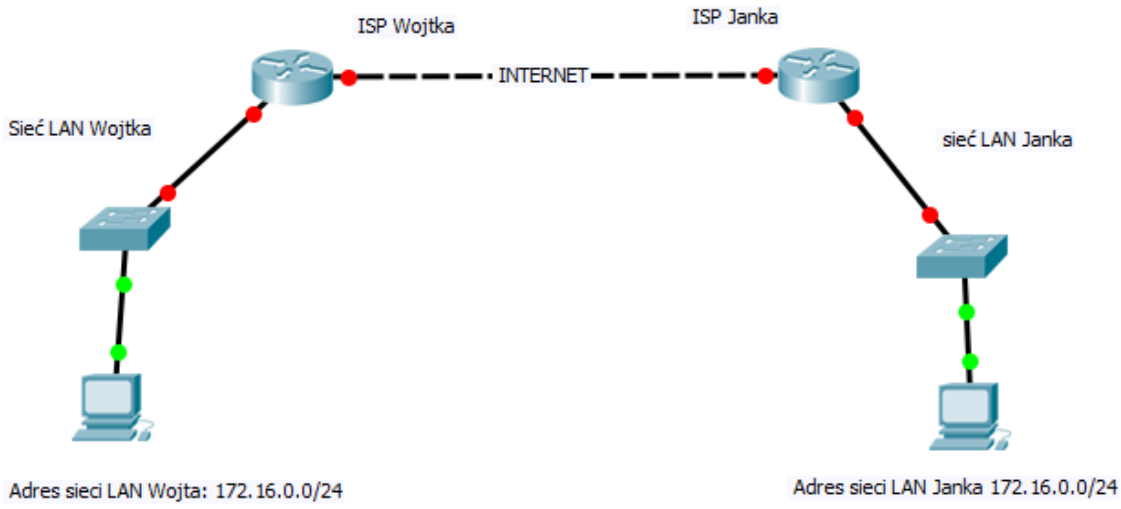
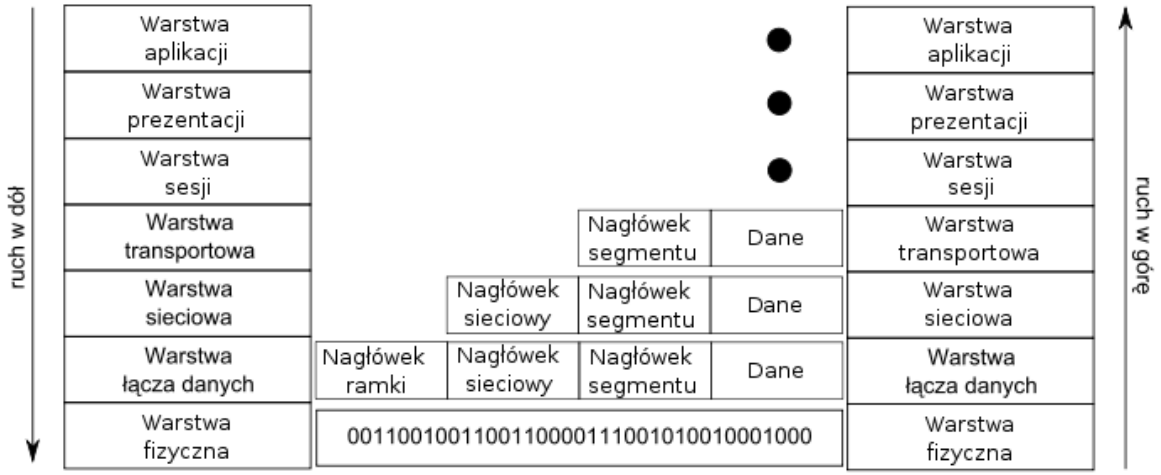
Nat teoria

1. Co to jest NAT?
   Według Wikipedii:
   Network Address Translation (NAT, pol. translacja adresów sieciowych; czasem Native Address Translation, translacja adresów rodzimych, znane również jako maskarada sieci lub maskarada IP, od ang. network/IP masquerading) – technika przesyłania ruchu sieciowego poprzez router, która wiąże się ze zmianą źródłowych lub docelowych adresów IP, zwykle również numerów portów TCP/UDP pakietów IP podczas ich przepływu. Zmieniane są także sumy kontrolne (zarówno w pakiecie IP, jak i w segmencie TCP/UDP), aby potwierdzić wprowadzone zmiany.
2. Jak to rozumieć?
   Proszę sobie wyobrazić sieć taką jak na rysunku poniżej:



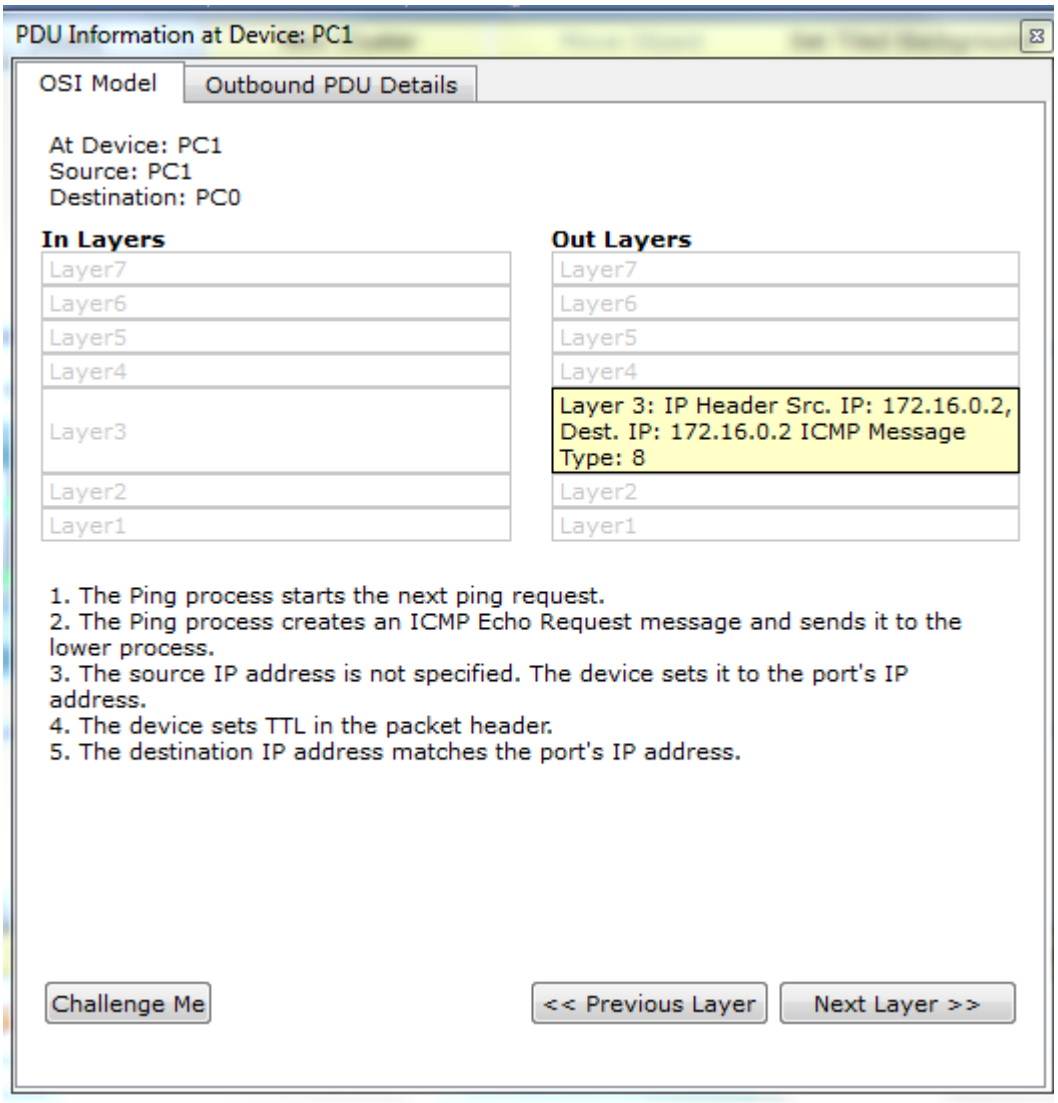
   Czy jest coś takiego możliwe? Czy może istnieć na świecie kilka (wiele) na świecie podsieci lokalnych o tym samym adresie IPv4.
   Oczywiście.
   A dlaczego? bo administrator sam nadaje adresy wewnątrz swojej podsieci 😊.

   A teraz powtórka z podstaw sieci: Model ISO/OSI



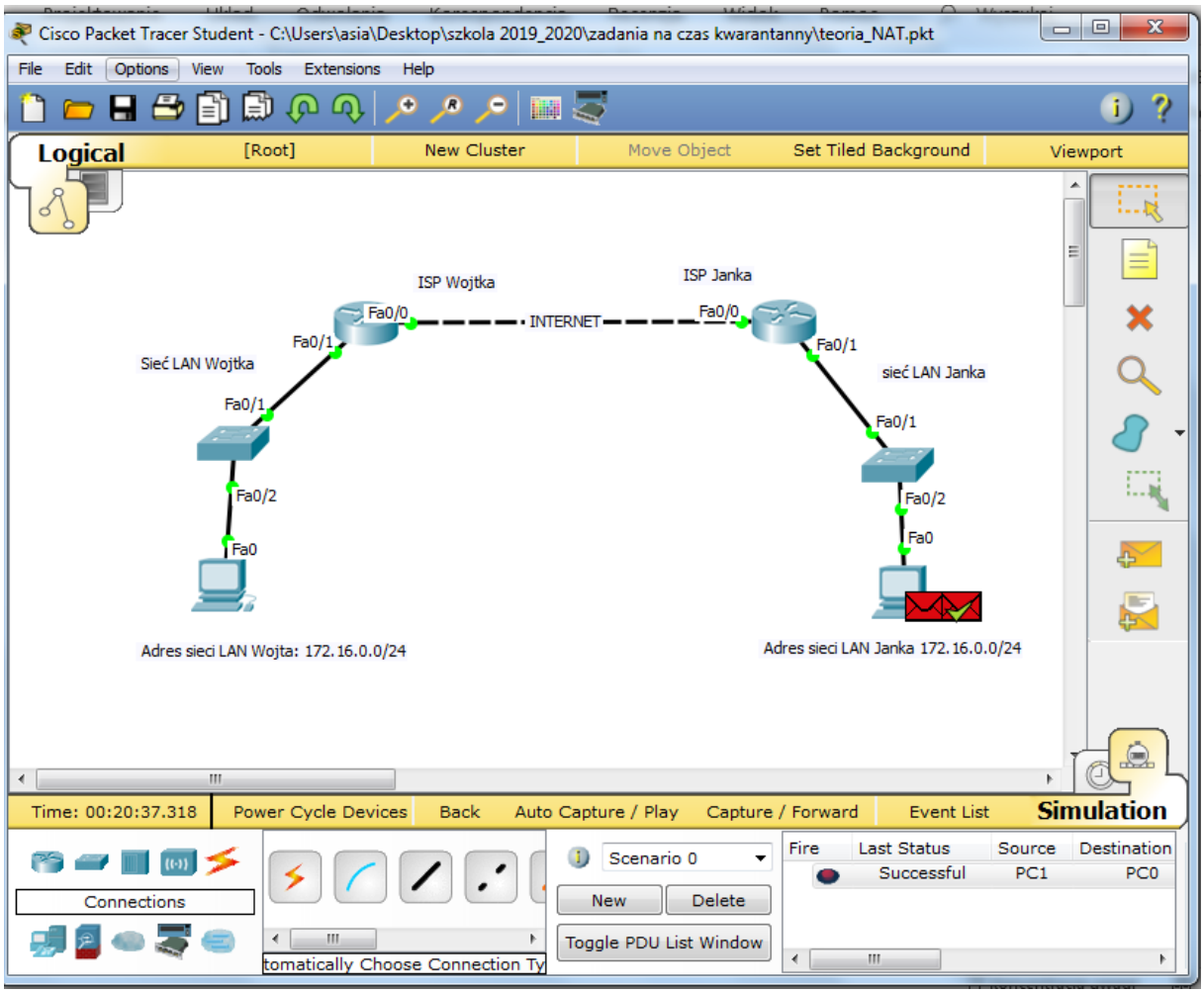
Źródło: https://pl.wikipedia.org/wiki/Model_OSI

Nagłówek sieciowy – jakie niesie informacje?
Przekazuje adres IP nadawcy i adres IP odbiorcy. (przypominam, pomimo przejścia przez ruter te adresy nie zmieniają się od początku do końca trasy, na każdym ruterze jest tak samo)
W przypadku naszej podsieci pakiet (czyli jednostka PDU z nagłówkiem sieciowym) adres IP nadawcy i odbiorcy jest taki sam. Co widać na poniższym zrzucie.



Oczywiście nie ma prawa to działać

Jak widać poniżej pomimo skonfigurowania rutingu pakiet nawet nie wychodzi z komputera a mamy komunikat successfull



Jak widać takie sieci nie mają prawa działać. Tu z pomocą przychodzi nam NAT.

3. Rodzaje NAT.

   Rodzajów NAT jest wiele. Dzisiaj zajmiemy się podziałem według Cisco.

   a) Nat statyczny – czyli jeden-do-jednego. Oznacza, że dla każdego adresu prywatnego mamy adres publiczny i jest to trwale powiązana para. Bardzo rzadko stosowane, bo mało kto dysponuje taką ilością adresów publicznych ile ma prywatnych. Sprawdza się w przypadku ważnych serwerów.
   b) Nat dynamiczny – wiele-do-wielu. Czyli mamy taką adresów prywatnych i publicznych a rutery je dowolnie łączą w pary.
   c) Nat zwany **PAT** czyli przeciążenie **NAT** zwane **overload –** czyli najczęściej spotykana – mamy tylko **jeden adres publiczny**, którego mamy użyć **dla wielu adresów prywatnych.**
   d) Szczególny **PAT –** kiedy mamy kilka adresów publicznych dla wielu adresów prywatnych. (Zawsze prywatnych jest więcej niż publicznych)

   Co trzeba zapamiętać - NAT jest to zamiana adresów lokalnych najczęściej prywatnych na publiczne funkcjonujące w sieci.

4. Jak skonfigurować NAT statyczny
   a. W trybie konfiguracji (conf t) wpisujemy polecenie:
   b. ip nat inside source static *<adres lokalny/do zamiany> <adres globalny/ ten na który zamieniamy>*
   c. następnie na interfejsie wchodzącym pisujemy polecenie

ip nat inside

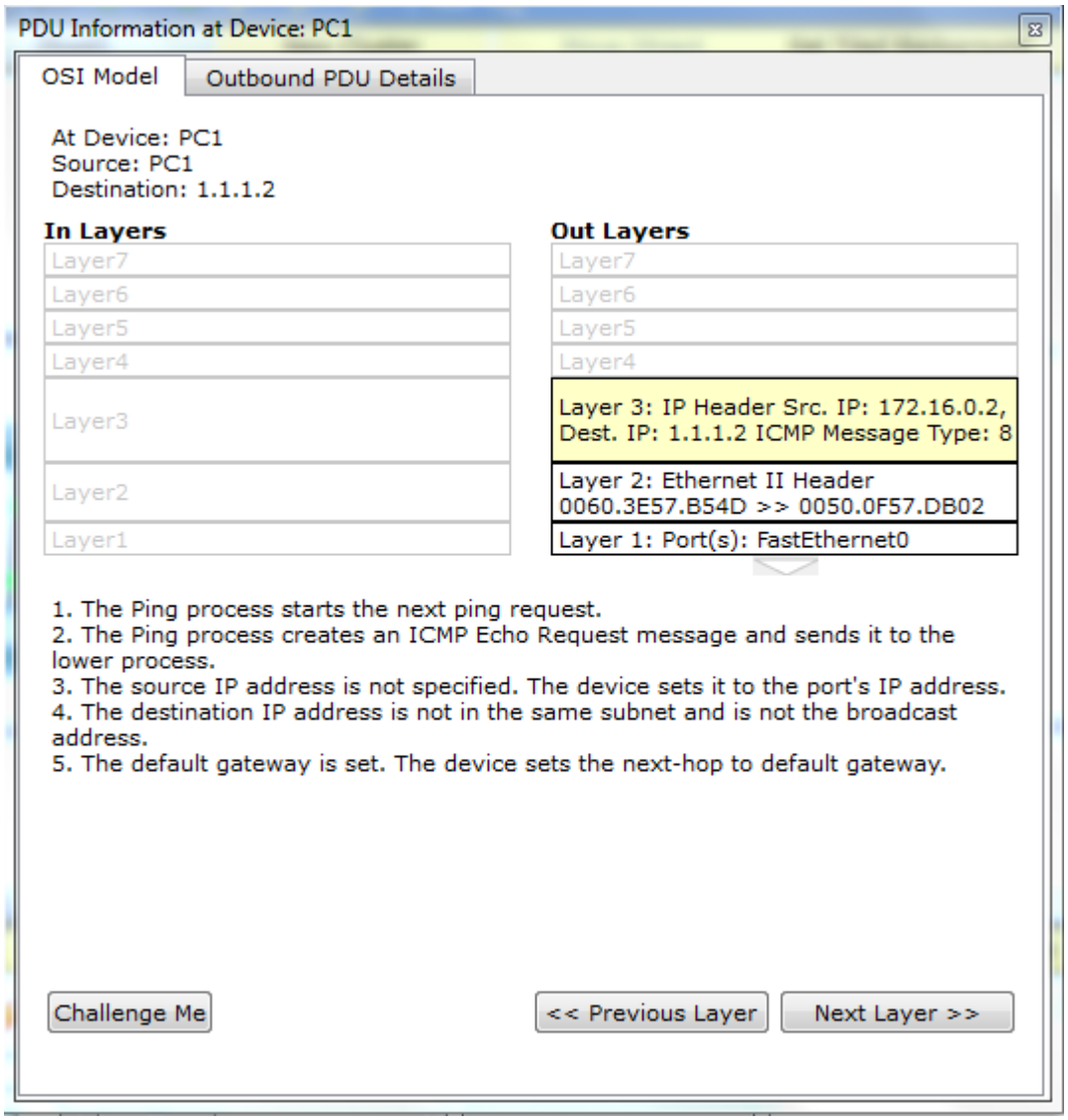
d. a na interfejsie wychodzącym

ip nat outside

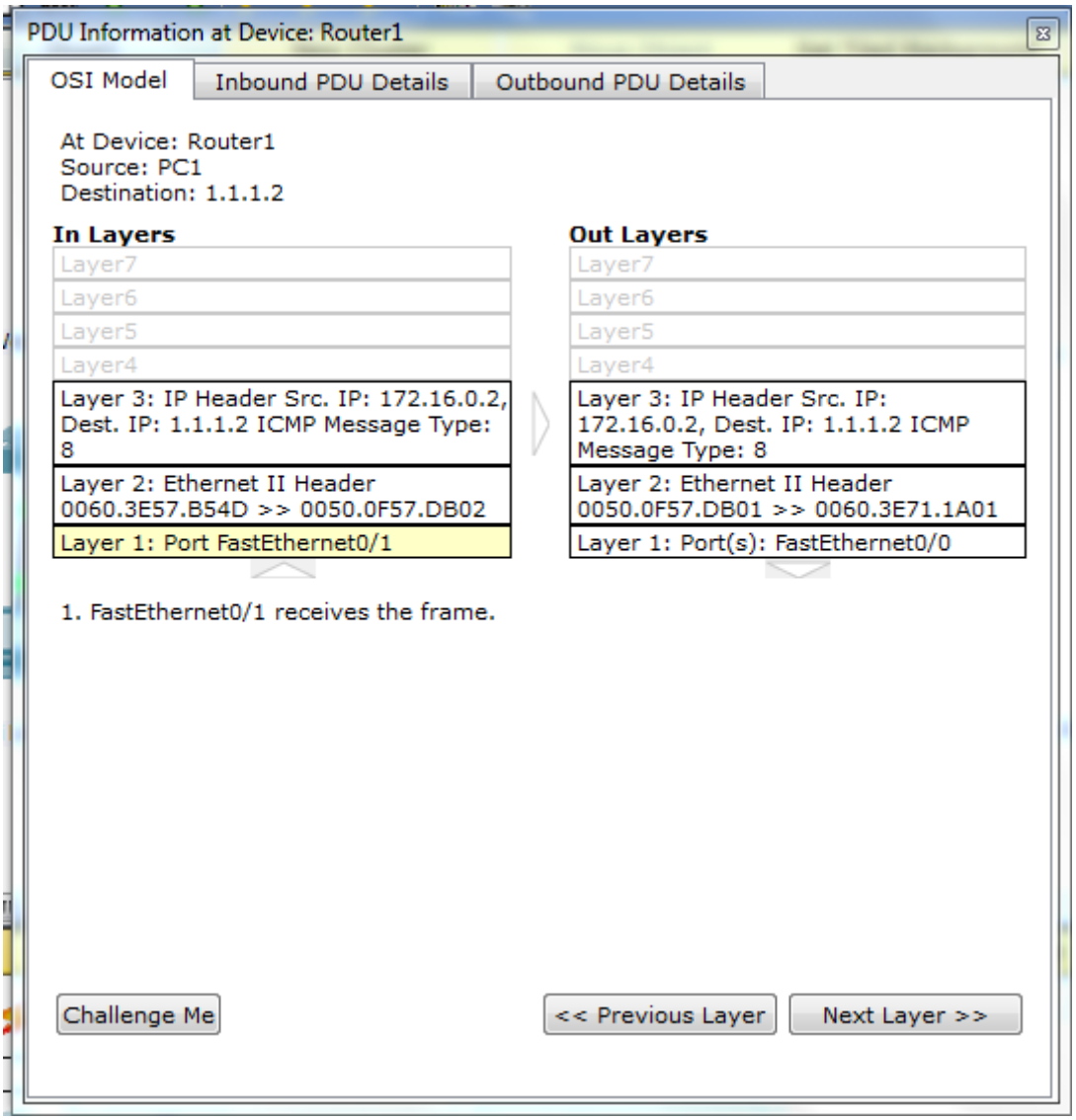
5. Problemy z PAT'em.
   Problem: Komputery o adresie 172.16.0.2/24, 172.16.0.3/24, 172.16.0.4/24 z sieci Janka łączą się z zewnętrzny serwerem. Janek ma do dyspozycji tylko jeden adres publiczny 1.1.1.1/30, czyli każde połączenie z tej podsieci ma adres 1.1.1.1/30. **Skąd wiadomo do którego komputera serwer ma skierować odpowiedź jak wszystkie połączenia do niego przyszły z tego samego adresu?**
   To jest rola rutera z NAT'em. Ruter wychodzący czyli Janka zamieniając adresy prywatne na jeden publiczny musi jakoś identyfikować połączenia. Tu z pomocą przychodzi nam warstwa 4 modelu ISO/OSI czyli transportowa. Do każdego połączenia dodaje numer portu powiązany z usługą. Takie numery portów są z reguły wysokie.
6. Jak skonfigurować PAT?
   a) Tworzymy access-listę zawierającą adresy prywatne, które będą zamieniane na adres publiczny
   b) Wyznaczamy pulę adresów publicznych (w naszym wypadku zawierającą tylko jeden adres)
   c) Łączymy pulę adresów prywatnych (access listę) z pulą adresów publicznych
   d) Wskazujemy na którym interfejsie ma się dokonywać zamiana
7. Polecenia dla instrukcji powyżej na ruterze Janka
   a. access-list 1 permit 172.16.0.0 0.0.0.255
   b. ip nat pool PULAJ 1.1.1.1 1.1.1.1 netmask 255.255.255.252 (nazwy puli piszemy wielką literą)
   c. ip nat inside source list 1 pool PULAJ overload
   d. ip nat outside
8. Jak graficznie zobaczyć, że działa

Na komputerze w sieci Janka wpisać ping 1.1.1.2 czyli interfejs na ruterze Wojtka i zaobserwować co się dzieje na kolejnych urządzeniach:

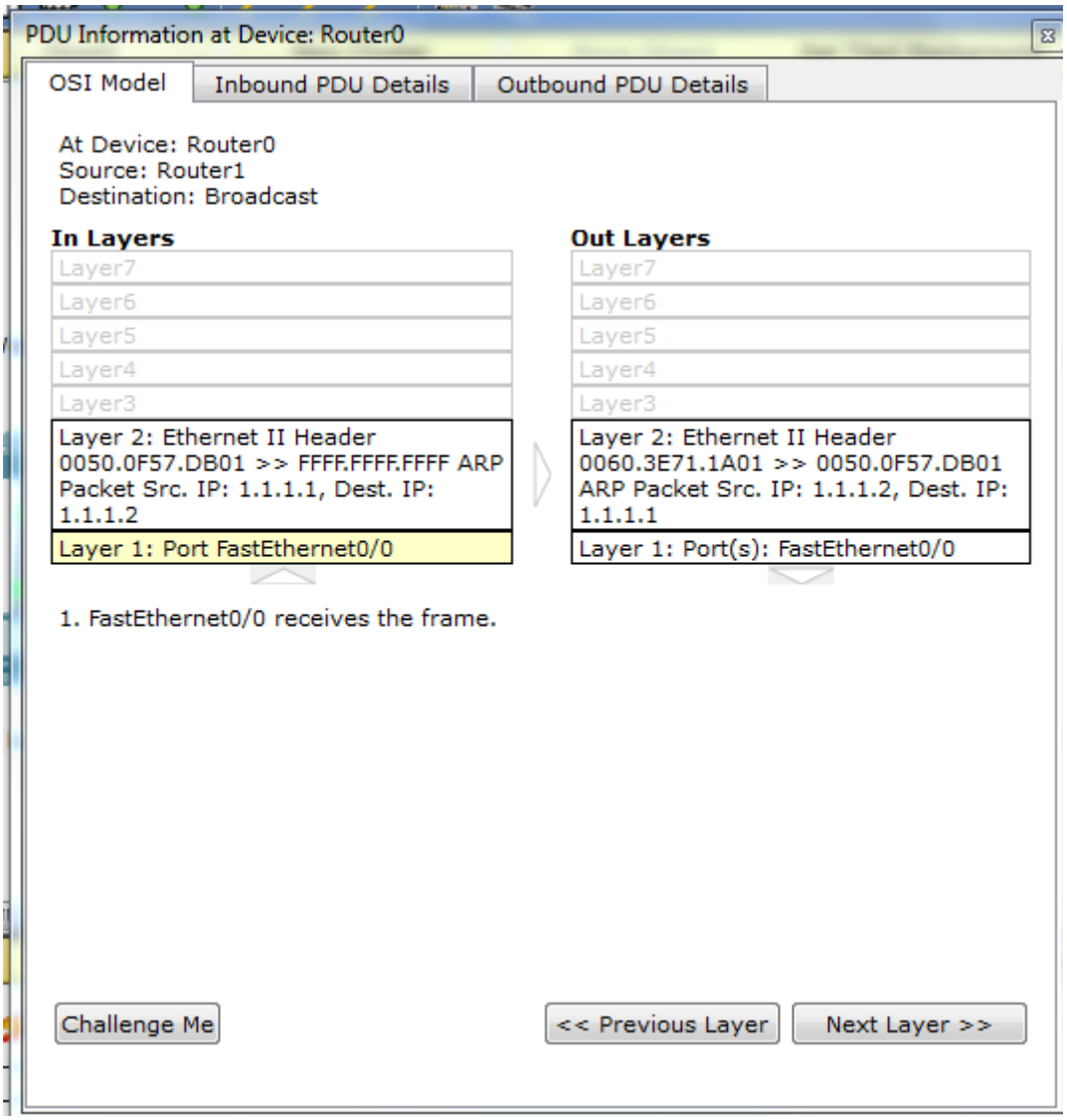
- tak jest na komputerze w sieci Janka



- tak jest na ruterze Janka



- tak jest na ruterze Wojtka – proszę zwrócić uwagę na **<u>IP źródła na IN Layers i porównać z poprzednimi zrzutami</u>**



9. A jak to sprawdzić profesjonalnie czyli z linii poleceń
   - Wykonać polecenie show ip nat translation – dla polecenia ping widać 4 połączenia (numery portów)

```
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip nat tr
Pro  Inside global     Inside local       Outside local      Outside global
icmp 1.1.1.1:26        172.16.0.2:26      1.1.1.2:26         1.1.1.2:26
icmp 1.1.1.1:27        172.16.0.2:27      1.1.1.2:27         1.1.1.2:27
icmp 1.1.1.1:28        172.16.0.2:28      1.1.1.2:28         1.1.1.2:28
icmp 1.1.1.1:29        172.16.0.2:29      1.1.1.2:29         1.1.1.2:29
```

   - Wykonać polecenia show ip nat statistics

```
Router#show ip nat st
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: FastEthernet0/0
Inside Interfaces: FastEthernet0/1
Hits: 4  Misses: 5
Expired translations: 4
Dynamic mappings:
-- Inside Source
access-list 1 pool PULAJ refCount 0
 pool PULAJ: netmask 255.255.255.252
       start 1.1.1.1 end 1.1.1.1
       type generic, total addresses 1 , allocated 0 (0%), misses 0
Router#
```

10. Jako podpowiedź wklejam konfiguracje rutera Janka (oczywiście musi być ruting, ja wykorzystałam trasę domyślną bo mam tylko dwa rutery, przypominam, że sieci lokalnych nie rozgłaszmy)

```
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 1.1.1.1 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.0.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip nat pool PULAJ 1.1.1.1 1.1.1.1 netmask 255.255.255.252
ip nat inside source list 1 pool PULAJ overload
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
!
ip flow-export version 9
!
!
access-list 1 permit 172.16.0.0 0.0.0.255
!
!
!
```