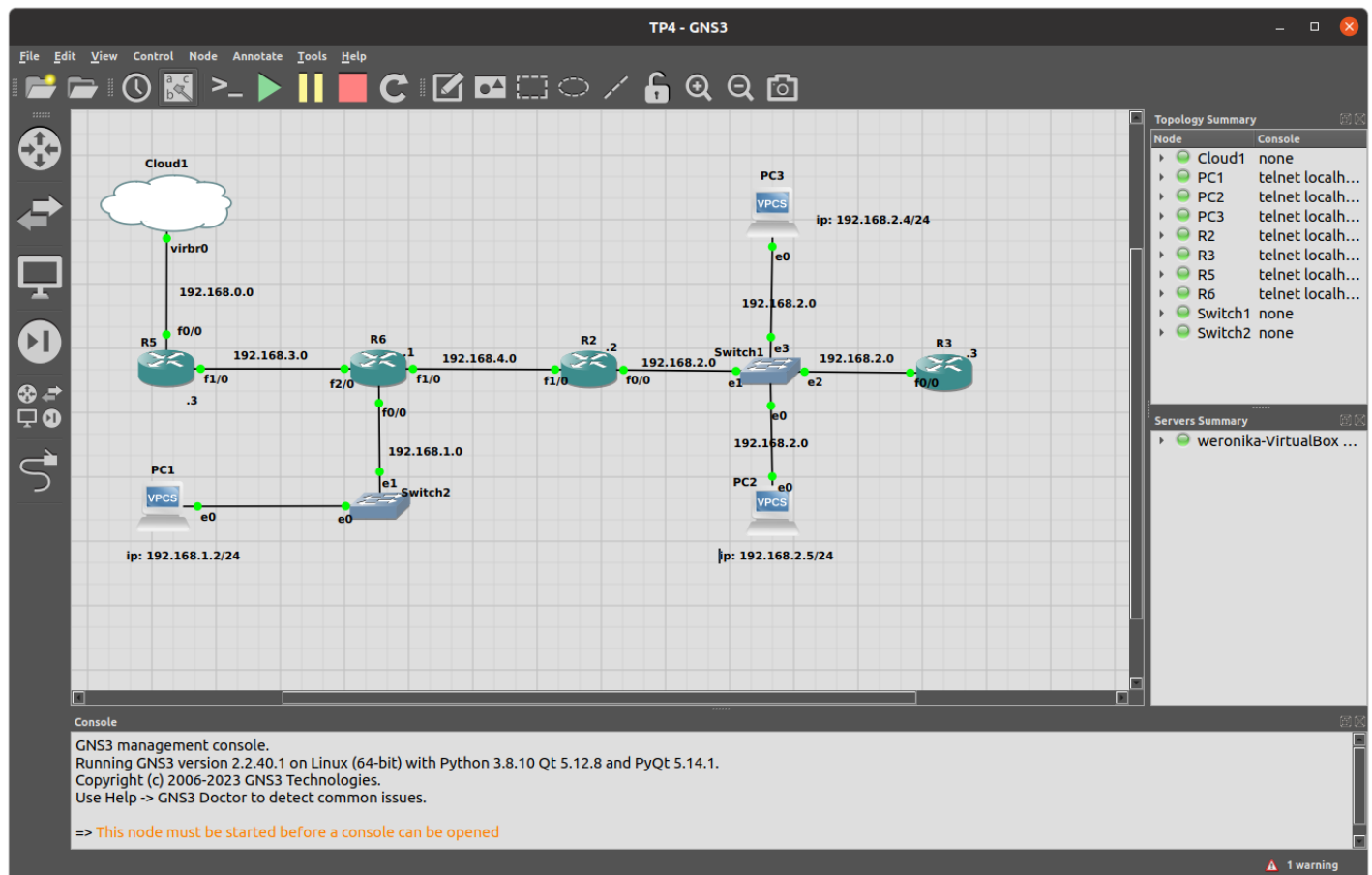


# Sprawozdanie

## Lista 4

Sieć w GNS3 z użyciem routera c7200:



Połączone z siecią zewn. Cloud, przez którą router R5 ma ustalony dynamiczny adres IP z użyciem technologii dhcp (po stworzeniu było to 192.168.122.113). Pozostałe routery mają ustawione stałe adresy.

Skonfigurowano wszystkie routery i Vpcs:

R5	R6	R2	R3
//ustaiwa polaczenie do cloda configure terminal interface FastEthernet 0/0 ip address dhcp ip nat outside no shutdown end	conf t int fa2/0 no shut ip address 192.168.3.1 255.255.255.0 end	conf t int fa1/0 ip address 192.168.4.2 255.255.255.0 no shut end conf t	conf t int fa0/0 ip address 192.168.2.3 255.255.255.0 no shut end
//uzywaj odpowiedni dns configure terminal ip domain-lookup ip name-server 8.8.8.8 end	conf t ip domain-lookup source-interface fa2/0 ip name-server 8.8.8.8 end	ip address 192.168.2.2 255.255.255.0 no shut end	conf t router rip version 2 no auto-summary network 192.168.2.0 end
configure terminal interface FastEthernet 1/0 ip address 192.168.3.3 255.255.255.0 ip nat inside no shutdown end	//dolne conf t int fa0/0 no shut ip address 192.168.1.1 255.255.255.0 end	conf t ip domain-lookup ip name-server 8.8.8.8 end	conf t ip domain-lookup ip name-server 192.168.0.1 end
configure terminal router rip version 2 //indyw. trasy dla sieci no auto-summary network 192.168.0.0 network 192.168.3.0 default-information originate end	//prawe conf t int fa1/0 no shut ip address 192.168.4.1 255.255.255.0 end	conf t router rip version 2 no auto-summary network 192.168.4.0 network 192.168.2.0 end	wr
write			
PC1	PC2	PC3	
ip 192.168.1.2/24 192.168.1.1 ip dns: 8.8.8.8 write	ip 192.168.2.5/24 192.168.2.2 ip dns: 8.8.8.8 write	ip 192.168.2.4/24 192.168.2.2 ip dns: 8.8.8.8 write	

ip domain-lookup – enables DNS-based address translation

ip name-server – (to supply name information for DNS) specyfikuje wszystkie adresy, które mogą funkcjonować jako nazwy serwera

router rip – służy do przejścia do konfiguracji RIP (Routing Information Protocol)

The Routing Information Protocol (RIP) is a distance-vector, interior gateway (IGP) routing protocol used by routers to exchange routing information. RIP uses the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. RIP version 2 (RIPv2) was developed due to the deficiencies of the original RIP.

network – is used to specify the directly connected subnets on the router to be configured and that are intended to be included in the routing updates

shutdown – enable/disable an interface

default information originate – when there is not a route to a specific network in the routing table the router will use the default-information

overload – it enables the whole network to access the Internet using one single real IP address

Internet Control Message Protocol (ICMP) is a network layer protocol used to diagnose communication errors by performing an error control mechanism.

**DNS** to protokół, usługa, zamieniająca **nazwy domenowe**, zrozumiałe dla człowieka na **adresy IP** urządzeń w sieci.

The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.

Address Resolution Protocol (ARP) – protokół sieciowy umożliwiający mapowanie logicznych adresów warstwy sieciowej na fizyczne adresy warstwy łącza danych.

## Użycie ping:

PC2 na zewnętrzny adres (google.com, interia.pl) oraz z innym urządzeniem (PC3)

```
PC2> ping google.com
google.com resolved to 216.58.215.78

84 bytes from 216.58.215.78 icmp_seq=1 ttl=113 time=80.719 ms
84 bytes from 216.58.215.78 icmp_seq=2 ttl=113 time=46.326 ms
84 bytes from 216.58.215.78 icmp_seq=3 ttl=113 time=48.905 ms
84 bytes from 216.58.215.78 icmp_seq=4 ttl=113 time=48.865 ms
84 bytes from 216.58.215.78 icmp_seq=5 ttl=113 time=51.077 ms

PC2> ping interia.pl
interia.pl resolved to 217.74.75.90

84 bytes from 217.74.75.90 icmp_seq=1 ttl=54 time=61.154 ms
84 bytes from 217.74.75.90 icmp_seq=2 ttl=54 time=49.537 ms
84 bytes from 217.74.75.90 icmp_seq=3 ttl=54 time=91.496 ms
84 bytes from 217.74.75.90 icmp_seq=4 ttl=54 time=101.996 ms
84 bytes from 217.74.75.90 icmp_seq=5 ttl=54 time=44.442 ms

PC2> ping 192.168.2.4

84 bytes from 192.168.2.4 icmp_seq=1 ttl=64 time=0.399 ms
84 bytes from 192.168.2.4 icmp_seq=2 ttl=64 time=0.947 ms
84 bytes from 192.168.2.4 icmp_seq=3 ttl=64 time=0.487 ms
84 bytes from 192.168.2.4 icmp_seq=4 ttl=64 time=0.574 ms
84 bytes from 192.168.2.4 icmp_seq=5 ttl=64 time=0.660 ms

PC2> 
```

R6 (router) z R3, PC2, PC1, zewnętrznymi adresami (google.com interia.pl)

```
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 = 40/44/48 ms
R6#
R6#ping 192.168.2.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.5, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/45/52 ms
R6#
R6#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/34/40 ms
R6#
R6#ping google.com
Translating "google.com"...domain server (8.8.8.8) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 216.58.215.78, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/44/48 ms
R6#
R6#ping interia.pl
Translating "interia.pl"...domain server (8.8.8.8) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 217.74.72.58, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/45/52 ms
R6#
```

Obserwacja sieci 192.168.0.0 (lewo góra), 192.168.2.0 (lewo sam dół lub prawo góra), 192.168.3.0 (lewo niżej/środek)

Po uruchomieniu ping google.com na PC1 (192.168.1.2) widać, że sygnał przechodzi przez sieci na jego trasie - tutaj – 192.168.0.0 i 192.168.0.3.

Można zauważyć, że najpierw sygnał jest przesyłany od PC1 do 8.8.8.8 (dns udostępniany przez Google) i spowrotem. Ale po przejściu przez R5 zmienia się źródło na adres ustalony mu przez Cloud-a. Było to zapytanie DNS o przetłumaczenie adresu strony i odpowiedź.

Pojawiają się też powtarzające komunikaty Echo request i echo reply w protokole ICMP – odpowiadają ilości pingów od urządzenia

The screenshot displays a GNS3 network simulation with three main windows showing packet captures:

- Przechwytywanie z [R5 FastEthernet0/0 to Cloud1 vlab0]**: Shows DNS queries to 8.8.8.8 and ICMP echo requests/replies.
- Przechwytywanie z [R5 FastEthernet1/0 to R6 FastEthernet2/0]**: Shows ICMP echo requests/replies between R5 and R6.
- Przechwytywanie z [R2 FastEthernet0/0 to Switch1 Ethernet1]**: Shows ICMP echo requests/replies between R2 and Switch1.

On the right, a terminal window for PC1 shows the command 'ping google.com' and the output, including the IP address resolved (216.58.215.78) and the sequence of ICMP echo requests and replies with their respective times.

Przy wykorzystaniu PC2 (192.168.2.5) sygnał przechodzi już przez wszystkie sieci. Największe wartości czasu komunikatów pojawiają się dla dalszych sieci

This screenshot shows a more extensive network simulation with traffic capture on multiple devices:

- [R5 FastEthernet0/0 to Cloud1 vlab0]**: Shows DNS queries and ICMP echo requests/replies.
- [R2 FastEthernet0/0 to Switch1 Ethernet1]**: Shows ICMP echo requests/replies.
- [R5 FastEthernet1/0 to R6 FastEthernet2/0]**: Shows ICMP echo requests/replies.

On the right, a terminal window for PC2 shows the command 'ping google.com -t' and the output, displaying a continuous stream of ICMP echo requests and replies with their respective times, indicating a continuous ping operation.

Router R5 – podpięty do Clouda otrzymał zapytania ARP z zapytaniem o przynależność IP

Three screenshots of Wireshark network traffic analysis:

- Top Left:** Filter: `arp or dns or icmp`. Shows traffic between 192.168.122.113 and 8.8.8.8. Includes DNS queries and ICMP Echo (ping) requests/replies.
- Top Right:** Filter: `ns or icmp`. Shows traffic between 192.168.2.5 and 142.250.203.142. Includes DNS queries and ICMP Echo (ping) requests/replies.
- Bottom:** Filter: `arp or dns or icmp`. Shows traffic between 192.168.1.2 and 8.8.8.8. Includes DNS queries and ICMP Echo (ping) requests/replies. The packet list shows a frame with 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -.

Packet details for the selected packet (Frame 206):

- Frame 206: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
- Ethernet II, Src: ca:06:12:5f:00:38 (ca:06:12:5f:00:38), Dst: ca:05:12:40:00:1c (ca:05:12:40:00:1c)
- Internet Protocol Version 4, Src: 192.168.2.5, Dst: 142.250.203.142
- Internet Control Message Protocol

Packet bytes (hex):

```
0000 ca 05 12 40 00 1c ca 06 12 5f 00 38 00 00 45 00 ..@....8..E-
0010 00 54 73 fb 00 00 20 01 0b 77 00 00 00 00 00 00 ..T.....
```

Na podstawie obserwacji wartości ttl można było zauważyć zmianę wartości dla różnych sieci. Większa wartość dla „bliskiej” sieci 0.2. Dla odpowiedzi większa wartość była dla sieci połączonej z cloudem. Zmiana ttl ma sens zważywszy na konieczność przejścia przez następne routery