Dodawanie drukarki sieciowej za pomocą adresu TCP/IP

1. Start na większości „Urządzenia i drukarki”,
2. Kliknąć w menu „dodaj drukarki”,
3. Wybieramy Dodać drukarkę sieciową,
4. W oknie dodawania drukarki wybrać „Drukarki której szukam nie ma na liście”,
5. Zaznaczyć opcję „Dodaj drukarkę używając adresu TCP\IP lub nazwy hosta”,
6. W polu nazwa hosta drukarki lub adres IP, wprowadzić adres IP drukarki (nazwa portu zostanie wprowadzona automatycznie),
7. Zaakceptować typ urządzenia „Standardowy Generic Network Card”,
8. Jeżeli instalowanej drukarki nie ma na liście należy kliknąć przycisk „z dysku…” w celu instalacji sterowników z dysku,
9. Za pomocą przycisku „przeglądaj…” wskazać lokalizację plików sterownika drukarki i kliknąć przycisk otwórz,
10. W oknie „Instalowanie z dysku” kliknąć OK,
11. Zaakceptować sterowniki drukarki,
12. Zaakceptować przyciskiem „Dalej”,
13. Wprowadzić nazwę drukarki,
14. Nie udostępniać drukarki,
15. W celu sprawdzenia poprawności instalacji drukarki sieciowej, kliknąć przycisk „drukuj stronę testową”.

UWAGA!!!

Zainstalowana drukarka powinna pojawić się w panelu „Urządzenia i drukarki”.

Do wyszukiwania informacji służą **wyszukiwarki internetiwe**. Wyszukiwarka internetowa to program lub strona internetowa, którego / której zadaniem jest ułatwienie użytkownikom wyszukiwania informacji w sieci. Przykładem wyszukiwarki może być **www.google.pl**.

Przeglądarki internetowe oferują możliwość pracy w trybie **bez połączenia z siecią** (*offline*). Aby przeglądanie stron było możliwe, stronę internetową należy wcześniej pobrać i zapisać na dysku. Rozwiązanie takie może być przydatne, gdy przepustowość łącza jest niewielka lub komputer, na którym będziemy przeglądać stronę, nie ma łączności z internetem. Do pobierania stron internetowych możemy wykorzystać specjalistyczny program, np. teleport (program komercyjny), lub odpowiednią funkcję przeglądarki. Alternatywą dla programu teleport może być linuksowy program wget lub HTTrack Website Copier – bezpłatny program, który umożliwia pobieranie i zapisywanie w całości wybranej strony internetowej w postaci statycznych plików HTML.

Na przykład w przeglądarce Mozilla Firefox należy:

1. Otworzyć stronę, którą zamierzamy zapisać.
2. Plik>Zapisz stronę jaki… lub ^S.
3. W oknie zapisywania strony wskazać folder, w którym ma być zapisana strona, wprowadzić nazwę pod jaką strona ma być zapisana oraz jako typ zapisu wybrać Strona sieci Web, kompletna.

Po zapisaniu strony tworzony jest plik w formacie **.html** oraz folder zawierający wszystkie pozostałe pliki, z których składa się strona. Aby otworzyć stronę w trybie offline, należy dwukrotnie kliknąć plik strony.

**Korzystanie z usługi transferu plików**

**FTP** (*File Transfer Protocol*) jest protokołem służącym do transmisji plików w sieci. Działa na bazie protokołu TCP/IP, zazwyczaj wykorzystując do transmisji danych port **20**, a do kontroli transmisji port **21**. Podstawową zaletą FTP jest to, że rozpoczęty, ale niezakończony pomyślnie, transfer danych może zostać wznowiony aż do uzupełniania brakujących części pliku (jednak nie wszystkie serwery oferują tę usługę). Głównymi wadami protokołu są brak możliwości szyfrowania transmisji oraz problemy z implementacją filtrów pakietów na routerach. Mimo tych wad FTP jest nadal jednym z najpopularniejszych w internecie protokołów przesyłania danych.

Protokół ten działa z wykorzystaniem architektury klient serwer. Użytkownik (klient) łączy się z serwerem FTP za pomocą specjalnego programu, nazywanego **klientem FTP**. W większości systemów operacyjnych jest wbudowany klient FTP pracujący w trybie tekstowym. Operacje wykonuje się, wpisując odpowiednie polecenia. Nie jest metoda wygodna, wymaga znajomości poleceń oraz protokołu, ale działa zawsze i we wszystkich systemach operacyjnych. Funkcję klienta FTP mogą pełnić także przeglądarki internetowe, choć pod względem możliwości nie mogą się one równać z dedykowanymi klientami FTP. Klient FTP jest wbudowany także do wielu menedżerów plików, np. Total Commandera.

Sesja FTP składa się z trzech części. Pierwsza z nich to zalogowanie się na odległy komputer: należy podać nazwę użytkownika i hasło. Na ich podstawie serwer FTP identyfikuje użytkownika i przydziela mu na czas sesji określone prawa dostępu do swoich zasobów. Posiadanie konta i związanych z nim odpowiednich uprawnień na komputerze docelowym jest warunkiem koniecznym do rozpoczęcia transmisji jakichkolwiek danych. Konto takie jest przydzielane przez administratora systemu. Podczas drugiej części wykonywane są operacje na odległych plikach i folderach – kopiowanie, przenoszenie, zmiana nazwy itp. Etap ostatni to zamknięcie sesji. Niektóre serwery wysyłają na zakończenie, przenoszenie zmiana nazwy itp. Etap ostatni to zamknięcie sesji. Niektóre serwery wysyłają na zakończenie krótką statystykę, w której zawarte są m.in. informacje o czasie trwania sesji oraz ilości przesyłanych danych.

Większość serwerów FTP oferuje również dostęp **publiczny** (anonimowy) – identyfikatorem użytkownika jest zazwyczaj „anonymous”, a hasłem – własny adres poczty elektronicznej. Podczas korzystania z konta anonimowego dysponujemy na ogół bardzo ograniczonymi uprawnieniami, umożliwiającymi jedynie pobieranie zbiorów z serwera. Jak każdy komputer dostępny w internecie, serwer FTP posiada własny, indywidualny adres pozwalający jednoznacznie go zidentyfikować. Aby połączyć się z serwerem FTP, możemy się posłużyć jego adresem IP, np.. 10.1.114.31. Z tego typu adresów korzystamy najczęściej, gdy nasz serwer znajduje się w sieci lokalnej, której nie obsługuje serwer DNS. Jeżeli w sieci działa serwer DNS lub korzystamy z internetu, to zamiast adresu IP możemy posługiwać się nazwami domenowymi, np. [ftp.task.gda.pl](ftp://ftp.task.gda.pl). Pełny adres internetowy (URL) zawiera prefiks ftp://, np.:

<ftp://ftp.task.gda.pl>

Jeżeli dostęp do serwera wymaga podania nazwy użytkownika oraz hasła, należy dołączyć te dane do adresu w następujący sposób:

<ftp://uzytkownik:haslo@ftp.tak.gda.pl>

Często stosowaną praktyką jest wydzielanie części publicznej serwera i udostępnianie jej zawartości każdemu zainteresowanemu internaucie. Serwery te są nazywane **anonimowymi**, ponieważ korzystający z nich użytkownik podczas porcedury logowania podaje nazwę konta „anonymous a jako hasło – własny adres e-mail. W standardowej konfiguracji uprawnienia anonimowego użytkownika pozwalają jedynie na pobieranie plików (i to tylko z wydzielonych, publicznych folderów), nie dając możliwości ich wysyłania na serwer. Najczęściej do dyspozycji anonimowych użytkowników jest przeznaczony folder **pub**, w którym są gromadzone zbiory dostępne dla każdego użytkownika (prawa tylko do pobierania danych z serwera). Administrator serwera FTP może udostępnić oddzielne foldery przeznaczone na pliki do przesyłania na serwer przez użytkowników anonimowych. Jest to najczęściej pojedynczy folder o nazwie **upload** lub  **incoming**, gdzie można umieścić ciekawy program lub dokument. Po sprawdzeniu jego zawartości administrator może skopiować go do folderu pub, tak aby był dostępny dla innych użytkowników.

Po zalogowaniu się na konto anonimowe jesteśmy przenoszeni do folderu głównego usługi FTP. Folder ten w Linuksie jest zlokalizowany w /**var**/**ftp**. W folderze na ogół dysponujemy uprawnieniami umożliwiającymi tylko pobieranie plików.

Po zalogowaniu się na konto lokalne na serwerze jesteśmy przenoszeni do folderu domowego użytkownika. Standardowo w Linuksie jest to /**home**/**użytkownik**. W folderze tym dysponujemy pełnymi uprawnieniami (możemy pliki pobierać z serwera, przenosić na serwer, kasować oraz zarządzać folderami).

Przesyłanie plików przez FTP może odbywać się w dwóch trybach:

* **ASCII** (*American Standard Code for Information Interchange*) – jest przeznaczony tylko do plików zapisanych w standardzie ASCII (pliki takie zawierają tylko tekst, np. pliki wsadowe, dokumenty HTML, dokumenty tekstowe z rozszerzeniem \*.txt),
* **Binarnym** – jest przeznaczony do przesyłania wszystkich pozostałych typów plików.

Dokumenty popularnych programów biurowych, np. MS Word, nie są plikami ASCII – oprócz tekstu zawierają wiele dodatkowych informacji i nie mogą być przesyłane w trybie ASCII. Plik binarny (program, grafika, archiwum ZIP) przesyłany w trybie ASCII zostałby uszkodzony. Klient FTP i przeglądarka internetowa na ogół automatycznie rozpoznają typ przesyłanego pliku i uruchamiają odpowiedni tryb przesyłania. Jednym z bezpłatnych klientów FTP jest FileZilla.

Jak większość klientów FTP, ma klasyczny interfejs składający się z dwóch paneli. Po lewej stronie jest umieszczony folder komputera lokalnego. Po prawej stronie jest wyświetlona zawartość folderu na serwerze. Dodatkowo w górnej części okna znajduje się lista poleceń i komunikatów przesyłanych między komputerami. W dolnej części okna jest umieszczona kolejka zadań do wykonania. Połączenie z serwerem nawiązujemy przez wpisanie w odpowiednie okna nazwy lub adresu IP serwera, nazw użytkownika, hasła oraz numeru portu (domyślnie **21**).

Wszelkie operacje na plikach wykonuje się metodą przeciągnij i upuść. Jeżeli połączenie zostanie zerwane, możemy je przywrócić, wybierając przycisk „Szybkie łączenie”. W oknie dialogowym pojawi się lista połączeń, spośród których wybieramy to, które chcemy przywrócić.

Jeżeli połączenie zostanie przerwane w czasie transmisji danych, możemy kontynuować transfer danych do miejsca, w którym transmisja została przerwana (niestety, nie wszystkie serwery oferują tę usługę). W otwartym oknie dialogowym możemy wybrać nadpisanie istniejącego pliku (rozpoczęcie transmisji od początku) lub wznowienie transmisji.

Przeglądarka internetowa standardowo jest tak skonfigurowana, aby obsługiwać przeglądanie stron internetowych za pomocą protokołu http. Większość współczesnych przeglądarek ma wbydowanego klienta FTP. Aby jednak połączyć się z serwerem FTP, należy w sposób jawny poinformować serwer o zamiarze korzystania z protokołu ftp. W tym celu w polu Adres przeglądarki wpisujemy pełny adres URL (np. <ftp://ftp.task.gda.pl>).

Klient w przeglądarce internetowej jest skonfigurowany w taki sposób, aby automatycznie logowany był użytkownik anonimowy. Serwery mogą mieć – ale nie muszą – skonfigurowane konta anonimowe, które nie wymagają podania hasła. Dzięki temu bezpośrednio po wpisaniu adresu przenoszeni jesteśmy do folderu **pub** ( bez konieczności wpisywania hasła). Operacje na plikach możemy wykonywać za pomocą myszy, tak jak w oknie Eksploratora Windows. Mała strzałka po lewej stronie ikony folderu oznacza, że tak naprawdę nie jest to folder, a tylko skrót do niego. Po kliknięciu system automatycznie przeniesie nas w miejsce wskazane za pomocą skrótu. Podczas korzystania z konta anonimowego nasze uprawnienia na ogół są ograniczone tylko do pobierania danych z folderu **pub**. Próba przejścia do folderu nadrzędnego powoduje zakończenie sesji FTP i rozłączenie z serwerem. Jeżeli na serwerze FTP mamy konto lokalne, to podczas logowania w polu Adres przeglądarki wpisujemy nazwę konta i adres serwera oddzielone znakiem @ (np. <ftp://student1@192.168.0.200>).

W czasie kopiowania pliku na bieżąco jest wyświetlana statystyka połączenia pozwalająca na zorientowanie się w szacunkowym terminie zakończenia operacji.

Zadanie

Z serwera [ftp.task.gda.pl](ftp://ftp.task.gda.pl) pobierz na własny komputer plik Sieciowy\_Savoir-vivre.txt (z katalogu /pub/doc).

**Standard adresacji URL**

**URL** (*Uniform Resource Locator*) – oznacza ujednolicony format adresowania zasobów (informacji, danych, usługi) stosowany w Internecie i w sieciach lokalnych.

URL najczęściej kojarzony jest z adresami stron WWW, ale ten format adresowania służy do identyfikowania wszelkich zasobów dostępnych w Internecie. Standard URL, opisany jest w dokumencie **RFC 1738.**

Adres URl składa się z części określającej rodzaj zasobu **lub usługi** (*scheme*), dwukropka i części zależnej od rodzaju zasobu (*scheme-specific part*), np.:

<http://www.wikipedia.com/wiki/URL>

| | |

| | ścieżka dostępu do zasobu

| host (adres serwera)

Protokół (scheme)

Nazwa rodzaju zasobu może składać się z małych liter, cyfr, plusa, myślnika oraz kropki,

Część zależna od rodzaju zasobu przyjmuje postać:

//adres\_serwera:port/sciezka\_dostępu

Jeśli numer portu jest domyślny dla danej usługi, to może być pominięty.

**Korzystanie z poczty elektronicznej i grupy dyskusyjnych**

**Usługa poczty elektronicznej** (*e-mail*) umożliwia wymianę wiadomości tekstowych oraz załączników w postaci plików innych formatów, zawierających np. zdjęcia, muzykę. Korzystanie z poczty elektronicznej jest możliwe nie tylko za pomocą komputera, lecz także innych urządzeń, np. telefonu komórkowego. Program umożliwiający korzystanie z poczty elektronicznej składa się z dwóch części – **klienta i serwera**. Aby korzystać z poczty, musimy zainstalować odpowiedniego klienta oraz mieć konto (skrzynkę pocztową) na serwerze poczty elektronicznej. Adres składa się z nazwy skrznki (musi być unikatowa na danym serwerze), znaku rozdzielającego @ oraz unikatowego adresu serwera usługodawcy, na serwerze, na którym założyliśmy konto:

nazwa\_uzytkownika@adres\_serwera

Obecnie większość dostawców usług poczty elektronicznej oferuje dostęp do skrzynki e-mail przez WWW.

Do wysyłania e-mail służy protokół **SMTP** (*Simple Mail Transfer Protocol*). Wiadomość jest wysyłana na skrzynkę pocztową adresata i tam czeka na jej odebranie lub skasowanie. Do odbioru poczty stosuje się protokoły **POP3** (*Post Office Protocol version 3*) i **IMAP** (*Internet Message Access Protocol*). POP3 jest znacznie prostszy i powszechnie wykorzystywany. Program do obsługi poczty zainstalowany na komputerze może po uzyskaniu połączenia pobrać wszystkie wiadomości do naszego lokalnego komputera i usunąć je z serwera (ustawienie to można zmienić w konfiguracji programu pocztowego). Wiadomości możemy w dowolnej chwili odczytywać bez konieczności ponownego połączenia się z serwerem. IMAP po nawiązaniu połączenia z serwerem poczty pobiera do naszego komputera wyłącznie nagłówki wiadomości. Dopiero po kliknięciu nagłówka jest pobierana cała wiadomość. Wiadomości przesyłane za pomocą poczty elektronicznej powinny być szyfrowane w celu zapewnienia poufności, np. za pomocą programu PGP.

(rysunek)

Dostarczanie poczty elektronicznej

* **Mail User Agent** (MUA) – program klienta przeznaczony do wysyłania i odbierania wiadomości pocztowych (np. Outlook, Thunderbird itp.)
* **Mail Transfer Agent** (MTA) – oprogramowanie uruchomione na serwerze, które na podstawie adresu wiadomości oraz własnej listy odbiorców podejmuje decyzję, czy wiadomość powinna być przekazana do skrzynki odbiory (jeżeli adresat ma skrzynkę na tym serwerze), czy do innego serwera.
* **Mail Delivery Agent** (MDA) – oprogramowanie uruchomione na serwerze dostarcza wiadomość do skrzynki pocztowej adresata.

Za pomocą poczty elektronicznej możemy:

* Wysyłać teksty do dowolnego użytkownika internetu na całym świecie;
* Dołączyć do listu załączniki, które nie są tekstem, np. programy komputerowe, obrazy dźwięk;
* Wysyłać wiadomości do wielu adresatów jednocześnie za pomocą list mailowych;
* Odpowiadać na listy lub przekazywać je dalej.

Posiadanie konta poczty elektronicznej umożliwia użytkownikowi korzystanie z innych usług dostępnych w internecie, np. anonimowego dostępu do serwerów FTP lub grup dyskusyjnych.

Wraz z systemem Windows XP dostarczany jest program Outlook Express, będący klientem poczty elektronicznej (w systemie Vista zmieniono nazwę programu na Poczta, jednak obsługa pozostała bez zmian). Aby skorzystać z konta poczty elektronicznej za pomocą programu klienta pocztowego, należy go skonfigurować za pomocą danych uzyskanych podczas tworzenia konta przez użytkownika.

W systemie Windows 7 zrezygnowano z domyślnego programu pocztowego. Dedykowanym klientem pocztowym dla tego systemu jest Windows Live Mail (poczta usługi Windows Live). Program jest częścią pakietu **Podstawowe programy Windows**, można go pobrać ze strony

<http://windows.microsoft.com/pl-PL/windows-live/essentials-other-programs>

Zadanie

W tym ćwiczeniu wykonana zostanie instalacja i konfiguracja programu pocztowego dla Windows 7. Aby skonfigurować program Windows Live Mail, należy:

1. Pobrać ze strony wskazanego we wcześniej podanym adresie plik instalacyjny programu i zainstalować go w systemie. Można zainstalować cały pakiet programów lub tylko klienta poczty.
2. Podczas pierwszego uruchomienia programu włączony zostanie kreator pomagający w konfiguracji konta pocztowego. W pierwszym oknie kreatora należy wprowadzić adres e-mail, dla którego konfigurowane jest konto, hasło ora komunikat tekstowy, jaki ma się pojawiać w wiadomościach wysłanych z tego konta.
3. W przypadku skrzynek zlokalizowanych na popularnych serwerach, np. Hotmail, Gmail i wielu innych, konfiguracja serwerów poczty zostanie wykonana automatycznie. Ustawienia serwerów można wprowadzić ręcznie w przypadku, gdy automatyczna procedura zawiedzie.

Działanie **grup dyskusyjnych** (*Usenet*) jest podobne do usługi e-mail. Usenet składa się z kilkudziesięciu tysięcy **grup tematycznych**, ułożonych w strukturę hierarchiczną. Użytkownicy wysyłają wiadomości do **serwerów Usenet**. Serwery automatycznie wymieniają je między sobą i udostępniają wszystkim użytkownikom konkretnej grupy. Każdy z członków grupy ma możliwość dopisywania swoich wiadomości, tworząc w ten sposób pewien rodzaj dyskusji na wybrany temat. Wiadomości mogą być publiczne dostępne dla wszystkich członków grupy, lub prywatne – skierowane tylko do konkretnego użytkownika grupy.

Aby móc używać Usenetu, należy zainstalować oprogramowanie klienta grup dyskusyjnych. Może to być oddzielna aplikacja lub odpowiednią funkcją wbudowana do klienta poczty elektronicznej. Hierarchiczna budowa nazw grup dyskusyjnych ułatwia wyszukanie interesującego nas tematu dyskusji.

Podstawowe grupy, dostępne na większości serwerów, są zebrane w ośmiu kategoriach:

- comp – wszystko o komputerach

- sci – zagadnienia naukowe

- soc – zagadnienia socjologiczne

- rec – rekreacja, sztuka, hobby, wypoczynek

- news – nowości (głównie z dziedziny oprogramowania i sieci)

- misc – różne

- talk – wielotematyczne, niekończące się dyskusje

- alt – tematy nietypowe, które nie uzyskały większego grona sieciowej społeczności

Obowiązującym językiem w Usenecie jest angielski. Istnieją jednak grupy lokalne, w których rozmawia się ojczystym językiem np. nazwy grup z j.polskim zwykle mają przedrostek .pl. Kolejne składniki nazwy precyzują temat dyskusji np. pl.comp.sys.novell lub pl.comp.sieci.bezprzewodowe. korzystając z Usenetu, należy przestrzegać netykiety, czyli sieciowej – zbioru zasad dobrego wychowania. Polska wersja etykiety sieciowej dostępna jest w internecie pod adresem [ftp://ftp.task.gda.pl/pub/doc/sieciowy - savoir-vivre.txt](ftp://ftp.task.gda.pl/pub/doc/sieciowy%20-%20savoir-vivre.txt). Więcej informacji o netykiecie można uzyskać pod adresem <ftp://ftp.task.gda.pl/pub/doc/sieciowy>.

Zad 1. Utworzyć konto pocztowe o nazwie [ti2zs1stdnr@onet.pl](mailto:ti2zs1stdnr@onet.pl) i haśle Zs1tiL

Zapisać w swoim zeszycie do przedmiotu adresy serwerów SMTP i POP3 lub IMAP utworzonej skrzynki pocztowej.

2. Wysłać do kolegi wiadomość z załącznikiem /dowolny plik graficzny

3. Wyszukane ma serwerze nazwy informacji o dowolnej grupie dyskusyjnej, której tematem jest system operacyjny Linux. Przyłącz się do grupy `i odczytaj kilka wiadomości.

4. Najbardziej typowe zachowania, które nie są lubiane w grupach dyskusyjnych mają swoje nazwy są to m.in. spamowanie trollowanie, flamowanie, towarzystwa wzajemnej adoracji. Wyszukaj w internecie lub wyjaśnij na podstawie własnych doświadczeń, jakich doświadczeń/zachowań/ dotyczą te określenia

Korzystanie z usługi telnet

Telnet jest protokołem umożliwiającym wykonywanie operacji na odległym komputerze. Daje on użytkownikowi możliwość interakcyjnej pracy w środowisku tekstowym na odległych komputerach uruchamiania programów dostępu do baz danych itp. Pozwala korzystać z usług oferowanych przez komputer niezależnie od tego, czy znajduje się on w sąsiednim pokoju, czy na innym komputerze.

Lokalny komputer emuluje terminal odległego komputera co stwarza wrażenie pracy w systemie z którym nawiązano połączenie. Klient telnetu musi emulować terminal właściwy dla zdalnego systemu, korzystanie z niewłaściwego typu terminalu mogłoby bowiem spowodować błędne interpretowanie poszczególnych klawiszy lub znaków.

Aby połączenie było możliwe na zdalnym systemie musi być uruchomiony serwer usługi telnet. Standardowo telnet korzysta z portu 23. Klient telnetu jest wbudowany w większość systemów operacyjnych np. Linux, Windows XP. Nie jest natychmiast wbudowany w Windows 7. W systemie Windows 7 należy pobrać i zainstalować dodatkowy program np. PUTTY

Aby uruchomić sesję telnetu, np. w Kubuntu uruchamiamy konsole (terminal). W oknie dialogowym wpisujemy polecenie telnet i wprowadzamy adres IP lub nazwę komputera z którym nawiązujemy połączenie (np. telnet 192.168.1.103). Po nawiązaniu połączenia należy zalogować się na konto w serwerze odległym. Podajemy nazwę konta (login) oraz hasło (password). Zalogowanie na serwerze pozwala na rozpoczęcie pracy w terminalu. W celu zapewnienia bezpieczeństwa w niektórych systemach logowanie na konto administratora może być zablokowane.

Telnet umożliwia logowanie się na zdalnych komputerach i wykorzystanie poleceń systemowych. Usługa jest bardzo niebezpieczna, gdyż wszystkie dane, takie jak nazwa użytkownika i hasła są przesyłane przez sieć w nieszyfrowanej postaci. Z tego powodu dostęp przez telnet jest blokowany lub wyłączany przez wielu administratorów. Tam, gdzie jest to możliwe powinno się unikać, stosując w zamian usługę SSH o podobnych możliwościach, ale bezpieczną ze względu na szyfrowanie danych.

**Korzystanie z usługi bezpiecznego terminalu**

Usługa SSH (Secure Shell) jest następcą protokołu telnet i również służy do terminalowego łączenia się ze zdalnymi komputerami. W odróżnieniu od telnet transfer danych jest szyfrowany. Najczęściej stosowane jest szyfrowanie algorytmem AES. Każdy komputer podczas instalacji generuje dwa klucze. Jeden z nich (publiczny) jest dostępny dla wszystkich, drugi (prywatny) musi być starannie ukryty. Klucze te są wykorzystywane do szyfrowania transmisji. Identyfikacja użytkownika może polegać na weryfikacji konta i hasła lub za pomocą klucza wygenerowanego dzięki poleceniu ssh – keygen. SSH pracuje w architekturze klient – serwer. Klient będzie mógł nawiązać połączenie z serwerem tylko wtedy, gdy administrator uruchomi na serwerze usługę dostępu przez SSH. Oprogramowanie serwera standardowo nasłuchuje przychodzących połączeń od klientów w porcie 22 protokołu TCP. Klientom SSH może być program PUTTY, który umożliwia bezpieczny dostęp do powłoki (shell) systemu operacyjnego. Po uruchomieniu programu w oknie dialogowym wprowadzamy dane serwera, z którym zamierzamy nawiązać połączenie.

W polu Host Name (or IP address) wpisujemy nazwę komputera lub jego adres IP /np. 192.168.0.200 i zaznaczymy wybór protokołu SSH (oraz sprawdzamy numer portu – powinien wskazać 22) Po wpisaniu danych możemy wybrać przycisk Open.

Jeżeli wcześniej między komputerami nie została nawiązane połączenie za pomocą PUTTY to zostanie wygenerowana para kluczy służących do szyfrowania połączenia. W oknie informującym o tworzeniu kluczy należy wybrać przycisk Tak.

W oknie możemy się zalogować, podając identyfikator konta użytkownika (np. u2til-l) i naciskając klawisze Enter. Wpisujemy hasło użytkownika i ponownie naciskamy Enter. W czasie pisania hasła komputer nie wyświetla żadnych znaków – nawet gwiazdek (nie można policzyć wprowadzanych znaków).

Po zalogowaniu można uzyskać dostęp do wszystkich usług dostępnych za pomocą terminalu dla użytkownika, z którego konta korzystamy.

Usługa SSH umożliwia funkcjonowanie innych usług pozwalających np. na bezpieczne przesyłanie danych. W systemach Unix/Linux do bezpiecznego kopiowania plików jest wykorzystywane polecenie scp. Dla systemu Windows została utworzona aplikacja WinSCP.

**Korzystanie z usługi bezpiecznego terminalu w systemie Windows**

**WinSCP** jest programem umożliwiającym nawiązanie bezpiecznego połączenia z serwerem oraz zarządzanie plikami i folderami. Program WinSCP jest przeznaczony dla systemu Windows i nie wymaga instalacji w systemie. Program można bezpłatnie pobrać z internetu. Po skopiowaniu pliku należy go uruchomić. Po uruchomieniu programu wybieramy przycisk Nowa, aby utworzyć nowe połączenie.

Po nawiązaniu połączenia w lewym panelu zostanie pokazana zawartość dysku logicznego, a w prawym – zawartość folderu domowego użytkownika. Operacji na plikach i folderach dokonujemy mysz, metodą „przeciągnij i upuść” **DND** (*Drag and Drop*), lub za pomocą klawiszy funkcyjnych (ich znaczenie jest opisane w dolnej części ekranu). W celu zmiany dysku lokalnego należy wybrać pole wyboru dysku i wskazać nowy dysk, którego zawartość ma być wyświetlana w lewym panelu.

**Sieciowy system operacyjny Novell NetWare**

System Novell NetWare to sieciowy system operacyjny instalowany na dedykowanym serwerze, którego podstawowym zadaniem jest udostępnianie zasobów klientom. Klientami systemu NetWare mogą być stacje robocze, na których jest instalowane dodatkowe oprogramowanie klienta, umożliwiające współpracę z serwerem. Stacje robocze mogą być wyposażone w różne systemy operacyjne, np. DOS, Windows, Linux, MacOS.

Architektura systemu NetWare składa się z trzech warstw:

* Jądra systemu zarządzającego jego wszystkimi istotnymi mechanizmami (m. in. biezpieczeństwem),
* Sterowników odpowiedzialnych za komunikację z urządzeniami peryferyjnymi,
* Aplikacji i usług odpowiedzialnych za funkcjonowanie wielu usług systemu NetWare.

**Jądro NetWare** udostępnia podstawowe funkcje używane przez aplikacje uruchamiane na serwerze. Dodatkowe usługi zapewniają **moduły wczytywane** (ładowalne) **NLM** (*NetWare Loadable Module*). Moduły NLM obsługują między innymi dyski, karty sieciowe, moduły przestrzeni nazw, programy narzędziowe. Moduły te mogą być wczytywane i usuwane z pamięci serwera podczas jego pracy.

W systemie NetWare występują cztery rodzaje wczytywanych modułów:

* **Programy obsługi dysków** – sterują komunikacją między systemem operacyjnym serwera a urządzeniami pamięci masowej,
* **Programy obsługi kart sieciowych** – sterują komunikacją między systemem operacyjnym serwera a kartami sieciowymi,
* **Moduły przestrzeni nazw** – pozwalają na przechowywanie na wolumenach NetWare nazw plików niezgodnych z formatem DOS-u,
* **Programy narzędziowe NLM** – pozwalają na uruchamianie usług niewbudowanych w jądro systemu operacyjnego, np. usługi drukowania.

**Usługi katalogowa firmy Novell**

Usługę katalogową **Novell Directory Services NDS** stworzyła w roku 1993 firma Novell wraz z wersją serwera NetWare oznaczoną numerem 4. Był to pierwszy tak zaawansowany produkt z rodziny usług katalogowych. Celem NDS było zebranie w jednej bazie informacji o kontach użytkowników i grupach, a także informacji o innych elementach systemu, takich jak serwery, podsieci, zasady zarządzające stacjami, informacje o bramach itp. Baza ta została rozproszona między wiele serwerów sieciowych. Od wersji 6.0 serwer NetWare NDS został przemianowany na **eDirectory** i przestał być na stałe związany z serwerami NetWare.

**Katalog i obiekty NDS**

Usługi katalogowe NDS udostępniają bazę danych o wszystkich zasobach sieciowych. Baza ta jest nazywana **Katalogiem**. Wszystkie serwery NetWare znajdujące się w tej samej sieci mają informacje o wszystkich zasobach sieciowych, ponieważ używają tego samego Katalogu. Każdy zasób sieciowy ma swój własny wpis w Katalogu identyfikowany przez unikatową nazwę. Użytkownik, aby uzyskać dostęp do zasobu, musi podać jego nazwę.

Katalog składa się z obiektów cech i wartości:

* **Obiekt** – zawiera informacje o konkretnym zasobie, np. drukarce;
* **Cecha** (**właściwość**) – jednostkowa informacja charakteryzująca dany obiekt, np. cechą drukarki może to być jej nazwa;
* **Wartość** – informacja przypisana do cechy, np. nazwę drukarki może być HP-560C.

Obiekty NDS można podzielić na trzy klasy:

* **[Root]** – korzeń struktury – może zostać utworzony tylko podczas instalowania pierwszego serwera w sieci (Katalog może mieć tylko jeden korzeń) i reprezentuje najwyższy poziom w drzewie;
* **Kontener** (*container* – pojemnik) – służy do organizowania i porządkowania struktury Katalogu. Może zawierać obiekty typu liść (użytkownicy czy drukarki) lub inne kontenery. Może reprezentować kraje, lokalizacje w kraju, firmy, działy, grupy robocze czy wspólne zasoby. Obiektami typu kontener są:
* **Kraj C** (*Country*) – jest tworzony poniżej korzenia i pozwala wprowadzić w strukturze sieci korporacji podział międzynarodowy,
* Organizacja **O** (*Organization*) – służy do dzielenia opisu sieci na struktury, np. przedsiębiorstwo, szkoła lub dział . Drzewo Katalogu musi zawierać minimum jeden obiekt typu organizacja. Organizacja może zawierać kolejne obiekty typu jednostka organizacyjna lub obiekty podrzędne typu liść,
* Jednostka organizacyjna **OU** (*Organizational Unit*) opisuje istniejące grupy organizacyjne, np. działy w przedsiębiorstwie;
* **Liść** CN (*leaf*) – reprezentuje fizycznie i logiczne i zasoby sieciowe i nie może zawierać innych obiektów.

Drzewo NDS powinno odpowiadać strukturze organizacyjnej firmy. Przykładowa struktura drzewa NDS:

{rysunek}

Usługi NDS nie przeszukują całego Katalogu, dlatego aby znaleźć obiekt, potrzebują precyzyjnych informacji określających położenie obiektu w drzewie. Pozycję obiektu w drzewie NDS określa **kontekst** (*context*). Jest to lista obiektów klasy kontener prowadząca od danego obiektu do korzenia (jak ścieżka dostępu służąca do wskazania pliku do katalogu). W drzewie NDS nie mogą występować w tym samym kontenerze dwa obiekty o jednakowej nazwie. Dwa takie obiekty mogą być natomiast w różnych kontenerach.

Nazwa obiektu precyzyjnie identyfikuje obiekt i jego położenie w drzewie NDS. Podając nazwę obiektu, można użyć:

* **Nazwy pełnej DN** (*Distinguished Name*), która jest połączeniem nazwy zwykłej o kontekstu. Nazwa pełna zaczyna się od kropki, a obiekty występujące w nazwie są oddzielone kropkami, na przykład **.CN=uczen.OU=TLO=ZSP;**
* **Nazwy względnej RDN** (*Relative Distinguished Name*), która jest listą obiektów tworzących ścieżkę prowadzącą od nazywanego obiektu do kontekstu bieżącego. NDS musi z niej utworzyć nazwę pełną przez połączenie nazwy względnej z kontekstem bieżącym:

**Nazwa względna + kontekst bieżący = nazwa pełna.**

Przykład nazwy pełnej i względnej:

{rysunek}

Nazwa względna **CN=uczen** w kontekście **OU=TLO=ZSP** zostanie zamieniona na ścieżkę pełną **.CN=uczen.OU=TLO=ZSP**, a w kontekście **O=ZSP** na **.CN=uczen.O=ZSP**.

**Zarządzanie kontami użytkownika**

Odzwierciedleniem użytkowników w każdym systemie operacyjnym są konta. W celu zapewnienia właściwej pracy każdego z użytkowników administrator musi zadbać o łatwy orz bezpieczny sposób dostępu do zasobów systemu. Administrator powinien monitorować pracę użytkowników w systemie, aby wychwycić nieprawidłowości w jego działaniu oraz wykluczyć nieautoryzowane próby skorzystania z niego.

Konto użytkownika (account) – to zbiór zasad i uprawnień w ramach danego systemu przypisanych konkretnemu użytkownikowi. Przed rozpoczęciem tworzenia kont użytkowników administrator powinien dokonać analizy i w odpowiedni sposób zaplanować system kont, a w szczególności.

* Określić spójną konwencję nazw użytkowników – ma umożliwić administratorowi łatwiejszą administrację kontami, np. tworzenie nazw składających się z pierwszej litery imienia i całego nazwiska (bez polskich znaków). Przykładowo użytkownik Jan Kowalski będzie miał zgodnie z tą konwencją nazwę JKowalski,
* Określić wymagania dotyczące haseł użytkowników np. minimalną długość hasła, złożoność haseł,
* Określić czy użytkownik ma prawo do zmiany hasła,
* Określić grupy użytkowników mających te same lub podobne uprawnienia
* Określić restrykcje dotyczące godzin i miejsca logowania,
* Określić jednostki organizacyjne, do których mają należeć użytkownicy i grupy użytkowników.

Proces tworzenia struktury kont obejmuje:

* utworzenie jednostek organizacyjnych odpowiadających strukturze organizacyjnej firmy,
* utworzenie kont użytkowników indywidualnych,
* utworzenie grup użytkowników,
* przydzielanie użytkowników do grup.

Konta użytkowników tworzone są w jednostkach organizacyjnych (kontenerach) odpowiadających strukturze organizacyjnej firmy (każdy użytkownik powinien posiadać własne konto).

Do zarządzania obiektami i użytkownikami sieci NetWare wykorzystać możemy program narzędziowy NetWare. Administrator uruchamiany plikiem zlokalizowanym w folderze Public\Win32\nwadmu32 na serwerze, co odpowiada ścieżce Z:\\Win32\nwadmu32 na stacji roboczej. Inną zalecaną przez producenta aplikacją służącą do zarządzania obiektami, użytkownikami oraz całą siecią jest consoleOne. Narzędzie to spełnia rolę konsoli centralnej, za której pośrednictwem można sterować każdym aspektem sieci.

Korzystając z ConsoleOne, pracującego na komputerze z Windows, serwerze NetWare lub w systemie Unix, można wykonać następujące czynności:

* Konfigurować IDAP oraz dostęp do NDS za pomocą XML,
* Tworzyć obiekty odpowiadające użytkownikom, urządzeniom i zasobom sieciowym,
* Definiować szablony przydatne podczas tworzenia nowych kont użytkowników,
* Wyszukiwać, modyfikować, przenosić i usuwać obiekty wchodzące w skład sieci,
* Definiować uprawnienia i role w celu przydzielania uprawnień administracyjnych,
* Partycjonować i replikować bazy danych NDS na wielu serwerach,
* Zarządzać plikami i folderami w wolumenach.

**Pliki i foldery w systemie NetWare**

W systemie NetWare istnieje 8 praw określających reguły dostępu do plików i folderów. Prawa dotyczą wszystkich użytkowników systemu NetWare. Prawa te są jednostkowe co znaczy, że do wykonania operacji jest wymagane złożenie kilku praw jednostkowych, np.: uruchamianie programów wymaga uprawnień Read oraz File Scan. Do otworzenia i zmiany zawartości istniejącego pliku niezbędne są uprawnienia: Write, Create, Erase oraz Modify.

Prawa do plików i folderów:

|  |  |
| --- | --- |
| **Prawo** | **Opis** |
| **S** – *Supervisor*  (**nadzorowanie**) | Daje wszystkie prawa do folderu i znajdujących się w nim plików oraz do jego podfolderów i znajdujących się w nich plików. Pozwala nadawać dowolne prawa innym użytkownikom. Prawo Supervisor do folderu lub pliku nie może być zablokowane przez filtr IRF. |
| **R** – *Read* (**odczytywanie**) | Daje prawo do otwierania plików w folderze i czytania ich zawartości oraz do uruchomiania programów. |
| **W** – *Write* (**zapisywanie**) | Daje prawo do otwierania i zmiany zawartości plików. |
| **C** – *Create* (**tworzenie**) | Daje prawo do tworzenia nowych plików i podfolderów. |
| **E** – *Erase* (**usuwanie**) | Daje prawo do usuwania folderu, jego plików i podfolderów. |
| **M** – *Modify* (**modyfikowanie**) | Daje prawo do zmiany atrybutów lub nazwy pliku bądź folderu. |
| **F** – *File Scan* (**przeglądanie**) | Daje prawo do przeglądania struktury plików i folderów. |
| **A** – *Access Control* (**kontrolowanie dostępu**) | Daje prawo do zmiany przypisani dysponentów i filtrów IRF, co oznacza możliwość nadania wszystkim praw z wyjątkiem prawa Supervisor. |

W określaniu finalnych uprawnień obiektu NDS dużą rolę odgrywa **filtr IRF** (*Inherited Rights Filter*). Filtr ten określa, które prawa mogą być dziedziczone.

1. Dysponenci praw

Każdy plik, folder i obiekt ma swoją **listę kontroli dostępu ACL** (*Access Control List*), która określa, jakie prawa mają do niego poszczególni użytkownicy. Lista ta jest też nazywana listą dysponentów (*trustees*). **Dysponent** jest obiektem, który został umieszczony na liście ACL danego folderu lub pliku. Przed uzyskaniem praw dostępu użytkownik musi zostać zdefiniowany jako dysponent tego zbioru lub obiektu. Uprawnienia mogą być nadane użytkownikom, grupom lub kontenerom.

2. Dziedziczenie praw

Praw nadane dysponentowi folderu są **dziedziczone** przez wszystkie pliki i foldery w danym folderze i jego podfolderach.

{rysunek}

W przykładzie prawa [RWF] nadane dysponentowi do folderu *szkola* są dziedziczone, w wyniku czego dysponent ma takie same prawa do *ti* i *kl3*. Uprawnienia nadane kontenerowi są dziedziczone przez wszystkie znajdujące się w nim kontenery. Jeżeli kontener zawiera obiekty, np. użytkowników lub grupy, to każdy obiekt w kontenerze (i jego podkotenerach) uzyska prawa przypisane do kontenera.

3. Wyznaczanie praw efektywnych

**Prawa efektywne** określają wszystkie uprawnienia danego dysponenta do określonego zasobu. Prawa te są sumą praw:

* Nadanych dysponentowi lub odziedziczonych z folderów nadrzędnych,
* Wynikających z przynależności do grup, którym nadano uprawnienia.

Wpływ na prawa efektywne może mieć również filtr IRF, który umożliwia blokowanie dziedziczenia praw.

{rysunek}

Na powyższym rysunku użytkownik *JKowalski* otrzymał prawa [RWF] do folderu *szkola*. Grupa *gr1* której członkiem jest *JKowalski*, otrzymała prawa [RCEMF] do folderu *ti*. Prawa te są dziedziczone i w konsekwencji *JKowalski* uzyska efektywne prawa [RWCEMF] do folderu *kl3*.

4. Blokowanie uprawnień dziedziczonych

Prawo *Supervisor* jest dziedziczone zawsze i nie można tego dziedziczenia zablokować. Dziedziczenie pozostałych praw można blokować przez:

* Ponownie przypisanie praw dysponenta w podfolderze, np. jeśli dysponentowi nadamy prawa do folderu *ti*, to nie będzie mógł on dziedziczyć praw z foleru nadrzędnego (*szkola*);
* Zastosowanie filtru uprawnień dziedziczonych IRF.

**Filtr uprawnień dziedziczonych IRF** (*Inheritance Right Filter*) decyduje, które prawa dysponent może dziedziczyć z folderów nadrzędnych. Za pomocą filtru IRF można wpływać wyłącznie na prawa wynikające z przypisani tego dysponenta dokonanych w folderach nadrzędnych.

{rysunek}

Na powyższym rysunku pokazano działanie filtru [SRF], Filtr ten zezwala na dziedziczenie praw S,R,F, pozostałe prawa są blokowane, to znaczy, że nie mogą być dziedziczone z folderów nadrzędnych. Dysponent otrzymał prawa [RWF] do folderu *szkola*. Prawa te są dziedziczone w folderze *ti* i uprawnienia dysponenta w tym folderze są takie same. W folderze *kl3* jest zdefiniowany filtr IRF zezwalający na dziedziczenie praw [SR F]. Uprawnienia efektywne dysponenta w folderze *kl3* zawierać będą tylko [R F], ponieważ dziedziczenie prawa W jest blokowane.

5. Prawa do obiektu i właściwości

NDS przypisuje dysponentom prawa użytkowania obiektów. Dysponent obiektu jest dowolnym użytkownikiem (lub innym obiektem), któremu nadano prawa do tego obiektu.

Istnieją dwie kategorie praw:

* **Prawa do obiektu** (*Object rights*) – zadania, które dysponent może wykonać na obiekcie;

|  |  |
| --- | --- |
| **Uprawnienie** | **Znaczenie uprawnienia** |
| Browse | Umożliwia „zobaczenie” obiektu w strukturze NDS. Nie gwarantuje odczytu jego właściwości. |
| Create | W wypadku kontenerów umożliwia tworzenie w nich nowych obiektów. |
| Delete | Umożliwia usunięcie obiektu. |
| Rename | Daje możliwość zmiany obiektu. |
| Supervisor | Oznacza posiadanie wszystkich praw obiektowych do obiektu. |

Prawa te pozwalają delegować uprawnienia do administrowania poszczególnymi kontenerami , np. jednostkami organizacyjnymi. Prawa mogą być delegowane przez dołączenie użytkownika do grupy mającej określone uprawnienie, np. do grupy *nauczyciele*, lub przez nadanie uprawnień użytkownikowi.

6. Dostęp do zasobów serwera

Dostęp do zasobów serwera w celu zapisu, odczytu danych bądź uruchomienia aplikacji odbywa się ze stacji roboczej. Po zalogowaniu na konto można przeglądać otoczenie sieciowe, wykorzystując Eksplorator Windows. Odwołanie się do zasobów serwera odbywa się przez wskazanie elementów w otoczeniu sieciowym.

Inną metodą uzyskania dostępu do zasobów jest mechanizm **mapowania dysków**. Mechanizm ten tworzy w systemie Windows nowy dysk sieciowy i przypisuje mu zasób sieciowy serwera, np. folder. W takim wypadku odwołanie do zasobów sieciowych odbywa się przez wskazanie odpowiedniego dysku oznaczonego literą, tak jak dyski lokalne.

7. Zarządzanie środowiskiem pracy za pomocą programu zgłoszeniowego

Każdy użytkownik systemu NetWare może mieć utworzony **program zgłoszeniowy** (*login script*), wykonywany po zalogowaniu się użytkownika w sieci. Administrator lub użytkownik może w ten sposób dopasować środowisko pracy do swoich potrzeb, np. program zgłoszeniowy może wykonać mapowanie dysków. W ten sposób każdy z użytkowników może szybko uzyskać dostęp do potrzebnych zasobów. Środowisko to będzie jednakowe, niezależnie od komputera, na którym loguje się użytkownik. Istnieją trzy rodzaje programów zgłoszeniowych, a kolejność ich wykonania jest następująca:

* **login script systemowy (kontenerowy)** – wykonywany podczas logowania dla każdego z użytkowników utworzonych w danym kontenerze, np. w kontenerze *szkola*;
* **login script profilowy (grupowy)** – umożliwia stworzenie identycznego środowiska pracy dla grupy użytkowników, np. *klasa2*;
* **login script indywidualny** – umożliwia każdemu użytkownikowi samodzielne skonfigurowanie środowiska pracy systemu w zależności od potrzeb.

W przypadku braku loginu scriptu indywidualnego zostaje wykonany domyślny program zgłoszenia. Zdefiniowanie login scriptu kontenerowego i profilowego, a nie zdefiniowanie indywidualnego powoduje, że zostanie wykonany program domyślny, który może zmieniać parametry środowiska pracy użytkownika (również te ustawione przez wcześniej wykonywane scripty). Jeżeli jest zdefiniowany login script kontenerowy lub profilowy, to należy również zdefiniować program zgłoszeniowy indywidualny użytkownika (nawet poprzez np. wpisanie pustej linii).

W programach zgłoszeniowych często używane jest polecenie map, służące do mapowania zasobów sieciowych. Przykładowo, aby utworzyć dysk sieciowy oznaczony literą f: i przypisać do niego folder **public** na wolumenie **fserver\_sys**, należy użyć polecenia:

**Map f:=fserver\_sys:public.**

8. Atrybuty plików i folderów

Każdy plik I folder może opisać za pomocą **atrybutów**, które określają sposób ich wykorzystania przez system. Atrybuty pozwalają na wprowadzenie restrykcji niezależnie od uprawnień użytkowników. Atrybuty dotyczą plików lub folderów i działają niezależnie od tego, jaki użytkownik zamierza uzyskać do nich dostęp.

**Drukowanie w sieci NetWare**

Drukarka w sieci NetWare może być współdzielona, to znaczy skonfigurowana w taki sposób, aby mogli na niej drukować uprawnieni użytkownicy z całej sieci, korzystający z dowolnej stacji roboczej. Drukarki przeznaczone do obsługi wszystkich stacji roboczych są nazywane **drukarkami sieciowymi**. Drukarka jest reprezentowana jako obiekt w bazie NDS. Każda drukarka sieciowa musi być przyłączona do węzła sieci, np. stacji roboczej albo **serwera drukowania** (*print server*). Serwera drukowania musi być zdefiniowany jako obiekt w NDS. Na serwerze tym jest uruchomiony, jako moduł ładowalny, proces nadzorujący obsługę wydruków. Wydruk jest kierowany do **kolejki drukowania** (*print queue*). Kolejka drukowania jest podfolderem, w którym są magazynowane zadania drukowania (*print job*). Kolejka drukowania jest obsługiwana przez określoną drukarkę fizyczną, na której powstaje rzeczywisty wydruk. Do kolejki mogą być kierowane nowe zadania, ustawiające się na jej końcu. **Zadanie drukowania** powstaje w wyniku wydania polecenia przez oprogramowanie stacji roboczej. Po przekazaniu wszystkich danych stanowiących wydruk program drukujący deklaruje koniec tworzenia zadania i od tego momentu zadanie drukowania nie jest związane z programem, który je utworzył. Każde zadanie jest przechowywane w postaci pliku w kolejce, do której zostało skierowane. Plik zadania drukowania jest usuwany po zakończeniu wydruku.

1. Tworzenie systemu usług drukarskich

Uruchomienie usługi drukowania obejmuje wykonanie pewnych czynności po stronie serwera i po stronie stacji roboczej, po których drukarka jest gotowa do użytku i może przyjmować zadania.

Konfigurowanie usługi drukowania po stronie serwera polega na utworzeniu obiektu kolejki drukowania w kontenerze np. *szkola*, w którym następnie należy utworzyć obiekt drukarka i ustawić jego właściwości. Następnie należy dodać kolejkę do drukarki, utworzyć obiekt serwera wydruku i dodać do niego drukarkę.

UWAGA!!!

Aby serwer podczas uruchamiania ładował moduł PrintServer, w pliku **autoexec.ncf** (wolumin SYS) musi znajdować się wpis LOAD PSERVER nazwa\_serwera\_wydruku. Jeżeli wpis nie istnieje, należy go dodać do pliku.

Konfigurowanie usługi drukowania po stronie stacji roboczej z systemem Windows polega na dodaniu do systemu drukarki sieciowej. O wystąpieniu błędów w drukowaniu spowodowanych np. brakiem papieru lub wyłączeniem drukarki użytkownik jest informowany za pomocą specjalnych komunikatów.

2. Środowisko drukowania NDPS

**Rozproszenie środowisko drukowania NDPS** (*Novell Distributed Print Services*) jest wykorzystywane w NetWare 5.x i nowszych. Usługi NDPS łączą drukarkę, kolejkę drukowania i serwer drukowania w jedną całość, nazywaną **agentem drukowania**. Użytkownicy przesyłają zadania drukowania bezpośrednio do drukarki, a nie do kolejki drukowania. Na stacji roboczej nie muszą być przechowywane programy obsługi drukowania, gdyż usługi NDPS wczytują je do stacji roboczej z sieci.

W skład środowiska wchodzą następujące komponenty:

* **agent druku** (*Printer Agent*) – jest to aplikacja uruchomiana na serwerze NetWare (dla drukarek niezgodnych z NDPS) lub program wbudowany w drukarkę sieciową (dla drukarek zgodnych z NDPS), Agent może reprezentować tylko jedną drukarkę i zwykle drukarka ma tylko jednego agenta. Agent druku zajmuje się przetwarzaniem informacji o zadaniach drukowania, statusie i konfiguracji drukarki, bierze udział w generowaniu powiadomień o stanie drukarki i zadań wydruku.
* **Menedżer drukowania NDPS** (*NDPS Manager*) – służy do tworzenia i zarządza agentami wydruku. Musi być stworzony, zanim do sieci zostanie przyłączona drukarka. Jest reprezentowany przez ładowalny moduł NDPSM.NLM, uruchamiany z konsoli serwera. W serwerze może istnieć tylko jeden menedżer NDPS.
* **bramka drukarki** (*Printer Gateway*) – pozwala na wysyłanie zadań drukowania do drukarki niezgodnej z NDPS poprzez tłumaczenie zadań drukowania z języka NDPS na język konkretnej drukarki. Drukarki sieciowe zgodne z NDPS mają interfejsy umożliwiające ich bezpośrednie przyłączenie do sieci, pozostałe drukarki korzystają ze standardowej bramki Novell Gateway.

!!!!!!!!!!!!

**Sieciowy system operacyjny Windows Server**

**Podstawowe pojęcia związane z Active Directory**

W systemach Windows Server można podzielić użytkowników i grupy na:

* **użytkowników lokalnych i grupy lokalne** – konta są tworzone na lokalnym dysku komputera i umożliwiają korzystanie z jego zasobów. Przechowywane są tylko na komputerach, na których zostały stworzone. Miejscem przechowywania kont jest **baza SAM** (*Security Accounts Manager*) zapisana lokalnie na komputerze. Konta użytkowników lokalnych są inne na każdym komputerze, nawet gdy nazwy użytkowników są takie same.
* **użytkowników domenowych i grupy domenowe** – konta mają na celu umożliwienie logowania użytkowników do domeny, co umożliwia korzystanie z zasobów z dowolnego komputera przyłączonego do domeny. Konta użytkowników domenowych przechowywane są w **usługach katalogowych** (*Active Directory*) na kontrolerach domeny i następnie replikowane pomiędzy wszystkimi kontrolerami w domenie.

Active Directory (AD) jest to usługa katalogowa dla systemów Windows. Od systemu Windows 2008 otrzymała nazwę Active Directory Domain Services (AD DS), aby identyfikować usługę katalogową jako zapewniającą uwierzytelnianie zasobów w obrębie organizacji, w której usługi sieciowe kontroluje wewnętrzna domena, i zarządzanie nimi. Opisuje ona strukturę sieci i jej składników. Można pracować w trybie natywnym (*native*) lub w trybie zgodności ze starszymi wersjami Windows. W trybie natywnym w sieci obsługiwane są tylko systemy Windows 2000 i nowsze. Jeżeli w sieci znajdują się komputery z systemami Windows Millenium i starszymi, to konieczny jest tryb zgodności, aby mogły one łączyć się do naszej domeny. Domyślnie wybierany jest tryb natywny, a włączenie trybu zgodności możliwe jest w konfiguracji niestandardowej.

Active Directory jest przestrzenią nazw. **Przestrzeń nazw** (*namespace*) to ograniczony obszar, w którego obrębie nazwa może być odnaleziona i wykorzystana do uzyskania dostępu do obiektu oraz jego atrybutów lub usług (przykładem przestrzeni nazw może być system plików w systemie operacyjnym, w którym na podstawie nazwy plików i ścieżki dostępu możemy zlokalizować plik). Przestrzeń nazw w AD może być ciągła lub nieciągła. Przestrzeń jest ciągła, jeśli w całej strukturze istnieje dokładnie jeden obiekt typu korzeń (*root*) i nazwa obiektu podrzędnego (*child*) – powstaje przez dodanie prefiksu do nazwy obiektu nadrzędnego (*parent*). Gdy nie ma jednego korzenia, przestrzeń jest nieciągła.

**Obiekt** to wyróżniony, nazwany zbiór atrybutów reprezentujący np. użytkownika, drukarkę lub komputer. Zbiór wszystkich możliwych rodzajów obiektów występujących w Active Directory i związanych z nimi atrybutów stanowi **schemat** (*schema*).

W Active Directory podstawowym elementem konstrukcji jest domena. **Domena** to grupa komputerów połączonych w sieć, składająca się z serwera pełniącego rolę kontrolera domeny oraz stacji roboczych – klientów współdzielących bazę katalogową. Kontroler domeny przechowuje informacje o użytkownikach sieci i ich uprawnieniach. Dzięki temu informacje te gromadzone są w jednym miejscu i dostępne dla wszystkich klientów, co ułatwia zarządzanie siecią. W dużych sieciach może być więcej kontrolerów domeny, ale w takim przypadku wymieniają się między sobą przechowywanymi informacjami o sieci. Kontrolery domeny są równoprawne – każdy ma zapisywalną replikę tej samej bazy danych.

Domena wchodzi w skład **drzewa**, czyli związku wielu domen mających ten sam schemat, konfigurację i tworzących ciągłą hierarchiczną przestrzeń nazw. Przyłączenie domeny do drzewa jest określone w momencie instalacji jej pierwszego kontrolera.

Las to struktura złożona z wielu drzew, także o wspólnym schemacie i konfiguracji, ale nieposiadająca ciągłej przestrzeni nazw. Las może składać się z jednego drzewa lub wielu drzew. Przynależność do lasu jest określana w momencie instalacji pierwszego kontrolera domeny – przed określeniem przynależności do drzewa.

Przykładowy las pokazany jest na poniższym rysunku:

{rysunek}

Przestrzeń nazw w Active Directory została zorganizowana hierarchicznie. Obiekty typu kontenery (pojemniki) mogą przechowywać inne obiekty. Nazwa obiektu w Active Directory opisuje jego położenie w strukturze hierarchicznej. Taką nazwę określa się mianem **pełnej nazwy DN** (*Distinguished Name*).

Podstawowe składniki DN to:

* **DC** – komponent domenowy (*Domain Component*)
* **CN** – nazwa obiektu (*Common Name*),
* **OU** – jednostka organizacyjna (*Organizational Unit*),
* **O –** organizacja (*Organization*).

Na przykład zapis **O=Internet/DC=PL/OU=ZSP/CN=uczen** oznacza, że obiekt **uczen** jest zlokalizowany w jednostce organizacyjnej **ZSP** domeny **PL** w organizacji **Internet**.

**Nazwa względna obiektu RDN** (*Relative Distinguished Name*) jest to część pełnej nazwy DN, zawierająca tylko atrybuty obiektu, np. w nazwie pełnej DN atrybutem obiektu jest „uczen” i jest to nazwa względna RDN tego obiektu.

Domena AD jest zorganizowana hierarchicznie, a jej podstawowym składnikiem jest jednostka organizacyjna OU. Jest ona kontenerem, dzięki czemu może zawierać w sobie inne obiekty, co pozwala grupować zasoby i użytkowników oraz delegować prawa administracyjne. Jednostki organizacyjne mogą być uporządkowane hierarchicznie, np. w modelu geograficznym jednostki są tworzone zgodnie z lokalizacjami oddziałów firmy, natomiast w modelu organizacyjnym struktura jednostek powinna odpowiadać strukturze organizacyjnej firmy.

Oprócz jednostek organizacyjnych w Active Directory możemy tworzyć obiekty reprezentujące:

* Użytkowników,
* Komputery,
* Drukarki,
* Grupy,
* Udostępnione foldery,
* Kontrakty.

Obiekty tworzone w Active Directory są reprezentantami rzeczywistych zasobów sieci.

W Active Directory są dwie kategorie grup:

* **Grup dystrybucyjna** (*Distribution*) – grupa używana jedynie do dystrybuowania wiadomości e-mail. Grupa Dystrybucyjna nie jest związana z zabezpieczeniami, tzn. nie można jej przypisać uprawnień.
* **Grup zabezpieczeń** (*Security*) – grupa przeznaczona do przyznawania uprawnień do obiektów (posiada możliwości grup dystrybucyjnych).

Występują trzy rodzaje grup bezpieczeństwa:

* **Grupa globalna** – do grupy globalnej mogą należeć konta użytkowników, komputerów i grupy globalne należące tylko do tej samej domeny co grupa globalna. Grupie globalnej można przypisać uprawnienia do obiektów z dowolnej domeny. Wykorzystywane są do grupowania użytkowników w zależności od ich uprawnień,
* **Grupa lokalna w domenie** – do grupy lokalnej w domenie mogą należeć konta użytkowników, komputerów i grupy globalne z dowolnej domeny oraz grupy uniwersalne. Grupie lokalnej w domenie można przypisać jedynie uprawnienia do obiektów z tej samej domeny. Wykorzystywane są do grupowana grup globalnych z różnych domen, które mają posiadać takie same uprawnienia do obiektu (np. drukarki) znajdującego się w tej samej domenie co grupa lokalna w domenie.
* **Grupa uniwersalna –** występuje jedynie w trybie natywnym. Mogą do niej należeć konta użytkowników, komputerów oraz grupy uniwersalne i globalne z dowolnej domeny. Grupie uniwersalnej można przypisać uprawnienia do obiektów z różnych domen.

Tworząc strukturę grup, należy przydzielić użytkowników do grup globalnych, przydzielić grupy globalne do grup lokalnych, a następnie nadać prawa grupom lokalnym.

Przykład szkolnej sieci zbudowanej z trzech domen

Domena główna o nazwie **zsp.local** ma dwie poddomeny: **administracja.zsp.local** oraz **szkola.zsp.local**. W domenie **zsp.local** znajduje się drukarka, z której mają korzystać