

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 dydaktyczne dla trenerek i trenerów
prowadzących warsztaty



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI



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:

Michał Dwużnik, Bartłomiej Konarczak

Korekta:

Katarzyna Goszczyńska-Jurgielaniec

Skład:

Emilia Zgiriska

Okladka:

Katarzyna Banacińska

ISBN 978-83-63120-04-7

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.....	5
Współdzielenie zasobów w sieci.....	8
Obliczenia dokonywane w chmurze	11
Rodzaje topologii sieciowych	12
Domeny rozgłoszeniowe i domeny kolizyjne	14
Warstwowy model sieci OSI	16
Pytania testowe.....	18
Stos protokołów TCP/IP.....	19
Charakterystyka protokołu IP	20
Struktura adresu IP	21
Klasy adresów IP	23
Prywatne adresy IP	24
Protokół DHCP	25
Protokół DNS	26
Sieci LAN i WAN.....	32
Koncepcja sieci lokalnej.....	32
Technologia Ethernet.....	32
Rodzaje komunikacji wewnątrz sieci LAN.....	33
Składniki adresu MAC	36

Sieci WAN	36
Pytania testowe.....	38
Protokół IPv6.....	40
Reprezentacja adresu IP.....	41
Wdrożenie protokołu IPv6	43
Pytania testowe.....	45
Podsumowanie	46
Odpowiedzi do pytań testowych	47
Bibliografia.....	48

Wstęp

Prezentowane materiały dydaktyczne dla trenerów 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 jest adresowany do nauczycieli przedmiotów zawodowych oraz instruktorów praktycznej nauki zawodu kształcących na potrzeby sektora informatycznego i telekomunikacyjnego.

Projektodawca – firma Tylda Sp. z o.o. – 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.

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

Projektodawca – firma Tylda Sp. z o.o. – 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 za-

awansowanych 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. W materiałach zaprezentowane są podstawowe topologie sieci oraz modele stosów protokołów sieciowych modelu OSI oraz TCP/IP.

W dalszej części przedstawione zostają protokoły sieciowe IP, TCP oraz UDP. Są to podstawowe protokoły, na podstawie których opiera się zdecydowana większość współczesnej komunikacji sieciowej, w tym komunikacja w Internecie.

Kolejna część materiałów zawiera omówienie zasad, na których opierają się sieci lokalne LAN oraz sieci rozległe WAN. W przypadku sieci lokalnych uwaga koncentruje się na najpopularniejszej obecnie technologii Ethernet. W przypadku sieci WAN przybliżone zostały różne technologie, wykorzystywane przy łączeniu sieci w sieci rozległe.

Ostatnia część poświęcona jest protokołowi IP w wersji 6., który ma zastąpić obecnie funkcjonujący protokół IP w wersji 4. Rozdział porusza problemy związane z używanym obecnie protokołem IPv4, między innymi problem kończącej się puli publicznych adresów IP.

Prezentowane materiały zawierają wyszczególnione cele dydaktyczne. W każdym rozdziale nacisk położony jest na zrozumienie poszczególnych mechanizmów sieciowych, a nie na szczegóły techniczne implementacji konkretnych rozwiązań.

Materiały zawierają ćwiczenia praktyczne. Do wykonania niektórych z nich niezbędne będą komputery działające pod kontrolą systemu operacyjnego MS Windows 98 (lub nowszego) i posiadające połączenie z Internetem.

Materiały dla prowadzących zawierają również otwarte pytania do uczestników. W zależności od preferencji prowadzącego mogą być one zadawane przed przedstawieniem tematyki poszczególnych zagadnień, lub po w celu sprawdzenia wiedzy.

Niektóre rozdziały zawierają pytania testowe. Odpowiedzi do nich umieszczone są na końcu opracowania.

Współdzielenie zasobów w sieci

Cele	1. przedstawienie koncepcji sieci komputerowej,
dydaktyczne:	2. przedstawienie podstawowych komponentów sieci, 3. przedstawienie graficzne sieci za pomocą diagramów, 4. przybliżenie rodzajów aplikacji korzystających z usług sieciowych.
Podstawowe wiadomości:	<p>Pojęcie sieci komputerowej istnieje w naukach informatycznych od wczesnych lat 70. Podobnie jak większość technologii, również sieci komputerowe rozwijane były na potrzeby wojska. Początkowo, kiedy wprowadzano rozwiązania informatyczne w przedsiębiorstwach prywatnych, za pierwowzór współczesnych sieci uchodziły tak zwane „sieci trampkowe” (angielskie określenie: <i>sneakers networks</i>). Polegały one na przegrywaniu informacji na nośniki danych – takie jak dyskietki – i przenoszeniu ich pomiędzy komputerami. Pomimo tego, że na pozór rozwiązanie to ma niewiele wspólnego z nowoczesnymi sieciami, to jednak realizuje ono te same cele, co współczesne sieci – umożliwia współdzielenie danych pomiędzy oddalonymi od siebie systemami komputerowymi. Obecnie funkcjonuje termin <i>sneakernet</i>, określający przenoszenie danych na wszelkiego rodzaju nośnikach, takich jak pendrive, karty pamięci czy przenośne dyski twarde.</p>

Do graficznego ilustrowania struktury sieci używa się diagramów sieciowych. Diagramy składają się z urządzeń sieciowych, połączeń oraz urządzeń końcowych. Koncentrują się one na wybranym fragmencie sieci, zaznaczając zewnętrzne połączenia w postaci chmury. Do reprezentacji urządzeń sieciowych wykorzystane zostały standardowe reprezentacje graficzne wprowadzone przez firmę CISCO. Są one powszechnie rozpoznawane i uznawane.

W diagramach występujących w opracowaniu pojawiają się następujące urządzenia:



Hub – jest urządzeniem działającym w pierwszej warstwie modelu OSI. Zasada działania jest bardzo prosta – powiela on otrzymany sygnał na wszystkie porty za wyjątkiem tego, na którym pojawił się sygnał.



Switch – urządzenie działające w drugiej warstwie modelu OSI; do jego funkcji należy filtrowanie i dostarczenie wiadomości do adresata na podstawie adresu zawartego w każdej z ramek wiadomości. Istnieją również switche, działające w wyższych warstwach modelu OSI.



Router – mechanizm działający w trzeciej warstwie modelu OSI (może być to urządzenie fizyczne lub oprogramowanie). Router odpowiada za wyznaczanie

optymalnych ścieżek komunikacji w sieci. Historycznie router był niekiedy określany jako bramka.

Pytanie Jakie aplikacje sieciowe wykorzystuje się do użytku
otwarte: domowego, a jakie do użytku biznesowego?

Obliczenia dokonywane w chmurze

Cele	1. Na czym polega <i>Cloud Computing</i> ?
dydaktyczne:	2. Co oznacza określenie <i>software as a service</i> ?
Podstawowe wiadomości:	<p>Obliczenia dokonywane w chmurze stanowią stosunkowo nowe spojrzenie na zagadnienia związane z udostępnianiem usług sieciowych. W klasycznych rozwiązaniach użytkownik kupował daną aplikację, instalował ją na komputerze i za jej pomocą korzystał z danych usług sieciowych, na przykład wspólnej pracy nad dokumentem. <i>Cloud computing</i> zakłada natomiast, że dany program żyje w sieci. Użytkownik nie musi instalować go na swoim komputerze. Wystarczy, że zaloguje się z dowolnego urządzenia na swoje konto i za pomocą zwykłej przeglądarki będzie mógł korzystać z danego programu.</p> <p>Przykładami takich aplikacji są na przykład: Gmail, Google Docs, MS Office Live, MobileMe czy choćby gry on-line uruchamiane w przeglądarce.</p>

Rodzaje topologii sieciowych

Cele dydaktyczne:

1. przedstawienie trzech podstawowych typów topologii sieciowych;
2. omówienie różnic między topologiami logicznymi a fizycznymi.

Podstawowe wiadomości: Topologia sieci komputerowej to model układu połączeń pomiędzy urządzeniami pracującymi w sieci.

Określenie topologii może odnosić się do topologii fizycznej, czyli fizycznego połączenia pomiędzy urządzeniami, natomiast topologia logiczna przedstawia przepływ sygnałów w danej sieci.

Podstawowe typy topologii fizycznych to:

1. topologia magistrali,
2. topologia pierścienia,
3. topologia gwiazdy,
4. topologia kratowa.

Pytanie otwarte 1.: Która z topologii jest najbardziej niezawodna?

Odpowiedź 1.: Najbardziej niezawodna jest tak zwana pełna topologia kratowa. W tej topologii wszystkie punkty sieci są ze sobą połączone. Oznacza to, że awaria któregośkolwiek komponentu sieci nie powoduje unieruchomienia sieci.

Pytanie otwarte 2.: Czym są i do czego wykorzystuje się terminatory?

Odpowiedź 2.: Terminatory to rezystory używane w sieciach opartych na kablu koncentrycznym o topologii magistrali.

Są one konieczne, aby wyeliminować odbicia sygnałów.

Pytanie Jakie są trzy podstawowe typy skrętek UTP?

otwarte 3.:

Odpowiedź 3.: Najczęściej stosowanymi rodzajami kabli w sieciach LAN są: kabel prosty (*straight-through*), kabel krosowy (*cross-over*) oraz kabel konsolowy.

Pytanie Jakim rodzajem kabla należy podłączyć dwa komputery

otwarte 4.: ze sobą?

Odpowiedź 4.: Do połączenia hostów między sobą stosujemy kabel krosowy.

Pytanie Jakim typem kabla połączyć komputer z routerem?

otwarte 5.:

Odpowiedź 5.: Do połączenia komputera z routerem stosuje się kabel prosty.

Domeny rozgłoszeniowe i domeny kolizyjne

Cel dydaktyczny: Omówienie koncepcji domen kolizyjnych i rozgłoszeniowych.

Podstawowe wiadomości: Domena kolizyjna jest to obszar sieci, w którym dochodzić może do kolizji pomiędzy sygnałami wysyłanymi z różnych urządzeń jednocześnie. Domeny kolizyjne tworzą urządzenia podłączone do tego samego przewodu, lub połączone za pomocą hubów. Domeny rozgłoszeniowe, to domeny, w których propagować się mogą sygnały typu broadcast, czyli sygnały wysyłane do wszystkich urządzeń w sieci. Domeny te tworzone są przez urządzenia podłączone za pomocą switchy.

Transmisja broadcast jest wykorzystywana między innymi w protokołach ARP, umożliwiających określenie adresu MAC (koniecznego do dostarczenia danych) na podstawie adresu IP znajdujących się w obrębie domeny rozgłoszeniowej. Nawiązanie komunikacji polega na rozesłaniu do wszystkich urządzeń specjalnie nieprzygotowanej ramki, zawierającej adres IP adresata transmisji. Prawidłowy odbiorca porównuje adres IP z ramki ze swoim adresem i odsyła do nadawcy komunikat ze swoim adresem MAC. Protokół wykonujący takie dopasowanie nosi nazwę ARP (Address Resolution Protocol) i jest powszechnie wykorzystywany w sieciach Ethernet, Token Ring i FDDI.

Pytanie Jaka jest różnica pomiędzy domeną kolizyjną a domeną
otwarte 1.: rozgłoszeniową?

Odpowiedź 1.: Domena kolizyjna to domena, w której jedno urządzenie, wysyłając sygnał do innych urządzeń znajdujących się w obrębie jej działania, wymusza dotarcie sygnału do wszystkich urządzeń. W domenie rozgłoszeniowej do urządzeń docierają komunikaty typu broadcast.

Pytanie Czym jest i na czym polega podcast?
otwarte 2.:

Odpowiedź 2.: Podcast to dziś bardzo popularna forma rozgłaszania informacji w Internecie tekstowych, dźwiękowych oraz wideo. Tekstowe podcasty to inaczej bardzo popularne kanały RSS. Podcasty audio to wszelkiego rodzaju audycje radiowe, natomiast podcasty wideo to materiały udostępniane np. w portalach informacyjnych.

Pytanie Jaką czynność jako pierwszą należy wykonać przy braku
otwarte 3.: transmisji na kablu światłowodowym?

Odpowiedź 3.: Największym wrogiem podczas montażu infrastruktury opartej na światłowodzie jest kurz. W przypadku braku sygnału na przewodzie należy przeczyścić łączenie kabla, idąc od miejsca, w którym stwierdzono brak sygnału, w górę.

Pytanie Jaka może być maksymalna długość kabla UTP kat 5e?
otwarte 4.:

Odpowiedź 4.: Kable UTP kategorii 5e potrafią prowadzić transmisję danych bez zakłóceń do długości maksymalnie 100 m.

Warstwowy model sieci OSI

Cele	1. prezentacja warstwowego modelu OSI,
dydaktyczne:	2. przedstawienie poszczególnych warstw modelu OSI.
Podstawowe wiadomości:	<p>OSI (Open Systems Interconnection) oznacza otwarty system połączeń. Standard ten został opracowany przez Międzynarodową Organizację Normalizacyjną (ISO). Model OSI jest traktowany jako wzorzec dla producentów związanych z sieciami komputerowymi. Model zakłada podział na siedem niezależnych warstw. Każda warstwa świadczy usługi dla warstw wyższych, komunikacja odbywa się tylko pomiędzy sąsiednimi warstwami. Warstwy modelu OSI:</p> <ol style="list-style-type: none">1. aplikacji – warstwa ta dostarcza usługi sieciowe za pomocą aplikacji użytkownika. Usługi te mogą być związane z pocztą elektroniczną, przesyłaniem plików czy zdalnymi połączeniami;2. prezentacji – warstwa ta sprawia, że informacje wysyłane przez jedno urządzenie sieciowe będą mogły być prawidłowo odczytane przez warstwę prezentacji urządzenia odbierającego transmitowane dane;3. sesji – warstwa zajmuje się nawiązaniem, utrzymaniem i terminacją sesji pomiędzy dwoma urządzeniami działającymi w sieci;4. transportowa – warstwa ma za zadanie segmentację danych podczas przygotowywania ich do transportu, oraz desegmentację po ich otrzymaniu;

5. sieciowa – warstwa ta odpowiedzialna jest za umożliwienie połączenia pomiędzy dwoma systemami które mogą być oddalone od siebie pod względem lokalizacji geograficznej, czyli między urządzeniami znajdującymi się w różnych sieciach LAN;
6. łącza danych – określa, w jaki sposób formatowane są dane podczas transmisji oraz jak kontrolowany jest dostęp do danego łącza;
7. fizyczna – dostarcza specyfikacje sygnałów elektrycznych, mechanicznych i procedury dotyczące nawiązania, utrzymania i dezaktywacji fizycznego łącza pomiędzy dwoma systemami.

Model OSI zakłada enkapsulację i dekapulację danych. Dane łączone są w struktury umożliwiające dostarczenie ich do adresatów.

Enkapsulacja przebiega następująco:

Dane → Segmenty → Pakiety → Ramki → Bity

Natomiast dekapulacja przebiega następująco:

Bity → Ramki → Pakiety → Segmenty → Dane

Enkapsulacja to proces dodawania kolejnych nagłóweków przez poszczególne warstwy modelu OSI podczas wysyłania danych. Enkapsulacja zapewnia właściwe formatowanie informacji podczas ich wysyłania. Dekapsulacja jest procesem odwrotnym i ma miejsce podczas odbierania informacji.

Pytania testowe

1. Segmentacja danych następuje w warstwie:
 - a) fizycznej
 - b) łącza danych
 - c) aplikacji
 - d) transportowej

1. Która warstwa systemu OSI odpowiedzialna jest za konwertowanie pakietów danych, otrzymanych z warstwy łącza danych na sygnały elektryczne?
 - a) warstwa aplikacji
 - b) warstwa sieci
 - c) warstwa fizyczna
 - d) warstwa transportowa

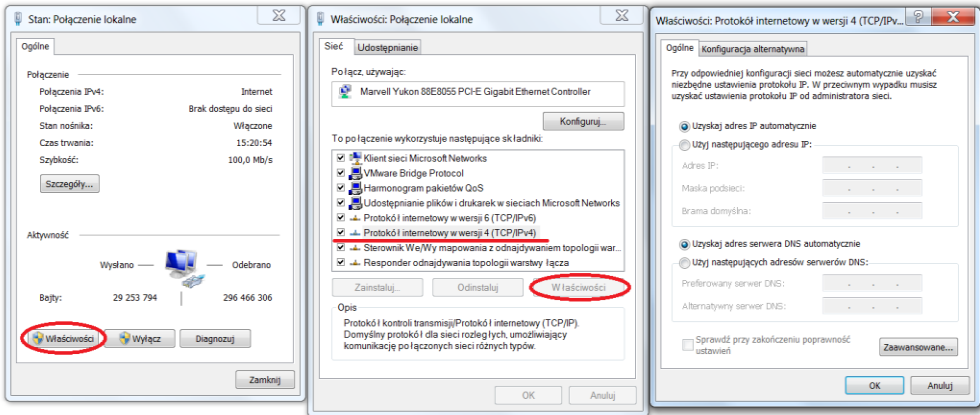
2. Która warstwa jest odpowiedzialna za rozdzielanie danych przeznaczonych dla różnych aplikacji?
 - a) warstwa sieci
 - b) warstwa sesji
 - c) warstwa aplikacji
 - d) warstwa łącza danych

3. Wskaż prawidłową kolejność enkapsulacji danych podczas komunikacji.
 - a) dane, ramka, pakiet, segment, bit
 - b) ramka, dane, pakiet, segment, bit
 - c) dane, segment, pakiet, ramka, bit
 - d) segment, pakiet, dane, ramka, bit

Stos protokołów TCP/IP

- Cele dydaktyczne:**
1. przedstawienie stosu protokołów TCP/IP,
 2. omówienie warstw modelu TCP/IP.
- Podstawowe wiadomości:**
- Określenie „protokół” w sieciach komputerowych oznacza formalny opis formatu cyfrowych sygnałów. Mówiąc inaczej – protokół to zbiór zasad odnośnie składni i semantyki komunikacji. Zadania poszczególnych protokołów mogą być realizowane programowo lub przez dedykowany sprzęt.
- Stos protokołów TCP/IP jest alternatywnym rozwiązaniem dla modelu OSI. Ze względu na fakt, że protokoły TCP oraz IP są obowiązującymi standardami komunikacji internetowej, można powiedzieć, że to właśnie stos protokołów TCP/IP jest obowiązującym praktycznym rozwiązaniem warstwowego modelu sieciowego.
- Zadanie praktyczne:**
- Sprawdzić konfigurację protokołu TCP/IP.
- Rozwiązanie:**
- W celu wykonania tego zadania należy w panelu sterowania odnaleźć zakładkę opowiedzianą za konfigurację sieci, a następnie wybrać właściwości aktywnego połączenia lokalnego. Przykładową konfigurację protokołu TCP/IP przedstawia rysunek 1.

Rysunek 1. Konfiguracja protokołu TCP/IP



Konfiguracja protokołu TCP/IP może różnić się w zależności od tego, czy dany komputer używa protokołu DHCP do ustawienia konfiguracji protokołu IP, czy posiada on adres IP przypisany ręcznie.

Charakterystyka protokołu IP

Cel dydaktyczny:

Przedstawienie cech i zastosowania protokołu IP.

Podstawowe wiadomości:

Protokół IP (Internet Protocol) jest protokołem bezpołączeniowym. W przeciwieństwie do protokołów połączeniowych, które można porównać do rozmowy telefonicznej, protokół IP nie wymaga nawiązania połączenia przed rozpoczęciem transmisji. Zasadę działania protokołów bezpołączeniowych można porównać do wysyłania listu pocztą. Adresat podaje adres odbiorcy i ufa, że przesyłka zostanie do niego dostarczona.

Struktura adresu IP

Cele	1. przedstawienie struktury adresu IP,
dydaktyczne:	2. przedstawienie notacji zapisu adresu IP.
Podstawowe wiadomości:	<p>Adres IP w wersji 4 złożony jest z 32 bitów (bit to pojedyncza wartość wyrażona w systemie dwójkowym, czyli zero lub jedynka). Adres IP składa się z dwóch części, bity znajdujące się na początku adresu oznaczają identyfikator sieci, natomiast bity znajdujące się na końcu adresu oznaczają identyfikator sieci.</p> <p>Aby poprawić czytelność adresu IP, został on podzielony na cztery części, które następnie zapisuje się w formie dziesiętnej oddzielonej kropkami. Przykładowa postać adresu IP to 192.168.55.19.</p>

Ważne jest, aby uczestnicy kursu znali zasady konwersji liczb z systemu dwójkowego do dziesiętnego i z systemu dziesiętnego do dwójkowego.

System dwójkowy jest to system, który do reprezentowania liczb używa dwóch symboli: 0 i 1. System ten jest naturalny dla wszystkich cyfrowych urządzeń elektronicznych, które rozróżniają tylko dwa stany: brak sygnału i jego obecność. Używając systemu dwójkowego można zapisać dowolną liczbę dziesiętną. Liczby w systemie dziesiętnym zapisujemy używając podstawy dziesiętnej. Oznacza to, że dana liczba może być przedstawiona w postaci sum odpowiednich potęg dziesiątki. Na przykład liczbę **1024** można zapisać jako sumę $1 \times 10^3 + 0 \times 10^2 + 2 \times 10^1 + 4 \times 10^0$.

Takie same zasady odnoszą się do systemu binarnego, z tą różnicą że podstawą potęgi jest liczba 2. Na przykład liczbę **100101** można zapisać jako sumę $1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$.

Aby uzyskać reprezentację dziesiętną liczby **100101** wystarczy zsumować ze sobą rozpisany wyżej zapis: $1 \times 32 + 0 \times 16 + 0 \times 8 + 1 \times 4 + 0 \times 2 + 1 \times 1 = 37$.

Do konwersji liczb dziesiętnych na binarne można posłużyć się prostym algorytmem. Liczbę dziesiętną dzielimy przez dwa. W przypadku, gdy liczba jest podzielna przez dwa jako wynik zapisujemy zero, w przeciwnym razie zapisujemy jedynekę. Wynik tej operacji również dzielimy przez dwa i ponownie zapisujemy wynik. Liczbę 67 przekształcić możemy w sposób następujący:

Tabela 1. Algorytm dla liczby 67

Liczba dziesiętna	Podzielnik	Reszta z dzielenia
67	2	1
33	2	1
16	2	0
8	2	0
4	2	0
2	2	0
1	2	1

Źródło: opracowanie własne.

Wynik działania zapisujemy w postaci 1000011.

Zadanie Przedstawić w formie binarnej liczby 255, 198 i 55.

praktyczne 1.:

Rozwiązanie 1.: 255 – 11111111, 198 – 11000110, 55 – 110111.

Zadanie Przedstawić w formie dziesiętnej liczby 1101101, 100001,

praktyczne 2.: 10000000.

Rozwiązanie 2.: 1101101 – 109, 100001 – 33, 10000000 – 128.

Klasy adresów IP

- Cele dydaktyczne:**
1. przybliżenie działalności organizacji IANA,
 2. przedstawienie etymologii i zastosowania klas adresów IP.

Podstawowe wiadomości: IANA (Internet Assigned Numbers Authority) – organizacja przydzielająca numery internetowe. Zajmuje się ona zarządzaniem globalną pulą adresów IP, a także domenami, znajdującymi się najwyżej w strukturze serwerów DNS.

Klasy adresów wprowadzone zostały przez IANA w początkach rozwoju Internetu.

Istnieje kilka rodzajów klas, podstawowe trzy typy klas to:

1. klasa A 1.0.0.1 do 126.255.255.254
2. klasa B 128.1.0.1 do 191.255.255.254
3. klasa C 192.0.1.1 do 223.255.254.254

W adresach IP część bitów przeznaczona jest na identyfikator sieci, a pozostała część służy do jednoznacznego identyfikowania urządzenia podłączonego do sieci (urządzenie takie często określane jest angielskim określeniem *host*). Klasy typu A rezerwują siedem pierwszych bitów (z wyjątkiem najbardziej znaczącego bitu, który jest zawsze zerem) na adres sieci, a pozostałe trzy oktety na adres urządzenia. Oznacza to, że w tej sieci może działać aż 16 milionów urządzeń. Klasa B przeznaczona dwa oktety na adres sieci i dwa na adres urządzenia. Oznacza to, że w sieciach tego typu można zaadresować 65 000 urzą-

dzeń, a w skali globalnej może istnieć 16 000 takich sieci. W sieciach klasy D mogą działać 254 urządzenia, natomiast liczba takich sieci może wynosić 2 miliony w obrębie całego Internetu.

Prywatne adresy IP

- Cele dydaktyczne:**
1. przedstawienie potrzeby stosowania adresów prywatnych;
 2. przedstawienie zasad działania mechanizmu NAT;
 3. przedstawienie zakresów adresów prywatnych.

Podstawowe wiadomości:

Prywatna adresacja w protokole IP w wersji 4. wprowadzona została z myślą o urządzeniach pracujących w sieciach nie podłączonych do sieci globalnej. Urządzenia takie (na przykład maszyny służące do automatyzacji produkcji, kasy sklepowe itd.) nie potrzebują unikalnych w skali całego Internetu adresów IP.

Prywatne adresy zostały również wprowadzone przez organizację IANA. Zakresy adresów prywatnych protokołu IPv4 przedstawia tabela 1.

Obecnie adresy prywatne wraz z mechanizmami takimi jak NAT służą do omijania problemów związanych z niewystarczającą liczbą publicznych adresów IP. Mechanizm NAT umożliwia przekazywanie informacji do urządzeń znajdujących się w danej sieci, ale nie posiadających publicznego adresu.

Tabela 2. Zakresy adresów prywatnych protokołu IPv4

Klasa	Adres początkowy	Adres końcowy	Liczba urządzeń
A	10.0.0.0	10.255.255.255	16777216
B	172.16.0.0	172.31.255.255	1048576
C	192.168.0.0	192.168.0.255	65536

Źródło: opracowanie własne.

- Zadania praktyczne:**
1. Zaproponować przestrzeń adresową, maskę dla prostej sieci lokalnej z sześcioma hostami i serwerem.
 2. Podać zakres i maksymalną liczbę hostów w sieci.
 3. Podać adres rozgłoszeniowy dla tej sieci.

- Rozwiązania:** Wybrane adresy pochodzą z kategorii C
1. Adres serwera (bramki) 192.168.1.1
Maska 255.255.255.0
Adresy hostów 192.168.1.2–192.168.1.7
 2. Maksymalny zakres hostów:
192.168.1.2–192.168.1.254
Maksymalna liczba hostów to 253
 3. Adres rozgłoszeniowy 192.168.1.255

Protokół DHCP

Cel dydaktyczny: Przedstawienie zasady działania protokołu DHCP.

Podstawowe wiadomości: Protokół DHCP (Dynamic Host Configuration Protocol) – służy do dynamicznego konfigurowania urządzeń podłączonych do sieci. Każde urządzenie w sieci IP musi

zostać odpowiednio skonfigurowane, aby mogło rozpocząć komunikację. Protokół DHCP pozwala na zarządzanie pewną pulą adresów IP. Protokół DHCP umożliwia konfigurację następujących elementów:

1. adres IP urządzenia – unikalny w obrębie sieci, należący do określonej puli adres IP;
2. domyślna brama – adres urządzenia sieciowego, które umożliwia komunikację ze światem zewnętrznym;
3. serwer DNS – adres serwera domenowego, umożliwiającego tłumaczenie mnemoniczych adresów serwisów internetowych na adresy IP.

Protokół DNS

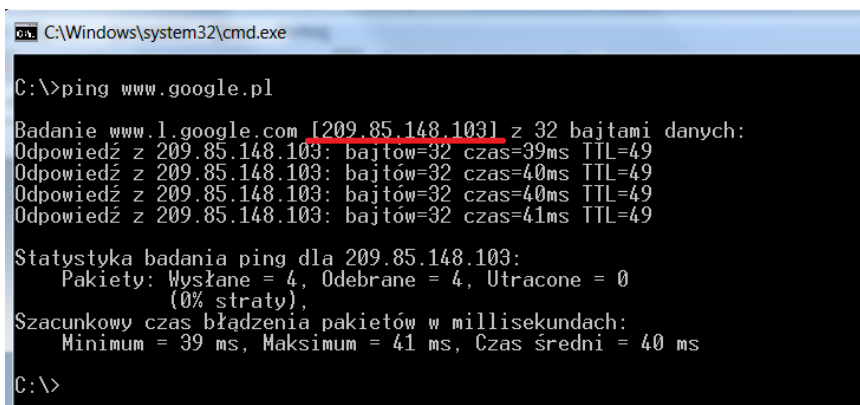
Cel dydaktyczny:	Zaprezentowanie ogólnej zasady działania protokołu DNS.
Podstawowe wiadomości:	Protokół DNS ma ogromny wkład w rozwój Internetu. Umożliwia używanie nazw domenowych zamiast adresów IP. Nazwy domenowe są nazwami jednoznacznie określającymi dany serwis w sieci. Po wpisaniu do przeglądarki danego adresu (na przykład www.pajacyk.pl) system komunikuje się z najbliższym serwerem DNS i kieruje do niego zapytanie, czy w swojej bazie danych serwer DNS posiada adres IP danego serwisu. Serwery DNS połączone są ze sobą w układzie hierarchicznym. Gdy dany serwer nie posiada informacji o tym adresie, komunikuje się z serwe-

rem znajdującym się wyżej w hierarchii. System DNS tworzy więc globalną bazę danych, zawierającą powiązania pomiędzy adresami domenowymi oraz adresami IP. Oczywiście w sieci nie mogą istnieć dwa serwisy posiadające taki sam adres IP.

Zadanie praktyczne 1.: Przy użyciu polecenia PING ustalić adres IP domeny `www.google.pl` oraz wykorzystać uzyskany adres IP do połączenia się z domeną za pomocą przeglądarki.

Rozwiązanie 1.: Usługa ping pozwala określić, czy dane urządzenie jest dostępne w sieci. Aby ją uruchomić, należy użyć konsoli system Windows (menu start → uruchom → cmd). Po wpisaniu polecenia: „ping `www.google.pl`” powinniśmy na ekranie uzyskać widok, który przedstawia rysunek 2. Oprócz informacji o czasie przesłania poszczególnych pakietów, użytkownik odnaleźć może adres IP serwisu. Adres ten należy skopiować i wkleić do paska adresowego przeglądarki.

Rysunek 2. Widok ekranu komputera po wpisaniu polecenia „ping `www.google.pl`”



```
C:\Windows\system32\cmd.exe

C:\>ping www.google.pl

Badanie www.l.google.com [209.85.148.103] z 32 bajtami danych:
Odpowiedź z 209.85.148.103: bajtów=32 czas=39ms TTL=49
Odpowiedź z 209.85.148.103: bajtów=32 czas=40ms TTL=49
Odpowiedź z 209.85.148.103: bajtów=32 czas=40ms TTL=49
Odpowiedź z 209.85.148.103: bajtów=32 czas=41ms TTL=49

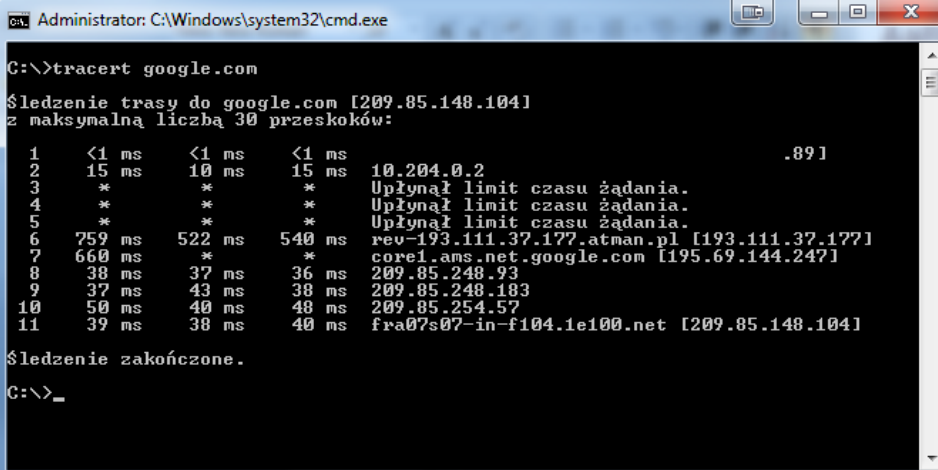
Statystyka badania ping dla 209.85.148.103:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0
            (0% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
    Minimum = 39 ms, Maksimum = 41 ms, Czas średni = 40 ms

C:\>
```

Zadanie Przy użyciu polecenia TRACERT ustalić trasę pakietów
praktyczne 2.: z komputera osobistego do serwerów Google.com.

Rozwiązanie 2: Usługa tracert pozwala określić trasę pakietów od hosta do serwera docelowego. Aby ją uruchomić, należy użyć konsoli systemu Windows (Menu start → uruchom → cmd). Po wpisaniu polecenia: „tracert www.google.com” powinniśmy na ekranie uzyskać widok, który przedstawia rys. 3.

Rysunek 3. Widok ekranu komputera po wpisaniu polecenia „tracert www.google.com”



```
Administrator: C:\Windows\system32\cmd.exe
C:\>tracert google.com

Śledzenie trasy do google.com [209.85.148.104]
z maksymalną liczbą 30 przeskoków:

  1  <1 ms    <1 ms    <1 ms    .89 ]
  2  15 ms    10 ms    15 ms    10.204.0.2
  3  *         *         *         Upłynął limit czasu żądania.
  4  *         *         *         Upłynął limit czasu żądania.
  5  *         *         *         Upłynął limit czasu żądania.
  6  759 ms   522 ms   540 ms   rev-193.111.37.177.atman.pl [193.111.37.177]
  7  660 ms   *         *         core1.ams.net.google.com [195.69.144.247]
  8  38 ms    37 ms    36 ms    209.85.248.93
  9  37 ms    43 ms    38 ms    209.85.248.183
 10  50 ms    40 ms    48 ms    209.85.254.57
 11  39 ms    38 ms    40 ms    fra07s07-in-f104.1e100.net [209.85.148.104]

Śledzenie zakończone.
C:\>_
```

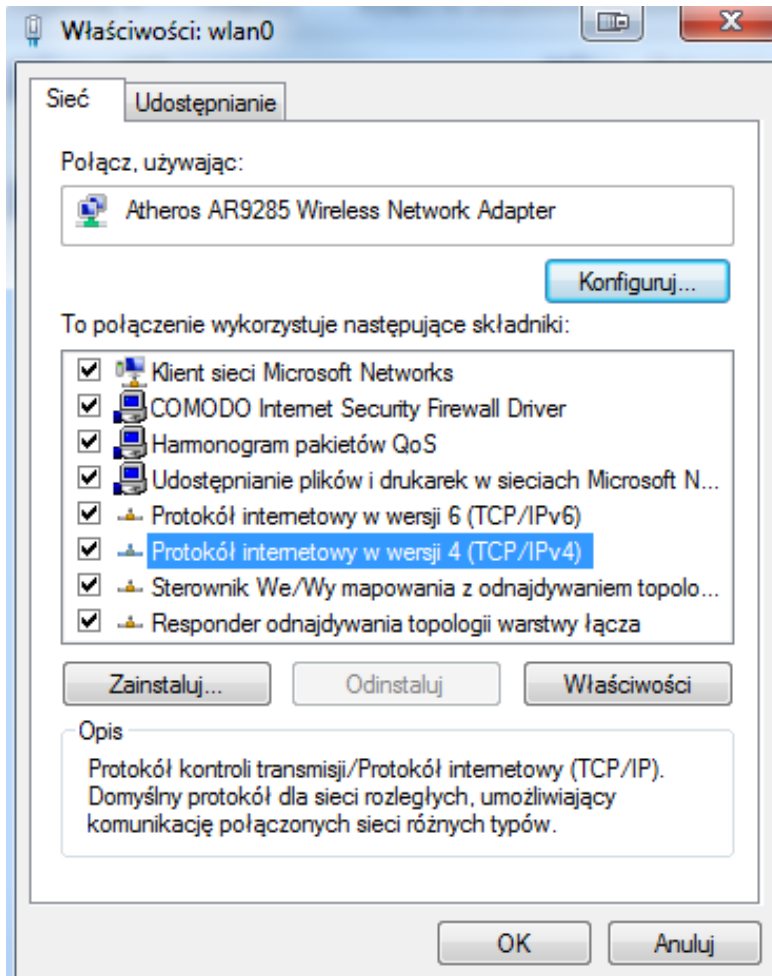
Zadanie Zmienić adresy serwerów DNS na hoście z systemem
praktyczne 3. Windows. Nowe adresy DNS:

1. podstawowy: 194.204.152.34
2. pomocniczy: 194.204.159.1

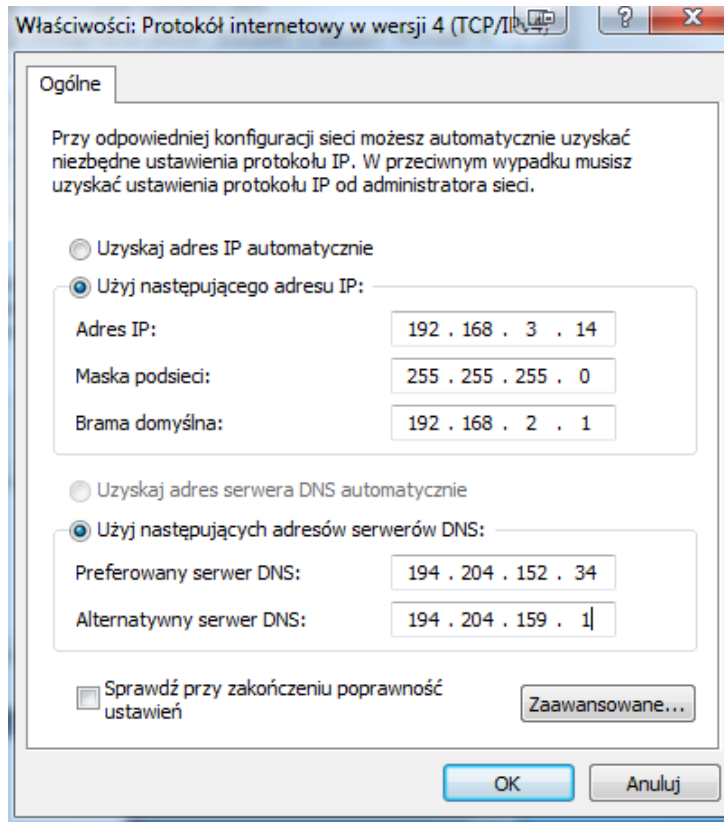
Rozwiązanie 3.: Aby dokonać zmian w adresacji sieciowej w systemie Windows, należy wyświetlić właściwości aktywnego połączenia sieciowego, co przedstawia rysunek 4.

Następnie na właściwościach protokołu IPv4 na zakładce Ogólne w sekcji DNS wpisujemy zadane adresy DNS (rysunek 5.).

Rysunek 4. Właściwości aktywnego połączenia sieciowego



Rysunek 5. Właściwościach protokołu IPv4



Zadanie praktyczne 4.: Określić adres IP, adres bramy, serwera DHCP, oraz domyślny serwer DNS komputera.

Rozwiązanie 4.: Aby uzyskać dane o adresie lokalnego komputera, można użyć polecenia „ipconfig” z parametrem „/all”. Polecenia, podobnie jak komendę „ping”, wpisujemy w konsoli systemu Windows. Po jej wpisaniu powinniśmy uzyskać na ekranie widok, który przedstawia rysunek 6. Polecenie „ipconfig” umożliwia wyświetlenie wielu istotnych informacji na temat interfejsów sieciowych danego komputera. Oczywiście komputer może mieć więcej niż jeden interfejs

sieciowy. W powyższym przykładzie komputer posiada bezprzewodową kartę sieciową oraz kartę Ethernet.

Polecenie „ipconfig” jest często używane z argumentem „renew”, umożliwiającym wymuszenie ponownego skonfigurowania interfejsów sieciowych za pomocą protokołów DHCP. Zabieg ten bywa konieczny po przeprowadzeniu jakichkolwiek zmian w konfiguracji sieci.

Rysunek 6. Widok ekranu komputera po wpisaniu polecenia „ipconfig”

```
C:\Windows\system32\cmd.exe
C:\>ipconfig /all

Konfiguracja IP systemu Windows

Nazwa hosta . . . . . : PCUSSER
Sufiks podstawowej domeny DNS . . . . . :
Typ węzła . . . . . : Hybrydowy
Routing IP włączony . . . . . : Nie
Serwer WINS Proxy włączony . . . . . : Nie

Karta bezprzewodowej sieci LAN Połączenie sieci bezprzewodowej 2:

Stan nośnika . . . . . : Nośnik odłączony
Sufiks DNS konkretnego połączenia :
Opis . . . . . : Intel(R) WiFi Link 5100 AGN
Adres fizyczny . . . . . : 00-24-D6-27-C2-E4
DHCP włączone . . . . . : Tak
Autokonfiguracja włączona . . . . . : Tak

Karta Ethernet Połączenie lokalne:

Sufiks DNS konkretnego połączenia :
Opis . . . . . : Marvell Yukon 88E8055 PCI-E Gigabit Ethernet Controller
Adres fizyczny . . . . . : 00-24-BE-42-2A-35
DHCP włączone . . . . . : Tak
Autokonfiguracja włączona . . . . . : Tak
Adres IPv6 połączenia lokalnego . . . . . : fe80::1c86-77b:522b:6932%11(Preferowane)
Adres IPv4 . . . . . : 10.101.83.34(Preferowane)
Maska podsieci . . . . . : 255.255.252.0
Dzierżawa uzyskana . . . . . : 30 maja 2011 13:11:54
Dzierżawa wygasa . . . . . : 31 maja 2011 07:11:54
Brama domyślna . . . . . : 10.101.80.1
Serwer DHCP . . . . . : 195.13.38.7
Identyfikator GUID DHCPv6 . . . . . : 208443066
Identyfikator DUID klienta DHCPv6 . . . . . : 00-01-00-01-12-a0-c9-03-00-24-be-42-2a-35
Serwery DNS . . . . . : 195.13.38.3
                          195.13.38.8
NetBIOS przez Tcpip . . . . . : Włączony
```

Sieci LAN i WAN

Koncepcja sieci lokalnej

Cel dydaktyczny:	Przedstawienie podstawowych cech sieci lokalnej.
Podstawowe wiadomości:	Sieć lokalna LAN charakteryzuje się fizyczną bliskością podłączanych ze sobą urządzeń, dużą przepustowością (obecnie w komputerach osobistych używa się interfejsów sieciowych o przepustowości jednego gigabita danych na sekundę) oraz tym, że nie wymagają one korzystania z usług zewnętrznych dostawców. Sieć lokalna może działać w odizolowaniu od innych sieci, jednak obecnie ogromna część sieci lokalnych posiada interfejsy łączące je z sieciami publicznymi.

Technologia Ethernet

Cele dydaktyczne:	<ol style="list-style-type: none">1. przedstawienie technologii Ethernet;2. przybliżenie zasad działania protokołu CSMA/CD.
Podstawowe wiadomości:	Technologia Ethernet jest obecnie najpopularniejszą technologią używaną w sieciach LAN. Ethernet w początkach swojego rozwoju wykorzystywał jako medium transmisyjne kabel koncentryczny. Obecnie najczęściej stosowana jest skrętka oraz światłowody. W sieciach Ethernet ramki

dostarczane są na postawie fizycznego adresu MAC interfejsu sieciowego.

Ethernet wykorzystuje jako metodę dostępu do łącza technologię CSMA/CD. Jest to protokół zapewniający wszystkim urządzeniom jednakowe prawa do transmisji danych. Protokół ten umożliwia badanie stanu łącza w celu określenia, czy w danym momencie żadne inne urządzenie pracujące w określonym segmencie sieci nie rozpoczęło nadawania. CSMA/CD realizuje również wykrywanie kolizji. Mechanizm ten pozwala wznowić transmisję po tym, jak dwa urządzenia rozpoczynające transmisję w tym samym momencie wywołały kolizję w sieci.

Rodzaje komunikacji wewnątrz sieci LAN

Cel dydaktyczny: Przedstawienie trzech rodzajów komunikacji w sieci LAN.

Podstawowe wiadomości: W sieciach LAN istnieją trzy podstawowe rodzaje komunikacji:

1. unicast – podstawowy rodzaj komunikacji, komunikacja jeden do jednego;
2. broadcast – komunikacja jeden do wszystkich;
3. multicast – komunikacja jeden do wielu.

Komunikacja broadcast może być wykorzystywana między innymi w protokole ARP, który służy do określenia adresu fizycznego MAC na podstawie adresu IP.

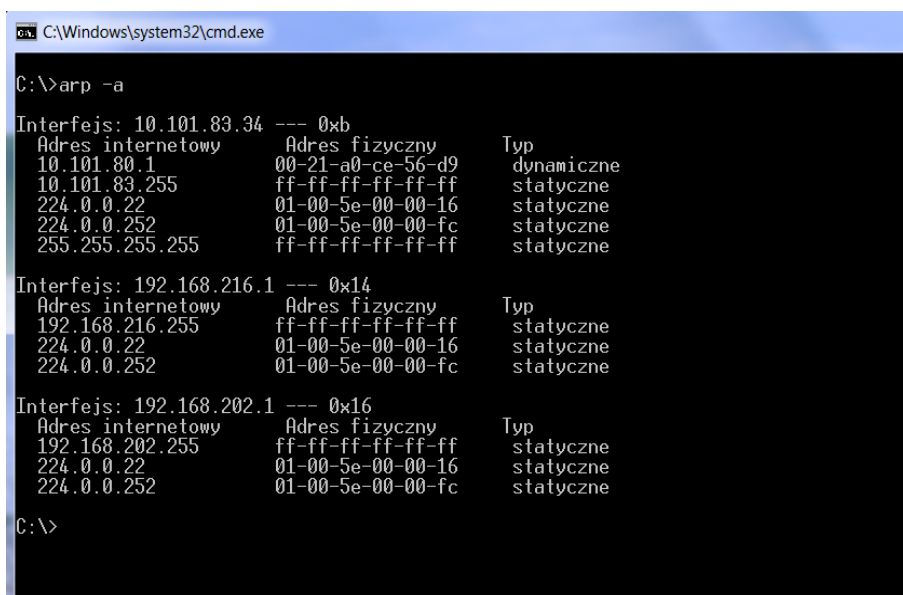
Protokół IP w wersji 6. wprowadza inne rozdzaje komunikacji, przede wszystkim zrezygnowano w nim z komunikacji broadcast.

Zadanie Sprawdzić, jak na danym komputerze wyglądają wpisy **praktyczne 1.:** w tabeli protokołu ARP.

Rozwiązanie 1.: W celu sprawdzenia zawartości tabeli ARP należy użyć w konsoli systemu Windows polecenia „arp-a”. Po jego wpisaniu na ekranie uzyskamy widok, który przedstawia rysunek 7.

Polecenia „arp-a” możemy również użyć do usuwania i dodawania statycznych wpisów na przykład za pomocą polecenia „arp-s 157.55.85.212 00-aa-00-62-c6-09”.

Rysunek 7. Widok ekranu komputera po wpisaniu polecenia „arp-a”



```
C:\Windows\system32\cmd.exe
C:\>arp -a

Interfejs: 10.101.83.34 --- 0xb
Adres internetowy   Adres fizyczny   Typ
10.101.80.1         00-21-a0-ce-56-d9 dynamiczne
10.101.83.255      ff-ff-ff-ff-ff-ff statyczne
224.0.0.22         01-00-5e-00-00-16 statyczne
224.0.0.252        01-00-5e-00-00-fc statyczne
255.255.255.255    ff-ff-ff-ff-ff-ff statyczne

Interfejs: 192.168.216.1 --- 0x14
Adres internetowy   Adres fizyczny   Typ
192.168.216.255    ff-ff-ff-ff-ff-ff statyczne
224.0.0.22         01-00-5e-00-00-16 statyczne
224.0.0.252        01-00-5e-00-00-fc statyczne

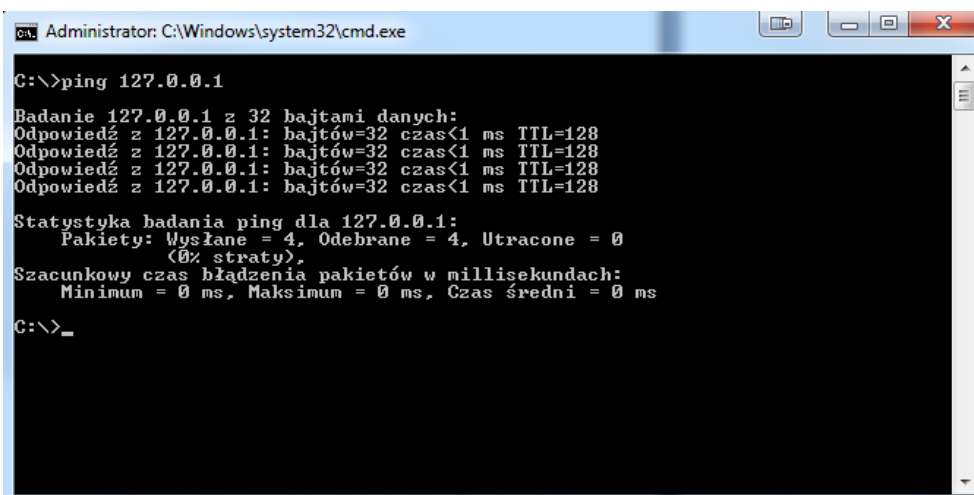
Interfejs: 192.168.202.1 --- 0x16
Adres internetowy   Adres fizyczny   Typ
192.168.202.255    ff-ff-ff-ff-ff-ff statyczne
224.0.0.22         01-00-5e-00-00-16 statyczne
224.0.0.252        01-00-5e-00-00-fc statyczne

C:\>
```

Zadanie Sprawdzić komunikację, stan interfejsu karty sieciowej
praktyczne 2.:

Rozwiązanie 2.: Aby wykonać test na interfejsie karty sieciowej w systemie Windows, uruchamiamy (Menu start → uruchom → cmd). Po wpisaniu polecenia: ping 127.0.0.1 powinniśmy na ekranie uzyskać widok, który przedstawia rysunek 8. Jeśli wynikiem jest 0 błędów, oznacza to, że interfejs karty sieciowej jest podniesiony i możliwa jest na nim komunikacja.

Rysunek 8. Widok ekranu konsoli po wykonaniu testu „pętli zwrotnej”



```
Administrator: C:\Windows\system32\cmd.exe
C:\>ping 127.0.0.1
Badanie 127.0.0.1 z 32 bajtami danych:
Odpowiedź z 127.0.0.1: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 127.0.0.1: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 127.0.0.1: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 127.0.0.1: bajtów=32 czas<1 ms TTL=128

Statystyka badania ping dla 127.0.0.1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0
            (0% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
    Minimum = 0 ms, Maksimum = 0 ms, Czas średni = 0 ms

C:\>_
```

Składniki adresu MAC

Cel	Przedstawienie budowy adresu MAC.
dydaktyczny:	
Podstawowe wiadomości:	Technologia Ethernet wykorzystuje adres MAC do lokalizowania urządzeń w sieci. Adres MAC składa się z 48 bitów. Adres fizyczny MAC zapisany jest w formie szesnastkowej. Przykładowy adres to: 00-24-BE-42-2A-35.

Sieci WAN

Cele dydaktyczne:	<ol style="list-style-type: none">1. przedstawienie podstawowych cech sieci rozległych,2. przedstawienie technologii umożliwiających przekazywanie informacji w sieciach WAN.
Podstawowe wiadomości:	<p>Sieci WAN mają za zadanie łączenie sieci lokalnych rozmieszczonych w różnych odległościach geograficznych. Sieci WAN charakteryzują się:</p> <ol style="list-style-type: none">1. dużą odległością pomiędzy łączonymi urządzeniami,2. mniejszą od sieci LAN przepustowością,3. koniecznością korzystania z usług firm zewnętrznych. <p>W sieciach WAN wykorzystywane są zupełnie inne technologie działające w warstwach fizycznych i inne łącza danych niż w sieciach LAN. Powodem jest to, że przesyłanie danych na duże odległości odbywa się na zupełnie innych zasadach. Protokoły realizujące zadania pierwszych dwóch warstw modelu OSI są bardzo złożo-</p>

ne. Uczestnicy kursu nie muszą znać ich budowy. Ważne jest jednak, aby zdawali sobie sprawę z istnienia podstawowych rodzajów technologii, wykorzystywanych w sieciach WAN:

1. łącza dziedziczone – niezawodne i szybkie łącze i jednocześnie najdroższa metoda łączenia;
2. komutację łączy (PSTN) – tańsze, lecz wolniejsze rozwiązanie;
3. komutację pakietów (Frame Relay, DSL) – popularne rozwiązanie stosunkowo szybkie i niedrogi;
4. komutacja komórek (ATM) – rozwiązanie najlepiej sprawdzające się do komunikacji głosowej VoIP oraz wideokonferencji.

Pytania testowe

1. Którego protokołu należy użyć w celu automatycznego skonfigurowania adresu IP, bramy domyślnej oraz serwera DNS?
 - a) SMTP
 - b) SNMP
 - c) DHCP
 - d) ARP

2. Która klasa adresów IP umożliwia zaadresowanie maksymalnie 254 urządzeń?
 - a) klasa A
 - b) klasa B
 - c) klasa C

3. Którego protokołu warstwy 4 używa usługa Telnet?
 - a) IP
 - b) TCP
 - c) TCP/IP
 - d) UDP
 - e) ICMP

4. Który z powyższych warstw należy do stosu protokołów TCP/IP?
 - a) aplikacji
 - b) sesji
 - c) transportowa
 - d) Internetu
 - e) łącza danych
 - f) fizyczna

5. Jaki protokół jest używany aby odnaleźć adres fizyczny lokalnego urządzenia?
- a) RARP
 - b) ARP
 - c) IP
 - d) ICM

Protokół IPv6

- Cele**
1. przedstawienie wad protokołu IPv4,
 2. zaprezentowanie możliwości protokołu IPv6.
- dydaktyczne:**
- Podstawowe wiadomości:**
- Protokół IP w wersji 4. (IPv4) został opracowany w roku 1981. IP jest protokołem komunikacyjnym, transportującym informacje w postaci pakietów. Każdy pakiet zawiera niezbędną porcję informacji, umożliwiającą mu dotarcie do adresata. Najważniejszą z nich jest oczywiście adres. Protokół IPv4 używany jest do adresowania 32-bitowych ciągów binarnych. W teorii oznacza to możliwość zaadresowania 4 miliardów urządzeń, jednak poprzez wyłączenie niektórych adresów z użytku (na przykład przez system klas, czy wyłączenie grupy adresów multicast), dla użytkowników dostępna jest pula około 280 milionów publicznych adresów IP.
- Protokół IP w wersji 6. jest rozwinięciem protokołu IPv4. Rozwiązuje on problem brakującej liczby adresów IP. Cechami odróżniającymi IPv6 od wersji 4. są:
1. rozmiar adresu IP – 128 bitów w przypadku adresu IPv6;
 2. wydajniejszy sposób adresowania i routingu;
 3. lepsze wsparcie dla transmisji multimediów;
 4. możliwość autoryzacji i zapewnienia bezpieczeństwa poprzez mechanizm IPSec;
 5. rozbudowane opcje autokonfiguracji.

Reprezentacja adresu IP

Cele	1. przedstawienie budowy adresu IPv6,
dydaktyczne:	2. przybliżenie rodzajów notacji w adresie IPv6.
Podstawowe wiadomości:	Adres IPv6 ma długość 128 bitów i składa się z trzech części, prefiksu globalnego, identyfikatora podsieci oraz ID interfejsu. Adres IPv6 zapisywany jest w notacji szesnastkowej. Przykładowy adres IP może mieć postać: fe80:0000:0000:0000:0202:b3ff:fe1e:8329, którą w wersji skróconej (pomijając początkowe zera z każdego oktetu) zapisać możemy jako: fe80::202:b3ff:fe1e:8329.

Konwersja liczb szesnastkowych

Liczby szesnastkowe to liczby posiadające jako bazę liczbę 16. Do tej pory uczestnicy kursu poznali system dwójkowy, w którym liczbą-bazą jest liczba 2. System szesnastkowy pozwala na zapisanie długich liczb w zwartej formie, jest on również łatwy do konwertowania na system dwójkowy. Oprócz systemu dwójkowego i szesnastkowego w informatyce używa się czasem zapisu ósemkowego. W zapisie szesnastkowym wykorzystuje się cyfry od 0 do 9 oraz litery od A do F.

Tabela 3. Zapisy

Zapis szesnastkowy	Zapis dziesiętny	Zapis ósemkowy	Zapis dwójkowy
0	0	0	0 0 0 0
1	1	1	0 0 0 1
2	2	2	0 0 1 0
3	3	3	0 0 1 1
4	4	4	0 1 0 0
5	5	5	0 1 0 1
6	6	6	0 1 1 0
7	7	7	0 1 1 1
8	8	8	1 0 0 0
9	9	10	1 0 0 1
A	10	12	1 0 1 0
B	11	13	1 0 1 1
C	12	14	1 1 0 0
D	13	15	1 1 0 1
E	14	16	1 1 1 0
F	15	17	1 1 1 1

Źródło: opracowanie własne.

Konwersja liczb szesnastkowych na dziesiętne odbywa się na tych samych zasadach co konwersja liczb dwójkowych. Szesnastkową liczbę **2AF3** możemy zapisać jako: $2 \times 16^3 + 10 \times 16^2 + 15 \times 16^1 + 3 \times 16^0$ co daje zapis w postaci dziesiętnej **10995**.

Konwersja z zapisu dziesiętnego na szesnastkowy wymaga więcej wysiłku. Należy bowiem odnaleźć najmniejszą potęgę liczby szesnaście, która jest mniejsza od liczby zapisanej w postaci dziesiętnej, odjąć liczbę dziesiętną od wyszukanej potęgi liczby szesnaście, a z otrzymanym wynikiem postępować analogicznie.

Konwersja z systemu dwójkowego na szesnastkowy

W prosty sposób można natomiast dokonać konwersji między systemami dwójkowym i dziesiętnym. Liczbę dwójkową dzielimy na czterobitowe elementy: **0101 1110 1011 0101 0010**. Następnie każdemu elementowi przypisujemy odpowiednią cyfrę szesnastkową. W rezultacie otrzymujemy: **5 E B 5 2**

Wdrożenie protokołu IPv6

Cele dydaktyczne:	Przedstawienie etapów wdrażania protokołu IPv6.
Podstawowe wiadomości:	<p>Protokół IP w wersji 6. osiągnął swoją pełną funkcjonalność w 2008 roku. W tym samym czasie zaczęły powstawać pierwsze serwisy wykorzystujące protokół IPv6.</p> <p>Na początku 2011 roku oficjalnie wyczerpała się pula wolnych publicznych adresów IP. Wyczerpanie adresów nastąpiłoby dużo wcześniej, gdyby nie mechanizmy takie jak NAT, które umożliwiają wykorzystywanie adresów prywatnych i tłumaczenie ich na adresy publiczne, dzięki czemu wiele urządzeń może komunikować się z otoczeniem za pomocą niewielkiej liczby publicznych adresów IP. NAT nie stanowi jednak rozwiązania problemu, a używanie tej technologii na ogromną skalę prowadzi do problemów z routowaniem w sieciach.</p>

Liczba serwisów opartych o protokół IPv6 w ostatnim czasie bardzo wzrosła. Organizacje związane z wdrażaniem IPv6 wykonują ogromną pracę, tak aby obecny w sieci praktycznie od samego początku jej rozwoju protokół IPv4 został zastąpiony przez nowsze rozwiązanie.

Pytania testowe

1. Które określenia są prawdziwe w odniesieniu do globalnych adresów unicast?
 - a) pakiety adresowane za pomocą jednego adresu unicast dostarczane są do jednego użytkownika;
 - b) są to odpowiedniki publicznych routowalnych adresów protokołu IPv4;
 - c) są to odpowiedniki prywatnych adresów protokołu IPv4;
 - d) te adresy nie są przeznaczone do routowania poza sieci lokalne, ale są niemal unikalne w skali globalnej.

2. Które określenia są prawdziwe w odniesieniu do adresów IPv6?
 - a) zera na początku oktetów są niezbędne;
 - b) dwa dwukropki (::) reprezentują bloki zer;
 - c) pojedynczy dwukropek jest używany do oddzielenia oktetów;
 - d) jeden interfejs może mieć przypisany tylko jeden rodzaj adresu IPv6.

3. Które para stwierdzeń jest prawdziwa dla protokołu IPv6?
 - a) adres IPv6 składa się z 32 bitów i ma reprezentację szesnastkową;
 - b) adres IPv6 składa się z 128 bitów i ma reprezentację ósemkową;
 - c) adres IPv6 składa się z 64 bitów i ma reprezentację dwójkową;
 - d) adres IPv6 składa się z 128 bitów i ma reprezentację szesnastkową.

Podsumowanie

Celem kursu było zaprezentowanie od podstaw koncepcji sieci komputerowej. Po jego zakończeniu uczestnicy posiadli wiedzę na temat różnych elementów składowych sieci. Poznali zasady działania różnego rodzaju sprzętu sieciowego, protokołów różnych warstw modelu OSI oraz różne rodzaje aplikacji wykorzystujących możliwości stwarzane przez sieć. Istnieje wiele alternatywnych technologii sieciowych, jednak na przestrzeni ostatnich lat największego znaczenia nabrały protokoły i rozwiązania związane z rozwojem Internetu. W niższych warstwach sieci dominuje technologia Ethernet, natomiast w warstwach wyższych, odpowiedzialnych za komunikację pomiędzy sieciami, obowiązującym standardem jest protokół IP. Materiały skupiają się więc na tych technologiach oraz na przybliżeniu innych obecnie stosowanych rozwiązań.

Celem zaproponowanych ćwiczeń jest praktyczne zaprezentowanie omawianych tematów na przykładzie konfiguracji standardowych komputerów podłączonych do sieci Internet. Uczestnicy odkrywają zasady działania mechanizmów, których używają na co dzień, często nie zdając sobie sprawy z ich złożoności.

Materiały oraz ćwiczenia zostały przygotowane z nadzieją, iż zdobyta wiedza zostanie wykorzystana w praktyce, oraz że stanie się ona dobrym punktem wyjścia do dalszego zgłębiania fascynującego świata sieci komputerowych.

Odpowiedzi do pytań testowych

Pytania testowe s. 18:

1 – d

2 – c

3 – b

4 – c

Pytania testowe s. 38:

1 – c

2 – c

3 – b

4 – a, c, d

5 – b

Pytania testowe s. 45:

1 – b

2 – b, c

3 – d

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*.