Sieci komputerowe

Model OSI

Model OSI

- W celu umożliwienia współpracy urządzeń pochodzących od różnych dostawców, konieczne stało się opracowanie zasad opisujących sposoby komunikacji.
- Do najbardziej znanych należą **ISO** (ang. International Standard Organization) oraz **IEEE** (ang. Institute of Electrical and Electronic Engineers)
- Ich postanowienia nie mają mocy prawnej, jednak wiele rządów czyni z nich obowiązujące standardy.

- W 1978 roku Międzynarodowa Organizacja Normalizacyjna (ISO) zaproponowała model architektury sieci zwany modelem OSI (ang. Open System Interconnection), integrujący wszystkie lokalne podsieci.
- Podstawowym założeniem modelu jest podział systemów sieciowych na siedem warstw współpracujących ze sobą w ściśle określony sposób. Model ten nie określa fizycznej budowy poszczególnych warstw, lecz na sposobach ich współpracy.

Warstwy modelu OSI

7	**Aplikacji**
6	**Prezentacji**
5	**Sesji**
4	**Transportowa**
3	**Sieciowa**
2	**Łącza danych**
1	**Fizyczna**

Warstwy górne – współpracują z oprogramowaniem systemu komputerowego

Warstwy dolne – zajmują się znajdowaniem właściwej drogi do celu, gdzie ma być przekazana dana informacja. Dzielą dane na odpowiednie pakiety (ramki)

Ramka jest formą organizacji danych warstwy łącza danych, która zawiera ilość informacji wystarczającą do pomyślnego przesyłania danych przez sieć lokalną do ich miejsca docelowego.

Warstwy dolne

1. Warstwa fizyczna – fundament na którym zbudowany jest model referencyjny OSI. Określa wszystkie składniki sieci niezbędne do obsługi elektrycznego, optycznego, radiowego wysyłania i odbierania sygnałów. Jest odpowiedzialna za przesyłanie strumieni bitów. Odbiera ramki danych z warstwy 2 (Łącza danych) i przesyła szeregowo bit po bicie. Operuje jedynie wartościami 0 i 1 czyli jest uzależniona od fizycznych własności przesyłania sygnałów.

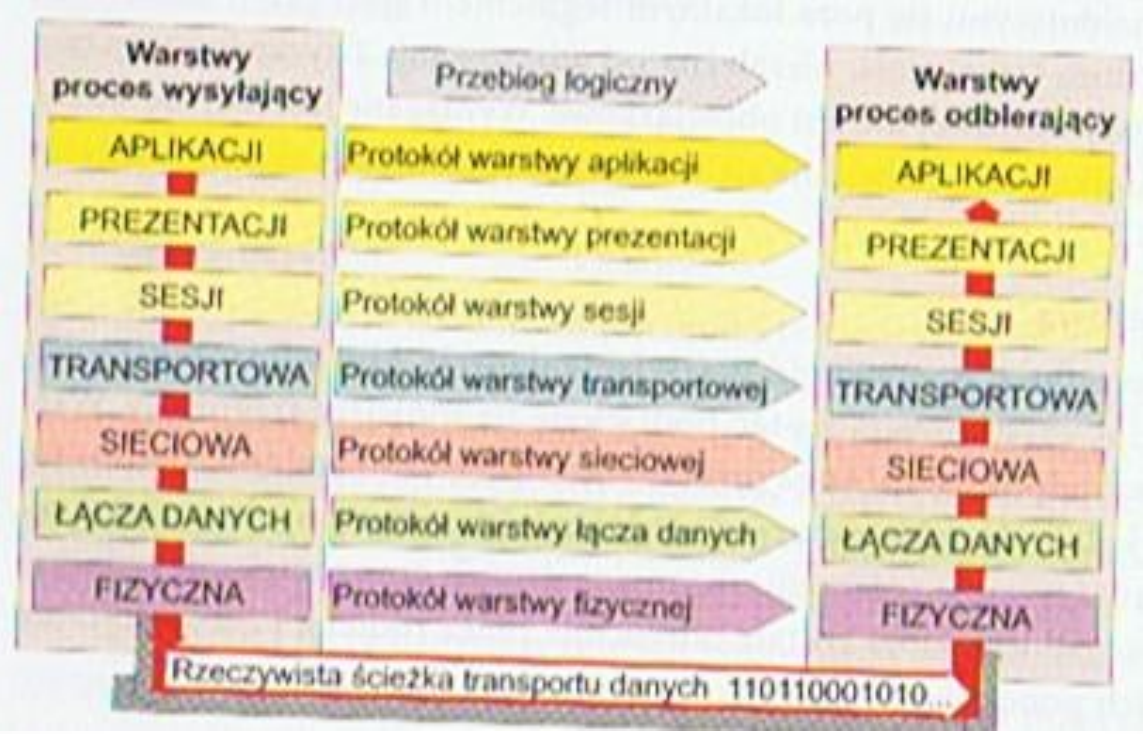
Warstwy dolne

2. Warstwa łącza danych – jest odpowiedzialna za końcową zgodność przesyłania danych. Zajmuje się pakowaniem danych w tzw. **ramki** i wysyłaniem ich do warstwy fizycznej. Warstwa ta jest odpowiedzialna za rozpoznawanie i naprawianie błędów spowodowanych uszkodzeniem podczas transmisji.
3. Warstwa sieciowa – odpowiedzialna za określenie trasy transmisji między komputerem nadawcą a komputerem odbiorcą.
4. Warstwa transportowa – dba o poprawność przesyłanych danych, jest odpowiedzialna za przesyłanie danych i integralność transmisji. Ustala odpowiednią kolejność przed wysłaniem pakietów do warstwy sesji. Potrafi wykryć pakiety, które zostały odrzucone przez routery i automatycznie generuje żądanie ich ponownej transmisji.

Warstwy górne

5. Warstwa sesji – otrzymuje od różnych aplikacji dane, które muszą zostać odpowiednio zsynchronizowane. Rozpoznaje połączenia między aplikacjami, dzięki czemu może zapewnić odpowiedni kierunek przepływu informacji.
6. Warstwa prezentacji – zarządza sposobem kodowania wszelkich danych, odpowiada za translację między niezgodnymi schematami kodowania.
7. Warstwa aplikacji – pełni funkcję interfejsu pomiędzy aplikacjami użytkownika a usługami sieci. Warstwa ta jest inicjatorem sesji komunikacyjnych.

Przepływ informacji między warstwami



Aby dane mogły pokonać stos złożony z poszczególnych warstw, warstwy te muszą się miedzy sobą komunikować. Prawdziwa komunikacja odbywa się poprzez warstwę fizyczną

Protokoły sieciowe

W sieci przesyłane są dane oraz informacje sterujące. Jedne i drugie mogą przyjmować różne formaty

Protokoły sieciowe to zbiór ścisłych reguł i kroków postępowania, które są automatycznie wykonywane przez urządzenia komunikacyjne w celu nawiązania łączności i wymiany danych

Model protokołu TCP/IP

Protokół Internetu (IP) został opracowany dla Departamentu Obrony USA, który szukał sposobu połączenia różnych rodzajów komputerów i sieci je obsługujących w jedną wspólną sieć.

TCP/IP (ang. Transmission Control Protocol/Internet Protocol) jest pakietem najbardziej rozpowszechnionych protokołów komunikacyjnych współczesnych sieci komputerowych. TCP/IP to najczęściej wykorzystywany standard sieciowy, stanowiący podstawę współczesnego internetu. Nazwa pochodzi od dwóch najważniejszych jego protokołów: **TCP** oraz **IP.**

Porównanie modelu OSI i TCP/IP

OSI

TCP/IP

7	**Aplikacji**	**Warstwa aplikacji**
6	**Prezentacji**	
5	**Sesji**	
4	**Transportowa**	**Transportowa**
3	**Sieciowa**	Warstwa internetu
2	**Łącza danych**	Warstwa dostępu do sieci
1	**Fizyczna**	

Dane przekazywane z TCP do IP nazywane są **segmentem TCP**
Dane, które IP przesyła do interfejsu sieciowego nazywane są **datagramem IP**
Ciąg bitów przepływający w sieci Ethernet nazywany jest **ramką**

Zadania warstw w TCP/IP

Warstwa aplikacji – to najwyższy poziom, w którym pracują niezbędne dla użytkownika aplikacje, takie jak serwer WWW czy przeglądarka internetowa

Warstwa transportowa – jej podstawowym zadaniem jest zapewnienie przesyłania danych oraz kierowanie właściwych informacji do odpowiednich aplikacji. Opiera się to na wykorzystaniu portów określonych dla każdego połączenia.

Warstwa internetu – odpowiada za obsługę komunikacji w sieci. W tej warstwie przetwarzane są datagramy mające adresy IP

Warstwa dostępu do sieci lub warstwa fizyczna – zajmuje się przekazywaniem danych przez fizyczne połączenia między urządzeniami sieciowymi.

Zbiór usług powiązanych z TCP/IP

Warstwa aplikacji	**Telnet, SSH, FTP, SMTP, HTTP, POP, IMAP**		**DNS, SNMP, DHCP**
Transportowa	TCP		UDP
Warstwa internetu	IP		ICMP
Warstwa dostępu do sieci	ARP		
	Ethernet	PPP,SLIP	

W warstwie transportowej działa protokół TCP, protokół IP zaś znajduje się w warstwie internetu. Warstwa transportowa odpowiedzialna jest za znalezienie drogi łączącej dwa hosty oraz określenie logicznej adresacji.

Host to każdy komputer podłączony do internetu lub innej sieci używającej protokołu TCP/IP i mający unikatowy adres IP.

Adres IP

Adres IP to unikatowy numer przyporządkowany do każdego urządzenia sieci komputerowych, na przykład komputera, drukarki, routera.

Adres IPv4 składa się z 32 bitów a więc 4 oktetów (oktet=8 bitów). Łatwiej jednak zapamiętać każdy oktet jako liczbę dziesiętną rozdzielając je kropkami np. 83.3.250.66. Ten sposób nosi nazwę *formatu bajtowo-dziesiętnego* lub też nazywamy go **notacją dziesiętną z kropkami.**

32 bitowy adres 10000010 00001010 00001100 00011111 to adres zapisany jako 130.10.12.31

Uniwersalność tego systemu adresowania polega na umożliwieniu wyznaczania tras pakietów. Adres IP zawiera informację do jakiej sieci jest włączony komputer a także jednoznaczny adres komputera w tej sieci.

Tak więc w obrębie adresu mamy **identyfikator sieciowy oraz identyfikator komputera.**

Klasy adresowe

- Klasa A to adresy o 8 bitowym identyfikatorze sieciowym i 24 bitowym identyfikatorze hosta czyli 8/24
- Klasa B to adresy o 16 bitowym identyfikatorze sieciowym i 16 bitowym identyfikatorze hosta czyli 16/16
- Klasa C to adresy o 24 bitowym identyfikatorze sieciowym i 8 bitowym identyfikatorze hosta czyli 24/8

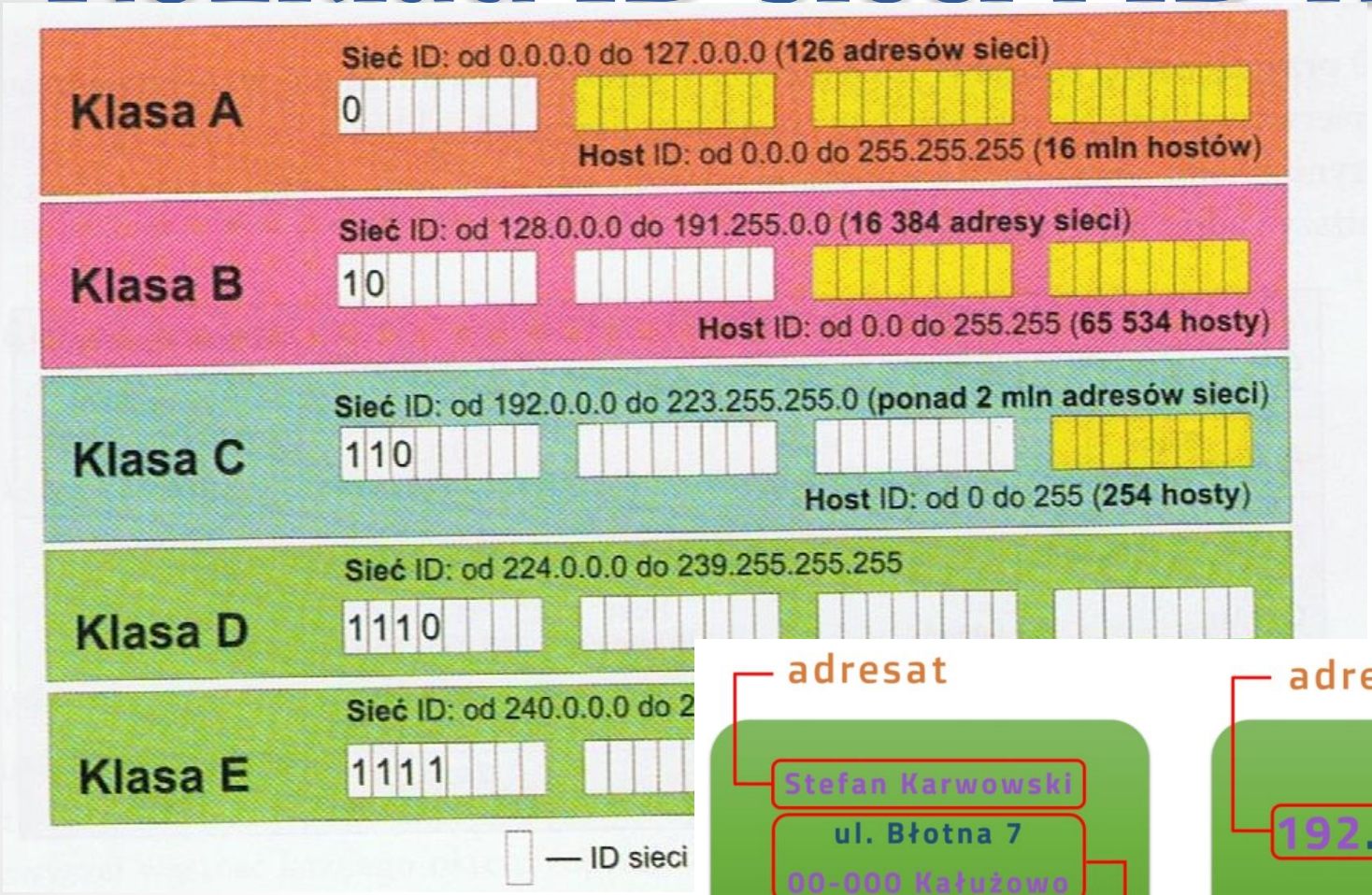
Bity w adresie IP są interpretowane jako adres sieci, adres hosta.

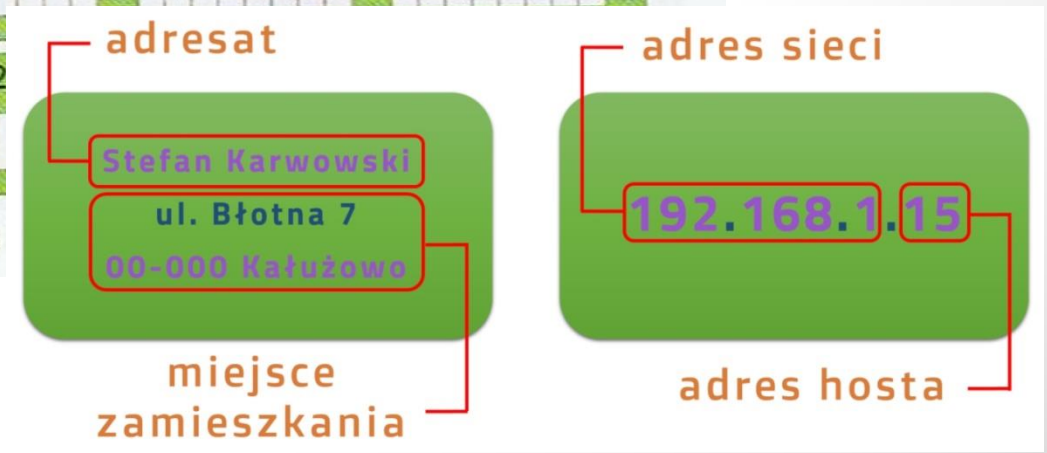
Struktura bitowa adresu IP

Klasa	Struktura bitowa adresu IP	Zakres adresów	Zakres adresów IP dostępnych dla użytkowników
A	0 Sieć (7 bitów) Host (24 bity)	0.0.0.0 127.255.255.255	1.0.0.0 126.0.0.0
B	10 Sieć (14 bitów) Host (16 bitów)	128.0.0.0 191.255.255.255	128.0.0.0 191.254.0.0
C	110 Sieć (21 bitów) Host (8 bitów)	192.0.0.0 223.255.255.255	192.0.0.0 223.255.254.0
D	1110 adres grupowy (28 bitów)	224.0.0.0 239.255.255.255	żaden
E	1111 zarezerwowane na przyszłość	240.0.0.0 255.255.255.255	żaden

- **Adresy klasy A** wykorzystywane przez duże sieci. W tej klasie może istnieć 126 sieci, z których każda ma ponad 16 mln hostów. Na adresy sieci przeznaczonych jest 7 bitów, skrajne czyli 0 i 127 są zarezerwowane czyli 2^7-2=126 adresów sieci.
- **Klasa B** przeznaczona jest dla sieci średniej wielkości. 14 bitów określa sieć, 16 bitów dla hostów czyli 2^{14} = 16384 sieci, 2^{16}-2 = 65534 hostów każda.
- **Klasa C** adresowana jest za pomocą 21 bitów – daje to 2^{21} sieci ale w każdej z nich może być co najwyżej 2^8 czyli 256 adresów IP tzn. 254 hosty
- **Adresy klasy D** stosowane są w sytuacjach szczególnych
- **Adresy klasy E** mają specjalne znaczenie.

Rozkład ID sieci i ID hosta





Problem

Skończona liczba sieci i hostów spowodowała rozwój koncepcji zastosowania puli adresów IP prywatnych w sieciach lokalnych i podłączenie jej do internetu poprzez jeden **adres publiczny**. Proces tłumaczenia adresu z puli prywatnej na publiczną to translacja NAT (*Network Address Translation*). W praktyce oznacza to, że korzystając z jednego adresu publicznego IP możemy podłączyć do internetu wiele komputerów.

Adresy…..

- **Adres rozgłoszeniowy** – wszystkie bity w części hosta przyjmują wartość 1 (ang. Broadcast). Taki adres jest zarezerwowany w każdej sieci, przeznaczony jest jako *adres rozgłoszeniowy* dla wszystkich hostów np. adres 152.23.255.255 oznacza adres rozgłoszeniowy w sieci 152.23.0.0 (klasa B).
- **Adres sieci** – adres w którym wszystkie bity w segmencie hosta przyjmują wartość 0 (ang. Network addres).

Dlatego liczba hostów jest mniejsza od całej puli adresów o 2

Adresy specjalne

- **Adres pętli zwrotnej** np. 127.0.0.1 – należący do sieci 127.0.0.0 nie łączy się z żadną siecią . Używany głównie w celach testowych np. klient i serwer uruchomiony na jednej maszynie.
- **Adres domyślny** – 0.0.0.0 adres specjalny oznacza lokalną sieć. Adres 0.0.0.88 oznacza hosta z numerem 88 w tej sieci.

Adresy niepubliczne (prywatne)

Adresów niepublicznych nie można używać w Internecie. Są przeznaczone do budowy sieci lokalnych. Hosty które mają mieć dostęp do internetu muszą być odpowiednio maskowane inaczej zwane NAT-owaniem.

Klasa	Zakres adresów prywatnych w danych klasach	
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Maski sieciowe

Maska sieci składa się, podobnie jak adres IP z 4 oktetów. Używana jest do wydzielenia z adresu IP części odpowiadającej za identyfikację sieci i części odpowiadającej za identyfikację hosta.

Klasa adresów sieciowych wyznacza maskę sieciową.

Klasa	Bity-maska podsieci	Notacja dziesiętna
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

Adresowanie bezklasowe IPv4

Załóżmy, że potrzebujemy 300 adresów IP. Klasa C, która daje 254 adresy hostów jest niewystarczająca, natomiast klasa B zapewni nam 65 534 adresów, ale zmarnujemy 65 234 (65 534-300) adresy.

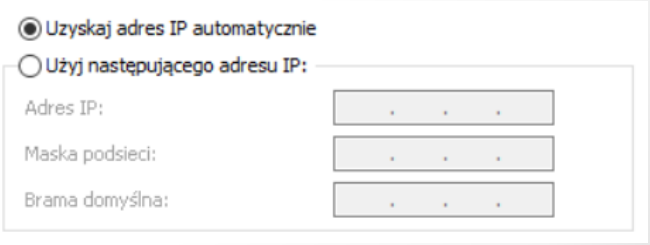
Od 1997 podział na klasy jest nieaktualny. Obecnie adresy IPv4 są przydzielane bez specjalnego zwracania uwagi na klasy sieci (zobacz CIDR).

Zaczęto nadawać maski, które stały się częścią adresacji hostów.

Adresowanie bezklasowe IPv4

W tabelce przedstawiono wszystkie możliwe podsieci dla zakresu od 2 do 254 hostów. Pozwoliło to na ekonomiczne wykorzystanie adresów IPv4.

Maska *(dziesiętnie)*	Maska *(binarnie)*	Liczba podsieci	Liczba hostów w podsieci
255.255.255.0	11111111 11111111 11111111 00000000	1	254
255.255.255.128	11111111 11111111 11111111 10000000	2	126
255.255.255.192	11111111 11111111 11111111 11000000	4	62
255.255.255.224	11111111 11111111 11111111 11100000	8	30
255.255.255.240	11111111 11111111 11111111 11110000	16	14
255.255.255.248	11111111 11111111 11111111 11111000	32	6
255.255.255.252	11111111 11111111 11111111 11111100	64	2
255.255.255.254	11111111 11111111 11111111 11111110	128	0



Host jest zatem określany przez adres IP i maskę podsieci

Adres sieci w adresowaniu bezklasowym

Znając adres IP oraz jego maskę można określić adres sieci. W tym celu należy wykonać funkcję AND pomiędzy adresem IP a jego maską sieci.

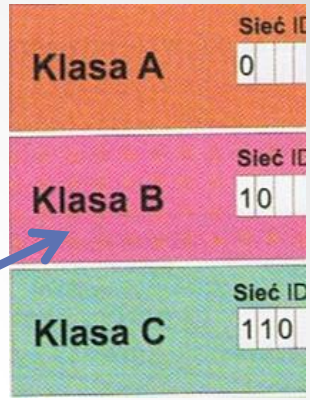
Kombinacja bitów	Wartość
1 AND 1	1
0 AND 1	0
1 AND 0	0
0 AND 0	0

Przykład

Dla adresu IP 131.105.15.61 i maski 255.255.255.0 określ jego klasę, adres sieci, oraz adres hosta.

Przykład

IP 131.105.15.61 maska 255.255.0.0



Określenie klasy polega na sprawdzeniu pierwszych bitów pierwszego oktetu badanego adresu czyli 131

10000011

Wykonując binarne AND adresu IP i maski otrzymamy adres sieci.

	131	**105**	**15**	**61**
IP	10000011	01101001	00001111	00111101
maska	255	255	0	0
AND	11111111	11111111	00000000	00000000
Adres sieci	10000011	01101001	00000000	00000000
	131	105	0	0

Może inaczej, posłuchaj

http://pasja-informatyki.pl/sieci-komputerowe/adresowanie-ipv4

Adresowanie IPv6

Jest „nową" wersją protokołu IP, który ma zastąpić IPv4. Pierwsze dokumenty opisujące IPv6 pochodzą z 1995 r.

Cechy nowego protokołu:

- Nowy format nagłówka (nie zgodny z IPv4)
- Olbrzymia przestrzeń adresowa
- Ułatwiona konfiguracja adresów (możliwość konfiguracji bez serwera DHCP).

Budowa IP v6

Adresy IPv6 składają się z 128 bitów. Łatwo jest sprawdzić, że liczba wszystkich adresów IPv6

to liczba 39 cyfrowa !

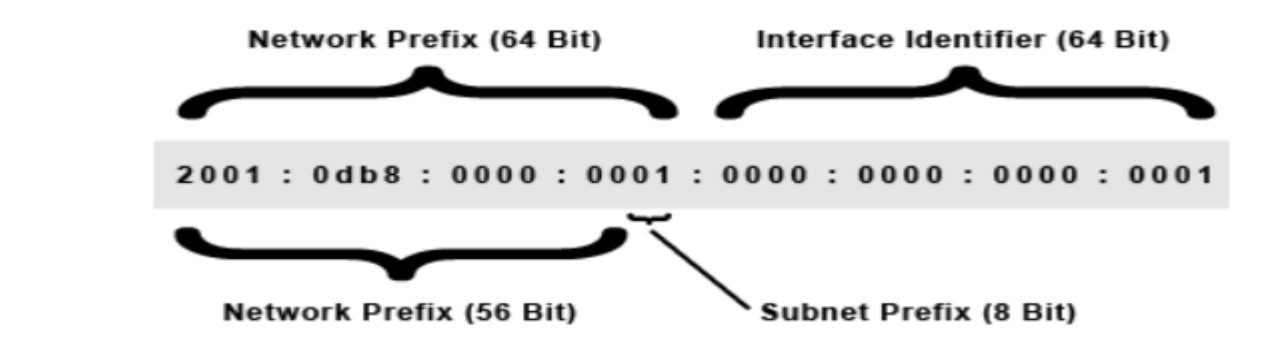
Przykład:

1101100101011100 0000110011001100 1000000100001010 1111110001000010 1111010110100001 0111001000100001 0001000010011010 0000000000010011

Każdy 16 bitowy człon adresu jest, jest dla skrócenia zapisu, zapisywany w postaci szesnastkowej i oddzielony dwukropkiem. Oto rezultat:

D95c:0ccc:810a:fc42:f5a1:7221:109a:0013

Szczegółowy adres IPv6



Adres IPv6 składa się z dwóch części. Prefiks sieci (prefiks lub identyfikator sieci) i identyfikator interfejsu (sufiks, IID lub EUI).

Prefiks sieci identyfikuje sieć, podsieć lub zakres adresów. Identyfikator interfejsu identyfikuje hosta w tej sieci. Tworzony jest z 48-bitowego adresu MAC interfejsu i konwertowany na adres 64-bitowy. Jest to zmodyfikowany format EUI-64.

W ten sposób interfejs jest jednoznacznie identyfikowalny, niezależnie od prefiksu sieciowego.

Podstawowe rodziny protokołów

Protokół nierutowalny

Np.. **NetBUI** opracowany przez firmę IBM w 1995, wykorzystuje jedynie adresowanie przez 1 i 2 warstwę na poziomie MAC karty Ethernet. Protokoły te sprawdzają się jedynie w niewielkich odizolowanych sieciach LAN. Protokół ten nie jest „przepuszczany" przez routery

Protokół rutowalny

Omawiany wcześniej **TCP/IP**, najczęściej stosowany zestaw protokołów sieciowych, który łączy komputery pracujące na różnych platformach sprzętowo-systemowych.

Innym jest **IPX/SPX** opracowany w latach 70 przez firmę NOWELL, pozwalającą na przesyłanie danych pomiędzy sieciami.

Protokoły internetowe: HTTP

HTTP *(ang. Hypertext Transfer Protocol)* – protokół przesyłania dokumentów hipertekstowych to protokół sieci WWW (ang. World Wide Web). Za pomocą protokołu HTTP przesyła się żądania udostępnienia dokumentów WWW i informacje o kliknięciu odnośnika oraz informacje z formularzy. Zadaniem stron WWW jest publikowanie informacji – natomiast protokół HTTP właśnie to umożliwia.

Protokoły internetowe: HTTPS

HTTPS (*ang. Hypertext Transfer Protocol Secure*) – szyfrowana wersja protokołu HTTP. W przeciwieństwie do komunikacji niezaszyfrowanego tekstu w HTTP klient-serwer, HTTPS szyfruje dane przy pomocy protokołu SSL.

HTTPS działa domyślnie na porcie nr 443 w protokole TCP. Wywołania tego protokołu zaczynają się od https://, natomiast zwykłego połączenia HTTP od http://. Protokół HTTPS jest warstwę wyżej od standardu TLS (który znajduje się na warstwie prezentacji), najpierw następuje więc wymiana kluczy TLS, a dopiero później żądanie HTTP.

Protokoły internetowe: FTP I SFTP

Protokół transferu plików, FTP (od *ang. File Transfer Protocol*) – protokół komunikacyjny typu klient-serwer wykorzystujący protokół sterowania transmisją (TCP) według modelu TCP/IP (krótko: połączenie TCP), umożliwiający dwukierunkowy transfer plików w układzie serwer FTP–klient FTP.

SFTP (*ang. SSH File Transfer Protocol*) – protokół komunikacyjny typu klient-serwer, który umożliwia przesyłanie plików poprzez sieć TCP/IP.

Przesyłając plik przy użyciu protokołu FTP uzyskujemy dobre przepływności, ale nie zyskujemy bezpieczeństwa – nasze hasła i dane nie są szyfrowane podczas przysyłania, co potencjalnie stwarza zagrożenie ich kradzieży. Znaczną poprawę bezpieczeństwa przynosi protokół SFTP,a przesyłane dane są szyfrowane z wykorzystaniem klucza szyfrującego.

Protokoły internetowe: SMTP

SMTP (*ang. Simple Mail Transfer Protocol*) – protokół komunikacyjny opisujący sposób przekazywania poczty elektronicznej w Internecie.

SMTP to względnie prosty, tekstowy protokół, w którym określa się co najmniej jednego odbiorcę wiadomości (w większości przypadków weryfikowane jest jego istnienie), a następnie przekazuje treść wiadomości. Demon SMTP działa najczęściej na porcie 25.

Jednym z ograniczeń pierwotnego SMTP jest brak mechanizmu weryfikacji nadawcy, co ułatwia rozpowszechnianie niepożądanych treści poprzez pocztę elektroniczną (wirusy komputerowe, spam).

Protokoły internetowe: POP3 i IMAP

Post Office Protocol ***(POP***) – protokół internetowy z warstwy aplikacji pozwalający na odbiór poczty elektronicznej ze zdalnego serwera do lokalnego komputera poprzez połączenie TCP/IP. Ogromna większość współczesnych internautów korzysta z POP3 do odbioru poczty.

IMAP (*ang. Internet Message Access Protocol*) – internetowy protokół pocztowy zaprojektowany jako następca POP3.

W przeciwieństwie do POP3, który umożliwia jedynie pobieranie i kasowanie poczty, IMAP pozwala na zarządzanie wieloma folderami pocztowymi oraz pobieranie i operowanie na listach znajdujących się na zdalnym serwerze.

IMAP pozwala na ściągnięcie nagłówków wiadomości i wybranie, które z wiadomości chcemy ściągnąć na komputer lokalny. Pozwala na wykonywanie wielu operacji, zarządzanie folderami i wiadomościami.

Protokoły internetowe: DNS

Domain Name System (DNS, pol. „system nazw domenowych") – system serwerów, protokół komunikacyjny oraz usługa obsługująca rozproszoną bazę danych adresów sieciowych. Pozwala na zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową. Dzięki DNS nazwa mnemoniczna, np. www.nasza-szkola.pl jest tłumaczona na odpowiadający jej adres IP, czyli 85.11.114.135.

DNS to złożony system komputerowy oraz prawny.

Protokoły internetowe: DHCP

DHCP (*ang. Dynamic Host Configuration Protocol* – protokół dynamicznego konfigurowania hostów) – protokół komunikacyjny umożliwiający hostom uzyskanie od serwera danych konfiguracyjnych, np. adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski podsieci.

W kolejnej generacji protokołu IP, czyli IPv6, jako integralną część dodano nową wersję DHCP, czyli DHCPv6.

W sieci opartej na protokole TCP/IP każdy komputer ma co najmniej jeden adres IP i jedną maskę podsieci; dzięki temu może się komunikować z innymi urządzeniami w sieci.

Protokoły internetowe: telnet i SSH

Telnet – standard protokołu komunikacyjnego używanego w sieciach komputerowych do obsługi odległego terminala w architekturze klient-serwer.

Protokół obsługuje tylko terminale alfanumeryczne, co oznacza, że nie obsługuje myszy ani innych urządzeń wskazujących. Nie obsługuje także graficznych interfejsów użytkownika. Wszystkie polecenia muszą być wprowadzane w trybie znakowym w wierszu poleceń.

SSH (ang. secure shell) to standard protokołów komunikacyjnych. W ścisłym znaczeniu SSH jest następcą protokołu Telnet. SSH różni się od Telnetu tym, że transfer wszelkich danych jest zaszyfrowany oraz możliwe jest rozpoznawanie użytkownika na wiele różnych sposobów.

Bezpieczeństwo sieci

- W jaki sposób dane mogą zostać ukradzione ?
- Bezpieczne hasła
- Szyfrowanie a prywatność
- Bezpieczeństwo dostępu do sieci bezprzewodowej
- Programy antywirusowe i zapora sieciowa
  - Wirus
  - Robak
  - Trojan
  - Skaner i exploit
  - Sniffing
  - Spoofing
  - Rootkity
  - Adwere
  - Spyware
  - Atak DDoS
  - Zatruwanie DNS