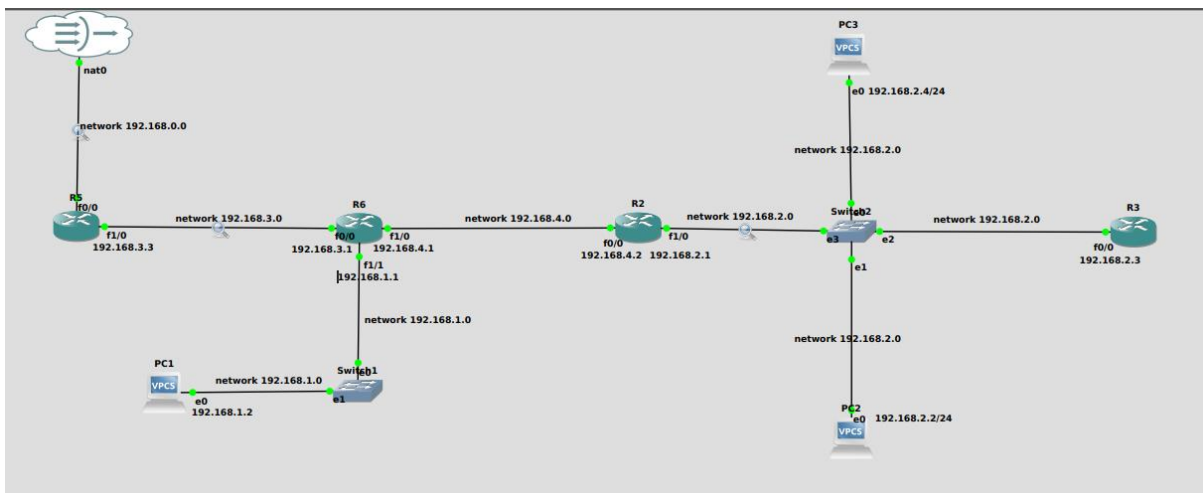


Zadanie 1:



R5:

```
R5#enable
R5#show ip interface brief
Interface                IP-Address      OK? Method Status      Prot
FastEthernet0/0          192.168.122.144 YES DHCP    up          up
FastEthernet1/0          192.168.3.3     YES manual  up          up
NVI0                     192.168.122.144 YES unset   up          up

R5#asciiinema rec r5
^
% Invalid input detected at '^' marker.

R5#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/89/220 ms
R5#
```

R6:

```
R6#enable
R6#show ip interface brief
Interface                IP-Address      OK? Method Status      Prot
FastEthernet0/0          192.168.3.1     YES manual  up          up
FastEthernet1/0          192.168.4.1     YES manual  up          up
FastEthernet1/1          192.168.1.1     YES manual  up          up

R6#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/77/116 ms
R6#
```

R2:

```

R2#enable
R2#show ip interface brief
Interface              IP-Address      OK? Method Status    Prot
ocol
FastEthernet0/0        192.168.4.2     YES manual up        up
FastEthernet1/0        192.168.2.1     YES manual up        up

R2#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/72/96 ms

```

R3:

```

R3#enable
R3#show ip interface brief
Interface              IP-Address      OK? Method Status    Prot
ocol
FastEthernet0/0        192.168.2.3     YES manual up        up

R3#ping google.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 142.250.203.142, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/76/88 ms

```

Wysyłanie pakietów z R6 do R3:

```

R6#ping 192.168.2.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/16/20 ms
R6#

```

Wysyłanie pakietów Z PC2 do R5:

```

PC2> ping 192.168.3.3

84 bytes from 192.168.3.3 icmp_seq=1 ttl=253 time=40.429 ms
84 bytes from 192.168.3.3 icmp_seq=2 ttl=253 time=27.323 ms
84 bytes from 192.168.3.3 icmp_seq=3 ttl=253 time=27.420 ms
84 bytes from 192.168.3.3 icmp_seq=4 ttl=253 time=27.347 ms
84 bytes from 192.168.3.3 icmp_seq=5 ttl=253 time=27.291 ms

PC2>

```

Zadanie 2 i 3:

```

PC2> ping google.com
google.com resolved to 142.250.203.142

84 bytes from 142.250.203.142 icmp_seq=1 ttl=109 time=82.190 ms
84 bytes from 142.250.203.142 icmp_seq=2 ttl=109 time=78.136 ms
84 bytes from 142.250.203.142 icmp_seq=3 ttl=109 time=87.706 ms
84 bytes from 142.250.203.142 icmp_seq=4 ttl=109 time=76.773 ms
84 bytes from 142.250.203.142 icmp_seq=5 ttl=109 time=88.166 ms

```

Analiza do network_192_168_2_0 z PC2:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-------------|-------------|----------|--------|---|
| 1 | 0.000000 | 192.168.2.2 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x8768, seq=1/256, ttl=64 (reply in 2) |
| 2 | 0.057874 | 8.8.8.8 | 192.168.2.2 | ICMP | 98 | Echo (ping) reply id=0x8768, seq=1/256, ttl=109 (request in 1) |
| 3 | 0.058747 | 192.168.2.2 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x8868, seq=2/512, ttl=64 (reply in 4) |
| 4 | 1.115822 | 8.8.8.8 | 192.168.2.2 | ICMP | 98 | Echo (ping) reply id=0x8868, seq=2/512, ttl=109 (request in 3) |
| 5 | 2.116725 | 192.168.2.2 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x8968, seq=3/768, ttl=64 (reply in 6) |
| 6 | 2.117393 | 8.8.8.8 | 192.168.2.2 | ICMP | 98 | Echo (ping) reply id=0x8968, seq=3/768, ttl=109 (request in 5) |
| 7 | 3.174578 | 192.168.2.2 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x8a68, seq=4/1024, ttl=64 (reply in 8) |
| 8 | 3.232857 | 8.8.8.8 | 192.168.2.2 | ICMP | 98 | Echo (ping) reply id=0x8a68, seq=4/1024, ttl=109 (request in 7) |
| 9 | 4.232520 | 192.168.2.2 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x8b68, seq=5/1280, ttl=64 (reply in 10) |
| 10 | 4.298297 | 8.8.8.8 | 192.168.2.2 | ICMP | 98 | Echo (ping) reply id=0x8b68, seq=5/1280, ttl=109 (request in 9) |

- **Identyfikatory i Sekwencje:** Każde zapytanie ma unikalny identyfikator (id) i numer sekwencji, co pozwala na sparowanie odpowiedzi z odpowiednim zapytaniem.
- Przykładowo, pierwsze zapytanie (seq=1/256, ttl=109) ma identyfikator 0x8768 i otrzymuje odpowiedź z tym samym identyfikatorem, co potwierdza, że odpowiedź dotyczy tego zapytania.
- **Time to Live (TTL):** Wartość TTL zmienia się w odpowiedziach na 64, co jest typową wartością dla odpowiedzi ping. Zapytania mają TTL 109, co sugeruje, że mogły przejść przez kilka urządzeń sieciowych, zanim dotarły do celu.

Analiza do network_192_168_3_0:

Jeżeli korzystam z Cloud

| | | | | | | |
|----|-----------|-------------|-------------|------|----|--|
| 34 | 53.930295 | 192.168.2.2 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x4376, seq=2/512, ttl=62 (no response found!) |
| 35 | 53.932533 | 192.168.3.3 | 192.168.2.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 36 | 54.968467 | 192.168.2.2 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x4476, seq=3/768, ttl=62 (no response found!) |
| 37 | 54.970524 | 192.168.3.3 | 192.168.2.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 38 | 56.009217 | 192.168.2.2 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x4576, seq=4/1024, ttl=62 (no response found!) |
| 39 | 56.008511 | 192.168.3.3 | 192.168.2.2 | ICMP | 70 | Destination unreachable (Host unreachable) |
| 40 | 57.044121 | 192.168.2.2 | 8.8.8.8 | ICMP | 98 | Echo (ping) request id=0x4676, seq=5/1280, ttl=62 (no response found!) |
| 41 | 57.046533 | 192.168.3.3 | 192.168.2.2 | ICMP | 70 | Destination unreachable (Host unreachable) |

| |
|---|
| Frame 32: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface -, id 0 |
| Ethernet II, Src: ca:03:97:a3:00:1c (ca:03:97:a3:00:1c), Dst: ca:01:97:07:00:00 (ca:01:97:07:00:00) |
| Internet Protocol Version 4, Src: 192.168.3.3, Dst: 192.168.2.2 |
| 0100 = Version: 4 |
| 0101 = Header Length: 20 bytes (5) |
| Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) |
| Total Length: 56 |
| Identification: 0x0000 (0) |
| Flags: 0x00 |
| ...0 0000 0000 0000 = Fragment Offset: 0 |
| Time to Live: 255 |
| Protocol: ICMP (1) |
| Header Checksum: 0x3509 [validation disabled] |
| [Header checksum status: Unverified] |
| Source Address: 192.168.3.3 |
| Destination Address: 192.168.2.2 |
| Internet Control Message Protocol |
| Type: 3 (Destination unreachable) |
| Code: 1 (Host unreachable) |
| Checksum: 0xd4f2 [correct] |
| [Checksum Status: Good] |
| Unused: 00000000 |
| Internet Protocol Version 4, Src: 192.168.2.2, Dst: 8.8.8.8 |
| 0100 = Version: 4 |
| 0101 = Header Length: 20 bytes (5) |
| Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) |
| Total Length: 84 |
| Identification: 0x7642 (30274) |
| Flags: 0x00 |
| ...0 0000 0000 0000 = Fragment Offset: 0 |
| Time to Live: 61 |
| Protocol: ICMP (1) |
| Header Checksum: 0x34ad [validation disabled] |
| [Header checksum status: Unverified] |
| Source Address: 192.168.2.2 |
| Destination Address: 8.8.8.8 |
| Internet Control Message Protocol |

- **Src (Źródło):** 192.168.3.3 (R5)
- **Dst (Cel):** 192.168.2.2 (PC2)
- **Typ ICMP:** Destination Unreachable, Code: Host Unreachable, co oznacza, że host docelowy jest nieosiągalny (dlatego że Cloud nie jest połączone z siecią).
- **ICMP zawiera w sobie:**
- Fragment oryginalnego pakietu ICMP wysłanego przez źródło, pokazujący, że host 192.168.2.2 próbował się połączyć z 8.8.8.8.

Jeżeli korzystam z NAT:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|-----------------|-----------------|----------|--------|--|
| 45 | 130.352034 | 192.168.2.2 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0x90aa, seq=1/256, ttl=62 (reply in 46) |
| 46 | 130.433375 | 142.250.203.142 | 192.168.2.2 | ICMP | 98 | Echo (ping) reply id=0x90aa, seq=1/256, ttl=111 (request in 45) |
| 47 | 131.471313 | 192.168.2.2 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0x9aaa, seq=2/512, ttl=62 (reply in 48) |
| 48 | 131.531678 | 142.250.203.142 | 192.168.2.2 | ICMP | 98 | Echo (ping) reply id=0x9aaa, seq=2/512, ttl=111 (request in 47) |
| 50 | 132.569872 | 192.168.2.2 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0x9baa, seq=3/768, ttl=62 (reply in 51) |
| 51 | 132.649176 | 142.250.203.142 | 192.168.2.2 | ICMP | 98 | Echo (ping) reply id=0x9baa, seq=3/768, ttl=111 (request in 50) |
| 52 | 133.678110 | 192.168.2.2 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0x9daa, seq=4/1024, ttl=62 (reply in 53) |
| 53 | 133.728326 | 142.250.203.142 | 192.168.2.2 | ICMP | 98 | Echo (ping) reply id=0x9daa, seq=4/1024, ttl=111 (request in 52) |
| 54 | 134.756398 | 192.168.2.2 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0x9eaa, seq=5/1280, ttl=62 (reply in 55) |
| 55 | 134.816591 | 142.250.203.142 | 192.168.2.2 | ICMP | 98 | Echo (ping) reply id=0x9eaa, seq=5/1280, ttl=111 (request in 54) |

Frame 45: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface ..., id 0

Ethernet II, Src: ca:01:97:07:00:00 (ca:01:97:07:00:00), Dst: ca:03:97:a3:00:1c (ca:03:97:a3:00:1c)

Internet Protocol Version 4, Src: 192.168.2.2, Dst: 142.250.203.142

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

0000 00.. = Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 84

Identification: 9xaa99 (43673)

Flags: 0x00

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 62

Protocol: ICMP (1)

Header Checksum: 0xb4dc [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.2.2

Destination Address: 142.250.203.142

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x8660 [correct]

[Checksum Status: Good]

Identifier (BE): 39338 (0x99aa)

Identifier (LE): 43673 (0xaa99)

Sequence Number (BE): 1 (0x0001)

Sequence Number (LE): 256 (0x0100)

[Response frame: 46]

Data (56 bytes)

Nie jest widoczne że 192.168.2.2 kontaktuje się z 192.168.3.3 kiedy wysyła ping do 8.8.8.8, ale TTL zmienia się z 64 na 62

Analiza do network_192_168_0_0:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|-----------------|-----------------|----------|--------|---|
| 144 | 213.059290 | 192.168.122.144 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0x99aa, seq=1/256, ttl=61 (reply in 145) |
| 145 | 213.097602 | 142.250.203.142 | 192.168.122.144 | ICMP | 98 | Echo (ping) reply id=0x99aa, seq=1/256, ttl=112 (request in 144) |
| 147 | 214.147529 | 192.168.122.144 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0x9aaa, seq=2/512, ttl=61 (reply in 148) |
| 148 | 214.194350 | 142.250.203.142 | 192.168.122.144 | ICMP | 98 | Echo (ping) reply id=0x9aaa, seq=2/512, ttl=112 (request in 147) |
| 149 | 215.246013 | 192.168.122.144 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0x9baa, seq=3/768, ttl=61 (reply in 150) |
| 150 | 215.297528 | 142.250.203.142 | 192.168.122.144 | ICMP | 98 | Echo (ping) reply id=0x9baa, seq=3/768, ttl=112 (request in 149) |
| 152 | 216.354246 | 192.168.122.144 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0x9daa, seq=4/1024, ttl=61 (reply in 153) |
| 153 | 216.387465 | 142.250.203.142 | 192.168.122.144 | ICMP | 98 | Echo (ping) reply id=0x9daa, seq=4/1024, ttl=112 (request in 152) |
| 154 | 217.432359 | 192.168.122.144 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0x9eaa, seq=5/1280, ttl=61 (reply in 155) |
| 155 | 217.478205 | 142.250.203.142 | 192.168.122.144 | ICMP | 98 | Echo (ping) reply id=0x9eaa, seq=5/1280, ttl=112 (request in 154) |
| 183 | 253.126671 | 192.168.122.144 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0xc1aa, seq=1/256, ttl=61 (reply in 184) |
| 184 | 253.167514 | 142.250.203.142 | 192.168.122.144 | ICMP | 98 | Echo (ping) reply id=0xc1aa, seq=1/256, ttl=112 (request in 183) |
| 186 | 254.204761 | 192.168.122.144 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0xc2aa, seq=2/512, ttl=61 (reply in 187) |
| 187 | 254.248121 | 142.250.203.142 | 192.168.122.144 | ICMP | 98 | Echo (ping) reply id=0xc2aa, seq=2/512, ttl=112 (request in 186) |
| 188 | 255.283143 | 192.168.122.144 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0xc4aa, seq=3/768, ttl=61 (reply in 189) |
| 189 | 255.337772 | 142.250.203.142 | 192.168.122.144 | ICMP | 98 | Echo (ping) reply id=0xc4aa, seq=3/768, ttl=112 (request in 188) |
| 191 | 256.371434 | 192.168.122.144 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0xc5aa, seq=4/1024, ttl=61 (reply in 192) |
| 192 | 256.414448 | 142.250.203.142 | 192.168.122.144 | ICMP | 98 | Echo (ping) reply id=0xc5aa, seq=4/1024, ttl=112 (request in 191) |
| 193 | 257.449877 | 192.168.122.144 | 142.250.203.142 | ICMP | 98 | Echo (ping) request id=0xc6aa, seq=5/1280, ttl=61 (reply in 194) |
| 194 | 257.500060 | 142.250.203.142 | 192.168.122.144 | ICMP | 98 | Echo (ping) reply id=0xc6aa, seq=5/1280, ttl=112 (request in 193) |

Analiza Echo (ping) Request

Type 8, Code 0: Typowo dla żądań ping (ICMP Echo Request), co oznacza inicjację procesu pingowania.Checksum: Zapewnia, że pakiet nie został zmieniony podczas transmisjiIdentifier i Sequence Number: Służą do identyfikacji i parowania żądań z odpowiedziami. W tym przypadku, identyfikator i numer sekwencyjny są pomocne w śledzeniu, jakie żądanie ping odpowiada której odpowiedzi, zwłaszcza w dynamicznej sieci z wieloma urządzeniami. Adresy IP (źródłowy i docelowy): 192.168.122.144 do 142.250.203.142. Pierwszy adres należy do lokalnej sieci, a drugi jest zewnętrzny, co wskazuje na komunikację poza lokalną sieć. To sugeruje, że R5, mimo uzyskania adresu IP dynamicznie, prawidłowo routuje pakiety na zewnątrz sieci lokalnej. Długość danych wynosząca 56 bajtów wraz z zamieszczonymi danymi pokazuje, co dokładnie jest wysyłane w ramach żądania ICMP.

- Rola DHCP: W GNS3, gdy router uzyskuje adres dynamicznie, używa DHCP do otrzymania adresu, maski, bramy oraz innych informacji konfiguracyjnych. To ułatwia integrację routera z większymi, dynamicznie zarządzanymi sieciami.
- Dostęp do Internetu: Fakt, że R5 może wysyłać żądania do adresu IP, który jest zewnętrzny i otrzymywać odpowiedzi, sugeruje prawidłową konfigurację routingu i działanie DHCP.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|-----------------|-----------------|----------|--------|---|
| 142 | 212.948203 | 192.168.122.144 | 8.8.8.8 | DNS | 78 | Standard query 0x353f A google.com |
| 143 | 213.007888 | 8.8.8.8 | 192.168.122.144 | DNS | 86 | Standard query response 0x353f A google.com A 142.250.203.142 |
| 181 | 253.025761 | 192.168.122.144 | 8.8.8.8 | DNS | 78 | Standard query 0x6e95 A google.com |
| 182 | 253.085594 | 8.8.8.8 | 192.168.122.144 | DNS | 86 | Standard query response 0x6e95 A google.com A 142.250.203.142 |

komputer (DNCp adres dla R5 192.168.122.144) pytał serwer DNS (8.8.8.8) o adres IP dla google.com i otrzymał odpowiedź z adresem 142.250.203.142. To oznacza, że komputer mógł potem użyć tego adresu IP, aby komunikować się z serwerem Google.

Rekord A (Address Record) służy do mapowania nazw domenowych na adresy IPv4, które są używane do identyfikacji urządzeń w sieci Internet. Innymi słowy, kiedy wpisujesz w przeglądarce internetowej nazwę domeny, jak google.com, system DNS używa rekordu A, aby przekształcić tę nazwę w odpowiadający jej adres IP.

```

* Frame 26: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface -, id 0
* Ethernet II, Src: ca:02:97:85:00:1c (ca:02:97:85:00:1c), Dst: IPv4mcast_09 (01:00:5e:00:00:09)
  * Destination: IPv4mcast_09 (01:00:5e:00:00:09)
  * Source: ca:02:97:85:00:1c (ca:02:97:85:00:1c)
  * Type: IPv4 (0x0800)
* Internet Protocol Version 4, Src: 192.168.2.1, Dst: 224.0.0.9
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  * Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  Total Length: 112
  Identification: 0x0000 (0)
  * Flags: 0x00
  ...0 0000 0000 0000 = Fragment Offset: 0
* Time to Live: 2
  * [Expert Info (Note/Sequence): "Time To Live" != 1 for a packet sent to the Local Network Control Block (see RFC 3171)]
  Protocol: UDP (17)
  Header Checksum: 0x150b [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.2.1
  Destination Address: 224.0.0.9
* User Datagram Protocol, Src Port: 520, Dst Port: 520
  Source Port: 520
  Destination Port: 520
  Length: 92
  Checksum: 0x0f64 [unverified]
  [Checksum Status: Unverified]
  [Stream Index: 0]
  * [Timestamps]
  UDP payload (84 bytes)
* Routing Information Protocol
  Command: Response (2)
  Version: RIPv2 (2)
  * IP Address: 0.0.0.0, Metric: 3
  * IP Address: 192.168.1.0, Metric: 2
  * IP Address: 192.168.3.0, Metric: 2
  * IP Address: 192.168.4.0, Metric: 1

```

Funkcja RIPv2

RIPv2 jest prostym protokołem routingu używanym w mniejszych sieciach. Pakiety RIPv2 są wysyłane cyklicznie co 30 sekund lub w odpowiedzi na zmiany w sieci. Każdy router odbierający takie informacje może aktualizować swoją tabelę routingu na podstawie otrzymanych danych, co pozwala na dynamiczne dostosowywanie do zmieniającej się topologii sieci. Wszystkie informacje są rozgłaszane na adres multicast, co oznacza, że są one odbierane przez wszystkie urządzenia nasłuchujące na ten adres w sieci lokalnej.

Ten konkretny pakiet jest przykładem tego, jak RIPv2 pomaga w utrzymaniu spójności informacji o trasach w sieci, co jest kluczowe dla efektywnego i poprawnego routingu pakietów.

Ethernet II

- **Source (Źródło):** ca:03:07:90:00:1c - Adres MAC urządzenia wysyłającego ramkę.
- **Destination (Cel):** IPv4mcast_09 (01:00:5e:00:00:09) - Adres MAC multicast, który jest standardowym adresem używanym przez RIPv2 do rozgłaszania informacji routingowych.

Internet Protocol Version 4 (IPv4)

- **Src (Źródło):** 192.168.2.1 - Adres IP urządzenia wysyłającego, prawdopodobnie router.
- **Dst (Destynacja):** 224.0.0.9 - Adres IP multicast używany przez RIPv2 do rozgłaszania informacji o trasach.
- **Differentiated Services Field:** 0xc0 (DSCP: CS6) - Wysoki priorytet ruchu, co jest typowe dla ruchu kontrolnego w sieci, jakim jest routing.
- **Time to Live (TTL):** 2 - Ograniczona wartość TTL, sugerująca, że pakiet powinien być rozgłaszany tylko lokalnie (w obrębie jednego lub dwóch segmentów sieci).

Routing Information Protocol (RIP)

- **Command:** Response (2) - Typ komendy RIP, tutaj odpowiedź, która zawiera informacje o dostępnych trasach.
- **Version:** RIPv2 (2) - Wersja protokołu RIP, tutaj RIPv2.
- **Routes Information:**
 - **0.0.0.0:** Brak specyficznej trasy; używane do ogłaszania metryki domyślnej.
 - **192.168.1.0/24, 192.168.3.0/24, 192.168.4.0/24:** Adresy sieci ogłaszane z odpowiednimi metrykami (2, 2, 1), które wskazują na koszt (liczbę przeskoków) do każdej z sieci.