Wyższa Szkoła Informatyki i Zarządzania

LOKALNE I ROZLEGŁE SIECI KOMPUTEROWE

mgr inż. Marcin Tomana

Bielsko-Biała 1999

Spis treści

Spis treści 2

1 Wprowadzenie do sieci komputerowych 4

1.1 Historia sieci komputerowych 4
1.2 Zalety korzystania z sieci 4
1.3 Komponenty sieci 5
1.4 Model sieci OSI 5
1.5 Instytucje standaryzujące w dziedzinie sieci 6

2 Technologie sieci lokalnych 8

2.1 Okablowanie sieci 8
2.2 Topologie sieci 8
2.3 standardy IEEE 9
2.4 Ethernet 9

3 Technologie sieci rozległych 11

3.1 Transmisja cyfrowa ISDN 11
3.2 Technologie transmisji xDSL 12
3.3 Sieci pakietowe X.25 13
3.4 Sieci FrameRelay 13
3.5 Sieci ATM 15

4 Protokoły komunikacyjne 18

4.1 NetBIOS, NetBEUI 18
4.2 Protokół IPX/SPX 18
4.3 Protokół IP 18
4.4 Zamiana adresu IP na adres MAC – ARP/RARP 19
4.5 Protokół ICMP 19
4.6 Routing - trasowanie 20
4.7 Typy algorytmów routowania 21
4.8 Wybór protokołów i trasowanie 21
4.9 Protokół TCP i UDP 22

5 Sprzęt sieciowy 23

5.1 Regenerator – Repeater 23
5.2 Koncentrator – Hub 23
5.3 Most – Bridge 23
5.4 Przełącznik – Switch 23
5.5 Router 24

6 Sieci typu Peer-To-Peer 25

6.1 Lantastic 25
6.2 Microsoft Network 26

7 Sieci oparte o Windows NT/2000 27

7.1 Domeny użytkowników 27
7.2 Współpraca z Windows 95/98 28

8 Sieć Novell Netware 31

8.1 Usługi katalogowe bindery i NDS. 31
8.2 Oprogramowanie serwera 31
8.3 Netware SFT (System Fault Tolerancy) 32
8.4 Oprogramowanie klienckie 32
8.5 Prawa do plików 34

9 Sieci opierające się na systemach UNIX 35

9.1 Praca terminalowa 35
9.2 Serwery terminali 35
9.3 Praca sieciowa systemów UNIX 36

10 Bezpieczeństwo sieci 38

10.1 Zabezpieczenie sprzętowe serwerów 38
10.2 Serwery dublujące 39
10.3 Zabezpieczenie ciągłości zasilania 39
10.4 Archiwizacja danych 40
10.5 Zabezpieczenia serwerów sieciowych przed włamaniami 40
10.6 Zabezpieczanie sieci – Firewall 42

Spis rysunków 44

Literatura dodatkowa 45

1 Wprowadzenie do sieci komputerowych

1.1 Historia sieci komputerowych

Rozwój sieci można przedstawić równolegle z rozwojem sprzętu komputerowego na przestrzeni lat w następujący sposób:
lata 50-te: brak sieci, bardzo drogie komputery, era komputerów typu MainFrame
lata 60-te: terminale znakowe - podział czasu komputera, pierwsze łącza modemowe i zdalna praca na serwerze
lata 70-te: minikomputery - masowa produkcja, rozproszenie zasobów na komputerach
lata 80-te: rozwój PC i sieci lokalnych, rozwój pierwszych systemów sieciowych dostępnych powszechnie dzisiaj.

Sieć lokalna obejmuje ograniczony obszar, ułatwia współdzielenie danych i zasobów, pierwsze sieci - zasada *file locking'u* – blokowanie całych plików w przypadku dostępu określonej stacji. Później wprowadzono wygodniejszy *record locking* – dostęp do pliku równoczesny wielu stacji, blokowanie tylko fragmentów pliku przez określoną stację.

Sieci rozległe obejmują obszary całych miast, regionów, krajów a nawet świata. Sieć rozległa łączy ze sobą sieci lokalne przy pomocy specjalnych łącz – najczęściej dużo wolniejszych niż przepustowości sieci lokalnych.

1.2 Zalety korzystania z sieci

- wspólny dostęp do danych (plików, baz danych),
- wspólne korzystanie z urządzeń peryferyjnych (drukarek, modemów),
- przesyłanie informacji pomiędzy użytkownikami sieci - poczta elektroniczna (tekst, grafika, dźwięk),
- szybka dystrybucja informacji, uaktualnień, poprawek oprogramowania,
- w przypadku organizacji możliwość zdalnego zarządzania sprzętem w oddziałach, filiach itp.,
- możliwość integracji głosu w ramach sieci rozległej,

1.3 Komponenty sieci

- SERWER PLIKÓW – (ang. File Server) - Początkowo serwer dysków, główna funkcja to udostępnianie plików na zasadzie uwspólniania, może udostępniać również inne zasoby. Można wyróżnić serwery dedykowane i niededykowane (np. sieci peer-to-peer).
- STACJA ROBOCZA – (ang. Workstation). Niezależna stacja, która jest wyposażona w kartę sieciową i może korzystać z zasobów sieci.
- TERMINAL – (ang. Terminal). Stacja sieciowa, która bez działającego serwera sieci nie może wykonywać żadnych zadań. Podłączony przez sieć przez łącze szeregowe najczęściej do serwera terminali a nie bezpośrednio do koncentratora czy przełącznika. Wykorzystywany najczęściej w sieciach Unix.
- SERWER WYDRUKU – (ang. Print Server) – Może być dedykowany lub nie. Obsługuje zlecenia drukowania w sieci. Najczęściej stosowane są techniki kolejkowania zadań drukowania. Obsługa drukarek lokalnych i zdalnych – podłączonych do innych stacji w sieci.
- SERWER BAZY DANYCH – (ang. Database Server) – Obsługa bazy danych w konkretnej implementacji. Zasada obsługi bazy – Klient-Serwer. Najczęściej obsługiwany standard – język SQL, np. Gupta SQL Base, Microsoft SQL Server, PostrgreSQL, Interbase.
- SERWER TERMINALI – (ang. Terminal Server) – Najczęściej urządzenie wyłącznie sprzętowe. Może być również komputer z kartą wieloportową. Obsługuje dostęp do serwera terminali, drukarek lub połączeń dialup z modemów. Wpięty bezpośrednio do sieci np. koncentratora lub przełącznika.

1.4 Model sieci OSI

Zatwierdzony przez organizację ISO.
Model ten opisuje określone warstwy, z czego każda ma zdefiniowane funkcje i cele.
Warstwy te można podzielić na dwie grupy:

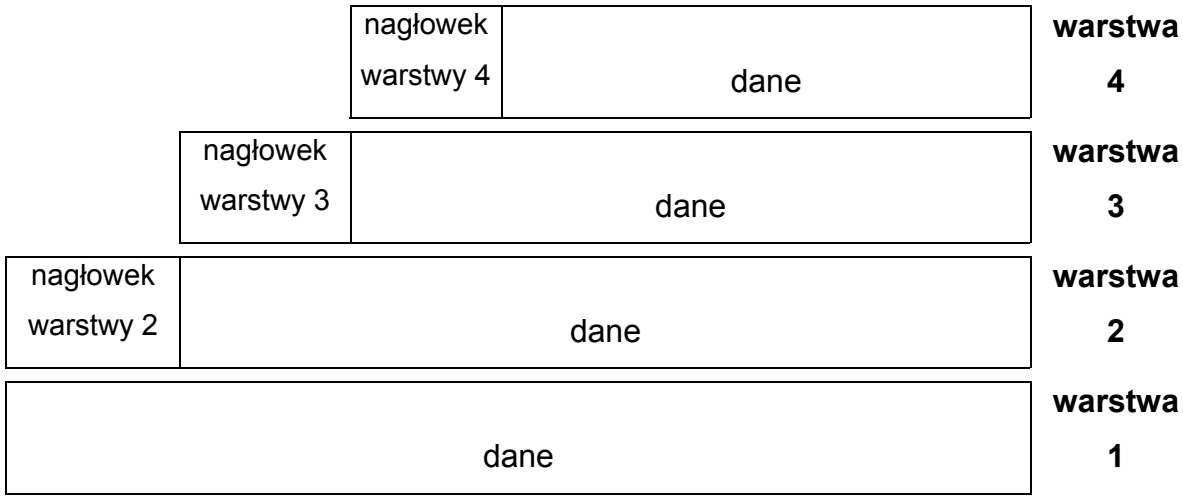
- warstwy niższe - transport danych
- warstwy wyższe – aplikacji

Standard OSI – (Open Systems Interconnection) opisuje następujące 7 warstw:

1. warstwa fizyczna - definiuje sprzęt, poziomy napięć, par. czasowe, handshaking
2. warstwa łącza danych - formatowanie *ramek* przed transmisją, dane kontrolne, korekta danych

3. warstwa sieci - tworzenie *pakietów* danych, ustawianie połączeń wirtualnych dwóch komputerów
4. warstwa transportowa - kierowanie przesyłem danych, rozpoznawanie błędów
5. warstwa sesji - zarządzanie siecią - hasła, konta, logowanie
6. warstwa prezentacji - transfer plików, bezpieczeństwo sieci, konwersje formatów
7. warstwa zastosowań - programy użytkowe wykorzystujące sieć

Wymiana informacji następuje między równorzędnymi warstwami stacji nadawczej i odbiorczej. Każda warstwa dodaje informacje sterujące (nagłówki) do danych. W praktyce bardzo dużo danych przesyłanych przez sieć to dodatkowe informacje sterujące a nie fizyczne dane.



Rys. 1 Schemat budowy ramki przy transmisji danych w sieci

Wielkość i zawartość nagłówka w danej warstwie definiuje określony protokół wybrany do transmisji danych. W warstwie 1 wyróżnia się tylko strumień danych (bitów) przesyłanych po medium.

W warstwie drugiej definiowana jest wielkość przesyłanej paczki danych zwanych *ramką*. W nagłówku pojawiają się zawsze (niezależnie od protokołu) dane o stacji wysyłającej i odbierającej ramkę – fizyczne adresy sieciowe. Dane w warstwie drugiej zawierają paczkę danych z warstwy trzeciej zwaną *pakietem,* w którego nagłówku dodawane są informacje protokołu wykorzystywanego w tej warstwie. Zasada ta jest stosowana na wyższych warstwach identycznie. Zawsze warstwa niższa w danych zawiera paczkę danych protokołu warstwy wyższej.

1.5 Instytucje standaryzujące w dziedzinie sieci

ISO – International Organization for Standardization

Odpowiada za bardzo szeroki zakres standardów. W zakresie sieci komputerowych najbardziej znany jest udział ISO w opracowaniu modelu OSI.

ANSI – American National Standards Institute

jest członkiem ISO. Opracował standard sieci FDDI

EIA – Electronic Industries Association

Opracowuje standardy dotyczące transmisji. np. RS-232

IEEE – Institute of Electrical and Electronic Engineers

Profesjonalna organizacja, która dla sieci opracowała standardy szeroko stosowane w sieciach lokalnych: IEEE 802.3, IEEE 802.5

IAB – Internet Activities Board

Proponuje dokumenty zwane RFC (Requests for Comments) jako standardy internetu, np. TCP/IP, SNMP, RIP

2 Technologie sieci lokalnych

2.1 Okablowanie sieci

W sieciach lokalnych zakłada się wysoką przepustowość danych więc stosowane okablowanie musi być wysokiej jakości.

- Koncentryk – (ang. Coaxial Cable). Kilka odmian grubości, duża długość. Prędkość transmisji 10-80 Mbit/sek. w paśmie podstawowym. Dość prosty w instalacji.
- Skrętka – (ang. Twisted Pair). Szereg skręconych wokół siebie par kabli miedzianych. Technologia tania, prosta w instalacji. Duży problem stanowią zakłócenia – wprowadzono w tym celu pojęcie kategorii sieci, która definiuje parametry kabli (najpopularniejsze - kat. 3 i 5) Długość 100 do 300m od szafy krosującej. Prędkość transmisji: 10Mbit, 100Mbit, 1GBit.
- Światłowód - Bardzo duża prędkość transmisji od 100Mbit. Względnie duży koszt ze względu na urządzenie przetwarzające światło na sygnał elektryczny. Niemożność podsłuchu. Nadawanie światła przez laser lub LED.
- Bezprzewodowo - Transmisja bezprzewodowa – niepotrzebna instalacji i budowa infrastruktury sieci. Specjalne radiowe karty sieciowe przesyłające na poziomie fal radiowych. Transmisja w falach podczerwieni – większa przepustowość, ale ograniczenia w odległości i kanale transmisji.

2.2 Topologie sieci

Przez topologie sieci rozumie się układ wszystkich połączeń sieci umożliwiający wzajemną pracę komputerów. Niektóre topologie są bardziej uniwersalne. Budowane są wtedy tzw. sieci strukturalne. Rozwiązanie takie daje możliwość wykorzystania infrastruktury sieci do różnych zastosowań od przesyłania w sieci normalnej transmisji komputerowej przez połączenia szeregowe (terminale, drukarki) do podłączania telefonów cyfrowych i analogowych czy telewizji przemysłowej.

Wyróżnić można następujące topologie:

- gwiazda – technologia dziś najbardziej popularna. Opiera się na centralnym miejscu z którego rozchodzą się wszelkie kable do gniazd sieciowych. Bardzo łatwe w zarządzaniu i wszelkich zmianach połączeń. Najczęściej buduje się w postaci tzw. sieci strukturalnych zintegrowanych z sieciami telefonicznymi lub telewizji przemysłowej.

- magistrala – bardzo często stosowana. Opiera się na szeregowym połączeniu komputerów. Bardzo duża wadą jest brak działania całej sieci w przypadku awarii jednego z połączeń.
- gwiazda rozproszona – żadko używana technologia stosowana jako ArcNet. Opiera się na zastosowanie sprzętu aktywnego w różnych miejscach sieci co bardzo komplikuje zarządzanie i usuwanie awarii.
- pierścień – stosowana w przypadku sieci Token Ring, opiera się na rotacyjnym dostępie do medium, bardzo efektywna przy dużym natężeniu ruchu.

2.3 standardy IEEE

Organizacja IEEE wprowadziła w sieciach lokalnych następujące standardy:

802.3 – Występuje tu rywalizacja o dostęp do medium. Stosowana w sieci ethernet. Definiuje format ramki - 46-1500 bajtów danych, zasięg 500m, kabel 50Ω. Wykorzystuje się tu protokół CSMA/CD, który określa metody unikania kolizji w sieci. Każda karta sieciowa wysyła sygnał próbny i sprawdzane jest czy w tym momencie nikt inny równocześnie tego nie zrobił. Urządzenie ma wtedy dostęp do medium i może transmitować dane. W przypadku detekcji kolizji oba urządzenia po losowym czasie opóźnienia powtarzają próbę transmisji.

Standard ten ma kilka rozwiązań praktycznych:

802.3 10Base5 - gruby ethernet - yellow ethernet, zasięg 500m 10 Mbit/sek.

802.3 10Base2 - cieńki ethernet, zasięg 200m 10 Mbit/sek.

802.3 10BaseT - twisted pair, skrętka do 100m 10 Mbit/sek.

802.4 – Dostęp do medium jest według tablicy kolejności. Dostęp przekazywany jest od stacji do stacji. Rozwiązanie stosowane w sieciach ArcNet o dość skomplikowanej topologii, która już nie jest stosowana.

802.5 – Dostęp do medium jest przekazywany od stacji do stacji. Stacje dodatkowo regenerują sygnał, który jest przekazywany przez sieć. Dostęp realizowany jest jako krążący token w sieci. Standard ten wykorzystywany jest w sieciach Token Ring.

2.4 Ethernet

Najczęściej stosowana technologia w sieciach lokalnych. Wykorzystywana może być topologia gwiazdy lub szeregowa. Dostęp do medium realizowany jest przy pomocy zasady CSMA/CD (patrz Rozdział 2.3) opierającej się na prostej zasadzie, że każdy uczestnik nasłuchuje czy w danym momencie nie transmituje ktoś inny. Jeśli medium jest wolne to dochodzi do transmisji. W przypadku wystąpienia dwóch równoczesnych prób transmisji

(kolizja) transmisja jest przerywana i po losowym czasie wznawiana. Bardzo dobrze się sprawdza w przypadku niewielkiego natężenia ruchu. W momencie gdy natężeniu ruchu dochodzi do dużych wartości wydajność tej technologii drastycznie spada przez zbyt dużą liczbę kolizji. Jest dość wydajna przy jednostkowych dużych transferach małej liczby stacji.

Ethernet działa na poziomie warstwy drugiej i wprowadza pojęcie adresu fizycznego urządzenia w sieci. Adres fizyczny tzw. MAC Address nadawany jest przez producenta i użytkownik nie ma możliwości zmiany tego adresu. MAC Address składa się z 6 bajtów zapisywanych zazwyczaj w postaci szesnastkowej. Poszukiwanie adresu fizycznego w sieci opiera się na zasadzie broadcastu, czyli ramki rozgłoszeniowej o adresie FF:FF:FF:FF:FF:FF, która jest odbierana przez wszystkie urządzenia ethernet.

3 Technologie sieci rozległych

3.1 Transmisja cyfrowa ISDN

Technologia ISDN (Integrated Services Digital Network) powstała z rozwojem systemów telekomunikacyjnych. Jest to system cyfrowej transmisji danych (w telekomunikacji głosu) umożliwiający wykorzystanie istniejącej infrastruktury telekomunikacyjnej. W telekomunikacji wykorzystywany jest jako system łączący centrale abonenckie oraz centrale z końcowymi użytkownikami. Dla docelowych użytkowników cenne są różnorakie dodatkowe usługi oraz możliwość integracji przekazów cyfrowych po liniach telefonicznych (np. obraz video). Dzięki specjalnym adapterom można wykorzystywać standardowe urządzenia analogowe do transmisji głosu (telefony, modemy, faxy grupy 3).

Łącza ISDN są również w sieciach rozległych wykorzystywane jako połączenia awaryjne (backup interface) uaktywniane w momentach awarii standardowych łącz sieci rozległych a normalnie wykorzystywanych do normalnych linii telefonicznych.

Istnieją dwie metody dostępu: dostęp podstawowy BRA (Basic Rate Access) oznaczany jako 2B+D oraz dostęp pierwotny PRA (Primary Rate Access) oznaczany jako 30B+D. Dostęp typu BRA umożliwia zestawienie 2-ch kanałów 64kbit/s zaś PRA 30-tu kanałów. Dla dostępu typu PRA często wykorzystywany jest HDSL 2Mbit/s (patrz rozdział 3.2).

ISDN podłącza się przy pomocy specjalnego urządzenia – zakończenia sieciowego (NT), z którego wyprowadzany jest tzw. styk S (maksymalnie 8 linii), do którego można podłączyć urządzenia ISDN (telefon ISDN, fax grupy 4, komputer z kartą ISDN) lub specjalne adaptery. Następnie tworzą one tzw. styk R, do którego można podłączyć już dowolne urządzenie analogowe pracujące na standardowych liniach telefonicznych (np. analogowy modem).

Sieci ISDN bardzo często używa się do łączenia lokalnych centralek PABX z centralami operatora telekomunikacyjnego. Umożliwia to wykorzystanie dodatkowych usług i przeniesienia całego ruchu dotyczącego dużej strefy numeracyjnej na centrale klienta a nie operatora. W ten sposób tworzone są tzw. call centers – centra informacyjne. Najcenniejszą usługą ISDN jest tu usługa DDI (xxx) umożliwiająca przy pomocy kanału PRA lub kilku BRA przeniesienie zestawiania połączeń do lokalnej centrali PABX klienta. Daje to bardzo wygodny i łatwo modyfikowalny przez klienta system połączeń głosowych, faxowych, wideokonferencyjnych.

3.2 Technologie transmisji xDSL

Cała technologia DSL (Digital Subscriber Line) została stworzona dla wzrastającego zapotrzebowania na szerokopasmowe usługi wymagające wysokich transferów danych. Technologia umożliwia korzystanie z normalnych dwuprzewodowych linii telefonicznych bezpośrednio w otoczeniu abonenta typowej sieci telekomunikacyjnej. Wspólną cechą urządzeń xDSL jest asymetryczny dostęp do medium. Technologia zapewnia transfer od 16kb/s do 8Mb/s. Jest to bardzo konkurencyjna technologia w stosunku do ISDN.

Rodzaje technologii xDSL

IDSL (ISDN DSL) – zintegrowaną

HDSL (High bitrate DSL) – o podwyższonej przepływności

ADSL (Asymetric DSL) – asymetryczną

CDSL (Consumer DSL) – powszechną

SDSL (Symetric DSL) – symetryczną

RADSL (Rape adaptive DSL) – adaptacyjną

VDSL (Very High Speed DSL) – o bardzo wysokiej przepływności (52Mb/s w kierunku dosyłowym)

Najbardziej rozpowszechnione do zestawiania łącz stałych (nie komutowanych) są technologie ADSL i HDSL.

W technologii ADSL korzystając z istniejących łączy telefonicznych można w ograniczonym zasięgu (max. 5,6km) uzyskać w kierunku abonenta przepływność od 1,5Mbit/s do 6-8Mbit/s. Łącza ADSL można niestety zestawiać tylko dla określonych, stałych, z góry zdefiniowanych tras. Nie ma, tak jak w przypadku np. ISDN, możliwości wykorzystania central telefonicznych, przełączania i zestawiania różnych tras. ADSL przy inicjalizacji połączenia system automatycznie sprawdza maksymalną szybkość transmisji dostępną w każdym podpaśmie kanału i ustala na bieżąco sumaryczną wartość przepływności użytkowej kanału w bezpiecznych marginesach, z uwzględnieniem istniejących zakłóceń. Optymalizacja przepływnościa łącza jest powtarzana przed każdą kolejną transmisją.

W technologii HDSL istnieje możliwość przesyłania danych zwykłą linią telefoniczną z szybkością 2Mbit/s. Łącza HDSL wykorzystywane są również w telekomunikacji do łączenia central oraz do zestawienia 30 kanałów telefonicznych (cyfrowych, każdy po 64 kbit/s). Odległość pomiędzy dwoma urządzeniami HDSL bez konieczności stosowania wzmacniaczy pośrednich (regeneratorów sygnału) może być od kilku do kilkunastu kilometrów.

3.3 Sieci pakietowe X.25

Przełączanie pakietów, które stało się podstawą budowy rozległych sieci pakietowych, zostało wprowadzono po raz pierwszy w sieci ARPANET (Advanced Research Project Agency Network), która była początkiem dzisiejszego internetu. Protokół X.25 jest pierwszym wykorzystywanym do takich celów i jest stosowany do dzisiaj przy wolniejszych sieciach o przepustowości od 64kb/s do 2Mb/s.

Technologia X.25 charakteryzuje się dość dużym mechanizmem korekcji błędów i sterowania przepływem, co oznacza, że każdy węzeł sprawdza kompletność i poprawność odebranego pakietu.

Protokół X.25 jest definiowany w trzech pierwszych warstwach modelu OSI. Poziom warstwy fizycznej określa charakterystyki mechaniczne, elektryczne do aktywacji, utrzymania i likwidacji łączy fizycznych między DTE i DCE. Zasadniczym elementem warstwy fizycznej protokołu X.25 są styki fizycznego kontaktu z medium transportowym według zaleceń : X.21. Poziom łącza danych wykorzystuje protokół LAP-B (Link Access Procedure-Balanced). Poziom ten definiuje pojęcie ramki. Ramki są numerowane w sposób standardowy (modulo 8) i rozszerzony (modulo 128) oraz mają określone typy: informacyjne, zarządzające, nie numerowane. Poziom pakietowy to protokół PLP (Packet Level Protocol) zajmuje się zestawianiem połączeń (według określonej trasy – virtualizacja połączeń), fragmentacją na ramki (16,32,...2048,4096 bajtów).

3.4 Sieci FrameRelay

Technologia FrameRelay od początku miała być technologią przejściową, lecz bardzo szybko, ze względu na większą szybkość w porównaniu do sieci X.25 oraz mniejsze koszty w stosunku do sieci ATM, została powszechnie zaakceptowana. W Polsce wykorzystywana jest przez większość operatorów dostarczających usługi tworzenia sieci korporacyjnych oraz dostępu do internetu. Przykładem może być sieć Polpak-T Telekomunikacji Polskiej.

Technologia wnosi niewielkie opóźnienia i zapewnia sprawiedliwy dostęp do medium (pasma przenoszenia) dla wszystkich użytkowników. Funkcjonuje tylko na łączach cyfrowych o dobrej jakości, odznaczających się niską stopą błędów. FrameRelay zapewnia komunikację o przepływności do 45Mb/s.

Jest to sieć przenosząca dane w postacie pakietowej o prostym mechanizmie korekcji błędów. FR wykrywa błędy nagłówka, formatu itp. Ramki takie są usuwane a ich skompletowaniem zajmują się stacje bazowe korzystając z procedur powtarzania części sesji,

gdyż ramki nie są numerowane. Dlatego bardzo ważna jest jakość łącza, gdyż na łączu o dużej liczbie błędów wydajność FR bardzo spada.

W ramach sieci FR funkcjonują dwa typy urządzeń: DTE (Data Terminal Equipment) jako urządzenie poza szkieletem sieci – najczęściej u klienta podłączonego do sieci FR np. w Polsce Polpak-T oraz urządzenia DCE (Data Circuit – terminating Equipment) – wykorzystywane do budowy szkieletu jako urządzenia międzysieciowe zajmujące się przełączaniem ramek. Sieć zapewnia dwukierunkową komunikację połączeniową każdej parze urządzeń dostępowych DTE. Ścieżka łącząca dwa takie urządzenia może przebiegać przez kilka węzłów DCE połączonych kanałami fizycznymi. Taka wirtualna ścieżka może być ustalana na stałe – PVC (Permanent Virtual Circuits) bądź tworzona dynamicznie – SVC (Switched Virtual Circuits). Każda ścieżka przechodzi od urządzenia DTE przez kolejne urządzenia DCE aż do końcowego DTE. Każde połączenie dwóch urządzeń oznaczone jest w sieci specjalnym numerem DLCI. Na tej podstawie urządzenia DCE wiedzą gdzie przełączać pakiety tak, żeby dotarły do końcowego DTE.

Do samego protokołu FR wprowadzono protokół LMI (Local Management Interface) przyczyniający się do poszerzenia funkcjonalności sieci FR. LMI wnosi do FR adresowanie globalne i połączenia grupowe (multicasting). Dzięki adresowaniu globalnemu cała sieć FR przeobraża się w switchowaną LAN. Połączenia grupowe wpływają na lepsze wykorzystanie pasma w przypadkach równoczesnej transmisji do wielu stacji.

Operator dostarczający dostęp do sieci FR posiada w ramach protokołu pewne mechanizmy sterowania parametrami transmisji umożliwiające dostarczanie różnej jakości usługi. Najważniejszymi parametrami transmisji są EIR (Excess Information Rate) oraz CIR (Committed Information Rate). EIR to nie gwarantowana przepływność maksymalna, której nie wolno przekroczyć zaś CIR to gwarantowana przepływność minimalna.

Podstawą nowoczesnej sieci jest wprowadzanie usług QoS (Quality of Service) i CoS (Class of Service), usługi te opierają się na zdefiniowaniu pewnych poziomów gwarantowanej jakości transmisji danych. Wprowadzono trzy klasy (poziomy) jakości:

- Real Time Variable Frame Rate – ustalone pasmo, niewielkie opóźnienia i niskie straty ramek. Klasa dla transferu danych wrażliwych na opóźnienie i zdekompletowanie, np. głos.
- Non-Real Time Variable Frame Rate – ustalone pasmo, umiarkowane opóźnienia i małe straty ramek. Klasa odpowiednia dla ruchu LAN-LAN i usług dostępu Internet-Intranet w biznesie.
- Available/Unspecified Frame Rate – zmienna przepływność i w miarę sprawiedliwy dostęp do pasma. Klasa odpowiednia dla transferów plików, poczty elektronicznej i usług dostępu internetowego.

3.5 Sieci ATM

Technologia ATM (Asynchronous Transfer Mode) powstała jako kompromis pomiędzy dwoma technikami przesyłania danych w sieciach: STM (Synchronous Transfer Mode) – np. sieci ISDN oraz PTM (Packet Transfer Mode) – stosowaną w sieciach lokalnych. ATM stosowany jest do budowy szkieletów dużych sieci rozległych.

Sieć ATM w standardzie nie definiowała medium transmisyjnego więc może być stosowana w różnych środowiskach, zarówno WAN (FrameRelay) jak i LAN (Ethernet, FDDI). Do tej pory są na raize następujące klasy przepływności: 25Mb/s, 100Mb/s, 155,52Mb/s (najczęściej) oraz 622Mb/s i 2,5Gb/s. Poszczególne ramki danych maja wielkość 53 bajty (48 bajtów danych). Dzięki bardzo szybkim przełącznikom komórek i połączeń obsługa transmisji może być stosowana do transmisji głosu, obrazu. ATM bardzo efektywnie potrafi zarządzać dostępnymi łączami opartymi o dowolne medium. Przekaz jest w trybie połączeniowym co oznacza że przed wysłaniem informacji występuje faza zestawienia łącza – według parametrów deklarowanych przez abonenta (typ przesyłanych danych). W sieci ATM wprowadzono wirtualizację połączeń opierającą się na tym, że dla połączenia definiowana jest wirtualny kanał (Virtual Channel) który idzie po wirtualnej ścieżce (Virtual Path). Takie zdefiniowanie umożliwia np. przy zmianie trasy przesyłu danych – zmianie wirtualnej ścieżki automatyczną zmianę wszystkich przyporządkowanych kanałów wirtualnych. Sieć ATM zapewnia pewną przeźroczystość a więc może być swobodnie wykorzystywana z różnymi protokołami komunikacyjnymi i do realizacji różnych usług.

Organizacja ATM Forum (zajmująca się standaryzacją technologii ATM) w 1995 opracowała standard PNNI (Private Network to Network Interface) definiujący szczegółowo współpracę przełączników ATM wraz z możliwością „uczenia się" topologii sieci, w której są instalowane. Przekaz i wzajemne pamiętanie w przełącznikach dodatkowych informacji o stanie i parametrach poszczególnych łączy (szerokość pasma, poziom QoS, opóźnienia przekazu) obniża ruch w sieci.

Technologia ATM w odniesieniu do modelu sieci OSI definiuje trzy początkowe warstwy:

- warstwa fizyczna (ATM Physical layer) – funkcje dostępu do medium transmisyjnego, bez definiowania konkretnego medium transmisyjnego
- warstwa ATM (ATM Layer) – właściwe protokoły transmisji pakietów (komórek) i definicje routingu dla kanałów wirtualnych, bez względu na typ realizowanej usługi. W tej warstwie działają wszelkie przełączniki ATM zajmujące się kierowaniem ruchu.

- warstwa adaptacyjna AAL (ATM Adaptation Layer) – funkcje dla usług związanych z segmentacją i składaniem jednostek transmisyjnych między wyższymi warstwami a warstwą ATM.

ATM z definicji obsługuje transmisje zgodnie z QoS (Quality of Service). Umożliwia to zdefiniowanie z góry określonej jakości usługi i tak można zdefiniować kilka klas jakości (CoS – Class of Service). Ze względu na usługi ATM definiuje klasy A,B,C,D zaś jeśli chodzi o przepustowość to zdefiniowane są następujące poziomy:

- CBR (Constant Bit Rate) – usługi o stałym zapotrzebowaniu na pasmo (np. głos bez kompresji i mechanizmów wykrywania ciszy)
- VBR (Variable Bit Rate) – usługi, którym wystarcza zmienna przepływność (np. transakcje bankowe, sygnalizacja w systemie nadzoru)
- ABR (Available Bit Rate) – przekaz danych bez istotnych wymagań czasowych, ale z gwarancja pewnego minimalnego poziomu (np. aplikacje poczty elektronicznej, transfer zbiorów, dostep do internetu)
- UBR (Unspecified Bit Rate) – bez jakichkolwiek gwarancji jakościowych

Routing w sieciach ATM może być rozwiązany na kilka sposobów: routing centralny, rozproszony oraz mieszany (przełączniki z protokołem MPOA).

Najstarszy jest routing centralny z dużym centralnym routerem. Rozwiązanie to nie nadaje się do dużych sieci ATM.

Powiązanie protokołem OSPF (Open Shortest Path First) kilku równolegle działających routerów centralnych, rozmieszczonych w różnych punktach sieci pozwala na zwiększenie niezawodności i wzrost ich wydajności. Brak jednak wiedzy o topologii sieci może doprowadzić do sytuacji, że dane będę przesyłane okrężnymi trasami.

W routingu rozproszonym wszystkie urządzenia dostępowe są jednocześnie przełącznikami warstwy 2 oraz routerami warstwy 3. Do wyboru najlepszego routera wykorzystywany jest protokół OSPF stosowany w TCP/IP. Poważną wadą takiego rozwiązania jest wysoki koszt urządzeń oraz problemy z bezpieczeństwem.

Współczesna odmiana routingu rozproszonego to protokół MPOA (Multi-Protocol Over ATM) mający zalety routingu centralnego a pozbawiony jego wad. Wybrane nieliczne routery lecz technicznie bardzo zaawansowane zajmują się trasowaniem. Przy dużym ruchu routery te przerzucają ruch na szybkie przełączniki wybierając najszybsze alternatywne trasy. Po pewnym czasie przełączniki zapominają trasy i znów wszystko wraca na ruch przez wybrane główne routery.

Bardzo cenną funkcją sieci ATM jest emulacja sieci lokalnej przez łącze ATM. Standard LANE (LAN Emulation) gwarantuje normalny ruch standardowymi technologiami sieci lokalnych takich jak np. Ethernet, Token Ring i stosowanie protokołów wykorzystywanych w sieciach lokalnych takich jak np. TCP/IP, Apple Talk i innych.

4 Protokoły komunikacyjne

4.1 NetBIOS, NetBEUI

Protokół ten jest wykorzystywany przez jeden z najpopularniejszy system sieciowy stosowany na końcówkach sieci – Windows 95/98/NT. Protokół ten wykorzystywany jest również w sieciach Peer-to-Peer takich jak Lantastic. Protokół ten działa na poziomie warstwy trzeciej i wyższych. Wprowadza więc pojęcie adresu logicznego. Adres logiczny składa się z opisu tekstowego, który najczęściej wiąże się z opisem komputera w sieci, np. JACEK – komputer przy którym pracuje osoba o takim imieniu lub KSIEG1 – komputer numer 1 znajdujących się w księgowości. Adres logiczny może być dowolny i jest nadawany przez administratora (osobę konfigurującą stację roboczą). W całej sieci nie mogą istnieć dwa komputery o takiej samej nazwie (adresie).

Ponieważ w adresie komputera nie ma żadnego wyróżnika sieci/podsieci adresy takie mogą dotyczyć tylko jednego segmentu sieci. Protokół ten nie jest rutowalny – nie da się tak skonfigurować routera (Patrz rozdział 5.5 na stronie 24) aby potrafił przenosić pakiety protokołu NETBIOS. Jest to bardzo istotny powód, dyskwalifikujący stosowanie rozwiązań opartych na tym protokole w sieciach rozległych.

4.2 Protokół IPX/SPX

Protokół ten jest wykorzystywany i bardzo mocno spopularyzowany przez producenta Novell, który zaimplementował ten protokół w systemach Netware do wersji 4. Od wersji 5 stosowany jest już protokół TCP/IP. Protokół IPX działający na poziomie warstwy 3 oraz SPX na poziomie warstwy 4 umożliwiają bardzo szybką i efektywną transmisję danych w sieci (o wiele lepszą niż np. NetBIOS). Adres logiczny w IPX składa się z adresu numerycznego sieci/podsieci znaku ‘:’ oraz adresu numerycznego komputera w ramach tej sieci/podsieci. Protokół ten jest w pełni rutowalny – można go stosować do budowy sieci o większych rozmiarach.

4.3 Protokół IP

Każda stacja - końcówka internetu, serwer czy router musi posiadać swój własny unikalny adres logiczny IP w internecie. Przydział oczywiście nie jest przypadkowy i każdy kto

się podłącza do internetu od swojego provider'a dostaje określoną pule adresów IP do wykorzystania dla własnej sieci bądź tylko serwera, który podłącza do internetu.
Stacje robocze mogą mieć adres wraz z wszystkimi parametrami ustawione samodzielnie, bądź parametry te mogą być ustawiane z serwera sieci lokalnej.
Wraz z adresem IP musza być ustawione dodatkowe parametry potrzebne do pełnego działania protokołu TCP/IP.

Wszystkie adresy IP podzielone są na podsieci w celu łatwiejszego kierowania (routowania) pakietów danych w sieci. Otóż łatwiej ustawić kierunkowskaz na całe miasto niż na każdego jego mieszkańcaz osobna. Taką określoną podsieć specyfikuje tzw. maska sieciowa (netmask) która składa się binarnie z określonej liczby jedynek i potem zer np. 255.255.255.128 co binarnie oznacza: 11111111.11111111.11111111.10000000. Zapis taki umożliwia przy pomocy prostych funkcji logicznych (AND) wyznaczyć z określonego adresu IP adres sieci do jakiego dany adres IP należy.
I tak np. dla adresu 192.168.1.77 przy masce sieciowej 255.255.255.192 łatwo można wyliczyć, że ten adres należy do podsieci o adresie: 192.168.1.64. Na podstawie tych masek sieciowych definiuje się tzw. routing (patrz rozdział 4.6 na stronie 20) - czyli tabele reguł kierowania pakietami w węźle (routerze).
Każdy komputer wykorzystujący TCP/IP przechowuje również informację o serwerach DNS w postaci ich adresów IP. Serwery DNS zajmują się tłumaczeniem nazw komputerów w postaci domenowej (zapis tekstowy) np. www.wsi.edu.pl na konkretne adresy IP.

4.4 Zamiana adresu IP na adres MAC – ARP/RARP

Paczka przesyłana pomiędzy dwoma adresami logicznymi IP tylko w sieci lokalnej. ARP zamienia adres IP na MAC adres – wysyła broadcast MAC pytając się: „Kto ma dany adres logiczny IP" – zwraca wynik – adres fizyczny MAC. Każde urządzenie sieciowe ma wewnętrzny cache ARP po to, żeby nie pytać się za każdym razem o adresy MAC. Cache ARP jest automatycznie po pewnym czasie czyszczony żeby umożliwiać ewentualne zmiany adresacji logicznej sieci.

4.5 Protokół ICMP

Wykorzystywany w celach testowych do sprawdzania sieci IP. Każda stacja obsługująca protokół IP musi odpowiadać na pakiety ICMP. Najczęściej wykorzystywany przez aplikacje *ping* sprawdzająca czy dany adres IP „żyje" – tzn. czy istnieje normalna nieprzerwana trasa

przesyłania do danego adresu w sieci. Dane zwracana przy okazji to czas przesyłania danych pomiędzy adresami oraz stopa błędów.

```
H:\Marcin>ping -n 10 -w 2000 192.168.33.241

Badanie 192.168.33.241 z użyciem 32 bajtów danych:

Odpowiedź z 192.168.33.241: bajtów=32 czas=20ms TTL=124
Odpowiedź z 192.168.33.241: bajtów=32 czas=10ms TTL=124
Odpowiedź z 192.168.33.241: bajtów=32 czas=10ms TTL=124
Odpowiedź z 192.168.33.241: bajtów=32 czas=10ms TTL=124
Odpowiedź z 192.168.33.241: bajtów=32 czas=10ms TTL=124
```

Protokół wykorzystuje się również w celach sprawdzania trasy przesyłu danych i ewentualnych spowolnień na określonych odcinkach.

```
[marcin@dino marcin]$ traceroute 207.46.131.13
traceroute to 207.46.131.13 (207.46.131.13), 30 hops max, 40 byte packets
 1  rtr (195.117.114.131)  2.156 ms  2.112 ms  2.055 ms
 2  rtr.w.tpsa.pl (194.204.144.77)  6.447 ms  3.650 ms  3.676 ms
 3  do-katwct.r1.tpnet.pl (194.204.128.49)  9.853 ms  13.155 ms  9.995 ms
 4  bb4.NewYork.Teleglobe.net (207.45.199.137)  103.835 ms * *
 5  core1.NewYork.Teleglobe.net (207.45.223.158)  108.444 ms  108.579 ms  105.615 ms
 6  core1.PaloAlto.Teleglobe.net (207.45.222.177)  173.414 ms  177.650 ms  172.612 ms
 7  core1.Seattle.Teleglobe.net (207.45.222.13)  187.326 ms  189.909 ms  191.064 ms
 8  bb1.Seattle.Teleglobe.net (207.45.222.34)  190.511 ms  248.060 ms  281.755 ms
 9  Teleglobe.net (207.45.213.254)  191.701 ms  195.641 ms *
10  * 207.46.190.97 (207.46.190.97)  204.573 ms  194.885 ms
11  icpmscomc7501-a0-00-1.cp.msft.net (207.46.129.3)  193.220 ms *  192.663 ms
12  icpmscomc7501-a0-00-1.cp.msft.net (207.46.129.3)  194.977 ms  192.958 ms  191.799 ms
...
```

4.6 Routing - trasowanie

Kierowanie ruchu w sieci musi być robione na podstawie ściśle określonych reguł. Reguły te zapisane są w tzw. tabelach routingu, które musi mieć każdy węzeł sieci - router.

Tablica routingu składa się z zapisów typu: jeśli adresy z sieci o adresie: 192.168.1.64 z netmaską 255.255.255.192 to kieruj je na adres 192.168.3.3 (do którego musi być zdefiniowana oddzielna informacja o trasie). Podstawowe podsieci są związane z konkretnymi urządzeniami (np. kartami sieciowymi) i dla nich nie ma adresu następnego węzła (tzw. gateway'a - bramy) - lub jest on równy adresowi samego urządzenia. Domyślna trasa to 0.0.0.0. Oznacza ona kierunek, gdzie mają być przesyłane wszelkie pakiety, które nie pasują do żadnych innych zapisów.

```
H:\Marcin>route print
===========================================================================
Lista interfejsów
0x1 ........................... MS TCP Loopback interface
0x2 ...00 c0 4f 89 10 f2 ...... 3Com 3C90x Ethernet Adapter
===========================================================================
===========================================================================
Trasy aktywne:
Cel sieci             Maska sieci             Brama       Interfejs Metryka
          0.0.0.0          0.0.0.0   192.168.65.254   192.168.65.24       1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
```

```
     192.168.65.0    255.255.255.0    192.168.65.24   192.168.65.24       1
    192.168.65.24  255.255.255.255        127.0.0.1       127.0.0.1       1
   192.168.65.255  255.255.255.255    192.168.65.24   192.168.65.24       1
        224.0.0.0        224.0.0.0    192.168.65.24   192.168.65.24       1
  255.255.255.255  255.255.255.255    192.168.65.24   192.168.65.24       1
===========================================================================
```

Miary trasowania (metryki) określają którą trasę wybrać jeśli są jakieś alternatywne. Traktowane jest to jak koszt. Czyli w każdym węźle jeśli istnieją dwie możliwości przesłania to wybierana jest ta tańsza, czyli z mniejszą miarą trasowania.

4.7 Typy algorytmów routowania

Statyczne – wymagają od administratora sieci wpisywania zawartości tabel trasowania – wynikających ze znanej topologii sieci. Dla sieci o prostej strukturze. Sieci oparte o statyczny routing nie mogą reagować na zmiany.
Dynamiczne – routery samodzielnie uczą się topologii sieci. Istnieją całe rodziny protokołów do tego celu np. RIP, OSPF.
W przypadku protokołu RIP, który jest bardzo popularny w zastosowaniach internetu, routery żądają od innych routerów aktualnych informacji o trasach routowania, odpowiadają na analogiczne żądania innych routerów. W ten sposób przekazywana jest informacja o tabeli routingu dla poszczególnych sieci.

4.8 Wybór protokołów i trasowanie

Protokoły nietrasowalne (np. NetBIOS) gdzie adres komputera w sieci to nazwa definiowana przez użytkownika. Poszukiwanie komputera o konkretnej nazwie w sieci lokalnej odbywa się przez skomplikowany broadcast. Protokół ten stosowany jest w sieciach Windows i nie ma możliwości zastosowania go w sieci rozległej, gdzie musi istnieć zaawansowany routing.
Protokoły trasowalne np. IP gdzie adres komputera jest w postaci numerycznej i jest tak skonstruowany, że da się wydzielić z niego adres sieci i adres komputera w tej sieci. Trasowanie jest wtedy dość łatwe.

W przypadku sieci Windows stosuje się często oba protokoły np. NetBIOS dla celów sieci lokalnej i IP dla łączenie z siecią rozległą. Często stosuje się usługę WINS (w sieciach Windows) zamieniającą adres NetBIOS na adres IP – nie ma potrzeby wtedy przesyłania dużo paczek broadcast co znacznie zwiększa szybkość pracy sieci.

4.9 Protokół TCP i UDP

Protokoły TCP oraz UDP działają na poziomie warstwy czwartej i nie zajmują się funkcjami takimi jak routing. Te dwa protokoły są bardzo podobne w swych założeniach. UDP jest wersją znacznie prostszą i zazwyczaj stosowana jest w zastosowaniach sieci lokalnych, gdzie zakłada się wysoką gwarancję dostarczania pakietów, ponieważ sam protokół nie ma wbudowanych takich mechanizmów. W nagłówku protokołu UDP występują tylko dwie istotne informację – port nadawcy i port odbiorcy. Pojęcie portu na określonym komputerze o adresie IP wprowadzono po to, aby istniała możliwość przesyłania danych do określonych serwisów zajmujących się określonymi funkcjami. I tak równocześnie serwer może pełnić funkcję serwera WWW (protokół http) odbierając pakiety wysyłane na port o adresie 80 oraz funkcję serwera FTP odbierając pakiety wysyłane na port o adresie 21. Mechanizm ten również działa na stacji klienckiej, umożliwiając niezależny transfer różnych aplikacji z tego samego adresu IP, np. dwa okna przeglądarki WWW posiadające przydzielone dynamicznie dwa osobne porty odczytują z tego samego serwera WWW (ten sam adres IP oraz port docelowy) dane, które trafiają do każdego okna osobno.

Protokół TCP działa identycznie jak UDP. Wprowadza tylko kilka dodatkowych mechanizmów takich jak np. kompletowanie transmisji danych i powtarzanie zgubionych danych. Bardzo często wykorzystywany jest do transmisji danych na większych odległościach, gdzie bardzo często istnieją bardzo duże przekłamania i część transmisji może być zagubiona.

5 Sprzęt sieciowy

5.1 Regenerator – Repeater

Urządzenie które wzmacnia sygnał. Działa na poziomie warstwy 1 modelu OSI. Posiada 2 porty – Repeater zwiększa zasięg sieci – przedłuża długość segmentu.

5.2 Koncentrator – Hub

Urządzenie służące do łączenia wielu komputerów. Wzmacnia sygnał. Działa na poziomie warstwy 1. Hub posiada wiele portów. Do portu może być podłączony następny hub (przez port uplink - normalne kable są proste, skrzyżowanie jest w hubie – w przypadku dwóch hubów: 1 musi być bez skrzyżowania – port uplink)

Można wyróżnić:

Huby pasywne: transmitują pojawiający się sygnał z dowolnego portu na wszystkie pozostałe. Jedna domena kolizyjna.

Huby przełączające: wbudowane mechanizmy analizy ramek z warstwy 2 (tak jak przełączniki). Kilka domen kolizyjnych.

Ze względu na konstrukcję hubów: *wolno stojące, wieżowe, modularne*

5.3 Most – Bridge

Działa na poziomie warstwy 2. Analizuje ramki danych i na podstawie adresu fizycznego kieruje je do odpowiedniej gałęzi sieci. Zazwyczaj ma 2 porty.

5.4 Przełącznik – Switch

Urządzenie służące do łączenia komputerów, hubów lub kolejnych switch'y. Wiele portów. Każdy port to niezależna domena kolizyjna. Działa na poziomie warstwy 2 modelu OSI. Przełącznik zapamiętuje i tworzy tabelę adresów fizycznych (MAC Address) komputerów pojawiających się na poszczególnych portach. Analizuje poszczególne ramki i odpowiednio według adresu fizycznego odbiorcy przesyła ramkę do odpowiedniego portu. Switch'e mogą być zarządzane (protokół SNMP lub przez WWW)

5.5 Router

Urządzenie działające na poziomie warstwy 3 modelu OSI. Analizuje pakiety danych i na podstawie adresu logicznego kieruje do odpowiedniej gałęzi sieci. Zazwyczaj nie posiada wiele portów (np. 2 porty sieci lokalnej i 1 sieci rozległej). Zazwyczaj posiada porty o różnej prędkości. Umożliwia translację protokołów. Musi być wyposażony w odpowiednie oprogramowanie, które obsługuje konkretny protokół warstwy 3 (np. IPX, IP). Router musi być skonfigurowany co jest dość skomplikowane.

6 Sieci typu Peer-To-Peer

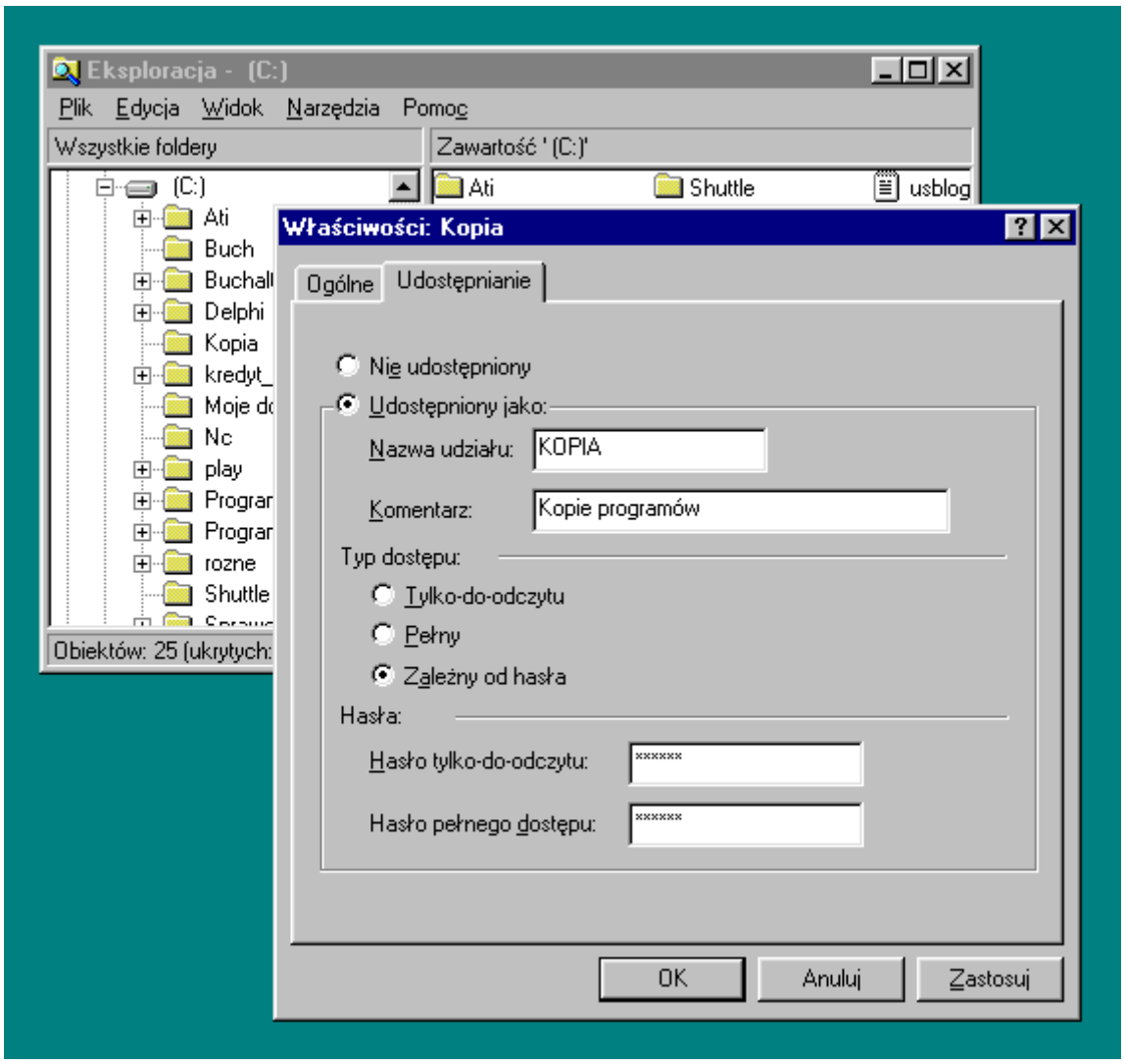
6.1 Lantastic

Sieć Lantastic jest najprostszym lecz bardzo dobrze się sprawującym rozwiązaniem, który można pokazać jako sieć typu Peer-To-Peer. W wersji pod DOS oprogramowanie działa jako programy TSR instalowane w pamięci. Jeśli stacja pełni funkcję klienta sieci – tzn. nic w sieci nie udostępnia to oczywiście nie będzie uruchamiać programu serwera niepotrzebnie zajmując drogocenną pamięć w trybie MSDOS. udostępniane mogą być zarówno całe dyski jak i porty - również szeregowe – co daje możliwość udostępnienie np. modemu przez sieć. Wykorzystywany jest protokół NETBIOS i adresy logiczne komputerów w sieci są wykorzystywane do prostego systemu praw.

Lantastic istnieje również w wersji dla Windows, lecz jego popularność w tej wersji jest bardzo niewielka, ze względu na wbudowany automatyczny system sieci w Windows. Istnieje wiele rozwiązań gwarantujących działanie sieci Peer-to-Peer lecz tylko wersje pod DOS się przyjęły. W dobie dzisiejszych komputerów, gdzie zazwyczaj jest Windows 95/98 nie ma potrzeby korzystania z żadnych dodatkowych mechanizmów sieci Peer-To-Peer.

6.2 Microsoft Network

Sieć Microsoft Network to sieć komputerów opartych o systemy operacyjne MS Windows 3.11/95/98/NT. Obsługa tych systemów jest bardzo podobna i z wyłączeniem Windows NT systemy te tworzyć mogą typową sieć Peer-To-Peer czyli komputerów pracujących niezależnie a jedynie mających możliwość komunikacji między sobą. Każdy komputer może udostępniać pewne zasoby takie jak folder czy drukarka z określonymi prostymi uprawnieniami szeregowanymi jedynie przez hasło, na zasadzie, że jeśli ktoś zna publiczne hasło do modyfikacji to może automatycznie zapisywać do udostępnionego zasobu (patrz Rys. 2)



Rys. 2 Udostępnianie zasobów w sieci Microsoft Network

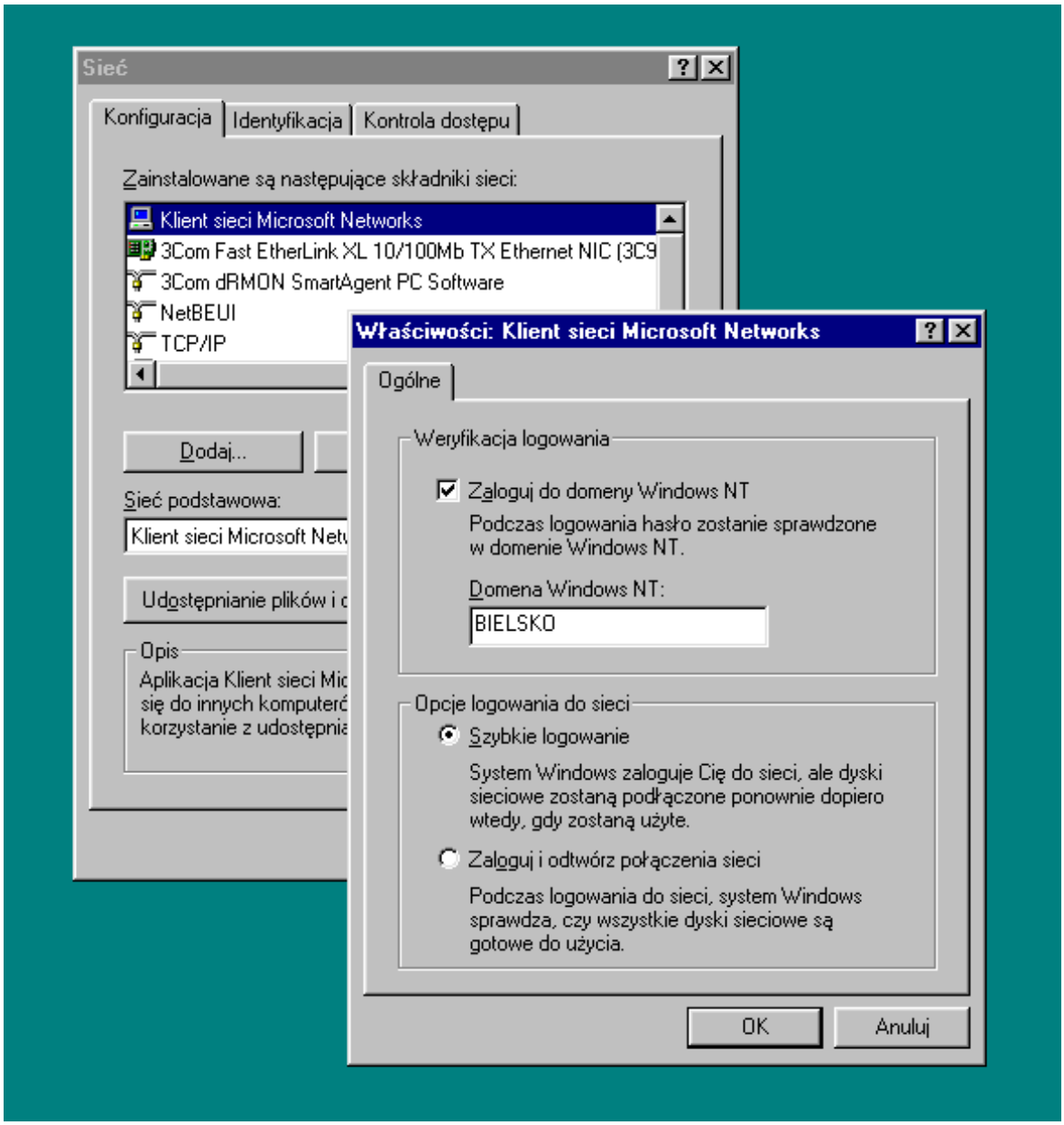
7 Sieci oparte o Windows NT/2000

7.1 Domeny użytkowników

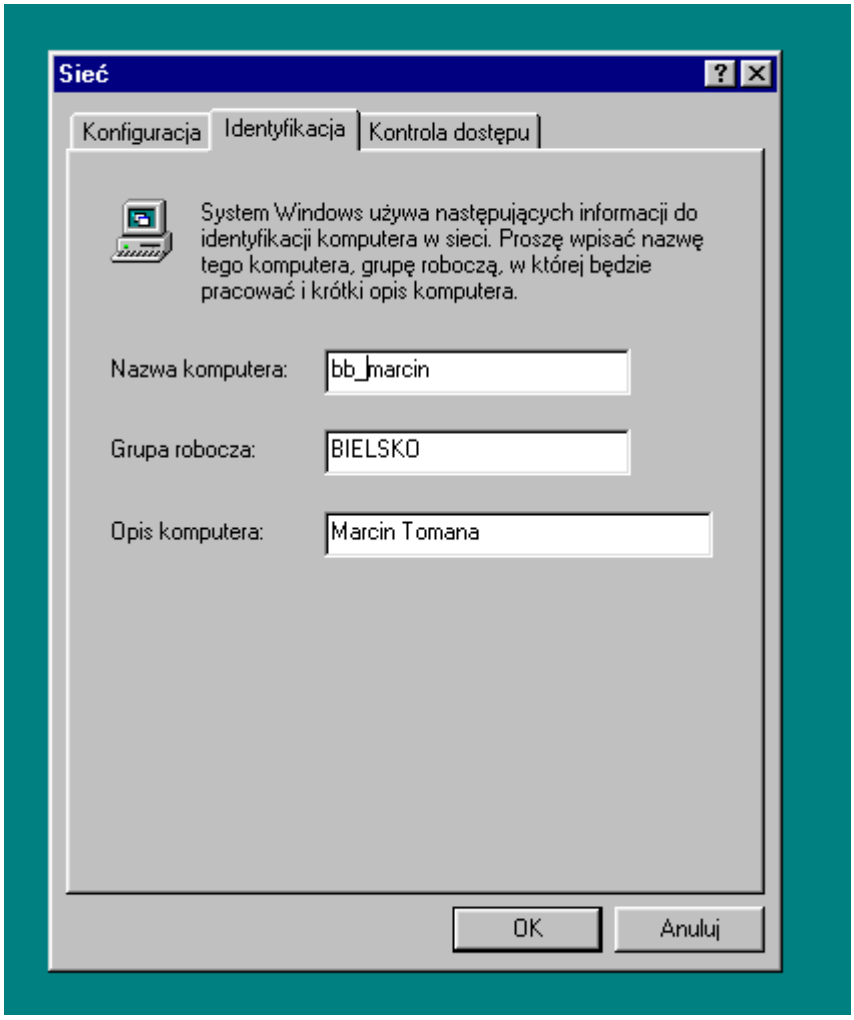
Systemy operacyjne Windows 95/98 mają wbudowaną automatyczną współpracę z serwerami Windows NT. Sieć Microsoft Network wprowadza pojęcie otwartej grupy roboczej do której każdy może się dołączyć oraz pojęcie Domeny użytkowników dla której informacje są przechowywane na serwerze Windows NT i nie ma wolnego dostępu do niej. Informacje te są chronione i używane są specjalne systemy zabezpieczeń poufności tych danych. Domena zawiera listę użytkowników wraz z prawami w całej sieci (zasobach domeny). Nie da się zalogować do domeny nie znając użytkownika wraz z hasłem w domenie. Nowych użytkowników może dopisywać tylko użytkownik posiadający prawo administratora sieci. Użytkownicy pogrupowani są w grupy którym mogą również być nadawane uprawnienia.

7.2 Współpraca z Windows 95/98

Komputer z systemem Windows 95/98 może należeć do domeny Windows NT - musi być ona ustawiona jako grupa robocza komputera w identyfikacji komputera dla sieci MS Network (patrz Rys. 4) oraz musi być ustawione logowanie się do tej domeny (patrz Rys. 3) - będzie trzeba wtedy podać uzytkownika i hasło z domeny - inaczej nie będzie możliwe zalogowanie się do domeny.

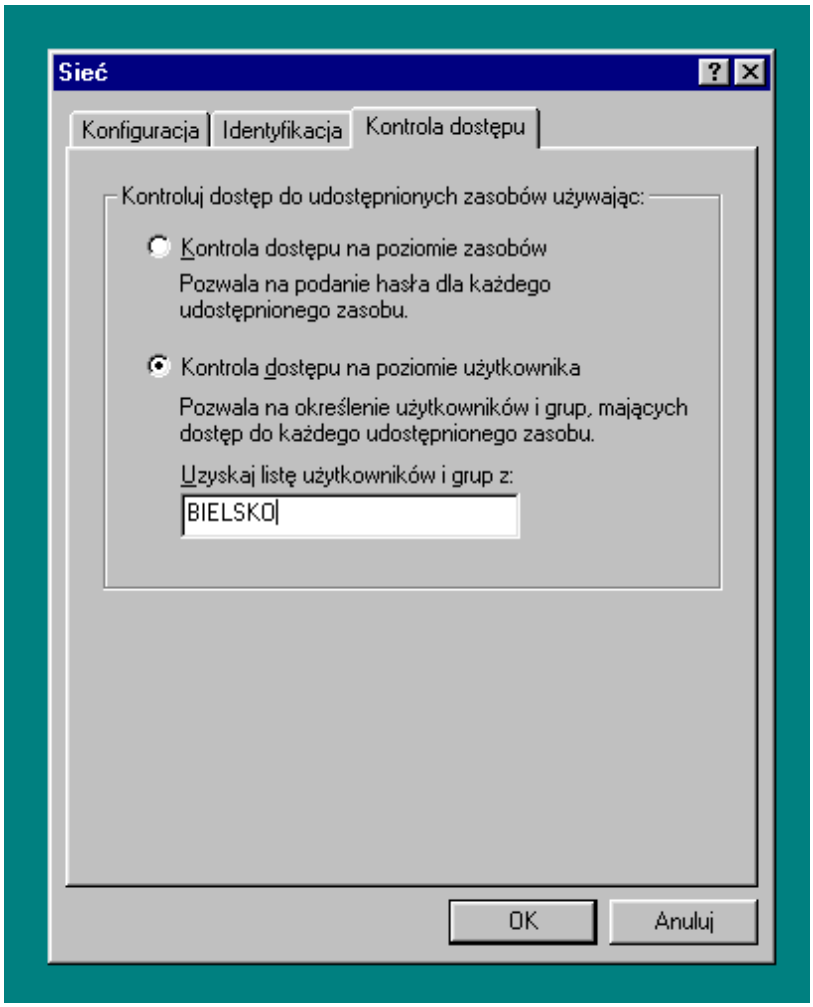


Rys. 3 Ustawianie logowania się do domeny w Windows 95



Rys. 4 Ustawianie grupy roboczej w Windows 95/98

Windows 95/98 potrafi udostępniać zasoby w ramach sieci Microsoft Network. W przypadku sieci gdzie nie korzysta się z Windows NT i domeny nie istnieje zaawansowany system praw. Udostępniany zasób może być udostępniony standardowo na tej zasadzie jedynie, że jeśli ktoś zna hasło do zapisu to może modyfikować zasób a jeśli ktoś zna hasło do odczytu to może tylko czytać. Jeśli ktoś nie zna żadnych haseł to nie będzie mógł z niczego korzystać. Problem jest w zbyt słabym systemie zabezpieczeń i w zbyt małych możliwościach dysponowania zasobami. Jedno hasło dla wszystkich to zdecydowanie za mało jak na rozwinięty system sieciowy. Dlatego dopiero zastosowanie Windows NT i domeny w sieci z komputerami Windows 95/98 daje odpowiednie możliwości. Wystarczy we właściwościach sieci ustawić, że kontrola dostępu jest na poziomie użytkownika i podać domene, z której ma pobierać użytkowników i hasła. Od tego momentu zasoby udostępniane są podstawie listy użytkowników i szczegółowych praw dla użytkowników domeny.



Rys. 5 Ustawianie kontroli dostępu do udostępnionych zasobów

8 Sieć Novell Netware

8.1 Usługi katalogowe bindery i NDS.

Usługi katalogowe w systemie sieciowym Novell Netware mogą opierać się na dwóch metodach dostępu do baz danych informacji o użytkownikach. Pierwsza, starsza, stosowana jeszcze w wersjach 2.20 i 3.12 i polega na tzw. bazie BINDERY, do której dostęp ma tylko serwer i w której zapisane są informacje o użytkownikach i ich hasłach. Baza ta zawiera jedną listę użytkowników i nie może być dwóch obiektów (użytkowników) w niej o takiej samej nazwie. Każdy serwer przechowuje swoją własną bazę BINDERY i udostępnia swoje zasoby tylko użytkownikom z tej listy. Prawa do plików serwera również są nadawane i udostępniane tylko i wyłącznie wg użytkowników i grup z tej lokalnej bazy.

Od wersji Netware 4.0 wprowadzono ideologicznie całkowicie nowe rozwiązanie (NDS – Netware Directory Services) opierające się na rozproszonej bazie danych informacji o wszelkich obiektach (zasobach) całej sieci rozmieszczonej na wielu serwerach. Operacja identyfikacji przeprowadzana jest tylko i wyłącznie raz i posiada się dostęp do całej struktury w której znajdować się może kilka tysięcy serwerów. Prawa do samych obiektów jak i plików nadaje się obiektom z całej struktury i funkcjonują one na wszystkich serwerach w strukturze NDS.

8.2 Oprogramowanie serwera

Serwer ma swoje własne firmowe oprogramowanie systemowe. jest ono wykorzystywane typowo do celów zarządzania serwerem i nie da się na nim uruchamiać typowych programów. Wykonywane programy muszą być skompilowane tylko i wyłącznie dla platformy Netware. Programy te maja rozszerzenie NLM (Netware Loadable Module). Serwer potrafi odczytywac tylko pamięć dyskową na której założona jest partycja Novell i system plików zgodny z Novell. Cała przestrzeń dyskowa jest podzielona na tzw. wolumeny, które są podstawową jednostką udostępnianą w sieci. Wolumen ma normalną strukturę katalogową z plikami. Cała tablica alokacji plików - FAT (File Alocation Table) jest przechowywany w pamięci serwera, dlatego istotne jest, aby przy dużych dyskach lub małych sektorach serwer posiadał dużo pamięci RAM. Nazwy plików mogą być kompatybilne z innymi systemami operacyjnymi, np. OS/2, Windows - należy tylko wgrać odpowiedni moduł nazw (NAME SPACE). W celu zwiększenia miejsca na dyskach od wersji 4 wprowadzono kilka ciekawych mechanizmów wbudowanych w system plików serwera:

- kompresja - bardzo często stosowany mechanizm w wielu systemach operacyjnych. W Novell jest to bardzo zaawansowana technologia, która spowalnia serwer kompresując pliki tylko w momentach przestoju. Używane są mechanizmy dające kod o bardzo wysokim współczynniku szybkości rozkompresowywania.
- subalokacja - dzielenia pojedyńczych sektorów na mniejsze. Przy dużych dyskach wielkość jednego sektora może nawet dochodzić do 32kB, więc normalnie każdy plik zajmuje min. 1 sektor, a zawsze pełną ich liczbę. Subalokacja umożliwia wykorzystanie tych niezapełnionych sektorów.
- migracja - możliwość automatycznego przenoszenia plików z dysków na pamięci większe, tańsze lecz z wolniejszym czasem dostępu np. dyski magnetooptyczne. Użytkownik widzi normalnie plik w swoim katalogu ale jeśli go nie używał długo to serwer przenosi go na inny nośnik i w katalogu na pliku zostaje tylko flaga.

Standardowe oprogramowanie NLM zawiera takie programy jak np. serwer drukowania (Print Server), który obsługuje kolejki drukowania i wszystkie drukarki, które mogą być podłączone bezpośrednio do niego lub zdalnie do jakiegoś klienta w sieci z uruchomionym programem TSR - RPRINT.EXE

8.3 Netware SFT (System Fault Tolerancy)

Novel wprowadził w systemie Netware 3 poziomy bezpieczeństwa na których może znajdować się system.

- Level I - Standardowo na wolumenach takie rzeczy jak: nadmiarowe katalogu, kopia FAT'u, obszar HotFix na uszkodzone sektory, testowanie spójności wolumenu przy starcie.
- Level II - Zakłada się że jest już UPS monitoring. Wolumeny są na dysku sprzętowo chronionym czyli np. mirroring, duplexing, RAID 5. Na bazach danych (plikach) uruchomiony TTS (Transaction Tracking System) - system transakcji.
- Level III - duplikacja całych serwerów. Specjalne oprogramowanie Netware SFT III instalowane na dwóch niezależnych maszynach. Oprogramowanie bardzo drogie, bo samo rozwiązanie jest aktualnie najbardziej bezpieczne. (Patrz również rozdział 10.2 na stronie 39)

8.4 Oprogramowanie klienckie

Klientem sieci Netware może być dowolny komputer, który ma zainstalowane oprogramowanie klienta sieci Netware. Oprogramowanie to może być dystrybuowane zarówno przez producenta samego systemu operacyjnego jak i samego Novel'a.

W przypadku systemu DOS sytuacja jest dość prosta, gdyż od dłuższego czasu ustandaryzowana jest obsługa kart sieciowych różnych producentów. Każda karta sieciowa posiada w swoich sterownikach tzw. sterownik ODI. Sterownik ten może być wykorzystywany do wielu zastosowań - nie tylko Netware. Zaletą sterowników ODI jest bardzo duża konfigurowalność tego rozwiązania. Wszystkie te sterowniki są programami rezydentnymi - TSR (Terminate and Stay Resident). Najpierw żeby sterowniki mogły się porozumieć musi być uruchomiana komunikacja ODI - program LSL.COM. Następnie uruchamia się odpowiedni sterownik karty sieciowej dostarczany na dyskietce ze sterownikami dla karty, np. dla karty sieciowej 3COM jest program 3C90X.COM. Konfiguracja karty sieciowej zapisywana jest w pliku NET.CFG. Następnie uruchamia się driver odpowiedzialny za wykorzystywany protokół. W przypadku Netware standardowo włącznie z wersją 4 jest to protokół IPX/SPX i program nazywa się IPXODI.COM. W tym momencie należy już tylko uruchomić odpowiedni program obsługi klienta Netware i może to być albo NETX.EXE w starszych wersjach lub VLM.EXE w nowszych. Programy te konfigurowane są przy pomocy pliku SHELL.CFG. Po tej operacji powinien pojawić się napęd dysków (następny za LASTDRIVE definiowany w CONFIG.SYS) przy pomocy którego możemy przeprowadzić proces logowania się do sieci.

Pod system DOS wprowadzono również wersję innego klienta. Wykorzystywane są wtedy sterowniki stosowane przez oprogramowanie NLM na serwerze. Wszystkie te programy działają w trybie procesora protected i alokują się w pamięci Extended. Jest to najlepsze rozwiązanie klienta Netware.

W systemie Windows 95,98,NT może być stosowany standardowy klient Netware, lecz jest on bardzo ubogi i w wielu zastosowaniach nie może być stosowany. Najlepiej korzystać z klienta produkcji Novel pod te systemy. Oprogramowanie to instaluje się w system tak jak normalne sterowniki w konfiguracji sieci Microsoft'a. Logowanie może być pierwszorzędne do Netware następnie automatycznie do pozostałych sieci typu Microsoft Network.
Klient ten umożliwia np. w opcji Właściwości pliku lub katalogu zmianę praw na dysku netware lub np. bezpośredni dostęp przez otoczenie sieciowe do volumenów Netware.

W wyżej wymienionych systemach operacyjnych, które w Polsce są najczęściej wykorzystywane, istnieje pojęcie dysku oznaczonego literką (A,B,C itd.). Wszelkie aplikację działające np. tylko na platformie DOS dostęp do plików wykorzystują przez dysk z oznaczeniem takiej właśnie literki. Wygodne jest dlatego wprowadzenie usługi mapowania całego volumenu lub jego fragmentu jako konkretny dysk np. F,G itp.
Podobna sytuacja jest z drukowaniem. Można zmapować istniejącą kolejkę drukowania na serwerze drukowania Netware na konkretny lokalny port równoległy, np. LPT1, LPT2 itp.

8.5 Prawa do plików

Prawa do plików i katalogów w systemie Netware są bardzo rozbudowane i dają bardzo duże możliwości precyzyjnego dostępu użytkowników. Istnieją takie prawa jak: Przeglądanie, odczyt, zapis, zmiana, tworzenie, usuwanie, kontrola dostępu. Prawa do katalogów są dziedziczone w dół, tzn. w podkatalogach użytkownicy również mogą je wykorzystywać. Istnieje możliwość ograniczania praw w strukturze podkatalogów dla konkretnych użytkowników lub dla wszystkich. Prawa mogą być również nadawane grupom użytkowników.
Na prawa efektywne użytkownika (prawa, które użytkownik może wykorzystać) składają się: prawa bezpośrednio mu nadane + prawa nadane grupom do których należy + prawa nadane użytkownikom do których posiada ekwiwalent - prawa fizyczne (np. atrybut DeleteInhibit - zakaz kasowania dla pliku).

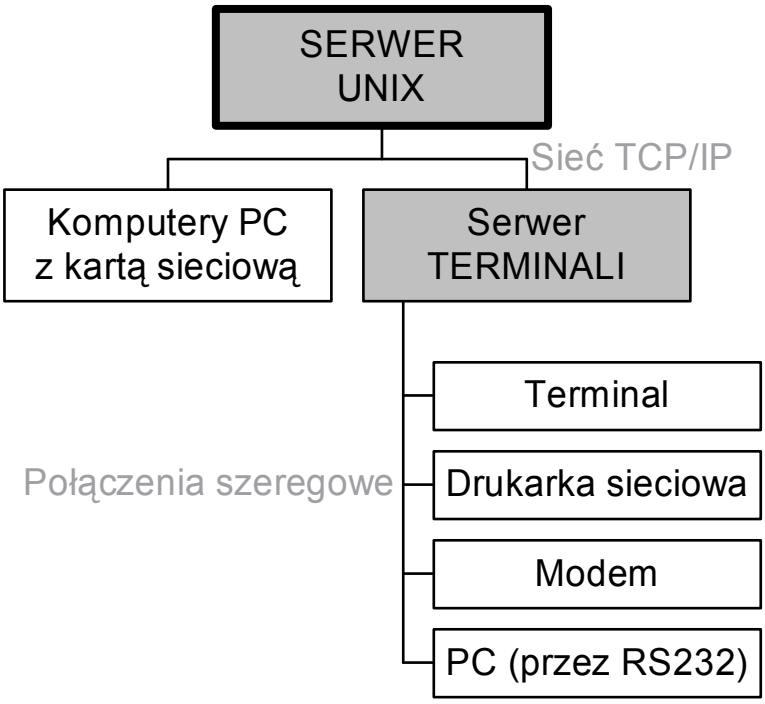
9 Sieci opierające się na systemach UNIX

9.1 Praca terminalowa

W systemie operacyjnym UNIX praca na końcówkach zazwyczaj ogranicza się do pracy terminalowej w trybie tekstowym. Do tego celu nie muszą być wykorzystywane normalne komputery rozbudowane typu PC lecz mogą być stosowane tzw. terminale. Terminal taki to w uproszczeniu: klawiatura, monitor (najczęściej mono), oraz prosty układ do komunikacji przez port szeregowy. Terminale takie przez sieć strukturalną podłącza się dopiero do specjalnego serwera terminali lub do karty wieloportowej posiadającej porty szeregowe zainstalowanej w normalnym komputerze, który ma zainstalowane oprogramowanie serwera terminali. Praca terminalowa może być również wykonywana bezpośrednio na komputerze PC przy pomocy specjalnej aplikacji terminala. Aplikacja taka może obsługiwać komunikację z serwerem UNIX zarówno przez port szeregowy (np. COM1) podłączony do serwera terminali jak i przez sieć - wykorzystywana jest wtedy usługa telnet protokołu TCP/IP. To drugie rozwiązanie jest najczęściej praktykowane ze względu na koszty. Komputer PC jest zazwyczaj i tak podłączony do sieci do której wpięty jest zawsze serwer terminali i serwer UNIX. Komunikacja wtedy może być wykonywana z pominięciem serwera terminali co bardzo upraszcza sprawę i minimalizuje koszty, gdyż koszt każdego portu serwera terminali jest bardzo wysoki.

9.2 Serwery terminali

Serwery terminali to specjalizowane urządzenia posiadające wiele portów szeregowych oraz kartę sieciową. Montowane są one najczęściej w szafie rozdzielczej sieci strukturalnej, ponieważ jest to bardzo wygodne przy wszelkich zmianach układu urządzeń w sieci. Dlatego też rozwiązania oparte o komputer z kartą wieloportową są mniej wygodne, ponieważ nie da się ich umieścić w szafie krosującej. Do portów szeregowych mogą być podłączone terminale i to jest najczęstsza funkcja tych urządzeń. Serwer terminali zamienia wtedy normalną komunikację na porcie szeregowym na transmisję telnet po sieci TCP/IP. W terminalu nie musi być wtedy żadnej rozbudowanej obsługi, po naciśnięciu jakiegoś klawisza serwer terminali automatycznie zestawia połączenie ze zdefiniowanym hostem.



Rys. 6 Schemat połączenia z serwerem UNIX.

Oprogramowanie serwerów terminali umożliwia również wykorzystanie portów do innych celów. Najczęściej porty wykorzystywane są do drukarek sieciowych. Drukarki mogą być podłączane również przy pomocy portów szeregowych. Specjalne oprogramowanie serwera terminali zainstalowane na serwerze UNIX potrafi podłączyć się pod systemową kolejkę drukowania i przesyłać zlecenia na konkretny port serwera terminali. Jest to bardzo przydatna i często wykorzystywana funkcja.

Do portu serwera terminali może również być podłączony modem, który można wykorzystywać do wielu rzeczy. Najczęściej wykorzystywany jest do celów obsługi łącz komutowanych. Oprogramowanie serwera terminali potrafi ustawić modem w tryb AutoAnswer i przy połączeniu przeprowadzić identyfikację użytkownika oraz przejść do wielorakich funkcji, np. wykonać usługę telnet na serwer UNIX lub przydzielić IP i zestawić połączenie z siecią lokalną. Takie serwery terminali z modemami najczęściej stawiane są za urządzeniem Firewall (patrz rozdział 10.6 na stronie 42). Po zestawieniu połączenia Firewall pozwoli tylko na określoną transmisję z konkretnego portu. Modem może być również wykorzystywany do zestawiania stałych połączeń z innymi jednostkami firmy. Standardem tutaj jest protokół PPP oraz SLIP.

9.3 Praca sieciowa systemów UNIX

Komputer Unix komunikuje się z siecią przy pomocy tzw. demonów (daemon). Są to programy, które nonstop pracują i odpowiadają na określonych portach protokołu TCP na

zlecenia. Informację o tym jak mają one odpowiadać i przy pomocy jakich programów zdefiniowane jest w pliku /etc/inetd.conf. Standardowo na każdym komputerze Unix wykonywany jest jako pierwszy proces Init. On dopiero na podstawie konfiguracji uruchamia odpowiedni demony, m.in. demon obsługi sieci, który to dopiero na określonych portach uruchamia poszczególne aplikacja, takie jak serwer WWW,FTP,IRC.

System plików w UNIX jest tak zorganizowany, że wszystko jest widoczne w jednym spójnym drzewie katalogów. Inna partycja lub całe urządzenie jest widoczne jako podkatalog. Definicje wszystkich File Systemów można znaleźć w pliku /etc/fstab. Stacja dyskietek lub CD jest traktowany jak oddzielny File System i montowany jest w osobnych podkatalogach. Po zamontowaniu już konkretnego FileSystemu dostęp do niego jest już przy pomocy standardowych poleceń Unix'a wykonywanych w katalogu danego systemu plików.

Komputery Unix mogą się ze sobą komunikować przy pomocy sieci na kilka sposobów. Do zdalnej pracy wykorzystuje się telnet - każdy serwer unix może również być klientem (terminalem). W bardziej zaawansowanych rozwiązania wykorzystywany jest protokół SSH umożliwiający szyfrowanie przy pomocy kluczy RSA transmisję danych pomiędzy serwerami. Do transmisji plików najczęściej wykorzystywany jest protokół FTP. Jest on jednak bardzo nieporęczny i wymaga odpowiednich aplikacji do transmisji - nie jest wbudowany bezpośrednio w system. Jeśli jest potrzeba stałego połączenia komputerów Unix robi się to przy pomocy NFS (Network File System). NFS umożliwia zamontowanie jako lokalny File System fragmentu drzewa katalogów z innego serwera. Oczywiście problem pojawia się z prawami i użytkownikami. Istnieje bardzo wiele zazwyczaj autorskich rozwiązań przenoszenia tych danych i zrobienia wspólnej globalnej bazy danych użytkoników (np. NIS w Sun Solaris)

10 Bezpieczeństwo sieci

10.1 Zabezpieczenie sprzętowe serwerów

W celu zapewnienia stabilnej pracy całej sieci należy w pierwszej kolejności zapewnić pewną i ciągłą prace serwerów sieciowych zajmujących się przechowywaniem danych użytkowników oraz systemowych aplikacji.

Najczęstsze awarie sprzętu komputerowego przy założeniu, że sprzęt jest markowy mogą wystąpić w postaci awarii urządzeń takich jak zasilacz bądź dysk. Sprzęt markowy ma wbudowane pewne mechanizmy wymiany urządzeń uszkodzonych nawet podczas pracy co czasem może mieć zasadnicze znaczenie.

Co do zabezpieczeń zasilaczy najwygodniejszym rozwiązaniem jest specjalna obudowa z podwójnym zasilaczem.

Najczęściej zabezpiecza się przed utratą dane, które przechowuje się na dyskach i tu najprostsze rozwiązanie to tzw. mirroring. Rozwiązanie to bazuje na podłączaniu dwóch dysków o podobnej pojemności i automatyczne (systemowe) zapisywanie wszelkich zmian równocześnie na dwóch dyskach. Operację tę może robić wyspecjalizowany sterownik (najczęściej SCSI) lub software'owo system operacyjny. W przypadku awarii system umożliwia dalszą normalną pracę na zapasowym dysku. Stosuje się czasem również rozwiązanie bardzo podobne nazywane duplexing'iem. Różnica jest jedynie taka, że zapisem na drugim dysku zajmuje się drugi sterownik dyskowy. Daje to szybsze rozwiązanie i mniej awaryjne. Rozwiązania te mają bardzo jedną dużą wadę - należy wyposażyć system w podwójną ilość przestrzeni dyskowej co nie jest tanim rozwiązaniem.

Bardzo atrakcyjnym systemem jest rozwiązania tzw. macierzy dyskowych opierających się na technologii RAID 5. Rozwiązanie to polega na tym, że specjalny sterownik macierzowy zapisuje równocześnie dane przez kilka kanałów na wielu dyskach. Teoretycznie można to wytłumaczyć że dla podłączonych 5-ciu dysków system zapisuje informacje na 4-ch dyskach a na ostatnim zapisywane są sumy kontrolne. Macierz może obsługiwać również np. 3 dyski lecz strata przestrzeni jest wtedy 33% a nie np. 20% przy 5-ciu dyskach co i tak jest dobrym rozwiązaniem bo np. przy mirroringu traci się 50% przestrzeni dyskowej.

System taki daję gwarancję ciągłości pracy tak jak mirroring przy mniejszym wykorzystaniu przestrzeni dyskowej. Rozwiązanie oparte o macierz dyskową ma jeszcze jedną bardzo cenną zaletę, mianowicie dzięki wielokanałowemu równoczesnemu zapisowi na wiele dysków skraca

się znacznie czas zapisu i odczytu informacji. Istnieją również rozwiązania umożliwiające podłączenie do macierzy dysku zapasowego. Sterownik macierzowy w momencie awarii potrafi automatycznie odbudować uszkodzony dysk na dysku zapasowym, co powoduje że sytuacja awaryjna możliwości utraty danych (w przypadku awarii drugiego dysku) istnieje tylko przez kilkanaście minut. Oczywiście na wypadek awarii dwóch dysków system RAID 5 nie jest odporny.

10.2 Serwery dublujące

Istnieje możliwość również dyblowanie nie tylko zasilaczy czy dysków lecz całych serwerów. Operacja taka jest robiona całkowicie software'owo i musi być wbudowana w system operacyjny. Istnieją rozwiązania systemowe takie jak np. Netware SFT Level III, który umożliwia instalacji dwóch serwerów na jednym współpracującym ze sobą identycznym systemie sieciowym. Serwery takie można ustawić np. w dwóch osobnych pomieszczeniach, co wpływa dodatkowo na bezpieczeństwo danych np. przed pożarem.

Systemy takie są bardzo drogie w momencie zakupu, ale również w późniejszej eksploatacji. Uwzględnić należy również podwójny rozwój sprzętu serwera. Zarządzanie i skonfigurowanie systemu jest dość skomplikowane.

10.3 Zabezpieczenie ciągłości zasilania

Bardzo często i jest to całkiem niezależne od przyjętych nawet bardzo zaawansowanych rozwiązań informatyczny ulega awarii instalacja zasilania. Powszechnie wiadomo, jakie mogą być skutki wyłączenia komputera bez wcześniejszego zamknięcia systemu. W przypadku systemu sieciowego ma to całkiem inny wymiar i zagrożenie utraty danych jak i całej spójności systemu jest bardzo duże. Należy więc koniecznie zagwarantować stabilne zamknięcie systemu nawet w przypadku całkowitej awarii zasilania. Do tego celu służą urządzenia UPS. Istnieją instalację podtrzymujące nawet całą sieć komputerową, lecz są to rozwiązania bardzo drogie i stosuje się najczęściej rozwiązania podtrzymujące część sprzętu sieci - tylko komputery najbardziej istotne. Serwer sieciowy powinien być podłączony do UPS'a przy pomocy kabla RS232 albo specjalnego modułu SNMP umożliwiającego wysyłanie komunikatów przez sieć do serwera o aktualnym stanie baterii UPS i stanu zasilania sieciowego. Serwer w przypadku utraty zasilania powinien, w zależności od czasu podtrzymania prądu przez UPS, zamknąć wszystkie pracujące aplikacje, i normalnie się wyłączyć. Powinno stosować się pewne opóźnienie i bardzo przydatne są tutaj urządzenia UPS, które potrafią informować komputer o staniu akumulatorów.

W takim przypadku serwer może przejść do procedury wyłączającej jeśli stan akumulatorów wynosi np. 10% co starcza np. na 20 min. pracy.

10.4 Archiwizacja danych

Najistotniejszym elementem bezpieczeństwa jest zabezpieczenie przed utratą danych. Ciągłość pracy jest potrzebna tylko w bardzo niewielu systemach. Utrata danych księgowych jest wręcz katastrofą dla wielu firm. Sama utrata danych nie musi się zawsze wiązać z awarią sprzętu. Czasem utrata danych może być spowodowana przez niewykwalifikowaną obsługę bądź przypadkowe usunięcie danych na serwerze. W celu zabezpieczenia przed utratą danych należy regularnie (np. codziennie lub raz na tydzień) wykonywać kopie najistotniejszych danych systemowych, np. danych systemu księgowego.

Kopie wykonuje się na nośnikach niekoniecznie szybkich z wygodnym dostępem ale za to o dużych pojemnościach. Wygodny dostęp (do jakiego jesteśmy przyzwyczajeni - np. dysk twardy) nie jest tutaj potrzebny ponieważ z kopii tych korzysta się tylko w przypadkach awarii i często jest tak, że kopie te robi się codziennie a przez całe lata nie wystąpi potrzeba odczytania zabezpieczonych danych. Do tego celu bardzo często stosuje się tzw. taśmy magnetyczne. Urządzenie zapisujące dane na taśmach nazywa się streamer. Umożliwia on do zapisania np. w systemie DDS-3 do 24GB na jednej tasiemce co daje duże możliwości przechowywania np. stanu bazy z ostatniego tygodnia czy miesiąca. Zapis jak i odczyt jest sekwencyjny co oznacza potrzebę przewinięcia taśmy do odpowiedniego miejsca i zapis lub odczyt danych.

Innym bardziej wygodnymi nośnikami danych mogą być: dyski magneto-optyczne. Napędy dysków magneto-optycznych jak i sama technologia umożliwia bardzo szybki i wygodny dostęp do danych stąd wykorzystywane są one jak normalne dyski. Technologia ta jest jednak dość droga i przy większej ilości danych nieopłacalna.

Bardzo często istnieje potrzeba zabezpieczenia danych w sposób niemożliwy do późniejszej zmiany. Do tego celu wykorzystuje się urządzenia jednorazowego zapisu takie jak napędy CDR umożliwiające zapis danych na normalnym dysku CD w sposób niemożliwy do późniejszej zmiany.

10.5 Zabezpieczenia serwerów sieciowych przed włamaniami

W przypadkach kiedy serwery sieciowe podłączone są do internetu, lub występuje bardzo duża sieć rozległa firmy na której pracuje bardzo dużo często anonimowych osób znacznym zagrożeniem danych jak i pracy systemu jest włamanie osoby niepowołanej do systemu. Nie

musza to wcale być bardzo dobrzy hackerzy czy ludzie o wysokich kwalifikacjach. Oni najczęściej jeśli nawet się włamią gdzieś to informują administratorów systemu o znalezionych dziurach bądź lukach w bezpieczeństwie systemu. Najgroźniejsi są tutaj użytkownicy, którzy uważają, że włamanie się do systemu jest ich zasługą a ogranicza się to do uruchomienia prostych programów, które umożliwiają włamanie.

Najczęstszym problemem jest przejęcie lub odgadniecie hasła użytkownika. Odgadniecie hasła najczęściej wiąże się ze zbyt prostymi hasłami użytkowników, dlatego hasło nie powinno być słowem na które łatwo może ktoś wpaść, powinno być jak najdłuższe i najlepiej zawierać oprócz znaków również cyfry.

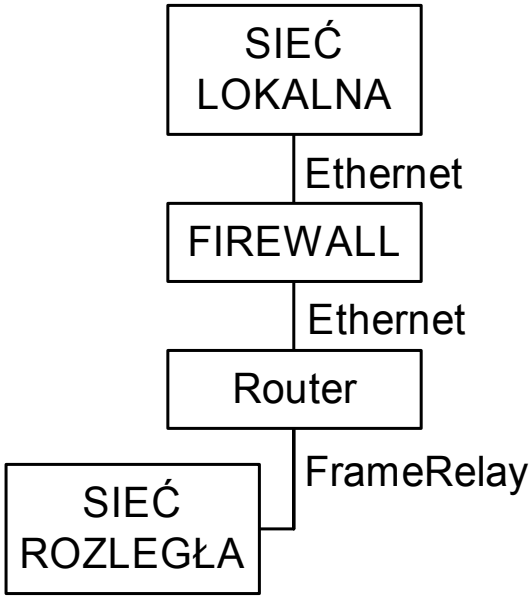
Przejęcie haseł ogranicza się do dwóch najczęstszych rozwiązań. Bardzo prostym rozwiązaniem jest zainstalowanie na komputerze specjalnego programu, który będzie od tego momentu zapisywał wszystko co się wprowadza z klawiatury do specjalnego pliku. Każda osoba która na tym komputerze się w późniejszym czasie będzie logowała do systemu to jej hasło zostanie zapisane na dysku. Oczywiście takie rozwiązanie jest zawsze możliwe w przypadku systemów takich jak Windows 95/98. Nie jest możliwa w przypadku Windows NT Workstation w przypadku oczywiście nieznajomości hasła administratora lokalnego komputera.

Druga metoda przechwytywania haseł jest bardziej wyrafinowana, aczkolwiek nie wymaga jakiejkolwiek wiedzy o sieciach i o funkcjonowaniu samego rozwiązania. Mianowicie rozwiązanie to polega na podsłuchaniu danych przesyłanych przez sieć. Wiele aplikacji takich jak np. telnet przesyła hasło przez sieć w postacie całkowicie niezakodowanej. Aplikacje takiej jak sniffer potrafią takie dane wyłapać i z innego komputera podsłuchać sesję logowania. Obejście takiej możliwości daje wykorzystanie aplikacji ssh zamiast telnet, która korzysta z kluczy RSA do kodowania transmisji zarówno hasła jak i późniejszych danych.

Najgroźniejszym problemem z włamaniami jest przejęcie kontroli nad użytkownikiem administratora w sieci. Użytkownik taki może zrobić wszystko począwszy od całkowitego usunięcia zbiorów do dowolnych przekłamań w zapisywanych danych. Tego typu problemy związane są zazwyczaj z błędami w programach, które muszą pracować z prawami administratora systemu. W systemach unix istnieje coś takiego jak prawo SUID umożliwiające uruchamianie programu z prawami jego właściciela. Bardzo wiele programów, np. program poczty elektronicznej musi pracować z prawami root. Ważne jest aby wgrywać wszelkie poprawki do systemu na bieżąco tak żeby zminimalizować czas pracy systemu niezabezpieczonego. Wszyscy producenci dystrybuują regularnie wszystkie aktualizację programów w postaci tzw. Service Pack.

10.6 Zabezpieczanie sieci – Firewall

Zabezpieczenie typu FIREWALL to obecnie najpewniejsze zabezpieczenie całej sieci lokalnej przed dostępem z zewnątrz osób niepowołanych. Zasada działania jest bardzo prosta. FireWall (Ściana Ognia) jak sama nazwa mówi odgranicza ruch wewnętrzny od ruchu zewnętrznego przepuszczając tylko to co jest dozwolone. Działanie firewall'a opiera się na zasadzie: że wszystko z góry jest zabronione. Następnie definiuje się reguły dla FireWall'a co może być przepuszczone. FireWall przegląda dokładnie każdy pakiet przesyłany przez sieć i sprawdza czy dany pakiet pasuje do zdefiniowanych reguł. Jeśli pakiet nie spełnia żadnej z reguł jest odrzucany.



Rys. 7 Przykładowa fizyczna implementacja FireWall

Na powyższym rysunku widać przykładową fizyczną implementacje FireWall. FireWall najczęściej realizowany jest przy pomocy normalnego komputera z bezpiecznym systemem operacyjnym (np. Windows NT lub dowolny Unix – najczęściej Solaris firmy SUN) oraz z zainstalowaną aplikacją FireWall, która przejmuje cały ruch sieciowy i zaczyna filtrować wszystkie przesyłane pakiety wg zdefiniowanych reguł. Firewall wyposarzony jest w dwie karty sieciowe (w powyższym przykładzie jest to Ethernet) i ważne jest aby obie te karty nie znajdowały się w tej samej domenie rozgłoszeniowej Ethernetu. W zasadzie chodzi o to aby to co za firewall'em czyli zewnętrzna karta sieciowa Firewall'a oraz karta sieciowa routera były wpięte do osobnego przeznaczonego tylko do tego celu koncentratora (hub'a).

Reguły FireWall'a opierają się na możliwości zdefiniowania w nich od kogo mogą być przesyłane dane (adres IP), gdzie mogą być przesyłane dane (adresy IP), jakie mogą być przesyłane dane (port TCP).
Oczywiście istnieją również bardziej zaawansowane metody identyfikacją „od kogo" przesyłane są dane. Wchodzi tu w grę wiele metod autentyfikacji wykorzystywanych w systemach operacyjnych takich jak Windows NT czy NIS w Unix'ach. Wtedy oczywiście nie jest istotne z jakiego IP dana osoba się zalogowała w sieci lokalnej. Tego typu metody są oczywiście bardziej zawodne i łatwiejsze do złamania. Sieć chroniona FireWall'em wcale nie jest bezpieczne przez fakt, że sam FireWall istnieje, lecz przez fakt że istnieją na nim dobrze zaprojektowane reguły gwarantujące bezpieczeństwo. Projektowanie reguł FireWall'a to bardzo skomplikowane i często bardzo trudne zadanie. Istnieje wiele opracowań, z których można skorzystać. Zawsze wymagana jest bardzo duża wiedza zagadnień sieciowych osoby projektującej FireWall'a.

Spis rysunków

Rys. 1 Schemat budowy ramki przy transmisji danych w sieci 6
Rys. 2 Udostępnianie zasobów w sieci Microsoft Network..... 26
Rys. 3 Ustawianie logowania się do domeny w Windows 95..... 28
Rys. 4 Ustawianie grupy roboczej w Windows 95/98 29
Rys. 5 Ustawianie kontroli dostępu do udostępnionych zasobów..... 30
Rys. 6 Schemat połączenia z serwerem UNIX..... 36
Rys. 7 Przykładowa fizyczna implementacja FireWall 42

Literatura dodatkowa

[1] Vademecum Teleinformatyka. Wydanie specjalne miesięcznika NETWORLD Część 1,2,3. IDG Poland S.A. 1998.

[2] Mała encyklopedia teleinformatyki. Wydanie specjalne miesięcznika NETWORLD. IDG Poland S.A. 1997.

[3] Papir Zbigniew, *Sieci z komutacją pakietów od X.25 do Frame Relay i ATM.* Wydawnictwo Fundacji Postępu Telekomunikacji. 1996.

[4] Cichocki Tadeusz, *Novell Netware i sieci komputerowe – Przewodnik i koncepcje.* Intersoftland. 1993.

[5] Networld - Sieci komputerowe i Telekomunikacja. IDG Poland S.A. Miesięcznik.