EXERCÌCIO 1
Considere as seguintes afirmações, com uma elevada probabilidade de estarem incompletas ou mesmo incorrectas. Corrija, complete e, se necessário (para
mostrar que sabe do que fala), justifique cada afirmação, consoante o caso.

(a) Um protocolo Go-Back-N com janela de tamanho 4 é sempre mais eficiente se a janela do receptor for ...
Um protocolo Go-Back-N com janela de tamanho 4 é sempre mais eficiente se a janela do receptor for pelo menos igual ao tamanho da janela do remetente,
permitindo que todos os pacotes dentro da janela de transmissão possam ser enviados antes de esperar por ACKs.

(b) O protocolo DHCP é especialmente útil em redes onde ...
O protocolo DHCP é especialmente útil em redes onde os dispositivos se conectam e desconectam frequentemente, permitindo a atribuição dinâmica de
endereços IP e simplificando a gestão de endereços de rede.

(c) O encaminhamento por inundação com aprendizagem pelo caminho inverso é útil em redes de grandes dimensões (por exemplo, na Internet), desde que
estas não contenham ciclos.
O encaminhamento por inundação com aprendizagem pelo caminho inverso é útil apenas em redes pequenas e sem ciclos, pois em redes de grandes dimensões
pode causar tráfego redundante e congestionamento. Redes grandes utilizam protocolos de roteamento mais eficientes.

(d) Uma entrada na tabela ARP tem um TTL na ordem dos segundos (60 a 120) enquanto que uma entrada na tabela DHCP tem TTL na ordem das horas (12 a 24).
Isto deve-se a ...
Uma entrada na tabela ARP tem um TTL na ordem dos segundos (60 a 120), enquanto que uma entrada na tabela DHCP tem TTL na ordem das horas (12 a 24).
Isto deve-se a diferenças nos requisitos de atualização e estabilidade. As entradas ARP são frequentemente atualizadas devido à mobilidade dos dispositivos, enquanto as entradas DHCP são mais estáveis, pois os endereços IP são alocados por períodos mais longos.

(e) A rede 192.168.1.128/25 pode ter 2^25 hosts diferentes, sendo o primeiro ...
A rede 192.168.1.128/25 pode ter 126 hosts diferentes, sendo o primeiro endereço IP válido 192.168.1.129 e o último 192.168.1.254. Os endereços 192.168.1.0 (rede) e 192.168.1.255 (broadcast) não são utilizáveis para hosts.

(f) O NAT (Network Address Translation) permite que computadores com endereços IP privados passem a ter endereços IP públicos.
O NAT (Network Address Translation) permite que computadores com endereços IP privados acessem a internet através de um endereço IP público compartilhado, traduzindo os endereços nos pacotes de saída e mantendo uma tabela de tradução para o retorno dos pacotes.

(g) Poison Reverse é uma forma de atacar redes inseguras.
Poison Reverse é uma técnica usada em protocolos de roteamento para prevenir loops de roteamento, onde um roteador anuncia uma rota para um destino
através de um vizinho com um custo infinito.

(h) O protocolo ICMP pode ser utilizado para mapear os routers pelos quais passa um pacote, tirando proveito do ...
O protocolo ICMP pode ser utilizado para mapear os roteadores pelos quais passa um pacote, tirando proveito do campo “Time Exceeded” (Tempo Excedido).
Quando um pacote atinge o limite de saltos (TTL), o roteador envia uma mensagem ICMP de “Tempo Excedido” de volta ao remetente, revelando informações
sobre os roteadores intermediários.

EXERCÌCIO 3
Considere uma rede ethernet 192.168.1.0/24 com gateway 192.168.1.1 e a seguinte tabela ARP: (VER TABELA).

Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.1.1	ether	b0:b9:8a:51:92:a2	C		eth0
192.168.1.34	ether	00:04:4b:a9:87:92	C		eth0
192.168.1.200	ether	c4:82:b2:2e:9d:2a	C		eth0
192.168.1.5	ether	9c:28:40:92:1f:43	C		eth0

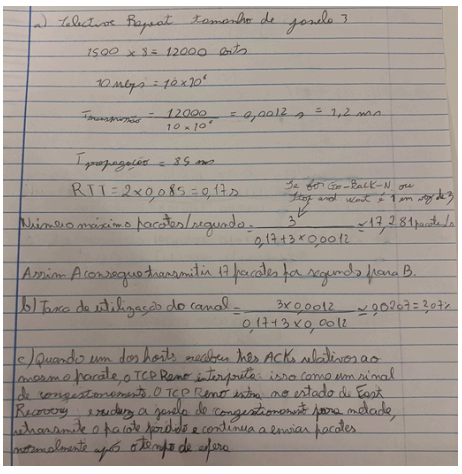
Descreva, passo a passo, o que acontece, ao
nível do protocolo em questão (dê também detalhes relevantes sobre a frame ethernet enviada), quando enviamos um pacote para o host:

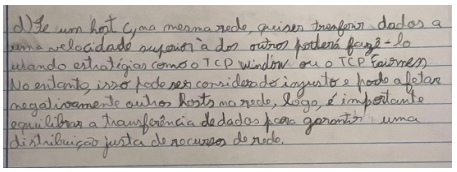
(a) 192.168.1.5
O sistema verifica a tabela ARP de modo a encontrar o endereço MAC correspondente ao IP 192.168.1.5. Como o IP 192.168.1.5 está na tabela ARP com o MAC
9c:28:40:92:1f:43. O sistema cria uma frame Ethernet, com o endereço MAC de destino 9c:28:40:92:1f:43 e o endereço MAC de origem do dispositivo de
envio. O pacote IP destinado ao IP 192.168.1.5 é encapsulado dentro da frame Ethernet e a mesma é enviada através da interface eth0.

(b) 192.168.1.10
O sistema verifica a tabela ARP de modo a encontrar o endereço MAC correspondente ao IP 192.168.1.10. Como o IP 192.168.1.10 não está na tabela ARP, o
sistema envia uma solicitação ARP em broadcast para descobrir o endereço MAC correspondente ao IP 192.168.1.10. Se o host 192.168.1.10 estiver ativo e
configurado corretamente, ele responde com uma solicitação ARP contendo o seu endereço MAC. O sistema atualiza a tabela ARP com o endereço MAC do host
192.168.1.10 e cria uma frame Ethernet com o endereço MAC de destino (recebido da solicitação ARP) e o endereço MAC de origem do dispositivo de envio.
O pacote IP destinado ao IP 192.168.1.10 é encapsulado dentro da frame Ethernet e a mesma é enviada através da interface eth0.

(c) 10.1.1.1
O sistema verifica a tabela de roteamento e determina que o destino 10.1.1.1 não está na rede local (192.168.1.0/24). Este decide enviar o pacote para
o gateway padrão (192.168.1.1). O sistema verifica a tabela ARP de modo a encontrar o endereço MAC do gateway 192.168.1.1. O IP 192.168.1.1 está na
tabela ARP com o MAC b0:b9:8a:51:92. O sistema cria uma frame Ethernet com o endereço MAC de destino b0:b9:8a:51:92 e o endereço MAC de origem do
dispositivo de envio. O pacote IP destinado ao IP 10.1.1.1 é encapsulado dentro da frame Ethernet e a mesma é enviada através da interface eth0 para o
gateway, que então encaminhará o pacote para a rede apropriada.

EXERCÌCIO 4
4. Considere dois hosts de rede A e B ligados por um canal de 10Mbps e com um tempo de propagação entre extremidades de 85 milissegundos. A está a enviar pacotes com 1500 bytes de comprimento para B.
(a) Qual é o número máximo de pacotes por segundo que A consegue transmitir para B, usando o protocolo Selective Repeat com uma janela de tamanho 3?
(b) Qual é a taxa de utilização do canal nas condições da alínea anterior?
(c) Um dos hosts recebeu três ACKS relativos ao mesmo pacote. O que vai acontecer, assumindo que estamos a usar TCP Reno?
(d) Se um host C, na mesma rede, quiser transferir dados a uma velocidade superior (i.e., injusta-mente) à dos outros, poderá fazê-lo? Se sim, como?





5. Explique como, através do NAT e do DNS, é possível ter um webserver a correr no host com endereço IP privado 192.168.1.2, na porta 8000 e aquele ficar acessível à internet através do endereço https://www.qualquercoisa.pt (i.e., na porta 443). Diga o que acontece de ambos os lados da ligação.

1. **Registro DNS:**
   - No seu servidor DNS, você cria um registro que associa `www.qualquercoisa.pt` ao endereço IP público do seu roteador.
   - Exemplo: `www.qualquercoisa.pt` aponta para `203.0.113.10` (este é o IP público do seu roteador).

Configuração do NAT

2. **Regra de NAT:**
   - No roteador, você configura uma regra para redirecionar o tráfego que chega na porta 443 (HTTPS) do IP público `203.0.113.10` para o IP privado `192.168.1.2` na porta 8000.
   - Isto significa que qualquer conexão que chegue na porta 443 será encaminhada para o webserver interno na porta 8000.

O que acontece quando alguém acessa `https://www.qualquercoisa.pt`:

Do lado do Cliente (Internet)

1. **Resolução de DNS:**
   - O cliente digita `https://www.qualquercoisa.pt` no navegador.
   - O navegador resolve `www.qualquercoisa.pt` para `203.0.113.10` (IP público).
2. **Conexão Inicial:**
   - O navegador do cliente tenta se conectar a `203.0.113.10` na porta 443.

Do lado do Servidor (Rede Interna)

3. **Roteador/Firewall (NAT):**
   - O roteador recebe a solicitação na porta 443 e redireciona essa solicitação para o servidor interno `192.168.1.2` na porta 8000.
4. **Webserver Interno:**
   - O webserver no IP `192.168.1.2`, ouvindo na porta 8000, recebe a solicitação e responde.
5. **Resposta ao Cliente:**
   - O roteador envia a resposta do webserver de volta ao cliente, fazendo parecer que veio de `203.0.113.10` na porta 443.

Resumo:
- O DNS aponta `www.qualquercoisa.pt` para o IP público do roteador.
- O roteador redireciona as conexões recebidas na porta 443 para o webserver interno na porta 8000.
- O cliente acessa `https://www.qualquercoisa.pt` e a conexão é redirecionada para o webserver interno, que responde através do roteador.

Assim, o webserver com IP privado `192.168.1.2` na porta 8000 fica acessível pela internet através de `https://www.qualquercoisa.pt` na porta 443.

EXERCÌCIO 6
6. Considere os algoritmos de Routing Inundação (com aprendizagem pelo caminho inverso) e Link state. Numa rede pequena, sem ciclos, qual será mais eficiente? Porquê?

O algorirmo Rounting Inundação (com aprendizagem pelo caminho inverso) envia pacotes pacotes para todos os vizinhos, que por sua vez retransmitem para
os seus vizinhos e assim sucessivamente. Este algoritmo permite que os roteadores mantenham informações sobre o caminho de volta para o remetente
original. No entanto, em redes pequenas, a inundação gera tráfegos desnecessários. Numa rede sem ciclos, a inundação não causa loops, mas ainda pode
ser ineficiente. Já o algoritmo Link State é baseado em informações detalhadas sobre o estados de todos os links na rede. Cada roteador mantém uma
visão completa da topologia da rede, incluindo informações sobre os links, os custos e os estados. Quando ocorre uma alteração, por exemplo, um link
falha ou é restaurado, apenas os roteadores afetados recalculam as suas tabelas de roteamento. Assim sendo, numa rede pequena, sem ciclos, o mais
eficiente será o algoritmo Link State porque evita a inundação e minimiza o tráfego de controlo; porque em redes pequenas, a sobrecarga de inundação
pode ser significativa, mesmo sem ciclos; e porque o Link State permite cálculos mais precisos de rotas.

EXERCÌCIO 7
7. Imagine que na rede do edifício CLV da Universidade de Évora é usado o algoritmo de Bellman-Ford para encaminhamento. Dê um exemplo prático de um evento que poderia provocar um problema de convergência nos routers.
O algoritmo de Bellman-Ford é usado para encontrar o caminho mais curto numa rede, mas também pode enfrentar problemas de convergência. Um exemplo prático que poderia causar problemas de convergência nos routers é uma mudança frequente na topologia da rede. Quando os routers adicionam ou removem rotas constantemente, o algoritmo pode levar tempo para se ajustar, resultando em instabilidade ou loops. Isso pode afetar a convergência e a eficiência do encaminhamento.