UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

CENTRO DE ENSINO SUPERIOR DO SERIDÓ

CURSO DE SISTEMAS DE INFORMAÇÃO

BRUNO COSTA SOUTO E FELIPE AUGUSTO ARAÚJO DA CUNHA

RELATÓRIO:

CAPTURA DE REDE

CAICÓ

2025

SUMÁRIO

Questão 1.

A.

A comunicação consiste inteiramente em mensagens ICMP. Foram identificados 6 pacotes ICMP, representando 100% do tráfego capturado. Isso indica que se trata provavelmente de um teste de conectividade, como um comando ping sendo realizado entre as máquinas de IP 192.168.0.2 e 192.168.0.3.

B.

Os endereços envolvidos são:

Endereços IP

- **Origem:**
  - 192.168.0.2 → 3 pacotes
  - 192.168.0.3 → 3 pacotes
- **Destino:**
  - 192.168.0.2 → 3 pacotes
  - 192.168.0.3 → 3 pacotes

Isso mostra que a comunicação é bilateral, os dois hosts enviam e recebem pacotes.

Endereços MAC

- **Origem:**
  - 0e:73:75:0f:b9:47 → 3 pacotes
  - 8a:0e:1b:fa:d3:1f → 3 pacotes
- **Destino:**
  - 0e:73:75:0f:b9:47 → 3 pacotes
  - 8a:0e:1b:fa:d3:1f → 3 pacotes

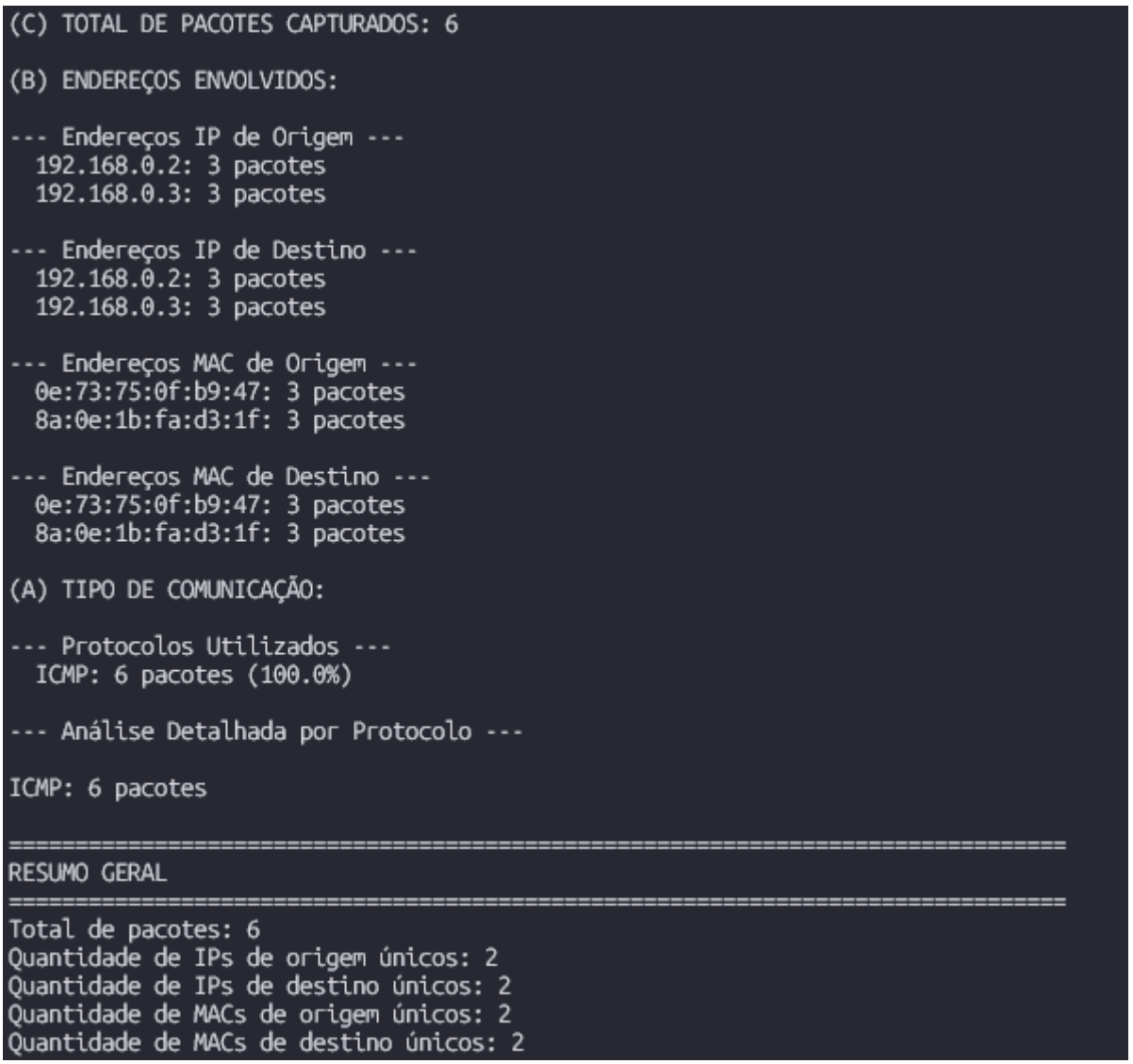
Assim como os IPs, os MACs também alternam, caracterizando troca de mensagens entre duas máquinas dentro da mesma rede local.

C.

A captura contém 6 pacotes, conforme exibido pelo programa.

```
total_packets = len(packets)
print(f"\n(C) TOTAL DE PACOTES CAPTURADOS: {total_packets}")
```

PRINT GERAL:


(C) TOTAL DE PACOTES CAPTURADOS: 6
(B) ENDEREÇOS ENVOLVIDOS:
--- Endereços IP de Origem ---
192.168.0.2: 3 pacotes
192.168.0.3: 3 pacotes
--- Endereços IP de Destino ---
192.168.0.2: 3 pacotes
192.168.0.3: 3 pacotes
--- Endereços MAC de Origem ---
0e:73:75:0f:b9:47: 3 pacotes
8a:0e:1b:fa:d3:1f: 3 pacotes
--- Endereços MAC de Destino ---
0e:73:75:0f:b9:47: 3 pacotes
8a:0e:1b:fa:d3:1f: 3 pacotes
(A) TIPO DE COMUNICAÇÃO:
--- Protocolos Utilizados ---
ICMP: 6 pacotes (100.0%)
--- Análise Detalhada por Protocolo ---
ICMP: 6 pacotes
RESUMO GERAL
Total de pacotes: 6
Quantidade de IPs de origem únicos: 2
Quantidade de IPs de destino únicos: 2
Quantidade de MACs de origem únicos: 2
Quantidade de MACs de destino únicos: 2

Questão 2.

A.

```
(a) SEQUÊNCIA DE PACOTES (mostrando os primeiros 18 pacotes):
#0001  1736447014.214524  Ether / IP / UDP / DNS Qry b'labepi.ufrn.br.'
#0002  1736447014.214581  Ether / IP / UDP / DNS Qry b'labepi.ufrn.br.'
#0003  1736447014.216903  Ether / IP / UDP / DNS Ans 177.20.148.218
#0004  1736447014.217000  Ether / IP / UDP / DNS Ans
#0005  1736447014.217212  Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http S
#0006  1736447014.240314  Ether / IP / TCP 177.20.148.218:http > 192.168.0.3:59208 SA
#0007  1736447014.240415  Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http A
#0008  1736447014.240518  Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http PA / Raw
#0009  1736447014.263568  Ether / IP / TCP 177.20.148.218:http > 192.168.0.3:59208 A
#0010  1736447014.265509  Ether / IP / TCP 177.20.148.218:http > 192.168.0.3:59208 A / Raw
#0011  1736447014.265525  Ether / IP / TCP 177.20.148.218:http > 192.168.0.3:59208 PA / Raw
#0012  1736447014.265534  Ether / IP / TCP 177.20.148.218:http > 192.168.0.3:59208 PA / Raw
#0013  1736447014.265580  Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http A
#0014  1736447014.265593  Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http A
#0015  1736447014.265601  Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http A
#0016  1736447014.266014  Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http FA
#0017  1736447014.289641  Ether / IP / TCP 177.20.148.218:http > 192.168.0.3:59208 FA
#0018  1736447014.289865  Ether / IP / TCP 192.168.0.3:59208 > 177.20.148.218:http A
```

A captura registra a comunicação completa envolvendo uma consulta DNS seguida de uma conexão HTTP, mostrando um fluxo típico de acesso a um site.

Etapa 1 — Resolução DNS (Pacotes #1 a #4)

Os primeiros pacotes são solicitações DNS:

- Pacotes #0001 e #0002: consultas DNS para o domínio labepi.ufrn.br
- Pacotes #0003 e #0004: respostas DNS contendo o IP 177.20.148.218

Ou seja, o computador perguntou ao servidor DNS qual é o IP do domínio, e recebeu a resposta.

Etapa 2 — Estabelecimento da conexão TCP (Three-way Handshake)

Após descobrir o IP do servidor, a máquina inicia uma conexão HTTP:

- #0005 → SYN (cliente → servidor)
- #0006 → SYN/ACK (servidor → cliente)
- #0007 → ACK (cliente → servidor)

Isso completa o handshake, estabelecendo a sessão TCP entre:

192.168.0.3:59208 → 177.20.148.218:80

Etapa 3 — Transferência de dados HTTP

Depois da conexão:

- #0008 → Cliente envia dados HTTP
- #0009 a #0012 → Servidor responde com pacotes contendo dados HTTP
- #0013 a #0015 → Cliente envia ACKs confirmando o recebimento

Esses pacotes mostram a troca de dados da página web.

Etapa 4 — Encerramento da conexão TCP (Four-way FIN)

A comunicação termina corretamente:

- #0016 → FIN (cliente encerra a conexão)
- #0017 → FIN (servidor confirma)
- #0018 → ACK (cliente confirma o término)

Conclusão — Essa captura se trata de uma resolução DNS seguida do acesso a um servidor web, incluindo handshake TCP, troca de dados HTTP e encerramento da conexão. Ou seja, o computador acessou o site labepi.ufrn.br.

B.

Estatísticas sobre a quantidade e tipos de pacotes com base na saída:

Quantidade total de pacotes: 18

Protocolo	Quantidade
TCP	14
UDP (DNS)	4

O tráfego é majoritariamente TCP (por causa do HTTP). A UDP aparece apenas nas consultas DNS.

Endereços IP envolvidos:

Origem	
IP de origem	**Quant. Pacotes**
192.168.0.3	10
177.20.148.218	6
192.168.1.1	2
Destino	
IP de destino	**Quant. Pacotes**
192.168.0.3	8
177.20.148.218	8
192.168.1.1	2

MACs envolvido:

Origem	
MAC Origem	**Quant. Pacotes**
4e:4f:b4:33:13:f6	10
ea:28:c2:57:03:42	8
Destino	
MAC Destino	**Quant. Pacotes**
ea:28:c2:57:03:42	10
4e:4f:b4:33:13:f6	6

Portas envolvidas:

Portas TCP (origem -> destino)		
Origem	**Destino**	**Pacotes**
59208	80	8
80	59208	6
Portas UDP (origem -> destino)		
Origem	**Destino**	**Pacotes**
41097	53	2
53	41097	2

Tamanhos de pacotes mais comuns (bytes)

Bytes (bytes)	Quant. Pacotes
66	8
74	4
1494	2
90	1
119	1
144	1
890	1

Foram capturados 18 pacotes. Os protocolos observados foram: Ethernet (18), IP (18), UDP (4 — DNS) e TCP (14 — HTTP). Há três IPs envolvidos: 192.168.0.3, 177.20.148.218 e 192.168.1.1. As portas utilizadas foram UDP 41097→53 e TCP 59208→80, caracterizando tráfego DNS seguido de comunicação HTTP.

Questão 3

A. Estatísticas sobre os IPs de origem e destino

A análise dos arquivos *captura3-1.pcap* (antes do NAT) e *captura3-2.pcap* (depois do NAT) permitiu observar o seguinte:

Antes do NAT (rede interna):

IP de origem predominante: **192.168.1.100**

IPs de destino encontrados e sua quantidades:

Antes do NAT (rede interna)	
Portas de origem mais frequentes	**Portas de destino mais frequentes**
IP de origem	**Quantidade**
192.168.1.100	62
64.233.169.104	40
74.125.106.31	18
74.125.91.113	7
68.87.71.230	5
192.168.1.1	1
69.183.241.120	1

Depois do NAT (rede externa):

IP de origem predominante**: 71.192.34.104**

IPs de destino encontrados e suas quantidades:

Depois do NAT (rede externa)	
Portas de origem mais frequentes	**Portas de destino mais frequentes**
IP de origem	**Quantidade**
192.168.1.100	72

64.233.169.104	30
74.125.106.31	13
74.125.91.113	9
68.87.71.230	5
10.119.240.64	2
192.168.1.1	1
69.183.241.120	1
128.119.47.218	1

Esses resultados mostram que o NAT atuou **somente no IP de origem**, substituindo o endereço interno pelo endereço público.

B. Estatísticas sobre as portas de origem e destino:

Antes do NAT (Top 10)			
Portas de origem mais frequentes		**Portas de destino mais frequentes**	
Porta	**Quantidade**	**Porta**	**Quantidade**
80	65	80	52
4335	22	4335	33
4331	13	4331	18
53	5	53	5
4330	5	4330	4
4336	4	4338	4
4337	4	161	3
4338	4	4336	3
1028	3	4337	3
51554	1	51554	1

Depois do NAT (Top 10)			
Portas de origem mais frequentes		**Portas de destino mais frequentes**	
Porta	**Quantidade**	**Porta**	**Quantidade**
80	65	80	52
4335	22	4335	33
4331	13	4331	18
53	5	53	5
4330	5	4330	4
4336	4	4338	4
4337	4	137	3
4338	4	4336	3
137	3	4337	3
15525	2	5355	2

Nas capturas antes do NAT, o principal IP de origem é o endereço interno 192.168.1.100, mostrando que o tráfego parte diretamente da máquina da rede local. Já depois do NAT, esse endereço deixa de aparecer e é substituído por IPs públicos como 71.192.34.104 e 71.192.32.1, que pertencem ao roteador ou ao provedor. Isso confirma que o NAT atuou exatamente como esperado: ele reescreveu apenas o IP de origem, trocando o endereço privado pelo endereço público para permitir a comunicação com a internet, enquanto o restante das informações dos pacotes permaneceu inalterado.

C. Análise do funcionamento do NAT

(i) IP de origem e destino antes e após o NAT

Situação	IP de Origem	IP de Destino
Antes do NAT	192.168.1.100	Servidores externos
Depois do NAT	71.192.34.104	Servidores externos

Conclusão:
O endereço interno 192.168.1.100 foi traduzido para o endereço público 71.192.34.104.

(ii) Portas de origem e destino antes e após o NAT

O script identificou correspondências claras entre portas antes e depois do NAT:

```
--- Mapeamentos NAT candidatos (pre -> post) e contagem de ocorrências ---
  192.168.1.100:4335  ->  71.192.34.104:4335: 22 pacote(s)
  192.168.1.100:4331  ->  71.192.34.104:4331: 13 pacote(s)
  192.168.1.100:4330  ->  71.192.34.104:4330: 5 pacote(s)
  192.168.1.100:4336  ->  71.192.34.104:4330: 4 pacote(s)
  192.168.1.100:4337  ->  71.192.34.104:4335: 4 pacote(s)
  192.168.1.100:4338  ->  71.192.34.104:4335: 4 pacote(s)
  192.168.1.100:1028  ->  71.192.34.104:1028: 3 pacote(s)
  192.168.1.100:51554  ->  71.192.34.104:51554: 1 pacote(s)
  192.168.1.100:58982  ->  71.192.34.104:51554: 1 pacote(s)
  192.168.1.100:15525  ->  71.192.34.104:15525: 1 pacote(s)
  192.168.1.100:49200  ->  71.192.34.104:51554: 1 pacote(s)
  192.168.1.100:57244  ->  71.192.34.104:51554: 1 pacote(s)
  192.168.1.100:60524  ->  71.192.34.104:51554: 1 pacote(s)
```

Conclusão:
As portas de destino permanecem iguais antes e depois do NAT. As portas de origem, na maioria dos fluxos, também são mantidas, mudando apenas em poucos casos para evitar conflitos. Isso mostra que o NAT preserva as portas sempre que possível.

(iii) Justificativa e observações

- O IP interno (192.168.1.100) aparece somente na captura “antes do NAT”.
- Na captura “depois do NAT”, todo o tráfego originado desse host aparece como vindo de 71.192.34.104, que é o IP público do roteador.
- Os destinos permanecem idênticos, mostrando que o NAT só altera o endereço IP de origem.
- As portas antes e depois são, em sua maioria, idênticas, indicando preservação de portas durante a tradução.

  Assim, as capturas demonstram o funcionamento típico do NAT:
  Substituir o IP interno por um IP público, mantendo as portas para garantir o correto retorno dos pacotes.