Sieciowe systemy operacyjne oraz usługi katalogowe i domeny

Sieciowe systemy operacyjne

- Network operating system to system który został zoptymalizowany w celu dostarczania usług sieciowych.
- System musi:
  - Obsługiwać sprzęt sieciowy
  - Obsługiwać protokoły i usługi sieciowe
  - Dostarczać te usługi klientom.

Sieciowe systemy operacyjne

- Ponadto może/powinien:
  - Posiadać narzędzia administracyjne i zarządzające
  - Usługi katalogowe oraz nazw
  - Serwery plików
  - Serwery wydruku
  - Tworzenie kopii zapasowej
  - Gwarantować bezpieczeństwo
  - Routing sieciowy

Sieciowe systemy operacyjne

- Platformy:
  - Unix
  - Linux
  - Microsoft Windows
  - Cisco IOS

LANtastic

- Opracowany przez Artisoft (najnowszy 8.0)
- Połączenie klientów MS-DOS, Nowell NetWare oraz OS/2
- Współdzielony dostęp do aplikacji, plików, drukarek i napędów optycznych.

NetWare

- Firma Novell – 1983 rok
- Pierwszy sieciowy system operacyjny
- Nacisk na współdzielenie plików
- Administracja dostępem do plików
- TSR (Terminate and Stay resident)
- Mapowanie woluminów do liter dysków lokalnych
- Lider rynku aż do Windows NT (nawet Windows 95 nie pokonał rywala)
- Protokół IPX firmy Novell wyparty przez TCP/IP

Obecne systemy sieciowe

- Trzy podstawowe warunki:
  - Dostarczać system operacyjny obsługujący sprzęt komputerowy
  - Udostępniać różne protokoły sieciowe i usługi, takie jak adresowanie
  - Uruchamiać aplikacje serwerowe i umożliwiać do nich dostęp klientom lub w przypadku sieci równorzędnych dostęp innym systemom operacyjnym

Po za tym

- Zarządzanie i administrowanie siecią
- Nazwy oraz inne usługi katalogowe
- Współdzielenie plików i drukarek
- Usługi sieciowe
- Tworzenie kopii zapasowych
- Usługi replikacji
- Bezpieczeństwo (potrójne A – authentication, authorization i accounting)
- Routing sieciowy i firewall
- Odporność na awarie
- Możliwość skalowalności

Obecnie?

- Wiele firm udostępnia systemy operacyjne z tym samym jądrem dla klienta i serwera.
- Dodają tylko dodatkowe ograniczenia (np. windows XP i Windows Server 2003)
- Kilka dystrybucji Linuxa podobnie jak Windows.
- Solaris nie rozróżnia pomiędzy komputerami klientów a serverami

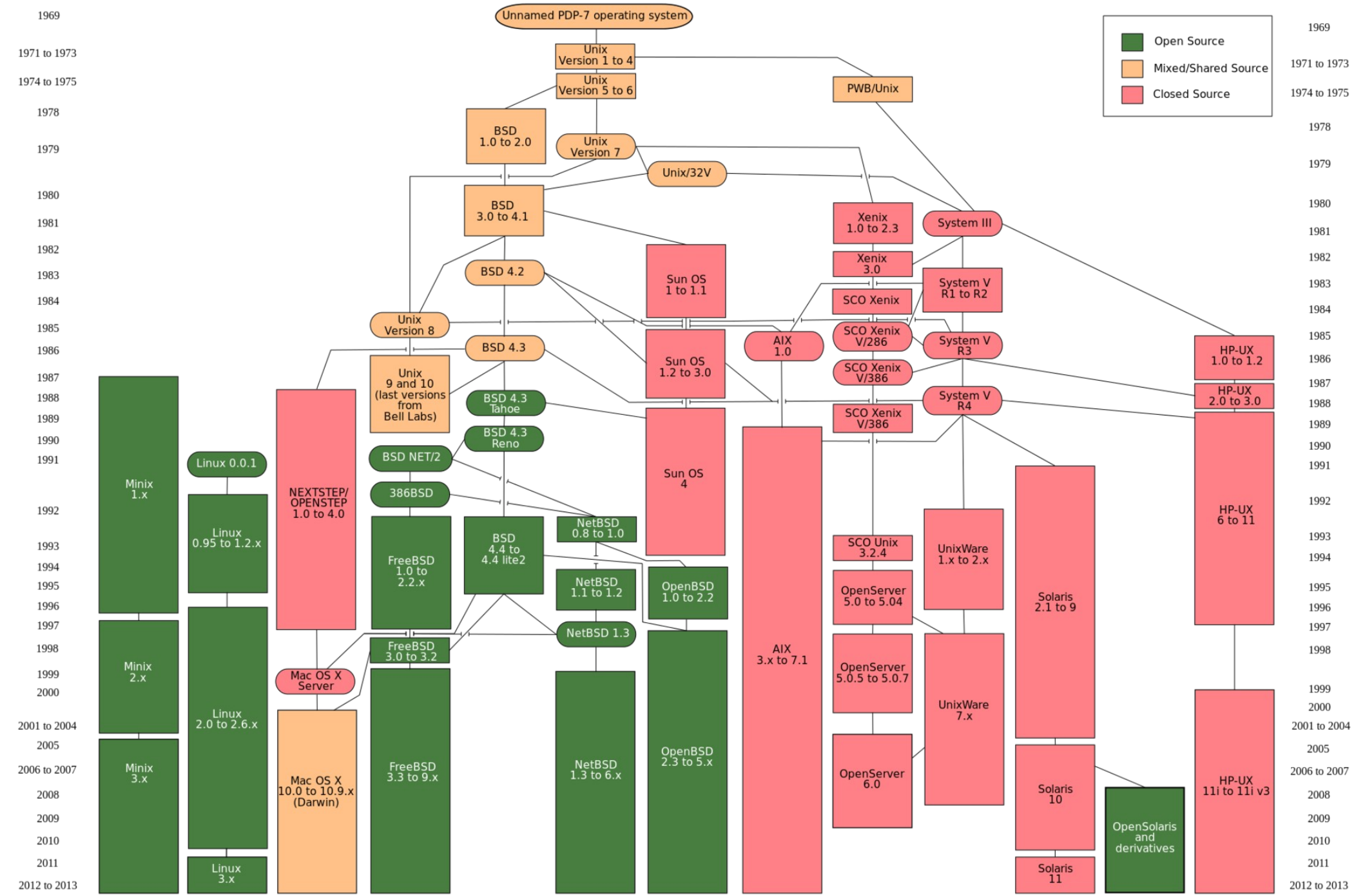
Powszechnie używane platformy

Tabela 20.1. *Powszechnie używane platformy sieciowych systemów operacyjnych*

Nazwa systemu NOS	Właściciel	Wersja bieżąca	Obsługiwany sprzęt
AIX	IBM	7.1	64-bitowe systemy RISC
BSD	Projekt FreeBSD, NetBSD i OpenBSD	8.1, 5.1, 4.8	Alpha, ARM, x86, IA64, MIPS, PPC, SPARC64, SunOS4 oraz Xbox
Digital Unix (TruUnix)	Hewlett-Packard (pomimo przejęcia)	5.1B-5	Alpha (do 2012 roku)
HP-UX	Hewlett-Packard	UNIX System V Release 4	IA64, PA-RISC (do 2012 roku)
IOS	Cisco Systems	15	Routery i przełączniki sieciowe firmy Cisco
IRIX	Silicon Graphics	6.5.30	Systemy SGI, procesory PowerPC
Mac OS X	Apple Computer	10.6.6	x86, PowerPC oraz ARM v6
NetWare (wyparty przez OES)	Novell	6.5 SP8 (odpowiednik OES 2)	x86
Open Enterprise Server	Novell	OES 2 SP3	x86
OpenVMS	Hewlett-Packard (pomimo przejęcia)	8.4	Alpha, VAX, IA64 (Itanium)
Red Hat Linux	Red Hat	6	x86, IA64
SCO Open Server 6	The SCO Group	6	x86
Solaris	Oracle	11	SPARC, x86, IA64
Ubuntu	Canonical	10.10	x86, IA64
Windows	Microsoft	2008 R2	x86, IA64
z/OS (poprzednio MVS)	IBM	1.12	IBM zSeries (MVS działa na komputerach Mainframe System 360/390)

Unix

- Wielozadaniowy, wieloużytkownikowy sieciowy system operacyjny z funkcja podziału czasu.
- Zbudowany na bazie jądra które łatwo dostosowuje się do rożnej architektury.
- Oddziela operacje jądra od funkcji użytkownika.
- Opracowany w Bell Labs dla AT&T w latach 60.
- W 1972 na jego potrzebny opracowana język C
- Standard przemysłowy.

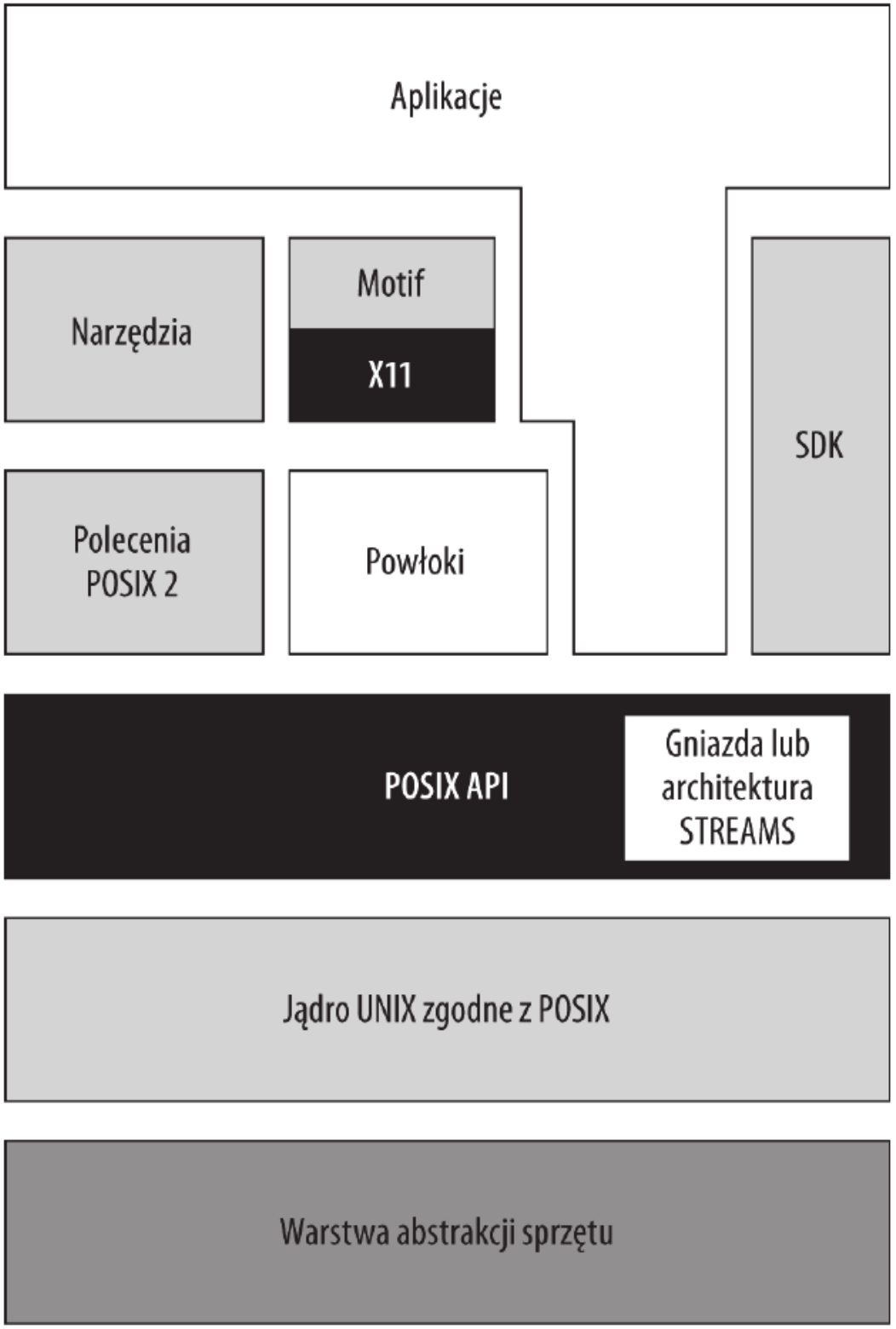

1969
1971 to 1973
1974 to 1975
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001 to 2004
2005
2006 to 2007
2008
2009
2010
2011
2012 to 2013
Unnamed PDP-7 operating system
Unix Version 1 to 4
Unix Version 5 to 6
PWB/Unix
BSD 1.0 to 2.0
Unix Version 7
Unix/32V
BSD 3.0 to 4.1
Xenix 1.0 to 2.3
System III
Xenix 3.0
BSD 4.2
Sun OS 1 to 1.1
System V R1 to R2
SCO Xenix
Unix Version 8
SCO Xenix V/286
AIX 1.0
System V R3
BSD 4.3
Unix 9 and 10 (last versions from Bell Labs)
Sun OS 1.2 to 3.0
SCO Xenix V/386
HP-UX 1.0 to 1.2
HP-UX 2.0 to 3.0
BSD 4.3 Tahoe
System V R4
BSD 4.3 Reno
BSD NET/2
Sun OS 4
SCO Xenix V/386
Minix 1.x
Linux 0.0.1
NEXTSTEP/ OPENSTEP 1.0 to 4.0
386BSD
NetBSD 0.8 to 1.0
SCO Unix 3.2.4
UnixWare 1.x to 2.x
Solaris 2.1 to 9
HP-UX 6 to 11
Linux 0.95 to 1.2.x
FreeBSD 1.0 to 2.2.x
BSD 4.4 to 4.4 lite2
NetBSD 1.1 to 1.2
OpenBSD 1.0 to 2.2
OpenServer 5.0 to 5.04
AIX 3.x to 7.1
Minix 2.x
NetBSD 1.3
FreeBSD 3.0 to 3.2
OpenServer 5.0.5 to 5.0.7
UnixWare 7.x
Mac OS X Server
Linux 2.0 to 2.6.x
Minix 3.x
Mac OS X 10.0 to 10.9.x (Darwin)
FreeBSD 3.3 to 9.x
NetBSD 1.3 to 6.x
OpenBSD 2.3 to 5.x
OpenServer 6.0
Solaris 10
OpenSolaris and derivatives
HP-UX 11i to 11i v3
Linux 3.x
Solaris 11
Open Source
Mixed/Shared Source
Closed Source

POSIX

- Interfejs systemu Unix oraz standaryzacja wokół języka C ostatecznie doprowadziły dopowstania zestawu wskazówek projektowych i API, które stały się architekturą modelu sieciowego systemu operacyjnego. POSIX (ang. Portable Operating System Interface for Unix to API (ang. Application Programming Interface) zdefiniowane przezstandardy IEEE 1003 i ISO/IEC9945.
- POSIX zapewnia systemom sieciowymstandaryzacjeinterfejsów programistycznych, użytkownika i właściwości powłok systemów i dlategozostał niemal powszechnie zaadaptowany

POSIX

- Funkcje nowoczesnego systemu sieciowego — takie jak hierarchiczny system plików, prze-chowywanie zwykłego tekstu, interpreter wiersza poleceń, komunikacja między aplikacjami i komunikacja między procesami (ang. Inter-Process Communication, IPC), koncepcjapamięci współdzielonej, wiadomości i zapytań, semaforów, gniazd itp. — są wynalazkami wyrastającymi z systemu Unix, chociaż nie stanowiły części oryginalnego systemu Unix



Architektura STREAMS i gniazda

- Architektura STREAMS i gniazda to dwie metody używane przez Unix do ustanowienia interfejsu sieciowego. Ponadto odgrywają one główną rolę w tworzeniu usług sieciowych.

Gniazda

- Gniazdo to punkt końcowy połączenia sieciowego. Kiedy gniazdo pozwala na dwukierun-kowy przepływ danych IP, jest określane mianem gniazda internetowego.
- Gdy gniazdo używa innych typów protokołów, nosi nazwę gniazda sieciowego lub jeszcze prościej — gniazda.
- Gniazda internetowe mają określone właściwości, takie jak używany protokół, przypisany adres IP, numer portu, numer usługi oraz (po nawiązaniu połączenia) zdalny adres IP i zdalny numer portu.
- Wymienione cechy charakterystyczne nadają gniazdom unikalną identyfikację.
- Sieciowe systemy operacyjne wykorzystują koncepcję gniazda jako interfejsu między procesem aplikacji i stosem sieciowym, pozwalając na przepływ danych pomiędzy nimi.

Gniazda

- Prawdopodobnie najbardziej znaną architekturą gniazda sieciowego jest architektura Berkeley Sockets API, która została wprowadzona wraz z BSD UNIX v4.2.
- Obecnie architektura Berkeley Sockets jest uznawana za standardowy model projektu gniazda sieciowego.

Architektura STREAMS

- Architektura STREAMS jest alternatywą dla Berkeley Sockets.
- Po raz pierwszy pojawiła się w UNIX System V używana dla operacji wejścia-wyjścia w celu umożliwienia urządzeniu bądź plikowi specjalnemu systemu na komunikację z urządzeniem za pomocą sterownika tego urządzenia z użyciem standardowych systemowych wywołań wejścia-wyjścia.
- Architektura STREAMS ma konstrukcję modułową i pozwala na łączenie sterowników (które są modułami).
- Obciążenie powodowane przez architekturę STREAMS jest większe niż w przypadku gniazd. Wewszystkich systemach operacyjnych używających architektury STREAMS dołączane jest również Sockets API.
- W początkowej specyfikacji Single UNIX Specification architektura STREAMS była komponentem obowiązkowym, natomiast w bieżącej specyfikacji SUS v3 stanowi komponent opcjonalny.

Single Unix specification

- Specyfikacja SUS jest wynikiem wysiłków w celu utworzenia standardu systemu Unix, które zostały zapoczątkowane przez IEEE oraz The Open Group w latach osiemdziesiątych.
- Skutkiem tych działań był standard POSIX.1 (skrót od Portable Operating System Interface for Unix), który wpłynął na prace prowadzone nad wieloma systemami sieciowymi w latach osiemdziesiątych i dziewięćdziesiątych w celu utworzenia zestawu standardów Unix.
- Okres ten był znany jako „wojny Unix” i doprowadził niektórych z głównych producentów systemu Unix do założenia COSE (ang. Common Open Software Environment). Największym osiągnięciem COSE było utworzenie środowiska CDE (ang. Common Desktop Environment), które łączyło środowisko X11 z interfejsem użytkownika OSF Motif oraz pakietem narzędziowym.

Specyfikacji SUS

- Specyfikacja SUS dostarczyła zestawu interfejsów użytkownika oraz oprogramowania, które stanowiły standard programowania w powłoce POSIX.
- Ponadto opracowana została pewna liczba systemowych narzędzi i usług, włączając w nie plik, terminal oraz usługi sieciowe.

Linux

- Linux jest systemem operacyjnym z rodziny Unix, używającym jądra Linux dostępnego jako open source.
- Obecnie pod kontrolą systemu Linux działa największa liczba serwerów internetowych, jak wynika z danych statystycznych dotyczących wykorzystywania internetu.
  - połowa serwerów WWW działa pod kontrolą różnych wersji systemu Linux,
  - FreeBSD to około 30%,
  - natomiast pozostałe 20% należy do Windows Server.
  - Inne badania, przeprowadzane na podstawie sprzedaży sprzętu i uwzględniające cały rynek serwerowy, wskazują, że Linux ma w nim około piętnastoprocentowy udział.

- Linux jest zainstalowany na 91,8% najpotężniejszych superkomputerów, wymienionych na liście Top 500 Supercomputer Sites
- Przy użyciu systemów Linux zbudowana jest duża liczba ważnych witryn internetowych, łącznie z czterema największymi: Amazon, eBay, Google oraz Yahoo!.
- W niektórych krajach Linux stał się standardowym systemem operacyjnym dla rządów. Przykładami takich krajów są Brazylia, Rosja, Indie, Chiny, Niemcy oraz Francja.


debian
ubuntu
linux for human beings
redhat
CentOS
fedora
Mandriva
slackware
linux
FreeBSD
PCBSD
solaris 10
opensolaris
suse

LAMP

- Linux jest często instalowany na sprzęcie przemysłowym i pozwala na osiągnięcie dużej skalowalności przez skalowanie poziome.
- Wiele serwerów Linux ma zainstalowane oprogramowanie nazywane LAMP.
- Pakiet LAMP składa się z następujących komponentów:
  - Linux — system operacyjny;
  - Apache — serwer WWW;
  - MySQL — serwer bazy danych;
  - P — jeden z języków programowania lub języków skryptowych: PHP, Perl lub Python.

Solaris

- System operacyjny Solaris firmy Oracle (dawniej Sun2) to obecnie najczęściej używany sieciowy system operacyjny Unix.
- Solaris został zaprezentowany w roku 1992 w celu zastąpienia systemu operacyjnego SunOS i wprowadził zaawansowany stos sieciowy obsługujący sieci TCP/IP.
- Solaris istnieje w dwóch wersjach:
  - działającej w systemach komputerowych bazujących na procesorach SPARC firmy Oracle
  - w wersji x86 działającej na standardowej architekturze Intel.
- Firma Sun uznała Solaris za jeden z podstawowych sieciowych systemów operacyjnych dla dużych przedsiębiorstw, jak również za preferowaną platformę dla sieci pamięci masowej.

Solaris

- Dostępny bezpłatnie docelów testowych i niekomercyjnych.
- Solaris można zainstalować w postaci serwera lub stacji roboczej.
- Istnieje możliwość instalacji wyłącznie podstawowych usług sieciowych, użytkownika, programisty bądź też instalacji całego pakietu, zawierającego oprogramowanie niezbędne do zarządzania siecią oraz narzędzia do zarządzania jej polityką.

- Oryginalny stos sieciowy w systemie Solaris 1.x bazował na wersji BSD.
- Aby poprawić wydajność Solarisa, w wersji Solaris 2.x stos sieciowy przeniesiono na architekturę AT&T SVR4.
- Różne wersje 2.x kontynuowały przejście w kierunku stosu sieciowego STREAMS, który stał się podstawą dla funkcji sieciowych w UNIX System V.
  - Architektura STREAMS jest znana zarówno ze względu na swoją modułową naturę, jak i możliwość przekazywania komunikatów między modułami.
  - Tworzenie połączenia w architekturze STREAM wiąże się ze znaczącym obciążeniem, ale w przypadku długich sesji powiązanych z protokołami takimi jak FTP i NFS obciążenie to nie stanowi problemu.

- Do późnych lat dziewięćdziesiątych serwery i stacje robocze Sun były najczęściej stosowaną platformą zarówno do routingu, jak i w przypadku aplikacji serwerowych, na których działało oprogramowanie serwerów WWW.
- Protokoły internetowe, w szczególności HTTP, są krótkotrwałymi połączeniami, a architektura STREAM pokazuje tutaj swoje wady.
- Podczas prac nad systemem Solaris 10 firma Sun dokonała przebudowania swojego stosu sieciowego.

- Stos sieciowy w systemie operacyjnym Solaris 10 został przebudowany z użyciem architektury „FireEngine”, która połączyła wszystkie warstwy protokołów w pojedynczy moduł STREAM wraz z pełną obsługą wątkowania.
- Mechanizm określany jako Vertical perimeters pozwala na synchronizację per-procesor w module TCP/IP, co jest wdrożone przy użyciu squeue.
- Obsługuje system plików NFS 4.0 i został zaprojektowany w celu obsługi sieci o przepustowości do 10 Gb/s.

- Solaris ma również możliwość dołączania systemu plików ZFS (jego początkowa nazwa kodowa to Zettabyte File System), który oferuje kilka unikalnych funkcji przemysłowych.
- ZFS obsługuje bardzo duże wielkości woluminów oraz integruje system plików wraz z zarządzaniem woluminami.
- Oprócz wbudowanych funkcji tworzenia kopii migawkowych i pełnych system ZFS zawiera także schemat replikacji o nazwie RAID-Z.
  - Technologia ta traktowana jako całość ma pewne unikalne możliwości w zakresie automatycznej naprawy

- System Solaris jest dostarczany wraz z narzędziem o nazwie DTrace (ang. Dynamic Tracing), które diagnozuje wydajność aplikacji sieciowych oraz wykrywa miejsca występowania potencjalnych wąskich gardeł.
- Informacja ta może być przekazana do podsystemu zarządzającego awariami, odpowiedzialnego za usunięcie problemu, optymalizację i (lub) zgłoszenie administratorom systemu.

Novell NetWare oraz Open Enterprise Server

- Oprogramowanie NetWare firmy Novell miało bardzo ważną pozycję w czasie opracowywania sieciowych systemów operacyjnych.
- Przez niemal dekadę NetWare był najważniejszym systemem sieciowym dla komputerów PC, w szczególności dla serwerów plików i wydruku oraz sieci heterogenicznych zawierających różne typy klientów.

- Kiedy Microsoft Windows Server i serwery Linux stały się popularniejsze firma Novell skoncentrowała swoje wysiłki programistyczne
  - na narzędziach zarządzania siecią (ZenWorks),
  - usługach katalogowych klasy przemysłowej (eDirectory)
  - oraz innych produktach, które reprezentowały aktualny stan rozwoju w tej dziedzinie.
- Oprogramowanie NetWare 6.5 zostało zastąpione przez Open Enterprise Server (OES), które w wersji 2 SP1 bazuje na jądrze NetWare 6.5 SP8.
  - System OES 1 pojawił się w marcu 2005 roku, natomiast wersja OES 2 SP3 została wydana w grudniu 2010 roku.

- OES 2 to system sieciowy, który może działać na bazie jądra NetWare albo Linux.
- Novell umieścił OES jako rozwiązanie przemysłowe do obsługi serwera plików, serwera wydruku, usług katalogowych oraz aplikacji sieciowych.
- Na bazie jądra NetWare - OES-NetWare i umożliwia dodanie modułów NLM (ang. NetWare Loadable Modules).
- NLM = różne aplikacje: Apache, eDirectory, GroupWise, iPrint, NSS, OpenSSH, Tomcat oraz innych.

Windows Server

- Windows Server jest uznawany za serwer ogólnego przeznaczenia, który oferuje najlepszą i najszerszą obsługę aplikacji sieciowych ze wszystkich.
- Ogromną liczba cennych funkcji, takich jak zautomatyzowana implementacja,zarządzanie polityką (ang. policy engine) sieciowego systemu operacyjnego oraz inne dostępne funkcje.

- Pod marką Microsoft Server firma Microsoft sprzedaje także rozbudowany zestaw aplikacji serwerowych.
- Przykłady produktów Microsoft Server to między innymi:
  - Biz Talk Server,
  - Commerce Server,
  - Exchange Server,
  - Internet Information Server (dołączony do Windows Server),
  - ISA Server,
  - SQL Server,
  - Windows Storage Server (w postaci oddzielnego wydania Windows) itp.

- Różne wersje Windows Server obejmują produkty od Windows Home Server,
  - przez Windows Small Business Server,
  - aż do Windows Datacenter Edition.
- Spośród wszystkich produktów
  - Microsoft Exchange osiągnął najwyższą pozycję na rynku poczty korporacyjnej,
  - SQL Server to najlepiej sprzedający się komercyjny serwer bazy danych klasy przemysłowej.

Usługi katalogowe i domeny

- Usługi katalogowe odgrywają ważną rolę w bieżącej architekturze klient-serwer sieciowych systemów operacyjnych.
- Zapewniają
  - usługi nazw,
  - przechowują informacje na temat obiektów w sieci
  - pozwalają na przekazywanie tych informacji dalej, do innych serwerów i aplikacji.
- Obecnie w użyciu jest wiele usług katalogowych, a nowoczesne sieci bardzo intensywnie z nich korzystają.

Domena

- Najmniejszą podstawową jednostką w usłudze katalogowej jest domena.
- Domena to zbiór systemów współdzielących tę samą bazę danych bezpieczeństwa.
- Domeny mogą być różnych typów i zawierać takie elementy, jak jednostki organizacyjne, konta użytkowników i komputerów, a także inne obiekty, do których można uzyskać dostęp za pomocą unikalnej nazwy.

Usługi katalogowe i domeny

- Duże sieci komputerowe stanowią problem dla projektantów sieciowych systemów operacyjnych działających w modelu klient-serwer.
  - W jaki sposób zarządzać ogromną liczbą systemów, użytkowników, urządzeń peryferyjnych oraz innymi elementami znajdującymi się w sieci?
  - Rozwiązanie sprowadza się do takiego przechowywania informacji w baziedanych położonej w pewnym miejscu sieci, aby dostęp do tych informacji był szybki i niezawodny.
  - Oprogramowanie zarządzające takimi informacjami nosi nazwę usługi katalogowej, a podstawowa jednostka używana do przechowywania informacji sieciowych nosi nazwę domeny. Domena jest zwykle powiązana z własną bazą danych bezpieczeństwa.
-

- Sieciowe bazy danych, które zostały zaimplementowane jako usługi katalogowe, działają na zasadzie podobnej do słownika. Są one bliskie idei książki telefonicznej; w wielu ogromnych projektach baz danych słowo katalog zostało zastosowane w latach siedemdziesiątych.
- Ponieważ katalog ten opracowano w celu dostarczania usługi sieciowej, ostatecznie zaczęto stosować pojęcie usługi katalogowe. Standaryzacja usług katalogowych w postaci kilku modeli przemysłowych doprowadziła do rozprzestrzenienia się usług katalogowych we wszystkich sieciowych systemach operacyjnych.
- Ponadto spowodowała zastosowanie ich w ogromnych aplikacjach przemysłowych, służących do zarządzania przechowywanymi danymi różnych rodzajów.

- Ponieważ informacje przechowywane w centralnych sieciowych bazach danych niewątpliwie są poufne, muszą być odpowiednio chronione, a ochrona tych danych musi być w pełni powiązana z centralnym magazynem informacji i za jego pośrednictwem zarządzana.
- Niektóre usługi katalogowe traktują bezpieczeństwo sieci jako jedną całość, podczas gdy inne współpracują z zewnętrznymi systemami bezpieczeństwa.

- Usługa katalogowa może być zbudowana za pomocą dowolnego rodzaju bazy danych:
  - pliku jednorodnego, relacyjnie, hierarchicznie, na zasadzie „równy z równym” itd.
- Najpopularniejsze usługi katalogowe to takie, które są półrelacyjne, hierarchiczne, wysoce skalowalne i przechowują obiekty danych.
- Skalowalność jest ważnym czynnikiem, ponieważ zawsze występuje potrzeba zachowania wszystkich informacji wraz z rozwojem.

- Wprawdzie usługa katalogowa jest podobna do bazy danych, ale istnieją pewne istotne różnice.
  - Informacje usługi katalogowej są odczytywane znacznie częściej, niż są w niej zapisywane. Dlatego też nie jest konieczne stosowanie mechanizmów takich jak wycofywanie transakcji.
  - Poza tym usługi katalogowe nie mają takich samych wymagań w zakresie wydajności i normalizacji (optymalizacji) jak w przypadku relacyjnych baz danych. Można się przekonać, że wiele usług katalogowych tworzy w wielu miejscach powtarzające się zbiory danych, o ile może to przyczynić się do zwiększenia wydajności. Relacyjna baza danych może
  - Usługa katalogowa może być wykorzystywana do przechowywania różnorodnych danych, powiązanych ze sobą w losowy sposób, a więc wymaga mniej strukturalnego schematu.

Banyan VINES

- Obszar usług katalogowych zawdzięcza bardzo wiele opracowaniu Banyan VINES, powstałemu we wczesnych latach osiemdziesiątych. VINES to skrót od Virtual Integrated NEtwork Service; był to sieciowy system operacyjny bazujący na systemie Unix.
- W swoim stosie sieciowym system VINES używał bardzo popularnego w tamtych czasach zestawu protokołów XNS (ang. Xerox Network Services) i miał wbudowany wariant o nazwie VIP (ang. VINES Internetwork Protocol).
- Sieci VINES bazowały na pakietach, używały automatycznego adresowania klientów oraz miały protokół routingu i protokół kontroli internetu.
- Protokoły warstwy górnej aplikacji zawierały standardowe usługi plików oraz wydruku.
- Żadna z tych technologii nie jest szczególnie interesująca. Jednak system VINES był unikalny dzięki StreetTalk, usłudze nazw wysokiego poziomu.

- Większość nowoczesnych usług katalogowych bazuje na standardzie X.500.
  - Wersja LDAP dla X.500 została utworzona dla sieci TCP/IP i jest używana w większości obecnie dostępnych produktów.
- Microsoft Active Directory (AD) to najlepiej znana i najczęściej używana usługa katalogowa.
  - Technologię AD zbudowano w celu przechowywania obiektów różnego typu z uwzględnieniem aspektów bezpieczeństwa.

- Usługa StreetTalk była jedną z wczesnych usług katalogowych.
- W rozproszonej, replikowanej bazie danych tworzyła przestrzeń nazw dla całej sieci i pozwalała różnym sieciom na współdzielenie zasobów.
- W technologii StreetTalk adres był tworzony na podstawie hierarchicznego schematu nazw, odwzorowującego hierarchię obiektu, i miał postać obiekt@grupa@organizacja.
- Obiekt mógł być udziałem sieciowym, drukarką sieciową bądź kontem użytkownika.
- W tamtym czasie oprogramowanie klientów działało w systemach MS-DOS i Windows 3.x. W sieci VINES nie występowały domeny.

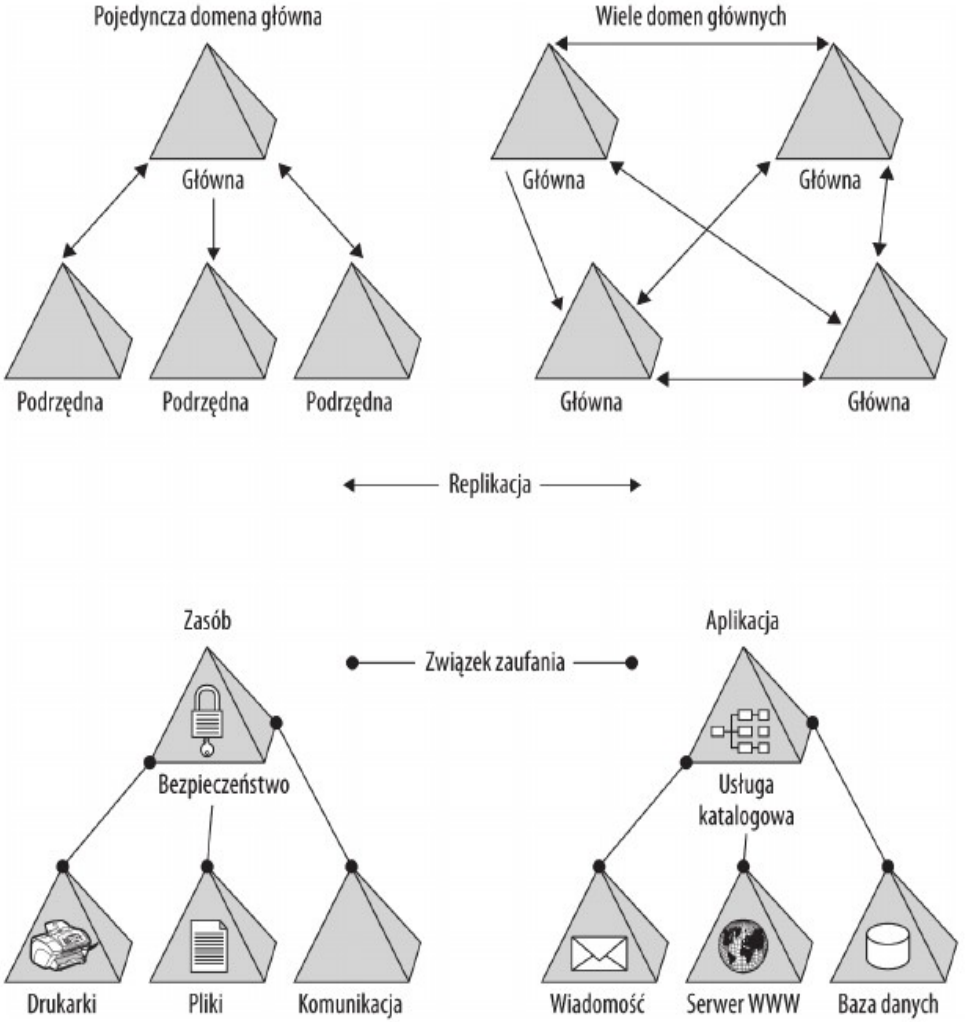
Domena

- Każdy system informacji jest zorganizowany wokół jednostki podstawowej.
- W usłudze katalogowej będzie to domena.
- Domena sieciowa opisuje grupę systemów i powiązanych z nimi zasobów, które są zorganizowane przez usługę katalogową i współdzielą bazę danych bezpieczeństwa oraz model bezpieczeństwa.

Typy domen

Istnieje wiele różnych schematów używanych do organizowania typów domen. Wśród najczęściej spotykanych można napotkać:

- centralna domena główna zorganizowana z domenami podrzędnymi w strukturę
- drzewa, hubu bądź gwiazdy, tzw. „pojedyncza domena główna”;
- struktura wielu domen głównych;
- domeny zasobów;
- domeny zdalne, gdzie łącza przedstawiają zaufane związki i (lub) replikacje, są połączone siecią WAN;
- domeny charakterystyczne dla aplikacji.



Wzajemna współpraca

- Migracja usługi katalogowej utworzonej dla dużej sieci do innej usługi katalogowej to jedno z najboleśniejszych zadań dla zespołu IT organizacji, które musi być wykonane.
- Z dwóch powodów zadanie to okazuje się znacznie trudniejsze niż przeniesienie danych z jednej, przemysłowej bazy danych do innej.
  - Pierwszy — większość baz danych jest dostarczana z funkcjami eksportu i importu albo istnieją dla nich narzędzia firm trzecich, pozwalające na wykonanie tego rodzaju operacji.
  - Drugi — usługi katalogowe są powiązane z funkcjami bezpieczeństwa oraz strukturami własnościowymi, co znacznie utrudnia rozgryzienie i wyodrębnienie danych znajdujących się w usługach katalogowych.

- Heterogeniczna usługa katalogowa przechowuje informacje o systemach działających podkontrolą różnych systemów operacyjnych, co jest funkcją cenną z wielu powodów.
- Sposób, w jaki obce systemy są przedstawiane w usłudze katalogowej, pokazuje, ile producent tego systemu katalogowego włożył pracy, aby osiągnąć dany efekt.
- W przypadku wielu usług katalogowych heterogeniczność niekoniecznie będzie zaletą, a preferowana będzie homogeniczność.

- Wcale nie tak rzadko można się spotkać z sytuacją, w której wiele usług katalogowych działa na różnych serwerach znajdujących się w całej sieci.
- Usługa katalogowa istnieje dla każdego ważniejszego sieciowego systemu operacyjnego.
- Wiele z nich może być powiązanych z serwerami WWW, na przykład Apache, podczas gdy inne mogą być częścią korporacyjnego programu do obsługi poczty elektronicznej.

Serwery domen

- System komputerowy, w którego ramach działa usługa katalogowa, jest nazywany serwerem domen sieci lub kontrolerem domen.
- Ze względów bezpieczeństwa niemal wszystkie usługi katalogowe przechowują swoje dane oraz powiązane z nimi informacje bezpieczeństwa w tym samym serwerze domen.

- W małych sieciach serwery domen poza usługą katalogową mogą oferować także kilka innych usług.
- Przykładem tego rodzaju systemu jest Microsoft Small Business Server (SBS): usługi katalogu AD, DHCP, DNS, Exchange Server, IIS Web Server, ISA (Microsoft Internet Security and Acceleration) oraz SQL Server.

- W zależności od natury domeny i usługi katalogowej, a także przeprowadzanych zadań, domena może mieć jeden serwer domen dla dwóch lub trzech systemów.
- W przypadku tejwielkości sieci wprowadza się na rynek wiele serwerów domowych bazujących na systemie Linux.
- W ogromnych sieciach serwer domen może obsługiwać od 50 do 500 systemów.
- Inne serwery w domenie, które nie są serwerami domen, są nazywane serwerami zasobów i aplikacji.
  - Mogą mieć także inne określenia w zależności od wykonywanych zadań: serwer plików i wydruku, serwer tworzenia kopii zapasowej, serwer odpowiedzialny za bezpieczeństwo lub jakikolwiek inny wymagany przez serwer usługi katalogowej.

Usługi katalogowe

- Usługi katalogowe przechowują metadane, czyli dane dotyczące danych.
- W obiektowej bazie danych przechowującej dane sieciowe metadane dostarczają kontekstu pozwalającego systemowi na określenie sposobu organizacji danych.
- Schemat katalogu definiuje zestaw klas obiektu, do których są przypisane zestawy atrybutów wymaganych bądź opcjonalnych.
- Kiedy to tylko możliwe, większość usług katalogowych używa klas obiektu, atrybutów i numerów identyfikacyjnych, które są zarejestrowane przez IANA (ang. Internet Assigned Numbers Authority) jako standardy.
- Każdy obiekt będący zasobem chronionym jest dołączony do listy ACL (ang. Access Control List), która określa, kto może używać tego obiektu.

- Usługa katalogowa staje się konieczna, kiedy względem sieci zostają wysunięte następujące wymagania:
  - scentralizowane zarządzanie usługami sieciowymi;
  - zdefiniowana polityka bezpieczeństwa wraz z odpowiednio dobranymi uprawnieniami;
  - możliwość przydzielenia różnym osobom odpowiedzialności za określone zasoby;
  - możliwość skalowania sieci w celu obsługi większej liczby użytkowników, niż jest obsługiwana w modelu „równy z równym”;
  - możliwość obsługi różnorodnych klientów oraz systemów operacyjnych;
  - możliwość przeprowadzania nadzoru zdarzeń sieciowych.

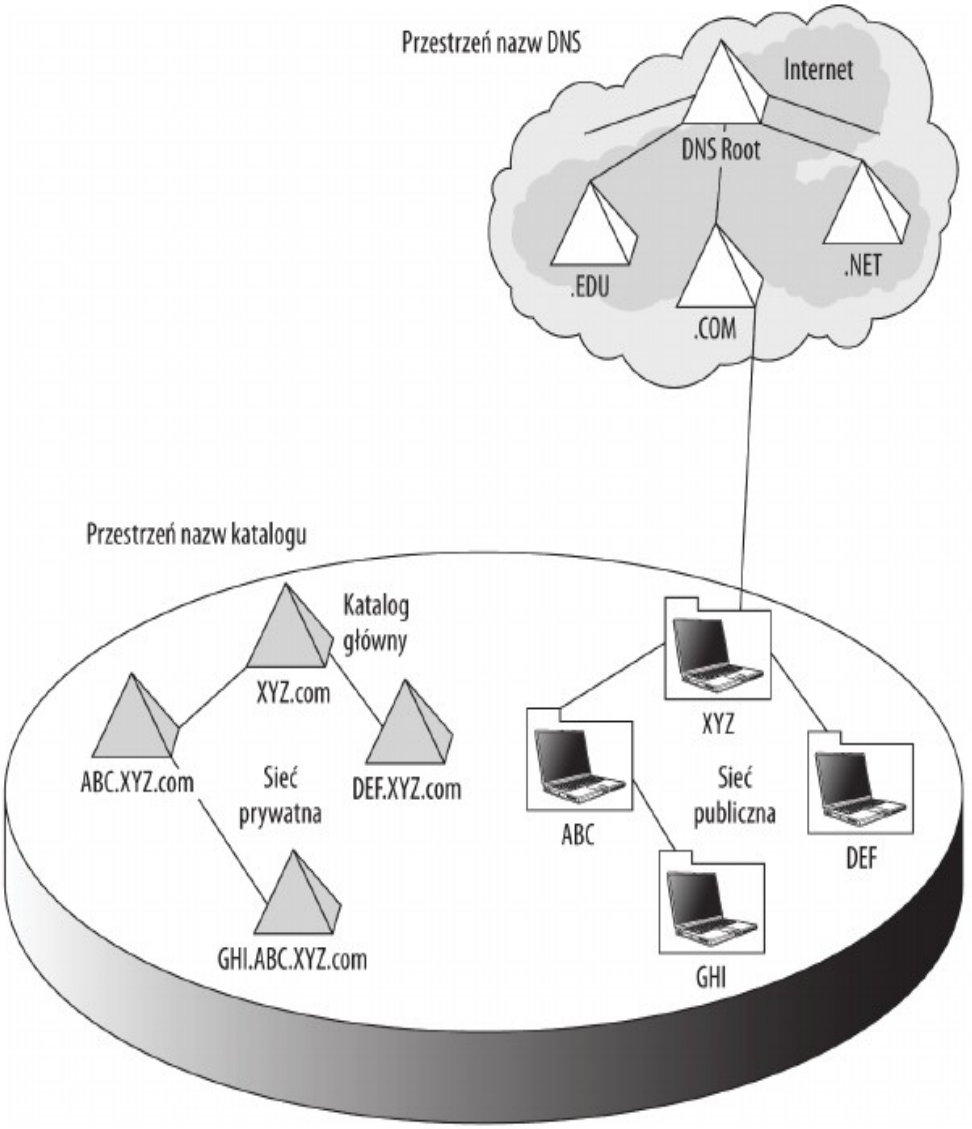
Wady

- Usługi katalogowe mają nie tylko zalety, lecz także pewne wady.
- Oprócz dodatkowego kosztu i zwiększenia stopnia skomplikowania sieci do prawidłowego funkcjonowania usługi katalogowe wymagają również usług domeny, które zawsze powinny być dostępne w sieci.
- W większości przypadków te dodatkowe wymagania ograniczają wykorzystanie domen w sieciach domowych i małych biurach, gdzie podłączonych jest mniej niż 20 systemów.

Przestrzenie nazw

- Usługa katalogowa definiuje przestrzeń nazw dla wszystkich przechowywanych obiektów.
- Aby zapewnić efektywność, przestrzeń nazw musi tworzyć unikalne oznaczenie, które powinno być logicznym połączeniem różnych gałęzi drzewa.
  - W przypadku DNS będzie to URI (ang. Uniform Resource Identifier).

- Wiele organizacji zastosowało dla domen schemat nazw odpowiadający sposobowi, w jaki DNS oznacza strukturę katalogów witryny internetowej.
  - możliwość późniejszego udostępnienia w internecie struktury domeny bez konieczności wprowadzania znaczących zmian w nazewnictwie.



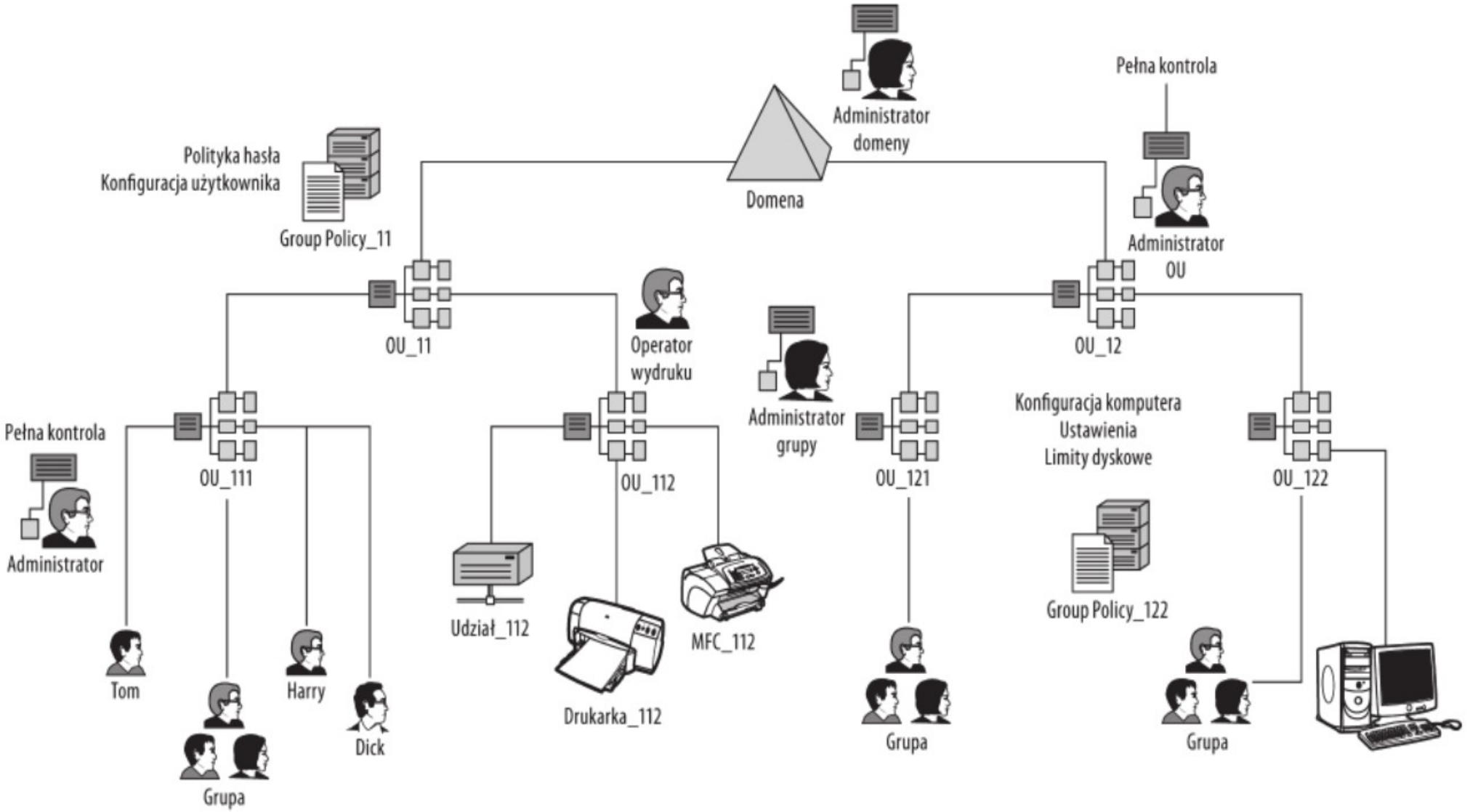
- Jeżeli w sieci prywatnej ma być używana publiczna przestrzeń nazw DNS,
  - na przykład .com, .gov lub .edu,
- to trzeba się upewnić, że wewnętrzne i zewnętrzne nazwy domen nie kolidują ze sobą.
- Publiczny serwer DNS powinien być skonfigurowany w celu przekazywania żądań adresów do wewnętrznego serwera DNS sieci prywatnej.

Polityka

- Podczas przechowywania w bazie danych obiektów z informacjami sieciowymi możliwe jest utworzenie zestawu reguł, które będą określały sposób używania tych obiektów.
- Wspomniane reguły są przechowywane oddzielnie od mechanizmu bezpieczeństwa wykorzystywanego przez sieciowy system operacyjny, choć niektóre reguły mogą się wzajemnie nakładać.

- Polityka będzie definiowała pewne zachowanie sieciowe, włączając w to między innymi:
  - konfigurację systemu klienta;
  - częstotliwość przeprowadzania uaktualnień i instalacji poprawek;
  - zachowanie mechanizmu nadzoru;
  - stopień skomplikowania haseł;
  - zadania przeprowadzane w trakcie operacji logowania i wylogowania.

- Najbardziej znaną usługą zarządzania polityką jest Group Policies firmy Microsoft (przechowywana w Active Directory).
- SRM (ang. Solaris Resource Manager) firmy Sun oferuje zarządzanie polityką ustawiania ograniczeń zasobów.
  - Za pomocą SRM można określić maksymalną liczbę dozwolonych procesów, połączonych użytkowników, liczbę operacji logowania itp.
  - Za pomocą skryptów SRM może wprowadzać nowe zasady polityki tuż po uruchomieniu systemu operacyjnego.
  - Każdy sieciowy system operacyjny implementuje pewną formę zarządzania polityką.
- Po rozpoczęciu przeglądania usług zarządzania polityką oferowanych przez firmy trzecie można się przekonać o dostępności ogromnej ilości rozwiązań.


Administrator domeny
Pełna kontrola
Polityka hasła
Konfiguracja użytkownika
Domena
Group Policy_11
Administrator OU
OU_11
Operator wydruku
OU_12
Administrator grupy
Pełna kontrola
OU_111
OU_112
OU_121
Konfiguracja komputera
Ustawienia
Limity dyskowe
OU_122
Administrator
Udział_112
MFC_112
Group Policy_122
Tom
Harry
Drukarka_112
Grupa
Dick
Grupa
Grupa

Server IDA

Serwer IDA (ang. Identity and Access) musi funkcjonować w różnych systemach sieciowych, aby mógł być użyteczny.

- W przypadku serwera IDA może być konieczne zapewnienie obsługi następujących funkcji:
- Zarządzanie certyfikatami oraz kartami smart card, a także połączeniami z różnymi usługami certyfikacji.
- Zapewnienie federacyjnej usługi wśród wielu usług katalogowych znajdujących się w sieci; zadaniem tej usługi będzie przekazywanie tożsamości między nimi.
  - Najważniejsze usługi katalogowe, których obsługę należy zapewnić, to Microsoft Active Directory, Sun Directory Server, Novell eDirectory oraz IBM Tivoli Directory Server.
- Praca z usługami tożsamości poczty elektronicznej i komunikatorów internetowych oraz zapewnienie ich synchronizacji, jeśli to konieczne.
  - Lotus Notes i Microsoft Exchange to przykłady dwóch serwerów przechowujących tożsamości, którecz̨sto współdziałają z tożsamościami innych usług katalogowych.
- Zarządzanie tożsamościami sieciowej bazy danych tak, aby użytkownik nie mógł się do niej zalogować bez ważnej tożsamości.
  - Oracle, IBM DB2 oraz Microsoft SQL Server to przykłady systemów zarządzania bazami danych, które mogą przechowywać własne konta użytkowników.
- Praca z aplikacjami korporacyjnymi, takimi jak SAP, aplikacje telefoniczne itd.

X500

- Przemysł telekomunikacyjny utworzył standard w celu umożliwienia współpracy różnych katalogów.
- Standard ten nosi nazwę X.500 Directory Access Protocol (DAP). Protokół ten jest akceptowany przez sieć dowolnego rodzaju. Standard DAP może przechowywać informacje o obiektach dowolnej z siedmiu warstw modelu ISO/OSI.
- W protokole X.500 klient może wykonać zapytanie do serwera w usłudze katalogowej, używając DAP do komunikacji.
- Następnie DSA (ang. Directory System Agent), czyli baza danych przechowująca informacje, udziela odpowiedzi na to żądanie. Bazy danych DSA są hierarchiczne i połączone ze sobą za pomocą drzewa DIT (ang. Directory Information Tree).
- Z kolei DUA (ang. Directory User Agent) to program taki jak whois, finger bądź polecenie GUI uzyskujące dostęp do DSA

NIS

- NIS (ang. Network Information Service) to bazujący na RPC system katalogowy klient-serwer przechowujący w bazie danych nazwy użytkowników i systemów dla komputerów w sieci.
- Ponadto NIS definiuje zestaw procesów używanych w celu zarządzania i uzyskiwania dostępu do usługi katalogowej.
- Za pomocą NIS administrator może zdefiniować domenę NIS współdzielącą zestaw powszechnie używanych plików konfiguracyjnych.
- Operacje dodawania tych plików konfiguracyjnych do nowych systemów lub ich modyfikacja mogą być przeprowadzane zdalnie i są względnie łatwe.

Serwery LDAP

- Obecnie niemal wszystkie nowoczesne usługi katalogowe bazują na protokole LDAP, który zapewnia możliwość współdziałania.
- Dwoma wyjątkami, o których trzeba tutaj wspomnieć, są DNS (ang. Domain Name System) i NIS (ang. Network Information System), opracowane przed powstaniem standardu X.500 i LDAP.
- Lista kilku z wielu usług katalogowych bazujących na LDAP:
  - Microsoft Active Directory
  - Novell eDirectory (wcześniej NDS, czyli NetWare Directory Services);
  - Fedora Directory Server;
  - OpenDS;
  - Oracle Directory Server Service Plus;
  - IBM Tivoli Directory Server;
  - Apple Open Directory;
  - ApacheDS.

LDAP – nazwy wyróżniające

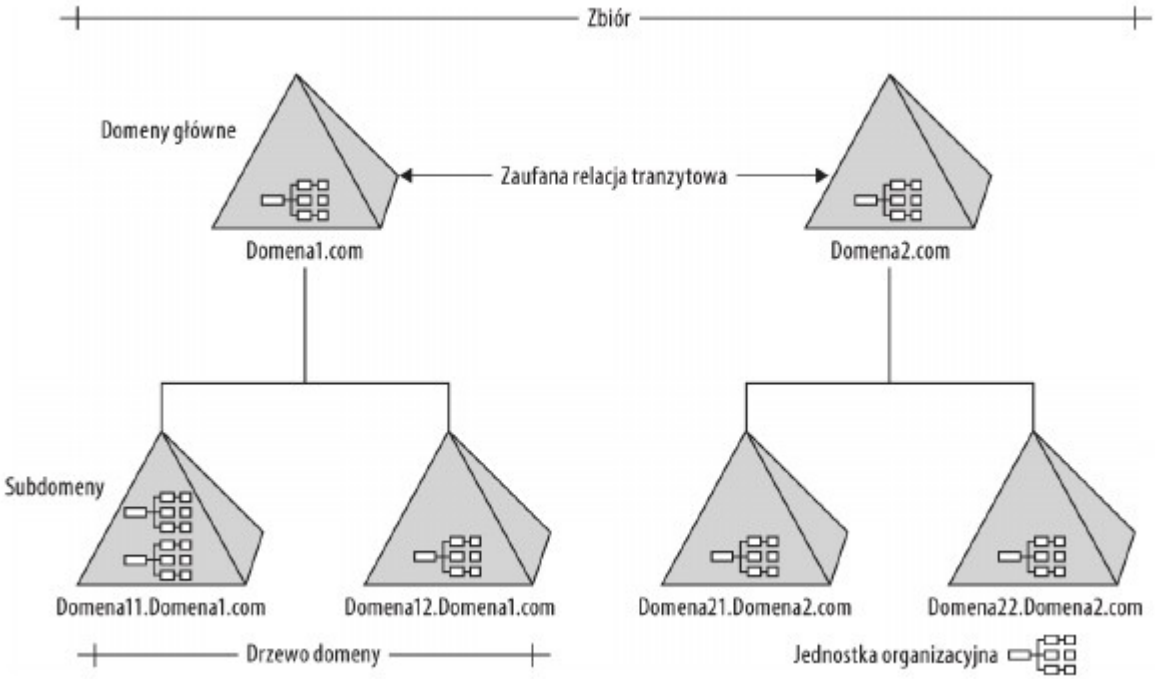
Wszystkie katalogi LDAP współdzielą zestaw zdefiniowanych obiektów oraz powszechnych metod adresowania, które tworzą nazwę wyróżniającą (ang. Distinguished Name, DN) dla obiektu. Funkcje katalogu LDAP to:

- **Drzewo katalogu.** Hierarchiczne drzewo wraz z obiektami katalogu jako węzłami.
- **Węzły**. Węzły to nazwane obiekty pojemników bądź jednostek, którym przypisano zestaw właściwości lub atrybutów. LDAP pozwala na to, aby obiekty miały możliwości rozszerzania, czyli definiowania dodatkowych właściwości.
- **Atrybuty**. Atrybut jest właściwością, której nazwa jest uznawana jako typ lub opis. Atrybuty mogą mieć jedną lub wiele wartości.
- **Wpisy**. Wpis stanowi unikalny egzemplarz typu obiektu. Obiekt może mieć przypisaną nazwę wyróżniającą i przez porównanie z jego węzłem nadrzędnym może mieć przypisany RDN (ang. Relative Distinguished Node).

LDAP – nazwy wyróżniające

- Nazwa wyróżniająca jest bardzo ważna, ponieważ pozwala systemowi na wyszukanie i pobranie informacji.
- Dzięki nazwie wyróżniającej wiadomo, w jaki sposób obiekt jest powiązany z wieloma innymi obiektami.
- Ogólnie rzecz biorąc, to sposób zapewnienia relacji „jeden do wielu”, która nie jest bezpośrednio obsługiwana w usługach katalogowych.

- Kolekcja domen może być ze sobą połączona w postać zbioru — każda domena będzie miała własną bazę danych bezpieczeństwa.
- Aby w sieci możliwa była komunikacja użytkowników i systemów w różnych domenach, trzeba nawiązać zaufaną relację.
- **Kontrolery domen w zbiorze** zawierają informacje o innych domenach w zbiorze dzięki użyciu **replikacji**.
- Zaufana **relacja tranzytowa** spełnia następujący warunek: jeśli automatyczna zaufana relacja istnieje między domenami A i B oraz B i C, to zaufana relacja istnieje również między domenami A i C.




MEMYTUTAJ.PL
DZIĘKUJĘ ZA UWAGĘ
WSZYSTKIM KTÓRZY NIE ZASNĘLI :)