Universidade do Minho
Licenciatura em Ciências da Computação
Sistemas de Comunicações e Redes

TP2: Aplicações e Camada de Transporte (2 aulas)

1. Objetivo

Este trabalho tem como objetivo a familiarização com protocolos e ferramentas do nível aplicacional, e análise dos protocolos de transporte em uso. Para tal, deve usar a sua máquina nativa (preferencialmente com o sistema operativo Linux), e não a máquina virtual.

2. Nível aplicacional

Tomando como base o trabalho realizado no TP1, e assumindo que está ligado à rede Eduroam:

1. Ative um browser na sua máquina nativa e certifique-se que não tem outras instâncias web ativas.
   Ative o Wireshark, certificando-se que está em modo privilegiado (root), e proceda à captura de tráfego na interface de rede em uso.
   Aceda à página *http://www.scom.uminho.pt* e espere que o conteúdo seja carregado. Pare a captura (e grave-a para eventual uso posterior).
   Para localizar mais facilmente o tráfego correspondente ao acesso web realizado, comece por filtrar pelo protocolo *dns*. Para tal, introduza *dns* na caixa do *display filter* e aplique o filtro. Localize a resolução do nome *www.scom.uminho.pt*. Identifique o endereço IP da estação que formulou a *query* e o tipo de *query* realizada.
   Nota: Caso não consiga encontrar a referida *query*, limpe a cache DNS da sua máquina, executando num terminal do Ubuntu: sudo systemd-resolve --flush-caches; ou sudo /etc/init.d/dns-clean restart. No Windows deve executar: ipconfig /flushdns.
2. Identifique a trama com resposta à *query* formulada. Identifique também o servidor de nomes que deu a resposta, através do seu IP e nome (consulte o Additional Records).
3. Limpe o filtro anteriormente estabelecido e filtre agora pelos protocolos *http || tcp*.
4. Tente identificar as tramas correspondentes ao estabelecimento da ligação entre o cliente e o servidor HTTP.
5. Com base na sequência de dados trocados entre cliente e servidor explique se o servidor HTTP está a funcionar em modo de conexão persistente ou não persistente.
6. Limpe o filtro anteriormente estabelecido e filtre agora pelo protocolo *http*.
7. O *hard refresh* permite limpar a cache do browser para uma determinada página, forçando o browser a carregar a última versão da página existente no servidor. Normalmente o *hard refresh* duma página faz-se com CTRL+F5 (caso não funcione, procure na Internet a forma de fazer *hard refresh* no seu browser). Coloque o `wireshark` a capturar tráfego e faça *hard refresh* da página indicada anteriormente. Depois volte a aceder à mesma página mas sem fazer *hard refresh*. Pare a captura de tráfego. Identifique a principal diferença observada no tráfego HTTP entre carregar a referida página com e sem *hard refresh*. Quais os campos do cabeçalho HTTP envolvidos nesta ação? Qual a principal vantagem e desvantagem inerente ao *hard refresh*?
8. Aceda a https://alunos.uminho.pt, ao mesmo tempo que captura o tráfego desse acesso com o wireshark. Porque razão o tráfego HTTP não é identificado como tal? (Apesar disso, pode detetar-se qual o protocolo aplicacional.)

3. Consultas ao serviço de resolução de nomes DNS

A maioria dos sistemas operativos (Windows, Linux, etc) inclui um cliente DNS genérico designado por "`nslookup`". No entanto este cliente tem vindo a ser preterido a favor de outros como o "`dig`" e o "`host`". O package "dnsutils" inclui todos. Se no Linux não conseguir usar nenhum deles tente reinstalar o package com o comando: `$ sudo apt-get install dnsutils`

Usando o nslookup ou o dig e com base nos seus manuais (`man nslookup` ou `man dig`) procure responder às seguintes questões, devendo incluir os resultados que sustentam as suas respostas:

1. Se estiver a usar o Linux, observe o conteúdo do ficheiro */etc/resolv.conf.* Se estiver a usar o Windows, abra uma janela de comandos e execute *nslookup*. Para que serve a informação apresentada?

2. A base de dados dum servidor DNS é constituida por registos de diversos tipos, como por exemplo: A, AAAA, NS, SOA, MX, PTR. Usando os registo do tipo A, identifique os endereços IPv4 dos servidores `www.uminho.pt` e `www.ebay.com`?

3. Usando os registo NS, identifique os servidores de nomes definidos para os domínios: "`ebay.com.`", "`utad.pt.`" e "`.`"?

4. Usando o registo SOA, identifique o servidor DNS primário definido para o domínio `uminho.pt.`? Em que difere o servidor primário de um servidor secundário e qual o significado dos parâmetros temporais associados ao servidor primário?

5. Usando os registos MX, diga qual(quais) o(s) servidor(s) de mail do domínio de mail `alunos.uminho.pt`? A que sistema são entregues preferencialmente as mensagens dirigidas a `user@di.uminho.pt`?

6. Consegue interrogar o DNS sobre o endereço IPv6 `2001:690:a00:1036:1113::247`? E sobre o endereço IPv4 `193.136.9.254`? A que sistemas correspondem? Experimente fazer uma *query* aos registos PTR para o nome `254.9.136.193.in-addr.arpa.` e comente o resultado obtido.

7. Qual a diferença entre uma resposta adjetivada como *non-authoritative answer* ("não-autoritativa") e uma resposta "autoritativa" para uma determinada *query*?

4. Uso da camada de transporte por parte das aplicações

Verifique se na sua máquina de trabalho tem disponíveis as seguintes aplicações / ferramentas: clientes ftp, ssh, traceroute (tracert em Windows) e ping, senão instale. Corra novamente o `wireshark`. Capturando o tráfego nos momentos que considere adequados, observe atentamente como as várias aplicações utilizam o serviço de transporte, quando é efetuado:

a. Acesso via browser ao URL: http://marco.uminho.pt/CCG/
b. Acesso em *ftp* para ftp.di.uminho.pt (login: *anonymous*)
c. *ping* marco.uminho.pt
d. Acesso *ssh* para marco.uminho.pt
e. *nslookup* www.uminho.pt
f. *traceroute* cisco.di.uminho.pt

1. Preencha a seguinte tabela com base nos resultados que obteve:

Comando usado (aplicação)	Protocolo de transporte (se aplicável)	Porta de atendimento (se aplicável)
`ping`		
`traceroute`		
`ftp`		
`Browser http`		
`nslookup / dig`		
`ssh`		

Inclua todos os extratos dos *outputs* que lhe permitem chegar às conclusões acima.

2. Comente as principais diferenças entre os protocolos TCP e UDP. Relacione-as com as experiências realizadas onde observou os campos dos cabeçalhos respetivos e o *overhead* protocolar. Em particular, identifique os campos do TCP responsáveis pelo controlo de fluxo, ordenação e fiabilidade do protocolo.

Relatório do trabalho

O relatório final do TP2 apenas deve incluir apenas:
- título e identificação do grupo;
- uma secção "Questões e Respostas" relativas ao enunciado acima (formato: transcrição da questão, resposta, ...);
- uma secção de "Conclusões" que autoavalie (de forma completa) os resultados da aprendizagem decorrentes das várias vertentes estudadas no trabalho.

O relatório deve seguir preferencialmente o formato LNCS (Springer, existem *templates* .tex e .docx) e ser submetido obrigatoriamente na plataforma de ensino com o nome SCR-TP2-PLxx.pdf (por exemplo, SCR-TP2-PL11.pdf para o grupo PL11) até final do dia previsto para a conclusão do trabalho.