Mestrado Integrado em Engenharia de Telecomunicações e Informática

**UC de Redes de Computadores I**

Ano Letivo 2021/2022



**UNIVERSIDADE DO MINHO**

ESCOLA DE ENGENHARIA

Eva Castro, a93097

Filipe Peixoto, a93096

José Gomes, a

Índice

[1. Introdução 3](#_Toc90848056)

[*2.* Emulação de LANs (*Local Area Networks*) *Ethernet* 4](#_Toc90848057)

[Figura 1 - Topologia em árvore 4](#_Toc90848085)

[Figura 2 - Wireshark n5 5](#_Toc90848086)

[Figura 3 - Wireshark n5 (segunda vez) 5](#_Toc90848087)

[Figura 4 - Wireshark n1 6](#_Toc90848088)

# Introdução

No âmbito da unidade curricular de Redes de Computadores I, foi-nos proposta a realização de um trabalho prático cujo objetivo é emular vários tipos de redes locais e interligá-las entre si, utilizando a ferramenta CORE. Esta ferramenta disponibiliza meios para podermos desenhar as diferentes tipologias de rede, configurar as ligações entre os componentes da rede, endereços e serviços.

Utilizaremos ainda, a ferramenta *Wireshark* para efetuarmos diagnósticos de conetividade e capturas de tráfego, para melhor entendimento do funcionamento dos componentes de cada rede e também comparar o modo de funcionamento das redes. Utilizaremos comandos como *ping* e *traceroute* para podermos executar os testes experimentais.

# Emulação de LANs (*Local Area Networks*) *Ethernet*

Neste primeiro exercício, desenhamos uma rede com tipologia em árvore, que possui 2 HUBs e 1 SWITCH, como se pode observar na figura 1. O objetivo é efetuar capturas de tráfego utilizando o *Wireshark*, de forma a melhor compreender o funcionamento, na prática, dos HUBs e SWITCHs e também dos protocolos ARP e ICMP.



Figura - Topologia em árvore

Deste modo, antes de resolvermos o exercício tivemos de entender o funcionamento destas tecnologias.

O HUB quando recebe informação por uma porta, ele transmite essa informação para todas as outras portas, este comportamento diminuiu a performance, pois qualquer outro sistema terminal, ao qual a informação não lhe é dirigida, pode ter acesso à mesma. Este tipo de equipamento não possui tecnologia que lhe permita armazenar informação sobre os sistemas terminais que se encontram conectados a ele.

O SWITCH possui um comportamento semelhante ao do HUB, no entanto possui tecnologia que lhe permite armazenar os endereços MAC (*Medium Access Control*) dos sistemas terminais a ele conectados (algo que ele vai “aprendendo” com o decorrer das ligações, na primeira ligação possui um comportamento igual ao do HUB). Esta funcionalidade dos SWITCHs permite-lhes comutar pacotes diretamente para a porta de destino.

O protocolo ARP (*Address Resolution Protocol*) faz a ponte de ligação entre a cama de rede e a camada de ligação de dados, portanto mapeia endereços IP (*Internet Protocol*) em endereços MAC. São enviados dois tipos de mensagens: ARP *request*, onde o dispositivo de origem pede a resolução de um endereço IP em endereço MAC e ARP *reply*, onde o dispositivo de destino envia o endereço físico resolvido. Para reduzir o fluxo e o número de solicitações de resolução de endereços, recorre-se ao uso de uma tabela, cache ARP, em cada *host* cuja funcionalidade é guardar os mapeamentos dos endereços por algum tempo.

O protocolo ICMP (*Internet Control Message Protocol*) é utilizado para enviar mensagens de diagnóstico e relatório de erros sobre a rede para a fonte de destino, as mensagens podem ser *echo reply*, *echo request*, TTL (*Time To Live*) *expired*, etc. Qualquer dispositivo de rede IP pode enviar, gerar, receber e processar mensagens de erro ICMP. Este protocolo é utilizado por alguns diagnósticos de utilidade como o *ping* e o *traceroute*.

Agora estamos em condições de avaliar a conetividade entre os sistemas. Para tal, executamos, no PC n8, o comando *arp -a* para verificar as tabelas ARP dos sistemas terminais, de seguida executamos o comando *ping 10.0.0.25* e, num primeiro momento colocamos o sistema n5 à escuta e obtivemos os resultados que se encontram na figura 2. As capturas de tráfego foram efetuadas no *Wireshark*.

Uma imagem com mesa

Descrição gerada automaticamente

Figura - Wireshark n5

Como podemos observar, antes de serem comutados pacotes entre os dois sistemas terminais, é enviado, em *broadcast*, um ARP *request* a perguntar qual o sistema terminal que possui o endereço IP 10.0.0.25, pois é a tentativa do protocolo ARP mapear o endereço IP no endereço MAC e vemos que depois é enviada um ARP *reply* com o endereço mapeado. Este sistema (n5) consegue captar todos os pacotes comutados entre o sistema n8 e n7 pois está ligado ao mesmo HUB que o sistema n7 (destino).

Voltamos a executar o comando *ping 10.0.0.25* no PC n8 e colocamos o PC n5 à escuta e o resultado obtido encontra-se na figura 3.

Uma imagem com mesa

Descrição gerada automaticamente

Figura - Wireshark n5 (segunda vez)

Notamos que quando ocorre a primeira comutação de pacotes não é enviado um ARP *request*, isto porque o mapeamento dos endereços já se encontra em cache na ARP *table*.

De seguida, colocamos o PC n1 à escuta e podemos observar os resultados na figura 4.

Uma imagem com mesa

Descrição gerada automaticamente

Figura - Wireshark n1

Como podemos ver, o sistema n1 apenas recebeu o ARP *request* e não voltou a receber mais nenhum pacote, isto porque o SWITCHarmazenou as informações deste sistema e percebeu que os pacotes não se dirigiam a ele.

Assim, concluímos que o HUB comuta os pacotes para todos os sistemas a ele conectados, enquanto o SWITCH apenas faz isso a primeira vez, depois comuta os pacotes diretamente para a porta de saída correspondente e que o protocolo ARP mapeia os endereços IP em endereços MAC.