Observe a *tab "Outbound PDU Details"* e preencha a Tabela 2.

Tabela 2 - Análise dos endereços IPs e físicos MAC

IP Origem	IP Destino
	
MAC Destino	MAC Origem
	

<próxima página p.f.>

Comente as diferenças entre o Exercício 14 e Exercício 15?
