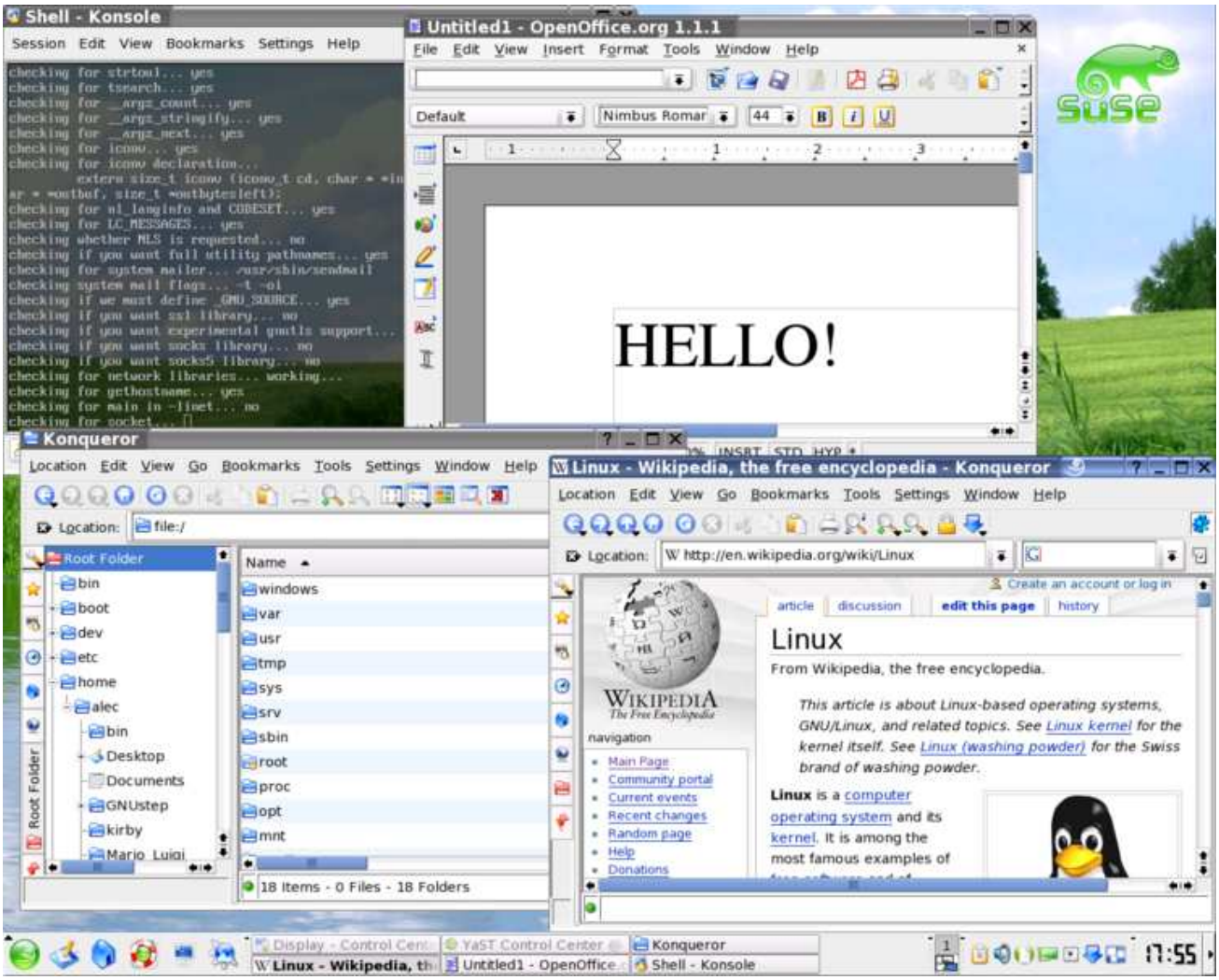
System operacyjny



Przykład graficznego interfejsu systemu operacyjnego wraz z uruchomionym oprogramowaniem

System operacyjny (ang. skrót ***OS Operating System***) – oprogramowanie, które zarządza sprzętem oraz aplikacjami komputera. Podstawą wszystkich systemów operacyjnych jest wykonywanie podstawowych zadań takich jak: kontrolowanie i przypisywanie pamięci, przydział czasu procesora, obsługa urządzeń, ustalanie połączeń sieciowych oraz zarządzanie plikami. Wiele systemów operacyjnych posiada środowiska graficzne ułatwiające ich obsługę.

Określenie to jednak nie jest w pełni ścisłe. Czasem potocznie[*potrzebne źródło*] mówi się tak mając na myśli całość oprogramowania dostarczanego z zakupionym komputerem (zobacz: dystrybucja), czasem samo jądro systemu operacyjnego, czasem program rozruchowy, czasem z kolei chodzi o całą rodzinę systemów operacyjnych (np. Microsoft Windows).

Spis treści

- 1 Zasoby sprzętowe
- 2 Zarządzanie zasobami
- 3 Budowa systemu operacyjnego
- 4 Systemy operacyjne
  - 4.1 Amiga
  - 4.2 Apple
  - 4.3 Atari
  - 4.4 Be i pochodne
  - 4.5 DEC/Compaq
  - 4.6 IBM
  - 4.7 ICL
  - 4.8 Microsoft i pochodne
  - 4.9 Novell
  - 4.10 NeXT
  - 4.11 Unisys
  - 4.12 UNIX i jego pochodne
  - 4.13 systemy czasu rzeczywistego (realtime systems)
  - 4.14 Pozostałe
- 5 Systemy operacyjne pracujące na maszynie wirtualnej
- 6 Język programowania jako system operacyjny
- 7 Zobacz też

Zasoby sprzętowe

Zasoby sprzętowe zarządzane przez system operacyjny:

- *Procesor* – przydział czasu procesora,
- *Pamięć*
  - alokacja przestrzeni adresowej dla procesów,
  - transformacja adresów,
- *Urządzenia zewnętrzne*
  - udostępnianie i sterowanie urządzeniami pamięci masowej np. dysk twardy.
  - alokacja przestrzeni dyskowej,
  - udostępnianie i sterowanie drukarkami, skanerami, aparatami itp.
- *Informacja* (system plików)
  - organizacja i udostępnianie informacji,
  - ochrona i autoryzacja dostępu do informacji.

Zarządzanie zasobami

Zarządzanie zasobami w systemie wielozadaniowym polega na takim ich rozdzieleniu pomiędzy użytkowników, aby każdy z nich miał wrażenie, że pracuje na własnym komputerze.

Główne zadania systemu operacyjnego podczas zarządzania zasobami systemu komputerowego:

- tworzenie deskryptora zasobu,
- usuwanie deskryptora zasobu,
- realizacja żądania przydziału,
- zwolnienie i odzyskiwanie zasobu.

Zarządzanie zasobami systemu komputerowego:

- przydział zasobów,
- synchronizacja dostępu do zasobów,
- ochrona i autoryzacja dostępu do zasobów,
- odzyskiwanie zasobów,
- rozliczanie – gromadzenie danych o wykorzystaniu zasobów.

Zarządzanie procesem – proces to program w stanie uruchomiony, każdy proces wymaga przydziału pewnych zasobów, włączając w to czas procesora, pamięć, pliki oraz urządzenia wejścia/wyjścia, aby w pełni wykonać swoje zadanie. System operacyjny jest odpowiedzialny w fazie zarządzania procesami za:

- tworzenie i usuwanie procesu,
- wstrzymywanie i przywracanie procesu,
- zapewnienie mechanizmów pozwalających na synchronizację procesów oraz komunikację między procesami.

Zarządzanie pamięcią operacyjną – pamięć to duża tablica słów lub bajtów, każda z własnym adresem, pamięć jest szybko dostępna i dzielona jest pomiędzy procesor oraz urządzenia wejścia/wyjścia. Pamięć główna jest ulotnym miejscem przechowywania danych, traci swoją zawartość w czasie awarii systemu. System operacyjny jest odpowiedzialny w fazie zarządzania pamięcią za:

- utrzymywanie informacji która część pamięci jest aktualnie używana i przez kogo,
- decydowania który proces powinien zostać wczytany do pamięci jeżeli pamięć jest wolna,
- przydzielanie i zwalnianie pamięci.

Zarządzanie plikami – plik jest zbiorem informacji zdefiniowanym przez twórcę pliku. Zazwyczaj, pliki reprezentują programy (źródła programów lub pliki wykonywalne) oraz dane. System operacyjny jest odpowiedzialny w fazie zarządzania plikami za:

- tworzenie i kasowanie plików,
- tworzenie i kasowanie katalogów,
- wsparcie dla użytkowników końcowych przy operacjach na plikach,
- mapowanie plików na nośniku danych,
- tworzenie kopii plików.

Zarządzanie wejściem/wyjściem – system wejścia/wyjścia składa się z: systemu buforowania, interfejsu urządzeń głównych, sterowników (kontrolerów) dla specyficznych urządzeń.

Zarządzenie nośnikami danych – pamięć główna jest ulotna i często za mała aby obsłużyć wszystkie programy i dane, dlatego stosuje się nośniki danych (najczęściej dysk twardy) do

powiększania tej pamięci tak zwanej pamięć drugiego rzędu, na napędach tych mapuje się pamięć główną. System operacyjny jest odpowiedzialny w fazie zarządzania nośnikami danych za:

- zarządzanie wolną pamięcią,
- alokacją zapisu,
- planowaniem dysku.

Budowa systemu operacyjnego

Przyjęto podział na trzy główne elementy budowy systemu operacyjnego:

- jądro systemu wykonujące ww. zadania,
- powłoka – specjalny program komunikujący użytkownika z systemem operacyjnym,
- system plików – sposób zapisu struktury danych na nośniku.

Systemy operacyjne

Amiga

- AmigaOS
- AROS Research Operating System (AROS)
- MorphOS

Apple

- Apple DOS, ProDOS
- GS/OS
- Mac OS
- Mac OS X, Mac OS X Server
- A/UX
- Lisa OS

nieukończone projekty:

- Rhapsody

Atari

- Atari TOS
- MultiTOS
- FreeMiNT

Be i pochodne

- BeOS
- BeIA
- NewOS/Haiku
- yellowTAB Zeta

DEC/Compaq

- AIS
- OS-8
- RSTS/E
- RSX
- RT-11
- TOPS: TOPS-10, TOPS-20
- VMS (później przemianowany na OpenVMS)

IBM

- OS/2
- AIX
- OS/400
- OS/390
- VM/CMS
- DOS/VSE
- DOS/360
- OS/360
- MFT
- MVT
- PC-DOS
- SVS
- MVS
- TPF
- ALCS
- z/OS

ICL

- EXEC
- JEAN
- MINIMOP
- GEORGE

Microsoft i pochodne

- MS-DOS
  - PC-DOS, DR-DOS, FreeDOS, DOS, QDOS
- Microsoft Windows: 1.0, 2.0, 3.x, 95/98/98 SE/Me, CE, NT/2000/XP/2003/FLP/Vista
  - PetrOS, ReactOS

Novell

- NetWare
- Novell DOS

Zobacz też: SuSE Linux

NeXT

- NeXTStep

Unisys

- MCP(Master Control Program)
- OS 2200.

UNIX i jego pochodne

- AIX
- BSD, FreeBSD, NetBSD, OpenBSD, DragonFly BSD, DesktopBSD, PC-BSD
- Digital UNIX
- HP-UX
- IRIX
- Mac OS X
- Minix
- OSF/1
- SCO UNIX
- Sun Solaris (dawniej SunOS)
- System V
- QNX
- Ultrix
- Venix
- Xenix
- GNU/Linux (system GNU z jądrem Linux)
- GNU/Hurd (system GNU z jądrem Hurd),
- Linux

systemy czasu rzeczywistego (realtime systems)

- LynxOS
- OS9
- Phoenix-RTOS
- QNX
- Nut/OS
- RT-Linux
- SenseOS
- VxWorks
- Suse Linux Enterprise Real Time
- MicroC/OS-II

.

Pozostałe

- Agnix
- Amoeba

- AtariDOS
- Commodore DOS (zapisany w stacji dysków)
- AtheOS/Syllable
- Athene
- CP/J
- CP/M
- CROOK
- eComStation
- Egzekutor RTX
- EMOS
- EPOC32
- GEOS
- Inferno
- IOS
- iRMX
- ISIS-II
- Kylin
- MenuetOS
- Mikros
- Multics
- Palm OS
- Quarn OS
- SkyOS
- Symbian
- UDOS
- Unununium
- System V7

Systemy operacyjne pracujące na maszynie wirtualnej

Możliwe jest uruchomienie systemu operacyjnego na maszynie wirtualnej. Przykłady to: Argante, Inferno a także *User Mode Linux*, czyli Linux skonfigurowany w ten sposób, by mógł działać jako system wirtualny w postaci procesu działającego pod kontrolą drugiego Linuksa. Systemy wirtualne dzielone są na para-wirtualne i w pełni wirtualne. Te ostatnie umożliwiają pracę niemodyfikowanego OS_2 w środku innego systemu OS_1 z pełną, (niemulowaną) szybkością, np. OS_2 – Windows Vista wewnątrz OS_1 Linuksa z np Xen. Pełna wirtualizacja OS była dostępna od dawna na superkomputerach, nowe instrukcje procesorów rozszerzają ją na komputery osobiste.

Język programowania jako system operacyjny

Funkcję systemu operacyjnego spełniać może Implementacja określonego języka programowania. Miało to miejsce szczególnie w historycznych już czasach dominacji komputerów 8-bitowych. Rolę powłoki systemu operacyjnego spełnia w tym przypadku interpreter poleceń języka. Dlatego funkcję takiego systemu może pełnić implementacja danego języka oparta na interpretacji lub mieszana (interpretacyjno-kompilacyjna).

W komputerach 8-bitowych często interpreter języka był przechowywany w pamięci ROM i stanowił podstawowy system operacyjny. Najbardziej znanym przykładem takiego języka jest BASIC stosowany szeroko w komputerach 8-bitowych - w zasadzie jedynym wyjątkiem jest rodzina

8-bitowych Atari, bo BASIC jest nie we wszystkich modelach, a DOS ma zawsze własną powłokę. Innym, historycznym już przykładem, jest język Jean, implementowany w dużych systemach komputerowych (np. serii ODRA 1300), który mógł pracować zarówno pod kontrolą innego systemu operacyjnego (np. GEORGE 3), jak również samodzielnie jako mały system operacyjny o charakterze konwersacyjnym.

Językami programowania (a właściwie pewnymi implementacjami języków programowania), które także stanowią samodzielne systemy operacyjne są również FORTH oraz Smalltalk. Język i zarazem system operacyjny FORTH szczególnie zastosowanie znajdował w systemach sterowania automatyki przemysłowej. Jest to najlepszy przykład języka w interpretacyjno-kompilacyjnego, w którym wprowadzane słowa są interpretowane i natychmiast wykonywane, natomiast definicje słów są natychmiast kompilowane. Smalltalk to pierwszy język "czysto obiektowy", który w wielu swoich implementacjach buduje własne środowisko stanowiące system operacyjny komputera.

W systemach serii MERA 300 funkcję systemu operacyjnego mógł pełnić nawet asembler o nazwie MOTIS.

Zobacz też

- Historia systemu operacyjnego Unix
- testbed
- systemy operacyjne opisane na Wikipedii
- Kubuntu
- Ubuntu
- Gentoo
- Debian
- openSUSE
- Arch Linux
- Fedora Core
- Mandriva
- Slackware
- PLD

File Allocation Table

FAT (akronim z ang. *File Allocation Table*) – system plików powstały pod koniec lat 70. Zastosowany w systemach operacyjnych, m.in. DOS i Windows. Podobnie jak sam DOS, wywodzi się z systemów CP/M. Określa on rozmieszczenie plików, katalogów i wolnej przestrzeni na takich nośnikach danych jak dyskietki i twarde dyski. Najważniejszym elementem systemu jest tablica informująca o rozmieszczeniu plików na partycji (FAT) - od nazwy tej tablicy pochodzi nazwa systemu.

	FAT12	FAT16	FAT32	exFAT (FAT64)
Developer			Microsoft	

Pełna nazwa	File Allocation Table			
	(wersja 12-bit)	(wersja 16-bit)	(wersja 32-bit)	(wersja 64-bit)
Wprowadzona w	1980 (Seattle QDOS)	Listopad 1987, (Compaq DOS 3.31)	Sierpień 1996 (Windows 95 OSR2)	Marzec 2008 (Vista SP1)
Indentyfikator Partycji	0x01 (MBR)	0x04, 0x06, 0x0E (MBR)	0x0B, 0x0C (MBR) EBD0A0A2-B9E5-4433-87C0-68B6B72699C7 (GPT)	czeka na aktualizacje
Struktura				
Zawarty katalog	Tabela			
Alokacja pliku	Lista			
Złe bloki	Tagowanie klastrów			
Ograniczenia				
Największa wielkość pliku	4 GiB			16 EiB
Największa ilość klastrów	4,077 (2^{12}-19)	65,517 (2^{16}-19)	268,435,437 (2^{28}-19)	czeka na aktualizację
Długość najdłuższej nazwy pliku	8.3 (nazwy plików)		255 znaków, gdy używany jest LFN/vfat	czeka na aktualizację
Największa pojemność woluminu	32 MiB	2 GiB 4 GiB z 64kb klastrami	8 TiB	2^{64} bajtów (16 EiB)

Spis treści

- 1 Typy FAT
- 2 Sektor
- 3 Klaster
- 4 Zalety i wady tablicy alokacji
- 5 Regiony partycji FAT
- 6 Historia systemu FAT

Typy FAT

W czasach gdy projektowane nośniki danych miały niewielką pojemność (dyskietka 180kB), z biegiem czasu obsługiwane były coraz większe nośniki.

Aktualnie istnieją cztery rodzaje FAT:

- FAT12

- FAT16
- FAT32
- exFAT (FAT64)

Podstawowa różnica między nimi to liczba bitów, na których koduje się numery jednostek alokacji plików zwanych klastrami. Liczbę tę podaje się jako wyróżnik w nazwie systemu w FAT (podana w nazwie).

Sektor

Nośniki danych typu dyskietka, dysk itp. przechowują informacje w porcjach zwanych sektorami. Sektor jest zawsze w całości odczytywany i zapisywany. Większość urządzeń posiada sektory o wielkości 512 bajtów (0,5kB).

Klaster

W formacie FAT partycja (poza początkowymi zarezerwowanymi sektorami) jest podzielona na klastry (jednostki alokacji pliku). Każdy klaster składa się z jednego lub kilku sektorów, klastry są numerowane. System operacyjny na podstawie numeru klastra oblicza numer logiczny sektora (numer sektora od początku partycji), a na tej podstawie numer ścieżki, głowicy i sektora na ścieżce (dawniej fizyczne położenie na dysku), identyfikując jednoznacznie sektor i dokonując odczytu lub zapisu wybranego sektora.

Klaster w całości jest przydzielony jednemu plikowi. Plik w katalogu zawiera numer pierwszego klastra pliku, gdzie znajdują się dalsze części pliku opisuje wpis w FAT. W tablicy FAT pod numerem odpowiadającym numerowi pierwszej części pliku jest umieszczony numer kolejnego klastra przydzielonego plikowi lub liczba z zakresu FFF8h-FFFFh, jeśli to jest ostatni klaster pliku. Jeżeli dany klaster jest wolny, to w FAT odpowiada mu wpis 0000h, a FFF7h oznacza uszkodzony klaster.

> **Przykład**
> Wielkość klastra zależy od maksymalnego numeru klastra zależnego od wersji FAT, czyli 12, 16 albo 32, jednak ta nie określa bezpośrednio liczby dostępnych klastrów. Np. w FAT12 będzie ich mniej niż 4096 (2^{12}), ponieważ niektóre z nich mają znaczenie wyłącznie systemowe i nie są dostępne dla użytkownika. Liczba dostępnych klastrów jest jednocześnie maksymalną liczbą możliwych do zapisania plików na partycji. FAT12 użyjemy dla dysku o pojemności 20MiB – dysk ten ma 40960 sektorów, więc klaster musi zawierać 10 sektorów, co odpowiada 5KiB.

Zalety i wady tablicy alokacji

Tablica FAT umożliwia szybkie odszukanie miejsca dla nowego pliku lub dalszej części, łatwe odszukiwanie kolejnych części plików. Wadą systemu FAT jest to, że dla partycji o dużej pojemności klaster jest równie duży i znaczna część pozostaje pusta (średnio pół klastra na plik), w trakcie zapisywania i kasowania plików ulegają one fragmentacji (kolejne fragmenty pliku mogą leżeć w znacznej odległości od siebie), a przestawianie głowic dysku zajmuje czas. Inną wadą jest to, że każde założenie, skasowanie, każda zmiana wielkości pliku pociąga za sobą konieczność zmiany tablicy FAT, co przy niepoprawnym działaniu komputera może doprowadzić do utraty wszystkich danych na partycji.

Regiony partycji FAT

Partycja systemu FAT składa się z 4 regionów:

1. *zarezerwowany* (z boot sectorem) – a w nim tablica BPB (Bios Parameter Block) oraz program ładujący system operacyjny (boot loader) dla partycji systemowej. Blok BPB zawiera informacje potrzebne do wyliczenia położenia i rozmiaru pozostałych regionów.
2. *tablica alokacji* (tablica FAT) – przechowywana zaraz za boot sektorem struktura, zajmująca kilka sektorów, która zawiera informacje dla systemu operacyjnego na temat klastrów. Każda pozycja w tablicy FAT odpowiada jednemu klastrowi. Sposób kodowania informacji opisano wyżej. Na partycji może być kilka kopii tablicy FAT, zazwyczaj dwie.
3. *katalog główny* (w FAT32 nie istnieje w tej formie) – katalog główny (root directory) i jego podkatalogi zawierają nazwę pliku, atrybuty, informacje o czasie utworzenie i modyfikacji, wskaźnik na pierwszy klaster z danymi.
4. *region danych* – zajmowany przez podkatalogi i wszystkie pliki; podzielony na logiczne bloki zwane klastrami.

Historia systemu FAT

System plików FAT został pierwszy raz zastosowany w sierpniu 1980 roku razem z pierwszą wersją QDOS-a, czyli poprzednika systemów PC-DOS oraz MS-DOS. Pierwsza wersja FAT oznaczana jest jako **FAT12**. Jako system plików przeznaczony dla dyskietek miał on wiele ograniczeń. Brakowało w nim wsparcia dla katalogów. Adresy klastrów miały tylko 12 bitów, co ograniczało rozmiar partycji do ok 2MiB. W tym czasie dyskietki miały 360KiB.

W roku 1983 Microsoft wprowadził nową wersję FAT razem z MS-DOS w wersji 2. Nowy system plików powstał z myślą o dyskach twardych i pozwala już na tworzenie katalogów. Adresy klastrów były 16-bitowe, co dawało teoretycznie 65536 numerów. Dla rozmiaru klastra 512 bajtów można było uzyskać całe 32MiB pojemności. FAT16 doskonale nadaje się do 10-20MiB dysków z komputerów XT. Pliki identyfikowano za pomocą 8-literowej nazwy oraz 3-literowego rozszerzenia, np. `plik1234.txt`. Nazwa mogła zawierać tylko znaki alfanumeryczne, _ i `-`. W samym systemie plików kropka (`.`) nie jest częścią nazwy, jednak używa się jej w systemie w celu odróżnienia nazwy podstawowej od rozszerzenia.

Kiedy rozmiary dysków się zwiększyły, za nimi podążył rozmiar klastra, który powiększono do 8192 bajtów. W efekcie można było stworzyć system plików o „zawrotnym” rozmiarze 512MiB. Niestety taki zabieg spowodował pojawienie się bardzo silnej fragmentacji. Jeżeli ktoś zapisał plik o rozmiarze 1 bajta, to w systemie FAT16 zajmował on cały 8192-bajtowy klaster. W ten sposób marnowało się 8191 bajtów miejsca na dysku.

Z drugiej strony użytkownicy komputerów chcieli nadawać plikom dłuższe nazwy zawierające znaki narodowe. W Windows 95 wprowadzono nakładkę na system plików nazwaną **VFAT** (Virtual FAT). Wsparcie dla nakładki zawarto też w systemie Windows NT 4.0.

W roku 1997 rozmiar partycji FAT16 stał się zbyt mały. Klaster nie mógł być większy niż 32KiB, co dawało partycje o pojemności do 2GiB. Microsoft wprowadził nową wersję FAT32, zawierającą teoretycznie 32-bitowe numery klastrów. W rzeczywistości tylko 28-bitów było dostępnych dla numeracji. Oznaczało to możliwość adresowania do 268.435.438 klastrów. Partycje tego typu mogłyby mieć rozmiar wielu TiB, jednak ograniczenia napisanego przez Microsoft programu ScanDisk spowodowały wprowadzenie ograniczenia do 4.177.920 klastrów, co dawało partycje o

rozmiarze ok. 124.55GiB (więcej informacji na ten temat). FAT32 jest obsługiwany przez systemy od wersji Windows 95 OSR 2 wzwyż (z wyjątkiem NT4).

Inne systemy operacyjne, jak OS/2, Linux, FreeBSD, oraz BeOS też zostały wyposażone w obsługę FAT, FAT32 oraz VFAT. System Mac OS X w komputerach Apple również obsługuje FAT, ale nie na partycji startującej.

Obecnie system FAT jest zastępowany w produktach Microsoft przez NTFS, który jest wydajniejszy i pewniejszy (jednak nie pozbawiony wad w stosunku do FAT). Systemy operacyjne pochodzące z innych źródeł również wykorzystują własne systemy plików (np. Ext3 w Linuksie). Mimo to FAT jest nadal powszechnie używany w związku z jego dostępnością i prostotą. Używa się go na dyskach o małej pojemności, dyskietkach, kartach pamięci flash używanych np. w kamerach i napędach USB oraz wszędzie tam, gdzie z powodów technicznych nie można zastosować bardziej zaawansowanego systemu bądź użytkownikowi zależy na kompatybilności (NTFS nie jest obsługiwany w starszych wersjach Windows).

Microsoft wraz z Windows Vista SP1 oraz Windows Embedded CE 6.0 wprowadził nowy stystem plikow FAT: exFAT(FAT64). exFAT jest systemem plików stworzonym specjalnie na potrzeby pamięci flash, wg. Microsoftu FAT64 może być używany wszędzie tam gdzie system plików NTFS nie jest najlepszym rozwiązaniem, ze względu na dużą nadmiarowość struktury danych.

WYBRANE KOMENDY SO WINDOWS XP / MS DOS.

ASSOC	Wyświetla lub modyfikuje skojarzenia rozszerzeń plików.
AT	Planuje wykonanie poleceń i programów.
ATTRIB	Wyświetla lub zmienia atrybuty pliku.
BREAK	Wyłącza lub włącza rozszerzone sprawdzanie klawiszy CTRL+C.
CACLS	Wyświetla lub modyfikuje listy kontroli dostępu (ACL) plików.
CALL	Wywołuje jeden program wsadowy z innego.
CD	Wyświetla lub zmienia nazwę bieżącego katalogu.
CLS	Czyści ekran.
CMD	Uruchamia nowe wystąpienie interpretera poleceń systemu Windows.
CONVERT	Konwertuje woluminy FAT na woluminy NTFS. Nie można konwertować
COPY	Kopiuje jeden lub wiele plików w inne miejsce.
DATE	Wyświetla lub ustawia datę.
DEL	Usuwa jeden lub wiele plików.
DIR	Wyświetla listę plików i podkatalogów katalogu.
ECHO	Wyświetla komunikaty lub wyłącza i włącza echo poleceń.
FIND	Wyszukuje ciąg tekstowy w pliku lub plikach.
FORMAT	Formatuje dysk do użytku w systemie Windows.
HELP	Podaje informacje o poleceniach systemu Windows.
LABEL	Tworzy, zmienia lub usuwa etykietę(etykiety) woluminu dysku.
MD	Tworzy katalog.
MKDIR	Tworzy katalog.
PATH	Wyświetla lub ustawia ścieżkę przeszukiwania dla plików wykonywalnych.
PRINT	Drukuje plik tekstowy.
PROMPT	Zmienia znak zachęty wiersza polecenia systemu Windows.
RD	Usuwa katalog.
RECOVER	Odzyskuje możliwe do odczytania informacje z uszkodzonego dysku.
REM	Oznacza komentarze w pliku wsadowym lub pliku CONFIG.SYS.
REN	Zmienia nazwę pliku lub plików.

RENAME	Zmienia nazwę pliku lub plików.
RMDIR	Usuwa katalog ale nie może być w nim plików.
SUBST	Przypisuje ścieżce literę dysku.
TIME	Wyświetla lub ustawia czas systemowy.
TYPE	Wyświetla zawartość pliku tekstowego.
VER	Wyświetla wersję systemu Windows.
VOL	Wyświetla etykietę oraz numer seryjny dysku.
XCOPY	Kopiuje pliki i katalogi.

Sieć komputerowa

Sieć komputerowa - grupa komputerów lub innych urządzeń połączonych ze sobą w celu wymiany danych lub współdzielenia różnych zasobów, na przykład:

- korzystania ze wspólnych urządzeń, np. drukarek, skanerów,
- korzystania ze wspólnego oprogramowania,
- korzystania z centralnej bazy danych,
- przesyłania informacji między komputerami (komunikaty, listy, pliki).

Spis treści

- 1 Topologie okablowania sieci komputerowych
- 2 Elementy tworzące sieć komputerową
- 3 Znane sieci
- 4 Zobacz też
- 5 Linki zewnętrzne

Topologie okablowania sieci komputerowych

- gwiazda - komputery są podłączone do jednego punktu centralnego, koncentratora (koncentrator tworzy fizyczną topologię gwiazdy, ale logiczną magistralę) lub przełącznika (jedna z częstszych topologii fizycznych Ethernetu)
- gwiazda rozszerzona - posiada punkt centralny (podobnie jak w topologii gwiazdy) i punkty poboczne (jedna z częstszych topologii fizycznych Ethernetu)
- hierarchiczna - budowa podobna do drzewa binarnego
- szyna (magistrala) - komputery współdzielą jedno medium kablowe
- pierścień - komputery są połączone pomiędzy sobą odcinkami kabla tworząc zamknięty pierścień (np. topologia logiczna Token Ring)
- pierścień podwójny - komputery są połączone dwoma odcinkami kabla (np. FDDI)
- sieć (ang. mesh) - oprócz koniecznych połączeń sieć zawiera połączenia nadmiarowe; rozwiązanie często stosowane w sieciach, w których jest wymagana wysoka bezawaryjność.

Elementy tworzące sieć komputerową

- serwer sieciowy, zazwyczaj powinien to być komputer o dużej mocy obliczeniowej, zarówno wydajnym jak i pojemnym podsystemie dyskowym niezbędnym do przechowywania oprogramowania i danych użytkowników. Na maszynie tej można uruchomić aplikacje realizujące usługi sieciowe, również nazywane serwerami.
- komputery - stacje robocze, (terminale), na których instalujemy oprogramowanie sieciowe nazywane klientem.
- media transmisji - kable miedziane, światłowody, fale radiowe.
- osprzęt sieciowy - karty sieciowe, modemy, routery, koncentratory (huby), przełączniki (switche), access pointy.
- zasoby sieciowe - wspólny sprzęt, programy, bazy danych.
- oprogramowanie sieciowe - to programy komputerowe, dzięki którym możliwe jest przesyłanie informacji między urządzeniami sieciowymi. Rozróżnia się trzy podstawowe rodzaje oprogramowania sieciowego:
    - klient-serwer (system użytkownik) - system, w którym serwer świadczy usługi dołączonym stacjom roboczym. W systemie tym programy wykonywane są w całości lub częściowo na stacjach roboczych.
    - host-terminal (system baza) - do komputera głównego (hosta) dołączone zostają terminale lub komputery emulujące terminale. W systemie tym programy wykonywane są na hoście.
    - peer-to-peer - połączenia bezpośrednie; każdy komputer w sieci ma takie same prawa i zadania. Każdy pełni funkcję klienta i serwera.

Znane sieci

- Internet
- ARPANET - przodek Internetu
- ALOHAnet
- BITNET

Zobacz też

- Internet, Intranet
- sieć lokalna, sieć rozległa, sieć szkieletowa
- protokoły komunikacyjne
- architektura sieci

Sieć lokalna

Sieć lokalna (ang. *Local Area Network* stąd używany także w języku polskim skrót **LAN**) (wewnętrzna sieć) - najmniej rozległa postać sieci komputerowej, zazwyczaj ogranicza się do jednego budynku lub kilku pobliskich budynków (np. bloków na osiedlu).

Technologie stosowane w sieciach lokalnych można podzielić na rozwiązanie oparte na przewodach (kable miedziane, światłowody) lub komunikacji radiowej (bezprzewodowe). W sieciach lokalnych

przewodowych najczęściej używaną technologią jest Ethernet (za pośrednictwem kart sieciowych i urządzenia pośredniczącego huba tzw. koncentratora funkcję tę może pełnić również switch). Czasem są to takie urządzenia, jak np. port szeregowy, port równoległy czy port podczerwieni. W sieciach lokalnych bezprzewodowych najczęściej używaną technologią jest WLAN, zwany także Wi-Fi, określony standardami IEEE 802.11. Sieci lokalne podłączone są często do Internetu wspólnym łączem, takim jak SDI (obecnie coraz rzadziej stosowane), DSL, ADSL lub coraz częściej modemem kablowym od dostawcy TV kablowej.

Sieci lokalne mogą być budowane w oparciu o różne topologie, takie jak gwiazda (najczęściej stosowana), magistrala, pierścień, drzewo czy siatka.

Zobacz też

- Intranet
- Ethernet
- Karta sieciowa,
- Wtyczka RJ-45
- routing
- MAN,
- WAN
- WLAN
- Trans-net

Sieć rozległa

Sieć WAN (z ang. Wide Area Network, rozległa sieć komputerowa) - sieć komputerowa znajdująca się na obszarze wykraczającym poza jedno miasto (bądź kompleks miejski).

Główne cechy sieci WAN

- Łączą ze sobą urządzenia rozmieszczone na dużych obszarach geograficznych (np. kraju, kontynentu);
- W celu zestawienia łącza lub połączenia między dwoma miejscami korzystają z usług operatorów telekomunikacyjnych, np. TP S.A., NASK, Energis;
- Wykorzystują różne odmiany transmisji szeregowej.

Sieć WAN działa w warstwie fizycznej oraz warstwie łącza danych modelu odniesienia OSI. Łączy ona ze sobą sieci LAN, które są zazwyczaj rozproszone na dużych obszarach geograficznych. Sieci WAN umożliwiają wymianę ramek i pakietów danych pomiędzy routerami i przełącznikami oraz obsługiwanymi sieciami LAN.

Standardy sieci WAN są opracowywane przez organizacje, takie jak:

- Sektor Normalizacji Telekomunikacji Międzynarodowego Związku Telekomunikacyjnego (ITU-T, ang. *International Telecommunication Union-Telecommunication Standardization Sector*), dawniej *Committee for International Telegraph and Telephone* (CCITT);
- Międzynarodowa Organizacja Normalizacyjna (ISO, *International Organization for Standardization*);

- Grupa Robocza ds. Technicznych Internetu (IETF, *Internet Engineering Task Force*);
- Stowarzyszenie Przemysłu Elektronicznego (EIA, *Electronic Industries Association*).

Zobacz też

- ARPANET
- sieć szkieletowa
- LAN
- MAN

Protokoły komunikacyjne

Protokoły komunikacyjne to zbiór ścisłych reguł i kroków postępowania, które są automatycznie wykonywane przez urządzenia komunikacyjne w celu nawiązania łączności i wymiany danych. Dzięki temu, że połączenia z użyciem protokołów odbywają się całkowicie automatycznie, typowy użytkownik zwykle nie zdaje sobie sprawy z ich istnienia i nie musi o nich nic wiedzieć.

Klasyczne protokoły, których pierwowzorem był protokół teleksu, składają się z trzech części:

- procedury powitalnej (tzw. "handshake"), która polega na przesłaniu wzajemnej podstawowej informacji o łączących się urządzeniach, ich adresu (np. nr telefonu), szybkości i rodzaju transmisji itd.
- właściwego przekazu danych
- procedury analizy poprawności przekazu (np. sprawdzania sum kontrolnych) połączonej z procedurą pożegnania, żądaniem powtórzenia transmisji lub powrotem do procedury powitalnej

Przesyłana informacja może być porcjowana – protokół musi umieć odtworzyć informację w postaci pierwotnej.

Protokołami tego rodzaju posługują się:

- teleksy
- faksy
- modemy
- programy komputerowe
- wiele innych urządzeń, włącznie z np. pilotami do telewizorów

Protokoły służące programom komputerowym do porozumiewania się między sobą poprzez Internet są określone przez IETF w dokumentach zwanych RFC.

Warstwy

Przesyłanie danych komputerowych to niezwykle trudny proces, dlatego rozdzielono go na kilka "etapów", warstw. Warstwy oznaczają w istocie poszczególne funkcje spełniane przez sieć. Najbardziej powszechny sposób organizacji warstw komunikacji sieciowej to Model OSI.

Popularne protokoły wysokopoziomowe (*aplikacyjne*) i ich standardowe porty:

- BOOTP – serwer 67, klient 68
- DNS – 53
- Finger – 79
- FTP – 21
- Gopher – 70
- HTTP – 80, dodatkowe serwery, np. proxy, są najczęściej umieszczane na porcie 8080
- HTTPS – 443 (HTTP na SSL)
- IMAP – 143
- IMAP3 – 220
- IRC – 6667
- XMPP – 5222 dla serwera sieci Jabber
- XMPP – 5223 dla serwera sieci Jabber w serwisie Wirtualna Polska
- LDAP – 389
- LDAPS – 636 (LDAP na SSL)
- MySQL – 3306
- NNTP – 119
- POP3 – 110
- SPOP3 – 995 (POP3 na SSL)
- PostgreSQL – 5432
- Rsync – 873
- SMTP – 25
- SSH – 22
- Telnet – 23
- TFTP – 69
- WAP
- X11 – od 6000 do 6007

Osobną klasą protokołów komunikacyjnych są protokoły do komunikacji grupowej (multicast), używane m.in. do transmisji telewizyjnych przez Internet, telekonferencji itp. Przykładami takich protokołów są RMTP (Reliable Multicast Transport Protocol), TOTEM, XTP, Muse i inne.

Protokoły stosowane w automatyce przemysłowej:

- modbus
- profibus
- M-BUS
- s-bus

Modem

Modemy (2x ZyXEL Elite 2864 (ISDN, V90server,V90client) USR Courier V32.bis (21600 bps) Hayes Smartmodem Optima 9600 (9600bps) ZyXEL U-1496E (16800bps) IBM 5858-01 (synchrones Mainframe-Modem, 2400bps))

Modem (od ang. ***MO**dulator-**DEM**odulator*) - urządzenie elektroniczne, którego zadaniem jest zamiana danych cyfrowych na analogowe sygnały elektryczne (modulacja) i na odwrót (demodulacja) tak, aby mogły być przesyłane i odbierane poprzez linię telefoniczną (a także łącze telewizji kablowej lub fale radiowe). Jest częścią DCE (Data Communications Equipment), które w całości wykonuje opisane wyżej czynności. Nieodzowne do współpracy jest DTE (Data Terminal Equipment) i to dopiero stanowi całość łącza przesyłania danych. Dzięki modemowi można łączyć ze sobą komputery i urządzenia, które dzieli znaczna odległość.

Spis treści

- 1 Zasada działania

- 1.1 Modemy akustyczne
- 1.2 Modemy elektryczne
- 2 Inne modemy
- 3 Rodzaje modemów
- 4 Galeria zdjęć
- 5 Zobacz też

Zasada działania

Modemy akustyczne

Modem akustyczny (Novation CAT)

W najstarszych modemach dane były zamieniane na przerywane dźwięki o częstotliwości 5 kHz i składały się z przetwornika elektrycznego, głośnika i mikrofonu. W urządzenie to wkładało się zwykłą słuchawkę telefoniczną, która ponownie przetwarzała dźwięki na impulsy elektryczne. W tamtych czasach firmy telefoniczne dopuszczały przesyłanie torem telefonicznym tylko sygnałów o przebiegu sinusoidalnym, co znacznie ograniczało dopuszczalne prędkości transmisji, pierwsze modemy miały prędkość transmisji 300 bodów.

Modemy elektryczne

Współczesne modemy generują wprost impulsy elektryczne, które przesyłane są bezpośrednio do kabla telefonicznego bez pośrednictwa jakichkolwiek głośników i mikrofonów. Współczesne modemy wykorzystujące sieć telefoniczną nie generują przerywanych dźwięków o stałej częstotliwości lecz sygnał jest kodowany za pomocą modulowanych fal o częstotliwości od 5 do 15 kHz. Górna, fizyczna granica szybkości przesyłu informacji od centrali do abonenta przez zwykłe łącze telefoniczne to 56 kb/s, co można osiągnąć za pomocą protokołów takich jak K56Flex i X2. Wartość ta wynika z tego, że wewnątrz centrali sygnał przesyłany jest cyfrowo w standardzie: poziom - 8 bitów, częstotliwość 8 kHz, jeden bit musi być wykorzystany jako zegar i dlatego maksymalna prędkość transmisji jest równa 56 kb/s.

Publiczną sieć telefoniczną wykorzystuje się również do znacznie szybszych połączeń, wymaga to jednak stosowania odpowiednich urządzeń na centrali telefonicznej.

Inne modemy

Inne urządzenia do przesyłania danych cyfrowych w mediach, które pierwotnie lub z głównego założenia nie są cyfrowe także nazywa się modemami. Przykładowo modemy stosuje się do połączeń innych niż sieć telefoniczna, jak np. sieć telewizji kablowej, czy łącza dedykowane.

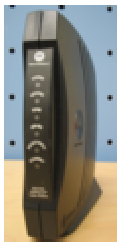
Rodzaje modemów

Modem może być tzw. *zewnętrzny*, czyli znajdujący się poza komputerem i połączony z nim (lub innym odbiornikiem) przy użyciu przewodu (interface : RS-232, USB, LPT, ethernet) oraz charakteryzujący się pełną samodzielnością sprzętową, albo *wewnętrzny* kiedy mamy do czynienia ze specjalną kartą rozszerzeń montowaną wewnątrz komputera (PCI, ISA), zazwyczaj wykorzystującą w pewnym stopniu procesor komputera.

Inną klasyfikację dokonuje się ze względu na medium. Wyróżniamy modemy:

- telefoniczne (klasyczne i xDSL)
- kablowe
- radiowe

Modem pracujący w technologii DSL



Modem kablowy

Modem z technologią 3G GSM jako karta PCMCIA

NetBEUI

Interfejs **NetBEUI** został opracowany przez IBM i wprowadzony na rynek w 1985 roku. Jest stosunkowo małym, ale wydajnym protokołem komunikacyjnym LAN. NetBEUI jest wyłącznie protokołem transportu sieci LAN dla systemów operacyjnych Microsoft. Nie jest trasowany. Dlatego jego implementacje ograniczają się do warstwy 2 modelu OSI, w których działają wyłącznie komputery wykorzystujące systemy operacyjne firmy Microsoft. Aczkolwiek staje się to coraz mniejszą przeszkodą, to jednak ogranicza dostępne architektury obliczeniowe i aplikacje technologiczne. Zalety korzystania z protokołu NetBEUI są następujące: komputery korzystające z systemów operacyjnych lub oprogramowania sieciowego firmy Microsoft mogą się komunikować. NetBEUI jest w pełni samodostrajającym się protokołem i najlepiej działa w małych segmentach LAN. Ma minimalne wymagania odnośnie pamięci. Zapewnia doskonałą ochronę przed błędami transmisji, a także powrót do normalnego stanu w razie ich wystąpienia. Wadą protokołu NetBEUI jest fakt, że nie może być trasowany (za wyjątkiem usług IPTunnel) i niezbyt dobrze działa w sieciach WAN.

TCP

TCP (ang. *Transmission Control Protocol* - protokół kontroli transmisji) – strumieniowy protokół komunikacji między dwoma komputerami. Został stworzony przez Vintona Cerfa i Roberta Kahna.

Jest on częścią większej całości określanej jako stos TCP/IP. W modelu OSI TCP odpowiada warstwie Transportowej.

Spis treści

- 1 Charakterystyka protokołu
- 2 Zastosowania
- 3 Nagłówek TCP
  - 3.1 Znaczenie pól nagłówka
- 4 Zobacz też
- 5 Linki zewnętrzne

Charakterystyka protokołu

W przeciwieństwie do UDP, TCP zapewnia wiarygodne połączenie dla wyższych warstw komunikacyjnych przy pomocy sum kontrolnych i numerów sekwencyjnych pakietów, w celu weryfikacji wysyłki i odbioru. Brakujące pakiety są obsługiwane przez żądania retransmisji. Host odbierający pakiety TCP porządkuje je według numerów sekwencyjnych tak, by przekazać wyższym warstwom modelu OSI pełen, złożony segment.

Chociaż protokół definiuje pakiet TCP, to z punktu widzenia wyższej warstwy oprogramowania, dane płynące połączeniem TCP należy traktować jako ciąg oktetów. W szczególności – jednemu wywołaniu funkcji API (np. send()) nie musi odpowiadać wysłanie jednego pakietu. Dane z jednego

wywołania mogą zostać podzielone na kilka pakietów lub odwrotnie – dane z kilku wywołań mogą zostać połączone i wysłane jako jeden pakiet (dzięki użyciu algorytmu Nagle'a). Również funkcje odbierające dane (recv()) w praktyce odbierają nie konkretne pakiety, ale zawartość bufora stosu TCP/IP, wypełnianego sukcesywnie danymi z przychodzących pakietów.

Charakterystyczny dla TCP jest moment nawiązania połączenia, nazywany ang. *three-way handshake*. Host inicjujący połączenie wysyła pakiet zawierający segment TCP z ustawioną flagą SYN (*synchronize*). Host odbierający połączenie, jeśli zechce je obsłużyć, odsyła pakiet z ustawionymi flagami SYN i ACK (*acknowledge* – potwierdzenie). Inicjujący host powinien teraz wysłać pierwszą porcję danych, ustawiając już tylko flagę ACK (gasząc SYN). Jeśli host odbierający połączenie nie chce lub nie może odebrać połączenia, powinien odpowiedzieć pakietem z ustawioną flagą RST (Reset). Prawidłowe zakończenie połączenia polega na wysłaniu flagi FIN.

Zastosowania

Aplikacje, w których zalety TCP przeważają nad wadami (większy koszt związany z utrzymaniem sesji TCP przez stos sieciowy) to m.in. HTTP, SSH, FTP czy SMTP/POP3 i IMAP4.

Nagłówek TCP

Opis nagłówka TCP

	Bity 0 - 3	**4 - 7**	**8 - 15**	**16 - 31**
0	Port nadawcy			Port odbiorcy
32	Numer sekwencyjny			
64	Numer potwierdzenia			
96	Długość nagłówka	Zarezerwowane	Flagi	Szerokość okna
128	Suma kontrolna			Wskaźnik priorytetu
160	Opcje (opcjonalnie)			
160/192+	Dane			

Znaczenie pól nagłówka

Port nadawcy/odbiorcy - 16-bitowe numery oznaczające poszczególne porty, z których korzysta protokół TCP przy nawiązywaniu połączenia, oraz aplikacje, które z tego protokołu korzystają. Często jest podawany po adresie sieciowym, oddzielony od niego dwukropkiem.

Numer sekwencyjny - 32-bitowy identyfikator określający miejsce pakietu danych w pliku przed fragmentacją (dzięki niemu, można "poskładać" plik z poszczególnych pakietów).

Numer potwierdzenia - 32-bitowy numer będący potwierdzeniem otrzymania pakietu przez odbiorcę, przez co pozwala na synchronizację nadawanie-potwierdzenie.

Długość nagłówka - 4-bitowa liczba, która oznacza liczbę 32-bitowych wierszy nagłówka, co jest niezbędne przy określaniu gdzie zaczynają się dane. Przez to też nagłówek może mieć tylko taką długość, która jest wielokrotnością 32 bitów.

Zarezerwowane - 4-bitowy ciąg zer, zarezerwowany dla ewentualnego przyszłego użytku.

Flagi 8-bitowa informacja/polecenie dotyczące bieżącego pakietu. Poszczególne flagi oznaczają:

- **CWR** - (ang. Congestion Window Reduced) flaga potwierdzająca odebranie powiadomienia przez nadawcę, umożliwia odbiorcy zaprzestanie wysyłania echa.
- **ECE** - (ang. ECN-Echo) flaga ustawiana przez odbiorcę w momencie otrzymania pakietu z ustawioną flagą CE
- **URG** - informuje o istotności pola "Priorytet"
- **ACK** - informuje o istotności pola "Numer potwierdzenia"
- **PSH** - wymusza przesłanie pakietu
- **RST** - resetuje połączenie
- **SYN** - synchronizuje kolejne numery
- **FIN** - oznacza zakończenie przekazu danych

Szerokość okna - 16-bitowa informacja o tym, ile danych może aktualnie przyjąć nadawca. Wartość 0 wskazuje na oczekiwanie na segment z innym numerem tego pola. Jest to mechanizm zabezpieczający komputer nadawcy przed zbyt dużym napływem danych.

Suma kontrolna - 16-bitowa liczba, będąca wynikiem działań na bitach całego pakietu, przez co pozwala na sprawdzenie tego pakietu pod względem poprawności danych.

Wskaźnik priorytetu - jeżeli flaga URG jest włączona, informuje o ważności pakietu.

Opcje - czyli ewentualne dodatkowe informacje i polecenia:

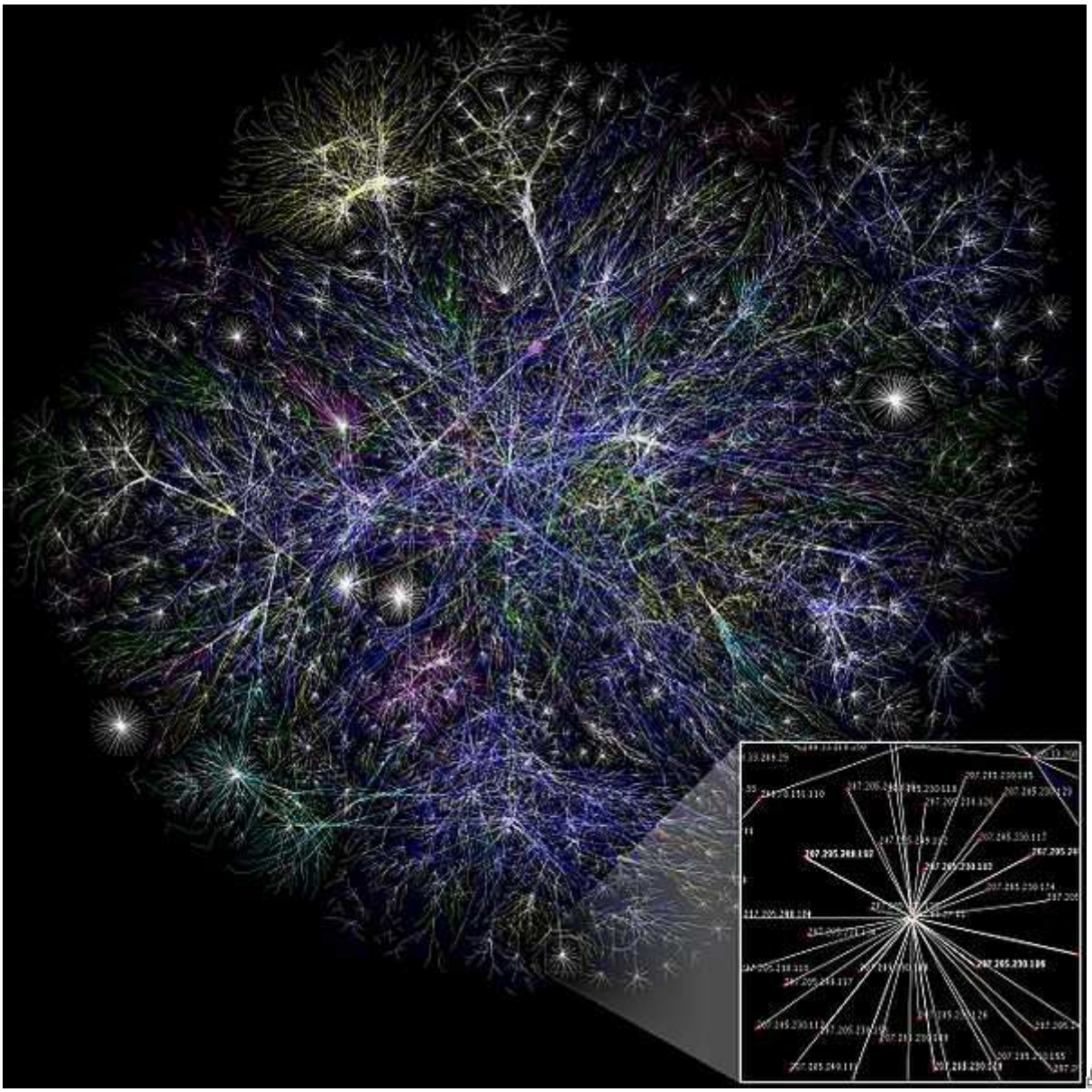
- **0** - koniec listy opcji
- **1** - brak działania
- **2** - ustawia maksymalna długość segmentu

W przypadku opcji **2** to tzw. **Uzupełnienie**, które dopełnia zerami długość segmentu do wielokrotności 32 bitów (patrz: informacja o polu "Długość nagłówka")

Zobacz też

- TCP/IP
- ICMP
- IP
- porty protokołu
- RTP
- SCTP
- UDP
- problem bizantyjskich generałów

Internet



Wizualizacja różnych dróg w części Internetu

Internet (łac. *inter* między, ang. *net* sieć, dosłownie *międzysieć*) - ogólnoświatowa sieć komputerowa[1] logicznie połączona w jednorodną sieć adresową opartą na protokole IP (ang. *Internet Protocol*). Dostarcza lub wykorzystuje usługi wyższego poziomu oparte na telekomunikacji i związanej z nią infrastrukturze.

Spis treści

- 1 Historia
- 2 Internet dzisiaj
  - 2.1 Połączenie komputera z Internetem

    - 2.2 ICANN
- 3 Usługi
- 4 Terminologia
    - 4.1 Internet a WWW
    - 4.2 Pisownia
- 5 Kontrowersje
- 6 Przypisy
- 7 Zobacz też
- 8 Linki zewnętrzne

Historia

Początki Internetu wiążą się z powstaniem internetu ARPANET i sięgają końca lat 60. XX wieku, gdy amerykańska firma RAND Corporation prowadziła badania studyjne nad możliwościami dowodzenia i łączności w warunkach wojny nuklearnej. Na podstawie jej raportów podjęto prace projektowe nad skonstruowaniem sieci komputerowej mogącej funkcjonować pomimo zniszczenia jej części.

Internet dzisiaj

Połączenie komputera z Internetem

Przyłączenie komputera do Internetu możliwe jest z wykorzystaniem wielu technologii, które pozwalają urządzeniu komunikować się z pobliską bramką posiadającą stałe połączenie z innymi systemami w Internecie. Typowe rozwiązania wykorzystują linie telefoniczne (modemy, cyfrowe linie ISDN, modemy ADSL), inne technologie przewodowe (transmisja przez sieci energetyczne, telewizję kablową) oraz bezprzewodowe (GPRS, łącza satelitarne, Wi-Fi).

Aby pracować w Internecie, komputer musi być w stanie komunikować się z innymi systemami przez protokoły z rodziny TCP/IP, a także posiadać oprogramowanie klienckie pozwalające na praktyczne wykorzystanie usług oferowanych przez innych użytkowników.

ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) jest powołaną przez rząd USA organizacją koordynującą przyznawanie unikalnych adresów IP i wysokopoziomowych nazw DNS w Internecie, na Ujednolicony system nazywania, pozwalający na prawidłowe kierowanie ruchem w skali globalnej, jest konieczny do poprawnego działania Internetu. Siedziba główna ICANN znajduje się w Marina del Rey w Kalifornii, a organizacja jest nadzorowana przez międzynarodowy zarząd, którego członkowie wybierani są przez techniczne, biznesowe, akademickie i niekomercyjne kręgi użytkowników sieci. Ponieważ Internet jest siecią wielu dobrowolnie połączonych węzłów, nie ma jako takiego centrum zarządzania, a rola ICANN jest po prostu umowną konwencją, która nie musi być przestrzegana przez użytkowników.

Usługi

Dostawca usługi Internetu (**ISP** – po angielsku *Internet Service Provider*), czasem skrótowo tylko *provider* (wym. *prowajder*), często oprócz łącza do Internetu oferuje następujące usługi dodane:

- hosting stron internetowych WWW lub serwerów internetowych FTP;
- pocztę elektroniczną (*e-mail*) na swoim portalu lub serwerze.

Jeżeli ISP je oferuje, to ich koszt może być wliczony w koszt usługi podstawowej.

Samo korzystanie z Internetu nie wymaga wykupienia żadnych innych dodatkowych usług od ISP. Obojętnie czy w domu czy w kafejce internetowej można bez dodatkowych opłat:

- przeglądać strony internetowe – WWW;
- transferować pliki – FTP, P2P;
- korzystać z darmowych skrzynek poczty elektronicznej;
- dyskutować w grupach dyskusyjnych Usenetu.

Oprócz wyżej wymienionych, Internet umożliwia dostęp do szerokiej gamy usług takich jak m.in.:

- dyskusje internetowe (grupy dyskusyjne, e-mailowe listy dyskusyjnych, fora dyskusyjne)
- rozmowy tekstowe w czasie rzeczywistym (IRC)
- komunikatory internetowe (np. Gadu-Gadu, ICQ, Jabber, Skype, Tlen)
- telefonia internetowa (VoIP)
- radio internetowe
- telewizja internetowa
- telekonferencje
- faksowanie
- sklepy internetowe
- aukcje internetowe
- giełda internetowa
- bankowość elektroniczna
- gry online

Niektóre z usług wymagają odpłatności. Należy ją uiścić usługodawcy, którym zwykle nie jest ISP użytkownika. Jest to analogiczne do sytuacji znanej z życia codziennego, gdy wprawdzie można za darmo wejść do sklepu lub punktu usługowego, ale za każdy towar lub wykonanie usługi trzeba oddzielnie zapłacić.

Terminologia

Internet a WWW [edytuj]

Internet i World Wide Web (WWW) nie są synonimami. Internet to sieć komputerowa – wiele połączonych ze sobą komputerów. WWW jest jednym z dóbr dostępnych przy pomocy Internetu. Innymi bardzo popularnymi są poczta elektroniczna i wymiana plików w sieciach P2P. WWW jest zbiorem dokumentów i innych zasobów połączonych hiperłączami i URL-ami.

Ścisłe podanie różnicy między tymi pojęciami odwołuje się do protokołów internetowych. Protokoły komunikacyjne są podzielone na warstwy. Każda warstwa zapewnia funkcjonalność wymaganą przez wyższą warstwę. Internet to sieci komputerowe komunikujących się za pomocą IP (ang.

Internet Protocol) i TCP (ang. *Transmission Control Protocol*). Inne protokoły, takie jak HTTP (ang. *Hypertext Transfer Protocol*), który jest wykorzystywany przez WWW, działają na wierzchu warstwy komunikacyjnej (IP) i kontroli transmisji (TCP). HTTP jest protokołem warstwy aplikacji.

Pisownia

Słowo **Internet** piszemy wielką literą (nazwa własna), jeśli mamy na myśli Internet jako sieć komputerową. Małą literą możemy pisać o medium, np.: "Przeczytałem to w internecie" [2]. Czasami używa się słowa *internet* (małą literą) w znaczeniu ekstranet (połączona ze sobą grupa sieci komputerowych).

Kontrowersje

Łatwo jest zauważyć, że wiele osób źle korzysta z Internetu lub też uzależnia się od niego. Zbyt częste korzystanie z "sieci" może prowadzić do osłabienia więzi międzyludzkich, a nawet do zaburzeń osobowości jak socjopatia. Dzieci posiadające komputer z dostępem do Internetu są narażone na kontakt z treściami nieodpowiednimi lub szkodliwymi dla ich rozwoju psychicznego (sceny przemocy oraz pornografia z udziałem dzieci/zwierząt/przemocy). Coraz częściej wskazuje się na odpowiednie umiejętności, pozwalające właściwie korzystać z Internetu[3].

Adres IP

Adres IP – liczba nadawana interfejsowi sieciowemu, grupie interfejsów (broadcast, multicast), bądź całej sieci komputerowej opartej na protokole IP, służąca identyfikacji elementów warstwy trzeciej modelu OSI - w obrębie sieci oraz poza nią (tzw. *adres publiczny*).

Adres IP nie jest "numerem rejestracyjnym" komputera - nie identyfikuje jednoznacznie fizycznego urządzenia - może się dowolnie często zmieniać (np. przy każdym wejściu do sieci Internet), ustalenie prawdziwego adresu IP użytkownika, do którego następowała transmisja w danym czasie jest możliwe dla systemu/sieci odpornej na przypadki tzw. IP spoofingu (por. man in the middle, zapora sieciowa, ettercap) - na podstawie historycznych zapisów systemowych.

W najpopularniejszej wersji czwartej (IPv4) jest zapisywany zwykle w podziale na oktety w systemie dziesiętnym (oddzielane kropkami) lub rzadziej szesnastkowym bądź dwójkowym (oddzielane dwukropkami bądź spacjami).

Spis treści

- 1 IP a pozostałe warstwy
- 2 Rodzaje
- 3 Zapis
- 4 Bibliografia

- 5 Zobacz też

IP a pozostałe warstwy

W przeciwieństwie do adresu sprzętowego (MAC; warstwa druga modelu OSI) adres IP nie musi identyfikować jednoznacznie urządzenia ani w czasie, ani fizycznie (szczególnie, jeśli nie należy on do zakresu publicznego – jest adresem podlegającym translacji, bądź jest przydzielany dynamicznie). Protokół komunikacyjny IP pracuje w trzeciej warstwie modelu (warstwie sieciowej) **niezależnie** od rodzaju nośnika warstwy pierwszej. Jest trasowalny (routowalny), a więc umożliwia trasowanie (routing), które odbywa się właśnie w warstwie trzeciej. Aby zapewnić pomyślność komunikacji w tym protokole konieczne jest przyporządkowanie adresów IP interfejsom sieciowym urządzeń.

Z warstwą łącza danych, drugą warstwą rzeczonego modelu, komunikuje się zwykle za pomocą protokołów ARP i RARP. Pierwszy z nich informuje warstwę trzecią o adresie sprzętowym urządzenia, drugi umożliwia wskazanie adresu IP urządzenia przy znajomości adresu sprzętowego.

Protokół IP gwarantuje jedynie odnalezienie interfejsu lub grupy interfejsów sieciowych w pewnej sieci, jednak nie zapewnia poprawności transmisji danych. Współpracę z czwartą we wspomnianym modelu OSI warstwą transportową, która służy właśnie temu celowi, umożliwia m.in. protokół TCP w niej działający. Z tego powodu powstał stos protokołów TCP/IP będący kombinacją m.in. tych dwóch protokołów.

Adresy IP stosuje się nie tylko w Internecie, ale również w sieciach lokalnych korzystających z TCP/IP. W pierwszym przypadku przypisywany jest on przez dostawcę internetu, w drugim o poprawne jego przypisanie dba zwykle jej administrator.

W celu zapewnienia jednoznaczności rozpoznawania się poszczególnych uczestników komunikacji stosuje się system odwzorowania unikatowej nazwy symbolicznej do adresów IP (protokół DNS), dzięki czemu użytkownicy Internetu nie muszą ich pamiętać i aktualizować. Np. adresowi 208.80.152.2 odpowiada obecnie interfejs sieciowy urządzenia/urządzeń (por. redundancja) obsługujących serwis Wikipedii. Aby korzystać z encyklopedii: wystarczy zapamiętanie łatwiejszej nazwy *wikipedia.org*, która tłumaczona jest na adres IP serwera przez serwery DNS (warstwy: piąta, szósta i siódma modelu OSI nazywane odpowiednio: sesji, prezentacji i aplikacji).

Rodzaje

Zobacz więcej w osobnych artykułach: IPv4, IPv5, IPv6.

Obecnie w Internecie używane są adresy IP protokołu w wersji czwartej, **IPv4**. Zapotrzebowanie na adresy IPv4 stało się na tyle duże, że pula nieprzydzielonych adresów zaczyna się wyczerpywać, z tego powodu powstała nowa, szósta wersja protokołu – **IPv6**. Piąta wersja, *IPv5* mająca rozszerzyć możliwości poprzedniczki nie zdobyła popularności, protokół ten znany jest szerzej pod angielską nazwą *Internet Stream Protocol* (pol. „protokoł strumieni internetowych”), skracaną do **ST**.

Zapis

Adresy IPv4 są 32-bitowymi liczbami całkowitymi. Tak więc adres serwisu działający pod adresem *wikipedia.org* to liczba 3 494 942 722, która w zapisie szesnastkowym ma postać D0 50 98 02. Adres w postaci szesnastkowej zapisywany jest zwykle jako D0:50:98:02, z której łatwo przekształcić go na łatwiejszą do zapamiętania formę dziesiętną, oddzielaną już kropkami: 208.80.152.2 (każdą z liczb szesnastkowych zamienia się na jej dziesiętny odpowiednik z zakresu 0-255). Adresy IP w postaci dwójkowej wykorzystywane są niezmiernie rzadko, najczęściej do wyznaczenia maski sieci lub maski podsieci, powyższy adres w postaci dwójkowej to

11001111 10001110 10000011 11101100.

Adresy IPv6 są 128-bitowymi liczbami całkowitymi, dlatego przykładowy adres sieci IPv6 w zapisie szesnastkowym, zgodnym ze specyfikacją Media:CIDR, która dotyczy również IPv4 (RFC1518, RFC1519, RFC1812), wygląda następująco:

3ffe:0902:0012:0000:0000:0000:0000:0000/48,

gdzie /48 oznacza długość pierwszego prefiksu wyrażoną w bitach (człony adresu grupuje się po 16 bitów i oddziela dwukropkiem).

Przyjmuje się, że najstarsze niepodane bity danej sekcji są zerami (np. :: oznacza :0000:), dlatego jego skrócona wersja to 3ffe:902:12::/48. Adres IPv6 w zapisie dziesiętnym byłby cztery razy dłuższy, a więc składałby się z 16 liczb dziesiętnych z zakresu 0-255.

IPv4

IPv4 (ang. ***I**nternet **P**rotocol **v**ersion **4***) - czwarta wersja protokołu komunikacyjnego IP przeznaczonego dla Internetu. Identyfikacja hostów w IPv4 opiera się na adresach IP. Dane przesyłane są w postaci standardowych datagramów. Wykorzystanie IPv4 jest możliwe niezależnie od technologii łączącej urządzenia sieciowe – sieć telefoniczna, kablowa, radiowa, itp. IPv4 znajduje się obecnie w powszechnym użyciu. Dostępna jest również nowsza wersja - IPv6. Dokładny opis czwartej wersji protokołu IP znajduje się w RFC 791. W modelu DoD protokół IPv4 znajduje się w warstwie sieciowej.

Spis treści

- 1 Budowa datagramu
- 2 Adres IP
  - 2.1 Adresy i maski
  - 2.2 Rozdzielanie adresów
  - 2.3 Podział IP
- 3 A 8 24 1.0.0.0 - 126.0.0.0 bardzo duże 127 16.777.214 pierwszy bit = 0
- 4 B 16 16 128.1.0.0 - 191.254.0.0 średniej wielkości 16.382 65.534 pierwsze dwa bity = 10
- 5 C 24 8 192.0.1.0 - 223.255.254.0 małe 2.097.150 254 pierwsze trzy bity = 110
- 6 D - - 224.0.0.0 - 239.255.255.254 do transmisji grupowej brak podziału brak podziału pierwsze cztery bity = 1110
- 7 E - - 240.0.0.0 - 255.255.255.255 zarezerwowane dla IETF - - pierwsze cztery bity = 1111

- 7.1 Prywatne adresy IPv4
- 7.2 Wykorzystanie adresów IPv4
- 8 Zobacz też
- 9 Linki zewnętrzne

Budowa datagramu

+	Bity 0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Wersja	Długość nagłówka	Typ usługi	Całkowita długość	
32	Numer identyfikacyjny			Flagi	Kontrola przesunięcia
64	Czas życia pakietu (TTL)		Protokół warstwy wyższej	Suma kontrolna nagłówka	
96	Adres źródłowy IP				
128	Adres docelowy IP				
160	Opcje IP				Uzupełnienie
192	Dane				

Pierwsze, 4-bitowe pole zawiera numer wersji protokołu IP (dla IPv4 jest to 4).

Kolejne 4-bitowe pole zawiera długość samego nagłówka protokołu (bez danych).

Następne 8 bitów prezentuje tzw. "typ usługi" (ang. Type of Service). Jest to najbardziej podstawowy sposób wyznaczania priorytetu danego datagramu. Na podstawie ToS routery mogą szybciej (np. dla sesji SSH), lub wolniej (np. dla przesyłania danych) przepuszczać przez siebie dane datagramy, zwiększając bądź też zmniejszając w ten sposób interaktywność transmisji.

Kolejnym 16-bitowym polem jest całkowita długość pakietu (razem z danymi). Jego długość (wynosząca 2^16) umożliwia ustawienie rozmiaru pakietu na 65536 bajtów. Warto dodać, że minimalny rozmiar pakietu to 20 bajtów.

Kolejne 16-bitowe pole to numer identyfikacyjny, potrzebny między innymi do fragmentacji i defragmentacji pakietów.

Kolejnym 3-bitowym polem są flagi, które są używane przy fragmentacji pakietów.

Następne 13-bitowe pole służy do odpowiedniego "poukładania" pofragmentowanych pakietów w taki sposób, aby dane zawarte w tych pakietach miały taki sam układ, jak w pakiecie przed fragmentacją.

Pole TTL (8 bitów) to czas życia pakietów (ang. time to live). Jest to liczba z zakresu 0-255. Przy przechodzeniu pakietu przez router jest ona zmniejszana o jeden. W momencie osiągnięcia przez TTL zera, router nie przekazuje pakietu do kolejnego urządzenia sieciowego.

Kolejne, 8-bitowe pole to numer protokołu warstwy wyższej, takimi jak ICMP (1), TCP (6) czy UDP (17).

Następnym polem jest suma kontrolna nagłówka pakietu. Służy ona kontroli, czy wszystkie dane zostały przetransmitowane. Przy każdej zmianie zawartości pakietu, router oblicza sumę kontrolną dla pakietu i zapisuje ją w odpowiednim polu.

Dalsze pola zawierają adres źródłowy i docelowy. To właśnie na podstawie nich można określić pochodzenie i miejsce docelowe pakietu w sieci.

Ostatnim, 32-bitowym polem są opcje, które w normalnej transmisji zwykle nie są używane.

Pole Padding (wypełnienie) jest opcjonalne i jego zawartością są zera dopełniające długość nagłówka do wielokrotności 32 bitów

Adres IP

Aby możliwa była komunikacja w protokole IP konieczne jest nadanie każdemu hostowi adresu IP czyli unikalnego identyfikatora, który pozwoli na wzajemne rozpoznawanie się poszczególnych uczestników komunikacji. Użytkownicy Internetu nie muszą znać adresów IP. Nazwa *www.wikipedia.org* jest tłumaczona na adres IP dzięki wykorzystaniu protokołu DNS. Adres IP jest dostarczany każdemu użytkownikowi przez dostawcę internetu (ISP). Może być przydzielany statycznie lub dynamicznie. Zapotrzebowanie na adresy IP jest tak duże, że pula nieprzydzielonych adresów zaczyna się wyczerpywać.

Adresy i maski

W **IPv4**, czyli obecnym standardzie adresowania internetu, adres IP to liczba 32-bitowa (od 0 do 4294967295), zapisywana w porządku big endian. Liczby w adresie IP nazywają się oktetami, ponieważ w postaci binarnej mają one osiem bitów. Te osiem bitów daje w sumie 256 kombinacji, więc każdy oktet przedstawia liczbę od 0 do 255.

Najpopularniejszy sposób zapisu adresów IP, to przedstawianie ich jako 4 dziesiętnych liczb od 0 do 255 oddzielonych kropkami. W rzeczywistości komputery traktują adres Wikipedii jako liczbę 32-bitową:

3482223596

Taki zapis jest mało czytelny, wobec czego stosuje się podział adresu IP na cztery oktety. Adres Wikipedii zapisujemy binarnie:

11001111 10001110 10000011 11101100

po czym każdą grupę 8-bitów przekształcamy do postaci dziesiętnej:

207 142 131 236

Z adresowaniem IP wiąże się pojęcie maski sieciowej. Wyobraźmy sobie sieć złożoną z 3 komputerów o adresach:

Komputer 1: 192.168.1.1
Komputer 2: 192.168.1.2
Komputer 3: 192.168.1.3

Łatwo zauważyć, że początek adresu dla wszystkich z nich jest ten sam, a końcówka się zmienia. Aby ściśle zdefiniować adresy przynależne do danej sieci wymyślono pojęcie maski podsieci. Umawiamy się, że określona ilość pierwszych bitów adresu IP ma być taka sama, a pozostałe bity w sieci mogą się różnić. W ten sposób powstaje proste kryterium, pozwalające komputerom na określenie swojego położenia na podstawie adresu. Maskę sieci zapisuje się podobnie jak adres IP. Dla przykładu

255.255.255.0

co binarne daje:

11111111	11111111	11111111	00000000
255	255	255	0

Jeżeli komputery oprócz komunikacji w swojej sieci lokalnej mają łączyć się z internetem, to maska sieciowa staje się bardzo ważna. Gdy urządzenie sieciowe stwierdzi, że adres docelowy, z którym chce wymieniać dane nie pasuje do maski, to próbuje się z nim łączyć przez bramę sieciową. Porównywanie opiera się na zerowaniu w adresie bitów równych zeru w masce (logiczny AND bitów maski i adresu IP). Jeżeli komputer 3 łączy się komputerem 2, to wykonuje następujące operacje:

Maska	11111111	11111111	11111111	00000000
	255	255	255	0
Mój IP	11000000	10101000	00000001	00000011
	192	168	1	3
Wynik a	11000000	10101000	00000001	00000000
	192	168	1	0
Maska	11111111	11111111	11111111	00000000
	255	255	255	0
Docelowy IP	11000000	10101000	00000001	00000010
	192	168	1	2
Wynik b	11000000	10101000	00000001	00000000
	192	168	1	0

Wynik a oraz *Wynik b* są równe wobec czego komputer 3 wie, że komputer 2 jest w tej samej podsieci. Jeżeli komputer 3 będzie chciał pobrać stronę z serwera Wikipedii to operacja porównania będzie następująca:

Maska	11111111	11111111	11111111	00000000
	255	255	255	0
Mój IP	11000000	10101000	00000001	00000011
	192	168	1	3
Wynik a	11000000	10101000	00000001	00000000
	192	168	1	0
Maska	11111111	11111111	11111111	00000000
	255	255	255	0
IP Wikipedii	11001111	10001110	10000011	11101100
	207	142	131	236
Wynik b	11001111	10001110	10000011	00000000
	207	142	131	0

Jak widać wynik a, oraz wynik b są różne. W takiej sytuacji komputer 1 będzie się próbował połączyć z Wikipedią przez skonfigurowaną w nim bramę sieciową.

Rozdzielanie adresów

Nazwa	Pierwszy adres IP	Ostatni adres IP	Klasa	Największy ciągły blok
Blok 24-bitowy	10.0.0.0	126.0.0.0	pojedyncza sieć klasy A	10.0.0.0/8
Blok 20-bitowy	128.1.0.0	191.254.0.0	16 kolejnych sieci klasy B	172.16.0.0/16
Blok 16-bitowy	192.0.1.0	223.255.254.0	256 kolejnych sieci klasy C	192.168.0.0/24
Blok 12-bitowy	224.0.0.0	239.255.255.254	Klasa D	224.0.0.0/20
Blok 8-bitowy	240.0.0.0	255.255.255.254	Klasa E	240.0.0.0/24

W adresach klasy A tylko pierwszy oktet wskazuje adres sieci; pozostałe trzy oktety opisują unikatowy adres węzła w sieci. Choć jest tylko 127 adresów sieci klasy A, każdy taki adres może obejmować w przybliżeniu 17 milionów węzłów. Jak nietrudno zgadnąć, adresy klasy A zostały przyznane organizacjom rządowym i wielkim instytucjom.

Adresy klasy B używają pierwszych dwóch oktetów do wskazania adresu sieci i ostatnich dwóch jako unikatowego węzła sieci. Z uwagi na większą długość, adresów klasy B jest więcej, ale w ramach każdego można unikatowo opisać tylko około 65 000 węzłów.

W adresach klasy C używa się pierwszych trzech oktetów jako adresu sieciowego i tylko ostatniego oktetu jako adresu węzła. Stąd istnieje wiele dostępnych adresów klasy C, ale każdy z nich może być użyty tylko do 254 węzłów.

Ze względu na skończoną ilość adresów oraz konieczność ich agregacji dla celów uproszczenia routingu powstały Regionalne Rejestry Internetowe (ang. *RIR*) - organizacje zajmujące się przydzielaniem puli adresów dla poszczególnych dostawców Internetu (ang. *ISP*). Organizacją nadrzędną jest Agencja Zarządzania Numeracją Internetową (ang. *IANA*), która zajmuje się dystrybucją poszczególnych klas A. Do organizacji regionalnych należą:

- APNIC (ang. *Asia Pacific Network Information Centre*) - dla rejonu Azji i Pacyfiku,
- ARIN (ang. *American Registry for Internet Numbers*) - dla rejonu Ameryki Północnej,
- LACNIC (ang. *Regional Latin-American and Caribbean IP Address Registry*) - dla rejonu Ameryki Łacińskiej i wysp Karaibskich,
- RIPE (fr. *Réseaux IP Européens*) - dla rejonu Europy, Bliskiego Wschodu i centralnej Azji,
- AfriNIC - dla rejonu Afryki (Rozpoczęła działanie 22 lutego 2005, wcześniej dystrybucją zajmowały się RIPE NCC,APNIC i ARIN.

Jeżeli ISP potrzebuje więcej adresów zwraca się do właściwej organizacji regionalnej i otrzymuje kolejny zakres numerów IP. Dla przykładu ARIN przydzielił adresy od 64.78.200.0 do

64.78.207.255 firmie Verado, Inc, która przekazała pulę od 64.78.205.0 do 64.78.205.15 firmie Bomis. Bomis adres 64.78.205.6 udostępnił Wikipedii.

Powszechnie panuje pogląd, że pula dostępnych adresów jest na wyczerpaniu, jednak w oficjalnym zestawieniu zajętości adresacji IP jest jeszcze wiele bloków zarezerwowanych przez IANA ([[1]]).

Adresy należące do puli 127.0.0.0/8 (127.x.x.x) są przypisane do urządzenia loopback i zawsze odnoszą się do komputera lokalnego. Adres 0.0.0.0 to adres domyślny (ang. *default*).

Podział IP

W istniejącej klasyfikacji wyróżnia się pięć klas adresów:

* Klasa A,
* Klasa B,
* Klasa C,
* Klasa D,
* Klasa E.

Adresy klasy A odnoszą się najczęściej do dużych sieci zawierających wiele komputerów, adresy klasy B odpowiadają sieciom średniej wielkości, zaś adresy klasy C małym sieciom. Adresy klasy D to tzw. adresy grupowe, wykorzystywane przy przesyłaniu wiadomości do grupy komputerów w Internecie. Tego typu system umożliwia znaczne zmniejszenie ruchu w sieci w stosunku do systemu nawiązywania oddzielnych połączeń z każdym z użytkowników. Obecnie istnieją jednak lepsze techniki rozgłaszania wiadomości grupowych w sieci. Klasa E jest eksperymentalna i zarezerwowana dla IETF. Jeśli sieć jest przyłączona do Internetu, to adres sieci oraz adresy komputerów są przydzielane przez organizację zarządzająca Internetem. Jeśli natomiast jest to lokalna sieć firmowa, to odpowiednie adresy przydziela administrator. Wybierając odpowiednią klasę adresów można przyporządkować danej sieci: więcej adresów podsieci, a mniej komputerów (adresy klasy C); równą liczbę adresów podsieci i komputerów (klasa B) lub mniej adresów podsieci, a więcej komputerów (klasa A). W sieciach lokalnych wykorzystuje się adresy klasy A, B lub C. Adres IP zapisuje się dziesiętnie w czterech blokach trzycyfrowych rozdzielonych kropkami (każdy blok trzycyfrowy odpowiada 8 bitom, więc może być to liczba do 0 do 255). klasa liczba bitów adresujących sieć liczba bitów adresujących host zakres adresów rodzaj sieci liczba sieci liczba hostów w obrębie sieci identyfikacja

A 8 24 1.0.0.0 - 126.0.0.0 bardzo duże 127 16.777.214 pierwszy bit = 0

B 16 16 128.1.0.0 - 191.254.0.0 średniej wielkości 16.382 65.534 pierwsze dwa bity = 10

C 24 8 192.0.1.0 - 223.255.254.0 małe 2.097.150 254 pierwsze trzy bity = 110

D - - 224.0.0.0 - 239.255.255.254 do transmisji grupowej brak podziału brak podziału pierwsze cztery bity = 1110

E - - 240.0.0.0 - 255.255.255.255 zarezerwowane dla IETF - - pierwsze cztery bity = 1111

Szczególnym przypadkiem jest adres 127.0.0.1, który jest adresem zarezerwowanym do testowania pętli zwrotnej danego hosta.

Braki podziału na klasy adresów

Duże różnice między klasami od lat marnowały dużą potencjalną liczbę adresów IP. Przykładem może być sieć lokalna dla firmy posiadającej 300 komputerów, które należy przyłączyć do Internetu. Pojedyncza grupa adresów klasy C daje 254 adresy co jest liczbą niewystarczającą. Dwie grupy dają zbyt wiele adresów i wymagają obsługi dwóch sieci. Wybranie adresów klasy B daje odpowiednią liczbę adresów w jednej sieci, ale odznacza się dużym marnotrawstwem (65 234) adresów. W początkowej fazie rozwoju Internetu zbyt często przydzielano bezpodstawnie adresy klasy B co zpowodowało, że przestwrzeń adresowa tej klasy wyczerpała się szybciej od innych, równocześnie przyczyniając się do obecnych braków wolnych adresów dla nowo przyłączanych komputerów. W celu ulepszenia wykorzystania 32-bitowej przestrzeni adresowej zaprojektowano wiele specjalnych rozszerzeń protokołu IP. Do jaważniejszeych należą:

* maski podsieci o stałej długości,
* maski podsieci o zmiennej długości (VLSM),
* bezklasowy wybór marszruty między domenami (CIDR),

Mechanizmy te nie wykluczają się nawzajem - należy korzystać z nich łącznie.

Podział przestrzeni adresowej na podsieci.

Podział na podsieci umożliwia podział sieci IP dowolnej klasy (A,B lub C) na mniejsze sieci. Adres IP w podsieci składa się z czterech części:

* bitów określających klasę adresu,
* adresu sieci,
* adresu podsieci,
* adresu hosta,

Możliwość podziału na podsieci zależy od typu wykorzystywanego adresu IP. Im więcej bitów hosta w pierwotnym adresie IP, tym więcej można utworzyć podsieci. Podsieci zmniejszają jednak liczbę możliwych do zaadresowania hostów , gdyż bity z adresu hosta pobierane są do identyfikacji podsieci. Podsieci identyfikuje się za pomocą pseudo-adresu IP, zwanego maską podsieci. Maska podsieci jest, podobnie jak sam adres IP, liczbą 32-bitową. Budowa maski podsieci wygląda w ten sposób że pierwsze n-bitów jest jedynkami pozostałe natomiast są zerami. Stąd też dość łatwo można zidentyfikować czy maska podsieci została podana poprawnie. Bity maski identyfikujące część

sieciową zawierają jedynki, natomiast bity identyfikujące hosta zawierają zera. Przykładowo, maska 11111111.11111111.11111111.11000000 (inaczej 255.255.255.192) daje 64 teoretycznie możliwe adresy hostów. Praktycznie jednak dwa z nich (000000 i 111111) są zarezerwowane do identyfikacji samej podsieci i do rozgłaszania w niej.

Podział przestrzeni adresowej klasy B na podsieci. Liczba bitów przedrostka sieci Maska podsieci Liczba nadających się do użytku adresów podsieci Liczba nadających się do użytku adresów hostów na podsieć 2 255.255.192.0 2 16.382 3 255.255.224.0 6 8.190 4 255.255.240.0 14 4.094 5 255.255.248.0 30 2.046 6 255.255.252.0 62 1.022 7 255.255.254.0 126 510 8 255.255.255.0 254 254 9 255.255.255.128 510 126 10 255.255.255.192 1.022 62 11 255.255.255.224 2.046 30 12 255.255.255.240 4.094 14 13 255.255.255.248 8.190 6 14 255.255.255.255 16.382 2

Podział przestrzeni adresowej klasy C na podsieci. Liczba bitów przedrostka sieci Maska podsieci Liczba nadających się do użytku adresów podsieci Liczba nadających się do użytku adresów hostów

na podsieć 2 255.255.255.192 2 62 3 255.255.255.224 6 30 4 255.255.255.240 14 14 5 255 .255.255.248 30 6 6 255.255.255.255 62 2

Przykład podziału na podsieci

Przypuśćmy, że trzeba podzielić na 6 podsieci sieć 192.168.125.0 (Klasy C). Numer sieci adres dwójkowy adres dziesiętny Podstawowy 11000001.10101000.01111101.0000000 192.168.125.0 Podsieć 0 11000001.10101000.01111101.000-0000 192.168.125.0 Podsieć 1 11000001.10101000.01111101.001-0000 192.168.125.32 Podsieć 2 11000001.10101000.01111101.010-0000 192.168.125.64 Podsieć 3

11000001.10101000.01111101.011-0000 192.168.125.96 Podsieć 4 11000001

.10101000.01111101.100-0000 192.168.125.128 Podsieć 5 11000001

.10101000.01111101.101-0000 192.168.125.160 Podsieć 6 11000001

.10101000.01111101.110-0000 192.168.125.192 Podsieć 7 11000001 .10101000.01111101.111-0000 192.168.125.224

W praktyce podsieci 0 i 7 nie będą wykorzystywane. Ich adresy - 000 i 111 - powinno się traktować jako zarezerwowane (nie adresujące podsieci). Same zera identyfikują podsieć, a same jedynki służą do rozgłaszania w niej.

Maski podsieci o zmiennej długości

Maski VLSM pozwalają na lepsze wykorzystanie przestrzeni adresów IP w organizacji, umożliwiając administratorom dostosowanie maski do określonych wymagań każdej podsieci. Istnieje możliwość podzielenia sieci fizycznej na podsieci logiczne o różnych wielkościach. Rozmiar rozszerzonego przedrostka sieci można określać za pomocą kreski ułamkowej (/), po której następuje liczba bitów stosowanych do adresowania sieci i podsieci. Przykładowo: 193.156.230.0/27

Prywatne adresy IPv4

Istnieje pula prywatnych adresów IP. Mogą być one wykorzystane tylko w sieciach lokalnych. Infrastruktura Internetu ignoruje te adresy IP. IANA (*Internet Assigned Numbers Authority*) zarezerwował następujące trzy bloki przestrzeni adresów IP dla prywatnych sieci:

- 10.0.0.0 - 10.255.255.255 - dla sieci prywatnych klasy A (maska: 255.0.0.0)
- 172.16.0.0 - 172.31.255.255 - dla sieci prywatnych klasy B (maska: 255.240.0.0)
- 192.168.0.0 - 192.168.255.255 - dla sieci prywatnych klasy C (maska: 255.255.255.0)

Adresy prywatne można wykorzystywać za pomocą lokalnych routerów w sieciach lokalnych, ale nie działają one w publicznej części internetu. Jeżeli administrator sieci lokalnej przydzieli swoim komputerom adresy IP z puli prywatnej, to routery mogą łatwo rozpoznać kiedy komputery chcą się łączyć z internetem. W takiej sytuacji brama internetowa wykorzystuje technikę maskowania adresów sieciowych NAT, która pozwala na łączenie się z internetem komputerom nie posiadającym własnych publicznych adresów IP. Komputery z adresami prywatnymi nie mogą pełnić roli serwerów sieciowych w Internecie chyba, że posłużymy się techniką maskowania adresów docelowych (DNAT).

Automatyczne przydzielanie adresów IPv4 może być realizowane poprzez zastosowanie protokołów DHCP, RARP, BOOTP, PPP.

Wykorzystanie adresów IPv4

Początkowo wszystkie adresy IPv4 były zarządzane bezpośrednio przez IANA, która w zależności od wnioskowanych potrzeb przydzielała określoną pulę adresów klasy A, B lub C. Wielkie firmy, jak Xerox, Ford czy IBM automatycznie otrzymywały po ponad 16 mln adresów internetowych, nawet jeżeli tak duża liczba nie była im potrzebna. Jeżeli mała firma z kilkunastoma węzłami chciała podłączyć się do Internetu przyznawano jej adresy z klasy C. To z kolei dawało jej kontrolę nad ponad dwustoma adresami węzłów, z których nikt inny nie mógłby skorzystać. Ze względu na marnotrawstwo oraz niespodziewanie duże zapotrzebowanie na adresację internetową z całego świata zmieniono zasady i powołano do życia organizacje regionalne, których zadaniem stało się nadzorowanie wykorzystania dostępnych adresów.

Obecnie klasy A przydzielane są organizacjom regionalnym, te dalej rozdzielają je do ISP w blokach po 4 klasy C (1024 adresy), a następnie ISP przydzielają adresy swoim klientom. Duży nacisk kładzie się na wykorzystywanie mechanizmów NAT, umożliwiających korzystanie z jednego adresu zewnętrznego przez wiele urządzeń posiadających adresy lokalne. W ten sposób ogranicza się przydzielanie adresów urządzeniom (tj. drukarki, access pointy, itp) działającym jedynie w obrębie zamkniętych sieci. Wciąż można dostać przypisanie do klasy C dla swojej organizacji, ale staje się to coraz trudniejsze. Trzeba wykazać rzeczywistą potrzebę dysponowania taką liczbą adresów.

Istnieją koncepcje, według których każde urządzenie elektroniczne ma zostać podłączone do Internetu. W takiej sytuacji pula adresów IPv4 będzie stanowczo za mała. Z tego powodu nastąpi prawdopodobnie przejście z protokołu IPv4 na IPv6 który zwiększy o cztery rzędy wielkości pulę dostępnych adresów.

W ramach klasy C adresów istnieje podział na tzw. podsieci (subnets). Rozmiar podsieci wyznaczany jest przez jej maskę. Najmniejszą podsiecią jest sieć składająca się z 4 adresów, największą ze 128. Dla sieci 4 komputerowej maska wynosi: 256 - 4 = 252 (NETMASK = 255.255.255.252). Dla tak wyznaczonej podsieci można określić następujące parametry:

> NETWORK = 195.205.36.32 (Adres IP - przykładowa podsieć sieci klasy C przyznana przez dostawcę)
> NETMASK = 255.255.255.252 (maska podsieci)
> adresy komputerów = 195.205.36.33 i 195.205.36.34
> BROADCAST = 195.205.36.35 (adres rozgłoszeniowy)

W praktyce maska 255.255.255.252 oznacza, iż do sieci tej można podłączyć 2 komputery i używana jest przez administratorów sieci komputerowych do spinania poszczególnych segmentów sieci.

Aby znaleźć adres rozgłoszeniowy musimy przekształcić Adres IP oraz maskę podsieci na system binarny:

Adres IP:	11000011	11001101	00100100	00100000
	195	205	36	32
Maska podsieci:	11111111	11111111	11111111	11111100
	255	255	255	252

Teraz patrzymy na maskę i zamiast zer wpisujemy w adresie IP jedynki. To jest nasz adres rozgłoszeniowy (broadcast):

Broadcast	11000011	11001101	00100100	00100011
	195	205	36	35

World Wide Web

Historyczne logo WWW zaprojektowane przez Roberta Cailliau

World Wide Web (w skrócie określany jako **WWW** lub **Web**) - hipertekstowy, multimedialny, sieciowy (TCP/IP) system informacyjny oparty na publicznie dostępnych, otwartych standardach IETF i W3C. Pierwotnym i w chwili obecnej nadal podstawowym zadaniem WWW jest publikowanie informacji. WWW jest często błędnie utożsamiane z całym Internetem, w rzeczywistości stanowi tylko jedną z jego najpopularniejszych usług. Odniósł niebywały sukces w walce z systemem Gopher

Aby uzyskać dostęp do tak udostępnianej informacji, trzeba posłużyć się programem komputerowym, który nazywamy przeglądarką internetową. Przeglądarka łączy się z serwerem internetowym, skąd pobiera pewien zbiór informacji określany jako strona internetowa. Strona internetowa może zostać wyświetlona, zapisana w lokalnym systemie plików czy wydrukowana.

Zawartość strony internetowej jest hipertekstem, znaczy to, że użytkownik oglądając stronę internetową może podążać za hiperłączami, które przenoszą go do innych stron internetowych w ramach tego samego serwera internetowego lub innych dostępnych w ramach sieci. Częste korzystanie z WWW nazywa się "surfowaniem po sieci".

World Wide Web został zapoczątkowany na początku lat dziewięćdziesiątych w CERN jako system dostępu do danych, informacji (w tym graficznych) w heterogenicznym środowisku dużej organizacji naukowej.

Tim Berners-Lee, nazywany twórcą WWW, zbudował prototyp systemu, który później został przekształcony do obecnej formy. WWW szybko przekroczył (podobnie jak Internet) granice środowiska naukowego, a po kilku latach został zaadaptowany na całym świecie.

Zobacz też

- HTTP
- URL
- HTML
- World Wide Web Consortium
- Historia Internetu
- Blog
- Webmaster
- Użyteczność (web-usability)
- Dostępność (WWW)
- Web 2.0
- Chat
- FTP
- Gopher