# Rozbudowa i naprawa sieci. Kompendium


Autorzy: Scott Mueller, Terry W. Ogletree
Tłumaczenie: Pod redakcją Bartłomieja Królickiego na podstawie tłumaczenia Pawła Gonery, Adama Jarczyka, Piotra Pilcha i Mikołaja Szczepaniaka
ISBN: 83-7361-440-0
Tytuł oryginału: Upgrading and Repairing Networks: Field Guide, 4th Edition
Format: B5, stron: 280

### Przewodnik po sprzęcie komputerowym dla hobbystów i profesjonalistów

Zgodnie ze znanym sloganem firmy Sun Microsystems sprzed czterdziestu lat („The network is the computer") komputery ujawniają w pełni swe możliwości dopiero po połączeniu ich w sieć. Nieustanny rozwój technologiczny sprawia, że (coraz lepsze) sieci komputerowe zdobywają sobie coraz większą popularność i coraz szersze obszary zastosowań. Jednocześnie ich projektowanie, budowanie, konfigurowanie i (przede wszystkim) efektywne wykorzystywanie wymaga posiadania odpowiednich kwalifikacji i nieustannego ich doskonalenia. Także ze względu na rozmaite konsekwencje potencjalnych problemów w funkcjonowaniu sieci zagadnieniem pierwszej wagi staje się wypracowanie środków i metod sprawnego radzenia sobie z tymi problemami – ich rozwiązywania i zapobiegania im.

Niniejsza książka stanowi kompendium poświęcone niezliczonym zagadnieniom z zakresu sieci komputerowych – ich tworzeniu, diagnozowaniu, naprawianiu, ulepszaniu i rozbudowywaniu. Czytelnik znajdzie tu omówienie takich zagadnień, jak (między innymi):

- Topologie sieci
- Sprzęt sieciowy (routery, przełączniki, mosty, krosownice, modemy) i okablowanie (skrętki, kable koncentryczne, światłowody)
- Protokół Ethernet
- Sieci wirtualne
- Model referencyjny OSI i protokoły sieciowe
- Połączenia sieciowe
- Sieci bezprzewodowe
- Bezpieczeństwo, związane z nim zagrożenia i środki zapobiegawcze (uprawnienia dostępu, szyfrowanie, zapory sieciowe)
- Problemy w działaniu sieci, ich diagnozowanie i służące do niego narzędzia
- Modernizacja i rozbudowa sieci

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

# Spis treści

Rozdział 2.

# Protokół Ethernet

Mimo że inne technologie sieci lokalnych, jak Token-Ring czy IPX/SPX firmy Novell, nadal są stosowane, popularność sieci Ethernet znacznie przewyższa popularność wszystkich pozostałych.

## Standardy sieci Ethernet

Za tworzenie standardów dla sieci lokalnych i rozległych odpowiada komitet IEEE 802 sieci LAN i MAN (*IEEE 802 LAN/MAN Standards Committee*).

Oto najbardziej popularne standardy sieci Ethernet (w kolejności ich powstawania):

- **10BASE-5** — zwany często „grubym" Ethernetem standard wykorzystywał grube przewody koncentryczne. „10" w nazwie oznacza maksymalną przepustowość sieci, czyli 10 megabitów na sekundę (Mb/s). Liczba „5" oznacza, że maksymalna długość segmentu wynosi 500 metrów. Aby zainstalować nowy węzeł w sieci, należy użyć tzw. wampira, który jest podłączany do okablowania szkieletowego.
- **10BASE-2** — zwany często „cienkim" Ethernetem standard przewiduje pracę sieci z maksymalną szybkością 10 Mb/s i wykorzystuje cieńsze, łatwiejsze w instalacji przewody. Maksymalna długość segmentu wynosi 185 metrów. Jeśli zastosujemy repeatery, łączna długość przewodów może wynosić nawet 925 metrów. Tworzenie prostych magistral jest możliwe dzięki stosowaniu złącza BNC w kształcie T.
- **10BASE-36** — ten rzadko stosowany standard sieci Ethernet wykorzystuje sygnalizację szerokopasmową. Technologia przewiduje stosowanie przewodu koncentrycznego zawierającego trzy zestawy przewodów, każdy w oddzielnym kanale, z których każdy operuje z szybkością 10 Mb/s i może mieć długość do 3600 metrów.

- **10BASE-T** — połączenia sieciowe są prowadzone od stacji roboczych do centralnego koncentratora lub przełącznika, o maksymalnej długości 100 metrów, tworząc fizyczną topologię gwiazdy. Zastosowanie okablowania nieekranowanej skrętki ( „T" w nazwie standardu) sprawia, że sieć jest tańsza i znacznie łatwiejsza w instalacji. Ponadto centralizacja sieci umożliwia jej łatwe testowanie w poszukiwaniu błędów, izolowanie wadliwych portów oraz przenoszenie użytkowników pomiędzy segmentami.
- **10BASE-FL** — pracuje z szybkością 10 Mb/s i wykorzystuje przewody światłowodowe; w szczególności światłowody wielomodowe (ang. *multimode fiber cable — MMF*) z rdzeniem o średnicy 62,5 mikrona i płaszczem o średnicy 125 mikronów. Wykorzystuje się w nich dwa osobne włókna do wysyłania i odbierania danych, co umożliwia komunikację w pełnym dupleksie.
- **100BASE-TX** — standard umożliwiający przesyłanie danych z szybkością 100 Mb/s. Wykorzystuje się przewody kategorii 5, co umożliwia zwiększenie odległości dzielącej stację roboczą i koncentrator do 100 metrów. Do przesyłania danych są wykorzystywane cztery żyły w przewodzie.
- **100BASE-T4** — wykorzystuje przewody kategorii 3 lub 5, więc maksymalna odległość pomiędzy stacją roboczą a koncentratorem wynosi 100 metrów. Komunikacja odbywa się za pomocą czterech żył w przewodzie. Jest to kolejny standard umożliwiający przesyłanie danych z szybkością 100 Mb/s.
- **100BASE-FX** — wykorzystuje wielomodowe przewody światłowodowe, dzięki czemu maksymalna odległość dzieląca stację roboczą i koncentrator może wynosić nawet 412 metrów. Jedno włókno światłowodu jest wykorzystywane do nadawania, drugie do odbierania danych.
- **1000BASE-SX** — dokument opisujący standardy IEEE 802.3z został zatwierdzony w roku 1998 i definiuje kilka technologii sieciowych z rodziny nazwanej Gigabit Ethernet. Standard 1000BASE-SX został zaprojektowany z myślą o pracy z wielomodowymi przewodami światłowodowymi wykorzystującymi fale świetlne o długości około 850 nanometrów (nm). „S" w nazwie standardu oznacza mniejszą długość (ang. *short*) generowanych fal świetlnych. Maksymalna długość segmentu sieci wynosi 550 metrów.
- **1000BASE-LX** — kolejny standard gigabitowego Ethernetu zakładający pracę sieci z wykorzystaniem jednomodowego lub wielomodowego okablowania światłowodowego. Litera „L" w nazwie standardu oznacza większą długość fal świetlnych, od 1270 do 1335 nanometrów. Maksymalna długość segmentu sieci wynosi 550 metrów w przypadku stosowania przewodów wielomodowych i 5000 metrów w przypadku wykorzystania przewodów jednomodowych.
- **1000BASE-CX** — ten standard umożliwia wykorzystanie przez gigabitowy Ethernet ekranowanych przewodów miedzianych. Technologia została zaprojektowana z myślą o łączeniu urządzeń znajdujących się w niewielkich odległościach (do 25 metrów).
- **1000BASE-T** — standard IEEE 802.3ab dodano do warstwy fizycznej technologii Gigabit Ethernet wykorzystującej nieekranowaną skrętkę kategorii 5. Maksymalna długość segmentu sieci 1000BASE-T wynosi 100 metrów.

# Kolizje oraz IEEE 802.3: Metoda dostępu CSMA/CD

Zanim opracowano przełączniki pracujące w pełnym dupleksie, komunikujące się węzły sieci Ethernet uzyskiwały dostęp do współdzielonego nośnika sieciowego za pomocą mechanizmu zwanego *Carrier Sense Multiple Access/Collision Detect* (*CSMA/CD*). Oznacza to, że przed podjęciem próby przesłania danych we współużytkowanym segmencie sieci LAN, komputer (lub urządzenie sieciowe) sprawdza (ang. *Carrier Sense*) najpierw, czy w danym momencie inne urządzenie nie przesyła danych w sieci (ang. *Multiple Access*). Jeśli nie, węzeł może rozpocząć transmisję danych do sieci. Jeśli więcej niż jeden węzeł wykryje, że nośnik sieci nie jest wykorzystywany, i oba (lub więcej) węzły rozpoczną w tym samym czasie przesyłanie danych, nastąpi kolizja (ang. *Collision Detect*). W takim przypadku wszystkie węzły zakończą przesyłanie danych i po losowym (oczywiście z pewnymi ograniczeniami) czasie spróbują wznowić transmisję.

Używany we wczesnych implementacjach Ethernetu schemat kodowania Manchester wykorzystywał sygnały elektryczne o napięciu od –1,85 V do 1,85 V. Kolizje były wówczas wykrywane za pomocą pomiarów napięcia, które w przypadku ich wystąpienia wykraczało poza dopuszczalny przedział.

W sieciach zgodnych ze standardem Ethernet 10 Mb/s dane są przesyłane z szybkością 10 milionów bitów na sekundę. Specyfikacja standardu określa, że czas propagacji pakietu w sieci nie przekracza 51,2 milisekund (czas zbliżony do przesłania 64 bajtów przy szybkości 10 Mb/s). Stacja robocza nie może rozpocząć transmisji nowego pakietu, dopóki nie minie czas potrzebny do przesłania pakietu pomiędzy dwoma najbardziej oddalonymi węzłami w sieci Ethernet. Jeśli urządzenie nie będzie nadawało w czasie propagacji pakietu w sieci, straci możliwość wykrycia kolizji, zanim przystąpi do nadawania następnej ramki. Jeśli rozmiar ramki, która wymaga ponownego przesłania, jest mniejszy niż 64 bajty, węzeł nadawczy wypełni ją zerami, by spełnić warunek minimalnej długości ramki.

W specyfikacji standardu Ethernet II zdefiniowano także maksymalny rozmiar ramki — ramka o minimalnej długości 64 bajtów może mieć maksymalnie 1500 bajtów.

Komunikacja urządzeń w sieci Ethernet w 6 krokach:

1. Nasłuchuj sieć, by określić, czy którekolwiek inne urządzenie aktualnie nie transmituje swoich danych (ang. *Carrier Sense — CS*).
2. Jeśli żadne inne urządzenie nie nadaje, rozpocznij transmisję.
3. Jeśli więcej niż jedno urządzenie wykryje w danej chwili brak transmisji, urządzenia mogą jednocześnie rozpocząć nadawanie.
4. Kiedy dwa urządzenia rozpoczynają nadawanie swoich danych w tym samym momencie, wysyłany przez nie sygnał jest zniekształcony, co transmitujące urządzenia powinny wykryć (ang. *Collision Detect — CD*).
5. Po nadaniu danych w sieci urządzenie przez chwilę nasłuchuje sieć, by określić, czy transmisja zakończyła się pomyślnie, czy też nastąpiła kolizja. Pierwsze

urządzenie, które wykryje kolizję, rozsyła sygnał blokujący z kilkoma bajtami przypadkowych danych, by poinformować o zaistniałej sytuacji pozostałe urządzenia w sieci.

6. Każde urządzenie, którego działalność miała związek z wykrytą kolizją, wstrzymuje na krótko (kilka milisekund) swoją pracę i nasłuchuje sieć, by określić, czy nośnik sieciowy jest używany, i próbuje wznowić transmisję. Każdy węzeł powodujący kolizję wykorzystuje algorytm losowo generujący czas oczekiwania, ograniczając tym samym możliwość ponownego wystąpienia kolizji.

## Algorytm oczekiwania

Algorytm oczekiwania jest jednym z podstawowych elementów mechanizmu CSMA/CD. Zamiast oczekiwać przez określony czas, urządzenie sieciowe wstrzymuje swoją pracę i przestaje nadawać dane, obliczana jest losowa wartość, którą urządzenie wykorzystuje do wyznaczenia liczby milisekund, po upłynięciu których wznowi transmisję.

Do wyznaczania tego czasu mechanizm obliczeń nosi nazwę skróconego binarnego algorytmu odczekiwania wykładniczego (ang. *Truncated Binary Exponential Backoff Algorithm*). Za każdym razem, gdy z powodu próby wysłania konkretnej ramki w sieci następuje kolizja, urządzenie nadające wstrzymuje pracę na czas, który z każdą kolizją jest dłuższy. Urządzenie podejmuje maksymalnie 16 prób transmitowania danych. Jeśli po ich wykonaniu stwierdzi, że przesłanie tych informacji za pomocą nośnika sieciowego jest niemożliwe, opuszcza daną ramkę i informuje o zaistniałej sytuacji składową wyższego poziomu stosu protokołów, która odpowiada albo za wznowienie transmisji, albo za raportowanie o błędzie użytkownikowi aplikacji.

# Ramki Ethernet

Jednostka danych w warstwie sieci jest nazywana *pakietem* lub *datagramem* (patrz rysunek 2.1). Pojęcie *datagramu* odnosi się zwykle do jednostek danych w usługach bezpołączeniowych, pojęcie *pakietu* dotyczy zazwyczaj jednostek danych w usługach połączeniowych. W warstwie łącza danych te datagramy nazywamy *ramkami*. Każda ramka zawiera zarówno informacje wymagane do jej dostarczenia do odpowiedniego adresata przez nośnik sieciowy, jak i wymieniane za jej pomocą właściwe dane. W warstwie fizycznej ramka jest transmitowana w postaci ciągu bitów, który jest uzależniony od konkretnej technologii wykorzystywanej do kodowania danych w nośniku sieciowym.

Porcja danych w ramce składa się zwykle z bajtów zawierających informacje, które zostały tam umieszczone przez protokół wyższego poziomu i dostarczone do warstwy łącza danych, która odpowiada za transmisję ramki ethernetowej do węzła docelowego. Przykładowo, protokół IP określa zarówno wykorzystywane przez siebie informacje w nagłówku, jak i dane przenoszone za pomocą datagramu IP. Kiedy datagram IP przechodzi w dół do warstwy łącza danych, wszystkie potrzebne informacje znajdują się jednak w jednostce danych ramki Ethernetu.


**Rysunek 2.1.** *Model referencyjny OSI*

Skład ramki zależy od typu sieci. Format ramki Ethernetu i Ethernetu II w niewielkim stopniu różni się od IEEE 802.3. Standard IEEE 802.5 (Token-Ring) definiuje natomiast ramkę, która różni się zasadniczo od ramek sieci Ethernet.

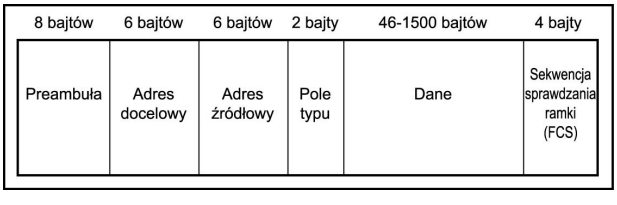
## XEROX PARC Ethernet i Ethernet II

Ramka oryginalnego standardu Ethernet definiuje kilka pól, które wykorzystano później także w specyfikacji ramki standardu Ethernet II:

- **Preambuła** — 8-bajtowa sekwencja zer i jedynek wykorzystywana do oznaczania początku ramki i ułatwiająca synchronizację transmisji.
- **Docelowy adres MAC (Media Access Control)** — 6-bajtowy adres wyrażany zwykle w formacie liczby szesnastkowej.
- **Adres MAC nadawcy** — kolejne 6-bajtowe pole reprezentujące adres stacji roboczej, która wygenerowała ramkę.
- **Pole typu** — 2-bajtowe pole oznaczające protokół klienta (np. IPX, IP lub DECnet) wykorzystywany w polu danych.
- **Pole danych** — pole o nieokreślonej długości, w którym znajdują się właściwe dane.

Określenie długości ramki pozostawiono protokołowi wyższego poziomu. Pole typu jest z tego powodu bardzo ważną częścią ramki.

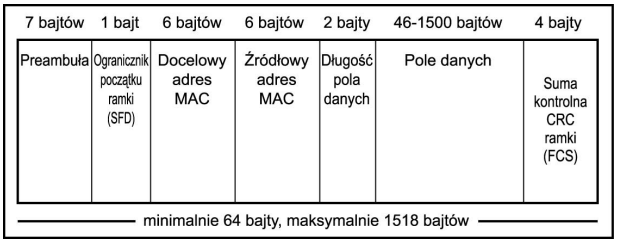
Na rysunku 2.2 widać rozmieszczenie poszczególnych pól w ramce oryginalnego standardu Ethernet.




**Rysunek 2.2.** *Ramka standardu Ethernet*

## Standard 802.3

Rozmieszczenie pól w ramce standardu Ethernet 802.3 zostało przedstawione na rysunku 2.3.




**Rysunek 2.3.** *Format ramki standardu IEEE 802.3*

Podstawowa zmiana polega na wprowadzeniu nowego pola w miejsce wykorzystywanego wcześniej pola typu. Te 2 bajty są w standardzie 802.3 wykorzystywane do określania długości następującego po nich pola danych. Kiedy wartość w tym polu nie przekracza 1500, możemy powiedzieć, że jest to pole długości. Jeśli omawiane pole zawiera wartość 1536 lub większą, oznacza to, że jest ona wykorzystywana do definiowania typu protokołu.

Dodatkowo ograniczono rozmiar preambuły z 8 do 7 bajtów, zaraz po niej następuje 1-bajtowy ogranicznik początku ramki (ang. *Start of Frame Delimiter — SFD*). Pole SFD zawiera ciąg bitów 10101011 (ostatni bajt stosowanej wcześniej 8-bajtowej preambuły zawierał w ostatnich dwóch bitach cyfry 10).

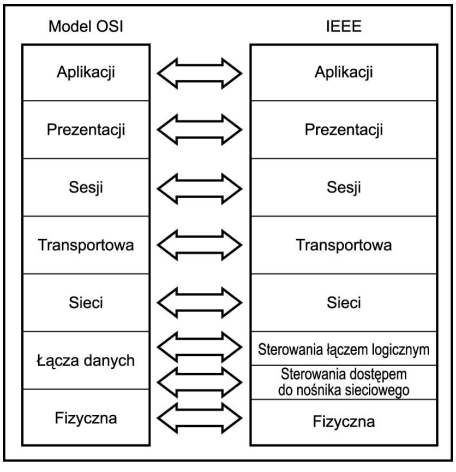
Ostatnią częścią ramki jest 4-bajtowa suma kontrolna ramki (ang. *Frame Check Sequence — FCS*), której celem jest przechowywanie obliczanej dla ramki sumy kontrolnej CRC. Stacja nadająca ramkę oblicza tę wartość na podstawie pozostałych bitów tej ramki. Stacja odbiorcza także oblicza wartość CRC na podstawie otrzymanych bitów i porównuje ją z liczbą otrzymaną w polu FCS. Jeśli nie są identyczne, wiadomo, że ramka musiała ulec uszkodzeniu podczas przesyłania i musi zostać nadana ponownie.

## IEEE 802.2: Sterowanie łączem logicznym

W siedmiowarstwowym referencyjnym modelu sieci OSI dwie najniższe warstwy to warstwa fizyczna i warstwa łącza danych. Wersja opracowana przez IEEE zawiera ponad warstwą fizyczną podwarstwy sterowania łączem logicznym (ang. *Logical Link Control — LLC*) i sterowania dostępem do nośnika sieciowego (ang. *Media Access Control — MAC*), co widać na rysunku 2.4. Dzięki temu możliwe jest korzystanie w jednej sieci z różnych rodzajów nośników transmisyjnych i różnych metod uzyskiwana dostępu do tych nośników.

### Ramka i nagłówek LLC

Podwarstwa sterowania dostępem do nośnika sieciowego odpowiada za właściwe wykorzystanie usług udostępnianych przez warstwę fizyczną i obsługi danych przesyłanych do i od zdalnych stacji roboczych w sieci. Do zadań podwarstwy LLC należy więc




**Rysunek 2.4.**
*Model IEEE*

wykrywanie błędów i lokalne adresowanie (z wykorzystaniem adresów fizycznych, czyli adresów MAC).

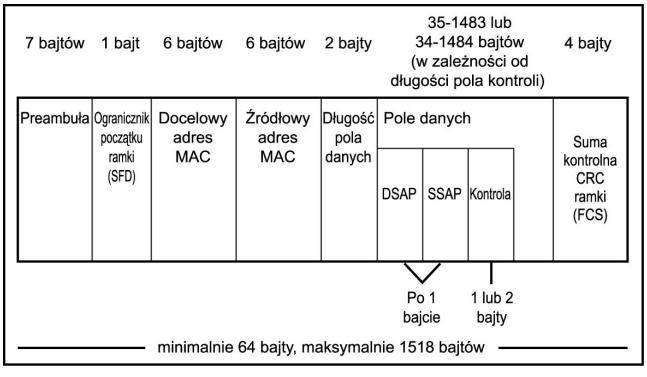
Podwarstwa LLC udostępnia wyższym warstwom usługi, które można podzielić na następujące trzy typy:

- **Usługa bezpołączeniowa bez potwierdzeń** — niektóre protokoły wyższego poziomu (np. TCP) udostępniają już funkcje sterowania przepływem i potwierdzania odbiorów, które umożliwiają weryfikację prawidłowego dostarczania pakietów. Nie ma potrzeby powielania tych funkcji w podwarstwie LLC.
- **Usługa połączeniowa** — ten rodzaj usługi wymaga, by przed nawiązaniem komunikacji i 11rozpoczęciem przesyłania danych było stworzone łącze logiczne. Przykładem jest protokół TCP, który w fazie ustanawiania połączenia wykorzystuje mechanizm wymiany potwierdzeń otrzymania pakietów sieciowych, zanim będą przesyłane właściwe dane. Ten typ usług oferuje funkcje wykrywania błędów i sterowania przepływem.
- **Usługa bezpołączeniowa z potwierdzeniami** — ta usługa jest kombinacją dwóch pozostałych. Oferuje komunikację bezpołączeniową, która także nie wymaga nawiązywania i sprawdzania połączenia przed rozpoczęciem transmisji. Ten rodzaj komunikacji wykorzystuje jednak mechanizmy potwierdzeń, które dają pewność, że pakiety sieciowe dotarły nienaruszone i we właściwej kolejności (zgodnej z kolejnością nadania) do adresata.

Aby umożliwić implementację tych funkcji, zdefiniowano umieszczany w ramce „podnagłówek", który znajduje się bezpośrednio przed polem danych. Pole nagłówka LLC ma długość 3 bajtów. Pierwszy bajt reprezentuje punkt dostępu usługi docelowej (ang. *Destination Service Access Point — DSAP*), drugi — punkt dostępu usługi źródłowej (ang. *Source Service Access Point — SSAP*), ostatni to pole kontroli.

Na rysunku 2.5 widać kombinację podnagłówka LLC z ramką standardu 802.3.

**Rysunek 2.5.** *Ramka 802.3 z podnagłówkiem LLC*



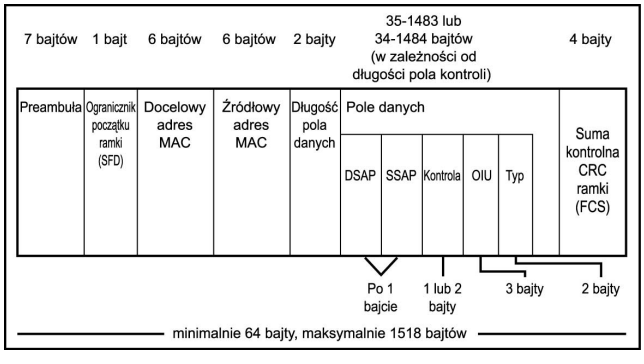

## Standard ramki SNAP, 802.3

Aby zapewnić zgodność z wcześniejszymi technologiami sieciowymi, wprowadzono podramkę SNAP (od ang. *Sub-Network Access Protocol*). Konstruuje się ją dodając dwa nowe pola do podnagłówka LLC zaraz po właściwych polach LLC:

- 3-bajtowy unikalny identyfikator OUI (od ang. *Organizationally Unique Identifier*),
- 2-bajtowe pole typu protokołu.

Rozszerzenia SNAP muszą się znajdować w polach nagłówka LLC. Pełną postać ramki standardu 802.3 widać na rysunku 2.6.

**Rysunek 2.6.** *Ramka standardu 802.3 zawierająca podnagłówek LLC i rozszerzenia SNAP*




# IEEE 802.3u — Fast Ethernet

Technologia Fast Ethernet została zaprojektowana w taki sposób, by zapewnić zgodność z istniejącymi sieciami 10BASE-T. Wykorzystuje ten sam format ramki i nadal stosuje zdefiniowaną w standardzie 802.3 metodę dostępu do nośnika CSMA/CD.

### 100BASE-T

Jedną z zalet sieci 100BASE-T jest możliwość przejścia na tę technologię bez konieczności zmiany istniejącego w budynku okablowania kategorii 3. Jedynym standardem umożliwiającym wykorzystanie okablowania kategorii 3 jest 100BASE-T4. Istnieje ważna różnica pomiędzy standardami 100BASE-T4 i 100BASE-TX: nie używają tych samych par żył w przewodach do nadawania i odbierania danych. W standardzie 100BASE-T4 do komunikacji wykorzystuje się wszystkie cztery pary żył i zupełnie inną technikę przesyłania sygnałów.

W przypadku sieci, które zostały skonstruowane na podstawie okablowania kategorii 5 mimo stosowania mało wymagającej technologii 10BASE-T, przejście do standardu o przepustowości 100 Mb/s będzie najlepszym dowodem trafności tamtej inwestycji. Ta przewidująca pracę ze skrętką specyfikacja standardu 100BASE-T może być stosowana zarówno z przewodami nieekranowanymi, jak i ekranowanymi (STP), które są zwykle stosowane w sieciach Token-Ring. Standard 100BASE-TX oparto na specyfikacji ANSI TP-PMD (od ang. *Twisted-Pair Physical Medium Dependent*).

### 100BASE-T4

W przypadku sieci opartych na okablowaniu kategorii 3 i 4 jedynym sposobem jej modernizacji bez wymiany przewodów jest zastosowanie urządzeń technologii 100BASE-T. Standard ten wykorzystuje metodę przesyłania sygnałów w trybie półdupleksu za pomocą czterech par żył. Trzy z tych par żył są wykorzystywane do przesyłania właściwych danych, czwarta służy do wykrywania kolizji. Każda z tych trzech par umożliwia transmisję danych z szybkością 33,3 Mb/s, co daje razem 100 Mb/s (ten rodzaj sygnalizacji nosi nazwę 4T+). W przewodach stosuje się trzypoziomowy schemat kodowania, zamiast używanego w większości innych nośników schematu dwupoziomowego. 100BASE-T4 wymaga specjalnego sprzętu (kart sieciowych i koncentratorów) i działa w trybie półdupleksu.

### 100BASE-FX

Sieć 100BASE-FX wykorzystuje przewody światłowodowe z dwiema wiązkami (jedna do nadawania, druga do odbierania danych) i może mieć nawet 2 kilometry długości.

Światłowody są dobrym rozwiązaniem dla sieci szkieletowych. W przeciwieństwie do przewodów miedzianych, które wykorzystują do komunikacji impulsy elektryczne, przewody światłowodowe wykorzystują impulsy świetlne. To sprawia, że znacznie lepiej się sprawdzają w środowiskach charakteryzujących się dużymi zakłóceniami elektrycznymi. Przewody tego typu są także znacznie bezpieczniejsze, ponieważ nie emitują sygnałów elektrycznych, które mogłyby być przechwytywane przez specjalistyczne urządzenia podsłuchowe.

## IEEE 802.3z — Gigabit Ethernet

W roku 1998 ukończono prace nad specyfikacją technologii 802.3z nazwanej Gigabit Ethernet (gigabitowym Ethernetem), na którą składają się następujące standardy:

- **1000BASE-SX** — wykorzystuje światłowody wielomodowe do łączenia na niewielkie odległości. W przypadku przewodów o średnicy rdzenia 50 mikronów maksymalna długość wynosi 300 metrów, w przypadku przewodów o średnicy rdzenia 62,5 mikronów maksymalna długość wynosi 550 metrów.
- **1000BASE-LX** — wykorzystuje światłowody jednomodowe o maksymalnej długości 3000 metrów lub wielomodowe o maksymalnej długości 550 metrów.
- **1000BASE-CX** — wykorzystuje przewody miedziane, czyli skrętkę, zapewniające dużą wydajność na odległości maksymalnie 25 metrów. Standard ten został zaprojektowany z myślą o szafach kablowych.
- **1000BASE-T** — wykorzystuje przewody skrętki kategorii 5 o maksymalnej długości 100 metrów.

Definiujący tzw. gigabitowy Ethernet standard IEEE 802.3z przewiduje dodanie nowego pola do podstawowej ramki 802.3 — pola *rozszerzenia*, bezpośrednio za polem sekwencji sprawdzania ramki. Jest ono wykorzystywane do zwiększenia minimalnego rozmiaru ramki do 512 bajtów (zamiast wykorzystywanych w wolniejszych sieciach 64 bajtów). Zwiększony minimalny rozmiar ramki jest potrzebny tylko wtedy, gdy sieć standardu Gigabit Ethernet działa w trybie półdupleksu i nadal wykorzystuje mechanizm wykrywania kolizji. Wspomniane pole jest zbędne w pełnym dupleksie.

Kolejną metodą zwiększenia szybkości przesyłania danych w sieciach Gigabit Ethernet jest ograniczenie kosztów związanych z wykorzystywaniem mechanizmu CSMA/CD dla każdej ramki przesyłanej w sieci. Do standardu 802.3z dodano tzw. tryb wiązkowy (ang. *burst mode*), który umożliwia kolejne przesyłanie wielu ramek zaraz po otrzymaniu dostępu do nośnika sieciowego. Jest to możliwe dzięki specjalnym tzw. *bitom rozszerzającym* wstawianym w wolnych przestrzeniach pomiędzy normalnymi ramkami. Te bity utrzymują aktywność nośnika, dzięki czemu pozostałe stacje nie mogą wykryć jego bezczynności i próbować transmitować swoje dane.

Standard Gigabit Ethernet jest obecnie powszechnie stosowany w szkieletowych sieciach lokalnych łączących mocno obciążone usługi lub przełączniki.

## IEEE 802.3ae — 10Gigabit Ethernet

W standardzie 10Gigabit Ethernet utrzymano format ramki 802.3 oraz znane z wcześniejszych wersji Ethernetu minimalne i maksymalne rozmiary ramek. Nowa technologia wyklucza możliwość komunikacji w trybie półdupleksowym oraz stosowania mechanizmów współdzielonego dostępu do nośnika sieciowego.

Specyfikacja standardu 802.3ae przewiduje istnienie dwóch typów warstwy fizycznej (ang. *Physical layer — PHY*): warstwa sieci LAN i warstwa sieci WAN. Warstwa PHY jest dalej dzielona na dwie podwarstwy: podwarstwę zależną od fizycznego nośnika (ang. *Physical Media Dependent — PMD*) oraz podwarstwę fizycznego kodowania (ang. *Physical Coding Sublayer — PCS*). Podwarstwa PCS odpowiada za sposób kodowania danych w fizycznym nośniku sieciowym. Podwarstwa PMD reprezentuje parametry fizyczne, np. stosowaną długość fal laserowych lub świetlnych.

Warstwy LAN PHY i WAN PHY obsługują te same podwarstwy PMD. Podwarstwy PMD sieci 10Gigabit Ethernet wykorzystują zakres od lasera 850 nm w wielomodowych światłowodach (50,0 mikronów) dla mniejszych odległości (do 65 metrów) do lasera 1550 nm w jednomodowych światłowodach (9,0 mikronów) dla sieci o długości nawet 40 kilometrów. Warstwa LAN PHY będzie przeznaczona do działania z istniejącym kodowaniem sieci lokalnych standardu Gigabit Ethernet, jednak z większą szybkością przesyłania danych.

Warstwa LAN PHY jest osobnym fizycznym interfejsem umożliwiającym komunikację na większe odległości z opcjonalnym (rozważanym obecnie) interfejsem umożliwiającym wykorzystanie przez sieci 10Gigabit Ethernet sieci SONET/SDH. SONET OC-192 oferuje przepustowość zbliżoną do tej proponowanej w standardzie 10Gigabit Ethernet. Potrzebny jest jedynie prosty mechanizm buforujący, który umożliwi połączenie urządzeń obu standardów.

Obecnie standard 10Gigabit Ethernet jest jednak powszechnie uważany za protokół sieci WAN. Szacuje się, że implementacja usług sieci 10Gigabit Ethernet będzie tańsza niż konstrukcja podobnych rozwiązań T3 dla środowisk MAN i WAN.

Sceptycy twierdzą, że sieci Ethernet nigdy nie będą posiadały mechanizmów gwarancji jakości usługi (ang. *Quality of Service — QoS*), oferowanych przez sieci ATM. Poza tym, w porównaniu z technologią SONET i innymi szybkimi protokołami transmisyjnymi, Ethernet oferuje stosunkowo niewiele narzędzi administracyjnych. Prostota standardu Ethernetu i fakt, że kosztuje znacznie mniej niż inne rozwiązania sieci WAN, czyni z niego jednak atrakcyjnego konkurenta na tym rynku.

# Problemy w sieciach Ethernet

Najczęściej spotykanym źródłem problemów (oprócz zagięcia, przerwania przewodów czy awarii kart sieciowych) jest nadmierna liczba kolizji.

## Kolizje

Chociaż w tradycyjnych sieciach Ethernet kolizje są zjawiskiem naturalnym, zawsze istnieje możliwość wystąpienia nadmiernej liczby kolizji, która powoduje zauważalny dla końcowych użytkowników spadek wydajności.

Kiedy jakieś urządzenie zacznie generować kolizje stanowiące 1% łącznego obciążenia sieci, może to oznaczać problem. Jest to jeden ze wskaźników, o którym warto pamiętać podczas monitorowania obciążenia sieci lokalnej. Jeśli Twoja sieć spełnia założenia zastosowanej topologii oraz jej obciążenie jest na niskim poziomie, nadmierna liczba kolizji może wynikać z niewłaściwie działającej karty sieciowej, która nie nasłuchuje sieci przed podjęciem próby transmisji danych.

## Wykrywanie kolizji

Najprostszą metodą określenia liczby kolizji w sieci lokalnej jest obserwacja odpowiednich diod koncentratora lub przełącznika. Większość koncentratorów ma diodę zapalającą się w momencie wykrycia kolizji. Jeśli stwierdzisz, że taka dioda świeci się niemal ciągle lub miga bardzo często, należy sprawdzić, czy liczba kolizji przekracza dopuszczalny limit. Jeśli tak, to stosując oprogramowanie monitorujące sieć można określić jej obciążenie — jeśli przekracza 30 – 40%, trzeba rozważyć podzielenie sieci LAN na mniejsze domeny kolizyjne.

Analizatory sieci lokalnych i narzędzia monitorujące mogą pomóc w wyznaczeniu liczby występujących kolizji. Specjalne pulpity zarządzania wykorzystujące protokół SNMP i sondy RMON mogą się przydać do zebrania informacji statystycznych pomocnych w przypadku lokalizowania segmentów sieci o najwyższych wskaźnikach występowania kolizji. W przypadku małych sieci lokalnych zawierających tylko kilka przełączników zastosowanie wbudowanego oprogramowania zarządzającego jest znacznie tańszym rozwiązaniem niż inwestycja w zaawansowane oprogramowanie zarządzania siecią, np. HP OpenView.

## Typy kolizji

Dobre analizatory sieci oferują mnóstwo informacji. W przypadku poszukiwania przyczyn kolizji oprogramowanie dostarcza zwykle więcej niż jeden rodzaj danych, który ułatwia znalezienie ich przyczyny.

### Kolizje lokalne

Z *kolizją lokalną* (nazywaną także *wczesną kolizją*) mamy do czynienia w sytuacji, gdy wystąpi w lokalnym segmencie już w trakcie nadawania pierwszych 64 bajtów ramki. Jest to najbardziej popularny rodzaj kolizji. Dochodzi do niej, gdy dwie różne stacje sieci LAN wykryją brak transmisji w nośniku sieciowym i jednocześnie rozpoczną nadawanie swoich danych. Efektem jest tzw. krótka ramka (ang. *runt*), ponieważ przed wystąpieniem zdarzenia kolizji została pomyślnie wysłana tylko mała część ramki. Specyfikacja standardu Ethernet przewiduje tego typu sytuacje — obie stacje wykorzystują algorytm wyczekiwania, który opóźnia wznowienie transmisji.

Jeśli wskaźnik występowania wczesnych kolizji jest wysoki, przyczyną może być obciążenie segmentu sieci zbliżające się do 40%. W większości przypadków oznacza to, że sieć jest przeciążona. Należy wtedy rozważyć zainstalowanie dodatkowego przełącznika, który pozwoli ograniczyć liczbę kolizji. Jeśli można wskazać konkretny węzeł, w którym dochodzi do największej liczby kolizji lokalnych, może to oznaczać jakiś problem sprzętowy tej stacji, np. wadliwa karta sieciowa.

### Późne kolizje

*Późne kolizje* występują w momencie, gdy dwa urządzenia sieciowe rozpoczynają nadawanie danych w tym samym czasie, ale nie wykrywają zaistniałej kolizji natychmiast. Przyczyną występowania tego typu kolizji są zwykle zbyt długie segmenty sieci. Jeśli

czas nadania ramki w sieci jest krótszy od czasu potrzebnego do dostarczenia tej ramki do najbardziej oddalonego węzła, żaden z transmitujących dane węzłów nie zostanie poinformowany o rozpoczęciu transmisji przez inny węzeł w trakcie nadawania pierwszych 64 bajtów ramki (64 bajty to rozmiar najmniejszej ramki).

Późne kolizje nie powodują wznawiania transmisji ramki, ponieważ jej nadawca nie ma pojęcia o wystąpieniu kolizji. Odpowiedzialność za wykrycie i obsłużenie błędu (zażądanie ponownej transmisji) spoczywa w takim przypadku na protokole wyższego poziomu.

Jeśli istnieje wysoki poziom wskaźnika występowania późnych kolizji w danej sieci lokalnej, należy sprawdzić, czy problem nie wynika ze złej topologii. Nie chodzi wyłącznie o przekroczenie dopuszczalnych długości przewodów, ale także o wykorzystywanie zbyt wielu koncentratorów i innych urządzeń. Jeśli to nie jest przyczyną, to problem wynika prawdopodobnie z awarii sprzętu.

## Ograniczanie liczby kolizji

Istnieje kilka przyczyn występowania nadmiernej liczby kolizji. Niektóre z nich są następstwem zignorowania reguł zdefiniowanych dla topologii, wadliwie działającego sprzętu lub przeciążenia segmentu sieci (zbyt dużej liczby użytkowników).

### Niepoprawna topologia sieci

Jeśli występują segmenty, których rozmiary przekraczają długości dopuszczalne przez specyfikację stosowanej topologii sieciowej, niektóre z urządzeń sieciowych mogą nie mieć możliwości wykrycia transmisji danych przeprowadzanych przez pozostałe węzły. Kiedy konieczna jest rozbudowa sieci, nigdy nie powinno się w nieprzemyślany sposób dodawać nowych segmentów dołączając do sieci nowy repeater, koncentrator czy most. Z tego właśnie powodu istotne znaczenie ma konstruowanie aktualnych map fizycznych topologii sieci, co umożliwi w przyszłości właściwe planowanie rozbudowy sieci.

### Wadliwe karty sieciowe

Problem nadmiernej liczby kolizji może wynikać ze złego funkcjonowania karty sieciowej, która nie wykrywa transmisji sygnału w nośniku sieciowym i rozpoczyna nadawanie swoich danych, niezależnie od dostępności tego nośnika. Najprostszą metodą jest zastąpienie podejrzanego urządzenia innym, co do którego mamy pewność, że działa prawidłowo. Jeśli to nie rozwiąże problemu, warto spróbować wykorzystać inny przewód łączący tę kartę z siecią lub przełożyć tę samą kartę do innego gniazda komputera. Kolejna taktyka rozwiązywania tego typu problemów polega na wykorzystaniu oprogramowania diagnostycznego dołączanego do sprzedawanych urządzeń przez producentów kart sieciowych.

### Nadawcy generujący największe obciążenie

Liczba urządzeń, które można połączyć w jednej domenie rozgłaszania sieci komputerowej, jest ograniczona z powodu spadającej wydajności. Spadek wydajności może spowodować także stosunkowo niewielka liczba komputerów generujących duży ruch

w sieci. Kiedy rośnie obciążenie sieci, rośnie także liczba kolizji. Kiedy więc w sieci występuje nadmierna liczba kolizji, oznacza to zwykle, że obciążenie w danym segmencie zbliżyło się lub przekroczyło poziom 40% — warto wówczas podzielić tę część sieci lokalnej na segmenty za pomocą przełącznika lub podobnego urządzenia.

# Błędy w sieci Ethernet

Większości z omawianych poniżej problemów można zaradzić wprowadzając w sieciach stosunkowo niewielkie modyfikacje. Jeśli nadal korzystamy z koncentratorów, należy rozważyć zastosowanie w ich miejsce nowocześniejszych przełączników. Jeśli decydujemy się na używanie urządzeń korzystających z mechanizmu CSMA/CD, decydujemy się tym samym na kolizje i problemy z nimi związane.

## Wykrywanie prostych błędów

Najprostszą metodą wykrywania błędów jest kontrola parzystości (ang. *parity check*). Przykładem tej metody jest przesyłanie znaków za pomocą 7-bitowego zbioru znaków ASCII z dodatkowym ósmym bitem. Jeśli dany protokół sieciowy wykorzystuje mechanizm *kontroli parzystości*, ósmemu bitowi przypisuje się wartość jeden lub zero, w zależności od tego, czy liczba wartości „1" w pozostałych siedmiu bitach jest odpowiednio parzysta czy nieparzysta. Jeśli stosuje się mechanizm *kontroli nieparzystości*, wartość „1" w ósmym bicie oznacza nieparzystą liczbę wartości „1" w pozostałych siedmiu bitach. Stacja odbiorcza może w prosty sposób sama obliczyć wartość bitu parzystości analizując pierwsze siedem bitów i porównać go z otrzymaną wartością. Ten schemat wykrywania błędów może się nie sprawdzić, jeśli podczas transmisji uszkodzeniu uległ więcej niż jeden bit.

Ten sposób kontrolowania otrzymywanych danych może być wykorzystywany wyłącznie na poziomie pojedynczych bajtów, nie jest więc pomocny podczas weryfikacji poprawności ramki danych mającej długość 1518 bajtów. W ramkach sieci Ethernet wykorzystuje się do wykrywania ewentualnych niespójności 4-bajtowe sumy kontrolne CRC ramki (ang. *Frame Check Sequence — FCS*).

## Zła wartość FCS lub niedopasowana ramka

Warstwa MAC oblicza, na podstawie zawartości ramki, wartość sumy kontrolnej CRC, którą umieszcza w polu FCS. Stacja docelowa może wykonać te same obliczenia i — porównując otrzymany wynik z wartością umieszczoną w ramce przez stację nadawczą — określić, czy ramka została uszkodzona podczas przesyłania.

Istnieje możliwość, że wartość FCS została błędnie obliczona przez stację nadawczą z powodu problemów sprzętowych związanych z realizacją tej funkcji w warstwie MAC. Nie można także wykluczyć sytuacji, w której problem spowodowała karta sieciowa

odpowiedzialna za transmisję ramki, czego efektem mogło być niewłaściwe przekazanie bitów do nośnika sieciowego. Jak w przypadku większości błędów, problem może także wynikać z zakłóceń, jakim podlegają miedziane przewody łączące sieć komputerową.

Kiedy poziom występowania błędnych wartości FCS przekroczy 2 – 3% łącznego obciążenia pasma sieci komputerowej, powinno się rozpocząć poszukiwanie urządzenia, które generuje błędy. Zlokalizowanie adresu źródłowego wadliwego urządzenia jest możliwe za pomocą analizatorów sieciowych.

Ponieważ ramka składa się z bajtów (jednostek 8-bitowych), po dotarciu do węzła docelowego jej rozmiar powinien być zawsze podzielny przez osiem. Jeśli nie jest, to wystąpił tak zwany błąd niedopasowanej ramki (ang. *misaligned frame*) — występuje zwykle w połączeniu z błędem niewłaściwej wartości FCS. Najczęstszym powodem są zakłócenia elektryczne w okablowaniu lub kolizja. Inną przyczyną może być niewłaściwa topologia sieci, w której wykorzystuje się więcej niż dwa połączone kaskadowo wieloportowe repeatery.

## Krótkie ramki

Rozmiar tzw. krótkiej ramki (ang. *runt*) w sieci Ethernet jest mniejszy niż 64 bajty, czyli mniejszy od rozmiaru najmniejszej dopuszczalnej ramki. Należy pamiętać, że transmitujące pakiet urządzenie sieciowe nie może zakończyć nadawania w czasie krótszym niż wynosi czas propagacji pakietu w lokalnej domenie rozgłaszania. W przeciwnym przypadku urządzenie nie miałoby możliwości wykrycia ewentualnej kolizji.

Jeśli krótka ramka ma poprawną wartość FCS, to problem prawdopodobnie wynika z niewłaściwego funkcjonowania karty sieciowej, która wygenerowała tę ramkę. Jeśli natomiast wartość FCS nie jest zgodna z zawartością ramki, prawdopodobnym źródłem problemu jest kolizja lub błędna topologia.

Niekiedy skutkiem ubocznym występowania kolizji są przesyłane sygnały interpretowane jako krótkie ramki. Jeśli tego typu błędy pojawiają się w sieci stosunkowo często, konieczne trzeba sprawdzić wskaźniki obciążenia danego segmentu sieci. Jeśli maksymalne obciążenie jest wysokie, a średnie obciążenie jest na dobrym poziomie, to można zmienić harmonogram pracy użytkowników, by szczególnie wymagające zadania były realizowane w czasie, gdy sieć jest mniej obciążona. Innym rozwiązaniem jest umieszczenie wydajnych stacji roboczych generujących duże obciążenie sieci w osobnym segmencie LAN, zwalniając pasmo dostępne dla zwykłych stacji roboczych.

Jeśli obciążenie sieci jest niskie, problem będzie wymagał głębszej analizy polegającej na zidentyfikowaniu stacji roboczej lub urządzenia sieciowego generującego krótkie ramki. Może to być dosyć trudne, ponieważ znaczna część błędów tego typu polega na przesyłaniu ramek tak krótkich, że niemożliwe jest określenie adresu źródłowego.

Generowanie krótkich ramek może także wynikać ze zignorowania określonych w standardzie Ethernet reguł dla stosowanej topologii. Typowym błędem jest zastosowanie więcej niż czterech repeaterów w jednej domenie kolizyjnej.

## Olbrzymie i niezrozumiałe ramki

Karty sieciowe generują niekiedy ramki, których rozmiar przekracza dopuszczalne maksimum — noszą one nazwę błędów olbrzymich ramek (ang. *giant frame error*).

Zlokalizowanie urządzenia generującego takie ramki może być proste, jeśli używany analizator sieci LAN jest w stanie wykryć ich adres źródłowy. W niektórych przypadkach nie da się wykryć adresu wadliwego urządzenia, jeśli np. działająca nieprawidłowo karta sieciowa z pewną częstotliwością rozsyła w sieci nic nieznaczące sygnały. W takim przypadku powinno się kolejno odłączyć każdą stację roboczą danego segmentu sieci, by sprawdzić, czy usunięcie tych węzłów nie eliminuje omawianego problemu.

Chociaż określenie *jabber* (niezrozumiała ramka) dotyczy niekiedy ramek przekraczających dopuszczalny rozmiar, w zasadzie odnosi się do wszystkich sytuacji, w których urządzenie sieciowe nie działa zgodnie z jej regułami i transmituje do nośnika sieciowego nieprawidłowe sygnały. Wadliwe urządzenie sieciowe może zarówno rozsyłać zbyt duże ramki, jak i bez przerwy nadawać niezrozumiały sygnał. Taki błąd może unieruchomić nawet cały segment sieci, ponieważ karta sieciowa bez przerwy przesyłająca swoje sygnały uniemożliwia uzyskanie dostępu do współdzielonego nośnika sieciowego wszystkim innym stacjom.

## Fala rozgłaszań

Ze zjawiskiem *fali rozgłaszań* ma się zwykle do czynienia w momencie, gdy urządzenia sieciowe generują obciążenie sieci powodujące dalsze generowanie tego obciążenia. Chociaż dodatkowe obciążenie może teoretycznie wynikać z fizycznych problemów urządzeń sieciowych, zwykle jest powodowane przez protokoły wyższego poziomu. Problem z wykryciem źródła tego typu zachowań polega na tym, że zwykle w momencie ich wystąpienia uzyskanie dostępu do sieci jest niemożliwe. Fale rozgłaszań mogą znacząco ograniczyć szybkość przesyłania danych w sieci, a nawet całkowicie wstrzymać jej pracę.

Monitorując operacje rozgłaszania w sieci widać wskaźnik nieprzekraczający około 100 rozgłaszanych ramek na sekundę. Jeśli wartość tego wskaźnika na stałe przekroczy tę wartość, to przyczyną może być wadliwie działająca karta sieciowa lub należy podzielić domenę kolizyjną na mniejsze segmenty.

# Monitorowanie błędów

Istnieje wiele narzędzi, które można wykorzystać do monitorowania sieci w celu wykrywania błędów. Np. analizator sieciowy *Network Sniffer* wyświetla informacje o ramkach zwierających rozmaite błędy (włącznie ze słabymi ramkami, błędami CRC czy

niewłaściwymi rozmiarami). Niektóre programowe narzędzia, np. *Monitor sieci* dołączany m.in. do systemu Windows NT Server firmy Microsoft, umożliwiają przeglądanie statystyk na temat zgubionych ramek, błędów CRC oraz rozgłaszań.

W przypadku sieci wymagających centralnego zarządzania i kontroli do monitorowania sieci i automatycznego powiadamiania o sytuacjach alarmowych można wykorzystać aplikacje protokołu SNMP i standard RMON.

W zależności od producenta, do wielu urządzeń pracujących (np. routerów lub inteligentnych koncentratorów) jest dołączane specjalne oprogramowanie zarządzające, którego działanie można ograniczyć do wyświetlania statystyk o błędach, jeśli oczywiście nie korzystamy z bardziej zaawansowanych funkcji.