Simulação de LANs Ethernet e redes TCP/IP usando CORE

TRABALHO PRÁTICO | REDES DE COMPUTADORES I

Mestrado Integrado em Engenharia de Telecomunicações e Informática

Grupo 6:



Carlos Fonseca
A81868

Leandro Lopes
A82157

J. Eduardo Santos
A82350

UNIVSERSIDADE DO MINHO | ANO LETIVO 2018/2019

Índice

1 Introdução

Este trabalho prático tem por objetivo promover a aquisição de competências na área do projeto da UC de Redes de Computadores I, com base nas tecnologias Ethernet e TCP/IP e através da ferramenta de emulação CORE (*Common Open Research Emulator*) devemos aplicar os conhecimentos já adquiridos.

Com este projeto, pretende-se emular e interligar diversas redes, presentes nas várias fases e recorrendo a uma outra ferramenta, o *wireshark*, poderemos ver e analisar o funcionamento da rede.

2 Fase 2 - Emulação de LANs Ethernet

Nesta fase, pretende-se emular no CORE uma pequena rede local, constituída por dois *Hubs* e um *Switch*. A cada um destes equipamentos de interligação deve ser ligado, pelo menos, dois PCs.

Na realização desta fase, decidimos optar por uma topologia composta por três PCs ligados ao Switch (n1) e dois PCs em cada Hub (n2 e n3), tal como mostra a **Figura 1**.

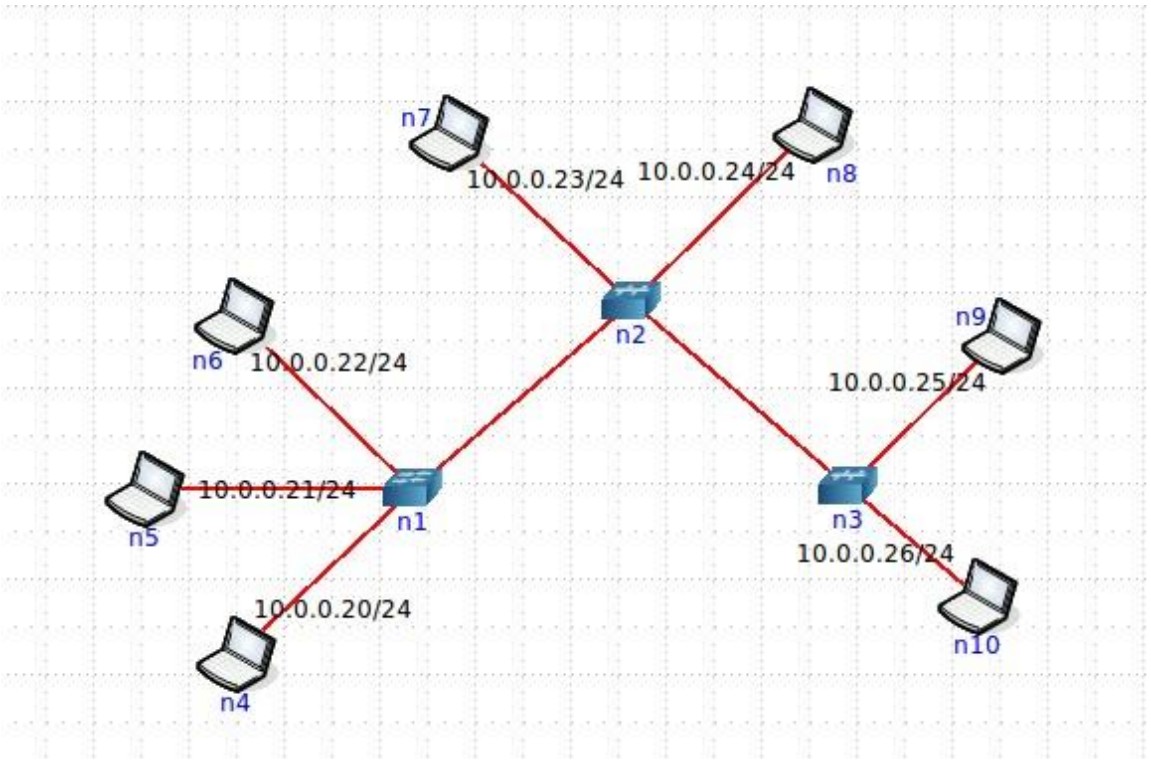

Figura 1 - **Topologia da rede local**

Na simulação desta rede local, efetuaram-se testes de conetividade através do comando *ping* entre alguns terminais para melhor perceção do funcionamento do *Hub*, do *Switch* e do protocolo ARP. Neste último, para observar com mais detalhe a sua função, realizou-se o teste de conetividade ente os terminais n4 e n5 com captura de tráfego no terminal n5, como se pode ver na **Figura 2**.

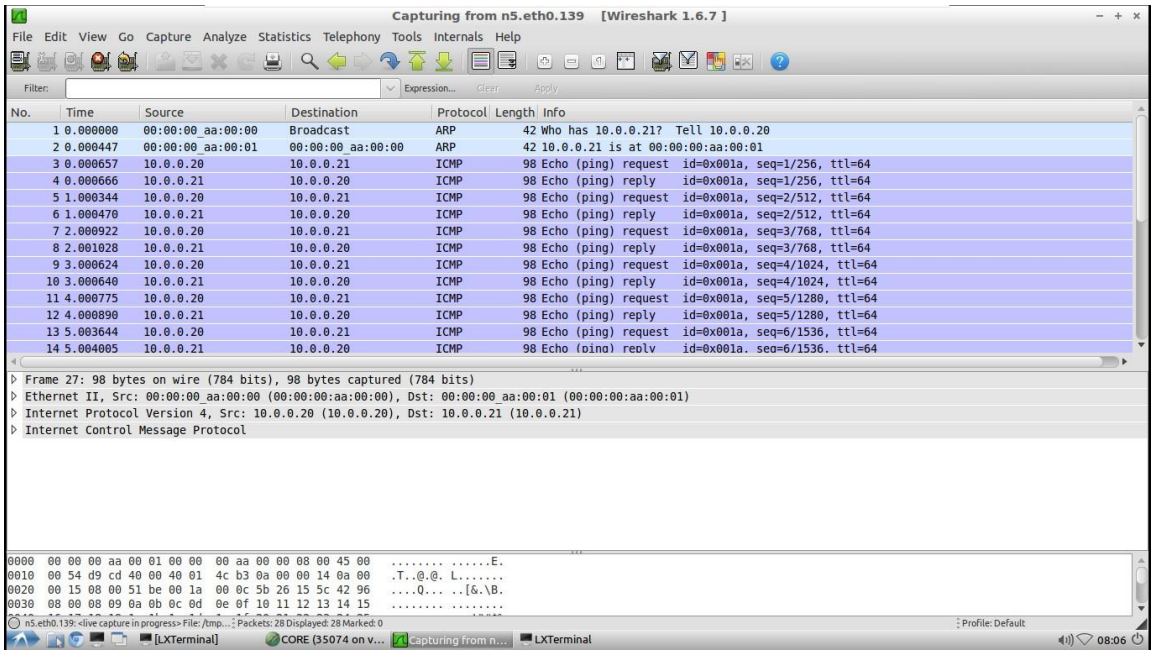

Figura 2 - **Captura de tráfego no terminal n5**

Com base nestes resultados, o protocolo ARP (*Address Resolution Protocol*), numa primeira utilização da rede, envia uma mensagem de *broadcast*. Nesta mensagem, este questiona (*ARP Request*) toda a rede sobre a identidade (endereço MAC) do endereço IP (*Internet Protocol*) correspondente, neste caso, o do terminal n5 (10.0.0.21). Quando a mensagem chega ao destino, este responde (*ARP Reply*) enviando o seu endereço MAC.

3 Fase 3 – Interligação de LANs e redes IP

Nesta fase, o objetivo é construir uma rede de interligação que permita interligar várias redes locais Ethernet. Para isto, é necessário utilizar *routers* capazes de encaminhar o tráfego IP de umas redes para outras.

Para a realização desta fase, é importante criar uma topologia com 5 LANs (Local Area Network) diferentes, cada uma delas centrada num *Hub* ou *Switch,* interligando, pelo menos dois PCs. Cada LAN deve estar conectada a um *router*, consequentemente estes devem estar ligados entre si por caminhos alternativos, formando assim uma rede parcialmente conectada.

A topologia optada, respeitando os requisitos acima descritos, foi a presente na **Figura 3**.

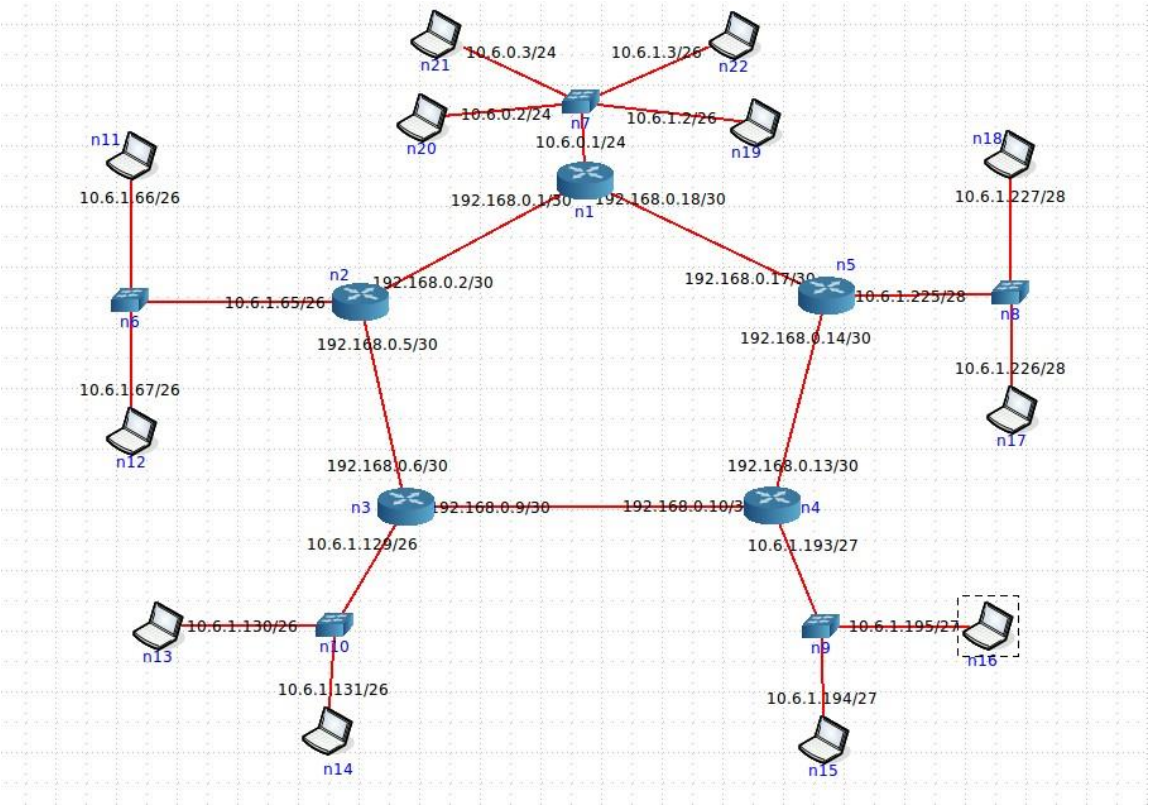

Figura 3 - **Topologia com 5 LANs diferentes**

Nas ligações, entre cada par de *routers,* foram utilizados endereços IP de uma sub-rede com uma máscara de 30 bits, todos obtidos a partir da gama 192.168.0.0/24. Na **Tabela 1**, está representado o endereço IP de cada uma das ligações.

Router	Ligação 2º Router	Endereço IP	Máscara
n1	n2	192.168.0.1	/30
n2	n1	192.168.0.2	/30
n2	n3	192.168.0.5	/30
n3	n2	192.168.0.6	/30
n3	n4	192.168.0.9	/30
n4	n3	192.168.0.10	/30
n4	n5	192.168.0.13	/30
n5	n4	192.168.0.14	/30
n5	n1	192.168.0.17	/30
n1	n5	192.168.0.18	/30

Tabela 1 - **Endereçamento das redes de interligação dos *routers***

Cada rede local (A, B, C, D e E) deve agrupar os seguintes números de estações 288, 59, 59, 27 e 11, respetivamente. Para este agrupamento, devem-se usar endereços na gama 10.**G**.0.0/23 (G é o número do grupo). Na Tabela 2, segue-se o endereçamento das redes locais apresentadas.

Rede		End. rede	End. difusão	Máscara	Gama	End. router
A	A1	10.6.0.0	10.6.0.255	/24	.1 -.254	10.6.0.1
	A2	10.6.1.0	10.6.1.63	/26	.1 -.62	10.6.1.1
B		10.6.1.64	10.6.1.127	/26	.65 -.126	10.6.1.65
C		10.6.1.128	10.6.1.191	/26	.129-.190	10.6.1.129
D		10.6.1.192	10.6.1.223	/27	.193-.222	10.6.1.193
E		10.6.1.224	10.6.1.239	/28	.225-.238	10.6.1.225

Tabela 2 - **Endereçamento das redes locais**

Para o correto e total funcionamento dos *routers* foi necessário recorrer a uma tabela de encaminhamento, para que se pudesse configurar adequadamente as rotas (encaminhamento estático) para garantir a conetividade entre todas as redes disponíveis. Na **Tabela 3** está representado todas as rotas possíveis das redes locais criadas, com os respetivos encaminhamentos.

Orig.	Destino	Rede	Máscara	Interf. de saída	Próximo nó
A	A1	10.6.0.0	/24	10.6.0.1	–
	A2	10.6.1.0	/26	10.6.1.1	–
	B	10.6.1.64	/26	192.168.0.1	192.168.0.2
	C	10.6.1.128	/26	192.168.0.1	192.168.0.2
	D	10.6.1.192	/27	192.168.0.18	192.168.0.17
	E	10.6.1.224	/28	192.168.0.18	192.168.0.17

B	A1	10.6.0.0	/24	192.168.0.2	192.168.0.1
	A2	10.6.1.0	/26	192.168.0.2	192.168.0.1
	B	10.6.1.64	/26	10.6.1.65	–
	C	10.6.1.128	/26	192.168.0.5	192.168.0.6
	D	10.6.1.192	/27	192.168.0.5	192.168.0.6
	E	10.6.1.224	/28	192.168.0.2	192.168.0.1
C	A1	10.6.0.0	/24	192.168.0.6	192.168.0.5
	A2	10.6.1.0	/26	192.168.0.6	192.168.0.5
	B	10.6.1.64	/26	192.168.0.6	192.168.0.5
	C	10.6.1.128	/26	10.6.1.129	–
	D	10.6.1.192	/27	192.168.0.9	192.168.0.10
	E	10.6.1.224	/28	192.168.0.9	192.168.0.10
D	A1	10.6.0.0	/24	192.168.0.13	192.168.0.14
	A2	10.6.1.0	/26	192.168.0.13	192.168.0.14
	B	10.6.1.64	/26	192.168.0.10	192.168.0.9
	C	10.6.1.128	/26	192.168.0.10	192.168.0.9
	D	10.6.1.192	/27	10.6.1.193	–
	E	10.6.1.224	/28	192.168.0.13	192.168.0.14
E	A1	10.6.0.0	/24	192.168.0.17	192.168.0.18
	A2	10.6.1.0	/26	192.168.0.17	192.168.0.18
	B	10.6.1.64	/26	192.168.0.17	192.168.0.18
	C	10.6.1.128	/26	192.168.0.14	192.168.0.13
	D	10.6.1.192	/27	192.168.0.14	192.168.0.13
	E	10.6.1.224	/28	10.6.1.225	–

Tabela 3 - **Encaminhamento das redes locais**

Para a realização de testes de conetividade, devem ser utilizados os comandos *ping* e *traceroute.* Na **Figura 4**, podemos analisar o tráfego gerado (comando *traceroute*) entre os terminais n11 (10.6.1.66) e n14 (10.6.1.131). Na **Figura 5**, podemos ver o resultado de quando se usou o comando *ping* nas estações ditas atrás. Em ambos os casos, os testes foram realizados entre a rede B (localização do terminal n11) e a rede C (localização do terminal n14).

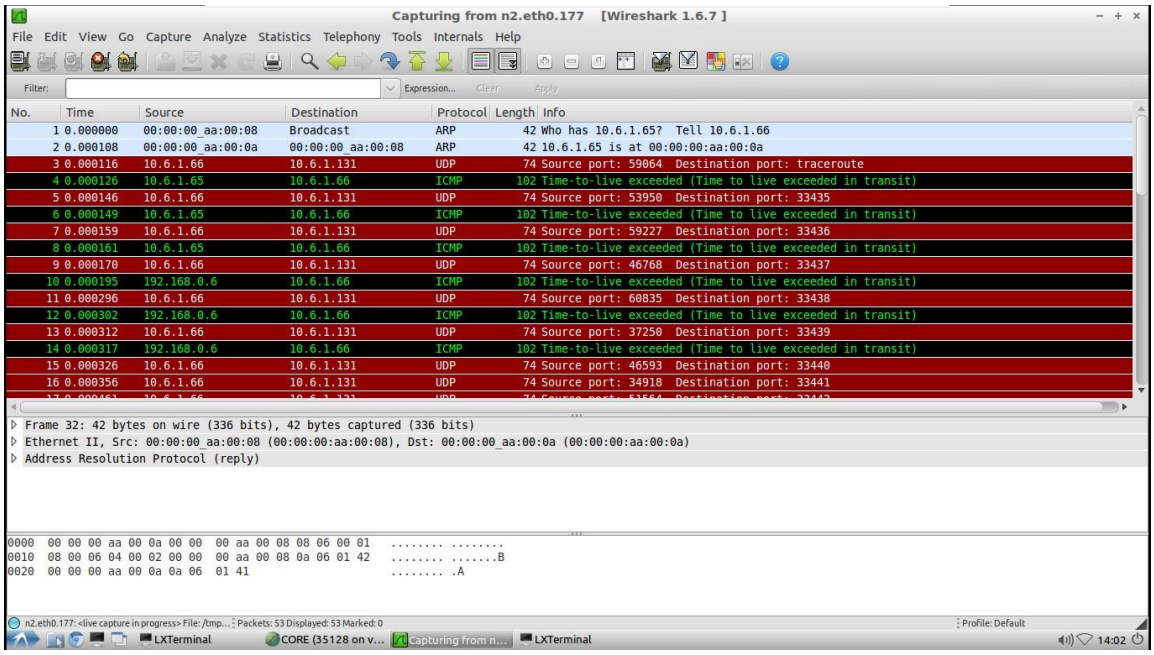

Figura 4 - **Captura de tráfego utilizando o comando *traceroute***

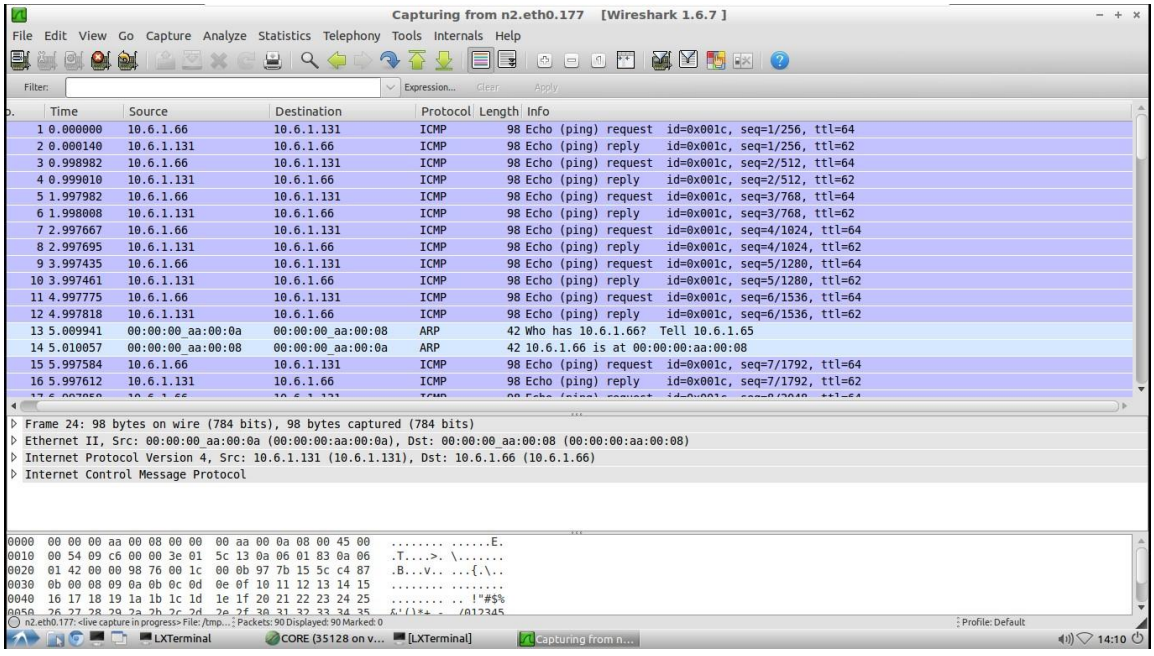

Figura 5 - **Captura de tráfego utilizando o comando *ping***

4 Fase 4 – DHCP (Dynamic Host Configuration Protocol)

Nesta fase, o objetivo é ativar a configuração automática dos endereços IP numa rede local recorrendo ao protocolo DHCP. Para isso, usou-se a rede local B para implementar o protocolo anterior.

A topologia da rede local B foi alterada de modo a ter um servidor de DHCP (para atribuição de endereços IP) e dois terminais que, inicialmente, não tem a si atribuído um IP, como mostra a **Figura 6**.

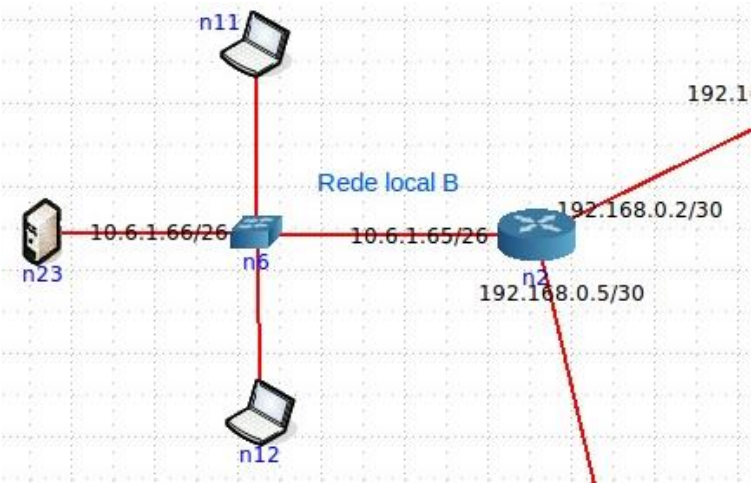

Figura 6 - **Rede local B com servidor DHCP (n23)**

Utilizou-se a captura de tráfego para a obtenção da sequência de interações entre um cliente, neste caso o terminal n11, e um servidor DHCP, como ilustra a **Figura 7.**

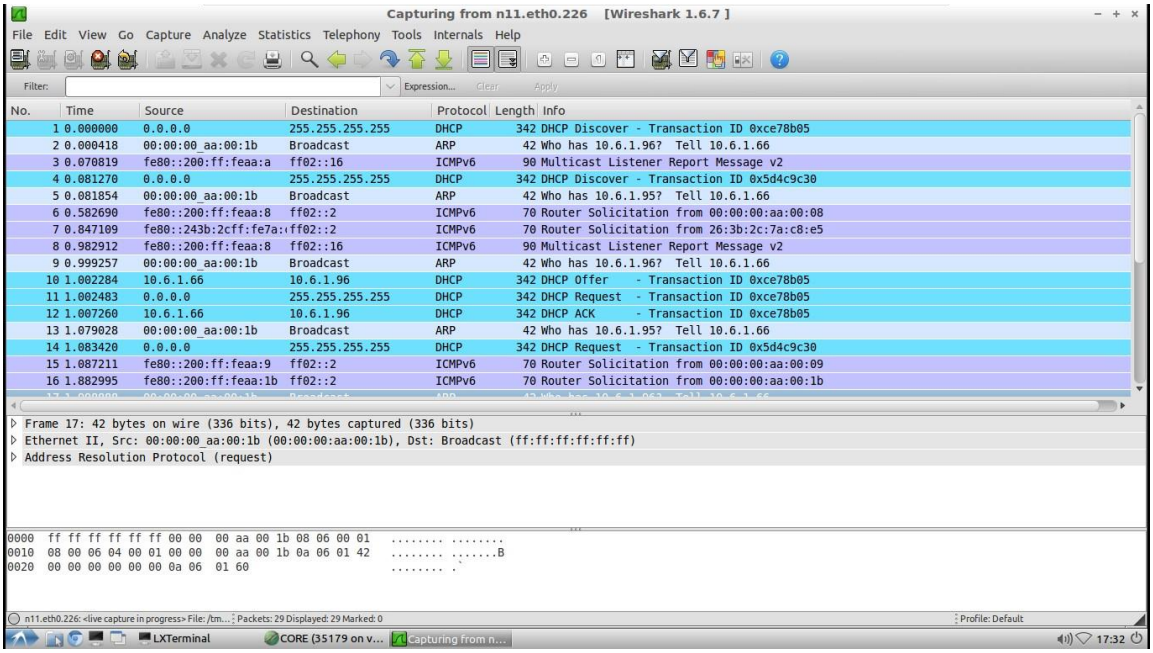

Figura 7 - **Captura de tráfego com servidor DHCP**

Como podemos reparar, o protoloco DHCP está dividido em quatro fases, DHCP *Discover*, DHCP *Offer*, DHCP *Request* e por último DHCP ACK.

Na primeira fase (DHCP *Discover*), o cliente envia uma mensagem/pedido em *broadcast* (para toda a rede).

Na segunda fase (DHCP *Offer*), o servidor DHCP envia em *unicast* (só para o cliente) uma oferta de um endereço IP que, neste caso, corresponde ao endereço 10.6.1.96.

Na terceira fase (DHCP *Request*), o cliente comunica, ainda em *broadcast,* ao servidor que aceita a oferta do endereço IP que este lhe concedeu .

Por fim (DHCP ACK), o servidor confirma ao cliente que o endereço IP lhe foi atribuído.

5 Fase 5 - Uso das camadas de rede e transporte por parte das aplicações

Nesta fase, o objetivo é colocar uma rede local a suportar serviços e executar aplicações de rede, como por exemplo, um servidor HTTP (*Hypertext Transfer Protocol*). Para isso, é necessário a ativação do servidor HTTP num dos PCs da rede local e configuração do mesmo no CORE.

Como pedido, foi ativado, num dos PCs da rede local C, o servidor HTTP, como mostra a **Figura 8**.

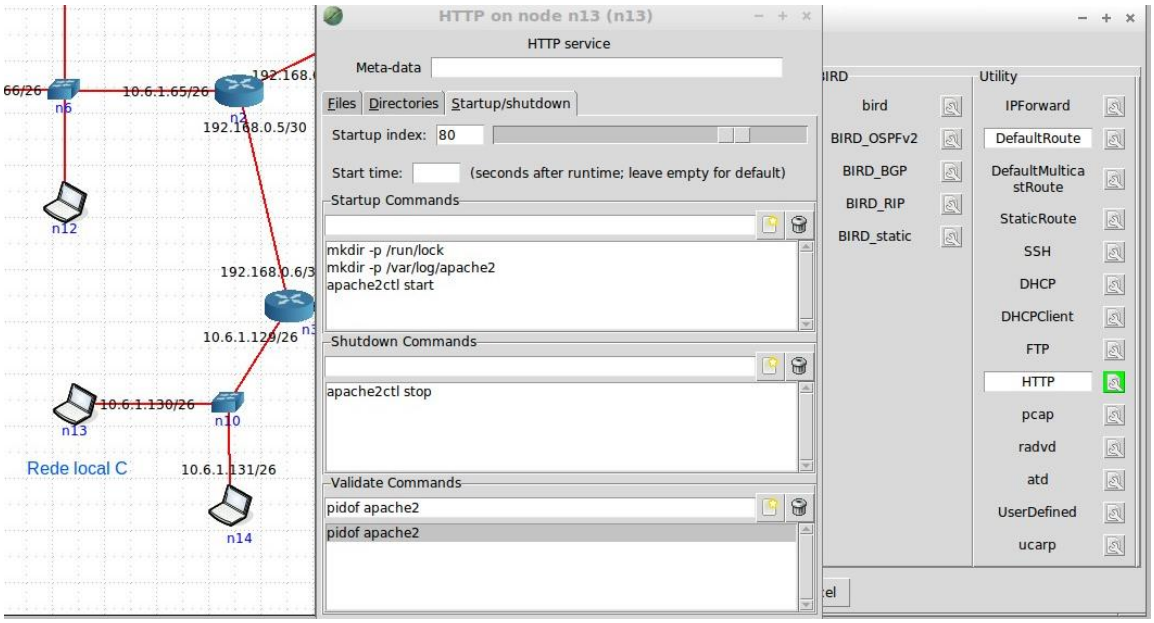

Figura 8 - **Ativação e configuração do servidor HTTP no PC n13**

Após feita a ligação entre o cliente (terminal n15), presente na rede local C, e o servidor HTTP, através do comando `wget -S [URL]`, em que o URL é o endereço IP do terminal que está a correr o servidor, obtivemos a seguinte captura de tráfego, **Figura 9**.

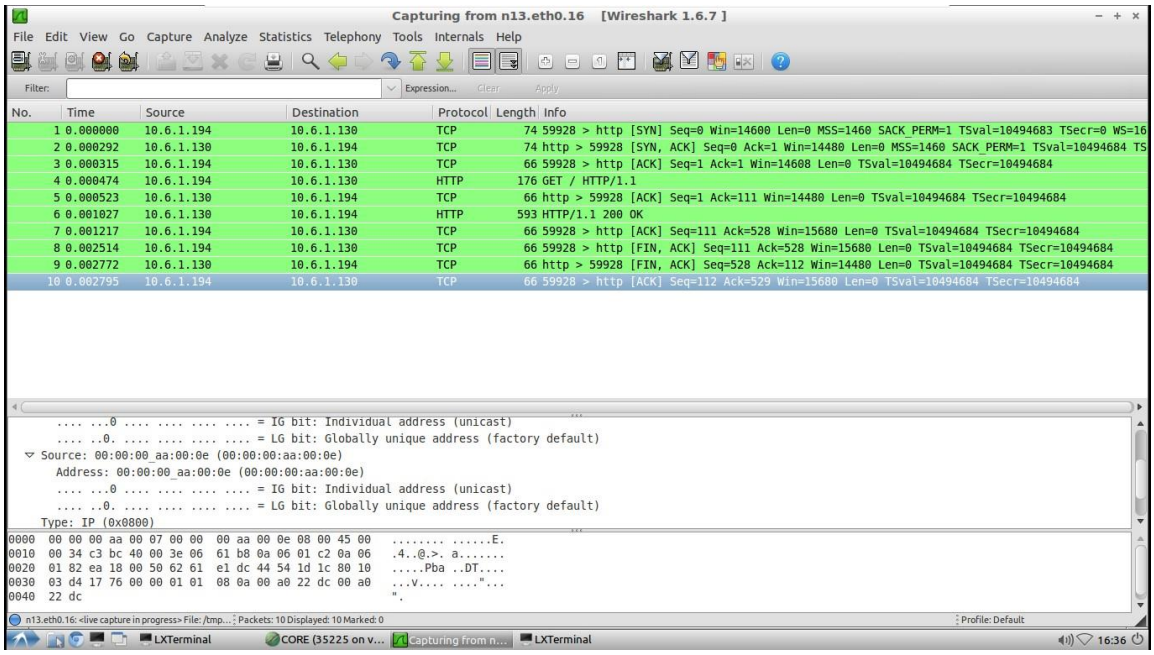

Figura 9 - **Captura de tráfego no servidor HTTP**

A partir da figura acima, reparamos que existem pacotes que ilustram o estabelecimento de uma conexão TCP (*Transmission Control Protocol*), correspondentes aos três primeiros pacotes, assinalados como [SYN] e [SYN, ACK]. Temos também os três últimos que correspondem ao fim da ligação ([FIN,ACK]).

Quando à ligação HTTP, podemos ver que o cliente envia um pedido ao servidor, o qual correspondente ao pacote nº4, com a seguinte informação `GET / HTTP/1.1`. O servidor responde ao cliente (pacote nº 6) enviando-lhe como mensagem `HTTP/1.1 200 OK`.

6 Interligação via NAT (Network Address Translator)

Nesta fase, é pedido que se acrescente uma rede privada à topologia já existente, usando endereços privados da gama 192.168.1.0/24. Esta rede terá de ser ligada a uma rede local, através de um *router* NAT. Para a configuração deste deverá ser usado o programa *iptables*, que já vem instalado na máquina virtual do CORE.

Decidimos adicionar esta rede privada à rede local C já presente na topologia anteriormente criada. Para o funcionamento correto destas, foi dado, à interface de ligação entre o router NAT (rede privada) e o router n10 (rede local C), o endereço IP 10.6.1.132 Quanto à rede privada foi definido como endereço do router NAT, o IP 192.168.1.1, deixando assim, o resto dos endereços possíveis (192.168.1.2 ao 192.168.1.254) para os servidores HTTP, FTP e PCs. A **Figura 10** representa a rede privada associada à rede local C.

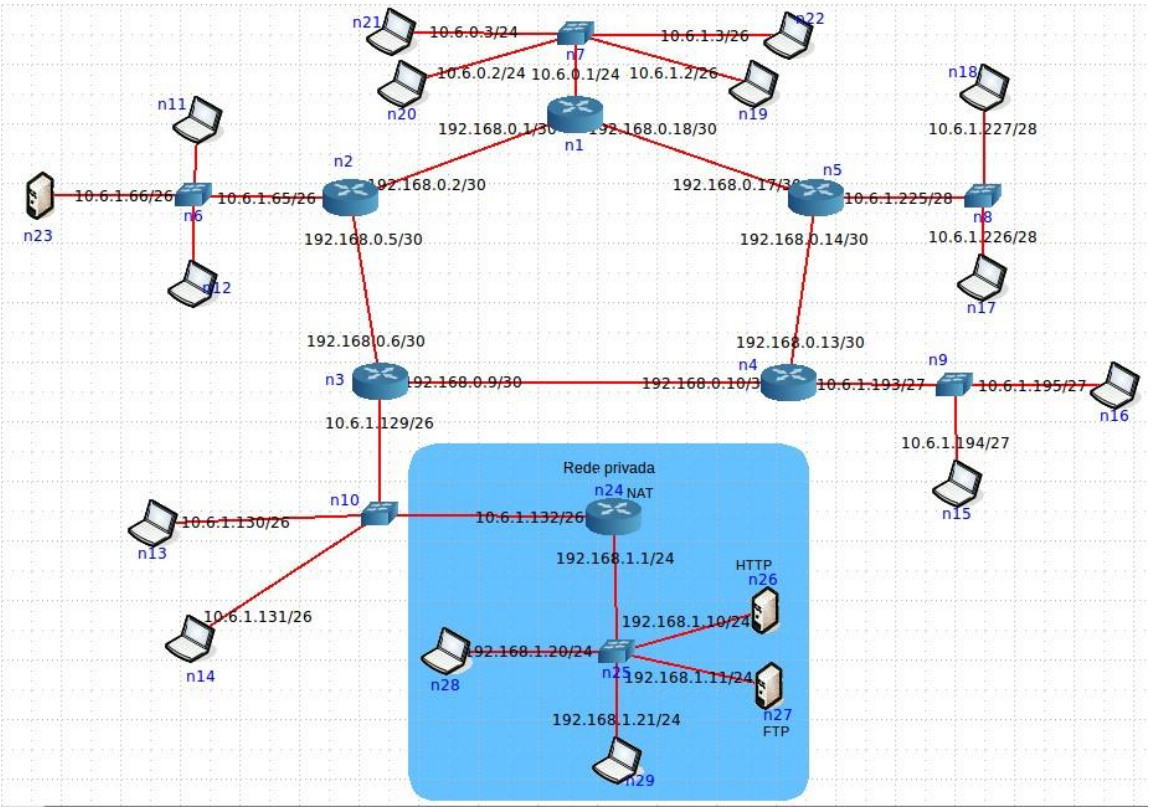

Figura 10 - **Rede privada associada à rede local existente**

Realizaram-se testes de conetividade entre a rede privada e a rede externa, neste caso, utilizou-se a rede local D, para ver o funcionamento do serviço NAT. Nas **Figura 11** e Figura 12, estão representadas as capturas de tráfego nos terminais n28 (rede privada) e n15 (rede local D), respetivamente.

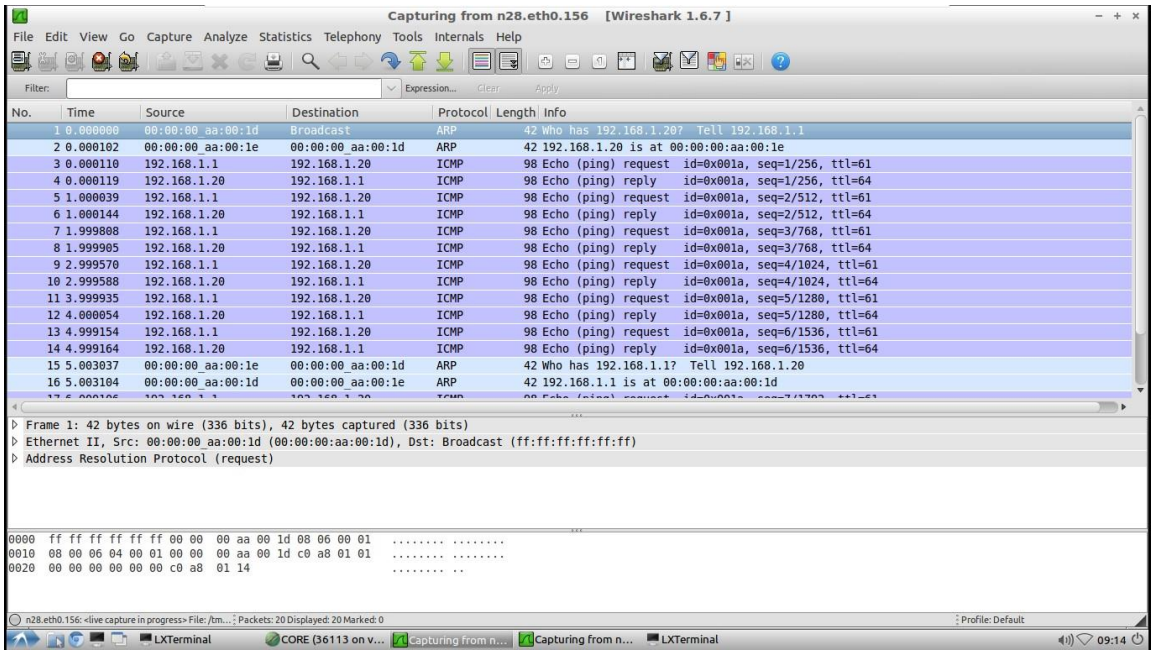

Figura 11 - **Captura de tráfego na rede privada**

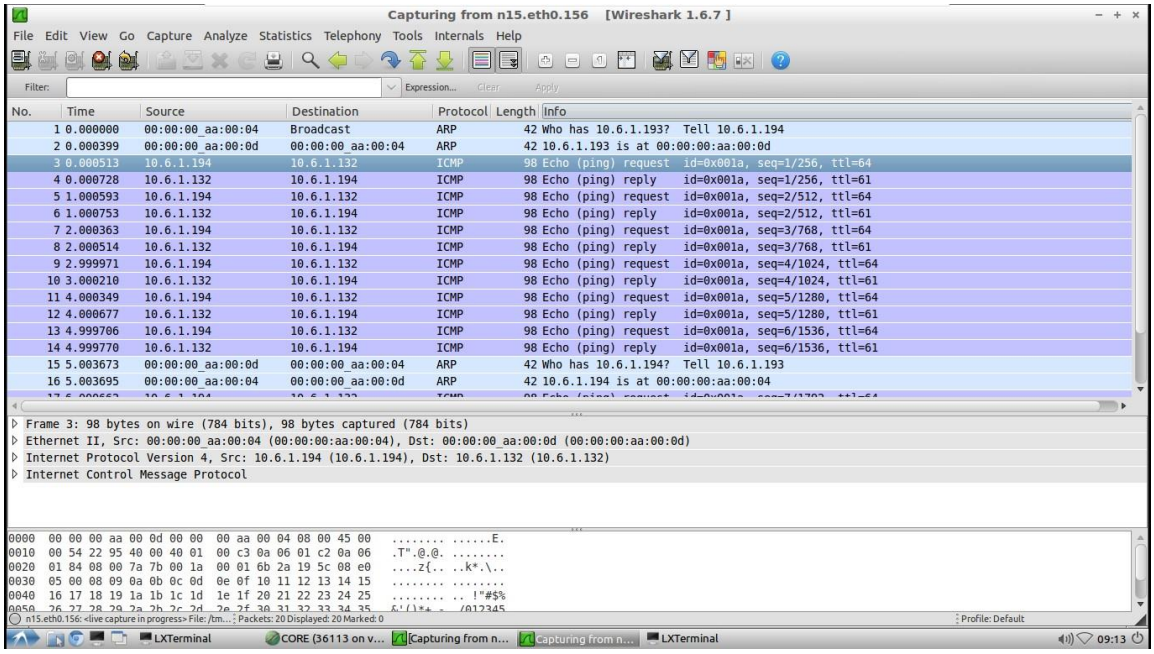

Figura 12 - **Captura de tráfego na rede local**

Efetuaram-se testes com o servidor HTTP presente na rede privada, para se poder ver se o mesmo era acedido por um terminal na rede externa. Na Figura 13, obtemos a captura de tráfego no terminal n26 (servidor HTTP) e o comando necessário para se efetuar a ligação HTTP, a partir do PC n15.

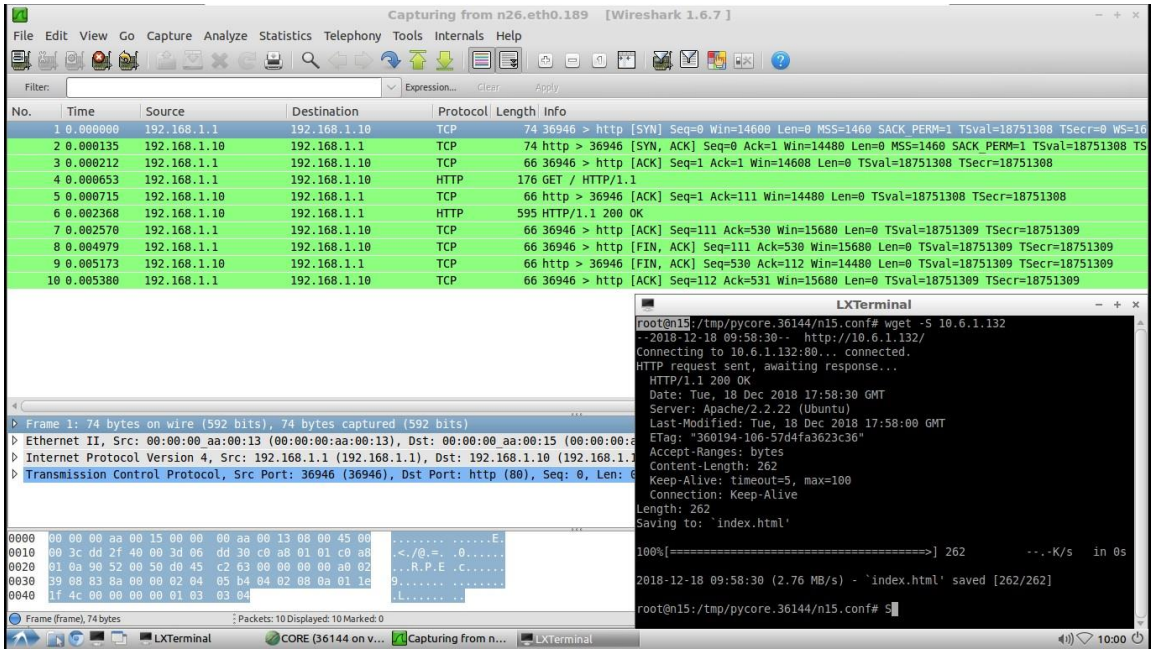

Figura 13 - **Captura de tráfego no servidor HTTP da rede privada**

7 Conclusão

Este projeto ajudou-nos a compreender melhor a matéria e os conhecimentos adquiridos na UC de Redes e Computadores I, pois foi possível observar com melhor detalhe a comunicação entre várias redes locais, bem como o funcionamento de vários protocolos, tais como, o protocolo ARP.

Por outro lado, com a realização deste trabalho ficamos a conhecer melhor o *sofware* CORE, porque foi com este que nos permitiu criar as várias redes e a ferramenta *wireshark*, pois este permitiu que nós pudéssemos ver os protocolos usados em cada fase.

Porém, houve algumas dificuldades na realização deste projeto, uma vez que estávamos a usar uma ferramenta nova, o CORE, e pouco sabíamos sobre ele, o mesmo aconteceu, no que diz respeito à configuração dos routers, por exemplo, no router NAT.

No final, todas os obstáculos foram ultrapassados com sucesso e pensamos que as fases propostas no enunciado foram concluídas com êxito.