Futura – Policealna Szkoła dla Dorosłych w Lublinie

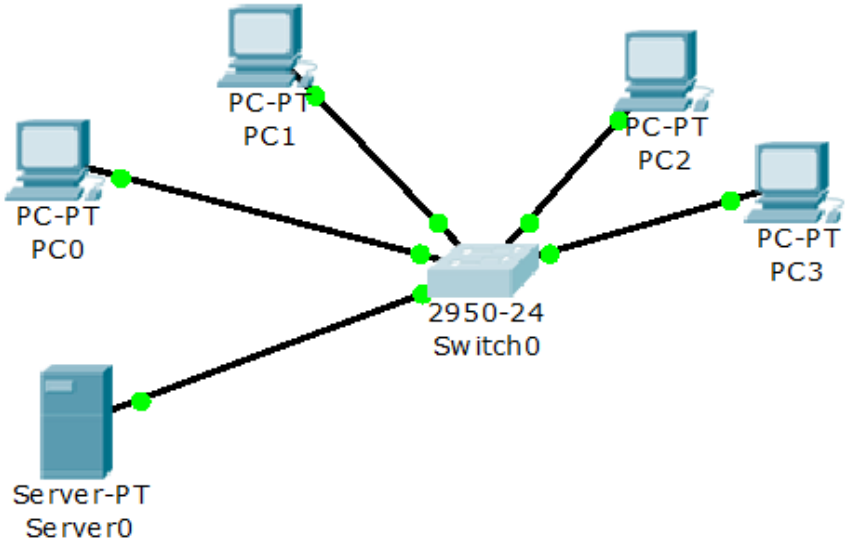
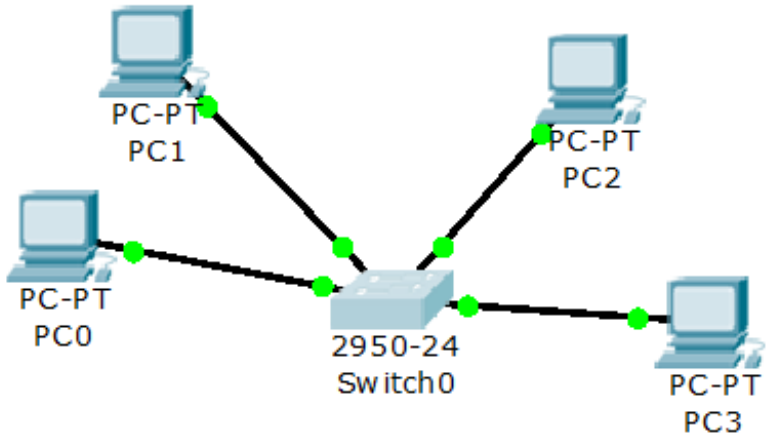
Kierunek: technik informatyk 351203

Semestr: I
Przedmiot: Sieci komputerowe
Nauczyciel: Mirosław Ruciński

Temat 6. <u>Rodzaje środowisk sieciowych (klient-serwer I peer to peer)</u>

Sieci client-server (dedykowany serwer)

Peer to peer Network

Sieci client-server (dedykowany serwer)	Peer to peer Network (sieć równorzędna)
	
Sieć typu klient-serwer jest rozwiązaniem z dedykowanym serwerem zarządzającym. Komputery użytkowników są administrowane, monitorowane i zarządzane centralnie. Klienci serwera mogą pracować w środowisku Domenowym lub Grupie Roboczej	**Sieć peer to peer network. Wszystkie podłączone do sieci komputery są traktowane jednakowo (posiadają takie same prawa, wynikające z praw określonych na danym stanowisku komputerowym). Użytkownicy mogą pracować w Grupie Roboczej.**

Zalety sieci client-server

- Dzięki centralnemu zarządzaniu bezpieczeństwem sieci oparte na serwerach są o wiele bezpieczniejsze od peer-to-peer.
- Zmniejszenie ilości haseł wymaganych do zapamiętania przez użytkownika (najczęściej do jednego)
- Zwiększenie wydajności pracujących w niej komputerów poprzez zdjęcie z nich ciężaru przetwarzania żądań innych klientów, żądania są przetwarzane przez serwer, który najczęściej ma większą moc obliczeniową niż zwykły komputer
- Skalowalność sieci, łatwość zmieniania rozmiarów sieci. Zasoby są centralnie zabezpieczone i zarządzane znajdują się w jednym miejscu, przez co wydajność sieci nie spada wraz z jej powiększaniem.

Wady sieci client-server

- Duże koszty budowy i eksploatacji tego typu sieci wynikająca z konieczności zakupu, sieciowego systemu operacyjno oraz wyznaczenia administratora zarządzającego.
- Awaria serwera powoduje unieruchomienie całej sieci. Można tego uniknąć poprzez np. grupowanie serwerów w celu uzyskania nadmierności. Jednak zwiększa to koszty budowy sieci.

Zastosowanie sieci client-server

Sieci oparte na serwerach są stosowane zwłaszcza w dużych sieciach, wymagających zwiększonego bezpieczeństwa oraz centralnego zarządzania zasobami.

Zalety sieci peer-to-peer

Sieci peer-to-peer są łatwe do wdrożenia, tanie w eksploatacji, ponieważ nie wymagają one skomplikowanych a co za tym idzie drogich serwerów. Nie wymagają opieki ze strony wykwalifikowanych administratorów.

Wady sieci peer-to-peer

Użytkownicy zmuszeni są pamiętać wiele haseł, zwykle po jednym dla każdego komputera pracującego w tego typu sieci.

Brak centralnego składowania i udostępniania danych wymaga od użytkowników samodzielnego wyszukiwania danych rozproszonych na wielu komputerach.

Mniejsza wydajność spowodowana, gdy zdalni użytkownicy współdzielą zasoby. Dostęp do zasobów danego użytkownika jest możliwy tylko wtedy, gdy jest on dostępny, (jeśli użytkownik wyłączy swój komputer jego zasoby będą niedostępne).

Temat 7. <u>Model ISO-OSI oraz DOD. Protokoły sieciowe</u>

ISO Międzynarodowa Organizacja Normalizacyjna (ang. International Organization for Standardization)

OSI (ang. Open System Interconnection) Model OSI (pełna nazwa ISO OSI RM, ISO OSI Reference Model – model odniesienia łączenia systemów otwartych).

Model ISO OSI RM jest traktowany, jako model odniesienia (wzorzec) dla większości rodzin protokołów komunikacyjnych. Podstawowym założeniem modelu jest podział systemów sieciowych na 7 warstw (ang. layers) współpracujących ze sobą w ściśle określony sposób.

Model OSI		Protokoły	Model TCP/IP
7	***Warstwa - Aplikacji***	***HTTP, HTTPS, FTP, TFTP SMTP, POP3, TELNET, IMAP, SSH***	***Aplikacji***
6	***Warstwa - Prezentacji***		
5	***Warstwa - Sesji***		
4	***Warstwa - Transportowa***	***TCP, UDP***	***Transportowa***
3	***Warstwa - Sieciowa***	***IP, RIP, ARP***	***Internetu***
2	***Warstwa - Łącza danych***	***MAC***	***Dostępu do sieci***
1	***Warstwa - Fizyczna***	***Ethernet, Token Ring, Frame Relay, ATM***	

Warstwa aplikacji

Warstwa aplikacji jest warstwą najwyższą, zajmuje się specyfikacją interfejsu, który wykorzystują aplikacje do przesyłania danych do sieci (poprzez kolejne warstwy modelu ISO/OSI). W przypadku sieci komputerowych aplikacje są zwykle procesami uruchomionymi na odległych hostach. Interfejs udostępniający programistom usługi dostarczane przez warstwę aplikacji opiera się na obiektach nazywanych gniazdami(ang. socket). Kiedy klient chce przesłać żądanie do serwera, przekazuje komunikat w dół do warstw niższych, które fizycznie przesyłają go do odpowiedniej maszyny, gdzie informacje ponownie wędrują w górę i są ostatecznie odbierane przez serwer. Jednocześnie zapewnia interfejs między aplikacjami, których używamy, a siecią (umożliwia komunikację).

Warstwa prezentacji

Podczas ruchu w dół zadaniem warstwy prezentacji jest przetworzenie danych od aplikacji do postaci kanonicznej (ang. canonical representation) zgodnej ze specyfikacją OSI-RM, dzięki czemu niższe warstwy zawsze otrzymują dane w

tym samym formacie. Kiedy informacje płyną w górę, warstwa prezentacji tłumaczy format otrzymywanych danych na zgodny z wewnętrzną reprezentacją systemu docelowego. Warstwa ta odpowiada za kodowanie i konwersję danych oraz za kompresję / dekompresję; szyfrowanie / deszyfrowanie. Warstwa prezentacji obsługuje np. MPEG, JPG, GIF itp.

Warstwa sesji

Warstwa sesji otrzymuje od różnych aplikacji dane, które muszą zostać odpowiednio zsynchronizowane. Synchronizacja występuje między warstwami sesji systemu nadawcy i odbiorcy. Warstwa sesji "wie", która aplikacja łączy się z którą, dzięki czemu może zapewnić właściwy kierunek przepływu danych – nadzoruje połączenie. Wznawia je po przerwaniu.

Warstwa transportowa

Warstwa transportowa dba o poprawność przesyłania danych. W tej warstwie standardowa paczka danych oznaczana jest, jako TPDU (ang. Transport Protocol Data Unit). Aby informacje mogły zostać przesłane w dół, często muszą zostać podzielone na mniejsze fragmenty. Jeżeli informacji nie uda się przesłać poprawnie za pierwszym razem, warstwa transportowa próbuje to zrobić, aż do wyczerpania limitu przekazów. Ważnym zadaniem warstwy transportowej jest szeregowanie przekazywanych informacji według priorytetów i przydzielanie im określonego pasma transmisji. Jeżeli wydajność niższych warstw sieciowych jest zbyt mała w stosunku do ilości przekazywanych z góry informacji, to warstwa transportowa układa je w określonych kolejkach według priorytetu. W ostateczności, kiedy kolejki się przepełniają warstwa transportowa zwraca do góry komunikaty o ich zapełnieniu i usuwa nadmiarowe dane. Warstwa transportowa rejestruje również komunikaty o przerwaniu połączenia i pozwala na bezpieczne zakończenie komunikacji..

Warstwa sieciowa

Warstwa sieciowa, jako jedyna dysponuje wiedzą dotyczącą fizycznej topologii sieci. Rozpoznaje drogi łączące poszczególne komputery (ang. routing) i decyduje ile informacji należy przesłać jednym z połączeń a ile innym. Jej zadanie, to zapewnienie sprawnej łączności między punktami sieci. Routery są podstawą budowy rozległych sieci informatycznych takich jak Internet, potrafią odnaleźć najlepszą drogę do przekazania informacji. Warstwa sieciowa podczas ruchu w dół

umieszcza dane wewnątrz pakietów zrozumiałych dla warstw niższych (enkapsulacja).

Warstwa łącza danych

Warstwa łącza danych nadzoruje jakość przekazywanych informacji. Warstwa łącza danych ma możliwość zmiany parametrów pracy warstwy fizycznej tak, aby obniżyć ilość pojawiających się podczas przekazu błędów. Zajmuje się pakowaniem danych w ramki i wysyłaniem do warstwy fizycznej. Rozpoznaje błędy związane z niedotarciem pakietu oraz uszkodzeniem ramek i zajmuje się ich naprawą. Podczas ruchu w dół w warstwie łącza danych zachodzi enkapsulacja pakietów z warstwy sieciowej tak, aby uzyskać ramki zgodne ze standardem.

Warstwa fizyczna

Warstwa fizyczna to konkretny układ elektroniczny tworzący kanał komunikacyjny poprzez medium fizyczne (kabel miedziany, światłowód, fale radiowe, itd.) pozwalający na wymianę informacji pomiędzy urządzeniami sieciowymi. Odbiera ramki od warstwy łącza danych i wysyła je - bit po bicie - do nośnika (i odwrotnie), którego łącze stanowi jej granicę. Warstwa fizyczna posiada tylko informacje o właściwościach fizycznych / optycznych przesyłanych bitów. Musi być tak skonstruowana, aby większość przesyłanych nią danych bez zniekształceń trafiła do odbiorców. Warstwa ta często posiada własny system identyfikacji poszczególnych uczestników komunikacji, całkowicie przezroczysty dla warstw wyższych. W niektórych zastosowaniach dodatkowym celem warstwy fizycznej jest ochrona informacji przed zmianą lub podsłuchem przez niepowołane osoby. Zwykle zabezpieczenia te mają charakter fizyczny, a nie algorytmiczny.

Model odniesienia TCP/IP, zwany również modelem DoD (Departament of Defense), inaczej niż OSI nie przypisuje sztywno funkcji do każdej warstwy, jest bardziej elastyczny od modelu OSI. Podstawowa różnica między modelem OSI a TCP/IP polega na braku stałej gwarancji dostarczania pakietów przez warstwę transportową. Protokoły TCP i IP łącznie zarządzają przepływem danych przez sieć w obydwu kierunkach. Warstwami dla modelu TCP/IP są:

warstwa aplikacji – obejmuje protokoły HTTP, SMTP, FTP, NFS, NIS, LPD, Telnet, SSH.

warstwa transportowa – obejmuje protokoły UDP i TCP. Pierwszy dostarcza pakiety prawie bez sprawdzania poprawności transmisji, drugi natomiast gwarantuje bezstratne ich dostarczenie. Ramki warstwy transportowej zawierają dane w protokole IP z warstwy sieciowej.

warstwa Internetu – zawiera protokoły ICMP, IP, IGMP, RIP, OSPF i EGP. Protokół IP odpowiada za odnalezienie adresata danych w sieci. Pakiety tych protokołów są transportowane przez protokoły z warstwy łącza.

Warstwa dostępu do sieci – zawiera protokoły ARP i RARP obsługujące niskopoziomową transmisję pakietów

Protokół jest to zbiór procedur oraz reguł rządzących komunikacją, między co najmniej dwoma urządzeniami sieciowymi. Istnieją różne protokoły, lecz nawiązujące w danym momencie połączenie urządzenia muszą używać tego samego protokołu, aby wymiana danych pomiędzy nimi była możliwa.

W celu komunikacji między różnymi protokołami wykorzystuje łącza *(ang. gateway)* - czyli urządzenia, które tłumaczącą rozkazy jednego protokołu na drugi. Kolejnym rozwiązaniem może być skonfigurowanie komputerów w taki sposób, by wykorzystywały kilka protokołów równocześnie, jednak i to rozwiązanie może prowadzić do dodatkowego obciążania sieci.

Do najważniejszych protokołów należą:

- TCP/IP
- IP

TCP/IP (ang. Transmission Control Protocol / Internet Protocol) -to zespół protokołów sieciowych używany w sieci Internet. Najczęściej wykorzystują go systemy Unixowe oraz systemy Windows, choć można stosować go również w systemach Novell NetWare. Zadanie protokołu TCP/IP polega na dzieleniu danych na pakiety odpowiedniej wielkości, ponumerowaniu ich w taki sposób, aby odbiorca mógł sprawdzić, czy dotarły wszystkie pakiety oraz ustawieniu ich we właściwej kolejności. Kolejne partie informacji wkładane są do kopert TCP, a te z kolei umieszczane są w kopertach IP.

Oprogramowanie TCP po stronie odbiorcy zbiera wszystkie nadesłane koperty, odczytując przesłane dane. Jeśli brakuje którejś koperty, wysyła żądanie ponownego jej dostarczenia. Pakiety wysyłane są przez komputery bez uprzedniego sprawdzenia, czy możliwa jest ich transmisja. Może się zdarzyć taka sytuacja, że do danego węzła sieci, gdzie znajduje się router, napływa więcej pakietów, aniżeli urządzenie może przyjąć, posegregować i przesłać dalej. Każdy router posiada bufor, który gromadzi pakiety czekające na wysłanie. Gdy bufor ulegnie całkowitemu zapełnieniu, nowo nadchodzące pakiety zostaną odrzucone i bezpowrotnie przepadną. Protokół, który obsługuje kompletowanie pakietów zażąda, więc wtedy ponownego ich wysłania.

IP (Internet Protocol) - to protokół do komunikacji sieciowej, gdzie komputer klienta wysyła żądanie, podczas gdy komputer serwera je wypełnia. Protokół ten wykorzystuje adresy sieciowe komputerów zwane adresami IP. Są to 32-bitowa liczby zapisywana, jako sekwencje czterech ośmiobitowych liczb dziesiętnych (mogących przybierać wartość od 0 do 255), oddzielonych od siebie kropkami. Adres IP dzieli się na dwie części: identyfikator sieciowy (network id) i identyfikator komputera (host id). Istnieje kilka klasy adresowych, o różnych długościach obydwu składników.

W celu ułatwienia zapamiętania adresów wprowadzono nazwy symboliczne, które tłumaczone są na adresy liczbowe przez specjalne komputery w sieci, zwane ***serwerami DNS***.

Do innych popularnych protokołów sieciowych należą:

- FTP
- SNMP
- SMTP
- CSMA/CD
- DNS
- DHCP
- Http
- ICMP

FTP (ang. File Transfer Protocol) - to protokół służący do transmisji plików. Przeważnie usługę ftp stosuje do przesyłania danych z odległej maszyny do lokalnej lub na odwrót. Protokół ten działa w oparciu o zasadę klient-serwer i korzystanie z usługi polega na użyciu interaktywnej aplikacji. Technologia FTP zapewnia ochronę stosując hasła dostępu.

SNMP (ang. Simple Network Managment Protocol) - to podstawowy protokół służący do zarządzania siecią. SNMP stanowi standard internetowy, jeżeli chodzi o zdalne monitorowanie i zarządzanie routerami, hostami oraz innymi urządzeniami sieciowymi.

SMTP (ang. Simple Mail Transfer Protocol) - jest podstawowym protokołem realizującym transfer poczty elektronicznej, SMTP należy do rodziny protokołów TCP/IP i służy do wysyłania poczty elektronicznej.

CSMA/CD (ang. Carrier Sense Multiple Access with Collision Detection) - to metoda wielodostępu do łącza sieci z wykrywaniem kolizji oraz badaniem stanu kanałów, stosowana w sieciach Ethernet w celu przydziału nośnika dla poszczególnych węzłów. Węzeł zaczyna nadawanie, kiedy nie wykryje w sieci transmisji z innego węzła, sprawdzając przez cały czas, czy nie doszło do kolizji. W przypadku zaistnienia kolizji próba transmisji zostaje ponowiona po przerwie o losowej długości.

DNS (ang. Domain Name Service) - protokół używany w sieci Internet obsługujący system nazywania domen. Umożliwia on nadawanie nazw komputerom, które są zrozumiałe i łatwe do zapamiętania dla człowieka, tłumacząc je na adresy IP. Nazywany czasem usługą BIND (BSD UNIX), DNS oferuje hierarchiczną, statyczną usługę rozróżniania nazw hostów. Administratorzy sieci konfigurują DNS używając listę nazw hostów oraz adresów IP. DNS nie posiada centralnego repozytorium przechowującego adresy IP maszyn w sieci. Dane dotyczące tych adresów dzielone są między wiele komputerów, zwanych serwerami DNS (nazw domenowych), które są zorganizowane hierarchicznie w formie drzewa. Początek drzewa nazywany jest korzeniem. Nazwy najwyższego poziomu składają się z dwuliterowych domen narodowych opartych na zaleceniach ISO 3166 (wyjątek stanowi brytyjska domen uk). Nadrzędna domena narodowa w Polsce oznaczona jest przez pl.

DHCP (ang. Dynamic Host Configuration Protocol) - to standardowy protokół przydzielający adresy IP poszczególnym komputerom. Serwer DHCP przypisuje adresy IP poszczególnym końcówkom.

HTTP (ang. HyperText Transfer Protocol) - to protokół internetowy, używany do obsługi stron WWW. HTTP stanowi podstawowy protokół, przy pomocy którego przebiega komunikacja między klientami i serwerami sieci Web. Jest to protokół poziomu aplikacji dla współpracujących ze sobą, hipermedialnych, rozproszonych systemów informacyjnych. HTTP jest bezstanowym i generycznym protokołem zorientowanym obiektowo. Cechą charakterystyczną tego protokołu możliwość wpisywania oraz negocjowania reprezentacji danych, co umożliwia budowę systemów niezależnie od typu transferowanych danych.

ICMP (ang. Internet Control Message Protocol) - jest to rozszerzenie protokołu IP (Internet Protocol). Protokół ICMP służy generowaniu komunikatów o występujących błędach, wysyłaniu pakietów testowych oraz komunikatów diagnostycznych związanych z protokołem IP.

Temat 8. <u>Rodzaje metod dostępu do sieci (rywalizacja, przesyłanie tokenu, priorytet żądań oraz przełączanie)</u>

http://www.teorialan.ttd.pl/metodydo.html

Każda sieć musi w jakiś sposób regulować dostęp do nośnika. Mechanizm regulacji dostępu do nośnika realizowany jest przez warstwę 2 modelu referencyjnego OSI (warstwę danych). W sieciach LAN dostęp do nośnika regulowany może być na jeden z czterech różnorodnych sposobów:

rywalizacji

przesyłania tokenu

priorytetu żądań

przełączania

Cisco switch

Przełączniki umożliwiają zmniejszenie obciążenia w sieci, poprzez jej podział na mikrosegmenty i tzw. **przełączanie (komutowanie)**. Polega to na tym, iż do jednego segmentu można przydzielić zaledwie jedną stacje roboczą, co znacznie redukuje rywalizację o dostęp do medium. Użytkownik otrzymuje całą szerokość pasma dla siebie. Każdy port switcha stanowi wejście do jednego segmentu sieci. W efekcie pracy, przykładowo przełącznika posiadającego 10 portów, jest uzyskanie 10 niezależnych segmentów z całą szerokością pasma (np. pełnych 10 Mbps w przypadku 10Base-T).

Hub - Nazywany jest również **koncentratorem.** Jest to urządzenie posiadające wiele **portów** służących do przyłączenia stacji roboczych zestawionych w **topologii gwiazdy.**

Hub 8-portowy

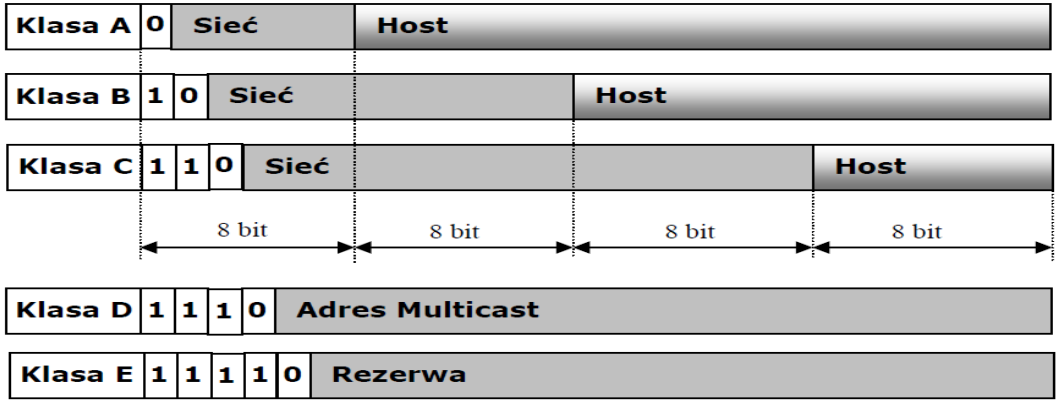
Komputery podłączone są do centralnego huba, który po nadejściu sygnału rozprowadza go do wszystkich linii wyjściowych.

Temat 9, 10 <u>Klasy adresów IPv4 Adresy IPv6</u>

Adres IP (w wersji 4 protokołu) składa się z 4 wartości, z których każda może przyjmować wartości od 0 do 255. Adresy internetowe możemy podzielić na dwie grupy: ***publiczne i lokalne.***

Klasa	Pierwsze 8 bitów adresu IP zapisanych w systemie dziesiętnym	Ile sieci	Ile komputerów w 1 sieci
A	1÷126	126	16,5 mln.
B	128÷191	16 tys.	65 tys.
C	192÷223	2 mln.	254
D	224÷239	Adresy Multicast	
E	240÷247	Rezerwa	

Tabela adresów IP v4



Podział adresów IP (32 bit, 4 oktety 8 bitowe) z wydzieloną częścią Sieci i Hostów

Adres prywatny IPv4 – adres IP przydzielany urządzeniom przyłączonym do sieci lokalnej (LAN). Na żądanie IETF, IANA zarezerwowała niektóre pule adresów do użytkowania prywatnego i opublikowała je w RFC 1918:

Adres sieci	Maska sieci	Dostępne adresy	Adres rozgłoszeniowy
10.0.0.0	255.0.0.0 (8 bitów)	10.0.0.0 – 10.255.255.255	10.255.255.255
172.16.0.0...172.31.0.0	255.255.0.0 (16 bitów)	172.16.0.0 – 172.31.255.255	172.16.255.255 ... 172.31.255.255
192.168.0.0…192.168.255.0	255.255.255.0 (24 bitów)	192.168.0.0 – 192.168.255.255	192.168.255.255

IPv6 (ang. Internet Protocol version 6) – protokół komunikacyjny, będący następcą protokołu IPv4, do którego opracowania przyczynił się w głównej mierze problem małej, kończącej się liczby adresów IPv4. Podstawowymi zadaniami nowej wersji protokołu jest zwiększenie przestrzeni dostępnych adresów poprzez zwiększenie długości adresu z 32-bitów do 128-bitów, uproszczenie nagłówka protokołu oraz zapewnienie jego elastyczności poprzez wprowadzenie rozszerzeń, a także wprowadzenie wsparcia dla klas usług, uwierzytelniania oraz spójności danych. Głównymi dokumentami opisującymi protokół są RFC2460 oraz RFC4291.

Adresowanie w sieci komputerowej.

1. Adres fizyczne

Adres fizyczny MAC (ang. Media Access Control) – unikatowy w skali światowej, nadawany przez producenta danej karty podczas produkcji, sprzętowy adres karty sieciowej Ethernet i Token Ring. unikatowy w skali światowej, nadawany przez producenta danej karty podczas produkcji.

Adres MAC jest 48-bitowy i zapisywany jest heksadecymalnie (szesnastkowo). Pierwsze 24 bity oznaczają producenta karty sieciowej, pozostałe 24 bity są unikatowym identyfikatorem danego egzemplarza karty.

Przykład adresu fizycznego karty sieciowej: **Physical Address : B8-88-E4-98-7E-E9**

2. Adresowanie IPv4

Adresowanie sieci w przypadku małych sieci komputerowych można oprzeć na klasowości adresów IP. Korzystając z metody VLSM możemy zmieniać długość maski podsieci i wpływając w ten sposób na liczbę hostów w danej podsieci.

VLSM (Variable Length Subnet Mask) – cecha niektórych protokołów trasowania umożliwiająca podzielenie i rozróżnianie podsieci z już istniejących podsieci.

VLSM umożliwia podział adresu np. klasy C (254 hosty, maska 255.255.255.0). Aby informacja o sieciach była dobrze rozprowadzana pomiędzy routerami, odpowiednie protokoły trasowania muszą wymieniać pomiędzy sobą pełną informację o sieciach łącznie z maskami.

VLSM wspierają następujące protokoły trasowania: RIP v2, EIGRP,EIGRP, OSPF, IS-IS, BGP.

Tabela przedstawia długość masek podsieci oraz liczbę adresów IP które można przydzielić hostom.

Maska	**Liczba adresów IP**	**Liczba adresów użytecznych** (czyli tych których możemy przypisać hostom).
255.255.255.252 /30	4	2
255.255.255.248 /29	8	6
255.255.255.240 /28	16	14
255.255.255.224 /27	32	30
255.255.255.192 /26	64	62
255.255.255.128 /25	128	126
255.255.255.0 /24	256	254
255.255.254.0 /23	512	510
255.255.252.0 /22	1024	1022

Przykład: Adres prywatny sieci klasy A - 10.0.0.0 Maska 255.255.255.128 /25 liczba hostów 126

Maska	Adres sieci	Adres rozgłoszeniowy	Adresy hostów.
255.255.255.128 /25	10.0.0.0	10.0.0.127	od 10.0.0.1 do 10.0.0.126

Stosując metodę ze zmienną maską VLSM zaczynamy dzielić sieć od tej podsieci do której trzeba przypisać największą liczbę hostów.

Literatura:

Urządzenia techniki komputerowej – Tomasz Kowalski
Sam składam komputer – Bartosz Danowski, Andrzej Pytchla

Wikipedia- wolna encyklopedia internetowa

Strona internetowa:

http://standards.ieee.org/regauth/oui/oui.txt

http://itpedia.pl/index.php/LAN#Sposoby_transmisji_i_adresowania_w_LAN

http://www.bryk.pl/teksty/liceum/pozosta%C5%82e/informatyka/15947-protoko%C5%82y_sieciowe.html

http://sieci.res.pl/%21start.htm

http://www.teorialan.ttd.pl/metodydo.html

Przykłady podziału na podsieci strona WWW: http://slow7.pl/sieci-komputerowe/90-sow-kilka-o-adresacji-sieci

Opracował Mirosław Ruciński

e-mail: nauczyciel.zsen@gmail.com