NAUKOWA I AKADEMICKA SIEĆ KOMPUTEROWA

SEMINARIUM

Miedzeszyn, wrzesień 1994 r.

ISBN 83-902314-0-9

NAUKOWA I AKADEMICKA SIEĆ KOMPUTEROWA

SEMINARIUM

Miedzeszyn '94

Wydawca:
Naukowa i Akademicka Sieć Komputerowa
00-716 Warszawa
ul. Bartycka 18
tel./fax 41-00-47

Skład i łamanie komputerowe, opracowanie graficzne:
Redakcja Wydawnictw Ośrodka Przetwarzania Informacji, 00-950 Warszawa, al. Niepodległości 188 B
Druk:
Zakład Poligraficzny Ośrodka Przetwarzania Informacji, 00-950 Warszawa, al. Niepodległości 186

Spis treści

Wstęp do wydania 1994 r.

Naukowa i Akademicka Sieć Komputerowa rozwijała się w zaskakującym tempie. W ciągu przeszło roku od ostatniego seminarium w maju 1993 roku zmieniła się technologia, zasadniczo zwiększył się ruch w sieci i zmieniły się poglądy na wykorzystanie sieci NASK.

Rozważaliśmy formę przekazania informacji o sieci NASK. Z jednej strony pouczające jest pokazanie ewolucji sieci oraz poglądów na jej funkcje. Z drugiej jednak nadmiar informacji nie służy jasności wykładu. Wobec tego przekazujemy aktualny stan sieci, organizacji obsługi oraz plany jej wykorzystania i modyfikacji w 1994 roku.

Zdajemy sobie sprawę, że są one w pewnym stopniu odmienne od przekazywanych w roku ubiegłym. Tam gdzie jest to szczególnie istotne postaramy się zaznaczyć odmienności w poszczególnych referatach.

Wstęp

Naukowa i Akademicka Sieć Komputerowa powstała wysiłkiem długoletniej pracy wielu zespołów w uczelniach i instytutach badawczych w Polsce.

Pierwsze przymiarki do budowy sieci akademickich miały miejsce w końcu lat siedemdziesiątych równolegle we Wrocławiu w ramach problemu resortowego RI.14 oraz w Warszawie w ramach problemu IV.6. Jednak te pierwsze próby, jak również kontynuacja prac aż do 1987 roku nie miały znaczenia utylitarnego. Z jednej strony środki były tak małe, że pozwalały jedynie na utrzymanie bardzo małych zespołów pracowniczych, z drugiej strony w tamtym okresie swobodna wymiana informacji w społeczeństwie nie była preferowana. Wobec tego nie było wystarczających środków państwowych, a działalność usługowa nie mogła się rozwijać. Oczywiście i w samym społeczeństwie nie obserwowało się pędu do zdobywania informacji.

Dopiero w roku 1987 uruchomiony został Centralny Program Badawczo-Rozwojowy CPBR 8.13 pod nazwą Budowa Krajowej Akademickiej Sieci Komputerowej KASK. W programie tym nastąpiła kontynuacja budowy zorientowanej terminalowo Akademickiej Sieci Komputerowej z Warszawy oraz zorientowanej komputerowo Miedzyuczelnianej Sieci Komputerowej z Wrocławia. Program mający do dyspozycji znaczące środki, sprawnie kierowany przez prof. dr hab. Daniela J. Bema z Politechniki Wrocławskiej, pozwolił na zbudowanie zrębów sieci akademickiej w kraju.

Podstawową zasługą tego programu było zebranie i rozbudowanie zespołu specjalistów z całego kraju, danie im szansy zdobycia kwalifikacji przy projektowaniu, wytwarzaniu i uruchamianiu urządzeń oraz sieci prototypowych.

Jednak i ten wysiłek podzieliłby prawdopodobnie los poprzednich prac, gdyby nie uwieńczone powodzeniem działania wielu zespołów w Polsce i Polaków za granicą, rozpoczęte jeszcze w 1987 roku, w wyniku których Departament Handlu Stanów Zjednoczonych AP wyraził zgodę na przyłączenie Polski do sieci EARN (łącznie Polska, CSRS, ZSRR, Węgry i Bułgaria).

W grudniu 1989 roku z inicjatywy Jacka Gajewskiego z Wydziału Fizyki Uniwersytetu Warszawskiego oraz Macieja Kozłowskiego z Centrum Astronomicznego Mikołaja Kopernika z Polskiej Akademii Nauk złożyliśmy wizytę ówczesnemu viceministrowi w Urzędzie Postępu Technicznego i Wdrożeń prof. Stefanowi Amsterdamskiemu w celu uzgodnienia możliwości finansowania przez urząd przyłączenia Polski do sieci EARN. Po uzyskaniu pozytywnej odpowiedzi 6 marca 1990 r. złożyliśmy odpowiedni kosztorys i następnie wniosek na Jednostkowe Przedsięwzięcie Badawczo-Rozwojowe JPBR 8.29 pod nazwą Przyłączenie Polskiego Środowiska Akademickiego i Naukowego do Sieci EARN. 21 marca 1990 r. prof. Tomasz Hofmokl został powołany na pełnomocnika Urzędu Postępu Naukowego, Technicznego i Wdrożeń do spraw związanych z przyłączeniem Polski do sieci EARN.

Powstanie dwóch równoległych problemów sieciowych w szkolnictwie wyższym groziło powstaniem konfliktu. Obiektywnie jednak pojawienie się EARN stanowiło znakomitą okazję do udowodnienia przydatności prac prowadzonych w ramach KASK. Ponieważ byłem jednocześnie kierownikiem tematu w KASK jako realizator budowy Stołecznej Akademickiej Sieci Komputerowej oraz realizatorem przyłączenia Polski do EARN, zainicjowałem współpracę w obu tematach. Również powołany pełnomocnik UPNTiW i Dyrektor Krajowy sieci EARN prof. Tomasz Hofmokl nawiązał współpracę z kierownikiem KASK prof. Danielem Bemem. Integracja sił oraz środków pozwoliła na szybkie, znacznie szybsze niż w innych krajach piątki uruchomienie sieci w Polsce. Jakkolwiek jeszcze dziś istnieją tendencje odśrodkowe, zwłaszcza wśród później dołączających się kolegów, zespół sieciowy pracuje w Polsce zgodnie.

Oba problemy, CPBR 8.13 KASK oraz JPBR 8.29 EARN, zakończyły się w końcu 1990 roku. Od maja 1991 roku sieci akademickie i naukowe funkcjonują już pod wspólną nazwą Naukowa i Akademicka Sieć Komputerowa NASK. Na czele realizacji sieci stoi zespół koordynacyjny składający się z ludzi już poprzednio uczestniczących w przygotowaniu i realizacji sieci. Zespół ten powstawał z inicjatywy własnej (oddolnej) przy akceptacji władz, które wykazały w tym okresie maksimum zrozumienia i dobrej woli.

Andrzej Zienkiewicz

Warszawa, kwiecień 1992

Organizacja Sieci NASK

Tomasz Hofmokl, Andrzej Zienkiewicz

1. Wprowadzenie

Siec NASK jest i będzie w dającej się przewidzieć przyszłości ściśle zintegrowana z sieciami publicznymi administrowanymi przez Telekomunikację Polską SA oraz z innymi sieciami działającymi w jej otoczeniu.

W takiej sytuacji jest zasadne pytanie o celowość wydzielenia tej sieci, czy sieć NASK ma sens jako odrębnie operowany system ?

Sieci komputerowe w nauce i szkolnictwie wyższym składają się w Polsce, podobnie jak w krajach rozwiniętych, z dwóch części czy systemów. Jeden stanowi sieć szkieletowa *(backbone)* stanowiąca podstawowy system łączności w ramach kraju, połączony z podobnymi sieciami na świecie. Drugi - cała masa ośrodków obliczeniowych, ewentualnie z maszynami wielodostępnymi, sieci lokalnych często rozbudowanych w duże systemy uczelniane lub miejskie, z maszynami wielkiej mocy pracującymi w tych sieciach itp. Sieci uczelniane łączą się z siecią szkieletową i z innymi sieciami publicznymi i prywatnymi w zależności od potrzeb oraz korzyści ekonomicznych i funkcjonalnych. Sieć szkieletowa stanowi zdefiniowany system, z określonymi protokołami przyłączenia, centralnie finansowany i utrzymywany. Sieci uczelniane są różnorodnie zarządzane i finansowane w sposób zdecentralizowany. Ich ewentualna jednolitość może być podyktowana tylko korzyściami ekonomicznymi lub funkcjonalnymi. W środowisku akademickim istnieje uzasadniony konflikt pomiędzy chęcią badania i tworzenia nowych rozwiązań oraz brakiem środków zmuszających do korzystania z już istniejących.

Po powyższych wyjaśnieniach oczywistym jest, że pytanie postawione poprzednio odnosi się do sieci szkieletowej. Sądzimy, że są co najmniej dwa powody, dla których sieć szkieletowa środowiska naukowego i akademickiego jest i będzie wyodrębniona.

Środowisko naukowe i akademickie na świecie tworzy coś w rodzaju nieformalnej wspólnoty. Wspólnota ta jest wynikiem obiektywnych konieczności zapewniających znaczący udział w nauce i badaniach na świecie. Jednym z czynników integrujących jest ogrom środków potrzebnych na budowę odpowiedniej aparatury, z drugiej ogromna masa informacji generowanych przez tę aparaturę. Przykładem może tu być fizyka jądrowa, astronomia itp. dziedziny, gdzie istnieje problem przetworzenia danych z eksperymentów czy pomiarów z bardzo drogiej i wspólnie budowanej aparatury.

Innym przykładem może być biologia, badająca w zasadzie to samo środowisko, występujące w ogromnej ilości odmian, gdzie publikowanie i odczytywanie publikowanych danych jest stratą czasu w porównaniu z dostępem do wspólnie wytwarzanych i gromadzonych danych badawczych.

Można mnożyć przykłady wspólnych publikacji, opracowań badań itp. skłaniających z jednej strony środowisko naukowe do współpracy, z drugiej eliminujące tych, którzy we wspólnym dziele nie uczestniczą.

Oczywiście środowisko akademickie nie różni się od naukowego, co więcej trudno sobie wyobrazić dobrego dydaktyka na wyższej uczelni, który w ten czy inny sposób nie uczestniczy w badaniach naukowych czy ich upowszechnianiu. Powyższe problemy skłaniają środowisko do tworzenia systemów wzajemnego udostępniania informacji na zasadzie wspólnych korzyści. Wobec tego powstają systemy wymiany informacji w postaci poczty, transferu zbiorów danych, programów, wspólnej obróbki danych itp. działające na zasadach niekomercyjnych. Środowisko naukowe i akademickie ma własne sieci wymiany informacji, nawet jeśli ich podłożem technicznym są sieci publiczne czy prywatne. Sieci akademickie i naukowe działają na warunkach specjalnych i na podstawie odrębnego statusu. Na przykład w sieciach tych nie wolno wymieniać informacji komercyjnych, politycznych, religijnych, podjudzających, itp. Co dziwne, mimo że umowa ma w końcu charakter gentleman agreement, to jest powszechnie przestrzegana. Karą niesłychanie dotkliwą jest eliminacja z systemów informowania, a wobec ich powszechności łatwa do rozpowszechnienia.

Drugim powodem wyodrębniania sieci naukowych i akademickich jest ich naturalny wyprzedzający charakter. W środowisku naukowym i akademickim każda nowość jest próbowana, a co więcej ograniczanie prób spotyka się z powszechnym potępieniem. Za tę chęć do innowacji środowisko płaci zgodą na uciążliwości wynikające z nieudanych eksperymentów oraz niedoskonałość prototypowych rozwiązań. To co jest niedopuszczalne i zagrożone poważnymi sankcjami ekonomicznymi w sieciach publicznych jest tolerowane w sieciach akademickich. Z drugiej strony jest to ogromna wartość dla twórców rozwiązań komercyjnych, ponieważ tworzy doskonały poligon dla prób. Poligon ten jest rozległy, ponieważ sieci naukowe i akademickie należą do najbardziej rozbudowanych w krajach, gdzie sieci istnieją. Do tego środowisko dysponuje na ogół

kadrą, która jest skłonna i ma możliwości współdziałania w eksperymencie. Z tego powodu w rozwiniętym świecie duża część sieci akademickich jest fundowana przez producentów i dostawców systemów komercyjnych. Istotną rolę odgrywa tu duża wartość promocyjna instalacji sprzętu na uczelni w czasie doraźnym (reklama) jak i długofalowym (kadra wychowana na sprzęcie danej firmy).

Wyżej wymienione argumenty skłaniają nas do przekonania, że sieci akademickie, tak jak to się dzieje na przykład w Stanach Zjednoczonych AP będą zjawiskiem trwałym, niezależnie od rozwoju sieci publicznych oraz prywatnych. Sądzimy, że podobnie będzie się działo z wieloma sieciami w Polsce, tworzącymi odrębne systemy wykorzystujące publiczne sieci teleinformatyczne do swoich celów.

Zasadnicze poglądy na sieć akademicką nie uległy w ciągu ostatniego roku zmianie. Jednak coraz większa atrakcyjność sieci powoduje zainteresowanie jej usługami coraz większego grona użytkowników spoza środowiska naukowego i akademickiego. Z jednej strony środowisko to jest odmienne co skłania do odcinania go od sieci akademickiej, z drugiej jednak trudno uzasadnić społecznie oraz ekonomicznie zakaz udostępniania sieci dla administracji centralnej, państwowej oraz innych użytkowników. Wobec tego wszędzie tam, gdzie jest to uzasadnione unikalnością usług świadczonych przez NASK lub szczególnie ważnymi względami ekonomicznymi sieć jest udostępniana dla użytkowników nieakademickich. W dolnych warstwach sieci coraz mniej jest eksperymentu, a coraz więcej rutyny wymagającej dobrego rzemiosła i profesjonalizmu. Środowisko naukowe i akademickie nie jest przystosowane do tego rodzaju działalności oraz zbyt biedne, aby ją samodzielnie prowadzić. Wobec tego powstają pomysły wspólnego wykorzystywania dolnych warstw sieci NASK dla wielu użytkowników.

Sieć teleinformatyczną od wielu lat rozpatruje się jako szereg współpracujących ze sobą warstw, z których niższe świadczą usługi komunikacyjne dla wyższych. Zgodnie ze standardem tych warstw jest siedem - w naszym przypadku wystarczy wyodrębnić tylko cztery.

Warstwę pierwszą stanowią łącza fizyczne przenoszące sygnały cyfrowe. Są to przewody galwaniczne, łącza radiowe, satelitarne , światłowodowe itp. przenoszące tak zwane bity informacji cyfrowej.

W naszych warunkach dostarczycielem łącz fizycznych w skali międzynarodowej oraz krajowej jest TP SA oraz w ograniczonym zakresie TELBANK. W zasadzie na podstawowej sieci krajowej działają wszyscy interesujący nas operatorzy sieci. Tylko w sieciach lokalnych występują sieci budowane przez różnych operatorów.

Warstwę drugą stanowią łącza logiczne przesyłające tak zwane ramki informacji cyfrowej. Tworzą ją specjalizowane urządzenia komputerowe zajmujące się nadawaniem i odbiorem ramek z jednoczesną kontrolą ich poprawności. Sieć ta jest podstawowym elementem szkieletu sieci - backbone. Nie jest ona zorientowana w żaden sposób na konkretnego użytkownika i powinna być eksploatowana przez jednego operatora.

Warstwę trzecią stanowią łącza sieciowe zajmujące się przesyłaniem pakietów informacji. Sieć ta w części zajmującej się sterowaniem przesyłania jest elementem backbone. Jednak w części doprowadzającej informacje do urządzeń i sieci lokalnych użytkownika jest elementem specyficznym dla różnych sieci. Oczywiście część należąca do backbone wymaga zarządzania wspólnego, natomiast części specyficzne powinny być przedmiotem zarządzanym przez odrębnych operatorów sieci.

Wreszcie warstwa czwarta - w modelu formalnym warstwy od 4 do 7 - obejmuje już usługi dla użytkowników i powinna być zarządzana przez odpowiednich operatorów sieci. Dopiero w tej warstwie pojawia się informacja użytkownika w postaci czytelnej. W pozostałych warstwach informacja jest ciągiem bitów, które mogą reprezentować teksty, liczby, głos, obraz itp. W szczególnych przypadkach, w celu ochrony przed nieuprawnionym odebraniem treści, przesyłana informacja w sieci powinna być szyfrowana przez ogólnie dostępne urządzenia i programy. Urządzenia i programy są indywidualne dla każdego użytkowania i w szczególnych przypadkach powinny być wymieniane co 2 lata, tyle bowiem wynosi czas potrzebny na ich złamanie.

W opisanej wyżej sytuacji rysuje się możliwość wspólnych działań pozostawiających specyfikę sieci naukowej i akademickiej tam, gdzie jest to uzasadnione potrzebą rozwoju i eksperymentu. Natomiast tam, gdzie potrzebne jest solidne profesjonalne działanie można prowadzić działania zapewniające usługi wielu użytkownikom.

Warstwę łącz logicznych obecnie eksploatuje zespół NASK. Docelowo eksploatacja całego backbone, powinna trafić do TP SA lub podobnej zawodowej organizacji. Proces ten jednak może być długi wobec konieczności zorganizowania i wyszkolenia odpowiedniej kadry. Warstwę trzecią w zakresie backbone proponujemy potraktować podobnie jak drugą.

Natomiast jej część specyficzną jak i warstwę czwartą zostawić jako domenę działania operatorów sieci w tym i NASK w zakresie obsługi środowiska naukowego i akademickiego.

Oczywiście wymienianie TP SA wynika z dzisiejszego stanu rynku usług telekomunikacyjnych. Można sobie jednak wyobrazić inny rozwój sytuacji na przykład powołanie profesjonalnego operatora dla wydzielonej grupy użytkowników obsługującego ogólnie administrację państwową, kierowanie państwem, naukę itp. dziedziny finansowane w dużej mierze przez zamówienia rządowe. Dziedziny te są na tyle specyficzne, że pojawiają się na świecie tendencje dla powierzania ich obsługi specjalnie powołanym organizacjom o charakterze komercyjnym lub niedochodowym lecz działającym na warunkach rynkowych.

2. Naukowa i Akademicka Sieć Szkieletowa NASK

Zmiany w sieci NASK następują bardzo szybko. Prawdopodobnie już w czasie konferencji we wrześniu nie wszystko tutaj napisane będzie prawdziwe.

Zmiany w samej sieci są wymuszane trzema przyczynami. Po pierwsze bardzo szybko wzrasta ruch w sieci. Jedną przyczyną jest pojawianie się nowych, bardzo przystępnych dla użytkownika usług jak Gopher, World Wide Web, które pozwalają zupełnemu "profanowi" łatwo sięgać do potrzebnych mu informacji. Związany z tym jest szybki rozwój technologii oraz wzrost udziału informacji graficznej w ogólnym ruchu w sieci. Wreszcie wzrost liczby użytkowników końcowych wynikający z coraz szerszego dopuszczania do bezpośredniego korzystania z sieci studentów, a nawet uczniów szkół średnich.

Drugą przyczyną zmian jest powstawanie licznych sieci metropolitalnych, administrowanych poprzez środowiska lokalne.

Ograniczeniu podlega lokalna sieć NASK na terenach, gdzie powstają sieci miejskie. Podział abonentów pomiędzy NASK, a administratorów lokalnych jest zróżnicowany i wynika ze zróżnicowanych sytuacji w poszczególnych regionach.

Wreszcie trzecią przyczyną zmian jest stopniowy proces zmiany charakteru sieci NASK. Zgodnie z tendencjami światowymi, staje się ona coraz bardziej siecią bazową, na której działają operatorzy wirtualni *(service provider)* oraz różne sieci dostępowe (X.25, Internet, EARN, DecNet, itp.).

Zalążki sieci bazowej istniały już od początku działania sieci NASK, ponieważ podstawowe połączenia komunikacyjne były realizowane przy pomocy urządzeń DM 504 i DM 404, które wymieniały pomiędzy sobą strumienie ramek według protokołu HDLC. Dostęp do łącza z czterech portów był realizowany według zasady FIFO co powodowało multipleksację statystyczną ramek pochodzących ze wszystkich portów.

Kompresja danych jak i multipleksacja podwyższały wyraźnie średnią przepustowość łącza. Protokoły dostępowe pojawiały się dopiero poza siecią multiplekserów. W tej fazie jednak przełączanie informacji odbywało się na poziomie sieci dostępowych.

Kolejnym krokiem w kierunku powstawania sieci bazowej było ujednolicenie przesyłania polegające na połączeniu funkcji warstwy drugiej i pseudotrzeciej tzn. na przyjęciu zasady, że wszystkie komunikaty protokołów dostępowych ładowane są w datagramy IP. Następuje tym samym opatrzenie ramki HDLC w dodatkową możliwość komutowania jej poprzez jednolite urządzenia przełączające. Wybór IP wynikał z przeważającej ilości tego rodzaju komunikatów w sieci dostępowej oraz uniknięcie tym sposobem potrzeby dzielenia komunikatów (długie komunikaty/ramki). Jako urządzenia przełączające oraz tłumaczące na standardy dostępowe użyto routery CISCO.

Obecnie realizowany jest trzyletni plan przejścia na bezpośrednie przełączanie ramek, czyli protokół Frame Relay.

Wiąże się to z jednej strony ze zwiększeniem szybkości łącz, z drugiej z udoskonaleniem technologii oraz pojawieniem się stosunkowo tanich i bogatych w protokoły dostępowe urządzeń. Obecnie funkcjonuje jeden switch Frame Relay w Warszawie oraz połączenia Frame Relay do części routerów w regionach. W tym roku nastąpi rozbudowa urządzeń przełączających w głównych regionach, a w następnym uzupełnienie ich konfiguracji odpowiednio do pełnego zakresu potrzeb.

Odmiennie od potrzeb transmisji głosowej, gdzie z uwagi na charakter medium wystarcza stała szerokość pasma 64 Kbps, a po kompresji 6-8 Kbps , środowisko akademickie i naukowe potrzebuje elastycznej szerokości pasma transmisji. Jak pokażą to koledzy w dalszych referatach zmienność ta jest bardzo duża. Sztywny podział pasma powoduje marnotrawienie jego przepustowości przy jednoczesnym istotnym pogorszeniu jakości usług dla użytkownika (niepotrzebne opóźnienia reakcji). Z tego powodu w sieci akademickiej stosowaliśmy różne formy multipleksacji statystycznej na fizycznym łączu transmisji danych.

Na sieci bazowej funkcjonuje szereg sieci wirtualnych:

- Historycznie najstarsza jest sieć pakietowa, oparta na protokole CCITT X.25, pierwotnie realizowana na urządzeniach krajowej produkcji. Sieć ta stanowi i stanowić będzie w przyszłości narzędzie komuni-

kowania się z innymi sieciami, dostępu do komputerów obliczeniowych oraz maszyn i sieci bezpośrednio do niej dołączonych w kraju i na świecie. Obecnie z powodu jej małej przydatności dla szybkiej transmisji oraz koszt. W sieć ta ma podrzędne znaczenie w sieci NASK

- Kolejna sieć EARN, która w ścisłych kategoriach nie jest siecią komputerową. Stanowi ją system maszyn w zasadzie IBM wymieniających ze sobą zbiory danych w postaci poczty elektronicznej, zbiorów danych ograniczonej wielkości oraz komend umożliwiających niebezpośredni dostęp do baz danych. Sieć ta pracuje na zasadzie przesyłania danych od komputera do komputera. Wobec jej powszechności w pewnym okresie czasu na maszynach VAX oraz SUN pojawiło się oprogramowanie symulujące przesyłanie według standardu IBM. Jednak ruch w sieci EARN stanowi obecnie tylko 1 do 5% ruchu w sieci NASK. Sieć EARN, tak jak na świecie jest w szybkim zaniku.
- Dynamicznie rozwija się sieć INTERNET. Obecnie ruch w sieci INTERNET stanowi prawie 100% ruchu w sieci NASK. Sieć nie ma określonego typu maszyn, które mogą w niej pracować. Istotnym jest możliwość przyłączenia ich do ETHERNETu (standard 802.3) oraz zainstalowania oprogramowania TCP/IP (Transport Control Protocol/Internet Protocol). W sieci Internet pracuje obecnie ponad 8000 maszyn, natomiast strumień przesyłanej informacji przekracza kilka miliardów znaków na dobę, w tym przeważająca jeszcze część poprzez granice kraju.

- Szczególnie lubiana w południowej i zachodniej Polsce jest sieć DECNET maszyn VAX. Z pewnością zaletą tej sieci jest przyjemny dla użytkownika sposób działania na tych maszynach. Sieć ta w skali NASK jest obecnie zupełnie marginalna.

Wszystkie wymienione sieci dostępowe są ze sobą połączone w taki sposób, że użytkownik jednej może korzystać z usług drugiej.

Podobnie wszystkie poczty, pracujące na maszynach dowolnego typu, mogą być wzajemnie tłumaczone.

Wszystkie sieci NASK działają na łączach dzierżawionych od TP SA, fragmentarycznie innych operatorów oraz lokalnie na łączach własnych.

Obecnie NASK dysponuje w relacjach międzynarodowych łączem 2 Mbps do Sztokholmu, łączem 128 Kbps do Wiednia oraz łączami 9.6 Kbps do Lwowa i Moskwy. W relacjach krajowych NASK ma możność korzystania z łącz 2 Mbps do głównych miast oraz 64 Kbps (satelitarne) lub analogowymi 9.6 Kbps w pozostałych miejscach.

Zarządzanie siecią jest możliwe z jednego miejsca. I tak praca wszystkich multiplekserów połączonych z Warszawą kontrolowana i modyfikowana jest z konsoli operatorskiej w centralnym węźle NASK.

Wszystkie węzły sieci X.25 kontrolowane i konfigurowane są z Warszawy. Podobnie routery Internetu sterowane są z Warszawy. Miejsce sterowania siecią jest określone organizacyjnie, gdyż obecny system techniczny umożliwia to z dowolnego miejsca oczywiście chronionego odpowiednim systemem zabezpieczeń.

Sieć NASK pracuje ciągle przez cały rok i przez całą dobę. To stwierdzenie jest prawdziwe w stosunku do węzłowych punktów sieci.

W 1994 roku sieć NASK będzie składać się z trzech poziomów.

Połączenia międzynarodowe będą realizowane poprzez EBONE europejski sterowany ze Sztokholmu, który ma przepustowość w jednej relacji 2 Mbps (250.000 znaków na sekundę). Podstawowy backbone krajowy oparty na sieci jednolicie sterowanych z Warszawy routerów, w głównych relacjach ma przepustowość 2 Mbps i jest częściowo oparty na technice przesyłania Frame Relay. Sieci lokalne w większych ośrodkach, sterowane odrębnie w każdym mieście, mają przelotowość co najmniej 100 Mbps (12.500.000 znaków na sekundę) i są oparte na technice FDDI. Dołączanie użytkowników przez poszczególnych operatorów, poza backbone, jest ogromnie zróżnicowane pod względem przepustowości oraz technik podłączenia i nie jest przedmiotem eksploatowanym przez sieć szkieletową - backbone.

Rozbudowywana sieć musi być utrzymywana w ruchu. Przy obecnie bardzo wysokiej automatyzacji utrzymanie sieci składa się z trzech elementów:

- sterowania pracą sieci polegającego na stałej obserwacji z centrum sterowania i odpowiedniej modyfikacji parametrów jej pracy,
- reagowania na sytuacje awaryjne poprzez działanie ekip wyspecjalizowanych lub zdalne zmiany w konfiguracji ruchu w sieci,
- obsługa nowych instalacji i przyłączeń do sieci.

Z doświadczenia wynika, że przy tym typie działalności najmniej czasu wymaga reagowanie na sytuacje awaryjne, najwięcej sterowanie pracą sieci.

Organizacja NASK, poza zajmowaniem się siecią szkieletową NASK obejmującą kraj oraz połączenia międzynarodowe jest realizatorem sieci metropolitalnej w Warszawie. Sieć metropolitalna Warszawy ze względu na jej rozległość, liczba i różnorodność abonentów nie może mieć charakteru ringu FDDI. Z tego powodu od początku założyliśmy, że jedyną techniką możliwą do zastosowania w sieci jest ATM oparty na transmisji celek (Cell Relay). Proces przekonywania o słuszności wyboru oraz udowadniania tego wyboru trwał prawie dwa lata. Jednocześnie następował szybki rozwój tej technologii na świecie. Zdając sobie sprawę z ryzyka wynikającego z nowoczesności przyjętych rozwiązań zawarliśmy kontrakt oraz przystąpiliśmy do realizacji, której pierwszy etap zgodnie z umową zakończy się w styczniu 1995 roku. W tym miejscu przypomnimy podstawowe przesłanki dokonanego wyboru:

- Metropolitalna sieć warszawska WARMAN nie może opierać się na ringu FDDI z powodu trudnej ochrony sieci i informacji oraz wrażliwości tego rodzaju technologii na wzrost ruchu oraz zakłócenia w pracy.
- Drogi przesyłania w sieci muszą być możliwie ograniczone w sensie możliwie najkrótszej trasy pomiędzy przesyłającymi.
- Sieć musi mieć zdolność do rozbudowy bez zakłócania pracy jej funkcjonujących elementów.

Wyżej wymienione elementy mają charakter technologiczny i przesądzają o wyborze sieci typu WAN (Wide Area Network) w miejsce sieci typu LAN (Lokal Area Network).

Istnieją również argumenty poza technologiczne:

- Wydaje się nam, że jesteśmy najlepiej przygotowanym zespołem, ze względu na liczność jak i doświadczenie, do realizacji tego rodzaju przedsięwzięcia.
- Rozumiemy naszą rolę społeczną, jako jednostki przeznaczonej do wykonywania eksperymentów oraz wdrażania nowych technologii, z których potem korzysta pozostała część społeczeństwa.

3. Organizacja rozwoju i utrzymania NASK

W grudniu 1993 roku Przewodniczący Komitetu Badań Naukowych wydał zarządzenie powołujące jednostkę badawczo-rozwojową o nazwie Naukowa i Akademicka Sieć Komputerowa. Po przeprowadzeniu odpowiednich czynności prawnych jednostka została zarejetrowana w sądzie w lutym 1994 roku i od tego czasu prowadzi całkowicie samodzielną działalność. Naukowa i Akademicka Sieć Komputerowa jest przedsiębiorstwem państwowym o statusie jednostki badawczo-rozwojowej z siedzibą w Warszawie przy ul. Bartyckiej 18.

Do jednostki badawczo-rozwojowej przeszedł cały personel zatrudniany w różnych formach przez Uniwersytet Warszawski - Zespół Koordynacji Naukowej i Akademickiej Sieci Komputerowej w Polsce oraz personel obsługujący NASK zatrudniony w NASK-SERVICE. NASK-SERVICE stał się spółką mieszaną join-venture z udziałem kapitału zagranicznego, w której udziały ma NASK. Udziały zostały odkupione od założycieli, którzy stali się pracownikami NASK.

Wobec przejścia całości załogi nie nastąpiły zmiany w rzeczowych funkcjach pełnionych poprzednio. I tak Dyrektorem NASK jest prof. dr hab Tomasz Hofmokl, Dyrektorem Technicznym - Operatorem Sieci NASK jest mgr inż. Andrzej Zienkiewicz. Obaj Dyrektorzy posiadają pełnomocnictwa w zasadzie w pełnym zakresie działania NASK. Ustalone zostało stanowisko Dyrektora- Pełnomocnika d/s budowy sieci WARMAN, które pełni dr Maciej Kozłowski.

W NASK działa Rada Naukowa - przewodniczącym jest prof. dr hab. inż. Andrzej Wierzbicki, a prof. dr hab. inż. Józef Daniel Bem jego zastępcą.

Działalność operacyjna NASK jest podzielona na dwa piony.

Jeden do spraw sieci rozległej NASK - kierowany przez Zastępcę Dyrektora Technicznego d/s sieci NASK WAN mgr inż. Wiktora Krzanowskiego oraz drugi - kierowany przez Zastępcę Dyrektora Technicznego d/s sieci metropolitalnej WARMAN mgr inż. Tadeusza Rogowskiego. Pojawiły się nowe stanowiska Zastępców Dyrektora d/s Promocji i Organizacji obsadzone przez Marię Baranowską oraz Marię Ziółkowską.

Zmienia się zasadniczo struktura regionalna NASK. Wobec powstawania sieci metropolitalnych oraz związanych z nimi organizacji zanika rola Operatora Regionalnego NASK. Obecnie komórki regionalne NASK obsługują urządzenia sieci w regionie w zakresie ogólnego nadzoru oraz pośredniczą w organizacji podłączania nowych abonentów. Całkowite sterowanie siecią odbywa się centralnie bez prawa dostępu do urządzeń regionalnych przez służby terytorialne. Wynika to z trzech powodów. Po pierwsze - ograniczeniu ulega struktura NASK w regionie, a po jej zlokalizowaniu w jednym obiekcie np. TP SA, nie ma możliwości ani potrzeby jej obsługi. Po drugie - wymogi centralnego sterowania siecią wykluczają możliwość ingerencji w elementy sieci przez środowisko rozproszone. Po trzecie - coraz bardziej profesjonalna sieć wymaga specjalnej ochrony, która wymaga zasadniczego ograniczenia liczby osób mających do niej dostęp.

Zmienia się również charakter obsługi struktur regionalnych NASK. W miejsce bezpośrednio zatrudnionych osób wchodzą różnego rodzaju organizacje przejmujące funkcje obsługowe. Dawna kadra NASK w przeważającej części przechodzi do obsługi sieci metropolitalnych.

Jednostka badawczo-rozwojowa NASK ze względu na brak odpowiedniej formy prawnej nie jest formalnie jednostką nonprofit. Jednak z założenia zysk tej jednostki ma być zerowy. To znaczy, że rozwój sieci na obecnym etapie odbywa się ze środków na dofinansowanie inwestycji, otrzymywanych od organu założycielskiego oraz z odpisów amortyzacyjnych. Koszty bieżące działania sieci pokrywają abonenci sieci. Abonenci wytypowani przez Komitet Badań Naukowych otrzymują zniżki w opłatach - wartość tych zniżek pokrywa Komitet Badań Naukowych w ramach tak zwanego Specjalnego Programu/Urządzenia Badawczego.

Całe dotychczasowe wyposażenie sieci NASK zostało przekazane z Uniwersytetu Warszawskiego do NASK jako inwestycja w toku i stało się jej funduszem założycielskim.

4. NASK a inni operatorzy sieci komputerowych

NASK nie jest i nie będzie siecią, której głównym zadaniem jest przynoszenie dochodu właścicielowi. Obecnie działa jednostka badawczo-rozwojowa, czyli przedsiębiorstwo państwowe w głównej części realizuje zamówienia rządowe. Nie oznacza to, że usługi NASK są i zawsze będą bezpłatne. Działalność NASK kosztuje i na razie, żadna z organizacji obsługujących NASK nie czyni tego za darmo. Podobnie system podatkowy nie wiąże opodatkowania usług świadczonych przez NASK z wielkością ponoszonych opłat, tylko z wartością tych usług. Wobec tego wszystkie usługi NASK są odpłatne. Natomiast stosowane są zwolnienia z opłat dla poszczególnych abonentów na podstawie decyzji zleceniodawców - wszyscy abonenci (użytkownicy) sieci EARN nie ponoszą opłat za tranzyt informacji zgodnie ze statutem tej sieci określającym, że odpowiednie opłaty w postaci składek za ruch międzynarodowy i wkładu rzeczowego w ruch krajowy wnoszą rządy odpowiednich krajów członkowskich, podobnie decyzją Komitetu Badań Naukowych są zwolnieni z opłat za korzystanie z sieci Internet abonenci, których działalność statutowa jest finansowana przez ten sam komitet.

Dofinansowujący działalność sieci szkieletowej NASK Komitet Badań Naukowych ostrzega, że nie będzie pokrywał ciągle rosnących kosztów działania sieci. To znaczy, że część środków na działanie sieci przedsiębiorstwo będzie musiało zdobywać poza zamówieniami rządowymi. Środki te nigdy nie pokryją całości kosztów przy stosowaniu obligatoryjnych zwolnień z opłat, jednak z czasem muszą pokryć znaczącą ich część. Problem w tym, że potrzeby środowiska akademickiego są właściwie nieograniczone. Rośnie szybko zapotrzebowanie na przesyłanie obrazów rozumianych nie tylko jako przesyłanie obrazu wizualnego, ale również jako przesyłanie zapisów aparatury rejestrującej itp., rozwijają się usługi multimedialne, szybkie zastosowanie znajduje hypertekst.

Zapotrzebowanie to oznacza zwielokrotnienie strumienia przesyłanej informacji co najmniej kilkaset razy. Wobec tego trzeba stawiać tamy nieograniczonym apetytom, najlepiej poprzez stosowanie całkowitej lub częściowej odpłatności za przyrosty zapotrzebowania na transmisje pewnego rodzaju danych. Odpłatność usług może mieć również na celu ograniczenie nadmiernej rozbudowy sieci wynikającej wyłącznie ze względów ambicjonalnych osób lub środowisk akademickich i naukowych.

Koszty każdej działalności muszą być całkowicie pokryte z różnych źródeł finansowania. W przypadku NASK mamy do czynienia z kilkoma rzeczywistymi i potencjalnymi kierunkami pokrywania kosztów:

- Obecnie ponad 90%, a w przyszłości znacząca część kosztów będzie pokrywana z budżetu poprzez zamówienie na utrzymanie sieci szkieletowej. To źródło finansowania będzie zawsze konieczne dla pokrycia składek międzynarodowych oraz dla utrzymania pewnych usług, które zgodnie z porozumieniami międzynarodowymi, muszą być świadczone nieodpłatnie.
- Drugim obecnie funkcjonującym źródłem finansowania jest zwrot kosztów za korzystanie z usług NASK przez organizacje pozanaukowe, które określonych usług nie mogą uzyskać od innych operatorów lub usługi NASK są istotnie lepsze.
- Już w niedalekiej przyszłości będziemy musieli wprowadzić ograniczenia administracyjne na rozbudowę sieci INTERNET, lub co słuszniejsze ograniczyć zwolnienia z opłat za korzystanie z tej sieci.
- Liczymy na współpracę z Telekomunikacją Polską, dla której potencjalnie jesteśmy istotnym poligonem doświadczalnym oraz źródłem kwalifikowanych kadr. Współpraca ta może przynieść środki na działalność NASK w kilku formach:
- poprzez bezpośrednie finansowanie prac rozwojowych i wdrożeniowych, służących obu organizacjom,

- poprzez stosowanie ulg na usługi świadczone dla środowiska, tak jak to się dzieje na przykład w Stanach Zjednoczonych AP,
- poprzez finansowanie wspólnych przedsięwzięć, przynoszących korzyści obu stronom, jak na przykład uruchamianie nowych usług.

Dotychczas współpraca z TP SA odbywa się na w pełni komercyjnych warunkach, łącznie z częściowym finansowaniem przez NASK koniecznych prac rozwojowych w telekomunikacji.

- Wreszcie istotnym źródłem finansowania NASK są i mogą być różne fundusze międzynarodowe.

Podobną rolę względem NASK może odegrać i inny operator sieci, który przejmie podstawowe usługi i korzyści wynikające ze współdziałania z NASK. Sądzimy, że ewolucja NASK w kierunku szerokopasmowej sieci bazowej doprowadzi do przekazania wyposażenia operatorowi wykreowanemu dla obsługi wydzielonej grupy użytkowników związanych z budżetem państwa.

Wyżej opisane uwarunkowania ekonomiczne NASK sytuują operatora sieci wobec innych operatorów, a zwłaszcza TP SA. NASK nie konkuruje i nie będzie konkurować z innymi operatorami o masowego klienta. Środowisko, w którym działa NASK wymusza szybki postęp i adaptowanie wszelkich nadających się do zastosowania nowinek. Z natury więc rzeczy NASK poza środowiskiem naukowym będzie dostarczycielem usług nowych, jeszcze nieznanych w sieciach publicznych. Tak samo NASK służy i będzie chętnie służył swoimi doświadczeniami oraz swoimi sieciami jako poligonem doświadczalnym. Z drugiej strony NASK wszędzie, gdzie tylko będzie to możliwe ze względów technicznych i ekonomicznych, chętnie będzie korzystał z usług innych operatorów, zwłaszcza TP SA.

Sieć dzierżawionych łącz jest powiększana tylko w przypadkach ekonomicznie (taniej niż przez POLPAK) uzasadnionych przyłączaniem większych aktywnych zasobów pracujących w sieci INTERNET. Podstawową łączność z rozrzuconymi po kraju mniejszymi uczelniami, instytutami naukowymi oraz oddziałami i filiami instytutów i uczelni chcemy uzyskać poprzez POLPAK. W ten sposób posiadacz komputera osobistego pojedynczego lub włączonego w sieć lokalną będzie mógł stosunkowo tanio uzyskać dostęp terminalowy do podstawowych zasobów i funkcji sieci typowo akademickich.

Ze swojej strony liczymy na współpracę przy podłączaniu do POLPAKu innych nieakademickich użytkowników sieci z instalowaniem sprzętu, wdrażaniem pracy w sieci, szkoleniem itp. usługami wymagającymi znajomości pracy sieci.

Obecnie rozpoczął się proces inwestowania w sieci metropolitalne budowane w zasadzie dla środowiska naukowego. Chociaż budowane są one na ogół w ramach zezwolenia telekomunikacyjnego dla środowiska naukowego, NASK nie chce bezpośrednio być operatorem tych sieci. Wyjątek stanowi Warszawa i WARMAN, ponieważ charakter tej sieci bardziej przypomina sieć rozległą niż lokalną. Przed środowiskiem budującym sieci metropolitalne NASK stawia dwie możliwości:

- samodzielne staranie się o zezwolenie telekomunikacyjne i zawarcie umowy międzyoperatorskiej na tranzyt informacji przez NASK,
- zawarcie umowy na powiernicze pełnienie funkcji operatora w imieniu NASK na podstawie zezwolenia telekomunikacyjnego udzielonego dla NASK.

W dłuższej perspektywie czasu chcemy podstawowe połączenia cyfrowe uzyskać od TP SA w trzech możliwych wariantach:

- Wspólne inwestycje na kanałach 2 Mbps uruchamiające usługi dla obu partnerów z preferencyjnym kosztem użytkowania dla NASK.
- Kanały komutowane w miejskiej i w przyszłości międzymiastowej ISDN pozwalające na dynamiczne dostosowanie przepustowości oraz istnienia połączenia do potrzeb sieci NASK,
- kanały cyfrowe w sieciach o dużej przepustowości (w przyszłości SDH) w miarę potrzeb E1, E2, E3 oraz OC1 uzyskiwane drogą wynajmu lub wspólnych inwestycji z innymi partnerami.

Oczywiście warunkiem wyboru są warunki ekonomiczne i funkcjonalne. Nie wykluczone, że dla podniesienia niezawodności sieci konieczne będzie doprowadzenie połączeń do wszystkich podstawowych węzłów NASK co najmniej przy pomocy linii dwóch operatorów.

5. Formalne i rzeczowe problemy działania NASK jako operatora sieci.

Od września 1992 roku sieć NASK działa na podstawie zezwolenia Ministra Łączności na prowadzenie działalności telekomunikacyjnej. Z tego powodu nastąpiło szereg regulacji prawnych działalności, obsługi sieci oraz korzystania z jej usług. W tym celu został opracowany i wdrożony regulamin wewnętrzny sieci NASK oraz regulamin korzystania z sieci NASK.

Odrębnym problemem jest homologacja urządzeń pracujących w sieci. Dotychczas homologacji podlegały wyłącznie urządzenia pracujące bezpośrednio w liniach publicznych, to znaczy modemy, besebanad'y itp. Homologacja urządzeń zwłaszcza przy przyjaznych stosunkach w Ministerstwie Łączności oraz w Instytucie prowadzącym badania była dla nas korzystna.

Obecnie wobec pojawiania się bardziej zaawansowanych usług jak sieć pakietowa POLPAK, w najbliższym czasie ISDN, wydaje się konieczne wdrożenie homologacji również urządzeń obsługujących i wyższe warstwy protokołów sieciowych. Urządzenia wykonywane przez nas w kraju mogą być łatwo przystosowane do dowolnej sieci pakietowej. Gorzej z urządzeniami produkowanymi poza granicami kraju. Polska jest zbyt małym krajem i ma za słabo rozwinięty przemysł, aby w zakresie produkcji urządzeń mogła być sensownie samowystarczalna. Naszym interesem jest dopasowywać profesjonalnie i w dużych seriach wytwarzane urządzenia do potrzeb użytkownika krajowego.

Odrębnym problemem jest nieprzystosowanie obecnego zezwolenia telekomunikacyjnego do realiów NASK. Nieprzystosowanie to obejmuje trzy zagadnienia:

- nastąpiła zmiana operatora sieci z Uniwersytetu Warszawskiego na przedsiębiorstwo Naukowa i Akademicka Sieć Komputerowa, które przejęło majątek oraz wszelkie zobowiązania w zakresie sieci NASK i WARMAN,
- obecne zezwolenie posiada zbyt sztywny załącznik opisujący konfigurację sieci wobec czego formalnie konieczna jest jego zmiana w ten sposób, aby rozwój sieci NASK nie zmuszał do każdorazowej zmiany załącznika do zezwolenia,
- usługi NASK w ograniczonym zakresie, o czym było poprzednio wykraczają poza obsługę środowiska naukowego i akademickiego i tak będzie w przyszłości co może budzić wątpliwości przy interpretacji zapisów zezwolenia.

Obecnie NASK powierniczo pełni funkcje operatora na podstawie zlecenia Uniwersytetu Warszawskiego.

Mamy nadzieję, że powyższe nieprzystosowania będą w najbliższym czasie usunięte.

Warszawa, lipiec 1994

Struktura łącz w sieci NASK WAN

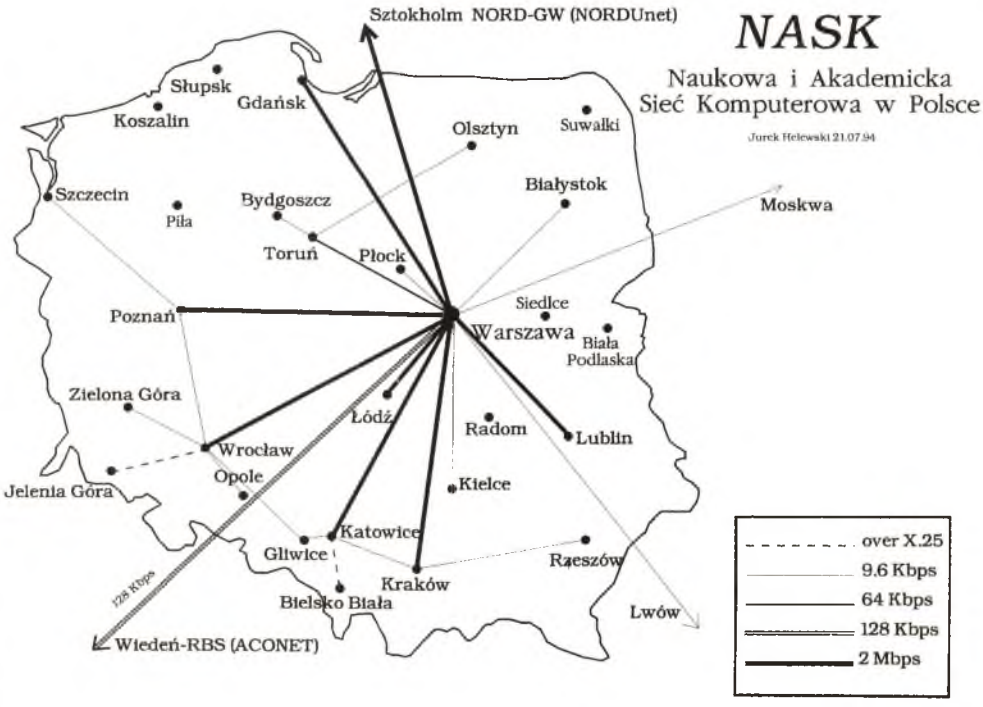
Tadeusz Bieńkowski

Wprowadzenie

Wszelkie usługi sieci NASK opierają się na sieci łącz fizycznych, których opis jest przedmiotem niniejszego referatu. NASK jest siecią szkieletową, dostarczającą usługi dla środowiska naukowego i akademickiego traktowanego jako całość. Wobec tego, nie należą do NASK ośrodki uczelniane, sieci lokalne i tym podobne systemy, zarządzane i obsługiwane w sposób zdecentralizowany. W warstwie łącz do NASK należą natomiast połączenia międzynarodowe, międzyregionalne, międzyuczelniane i międzykampusowe w regionach, oraz wyposażenie łącz dial up, zapewniajace dostęp do sieci pojedyńczemu użytkownikowi.

Sieć NASK obejmuje obszar Polski i jest podzielona na dziesięć regionów:

Stołeczny	Warszawa, Białystok, Płock, Kielce.
Dolnośląski	Wrocław, Opole, Jelenia Góra, Zielona Góra.
Górnośląski	Katowice, Gliwice, Częstochowa, Bielsko Biała.
Lubelski	Lublin, Rzeszów, Puławy.
Łódzki	Łódź
Małopolski	Kraków.
Pomorski	Toruń, Bydgoszcz, Olsztyn.
Wielkopolski	Poznań.
Gdański	Gdańsk, Gdynia.
Zachodniopomorski	Szczecin.



W ostatnim okresie występował bardzo szybki rozwój sieci łącz NASK. Powstały nowe subregiony i nowe połączenia międzynarodowe . Uruchomiono także dodatkowe linie obejściowe . Jeszcze większy postęp nastąpi w zakresie szybkości łącz i jakości ich pracy . Łącza analogowe, o ograniczonym ze swej natury paśmie, są zastępowane szybkimi łączami cyfrowymi o wysokiej niezawodności. Poniżej zostanie przedstawiona struktura łącz Naukowej i Akademickiej Sieci Komputerowej, w nawiązaniu do historii jej rozwoju.

Istnieją następujące łącza międzyregionalne i międzynarodowe:

1. Łącza analogowe dzierżawione od Telekomunikacji Polskiej SA

Warszawa	- Białystok
Warszawa	- Płock
Warszawa	- Kielce
Poznań	- Wrocław
Katowice	- Kraków
Toruń	- Bydgoszcz
Toruń	- Olsztyn
Katowice	- Gliwice
Poznań	- Szczecin
Rzeszów	- Kraków
Wrocław	- Opole
Gliwice	- Wrocław
Wrocław	- Zielona Góra
Warszawa	- Lwów
Warszawa	- Moskwa

Obecnie zestawiane jest łącze międzynarodowe Warszawa - Mińsk.

W skład tych łączy najczęściej wchodzą:
- dwa tory, oddzielny dla nadawania i odbioru,
- modemy synchroniczne V.29 9600 bit/s,
- multipleksery statystyczne DM 404 produkcji MEMOTEC w Kanadzie.

W zasadzie wszystkie analogowe łącza międzyregionalne, a także część regionalnych jest multipleksowana. W naturalnie wieloprotokołowej sieci naukowej i akademickiej, multipleksacja była w początkowym okresie rozwiązaniem tańszym niż mnożenie łącz, lub przekładanie transmisji z różnych protokołów na jeden, na przykład X.25. W sieci NASK obsługiwane były cztery protokoły:

X.25 dla sieci pakietowych,
TCP/IP dla sieci INTERNET łączącej sieci lokalne,
BSC/SNA duże komputery IBM,
DECNET maszyny VAX.
Obecnie, dwa ostatnie protokoły praktycznie zanikają.

Multipleksery są rodzajem specjalizowanych komputerów, umożliwiających wprowadzenie w każde z łączy czterech niezależnych kanałów, oddzielnego dla każdego protokołu komunikacyjnego. Styki portów spełniają zalecenia CCITT V.24, V.28. Każdy port charakteryzuje się maksymalną szybkością transmisji 19200 bit/s. Multipleksery stosują sprzętową kompresję danych na wyjściu. Przesyłają dane za pomocą protokołu zbliżonego do HDLC.

Multipleksery posiadają rozbudowany system kontroli i statystyki pracy łączy. W tym celu, korzysta się z komputera IBM PC XT z zainstalowanym programem DCC. Jest on połączony przez specjalne sterowniki z portami konsoli multiplekserów. Program ten umożliwia połączenie się z każdym multiplekserem w sieci, sprawdzenie lub zmianę jego konfiguracji i obejrzenie statystyki poszczególnych portów. Program sygnalizuje sytuacje awaryjne, np: uszkodzenie linii, większą od założonej ilość błędów transmisji, wypełnienie łącza większe od przyjętego itp. Zapisuje także w sposób ciągły w specjalnym zbiorze występowanie takich sytu-

acji z podaniem daty i godziny. Powyższe możliwości pozwalają zarządzać siecią z jednego miejsca, przez obsługę o najwyższych kwalifikacjach, co jest olbrzymią zaletą.

Obecnie jednak, przy przechodzeniu na szybkie i niezawodne połączenia cyfrowe, wraz z nowymi możliwościami technicznymi, zostaje zmieniona technologia obsługi występujących w NASK protokołów komunikacyjnych. Regułą jest odejście od multipleksacji łącz. Podstawowym staje się protokoł TCP/IP, natomiast X.25 i SDLC są tunelowane przez IP. Niestety, brak jest takiej możliwości dla protokołu BSC i musi on być zastąpiony innym.

2. Cyfrowe łącza satelitarne

Szybkość transmisji 9600 b/s stosowana na łączach analogowych, jest stanowczo zbyt niska. Szczególnie w sieci INTERNET występują duże strumienie danych, które blokują łącza. Problem ten lawinowo narasta wraz z rozwojem sieci, oraz wzrostem przesyłań danych typu obrazów. Obecnie pojawiły się wprawdzie modemy pracujące z szybkością 28.8 kbps. Jednak są one przeznaczone głównie dla łącz wykorzystujących trakty PCM. Nie jest to także rozwiazanie z przyszłością. Radykalne zwiększenie szybkości w stosunkowo prosty sposób umożliwiają łącza satelitarne. Należy liczyć się jednak z pewnymi wadami wynikającymi z ich istoty, a mianowicie:

a/ wnoszą duże opóźnienie transmisji wynoszące ok. 0.3s w jednym kierunku,
b/ istnieje wpływ warunków atmosferycznych na pracę łącza,
c/ dla pewnych typów satelitów, korzystających tylko z baterii słonecznych występuje wpływ cienia Ziemi, co obiawia się brakiem zasilania satelity około północy czasu lokalnego w okresach równonocy.

Pierwsza z wymienionych wad jest bardzo istotna. Protokoły komunikacyjne opracowane dla niewielkich opóźnień transmisji na łączach, źle pracują w takich warunkach. Nie mogą doczekać się na potwierdzenie prawidłowości transmisji i ponawiają ją. Można temu w pewnym sensie zaradzić następującymi sposobami:

a/ Wydłużając czas oczekiwania na potwierdzenie, co powoduje jednak znaczne spowolnienie pracy,
b/ zmienić długość okna z 8 na np. 128 ramek,
c/ najbardziej radykalnym sposobem jest rezygnacja z potwierdzeń i przeniesienie kontroli do wyższych warstw sieci.

Na stan pogody użytkownik ma wpływ minimalny. Silne opady deszczu mogą powodować tłumienie mikrofal, do poziomu poniżej dopuszczalnego. Padający śnieg jest mniej groźny.Stosuje się jednak podgrzewanie czaszy anteny w okresie zimowym, aby uniknąć szkodliwego oblodzenia.

Obecnie istnieją cyfrowe łącza satelitarne w relacjach:
Warszawa - Sztokholm 2 Mb/s
Warszawa - Toruń 64 kb/s

Do obsługi obu połączeń, na terenie Uniwersytetu Warszawskiego, bezpośrednio przy centralnym węźle NASK, została zainstalowana antena satelitarna nadawczo-odbiorcza. Druga antena jest w Toruniu na dachu Uniwersytetu Mikołaja Kopernika. Trzecia po stronie szwedzkiej w Wyższej Szkole Technicznej w Sztokholmie.

Łącze Warszawa - Sztokholm jest multipleksowane. TDM multiplekser typu IDM-200 wydziela z pasma 2048 kb/s kanały: 1792 kb/s dla Internetu, 64 kb/s dla X.25, oraz kanał 64 kb/s dla X.75. Pozostałe pasmo służy synchronizacji i kontroli systemu.

W trakcie zestawiania są połączenia satelitarne 64 kb/s do Lwowa, Mińska i Moskwy. Przewidziane jest oddanie do eksploatacji łącza do Lwowa na przełomie sierpnia i września br.

3. Cyfrowe łącza Telbanku

Sieć teletransmisyjna TELBANK dysponuje międzymiastowymi łączami radiowymi o przepływności całkowitej do 4x2 Mb/s. NASK wykorzystywał (dzierżawił) połączenia o szybkościach 64 kb/s w relacjach:
Warszawa - Wrocław
Warszawa - Kraków *
Warszawa - Poznań
Warszawa - Lublin *

Zakończenia łączy telbankowych zlokalizowane są w bankach. Lokalne połączenia pomiędzy siecią TELBANK a węzłami sieci NASK sa zrealizowane na dzierżawionych liniach dwuparowych, wyposażonych w konwertery MIL 2x48k o szybkości 64 kbps, produkcji GORAMO w Warszawie.

Obecnie, jesteśmy w trakcie zestawiania łącz 2 Mb/s w w/w relacjach, eksploatowanych wspólnie z TPSA, które zastąpia połączenia dzierżawione od TELBANKU.

Łącza oznaczone gwiazdką są już zlikwidowane.

4. Łącza cyfrowe oferowane przez TP SA.

W związku z realizacją przez TPSA łączy cyfrowych o przepływności 140Mb/s w relacjach międzymiastowych, planowane jest dzierżawienie od TPSA łączy o przepływności 64kb/s lub więcej.

Obecnie sa zestawione łącza:

Warszawa	- Wiedeń	128 kb/s	
Warszawa	- Katowice	2 Mb/s	
Warszawa	- Gdańsk	2 Mb/s	
Warszawa	- Kraków	2 Mb/s	
Warszawa	- Łódź	2 Mb/s	
Warszawa	- Poznań	2 Mb/s	
Warszawa	- Lublin	2 Mb/s	
Warszawa	- Wrocław	2 Mb/s	
Warszawa	- Bydgoszcz	2 Mb/s	
Poznań	- Szczecin	2 Mb/s	obecnie zestawiane.

Trakty E1 - 2 Mb/s kończą się stykiem symetrycznym G-703 w centralach cyfrowych TPSA. Na mocy specjalnego porozumienia NASK - TPSA, w tych centralach zostały urządzone węzły NASK. Zostały one wyposażone w wieloportowe routery CISCO. Przejście ze styku G-703 na V-35, typowy dla w/w routerów, zapewniają adaptery GORAMO

W niedalekiej przyszłości, zamierzane jest objęcie wszystkich subregionów NASK dla których istnieją warunki techniczne, tego typu połączeniami, i stworzenie przez to sieci szkieletowej 2 Mb/s. W dalszej przyszłości, szybkość zostanie zwiększona do 34 Mb/s.

5. Połączenia poprzez publiczną sieć pakietową POLPAK.

Przyłączanie nowych subregionów, takich jak np. Bielsko Biała, Rzeszów, Olsztyn, Jelenia Góra, realizowane jest poprzez sieć pakietową POLPAK. Rozwiązanie takie dla środowisk, które w początkowym okresie nie generują dużego ruchu, jest najbardziej uzasadnione ekonomiczne. Łącze do sieci POLPAK jest wyposażane przez NASK w urządzenia, które w podstawowej wersji umożliwiają obsługę do 11 użytkowników, grupowych bądź indywidualnych.

6. ISDN (Integrated Service Digital Network)

Rozwój nowoczesnych technologii w dziedzinie telekomunikacji, szczególnie poprzez jej cyfryzację, pozwala uzyskać zintegrowaną sieć cyfrową ISDN. Oznacza to, że połączone zostają usługi: telefoniczne, przesyłania danych, telemetrii, sygnalizacji i inne. Ponieważ przetworzony bez specjalnych zabiegów na postać cyfrową sygnał mowy zajmuje kanał 64kb/s, abonentowi przydziela się kilka kanałów cyfrowych. Stosowany jest system 2B+D, przy czym:

B = 64kbps użytkowe

D = 16kbps dla telemetrii i sygnalizacji

W chwili pojawienia się w ofercie publicznego operatora takiej usługi, abonent ISDN będzie mógł połączyć się z siecią NASK i pracować z jej zasobami. Odczuwał będzie, jakby pracował na szybkim łączu dzierżawionym, natomiast płacił będzie operatorowi za efektywny czas połączenia. Będzie to następna, obok dołączenia się do budowanych układów MAN'owskich, możliwość dostępu dla końcowych abonentów do NASK.

Tego typu połączenia, wydają się jednak odpowiednie tylko dla indywidualnych użytkowników lub niewielkich instytucji.

ŁĄCZA REGIONALNE

Łącza regionalne obsługują w zasadzie teren w promieniu kilkunastu kilometrów. Można je podzielić na dwa rodzaje:

1. Analogowe

Są utworzone jedynie z toru miedzianego, bez jakichkolwiek urządzeń pośredniczących, a w szczególności wzmacniaków. Łącza takie nazywają się naturalnymi. Ze względu na ich szerokopasmowość można stosować proste i tanie modemy GORAMO BpH 2x9600. Umożliwiają one transmisję asynchroniczną lub synchroniczną z szybkością do 9600 bitów/s po jednym torze, kanałami na różnych częstotliwościach. Ich zasięg wynosi ok. 10 km. Przy większych odległościach lub bardzo złych liniach stosowane są modemy DA 296 produkcji MEMOTEC działające w kanale 0.3 - 3.4 kHz z szybkością 9600b/s. Problem zwiększenia szybkości transmisji dotyczy także łączy regionalnych. W tym celu stosowane są konwertery MIL 2X48k produkcji GORAMO lub RAD pracujące z szybkością 64kb/s, na dwóch lub w przypadku niektórych modeli jednej parze galwanicznej. Ich zasięg wynosi 5 do 15 km.

Stosując bardziej skomplikowane modemy można uzyskać transmisję z szybkością 2Mb/s na odległość ok 5 km., czego przykładem jest połączenie Cyfronetu do węzła NASK w Krakowie, za pomocą modemów firmy Teleindus.

2. Cyfrowe

Obecnie są zestawione w Warszawie dwa łącza cyfrowe 2 Mb/s, wykorzystujące światłowodową sieć TPSA w relacjach:

1/ NASK Węzeł Centralny ul.Krakowskie Przedmieście 26 - CRiT ul. Barbary,

2/ CRiT ul. Barbary 2 - NASK Węzeł Ochota ul. Banacha 2.

W zasadzie, łącza te są podobne do międzymiastowych, jednak na części przebiegu pracują na parach miedzianych, gdzie stosuje się konwertery (modemy) i regeneratory RAD. Podobne łącza powstaną w innych regionach.

Planowane było, wykorzystanie krotnic PCM dla uzyskania lokalnych łączy 64 kb/s, pomiędzy Węzłem Centralnym NASK a centralą cyfrowa przy ul. Pięknej, które mogły by być wykorzystane przez pobliskich użytkowników sieci NASK.

3. Sieci MAN

W/w tradycyjne metody dołączenia użytkowników w aglomeracjach miejskich, ewoluuje w kierunku tworzenia sieci metropolitalnych MAN. Tworzą one szybki, np. 155 Mb/s, szkielet łączności w mieście, do którego dołączają się użytkownicy. MANy natomiast dołączone są do węzłów NASK, co zapewnia ich łączność z siecią krajową i światową. Przykładem tego jest budowana obecnie, Warszawska Miejska Sieć Światłowodowa WARMAN.

ŁĄCZA KOMUTOWANE

Następnym, specyficznym rodzajem są łącza na liniach komutowanych (dial up). W każdym węźle regionalnym NASK są, lub w najbliższym czasie będą zainstalowane modemy, na miejscowych liniach telefonicznych. W centralnym węźle NASK w Warszawie, modemy są dołączone do linii miejskich o numerach: 26-23-22, 26-80-07, 26-80-08 i 26-80-09. Na ogół są stosowane modemy produkcji kanadyjskiej Memotec Dial Access 296, pracujące z szybkościami 1200 - 9600 b/s. Posiadają sprzętową korekcję błędów i kompresję danych według protokołów MNP 2, 3, 4 i 5. Dla przykładu, stosując MNP 4, poprzez przesyłanie wydłużonych ramek i redukcję długości nagłówków, osiąga się przy 9600 b/s ekwiwalentną szybkość transmisji ok. 11600 b/s. Dla MNP 5 szybkość ta wzrasta do 19200 b/s. Inne używane modemy to DA 3214 pracujące z prędkością do 14400 b/s i protokołem V42 bis oraz niższymi.

Po stronie użytkowników stosowane są modemy SCAN 245E, Everex 24E+, DA296, Zyxel, GVC oraz inne. Modemy stosują ogólnie przyjęty standard rozkazów Hayes.

Z łączy komutowanych korzystają użytkownicy nie posiadający rozbudowanych systemów komputerowych, oraz dużych potrzeb w zakresie korzystania z sieci. Są to najczęściej użytkownicy indywidualni, posiadający pojedyńczy mikrokomputer w pracy lub w domu.

Należy jednak stwierdzić, że jakość połączeń komutowanych nie jest jednolita. Są miejsca oraz okresy, kiedy praca na łączach komutowanych jest trudna lub wręcz niemożliwa. Wobec tego, przed zdecydowaniem się na ten rodzaj łączności, konieczne jest wykonanie prób.

Warszawa, lipiec 1994r.

Wieloprotokołowość w sieci NASK.

Tadeusz Wiśniewski

Sieć komputerowa NASK powstała dla obsługi potrzeb środowiska naukowego i akademickiego. Sieć ta od początku swego istnienia musiała być siecią wieloprotokołową w celu zaspokojenia różnorodnych wymagań ze strony środowiska. W swych początkach (rok 1990) sieć NASK tworzyły dwie sieci - sieć X.25 oraz sieć EARN/BITNET. W drugiej połowie 1991 roku nastąpił bardzo gwałtowny rozwój sieci INTERNET opartej o protokół TCP/IP, a niedługo później w sieci NASK pojawiły się komputery tworzące krajową sieć DECNet. Wymienione powyżej sieci wykorzystywały dokładnie te same łącza fizyczne na poszczególnych relacjach międzymiastowych (początkowo o przepustowości 9600bps). Tak więc na określoną topologię łączy fizycznych były nałożone cztery sieci logiczne komunikujące się według następujących protokołów :

- X.25 (HDLC) dla sieci X.25
- BSC dla sieci EARN
- TCP/IP (SLIP oraz HDLC) dla sieci INTERNET
- DDCMP dla sieci DECNet.

Tego typu operacja była możliwa po wyposażeniu każdego międzymiastowego łącza fizycznego w parę tzw. czterokanałowych multiplekserów statystycznych, których kanały mogły być konfigurowane dla transmisji różnych protokołów.

Kolejnym krokiem przeprowadzonym w sieci NASK było stopniowe przechodzenie z wieloprotokołowej sieci szkieletowej w kierunku jednoprotokołowej sieci szkieletowej opartej o protokół TCP/IP. Z punktu widzenia użytkowników sieć NASK jest nadal postrzegana jako sieć wieloprotokołowa, gdyż użytkownicy mają możliwość dołączenia się do sieci X.25, EARN oraz DECNet, które tworzą tzw. sieci wirtualne położone na sieci TCP/IP. Oznacza to, że informacja właściwa dla sieci X.25, EARN oraz DECNet jest przenoszona przez sieć szkieletową za pomocą protokołu TCP/IP. Obecnie niektóre regionalne łącza międzymiastowe nadal są wyposażone w multipleksery statystyczne umożliwiające dzielenie łącz fizycznych przez sieci poszczególne NASK.

1. Sieć X.25.

Sieć X.25 NASK jest siecią otwartą umożliwiającą nawiązywanie połączeń typu terminal-terminal, terminal-host oraz host-host. Intensywny rozwój sieci X.25 NASK rozpoczął się w roku 1990 i związany jest z pojawieniem się możliwości połączenia z duńską publiczną siecią pakietową DATAPAK oraz oferowania użytkownikom dostępu do światowych serwisów informacyjnych i baz danych. W latach poprzednich sieć X.25 była projektowana i rozwijana min. w ramach programu CPBR 8.13 pod nazwą "Krajowa i Akademicka Sieć Komputerowa". Wówczas to uruchomiono pilotową sieć X.25 oraz opracowano urządzenia dla sieci X.25 (węzły, koncentratory terminali, procesory czołowe).

1.1. Urządzenia sieci X.25 NASK.

W sieci X.25 NASK pracują obecnie następujące typy urządzeń :
- węzły
- koncentratory terminali
- gateway'e

a) węzły

W sieci X.25 NASK wykorzystywane są dwa typy węzłów X.25 produkcji Memotec (Kanada) typu MP9500 oraz SP9700. Węzło-pad SP9700 posiada w zależności od ilości kart 6, 12 lub 18 portów użytkownika. Węzeł X.25 typu MP9500 może być skonfigurowany w wersji od 6-ciu do maksymalnie 54-ch portów użytkownika. Te dwa typy węzłów umożliwiają wykorzystanie następujących rodzajów usług (poza wyborem drogi i komutacją pakietów) :

- definiowanie Closed User Group z nieograniczoną liczbą połączonych urządzeń typu DTE

- definiowanie Bilateral Closed User Group obejmującej tylko dwa urządzenia typu DTE
- definiowanie gateway'a umożliwiającego połączenie z siecią posiadającą inną strukturę adresacji
- tworzenie trwałych połączeń wirtualnych
- monitoring stanu sieci i poszczególnych połączeń
- rejestracja ilości i czasu trwania połączeń poszczególnych użytkowników
- zdalne konfigurowanie węzła

b) koncentratory terminali

Obecnie w sieci X.25 NASK wykorzystywane są dwa typy koncentratorów terminali. Pierwszym z nich jest koncentrator firmy Memotec typu SP 8300 pracujący w/g protokołów X.25, X.3, X.28, X.29. W wersji minimalnej obsługuje on jeden port sieci X.25, jeden port operatorski STP oraz cztery asynchroniczne porty użytkownika. Istnieje możliwość rozszerzenia ilości portów o dalsze 6 lub 12 portów użytkownika. Jako koncentrator terminali może również pracować wspomniany wcześniej węzło-pad SP 9700 (poszczególne porty SP9700 są definiowane jako asynchroniczne PAD).

c) gateway'e międzysieciowe

W eksploatacji znajdują się dwa typy gateway'ów : N1500 szwedzkiej firmy Data Delecta oraz Access Server XL/Starmaster kanadyjskiej firmy Gandalf.

1.2. Połączenia w sieci X.25 NASK.

Sieć X.25 NASK posiada połączenia z sieciami DATAPAK, POLPAK oraz CUPAK.

Sieć DATAPAK jest szwedzką publiczną siecią pakietową X.25. Połączenie sieci NASK z DATAPAKiem umożliwia użytkownikom NASK nawiązywanie połączeń międzynarodowych i gwarantuje użytkownikom spoza Polski dostęp do zasobów oferowanych w sieci NASK. Obecnie zestawione są dwa łącza X.25 z siecią DATAPAK : łącze abonenckie o przepustowości 9600bps oraz łącze międzyoperatorskie o przepustowości 64kbps będące w trakcie testów eksploatacyjnych. Sieć POLPAK jest również publiczną siecią pakietową X.25. Jest ona własnością przedsiębiorstwa Telekomunikacja Poska S.A. Współpraca z nią umożliwia łatwe i tanie włączanie do sieci NASK tych ośrodków naukowych i akademickich, do których z różnych względów nieopłacalne ekonomicznie jest zestawianie łącz dzierżawionych. Sieć X.25 NASK jest połączona z siecią POLPAK w kilku punktach łączami abonenckimi o przepustowości 9600bps oraz łączem międzyoperatorskim o przepustowości 9600bps, a w przyszłości 64kbps będącym w trakcie testów eksploatacyjnych. Sieć CUPAK jest prywatną siecią pakietową X.25 obejmującą swym zasięgiem centralne urzędy administracji państwowej RP. Jest ona z punktu widzenia adresacji abonentem sieci X.25 NASK. W niedalekiej przyszłości planowane jest uruchomienie łącza międzyoperatorskiego pomiędzy sieciami X.25 NASK i CUPAK.

Z punktu widzenia adresacji sieć X.25 NASK jest prywatną podsiecią sieci DATAPAK (dla połączeń nawiązywanych przez łącze abonenckie) jak i POLPAK. W przypadku łącza międzyoperatorskiego z DATAPAK sieć X.25 NASK jest identyfikowana przez swój własny międzynarodowy DNIC - 2602. W ramach 15-to znakowego wewnętrznego adresu w sieci POLPAK (łącza abonenckie) sieć NASK wykorzystuje 7-mio znakową wolną przestrzeń adresową, natomiast w ramach DATAPAKu (łącze abonenckie) 6-cio znakową. W sieci X.25 NASK została przyjęta następująca struktura adresu (rys. 1): adres składa się z 7-miu znaków, przy czym pierwszy jest numerem identyfikacyjnym sieci NASK w Polsce, drugi jest numerem strefy, trzeci jest numerem węzła sieci X.25 w danej strefie (dla głównego węzła danej strefy przyjęty został numer 0). Kolejne dwa znaki są numerem urządzenia końcowego, a ostatnie dwa znaki są numerem terminala podłączonego do urządzenia końcowego (np. koncentratora terminali). Dokładny opis sposobów adresowania w sieci X.25 NASK został przedstawiony w Dodatku.

1.3. Struktura sieci X.25 NASK.

Centralnym urządzeniem sieci X.25 NASK jest 42-portowy węzeł firmy Memotec typu MP 9500 zainstalowany w centralnym węźle NASK w budynku Centrum Informatycznego Uniwersytetu Warszawskiego (ul. Krakowskie Przedmieście). Posiada on połączenia z sieciami DATAPAK, POLPAK, CUPAK, z 18-portowymi węzłami strefowymi NASK typu MP9500 zainstalowanymi we Wrocławiu, Poznaniu, Gliwicach, Gdańsku, Krakowie i Toruniu, 18-to portowymi węzłami typu MP9500 regionu warszawskiego w Łodzi i Lublinie, 12-to portowymi węzłami typu SP9700 w Białymstoku, Płocku, Politechnice Warszawskiej i IMiGW, 18-to portowy węzeł typu MP9500 w Szczecinie został dołączony do węzła w Poznaniu, natomiast 12-to portowy

węzeł typu SP9700 w Opolu do węzła strefowego we Wrocławiu. Dodatkowo do węzłów strefowych i regionalnych we Wrocławiu, Poznaniu, Szczecinie, Gliwicach i Krakowie dołączono 12-to portowe węzło-pady typu SP9700 posiadające porty obsługujące protokół PADa (X.3, X.28, X.29). W podregionach NASK obejmujących Zieloną Górę, Rzeszów, Olsztyn i Bielsko Białą zostały zainstalowane 12-to portowe węzło-pady typu SP9700 dołączone do publicznej sieci pakietowej POLPAK. Schemat połączeń sieci X.25 NASK przedstawiony jest na rys. 2.

2. Sieć EARN.

Sieć EARN (European Academic & Research Network) tworzą komputery połączone ze sobą za pomocą sieci TCP/IP lub bezpośrednio ze sobą punkt-punkt za pomocą protokołu BSC. Węzły sieci EARN są obecnie zainstalowane w następujących miastach :

- Warszawa – Uniwersytet Warszawski (PLEARN, PLWAUW61), Politechnika Warszawska (PLWATU21), Instytut Fizyki PAN (PLANIF61)
- Łódź – Uniwersytet Łódzki (PLUNLO51)
- Białystok – Politechnika Białostocka (PLBIAL11)
- Toruń – Uniwersytet Mikołaja Kopernika (PLTUMK11)
- Lublin – Uniwersytet Marii Curie-Skłodowskiej (PLUMCS11)
- Poznań – Uniwersytet Adama Mickiewicza (PLPUAM11), Politechnika Poznańska (PLPOTU11)
- Szczecin – Uniwersytet Szczeciński (PLSZUS11)

Węzeł sieci EARN - PLEARN pełni funkcję krajowego węzła sieci EARN. Jest on połączony z krajowymi węzłami w Rosji (SUEARN2), Szwecji (SEARN), Austrii (AEARN). Sieć EARN jest siecią wirtualną położoną na bazowej sieci szkieletowej TCP/IP, komputery w Szczecinie, Wrocławiu i Białymstoku są nadal dołączone do sieci EARN za pomocą protokołu BSC. Schemat połączeń w sieci EARN pokazano na rysunku 3.

3. Sieć INTERNET.

Sieć INTERNET jest przedstawiona w opracowaniu pt. "Internet w Polsce".

4. Sieć DECNet.

Krajową sieć DECNet w ramach sieci NASK tworzą komputery typu VAX, które są połączone ze sobą w sieć za pomocą protokołu firmowego DECNet w następujących miastach :

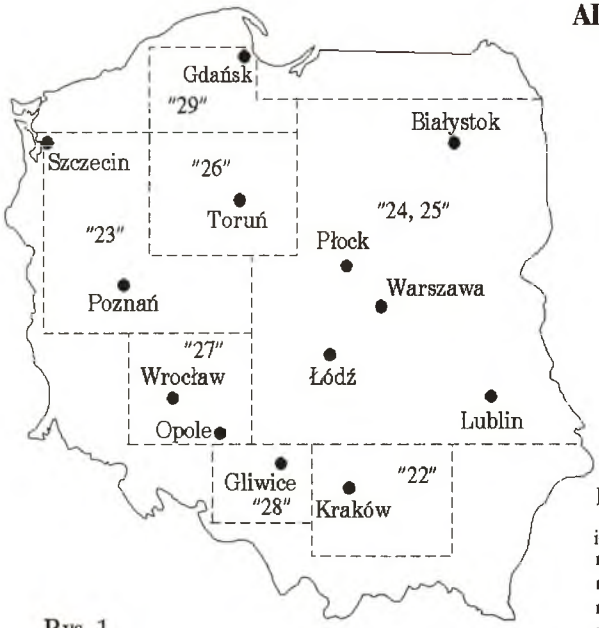
- Warszawa – NASK, KBN, Uniwersytet Warszawski
- Łódź – Politechnika Łódzka, Uniwersystet Łódzki
- Gliwice – Politechnika Śląska
- Wrocław – Politechnika Wrocławska

Sieć DECNet podobnie jak i sieć EARN w pewnym swym fragmencie jest widziana jako sieć wirtualna posadowiona na bazowej sieci szkieletowej TCP/IP, komputery w Krakowie i Gliwicach są połączone ze sobą za pomocą protokołu DDCMP. Schemat połączeń w sieci DECNet pokazano na rysunku 4.

5. Gateway'e w sieci NASK.

Jak już zostało wcześniej powiedziane sieć NASK jest siecią wieloprotokołową. Umożliwia ona użytkownikom dołączanie komputerów pracujących w/g różnych protokołów sieciowych, a także dostęp do usług oferowanych na świecie przez różnych operatorów i dostarczycieli usług. Aby umożliwić użytkownikom dołączonym do jednej określonej sieci dostęp do zasobów oferowanych tylko i wyłącznie w innej sieci, w sieci NASK zostały zainstalowane gateway'e międzysieciowe.

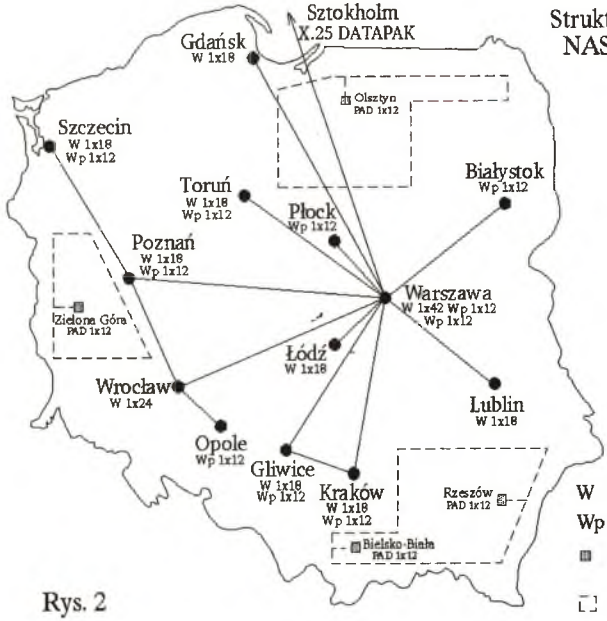
ADRESACJA SIECI X.25



Format adresu: 2-S-W-DD-TT

- identyfikator sieci
- numer strefy
- numer węzła
- numer DTE
- numer terminala

Rys. 1



Struktura połączeń sieci NASK X.25 w Polsce

9.6 Kb/s

W - Węzeł sieci X.25

Wp - Węzłopad sieci X.25

- Koncentrator (PAD) sieci X.25

- połączenie przez POLPAK

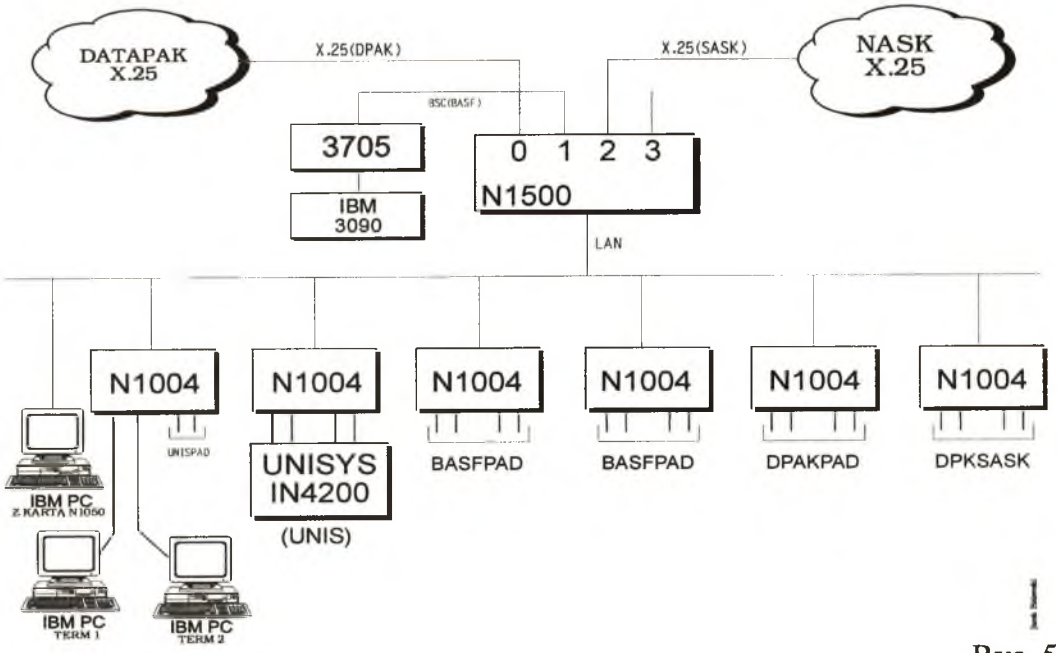
Rys. 2


Sztokholm
SEARN
Struktura połączeń sieci
EARN w Polsce
Szczecin
PLSZUS11
Toruń
PLUMK11
Białystok
PLBIAL11
Poznań
PLPUAM11
PLPOTU51 (BSC)
Moskwa
SUEARN2
Warszawa
PLEARN
PLWALW61 TCP/IP)
PLWATU21 (BSC)
PLANIF61 (BSC)
Łódź
PLUNLO51
Lublin
PLUMCS11
PLUMCS12 (BSC)
połączenie za pomocą
protokołu BSC
połączenie za pomocą
protokołu TCP/IP
Wiedeń
AEARN

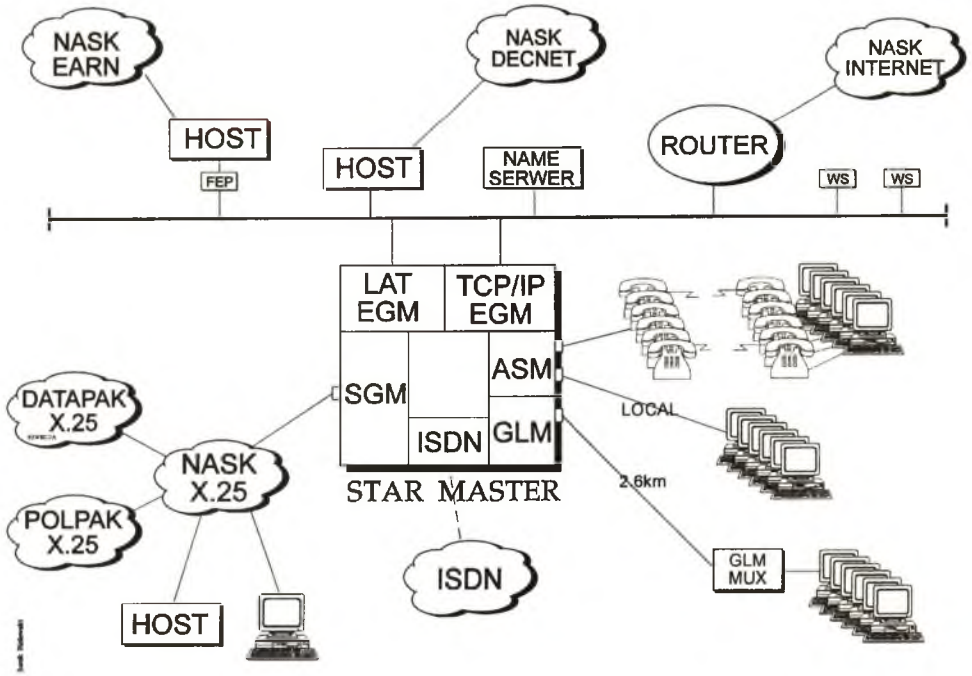
Rys. 3


Struktura połączeń sieci
DECNet w Polsce
Warszawa
Łódź
Wrocław
Gliwice
połączenie za pomocą
protokołu DDCMP
połączenie za pomocą
protokołu TCP/IP

Rys. 4


DATAPAK X.25
X.25(DPAK)
X.25(SASK)
NASK X.25
BSC(BASF)
3705
IBM 3090
0 1 2 3
N1500
LAN
N1004
N1004
N1004
N1004
N1004
N1004
UNISPAD
UNISYS IN4200
(UNIS)
BASFPAD
BASFPAD
DPAKPAD
DPKSASK
IBM PC
Z-KARTA N1050
IBM PC
TERM 1
IBM PC
TERM 2

Rys. 5


NASK EARN
NASK DECNET
NASK INTERNET
HOST
FEP
HOST
NAME SERWER
ROUTER
WS
WS
LAT EGM
TCP/IP EGM
SGM
ASM
ISDN
GLM
STAR MASTER
LOCAL
2.6km
DATAPAK X.25
NASK X.25
POLPAK X.25
HOST
ISDN
GLM MUX

Rys. 6

5.1 System Netlan N1500 w sieci NASK.

W marcu 1990 roku Rada Dyrektorów sieci EARN jednogłośnie przyjęła Polskę do sieci EARN. Niedługo później bo od lipca 1990 roku zaczął w CIUW oficjalnie funkcjonować krajowy węzeł sieci EARN - PLEARN. W celu udostępnienia usług sieci EARN jak najszerszemu gronu użytkowników zdecydowano się na wykorzystanie istniejącej już sieci X.25 rozwijanej od wielu lat w ramach programu CPBR 8.13. Została nawiązana współpraca ze szwedzką firmą DATA DELECTA AB sprzedającą systemy Netlan N1500, mogące spełniać między innymi funkcję gateway'a pomiędzy siecią EARN, a siecią X.25.

System Netlan N1500 został zaprojektowany w celu umożliwienia użytkownikom pracy z różnych typów terminali z różnymi typami komputerów. Podstawowym elementem systemu Netlan N1500 jest urządzenie - węzeł N1500, do którego przez porty szeregowe mogą być dołączane komputery komunikujące sił w/g następujących protokołów:

- IBM SNA/SDLC
- BSC - emulacja jednostki grupowej IBM 3270
- UNISCOP - UNIVAC UTS 4020
- Siemens MSV1 - 9750 MSV1 MSF 8171
- Bull VIP - Honeywell VIP 7800
- ICL CO3 - BURROUGHS poll/select
- X.25 - wraz z protokołem PAD (X.3, X.28, X.29)

Terminale dołączane są do systemu Netlan N1500 za pośrednictwem urządzeń N1004 (urządzenia te komunikują się z węzłem N1500 za pomocą sieci LAN - ARCNET lub ETHERNET). Dostępne są następujące emulatory terminali:

- Norsk Data VT100
- Data General, DG 461 terminal
- Data Point, DP 8220 terminal
- Tandberg TDV/1200, TDV2200/9, TDV2231, TDV2240/1, TDV2240/2, TDV2240/3, TDV2240/4,
- VT100, VT220

System Netlan N1500 umożliwia także dostęp do dowolnego komputera w systemie z sieci X.25.

System Netlan N1500 do marca 1992 roku pełnił funkcję gateway'a pomiędzy siecią X.25 NASK, a duńską siecią X.25 DATAPAK, umożliwiał dostęp z sieci X.25 do komputera IN4200 pracującego pod systemem operacyjnym UNIX oraz dostęp z sieci X.25 do komputera IBM 3090 pełniącego funkcję krajowego węzła sieci EARN - PLEARN.

Konfiguracja systemu Netlan N1500 zainstalowanego w centralnym węźle NASK do marca 1992 roku została przedstawiona na rysunku 5.

W marcu 1992 roku po zainstalowaniu gateway'a Gandalf STARMASTER system Netlan N1500 został odłączony od sieci X.25 DATAPAK, a także zostało zlikwidowane połączenie z komputerem IN4200. Obecnie umożliwia on dostęp do komputera IBM 3090 (węzeł PLEARN) z sieci pakietowej X.25 NASK. Systemy Netlan N1500 o podobnych funkcjach zostały zainstalowane również we Wrocławiu oraz w Lublinie.

5.2. Access Server XL/STARMASTER w sieci NASK.

W drugiej połowie 1991 roku nastąpił gwałtowny rozwój sieci INTERNET w Polsce opartej o protokół TCP/IP stwarzając użytkownikom możliwość połączenia się z dowolnymi komputerami sieci INTERNET w świecie. Równocześnie została w Polsce uruchomiona w wielu ośrodkach akademickich sieć DECNET. W tym momencie pojawiła się oczywista konieczność zakupu i instalacji urządzenia umożliwiającego wykonywanie dodatkowych połączeń międzysieciowych. W lutym 1992 roku w centralnym węźle NASK został zainstalowany ACCESS SERVER XL/STARMASTER kanadyjskiej GANDALF INFOTRON. STARMASTER może pełnić funkcję gateway'a pomiędzy następującymi sieciami:

- INTERNET - protokół TCP/IP lub SLIP
- DECNET - protokół LAT
- X.25 - protokół X.25 oraz PAD (X.3,X.28,X.29)
- firmową siecią IBM - protokół SNA/SDLC

Oznacza to, że użytkownik pracujący na terminalu dołączonym do STARMASTERA lub do jednej z wymienionych powyżej sieci może korzystać z zasobów udostępnianych w pozostałych sieciach. Urządzenie STARMASTER cechuje modułowa budowa ułatwiająca rozbudowę systemu w miarę wzrastających potrzeb, możliwość zwielokrotnienia logiki w celu zabezpieczenia się przed ewentualnymi usterkami, łatwość konfigurowania zarówno z systemowej konsoli jak i z dowolnego terminala dołączonego do systemu (zmiany konfiguracji nie wymagają konieczności przeładowywania oprogramowania), informacje o pracy systemu mogą być ciągle wysyłane i zapamiętywane na urządzeniu podłączonym do tzw. listening port.

Z punktu widzenia użytkowników istotna jest łatwość komunikowania się ze STARMASTEREM (zgłoszenia mogą być wyświetlane w narodowych językach użytkowników), wielopoziomowy redefiniowany "help", usługom dostępnym w systemie można nadawać dowolne nazwy, a także dla zaoszczędzenia czasu stosować nazwy skrócone tzw. "aliases". Należy również wspomnieć o bardzo rozbudowanym systemie ochrony dostępu do STARMASTERA przez kontrolę nazw i haseł użytkowników, możliwości definiowania haseł do poszczególnych usług, ograniczenie dostępu określonych użytkowników do określonych usług, możliwość łączenia użytkowników w grupy mające ściśle zdefiniowane uprawnienia. Ograniczenia mogą być związane z grupami terminali dołączonych do STARMASTERA. Dostępna jest również opcja "DIALBACK" (po nawiązaniu połączenia i zidentyfikowaniu użytkownika STARMASTER rozłącza połączenie, a następnie sam nawiązuje połączenie telefoniczne ze wskazanym użytkownikiem) zabezpieczająca system przed niepowołanym dostępem przez publiczną sieć telefoniczną.

Konfiguracja STARMASTERA zainstalowanego w centralnym węźle NASK została pokazana na rysunku 6. Gateway został dołączony do sieci X.25 NASK (za pomocą karty SGM, adres w sieci X.25 NASK - 24052), sieci DECNet (za pomocą karty EGM i protokołu LAT) oraz sieci INTERNET (za pomocą karty EGM, adres w sieci INTERNET - 148.81.16.49 lub gandalf.nask.org.pl). Do STARMASTERA zostały dołączone również modemy asynchroniczne, aby umożliwić użytkownikom dostęp przez publiczną sieć telefoniczną oraz szereg asynchronicznych terminali zdalnych i lokalnych.

W przyszłości w STARMASTERZE zostanie zainstalowana karta do sieci ISDN (Integrated Service Data Network). Pozwoli to każdemu użytkownikowi sieci ISDN na bardzo dobre jakościowo połączenie się z gateway'em i dostęp do oferowanych sieci X.25, DECNET, INTERNET oraz EARN.

W najbliższej przyszłości w sieci NASK planowana jest migracja urządzeń tworzących bazową sieć szkieletową w kierunku nowszych technologii. Rozważane jest wyposażenie regionów NASK w węzły Frame Relay, które będą posiadały także możliwość koncentracji przez sieć Frame Relay protokołów synchronicznych i asynchronicznych. Maksymalna przepustowość pomiędzy węzłami Frame Relay będzie wynosiła 2Mbps. Sieć Frame Relay będzie stanowiła sieć bazową, na którą zostaną przeniesione wirtualne sieci TCP/IP oraz X.25. Informacje dla sieci EARN oraz DECNet będą transportowane przez sieć TCP/IP.

Warszawa, lipiec 1994

DODATEK

Struktura adresowania w Naukowej i Akademickiej Sieci Komputerowej X.25.

Tadeusz Wiśniewski

1. Sieć komputerowa X.25 NASK jest widziana jako wielowarstwowa struktura hierarchiczna.

- Najwyższy poziom struktury tworzy węzeł centralny NASK.
- Z węzłem centralnym są połączone węzły strefowe NASK.
- Z węzłem strefowym jest połączony układ węzłów w strefie.
- Do węzła mogą być dołączone urządzenia końcowe DTE lub zakończenia sieci specjalnej jako DTE.
- Do urządzenia końcowego dołączony jest układ terminali lub odpowiadających jednostek. Adres terminala jest przenoszony jako parametr protokołu transportowego sieci lub jako rozszerzenie adresu X.25.

2. Struktura adresowania w sieci X.25 NASK.

W sieci X.25 NASK dla połączeń międzynarodowych wykorzystywany jest następujący schemat adresacji:

p + DNIC + Network Terminal Number (NTN)

gdzie:

p = 0 dla połączeń międzynarodowych
DNIC = 2602 (260 - w/g standardu X.121, 2 - otrzymany przez NASK)
NTN = S-W-DD-TT - maksymalnie 6-cio cyfrowy numer zakończenia
S - numer strefy NASK
W - numer węzła w strefie
DD - numer urządzenia końcowego DTE
TT - numer terminala dla opcji PAD

Dla połączeń wewnątrz sieci X.25 NASK adres ma następującą postać:

2 + Network Terminal Number

gdzie:

2 – Network Identifier otrzymany przez NASK
NTN = S-W-DD-TT - maksymalnie 6-cio cyfrowy numer zakończenia
S - numer strefy NASK
W - numer węzła w strefie
DD - numer urządzenia końcowego DTE
TT - numer terminala dla opcji PAD

3. Numeracja stref w sieci X.25 NASK.

Sieć NASK została podzielona na 7 stref. W każdej strefie jest wyznaczony węzeł centralny (tzw. węzeł strefowy). Przyjęto następującą numerację stref NASK:

Numer strefy	Miasto, numer węzła centralnego w strefie		Regiony dołączone do węzła strefowego
2	Kraków	(nr 20)	
3	Poznań	(nr 30)	Szczecin
4,5	Warszawa	(nr 40)	Płock, Łódz, Lublin, Białystok
6	Toruń	(nr 60)	
7	Wrocław	(nr 70)	Opole
8	Gliwice	(nr 80)	
9	Gdańsk	(nr 90)	

Uwaga: węzeł centralny w Warszawie o numerze 40 pełni jednocześnie funkcję centralnego węzła sieci X.25 NASK. W strukturze adresowania brak stref o numerach 0 i 1, które zostały potraktowane jako rezerwa na przyszłość.

4. Adresowanie w sieci X.25 NASK na styku z sieciami DATAPAK i POLPAK.

Z punktu widzenia adresacji sieć X.25 NASK jest widziana jako prywatna podsieć publicznych sieci pakietowych X.25 DATAPAK (łącze abonenckie) i POLPAK (łącza abonenckie). W przypadku łączy międzyoperatorskich z DATAPAK oraz POLPAK sieć X.25 NASK jest identyfikowana przez swój własny międzynarodowy DNIC. Sieć DATAPAK przewiduje maksymalnie 6-cio cyfrową przestrzeń adresową dla dołączonej podsieci prywatnej, natomiast sieć POLPAK 7-mio cyfrową. W sieci X.25 NASK wykorzystywany jest adres 7-mio cyfrowy (NI + NTN) opisany w punkcie 2-gim opracowania.

4.1. Adresowanie w sieci POLPAK na styku z siecią NASK.

W sieci POLPAK (łącza abonenckie) jest przewidziany dla abonenta synchronicznego wewnętrznego 15-to cyfrowy adres zakończenia o postaci:

p-xxxxxxx-yyyyyyy

gdzie: p=1 - prefix dla połączeń w sieci POLPAK
xxxxxxx - adres zakonczenia w sieci POLPAK dla abonenta
synchronicznego (w szczególności adres styku sieci POLPAK i NASK)
yyyyyyyy - przestrzeń adresowa do dyspozycji abonenta
wykorzystywana, gdy abonentem jest podsieć prywatna (w szczególnych przypadkach długość adresu w tym polu wynosi zero).

Natomiast dla łącza międzyoperatorskiego adres abonenta będzie miał postać:

p-2601-xxxxxxx-yyy

gdzie: p=0 - prefix
xxxxxxx - adres zakończenia w sieci POLPAK
yyy - przestrzeń adresowa do dyspozycji abonenta (w szczególnych przypadkach długość adresu w tym polu wynosi zero)

4.2. Adresowanie w sieci DATAPAK na styku z siecią NASK.

4.2.1. Adresowanie dla łącza abonenckiego.

Sieci NASK jako prywatnej podsieci publicznej sieci pakietowej DATAPAK przyznano adres zakończenia o postaci:

0-2407-9001-yyyyyy

gdzie: yyyyyy - przestrzeń adresowa możliwa do wykorzystania w sieci NASK.

4.2.2. Adresowanie dla łącza międzyoperatorskiego.

Sieć X.25 NASK jest widziana z sieci DATAPAK (oraz z sieci innych operatorów) pod następującym adresem :

0-2602-yyyyyyyyyy

gdzie: yyyyyyyyyy - przestrzeń adresowa możliwa do wykorzystania w sieci NASK.

4.3. Struktura adresu w sieci NASK.

4.3.1. Struktura adresu dla połączeń międzynarodowych.

4.3.1.1. Dla przychodzących połączeń międzynarodowych (przez łącze abonenckie) adres w sieci NASK ma nastepującą postać:

0-2407-9001-s-w-dd-tt

gdzie: s - numer strefy NASK
w - numer węzła w strefie
dd - numer urządzenia końcowego DTE
tt - numer terminala dla opcji PAD

W tym przypadku identyfikator sieci NI jest dopisywany do adresu przez węzeł X.25.

4.3.1.2. Dla przychodzących połączeń międzynarodowych przez łącze międzyoperatorskie adres w sieci NASK na następującą postać:

0-260-2-s-w-dd-tt

gdzie: s, w, dd, tt - jak w p-cie 4.3.1.1.

4.3.2. Struktura adresu dla połączeń wewnątrz sieci NASK.

Dla połączeń wewnątrz sieci NASK adres ma następującą postać (tzw. forma skrócona adresu):

2-s-w-dd-tt

gdzie: s, w, dd, tt - jak w p-cie 4.3.1.1.

4.3.3. Struktura adresu dla połączeń z sieci POLPAK.

Dla połączeń z sieci POLPAK przez łącza abonenckie adres ma następującą postać:

1-xxxxxxx-2-s-w-dd-tt

gdzie: xxxxxxx - adres styku sieci POLPAK z siecią NASK
s, w, dd, tt - jak w p-cie 4.3.1.1.

Dla połączeń z sieci POLPAK przez łącze międzyoperatorskie adres ma następującą postać:

0-2602-s-w-dd-tt

gdzie: s, w, dd, tt - jak w p-cie 4.3.1.1

5. Sposoby nawiązywania połączeń dla abonentów sieci NASK, POLPAK oraz międzynarodowej sieci X.25.

5.1. Abonent sieci NASK z abonentem sieci NASK.

Dla uzyskania połączenia wykorzystywany jest adres skrócony o postaci:

2-s-w-dd-tt

gdzie: s, w, dd, tt - jak w p-cie 4.3.1.1.
np. 2407101, aby uzyskać połączenie z komputerem IBM 3090 (sieć EARN) w CIUW.

5.2. Abonent sieci NASK z abonentem sieci międzynarodowej.

Dla uzyskania połączenia wykorzystywany jest pełny adres X.25 właściwy dla adresata o postaci:

0-kkk-nn...n

gdzie: kkk - numer kraju
nn...n - do 11 cyfr adresu DTE w danym kraju
np. 0-310-690157800, aby uzyskać połączenie z bazą McGrawHill w USA.

5.3. Abonent sieci NASK z abonentem sieci POLPAK lub abonentem sieci NASK dołączonym poprzez sieć POLPAK.

5.3.1. Dla uzyskania połączenia (łącze abonenckie) wykorzystywany jest adres o postaci:

1-xxxxxxx-2-s-w-dd-tt

gdzie: xxxxxxx - adres abonenta sieci NASK w sieci POLPAK
s, w, dd, tt - jak w p-cie 4.3.1.1.
jeśli adresatem jest abonent NASK dołączony poprzez sieć POLPAK

lub

1-xxxxxxx-yy...y

gdzie: xxxxxxx - adres abonenta sieci POLPAK
yy...y - część adresowa do dyspozycji abonenta np. używana jeśli do sieci POLPAK dołączona jest dowolna podsieć prywatna (w szczególności długość tej części adresu może być równa zeru).

5.3.2. Dla uzyskania połączenia (łącze międzyoperatorskie) wykorzystywany jest adres o postaci:

1-xxxxxxx-yyy

gdzie: xxxxxxx - adres abonenta sieci POLPAK
yyy - część adresowa do dyspozycji abonenta używana jeśli do sieci POLPAK dołączona jest dowolna podsieć prywatna (w szczególności długość tej części adresu może być równa zeru). Kod kraju jest w tym przypadku uzupełniany przez węzeł X .25.

5.4. Abonent sieci międzynarodowej z abonentem sieci NASK.

5.4.1 Dla uzyskania połączenia przez łącze abonenckie wykorzystywany jest pełny adres o postaci:

0-2407-9001-s-w-dd-tt

gdzie: s, w, dd, tt - jak w p-cie 4.3.1.1.
np. 0-2407-9001-407101, aby uzyskać połączenie z komputerem IBM 3090 (sieć EARN) w CIUW.

5.4.2. W przypadku nawiązywania połączenia przez łącze międzyoperatorskie wykorzystywany jest adres międzynarodowy o postaci:

0-260-2-s-w-dd-tt

gdzie: s, w, dd, tt - jak w p-cie 4.3.1.1.
np. 0-260-2-407101, aby uzyskać połączenie z komputerem IBM 3090 (sieć EARN) w CIUW.

5.5. Abonent sieci międzynarodowej z abonentem sieci POLPAK.

W tym przypadku połączenie przebiega w sposób dwuetapowy:

- nawiązanie połączenia z gateway'em NASK na właściwy adres o strukturze:

0-2407-9001-s-w-dd-tt - opisane w p-cie 5.4.1
0-260-2-s-w-dd-tt - opisane w p-cie 5.4.2

- po uzyskaniu połączenia z gateway'em i stając się w ten sposób abonentem NASK należy wykonać połączenie opisane w p-cie 5.3.

lub abonent sieci międzynarodowej może od razu wybrać adres abonenta sieci POLPAK o postaci:

0-2601-xxxxxxx-yyy

gdzie: xxxxxxx - adres portu X.25 w sieci POLPAK
yyy - część adresowa używana jeśli do sieci POLPAK dołączona jest dowolna podsieć prywatna (w szczególności długość tej części adresu może być równa zeru).

5.6. Abonent sieci POLPAK z abonentem sieci NASK.

5.6.1. Dla uzyskania połączenia przez łącza abonenckie wykorzystywany jest adres o postaci:

1-xxxxxxx-2-s-w-dd-tt

gdzie: xxxxxxx - adres styku sieci POLPAK i NASK
s, w, dd, tt - jak w p-cie 4.3.1.1
np. 1-xxxxxxx-2407101, aby uzyskać połączenie z komputerem IBM 3090 (sieć EARN) w CIUW.

5.6.2. Dla uzyskania połączenia przez łącze międzyoperatorskie wykorzystywany jest adres o postaci:

0-2602-s-w-dd-tt

gdzie: s, w, dd, tt - jak w p-cie 4.3.1.1
np. 0-2602-407101, aby uzyskać połączenie z komputerem IBM 3090 (sieć EARN) w CIUW.

5.7. Abonent sieci POLPAK z abonentem sieci POLPAK lub abonentem sieci NASK dołączonym poprzez sieć POLPAK.

Dla uzyskania połączenia wykorzystywany jest adres o postaci:

1-xxxxxxx-yy...y

gdzie: xxxxxxx - adres abonenta sieci POLPAK
yy...y - cześć adresowa używana jeśli do sieci POLAPAK dołączona jest dowolna podsieć prywatna (w szczególności długość tej części adresu może być równa zeru), lub

1-xxxxxxx-2-s-w-dd-tt

gdzie: xxxxxxx - adres abonenta sieci NASK w sieci POLPAK
s, w, dd, tt - jak w p-cie 4.3.1.1
jeśli adresatem jest abonent NASK dołączony poprzez sieć POLPAK

5.8. Abonent sieci POLPAK z abonentem sieci międzynarodowej.

W tym przypadku połączenie przebiega w sposób dwuetapowy:

- nawiązanie połączenia z gateway'em NASK na właściwy adres o strukturze:

1-xxxxxxx-2-s-w-dd-tt opisane w p-cie 5.6

- po nawiązaniu połączenia z gateway'em i stając się w ten sposób abonentem sieci NASK należy wykonać połączenie opisane w p-cie 5.2,

lub abonent sieci POLPAK może od razu wybrać adres abonenta sieci międzynarodowej w/g schematu przedstawionego w p-cie 5.2.

Warszawa, lipiec 1994

Sieć Internet w Polsce

Janusz Motoszko, Ireneusz Neska

Internet - "Sieć sieci" - oparta o protokół TCP/IP skupia w Polsce obecnie ponad 8000 komputerów w placówkach naukowo-badawczych, akademickich a także komercyjnych ciesząc się w kraju wciąż rosnącą popularnością. W NASK jest to sieć o największym tempie rozwoju liczby użytkowników w ostatnich latach. W celu przybliżenia tego rodzaju sieci przedstawiony zostanie krótki przegląd podstawowych idei, którymi kierowali się ludzie tworzący Internet oraz nierozerwalnie związany z nim protokół TCP/IP.

Internet jest technologią powstałą z myślą o ułatwieniu połączenia wielu sieci różnych typów. Ukrywa on detale sprzętu sieciowego i umożliwia komunikowanie się komputerów niezależnie od miejsca i rodzaju ich fizycznego połączenia.

Elementy sieci generalnie można podzielić na trzy klasy:

a) sieci lokalne (Local Area Networks - LAN)
Istnieje tu bardzo duża różnorodność wykonania. Typowo mogą one być wykonane na bazie topologii magistrali, pierścienia lub gwiazdy. Sieci te z reguły pokrywają małe obszary geograficzne (pojedyncze budynki lub kompleksy budynków). Występują tu duże prędkości i małe opóźnienia transmisji.

b) sieci miejskie (Metropolitan Area Networks - MAN)
Jest to specjalny rodzaj sieci, tworzonych na terenie większych ośrodków miejskich. Tworzą one podstawową strukturę połączeń instytucji na terenie danego miasta, przy czym najczęściej tworzone są one na bazie bardzo szybkich połączeń cyfrowych, np. FDDI, ISDN, ATM itp.

c) sieci rozległe
Geograficznie rozproszone komputery i sieci lokalne są łączone ze sobą w kompleksy zwane sieciami rozległymi. Sieci te mają rozbudowaną strukturę linii połączeniowych i urządzeń do przesyłania danych.

Struktura Internetu jest hierarchiczna. Zgodnie ze swoją nazwą Internet jest zespołem połączonych ze sobą sieci, z których każda może być podzielona na podsieci. Te podsieci najczęściej są sieciami lokalnymi. Komunikacja między komputerami w tej samej podsieci jest bardzo prosta i polega na bezpośrednim przesyłaniu danych między dwoma komputerami. Przesyłanie informacji między różnymi sieciami wymaga natomiast znajomości drogi połączeń miedzy nimi. Znajdowaniem tej drogi i przesyłaniem danych między kolejnymi sieciami od nadawcy do adresata zajmują się urządzenia zwane "router'ami" lub czasami "gateway'ami". Mogą to być dedykowane urządzenia przeznaczone tylko do tego celu lub komputery ogólnego przeznaczenia z odpowiednim oprogramowaniem.

Routery są połączone jednocześnie do dwóch lub więcej sieci. W każdej sieci posiadają fizyczny interfejs oraz adres IP odpowiedni dla niej. Przy przesyłaniu danych generalnie wymagane jest, aby router wybrał adres następnego routera na drodze do adresata lub (dla końcowej sieci) adres docelowego komputera. Algorytm wybierania tej drogi nazywany jest "routingiem" i zależy od bazy danych zgromadzonej w routerze. Baza danych routingu może być stała (statyczna), niezależna od aktualnego stanu sieci. Może być również zmieniana dynamicznie, odzwierciedlając aktualną topologię systemu sieciowego. Routery tworzą więc drogi połączeń całych sieci, a nie tylko pojedynczych maszyn, odgrywając kluczową rolę w komunikacji Internetowej. Widać z tego, że Internet stanowi jakby jedną ogromną sieć z tą tylko różnicą, że jest to struktura wirtualna utworzona przez programistów, składająca się z tysięcy fizycznych sieci lokalnych.

W celu umożliwienia przesyłania informacji między poszczególnymi sieciami na początku lat siedemdziesiątych został opracowany protokół komunikacyjny TCP/IP (Transmission Control Protocol/Internet Protocol). Początkowo został on stworzony na potrzeby wojskowe dla Departamentu Obrony USA (DoD). Bardzo szybko został on jednak wykorzystany do celów cywilnych. Na początku lat osiemdziesiątych większość amerykańskich ośrodków naukowych i akademickich połączyła się Internetem. W dalszej kolejności sieć Internet zaczęły wykorzystywać ośrodki przemysłowe oraz instytucje państwowe i firmy prywatne. Internet w ciągu kilkunastu lat stał się "de facto" standardem połączeń międzysieciowych. Wiele szanujących się firm uważa za punkt honoru posiadanie dostępu do Internetu, a w Stanach Zjednoczonych czy Europie Zachodniej jest to po prostu rzecz normalna. Przykładami mogą być tu CERN, NASA, US Navy, Microsoft, Novell. Najważniejszym z czynników, które wzmogły popularność tego protokołu było wbudowanie go w większość odmian systemu operacyjnego UNIX.

TCP/IP jest obecnie jedynym w pełni udokumentowanym protokołem nie związanym z żadnym producentem czy typem komputera. Jest on uniwersalny, a jego implementacje dostępne są praktycznie na wszystkie typy maszyn i systemy operacyjne. Z tych powodów jest on, standardem używanym niezwykle często zarówno w sieciach lokalnych jak i rozległych. Obecnie trudno jest znaleźć komputer, na którym nie stworzono oprogramowania TCP/IP. Przykładami mogą być osobiste PC z oprogramowaniem FTP Software lub pracujące pod różnymi odmianami UNIX-a (np.'SCO UNIX), stacje robocze i serwery (np. SUN, Silicon Graphics, Hewlett Packard, VAX 6000 z VMS Ultrix Connection). Również wiele systemów sieci lokalnych, np. Bayan VINES lub Novell NetWare, może pochwalić się możliwością integracji z sieciami TCP/IP.

Pod nazwą TCP/IP kryją się de facto dwa standardy protokołów używanych do komunikacji w sieciach (IP - Internet Protocol oraz TCP - Transmission Control Protocol). Opisują one formy przesyłania informacji, specyfikują ich detale, obsługę błędów itp.

Wszystkie programy Internetu używają IP jako podstawowego mechanizmu transportu danych. IP realizuje tzw. datagramowy lub bezpołączeniowy model komunikacji. Polega on na podziale całkowitej informacji na części zwane datagramami, zawierającymi w nagłówku między innymi adres nadawcy i docelowy. IP zajmuje się zaopatrzeniem datagramów w odpowiednie adresy, specyfikacją typu usługi sieciowej oraz zabezpieczeniem informacji. Ma on za zadanie również przetransportowanie datagramów do ich miejsca docelowego nie dbając o błędy powstałe podczas transmisji, przy czym drogi przesyłania tych datagramów mogą być różne w zależności od aktualnego stanu sieci i natężenia ruchu na poszczególnych liniach przesyłowych.

TCP jest protokołem wyższego poziomu odpowiadającym za dzielenie danych na części i ich składanie w miejscu przeznaczenia we właściwej kolejności. Zapewnia on również retransmitowanie datagramów zgubionych lub zniszczonych oraz kontrolę połączenia między stacjami końcowymi. Realizuje on w praktyce ideę niezawodnego transportu danych.

Najważniejszą cechą tych protokołów jest jednak to, że pozwalają rozpatrywać standardy komunikacyjne bez względu na sprzęt jakim dysponują poszczególne sieci lokalne.

Twórcy TCP/IP przyjęli schemat adresowania analogiczny do fizycznej sieci, w której każdy komputer ma przypisany swój unikalny w świecie 32-bitowy identyfikator, stanowiący tzw. numer Internetowy, zwany też numerem IP. Dla uproszczenia jest on zapisywany jako sekwencja czterech liczb ośmiobitowych oddzielonych kropkami (np. 148.81.16.50). Koncepcyjnie numer ten jest parą identyfikującą numer sieci (net-id) oraz numer komputera w sieci (host-id). W naszym przykładzie numerem sieci jest część 148.81, natomiast numerem komputera w sieci jest 16.50. Adresy sieci zostały podzielone na pięć grup zwanych klasami adresowymi, różniących się ilością komputerów możliwych do zainstalowania w pojedynczej sieci. Klasy te oznacza się wielkimi literami od A do E. Numerów Internetowych nie przydziela się pojedynczo tylko grupami. W warunkach polskich jest możliwe uzyskanie adresów z jednej lub wielu klas C (do 254 komputerów w jednej sieci) oraz w szczególnych przypadkach z klasy B (ponad 65 tysięcy komputerów).

Symbolicznie adres Internetowy można przedstawić następująco:
adres-IP = {<numer - sieci>,<numer - komputera>}

Aby dostarczyć datagram do adresata poszczególne routery znajdują drogę tylko na podstawie adresu IP zawartego w części <numer - sieci>, natomiast ostatni router na drodze pakietu musi na podstawie adresu IP podanego w części <numer - komputera> przekształcić w adres fizyczny hosta dołączonego do tej sieci i przesłać datagram do tego komputera. Ta prosta notacja została jednak rozszerzona o koncepcję "podsieci". Ze względu na gwałtowny wzrost liczby numerów sieci i skomplikowania routingu stało się to konieczne w architekturze Internetu. Pozwoliło to na prostsze odzwierciedlenie zawiłości struktury połączeń sieci lokalnych w sposobie routingu. Podsieci pozwalają na dwu- lub wielopoziomową hierarchiczną strukturę routingu. Polega to na podziale pola <numer - komputera> na dwie części: numer podsieci i rzeczywisty numer komputera w tej podsieci. Miejsce podziału tego rozszerzonego numeru sieci jest wskazywane przez 32 bitową liczbę, zwaną "maską podsieci". W połączonych sieciach lokalnych jednej organizacji może teraz występować jeden numer sieci, lecz różne numery podsieci, co ułatwia administratorowi obsługę sieci.

W celu ułatwienia użytkownikom komunikacji między komputerami poza numerem Internetowym dla oznaczania komputerów wprowadzono również nazwy symboliczne (np. frodo.nask.org.pl). Obsługą tych nazw zajmuje się tzw. DNS (Domain Name Service), pozwalający na konwersję adresu symbolicznego na liczbowy i odwrotnie w sposób niewidoczny dla użytkownika. Nazwa składa się z kilku (najczęściej od dwóch do pięciu) członów oddzielonych kropkami i ma również strukturę hierarchiczną. Hierarchia ta nie musi się jednak

pokrywać z hierarchią sieci i podsieci. Najbardziej ogólna klasa umieszczana jest po prawej stronie. Z reguły jest to dwuliterowy skrót nazwy państwa, np.

pl - Polska,
uk - Wielka Brytania,
us - nowa domena Stanów Zjednoczonych, itd.

Wyjątkiem są tu Stany Zjednoczone, gdzie nazwy symboliczne nie miały w ogóle ostatniego dwuliterowego członu. Dopiero niedawno powstał projekt zmodyfikowania nazewnictwa w USA, w którym uwzględniono już tę część nazwy. Również główne urządzenia związane bezpośrednio z obsługą sieci (np. routery) nie mają w nazwie określenia państwa (tu z reguły jako ostatni człon nazwy występuję skrót "net").

Przykładem nazwy symbolicznej może być nazwa frodo.nask.org.pl, która oznacza komputer o nazwie frodo, znajdujący sie w NASK, organizacji w Polsce. W ten sposób nie trzeba pamiętać adresów numerycznych np. 148.81.16.50, co przy większej ilości adresów byłoby kłopotliwe.

W Polsce nowotworzone nazewnictwo opiera się na określeniu miejsca danego komputera w sieci. Stąd jako drugi od prawej człon nazwy podaje się nazwę miasta, a jako trzeci nazwę instytucji, w której znajduje się komputer. Następnie może bezpośrednio znajdować się nazwa komputera w sieci lokalnej lub nazwa wydziału, instytutu, bądź jednostki organizacyjnej, w której znajduje się komputer. Według tej konwencji nazwa frodo.nask.waw.pl oznacza komputer o nazwie frodo znajdujący sie w instytucji o nazwie NASK mieszczącej się w Warszawie (waw) w Polsce (pl).

Dla każdej domeny musi być jeden nadrzędny (tzw. primary) oraz powinien być co najmniej jeden podrzędny (tzw. secondary) komputer obsługujący tą domenę. W nadrzędnym serwerze wprowadza się wszelkie zmiany w strukturze nazewnictwa na poziomie tej domeny. Tu również dopisuje się nowe nazwy domenowe. Komputery podrzędne stanowią serwery zapasowe, trzymające kopie danych ściągnięte z serwera nadrzędnego i wykorzystywane w przypadku awarii tego komputera. W Polsce nadrzędne serwery dla głównej domeny krajowej (pl) i większości domen regionalnych obsługiwane są właśnie przez NASK. NASK oferuje również swoje komputery jako serwery podrzędne *(secondary)* dla swoich klientów.

Z punktu widzenia użytkownika Internet jest zbiorem programów, które wykorzystują sieć do komunikowania się między sobą. Najważniejsze z nich to: poczta komputerowa, zdalna interakcyjna praca na odległych maszynach, zdalna transmisja zbiorów, dostęp do serwisów informacyjnych i zbiorów danych oraz bezpośrednia komunikacja między terminalami.

- **poczta komputerowa** *(ang. Mail)*

  Umożliwia szybkie i tanie przesyłanie korespondencji pomiędzy użytkownikami, przy zachowaniu listu w postaci zbioru. Przygotować list można w dowolnym edytorze, jest również możliwe napisanie listu bezpośrednio przed wysłaniem. Wysłanie odbywa się przez wywołanie programu obsługującego pocztę (najczęściej jest to program mail), podanie adresu odbiorcy (np. irek@frodo.nask.org.pl) oraz tematu korespondencji pod hasłem "Subject:" i skierowanie treści do wysłania. Istnieją również komputery realizujące konwersję listów między różnymi typami sieci, dzięki czemu możliwa jest komunikacja z sieciami EARN/BITNET, DECnet, UUCP, Fido, czy też Janet.

  Podstawową zaletą poczty komputerowej jest jej szybkość i niezawodność. Przesyłka dociera do adresata odległego o setki lub tysiące kilometrów najczęściej w czasie najwyżej kilku minut. Gdy adresat listu jest niedostępny w danej chwili (niedostępny lub wyłączony komputer) przesyłka jest przechowywana w pewnych komputerach, które co jakiś czas próbują przesłać list do adresata. Dopiero, gdy upłynie założony czas przesłania listu (najczęściej kilka dni do tygodnia) list jest zwracany do nadawcy z odpowiednim komunikatem.

  Jednak możliwości poczty elektronicznej daleko odbiegają od ich początkowych założeń. Istnieje prosta możliwość powielania listów w dowolnej liczbie egzemplarzy, co pozwala na rozsyłanie tej samej informacji do wielu odbiorców. Jest to podstawą do tworzenia tzw. list dyskusyjnych, w których wymienia się informacje na konkretny temat, między wszystkimi osobami zapisanymi do danej listy.

- **zdalna transmisja zbiorów** *(ang. File Transfer)*

  Krótkie zbiory tekstowe można transportować przy pomocy poczty komputerowej, ale nie jest to metoda efektywna przy zbiorach dużej wielkości. Został stworzony więc specjalny protokół FTP (File Transfer Protocol) do transmisji dowolnie dużych zbiorów i to zarówno tekstowych jak i binarnych. Zapewnia on pełną kontrolę poprawności transmisji oraz praw dostępu do danych. Aby uzyskać dostęp do odległej maszyny wymagane jest podanie identyfikatora użytkownika oraz hasła. Z drugiej strony wiele ośrodków

utworzyło na swoich komputerach publiczne, ogólnie dostępne archiwa (tzw. anonymous FTP). Jako identyfikatora używa się wtedy zwykle słowa 'anonymous', a jako hasło do celow statystycznych podaje się własny identyfikator użytkownika. W archiwach takich udostępniana jest ogromna ilość oprogramowania publicznie dostępnego *(ang. public domain)* na dowolne typy maszyn i systemy operacyjne. Mogą to być bardzo proste programy, ale również ogromne pakiety oprogramowania specjalistycznego, które można skopiować na dysk komputera lokalnego.

- **interakcyjna praca na odległych maszynach**
  Umożliwia zdalną interakcyjną pracę na maszynach znajdujących się w dowolnym miejscu w sieci, być może oddalonych o setki kilometrów. Stwarza to możliwości pracy na komputerach o ogromnej mocy obliczeniowej niedostępnych w lokalnym systemie, uruchamiania tam programów, dostępu do baz danych itp. Zapewniona jest przy tym duża wygoda pracy, gdyż lokalny terminal emuluje terminal odległego komputera co stwarza wrażenie pracy na zdalnym systemie. W ten sposób jest również możliwy dostęp do baz danych. Szereg baz danych komercyjnych udostępnia swoje zasoby odpłatnie, ale istnieją również bazy naukowe czy też akademickie, do których dostęp jest możliwy za darmo. W USA ok. 500 uczelni udostępnia bezpłatnie swoje katalogi biblioteczne, w których można znaleźć informacje na temat literatury z całego świata.
- **dostęp do serwisów informacyjnych i zbiorów danych**
  W sieci Internet istnieje szereg programów umożliwiających użytkownikowi dostęp do serwisów informacyjnych i zbiorów danych znajdujących się na lokalnym komputerze lub dowolnym innym serwerze udostępniającym swoje zasoby. Do programów tych należą: gopher, www, wais, whois, archie. Wszystkie te programy zostały opisane szczegółowo w oddzielnym artykule.
- **bezpośrednia komunikacja między terminalami (talk, write)**
  Programy te zapewniają natychmiastową interakcyjną wymianę komunikatów między użytkownikami obecnymi na dowolnych komputerach. Stwarza to warunki do rozmów koleżeńskich oraz organizowania konferencji w miejscach od siebie odległych.
- **dostęp do odmiennych struktur plikowych (NFS)**
  Network File System (NFS) jest to standard współpracy komputerów, posługujących się odmiennymi systemami plików (np. różne wersje UNIX, DOS, VMS). Standard ten daje użytkownikowi możliwość łatwego dostępu przez sieć do zbiorów zapisanych przez różne systemy operacyjne.

Jak już wcześniej wspomniano każde urządzenie w sieci powinno mieć unikalny adres. Dlatego też przydzielanie adresów musi być nadzorowane z jednego miejsca. Nadrzędną organizacją, która zajmuje się przyznawaniem numerów sieci jest InterNIC w Stanach Zjednoczonych. Dba ona o to, by wszystkie numery były unikalne w skali światowej. Jednak z powodu gwałtownego rozrostu sieci Internet taki sposób przyznawania adresów stał sie nieefektywny. Z tego też powodu w kilku regionach świata powstały ośrodki, które są odpowiedzialne za przyznawanie adresów na danym terenie. Dla Europy jest to organizacja RIPE (Reseau IP Europeen - Europejska Sieć IP) z siedzibą w Amsterdamie. Poza przyznawaniem adresów zajmuje się ona koordynacją i współdziałaniem europejskich sieci z protokołem TCP/IP. Nadzoruje ona również prace europejskiej sieci szkieletowej TCP/IP oraz stanowi forum dyskusji nad rozwiązaniami technicznymi i organizacyjnymi.

Od połowy 1992 r. przyznawanie adresów IP zostało całkowicie zdecentralizowane. W ramach poszczególnych państw pewne organizacje sieciowe mogą otrzymać grupę adresów klas C, które będą następnie delegowane dla zainteresowanych na terenie danego kraju. Są to tak zwani lokalni rejestratorzy IP (ang. Local IP Registers) i oni decydują o rozdzielaniu adresów IP w ramach danego państwa. NASK jest właśnie organizacją, która zajmuje się przydziałem i administracją adresów Internetowych na terenie Polski.

W obrębie sieci lokalnych nad przydziałem numerów Internetowych konkretnym komputerom czuwa odpowiedzialny za daną sieć administrator.

Rozwój Internetu na świecie przekroczył pierwotne szacunki. Gwałtowny wzrost ilości sieci i komputerów uwypuklił kilka dotąd niedocenianych problemów:

- wyczerpanie się adresów klasy B. Jednym z fundamentalnych powodów tego problemu jest brak klas adresowych odpowiednich dla średnich organizacji; klasa C z maksymalną liczbą 254 adresów jest za mała, natomiast klasa B (do 65534 adresów) jest za duża do prawidłowego wykorzystania w takiej organizacji.
- znaczny rozrost tablic routingu w routerach Internetowych stał się poza możliwościami efektywnego zarządzania przez obecne oprogramowanie i ludzi. Dane statystyczne podają, że w węzłowych routerach w EBONE lub NSF znajduje się w tej chwili ponad 12 tysięcy pól w tablicach routingu.
- ewentualne wyczerpanie 32-bitowej przestrzeni adresowej.

Stało się jasne, że pierwsze dwa problemy będą krytyczne w ciągu następnych kilku lat. Rozwiązaniem ich zajął się projekt o nazwie CIDR (Classless Interdomain Routing - Bezklasowy Routing Międzyoperatorski) proponując wprowadzenie mechanizmu spowalniającego rozrost tablic routingu i potrzeby przyznawania nowych numerów IP. Dokonywane jest to w ten sposób, że pewne ciągłe grupy adresów klas B i C są reprezentowane przez jedno pole w tablicy routingu. Temu celowi ma też służyć hierarchiczne przyznawanie klas adresowych. I tak Europie zostały przyznane dwie grupy po 65536 klas C: 193.0.0.0 i 194.0.0.0. W tablicach routingu między USA a Europą wszystkie klasy C z tych dwóch grup reprezentowane jest przez jedno pole 193.0.0.0 z maską 254.0.0.0. RIPE w dalszej kolejności deleguje grupy klas C do poszczególnych operatorów sieciowych. I tak dla Polski została przyznana grupa 256 klas C: 193.59.0.0. W tablicach routingu routerów europejskich wszystkie klasy C z tej grupy reprezentowane są przez jedno pole: 193.59.0.0 z maską 255.255.0.0. Dalej tą hierarchię można rozszerzyć na sieci w ramach operatora.

CIDR nie zamierza jednak rozwiązać trzeciego problemu, który jak do tej pory nie jest krytyczny, pozwoli jednak na funkcjonowanie Internetu przez następne lata, póki nie zostanie zaproponowane rozwiązanie długoterminowe. Planowany koniec tradycyjnego IP jest szacowany na rok 2010. Ponieważ system ISO/OSI nie rozpowszechnia się tak szybko jak sądzono, już dziś wiele ośrodków prowadzi prace mające na celu stworzenie nowego rodzaju Internetu - tzw. IPng (IP next generation). Nie wiadomo jeszcze w tej chwili jak ten nowy Internet będzie wyglądać, ale większość projektantów jest zgodna, że rozwiązaniem może być rozszerzenie długości adresu IP do 64 bitów.

Równolegle z CIDR trwają prace nad drugim projektem o nazwie PRIDE (Policy based Routing Implementation, Deployment in Europe). PRIDE ma za zadanie stworzenie kilku baz danych (w Europie jest to RIPE), w których gromadzone byłyby informacje o polityce routingu poszczególnych operatorów sieciowych. Zawierałyby one szczegóły tej polityki - przede wszystkim jakie sieci każdy operator akceptuje od innych operatorów oraz jakie sam do nich wysyła. Służyłoby to między innymi do generowania zbiorów konfiguracyjnych routerów (access listy).

Perspektywy na najbliższe lata lokują TCP/IP jako jeden z protokołów dostępowych zapewniających komunikację międzysieciową.

Rozwój Internetu w Polsce rozpoczął się w połowie 1991 roku, kiedy to uzyskaliśmy zezwolenie na dołączenie do sieci światowej. Zalążki sieci zostały stworzone na kilku komputerach pracujących z systemem operacyjnym UNIX oraz komputerach PC z oprogramowaniem Public Domain jako routery. Połączenia międzymiastowe oraz łącze międzynarodowe do Kopenhagi realizowane były na liniach analogowych z prędkością 9.6 Kb/s. Szybko jednak takie rozwiązanie okazało się niewystarczające a zwiększenie prędkości linii międzynarodowej w relacji Warszawa-Sztokholm do 64 Kb/s oraz zastosowanie profesjonalnych routerów CISCO poprawiło sytuację tylko na krótko.

W chwili obecnej NASK jest w Polsce największym dostarczycielem usługi połączeniowej TCP/IP. Od początku istnienia tej sieci w NASK były prowadzone intensywne działania mające na celu modernizację urządzeń i podnoszenie prędkości linii przesyłowych. Utworzona i ciągle rozwijana sieć podkładowa ma służyć podwyższeniu jakości i niezawodności, a także bezpieczeństwa oferowanych przez NASK usług Internetowych. W ośrodkach regionalnych instalowane są profesjonalne routery zapewniające niezawodną oraz dużo szybszą transmisję danych. W tej chwili na liniach międzymiastowych stosowane są głównie połączenia cyfrowe o prędkości 2 Mb/s (stare połączenia analogowe są sukcesywnie likwidowane). Łączność ze światem jest zapewniona przez łącze satelitarne do Sztokholmu (NORDUnet) o prędkości 2 Mb/s oraz łącze cyfrowe do Wiednia (EBONE) o przepustowości 128 Kb/s. Również Ukraina (Lwów) oraz Rosja (Moskwa) posiadają połączenia do Polski. Planowane jest również połączenie do Białorusi.

NASK jest pełnoprawnym partnerem na arenie międzynarodowej. Współpracuje z wieloma międzynarodowymi organizacjami sieciowymi. Naszymi bezpośrednimi partnerami są EBONE (międzynarodowy operator dostarczający usługi sieciowe na terenie Europy; posiada węzły między innymi w Paryżu, Londynie, Amsterdamie, Genewie, Sztokholmie i Wiedniu) oraz NORDUnet (wspólna nazwa akademickich operatorów sieciowych państw skandynawskich). Z inicjatywy NASK powstała organizacja skupiająca akademickich operatorów sieciowych środkowej i wschodniej Europy - CEENET (Central and Eastern Europe Network). NASK aktywnie uczestniczy również w pracach RIPE. Szerzej na temat działalności NASK na arenie międzynarodowej opisane zostało w oddzielnym artykule.

Internet w NASK w ciągu niecałych trzech lat dokonał znaczącego postępu. Liczba i wielkość sieci dołączonych do Internetu stale rośnie. W lipcu 1994 roku przekroczyliśmy liczbę 8000 zarejestrowanych komputerów pracujących pod różnymi systemami.

Ogromna popularność tej sieci wynika z niedużych wymagań sprzętowych i niewielkiego kosztu instalacji w stosunku do oferowanych usług. W najprostszym przypadku do sieci Internet można dołączyć istniejącą instalację UNIX-ową lub NOVELL-ową lub VMS. Jako najprostszy router może pracować zwykły komputer PC z odpowiednim oprogramowaniem.

W obecnej chwili Internet w Polsce ma konfigurację gwiazdy, z połączeniami obejściowymi. Większość głównych ośrodków w kraju jest (lub będzie w niedługim czasie) dołączone szybkimi liniami do Warszawy. Struktura routerów NASK jest warstwowa. Poziom krajowy stanowi urządzenie AGS+ firmy CISCO zainstalowane w Centralnym Węźle NASK w Warszawie. Konfiguracja regionalnych węzłow NASK z reguły składa się z routera CISCO (AGS+ lub 4000) zapewniającego połączenia synchroniczne z prędkościami maksymalnie do 4 Mb/s, serwera komunikacyjnego (CISCO 516-CS) umożliwiającego dostęp asynchroniczny pojedynczym osobom i małym ośrodkom poprzez łącza dzierżawione lub komutowane z prędkościami do 38.4 Kb/s oraz maszyn typu SUN pracujących jako serwery sieciowe. Lokalnie w poszczególnych regionach routing jest rozwiązywany indywidualnie przez zainteresowane instytucje w zależności od ich potrzeb i możliwości. W kilku większych ośrodkach powstały sieci miejskie (MAN) oparte na połączeniach światłowodowych, które są wykorzystywane w Internecie i zapewniają bardzo szybkie i niezawodne przesyłanie danych między dołączonymi instytucjami. Podobna inwestycja jest w tej chwili realizowana w Warszawie.

Pomimo, iż Internet w NASK rozpoczął swą działalność stosunkowo niedawno, znacznie się już rozwinął dominując w większości ośrodków nad innymi typami sieci. W skali kraju na transmisje Internetowe przypada w tej chwili ponad 90% ogólnego ruchu po łączach komputerowych, co wskazuje, że jest to w tej chwili najbardziej popularna sieć w środowisku akademickim, stanowiąca podstawowy rodzaj łączności.

Warszawa, lipiec 1994

NASK w sieciach komputerowych Europy i świata

Maciej Kozłowski

Niniejszy przegląd jest poświęcony prawie w całości Internetowi. Zapewne Internet jest rozwiązaniem dalekim od ideału, który można by dziś zaprojektować. Słusznie czy nie - to jednak właśnie Internet jest siecią, która podbija świat. Co więcej, Internet przestał być "własnością" środowisk akademickich i naukowych i coraz powszechniej jest wykorzystywany przez komercję.

Główne systemy szkieletowe Internetu (NSFnet w USA, EuropaNET w Europie Zachodniej) ciągle są tworzone z myślą o użytkowniku akademickim, a komercja jest w nich nielegalna. Celem takiego podejścia nie jest jednak wąsko rozumiana potrzeba wsparcia technicznego środowisk naukowych i akademickich. Oznacza to tyle, że światowe sieci komputerowe są ciągle na wczesnym etapie rozwoju, zaś środowisko naukowe i akademickie, ze swej natury otwarte na nowości techniczne, stosunkowo tolerancyjne wobec pojawiających się czasem kłopotów technicznych oraz powiązane w skali światowej, jest najlepszym propagatorem, a w pewnym zakresie także twórcą tej nowoczesnej technologii telekomunikacyjnej.

1. Międzynarodowe łącza sieci NASK

Sieć NASK łączy się ze światowymi sieciami komputerowymi za pomocą linii Warszawa - Sztokholm (2 Mbps, satelitarna) i Warszawa - Wiedeń (128 Kbps, naziemna). Linie te prowadzą do do dwóch różnych ponadnarodowych systemów szkieletowych. Sztokholm jest miejscem dołączenia sieci NASK do sieci **NORDUNET**, zaś Wiedeń do **EBONE.** Linia do Sztokholmu stanowi także łącze podsieci X.25 do publicznych sieci pakietowych opartych o protokół X.25; stanowi ona także łącze w zakresie sieci **EARN.**

Linie Warszawa - Lwów oraz Warszawa - Moskwa (obie 9.6 Kbps; planowane jest zwiększenie szybkości transmisji do 64 kbps) pełnią rolę linii dołączeniowych naszych sąsiadów do sieci światowych za pośrednictwem sieci NASK. Podobny charakter będzie miała uruchamiana obecnie linia Warszawa - Mińsk oraz prawdopodobne łącze Warszawa - Wilno.

Przedstawmy teraz europejskie systemy szkieletowe; przede wszystkim wymienione wyżej **NORDUNET** i **EBONE** oraz **EuropaNET/DANTE**.

2. Międzynarodowe sieci szkieletowe w Europie

NORDUNET

NORDUNET jest ponadnarodową siecią szkieletową krajów nordyckich, utrzymywaną na mocy porozumienia krajowych sieci akademickich: SUNET (Szwecja), FUNET (Finlandia), DENet (Dania), UNINETT (Norwegia), SURIS (Islandia). Centrum operacyjne sieci znajduje się na Politechnice KTH w Sztokholmie. NORDUNET ma własne łącze transatlantyckie 1.5 Mbps. Jest włączony do GIX *(Global Internet Exchange)* w Waszyngtonie. Ważną okolicznością jest, że NORDUNET nie ogranicza się do tranzytu ruchu akademickiego, lecz akceptuje także ruch komercyjny.

EBONE

Międzynarodowa sieć transferowa EBONE została utworzona w 1991 r. jako konsorcjum naukowych i komercyjnych europejskich sieci komputerowych, koncentrujących się na IP. W 1993 r. EBONE liczyła ok. 25 organizacji członkowskich. Do połowy 1994 r. węzły głównej pętli EBONE znajdowały się w Paryżu, Amsterdamie, Londynie, Sztokholmie, Bonn, Genewie; węzłami dołączeniowymi były ponadto Madryt, Monachium, Wiedeń, Ateny. W II połowie 1994 r., po wykształceniu się transportu IP w ramach sieci EuropaNET, sieć EBONE zmniejszyła się. Obecnie podstawowe węzły są ulokowane w Paryżu, Genewie i Wiedniu. Najszybsze łącza, stanowią Paryż - Genewa (2 Mbps) i Paryż - Wiedeń (1 Mbps). Transportują one protokoły IP i ISO CLNS. Organizacje członkowskie to ACONET (Austria), BELNET (Belgia), CESNET (Czechy), CINECA (Włochy), DATANET (Finlandia), ECRC (Niemcy), FORTH (Grecja), HEANET (Irlandia), HUNGARNET (Węgry), NASK (Polska), PIPEX (Wielka Brytania), RCCB (Portugalia), RENATER (Francja), SANET (Słowacja), SWIPNET (Szwecja), TRANSPAC (Francja), Rumuńska Sieć Akademicka.

EBONE dysponuje łączem T1 do GIX w Waszyngtonie (współfinansowanym przez NSF). Od początku 1994 r. w EBONE, jest stosowany routing BGP-4, zapewniający CIDR - *Classless Interdomain Routing*, co stanowi antidotum na nadmiernie rozrośnięte tablice routingowe Internetu.

EBONE jest organizacją nie uprawiającą polityki, otwartą zarówno dla użytkowników akademickich jak i komercyjnych.

EuropaNET

EuropaNET wywodzi się z programu COSINE *(Cooperation for Open Systems Interconnection Networking in Europe)*, stanowiącego projekt nr 8 w ramach zachodnioeuropejskiej inicjatywy EUREKA, mającej na celu wzmocnienie współpracy krajów Europy Zachodniej w dziedzinie tworzenia i wykorzystania zaawansowanych technologii. Program ten, wykonywany w latach 1990-1993, doprowadził do utworzenia w 1992 r. systemu połączeń kilku akademickich i naukowych sieci komputerowych, znanego jako **IXI**, opartego o technologię OSI; w praktyce X.25 o szybkości przesyłania danych 64 kbps. Żywiołowy rozwój Internetu wymusił przekształcenie się IXI w **EMPB** - *European MultiProtocol Backbone*, oferujący oprócz X.25 także transmisję IP i CLNP *(Connectionless Network Protocol)*. EMPB stanowi obecnie fizyczne medium dla utworzonej pod koniec 1992 r. sieci **EuropaNET**. Sieć ta jest budowana przez holenderski PTT Telecom, zaś operowana przez **Unisource Business Networks** - mającą siedzibę w Hadze spółkę utworzoną przez szwedzki PTT Televerket, Szwajcarski PTT i holenderski PTT Telecom. W lipcu 1993 r. powstała "nieprofitowa spółka" **DANTE** *(Delivery of Advanced Network Technology to Europe Limited)*, za pośrednictwem której Komisja Wspólnot Europejskich finansuje rozwój szkieletu naukowych i akademickich sieci komputerowych w Europie. Właścicielem DANTE przez pierwszy rok była RARE (patrz dalej), zaś od połowy 1994 r. jest to spółka narodowych akademickich sieci komputerowych: niemieckiej DFN, szwajcarskiej SWITCH, włoskiej CNUCE, holenderskiej SURFNET, portugalskiej FCCN, brytyjskiej HEFC, słoweńskiej ARNES, a także przedstawionej wyżej nordyckiej ponadnarodowej sieci NORDUNET; prawdopodobne jest rozszerzenie tego grona o hiszpańską REDIRIS, grecką FORTHNET i belgijską BELNET. Siedzibą DANTE jest Cambridge. DANTE przejęła merytoryczną kontrolę nad siecią EuropaNET; odtąd nazwy DANTE i EuropaNET używane są zamiennie.

Zasadniczy szkielet sieci EuropaNET stanowią łącza 2 Mbps pomiędzy Londynem, Amsterdamem, Düsseldorfem, Brukselą, Bernem, Mediolanem i Madrytem. Ważniejsze linie dołączeniowe prowadzą do NORDUNETu i genewskiego CERN; linia do CERN - po zwiększeniu jej przepustowości do 2 Mbps - będzie stanowić główne łącze pomiędzy EuropaNETem i EBONE. Na czas konferencji INET'94/JENC5 w maju 1994 została uruchomiona (w oparciu o fundusze PHARE) linia 512 kbps Amsterdam-Praga.

Od połowy marca 1994 r. EuropaNET dysponuje transatlantyckim łączem 2 Mbps do GIX w Waszyngtonie. Planowane jest zwiększenie przepustowości tego łącza do 8 Mbps jeszcze w 1994 r. EuropaNET wykorzystuje także międzykontynentalną linię T1 1.5 Mbps CERN - Waszyngton.

W wieloprotokółowym szkielecie EuropaNETu są multipleksowane na zasadzie statystycznej protokóły X.25, IP, CLNP. W zakresie IP stosowany jest routing EGP i BGP-3; od kwietnia 1994 r. jest wdrażany routing BGP-4.

W planach DANTE jest koordynacja MHS w Europie (projekt pod nazwą MailFLOW; ogłoszono przetarg na wykonywanie tego zadania) oraz koordynacja słownika X.500 (będzie to kontynuacja wykreowanego przez EUREKA/COSINE projektu PARADISE). W kwietniu 1994 r. DANTE wygrał kontrakt Eureka/EuroCAIRN *(European Cooperation for Academic and Research Networking)* na wykonanie studium planu budowy "High Speed Service" - szkieletu sieci komputerowych w Europie dla środowiska akademickiego, opartego o linie 34 - 155 Mbps.

Częściowe finansowanie EuropaNETu przez Komisję Wspólnot Europejskich zapewnia tej inicjatywie bezpieczny sukces. Pewną niedogodnością EuropaNETu jest ograniczenie usług do środowiska naukowego i akademickiego; aktualnie sieć ta nie prowadzi tranzytu ruchu komercyjnego. Historycznym mankamentem inicjatywy IXI-EMPB było forsowanie protokołów OSI (tzn. w praktyce X.25) - już w sytuacji "eksplozji" IP w Europie.

3. CEENet

Stowarzyszenie CEENet *(Central and Eastern European Networking Association)* zostało ustanowione w dniach 14 - 15 lutego 1994 r. w Warszawie w wyniku porozumienia organizacji mających na celu budowę i utrzymanie akademickich i naukowych sieci komputerowych w krajach Europy Środkowej i Wschodniej.

CEENet skupia organizacje narodowe, mające na celu budowę i utrzymanie sieci komputerowych - przede wszystkim sieci naukowych i akademickich w krajach Europy Środkowej i Wschodniej. Każdy kraj jest reprezentowany przez jedną organizację, upoważnioną przez stosowny urząd centralny.

Aktualnie członkami CEENETu są:

ACONET - Austria,
ARNES - Słowenia,
CARNET - Horwacja,
CESNET - Czechy,
FREENET - Rosja,
HUNGARNET - Węgry,
LITNET - Litwa,
MARNET - Macedonia,
NASK - Polska,
SANET - Słowacja,
UARNET - Ukraina,
UNICOM - Bułgaria,
Białoruś,
Rumunia.

Konstytucja CEENetu stanowi, że każdy kraj dysponuje jednym głosem w ramach "Zgromadzenia Ogólnego". Organizacją kieruje pięcioosobowy międzynarodowy Zarząd. Jego przewodniczącym jest aktualnie prof. T. Hofmokl. Sekretariat CEENetu jest ulokowany w Warszawie.

Celem CEENetu jest koordynacja działań w skali międzynarodowej akademickich i naukowych sieci komputerowych w krajach Europy Centralnej i Wschodniej. Przyjęto następujące ustalenia robocze, porządkujące docelowo międzynarodową łączność komputerową w tej części Europy:

- dąży się do ustanowienia szkieletu sieci, ze wskazaniem na oś Północ - Południe,
- Wiedeń jest miejscem dołączenia szkieletu do zachodnioeuropejskich systemów szkieletowych EBONE i EuropaNET,
- Warszawa jest miejscem dołączenia do sieci NORDUNET.
- Stosownie do potrzeb większości członków CEENetu w sieci szkieletowej będzie transferowany zarówno ruch akademicki jak i pozaakademicki.

Inicjatywa utworzenia CEENet'u była między innymi reakcją na niską efektywność pomocy Komisji Wspólnot Europejskich dla rozwoju akademickich sieci komputerowych w krajach Europy Środkowej (Polska, Węgry, Czechy, Słowacja, Bułgaria, Rumunia) w ramach programu PHARE/TACIS/COSINE, realizowanego w okresie 1991 - marzec 1994. II edycja tego programu (rozszerzonego na kraje bałtyckie, Słowenię i Albanię), planowana na lata 1994-1996, będzie realizowana (przez DANTE) w porozumieniu z CEENet.

4. EARN

EARN *(European Academic and Research Network)* jest organizacją, której głównym celem jest utrzymanie europejskiej gałęzi sieci komputerowej BITNET. Członkami EARN są narodowe organizacje odpowiedzialne za utrzymanie naukowych i akademickich sieci komputerowych w krajach europejskich (w tym NASK; prof. T. Hofmokl jest członkiem sześcioosobowego *Executive Committee EARN*), w północnej Afryce (Egipt, Tunezja, Algieria, Maroko, Kamerun), na Bliskim Wschodzie (Izrael, Syria, Iran, Jordania, Bahrein, Arabia Saudyjska) i w rejonie zakaukaskim (Azerbejdżan, Gruzja). Członkowstwo EARN nie jest obecnie związane z deklaracją utrzymywania lub budowy sieci EARN w danym kraju. W 1995 r. planowana jest fuzja organizacyjna EARN i RARE - *Reseux Asocies pour la Recherche Europeenne*; organizacji pełniącej rolę "parasola" nad wszystkimi naukowymi i akademickimi organizacjami sieciowymi w Europie (wspólna organizacja występuje pod roboczą nazwą NEWorg; rozpisano konkurs na ostateczną nazwę).

Stricte akademicka i naukowa sieć BITNET *(Because It's Time Network)* jest najstarszą obecnie akademicką siecią komputerową o zasięgu światowym. Została podarowana społeczności akademickiej w 1984 r. przez koncern IBM. Jest to hierarchiczna sieć, w której dane są przesyłane na zasadzie *"store and forward"* pod nadzorem protokołu *Network Job Entry - NJE*. Ta ostatnia nazwa ściśle definiuje granice sieci EARN/BITNET, stąd mówi się o niej jako o sieci NJE. NJE ma realizacje na platformach "mainframe'ów" IBM, VAX/VMS, SUN/OS, HP/UX.

Sieć obejmuje obecnie ok. 3000 komputerów. Rozwój Internetu powoduje powolny spadek ilości komputerów w sieci NJE (większość z nich jest włączona także do Internetu; możliwa jest także transmisja *"NJE over IP"*). Wydajne i dobrze zorganizowane usługi (przede wszystkim LISTSERV i BITFTP), a także aktywność grup operujących siecią każą przypuszczać, że utrzyma się ona jeszcze przez kilka lat. Na dowód znaczenia sieci NJE przytoczmy fakt "z własnego podwórka": pomimo że tylko 16 komputerów sieci NASK jest

włączonych do sieci EARN, to generują one ponad 10% ruchu na międzynarodowej linii Warszawa - Sztokholm.

Odpowiednikami europejskiej sieci EARN są CREN w USA i Meksyku, NETNORTH w Kanadzie, SCARNET w Południowej Ameryce, CAREN w Azji.

5. NSFNET

Spośród pozaeuropejskich sieci szkieletowych przedstawimy NSFNET - National Science Foundation Network w USA. Scharakteryzujemy także program jej rozwoju, ponieważ może on być modelowy dla rozwoju sieci komputerowych w innych krajach.

Sieć ta w założeniach służy środowisku naukowemu i akademickiemu, instytucjom zajmującym się szkoleniem oraz naukowym jednostkom firm komercyjnych w USA (inne zastosowania w zakresie komercji są nielegalne). Za pośrednictwem sieci regionalnych łączy ona ponad 1100 uniwersytetów i college'ów; także szkoły średnie, biblioteki i publiczne jednostki medyczne .

Sieć jest zarządzana przez spółkę *Advanced Network & Services Inc.*, która z kolei zawarła kontrakt na operowanie siecią ze spółką *Merit Network Inc.*

Połączenia długodystansowe są oparte o linie T3-45 Mbps. Ich topologię przedstawia załączony rysunek. W 1995 r. NSFNET będzie realizować program vBNS *(very-high-speed Backbone Network Service)*, przewidujący połączenie w pierwszej kolejności czterech centrów superkomputerowych NSF za pomocą linii 155 Mbps i w dalszej stopniowe zastępowanie szkieletowych linii T3 przez linie 155 Mbps. NSFNet transmituje średnio 400 GB danych w ciągu doby; od co najmniej trzech lat wielkość ta ulega podwojeniu w ciągu roku.

Plany na przyszłość są związane z angażującym 10 agencji federalnych (ARPA, NSF, DOE, NASA, NIH, NSA, NIST, NOAA, EPA, ED) programem HPCC - *"High Performance Computing and Communications: Toward a National Information Infrastructure"*. Jego strategiczne cele to: (1) umocnienie przodownictwa technologicznego USA w dziedzinie budowy i wykorzystania komputerów dużej mocy oraz w zakresie łączności komputerowej, (2) przyspieszenie rozwoju nowych technologii, wzmocnienie bezpieczeństwa narodowego, edukacja, rozwój służby zdrowia, ochrona środowiska, (3) włączenie kluczowych technologii do budowy Narodowej Infrastruktury Informacyjnej (NII) i promocja wybranych aplikacji NII. Kluczowymi zadaniami programu HPPC są: (1) Systemy Komputerowe Dużej Mocy, (2) Narodowa Sieć Naukowa i Edukacyjna NREN *(National Research and Education Network)*, (3) Zaawansowane algorytmy i technologia oprogramowania (4) infrastruktura w zakresie technologii informacyjnej, (5) zasoby naukowe i ludzkie (wspomaganie nauki, edukacja w dziedzinie technologii komputerowych). Szczególne znaczenie ma koordynowane przez NSF zadanie NREN, przed którym stawiane są następujące cele: (1) dostarczenie wydajniejszej łączności komputerowej dla środowiska naukowego i akademickiego, (2) przyspieszenie badań mających na celu rozwój i zastosowania technologii sieciowych .

Miarą sukcesu NREN jest przedstawienie opinii o możliwości zbudowania przeznaczonej dla użytku publicznego *"Information Superhighway"*.

W ramach programu NREN zostało utworzonych 6 rozległych systemów testowych dla gigabitowych technik sieciowych (do 2.4 Gbps w sieciach rozległych; laboratoryjnie do 30 Gbps obecnie i 100 Gbps w perspektywie). W skład grup testowych wchodzą przedstawiciele agencji rządowych, uniwersytetów, koncernów komputerowych i kompanii telefonicznych. Całość jest koordynowana przez CNRI - *Corporation for National Research Initiatives*. Kilka przedsięwzięć podobnego typu jest prowadzonych poza programem NREN.

6. Krajowe akademickie sieci komputerowe w Europie

Przykładem godnym naśladowania może być norweska sieć **UNINETT**, która już od ponad roku opiera się o szkielet 34 Mbps, rozciągający się od Oslo i Bergen po Tromso za kołem polarnym.

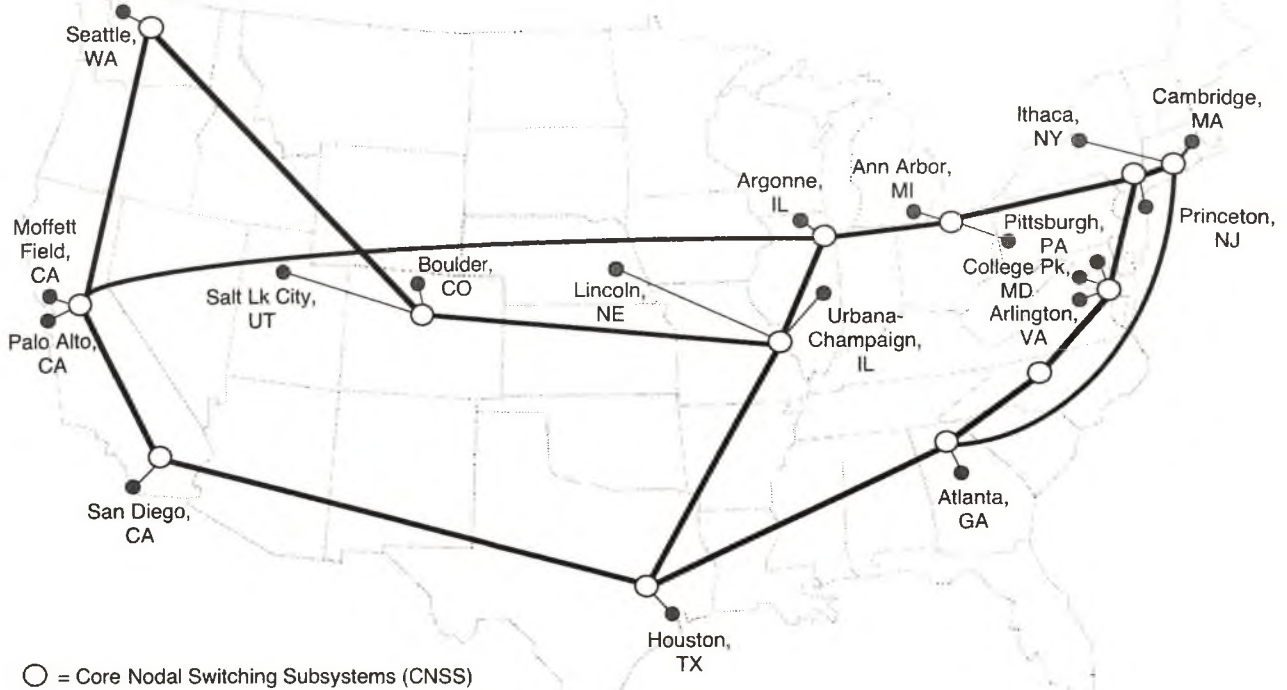
Holenderska sieć **SURFnet** buduje szkielet krajowy, którego trzonem będzie 9 linii 34 Mbps.

Francuska sieć **RENATER** przechodzi okres wielkich przeobrażeń, które mają doprowadzić do zbudowania krajowego szkieletu IP o zróżnicowanej architekturze.

Brytyjska sieć **JANET** buduje SUPERJANET - pilotowy szkielet ATM, z węzłami w Londynie, Manchesterze, Cambridge i Edynburgu.

Niemiecka **DFN**, po okresie wierności dla OSI, zdecydowała się na rozwijanie IP. Budowana jest pilotowa realizacja ATM z węzłami w Berlinie, Hamburgu i Kolonii.

NSFNET Backbone Service 1993



NSFNET Backbone Services provided by Advanced Network & Services (ANS)

Jak prezentuje się NASK w tym towarzystwie? Otóż dzięki silnym połączeniom międzynarodowym i krajowemu szkieletowi zdążającemu ku liniom 2 Mbps prawdopodobnie lepiej, niż mogłoby to wynikać z jego pozycji w tabeli 1, przedstawiającej liczbę komputerów włączonych do Internetu w krajach europejskich.

Tabela 1. Liczba komputerów zarejestrowanych w sieci Internet w poszczególnych krajach Europy. Źródło: baza RIPE; dane z 30 czerwca 1994 r.

Albania	0	Litwa	53
Algieria	7	Luksemburg	414
Łotwa	187	Macedonia	0
Austria	19614	Malta	0
Azerbejdżan	0	Maroko	0
Belgia	12115	Niemcy	142127
Białoruś	0	Norwegia	38788
Bułgaria	81	Polska	7184
Cypr	38	Portugalia	4312
Czechy	7326	Rosja	453
Dania	12138	Rosja	3223
Egipt	57	Rumunia	414
Estonia	638	Słowacja	1057
Finlandia	46924	Słowenia	836
Francja	68601	Szwajcaria	46415
Grecja	2798	Szwecja	55735
Gruzja	0	Tunezja	46
Hiszpania	21741	Turcja	1206
Holandia	59386	Ukraina	277
Horwacja	828	Węgry	5418
Irlandia	2542	Wielka Brytania	160209
Islandia	3161	Włochy	23513
Izrael	8171		
Jugosławia	0		
		razem	**758060**

7. Niepubliczne sieci prywatne o zasięgu światowym

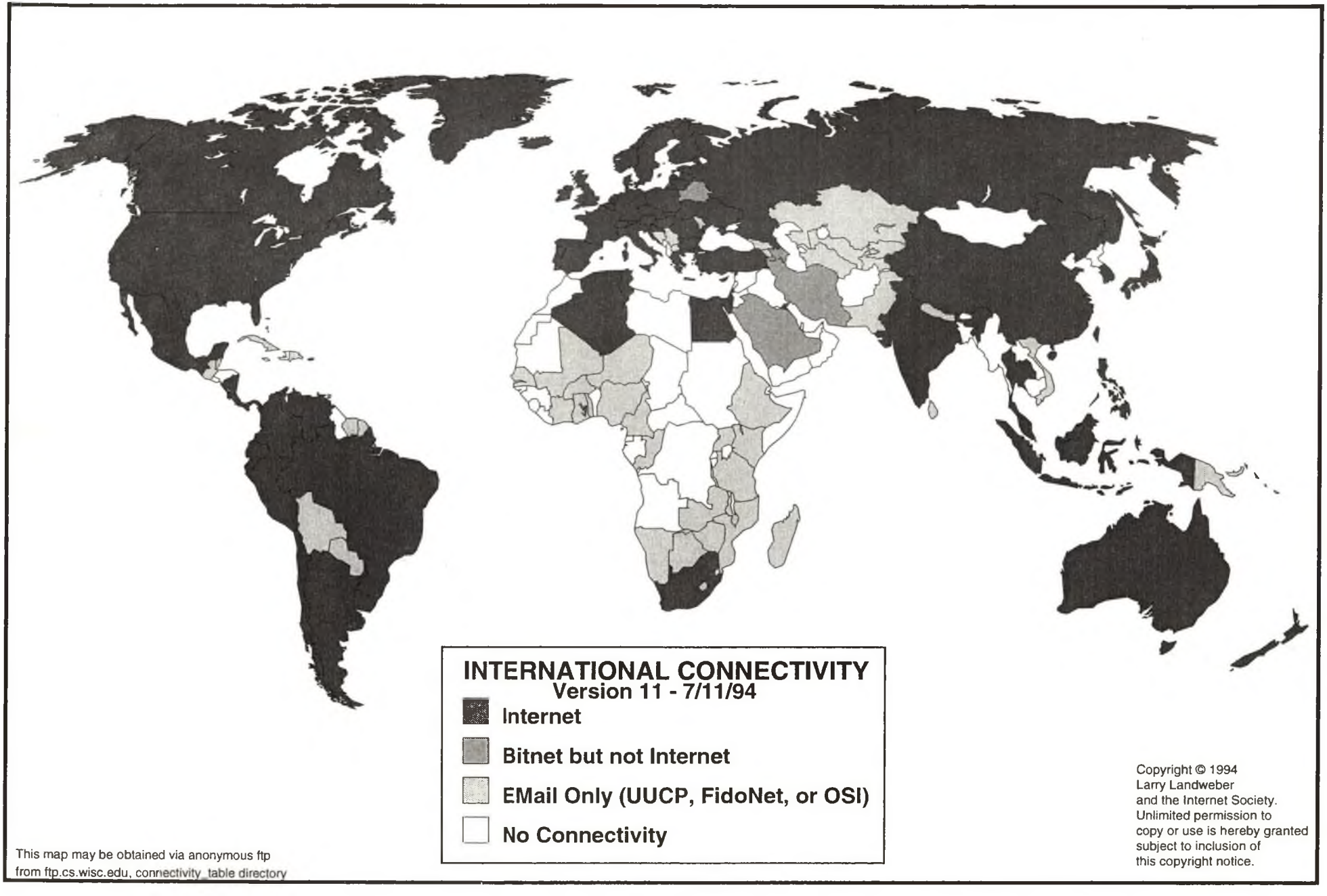
Jako przykłady takich sieci wymienimy HEPnet - *High Energy Physics Network*, SPAN - *Space Agency Network*, NSI - *NASA Science Internet*, ESNet - *Energy Science Network*, EASYnet - firmowa sieć *Digital Equipment*. Niektóre z nich to sieci dość stare: HEPnet, SPAN i EASYnet opierają się o nie stosowany dziś w otwartych sieciach światowych protokół DECnet phase IV.

8. Internet komercyjny

Compuserve, Sprintlink i Sprintmail, MCIMail, Alternet, Tymnet, Datapac, PSInet, EasyLink to publiczne sieci i serwisy komputerowe w USA i Kanadzie, dostępne za pośrednictwem "dial-up" w całym świecie. Nie miejsce tu na ich omawianie; ograniczmy się jedynie do uwagi, że obsługują one większą liczbę użytkowników, niż wszystkie naukowe i akademickie sieci komputerowe obsługują użytkowników naukowych i akademickich.

PIPEX (Wielka Brytania), **SWIPnet** (Szwecja), **TIPnet** (Szwecja), **ECRC** (Niemcy), **Transpac** (Francja) to przykłady komercyjnych sieci komputerowych w Europie, opierających się w przewadze o IP.

EUnet jest kooperacją ok. 30 opartych o Internet, komercyjnych sieci komputerowych w Europie, północnej Afryce i w krajach byłego Związku Radzieckiego (podług folderu: "od kręgu polarnego do północnej Afryki i od Islandii do Władywostoku"). Oprócz budowy sieci komputerowych w poszczególnych krajach EUNet posiada własne (dzierżawione) połączenia międzynarodowe. W krajach o słabo rozwiniętej infrastrukturze telekomunikacyjnej EUNet opiera się o sieci UUCP *(Unix-to-Unix-CoPy)*, ograniczając się w tym przypadku do transmisji poczty komputerowej. Szczególne znaczenie, ze względu na praktyczny brak innych połączeń komputerowych w tym obszarze, ma należąca do EUNet'u sieć UUCP Relcom, działająca w krajach byłego Związku Radzieckiego.



This map may be obtained via anonymous ftp
from ftp.cs.wisc.edu, connectivity_table directory

9. Koordynacja w zakresie Internetu

RIPE

RIPE *(Resaux IP Europeens)* z siedzibą w Amsterdamie jest organizacją stawiającą przed sobą cele koordynacji w zakresie administracji europejskich sieci IP; RIPE utrzymuje *Network Coordination Center - NCC*. NCC jest między innymi koordynatorem w zakresie udostępniania klas adresowych IP oraz "Domain Name Service". Nie miejsce tu na pełną charakterystykę RIPE; ograniczmy się do ogólników, że jest to organizacja bardzo aktywna, działająca na zasadzie spontanicznego porozumienia jej pracowników i licznych współpracowników.

GIX - the Global Internet Exchange

Internet przeewoluował od pojedynczej domeny z nie-hierarchicznym protokółem routowania EGP do kolekcji wielkich domen, w których obowiązują odmienne polityki routingu. Sztywne zasady wypracowane w pionierskim okresie rozwoju Internetu dziś ograniczają możliwości jego wzrostu. Idee systemu *"Global Internet eXchange"* to (1) umożliwić dołączanie nowych domen bez względu na ich wewnętrzną politykę, (2) wdrożyć skalowalną strukturę zarządzania routingiem, (3) umożliwić podejmowanie decyzji o drogach transferu ruchu w sytuacji, gdy są różne możliwości. Pilotowy GIX został wdrożony w 1993 r. w Waszyngtonie; opracowano plany utworzenia D-GIX - *Distributed Global Internet eXchange*. Węzły D-GIX znane są pod nazwami *De-Militarized Zones lub Neutral Interconnects*. Oprócz GIX w Waszyngtonie czynny jest CIX *(Commercial Internet eXchange)* w San Francisco.

Z inicjatywy DANTE, EBONE, EUNet, NORDUnet i RENATER (Francja) podjęto prace nad utworzeniem rozproszonego (Sztokholm, Amsterdam, Paryż) GIX w Europie.

10. Zakończenie (a właściwie początek)

Obecnie Internet - "sieć sieci" - łączy 32.000 sieci lokalnych (w tym 18.000 w USA); ich liczba podwaja się w skali 10 miesięcy. Tempo to może nawet wzrosnąć; co najmniej 30.000 sieci używających TCP/IP nie jest włączonych do Internetu, zaś dostępność oprogramowania sieciowego (w tym Mosaic) pod MS Windows spowoduje wzmożony nacisk na włączanie ich do Internetu.

W Internecie znajduje się obecnie 2.4 mln komputerów. Ich liczba podwaja się w skali 1 roku. Liczbę użytkowników trudno jest oszacować. Zapewne "10 użytkowników na 1 komputer", co się czasem podaje, jest wielkością zawyżoną, ale zważywszy na zasięg wielkich komercyjnych serwisów komputerowych w USA, z dokładnością do 30% można powiedziać że z Internetu korzysta 20 mln ludzi. W 1997 r. należy spodziewać się 70 mln użytkowników. Naturalnie, większość z nich będą to użytkownicy pozaakademiccy; nie ma tylu studentów i uczonych w tej części świata, w której obecnie rozwija się Internet. I tu jest odpowiedź na pytanie, czy Internet zachowa swój akademicki charakter. Oczywiście, że nie, chociaż... jak wspomniano wyżej, główne inwestycje w zakresie budowy szybkich sieci szkieletowych w USA i w Europie Zachodniej dotyczą środowiska naukowego i akademickiego. Powód jest przejrzysty: następuje nie tylko wzrost ilościowy sieci, ale także zmienia się ona technologicznie, zaś najlepszym użytkownikiem, którego można użyć do testowania i propagowania nowych technologii jest użytkownik akademicki. A więc początek; sieć jest ciągle młoda!

Warszawa, lipiec 1994

Usługa poczty elektronicznej według zalecenia X.400 w sieci NASK

Józef Janyszek

Wstęp

W każdej sieci komputerowej podstawową usługą jest poczta elektroniczna, czyli przesyłanie wiadomości (listów) między komputerami. Usługa poczty elektronicznej występuje zarówno w sieciach lokalnych jak i rozległych.
Naukowa i Akademicka Sieć Komputerowa "NASK" udostępnia usługi czterech podstawowych sieci rozległych:

- Bitnet-u/EARN-u
- Internet-u
- Decnet-u
- X.25

W sieci Bitnet/EARN usługa poczty elektronicznej jest realizowana w/g protokołu RSCS *(Remote Spooling Communication Subsystem)*. W sieci Decnet przesyłanie listów realizowane jest w/g protokołu Mail-11. Protokół SMTP *(Simple Mail Transfer Protocol)* stosowany jest do przesyłania listów w sieci Internet. Sieć X.25 realizuje usługę poczty elektronicznej w/g zaleceń CCITT i ISO znanych pod nazwą serii X.400. Wyszczególnione protokoły stosują różne sposoby przesyłania listów. W sieci Bitnet/EARN list jest zapamiętywany, a następnie przesyłany dalej *(store and forward)*. Przesyłanie listu w sieci Decnet wymaga bezpośredniego połączenia między komputerami. W sieciach X.25 i Internet listy przesyła się w trybie "zapamiętaj i przekaż" jak i w trybie połączeniowym.

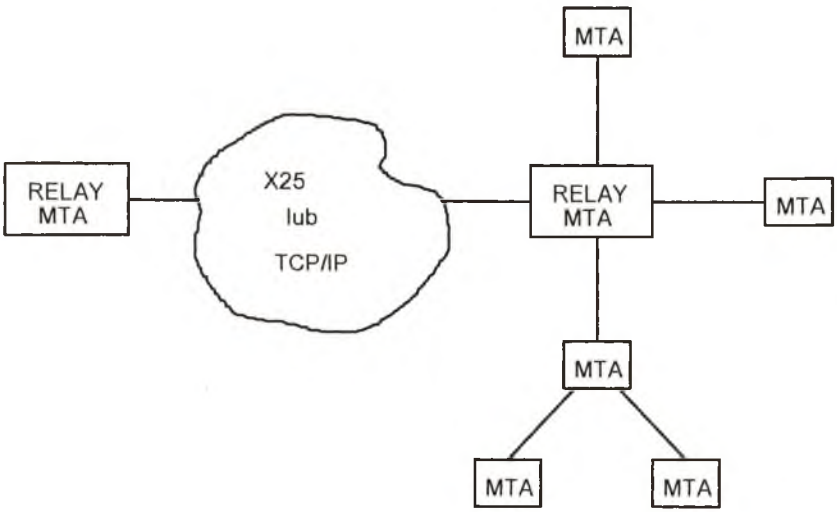
Sieci rozległe Bitnet/EARN, Internet, Decnet udostępnione poprzez sieć szkieletową NASK mają usługę poczty elektronicznej. Przedstawiona niżej usługa poczty elektronicznej w/g X.400 ma na celu wprowadzenie tej usługi również do sieci X.25.

Usługa poczty w/g protokołu RSCS i SMTP ma zasięg globalny (międzynarodowy). Poczta elektroniczna w/g protokołu MAIL-11 zapewnia tylko zasięg krajowy. Proponowana poczta elektroniczna w/g zalecenia X.400 będzie miała również zasięg globalny.

1. Infrastruktura poczty elektronicznej według zalecenia X.400

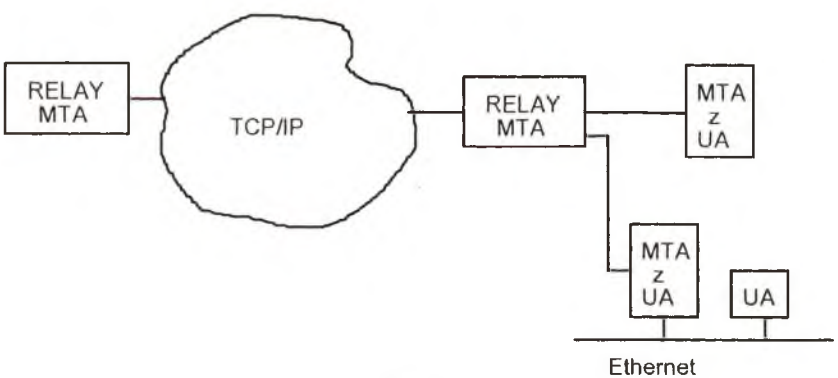
Poczta w/g zalecenia X.400 jest usługą sieci X.25. Do realizacji takiej usługi potrzebna jest typowa sieć X.25 (węzły - centrale komutacji pakietów połączone liniami telekomunikacyjnymi) oraz komputery dołączone do tych węzłów zwane MTA (Message Transfer Agent - agencja transportu wiadomości). W każdym krajowym środowisku poczty w/g X.400 znajdują się 1 lub 2 wyróżnione węzły wejściowe zwane RELAY - MTA, które komunikują się z podobnymi węzłami poczty X.400 poza granicami kraju. Aby węzeł poczty X.400 (MTA) mógł wysyłać lub odbierać pocztę elektroniczną musi być wyposażony w odpowiednie oprogramowanie znane pod nazwą UA (User Agent - agencja użytkownika), który komunikuje się z MTA w trybie serwer - klient. Krajowe środowiska poczty X.400 tworzą środowiska globalne tzw. MHS - Community. Sieci akademickie i badawcze tworzą środowisko poprzednio znane pod nazwą COSINE MHS, a obecnie pod nazwą GO - MHS (Global - MHS). Podobne środowisko tworzą środowiska krajowe udostępniające usługę poczty w/g X.400 w publicznych sieciach pakietowych. W każdym środowisku występuje jednostka koordynująca rozwój poczty elektronicznej w/g X.400 (włączanie nowych środowisk krajowych). Dla sieci akademickich i badawczych jednostką koordynującą jest zespół szwajcarskiej akademickiej sieci komputerowej SWITCH znany początkowo pod nazwą MHS-Project-Team. Z chwilą powołania do życia sieci Europanet i zespołu Dante - koordynującego działalność tej sieci, zespół ten przyjął nazwę MailFLOW - DANTE. Konfigurację typowego środowiska poczty w/g X.400 przedstawia rys. 1.

W publicznych sieciach pakietowych przesyłanie informacji między MTA odbywa się poprzez sieć X.25. Dostęp do węzłów poczty X.400 powinien też być zapewniony z sieci telefonicznej (fax) i dalekopisowej (telex). W sieciach akademickich i badawczych połączenie między węzłami poczty elektronicznej może być realizowane poprzez inne kanały niż X.25. Powszechnie do połączeń węzłów MTA stosowany jest kanał z połą-



Rys. 1.

czeniem pracującym w/g protokołu TCP/IP. W sieciach akademickich połączenie TCP/IP stosuje się również wtedy, gdy software UA załadowany jest na innym komputerze niż MTA. Takie rozwiązanie przedstawia rys. 2.



Rys. 2.

2. Adresowanie poczty X.400 w sieci NASK

Pole adresowe w/g X.400 składa się z części, które nazywamy atrybutami. Atrybuty dzielą się na atrybuty obowiązkowe i warunkowe. W polu adresowym mogą być też atrybuty określone przez domenę administracyjną.

Lista standardowych atrybutów przedstawia się następująco:

G – imię *(given name)*
I – inicjały *(initials)*
S – nazwisko *(surname)*
Q – wskaźnik pokoleniowy *(generation qualifier)*

O – organizacja *(organisation)*
OU1 – jednostka organizacyjna *(organisation unit 1)*
OU2 – jednostka organizacyjna 2
.
.
.
P – prywatna domena zarządzania *(private management domain)*
A – administracyjna domena zarządzania *(administration management domain)*
C – kraj *(country)*

Atrybuty S, A, C są atrybutami obowiązkowymi, pozostałe atrybuty z wyżej wyszczególnionej listy są atrybutami warunkowymi. Do listy atrybutów warunkowych zalicza się atrybuty niestandardowe, np.:
X.121 – adres sieciowy WTE121 - X.122 Network Address
E.164 – adres sieciowy ISDN - E.164 Network Address
N-ID – cyfrowy identyfikator agencji użytkownika *(User Agent Numeric ID)*
T-TY – rodzaj terminala *(Terminal Type)*
DDA: <type> atrybut określony przez domenę *(Domain Defined Attribute)*, gdzie <type> jest rodzajem atrybutu określonego przez domenę.

W sieci NASK przyjęto następujące atrybuty występujące w polu adresu w/g X.400:
G – imię
I – inicjały
S – nazwisko
OU1 – jednostka organizacyjna 1
.
.
.
OU4 – jednostka organizacyjna 4
O – organizacja
P – prywatna domena zarządzania
A – administracyjna domena zarządzania
C – kraj

3. Wartości atrybutów w sieci NASK

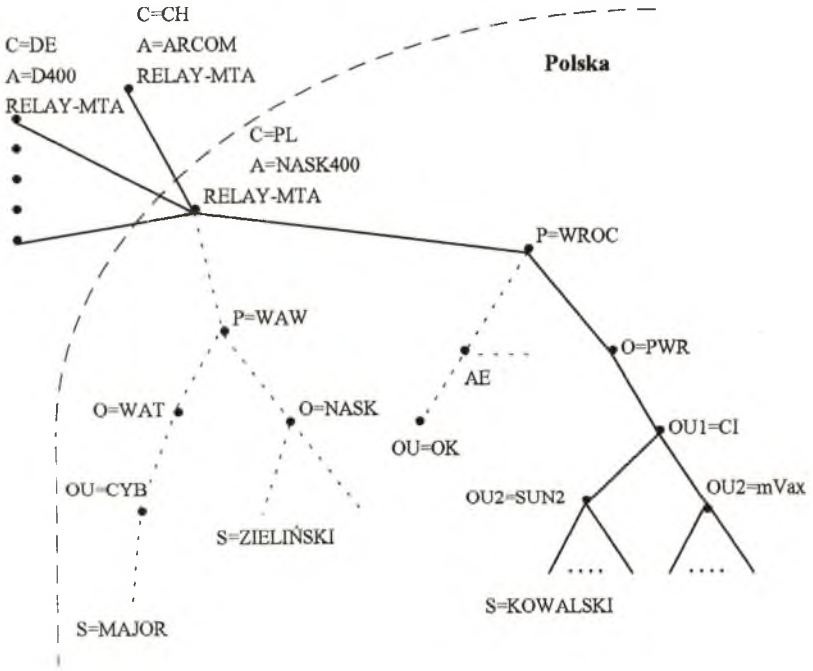
W sieci NASK atrybuty przyjmują następujące wartości:
Atrybut C = PL – wartość tego atrybutu jest ustalona przez międzynarodową instytucję normalizacji ISO *(International Standard Organisation)*
Atrybut A = NASK400 – wartość tego atrybutu przyjęto arbitralnie w konsultacji z kierownictwem JBR NASK. W kraju brak ostatecznych ustaleń jaka instytucja ten atrybut ma przydzielać. W opracowanych przez Instytut Łączności Oddział Gdańsk "Wymaganiach technicznych i eksploatacyjnych w systemie obsługi wiadomości" przedstawiono propozycję, aby wartość atrybutu przydzielał resort łączności
* UWAGA: Atrybuty C i A są atrybutami obowiązkowymi i muszą być umieszczone w każdym polu adresowym w/g zalecenia X.400.

Atrybut P – należy do atrybutów warunkowych, to znaczy że może się znaleźć w adresie X.400 ale nie musi. W sieci NASK wartości atrybutu P korespondują z regionami NASK. Przyjęto zasadę, że wartość atrybutu P odpowiada zarejestrowanej regionalnej, internetowej domenie. Zakłada się, że w najważniejszych regionach NASK będzie zainstalowany przynajmniej jeden węzeł poczty X.400. Oprócz istniejącego atrybutu P = wroc pojawią się atrybuty P = waw; P = poznan; P = lodz; P = torun; P = gda; itp
Atrybut O – atrybut O będzie przyjmował skrócone nazwy istytucji korzystających z usługi poczty X.400. Przykład dla Politechniki Wrocławskiej O = pwr; dla JBR NASK O = nask
Przykłady:
O=pwr - Politechnika Wrocławska
O=nask - JBR NASK

Atrybut OU1OU4 – wartościami atrybutu OU w sieci NASK są skrócone nazwy jednostek organizacyjnych korzystających z usługi w/g X.400. Przykłady OU=ci dla Centrum Informatycznego Politechniki Wrocławskiej. Jeśli jednostka organizacyjna posiada tylko jeden węzeł poczty X.400 (MTA), to atrybut OU może występować bez numeru. W przypadku większej ilości węzłów należy je zróżnicować poprzez wprowadzenie drugiego atrybutu OU.

Przykład:
CI posiada dwa węzły poczty X.400, które mają adresy:
OU2 = sun2; OU1 = CI; O = pwr; P = wroc; A = nask400;
C = PL
OU2 = mVax; OU1 = CI; O = pwr; P = wroc; A = nask400;
C = PL

Zainstalowane w sieci węzły poczty X.400 (RELAY-MTA i MTA) dopuszczają użycie do czterech atrybutów OU.



Rys. 3.

Znaczenie poszczególnych atrybutów pola adresowego pokazuje rys. 3.

4. Realizacja poczty w sieci NASK

W sieci NASK węzeł wejściowy poczty X.400 znajduje się we Wrocławiu i jest zrealizowany na bazie komputera SUN SPARC 2 z oprogramowanem ISODE/PP. Węzeł wejsciowy (RELAY - MTA) posiada możliwość komunikowania się ze światem zewnętrznym poprzez kanał X.25 i TCP/IP. Ze względu na dużą zawodność połączenia X.25 (przez NASK, DATAPAK, EUROPANET), a także związaną z tym odpłatność zrezygnowano z połączenia poprzez kanał X.25. Węzeł wejściowy (RELAY- MTA) we Wrocławiu komunikuje się z innymi węzłami wejściowymi poza

granicami kraju tylko poprzez kanał TCP/IP, MTA wejściowe poza granicami kraju, które ma tylko kanał X.25 nie może się bezpośrednio komunikować z MTA wejściowym w sieci NASK.

Oprócz MTA wejściowego w sieci NASK zainstalowano jeden węzeł poczty X.400 (MTA) we Wrocławiu. Jest zrealizowany na bazie komputera SUN SPARC 2 z oprogramowaniem OSITEL. Połączenie między RELAY - MTA i MTA jest zrealizowane poprzez kanał X.25.

5. Wymiana listów między różnymi systemami poczty elektronicznej w sieci NASK

Po wdrożeniu poczty elektronicznej w/g zaleceń X.400 w sieci NASK będą występowały trzy różne systemy poczty elektronicznej: X.400, SMTP (Internet), RSCS (Bitnet).

Użytkownicy poczty w/g X.400 powinni mieć możliwość przesłania listów do użytkowników poczty sieci Internet i sieci Bitnet. Aby to umożliwić muszą być znane zasady konwersji adresów ze środowiska X.400 do środowiska w/g RFC 822 (adresowanie w sieci Internet) i odwrotnie.

Możliwe są trzy rozwiązania:

1. konwersja domyślna - kolejne atrybuty adresu X.400 opisywane są poddomenami adresu w/g RFC-822 i odwrotnie
2. konwersja poprzez tablice *(mapping)*
3. konwersja poprzez wprowadzenie własnego atrybutu tzw. DDA *(Domain Defined Attribute)*

Ze względu na występujące różnorodne systemy adresowania w polskiej części sieci Internet konwersja domyślna nie jest możliwa do zastosowania. Również konwersja poprzez zbudowanie odpowiednich tablic jest trudna do realizacji w sieci NASK, a ponadto wymaga uruchomienia specjalnego, automatycznego systemu konwersji typu "helpdesk".

W sieci NASK zastosowano więc konwersję poprzez zdefiniowanie własnych atrybutów.

5.1. Przesyłanie listów ze środowiska X.400 do sieci Internet

Wysyłając list z węzła poczty X.400 (MTA) do komputera w sieci Internet adresujemy go następująco:
C=PL; A=NASK400; P=INTERNET; DD RFC-822= Internet address

Tak zaadresowany list trafia do gateway'a. Gateway łączy środowiska X.400 i Internetu. Z pola adresu odrzucane są atrybuty C, A, P a wartość atrybutu DD RFC-822 posłuży do wysłania listu w kanał SMTP (Internet). Funkcję gateway'a spełnia komputer, który jest jednocześnie węzłem wejściowym poczty X.400 w sieci NASK.

5.2. Przesyłanie listów z komputerów w sieci Internet do węzła poczty X.400

List adresujemy w sposób naturalny oddzielając wartości poszczególnych atrybutów kropkami.
Przykład: chcąc wysłać list pod adres C=pl; A=nask400; P=wroc; O=pwr; OU1=ci; OU2=sun; S=kowalski piszemy
kowalski@sun2.ci.pwr.wroc.nask400.pl
Tak zaadresowany list trafia na gateway'a we Wrocławiu, a dalej jest wysyłany w kanał X.400. Aby taka realizacja była możliwa konieczne było stworzenie domeny internetowej "nask400.pl".

5.3. Przesyłanie ze środowiska X.400 do sieci EARN/Bitnet

Listy do sieci EARN/Bitnet przesyłamy analogicznie jak do sieci Internet tj. poprzez tzw. atrybut określony przez domenę (DDA). Różnica polega tylko na tym, że w polu "Internet address" podajemy nazwę komputera w sieci Bitnet oraz po kropce dopisujemy słowo "bitnet".

Przykład:
C=pl; A=nask400; P=internet; **DD RFC-822=bitnet address.bitnet**
Tak zaadresowany list trafia do gateway'a, który poprzez kanał SMTP przesyła go do centralnego komputera sieci EARN/Bitnet w Polsce tj. do komputera PLEARN i dalej poprzez sieć Bitnet trafia do odbiorcy.

5.4. Przesyłanie poczty z sieci Bitnet do środowiska X.400

Podobnie jak w Internecie list adresujemy w ten sposób, że wartości atrybutów, oddzielone kropką piszemy od końca.
Przykład:
chcąc wysłać list na adres X.400
C=pl; A=nask400; P=wroc; O=pwr; OU1=ci; OU2=sun2; S=xxx
piszemy
xxx at sun2.ci.pwr.wroc.nask400.pl

6. Rozwój poczty X.400 w sieci NASK

Przewiduje się, że w każdym rejonie NASK powinien być przynajmniej jeden węzeł poczty X.400 (MTA). Węzły poczty X.400 mogą być połączone z węzłem wejściowym zarówno przez kanał X.25 jak i kanał TCP/IP.

W 1994 roku przewiduje się instalację węzłów poczty X.400 w następujących ośrodkach akademickich: Warszawy, Krakowa, Lublina, Białegostoku, Katowic, Gliwic, Poznania, Gdańska, Szczecina, Torunia, Łodzi. Węzły poczty X.400 będą instalowane w oparciu o następujące oprogramowanie: PP, OSITEL, MRX400.

Bibliografia:

[1.] Materiały udostępnione drogą elektroniczną w kartotece MHS na serwerze "Gopher nic.switch.ch"

[2.] Wymagania techniczne i eksploatacyjne na system obsługi wiadomości - Instytut Łączności - Zakład Służb i Usług Telekomunikacyjnych.

Wrocław, lipiec 1994

Serwisy baz danych i katalogi biblioteczne dostępne poprzez NASK

Bożena Zaperty

Wśród systemów informacyjnych dostępnych on-line zarysowują się dwie grupy:

1. Serwisy informacyjne on-line
2. Katalogi biblioteczne on-line

W trybie on-line system udostępniany jest wszystkim użytkownikom będącym abonentami komputerowych sieci regionalnych.

Serwisy informacyjne on-line to systemy wielobazowe gdzie bazy składowe zawierają informacje bibliograficzne lub faktograficzne z jednej dziedziny lub grupy nauk.

Katalogi biblioteczne on-line są narzędziem informacji służącym do znalezienia dokumentu, którego cechy znamy. Informują nas również czym dysponuje biblioteka i przyczyniają się do skrócenia czasu potrzebnego na odnalezienie opisu dokumentu.

Długo trzeba byłoby wymieniać wszystkie serwisy informacyjne on-line i dostępne w nich bazy danych osiągalne poprzez Naukową i Akademicką Sieć Komputerową. Do najbardziej popularnych zasobów informacyjnych wśród polskich użytkowników sieci komputerowych należą między innymi: DATA- STAR, DIALOG, STN, ECHO, EUROBASES, DISCUS, EUROKOM, ASTRA, QALICE, QSPIRES, PREPRINTY, EMBL, PATENTY. Od czerwca 1994 r. jest już w sieci polski serwis informacyjny KOLIBER.

Większość z baz danych dostępna jest za pośrednictwem więcej niż jednego serwisu. Dlatego pozwolę sobie na szczegółowy opis baz jednego z największych serwisów europejskich Data-Star.

DATA-STAR

Tematyka baz danych Systemu Data-Star.

Data-Star jest jednym z największych, europejskich serwisów informacyjnych z siedzibą w Bernie. Powstał w 1981 r. dzięki Radio Suisse. System ten oferuje ponad 300 baz danych i specjalizuje się w dostarczaniu informacji o Europie i dla Europy.

Tematyka informacji w Data-Star obejmuje następujące dziedziny: biznes, biomedycynę, chemię oraz technikę. Oprócz tego są bazy informacji prasowej, obsługi systemu a także bazy szkoleniowe.

Wśród baz biomedycznych znajdują się wszystkie najważniejsze bazy dostępne na świecie, takie jak:

Medline - obszerne źródło informacji medycznej obejmujące stomatologię, weterynarię, medycynę i psychologię.

Exerpta Medica - zapewnia aktualną i wszechstronną informację o lekach i farmakologii.

Biosis - prezentuje osiągnięcia badawcze z podstawowych dyscyplin biologicznych: zoologii, genetyki, botaniki i mikrobiologii.

CAB Abstracts - obejmuje rolnictwo w szerokim znaczeniu łącznie z leśnictwem, żywieniem zwierząt, naukami weterynaryjnymi, produkcją rolną, zabezpieczeniem plonów, ogrodnictwem, biotechnologią i wieloma dziedzinami pokrewnymi.

Martindale Online - zawiera informacje o lekach i środkach terapeutycznych używanych na całym świecie.

IMSWorld Patents International - baza patentów ocenionych produktów farmaceutycznych z IMSWorld. Obejmuje ponad 1000 rodzin opatentowanych produktów farmaceutycznych.

Science Citation Index - najbardziej aktualny, wielodyscyplinarny indeks międzynarodowej literatury naukowej i technicznej.

AIDS Database - zawiera autorytatywne komentarze jak również streszczenia prac o AIDS, HIV.

PsycINFO-Psychological Abstracts - obejmuje światową literaturę ze wszystkich obszarów psychologii i związanych z nią dyscyplin.

Wśród baz chemicznych występują znane bazy chemiczne, takie jak:

Chemical Abstracts - zapewnia informację o nowych osiągnięciach odnośnie reakcji, substancji chemicznych, materiałów, technik, procesów, aparatury, własności, teorii i zastosowań w chemii i inżynierii chemicznej.

Food Science & Technology Abstracts - zbiera informacje publikowane na cały świat o żywności i jej technologii. Producentem bazy jest International Food Information Service.

Chemical Business Newsbase - główne źródło informacji o biznesie w przemyśle chemicznym Europy, USA i Japonii.

Chemical Registry Nomenclature - baza stowarzyszona z Chemical Abstracts i Chemical Abstracts-Search, pozwala jednoznacznie identyfikować substancje chemiczne poprzez strukturę i nazwę.

East European Monitor-Chemicals - wyczerpujące źródło informacji biznesowej o Wschodniej Europie w sektorze przemysłu chemicznego.

Wśród baz z zakresu techniki występują między innymi:

Inspec - główne źródło międzynarodowej informacji z fizyki, inżynierii elektrycznej i elektronicznej, techniki komputerowej i kontroli sprzętu.

Energyline - unikalne źródło informacji o energii rozpatrywanej w aspekcie naukowym, inżynieryjnym, politycznym i społeczno-ekonomicznym.

Compendex Plus - baza zawierająca publikacje wydawnictwa Engineering Index Monthly.

Volkswagen-Vehicles Technology - dostarcza informacji o samochodach i przemyśle transportowym.

Najliczniejszą grupę stanowią bazy dotyczące biznesu, są wśród nich:

American Banker - wersja wpływowego dziennika American Banker.

CELEX - obejmująca pełną legislację wspólnot europejskich począwszy od traktatów poprzez akty wtórne, aż do propozycji.

Dun and Bradstreet Eastern Europe - rozszerza informację biznesową o szybko rozwijające się kraje takie jak: Polska, Węgry, Czechy i Słowacja. Informacja rynkowa obejmuje nazwę firmy, adres, datę założenia, liczbę zatrudnionych, sprzedaż, zysk i eksport.

Financial Times Business Reports - zawiera wiadomości, komentarze i analizy rynku w szerokim zakresie tematycznym.

Financial Times Reports-Eastern Europe - oferuje wiadomości i komentarze polityczne o rozwoju ekonomicznym na obszarze Wschodniej Europy. Analizuje aspekty przebudowy ekonomicznej i politycznej uwzględniając inwestycje, bankowość, zadłużenia, relacje pieniądza oraz wynikające z nich wnioski dla handlu z Zachodem. W tej bazie można znaleźć odpowiedź na pytanie, jak postępuje rozwój prywatyzacji w Polsce?

Investext Broker Reports - największa światowa baza o firmach i przemyśle, zawierająca pełne teksty raportów.

Predicasts - oferuje obszerną, międzynarodową sprawozdawczość o całej produkcji i usługach przemysłowych potrzebną do badania rynku oraz planowania.

Harvard Business Review Online - obejmuje tematykę strategii zarządzania dla profesjonalnych menedżerów.

Reuter Textline - zapewnia najwierniejszą i najszybszą informację o biznesie i wydarzeniach światowych. Zawiera wiadomości i komentarze z publikacji międzynarodowych o firmach, przemyśle, rynku, ekonomii oraz Raport Wspólnot Europejskich.

Od listopada 1992 r. dostępna jest największa baza edukacyjna **ERIC**, która umożliwia przegląd literatury edukacyjnej, obejmującej cały zakres szkolnictwa od przedszkola po szkoły dla dorosłych.

W maju 1993 r. włączona została wielodyscyplinarna baza spisów treści **Current Contents Search** stworzona przez Institute for Scientific Information. Udostępnia rekordy bibliograficzne z autorem i streszczeniem oraz pełną indeksację dla każdej znaczącej pozycji. Dodatkowo dostarcza kompletny spis treści wydawnictwa, z którego pochodzi artykuł.

System D-S posiada równie bazy informacji prasowej takie jak: **Swiss News Agency** w wersji francuskiej, niemieckiej i włoskiej, **Japan News Wire, USA Today**, brytyjska **Independent**, belgijska **De Financieel Ekonomische Tijd, Russian & CIS News,** włoskie **LaStampa, Mondo Economico, II Sole 24 Ore i L'Impresa oraz Jerusalem Post Electronic Edition.**

Bazy obsługi systemu to przede wszystkim:

Cross Directory Database - indeks wszystkich baz danych dostępnych w Data-Star, prosty w użyciu poprzez rozwijające się menu.

News Database - zawiera najnowsze informacje o bazach Data-Star, cenach i nowych cechach systemu.

Base Database - kompletny przewodnik online po każdej z baz danych Data- Star.

BiblioData-Full Text Sources Online - wersja online skorowidza źródeł pełnotekstowych, pomaga w poszukiwaniu baz danych, które zawierają pełne teksty gazet lub artykułów.

Ponadto dostępny jest światowy katalog baz danych **CUADRA DIRECTORY of Databases.**
Wszystkie bazy aktualizowane są raz albo dwa razy w miesiącu, a niektóre nawet co tydzień lub codziennie.
Serwis czynny jest 22 godziny na dobę z przerwą między 5.00 i 7.00 czasu GMT(Greenwich Mean Time).

Strategia poszukiwania informacji:

W większości baz danych wybór drogi przeszukiwania jest dość prosty, co sprawia, że Data-Star jest systemem przyjaznym. Podstawą wyszukiwania informacji w bazie danych jest sprecyzowanie wyrazu, frazy lub kilku wyrazów interesujących użytkownika. System odpowiada ile dokumentów zawiera wyszczególnione wyrazy, a następnie umożliwia wyprowadzenie tych dokumentów na ekran w całości lub wskazanej części.

Początkujący użytkownik, nie znający komend może poruszać się po bazach korzystając z rozwijającego się menu. Jednym z udogodnień systemu Data- Star są bazy treningowe, na których można ćwiczyć sposoby przeszukiwania bezpłatnie.

Bazy medyczne mają wbudowany tezaurus obejmujący całe słownictwo z dziedziny medycyny - Medical Subject Headings Vocabulary oraz spis periodyków z dziedziny biomedycyny. Często w trakcie połączenia z bazą pojawia się potrzeba przemyślenia strategii przeszukiwania, przejrzenia uzyskanych wyników. System umożliwia zawieszenie sesji i wstrzymuje na ten czas naliczanie kosztów pamiętając jednocześnie wyniki dotychczasowych przeszukiwań.

Data-Star udostępnia ponadto dodatkowe usługi, takie jak: poczta elektroniczna i możliwość zamówienia kopii oryginalnego artykułu, na podstawie którego powstał wybrany dokument bazy. Jednym z dostarczycieli dokumentów źródłowych jest British Library Document Supply Centre (BLDSC). Aby zamówić dokument źródłowy należy zarejestrować się jako użytkownik Data-Mail i BLDSC.

Przykładowy dialog z bazą:

Po zarejestrowaniu się w serwisie otrzymujemy na ekranie monitora menu:

```
Choice of Service
  1  Data-Star
  2  Data-Star FOCUS
  3  Tradstat
  4  Fiz-Technik, OAG, other gateways
  5  Data-Mail and Bulletin Boards

  7  Press
  8  Information on Networks
  9  Disconnect

ENTER SHORT CUT LABEL OR CHOICE :
```

Wybieramy opcję "1" aby przeszukiwać przy pomocy języka komend. W odpowiedzi system zapytuje nas czy chcemy obejrzeć dzisiejsze aktualności, a następnie prosi o podanie nazwy bazy.

```
ENTER YES IF YOU WOULD LIKE TO SEE TODAY'S ANNOUNCEMENTS_:

 TYPE DATAB SE NAME_:
```

Podajemy czteroliterowy akronim bazy np. CABI. Jest to baza informacji o rolnictwie i zgłasza się następująco:

```
D-S/CABI/CAB AGRICULTURAL ABS - FROM 1984 SESSION   5
  COPYRIGHT BY C.A.B INTERNATIONAL, WALLINGFORD UK

  D-S SEARCH MODE - ENTER SEARCH TERMS
  CABI    1_:
```

Poszukiwanym słowem niech będzie "sggw", od nazwy Szkoła Główna Gospodarstwa Wiejskiego. System odpowiada nam, że znalazł 36 dokumentów zawierających to słowo i zgłasza się promptem zawierającym nazwę bazy i nr kolejnego pytania.

```
RESULT    36
  CABI   2_:
```

Życzeniem naszym jest obejrzenie jednego ze znalezionych dokumentów. Wysyłamy polecenie: ..p all 1 co oznacza: wyświetl wszystko z pierwszego znalezionego dokumentu.

```
    1  CABI
AN  92-07-58307 921216
TI  Effect of cultivar, crop type, plant density and fertilizer
    application on yield and fodder value of beets. II. Fodder value
TT  Wplyw odmiany, formy użytkowej, obsady roslin i nawozenia na
    plonowanie i wartosc pastewna burakow. Cz. II. Wartosc.
AU  Kalinowska-Zdun-M, Podlaska-J, Broniecka-B.
IN  Katedra Szczegolowej uprawy, SGGW, Warsaw, Poland.
SO  Roczniki-Nauk-Rolniczych.-Seria-A-Produkcja-Roslinna 1991, VOL
    108, ISS 3, PG 125-137.
AT  NP(PART OF NUMBERED DOCUMENT).
YR  91.
LG  PO.
LS  RU, EN.
SC  0Q10101:    ROOT CROPS/ SUGARBEET (= SUGAR BEET 1973-1982)/
                AGRONOMY;
    0G2640:     COMPARISON OF SPECIES AND MIŻTURES/
                NONLEGUME FODDER CROPS.
DE  Sugarbeet; plant-density; Fodder-beet; fertilizers;
    nitrogen; phosphorus; potassium; roots; composition;
    proteins; fibre; oils; ash; leaves;Beta-vulgaris;
    chemical-composition; crude-fibre; crude-protein;
    nutritive-value.
CN  Poland
AB  In fieldtrials on good rye complex soil near Warsaw
    in 1976-78, sugarbeet cv. AJ Poly 1, sugar-fodder beet cv.
    Poly Past IHAR and fodder sugarbeet cv. Cyklop Poly were
    grown at 40 000 or 80 000 plants/ha and given 120, 160
    or 200 kg N + 90, 130 or 160 kg P + 120, ...
AV  0G03729062, 0Q08653045.
          END OF DOCUMENT
```

Powyższy przykład pokazuje najprostszy sposób przeszukiwania komputerowej bazy danych.

Adres DATA-STAR w sieci X.25:	022846431007014
w sieci Internet:	192.82.124.34 albo: atlas.rs.ch

DIALOG

DIALOG jest amerykańskim serwisem informacyjnym, który obejmuje następujące dziedziny: rolnictwo, żywność, chemię, energię, środowisko, medycynę, biologię, technikę, technologię komputerową, biznes, przemysł, firmy, patenty, znaki zastrzeżone, prawo, ustawy rządowe, socjologię, książki, czasopisma, artykuły, architekturę, sztukę, stowarzyszenia i tym podobne. Serwis DIALOG ma swoją główną siedzibę w Palo Alto w Kalifornii. Powstał on przede wszystkim jako system informacji bibliograficznej, choć zawiera również bazy faktograficzne i pełnotekstowe.

Adresy DIALOG-u w sieci X.25:	03106900803
	03106900061

STN International (The Scientific and Technical Information Network)

STN International udostępnia dane za pośrednictwem trzech ośrodków: Karlsruhe-Niemcy, Columbus-USA i Tokio-Japonia.

Informacje obejmują ważniejsze dziedziny nauki i techniki takie jak: chemia, energia, elektronika, telekomunikacja, inżynieria, architektura, budownictwo, środowisko, geologia, metalurgia, matematyka, komputery, medycyna, biologia, rolnictwo, fizyka, socjologia oraz patenty. Do obsługi systemu został stworzony specjalny język - messenger.

Umożliwia on wprowadzanie poleceń w trybie NOVICE dla początkujących użytkowników oraz w trybie EXPERT dla zawansowanych w przeszukiwaniu.

Adresy STN w sieci X.25:	026245724720001
	026245724790114
w sieci Internet:	192.132.3.254 albo: dialog.com

ECHO – **EUROPEAN COMMISSION HOST ORGANISATION**
EUROBASES – **THE COMMISSION'S COMMERCIALLY ACTING DATABASE HOST**

Serwisy Eurobases i ECHO powstały w 1980 roku jako systemy informacji wspomagające proces integracji krajów członkowskich Wspólnot Europejskich.

Bazy ECHO są podzielone na następujące kategorie:

1. Pomoc dla użytkownika.
2. Badawczo-Rozwojowe.
3. Struktury językowe.
4. Przemysł i ekonomia.

We współpracy z EUROBASES niektóre katalogi z ECHA są oferowane na zasadzie eksperymentu na rynku, jeżeli się sprawdzą są przenoszone do serwisu komercyjnego EUROBASES.

Hasło ECHO daje dostęp do czterech baz: I'M GUIDE, DG XIII MAGAZINE, EUREKA i NEWS ONLINE.

Baza **I'M GUIDE** zapewnia informację o bazach i bankach danych oraz ich producentach, CD-ROM'ach, host'ach, gateway'ach i brokerach informacji. Może pomóc nowemu i doświadczonemu użytkownikowi w wejściu w świat elektronicznej informacji.

Baza **DG XIII MAGAZINE** dostarcza informacji o działalności i programach utrzymywanych przez Generalny Dyrektoriat DG XIIItakich jak: ESPRIT, RACE, DELTA, VALUE, IMPACT. Informuje o aktualnych wydarzeniach, kluczowych decyzjach, nowych usługach i konferencjach.

EUREKA dostarcza szczegółów o projektach finansowanych przez program Eureka. Tworzy strukturę dla europejskiej, szeroko rozumianej, wychodzącej poza wspólnotę państw członkowskich, kooperacji w bada-

niach i rozwoju nowych technologii. Badania obejmują następujące dziedziny: transport, energię, lasery, biotechnologię, nowe materiały i środowisko.

NEWS ONLINE zawiera wiadomości z takich dziedzin jak: usługi oferowane przez europejskie hosty, poradniki dla użytkowników baz ECHO, aktualności o projektach, terminologia, wystawy, baza TED, serwis CORDIS.

Językiem wyszukiwawczym jest CCL - Common Command Language. Komendy CCL mogą być wprowadzane w trybie CCL po wyświetleniu "?".

Przeszukiwanie składa się z czterech etapów:

1.Wybranie bazy
BASE - wyświetla nazwy dostępnych baz
albo:
BASE nazwa_bazy

2.Sformułowanie pytania przy pomocy komend:
DISPLAY słowo_kluczowe - wyświetla alfabetyczny indeks słów rozpoczynając od podanego słowa
FIND słowo_kluczowe

3.Wyświetlenie wyników komendą:
SHOW
SHOW R=1 TO 2 - wyświetla dokument 1 i 2

4.Opuszczenie trybu CCL i powrót do głównego menu:
CALL ECHO
albo:
STOP - rozłączenie z ECHO

Użytkownicy powinni być zarejestrowani w ECHO aby mieć dostęp do wszystkich baz.

Serwis **EUROBASES** obejmuje siedem baz danych:

CELEX – zawierająca przepisy prawne Wspólnot Europejskich

ECLAS – katalog Biblioteki Centralnej Wspólnot Europejskich w Brukseli

EUROCRON – dane statystyczne o sytuacji socjalnej i ekonomicznej państw członkowskich Wspólnot Europejskich

INFO 92 – dane bibliograficzne i faktograficzne na temat tworzenia jednolitego rynku oraz informacje dotyczące usuwania barier fizycznych i monetarnych

RAPID – pełnotekstowy serwis prasowy oraz tzw. "Spokesman's Service"

SCAD – największa bibliografia Wspólnot Europejskich

SESAME – opisy projektów naukowo-badawczych

Dane z EUROBASES udostępnia się odpłatnie.

Adres ECHO w sieci X.25:	0270448112
w sieci Internet:	echo.lu
Adresy EUROBASES w sieci X.25:	0270429200
	0270429121

DISCUS (dawniej CONCISE)

Pod nazwą DISCUS kryje się Central European Information Server założony podczas realizacji programu COSINE, który będzie kontynuacją bazy CONCISE. Serwis DISCUS będzie dalej zapewniał informację o programie COSINE dzięki współpracy z organizacją DANTE, która zarządza siecią europejską dla potrzeb

nauki- EUROPANet. Przeszukiwanie bazy odbywa się przy użyciu komendy FIND albo rozwijającego się menu. Po wysłaniu komendy FIND podajemy słowo kluczowe albo wyrażenie logiczne zbudowane przy pomocy operatorów: and, or, not.

Baza DISCUS dostępna jest w sieci X.25, Internet oraz w systemie Gopher.
Adres DISCUS w sieci X.25: 023423440019315
w sieci Internet: discus.dante.net
Gopher Server: discus.dante.net

EuroKom

Eurokom jest komercyjnym systemem informacyjnym z siedzibą w Brukseli. Początkowo był sponsorowany przez Komisję Wspólnot Europejskich aby sprostać potrzebom komunikacyjnym programu ESPRIT. Obecnie udostępnia szeroki zakres usług dla tysięcy użytkowników z ponad dwudziestu krajów:

1. Pocztę elektroniczną
2. Konferencje komputerowe
3. Transfer plików
4. Połączenia teleksowe
5. Połączenia faksowe
6. Połączenia pocztą wewnętrzną ze światowymi ośrodkami badawczymi
7. Eurocontact - dobieranie partnerów badań

Serwis Eurocontact daje dostęp do czterech baz zawierających informacje o projektach naukowo-badawczych:

1. ESPRIT
2. DELTA
3. BRITE/EURAM
4. CRAFT

Dostęp do serwisu wymaga rejestracji, którą wysyłamy pocztą elektroniczną na adres:
eurokom_dublin at eurokom.ie

Adres EuroKom w sieci X.25: 0272431001992

ASTRA – APPLICATION SOFTWARE AND TECHNICAL REPORT FOR ACADEMIA

Dla użytkowników EARN/BITNET dostęp do serwisu ASTRA jest możliwy przez Interface z FTP lub MSG Protocol.
Aby zapisać się do grona użytkowników serwisu wysyłamy wiadomość:

tell astradb at icnucevm subscribe sys=vm imię nazwisko

Po zapisaniu się do ASTRY użytkownik otrzymuje dwa zbiory: "ASTRA EXEC" i "ASTRA INFO".
Pierwszy zbiór jest programem do zainstalowania Interface użytkownika ASTRA/VM i rozpoczęcia pierwszej sesji, drugi jest podręcznikiem. Na dysku systemowym powinien znajdować się uniwersalny moduł "IUCVTRAP MODULE", jeśli go nie ma należy pobrać komendą:

tell astradb at icnucevm get iucvtrap module

Język wyszukiwania: STAIRS *(Storage and Information Retrieval System)*
Informacje o bazach danych dostępnych w serwisie ASTRA są przechowywane w bazach META. Dla każdej bazy został zdefiniowany ABSTRACT, który zawiera tytuł, nazwisko autora, krótki opis bazy, tematykę i język.

Niektóre bazy tworzą logiczny związek dla tych samych argumentów. Kiedy użytkownik wysyła zapytanie do logicznej bazy, to pytanie jest wysłane do wszystkich baz będących w relacji z nią.

QALICE (Queries to ALEPH Library Information for CERN)

ALICE jest bazą bibliograficzną z dziedziny fizyki wysokich energii zlokalizowaną w CERN. Językiem wyszukiwawczym jest CCL -Common Command Language. Akceptuje zapytania wysłane komendą MAIL. Treść listu jest pusta, a zlecenie jest w polu "subject"

Adres systemu QALICE w sieci Internet: **qalice at uxlib.decnet.cern.ch**

QSPIRES (Queries to Stanford Public Information Retrieval System)

SPIRES jest to system baz z dziedziny fizyki cząstek elementarnych zlokalizowany w laboratorium SLAC w Kalifornii. Polecenia do bazy wysyłamy w trybie interakcyjnym komendą TELL, albo komendą MAIL. Pracując w trybie "MAIL" zlecenia piszemy w treści listu, każde w oddzielnej linii. Pomoc w korzystaniu z systemu QSPIRES można otrzymać wysyłając wiadomość:

tell qspires at slacvm help

Adres QSPIRES w sieci EARN/BITNET: **qspires at slacvm**

EPL - Electronic Preprint Library

W kwietniu 1992 r. w Międzynarodowej Szkole Studiów Podyplomowych SISSA-ISAS w Trieście uruchomiono Elektroniczną Bibliotekę Preprintów. EPL jest ogólnodostępną bazą danych. Za pośrednictwem poczty elektronicznej można przekazywać do bazy własne prace, jak również zamawiać preprinty znajdujące się w bazie.

Prace muszą być napisane pod edytorem klasy TEX-a.

EPL obejmuje następujące dziedziny badań:

-fizyka materii skondensowanej
-astrofizyka
-analiza funkcjonalna
-teoretyczna fizyka jądrowa
-fizyka doświadczalna cząstek elementarnych
-fizyka teoretyczna wysokich energii
-ogólna teoria względności i kosmologia kwantowa

Aby stać się subskrybentem jednej z baz wystarczy wysłać za pośrednictwem poczty elektronicznej zlecenie wpisane w pole "subject":

subscribe imię nazwisko

na adresy archiwów:

cond-mat at babbage.sissa.it - fizyka materii skondensowanej
astro-ph at babbage.sissa.it - astrofizyka
funct-an at babbage.sissa.it - analiza funkcjonalna
gr-qc at babbage.sissa.it - ogólna teoria względności i kosmologia kwantowa
hep-ph at babbage.sissa.it - fizyka doświadczalna cząstek elementarnych
hep-th at babbage.sissa.it - fizyka teoretyczna cząstek elementarnych
nucl-th at babbage.sissa.it - teoretyczna fizyka jądrowa

Po otrzymaniu potwierdzenia subskrypcji można zamówić HELP objaśniający jak korzystać z EPL.
Abonenci będą otrzymywać biuletyn informacyjny ze spisem nowowprowadzonych prac.

EMBL - EUROPEAN MOLECULAR BIOLOGY LABORATORY

W Europejskim Laboratorium Biologii Molekularnej w Heidelbergu dostępne są bazy z dziedziny badań genetycznych takie jak:

bazy sekwencji nukleotydów
bazy sekwencji protein.

Przeszukiwanie baz odbywa się poprzez wysłanie zapytań pocztą elektroniczną.

Format treści listu do bazy jest następujący:
1. W jednej linii może być tylko jedna komenda.
2. Obowiązkowa jest komenda SEQ, wszystkie pozostałe są opcjonalne i będą użyte ich domyślne wartości.
3. Można używać dużych i małych liter.
4. Kolejność komend nie jest ważna, ale SEQ powinna być ostatnia ponieważ wszystko co następuje po tej komendzie jest traktowane jako sekwencja.
5. Pusta linia i znak spacji są akceptowane.

Opis komend można otrzymać wysyłając list zawierający polecenie HELP na adresy:
netserv at embl-heidelberg.de
fasta at embl-heidelberg.de
quick at embl-heidelberg.de

Użytkownicy Naukowej i Akademickiej Sieci Komputerowej nie są już tylko biernymi odbiorcami informacji zagranicznych ale stopniowo wnoszą swój wkład udostępniając polskie bazy i katalogi biblioteczne.

W Centrum Informatycznym Uniwersytetu Warszawskiego, na komputerze IBM 3090 są zainstalowane dwie bazy danych Urzędu Patentowego.

INFPOL - zawiera informacje o patentach polskich od 1973 r. do chwili obecnej (187 tys. dokumentów).

INFPAT - obejmuje informacje o patentach międzynarodowych od 1985 r. do 1992r. (5 mln 276 tys. dokumentów). Źródłem informacji dla bazy INFPOL są dane bibliograficzne opracowane w Urzędzie Patentowym RP, a dla bazy INFPAT dostarczone przez Międzynarodowe Centrum Dokumentacji Patentowej INPADOC rejestrujące patenty z całego świata.

Bazy danych **INFPAT** i **INFPOL** są relacyjnymi bazami, zarządzanymi przez system SQL/DS *(The Structured Query Language/DataSystem).*

Informacje o interesujących patentach można uzyskać poprzez:
- zgłoszenie zamówienia do CIUW lub Urzędu Patentowego RP, które jest realizowane przez osoby upoważnione,
- samodzielne wyszukanie po uprzednim uzyskaniu zezwolenia na dostęp do bazy.

Do wyszukiwania informacji w bazach użytkownik dysponuje następującymi narzędziami:
1. Oprogramowany zestaw pytań.
   Są to programy napisane w języku PL/I umożliwiające wyszukanie pełnej informacji o patencie.
2. Pakiet QMF umożliwiający pracę w trybie PROMPT i SQL.

Aby otrzymać uprawnienia na dostęp do bazy należy wysłać prośbę na adres:
ewarz at plearn.end.pl albo **sqluser at plearn**.end.pl

Na serwerze **plearn.end..pl** są również dostępne polskie katalogi biblioteczne:
- Katalog Centrum Europejskiego UW
- Katalog Wydziału Filozofii i Socjologii UW
- Katalog Federacji Bibliotek Kościelnych FIDES

Przeglądanie katalogów odbywa się w systemie STAIRS. Wystarczy zarejestrować się na jedno z dziewięciu ogólnie dostępnych kont STAIRS1 do STAIRS9 z hasłem STAIRS.

SERWIS INFORMACYJNY "KOLIBER"

Twórcą serwisu informacyjnego **"KOLIBER"** jest poznańska firma *EUROSTART.* Niektóre z baz danych udostępniane w tym serwisie są bezpłatne, np.:
- Oferty firm polskich i zagranicznych
- Katalog polskiego oprogramowania
- Polskie firmy, "Pierwszy Kontakt"

Bazy komercyjne to:
- Międzynarodowe Targi Poznańskie (Wystawcy i ich oferty)
- Business Club 64 (Baza Klubowa)
- TELEFAX Poland (Dane adresowefirm i oferty)

W przygotowaniu jest baza **KOMPASS POLAND** czyli katalog polskich firm. Komendy systemu KOLIBER i jego organizacja odpowiadają rozwiązaniom przyjętym w amerykańskim serwisie DIALOG.

Połączenie z bazami danych można otrzymać w godzinach 8-18.

Adres serwisu KOLIBER w sieci X.25: 16111080

VTLS

Wdrażanie systemu VTLS (Virginia Tech Library System) w Polsce można śledzić na liście dyskusyjnej: **aibibl at plearn.edu.pl**

W systemie VTLS wyszukiwania prowadzone są według następujących kluczy:
- nazwiska autora
- tytułu
- hasła przedmiotowego
- słowa kluczowego
- wyrażenia logicznego
- sygnatury
- międzynarodowego znormalizowanego numeru książki (ISBN)
- międzynarodowego znormalizowanego numeru czasopisma (ISSN)

Komendę HELP można zastosować praktycznie w każdym momencie poszukiwania, aby uzyskać niezbędne wyjaśnienia, a "?" służy do uzyskania na ekranie terminala menu dla nowicjusza.

Adresy VTLS w sieci Internet:

Biblioteka Jagiellońska: **149.156.73.10** albo: **fridge.bj.uj.edu.pl**

Biblioteka UW: **148.81.207.1** albo: **limba.buw.uw.edu.pl**

Wśród zagranicznych katalogów bibliotecznych na uwagę zasługują Katalog Biblioteki Kongresu USA i System MELVYL.

BIBLIOTEKA KONGRESU USA

Katalog Biblioteki Kongresu USA dostępny jest w sieci Internet poprzez Data Research Associates (DRA). Zawiera on dokumentację książek, map, nut, czasopism, gazet, filmów, slajdów i wideokaset. Ogólnie dostępne konto GUEST umożliwia przeszukiwanie wg autorów i tytułów. Katalog przedmiotowy i słów kluczowych nie jest dostępny dla użytkowników GUEST'a. Pełen zakres możliwości wyszukiwawczych daje system LOCIS (Library of Congress Information System). Składa się on z dwóch systemów: SCORPIO i NUMS, ale przeszukiwania można prowadzić jednocześnie na obydwu systemach.

Adresy Biblioteki Kongresu USA w sieci Internet: **192.65.218.43** albo: **dra.com**
140.147.254.3 albo: **locis.loc.gov**

MELVYL

Na uwagę zasługuje również system MELVYL na Uniwersytecie w Kalifornii, który zawiera bazy MEDLINE, Current Contents, INSPEC dostępne przez Data-Star i DIALOG. Aby mieć dostęp do w/w zbiorów trzeba zawrzeć umowę z Uniwersytetem Kalifornijskim . Katalogi biblioteczne systemu MELVYL są ogólnie dostępne.

Wyszukiwania można dokonywać według:
- hasła autorskiego
- tytułu dokumentu
- hasła przedmiotowego
- wyrażeń logicznych zbudowanych przy pomocy operatorów: and, or, and not
- fragmentów słów

Można zawężać wyszukiwanie przez datę wydania dokumentu i jego język, poszukiwać według regionu geograficznego i poszczególnych miasteczek uniwersyteckich.

Adres MELVYL w sieci Internet: **melvyl.ucop.edu**

Prawie wszystkie istniejące systemy informacyjne mogą być przedstawione w modelu WWW (World-Wide Web). Inicjatywa światowej pajęczyny WWW jest praktycznym projektem, który ma stworzyć wszechświat globalnej informacji używając dostępnej technologii. Pajęczyna rozciąga się od małych notatek własnych na lokalnej stacji roboczej do dużych baz danych na innych kontynentach. System informacyjny WWW zbudowany jest w oparciu o hypertext tzn. tekst, który zawiera "łączniki" do innych tekstów. Na serwerze WWW w Instytucie Fizyki Doświadczalnej UW można znaleźć Bazę Informacji Skierowującej (BIS), która zawiera opisy polskich firm świadczących usługi informacyjne.

Adres serwera WWW: **info.fuw.edu.pl**

Drugim rozproszonym systemem informacyjnym umożliwiającym dostęp do różnych zasobów sieciowych jest Gopher. Struktura tego systemu podobna jest do organizacji katalogów z wieloma podkatalogami i zbiorami. Rozwijające się menu pozwala na przeszukiwanie katalogów znajdujących się na lokalnym komputerze jak również baz danych posadowionych na dowolnie oddalonym komputerze.

Do cenniejszych serwerów gopher'owych należą te, które dają możliwość poszukiwania źródeł informacji wg tematyki i lokalizacji a także adresów elektronicznych w różnych systemach.

Gopher serwer:	**umslvma.umsl.edu**	-źródła informacji wg tematyki
katalog:	library/subjects	
Gopher serwer:	**tcsul.texshare.utexas.edu**	-katalogi biblioteczne wg lokalizacji
katalog:	library_services	
Gopher serwer:	**gopher.cs.ttu.edu**	-adresy elektroniczne w różnych systemach
katalog:	Phone Books	

Warszawa, lipiec 1994 r.

X.500 Directory

M. Górecka, T. M. Wolniewicz, J. Żenkiewicz

1. Wstęp

Dynamiczny rozwój sieci komputerowych umożliwia kontakt pomiędzy rozproszonymi użytkownikami oraz wzajemny dostęp do zasobów i wymianę informacji o zasięgu zarówno lokalnym jak i globalnym.

Jednym z najbardziej rozpowszechnionych zastosowań sieci komputerowych są m.in. usługi poczty elektronicznej i dostępu do zasobów informacyjnych. Różnorodność i mnogość sieci komputerowych oraz protokołów sieciowych spowodowała konieczność unifikacjipoczty elektronicznej i usług w sieciach komputerowych. Przykładem tego podejścia jest rozwój, w ramach standardów OSI, protokołów poczty elektronicznej X.500 i usług informacyjnych X.500 Directory.

Niniejszy referat zawiera podstawowe informacje o usługach X.500 *(X.500 Directory Services)* oraz przedstawia koncepcję rozwoju pilotowej sieci X.500 Directory dla środowiska naukowo-akademickiego w Polsce w oparciu o Naukową i Akademicką Sieć Komputerową NASK.

2. Ogólne informacje o X.500 Directory

2.1 Definicje

X.500 jest zbiorem norm CCITT z 1988 roku, uaktualnionych w 1992. Normy te definiują system rozproszonej bazy danych opartej na wielorakich protokołach łączności. W założeniu X.500 miało służyć powstaniu globalnej informacji adresowej wykorzystywanej między innymi przy transporcie poczty elektronicznej (X.400).

Obecnie przez X.500 rozumie się zarówno sam zbiór norm, jak również działającą ogólnoświatową służbę, w ramach europejskiego projektu PARADISE i amerykańskiego WhitePages .

2.2 ISODE

ISODE *(ISO Development Environment)* jest implementacją wybranych protokołów i aplikacji OSI, które pracują w szerokim zakresie środowiska systemów operacyjnych UNIX lub UNIX-o podobnych.

Pakiet ten jest w chwili obecnej absolutnie dominującym na rynku dostępnego oprogramowania implementującego OSI Directory services. Spowodowane jest to przede wszystkim tym, że ta dojrzała implementacja była do tej pory dostępna bez ograniczeń. Z końcem roku 1992 zakończone zostały prace nad ogólnodostępnymi wersjami ISODE. Sytuacja ta najprawdopodobniej ułatwi wejście na rynek innym - komercyjnym implementacjom standardu; przez długi okres należy jednak spodziewać się dominacji ISODE zwłaszcza, że ośrodkom uniwersyteckim udostępniane ono będzie w formie niedopłatnych licencji.

Zasadnicze komponenty ISODE to:

- obsługa katalogów OSI Directory Service (QUIPU): DSA *(Directory System Agent)* oraz DUA *(Directory User Agent)*,
- implementacja systemu dostępu i zarządzania transferem zbiorów (FTAM),
- implementacja protokółu zdalnego dostępu *(VT - virtual terminal)*,
- implementacja protokółu SNMP w postaci serwera i prostego klienta,
- obsługa poczty MHS *(Message Handling Services)* : MTA *(Message Transfer Agent)* - oprogramowanie PP korzysta z bibliotek ISODE.

Część ISODE obejmującą X.500 Directory (QUIPU) jest kompletną implementacją zarówno serwera (DSA) jak i kilku interfejsów użytkownika (DUA). Dokładniejszy ich opis podajemy w części "Dostęp do zasobów".

Poza ISODE na szczególną uwagę zasługuje implementacja LDAP *(Lightweight Directory Access Protocol)* tworzona na Uniwersytecie w Michigan, która nadzwyczajnie upraszcza tworzenie interfejsów DUA.

2.3 Struktura X.500 Directory w ramach projektu PARADISE

X.500 Directory jest rodzajem "światowej książki telefonicznej". Zawiera szeroki wachlarz informacji o organizacjach, jednostkach i osobach, łącznie z możliwością zapisu fotograficznego i dźwiękowego. Zasada działania X.500 Directory jest podobna do internetowych Name-Serwerów. Ustanowiona jest sieć serwerów, komunikujących się między sobą za pomocą specjalnego protokółu X.500 *(DSP - Directory Service Protocol)*. Zaimplementowana jest metoda replikacji i buforowania danych przez serwery.

Projekt pilotowy X.500 Directory jest inicjatywą rozwijającą się głównie w środowisku akademickim znaną w Europie jako PARADISE Project. Analogiczna inicjatywa w USA znana jest jako PSI White Pages Project. Zadaniem PARADISE było ustanowienie pilotowej instalacji X.500 i wykorzystanie jej do testowania protokołu i jego różnych implementacji.

Każdy kraj biorący udział w projekcie ma serwer na szczeblu kraju, zarejestrowany w serwerze poziomu "root". Administrator serwera poziomu krajowego jest odpowiedzialny za koordynację łączności (komunikacji) z serwerami niższego poziomu, które obsługują organizacje. Organizacje mogą być podzielone na mniejsze jednostki obsługiwane przez serwery niższych szczebli. Analogicznie jak administratora poziomu krajowego, ustanawia się administratorów serwerów niższych poziomów z podobną odpowiedzialnością.

Inicjatywa projektu PARADISE sponsorowana przez RARE powstała w 1990 roku w ramach programu COSINE. Eksperymentalna wersja projektu pilotowego PARADISE została zakończona. Kontynuacja będzie w przyszłości koordynowana w oparciu o składki od uczestniczących w projekcie krajów pokrywające koszty służb centralnych.

Rozwój fazy pilotowej X.500 Directory w poszczególnych krajach jest bardzo zróżnicowany. Część krajów ma szeroko zakrojone programy i udostępnia znaczne ilości danych, inne mają bardzo wyrywkowe dane, rzadko aktualizowane. W obecnej chwili w projekcie biorą udział wszystkie kraje europejskie z wyjątkiem krajów dawnej Jugosławii i niektórych krajów byłego Związku Radzieckiego. Najbardziej zaawansowane są W. Brytania, Holandia, Szwajcaria, Dania, Finlandia, Francja i Norwegia.

Pilotowy program PARADISE koordynowany był do tej pory przez University College London. Usługi X.500 Directory zabezpiecza University of London Computer Centre (ULCC) przy wsparciu firmy NEXOR. Punktem podstawowym usług jest udostępnienie centralnego DSA (serwera) i DUA (interfejsu użytkownika).

Polska bierze udział projekcie PARADISE od lipca 1992. Od października 1992 patronat nad polskim projektem sprawuje NASK. W chwili obecnej pracuje sześć serwerów (centralny - na UMK Toruń oraz regionalne: Toruń, Warszawa, Kraków, Wrocław, Poznań). Regionalny serwer toruński prezentuje kompletne dane na temat Uniwersytetu Mikołaja Kopernika, pozostałe serwery są w fazie rozruchowej lub eksperymentalnej.

2.4 Dostęp do zasobów

Jak już zostało wspomniane X.500 jest rozproszoną bazą danych przechowującą zasoby w serwerach DSA. Konkretna implementacja samego serwera nie jest oczywiście zdefiniowana przez X.500. W przypadku QUIPU hierarchiczna struktura X.500 Directory jest odwzorowywana wprost na strukturze drzewa katalogów serwera. Dane przechowywane są w postaci tekstowej i w całości ładowane do pamięci w momencie startu serwera; nie ładuje się jedynie danych przechowywanych w postaci oddzielnych zbiorów (np. obraz czy dźwięk). Z uwagi na taki sposób rozwiązania serwera, duże bazy danych wymagają maszyn o rozbudowanej pamięci operacyjnej. Kolejne wersje ISODE mają mieć możliwość odwoływania się do danych bezpośrednio na dysku i w ten sposób umożliwiać obsługę dużych baz bez zajmowania wielkich obszarów pamięci operacyjnej.

Internetowe serwery w projekcie PARADISE nasłuchują z reguły na porcie 17003, ale jest to parametr zawarty w opisie każdego serwera i może być dowolnie modyfikowany. Serwer QUIPU jest w stanie obsługiwać wielokrotne połączenia nie rozczłonkowując się (bardzo istotne ze względu na duże rozmiary programu).

Struktura danych jest całkowicie modyfikowalna i zapisywana w tekstowych plikach konfiguracyjnych. Oczywiście niezbędne jest zachowywanie umiaru w wykorzystywaniu tych możliwości konfiguracyjnych, tak aby nie doprowadzić do nieczytelności danych przez nieprzystosowane specjalnie interfejsy.

X.500 zawiera mechanizmy ochrony danych. Możliwe jest udostępnianie tylko części atrybutów wszystkim użytkownikom, a wszystkich jedynie wybranej grupie. Można żądać, aby każdy użytkownik musiał być zarejestrowany w bazie X.500, podobnie można wymagać, aby tożsamość była potwierdzana podaniem hasła. Istnieją mechanizmy pozwalające na przykład, na wyświetlanie zasobów bazy, ale niedopuszczające do jej

przeszukiwania. Trzeba przy tym podkreślić, że ochrona danych jest obecnie mało stosowana, ale trwają prace nad jej rozszerzeniem, prowadzone w ramach projektu PASSWORD.

W skład ISODE wchodzi DSA oraz kilka DUA, między innymi interfejs administratora (dish), prosty interfejs dla terminali tekstowych (de) i zaawansowany interfejs dla X-windows (pod).

W oparciu o biblioteki ISODE rozwijane są DUA nie będące częścią składową ISODE, ale znacznie wzbogacające możliwości kontaktu użytkownika z Directory. Wspomniany wcześniej LDAP jest systemem pośredniczącym pomiędzy klientem a serwerem. Jest to proces, który spełnia rolę klienta dla DSA oraz serwera dla specjalnie skonstruowanego DUA. Standardowy protokół dostępu do danych *(DAP - Directory Access Protocol)* jest bardzo rozbudowany i w większości wypadków klient wykorzystuje zaledwie część możliwości. W tej sytuacji protokół implementujący tylko te najważniejsze cechy DAP umożliwia znaczne "odchudzenie" programów i uproszczenie ich tworzenia. W oparciu o LDAP powstaje większość nowych interfejsów. Zaimplementowane są między innymi interfejsy sprzęgające X.500 z pocztą elektroniczną, gopherem i WWW, jak również implementacje DUA na komputerach klasy PC czy Macintosh.

Wiele ośrodków posiada anonimowe konta udostępniające interfejsy de i dish. Przykładowo w Polsce konta takie są na komputerach: **jaguar.cc.uni.torun.pl** oraz **anna.mat.uni.torun.pl**. Podstawowe funkcje interfejsu de są tak proste w obsłudze, że nie wymagają żadnej instrukcji. Bardziej zaawansowane opisane są w dokumentacji autorstwa M. Kus *X.500 Directory - opis użytkowy programu DE.*

Dostęp do danych można uzyskać rownież za pomocą gophera (np. na **gopher.mat.uni.torun.pl**) czy WWW (**http://jaguar.cc.uni.torun.pl:8888/MC=PL**). Poczta na adres **X.500@mat.uni.torun.pl** uruchamia e-mailowy interfejs do zasobów UMK. List zawierający linię help spowoduje wysłanie prostej instrukcji obsługi.

3. Koncepcja X.500 Directory w sieci NASK

3.1 Struktura danych w X.500 Directory

Zgodnie z założeniami X.500 Directory struktura danych jest zgodna z administracyjno-organizacyjnym podziałem. Dokładniej mówiąc dane należą z reguły do jednej z kategorii: *kraj* (country), *instytucja* (organization), *jednostka organizacyjna* lub *oddział* (organizationalUnit), *osoba* (person). Istnieje również kategoria obiektu locality, jest ona jednak stosowana rzadko i tylko w przypadkach nie dających się wpasować do wspomnianych powyżej schematów, np. organizacje z natury międzynarodowe znajdują się bezpośrednio pod locality=Europe.

Nie ma ograniczeń co do ilości szczebli instytucji czy jednostek organizacyjnych; przesadne rozbudowanie drzewa doprowadza jednak do zaciemnienia obrazu i nie jest zalecane.

Dane przechowywane są w serwerach (DSA) i struktura danych musi być odzwierciedlona w strukturze serwerów. Optymalnym rozwiązaniem jest, gdy poszczególne instytucje posiadają własne serwery. Na obecnym stopniu rozwoju techniki sieci komputerowych unikać należy zbytniego rozczłonkowania sieci serwerów w ramach pojedynczych instytucji, tak aby nie doprowadzać do sytuacji, w której w celu odszukania pojedynczego hasła (osoby) na terenie danej instytucji konieczna jest konsultacja ze znaczną liczbą serwerów niższego szczebla i w efekcie uruchamianie dużej ilości połączeń, startowanie ze stanu uśpienia kilku serwerów, co w rezultacie znacznie spowalnia dostęp do danych. Z drugiej jednak strony bardzo duże zbiory danych stanowią znaczne obciążenie dla poszczególnych komputerów, a budowa sieci w oparciu o niewielką tylko liczba serwerów zwiększa szanse chwilowej niedostępności dużych zbiorów danych.

3.3 Organizacja i utrzymanie zasobów

Przewidujemy, że faza pilotowa rozwijać się będzie pod patronatem NASK w ośrodkach akademickich kraju. Ze względu na ograniczenia organizacyjno-sprzętowe oraz stosunkowo niewielką ilość danych (w początkowej fazie projektu) można uznać za wystarczające, jeżeli uruchamiane serwery będą odgrywały rolę serwerów regionalnych, obsługując kilka uczelni zlokalizowanych w pobliżu. Do lokalnych administratorów należeć będzie decyzja, czy odpowiedzialność za dane poszczególnych instytucji przekażą reprezentantom tych instytucji.

Finansowanie projektu w 1994 r. opierać się będzie o grant KBN przeznaczony na ładowanie pilotowych baz danych, fundusze JBR NASK oraz wsparcie partycypujących uczelni w postaci udostępnienia sprzętu.

Wyniki prac będą udostępnione zainteresowanym użytkownikom poprzez sieć naukowo-akademicką NASK.

Jednym z podstawowych zadań, jakie stoją przed polskim projektem X.500 jest dostosowanie go do naszych lokalnych potrzeb (polskie znaki). Szczęśliwie w X.500 znaki spoza standardowego zestawu ASCII reprezentowane są w standardzie T.61, który zawiera wszystkie polskie znaki diakrytyczne. Oprogramowanie ISODE dopuszcza jednak po stronie DUA jedynie znaki z tabeli ISO-Latin 1 i niezbędne jest zmodyfikowanie DUA, tak aby wyświetlane były również znaki Latin 2. Opracowania wymagają również standardy wprowadzania polskich danych, tak aby mogły one być wykorzystywane zarówno na obszarze Polski (w poprawnej pisowni) jak i z zagranicy (z wykorzystaniem niemodyfikowanych DUA). Wstępne prace we wspomnianym zakresie są już obecnie prowadzone.

Bardzo ważnym zagadnieniem jest rozwijanie samej bazy danych. Przewidywana jest w tym zakresie między innymi współpraca z Ośrodkiem Przetwarzania Informacji (OPI). Konieczne będzie zaimplementowanie mechanizmów, które pozwalałyby powiązać X.500 z istniejącymi kadrowymi bazami danych, przynajmniej w stopniu umożliwiającym weryfikację prawidłowości zasobów X.500.

4. Dokumentacja

Dokumentacja ISODE składa się z pięciu tomów i jest zorganizowana zgodnie z warstwowym modelem odniesienia OSI. Charakteryzuje od podstaw usługi oferowane przez poszczególne warstwy. Dwa pierwsze tomy dokumentacji opisują narzędzia programowe, implementujące podstawową obsługę kolejnych warstw sieciowych, tom trzeci opisuje aplikacje utworzone na bazie tych usług. Czwarty tom przedstawia narzędzia służące do budowania aplikacji na bazie języka programowania, abstrahującego od modelu sieciowego. Tom piąty to kompletny opis implementacji X.500 Directory.

Dokumentacja ISODE, liczne RFC związane z tematyką X.500, jak również całość oprogramowania (w postaci źródłowej) jest dostępna na serwerze NASK **ocelot.mat.uni.torun.pl.**

UMK uruchomił w imieniu NASK "helpdesk" na tematy związane z instalacją i eksploatacją oprogramowania X.500. Pomoc dostępna jest za pomocą poczty elektronicznej pod adresem **help-X.500@cc.uni.torun.pl.**

4.1 Standardy OSI

1. CCITT X.500 / ISO DIS 9594-1: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Overview of Conspects, Models and Services.
2. CCITT X.501 / ISO DIS 9594-2: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Models.
3. CCITT X.509 / ISO DIS 9594-8: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Authentication Framework.
4. CCITT X.511 / ISO DIS 9594-3: [ISO: InformationProcessing Systems] Open Systems Interconnection - The Directory - Abstract Service Definition.
5. CCITT X.518 / ISO DIS9594-4: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Procedures for Distributed Operations.
6. CCITT X.519 / ISO DIS 9594-5: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Protocol Specifications.
7. CCITT X.520 / ISO DIS 9594-6: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Selected Attribute Types.
8. CCITT X.521 / ISO DIS 9594-7: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Selected Object Classes.
9. CCITT X.200 / ISO DIS 7498: [ISO:Information Processing Systems] Open Systems Interconnection - Basic Reference Model.
10. CCITT X.208 / ISO DIS 8824: [ISO:Information Processing Systems] Open Systems Interconnection - Specifications of Abstract Syntax Notation One (ASN.1).
11. CCITT X.219 / ISO DIS 9072-1: [ISO: Information Processing Systems - Text Communication] Remote Operations [ISO: PART 1]: -Model, Notation and Service Definition.
12. CCITT X.229 / ISO DIS 9072-2: [ISO: Information Processing Systems - TextCommunication] Remote Operations [ISO: PART 2]: - Protocol Specification.

4.2 Literatura uzupełniająca

[1.] Kille S.E.: *An Introduction to the ISODE Consortium*, University College London, March 12, 1992.
[2.] Kille S.E.: *The ISODE Consortium, University* College London, May 10, 1992.
[3.] Kirstein P.T.: *CCITT Recommendations of the X.500 Series, The Directory*, University College London, April 1992.
[4.] PARADISE, *International Report*, No.2, November 1991.
[5.] PARADISE, *International Report*, No.3, May 1991.
[6.] Robbins C.J., Kille S.E.: *The ISO Development Environment: Users Manual, Volume 5: QUIPU*, version 7, X-Tel Services Ltd., University College London, July 1, 1992.
[7.] Robbins C.J., Onions J.P.: *The ISO Development Environment: Users Manual*, Update Release, version 8, X-Tel Services Ltd., University College London, June 17, 1992.
[8.] Schnabel F.: *X.500 Directory and Information Services*, University of Technology, Graz, July 15, 1991.
[9.] M. Rose: *RFC 1085 ISO Presentation Services ontop of TCP/IP based internets*, December 1988.
[10.] M. Rose The Little Black Book, Prentice Hall, 1992
[11.] Górecka M.,Wolniewicz T., Żenkiewicz J.: *Projekt wstępny rozwoju X.500 w Polsce*, Toruń, listopad 1992.
[12.] M. Kus: *X.500 Directory - opis użytkowy programu DE.*

Toruń, kwiecień 1994

Serwisy informacyjne dostępne w sieci Internet

Ireneusz Neska

W sieci Internet oprócz standardowych programów do komunikacji w sieci istnieje szereg innych programów i aplikacji umożliwiających dostęp użytkownikowi do serwisów informacyjnych lub zbiorów danych. W niniejszym artykule chciałbym przedstawić kilka z nich o nazwach Gopher, World-Wide Web, Wais, Whois i Archie.

Gopher

Gopher jest to rozproszony system informacyjny umożliwiający dostęp do różnego rodzaju dokumentów. Pozwala on na przeszukiwanie i zbieranie informacji znajdujących się w różnych miejscach w bardzo prosty dla użytkownika sposób. W trakcie pracy dane pojawiają się jako szereg kolejnych menu. Taka struktura podobna jest do organizacji katalogów z wieloma podkatalogami i zbiorami. Te podkatalogi i zbiory mogą znajdować się na lokalnym komputerze lub dowolnym innym serwerze dostępnym przez sieć. Z punktu widzenia użytkownika wszystkie pozycje prezentowane w menu wyglądają jakby były dostępne w tym samym miejscu. Operując trybem kolejnych menu Gopher pozwala użytkownikowi "wędrować" po różnych włączonych do tego systemu komputerach w poszukiwaniu określonej informacji. Dane dostępne w strukturze Gopher mogą być zbiorami tekstowymi lub binarnymi, jak również mogą zawierać katalogi informacyjne lub bazy przeszukiwań. Dodatkowo Gopher może oferować dostęp do innych systemów informacyjnych (np. WWW, WAIS, archie, whois, News, X.500) oraz usług sieciowych (Telnet, FTP).

Z serwerem Gopher można uzyskać połączenie pisząc polecenie:
telnet nazwa.węzła

Na terenie Polski w ten sposób można połączyć sie z co najmniej dwoma komputerami:
gopher.torun.edu.pl
hum.amu.edu.pl
Jako login name należy podać: gopher. Hasło nie jest wymagane.

Większość serwerów nie akceptuje takiego trybu połączenia. Aby uzyskać z nimi połączenie należy użyć polecenia w postaci:
gopher nazwa.węzła
Pisząc samą komendę gopher uzyskuje się połączenie z domyślnym serwerem ustalonym podczas instalacji programu, natomiast nazwa.węzła jest opcjonalną nazwą serwera Gopher, z którym chcemy pracować. Po połączeniu jest możliwy dostęp do innych serwerów Gopher w kraju i na świecie oraz do innych usług oferowanych przez dany serwer.

Po nawiązaniu połączenia przykładowe menu może wyglądać następująco:

```
                    Internet Gopher Information Client v1.1

                  Root gopher server: galaxy.uci.agh.edu.pl

 -->  1.  Przeczytaj to                - Read me first/
      2.  Lokalny system informacyjny  - Local Infosystem/
      3.  Inne swistaki                - Other gophers/
      4.  Inne systemy informacyjne    - Other infosystems/
      5.  Roznosci                     - Miscellany/
      6.  Katalog plikow publicznych   - Public access files/
      7.  Dyski CD-ROM (SIMTEL, itp)   - Walnut Creek CD-ROMs/

Press ? for Help, q to Quit, u to go up a menu                    Page: 1/1
```

Aby wybrać dowolną pozycję w spisie należy podac jej numer lub przesunąć kursor (-->) na tą pozycję i naciśnąć klawisz <Enter>. Każda pozycja wyświetlana jest z identyfikującym ją symbolem. I tak pozycjami w menu mogą być:

/ – podkatalog
. – zbiór tekstowy
<Bin> – zbiór binarny
<Sound> – zbiór dźwiękowy
<Picture> – obraz
<?> – indeks przeszukiwań
<Talent> – sesja Telnetu

Operacje możliwe do wykonania na danym polu zależą od jego typu. I tak:

podkatalog wyświetlana jest jego zawartość. Aby przejść na wyższy poziom należy użyć komendy **"up"**.

zbiór tekstowy na ekranie wyświetlana jest treść zbioru. Można go przejrzeć, poszukać określonego ciągu znaków, wydrukować na drukarce, skopiować na lokalny dysk lub przesłać pocztą elektroniczną.

zbiór binarny zbiór może być skopiowany na dysk lokalnego komputera.

zbiór dźwiękowy zbiór może być odtworzony przez urządzenie audio lokalnego komputera (jeśli jest do tego przystosowane) lub skopiowany na lokalny dysk.

obraz może być wyświetlony na ekranie lokalnego komputera lub skopiwany na lokalny dysk komputera.

indeks należy podać ciąg znaków, który może być jednym lub wieloma słowami, plus specjalne operatory and, or lub not. Jako wynik uzyskuje się listę zbiorów zawierających podany ciąg znaków, które następnie można przejrzeć jak każdy inny zbiór.

sesja Telnetu uzyskuje sie połączenie z podanym komputerem, na którym oferowane są inne usługi (z reguły bazy danych lub katalogi biblioteczne).

W każdym momencie możliwe jest zakończenie pracy (komenda **quit**) oraz dostępny jest tekst pomocy (komenda **help**).

Poniżej przedstawiona jest lista niektórych serwerów gopher w Polsce:

galaxy.uci.agh.edu.pl	**Kraków**
gopher.cyf-kr.edu.pl	**Kraków**
gopher.torun.edu.pl	**Torun**
gopher.nask.org.pl	**Warszawa**
gopher.fuw.edu.pl	**Warszawa**
gopher.ia.pw.edu.pl	**Warszawa**
plearn.edu.pl	**Warszawa**
gopher.ae.poz.edu.pl	**Poznań**
hum.amu.edu.pl	**Poznań**
gopher.umcs.lublin.pl	**Lublin**

Z każdego serwera jest możliwe przejście do innych serwerów na terenie Polski i na świecie.

World-Wide Web

World-Wide Web (zwany inaczej WWW lub W3) jest to rozproszona baza informacyjna oparta o "hypertekst", oferująca użytkownikowi możliwość przeszukiwania dokumentów bez wiedzy, gdzie się one znajdują.

Filozofia hypertekstu polega na tym, że różne dokumenty mogą być ze sobą w pewien sposób powiązane. Każdy tekst może zawierać odwołania do innych dokumentów. Hypertekst umożliwia użytkownikowi przejście do nowego dokumentu przez wskazanie interesującego go fragmentu tekstu, a następnie powrót do czytanego dokumentu. Zbiór wszystkich dokumentów tworzy bazę danych WWW.

Dane dostępne w systemie WWW mogą być praktycznie dowolnego rodzaju. Mogą to być zbiory tekstowe lub binarne (np. programy), obrazy, zbiory dźwiękowe i inne. Poza tym WWW może oferować dostęp do innych systemów informacyjnych (gopher, News, X.500, serwery FTP, bazy danych, indeksy przeszukiwań).

W systemie WWW odwołania do innych dokumentów mogą być podawane w różny sposób. W zależności od używanego programu mogą to być liczby pisane w nawiasach kwadratowych lub podświetlenie odpowiedniego fragmentu tekstu. Przejście do nowego dokumentu polega na wpisaniu odpowiedniej liczby lub podświetleniu interesującego nas tekstu i naciśnięciu klawisza **<Enter>.**

Od niedawna dostępna jest również graficzna wersja programu umożliwiającego pracę w sytemie WWW o nazwie Mosaic. Dostępne są wersje tego programu na stacje robocze UNIX z X-Widnows i komputery osobiste PC z MS Windows.

Połączenie z serwerm WWW można uzyskać na dwa sposoby:

a) gdy używamy terminala tekstowego należy wydać polecenie w postaci:

www [typ://nazwa.węzła:[port]/[katalog]/]

Pisząc samą komendę www uzyskujemy połączenie z domyślnym serwerem ustalonym podczas instalacji programu. Opcjonalne parametry są następujące:

typ – rodzaj serwera, z którym chcemy pracować. Mogą być użyte trzy typy:
file - dla serwera FTP,
gopher - dla serwera gopher,
http - dla serwera WWW.

nazwa.węzła – nazwa lub adres komputera, z którym chcemy pracować.

port – opcjonalny numer portu jeśli serwer, z którym się łączymy nie jest standardowo skonfigurowany.

katalog – pełna ścieżka do zbioru, który chcemy obejrzeć. Jeśli katalog nie jest podany otwierany jest zbiór o nazwie **Welcome.html** w głównym katalogu serwera WWW.

Przykłady wywołań programu www:

www
www file://galaxy.uci.agh.edu.pl/
www gopher://gopher.nask.org.pl/
www http://info.fuw.edu.pl/
www http://jaguar.cc.uni.torun.pl:8888/Mc=PL/
Ostatni przykład jest to adres serwera X.500 w Toruniu.

b) Używając terminala graficznego możemy użyć programu Mosaic. W zależności od systemu postać wywołania programu może być różna, ale najczęściej wystarczy wpisać polecenie:

Mosaic

Program łączy się z domyślnym serwerem ustalonym w konfiguracji. Następnie nawigacja w poszczególnych dokumentach i serwerach WWW polega na wskazaniu wyznaczonego fragmentu tekstu lub rysunków (ewentualnie ikon) i naciśnięciu klawisza myszy.

Poniżej przedstawiony jest przykład pracy na terminalu tekstowym z serwerem w CERN-ie w Szwajcarii.

Po połączeniu menu główne serwera wygląda następująco:

```
                                                    Overview of the Web

                                    GENERAL OVERVIEW OF THE WEB

  There is no "top" to the World-Wide Web. You can look at it from
  many points of view. Here are some places to start.

  by Subject[1]        The Virtual Library organises information by subject
                       matter.

  List of servers[2]   All registered HTTP servers by country

  by Service Type[3]   The Web includes data accessible by many other
                       protocols. The lists by access protocol may help if
                       you know what kind of service you are looking for.

  If you find a useful starting point for you personally, you can configure
  your WWW browser to start there by default.

   See also: About the W3 project[4] .
     [End]


1-4, Up, Quit, or Help:
```

W tym momencie możemy wybrać jedną z czterech dostępnych opcji. Aby uzyskać informacje na temat WWW wybieramy numer 4 i otrzymujemy następujący opis:

```
                                                    The World Wide Web project
  (23/36)
                                        WORLD WIDE WEB

  The WorldWideWeb (W3) is a wide-area hypermedia[1] information
  retrieval initiative aiming to give universal access to a large
  universe of documents.

  Everything there is online about W3 is linked directly or indirectly to
  this document, including an executive summary[2] of the project, an
  illustrated talk[3], Policy[4] and Conditions[5], May's W3 news[6],
  Frequently Asked, Questions[7].

  What's out there?[8]  Pointers to the world's online information,
                        subjects[9] , W3 servers[10] , etc.

  WWW Software Products[11]
                        What there is and how to get it: clients[12],
                        servers[13], gateways[14], libwww[15] and tools[16]

  Discussion            Newsgroup comp.infosystems.www[17], other
                        groups[18], specialised mailing lists[19]

Technical[20]   Details of protocols, formats, program internals etc
1-27, Back, Up, <RETURN> for more, Quit, or Help: 1
```

Aby uzyskać więcej informacji na temat hypertekstu ("hypermedia") wybieramy numer 1 i uzyskujemy:

```
                                        What is Hypertext? (23/29)

                        WHAT IS HYPERTEXT

   Hypertext is text which is not constrained to be linear.

   Hypertext is text which contains links[1] to other texts. The term
   was coined by Ted Nelson[2] around 1965 (see History[3] ).

   HyperMedia is a term used for hypertext which is not constrained to
   be text: it can include graphics, video and sound[4] , for example.
   Apparently Ted Nelson was the first to use this term too.

   Hypertext and HyperMedia are concepts, not products.

   See also:

     A list of terms[5] used in hypertext litterature.

     Conferences[6]

     Commercial (and academic) products[7]

     A newsgroup on hypertext, "alt.hypertext"[8] .
1-10, Back, Up, <RETURN> for more, Quit, or Help:
```

W ten sposób można poruszać się po kolejnych dokumentach, uzyskując potrzebną informację. Wciskając klawisz <RETURN> możemy przeglądać kolejne strony danego dokumentu, wydając komendę Up możemy przeglądać jego poprzednie strony, natomiast wydanie polecenia Back powoduje powrót do poprzedniego dokumentu. W każdym momencie możemy zakończyć prace (polecenie Quit) oraz uzyskać tekst pomocy (polecenie Help).

Niektóre z dokumentów WWW mogą być indeksami przeszukiwań, w których możemy szukać interesujących nas słów kluczowych. Dostępne jest wtedy dodatkowo jedno polecenie:

find słowo_kluczowe

Poniżej przedstawiony jest jeden z takich indeksów.

```
                                                        local index

                        LOCAL

   This is a document index whose cover page has not yet been retrieved.
   (Select full cover page[1] for more information about this database.)

   Please specify search words to find documents. The WWW/WAIS Gateway will
   do a full text search and return a list of documents that you can browse.

   For other databases, see thedirectory of servers.[2]

     [End]


FIND <keywords>, 1-2, Back, Up, Quit, or Help: find perl
```

Wydając polecenie:

find perl

uzyskujemy listę dokumentów uszeregowanych według ilości występowania słowa kluczowego perl. Takich dokumentów jest 14:

```
                                                        perl (in local)
                                    PERL

    Index local contains the following 14 items relevant to 'perl'.

    perl.1.html[1]          Score: 1000, lines:5685
    taintperl.1.html[2]     Score: 1000, lines:5685
    a2p.1.html[3]           Score:  173, lines: 207
    pman.1.html[4]          Score:  126, lines: 471
    s2p.1.html[5]           Score:  102, lines:  75
    cfman.81.html[6]        Score:   78, lines: 207
    cmore.1.html[7]         Score:   63, lines: 141
    h2ph.1.html[8]          Score:   63, lines:  75
    etherstat.1.html[9]     Score:   47, lines:  75

FIND <keywords>, 1-14, Back, Up, <RETURN>  for more, or Help:
```

W tym momencie możemy przejrzeć dowolny z podanych dokumentów, ponownie przeszukać bazę danych lub wrócić na wyższy poziom.

WWW jest w tej chwili najbardziej popularnym i dynamicznie rozwijającym się systemem informacyjnym. W ciągu zaledwie kilku miesięcy na świecie powstało kilkaset serwerów WWW i do końca roku z pewnością liczba ta przekroczy tysiąc. Również w Polsce system cieszy się coraz większą popularnością. Obecnie jest już ponad trzydzieści serwerów WWW działających w obrębie sieci NASK. Poniżej przedstawiona jest ich lista:

Warszawa

info.fuw.edu.pl
info.ippt.gov.pl
www.nask.org.pl
www.ia.pw.edu.pl
www.ire.pw.edu.pl
www.elka.pw.edu.pl
www.camk.edu.pl
www.astrouw.edu.pl
www.icm.edu.pl
vulcan.mimuw.edu.pl
hydra.mimuw.edu.pl
andante.iss.uw.edu.pl

Gdańsk

www.pg.gda.pl
www.gumbeers.elka.pg.gda.pl
www.amg.gda.pl

Gliwice

www.polsl.gliwice.pl

Kraków
www.cyf-kr.edu.pl
www.uci.agh.edu.pl
druid.if.uj.edu.pl

Lublin
www.umcs.lublin.pl

Łódź
zsku.p.lodz.pl

Poznań
www.amu.edu.pl

Toruń
www.ncan.torun.pl
www.uni.torun.pl
www.astri.uni.torun.pl
www.mat.uni.torun.pl
www.cc.uni.torun.pl
vm.cc.uni.torun.pl
class1.phys.uni.torun.pl

Wrocław
www.immt.pwr.wroc.pl
www.ict.pwr.wroc.pl
www.ita.pwr.wroc.pl
sun10.ci.pwr.wroc.pl

WAIS

WAIS *(Wide Area Information Server)* jest to rozproszony system pomocny przy przeszukiwaniu baz danych. Bazy danych z reguły zawierają pewną ilość zbiorów danych, natomiast mogą być zorganizowane w bardzo różny sposób. Użytkownik nie potrzebuje jednak uczyć się wielu języków do przeszukiwania różnych typów baz danych. WAIS używa naturalnego języka pytań do poszukiwania odpowiednich dokumentów. Wynikiem każdego zapytania jest zestaw dokumentów zawierających podane słowa, które następnie można przejrzeć.

Procedura przeszukiwania baz danych jest następująca:

1. Wśród dostępnych baz danych wybieramy bazy nas interesujące, które będziemy następnie przeglądać.
2. Formułujemy zapytanie przez podanie słowa, lub słów kluczowych.
3. Po uruchomieniu zapytania, przeszukiwane są wszystkie zaznaczone bazy danych.
4. Jako wynik przeszukiwania wyświetlane są nagłówki wszystkich dokumentów zawierających podane słowa kluczowe. Jest on uszeregowany według ilości występowania tych słów w tekście.
5. Aby przejrzeć interesujący nas dokument wystarczy po prostu go zaznaczyć (**klawisz <return>**).
6. Jeśli rezultat nie jest satysfakcjonujący przeszukiwanie można powtórzyć z innym słowem kluczowym, wrócić na poprzedni poziom systemu lub przejrzeć inny dokument.
7. Jeśli uruchomimy ponownie przeszukiwanie wynik zostanie rozszerzony o dokumenty "podobne" do zaznaczonych, to znaczy dołączone zostaną dokumenty zawierające największą liczbę wspólnych słów.

W celu połączenia z serwerem WAIS należy wydać polecenie:
telnet nazwa.węzła
gdzie nazwa.wezła jest nazwą serwera oferującego usługę WAIS. Obecnie co najmniej dwie bazy treningowe są ogólnie dostępne:

quake.think.com **(login: wais)**
sunsite.unc.edu **(login: swais)**

Poniżej przedstawiony jest przykład pracy z bazą WAIS. Po zalogowaniu się na serwerze sunsite.unc.edu uzyskujemy listę dostępnych baz danych:

```
SWAIS                          Source Selection                  Sources:612
  #             Server                              Source             Cost
001:   [           archie.au]  aarnet-resource-guide                    Free
002:   [ndadsb.gsfc.nasa.gov]  AAS_jobs                                 Free
003:   [ndadsb.gsfc.nasa.gov]  AAS_meeting                              Free
004:   [weeds.mgh.harvard.ed]  AAtDB                                    Free
005:   [     munin.ub2.lu.se]  academic_email_conf                       Free
006:   [wraith.cs.uow.edu.au]  acronyms                                 Free
007:   [    archive.orst.edu]  aeronautics                              Free
008:   [ bloat.media.mit.edu]  Aesop-Fables                            Free
009:   [ bloat.media.mit.edu]  aesop                                    Free
010:   [ ftp.cs.colorado.edu]  aftp-cs-colorado-edu                     Free
011:   [nostromo.oes.orst.ed]  agricultural-market-news                Free
012:   [     sunsite.unc.edu]  alt-sys-sun                              Free
013:   [    archive.orst.edu]  alt.drugs                                Free
014:   [    wais.oit.unc.edu]  alt.gopher                               Free
015:   [sun-wais.oit.unc.edu]  alt.sys.sun                             Free
016:   [    wais.oit.unc.edu]  alt.wais                                 Free
017:   [alfred.ccs.carleton.]  amiga-slip                              Free
018:   [     munin.ub2.lu.se]  amiga_fish_contents                      Free

  Keywords:

<space> selects, w for keywords, arrows move, <RETURN>  searches, q quits, or ?
```

Klawiszem spacji możemy zaznaczyć interesujące nas bazy danych, które następnie będziemy przeszukiwać. Po wciśnięciu klawisza "w" możemy wpisać interesujące nas słowa kluczowe. Naciśnięcie klawisza <return> powoduje rozpoczęcie przeszukiwania. Poniżej przedstawiony jest wynik przeszukiwania dwóch baz danych:

internet-standards i stds, przy czym słowem kluczowym był wyraz "internet".

```
SWAIS                          Search Results                 Items: 40
  #    Score     Source                      Title                Lines
001:   [1000] (           stds)  /ftp/std/std1                     1907
002:   [1000] (           stds)  /ftp/std/std3                    12624
003:   [1000] (           stds)  /ftp/std/std4                     3134
004:   [1000] (           stds)  /ftp/std/std5                     7227
005:   [1000] (internet-standa)  std01-rfc1540                     1907
006:   [1000] (internet-standa)  std03-rfc1122                     6844
007:   [1000] (internet-standa)  std03-rfc1123                     5782
008:   [1000] (internet-standa)  std04-rfc1009                     3134
009:   [1000] (internet-standa)  std05-rfc0791                     2887
010:   [ 780] (           stds)  /ftp/std/std2                     7787
011:   [ 733] (internet-standa)  std02-rfc1060                     4819
012:   [ 583] (           stds)  /ftp/std/std7                     5247
013:   [ 583] (internet-standa)  std07-rfc0793                     5247
014:   [ 567] (           stds)  /ftp/std/std16                    2303
015:   [ 535] (           stds)  /ftp/std/std11                    3350
016:   [ 504] (internet-standa)  std05-rfc0950                     1026
017:   [ 496] (           stds)  /ftp/std/std13                    6156
018:   [ 480] (internet-standa)  std11-rfc0822                     2901

<space> selects, arrows move, w for keywords, s for sources, ? for help
```

W tym momencie można przejrzeć dowolny z powyższych dokumentów, np. pierwszy z nich /ftp/std/std1 wygląda następująco:

```
SWAIS                          Document Display                    Page:  1


Network Working Group                          Internet Architecture Board
Request for Comments: 1540                                   J. Postel, Editor
Obsoletes: RFCs 1500, 1410, 1360,                                 October 1993
1280, 1250, 1100, 1083, 1130, 1140, 1200
STD: 1
Category: Standards Track


                    INTERNET OFFICIAL PROTOCOL STANDARDS

Status of this Memo

   This memo describes the state of standardization of protocols used
   in  the Internet as determined by the Internet Architecture Board
   (IAB).

Press any key to continue, 'q' to quit.
```

Jeśli podamy więcej niż jedno słowo kluczowe, wyświetlone zostaną wszystkie dokumenty zawierające dowolne z tych słów.

W każdym momencie możliwe jest zakończenie pracy z systemem (klawisz **'q'**) oraz dostępny jest tekst pomocy (klawisz **'?'**).

Chociaż system WAIS powstał dużo wcześniej od WWW jednak w tej chwili stał się usługą marginalną, która prawdopodobnie wkrótce zaniknie.

Whois

Whois jest to usługa dostarczająca jakby elektroniczną książkę adresową dla użytkowników sieci. Umożliwia ona odszukiwanie adresów e-mail'owych, pocztowych i numerów telefonicznych osób związanych z sieciami komputerowymi. Może również dostarczać informacji na temat organizacji sieciowych, samych sieci, numerów internetowych, nazw domenowych i hostów.

Główna baza danych nazw związanych z sieciami komputerowymi (organizacji, instytucji, sieci, osób itp.) utrzymywana jest przez InterNIC *(Internet Registration Service)* w USA. W wielu częściach świata rozmieszczone są serwery, gromadzące dane z poszczególnych regionów. W Europie taka baza danych utrzymywana jest przez organizację RIPE w Holandii i zawiera informacje na temat wszystkich sieci i organizacji działających na terenie Europy. Wiele uczelni utrzymuje również swoje własne bazy danych, oferujące informacje na tematy lokalne.

Bazy danych whois zawierają rekordy różnych typów. Podstawowymi typami rekordów są: osoba, numer Internetowy, nazwa domeny, nazwa hosta, nazwa sieci lub organizacji sieciowej itp. Każdy rekord w bazie danych posiada swój własny, unikalny identyfikator *(handle)*, nazwę, typ oraz wiele innych pól zależnych od typu danego rekordu. Możliwe do uzyskania informacje są następujące:

- dla osoby: nazwa i adres instytucji, w której pracuje, numer telefonu i faxu oraz adres e-mail'owy,
- dla numeru sieci: nazwa instytucji, do której należy dana sieć, nazwy sieci, do których jest ona dołączona oraz nazwiska osób administrujących tą siecią,
- dla domeny: nazwa i opis instytucji, do której należy domena, nazwiska osób administrujących, adresy serwerów obsługujących tę domenę oraz opcjonalnie lista poddomen.

Wszystkie serwery Whois gromadzą dane w zasadzie tylko na temat organizacji, do której należą. Przy znajdowaniu informacji nie korzystają one z innych serwerów, nie wiedzą również, gdzie można znaleźć informacje o innych instytucjach i organizacjach.

Przeszukiwanie baz Whois można przeprowadzić na dwa sposoby:
- wykorzystując program whois, którego format wywołania jest następujący:

whois <-h nazwa.serwera> wzorzec

gdzie:

nazwa.serwera – nazwa lub adres hosta, na którym znajduje się serwer whois (np. whois.ripe.net lub whois.internic .net).
wzorzec – imię lub nazwisko osoby, nazwa hosta, nazwa domeny lub sieci, numer Internetowy lub identyfikator.

- przeszukując interakcyjnie bazę danych. Aby to wykonać należy połączyć się z serwerem poleceniem telnet, np.:

telnet whois.internic.net

Nie jest wymagane podawanie login name, ani hasła. Następnie należy wybrać usługę WHOIS. W tym momencie możemy rozpocząć przeszukiwanie. Format polecenia jest następujący:

<opcja> wzorzec

Polecenie to przeszukuje bazę w poszukiwaniu wzorca, opcja natomiast ogranicza przeszukiwanie tylko do wymienionego typu rekordów. Opcje mogą być następujące:

```
PErson          ogranicza przeszukiwanie do osób (np. PE NESKA).
DOmain          ogranicza przeszukiwanie do nazw domenowych (np. DO PL).
HOst            ogranicza przeszukiwanie do hostów (np. HO PRINCETON).
NEtwork         ogranicza przeszukiwanie do sieci (np. NE EBONE).
Organisation    ogranicza przeszukiwanie do organizacji (np. O CERN).
```

Poza tym dostępne są we wzorcu pewne znaki specjalne:

. przed wzorcem powoduje przeszukiwanie tylko osób.
! przed wzorcem powoduje przeszukiwanie tylko identyfikatorów.
... za wzorcem powoduje wyświetlenie wszystkich rekordów, których nazwy zaczynają się od wzorca.
@ we wzorcu powoduje przeszukiwanie adresów e-mail'owych.

Poniżej przedstawione jest kilka przykładów wykorzystania usługi whois. Pierwsze trzy zapytania skierowane są do serwera europejskiego whois.ripe.net. Ostatnie skierowane jest do serwera whois obsługiwanego przez InterNIC.

a) zapytanie o numer sieci

whois -h whois.ripe.net 148.81.0.0

```
inetnum:    148.81.0.0
netname:    WAWPOLIP
descr:      Warsaw academic subnets
descr:      first IP in Warsaw
country:    PL
admin-c:    Ireneusz Neska
tech-c:     Ireneusz Neska
connect:    RIPE NORDU NSF
bdrygw-1:   ACONET
changed:    Rafal_Pietrak@camk.edu.pl 931002
```

```
source:     RIPE
```

b) zapytanie o osobę

whois -h whois.ripe.net neska

```
person:     Ireneusz Neska
address:    Research and Academic Networks in Poland
address:    Bartycka 18
address:    00-716 Warsaw
address:    Poland
phone:      +48 22 268000
phone:      +48 22 417295
fax-no:     +48 22 268000
e-mail:     irek@nask.org.pl
changed:    irek@nask.org.pl 940204
source:     RIPE
```

c) zapytanie o domenę

whois -h whois.ripe.net pl

```
domain:     pl
descr:      Top level domain for Poland
descr:      NASK, Research and Academic Networks in Poland
descr:      Bartycka 18, PL-00-716 Warszawa
admin-c:    Ireneusz Neska
tech-c:     Ireneusz Neska
tech-c:     Janusz Motoszko
zone-c:     Ireneusz Neska
zone-c:     Janusz Motoszko
nserver:    bilbo.nask.org.pl
nserver:    cocos.fuw.edu.pl
nserver:    sunic.sunet.se
sub-dom:    bialystok bielsko bydgoszcz com edu
sub-dom:    gda gliwice gov katowice kielce krakow
sub-dom:    lodz lublin nowy-sacz olsztyn org poznan
sub-dom:    szczecin torun waw wroc
changed:    irek@nask.org.pl 940109
source:     RIPE
```

d) zapytanie główną domenę dla Polski

whois -h whois.internic.net pl-dom

```
Poland (Republic of) top-level domain (PL-DOM)
   Research and Academic Computer Network
   Krakowskie Przedmiescie 26/28
   00-927 Warsaw
   POLAND

   Domain Name: PL

   Administrative Contact, Technical Contact, Zone Contact:
      Neska, Ireneusz  (IN3)  hostmaster@NASK.ORG.PL
      +48 22 268000 +48 22 200381 ext. 843 (FAX) +48 22 268000
```

```
Record last updated on 10-Nov-93.

Domain servers in listed order:

BILBO.NASK.ORG.PL              148.81.16.51
COCOS.FUW.EDU.PL               148.81.4.6
SUNIC.SUNET.SE                 192.36.125.2, 192.36.148.18
```

Archie

W sieci Internet znajduje się szereg ogólnie dostępnych serwerów FTP, na których można znaleźć ogromną liczbę programów i zbiorów danych. Wyszukanie tego, co jest nam potrzebne i co nas rzeczywiście interesuje może więc niejednokrotnie sprawiać ogromną trudność. Pomocą w tej kwestii służy sieciowy system informacyjny Archie. Umożliwia on przeszukiwanie specjalnych baz danych (zwanych bazami archie) w poszukiwaniu interesujących nas zbiorów. Bazy danych archie zawierają informacje o ponad 2.500.000 nazwach programów zgromadzonych na ponad 2000 publicznych (anonymous) FTP serwerach. Stosując ten system użytkownik może zatem bardzo szybko zlokalizować zbiór znając jedynie jego nazwę (lub nawet jej część) bez potrzeby przeszukiwania katalogów wielu maszyn.

Serwery archie oferują dodatkowo dostęp do bazy danych opisu pakietów oprogramowania (Software Description Data Base), która zawiera nazwy oraz krótkie opisy wielu pakietów oprogramowania, dokumentów i zbiorów danych przechowywanych w archiwach FTP.

Aby uzyskać dostęp do bazy danych archie należy wydać polecenie o postaci:

telnet nazwa.węzła

gdzie nazwa.węzła jest adresem komputera oferującego usługę archie. Po zgłoszeniu się zdalnego systemu jako login name należy podać archie. Hasło nie jest wymagane. Poniżej podane zostały adresy ważniejszych serwerów archie na świecie:

```
archie.au*                  139.130.4.6      Australia
archie.edvz.uni-linz.ac.at* 140.78.3.8       Austria
archie.univie.ac.at*        131.130.1.23     Austria
archie.uqam.ca*             132.208.250.10   Kanada
archie.funet.fi             128.214.6.100    Finlandia
archie.th-darmstadt.de*     130.83.22.60     Niemcy
archie.ac.il*               132.65.6.15      Izrael
archie.unipi.it*            131.114.21.10    Włochy
archie.wide.ad.jp           133.4.3.6        Japonia
archie.kr*                  128.134.1.1      Korea
archie.sogang.ac.kr*        163.239.1.11     Korea
archie.rediris.es*          130.206.1.2      Hiszpania
archie.luth.se*             130.240.18.4     Szwecja
archie.switch.ch*           130.59.1.40      Szwajcaria
archie.ncu.edu.tw*          140.115.19.24    Taiwan
archie.doc.ic.ac.uk*        146.169.11.3     Wielka Brytania
archie.unl.edu              129.93.1.14      USA (NE)
archie.internic.net*        198.48.45.10     USA (NJ)
archie.rutgers.edu*         128.6.18.15      USA (NJ)
archie.ans.net              147.225.1.10     USA (NY)
archie.sura.net*            128.167.254.179  USA (MD)
```

Serwery oznaczone gwiazdką pracują z nową wersją oprogramowania archie 3.0.

Podstawowe polecenia dostępne na serwerach archie są następujące:

Uwaga:

Polecenia oznaczone (+) są akceptowane tylko przez wersję 3.0 oprogramowania, natomiast oznaczone (*) akceptowane są tylko przez starsze wersje.

exit, quit, bye
zakończenie pracy z serwerem.

help <polecenie>
bez parametru przechodzi do interakcyjnego trybu pomocy. Z parametrem wyświetla informacje o podanym poleceniu. Naciśnięcie klawisza <return> powoduje wyjście z trybu interakcyjnego.

list <wzorzec>
wyświetla listę FTP serwerów, znajdujących się w bazie archie. Opcjonalny parametr ogranicza tą liczbę tylko do nazw pokrywających się z wzorcem.

mail <adres>, <adres2 ...>
przesyła wynik ostatniego polecenia pod podane adresy pocztowe. Gdy użyte jest bez parametrów, rezultat wysyłany jest pod adres podany w zmiennej mailto.

prog tekst | wzorzec
find (+) tekst | wzorzec
przeszukuje bazę danych w poszukiwaniu podanego tekstu lub wzorca. Jako wynik otrzymujemy listę adresów FTP serwerów wraz z nazwą zbioru, jego wielkością, datą ostatniej modyfikacji oraz katalogiem, w którym można go znaleźć.

set zmienna wartość
ustawia wartość podanej zmiennej.

show <zmienna>
wyświetla wartość podanej zmiennej (lub wszystkich zmiennych).

site(*) nazwa-hosta
wyświetla rekursywnie wszystkie katalogi, podkatalogi i zbiory znajdujące się na podanym FTP serwerze. Format wyjściowy podobny jest do UNIX'owej komendy ls -lR.

whatis tekst
przeszukuje oddzielną bazę danych opisu pakietów oprogramowania (Software Description Data Base) w poszukiwaniu podanego tekstu. Baza ta zawiera nazwy oraz krótkie opisy wielu pakietów oprogramowania, dokumentów i zbiorów danych przechowywanych w Internecie.

Znaki specjalne stosowane do opisu wzorca:

. dowolny znak, np "...." oznaczają cztery dowolne znaki. Aby w tekście wprowadzić znak "." należy go poprzedzić znakiem "\".

^ jeśli pojawia się na początku wzorca, to poszukiwany tekst musi zaczynać się od tekstu podanego za "^". Jeśli pojawia sie w dowolnym innym miejscu, traktowany jest jako zwykły znak.

$ jeśli pojawia się na końcu wzorca, to poszukiwany tekst musi kończyć się tekstem podanym przed "$". Jeśli pojawia się w dowolnym innym miejscu, traktowany jest jako zwykły znak.

Przykładowa sesja przeszukiwania serwera archie może wyglądać następująco:

```
archie.aco.net> prog internet
# Search type: regex.
# Your queue position: 1
# Estimated time for completion: 00:03
working... -

Host ftp.uni-frankfurt.de     (141.2.1.7)
Last updated 04:03 29 Jan 1994
```

```
    Location: /pub/SunOS/Netzwerkeln/pc
      FILE    -rwxr-xr-x   17017 bytes  22:00 17 Jul 1991  internet.arc

Host ftp.idiap.ch    (192.33.221.1)
Last updated 23:32  6 Feb 1994

    Location: /pub/Lib
      FILE    -rw-rw-r--    5166 bytes  00:00 15 Jun 1993  internet.data-
bases

Host ftp.imag.fr    (129.88.32.1)
Last updated 00:14  4 Feb 1994

    Location: /archive_sites/bibliotheques
      FILE    -rw-r--r--    5166 bytes  22:00 11 Oct 1992  internet.data-
bases

Host ftp.uni-frankfurt.de    (141.2.1.7)
Last updated 04:03 29 Jan 1994

    Location: /pub/networking
      FILE    -rw-r--r--    5166 bytes  22:00 30 Jul 1992  internet.data-
bases

Host cnri.reston.va.us    (132.151.1.1)
Last updated 07:26  7 Feb 1994

    Location: /
      DIRECTORY    drwxrwxr-x   23040 bytes  22:44  4 Feb 1994  internet-
drafts

itd...

archie.aco.net> whatis kermit
c-kermit.ann    C-Kermit & USENET
ckermit         The 'C' implementation of Kermit
cu-shar         Allows kermit, cu, and UUCP to all share the same lines
dialout         Kill getty and kermit programs
kermit          Communications software package
kermit.hdb      Kermit patches to enable dial to use HDB database
okstate         UUCP Access to Kermit Distribution
unboo.bas       Decode Kermit boo format

archie.aco.net> list \.edu$
# Your queue position: 1
# Estimated time for completion: 00:01
working... -

                129.16.79.20     06:54 28 Jan 1994
acfcluster.nyu.edu            128.122.128.93     16:08 19 Jan 1994
aix.rpi.edu                    128.113.26.11     06:14  6 Feb 1994
ajpo.sei.cmu.edu               128.237.2.253     03:33  6 Feb 1994
allspice.berkeley.edu          128.32.150.27     03:27  6 Feb 1994
almach.chpc.utexas.edu          129.116.3.15     17:14 19 Jan 1994

itd...
```

```
archie.aco.net> exit
# Bye.
Connection closed by foreign host.
36 sam:/mnt/workers/irek/sam>
```

Warszawa, lipiec 1994

WARMAN, miejska sieć komputerowa w Warszawie*)

Maciej Kozłowski, Tadeusz Rogowski

1. Koncepcja sieci WARMAN.

WARMAN (WAR jak Warszawa, MAN od ang. *Metropolitan Area Network*) jest przedsięwzięciem polegającym na budowie szybkiej infrastruktury telekomunikacyjnej na terenie Warszawy, przeznaczonej w pierwszej kolejności do transmisji danych dla potrzeb środowiska naukowego i akademickiego.

Środowisko naukowe Warszawy tworzą w pierwszej kolejności wielkie uczelnie: Uniwersytet Warszawski, Politechnika Warszawska, Akademia Medyczna, Szkoła Główna Gospodarstwa Wiejskiego, Szkoła Główna Handlowa. Ponadto w Warszawie lokuje się powyżej 200 innych instytucji akademickich, naukowych i badawczo-rozwojowych:

- 12 innych państwowych szkół wyższych,
- 10 uczelni niepaństwowych,
- 47 placówek Polskiej Akademii Nauk,
- 140 jednostek badawczo-rozwojowych, podległych różnym resortom.

Lista, uwzględniająca oddziały rozlokowane poza jednostkami macierzystymi, obejmuje około 500 pozycji, w ok. 200 lokalizacjach rozproszonych na terenie miasta.

Główne skupiska jednostek akademickich i naukowych to:

- Rejon Krakowskiego Przemieścia (UW, ASP, PWSM, AM, PAN, inne),
- Rejon Politechniki (PW, UW, AM, PAN, inne),
- Zgrupowanie naukowe "Ochota" (UW, AM, PAN, inne),
- Rejon ulic Rakowieckiej, Narbutta, Chocimskiej (SGGW, SGH, PW, inne),

Można wyróżnić kilka skupisk o charakterze mniej zwartym:

- Służewiec/Ursynów (SGGW, PAN, UW, inne),
- Żoliborz (AWF, ATK, IMGW, PAN, inne),
- Rejon ul. Kasprzaka,
- Rejon ul. Jagiellońskiej,
- Rejon ul. Grochowskiej,
- Międzylesie/Anin/Wawer
- Świerk za Otwockiem.

Dołączenie wszystkich (lub większości) jednostek naukowych i akademickich Warszawy do sieci nie jest możliwe bez zbudowania następującej minimalnej infrastruktury:

- punkty koncentracji, ulokowane w różnych rejonach miasta,
- wydajne połączenia pomiędzy punktami koncentracji, z zapewnieniem redundancji.

Ze względu na rozmieszczenie oraz potrzeby poszczególnych jednostek naukowych i akademickich przyjęto następujące założenia koncepcyjne:

- powstanie 10 węzłów, ulokowanych w rejonach koncentracji jednostek lub w miejscach istotnych z punktu widzenia istniejącej infrastruktury telekomunikacyjnej;
- zostaną uruchomione szybkie łącza międzywęzłowe, docelowo na dedykowanych liniach światłowodowych; przejściowo dopuszcza się kanały cyfrowe dzierżawione od innych operatorów;
- nastąpi bezpośrednie połączenie każdego z węzłów z co najmniej dwoma innymi węzłami - docelowo w oparciu o osobne kable światłowodowe; przejściowo dopuszcza się różne włókna w ramach tego samego kabla;
- węzeł jest obiektem rozproszonym; wyróżnia się dwa typy węzłów: focus i campus;
- węzeł typu *focus* jest wyposażony w koncentratory, na ogół oddalone od urządzenia przełączającego. Koncentratory umożliwiają dołączanie poszczególnych użytkowników, z zapewnieniem pożądanych przez nich protokołów komunikacyjnych.
- w węźle typu *campus* przeważa zwarta struktura przestrzenna o rozmiarach rzędu 2x2 km, zawierająca kilkanaście różnych podmiotów dołączanych do sieci; w otoczeniu tych węzłów powstaną sieci kampusowe.

---

* jest to zaktualizowana wersja artykułu zaprezentowanego na konferencji POLMAN '94 (Poznań, 16-17 maja 1994 r.)

Rysunek 1. Rozmieszczenie jednostek naukowych i akademickich w centralnej części Warszawy. Na mapie zaznaczono orientacyjnie lokalizację węzłów (trójkąty) i koncentratorów (kwadraty) sieci WARMAN.

WARMAN, miejska sieć komputerowa w Warszawie*)

Maciej Kozłowski, Tadeusz Rogowski

1. Koncepcja sieci WARMAN.

WARMAN (WAR jak Warszawa, MAN od ang. *Metropolitan Area Network*) jest przedsięwzięciem polegającym na budowie szybkiej infrastruktury telekomunikacyjnej na terenie Warszawy, przeznaczonej w pierwszej kolejności do transmisji danych dla potrzeb środowiska naukowego i akademickiego.

Środowisko naukowe Warszawy tworzą w pierwszej kolejności wielkie uczelnie: Uniwersytet Warszawski, Politechnika Warszawska, Akademia Medyczna, Szkoła Główna Gospodarstwa Wiejskiego, Szkoła Główna Handlowa. Ponadto w Warszawie lokuje się powyżej 200 innych instytucji akademickich, naukowych i badawczo-rozwojowych:

- 12 innych państwowych szkół wyższych,
- 10 uczelni niepaństwowych,
- 47 placówek Polskiej Akademii Nauk,
- 140 jednostek badawczo-rozwojowych, podległych różnym resortom.

Lista, uwzględniająca oddziały rozlokowane poza jednostkami macierzystymi, obejmuje około 500 pozycji, w ok. 200 lokalizacjach rozproszonych na terenie miasta.

Główne skupiska jednostek akademickich i naukowych to:

- Rejon Krakowskiego Przemieścia (UW, ASP, PWSM, AM, PAN, inne),
- Rejon Politechniki (PW, UW, AM, PAN, inne),
- Zgrupowanie naukowe "Ochota" (UW, AM, PAN, inne),
- Rejon ulic Rakowieckiej, Narbutta, Chocimskiej (SGGW, SGH, PW, inne),

Można wyróżnić kilka skupisk o charakterze mniej zwartym:

- Służewiec/Ursynów (SGGW, PAN, UW, inne),
- Żoliborz (AWF, ATK, IMGW, PAN, inne),
- Rejon ul. Kasprzaka,
- Rejon ul. Jagiellońskiej,
- Rejon ul. Grochowskiej,
- Międzylesie/Anin/Wawer
- Świerk za Otwockiem.

Dołączenie wszystkich (lub większości) jednostek naukowych i akademickich Warszawy do sieci nie jest możliwe bez zbudowania następującej minimalnej infrastruktury:

- punkty koncentracji, ulokowane w różnych rejonach miasta,
- wydajne połączenia pomiędzy punktami koncentracji, z zapewnieniem redundancji.

Ze względu na rozmieszczenie oraz potrzeby poszczególnych jednostek naukowych i akademickich przyjęto następujące założenia koncepcyjne:

- powstanie 10 węzłów, ulokowanych w rejonach koncentracji jednostek lub w miejscach istotnych z punktu widzenia istniejącej infrastruktury telekomunikacyjnej;
- zostaną uruchomione szybkie łącza międzywęzłowe, docelowo na dedykowanych liniach światłowodowych; przejściowo dopuszcza się kanały cyfrowe dzierżawione od innych operatorów;
- nastąpi bezpośrednie połączenie każdego z węzłów z co najmniej dwoma innymi węzłami - docelowo w oparciu o osobne kable światłowodowe; przejściowo dopuszcza się różne włókna w ramach tego samego kabla;
- węzeł jest obiektem rozproszonym; wyróżnia się dwa typy węzłów: focus i campus;
- węzeł typu *focus* jest wyposażony w koncentratory, na ogół oddalone od urządzenia przełączającego. Koncentratory umożliwiają dołączanie poszczególnych użytkowników, z zapewnieniem pożądanych przez nich protokołów komunikacyjnych.
- w węźle typu *campus* przeważa zwarta struktura przestrzenna o rozmiarach rzędu 2x2 km, zawierająca kilkanaście różnych podmiotów dołączanych do sieci; w otoczeniu tych węzłów powstaną sieci kampusowe.

---

* jest to zaktualizowana wersja artykułu zaprezentowanego na konferencji POLMAN '94 (Poznań, 16-17 maja 1994 r.)

- *Study of Metropolitan Area Networks (Technology, trends, vendors and products)*, wykonana przez firmę GANDALF; autorzy: Jan Bartl, Stan Michalak
- Ekspertyza sieci MAN w Warszawie, wykonana przez zespół prof. Janusza Filipiaka w Katedrze Telekomunikacji AGH.

Obie ekspertyzy uznały, że technologią, która posłuży jako podstawa dla szerokopasmowych sieci z integracją usług B-ISDN *(Broadband Integrated Services Data Network)* będzie ATM *(Asynchronous Transfer Mode)*. Z uwagi na stosunkowo wczesny etap wprowadzania tej technologii na rynek i braki w standaryzacji rozważono następujące alternatywy:

- **Ethernet** ewoluujący do szybkiego ethernetu. Propozycja ta dotyczyła raczej rozwiązań lokalnych, niż szkieletu sieci, z uwagi na ograniczony zasięg ethernetu.
- **Frame Relay**. Zalety: (1) topologia typowo sieciowa, (2) łatwa migracja w kierunku sieci B-ISDN/ATM, (3) niezawodność, (4)dobra ochrona danych. Wada: technologia przystosowana do prędkości transmisji 2 Mbps, a więc przydatna tylko jako rozwiązanie przejściowe.
- **FDDI**. Podkreślono bogatą ofertę rynkową w tej kategorii. Topologicznie - szkielet sieci WARMAN musiałby składać się z kilku pierścieni FDDI. Minusy FDDI to: (1) jest to technologia rozgłoszeniowa, a więc generująca stosunkowo duży przepływ danych i źle chroniąca dane przed niepowołanym dostępem, (2) brak skalowalności, (3) brak transmisji izochronicznych, (4) brak prostej drogi migracyjnej do docelowej sieci B-ISDN.
- **FDDI-II.** Zaleta: możliwość transmisji izochronicznej. Wada: brak oferty rynkowej (w chwili sporządzania ekspertyzy).
- **IEEE** 802.6 DQDB *(Dual Que Distributed Bus)* z usługą w warstwie sieciowej SMDS/CBDS. Zalety: (1) zróżnicowane mediatransmisyjne; prędkość transmisji skalowana od 1.5 Mbps do 155 Mbps, (2) niezawodność i elastyczność konfiguracji wyższa niż FDDI, (3) lepsza ochrona danych niż w sieci FDDI, (4) kilka realizacji w sieciach miejskich w Europie. Wada: koszt urządzeń wyższy niż w przypadku sieci FDDI.
- **ATM** *(Asynchronous Transfer Mode)* z protokołem SDH *(Synchronous Digital Hierarchy)* w warstwie fizycznej, jeśli dostawca zapewni uzupełnienia technologii w miarę postępu w jej standaryzacji.

Ponieważ ekspertyzy nie wytypowały jednoznacznie technologii, która winna być użyta w szkielecie sieci WARMAN, realizatorzy przedsięwzięcia postanowili znaleźć odpowiedź na to pytanie w ofercie rynkowej. Posłużono się formułą dwuetapowego konkursu/przetargu.

W lipcu 1993 r. do kilkudziesięciu firm (w większości zrzeszonych w *ATM Forum*) został wystosowany *"Request for Information -WARMAN"*, traktowany jako I etap postępowania konkursowego. W odpowiedzi otrzymano oferty oraz materiały informacyjne od 19 firm lub grup firm - bez wyjątku zagranicznych lub zagranicznych z partnerami krajowymi, w tym wielkich firm telekomunikacyjnych.

Analiza nadesłanych materiałów pozwoliła na następujące wnioski:

- technologia ATM jest dostępna rynkowo; są już sieci zrealizowane w tej technologii;
- ceny urządzeń stają się konkurencyjne w stosunku do FDDI,
- zasadne jest szukanie dostawcy technologii i urządzeń wśród uczestników I etapu,

"The Second Request for Information - WARMAN; Call for Limited Tender" został wysłany do 9 uczestników I etapu konkursu. W wyniku analizy ofert i przeprowadzonych rozmów ostatecznie zdecydowano się na zastosowanie technologii ATM w szkielecie sieci WARMAN.

Przetarg został zakończony 1 lipca 1994 r. wyborem firmy Schrack Ericsson jako dostawcy technologii i urządzeń ATM dla sieci WARMAN. Podstawowymi urządzeniami będą switche i koncentratory APEX firmy General DataComm. Międzywęzłowe łącza światłowodowe zostaną wyposażone w protokół SDH/STM-1 155 Mbps. Instalacja urządzeń zostanie wykonana wspólnie przez Schrack Ericsson i NASK.

Umowa z firmą Schrack Ericsson zawiera klauzulę o kilkuletniej współpracy pomiędzy Schrack Ericsson i NASK. Jest to istotne wobec ciągłego rozwoju technologii ATM. Schrack Ericsson zobowiązał się do wyposażenia sieci w nowości, w miarę postępu standaryzacji ATM. Obaj partnerzy utworzą laboratorium umożliwiające testowanie elementów sieci przed ich wprowadzeniem do eksploatacji. Zasadniczą dostawę sprzętu

- sieć musi zapewniać wieloprotokołowość;
- rozwiązaniem docelowym jest B-ISDN - Broadband Integrated Services Data Network; aktualnie B-ISDN opiera się o technologię ATM); możliwe jest stosowanie rozwiązań przejściowych, ale powinny one zapewniać drogę migracyjną do rozwiązania docelowego;
- część abonentów powinna zostać dołączona do sieci za pomocą łączy optycznych; nie jest możliwe ani celowe dołączenie wszystkich użytkowników w ten sposób.
- ważnym elementem jest zapewnienie możliwości przyłączania użytkowników w oparciu o linie galwaniczne - na ogół dzierżawione od TP SA. Dlatego szczególnie istotna jest współpraca z TP SA, a w szczególności możliwość umieszczania koncentratorów sieci w centralach telefonicznych;
- w celu zapewnienia profesjonalnej niezawodności sieci urządzenia przełączające - stanowiące jądro systemu - powinny być umieszczone w obiektach o szczególnej ochronie, z zapewnieniem zasilania awaryjnego;
- granicę sieci od strony użytkownika wyznaczają koncentratory przyłączeń. Łącza do użytkownika oraz sieci lokalne nie są finansowane w ramach WARMANu;
- w sieci zostaną zainstalowane komputery dużej mocy obliczeniowej. Przewiduje się możliwość połączenia ich za pomocą wydzielonych nitek światłowodowych, w celu integracji ich zasobów;
- ważnym elementem sieci są serwery zasobów/usług. Przewiduje się zakup serwera czołowego dla działającego już komputera CRAY, podobnego serwera dla superkomputera o architekturze równoległej, planowanego do zainstalowania na Politechnice Warszawskiej oraz serwera NFS przewidzianego do zainstalowania na UW.
- inwestycja została zaplanowana na 3 lata, z zakończeniem w 1996 r.

Przyjęto następującą lokalizację węzłów sieci:

- Krakowskie Przedmieście *(campus)*,
- Politechnika *(campus)*,
- Ochota - Banacha *(campus)*,
- Plac na Rozdrożu,
- Plac Trzech Krzyży,
- Mokotów - Rakowiecka,
- Południe - Służewiec/Ursynów,
- Wola - w rejonie ul. Kasprzaka,
- Żoliborz - w rejonie ul. Podleśnej
- Praga - ul. Jagiellońska.

Z uwagi na rozmiar i zasięg terytorialny przedsięwzięcia nietrudno dojść do wniosku, że powinno być ono realizowane we współpracy z innymi operatorami telekomunikacyjnymi działającymi na terenie Warszawy.

2. Porozumienie środowiskowe.

"Porozumienie placówek naukowo-badawczych i uczelni warszawskich w sprawie uczestnictwa w budowie i przyszłego korzystania z Miejskiej Sieci Komputerowej w Warszawie oraz Komputerów Dużej Mocy" z 9 kwietnia 1993 r. zostało podpisane przez Prezesa PAN w imieniu warszawskich placówek PAN, Rektorów Politechniki Warszawskiej, Uniwersytetu Warszawskiego, Akademii Medycznej, Szkoły Głównej Gospodarstwa Wiejskiego, Szkoły Głównej Handlowej i przez Prezesa Państwowej Agencji Atomistyki w imieniu warszawskich placówek Agencji. "Porozumienie" powołało 8-osobowy Zespół Koordynacyjny - Radę Użytkowników, w składzie praktycznie tożsamym z zespołem do spraw miejskiej sieci komputerowej, wyłonionym na zebraniu przedstawicieli wszystkich wyższych uczelni warszawskich i wybranych placówek PAN 11 stycznia 1993 r. "Porozumienie" określiło Uniwersytet Warszawski jako placówkę wiodącą dla realizacji inwestycji.

Przygotowania do inwestycji - w ramach jednostki wiodącej - były prowadzone przez Zespół Koordynacyjny NASK.

29 marca 1994 r. został podpisany aneks do "Porozumienia" z 9 kwietnia 1993 r., który: (1) zmienił jednostkę wiodącą na utworzoną w grudniu 1993 NASK j.b.r., (2) powołał nową 10-osobową Radę Użytkowników, (3) określił odpowiedzialność Rady Użytkowników przed Radą Założycielską, złożoną z kierowników placówek, które podpisały "Porozumienie".

Jakkolwiek nie wszystkie warszawskie placówki naukowe i akademickie są sygnatariuszami "Porozumienia", to sieć WARMAN będzie służyć całemu środowisku.

"Porozumienie" dotyczy również inwestycji superkomputerowych i wykorzystywania komputerów dużej mocy.

3. Przygotowania wstępne; konkurs na dostawę technologii i urządzeń dla sieci WARMAN.

W okresie grudzień 1992 - maj 1993 r. zostały wykonane na zamówienie Zespołu Koordynacyjnego NASK ekspertyzy odnośnie wyboru technologii komunikacyjnej w szkielecie sieci WARMAN:

5. Standardy w zakresie ATM.

Standaryzacją urządzeń i protokołów dla ATM zajmują się dwie grupy. Pierwsza z nich to ATM Forum skupiające ponad 500 instytucji, w tym producentów sprzętu i oprogramowania, producentów elementów i podzespołów elektronicznych, agencje rządowe, instytucje telekomunikacyjne PTT, instytuty badawcze, użytkowników.

Druga organizacja to **ITU** (daawniej CCITT) - międzynarodowa organizacja standardów telekomunikacyjnych. Praktyka ostatnich lat pokazuje, że ATM Forum dość sprawnie uzgadnia kolejne standardy. Z pewnym opóźnieniem uzgadniane są standardy ITU.

Główne problemy ze standaryzacją powstają w trzech punktach:
- fizyczny styk interfejsów,
- komunikacja pomiędzy aplikacjami via ATM,
- sygnalizacja oraz SVC *(Switched Virtual Channel)*.

Należy także pamiętać o systemie zarządzania siecią i rozliczeniami międzyoperatorskimi.

Fizyczny styk - interfejsy.

ATM Forum uzgodniło m.in. następujące standardy:
- SDH STM1 - public & private UNI *(User-Network Interface)*: 155.52 Mbps, single mode & multi mode fiber,
- TAXI 100 Mbps multimode - private UNI: nawiązanie do FDDI,
- 155 Mbps multimode - private UNI: 2 km, 155.52 Mbps, 1330 nm.
- DS3 - public & private UNI: 44.736 Mbps (dla USA).

Tylko pierwszy standard został również przyjęty przez ITU. Dąży się do wspólnych standardów dla publicznych i prywatnych interfejsów UNI *(User-Network Interface)* i NNI *(Network-Network Interface)*.

Komunikacja pomiędzy aplikacjami.

Odwołamy się tu do warstwowego modelu ATM zilustrowanego w tabeli 1.

Wyższe warstwy ISO/OSI			
AAL 1 VOICE	AAL 2 HDTV	AAL 3 / AAL 4 Frame Relay, SMDS	AAL 5 Data
Warstwa adaptacyjna			
ATM			
Warstwa fizyczna			
SONET/SDH	DS3	Multimode	.....

Tabela 1. Schemat warstwowy technologii ATM i jej usług

Istotnym elementem w komunikacji pomiędzy aplikacjami jest zgodność standardów warstwy adaptacyjnej *(Adaptation Layer)*. Zdefiniowanych jest pięć warstw adaptacyjnych AAL1, ..., AAL5, z czego warstwa AAL3 i 4 występują łącznie.

Warstwa AAL1 jest zorientowana połączeniowo *(connection oriented)* dla transmisji o stałej szybkości *(fixed bit rate)*. Przeznaczona jest do przesyłania głosu.

Warstwa AAL2 jest również zorientowana połączeniowo, ale dla transmisji o zmiennej szybkości *(variable bit rate)*. Przeznaczona jest do transmisji aplikacji typu HDTV *(High Definition Television)*. W obu przypadkach wymagana jest transmisja izochroniczna.

Warstwy AAL3/4 są to bezpołączeniowe protokoły dla transmisji o zmiennej szybkości, bez wymogu izochronizmu. Warstwa AAL5 przeznaczona jest do transmisji LAN-LAN.

Według aktualnych informacji, na ukończeniu są prace nad standardem warstwy AAL3/4, natomiast nie ma standardu dla warstwy AAL2 (dla SAR - *segmenting/reasembly*). Pozostałe warstwy są objęte standardami ATM Forum oraz ITU.

Komunikacja pomiędzy operatorami

W tym punkcie problem dotyczy w zasadzie sieci publicznych; trudności mogą wynikać z konkurencyjnych interesów potentatów telekomunikacyjnych. Standard na styku pomiędzy operatorami jest nieustalony. Natomiast prace nad standardem ITU trwają, i planuje się uzgodnienie standardu do końca 1995 roku.

Jak zapewniają producenci, aktualnie proponowane rozwiązania są na tyle elastyczne, że nie powinno być problemu z dostosowaniem aktualnie stosowanej sygnalizacji do przyszłego standardu.

7. Charakterystyka urządzeń ATM w sieci WARMAN.

Podstawową strukturę węzłów tworzyć będą urządzenia *(switches)* GDC Apex-DV2. Urządzenia te charakteryzuje:

- szybkość przełączania matrycy 6.4 Gbps lub 3.2 Gbps (w sieci WARMAN, w głównych węzłach będą zastosowane switche o szybkości 6.4 Gbps),
- konstrukcja modułowa o 19 slotach, z czego 16 może być wykorzystanych na karty interfejsów, pozostałe sloty są przeznaczone na moduły przełączające *(switching fabric: main, standby)*,
- realizacja funkcji PVC i SVC (standard Q.2931, ATM Forum),
- w warstwie AAL5 można realizować przełączanie protokołu Frame Relay,
- redundantna architektura *(redundant fault tolerant architecture)* oraz możliwość wymiany kart podczas pracy,
- możliwe jest zestawienie na każdym z portów 7168 kanałów VC/PC.

Dostępne są następujące interfejsy fizyczne:

- E1 - styk cyfrowy G.703 o szybkości 2,048 Mbps, dwa porty na karcie,
- E2 - styk cyfrowy G.703 o szybkości 8.448 Mbps, dwa porty na karcie,
- E3 - styk cyfrowy G.703 o szybkości 34,368 Mbps, dwa porty na karcie,
- HSSI do 52 Mbps, dwa porty na karcie,
- RS449/V.11 do 10 Mbps, dwa porty na karcie,
- X.21 do 10 Mbps, dwa porty na karcie,
- TAXI 100 Mbps, światłowód wielomodowy, kodowanie 4B/5B, dwa porty na karcie,
- SDH/STM1 155.52 Mbps, światłowód jednomodowy, jeden lub dwa porty na karcie,
- Ethernet 802.3 AUI, 4 porty na karcie.

W zestawieniu pominięto standardy nieeuropejskie (DS1, DS3, SONET).

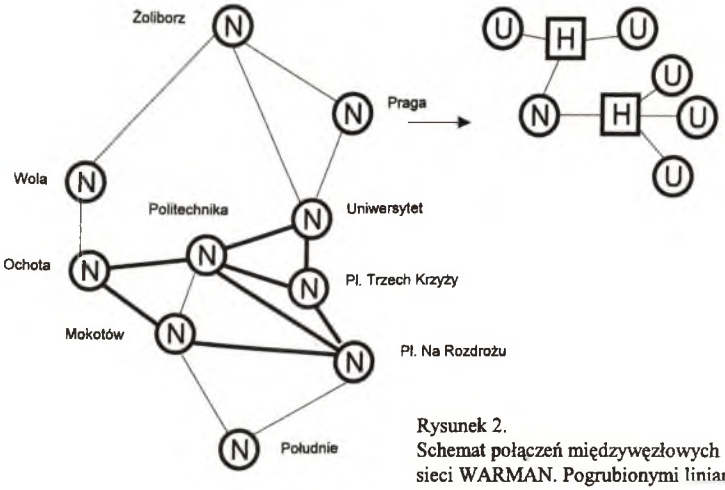
Przedstawione wyżej styki wskazują jedynie fizyczne możliwości połączenia ze sobą poszczególnych urządzeń. Z punktu widzenia infrastruktury sieciowej istotne są protokoły jakie są realizowane na tych stykach. W strukturze sieci ATM naturalne jest przesyłanie celek ATM łącznie z adresowaniem E.164. Taką sytuację, w pewnym uproszczeniu, można sobie wyobrazić, jeśli komunikują się między sobą dwie stacje robocze wyposażone w interfejsy ATM i których aplikacje bezpośrednio komunikują się z warstwą ATM. Wszystkie powyższe styki (bez Ethernetu) pozwalają na taką transmisję.

Jak już wspomniano, sieć ATM musi być również przezroczysta dla innych protokołów. Umożliwiają to tzw. warstwy adaptacyjne. Urządzenia APEX DV2 pozwalają na podłączenie np:

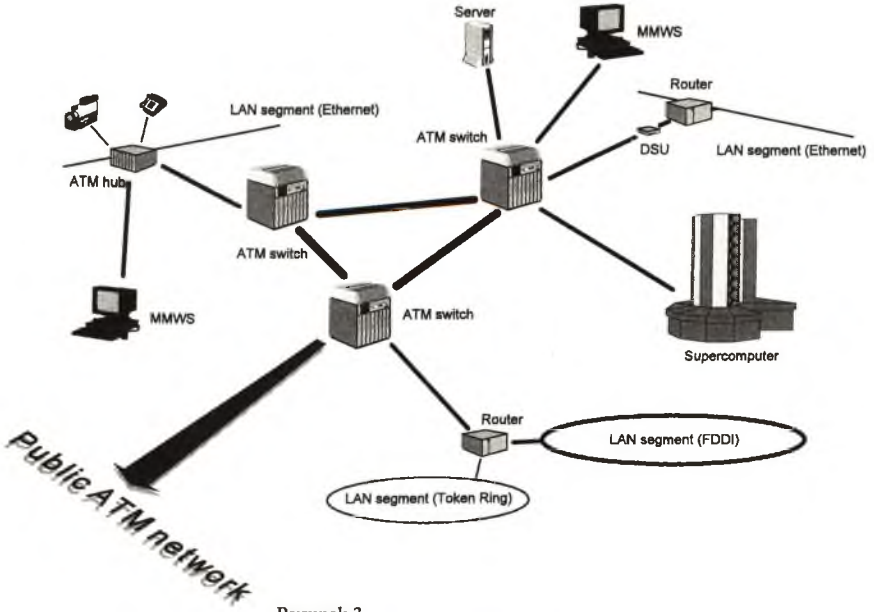
- routera z protokołem Frame Relay,
- urządzenia typu FEP *(front end processor)* z protokołem HDLC lub SNA/SDLC,
- urządzenia typu *video/voice* wymagające *Virtual Circuit Emulation - VCE*,
- segmentu Ethernet; realizowana jest virtualna sieć na ATM (styk 802.3 AUI).

Jak wynika z przedstawionej powyżej krótkiej charakterystyki, urządzenia APEX DV2 mogą pełnić funkcję switcha lub koncentratora, w zależności od konfiguracji i sposobu włączenia do infrastruktury sieciowej *(backbone)*. W przypadku sieci WARMAN APEX DV2 będzie pełnił funkcję klasycznego switcha - wyposażony będzie w karty typu SDH/STM1.

Jako koncentratory (huby) będą zastosowane inne produkty firmy GDC - APEX MAC *(Media Access Concentrator)* i APEX MAC1. Jest to urządzenie mniejsze, ma 8 slotów (APEX MAC), z czego 7 może być wykorzystanych do włączenia kart interfejsów. Szybkość przełączania matrycy jest 1.4 Gbps. APEX MAC1 ma 5 slotów, w tym 4 do wykorzystania. Oba typy urządzeń mają możliwość zastosowania wszystkich wyżej wymienionych interfejsów fizycznych i logicznych. Z racji swojej architektury są to typowe urządzenia dostępowe.



Rysunek 2.
Schemat połączeń międzywęzłowych sieci WARMAN. Pogrubionymi liniami zaznaczono już istniejące linie światłowodowe.
Węzeł (N) jest strukturą rozproszoną, dołączone są do niego koncentratory (H) łączy do użytkowników (U).



Rysunek 3.
Przykład sposobu włączenia urządzeń użytkowników i sieci lokalnych do Miejskiej Sieci Komputerowej WARMAN.
W przyszłości sieć WARMAN zostanie dołączona do sieci publicznych, opartych o technologię ATM.

W maksymalnie rozbudowej konfiguracji - w zależności od potrzeb - punkt koncentracji może się składać z:
- koncentratora ATM APEX-MAC lub ATM DV2, który umożliwia abonentowi "uzyskanie" protokołu ATM w swojej sieci; wymagany jest w zasadzie światłowód lub kanał cyfrowy,
- serwera komunikacyjnego, który umożliwia podłączenie abonenta za pomocą łącza stałego, asynchronicznego o szybkości 9.6-57.6 Kbps z protokołem SLIP *(Serial Line IP Protocol)*,
- routera, który w zależności od wyposażenia udostępni abonentowi zestaw protokołów za pośrednictwem łącza stałego i transmisji szeregowej o szybkości do 2 Mbps.

8. Kolejność realizacji inwestycji

Koniec 1994 r.
- Węzeł "Krakowskie Przedmieście", obsługujący jednostki Śródmieścia na północ od Al. Jerozolimskich i Stare Miasto,
- Węzeł "Politechnika", obsługujący jednostki południowo-zachodniego Śródmieścia, w tym Wydział Fizyki UW przy ul. Hożej oraz rejon Akademii Medycznej.
- Węzeł "Ochota", obsługujący w pierwszej kolejności jednostki zgrupowania naukowego w rejonie ul. Banacha.
- Węzeł "Mokotów", obsługujący w pierwszej kolejności zgrupowanie naukowe w rejonie ulic Rakowieckiej i Narbutta.
- Węzeł "Plac na Rozdrożu".
- Węzeł "Plac Trzech Krzyży".

1995 r.
- Węzły: "Południe", "Wola", "Żoliborz", "Praga"

1996 r.
- doposażenie sieci, pełne wdrożenie scenariuszy i regulaminów działania sieci, przekazanie sieci docelowemu operatorowi.

W trakcie budowy WARMAN będzie korzystać z zezwolenia telekomunikacyjnego udzielonego dla NASK.

9. Sieć infrastrukturalna i sieci wirtualne.

Operator infrastruktury sieci WARMAN będzie miał za zadanie wyłącznie obsługę transmisji na poziomie podstawowym.

Zadaniem operatorów sieci wirtualnych będzie bezpośrednia obsługa użytkowników końcowych i realizacja ich potrzeb - zupełnie różnych dla różnych środowisk.

10. Komputery dużej mocy w sieci WARMAN.

Wspólny wniosek inwestycyjny zakładał zainstalowanie w Warszawie dwóch komputerów dużej mocy, o różnych architekturach: (1) projekt Uniwersytetu Warszawskiego, dotyczący systemu wektorowo-równoległego, (2) projekt Politechniki Warszawskiej, odnośnie skalowalnego systemu równoległego MIMD *(Multiple Instruction Multiple Data)*.

W lutym 1994 r. nastąpiła instalacja komputera CRAY EL98 w Interdyscyplinarnym Centrum Algorytmów Modelowania Uniwersytetu Warszawskiego. Konfiguracja:
- system o architekturze wektorowo-równoległej
- 8 procesorów (po 133 Mflops)
- 1GB pamięci operacyjnej
- ponad 30 GB dysków

Oprogramowanie (wybór): System operacyjny Unicos 7.0.6, Kompilatory (C, C++, Fortran) Emulator T3D, System PVM, AVS, dGauss,Unichem, Biosym, NASTRAN.

Bibliografia

[1.] M. Kozłowski, T. Rogowski; *WARMAN, miejska sieć komputerowa w Warszawie*; Konferencja POLMAN, Poznań, 16-17 maja 1994 r.

[2.] Jan Bartl, Stan Michalak; *Study of Metropolitan Area Networks (Technology, trends, vendors and products)*; ekspertyza wykonana przez firmę GANDALF, luty 1993.
[3.] Janusz Filipiak, Andrzej Pach, Artur Lasoń, Dariusz Wittek; *Ekspertyza sieci MAN w Warszawie*; ekspertyza wykonana przez zespół Katedry Telekomunikacji AGH w Krakowie; maj 1993.
[4.] *Założenia Techniczno-Ekonomiczne sieci WARMAN. Etap I - Rozpoznanie Potrzeb*; lipiec 1993.
[5.] WARMAN; *Założenia Inwestycyjne Sieci Teleinformatycznej dla M. St. Warszawy*; listopad 1993.
[6.] Martin de Prycker; *ATM Technologies, Applications and Services Tutorial on ATM*; The First European Interoperability Conference and Exhibition; Paris 1993.
[7.] Rainer Handel, Manfred N. Huber; *Integrated Broadband Networks*; *An Introduction to ATM-Based Networks*. Adison Wesley Publishing Company, 1991-1992-1993.
[8.] M. Gromisz, M. Jankowski, R. Adamiec, M. Kozłowski, J. Motoszko, R. Pietrak, J. Sobczyk; *Studium Projektowe Warszawskiej Akademickiej Sieci Komputerowej*; czerwiec 1992.
[9.] Materiały firmowe: Alcatel, AT&T, Cisco, Digital Equipment, Fore Systems, General DataComm, Schrack Ericsson, Stratacom, Synoptics.

Bezpieczeństwo w sieciach komputerowych

Krzysztof Silicki

Bezpieczeństwo czyli po angielsku *security* w odniesieniu do otwartych systemów sieciowych *(ang. Open Systems)* już przez samo zestawienie pojęć ujawnia skalę problemu. Znany jest żart, że najlepszym sposobem zapewnienia bezpieczeństwa systemowi jest jego całkowite odłączenie. W praktyce całkowite odseparowanie systemu od świata zewnętrznego może okazać się trudne (pomijając już fakt, że nie przynosi korzyści wynikających z komunikacji sieciowej). Istnieją jednak metody zabezpieczania sieci pozwalające łączyć otwartość z bezpieczeństwem.

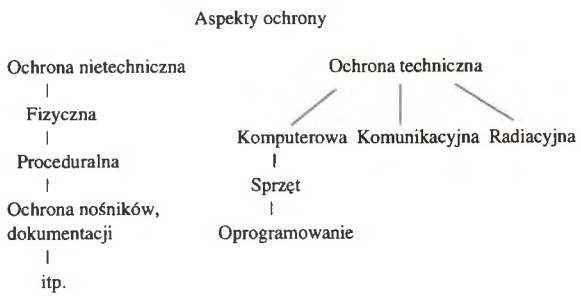
Świadomość

Bardzo cenna jest po pierwsze świadomość potrzeby ochrony własnych zasobów. Brak takiej świadomości może drogo kosztować. Im szerzej pojęte jest bezpieczeństwo jako problem tym oczywiście lepiej. Badania prowadzone w krajach rozwiniętych dowodzą na przykład, że największym niebezpieczeństwem dla systemu firmy mogą stanowić ludzie w niej pracujący. Aby pogłębić ten paradoks dodajmy, że największe możliwości pod względem narażenia sieci lokalnej na różnorakie niebezpieczeństwa ma oczywiście manager systemu i inni uprzywilejowani użytkownicy, którzy przez zwykłą nieuwagę mogą odkryć karty, które powinny były pozostać zakryte. W skrócie rzecz ujmując można powiedzieć, że warto sobie uświadomić jak ważne są poszczególne zasoby dla nas, jaką mogą przedstawiać wartość dla potencjalnego "włamywacza", co będzie jeśli zostaną przez nas utracone na skutek zdarzeń losowych lub przechwycone przez niepowołane osoby a następnie wdrożyć odpowiednie procedury i mechanizmy zabezpieczające.

Polityka ochrony

Polityka bezpieczeństwa to dokument zaakceptowany przez daną instytucję gdzie opisany jest docelowy model wdrażanego systemu bezpieczeństwa traktowanego w sposób całościowy. Powinien on dotyczyć wielu aspektów bezpieczeństwa. Elektroniczna ochrona informacji jest tu tylko jednym z wielu aspektów. Być może zajmowanie się aspektem nietechnicznym ochrony wyda się komuś nadwrażliwością jednak tak na prawdę skoncentrowanie się na jednym aspekcie security prowadzi do sytuacji kiedy w jednym miejscu są skoncentrowane zbyt duże środki a inny słaby punkt jest bezpośrednio narażony na atak. Potraktujmy więc sprawę kompleksowo.

Przyjrzyjmy się kilku aspektom ochrony przedstawionym na poniższym diagramie:



Ochrona nietechniczna:

– ochrona fizyczna - stosowana jest aby zapobiec nieautoryzowanemu fizycznemu dostępowi do obszarów, gdzie wykonywana jest praca o określonym ciężarze gatunkowym i składowane są efekty tej pra-

cy; polityka ochrony fizycznej powinna też precyzować jak minimalizować ryzyko zagrożeń naturalnych takich jak powódź czy pożar,
- polityka proceduralna i kadrowa - powinna kierować się zasadą: nie więcej przywilejów niż jest to wymagane, powinna określać procedury postępowania w różnych sytuacjach, obiegu dokumentów i informacji w firmie, kłaść odpowiedni nacisk na szkolenie personelu pod kątem odpowiedzialności za zasoby, do których ma on dostęp, chronić pomieszczenia z nośnikami informacji itp.

Jako dygresję a'propos szerokiego pojęcia ochrony można potraktować fakt, że codzienna świadomość personelu firm zachodnich o tym jakie informacje nie są przeznaczone do rozgłaszania na zewnątrz firmy wydaje się być czymś powszechnym natomiast w polskich przedsiębiorstwach będących często w ścisłym związku z zagranicznymi korporacjami sprawa ta z reguły bywa traktowana w sposób dowolny.

Ochrona techniczna

Sprowadza się ona w gruncie rzeczy do elektronicznej ochrony informacji. Cała gra polega na rozpoznaniu sposobów i technik zarówno po stronie zagrożeń jak i środków zaradczych. Poniżej dokonano przeglądu zagadnień z tej dziedziny.
- radiacja - istnieją sposoby przechwytywania informacji wypromieniowywanej przez okablowanie transmisyjne lub ekrany monitorów ; jest to atak pasywny, trudny do wykrycia.
- podsłuch - oprócz przechwycenia informacji emitowanej przez okablowanie podsłuch może być zrealizowany na szereg sposobów łącznie z wpięciem się z analizatorem w linię transmisji danych.
- ochrona komunikacyjna
  - sieci w istotny sposób czułe na niepowołany dostęp nie powinny mieć dostępu typu dial-up (możliwość dodzwonienia się za pomocą modemu do komputera w jakiejś sieci jest ulubionym celem hackerów) lub powinno się stosować mechanizmy zabezpieczające typu call-back (komputer sprawdza czy numer telefoniczny, który żąda połączenia jest mu znany)
  - duże sieci (niesegmentowane) stanowią potencjalne ryzyko wymykania się spod kontroli administratora
  - sieci prywatne dołącza się do sieci o charakterze publicznym za pomocą elementów o szczególnie bezpiecznej konfiguracji (tzw . firewalls)
  - stosuje się szyfratory oraz urządzenia potwierdzające autentyczność (wymieniają one odpowiednie kody zanim połączenie zostanie nawiązane)
  - nowymi tendencjami ochrony w aspekcie komunikacyjnym jest przenoszenie szyfrowania i mechanizmów potwierdzania autentyczności do wyższych warstw modelu OSI aż do warstwy aplikacji włącznie (np. szyfrowanie listów przez użytkowników systemów poczty elektronicznej)
- ochrona komputerów i oprogramowania
  - sprzęt powinien zapewniać ochronę systemu operacyjnego przed "zagłuszeniem" funkcji systemowych przez aplikację uruchomioną na tym sprzęcie
  - oprogramowanie powinno mieć zaimplementowane funkcje security, testowania, obronę przed forsowaniem (tzw. bypass)

Pod względem funkcjonalnym stosuje się na przykład: tzw. logi czyli pamiętniki odwołań do funkcji i usług oferowanych przez system komputerowy, audit czyli proces na bieżąco informujący o tym co dzieje się w systemie (np. nieudane próby logowania się na komputerze), etykiety security, szyfrowanie, elektroniczne podpisy itp. Natomiast to jak dobrze owe mechanizmy zostały zaimplementowane wyznacza stopień pewności *(assurance)* tych systemów. Stopień pewności może być określany zarówno w stosunku do systemów operacyjnych jak i aplikacji. Wartość assurance jakiegoś systemu jest łatwiej oszacować jeśli metodologia projektowania tego systemu odpowiadała zaleceniom organizacji standaryzujących. Oszacowanie prawidłowości mechanizmów security z reguły następuje w wyniku przeprowadzenia testów. W Europie kryteria oceny "wartości" systemu pod względem security zostały określone przez ITSEC a w USA zawarte zostały w Orange Book Departamentu Obrony (DoD). Organizacje te wydają odpowiednie certyfikaty.

Podstawowe aspekty bezpieczeństwa informacji

W ogólnym przypadku zagrożenia i mechanizmy obronne można rozpatrywać w czterech podstawowych aspektach dotyczących przepływu i składowania informacji:

- poufność *(confidentiality),*
- nienaruszalność *(integrity),*

- zdolność oceny *(accountability)*,
- dostępność *(availability)*.

* **Poufność informacji**

Powinna być zasadą -podstawowymi zagrożeniami przeciwko poufności jest monitorowanie ruchu w sieci oraz niedozwolony dostęp (odczyt) informacji. Do mechanizmów obronnych należy zaliczyć stosowanie kontroli dostępu do odczytu informacji (np. MAC - Mandatory Access Controll), szyfrowanie oraz rzadko stosowany tzw. traffic padding czyli generowanie sztucznego ruchu w sieci w celu zaciemnienia obrazu atakującemu poprzez monitoring.

* **Nienaruszalność informacji**

Użytkownik musi być świadom istnienia zagrożeń, które powodują, że informacja nie dociera do adresata w postaci nienaruszonej . Wymieńmy tu wszelkie świadome i nieświadome modyfikacje oraz powtórzenia (wyobraźmy sobie konsekwencje powtórzenia zlecenia przelewu w wyniku błędu systemu lub ataku). Oczywistym zagrożeniem jest wszelki niedozwolony dostęp (zapis) informacji. Wśród mechanizmów, które zwalczają zagrożenia znajdują się:

- kontrola integralności (np. stosowanie sum kontrolnych),
- kontrola ważności i autentyczności,
- numerowanie sekwencyjne, oznaczanie okresu ważności *(tzw. timestamps)*,
- normalna kontrola praw dostępu do zapisu informacji.

* **Zdolność oceny**

Chodzi tu głównie o umiejętność oceny czy mamy do czynienia z tym użytkownikiem (lub aplikacją), za kogo się podaje. Zagrożeniem jest podszywanie się czyli udawanie, że jest się kimś kto ma prawa do żądania danej usługi. Mechanizmami obronnymi są:

- poświadczanie (np. za pomocą elektronicznego podpisu),
- tzw. audit czyli śledzenie "wejść" do systemu oraz wszelkich podejrzanych akcji,
- notarization czyli np. system certyfikatów wydawanych użytkownikom przez ustanowioną do tego celu organizację.

* **Dostępność**

Ta cecha informacji, która musi być przecież spełniona stanowi jednocześnie potencjalne zagrożenie. Najlepszym mechanizmem obronnym jest kontrola w samym systemie operacyjnym lecz jeśli jej brak, tak jak w DOS-ie to trzeba ją zapewnić w inny sposób. Wśród nowoczesnych mechanizmów kontrolujących dostępność informacji jest tzw. etykietowanie czyli przypisywanie dokumentom cechy mówiącej o jego rodzaju i przynależności do pewnej kategorii (np. "do użytku wewnętrznego").

Otwarte systemy sieciowe nie mogą być otwarte dla wszystkich. Muszą być zamknięte dla nieuprawnionego dostępu oraz innych zagrożeń umyślnych i nieumyślnych. (Otwartość z resztą to nie tylko kontrolowany dostęp lecz także możliwość przyszłej rozbudowy sieci niezależnie od wybranego w danym momencie producenta sprzętu czy oprogramowania).

Opis zagrożeń pozostał by niepełny gdyby nie zostało uwypuklone zagrożenie ze strony wirusów komputerowych.

Wirusy

Wirusy należy traktować jako stałe realne zagrożenie. Niestety najbardziej podatne na działanie wirusów są komputery pracujące pod kontrolą DOSa choć w sieciach komputerowych pojawiają się także wirusy atakujące inne systemy. Pomijając w tym miejscu wskazówki dotyczące ostrożności ze strony użytkowników i administratorów systemów, wymieńmy tylko kilka typów oprogramowania na PC zwalczającego wirusy.

- **"skanery"** - są to programy, które poszukują w pamięci komputera, boot sektorach dysków i zbiorach wykonywalnych określonego wzorca, który stanowi jakby podpis znanego wirusa.
- **"aktywne monitory"** - programy rezydentne analizujące na bieżąco odwołania do DOS-a i BIOS-a w poszukiwaniu akcji typowych dla wirusów - za każdym razem kiedy rozpoczyna się jakaś 'podejrzana' z punktu widzenia monitora akcja program przerywa ją i odpytuje użytkownika czy rzeczywiście jego intencją jest np. wykasowanie grupy zbiorów czy formatowanie dysku.

- **"strażnicy integralności"** - programy używające bazy danych, w których przechowywane są CRC (Cyclic Redundancy Check) zbiorów typu EXE i boot sektorów dyskowych. Ponieważ zbiory wykonywalne i sektory ładujące na dyskach nie podlegają częstym zmianom wirusy mogą być wykryte poprzez porównanie CRC nowej wersji zbioru w stosunku do zapisanej na dysku -różnica w CRC świadczy o zmianie wielkości zbioru.

Jak łatwo się domyśleć każdy ze sposobów ma swoje cienie. "Skanery" bywają oszukiwane przez nowe wirusy lub takie, które nie mają określonego podpisu. Aktywne monitory oprócz ewentualnych problemów wynikających z 'rezydentności' mogą być denerwujące w praktyce ze względu na swą "podejrzliwość" - spowalniają one pracę przez wielokrotne odpytywanie użytkownika kiedy na przykład chce on skasować jakąś grupę zbiorów lub sformatować dysk. "Strażnik integralności" informuje użytkownika jedynie o fakcie zaistnienia modyfikacji zbioru. Czy jest to działanie wirusa czy efekt legalnej akcji pozostaje do rozstrzygnięcia samemu użytkownikowi.

Istnieją programy, które stosują wszystkie trzy techniki dając użytkownikowi pole wyboru. Należy mieć jednak świadomość, że każda z opisanych trzech technik może produkować fałszywe alarmy. Dobrze jest też do końca nie ufać programom usuwającym wirusy. Lepiej odtworzyć zbiór z niezainfekowanej kopii zapasowej - trzeba ją jednak mieć a więc ważna jest świadomość, iż backup jest jednym z mechanizmów bezpieczeństwa.

Na obecnym etapie wojny przeciwko wirusom firmy usilnie starają stworzyć dobre programy zabezpieczające nie tylko stacje robocze pracujące pod kontrolą systemu DOS lecz także serwery (np. NetWare). W przypadku Unixa natomiast rozróżnianie pomiędzy serwerem a stacją roboczą nie ma tak wielkiego znaczenia, gdyż obie kategorie pracują w tym samym (lub podobnym) systemie operacyjnym, w którym można oddzielnie zaimplementować rozmaite mechanizmy zabezpieczające. Inną sprawą jest, że "goły" Unix może stwarzać całkiem spore zagrożenia dla bezpieczeństwa sieci.

Security w standardach

Ochrona systemu sieciowego może być zastosowana w niższych, środkowych lub wyższych warstwach modelu odniesienia OSI. Jak było powiedziane wcześniej istnieje tendencja do przenoszenia funkcji ochronnych do warstw wyższych.

***Mechanizmy protekcji:**

- w warstwie fizycznej można stosować medium swiatłowodowe tam gdzie istnieje obawa nieuprawnionego monitoringu ruchu w sieci oraz tzw. point - to - point encryption czyli szyfratory stosujące odpowiednie algorytmy zainstalowane na końcowych urządzeniach użytkowników;

Algorytmy szyfrowania i funkcje szyfrujące

**DES (Data Encryption Standard)* jest popularnym standardem algorytmu szyfrującego opartego na technice symetrycznej. Oznacza to, że ten sam klucz jest używany do szyfrowania i rozszyfrowywania danych. Dwie strony porozumiewające się między sobą muszą wymienić między sobą tajny klucz, który jest właściwy tylko dla tej pary. Liczba potrzebnych kluczy jest więc proporcjonalna do kwadratu liczby użytkowników.

**RSA*-Algorytm kryptografii asymetrycznej opracowany w 1978 roku przez trzech twórców (Rivest,Shamir,Adleman), których pierwsze litery nazwisk tworzą nazwę systemu. Jest stosowany w tzw. systemach klucza publicznego *(public key cryptosystem)*. Klucze publiczne mogą być udostępniane w nieutajnionych katalogach na dyskach komputerów w sieci.

**one way function* - funkcja matematyczna f(x)=y,która choć łatwa do policzenia jest trudna do przeprowadzenia operacji odwrotnej tzn. znalezienia x na podstawie y. Jak łatwo się domyśleć funkcje takie stosowane są w celu kodowania informacji. Sprawdzający poprawność przesłanej informacji (odbiorca) nie rozkodowuje części kodowanej lecz również dokonuje kodowania części niekodowanej i porównuje z częścią zakodowaną, którą otrzymał

**hash functions* - są skomplikowanymi funkcjami kodującymi "w jedną stronę" *(one-way function)*, które nie powodują kolizji a więc nie mogą istnieć dwie różne informacje wejściowe, które dadzą ten sam wynik wyjściowy po zastosowaniu funkcji hash. Powinny one dokonywać maksymalnie dużej kompresji danych - tzw. skrótu wiadomości (dane kodowane są często używane jako dodatkowe do przesyłania- n.p. elektroniczny podpis- i spowalniają komunikację) a jednocześnie nie powodować niejednoznaczności (kolizji).

Podpis elektroniczny (cyfrowy)

Termin ten *(ang. digital signature)* oznacza uwiarygodnienie porcji wysyłanej przez użytkownika informacji (n.p. listu poprzez dołączenie do tej informacji zaszyfrowanego skrótu tej informacji). Ów skrót jest tworzony poprzez użycie tzw. "one-way hash function" podczas gdy szyfrowanie odbywa się przy użyciu tajnego klucza użytkownika wysyłającego. Szyfrowanie przy użyciu tajnego klucza gwarantuje, że ów elektroniczny podpis nie zostanie podrobiony. Odbiorca podpisanej w ten sposób informacji dokonuje weryfikacji poprzez:

- zastosowanie tej samej funkcji hash w celu stworzenia skrótu otrzymanej porcji informacji (n.p. dokumentu w postaci elektronicznej)
- porównanie rezultatu z tym, który otrzymuje dzięki rozszyfrowaniu podpisu elektronicznego przy użyciu publicznego klucza nadawcy.

Istnieją także naturalne i sztuczne sposoby utrudniające monitoring jak np. linie multipleksowane, tunelowanie czy generowanie sztucznego ruchu,

(Należy przy tym mieć świadomość, że zabezpieczenie warstw niższych nie daje jeszcze pewności działania warstw wyższych)

- w warstwach od liniowej do warstwy prezentacji mechanizmy protekcji zostaną omówione w dalszej części,
- w tzw. protokołach dystrybucji informacji są zdefiniowane odpowiednie mechanizmy security:

  # MHS (Message Handling System) Security w standardzie poczty elektronicznej X.400,
  # Directory Accesss Security w standardzie X.500,
  # File Access Security we FTAMie,
  # Transaction security.

- w informacji specyficznej dla danych aplikacji:

  # Document Security (np. WordPerfect)
  # EDI Security w standardzie Electronic Data Interchange
  # Financial Security w systemach bankowych.

Głównymi organizacjami zajmującymi się standaryzowaniem mechanizmów ochrony są ISO, CCITT (obecnie ITU-T) oraz ECMA. Obecnie isnieją standardy (architektury) security opracowane przez ISO (ISO 7498-2) zwane OSI Security Architecture oraz CCITT (X .402) wchodzący w skład standardu X.400. Oprócz tego istnieją mniej lub bardziej popularne protokoły różnych warstw modelu OSI zapewniające mechanizmy ochronne. W niższych warstwach są to tzw. standardy lower-layer:

- Transport Layer Security Protocol (ISO DIS 10736)
- IEEE Secure Interoperable LAN Standard (IEEE 802.10)
- Physical Layer Encryption (ISO 9160).

Security wyższych warstw

Warstwy pomiędzy warstwą transportową a warstwą zastosowań mogą stanowić odpowiednią bazę dla security np. warstwa prezentacji może pełnić rolę szyfrowania i deszyfracji. W ramach organizacji ISO definiuje się protokół Security Exchange ASE (jest to prosty protokół ochrony wymiany pól security i przesyłania zabezpieczonych danych) oraz Security Transfer Syntax (dotyczy notacji i procedur kodowania). Alternatywnym rozwiązaniem poza ISO są:

* amerykański system Kerberos
* ECMA Authentication & Priviledge Attribute Service - opracowany dla potrzeb Wspólnoty Europejskiej
* Directory Authentication w standardzie X.509 - początkowo opracowanym dla potrzeb X.500, który później zyskał szersze zastosowanie.

Kerberos

System ten opracowany przez MIT (Massachussets Institute of Technology) w ramach projektu Athena jest możliwy do zaimplementowania w systemach UNIXowych a dokładnie w środowiskach TCP/IP lecz także OSI. Jako ciekawostkę można podać, że Kerberos stał się częścią OSF Unixa. System bazuje na technice wykorzystującej tzw. Authentication Server (dedykowany komputer zajmujący się rozdawaniem biletów na

czas jednej sesji). Kerberos bazuje na szyfrowaniu DESem "czułych" informacji takich jak hasła przesyłane przez sieć ze stacji klienta do serwera. Do podstawowego wyposażenia Kerberosa należą:

- dystrybucja klucza szyfrującego i klucza podpisu elektronicznego dla użytkownika na czas sesji,
- symetryczne szyfrowanie,
- opcjonalny "ticket-granting ticket" na początkowe zalogowanie się w sieci,
- Kerberos działa w środowisku wielodomenowym i z wieloma serwerami autentykacji.

ECMA Authentication and Priviledge Attibute Service

Jako standard ECMA Authentication and Priviledge Attribute Service powstał w 1992 roku i nakierowany jest na sieci OSI. Do podstawowego wyposażenia należą:

* symetryczne i asymetryczne szyfrowanie
* mechanizm certyfikatów wydawanych przez "trzecią stronę" - odpowiednik mechanizmu wydawania biletów przez server w systemie Kerberos,
* klucz szyfrujący i podpisu elektronicznego wydawany na sesję.

Przykład zaimplementowania mechanizmów bezpieczeństwa w standardzie X.400

X.400 jest standartem CCITT definiującym bezpieczny sposób przesyłania poczty elektronicznej. Opublikowany po raz pierwszy w 1984 roku, został wzbogacony w kolejnych edycjach w 1988 i 92 roku. Standard ten, na bazie którego istnieje już wiele produktów komercyjnych przewiduje całą gamę środków i mechanizmów pozwalających całkowicie kontrolować wszelkie aspekty przesyłania informacji. Wśród możliwości X.400 znajduje się:

- potwierdzenie autentyczności nadawcy - mechanizm pozwalający odbiorcy sprawdzenie autentyczności nadawcy,
- wiarygodność dostarczenia - funkcja pozwalająca nadawcy przekonać się, że informacja (w niezmienionej formie) dotarła do właściwego odbiorcy,
- nienaruszalność zawartości - opcja dająca odbiorcy możliwość zweryfikowania czy oryginalna zawartość informacji nie została zmodyfikowana w drodze,
- poufność - właściwość uniemożliwiająca odczytanie wiadomości wszystkim oprócz adresata,
- ustalanie kontekstu bezpieczeństwa - mechanizmy pozwalające na ustalanie pomiędzy przesyłającymi sobie komponentami systemu właściwych opcji security,
- etykietowanie - możliwość nadania przesyłanej wiadomości odpowiedniej etykiety świadczącej o przynależności do określonej kategorii np. tajności,
- nienaruszalność sekwencji - zapobiega zaburzeniom w kolejności otrzymywania wysyłanej sekwencji listów oraz zabezpiecza przed powtórzeniami (kilkukrotne nadejście tego samego listu),
- brak możliwości wyparcia się raz wysłanej przez nadawcę informacji a także faktu otrzymania jej przez adresata.

Możliwości zabezpieczające w X.400 są opcjami, w które wyposażony jest MHS (Message Handling System). Mogą być one zastosowane w celu zminimalizowania ryzyka narażenia przesyłanych treści na rozmaite zagrożenia - opisane na początku referatu. Security oferowane przez MHS jest zaimplementowane na poziomie usługi i jest w zasadzie niezależne od innych form bezpieczeństwa, które można przedsięwziąć na różnych poziomach przesyłania informacji. W praktyce mechanizmy przewidziane w MHS są wystarczające tak że np. dodatkowe szyfrowanie na poziomie łączy fizycznych jest zbyteczne.

To z jakich elementów zbudowano security w konkretnym systemie MHS jest zawarte w kopercie (*envelope*) czyli opakowaniu treści do przesłania. Wiele z tego na czym opiera się bezpieczeństwo poczty X.400 polega na mechanizmach szyfrowania. MHS nie narzuca z góry określonych algorytmów dając tym samym, przynajmniej teoretycznie możliwości wyboru. Jednak w praktyce główny nacisk w standardzie położono na mechanizmy szyfrowania asymetrycznego. W tym kontekście duże znaczenie odgrywa tu standard RSA.

Security w standardzie X.500

W stosunku do użytkownika chcącego skorzystać z informacji zawartej w bazie danych serwisu Directory X.500 mogą być zastosowane generalnie dwa podejścia:

- tzw. proste poświadczanie *(simple authentication)*,

– tzw. silne poświadczenie *(strong authentication)*.

Proste poświadczanie opiera się na sprawdzeniu czy hasło, którym posłużył się użytkownik w celu wejścia do zasobów jest właściwe. Użytkownik może mieć jedno hasło na korzystanie z wielu serwisów Directory. W przypadku, kiedy pożądane jest zwiększenie bezpieczeństwa hasła mogą być kodowane za pomocą one-way function.

Bardziej kompleksowym podejściem do problemu bezpieczeństwa jest stosowanie silnego poświadczania. Bazuje ono na wykorzystaniu mechanizmów szyfrowania asymetrycznego *(public key cryptography)*. Directory jest wykorzystywane wtedy jako składnica kluczy publicznych użytkowników. Klucze są oczywiście chronione przed zafałszowaniem. W ten sposób Directory X.500 może stanowić ważny składnik bezpiecznego systemu wymiany poczty elektronicznej standardu X.400.

Oba podejścia są kolejnym przykładem, ze tak na prawdę decydująca jest polityka bezpieczeństwa, którą się przyjmie - dopiero w dalszej konsekwencji można mówić o zastosowaniu tych czy innych mechanizmów. Generalnie uwaga ta dotyczy wszystkich sieci wymagających ochrony - nie tylko systemu X.500.

Techniki szyfrowania

*Szyfrowanie symetryczne

W konwencjonalnych systemach kryptograficznych klucz użyty do zaszyfrowania informacji przez jednego użytkownika (nadawcę) w celu przesłania tajnej informacji jest tym samym kluczem, który zostanie użyty przez właściwego odbiorcę w celu odszyfrowania informacji. Klucz ten powinien być na tyle trudny do złamania, aby chronić informację przez czas jej ważności. Odrębnym problemem jest odpowiednio częsta zmiana kluczy i sposoby przesyłania aktualnego klucza właściwym odbiorcom.

*Szyfrowanie asymetryczne

W tej metodzie klucz szyfrujący jest różny od klucza potrzebnego do zdeszyfrowania przesyłki (wiadomości). Z danym użytkownikiem związana jest więc para kluczy. Jeden klucz owej pary jest publicznie znany i może być użyty przez wielu użytkowników do zaszyfrowania informacji skierowanej do użytkownika X. Drugi z kluczy danej pary jest tajny i należy on wyłącznie do X, który używa go w celu rozszyfrowania przychodzących informacji. X może rozdawać swój klucz 'publiczny' komu chce bez obaw, że ktoś inny znający ten klucz będzie w stanie odczytać informację raz zaszyfrowaną. Jest rzeczą niewykonalną obliczeniowo dojść do tajnego klucza znając klucz publiczny. Najważniejsze jest aby istniała pewność, że dany klucz publiczny należy rzeczywiście do właściwej osoby.

W przypadku Directory dwa aspekty strategii bezpieczeństwa są godne podkreślenia:
– autoryzacja (określenie praw dostępu, kontrola dostępu, zarządzanie prawami dostępu),
– poświadczanie (sprawdzanie tożsamości użytkowników, sprawdzenie przez użytkownika tożsamości źródła informacji).

Pierwszy aspekt wiąże się z lokalną realizacją dostępu do katalogów i ich obiektów i podlega zarządzaniu w zwykły sposób dostępem do zasobów serwera. Twórcy standardu X.500 podkreślają natomiast, że istnieje potrzeba zdefiniowania aż pięciu kategorii praw dostępu:
– detekcja (użytkownik posiadający jedynie prawo detekcji może co najwyżej stwierdzić istnienie tego o co pyta)
– porównanie,
– prawo do czytania,
– prawo do modyfikacji,
– tworzenie nowych i kasowanie istniejących komponentów,
– prawo do modyfikacji nazewnictwa.

Jeśli nie zostanie dla danego obiektu chronionego nadane żadne z pięciu praw baza ma obowiązek odpowiedzieć na żądania tak jakby dany obiekt w ogóle nie istniał.

Drugim aspektem czyli poświadczaniem zajmuje się w standardzie rekomendacja X.509. Szerokie omówienie jej przekracza ramy niniejszego referatu. X.509 jest jądrem X.500 jeśli chodzi o security.

Directory jest naturalnym i idealnym miejscem, gdzie komunikujące się w ten czy inny sposób strony mogą uzyskać informacje poświadczające tożsamość każdej ze stron. Zupełnie nowym pojęciem jest tzw. certyfikat użytkownika czyli klucz publiczny użytkownika wraz z innymi informacjami zaszyfrowanymi przy pomocy tajnego klucza organizacji wydającej certyfikaty *(certification authority)*. Certification authority jest w tym przypadku organizacją, której zaufa pewna grupa użytkowników - mającą za zadanie kreowanie i wyda-

wanie certyfikatów. Organizacja ta może również produkować klucze użytkowników. Już w tym momencie widać jak skomplikowany może być system a wszystko po to by zapewnić bezpieczeństwo i wiarygodność.

Prześledźmy drogę jaką musi pokonać użytkownik aby skomunikować się z innym użytkownikiem - jeśli zastosowano public cryptography...

Jeśli ktoś chce powiedzmy wysłać zaszyfrowany list do innego użytkownika musi mieć jego klucz publiczny. Otrzymuje go ze źródła, któremu ufa czyli z certification authority (urząd d/s certyfikatów). Musi jednak dysponować kluczem publicznym organizacji wydającej certyfikaty. Chcąc umieścić swój klucz publiczny w bazie urzędu d/s certyfikatów użytkownik musi osobiście wylegitymować się, że jest tym za kogo się podaje.

Certyfikaty dzięki zastosowaniu odpowiednich technik szyfrowania i podpisowi elektronicznemu (*cyfrowemu - ang. digital signature*) są niepodrabialne. Mając już klucz publiczny adresata nadawca wysyła zaszyfrowany list, który może być odczytany jedynie przez właściwego odbiorcę - ponieważ tylko on dysponuje "parą" do klucza publicznego, za pomocą którego stworzono przesyłkę - tajny klucz adresata.

EDI

Wiele firm proponuje rozwiązania oparte o standard elektronicznego przesyłania dokumentów EDI (*Electronic Data Interchange*). W standardzie EDIFACT przewiduje się zastosowanie usług ochrony informacji na poziomie wiadomości (każdy komunikat jest chroniony oddzielnie). Oprócz tego przewidziana jest kontrola integralności sekwencji chroniąca przed np. zwielokrotnieniem wiadomości. Proces standaryzacji nagłówków odpowiedzialnych za security jeszcze nie został zakończony jednak twórcy istniejących rozwiązań komercyjnych mają nadzieję, że ewentualne zmiany dotyczyć będą szczegółów - sama zasada pozostanie niezmieniona. W standardzie EDIFACT przewidziano następujące usługi związane z bezpieczeństwem:

- poufność,
- niezaprzeczalność odbioru,
- niezaprzeczalność nadania,
- integralność wiadomości,
- uwierzytelnienie,
- integralność sekwencji wiadomości.

W skrócie rzecz ujmując nagłówki odpowiedzialne za poszczególne usługi ochrony stanowią jakby dodatkową kopertę dla przesyłanej wiadomości. Standard przewiduje też dwa specjalne komunikaty AUTACK oraz CIPHER dla realizacji security. AUTACK służy do przesyłania podpisu cyfrowego natomiast CIPHER - jak łatwo się domyśleć - służy do realizacji usługi poufności czyli szyfrowania.

Gadżety

Przy istniejącej konieczności coraz pewniejszego zabezpieczania zasobów komputerowych oraz transmisji sieciowych nie dziwi fakt, iż podaż rozmaitego sprzętu i oprogramowania, w które możemy doposażyć nasze komputery i urządzenia teleinformatyczne rośnie.

Chip Card - krok dalej niż karta magnetyczna

Wszędzie tam, gdzie rozliczenia dokonywane są za pomocą kart magnetycznych obsługiwanych przez sieciowe systemy komputerowe istnieje obawa użytkowników przed skradzeniem karty. Nowa generacja kart zwanych Chip Card (zwana też Smart Card) zapewnia poświadczenie użytkownika. Karta jest w istocie małym komputerem zawierającym mikroprocesor i pamięć a pozwala na dostęp (modyfikacje) do danych w niej zgromadzonych jedynie po wprowadzeniu przez użytkownika do czytnika odpowiedniego numeru zwanego PIN (*personal identification number*). Chip card bez zasilania może być przechowywana do 10 lat.

Aktywatory - dodatkowe zabezpieczenia

Małe pudełeczka wpinane przeważnie w port RS komputera (ale także n.p. SCSI) pozwalają na wprowadzenie dodatkowej przeszkody przed nieautoryzowanym działaniem. Mogą zabezpieczać przed nielegalnym kopiowaniem oraz przed uruchamianiem pirackich kopii nie tylko w środowisku "pecetowym" lecz także np. na Unixowych stacjach roboczych. Mogą również zabezpieczyć przed przekroczeniem dozwolonej liczby

użytkowników w sieci. Oczywiście aktywator współpracuje z odpowiednim oprogramowaniem instalowanym na komputerze, w który jest wpięty.

Karty szyfrujące do PC

Obecnie nowa generacja kart implementująca mechanizmy kryptograficzne na PC pozwala na szybkie szyfowanie zarówno w standardzie DES jak i RSA, generowanie oraz bezpieczne przechowywanie kluczy, zapewnia możliwość stosowania podpisu elektronicznego.

PC - mainframe

Niektóre systemy security zajmują się integracją stacji PC lub sieci lokalnych podłączonych do komputerów typu mainframe. Oprócz rozwiązań typowo software'owych stosowane są rozwiązania łączne, gdzie między klawiaturę a PC włączony jest moduł kryptograficzny wyposażony w czytnik karty magnetycznej, spełniający funkcje szyfrujące, deszyfrujące (DES, RSA), generowanie kluczy, elektroniczny podpis. W takim układzie hasło wprowadzone z klawiatury nigdy nie jest przesyłane dalej niż do modułu kryptograficznego. Metoda ta zabezpiecza przed programami hackerów czytającymi hasła z klawiatury.

End - to end protection

Termin ten oznacza technikę szyfrowania strumienia informacji na początku tej drogi do celu i deszyfrowania jej przez użytkownika, do którego jest ona przeznaczona. Dotyczy to zarówno połączeń typu punkt-punkt jak też korzystania z - na przykład - sieci X.25. W tym ostatnim przypadku jest to coś w rodzaju prywatnego security pomiędzy dwoma użytkownikami (przykładowo oddziałami tej samej firmy) połączonymi przez sieć publiczną. W praktyce systemy te opierają się na dodatkowych "pudełkach szyfrujących" wstawionymi pomiędzy powiedzmy PC a modem lub pomiędzy urządzenie typu koncentrator terminali-PAD a modem synchroniczny. Szyfratory te mogą opierać się o znane algorytmy typu DES, lecz często realizują funkcje kryptograficzne w oparciu o algorytmy firmowe będące tajemnicą korporacji produkującej sprzęt. Szyfrowanie powinno być oczywiście transparentne w stosunku do protokołów przesyłanych przez sieć. Tego typu rozwiązania mogą być wyposażone w interfejsy najczęściej spotykane w instalacjach sieciowych (V24 asynchroniczne i synchroniczne, V.35, V.36, X.21bis, G 703 , fax grupa 3 T.30,T.4), pozwalają stosować protokoły typu X.25, X.28, X.21 a dostępne szybkości znajdują się w przedziale 2400 b/s do 2.048 Mbps i więcej.

Niektóre firmy oferują też urządzenia szyfrujące faxy a nawet głos (telefony zwykłe i ISDN).

Modemy i multipleksery szyfrujące

Innym podejściem do szyfrowania treści przesyłanych liniami dzierżawionymi lub komutowanymi jest wyposażenie modemów oraz multiplekserów w systemy kodowania. Za pomocą tego typu urządzeń wprowadzana jest ochrona całości przesyłanego strumienia danych w szczególnie narażonych liniach. Warto tu zwrócić uwagę, że w tym przypadku ochrona jest implementowana po stronie budującego sieć a nie użytkownika z niej korzystającego. W praktyce tego typu instalacje są rzadko spotykane - szyfrowanie 100% informacji krążącej w całej sieci, w wielu przypadkach jest nadmiarowe (dla mniej wymagających użytkowników) a w innych niewystarczające (dla bardzo wymagających użytkowników czy aplikacji). Stanowi też łatwy łup dla atakującego - ten sam system chroni wszystkich i wszystko, można próbować np. ataku Shamira.

Security w NetWare 4.0

W najnowszej wersji systemu Novell NetWare mechanizmy bezpieczeństwa wzbogaciły się o możliwość stosowania technik kryptograficznych w oparciu o klucz publiczny. Tak więc poświadczenie autentyczności użytkownika odbywa się przy użyciu asymetrycznych metod szyfrowania. Zaszyfrowany klucz publiczny jest przesyłany poprzez sieć z serwera do stacji użytkownika w momencie logowania. Hasło wprowadzone przez użytkownika po pierwsze jest konieczne do wejścia do sieci a po drugie modyfikuje klucz publiczny tak, że staje się on kluczem tajnym danego użytkownika na czas sesji. Każdorazowo kiedy użytkownik wystawia żądanie dostępu do konkretnego zasobu sieci tajny klucz służy do potwierdzenia praw użytkownika do korzystania z tego zasobu. NetWare 4.0 ma zaimplementowany mechanizm ACL (Access Control List) charakterystyczny dla systemów o podwyższonym bezpieczeństwie a pozwalający na precyzyjne ustalenie praw konkretnych użytkowników do poszczególnych zasobów (zbiorów, drukarek i.t.p.).

Przy każdym logowaniu użytkownik otrzymuje nowy klucz tajny. W ten sposób hasło użytkownika nie jest w ogóle przesyłane przez sieć. Istnieje ono w pamięci stacji klienta do momentu kiedy zostanie wygenerowany klucz tajny użytkownika ważny podczas bieżącej sesji - po czym jest usuwane. Część zatem "zabiegów" służących do uwierzytelniania użytkownika jest wykonywana "u klienta" co jak łatwo przewidzieć wymaga zainstalowania dodatkowego oprogramowania na stacji użytkownika.

Problem przesyłania haseł użytkownika poprzez sieć do serwera okazał się problemem o kluczowym znaczeniu dla bezpieczeństwa. Znane są przykłady przechwytywania haseł w NetWare 3.11 i podszywania się pod innego użytkownika. Dlatego też firmy wcześniej czy później implementują mechanizmy kodowania haseł przesyłanych ze stacji do serwera (Banyan, Novell). NetWare 4.x wprowadza też Directory Services powstały w oparciu o X.500.

Oprogramowanie antywirusowe dedykowane do pracy w sieci Novell.

Pakiety tego typu zawierają część w postaci NLM (NetWare Loadable Module) oraz część DOSową, spełniają więc funkcje przeszukiwania w serwerach sieci i dyskach stacji lokalnych.

Sieć Banyan Vines

System Vines firmy Banyan łączy w sobie zalety sieci lokalnej (łatwość operowania zasobami np. pod DOSem i Windowsami) i rozległej (możliwość dołączania odległych lokalizacji przy pomocy rozmaitych transportów: linie dzierżawione, X.25, TCP/IP). Sieć Vines zyskała zwolenników również dzięki solidnym mechanizmom security. Przy budowaniu rozległej sieci Banyan Vines poszczególne serwery mogą być tak skonfigurowane aby komunikacja pomiędzy nimi była możliwa jedynie po wymianie między serwerami odpowiedniego hasła, które przekazywane jest automatycznie w postaci zaszyfrowanej. Administratorzy mogą wybrać jeden z trzech poziomów bezpieczeństwa w komunikacji pomiędzy serwerami: bez żadnych barier, tylko poczta elektroniczna, całkowite ograniczenie komunikacji.

System ponadto przewiduje kilka kategorii użytkowników: administrator serwera, administrator grupy użytkowników, operator zarządzający serwisami drukarkowymi oraz "zwykły" użytkownik. Użytkownicy każdej kategorii mogą bardzo precyzyjnie zarządzać dostępem do określonych zasobów jak zbiory, katalogi, drukarki, które są w ich gestii (w zależności od praw wynikających z kategorii użytkownika). Administratorzy mogą zakładać dzienniki zdarzeń oraz alarmy sygnalizujące określone zdarzenie w sieci (np. nieautoryzowane próby wlogowania się).

Należy przy tym wszystkim zwrócić uwagę na rzecz wymagającą ostrzeżenia. W sieci Banyan wartości domyślne (*default*) wszystkich parametrów mających wpływ na security są ustawione tak, że praktycznie silna ochrona nie istnieje. Dopiero praca administratora nad bezpieczeństwem systemu, wybór i ustawienie odpowiednich opcji (np. forsowanie minimalnej długości hasła i częstej jego zmiany przez użytkownika) może stworzyć prawdziwie bezpieczne środowisko pracy. Z resztą w większości systemów fabryczne ustawienia nie dają jeszcze właściwej ochrony - pozostawiając miejsce dla pracy administratora.

Bezpieczeństwo w systemach UNIX

Jak wiadomo ten system operacyjny nie powstał z myślą o security, przeciwnie dawał i daje do tej pory ogromne możliwości przesyłania informacji na dowolne odległości (pozyskiwania zasobów) gdyż standardowo jest wyposażony w podstawowe mechanizmy sieciowe. Jednak zachowanie odpowiedniej równowagi pomiędzy otwartością a prywatnością wymaga od twórców oprogramowania i administratorów implementowania mechanizmów zapewniających ochronę na odpowiednim poziomie. Wśród zarejestrowanych przypadków hackingu istnieją tak kuriozalne jak zdalny podsłuch poprzez mikrofon montowany fabrycznie w komputerach SUN. Pomysłowość hackerow jest tak wielka, iż dostawcy systemów unixowych poczęli implementować poziomy security C2 lub nawet B1 na poziomie systemu (lub nazywają to "*trusted system*"). Jednocześnie powstało wiele oprogramowania public domain poprawiającego security w Unixie - często nawet o szerszych możliwościach niż mechanizmy fabryczne. Szczegółowe potraktowanie zagrożeń w Unixie i mechanizmów obronnych przekracza ramy niniejszego referatu - istnieje w USA organizacja zajmująca się rejestrowaniem przypadków ataków i doradzająca środki przeciwdziałające; jest to CERT (Computer Emergency Response Team) na uniwersytecie Carnegie Mellon oraz FIRST (Forum of Incident Response and Security Teams) - forum o zasięgu światowym wykreowane przez organizacje rządowe Stanów Zjednoczonych i innych państw.

Aby zasygnalizować problem przyjrzyjmy się jakie funkcje spełnia jeden z najpopularniejszych pakietów bezpieczeństwa - produkt public domain o nazwie COPS. Jest to:

- sprawdzanie trybów dostępu do katalogów, zbiorów i urządzeń (*device*) pod kątem nieuprawnionych modyfikacji,
- kontrola haseł stosowanych przez użytkowników aby nie były zbyt łatwe do odgadnięcia,
- kontrola zawartości, formatu i bezpieczeństwa zbiorów z hasłami,
- nadzór nad przypadkami mechanicznego uruchamiania procedur (np. porzez cron),
- sprawdzanie sum kontrolnych ważnych zbiorów,
- czuwanie nad prawami zapisu do newralgicznych zbiorów konfiguracyjnych użytkownika (np. .cshrc)
- kontrola opcji anonymous ftp,
- sprawdzanie wielu znanych potencjalnych luk w systemie,
- porównywanie dat i wersji zbiorów systemowych w stosunku do raportów CERT o wykrytych błędach i lukach w konkretnych wersjach systemów.

Jest to tylko drobny przykład dostępnych narzędzi. Oprócz aspektów bezpieczeństwa oferowanego przez systemy, sami użytkownicy Internetu mogą stosować w prywatnej korespondencji szyfrowaną pocztę elektroniczną opartą o technikę kluczy publicznych.

Department of Defense
Orange Book
(Trusted Computer System Evaluation Criteria)

Opracowanie klasyczne poświęcone zdefiniowaniu poziomów zabezpieczeń systemów komputerowych.
Systemy podzielono na cztery grupy. W grupie jest podział na klasy.
Grupy:
D - minimalne zabezpieczenia,
C - zabezpieczenie dyskrecjonalne,
B - zabezpieczenia obowiązkowe *(mandatory protection)*,
A - weryfikowalne zabezpieczenia.
Klasy:
C1 - podstawowe mechanizmy chroniące zbiory użytkowników przed nieuprawnionym dostępem (*access control*) wraz z koniecznością podania hasła na wejściu do systemu.
C2 - mechanizmy ochrony dostępu są precyzyjniejsze niż w klasie C1, oprócz tego wymagana jest możliwość sygnalizowania przez system wszystkich zdarzeń związanych z bezpieczeństwem *(audit)*
B1 - wszystko to co w klasie C2 plus mechanizm etykietowania - nadrzędny w stosunku do ustaleń użytkowników jeśli chodzi o nadawanie uprawnień dostępu do określonych zbiorów; tak zwana mandatory access controll (MAC) wymusza ustalenie relacji dostępności zasobów (obiektów) dla poszczególnych użytkowników.
B2 - zabezpieczenie strukturalne - jeszcze precyzyjniej zdefiniowane mechanizmy zabezpieczania oraz interfejs modułu odpowiedzialnego za bezpieczeństwo
B3 - domeny security - architektura systemu musi być w najwyższym stopniu odporna na nieuprawnioną penetrację; muszą być określone porcedury alarmowania i odtwarzania po ewentualnym ataku; osobnym wymaganiem jest możliwie mała komplikacja domen security aby łatwo można było przeanalizować (oszacować) i przetestować konstrukcję.
A1 - najwyższy poziom security - cała konstrukcja systemu musi być weryfikowalna tzn musi poddawać się ocenie formalnej czy i jak obowiązujące mechanizmy - w zasadzie nic więcej niż w B3 - są w praktyce realizowane.

Ochrona sieci "pecetowych"

Sieci, w których stacjami roboczymi są komputery PC pracujące pod DOS/Windows to wciąż popularna konstelacja w naszym kraju. Dyski sieciowe w takich systemach (np. Novell czy Banyan) są po wykonaniu odpowiednich zabiegów łatwo administrowane pod względem bezpieczeństwa. Jednak PC z własnym dyskiem z systemem DOS i np. w środowisku Windows jest pod względem "security" potencjalnie dużym zagrożeniem dla sieci z powodu dużej dostępności rozmaitego oprogramowania i brakiem mechanizmów zabezpieczających. Komputery takie włączone do sieci korzystają wprawdzie z mechanizmów dostarczanych w systemie (Vines, NetWare) lecz sam PC w dalszym ciągu nie jest chroniony przed nieuprawnionym dostępem (dyski lokalne nie są zabezpieczane oraz nie ma kontroli bootowania ze stacji dyskietek).

"Usieciowiony" komputer w gruncie rzeczy może być traktowany w aspekcie bezpieczeństwa również jako wolnostojący jeśli użytkownik na przykład nie zaloguje się do sieci tylko pracuje z dyskami lokalnymi.

Należy więc zaimplementować poziom bezpieczeństwa C2 względnie C1 na komputery PC niezależnie od tego czy są one w sieci czy też nie. Poziomy C1 czy C2 w/g Orange Book są często stosowane przez producentów z pewną dowolnością (dopóki nie mają formalnej ewaluacji NSCA lub odpowiednika Europejskiego -

poziomy E) więc zdarza się, że C1 jednego producenta przewyższa realnie C2 oferowany przez innego dostawcę.

Niemniej jednak bezpieczny system powinien zapewniać co najmniej poniższe warunki:

1. Komputery PC powinny posiadać możliwość zdefiniowania użytkowników i ich praw do zasobów zarówno w trybie lokalnym jak i sieciowym.
2. Powinny istnieć zabezpieczenia przed bootowaniem z dyskietki w sposób nieuprawniony (może to dotyczyć wszystkich komputerów lub tylko tych, które są objęte zwiększoną ochroną).
3. Komputery PC muszą zapewniać możliwość administrowania (centralnego lub/i lokalnego) jak np.:
   - wymuszanie zmiany haseł,
   - precyzyjne definiowanie praw użytkowników do zbiorów, drukarek, dysków,
   - nadzór *(audit)* czyli sygnalizowanie i rejestrowanie zdarzeń w systemie,
4. Wskazana jest możliwość utrudnienia w dostępie do komend takich jak: format czy fdisk,
5. Na niektórych komputerach wskazane jest zablokowanie dostępu do systemu DOS zwykłemu użytkownikowi na rzecz komunikowania się z systemem poprzez system definiowalnych menus.
6. Należy rozważyć możliwość wyposażenia szczególnie newralgicznych komputerów w system identyfikacji użytkownika w oparciu o karty magnetyczne, smartcard, chip-card.
7. Każdy PC powinien mieć opiekuna odpowiedzialnego za system i jego bezpieczeństwo. Do opiekuna należy odpowiednio częste sprawdzanie dysku (dysków) oprogramowaniem antywirusowym oraz dokonywanie archiwizacji istotnych danych według grafika. Oprócz tego sami użytkownicy są odpowiedzialni za archiwizowanie swoich" zbiorów.

Możliwe do zastosowania rozwiązania

Obecnie dominującą tendencją w zabezpieczaniu sieci takich jak Banyan lub Novell jest doposażanie stacji roboczych (lub serwerów) w dodatkowe oprogramowanie mające rozszerzać pojęcie security na ochronę nie tylko serwerów (do czego sprowadza się administrowanie użytkownikami zalogowanymi do sieci) ale też stacji roboczych czyli pecetów, które powinny być chronione jako potencjalne miejsce wystąpienia zdarzenia mogącego mieć destrukcyjny wpływ na działanie sieci. Istnieje kilka komercyjnych pakietów spełniających te warunki.

Powinności i odpowiedzialność

Zrozumienie problematyki ochrony i bezpieczeństwa jest powinnością zarówno użytkownika jak też oferenta usług sieciowych czy wielodostępnych. Jeżeli mamy do czynienia z komputerem rzeczywiście osobistym to osobiście odpowiadamy przed sobą za jego funkcjonowanie. Osobiście archiwizujemy pliki, sprawdzamy programem antywirusowym czy osobiście nie przynieśliśmy na dyskietce jakiegoś wirusa, osobiście też przechowujemy sprawdzoną kopię systemu operacyjnego. Jeśli jednak jesteśmy współużytkownikiem serwera wielodostępnego to często zakładamy, że wszystkie obowiązki spadają na administratora tego systemu. Jednak takie podejście jest po prostu jeszcze jednym zagrożeniem dla całego systemu.

Jak już było wspomniane wcześniej, według zachodnich opracowań użytkownicy sieci lokalnej często stanowią podstawowe zagrożenie dla bezpiecznej pracy organizacji. Dlaczego? Każdy użytkownik ma bowiem przydzielone przez administratora konto *(account, username)* na określonym serwerze lub ogólnie w sieci (istnieją systemy, w których username nie jest związany z jednym serwerem) i jest za ten "skrawek" dysku czy też prawa jakie otrzymał od administratora odpowiedzialny. Przed sobą i innymi użytkownikami tego systemu. Odpowiedzialność ta po pierwsze jest ściśle związana z ochroną osobistego hasła *(password)* dającego wejście do systemu. Tu pojawia się problem. Hasła bezpieczne są skomplikowane a przez to trudne do zapamiętania a więc użytkownicy zapisują je (najchętniej gdzieś blisko terminala) i w ten sposób hasła te przestają być bezpieczne. Hasła proste są łatwe do zapamiętania i nie zapisuje się ich - z reguły stają się one więc łatwym łupem hackerów ...

Analizy haseł stosowanych przez użytkowników dowodzą, że często używa się jako haseł imion (swoje, bliskich), numeru swego telefonu, części adresu a w najlepszym razie słów występujących w słownikach - po to w końcu wymyślono słowa. A jednak...

Współczesne programy łamiące hasła...

...potrafią sprawdzić czy nasze hasło jest imieniem własnym lub nawet czy występuje w obszernym słowniku danego języka. Dane dotyczące adresu czy numeru telefonu użytkownika też są łatwo zdobywalne... Pro-

gramy łamiące sprawdzają wiele set tysięcy haseł w stosunkowo krótkim czasie i bez problemu odgadują hasło KeIsYzRk, które z pozoru wygląda na dość trudne lecz de facto jest to imię Krzysiek pisane wspak dużymi i małymi literami. Programy, którymi posługują się hackerzy sprawdzają nawet rozmaite "wariacje" prostych haseł (np. imion żeńskich).

Co więc robić? Czy jest to ta chwila kiedy należy się poddać? Oczywiście nie. Jedną z lepszych metod 'wymyślania' bezpiecznych haseł jest stosowanie zasady wybierania pierwszych liter (lub innych znaków) z wyrazów określonej frazy. Weźmy chociażby zdanie:

"Nie trzeba 3 razy Wojtkowi powtarzać - zapamięta" i zbudujmy na tej bazie łańcuch znaków:

Nt3rWp-z

Oto mamy hasło bezpieczne, zapamiętywalne i już po kilku razach potrafimy je szybko wprowadzić z klawiatury (to też jest nie bez znaczenia).

Należy zwrócić uwagę, iż hasło jest tym trudniejsze do złamania im mniej przypomina cokolwiek człowiek ma w swym użytkowaniu. Mieszanie małych liter z dużymi (jeśli system rozróżnia małe i duże litery - jak np. Unix), wplatanie cyfr i znaków specjalnych jak na przykład !,$ i tym podobnych poprawia security systemu. Jednak jeśli znajdziemy na urządzeniu stojącym obok "świetne" hasło np. OKI320-ML (typ drukarki!) to już nie jest to bezpieczne hasło mimo, że spełnia reguły (litery przemieszane z cyframi i znakiem specjalnym).

Jak działa hacker?

Jeśli już pieczołowicie wybieramy i chronimy swe hasło to z pewnością w którymś momencie wyda nam się to wszystko przesadą. Chyba, że na własnej skórze przekonamy się, że komputerowi włamywacze są na świecie. Czasami bowiem hackerzy postrzegani są w kategoriach krasnoludków czy też ufo. Hacker w każdym razie to taki osobnik, który szuka słabego miejsca w systemie. Jeśli je znajdzie i włamie się do systemu może zrobić co zechce:

- poinformować administratora o wykrytej "dziurze" (jeśli jest gentelmenem włamywaczem),
- nic nie zrobi ("kolekcjoner kont" w czystej postaci lub "turysta"),
- spenetruje system i przywłaszczy sobie dane (szpieg?, hobbysta?),
- zniszczy system, zablokuje jego pracę (anarchista?, sabotażysta?, niedorajda?).

Tak czy inaczej jesteśmy wydani na pastwę intruza co bezwzględnie jest pogwałceniem naszego prawa do prywatności.

W jaki sposób włamywacz wnika do systemu komputerowego? Wystarczy jeśli trafi na użytkownika ze słabym lub źle przechowywanym hasłem. Jeśli na serwerze jest zarejestrowanych kilkudziesięciu użytkowników istnieje niestety bardzo duże prawdopodobieństwo, że ktoś używa zbyt prostego hasła (np. username: TADEUSZ, password: TADEK). Badania czynione przez analityków potwierdzają, że przynajmniej kilkanaście procent użytkowników używa haseł łatwych do odgadnięcia. Mając jedno konto "złamane" hacker *(cracker)* może pozostawić tzw. "konia trojańskiego" (którego gwoli ścisłości można wprowadzić do systemu nawet nie mając tam w ogóle żadnego konta), wirusa lub po prostu posłużyć się odpowiednim programem aby łamać kolejne konta. Następnie włamywacz uzyskuje coraz wyższe uprawnienia w systemie, może więc coraz głębiej penetrować zasoby i w rezultacie może wejść w posiadanie uprawnień administratora systemu (supervisor, root, system, itp). To oczywiście tylko jeden z możliwych scenariuszy. Z resztą nawet ten sam schemat różnie wygląda podczas "realizacji" w różnych systemach operacyjnych.

Nic więc dziwnego, że odpowiedzialny administrator systemu wymusza na użytkownikach stosowanie haseł o pewnej minimalnej ilości znaków np. ośmiu oraz wprowadza obowiązek zmiany hasła odpowiednio często. Hackerowi wystarcza bowiem często wykradzenie z systemu zbioru, gdzie przechowywane są dane i hasła użytkowników (są one zaszyfrowane przez jądro danego systemu - dobrze jeśli przy pomocy mocnych algorytmów (DES) a nie np. elektronicznej Enigmy -co się zdarza nawet do tej pory, z powodów, nazwijmy to politycznych. Wykradziony zbiór można już "spokojnie" łamać na innym komputerze (np. PC). Jeśli hasła są dłuższe łamanie trwa dłużej a jeśli są często przez użytkowników zmieniane - istnieje szansa, że złamane przez hackera hasło jest bezużyteczne.

Jeśli algorytmy szyfrujące zastosowane przez producenta są silne (jak np. DES) to łamanie w gruncie rzeczy polega na podjęciu wieluset tysięcy lub nawet milionów prób odgadnięcia hasła w oparciu o rozmaite słowniki i wariacje. Jeżeli w tym momencie oburzamy się na programy "crackerskie" to być może zdumiewającym wyda się fakt, że mogą one być pożyteczne. To przecież tylko narzędzie. Programy takie mogą być (i

stają się w wielu wypadkach) kontrolerem stopnia narażenia systemu na ataki wykorzystujące słabe hasła użytkowników.

Chcielibyśmy lecz boimy się...

Jeśli sieć lokalna jest włączona do sieci rozległej (np. Internet) potencjalne zagrożenia rosną. To często jest powodem rezygnowania z dołączania do większych organizmów. Traci się wtedy możliwość szybkiego skorzystania z dorobku światowej wiedzy otrzymując za to... dokładnie nic! Nic, bowiem jeśli ktoś zaniechał wprowadzenia mechanizmów bezpieczeństwa i kontroli tego co się w sieci dzieje gdyż nie planuje włączać się do np. Internetu to sieć nie staje się ani trochę bezpieczniejsza bowiem wystarczy jeden użytkownik, który dla własnej wygody "zmajstruje" dial-up'owe (komutowane) połączenie do swej sieci z zewnątrz i otrzymujemy sytuację kiedy sieć ma niekontrolowany "styk" ze światem zewnętrznym (hackerzy łatwo wychwytują numery telefonów, na które odpowiada modem i próbują wedrzeć się do systemu)

Ściany ogniowe (firewalls)

Część administratorów decyduje się na włączenie do Internetu za pomocą tzw. "firewalls" . Są to komputery, gateway'e, specjalnie skonfigurowane routery na styku sieci lokalnej i rozległej spełniające funkcje separujące lub filtrujące. Oczywiście tego typu zapory" podnoszą całkowity koszt instalacji. Zawsze jednak w końcowym efekcie to właściciel jest odpowiedzialny (bo stratny) za przedsięwzięcie odpowiednich kroków w celu ochrony swego systemu i danych. Ściany ogniowe stosują np. duże korporacje, które posiadają jeden jedyny styk swej wewnętrznej sieci z Internetem. Wtedy punkt ten staje się bastionem najbardziej narażonym na ataki a więc jest odpowiednio chroniony. Stosuje się metody filtracji adresów (tylko pakiety z określonych adresów), portów (tylko określone usługi np. poczta elektroniczna) lub całkowicie blokuje się bezpośredni ruch pomiędzy siecią wewnętrzną a światem na zewnątrz (pośredni host na styku).

Stopień tajności (poufności) informacji

Jak powiedzieliśmy to użytkownik (i tylko on) wie jaki jest ciężar gatunkowy wysyłanej informacji. Jeśli bowiem wysyłam w poczcie elektronicznej bardzo ważne sprawozdanie do centrali poprzez sieć jakiegoś operatora telekomunikacyjnego to osobiście kwalifikuje ją według znaczenia i jeśli trzeba - szyfruje ją. Nieporozumieniem jest obarczanie operatora "obowiązkiem" zapewnienia jakiejś szczególnej ochrony memu sprawozdaniu bo przecież tenże operator z zasady nie wie z jaką treścią ma do czynienia i nie ma prawa klasyfikować przesyłanych przez siebie treści. Operator działający na podstawie zezwolenia telekomunikacyjnego "z urzędu" zobowiązany jest do zapewnienia normalnej ochrony przesyłanym danym - i to operatorzy czynią. Operator przesyła informację "przeźroczyście" - taką jaka ona (ta informacja) jest i nie klasyfikuje jej w celu np. zapewnienia jakichś super środków. Jeśli z jakichś przyczyn operator "widzi" część danych użytkownika (np. w czasie monitorowania sieci dla celów diagnostycznych) jest zobowiązany do zachowania tajemnicy. Tu między innymi zaznacza się przewaga operatora telekomunikacyjnego posiadającego zezwolenie nad innymi organizacjami lub osobami, które oferują usługi wielodostępne, które to firmy właściwie nie są do niczego zobowiązane.

Operatorzy sieci nawet przy najlepszych chęciach nie są w stanie jednak zapewnić 100% ochrony przed włamywaczem czy podsłuchem. Przecież właściwie to rozumiemy skoro mówimy do słuchawki telefonu: to nie jest rozmowa na telefon. Mimo wszystko telefon pozostaje bardzo pożytecznym sposobem komunikowania się. Każdy też samodzielnie dokonuje wyboru kiedy pisać na kartkach pocztowych a kiedy stosować kopertę lub pocztę kurierską.

Jak już wspomniano we współczesnym świecie operatorzy nie stosują szyfrowania linii połączeniowych sieci a więc nie koduje się całego ruchu w sieci. Dane różnych użytkowników są w naturalny sposób wymieszane z powodu typu transmisji (np. datagramowa) jak też współbieżności (multipleksacja, tunelowanie). Użytkownicy natomiast w zależności od potrzeb stosują opisaną wyżej "end-to-end protection".

Szyfrować - ale jak?

Wybór odpowiedniego mechanizmu szyfrowania (sprzęt, oprogramowanie) to ważna domena należąca do użytkownika. I tu ostrożności nigdy nie za wiele. Zły szyfrator (łatwy do rozpracowania) wygląda tak samo

dobrze jak dobry szyfrator (zapewniający odpowiedni poziom bezpieczeństwa). Zły algorytm szyfrowania (łatwy do złamania) wygląda tak samo dobrze jak dobry (mocny). Stosując słaby lub nie znany (niejawny) algorytm jesteśmy w sytuacji jeszcze gorszej niż gdybyśmy nie stosowali żadnych mechanizmów security - mamy niezweryfikowane bezpieczeństwo (często jest ono pozorne). Współcześni specjaliści od kryptografii wyrażają zgodny pogląd, że siła określonego kryptosystemu nie leży w tajności algorytmu szyfrującego - ten może i nawet lepiej jeśli jest jawny - lecz w kluczach.

Klasyczny algorytm szyfrujący DES już od dwudziestu lat jest poddawany próbom łamania i z grubsza wiadomo jak go stosować aby bezpieczeństwo nie było jedynie ułudą... Z drugiej strony istnieje na rynku pakiet (i nie jest on nawet specjalnie drogi), który potrafi łamać algorytmy kryptograficzne wbudowane w takie popularne programy jak: WordPerfect, Lotus 1-2-3, MS Excel, Quattro Pro czy MS Word 2.0. Jest to przy tym autentyczne łamanie kryptograficzne a nie np. zgadywanie haseł. Niektórzy stosują to kiedy zapomną swych haseł... Inni zaś - wiadomo. Nie jest to więc wszystko takie proste i czasami rzeczywiście obcujemy z pewną iluzją miast rzeczywistym bezpieczeństwem. Istotna jest jak widzimy świadomość "siły" naszych zabezpieczeń w stosunku do wartości jaką przedstawiają dla nas określone zasoby i wartości jaką mogą one przedstawiać dla potencjalnego włamywacza. I nie ma tu specjalnie znaczenia czy w określonym środowisku "widuje" się włamywaczy czy jest to raczej "bezpieczna okolica" - ważne jest czy chronimy "maluchy" czy "mercedesy", z tego bowiem wyniknie potencjalne zagrożenie i nasza akcja w postaci odpowiedniego systemu zabezpieczeń.

Klucze

Skoro już wybraliśmy sprawdzony algorytm kryptograficzny to jak się rzekło istotne są klucze a dokładniej ich przechowywanie i dystrybucja. Klucze można głęboko schować ale najpierw trzeba je jakoś dostarczyć do partnera. W drodze będą oczywiście narażone na "podpatrzenie" więc trzeba zastosować pewny środek transportu (kurier z zalakowaną kopertą?). Aby było bezpiecznie należy klucze co jakiś czas zmieniać i znowu je przewozić... Dystrybucja kluczy może stać się uciążliwa a wtedy zastosujemy pewnie jakieś "usprawnienia", które ujemnie wpłyną na bezpieczeństwo. W konwencjonalnym systemie szyfrowania/deszyfracji nadawca i odbiorca posługują się tym samym kluczem a więc powstają wyżej wzmiankowane problemy związane z ich dystrybucją. W systemach klucza publicznego, gdzie jeden użytkownik posiada parę kluczy: tajny i publiczny jest możliwe bezpieczne szyfrowanie w oparciu o zasadę, że np. użytkownik A zaszyfrował coś przy pomocy klucza publicznego B a użytkownik B odszyfrował to coś przy pomocy sobie jedynie znanego swego klucza tajnego." B" może bez obaw udostępnić swój klucz publiczny innym użytkownikom aby móc z nimi korespondować i niepotrzebne jest każdorazowe przewożenie czy przesyłanie sekretnych kluczy. Tu pojawia się wprawdzie problem Urzędu d/s Certyfikatów czyli organizacji, która "głową" odpowiada za to, że klucz publiczny B w rzeczywistości należy do B a nie do innego użytkownika, który się jedynie pod B podszył ale to w każdym razie daje się zorganizować. W najgorszym przypadku można swój klucz publiczny osobiście rozdać (w zasadzie "raz na zawsze") swoim respondentom. Aby jeszcze sprawę "zagmatwać" czyli usprawnić współczesne systemy kryptograficzne posługują się kombinowaną formą:

- algorytmy symetryczne (klasyczne np. DES) do szyfrowania wiadomości,
- algorytmy klucza publicznego (np. RSA) do podpisywania wiadomości tak aby nie można było jej zmienić i aby była pewność nadawcy i odbiorcy oraz do przesyłania kluczy dla algorytmu klasycznego.

Tak więc w takim przypadku odpada uciążliwość dystrybucji kluczy dla "klasycznej" części systemu bowiem zapewnia to algorytm niesymetryczny (klucza publicznego). Na świecie w wielu krajach systemy takie są stosowane i to nie tylko w organizacjach typu banki czy instytucje wojskowe lub rządowe - również w sieciach o szerokim "publicznym" czy akademickim charakterze istnieją udane implementacje bezpiecznej poczty elektronicznej.

Bezpieczeństwo w sieci NASK

W sieci NASK można spotkać większość mechanizmów zaprezentowanych w niniejszym referacie. Przyjmuje się przy tym zasadę, że jeśli chodzi o bezpieczeństwo sieci to bardziej należy je stosować niż o nim opowiadać. NASK jest siecią szkieletową, której zrąb w obecnym kształcie stanowi sieć routerów rozlokowanych w węzłach w całej Polsce. Routery pozwalają na stosowanie w zasadzie dowolnej filtracji pakietów, portów (usług), protokołów. Są chronione dwupoziomowym systemem haseł a dodatkowo zastosowano system autoryzacji TACACS. System centralnego managementu zaimplementowany na dedykowanym ser-

werze wykrywa wszelkie nieprawidłowości w działaniu sieci. Istnieje możliwość definiowania sytuacji alarmowych, o których system automatycznie informuje administratora.

Na styku z routerami użytkowników w sieci NASK jest stosowany protokół routingu OSPF pozwalający na wymianę kluczy autoryzacyjnych pomiędzy routerami.

W sieci NASK występują oczywiście również serwery. We wszystkich serwerach w węzłach regionalnych serwery te mają zabezpieczenia zgodne z poziomem C2. Administratorzy serwerów dla użytkowników mają do dyspozycji całą gamę narzędzi czuwających nad bezpieczeństwem powierzonych danych (programy wspomagające pracę administratora, możliwość działań kontrolnych zmuszających użytkownika do odpowiedniego stosowania haseł, archiwizacja danych, itp).

Sieć X.25 NASK jest również zarządzana centralnie. Dostęp do konfiguracji w węzłach X.25 jest chroniony na kilka sposobów. Hasła są przechowywane w pancernej szafie.

Sprzęt stosowany przy budowie sieci szkieletowej odznacza się dużą niezawodnością pracy. W niedalekiej przyszłości w sieci NASK wejdą protokoły frame relay i ATM jeszcze bardziej ograniczające możliwość podsłuchu.

Bezpieczeństwem w NASK zajmuje się osobny zakład powołany do tego celu. Wypracowywana strategia bezpieczeństwa jest dokumentowana. Dużą wagę położono na stworzenie odpowiednich regulaminów dla operatorów określających czynności w stanie normalnego działania sieci (np. backup-y) oraz w razie wystąpienia sytuacji alarmowych. Szczególny nacisk kładzie się także na ochronę węzła centralnego NASK - zarówno fizyczną (dostęp do pomieszczeń) jak też techniczną.

W "centrali" NASK działa sieć Banyan Vines, której zalety pod względem security zostały już opisane wyżej. Również same stacje robocze PC podlegają zróżnicowanej ochronie.

Dla komunikacji wewnętrznej wprowadza się system bezpiecznej poczty elektronicznej w oparciu o pakiet HEART stworzony na Politechnice Warszawskiej. Pakiet ten zapewnia przy zastosowaniu 64 bitowego algorytmu DES i 512 -bitowego algorytmu RSA szyfrowanie i dystrybucję kluczy szyfrujących a także podpis elektroniczny. Jest to zresztą często używany na świecie tandem: DES - do szyfrowania i RSA - do obsługi kluczy szyfrujących w systemie kluczy publicznych. Heart umożliwia też dołączanie innych algorytmów kryptograficznych. Zapewnia jak już wspomnieliśmy stosowanie podpisu elektronicznego (cyfrowego) oraz wykorzystuje kilka algorytmów silnych funkcji kompresji danych *(hash function)* służące do obliczania skrótów wiadomości. Po zalogowaniu się odpowiednie pliki z kluczami dla kryptosystemu RSA zostają wczytane np. z dyskietki lub lokalnego dysku twardego. Użytkownik może następnie wysłać lub odebrać wiadomość. Dla potrzeb wysyłania wiadomości system generuje jednorazowe klucze dla kryptosystemu DES. System przewiduje również ustanowienie urzędu d/s certyfikatów - rolę te de facto pełni wydzielony komputer.

Dla użytkowników zewnętrznych istnieje możliwość konsultacji i pomocy w dobraniu takich czy innych narzędzi (np. public domain lub firmowych) spełniających wymagania użytkownika w określonym zakresie.

Rady praktyczne

Istnieje wiele kroków które ludzie odpowiedzialni za "network security" mogą zrobić dziś, zaraz - niewielkim kosztem w celu podniesienia bezpieczeństwa systemów sieciowych. Powróćmy więc do początku i przypomnijmy, że największym zagrożeniem są luki w organizacji systemu rozumianego jako jeden organizm: sprzęt plus obsługa i legalni użytkownicy. Wystarczy zwrócić uwagę na problem dostępności pomieszczeń dla osób postronnych, uświadomić administratorom systemów ich odpowiedzialność za utrzymanie szczelnego systemu, forsować wśród użytkowników nawyki do stosowania haseł trudnych do odgadnięcia.

Przy wyborze systemu operacyjnego naszego komputera warto dowiedzieć się jakim poziomem security może się ów wylegitymować - nie warto w zasadzie angażować się w coś o poziomie poniżej C2. Czasem jest możliwy upgrade naszego "starego" systemu do C2 - rozsądnie jest szukać takiej możliwości.

W kontekście topologii sieci gorsze pod względem bezpieczeństwa są układy magistralowe, gdzie każdy pakiet może być praktycznie "podsłuchany" przez każdego. Należy stosować metody separowania segmentów sieci lub przechodzić na połączenia typu gwiazda.

Nowoczesne metody transmisji danych takie jak Frame Relay lub ATM są z samej zasady dość odporne na ataki pasywne (podsłuchanie). Czasem można mieć wyższe security niejako "przy okazji": linie multipleksowane są trudniejsze do podsłuchania.

Tam gdzie zachodzi potrzeba pewnego, potwierdzonego przesłania należy implementować mechanizmy poświadczania, szyfrowania, podpisu elektronicznego.

Wśród koniecznych zasad jakimi powinni się kierować twórcy lokalnych systemów bezpieczeństwa należy wymienić:

- stworzenie, opublikowanie i wdrożenie udokumentowanej polityki bezpieczeństwa, która winna odpowiedzieć na szereg kardynalnych pytań w rodzaju:
  * jakie są funkcjonalne wymagania sieci?
  * co w sieci musi być chronione, jak bezpieczne powinny być poszczególne elementy sieci?
  * jak będą wyglądały procedury raportowania incydentów i jakie pociągną reakcje,
  * jakie są uwarunkowania prawne,
  * co wolno użytkownikom i administratorom (jakie narzędzia security mogą stosować),
  * w jaki sposób można pokusić się o zweryfikowanie zastosowanych rozwiązań,
- obowiązujące procedury muszą być proste i zrozumiałe,
- należy zagwarantować wsparcie techniczne dla realizacji procedur,
- proste administrowanie bezpieczeństwem jest istotą powodzenia systemu,
- konieczne jest ścisłe zdefiniowanie zakresów odpowiedzialności,
- muszą zostać ustalone procedury administracyjne systemu bezpieczeństwa,
- system nie może być zbyt uciążliwy bo użytkownicy zaczną go obchodzić,
- użytkownicy powinni być przyzwyczajani możliwie wcześnie do stosowania zasad bezpieczeństwa; konieczne stałe szkolenia,
- o bezpieczeństwie systemu decyduje jego najsłabszy punkt.

Laboratorium utrzymania sieci komputerowych Politechniki Wrocławskiej

Daniel J. Bem*) , Marcin Głowacki) , Waldemar E. Grzebyk*)**

1. Wprowadzenie

Zasadniczym problemem utrzymania sieci komputerowych jest jednolitość oraz rekomendacje stosowanego sprzętu sieciowego. Istotnym elementem utrzymania sieci komputerowych jest również ich administrowanie. Nabywcy oraz dystrybutorzy sprzętu komputerowego zauważają te problemy i dostosowują oferowany sprzęt do wymogów istniejących standardów. Badania zgodności produktów informatycznych i telekomunikacyjnych dają zaufanie do ich poprawnego działania. W wielu przypadkach wymagana jest weryfikacja sprzętu, przeprowadzona przez akredytowane laboratorium. Pozytywny wynik badań jest warunkiem stosowania urządzenia i oprogramowania w sieciach rzeczywistych.

Jednym z podstawowych warunków koniecznych do prawidłowego wykorzystania sieci komputerowych jest poprawne funkcjonowanie sieci transmisji danych. Funkcjonowanie to jest sprawdzalne obiektywnie za pomocą odpowiednich pomiarów oraz monitorowania pracy sieci. Istnieją zalecenia i standardy międzynarodowe, które określają jakie parametry jakości usług (ang. Quality of Service - QOS) muszą być spełnione, aby można było określić sieć transmisji danych jako funkcjonującą poprawnie.

Laboratorium Utrzymania Sieci Komputerowych Politechniki Wrocławskiej wykonuje badania tego typu. Jest ono wyposażone w odpowiednie urządzenia pomiarowe i dysponuje wykwalifikowaną kadrą oraz dysponuje oprogramowaniem potrzebnymdo administrowania i zarządzania sieciami. W artykule przedstawiono obecną strukturę Laboratorium Utrzymania Sieci Komputerowych (LUSK) oraz zakres prowadzonych przezeń prac.

2. Zasady funkcjonowania Laboratorium

Laboratorium Utrzymania Sieci Komputerowych powstało na początku 1992 roku Powstanie laboratorium i jego ciągły rozwój jest podyktowany rozwojem sieci komputerowych w środowisku akademickim oraz prywatnych i publicznych sieci transmisji danych. Przykładem są funkcjonujące w Polsce od kilku lat Naukowa i Akademicka Sieć Komputerowa (NASK), publiczna komputerowa sieć pakietowa - POLPAK, sieć kolejowa - KOLPAK, sieć bankowa - TELBANK. W okresie ostatnich dwóch lat w ośrodkach akademickich zaczęły także powstawać sieci metropolitalne.

Część pomiarowa LUSK jest zorganizowana według wzorców zachodnioeuropejskich. Podstawą jej funkcjonowania jest standard EWG - EN45XXX. Wyposażenie Laboratorium umożliwia przeprowadzanie większości pomiarów zgodnie z zaleceniami CCITT***) oraz standardami międzynarodowymi ISO.

Nie ulega wątpliwości, że pomyślne przejście badań w laboratorium przez produkt i uzyskanie certyfikatu stanowi istotny czynnik marketingowy dla tego produktu. Tak więc klientelę laboratorium stanowią wytwórcy oraz dostawcy produktów informatycznych i telekomunikacyjnych .

Inną kategorię klientów stanowią dostawcy usług sieciowych, potrzebujący poświadczeń zgodności dla implementacji usługi w sieci. Poświadczenie takie jest wymagane również w przypadku wejścia z usługą w inne sieci lub prywatne systemy końcowe.

Potencjalne problemy z uzyskaniem zgodności ze standardami są identyfikowane wcześniej w cyklu opracowywania produktu, umożliwiając oszczędności na kosztach późniejszych koniecznych adaptacji. Dobre oprogramowanie testujące umożliwia też precyzyjne określenie powodu niezgodności i sposobu jej korekcji. Poza tym włączenie do sieci produktów przebadanych na zgodność znacznie ułatwia uruchamianie ich w sieci.

Badania zgodności dotyczą nie tylko produktów gotowych. Mogą one dostarczyć wsparcia już na etapie projektowania, a także dalszej fazy rozwojowej produktu. Monitorowanie działania produktu w czasie rzeczywistym umożliwia wykrycie błędów będących wynikiem niezgodności dynamicznej, czy błędnej interpretacji zaleceń.

---

* Naukowa i Akademicka Sieć Komputerowa
** Instytut Telekomunikacji i Akustyki Politechniki Wrocławskiej
*** Obecnie

Uzgodnione w skali międzynarodowej testy umożliwiają uniknięcie konieczności opracowywania własnych metod testowania. Umożliwiają uniknięcie indywidualnej interpretacji standardów i wyników badań. Powodują więc zmniejszenie wydatków związanych z uruchomieniem nowego produktu, a jednocześnie skracają okres jego projektowania i rozwoju.

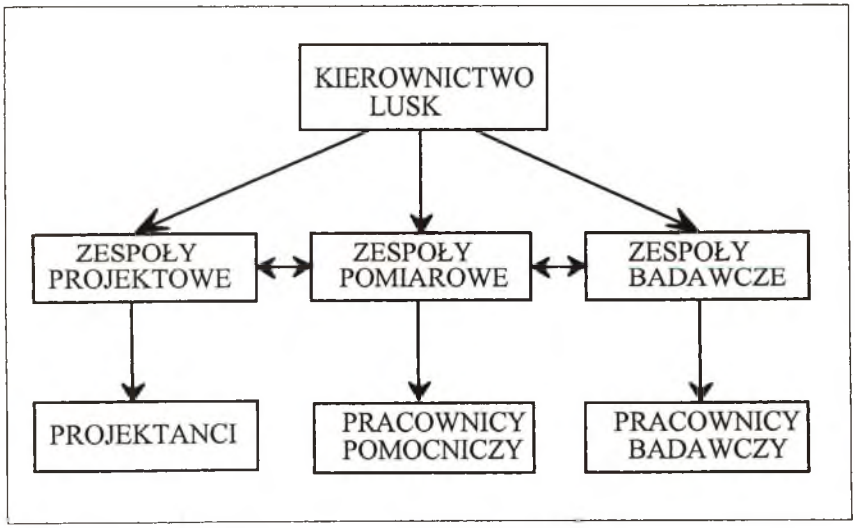
Jeżeli procedury i oprogramowanie testujące, stosowane przez różne laboratoria, są wzajemnie zharmonizowane, także w skali międzynarodowej, to protokoły badań i certyfikaty (świadectwa zgodności) są wzajemnie uznawane we wszystkich krajach, co eliminuje koszt poddawania produktu wielokrotnym badaniom na różnych rynkach. Harmonizacja taka jest zresztą bezpośrednio zawarta w idei standardów.

ECITTC (European Committee for I-T Testing and Certification) sformułował kryteria dla wzajemnego uznawania raportów i protokołów z testów OSI. Są one zebrane w dokumencie ECITC N-120 i obejmują zarówno sprawy organizacyjne, jak i techniczne. Sprawy techniczne obejmują dostępność specyfikacji, środki testowe (urządzenia i zestawy testów) oraz wymóg uzyskania akredytacji zgodnie z EN 45XXX. Sprawy organizacyjne dotyczą równoprawnych i zrównoważonych rozwiązań dla osiągnięcia wzajemnego uznawania.

Wyboru lokalizacji Laboratorium dokonano kierując się zaleceniami norm EWG-EN45XXX, które podkreślają niezależność organizacyjną i funkcjonalną laboratorium od innych jednostek organizacyjnych.

2.1. Struktura organizacyjna LUSK

Laboratorium nie zatrudnia pracowników etatowych. Do realizacji określonych prac powoływane są odpowiednie zespoły robocze. Pracownicy realizujący prace w ramach LUSK posiadają niezbędne wykształcenie, przeszkolenie, wiedzę techniczną i doświadczenie.



Rys.1 *Struktura organizacyjna LUSK*

Personel laboratorium pracujący w ramach zespołów roboczych można podzielić na cztery grupy:

- kierownictwo laboratorium,
- pracowników badawczych,
- pracowników pomocniczych,
- projektantów.

Dobiegają końca starania o uzyskanie akredytacji krajowej wydawanej przez Centrum Przeprowadzania Badań i Akredytacji. W tym celu została stworzona Księga Jakości.

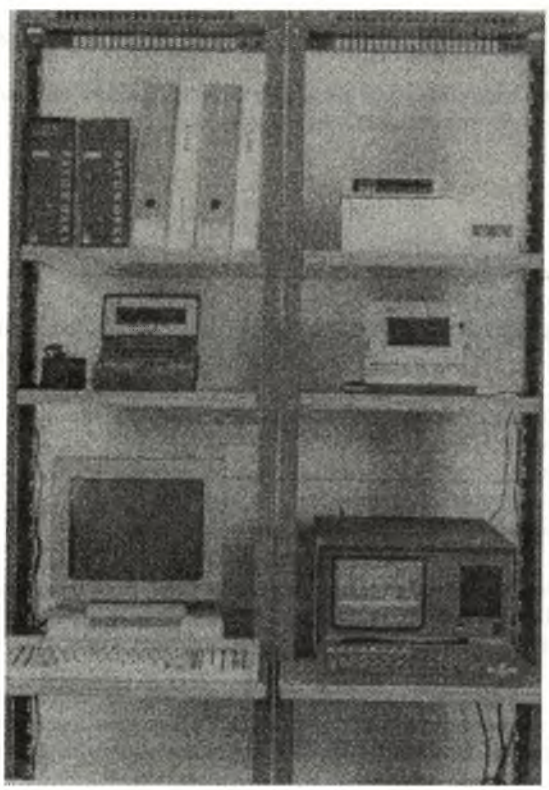
Jest to opracowanie, w którym zawarty jest dokładny opis procedur testowania oraz weryfikacji, a także zasad współpracy z klientami laboratorium.

3. Wyposażenie laboratorium

Laboratorium jest wyposażone w nowoczesną aparaturę diagnostyczno-pomiarową umożliwiającą prowadzenie badań i testowanie urządzeń zgodnie z zaleceniami międzynarodowymi:

1. Data Analyser DA-15 firmy Wandel & Goltermann
2. Data Line Analyser DLA-5A firmy Wandel & Goltermann
3. Data Tester DT-10 firmy Wandel & Goltermann
4. HP Lan Probe System firmy Hewlett Packard, - umożliwia monitorowanie oraz diagnostykę segmentu sieci pracującej w standardzie Ethernet,
5. Miernik stopy błędu TREND 1-4 - przyrząd umożliwia pomiary elementowej stopy błędu i zniekształceń telegraficznych w układzie "pętla".
6. Miernik mocy optycznej K 2401 firmy SIEMENS.
7. Miernik przerw i zakłóceń MPZ-4.. Miernik tłumienności światłowodów OPM-11 firmy PRÄCITRONIC - umożliwia pomiary tłumienności światłowodów do długości fali = 0.85 mm.
8. Protocol Tester Siemens K 1195 z oprogramowaniem "NET2" - umożliwia przeprowadzenie badań homologacyjnych na zgodność z protokołem X.25,
9. Zestaw do pomiaru tłumienności światłowodów K 1186 firmy SIEMENS.
10. Zestaw pomiarowy (nadajnik i odbiornik) do analizy danych TREND 1A - zestaw umożliwia pomiary stopy błędu i zniekształceń telegraficznych dla telegrafii - praca wartością i kierunkiem prądu.
11. Zestaw pomiarowy do pomiaru zniekształceń tłumieniowych i opóźnieniowych LD-3 firmy Wandel & Goltermann.

W pomieszczeniach laboratorium zainstalowano następujący sprzęt komputerowy:



- μVAX 3100 - gateway do sieci POLPAK
- PC AT-386/40 wyposażony w kartę sieciową X.25 i oprogramowanie X.29 PAD,
- komputer SUN SPARCstation IPX wraz z oprogramowaniem "CISCO Works", umożliwiającym administrowanie i kontrolę pracy sieci,
- ruter AGS+ firmy CISCO stanowiącego jeden z węzłów światłowodowej sieci metropolitalnej WASK (Wrocławska Akademicka Sieć Komputerowa),
- terminal sieci VSAT systemu SPACE-NET przeznaczony do badań nad wykorzystaniem go w sieciach lokalnych, i rozległych.

Rys.2. Stanowisko pomiarowo-diagnostyczne:

- łączy komunikacji danych z wykorzystaniem Data Tester DT-10 i Data Analyser DA-15

- łączy z komutacją pakietów z wykorzystaniem Protocol Testera SIEMENS K1195 z oprogramowaniem "NET2"

3. Zakres usług świadczonych przez LUSK

Laboratorium Utrzymania Sieci Komputerowych świadczy następujące usługi:

W zakresie pomiarowym:

1) pomiary urządzeń sieci transmisji danych (DCE) oraz urządzeń końcowych użytkownika (DTE) w zakresie zgodności z zaleceniami CCITT oraz ISO,
2) pomiary i ocena linii transmisji danych oraz interfejsów sieciowych warstwy fizycznej,
3) testowanie i ocena urządzeń sieciowych,
4) pomiary parametrów jakości usług sieciowych QOS (Quality of Service).

Pomiary mogą obejmować:

- sieci nowo zbudowane lub będące w stanie rozruchu,
- okresowe pomiary sieci eksploatowanych,
- pomiary w sytuacjach awaryjnych i poawaryjnych,
- sieci (lub ich fragmenty) prywatne i publiczne.

Wykonywanie zleconych pomiarów może odbywać się u użytkownika lub zdalnie z pomieszczeń LUSK (gdy jest to możliwe). Łącznie z pomiarami prowadzana jest diagnostyka, zmierzająca do identyfikacji przyczyn niesprawności lub niezgodności sieci transmisji danych z wymaganiami.

W zakresie projektowym:

1) projekty i nadzór nad wykonawstwem infrastruktury telekomunikacyjnej sieci lokalnych - LAN (Local Area Network), sieci metropolitalnych - MAN (Metropolitan Area Network), sieci rozległych - WAN (Wide Area Network),
2) projekty topologii, wybór sprzętu i uruchomienie sieci LAN, MAN i WAN,
3) konsultacje i doradztwo techniczne przy projektowaniu i budowie sieci LAN.

W zakresie administrowania sieciami:

1) monitorowanie pracy sieci LAN, MAN i WAN,
2) sterowanie działaniem wszystkich urządzeń w sieci LAN, MAN lub WAN pracujących z protokołem SNMP (Simple Network Management Protocol),
3) tworzenie, edytowanie, uaktywnianie zbiorów konfiguracyjnych ruterów, a także reagowanie na zdarzenia, które wystąpiły w sieci, takie jak awarie czy zbytnie obciążenie segmentów sieci.

4. Zakres pomiarów

Zakres pomiarów i testów wykonywanych przez LUSK obejmuje:

1. pomiary i testowanie podsieci transmisji danych (DCE):
   - pomiary podstawowych parametrów linii transmisji danych,
   - testowanie funkcjonalne podsieci transmisji danych na zgodność ze standardami międzynarodowymi,
   - pomiary ogólnych parametrów jakości QOS podsieci transmisji danych na zgodność z zaleceniami CCITT,
   - testowanie funkcjonalne podsieci transmisji danych na zgodność ze standardami firmowymi.
2. testowanie funkcjonalne urządzeń końcowych sieci (DTE):
   - na zgodność ze standardami międzynarodowymi w zakresie procedur komunikacyjnych,
   - na zgodność ze standardami międzynarodowymi w zakresie procedur aplikacyjnych,
3. pomiary specjalistyczne na zamówienie użytkowników.

Można prowadzić dwa rodzaje testowania:

a) **monitorowanie** - polegające na tym, że aparatura pomiarowa jest podłączona do linii transmisji danych, łączącej dwa urządzenia sieci komputerowej (np. DTE-DCE, DCE-DCE, DTE-DTE); umożliwia ono obserwację oraz rejestrację wymienianej pomiędzy urządzeniami informacji, bez oddziaływania na tę wymianę,
b) **emulacja** - polegającą na tym, że aparatura pomiarowa funkcjonalnie zachowuje się we współpracy z urządzeniem testowanym tak, jak urządzenie sieci komputerowej (DTE lub DCE); umożliwia ona obserwację oraz rejestrację reakcji testowanego urządzenia, na standardowe akcje generowane przez aparaturę pomiarową.

Ogólna metodologia testowania wszystkich warstw modelu jest zgodna ze standardami ISO 9646/1-5 *(Conformance Testing Methodology and Framework).* Ustalanie parametrów testowania poszczególnych warstw odbywa się w oparciu o dokumenty (odrębne dla każdej warstwy) określające stany zgodności implementacji protokołu *(ang. Protocol Implementation Conformance Statement - PICS).*

4.1. Pomiary właściwości fizycznych łączy w sieci transmisji danych

Pomiary w sieci transmisji danych mają za zadanie ocenę jakości tej sieci oraz jej elementów. Aby ocenić stan techniczny sieci muszą zostać poddane pomiarom procesy zachodzące w jej wnętrzu. Pomiary te najogólniej można podzielić na dwie grupy:

- pomiary typu homologacyjnego,
- pomiary typu utrzymaniowego.

Pomiary pierwszej grupy dotyczą zgodności parametrów urządzeń przewidzianych do stosowania w sieciach komputerowych z odpowiednimi standardami, wymaganymi przez te sieci zarówno od strony elektrycznej, jak i funkcjonalnej (protokoły). Badania te mają na celu wydanie odpowiednich certyfikatów zgodności dla producentów i dostawców sprzętu stosowanego w tych sieciach. Pomiary typu utrzymaniowego mają na celu bieżącą kontrolę parametrów technicznych sieci i ogólnie pojętą diagnostykę sieci.

Zadania pomiarowe są określone przez możliwości ich wykonania. Stąd zasadnicze znaczenie w procesie pomiarowym w sieci takich czynników jak:

- styki,
- protokoły komunikacyjne.

Normowanie przez CCITT (zalecenia serii V i X) obejmuje najważniejsze rodzaje styków i ich właściwości (np. V.24, V.35, V.36. X.20, X.21). Obok zaleceń CCITT spotyka się tu także inne, np. IEEE. Do najczęściej spotykanych protokołów można zaliczyć przykładowo:

- BSC (znakowo zorientowany) wprowadzony przez IBM,
- HDLC (bitowo zorientowany, w wersjach -NRM i -ABM),
- SDLC.

Stosowanie tych protokołów ma miejsce w różnych przypadkach, odpowiednio do ich właściwości (np. BSC - przy transmisji półdupleksowej).

Dysponowanie dokumentacją pomiarową sieci transmisji danych usprawnia bieżącą eksploatację łączy, ułatwia określenie i lokalizację występujących ewentualnie nieprawidłowości w transmisji. Ponadto usprawnia wszelkiego rodzaju odbiory itp. czynności, ponieważ pomiary są wykonywane zgodnie z odpowiednimi zaleceniami CCITT. Zalecenia te precyzują sposób przeprowadzania pomiarów i określają dopuszczalne tolerancje wartości mierzonych parametrów (odpowiednie zalecenia podano przy omawianiu poszczególnych pomiarów).

Oferta Laboratorium dotyczy w głównej mierze pomiarów z warstw 1-3 modelu OSI. W szczególności zakres proponowanych pomiarów obejmuje np. zniekształcenia tłumieniowe i opóźnieniowe, zakłócenia (o charakterze szumowym i impulsowym), rejestrację wszelkiego rodzaju zjawisk losowych itp.

4.2. Pomiary parametrów jakości usług sieciowych (QOS)

Zalecenie CCITT X.140 określa zbiór ogólnych parametrów jakości usług sieciowych (QOS) dla publicznych sieci cyfrowych. Parametry QOS charakteryzują się one dwoma podstawowymi cechami:

1) skupiają się na skutkach wydajności działania sieci, które są zauważalne na jej interfejsach; nie zajmują się ich przyczynami wewnątrz samej sieci.;
2) definicje parametrów QOS opierają się o zdarzenia niezależne od typu protokołu.

Walory te sprawiają, że parametry QOS stają się niezależne od oprogramowania użytkownika, rodzaju sieci oraz typu usług. Ich ogólne definicje umożliwiają ich użycie do określania jakości usług dowolnej sieci transmisji danych. W każdym z przypadków niezbędne jest rozszerzenie definicji uwzględniające charakterystykę działania danego protokołu komunikacyjnego. Parametry QOS mogą być zastosowane w odniesieniu do sieci pracujących zarówno z komutacją pakietów, jak i z komutacją kanałów, a także sieci opartych o łącza dzierżawione. Mogą być stosowane do trybów komunikacji połączeniowej i bezpołączeniowej. Parametry QOS są doskonałym narzędziem dla określania przez użytkowników partykularnych potrzeb i wymagań oraz jednocześnie stanowią sposób reprezentacji jakości proponowanych usług przez operatorów poszczególnych sieci. Istnieje zatem "wspólny język", do porozumiewania się obu zainteresowanych stron.

Parametry QOS zostały głównie stworzone z myślą o badaniu jakości styku urządzeń końcowych użytkownika (DTE) z publicznymi sieciami transmisji danych. Szczegółowe charakterystyki takiego typu styku zależą od typu usług sieciowych oraz aplikacji użytkownika.

Definicje parametrów ogólnych QOS opierają się na zdarzeniach niezależnych od typu protokołu, a zatem mogą z powodzeniem być użyte do określania jakości usług na wyższych warstwach modelu OSI.

Ze względu na fakt, że krajowe rozległe sieci komputerowe (TELBANK, KOLPAK, NASK i in.) oraz publiczne sieci transmisji danych (POLPAK) działają w oparciu o technikę komutacji pakietów zgodnie z zaleceniami X.25 i X.75, LUSK skoncentrowało się na pomiarach parametrów QOS tego rodzaju sieci.

Wyposażenie LUSK umożliwia prowadzenie pomiarów parametrów QOS. Oprócz Analizatora Protokołów K1195C firmy Siemens, LUSK jest wyposażony w komputer μVax 3100 z w pełni programowalnym interfejsem X.25. W laboratorium prowadzi się zaawansowane prace nad opracowaniem metodologii pomiarów parametrów QOS usług komutacji pakietów.

4.3. Testowanie urządzeń sieciowych DTE na zgodność ze standardem X.25

Zestaw procedur testujących NET 2 określa wymagania i opisuje testy interfejsów sieciowych. Dotyczą one urządzeń DTE pracujących w technologii pakietowej oraz styków z dedykowanymi łączami w sieciach z komutacją pakietów działających według zaleceń CCITT X.25.

Laboratorium Utrzymania Sieci Komputerowych jest wyposażone w analizator protokołów PROTOCOL TESTER K1195C firmy SIEMENS. Zakupiono u producenta pakiet oprogramowania umożliwiający przeprowadzenie kompletu testów NET 2 na urządzeniach końcowych DTE oraz DCE pracujących według zaleceń CCITT X.25 (1984).

W Laboratorium przeprowadza się testy urządzeń wyposażonych w karty sieciowe i interfejsy X.25 wraz z kompletem oprogramowania.

Sporządzane są raporty, które rozstrzygają zgodność urządzeń z zaleceniami i mogą stanowić podstawę do wydania certyfikatu homologacyjnego. Formularz raportu jest sporządzony na podstawie zaleceń międzynarodowych ISO/IEC 9646-5 wyd.I (1991/07/15): *Information technology - Open Systems Interconnection - Conformance testing methodology and framework, Part 5; Requirements on test laboratories and clients for the conformance asessment process*.

5. Administrowanie sieciami

Sieć komputerowa zaczyna działać po zainstalowaniu i uruchomieniu urządzeń sieciowych. Aby sieć pracowała poprawnie i niezawodnie konieczne jest utrzymanie sieci polegające na jej zarządzaniu. Podmiotem, który zarządza siecią komputerową jest administrator lub tzw. operator. Niezawodność sieci polega na pracy urządzeń w ruchu ciągłym. Zadaniem operatora jest zatem szybkie reagowanie na sytuacje awaryjne oraz brak łączności. Ze względu na duże rozproszenie urządzeń w sieciach typu MAN i WAN stosuje się systemy centralnego zarządzania. Tworzone są centra zarządzania sieciami, gdzie gromadzi się odpowiedni sprzęt oraz oprogramowanie wspomagające.

Podstawowym zadaniem operatora sieci jest monitorowanie pracy urządzeń. Może ono odbywać się w sposób ciągły lub periodyczny . Informacje o błędnym działaniu sieci operator otrzymuje od systemu automatycznego raportowania sytuacji awaryjnych lub użytkowników.

Laboratorium Utrzymania Sieci Komputerowych jest wyposażone w wysokiej klasy oprogramowanie do zarządzania i monitorowania pracy sieci pod nazwą "Sun Network Manager" i "CISCO WORKS". Za pomocą tego oprogramowania administrator sieci może z jednego miejsca sterować działaniem wszystkich urządzeń w sieci, pracujących z protokołem SNMP (Simple Network Management Protocol). Może tworzyć, edytować, uaktywniać zbiory konfiguracyjne ruterów, a także reagować na zdarzenia, które wystąpiły w sieci, takie jak awarie lub zbytnie obciążenie segmentów sieci.

Zintegrowana z "CISCO WORKS" relacyjna baza danych "SYBASE" umożliwia zbieranie danych o pracy sieci i ich analizę, a poprzez planowanie topologii sieci, zarządzanie ruchem pakietów. Interfejs graficzny "Sun Network Manager" daje możliwość tworzenia wielobarwnych map zarządzanej sieci komputerowej, na których widoczne jest każde urządzenie sieciowe pracujące z protokołem SNMP. Mapa jest aktualizowana automatycznie. Przy pomocy różnych kolorów przedstawia się aktualny stan urządzeń pracujących w sieci.

Laboratorium Utrzymania Sieci Komputerowych spełnia obecnie funkcję administratora sieci WASK. W Laboratorium opracowuje się system awaryjnej sygnalizacji i sterowania metropolitalnej sieci komputerowej pracujący na niezależnych łączach.

6. Podsumowanie

Laboratorium Utrzymania Sieci Komputerowych Politechniki Wrocławskiej oferuje szeroki zakres usług diagnostyczno-pomiarowych oraz projektowych. W okresie ostatnich dwóch lat istnienia, Laboratorium wykonało szereg usług w zakresie pomiarowym, projektowym i administrowania siecią. Niektóre z ważniejszych przedsięwzięć zrealizowanych w ramach prac prowadzonych przez LUSK to:

- testowanie urządzeń sieciowych na zgodność ze standardem X.25,
- pomiary parametrów łączy transmisji danych,
- monitorowanie pracy urządzeń sieci pracującej z komutacją pakietów,
- testowanie terminala sieci VSAT pracującego jako getway do sieci lokalnej,
- projekt koncepcyjny i nadzór nad budową Uczelnianej Sieci komputerowej Politechniki Wrocawskiej,
- projekt koncepcyjny i nadzór nad wykonawstwem Wrocławskiej Akademickiej Sieci Komputerowej,
- projekt Koncepcyjny i nadzór nad budową sieci komputerowej Administracji Centralnej Politechniki Wrocawskiej.

Bibliografia

[1.] Daniel J. Bem - praca zbiorowa, *Laboratorium Utrzymania Sieci Komputerowych*, Raport I-28/S-011/94 Instytutu Telekomunikacji i Akustyki Politechniki Wrocławskiej

[2.] Marcin Głowacki, Waldemar E. Grzebyk, *Zarządzanie sieciami komputerowymi i badania zgodności produktów informatycznych i telekomunikacyjnych w Laboratorium Utrzymania Sieci Komputerowych Politechniki Wrocławskiej*, Ośrodek Wydawnictw Naukowych Poznań, 1994 r.

[3.] Daniel J. Bem - praca zbiorowa, *Projekt Miejskiej Sieci Komputerowej dla Wrocławskiego Środowiska Akademickiego i Naukowego*, Wrocław, lipiec 1992.

[4.] Daniel Minoli, *Telecommunications Technology Handbook*, Artech House, Inc 1991.

[5.] European Telecommunication Standard, *NET2*, First edition, CEPT Liaison Office, Bern 1988.

Zastosowanie systemów VSAT w naziemnych sieciach transmisji danych

Daniel J. Bem *) , Ryszard J. Zieliński **)

1. Wprowadzenie

Sieci satelitarne z terminalami wyposażonymi w małe anteny VSAT *(ang. Very Small Aperture Terminals)* znajdują coraz więcej zastosowań jako rozwiązania alternatywne do naziemnych systemów transmisji danych. Do głównych zalet systemów VSAT można zaliczyć łatwość instalacji, bardzo dużą elastyczność i rekonfigurowalność sieci oraz dużą niezawodność.

Sieci VSAT oferują podobną jakość transmisji jak sieci naziemne oraz zapewniają użytkownikowi dostęp do sieci poprzez najszerzej rozpowszechnione protokóły komunikacyjne. W Europie większość publicznych sieci transmisji danych zalicza się do sieci z komutacją pakietów stosujących protokół CCITT X.25. Jako przykład można wymienić sieć TRANSPAC we Francji, PSS w Wielkiej Brytanii, DATEX-P w Niemczech, DATANET-1 w Holandii, DATAPAK w Szwecji oraz POLPAK i NASK (jeden z protokółów stosowanych w tej sieci) w Polsce. W USA stosuje się protokóły synchroniczne, takie jak BISYNC *(ang. Binary Synchronous Communications)* oraz SDLC *(ang. Synchronous Data Link Control)*.

2. Architektura sieci VSAT

Większość sieci VSAT pracuje w oparciu o topologię gwiazdy (rys. 1). W tego typu architekturze wyróżnia się stację centralną *(ang. Hub station)* oraz wiele oddalonych od siebie stacji tzw. terminali VSAT.

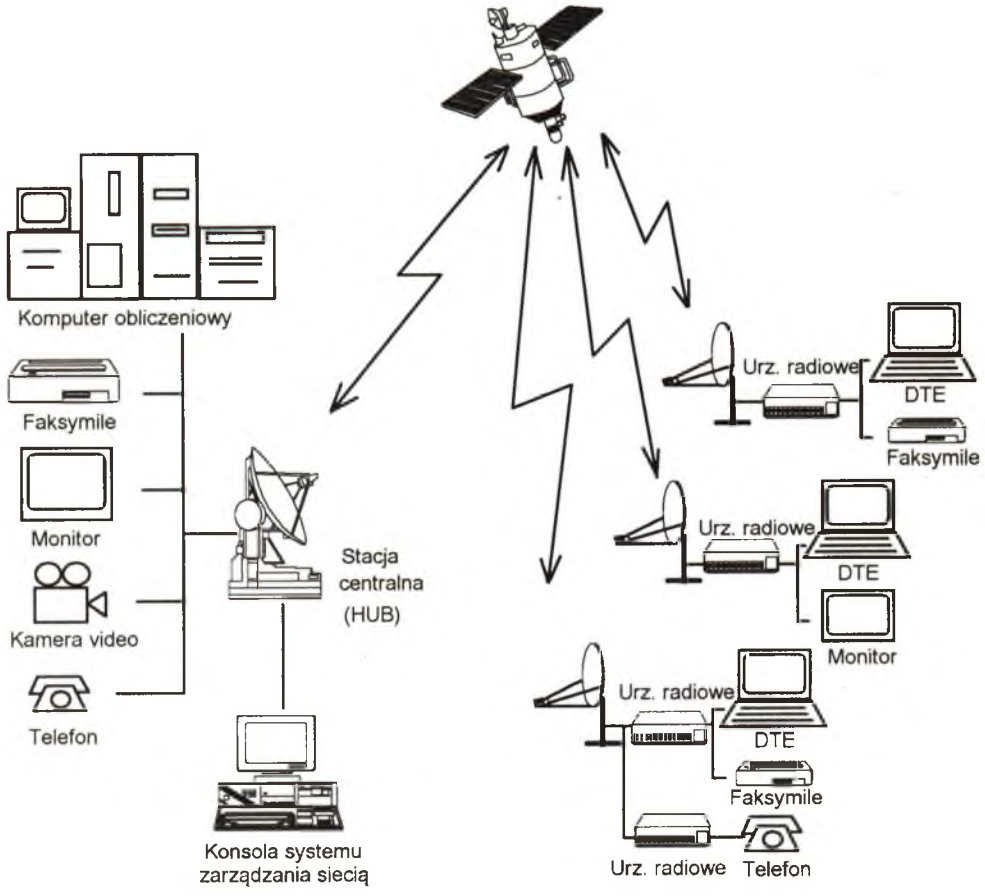
Typowy naziemny terminal VSAT składa się z dwóch części: zewnętrznej *(ang. outdoor unit)*, obejmującej antenę i część radiową oraz wewnętrznej *(ang. indoor unit)*. Schemat blokowy terminala nadawczo-odbiorczego przedstawia rys. 2. W odróżnieniu od stacji centralnej HUB, której koszt zawiera się w przedziale 300 000 do 5 000 000 USD, zwykły terminal jest znacznie tańszy (ok. 12 000 USD). Jest on wyposażony w antenę o niewielkiej średnicy i nadajnik małej mocy. Każdy terminal dupleksowy ma dwa odrębne tory sygnałowe: nadawczy i odbiorczy, pracujące na różnych częstotliwościach i przełączane przez przetwornik ortomodalny OMT *(ang. Orthogonal Mode Transducer)*. Poprzez odpowiedni dobór średnicy anteny i parametrów promiennika, dąży się do uzyskania wąskiej, głównej wiązki promieniowania i małego poziomu listków bocznych, tak aby nie zakłócać pracy sąsiednich stacji.

Przedstawione na schemacie elementy to:

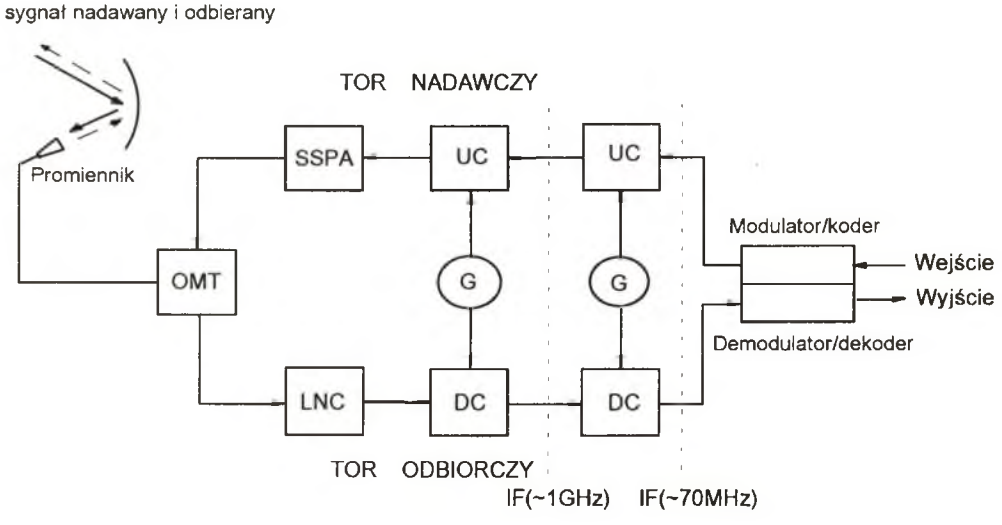
- przetwornik ortomodalny OMT przełączający tory sygnałowe *(ang. Orthogonal Mode Transducer)*;
- wzmacniacz mocy SSPA *(ang. Solid State Power Amplifier)* o mocy wyjściowej sięgającej 50 W w pasmie C i 20 W w pasmie Ku;
- konwerter niskoszumowy LNC *(ang. Low Noise Converter)* pełniący podwójną funkcję: wzmocnienia (LNC) i pierwszej przemiany (DC) odebranego sygnału przy minimalnym wprowadzaniu szumów własnych; typowe temperatury szumowe to: 75 K w pasmie C i 100 K w pasmie Ku oraz odpowiednio współczynniki szumów: 1,0 dB i 1,3 dB;
- konwerter łącza Ziemia - satelita UC przesuwający sygnał pośredniej częstotliwości (typowo IF70 MHz) w zakres mikrofalowy (6 GHz - pasmo C, 14 GHz - pasmo Ku);
- konwerter łącza satelita - Ziemia DC spełniający funkcję odwrotną, tj. przesuwający częstotliwość sygnału odebranego z pasma C (4 GHz) lub pasma Ku (11/12 GHz) do częstotliwości pośredniej (IF70 MHz);
- modulator/demodulator zawarte w modemie;
- urządzenie kodująco-dekodujące *(ang. codec)*.

Transmisja danych od stacji centralnej *(ang. Hub)* do terminali odbywa się w kanale (lub w kilku kanałach) ze zwielokrotnieniem z podziałem czasu TDM *(ang. Time Division Multiplex)*. Prędkość transmisji zawiera się w przedziale od 64 kb/s do 1,544 Mb/s. Dzięki odpowiedniej adresacji danych istnieje możliwość transmisji do wybranego terminala, do wybranej grupy terminali lub do wszystkich terminali współpracujących z daną stacją centralną. Tego typu właściwość związana z przesyłaniem danych do wielu punktów podczas pojedynczej transmisji nie jest zwykle możliwa w konwencjonalnych sieciach naziemnych.

* Naukowa Akademicka Sieć Komputerowa w Polsce JBR, ul. Bartycka 18, 00-716 Warszawa
** Instytut Telekomunikacji i Akustyki, Politechnika Wrocławska, Wybrzeże St. Wyspiańskiego 27, 50-370 Wrocław



Rys. 1. Podstawowa architektura sieci VSAT

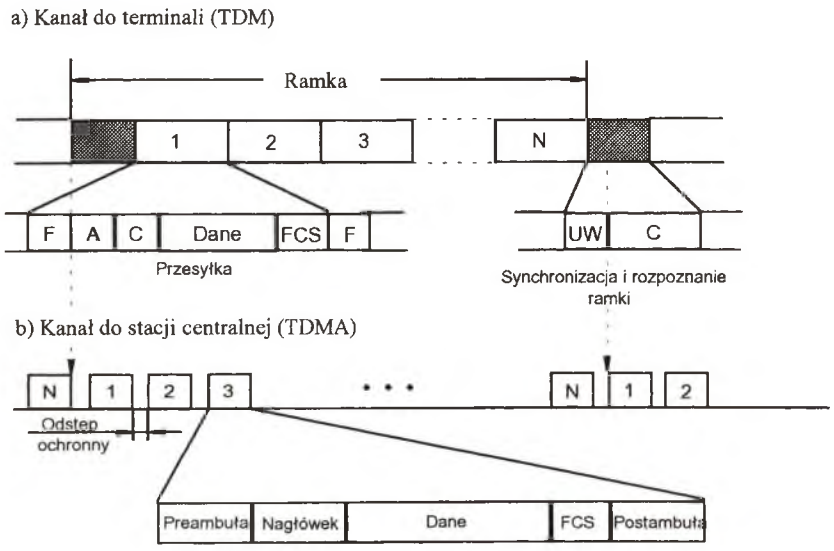


Rys. 2. Schemat blokowy typowego dupleksowego terminala VSAT

Przesyłanie danych od terminala do stacji centralnej jest możliwe dzięki zastosowaniu jednego lub kilku kanałów z czasowym zwielokrotnieniem dostępu TDMA *(ang. Time Division Multiple Access)*. Ograniczenia dotyczące szerokości kanałów i mocy nadajnika oraz wymagane małe opóźnienia, umożliwiają transmisję z prędkością od 9,6 kb/s do 128 kb/s. Typ protokółu dostępu czasowego stosowany w sieci VSAT ma kluczowe znaczenie. Decyduje on o możliwościach, kosztach i złożoności wyposażenia urządzeń sieciowych.

Transmisja danych w kierunku hub-terminal lub terminal-hub wymaga pojedynczego skoku przez satelitę, podczas gdy transmisja danych między terminalami wymaga podwójnego skoku przez satelitę. W drugim przypadku pierwszy skok przez satelitę jest związany z odebraniem przez hub danych wysłanych z terminala nadawcy poprzez kanał TDMA, a drugi - gdy wiadomość jest retransmitowana przez hub w kanale TDM do terminala odbiorcy.

Transmisja w sieci VSAT jest typu pakietowego; sieć działa tak, jak sieć z komutacją pakietów. Wewnętrzny protokół sieciowy gwarantuje niezawodną transmisję. Nie ogranicza to jednak użytkownika sieci do transmisji jedynie danych typu pakietowego. Zarówno hub, jak i terminale są wyposażone w odpowiednie interfejsy umożliwiające pakietyzację danych. Interfejsy te można odpowiednio skonfigurować tak, by dostosowane były do obsługi każdego z wielu typów protokółów interfejsu użytkownika. Sieci VSAT mogą jednocześnie obsługiwać wielu użytkowników zapewniając im poufność transmitowanych danych.



Rys. 3. Sposób dostępu w sieci VSAT: a) ramka TDM w kanale wyjściowym, b) szczelina TDMA w kanale wejściowym: UW (*Unique Word*) - wzorzec ramki, F - flaga, A - adres, C - bity synchronizacji, FCS - bity kontrolne

Dla sieci VSAT z komutacją pakietów o strukturze gwiazdy centralne pole komutacyjne wykonuje funkcje wyboru drogi *(ang. routing)* i połączenia *(ang. relay)*. Ze względu na duże podobieństwo funkcji sieci VSAT do funkcji naziemnych sieci z komutacją pakietów, w wielu sieciach VSAT stosuje się zmodyfikowane pole komutacji pakietów, opracowane na potrzeby sieci z komutacją pakietów X. 25. Od centralnego pola komutacyjnego w sieci VSAT wymaga się aby zapewniło ono:

- niezawodną transmisję w warstwie liniowej do terminali VSAT i do komputera centralnego *(ang. host)*,

- sterowanie procesem dostępu do satelity,
- wybór drogi dla danych *(ang. routing)* pomiędzy terminalami VSAT i centralnym komputerem *(ang. host),*
- łącze dla systemu zarządzania siecią,
- łącza do innych sieci.

3. Zastosowania sieci VSAT

Sieci VSAT mogą świadczyć zarówno nowe typy usług, jak również z powodzeniem zastępować, bądź dublować istniejące sieci. Usługi, które wymagają transmisji danych w obie strony pomiędzy centralnym komputerem i odległymi urządzeniami użytkowników mogą być realizowane przez sieć VSAT, w której centralny komputer jest dołączony do sieci VSAT poprzez stację centralną, urządzenia użytkownika zaś są dołączone do sieci poprzez terminale VSAT. Przykładami tego typu wykorzystania sieci VSAT jest scentralizowany system wymiany informacji giełdowych, system weryfikacji kart kredytowych i scentralizowany system rezerwacji biletów. W systemie wymiany informacji giełdowej centralny komputer inicjuje zazwyczaj transmisję danych giełdowych poprzez okresowe odpytywanie *(ang. pooling)* terminali. Terminale po otrzymaniu polecenia wysyłają wymagane informacje do komputera centralnego. Wymiana danych w systemie weryfikacji kart kredytowych lub systemie rezerwacji biletów jest inicjowana przez użytkownika. Komputer centralny udziela w tym przypadku odpowiedzi użytkownikowi. Istnieje również możliwość lokalizacji centralnego komputera przy terminalu. W takim przypadku transmisja danych wymaga podwójnego skoku przez satelitę.

4. Protokoły komunikacyjne

4.1. Specyficzne wymagania stawiane przez sieci satelitarne

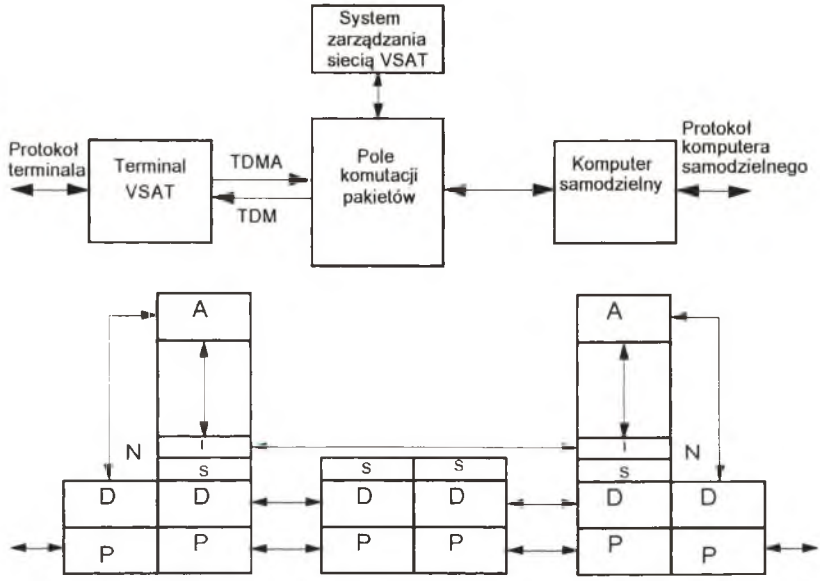
Pola komutacji pakietów w sieciach VSAT cechują się niespotykanymi w typowych polach komutacji pakietów X. 25 właściwościami. Występująca w większości sieci VSAT topologia gwiazdy wymusza przepływ wszystkich danych przez pojedyncze pole komutacyjne. W naziemnych sieciach komputerowych z komutacją pakietów stosuje się wiele pól komutacji pakietów, z których każde komutuje jedynie część całkowitego ruchu. Wymagania stawiane polu komutacji pakietów w sieciach VSAT są bardzo wysokie. Pole komutacji pakietów musi zapewnić w niektórych przypadkach przepływność ponad 1000 pakietów/s w sieci składającej się z setek, a nawet tysięcy terminali VSAT pracujących w trybie interakcyjnym. Kolejnym specyficznym wymaganiem dotyczącym pola komutacji pakietów jest jego duża przepływność binarna. W typowych sieciach VSAT szybkość transmisji w kanale satelitarnym przekracza 64 kb/s. W kanale hub - terminal VSAT transmisja odbywa się z szybkością będącą wielokrotnością 64 kb/s. Zazwyczaj jest to 512 kb/s. W nowszych systemach szybkość transmisji dochodzi do 2,048 Mb/s. Tak duże przepływności nie są zwykle stosowane w naziemnych sieciach z komutacją pakietów, a zatem pola komutacji pakietów nie są dostosowane do takich szybkości. Trzecią istotną różnicą pomiędzy naziemnymi sieciami pakietowymi i sieciami VSAT jest niezawodność. W większości naziemnych sieci pakietowych przewiduje się drogi alternatywne do transmisji sygnału. W przypadku uszkodzenia jednego z pól komutacji pakietów buduje się obejścia, tak że tylko niewielka część ruchu w sieci jest przerywana . W typowych sieciach VSAT ruch pomiędzy setkami lub tysiącami węzłów zależy od działania pojedynczego pola komutacji pakietów. Problem jego niezawodności jest zatem sprawą zasadniczą dla sieci VSAT. Z problemem tym wiąże się odpowiednia konstrukcja pola komutacji i zapewnienie rezerwy w sytuacjach awaryjnych. Podobne wymagania związane z niezawodnością dotyczą transponderów na satelicie.

4.2. Protokoły ISO

ISO *(ang. International Standards Organisation)* opracowało standardy protokółów z punktu widzenia ich przydatności jako protokółów ułatwiających przepływ danych między sieciami. Dlatego też mogło by się wydawać, że tego typu protokóły nie znajdą zastosowania jako protokóły wewnętrzne sieci z komutacją pakietów. Jeśli jednak weźmiemy pod uwagę, że większość sprzętu realizującego komutację pakietów stanowią w zasadzie sieci jako takie, a elementy przetwarzające tego sprzętu są połączone ze sobą magistralą równoległą lub lokalną siecią komputerową, to na problem ten można spojrzeć jak na problem połączenia międzysieciowego. Dlatego też warstwowa struktura protokółów sieciowych ISO może być rozważana jako możliwa struktura wewnętrzna sieci z komutacją pakietów. Przykład tego typu struktury pokazano na rys. 4. Warstwa sieciowa sieci wewnętrznej została podzielona na dwie podwarstwy: podwarstwę odpowiedzialną za wybór drogi w sieci wewnętrznej zwaną pod-

warstwą podsieciową 3S *(ang. subnetwork sublayer)* oraz podwarstwę odpowiedzialną za funkcje wejścia i wyjścia, takie jak multipleksowanie połączeń wirtualnych oraz integralność danych od wejścia do wyjścia. Podwarstwę tę nazywa się podwarstwą międzysieciową *(ang. internet sublayer)* 3I. Jako przykład zastosowania tego typu podejścia może służyć system VSAT o nazwie Clearlink. W systemie tym sieć wewnętrzna stosuje strukturę datagramową z protokółami wejścia - wyjścia rezydującymi jedynie w procesorach końcowych terminala VSAT oraz procesora grupowego *(ang. Host Interface)*. Protokół bezpołączeniowy IP opracowany przez ISO *(ang. Connectionless Internet Protocol)* stosowany jest jako element podwarstwy podsieciowej 3S.

Jest on odpowiedzialny za podstawowe funkcje związane z wyborem drogi i połączeniem między terminalem VSAT, centralnym polem komutacji pakietów oraz procesorem grupowym (spełniającym rolę translatora pomiędzy protokółami użytkownika i siecią VSAT). Protokół TP4 *(ang. ISO Transport Class 4 Protocol)* stosuje się w podwarstwie międzysieciowej 3I, zapewniając odpowiedni protokół wejścia - wyjścia wraz z podstawowymi funkcjami multipleksowania potrzebnymi do zestawienia połączenia wirtualnego. Protokół TP4 wykorzystuje również odpowiedni mechanizm potwierdzenia *(ang. sliding window acknowledgment)* umożliwiający skuteczną transmisję danych przy dużym opóźnieniu transmisji cechującym łącze satelitarne.

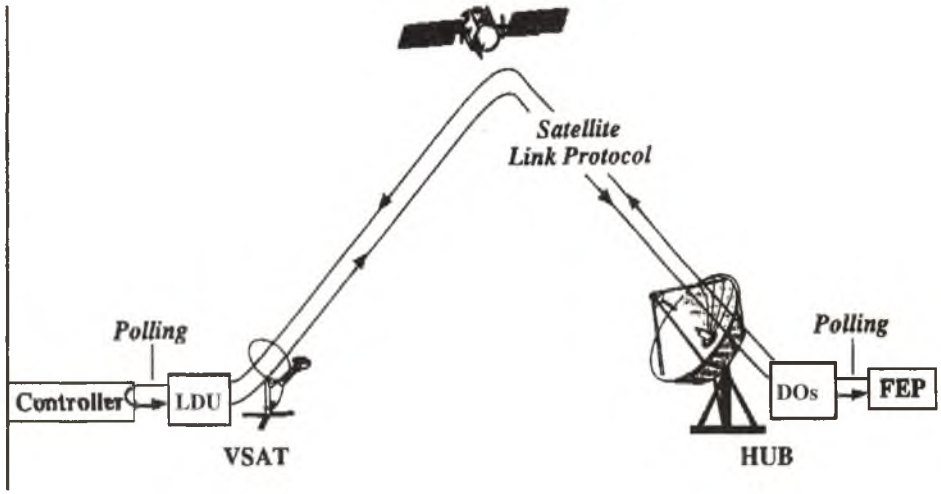


Rys. 4 Struktura sieci VSAT według modelu odniesienia OSI

4.3. Interfejsy wielopunktowych protokółów synchronicznych

Wiele potencjalnych zastosowań systemów VSAT opiera się na możliwości budowy alternatywnych sieci transmisji danych. Sieci te umożliwiają stosowanie protokółów z warstwy liniowej, takich jak BISYNCH *(ang. Binary Synchronous Communications firmy IBM)* czy też SDLC *(ang. Synchronous Data Link Control)*. Protokoły tego typu zapewniają łączność punkt - punkt oraz punkt - wiele punktów oraz umożliwiają wielu urządzeniom komunikacyjnym wykorzystanie wspólnego łącza cyfrowego lub analogowego. W celu skutecznej transmisji danych poprzez łącze satelitarne niezbędna staje się emulacja funkcji protokółu związanej z procesem sterowania zgłoszeniem *(ang. polling process)*. Emulacja ta *(ang. spoofing)* obejmuje dwa współpracujące ze sobą procesy. Jeden z nich odbywa się w komputerze grupowym *(ang. host)* a drugi w terminalu VSAT. Oba procesy obsługują i nadzorują proces sterujący zgłoszeniem lokalnie. Ponadto procesy te zapew-

niają synchronizację na obu końcach łącza. Dzięki temu stan połączenia jest emulowany prawidłowo, a mechanizm detekcji i korekcji błędów *(ang. error recovery mechanism)* działa poprawnie zarówno w komputerze grupowym, jak i w terminalu VSAT w przypadku, gdy łącze satelitarne zastępowane jest typowym łączem telefonicznym. Obsługę procesu wywołań przedstawiono na rys. 5. Jako przykłady synchronicznego interfejsu, sterującego procesem zgłoszenia w systemie VSAT omówione zostaną interfejsy SDLC i BISYNC.



Rys. 5. Obsługa procesu wywołań w łączu satelitarnym

4.3.1. SDLC

Protokół SDLC jest protokółem zorientowanym bitowo. Reprezentuje on nowoczesną klasę protokółów opartych na koncepcji wyizolowania procesów związanych z niezawodnym przemieszczaniem danych od punktu do punktu i umieszczeniem ich w warstwie liniowej. SDLC stanowi podzbiór procedur protokółu HDLC *(ang. High Level Data Link Control)*. Protokoł HDLC jest normą ISO i CCITT. W przypadku stosowania go jako protokółu transmisji od komputera samodzielnego do terminala stosuje się tryb NRM *(ang . Normal Response Mode)*. W trybie tym stacja pierwotna jest przypisana komputerowi samodzielnemu, stacja wtórna natomiast terminalowi. Transmisja danych jest inicjowana jedynie przez komputer samodzielny, natomiast proces sterowania zgłoszeniem *(ang. polling process)* wykorzystywany jest jedynie w celu uzyskania danych od stacji wtórnej (terminala). Typowy diagram przepływu danych w SDLC przy zastosowaniu NRM pokazano na rys. 6. Ramka inicjująca połączenie SNRM, jak również sekwencja UA, są zdefiniowane w HDLC. W przeciwieństwie do protokółu BISYNC protokół SDLC umożliwia pracę przy niepełnym potwierdzaniu ramek. Zwykle konieczne jest potwierdzenie co najmniej co 7 ramki, ale w niektórych przypadkach okno czasowe może być poszerzone do 127 ramek. W systemach VSAT w celu zapewnienia ich skutecznej pracy musi być jednak zapewniona emulacja procesu sterowania zgłoszeniem.

Interfejs pomiędzy siecią SDLC w stacji pierwotnej i SDLC w stacji wtórnej realizowany za pomocą systemu VSAT spełnia funkcje synchronizujące obie sieci oraz przesyła jedynie dane oraz informacje o ważnych dla sieci zdarzeniach poprzez łącze satelitarne. Do opracowania interfejsów pomiędzy systemami VSAT i siecią z komutacją pakietów SDLC wykorzystano doświadczenie nabyte przy tworzeniu publicznych sieci transmisji danych. Firma IBM zmodyfikowała protokół QLLC *(ang. Qualified Link Level Control)* w celu budowy interfejsu pomiędzy sieciami SNA i publicznymi sieciami transmisji danych. Na rysunku 7 pokazano sekwencję występujących po sobie transmisji umożliwiających budowę połączenia w oparciu o SDLC i wymianę danych w sieci VSAT. Bardziej zaawansowane rozwiązania interfejsu SDLC obejmują emulacją sesji jednostki logicznej *(ang. LU - Logical Unit session)*. Umożliwia to komutację pakietów wewnątrz sieci SNA

dla pojedynczych sesji. Wadą tego rozwiązania jest złożoność dodatkowego oprogramowania, które ponadto musi uwzględniać wszelkie zmiany, jakie firma IBM może dokonać w protokole SNA. Protokoł QLLC przekształca sieć VSAT w kanał logiczny pomiędzy komputerem samodzielnym i kontrolerem w taki sposób, że nie zostają zakłócone procesy sterowania sesją oraz zarządzania siecią.

4.3.2. BISYNC

Protokoł BISYNC *(ang. Binary Synchronous Communications)* był jednym z pierwszych protokółów komunikacyjnych stosowanych do łączenia terminali z komputerem samodzielnym. Opracowany został w latach sześćdziesiątych przez firmę IBM i w pierwszym rzędzie był stosowany w kontrolerach komunikacyjnych. Operacje logiczne wykonywane przez te kontrolery zależały od wewnętrznej struktury połączeń. Nie było wtedy jeszcze mowy o stosowaniu w tego typu urządzeniach sterowania za pomocą oprogramowania. Stąd też protokół ten łączy w sobie zarówno funkcje związane z tworzeniem połączenia, jak również funkcje należące w modelu OSI do warstwy aplikacji.

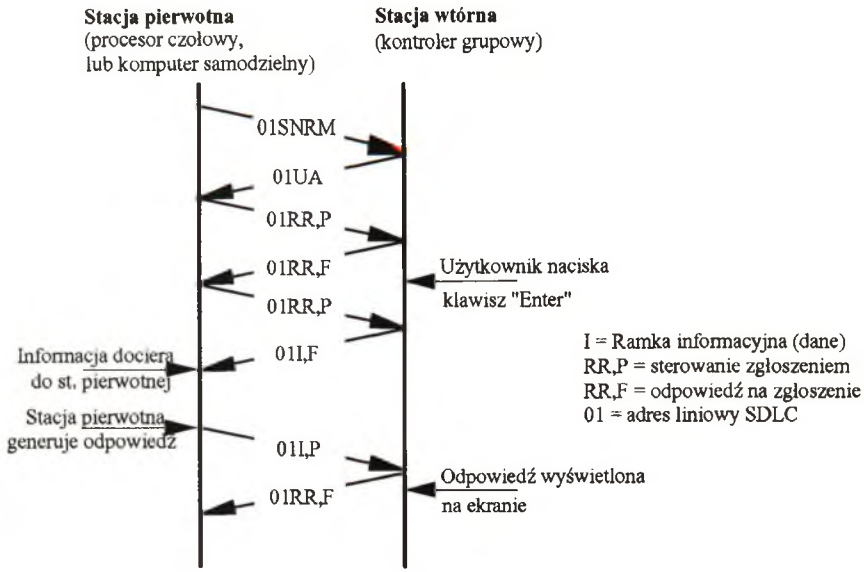
Funkcje takie jak sterowanie zgłoszeniem, selekcja oraz transmisja danych pomiędzy stacją główną a terminalem są pod względem koncepcji podobne do rozwiązań w SDLC. W typowym rozwiązaniu sieci wielopunktowej stacja główna w sposób ciągły ubiega się o dane od terminali. Odbywa się to poprzez wysyłanie sekwencji sterującej zgłoszeniem zawierającej unikalny adres terminala. Terminal może przesłać dane do stacji centralnej w momencie przyjścia następnej sekwencji sterującej zgłoszeniem. Do transmisji od stacji głównej do terminala stosuje się sekwencję selekcyjną oraz dołączony do niej ciąg danych. Do każdej transmitowanej wiadomości jest dołączana sekwencja kontrolna umożliwiająca wykrywanie błędów transmisji. W przypadku wykrycia błędów stacja odbiorcza wysyła potwierdzenie niezgodności NAK *(ang. negative acknowledgement)* lub wcale nie odpowiada. Proces wysyłania sekwencji selekcyjnej jest wtedy powtarzany. Z tego względu protokół BISYNC nie pozwala na przesyłanie wielu ramek jednocześnie z potwierdzeniami i wymusza pracę z naprzemiennym potwierdzaniem. Tego rodzaju działanie jest skuteczne jedynie w przypadku opóźnień transmisji dużo krótszych niż długość transmitowanej informacji.

W celu skutecznego przesyłania danych BISYNC poprzez sieci charakteryzujące się długim czasem opóźnienia np. naziemne sieci transmisji danych lub sieci VSAT, należy za pomocą emulacji protokółu usunąć konieczność pracy w trybie z naprzemiennym potwierdzaniem. Problem ten został rozwiązany przez operatorów publicznych sieci transmisji danych. Opracowali oni normę emulacji protokółu BISYNC umożliwiającą transmisję danych w sieciach z komutacją pakietów. Emulacja protokółu BISYNC znana pod nazwą DSP *(ang. Display Systems Protocol)* ustala nie tylko postać standardowej sekwencji sterującej zgłoszeniem ale również określa zachowania w sytuacjach nietypowych, jak np. błędy w łączu czy też naruszenie struktury protokółu. Sieci VSAT są dołączane do procesu DSP poprzez stworzenie ciągłego połączenia wirtualnego. Połączenie to zestawiane jest w procesie inicjalizacji sieci.

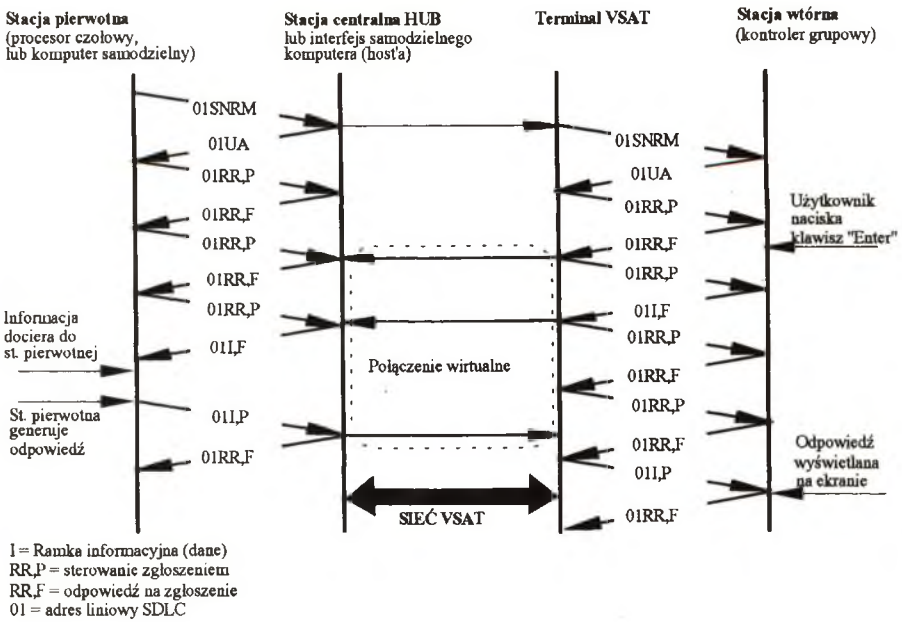
4.4. Interfejs X.25 w sieciach VSAT

Przy zastępowaniu istniejących cyfrowych sieci komutacji pakietów sieciami VSAT interfejsy sieciowe X.25 są znacznie prostsze niż w przypadku interfejsów sieci synchronicznych. W tym przypadku interfejs sieciowy łączy w sobie fizyczne połączenie pomiędzy terminalem użytkownika a siecią (styk CCITT V.24), interfejs protokółu X.25 warstwy 2. i 3. oraz adapter międzysieciowy X.25/VSAT (rys. 8). Warstwy 2. i 3. w interfejsie sieciowym realizują lokalnie potwierdzenia w stosunku do terminala użytkownika i nie mają na ich pracę wpływu opóźnienia w łączu satelitarnym. Oznacza to, że ograniczenia czasowe i wielkości okien czasowych nie muszą być modyfikowane w terminalu użytkownika, gdy korzysta on z sieci VSAT. Ograniczenia czasowe warstwy 3 związane z procedurami wymiany danych między końcami sieci (np. CALL CONNECT, CALL CLEAR, itd.) są dłuższe niż opóźnienie w łączu satelitarnym, dlatego też nie wymagają modyfikacji w terminalu użytkownika.

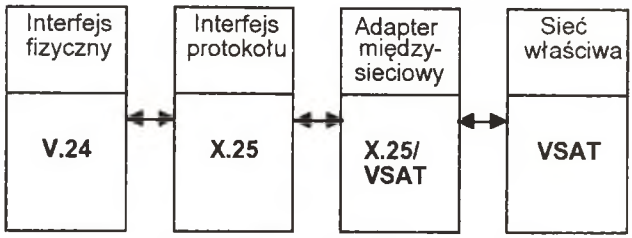
Adapter międzysieciowy X.25/VSAT wykonuje następujące funkcje: translację adresów, zestawianie połączenia dla pakietów, sterowanie i nadzór nad połączeniem wirtualnym, wymiana danych, zarządzanie przepływem danych w warstwie 3. i między innymi adapterami międzysieciowymi. Na przykład odebranie przez adapter międzysieciowy pakietu CALL CONNECT z lokalnej warstwy 3. powoduje inicjację funkcji zarządzających połączeniem wirtualnym, transformację pakietu do postaci akceptowanej przez sieć wewnętrzną, dołączenie odpowiedniego adresu sieciowego i przesłanie do sieci właściwej, w której odbywa się transmisja



Rys. 6 Uproszczony schemat inicjalizacji połączenia, sterowania zgłoszeniem oraz transmisji danych za pomocą protokołu SDLC



Rys. 7. Inicjacja połączenia, sterowanie zgłoszeniem oraz transmisja danych zgodnie z protokołem SDLC w sieci VSAT



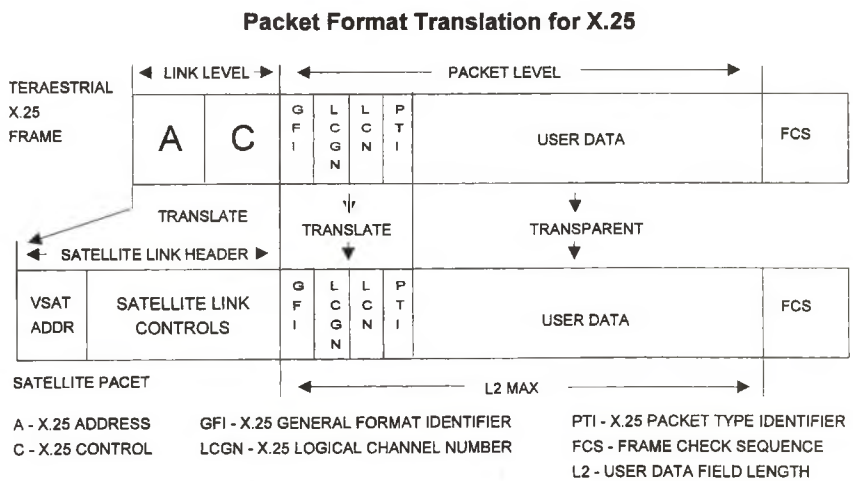
Rys. 8. Interfejs użytkownika X.25 do sieci VSAT

do odległego adaptera międzysieciowego. W odległym adapterze po odebraniu pakietu odbywa się proces odwrotny. Usuwa on i analizuje informację dopisaną przez wysyłający adapter międzysieciowy, transformuje postać pakietu i przesyła go do 3. warstwy sieci lokalnej. Pakiet jest przesyłany do terminala użytkownika poprzez niższe warstwy. Jeśli terminal użytkownika zaakceptuje nawiązanie połączenia to odpowiada on wysłaniem pakietu CALL ACCEPT, który jest przesyłany do terminala inicjującego połączenie. Oba adaptery międzysieciowe przyznają odpowiednie zasoby systemu do budowy połączenia wirtualnego.

Translację struktury protokółu CCITT X.25 stosowanego w sieciach naziemnych do postaci przydatnej dla sieci satelitarnych pokazano na rys. 9. Przez łącze satelitarne są przesyłane jedynie pakiety zawierające informację użytkownika (pakiety typu I). Nagłówek ramki pakietu X.25 wykorzystywanego w łączu naziemnych ulega konwersji i staje się nagłówkiem warstwy liniowej łącza satelitarnego i odwrotnie. Proces ten jest realizowany w sterowniku dostępu do satelity i w procesorze pasmowym *(ang. baseband processor)*. W odpowiedni sposób zmienia się również sekwencję kontrolną ramki *(ang. FCS - Frame Control Sequence)*.

Po zestawieniu połączenia wirtualnego ramki informacyjne są swobodnie wymieniane między terminalami użytkowników podlegając jedynie ograniczeniom związanym ze sterowaniem przepływem. Obie warstwy 3. lokalnie potwierdzają ramki informacji tak, że opóźnienie w łączu satelitarnym jest niewidoczne dla warstwy 3. w terminalu użytkownika.

Przerwanie połączenia wirtualnego poprzez przesłanie przez jedną ze stron pakietu CALL CLEAR lub na skutek przerwy w sieci powoduje zwolnienie wszystkich zasobów przyznanych do zestawienia połączenia wirtualnego.



Rys. 9. Porównanie struktury pakietu X.25 stosowanego w łączu naziemnym i satelitarnym

5. Protokoły dostępu wielokrotnego stosowane w sieciach VSAT

Jak wcześniej wspomniano, protokoły transmisji w sieci VSAT są jednym z najważniejszych jej elementów. Dlatego też niezwykle istotnym jest umiejętne dobranie rodzaju protokółu zależnie od potrzeb użytkowników sieci.

Przy wyborze optymalnej metody przydziału kanału wyznacznikami mogą być:

- przepustowość kanału, tj. część kanału przenosząca użyteczną informację,
- opóźnienie dostępu dla średniego i maksymalnego natężenia ruchu,
- stabilność systemu w przypadkach niepożądanych, np. dużych odchyleń w natężeniu ruchu,
- odporność systemu na błędy transmisji i usterki urządzeń,
- właściwości operacyjne, jak np.: restart systemu, obsługa nowych stacji lub innych rodzajów trafiku, itp.,
- koszty implementacji i złożoność, tj. wymagany sprzęt i oprogramowanie.

Protokoły dostępu wielokrotnego możemy podzielić ze względu na stosowanie bądź nie stosowanie czasowego podziału kanału na: szczelinowe i nieszczelinowe; ze względu na sposób przydziału dostępu do kanału na: stałe, z ustalonym dostępem *(ang. fixed assigned)*, rywalizacyjne, z losowym dostępem *(ang. contention (random access))* i rezerwacyjne ze sterowanym dostępem *(ang. reservation (controlled access))*.

Tabela 1 zawiera zestaw satelitarnych protokółów dostępu wielokrotnego pogrupowanych według wymienionych kryteriów.

Tabela 1. Satelitarne protokóły dostępu wielokrotnego

Typ dostępu	Nieszczelinowy *(unslotted)*	Szczelinowy *(slotted)*
Stały *(fixed assigned)*	SCPC-FDMA	TDMA
	CDMA	
Rywalizacyjny *(contention/random access)*	Pure ALOHA	Slotted ALOHA
	SREJ-ALOHA	Tree CRA
	Time-Of-Arrival CRA* (TARA)	ARRA
	Unslotted RA-CDMA	Slotted RA-CDMA
	SREJ-ALOHA/FCFS*	
Rezerwacyjny *(reservation/controlled access)*	Rezerwacja z lokalną* synchronizacją, z dostępem:	DAMA, rezerwacja z dostępem:
	Time-Of-Arrival (TARA)	TDMA
	SREJ-ALOHA	Slotted ALOHA
	ALOHA	Tree CRA
		Wielodostęp mieszany *Hybrid reservation/random access*

* Częstotliwość taktowania lokalnego zegara zależna od obciążenia kanału.

5.1. Protokoły ze stałym przydziałem dostępu

FDMA SCPC. Jest to najprostsza forma dostępu wielokrotnego, w której pasmo przenoszenia transpondera jest podzielone na pewną liczbę kanałów *(FDMA - ang. Frequency Division Multiple Access)* z odrębnymi sygnałami nośnymi *(SCPC - ang. Single Channel Per Carrier)*. Pomimo, że współczynnik wykorzystania kanału może osiągnąć wartość idealną 1,0 (przy zerowym opóźnieniu dostępu), to protokół ten w sieciach z użytkownikami interakcyjnymi jest generalnie mało skuteczny ze względu na niezgodność pomiędzy wymaganą dużą prędkością transmisji *(ang. burst speed)* krótkich wiadomości nadawanych przez użytkowników a średnią wielkością transmisji danych z terminala. Innymi słowy, krótkie transmisje typu burst, ze względu na wymaganą przez nie szybkość transmisji, zajmują szerokie pasmo w krótkim czasie, co oznacza małą skuteczność wykorzystania pasma.

CDMA. Protokół z kodowym zwielokrotnieniem dostępu CDMA *(ang. Code Division Multiple Access)*, jest protokółem systemu, w którym sygnał informacyjny jest rozpraszany przy użyciu technik systemów szerokopasmowych. Protokoł CDMA ze stałym przydziałem dostępu wykorzystuje takie zalety systemów szerokopasmowych, jak: małą gęstość mocy niezbędną do odebrania sygnału, dużą odporność na interferencje

od sąsiadujących satelitów i stacji naziemnych oraz odporność na celowe zakłócanie *(ang. anti-jam capability)*. Ze względu na wymienione cechy w systemach z CDMA można używać anten o średnicy mniejszej od 1 m bez obawy o wpływ zakłóceń, bądź zbyt niski poziom sygnału użytecznego.

Współczynnik wykorzystania pasma osiągany przez protokół CDMA ze stałym przydziałem *(ang. fixed assigned CDMA)* bez korekcji błędu *(FEC - ang. Forward Error Correction)* wynosi 0,05 - 0,1, natomiast przy użyciu FEC wzrasta do 0,2 - 0,3.

Systemy CDMA ze stałym przydziałem zapewniają szybki i prosty dostęp tylko w przypadku, gdy system nie jest przeciążony. W przypadku przeciążenia konieczna jest zmiana reguły dostępu. Każda stacja jest przystosowana do odbioru określonego ciągu adresowego. "Dostrojenie" odbiornika do przychodzącego sygnału jest szybkie i nie wymaga skomplikowanej aparatury. Po "dostrojeniu" stacja wysyła potwierdzenie nawiązania łączności posługując się odpowiednim kodem.

TDMA. Protokoł wielodostępu z podziałem czasowym TDMA (ang. Time Division Multiple Access), w którym zsynchronizowane odcinki czasu zawierają N szczelin czasowych rezerwowanych przez N stacji wykorzystujących dany kanał. Zwiększanie liczby stacji (użytkowników) powoduje wydłużenie czasu oczekiwania na dostęp i prowadzi do zmniejszenia skuteczności wykorzystania kanału. Z tego też względu TDMA stosuje się w systemach z małą liczbą użytkowników przesyłających duże ilości danych. W takich przypadkach współczynnika wykorzystania kanału osiąga wartość 0,6 - 0,8.

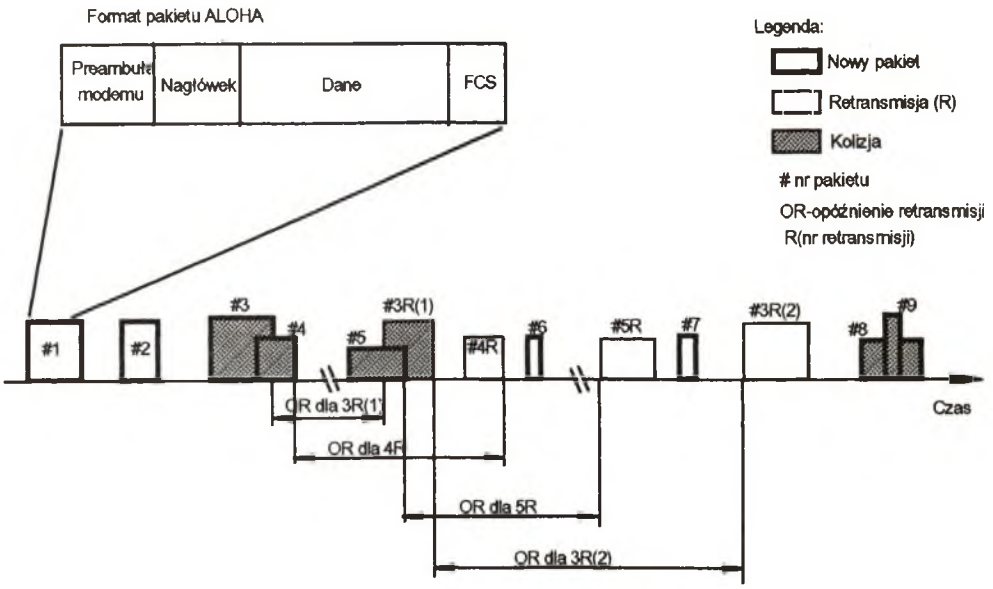
5.2. Protokoły z dostępem rywalizacyjnym

ALOHA. Zwykły protokół ALOHA *(ang. pure ALOHA)* jest najprostszym asynchronicznym protokółem rywalizacyjnym. Nie wymaga on ani czasowej ani logicznej koordynacji pomiędzy stacjami nadającymi we wspólnym kanale. Schemat działania protokółu przedstawiono na rys. 10.

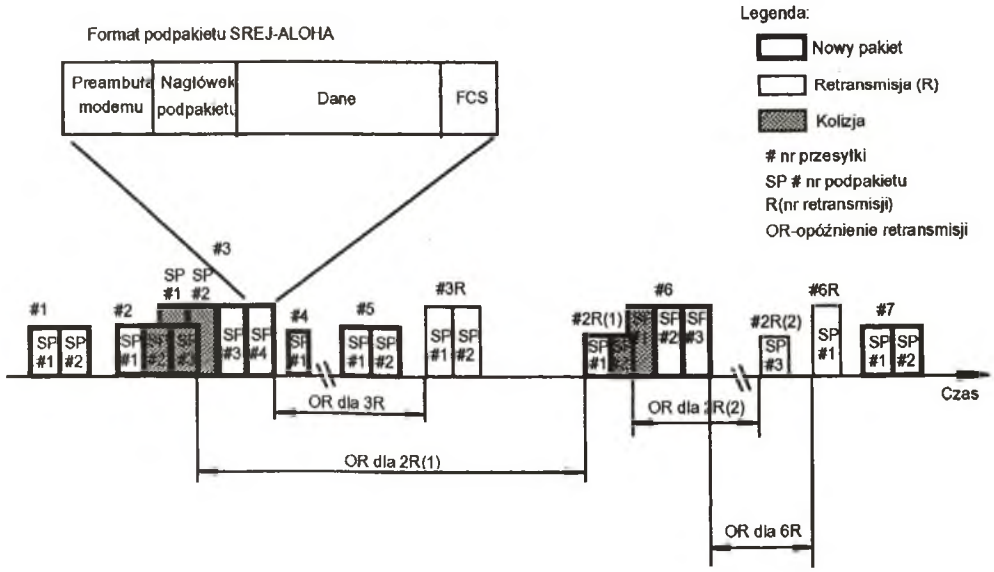
SREJ-ALOHA. Jest protokółem stosującym dodatkową podpakietyzację przesyłki w połączeniu z systemem retransmisji ARQ *(ang. automatic request for repeats)* zapewniającym ochronę przed błędami. Jak to pokazano na rys. 9.3, w SREJ-ALOHA pakiet informacji jest dzielony na ciągłą sekwencję niezależnych podpakietów *(ang. subpacket)* o ustalonych długościach, każdy z własną preambułą i nagłówkiem. Wykorzystano tu fakt, iż większość kolizji w protokółach asynchronicznych, np. zwykła ALOHA, jest spowodowana częściowym nakładaniem się pakietów. Retransmitowanie zatem tylko części pakietu staje się korzystniejsze z punktu widzenia przepustowości, opóźnień i stabilności systemu. Teoretycznie, współczynnik wykorzystania pasma dla protokółu SREJ-ALOHA wynosi 0,368. W praktyce jednak, głównie ze względu na konieczność umieszczania preambuły i nagłówka w każdym podpakiecie, pojemność systemu jest średnio dwukrotnie większa od pojemności zwykłej ALOHA i zawiera się w przedziale 0,2 - 0,3. W związku z tym zaleca się stosowanie odpowiednich modemów z krótką identyfikującą preambułą, co nie ma jednak większego wpływu na koszty i kompleksowość systemu. Protokoł SREJ-ALOHA należy obok protokółu ALOHA do najtańszych i najprostszych.

ALOHA szczelinowa. Jest to najbardziej znany protokół dostępu losowego *(ang. random access protocol)*. W protokole tym pakiety o ustalonej długości mogą być transmitowane w ściśle określonych przedziałach czasu (szczelinach), jak to pokazano na rys. 12. Dzięki temu współczynnik wykorzystania pasma wzrasta do 0,368 (dokładnie dwukrotnie w stosunku do zwykłego ALOHA), lecz wzrasta także stopień skomplikowania systemu z uwagi na konieczność synchronizacji użytkowników.

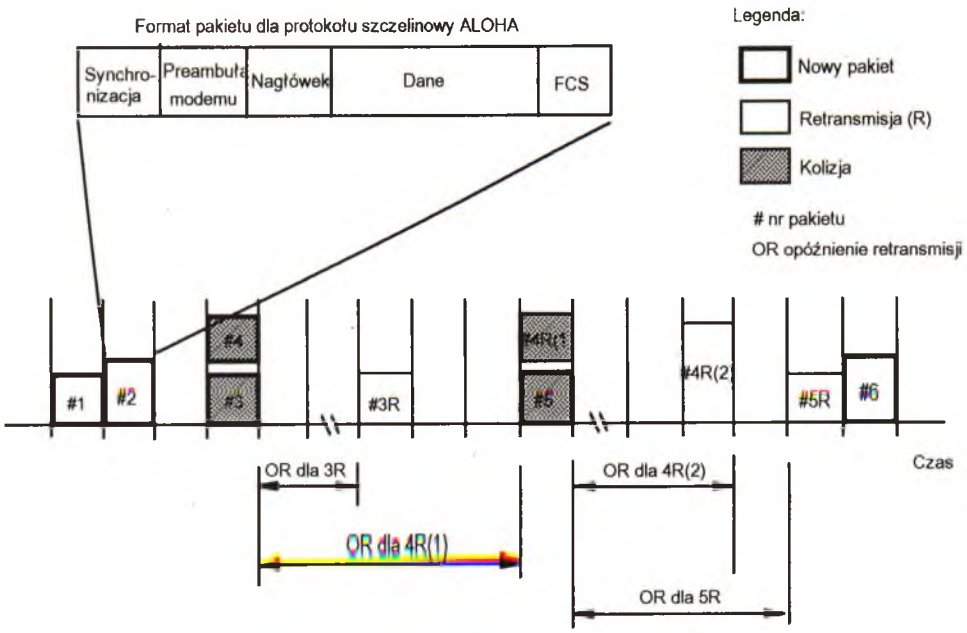
Tree CRA, zwany także adaptacyjnym protokółem chodzenia po drzewie, jest przykładem kolejnego protokółu szczelinowego z dostępem rywalizacyjnym. W protokole tym stosuje się algorytm rozwiązywania kolizji *(ang. collision resolution algorithm - CRA)* ze strukturą decyzyjną drzewa. Na rys. 13 przedstawiono stacje w postaci binarnego drzewa. W szczelinie 0, pierwszej szczelinie rywalizacji o dostęp do kanału, wszystkie stacje są dopuszczone do prób zdobywania kanału. Jeżeli nastąpi kolizja , to w szczelinie 1 tylko stacje leżące poniżej węzła B będą mogły ubiegać się o kanał. Jeżeli jedna z nich zdobędzie kanał, to szczelina następująca po pakiecie jest zarezerwowana dla stacji poniżej węzła C. Jeżeli natomiast dwie lub więcej stacji poniżej węzła B chcą nadawać, to wystąpi kolizja w szczelinie 1 i wówczas w szczelinie 2 będzie nadawał węzeł D.



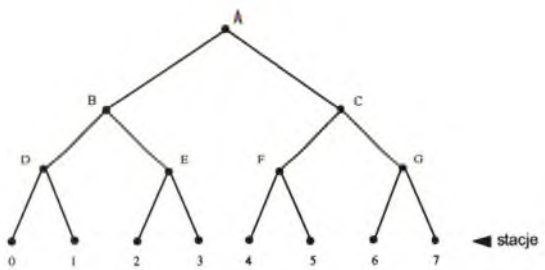
Rys. 10. Ilustracja zdarzeń w kanale dla zwykłego protokołu ALOHA



Rys. 11. Ilustracja zdarzeń w kanale dla protokołu SREJ-ALOHA



Rys. 12. Ilustracja zdarzeń w kanale dla protokołu ALOHA szczelinowa



Rys. 13. Drzewo dla ośmiu stacji

Jeżeli kolizja wystąpi w szczelinie 0, to nastąpi przeszukanie całego drzewa na pierwszej głębokości w celu znalezienia wszystkich gotowych stacji. Każda szczelina bitowa jest związana z pewnym węzłem w drzewie. W razie kolizji przeszukiwanie postępuje dalej rekursywnie od lewego i prawego rozgałęzienia tego węzła. Jeżeli szczelina bitowa przejdzie pusta lub jeżeli istnieje dokładnie jedna stacja, która nadaje do niej, to przeszukiwanie jej węzła może zatrzymać się, ponieważ wszystkie gotowe stacje są już odnalezione.

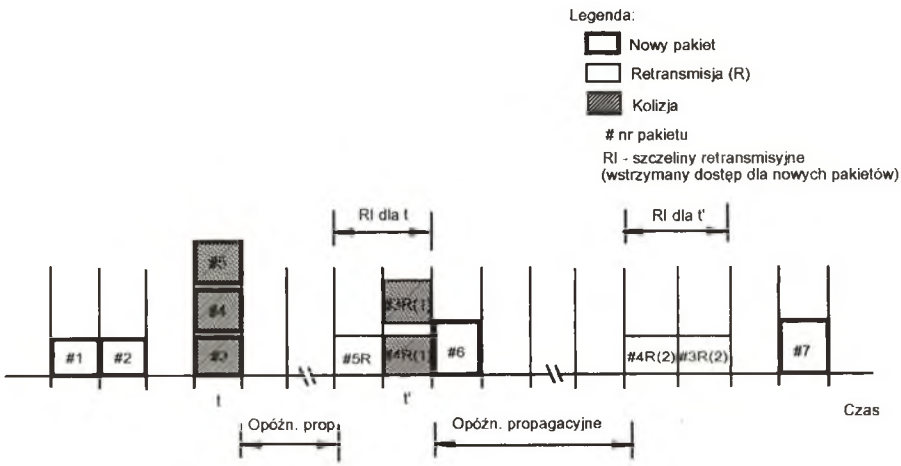
Kiedy obciążenie w systemie jest duże, nie warto przeznaczać szczeliny 0 dla węzła A, ponieważ ma to sens przy mało prawdopodobnej sytuacji, że dokładnie jedna stacja ma pakiet do nadania. Podobnie można by twierdzić, że węzły B i C powinny być także przeskoczone z tego samego powodu. Zatem, im większe obciążenie, tym niżej w drzewie powinno rozpocząć się szukanie. Jeśli ponumerujemy poziomy drzewa, to można zauważyć, że poniżej każdego węzła na poziomie "i" znajduje się część 2^{-i} całego drzewa. Jeżeli q gotowych stacji jest jednolicie rozłożonych, to ich oczekiwana liczba poniżej określonego wierzchołka na poziomie "i"

jest właśnie $2^{-i}q$. Optymalnym poziomem do rozpoczęcia przeszukiwania drzewa jest ten, na którym oczekiwana liczba rywalizujących stacji na szczelinę jest 1, czyli poziom, na którym 2-iq=1. Rozwiązując to równanie znajdujemy $i = \log_2 q$.

W przeciwieństwie do protokółów ALOHA, algorytm CRA jest zbieżny, co gwarantuje stabilność kanału dla skończonej i nieskończonej liczby stacji. Współczynnik wykorzystania pasma dla Tree CRA jest w zakresie 0,43 - 0,49, w zależności od specyfiki użytego CRA. System ten wydaje się być atrakcyjniejszy niż szczelinowy ALOHA, zarówno pod względem wykorzystania pasma, jak i stabilności.

Niestety, Tree CRA ma także i swoje wady. Ze względu na dość skomplikowaną procedurę rozwiązywania kolizji, w przypadku błędu w obserwacji kanału, system ten zakleszcza się *(ang. deadlock)*. Szczelinowa ALOHA, jako protokół gwarantujący stabilność dla skończonej liczby użytkowników, jest wolny od tego typu zakleszczeń ze względu na prostotę stosowanego w nim algorytmu rozwiązywania kolizji. Inną wadą protokółu Tree CRA jest konieczność stosowania przeplotu w kanałach na satelicie, co zwykle wiąże się z dodatkowym opóźnieniem. Opóźnienie to można wyeliminować tylko kosztem zmniejszenia maksymalnej przepustowości systemu.

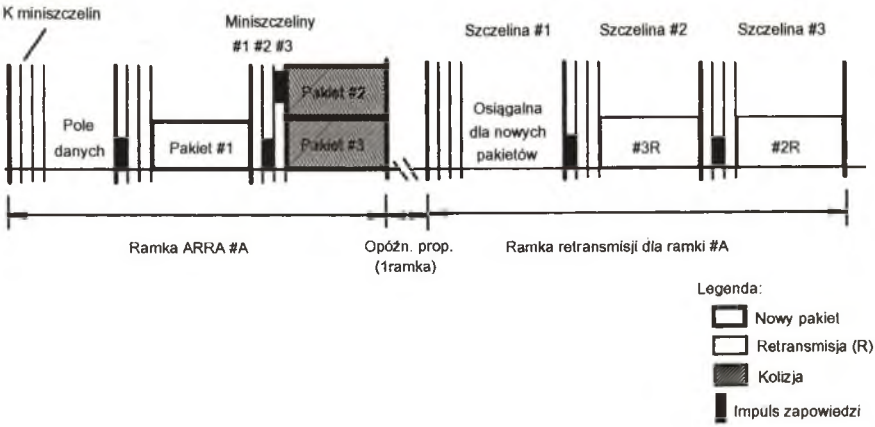
Podsumowując, problemy z zakleszczaniem i przeplotem oraz duża złożoność systemu ograniczają nieco jego główną zaletę, jaką jest duża pojemność. Podobnie jak i dla szczelinowego ALOHA, dużą słabością Tree CRA jest nieumiejętność dostosowania optymalnego formatu pakietu do zmiennej długości przesyłek, cechy tak charakterystycznej dla komunikacji w sieciach VSAT.



Rys. 14. Ilustracja pracy systemu Tree CRA

ARRA. Protokół z zapowiedzianą retransmisją ARRA *(ang. Announced Retransmission Random Access)* oferuje większą pojemność od szczelinowej ALOHA poprzez dodanie do każdego pakietu informacji przesyłki zapowiadającej w postaci mini-szczeliny czasowej. W protokole ARRA wykorzystuje się fakt, iż próby retransmisji generowane są pseudolosowo, a zatem są przepowiadalne. Zapowiedzenie przyszłej retransmisji w danej szczelinie może zapobiec kolizji tej retransmisji z nowo transmitowanym pakietem. Dodatkowo, poprzez przewidzenie przyszłych kolizji pomiędzy zapowiadającymi retransmisję stacjami, takie retransmisje mogą być odwołane i umieszczone w innych, niewykorzystanych a przeznaczonych dla nowych przesyłek szczelinach kanału. Ilustrację pracy protokółu ARRA przedstawiono na rys. 15.

Typowa wartość współczynnika wykorzystania pasma zawiera się w przedziale 0,53 - 0,6. Zastosowanie tego protokółu w sieciach VSAT jest jednak ograniczone ze względu na skomplikowaną implementację miniszczelin oraz tradycyjne już dla systemów szczelinowych kłopoty z ustaleniem formatu dla przesyłek o zmiennej długości.



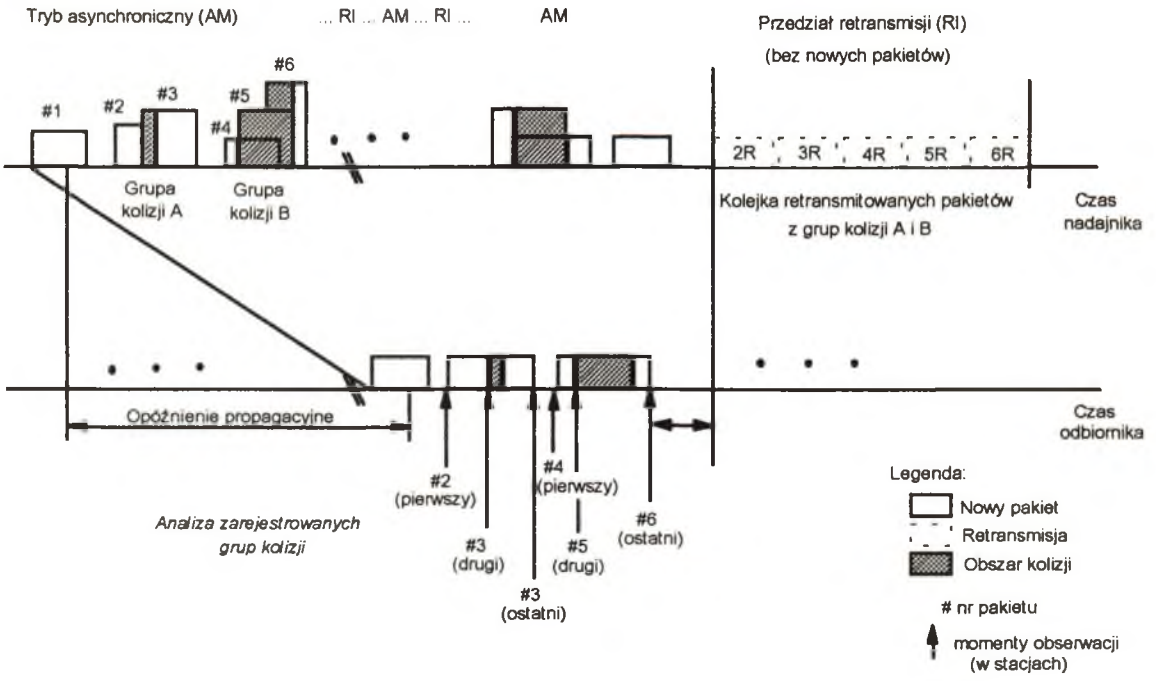
Rys. 15. Ilustracja pracy protokołu ARRA (K = 3)

TARA. Protokoł TARA (ang. *Time-of-Arrival based Random Access*) jest nieszczelinowym protokółem z lokalną synchronizacją bazującym na obserwacji zdarzeń zachodzących w kanale. Zastosowany tu algorytm CRA wykorzystuje dzięki sprzężeniu zwrotnemu sekwencje nadchodzących pakietów informujące go o liczbie kolizji w systemie. Dla pakietów o ustalonej długości stosuje się analizę z ciągłą detekcją sygnału (SD), która umożliwia wykrycie pierwszego i ostatniego pakietu biorących udział w kolizji. Zwolnione są więc od kolizji dwa retransmitowane pakiety. Jeżeli dodatkowo stacja ma możliwość detekcji kolizji (CD), przynajmniej trzy pakiety (pierwszy, drugi i ostatni) z wszystkich biorących udział w kolizji, będą rozpoznane. Następnie pakiety te zostaną retransmitowane w ustalonym porządku dzięki lokalnej synchronizacji (częstotliwość taktowania zależna od obciążenia kanału) w specjalnym interwale czasowym. Aby zminimalizować niepożądane kolizje, stacje wstrzymują transmisję nowych pakietów w wiadomych sobie przedziałach czasu potrzebnych na zaplanowaną retransmisję. Rys. 16 ilustruje analizę sytuacji kolizyjnej przy użyciu detekcji sygnału i kolizji (SD/CD) oraz proces lokalnie synchronizowanej retransmisji.

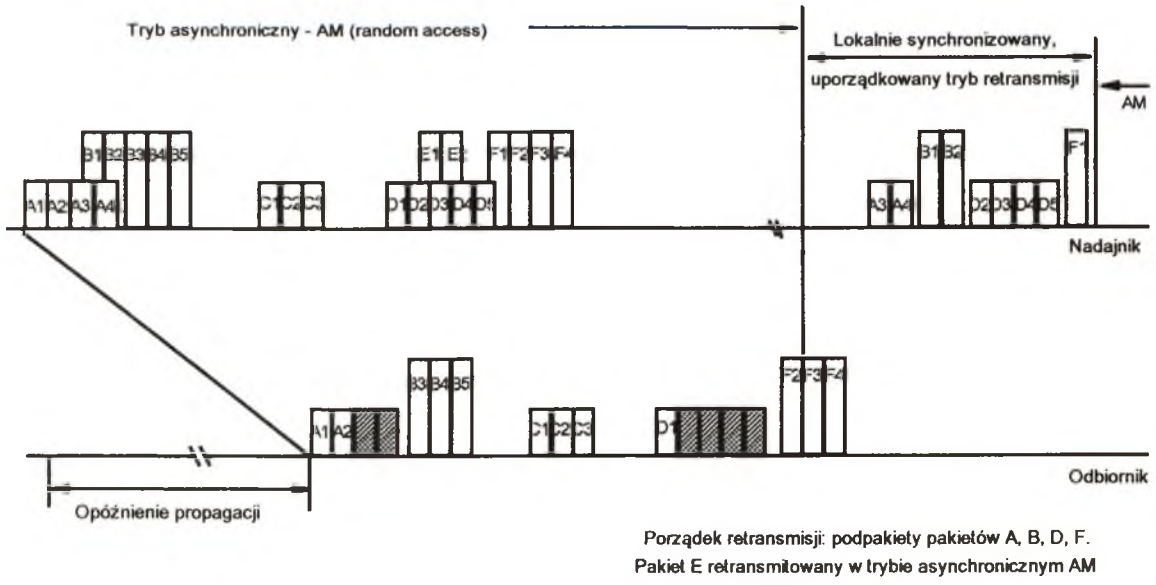
Typowy współczynnik wykorzystania pasma w systemie TARA z detekcją sygnału SD wynosi 0,41, zaś z SD/CD zawiera się w przedziale 0,47 - 0,51. Jest to zatem konkurencja dla złożonego, szczelinowego systemu Tree CRA. Oczywistym jest jednak fakt , iż podobnie jak w przypadku wymienionych konkurentów, pojemność systemu maleje dla trafiku o zmiennej długości przesyłek.

Protokoły TARA mogą być atrakcyjne dla drugiej generacji VSAT-ów, zaprojektowanych specjalnie do pracy ze zwykłym protokółem ALOHA, gdyż od momentu rozpoczęcia stosowania lokalnej synchronizacji opartej na zdarzeniach w kanale, zauważono kilka bardzo istotnych zalet - operacyjnych i sprzętowych - stawiających w nieco lepszym świetle asynchroniczne protokóły z dostępem rywalizacyjnym.

SREJ-ALOHA/FCFS. Opisany wcześniej algorytm bazujący na obserwacji obciążenia kanału (TARA) może cechować się dobrymi właściwościami przy wymianie przesyłek o zmiennej długości, gdy zastosuje się go wewnątrz struktury SREJ-ALOHA. Można tego dokonać bez dodatkowego sprzętu potrzebnego do detekcji sygnału (SD) lub detekcji kolizji (CD). Analiza kolizji na poziomie podpakietów w systemie SREJ-ALOHA daje dostateczną ilość informacji, aby retransmitować je w porządku: pierwszy przyszedł - pierwszy obsłużony *(FCFS -ang. first-come-first-served).* Ilustrację pracy systemu SREJ-ALOHA z lokalnie synchronizowanym procesem retransmisji FCFS przedstawia rys.17.



Rys. 16. Ilustracja zdarzeń w kanale z protokołem TARA z SD/CD i K = 2



Rys. 17. Ilustracja pracy protokołu SREJ-ALOHA/FCFS

Zastosowanie opisanego algorytmu CRA znacznie zwiększa możliwości tego systemu w porównaniu z podstawowym asynchronicznym SREJ-ALOHA. Osiągany współczynnik wykorzystania pasma zawiera się w granicach 0,4 - 0,5 zależnie od długości przesyłanych pakietów. Należy jednak zauważyć, że w tak istotnej kwestii jak transmisja pakietów o zmiennej długości, system SREJ-ALOHA/FCFS przewyższa najlepsze, jak np. Tree CRA, szczelinowe systemy z dostępem rywalizacyjnym i osiąga poziom przepustowości dorównujący typowej pojemności systemów z rezerwacją dostępu. Stanowi on zatem atrakcyjne unowocześnienie dla typowych systemów ALOHA zapewniające im poprawę podstawowych parametrów jak przepustowość, stabilność i opóźnienie w szerokim zakresie rodzajów trafiku.

RA-CDMA. Transmisja szerokopasmowa, o której wspomniano przy okazji omawiania protokółu CDMA ze stałym przydziałem, może mieć zastosowanie także w przypadku protokółów z pseudolosowym przydziałem dostępu. Stacje końcowe wykorzystują szerokie, wspólne dla wszystkich stacji, pasmo częstotliwości. Każda stacja ma odrębny adres, który w ogólnym przypadku tworzy się na podstawie matrycy czasowo-częstotliwościowej (rys. 18b). Adres tworzy ciąg jednakowej długości impulsów o częstotliwościach wybranych ze zbioru M dostępnych częstotliwości. Częstotliwości stosowane w sygnale kodowym powinny być tak dobrane, aby widma elementarnych impulsów nawzajem na siebie nie zachodziły. Między impulsami mogą występować przerwy o długościach będących wielokrotnością czasu trwania elementarnego impulsu (rys. 18c). Elementarny sygnał informacji, np. impuls z wyjścia modulatora delta, jest reprezentowany przez ciąg kodowy (rys. 18a). Jeśli w elementarnym sygnale informacji zawarte jest N elementarnych impulsów, to można utworzyć N!/(N-M)! kombinacji adresowych (w każdej po N impulsów o różnych częstotliwościach). Przykładowo, dla M=3 i N=8 liczba adresów wynosi 336.

Nie wszystkie adresy mogą być stosowane w praktyce. Ze względu na wymaganą odporność na wzajemne zakłócenia określa się mianowicie minimalną dopuszczalną odległość między ciągami adresowymi. Dodatkowe ograniczenia wynikają z braku synchronizacji w sieci. W systemie asynchronicznym po stronie odbiorczej znana jest tylko kolejność, a niewiadoma pozostaje numeracja przychodzących impulsów ciągu tak, że np. ciągu 1 0 3 0 0 0 2 (rys. 18c)) nie można odróżnić od ciągu 3 0 0 0 2 1 0 ani od żadnego innego powstałego wskutek cyklicznego przesunięcia pozycji ciągu. W systemach asynchronicznych więc żaden z adresów nie może stanowić cyklicznego przesunięcia innego adresu. Systemy szczelinowe, w których ograniczenie to nie występuje, umożliwiają utworzenie większej liczby adresów przy danej powierzchni matrycy czasowo-częstotliwościowej, kosztem jednak wzrostu złożoności systemu.

Kodowanie z rozproszonym widmem umożliwia rywalizującym pakietom wielokrotne niedestrukcyjne wzajemne interferowanie, zapewniając większą stabilność systemu. Jak pokazano na rys. 19, dla asynchronicznego protokółu rywalizacyjnego RA-CDMA, zmiany w liczbie interferujących ze sobą transmisji objawiają się zmiennym prawdopodobieństwem wystąpienia błędu w czasie trwania transmisji danego pakietu. Pakiety, w których wykryto błędy są retransmitowane z losowym opóźnieniem za pomocą algorytmu podobnego do stosowanego w zwykłym protokole ALOHA.

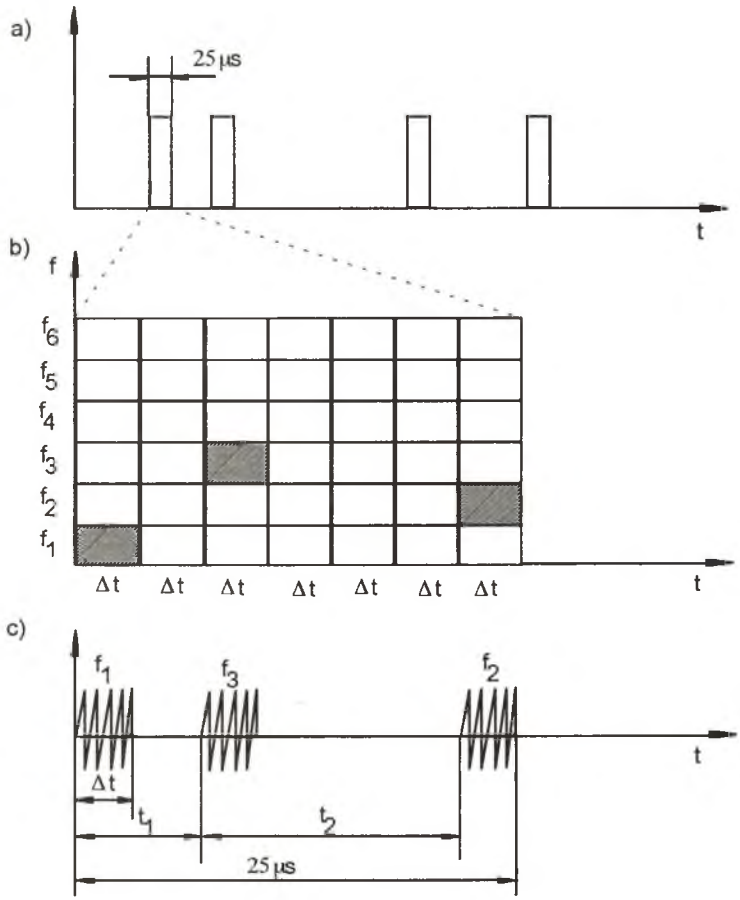
Zdolność utrzymania wielu jednoczesnych transmisji zapewnia mniejsze opóźnienie dostępu niż zwykły protokół ALOHA, choć unormowana pojemność systemu RA-CDMA ma wartość zbliżoną do pojemności zwykłego systemu ALOHA (ok. 0,1). Po zastosowaniu korekcji błędów (FEC), pojemność systemu może wzrosnąć do 0,2 - 0,3, wiąże się to jednak ze wzrostem kosztów i złożoności urządzeń.

5.3. Protokoły z dostępem rezerwacyjnym

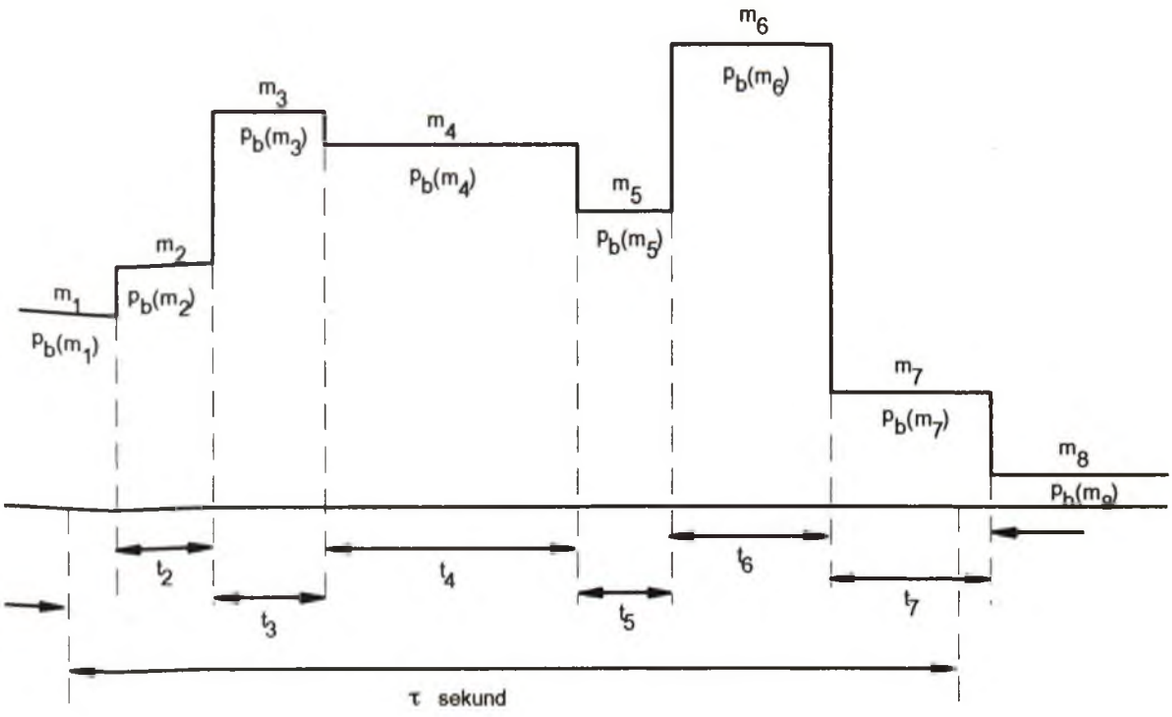
Wielodostęp na żądanie - DAMA *(ang. Demand Assigned Multiple Access)* jest systemem najlepiej rozwiązującym problem satelitarnej komunikacji interakcyjnej pomiędzy stacjami transmitującymi krótkie przesyłki *(ang. bursty stations)*. W systemach DAMA stosuje się dwupoziomowy dostęp do kanału. Pierwszy poziom dostępu jest przeznaczony dla krótkich pakietów rezerwacyjnych zawierających żądanie dostępu przez daną stację, natomiast drugi poziom służy do transmisji pakietów danych. Dostęp na poziomie rezerwacyjnym może być realizowany przez dowolny z opisanych poprzednio protokółów stałego bądź rywalizacyjnego dostępu. Jeśli rezerwacja przebiegnie pomyślnie, to pakiety danych są formowane w wolne od kolizji, scentralizowane bądź pogrupowane kolejki i przesyłane w kanale o dużej przepustowości. Odpowiednio zaprojektowany system DAMA dobrze sobie radzi z transmisją przesyłek o zmiennej długości, adaptując się do trafiku będącego mieszanką transferu plików i ruchu interakcyjnego. Jednakże, jak to widać na rysunku 20, duża przepustowość połączona jest z relatywnie dużym opóźnieniem (ok. 0,5s) związanym z procesem rezerwacji. To niezbędne minimum zwłoki jest nagradzane później niewielką zmianą opóźnienia dostępu do kanału w szerokim zakresie przepustowości.

Typowy dla systemów VSAT protokół DAMA, ma zbliżony do TDMA format kanału podzielonego na periodyczne ramki zawierające grupy wąskich szczelin służących do rezerwacji i większe szczeliny przeznaczone dla pakietów danych. Proporcje pomiędzy szczelinami danych a szczelinami rezerwacyjnymi są zależne od przewidywanego profilu obciążenia komunikacyjnego oraz typu protokółu użytego do rezerwacji.

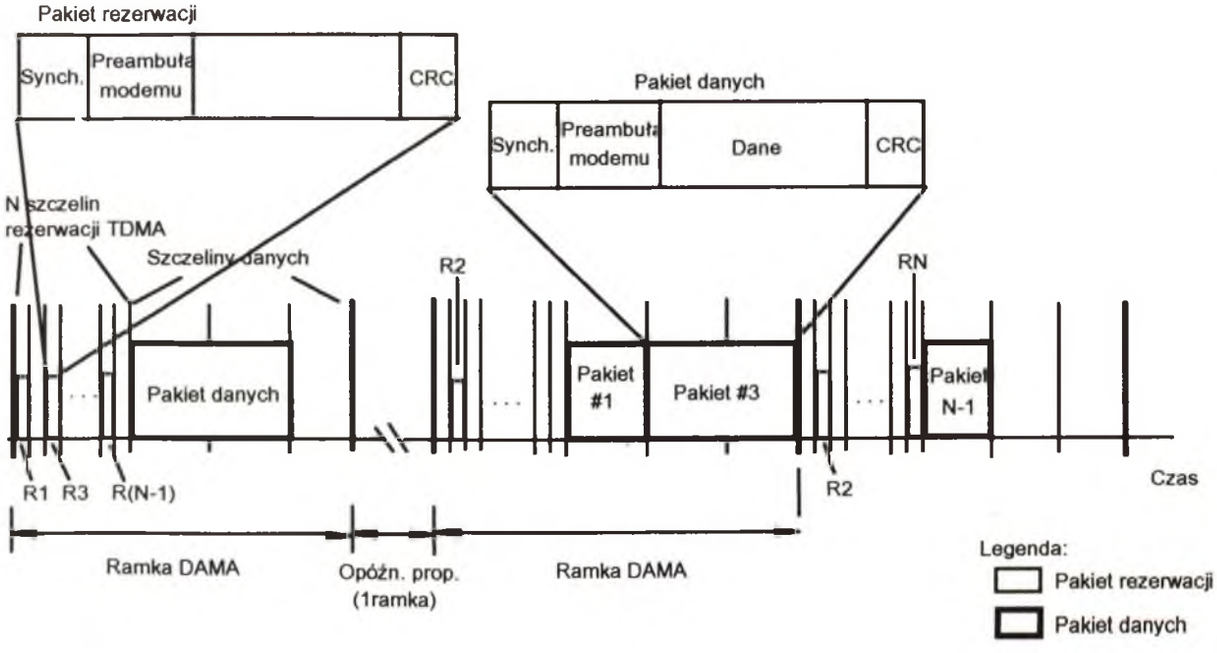
DAMA/TDMA. W systemie DAMA z rezerwacją TDMA (rys. 20), w skład ramki wchodzą wąskie szczeliny rezerwacyjne w liczbie odpowiadającej liczbie stacji VSAT, oraz szczeliny przeznaczone do transmisji danych. Podczas trwania jednej ramki, użytkownik może żądać rezerwacji jednej lub większej liczby szczelin danych. W sieciach VSAT opartych o topologię gwiazdy, pakiet żądania rezerwacji zostaje odebrany przez stację centralną, dołączany do kolejki i odesłany z powrotem do terminala w kanale TDM. Protokoły mające strukturę ramki TDMA, oprócz opóźnień propagacyjnych, charakteryzują się także wcześniej wspomnianym



Rys. 18. Tworzenie sygnału kodowego w systemie kodowo-adresowym: a) ciąg impulsów na wyjściu modulatora delta, b) matryca czasowo-częstotliwościowa, c) ciąg kodowy



Rys. 19. Wynik interferencji podczas transmisji τ sekundowego pakietu danych w kanale z asynchronicznym RA-CDMA



Rys. 20. Ilustracja zdarzeń w kanale dla protokołu DAMA/TDMA

dużym opóźnieniem zwłoki *(ang. latency delay)* (ok.0,6-0,7 s) oraz ograniczeniem liczby obsługiwanych użytkowników. Jeśli dane przesyłane są bezkonfliktowo, to system osiąga bardzo dużą skuteczność.

Protokoł DAMA z rezerwacją TDMA jest przeznaczony zatem dla mocno obciążonego systemu VSAT, transmitującego długie, zmieniającej się długości przesyłki. W systemach rywalizacyjnych, wpływ na obniżenie skuteczności i przepustowości systemu mają kolizje. W przypadku systemów DAMA, konieczność odpowiedniej synchronizacji *(ang. guard time)* oraz umieszczania preambuły w każdym pakiecie (włącznie z rezerwacyjnymi), powoduje, że współczynnik wykorzystania pasma nie przekracza 0,5 - 0,6.

Protokoł podobny do DAMA/TDMA znalazł zastosowanie w systemie SATNET pod nazwą PODA *(ang. Priority-Oriented Demand Assignment)*. Jest to protokół z przydziałem priorytetów na żądanie i występuje on w dwóch wariantach: FPODA (stały PODA) oraz CPODA (PODA z rywalizacją). Każda ramka jest podzielona na część danych i część sterującą dla rezerwacji. Względne wielkości tych dwóch części są ustalane dynamicznie, zależnie od obciążenia.

DAMA/Slotted ALOHA. System DAMA może także obsługiwać dużą liczbę terminali VSAT, pod warunkiem, że dostęp do rezerwacji będzie realizowany przez protokół rywalizacyjny (zamiast stały TDMA). Typową implementacją protokółu rezerwacji w systemie DAMA, zapewniającą niezależność procesu rezerwacji od liczby obsługiwanych użytkowników, jest szczelinowa ALOHA. Obraz pracy systemu DAMA/S-ALOHA przedstawia rys. 21. Mimo, że kształt ramki jest bardzo podobny do DAMA/TDMA, możliwy jest także do zrealizowania format przeplatany, znacznie zmniejszający opóźnienie zwłoki ramki.

Rezerwacja z lokalną synchronizacją. Systemy z kontrolowanym (rezerwowanym) dostępem wymagają zazwyczaj podziału czasu i synchronizacji, aby zidentyfikować i przydzielić żądającej stacji daną szczelinę czasową. Zajmiemy się teraz niedawno zaproponowanym, alternatywnym rozwiązaniem systemu, klasyfikowanym jako "lokalnie synchronizowany" lub "samo synchronizujący się".

Protokoły tego typu zostały stworzone jako rozszerzenia dla nieszczelinowych systemów: zwykła ALOHA, SREJ-ALOHA, TARA, aby dodatkowo usprawnić ich pracę w trafiku z dużymi proporcjami długości przesyłek lub w trafiku mieszanym (interakcja/transfer plików).

W systemach z lokalnie synchronizowaną rezerwacją, regułą jest aby początkowo umożliwić żądającej stacji dostęp do kanału jak w zwykłym protokole ALOHA. W chwili, gdy system odbierze ustaloną liczbę żądań dostępu K (K 1), przełącza się w lokalnie synchronizowany tryb rezerwacyjny z szybkością taktowania (podobnie jak w TARA) zależną od obciążenia sieci. Przykład pracy takiego protokółu z dostępem ALOHA przedstawia rys. 22.

Wielodostęp mieszany. Omówione wcześniej rezerwacyjne systemy wielodostępu na żądanie sprawdzają się najlepiej w dużym trafiku z długimi przesyłkami. Użycie zwykłego protokółu DAMA przy obciążeniu mieszanym jest nieefektywne dla krótkich przesyłek ze względu na duże opóźnienie.

Z drugiej zaś strony systemy rywalizacyjne, dobrze pracujące z trafikiem interakcyjnym, są generalnie nieskuteczne przy trafiku mieszanym. Warto więc zatem stworzyć schemat mieszany, łącząc małe opóźnienie dostępu sytemów rywalizacyjnych z dużą przepustowością charakteryzującą systemy z rezerwacją.

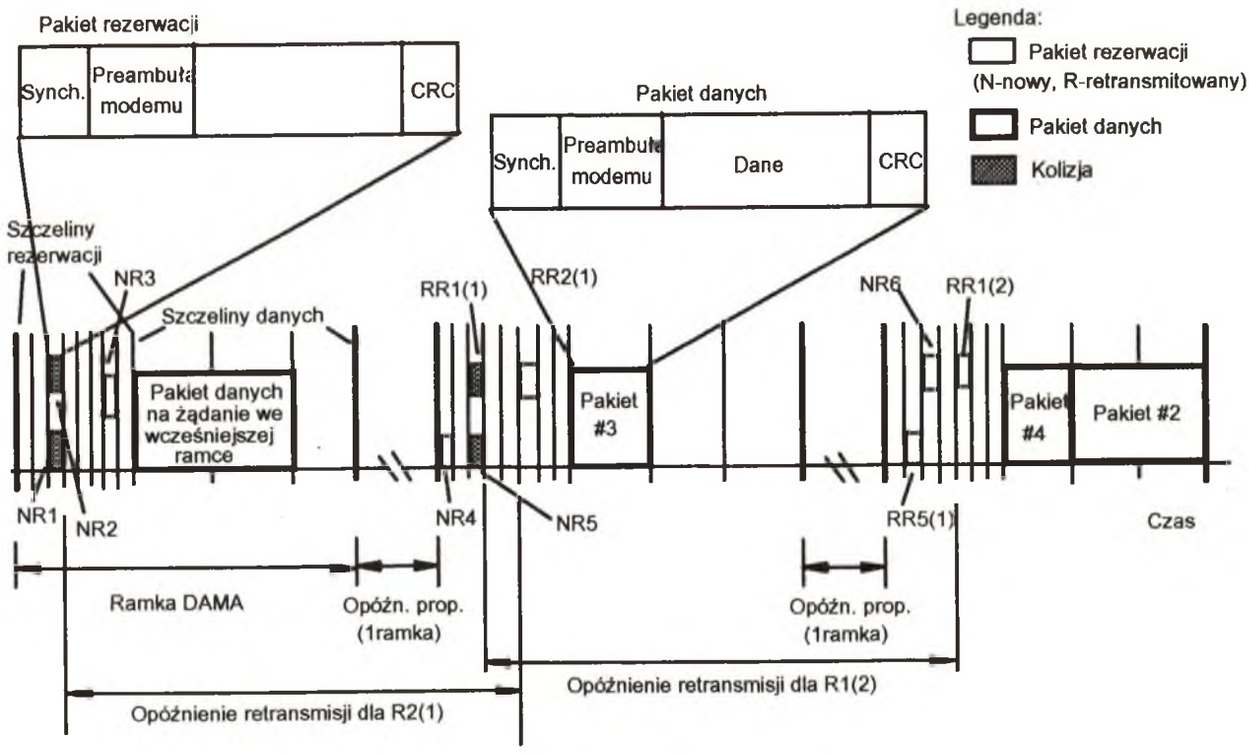
Najprostszą strategią jest, by transmitować krótkie przesyłki bezpośrednio w szczeliny rezerwacyjne unikając opóźnienia związanego z procesem rezerwacji oraz aby transmitować pakiety rezerwacji razem z krótkimi pakietami danych tylko w razie konieczności zwiększenia pojemności kanału.

Można by także zrealizować procedurę rezerwacji, według której pomyślnie przesłany, rywalizujący pakiet większej przesyłki mógłby rezerwować dla niej tę samą szczelinę w następnej ramce. Tego typu protokóły oferują przepustowość równą przepustowości DAMA i małe opóźnienie dostępu dla krótkich przesyłek interakcyjnych.

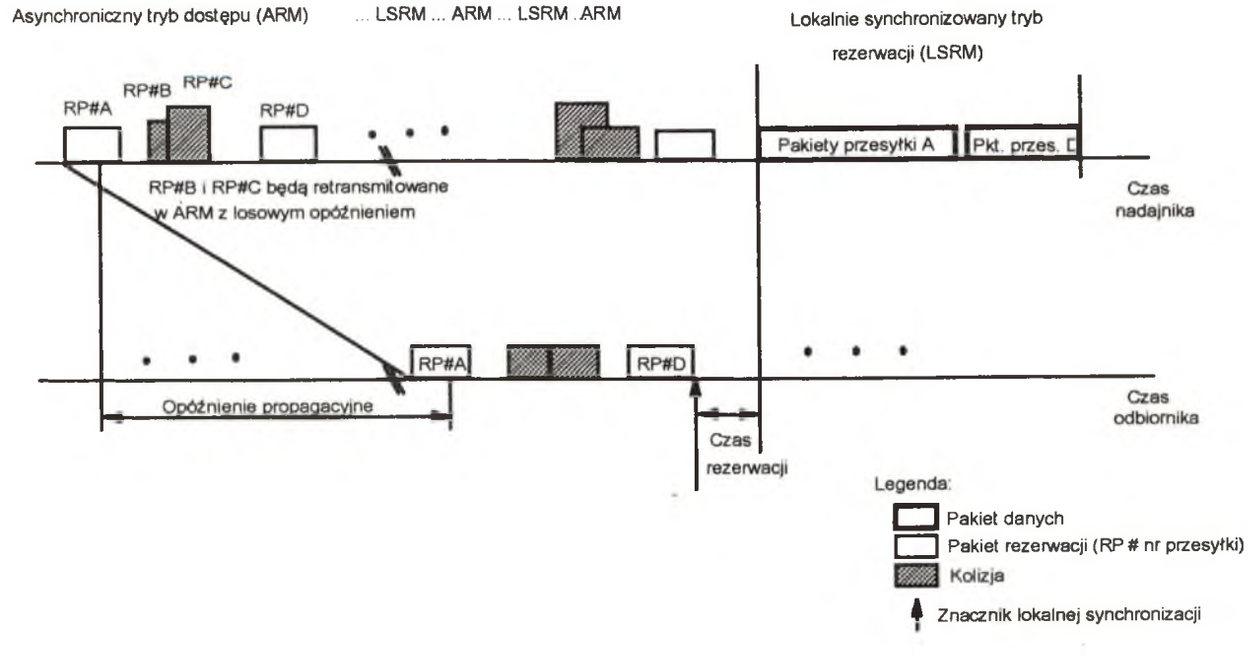
6. Pomiary jakości usług sieciowych świadczonych przez sieci VSAT

W zaleceniu 140 CCITT określono zbiór parametrów jakości usług sieciowych QOS *(ang. Quality of Service)*. Parametry te opisują cechy sieci od strony użytkownika nie wchodząc głębiej w strukturę sieci i sposób jej działania oraz nie zależą one od stosowanego w sieci protokółu. Taki sposób podejścia umożliwia zastosowanie tych parametrów do opisu dowolnej sieci transmisji danych.

W ramach grantu finansowanego przez KBN przewidziano pomiar wybranych parametrów QOS dla transmisji danych wykorzystującej łącze satelitarne. W tym celu nawiązano współpracę z prywatnym operatorem sieci VSAT w Polsce Telekomunikacją Satelitarną S.A. z Bielska-Białej. Operator ten wyraził chęć współpracy i zainteresowanie wynikami eksperymentu. Bez pełnej współpracy z operatorem nie jest możliwe wykona-



Rys. 21. Ilustracja zdarzeń w kanale z protokołem DAMA/Slotted ALOHA



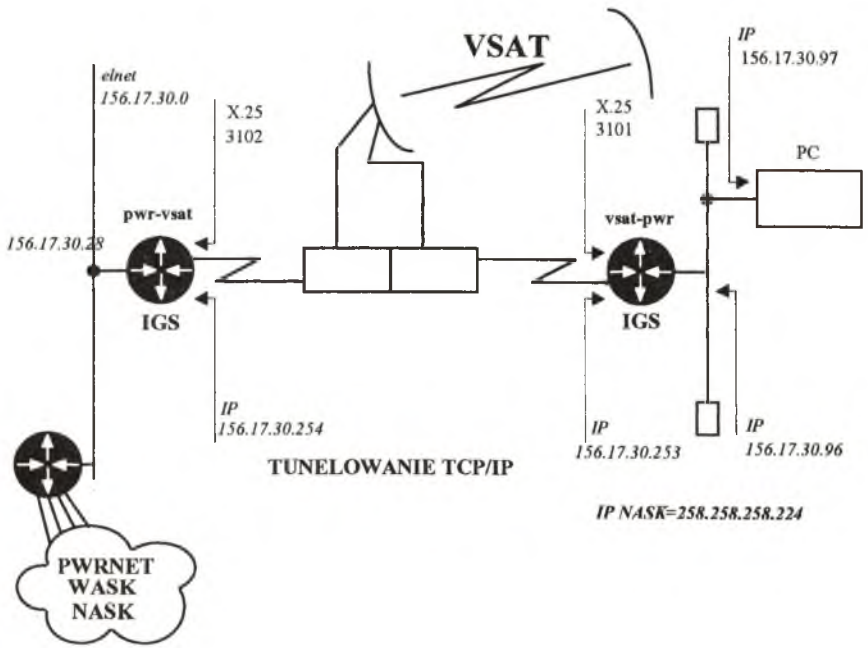
Rys. 22. Ilustracja zdarzeń w kanale z lokalnie synchronizowaną rezerwacją i dostępem ALOHA

nie zamierzonych pomiarów jakości świadczonych usług. Na operatorze ciąży bowiem konieczność odpowiedniej konfiguracji i monitorowania łącza satelitarnego oraz dostarczanie niezbędnych informacji. Telekomunikacja Satelitarna S.A. ma nowoczesny system VSAT firmy GTE Spacenet o nazwie Skystar Plus. System ten pozwala na działanie łącza satelitarnego w trybie dostępu losowego (szczelinowy protokół ALOHA) oraz rezerwacyjnego. Tryb dostępu jest dostosowany automatycznie w zależności od charakteru przesyłanych danych i obciążenia łącza. W celu dołączenia terminala VSAT zbudowano niezależną sieć komputerową, do której dołączono komputer z kartą X.25. Sieć ta jest połączona z częścią domową terminala VSAT poprzez ruter IGS. Dane generowane w tej sieci są transmitowane poprzez satelitę EUTELSAT II F4 do stacji centralnej sieci VSAT w Bielsku Białej. Konfigurację eksperymentalnego łącza satelitarnego przedstawiono na rys. 23. Stacja centralna została w taki sposób skonfigurowana, że dane są odpowiednio przeadresowywane i powtórnie transmitowane w kierunku satelity by po przejściu przez transponder zostać odebrane przez ten sam terminal VSAT. Jest to możliwe dzięki wyposażeniu terminala w uniwersalną kartę protokółów UPC. Karta ta ma cztery niezależnie programowane porty. Dwa z nich skonfigurowano odpowiednio do transmisji, zgodnie z protokółem X.25.

W przedstawionej na rysunku 23 konfiguracji odbywać się będą pomiary jakości usług świadczonych przez sieć VSAT.

6.1. Uniwersalna karta protokółów

Łączenie sieci VSAT z naziemnymi sieciami komputerowymi odbywa się poprzez uniwersalną kartę protokółów. Karta ta stanowi wysokiej klasy urządzenie przetwarzające dane i stanowiące interfejs pomiędzy urządzeniem użytkownika np. terminalem komputerowym lub procesorem czołowym i sterownikiem dostępu do satelity SAC *(ang. Satellite Access Controller)* oraz główną jednostką przetwarzającą MPU *(ang. Main*



Rys. 23. Eksperymentalna sieć VSAT

Processing Unit) stanowiącą część domową terminala VSAT. Uniwersalna karta protokółu może współpracować ze sterownikiem dostępu do satelity jak również z koncentratorem danych. Karta tego typu zapewnia:

- obsługę różnorodnych protokółów na tej samej platformie sprzętowej,
- wykorzystywanie procesora CPU w zakresie i z szybkością wymaganą przez użytkownika,
- udostępnienie pamięci RAM w rozmiarze wymaganym przez użytkownika,
- możliwość stworzenia do ośmiu interfejsów linii komunikacyjnych poprzez 4 (dla każdej linii) sterowniki podwójnych portów szeregowych 8530.

Uniwersalna karta protokółów udostępnia do ośmiu w pełni dupleksowych portów szeregowych. Protokoł portu i interfejs elektryczny może być wybrany indywidualnie dla każdego z portów. Karta wykorzystuje procesor z rodziny Motorola 68000 z 512 lub 1 Mb pamięci dynamicznej RAM. Dla diagnostyki i restartu systemu przewidziano 64 kb pamięci EPROM i 32 kb EEPROM.

6.2. Oprogramowanie uniwersalnej karty protokółów

Oprogramowanie rezydentne uniwersalnej karty protokółów zostało napisane w języku "C". Oprogramowanie to można podzielić na cztery kategorie:

- drajwery protokółów (PD),
- aplikacje transmisji danych (DTA),
- interfejs logiczny systemu zarządzania siecią (NMS/IL),
- opcjonalne oprogramowanie specjalistyczne.

Obsługa protokółów odbywa się poprzez drajwery protokółów i aplikacje transmisji danych. Drajwery protokółów (PD) obsługują we/wyj i tworzą ramki do transmisji do i z aplikacji transmisji danych (DTA). Aplikacje transmisji danych obsługują procesy odpowiedzi dla protokółów i transmisję end-to-end w kierunku łącza satelitarnego i od niego. Kody PD i DTA zależą od typu protokółu i tylko jedna kopia kodu jest potrzebna karcie do obsługi od jednego do ośmiu portów stosujących dany protokół. PD i DTA wykorzystują architekturę wielozadaniową do obsługi wielu linii i stacji. Nowe PD i DTA mogą być wprowadzone do karty bądź może być zmieniana konfiguracja bez potrzeby przeładowania karty i bez przerywania pracy na innych nie związanych z tą operacją portach. Obsługiwane mogą być co najwyżej cztery różne protokóły.

6.3. Drajwery protokółów

Drajwery protokółów PD *(ang. Protocol Drivers)* zostały opracowane w sposób dający się łatwo konfigurować. Współpracują one z wirtualnym środowiskiem użytkownika wykorzystując odpowiednie protokóły. Drajwery protokółów zostały opracowane dla protokółów:

- ASYNC
- BSC (2780/3780 i 3270)
- SDLC
- Burroughs Poll/Select
- X.25

6.4. Aplikacje transmisji danych

Aplikacje transmisji danych DTA *(ang. Data Transfer Applications)* są odpowiedzialne za odpowiednie rutowanie i funkcje sterowania ruchem. Aplikacje te sterują pracą drajwerów poprzez komendy read/write. Nagłówki rutowania są generowane dla każdego bloku danych przesyłanych przez łącze satelitarne.

6.5. Interfejs logiczny systemu zarządzania siecią

Interfejs NMS/IL *(ang. Network Management System Interface Logic)* odpowiada za współpracę uniwersalnej karty protokółów z systemem zarządzania siecią (NMS). Organizuje on stałą sesję z systemem zarządzania w stacji centralnej. W ciągu dnia dane statystyczne dotyczące uniwersalnej karty protokółów i stacji są wysyłane do systemu zarządzania. Dane diagnostyczne i komendy sterujące generowane w systemie zarządzania siecią interpretowane są przez interfejs logiczny i wykonywane poprzez inicjację odpowiednich wywołań do drajwerów. Interfejs ten formatuje również odpowiedzi dla systemu zarządzania. Wykryte przez oprogramowanie uniwersalnej karty protokółów błędy formatowane są do postaci wiadomości alarmowych i przesyłane do systemu zarządzania.

7. Transmisja protokółu X.25 w łączu satelitarnym

W eksperymencie skupiono się na wykorzystaniu łącza satelitarnego do transmisji danych według protokółu X.25. Od strony terminala protokół X.25 jest obsługiwany przez drajwer protokółu X.25, który obsługuje wszystkie linie tego typu oraz przez aplikację transmisji danych odpowiedzialną za sterowanie end-to-end oraz transmisję poprzez łącze. Aplikacja transmisji danych może komunikować się maksymalnie ze 100 innymi aplikacjami X.25. Dodatkowo, aby zapewnić połączenie poprzez terminal aplikacja obsługuje lokalne wywołania od jednej linii do drugiej należącej do tej samej uniwersalnej karty protokółów. Trudność tę należy w odpowiedni sposób ominąć w proponowanej strukturze sieci eksperymentalnej. Należy wymusić transmisję danych od jednego portu X.25 do drugiego portu X.25 poprzez łącze satelitarne. W przeciwnym przypadku karta dokona rutowania lokalnego z pominięciem łącza satelitarnego.

Zastosowana uniwersalna karta protokółu obsługuje protokół 1984 CCITT X.25 z ramkami typu: DM, UA, SABM, DISC, FRMR, RR, RNR , REJ, I, SABME.

Transmisja danych odbywa się z szybkościa do 19200 b/s bez DMA i do 56000 b/s przy wykorzystaniu dwóch kanałów DMA (jednego do nadawania i jednego do odbioru). Drajwer uniwersalnej karty protokółów wykorzystuje tabele rutowań wyjścia i wejścia do obsługi połączeń w sieci. Rutowania alternatywne są również możliwe.

Bibliografia

[1.] Alper R. J. i inni: *The book on VSATs*, Gilat Communications Ltd., 1991, Izrael
[2.] Bem D.J.: *Sieci satelitarne z małymi terminalami* Sat-Audio-Video, Nr 1, 1994, pp.36-39, Nr 2, 1994, pp. 40-43
[3.] Everett J. (redaktor): *VSATs very small aperture terminals*, Peter Peregrinus Ltd., London, 1992, UK
[4.] Killen H. B.: *Transmisja cyfrowa w systemach światłowodowych i satelitarnych*, WKiŁ, Warszawa, 1992
[5.] Maral G., Bousquet M.: *Satellite Communications Systems, Techniques and Technology*, Second Edition, John Wiley & Sons , 1993
[6.] Raychaudhuri D., Joseph K.: *Channel Access Protocols for Ku-band VSAT Networks: A Comparative Evaluation*, IEEE Communications Magazine, May 1988, Vol. 26, No. 5, pp. 34-44
[7.] Shimabukuro T. i inni: *VSATs for IBM SNA Networks*, GTE Spacenet Corp., 1992
[8.] Stratigos J., Mahindru R.: *Packet Switch Architectures and User Protocol Interfaces for VSAT Networks*, IEEE Communications Magazine, July 1988, Vol. 26, No. 7, pp. 39-47

Problemy konstrukcji systemów zarządzania bazami danych

Jerzy Brzeziński, Tomasz Koszlajda

1. Wstęp

Organizacja nowoczesnego społeczeństwa opiera się na szerokim zastosowaniu systemów informatycznych. Stanowią one podstawę systemów bankowych, systemów rezerwacji lotniczej, hotelowej i kolejowej, systemów administracyjnych, gospodarki materiałowej i magazynowej, systemów ewidencji ludności, systemów wspomagania projektowania i inżynierii oprogramowania, systemów zarządzania sieciami komputerowymi i telekomunikacyjnymi itp. Zdecydowana większość tych systemów jest konstruowana jako aplikacje rozproszonego systemu bazy danych.

Najogólniej rzecz biorąc, przez system bazy danych rozumiemy bazę danych i jej system zarządzania. Baza danych jest komputerową reprezentacją wybranego fragmentu świata rzeczywistego. Na przykład dla systemu bankowego reprezentacja ta dotyczy klientów banku, ich kont oraz operacji finansowych realizowanych na tych kontach. System zarządzania bazą danych jest natomiast zbiorem programów, które umożliwiają proste i efektywne operowanie na niej.

System zarządzania bazą danych powinien spełniać szereg wymagań dotyczących efektywności działania systemu, bezpieczeństwa danych, weryfikacji poprawności danych, określonych reguł dostępu do nich, możliwości równoległego dostępu do danych i ich geograficznego rozproszenia. Osiągnięcie tego celu wymaga jednak rozwiązania wielu problemów teoretycznych i implementacyjnych, takich jak: adekwatne modelowanie świata rzeczywistego, ochrona spójności i trwałości danych, zarządzanie współbieżnością wykonywania transakcji, autoryzacja dostępu do danych, fizyczne zarządzanie danymi, optymalizacja wykonywania operacji, zarządzanie rozproszoną bazą danych. Wymienione problemy są od kilkunastu lat przedmiotem intensywnych badań. Osiągnięte w tym zakresie wyniki teoretyczne zaowocowały już szeregiem produktów komercyjnych jak Oracle, Ingres, Sybase, Informix, O_2. Badania są jednak wciąż kontynuowane, gdyż uzykane dotychczas rozwiązania pozostawiają jeszcze pole dla dalszego rozwoju. Dziedziny tej w żadnym przypadku nie można uznać za zamkniętą. Niniejsza praca ma przybliżyć problemy konstrukcji systemów zarządzania bazami danych i podkreślić podstawowe znaczenie tej problematyki dla realizacji efektywnych i niezawodnych systemów informatycznych.

Rozdział drugi pracy omawia podstawowe pojęcia związane z bazą danych i modelem danych. Rozdział trzeci opisuje wymagane własności funkcjonalne systemów zarządzania bazą danych: trwałość i spójność danych, współbieżność dostępu do danych, autoryzację dostępu do bazy danych, optymalizację zapytań i zarządzanie rozproszoną bazą danych. Rozdział czwarty zawiera podsumowanie artykułu.

2. Baza danych

Baza danych jest komputerową reprezentacją (modelem) wybranego fragmentu świata rzeczywistego [Date81, Ullman82]. Przykładem takiego fragmentu jest: hurtownia, bank, wydział ewidencji ludności, firma ubezpieczeniowa, projekt samochodu itp . Świat rzeczywisty jest tu postrzegany jako zbiór wzajemnie powiązanych obiektów, przy czym mogą to być zarówno obiekty materialne (na przykład towary w hurtowni lub klientów firmy ubezpieczeniowej), zdarzenia (na przykład wypadek pociągający za sobą konieczność wypłacenia odszkodowania), lub pojęcia abstrakcyjne (takie jak salda, konta czy grupy marżowe).

Obiekty świata rzeczywistego charakteryzuje zbiór własności statycznych, zbiór własności dynamicznych i tożsamość. Przykładami statycznych własności obiektów są: nazwisko, imię i data urodzenia klienta firmy ubezpieczeniowej lub nazwa, cena i data produkcji towaru magazynowanego w hurtowni. Przykładami własności dynamicznych są wiek klienta firmy ubezpieczeniowej lub reakcja wału korbowego samochodu na naprężenia. Tożsamość obiektu jest to niezmienna własność obiektu, która umożliwia jego identyfikację niezależnie od zmieniających się jego własności statycznych i dynamicznych. Na przykład pozwala ona na jednoznaczną identyfikację osoby, która zmieniła imię, nazwisko, adres i płeć.

Obiekty świata rzeczywistego są powiązane różnymi związkami. Za przykład niech posłużą związek między towarem w magazynie a jego dostawcą, związek między klientem firmy ubezpieczeniowej a jego polisą ubezpieczeniową lub związek łączący cylinder z silnikiem samochodu.

2.1 Model danych

U podstaw każdego systemu bazy danych leży ***model danych*** [Date81, Ullman82, Lochovsky82, Codd81] będący zbiorem pewnych abstrakcyjnych pojęć, które umożliwiają opisanie w naturalny sposób wybranych fragmentów świata rzeczywistego i interpretację danych zawartych w bazie danych. W modelu danych wyróżnia się trzy podstawowe kategorie pojęć: ***struktury danych, więzy oraz operacje*** [Date81, Lochovsky82].

Struktury danych

Struktury danych umożliwiają opis statycznych własności obiektów świata rzeczywistego i łączących je związków. Struktura danych jest określonego rodzaju kolekcją - na przykład krotką, tablicą, listą lub zbiorem - atrybutów obiektu. Poszczególne atrybuty mogą przyjmować wartości z określonego zbioru nazywanego dziedziną atrybutu. Dowolna kombinacja wartości atrybutów obiektu tworzy ***stan obiektu***.

Aby umożliwić naturalny opis własności statycznych, zbiór struktur danych dostępny w danym modelu danych powinien być tak dobrany, aby umożliwiać reprezentację pojedynczego obiektu o dowolnej złożoności przez jedną daną o określonej strukturze. W tym celu niektóre modele danych pozwalają na definiowanie złożonych struktur danych przez ich zagnieżdżanie.

W celu wierniejszego oddania semantyki rzeczywistości, w niektórych modelach danych wyróżniono typy pewnych specyficznych związków łączących obiekty, zwane ***abstrakcjami*** [Smith77]. Abstrakcje służą do ukrycia szczegółów i skupieniu się na ogólnych, wspólnych cechach zbiorów obiektów. Wyróżnia się trzy typy abstrakcji: ***klasyfikację, uogólnienie i agregację***.

Klasyfikacja jest związkiem, który łączy obiekty tego samego typu, czyli dające się opisać przez tę samą strukturę danych. Związek ten łączy na przykład dwóch klientów tej samej firmy ubezpieczeniowej. ***Uogólnienie*** jest związkiem, który łączy obiekty bardziej ogólne z wyspecjalizowanymi. Związek taki łączy na przykład obiekt: ***pracownik*** z obiektami: ***sekretarka, agent ubezpieczeniowy i sprzątaczka. Agregacja*** obejmuje związki łączące złożone obiekty z obiektami składowymi. Przykładem agregacji są związki łączące obiekt ***samochód*** z obiektami: ***silnik, karoseria i podwozie***.

Struktury danych opisują zazwyczaj nie pojedyncze obiekty lecz zbiory obiektów tego samego typu czyli dających się opisać za pomocą takiej samej kolekcji atrybutów. Pojedyncze dane opisujące obiekty świata rzeczywistego są niezależnymi wystąpieniami tych struktur odzwierciedlającymi stan poszczególnych obiektów.

Więzy

Więzy, podobnie jak struktury danych, służą do opisu statycznych własności świata rzeczywistego. Przez specyfikację więzów wyklucza się niedozwolone stany obiektów. Na przykład, wypłata odszkodowania przez firmę ubezpieczeniową nie może być większa od wysokości ubezpieczenia. Specyfikacja takiej własności wyklucza pewne stany obiektu - te, w których odszkodowania byłyby większe od wysokości ubezpieczenia. Dzięki temu opis świata rzeczywistego przez bazę danych staje się pełniejszy i wierniejszy rzeczywistości.

Wyróżnia się trzy sposoby specyfikacji więzów: ***statyczną, dynamiczną i agregatową***. Specyfikacja statyczna nakłada ograniczenia na zbiór dozwolonych wartości atrybutów obiektu. Na przykład wartość atrybutu ***kolor_samochodu*** należy do zbioru wartości: ***biały, czerwony i granatowy***. Specyfikacja dynamiczna nakłada ograniczenia na zmiany wartości atrybutów obiektu. Na przykład dopuszczalne są następujące zmiany stanu cywilnego osób płci męskiej: z kawalera na żonatego, z żonatego na rozwiedzionego, z żonatego na wdowca, z wdowca na żonatego i z rozwiedzionego na żonatego. W związku z tym, niedozwolone są na przykład zmiany stanu cywilnego z kawalera na rozwiedzionego lub z kawalera na wdowca. Specyfikacja agregatowa nakłada ograniczenia na zagregowane wartości atrybutów zbioru obiektów. Na przykład suma płac pracowników przedsiębiorstwa nie może przekroczyć wysokości funduszu wypłat.

Oprócz ***więzów jawnych***, czyli jawnie specyfikowanych, model danych może także zawierać ***więzy wbudowane*** [Brodie78, Lochovsky82]. Ten rodzaj więzów wynika z immanentnych własności pewnych struktur danych przewidzianych w modelu danych. Innymi słowy, na mocy samej definicji struktury danych nie mogą pojawić się obiekty o określonej strukturze atrybutów lub pewne typy związków między obiektami. Na przykład w hierarchicznym modelu danych żaden związek nie może mieć innej struktury niż hierarchiczna.

Operacje

Operacje służą do opisu dynamicznych własności obiektów świata rzeczywistego. Modelują one reakcje obiektów na zewnętrzne pobudzenia. Na przykład obiekt ***wydział przedsiębiorstwa*** w wyniku zewnętrznego pobudzenia ***zwolnij pracownika*** zmieni swój stan przez modyfikację atrybutu ***liczba pracowników***, a obiekt ***belka*** w wyni-

ku zewnętrznego pobudzenia ***nacisk*** zmieni swój stan wewnętrzny przez modyfikację atrybutów opisujących kształt i wewnętrzne naprężenia belki.

Ze względu na możliwości modelowania dynamicznych własności obiektów świata rzeczywistego, modele danych można podzielić na dwie grupy. Do pierwszej zalicza się modele danych, które zawierają predefiniowany i niemodyfikowalny zbiór operacji. Modelowanie własności dynamicznych jest sprowadzone w tym wypadku do zastosowania określonych operacji na wystąpieniach określonych struktur danych. Jeżeli modelowane obiekty charakteryzują się własnościami dynamicznymi, którym nie odpowiadają żadne operacje modelu danych, to muszą one być zamodelowane poza modelem danych. Do drugiej grupy należą modele danych, które umożliwiają definiowanie nowych typów operacji na strukturach danych.

Procesy świata rzeczywistego są modelowane w bazie danych za pomocą aplikacji bazy danych, które są sekwencjami logicznie powiązanych operacji. Proponowane modele danych umożliwiają modelowanie procesów na jeden z dwóch sposobów: na zewnątrz lub wewnątrz struktur danych. W pierwszym podejściu struktury danych są elementami pasywnymi, pobudzanymi z zewnątrz przez aktywne procesy. Natomiast w drugim podejściu zakłada się, że struktury danych zintegrowane ze zbiorem właściwych dla nich operacji są elementami aktywnymi. Umożliwia to modelowanie świata jako zbioru aktywnych, wzajemnie komunikujących się obiektów.

3. Problemy konstrukcji systemów zarządzania bazą danych

System Zarządzania Bazą Danych - SZBD *(ang. Database Management System - DBMS)* jest programem, który umożliwia modelowanie danych i operowanie na nich. Narzędziem do specyfikacji struktur danych, więzów i operacji jest język definiowania danych *(ang. Data Definition Language - DDL)*. Specyfikacje struktur danych, więzów i operacji tworzą schemat bazy danych. Schemat umożliwia interpretację danych zawartych w bazie danych. Aktualny zbiór wartości wszystkich danych jest nazywany stanem bazy danych. Zbiór dostępnych operacji na stanie bazy danych stanowi język manipulacji danymi *(ang. Data Manipulation Language - DML)*. Język manipulacji danymi jest częścią języka tworzenia aplikacji bazy danych. Operacje wykonywane na bazie danych przez aplikacje w ogólności modyfikują jej stan. Zakłada się, że pomyślnie zakończona aplikacja pozostawia bazę danych w stanie spójnym, czyli zgodnym z stanem fragmentu świata rzeczywistego, który baza danych reprezentuje.

Aplikacje operujące za pomocą SZBD na bazie danych są zorganizowane w postaci zbiorów elementarnych jednostek interakcji z bazą danych zwanych transakcjami. ***Transakcja*** jest sekwencją logicznie powiązanych operacji, która posiada następujące własności: ***atomowość, trwałość i spójność*** [Bernstain87]. ***Atomowość*** oznacza, że jeżeli transakcja zawiera wywołania operacji zmieniających stan bazy danych, to wszystkie te operacje muszą być wykonane lub żadna z nich. ***Trwałość*** oznacza, że w przypadku pomyślnego zakończenia transakcji wszystkie zmiany wprowadzone przez nią do bazy danych nie zostaną później utracone nawet w wyniku awarii systemu. Własność ***spójności*** oznacza, że transakcja odwzorowuje spójny stan bazy danych w inny stan spójny, przy czym baza danych nie musi być w stanie spójnym w trakcie wykonywania transakcji.

Każda transakcja kończy się albo operacją ***zatwierdzenia*** *(ang. commit)* albo wycofania *(ang. abort, rollback)* danych wprowadzonych przez nią do bazy danych. Operacja zatwierdzenia jest inicjowana po pomyślnym wykonaniu wszystkich operacji składających się na transakcję. Natomiast operacja wycofania jest inicjowana w przypadku niepomyślnego zakończenia choćby jednej operacji składającej się na transakcję. Modyfikacje wprowadzone przez niepomyślnie zakończone transakcje należy traktować jako nigdy nie zaistniałe.

System zarządzania bazą danych musi mieć wbudowane mechanizmy, które zapewnią współbieżny dostęp wielu użytkowników do bazy danych, zagwarantują spójność i bezpieczeństwo danych w bazie danych, oraz zapewnią transparentny i efektywny dostęp do rozproszonej bazy danych. W związku z tym SZBD musi realizować funkcje ochrony spójności i trwałości danych, zarządzania współbieżnością transakcji, autoryzacji dostępu do danych, weryfikacji więzów, fizycznego zarządzania danymi, optymalizacji wykonywania operacji i zarządzania rozproszoną bazą danych [Gray93].

3.1 Ochrona spójności i trwałości danych

Ponieważ nie ma urządzeń w pełni niezawodnych, system bazy danych ma wbudowane mechanizmy ochrony danych na wypadek awarii komputera. Awaria komputera może doprowadzić do jednej z dwóch następujących sytuacji:

- zniszczenia danych w bazie danych w wyniku fizycznego uszkodzenia nośnika informacji;

– powstania niespójnego stanu bazy danych w wyniku przerwania wykonywania transakcji.

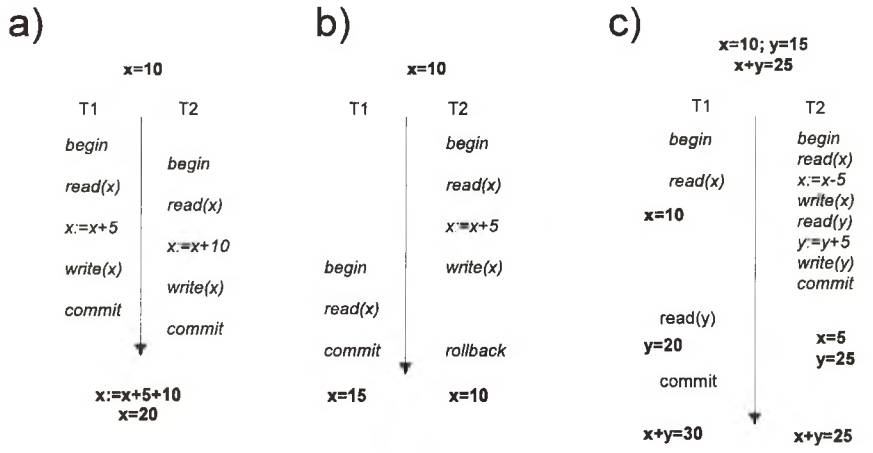
W systemach baz danych bezpieczeństwo danych jest zapewniane na drodze ich duplikowania. Każda operacja wstawiania, modyfikacji lub kasowania danych jest rejestrowana w specjalnym pliku zwanym ***rejestrem*** *(ang. log)*. W przypadku awarii, informacje zapamiętane w rejestrze służą do odtworzenia danych lub wycofania wyników operacji, w celu odtworzenia spójnego stanu bazy danych.

W przypadku awarii komputera, która spowodowała niespójny stan bazy danych, system bazy danych wycofuje niezakończone transakcje na podstawie zawartości rejestru. W przypadku awarii nośnika informacji i zniszczenia danych, system bazy danych odtwarza zawartość bazy danych sprzed momentu awarii na podstawie archiwalnej kopii bazy danych i zawartości rejestru, a następnie wycofuje modyfikacje wprowadzone przez niezakończone transakcje.

3.2 Zarządzanie współbieżnością transakcji

System bazy danych musi w ogólności obsługiwać strumień asynchronicznych i współbieżnych transakcji. Transakcje powinny być wykonywane współbieżnie w celu zwiększenia efektywności systemu. Jak wspomniano, każda pomyślnie zakończona transakcja przeprowadza bazę danych z jednego stanu spójnego do innego stanu spójnego. Jednakże z faktu, że każda transakcja wykonywana pojedynczo nie powoduje niespójności bazy danych, nie wynika poprawność realizacji całego zbioru współbieżnie wykonywanych transakcji. Transakcje mogą bowiem interferować ze sobą w wyniku operowania na tych samych danych, co w ogólności prowadzi do trzech rodzajów anomalii: utraty informacji, dostępu do niezatwierdzonych danych i niespójnego odczytu.

Utrata informacji *(ang. lost update)* jest wynikiem równoległej modyfikacji tej samej danej przez dwie lub więcej transakcji . Jeżeli dwie transakcje odczytują wartość tej samej danej i na podstawie odczytanej wartości wyznaczają jej nową wartość, którą następnie zapisują do bazy danych, to efekt jednego z tych zapisów zostanie zniszczony przez drugi zapis. W rezultacie nowa wartość danej nie będzie konsekwencją tych dwu modyfikacji, a jedynie wynikiem ostatniej z nich. Wynik pierwszej modyfikacji będzie bezpowrotnie stracony. Problem ten zilustrowano na rysunku 1.a. Transakcje T_1 i T_2 odczytują i modyfikują daną x. Transakcja T_1 zwiększa daną x o 5, a transakcja T_2 zwiększa ją o 10. Gdyby transakcje te były wykonywane sekwencyjnie wartość zmiennej x została by zwiększona o wartość 15. Jednakże w wyniku równoległego wykonywania tych transakcji modyfikacja wprowadzona przez transakcję T_1 została utracona.



Rysunek 1. Ilustracja interferencji współbieżnych transakcji

Dostęp do niezatwierdzonych danych (*ang. dirty read*) jest wynikiem odczytania przez transakcję wartości danej zmodyfikowanej przez inną niezakończoną transakcję. Anomalia typu dostęp do niezatwierdzonych danych polega na odczycie wartości danych, które później zostaną unieważnione z powodu niepomyślnego zakończenia transakcji, która im je nadała. Przypadek ten został zilustrowany na Rysunku 1.b. Transakcja T_1 odczytuje wartość danej x nadaną przez niezakończoną transakcję T_2. Następnie transakcja T_2 została wycofana. W wyniku, transakcja T_1 dysponuje błędną wartością zmiennej x. Nieodpowiada ona wartości zmiennej x ani przed ani po transakcji T_2.

Niespójny odczyt występuje w przypadku dwukrotnego dostępu przez transakcję do danych: przed ich modyfikacją przez inną współbieżnie wykonywaną transakcję i po pomyślnym zakończeniu modyfikującej je transakcji. W przypadku logicznych powiązań między tymi danymi transakcja otrzyma niespójny obraz bazy danych.

Przypadek niespójnego odczytu danej zilustrowano na Rysunku 1.c. Transakcja T_1 odczytuje dwie zmienne x i y, które są równolegle modyfikowane przez transakcję T_2.

System zarządzania bazą danych musi zapewnić poprawną, czyli wolną od anomali realizację współbieżnie wykonywanych transakcji. Istnieje wiele modeli transakcji właściwych dla różnych klas zastosowań systemów baz danych. Dla pewnej kategorii systemów informatycznych, wykorzystywanych na przykład w bankach, właściwy jest model w pełni izolowanych transakcji. W modelu tym za poprawną uważa się taką realizację współbieżnych transakcji, których wynik wykonania jest równoważny dowolnej sekwencyjnej realizacji tych transakcji [Bernstein87]. Jest to tak zwane ***kryterium uszeregowalności transakcji***. Z kolei inna kategoria systemów informatycznych służących jako systemy wspomagania projektowania wymaga modelu transakcji kooperujących, dla których kryterium uszeregowalności transakcji jest zbyt restrykcyjne. W modelu tym zakłada się, że pewne rodzaje interakcji między transakcjami nie są anomalią.

3.3 Autoryzacja dostępu do danych

Dane znajdujące się w bazie danych muszą być chronione przed niepowołanym dostępem. Niepowołany dostęp może przyjąć formę odczytu poufnych danych, nieuprawnionej modyfikacji danych lub zniszczenia danych. W związku z tym, system zarządzania bazą danych weryfikuje każdy dostęp do danych, umożliwiając jedynie uprawnionym osobom wykonywanie określonych operacji na określonych danych.

Weryfikacja osób uprawnionych do korzystania z bazy danych polega na identyfikacji i sprawdzaniu autentyczności użytkowników bazy danych. Weryfikacja danych, do których dostęp ma użytkownik, może być zrealizowana na poziomie struktur danych, poszczególnych wystąpień struktur danych lub wybranych atrybutów tych wystąpień. Weryfikacja operacji ogranicza sposoby dostępu do danych przez użytkownika do określonego podzbioru operacji.

3.4 Weryfikacja więzów

W celu weryfikacji więzów system zarządzania bazą danych musi monitorować wszystkie operacje wykonywane przez bieżące transakcje. W przypadku próby naruszenia więzów przez jakąś operację system zarządzania bazą danych może, w celu utrzymania spójnego stanu bazy danych, podjąć jedną z następujących akcji:

- odrzucić operację naruszającą spójność bazy danych lub całą zawierającą ją transakcję;
- nadać atrybutom wartości puste *(ang. null)* lub domyślne *(ang. default)*;
- wyzwolić kaskadę operacji, której celem jest przywrócenie spójności bazy danych;
- zasygnalizować lub zapamiętać naruszenie więzów.

Weryfikacja więzów może być natychmiastowa (po każdej operacji składającej się na transakcję), lub opóźniona do momentu zakończenia transakcji. Weryfikacja więzów ma na celu wyeliminowanie wielu błędów popełnianych przez użytkowników bazy danych. Pogwałcenie więzów oznacza bowiem, że albo interpretacja własności świata rzeczywistego jest niepoprawna albo stan bazy danych nie odpowiada stanowi świata rzeczywistego.

3.5 Fizyczne zarządzanie danymi

Fizyczna organizacja danych w bazie danych w istotny sposób wpływa na czas dostępu do nich. W celu skrócenia czasów wykonywania poszczególnych typów operacji są stosowane różne fizyczne organizacje plików danych, na przykład: pliki posortowane, wymieszane *(ang. hash)* lub stogowe *(ang. heap)*. Ponadto, dla przyśpieszenia operacji wyszukiwania danych na podstawie ich wartości są stosowane specjalne dodatkowe struktury danych zwane indeksami. Indeksy są plikami składającymi się z par: (wartość danej, adres bloku za-

wierającego daną o tej wartości). Pary te mogą być uporządkowane sekwencyjnie (mówi się wtedy o indeksie liniowym) lub tworzyć hierarchię (w przypadku indeksów hierarchicznych - [Elmasri89, Gray93]).

3.6 Optymalizacja wykonywania operacji

Efektywna implementacja struktur fizycznych nie jest równoznaczna z efektywnym operowaniem na nich. Złożone operacje mogą być realizowane na wiele sposobów istotnie różniących się czasami wykonywania. Poszczególne realizacje mogą różnić się kolejnością wykonywania operacji elementarnych składających się na operacje złożone i sposobem korzystania z fizycznych struktur danych. W związku z tym, system zarządzania bazą danych powinien posiadać mechanizm wyboru realizacji optymalnej w sensie czasu ze zbioru dopuszczalnych realizacji danej operacji złożonej.

3.7 Zarządzanie rozproszoną bazą danych

Rozproszony system zarządzania bazą danych (RSZBD), zapewnia efektywny i transparentny dostęp do geograficznie rozproszonych danych. W RSZBD rozproszone są zarówno same dane jak i proces zarządzania nimi. Rozproszony system bazy danych jest zbiorem RSZBD zlokalizowanych na komputerach połącznych siecią komputerową. Poszczególne RSZBD komunikują się ze sobą w celu optymalnej realizacji transakcji operujących na rozproszonych danych. W celu minimalizacji czasochłonnych transferów dużych wolumenów danych, na ogół poprzez sieć przesyłane są jedynie żądania wykonania operacji (do RSZBD zlokalizowanego na tym samym komputerze co przetwarzane dane) oraz wyniki tych operacji.

Transparentność dostępu do rozproszonych danych polega zasłonięciu przed użytkownikiem systemu bazy danych faktu rozproszenia danych. Pozwala to osiągnąć niezależność aplikacji bazy danych od sposobu lokalizacji danych. Dzięki temu te same aplikacje - bez jakiejkolwiek modyfikacji, będą poprawnie działały zarówno na scentralizowanej jak i rozproszonej bazie danych.

W celu osiągnięcia większej efektywności dostępu do danych oraz dla zwiększenia niezawodności systemu bazy danych w rozproszonych systemach baz danych jest stosowana replikacja danych. Pozwala ona na zastąpienie czasochłonnego zdalnego dostępu do danych zlokalizowanych na odległym węźle sieci - dostępem do lokalnej repliki tych danych. Ponadto w przypadku utracenia pewnych danych na jednym z węzłów sieci istnieje możliwość ich odtworzenia na podstawie ich replik utrzymywanych na innych węzłach sieci.

Zarządzanie w rozproszonym systemie bazy danych wiąże się ze znaczną komplikacją mechanizmów realizujących omówione już własności funkcjonalne SZBD [Cellary88]. Wprowadzenie RSZBD wymagało rozwiązania nowych problemów: zapewnienia globalnej spójności w rozproszonej bazie danych, rozproszonego zatwierdzania lub wycofywania transakcji, zarządzania rozproszonymi transakcjami, zapewnienia spójności i trwałości danych w przypadku wystąpienia nowych rodzajów awarii systemów (takich jak uszkodzenia sieci komputerowej) oraz optymalizacji zapytań rozproszonych.

4. Wnioski

Współczesne systemy informatyczne najczęściej są konstruowane w oparciu o systemy baz danych. Wykorzystanie systemu bazy danych odciąża konstuktora systemu informatycznego od konieczności rozwiązywania problemów związanych z efektywnym i poprawnym zarządzaniem wielodostępną i rozproszoną bazą danych. Podejście takie pozwala także istotnie zredukować czas realizacji systemu informatycznego oraz zwiększyć jego efektywność i niezawodność.

Problemy związane z zapewnieniem trwałości i spójności danych, współbieżnym dostępem do nich, autoryzacją dostępu do bazy danych, efektywnym dostępem do danych w środowisku scentralizowanym i rozproszonym są wspólne dla wszystkich zastosowań systemów baz danych. Dla pewnej klasy zastosowań baz danych, obejmującej systemy administracyjno-finansowe, znalazły one teoretyczne rozwiązania, co umożliwiło techniczną realizację systemamów komercyjnych, takich jak: DB2, Oracle, Ingres, Sybase, SQL/DS lub Informix.

Jednakże tematyka badań dotycząca zarządzania bazami danych jest ciągle otwarta. Pojawiają się nowe zastosowania systemów baz danych: systemy wspomagania projektowania, systemy zarządzania sieciami komputerowymi i telekomunikacyjnymi, bazy wiedzy , systemy wspomagania decyzji, itp. Charakteryzują się one specyficznymi modelami danych i transakcji. Pociąga to za sobą konieczność poszukiwania nowych rozwiązań dla problemów zarządzania danymi.

Relacyjne i obiektowe systemy baz danych

Tomasz Koszlajda

1. Wstęp

Systemy baz danych składające się z bazy danych (BD) i system zarządzania bazą danych (SZBD) są powszechnie stosowanym narzędziem do tworzenia różnego rodzaju systemów informatycznych. Wykorzystanie systemu bazy danych odciąża konstuktora systemu informatycznego od konieczności rozwiązywania problemów związanych z efektywnym i poprawnym zarządzaniem danymi.

Najogólniej rzecz *biorąc baza* danych jest komputerową reprezentacją wybranego fragmentu świata rzeczywistego. Przykładami takiego fragmentu są stany kont i dane personalne klientów banku, zasoby sieci komputerowej lub projekt nowego samochodu. Dane w bazie danych reprezentują stan poszczególnych obiektów świata rzeczywistego. Baza danych oprócz właściwych danych zawiera również ich interpretację odzwierciedlającą semantykę obiektów świata rzeczywistego. Do modelowania semantyki świata rzeczywistego w bazie danych są wykorzystywane pewne abstrakcyjne pojęcia składające się na *model danych* bazy danych. Pojęcia te powinny umożliwiać w sposób naturalny modelowanie w bazie danych statycznych i dynamicznych własności obiektów konkretnego fragmentu świata rzeczywistego.

System zarządzania bazą danych jest implementacją konkretnego modelu danych, która powinna charakteryzować się określonymi własnościami funkcjonalnymi. Do zbioru wymaganych własności funkcjonalnych należą: zagwarantowanie trwałości i spójności danych w bazie danych, zapewnienie współbieżnego dostępu do nich, autoryzacja dostępu do bazy danych, efektywny dostęp do danych w środowisku scentralizowanym i rozproszonym. Sposób implementacji tych własności silnie zależy od semantyki pojęć modelu danych.

Ekspansja informatyki we współczesnym świecie powoduje rozszerzanie się dziedziny zastosowań systemów baz danych. Poszczególne zastosowania różnią się nieraz istotnie semantyką odpowiadającego im fragmentu świata rzeczywistego. Na przykład systemy wspomagania projektowania różnią się od systemów bankowych dużo większą złożonością strukturalną danych, większą złożonością własności dynamicznych i innym sposobem interakcji między użytkownikami bazy danych. Potrzeba właściwego dopasowania pojęć modelu danych do własności modelowanego przez bazę danych fragmentu świata rzeczywistego powoduje, że pojawiające się nowe zastosowania danych pociągają za sobą konieczność poszukiwania nowych modeli danych i co za tym idzie nowych rozwiązań dla implementacji własności funkcjonalnych SZBD.

Zarówno w teorii jak i w praktyce - na rynku komercyjnym -zaproponowano wiele systemów baz danych. Z pewnym uproszczeniem można wyróżnić ich dwie podstawowe generacje: relacyjną i obiektową.

Relacyjne systemy baz danych powstały w latach siedemdziesiątych jako odpowiedź na zapotrzebowanie na informatyczne systemy administracyjno-finansowe. Relacyjne systemy baz danych opierają się na relacyjnym modelu danych wywiedzionym z algebry relacji, i na modelu transakcji zakładającym pełną niezależność transakcji.

Z kolei w latach osiemdziesiątych próby zastosowania systemów baz danych do systemów komputerowego wspomagania projektowania - CAD/CAM, systemów wspomagania inżynierii oprogramowania - CASE, systemów zarządzania sieciami komputerowymi, systemów kartograficznych i medycznych zaowocowały obiektowymi systemami baz danych. Obiektowe systemy baz danych są oparte na obiektowo-zorientowanym modelu danych *(ang. object-oriented data model)*, w którym kluczowym pojęciem jest pojęcie *obiektu*, który integruje strukturalne i operacyjne własności modelu danych. W dalszej części artykułu dla rozróżnienia od obiektów stanowiących elementy modelu obiektowego, obiekty świata rzeczywistego nazywać będziemy encjami *(ang. entity)*.

W tym artykule przedstawiono podstawowe charakterystyki relacyjnych i obiektowych baz danych. Rozdziały drugi i trzeci zawierają kolejno prezentację modelu danych i własności funkcjonalnych odpowiednich SZBD. Rozdział czwarty zawiera podsumowanie artykułu.

2. Relacyjne bazy danych

Relacyjny model danych został zaproponowany przez Codda w 1970 roku [Codd70]. Prace nad implementacją tego modelu i opracowaniem komercyjnego systemu zarządzania bazą danych były prowadzone do po-

czątku lat osiemdziesiątych. Najbardziej znane systemy prototypowe, które stały się później podstawą systemów komercyjnych, to System R opracowany przez firmę IBM w San Jose [Astrachan76] oraz system Ingres opracowany na Uniwersytecie Berkeley [Stonebraker76]. Najpopularniejsze obecnie systemy komercyjne to: Ingres, Oracle, DB2 i SQL/DS [Ingres90, Oracle90, Date88 i Date91].

Charakterystyka zastosowań

W latach siedemdziesiątych podstawową dziedziną zastosowań systemów baz danych była działalność finasowo-administracyjna przedsiębiorstw, bankowość, ubezpieczenia i systemy rezerwacji miejsc. Model świata rzeczywistego wystarczający do opisu tych dziedzin zastosowań charakteryzuje się prostymi typami encji, standardowymi własnościami dynamicznymi oraz nieskomplikowanymi i krótkimi transakcjami. Wartości atrybutów są ograniczone do zbiorów wartości numerycznych i krótkich łańcuchów znaków. Natomiast zbiór operacji jest ograniczony do operacji wstawiania, usuwania, modyfikacji i wyszukiwania informacji. Taka charakterystyka dziedziny zastosowań wpłynęła na własności relacyjnych systemów baz danych.

Model danych

Model relacyjny jest oparty na zaczerpniętym z teorii mnogości pojęciu relacji będącej podzbiorem iloczynu kartezjańskiego dziedzin. Iloczyn kartezjański dziedzin $D_1, D_2, ..., D_n$, zapisywany jako $D_1 \times D_2 \times ... \times D_n$ jest zbiorem wszystkich krotek $(v_1, v_2, ..., v_n)$ takich, że $v_1 \in D_1$, $v_2 \in D_2$ i $v_n \in D_n$. Relacją jest dowolny podzbiór powyższego iloczynu kartezjańskiego [Ullman81].

Istnieje alternatywna definicja relacji. Opiera się ona na pojęciu atrybutu relacji. Atrybuty relacji $A_1, A_2, ..., A_n$ są nazwami składowych $v_1, v_2, ..., v_n$ krotek relacji. Relacja jest zbiorem odwzorowań ze zbioru nazw atrybutów relacji $A_1, A_2, ..., A_n$ w zbiór wartości dziedzin atrybutów $D_1, D_2, ..., D_n$. Mówimy, że atrybut A_i jest zdefiniowany na dziedzinie D_i [Maier83].

W modelu relacyjnym *dziedziny* są predefiniowanymi zbiorami wartości. Wartości dziedzin są elementarne, to znaczy nierozkładalne na części składowe. Wartości danej dziedziny należą do tego samego typu danych. Poszczególne relacyjne bazy danych różnią się oferowanym zbiorem typów danych, jednakże propozycje nie wykraczają poza typy numeryczne, znakowe, daty i przedziały czasu. Niektóre relacyjne bazy danych oferują ponadto specjalny typ danych do przechowywania niesformatowanych, dużych wolumenów danych - BLOB *(ang. Binary Large Object)*. Typ ten umożliwia przechowywanie w bazie danych długich tekstów, obrazów lub innych nietypowych informacji. Model relacyjny nie oferuje jednak żadnych środków do interpretacji tego typu danych. Dane te są przechowywane w postaci worka bajtów *(ang. bag)*.

Relacja jest jedynym typem struktury danych występującym w modelu relacyjnym. W związku z tym służy ona do reprezentacji zarówno encji jak związków między encjami. Struktura relacji opisana jest przez schemat relacji. Schemat relacji jest zbiorem nazw atrybutów zdefiniowanych na określonych dziedzinach. Krotki relacji są reprezentantami poszczególnych encji opisanych tym samym schematem relacji. Tożsamość krotek wynika z unikalności kolekcji wartości atrybutów, które składają sie na krotkę. W związku z tym wyróżnia się pewne podzbiory atrybutów relacji, których wartości jednoznacznie odróżniają poszczególne krotki relacji. Podzbiory te są nazywane kluczami relacji, a jeden z nich jest wyróżniony jako klucz główny relacji.

Związki między encjami są modelowane przez relacje, których atrybutami są klucze główne relacji reprezentujących powiązane encje. Z trzech wyróżnionych w literaturze rodzajów abstrakcji, model relacyjny oferuje tylko klasyfikację.

Definicja relacji wnosi do modelu relacyjnego zbiór więzów wbudowanych. W znormalizowanym modelu relacyjnym można wyróżnić trzy rodzaje więzów wbudowanych. Pierwszy z nich wynika z faktu, że dziedziny są zbiorami wartości elementarnych. W związku z tym wartości atrybutów relacji również muszą być elementarne. Drugi rodzaj więzów wbudowanych jest spowodowany tym, że odwzorowania, które składają się na relację, są funkcyjne. W połączeniu z ograniczeniem elementarności wartości dziedzin, wynika z tego, że wartości atrybutów relacji nie mogą być wielowartościowe. Trzeci rodzaj więzów wbudowanych jest konsekwencją faktu, że relacja jest zbiorem krotek. Wynika stąd zakaz istnienia krotek o tych samych wartościach wszystkich atrybutów.

Model relacyjny przewiduje również definiowanie więzów jawnych. Standard ANSI (SQL89) [Shaw90] języka relacyjnej bazy danych przewiduje możliwość definiowania więzów ograniczających dziedziny atrybutów i więzów referencyjnych. Więzy ograniczające dziedziny atrybutów umożliwiają zawężenie zbioru wartości dziedzin. Więzy referencyjne umożliwiają zdefiniowanie zależności funkcyjnych między atrybutami relacji. Obydwa rodzaje więzów należą do kategorii więzów statycznych.

Operacje wykonywane na relacyjnej bazie danych są zazwyczaj adresowane do wybranych krotek relacji. W związku z tym wszystkie operacje muszą być poprzedzone wyselekcjonowaniem podzbioru krotek, do których są adresowane. Ponieważ tożsamość krotek wynika z wartości ich atrybutów, zatem ich adresowanie polega na wyszukaniu krotek, których wartości atrybutów spełniają określone warunki wyboru. Operacje umożliwiające wyszukiwanie krotek spełniających określone warunki tworzą język zapytań. Na język zapytań składa się siedem podstawowych operacji relacyjnych: *selekcji, projekcji, produktu kartezjańskiego , połączenia, sumy* relacji, *iloczynu* relacji i *różnicy* relacji [Date 81]. Operacje relacyjne są operacjami specyfikacji, ponieważ nie wymagają określenia jak należy szukać określonych danych, lecz podają warunki jakie dane te muszą spełniać. Operacje relacyjne mogą być łączone w złożone zapytania w celu precyzyjnego wyselekcjonowania dowolnego podzbioru danych.

Proponowane dla modelu relacyjnego języki zapytań dzieli się na dwie klasy: języki oparte na algebrze relacji oraz języki oparte na rachunku predykatów. W przypadku języków algebraicznych zapytania wyraża się za pomocą operatorów stosowanych do relacji. Natomiast w językach opartych na rachunku predykatów zapytania opisują żądany zbiór krotek przez podanie predykatu, który krotki muszą spełniać. Języki oparte na rachunku predykatów są dalej dzielone na dwie kategorie, w zależności od tego czy obiektami pierwotnymi są krotki, czy elementy dziedzin atrybutów. Te dwie kategorie są nazywane relacyjnym rachunkiem krotek i relacyjnym rachunkiem dziedzin [Ullman 82]. Przykładem języka algebraicznego jest język *ISBL* [Todd76], relacyjnego rachunku krotek - język *Quel* [Stonebraker76], natomiast relacyjnego rachunku dziedzin - język *Query-by-Example* [IBM78]. Standardem języków zapytań stał się jednak język *SQL* [Chamberlin76] będący językiem pośrednim między algebrą relacji a relacyjnym rachunkiem krotek.

Na grupie krotek wyselekcjonowanych z bazy danych za pomocą złożenia dowolnej liczby operacji relacyjnych można następnie wykonać jedną z operacji manipulowania danymi. Mogą to być operacje wstawiania, modyfikacji lub usuwania krotek.

Wymienione powyżej operacje stanowią zbiór predefiniowanych operacji modelu relacyjnego. Modelowanie niestandardowych własności dynamicznych umożliwiają w modelu relacyjnym *procedury wyzwalane (ang. triggered procedures)*. Procedura wyzwalana jest sekwencją predefiniowanych operacji, uaktywnianą w wyniku wystąpienia pewnego zdarzenia pod określonymi warunkami. Zdarzenia są określonymi operacjami wykonywanymi na określonych danych. Ze względu na trudności efektywnej implementacji, procedury wyzwalane są stosunkowo rzadko oferowanym elementem modelu danych w komercyjnych systemach baz danych.

Własności systemu zarządzania bazą danych

Dla relacyjnych baz danych zaproponowano wiele metod zarządzania współbieżnością transakcji. Można wyróżnić dwa główne podziały tych metod na metody jednowersyjne i K-wersyjne oraz na metody blokowania, znaczników czasowych i metody optymistyczne [Bernstein87, Gray93]. Prawie wszystkie komercyjnie dostępne bazy danych stosują metody blokowania danych.

W związku z nielicznym zbiorem operacji modelu relacyjnego metody blokowania wymagają jedynie dwóch typów blokad: współdzielonej blokady do odczytu i wyłącznej blokady do zapisu. Spośród różnych metod blokowania najczęściej jest stosowana metoda blokowania dwufazowego *(ang. Two-Phase Locking)* [Bernstein87]. Polega ona na wydzieleniu w transakcjach dwóch faz: zakładania i zdejmowania blokad.

Metody blokowania działają optymalnie w środowisku krótko trwających transakcji. Długo trwające transkacje wymagają utrzymywania przez długi czas dużej liczby blokad, co w istotny sposób ogranicza stopień współbieżności. Sposobem na zwiększenie stopnia współbieżności jest stosowanie K-wersyjnych metod blokowania [Hadzilacos86, Morzy92].

W relacyjnych systemach baz danych, dla większości operacji jednostką autoryzacji danych jest cała relacja. Jedynie dla operacji modyfikacji autoryzacja może dotyczyć poszczególnych atrybutów relacji. Do bardziej precyzyjnego ograniczenia praw dostępu są wykorzystywane relacje wirtualne nazwane perspektywami *(ang. view)*. Perspektywy są relacjami wywiedzionymi z innych relacji za pomocą operacji relacyjnych. Użytkownicy bazy danych mogą nie posiadać prawa dostępu do relacji bazowych, lecz mieć nadane prawo dostępu do perspektyw wywiedzionych z tych relacji. Odpowiednie zdefiniowanie perspektywy może, na przykład, umożliwiać dostęp jedynie do informacji statystycznych wywiedzionych z danych znajdujących się w relacji, bez udostępniania informacji szczegółowych, lub do dowolnego podzbioru krotek i atrybutów relacji bazowej.

Relacje są fizycznie reprezentowane jako pliki, w których format rekordu składa się z jednego pola dla każdego atrybutu ze schematu relacji. Języki definiowania danych najczęściej umożliwiają użytkownikowi wybór odpowiedniej organizacji tych plików. Dostępne opcje to organizacja wymieszana, indeksowo-sekwencyjna lub stogo-

Model danych

Model obiektowy jest oparty na przejętym z języków obiektowo-zorientowanych pojęciu obiektu. Obiekty umożliwiają modelowanie własności statycznych i dynamicznych encji. Własności statyczne encji są modelowane za pomocą struktury obiektu, a ich własności dynamiczne za pomocą metod, czyli procedur skojarzonych z obiektami.

Obiekty o takiej samej strukturze i metodach są grupowane w klasy. Obiekty należące do danej klasy są jej *wystąpieniami (ang . instance)*. Klasa pełni rolę zarówno definicji wystąpień klasy jak i zbioru wszystkich swoich wystąpień.

Struktura obiektów jest określona przez zbiór nazwanych atrybutów. Atrybuty są zdefiniowanych na dziedzinach, które są zbiorami wartości elementarnych, takich jak liczby naturalne, liczby rzeczywiste, czy łańcuchy znaków, lub klasami. Atrybuty obiektów mogą być wielowartościowe. Atrybuty zdefiniowane na zbiorach wartości elementarnych są nazywane atrybutami prostymi , natomiast zdefiniowane na klasach są nazywane atrybutami złożonymi.

Formalnie, przez obiekt rozumie się dwójkę: *o = (oid, v)*, gdzie *oid* jest unikalnym *identyfikatorem obiektu*, a *v* jest wartością obiektu [Abiteboul89]. Wartość obiektu, w zależności od jego struktury, może być wartością atrybutu, krotką wartości lub zbiorem wartości. Wartość atrybutu prostego jest wartością elementarną, a wartość atrybutu złożonego jest obiektem. Powyższa definicja jest rekurencyjna, a poziom zagnieżdżania struktur jest nieograniczony. Dzięki temu za pomocą struktury obiektów można modelować encje o dowolnej złożoności.

Identyfikatory obiektów określają tożsamość obiektu niezależnie od stanu wartości jego atrybutów. Dwa obiekty o takich samych wartościach atrybutów pozostają różne. Stąd w modelu obiektowym wyróżnia się pojęcia równości i identyczności obiektów. Własność ta wyraźnie odróżnia obiekty od krotek z modelu relacyjnego.

Model obiektowy *explicite* obejmuje pojęcia różnych typów związków między obiektami i między klasami. Atrybuty złożone definiują związki między obiektami. Ten typ powiązań nazywa się *związkiem referencyjnym*. Dwa obiekty są powiązane związkiem referencyjnym jeżeli jeden z nich jest wartością atrybutu drugiego. Związki referencyjne umożliwiają modelowanie związków typu: *Jan_Kowalski jest mężem Janiny_Kowalskiej*, lub *Jan_Kowalski posiada samochód Polonez_1500.*

Szczególnym rodzajem związku referencyjnego jest związek kompozycji (ang. is-part-of lub composite reference). Związek ten umożliwia modelowanie sytuacji, w której jedna encja jest częścią składową drugiej encji, a więc na przykład związku: silnik_1500_TD jest_częścią samochodu Polonez_1500. Obiekt, który wiąże inne obiekty związkiem kompozycji jest nazywany obiektem złożonym *(ang. complex lub composite object)*, natomiast obiekty związane związkiem kompozycji są nazywane obiektami składowymi *(ang. component object)*. Obiekty składowe również mogą być złożone, a zatem obiekt złożony jest w ogólności hierachią obiektów składowych. Związek kompozycji nadaje obiektom składowym dodatkową semantykę. Obiekty składowe są zależne *(ang. depend)* i powiązane w sposób wyłączny *(ang. exclusive)* przez obiekty złożone. Zależność obiektów składowych polega na tym, że ich istnienie jest zależne od istnienia zawierających je obiektów złożonych. Z kolei wyłączność zawierania obiektów składowych polega na tym, że mogą one należeć tylko do jednego obiektu złożonego. Związek kompozycji jest abstrakcją agregacji. Umożliwia on automatyczne wykonywanie pewnych operacji na wszystkich powiązanych nim encjach.

Związki referencyjne, które nie są związkami kompozycyjnymi są nazywane *słabymi związkami referencyjnymi (ang. weak reference)* [Kim87].

Paradygmat obiektowy przewiduje możliwość definiowania nowych klas na podstawie klas już istniejących. Definicja nowej klasy jest rozszerzeniem definicji klasy istniejącej. Powoduje to powstanie specyficznego związku między tymi klasami, zwanego *związkiem dziedziczenia*. Zbiór wszystkich klas powiązanych związkiem dziedziczenia tworzy acykliczny i skierowany *graf dziedziczenia (ang. inheritance lattice)*. Korzeniem tego grafu jest zazwyczaj predefiniowana klasa: *Obiekt*. Semantycznie, związek dziedziczenia odpowiada abstrakcji uogólnienia, ponieważ nawigacja wzdłuż krawędzi grafu dziedziczenia w kierunku korzenia grafu powoduje przechodzenie od klas bardziej wyspecjalizowanych do klas bardziej ogólnych.

Model obiektowy umożliwia modelowanie dynamicznych własności encji za pomocą *metod obiektów*, których specyfikacja, obok specyfikacji struktury obiektów, wchodzi w skład definicji klasy obiektów. Struktura obiektów oraz implementacja metod są ukryte przed użytkownikiem obiektu. Własność ta jest nazywana *hermetycznością* obiektu *(ang. encapsulation)*. Komunikacja z obiektem odbywa się przez wysyłanie do obiektu

któw, takich jak projekt samochodu, czy oprogramowanie systemu operacyjnego, jednostką autoryzacji są pojedyncze obiekty. Ponadto model autoryzacji uwzględnia specyficzne powiązania miedzy obiektami. Ten typ autoryzacji jest nazywany *autoryzacją domyślną (ang. implicite authorization)* [Rabitti88]. Jej mechanizm polega na dedukowaniu praw dostępu do obiektów na podstawie jawnie wyspecyfikowanej autoryzacji dostępu do obiektów z nimi powiązanych. Na przykład mechanizm ten może być wykorzystany do autoryzacji domyślnej obiektów należących do hierarchii kompozycji przy jawnej autoryzacji korzenia tej hierarchii.

W relacyjnych bazach danych relacje są implementowane w postaci plików danych w ten sposób, że jedna relacja jest implementowana przez jeden plik. W przypadku obiektowych baz danych duże rozmiary obiektów, ich złożona struktura i pewne typy związków między obiektami wymusiły wprowadzenie nowych sposobów fizycznej organizacji danych. Pojedyncze duże obiekty są reprezentowane przez całe pliki danych. Pliki te mają złożoną hierachiczną strukturę umożliwiającą efektywne operowanie na poszczególnych atrybutach obiektu [Carey86]. W celu efektywnego nawigowania wzdłuż związków kompozycji, obiekty składające się na hierarchię kompozycji są przechowywane w spójnym obszarze fizycznym.

Złożone atrybuty obiektów oraz hierachia dziedziczenia klas spowodowały wprowadzenie nowych rodzajów indeksów. Są to tak zwane *indeksy wielo-klasowe (ang. multi-class index)*. Indeksy te wyróżniają się tym, że adresują obiekty należące do wielu klas. Ze związkiem dziedziczenia są związane indeksy zakładane na atrybutach klas tworzących podgraf grafu dziedziczenia. Na przykład indeks wielo-klasowy może być utworzony na atrybucie *data_urodzenia* klas: *sekretarka, sprzątaczka, kierownik i inżynier*, tworzących podgraf, którego korzeniem jest klasa pracownik. Z kolei atrybuty złożone są związane z indeksami wielo-klasowymi, zakładanymi na atrybutach klas leżących na ścieżce utworzonej przez związek między klasą zawierającą atrybut złożony i klasą stanowiącą dziedzinę tego atrybutu.

4. Podsumowanie

Zarówno w teorii jak i w praktyce - na rynku komercyjnym - zaproponowano wiele systemów baz danych. Różnią się one między sobą przyjętym modelem danych oraz funkcjonalnymi własnościami systemu zarządzania bazą danych. Można wyróżnić dwie generacje systemów baz danych: relacyjną i obiektową. O ile jednak różnice między różnymi relacyjnymi systemami baz danych są nieznaczne, to dla obiektowych baz danych różnice te są znacznie większe. Dotyczą one zarówno modelu danych jak i własności funkcjonalnych SZBD.

Większość systemów baz danych była tworzona jako narzędzia uniwersalne, możliwe do wykorzystania w dowolnej dziedzinie zastosowań. Jednakże zastosowania systemów baz danych typowe dla okresu ich tworzenia rzutowały na własności modelu danych i systemu zarządzania.

Wartościujące porównania modeli danych i systemów zarządzania bazą danych należących do różnych generacji nie mają specjalnego sensu. Nie ma bowiem jednego najlepszego, uniwersalnego systemu bazy danych. Wartościować systemy baz danych można jedynie w kontekście konkretnego ich zastosowania. Można mówić o lepszym lub gorszym dopasowaniu pojęć modelu danych i funkcji systemu zarządzania bazą danych do wymagań związanych z danym zastosowaniem.

Bibliografia

[Abiteboul89] Abiteboul S., P.Kanellakis, *Object Identity As A Query Language Primitive*, Proc. of ACM SIGMOD Intl. Conf. on the Management of Data, 1989.

[Agraval89a] Agraval R., N.H.Gehani, *ODE (Object Database and Enviroment): The Language and the Data Model*, Proc. ACM-SIGMOD Int'l Conf. Management of Data, Portland, Oregon, May-June 1989, pp.36-45.

[Astrachan75] Astrachan M.M., D.D.Chamberlin, *Implementation of a structured Englisch query language*, ACM Communication, Vol.18, No.10, 1975.

[Astrachan76] Astrachan M.M., et al., *System R: a relational approach to data management*, ACM Transaction on Database Systems, Vol.1, No.2, 1976.

[Bancilhon89] Bancilhon F., C.Delobel, P.Kannelakis, *The O_2 Book*, Altair 1989.

[Banerjee87] Banerjee J., H. Chou, J.F.Garza, W.Kim, D.Woelk, N.Ballou, H.Kim, *Data Model Issues for Object-Oriented Applications*, ACM Transaction on Office Information Systems, 5, 1, pp. 311-322, 1987.

[Rabitti88] Rabitti F.D., W.Woelk, W.Kim, *A Model of Authorization for Object-Oriented and Semantic Databases*, Proc. Intl. Conf. on Extending Database Technology, Wenecja, March 1988.

[Schwarz83] Schwarz P.M., A.Z.Spector, *Synchronizing Shared Abstract Types*, Technical Report CMU-CS-83-163, Department of Computer Science, Cornegie-Mellon University, November 1983.

[Shaffert86] Schaffert C., et al., *An Introduction to Trellis/Owl*, Proc. 1st Intl. Conf. on Object-Oriented Programming Systems, Languages, and Applications, Portland (Oregon), Sept. 1986.

[Shaw90] Shaw P., *Database Language Standards: Past, Present and Future, Database Systems of 90s*, Proceedings International Symposium Mtggelsee, Berlin 5-7 listopada 1990 roku; strony 55-80.

[Skarra89] Skarra A.H., S.B.Zdonik, *Concurrency Control and Object-Oriented Databases, Object-Oriented Concepts, Databases, and Applications*, edited by W.Kim i F.H.Lochowsky, ACM Press, Addison Wesley Publ. Comp., 1989.

[Stonebraker76] Stonebraker M., E.Wong, P.Kreps, G.Held, *The design and implementation of INGRES*, ACM Transaction on Database Systems, Vol.1, No.3, 1976.

[Stroustrup86] Stroustrup B., *The C++ Programming Language*, Addison-Wesley Publ. Comp, 1986.

[Todd76] Todd S.J.P., *The Peterlee realtional test vehicle - a system overview*, IBM Systems Journal, 1976.

[Ullman82] Ullman J.D., *Principles of Database Systems*, 2nd Ed., Computer Science Press, Inc., 1982.

[Wilkerson89] Wilkerson B., A. Wirfs Brock, *Variables Limit Reusability' Journal of Object-Oriented Programming*, Vol.2, No. 1.1989.

Sł. Michalski

Wojciech Denkis Poczta Polska URM

PS: ~~dlaczego~~ czy ~~zapewnienie~~ zab
są autoryzacja podpisu i integralność bo
dlaczego urzęd nie zamienia tożsamości modem

Sławomir Michalski:
Poczta X400 w publicznej sieci transmisji danych
POLKOM X400 opracowana przez Michalskiego

Sosnowiec Sieci metropolitalne w TPSA

Studium wykonalności budowy
Sieci Metropolitalnej (MAN)
Kwiecień 1999
symetryczne 64 – 2MB
asymetryczne 19.6

Bydgoszcz 5
Warszawa 17

Dawek Widzierewicz ATM
customer@atom.com.pl

~~zacząć~~ się

Cav:
1) W przyszłym tygodniu
Rada Koordynacyjna d/s Telekomunikacji
Ogólnokrajowe Urządzenie Rządowe Służb
Telekomunikacyjnych Państwa
koordynacja i nadzór działalności ~~odbiorców~~ p
przedsiębiorstw przesyłów
koordynacja współpracy między
a ~~ośrodkiem~~ na wzór Rady Telekomunikacyjnej
państwowej d/s cyfryzacji
z NBNu, Główny Urząd Ceł, OUS, MF
Min Trans, PKP, Polska sieć, Min Łącz, MON
Zapewnienie
NBP
Sejm
5 osobowe prezydium
~~Biuro~~ Doradcze
Zespół Doradczy
Szkolenie koordynacja informacja

do Urzędu ~~ma~~ dostęp do internetu
Centralnego Państwowego. Wypożyczenie sprzętu
bezpłatnie, pracownicy z pełnym

sie struktura i metodami, a mających taki sam protokół. Własność umożliwi