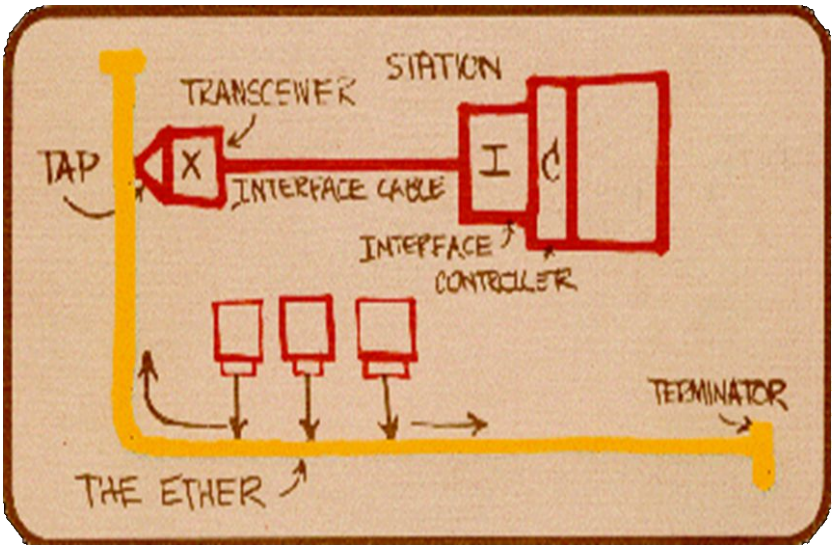
Wojciech Myszka

Media

wer. 41 z drobnymi modyfikacjami!

2023-05-18 10:31:23 +0200

Spis treści



Rysunek 1. Odręczny rysunek Boba Metcalfe'a obrazujący ideę sieci (1976)

Część I

Okablowanie

1. Ethernet

1.1. 10 Mbit/sek

10BASE5 Gruby kabel koncentryczny (5 — maksymalna długość segmentu: 500m), Komputery podłączone do kabla za pośrednictwem „wampira" i MAU (*Medium Attachment Unit*) oraz AUI (*Attachment Unit Interface*).

10BASE2 „Cienki Ethernet" (2 od maksymalnej długości segmentów kabli — 185m ∼ 200m)

FOIRL *Fiber Optic Inter-Repeater Link* — światłowód używany do połączeń między urządzeniami pośredniczacymi.

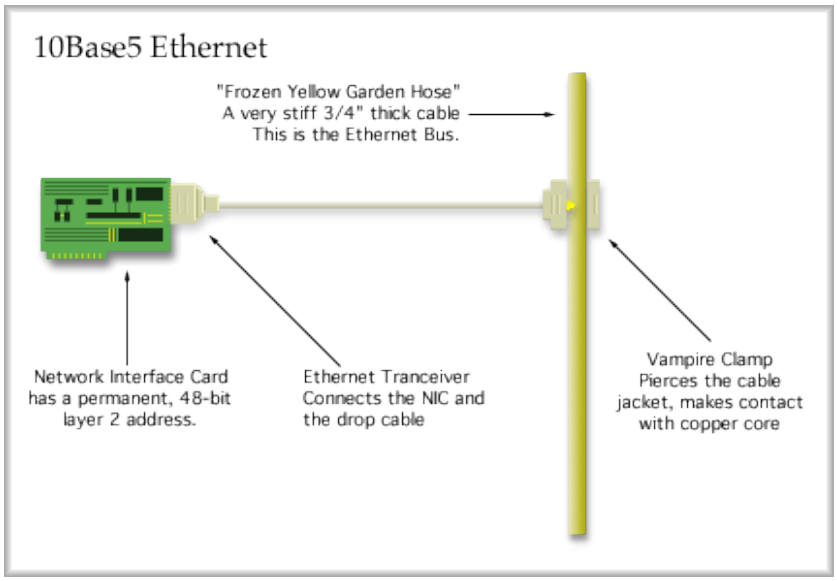
10BASE-T (T od *Twisted*) skrętka kategorii 3 lub wyższej.

10BASE-F (F od *Fiber*) połączenie stacji za pomocą światłowodu

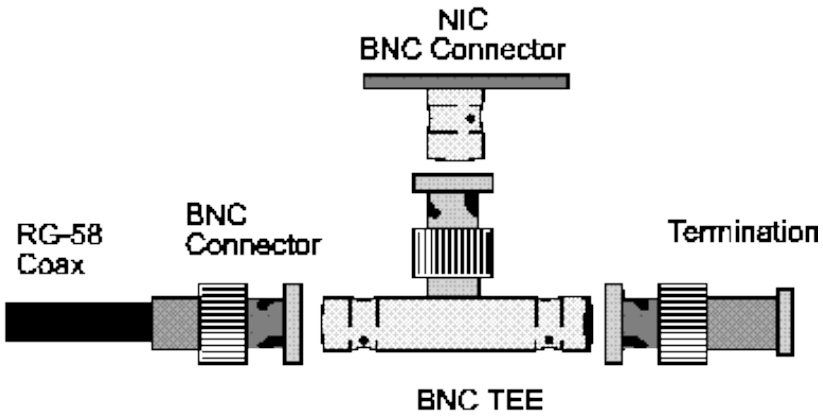
Pierwsze projekty sieci (por. rys. 1 przedstawiający jeden z pierwszych schematów sieci zaproponowany przez Boba Metcalfe'a w 1976 roku) zakładały, że urządzenia sieciowe będą poza komputerem i będą łączyły się z nim za pomocą jednolitego interfejsu. Jeszcze na początku lat 90. prawie wszystkie komputery i urządzenia aktywne wyposażone były w jedno gniazdo AUI.

Na rysunku 4 przedsawiony jest MAU pozwalający podłączyć kabel koncentryczny w standardzie 10BASE2 do AUI.

10BASE5/10BASE2



Rysunek 2. Podłączenie do „grubego” (żółtego) Ethernetu



Rysunek 3. „Cienki” Ethernet

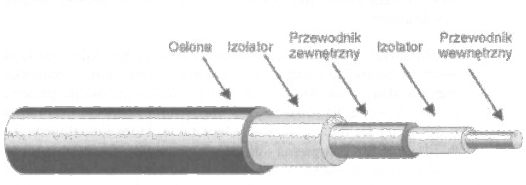
Kabel tego standardu (niezależnie od grubości) składa się z dwóch przewodów koncentrycznie umieszczonych jeden wewnątrz drugiego: jeden z nich wykonany jest w postaci drutu miedzianego i umieszczony w osi kabla (czasami zwany jest przewodem gorącym), zaś drugi (ekran) stanowi oplot (rys. 5).

Zalety: jest mało wrażliwy na zakłócenia i szumy. Wady: awaryjność — nie znosi ostrych zakrętów ani łagodnie przykładanej siły gniotącej. Jego struktura łatwo ulega uszkodzeniu, co powoduje bezpośrednie pogorszenie transmisji sygnału.

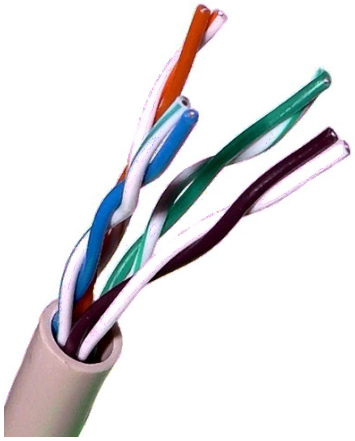
1.2. 100 Mb/s

100BASE-T generalnie wszystkie systemy 100 Mb/s
100BASE-X ogólna nazwa obejmująca 100BASE-TX i 100BASE-FX

Rysunek 4. Mikro-transceiver do standardu 10BASE2



Rysunek 5. Kabel koncentryczny



Rysunek 6. Skrętka UTP

100BASE-TX Fast Ethernet dwie pary skrętki kat. 5 (najczęściej używane)
100BASE-FX wielomodowy przewód światłowodowy

1.3. 1000 Mb/s

1000BASE-X wszystkie światłowodowe systemy przesyłu oparte na kodowaniu zaczerpniętym ze standardu Fibre Channel (1000BASE-SX, 1000BASE-LX, 1000BASE-CX (oparty ma miedzi, krótkie odcinki),
1000BASE-T Skrętka kategorii 5 lub wyższej

1.4. 10 Gb/s

10GBASE-T Skrętka kategorii 6 lub wyższej,
10GBASE-CX4 Krótkie odcinki kabla miedzianego,
10GBASE-SR Ethernet 10 Gb/s przez krótkie odcinki wielomodowych przewodów światłowodowych.
10GBASE-LR

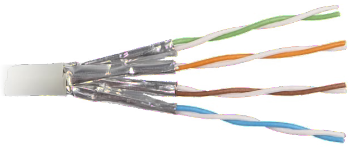
Ethernet 10 Gb/s przez długie odcinki jednomodowych przewodów światłowodowych. Światłowód (S — Short, L — Long); krótkie odcinki — wielomodowe, długie — jednomodowe.

40GBASE-CR4 Ethernet 40 Gb/s przez cztery krótkie odcinki koncentrycznego kabla symetrycznego (ang. twinaxial) splecionego w pojedynczy przewód.
40GBASE-SR4 Ethernet 40 Gb/s przez cztery krótkie odcinki wielomodowych przewodów światłowodowych.
40GBASE-LR4 Ethernet 40 Gb/s przez cztery długości fal przesyłanych przez pojedynczy dalekosiężny jednomodowy przewód światłowodowy.

Skrętka UTP

Skrętka nieekranowana (UTP — *Unshielded Twisted Pair*) kabel zbudowany ze skręconych ze sobą par przewodów i tworzy linię zrównoważoną (symetryczną). Skręcenie przewodów ze splotem 1 zwój na 6-10 cm

Rysunek 7. Skrętka FTP



Rysunek 8. Skrętka STP

chroni transmisję przed interferencją otoczenia. Tego typu kabel jest powszechnie stosowany w sieciach informatycznych i telefonicznych (rys. 6).

Skrętka FTP

Skrętka foliowana (FTP — *Foiled Twisted Pair*) jest to skrętka ekranowana za pomocą folii z przewodem uziemiającym. Przeznaczona jest głównie do budowy sieci komputerowych umiejscowionych w ośrodkach o dużych zakłóceniach elektromagnetycznych. Stosowana jest również w sieciach Ethernet (1 Gb/s) przy wykorzystaniu wszystkich czterech par przewodów (rys. 7).

Skrętka STP

Skrętka ekranowana (STP — *Shielded Twisted Pair*) ekran jest wykonany w postaci oplotu i zewnętrznej koszulki ochronnej (rys. 8). Jej zastosowanie wzrasta w świetle nowych norm europejskich EMC w zakresie emisji EMI (*Electro Magnetic Interference*).

1.5. Klasy skrętki

Klasy skrętki według europejskiej normy EN 50173:

— klasa A (kategoria 1) – realizacja usług telefonicznych z pasmem częstotliwości do 100 kHz;
— klasa B (kategoria 2) – okablowanie dla aplikacji głosowych i usług terminalowych z pasmem częstotliwości do 1 MHz;
— klasa C (kategoria 3) – używana najczęściej w sieciach telefonicznych, wykorzystuje pasmo częstotliwości do 16 MHz;
— klasa D (kategoria 5/5e) – najczęściej stosowana do budowy sieci lokalnych, obejmuje aplikacje wykorzystujące pasmo częstotliwości do 100 MHz;
— klasa E (kategoria 6) – rozszerzenie ISO/IEC 11801/TIA wprowadzone w 1999, obejmuje okablowanie, którego wymagania pasma są do czę-

stotliwości 250 MHz (przepustowość rzędu 200 Mb/s). Przewiduje ono implementację Gigabit Ethernetu (4 x 250 MHz = 1 GHz) i transmisji ATM 622 Mb/s;
— klasa EA (kategoria 6A) – wprowadzona wraz z klasą FA przez ISO/IEC 11801 2002:2 Poprawka 1. Obejmuje pasmo do częstotliwości 500 MHz;
— klasa F (kategoria 7) – opisana w ISO/IEC 11801 2002:2. Możliwa jest realizacja aplikacji wykorzystujących pasmo do 600 MHz. Różni się ona od poprzednich klas stosowaniem kabli typu S/FTP (każda para w ekranie plus ekran obejmujący cztery pary) łączonych ekranowanymi złączami. Dla tej klasy okablowania jest możliwa realizacja systemów transmisji danych z prędkościami przekraczającymi 1 Gb/s;
— klasa FA (kategoria 7A) – wprowadzona przez ISO/IEC 11801 2002:2 Poprawka 1. Obejmuje pasmo do częstotliwości 1000 MHz; umożliwia uzyskanie prędkości do 100 Gbit/s do 15 m i 40 Gbit/s do 100 m;
— klasa I (kategoria 8.1) — w trakcie rozwoju (opisana w ANSI/TIA-568-C.2-1, ISO/IEC 11801 3rd Ed.), wykorzystująca pasmo częstotliwości 1600-2000 MHz; prędkość transmisji > 40 Gbit/s;
— klasa II (kategoria 8.2) — w sprzedaży (opisana w ISO/IEC 11801 3rd Ed.), wykorzystująca pasmo częstotliwości 1600-2000 MHz.

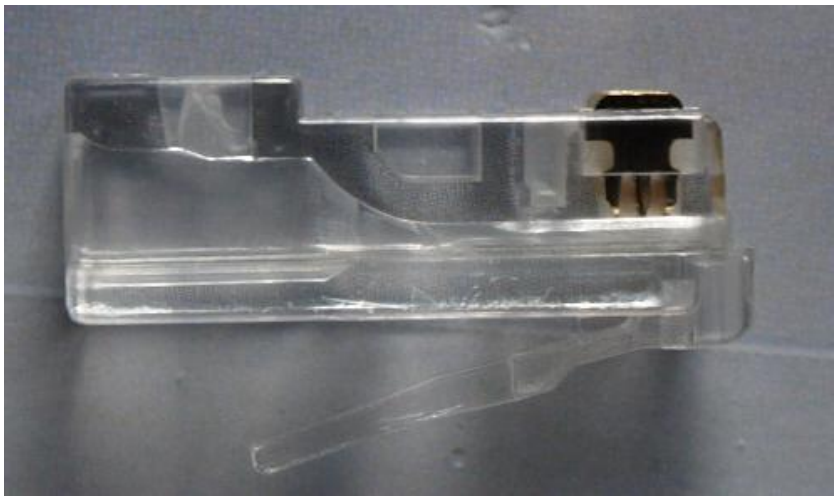
1.6. Wtyczki

Standardowa wtyczka stosowana do budowy sieci pochodzi od wtyczek stosowanych w połączeniach telefonicznych.
— Używany jest standard gniazda/wtyczki 8P8C (czasami nazywany RJ45 — co nie jest do końca słuszne); RJ45 to standard wtyczki telefonicznej,
— 8P8C tłumaczy się jako *8 position 8 contact*,
— kabel sieciowy (skrętka) ma cztery pary przewodów o kolorach:
  — zielony (przewody zielony i biało-zielony)
  — brązowy
  — niebieski
  — pomarańczowy
  w każdej parze kolor izolacji jednego przewodu jest jednolity, a drugiego biały z paskiem
— Ponieważ kable sieciowe są dwu rodzajów: linka oraz drut, do każdego trzeba stosować inny standard wtyczki

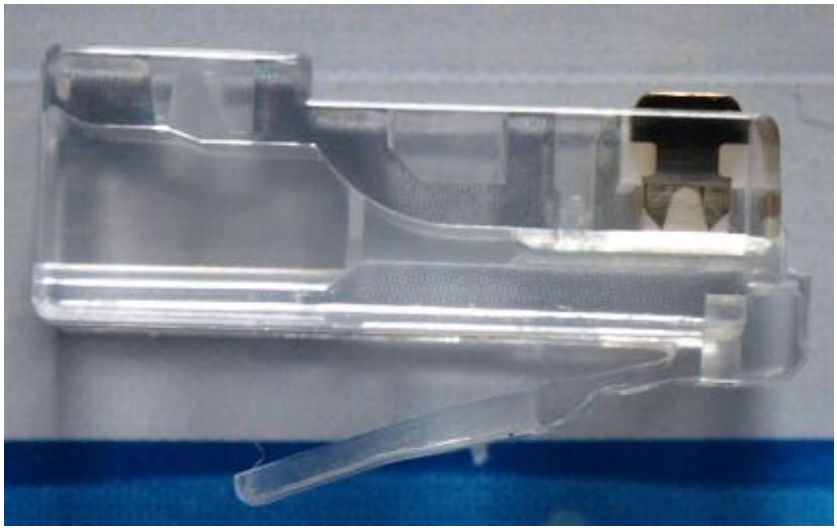
W przypadku linki, ostrza styku (rys. 10) przecinają izolację i wchodzą w środek linki, w przypadku drutu (rys. 9) przecinają izolację i powinny objąć drut — stąd zastsowano trzy ostrza.

1.7. Schemat połączeń kabla

Ta inteligencja obejmuje znacznie więcej niż tylko rozpoznanie czy kabel jest „prosty” czy „skrzyżowany”. Opracowany jest protokół auto-negocjacji pozwalający ustalić szybkość przesyłania danych (to że karty sieciowe są 1000 Mb/s nie oznacza, że dane będą przesyłane z tą prędkością — zależy to jeszcze od jakości kabla i połączeń: wtyczek i gniazd). Dodatkowo negocjowany jest tryb transmisji dupleksowy (równoczesna moż-



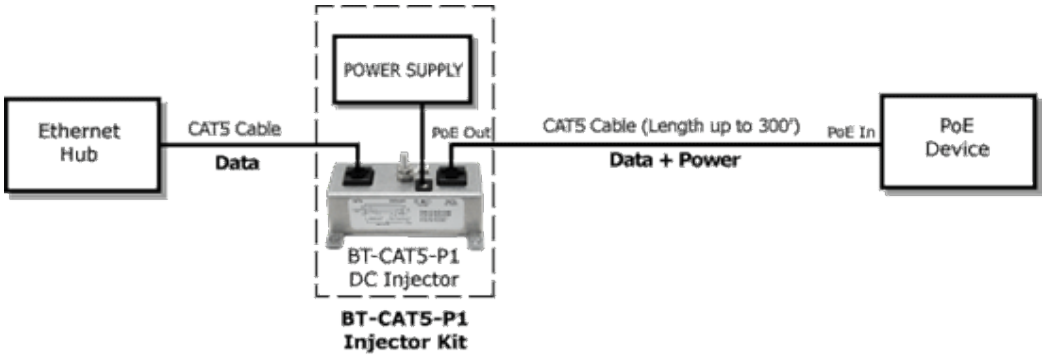
Rysunek 9. Wtyczka: drut



Rysunek 10. Wtyczka: linka

liwość nadawania i odbierania) i półdupleksowy — albo nadawani albo odbieranie. Ponieważ w skrętce osobne pary używane są do nadawania i odbierania, fakt, że karta pracuje w trybie półdupleksowym oznacza poważne problemy z okablowaniem.

W przypadku sieci światłowodowych z negocjacją jest znacznie trudniej — ciągle zdarzają się urządzenia nie obsługujące tej funkcjonalności.



Rysunek 11. Schemat połączeń PoE

Pin	T568A pair	T568B pair	10/100 BASE-T signal id.	1G/10 GBASE-T signal id.	T568A color	T568B color	Diagram
1	3	2	DA+	DA+	white/green stripe	white/orange stripe	
2	3	2	DA–	DA–	green solid	orange solid	
3	2	3	DB+	DB+	white/orange stripe	white/green stripe	
4	1	1	NC	DC+	blue solid	blue solid	
5	1	1	NC	DC–	white/blue stripe	white/blue stripe	
6	2	3	DB–	DB–	orange solid	green solid	
7	4	4	NC	DD+	white/brown stripe	white/brown stripe	
8	4	4	NC	DD–	brown solid	brown solid	

2. Power over Ethernet: PoE

Power over Ethernet oznacza zasilanie urządzeń przez Ethernet.

— POE to standard pozwalający na równoczesne przesyłanie kablem sygnału i zasilania.
— Technologia pozwala na zasilanie urządzeń o stosunkowo niewielkim poborze mocy (punkty dostępowe, kamery internetowe, telefony VoIP).
— Używa się napięcia „bezpiecznego" czyli poniżej 60 V napięcia stałego.
— Technologia może być stosowana dla 10BASE-T, 100BASE-T i 1000BASE-T.

Mogą być stosowana specjalne urządzenia aktywne wyposażone w jeden (lub więcej) portów z obsługą PoE. Czasami stosuje się „wstrzykiwanie" PoE i umieszcza zasilacz między urządzeniem aktywnym a odbiornikiem potrzebującym zasilania (rys. 19).

Rysunek 12. Logo Wi-Fi

Część II

Wi-Fi

3. Sieci bezprzewodowe: Wi-FI

Współczesne sieci Wi-Fi są „wnukami" sieci ALOHAnet.

Sieć bezprzewodowa promowana jest przez W-Fi Alliance, które opracowało i jest właścicielem logo (rys. 12). Konsorcjum ustaliło też oficjalną pisownię skrótu: Wi-Fi (choć stosowane bywają i inne pisownie).

Jest kilka standardów transmisji radiowej w paśmie 2,4 i/lub 5 GHz oferujących różne prędkości transmisji:

802.11a 54 Mb w paśmie 5 GHz (Wi-Fi 2: 1999),

802.11b 11 Mb (praktycznie 5,5 Mb) w paśmie 2,4 GHz; zasięg 30/120 m (Wi-Fi 1: 1999),

802.11g 54 Mb w paśmie 2,4 GHz (praktycznie 20–22 Mb) (Wi-Fi 3: 2003)

802.11n 300 Mb (5 GHz) lub 150 Mb (2,4); praktyczne transfery 150 Mb (w dobrych warunkach), (Wi-Fi 4: 2009)

802.11ac do 433–6928 Mb, (Wi-Fi 5: 2014) 2,4, 5,GHz

802.11ax do 575–9608 Mb (Wi-Fi 6, 6E: 2019) 2,4, 5, 6 (E) GHz

802.11be do 40 Gb (Wi-Fi 7: ????)

i jeszcze parę innych Wi-Fi korzysta z następujących protokołów w warstwie fizycznej:

DSSS *Direct Sequence Spread Spectrum* Sygnał mnożony jest przez (pseudo)losową sekwencję co upodabnia spektrum sygnału do białego szumu.

FHSS *Frequency Hopping Spread Spectrum* Sygnał jest przełączamy pomiędzy wieloma kanałami (w zdefiniowanym paśmie)

OFDM *Orthogonal Frequency-Division Multiplexing* Jednoczesna transmisja wielu strumieni danych na ortogonalnych częstotliwościach nośnych.

Te techniki modulacji są stosowane aby minimalizować interferencję sygnałów, ich przechwycenie oraz zakłócenie, albo likwidować problemy z sygnałami odbitymi, które docierają do odbiornika z pewnym opóźnieniem.

— USA: 1–11

— Japonia: 1–14
— Większość świata: 1–13

W przypadku częstotliwość 5 MHz (standardy 802.11a/h/j/n/ac/ax) sytuacja jest znacznie bardziej skomplikowana: Różnice pomiędzy regionami są znacznie większe, nieco inne normy obowiązują wewnątrz pomieszczeń, inne na zewnątrz co spowodowane jest możliwością interferencji z innymi urządzeniami, na przykład radarami pogodowymi.

W każdym przypadku obowiązują ograniczenia mocy nadajnika.

— Najczęściej korzystamy z sieci bezprzewodowych w trybie „infrastruktura".
— Punkt dostępowy (*access point*) rozgłasza nazwę sieci i wszyscy chcący z sieci skorzystać wskazują wybraną sieć i komputer łączy się z nim. Czasami zabrania się rozgłaszania nazwy sieci — przestaje być ona wówczas „widoczna" dla oprogramowania zwykłych użytkowników, ale łatwo odczytać ją z przesyłanych pakietów między stacją a punktem dostępowym. W pewnym sensie zwiększa to bezpieczeństwo…
— W przypadku gdy sieć ma pokryć większy obszar — punktów dostępowych jest więcej, wszystkie rozgłaszają tę samą nazwę sieci. W przypadku gdy niezbędne jest hasło — jest ono jednakowe dla wszystkich punktów dostępu. (A do zarządzania hasłami używa się bazy danych wspólnej dla całej sieci.) Oprogramowanie zawsze wybiera punkt dostępowy o najsilniejszym sygnale. Możliwy jest roaming (czyli swobodne przemieszczanie się stacji po obszarze z dostępem sieciowym).
— Sieć bezprzewodowa może być również używana w trybie *ad-hoc* — łącząc, na przykład, tylko dwa komputery.

Carrier Sense with Multiple Access/Collision Avoidance — CSMA/CA

— Sieci bezprzewodowe wykorzystują CSMA/CA do sterowania ruchem pakietów.
— Stosowanie (znanego z Ethernetu przewodowego) systemu CSMA/CD jest utrudnione — stacja nadająca zagłusza praktycznie wszystkie sygnały.
— Komunikacja jest nieco bardziej skomplikowana:
  — najpierw stacja chcąca nadawać wysyłą specjalną ramkę *Request To Send* informując inne stacje o zamiarze nadawania,
  — punkt dostępowy wysyła ramkę *Clear to Send* (gotowy do odbioru); informacja ta dociera również do odbiorcy.
  — teraz można wysłać ramkę z danymi, której otrzymanie
  — potwierdza odbiorca ramką ACK.

Bezpieczeństwo

1. Podstawowy problem związany jest z tym, że znacznie łatwiej uzyskać „fizyczny" dostęp do medium niż w przypadku sieci przewodowych.
2. Najstarszy standard szyfrowania (WEP — *Wired Equivalent Privacy*) okazał się bardzo łatwy do złamania.

3. Nowsze (WPA lub WPA2 *Wi-Fi Protected Access*) są nieco bardziej bezpieczne.
4. Trzeba pamiętać, że bardzo wiele punktów dostępowych/routerów bezprzewodowych domyślnie skonfigurowana jest do pracy w trybie nieszyfrowanym. Należy je zaraz po uruchomieniu odpowiednio skonfigurować.
5. Aby „ułatwić" podłączanie kolejnych urządzeń wymyślono WPS (*Wi-Fi Protected Setup*). Jest to sposób na podłączanie kolejnych urządzeń bez podawania hasła, po wprowadzeniu urządzenia dostępowego w specjalny tryb. Niestety okazało się, że stosunkowo łatwo wykorzystać ten sposób zabezpieczenia do uzyskania nieautoryzowanego dostępu.

Protokół szyfrowania WEP podatny był na atak słownikowy. I można było go złamać stosunkowo łatwo. W związku z tym wprowadzono metodę WPA, która — co do idei — właściwie nie różniła się od WEP, ale klucz zmieniany był cyklicznie co utrudniało (lub właściwie uniemożliwiało) złamanie go metodą podobną do WEP. Okres w jakim używany był jeden klucz, był stosunkowo krótki.

Dopiero WPA2 pozwoliło na poważne zabezpieczenie sieci bezprzewodowych. NA początku roku 2018 opublikowano standard WPA3 zawierający kolejne usprawnienia WPA2.

W-Fi 6

Część III

Urządzenia aktywne

4. Koncentratory i regeneratory sygnału

— Działa w najniższej warstwie (fizycznej).
— Służy do powtórzenia na swoim wyjściu (wyjściach) sygnału pojawiającego się na wejściu.
— Może być traktowany jako specyficzny wzmacniacz (wzmacniak) sygnału.
— Wykorzystywane do łączenia wielu segmentów (fragmentów) sieci Ethernet w jeden (większy) segment.
— Praktycznie już nie wykorzystywane, gdyż powiększanie domeny kolizyjnej w sieciach Ethernet to samobójstwo.

W szczególności, w początkowym okresie budowy sieci, gdy doświadczenia były niewielkie, a urządzenia zawodne zdarzały się sytuacje, gdy dwa segmenty sieci miały więcej niż jedno połączenie między sobą. Prowadziło to czasami od sytuacji gdy informacje zaczynały krążyć między segmentami (broadcast storm). Sytuacje takie potrafiły wysycić do zera przepustowość sieci.

5. Mosty

— Mosty to urządzenia nieco podobne do koncentratorów, ale nieco bardziej od nich inteligentne.
— Są wolniejsze od koncentratora, który natychmiast po otrzymani pierwszego bajtu ramki wysyła go poszczególnych portów; most zapisuje pakiet w pamięci, analizuje go i ewentualnie przesyła dalej.
— Używane są one do łączenia segmentów sieci.
— Na podstawie adresów fizycznych podejmowały one decyzję, czy pakiet ma być przesłany do następnego segmentu sieci.
— Most musi znać topologię sieci aby podejmować decyzję czy (i gdzie) przekazywać pakiet.
— Stosunkowo często używanie gdy jeden z segmentów sieci jest siecią bezprzewodową.

Na potrzeby optymalizacji pracy sieci łączonych mostami opracowano specjalny protokół (*Spanning Tree Protocol* — protokół drzewa rozpinającego), który podpowiada, które redundantne połączenia należy wyłączyć aby nie tworzyły się pętle. Urządzenia uczą się topologii sieci i potrafią włączyć wyłączone połączenia w sytuacji gdy sieć staje się niespójna.

6. Przełączniki

— Przełącznik (wizualnie) niewiele różni się od koncentratora.

— Natomiast zasada działania jest inna.
— Przełącznik działa w drugiej warstwie ISO/OSI.
— Zasada funkcjonowania jest podobna do mostu, z tym, że przełącznik ma, zazwyczaj, wiele portów.
— Oprócz najprostszych urządzeń można spotkać „przełączniki zarządzalne" — pozwalające na zaawansowaną konfigurację i monitorowanie ruchu.

7. Zapory sieciowe

— Zapora sieciowa to wyspecjalizowane urządzenie[1] (coraz rzadziej) lub specjalizowane oprogramowanie zainstalowane na:
  — stacji użytkowej,
  — bramie sieciowej.
— Zadaniem tego oprogramowania jest selektywne blokowanie ruchu sieciowego.
— Ruch może być blokowany/filtrowany z wykorzystaniem wielu kryteriów:
  — źródłowy/docelowy adres IP
  — źródłowy/docelowy numer portu
  — użyty protokół
  — czasami można zaglądać do wnętrza *deep packet inspection* pakietów i filtrować, na przykład, dostęp do wybranych stron WWW albo wybranych protokołów komunikacyjnych.

8. Network Address Translation (NAT)

— Translacja adresów sieciowych to usługa pozwalająca na „ukrycie" komputerów (korzystających z adresów IP publicznych lub prywatnych), tak, że na zewnątrz ich adresy są niewidoczne, a kontakt z internetem odbywa się przez wybrany publiczny adres IP.
— Funkcja realizowana jest (jako dodatkowa) przez bramę sieciową.
— Celem tej usługi może być oszczędzanie publicznych adresów IP.
— Ze względu na ograniczoną liczbę portów (65535)[2] liczba komputerów ukrytych za NAT jest ograniczona.
— Bardzo często zaawansowane systemy NAT korzystają więcej niż z jednego publicznego adresu IP.
— Stosowanie NAT w niektórych sytuacjach prowadzi do mniej lub bardziej poważnych problemów.

Inna nazwa NAT to *IP masquerading*.

9. Brama

— Brama to (najczęściej) wyspecjalizowany komputer wyposażony w kilka interfejsów sieciowych z zainstalowanym oprogramowaniem.

[1] Z odpowiednim oprogramowaniem.
[2] Jedna stacja może używać nawet 4000.

- Praktycznie każdy komputer z więcej niż jedną kartą sieciową może być wykorzystany w tym celu (pomijamy kwestie wydajności).
- Komputery z linuksem (w standardowej konfiguracji) nie przekazują pakietów między interfejsami sieciowymi, ale bardzo łatwo to zmienić.
- Wystarczy do tego dodać odpowiednie tablice routingu.
- Dodatkowo można zainstalować funkcje (i skonfigurować) funkcje:
  - translacji adresów,
  - zapory sieciowej.
- Dodatkowe funkcje popularnych routerów „domowych“ to:
  - punkt dostępowy WiFi,
  - „modem” DSL,
  - „modem” tv kablowej,
  - NAS (*Network Attached Storage*) czyli dysk sieciowy,
  - serwer wydruku,
  - głośnik sieciowy,
  - ...