

Album Album

Album Album

1. Konfiguracja IP w systemach MS Windows

Odczytaj konfigurację oraz zidentyfikuj adresy IP i MAC karty eth0 poleceniem

```
ipconfig /all
```

Wyłącz dynamicznie przydzieloną konfigurację.

```
ipconfig /release
```

Pobierz ponownie konfigurację z serwera DHCP.

```
ipconfig /renew
```

Na jaki przedział czasu serwer DHCP przydziela konfigurację?

1.1. Ręczna konfiguracja ustawień sieciowych (192.168.g.k/24; brama 192.168.g.254)

Ustaw adres IP, maskę sieci i bramę.

```
netsh .....
```

Ustaw podstawowy i zapasowy serwer DNS (153.19.48.1, 153.19.250.100)

```
netsh ..... set .....
```

```
netsh ..... add .....
```

Odczytaj konfigurację

```
ipconfig /all
```

Odczytaj tablicę routingu

```
route print
```

Sprawdź działanie łączności z pozostałymi członkami grupy poleceniem ping.

```
ping 192.168.g.k1
```

```
ping 192.168.g.k2
```

Sprawdź dostęp do Internetu

```
ping wp.pl
```

Przywróć konfigurację automatyczną przydzielaną przez serwer DHCP

```
netsh ..... address .....
```

```
netsh ..... dns .....
```

TU PREZENTUJEMY KONFIGURACJĘ PROWADZĄCEMU (ipconfig /all)

2. Konfiguracja IP w systemach Linux

Uwaga: Konfigurację systemów Linux przeprowadzamy używając dystrybucji LiveCD.

Sprawdź konfigurację interfejsów sieciowych.

```
ifconfig
```

Zapamiętaj nazwę interfejsu, do którego przypisany jest adres 10.1.1.k. Tej nazwy należy używać w dalszych poleceniach w miejsce eth0.

Sprawdź wpisy w tablicy routingu.

```
route
```

Sprawdź konfigurację przypisaną przez klienta usługi DHCP.

```
cat /var/lib/NetworkManager/dhclient*.lease
```

Wyłącz klienta usługi DHCP i usuń przypisaną konfigurację.

```
killall NetworkManager
```

```
killall dhclient
```

```
ip addr flush dev eth0
```

```
rm -f /etc/resolv.conf
```

2.1. Ręczna konfiguracja interfejsów (192.168.g.k/24)

```
ifconfig .....
```

Sprawdź łączność z pozostałymi członkami grupy poleceniem ping.

```
ping 192.168.g.k1
```

```
ping 192.168.g.k2
```

itd.

Sprawdź wpisy tablicy sąsiedztwa protokołu ARP.

```
arp
```

Ile różnych typów (producentów) kart sieciowych jest używanych w grupie?

Sprawdź łączność z Internetem.

```
ping wp.pl
```

Błąd: Nieznany host - nie jest jeszcze skonfigurowany adres serwera usługi DNS. Wykonaj kolejną próbę postępując się adresem IP.

```
ping 212.77.100.101
```

Błąd: Nie jest jeszcze skonfigurowany routing.

2.2. Ręczna konfiguracja routingu (brama 192.168.g.254)

Sprawdź łączność z bramą.

ping 192.168.g.254

Ustaw domyślną bramę (uwaga: proszę użyć składni ze słowem default)

route

Czytając numerycznie tablicę routing **route -n** można zauważyć, że domyślna brama to brama do sieci 0.0.0.0 przy masce 0.0.0.0

Poprawna jest zatem też składnia:

route add -net 0.0.0.0 netmask 0.0.0.0 gw 192.168.g.254

Sprawdź łączność ze światem:

ping 212.77.100.101

2.3. Konfiguracja DNSów

Adresy serwerów DNS są przechowywane w pliku konfiguracyjnym /etc/resolv.conf w kolejnych liniach poprzedzone napisem nameserver

np. nameserver 153.19.48.1

Przed konfiguracją proszę sprawdzić, który z poniższych DNSów odpowiada najszybciej i wybrać go jako podstawowy (pierwszy w pliku):

10.1.0.1

153.19.250.100

8.8.8.8

Przykład:

time nslookup wp.pl 10.1.0.1

Który z serwerów DNS odpowiada najszybciej?

2.4. Wpływ awarii podstawowego serwera DNS na szybkość pracy Internetu

1. Otwórz dowolny portal w przeglądarce obserwując szybkość ładowania strony

np. onet.pl, wp.pl albo interia.pl.

2. Zasymuluj awarię podstawowego serwera DNS poprzez zmianę pierwszego wpisu nameserver w pliku /etc/resolv.conf np. na nameserver 153.19.48.173. Drugi wpis w pliku powinien wskazywać na sprawny zapasowy serwer DNS.

3. Ponownie otwórz stronę z pkt.1 obserwując szybkość ładowania strony

Jaki jest przybliżony czas pełnego załadowania strony np. wp.pl?

Uwaga: Tu może być potrzebna cierpliwość.

4. Napraw konfigurację DNS i sprawdź poprawność działania sieci.

2.5. Konfiguracja interfejsu za pomocą pakietu ip (10.1.1.k/16)

~~**ip link set eth0 down**~~

ip addr flush eth0

ip addr

~~**ip link set eth0 up**~~

Tu warto porównać wynik działania polecenia ifconfig i jeżeli nie wszystkie parametry (adres, maska, broadcast) konfiguracji są poprawne to powtórz poprawnie konfigurację interfejsu poleceniem ip.

Sprawdź łączność z pozostałymi członkami grupy i odczytaj wpisy w tablicy arp

ip neigh show

Ustaw konfigurację domyślnej bramy na adres 10.1.0.1.

ip route

ip route show

Sprawdź poprawność działania sieci.

2.6. Trasy datagramów

traceroute wp.pl

W jakim mieście są najprawdopodobniej zlokalizowane serwery portalu www.onet.pl?

traceroute www.onet.pl

Jakie jest opóźnienie traktu transatlantyckiego na trasie do serwera microsoft.com?

Podpowiedź: obserwując trasę widać wyraźny wzrost czasu odpowiedzi kolejnych routerów.

traceroute microsoft.com

Interesujące może być też prześledzenie trasy na wschód np. do Japonii. Można wypróbować adres www.metro.tokyo.jp

traceroute www.metro.tokyo.jp

2.7. ICMP Redirect

Zmień bramę domyślną na 10.1.0.208

ip route del default

ip route

ip route show

W konfiguracji sytemu nigdzie nie występuje już informacja o istnieniu bramy 10.1.0.1.

1. Sprawdź trasę do dowolnego adresu
2. Wykonaj ping na ten adres (3-4 odpowiedzi)
3. Ponownie sprawdź trasę

Zauważ, że komputer pomija bramę domyślną 10.1.0.208 i przesyła pakiety przez bramę 10.1.0.1, która nigdzie nie występuje w jego konfiguracji. Jest to wynikiem optymalizacji tras w sieci lokalnej za pomocą mechanizmu ICMP Redirect.

Poleceniem ping z na adres jeszcze nie używany np. www.icm.edu.pl możesz zaobserwować pakiet ICMP Redirect pomiędzy pierwszymi odpowiedziami na na polecenie ping.

Który z routerów przesłał informację o krótszej trasie?

3. IPv6

3.1. Autokonfiguracja IPv6

Sprawdź adres autokonfiguracji IPv6 interfejsu

```
ip addr show
```

Warto tu porównać adres IPv6 autokonfiguracji z adresem MAC.

Sprawdź łączność z własnym interfejsem po IPv6

```
ping6 fe80::.....
```

Sprawdź łączność z sąsiednim komputerem (adres z ekranu sąsiedniego komputera):

```
ping6 fe80::.....
```

Uwaga: polecenie zadziała dopiero po określeniu interfejsu łącza parametr **-I eth0**

3.2. Sąsiedztwo IPv6

Sprawdź adresy sąsiadów używając adresu multicastowego łącza

```
ping6 -I eth0 ff02::1
```

Sprawdź wpisy w tablicy sąsiedztwa

```
ip -6 neigh show
```

Po jakim czasie od ostatniej transmisji wpisy sąsiedztwa zmieniają swój stan z REACHABLE?

....., a po jakim są usuwane?

3.3. Routing IPv6 (2000:g::k/64)

Dodaj do interfejsu adres o zasięgu globalnym

```
ip -6 addr add 2001:4070:11:4g00::k/64
```

Sprawdź łączność z kolegami w grupie

```
ping6 2001:4070:11:4g00::k
```

Warto zauważyć, że adresy o zasięgu globalnym podlegają normalnym zasadom routingu, co

pozwała automatycznie ustalić interfejs wyjściowy i nie trzeba używać opcji **-I**.

Sprawdź łączność z komputerami w innej grupie – powinno nie działać.

Sprawdź dostępność routera

```
ping6 2001:4070:4g00::FFFF
```

Ustaw routing do pozostałych grup poprzez router 2000:g::FFFF

```
ip -6 route add ..... via 2001:4070:11:4g00::FFFF
```

```
ip -6 route add ..... via 2001:4070:11:4g00::FFFF
```

```
ip -6 route add ..... via 2001:4070:11:4g00::FFFF
```

Ponownie sprawdź łączność z komputerami ze wszystkich grup.

Czy ustawienie routingu domyślnego w zakresie IPv6 zapewni łączność ze wszystkimi grupami?

3.4. Tunelowanie IPv6 w IPv4

Aby umożliwić tunelowanie datagramów IPv6 w sieci IPv4 można tworzyć tunele pomiędzy określonymi lokalizacjami.

Przed wykonaniem ćwiczenia z tunelami należy wyczyścić tablicę routingu (najprościej wyłączając, a następnie włączając wszystkie używane interfejsy).

Przykład tunelu między grupami 1 i 2 zrealizowanego na komputerach PC04 i PC05 (konfiguracja dla PC04).

1. Włączenie przekazywania pakietów IP i IPv6

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

```
echo "1" > /proc/sys/net/ipv6/conf/all/forwarding
```

2. Utworzenie tunelu

```
ip tunnel add sit1 local 192.168.1.4 remote 192.168.2.5 mode sit  
ttl 64
```

4. Ustalenie adresu i włączenie interfejsu sit0 (tunelu)

```
ip -6 addr add 2000:1::100/64 dev sit1
```

```
ip link set dev sit1 up
```

3. Ustawienie routingu do drugiej sieci przez tunel

```
ip -6 route add 2000:2::/64 dev sit1
```

Analogicznie postępujemy na drugim końcu tunelu (PC05):

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

```
echo "1" > /proc/sys/net/ipv6/conf/all/forwarding
```

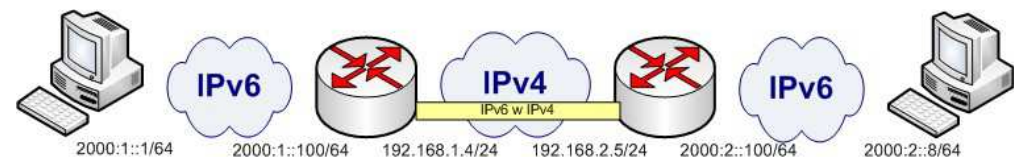
```
ip tunnel add sit1 local 192.168.2.5 remote 192.168.1.4 mode sit  
ttl 64
```

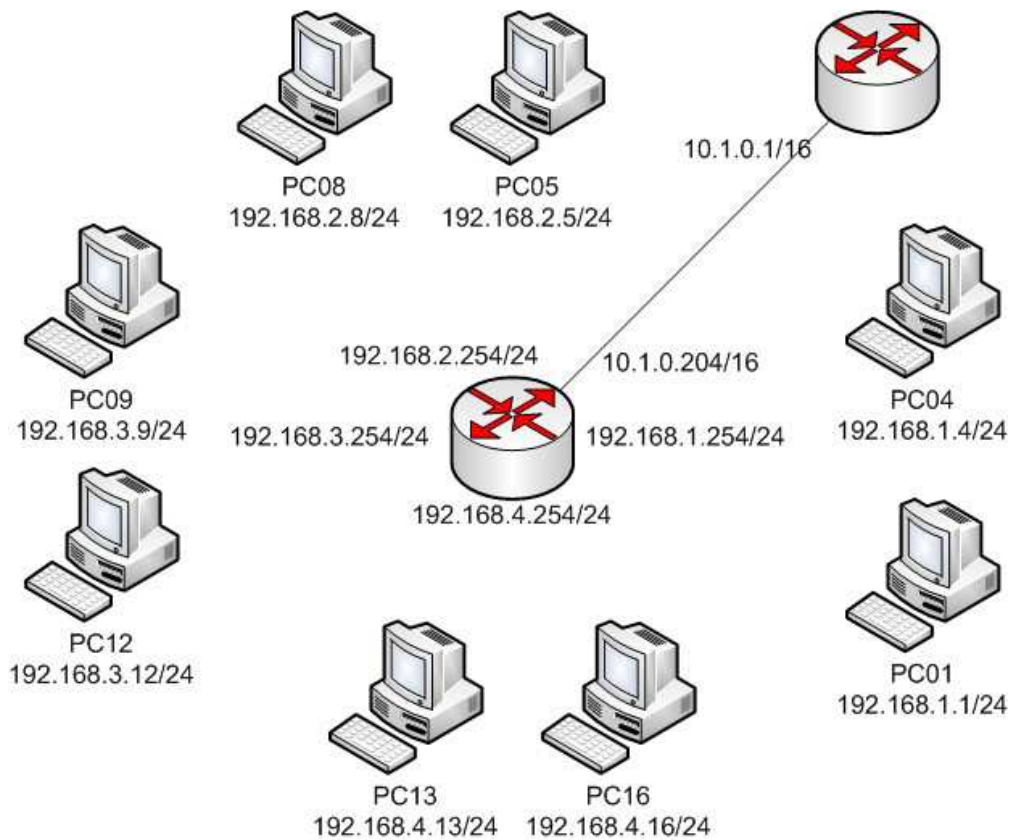
```
ip -6 addr add 2000:2::100/64 dev sit1
```

```
ip link set dev sit1 up
```

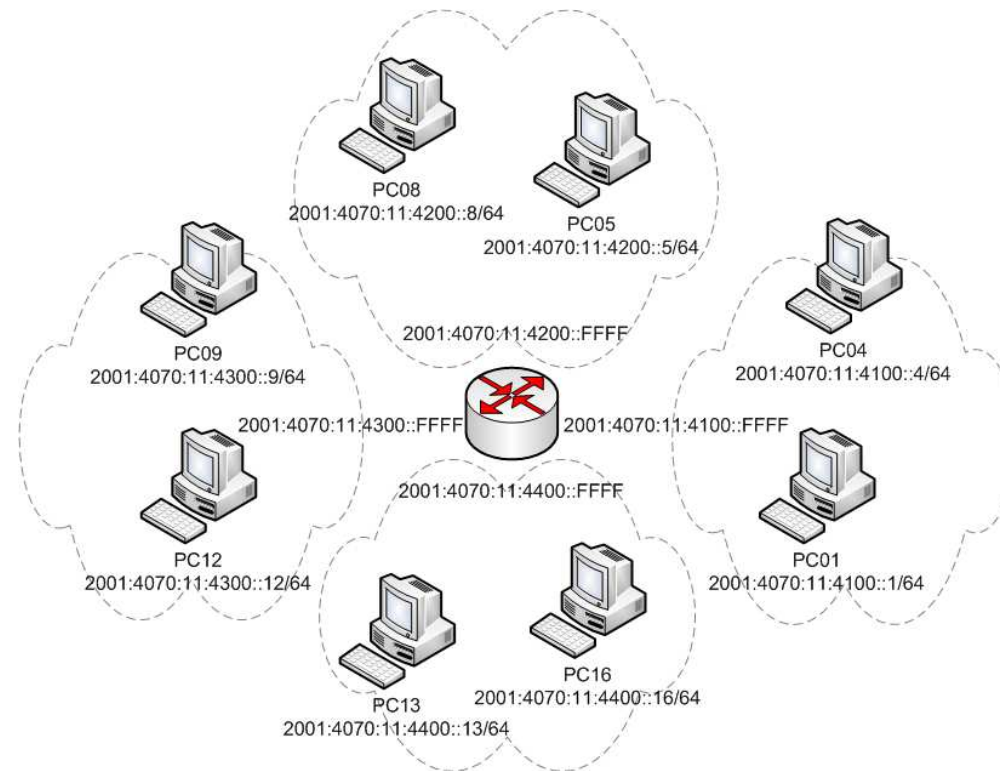
```
ip -6 route add 2000:1::/64 dev sit1
```

Pozostałe komputery w grupie 1 ustawiając jako bramę do sieci grupy drugiej 2000:1::100, a komputery grupy drugiej bramę 2000:2::100 do sieci grupy pierwszej uzyskają wzajemne połączenia po IPv6 pomimo, że transmisja pomiędzy grupami (routerami) odbywa się wyłącznie za pomocą protokołu IPv4.





Rys.1 Konfiguracja laboratorium dla IPv4



Rys.2 Konfiguracja laboratorium dla IPv6

Numer komputera k (1-18) jest naklejony na obudowie komputera.

- | | |
|-----------------------------------|-----|
| Grupa 1 to komputery 1-4 | g=1 |
| Grupa 2 to komputery 5-8 i 17-18 | g=2 |
| Grupa 3 to komputery 9-12 i 39-40 | g=3 |
| Grupa 4 to komputery 13-16 | g=4 |