SIECI KOMPUTEROWE - Wykłady

Opracowano z wykorzystaniem materiałów firmy CISCO

Wykład I – zagadnienia wstępne i definicje podstawowe

---

1. Zagadnienia wstępne

1.1. Charakterystyka przedmiotu
1.2. Warunki zaliczenia
1.3. Materiały źródłowe

2. Podstawowy podział sieci komputerowych

2.1. Podział ogólny sieci komputerowych ze względu na obszar:

- **lokalne** sieci komputerowe LAN *(Local Area Network)*,
- **metropolitalne** sieci komputerowe MAN *(Metropolitan Area Network)*,
- **rozlegle** sieci komputerowe WAN *(Wide Area Network)*.

Przykładem takiej sieci jest *Internet globalny*.

2.2. Technologie sieci rozległych:

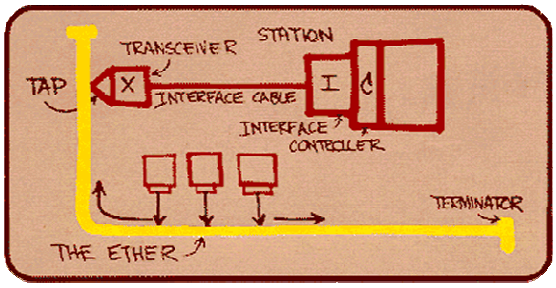
- PPP (*Poin-to-Point Protocol*),
- ISDN (*Integrated Services Digital Network*),
- X.25,
- ADSL (*Asymmetric Digital Subscribed Line*),
- DSL (*Digital Subscribed Line*),
- Frame Relay,
- ATM (*Asynchronus Transfer Mode*).

2.3. Technologie sieci lokalnych

- Arcnet
- Token Ring
- FDDI
- **Ethernet**

2.4. Odmiany technologii przewodowej Ethernet ze względu na przepustowość:

- 4 Mb/s
- **10 Mb/s**
- **100 Mb/s (fast Ethernet)**
- **1 Gb/s**
- **10 Gb/s**
- **40, 100 Gb/s**



Szkic Roberta Metcalfe'a

3. Niektóre podstawowe pojęcia terminologii sieciowej

3.1. Sieć komputerowa - struktura złożona ze stacji sieciowych, połączonych urządzeniami sieciowymi przy pomocy odpowiedniego medium. Każda stacja sieciowa musi posiadać swój **unikalny adres.**

3.2. Rozważane będą sieci komputerowe **pakietowe.**

3.3. Pakiet: najmniejsza porcja informacji transmitowana pomiędzy stacjami sieciowymi (np. 1000 B). Pakiety stanowią zazwyczaj elementy większych całości zwanych ***strumieniami***.

3.4. Multipleksacja – proces zmierzający do transmisji wielu wyodrębnionych strumieni pakietów pomiędzy dwoma stacjami sieciowymi.

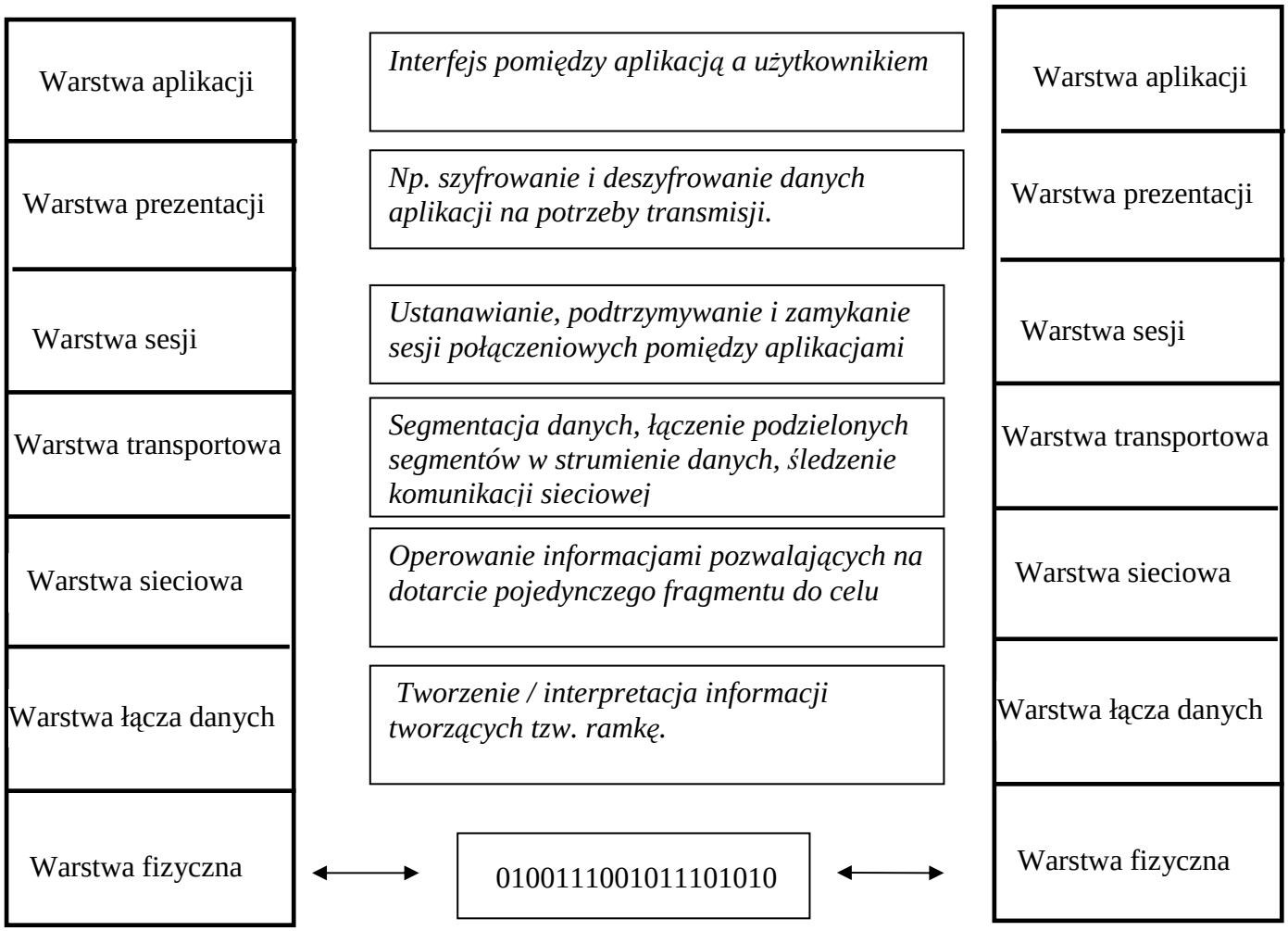
3.5. Intersieć (Internet): składa się z wielu sieci połączonych **routerami**. Aby możliwa była transmisja danych w Internecie, każda sieć składowa musi mieć swój unikalny adres, zaś w ramach danej sieci każda jej stacja sieciowa.

3.6. Protokół - zestaw ściśle określonych procedur wysyłania i odbierania pakietów,

3.7. Inne pojęcia: **Intranet, Extranet,** modele sieciowe *klient-serwer*, *peer-to-peer*

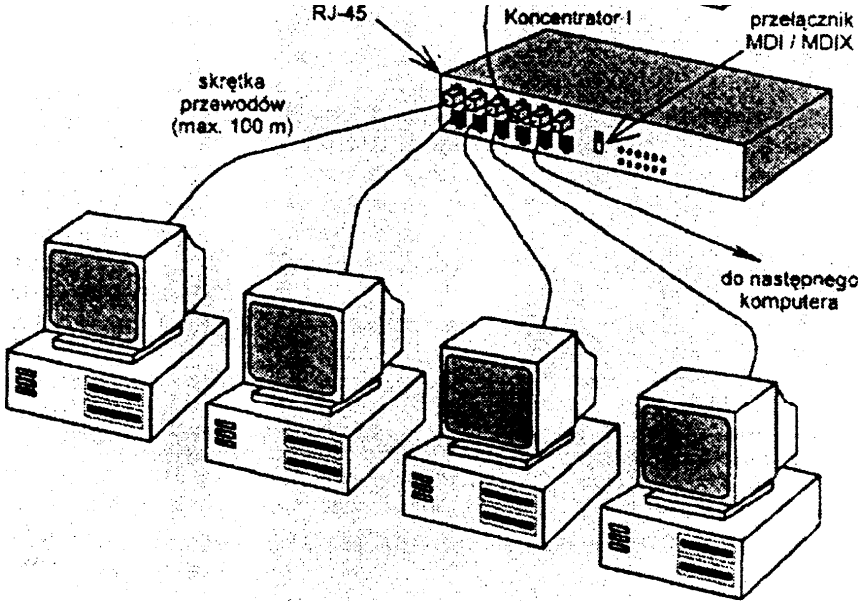
4. Architektura systemów otwartych - sieciowy model odniesienia OSI (*Open System Interconnection*).

Model abstrakcyjny, opisujący mechanizmy wymiany pakietów od aplikacji w systemie jednej stacji sieciowej do aplikacji w innej.



Wykład II – wybrane aspekty technologii Ethernet

1. Gwiazda jako elementarna topologia Ethernet



2. Format adresu sprzętowego (II warstwa OSI). Rola adresów fizycznych w komunikacji sieciowej.

2.1 Format adresu (wymuszony przez *IEEE*)

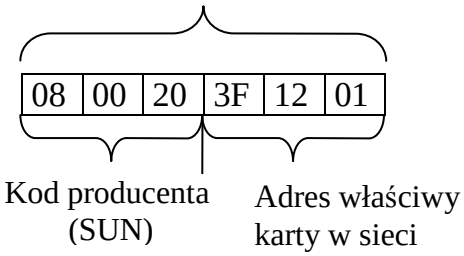
Adres fizyczny ETHERNET (*NIC*, interfejsy przełączników, routerów,) to 48 bitowa liczba. W odniesieniu do modelu OSI jest to adres funkcjonujący w warstwie II. Inna nazwa to adresy warstwy ***MAC*** (z ang. *Media Access Control*), lub po prostu adresy ***MAC***. Dla ułatwienia adres zapisywany jest poprzez zastosowanie systemu szesnastkowego (skrócenie zapisu).

2.2. Rodzaje adresów fizycznych:

- unikalne (sieciowe),

Przykład:

Adres kompletny - schemat wymuszony przez *IEEE*

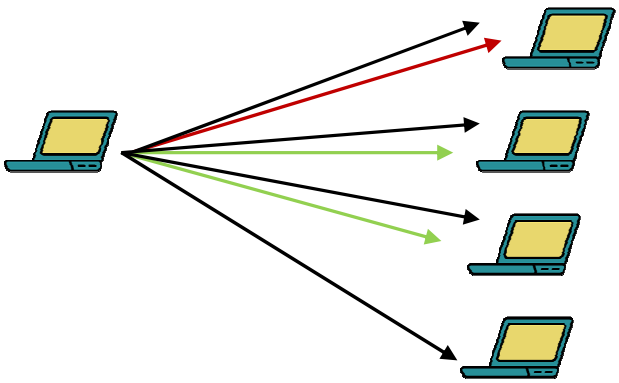


- rozgłoszeniowy: FF:FF:FF:FF:FF:FF

- grupowe: 01-00-5E-… lub 01-00-5F-…, 33:33:FF-…. (wykorzystywane przez protokoły warstw wyższych)

2.3. Modele komunikacji sieciowej

unicast, anycast, multicast



2.4. Rola adresów fizycznych.

Adresy fizyczne *MAC* unikalne i rozgłoszeniowe wykorzystywane są przez protokoły warstwy II w urządzeniach sieciowych (*NIC*, przełączniki, routery, AP) w rozmaitych aspektach funkcjonowania. Przykładowo, w kartach sieciowych *NIC* stacji docelowych, na ich podstawie podejmowana jest decyzja, czy pakiet może być przekazany do dalszego przetwarzania przez warstwy wyższe, czy też odrzucony. Poszczególne aspekty znaczenia adresów *MAC* zostaną poruszone w kolejnych wykładach.

2.5. Idea mechanizmu enkapsulacji (kapsułkowania) i dekapsulacji

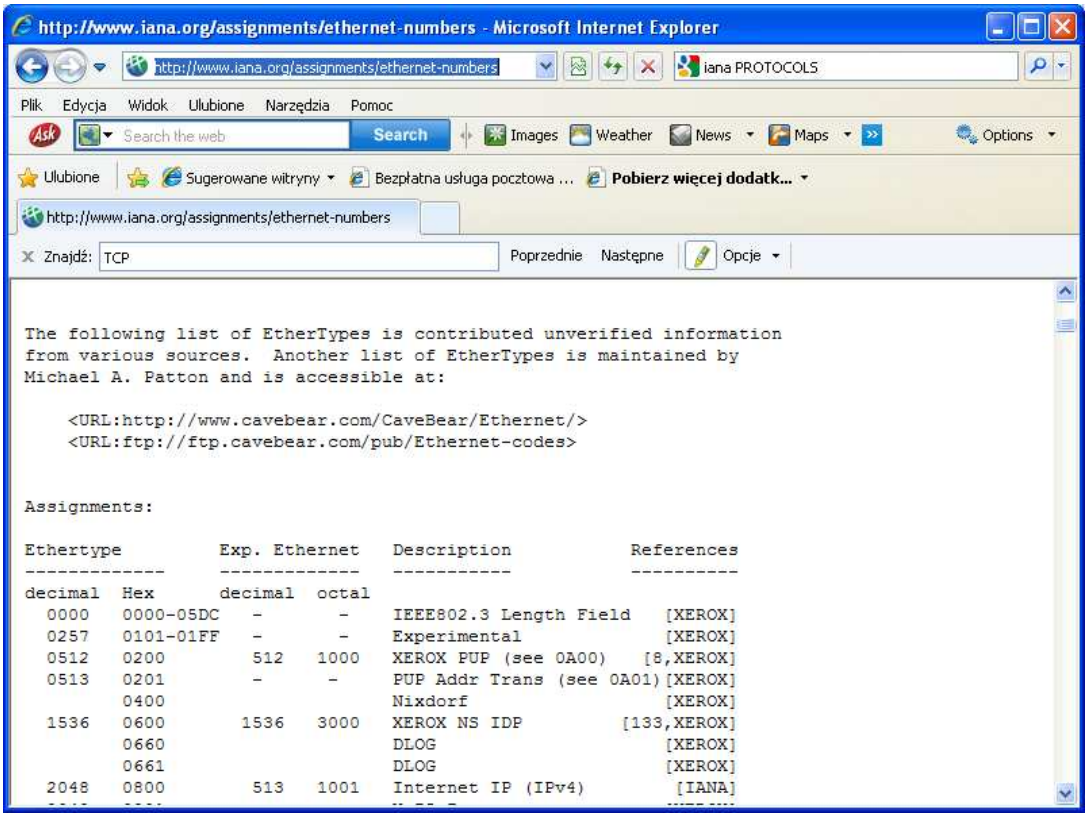
Mechanizm polega na dodawaniu (kapsułkowanie) lub usuwaniu (dekapsułkowanie) informacji do danych (tworzenie nowego lub usuwanie przeanalizowanego nagłówka) przez protokoły kolejnych warstw OSI. W wyniku kapsułkowania, za pomocą protokołów warstwy II (podwarstwy *MAC*) powstaje tzw. **ramka Ethernet.** Ruch sieciowy w sieciach Ethernet to ruch ramek. Ramka podlega dekapsulacji na stacjach docelowych.

Ogólny schemat ramki Ethernet

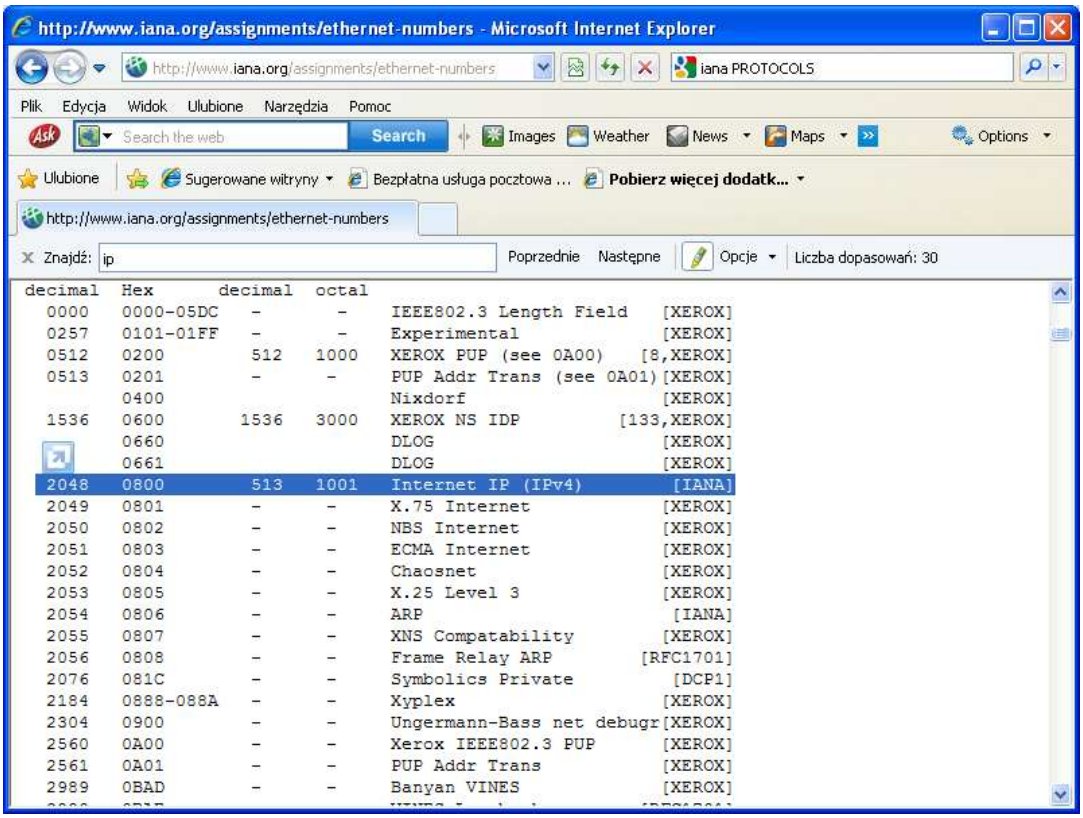
Pierwotny standard : *IEEE* 802.3: min. 64B, max. 1518 B
IEEE 802.3ac: max. 1522 B (Ethernet II)

Zawartość nagłówka (w następującej kolejności):

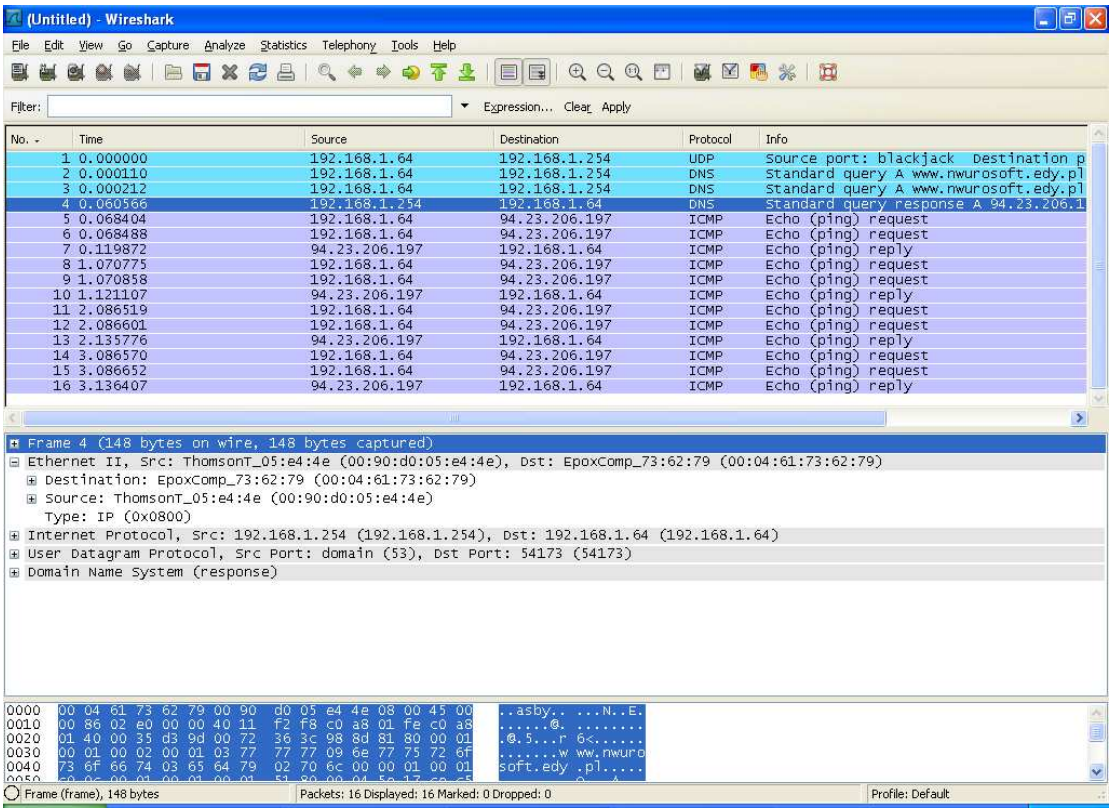
1. Preambuła (*Synchronicity*) - 7 B – sygnał identyfikujący ramkę Ethernet (np. po stanie bezczynności)
2. SFD (*Start Frame Delimiter*) - 1B – sygnalizuje, że następny bajt jest początkiem pola docelowego MAC
3. MAC docelowy – 6B
4. MAC źródła – 6B
5. Długość – 2B – określa długość pola Dane lub Typ protokołu dla Danych Jeżeli >=600h to oznacza Typ protokołu - liczba zdefiniowana przez *IANA:* http://www.iana.org/assignments/ethernet-numbers




```
The following list of EtherTypes is contributed unverified information
from various sources.  Another list of EtherTypes is maintained by
Michael A. Patton and is accessible at:

    <URL:http://www.cavebear.com/CaveBear/Ethernet/>
    <URL:ftp://ftp.cavebear.com/pub/Ethernet-codes>


Assignments:

Ethertype          Exp. Ethernet   Description           References
-------------      -------------   -----------           ----------
decimal  Hex       decimal  octal
  0000   0000-05DC   -        -    IEEE802.3 Length Field    [XEROX]
  0257   0101-01FF   -        -    Experimental              [XEROX]
  0512   0200         512    1000   XEROX PUP (see 0A00)    [8,XEROX]
  0513   0201         -      -      PUP Addr Trans (see 0A01)[XEROX]
         0400                       Nixdorf                 [XEROX]
  1536   0600        1536    3000   XEROX NS IDP          [133,XEROX]
         0660                       DLOG                    [XEROX]
         0661                       DLOG                    [XEROX]
  2048   0800         513    1001   Internet IP (IPv4)        [IANA]
```




```
decimal  Hex       decimal  octal
  0000   0000-05DC   -        -    IEEE802.3 Length Field    [XEROX]
  0257   0101-01FF   -        -    Experimental              [XEROX]
  0512   0200         512    1000   XEROX PUP (see 0A00)    [8,XEROX]
  0513   0201         -      -      PUP Addr Trans (see 0A01)[XEROX]
         0400                       Nixdorf                 [XEROX]
  1536   0600        1536    3000   XEROX NS IDP          [133,XEROX]
         0660                       DLOG                    [XEROX]
         0661                       DLOG                    [XEROX]
  2048   0800         513    1001   Internet IP (IPv4)        [IANA]
  2049   0801         -      -      X.75 Internet           [XEROX]
  2050   0802         -      -      NBS Internet            [XEROX]
  2051   0803         -      -      ECMA Internet           [XEROX]
  2052   0804         -      -      Chaosnet                [XEROX]
  2053   0805         -      -      X.25 Level 3            [XEROX]
  2054   0806         -      -      ARP                       [IANA]
  2055   0807         -      -      XNS Compatability       [XEROX]
  2056   0808         -      -      Frame Relay ARP        [RFC1701]
  2076   081C         -      -      Symbolics Private         [DCP1]
  2184   0888-088A    -      -      Xyplex                  [XEROX]
  2304   0900         -      -      Ungermann-Bass net debugr[XEROX]
  2560   0A00         -      -      Xerox IEEE802.3 PUP     [XEROX]
  2561   0A01         -      -      PUP Addr Trans          [XEROX]
  2989   0BAD         -      -      Banyan VINES            [XEROX]
```



6. Dane i wypełnienie 46-1500B, jeżeli Dane<46 B to są dodawane „sztucznie” dodatkowe bajty.
7. FCS – 4 B – sekwencja kontrolna ramki (algorytm *CRC*)

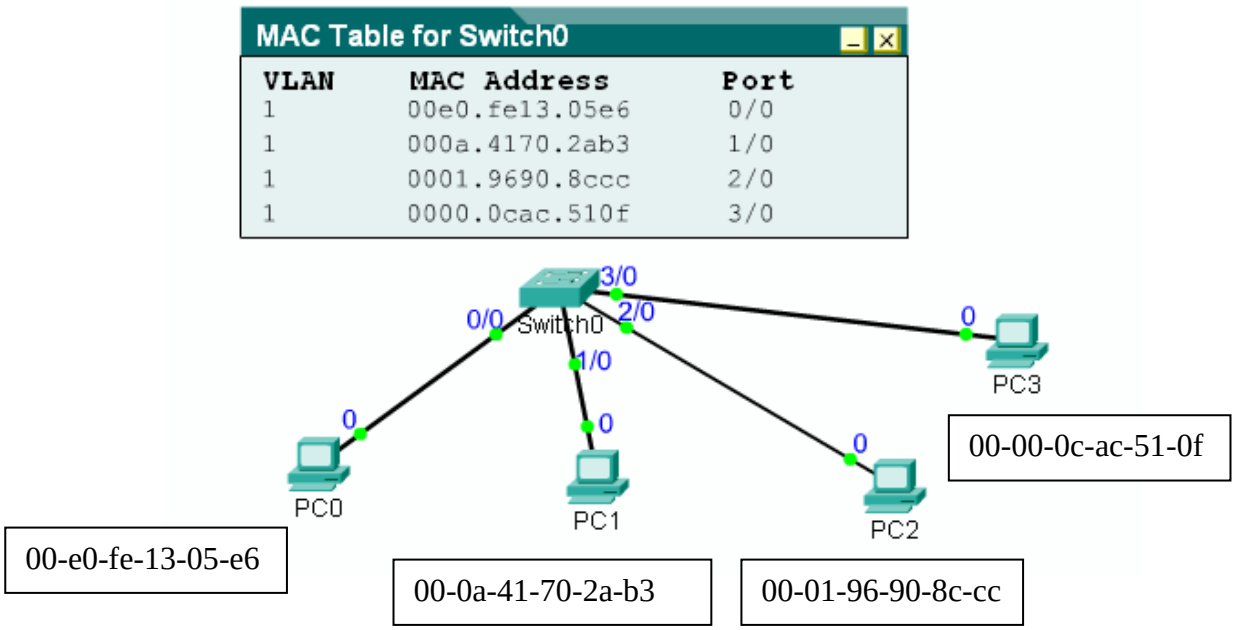
2.6. Generacje urządzeń aktywnych technologii Ethernet.

- Wzmacniacze (wzmacniaki, repeatery),
- Huby (koncentratory) (z ang.*hub*),
- Mosty (z ang. *bridge*)
- Przełączniki wartsyw II i III (routery)

2.7. Przełączniki wartwy II (z ang. *switches*)

Zaawansowane urządzenia elektroniczne, realizujące mechanizmy przełączania ramek na podstawie tzw. **tabeli przełączania** (*MAC Table*).

Przykładowa tabela przełączania



Podstawowe funkcje przełącznika:
- tworzenie tabeli przełączania *MAC Table* (statycznie lub dynamicznie), uzupełnianie lub modyfikacja wpisów,
- odbieranie ramek i wyszukiwanie w nich adresu docelowego MAC,
- przełączanie ramek na podstawie *MAC Table.*

***Zadanie**: Dokonać analizy tworzenia wpisów w tabeli MAC*

Zwykle współczesne przełączniki wyposażone są w różne algorytmy zbogacające funkcjonalność tychże urządzeń: przełączniki **zarządzalne** i **niezarządzane**.

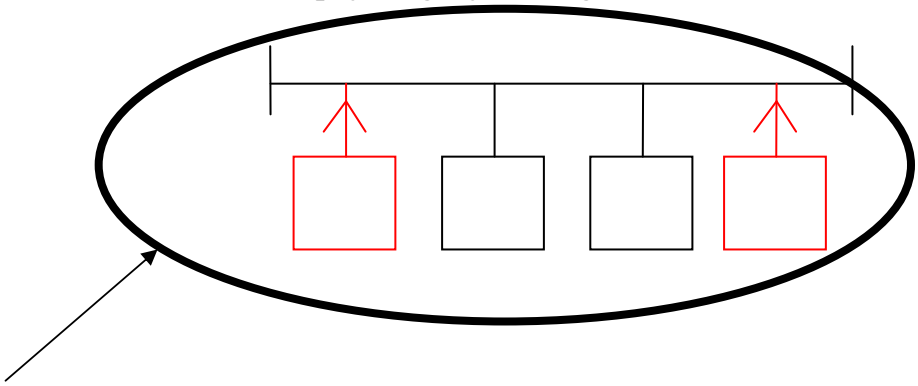
3. Algorytmy przełączania w warstwie II - przegląd

3.1. Algorytm CSMA/CD (z ang. *Carrier Sense Multiple Access/ Collision Detect*) jako najstarszy mechanizm działania sieci Ethernet

Algorytm definiuje reguły jakie muszą być przestrzegane przez kontrolery NIC (karty sieciowe) aby możliwa była transmisja sieciowa ramek. Procesy te dotyczą głównie sieci z urządzeniami starszej generacji.

W nowoczesnych przełącznikach implementowane są inne algorytmy, aczkolwiek urządzenia te mogą także pracować w trybie CSMA/CD.

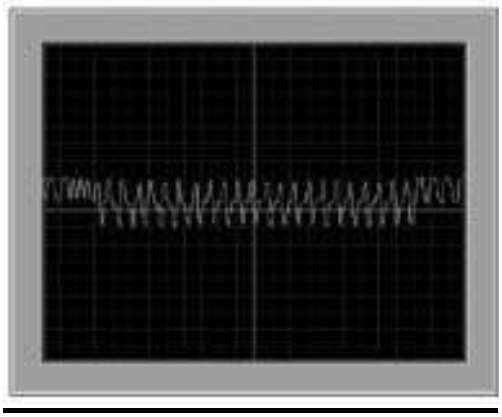
Koncepcja algorytmu wg. standardu 802.3 MAC



Pojedyncza domena kolizji obejmująca wszystkie NIC

I. Stacja nasłuchuje do momentu kiedy inne stacje nie będą wysyłać sygnałów (brak sygnału w kablu). Stacja nie może jednocześnie wysyłać i odbierać bitów.
II. Stacja wysyła swoją ramkę
III. Stacja nasłuchuje, czy w trakcie transmisji ramki nie wystąpiły kolizje.
IV. Jeżeli nie, to stacja „uznaje" proces wysyłania za ukończony.
V. Wszystkie stacje, których ramki uczestniczyły w kolizji wysyłają sygnał zagłuszający (32-bitowa sekwencja zer i jedynek). Pozostałe stacje dowiadują się o kolizji.
VI. Wszystkie stacje „kolizyjne" ustawiają niezależne quasi-losowe zegary oczekiwania po kolizji i nie mogą wysłać swojej ramki, dopóki nie upłynie odliczany przez zegary czas.

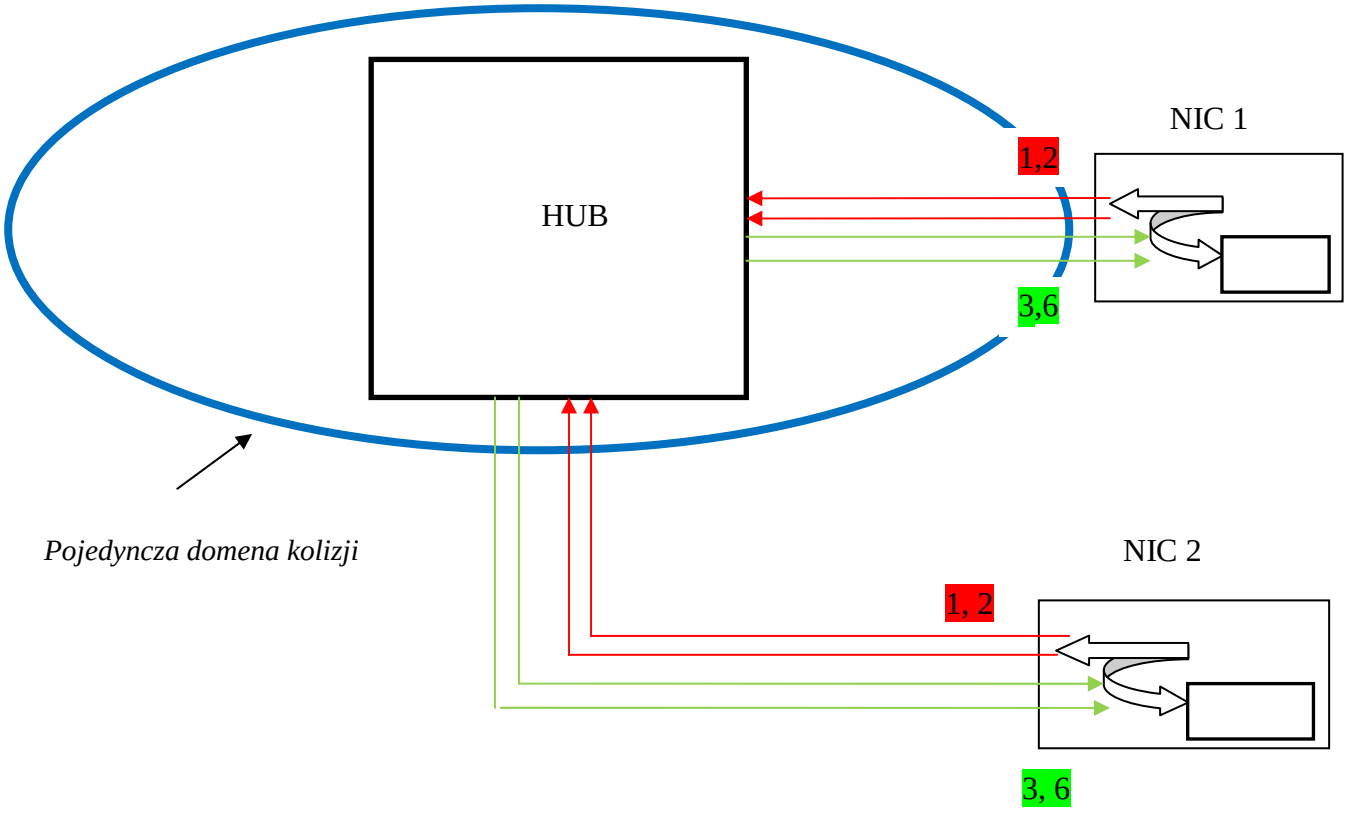
Oscylogram tzw. kolizji lokalnej (dla topologii szyny)



3.1.1. Algorytm CSMA/CD w sieciach z koncentratorami

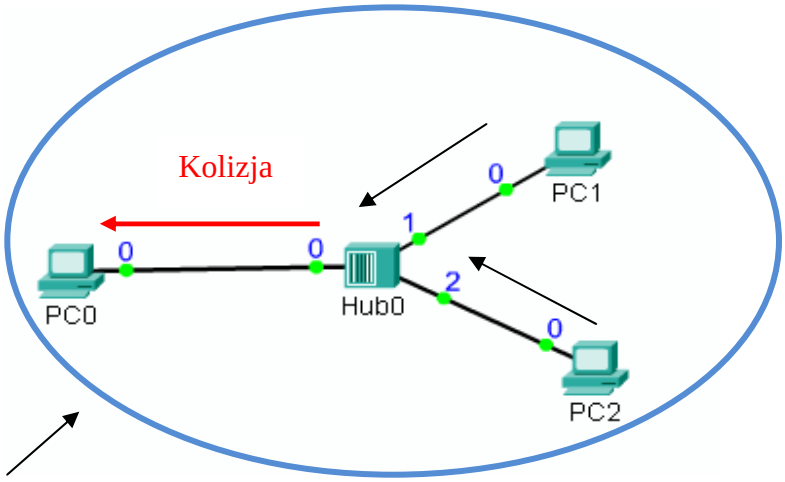
Detekcja kolizji przez urządzenie nadające odbywa się poprzez wykorzystanie mechanizmu pętli zwrotnej.

Domena kolizji – wszystkie urządzenia (NIC, interfejsy innych urządzeń), których ramki mogą potencjalnie uczestniczyć w kolizji.



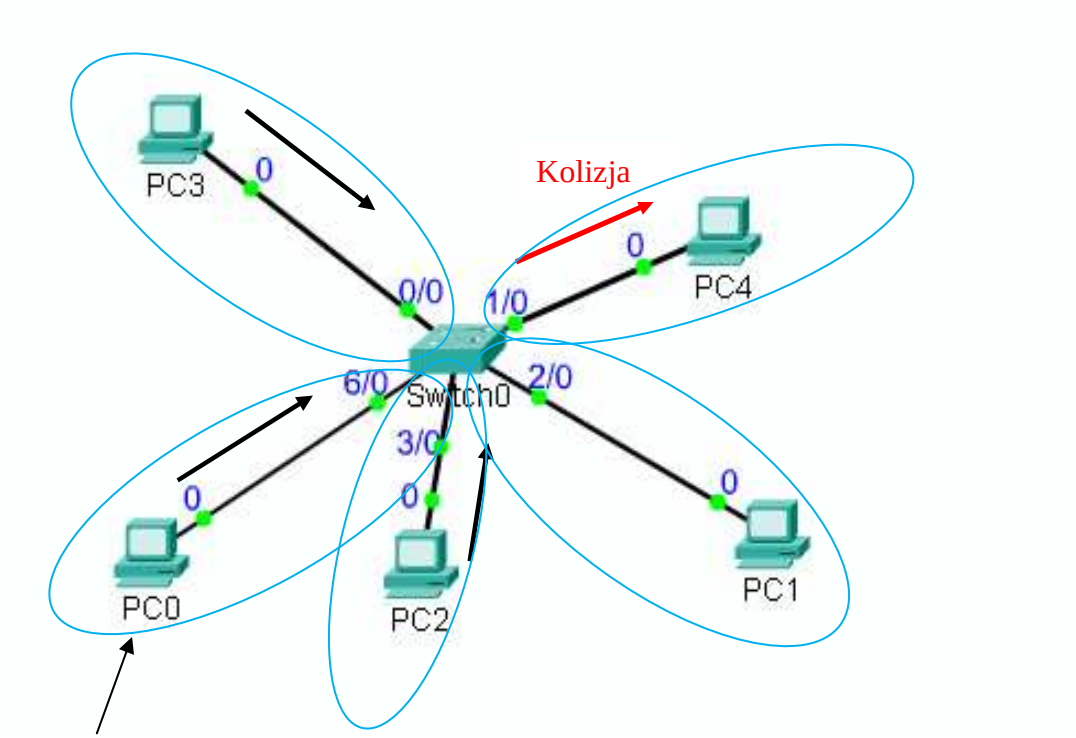
Pojedyncza domena kolizji

Detekcja kolizji przez stację nienadającą (PC0)



Pojedyncza domena kolizji

3.1.2. Domeny kolizji w przełączniku buforującym ramki



Pojedyncza domena kolizji

1. Stacje PC0, PC2, PC3 wysyłają ramki do PC4 jednocześnie.
2. Przełącznik przekazuje jedną z ramek do PC4, pozostałe buforuje
3. Przełącznik pobiera z bufora kolejno pozostałe ramki i przekazuje do PC4

3.1.3. Tryb full-dupleks w przełącznikach

Pełny dupleks może być stosowany w domenach kolizji, w których występują tylko dwie karty NIC lub tylko dwa interfejsy Ethernet.

Cechy trybu full-dupleks:
- karty NIC i interfejsy urządzeń innych mogą jednocześnie wysyłać i odbierać sygnały
- nie jest potrzebny algorytm CSMA/CD, nie ma możliwości kolizji, karty NIC wyłączają algorytm,
- przy wyłączonym CSMA/CD karta NIC wyłącza obwód pętli zwrotnej.

3.1.4. Automatyczna negocjacja dupleksu i pasma – algorytm IEEE 802.3X (*autonegotiation*)

Pakiety FLP (*Fast Link Pulse*) - serie 33 bitów NLP (*Network Link Pulse*) wysyłanych przez urządzenia znajdujące się po obydwu stronach skrętki. Pojedynczy FLP zawiera 16-bitową zakodowaną informacje o możliwościach interfejsów. Kolejność wysyłanych informacji:
- 1000 Mb/s, full-dupleks
- 1000 Mb/s, half-dupleks
- 100 Mb/s, full-dupleks
- 100 Mb/s, half-dupleks
- 10 Mb/s, full-dupleks
- 10 Mb/s, half-dupleks

Interfejsy urządzeń lub NIC mogą być konfigurowane “Ręcznie”

3.2. Współczesne algorytmy przełączania

3.2.1. Tablica przełączania MAC

CAM (*Content Addressable Memory*) – pamięć skojarzeniowa (asocjacyjna), adresowana zawartością – realizuje wyszukiwanie powiązań *MAC-Port* we wszystkich swoich komórkach jednocześnie. Posiada ograniczony rozmiar.
Szybkość działania pamięci decyduje o opóźnieniu w przekazywaniu ramek przez przełącznik.
Dane zawarte w pamięci **CAM** mogą być okresowo kasowane (brak odwołań do danych prze dłuższy czas) lub uzupełniane (przyłączenie stacji sieciowej do innego portu, przyłączenie nowej stacji sieciowej).

3.2.2. Typy ramek przetwarzanych przez przełączniki

Ramki pojedyncze – zawierają docelowy MAC pojedynczej karty NIC lub interfejsu innego urządzenia.
Nieznane ramki jednostkowe – ramki których MAC docelowy nie jest określony w CAM. W procesie analizy takiej ramki przełączniki uruchamiają tzw. proces zalewania portów (MAC flooding).
Ramki rozgłoszeniowe – ramki z rozgłoszeniowym docelowym MAC
Ramki grupowe – wysyłane pod adres grupowy MAC. Przełączniki niezarządzane – stosują metodę zalewania portów. Niektóre droższe przełączniki zarządzane umożliwiają przypisanie portów do rozgłaszania grupowego.

Opóźnienie (*latency*) - czas przesyłania ramki od nadawcy do odbiorcy.
Na ten parametr mają wpływ następujące czynniki:
- opóźnienie propagacji – czas potrzebny dla sygnału elektrycznego na przejście z jednej stacji do drugiej,
- opóźnienie w obwodach elektronicznych przełączników,
- opóźnienie związane z działanie algorytmów (programów) przełączania.

3.2.3. Algorytmy przełączania we współczesnych przełącznikach:

Algorytm *store-and-forward* (przechowaj i przekaż)

- możliwość kontroli ważnych pół nagłówka ramki (np. FCS, długość pola dane)
- jedyny algorytm możliwy do przełączania pomiędzy urządzeniami różnej prędkości, (przełączanie asymetryczne)
- wprowadzane duże opóźnienie w stosunku do innych algorytmów.

Algorytm *cut-trough* (przełączanie w locie)

- minimalne opóźnienie (najmniejsze w porównaniu z innymi algorytmami),
- nie jest sprawdzany FCS,
- może realizować przełączanie bezużytecznych ramek będących fragmentami kolizji. W praktyce kolizje występują podczas transmisji pierwszych 64 bajtów ramki,
- prawidłowo funkcjonuje tylko dla łączy symetrycznych.

Algorytm *fragment-free-switching*

- przekazanie ramki dopiero po przetworzeniu 64 B, właściwości podobnie jak ***cut-trough***, tylko nie są przełączane ramki kolizyjne.

Wykład III – zarządzanie przełącznikami warstwy II

1. Metody zarządzania urządzeniami sieciowymi:

- interfejsy „przyjazne” (graficzne),

- linie poleceń systemów operacyjnych wbudowanych.

2. Podstawowe cechy systemów operacyjnych dla urządzeń sieciowych na przykładzie Cisco IOS (*Internetworking Operating System*)

- zaimplementowane funkcje routingu i przełączania,
- zapewnienie niezawodnego i bezpiecznego dostępu do zasobów sieciowych,
- zapewnienie skalowalności sieci.
- dostęp do usług udostępnianych przez *IOS* odbywa się przy użyciu interfejsu linii komend (CLI). Dostępne funkcje zależą od wersji IOS oraz typu urządzenia,

- plik systemu jest przechowywany w pamięci typu Flash (możliwość zmian lub nadpisania),

- IOS może być kopiowany do pamięci RAM, co zwiększa wydajność urządzenia.

- podstawowe metody dostępu do środowiska CLI:
  - połączenie konsolowe z użyciem protokołu komunikacji szeregowej,
  - połączenie z uszyciem protokołu *Telnet* lub SSH,
  - połączenie „wdzwaniane” na port AUX poprzez modem.

Zadanie: *dokonać ogólnej prezentacji symulatora PT, utworzyć połączenie konsolowe*

System IOS funkcjonuje w oparciu o wykorzystanie plików konfiguracyjnych:

- plik konfiguracji startowej *startup-config* – przechowywany w NVRAM,

- plik konfiguracji bieżącej *running-config* – zawartość pliku tworzy się w RAM. Zmiany w tym pliku przez administratora natychmiast wpływają na działanie urządzenia. Można je skopiować do pliku startowego.

System IOS został zaprojektowany z podziałem na tryby o strukturze hierarchicznej:

- tryb EXEC użytkownika
- tryb EXEC uprzywilejowany
- tryb konfiguracji globalnej
- tryby konfiguracji szczegółowej

Zadanie: *podać przykład poszczególnych trybów, utworzyć plik startowy ze zmianami w konfiguracji przełącznika (np. hasło trybu uprzywilejowanego)*

3. Wybrane przykłady zarządzania przełącznikami Ethernet warstwy II.

Zadanie A: wyświetlić zawartość tabeli *MAC* przełącznika

Zadanie B: Dokonać analizy powstawania dynamicznych tabeli *MAC* dla przypadku 2 przełączników.

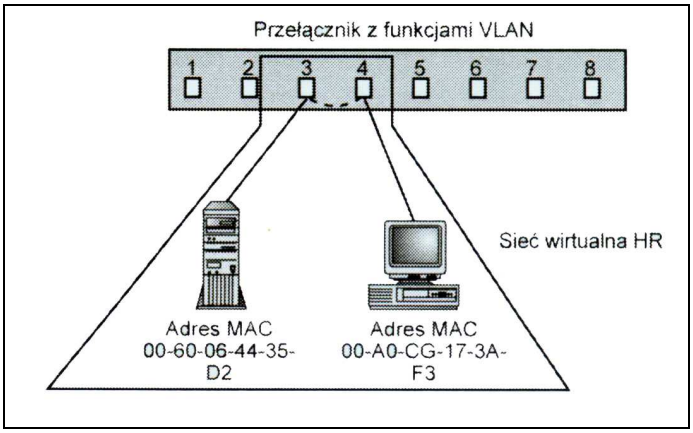
Zadanie C: dokonać przeglądu oraz zmian podstawowych parametrów dowolnego portu przełącznika.

3.1. Zarządzanie w warstwie II – sieci wirtualne VLAN (Virtual LAN)

Idea technologii VLAN

Podział sieci fizycznej opartej na jednym lub kilku przełącznikach na pewną liczbę sieci logicznych, poprzez separację ruchu ramek pomiędzy określonymi grupami portów. Wiąże się to z ograniczeniem zakresu rozgłaszania MAC.

Najprostszy przypadek sieci VLAN



Zalety technologii:

- administratorzy bardzo często stosują sieci VLAN w celu logicznego pogrupowania użytkowników niezależnie od ich rozmieszczenia,

- zawężenie ruchu pakietów rozłoszeniowych,

- możliwość łatwego przenoszenia bądź dodawania stacji sieciowych do VLAN-ów,

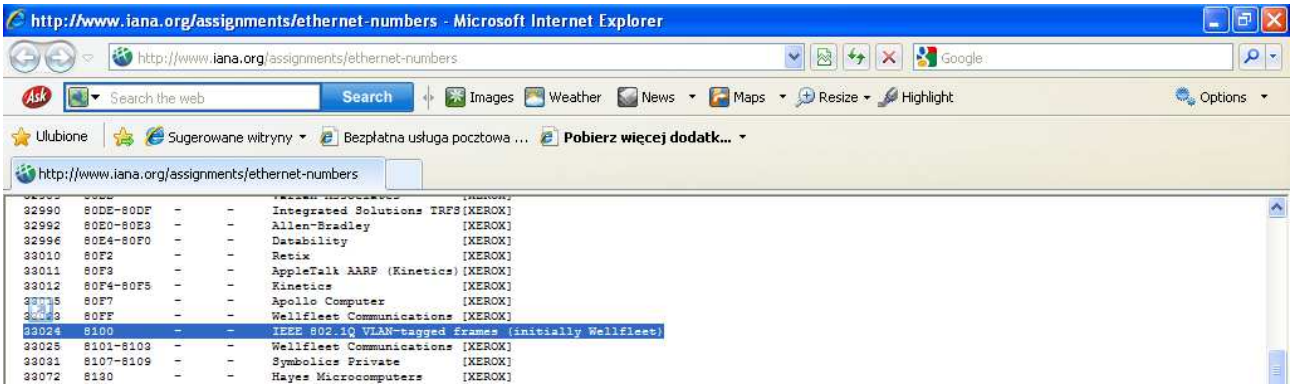
- łatwiejsze nadzorowanie ruchu w sieci.

Standardy technologii VLAN

- Cisco *ISL* (*Inter-Switch Link*) – obecnie nie implementowany – enkapsuluje oryginalną ramkę Ethernet,

- *IEEE* 802.1Q - stosowane jest tworzenie nowych 2 nowych pól w nagłówkach ramek „oryginalnych”

Pole nagłówka *Typ protokołu* przyjmuje wartość szesnastkową 8100h zgodnie ze standardem IANA: (oryginalne pole zostaje przesunięte za TCI):



Budowa pola „tagującego” *TCI* (*Tag Control Information*):

– *user_priority* (3b) – priorytet ramki,

– *CFI (Canonical Format Indicator)* (1b) – wskaźnik technologii bit 0 – Ethernet, bit 1 – Token Ring,

– *VLAN ID (VID)* (12b) – identyfikator VLAN. Wartość 0 oznacza brak przynależności.

Realizacja sieci VLAN na co najmniej 2 przełącznikach wymaga utworzenia miedzy nimi tzw. łącza rankingowego. Takie rozwiązanie pozwala oszczędnie gospodarować portami przełączników.

Zadanie A: dokonać konfiguracji sieci VLAN na jednym przełączniku.

Zadanie B: Zbudować łącze trunkingowe dla 2 przełączników z 3 sieciami VLAN

3.2 Filtracja ruchu ramek

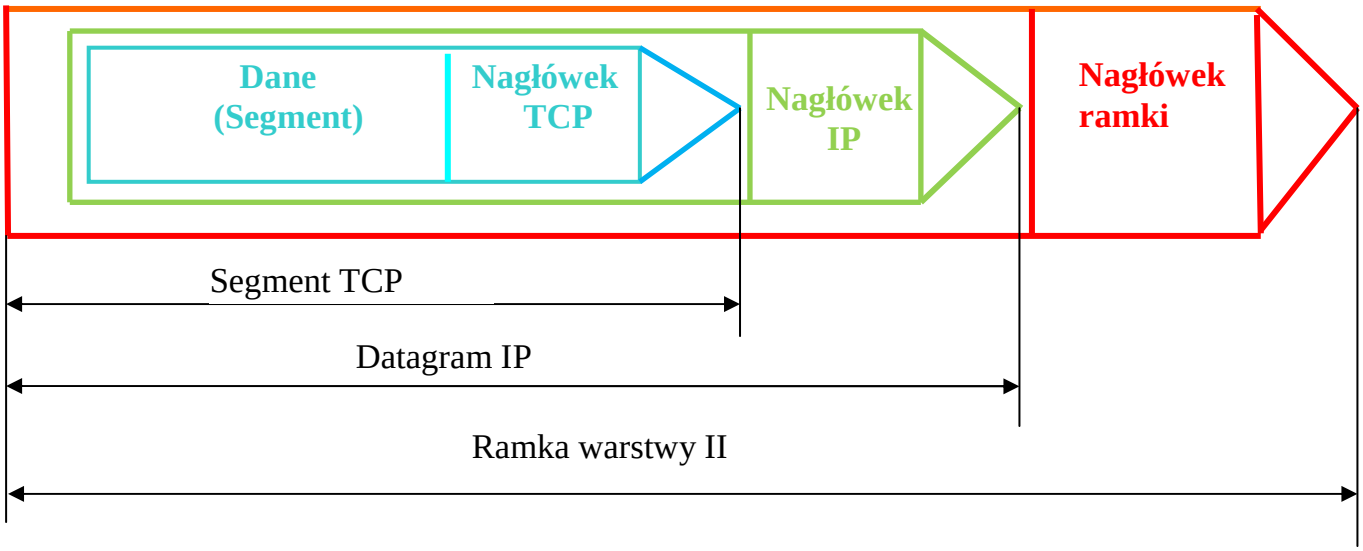
Niektóre modele przełączników umożliwiają odrzucanie ruchu ramek z nieautoryzowaną wartością pola *Source MAC* w nagłówku. Próba generowania ruchu sieciowego na porcie (portach) przełącznika powoduje, iż system operacyjny dokonuje jego (ich) wyłączenia.

Zadanie: dokonać konfiguracji zabezpieczenia portu przełącznika.

Wykład IV – Teoria protokołów IP oraz TCP

1. Podstawy protokołu IP v.4

1.1. Kapsułkowanie w sieciach Ethernet



1.2. Podstawowe funkcje protokołu IP:

- wsparcie dla komunikacji międzysieciowej (internetowej) ze szczególnym uwzględnieniem routingu, (warstwa III OSI)

- IP pełni funkcję „nośnika” dla protokołów warstw wyższych w komunikacji międzysieciowej, (np. TCP, UDP),

- jest protokołem dostarczającym datagramy w sposób bezpołączeniowy,

- jest niezależny od parametrów warstwy II,

- datagramy IP mogą być fragmentowane przez urządzenia sieciowe różnych technologii (różne MTU)

2. Elementy standardowego nagłówka IP oraz ich znaczenie.

a) **Version** 4b – oznacza wersję protokołu (4 dla IPv4 lub 6 dla IP v6) http://www.iana.org/assignments/version-numbers

b) **IP Header Length** (długość nagłówka) 4b – liczba 4-bajtowych bloków w nagłówku IP. Rozmiar nagłówka IP musi być zatem wielokrotnością 4B. Najkrótszy nagłówek IP posiada długość 20 B (wartość pola 0x5), najdłuższy 60 B (wartość pola 0xF),

c) **Type of service TOS (typ usługi)** – 8b – określa priorytet obsługi przy datagramu przez routery w internecie (RFC 791, 2474). Router może być tak skonfigurowany, że na podstawie pola TOS będzie decydował, który pakiet ma być obsłużony jako pierwszy.

d) **Total Length** 2B **–** całkowity rozmiar datagramu w bajtach (nagłówek + dane) **:**

Dane [B]=Total Length – 4*IP Header Length

e) **Identifier** 2B – identyfikacja pakietu, wartość ustawiana przez host nadawczy i zwiększana o 1 dla każdego następnego pakietu.

f) **Flags** (flagi) 3 b – 2 flagi dotyczące fragmentacji,

g) **Fragment Offset –** 13b – określa przesunięcie fragmentu względem początku pełnych danych (komunikatu)

h) **Time to Live –** 1B – liczba połączeń, przez które datagram będzie przekazywany do momentu odrzucenia. Wartość maksymalna to 255. Wartość domyślna jest ustawiana w systemie operacyjnym (np. w rejestrach Windows)

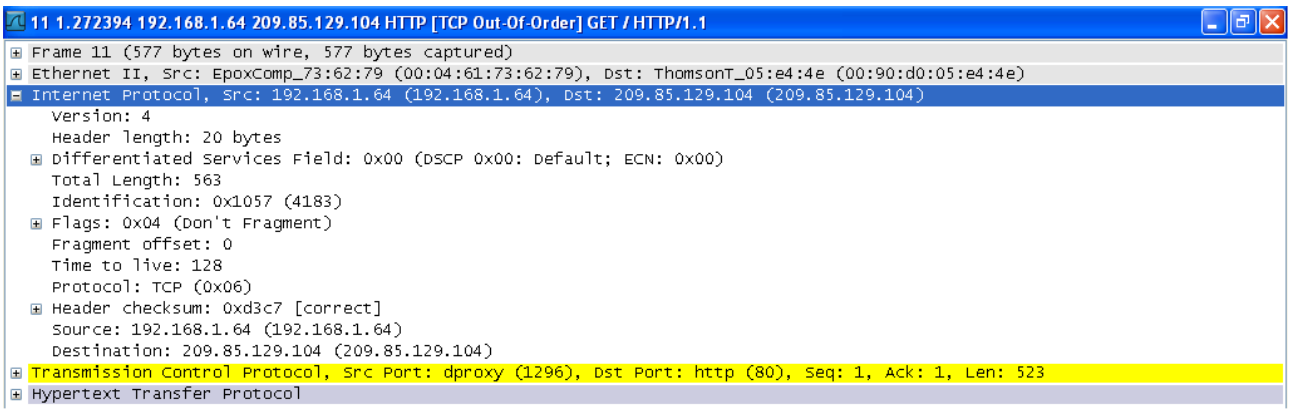
i) **Protocol** – 1B – typ protokołu zwartego w danych (ładunku) pakietu IP, np. 0x06 TCP. Pole to umożliwia stacji docelowej skierowanie danych do właściwego protokołu warstwy wyższej. Pełna lista dostępna jest na http://www.iana.org/assignments/protocol-numbers

j) **Header Checksum** – 2 B – wartość sumy kontrolnej dla nagłówka (z wykorzystaniem kodu uzupełnienieniowego do 1)

k) **Source Address** – 4B, IP źródłowy

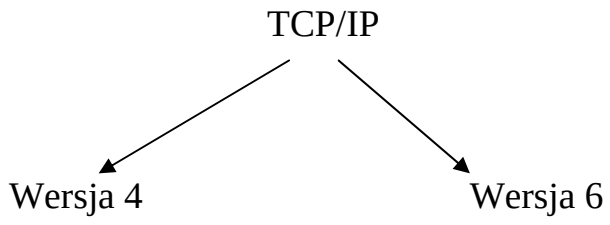
l) **Destination Address** – 4B, IP docelowy

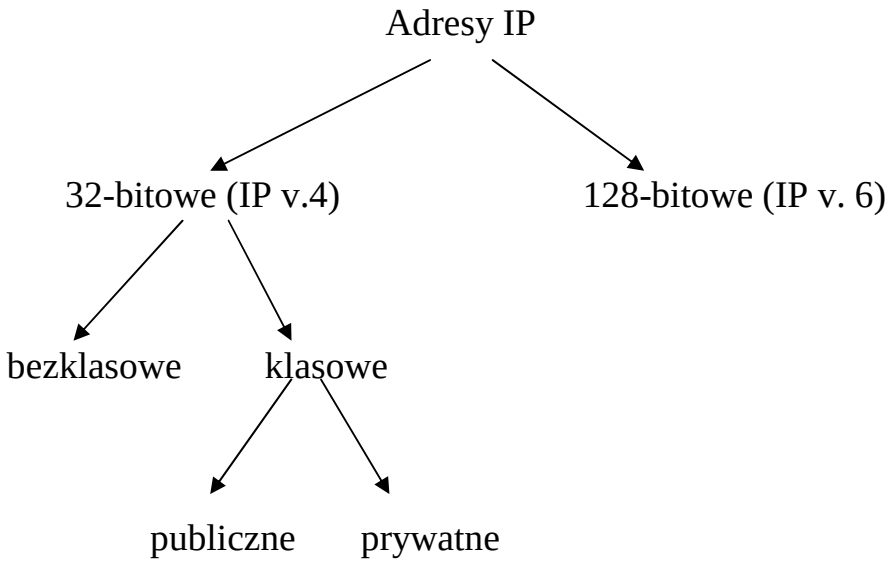
Pola nagłówka IP w analizatorze sieciowym



3. Adresowanie IP v.4

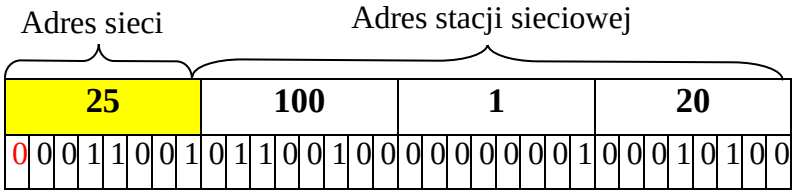
3.1. Miejsce adresów protokołu IP v.4 w strukturze protokołów



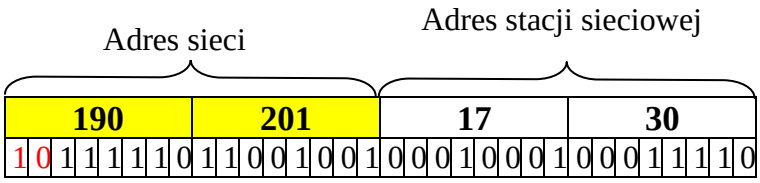


3.2. Adresy klasowe

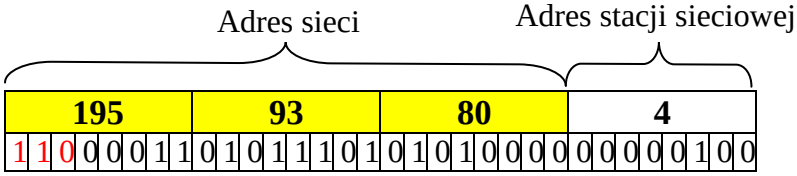
Klasa A (0-126)



Klasa B (128-191)



Klasa C (192-223)



Pule adresów prywatnych:

Klasa A: 10.0.0.0 – 10.255.255.255

Klasa A: 172.16.0.0 – 172.31.255.255

Klasa A: 192.168.0.0 – 192.168.255.255

Maski adresów 32-bitowych

Maska – 32 bitowe słowo pozwalające określić ile bitów adresu IP wskazuje na adres sieci, a ile bitów na adres stacji sieciowej w tejże sieci. Maki mogą być domyślne lub sztuczne.

Przykład 1 – maski domyślne (naturalne)

Adres IP klasy A: 11.25.65.32

11								25								65								32							
0	0	0	0	1	0	1	1	0	0	0	1	1	0	0	1	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0

255								0								0								0							
1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Maska domyślna 255.0.0.0

Adres IP klasy C: 192.168.2.3

192								168								2								3							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	1

255								255								255								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0

Maska domyślna 255.255.255.0

Przykład 2 – maska nienaturalna dla adresu klasy B

Adres IP klasy B: 141.91.73.65

141								91								73								65							
1	0	0	0	1	1	0	0	0	1	0	1	1	0	1	1	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0	1

255								255								255								192							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0

Maska nienaturalna 255.255.255.192

Interpretacja adresu z maską: podsieć 73.64 sieci 141.91, stacja sieciowa 1 w tejże podsieci

Typy adresów IP klasowych

1. *Adresy transmisji pojedynczej* – przypisywane pojedynczemu interfejsowi, przeznaczone do komunikacji indywidualnej, np. 192.168.2.1/24
2. *Adresy emisji w sieci* – złożone z samych jedynek na pozycji hosta – przeznaczone do komunikacji do wszystkich hostów o danym identyfikatorze sieciowym. Routery nie dokonują routingu takich pakietów, np. 131.107.255.255/16
3. *Adresy emisji w podsieci* – adres złożony z samych jedynek na pozycjach hosta w adresie z maską sztuczną, np.: 131.107.26.255/24
4. *Adresy emisji sieciowej do wszystkich podsieci* – adres złożony z samych jedynek na pozycjach hosta w adresie „pierwotnym" np.: 131.107.255.255 w sieci 131.107.26.0/24
5. *Adresy multiemisji* – adresy klasy D w zkresie od 224.0.0.0:239.255.255.255. Przeznaczone są do transmisji typu jeden do wielu (do grupy hostów) w dowolnej sieci (pakiety z takimi adresami są przetwarzane przez routery)

3.3. Techniki adresowania IP v.4

3.3.1. Technika masek naturalnych: podsieci z maską stałą

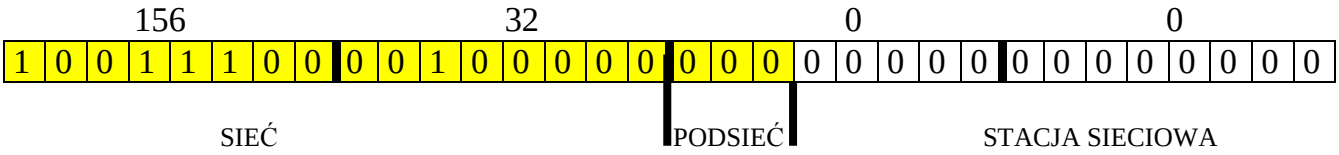
Metodę tą stosuje się w następujących przypadkach:

- sieć o topologii mieszanej, każda z podsieci (topologii) powinna posiadać własny adres sieciowy,

- potrzeba ograniczenia ruchu w sieci, izolacja grupy stacji sieciowych intensywnie obciążających łącza we własnej podsieci,

- lepsze gospodarowanie przestrzenią adresów IP v.4.

Przykład: Określić pulę adresów dla sieci złożonej z 3 segmentów, dla której przydzielono jeden unikalny adres klasy B: 156.32.x.x z maską domyślną.



Wyznaczenie maski:

Określanie wszystkich adresów sieciowych poszczególnych segmentów dla maski 224

Lp	Binarnie	Dziesiętnie
1	**000**00000	Kombinacja niedozwolona
2	**001**00000	32
3	**010**00000	64
4	**100**00000	128
5	**110**00000	192
6	**101**00000	160
7	**011**00000	96
8	**111**00000	Kombinacja niedozwolona

Ostatecznie dostępne adresy **podsieci** dla maski 255.255.224.0

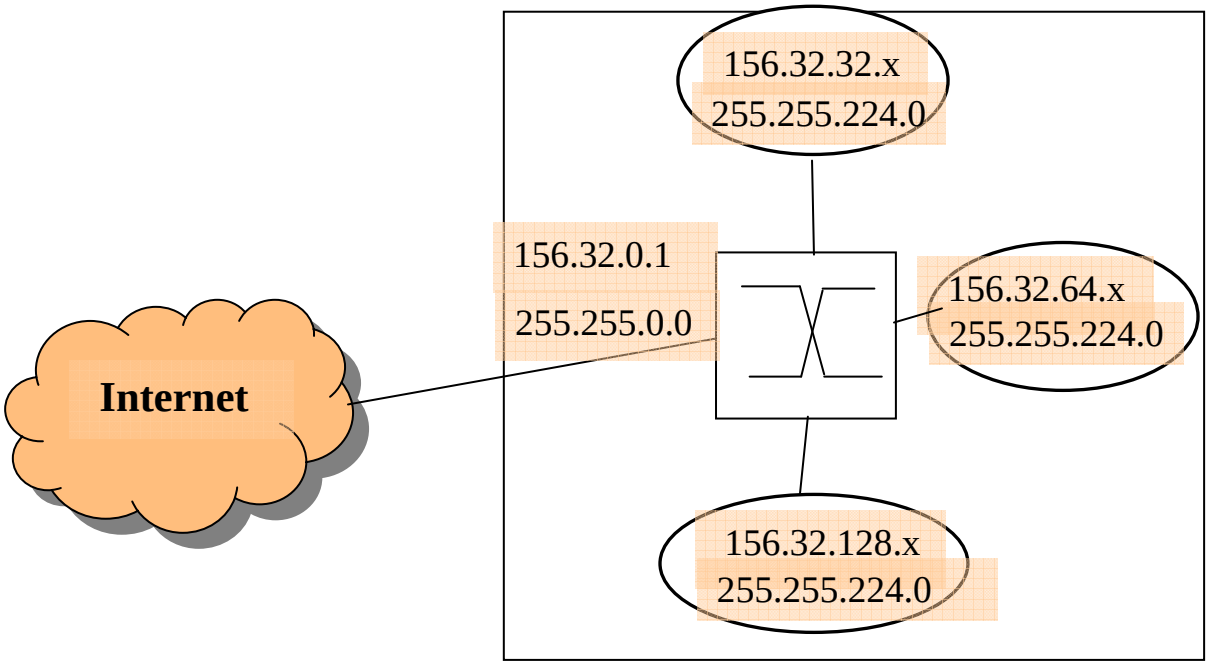
Lp	Binarnie	Dziesiętnie
1	**10011100 00100000 000**00000 00000000	Kombinacja niedozwolona
2	**10011100 00100000 001**00000 00000000	156.32.32.0
3	**10011100 00100000 010**00000 00000000	156.32.64.0
4	**10011100 00100000 100**00000 00000000	156.32.128.0
5	**10011100 00100000 110**00000 00000000	156.32.192.0
6	**10011100 00100000 101**00000 00000000	156.32.160.0
7	**10011100 00100000 011**00000 00000000	156.32.96.0
8	**10011100 00100000 111**00000 00000000	Kombinacja niedozwolona

Ostateczna pula adresów dla stacji sieciowych w poszczególnych segmentach dla maski 224 :

Lp	Adres sieci	Adres początkowy	Adres końcowy	Adres rozgłaszania
1	156.32.32.0	156.32.32.1	156.32.63.254	156.32.63.255
2	156.32.64.0	156.32.64.1	156.32.95.254	156.32.95.255
3	156.32.128.0	156.32.128.1	156.32.159.254	156.32.159.255
4	156.32.192.0	156.32.192.1	156.32.223.254	156.32.223.255
5	156.32.160.0	156.32.160.1	156.32.191.254	156.32.191.255
6	156.32.96.0	156.32.96.1	156.32.127.254	156.32.127.255

Wybrana pula adresów dla 3 segmentów IP (podsieci)

Schemat ogólny intersieci po podziale adresu 156.32.0.0 na podsieci za pomocą maski 255.255.224.0



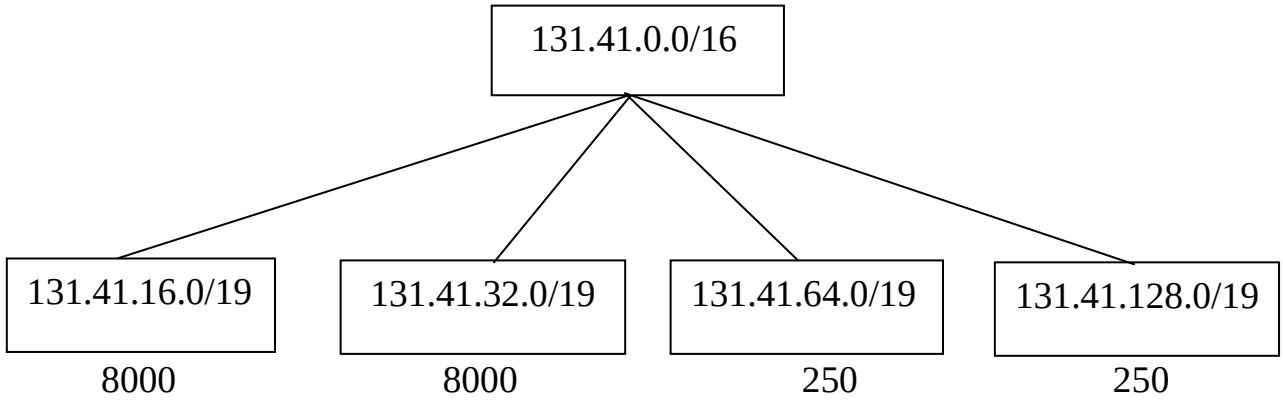
3.3.2. Technika masek zmiennych *VLSM* (*Variable Length of Subnet Masking*)

Podział rekursywny podsieci na podstawie pierwotnego adresu IP – możliwość tworzenia podsieci o różnych pulach adresowych (rozmiarach).

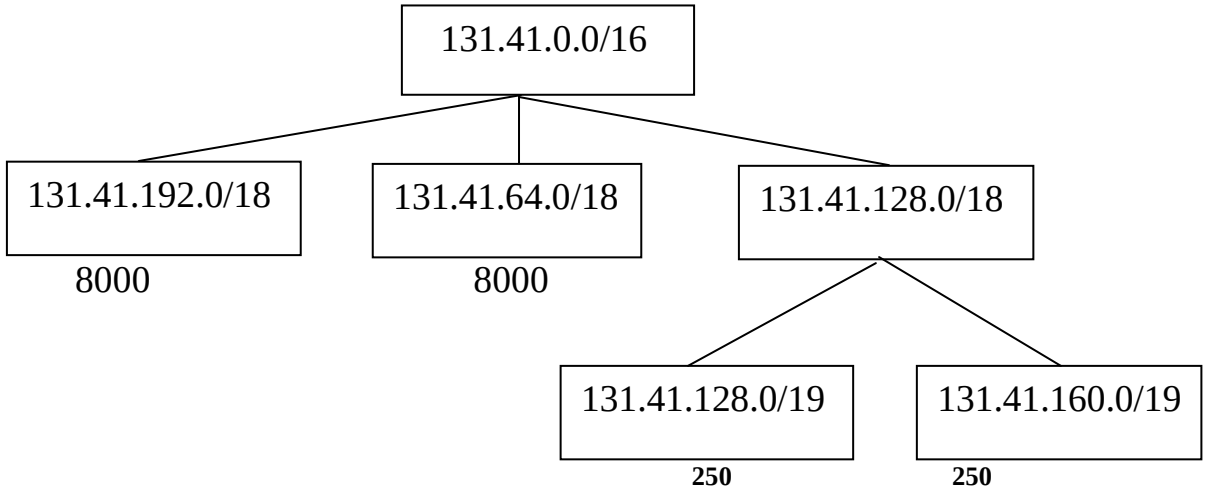
Przykład 1: na bazie adresu klasowego 135.41.0.0/16 wyznaczyć pule adresowe dla 2 podsieci z 8000 stacjami oraz dla 2 podsieci z 250 stacjami.

A. Rozwiązanie z maską stałą:

135.41.0.0/19 – 6 sieci po 8190 stacji sieciowych

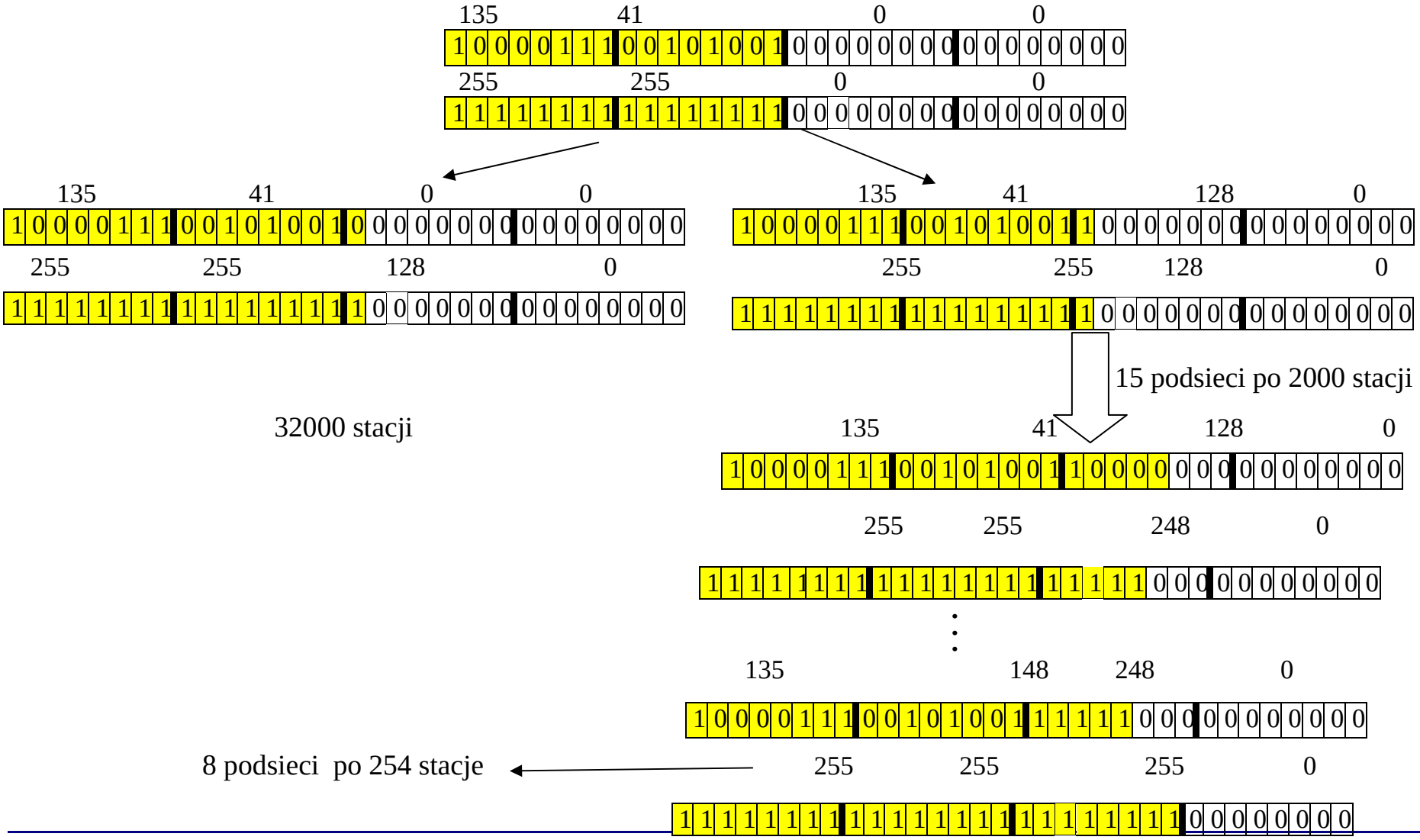


A. Rozwiązanie VLSM:



131.41.192.0/18 – 8000 stacji
131.41.64.0/18 – 8000 stacji
131.41.128.0/19 – 250 stacji
131.41.160.0/19 – 250 stacji

Przykład 2: na bazie adresu klasowego 135.41.0.0/16 wyznaczyć pule adresowe dla 1 podsieci z 32000 stacjami, 15 podsieci z 2000 stacji oraz dla 8 podsieci z 250 stacjami – **metoda masek stałych nie spełni wymagań !**


135 41 0 0
255 255 0 0
135 41 0 0
255 255 128 0
135 41 128 0
255 255 128 0
32000 stacji
15 podsieci po 2000 stacji
135 41 128 0
255 255 248 0
135 148 248 0
8 podsieci po 254 stacje
255 255 255 0

3.3 Adresy bezklasowe - technika *CIDR (Classless Inter Domain Routing)*

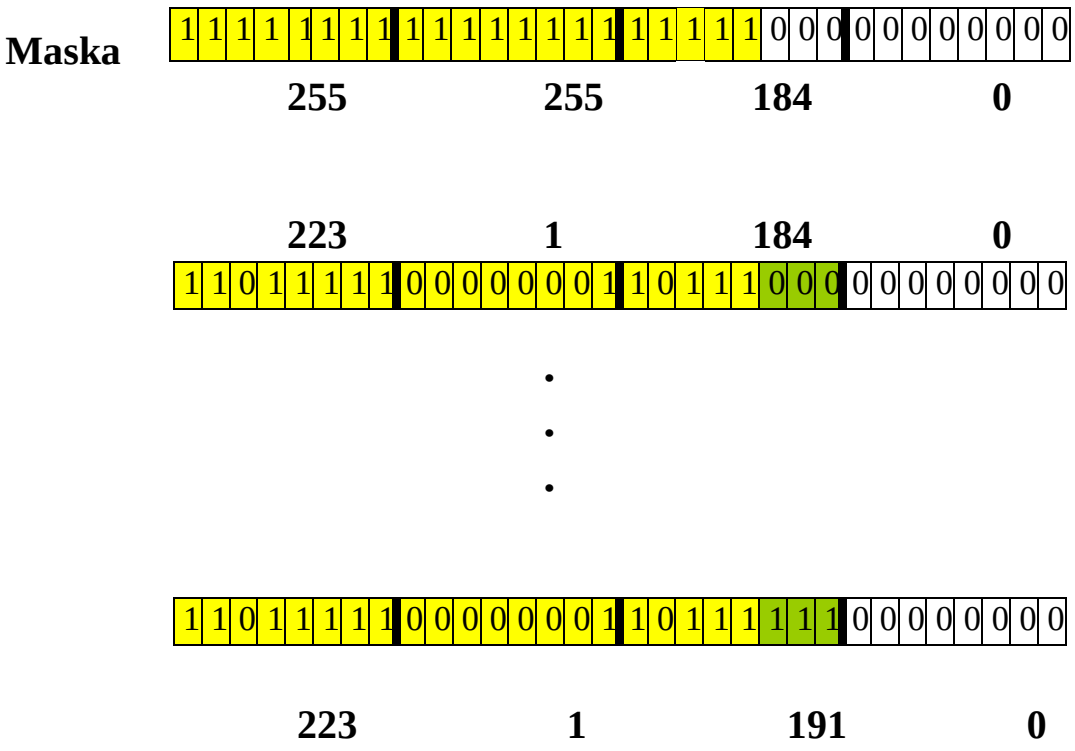
Przykład: wymagane jest przydzielenie 2000 adresów.

Możliwe rozwiązania tradycyjne:

- przydzielenie adresu klasy B
- przydzielenie 8 adresów klasy C
- podział na podsieci o stałej lub zmiennej długości masek

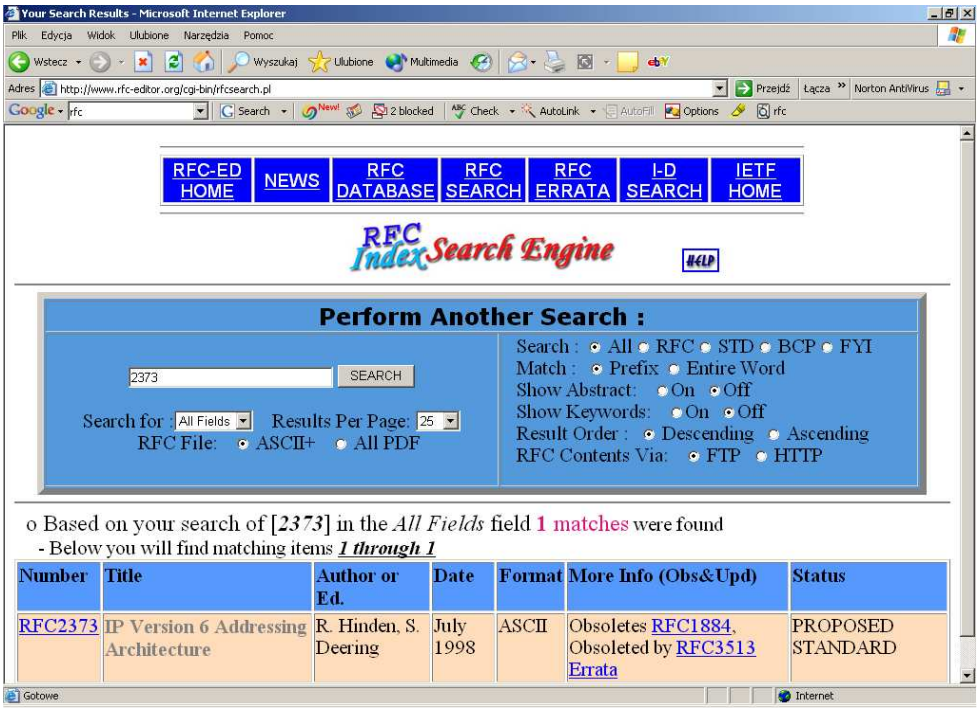
Interpretacja pierwsza - wystarczająca jest przestrzeń adresowa z numerem sieci 22.3.1.184.0/21 oraz 11 bitami dla stacji sieciowych (bity hosta) – brak podsieci

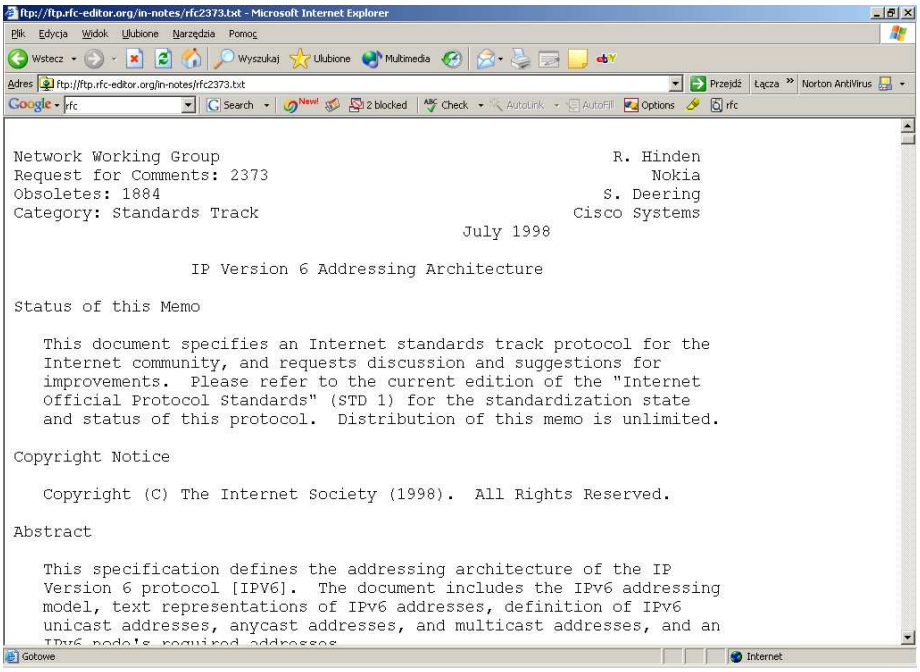
Interpretacja druga - agregowanie 8 adresów nadsieci– jeden wpis w tabeli routingu reprezentuje 8 tras w routerze



Wykład IV - Adresowanie IP v.6

Dokument RFC 2373





Pola nagłówków IP v4 i IP v6

IP v4	IP v6	Porównanie
Version 4b wartość =4	Version 4b wartość =6	Funkcje takie same
IP Header Length 4b	brak	IP v6 – wartość stała 320 b
Type of service TOS 8b	DSCP (Differential Services Code Point) - 8b	Funkcje takie same
-	Stream label - 20b	Nowe pole w IP v6
Identifier (fragmentation) 16b	-	Usunięte w IP v6
Flags for fragmentation 3b	-	Usunięte w IP v6
Fragment Offset – 13b	-	Usunięte w IP v6
Time to Live – 8b	Time to Live – 8b	Funkcje takie same
Protocol type – 8b http://www.iana.org/assignments/protocol-numbers	Protocol type – 8b	Funkcje takie same
Header Checksum – 16 b	-	Usunięte w IP v6
Source Address – 32b	Source Address – 128b	Rozszerzenie przestrzeni
Destination Address – 32b	Destination Address 128b	Rozszerzenie przestrzeni
Options (change of header length)	-	Usunięte w IP v6
-	Nagłówki rozrzeszeń	Nowy sposób obsługi fragmentacji, wprowadzenie elementów bezpieczeństwa sieciowego, wprowadzenie idei mobilności i inne.

Teoretyczna przestrzeń adresowa:
$P=2^{128}=3.4*10^{38}=$

$=340282366920938463463374607431768211456$

Obecnie Internet może wykorzystać 15 % tej przestrzeni.

Przykład adresu w reprezentacji bitowej:

00100001110110100000000011010011000000000000000000010111100111011000000101010100000000011111111111111110001010001001110001011010

Adres po podziale na osiem 16-bitowych bloków

0010000111011010 : 0000000011010011 : 0000000000000000 : 0010111100111011 : 0000001010101010 : 0000000011111111 : 1111111000101000 : 1001110001011010

Każdy blok konwertuje się na liczbę szesnastkową.

$[0010000111011010]_2=0*2^{15}+0*2^{14}+1*2^{13}+0*2^{12}+0*2^{11}+0*2^{10}+0*2^9+$

$+1*2^8+1*2^7+1*2^6+0*2^5+1*2^4+1*2^3+0*2^2+1*2^1+0*2^0=(8666)_{10}=$

$(21DA)_{16}$

$(21DA)_{16}=2*16^3+1*16^2+13*16^1+10*16^0=(8666)_{10}$

Przypomnienie

Zapis dwójkowy:	**Zapis szesnastkowy:**
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

Rozważany adres ma postać:

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

Usuwanie zer początkowych:

Adres przed: **21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A**

Adres po: **21DA:D3:0:2F3B:2AA:FF:FE28:9C5A**

Kompresowanie zer:

Adres przed: **FE80:0:0:0:2AA:FF:FE9A:4CA2**

Adres po: FE80::2AA:FF:FE9A:4CA2

Prefiks

Prefiks jest częścią adresu wskazującą bity, które mają ustalone wartości lub są bitami identyfikatora sieci. Prefiks IPv6 jest zapisywany jako: *adres/długość_prefiksu*.

Niektóre typy adresów IP v6:

a) adresy lokalne łącza: FE80::/10

b) adresy lokalne węzła : FEC0::/10

c) zagregowane globalne adresy jednostkowe

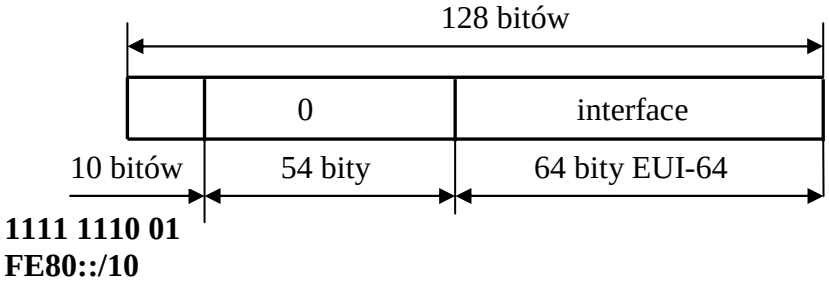
d) adresy grupowe żądania węzła: FF02:1:FF00:0000/104

Charakterystyka wybranych typów adresów

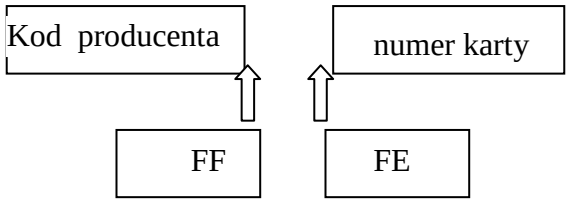
Ad. a) – *Link local address* – adresy specjalnego przeznaczenia - używane do komunikacji w ramach łącza lokalnego (np. router – host).

Adresy mogą być ustalone statycznie lub automatycznie w momencie uruchomienia na stacji stosu z IP v6.

Format	Wartość
Heksadecymalny pełny	FE80:0000:0000:0000:0000:0000:0000:0000/10
Skrócony	FE80::/10
Binarny	**1111 1110 01**



Konfiguracja adresu w formacie EUI 64 (Extended Unique Identifier)



Przykład adresu *link local*: FE80::250:3EFF:FEA4:5F12/64

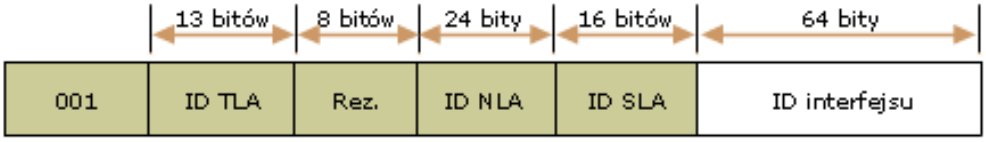
Ad. 1b) – *Node local address* – adres lokalny węzła – odpowiednik adresu prywatnego IP v.4. Mogą być używane do adresowania stacji wewnątrz lokalizacji bez możliwości routingu w sieci globalnej. Używane także do adresowania urządzeń, które nie wysyłają pakietów do sieci globalnej (np. drukarki, przełączniki zarządzalne)

Format	Wartość
Heksadecymalny pełny	FEC0:0000:0000:0000:0000:0000:0000:0000/10
Skrócony	FEC0::/10
Binarny	**1111 1110 11**

Przykład adresu *node local*: FEC0::12:250:3EAF:FEA4:5F12/64

Ad c) – zagregowane adresy globalne jednostkowe - odpowiedniki adresów publicznych IP v4.

Struktura adresów globalnych



ID TLA (*Top Level Aggregator*) – 13 bitów przydzielane lokalnym (krajowym) urzędom rejestracyjnym. Te z kolei przydzielają tą cześć dużym usługodawcom ISP.

Rez – rezerwa dla TLA lub NLA w przyszłości

ID NLA (*Next Level Aggregator*) - agregacja na poziomie dostawcy internetu. Routery wolne nie reagują na tą cześć adresu. NLA pozwala firmie typu ISP na tworzenie własnych hierarchi routingu.

ID SLA (*Site Level Aggregator*) **–** służą do identyfikacji podsieci u klienta końcowego

ID interfejsu - adres interfejsu w danej podsieci.

Format	Wartość
Heksadecymalny pełny	2xxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
Pierwszy z możliwych adresów	2000:0000:0000:0000:0000:0000:0000:0000
Ostatni z możliwych adresów	3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Przykład globalnego adresu jednostkowego (dla danego SLA):

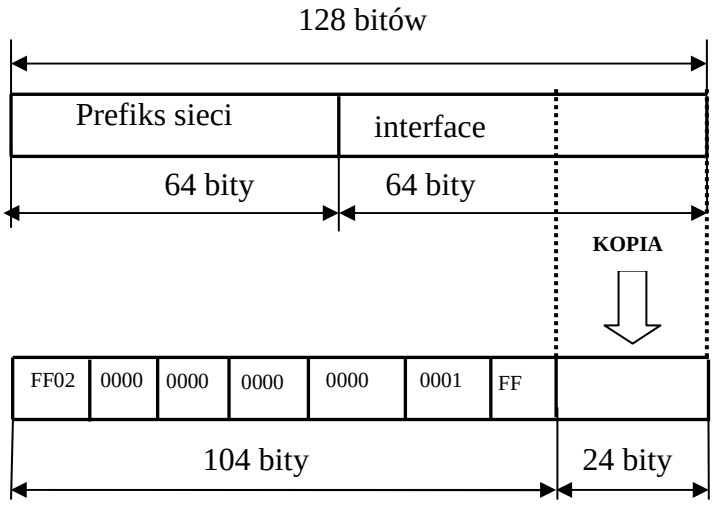
2001:410:110:**2312**:200:CBFC:1234:4402/64

Ad d) adresy grupowy żądania węzła: wykorzystywany między innymi w mechanizmach protokołów :

- NDP (*Neighbor Discovery Protocol*)
- DAD (*Duplicate Address Detection*)

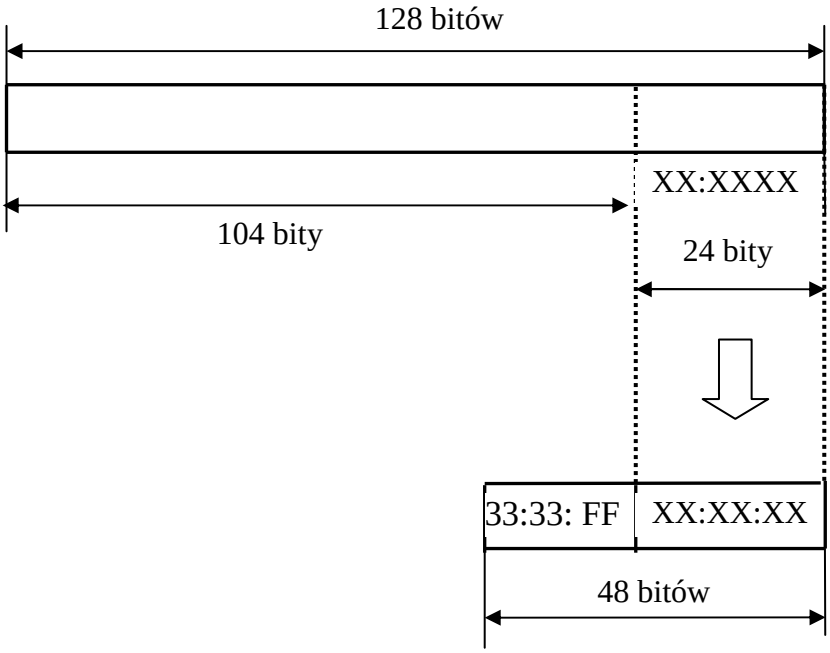
Format	Wartość
Heksadecymalny pełny	FF02:0000:0000:0000:0000:0001:FF00:0000/104
Skrócony	FF02::1:FF00:0000/104

Mechanizm tworzenia adresu grupowego żądania węzła na podstawie adresu jednostkowego



Przykład:
- adres jednostkowy: 2001:410:0:1:0000:0000:0000:45FF
- adres grupowy żądania węzła: **FF02::1:FF**00:45FF

Mechanizm mapowania adresów grupowych przez protokół IP v6



Uruchomienie stosu IPv6 na stacji powoduje nasłuch tej stacji na adresie mapowanym.

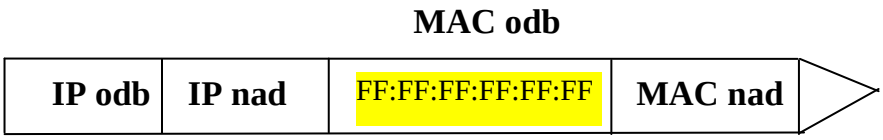
Zadanie: Dołączyć stację IP v6 do przełącznika, sprawdzić adres lokalny łącza, dokonać testu połączenia logicznego dla dołączonej stacji (plik *ipv6-topologia*).

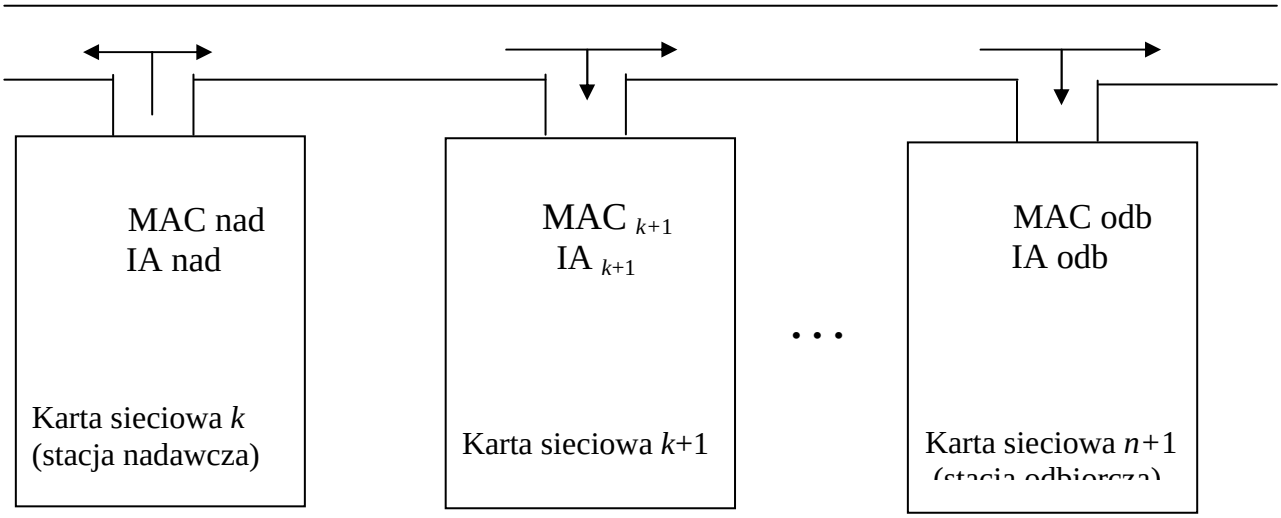
Wykład V- Odwzorowanie IP – MAC na przykładzie protokołów ARP oraz NDP.

1. Mechanizmy protokołu ARP (*Addrress Resolution Protocol*)

Mechanizm działania protokołu ARP w sieci lokalnej

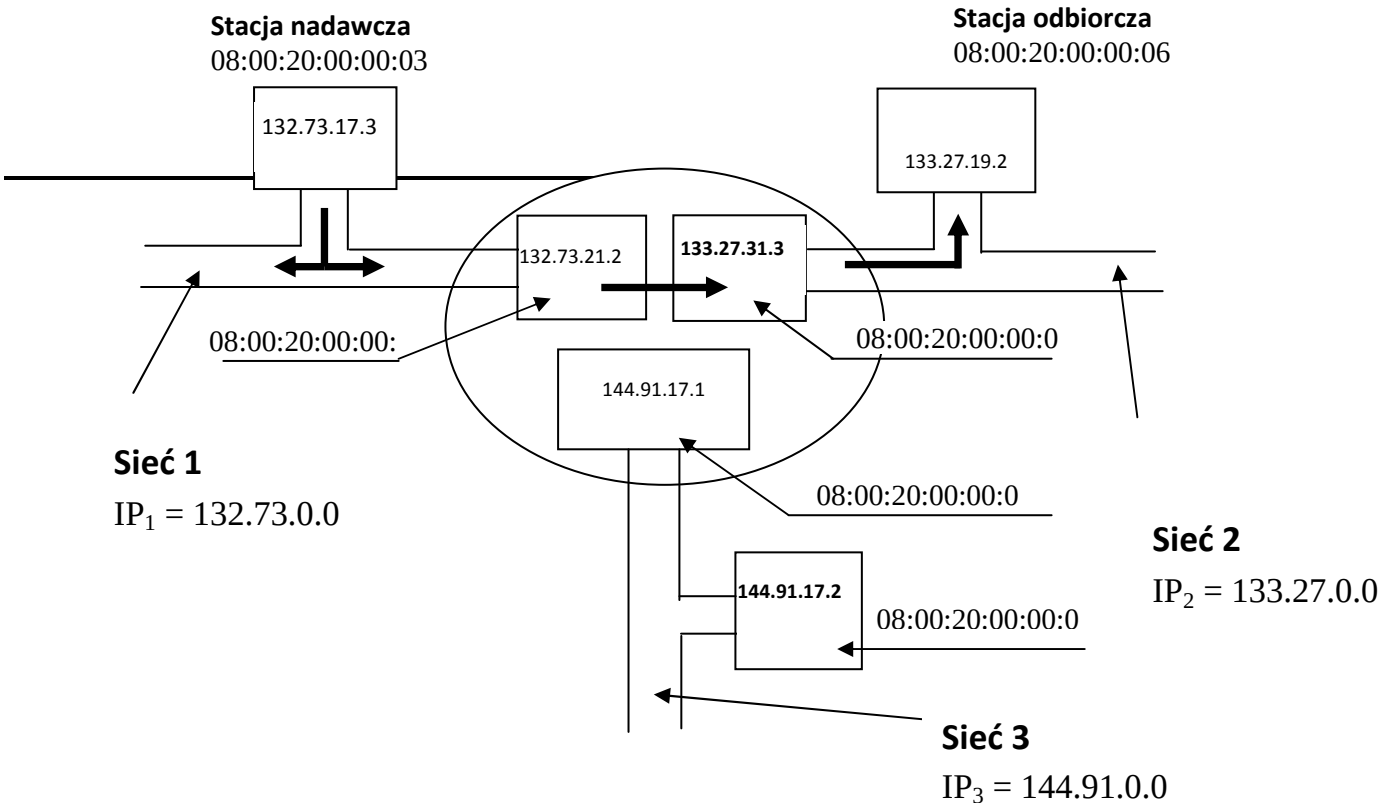
a) w pierwszym etapie stacja nadawcza wysyła ramkę z *ARP Request*, z adresem *MAC odb* równym rozgłoszeniowemu.



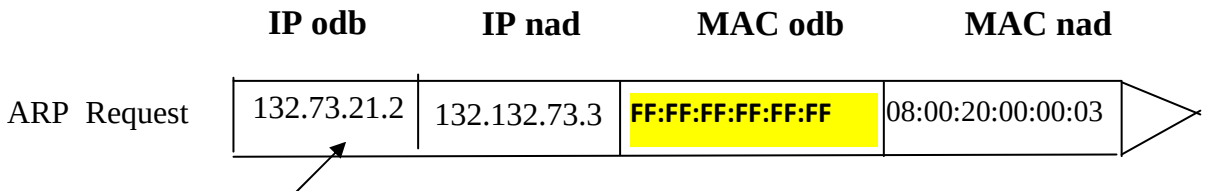


b) W etapie drugim tylko ta stacja której adres IP jest równy adresowi *IP odb* w ramce *ARP Request* wysyła do sieci ramkę z *ARP Response* wypełniając ją wcześniej własnym MAC - Rys. 2.

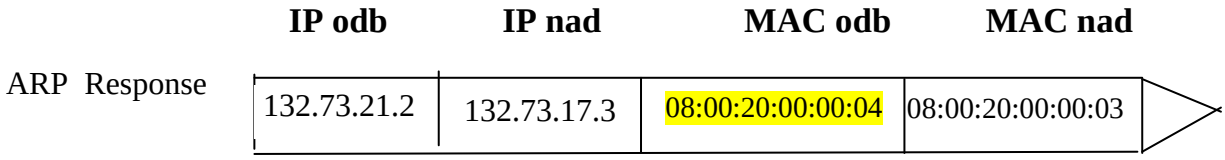
Mechanizm działania protokołu ARP w intersieci



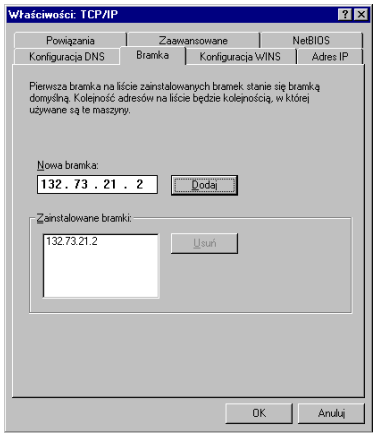
a) Etap 1 – celem jest znalezienie MAC karty sieciowej routera



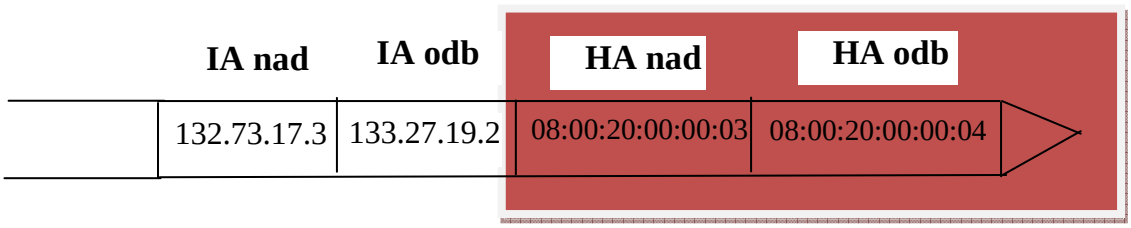
default gateway



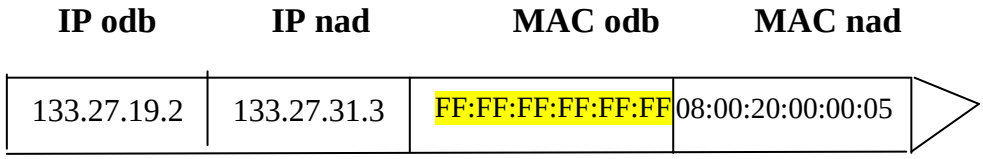
Okienko z adresem default gateway (Windows)



b) Etap 2 – znając MAC interfejsu routera stacja „nadawcza” wysyła ramkę Ethernet z właściwym danymi do routera.



c) Etap 3 – Pojawienie się ramki Ethernet w routerze już z adresem sieci nr 2 (133.27.0.0) w adresie IP odb powoduje, że router otwiera bramkę o adresie 133.27.31.3 „przerzucając” do niej ramkę. Nastepnie router generuje ramkę dla ARP Request tylko do sieci nr 2 o postaci:



4) Etap 4 – Uzyskanie przez router odpowiedzi na powyższy pakiet umożliwia sformowanie ostatecznie ramki Ethernet z właściwymi danymi i wysłanie jej do stacji docelowej.

Struktura danych wykorzystywanych przeprotokół ARP

a) **Hardware Type** - 2B – typ technologii warstwy łącza danych (np. Ethernet 0x0001), pełna lista na *www.iana.org/assignments/arp-parameters*

b) **Protocol Type** – 2B – tutaj określony jest protokół dla którego ARP realizuje swoje zadanie. Dla protokołu IP wartość pola wynosi 0x800

c) **Hardware Address Length** - 1B – określa w bajtach długość adresów w polach **Sender i Target Hardware Address –** 1B **-** (dla Ethernetu wartość pola wynosi 0x 6)

d) **Protocol Address Length** – 1B – określa w bajtach długość adresu protokołu w polach **Sender i Target Protocol Address**

e) **Operation -** 2B– kod operacji, np. 0x01 to operacja *ARP Request*, pełna lista kodów znajduje się na *www.iana.org/assignments/arp-parameters*

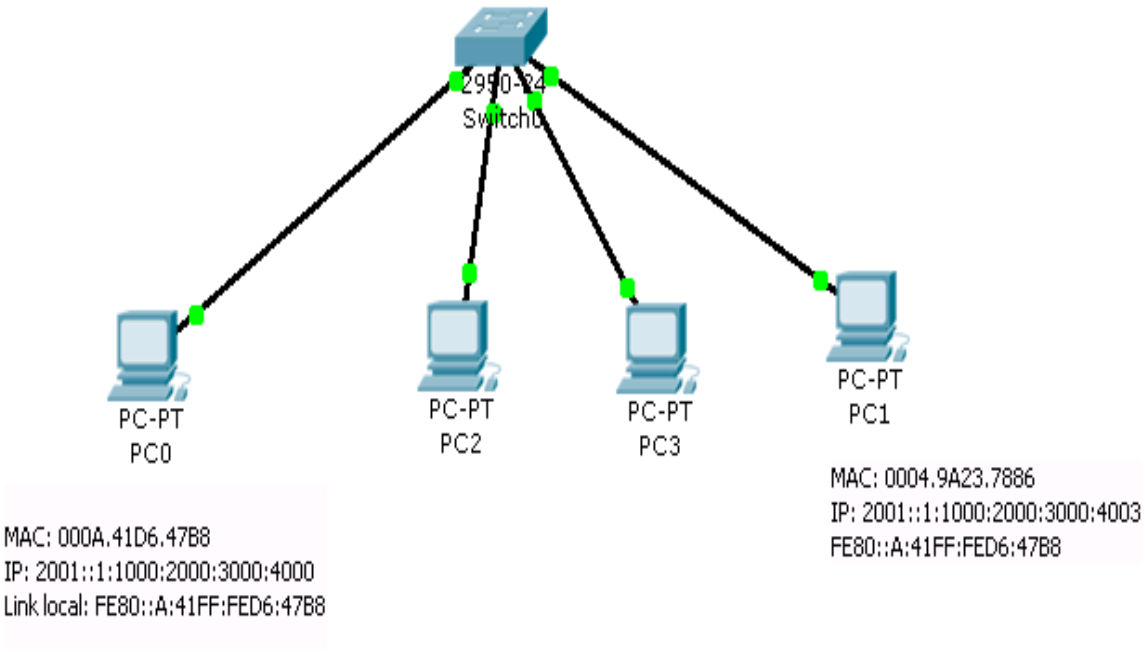
f) **Sender Hardware Address – sprzętowy adres nadawcy**

g) **Sender Protocol Address –adres protokołu nadawcy**

h) **Target Hardware Address – sprzętowy adres odbiorcy**

i) **Target Protocol Address –adres protokołu odbiorcy**

2. Mechanizmy protokołu NDP (*Neighbor Discovery Protocol*)



Etap 1 wysyłanie pakietu od PC0 do PC1

- adres źródłowy IP: 2001::1:1000:2000:3000:4000 (adres jednostkowy)
- adres docelowy IP: **FF02::1:FF**00:4003 - adres grupowy żądania węzła
- adres źródłowy MAC: 000A.41D6.47B8
- adres docelowy MAC: 3333.FF00.4003 (mapowanie *IP-MAC*)
- dane NDP: żądanie sąsiada (nr 135)

Etap 2 – Wysyłanie pakietu od PC1 do PC0

- adres źródłowy IP: 2001::1:1000:2000:3000:4003
- adres docelowy IP: 2001::1:1000:2000:3000:4000
- adres źródłowy MAC: 0004.9A23.7886
- adres docelowy MAC: 000A.41D6.47B8
- dane NDP: ogłoszenie sąsiada (nr 136):

WYKŁAD V. Podstawy protokołu TCP. Protokoły NAPT i NAT. Podstawy Routingu IP v.4. Intergracja sieci IP v4 oraz IP v6.

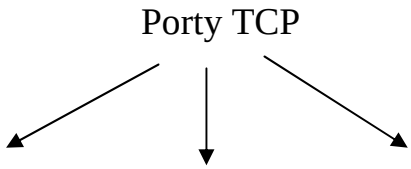
1. Podstawowa rola protokołu TCP

Pobranie danych z procesu aplikacji stacji nadawczej oraz dostarczenie tych danych do aplikacji na stacji odbiorczej (warstwa transportu).

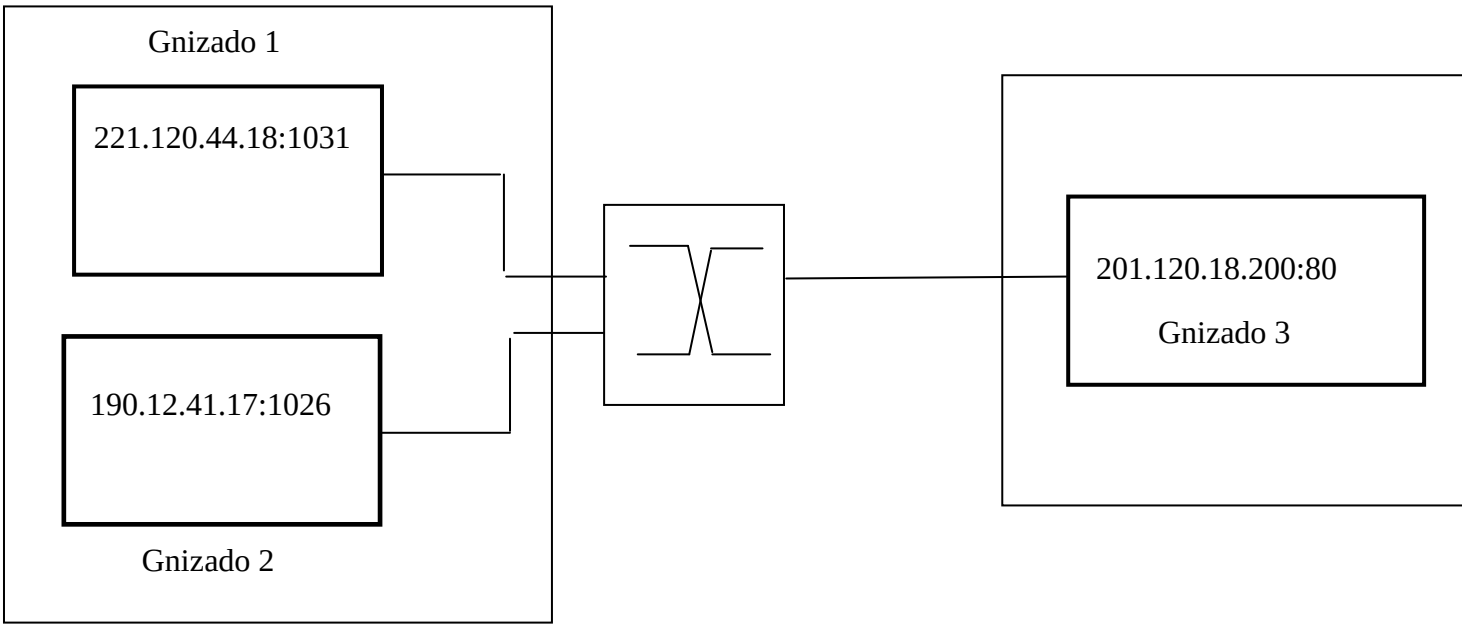
2. Elementy standardowego nagłówka TCP oraz ich znaczenie.

a) Source Port 2B – port aplikacji źródłowej,

b) Destination Port 2B – port aplikacji docelowej,



Ogólnie znane	Zarejestrowane	Prywatne (dynamiczne)
0-1023	1024-49151	49151-65535



c) **Sequence Number** – 4B – numer sekwencyjny pierwszego oktetu segmentu w wyjściowym strumieniu bajtów,

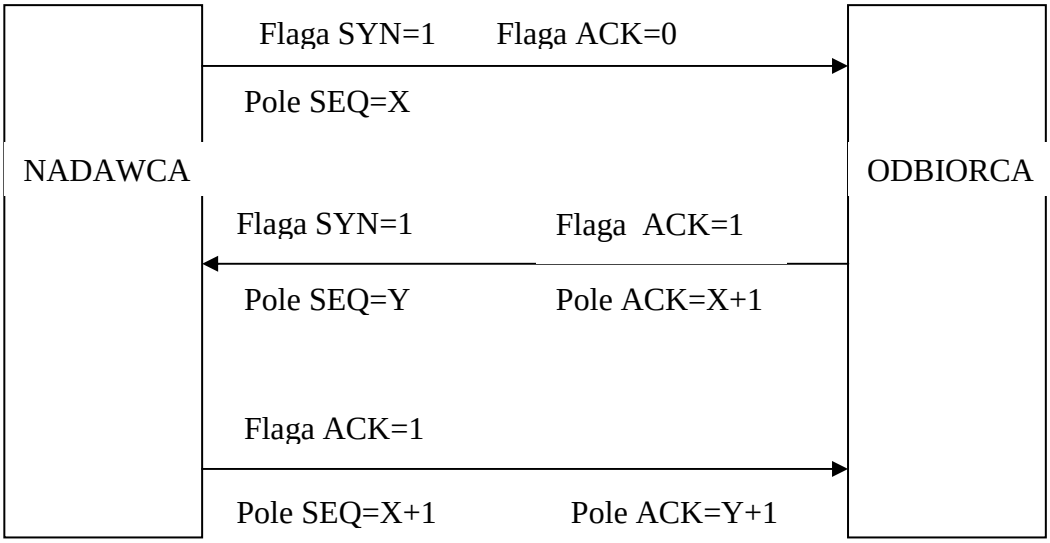
d) **Acknowledgment Number** – 4B **–** numer sekwencyjny kolejnego, oczekiwanego przez odbiorcę oktetu w wejściowym strumieniu danych,

e) **Data offset** – 4B – wskazuje początek danych,

f) **Reserved** – 6b – zastrzeżone do przyszłego użytku

g) **Flags** – 6 b – 6 jednobitowych flag TCP, np.: ACK, SYN, FIN

Trójstopniowe nawiązanie połączenia TCP



h) **Window –** 2B – liczba dostępnych bajtów w buforze pamięci, odbiorca przekazuje nadawcy informację o ilości danych jakie może do niego wysłać (*flow control*)

i) **Checksum** – 2 B – wartość sumy kontrolnej, zapewniającej integralność segmentu TCP (nagłówek + dane),

j) **Urgent Pointer** – 2B – pole do wskazania numerów sekwencyjnych dla których nadawca wymaga natychmiastowego potwierdzenia od odbiorcy

k) **Options** – 4B, dodatkowe opcje nagłówka.

3. Podstawowe usługi protokołu TCP

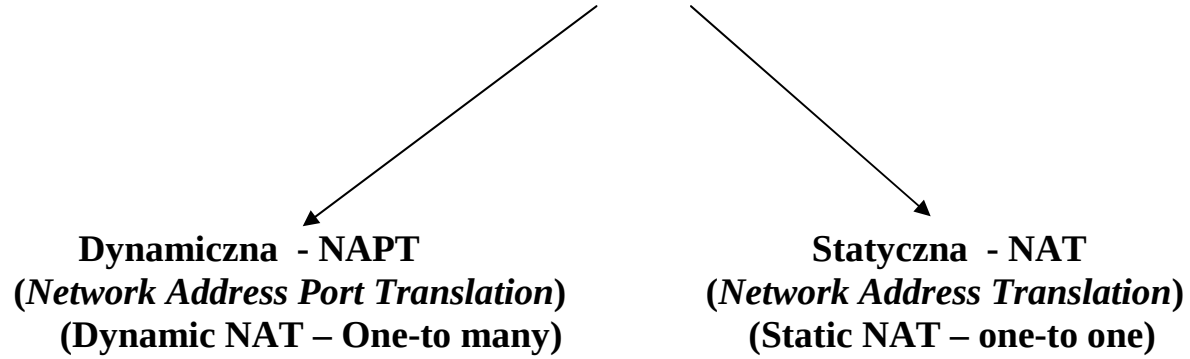
- segmentacja danych warstwy aplikacji,
- tworzenie logicznego połączenia w warstwie aplikacji typu jeden do jednego (z wykorzystaniem mechanizmu portów TCP),
- TCP jest zorientowany połączeniowo,
- niezawodność transmisji (potwierdzenie przyjęcia danych + suma kontrolna),
- pełnodupleksowość transmisji,
- sterowanie przepływem po stronie nadawcy i odbiorcy.

4. Protokoły translacji adresów i portów

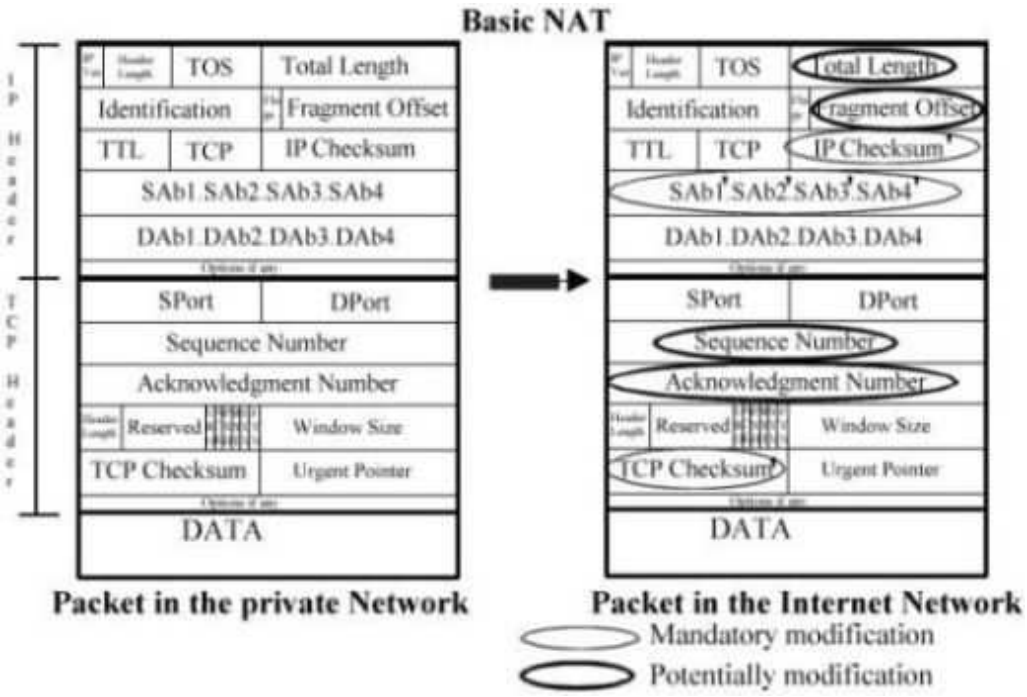
a) ograniczona przestrzeń adresowa IPv4 - głównym powodem stosowania protokołów translacji

b) Protokoły translacji implementowane są w systemach operacyjnych (Windows, Unix, Linux) oraz w routerach sprzętowych (routery graniczne LAN/WAN)

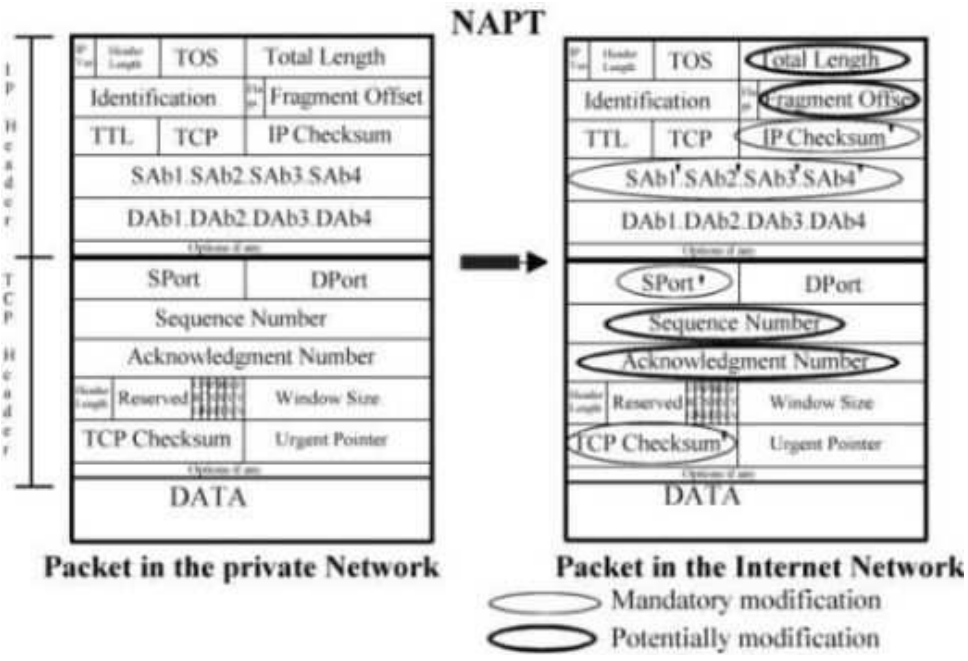
Odmiany translacji



c) Zasada działania protokołu NAT



d) Zasada działania protokołu NAPT



e) główne cechy protokołów

- bardzo korzystne zagospodarowanie przestrzeni adresowej IP v.4.0
- możliwość tworzenia serwerów usług internetowych (*Static* NAT),
- proces translacji wymaga czasu – spadek wydajności sieci

f) konfiguracja NAPT oraz Static NAT na routerach Cisco

Polecenia: *ip nat inside* – oznaczenie (wytypowanie) interfejsu prywatnego,

ip nat outside – oznaczenie (wytypowanie) interfejsu zewnętrznego, (np. publicznego),

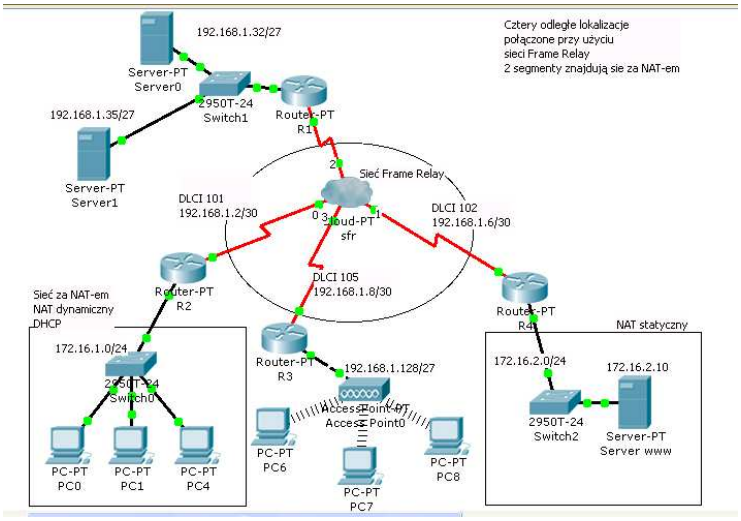
ip nat inside source static <adres_prywatny_IP> <adres zewnętrzny_IP> - określenie adresów translacji statycznej

ip nat pool <adres_zewn._IP_początkowy> <adres zewn. _IP_końcowy> <*maska_podsieci*> - określenie adresów (adresu) translacji dynalicznej

- powiązanie zasad list ACL z NAT:

ip nat inside source list <nazwa ACL> interface <nazwa _interfejsu> overload

Przykład rozwiązania NAT oraz NAPT dla połączeń technologii LAN/WAN



Konfiguracja routera R2

```
hostname R2
!
interface FastEthernet0/0
 no shutdown
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
!
interface Serial2/0
 no ip address
 no shutdown
 encapsulation frame-relay
 frame-relay lmi-type ansi
!
interface Serial2/0.1 point-to-point
 ip address 192.168.1.2 255.255.255.252
 frame-relay interface-dlci 101
 ip nat outside
!
router eigrp 50
 passive-interface FastEthernet0/0
 network 192.168.1.0
!
ip access-list extended sieczanatem
 permit ip 172.16.1.0 0.0.0.255 any
!
ip nat inside source list sieczanatem
interface Serial2/0.1 overload
!
ip dhcp excluded-address 172.16.1.1
!
ip dhcp pool siecprywatna
network 172.16.1.0 255.255.255.0
default-router 172.16.1.1
```

Konfiguracja routera R4

```
hostname R4
!
interface FastEthernet0/0
 no shutdown
 ip address 172.16.2.1 255.255.255.0
 ip nat inside
!
interface Serial2/0
 no ip address
 no shutdown
 encapsulation frame-relay
 frame-relay lmi-type ansi
!
interface Serial2/0.2 point-to-point
 ip address 192.168.1.6 255.255.255.252
 frame-relay interface-dlci 102
 ip nat outside
!
router eigrp 50
 passive-interface FastEthernet0/0
 network 192.168.1.0
!
ip nat inside source static 172.16.2.10
192.168.1.6
```

5. Podstawy routingu IP v4.

1. Podstawowe zadania routerów WAN:

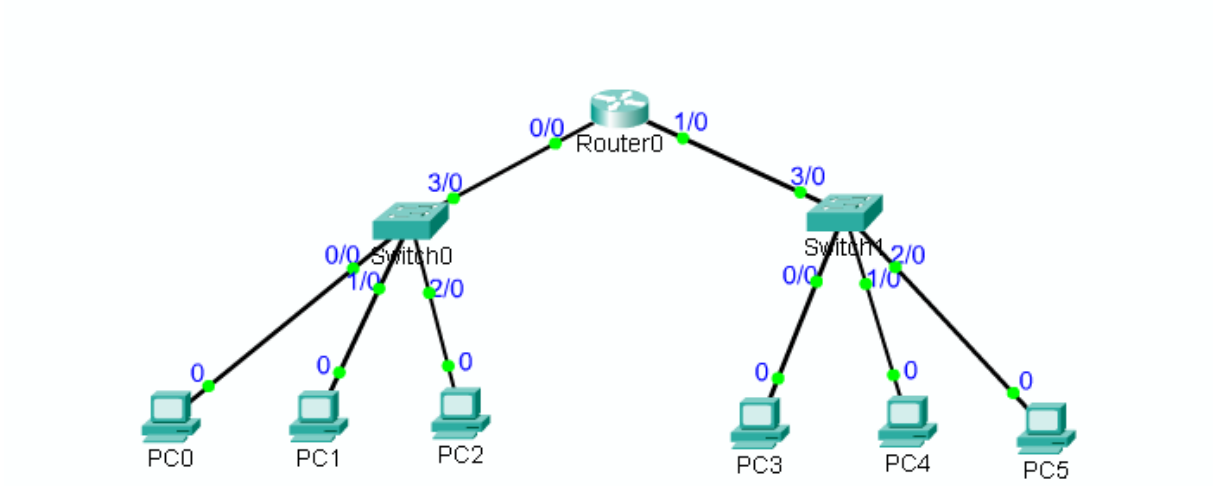
- przekazywanie pakietów IP od hosta nadawczego do odbiorczego przez różnorodne typy (technologie) sieci fizycznych (routing), na podstawie tabel routingu,

- utrzymywanie tablic routingu zawierających opis optymalnych tras, pozwalających dotrzeć do każdego możliwego miejsca poprzez wykorzystanie protokołów routingu dynamicznego (np. RIP, EIGRP, OSPF).

Routing - proces odbierania pakietów, podejmowanie decyzji o ich przekazaniu oraz ich przekazanie na poziomie warstwy 3.

Tabela routingu w routerze może być tworzona dynamicznie lub statycznie

Tabela routingu dla routera z dwoma podsieciami typu C



Routing Table for Router0

Type	Network	Port	Next Hop IP	Metric
C	10.0.0.0/8	1/0	--	0/0
C	221.23.23.0/24	0/0	--	0/0

Wybrane parametry tabeli routingu (dla routerów Cisco) :

TYPE – rodzaj definiowania trasy
C - connected directly (trasy połączone)
S – static (trasy statyczne) np. dla sieci małych, rzadko modyfikowanych
R – trasa RIP (trasy dynamiczne), ustalane przez protokół routingu dynamicznego RIP

NETWORK – adresy IP sieci (podsieci) docelowych oraz ich maski

PORT – interfejs wychodzący – przez ten interfejs router wysyła pakiety pasujące do trasy.

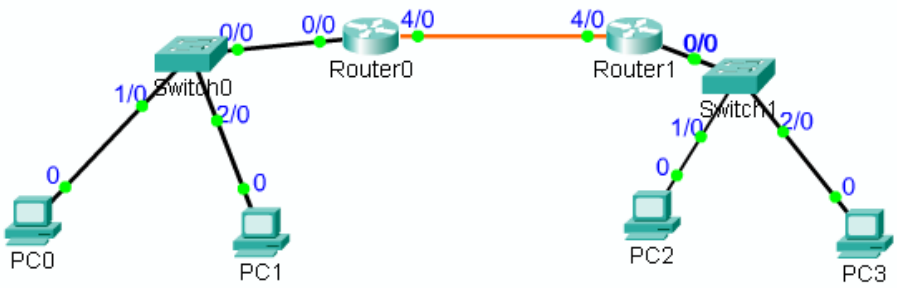
NEXT HOP IP – adres IP interfejsu następnego routera – dotyczy tras do sieci podłączonych do innego routera

METRIC – „jakość" trasy mierzona np. liczba przeskoków, szerokością pasma i innych. Każdy protokół routingu uwzględnia swoje własne parametry

Tabele routingu dla sieci typu C i S

Routing Table for Router0

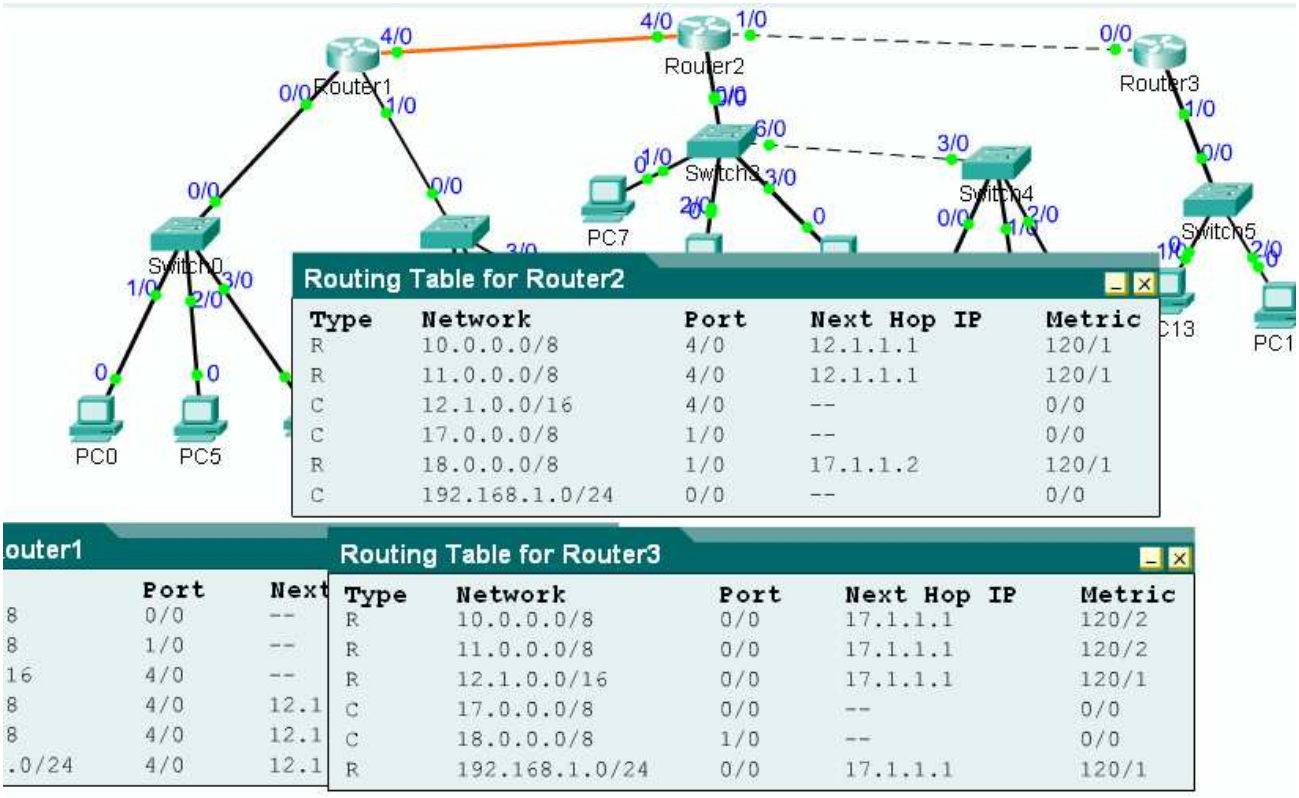
Type	Network	Port	Next Hop IP	Metric
C	10.0.0.0/8	0/0	--	0/0
C	120.0.0.0/8	4/0	--	0/0
S	192.168.1.0/24	--	120.1.1.2	1/0



Routing Table for Router1

Type	Network	Port	Next Hop IP	Metric
S	10.0.0.0/8	--	120.1.1.1	1/0
C	120.0.0.0/8	4/0	--	0/0
C	192.168.1.0/24	0/0	--	0/0

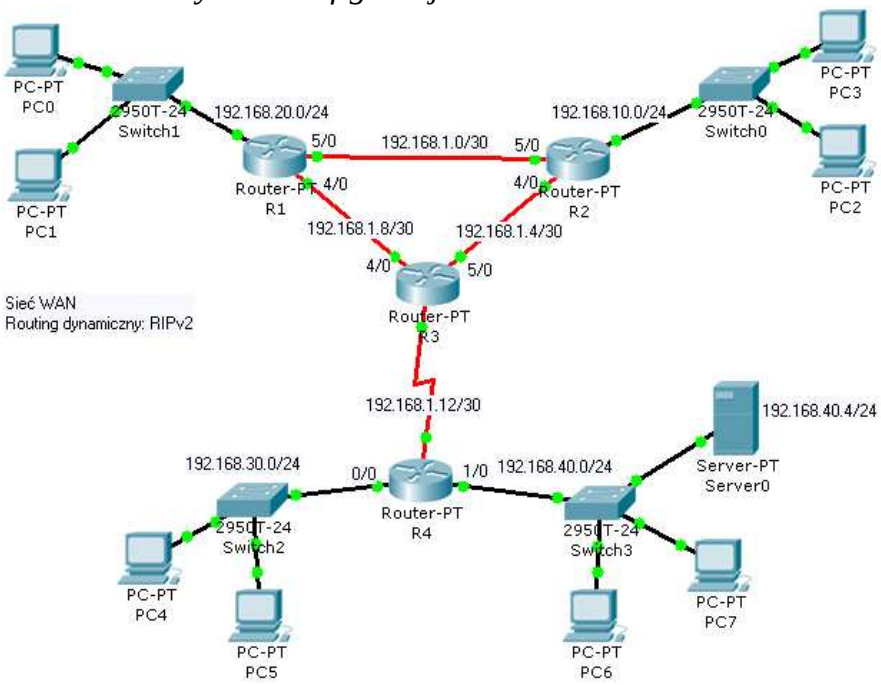
Tabele routingu z wpisami typu C oraz R



Funkcje protokołów routingu dynamicznego: RIP (*Routing Information Protocol*), IGRP (*Interior Gateway Routing Protocol*), EIGRP (*Enhanced IGRP*), OSPF (*Open shortest Path Firs*t), BGP (*Border Gateway Protocol*)

- zbieranie informacji o sieciach IP od sąsiednich routerów,
- ogłaszanie informacji o sieciach IP routerom sąsiednim,
- wybór najlepszej trasy na podstawie metryki
- wykrywanie zmian w topologii sieci, ogłaszanie tych zmian i wybór nowych, najlepszych z możliwych tras.

Przykład konfiguracji routeów RIP w intersieci



Konfiguracja routera R3

```
interface Serial2/0
 no shutdown
 ip address 192.168.1.13 255.255.255.252
 clock rate 56000
!
interface FastEthernet4/0
 no shutdown
 ip address 192.168.1.9 255.255.255.252
!
interface FastEthernet5/0
 no shutdown
 ip address 192.168.1.5 255.255.255.252
!
router rip
 version 2
 network 192.168.1.0
```

Konfiguracja routera R4

```
interface FastEthernet0/0
 no shutdown
 ip address 192.168.30.1 255.255.255.0
!
interface FastEthernet1/0
 no shutdown
 ip address 192.168.40.1 255.255.255.0
!
interface Serial2/0
 no shutdown
 ip address 192.168.1.14 255.255.255.252
!
router rip
 version 2
 passive-interface FastEthernet0/0
 passive-interface FastEthernet1/0
 network 192.168.1.0
 network 192.168.30.0
 network 192.168.40.0
```