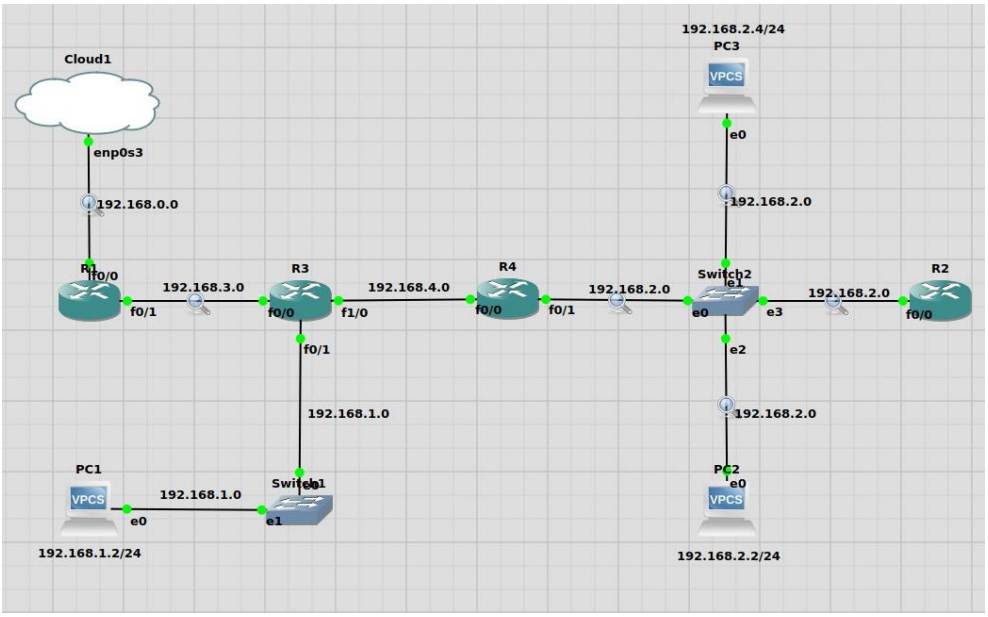
29.05.2020

Lista 4

Technologie sieciowe

Dominika Szydło

Celem listy 4 było utworzenie w programie GNS3 sieci o zadanej topologii i własnościach. Ilustracja poniżej przedstawia sieć, którą udało mi się stworzyć kierując się wskazówkami z wykładu.



Screenshot 1. Topologia sieci

Sieć wirtualna jest połączona z zewnętrzną siecią „Cloud" przez router R1. Uzyskuje on dynamiczny adres IP za pomocą protokołu DHCP, co można ustawić za pomocą polecenia „ip address dhcp" w konfiguracji routera. Adresy IP pozostałych urządzeń ustawiłam ręcznie na wartości zaznaczone na projekcie. W sieci można wysyłać ping na inne urządzenia jak i na zewnętrzne adresy.

```
conf t
int f0/0
ip address dhcp
ip nat outside
no shut
end

conf t
ip domain-lookup
ip name-server 8.8.8.8
end

conf t
int f0/1
ip add 192.168.3.3 255.255.255.0
ip nat inside
no shut
end

conf t
router rip
version 2
no auto-summary
network 192.168.0.0
network 192.168.3.0
default-information originate
end

conf t
access-list 10 permit 192.168.1.0 0.0.254.255
access-list 10 permit 192.168.2.0 0.0.253.255
access-list 10 permit 192.168.3.0 0.0.252.255
access-list 10 permit 192.168.4.0 0.0.251.255
ip nat inside source list 10 interface f0/0 overload
end
write
```

Screenshot 2. Przykładowa konfiguracja routera (R1)

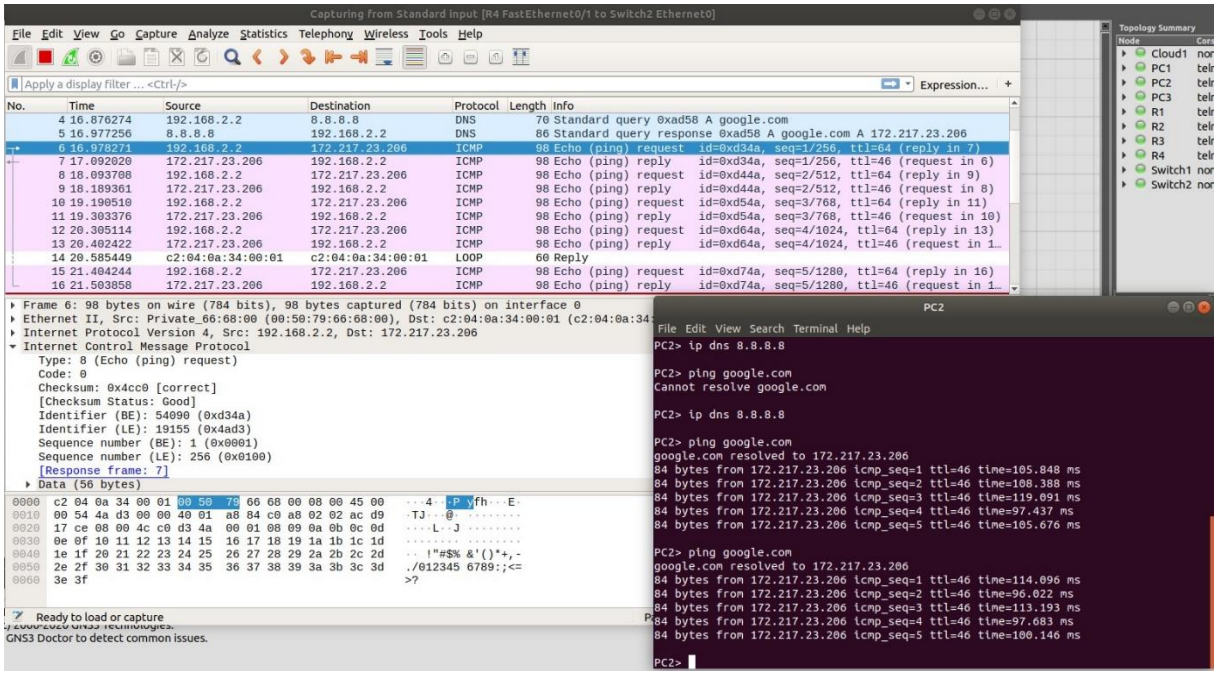
```
PC2> ping 192.168.4.1
84 bytes from 192.168.4.1 icmp_seq=1 ttl=254 time=15.704 ms
84 bytes from 192.168.4.1 icmp_seq=2 ttl=254 time=12.536 ms
84 bytes from 192.168.4.1 icmp_seq=3 ttl=254 time=29.841 ms
84 bytes from 192.168.4.1 icmp_seq=4 ttl=254 time=25.237 ms
84 bytes from 192.168.4.1 icmp_seq=5 ttl=254 time=26.577 ms

PC2> ping 192.168.1.2/24
84 bytes from 192.168.1.2 icmp_seq=1 ttl=62 time=32.547 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=62 time=32.198 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=62 time=40.792 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=62 time=40.601 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=62 time=39.856 ms
```

Screenshot 3. Pingowanie innych urządzeń w sieci z PC2

```
PC2> ping cs.pwr.edu.pl
cs.pwr.edu.pl resolved to 156.17.7.22
84 bytes from 156.17.7.22 icmp_seq=1 ttl=51 time=86.229 ms
84 bytes from 156.17.7.22 icmp_seq=2 ttl=51 time=76.433 ms
84 bytes from 156.17.7.22 icmp_seq=3 ttl=51 time=93.996 ms
84 bytes from 156.17.7.22 icmp_seq=4 ttl=51 time=101.890 ms
84 bytes from 156.17.7.22 icmp_seq=5 ttl=51 time=89.056 ms
```

Screenshot 4. Pingowanie zewnętrznego adresu

Przechwytywanie pakietów w sieci odbywa się za pomocą Wiresharka. Aby rozpocząć podsłuchiwanie wystarczy kliknąć na wybrane połączenie i wybrać opcję przechwytywania. Podsłuchiwane połączenia są zaznaczone lupą w projekcie. Oto co przechwycił Wireshark po pingowaniu strony google.com z PC2.



Screenshot 5. Okno Wiresharka podczas nasłuchiwania sieci

Widać pakiety, które wysłał lub otrzymał PC2 realizując dwa protokoły, z których korzysta ping – DNS i ICMP. Najpierw na adres 8.8.8.8 (serwer DNS udostępniany przez Google) z PC2 (192.168.2.2) zostało wysłane zapytanie o przetłumaczenie adresu google.com na adres IP, a z serwera odpowiedź -

172.217.23.206. Następnie na otrzymany adres PC2 wysłał (pięciokrotnie) komunikat ICMP Echo Request, a google.com odpowiedziało na niego komunikatem ICMP Echo Reply. Można również wyświetlić parametry tych komunikatów, gdzie zobaczymy, że sumy kontrolne się zgadzają, a więc wiadomość dotarła poprawnie.