

Krzysztof Bogusławski

Akademickie
Centrum
Informatyki PS



Wydział Informatyki PS



Wydział Informatyki

Sieci komputerowe i Telekomunikacyjne

Adresowanie w sieciach lokalnych

Krzysztof Bogusławski

tel. 449 41 82

kbogu@man.szczecin.pl

MENU

1. Wstęp

2. Adresowanie warstwy MAC

3. Adresowanie lokalne

4. Adresowanie warstwy sieciowej

5. Adresowanie warstwy transportowej

6. Podsumowanie

MENU

1. Wstęp

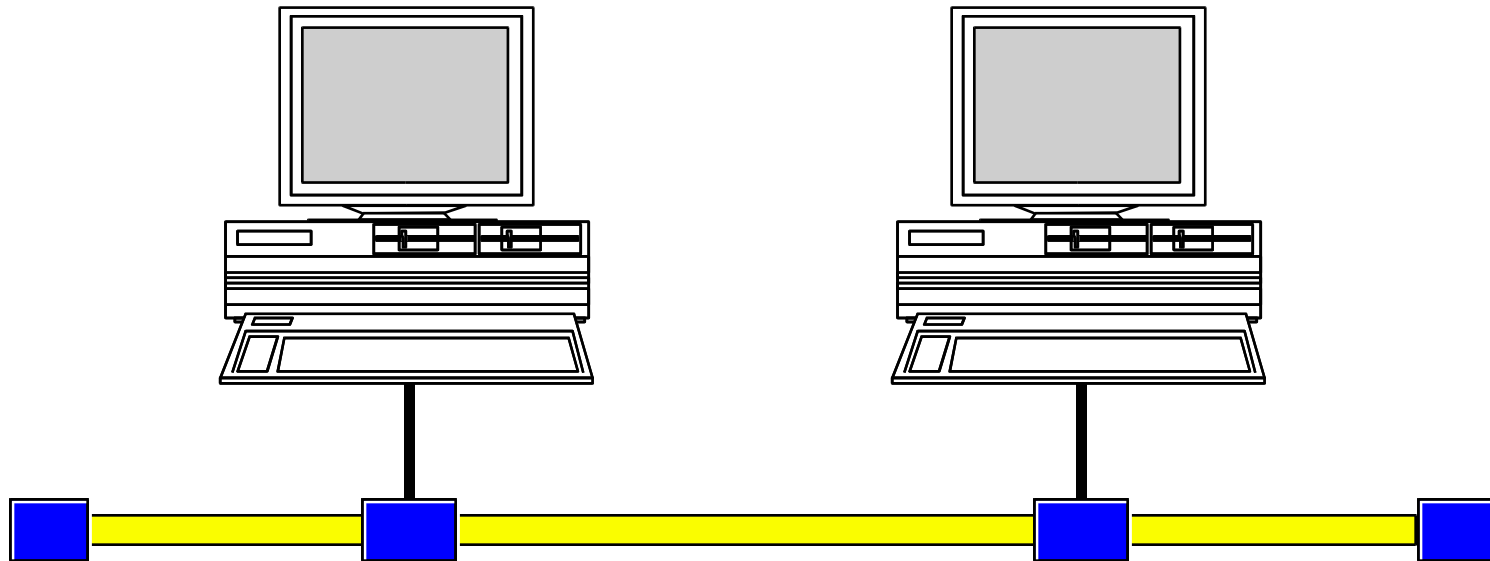
2. Adresowanie warstwy MAC

3. Adresowanie lokalne

4. Adresowanie warstwy sieciowej

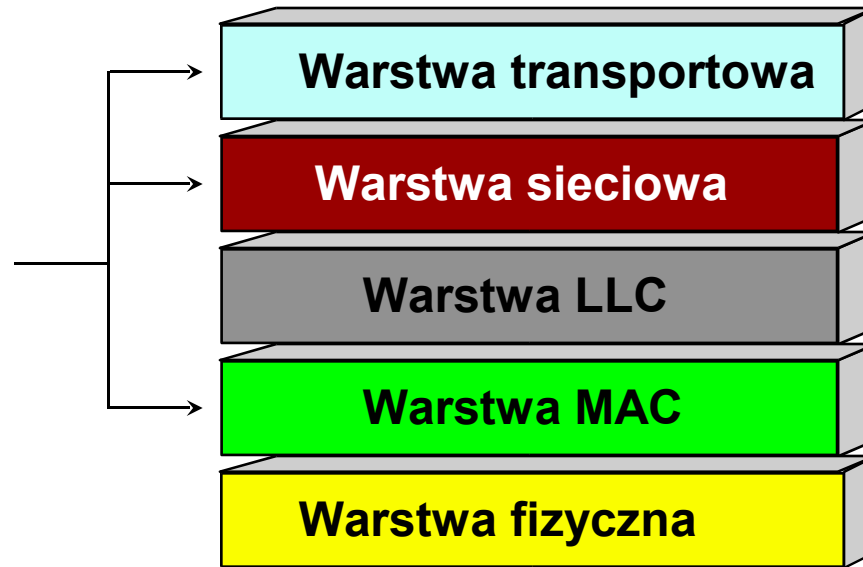
5. Adresowanie warstwy transportowej

6. Podsumowanie

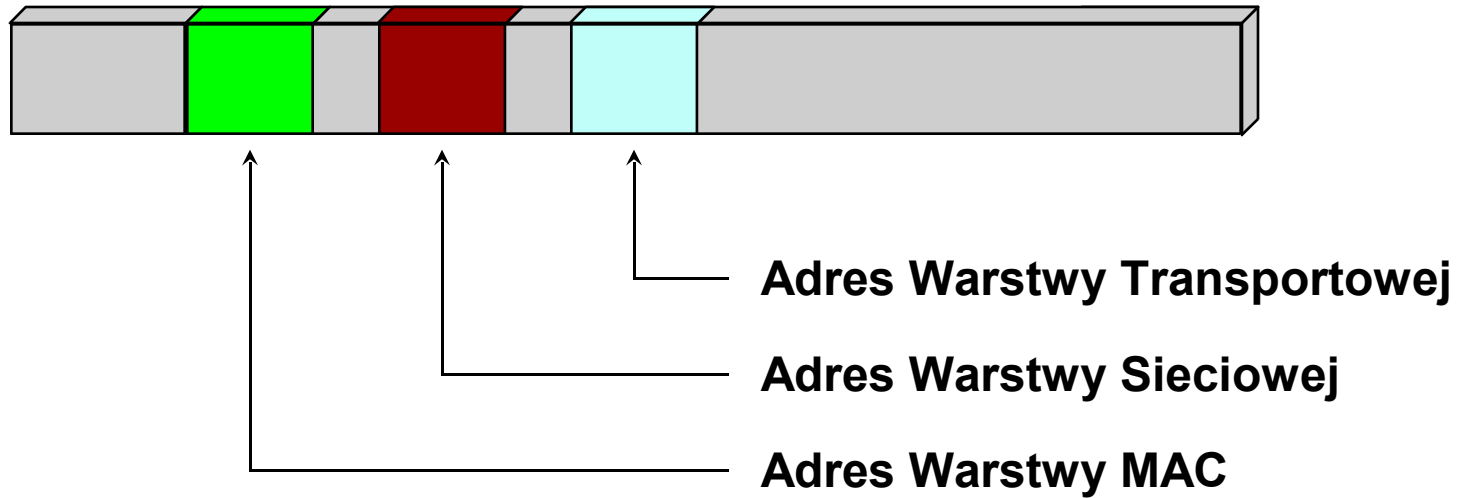


Sieci pozwalają nam przesyłać informacje pomiędzy komputerami. Częścią procedury przesyłania informacji jest *adresowanie* czyli mechanizm zapewniający, że przesyłane informacje docierają do właściwych miejsc.

**Schemat
adresowania**

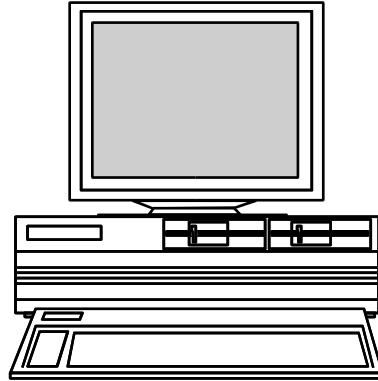
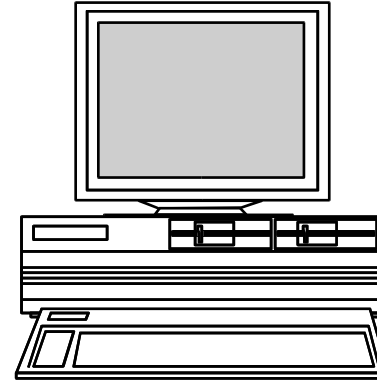


Jak przekonamy się w dalszej części wykładu, mechanizmy adresowania umieszczone są w kilku z warstw modelu OSI. Typowy pakiet TCP/IP zawiera adresy, które zostaną odpowiednio zinterpretowane przez warstwę MAC, warstwę sieciową oraz warstwę transportową.



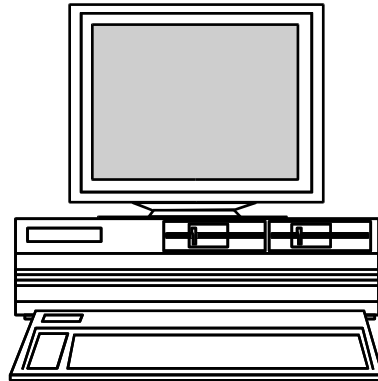
Adresy są przechowywane w specjalnie zdefiniowanych częściach pakietu IP oraz ramki LAN. Adres logiczny jest kluczem, który pozwala programowi właściwie zinterpretować informację adresową. Innymi słowy, jeżeli zapiszemy adres w nieodpowiednim formacie albo w niewłaściwym miejscu to oprogramowanie komunikacyjne, którego używamy będzie pracować niepoprawnie.

***Dlaczego potrzebujemy
adresowania?***

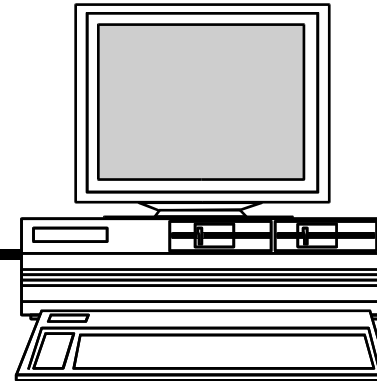
Harry**Sally**

Harry chce przesłać informacje do Sally. Zakładamy, że obydwa komputery wyposażone są w odpowiednie urządzenia, które pozwalają wysłać informacje do sieci.

Harry

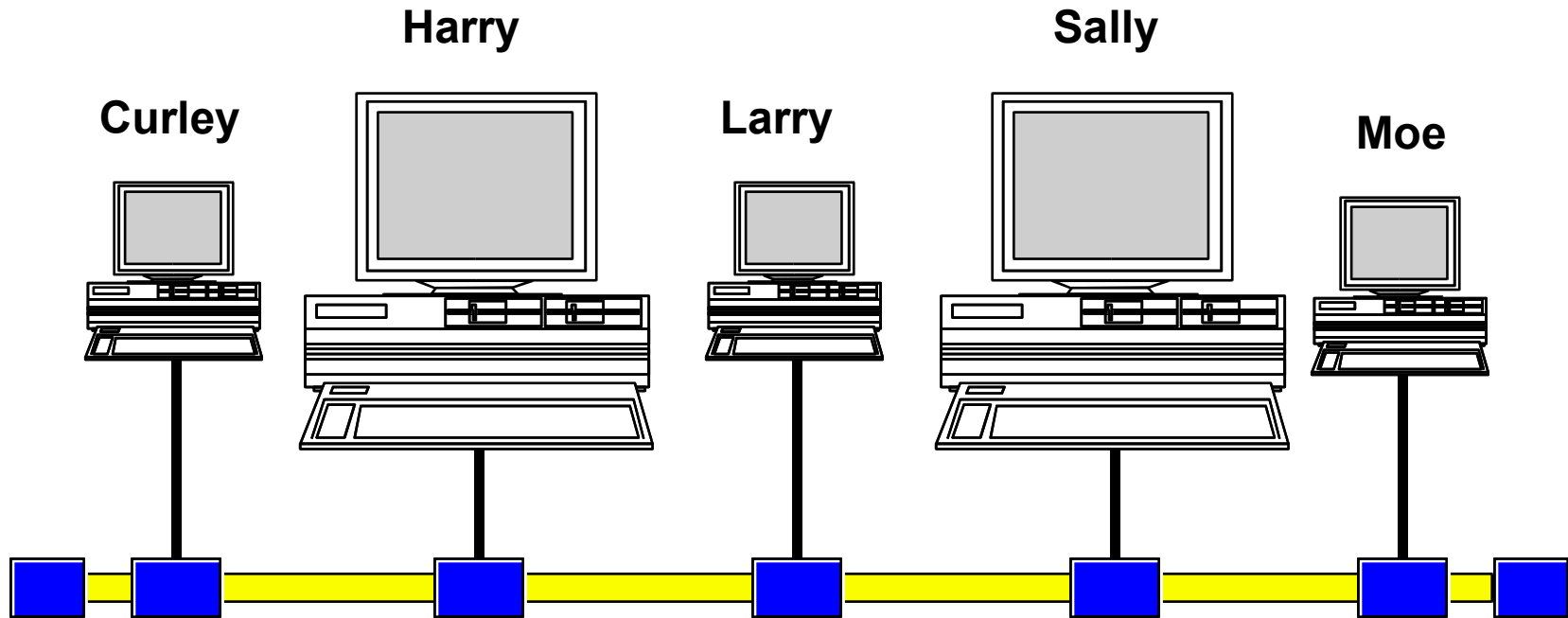


Sally



Jeżeli zwyczajnie połączymy kablem dwa komputery, oprogramowanie Harrego może wysłać informacje mając pewność, że dotrą one we właściwe miejsce.

Sytuacja taka występuje przy pozyskiwaniu informacji przez modem z użyciem programu Kermit lub podobnego.



W sieciach z dzielonym nośnikiem (np. Ethernet) Harry i Sally nie są jedynymi użytkownikami kanału komunikacyjnego. Kanał ten jest dzielony pomiędzy wszystkie komputery podłączone do sieci. W tym przypadku adresowanie jest używane aby upewnić się, że informacje przesyłane między dwoma komputerami nie są odbierane przez innych użytkowników.

MENU

1. Wstęp

2. Adresowanie warstwy MAC

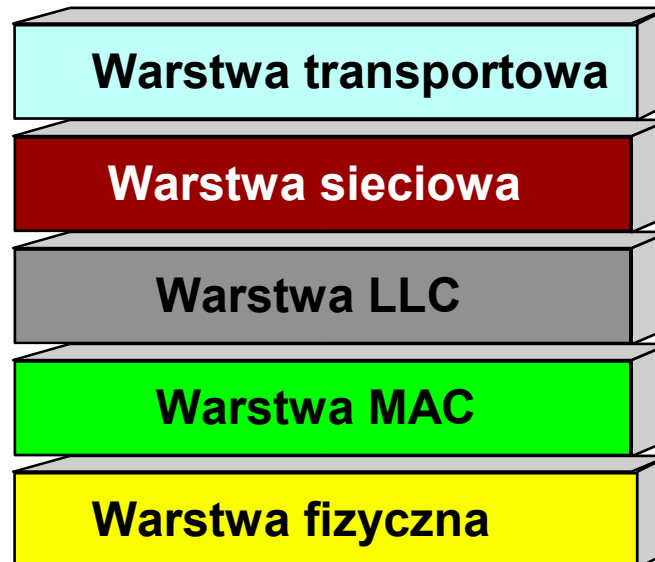
3. Adresowanie lokalne

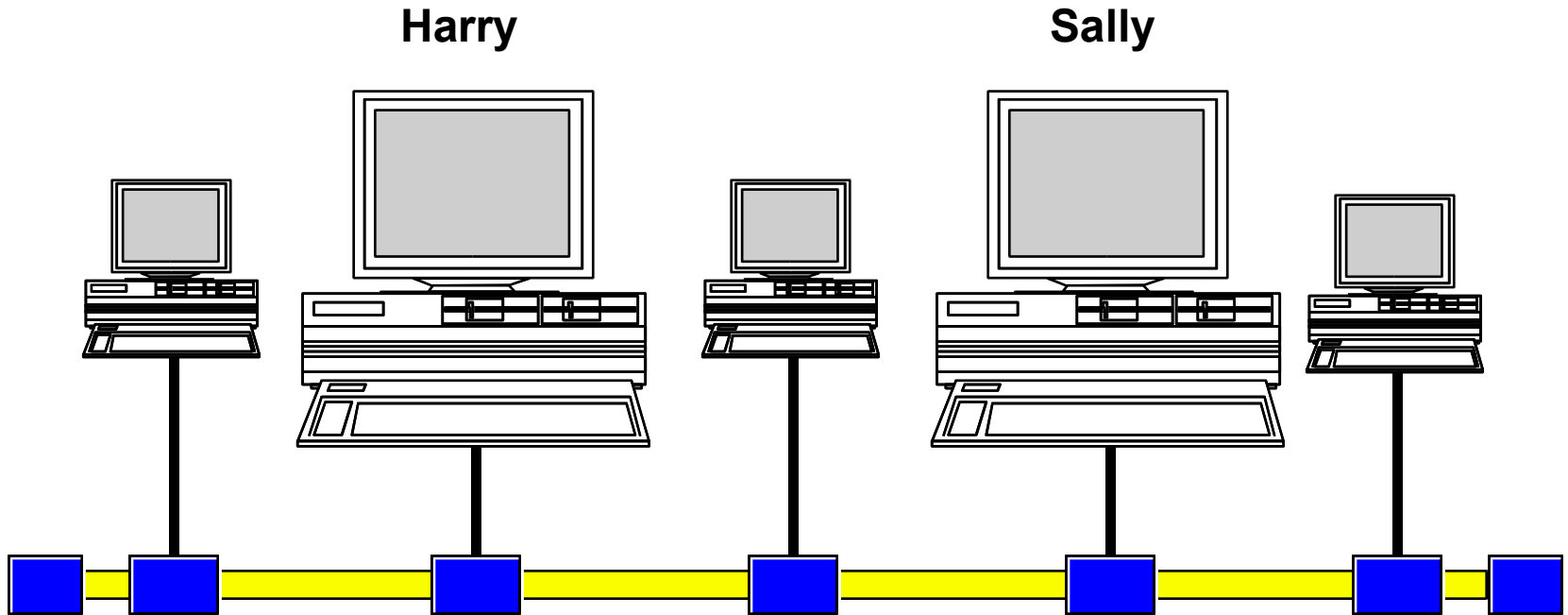
4. Adresowanie warstwy sieciowej

5. Adresowanie warstwy transportowej

6. Podsumowanie

Adresowanie warstwy MAC





Adresowanie warstwy MAC często wyjaśniane jest w oparciu o pojęcia bezpieczeństwa. Innymi słowy, adresowanie to zapewnia, że przy wielu węzłach w sieci dany węzeł nie może odczytać informacji przeznaczonych dla innego węzła. Jest to jednak znaczne uproszczenie – szczególnie biorąc pod uwagę fakt, że bardzo łatwo jest obejść ten rodzaj zabezpieczenia. Zamiast tego powinniśmy postrzegać ten rodzaj adresowania jako sposób upewnienia się, że użytkownicy sieci lokalnej (LAN) nie są zmuszeni do przetwarzania informacji przesyłanych aktualnie do kogoś innego.

•Lokalne Adresowanie Kablowe

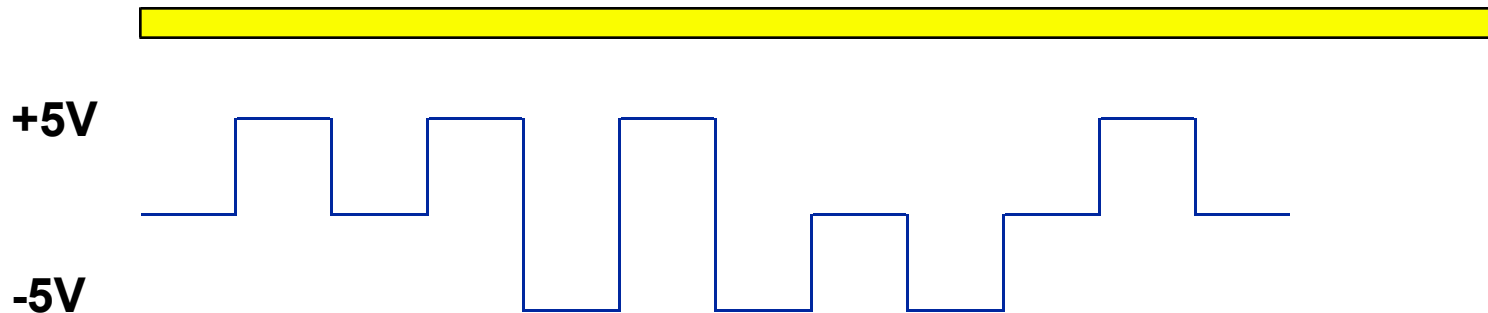
Istnieje wiele zwrotów używanych do opisu adresowania warstwy MAC. Wszystkie mają w zasadzie identyczne znaczenie. Lokalne adresowanie kablowe jest zwrotem slangowym, i odnosi się do faktu, że powodem adresowania jest konieczność odróżniania poszczególnych węzłów sieci LAN, które są podłączone do tego samego kabla. Osobiście staram się raczej nie używać tego określenia, ponieważ słabo oddaje ono istotę problemu – szczególnie w dniu dzisiejszym, kiedy używamy przełączników LAN oraz mostów wieloportowych.

- Lokalne Adresowanie Kablowe
- Adres Fizyczny**

Fizyczne adresowanie jest pojęciem używanym w dokumentacji RFC w celu opisu adresowania MAC. Sądzę, że podejście takie może się przyjąć, gdyż adres MAC jest związany z fizycznym hostem z którego ramka wywodzi się, lub do którego jest skierowana.

- Lokalne Adresowanie Kablowe
- Adres Fizyczny
- Adres MAC**

Adres MAC (*Media Access Control*) jest pojęciem używanym w żargonie przemysłowym. Używa się go w warstwie MAC modelu OSI i w tej warstwie znajduje się jego zakres ważności.



...1101011010...

W warstwie fizycznej modelu OSI, sygnały elektryczne są interpretowane jako serie binarnych zer i jedynek. Warstwa fizyczna w żaden sposób nie interpretuje tych danych.

← Kierunek Transmisji



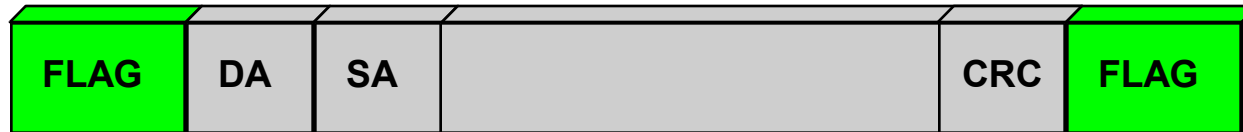
W warstwie MAC zera i jedyneki są umieszczane w strukturach zwanych ramkami. Ramka jest strukturą informacyjną najniższego poziomu w sieci typu LAN. Struktury te nie mogą być zbyt duże. W sieci Ethernet mają one pojemność do 1.5 kB (około 12 000 bitów), w sieci Token Ring 18 kB a w FDDI 4 kB. Określony jest również minimalny rozmiar ramki. Dla sieci Ethernet wynosi on 64 bajty.

← Kierunek Transmisji



Struktura ramki jest określona w zależności od technologii sieci LAN. Ethernet, Token Ring oraz FDDI nie różnią się bardzo pod tym względem. Powyższy diagram pokazuje ogólną strukturę ramki. Bity w ramce są przesyłane w kolejności od lewej do prawej. Jest to standardowa konwersja w większości opracowań.

← Kierunek Transmisji



Przy omawianiu budowy ramki bardzo ważnym pojęciem jest tzw. *flaga (flag)*. Flagi są specjalnymi zestawami bitów, które pozwalają sieci LAN zidentyfikować początek i koniec ramki.

← Kierunek Transmisji



W Ethernetie, flaga startowa ramki jest serią 62 bitów przyjmujących wartość zero lub jeden, a po nich dwa bity ustawione zawsze na jeden. Standard Ethernetu oraz IEEE przyjmuje to pole jako *wstępne (preamble)*.

Inną ważną cechą używania pola wstępnego jest możliwość „zawieszania” łączników LAN lub synchronizacja sygnałem zegarowym.

Flagą końcową ramki jest przerwa w transmisji – przerwa ta musi trwać co najmniej 9.6 mikrosekund ale może być dłuższa jeżeli żaden węzeł nie jest gotowy do transmisji. Standard Ethernetu oraz IEEE określają flagę końcową jako *przerwa międzyramkowa (interframe gap)*.

← Kierunek Transmisji



W sieci Token Ring oraz przy technologiach FDDI, flagi są interpretowane jako specjalne kodowanie linii. W Token Ring'u kodowanie zrealizowane jest jako kontrolowane zakłócenie zrealizowane w oparciu o schemat kodowania typu Manchester. W systemie FDDI na flagi rezerwuje się specjalne 5-bitowe bloki.

← Kierunek Transmisji



Przed końcem ramki znajduje się pole CRC (*Cyclic Redundancy Check*). Pole to służy do sprawdzania poprawności ramki.

← Kierunek Transmisji

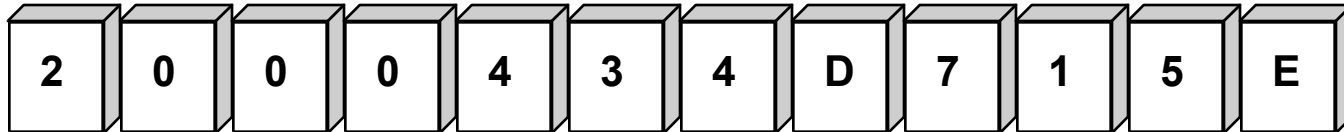


W początkowej części ramki znajdują się dwa pola przeznaczone na adresy MAC. Pierwsze z tych pól zawiera *adres przeznaczenia* (*Destination Address*) zwany w skrócie DA, zaś drugie przeznaczone jest na *adres nadawcy* (*Source Address*) oznaczone jako SA. W wiadomości przesyłanej między Harrym i Sally, Harry powinien wstawić adres MAC Sally w pole DA, zaś swój własny adres w pole SA.

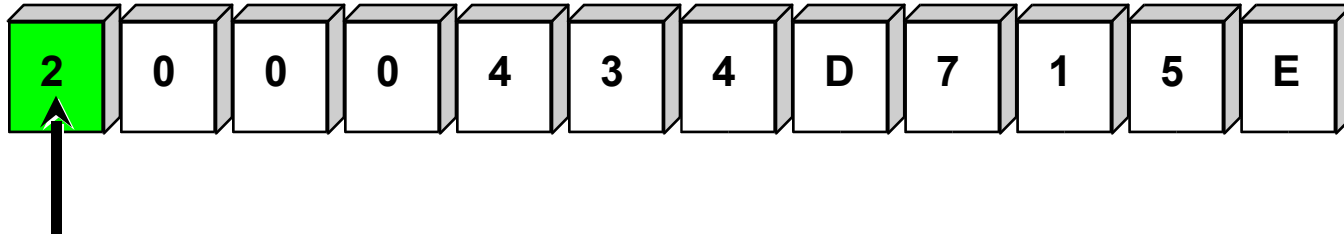
Struktura Adresu MAC



Pomimo tego, że ramki są specyficzne w zależności od danej technologii LAN, najbardziej znane systemy (Ethernet, Token Ring i FDDI) używają tych samych struktur adresowych.



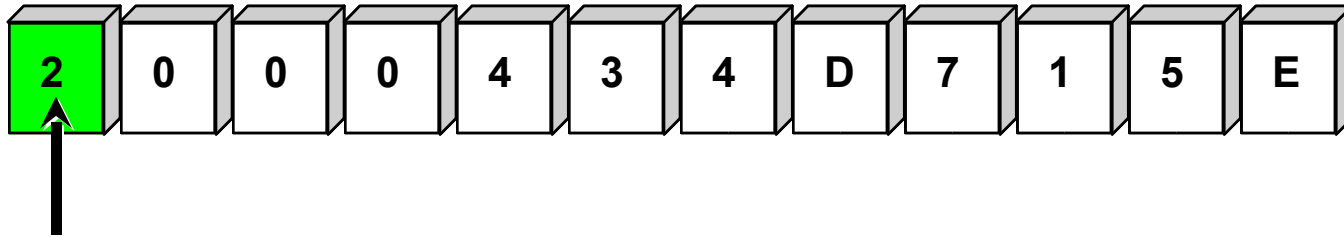
Powyżej przedstawiono typową strukturę adresu MAC w standardzie IEEE. Jak widać jest ona podzielona na cyfry szesnastkowe. Każda taka cyfra jest odpowiednikiem 4 bitów. .



Reprezentacja dwójkowa = 0010

Bit G/I

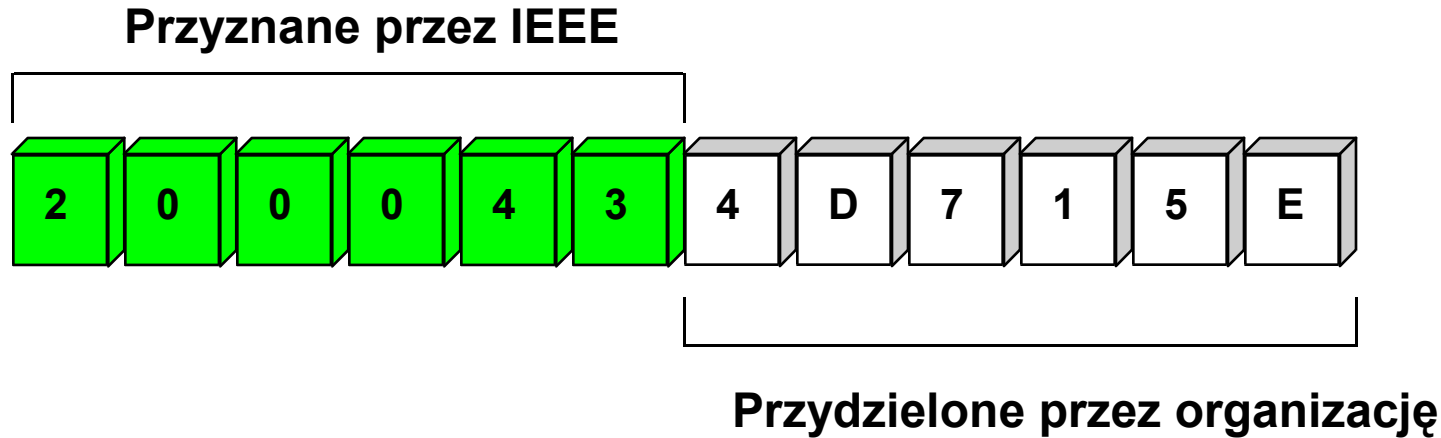
Pierwsze dwa bity adresu mają specjalne znaczenie. Pierwszy z nich znany jest jako bit G/I (*Group / Individual*). Jeżeli ten bit jest czysty (czyli równy zero) to dany adres jest adresem typu *Unicast*. Oznacza to, że ramka jest zaadresowana do tylko jednego możliwego interfejsu sieci LAN. Jeżeli bit G/I jest ustawiony (czyli równy jeden) to ramka jest typu *Multicast* bądź *Broadcast*.



Reprezentacja dwójkowa = 0010

Bit G/L

Drugi bit znany jest jako bit G/L (*Global/Local*). Jeżeli ten bit jest czysty, to wiadomo jest, że dany adres MAC został wyznaczony z bloku adresów zarejestrowanych przez IEEE. W takim wypadku, żaden inny interfejs LAN na całym świecie nie może mieć identycznego adresu. Adres taki nazywamy *Adresem Wyznaczonym Globalnie (Globally Administered Address)*. Jeżeli bit jest ustawiony, to wiadomo, że adres został stworzony przez administratora lokalnej sieci LAN i nie musi być unikalny w skali globalnej. Adres taki nazywamy *Adresem Wyznaczonym Lokalnie (Locally Administered Address)*.

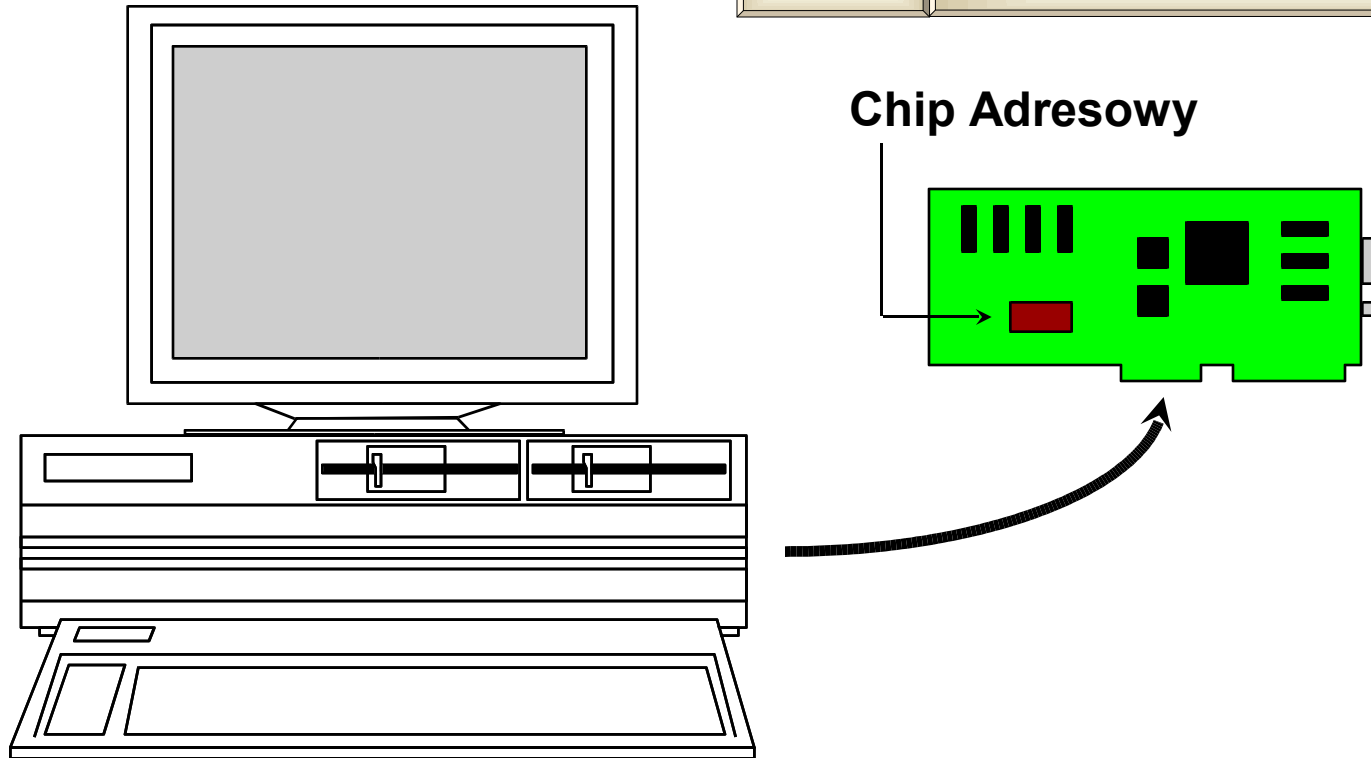


Jeżeli jakaś organizacja chce mieć adres wyznaczony globalnie to IEEE (*Instytut Inżynierów Elektryków i Elektroników* - amerykańska instytucja normalizacyjna) wyznacza jej specjalny 24-bitowy blok adresowy. Jeżeli blok został przydzielony to organizacja ta jest odpowiedzialna za unikalne wyznaczanie adresów wewnątrz swojego własnego bloku. Duże organizacje (np. DEC, IBM) posiadają po kilka bloków 24-bitowych.

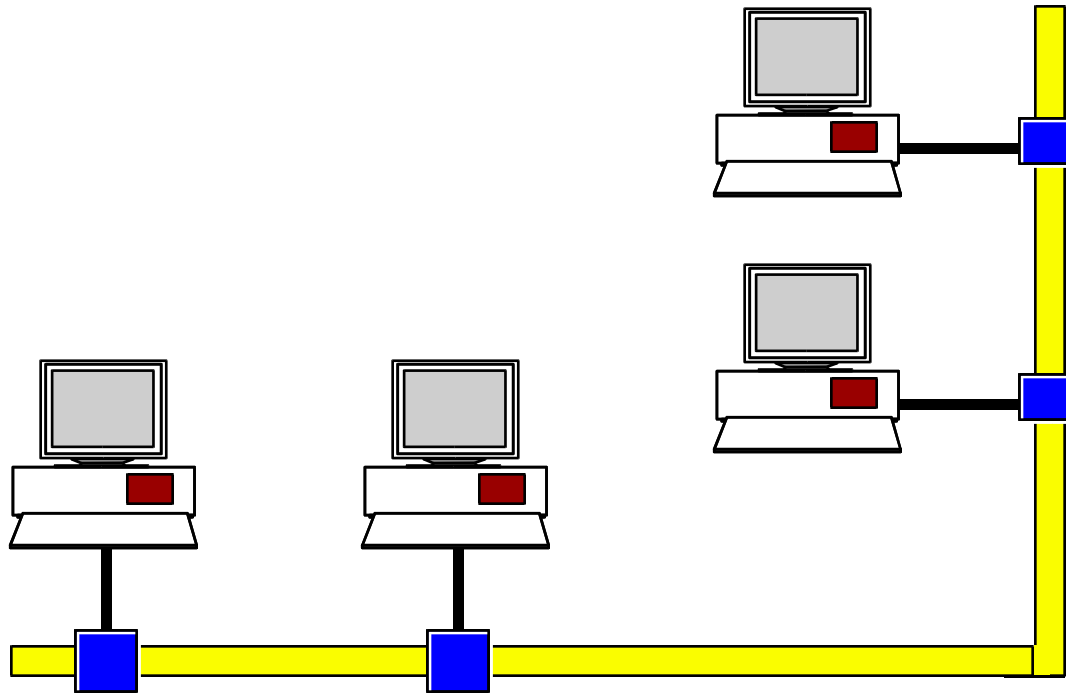
Organizacja	Adres Bloku
Cisco	0000Ch
DEC	08002B (et. al.)
IBM	08005A (et. al)
Sun	080020h
Proteon	000093h
Wellfleet	0000A2h

Powyżej przedstawiono kilka przykładów bloków adresowych przydzielonych przez IEEE. Kompletną listę tych adresów można znaleźć w najnowszej wersji „Assigned Numbers” RFC.

Adresy MAC w akcji



Założmy, że Joe Bloggs Inc. chce otrzymać adres wyznaczony globalnie i otrzymuje z IEEE 24-bitowy blok „200043”. Żadna inna organizacja nigdy nie dostanie tego samego bloku adresowego. Joe Bloggs tworzy interfejs Ethernetowy i oznacza pozostałe 24 bity, a następnie instaluje pełny adres w stałej pamięci (PROM lub PAL) na interfejsie. Teraz żaden inny interfejs sieci LAN (nawet przeznaczony dla Token Ring czy FDDI) nie będzie miał identycznego adresu jak Joe Bloggs.



Jeżeli zawsze bylibyśmy w stanie używać adresów wyznaczonych globalnie, moglibyśmy być pewni, że żadne dwie maszyny na świecie nie mają takiego samego adresu MAC. W tej chwili możesz myśleć, że adres MAC jest wszystkim czego potrzeba aby przesłać informacje pomiędzy dowolnymi dwoma komputerami na świecie. Niestety, z dwóch powodów nie jest to prawda. Pierwszym z nich jest *Adresowanie Lokalne*, zaś drugim *Skalowalność*.

MENU

1. Wstęp

2. Adresowanie warstwy MAC

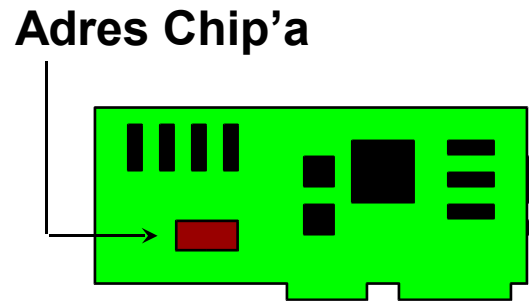
3. Adresowanie lokalne

4. Adresowanie warstwy sieciowej

5. Adresowanie warstwy transportowej

6. Podsumowanie

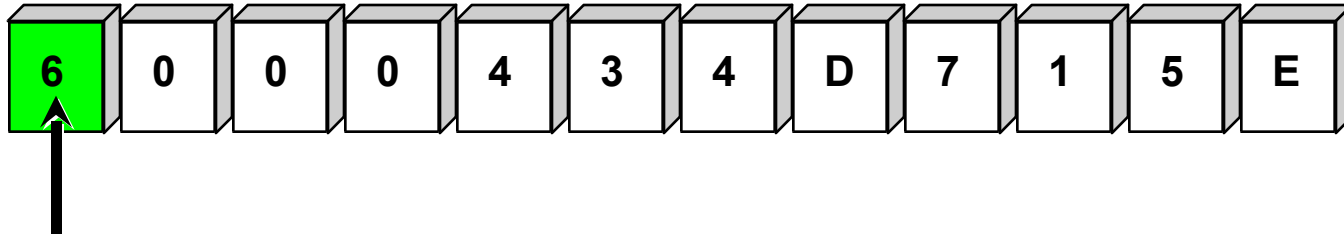
Adresowanie Lokalne – Jak ?



Jeśli adresy zarejestrowane przez IEEE są zainstalowane w każdej karcie LAN, jak możemy używać adresowania lokalnego ? Odpowiedź jest prosta. Kiedy chipset w interfejsie lan jest aktywny to czyta adres MAC z chipu, i przekazuje go oprogramowaniu sieciowemu. Oprogramowanie może opcjonalnie zamazać ten adres innym adresem który został wcześniej wprowadzony ręcznie albo (tak jak w przypadku sieci DECnet), został wygenerowany przez warstwę sieciową.

Większość nowoczesnych chipsetów LAN pozwala powielać adresy MAC i operować nimi równocześnie.

Adresowanie Lokalne – Dlaczego?



Reprezentacja binarna= 0110

G/L Bit

Dla lokalnego administrowania adresowaniem, ustawiliśmy bit G/L, aby w taki sposób "ostrzegać" inne stacje, że ten adres nie ma globalnego znaczenia.

Ale dlaczego mielibyśmy się trudzić używając lokalnego adresowania kiedy procedury IEEE gwarantują, że ten adres nigdy nie będzie duplikowany?

Nie ma jednoznacznej odpowiedzi na to pytanie, istnieje za to cały komplet opinii różnych producentów...

•Adresowanie Funkcjonalne IBM'a

Jeden z przypadków przedadresowywania dotyczy wyższego poziomu funkcjonalności SNA. IBM zdefiniował funkcjonalne adresowanie dla specyficznego urządzenia SNA i jest ono zaalokowane specyficzną grupą przedziałów adresów.

- Adresowanie Funkcjonalne IBM'a
- Adresowanie DECnet**

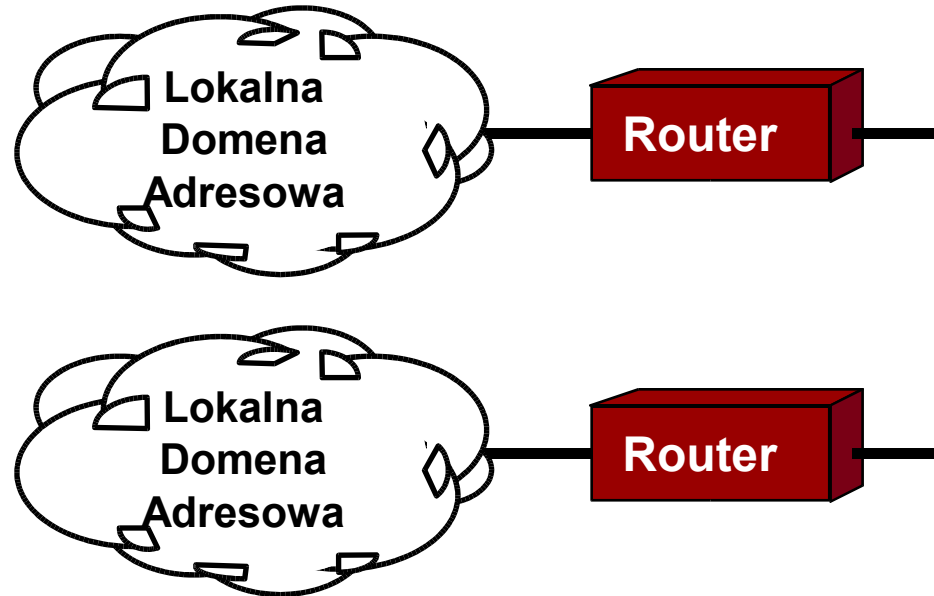
W węźle DECnet'a adres Warstwy Sieci, to jest adres wejściowy do węzła sieci, jest pobierany z adresu Warstwy MAC, który jest przepisywany z powrotem do interfejsu chipset'u.

Podobne procedury są zaadoptowane do innych protokołów.

- Adresowanie Funkcjonalne IBM'a
- Adresowanie DECnet
- Producenci niezarejestrowani**

Adres bloku IEEE jest drogi i powoduje dużo kłopotów administracyjnych przy jego przyporządkowywaniu. Niektórzy producenci nie zwracają sobie głowy rejestracją.

Adresowanie lokalne: skalowalność



Jeśli zaadoptowaliśmy lokalny adres administracji, jesteśmy zdolni do zbudowania sieci wewnątrz naszej własnej dziedziny kontroli. Ta dziedzina może obejmować cały budynek w którym pracujemy lub tylko piętro na którym nasza grupa robocza została umieszczona.

W celu połączenia lokalnego adresu dziedziny, bez obawy o zduplikowanie Adresu MAC, należy użyć Routerów.

Router'y tworzą swoje decyzje bazujące na Warstwowym Adresowaniu Sieciowym.

MENU

1. Wstęp

2. Adresowanie warstwy MAC

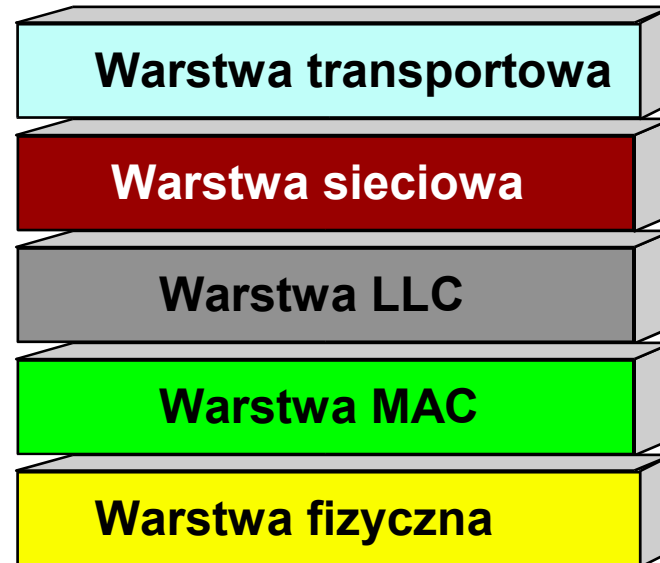
3. Adresowanie lokalne

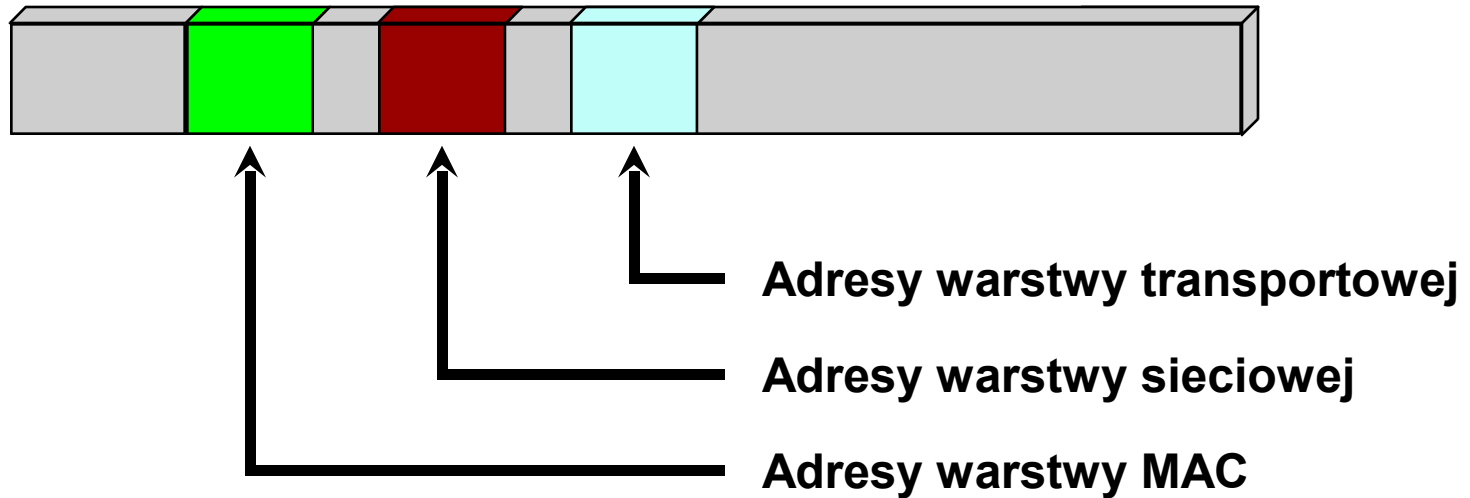
4. Adresowanie warstwy sieciowej

5. Adresowanie warstwy transportowej

6. Podsumowanie

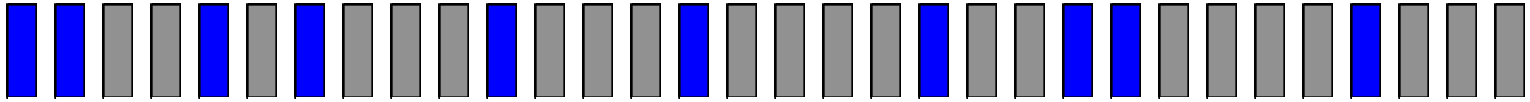
Adresowanie Warstwy Sieciowej





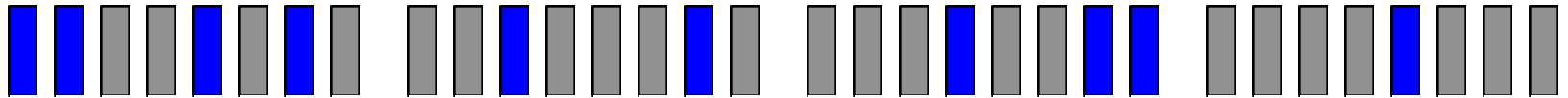
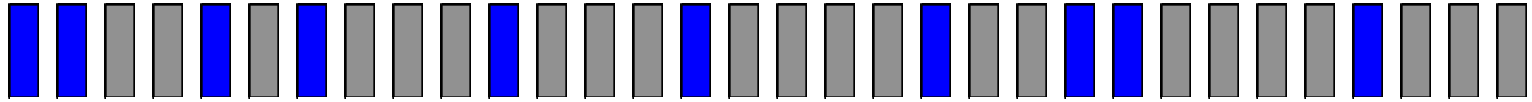
Adresy Warstwy Sieci znajdują się w środku Pola Danych, w obrębie ramki MAC'a.

UWAGA: Jest to podobne do konwersji Modelu OSI; dla struktury Warstwy N wszystkie adresowania w wyższych warstwach są traktowane jako dane z Warstwy N. Adresy Warstwy 3 są więc traktowane jak dane Warstwy 2, a adresy Warstwy 4 są traktowane jak dane Warstwy 2 i 3, itd.



Dla IP struktura adresu jest relatywnie prosta.

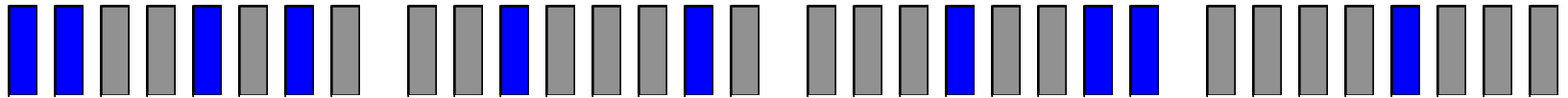
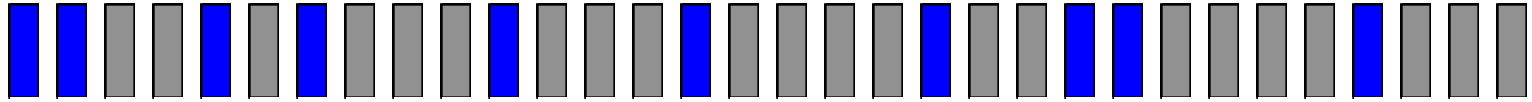
Bierzemy 32 bitowy adres.



Dla IP struktura adresu jest relatywnie prosta.

Bierzemy 32 bitowy adres.

Dzielimy to przez 4, 8-bitowe pole.

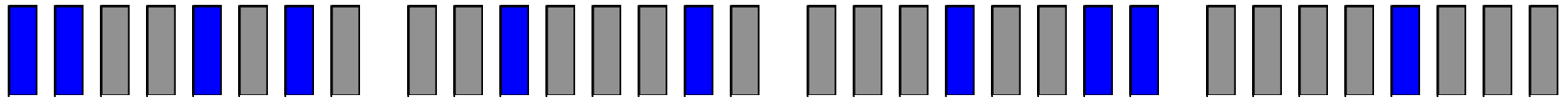
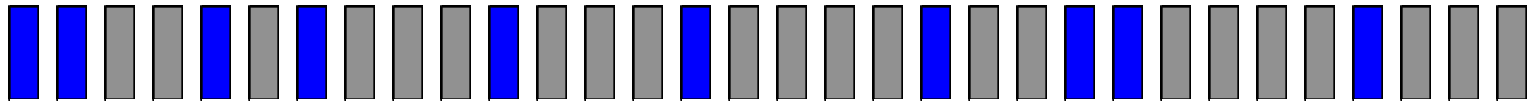
**202****34****19****8**

Dla IP struktura adresu jest relatywnie prosta.

Bierzemy 32 bitowy adres.

Dzielimy to przez 4, 8-bitowe pole.

Wtedy przeliczamy oddzielnie każde pole w liczbach dziesiętnych.



202 . 34 . 19 . 8

Dla IP struktura adresu jest relatywnie prosta.

Bierzemy 32 bitowy adres.

Dzielimy to przez 4, 8-bitowe pole.

Wtedy przeliczamy oddzielnie każde pole w liczbach dziesiętnych.

I piszemy te liczby z indywidualnymi polami-bitami oddzielonymi kropkami. Metoda ta jest nazwana kropkową notacją dziesiętną.

202 . 34 . 19

. 8

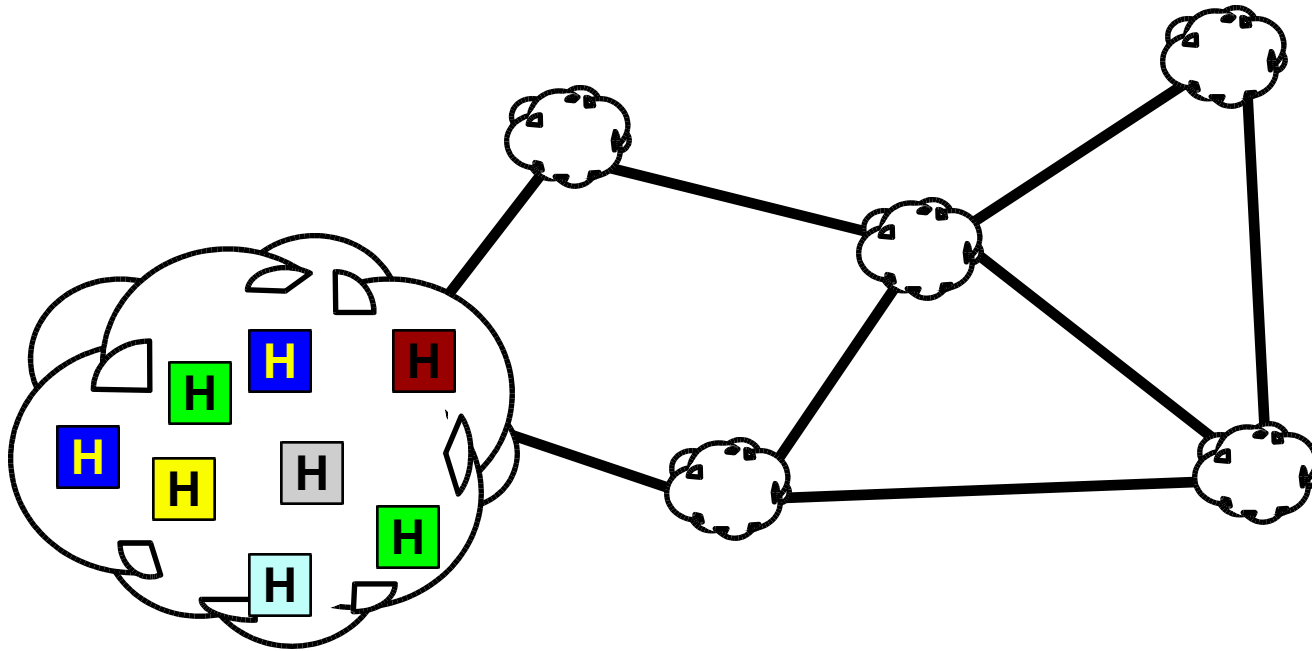
Network ID

Host ID

Adres IP ma dodatni element strukturalny. Część adresu jest zarezerwowana do wskazywania Network ID, podczas gdy pozostała część adresu reprezentuje Host ID. Relatywna wielkość pola Network i Host ID zmienia się w zależności od klasy adresu IP.

Używając Network ID, router'y są w stanie wybierać bezpośrednio trasę obejmującą wiele hop-ów, aż osiągną sieć właściwą.

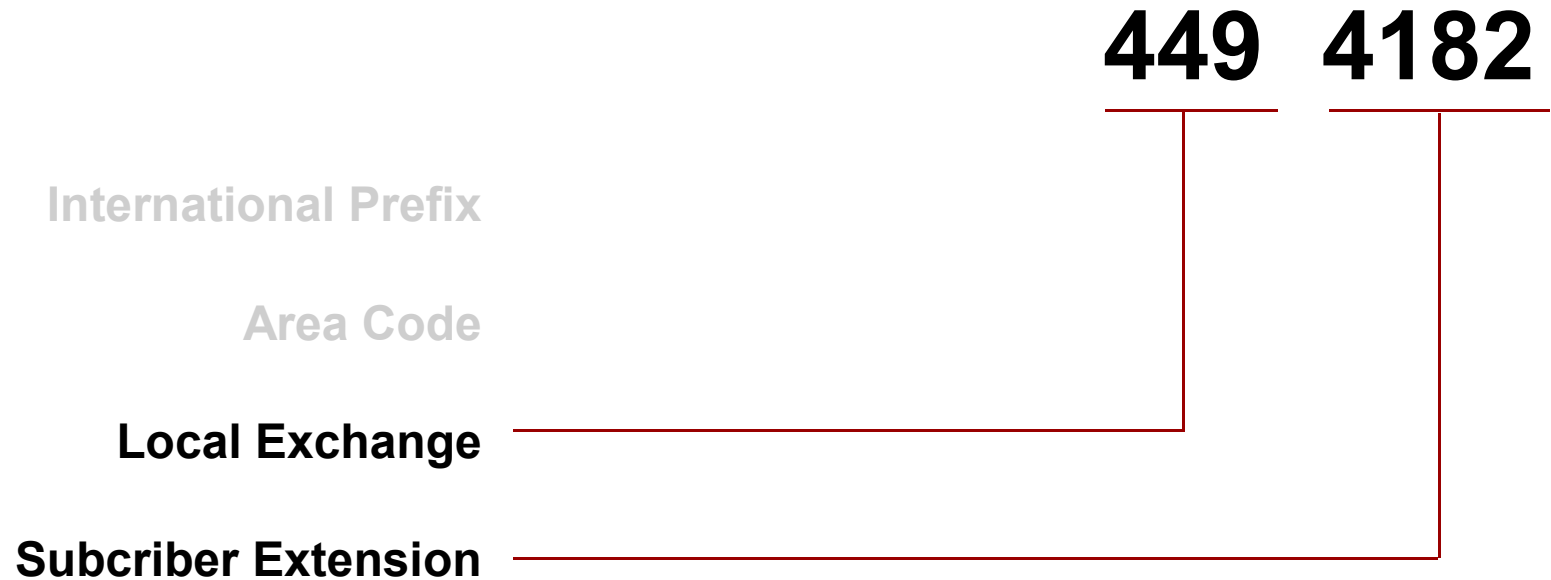
Kończący router w ścieżce używa Host ID do wykonania Rozdzielczości Adresu, znajdując koniec poprawności adresu MAC, host'u docelowego.



W przypadku ogólnosiwiatowego Internetu istnieją miliony aktualnie przyłączonych hostów, a tempo przyłączania wciąż rośnie. Poza hierarchiczną formą adresowania, pracujące w Internecie routery muszą pamiętać gdzie każdy indywidualny host jest umiejscowiony.

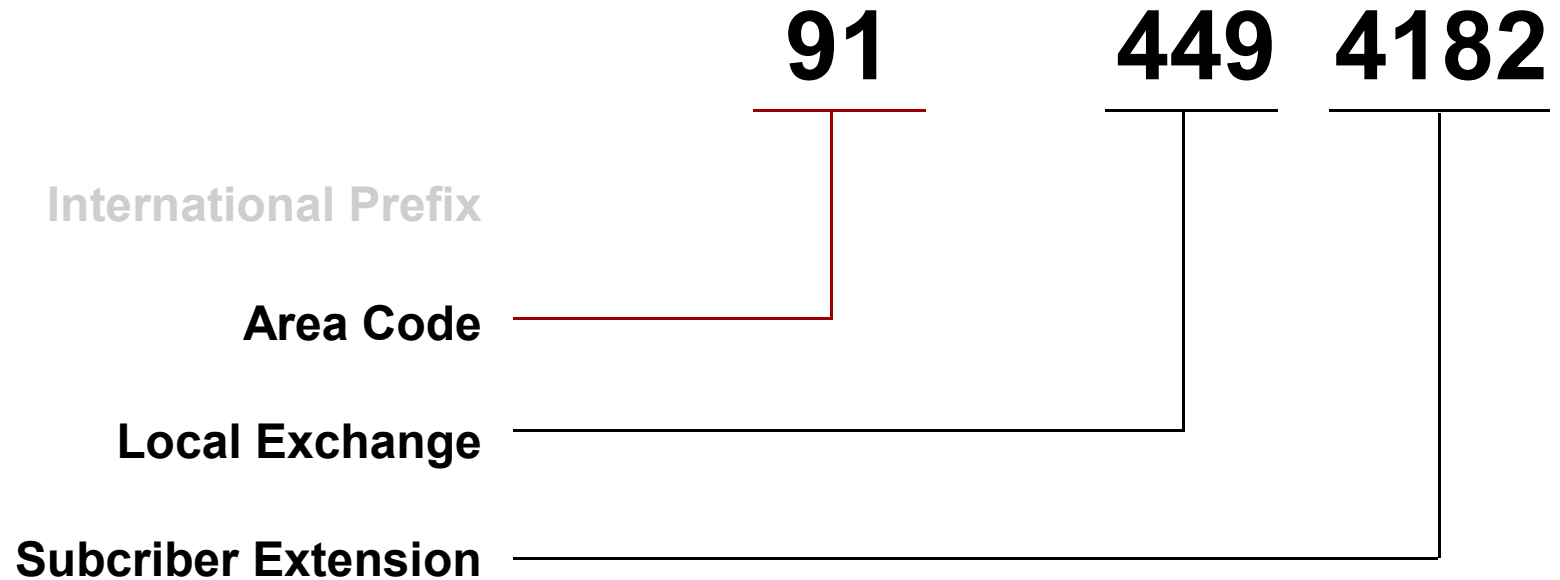
W hierarchicznym adresowaniu każdy router potrzebuje tylko drogi do hostu gdzie jest połączony z siecią za pomocą routera.

Hierarchiczne adresowanie jest używane w innej globalnej sieci - Systemie Telefonicznym.



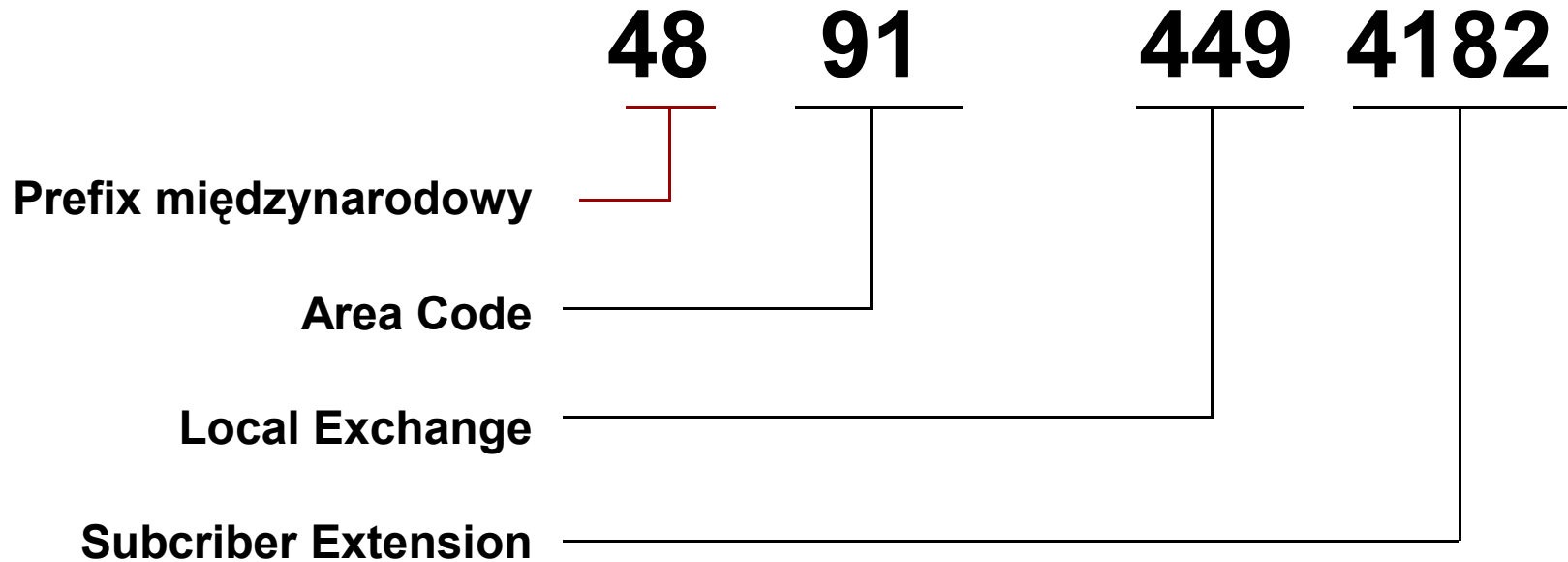
To jest numer telefonu w Politechnice Szczecińskiej. Posiada 7 cyfr które pozwalają na zaadresowanie 10 milionów indywidualnych użytkowników. To dużo, ale nie wystarczająco do narodowego bądź międzynarodowego planu adresowania.

Nawet ten siedmiocyfrowy numer jest aktualnie dzielony na rozszerzenie lokalne i abonenckie.

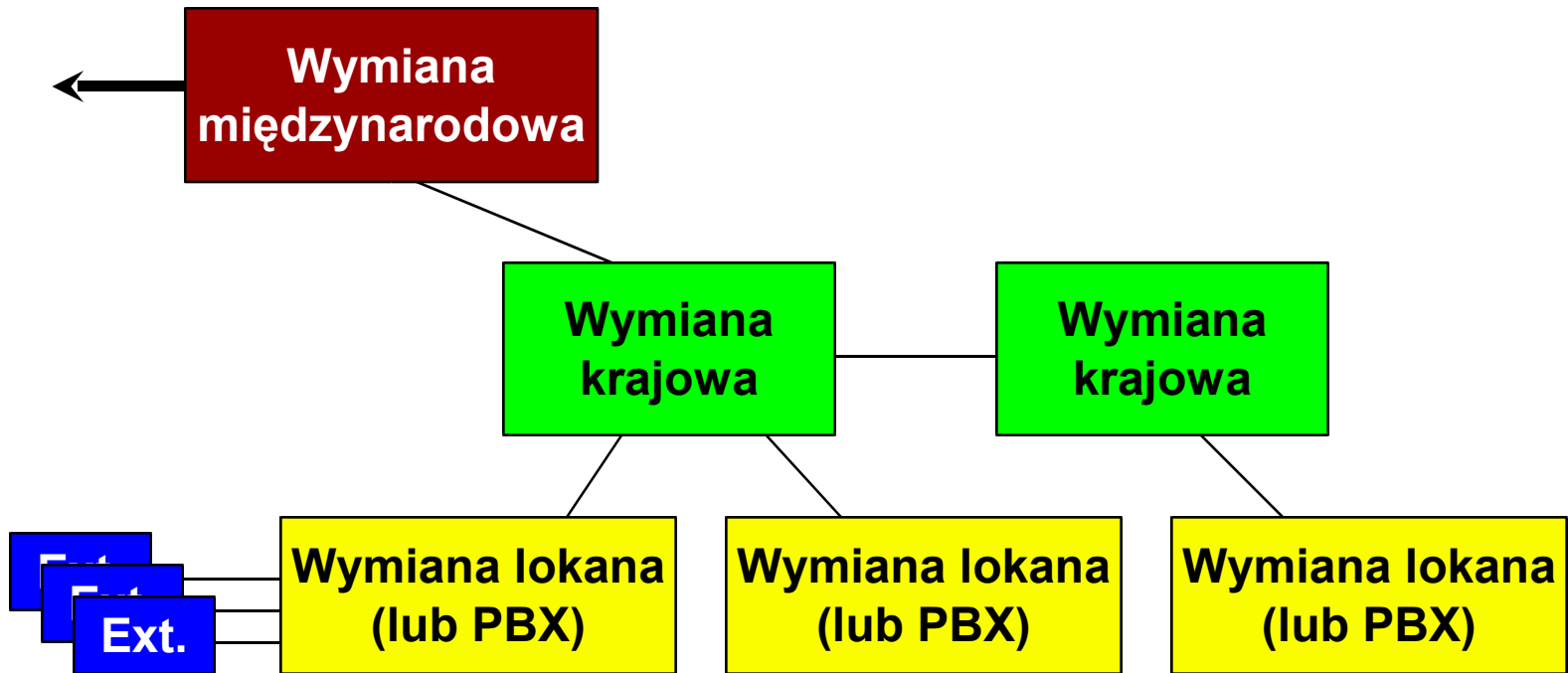


W Polsce dla zwiększenia schematu numerowania do numerów dodaje się kod rejonu.

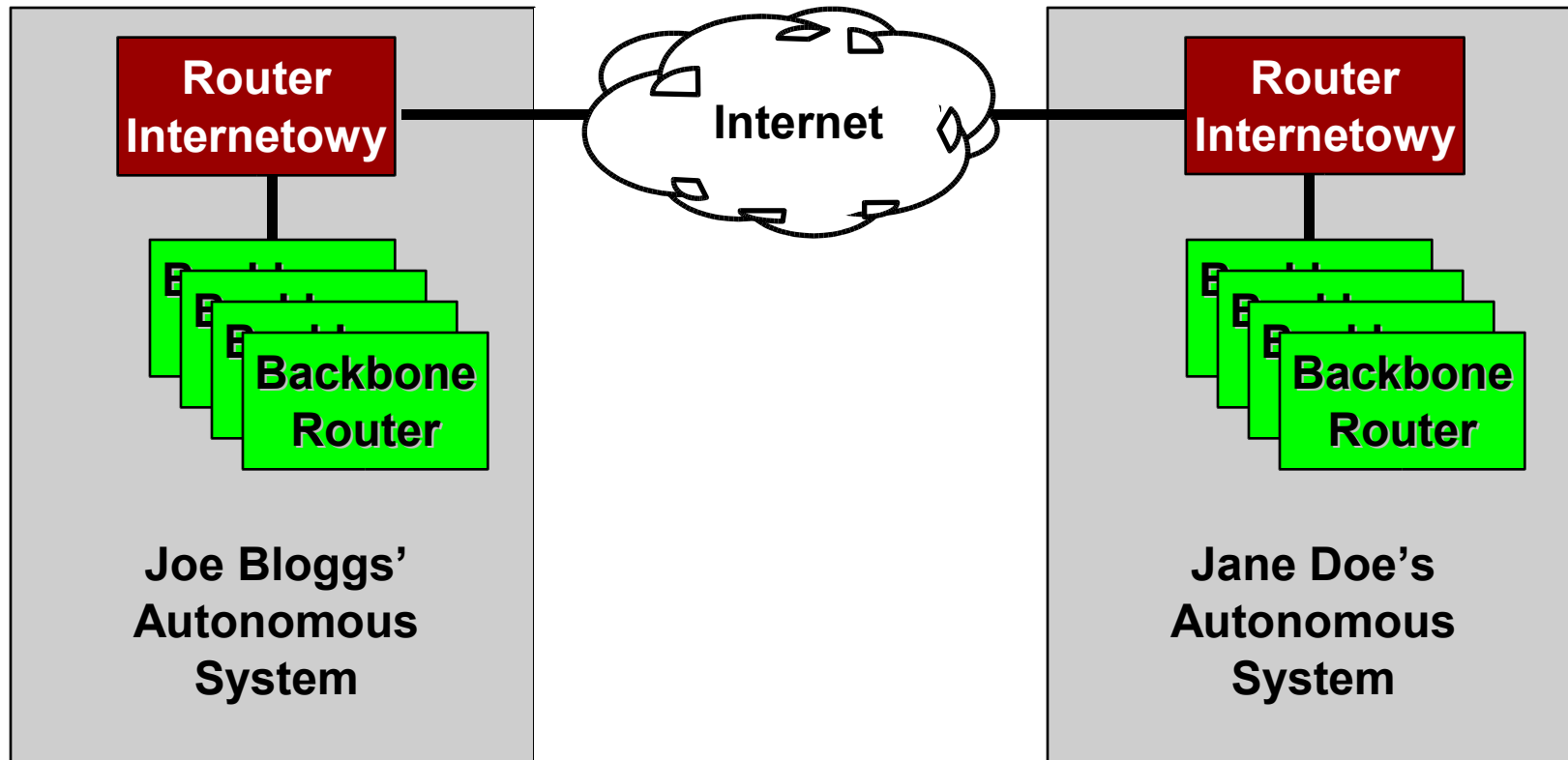
Kody rejonu są 2 cyfrowe.



Jeśli chcemy wybrać ten numer z poza Polski musimy dodać International Prefix. Dla USA jest to 1, dla Wielkiej Brytanii 44, dla Niemiec 49, a dla Polski 48.



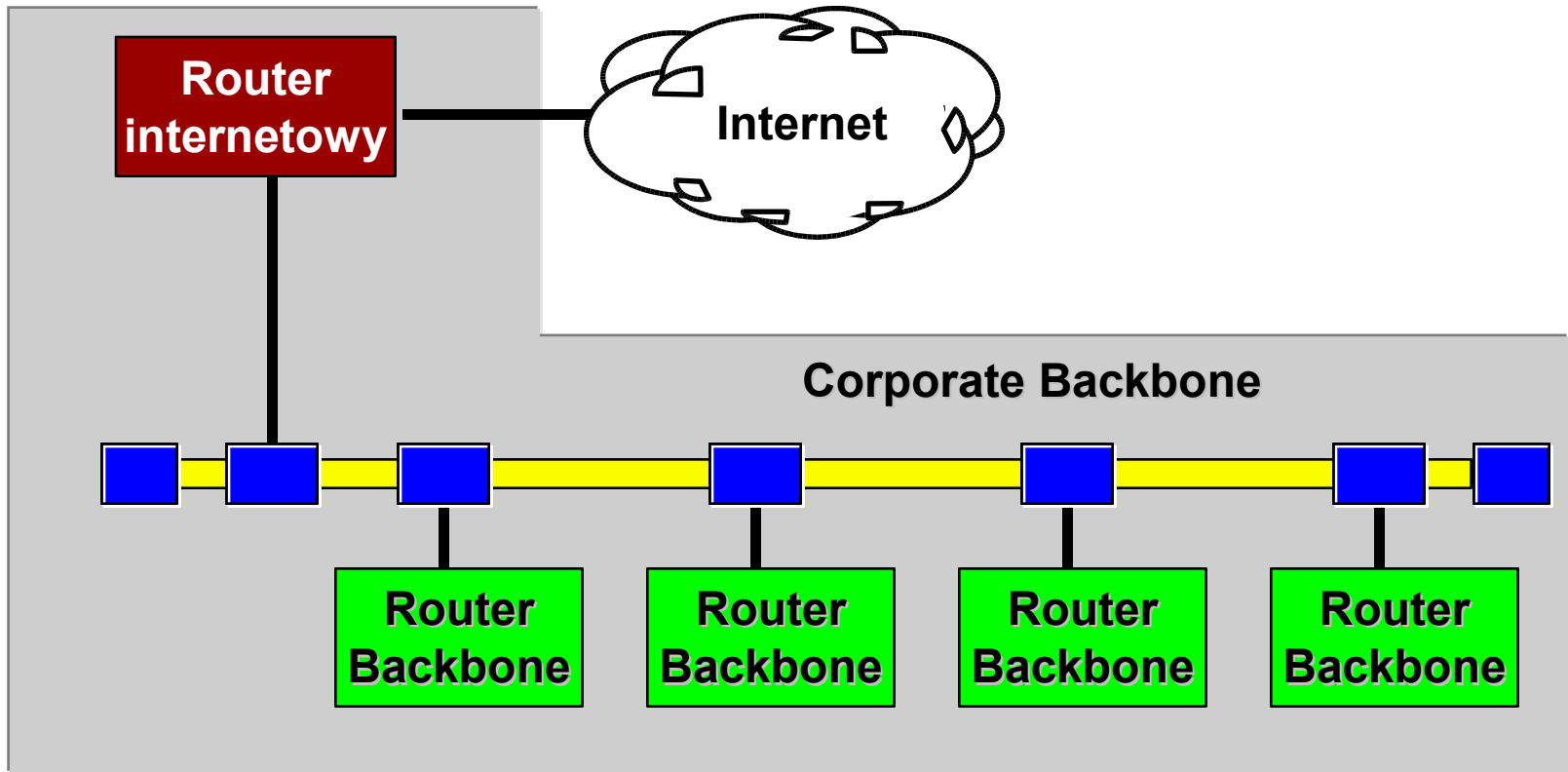
Taki hierarchiczny schemat numerowania jest niezbędny w systemie telefonicznym. Izolując pole na indywidualny numeru telefonu osiągamy wiele korzyści. Po pierwsze, użytkownicy systemu muszą pamiętać tylko siedem cyfr z każdego lokalnego numeru. Po drugie, narodowy system telekomunikacji może adoptować każdą rozsądną wewnętrzną strukturę, którą chce wykorzystać do numerowania. W ten sposób system jest "zabezpieczony" przed duplikowaniem adresu i pomyłkami związanymi z International Prefix. Ponadto każda centrala telefoniczna potrzebuje wiedzieć tylko o adresie poniżej siebie w hierarchii.



Chciałbym skoncentrować się na tym finałowym wykorzystaniu, ponieważ jest to podstawowy powód używania adresowania hierarchicznego w sieciach danych.

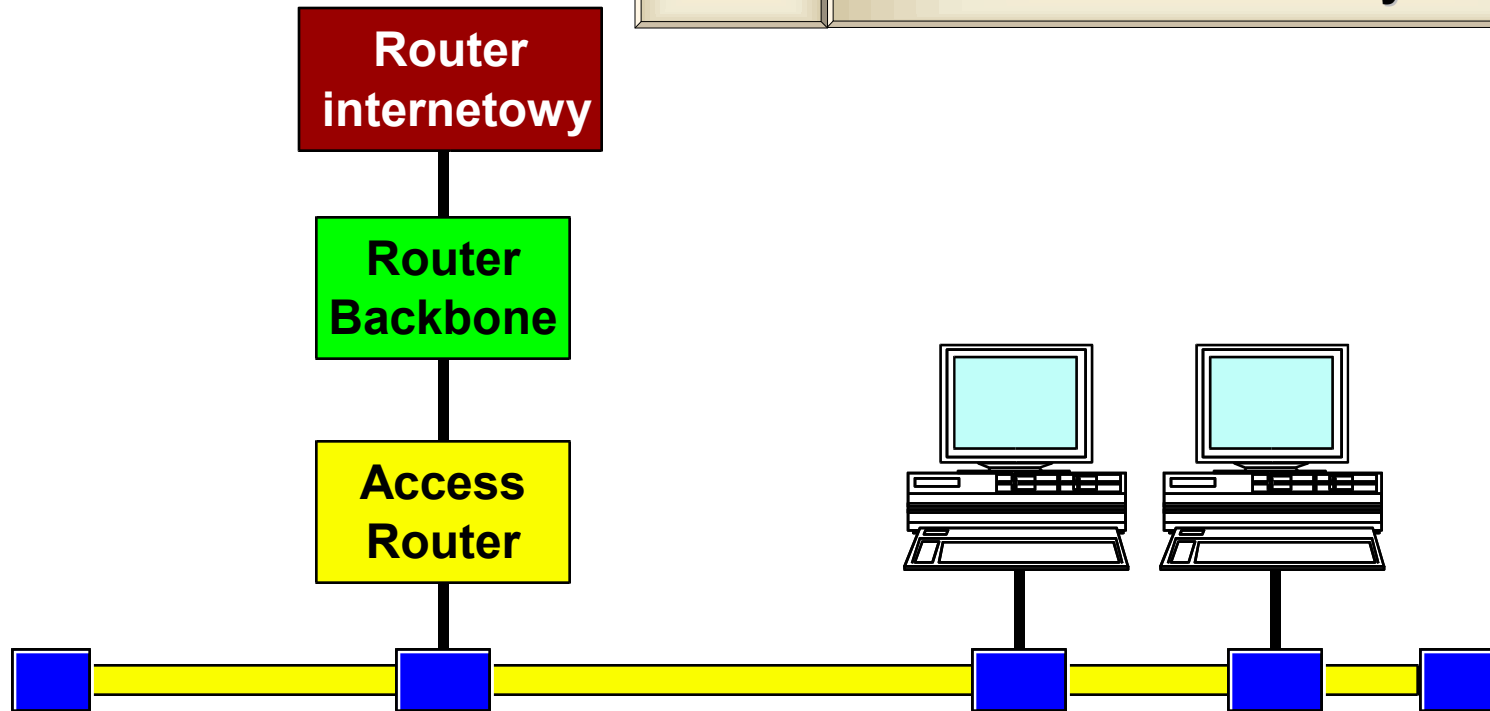
Najbardziej oczywistym dowodem adresowania hierarchicznego jest używanie go przez Internet dla zabezpieczenia jednego abonenta przed błędem routingu stworzonego przez innego abonenta. Ta koncepcja jest, oczywiście, Systemem Autonomicznym (AS).

Przyporządkowane Internetowi routery muszą rozpoznawać koncepcję AS i muszą obsługiwać lokalny routing poprzez protokoły, takie jak RIP albo OSPF.



Następny poziom w hierarchii to Backbone Routers używany do budowy Corporate Backbone.

Router'y Backbone operują wewnątrz AS, ale potrzebują utrzymywać dużą tabelę routingu zależną od wielkości indywidualnej organizacji.



Natomiast niżej w poziomie routerów hierarchicznych znajdują się Access Routers. Te urządzenia są dużo mniejsze, mniej wydajne, ale tańsze od swego złożonego kuzyna.

Access Routers mogą być używane do połączenia z pojedynczą grupą roboczą LAN w Corporate Backbone i nie potrzebują utrzymywania złożonej tablicy routingu.

Bez względu na typ użytego router'a, wszystkie te urządzenia tworzą swoje decyzje przełączania bazujące na Adresowaniu Warstwy Sieciowej, które już opisywałem.

MENU

1. Wstęp

2. Adresowanie warstwy MAC

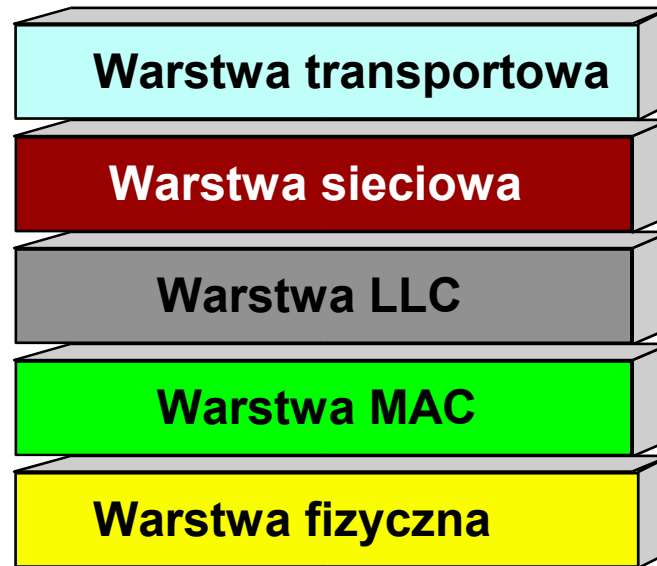
3. Adresowanie lokalne

4. Adresowanie warstwy sieciowej

5. Adresowanie warstwy transportowej

6. Podsumowanie

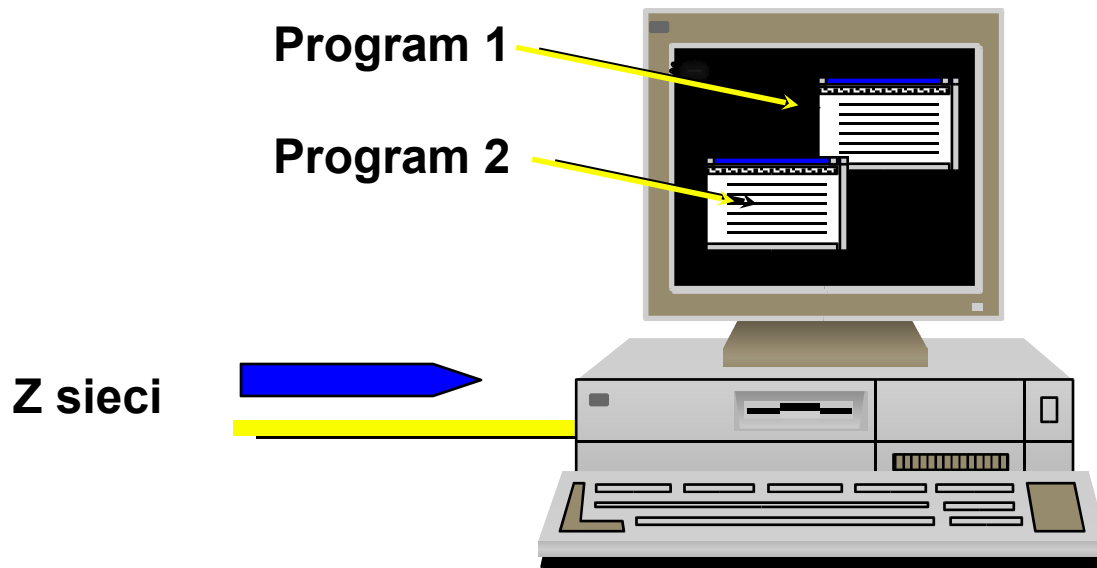
Adresowanie Warstwy Transportowej



Na koniec chciałbym przyjrzeć się adresowaniu Warstwy Transportowej.

Reasumując możemy powiedzieć, że adresowanie Warstwy MAC pozwala nam przesyłać wiadomość między dwoma host'ami poprzez wspólne medium.

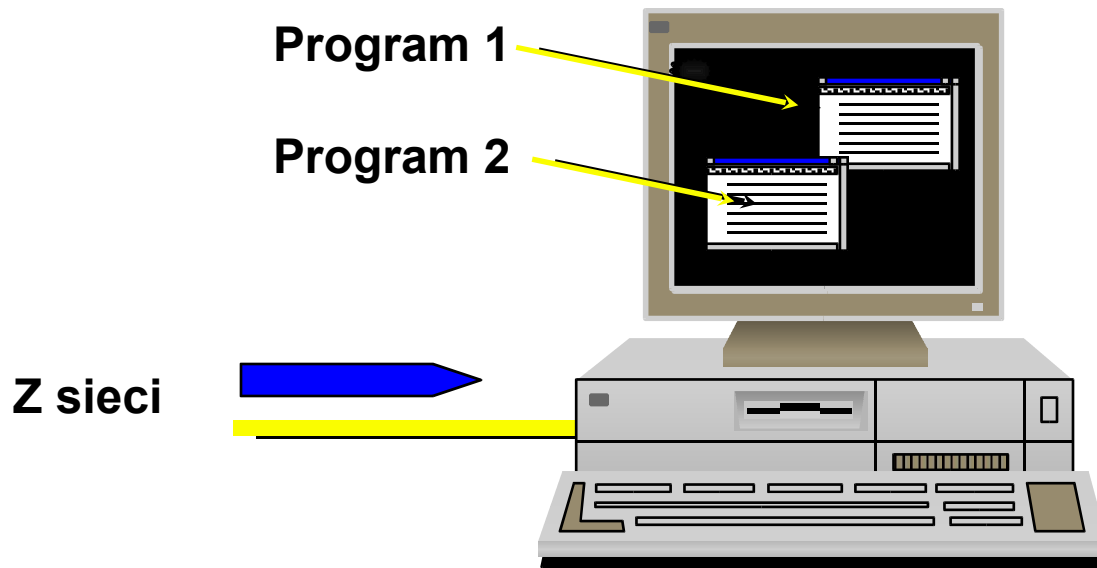
Adresowanie Warstwy Sieciowej rozszerza umiejętność komunikacji tak, iż możemy przesyłać dane pomiędzy sieciami lokalnymi. Adresowanie Warstwy Sieciowej jest także skalowalne ponieważ administrator sieci może wybrać adres w sposób hierarchiczny.



Możemy zaobserwować nagłówek ramki LAN przychodzącej do PC z sieci. Występuje tutaj następujący problem.

W PC'cie mamy uruchomione dwa programy komunikacyjne - Program 1 i Program 2.

Adresy MAC i IP na PC identyfikują jedynie maszynę, a nie program z którego paczka mogłaby być wysłana.



Do rozróżnienia między tymi programami używamy Adresowanie Warstwy Transportowej. Trzeba zaznaczyć, iż używanie adresu IP nie jest rzeczywiście stosowane w warstwie aplikacji z paru przyczyn. Po pierwsze musisz rejestrować każdy program z adresem IP kiedy go uruchamiasz. Ponieważ adres IP często przyznawany jest ręcznie, Administrator Sieci musi ograniczać liczbę programów, które możesz uruchomić z maszyny, więc może być zmuszony wcześniej przypisać twój adres IP. Na nieszczęście jest mało adresów IP które robią to w praktyce.

MENU

1. Wstęp

2. Adresowanie warstwy MAC

3. Adresowanie lokalne

4. Adresowanie warstwy sieciowej

5. Adresowanie warstwy transportowej

6. Podsumowanie

Warstwa MAC

Warstwa Fizyczna

Adresy Warstwy MAC są używane do przyznawania prywatnej komunikacji między specyficznymi hostami, mimo że dzieli ten sam kanał komunikacji z wieloma innymi systemami.

Warstwa Sieciowa

Warstwa MAC

Warstwa Fizyczna

Adresowanie Warstwy Sieciowej przyznaje komunikację między hostami bez względu na typ sieci, która używa do połączeń tego stanowiska sieciowego.

Warstwa transportowa

Warstwa Sieciowa

Warstwa MAC

Warstwa Fizyczna

Adresowanie Warstwy Transportowej przyznaje specyficzną aplikację uruchomioną w hoście komputera w celu komunikowania z równoważnym procesem uruchomionym w innym hoście.

Koniec

Inne prezentacje znajdują się na stronie:

[**http://kbogu.man.szczecin.pl**](http://kbogu.man.szczecin.pl)