

# Technologie sieciowe 4

Gabriel Wechta

28.05.2020

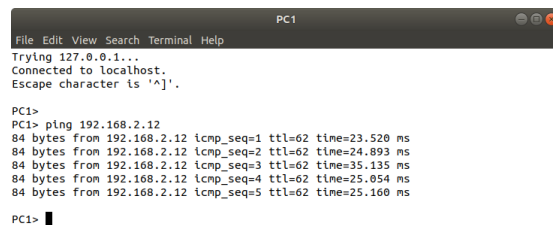
## 1 Konfiguracja

Z zewnętrzną, fizyczną siecią Cloud jestem połączony za pomocą portu vibr0.

IOS routera udało mi się znaleźć w internecie. Symuluje ono zachowanie routera Cisco z serii 7200. Konfiguracja wszystkich routerów była podobna, z wyjątkiem routera R5, który miał uzyskiwać dynamiczny adres IP z Cloud. Używa do tego protokołu DHCP. Wszystkie pozostałe urządzenia mają statyczne adresy w swoich sieciach. Oraz DNS szukają po portach, które prowadzą do R5, który zaś szuka ich pod 8.8.8.8.

W zasadzie konfigurację przeprowadziłem identycznie jak dr hab. Krzywiecki na wykładzie. Aby nie mylić się w adresach IP lokalnej sieci, przyjąłem standard, że dla router, IP portu to 192.168.(network).(id router) dla PC to 192.168.(network).(id PC + 10).

Przykłady ping, poniżej:



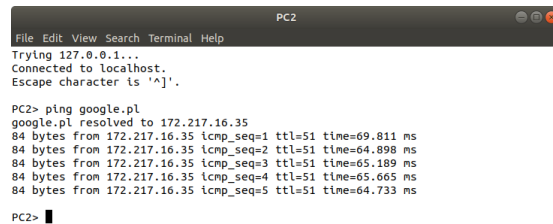
```
PC1
File Edit View Search Terminal Help
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^['.

PC1> ping 192.168.2.12
PC1> ping 192.168.2.12
84 bytes from 192.168.2.12 icmp_seq=1 ttl=62 time=23.520 ms
84 bytes from 192.168.2.12 icmp_seq=2 ttl=62 time=24.893 ms
84 bytes from 192.168.2.12 icmp_seq=3 ttl=62 time=35.135 ms
84 bytes from 192.168.2.12 icmp_seq=4 ttl=62 time=25.054 ms
84 bytes from 192.168.2.12 icmp_seq=5 ttl=62 time=25.160 ms

PC1> █
```

Rysunek 1: Ping z PC1 do PC2 (przykładowo)

oraz:



```
File Edit View Search Terminal Help
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

PC2> ping google.pl
google.pl resolved to 172.217.16.35
84 bytes from 172.217.16.35 icmp_seq=1 ttl=51 time=69.811 ms
84 bytes from 172.217.16.35 icmp_seq=2 ttl=51 time=64.898 ms
84 bytes from 172.217.16.35 icmp_seq=3 ttl=51 time=65.189 ms
84 bytes from 172.217.16.35 icmp_seq=4 ttl=51 time=65.665 ms
84 bytes from 172.217.16.35 icmp_seq=5 ttl=51 time=64.733 ms

PC2> █
```

Rysunek 2: Ping z PC2 do google.pl

## 2 Przechwytywanie komunikatów

Mamy ustawić przechwytywanie komunikatów na sieciach 192.168.0.0, 192.168.2.0, 192.168.3.0.

Na szczęście GNS3 bardzo elegancko współpracuje z Wiresharkiem. Poprzez kliknięcie na wybrane połączenie prawym przyciskiem myszy, możemy otworzyć Wiresharka z włączonym nasłuchiwaniami na właśnie tym połączeniu.

## 3 Analiza

Polecenie 'ping' otrzymuje parametr 'google.pl', tym samym potrzebuje użyć protokołów ARP oraz DNS, aby otrzymać odpowiedni adres IP. Propagacja zapytania kontynuuje na 192.168.3.0 i 192.168.0.0, a następnie wraca, co widać na załączonych obrazkach. Jak widzimy na rysunku 3, pole 'destination' ma wartość 8.8.8.8, natomiast adres, na który mamy wysłać ICMP to 216.58.209.3.

Rozpoczynamy wysyłanie. Wszystkie pakiety, jak widać trafiły i wróciły. Wireshark pozwala nam zobaczyć, że wszystkie pakiety opuszczając PC2 mają wartość ttl równą 64 (rysunek 3). Natomiast już na 192.168.3.0 (rysunek 4) ttl ma wartość o 2 mniejszą, R2 i R6 "zabrały" po jednym "życiu". Zmiana wartości ttl w ICMP 'reply' zachowuje się tak samo.

Ponadto możemy zaobserwować, że podczas nasłuchiwania pojawiły się również pakiety protokołów STP, RIPv2, CDP i LOOP. Są to protokoły, których używają routery do konfiguracji. Trzy ostatnie są wspólne dla wszystkich routerów, zaś STP jest potrzebny R5 jako, że jest podłączony do sieci Cloud.

Efekty dla 'ping google.pl' z PC2:

File

Edit

View

Go

Capture

Analyze

Statistics

Telephony

Wireless

Tools

Help

Apply a display filter

->Ctrl+F

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
6	24.041258	ca:03:44:e3:00:1c	Private, 66:00:01	ARP	60	192.168.2.2 is at ca:03:44:e3:00:1c
7	24.942007	192.168.2.12	8.8.8.8	DNS	60	Standard query 0xcfe5 A google.pl
8	24.121037	8.8.8.8	192.168.2.12	DNS	80	Standard query response 0xcfe5 A google.pl A 216.58.209.3
9	24.122304	192.168.2.12	216.58.209.3	ICMP	98	Echo (ping) request id=0x0095, seq=1/256, ttl=64 (reply in 18)
10	24.121977	216.58.209.3	192.168.2.12	ICMP	98	Echo (ping) reply id=0x0095, seq=1/256, ttl=64 (request in 9)
11	25.182456	192.168.2.12	216.58.209.3	ICMP	98	Echo (ping) request id=0x0195, seq=2/512, ttl=64 (reply in 12)
12	25.147700	216.58.209.3	192.168.2.12	ICMP	98	Echo (ping) reply id=0x0195, seq=2/512, ttl=64 (request in 11)
13	26.248684	192.168.2.12	216.58.209.3	ICMP	98	Echo (ping) request id=0x0295, seq=3/768, ttl=64 (reply in 14)
14	26.324283	216.58.209.3	192.168.2.12	ICMP	98	Echo (ping) reply id=0x0295, seq=3/768, ttl=64 (request in 13)
15	27.224816	192.168.2.12	216.58.209.3	ICMP	98	Echo (ping) request id=0x0395, seq=4/1024, ttl=64 (reply in 17)
16	27.380846	ca:03:44:e3:00:1c	CDP/VTP/PAgP/UD...	CDP	340	Device ID: R2 Port ID: FastEthernet1/0
17	27.390121	216.58.209.3	192.168.2.12	ICMP	98	Echo (ping) reply id=0x0395, seq=4/1024, ttl=64 (request in 15)
18	28.391255	192.168.2.12	216.58.209.3	ICMP	98	Echo (ping) request id=0x0495, seq=5/1280, ttl=64 (reply in 19)
19	28.460337	216.58.209.3	192.168.2.12	ICMP	98	Echo (ping) reply id=0x0495, seq=5/1280, ttl=64 (request in 18)
20	30.060519	ca:03:44:e3:00:1c	ca:03:44:e3:00:1c	LOOP	60	Recv.

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Ethernet II, Src: ca:03:44:e3:00:1c (ca:03:44:e3:00:1c), Dst: ca:03:44:e3:00:1c (ca:03:44:e3:00:1c)

Configuration Test Protocol (loopback)

Data (40 bytes)

0000

ca 03 44 e3 00 1c

ca 03 44 e3 00 1c

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

0010

01 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

0020

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

0030

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

00 00 00 00 00 00

Ready to load or capture

Packets 34 - Displayed: 34 (100.0%)

Profile: Default

Rysunek 3: 192.168.2.0

Rysunek 4: 192.168.3.0

Capturing from Standard Input [85 FastEthernet0/0 to Cloud1 vif0r0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl>F Expression...

No.	Time	Source	Destination	Protocol	Length	Info
34	43.445948	192.168.122.112	8.8.8.8	DNS	60	Standard query 8x6f5 A google.pl
35	43.479584	8.8.8.8	192.168.122.112	DNS	85	Standard query response 8x6f5 A google.pl A 216.58.209.3
36	43.548338	192.168.122.112	216.58.209.3	ICMP	96	Echo (ping) request id=8x0895, seq=1/256, ttl=61 (reply in 37)
37	43.545925	216.58.209.3	192.168.122.112	ICMP	96	Echo (ping) reply id=8x0895, seq=1/256, ttl=54 (request in 36)
38	44.000000	8.8.8.8	192.168.122.112	DNS	52	Standard query 11201 A google.pl
39	44.571972	192.168.122.112	216.58.209.3	ICMP	96	Echo (ping) request id=8x0195, seq=2/512, ttl=61 (reply in 40)
40	44.602080	216.58.209.3	192.168.122.112	ICMP	96	Echo (ping) reply id=8x0195, seq=2/512, ttl=54 (request in 39)
41	45.637758	192.168.122.112	216.58.209.3	ICMP	96	Echo (ping) request id=8x0295, seq=3/768, ttl=61 (reply in 42)
42	45.679174	216.58.209.3	192.168.122.112	ICMP	96	Echo (ping) reply id=8x0295, seq=3/768, ttl=54 (request in 41)
43	46.000000	8.8.8.8	192.168.122.112	DNS	52	Standard query 11201 A google.pl
44	46.713681	192.168.122.112	216.58.209.3	ICMP	96	Echo (ping) request id=8x0395, seq=4/1024, ttl=61 (reply in 45)
45	46.744292	216.58.209.3	192.168.122.112	ICMP	96	Echo (ping) reply id=8x0395, seq=4/1024, ttl=54 (request in 44)
46	47.792071	192.168.122.112	216.58.209.3	ICMP	96	Echo (ping) request id=8x0495, seq=5/1280, ttl=61 (reply in 47)
47	47.822668	216.58.209.3	192.168.122.112	ICMP	96	Echo (ping) reply id=8x0495, seq=5/1280, ttl=54 (request in 46)

Frame 1: 52 bytes on wire (416 bits), 52 bytes captured (416 bits) on interface 0

- Ethernet II, Src: Intel E1000 (82:55:08:00:20:00), Dst: Virtual (08:00:27:00:00:00)
- Logical Link Control
- Spanning Tree Protocol

```

0000  01 00 02 00 00 00 02 49 20 72 7c 48 00 20 42 42  ....b...rIF 488
0010  03 00 00 00 00 00 00 00 52 54 00 79 de c5 00 00  ....RT.y....
0020  00 00 00 00 52 54 00 79 de c5 00 82 00 00 14 00  ....RT.y....
0030  02 00 02 00

```

Ready to load or capture Packets: 142 - Displayed: 142 (100.0%) Profile: Default

Rysunek 5: 192.168.0.0