Adresy IP — format

- 32-bitowa liczba całkowita,
- zawiera identyfikację sieci (prefiks adresu)
- i o *przyłączenia* w niej (sufiks adresu)

Klasy adresów:

	7	6	5	4	3		
	1. oktet					2. oktet, 3. oktet, 4. oktet	
Klasa A	0	sieć					komputer
Klasa B	1	0	sieć				komputer
Klasa C	1	1	0	sieć			komputer
Klasa D	1	1	1	0	adres rozsyłania grupowego		
Klasa E	1	1	1	1	0	zarezerwowane na przyszłość	

W adresie

`148.81.12.166`

pierwszy oktet dwójkowo to

`10010100`

Zatem jest to adres klasy B.

- `20.81` to adres sieci,
- `12.166` to adres komputera (przyłączenia)

Adresy — zakresy

Klasa	**Najmniejszy pierwszy oktet**	**Największy pierwszy oktet**
A	0	126
B	128	191
C	192	223
D	224	239
E	240	247

Co się stało ze 127?

Adresy — konwencje (dla A, B, C)

- Adres sieci 127 oznacza sieć *pętli zwrotnej* (loopback). Dowolny komputer w tej sieci to komputer bieżący. Pojawianie się takiego adresu w ruchu sieciowym jest zabronione.
- Adres zawierający same zera w polu adresu komputera oznacza adres sieci; komputerom nie przypisuje się takiego adresu.
- Adres zawierający same jedynki w polu adresu komputera oznacza adres rozgłaszania w sieci.
- Adres zawierający same zera w polu adresu sieci odnosi się do komputera w sieci bieżącej.
- Adres zawierający same jedynki to adres rozgłaszania w sieci lokalnej.

Co oznacza adres?

- 0.0.0.0
- 128.0.0.0
- 148.81.0.0
- 148.81.255.255
- 128.0.255.255
- 0.255.255.255
- 0.0.12.166
- 128.0.12.166

Adresy — pytania

- Jaki jest najniższy adres klasy A dla komputera (B, C)?
- Ile może być sieci klasy A (B, C)?
- Ile komputerów może być przyłączonych do Internetu?
- Spóbuj oszacować liczbę potrzebnych sieci klasy B. Jak się to ma do liczby możliwych sieci tej klasy?

Adresy — mechanizmy

- rozgłaszanie
  - ukierunkowane (z adresem sieci);
  - ograniczone (ze specyfikacją adresu bieżącej siecią);
- specyfikacja bieżącego elementu
- adresowanie z podsieciami
- rozsyłanie grupowe

Adresy — wady

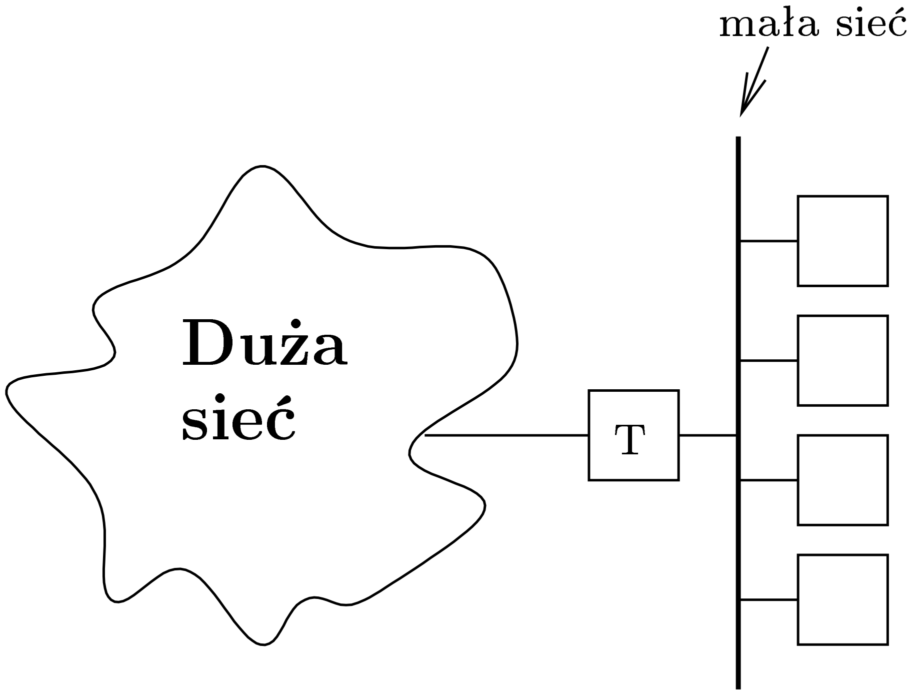
- adresy związane z przyłączeniem, a nie komputerem,
  - komputer zmieniając sieć musi zmienić adres,
  - do komputera podłączonego do wielu sieci pakiety mogą dochodzić na wiele różnych sposobów;
  - do komputera podłączonego do wielu sieci pakiety mogą dochodzić przy pomocy jednego adresu, a przy pomocy innego nie.
- kłopotliwość zmiany adresu sieci, gdy ulega ona przepełnieniu;
- za mała pojemność w stosunku do niektórych adresów sprzętowych — utrudnia to wiązanie adresu IP z adresem sprzętowym;
- za mała ilość adresów klasy B.

Mechanizmy łączenia sieci fizycznych

Istnieją co najmniej trzy mechanizmy łączenia sieci fizycznych w pojedynczą sieć logiczną:

- niewidoczne rutery;
- pośrednie ARP (*proxy ARP*, *promiscuous ARP*, *ARP hack*);
- podsieci IP

Niewidoczne rutery — zasada działania



- Komputer T wyłapuje z dużej sieci pakiety kierowane do komputerów w małej sieci i przekazuje je do tejże.
- Pakiety z małej sieci kierowane do komputerów z dużej sieci są wyłapywane również przez T i odp. przekazywane.
- Żaden uczestnik ruchu (oprócz T) nie wie o istnieniu tego rutera.

Niewidoczne rutery — wady i zalety

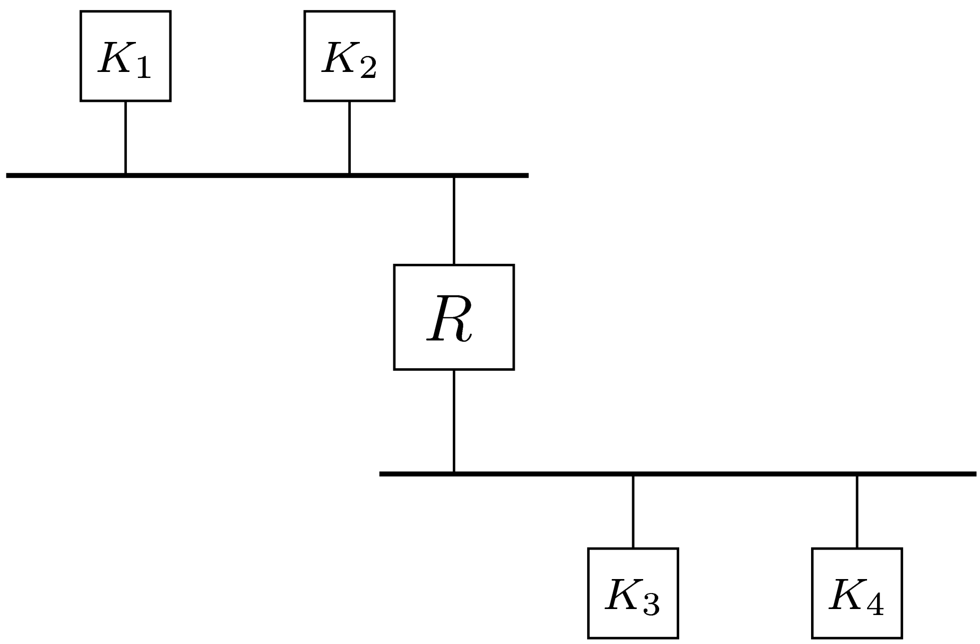
Zalety:

- zmniejszenie liczby potrzebnych adresów sieci,
- możliwość równoważenia obciążenia ruterów.

Wady:

- stosowalne tylko w przypadku dużych sieci,
- niemożność używania ICMP i innych protokołów zarządzania siecią,
- brak standardów działania takich ruterów.

Pośrednie ARP — zasada działania



- Ruter R przekazuje pakiety ARP pomiędzy dwoma sieciami fizycznymi;
- podszywa się pod inne komputery.

Pośrednie ARP — wady i zalety

Zalety:

- łatwość podłączenia, gdy nie chcemy zmieniać tablic tras IP.

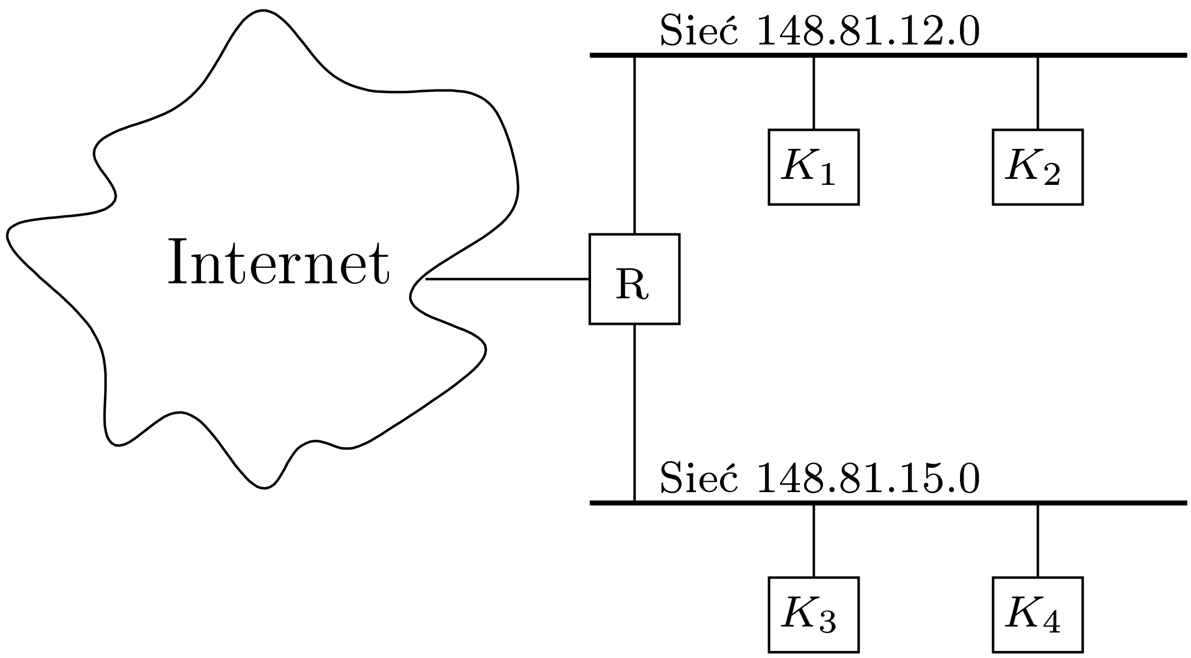
Wady:

- nie działa w sieciach nie używających ARP,
- brak możliwości łączenia dwu sieci za pomoćа wielu ruterów,
- podatność na podszywanie się,
- brak standardu,
- często wymaga ręcznego zarządzania tablicami adresów.

Kilka pytań

- Jak mogłaby wyglądać implementacja pośredniego ARP, która wymagałaby ręcznego modyfikowania tablicy adresów?
- Czy można używać niewidocznych ruterów w sieciach lokalnych?
- Czy można używać pośredniego ARP z trzema sieciami fizycznymi?

Adresowanie z podsieciami — zasada działania



Dodanie jeszcze jednego stopnia do hierarchii adresów:

Część identyfikująca sieć	Część lokalna

Część identyfikująca sieć	Sieć fizyczna	Komputer

Adresowanie z podsieciami — elastyczność

Jedni mają duże,

inni mają małe

Schemat podziału na podsieci może być dowolny — każda podsieć może mieć w zasadzie dowolny identyfikator.

Adresowanie z podsieciami — maska podsieci

Określa się maskę podsieci: bity równe 1 oznaczają część identyfikującą podsieć, bity równe 0 oznaczają część identyfikującą komputer, np:

11111111 11111111 11111111 00000000

Właściwie można stosować wiele masek w ramch jednej sieci, również maski mogą mieć dowolnie fikuśną postać np:

11111111 11111111 10101010 11000110

Jednak zaleca się nie stosować udziwnień.

Adresowanie z podsieciami — reprezentacja masek

- zapis dziesiętny z kropkami, np.:

  255.255.255.0

- zapis w postaci trójek w nawiasach klamrowych:

  {<numer sieci>, <numer podsieci>, <numer komputera>}

  na przykład

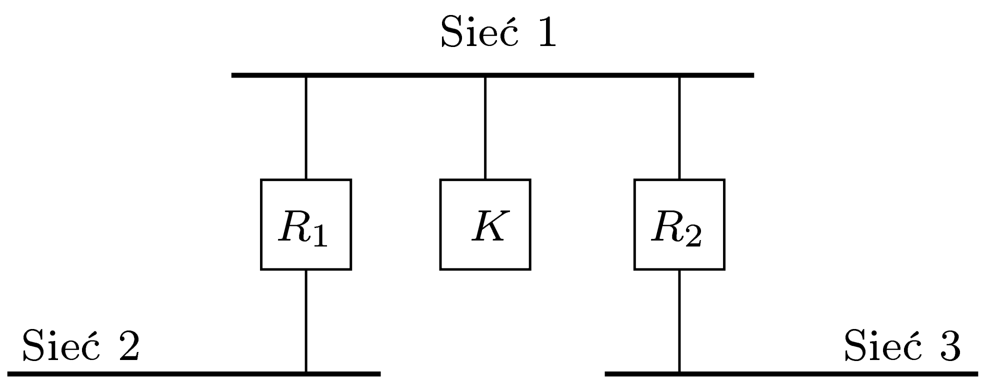
  {128.10, 255, 0}

  działa tu konwencja -1 to same jedynki, zapis ten abstrahuje od rzeczywistej reprezentacji podsieci.

Kilka pytań

- Podziel numer sieci klasy B, tak aby można było połączyć przynajmniej 76 sieci. Ile komputerów może zawierać każda z sieci?
- Czy ma sens podział adresu klasy C na podsieci?
- W pewnym ośrodku przyjęto, że trzeci oktet będzie oznaczał sieć, a czwarty będzie fragmentem adresu fizycznego. Rozczarowano się jednak, gdy okazało się, że nie można w takim układzie mieć ani 256, ani nawet 255 sieci. Dlaczego tak jest?
- Czy ma sens używanie na jednym ruterze pośredniego ARP i adresowania z uwzględnieniem podsieci?

Adresowanie z podsieciami — wyznaczanie tras



Maszyna M musi wykorzystywać trasowanie z podsieciami przy przesyłaniu informacji pod adresem sieci S, chyba że istnieje pojedyncza ścieżka P, która jest początkiem każdej najkrótszej ścieżką między M i podsiecią S.

Podsieci o danym adresie sieci powinny stanowić spójny kawałek, maski podsieci powinny być ujednolicone, wszystkie maszyny powinny używać trasowania z podsieciami.

Adresowanie z podsieciami — tablica tras

Zamiast formatu pozycji postaci:

(<adres_sieci>, <adres_następnego_etapu>)

używa się formatu:

(<maska_posieci>, <adres_sieci>, <adres_nast._etapu>)

W przypadku podsieci nie da się określić na podstawie samego adresu, które pola odpowiadają adresowi sieci, a które adresowi komputera. Maski używa się do wyodrębnienia części sieciowej.

Adresowanie z podsieciami — algorytm

Wejście: *datagram*, *tablica tras*.
Działanie:

1. na podstawie *datagramu* wyznacz adres IP odbiorcy — **ID**;
2. wyznacz adres IP sieci docelowej — **IN**;
3. jeśli **IN** zgadza się z adresem którejś z bezpośrednio przyłączonych sieci,
   - to dostarcz *datagram* do adresata **ID** za pośrednictwem tej sieci (trzeba tu wykonać:
     (a) wiązanie **ID** na adres fizyczny,
     (b) zakapsułkowanie datagramu w ramce fizycznej,
     (c) wysłanie ramki)
   - w przeciwnym razie
     (a) dla każdej pozycji w tablicy tras
        i. niech **N** będzie koniunkcją bitową **ID** i maski podsieci,
        ii. jeśli **N** jest równe polu adresu tej pozycji, to prześlij datagram pod wskazany adres do następnego etapu
     (b) jeśli nie było pasującej pozycji w tablicy tras, to zgłoś błąd trasowania.

Adresowanie z podsieciami — zarządzanie maskami

- Jak generuje się maski?
  - obierana na poziomie administratorów strategia przydzielania masek w ramach sieci,
  - zwykle jedna maska,
  - zwykle spójny ciąg bitów.
- Jak propaguje się informacje o maskach?
  - komunikaty ICMP *prośba o maskę*.

Adresowanie z podsieciami — rozgłaszanie

- Rozgłaszanie ze świata zewnętrznego:
  {sieć, -1, -1}
  - stosowane *przekazywanie z braniem pod uwagę odwrotnej ścieżki*

    Ruter wyznacza trasę do rozgłaszającego nadawcy. Jeżeli pakiet nie przyszedł z wyznaczonego w ten sposób następnego kroku, to porzuć pakiet.
- Rozgłaszanie z wnętrza sieci:
  {sieć, podsieć, -1 } (może się zdarzyć, że w niektórych sieciach nie można zastosować rozgłaszania przy skomplikowanych schematach przydzielania adresów podsieci)

Adresowanie z podsieciami — wady i zalety

Zalety:

- standardyzacja (wymagana część IP),
- zapewnia pewne rozwiązanie problemu wyczerpywania się adresów,
- szerokie możliwości dostosowania do potrzeb.

Wady:

- problem z elastycznością,
- skomplikowanie.

Nadsieci — ideologia

- inna forma radzenia sobie z problemem wyczerpywania się adresów,
- rozwiązanie przeznaczone dla komercyjnych usługodawców sieciowych,
- łączymy zakres sieci (zwykle klasy C) w jedną sieć — nadsieć,
- zwiększenie ilości informacji wymienianej przez rutery
- nietypowe oprogramowanie ruterów.

Nadsieci — bezklasowe wybieranie trasy

- blok adresów reprezentujemy jako parę

  (<adres_sieci>, <liczba>)

  na przykład (234.170.168.0, 2048)
- *liczba* jest potęgą dwójki
- faktyczna reprezentacja to para: maska, najmniejszy adres w zakresie, np.: dla bloku powyżej maska to: 255.255.248.0

  11111111 11111111 11111000 00000000
- rutery zmieniają działanie — zasada **najdłuższego pasującego odcinka**

Kilka pytań

- Rozważmy ośrodek, w którym zdecydowano się na podział adresu klasy B na podsieci tak, że jedne sieci używają 6 bitów do identyfikacji podsieci, a inne 8. Znajdź przyporządkowanie adresów komputerów, które spowoduje pojawienie się niejednoznacznych adresów docelowych.
- Porównaj działanie mostów i ruterów z oprogramowaniem obsługującym posieci?
- Co się dzieje, gdy przyjdzie pakiet adresowany do nieistniejącej podsieci?
- Jakie problemy związane z przeniesieniem się klienta od usługodawcy do usługodawcy mogłyby wystąpić, gdyby wszyscy usługodawcy używali nadsieci i przydzielali swoim subskrybentom zakresy adresów?
- Czy standard powinien wprowadzać ograniczenie powodujące, że maski podsieci będą składać się z kolejnych bitów adresu?

Kilka pytań

- Rozważmy dwa komputery A i B podłączone do tej samej sieci fizycznej N. Czy jest w ogóle możliwe, aby przy użyciu standardowego algorytmu trasowania komputer A dostał datagram przeznaczony dla B?
- Rozważmy zmodyfikowany algorytm trasowania, który służy do sprawdzania tras specyficznych dla poszczególnych komputerów, zanim sprawdzi, czy można wysłać pakiet do jednej z bezpośrednio połączonych sieci. W jakich warunkach użycie takiego algorytmu byłoby wskazane? a w jakich niewskazane?
- Nie istnieje komunikat ICMP, który pozwalałby poinformować nadawcę, że błędy w transmisji powodują, że przychodzące datagramy są uszkodzone. Wyjaśnij dlaczego?

Jeszcze kilka pytań

- Zagubienie potwierdzenia nie musi powodować retransmisji w TCP. Wyjaśnij dlaczego?
- Czy należy zamykać nieużywane połączenia?
- Czy wolałbyś używać maszyny, która pobiera swoją nazwę z serwera nazw, czy też z odległego pliku?
- Ilu adresów IP potrzeba, aby każdy dom w Twoim kraju miał osobny identyfikator sieci?