Sieciowe systemy operacyjne: Microsoft Windows Server i Novell

Cele: poznanie systemów operacyjnych, sieci komputerowych i nowych technologii.

Uczeń wymienia i charakteryzuje ogólnie sieciowe systemy operacyjne

Pojęcie sieci komputerowej

- **Sieć komputerowa** - *zespół urządzeń i oprogramowania pozwalającego na połączenie komputerów (terminali sieci) w celu wymiany danych, korzystania ze wspólnych zasobów (dysków, pamięci, informacji, programów, urządzeń peryferyjnych).*
- Jest to **zespół komputerów** i towarzyszących im **urządzeń peryferyjnych**.
  Urządzenia i komputery w sieci mogą się ze sobą komunikować.
- **Sieć komputerowa** jest to cały **zbiór sprzętu i oprogramowania**.
  Umożliwia wymianę informacji miedzy różnymi komputerami

Główne zadania sieci, urządzenia sieciowe

- Głównym zadaniem sieci jest podłączenie użytkowników do wspólnych **zasobów**, takich jak np. *dyski twarde, fax modemy, drukarki.*
- **Urządzeniami** niezbędnymi do uruchomienia sieci komputerowej są:
  - **komputery centralne** (**serwer**, **host**),
  - karty sieciowe,
  - okablowanie (skrętki, kable koncentryczne)
  - **sieciowy system operacyjny (NOS).**

  Przy większej liczbie terminali pracę sieci komputerowej wspomagają **koncentratory** aktywne i pasywne (hub) - do realizacji rozgałęzień.
- Transmisję między różnymi rodzajami sieci mogą wspomagać modemy, routery, bramki komunikacyjne (gateway), mosty (bridge) i tranceivery.

Podział sieci komputerowych

- Ze względu na sposób zdefiniowania komputera centralnego rozróżnia się sieci typu:
  - **Klient - serwer** (dedykowany serwer)
  - **Peer to peer** *(równorzędnych komputerów), gdzie rolę komputera centralnego można określić na poziomie oprogramowania.*
- Ze względu na zasięg sieci komputerowe dzieli się na:
  - **LAN** (lokalne)
  - **WAN** (rozległe)
  - **MAN** (metropolitalne)

Sieciowe Systemy operacyjne - SSO
NOS (*Network Operating System*)

- System operacyjny (OS)-stanowi programową podstawę, na której działają wszystkie programy i usługi
- **Sieciowy system operacyjny** (NOS)-umożliwia komunikacje miedzy wieloma urządzeniami a także zasobami sieci.
- Sieciowy system operacyjny tworzy środowisko, w którym użytkownicy maszyn mają dostęp zasobów sieciowych. Rejestrują się na zdalnych maszynach przesyłając dane między nimi i/lub własną maszyną.

Sieciowe systemy plików – SSO (NSO)

- Wsparcie przesyłania danych realizują sieciowe systemy plików, np:
  - NFS (*network file system*) - UNIX
  - SMB (*samba*) - Windows
  - NCP - Novell
- Do komunikacji SSO niezbędna jest sieć komputerowa, w której komputery porozumiewały się będą przy pomocy odpowiedniego protokołu, np.
  - TCP/IP - sieć Internet
  - IPX/SPX - siec Novell
  - NetBEUI - sieć komputerów pod kontrolą Windows

Charakterystyka sieciowych systemów operacyjnych:

- Systemy **wielodostępne** - umożliwia dostęp wielu użytkowników jednocześnie
- Systemy **wielozadaniowe-** musi pozwalać na wykonywanie wielu zadań i procesów jednocześnie
- Systemy **wieloprocesorowe**

Przykładowe systemy sieciowe

- **Microsoft Windows NT 4.0, Microsoft Windows 2000, Windows Server 2003, Windows Server 2008**
- **Novell Network**
- **Linux**
- **Unix**
- **Macintosh OS**

Sieciowe Systemy operacyjne Windows

- NT
- 2000,
- Windows Server 2003,
- Windows Server 2008

Microsoft Windows NT
(*New Technology*)

- Rodzina 32- i 64-bitowych systemów operacyjnych firmy Microsoft, początkowo przeznaczonych do *zastosowań profesjonalnych,* obecnie z tej rodziny pochodzą także najpopularniejsze systemy dla użytkowników domowych.
- Rodzina systemów NT, wywodzi się z systemu OS/2, nad którym pracowali Microsoft razem z IBM.
- Najnowsza stabilna wersja NT dla komputerów osobistych i stacji roboczych to 6.1 czyli Windows 7,
  a dla serwerów **Windows Server 2008 R2**.
- System NT działa wielozadaniowo i z wywłaszczeniem.
  Daje się przenosić na różne architektury procesorów.

Podstawowe cele systemu NT

- **przenośność**
- **bezpieczeństwo**
- częściowa zgodność ze standardem IEEE 1003 interfejsu przenośnego systemu operacyjnego
- możliwość korzystania z wielu procesorów
- **rozszerzalność**
- adaptacje międzynarodowe
- deklarowana zgodność z aplikacjami **MS-DOS**

Microsoft Windows 2000

- Biznesowy , 32-bitowy, wielozadaniowy z wywłaszczaniem, wielowątkowy, system operacyjny z serii NT.
- Jest to kolejny system operacyjny należący do rodziny Microsoft Windows NT. Został wydany 17 lutego 2000 roku. Jego następcami są **Windows XP**, wydany w październiku 2001 roku, oraz **Windows Server 2003,** wydany w kwietniu 2003 roku.
- Windows 2000 jest klasyfikowany jako system operacyjny o jądrze hybrydowym.

Wersje Windows 2000

- Powstały cztery edycje systemu operacyjnego Windows 2000:
  - **Professional,**
  - **Windows Server 2000,**
  - **Advanced Server, i**
  - **Datacenter Server.**
  - Ponadto Microsoft wydał także wersję **Advanced Server Limited Edition** i **Datacenter Server Limited Edition**, które zostały wprowadzone na rynek w 2001 roku i obsługiwały 64-bitowe mikroprocesory Intel Itanium.
- Mimo, że poszczególne edycje systemu operacyjnego Windows 2000 są przeznaczone dla różnych rynków docelowych, wszystkie dzielą zestaw najważniejszych funkcjonalności, włączając w to wiele narzędzi systemowych, takich jak Microsoft Management Console i aplikacje standardowe systemu administracji.
- Wszystkie wersje tego systemu operacyjnego obsługują system plików Windows NT, NTFS 3.0, z możliwością szyfrowania plików, jak również zwykłe i dynamiczne zarządzanie dyskami.

Cechy Windows 2000

- Rodzina Microsoft Windows 2000 posiada dodatkową funkcjonalność, włączając w to usługę Active Directory (hierarchiczny szkielet zasobów),
- Posiada możliwość pracy z systemem plików NTFS i FAT32, lepsze zabezpieczenia logowania, prawa dostępu do plików i ich szyfrowanie i kompresowanie (tylko NTFS), przydział pamięci dyskowej dla użytkowników, obsługi większości urządzeń cyfrowych.
- Windows 2000 jest pierwszym systemem z serii NT obsługującym technologię USB i IrDA.
- Na komputerach pracujących pod kontrolą tego systemu możliwe jest uruchamianie aplikacji napisanych dla DOS i Windows 3.x.
- Windows 2000 jest ostatnim pozbawionym konieczności aktywacji wydaniem systemu Windows z linii NT.

Windows Server 2003

- **Windows Server 2003** – wersja systemu Windows, oparta na edycji XP, przeznaczona do zastosowań serwerowych (NT Server).
- System wydany został 24 kwietnia 2003, a podstawowe wsparcie techniczne zakończy się 13 lipca 2010
- W porównaniu do wersji 2000 wprowadzono lub poprawiono wiele funkcji sieciowych.
  Do najważniejszych należą między innymi
  - **IIS** w wersji 6.0,
  - poprawki w usłudze **Active Directory**,
  - a także dodanie funkcji Kopii w tle.
- System nadal może współpracować z systemami plików FAT, FAT32 i **NTFS**.
- Wyposażono go w platformę **NET Framework** w wersji 1.1.
- System wyposażono w specjalną edycję przeglądarki Internet Explorer.
- Program jest też skonfigurowany w ten sposób, że praktycznie niemożliwe jest uruchamianie lub ściągnięcie plików lub rozszerzeń, które mogą zaszkodzić systemowi.

Edycje systemu Windows Server 2003
zależnie od zastosowań:

- Small Business Server,
- Web Edition,
- Standard Edition,
- Enterprise Edition,
- Datacenter Edition.

Bezpieczeństwo Windows Server 2003

- Microsoft w Windows 2003 Server położył szczególny nacisk na **bezpieczeństwo**, które w najnowszej wersji Windows było najważniejszym celem, jaki przyświecał projektantom i programistom tego systemu.
- Na **bezpieczeństwo** w Windows 2003 Server składa się kilka kluczowych elementów:
  - różne sposoby autoryzacji i identyfikacji użytkownika,
  - listy dostępu i praw
  - **polisy** i inne mechanizmy pozwalające tworzyć spójną politykę bezpieczeństwa obejmującą różne aspekty działania serwera

Autoryzacja

- **Autoryzacja** jest procesem weryfikacji obiektu – czy rzeczywiście jest tym, za kogo się podaje.
- Najpowszechniejszym przykładem autoryzacji jest logowanie się użytkownika do systemu.
  W najprostszym przypadku – podaje swój identyfikator oraz hasło.
  Jednak Windows 2003 Server obsługuje także **smart card** czy inne mechanizmy przekazywania informacji do autoryzacji.
- Kontrola oparta na liście praw dostępu.

Prawa

- **Prawa** definiują, *jakie operacje dany użytkownik (a raczej element o danym numerze SID) może wykonać na określonym obiekcie*.
- Prawa mogą być przypisane m.in. do następujących obiektów:
  - **użytkowników/grup** danej domeny,
  - **komputerów** i innych „specjalnych” obiektów występujących w Active Directory,
  - użytkowników czy grup należących do innej domeny, która jest połączona relacją zaufania z daną domeną,
  - lokalnie zdefiniowanych użytkowników/grup na danym komputerze.

Polisy

- **W Windows 2003** rozbudowane zostały możliwości tworzenia tzw. **polis bezpieczeństwa**.
  Dzięki nim administrator określa zestaw uprawnień obowiązujących w danej sieci.
- Dzięki mechanizmowi dystrybucji, **polisy** (czyli – zasady bezpieczeństwa) są *dystrybuowane na każdy z komputerów w sieci*.
- Polisa jest zbiorem zasad określających ogólne uprawnienia komputera pełniącego określoną rolę w domenie czy też prawa użytkownika.
- Określane są zasady postępowania z hasłami *(minimalna długość, po jakim czasie hasło musi zostać zmienione itp.)*, w jakich warunkach konto jest blokowane, dokładne mechanizmy dystrybucji informacji w Kerberos czy zasady audytu.
- Polisy mogą obowiązywać na lokalnym komputerze jak i na komputerach wykorzystującą usługę katalogową.
  Mechanizm ustawiania polis oraz zakres elementów jest bardzo podobny – w zależności od tego, gdzie polisa ma obowiązywać, należy otworzyć odpowiednią konsolę MMC – Ustawienia zabezpieczeń lokalnych, Ustawienia zabezpieczeń domeny lub Ustawienia zabezpieczeń kontrolera domeny

Prawa do uruchomiania aplikacji

- W Windows 2003 Server można na poziomie polis ustalać prawa do uruchamiania (dotyczy to zwłaszcza serwerów 2003 oraz stacji roboczych działających pod kontrolą Windows XP).
- Używając ustawień zabezpieczeń (czy to lokalnych, czy też na poziomie katalogu) można:
  - ograniczyć uruchamianie nieznanych programów *(w tym – wirusów)*
  - określić, jakiego typu komponenty ActiveX *mogą być ściągane i uruchamiane na komputerze*
  - wymóc, by można było uruchamiać tylko skrypty podpisane cyfrowo

Active Directory (AD)

- **AD**, to usługa katalogowa (hierarchiczna baza danych) dla systemów Windows – Windows 2003 Server oraz Windows 2000, będąca implementacją protokołu LDAP.
- W Active Directory *informacje grupowane są hierarchicznie.*
  Podstawową jednostką jest tzw. **liść**, który położony jest w **kontenerze** w Active Directory *nazywanym jednostką organizacyjną (ang. organizational unit, OU).*
  Liście i kontenery zorganizowane są w **domeny**.

Drzewo

- Domeny zorganizowane hierarchicznie mogą tworzyć strukturę **drzewa**.
- Drzewo posiada zawsze przynajmniej jedną domenę – domenę najwyższego poziomu (ang. root) – korzeń drzewa.
- Pozostałe domeny (o ile istnieją) mogą być umieszczone poniżej domeny najwyższego poziomu, tworząc drzewo.
  Niższe poziomy mogą się rozgałęziać.

Las

- Każde drzewo znajduje się w jakimś lesie (ang. forest).
- Las składa się z przynajmniej jednego drzewa. *Nie istnieje możliwość utrzymywania drzewa bez utrzymywania lasu*.
- *Uwaga ta odnosi się również do domeny Active Directory – domena nie może istnieć samodzielnie, musi istnieć w jakimś drzewie i jakimś lesie.*
  Jeżeli jest to pierwsza domena, to tworzy pierwsze drzewo (którego korzeniem się staje) oraz pierwszy las. Las bierze nazwę od tej domeny

Różnice między grupą roboczą a domeną

- W **grupie roboczej** *lista kont użytkowników, uprawnienia użytkowników i zabezpieczenia systemów (zasady) przechowywane są lokalnie,*
  tzn. osobno na każdym komputerze wchodzącym w skład grupy roboczej. Każdy komputer jest jednostką autonomiczną.
  - Aby móc pracować (zalogować się) na komputerze należącym do grupy roboczej, trzeba mieć konto na tym komputerze.
  - W przypadku osób pracujących na więcej niż jednym komputerze oznacza to konieczność powielania kont na różnych komputerach (i pamiętanych do nich haseł).
- W ***domenie*** zarządzanie informacją o kontach użytkowników, komputerach domeny oraz zasadach obowiązującymi w domenie jest scentralizowane.
  - Komputery współdzielą bazę danych kont, zasad, zabezpieczeń, która znajduje się w kontrolerach domeny.
  - W trakcie logowania się na konto w domenie Windows, dane użytkownika porównywane są z danymi zapisanymi w kontrolerze domeny.
  - Przestaje mieć znaczenie z którego konkretnie komputera loguje się dany użytkownik

Kontroler domeny

- **Kontroler domeny** - *jest to komputer w domenie, który zarządza realizacją wszystkich działań związanych z bezpieczeństwem zachodzących między użytkownikiem a domeną oraz ustala w jaki sposób użytkownicy mogą uzyskiwać dostęp, konfigurować czy korzystać z zasobów domeny, co przyczynia się do poprawienia procesu zarządzania zasobami i zabezpieczeniami.*
- Kontroler domeny *pełni rolę administratora danej domeny czy jednostki organizacyjnej w domenie* np. drzewa domen, lasu.
- Kontroler domeny umożliwia przydzielanie uprawnień do administrowania i zarządzania obiektami w całej domenie albo w jednej lub kilku jednostkach organizacyjnych.
  To pozwala ograniczyć liczbę administratorów czyli kontrolerów z szerokimi uprawnieniami
- Kontroler domeny wymaga systemu operacyjnego typu serwer – w rodzinie systemów MS Windows są to: Windows 2008 Server, Windows 2003 Server, Windows 2000 Server albo Windows NT Server.
- Możliwe jest również uruchomienie kontrolera domeny na systemie Linux, po zainstalowaniu pakietu **Samba**, *jednakże tak powstała domena nie będzie miała wszystkich funkcjonalności domeny Active Directory.*

Microsoft Windows Server 2008

- Kolejna wersja serwerowego systemu operacyjnego opracowywanego przez firmę Microsoft.
  Do 15 maja 2007 był znany jedynie pod nazwą kodową ***Windows Server "Longhorn"*.**
  Jest on następcą systemu Microsoft Windows Server 2003 i został oparty na tym samym jądrze co system Microsoft Windows Vista SP1. Premiera odbyła się 27 lutego 2008
- Windows Server 2008 jest ostatnim systemem serwerowym wydanym w wersji 32-bitowej.
  Przyszłe wersje (począwszy od Windows Server 2008 R2) będą tylko 64-bitowe.

Korzyści i zmiany w Windows Serwer 2008

- Windows Server 2008 przyniósł kilka znaczących nowości,
  z których prawdopodobnie najciekawszą jest
  *tryb instalacji **Core**, w którym nie jest instalowany graficzny menedżer powłoki explorer.exe ani inne programy posiadające GUI z wyjątkiem notatnika, edytora rejestru i menedżera zadań.*
- **Zarządzanie** odbywa się przez wiersz poleceń cmd.exe albo **Power Shell** lub zdalnie przez połączenie z użyciem **Microsoft Management Console.**

Oprócz tego Windows Server 2008 przyniósł:

- serwer Internet Information Services w wersji 7, podobnie jak Windows Vista
- ulepszony model łatek, nie wymagający restartów systemu
- przyspieszoną instalację z użyciem Windows Imaging Format, podobnie jak Windows Vista
- nowe narzędzia do zarządzania, zorientowane na role wykonywane przez serwer
- znacznie usprawnione usługi terminalowe (obsługa RDP w wersji 6.0) z możliwością uruchamiania tylko jednej aplikacji, zamiast całego pulpitu
- SharePoint Services 3.0
- Server Message Block 2.0, podobnie jak Windows Vista
- znaczne zmniejszenie jądra systemu – wiele dotychczasowych jego funkcjonalności, m.in. menedżer okien, zostało przeniesione do usług