Projekt

„Nauczyciel w teorii i praktyce.
Program doskonalenia zawodowego
w przedsiębiorstwach
dla nauczycieli kształcenia zawodowego
w sektorze informatycznym i telekomunikacyjnym”

Podstawy administrowania sieciami komputerowymi

Materiały szkoleniowe dla uczestniczek i uczestników warsztatów

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

TYLDA KOMPUTERY

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Materiały współfinansowane ze środków Unii Europejskiej
w ramach Europejskiego Funduszu Społecznego

Materiały współfinansowane ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego (Priorytetu III – Wysoka jakość systemu oświaty, Działania 3.4. Otwartość systemu edukacji w kontekście uczenia się przez całe życie, Poddziałania 3.4.3. Upowszechnienie uczenia się przez całe życie – projekty konkursowe).

Materiały opracowane przez
Instytut Nauk Społeczno-Ekonomicznych sp. z o.o.
ul. Polskiej Organizacji Wojskowej 17, lok. 4 A
90–248 Łódź
tel: (42) 633 17 19, faks: (42) 209 36 85

Materiały opracował:
Piotr Kotynia

Redakcja merytoryczna:
Bartłomiej Konarczak, Michał Dwużnik

Korekta:
Anna Strożek

Skład:
Katarzyna Banacińska

Okładka:
Katarzyna Banacińska

ISBN 978-83-63120-05-4

Druk:
Drukarnia Cyfrowa i Wydawnictwo „Piktor”
ul. Tomaszowska 27, 93–231 Łódź
tel: (42) 659 71 78, faks: (42) 617 03 07
www.piktor.pl

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Człowiek – najlepsza inwestycja
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Spis treści

Wstęp

Prezentowane materiały szkoleniowe dla uczestniczek i uczestników warsztatów pt. *Podstawy administrowania sieciami komputerowymi* zostały opracowane na potrzeby projektu *Nauczyciel w teorii i praktyce. Program doskonalenia zawodowego w przedsiębiorstwach dla nauczycieli kształcenia zawodowego w sektorze informatycznym i telekomunikacyjnym* realizowanego przez firmę Tylda Sp. z o.o. w ramach Programu Operacyjnego Kapitał Ludzki współfinansowanego ze środków Europejskiego Funduszu Społecznego.

Projekt adresowany jest do nauczycieli przedmiotów zawodowych oraz instruktorów praktycznej nauki zawodu, którzy kształcą na potrzeby sektora informatycznego i telekomunikacyjnego.

Projektodawcą jest firma Tylda Sp. z o.o., która funkcjonuje na rynku IT od 2000 roku. Od trzech lat zajmuje się organizacją kursów i warsztatów komputerowych. Poprzez swoje działania firma dąży m.in. do umocnienia rynku lokalnego i promowania usług. Obecnie Tylda Sp. z o.o. jest jednym z liderów w swojej branży w województwie lubuskim w zakresie wdrożeń zaawansowanych rozwiązań technologicznych, komunikacyjnych, sprzedaży hurtowej i szkoleń miękkich.

Celem kursu jest przedstawienie koncepcji sieci komputerowej jako medium służącego do wymiany informacji, współdzielenia zasobów i aplikacji. Na początku materiałów zaprezentowane zostały podstawowe topologie sieci oraz modele stosów protokołów sieciowych modelu OSI oraz TCP/IP.

W następnej części przedstawione są sieci lokalne LAN i sieci rozległe WAN. Obecnie najpopularniejszą technologią w sieci lokalnej jest technologia Ethernet i to właśnie ona jest bliżej opisana w niniejszych materiałach. Natomiast przy omawianiu sieci WAN są przedstawione róż-

nego rodzaju technologie, które są wykorzystywane przy łączeniu się sieci w sieci rozległe.

W ostatniej części materiałów opisany jest protokół IP w wersji 6., którego celem jest zastąpienie obecnie działającego protokołu IP w wersji 4. W tej części opisane są problemy związane z używaniem protokołu IPv4, wśród których wymienia się kwestię brakujących adresów IP.

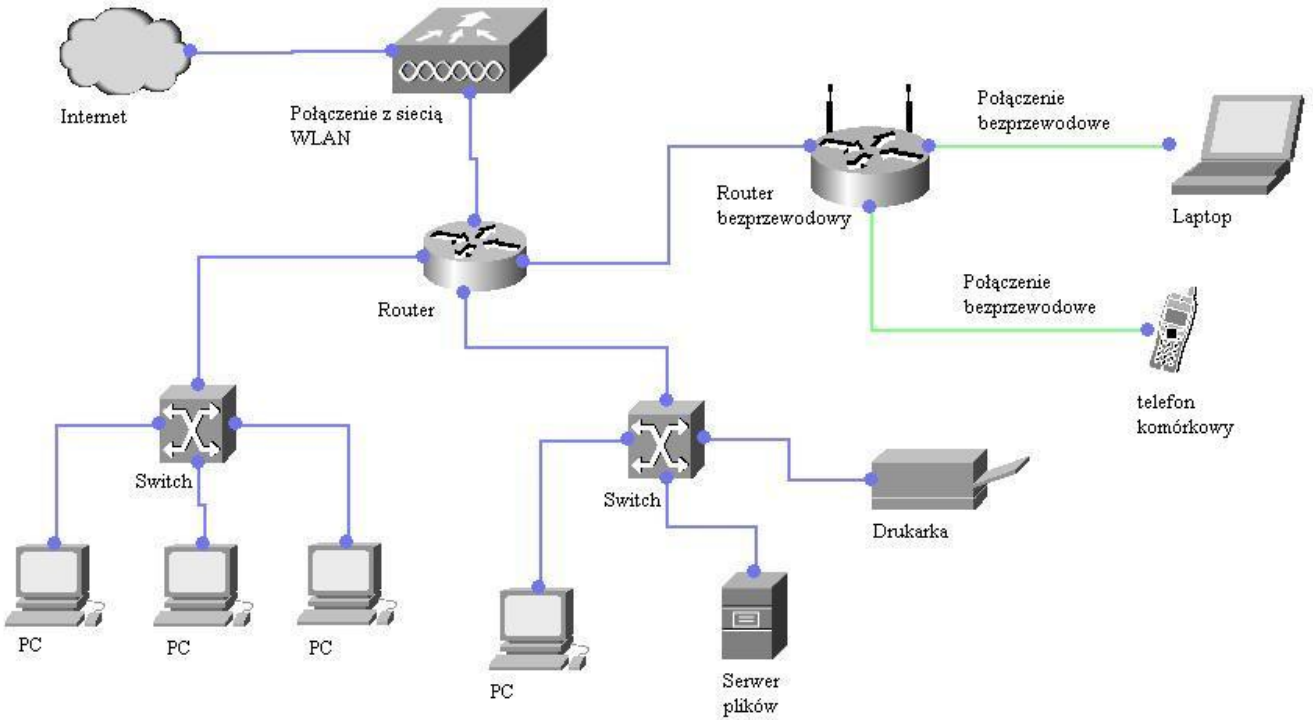
Sieć komputerowa

Sieć komputerowa to najprościej mówiąc zbiór połączonych ze sobą urządzeń sieciowych oraz systemów końcowych, w którym następuje wymiana informacji oraz współdzielenie zasobów. W dzisiejszych czasach systemami końcowymi mogą być nie tylko komputery, ale również telefony stacjonarne i komórkowe, urządzenia związane z automatyzacją produkcji i wiele innych. Wszystkie te urządzenia wymieniają za pomocą sieci informacje w postaci plików, dźwięku, obrazu, strumieni danych. Od połowy lat 90. coraz większego znaczenia nabiera Internet, czyli medium, które umożliwia połączenie wielu lokalnych i rozległych sieci w globalny łańcuch komunikacyjny. Budowa sieci komputerowych ma charakter hierarchiczny, można ją porównać do organizacji infrastruktury miast i państw gdzie poszczególne domy przynależą do danych ulic, ulice grupowane są w dzielnice, dzielnice tworzą miasta, a te połączone są z innymi miastami. Każdy obiekt posiada swój unikalny adres oraz możliwość dotarcia do niego z dowolnego miejsca. W sieci komputerowej komputery lub inne urządzenia (prędzej czy później nawet lodówki w naszych domach staną się systemami końcowymi) komunikują się ze sobą za pomocą urządzeń takich jak huby i switche. Połączenie takie stanowi podstawowy segment sieci. Segmenty łączone są ze sobą za pomocą routerów odpowiadających za określanie optymalnej ścieżki, po której informacja dotrze do celu. Urządzenia w sieci połączone są ze sobą za pomocą różnych rodzajów mediów transmisyjnych, kablowych (kable koncentryczne, skrętka, światłowody) i bezprzewodowych.

Przy projektowaniu, dokumentowaniu oraz zrozumieniu sieci komputerowej powszechnie wykorzystuje się diagramy sieciowe. Diagramy powinny zawierać jak najwięcej wartościowych informacji, będąc jednocześnie czytelnymi, przejrzystymi i spójnymi. Mogą być wykorzystane do przedstawienia fizycznej topologii sieci.

Przykładowy diagram sieci został zaprezentowany na następnej stronie.

Rysunek 1. Przykładowy diagram sieci



Źródło: opracowanie własne.

Współdzielenie zasobów w sieci

Sieci komputerowe tworzone są, aby umożliwić wygodne i wydajne współdzielenie zasobów w celu poprawienia produktywności pracowników i całych organizacji. W sieci można współdzielić na przykład dane, aplikacje, kopie zapasowe. Istnieje wiele różnych rodzajów programów użytkowych umożliwiających wykorzystanie potencjału sieci. Można je podzielić na kategorie związane z poszczególnymi usługami sieciowymi, z których korzystają aplikacje:

1. E-mail (MS Outlook, POP3, Gmail itd.),
2. Przeglądarki internetowe (Firefox, Explorer, Chrome itd.),
3. Komunikatory (Skype, Gadu-Gadu itd.),
4. Wideokonferencje (Whiteboard, NetMeeting, Livemeeting itd.),
5. Bazy danych (serwery plików).

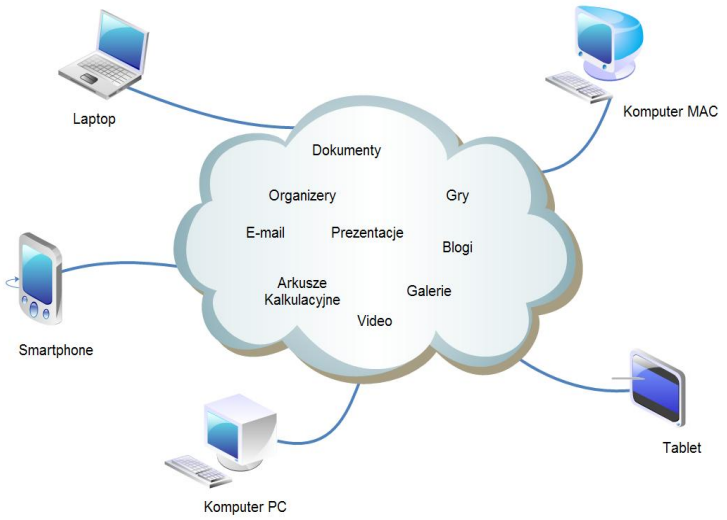
Programy umożliwiające zarządzanie korespondencją elektroniczną, przeglądarki internetowe oraz komunikatory to przykłady aplikacji powszechnie używanych. Programy do wideokonferencji czy rozwiązania dotyczące sieciowych baz danych to z kolei przykłady aplikacji stosowanych przeważnie przez korporacje i często tworzonych na potrzeby danej organizacji. Z punktu widzenia sieci aplikacje można podzielić na podstawie wymogów, jakie musi spełnić dane połączenie sieciowe, aby aplikacja poprawnie działała. Przykładowo w wypadku transferu plików ważna jest przepustowość sieci, tak aby duże pakiety danych mogły być przesyłane sprawnie, nie jest jednak istotne, czy opóźnienia pomiędzy wysłaniem kolejnych pakietów są mniejsze czy większe, w najgorszym wypadku plik dotrze do adresata kilka sekund później. Na prze-

ciwnym krańcu wymagań znajdują się aplikacje takie jak komunikatory głosowe czy programy do wideokonferencji. Są to aplikacje czasu rzeczywistego, w których kluczową rolę odgrywają opóźnienia pomiędzy przesyłaniem kolejnych niewielkich pakietów. Gdy opóźnienia te będą zbyt duże, może dochodzić do zniekształceń głosu i obrazu. Przepustowość natomiast nie jest tu tak istotna, po osiągnięciu wymaganej przez aplikacje przepustowości sieci dalsze jej zwiększanie nie ma sensu. Warto jednak pamiętać, że w sieci funkcjonują przeważnie oba typy aplikacji naraz. Podstawowym zadaniem stawianym przed administratorami sieci jest zapewnienie odpowiedniej jakości usług (ang. *Quality Of Service* – QoS), czyli umożliwienie prawidłowego funkcjonowania wszystkich wymaganych aplikacji przy często ograniczonych możliwościach infrastruktury sieciowej.

Obliczenia dokonywane w chmurze

W ostatnim czasie bardzo szybko rozwija się specyficzna forma aplikacji sieciowych. Usługi te polegają na udostępnianiu na żądanie zasobów i aplikacji sieciowych. Określane są jako obliczenia dokonywane w chmurze (ang. *cloud computing*). Na diagramach sieciowych chmura oznacza sieć zewnętrzną, na temat której niewiele wiadomo. Podobnie jest w przypadku obliczeń w chmurze – z punktu widzenia użytkownika nie jest istotne, z jakich urządzeń składa się sieć i na której fizycznie maszynie dokonywane są obliczenia, liczy się jedynie otrzymany rezultat. Zaletą takich rozwiązań jest fakt, że użytkownik nie musi instalować aplikacji ani posiadać wydajnego komputera spełniającego wymagania zaawansowanych aplikacji. W zasadzie na komputerze klienta może działać jedynie system operacyjny oraz przeglądarka internetowa.

Rysunek 2. Obliczenia wykonywane w chmurze



Źródło: opracowanie własne.

Komputer korzystający z aplikacji umieszczonych w chmurze musi oczywiście mieć dostęp do sieci. Wszystkie obliczenia dokonywane są na maszynach do niej podłączonych. Daje to olbrzymie możliwości – obecnie prawie każdy program może zostać przeniesiony w chmurę.

Aplikacje proponowane w chmurze często określa się jako oprogramowanie w postaci usługi (angielskie określenie: *software as a service* – SaaS).

Usługi udostępniane w chmurze często wykonywane są w sieciach publicznych takich jak Internet, w związku z tym dostęp do nich musi być odpowiednio zabezpieczony. Użytkownik, aby uzyskać dostęp do swojego konta, musi dokonać identyfikacji i uwierzytelnienia (najczęściej za pomocą loginu i hasła).

W chwili obecnej wydaje się, że aplikacje i usługi udostępniane w chmurze stanowią rozwinięcie koncepcji sieci komputerowych, sprawiając, że sieć nie jest już tylko medium łączącym komputery, ale staje się platformą udostępniającą kompletne, szybkie i bezpieczne rozwiązania informatyczne, działające tak samo niezależnie od tego, z jakiego urządzenia czy systemu łączymy się do nich.

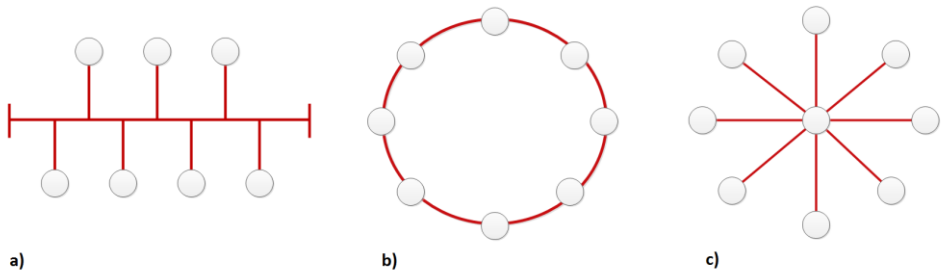
Rodzaje topologii sieciowych

Istnieją dwa podstawowe rodzaje topologii sieciowych:

1. topologia fizyczna,
2. topologia logiczna.

Topologia fizyczna opisuje okablowanie, czyli sposób, w jaki są ze sobą połączone elementy sieci, natomiast topologia logiczna to opis tego, w jaki sposób odbywa się przepływ danych w sieci.

Rysunek 3. Trzy podstawowe typy topologii: a) magistrala, b) pierścień, c) gwiazda



Źródło: opracowanie własne.

Rysunek 3. przedstawia trzy podstawowe typy fizycznych topologii sieciowych. Są one historycznie połączone z rodzajami okablowania. Jedną z topologii wykorzystywaną w sieciach komputerowych jest topologia magistrali, do łączenia urządzeń wykorzystywany był w niej kabel koncentryczny. W przypadku topologii magistrali wszystkie urządzenia dzielą to samo pasmo, odpowiednie dla kabla koncentrycznego. W przypadku topologii pierścienia każde urządzenie połączone jest z kolejnym, przy czym ostatni i pierwszy element sieci zamykają pierścień. Rozwiązanie to ma jed-

ną podstawową wadę. Przerwanie połączenia pomiędzy dwoma elementami sieci uniemożliwia działanie całego segmentu. W topologii gwiazdy centralne urządzenie odpowiada za połączenie pomiędzy urządzeniami.

Topologia magistrali

W tej topologii urządzenia podłączone są do jednego przewodu. Typowo jest to kabel koncentryczny. Na końcach kabla umieszczone są terminatory, których celem jest uniemożliwienie odbijania się sygnałów, co groziłoby zakłóceniem transmisji danych. We wczesnych fazach rozwoju sieci komputerowych topologia magistrali była powszechnie stosowana.

Topologia pierścienia

W topologii pierścienia wszystkie urządzenia podłączone są ze sobą i tworzą pętlę; w przeciwieństwie do topologii magistrali urządzenia nie są podłączone do pojedynczego przewodu, lecz są połączone ze sobą nawzajem. Sygnał porusza się w sieci w jednym kierunku – od nadawcy do odbiorcy.

Topologia gwiazdy

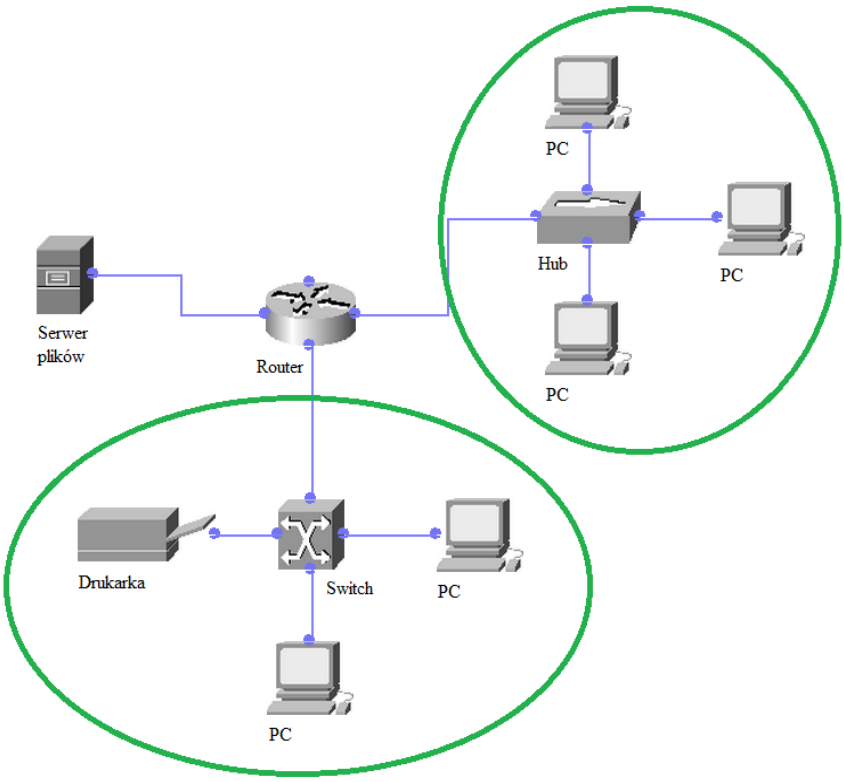
Topologia gwiazdy wykorzystuje pojedynczy centralny punkt, do którego podłączone są urządzenia zewnętrzne. Rozwiązanie takie zwiększa niezawodność sieci. Awaria pojedynczego połączenia nie powoduje unieruchomienia całej sieci, a jedynie odłączenie od niej jednego urządzenia. Centralny element sieci stanowi jednak pojedynczy punkt awarii (ang. *single point of failure*).

Optymalną pod kątem niezawodności metodą połączenia ze sobą urządzeń w sieci jest tak zwana pełna topologia kratowa (ang. *full mesh topology*). Zakłada ona, że każde urządzenie w sieci jest połączone z każdym innym urządzeniem. W praktyce zastosowanie takie wiąże się ze zbyt dużymi kosztami. Częściowe topologie kratowe stosuje się przy połączeniach pomiędzy sieciami WAN lub w sieciach korporacyjnych.

W przeciwieństwie do topologii fizycznej topologia logiczna określa, w jaki sposób sygnały przepływają przez fizyczną sieć. Topologia logiczna może pokrywać się z topologią fizyczną. Taki przypadek ma miejsce w topologiach magistralowych. Zarówno fizyczna, jak i logiczna topologia magistrali używa tej samej linii do przekazywania sygnału. Zdarzają się jednak również przypadki, gdy topologia logiczna nie odpowiada topologii fizycznej.

Na rysunku 4. zamieszczonym na kolejnej stronie przedstawiona została topologia fizyczna niewielkiej sieci komputerowej. Urządzenia w segmentach sieci zaznaczonych zielonymi elipsami są połączone ze sobą fizycznie poprzez centralne urządzenie sieciowe, czyli wykorzystują topologię gwiazdy. Z logicznego punktu widzenia mamy jednak do czynienia z topologią magistrali. Zarówno switch, jak i hub działają w ten sposób, że przesyłają sygnał do wszystkich urządzeń, które są do nich podłączone, tak więc z punktu widzenia topologii logicznej elementy końcowe współdzielą jedną linię, po której porusza się informacja.

Rysunek 4. Różnice między topologią fizyczną a logiczną



Źródło: opracowanie własne.

Domeny rozgłoszeniowe i domeny kolizyjne

Obecnie powszechnie stosowane są rozwiązania sieciowe oparte na technologii Ethernet. Jest ona najbardziej rozpowszechnioną technologią sieciową, która pomimo swoich wad zdominowała rozwój sieci lokalnych LAN. W sieciach Ethernet urządzenia końcowe podłączone są do różnych rodzajów urządzeń sieciowych, tworząc tak zwane domeny. Wyróżniamy dwa rodzaje domen. Domeny rozgłoszeniowe oraz domeny kolizyjne. W najprostszym przypadku kilka komputerów jest podłączonych do jednego huba, tworząc jeden segment sieci, który stanowi pojedynczą domenę kolizyjną. Sygnał w takiej domenie propagowany jest do wszystkich urządzeń jednocześnie. Oznacza to, że gdy kilka urządzeń rozpocznie równocześnie nadawanie sygnału, w sieci dochodzi do kolizji – w takim przypadku po odczekaniu pewnego losowego okresu urządzenia rozpoczynają nadawanie ponownie. Domeny kolizyjne są ograniczone przez switche. Switche określają adres odbiorcy na podstawie adresu MAC, tak więc transmisja danych może odbywać się pomiędzy różnymi urządzeniami, nie powodując kolizji. Domeny rozgłoszeniowe to z kolei takie segmenty sieci, w których mogą się poruszać sygnały przeznaczone do wszystkich urządzeń (transmisja broadcast). Domeny rozgłoszeniowe są tworzone przez urządzenie połączone ze sobą za pomocą hubów i switchy. Granicą dla domen rozgłoszeniowych są natomiast routery, które nie propagują dalej sygnałów typu broadcast.

Warstwowy model sieci OSI

W początkowych latach rozwoju sieci komputerowych organizacje badawcze zajmujące się tym zagadnieniem wprowadzały własne rozwiązania oparte o różne założenia. Wtedy nikt nie myślał o rozpowszechnianiu sieci poprzez umożliwienie włączania się w jej rozwój innych instytucji. Głównym celem pionierów rozwiązań sieciowych było na przykład połączenie za pomocą sieci kilku oddziałów uniwersytetu. W miarę rozwoju pojawiła się potrzeba standaryzowania rozwiązań, aby umożliwić producentom włączenie się w rozwój sieci poprzez określenie jasnych zasad komunikacji sieciowej. Jednym z najpełniejszych modeli komunikacji sieciowej jest model zaproponowany przez organizację ISO – warstwowy model OSI (Open System Interconnection). Warstwy, z których składa się model ISO, prezentuje poniższa tabela.

Tabela 1. Warstwowy model OSI

Numer warstwy	Warstwa	Rodzaj danych	Funkcja
7	aplikacji	dane	dostarczanie usług sieciowych
6	prezentacji	dane	reprezentacja danych, szyfrowanie, deszyfrowanie, konwertowanie danych
5	sesji	dane	utrzymanie komunikacji na poziomie aplikacji
4	transportowa	segmenty	tworzenie i utrzymanie połączenia typu end-to-end
3	sieciowa	pakiety	określanie trasy, adresowanie logiczne
2	łącza danych	ramki	adresowanie fizyczne
1	fizyczna	bity	transmisja sygnałów binarnych

Źródło: opracowanie własne.

Tabela prezentuje siedem warstw modelu OSI. Dzięki rozbiciu zagadnienia komunikacji sieciowej na niezależne warstwy udało się osiągnąć wiele celów:

1. redukowanie złożoności zagadnienia,
2. standaryzowanie interfejsów,
3. zapewnienie modularności,
4. zapewnienie przenośności technologii,
5. umożliwienie lepszego zrozumienia sieci.

Warstwy składające się na model OSI są niezależne od siebie, a każda warstwa świadczy usługi dla warstw wyższych oraz stanowi zestaw standardów, które umożliwiają stworzenie przez firmy własnych rozwiązań technicznych dla danej warstwy, zapewniając jednocześnie ich kompatybilność.

Warstwa fizyczna

Warstwa ta określa media transmisyjne, jest to związane z zagadnieniami mechanicznymi, elektrycznymi, proceduralnymi i funkcjonalnymi umożliwiającymi aktywację, utrzymanie i dezaktywację połączenia. W skład warstwy fizycznej wchodzą charakterystyki mediów transmisyjnych, typy mediów transmisyjnych (kable światłowodowe, skrętka, transmisja bezprzewodowa) oraz rodzaj urządzenia umożliwiającego połączenie do sieci.

Warstwa łącza danych

Warstwa ta określa zasady dostępu do mediów transmisyjnych i jest czasami nazywana warstwą liniową lub kanałową. Podstawową cechą jest

nadzorowanie jakości przekazywanych informacji przez warstwę niższą. Warstwa łącza danych ma możliwość zmiany parametrów pracy warstwy fizycznej, tak aby zminimalizować liczbę błędów pojawiających się podczas przekazu. Celem tej warstwy jest również pakowanie danych w ramki i przekazywanie ich do warstwy fizycznej oraz rozpoznawanie i naprawa błędów związanych z niedotarciem pakietu i uszkodzeniem ramek.

Warstwa sieci

Zadaniem tej warstwy jest dostarczenie mechanizmów pozwalających na wytyczanie tras pomiędzy urządzeniami znajdującymi się w różnych, połączonych ze sobą sieciach. Warstwa sieci zapewnia adresowanie fizyczne oraz zasady wybierania optymalnej ścieżki dostarczenia danych w przypadku gdy istnieje kilka alternatywnych ścieżek.

Warstwa transportowa

Jest to warstwa zaangażowana w segmentowanie i przesyłanie danych, które poddawane są tutaj także podziałowi i numeracji. Do zadań warstwy transportowej należy zapewnienie niezawodności połączenia pomiędzy punktami końcowymi.

Warstwa sesji

Warstwa sesji odpowiada za nawiązanie, utrzymanie oraz kończenie sesji. W odróżnieniu od warstwy transportowej, która jest z kolei odpowiedzialna za nawiązanie, utrzymanie i zakończenie połączenia między dwoma urządzeniami, warstwa sesji działa na poziomie aplikacji. Dla przykładu, do serwera WWW może być podłączonych wielu użyt-

kowników, tworząc w ten sposób wiele sesji. Warstwa sesji odpowiada za rozróżnienie i zarządzanie połączeniami poszczególnych użytkowników do serwera.

Warstwa prezentacji

Warstwa prezentacji zajmuje się formatowaniem danych, tak aby były one czytelne dla odbierającego je systemu. Różne rodzaje danych wymagają różnych form formatowania i segmentacji, tekst może być przekazywany w formacie ciągu znaków ASCII, obrazy mogą być przekazywane za pomocą formatu BMP czy JPG itd.

Warstwa aplikacji

Warstwa aplikacji jest ostatnią warstwą systemu OSI. Jest to warstwa odpowiedzialna za interakcję całego systemu z użytkownikiem. Jako przykłady usług dostępnych w tej warstwie można wymienić: usługi pocztowe, przesyłanie plików czy mechanizmy autentykacji i autoryzacji użytkowników. Warstwa aplikacji umożliwia również korzystanie z usług sieciowych innym aplikacjom.

Stos protokołów TCP/IP

Stos protokołu TCP/IP został opracowany w tym samym czasie co model OSI. Ma on podobne założenia, opiera jednak komunikację sieciową na dwóch podstawowych protokołach – IP oraz TCP. Stos protokołów TCP/IP składa się z czterech warstw:

1. aplikacji,
2. transportu,
3. Internetu,
4. dostępu do sieci.

W modelu TCP/IP warstwa dostępu do sieci określa zasady dostępu do medium transmisyjnego. Warstwa Internetu określa sposoby routingu oraz doboru optymalnej ścieżki. Warstwa transportu, podobnie jak w przypadku modelu OSI, odpowiedzialna jest za zapewnienie niezawodnego połączenia pomiędzy dwoma punktami sieci. Warstwa aplikacji stanowi połączenie trzech najwyższych warstw modelu OSI (sesji, prezentacji, aplikacji).

Charakterystyka protokołu IP

Podstawowym elementem stosu TCP/IP jest protokół IP. W dużym skrócie można powiedzieć, że jest on odpowiedzialny za routing pakietów pomiędzy adresatem a odbiorcą. Pakiet to podstawowa jednostka danych, zawiera pewną porcję danych oraz informacje umożliwiające niezależne dostarczenie każdego pakietu do odbiorcy. W celu dostarcze-

nia pakietu do odbiorcy protokół IP wykorzystuje adresowanie hierarchiczne urządzeń w sieci. Protokół IP jest protokołem bezpołączeniowym, co oznacza, że sam protokół nie daje gwarancji dostarczenia danych do adresata oraz nie zapewnia żadnych mechanizmów odzyskiwania utraconych lub uszkodzonych pakietów. Zadanie to spoczywa na protokołach wyższej warstwy.

Struktura adresu IP

Adres w protokole IP w wersji 4. jest 32-bitowym numerem binarnym, który jednoznacznie identyfikuje dane urządzenie w sieci. Adres ma charakter hierarchiczny, co oznacza, że jego początkowe segmenty identyfikują sieć, a ostatnie – konkretne urządzenie. Pakiety protokołu IP zawierają w swoich nagłówkach adresy nadawcy i odbiorcy. Dla wygody 32-bitowy adres IP podzielony został na cztery 8-bitowe fragmenty, które przedstawiane są w postaci dziesiętnej.

Tabela 2. Przykładowy adres IP

Adres w formie 32-bitowej	10101110000100010000000000001110			
Adres w formie czterech oktetów	10101110	00001000	10000000	00001110
Adres w formie dziesiętnej	174	16	128	14

Źródło: opracowanie własne.

Tabela przedstawia przykładowy adres IP przedstawiony w formie 32-bitowej liczby binarnej (ta forma jest zrozumiała dla urządzeń

sieciowych takich jak switche) oraz jego dziesiętną reprezentację. Adres IP można również zapisać z wykorzystaniem notacji z użyciem kropek. W takim przypadku adres będzie miał postać 174.16.128.14.

Klasy adresów IP

Adres IP składa się z części identyfikującej sieć oraz części identyfikującej urządzenie podłączone do danej sieci. Klasy adresów IP zostały wprowadzone we wczesnej fazie rozwoju Internetu przez organizację IANA (Internet Assigned Numbers Authority). Trzy podstawowe klasy adresów A, B, C pozwalają podzielić sieci pod względem liczy urządzeń, które można do nich podłączyć, oraz dozwolonej liczby sieci danej klasy mogących działać w Internecie. Klasy zostały tak skonstruowane, aby można było rozpoznać, do której z nich należy dana sieć, poprzez adres IP urządzenia z tej sieci.

Tabela 3. Klasy sieci

Klasa sieci	Pierwsze bity adresu	Zasięg pierwszego oktetu	Liczba sieci	Liczba urządzeń
A	0	0–127[1]	$2^7 = 128$	$2^{24} = 16777216$
B	10	128–191	$2^{14} = 16384$	$2^{16} = 65536$
C	110	192–223	$2^{21} = 2097152$	$2^8 = 256$

Źródło: opracowanie własne.

Tabela prezentuje, w jaki sposób tworzone są adresy IP urządzeń przynależących do poszczególnych klas sieci. W klasie typu A pierwszy

[1] 127 – zarezerwowany dla celów testowych – pętla zwrotna.

oktet adresu określa adres sieci, natomiast trzy pozostałe oktety wykorzystywane są do adresowania urządzeń działających w tej sieci. Taki podział oznacza, że w całym Internecie może istnieć jedynie 128 różnych sieci klasy A, jednak każda z sieci może składać się aż z 16 milionów urządzeń. Takie założenie na początku rozwoju Internetu wydawało się sensowne. W tamtym czasie sieć składała się głównie z sieci uniwersyteckich, których liczba nie była duża, jednak posiadały one znaczącą liczbę podłączonych urządzeń. Klasa B rezerwuje dwa oktety na identyfikator sieci oraz dwa na identyfikator urządzenia. Klasa C pozwala na zaadresowanie najmniejszej liczby urządzeń – 254 (256 minus dwa zarezerwowane adresy, adres sieci i adres broadcast), jednak liczba tych sieci jest największa.

Prywatne adresy IP

Internet składa się z wielu połączonych ze sobą sieci. Stanowi publiczną, globalną platformę, umożliwiającą komunikację. Zgodnie z zasadami protokołu IP każde urządzenie w sieci powinno mieć unikalny w obrębie całej sieci adres IP. Szybkość rozwoju Internetu zaskoczyła twórców protokołu IPv4. Bardzo szybko okazało się, że 32 bity przeznaczone na zaadresowanie urządzeń to za mało. Obecnie w Internecie funkcjonuje protokół IP w wersji 4. Od dłuższego czasu trwają również prace nad wdrożeniem protokołu IP w wersji 6., który zakłada 128-bitowe adresy IP (protokół IPv6 będzie omówiony w rozdziale czwartym). Do czasu wprowadzenia protokołu IPv6 problem niewystarczającej ilości adresów IP rozwiązywany jest przez zastosowanie adresacji prywatnej. Dla każdej

z klas adresów IP istnieją adresy prywatne, które mogą być używane tylko wewnątrz konkretnych sieci, nie mogą zaś być używane w sieci globalnej. Adresy te to:

1. klasa A: 10.0.0.0 – 10.255.255.255
2. klasa B: 172.16.0.0 – 172.31.255.255
3. klasa C: 192.168.0.0 – 192.168.255.255

W sieciach prywatnych mogą być używane adresy prywatne, zgodnie z polityką firmy. Komunikacja z siecią globalną działa poprzez mechanizmy tłumaczenia adresów, mechanizm NAT (Network Adress Translation). W przypadku gdy urządzenie chce wysłać dane do sieci publicznej, mechanizm NAT tłumaczy jego adres IP z prywatnego na publiczny. W ten sposób dana organizacja może wykorzystywać dużo mniejszą liczbę publicznych adresów IP niż liczba posiadanych urządzeń sieciowych.

Protokół DHCP

Kluczową cechą urządzeń działających w sieciach IP jest posiadanie unikalnego w obrębie danej sieci adresu IP. Zanim urządzenie będzie w stanie wysyłać i odbierać komunikaty, musi mu zostać przypisany adres IP. Protokół DHCP umożliwia automatyczne przypisanie adresu IP z pewnej puli adresów do urządzenia podłączonego do sieci.

Komunikacja urządzenia z serwerem, na którym działa DHCP, odbywa się w czterech krokach:

1. Klient wysyła komunikat rozgłoszeniowy DHCP DISCOVER (z ang. poszukiwanie DHCP) w celu zlokalizowania serwera DHCP;

2. Serwer DHCP wysyła do klienta komunikat DHCP OFFER (z ang. oferta DHCP) z proponowanym adresem IP;
3. Klient wysyła rozgłoszeniowo komunikat DHCP REQUEST (z ang. żądanie DHCP) z prośbą o przyznanie zaproponowanego wcześniej adresu IP;
4. Serwer odsyła komunikat DHCP ACKNOWLEDGMENT (z ang. potwierdzenie DHCP) pozwalający klientowi na skonfigurowanie połączenia sieciowego.

Protokół DHCP działa przeważnie na scentralizowanych serwerach, które zarządzają pulą adresów o określonym zakresie. Przydzielone adresy IP przechowywane są w odpowiednich strukturach. Z adresami wiąże się również czas, po którym ulegają one przedawnieniu. Po upłynięciu tego czasu urządzenie sieciowe musi ponownie skomunikować się z serwerem DHCP, aby uzyskać nowy adres IP.

Protokół DNS

Kolejnym przykładem protokołu ułatwiającego korzystanie z zasobów sieci jest Protokół DNS (Domain Name Server). Umożliwia on przedstawianie adresów IP w postaci łatwiejszej do zapamiętania dla człowieka. Protokół DNS wykorzystywany jest do tłumaczenia tak zwanej pełnej, jednoznacznej nazwy domenowej FQDN (*fully qualified domain name*), czyli mówiąc potocznie – adresu internetowego (na przykład www.nba.com czy www.tatry.pl) na adres IP. Po wpisaniu w przeglądarce adresu strony nasz system skomunikuje się z serwerem DNS w celu uzyskania adresu IP dla danej nazwy. W odpowiedzi serwer

DNS dostarczy odpowiadający naszemu zapytaniu adres IP, który zostanie użyty do nawiązania komunikacji.

Protokoły warstwy transportu

Warstwa transportowa świadczy usługi dla warstwy aplikacji, znajduje się ona ponad warstwą sieci, w której działa protokół IP. W warstwie transportu stosu protokołów TCP/IP działają dwa podstawowe protokoły, protokół połączeniowy TPC oraz bezpołączeniowy UDP. Z punktu widzenia tych dwóch protokołów możemy wskazać główne zadania warstwy transportowej:

1. Multipleksowanie sesji – oznacza to, że maszyna posiadająca wiele różnych aplikacji może używać jednego przypisanego do niej adresu IP przy komunikacji z innymi urządzeniami.
2. Segmentacja danych – podział danych na segmenty, które później są dzielone na pakiety wysyłane do urządzenia docelowego.
3. Kontrola przepływu – mechanizm kontrolujący prędkość przesyłania danych, zapewniający, że dane nie będą przesyłane do adresata szybciej, niż mógłby on je odebrać.
4. Zapewnienie niezawodności połączenia – mechanizm umożliwiający kontrolę nad tym, czy dane zostały poprawnie wysłane i odebrane.

Pierwsze dwa punkty są wykonywane zarówno przez protokół TCP, jak i UDP. Ze względu na to, iż protokół UDP nie wymaga nawiązania połączenia z urządzeniem docelowym, nie musi zapewniać kontroli przepływu i niezawodności połączenia.

Tabela 4. Protokoły TCP i UDP

	Niezawodny	Best-effort
Protokół	TCP	UDP
Typ połączenia	połączeniowy	bezpołączeniowy
Numerowanie pakietów	tak	nie
Zastosowania	e-mail pobieranie plików udostępnianie plików	streaming video rozmowy głosowe

Źródło: opracowanie własne.

Protokół TPC zapewnia niezawodne połączenie, co oznacza, że na przykład w przypadku wykrycia jakichś błędów transmisja danych zostaje powtórzona. Transmisja danych w protokole UDP nie wymaga sprawdzania poprawności danych i nawiązywania połączenia, dzięki temu jest szybsza i lepiej sprawdza się w usługach sieciowych takich jak rozmowy wideo. Określenie „best-effort" oznacza, że po wysłaniu pakietów do odbiorcy nadawca nie wykonuje żadnych dodatkowych czynności mających na celu potwierdzenie tego, czy dane pakiety bez problemów dotarły do adresata.

Protokoły warstwy aplikacji

Zadaniem warstwy transportu jest, podobnie jak w przypadku niższych warstw, świadczenie usług dla warstwy wyższej. W tym wypadku jest to warstwa aplikacji. Warstwa transportu umożliwia protokołom warstwy aplikacji korzystanie z dwóch rodzajów protokołów, połączeniowych lub bezpołączeniowych, niejako ukrywając przed nimi

wszystkie mechanizmy wykorzystywane w niższych warstwach służące do transmisji danych. Można powiedzieć, że działanie niższych warstw stosu protokołów TCP/IP jest przezroczyste dla warstwy aplikacji. W warstwie aplikacji działają takie usługi jak:

1. transfer plików – FTP, TFTP;
2. poczta elektroniczna – SMTP, POP3;
3. zdalne logowanie – telnet, login;
4. zarządzanie siecią – SNMP;
5. zarządzanie nazwami – DNS;
6. aplikacje internetowe – http.

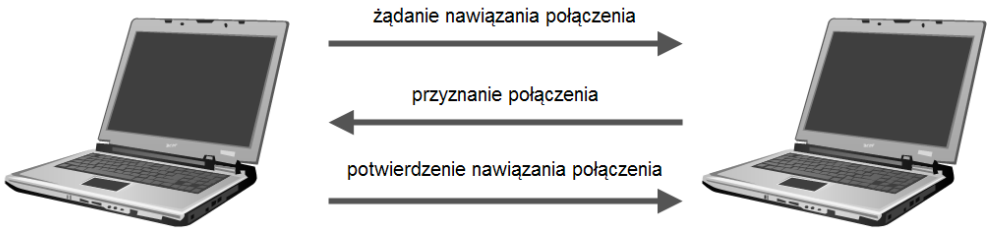
Protokoły warstwy transportowej wymagają dodatkowych informacji, aby móc określić, dla jakiej usługi warstwy aplikacji przeznaczone są otrzymane segmenty. W tym celu wprowadzone zostały numery portów umożliwiające identyfikację aplikacji. Przykładowo port 21 odpowiada usłudze FTP, numer 23 usłudze telnet, a port 80 jest zarezerwowany dla usług sieciowych HTTP. Numery portów mogą być liczbami z zakresu od 1 do 65535. Numery portów od 1024 do 49151 są zastrzeżone dla konkretnych aplikacji, a przydziela je organizacja IANA. Numery portów z zakresu 49152 do 65535 mogą być dynamicznie przydzielane w zależności od potrzeb danej aplikacji.

Nawiązywanie połączenia w sieciach TCP/IP

W przypadku protokołu połączeniowego TCP jest odpowiedzialne za nawiązanie połączenia. Proces ten ma na celu utworzenie sesji pomiędzy dwoma urządzeniami w sieci. Dzięki temu urządzenia mogą komunikować się ze sobą bez konieczności wykonywania czynności odpo-

wiednich dla niższych warstw modelu TCP/IP. Oznacza to, że urządzenia do komunikacji używają jedynie swoich identyfikatorów. Połączenie musi być nawiązane, utrzymane i skasowane po zakończeniu komunikacji. Nad prawidłowym przebiegiem tych czynności czuwa właśnie protokół TCP. Nawiązanie połączenia przybiera formę tak zwanego trójstronnego uścisku dłoni. Jest to proces synchronizacji pomiędzy dwoma urządzaniami przebiegający w trzech krokach. Mechanizm trójstronnego uścisku dłoni wykorzystuje specjalnie przygotowane pakiety TCP.

Rysunek 5. Ilustracja mechanizmu trójstronnego uścisku dłoni



Źródło: opracowanie własne.

W pierwszym kroku nawiązywania połączenia nadawca wysyła do adresata pakiet z ustawioną flagą SYN oznaczający chęć nawiązania połączenia. Adresat po otrzymaniu i przetworzeniu pakietu odsyła do nadawcy pakiet zawierający flagę ACK oraz SYN. Pakiet ten jest jednoznaczny z potwierdzeniem połączenia. Ostatnim krokiem jest wysłanie przez nadawcę7. pakietu z flagą ACK. Po wykonaniu tych czynności protokół TCP zyskuje pewność, że możliwa jest prawidłowa komunikacja przebiegająca w obu kierunkach.

Kontrola przepływu

Protokół TCP używa mechanizmu kontroli przepływu do wykrywania ewentualnych błędów mogących wynikać z zakłóceń w sieci lub z różnej szybkości przetwarzania informacji przez interfejsy sieciowe komunikujących się urządzeń. Mechanizm ten posługuje się specjalnie przygotowanymi pakietami ACK (skrót pochodzi od ang. *acknowledgment* oznaczającego potwierdzenie). Po każdym wysłanym pakiecie odbiorca musi wysłać do nadawcy pakiet z ustawioną flagą ACK, w przeciwnym razie komunikacja nie będzie mogła być prawidłowo kontynuowana. Oczywistą wadą tego rozwiązania jest konieczność przesyłania potwierdzenia po każdym pakiecie. W celu zoptymalizowania mechanizmu kontroli przepływu wprowadzony został mechanizm okienkowania (ang. *windowing*). Potwierdzenia ACK przesyłane są po otrzymaniu określonej ilości informacji. Mechanizm ten pozwala również na zakomunikowanie nadawcy, że bufor przechowujący odebrane, ale nie przetworzone dane przepełnia się. Gdy nadawca informacji otrzyma zamiast pakietu ACK pakiet, w którym odbiorca określa wielkość okna jako zero, jest to sygnał dla nadawcy, aby wstrzymał nadawanie informacji i poczekał na otrzymanie sygnału o ponownej gotowości odbiorcy. W mechanizmie okienkowania wielkość okna określana przez odbiorcę oznacza ilość przesłanych pakietów, po otrzymaniu których należy wysłać pakiet z flagą ACK.

Podstawowe zagadnienia związane z routingiem w protokole IP

Sieci mogą być od siebie oddalone pod względem położenia geograficznego. W innych przypadkach duże sieci dzielone są na podsieci w celu ułatwienia zarządzania nimi. W celu połączenia wielu sieci niezbędne są urządzenia trzeciej warstwy. Zapewniają one bowiem możliwość wyznaczania trasy pomiędzy punktami w różnych sieciach. Proces wyznaczania trasy w sieci nazywa się routingiem od ang. słowa *route* oznaczającego trasę. Urządzeniem sieciowym spełniającym tę funkcję jest router. Aby zapewnić możliwość lokalizowania sieci oraz urządzeń, każdy system posiada własną adresację trzeciej warstwy. Dla przykładu:

1. model OSI – adresacja NSAP,
2. model TCP/IP – adresacja IP.

W warstwie drugiej modeli OSI lub TCP do adresowania urządzeń wykorzystuje się ich adresy fizyczne. Za tłumaczenie adresów IP na adresy fizyczne odpowiedzialny jest protokół ARP (Adress Resolution Protocol), który na podstawie tablicy ARP przechowującej pary odpowiadających sobie adresów IP i MAC dokonuje tłumaczenia adresów. Tablica ARP powinna mieć możliwość dynamicznego tworzenia nowych wpisów, tak aby system mógł prawidłowo reagować na zmiany w otoczeniu sieciowym. Zależnie od systemu wpisy w tabeli mogą ulegać przedawnieniu po określonym czasie, w związku z tym wpisy w tabeli ARP muszą być cyklicznie odnawiane.

Sieci LAN i WAN

Koncepcja sieci lokalnej

Lokalna sieć komputerowa to grupa urządzeń połączonych ze sobą i znajdujących się w relatywnie bliskiej odległości od siebie. Podstawowe trzy cechy, które rozróżniają sieci LAN od innych typów sieci, to:

1. fizyczna bliskość urządzeń,
2. duża przepustowość,
3. brak konieczności korzystania z usług firm telekomunikacyjnych.

Na sieć LAN składają się urządzenia sieciowe (huby, switche, routery), urządzenia końcowe (komputery, telefony, drukarki), okablowanie, karty sieciowe urządzeń oraz protokoły takie jak protokół IP, Ethernet, ARP, DHCP itd. Sieci LAN spełniają wszystkie podstawowe zadania sieci związane z dzieleniem zasobów, umożliwieniem korzystania z aplikacji sieciowych oraz udostępnieniem usług takich jak na przykład wideokonferencje. Obecnie ogromna większość sieci LAN spełnia dodatkową funkcję, czyli umożliwia komunikację z siecią publiczną poprzez urządzenia określane jako bramki internetowe.

Wielkość sieci LAN może być zróżnicowana. Siecią LAN może być mała sieć biurowa. Takie sieci określane są skrótem SOHO (ang. Small Office / Home Office – małe biuro / domowe biuro). Sieci typu LAN to również duże sieci korporacyjne spinające ze sobą setki lub tysiące urządzeń sieciowych.

Sama koncepcja sieci LAN nie określa, jaka technologia powinna być wykorzystana do komunikacji pomiędzy urządzeniami w sieci lokalnej. Istnieje przynajmniej kilka technologii, które mogą być zastosowane w sieciach LAN. W przeszłości popularne były technologie takie jak Token ring czy FDDI. Obecnie najpopularniejszą i najbardziej rozpowszechnioną technologią działającą w dwóch pierwszych warstwach systemu OSI jest technologia Ethernet.

Technologia Ethernet

Rozwój technologii Ethernet został zapoczątkowany w latach 70. przez konsorcjum trzech firm: DEC, Intel oraz Xerox. Grupa robocza wydzielona przez te firmy opracowała standard sieci opartych o technologię Ethernet, który został oddany do powszechnego użytku w połowie lat 80. Opracowane standardy noszą nazwy Ethernet 802.3 oraz 802.2.

Standard Ethernet określa rodzaje okablowania i sygnałów wykorzystywane w transmisji danych definiowanej w warstwach fizycznej i łącza danych modelu OSI.

Poza wprowadzeniem adresowania urządzeń w sieci za pomocą ich adresów MAC technologia Ethernet wprowadza również mechanizm dostępu do łącza. Nazywa się on CSMS/CD (ang. Carrier Sense Multiple Access / with Collision Detection – wykrywanie łącza równoprawny dostęp / z wykrywaniem kolizji). Mechanizm ten umożliwia jednoczesne nadawanie dostępu do sieci wszystkim urządzeniom w dowolnym momencie. Wszystkie urządzenia mają takie samo prawo do nadawania danych. Przed rozpoczęciem transmisji nadawca sprawdza, czy łącze jest

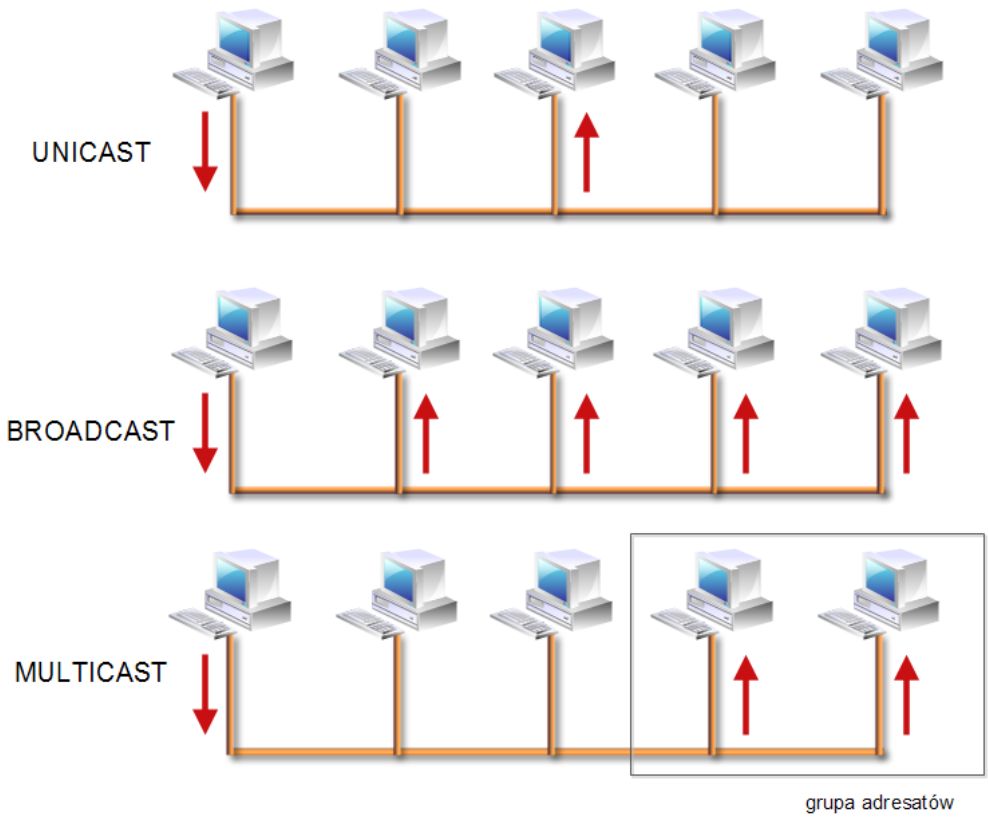
dostępne, czy w danym momencie żadne inne urządzenie nie rozpoczęło transmisji. Istnieje jednak prawdopodobieństwo, że dwa urządzenia podłączone do sieci rozpoczną transmisję w tym samym czasie. Takie zdarzenie skutkuje kolizją. Mechanizm skanowania stanu łącza pozwala również wykryć kolizję. W takim przypadku transmisja zostaje przerwana przez oba urządzania i ponownie wznowiona po upływie pewnego losowego czasu.

Protokół CSMA/CD posiada pewne wady, z których istnienia powinna zdawać sobie sprawę każda osoba projektująca sieci LAN. Jak wspomniano w pierwszym rozdziale, domeny kolizyjne to obszary sieci, w których urządzenia komunikują się ze sobą, współdzieląc to samo medium transmisyjne. Oznacza to, że posiadanie zbyt wielu urządzeń połączonych ze sobą np. za pomocą huba zwiększa prawdopodobieństwo wystąpienia kolizji, w znacznym stopniu ograniczając wydajność sieci. Innym zagrożeniem dla poprawnego działania CSMA/CD mogą być nieprawidłowo działające interfejsy lub oprogramowanie, powodujące wysyłanie do sieci uszkodzonych ramek, które mogą uniemożliwić prawidłowe działanie wszystkich urządzeń w domenie kolizyjnej.

Rodzaje komunikacji wewnątrz sieci LAN

W sieciach LAN możliwe są trzy rodzaje transmisji pomiędzy nadawcą a odbiorcą lub odbiorcami. Transmisja typu unicast, broadcast i multicast.

Rysunek 6. Ilustracja trzech typów sygnałów w sieciach LAN



Źródło: opracowanie własne.

Ramki typu unicast są standardowym typem ramek wykorzystywanym w komunikacji pomiędzy dwoma urządzeniami w sieci. Do identyfikacji adresata wykorzystywany jest adres MAC interfejsu sieciowego urządzenia. Istnieją jednak przypadki, gdy urządzenie musi wysłać wiadomości do wszystkich urządzeń w sieci. Dzieje się tak na przykład przy omawianym wcześniej protokole ARP, który pośredniczy w komunikacji między warstwą sieci a warstwą transportu.

Komunikacja typu multicast do zaadresowania ramki używa zamiast adresu pojedynczego odbiorcy adresu grupy odbiorców. Urządzenia mogą dynamicznie dołączać się do danej grupy adresatów i ją opuszczać.

Składniki adresu MAC

Adresowanie w sieciach Ethernet realizowane jest za pomocą adresów MAC (ang. *Media Access Control* – kontrola dostępu do łącza). W technologii Ethernet adres MAC jest jednocześnie adresem sprzętowym interfejsu sieciowego urządzenia.

Struktura adresu MAC wygląda następująco:

Tabela 5. Struktura adresu MAC

1 bit	1 bit	22 bity	24 bity
Broadcast	lokalny	OUI	określane przez producenta

Źródło: opracowanie własne.

Adres MAC składa się w sumie z 48 bitów podzielonych na cztery sekcje. Pierwsze dwie sekcje mają specjalne znaczenie, każda składa się z jednego bitu. Bit broadcast określa, czy dany adres jest adresem rozgłoszeniowym czy multicastowym. Bit lokal oznacza, czy adres MAC może być zmieniony, czy został ustawiony w danym urządzeniu na stałe. Sekcja OUI (*Organizationally Unique Identifier*) oznacza identyfikator unikalny w skali organizacji. Ostatnia 24-bitowa część adresu MAC jest natomiast ustawiana przez producenta. Producent musi wystąpić do organizacji przydzielającej adresy fizyczne. Po otrzyma-

niu unikalnego adresu producent umieszcza go na stałe w sprzęcie sieciowym. Adres MAC posiadają interfejsy sieciowe oraz porty routerów i switchy warstw wyższych.

Sieci WAN

Sieci WAN powstały po to, aby znieść ograniczenia geograficzne sieci LAN i umożliwić łączenie sieci znajdujących się w znacznej odległości od siebie. Podobnie jak w przypadku sieci LAN, możemy przedstawić trzy podstawowe charakterystyki sieci WAN, które odróżniają je od sieci lokalnych.

1. sieć WAN łączy urządzenia oddalone od siebie pod względem geograficznym;
2. sieci WAN są zarządzane i udostępniane przez dostawców usług sieciowych takich jak firmy telekomunikacyjne;
3. sieci WAN zapewniają zwykle mniejsze przepustowości niż sieci LAN.

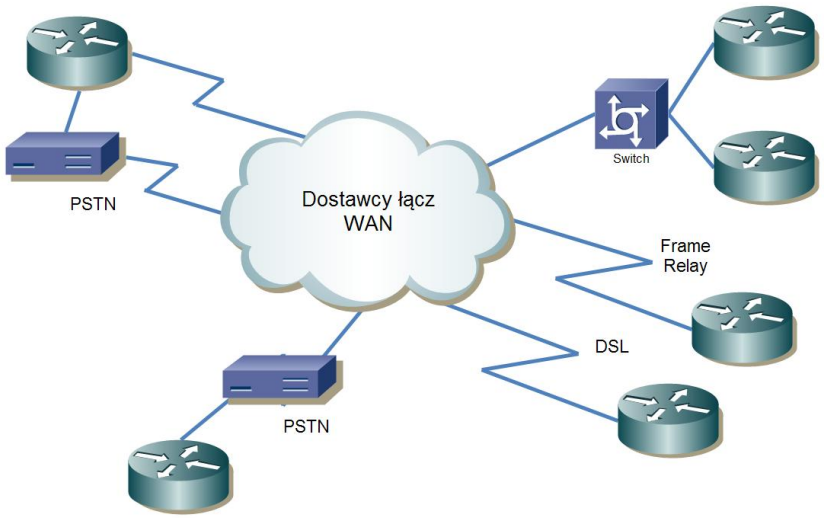
Internet może być postrzegany jako sieć WAN łącząca ze sobą poszczególne sieci. Należy jednak pamiętać, że Internet jest siecią publiczną, natomiast nie wszystkie sieci WAN są dostępne z zewnątrz. Niektóre organizacje czy firmy mogą posiadać własne pełnoprawne sieci WAN, które nie są publiczne.

W odróżnieniu od sieci LAN, które w całości należą do danej organizacji, sieci WAN działają w oparciu o usługi świadczone przez zewnętrzne firmy, które zajmują się na przykład dzierżawieniem łączy po-

między konkretnymi lokalizacjami czy udostępnianiem usług takich jak wideokonferencje lub telefonia VoIP.

Współcześnie ważnym zadaniem sieci LAN jest zapewnienie połączenia z siecią WAN. Z punktu widzenia modelu OSI komunikacja w sieci WAN odbywa się w dwóch najniższych warstwach, czyli w warstwie fizycznej i warstwie łącza danych. W przypadku sieci WAN w warstwie fizycznej mamy do czynienia z określeniem elektrycznych, mechanicznych oraz funkcjonalnych połączeń. W warstwie łącza danych pracują protokoły komunikacyjne takie jak Frame Relay, HDLC, ATM. Protokoły te zapewniają enkapsulację podczas przesyłania danych po łączach seryjnych.

Rysunek 7. Połączenie kilku sieci LAN z siecią WAN



Źródło: opracowanie własne.

Rysunek 7. przedstawia punkty graniczne połączenia sieci LAN z siecią WAN. Na granicy połączeń między sieciami musi dojść do tłumaczenia sygnałów do formy rozpoznawalnej przez sieci. Istnieje wiele rodzajów technologii służących do łączenia sieci.

Spośród urządzeń realizujących to zadanie można wymienić:

1. modemy,
2. urządzenia DSU/CSU,
3. switche ATM,
4. switche Frame Relay.

Na styku sieci LAN i WAN znajdują się przeważnie dwa urządzenia (lub jedno urządzenie pełniące dwie funkcje) określane jako DTE (*Data Terminal Equipment*) oraz DCE (*Data circuit-terminating equipment*). DTE to urządzenie końcowe działające po stronie klienta i stanowiące punkt połączenia z siecią WAN (zwykle jest to router wyposażony w odpowiednie porty). Natomiast określenie DCE odnosi się do urządzenia końcowego z punktu widzenia dostawcy usług sieciowych (przeważnie jest to modem realizujący funkcje tłumaczenia sygnałów). Najczęściej to urządzenie DCE stanowi punkt rozdzielający strefy odpowiedzialności providera i administratora sieci LAN.

Usługi oferowane przez firmy zajmujące się dostarczaniem połączeń z sieciami publicznymi mają różne charakterystyki. Przy wyborze należy zdawać sobie sprawę z wad i zalet konkretnych rozwiązań. Podstawowe dwie kategorie usług to rozwiązania dedykowane i komutowane. W pierwszym przypadku klient wynajmuje od firmy telekomunikacyjnej fizyczne połączenie pomiędzy dwoma lokacjami. Rozwiązanie to jest najdroższe spośród wszystkich dostępnych. Usługi komutowane korzystają z już istniejącej infrastruktury, dzięki czemu są rozwiązaniami tańszymi, przeważnie jednak zapewniają mniejszą przepustowość i słabszą dostępność niż łącza dedykowane.

Usługi komutowane dzielimy na:

1. komutację łącza (PSTN),
2. komutację pakietów (Frame Relay, DSL),
3. komutację komórek (ATM).

Połączenia z sieciami WAN wykorzystujące komutację pakietów są typowo stosowane do łączenia z Internetem, podczas gdy połączenia oparte o ATM są lepiej przystosowane do realizacji usług związanych z przekazywaniem głosu i obrazu.

Protokół IPv6

Protokół IP w wersji 6. powstał w celu wyeliminowania problemów związanych z niewystarczającą liczbą adresów IP w czwartej, aktualnie obowiązującej wersji tego protokołu. Protokół IPv4 pozwala na zaadresowanie około czterech miliardów urządzeń (2^{32} = 4294967296). Liczba ta nawet na dzień dzisiejszy wydaje się zupełnie wystarczająca, jednak bardzo duża część adresów z tej puli jest wyłączona z użytku (na przykład poprzez wprowadzenie klas adresów IP). W rzeczywistości dostępne jest jedynie około 250 milionów publicznych adresów IP, które można przypisać do urządzeń sieciowych. Biorąc pod uwagę, że obecnie ponad 10 procent populacji ludzkiej (około 700 milionów ludzi) posiada stały dostęp do Internetu, jasno widać, jak bardzo niewystarczający jest zasób adresów IP. Mechanizmy takie jak adresowanie prywatne, NAT czy VLSM pozwalają na przedłużenie życia protokołu IP, jednak nie stanowią one prawdziwego rozwiązania problemu, a jedynie jego obejście.

Protokół IP w wersji 6. stanowi rozwiązanie kwestii niewystarczającej liczby adresów oraz innych problemów, których nie mogli przewidzieć twórcy protokołu IPv4, rozpoczynając pracę w latach 80. Protokół IP używa 128-bitowych adresów, co pozwala na zaadresowanie ogromnej liczby urządzeń (2^{128} = 3.4 x 10^{38}). Poza tym protokół IPv6 zawiera wiele rozwiązań, które powstawały w celu ulepszenia działania protokołu IPv4. Jednym z takich nowych standardów jest IPSec – mechanizm, który zapewnia bezpieczeństwo komunikacji pomiędzy urządzeniami w sieci. Nowa wersja protokołu IP wprowadza również nowe rodzaje komunikacji, rezygnując z komunikatów typu broadcast, zastępując je komunikacją multicast. Elimunuje w ten sposób problemy związane z ograniczaniem wydajności sieci poprzez tak zwane burze sygnałów broadcastowych. IPv6 zapowiada nową jakość, jednak ze względu na duże zmiany oraz rozległość obecnie działającego systemu jego wprowadzenie będzie wymagać dużo czasu.

Reprezentacja adresu IP

Ze względu na fakt, iż adres IP w wersji 6. składa się z cztery razy większej liczby bitów od swojego poprzednika, reprezentacja tego adresu jest bardziej skomplikowana.

Postać przykładowego adresu IP prezentujemy w poniższej tabeli.

Tabela 6. Przykładowy adres IP

2001:0bd8:3c4d	:0012:	0000:0000:1234:56ab
prefiks globalny	podsieć	Id interfejsu

Źródło: opracowanie własne.

Adres składa się z czterocyfrowych sekwencji liczb oddzielonych dwukropkami. Liczby zapisane są w postaci szesnastkowej, podobnie jak w przypadku adresów MAC. Notacja adresów w protokole IPv6 zakłada pewne uproszczenia w zapisie.

Umieszczony w tabeli adres można skrócić do postaci:

2001:bd8:3c4d:12:0:0:1234:56ab

lub

2001:bd8:3c4d:12::1234:56ab

W zapisach takich usuwane są bloki zer oraz zera umieszczone z przodu oktetów. Pozwala to na skrócenie długiego adresu do formy bardziej czytelnej.

Rodzaje adresów IPv6

W protokole IPv6 wyróżniamy sześć rodzajów adresów (w protokole IPv4 występują trzy typy adresów: unicast, broadcast, multicast). Typy adresów przedstawionych w protokole IPv6 pozwalają w bardziej efektywny sposób realizować zadania związane z komunikacją w sieci.

Typy adresów protokołu IPv6 to:

1. Unicast – pakiety posiadające adres typu unicast są dostarczone do pojedynczego urządzenia. W niektórych przypadkach kilka interfejsów może posiadać ten sam adres unicast.
2. Globalny adres unicast – publiczne routowalne adresy, będące odpowiednikiem publicznych adresów IPv4.

3. Adresy łączone lokalnie – stanowią odpowiednik prywatnych adresów z protokołu IPv4. Oznacza to, że nie są routowalne. Łączone lokalnie adresy mogą być wykorzystane przy konfigurowaniu tymczasowych sieci lokalnych na potrzeby konkretnych spotkań czy projektów.
4. Unikalne adresy lokalne – podobnie jak adresy łączone lokalnie, unikalne adresy lokalne są przeznaczone do użytku lokalnego (nie są routowalne), jednak są one unikalne w skali globalnej.
5. Multicast – działają na tej samej zasadzie co adresy multicast w protokole IPv4, adresy multicast są często określane jako komunikacja jeden do wielu.
6. Anycast – podobnie jak multicast adresy anycast mają wielu odbiorców, jednak pakiet dostarczony zostanie tylko do jednego z nich, a konkretnie do pierwszego osiągalnego odbiorcy, w sensie odległości routowania. Komunikację taką można określić jako komunikację jeden do jednego z wielu.

Warto w tym miejscu wspomnieć o autokonfiguracji w protokole IPv6, jest ona bowiem niezwykle przydatnym mechanizmem. Służy do automatycznego nadawania urządzeniom działającym w sieci lokalnych i globalnych adresów IP. Adres przydzielony do urządzenia składa się z dwóch części. Pierwsza z nich uzyskiwana jest na podstawie informacji z routera o adresie sieci, w której pracuje dane urządzenie. Kolejna część adresu tworzona jest na podstawie adresu fizycznego MAC.

Wdrożenie protokołu IPv6

Wdrożenie protokołu IPv6 zostało zapoczątkowane w 1999 roku poprzez powołanie globalnego forum IPv6. Jednostka ta ma za zadanie koordynować globalne działania związane z wdrożeniem protokołu, nadzoruje również działanie lokalnych grup w obrębie danych krajów.

Według oficjalnych danych IANA, czyli organizacji zajmującej się przydzielaniem adresów IP, oficjalne wyczerpanie się puli adresów protokołu IP w wersji 4. miało miejsce w lutym 2011 roku. Protokół IP w wersji 6. osiągnął swoją pełną funkcjonalność w roku 2008. Pierwszym krokiem milowym dla popularyzacji protokołu IPv6 były igrzyska olimpijskie organizowane w 2008 roku w Pekinie, była to bowiem pierwsza impreza światowej rangi, którą można było śledzić za pomocą serwisu dostępnego dzięki IPv6 (http://ipv6.beijing2008.cn/en). W 2009 roku Google uruchomiło usługę Google Services, a od 2011 roku przez stowarzyszenie Internet Society organizowane są oficjalne testy funkcjonowania protokołu IPv6.

Z pewnością upłynie jeszcze wiele czasu, zanim protokół IPv6 stanie się obowiązującym standardem, należy jednak zdawać sobie sprawę ze zmian, które mają miejsce na naszych oczach.

Podsumowanie

Rozwój sieci komputerowych postępuje niezwykle szybko, zwłaszcza w ostatnich dwóch dekadach. Dzięki dążeniu do tego, aby coraz więcej urządzeń mogło się ze sobą komunikować, możemy obserwować powstawanie i rozszerzanie się fenomenów takich jak globalna sieć Internet. Internet zmienił naszą rzeczywistość, przybliżając do siebie ludzi w równie przełomowy sposób jak położenie w XIX wieku na dnie Atlantyku kabla telegraficznego łączącego Amerykę Północną z Europą. Obecnie większość nowych systemów komputerowych nie może funkcjonować bez podłączenia do Internetu. Postęp w technologiach sieciowych następuje w każdym aspekcie. Od coraz nowszych rozwiązań technologicznych związanych z mediami transmisyjnymi i urządzeniami sieciowymi, poprzez coraz nowocześniejsze protokoły sieciowe, aż po innowacyjne aplikacje.

Obecnie mamy do czynienia z sieciami komputerowymi praktycznie w każdym aspekcie życia. Telefony komórkowe komunikują się z komputerami pokładowymi w samochodach za pomocą protokołu bluetooth, inteligentne domy spinają wszystkie urządzenia za pomocą sieci, przeważnie bezprzewodowej, z centralnym komputerem sterującym. Firmy takie jak Google czy Apple, który pod marką iCloud promuje swoje rozwiązania obliczeń w chmurze, ściśle wiążą przyszłość swojej działalności z coraz większą integracją z siecią. Przyszłość technologii informatycznych jest nierozerwalnie związana z postępem w dziedzinie sieci komputerowych.

Bibliografia

1. C. Hunt, *TCP/IP network administration*.
2. T. Lammle, *CCNA Cisco Certified Network Associate Study Guide*.
3. W. Odom, *Computer networking first-step*.
4. A.S. Tanenbaum, *Computer networks*.