Temat: Wprowadzenie do sieciowych systemów operacyjnych.

Celem ogólnym lekcji jest wprowadzenie uczniów do podstawowych pojęć związanych z sieciowymi systemami operacyjnymi oraz zrozumienie roli, funkcji i odpowiedzialności administratorów sieci w zarządzaniu i utrzymaniu sieci komputerowych.

Cele szczegółowe lekcji: Po zakończeniu lekcji uczniowie powinni być w stanie:

1) Wyjaśnić pojęcie sieci komputerowej oraz zrozumieć, jakie cele może spełniać budowa sieci.
2) Opisać, czym są sieciowe systemy operacyjne (NOS) oraz jakie są ich główne cechy i funkcje.
3) Zrozumieć różnice między sieciami równorzędnymi (peer-to-peer) a sieciami klient-serwer.
4) Omówić architekturę klient-serwer w kontekście sieciowych systemów operacyjnych.
5) Przedstawić główne funkcje sieciowych systemów operacyjnych, takie jak współdzielenie zasobów, zarządzanie użytkownikami, serwery i usługi, bezpieczeństwo oraz zarządzanie zdalne.
6) Wymienić różne typy serwerów występujących w sieciowych systemach operacyjnych oraz ich funkcje.
7) Wyjaśnić pojęcie usług katalogowych oraz przedstawić przykłady różnych usług katalogowych, takich jak Active Directory, eDirectory, OpenLDAP itp.
8) Zrozumieć rolę i zadania administratorów sieciowych oraz wyjaśnić, dlaczego ich rola jest kluczowa w utrzymaniu działania sieci.
9) Omówić obszary, na które administratorzy sieci muszą zwracać uwagę, takie jak bezpieczeństwo, monitorowanie, zarządzanie zasobami, planowanie pojemności itp.
10) Zrozumieć znaczenie ciągłego rozwoju i edukacji w pracy administratora sieciowego oraz zdać sobie sprawę z roli certyfikacji branżowych.

Podczas lekcji uczniowie będą mieli okazję poznać podstawowe pojęcia i zagadnienia związane z sieciowymi systemami operacyjnymi oraz zrozumieć, jakie umiejętności i zadania są wymagane od administratorów sieci w dynamicznym środowisku sieciowym.

A. Sieć komputerowa

Sieć komputerowa to zbiór urządzeń połączonych ze sobą kanałami komunikacyjnymi oraz oprogramowanie w niej wykorzystywane, służy do łączenia punktów sieci, które mogą wymieniać informacje i współdzielić zasoby w postaci danych, sprzętu, usług i umożliwienie pracy grupowej.

Wyjaśnię elementy tej definicji:

Kanały komunikacyjne: W definicji mogłabyś dodać, że kanały komunikacyjne mogą być fizyczne (np. przewody, światłowody) lub logiczne (np. połączenia przez Internet).

Punkty sieci: Punkty sieci to nie tylko komputery i drukarki, ale także inne urządzenia, takie jak routery, przełączniki (switch-e), access pointy (do tworzenia sieci bezprzewodowych) itp.

Współdzielenie zasobów: To jest kluczowy aspekt sieci komputerowych. Pozwala użytkownikom na łatwy dostęp i wymianę danych, plików, urządzeń czy nawet aplikacji. Jest to jedno z głównych założeń, które różni sieci od samodzielnie działających komputerów.

Praca grupowa: Jest ważnym elementem, ponieważ sieci umożliwiają użytkownikom pracę wspólnie nad danymi, projektami czy dokumentami, niezależnie od tego, gdzie się fizycznie znajdują.

B. Sieciowy system operacyjny

Sieciowe systemy operacyjne stanowią kluczowy element nowoczesnych środowisk informatycznych, umożliwiając skuteczne zarządzanie i udostępnianie zasobów w sieciach komputerowych.

Sieciowe systemy operacyjne (Network Operating Systems - NOS) to specjalistyczne rodzaje systemów operacyjnych, które są instalowane na serwerach i służą do zarządzania sieciami komputerowymi. Każdy sieciowy system operacyjny ma możliwość korzystania z protokołów np. TCP/IP, jest wielozadaniowy oraz potrafi wydajnie obsługiwać duże dyski twarde, duże pamięci podręczne, karty sieciowe. Głównym celem NOS jest zapewnienie skutecznej komunikacji, współdzielenia zasobów oraz dostarczania usług w sieciach. Dzięki NOS możliwe jest tworzenie środowisk pracy grupowej, udostępnianie plików, drukarek, baz danych oraz dostarczanie aplikacji.

Wyjaśnię elementy tej definicji:

Centralny punkt zarządzania: NOS są zaprojektowane głównie z myślą o obsłudze i zarządzaniu siecią komputerową. Są instalowane na serwerach, co pozwala na centralne zarządzanie zasobami sieciowymi, kontrolę dostępu użytkowników oraz monitorowanie stanu i wydajności sieci.

Protokoły i usługi: NOS są zoptymalizowane pod kątem pracy z różnymi protokołami, takimi jak TCP/IP, które są powszechnie wykorzystywane w sieciach. Oprócz tego, NOS dostarczają różnorodne usługi, takie jak udostępnianie plików, drukarek, baz danych czy aplikacji, które ułatwiają współpracę i wymianę informacji między użytkownikami.

Wielozadaniowość: To kluczowa cecha NOS, ponieważ serwery obsługujące sieci zazwyczaj muszą wykonywać wiele zadań jednocześnie, takie jak przetwarzanie żądań użytkowników, przekazywanie danych czy obsługa różnych aplikacji.

Wydajność i skalowalność: NOS muszą efektywnie zarządzać dużymi zasobami sieciowymi, takimi jak duże dyski twarde, pamięci podręczne czy karty sieciowe. To pozwala na obsługę dużej ilości użytkowników i zapewnia płynne działanie sieci nawet w obciążonych warunkach.

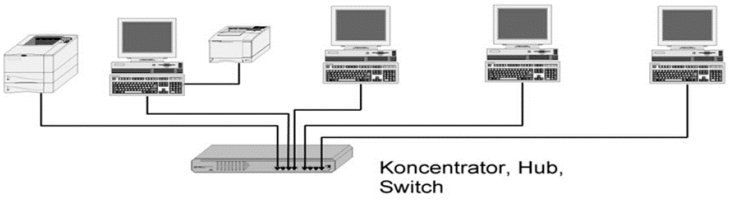
Współdzielenie zasobów: NOS także skupiają się na umożliwieniu współdzielenia zasobów, tak aby użytkownicy mieli łatwy dostęp do plików, drukarek czy aplikacji, niezależnie od swojej lokalizacji.

Tworzenie środowisk pracy grupowej: Dzięki NOS możliwe jest tworzenie środowisk, w których użytkownicy mogą wspólnie pracować nad projektami, udostępniać sobie dokumenty, a także korzystać z zasobów, które są dostępne w sieci.

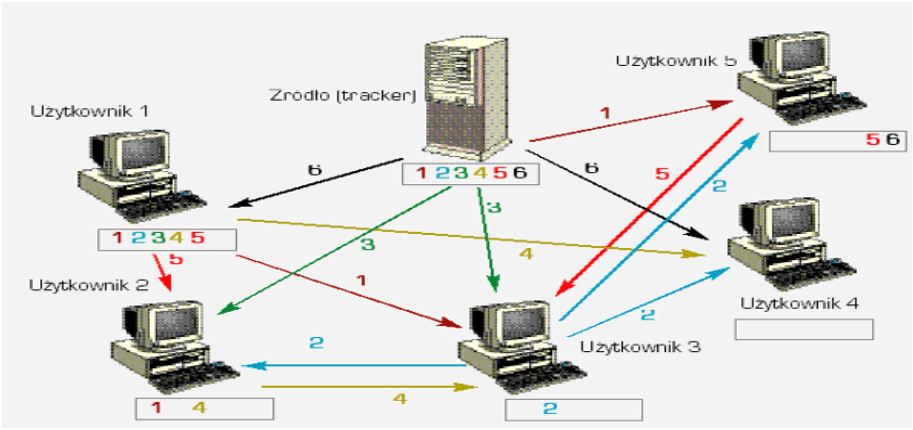
C. Typ sieci określa sposób udostępniania współdzielonych zasobów.

a) Sieci równorzędne - (peer-to-peer) każdy komputer może być klientem (korzystać z usług oferowanych przez inne urządzenia), serwerem (udostępniać usługi) lub jednocześnie klientem i serwerem. Rozwiązanie takie stosuje się w małych sieciach.

Każdy z użytkowników zarządza swoim komputerem i podejmuje decyzje, jakie zasoby udostępnić i komu, a informacje o udostępnionych zasobach przechowywane są na lokalnym komputerze.



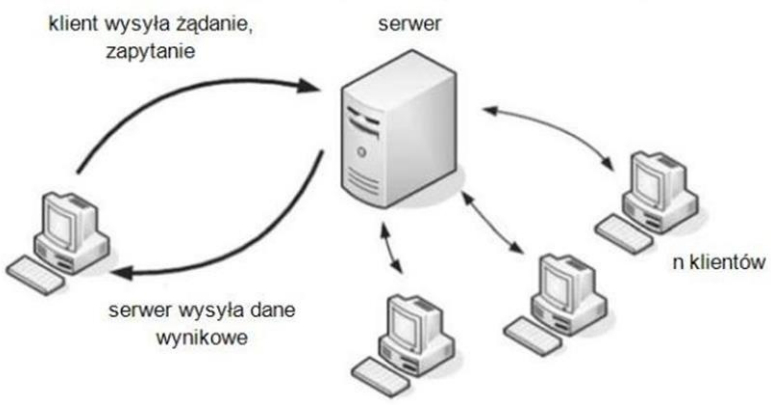
Przykład sieci peer-to-peer - sieć BitTorrent



Dodatkowe informacje:

1. Decentralizacja: W sieciach równorzędnych każdy komputer może pełnić rolę klienta, serwera lub obu jednocześnie. Brak centralnego serwera oznacza, że nie ma jednego punktu awarii, co zwiększa niezawodność i odporność sieci.
2. Skalowalność: Dzięki elastycznemu charakterowi sieci równorzędnych, można łatwo dodawać nowe urządzenia do sieci w miarę jej wzrostu. To ułatwia rozszerzanie sieci w miarę potrzeb.
3. Samodzielność użytkowników: W tym modelu każdy użytkownik jest odpowiedzialny za zarządzanie swoim komputerem i udostępniane zasoby. To daje większą kontrolę nad tym, kto ma dostęp do konkretnych danych.
4. Udostępnianie zasobów: Użytkownicy mogą udostępniać swoje pliki, foldery, drukarki czy inne zasoby. To umożliwia łatwe współdzielenie danych i usług między użytkownikami.
5. Lokalne przechowywanie informacji: Informacje o udostępnionych zasobach są przechowywane na lokalnym komputerze każdego użytkownika. To oznacza, że każdy użytkownik ma kontrolę nad tym, co udostępnia, i kto ma do tego dostęp.
6. Prostota w mniejszych sieciach: Model peer-to-peer jest szczególnie przydatny w małych sieciach, gdzie nie ma potrzeby skomplikowanej infrastruktury serwerowej. To tani i łatwy sposób na utworzenie sieci do współdzielenia plików czy drukarek.
7. Ograniczenia w skalowaniu: Choć sieci równorzędne są świetne w mniejszych środowiskach, mogą stać się mniej efektywne w większych sieciach, gdzie zwiększa się ilość urządzeń i komplikuje zarządzanie nimi.

b) Sieci o architekturze **klient-serwer** (**client-server**) urządzenia dzielą się na oferujące usługi (**serwery**) i korzystające z tych usług (**klienci**). Rozwiązanie to jest stosowane w większych sieciach. Sieć taka zarządzana jest przez użytkownika - administratora. Informacje o składnikach sieci, jej użytkownikach i zasobach przechowywane są na serwerze i udostępniane wszystkim użytkownikom sieci. Przykład komunikacji klient - serwer:



Dodatkowe informacje:

1. Podział na role: Urządzenia są jasno zdefiniowane jako serwery lub klienci. Serwery oferują różne usługi i zasoby, takie jak udostępnianie plików, bazy danych, aplikacji lub drukarek. Klienci korzystają z tych usług i zasobów, żądając ich od serwerów.
2. Skalowalność i zarządzanie: Ten model doskonale nadaje się do skalowalnych rozwiązań, ponieważ można łatwo dodawać nowe serwery w miarę wzrostu sieci, co umożliwia obsługę większej liczby klientów. Administratorzy mają centralną kontrolę nad zarządzaniem serwerami, co ułatwia monitorowanie, konfigurowanie i utrzymanie sieci.
3. Bezpieczeństwo i dostęp: Pozwala na zdefiniowanie dokładnych uprawnień dostępu do zasobów. Serwery mogą kontrolować, którzy klienci mają dostęp do określonych usług i danych. To pomaga w zabezpieczaniu informacji oraz unikaniu nieuprawnionego dostępu.
4. Efektywne zarządzanie zasobami: Dzięki centralnemu zarządzaniu na serwerze, administratorzy mogą skutecznie alokować, monitorować i optymalizować wykorzystanie zasobów, takich jak pamięć, przepustowość sieci, moc obliczeniowa itp.
5. Wspólna baza informacji: Przechowywanie informacji o składnikach sieci, użytkownikach i zasobach na serwerze ułatwia dostęp do tych danych przez różnych użytkowników. To zapewnia spójność i jednolitość informacji w sieci.
6. Komunikacja: Komunikacja między klientami a serwerami opiera się na żądaniach i odpowiedziach. Klienci wysyłają żądania, a serwery odpowiadają, dostarczając odpowiednie usługi lub zasoby.

D. Architektura klient-serwer w sieciowych systemach operacyjnych

W sieciowych systemach operacyjnych istnieje podział na rolę klienta i serwera, który ma kluczowe znaczenie dla efektywnego funkcjonowania sieci.

1. Model klienta cienkiego: W tym modelu większa część przetwarzania oraz zarządzania danymi odbywa się na serwerze. Klient pełni jedynie rolę uruchamiania oprogramowania prezentacyjnego, co pozwala na wydajne zarządzanie zasobami. Dodatkowe informacje:

a) Wydajność zasobów: Jednym z głównych atutów modelu klienta cienkiego jest to, że większość złożonych obliczeń i przetwarzania odbywa się na serwerze, co umożliwia bardziej efektywne wykorzystanie zasobów sprzętowych w centrach danych.

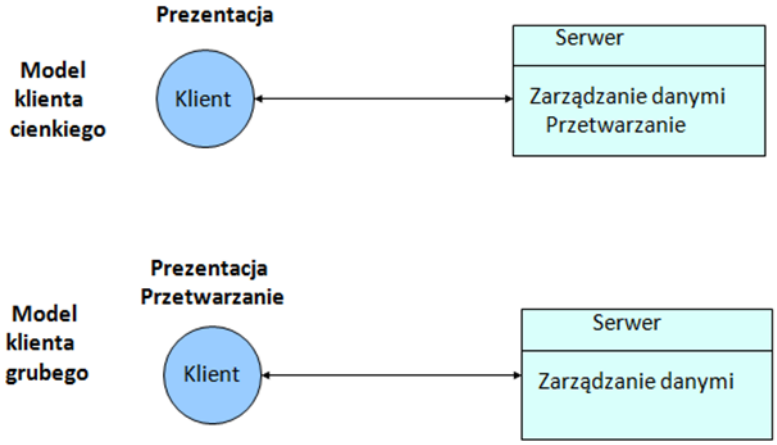
b) Zdalna administracja: Dzięki temu modelowi, administracja, aktualizacje i konserwacja oprogramowania mogą być skupione na serwerach, co upraszcza zarządzanie w porównaniu do tradycyjnego modelu, w którym konieczne jest aktualizowanie każdego klienta indywidualnie.

c) Zwiększona bezpieczeństwo: Dane i aplikacje znajdują się na serwerze, co może poprawić bezpieczeństwo, ponieważ utrzymanie centralnej ochrony i kontroli jest łatwiejsze niż na każdym pojedynczym urządzeniu klienta.
d) Łatwiejsze wdrożenie: Nowe klienty cienkie mogą być stosunkowo łatwe do wdrożenia, ponieważ nie wymagają kompleksowej konfiguracji aplikacji czy zasobów na każdym urządzeniu.
e) Ograniczone zasoby lokalne: Klient cienki zazwyczaj posiada ograniczone zasoby lokalne, co oznacza, że większość pamięci, mocy obliczeniowej i innych zasobów pochodzi z serwera. To może być ograniczeniem w przypadku bardziej wymagających aplikacji.
f) Zależność od łączności sieciowej: Model klienta cienkiego opiera się na ciągłej łączności sieciowej między klientem a serwerem. Przerwy w połączeniu mogą prowadzić do niedostępności aplikacji.
Model klienta cienkiego jest nadal stosowany w niektórych zastosowaniach, takich jak edukacja, administracja publiczna, bankowość czy zdalna praca. Jednak wraz z rozwojem technologii i oczekiwań użytkowników, model ten traci na popularności na rzecz modelu klienta grubego, który oferuje większą funkcjonalność, niezależność i elastyczność.

2. Model klienta grubego: Tutaj serwer odpowiada głównie za zarządzanie danymi, natomiast oprogramowanie klienta implementuje logikę programu użytkowego oraz kontakt z serwerem.
Model ten jest bardziej elastyczny i umożliwia bardziej złożone operacje po stronie klienta.
Dodatkowe informacje:
a) Rozproszenie logiki: Część logiki aplikacji przenoszona jest na stronę klienta. To oznacza, że nie wszystkie operacje wymagają komunikacji z serwerem, co może poprawić wydajność i responsywność aplikacji (zdolność aplikacji do dostosowywania się i reagowania na różne warunki oraz urządzenia, na których jest wyświetlane).
b) Większa elastyczność: W zakresie implementacji i interakcji użytkownika z aplikacją. To pozwala na bardziej zaawansowane operacje, gdyż część obliczeń może być wykonywana lokalnie.
c) Lepsza obsługa offline: Część logiki i danych jest dostępna lokalnie, użytkownik może kontynuować pracę nawet w przypadku braku połączenia z serwerem.
d) Potencjalne problemy: Złożoność i różnorodność platform oraz urządzeń klienta mogą prowadzić do problemów z utrzymaniem i wdrażaniem aplikacji klienta grubego.
e) Większe wymagania sprzętowe: Ze względu na większe obciążenie przetwarzaniem po stronie klienta, aplikacje klienta grubego mogą wymagać bardziej zaawansowanego sprzętu.
f) Rozwijające się technologie: Rozwój technologii takich jak nowoczesne przeglądarki internetowe czy platformy do tworzenia aplikacji desktopowych (np. Electron) wpłynął na rozwinięcie modelu klienta grubego.

g) Różnorodność podejść: W dzisiejszym środowisku istnieje wiele różnych hybrydowych podejść łączących cechy modelu klienta grubego i cienkiego.

Podsumowując, opis modelu klienta grubego jest dokładny. To podejście, daje większą kontrolę i elastyczność użytkownikom oraz umożliwia bardziej zaawansowane operacje po stronie klienta. Jednak wiąże się z wyzwaniami, takimi jak utrzymanie i dostosowanie do różnych platform.



E. Główne funkcje sieciowych systemów operacyjnych

1. Współdzielenie zasobów: NOS umożliwia użytkownikom współdzielenie plików, folderów oraz innych zasobów, co umożliwia dostęp do informacji dla uprawnionych użytkowników.
2. Zarządzanie użytkownikami: NOS pozwala na tworzenie i zarządzanie kontami użytkowników oraz grupami, kontrolując dostępy do zasobów na poziomie użytkownika.
3. Serwery i usługi: Systemy NOS dostarczają różnorodne usługi sieciowe, takie jak serwery plików, serwery druku, serwery poczty, serwery baz danych i serwery WWW, które umożliwiają efektywne korzystanie z sieci. Podziały serwerów:

a. biorąc pod uwagę formę:

1) serwer hardware'owy (sprzętowy) - specjalistyczne urządzenie, programowalne w niewielkim stopniu, w zależności od zakresu potrzeb sieci, w której pracuje. Serwer hardware'owy posiada również zainstalowane odpowiednie oprogramowanie, aby można go było efektywniej dostosować do zmiennych potrzeb. Dzięki specjalistycznym komponentom i optymalizacjom są bardziej wydajne w obsłudze wielu równoczesnych żądań od klientów.

2) serwery software'owe (programowe) - odpowiednie oprogramowanie, które jakby emuluje sprzęt, zapewniając poprawną pracę komputera, na którym jest zainstalowane tak, aby mógł on udostępniać swoje zasoby dla komputerów w sieci i spełniać te same funkcje co serwer sprzętowy. Mogą być bardziej opłacalne niż serwery hardware'owe, nie wymagają zakupu specjalistycznego sprzętu.

b. ze względu na spełnianą funkcję w sieci np:

1) serwer wydruku - zarządza zadaniami drukowania w sieci to jest kolejkowaniem - odpowiedna kolejności do odpowiednich drukarek, formatowanie wydruków - np. zamiana z popularnych formatów do postscriptu, rozliczanie i raportowanie o liczbie wydrukowanych stron. Pozwala udostępnić drukarkę, bez konieczności posiadania ciągle włączonego komputera - wyjątkiem jest serwer software'owy, który musi być uruchomiony, aby mógł obsłużyć zadania drukowania.

2) serwer plików - komputer przeznaczony do udostępniania miejsca dyskowego, plików na nim zgromadzonych dla wszystkich lub wybranych użytkowników. Serwery plików, udostępniają również sieci lokalnej określone przez administratora usługi internetowe innym użytkownikom sieci lokalnej. Taka maszyna, za względu na konieczność obsługi wielu żądań jednocześnie, powinna być wyposażona w szybki procesor (najczęściej są to platformy wieloprocesorowe), bardzo dużą ilość pamięci RAM, i przede wszystkim sporo przestrzeni dyskowej. Realizowane przez protokół komunikacyjny i sieciowy system plików.

3) serwer dostępowy - ich podstawowym zadaniem jest udostępnianie połączenia internetowego (modemowego, DSL itp.) wszystkim lub wybranym komputerom w sieci.

4) serwer wykonań - inaczej nazywany zarządcą czasu procesora. Odpowiada za przydzielanie zasobów procesora konkretnym procesom, a także administruje wszelkimi uruchomionymi procesami.

5) firewalle - specjalne maszyny lub oprogramowanie, służące zabezpieczeniu sieci, i udaremnienie nieautoryzowanego dostępu z zewnątrz i penetracji sieci.

6) serwery faksów - jak sama nazwa mówi, zarządzają odbieraniem i wysyłaniem faksów.
Dają możliwość wybrania numeru telefonu i wysłanie faksu, jak ze zwykłego urządzenia.
Faksy możemy wysyłać nawet do użytkowników w tej samej sieci.

7) serwer ftp - serwer umożliwiający wymianę plików z komputerami za pomocą protokołu komunikacyjnego FTP, serwer podobny do serwera plików, służący do przechowywania danych plikowych, aby się dostać do danych gromadzonych na serwerze ftp, potrzebujemy zawsze nazwy użytkownika i hasła. Serwer FTP może być również elementem pakietu programów i wtedy stanowi jedną z oferowanych usług. Przykładem takiego rozwiązania jest IIS (Internet Information Services) firmy Microsoft. *Serwery plików działają jako lokalny udostępniony dysk twardy dla biur i są dostępne tylko w wewnętrznej sieci firmy. Serwery FTP przechowują pliki na zdalnym serwerze, przesyłane przez Internet.* Za pomocą serwera FTP udostępniasz pliki za pomocą połączenia internetowego.

8) serwer poczty - jego zadaniem jest obsługa poczty przychodzącej i wychodzącej, zarządzanie e-mail'ami.

9) serwer list dyskusyjnych - niezastąpione rozwiązanie dla grup pracujących nad większymi projektami. Ściśle wiąże się z serwerem pocztowym, gdyż ma za zadanie grupować pracowników

w konkretne grupy tematyczne lub projektowe, a także rozsyłanie do nich wiadomości dotyczących ich konkretnych grup.

10) serwer www - na tym komputerze przechowywane są witryny www. czyli te które oglądamy wpisując adres w przeglądarce. Często bywa tak, że na serwerze www jest uruchomiona usługa bazy danych (o ile nie ma dedykowanego serwera) i wtedy można stworzyć zaawansowane narzędzie wspomagające gromadzenie i przetwarzanie danych w firmie, dające możliwość ogólnego dostępu do wszystkich niezbędnych informacji dla wszystkich pracowników.

11) serwer baz danych - dedykowany komputer do gromadzenia informacji i ich przetwarzania. Oprogramowanie bazodanowe, pozwala porządkować i udostępniać dane uprawnionym użytkownikom w sieci. Systemy bazy danych w architekturze klient-serwer to m.in.: DB2, Informix Dynamic Server, Firebird, MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL.

12) serwer nazw - przechowuje bazę danych o użytkownikach, zasobach sieciowych i usługach. Zajmuje się kojarzeniem adresów fizycznych maszyn, usług i zasobów z ich nazwami.
Może istnieć wiele serwerów nazw, które współdziałają ze sobą w tłumaczeniu nazw.

13) serwer czasu - dostarcza informację o czasie, wzorce informacji pobrane np. z satelity.
Ma on kluczowe znaczenie podczas synchronizacji czasu maszyn w systemach rozproszonych.

14) serwer sprawdzania tożsamości - odpowiadający za bezpieczeństwo system.
Sprawdza prawdziwość deklarowanej tożsamości klienta wysyłającego żądanie do komputera w sieci. Po sukcesie autoryzacji wydaje "przepustkę" aby dalsze korzystanie z zasobów mogło się odbywać bez podawania hasła za każdym razem.

15) serwer katalogów - komputer dokonujący tłumaczenia naturalnych, zrozumiałych dla człowieka nazw plików, katalogów lub innych obiektów, na identyfikatory rozumiane przez system.

16) Serwer podstawowy/wyróżniony - pierwszy serwer w sieci, który odpowiada za tworzenie oraz zarządzanie kopiami zapasowymi.

Dodatkowe spostrzeżenia:

a. Dywersyfikacja funkcji: Każdy typ serwera pełni specyficzną rolę w sieci, co pozwala na dostarczanie różnorodnych usług i funkcji, które są niezbędne dla różnych aspektów pracy w sieci.

b. Wspieranie efektywności pracy: Poszczególne serwery są zaprojektowane tak, aby ułatwiały zarządzanie konkretnymi zadaniami i zasobami w sieci. Na przykład serwer plików umożliwia udostępnianie i przechowywanie plików, a serwer poczty obsługuje komunikację e-mail.

c. Zabezpieczenie i kontrola: Serwery takie jak firewall, serwer dostępowy czy serwer sprawdzania tożsamości pełnią kluczową rolę w utrzymaniu bezpieczeństwa sieci oraz kontroli dostępu do zasobów.

d. Wsparcie dla działalności: Dostarczają narzędzi, które są niezbędne do efektywnego prowadzenia różnych działań w sieci, od komunikacji po przetwarzanie danych.
e. Zastosowanie w różnych dziedzinach: Różne rodzaje serwerów znajdują zastosowanie w różnych dziedzinach, takich jak biznes, edukacja, komunikacja czy zarządzanie.
f. Złożoność infrastruktury: W większych sieciach wiele różnych serwerów może współistnieć, tworząc kompleksową infrastrukturę, która zapewnia potrzebne usługi i funkcjonalności.
g. Rozwój technologiczny: Wraz z postępem technologii, funkcje niektórych serwerów mogą ewoluować i dostosowywać się do nowych wymagań i trendów.

4. Bezpieczeństwo: NOS zapewnia mechanizmy zabezpieczeń, takie jak autoryzacja, uwierzytelnianie i kontrola dostępu, aby chronić zasoby przed nieuprawnionym dostępem.
5. Zarządzanie zdalne: Administratorzy mogą zdalnie zarządzać serwerami NOS, konfigurując je, monitorując działanie oraz instalując aktualizacje.
6. Usługi katalogowe: Usługi katalogowe umożliwiają przechowywanie informacji o użytkownikach, zasobach i usługach w hierarchicznej strukturze. To ułatwia zarządzanie i odnajdywanie zasobów w sieci. Przyjrzymy się głównym definicjom, funkcjom oraz różnym rodzajom usług katalogowych, które pełnią istotną rolę w zarządzaniu sieciami.

F. Usługi katalogowe

Usługi katalogowe to specjalizowany typ bazy danych, zawiera obiekty: użytkowników, aplikacje, urządzenia sieciowe i inne zasoby sieciowe. Usługa katalogowa musi być przynajmniej częściowo obiektową bazą danych reprezentującą użytkowników sieci i zasoby, co pomaga zarządzać relacjami między ludźmi a sieciami, urządzeniami sieciowymi, aplikacjami sieciowymi i zawartymi w sieci informacjami. Usługi katalogowe służą do:

a. przechowywania informacji o obiektach,
b. przeszukiwania wszystkich zasobów sieci zorganizowanej w strukturze drzewa,
c. zarządzania w środowiskach sieciowych jako mechanizmy sieciowe,
d. szybkiego czytania, przeglądania,
e. przeszukiwania według właściwości, np. wyszukać wszystkie obiekty typu drukarka, niezależnie od miejsca w sieci, gdzie są zlokalizowane.

Standardy usług katalogowych:

a. X.500 DAP- Directory Access Protocol, jest usługą katalogową o międzynarodowym standardzie wyposażoną w komplet funkcji. Jednak X.500 posiada ich aż tyle, że posługiwanie się i zarządzanie nimi staje się prawie niemożliwe, dodatkowo DAP funkcjonuje tylko w strukturach OSI.

b. LDAP- Lightweight Directory Access Protocol, został opracowany jako podzestaw do X.500 w odpowiedzi na złożoność X.500 (dla struktur TCP/IP). Pokrewieństwo między LDAPi X.500 jest bardzo silne. LDAP został pomyślany jako metoda dostępu do katalogów X.500. Nie wymaga wprawdzie, ażeby to był konkretnie katalog X.500, ale używa jego terminów i definicji opisujących katalog. Jest on implementowany w różnych produktach bądź jako system identyfikujący, bądź też system pocztowy albo aplikacja handlu elektronicznego.
Dla systemu Linux dostępne są nieodpłatnie dwa serwery LDAP: U-MichLDAP i OpenLDAP.

To drugie rozwiązanie staje się standardem dla Linuksa (i innych systemów UNIX).

Dokumenty: RFC-1777, RFC-1778, RFC 1823, RFC 2251-2256

Kilka dodatkowych informacji:

1) Znaczenie usług katalogowych: Usługi katalogowe stanowią fundament dla skutecznego zarządzania sieciami i zasobami. Dzięki nim możliwe jest przechowywanie, wyszukiwanie i zarządzanie różnymi obiektami w sieci, co pozwala na efektywną organizację i dostępność zasobów.
2) Struktura hierarchiczna: Jedną z głównych cech usług katalogowych jest ich hierarchiczna struktura, oparta na drzewie. To umożliwia logiczne grupowanie i organizację obiektów, co odzwierciedla strukturę sieci i jej zasobów.
3) LDAP jako odpowiedź na złożoność: LDAP jest lżejszym i bardziej praktycznym rozwiązaniem, zwłaszcza dla środowisk opartych na architekturze TCP/IP, które dominują w dzisiejszych sieciach.
4) Współczesne znaczenie LDAP: Protokół LDAP zyskał ogromną popularność i jest szeroko stosowany w dzisiejszych sieciach. Stanowi podstawę dla usług katalogowych w różnych dziedzinach, od autoryzacji i zarządzania użytkownikami po dostęp do zasobów.
5) Serwery LDAP dla systemu Linux: Linux i otwarte oprogramowanie odegrały kluczową rolę w rozwijaniu i popularyzacji technologii LDAP.
6) RFC (Request for Comments): Wzmianka o dokumentach RFC, które definiują protokoł LDAP i związane z nim aspekty, podkreśla standardyzację i dokumentację tej technologii.

G. Różne typy usług katalogowych

Domeny WindowsNT nie są właściwie kompletnymi usługami katalogowymi, ale zapewniają kilka ich podstawowych funkcji. Domena posiada płaską strukturę pozbawioną podziału na kontenery - wszystkie obiekty położone są na jednym poziomie. Domena pozwala na przechowywanie informacji o ograniczonej stałej ilości typów obiektów (konto użytkownika lub komputera, grupa) z ograniczoną stałą ilością atrybutów. Domeny są technologiczne ograniczone ilością przechowywanych obiektów (do

ok. 40 tys. obiektów w jednej domenie) oraz nie są oparte na żadnym otwartym protokole - nie ma możliwości dostępu z aplikacji innych producentów bez wykorzystania bibliotek firmy Microsoft. Istnieją inne różnice między domenami Windows NT a domenami Active Directory.

Usługi katalogowe są kluczowym elementem zarządzania obiektami w sieciach komputerowych. Przykłady różnych typów usług katalogowych:

1. Active Directory: To usługa katalogowa firmy Microsoft, wykorzystywana w systemach Windows Server. Umożliwia hierarchiczne zarządzanie użytkownikami, grupami, zasobami i politykami w sieci. Jest to implementacja protokołu LDAP, który umożliwia komunikację z innymi usługami katalogowymi. Jest Active Directory dla chmury Azure, która oferuje dodatkowe funkcje bezpieczeństwa i integracji.
2. Od Windows 2003 Server oraz Windows 2000, zgodna ze specyfikacją LDAP w wersji 3.0. Active Directory jako następca domen systemu Windows NT usuwa największe wady domen, tj. wprowadzono:
   a. hierarchiczność przechowywania informacji,
   b. dużo wyższe limity przechowywania informacji (powyżej 1 miliona obiektów w domenie Active Directory),
   c. rozszerzalność schematu zawierającego definicje obiektów.
3. NDS - Novell Directory Services jest usługą, katalogową opartą na X.500, służącą do zarządzania użytkownikami, prawami dostępu i innymi zasobami sieciowymi. Usługa NDS jest uruchamiana na serwerach NetWare 4.x i nowszych jest również dostępna dla innych systemów operacyjnych (takich jak Windows NT/2000), co pozwala na wykorzystanie NDS jako pojedynczej usługi katalogowej do zarządzania siecią opartą na systemach wielu producentów.
4. eDirectory: Jest to usługa katalogowa firmy Novell, następca usługi NDS (od wersji 6.0) dostępny za pomocą protokołu LDAP, działająca na platformach NetWare 5.x i 6.x, Linux i Windows. Zapewnia zaawansowane możliwości zarządzania i autoryzacji.
5. OpenLDAP: Jest to oprogramowanie open source implementujące protokół LDAP. Dostępne jest na różne platformy uniksopodobne, zapewniając elastyczne usługi katalogowe.
6. Tivoli Directory Server: Jest to komercyjna implementacja serwera LDAP przez IBM, przeznaczona głównie dla dużych instytucji oraz korporacji.
7. Apache Directory Project: Projekt dostarczający narzędzi i serwerów do zarządzania usługami katalogowymi zgodnymi z protokołem LDAP.
8. Apple Open Directory: To usługa katalogowa dla systemu macOS, umożliwiająca integrację z systemami Windows oraz zarządzanie użytkownikami i zasobami.

9. Fedora Directory Server: Rozwiązanie oparte na otwartym kodzie źródłowym, umożliwiające tworzenie zaawansowanych usług katalogowych na platformach Linuxowych.
10. Red Hat Directory Server: Komercyjna wersja serwera katalogowego, która stanowi rozwinięcie usługi Fedora Directory Server. Jest dostępna na różne platformy.

H. Zadania administratora sieciowych systemów operacyjnych

Administrator pełni kluczową rolę w zarządzaniu sieciowymi systemami operacyjnymi.
Odpowiada za szereg istotnych zadań, które wpływają na funkcjonowanie i bezpieczeństwo sieci:
1. Umożliwianie korzystania z sieci: Musi zapewnić, że użytkownicy sieci mogą efektywnie korzystać z zasobów sieciowych, takich jak pliki, drukarki czy usługi.
2. Administracja użytkownikami: Zarządzanie użytkownikami obejmuje tworzenie i usuwanie kont użytkowników, nadawanie uprawnień dostępu, monitorowanie ich aktywności oraz rozwiązywanie problemów związanych z logowaniem.
3. Zarządzanie systemem plików: Musi odpowiednio zarządzać strukturą systemu plików, zapewniając dostęp do plików i katalogów dla uprawnionych użytkowników.
4. Tworzenie kopii bezpieczeństwa i archiwizacja danych: Zapewnienie bezpieczeństwa danych to kluczowy aspekt pracy administratora. Regularne tworzenie kopii zapasowych oraz archiwizacja danych chronią przed utratą informacji w przypadku awarii.
5. Audyt zdarzeń w systemie: Jest odpowiedzialny za monitorowanie i analizę zdarzeń w systemie, co pozwala wykryć potencjalne zagrożenia i niestandardowe działania.

I. Obszary, na które administratorzy sieci muszą zwracać uwagę:

1. Bezpieczeństwo sieci: Zapewnienie bezpieczeństwa sieci to jedno z najważniejszych zadań administratora sieci. To obejmuje konfigurację zabezpieczeń, monitorowanie aktywności sieciowej w celu wykrywania prób naruszenia, wdrażanie firewalli, antywirusów i innych narzędzi zabezpieczających.
2. Monitoring i diagnozowanie: Administratorzy muszą stale monitorować sieć, aby identyfikować potencjalne problemy i awarie. Wykorzystują narzędzia do monitorowania ruchu sieciowego, wydajności sprzętu i usług. Diagnozowanie problemów i szybkie ich rozwiązywanie jest kluczowe dla minimalizowania przestojów w pracy.
3. Aktualizacje: Regularne aktualizacje systemów operacyjnych, oprogramowania i zabezpieczeń oraz firmware są niezbędne są niezbędne, aby zapobiegać lukom w bezpieczeństwie. Administratorzy muszą śledzić nowe wersje oprogramowania i wdrażać aktualizacje zgodnie z planem. To dotyczy zarówno systemów operacyjnych, jak i urządzeń sieciowych.

4. Zarządzanie dostępem do zasobów: Jest kluczowa dla ochrony poufności danych. Administratorzy muszą kontrolować, kto ma dostęp do jakich zasobów i w jaki sposób.
5. Zarządzanie zasobami: Skuteczne zarządzanie zasobami sieciowymi obejmuje kontrolę nad przepustowością, wydajnością sprzętu, zarządzanie adresacją IP i zarządzanie dostępem do zasobów sieciowych.
6. Backup i odtwarzanie: Regularne tworzenie kopii zapasowych danych oraz testowanie procesu odtwarzania jest kluczowe dla minimalizowania ryzyka utraty informacji.
7. Awaryjne plany i przywracanie: Administratorzy sieci powinni mieć przygotowane plany awaryjne w przypadku dużych awarii czy katastrof. Odtworzenie sieci i danych po incydencie jest kluczowe dla ciągłości działania organizacji.
8. Rozwiązanie problemów: Administratorzy sieci muszą być biegli w rozwiązywaniu problemów. To wymaga umiejętności analitycznych, logicznego myślenia oraz szybkiego podejmowania decyzji w sytuacjach awaryjnych. Kiedy awarie czy inne problemy się pojawią, administratorzy muszą działać szybko i skutecznie, aby przywrócić normalne działanie sieci. Umiejętność diagnozowania i rozwiązywania problemów jest kluczowa.
9. Optymalizacja wydajności: Ciągła optymalizacja wydajności sieci jest istotna, aby zapewnić płynne działanie aplikacji i usług. To obejmuje zarządzanie przepustowością, rozkładanie obciążenia i identyfikowanie wąskich gardeł.
10. Zarządzanie politykami: Administratorzy sieci muszą wdrażać i egzekwować polityki dotyczące bezpieczeństwa, dostępu do zasobów, korzystania z sieci oraz innych regulacji związanych z funkcjonowaniem sieci.
11. Wsparcie użytkowników: Administratorzy sieci często pełnią rolę pierwszej linii wsparcia technicznego dla użytkowników, którzy napotykają problemy z dostępem do sieci, połączeniem, drukarkami i innymi zasobami.
12. Planowanie pojemności: Administratorzy muszą monitorować obciążenie sieci i przewidzieć, czy infrastruktura sieciowa jest wystarczająco skalowalna, aby sprostać rosnącym wymaganiom. Planowanie pojemności obejmuje także optymalne wykorzystanie zasobów, aby uniknąć nadmiernego przeciążenia.
13. Zgodność z regulacjami: W zależności od branży, w jakiej działa organizacja, administratorzy muszą upewnić się, że sieć spełnia określone regulacje i standardy, takie jak GDPR, czy PCI DSS, które dotyczą ochrony danych i bezpieczeństwa.
GDPR (General Data Protection Regulation) to unijne rozporządzenie o ochronie danych osobowych, które obowiązuje od 2018 roku. Dotyczy ono wszystkich podmiotów, które przetwarzają dane osób fizycznych związanych z Unią Europejską.

Polska implementacja GDPR to RODO (Rozporządzenie o Ochronie Danych Osobowych). To skrót od angielskiej nazwy General Data Protection Regulation. RODO zawiera przepisy o ochronie danych osobowych osób fizycznych w Unii Europejskiej i o swobodnym przepływie tych danych.
PCI DSS (Payment Card Industry Data Security Standard) to międzynarodowy standard bezpieczeństwa danych płatniczych, który obowiązuje od 2004 roku. Dotyczy on wszystkich podmiotów, które akceptują, przetwarzają lub przechowują dane kart płatniczych.

14. Rozwój technologiczny: Świat sieci ciągle się rozwija, pojawiają się nowe technologie i rozwiązania. Administratorzy muszą być na bieżąco z trendami i ewolucją technologiczną, aby dostosowywać sieć do nowych wymagań i możliwości.
15. Edukacja i szkolenia: Administracja wymaga nieustannego kształcenia się. Nowe technologie i narzędzia pojawiają się regularnie, więc administratorzy muszą uczestniczyć w szkoleniach i kursach, aby utrzymać swoją wiedzę na aktualnym poziomie.

Podsumowanie

Podsumowując, w miarę jak technologia sieciowa się rozwija, rola administratorów sieci staje się coraz bardziej istotna. Ich umiejętności w zarządzaniu sieciowymi systemami operacyjnymi oraz zapewnianiu bezpieczeństwa stanowią fundament skutecznego i niezawodnego funkcjonowania dzisiejszych sieci komputerowych. Sieciowe systemy operacyjne, takie jak Windows Server, Linux czy inne, umożliwiają współdzielenie zasobów, zarządzanie użytkownikami i usługami, a także gwarantują bezpieczeństwo sieci. Współczesne sieci są dynamiczne i wymagające, dlatego administratorzy muszą nie tylko utrzymywać i zarządzać tymi systemami, ale również dostosowywać się do nowych wyzwań, takich jak chmury obliczeniowe czy IoT. Certyfikacje branżowe, takie jak MCSA czy CompTIA Network+, stanowią potwierdzenie umiejętności i mogą zwiększyć wartość zawodową administratora sieci.
W skrócie, praca administratora sieci to ciągłe wyzwanie, które wymaga rozwijania umiejętności i dostosowywania się do ewoluującej technologii, by zapewnić efektywne i bezpieczne działanie dzisiejszych sieci komputerowych.