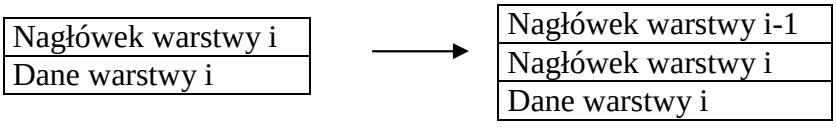
# Model warstwowy komunikacji sieciowej. Budowa nagłówka ramki Ethernet II i pakietu IP.

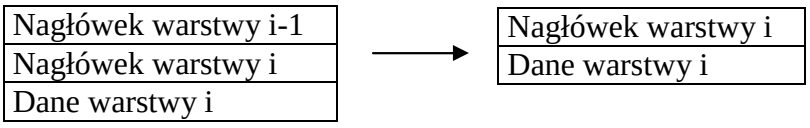
Model warstwowy OSI: (Open Systems Interconnection)

| |
|---|
| Aplikacji |
| Prezentacji |
| Sesji |
| Transportu |
| Sieci |
| Łącza danych |
| Fizyczna |

Każdy protokół sieciowy można opisać przy pomocy powyższego modelu, przy czym nie zawsze do opisu protokołu używane są wszystkie warstwy. Np. protokół IP składa się tylko z warstwy sieci, natomiast nie może funkcjonować bez wsparcia dwóch warstw niższych. Ogólna zasada stanowi, że protokół umiejscowiony w warstwie n wymaga wsparcia wszystkich warstw od 1 do n-1. Poszczególne warstwy (oprócz fizycznej) realizowane są przez oprogramowanie. W trakcie wysyłania dane są przekazywane z warstw wyższych do niższych, przy czym każda warstwa dodaje swój nagłówek. W rezultacie dane przekazywane przez warstwę i do warstwy i-1 składają się z danych i nagłówka warstwy i, co przedstawia następujący rysunek:




Po dotarciu do celu, dane przekazywane są w odwrotną stronę, mianowicie od warstw niższych do wyższych, przy czym każda warstwa usuwa swój nagłówek. Jest to przedstawione na kolejnym rysunku ilustrującym przekazywanie danych z warstwy i-1 do warstwy i:




Po dotarciu do warstwy n, usuwany jest jej nagłówek i dane ulegają przetworzeniu przez oprogramowanie tej warstwy.

Warstwy MAC i LLC

Warstwa łącza danych podzielona jest na dwie podwarstwy – MAC (Media Access Control) i LLC (Logical Link Control). Funkcje pierwszej z nich to: odczytywanie i zapis adresów sprzętowych (MAC), definiowanie formatu ramki, realizowanie metody dostępu do medium transmisyjnego (żeton, CSMA/CD), kontrola błędów. Podstawową funkcją podwarstwy LLC jest tzw. multipleksowanie i de-multipleksowanie protokołów warstwy sieci.

Model warstwowy TCP/IP:

Jest uproszczeniem modelu ISO, zawiera tylko 5 warstw:

| |
|---|
| Aplikacji |
| Transportu |
| Sieci |
| Łącza danych |
| Fizyczna |

Ethernet II:

W sieciach Ethernet stosowane jest kodowanie typu Manchester. Polega ono na tym, że bit 1 jest kodowany zmianą z wyższego napięcia na niższe, a bit 0 – odwrotnie. Zmiana zachodzi w połowie czasu trwania bitu.

Jest to najczęściej stosowany typ ramki w sieciach Ethernet. Budowa ramki Ethernet II przedstawia się następująco:

| Preambuła + SFD | Adres odb. | Adres nad. | Typ | Dane | FCS |
|---|---|---|---|---|---|
| 8 oktetów | 6 oktetów | 6 oktetów | 2 oktety | 46-1500 | 4 oktety |

Preambuła – ciąg 56 bitów (na przemian jedynki i zera) umożliwiający synchronizację nadawcy i odbiorcy. Nawet, jeśli karty sieciowe po obu stronach łącza ustawione są na tę samą prędkość, zazwyczaj występuje między nimi niewielka różnica, która musi być zniwelowana w wyniku synchronizacji.

SFD – znacznik początku ramki (Starting frame Delimiter), jest to ciąg następujących 8 bitów: 1 0 1 0 1 0 1 0 1 1

Adres odbiorcy – docelowy adres MAC składający się z 6 oktetów

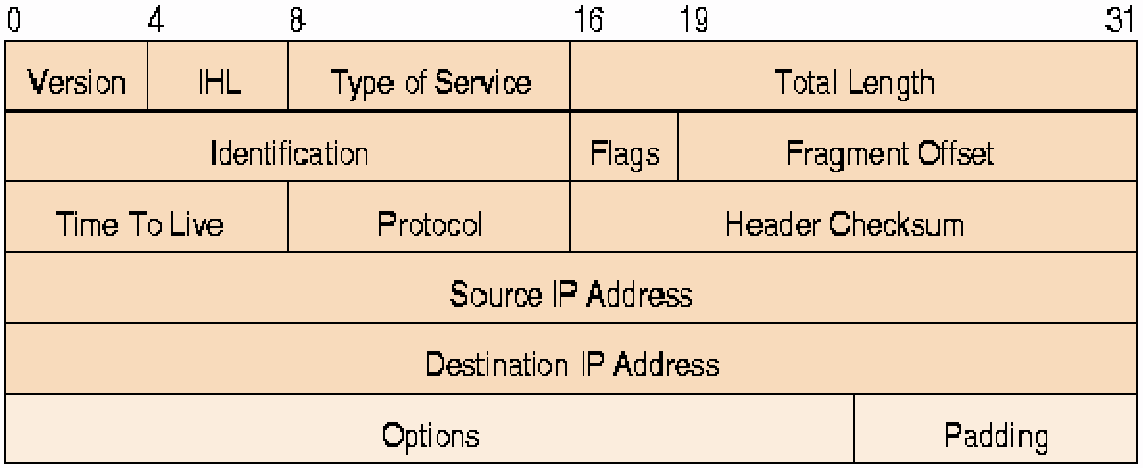
Adres nadawcy – źródłowy adres MAC składający się z 6 oktetów

Typ – W polu tym przesyłana jest informacja o protokole warstwy sieci. Dla IP jest to 0x800, dla ARP – 0x806, dla IPX – 0x8137. Ważne jest, aby wartość tego pola była większa od 1500 (0x5DC). W przeciwnym przypadku pole zawiera informację o **długości** pola danych i ramka nie jest typu Ethernet II, ale należy do typu Raw (standard IEEE 802.3) albo typu LLC (standard IEEE 802.2). Typ Raw nie zawiera informacji o protokole warstwy sieci i jest stosowany w sieciach Novell. W przypadku LLC, dwa pierwsze bajty znajdujące się za polem „Typ" zawierają informację o protokole warstwy sieci (DSAP, SSAP). Rozszerzeniem typu LLC jest typ SNAP.

Dane – ze względu na fizyczne parametry sieci Ethernet, wprowadzone są ograniczenia na całkowitą długość ramki. Jeśli w trakcie nadawania wystąpi kolizja, to stacja musi mieć możliwość stwierdzenia tego faktu jeszcze przed zakończeniem nadawania. Wynika stąd dolne ograniczenie na długość ramki. Ramki nie mogą być też zbyt długie, m.in. ze względu na możliwość utraty synchronizacji między stacją nadającą i odbierającą.

FCS – suma kontrolna (Frame Control Sequence), wykorzystywana wówczas, jeśli oprogramowanie warstwy łącza danych zawiera mechanizmy sprawdzania poprawności transmisji.

Budowa nagłówka IP:




Opis pól:

Version – numer wersji protokołu IP (4 – IPv4, 6 – IPv6)

IHL – długość nagłówka IP (Internet Header Length) w słowach 32-bitowych (4-bajtowych). Jest konieczne, ponieważ w skład nagłówka IP wchodzi pole opcji o zmiennej długości. Minimalna długość nagłówka IP wynosi 20 bajtów (brak opcji), natomiast maksymalna – 15x4=60 bajtów. Górne ograniczenie na długość nagłówka IP wynika z faktu, że pole IHL składa się z 4 bitów i 15 jest największą liczba, jaką można w nim zapisać.

TOS – typ obsługi (Type of Service), może zawierać wskazania dla routerów odnośnie wyboru trasy dla pakietu, standardowo składa się z samych zer. W tabeli routingu występuje rubryka TOS. Router wybiera daną trasę, jeśli zawartość pola TOS pakietu jest zgodna z zawartością rubryki TOS dla tej trasy. Bity 0, 1 i 2 oznaczają ważność pakietu (precedence), bit 3 – żądanie małego opóźnienia (delay), bit 4 – żądanie dużej przepustowości (throughput), bit 5 – żądanie dużej niezawodności (reliability). Bity 7 i 8 są zawsze zerami.

Total Length – całkowita długość pakietu IP (łącznie z nagłówkiem) mierzona w bajtach (słowach 8-bitowych). Pole to ma długość 16 bitów, z czego wynika, że maksymalna długość pakietu IP wynosi 2^16 - 1 = 65535 oktetów.

Trzy kolejne pola wykorzystywane są przez mechanizmy fragmentacji i składania pofragmentowanych pakietów IP. Fragmentacja polega na dzieleniu pakietu na części o długości nie przekraczającej MTU (maksymalna długość pola danych ramki) tej sieci, przez którą pakiet ma zostać bezpośrednio przesłany. Przykładowo, MTU wynosi 1500 dla sieci Ethernet, a 4470 dla FDDI. Fragmentacji mogą dokonywać zarówno hosty jak i routery. Jeśli

jest to konieczne, router fragmentuje pakiety przekazywane z sieci o większym MTU do sieci o mniejszym MTU.

Identification – liczba jednoznacznie identyfikująca pakiet, jest kopiowana z nagłówka pakietu, do nagłówków wszystkich fragmentów, na które pakiet jest dzielony. Informuje hosta docelowego, które fragmenty składają się na dany pakiet..

Flags – bit 0 jest zawsze zerem. Bit 1 (DF – do not fragment) służy do informowania routerów, czy mogą fragmentować pakiet; jeśli jest jedynką, to w przypadku konieczności fragmentowania, router odrzuca pakiet i wysyła do nadawcy komunikat o błędzie. Bit 2 (MF – more fragments) równy 1 oznacza, że dany fragment nie jest ostatni.

Fragment Offset – oznacza przesunięcie początku fragmentu względem pierwszego bajtu pakietu. Jest mierzone w słowach 8-bajtowych (64-bitowych). Dla pierwszego fragmentu ma wartość zero.

Time to Live – oznacza maksymalny czas w sekundach, przez jaki pakiet może przebywać w sieci. Każdy router na trasie pakietu sprawdza wartość tego pola i przed przekazaniem pakietu zmniejsza ją o liczbę większą lub równą 1 (czas w sekundach, przez jaki pakiet był przetwarzany). Jeśli router otrzyma pakiet z TTL równym 1, to odrzuca go. W ten sposób z sieci usuwane są np. pakiety krążące w pętli.

Protocol – określa protokół następnej warstwy, zgodnie z opisem w dokumencie RFC 1060. Przykładowe wartości to 6 dla TCP, 17 dla UDP, 2 dla IGMP, 1 dla ICMP.

Header Checksum – suma kontrolna nagłówka. Przy jej obliczaniu uwzględniane są wyłącznie pola nagłówka, bez pola danych. Musi być aktualizowana na każdym routerze, ponieważ zawartość pola TTL ulega, a niektórych innych pól (np. TOS, Options) – może ulec zmianie po przejściu pakietu przez router.

Następne dwa pola zawierają źródłowy i docelowy adres IP

Options – opcjonalne pole opcji. Każda opcja składa się z oktetu, w którym zapisany jest jej kod, opcjonalnego oktetu określającego jej długość, oraz opcjonalnego ciągu oktetów zawierających dane opcji. Pierwszy bit kodu opcji określa, czy opcje powinny być kopiowane do wszystkich fragmentów (wartość 1), czy tylko do pierwszego fragmentu (wartość 0). Dwa kolejne bity określają klasę opcji, natomiast pięc pozostałych – numer opcji. W poniższej tabeli przedstawione są najważniejsze opcje IP.

| Klasa | Numer | Długość | Opis |
|---|---|---|---|
| 0 | 0 | 1 | Koniec listy opcji. Zajmuje tylko 1 oktet. |
| 0 | 3 | zmienna | Swobodne trasowanie według nadawcy. |
| 0 | 9 | zmienna | Rygorystyczne trasowanie według nadawcy |
| 0 | 7 | zmienna | Zapisywanie trasy pakietu. |
| 2 | 4 | zmienna | Zapisywanie stempli czasowych wzdłuż trasy. |

Padding – wypełnienie do pełnego słowa 32-bitowego. Składa się z samych zer.

Przykłady fragmentacji:

**Przykład 1**

Przedstawić wynik fragmentacji możliwie największego pakietu IP (2^16 – 1 = 65 535 bajtów razem z nagłówkiem), jeśli pakiet ten jest wysyłany w sieć Ethernet (MTU = 1500), a nagłówek IP ma standardową długość wynoszącą 20 bajtów.

Długość pola danych pakietu = 65535 – długość nagłówka IP = 65535 – 20 = 65515

MTU = Długość nagłówka IP + Długość pola danych IP fragmentu, skąd wynika, że
Długość pola danych IP fragmentu = 1480

Z powyższych obliczeń wynika, że powstaną 44 fragmenty o długości 1480 bajtów, oraz 45-ty (ostatni) fragment o długości 395 bajtów (65515 = 44×1480 + 395). W standardowej notacji wynik powyższej fragmentacji zapisuje się w następujący sposób:

1 fragment: 1480@0 MF
2 fragment: 1480@1480 MF
3 fragment: 1480@2960 MF
...
44 fragment: 1480@63640 MF
45 fragment: 395@65120 LF

**Przykład 2**

W sieci Ethernet wysyłany jest datagram TCP zawierający 6580 bajtów danych użytkownika. Dane te przechodzą następnie przez łącze SLIP (MTU=520). Ile i jakie fragmenty powstaną przy przechodzeniu danych przez to łącze? Do opisu fragmentów użyj notacji wielkość@przesunięcieMF/LF. **Uwaga**: zakładamy, że nagłówek IP ma minimalną długość wynoszącą 20 oktetów, oraz że pole danych IP zawiera nagłówek TCP o długości 20 oktetów. Wielkość i przesunięcie mają być podane w bajtach (formalnie, przesunięcie powinno być podane w porcjach 8-bajtowych).

Długość pola danych IP = Długość nagłówka TCP + Długość pola danych TCP
Długość pola danych IP = 20 + 6580 = 6600

Każdy fragment zawiera nagłówek i pole danych IP, ponieważ MTU=520, więc
max długość pola danych IP + min długość nagłówka IP = 520,

skąd wynika, że

Max długość pola danych IP fragmentu = 500

Ze względu na to, że pole „Fragment Offset“ wyraża przesunięcie fragmentu w porcjach 8-bajtowych, długość każdego fragmentu, z wyjątkiem ostatniego, musi być wielokrotnością ośmiu. Formalnie, przesunięcia fragmentów powinny być podane w porcjach 8-bajtowych, tak jak ma to miejsce w nagłówku IP.

W standardowej notacji wynik powyższej fragmentacji zapisuje się w następujący sposób:

1 fragment: 496@0 MF
2 fragment: 496@496 MF
3 fragment: 496@992 MF
4 fragment: 496@1488 MF
...
13 fragment: 496@5952 MF
14 fragment: 152@6448 LF

**Uwaga:** Jeśli transmisja odbywa się w sieci Ethernet, wówczas minimalna długość pola danych ramki wynosi 46 oktetów. Przy założeniu, że nagłówek IP zajmuje 20 oktetów, dane fragmentu muszą mieć długość co najmniej 26 oktetów. **Zatem, dla pakietu IP ze standardowym (brak opcji) nagłówkiem, minimalna długość pola danych fragmentu IP wysyłanego w sieć Ethernet wynosi 26.** W razie konieczności pole danych ostatniego fragmentu uzupełniane jest bitami zerowymi.