

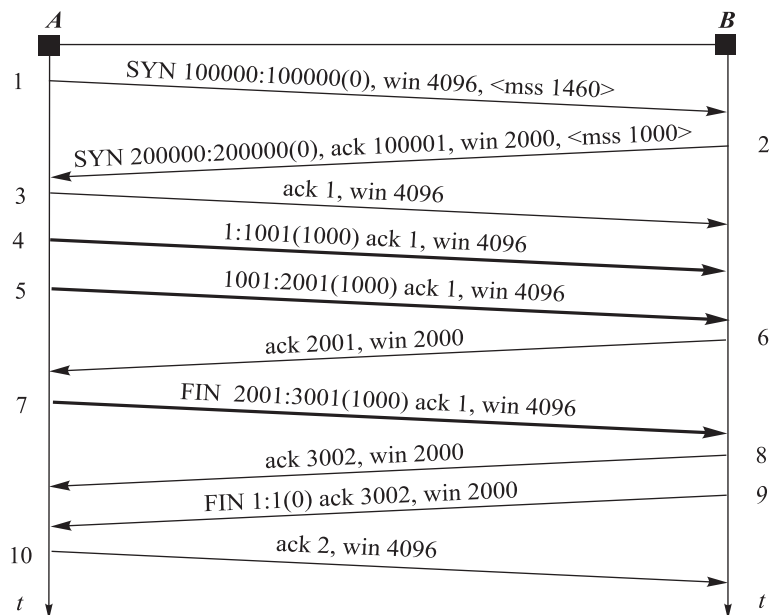
Utilize um caderno separado para responder a cada um dos grupos de questões I e II

I

1.
  - a) Qual a função do protocolo ARP?
  - b) Uma estação com endereço IP 193.12.100.5/24 terá necessidade de invocar o serviço do protocolo ARP para enviar um datagrama para o endereço IP 194.10.115.3/24? Justifique
  - c) Qual a função do protocolo ICMP?
  - d) O programa *traceroute* utiliza o ICMP para determinar o trajecto de datagramas IP ao longo dum internet, desde um interface de origem até a um interface de destino. Explique como é que tal se processa.
2. Pretende-se utilizar o TCP para o transporte fim-a-fim numa ligação de satélite geoestacionário (altitude aproximada de 36000 Km) a um ritmo binário de 1 Mbps. Considere que a velocidade de propagação na ligação é de  $3 \times 10^8$  m/s.
  - a) Qual o valor mínimo da abertura da janela de controlo de fluxo a utilizar de modo a maximizar a utilização da ligação sabendo que nestas condições se deverá ter  $W > 1 + 2a$  com  $a = \frac{t_p}{t_t}$ .
  - b) Considerando que o cabeçalho TCP possui 32 bits para numeração e 16 bits para abertura de janela, indique se o valor obtido na alínea a) é praticável e sugira o método de control de erros que lhe pareça mais rentável. Justifique as suas respostas.
3. Suponha que um analisador de protocolos (*sniffer*) instalado numa determinada LAN capturou as tramas MAC ethernet (*frame 3 e frame 4*) que se listam nas páginas 3 e 4.
  - a) Quais os protocolos que se encontram sucessivamente encapsulados nestas tramas e como os identificou?
  - b) Qual o protocolo da camada de aplicação e que operações foram efectuadas?
  - c) As tramas resultam de uma interacção cliente/servidor. Identifique as estações servidor e cliente bem como a *porta* de atendimento da aplicação no servidor.
  - d) Nesta interacção está a ser utilizada uma conexão de transporte? Justifique.

## II

4. O diagrama representado mostra a troca de segmentos TCP ocorrida ao longo de um certo intervalo de tempo entre as estações **pc1** e **pc2**.



- Interprete numa forma sucinta a sequência apresentada, destacando devidamente as diferentes fases existentes na ligação.
  - Observa-se que a estação **pc1** enviou os segmentos n<sup>os</sup> 4 e 5 contendo 1000 bytes cada. Seria possível enviá-los num só segmento com 2000 bytes? Justifique.
  - Seria possível a estação **pc1** enviar o segmento n<sup>o</sup> 7 logo a seguir ao n<sup>o</sup> 5 sem esperar pela recepção do segmento n<sup>o</sup> 6? Justifique.
  - Porque razão o segmento n<sup>o</sup> 8 confirmou 1001 bytes apesar da estação **pc1** só ter enviado 1000 bytes no segmento n<sup>o</sup> 7?
  - O protocolo TCP pode fazer confirmação em *piggyback*.
    - Em que consiste esta técnica e qual o interesse da sua utilização.
    - No diagrama apresentado diga, justificando, em que segmentos foi utilizada esta técnica.
5. Uma organização pretende instalar um internet local com 4 subredes, dispondo para isso apenas do endereço de rede IPv4 192.168.10.0/24.
- Apresente a máscara de subrede a usar que permita maximizar o número de estações endereçáveis em cada uma das subredes. Tendo em conta os endereços reservados, qual o número máximo de estações em cada subrede?
  - Suponha que existem apenas duas estações em cada subrede. Apresente um possível esquema de interligações válido para este internet, indicando os endereços das subredes e das várias interfaces dos equipamentos utilizados.
  - O internet local tem uma ligação externa ao interface 193.1.1.254. Apresente a tabela de encaminhamento do router local que faz a ligação externa. (**Nota:** as entradas da tabela deverão ser da forma <Destino | Próximo salto | Máscara | Interface> e os interfaces devidamente identificados.)
  - Escolha uma estação no internet local e apresente a sua tabela de encaminhamento por forma a que consiga aceder a qualquer estação local mas não às redes exteriores. (**Nota:** a estrutura da tabela deve ser idêntica à da alínea anterior.)

```

Frame 3
  Arrival time: Apr 14, 2003 16:07:55.7334
  Packet length: 146 bytes
Ethernet II
  Destination: 00:00:f8:1e:7c:a3 (kepler.labcom.uminho.pt)
  Source: 00:50:fc:5c:e9:ae (pc8.labcom.uminho.pt)
  Type: IP (0x0800)
Protocol-A
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field (TOS): 0x00
  Total length: 132
  Identification: 0x0000
  Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: UDP (0x11)
  Header checksum: 0x04ac (correct)
  Source: pc8.labcom.uminho.pt (192.168.90.18)
  Destination address: kepler.labcom.uminho.pt (192.168.90.90)
Protocol-B
  Source port: 800 (800)
  Destination port: nfs (2049)
  Length = 112
  Checksum = 0x3260 (correct)
Protocol-C
  Transaction ID: 0x71434413 (1900233747)
  Message type: Call (0)
  RPC version: 2
  Program: NFS (100003)
  Program version: 3
  Procedure: LOOKUP (3)
  Credentials
    Flavor: AUTH_UNIX (1)
    Length: 28
    Stamp: 0x00099c62
    Machine name: pc8
    UID: 807
    GID: 506
  Verifier Flavor: AUTH_NULL (0)
Protocol-D
  Program version: 3
  Procedure: LOOKUP (3)
  what
    dir
      length: 20
      type: unknown
      data: 0100000100080011020000000180000072AF1000
      Name: grupo@08

```

```

Frame 4
  Arrival time: Apr 14, 2003 16:07:55.7335
  Packet length: 270 bytes
Ethernet II
  Destination: 00:50:fc:5c:e9:ae (pc8.labcom.uminho.pt)
  Source: 00:00:f8:1e:7c:a3 (kepler.labcom.uminho.pt)
  Type: IP (0x0800)
Protocol-A
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field (TOS): 0x00
  Total length: 256
  Identification: 0x0000
  Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: UDP (0x11)
  Header checksum: 0x0430 (correct)
  Source: kepler.labcom.uminho.pt (192.168.90.90)
  Destination address: pc8.labcom.uminho.pt (192.168.90.18)
Protocol-B
  Source port: nfs (2049)
  Destination port: 800 (800)
  Length = 236
  Checksum = 0xe8f4 (correct)
Protocol-C
  Transaction ID: 0x71434413 (1900233747)
  Message type: Reply (1)
  Program: NFS (100003)
  Program version: 3
  Procedure: LOOKUP (3)
  Reply state: accepted (0)
  Verifier Flavor: AUTH_NULL (0)
  Accept state: RPC executed successfully (0)
Protocol-D
  Program version: 3
  Procedure: LOOKUP (3)
  Status: OK (0)
  object
    length: 20
    type: unknown
    data: 01000001000800110200000001C00300021B1C00
  obj_attributes
    attributes_follow: value follows (1)
    Type: Directory (2)
    mode: 040700
      0... .. = not SUID
      .0.. .. = not SGID
      ..0. .... = not save swapped text
      ...1 .... = Read permission for owner
      .... 1... = Write permission for owner
      .... .1.. = Execute permission for owner
      .... ..0. .... = no Read permission for group
      .... ...0 .... = no Write permission for group
      .... .... 0... = no Execute permission for group
      .... .... .0.. = no Read permission for others
      .... .... ..0. = no Write permission for others
      .... .... ...0 = no Execute permission for others
[rest of Protocol-D data]

```