T: <u>Udostępnianie połączenia sieciowego w systemie Linux (NAT).</u>

Zadanie1:

Odszukaj w Wolnej Encyklopedii Wikipedii informacje na temat NAT (ang. Network Address Translation).

Istnieje możliwość użycia Source Network Address Translation (**SNAT**) lub maskowania IP (**MASQUERADE**) w celu zezwolenia wszystkim komputerom sieci lokalnej z prywatnymi adresami IP na dostęp do internetu poprzez zaporę sieciową iptables. W przypadku stałego adresu IP dla połączenia z Internetem należy wybrać SNAT a dla dynamicznego adresu IP należy wybrać MASQUERADE. Podczas tworzenia reguł MASQUERADE lub SNAT zostają one dodane do tabeli NAT oraz łańcucha POSTROUTING. Dla MASQUERADE należy podać nazwę interfejsu (eth0, ppp0) w celu identyfikacji trasy do internetu lub zewnętrznej sieci. Dla SNAT trzeba dodatkowo podać rzeczywisty adres IP interfejsu.

Niejednokrotnie nasz ISP da nam tylko jedno IP, a my chcemy podłączyć do Internetu całą sieć. Dzięki maskowaniu adresów IP każdy komputer w sieci będzie miał adres lokalny, który przy wyjściu na świat jest zastępowany adresem serwera. Do ustawienia maskowania wykorzystamy narzędzia iptables. Przed przystąpieniem do konfiguracji należy się upewnić, że mamy wkompilowane w kernela następujące moduły:

- Routed Frames,
- Network Firewall,
- IP Firewall,
- IP Forwarding,
- IP Masquerade.

Możemy załadować następujące moduły kernela:

```
/sbin/modprobe ip_masq_autofw
/sbin/modprobe ip_masq_cuseeme
/sbin/modprobe ip_masq_ftp
/sbin/modprobe ip_masq_irc
/sbin/modprobe ip_masq_mfw
/sbin/modprobe ip_masq_portfw
/sbin/modprobe ip_masq_quake
/sbin/modprobe ip_masq_raudio ports=554,7070,7071,6970,6971
/sbin/modprobe ip_masq_user
/sbin/modprobe ip_masq_vdolive

/sbin/insmod ip_masq_ftp
/sbin/insmod ip_masq_irc
/sbin/insmod ip_masq_quake
/sbin/insmod ip_masq_raudio
/sbin/insmod ip_masq_user
/sbin/insmod ip_masq_vdolive
/sbin/insmod ip_masq_cuseeme
/sbin/insmod ip_masq_portfw
```

Konfiguracja dla routera - włączenie przekazywania pakietów (wyłączenie odpowiedzi na ping'a)

```
echo 1 > /proc/sys/net/ipv4/ip_forward
sysctl net.ipv4.ip_forward=1
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all
```

Przekazywanie pakietów na stałe możemy włączyć wpisując w pliku `/etc/sysconfig/network`

```
FORWARD_IP=yes
```

lub w pliku `/etc/sysctl.conf`

```
net.ipv4.ip_forward=1
```

Jeżeli nasz komputer ma udostępniać Internet w sieci wewnętrznej to dodajemy regułkę maskowania pakietów pochodzących z wewnętrznej sieci. Przykłady ustawień maskowania adresów:

```
#dynamicznie przydzielany adres IP
/usr/sbin/iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
/usr/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
/usr/sbin/iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -d 0/0
                   -j MASQUERADE
/usr/sbin/iptables -t nat -A POSTROUTING -s 192.168.10.201 -d 0/0
                   -j MASQUERADE

#statycznie przydzielany adres IP
/usr/sbin/iptables -t nat -A POSTROUTING -j SNAT --to-source 192.168.11.2
/usr/sbin/iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o eth0
                   -j SNAT --to 192.168.11.2
/usr/sbin/iptables -t nat -A POSTROUTING -s 192.168.10.201 -o eth0
                   -j SNAT --to 192.168.11.2
/usr/sbin/iptables -t nat -A POSTROUTING -j SNAT
                   --to-source 192.168.11.2-192.168.11.16
```

Inne przydatne reguły dla przekazywanych pakietów:

```
/usr/sbin/iptables -t filter -P FORWARD DROP
/usr/sbin/iptables -t nat -P FORWARD REJECT
/usr/sbin/iptables -t filter -A FORWARD -s 192.168.0.0/255.255.255.0
                   -d 0/0 -j ACCEPT
/usr/sbin/iptables -t filter -A FORWARD -s 0/0
                   -d 192.168.0.0/255.255.255.0 -j ACCEPT
```

Wyróżniamy następujące odmiany translacji adresów sieciowych NAT:
SNAT - zamienia adres źródłowy na inny. Przykładowa reguła:

```
/usr/sbin/iptables -t nat -A POSTROUTING -j SNAT --to-source 1.2.3.4
```

MASQUERADE - SNAT dla połączeń z dynamicznym adresem IP. Bardzo podobne do SNAT, ale gdy połączenie zostaje przerwane wszystkie śledzenia połączeń zostają zresetowane. Przykład:

```
/usr/sbin/iptables -t nat -A POSTROUTING -j MASQUERADE -o ppp0
```

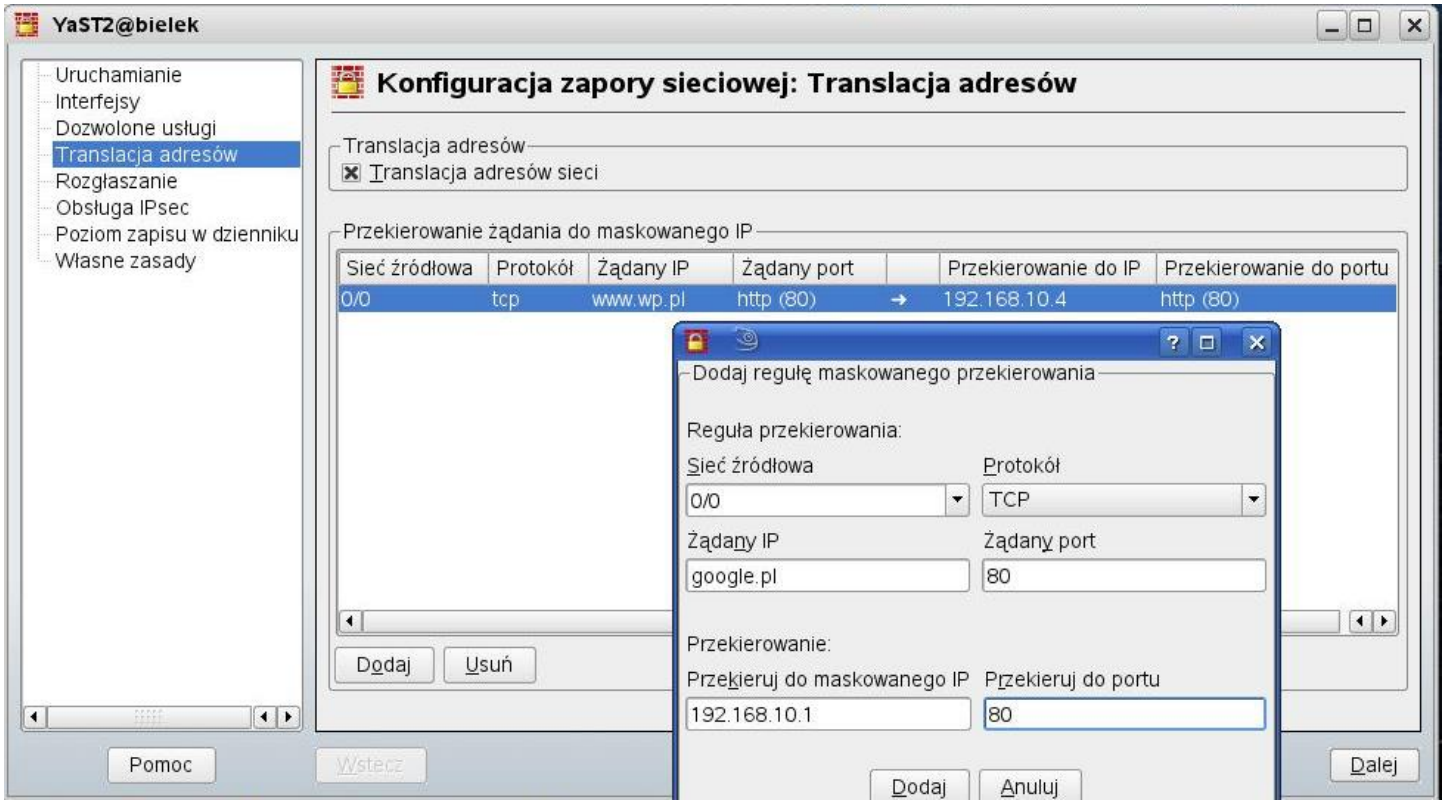
DNAT - zamienia adres docelowy na inny. Dzieje się to w łańcuchu PREROUTING. Przykład:

```
/usr/sbin/iptables -t nat -A PREROUTING -j DNAT --to-destination
1.2.3.4:8080 -p tcp --dport -i eth1
```

REDIRECT - jak sama nazwa wskazuje przekazuje pakiety do lokalnej sieci (będącej za maskaradą). Generalnie robi to samo co DNAT dla adresu z przychodzącej lokalizacji. Przykład:

```
/usr/sbin/iptables -t nat -A PREROUTING -j REDIRECT --to-port 3128
                   -i eth1 -p tcp --dport 80
```

Konfiguracja maskowania adresów IP w systemie Linux Open SUSE możliwa jest również w środowisku graficznym poprzez centrum sterowania YaST => Zabezpieczenia i uzytkownicy => Zapora sieciowa => Transtacja adresów.



Dodatkowe informacje na http://www.e-infomax.com/ipmasq/howto-trans/pl/ipmasq-HOWTO-pl.html.
Ustawienie gdy posiadamy zewnętrzny adres IP przypisywany dynamicznie:

```
/usr/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Ustawienie, gdy adres jest stały:

```
/usr/sbin/iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 12.12.12.12
```

Powrotne pakiety (z Internetu):

```
/usr/sbin/iptables -t nat -A PREROUTING -p tcp -d 15.15.15.15 --dport 80 -j DNAT --to-destination 10.0.0.25
/usr/sbin/iptables -t nat -A PREROUTING -p tcp -d 192.168.11.1/32 --dport 3389 -j DNAT --to-destination 192.168.10.4:3389
```

Ograniczenie ilości połączeń - 15 na sekundę:

```
/usr/sbin/iptables -A INPUT -p tcp --syn  --dport 80 -m limit --limit 15/second --limit-burst 35 -j ACCEPT
```

Dodatek:

Jeżeli chcemy trwale włączyć przekazywanie adresów IP należy do pliku /etc/sysctl.conf wpisać:

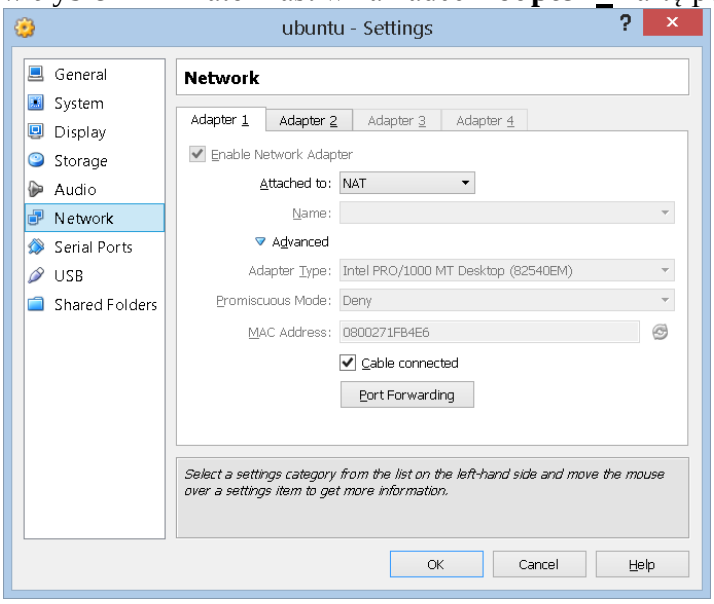
```
net.ipv4.ip_forward = 1
net.ipv4.ip_dynaddr = 1    #włączenie dynamicznego adresowania IP
route add -net 192.168.27.0/24 gw 192.168.27.1
route add default gw 192.168.27.1
ip route add 192.168.27.0/24 via 192.168.27.1
```

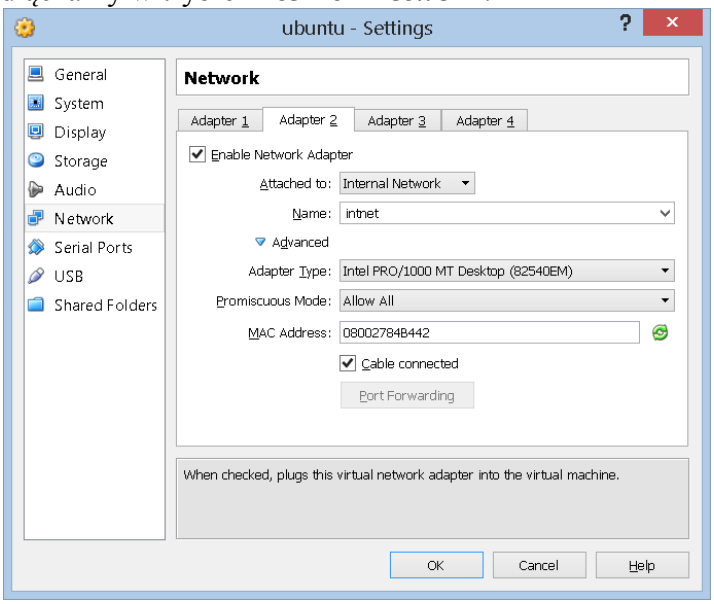
Zadanie2:

Wykorzystując maszynę wirtualną z systemem operacyjnym Linux Ubuntu należy skonfigurować dwie karty sieciowe w taki sposób, aby system udostępniał połączenie sieciowe innym użytkownikom sieci. Z przeprowadzonych działań należy sporządzić sprawozdanie w dowolnym procesorze tekstu. Na jednej stronie o rozmiarze A4, orientacji pionowej, należy umieścić dwa opisane zrzuty z ekranu, o szerokości minimum 14 cm. Każdą stronę należy podpisać swoim imieniem i nazwiskiem w nagłówku strony, natomiast w stopce numer strony wg schematu Strona X z Y. Pracę należy zachować w pliku pod nazwą **$nazwisko_ftp_linux** i przesłać pocztą elektroniczną do nauczyciela na adres greszata@zs9elektronik.pl.

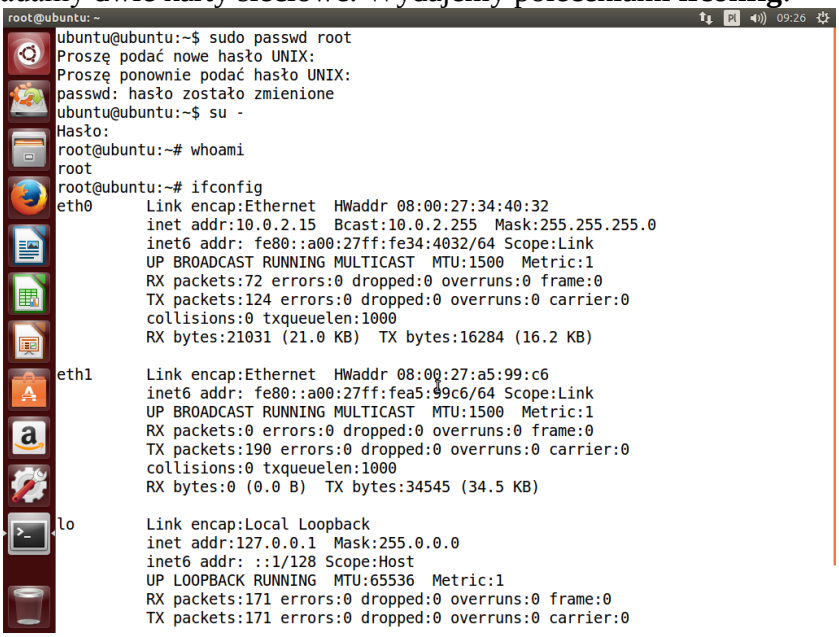
Zrzuty ekranowe przedstawiające rozwiązanie zadania 2:

Przed przystąpieniem do instalacji usługi DHCP należy sprawdzić, czy w maszynie wirtualnej systemu Linux włączyliśmy dwie karty sieciowe i odpowiednio je skonfigurowaliśmy. I tak dla maszyny wirtualnej **ubuntu** wybieramy ustawienia (**Settings**), przechodzimy do kategorii **Network** i w zakładce **Adapter 1** kartę podłączamy w trybie **NAT** natomiast w zakładce **Adapter 2** kartę podłączamy w trybie **Internal Network**.

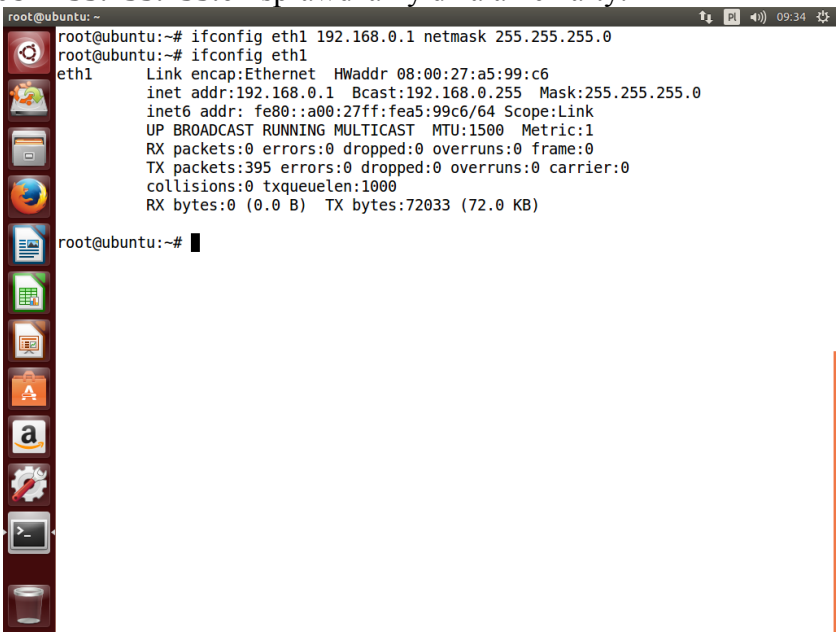




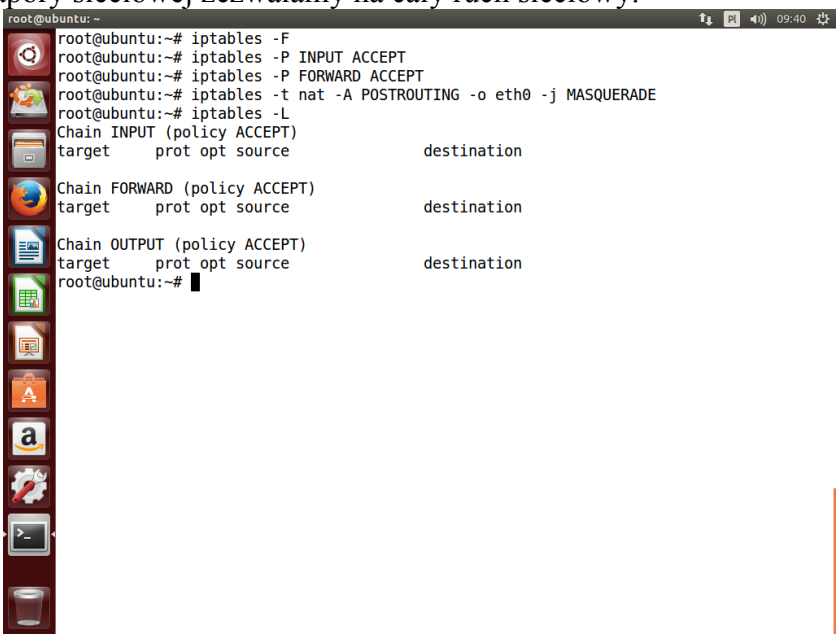
W systemie operacyjnym Linux Ubuntu uruchamiamy konsolę terminala. Uprawnienia do zarządzania systemem posiada administrator systemu, dlatego należy w oknie podać hasło użytkownika root. W oknie terminala upewniamy się, że posiadamy dwie karty sieciowe. Wydajemy poleceniami **ifconfig**:



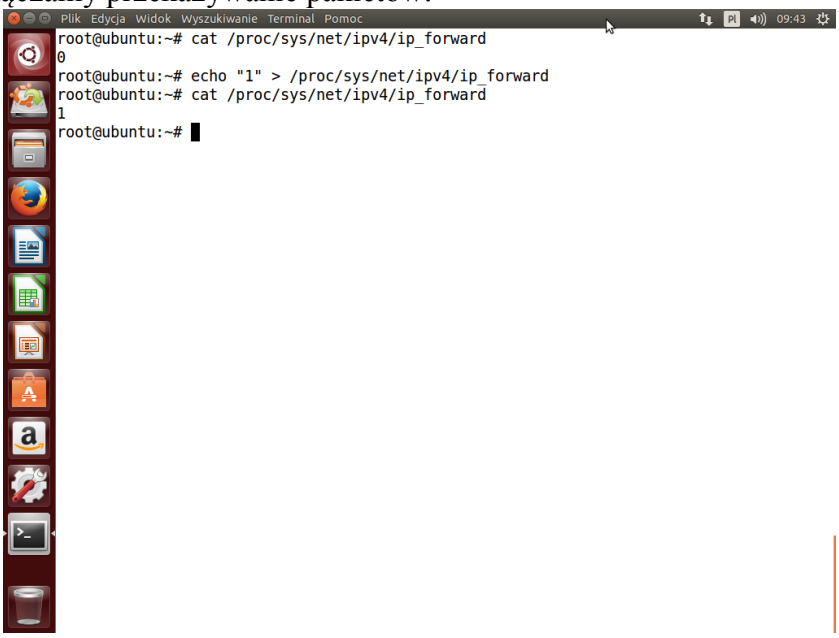
Następnie konfigurujemy statyczny numer IP dla drugiej karty sieciowej wydając polecenie **ifconfig eth1 192.168.0.1 netmask 255.255.255.0** i sprawdzamy działanie karty:



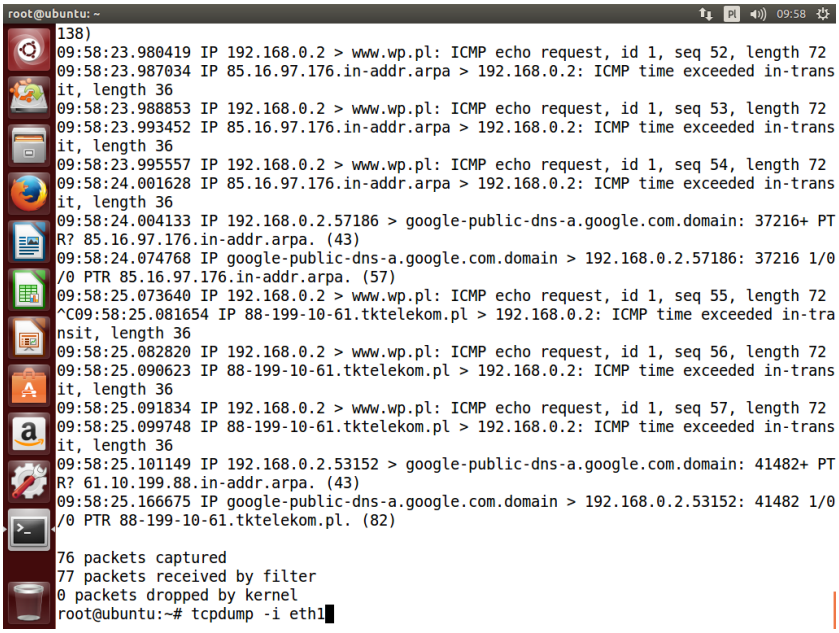
Teraz w konfiguracji zapory sieciowej zezwalamy na cały ruch sieciowy:



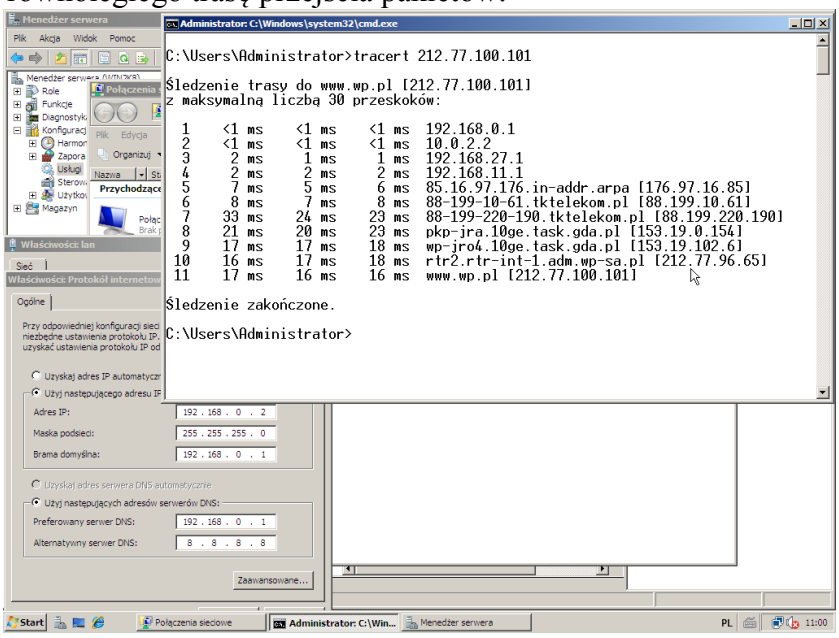
W następnym kroku włączamy przekazywanie pakietów:



Włączamy nasłuchiwanie ruchu na karcie:



I sprawdzamy z klienta równoległego trasę przejścia pakietów:



Sekwencja poleceń z czynności wykonanych podczas konfiguracji serwera (stanowisko nieparzyste):

- w celu ominięcia problemów z firewall-em należy na czas ćwiczenia wyłączyć zabezpieczenia oraz zdefiniować translację adresów NAT:
```
/sbin/iptables -F
/sbin/iptables -P INPUT ACCEPT
/sbin/iptables -P FORWARD ACCEPT
/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```
- konfigurujemy dodatkowy adres IP dla karty sieciowej:
```
/sbin/ifconfig eth0:1 192.168.9.1 netmask 255.255.255.0
```
- włączamy przekazywanie pakietów:
```
echo "1" > /proc/sys/net/ipv4/ip_forward
```
- sprawdzamy dokonane ustawienia poleceniami:
```
/sbin/ifconfig
/sbin/route -n
```
- włączamy nasłuch na karcie sieciowej:
```
/usr/sbin/tcpdump
```

Sekwencja poleceń z czynności wykonanych podczas konfiguracji klienta (stanowisko parzyste):

- wyłączamy kartę sieciową w celu usunięcia poprzedniego numeru IP:
```
/sbin/ifconfig eth0 down
```
- włączamy kartę sieciową z nową konfiguracją IP:
```
/sbin/ifconfig eth0 192.168.9.2 netmask 255.255.255.0
```
- dodajemy nową domyślną bramkę internetową:
```
/sbin/route add default gw 192.168.9.1
```
- sprawdzamy dokonane ustawienia poleceniami:
```
/sbin/ifconfig
/sbin/route -n
```
- sprawdzamy funkcjonowanie połączenia:
```
ping 212.77.100.101
ping wp.pl
```
- możemy dodać konfigurację serwera DNS w przypadku problemów z adresami domenowymi:
```
echo "nameserver 194.204.152.34" >> /etc/resolv.conf
```

Zakończenie:

- resetujemy dokonane zmiany poleceniem na obu komputerach:
```
/etc/init.d/network restart
```

Źródło instalatora programu traceroute:

https://sourceforge.net/projects/traceroute/files/traceroute/