

Sprawozdanie Lista 4

Przedmiot	Technologie sieciowe
Prowadzący	Mgr inż. Dominik Bojko
Autor	Joanna Kulig
Indeks	261743
Grupa	Czw. 17:05 - 18:45
Kod grupy	K03-76d

1. Opis zadania.

Celem zadania było skonfigurowanie sieci wirtualnej o podanej topologii za pomocą symulatora GNS3. Przy jej realizacji, należało się upewnić, że:

- sieć jest podłączona do zewnętrznej, fizycznej sieci **Cloud**
- router bezpośrednio połączony z siecią **Cloud** uzyskuje z niej dynamiczny adres IP
- pozostałe urządzenia posiadają dynamiczny adres IP w swoich sieciach
- możliwe jest wysyłanie komunikatów "ping" pomiędzy dowolną parą urządzeń oraz na adres zewnętrzny.

Następnie należało ustawić przechwytywanie pakietów na niektórych fragmentach sieci, a następnie je przeanalizować po wysłaniu zapytania "ping [google.com](#)" z jednego z urządzeń.

1 Środowisko

GNS3 (ang. Graphical Network Simulator) to emulator sieci, dzięki któremu można tworzyć i testować konfiguracje sieci.

Można go pobrać za darmo z [oficjalnej strony](#) GNS3.

1.1. GNS3 VM

Przy instalowaniu programu należy również zainstalować [odpowiednie narzędzie](#) do wirtualizacji. Należy go zaimportować do programu z zakładce Preferences -> GNS3 VM. Jest ono potrzebne, aby móc wirtualizować serwer oraz podpięte w symulacji urządzenia.

Specyfikacja maszyny wirtualnej w VirtualBox:

Ogólne

Nazwa: GNS3 VM
System operacyjny: Ubuntu (64-bit)

System

RAM: 2048 MB
Boot Order: Dysk twardy, Napęd optyczny
Akceleracja: VT-x/AMD-V, Zagnieżdżone stronicowanie, PAE/NX, Parawirtualizacja KVM

Ekran

Pamięć wideo: 8 MB
Graphics Controller: VBoxVGA
Remote Desktop Server Port: 5950
Recording: Disabled

Pamięć

Kontroler: IDE Controller
IDE Primary Device 0: GNS3 VM-disk001.vdi (Normalny, 19,53 GB)
Kontroler: SATA Controller
Port SATA 2: GNS3 VM-disk002.vdi (Normalny, 488,28 GB)

Dźwięk

Sterownik gospodarza: Windows DirectSound
Controller: ICH AC97

Network

Karta 1: Intel PRO/1000 MT Desktop (Karta sieci izolowanej, "VirtualBox Host-Only Ethernet Adapter")
Karta 2: Intel PRO/1000 MT Desktop (NAT)
Karta 3: Intel PRO/1000 MT Desktop (Mostkowana karta sieciowa, Realtek PCIe GbE Family Controller)

Podgląd

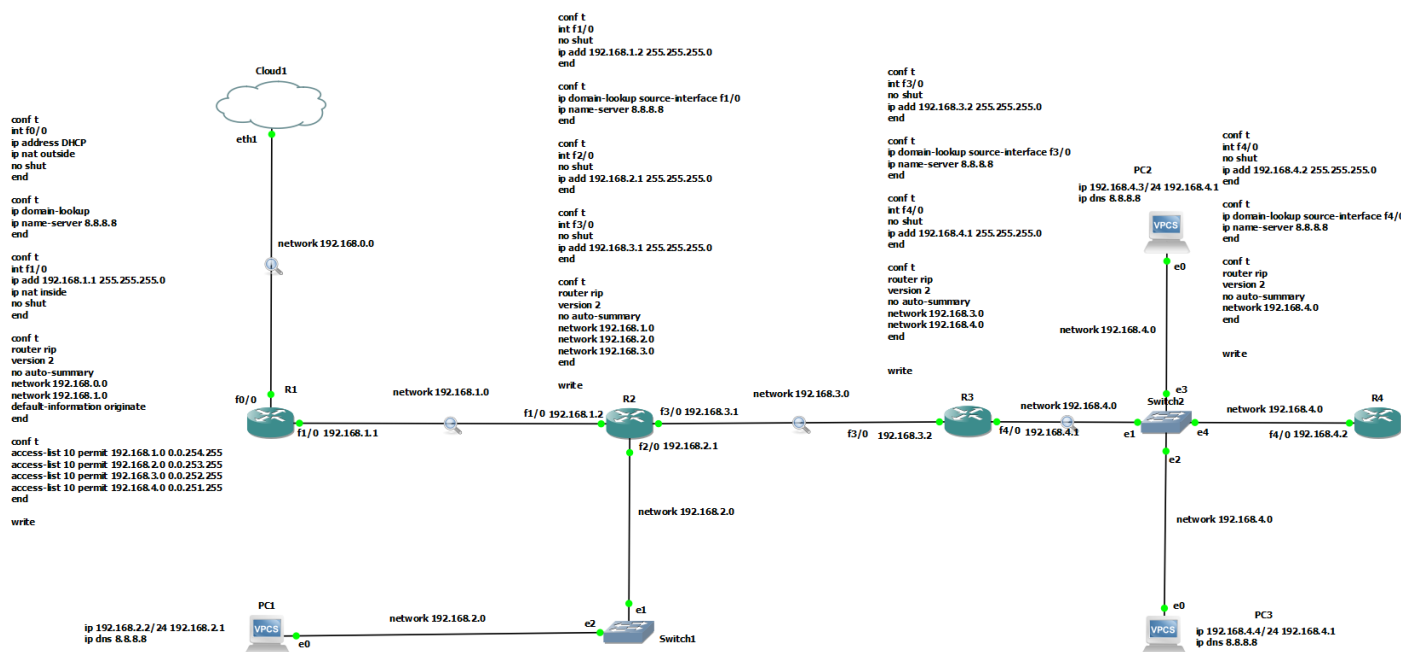
Rysunek 1. Specyfikacje maszyny wirtualnej GNS3.

Wybrane dla maszyny karty sieciowe mają znaczenie. Oprócz kart "VBox host-only" oraz NAT trzeba także podpiąć mostkowaną kartę sieciową, która wskazuje na faktyczną kartę w komputerze. GNS3 stanowczo odradza używania do tego celu wifi, zatem została wykorzystana karta ethernetowa. Dodatkowo ważne jest zaznaczenie opcji Nested VT-x/AMD-V, aby można było symulować maszyny wirtualne odpowiadające urządzeniom dodawanym do naszej topologii.

1.2 Obraz routera

Do zrobienia konfiguracji wykorzystany został router Cisco 7200. Jego obraz jest dostępny do pobrania na [GNS3 Marketplace](#). Należy go zaimportować do programu z zakładki Preferences -> DSynamips -> IOS routers.

2. Konfiguracja sieci



Rysunek 2. Zadania konfiguracja sieci.

2.1 Komendy do konfiguracji urządzeń.

Konfiguracja routerów:

```
sh ip int br          // pozwala na podpatrzenie interfejsów danego urządzenia
conf t                // wejście w tryb konfiguracji urządzenia
int X                 // przejście do konfiguracji interfejsu X
ip add X Y            // ustawienie urządzeniu adres X oraz maskę Y
no shut               // uruchamianie interfejsu

ip domain-lookup source-interface X // ustawienie wyszukiwania nazw serwerów przez interfejs X
ip name-server 8.8.8.8 // ustawienie adresu DNS

// RIP (ang. Routing Information Protocol) - służący do wyznaczania najlepszej trasy między źródłem, a celem
// skonfigurowanie routowania zgodnie z RIP w wersji 2
router rip
version 2
// konfiguracja RIP
default-information originate // ustawienie domyślnej ścieżki do sieci zewnętrznej
no auto-summary              // wyłącza auto-sumowanie ścieżek

network X                    // informowanie routera o bezpośrednim dostępie do sieci X

end                           // zakończenie konfiguracji
write                         // zapisanie danej konfiguracji
```

Konfiguracja komputerów:

```
ip X Y                // nadanie komputerowi ip wraz z maską X oraz adresu ip routera Y, który łą
ip dns 8.8.8.8         // nadanie adresu serwera DNS
sh ip all              // pokazanie ip oraz gateway'a komputera
```

2.2 Konfiguracja routera brzegowego:

Przy konfiguracji brzegowego routera R1 musimy go połączyć z **Cloud'em**, w celu uzyskaniu dostępu do internetu.

```
R1# conf t
R1(config)# int f0/0
R1(config-if)# ip address dhcp // ustawienie adresu ip routerowi przez sieć zgodnie z protokołem dhcp
R1(config-if)# ip nat outside // oznaczenie interfejsu jako publiczny
R1(config-if)# no shut
R1(config-if)# end
```

Następnie ustawiamy adres DNS, aby można było pingować serwery po ich nazwach, zamiast po ich adresach ip.

```
R1# conf t
R1(config)# ip domain-lookup      // ustawienie wyszukiwania nazw serwerów
R1(config)# ip name-server 8.8.8.8
R1(config)# end
```

Przed konfiguracją innych routerów niż brzegowy, musimy mu przygotować interfejs, dzięki któremu będzie się mógł łączyć z wewnętrznymi urządzeniami.

```
R1# conf t
R1(config)# int f1/0
R1(config-if)# ip add 192.168.1.1 255.255.255.0
R1(config-if)# ip nat inside      // oznaczenie interfejsu jako prywatny
R1(config-if)# no shut
R1(config-if)# end
```

Należy również skonfigurować routing oraz dostęp routera do odpowiednich sieci.

```
R1# conf t
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# no auto-summary
R1(config-router)# network 192.168.0.0
R1(config-router)# network 192.168.1.0
R1(config-router)# default-information originate.
R1(config-router)# end
```

Na końcu musimy ustawić routerowi R1 tzw. **access list**, czyli listę adresów, od których pakiety może przesyłać na zewnątrz. Podajemy adresy sieci, które chcemy przepuścić oraz odwróconą maskę.

```
R1# conf t
R1(config)# access-list 10 permit 192.168.1.0 0.0.0.255
R1(config)# access-list 10 permit 192.168.2.0 0.0.0.255
R1(config)# access-list 10 permit 192.168.3.0 0.0.0.255
R1(config)# access-list 10 permit 192.168.4.0 0.0.0.255
R1(config)# end
```

Zapisujemy konfigurację komendą **write**.

2.3 Konfiguracja pozostałych routerów:

Routery inne niż brzegowy konfigurujemy w podobny sposób, pomijając jedynie kilka komend, które zostały użyte przy routerze R1.

Nie ma sensu pokazywania konfiguracji każdego z nich, zatem pokażę ją na przykładzie routera R3.

```
R3# conf t
R3(config)# int f3/0
R3(config-if)# no shut
R3(config-if)# ip add 192.168.3.2 255.255.255.0
R3(config-if)# end

R3# conf t
R3(config)# ip domain-lookup source-interface f3/0
R3(config)# ip name-server 8.8.8.8
R3(config)# end

R3# conf t
R3(config)# int f4/0
R3(config-if)# no shut
R3(config-if)# ip add 192.168.4.1 255.255.255.0
R3(config-if)# end

R3# conf t
R3(config)# router rip
R3(config-router)# version 2
R3(config-router)# no auto-summary
R3(config-router)# network 192.168.3.0
R3(config-router)# network 192.168.4.0
R3(config-router)# end

R3# write
```

2.4 Konfiguracja switcha:

Urządzenia switch nie wymagają konfiguracji po ich odpowiednim podpięciu.

2.5 Konfiguracja komputera:

Konfiguracja na podstawie komputera PC1.

```
PC2> ip 192.168.4.3/24 192.168.4.1
PC2> ip dns 8.8.8.8
```

Sprawdzenie poprawności działania polecenia **ping** na inne urządzenia w sieci.

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/18/24 ms
R1#ping 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/44/56 ms
R1#ping 192.168.4.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/65/76 ms
R1#ping 192.168.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/44/124 ms
R1#ping 192.168.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.4, timeout is 2 seconds:
```

Rysunek 3. Polecenie ping na inne adresy w sieci wykonane z urządzenia R1

Sprawdzenie poprawności działania polecenia **ping** na serwery zewnętrzne z urządzenia PC2.

```
PC2> ping google.com
google.com resolved to 216.58.208.206

84 bytes from 216.58.208.206 icmp_seq=1 ttl=111 time=84.134 ms
84 bytes from 216.58.208.206 icmp_seq=2 ttl=111 time=85.211 ms
84 bytes from 216.58.208.206 icmp_seq=3 ttl=111 time=80.193 ms
84 bytes from 216.58.208.206 icmp_seq=4 ttl=111 time=88.125 ms
84 bytes from 216.58.208.206 icmp_seq=5 ttl=111 time=80.196 ms
```

Rysunek 4. Polecenie 'ping google.com' wykonane z urządzenia PC2

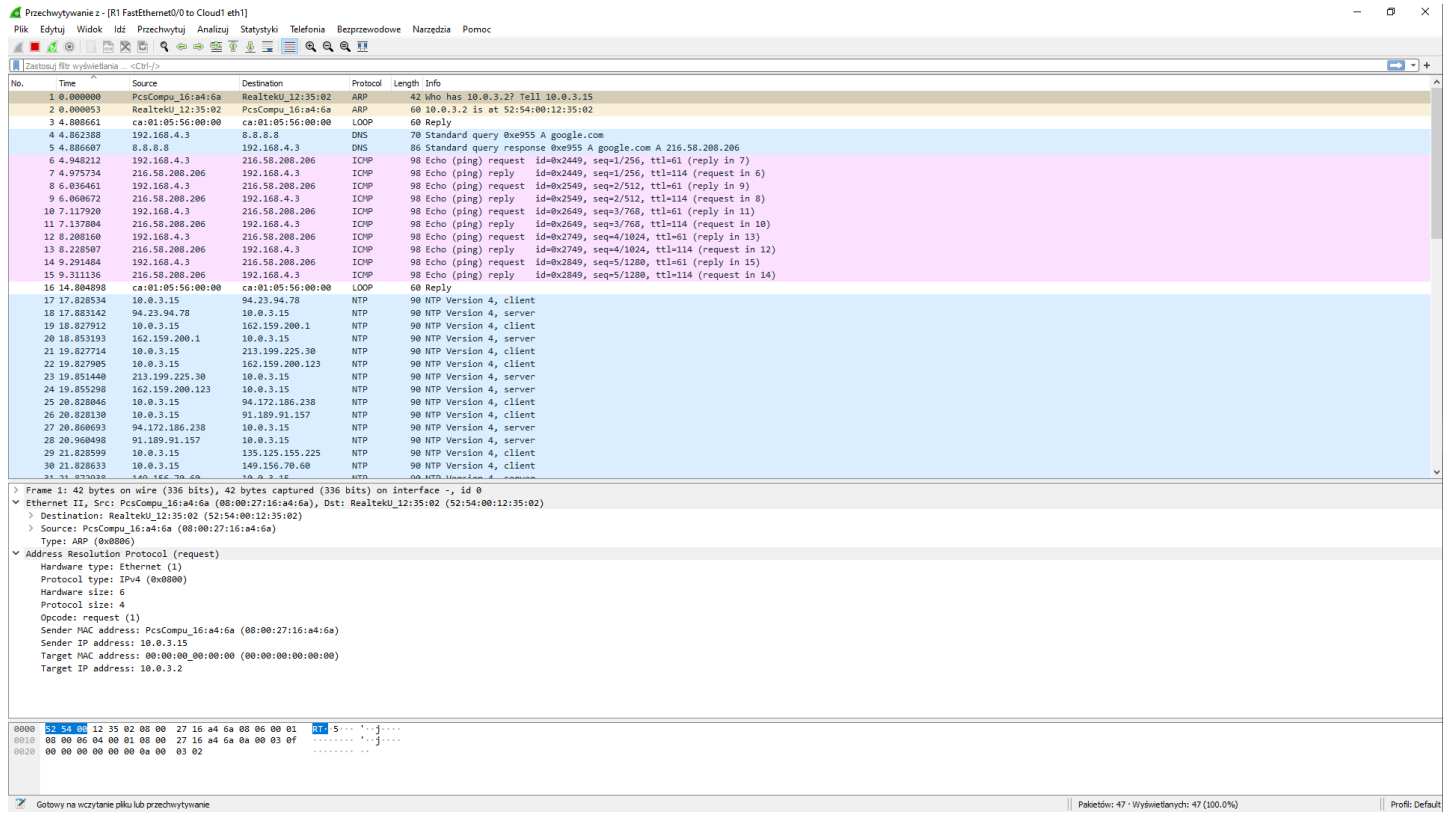
Przechwytywanie i analiza pakietów:

Nasłuchiwanie pakietów należało ustawić na sieciach 192.168.0.0, 192.168.1.0 oraz 192.168.4.0. Jest to zaznaczone na Rysunku 1. za pomocą lupki na danych fragmentach konfiguracji.

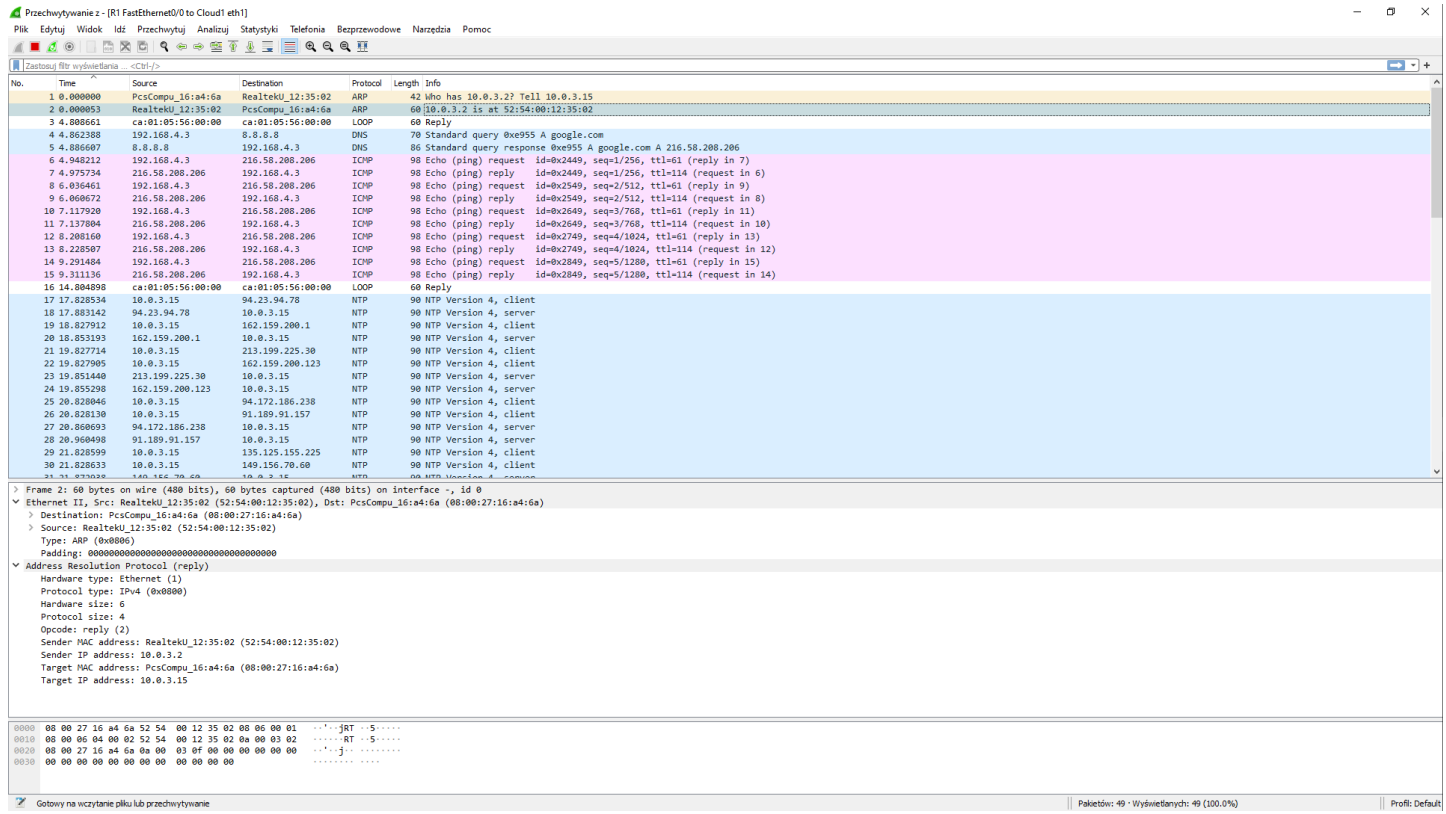
Do przechwytywania i podglądania pakietów został użyty program [wireshark](#).

Analizę pakietów przeprowadzimy w wyniku wydania polecenia `ping google.com` z urządzenia PC2.

Na początku komputer szuka urządzenia, które zostało mu przydzielone jako gateway, w tym celu wysyła zapytanie zgodnie z protokołem ARP. Odpowiada mu router R3 poprzez wysłanie mu swojego adresu MAC.



Rysunek 5. Zapytanie ARP, who has 10.0.3.2? Tell 10.0.3.15.



Rysunek 6. Odpowiedź ARP, 10.0.3.2 is at 52:54:00:12:35:02.

Adres ten jest potem użyty, aby wysłać zapytanie DNS, które pozwoli nam rozpoznać adres [google.com](#).

Rysunek 7. Zapytanie DNS.

Rysunek 8. Odpowiedź DNS.

Po uzyskaniu odpowiedzi z adresem serwera, komputer PC2 zaczyna na niego wysyłać pakiety.

Przechwytywanie z - [R3 FastEthernet4/0 to Switch2 Ethernet1]

Plik Edytuj Widok Idt Przechwyty Analizuj Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc

[Zasobnik filtr wyświetlania <Ctrl-F>]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	ca:03:06:28:00:70	224.0.0.9	CDP	366	Device ID: R3 Port ID: FastEthernet4/0
2	0.604702	192.168.4.1	192.168.4.3	RIPv2	126	Response
3	0.635743	ca:03:06:28:00:70	ca:03:06:28:00:70	LOOP	60	Reply
4	16.639795	192.168.4.3	8.8.8.8	DNS	70	Standard query 0xe955 A google.com
5	16.635442	ca:03:06:28:00:70	ca:03:06:28:00:70	LOOP	60	Reply
6	16.699855	8.8.8.8	192.168.4.3	DNS	86	Standard query response 0xe955 A google.com A 216.58.208.206
7	16.701705	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2449, seq=1/256, ttl=64 (reply in 8)
8	16.705762	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2449, seq=1/256, ttl=111 (request in 7)
9	17.788131	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2549, seq=2/512, ttl=64 (reply in 10)
10	17.873205	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2549, seq=2/512, ttl=111 (request in 9)
11	18.875375	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2649, seq=3/768, ttl=64 (reply in 12)
12	18.955426	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2649, seq=3/768, ttl=111 (request in 11)
13	19.957707	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2749, seq=4/1024, ttl=64 (reply in 14)
14	20.045658	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2749, seq=4/1024, ttl=111 (request in 13)
15	21.048905	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2849, seq=5/1280, ttl=64 (reply in 16)
16	21.128987	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2849, seq=5/1280, ttl=111 (request in 15)
17	26.728345	192.168.4.1	224.0.0.9	RIPv2	126	Response
18	26.631679	ca:03:06:28:00:70	ca:03:06:28:00:70	LOOP	60	Reply
19	36.632054	ca:03:06:28:00:70	ca:03:06:28:00:70	LOOP	60	Reply
20	46.637726	ca:03:06:28:00:70	ca:03:06:28:00:70	LOOP	60	Reply
21	50.154696	ca:04:06:6a:00:70	CDP/VTP/DTP/PagP/UDL	CDP	366	Device ID: R4 Port ID: FastEthernet4/0
22	52.133214	192.168.4.1	224.0.0.9	RIPv2	126	Response
23	56.630296	ca:03:06:28:00:70	ca:03:06:28:00:70	LOOP	60	Reply
24	59.872308	ca:03:06:28:00:70	CDP/VTP/DTP/PagP/UDL	CDP	366	Device ID: R3 Port ID: FastEthernet4/0
25	66.632102	ca:03:06:28:00:70	ca:03:06:28:00:70	LOOP	60	Reply
26	76.640117	ca:03:06:28:00:70	ca:03:06:28:00:70	LOOP	60	Reply
27	80.005540	192.168.4.1	224.0.0.9	RIPv2	126	Response
28	86.629676	ca:03:06:28:00:70	ca:03:06:28:00:70	LOOP	60	Reply
29	96.630864	ca:03:06:28:00:70	ca:03:06:28:00:70	LOOP	60	Reply
30	99.015414	ca:04:06:6a:00:70	CDP/VTP/DTP/PagP/UDL	CDP	366	Device ID: R4 Port ID: FastEthernet4/0
31	106.632230	ca:03:06:28:00:70	ca:03:06:28:00:70	LOOP	60	Reply
32	110.047072	192.168.4.1	224.0.0.9	RIPv2	126	Response
33	116.630163	ca:03:06:28:00:70	ca:03:06:28:00:70	LOOP	60	Reply

Frame 7: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: ca:03:06:28:00:70 (ca:03:06:28:00:70), Dst: ca:03:06:28:00:70 (ca:03:06:28:00:70)
Destination: ca:03:06:28:00:70 (ca:03:06:28:00:70)
Source: Private_66:68:01 (00:50:79:66:68:01)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.4.3, Dst: 216.58.208.206
Internet Control Message Protocol

0000 ca 03 06 28 00 70 00 50 79 66 68 01 00 00 45 00 ... p P yfh...E-
0010 00 54 49 24 00 00 40 01 c3 d0 c0 a8 04 03 d8 3a ... TIS-@:
Gotowy na wczytanie pliku lub przechwytywanie Pakietów: 51 · Wyświetlonych: 51 (100.0%) Profi: Default

Rysunek 9. Przesyłane pakiety między R3 a switchem.

Przechwytywanie z - [R2 FastEthernet1/0 to R1 FastEthernet1/0]

Plik Edytuj Widok Idt Przechwyty Analizuj Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc

[Zasobnik filtr wyświetlania <Ctrl-F>]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	ca:01:05:56:00:1c	ca:01:05:56:00:1c	LOOP	60	Reply
2	0.065858	ca:02:05:c2:00:1c	ca:02:05:c2:00:1c	LOOP	60	Reply
3	9.580554	ca:01:05:56:00:1c	ca:01:05:56:00:1c	LOOP	60	Reply
4	10.031842	192.168.4.3	8.8.8.8	DNS	70	Standard query 0xe955 A google.com
5	10.074872	8.8.8.8	192.168.4.3	DNS	86	Standard query response 0xe955 A google.com A 216.58.208.206
6	10.005541	ca:02:05:c2:00:1c	ca:02:05:c2:00:1c	LOOP	60	Reply
7	10.117661	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2449, seq=1/256, ttl=62 (reply in 8)
8	10.160705	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2449, seq=1/256, ttl=113 (request in 7)
9	10.636636	192.168.1.2	224.0.0.9	RIPv2	106	Response
10	11.205905	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2549, seq=2/512, ttl=62 (reply in 11)
11	11.248967	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2549, seq=2/512, ttl=113 (request in 10)
12	12.207342	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2649, seq=3/768, ttl=62 (reply in 13)
13	12.336300	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2649, seq=3/768, ttl=113 (request in 12)
14	13.377511	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2749, seq=4/1024, ttl=62 (reply in 16)
15	13.388450	192.168.1.1	224.0.0.9	RIPv2	66	Response
16	13.428584	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2749, seq=4/1024, ttl=113 (request in 14)
17	14.460872	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2849, seq=5/1280, ttl=62 (reply in 15)
18	14.503978	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2849, seq=5/1280, ttl=113 (request in 17)
19	19.995875	ca:01:05:56:00:1c	ca:01:05:56:00:1c	LOOP	60	Reply
20	20.091471	ca:02:05:c2:00:1c	ca:02:05:c2:00:1c	LOOP	60	Reply
21	29.996445	ca:01:05:56:00:1c	ca:01:05:56:00:1c	LOOP	60	Reply
22	30.002100	ca:02:05:c2:00:1c	ca:02:05:c2:00:1c	LOOP	60	Reply
23	34.198906	ca:01:05:56:00:1c	CDP/VTP/DTP/PagP/UDL	CDP	366	Device ID: R1 Port ID: FastEthernet1/0
24	38.479369	192.168.1.2	224.0.0.9	RIPv2	106	Response
25	40.002097	ca:01:05:56:00:1c	ca:01:05:56:00:1c	LOOP	60	Reply
26	40.067795	ca:02:05:c2:00:1c	ca:02:05:c2:00:1c	LOOP	60	Reply
27	42.076854	192.168.1.1	224.0.0.9	RIPv2	66	Response
28	49.581104	ca:02:05:c2:00:1c	CDP/VTP/DTP/PagP/UDL	CDP	366	Device ID: R2 Port ID: FastEthernet1/0
29	49.994622	ca:01:05:56:00:1c	ca:01:05:56:00:1c	LOOP	60	Reply
30	50.090165	ca:02:05:c2:00:1c	ca:02:05:c2:00:1c	LOOP	60	Reply
31	59.997284	ca:01:05:56:00:1c	ca:01:05:56:00:1c	LOOP	60	Reply
32	60.003120	ca:02:05:c2:00:1c	ca:02:05:c2:00:1c	LOOP	60	Reply
33	65.161375	192.168.1.2	224.0.0.9	RIPv2	106	Response

Frame 7: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: ca:02:05:c2:00:1c (ca:02:05:c2:00:1c), Dst: ca:01:05:56:00:1c (ca:01:05:56:00:1c)
Destination: ca:01:05:56:00:1c (ca:01:05:56:00:1c)
Source: ca:02:05:c2:00:1c (ca:02:05:c2:00:1c)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.4.3, Dst: 216.58.208.206
Internet Control Message Protocol

0000 ca 01 05 56 00 1c ca 02 05 c2 00 1c 00 00 45 00 ... V-... ..
0010 00 54 49 24 00 00 3e 01 c5 d0 c0 a8 04 03 d8 3a ... TIS->.....
Header length in 32-bit words (p.hdr_len), 1 byte(s) Pakietów: 51 · Wyświetlonych: 51 (100.0%) Profi: Default

Rysunek 10. Przesyłane pakiety między R1 a R2.

Przechwytywanie z - [R1 FastEthernet0/0 to Cloud1 eth1]

Plik Edytuj Widok Idź Przechwytyj Analizuj Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc

Zastosuj filtr wyświetlania -> <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	PcsCompu_16:a4:6a	RealtekU_12:35:02	ARP	42	who has 10.0.3.2? Tell 10.0.3.15
2	0.000053	RealtekU_12:35:02	PcsCompu_16:a4:6a	ARP	60	10.0.3.2 is at 52:54:00:12:35:02
3	4.000661	ca:01:05:56:00:00	ca:01:05:56:00:00	LOOP	60	Reply
4	4.052100	192.168.4.3	8.8.8.8	DNS	70	Standard query 0xe955 A google.com
5	4.896607	8.8.8.8	192.168.4.3	DNS	86	Standard query response 0xe955 A google.com A 216.58.208.206
6	4.948212	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2449, seq=1/256, ttl=61 (reply in 7)
7	4.975734	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2449, seq=1/256, ttl=114 (request in 6)
8	6.036461	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2549, seq=2/512, ttl=61 (reply in 9)
9	6.060072	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2549, seq=2/512, ttl=114 (request in 8)
10	7.117920	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2649, seq=3/768, ttl=61 (reply in 11)
11	7.137804	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2649, seq=3/768, ttl=114 (request in 10)
12	8.208160	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2749, seq=4/1024, ttl=61 (reply in 13)
13	8.228507	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2749, seq=4/1024, ttl=114 (request in 12)
14	9.291484	192.168.4.3	216.58.208.206	ICMP	98	Echo (ping) request id=0x2849, seq=5/1280, ttl=61 (reply in 15)
15	9.311136	216.58.208.206	192.168.4.3	ICMP	98	Echo (ping) reply id=0x2849, seq=5/1280, ttl=114 (request in 14)
16	14.804898	ca:01:05:56:00:00	ca:01:05:56:00:00	LOOP	60	Reply
17	17.828534	10.0.3.15	94.23.94.78	NTP	90	NTP Version 4, client
18	17.835142	94.23.94.78	10.0.3.15	NTP	90	NTP Version 4, server
19	18.827912	10.0.3.15	162.159.200.1	NTP	90	NTP Version 4, client
20	18.853193	162.159.200.1	10.0.3.15	NTP	90	NTP Version 4, server
21	19.827714	10.0.3.15	213.199.225.30	NTP	90	NTP Version 4, client
22	19.827905	10.0.3.15	162.159.200.123	NTP	90	NTP Version 4, client
23	19.851440	213.199.225.30	10.0.3.15	NTP	90	NTP Version 4, server
24	19.855298	162.159.200.123	10.0.3.15	NTP	90	NTP Version 4, server
25	20.828046	10.0.3.15	94.172.186.238	NTP	90	NTP Version 4, client
26	20.828130	10.0.3.15	91.189.91.157	NTP	90	NTP Version 4, client
27	20.868693	94.172.186.238	10.0.3.15	NTP	90	NTP Version 4, server
28	20.968498	91.189.91.157	10.0.3.15	NTP	90	NTP Version 4, server
29	21.828599	10.0.3.15	135.125.155.225	NTP	90	NTP Version 4, client
30	21.828633	10.0.3.15	149.156.70.60	NTP	90	NTP Version 4, client
31	31.873030	149.156.70.60	10.0.3.15	NTP	90	NTP Version 4, server

> Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
 > Ethernet II, Src: ca:01:05:56:00:00 (ca:01:05:56:00:00), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 > Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
 > Source: ca:01:05:56:00:00 (ca:01:05:56:00:00)
 > Type: IPv4 (0x0008)
 > Internet Control Message Protocol

Gotowy na wczytanie pliku lub przechwytywanie

Pakietów: 54 · Wyświetlonych: 54 (100.0%)

Profil: Default

Rysunek 11. Przesyłane pakiety między Cloudem a R1.

Na czerwono można zobaczyć jak zmienia się destination i source każdego pakietu ICMP dla danej podsięci. Zaczynając przesyłanie pakietów, PC2 musi je wszystkie przesłać przez router R3. W nim ramki są przepakowywane na nowy destination i source. Nowym sourcem zostaje R3, a destination to następny router na drodze do Clouda. Na ostatnim odcinku (między R1 a Cloudem) można zauważyć, że destination to RealtekU, czyli karta sieciowa ethernet. Potem pakiety idą do danego adresu serwera.