Naukowa i Akademicka Sieć Komputerowa

oraz

Telekomunikacja Polska S.A.

Materiały seminarium

MIEDZESZYN '95

10-12 maja 1995 r.

Spis Treści

Wstęp

W dniach 10-12 maja 1995 r. w Miedzeszynie odbywa się piąte już seminarium NASK. W tym roku jest ono organizowane wspólnie przez Naukową i Akademicką Sieć Komputerową oraz Telekomunikację Polską SA.

Ugruntowała się już tradycja, że spotkania w Miedzeszynie mają charakter roboczy. Stanowią one okazję do dokonania przeglądu nowości w dziedzinie budowy i eksploatacji rozległych sieci komputerowych, ale przede wszystkim są forum do dyskusji na jakże gorące tematy związane z rozwojem telekomunikacji i teleinformatyki.

Także i w tym roku chcemy zachować jego charakter. Tegoroczne seminarium stanowi jednocześnie próbę rozszerzenia podejścia tylko technicznego poprzez uwzględnienie w programie zagadnień ekonomicznych, prawnych i socjologicznych, wiążących się z funkcjonowaniem sieci komputerowych. Obserwowany w ostatnich latach gwałtowny i żywiołowy rozwój Internetu budzi wiele pytań i refleksji nad kierunkami rozwoju sieciowej komunikacji oraz konsekwencjami społecznymi rozszerzania się tej formy przesyłu informacji. Chcielibyśmy, aby "Miedzeszyn '95" stał się okazją do wymiany poglądów i doświadczeń operatorskich także i pod tym kątem.

Tomasz Hofmoki
Andrzej Zienkiewicz

Naukowa i Akademicka Sieć Komputerowa

NASK

W tym roku odbywa się piąte już z kolei seminarium NASK w Miedzeszynie. Po raz pierwszy natomiast organizowane jest wspólnie z Telekomunikacją Polską S.A. Rok temu inaugurując seminarium mówiliśmy o zmianach organizacyjnych jakie zaszły w zakresie budowania i organizowania obsługi rozległej sieci znanej pod nazwą NASK (Naukowa i Akademicka Sieć Komputerowa). Rok temu przedstawialiśmy podjęte decyzje organizacyjne i projekty na przyszłość. W niniejszej prezentacji przedstawimy podstawowe fakty i omówimy bieżącą działalność.

Powołanie NASKu

Po rozważeniu wielu możliwych rozwiązań Komitet Badań Naukowych powołał zarządzeniem Nr 5/93 Przewodniczącego Komitetu Badań Naukowych z dnia 14 grudnia 1993 r. Jednostkę Badawczo Rozwojową pod nazwą Naukowa i Akademicka Sieć Komputerowa. W dniu 30 grudnia 1993 r. Przewodniczący Komitetu Badań Naukowych zarządzeniem Nr 7/93 ustalił regulamin wyborów Rady Naukowej JBR NASK pierwszej kadencji określając liczebność Rady na 12 członków. Wybory do Rady Naukowej odbyły się 4 stycznia 1994 r. i tego samego dnia odbyło się pierwsze posiedzenie Rady na którym wybrano na przewodniczącego prof. dr hab. Andrzeja Wierzbickiego z Politechniki Warszawskiej a na wiceprzewodniczących prof. dr hab. Daniela J. Bema z Politechniki Wrocławskiej oraz dr Macieja Kozłowskiego z Centrum Astronomicznego im Kopernika w Warszawie. Nowa jednostka została zarejestrowana w Sądzie Rejonowym dla m.st. Warszawy w dniu 14 lutego 1994 r.

Formalne powołanie nowej jednostki zapoczątkowało dopiero żmudny proces przekształcania zespołów pracujących dotychczas w kilku miejscach a przede wszystkim na Uniwersytecie Warszawskim w jeden organizm. Wszystkie zmiany musiały odbywać się w taki sposób aby nie zakłócić działania sieci.

Sądzimy, że w znacznej mierze udało się wypełnić tak postawione zadanie.

Współpraca ze środowiskiem użytkowników

Od samego początku poszukiwaliśmy rozwiązań pozwalających na zabezpieczenie interesów całego środowiska naukowego i akademickiego w zakresie działalności nowo powołanej jednostki. Dlatego też Rada Naukowa NASKu na posiedzeniu w dniu 24 lutego 1994 r. rozważała problem stworzenia mechanizmów zabezpieczających interesy całego środowiska naukowego i akademickiego w Polsce w zakresie tworzenia i utrzymania sieci komputerowych. Postanowiono zaproponować powołanie Rady Użytkowników Sieci NASK. Kierownictwo NASKu zwróciło się do Rektorów Wyższych Uczelni, Dyrektorów Instytutów Polskiej Akademii Nauk oraz Dyrektorów Jednostek Badawczo Rozwojowych z listem, w którym czytamy:

.....dążąc do stworzenia możliwie dobrego sprzężenia zwrotnego między potrzebami środowiska i działalnością NASKu proponujemy powołanie Rady Użytkowników sieci NASK. Rozważając możliwe mechanizmy utworzenia takiego ciała proponujemy rozszerzenie koncepcji zaproponowanej przez Komitet Badań Naukowych na posiedzeniu w dniu 17 listopada 1993 r. W uchwale tej Komitet Badań Naukowych nakłada obowiązek powołania Rad Użytkowników przez

Porozumienia Środowiskowe w tych ośrodkach, w których ze środków Komitetu powstają miejskie sieci komputerowe (MAN) i są instalowane komputery dużej mocy. Proponujemy aby każde porozumienie środowiskowe wybrało swego przedstawiciela do Rady Użytkowników NASK. W ośrodkach, w których takie Porozumienie jeszcze nie zostało zawarte a istnieje połączenie z siecią szkieletową NASK, przedstawicielem środowiska mógłby być jeden reprezentant uczelni i placówek naukowych danego ośrodka wybrany w drodze odrębnego porozumienia tych jednostek. Rolą Rady użytkowników NASK powinno być, naszym zdaniem, między innymi wypowiadanie się na temat długofalowych projektów technicznych rozwoju i utrzymania sieci w Polsce z punktu widzenia interesu użytkowników

Dziś mogę powiedzieć, że Rada taka powstała w dniu 5 stycznia 1995 roku. Przewodniczącym jej został wybrany prof. dr hab. Marian Noga z Krakowa. Ustalono skład Rady. Są w niej reprezentowane wszystkie Rady Użytkowników oraz te ośrodki, w których jest zainstalowany węzeł NASKu. Na dzień dzisiejszy skład ten przedstawia się następująco: Maciej Kozłowski - Warszawa, Jerzy Ludwichowski - Toruń, Jan Zarzycki - Wrocław, Marian Noga - Kraków, Zbigniew Mikurenda - Łódź, Krzysztof Nałęcki - Górny Śląsk, Zdzisław Szyjewski - Szczecin, Stanisław Paszczyński - Rzeszów, Antoni Nowakowski - Gdańsk, Marek Miłosz - Lublin, Jacek Rychlewski - Poznań, Henryk Piech - Częstochowa, Włodzimierz Gogołek - Radom, Zbigniew Sender - Kielce, Władysław Poszewiecki - Olsztyn, Marek Malinowski - Płock, Maciej Stolarski - Białystok, Paweł Skalski - Zielona Góra, Grzegorz Pietrzyński - Opole, Janusz Szykowny - Toruń.

Powołano również Prezydium Rady w składzie: Jacek Rychlewski - Poznań, Krzysztof Nalecki - Gliwice, Stanisław Starzak - Łódź, Jerzy Ludwichowski - Toruń, którego celem jest bieżąca współpraca z Dyrekcją NASK w okresie pomiędzy zebraniami Rady. Rada jeszcze nie ustaliła regulaminu swojego działania.

Zgodnie z ustawą o jednostkach badawczo rozwojowych przeprowadzono konkurs na stanowisko dyrektora NASK, w wyniku którego został na nie powołany 27 czerwca 1994 r. prof. dr hab. Tomasz Hofmokl.

Współpraca z MAN'ami

Rok temu podnosiliśmy wagę współpracy z Miejskimi Sieciami Komputerowymi budowanymi w 11 miastach w Polsce.

Pisaliśmy:

Bardzo ważnym i niedocenionym zagadnieniem jest współpraca NASKu z sieciami miejskimi (MANami) Możliwe są dwa warianty współdziałania. Operator sieci miejskiej posiada uprawnienia operatorskie przyznane przez Ministerstwo Łączności i zawiera z NASKiem umowę międzyoperatorską lub jeżeli nie posiada uprawnień korzysta z uprawnień operatorskich NASKu. W tym drugim przypadku NASK sprawuje nad MANem nadzór formalny i jest pośrednikiem między MANem a Ministerstwem Łączności w przekazywaniu dokumentów. Każde z tych rozwiązań jest do przyjęcia. Niestety w wielu ośrodkach rysuje się możliwość, że kosztem dużych wysiłków sieć będzie zbudowana a nie będą załatwione formalności ani w wariancie pierwszym ani w drugim.

Sprawa ta jest już dziś jednoznacznie rozstrzygnięta. Na posiedzeniu w Ministerstwie Łączności w dniu 8 marca 1995 r. w obecności Podsekretarza Stanu w Komitecie Badań Naukowych Pani Minister Małgorzaty Kozłowskiej, zostało ustalone, że Jednostki Wiodące w każdym środowisku wystąpią o odpowiednie uprawnienia operatorskie. NASK jako operator sieci zawrze następnie z nimi odpowiednie porozumienia międzyoperatorskie. Takie rozwiązanie wydaje się być najprostsze.

Dzięki istnieniu Rady Użytkowników NASKu, możliwe jest już teraz koordynowanie wielu działań a na obecnym etapie uzgodnienie cenników usług w poszczególnych ośrodkach. Podkreślamy, że nie chodzi o narzucanie jakichkolwiek rozwiązań a jedynie o uzgadnianie zasad tworzenia cenników.

Współpraca z innymi operatorami

Generalnie NASK, poza układami metropolitalnymi, nie buduje własnej struktury łącz fizycznych. Łącza fizyczne analogowe i cyfrowe są dzierżawione od innych operatorów. Podstawowym partnerem NASK'u w tym zakresie jest TP SA. Współpracujemy również z Telbankiem i Teleenergo. W relacjach międzynarodowych partnerami NASK'u są Nordunet, E bone oraz DATAPAK - organizacje sieciowe w Szwecji i Austrii.
Rok temu podkreślaliśmy wagę współpracy z innymi operatorami pisząc:

Niezwykle ważną dla sprawnego funkcjonowania NASKU jest współpraca z Telekomunikacją Polską SA. TP SA jest głównym dostarczycielem łącz telekomunikacyjnych. Sieć NASK jest i będzie w dającej się przewidzieć przyszłości ściśle zintegrowana z sieciami publicznymi administrowanymi przez Telekomunikację Polską SA oraz innymi sieciami działającymi w jej otoczeniu.

Przez cały ubiegły rok trwała intensywna współpraca z Telekomunikacją Polską SA zarówno w zakresie technicznym jak i organizacyjnym. Od strony technicznej przeprowadzono udany moim zdaniem eksperyment wspólnego wykorzystywania łącz międzymiastowych co dało środowisku naukowemu i akademickiemu możność korzystania z łączy o przepływności 2 Mbps . Doświadczenie ubiegłego roku pokazało, że nasze środowisko wykorzystuje szerokopasmowe łącza bardzo nierównomiernie. Obciążenie średnie łączy 2 Mbps w relacjach międzymiastowych nie przekraczało 15%, ale wykorzystanie chwilowe sięgało powyżej 90%. Łączy się to z charakterem pracy - w czasie przesyłania zbiorów obciążenie linii wzrasta prawie do maksimum a w czasie na przykład pracy interakcyjnej jest bardzo małe. Byłoby więc nieuzasadnione ani technicznie ani ekonomicznie dzierżawienie (przynajmniej na obecnym etapie) tak szybkich łączy tylko dla środowiska naukowego.

Na poparcie tej tezy przytoczę wyniki analizy zamieszczonej w numerze grudniowym Data Communication. Zgodnie z tą analizą przewiduje się, że wzrost dochodów z dzierżawy linii spadnie z 9% w 1994 roku do 8% w 1995 roku i będzie dotyczył linii o stosunkowo małej przepływności (56/64 kb/s). To znaczy, że mimo wzrostu ruchu zmniejszy się dynamika zapotrzebowania na łącza dzierżawione. Przewidywania stają się zrozumiałe jeżeli przyjrzymy się jak szybko wchodzi do eksploatacji technologia frame relay i ATM (Asynchronous Transfer Mode). Porównanie lat 1993, 1994 i przewidywań dla roku 1995 przedstawia się następująco:

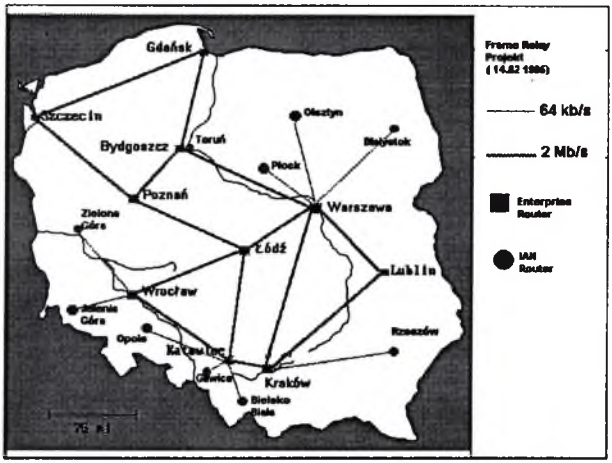
Wyrażone w milionach USD

	1993 dochód	1994 dochód	1994 wzrost w %	1995 dochód ocena	1995 wzrost w %
linie dzierżawione	11,445	12,475	9	13,473	8
usługa X25	1,412	1,567	11	1,708	9
frame relay	77	231	200	739	220
ATM	–	12	–	60	400

Widać wyraźnie, że technologia frame relay i ATM prawdopodobnie zdominują rynek. Nie będzie się opłacało dzierżawić linii dla wąskiego grona użytkowników. Nie będzie ona na ogół

efektywnie wykorzystana. Znacznie bardziej uzasadnione będzie korzystanie wspólnie z innymi użytkownikami z sieci ,w której jest frame relay i wykorzystywanie takiej przepływności pasma jakie jest w danej chwili potrzebne. To samo można powiedzieć o technologii ATM z tą tylko różnicą, że jest ona uzasadniona w sieciach o bardzo dużej przepływności i jeszcze cierpi na brak uzgodnień ostatecznych standardów.

Jest duże prawdopodobieństwo, że w najbliższym czasie topologia sieci rozległej (międzymiastowej) ulegnie zmianie. Dotychczasowa konfiguracja gwiazdy zostanie zastąpiona "siecią" składającą się z trójkątów o następującym kształcie:



Współpraca zagraniczna:

Sieci siłą rzeczy nie znają granic. NASK ma bardzo ścisłe kontakty zagraniczne z operatorami sąsiadujących krajów. Można je podzielić na dwa rodzaje:

- Kontakty operacyjne w ramach utrzymania sieci. Należy tu bezpośrednia współpraca z NORDUNETem, DATAPAKiem, ACONETem, sieciami ukraińskimi, białoruskimi i rosyjskimi. Austriacka organizacja sieciowa ACONET współfinansuje linię o przepływności 128 kb/s z Warszawy do Wiednia. Umowa jest w rzeczywistości trójstronna. Ponieważ ACONET w ramach polityki z krajami naszego regionu zobowiązuje się finansować połowę kosztów połączenia linii o przepływności 64 kb/s nie tylko do Polski ale i do innych krajów Zostało uzgodnione, że sfinansuje połowę linii 128 kb/s do Warszawy a NASK sfinansuje linię do Lwowa. W ten sposób środki zostały lepiej wykorzystane. NASK finansował również linię 9.6 kb/s do Moskwy. Dalsze utrzymywanie tej linii jest nieuzasadnione. NASK zobowiązał się do partycypowania w kosztach linii cyfrowej 64 kb/s z chwilą gdy partner rosyjski znajdzie środki na swoją część. Cała współpraca zagraniczna, implikująca wydatki po stronie polskiej, została uzgodniona z Komitetem Badań Naukowych i przez niego z Radą Ministrów.
- Kontakty na poziomie organizacji sieciowych.
  NASK aktywnie uczestniczy w pracach organizacji sieciowych.

1. W roku 1994 doprowadził do powstania organizacji CEENet (Central and Eastern European Networking Association) skupiającej organizacje sieciowe krajów Europy Środkowej i Wschodniej i reprezentującej ich interesy na forum międzynarodowym. Organizacja ta zyskuje coraz większą popularność. W chwili powstania liczyła siedmiu członków. Obecnie jest ich już 19. Są to Albania, Austria, Białoruś, Bułgaria, Chorwacja, Czechy, Estonia, Gruzja, Litwa, Łotwa, Macedonia, Mołdawia, Polska , Rumunia, Rosja, Słowacja, Słowenia, Ukraina i Węgry. Prezesem CEENet jest dyrektor NASKu Prof Tomasz Hofmokl. W ramach organizacji uzyskano fundusze z Fundacji Sorosa na zainstalowanie węzła WWW z informacjami o tych krajach. Sprzęt został zakupiony i zainstalowany w Polsce. Uzyskano również środki na organizację szkoły-warsztatów sieciowych w roku 1995 w Warszawie

2. W kadencji 1993 - 1994 dyrektor NASKu Prof T. Hofmokl był wybrany członkiem Komitetu Wykonawczego EARNu. W ramach podziału obowiązków zajmował się rozwojem sieci w Krajach Europy Wschodniej. W roku 1994 zostały zorganizowane warszataty sieciowe EARNu dla pracowników organizacji sieciowych z krajów nowo podłączonych.

3. Po połączeniu się dwóch sieciowych organizacji europejskich RARE i EARN w jedną TERENA (Trans European Research and Educational Networking Association) przedstawiciele NASKu są w zgromadzeniu ogólnym organizacji (Prof. Daniel J. Bem i Prof. T. Hofmokl)

4. Zostało podpisane porozumienie z firmą Ascom Timplex SA z Belgii w zakresie możliwości wspólnych działań w dziedzinie budowy i utrzymania sieci oraz szkoleń.

Bezpieczeństwo sieci:

W NASKu został utworzony Zespół d/s Bezpieczeństwa Sieci. Zajmuje się on zarówno zagadnieniami prawnymi bezpieczeństwa w sieci jak i wyborem oraz wdrożeniem oprogramowania specjalnego. W ramach umowy zawartej pomiędzy Komitetem Badań Naukowych a NASKiem nawiązano współpracę z Wyższą Szkołą Oficerską Wojsk Łączności w Zegrzu. Zespół Specjalistów z tej uczelni podjął się całościowego rozpatrzenia aspektów związanych z bezpieczeństwem sieci NASK. W ramach działania własnego zespołu uruchomiono system pozwalający na gwarancję całości przesyłanego dokumentu oraz autoryzację podpisu.

Okazało się po dokładnej analizie, że poważnym problemem jest niezadowalający stan prawny w tej dziedzinie. NASK nie ma prawnej możliwości wyłączenia z sieci użytkownika, który narusza regulamin wewnętrzny NASKu i na przykład łamie zabezpieczenia rozszyfrowując hasła. Analizujący zagadnienie prawnicy zasugerowali rozwiązanie aby elementy regulaminu włączać do umów cywilnych zawieranych z użytkownikami. Dalsza współpraca z Wyższą Szkołą Oficerską Wojsk Łączności może zaowocować w opracowaniu przejrzystych schematów organizacji sieci i postępowania prawnego zapewniającego maksymalne bezpieczeństwo informacji i niezawodności sieci.

Działalność promocyjno wydawnicza:

Podstawowym zadaniem w tej dziedzinie jest promowanie usług sieciowych jako narzędzia badań naukowych. Zrealizowana cały szereg zadań cząstkowych. Można wśród nich wymienić:

1. Wydawnictwa - wydano 2 książki:

   - "Przewodnik po sieci Internet" (OPI, 2 tys. egz.);
   - "Naukowa i Akademicka Sieć Komputerowa" (OPI, 2 tys. egz.);

2. Działalność informacyjno-promocyjna:

- produkcja ulotki informacyjnej nt. stanu i perspektyw rozwoju sieci NASK/WARMAN;
- organizacja i obsługa informacji on-line o NASK na gopherze NASK i serwerze WWW;
- nawiązanie współpracy w celu regularnego wydawania biuletynu informacyjnego "NASK" - dodatku do "PC-Kurier" w ramach umowy z wydawnictwem Lupus (pierwszy numer biuletynu ukazał się 5 stycznia 1995 r.);
- regularne przygotowywanie i rozsyłanie informacji prasowej, a także udział w konferencji prasowej nt. działalności NASK i postępów w budowie sieci WARMAN;
- stała współpraca z wieloma tytułami. Są to m.in.: "PC Kurier", "ComputerWorld", "Enter", "Rzeczpospolita", "Świat Telekomunikacji". Z inspiracji i przy współpracy NASK powstało i zostało opublikowanych kilkanaście dużych artykułów prasowych popularyzujących wiedzę o NASK i WARMAN;

3. Udział w konferencjach i wystawach:

- zorganizowano IV Seminarium NASK w Miedzeszynie k. Warszawy. Wzięło w nim udział 120 uczestników reprezentujących środowisko użytkowników sieci NASK oraz w części wystawowej zaprezentowało się 15 firm wiodących na rynku technologii teleinformatyki w Polsce;
- zorganizowano stoiska NASK na "Euroinfo" (czerwiec'94) i na "Infofestiwalu" (listopad '94). W ramach tych stoisk odbywały się pokazy usług internetowych ze szczególnym uwzględnieniem WWW;
- przedstawiciel NASK zaprezentował problematykę "Internetu dla Szkół" na stoisku w ramach wystawy "Komputer i Człowiek" (grudzień '94).
- przedstawiciele NASK przestawili problematykę sieci rozległej dla środowiska naukowego i akademickiego ze szczególnym uwzględnieniem NASK jako referenci w trakcie kilkunastu konferencji i i seminariów naukowych, w których brali udział w 1994 r.

4. Szkolenia: pracownicy Działu Informacji i Baz Danych NASK prowadzili regularne szkolenia użytkowników NASK (średnio ok. 6 szkoleń w miesiącu).

5. Badania końcowych użytkowników NASK: We współpracy z Agencją Badań Społecznych i Rynkowych RUN przygotowany został kwestionariusz badania sondażowego użytkowników sieci NASK.

Badania Naukowe:

Realizacja badań statutowych NASK

Badaniami naukowymi zajmują się dwa zespoły: we Wrocławiu pod kierunkiem prof D.J. Bema oraz w Poznaniu pod kierunkiem prof J. Brzezińskiego. W roku 1994 opublikowano 30 pozycji wliczając w to materiały konferencyjne. Zajmowano się następującymi zagadnieniami:

Strategia przechodzenia do asynchronicznego trybu transmisji (ATM) w sieciach metropolitalnych i w sieci krajowej.
Zapoznano się z najnowszymi trendami producentów sprzętu sieciowego w przechodzeniu do technologii ATM. Przedstawiono artykuł na konferencji POLMAN 94 w Poznaniu w maju 1994 roku. Uczestnictwo w konferencji NETWORKERS '94 FIRMY CISCO w Barcelonie w październiku 1994. Zebrano materiał na temat możliwych podejść do implementacji technologii ATM. Dokonano analizy porównawczej urządzeń ATM oferowanych przez różnych producentów z punktu widzenia ich wykorzystania w sieciach metropolitalnych i w sieci krajowej. Rozpoczęto formułowanie założeń strategii przejścia do ATM w sieciach metropolitalnych i w sieci krajowej.

Zarządzenie i monitorowanie sieci NASK
Zapoznano się z dostępnymi platformami do zarządzania siecią. Porównano platformy SunNet Manager i HP OpenView. Zaimplementowano system zarządzania dla sieci miejskiej - zbudowanej w oparciu o urządzenia firmy CISCO - na bazie platformy SunNet Menager z oprogramowaniem CISCO Works. Zdobyte doświadczenia pozwolą na określenie możliwości wykorzystania istniejących systemów do zarządzania i monitorowania sieci NASK. Wyniki prac przedstawiono na konferencjach w Miedzeszynie i w Poznaniu .

Badania mediów transmisyjnych stosowanych w sieciach komputerowych z punktu widzenia kompatybilności elektromagnetycznej.
Zapoznano się z istniejącymi normami i zaleceniami dotyczącymi pomiarów parametrów różnych typów mediów stosowanych w sieciach komputerowych opracowano metodykę pomiaru parametrów elektrycznych

kabli współosiowych. Przygotowano procedury wspomagające proces pomiarowy z wykorzystaniem sterownika IEEE 488. Zgromadzono materiał badawczy z pomiarów ponad 100 typów kabli. W ramach współpracy z Politechniką Wrocławską w 1994 roku. Opracowano i uruchomiono stanowisko do badań skuteczności ekranowania metodą "wstrzykiwania". Zdobyte wcześniej doświadczenia przy pomiarach homologacyjnych kabli współosiowych pozwoliły określić zestaw niezbędnej aparatury pomiarowej. Zamówiono sprzęt pomiarowy, który został dostarczony w końcu listopada 1994 roku. Po otrzymaniu sprzętu kontynuowane są badania mediów transmisji danych wykonano sieć lokalną w oparciu o skrętkę i kabel współosiowy, która jest badana z punktu widzenia kompatybilności elektromagnetycznej mediów transmisyjnych.
Dotychczasowe wyniki badań stały się podstawą do otworzenia zespołowego (dwie osoby) przewodu doktorskiego. Przedstawiono je także na Seminarium COST 243 w Budapeszcie w listopadzie 1994 roku .

Przygotowanie grantu pakietowego
Opracowano założenia do grantu pakietowego dotyczącego badania, analizy i wdrażania nowych technik i technologii mogących znaleźć zastosowanie w projektowaniu, budowie i eksploatacji sieci teleinformatycznych, które rozesłano do wszystkich potencjalnych realizatorów. Wobec braku zainteresowania, zrezygnowano z przygotowania grantu pakietowego.

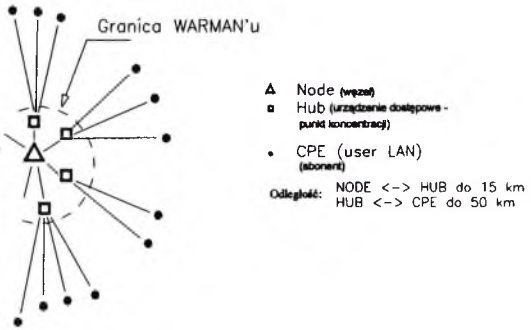
Doraźne ekspertyzy na potrzeby ZINISN
Opracowano trzy ekspertyzy na potrzeby ZINISN i Zespołu ds. Infrastruktury Informatycznej:
-. Sieci lokalne,
- Kryteria oceny sieci lokalnych,
- Syntetyczna informacja o sieci lokalnej.
Ekspertyzy te zostały włączone do "Programu Rozwoju Infrastruktury Informatycznej dla Polskich Środowisk Naukowych (PRI)".

Systemy baz danych w zarządzaniu sieciami komputerowymi
Badania dotyczyły :
- analizy związków modelu zarządzania ISO/OSI z systemami obiektowych baz danych, wyniki badań przedstawiono w Raporcie NASK i zgłoszono do publikacji ;
- problemów konstrukcji systemów zarządzania bazami danych ze szczególnym uwzględnieniem zagadnień optymalizacji wykonywania transakcji i zarządzania współbieżnością w obiektowych i relacyjnych bazach danych, wyniki badań przedstawiono na Konferencji NASK w Miedzeszynie i zgłoszono do publikacji ;
- oceny efektywności i problemów konstrukcji heterogenicznych, rozproszonych systemów baz danych na przykład baz danych Oracle i X.500, wyniki badań zawarto w Raporcie NASK, a także przedstawiono na Konferencji w Gdańsku i zgłoszono do publikacji .

Zrealizowanie pilotowej instalacji poczty elektronicznej według standartu X.400
Wykonano następujące prace :
- Uruchomiono węzeł wejściowy (RELAY-MTA) poczty X.400 dla sieci NASK w środowisku GO-MHS. Środowisko GO-MHS skupia sieci naukowe i akademickie Europy Zachodniej, a także USA, Indii, Chin, Słowenii, Chorwacji, Węgier, Litwy, Tunezji.
Przetestowano prawidłowość połączenia między węzłem RELAY-MTA sieci NASK i węzłami RELAY-MTA w wymienionych krajach.
- Uruchomiono dwa węzły MTA: we Wrocławiu i Toruniu.
- Uruchomiono adaptery między środowiskiem X.400 i SMTP (Internet) oraz środowiskiem SMTP i X.400.
- Opracowano plany rozwojowe instalacji węzłów MTA w sieci NASK. Plany te przewidują instalacje przynajmniej jednego węzła MTA w każdym regionie. W tym celu zarejestrowane prywatne domeny administracyjne dla każdego regionu. W planach rozwojowych przewiduje się integracje wszystkich sieci rozległych w Polsce poprzez pocztę X.400.
- Trwają prace nad wdrożeniem nowego licencjonowanego oprogramowania IC 2. Iv2.
Wdrożenie będzie możliwe po przystąpieniu JBR NASK do ISODE CONSORTIUM (Zespół posiada to oprogramowanie uzyskane jako tzw. ZERO COST LICENCE dla Politechniki Wrocławskiej).
- Trwają prace nad wdrożeniem oprogramowania UA (User Agent) w środowisku MS-Windows i XT-Windows. Oprogramowanie UA zapewnia łatwy dostęp do węzła MTA z odległego komputera.
- Wyniki prac przedstawiono na Seminarium NASK w Miedzeszynie, zostaną także przedstawione na Krajowym Sympozjum Telekomunikacji w Bydgoszczy.

Warman

Mówiąc o działalności NASKu nie można pominąć budowy miejskiej sieci szkieletowej WARMAN. Będzie temu poświęcona osobna prezentacja. Dlatego w tym miejscu podajemy tylko podstawowe informacje. Budowana w Warszawie metropolitalna sieć komputerowa WARMAN (Warszawski MAN) ma objąć swoim zasięgiem wszystkie dzielnice Warszawy, tak by umożliwić dostęp do sieci placówkom naukowym i akademickim oraz innym abonentom, w tym administracji państwowej. Główna struktura sieci bazuje na około 10 węzłach oraz urządzeniach dostępowych podłączonych do tych węzłów. Idea struktury węzła oraz urządzeń dostępowych została pokazana na rysunku.



Komunikacja pomiędzy węzłami odbywać się będzie na dedykowanych liniach światłowodowych z szybkością 155 Mb/s SDH. Protokołem w sieci jest ATM (Asynchronous Transfer Mode). Również urządzenia dostępowe będą podłączane w analogiczny sposób.
Wybór technologii ATM umożliwia także, przy wykorzystaniu tej samej struktury fizycznych połączeń szkieletu sieci, stworzenie wirtualnych sieci logicznych, rozłącznych z punktu widzenia zarządzania, dostępu do zasobów itd., dla różnych podmiotów. Np. **mogą to być odseparowane sieci wirtualne uczelni, administracji państwowej oraz innych abonentów**.
Technologia ATM umożliwia także, co zostało potwierdzone w naszym laboratorium przekazywanie obrazu i głosu na potrzeby video konferencji oraz łączenie central telefonicznych.
Koncepcja sieci WARMAN była przedmiotem wielokrotnych uzgodnień pomiędzy operatorem sieci rządowej - Biurem Łączności KGP. W wyniku tych uzgodnień została podpisana umowa pomiędzy MSW a NASK, która między innymi zakłada wspólną budowę i eksploatację infrastruktury sieci WARMAN. Założenia Techniczno-Ekonomiczne były również opiniowane przez Dyr. W. Łuczywo z Biura Informatyki URM.

Zgodnie z projektem oraz przyjętym harmonogramem, w pierwszym etapie planuje się uruchomienie sześciu węzłów:

UW - Krak. Przedmieście (uruchomiony),
PW - Pl. Politechniki 1 (uruchomiony),
Zgrupowanie Ochota (uruchomione częściowo)

SGGW -
CUP - Żurawia 4 - do uzgodnienia (światłowód istnieje),
URM - do uzgodnienia (j.w.),

oraz punkty koncentracji w CRiT przy ul. Barbary 2, Centrali Telefonicznej przy ul. Pięknej oraz PKiN.

Węzły planowane w drugiej połowie tego roku, to:

Wola - Instytuty PAN przy ul. Kasprzaka,
Mokotów - Instytut Fizyki w Al. Lotników,
Praga - prawdopodobnie Instytut Transportu Samochodowego, ul. Jagiellońska,
Żoliborz - IMGW i/lub Instytuty przy ul. Rydygiera.

Ponadto wykorzystując fakt położenia "na drodze" naszej inwestycji obiektów administracji państwowej, infrastruktura światłowodowa została wprowadzona do:

Ministerstwa Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa,
Ministerstwa Łączności,
Ministerstwa Transportu,
Ministerstwa Finansów,
GUSu.

Planowane w bieżącym roku jest uwzględnienie także Komitetu Badań Naukowych.
Lista nie obejmuje tych relacji, które pozostają w gestii BŁ KGP, a istotnie uzupełniają powyższe zestawienie.

Regulamin i cennik NASKu

Zgodnie z wymogami ustawy o łączności opracowano w ubiegłym roku regulamin i cennik usług świadczonych przez NASK. Uważamy, że regulamin ma w naszej sytuacji bardzo ważne znaczenie. Jak wykazała analiza uregulowań prawnych w zakresie działalności sieciowej istnieją w tej dziedzinie bardzo poważne luki. Dlatego wszelkie uregulowania muszą w chwili obecnej być zawarte w umowach zawieranych między dostarczycielem usług a usługobiorcą. Regulamin jest w tym przypadku traktowany jako nieodłączna część umów zawieranych z abonentami. Dlatego wydaje się, że warto go przytoczyć w całości:

Regulamin i Cennik Usług Świadczonych przez Naukową i Akademicką Sieć Komputerową

(8 marzec 1995)

Naukowa i Akademicka Sieć Komputerowa NASK jest państwową jednostką organizacyjną posiadającą osobowość prawną nadaną na podstawie postanowienia Sądu Rejonowego Miasta Stołecznego Warszawy, Wydz. XVI Gospodarczy o zarejestrowaniu jako jednostka badawczo-rozwojowa w rejestrze sądowym pod numerem RBR-131.

Sieć administrowana przez NASK stanowi zespół środków technicznych i organizacyjnych służących do wykonywania na rzecz różnych podmiotów prawa telekomunikacyjnych usług publicznych - z wyłączeniem usług o charakterze powszechnym (telefonicznych i telegraficznych). Sieć komputerowa NASK, jak i działanie przedsiębiorstwa nie jest związane z wybraną technologią, lecz dostosowuje rozwiązania techniczne, technologiczne i organizacyjne do charakteru aktualnych potrzeb.

Podstawą działania NASK w dziedzinie telekomunikacji jest Zezwolenie Ministra Łączności Nr 127/94 z dnia 9 grudnia 1994 roku. NASK pokrywa koszty bieżącej działalności z uzyskiwanych przychodów, na które składają się opłaty abonenckie. Wysokość opłat abonenckich

określa Cennik Usług NASK wprowadzany Zarządzeniem Dyrektora NASK. W opłatach abonenckich mogą być stosowane ulgi pokrywane z dotacji celowych oraz zleceń specjalnych.

Regulamin Świadczenia Usług

I Podstawa i zakres działalności oraz definicje pojęć

§ 1

1. Regulamin Świadczenia usług zwany dalej "regulaminem" określa zakres i warunki wykonywania usług przez operatora sieci - jednostkę badawczo-rozwojową Naukową i Akademicką Sieć Komputerową zwaną dalej NASK, oraz precyzuje zakres wzajemnych zobowiązań wynikających z umów zawieranych przez NASK z podmiotami korzystającymi z jego usług.

2. Do opracowania niniejszego regulaminu NASK został zobowiązany przez Ministra Łączności (pkt. 5 załącznika do zezwolenia nr 127/94 z dnia 9 grudnia 1994 roku).

§ 2

Ilekroć w regulaminie i cenniku jest mowa o:

1/ "operatorze sieci NASK" - rozumie się przez to NASK jako podmiot świadczący usługi telekomunikacyjne na podstawie zezwolenia nr 127/94 z dnia 9 grudnia 1994 roku na działalność w dziedzinie telekomunikacji

2/ "sieci NASK" - rozumie się przez to rozległą sieć międzymiastową NASK, miejską sieć w Warszawie pod nazwą WARMAN oraz inne sieci lub ich fragmenty, za które NASK ponosi odpowiedzialność w rozumieniu Ustawy o Łączności

3/ "abonamencie" - rozumie się przez to uprawnienie do korzystania z usług sieci NASK

4/ "abonencie" - rozumie się przez to usługobiorcę (osobę fizyczną, prawną lub inną jednostkę organizacyjną), któremu przyznano abonament

5/ "użytkowniku" - rozumie się przez to osobę fizyczną korzystającą bezpośrednio lub pośrednio z usług sieci NASK

6/ "sieci bazowej" - rozumie się przez to odpowiednik poziomu łącz fizycznych oraz łącz logicznych w modelu ISO/OSI (wydzielone lub komutowane kanały cyfrowe w sieci pierwotnej oraz stałe lub komutowane połączenia logiczne /do przesyłania ramek zawierających sekwencje bitów informacji/ w sieci wtórnej)

7/ "sieci dostępowej" - rozumie się przez to linie telekomunikacyjne oraz urządzenia końcowe zawierające sieciowy styk abonenta

8/ "telekomunikacji" - rozumie się przez to :
transmisję pomiędzy punktami lub pośród punktów określonych przez użytkownika, informacji ustanowionej przez użytkownika, bez zmiany formy i treści informacji pomiędzy nadaniem a odbiorem,
przy użyciu transmisji elektromagnetycznej, z wykorzystaniem lub bez łączności przewodowej,
włączając wszystkie przyrządy, udogodnienia i usługi (w tym gromadzenie, składowanie, przesyłanie, przełączanie z tym zastrzeżeniem, że takie usługi nie służą i nie są przystosowane do zarządzania, sterowania i operowania systemem telekomunikacyjnym oraz zarządzanie usługami telekomunikacyjnymi)

9/ "sieci telekomunikacyjnej" - rozumie się przez to linie i urządzenia służące do wykonywania usług telekomunikacyjnych

10/ "linii telekomunikacyjnej" - rozumie się przez to telekomunikacyjne połączenie fizyczne lub logiczne pomiędzy wyróżnionymi elementami sieci telekomunikacyjnej

11/ "elemencie sieci telekomunikacyjnej" - rozumie się przez to linię telekomunikacyjną lub urządzenie pracujące w sieci telekomunikacyjnej

12/ "wyróżnionym elemencie sieci telekomunikacyjnej" - rozumie się przez to urządzenia, pomiędzy którymi mogą być zestawione odcinki linii telekomunikacyjnej (połączenia)

13/ "telekomunikacyjnej linii trwałej" - rozumie się przez to linię zestawioną przez operatora pomiędzy stykami abonenckimi lub wyróżnionymi elementami sieci telekomunikacyjnej na czas określony (w skład linii mogą wchodzić odcinki linii komutowane przez operatora)

14/ "telekomunikacyjnej linii komutowanej" - rozumie się przez to linię zestawianą i rozłączaną poleceniami abonenta pomiędzy sieciowymi stykami abonenckimi lub poleceniami operatora pomiędzy wyróżnionymi elementami sieci telekomunikacyjnej

15/ "usługach telekomunikacyjnych" - rozumie się przez to wykonywanie telekomunikacji na rzecz abonentów NASK

16/ "usługach dodanych" - rozumie się przez to nietelekomunikacyjne usługi świadczone przez NASK na rzecz abonentów

17/ "usługach teleinformatycznych (telematycznych)" - rozumie się przez to usługi telekomunikacyjne i dodane łącznie

18/ "urządzeniach końcowych (DTE)" - rozumie się przez to urządzenie abonenckie przeznaczone do transmisji informacji dołączone i dostosowane do abonenckiego styku sieciowego

19/ "zakończeniu łącza telekomunikacyjnego (DCE)" - rozumie się przez to urządzenie abonenckie lub między operatorami umożliwiające połączenie telekomunikacyjne

20/ "sieciowym styku abonenckim" - rozumie się przez to miejsce połączenia infrastruktury technicznej operatora i abonenta lub między operatorami

21/ "bezpołączeniowych usługach telekomunikacyjnych" - rozumie się przez to przesyłanie informacji użytkownika bez zestawienia trwałego lub komutowanego połączenia (usługi datagramowe)

22/ "zaleceniach CCITT oraz ITU" - rozumie się przez to zbiór zaleceń międzynarodowych (Międzynarodowego Doradczego Komitetu Telegrafii i Telefonii) dotyczący całokształtu zagadnień w dziedzinie telekomunikacji

23/ "ISO" - rozumie się przez to Międzynarodową Organizację Standaryzacji (International Standarisation Organisation)

24/ "OSI" - rozumie się przez to siedmiowarstwowy model odwzorowania funkcji sieciowych (Open Systems Interconnections)

25/ "protokóle sieciowym" - rozumie się przez to zalecenie lub normę określającą działanie elementów systemu telekomunikacyjnego lub usług dodanych

26/ "sieci X.25" - rozumie się przez to cześć systemu telekomunikacyjnego realizującego usługi przesyłania pakietów informacji w trybie połączeniowym po uprzednio zestawionych liniach wg. zaleceń CCITT X.25, X.75, X.29

27/ "sieci internet" - rozumie się przez to cześć systemu telekomunikacyjnego realizującego usługi przesyłania pakietów bez uprzedniego zestawienia połączenia (datagramy) wg. zaleceń RFC 791, 793 - protokół TCP/IP (Transport Control Protocol / Internet Protocol) ; oraz związane usługi dodane jak telnet (remote login), ftp (file transfer protocol), e-mail (poczta elektroniczna), gopher, WWW (World Wide Web) oraz inne, a także DNS (Domain Network Service) umożliwiający adresowanie domenowe

28/ "sieci HDLC" - rozumie się przez to cześć systemu telekomunikacyjnego umożliwiającą przesyłanie ramek informacji opisaną zaleceniem X.25

29/ "sieci Frame Relay" - rozumie się przez to cześć systemu telekomunikacyjnego umożliwiającą przesyłanie ramek informacji opisaną zaleceniem CCITT I.122 i dalsze

30/ "sieci ATM" - rozumie się przez to cześć systemu telekomunikacyjnego umożliwiającą przesyłanie komórek informacji (ramki stałej długości) według zaleceń opracowywanych przez ATM Forum oraz ITU

31/ "sieci ISDN" - rozumie się przez to sieć cyfrową z integracją usług (Integrate Service Digital Network)

32/ "udogodnieniach abonenckich" - rozumie się przez to dodatkowe funkcje oferowane w celu realizacji specyficznych wymagań abonentów

33/ "dostępie przez łącze komutowane" - rozumie się przez to dostęp do abonenckiego styku sieciowego poprzez połączenie komutowane telefoniczne analogowe lub cyfrowe (ISDN) oferowane za pośrednictwem operatora usług powszechnych (telefon i telegraf)

34/ "dostępie przez łącze dzierżawione" - rozumie się przez to dostęp do abonenckiego styku sieciowego poprzez łącze trwale dzierżawione od operatora lub własne abonenta

35/ "dostępie do sieci internet, X.25" - rozumie się przez to usługę telekomunikacyjną umożliwiającą prace systemu teleinformatycznego abonenta w rozległej sieci pracującej według odpowiedniego protokółu

36/ "dostępie do sieci bazowej" - rozumie się przez to usługę telekomunikacyjną umożliwiającą prace systemu telekomunikacyjnego abonenta w rozległej sieci bazowej według protokołów HDLC, Frame Relay, ATM

37/ "udostępnieniu konta na serwerze internetu" - rozumie się przez to usługę dodaną polegającą na przydzieleniu abonentowi konta i hasła chroniącego na serwerze operatora, z którym abonent łączy się w trybie terminalowym poprzez linie telekomunikacyjną operatora NASK lub innego oferującego usługi telekomunikacyjne

38/ "serwerze internetu" - rozumie się przez to komputer w sieci internet wykorzystywany do świadczenia usług na rzecz abonentów

39/ "udostępnieniu usługi telekomunikacyjnej na serwerze internetu" - rozumie się przez to usługę telekomunikacyjną polegającą na przydzieleniu abonentowi udogodnienia polegającego na możliwości czasowego przyłączenia swojego systemu teleinformatycznego do sieci rozległej poprzez łącze komutowane lub dzierżawione z jednoczesnym zastępczym gromadzeniem informacji abonenta na serwerze w czasie jego odłączenia; odróżnia się trzy rodzaje usług:
. dostęp poprzez terminal sieciowy do sieci internet polegający na przydzieleniu czasowego (zastępczego) numeru IP przeznaczony do pracy na komputerach sieci internet, które nie są własnością operatora NASK,
. dostęp terminalowy w dowolnym trybie do serwera NASK polegający na przydzieleniu konta i odpowiednich zasobów komputerowych bez przydzielenia własnego adresu IP (użytkownik jest identyfikowany w sieci przez numer IP serwera oraz identyfikator na tym serwerze),
. przyłączenie komutowane do sieci internet polegające na przydzieleniu abonentowi numeru IP oraz odpowiednich zasobów umożliwiających zastępczą pracę serwera w czasie odłączenia abonenta od sieci

40/ "sile wyższej" - rozumie się przez to zdarzenie nadzwyczajne niemożliwe do zapobieżenia przez NASK.

§ 3

NASK świadczy telekomunikacyjne usługi krajowe i międzynarodowe o charakterze niepowszechnym w zakresie transmisji danych i poczty elektronicznej.

§ 4

Zakres usług świadczonych przez NASK:

1. Usługi teleinformatyczne świadczone przez NASK obejmują:
   1.1 Zakładanie i używanie urządzeń, linii i sieci telekomunikacyjnych
   1.2 Konserwacja i utrzymanie sieci telekomunikacyjnych
   1.3 Abonenckie usługi telekomunikacyjne
   1.4 Tranzytowanie ruchu krajowego i międzynarodowego dla innych operatorów telekomunikacyjnych
   1.5 Usługi dodane do usług telekomunikacyjnych, w tym pocztę elektroniczną, zdalny dostęp do zasobów teleinformatycznych w kraju i na świecie, transfer zbiorów, usługi informacyjne itp.

2. Prace badawczo-rozwojowe i wdrożeniowe w zakresie:
telekomunikacji
teleinformatyki
sieci i usług teleinformatycznych
3. Działalność usługowa i produkcyjna w zakresie:
3.1 Badanie, analiza i wdrażanie nowych technik i technologii mogących znaleźć zastosowanie przy projektowaniu, budowie i eksploatacji sieci teleinformatycznych
3.2 Budowa, rozwój i utrzymanie systemów teleinformatycznych
3.3 Projektowanie, konstruowanie i serwis systemów teleinformatycznych i ich elementów
3.4 Prace badawcze i dostosowawcze w zakresie udostępnienia usług świadczonych przez inne sieci komputerowe w kraju i za granica
3.5 Konsulting, ekspertyzy, wydawnictwa i doskonalenie kadr oraz inne działania w zakresie sieci i usług teleinformatycznych i komputerowych

§ 5

1. Ceny usług teleinformatycznych § 4 p.1 w sieci NASK określa cennik.

2. Wynagrodzenie za prace badawczo-rozwojowe i wdrożeniowe oraz działalność usługową i produkcyjną § 4 p. 2 i 3 kalkulowane są indywidualnie.

II. Ogólne warunki przyjmowania zleceń oraz zawierania umów

§ 6

1. Podstawą świadczenia usług przez NASK są umowy zawierane z abonentami oraz usługobiorcami określające warunki korzystania z usług NASK oraz wysokości opłat.

2. Postanowienia umów zawieranych przez NASK nie mogą być sprzeczne z niniejszym regulaminem.

3. W zawartej umowie ustala się zakres działań, które będą wykonywane przez każdą ze stron oraz obowiązki, które będą spełniane w czasie dalszej współpracy określonej umową.

4. Abonenci korzystający z usług teleinformatycznych w sieci NASK zobowiązani są przestrzegać norm, zasad i wymagań technicznych i eksploatacyjnych obowiązujących w publicznej sieci telekomunikacyjnej resortu łączności oraz w sieciach telekomunikacyjnych innych operatorów telekomunikacyjnych. Dotyczy to dotrzymania i spełnienia wymagań technicznych i eksploatacyjnych w czasie uruchamiania urządzeń i łączy w bieżącej eksploatacji oraz w przypadkach powstawania uszkodzeń lub w awariach.

5. Sprzęt i oprogramowanie wykorzystywane w sieci NASK oraz w komunikacji poprzez sieć NASK musi być licencjonowane oraz jeśli jest to wymagane posiadać homologację Ministerstwa Łączności.

6. Opłaty należne od abonenta mogą być wnoszone centralnie w pełnej lub częściowej wysokości z innych źródeł niż własne abonenta. Nie zwalnia to abonenta z obowiązku zawarcia umowy, o której mowa w pkt. 1.

7. Postanowienia określające zniżki opłat (por. pkt. 6) i czas ich stosowania nie mogą stanowić integralnej części umowy.

§ 7

1. NASK stosuje do regulowania stosunków prawnych ze swoimi usługobiorcami następujące typy umów:
1. umowy na budowę lub konserwację linii i sieci telekomunikacyjnych,
2. umowy na korzystanie z usług sieci bez prawa udostępniania sieci osobom trzecim,
3. umowy miedzy operatorskie regulujące wzajemne zobowiązania i rozliczenia z innymi operatorami sieci telekomunikacyjnych,
4. umowy z osobami świadczącymi usługi, nie wymagające posiadania zezwolenia telekomunikacyjnego, na rzecz osób trzecich
5. umowy na wykonanie prac badawczo-rozwojowych i innych opisanych w § 4 pkt. 2 i 3
6. umowy na administrowanie domenami adresowymi zgodnie w zakresie opisanym w § 14

2. W wypadku kiedy działalność zleceniodawcy wymaga zezwolenia telekomunikacyjnego lub istnieją w tym zakresie uzasadnione wątpliwości obowiązek uzyskania odpowiednich zezwoleń lub interpretacji Ministerstwa Łączności, zapewniających zgodność z prawem prowadzonej działalności, spoczywa na zleceniodawcy. Wraz z wnioskiem na zawarcie umowy zleceniodawca jest zobowiązany wylegitymować się odpowiednimi dokumentami.

§ 8

1. Umowy na usługi lub zmianę zakresu świadczonych usług zawierane są w następującym trybie:

1. zamawiający usługę składa pisemne zamówienie określające przedmiot usługi,

2. w ciągu 14dni NASK rozpatruje zamówienie i wysyła do zamawiającego powiadomienie o przyjęciu lub odmowie przyjęcia zamówienia,

3. w przypadku przyjęcia zamówienia dokonywane są uzgodnienia techniczne oraz zawierana jest umowa określająca zakres usług i jej parametry użytkowe oraz cenę,

4. umowy na usługi teleinformatyczne wchodzą w życie po powiadomieniu abonenta o uruchomieniu abonenckiego styku sieciowego.

§ 9

NASK może odmówić świadczenia usług teleinformatycznych, jeśli proponowany przez zamawiającego zakres korzystania z sieci może uniemożliwić zapewnienie umownego standardu usług dla abonentów przyłączonych do sieci.

§ 10

1. NASK i jego kontrahenci zobowiązani są do zachowania poufności informacji dotyczących istotnych warunków umowy oraz informacji uzyskanych o kontrahencie w wyniku negocjacji i realizacji umowy.
2. Wszelkie informacje, o których mowa w pkt. 1 mogą być udzielane osobom trzecim tylko w przypadkach przewidzianych prawem lub za obopólnym porozumieniem.
3. NASK jest uprawniony do publicznego ujawniania listy swoich kontrahentów, chyba że zleceniodawca zastrzegł sobie w umowie nie ujawnianie tych informacji.

§ 11

1. NASK jako operator sieci świadczy usługi teleinformatyczne z zastrzeżeniem następujących warunków:
   1/ sieciowy styk abonencki jest zlokalizowany na porcie telekomunikacyjnym operatora, chyba że umowa stanowi inaczej,
   2/ operator zapewnia konieczne warunki techniczne dla świadczenia usługi abonentowi,
   3/ abonent zapewnia warunki i środki techniczne dla przyłączenia do portu operatora.

2. Charakter świadczonych usług oraz indywidualne parametry świadczenia tych usług zawarte są w umowie.

3. Abonent uzgadnia z operatorem wymagania techniczno-eksploatacyjne dostępu do sieci operatora warunkujące przyłączenie.
Uzgodnienia dotyczą:
   1. urządzeń liniowych, rodzaju łączy, szybkości transmisji,
   2. procedur i protokołów transmisyjnych na urządzeniach komunikacyjnych, jeżeli komunikują się z odpowiednimi urządzeniami operatora,
   3. wymagań w czasie uruchamiania i eksploatacji połączenia,
   4. postępowania w przypadku awarii,
   5. taryfikacji i rozliczeń,

4. Operator ma prawo sprawdzenia uprawnień abonenta w zakresie wykorzystania usług oraz wykorzystania sprzętu w świetle obowiązującego prawa oraz niniejszego regulaminu.

5. Abonent ma obowiązek umożliwić operatorowi skontrolowanie sposobu wykorzystania usług oraz sprzętu.

6. Operator gwarantuje dostęp do sieci przez cały rok i całą dobę z prawdopodobieństwem w zakresie dostępu nie mniejszym niż 99% w postępującym okresie rocznym oraz nie mniejszym niż 99.5% w zakresie połączeń wewnątrz sieci operatora.

7. W przypadku nie spełnienia gwarantowanych warunków operator zobowiązany jest zapłacić karę w wysokości 150% stawki przeliczonej za czas braku dostępu czy połączeń niezależnie od zaniechania pobrania opłaty eksploatacyjnej za ten okres.

§ 12

1. Reklamacje mogą dotyczyć niespełnienia gwarantowanych warunków świadczenia usług zaistniałych nie dawniej niż 1 miesiąc przed datą złożenia reklamacji.

2. Reklamacje muszą być składane na piśmie i dotyczyć konkretnych uchybień w pracy sieci.

3. Abonent jest zobowiązany do niezwłocznego informowania operatora o zaistniałych uchybieniach w pracy sieci. Informacje kierowane do innych podmiotów lub po ustąpieniu uchybienia nie będą rozpatrywane.

§ 13

NASK nie odpowiada za niewykonanie lub nienależyte wykonanie usługi, gdy wynika to z:

1. działania siły wyższej,
2. awarii powstałej z winy abonenta, dzierżawcy lub nieprawidłowości w systemie abonenta,
3. zmiany obowiązujących standardów, po upływie 3 miesięcy od powiadomienia abonenta o konieczności zmiany abonenckiego styku sieciowego.

§ 14

1. NASK zawiera umowy na administrowanie domenami adresowymi oraz przydział klas adresowych w internecie.
2. W przypadku umowy abonenckiej bez możliwości świadczenia usług osobom trzecim świadczenie usług polegających na administrowaniu domeną adresową abonenta wchodzi w zakres umowy abonenckiej.

III Ochrona sieci NASK

§ 15

1. Dostęp do sieci NASK jest chroniony. W sieci nie mogą być użytkowane urządzenia i metody umożliwiające korzystanie z jej usług bez posiadania wynikającego z odpowiedniej umowy, upoważnienia. Używane lokalnie nazwy i hasła powszechnie dostępne nie mogą służyć do uzyskiwania połączeń w sieci NASK.

2. Podstawą statystyki, ewentualnie wyceny oraz reklamacji pracy sieci jest rejestracja zdarzeń w sieci NASK.

3. Rejestracja dotyczy każdego portu użytkownika.

§ 16

NASK zapewnia ochronę tajemnicy informacji abonenta, a w szczególności przez:

1. instalowanie urządzeń sieciowych oraz zakończeń traktów transmisyjnych w pomieszczeniach i obiektach chronionych,

2. przestrzeganie bezwzględnej tajemnicy informacji przez personel obsługujący sieć,

3. ochronę dostępu do usług teleinformatycznych poprzez system haseł dostępowych,

4. NASK może udostępnić abonentowi na uzgodnionych zasadach system szyfrowania informacji wraz z identyfikacją i autoryzacją (niezaprzeczalnością) nadania informacji przez określonego abonenta,

5. NASK może udostępnić na uzgodnionych zasadach stosowanie udogodnienia ograniczającego niepożądany dostęp do styku sieciowego abonenta jak "zamknięta grupa użytkowników" lub "sieć wirtualna".

§ 17

1. Informacja użytkownika nie jest szyfrowana na poziomie łącza.

2. W stosunku do abonentów posiadających konta na serwerach NASK stosuje ochronę sieci poprzez :
   stosowanie time-outów rozłączających nieaktywne sesję abonenta,
   likwidacje nieaktywnych uprawnień i haseł abonentów.

§ 18

W NASK działa specjalny zespół koordynujący bezpieczeństwo sieci STER oraz zespół ochrony sieci ZOS. Do ich obowiązków należy ciągła analiza pracy sieci oraz aktywne działanie na rzecz podniesienia bezpieczeństwa sieci NASK.

§ 19

1. Usługi świadczone przez NASK wykonywane są przy pomocy sprzętu i wyposażenia stanowiącego własność NASK, bądź używanego przez NASK na podstawie umów przekazujących sprzęt i wyposażenie w posiadanie NASK dających mu prawo nie ograniczonego użytkowania sprzętu i wyposażenia - w zakresie jego przeznaczenia.

2. Zbiory systemowe i konfiguracyjne sieci NASK są specjalnie chronione, a uprawnienia do nich są ściśle ograniczone do niezbędnego minimum.

3. Zbiory, o których mowa w pkt. 2 mogą być posadowione tylko na chronionym wyposażeniu sieci NASK.

§ 20

1. Abonent jest zobowiązany do bezpiecznego operowania uprawnieniami, którymi dysponuje w taki sposób, aby nie mogły być wykorzystane przez osoby nieuprawnione.

2. Użytkownik odpowiada za klasyfikację stopnia ochrony oraz wybór narzędzia ochrony informacji przesyłanej przez sieć.

3. NASK nie odpowiada za dostęp osób nieuprawnionych do informacji przesyłanej w sieci, gdy wynika to z winy abonenta lub jego użytkownika.

4. Za uprawniony dostęp do sieci uznaje się uzyskany na podstawie uzgodnionego z operatorem trybu weryfikacji użytkownika.

§ 21

Obowiązki użytkownika w zakresie ochrony informacji w sieci NASK :

1. Każdy użytkownik odpowiada za bezpieczne operowanie uprawnieniami do pracy w sieci i do kontaktu z siecią, a w szczególności: . nie może odstępować uprawnień innym osobom, . ma obowiązek operować hasłami nie krótszymi niż 6 znaków, . pod rygorem utraty dostępu do systemu musi zmieniać hasła w cyklu uzgodnionym z operatorem, . w przypadku posiadania kilku haseł nie może ich powtarzać, . nie może żądać zmiany hasła lub otwarcia zablokowanego konta na skutek przeterminowania hasła, drogą telefoniczną.

2. Informacje poufne mogą być przesyłane w sieci tylko zaszyfrowane,

3. Systemy teleinformatyczne abonenta dołączone do sieci NASK muszą być chronione przed niepowołanym dostępem.

4. Wszelkie przypadki nieuprawnionego działania w sieci NASK muszą być zgłaszane przez abonenta do Zespołu Ochrony Sieci NASK.

IV Organizacja obsługi sieci NASK

§ 22

1. Całością działalności NASK kieruje Dyrektor NASK przy pomocy oraz poprzez swoich zastępców i pełnomocników.

2. Całością spraw związanych z utrzymaniem i administrowaniem siecią kieruje Dyrektor Techniczny NASK - Operator Sieci NASK.

§ 23

1. Wyróżnia się cztery rodzaje stanowisk obsługi sieci:

specjalista upoważniony i odpowiedzialny za konfigurację sieci, system adresowania i routowania informacji oraz ich utrzymanie w zakresie przydzielonego segmentu sieci,
operator upoważniony i odpowiedzialny za nadzór nad pracą i sterowanie przydzielonym segmentem sieci,
administrator upoważniony i odpowiedzialny za przydzielanie uprawnień i rozliczanie abonentów wraz z związaną obsługą formalnoprawną,
osoby i firmy odpowiedzialne za współdziałanie ze specjalistami, operatorami i administratorami sieci w zakresie indywidualnie określonym.

2. Zadania NASK wykonują jego pracownicy. Obsługa niektórych fragmentów lub wydzielonych obszarów sieci może być powierzona innemu podmiotowi na warunkach określonych umową.

3. Pracownicy NASK oraz podmioty współpracujące w obsłudze sieci podpisują specjalne zobowiązania do szczególnej ochrony informacji abonentów NASK oraz tajemnicy firmowej NASK.

4. Pracownicy NASK upoważnieni pisemnie do dostępu do informacji stanowiącej tajemnicę służbową, są zobowiązani do jej zachowania.

§ 24

1. Specjalistą, operatorem i administratorem sieci NASK może być tylko etatowy pracownik NASK.

2. Osoby oraz firmy współpracujące w obsłudze sieci mogą wykonywać zadania:
1/ nadzór techniczny nad działaniem urządzeń NASK powierzonych jego pieczy,

2/współdziałanie z operatorami centralnymi kierującymi wydzielonymi obszarami systemu telekomunikacyjnego w zakresie utrzymania zdolności eksploatacyjnej sieci,

3/ zgłaszanie i współdziałanie w usuwaniu awarii,

4/ współdziałanie z odpowiednim specjalistą NASK w zakresie przygotowania, instalacji oraz uruchamiania urządzeń sieci,

5/ współdziałanie z odpowiednim administratorem w zakresie pozyskiwania nowych abonentów, określania technicznych parametrów przyłączenia oraz przygotowania umów,

6/ wykonywanie pomocniczych funkcji nadzoru teletechnicznego w zakresie wynikającym z Zezwolenia Telekomunikacyjnego i niniejszego regulaminu,

7/ dostarczanie bieżącej informacji koniecznej dla prowadzenia inwentaryzacji ciągłej.

§ 25

1. Sieć NASK jest uwidoczniona w ewidencji aktualizowanej na podstawie ciągłej inwentaryzacji prowadzonej na zasadach określonych w Zarządzeniu Ministra Łączności z dnia 25 maja 1993 r, w sprawie ewidencji sieci, linii i urządzeń telekomunikacyjnych.
2. Inwentaryzacja jest prowadzona w dwóch zakresach ogólnym i szczególnym:
   1/ całość sieci objęta zezwoleniem jest inwentaryzowana z dokładnością do elementów technicznych sieci istotnych dla zezwolenia telekomunikacyjnego, w szczególności : linii, urządzeń komutacji, urządzeń pośredniczących pomiędzy wydzielonymi częściami systemu telekomunikacyjnego, wyposażenia linii w urządzenia transmisji danych, sieci lokalnych, komputerów obliczeniowych itp.
   2/ inwentaryzacji sieci utrzymywanej i eksploatowanej przez NASK określającej status prawny użytkowania elementów sieci i jej połączeń: podstawę prawna użytkowania elementu sieci, podstawę prawną każdego przyłącza, konta użytkownika, jeśli jest ono założone na urządzeniach utrzymywanych przez NASK.

§ 26

1. Sieć NASK pracuje całą dobę we wszystkie dni w roku.

2. Dla zapewnienia ciągłej pracy sieci instalowane są urządzenia bezobsługowe oraz systemy zapewniające ciągłość zasilania.

3. Systemy sterowania urządzeniami i wydzielonymi częściami systemu telekomunikacyjnego muszą zapewniać automatyczny restart oraz odnowienie transmisji w przypadku wystąpienia nienaprawialnych błędów przesyłania.

4. Cały system telekomunikacyjny i jego wydzielone części musi być przystosowany do centralnego sterowania oraz rekonfigurowania.

§ 27

1. W NASK działa Zespół Obsługi Użytkownika.

2. Do zadań Zespołu Obsługi Użytkownika należy pierwszy kontakt i udzielanie podstawowych informacji, przyjmowanie i załatwianie reklamacji oraz współdziałanie z abonentem w załatwianiu wszystkich spraw w NASK.

Cennik NASK

I. Usługi telekomunikacyjne polegające na bezpośrednim przyłączeniu sieci lub komputera abonenta łączem dzierżawionym do międzymiastowej sieci Internet

1. Koszt przyłącza w zależności od jego przepływności

Przepływność	Opłata jednorazowa	Opłata kwartalna
9.6 kb/s przez CS	1 000.-	1 800.-
9.6 kb/s	3 000.-	3 900.-
64 kb/s	9 000.-	9 600.-
2 Mb/s	15 000.-	57 000.-

2. W przypadku szybkości odmiennych stosuje się ceny zwiększone o mnożnik ceny bezpośrednio mniej przepływnego łącza będący pierwiastkiem drugiego stopnia z ilorazu przepływności łącza i przepływności bezpośrednio mniejszej.

3. Ceny podano **w założeniu wykorzystania przepływności średnio 40% w godzinach 8.00 - 16.00.** Przy wykorzystaniu większym dla łącz o przepływności powyżej 64 kb/s stosuje się zwiększenie opłat.

		Zwiększenie opłaty o
Wykorzystanie łącza	do 40 %	
	do 60 %	40 %
powyżej	60 %	100 %

II. Usługi telekomunikacyjne polegające na bezpośrednim przyłączeniu sieci lub komputera abonenta do miejskiej sieci WARMAN.

1. Bezpośrednie przyłączenia do sieci WARMAN

1.1 Koszt przyłącza w zależności od przepływności połączenia

Przepływność łącza	Opłata kwartalna
do 128 kb/s	1500.-
do 2 Mb/s	4200.-
do 8 Mb/s	7800.-
ethernet 10 Mb/s	7800.-
do 34 Mb/s	14400.-
do 100 Mb/s	24300.-
do 155 Mb/s	30000.-

1.2 Opłata jednorazowa

Przyłączenie galwaniczne	1 600.-
Przyłączenie optyczne	3 200.-

2. Przyłączenie przez sieć kampusową w zależności od przepływności łącza

Przepływność łącza	Opłata kwartalna
10 Mb/s	3 400.-
100 Mb/s	10 800.-
155 Mb/s	13 500.-

Opłaty jednorazowe jak dla przyłączenia w pozycji 1.2

III. Usługi telekomunikacyjne polegające na przyłączeniu sieci lub komputera łączem dzierżawionym do sieci według protokołu X.25

Opłata jednorazowa	150.00
Polska	
- 1 minuta	0.06
Europa	
- 1 minuta	0.17
- 1 kilosegment	11.00
Ameryka Północna	
- 1 minuta	0.33
- 1 kilosegment	17.50
Reszta świata	
- 1 minuta	0.62
- 1 kilosegment	27.40

IV. Usługi polegające na udostępnieniu serwera internetu

1. Dostęp do sieci przez terminal sieciowy (tylko łącza komutowane)

Przepływność łącza	Opłata jednorazowa	Za 29 godz./mies.	Za nast. rozp. godz.
do 14.4 Kpbs	100.-	60.-	4.-

2. Dostęp terminalowy z założeniem konta na serwerze

Opłata jednorazowa (łącze dzierżawione)	1000.–
Opłata jednorazowa (łącze komutowane)	100.–
Korzystanie z serwera za pierwsze 29 godzin w miesiącu	50.–
Za każdą następną godzinę	3.50
Nielimitowane za 1 miesiąc	150.–
Za wykorzystanie pamięci dyskowej do 1MB	— –
Za każdy następny 1 MB miesięcznie	10.–
Maksymalne wykorzystanie pamięci dyskowej 11 MB miesięcznie	100.–

3. Przyłączenie komutowane do sieci internet

Przepływność łącza	Opłata jednorazowa	Za pierwsze 29 g/mies	Za nast. rozp. godz.
do 14.4 kb/s	100.-	60.-	4
64 kb/s (ISDN)	300.-	130.-	9

Opłata za zasoby komputerowe związane z obsługą adresu IP

Za minimalną pojemność dysku 5 MB miesięcznie	40.-
Za każdy nastepny 1 MB miesięcznie	10.-

Uwaga ! Cena za kompletną usługę obejmuje łącznie cenę za łącze i zasoby komputerowe

V. Usługi inne

1. Utrzymanie DNS dla usługobiorcy nie posiadającego abonamentu NASK oraz abonentów w zakresie przekraczającym zwykłą obsługę połączenia ceny negocjowane

2. Dostarczenie i prowadzenie poczty zaufanej gwarantującej niezmienność treści, niezaprzeczalność podpisu oraz szyfrowanie informacji za 1 stanowisko i 1 miesiąc ceny negocjowane

3. Praca w systemie umożliwiającym ochronę transmisji poprzez szyfrowanie pakietów, dystrybucję kluczy, certyfikację i autoryzację podpisu za stanowisko i 1 miesiąc ceny negocjowane

4. Prace techniczne po stronie abonenta związane z przyłączeniem do sieci ceny negocjowane

5. Abonament dla podmiotów świadczących usługi dla osób trzecich ceny negocjowane

6. Abonament dla podmiotów posiadających zezwolenie telekomunikacyjne ceny negocjowane

Andrzej Zienkiewicz

Warszawa 1995-05-10

Zagadnienia prawne, ekonomiczne i organizacyjne związane z budowa sieci komputerowych

1. Wprowadzenie

Nie znam kompendium wiedzy na temat problemów związanych z budową sieci telekomunikacyjnych używanych w teleinformatyce w Polsce. Sam również nie podejmuję się opracowania w miarę pełnego zakresu wiedzy na temat budowy takich sieci. Jednak dyskusje pośród operatorów, na seminariach oraz w prasie skłaniają do podjęcia próby przedstawienia chociaż zarysu problemu.

Przez sieci telekomunikacyjne używane w teleinformatyce w tym referacie rozumiem tylko te sieci, w których świadczone są usługi teleinformatyczne. To znaczy sieci nie służące wyłącznie dla zaspokojenia potrzeb telekomunikacyjnych właściciela, ale również lub wyłącznie służące do świadczenia usług dla innych podmiotów prawa. Z tym, że świadczenie usług rozumiem podobnie jak ustawodawca stanowiący prawo podatkowe, to znaczy, że fakt odpłatności lub nie za usługi nie ma znaczenia. Istotne jest, że podmiot świadczący zaspakaja potrzeby telekomunikacyjne innego podmiotu - forma rozliczenia jest tu bez znaczenia.

Problemy opisane w referacie nie odnoszą się w zasadzie do sieci wewnętrznych właściciela. Jednak pewne rodzaje sieci, jak na przykład sieci uczelni, na zasadach zdrowego rozsądku powinny uwzględniać wiele elementów typowych dla sieci usługowych. Praca w jednej sieci administracji uczelni, pracowników nauki oraz studentów niesie za sobą duże ryzyko wynikające z niewłaściwego wykorzystania informacji, wobec czego pewne, a może wszystkie elementy ochrony sieci i odpowiedzialności operatora powinny występować i w sieci wewnętrznej uczelni.

Swój referat opieram w pierwszym rzędzie na doświadczeniach zdobytych w budowie i eksploatacji sieci telekomunikacyjnych dla środowiska naukowego i akademickiego. Sieci w tym środowisku od początku były budowane jako otwarte dla wielu podmiotów prawa. Finansowanie budowy sieci dopiero w trakcie wypracowywania właściwych form organizacyjnych stawało się w miarę jednolite, jakkolwiek ta jednolitość do dziś nie jest do końca wypracowana. Również formy organizacyjne kształtowały się stopniowo pozwalając na dokonywanie wielu przymiarek i łamanie wielu oporów wewnętrznych i zewnętrznych. Tym samym i podstawy prawne działania sieci akademickich tworzyły się stopniowo i proces ten nadal nie jest zakończony. Formy finansowania, organizacja oraz podstawy prawne tworzyły się nie tylko wewnątrz środowiska, ale może przede wszystkim na styku środowisko naukowe i akademickie z innymi organami i podmiotami prawa.

Trzeba również wyjaśnić co rozumiem przez sieci telekomunikacyjne, ponieważ pojęcie telekomunikacji nie jest nigdzie jasno zdefiniowane. Posłużę się tutaj istotna częścią definicji ujętej w regulaminie NASK, a opartej na definicji telekomunikacji wziętej z normy obowiązującej w USA. Przez sieć telekomunikacyjną rozumiem więc taką sieć, w której pomiędzy portami lub pośród portów sieci określonych przez abonenta tej sieci, następuje przekazanie informacji ustanowionej przez abonenta, bez zmiany formy i treści informacji pomiędzy portem nadania i odbioru. To znaczy przekazywanie informacji jest całkowicie transparentne, abonent nie musi znać metod, dróg i technik przekazywania informacji oraz ma prawo domniemać i żądać, żeby

informacja była przekazywana pomiędzy i tylko pomiędzy portami sieci przez niego określonymi i że nie następuje żadna ingerencja w jego informacje.

Przepisy prawa karnego, administracyjnego, prasowego i autorskiego nie dają podstaw do regulacji działania operatora telekomunikacyjnego, czyli podmiotu świadczącego usługi telekomunikacyjne. Ustawa o Łączności daje tylko bardzo ogólne wskazówki w tym zakresie i wobec bardzo szybkiego rozwoju techniki i technologii inaczej być nie może. Wobec tego wydaje się uzasadnione takie czy inne licencjonowanie operatorów telekomunikacyjnych. Licencjonowanie to może dawać trzy efekty. Po pierwsze uświadamia licencjobiorcy odpowiedzialność związaną ze świadczeniem usług telekomunikacyjnych. Po drugie określa listę podmiotów uprawnionych do świadczenia usług telekomunikacyjnych co dla abonentów może stanowić źródło informacji o jednostkach uprawnionych, to znaczy zweryfikowanych pod katem przygotowania do świadczenia usług. Po trzecie daje w trakcie procesu weryfikacji szanse na przygotowanie się do świadczenia usług telekomunikacyjnych oraz określa adresata przyszłych regulacji w tym zakresie.

Wydaje się , ze telekomunikacja jest podobną dziedziną jak medycyna, budownictwo itp., gdzie strach byłoby powierzać swoje bezpieczeństwo zupełnie niekontrolowanym usługodawcom. Jakkolwiek podstawowe regulacje prawne pomiędzy abonentem i operatorem muszą i mogą być określone jedynie w umowie abonencckiej, to jednak stworzenie zdefiniowanego i określonego grona operatorów telekomunikacyjnych pozwala na tworzenie wspólnych reguł działania, które po sprawdzeniu w praktyce mogą być podstawa przyszłych uregulowań w zakresie telekomunikacji.

2. Podstawy prawne działalności telekomunikacyjnej

W tym referacie nie będę poruszał problemów związanych z uzyskaniem zezwolenia telekomunikacyjnego lub koncesji na świadczenie usług telekomunikacyjnych. Te sprawy, mam nadzieje będą poruszone przy okazji omawiania nowelizacji ustawy o łączności. Podam tylko, ze nasze doświadczenie uczy, że w przypadku konieczności posiadania zezwolenia lub wątpliwości w tym zakresie należy przenieść obowiązek uzyskania odpowiedniego dokumentu lub interpretacji Ministra Łączności na abonenta. Działania w imieniu abonenta lub w jego zastępstwie są nieracjonalne i konfliktogenne. Wobec tego w dalszym ciągu referatu skoncentruję się na mniej znanych zagadnieniach oraz propozycjach regulacji kontraktowych pomiędzy operatorem i abonentem umieszczanych w odpowiednich umowach.

Podstawym zagadnieniem rodzącym konieczność regulacji oraz budzącym wątpliwości jest ochrona informacji w sieci telekomunikacyjnej. Następuje tu konflikt pomiędzy prawem do uzyskania informacji oraz jej prywatnością. Sądzę, że operator nie może brać udziału w tym sporze. Ponieważ operuje informacją nie swoją, powierniczo powierzoną mu do przesłania, obowiązuje go bezwzględny obowiązek ochrony tej informacji w każdym aspekcie.

Mamy tu do czynienia z trzema problemami, które omówię kolejno. Trzeba jednak zaznaczyć, ze większość zagrożeń informacji wynika z błędów czynionych przez abonenta oraz obsługę sieci, tylko niewielka cześć zagrożeń jest wynikiem świadomego działania. Na szczęście metody ochrony przed błędem i agresją są podobne. Należy też zaznaczyć, że większość zagrożeń sieci pochodzi z jej wnętrza i jest generowana przez jej obsługę. Z tego powodu możliwości oddziaływania obsługi sieci na jej działanie oraz przesyłanie informacji muszą być maksymalnie możliwie ograniczane.

Po pierwsze trzeba chronić sama sieć w ten sposób, aby niemożliwe było zniekształcenie informacji w czasie przesyłania, aby informacja docierała wyłącznie do adresata i po trzecie, aby prawdopodobieństwo przesłania informacji było możliwie wysokie. Z tego powodu oczywistym

jest, ze operator musi być nieograniczonym dysponentem posiadanej sieci czyli jej wyłącznym właścicielem. Świadczenie usług na sprzęcie, który nie jest absolutnie wyłączony do dyspozycji operatora jest niemożliwe. Tak samo operowanie sprzętem musi być w całości wykonywane przez pracowników operatora, którzy zostają poddani specjalnej dyscyplinie. Ponad to wyposażenie sieci musi być posadowione w obiektach i pomieszczeniach chronionych. Dla operatorów wyrastających organizacyjnie lub kadrowo z telekomunikacji jest to naturalne. Natomiast w środowiskach nowych, zwłaszcza akademickich budzi wątpliwości i często nie jest przestrzegane. To jednak nie wszystko. Ponieważ zagrożenie sieci płynie w poważnej części z jej wnętrza oddziaływanie na sieć musi być ograniczone. Na podstawie doświadczenia oraz w wyniku ekspertyz przyjęliśmy na wstępie, że działania związane z konfiguracja sieci muszą być oddzielone od innych, sieć podzielona na obszary funkcjonalne, obsługa konfiguracji podzielona tak, aby możliwie mało osób mogło wpływać na konfiguracje poszczególnych obszarów oraz na całość konfiguracji sieci. Do tego wszelkie informacje i zbiory konfiguracyjne muszą być szczególnie chronione oraz posadowione na szczególnie chronionym sprzęcie. W ten sposób ogranicza się możliwość popełniania błędów jak i ingerencji zewnętrznych.

Tak samo musi być zorganizowane operowanie siecią to znaczy oddziaływanie na jej bieżące działania w ramach ustalonych przez konfigurujących sieć. Tak samo administrowanie siecią ograniczone do styku z abonentami oraz regulowania spraw formalnych na styku z siecią musi być wykonywane przez osoby zaufane z wyraźnie określonym zakresem kompetencji. Tylko prace pomocnicze, które nie wiążą się z konfiguracja, operowaniem siecią oraz ustalaniem abonentów i ich praw mogą być wykonywane przy mniejszej ochronie.

Po drugie operator powinien conajmniej określić postępowanie abonenta, aby zapewnić maksymalna ochrone treści informacji przed niepowołanym dostępem. Zwracam uwagę, że podstawowa część ataku na informacje następuje nie w samej sieci telekomunikacyjnej, ale na obiektach abonentów dołączonych do sieci. Sieć spełnia tu jedynie role środka komunikacyjnego poprzez który następuje dostęp do obiektów abonenta. Dla ochrony w tym zakresie operator sieci może wymagać szczególnego zachowania ochrony u abonenta oraz oferować pewne usługi dodatkowe.

Dziś uznaje się dość powszechnie, że za klasyfikacje stopnia koniecznej ochrony informacji oraz dobór metod może odpowiadać tylko nadawca informacji. Operator może wyłącznie udostępnić mu pewne metody zapewniające niezaprzeczalność nadania, niezmienność treści i ewentualnie szyfrowania informacji. Ponad to operator może udostępniać abonentom usługi pozwalające na tworzenia wzajemnie niedostępnych sieci "wirtualnych" w ogólnej sieci telekomunikacyjnej. Może udostępniać usługi zamkniętej grupy użytkowników oraz sądzę, że w niedalekiej przyszłości szyfrowanie informacji w ramach podsieci wirtualnej w celu ochrony treści informacji przez obsługą sieci.

Po trzecie operator powinien określić warunki ochrony abonentów przed agresja innych abonentów. Poza wyżej opisanymi środkami operator musi stworzyć warunki prawne pozwalające mu na wyciąganie konsekwencji w stosunku do abonentów, którzy dopuszczają do agresji w stosunku do innego abonenta sieci. Podkreślam jeszcze raz, ze agresja odbywa się poza siecią operatora, wobec czego operator może tylko stworzyć w umowie regulacje prawne wskazujące na niedopuszczalność czynu, pozwalające mu na odłączenia abonenta od sieci oraz ułatwiające poszkodowanemu abonentowi dochodzenia odszkodowania.

Zwracam uwagę, ze cały czas posługuję się określeniem abonent, a nie użytkownik sieci. Użytkownik nie ma żadnego stosunku prawnego z operatorem, wobec czego dyscyplinowanie użytkowników musi należeć do abonenta, którym w szczególnym przypadku może być inny operator. To abonent musi i tylko abonent może oddziaływać na swoich użytkowników, wobec czego on musi ponosić konsekwencje ich niedopuszczalnego działania. Specjalną grupę

abonentów sieci komputerowych stanowią provider'zy usług dodanych. Grupa ta obecnie w większości nie podlega dyscyplinujacemu oddziaływaniu systemu zezwoleń. W tej grupie o niesłychanie zróżnicowanym przygotowaniu do świadczenia usług telekomunikacyjnych i bardzo zróżnicowanych interesach ekonomicznych i innych występuje szczególnie dużo prób omijania zasad, które muszą być przestrzegane przy świadczeniu usług telekomunikacyjnych. Grupa ta w dużej części jest reprezentowana przez podmioty mające bardzo agresywne interesy ekonomiczne, ambicjonalne, propagandowe i inne. Osoby pracujące w tej grupie są na ogół przygotowane zawodowo do działania w sieciach telekomunikacyjnych. Wobec powyższego każdy operator szczególnie starannie musi uzgadniać z dostarczycielami usług warunki realizacji abonamentu oraz musi stosować dokładniejszą kontrolę działania w sieci tego rodzaju abonentów.

W sieciach telekomunikacyjnych następuje szybki rozwój nowych technik dostępu zmuszający operatorów do stałej obserwacji skutków działania tych technik. Głośnym zjawiskiem w sieci było pojawienie się tzw. "slipu dzwonionego". Usługa ta w pewnych przypadkach powoduje, ze provider usług dodanych zaczyna świadczyć usługi telekomunikacyjne. Dopiero dokładniejsza analiza pozwala na określenie rodzajów usług świadczonych pod tym hasłem i określenia wymagań koniecznych dla ich legalnego świadczenia.

3. Zagadnienia ekonomiczne

Środowisko naukowe i akademickie jest przyzwyczajone do zakupu wyposażenia w formie tak zwanej "aparatury specjalnej". Taka aparatura jest zakupywana w ramach i w celu wykonywania określonych badań i musi charaktaryzować się unikalnością conajmniej w środowisku, któremu ma służyć. Aparatura specjalna jest utrzymywana w czasie procesu badawczego w specjalnych rejestrach i po jego zakończeniu może być zagospodarowana jako normalny majątek uczelni czy jednostki badawczej. Sieci komputerowe nie są ze swej istoty aparaturą badawcza. Stanowią jedynie bardzo istotne wyposażenie nauki w środki komunikacji. Z tego powodu środki na wstępną budowę sieci pochodzą z dofinansowania inwestycji do czasu, kiedy dalszy rozwój sieci będzie mógł odbywać ze środków własnych operatora. To znaczy, że po zakończeniu inwestycji środki muszą być wpisane w majątek inwestora i ich wartość musi być umarzana obciążając koszty działalności. Powyższa dygresja skierowana jest wyłącznie do środowiska naukowego i akademickiego, ponieważ poza tym środowiskiem istnieje pełne zrozumienie problemu finansowania i rozliczania inwestycji co nie oznacza zaniechania stosowania różnych form wspomagania inwestycji operatorów telekomunikacyjnych.

Przedsięwzięcia infrastrukturalne w sieciach komputerowych sa bardzo kosztowne. Zainwestowane środki, niezależnie od źródła ich uzyskania, muszą być zwrócone. Zwrot tych środków musi nastąpić poprzez opłaty za użytkowanie sieci realizowane na rynku usług.

Rynek usług teleinformatycznych w Polsce jest płytki. Płytkość tego rynku wynika z kilku przyczyn. Pierwszą jest zbyt uboga struktura dostępowa do sieci, która w naturalny sposób ogranicza ilość abonentów sieci. Drugą jest segmentacja rynku wynikająca z jego sztucznego podziału, często w wyniku niefortunnych regulacji prawnych lub nadmiernych ambicji możliwych do realizacji w warunkach błędnych regulacji prawnych. Istotne znaczenie ma oddziaływanie efekty porównawczego z innymi rynkami, zwłaszcza USA. W efekcie jednostkowe dochody ze świadczenia usług nie mogą być wysokie. Jedynie odpowiednio duży segment rynku może spowodować normalna opłacalność inwestycji. Inaczej konieczne sa różne formy ekonomicznego podtrzymywania operatora.

Z powyższych powodów operatorzy starają się działać o ile to możliwe wspólnie, w dużej mierze w oparciu o największą zastaną strukturę techniczna Telekomunikacji Polskiej SA. Wobec tego pełny koszt inwestycji, które ponoszone są dla uruchomienia poszczególnych sieci jest

złożony. W części jest on ponoszony przez operatora formalnie uruchamiającego sieć, w części przez innego operatora, który zapewnia strukturę uzupełniającą. W pewnych przypadkach jawnej kooperacji koszty te są bezpośrednio dane. W innych, na przykład przy wynajmowaniu linii, kanałów kablowych itp., nie występują w sposób jawny, ponieważ wynajmujący ponosi jedynie opłaty bieżące.

Takie działania wspólne wydają się ze wszech miar zasadne. Przyśpieszają powstawanie rynku usług, zwiększają strukturę dostępowa do sieci, wreszcie pozwalają sprzedawać bezpośrednio zasoby infrastruktury sieciowej. Jednak obecna struktura rynku oraz stan regulacji prawnych stwarza duże trudności w realizacji współdziałania. Dosyć powszechne jest zjawisko bardzo dobrych wyników ekonomicznych operatora przy braku płynności w kasie. Jest to typowy sygnał przeinwestowania lub nienadążanie podaży rozwoju usług świadczonych z tych inwestycji. Kooperacja operatorów mogłaby te zjawiska łagodzić, gdyby nie stały na przeszkodzie inne czynniki.

4. Zagadnienia organizacyjne

Sądzimy, ze Polska jest zbyt małym krajem, żeby już teraz mogło na jej terenie powstać kilku niezależnych od siebie operatorów telekomunikacyjnych. Zwolennicy "absolutnej" konkurencji nie są łaskawi zauważyć, ze do tej pory nie powstała tak naprawdę żadna niezależna sieć teleinformatyczna. POLPAK wykorzystuje istniejąca strukturę telefoniczna TP SA, TELBANK wykorzystuje strukturę TP SA oraz współinwestuje z NASK, NASK wykorzystuje infrastrukturę TP SA i TELBANKu, KOLPAK wykorzystuje strukturę kolejowego systemu łączności, TELENERGO buduje sieć w oparciu o strukturę sieci energetycznych itp. itd. Pomimo pokrzykiwań i zachęt do bezwzględnej konkurencji operatorzy współpracują ze sobą. Zwolennikom nieograniczonej konkurencji należy przypomnieć, ze uruchomienie czterech sklepików w małej wsi nie poprawi zaopatrzenia, ale spowoduje wegetacje wszystkich lub upadek kilku ze nich. Istnieje konieczność dokonania inwestycji w przedsięwzięcie, aby mogło być funkcjonalne. Wyłożone pieniądze inwestycyjne muszą być zwrócone, a do tego musi istnieć rynek, który zakupi odpowiednia ilość usług.

Przedsięwzięcia telekomunikacyjne są kapitałochłonne, polski rynek usług teleinformatycznych płytki. Można mnożyć przykłady przeinwestowania prowadzące do upadku usługodawcy. Dlatego należy pochwalać dążenie operatorów do współpracy w zakresie przedsięwzięć infrastrukturalnych. Tylko rynek usług dodanych do telekomunikacji jest na tyle mało kapitałochłonny, że może na nim występować bardziej nasilona konkurencja.

Poważnym problemem organizacyjnym jest brak koniecznych regulacji prawnych w kilku zakresach. Po pierwsze za decyzjami ustalającymi formalny czy faktyczny monopol w zakresie całości lub części usług telekomunikacyjnych nie idą regulacje prawne ustalające warunki działania w przypadku istnienia monopolu. Pozwala to na zachowania monopolistyczne podmiotów świadczących usługi ze szkoda dla innych operatorów, a przeważnie i samych monopolistów.

Po drugie brak jest formalnych i praktycznych regulacji prawnych pozwalających na współprace operatorów w zakresie inwestycji oraz eksploatacji sieci. Pozostawienie wszystkiego do uregulowania w umowach między operatorskich nie rokuje szybkiego ustalenia reguł, do tego obowiązujące przepisy, zwłaszcza podatkowe taka współpracę w pewnych zakresach utrudniają lub wręcz uniemożliwiają.

Po trzecie struktura ekonomiczna operatorów, ich system organizacyjny i rozliczeń wewnętrznych oraz zewnętrznych nie sprzyja współpracy.

Po czwarte nadmiar bezpośrednich ingerencji władzy państwowej oraz nadmierny bezpośredni i pośredni udział finansowania z budżetu powodują zorientowanie operatora na władzę a nie na rynek. Stosowany system preferencji podatkowych i celnych nie sprzyja współpracy.

Sądzę, że najpilniejsze jest rozbicie rynku usług na dwie części. Rynek podaży bazowych usług telekomunikacyjnych obejmujący pierwotna sieć cyfrowa oraz wtórne usługi na tej sieci jak TDM, Frame Relay czy w przyszłości ATM oraz rynek usług dla abonentów sieci telekomunikacyjnych. Druga cześć rynku powinna obejmować podaż usług telekomunikacyjnych dla abonentów jak usługi głosowe, video, transmisja danych, usługi informacyjne itp. Pierwszy rynek jest przeznaczony dla usługodawców, drugi dla abonentów końcowych indywidualnych i zbiorowych.

Pomijając, że taki podział szybko rozwija się na świecie, w Polsce jest to zagadnienie podstawowe. Usługi bazowe z natury swojej przeznaczone sa dla wszystkich, w tym i użytkowników specjalnych. Budowa kilku sieci bazowych dla różnych operatorów nie wydaje się nie wydaje się niczym racjonalnym uzasadniona na polskim rynku. Konieczne jest powstanie silnego operatora sieci bazowej zdolnego do wybudowania i udostępniania struktury bazowej dla wszystkich potrzebujących. Szczególnie będzie to widoczne po otwarciu rynku europejskiego, kiedy drobni i słabi operatorzy nie będą mieli szans.

Rynek usług z natury przystosowujący się do potrzeb abonentów jest niesłychanie zróżnicowany. Wymaga on działania dużych operatorów, na przykład na rynku usług powszechnych jak telefon i telegraf, ale również małych jak na przykład dostarczających informacyjne serwisy lokalne. O ile na rynku pierwszym możliwy i celowy może być dziś monopol, pod warunkiem ustawowego ustalenia wykonywania usług przez monopolistę, w celu wykluczenia możliwości zachowań monopolistycznych, o tyle na rynku drugim wskazana jest konkurencja. Rynek pierwszy jest technologicznie znany, potrzebny jest na nim skoncentrowany wysiłek finansowy i kadrowy. Na rynku drugim prawie wszystko jest do wymyślenia wobec czego rozproszenie wysiłków, zapewniające maksymalny dopływ nowych pomysłów jest konieczne. W żadnym przypadku działania na obu rynkach nie mogą być identyczne. Niestety obecny stan regulacji zupełnie nie przystaje do aktualnych potrzeb.

Obecne regulacje prawne oraz praktyka działania władz powodują nieracjonalne zachowanie operatorów telekomunikacyjnych. W ramach aktualnej rzeczywistości funkcjonuje kilka nieracjonalnych zjawisk.

Operatorzy starają się skutecznie opanować poszczególne segmenty rynku, na których uzyskują monopol. Powstaje sieć dla banków TELBANK, dla kolei KOLPAK, dla PKO PKONET, dla nauki NASK, dla potrzeb specjalnych, administracji państwowej itp., itd. W najgorszej sytuacji jest Telekomunikacja Polska SA, której pozostaje monopol ogólnopaństwowy i która ustawia się jako przeciwnik pozostałych "monopolistów". W ramach takiego podziału rynku możliwe sa niezdrowe ambicje poszczególnych osób na stanowiskach kierowniczych, które z opanowania poszczególnych segmentów próbują osiągać osobiste korzyści. Mozliwe sa również aspołeczne zachowania poszczególnych załóg pracowniczych, które usiłują wymusić ograniczenie współdziałania operatorów celem ich wypchnięcia z rynku. Oczywiście "oko cyklony" występuje na styku Telekomunikacja Polska SA inni operatorzy. Jednak chciałbym zauważyć, ze wynika to wyłącznie ze znaczenia Telekomunikacji Polskiej SA na rynku, nie jest natomiast zjawiskiem wyjątkowym. Jeżeli jednak spojrzymy na działalność operatorów od strony abonentów i użytkowników sieci to uzyskamy inny obraz. Żaden operator nie jest w stanie samodzielnie zapewnić podaży koniecznych usług na rynek. Na przykład NASK obsługujący środowisko naukowe i akademickie bez Telekomunikacji Polskiej SA oraz częściowo TELBANKu nie może zapewnić łączności. Nikt nie dostarcza kompletu usług potrzebnych dla

administracji państwowej itp. Wszyscy razem operatorzy nie zapewniają kompletu usług potrzebnych użytkownikom. Czym dalej od czystej telekomunikacji w sieci pierwotnej tym gorzej.

Do takiego obrazu rzeczywistości przyczynia się również sam organ udzielający zezwolenia oraz interpretujący działalność w usługach telekomunikacyjnych i dodanych. W trakcie rozpatrywania spraw zbyt wiele uwagi poświęcane jest podziałowi rynku czyli zastępowanie mechanizmów rynkowych zbyt mało rzeczywistemu sprawdzaniu możliwości przyszłych operatorów i usługodawców. W obecnym stanie podaży dziś i potencjalnej podaży jutro sprawdzenie to przyniesie podobny skutek jak rozpatrywanie konkurencyjności operatorów i nie będzie sprzyjać pozostawianiu "białych" na mapie podaży usług.

Z tego wynika, ze obecna praktyka i regulacje prawne są nieracjonalne na dziś, a w perspektywie zbliżania się do wspólnego rynku groźne dla naszych krajowych interesów. Niestety kierowanie zarzutów do operatorów, w tym Telekomunikacji Polskiej SA, jest bezcelowe. Operatorzy i ich kadra chce współpracować i ma w tym interes. Dla poprawy sytuacji potrzebne są zmiany prawne, a tam gdzie to jest jeszcze niemożliwe rozsądna polityka koordynacyjna. Obecny sposób sprawowania koordynacji bardziej przypomina działania władcze z poprzedniego systemu niż oddziaływanie na rynek, do którego podobno usilnie dążymy. Mamy na rynku zaspakajać potrzeby, a nie dokonywać podziałów, które temu rynkowi w zasadniczy sposób szkodzą.

5. Wnioski

Sądzę, że obecne regulacje funkcjonowania rynku usług telekomunikacyjnych sa wadliwe. Charakteryzują się wadliwością regulacji istniejących nastawionych bardziej na podmiotowy podział rynku niż jego funkcjonowanie. Brak jest podstawowych regulacji funkcjonowania rynku, w tym przeciwdziałających zachowaniom monopolistycznym, nieuczciwej konkurencji, ochrony interesów ekonomicznych operatora itp.. Nadmierne jest nastawienie na ingerencje bezpośrednie w postaci prób oddziaływania władczego, bezpośredniego finansowania lub tworzenia preferencji finansowych jak ulgi podatkowe i celne oraz tworzenie instytucji centralnych nie w celu koordynacji działań lecz ich bezpośredniego wykonywania. Taki stan jest typowy dla wstępnej, "naiwnej" fazy kierowania. Dopiero nabywane doświadczenie i wiedza pozwalają na stosowanie skuteczniejszego, pośredniego kierowania procesami rozwojowymi. Władza wtedy koncentruje się na tworzeniem preferencji dla tego "co" trzeba zrobić, pozostawiając bardziej przygotowanym "jak" to należy wykonać.

KIERUNKI ROZWOJU TRANSMISJI DANYCH W SIECIACH TPSA

Jarosław Kępkowicz
Marian Suskiewicz
Telekomunikacja Polska S.A.

1. Wprowadzenie

Wraz z rozwojem i rozszerzaniem zastosowań komputerów powstała nowa dziedzina telekomunikacji - transmisja danych. Budowa sieci transmisji danych w krajach zaawansowanych w dziedzinie zastosowań techniki komputerowej jest problemem nie mniej ważnym niż rozwój innych usług w dziedzinie łączności (szeroko rozumianego systemu przesyłania informacji). Problem ten jest rozważany zarówno przez administracje łączności (ministerstwa) w tych krajach , jak i przez operatorów odpowiedzialnych za rozwój systemów teleinformatycznych. Również w Polsce stajemy coraz częściej przed koniecznością wyboru kierunków rozwoju systemów transmisji danych, doboru środków technicznych do ich realizacji, jak również przed problemem efektywnego wykorzystania już istniejących zasobów telekomunikacyjnych.
TPSA jako główny operator sieci telekomunikacyjnej w Polsce, opira rozwój sieci transmisji danych na bazie istniejących systemów telekomunikacyjnych. Do celów budowy sieci transmisji danych wykorzystuje z powodzeniem posiadaną sieć telefoniczną (łącza analogowe i cyfrowe oraz centrale telefoniczne różnego typu). Systemem podkładowym dla przesyłania sygnałów transmisji danych jest stale unowocześniana sieć telefoniczna (kablowa, radiowa) i systemy satelitarne. Na początku bieżącej dekady nastąpił przełom w rozwoju telekomunikacji w Polsce. Przyczyniły się do tego m.in. następujące czynniki:
- jasno sprecyzowane cele i plany rozwoju usług i sieci telekomunikacyjnych w TPSA;
- możliwość uzyskania kredytów zagranicznych na rozwój telekomunikacji;
- zniesienie wielu ograniczeń na eksport nowoczesnych technologii;
- zakup i wdrożenie do eksploatacji cyfrowych central telefonicznych i światłowodowych systemów przesyłania informacji.

Powyższe czynniki umożliwiły reorganizację systemów telekomunikacyjnych będących w posiadaniu TPSA i podjęcie śmiałej rozbudowy sieci transmisji danych stwarzając jednocześnie bazę transportową dla systemów przesyłania informacji również innych operatorów.

2. Cyfryzacja systemów telekomunikacyjnych

Do końca lat 80-tych dominującym systemem w transmisji danych były systemy analogowe. Wprowadzenie cyfrowych central telefonicznych spowodowało, że sieć oparta wyłącznie o linie analogowe stała się niewydolna i trudna do wykorzystania przy budowie nowoczesnych systemów transmisji danych. W związku z powyższym w TPSA podjęto decyzje o budowie linii cyfrowych optotelekomunikacyjnych (światłowodowych) i radiowych. Podstawowymi systemami cyfrowymi zbudowanymi w sieci magistralnej TPSA, o przepływności 140 Mbps, są:
- podmorski kabel optotelekomunikacyjny z Koszalina do Danii;
- cyfrowa linia radiowa pomiędzy Koszalinem i Warszawą;
- cyfrowy system łączności satelitarnej na region Oceanu Atlantyckiego;
- linia optotelekomunikacyjna od granicy zachodniej do Olsztyna ;
- linia optotelekomunikacyjna łącząca Wybrzeże z Cieszynem;

- szesnaście linii radiowych, prod.NEC.
Ponadto TPSA zainstalowała i rozpoczęła eksploatację wielu elektronicznych central cyfrowych w głównych miastach Polski [3].
W najbliższych latach przewiduje się dalszą rozbudowę cyfrowej sieci dalekosiężnej, co zapewni doprowadzenie łączy cyfrowych do wszystkich central międzymiastowych w Polsce oraz przejście z cyfrowych systemów plezjochronicznych (PDH) na systemy synchronicznej transmisji (SDH). Porównanie własności sieci PDH i SDH wskazuje na celowość i konieczność budowy sieci SDH z uwagi na:
- większą elastyczność i mniejszy koszt budowy sieci SDH;
- większą niezawodność;
- łatwość wdrażania systemów zarządzania i utrzymania.
Równolegle z budową sieci dalekosiężnych prowadzone są prace przy konstrukcji sieci cyfrowych na niższych poziomach. Utworzona podstawowa sieć cyfrowa będzie bazą do tworzenia sieci wtórnych powszechnego użytku (telefonia) jak i sieci teleinformatycznych - organizowanych zarówno przez TPSA, jak też przez innych operatorów.

3. Analiza stanu zapotrzebowań na transmisję danych

Z analizy obecnej sytuacji na krajowym rynku transmisji danych wynika potrzeba zbudowania przez TPSA uniwersalnej sieci, umożliwiającej dostarczenie różnym klientom szerokiego zakresu usług. Jednoznacznie trudno jest określić potencjalną ilość użytkowników poszczególnych usług, będą to ilości zróżnicowane w zależności od typu usługi, lokalizacji systemów komutacyjnych, istniejącej sieci łączy dostępowych i aplikacji posiadanych przez użytkowników na systemach komputerowych.
W Polsce wielu użytkowników sieci lokalnych posiada obecnie różnorodne routery i sieci LAN, stąd też są oni zainteresowani dzierżawą łączy typu punkt -punkt. Dla operatora oznacza to konieczność zapewnienia możliwości dołączenia użytkowników do dzierżawionych kanałów cyfrowych o określonej przepustowości lub dołączania użytkowników do sieci typu Frame Relay (retransmisja ramek). Również dotychczasowi użytkownicy istniejących sieci X.25, ograniczeni stosunkowo niską prędkością transmisji, mogą wkrótce chcieć uzyskiwać dostęp do szybkich sieci Frame Relay. Z punktu widzenia operatora publicznego, jakim jest TPSA , w pierwszej kolejności należy dostarczyć do siedziby klienta łącza o gwarantowanych parametrach transmisyjnych. Najwłaściwszym rozwiązaniem byłoby dostarczenie poprzez jedno łącze różnych usług (np. ISDN), dopasowanych do zmieniających się potrzeb użytkowników. Kolejnym problemem jest łączenie wieloprotokołowych sieci lokalnych poprzez wielowejściowe routery lub poprzez sieci typu Frame Relay. Problemem jest również doprowadzenie interfejsów bezpośrednio do siedziby użytkownika, co wiąże się z koniecznością doprowadzenia urządzeń transmisyjnych na niewielkie odległości od użytkownika , zwykle poprzez kabel miedziany (tzw. problem "ostatniej mili"). Wymaga to odpowiedniego sposobu kontroli i zarządzania siecią transmisji danych. Siłą TPSA jest to, iż jest właścicielem sieci kablowej i posiada odpowiednie urządzenia teletransmisyjne, może dostarczyć kompletny serwis, biorąc na siebie odpowiedzialność za całe łącze "od końca do końca" tj. łącznie z kablem. Problemem jednak pozostaje efektywne wykorzystanie łącza.

Drugą grupę zwiększonych zapotrzebowań na transmisję danych generują nowoczesne usługi teleinformatyczne typu: poczta elektroniczna, zdalne i rozproszone przetwarzanie, dostęp do baz informacyjnych, w szczególności poprzez ostatnio burzliwie rozwijającą się sieć Internet.

4. Trendy rozwoju sieci transmisji danych

W ostatnich latach obserwujemy podstawowe zmiany w transmisji danych na duże odległości. W chwili obecnej nowoczesne systemy transmisyjne muszą być przystosowane do przekazywania różnorodnych informacji (danych, obrazu, głosu, ...). Szczególnego znaczenia nabierają połączenia pomiędzy sieciami lokalnymi, o różnorodnych protokołach komunikacyjnych, ale wymagających szybkich łączy, o małych opóźnieniach. Po zastosowaniu światłowodów i wysoce niezawodego sprzętu transmisyjnego osiąga się bardzo dobre połączenia na obszarach miejskich. Obserwuje się natomiast zmniejszające się zainteresowanie usługami pakietowych sieci X.25.
Protokoł X.25 jest doskonałym mechanizmem do uzyskania bezbłędnych transmisji , ale jest obarczony dużymi narzutami systemowymi, które w rezultacie powodują obniżenie szybkości transmisji całego systemu. Dodatkowo obsługa kolejek i kontrola powodują powstawanie znaczących opóźnień. Wymienione powody wymusiły powstanie nowych systemów transmisyjnych o wysokiej wydajności, szybkości transmisji i małych opóźnieniach. Frame Relay(retransmisja ramek) i ATM (asynchroniczna transmisja komórek) to dwie technologie, które stworzono do realizacji tych nowych potrzeb. Charakteryzują się one wysokim wykorzystaniem pasma, przy prędkościach od 2 Mbps do 622 Mbps , bez wysokich narzutów związanych z korekcją błędów. Idealne rozwiązanie powinno połączyć zalety X.25 z wydajnością Frame Relay czy ATM.
Frame Relay jest technologią przewidzianą do stosowania na łączach cyfrowych, jest to protokoł komutacji pakietów, opracowany dla efektywnej i szybkiej transmisji pakietów o zmiennej długości, z minimalnym opóźnieniem. Sam protokoł jest podobny do X.25, tyle że nie posiada zbędnych narzutów kontrolnych, umożliwia transmisję z dużymi prędkościami, potencjalnie aż do 34 Mbps. W ostatnich latach obserwuje się wręcz lawinowy przyrost dochodów ze sprzedaży usług i urządzeń pracujących w standardzie Frame Relay.
Od szeregu lat nie obserwowano tak dużego zainteresowania żadną inną technologią w zakresie transmisji danych, jak usługami Frame Relay.
Protokoł ATM został w zasadzie opracowany jako protokoł warstwy fizycznej dla użycia w szerokopasmowym ISDN, przeznaczony do niezwykle szybkiej, jednoczesnej transmisji głosu, wideo, obrazów i danych. ATM opiera się na transmisji 53 bajtowych komórek (48 danych i 5 kontrolnych) poprzez bardzo szybkie łącza. Standardowe prędkości wg.IEEE 802.6 wynoszą 155 Mbps i 622 Mbps. Wszystkie źródła przewidują,że ATM wkrótce będzie dominującą na rynku technologią, zarówno na rynku WAN jak i LAN. ATM jest bardzo ciekawą technologią, która jak się wydaje , jest skalowalną technologią (nadaje się dla sieci lokalnych, rozległych, dla małych i dużych prędkości), dająca możliwość przesyłania zarówno danych, głosu jak i obrazu. ATM jest dobrym rozwiązaniem dla budowy sieci miejskich, oczywiście przy zachowaniu odpowiednich mechanizmów ochrony (security). Dla praktycznego zastosowania technologii ATM potrzebna jest odpowiednia infrastruktura teletransmisyjna w hierarchii SDH (którą właśnie buduje TPSA), o bardzo dużych prędkościach międzywęzłowych.
Prognozy rozwoju rynku komputerowego wskazują, że wielu użytkowników sieci planuje przeprowadzenie gruntownych zmian w swoich sieciach lokalnych i rozległych [4]. W zakresie sieci WAN utrzyma się trend polegający na przechodzeniu od dedykowanych, prywatnych sieci ku bardziej elastycznym usługom typu Frame Relay, jak również planuje się niebawem wprowadzać produkty i usługi ATM. Prawie połowa ankietowanych zamierza się pozbyć posiadanych protokołów komunikacyjnych na rzecz protokołu TCP/IP. Natomiast łącza internetowe planuje się używać jak strategicznego nośnika w wymianie informacji ekonomicznej. Siła, jaką niosą ze sobą otwarte protokoły sieciowe, nowe technologie LAN i WAN o dużej szybkości przesyłania oraz publiczne usługi, takie jak Internet - pozwoli przedsiębiorstwom znacznie rozszerzyć zasięg swoich sieci.

5. Kierunki zmian w zakresie transmisji danych w TPSA

TPSA na bazowej sieci telekomunikacyjnej (w znacznej części już cyfrowej) nadbudowuje warstwy usługowe w zakresie transmisji głosu (usługi serii 800- Infolinia 800, audioteks, itd.) jak również w zakresie transmisji danych (poczta elektroniczna, bazy danych, Internet, itd.). W przyszłości planuje się budować inteligentne sieci telefoniczne i wowczas będzie zacierać się granica między usługami telefonicznymi i transmisji danych, powstaną szeroko rozumiane usługi telekomunikacyjne.
Od samego początku usługi teleinformatyczne powstawały w Polsce w warunkach pełnej konkurencji. W obecnej chwili poza TPSA na rynku tym działa kilku innych operatorów oferujących zbliżoną usługę. Tym co wyróżnia TPSA jest integracja sieci transmisji danych o nazwie POLPAK z innymi sieciami telekomunikacyjnymi takimi jak: łączność satelitarna VSAT, system przywoławczy Polpager, sieć teleksowa a wkrótce połączenie z siecią ISDN oraz z siecią radiokomunikacyjną [2].
Rozbudowa sieci POLPAK odbywa się w kilku kierunkach m.in. poprzez:

a/ instalację kolejnych węzłów sieci i koncentratorów terminali. Zakup nowych dużych węzłów i 18 koncentratorów zwiększy pojemność sieci dwu i pół krotnie, a także rozszerzy zasięg sieci;

b/ zamianę łączy analogowych na łącza cyfrowe w połączeniach międzywęzłowych i dostępowych, tam gdzie będzie to możliwe. Cyfryzacja łączy międzywęzłowych i zapewnienie prędkości min. 64 Kbps oraz wprowadzenie protokołu Frame Relay i prędkości do 2 Mbps jako międzywęzłowej dla węzłów zlokalizowanych w Warszawie, Katowicach, Wrocławiu, Poznaniu, Gdańsku, Krakowie;

c/ wymianę oprogramowania węzłów komutacji pakietów na najnowowszą generację w pełni realizującą zalecenia serii X.25 i umożliwiającego również transmisję z protokołem Frame Relay;

d/ wymianę starych modemów na nowoczesne modemy o większych prędkościach transmisji;

Wykorzystując podstawową zaletę transmisji pakietowej X.25 (dopuszcza pracę na łączach o niższej jakości), można oczekiwać w niedalekiej przyszłości, że usługa ta będzie również w większym zakresie dostępna na poziomie mniejszych miast (np. gmin) przy czym jako sieć dostępowa może być wykorzystany system VSAT.
Przełomu w rozwoju telekomunikacji dokonało wprowadzenie cyfrowych sieci z tzw. integracją usług. Przesyłanie głosu, obrazu i danych komputerowych - równocześnie i tą samą linią - od niedawna jest możliwe także w sieci TPSA. Usługę tę wprowadzono na razie w ograniczonym zakresie, w wydzielonej sieci KOMERTEL przeznaczonej dla klientów biznesowych . Obecnie komertelowska sieć ISDN jest dostępna dla abonentów w Warszawie, Gdańsku i Kielcach. Ten dostęp ma być rozszerzony dla innych krajowych abonentów. Wkrótce dostęp do sieci ISDN mają uzyskać abonenci w Gdyni, Poznaniu, Szczecinie, Krakowie. Na powszechny dostęp do sieci ISDN w skali ogólnokrajowej trzeba jeszcze trochę poczekać ze względu na złożoność przedsięwzięcia pod względem technicznym (wymagana pełna cyfryzacja sieci i implementacja systemu sygnalizacyjnego nr.7), organizacyjnym i ekonomicznym, ponieważ terminale ISDN-owskie są stosunkowo drogie.
W 1995r. rozpoczęta zostanie budowa przez TPSA 12 miejskich sieci w głównych miastach Polski oraz sieci szkieletowej.
Sieć szkieletowa POLPAK -T będzie spełniać kilka postawowych zadań, m.in.:

- łączyć budowane sieci metropolitalne (MAN) w dwunastu miastach Polski. Protokołem miedzywęzłowym będzie protokoł Frame Relay z możliwością migracji w kierunku ATM. Początkowe szybkości międzywęzłowe będą wynosiły n x 2Mbps z możliwością migracji w kierunku 34Mbps, w zależności od potrzeb;

-będzie stanowić płaszczyznę transmisyjną dla obecnej sieci transmsji danych POLPAK, traktowanej później jako sieć dostępowa;
- będzie stanowić podstawę do wydzielania sieci wirtualnych na potrzeby dużych klientów, takich jak banki, duże przedsiębiorstwa handlowe, urzędy i instytucje państwowe mające szczególne wymagania dotyczące niezawodności transmsji, jej jakości i ochrony danych.

Ogólna koncepcja budowy sieci MAN polega na zainstalowaniu węzłów sieci (urządzeń komutacyjno - transmisyjnych) w obiektach central miejskich i połączeniu ich cyfrowymi łączami 2 Mbps. W obiektach central międzymiastowych będą zainstalowane urządzenia do połączeń międzysieciowych:
- z innymi sieciami MAN;
- z innymi sieciami transmisji danych np. POLPAK, ISDN;
- z sieciami innych operatorów;

oraz siecią szkieletową.

Sieci MAN będą miały strukturę dwupoziomową:
- poziom komunikacyjny realizowany przez węzły połączone kanałami cyfrowymi o przepływności 2 Mbps utworzonymi na bazie międzycentralowych łączy światłowodowych;
- poziom dostępowy realizowany poprzez przyłączenie systemów komputerowych użytkowników do najbliższych węzłów sieci MAN.

Topologia sieci MAN będzie dostosowana do istniejącej infrastruktury telekomunikacyjnej TPSA w poszczególnych miastach.

Urządzenia sieci MAN zapewnią wymianę danych pomiędzy sieciami LAN pracującymi zgodnie z protokołami: TCP/IP, Novell IPX, DECnet, HP Advancenet i innymi , a także współpracować będą z sieciami WAN realizującymi protokoły X.25, Frame Relay, PPP, SNA a w przyszłości ATM [1].

Niezależnie od budowanych sieci metropolitalnych , sieć POLPAK będzie w dalszym ciągu eksploatowana, stanowiąc naturalne uzupełnienie wszędzie tam, gdzie jeszcze nie istnieje struktura łączy cyfrowych (światłowodowych) wysokiej jakości.

6. Usługi teleinformatyczne

O atrakcyjności działania poszczególnych sieci poza ich szybkością transmisji decydują usługi teleinformatyczne, jakie są dostępne dla potencjalnych abonentów. Oczywiście w chwili obecnej trudno jest jeszcze mówić o powszechnych usługach multimedialnych, choć na pewno jest to niedaleka przyszłość, ale usługi takie jak poczta elektroniczna będą wkrótce dostępne dla klientów TPSA. Aktualnie jest na ukończeniu postępowanie przetargowe, prowadzące do instalacji poczty elektronicznej działającej zgodnie ze standardem X.400 wraz z książką teleadresową wg. X.500 oraz modułem EDI. Szerszy opis tych usług znajduje się w innym referacie.

Wychodząc naprzeciw potrzebom naszych klientów w zakresie transmisji danych, sieci będące w posiadaniu TPSA poza pocztą elektroniczną będą świadczyć usługi typu:
- dostęp do krajowych i zagranicznych baz informacyjnych;
- dostęp do usług sieci INTERNET;
- szybką obsługę połączeń i przydzielanie pasma przenoszenia na żądanie;
- ochronę przesyłanych i przechowywanych danych.

Ponadto rozwój sieci ISDN umożliwi realizację usług takich jak: widetelefonia, wideokonferencje, dostęp do baz grafiki i danych, jak również pozwoli na świadczenie usług multimedialnych.

TPSA stwarza możliwości dołączania prywatnych baz danych do swoich sieci. Jeśli właściciel bazy danych chce pobierać opłaty za korzystanie z tej bazy, to musi stworzyć własny system

taryfikacji, np. przydzielać każdemu użytkownikowi uprawnienia (hasło) do korzystania z bazy. Ponadto powinien ubiegać się o status service providera TPSA.
Telekomunikacja Polska S.A. planując rozwój usług teleinformatycznych, współpracuje i korzysta z doświadczeń z uczelni, instytutów, ośrodków naukowo - badawczych oraz innych operatorów (np.NASK).

7. Literatura

1. Karpeta M., Suskiewicz M.: Ogólnodostępne sieci metropolitalne TPSA, Materiały z konferencji POLMAN'95, OWN Poznań 1995r.
2. Kępkowicz J.: Tygodnik Gospodarczy, Informator Targów, Infosystem-Multimedia-Poligrafia, Poznań 1995r.
3. Lisiecki B.: SDH moda, czy konieczność, Świat Telekomunikacji, nr.2., Warszawa, październik 1994r.
4. Technology Planning Survey - Network World, 4 NetWorld, luty 1995r.

Krzysztof Trzewik
Telekomunikacja Polska S.A.

Centrum SystemówTeleinformatycznych Telekomunikacji Polskiej S.A.

Centrum SystemówTeleinformatycznych Telekomunikacji Polskiej S.A. mieści się w Warszawie, przy ul Nowogrodzkiej 47A. Jest jedną z kilku jednostek "centralnych" Telekomunikacji Polskiej S.A. działających na terenie całej Polski. Centrum zostało utworzone w styczniu 1993 r. przez wydzielenie ze struktury Centrum Radiokomunikacji i Telekomunikacji systemu do pakietowej transmisji danych wraz z dwunastososobową grupą pracowników technicznych obsługujących system. Zadanie zorganizowania jednostki powierzono Krzysztofowi Trzewikowi, który obecnie jest jej dyrektorem.

POLPAK bo tak brzmi potoczna nazwa systemu, zbudowany został na bazie urządzeń francuskiej firmy ALCATEL i oddany do eksploatacji 16 czerwca 1992 r. Sieć składa się z 19 central jest w pełni kompatybilna z międzynarodowymi standardami CCITT: X.25, X.28, X.29, X.32, X.75. Pod tymi technicznymi nazwami kryje się opracowany ponad 30 lat temu na potrzeby armii amerykańskiej specjalny protokół transmisji danych przez zwykłe, często złej jakości łącza telefoniczne. Protokół ten zapewnia bardzo wysoką wiarygodność transmisji. POLPAK umożliwia jednoczesną transmisję (nadawanie i odbieranie) danych do wielu abonentów sieci, którzy mogą pracować z różnymi szybkościami od 1200 do 64000bitów/s. Pozwala na definiowanie kanałów wirtualnych (PVC) oraz tworzenie zamkniętych grup użytkowników (CUG). Z sieci POLPAK, jej abonenci mogą łączyć się z abonentami i bazami danych w ponad 100 sieciach w całym świecie.

Sieć połączona jest z siecią satelitarną V-SAT, której operatorem również jest TP S.A i umożliwia błyskawiczne uruchomienie transmisji wszędzie tam gdzie brakuje infrastruktury kablowej. Umożliwia też wszystkim abonentom sieci POLPAK bezpośrednie przesyłanie wiadomości w ogólnopolskim systemie przywoławczym POLPAGER (popularne już "bipery").

Obecnie sieć liczy blisko 1500 portów i prawie wszystkie już są zajęte.

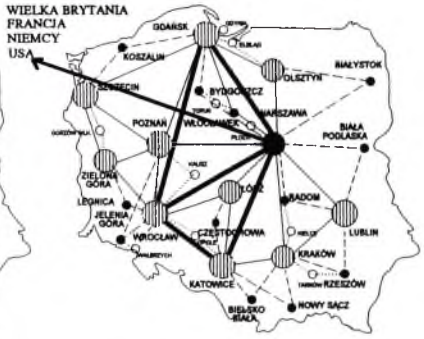
Rozpoczęta rozbudowa do końca 1995 roku zwiększy jej zasoby o ponad 20 następnych central i pojemność do ponad 3000 portów, umożliwi wydzielanie prywatnych sieci wirtualnych (VPN) i pracę z szybkościami 64 Kb/s a nawet 2 Mb/s. Szybkość 2 Mb/s będzie realizowana początkowo tylko pomiędzy Warszawą, Katowicami, Gdańskiem, Poznaniem i Wrocławiem. W miarę narastających potrzeb abonentów szybkość łączy międzywęzłowych sieci będzie zwiększana do 2 Mb/s na wszystkich kierunkach. Protokołem międzywęzłowym będzie protokół FRAME RELAY.

Podstawowymi użytkownikami sieci są duże firmy o rozproszonej strukturze jak hurtownie, duże firmy produkcyjne, firmy zagraniczne mające swoje centra zarządzania poza granicami Polski i w coraz większym zakresie administracja państwowa i samorządowa oraz banki. POLPAK wykorzystywany był do obsługi obsługi wyborów we wrześniu 1993 r. oraz w czerwcu1994 r.

Zapotrzebowanie na usługi teleinformatyczne narasta lawinowo. Dlatego najbliższe plany to uruchomienie, jeszcze w roku 1995 systemu obsługi wiadomości (MHS) popularnie zwanego pocztą elektroniczną X.400/X.500 oraz uruchomiemie szybkiej szieci szkieletowej z protokołem FRAME RELAY.

Poczta elektroniczna będzie dostępna w całej Polsce przez sieć telefoniczną dzięki rozbudowanej strukturze sieci POLPAK i będzie mogła obsłużyć początkowo ok. 5000 abonentów w tym również abonentów EDI. System będzie rozbudowywany w miarę narastających potrzeb.

OBECNY STAN SIECI TRANSMISJI DANYCH POLPAK



PRZEWIDYWANY STAN SIECI TRANSMISJI DANYCH POLPAK NA KONIEC 1994R. PO ZAKOŃCZENIU JEGO ROZBUDOWY. ORAZ SIECI REGIONALNE: LEGNICA, KOSZALIN, ZIELONA GÓRA

Budowa szybkiej, szkieletowej sieci transmisji danych POLPAK-T związana jest z rozpoczętą budową w 12 największych miastach Polski sieci metropolitalnych (MAN). Ponadto służyć będzie do tranzytu informacji prywatnych sieci pakietowych (WAN-WAN) oraz dużych sieci lokalnych (LAN-LAN). Sieć będzie pracowała z prędkością od 64 kb/s do 2 Mb/s. Zakłada się, że w miarę narastających potrzeb i rozwoju infrastruktury światłowodowej sieci pierwotnej, kolejne centrale będą zlokalizowane we wszystkich miastach wojewódzkich. Zakłada się również technologiczny rozwój sieci w kierunku ATM w perspektywie lat 3 w miarę standaryzacji protokołu oraz wzrost szybkości transmisji do 34 a nawet 155Mb/s.

Wreszcie INTERNET !

We współpracy z Naukową Akademicką Siecią Komputerową (NASK) trwają przygotowania do uruchomienia usługi Internetu komercyjnego. Usługa ta powinna wystartować jeszcze przed wakacjami.

Nowoczesne systemy na ogół pracują bezobsługowo, jednak dziś w CST zatrudnionych jest już ponad 50 pracowników. Są to młodzi ludzie, przeważnie z wykształceniem wyższym, którzy pracują głównie nad dalszym rozwojem systemów. Tu znajduje się laboratorium w którym testowane są najnowsze urządzenia pochodzące od najbardziej renomowanych firm światowych zanim zapadnie decyzja wyboru dostawcy lub zakupu wybranej technologii. W tym zakresie Centrum stale współpracuje z Politechniką Warszawską, z Naukową Akademicką Siecią Komputerową a w wybranych zagadnieniach z ekspertami z Katedry Informatyki Akademii Górniczo-Hutniczej w Krakowie, Politechniki Wrocławskiej oraz Instytutu Łączności.

Ponadto w CST zlokalizowane jest Centrum Zarządzania Siecią pracujące 24 godz/dobę, 365 dni w roku, wykonujące zdalne procedury testowe i świadczące bezpośredni serwis abonentom na zasadzie "gorącej linii". Ponadto w kraju zatrudnionych jest ok. 30 pracowników TP S.A. nadzorujących pracę pozostałych central i świadczących serwis ich abonentom.

Sieć charakteryzuje się wysoką niezawodnością ale na wypadek awarii (odpukać!) w Centrum Systemów Teleinformatycznych utrzymywany jest magazyn części zamiennych, które w ramach potrzeb przesyłane są przy pomocy poczty kurierskiej, przesyłek PKP nadawanych bezpośrednio do pociągów expresowych. W stałej gotowości do wyjazdu są 2 samochody serwisowe z kompletem cześci zamiennych i zapasowym węzłem sieci

gotowym do wymiany w przypadku katastrofalnego uszkodzenia centrali. Ekipy naprawcze w przypadku niemożności zdalnego usunięcia uszkodzenia w ciągu godziny od powstania awarii gotowe są do wyjazdu. Główne węzły sieci mają konstrukcję zdublowaną a wymiana uszkodzonych pakietów może odbywać się bez zatrzymywania pracy centrali.

Wojciech Hałka
Andrzej Zienkiewicz

Refleksje z posiedzeń klubu operatorów telekomunikacyjnych

Klub operatorów telekomunikacyjnych powstał z inicjatywy Zastępcy Dyrektora Biura d/s Informatyki Urzędu Rady Ministrów Witolda Łuczywo. Pierwsze posiedzenie klubu odbyło się w końcu 1993 roku w Rydzynie w czasie spotkania informatyków wojewódzkich z kierownictwem Biura d/s Informatyki.

Klub nie posiada struktury organizacyjnej, nie podejmuje żadnych postanowień, wobec czego nie odbywają się w czasie jego posiedzeń głosowania czy inne formy ustalania jednolitego stanowiska uczestników. Od początku w posiedzeniach klubu aktywnie uczestniczą przedstawiciele URM, Ministerstwa Łączności, POLPAKu, TELBANKu, KOLPAKu, NASKu, PKONETu i inni. Klub koncentruje przedstawicieli operatorów sieci przede wszystkim świadczących usługi teleinformatyczne.

Jak pisałem wyżej klub jest miejscem swobodnej dyskusji, w której każdy ma prawo pozostania przy swoim stanowisku. Nie świadczy to o zasadniczych rozbieżnościach między operatorami. Raczej uznałbym, że istnieje nadspodziewany konsensus wśród członków klubu. Napisałem powyższe stwierdzenie dlatego, że nie istnieje żądne oficjalne stanowisko klubu operatorów telekomunikacyjnych. Wobec tego poczynione obserwacje i refleksje są tylko moje własne i tylko ja ponoszę odpowiedzialność za wszystko co niżej napiszę.

Już od pierwszych spotkań klubu operatorów telekomunikacyjnych podstawowym przedmiotem zainteresowania był wyraźny niedostatek przepisów prawnych regulujących działalność w dziedzinie telekomunikacji oraz współdziałanie operatorów. Pomijam oczywiście emocjonalne wystąpienia szczególnie mniejszych operatorów oraz próby montowania koalicji przeciwko szczególnie Telekomunikacji Polskiej SA. Wszyscy więksi operatorzy nie są skłonni do brania udziału w rozgrywkach mających na celu dyskryminację innego operatora. Przeważa chęć do współpracy oraz poszukiwania właściwych form działania na rynku telekomunikacyjnym.

Analiza obowiązującego prawa wykazuje brak regulacji w prawie karnym, administracyjnym, prasowym i autorskim regulacji przydatnych lub obowiązujących w działalności operatorów telekomunikacyjnych. Podobnie regulacje Ustawy o Łączności nie są zadawalające zwłaszcza dla operatorów działających w obszarze teleinformatyki. Zgodzono się z przedstawicielem Ministerstwa Łączności, że opracowanie właściwych i ostatecznych regulacji przez ministerstwo lub przez sejm nie jest możliwe, ponieważ dziedzina jest zbyt młoda, szybko zmieniająca się, nie posiadająca ustabilizowanych reguł działania. Uznano, że operatorzy sami powinni opracować odpowiednie regulacje zawarte w regulaminach działania oraz stworzyć swojego rodzaju 'gentleman agreement' w stosunkach międzyoperatorskich. Dopiero po sprawdzeniu w praktyce prawa kontraktowego oraz zdobyciu koniecznych doświadczeń będzie można przystąpić do prac legislacyjnych.

Kolejnym przedmiotem dyskusji była problematyka współpracy międzyoperatorskiej, szczególnie w układzie Telekomunikacja Polska SA inni operatorzy. Dyskusja dotycząca współpracy wywoływała szczególnie dużo, wydaje się nieuzasadnionej emocji. Dla lepszego zbadania problemu zorganizowane jedno spotkanie w całości poświęcone zagadnieniom współpracy Telekomunikacji Polskiej SA jak szczególnie wyróżnionego Ustawą o Łączności i innych operatorów działających na podstawie uzyskanych zezwoleń telekomunikacyjnych. Z dyskusji wyniosłem wrażenie , że współpraca jest znacznie lepsza w praktyce niż w zakresie ustalania reguł tej współpracy.

Szczególnie zawzięte dyskusje toczyły się wokół koniecznego zakresu oraz ram i formy konkurencji. Zwolennicy niczym nie skrępowanej walki konkurencyjnej pochodzili z poza

środowiska operatorów lub reprezentowali małe lub dopiero rozpoczynające działalność organizacje. Uważali, że tylko istnienie nieskrępowanej konkurencji ułatwi im start. Operatorzy ustabilizowani takich tendencji nie mają. Uważam, że taki podział jest ekonomicznie uzasadniony. Wbrew popularnym czy forsowanym przez publikatory sądom dzika konkurencja w naszej dziedzinie musi przynieść szkody. Dzieje się tak, ponieważ budowa systemów telekomunikacyjnych jest przedsięwzięciem długotrwałym i kosztownym. Aby to się opłacało, lub tylko nie prowadziło do zniszczenia operatora konieczne jest istnienie rynku, który umożliwi chociaż zwrot poniesionych nakładów inwestycyjnych.

Rynek telekomunikacyjny dla usług interesujących operatorów telekomunikacyjnych jest potencjalnie duży, ale dziś jeszcze bardzo płytki. Jego nadmierne dzielenie musi doprowadzić do zniechęcenia do inwestowania lub spowodować upadek lub conajmniej straty u istniejących operatorów. Dotyczy to również tej działalności Telekomunikacji Polskiej SA, którą są zainteresowania operatorzy zrzeszeni w klubie, to znaczy działalności polegającej na budowie łączności pierwotnej w sieci przede wszystkim międzymiastowej. Pozornie istnieje głęboki deficyt telefonów, szczególnie na wsi, jednak potrzebne nakłady i konieczny czas realizacji nie stwarza dobrych perspektyw dla zwrotu nakładów już dziś lub najbliższym czasie.

Z tego powodu zrozumiałe jest stanowisko Ministra Łączności dążącego do zachowania monopolu Telekomunikacji Polskiej SA w zakresie łączności międzymiastowej do czasu uzyskania zwrotu lub gwarancji zwrotu nakładów poniesionych na budowę infrastruktury.

W tym świetle wydają się niezrozumiałe opory Telekomunikacji Polskiej SA prze dzierżawieniem tej infrastruktury innym operatorów, jak również niechęć do wspólnych przedsięwzięć. Oczywiście opory mają swoje podłoże wewnętrzne, ale to jest sprawa wewnętrzna spółki. Jednak obserwując trudności kolegów muszę zauważyć, że wynika to raczej z braku uregulowań prawnych. Wydaje się, że Minister łączności ustalając monopol w jakieś dziedzinie powinien wydać regulacje wykonywania tego monopolu. Inaczej możliwe są zachowania monopolistyczne, przypadkowe i bardziej zorganizowane, jak również próby regulacji tych zachowań na podstawie aktów wewnętrznych Telekomunikacji Polskiej SA i innych operatorów telekomunikacyjnych. Ministerstwo Łączności zamierza w tej sprawie skorzystać z zapisów nowelizowanej Ustawy o Łączności ustalając ogólne warunki świadczenia usług telekomunikacyjnych.

Tymczasem próba szukania uregulowań normujących współpracę między operatorami sieci telekomunikacyjnych doprowadziła tylko do Zarządzenia Ministra Łączności Nr. 9 dotyczącego współdziałania przy telefonizacji wsi. Nie ma w tym zarządzeniu żadnych odniesień pozwalających na odniesienie jej postanowień do operatorów działających w klubie operatorów. Ponadto zarządzenie ma charakter jedynie zalecenia, a nie bezwzględnie obowiązującego przepisu, gdyż do takiej regulacji nie ma stosownej delegacji w Ustawie o Łączności z 1990 roku. Oczywistym jest, że w tym stanie prawnym bez odpowiedniej nowelizacji regulacji ustawowych nie wiele można oczekiwać.

Czy formuła klubu operatorów jest słuszna. W trakcie spotkań klubu zgłaszano kilkakrotnie propozycje "uporządkowania " jego funkcjonowania, aby mógł stać się grupą nacisku, opiniującą itp. Wszystkie propozycje w tym zakresie nie spotkały się z pozytywnym oddźwiękiem. Jednocześnie występuje zmienność uczestników spotkań, ponieważ część uczestników, zwłaszcza usiłujących wykorzystać klub do załatwiania swoich interesów rezygnuje z uczestnictwa w spotkaniach. Podobnie operatorzy nie posiadający pełnej swobody decyzji w zakresie form działania, prawdopodobnie nie znajdują w klubie spraw interesujących. Luźna formuła klubu stwarza jednak płaszczyznę do nieskrępowanej wymiany doświadczeń oraz dyskusji. Tym samym klub jest miejscem, gdzie stosunkowo dobrze można wymienić szczere poglądy, ponieważ uczestnicy nie są związani oficjalną opinią swoich instytucji. Podobnie nie

istnieje bezwzględna konieczność ukrywania swoich słabości czy niepewności co do dalszego postępowania czy rozwoju działalności.

Z pewnością może razić pozorne ubóstwo zakresu tematyki refleksji. Wynika ono jedynie z wybrania przez autorów tematyki zdaniem ich podstawowej. Dojście w zakresie regulacji prawnych oraz uregulowania współpracy operatorów do konsensusu jest przedsięwzięciem gigantycznym, nie na skalę rozwiązań klubowych. Zresztą w tym zakresie nie odstajemy szczególnie od reszty nawet rozwiniętego świata. Uzyskanie w tej sytuacji nawet cząstkowej informacji dla dalszych własnych przemyśleń jest dla członków klubu szczególnie ważne.

dr Krzysztof Heller
Qumak International

Internet - najnowsze trendy

Popularność Internetu od pewnego czasu niezwykle rośnie. Temat ten wyszedł już dawno poza ramy środowisk naukowych i trafił nawet do popularnej prasy, zamieszczającej różnorakie, niekiedy wręcz sensacyjne, artykuły o możliwościach wykorzystania tej sieci w wielu dziedzinach życia. W niniejszym wystąpieniu spróbuję podsumować pojawiające się trendy i perspektywy rozwoju. Z góry zastrzegam, że prezentuję jedynie osobiste poglądy, a moje przewidywania mogą być błędne.

Usługi i narzędzia

Ostatnie kilka lat jest okresem niezwykle dynamicznego wzrostu wykorzystania Internetu i rosnącego zainteresowania ze strony środowisk komercyjnych. W ostatnim roku można wręcz mówić o modzie na Internet. Liczbę osób korzystających z Internetu szacuje się na 35 milionów, w tym ok. 25 milionów robi to prawie codziennie. Jest wiele organizacji oferujących dostęp do sieci i inne związane z tym usługi. W Londynie otworzono nawet kawiarnię Internetową "Cyberia", w której za niewielką opłatą można przez pół godziny posiedzieć przy stacji z WWW czy innymi usługami sieciowymi. Furorę robi WWW i inne serwery multimedialne, co oczywiście znacznie zwiększa ruch na sieci i wymagania wobec używanego sprzętu. Na bieżąco rozwijane są programy ułatwiające korzystanie z różnych zasobów informacyjnych. Najpoważniejsze firmy produkujące oprogramowanie wbudowują możliwość łączności z Internetem do swoich systemów operacyjnych i programów użytkowych. Microsoft zdecydowanie wierzy w nadejście ery 'sieciowego społeczeństwa', Wiele instytucji komercyjnych chce wykorzystać korzyści płynące z dostępu do sieci. Uważa się powszechnie, że dostęp do sieci pozwala uzyskać dodatkowe korzyści, przewagę nad konkurencją oraz przyspiesza rozwój. Otwierają się także całkowicie nowe możliwości prowadzenia działalności gospodarczej z wykorzystaniem sieci, jak na przykład prowadzenie marketingu i sprzedaży przez sieć, dostarczanie wsparcia technicznego i oprogramowania do użytkowników itp.

Internet oferuje olbrzymią różnorodność usług polegających na pozyskiwaniu lub wymianie informacji. Ponieważ rozwój mechanizmów prezentacji i wymiany informacji jest niezwykle żywiołowy, a ilość dostępnej informacji rośnie w niezwykle szybkim tempie, pojawia się problem efektywnego dotarcia do pożytecznej informacji. Niestety duża swoboda w generowaniu informacji przez użytkowników pociąga za sobą spory szum informacyjny, żeby nie powiedzieć bełkot. Ponadto jest wiele miejsc i sposobów przechowywania informacji. Chcąc znaleźć pożądaną wiadomość musimy wiedzieć gdzie jej szukać i użyć odpowiedniego narzędzia do przeglądania.

Aby ułatwić wyszukiwanie informacji buduje się różnego typu automatyczne systemy wyszukiwania, które na podstawie zadanego zapytania zawierającego słowa kluczowe mają odnaleźć "gdzieś w sieci" informacje na dany temat. Te wyszukiwacze są mniej lub bardziej zaawansowane; najlepsze, jak np. InfoSeek, potrafią analizować informacje zawarte w serwerach WWW, grupach news, artykułach z periodyków komputerowych, bazach danych o firmach, produktach, itp. Wydaje się, że w przyszłości staną się niezbędnymi asystentami użytkowników sieci. Oczywiście na razie mówimy o produktach pracujących w obszarze języka angielskiego, ktory jest uniwersalnym językiem sieci.

Dostawcy usług sieciowych

Usługi sieciowe świadczone są w sposób ograniczony - przez organizacje powołane dla obsługi określonych grup użytkowników (np. szkół wyższych) - bądź nieograniczony - przez organizacje obsługujące każdego płacącego za świadczone usługi. Ten pierwszy sposób jest początkowo łatwiejszy do zrealizowania, w ten sposób zaczynały wszystkie sieci narodowe. W miarę rozwoju sieci komercyjnych zaczyna się jednak problem podziału rynku - część instytucji używa subsydiowanej usługi, a część płaci pełne stawki. Biorąc pod uwagę zawsze istniejącą szarą strefę podziału między tymi dwiema grupami i trudność jednoznacznego zakwalifikowania wszystkich starających się o dostęp do sieci, w pewnym momencie należy przejść na subsydiowanie użytkowników, a nie usługodawców. Ten zdecydowany krok zrobiono w USA, gdzie zrezygnowano z finansowania NFSNET, na rzecz NREN opartego o prywatne firmy. Dzięki temu wprowadza się element konkurencji między dostawcami, co generalnie służy poprawie jakości usług i obniżce cen. Tworzy to nowy model funkcjonowania sieci narodowych, który powinien być poważnie przemyślany w Europie.

Komercyjni dostawcy usług sieciowych konkurują ze sobą, prześcigając się w oferowanych możliwościach i cenach. Na przykład w Wielkiej Brytanii jest obecnie ponad dwadzieścia firm oferujących dostęp do Internetu i inne usługi sieciowe. Wychodzą one z ofertą do wszystkich segmentów rynku, w tym do indywidualnych użytkowników, proponując ceny usług na stosunkowo niskim poziomie, nastawionym na obsługę masowego użytkownika.

Ponieważ wszyscy operatorzy, chcąc nie chcąc, muszą ze sobą współpracować aby dać swoim użytkownikom dostęp do całego Internetu, a nie tylko swojej części, tworzone są różne punkty łączności i wymiany. Historycznie pierwszy CIX (Commercial Internet Exchange) ciągle jest największym punktem spotkań różnych operatorów. W ślad za nim idą inne, mniejsze punkty wymiany, takie jak LINX (London Internet Exchange), łączące Pipex, EuNet, JANET i Demon. Są także bilateralne połączenia pomiędzy dwoma dostawcami. Skutkiem tych działań jest siatka połączeń międzyoperatorskich, z różnymi drogami zapasowymi, znakomicie zwiększająca niezawodność (i niekontrolowalność) sieci.

Bardzo istotnym aspektem komercjalizacji sieci jest stworzenie mechanizmów umożliwiających prawidłowe rozliczanie wykorzystania sieci (transportu danych) i usług (korzystania z serwerów informacyjnych). O ile to pierwsze jest, przy obecnie stosowanych protokołach, praktycznie niemożliwe, o tyle to drugie jest już praktycznie wbudowywane w istniejące serwery. Chodzi oczywiście o to, aby móc rozliczać wykorzystywanie pracowicie przygotowywanej informacji. Wprawdzie na razie większość serwisów informacyjnych jest darmowa, ale nie jest wykluczone, że niebawem dojdziemy do sytuacji, w której informacja posiadająca jakąkolwiek wartość będzie traktowana jako towar na sprzedaż. Może to spowodować wycofanie się z niektórych udogodnień technicznych, aby w pełni utrzymać kontrolę nad dostępem do informacji. Na przykład takie sensowne rozwiązanie jak przechowywanie zapytań (caching) aby nie zadawać ich powtórnie do serwera, co obniża ruch na sieci, jest sprzeczne z koniecznością rejestrowania na serwerze każdego zapytania.

Politycy i regulatorzy

Sieci komputerowe stały się tak ważnym tematem, że przyciągnęły uwagę polityków. Jak to często bywa, decydenci tworzący reguły nie do końca zdają sobie sprawę ze stopnia komplikacji problemów związanych z siecią. Nie przeszkadza to im jednak w wychodzeniu z różnorakimi inicjatywami. W lutym tego roku odbyło się spotkanie gupy G7 (siedmiu najbardziej rozwiniętych państw świata) poświęcone rozwojowi społeczeństwa informatycznego. W trakcie spotkania starano się ustalić podstawowe założenia przyświecające dążeniom do stworzenia globalnej

infrastruktury informatycznej (GII). Uzgodniono osiem punktów, przyjmujących, że GII powinno:

1. promować zdrową konkurencję
2. przyciągać prywatne inwestycje
3. określać odpowiednio dopasowaną strukturę regulującą jej działanie
4. zapewniać otwarty dostęp do sieci
5. dać uniwersalną możliwość oferowania i dostępu do usług
6. dawać jednakowe preferencje wszystkim obywatelom
7. promować zróżnicowane treści, w tym zróżnicowanie językowe i kulturowe
8. dostrzegać konieczność ogólnoświatowej współpracy, ze szczególnym uwzględnieniem słabiej rozwiniętych krajów

Te założenia, niewątpliwie słuszne, nie zawsze są łatwo realizowalne. Na przykład zapewnienie jednakowych preferencji wszystkim obywatelom jest tematem gorącej dyskusji w wielu krajach. Istnieje obawa, że pewne grupy obywateli, czy to ze względu na zamożność, czy też miejsce zamieszkania, mogą być odcięte od dostępu do sieci. Rejony o niskiej gęstości zaludnienia nie są ponętnym miejscem inwestycji w infrastrukturę telekomunikacyjną. Można to wymusić ustawowo, jak w USA, gdzie operator sieci telefonicznej nie ma prawa odmówić doprowadzenia linii do klienta; lub technologicznie, tworząc sieć satelitów komunikacyjnych pokrywających swym zasięgiem całą kulę ziemską.

Aby postąpić naprzód, należy podjąć konkretne kroki zmierzające do osiągnięcia przyjętych celów. Na początek postanowiono skoncentrować się na:

1. zapewnieniu powszechności dostępu
2. deregulacji rynku usług, infrastruktury, sprzętu i inwestycji, zwłaszcza w dziedzinie telekomunikacji
3. wprowadzeniu otwartych standardów
4. zapewnieniu otwartego dostępu dostawców usług do sieci
5. uczciwym podziale dostępnych częstotliwości i pasm pomiędzy kraje i usługi
6. wygaszaniu działań protekcjonistycznych i promowaniu produktywnej współpracy

Szereg z tych działań będzie godziło w istniejący stan rzeczy. Przykładem może być dziedzina monopoli telekomunikacyjnych w Europie. Natychmiastowa liberalizacja rynku nie będzie skuteczna, gdyż istniejący dotychczasowi monopoliści mają olbrzymią przewagę kilkudziesięciu lat inwestycji w infrastrukturę. Zamiast tego należy stworzyć odpowiedni system regulacji prawnych, doprowadzający stopniowo do w pełni otwartego rynku. Podobnie wygląda sytuacja dostawców usług sieciowych. Najlepszym przykładem skutecznej polityki otwierania na konkurencję jest Wielka Brytania, gdzie poziom usług telekomunikacyjnych i sieciowych jest bardzo wysoki, a ceny niskie.

Prawa użytkowników

Użytkownicy Internetu stanowią tradycyjnie raczej anarchistyczną społeczność, która bardzo sobie ceni swobodę jednostek i nie poddaje się łatwo uniformizacji i zewnętrznym naciskom. Wszelkie próby ograniczenia swobody spotykają się ze zdecydowanym oporem. Szczególnie widać to na rynku amerykańskim, gdzie przywiązanie do wolności jednostki walczy z

poszanowaniem cudzych poglądów. Trwa gorąca dyskusja, jakie treści mogą, a jakie nie mogą być transmitowane przez Internet. Pornografia, wypowiedzi nawołujące do czynów sprzecznych z prawem czy prezentujące rasistowskie poglądy powinny być, zdaniem jednych, zakazane. Zdaniem innych takie zakazy to naruszenie prawa do swobodnego wypowiadania swoich poglądów. Zupełnie inną sprawą jest oczywiście praktyczna niemożliwość kontrolowania takich wypowiedzi.

Choć Internet jest siecią publiczną, to jego użytkownicy powinni mieć prawo do prywatności i anonimowości. Mają prawo zakładać, że ich korespondencja nie będzie czytana przez osoby trzecie. Najprostszą metodą osiągnięcia tego celu jest szyfrowanie. To z kolei jest bardzo drażliwym tematem w USA, gdzie np. zakazany jest eksport wszelkich urządzeń czy oprogramowania szyfrującego. Służby bezpieczeństwa chcą mieć możliwośc deszyfracji każdej wiadomości przesyłanej w sieci. Oczywiście za zezwoleniem sądu, ale zawsze możliwe są nadużycia. Szerokie rzesze użytkowników są zasadniczo przeciwne jakimkolwiek tego typu pomysłom. Dzięki masowym protestom wydje się, że zrezygnowano z pomysłu kości szyfrującej Clipper z 'tylnim wejściem' zezwalającym na dostęp upoważnionym służbom. Obecnie władze proponują deponowanie kluczy szyfrujących, z możliwością wykorzystania ich do deszyfracji komunikatów w uzasadnionych przypadkach. Jednak i to rozwiązanie budzi szereg wątpliwości, a chęć wymuszenia takiego obowiązku na drodze prawnej jest torpedowana.

Pokrewnym zagadnieniem jest zachowanie anonimowości. Przy poszukiwaniu sprawcy włamań do sieci starano się dotrzeć do tożsamości autora poczty wysyłanej z pomocą anonimowego serwera anon.penet.fi. Ponieważ włamania miały miejse w USA, a serwer jest w Finlandii, dopiero działanie 'na granicy prawa' doprowadziło do ingerencji fińskiej policji i ujawnienia tożsamości. Rozpętało to wielką dyskusję o prawie do anonimowości i sytuacjach, w których można to prawo naruszać. I to zagadnienie będzie musiało być w przyszłości rozwiązane w klarowny i powszechnie akceptowalny sposób.

Odrębną sprawą jest rozwiązanie ochrony własności intelektualnej, w szczególności wypłacanie honorariów autorom dzieł wykorzystywanych w Internecie. Jest to łatwe koncepcyjnie, ale bardzo trudne technicznie. Na przykład wykorzystywanie fotografii czy rysunków w serwerze WWW wymagałoby rejestracji każdego wykorzystania i przekazywania odpowiednich opłat autorom. Z drugiej strony użytkownicy musieliby być w jakiś sposób rejestrowani i sami płacić za wykorzystanie tych materiałów. Wydaje się, że prowadzenie tego typu obliczeń wymaga więcej zachodu i nakładów niż korzyści z tego płynące.

Prawne aspekty sieci

Politycy przygotowują prawa i reguły postępowania, przygotowując grunt dla prawników. Dopóki Internet był domeną naukowców, nie było potrzeby do analizy przepisów prawnych pod kątem zastosowań w Internecie. Teraz jednak wydaje się, że przez najbliższe parę lat Internet będzie rajem dla prawników, wynajdujących nowe precedensy i szukających zastosowania istniejących przepisów do sieci komputerowych. Będzie też zapewne terenem walki z pojawiającymi się negatywnymi zjawiskami. Jednym z nich, bardzo spektakularnym i nagłaśnianym w prasie, są włamania do systemów komputerowych. Często są wyłącznie próbą 'sprawdzenia się', ale bywają też przestępstwem. Wykrycie sprawców jest trudne, a umocowanie prawne do ścigania tego typu przestępstw raczej słabe. Powstała organizacja (CERT) zajmująca się wyszukiwaniem słabych stron systemów komputerowych i zabezpieczaniem przed penetracją z zewnątrz. Rozpowszechnia ona informacje i programy mające służyć zwiększeniu poziomu zabezpieczeń. Wydaje się, że pozostaje kwestią czasu powołanie 'Internetowej policji' wykrywającej komputerowych przestępców.

Bardzo ważne jest rozstrzygnięcie kwestii odpowiedzialności za propagowane w sieci informacje czy obrazy. Szczególnie dotyczy to dostawców usług, takich jak serwery systemu news czy bazy danych z anonimowym ftp, w których są deponowane pliki. W przypadku rozpowszechniania poprzez ich serwer materiałów sprzecznych z prawem (np. pornografii) mogą być pociągani do odpowiedzialności. Jest kwestią dyskusyjną czy należy interpretować to jako rozpowszechnianie takie, jak np. przy wydawaniu gazety i stosować zasady prawa prasowego? Nie ma też praktycznych możliwości kontroli wszystkich materiałów, co czyni wątpliwym obarczanie całą odpowiedzialnością administratora serwera. Co więcej, prawo bywa różne w różnych krajach czy stanach. Sieć z natury swojej jest globalna, i obejmuje obszary o różnym prawodawstwie. Rodzi to szereg wątpliwości. Czy przy pobieraniu informacji sprzecznej z prawem w miejscu, gdzie jest ona odczytywana, może być zaskarżony operator serwera, jeżeli serwer ten stoi w miejscu, gdzie taka informacja jest legalna?

Prawo uwzględniające specyficzne możliwości sieci komputerowych nie jest jeszcze stworzone. Jestem przekonany, że wiele będzie się działo w tej dziedzinie w najbliższych latach, zwłaszcza w USA.

Komercyjne wykorzystanie sieci

Do czego można w praktyce wykorzystać narzędzia i zasoby Internetu? W przypadku tradycyjnych użytkowników, a więc głównie środowisk badawczych i edukacyjnych, odpowiedź jest dość prosta. Jakie są jednak pożytki dla instytucji komercyjnych? Do jakich celów mogą one wykorzystywać Internet? Nie ma jednej odpowiedzi na to pytanie. Komercyjne wykorzystanie Internetu jest zjawiskiem stosunkowo młodym, występującym zaledwie od paru lat. Trwa szukanie nowych sposobów prowadzenia działalności gospodarczej przez Internet. Jak na razie wydaje się, że więcej jest przekonania, iż 'coś w tym musi byc' i poszukiwania formuł działania, niż rzeczywistych sukcesów komercyjnych. Tym niemniej, już dzisiaj można wskazać na pewne możliwości komercyjnego użycia sieci.

Najprostsze jest wykorzystanie Internetu w zakresie usług podstawowych, do transmisji poczty i innych danych w obrębie firmy. Korzystamy wówczas z sieci tak, jak z dostawcy usługi telekomunikacyjnej, tyle, że o zwiększonych możliwościach transmisji. Dzięki temu możemy uzyskać sprawny obieg informacji i dokumentów, nawet w przypadku znacznych odległości dzielących poszczególne lokalizacje firmy. Przekazywanie danych między placówkami firmy odbywa się na bieżąco. Przykładowo codzienny spływ informacji o sprzedaży i zapotrzebowaniu na towary z magazynów z oddziałów do centrali pomaga w bieżącym zarządzaniu firmą i elastycznym reagowaniu na potrzeby rynku. Wewnętrzna poczta komputerowa pozwala na szybką dystrybucję istotnej informacji zgodnie z przygotowanymi ścieżkami obiegu dokumentów. Można też tworzyć tematyczne grupy dyskusyjne przygotowujące pewne zadania, np. dyskutujące zastosowanie nowych technologii czy zmiany w systemie wynagrodzeń. Rozszerzeniem komunikacji tekstowej są wideokonferencje przekazywane siecią komputerową z jednych stanowisk komputerowych do innych. Wymagają one jednak przesyłania znacznie większej ilości informacji, a co za tym idzie większego pasma.

Innym ciekawym rozwiązaniem jest umożliwienie personelowi biurowemu zdalnej pracy z domu. Przydziela się określone zadania, np. przygotowanie analizy rynku czy oferty, a następnie odbiera i kontroluje rezultaty. Pracownicy nie muszą wówczas tracić czasu na dojazdy. Mogą także swobodniej dysponować swoim czasem, gdyż są rozliczani z wyników pracy, a nie z liczby przesiedzianych w biurze godzin. Jest to szczególnie istotne dla matek mogących zostać w domu z dziećmi, i tak sobie ułożyć pracę by mieć czas na obowiązki domowe. W USA pracuje w ten sposób kilkadziesiąt tysięcy ludzi i liczba ta stale rośnie. Oczywiście ten sposób pracy możliwy jest

jedynie dla niektórych zawodów i w części etatu. Raz na jakiś czas trzeba się stawić w biurze, choćby po to, żeby nie zapomnieć, jak wyglądają koledzy z pracy.

Najważniejszym atutem Internetu nie jest jednak możliwość przesyłania informacji od jednego użytkownika do drugiego, ale dostęp do informacji w ogóle. Dzięki włączeniu się do sieci mamy dostęp do bardzo wielu zasobów informacji, w tym w pewien sposób również do wiedzy kilkunastu milionów użytkowników, będących niejednokrotnie wybitnymi specjalistami w swoich dziedzinach. Często zgłoszenie problemu do listy dyskusyjnej przynosi w ciągu kilku godzin odpowiedź z rozwiązaniem, którego znalezienie w inny sposób byłoby niemożliwie lub bardzo uciążliwe.

Są specjalnie przygotowywane i utrzymywane bazy danych, które zawierają "najczystszą" informację, zbieraną u źródeł. Korzystanie z nich jest najczęściej płatne. Większość informacji pochodzi jednak od użytkowników, a jej zawartość jest podawana na zasadzie "as is", czyli nie bierze się za nią odpowiedzialności. Za to jest udostępniana za darmo, a są to niejednokrotnie bardzo cenne informacje. Na przykład archiwum listy dyskusyjnej o systemie operacyjnym UNIX jest źródłem rozwiązań wielu problemów, które mogą spotkać administratora systemu.

Poza szukaniem informacji poprzez Internet można również szukać partnerów do współpracy w najróżniejszych przedsięwzięciach, a także takie przedsięwzięcia realizować. Znane są przykłady zespołów oddalonych od siebie programistów piszących wspólnie oprogramowanie, zespołów projektowych uzgadniających kolejne wersje projektów przez Internet, czy wreszcie firm negocjujących kontrakt. Partnerów można znaleźć ogłaszając się w odpowiednich grupach dyskusyjnych lub zgłaszając swoją ofertę do specjalnych baz danych.

Nowym elementem w Internecie są próby działań marketingowych, reklama różnych produktów. Jest to bardzo kuszące dla producentów, gdyż daje możliwości dotarcia do kilkunastu milionów potencjalnych odbiorców stosunkowo małym kosztem. Z drugiej strony pewne ograniczenia na reklamę nakładają przyjęte w sieci dobre zwyczaje, zabraniające wysyłania materiałów ludziom, którzy mogą sobie tego nie życzyć. W przeciwnym przypadku wszystkie firmy wysyłałyby dziesiątki tekstów reklamowych do potencjalnych odbiorców, straszliwie zaśmiecając sieć. I tak co jakiś czas pojawiają się 'łańcuszki św. Antoniego' czy inne teksty, niepotrzebnie zużywające pasmo. Najczęściej jednak autorzy takich przesyłek spotykają się z gwałtowną reakcją innych użytkowników, polegającą na bombardowaniu tysiącami komunikatów, wysyłaniu apeli do ich dostawcy usług sieciowych o wyłączenie z sieci, czy nawet wysyłaniu faxów o całych czarnych stronach, mających zużyć toner i bęben maszyny.

Są oczywiście konkretne przykłady firm komercyjnych, prowadzących w różnych formach działalność z pomocą Internetu. I tak wiele firm komputerowych, jak np. Oracle, Hewlett-Packard, Microsoft, Silicon Graphics, itd., oferuje swoim klientom pomoc ('help desk') także przez Internet. Zgłaszane problemy są analizowane, a odpowiedź przekazywana klientowi. Najczęściej są to problemy typowe, których opisy z sugerowanymi rozwiązaniami są następnie przechowywane w skomputeryzowanej, automatycznie przeszukiwanej, bazie danych. Nowe, wcześniej nie występujące problemy, są do takiej bazy dopisywane. Inne firmy, jak DEC, Programmer's Shop czy Lufthansa, oferują możliwość sprzedaży przez sieć. Na razie wygląda to podobnie do sprzedaży wysyłkowej, gdzie do zrealizowania transakcji podaje się numer karty kredytowej. Promocję swoich wyrobów prowadzą w Internecie Ford, Dell i O'Reilly & Associates. Polega ona na udostępnianiu w serwerach typu WWW informacji o produktach i katalogów. Jest też cała gama firm prowadzących współpracę w dziedzinie badań rozwojowych ze znanymi uczelniami i laboratoriami. Nie są to tylko firmy z branży komputerowej, jak IBM, ale również firmy typowo przemysłowe, np. Schlumberger.

Pracuje się obecnie nad rozwiązaniami umożliwiającymi znaczne poszerzenie możliwości wykonywanych operacji. Opracowanie powszechnie akceptowalnych, bezpiecznych i wiarygodnych mechanizmów przekazywania danych pozwoli na dokonywanie przez sieć transakcji, przekazywanie zamówień, wystawianie faktur czy zawieranie umów handlowych. Oczywiście warunkiem do tego jest możliwość jednoznacznego zindentyfikowania nadawcy i zabezpieczenie przed podrobieniem "elektronicznego podpisu". Na razie, pomimo istnienia tego typu mechanizmów, firmy są dość ostrożne i nie spieszą się z ich użyciem. Obawa przed hackerami włamującymi się do systemów jest bardzo silna. Być może w przyszłości, po rozwiązaniu problemów, robienie z domu elektronicznych zakupów stanie się czymś powszechnym.

Trendy rozwoju

W rozwiniętym społeczeństwie opartym na gospodarce rynkowej, w którym dostęp we właściwym czasie do odpowiedniej informacji może stanowić o przewadze nad konkurencją, umiejętne wykorzystanie tak potężnego narzędzia wymiany informacji jak Internet powoli staje się niezbędnym elementem funkcjonowania organizacji. Wymaga to jeszcze udoskonalenia wielu rozwiązań technicznych oraz stworzenia nowych wzorców zachowań, ale płynące z tego korzyści będą przyciągały kolejne rzesze użytkowników. Choć dzisiaj czynione są dopiero pierwsze kroki na drodze komercyjnego wykorzystania Internetu na większą skalę, to jesteśmy świadkami początku nowej ery działania na odległość. Internet, czy mówiąc szerzej globalna infrastruktura informacyjna, jest w trakcie poważnej przebudowy i rozbudowy. Kładzione są fundamenty pod budowę 'ery informacji'. Kształtują się już pewne rozwiązania, ale większość z nich wymaga przedyskutowania i ostatecznego uzgodnienia. Zmierzamy w kierunku struktury informacyjnej obejmującej wszystkie obszary działalności i większość społeczeństwa. Wymaga to odpowiedniego kształcenia społeczeństwa, aby było w stanie umiejętnie wykorzystać to potężne narzędzie. Niestety oznacza to także pogłębienie różnic cywilizacyjnych pomiędzy posiadającymi a nieposiadającymi dostępu do sieci.

Reguły funkcjonowania Internetu muszą gwarantować prawa jednostek i instytucji, kierować się mechanizmami rynkowymi i stymulować rozwój technologiczny. Jeżeli te wymogi zostaną spełnione, to wszyscy mający dostęp do sieci mają szansę na znaczne przyspieszenie rozwoju cywilizacyjnego. Jeżeli nawet zabraknie mądrej koordynacji i regulacji działania, to i tak Internet będzie się rozwijał, tak, jak robił to do tej pory, choć może mniej optymalnie niż mógłby.

Sieć Internet w NASK

Ireneusz Neska

Sieć Internet od chwili powstania w NASK, tj. od połowy 1991 roku, cieszy się nieustającą popularnością w środowisku naukowym i akademickim, wzbudzając coraz szersze zainteresowanie w ośrodkach rządowych i firmach prywatnych. Liczba instytucji dołączonych do Internetu w ramach NASK w szybkim tempie rośnie. W niniejszym artykule chciałbym przedstawić przegląd podstawowych idei, którymi kierowali się ludzie tworzący Internet oraz nierozerwalnie związany z nim protokół TCP/IP, jak również aktualny stan rozwoju sieci Internet w NASK.

1. Filozofia Internetu - sieci z protokołem TCP/IP.

W początkowej fazie rozwoju sieci komputerowych, powstawały sieci firmowe, które nie były przygotowane do obsługi połączeń między sobą. Szybko okazało się jednak, że taka komunikacja między różnymi sieciami lokalnymi jest niezbędna. Technologią powstałą z myślą o ułatwieniu połączenia wielu oddzielnych fizycznych sieci jest opracowany na początku lat siedemdziesiątych 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. Najważniejszym z czynników, które wzmogły popularność tego protokołu było zaimplementowanie go w systemie operacyjnym UNIX.

TCP/IP jest obecnie jedynym w pełni zaimplementowanym 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 tak naprawdę standardem używanym niezwykle często zarówno w sieciach lokalnych jak i rozległych. Obecnie trudno jest znaleźć komputer, dla którego nie stworzono oprogramowania TCP/IP. Również wiele systemów sieci lokalnych, np. Novell NetWare, Banyan Vines, Microsoft Windows może pochwalić się możliwością integracji z siecią Internet.

Pod nazwą TCP/IP kryją się de facto dwa standardy protokołów używanych do komunikacji w sieciach. Opisują one sposoby 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 adres docelowy. IP zajmuje sie zaopatrzeniem datagramów w odpowiednie adresy, specyfikacją typu usługi sieciowej itp. Ma on za zadanie 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 składanie ich 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. Ukrywają one detale sprzętu sieciowego i umożliwiają komunikowanie się komputerów niezależnie od miejsca i rodzaju ich fizycznego połączenia.

2. Struktura Internetu.

W stukturze Internetu można rozróżnić trzy rodzaje sieci:

a) sieci lokalne (Local Area Networks - LAN)

Najczęściej wykorzystywane do komunikacji między komputerami w ramach jednej instytucji. Z reguły pokrywają małe obszary geograficzne (pojedyncze budynki lub kompleksy budynków, do kilkuset metrów). Wykonywane są na bazie topologii magistrali, pierścienia lub gwiazdy. Przykładami sieci lokalnych są: Ethernet, Token Ring, Arcnet.

b) sieci miejskie (Metropolitan Area Networks - MAN)

Sieci te obejmują tereny większych aglomeracji miejskich, tworząc podstawową strukturę połączeń instytucji na terenie danego miasta. Oparte są na bazie bardzo szybkich połączeń, z regóły światłowodowych. Najczęściej stosowane w sieciach miejskich standardy to: Ethernet, FDDI oraz obecnie coraz częściej ATM.

c) sieci rozległe (Wide Area Networks - WAN)

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.

Wiadomym jest jak komputery są połączone do sieci lokalnych, ale jak są włączone do Internetu? Dwie sieci są połączone ze sobą poprzez specjalne urządzenie dołączone do obu sieci, zwane routerem lub czasem gatewayem. Może to być dedykowane urządzenie przeznaczone tylko do tego celu lub komputer ogólnego przeznaczenia z odpowiednim oprogramowaniem. Routery zajmują się znajdowaniem drogi połączeń między różnymi sieciami oraz przesyłają pakiety danych między nimi. Przy przesyłaniu danych generalnie wymagane jest, aby router wybrał adres następnego routera na drodze do adresata lub (dla końcowej sieci) adres docelowego komputera w sieci lokalnej. Proces wybierania tej drogi nazywany jest "routingiem" i zależy od bazy danych wewnątrz routera. Baza danych routingu może być stała (statyczna), niezależna od aktualnego stanu sieci. Może być również zmieniana dynamicznie, odzwierciedlając aktualną topologię systemu Internetowego. 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.

3. Adresowanie w Internecie.

Twórcy Internetu 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 oraz numer komputera w sieci. W naszym przykładzie numerem sieci jest część 148.81, natomiast numerem komputera w sieci jest 16.50. Adresy sieci zostały podzielone na pięć klas, różniących się ilością komputerów możliwych do zainstalowania w pojedynczej sieci. W warunkach polskich jest możliwe uzyskanie adresów z tzw. klasy B (ponad 65 tysięcy komputerów) oraz klasy C (do 254 komputerów w sieci).

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 cześci <numer-sieci>, natomiast ostatni router na drodze pakietu musi na podstawie adresu IP podanego w części <numer-komputera> odnaleźć adres fizyczny hosta dołączonego do tej sieci i przesłać datagram do tego komputera. Ta prosta notacja została jednak rozszerzona o koncepcję "podsieci". Podsieci pozwalają na dwupoziomową 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" (np. 255.255.255.0). W połączonych sieciach lokalnych jednej organizacji może teraz występować jeden numer sieci, lecz różne numery podsieci, co ułatwia administratorowi obsługę sieci. Ze względu na gwałtowny wzrost liczby numerów sieci i skomplikowania routingu stało się to w architekturze Internetu konieczne. Pozwoliło to na prostsze odzwierciedlenie zawiłości struktury połączeń sieci lokalnych w sposobie routingu.

Jak ogólnie wiadomo, każde urządzenie w sieci ma swój unikalny adres, dlatego też przydzielanie adresów musi być koordynowane w skali światowej. 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 w ostatnich latach, taki sposób przyznawania adresów stał się nieefektywny. Z tego też powodu w kilku regionach świata powstały ośrodki, które są odpowiedzialne za przyznawanie adresów na danym terenie. Dla Europy jest to 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 roku przyznawanie adresów zostało całkowicie zdecentralizowane. W ramach poszczególnych państw operatorzy sieci (ang. service providers) mogą otrzymać bloki

adresów, które są następnie delegowane dla klientów dołączających się do sieci danego operatora. Są to tak zwani lokalni rejestratorzy IP (ang. Local IP Registers) i oni decydują o przydzielaniu adresów IP dla dołączających się do nich abonentów. W Polsce istnieje w tej chwili dwóch operatorów, którzy mają prawo przydziału numerów IP dla swoich abonentów. Są to: PL-net (oddział sieci Eunet w Polsce) oraz NASK. Oprócz lokalnych rejestratorów IP w każdym kraju istnieje jedna organizacja, która ma pulę adresów dla abonentów, którzy w danej chwili nie dołączają się do sieci Internet, a z pewnych względów potrzbują oficjalnie zarejestrowanych numerów IP. Jest to tzw. Registry of Last Resort. W Polsce taką funkcję pełni NASK. W obrębie sieci lokalnych nad przydziałem numerów internetowych konkretnym komputerom czuwa odpowiedzialny za daną sieć administrator.

W celu uzyskania numerów IP należy na adres NASK przesłać odpowiedni formularz rejestracyjny, który zawiera między innymi:

- dane administracyjne
  - nazwa instytucji
  - nazwisko osoby odpowiedzialnej za obsługę techniczną sieci lokalnej
  - nazwisko osoby odpowiedzialnej za administrację numerami IP w ramach sieci lokalnej
  - dla tych osób: numer telefonu, fax, e-mail

- informacje techniczne
  - liczba urządzeń w sieci lokalnej, które wymagają numerów IP
  - liczba podsieci
  - plany rozwoju sieci na najbliższy rok
  - dla większych sieci (ponad dwie klasy C) dokładny plan adresacji sieci.

W celu ułatwienia użytkownikom komunikacji między komputerami, poza numerem Internetowym dla oznaczania komputerów wprowadzono również nazwy symboliczne. Obsługą tych nazw zajmuje się tzw. DNS (Domain Name Service), pozwalający na konwersję adresu symbolicznego na liczbowy w sposób niewidoczny dla użytkownika. Nazwa składa sie z kilku (najczęściej od trzech 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 - nowo powstająca domena dla 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 zwykle ostatnim członem nazwy jest skrót „net"). Dalsze człony nazwy ku lewej określają szczegółowo miejsce komputera w sieci. Pierwszy człon z lewej zawsze określa nazwę komputera w sieci lokalnej.

Dla każdej domeny musi być jeden nadrzędny (tzw. primary) komputer obsługujący domenę oraz powinien być przynajmniej jeden podrzędny (tzw. secondary). 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.

Na poziomie krajowym NASK zapewnia obsługę domeny pl. Ze względu na zaszłości historyczne na drugim poziomie istnieją w tej chwili w Polsce dwa systemy nazewnictwa:

a) ze względu na typ organizacji:

edu.pl	instytucje akademickie
com.pl	firmy komercyjne
gov.pl	instytucje rządowe
mil.pl	instytucje wojskowe
org.pl	inne organizacje

Administracją domen: edu.pl, com.pl, mil.pl i org.pl zajmuje się NASK (serwer *bilbo.nask.org.pl*), natomiast domeny gov.pl - Instytut Podstawowych Problemów Techniki PAN (serwer *lksu.ippt.gov.pl*).

b) podział regionalny:

Na drugim poziomie stosuje się nazwy lub skróty nazw miasta, np. waw.pl dla Warszawy. W większości domeny regionalne obsługiwane są przez serwery NASK znajdujące się w węzłach regionalnych NASK. W niektórych przypadkach domeny te są obsługiwane przez abonentów NASK.

Duże firmy i organizacje o zasięgu ogólnopolskim mogą rejestrować się również bezpośrednio w domenie pl.

W celu rejestracji nowej nazwy na dowolnym poziomie należy poprawnie skonfigurować primary name server dla tej domeny oraz zgłosić tę nazwę administratorowi domeny bezpośrednio wyższego poziomu. Stworzenie nowej domeny regionalnej lub innej domeny bezpośrednio w pl wymaga zgłoszenia tego faktu do administratora domeny pl w NASK.

4. Usługi dostępne w sieci Internet.

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 zbiorów danych, Usenet News (listy dyskusyjne).

- poczta komputerowa (ang. *Electronic Mail, e-mail*)

Umożliwia szybkie i tanie przesyłanie korespondencji pomiędzy dwoma użytkownikami, przy zachowaniu listu w postaci zbioru. Wysłanie odbywa się przez wywołanie programu

obsługującego pocztę, podanie adresu odbiorcy (np. *irek@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 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, miedzy 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 dostepne archiwa (tzw. anonymous FTP). Jako identyfikatora użytkownika używa się wtedy zwykle słowa 'anonymous', a jako hasło do celow statystycznych podaje się własny identyfikator. W archiwach takich udostępniana jest ogromna ilość oprogramowania publicznie dostępnego (ang. public domain) na dowolne typy maszyn i systemy operacyjne.

- interakcyjna praca na odległych maszynach (ang. *Telnet, Rlogin*)

Programy te 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 niedostepnej w lokalnym systemie, uruchamiania tam programów, dostepu 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, z którym nawiązano połączenie. Szereg komercyjnych baz danych 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 za darmo swoje katalogi biblioteczne, w których można znaleźć informacje na temat literatury z całego świata.

Połączenie z odległym węzłem uzyskuje się poprzez wydanie komendy **telnet <nazwa-maszyny>**, a następnie podanie identyfikatora użytkownika oraz hasła. Przy dostępie do darmowych baz danych z reguły nie potrzeba podawać identyfikatora i hasła lub czasami identyfikatory są ogólnie znane.

- dostęp do zbiorów danych

W sieci Internet oprócz baz danych istnieje szereg innych serwisów, umożliwiających dostęp użytkownikowi do zbiorów danych na innych maszynach. Należą do nich: Gopher, World Wide Web, WAIS, Whois oraz Archie.

Gopher jest to rozproszony system informacyjny umożliwiający dostęp do różnego rodzaju dokumentów, zasobów i usług sieciowych. Pozwala on na przeszukiwanie i zbieranie informacji znajdujących się w różnch miejscach w bardzo przejrzysty i prosty do opanowania sposób. Przy jego pomocy można przeglądać zbiory z lokalnego lub odległego komputera, łączyć się z serwerami FTP, przeszukiwać bazy danych, czytać news'y, korzystać z baz adresowych X.500 i wiele innych.

World Wide Web (zwany inaczej WWW lub W3) jest to rozproszona baza informacyjna oparta o „hipertekst", oferująca użytkownikowi możliwość przeszukiwania dokumentów bez wiedzy, gdzie się one znajdują. Hipertekst tworzy się przez umieszczanie w tekście odwołań do innych dokumentów, serwerów lub usług sieciowych. Dokumenty WWW oprócz zwykłego tekstu mogą zawierać zbiory binarne, programy (skrypty) do wykonywania, obrazy, dźwięk itp. Mogą się one również odwoływać do innych usług sieciowych: baz danych, Gophera, WAISa, Newsów, X.500 i innych.

WAIS (Wide Area Information Service) jest to rozproszony system pomocny przy przeszukiwaniu baz danych. WAIS używa naturalnego języka pytań do poszukiwania odpowiednich dokumentów. Wynikiem każdego zapytania jest zestaw dokumentów zawierających podane przez użytkownika słowa kluczowe. Bardzo często jest to system używany do przeszukiwania dokumentów dostępnych poprzez serwery Gopher lub WWW.

Whois jest to usługa dostarczająca jakby elektroniczną książkę adresową dla użytkowników sieci. Umożliwia ona odszukiwanie adresów e-mailowych, pocztowych i numerów telefonicznych zarejestrowanych osób. Może również dostarczać informacje na temat organizacji związanych z sieciami komputerowymi, samych sieci, numerów Internetowych, nazw domenowych i hostów.

Archie jest usługą umożliwiającą przeszukiwanie specjalnych baz danych (zwanych bazami archie) w poszukiwaniu zbiorów dostępnych na serwerach FTP. Dodatkowo serwery te mogą oferować bazę danych opisu pakietów oprogramowania (Software Description Data Base), która zawiera nazwy oraz krótkie opisy pakietów oprogramowania, dokumentów i zbiorów danych przechowywanych w archiwach FTP.

- News

News jest to publiczne forum wymiany artykułów i informacji, które są przesyłane między wybranymi komputerami w sieci, tzw. serwerami news. Maszyny te komunikją się wzajemnie zapewniając wymianę artykułów. Do obsługi systemu news od strony użytkownika mogą służyć różnorakie programy, wszystkie one jednak posiadają możliwość czytania i wysyłania artykułów do najbliższego serwera (są to tzw. Newsreader'y). Aby nie powodować zbytniego chaosu artykuły grupowane są tematycznie. W tej chwili w systemie News jest ponad 3000 grup z najróżniejszych dziedzin: technik komputerowych, informatyki, biologii, socjologii, kultury, historii, polityki, rekreacji i innych.

- bezpośrednie rozmowy w sieci Internet

Do bezpośrednich rozmów w Internecie służą dwa programy: *talk* i *write*. Zapewniają one natychmiastową interakcyjną wymianę komunikatów między dwoma użytkownikami obecnymi na dowolnych komputerach. Stwarza to warunki do rozmów koleżeńskich oraz organizowania konferencji w miejscach od siebie odległych. Do rozmów w Internecie służy również program IRC (Internet Relay Chat). Jest to oprogramowanie funkcjnalnie przypominające CB-radio z tą tylko różnicą, że jego zasięg jest ogólnoświatowy, a możliwości nieporównywalnie większe. Tak jak w przypadku CB-radia w IRC występują kanały umożliwiające jednoczesne połączenie teoretycznie nieograniczonej ilości rozmówców, znajdujących się w dowolnych punktach świata. Funkcje stacji przekaźnikowych spełniają serwery IRC pośredniczące w połączeniu, a rolę nadajników i odbiorników - terminale rozmówców.

- dostęp do odmiennych struktur plikowych (NFS)

Network File System (NFS) jest to standard współpracy komputerów, posługujących się oddmiennymi systemami plików (np. różne wersje UNIX, DOS, VMS). Standard ten daje użytkownikowi możliwość łatwego dostępu przez sieć do zbiorów zapisanych przez różne systemy operacyjne.

- inne

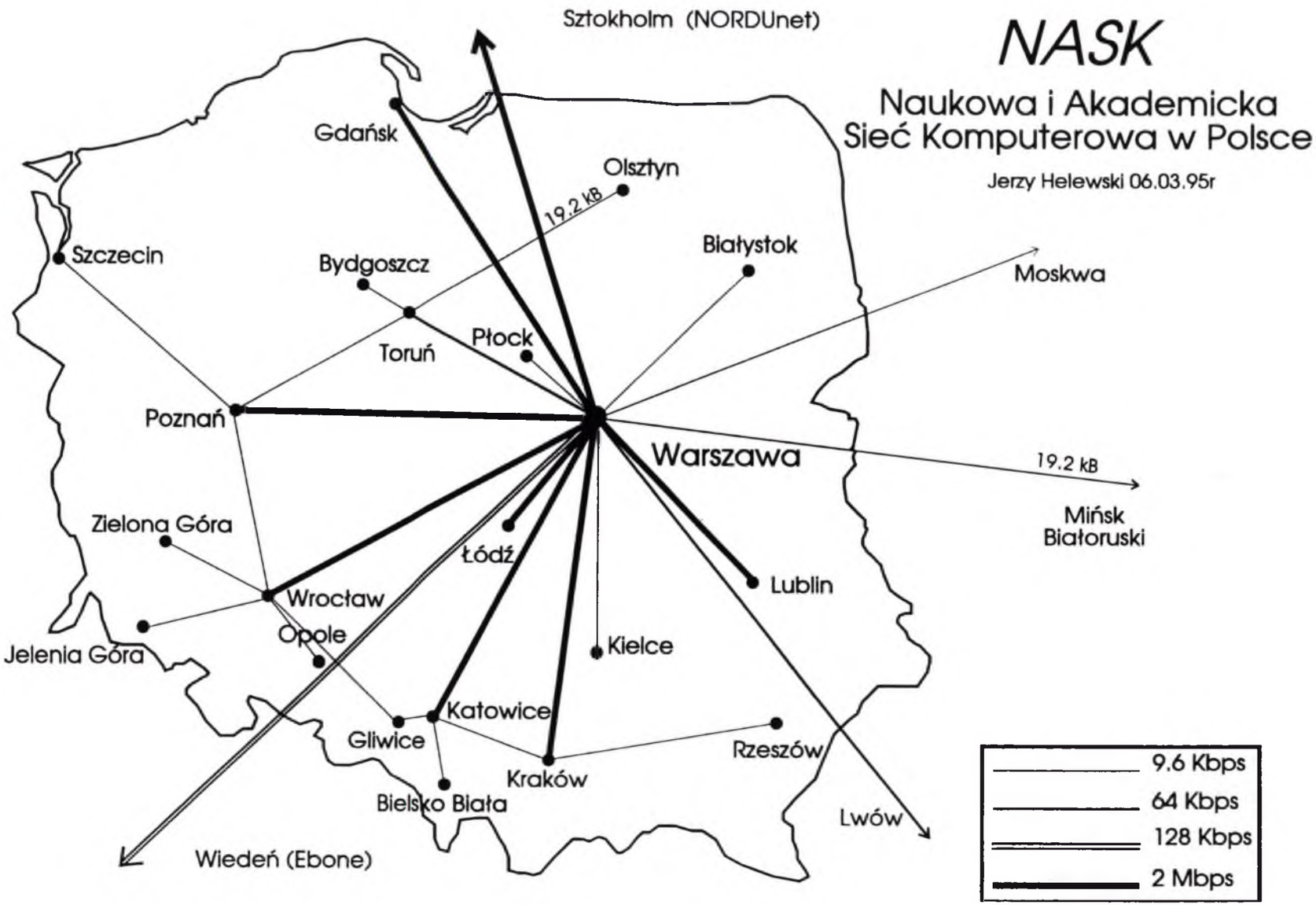
W Internecie istnieje poza tym wiele innych programów umożliwiających proste czynności, np. sprawdzanie aktywności komputera w sieci, znajdowanie drogi przepływu danych poprzez sieć, poszukiwanie komputera o podanej nazwie lub numerze, poszukiwanie użytkownika na odległej stacji prowadzenie obliczeń rozproszonych itp.

5. Internet w NASK.

Rozwój Internetu w Polsce rozpoczął się w połowie 1991 roku, kiedy to uzyskano zezwolenie na dołączenie do sieci światowej. Zalążki sieci zostały stworzone na kilku komputerach pracujących z systemem UNIX oraz komputerach PC z oprogramowaniem routerów typu public domain. Połączenia międzymiastowe oraz łącze międzynarodowe do Kopenhagi realizowane były na liniach analogowych ż prędkością 9.6 kb/s. Szybko jednak takie rozwiązanie okazało się niewystarczające, a zwiększenie prędkości linii międzynarodowej do 64 kb/s poprawiło sytuacje tylko na krótko.

W chwili obecnej na głównych liniach międzymiastowych stosowane są połączenia cyfrowe o przepustowości 2 Mb/s. Łączność ze światem jest zapewniona przez łącze satelitarne do Sztokholmu o przepustowości 2 Mb/s (z czego na komunikację Internetową przeznaczone jest pasmo 1792 kb/s) oraz łącze cyfrowe do Wiednia o przepustowości 128 Kb/s. W najbliższym czasie szybkość linii wiedeńskiej zostanie zwiększona do 256 kb/s. Również Ukraina (64 kb/s do Lwowa), Rosja (9.6 kb/s do Moskwy) i Białoruś (19.2 kb/s do Mińska) posiadają połączenia do Polski.

Schemat połączeń sieci Internet w NASK przedstawiony jest na rys. 1.


Sztokholm (NORDUnet)
NASK
Naukowa i Akademicka
Sieć Komputerowa w Polsce
Jerzy Helewski 06.03.95r
Gdańsk
Olsztyn
19.2 kB
Białystok
Moskwa
Szczecin
Bydgoszcz
Płock
Toruń
Poznań
Warszawa
19.2 kB
Mińsk
Białoruski
Zielona Góra
Łódź
Lublin
Wrocław
Opole
Kielce
Jelenia Góra
Katowice
Gliwice
Rzeszów
Kraków
Bielsko Biała
Lwów
Wiedeń (Ebone)
9.6 Kbps
64 Kbps
128 Kbps
2 Mbps

W obecnej chwili Internet w Polsce ma konfigurację gwiazdy z liniami obejściowymi. Wszystkie ośrodki w kraju są dołączone bezpośrednio do Warszawy. Stąd dopiero przesyłane są dane do żądanych miejsc w kraju i za granicą. Związane jest to z ogólną strukturą szkieletu połączeń sieci w naszym kraju. Odzwierciedleniem tego jest warstwowa struktura routerów. Poziom krajowy stanowi router CISCO 7000 zainstalowany w Centrum Radiokomunikacji i Telekomunikacji w Warszawie. Realizuje on połaczenia z większością regionów w kraju. Jest on połaczony linią 2 Mb/s z drugim takim samym routerem zainstalowanym w Centralnym Węźle NASK na Uniwersytecie Warszawskim, realizującym połączenia międzynarodowe. Konfiguracja regionalnych węzłów NASK z reguły składa się z routera CISCO (AGS+ lub 4000) zapewniającego połączenia synchroniczne z prędkościami do 4Mb/s, serwera komunikacyjnego (CISCO 516-CS) zapewniającego dostęp asynchroniczny pojedynczym osobom lub małym ośrodkom z prędkościami do 38.4 kb/s oraz maszyn typu SUN pracujących jako servery sieciowe. Lokalnie w poszczególnych regionach budowa sieci jest rozwiązywana indywidualnie przez zainteresowane instytucje w zależności od ich potrzeb i możliwości. W większych ośrodkach powstają sieci miejskie (MAN), które są wykorzystywane w Internecie i zapewniają bardzo szybkie i niezawodne przesyłanie danych między dołączonymi instytucjami. W Warszawie w trakcie realizacji jest sieć metropolitarna WARMAN oparta o protokół ATM (Asynchronous Transfer Mode).

Na liniach połączeniowych między routerami w sieci szkieletowej NASK stosowany jest przeważnie protokół HDLC i czasami PPP. Jako dostępowe dla abonentów oferowane są protokoły:

- dla linii asynchronicznych: SLIP, CSLIP, PPP,
- dla linii synchronicznych: HDLC, PPP, Frame Relay.

W najbliższym czsie w sieci szkieletowej NASK zostanie wprowadzony protokół Frame Relay. Technologia Frame Relay została przedstawiona w oddzielnym opracowaniu.

Cała sieć Internet w NASK zarządzana jest centralnie z jednego miejsca. Do zarządzania stosowane jest oprogramowanie Cisco Works oparte na bazie SUNnet Manager'a. Wszelkie zdarzenia w sieci (zmiany stanu linii połączeniowych, zmiany konfiguracji routerów) są rejestrowane. Zbiory konfiguracyjne routerów (ostatnie kilka wersji) gromadzone są w centralnej bazie. Na bieżąco prowadzone są statystyki natężenia ruchu na liniach międzynarodowych i międzymiastowych.

W jednej bazie danych zgromadzone są informacje o całej sieci szkieletowej, urządzeniach w niej pracujących, osobach odpowiedzialnych za sprzęt, wszystkich lokalizacjach, w których umieszczone są urządzenia NASK-u, dostawcach sprzętu, sieciach administrowanych przez NASK itp. Dla urządzeń w sieci podane są: rodzaj i wersja sprzętu, wersja oprogramowania, nazwa urządzenia w sieci, adresy wszystkich interfejsów, lokalizacja, w której urządzenie jest zainstalowane, nazwiska osób odpowiedzialnych za sprzęt. Dla osób podane są: dokładny adres kontaktowy tej osoby, telefony, fax, e-mail. Wszystkie te informacje dostępne są w prosty sposób po naciśnięciu klawisza myszy.

Ponadto Cisco Works zapewnia możliwość zdalnej konfiguracji routerów, monitorowania podstawowych parametrów urządzeń (np. zajętości pamięci, procesora, obciążenia linii, ilości błędów, statusu poszczególnych protokołów), ustawiania pułapek na pewne parametry routerów (po

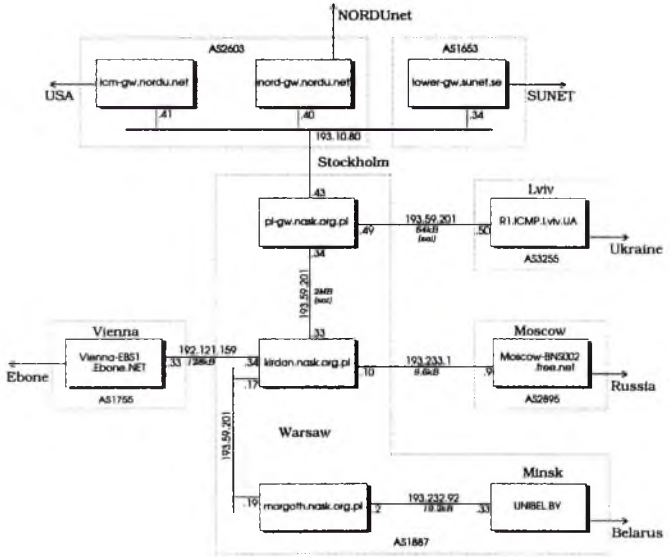
osiągnięciu przez monitorowany parametr założonej wartości wykonywana jest określona czynność), wysłanie pojedynczego lub cyklicznego zapytania protokołem SNMP o pewne parametry urządzeń itp.

6. Routing w NASK.

Routing w sieci NASK należy rozpatrywać w trzech aspektach: routing między siecią NASK a siecią Internet, routing w sieci szkieletowej NASK oraz routing na styku sieci NASK z abonentami.

a) Schemat połączeń międzynarodowych sieci NASK przedstawia rysunek 2.

Połączenia międzynarodowe z NASK



Routing między siecią NASK a rozległym Internetem realizowany jest w protokole BGP (Border Gateway Protocol). Do realizacji tego protokołu NASK ma przydzielony numer Systemu Autonomicznego (ang. Autonomus System) AS 1887. Styk z innymi operatorami realizowany jest na dwoch routerach: *pl-gw.nask.org.pl* (CISCO 4000) znajdujący się w Sztokholmie oraz *kirdan.nask.org.pl* (CISCO 7000) stojący w Centralnym Węźle NASK na Uniwersytecie Warszawskim. Między nimi uruchomiony jest dynamiczny protokół routingu Internal BGP wersja 4. Router *pl-gw* wymienia informacje o routingu z routerami: *r1.icmp.lviv.ua* (Ukraina, linia satelitarna 64 kb/s, AS3255, protokół External BGP wersja 3), *nord-gw.nordu.net* (sieć

NORDUnet, AS2603, protokół External BGP wersja 4) oraz w ograniczonym zakresie z *lower-gw.sunet.se* (sieć SUNET, AS1653, protokół External BGP wersja 4, tylko sieci należące do SUNET-u). Router *kirdan* wymienia informacje z routerami: *vienna-ebs.ebone.net* (węzeł sieci EBONE w Wiedniu, linia 128 kb/s, AS1755, protokół External BGP wersja 4) oraz *moscow-bns002.free.net* (węzeł sieci FreeNet w Moskwie, linia 9.6 kb/s, AS2895, protokół External BGP wersja 3). Dodatkowo przez NASK routowane są pakiety do Mińska Białoruskiego. W tej chwili wszystkie sieci białoruskie traktowane są jako należące do Systemu Autonomicznego NASK (AS1887) i tak też są widoczne na świecie.

NASK przesyła ruch do i ze świata dla sieci FreeNet w Rosji, oraz do wszystkich sieci na Ukrainie i Białorusi, natomiast nie jest drogą tranzytową dla ruchu między sieciami NORDUnet i EBONE.

b) Routing w sieci szkieletowej NASK realizowany jest w protokole IGRP (Interior Gateway Routing Protocol) z pewnymi wyjątkami. W niektórych miejscach (głównie na wolnych liniach połączeniowych, np. Warszawa-Płock, Kraków-Rzeszów) stosowany jest statyczny protokół routingu. Każdy router w sieci szkieletowej NASK ma pełną bazę routingu do sieci wszystkich abonentów NASK-u. W przypadku zerwania głównych połączeń międzyregionalnych protokół IGRP automatycznie w ciagu kilku minut rekonfiguruje routing na linie obejściowe. Obecnie w trakcie realizacji jest przejście w sieci szkieletowej na protokół OSPF (Open Shortest Path First).

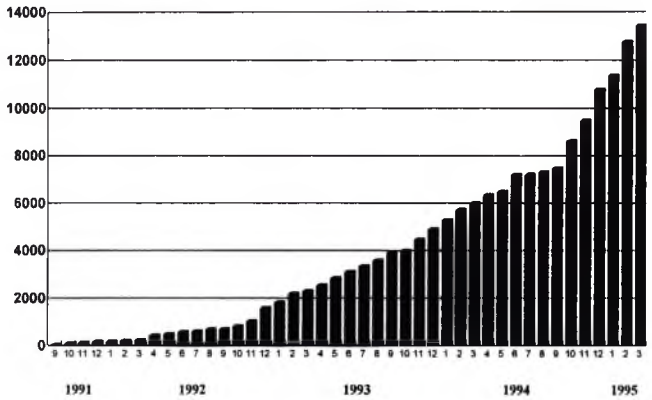
c) Routing na styku do abonentów sieci NASK w zasadzie realizowany jest w tej chwili statycznie. Na routerach NASK graniczących z siecią abonencką wpisywany jest statycznie routing do wszystkich sieci należących do danego abonenta. Następnie wszystkie te numery sieci redystrybuowane są dynamicznie do całej sieci szkieletowej NASK. W niektórych przypadkach na styku sieci abonenckiej z NASK-iem stosowany jest dynamiczny protokół routingu (np. w Warszawie i Poznaniu stosowany jest protokół OSPF, we Wrocławiu - protokoły RIP i OSPF).

W sieci szkieletowej NASK routowane są tylko numery sieci zarejestrowane w bazie danych RIPE. Również tylko te sieci są ogłaszane przez NASK protokołem BGP do Internetu i routowane w Eutopie. Routing w USA jest realizowany tylko dla tych sieci, które zarejestrowane są w bazie danych MERIT. NASK pośredniczy w rejestracji wszystkich istniejących i nowo przyznawanych klas adresowych w bazach danych RIPE i MERIT.

7. Podsumowanie.

Internet w NASK w ciągu niecałych czterech lat dokonał znaczącego postępu. Liczba i wielkość sieci dołączonych do Internetu stale rośnie. W kwietniu 1995 roku przekroczyliśmy liczbę 14 tysięcy zarejestrowanych komputerów pracujących w Internecie pod różnymi systemami. Na rys. 3. przedstawiona jest historia rozwoju sieci Internet w Polsce.

Rys. 3. Liczba komputerów w sieci Internet w Polsce



W skali kraju na transmisję protokołu TCP/IP przypada w tej chwili ponad 95% ogólnego ruchu po łączach komputerowych, stanowiąc podstawowy rodzaj łączności. Na liniach międzynarodowych podczas roboczego dnia przesyłane jest już około 10 GB danych (10 miliardów znaków) na dobę.

Coraz większym zainteresowaniem cieszy się Internet w kręgach pozanaukowych. Między innymi wiele instytucji państwowych i rządowych zaczyna wykorzystywać tę sieć do łączenia swoich zasobów. Powstają również zaczątki komercyjnej sieci Internet, która umożliwiłaby korzystanie z sieci firmom prywatnym.

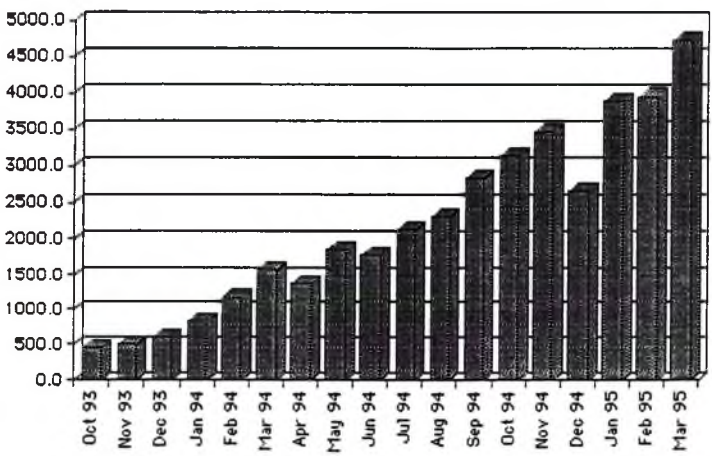
NASK w sieciach komputerowych Europy i świata

Maciej Kozłowski

Niniejsza notatka stanowi aktualizację opracowania zaprezentowanego pod tym samym tytułem podczas IV seminarium NASK w Miedzeszynie, we wrześniu 1994 r. Zostały w nim przedstawione główne sieci szkieletowe w Europie i na świecie oraz zostały wspomniane najważniejsze organizacje mające na celu koordynację współdziałania sieci komputerowych i ich promocję. Wydaje się, że w ciągu niecałego roku, który minął od tego czasu zaszły zdarzenia, które usprawiedliwiają powtórzenie tego tematu.

W Europie w ciągu ostatniego roku następował systematyczny rozwój sieci połączeń komputerowych i wzrost natężenia ruchu sieciowego. Dla ilustracji przytaczamy statystykę ruchu w jednej ze szkieletowych sieci europejskich - EuropaNET (rys.1), wskazującą na potrojenie wielkości ruchu w skali roku. Wydaje się, że w Europie nie nastąpiły w tym okresie zmiany organizacyjne, w sposób szczególny przyspieszające rozwój sieci. Wytworzyła się jednak atmosfera oczekiwania, że przyspieszenie nastąpi. Znalazło to wyraz w postanowieniach spotkania grupy G7 (przywódców siedmiu najbardziej rozwiniętych gospodarczo krajów świata) w lutym 1995 r. Spotkanie to było poświęcone rozwojowi społeczeństwa informatycznego; tezy tego spotkania są cytowane w artykule Krzysztofa Hellera, nie będziemy ich więc przytaczać i dokładniej omawiać.

Niewątpliwie, zasadnicza zmiana nastąpiła w USA w postaci likwidacji sieci szkieletowej NSFnet, a więc zaprzestania bezpośredniego utrzymywania centralnej struktury sieciowej przez organizację finansującą badania naukowe i rozwój technologii.



Rys. 1. Statystyka transmisji w sieci szkieletowej EUROPAnet, od grudnia 1993 r. do marca 1995 r. W ciągu ostatniego roku odnotowano trzykrotny wzrost natężenia ruchu sieciowego.

NSFNet, NREN

NSFnet utworzony w 1986 r. jako "network for research, education and technology transfer" pełnił rolę głównej struktury szkieletowej sieci komputerowych w USA; przede wszystkim w zakresie internetu. Dopóki internet miał prawie wyłącznie użytkowników akademickich, było to rozwiązanie poprawne. Wraz ze wzrostem ilości pozaakademickich użytkowników internetu pojawiły się napięcia; NSFnet nie czuł się powołany do komercji (pomimo że był administrowany przez prywatną kompannię MERIT), zaś nie

wytworzyły się struktury równoległe, które mogły ich obsługiwać (ściślej - powstawały, np. AlterNet, ale nie rozwinęły się na miarę NSFnetu). Sytuacja stała się paradoksalna; NSFnet, który miał misję stymulacji rozwoju sieci, zaczął ten rozwój hamować. Uznano więc, że swoją misję już spełnił. 30 kwietnia 1995 r. formalnie przestał istnieć.

Został zastąpiony przez dość złożoną strukturę NREN - National Research and Education Network. NREN opiera się o firmy prywatne, wyłonione w drodze przetargów i konkursów. Operacja konwersji została starannie przygotowana i przeprowadzona w okresie wrzesień 1994 - 30 kwietnia 1995. Z punktu widzenia europejskiego użytkownika sieci komputerowych wydaje się, że przebiegła dość sprawnie; jedynie w lutym i marcu wystąpiły problemy z routingiem z Ameryki do Europy, nie zawsze respektującym złożoną geografię połączeń europejskich.

Dostęp do NREN następuje poprzez Network Access Points - NAP. Główne NAP są ulokowane w stanie Nowy Jork, w Waszyngtonie, Chicago, San Francisco i Los Angeles. Obsługują je odpowiednio: Sprint, MFS-MAEA East, Ameritech, Pacific Bell i CERFnet. Dostarczycielami połączeń wiodących do do Network Access Points są "primary service providers": Sprintlink, MCInet i ANSnet (Advances Networks and Services) i w mniejszym stopniu Alternet. Z nimi zawierają umowy lokalni dostarczyciele usług oraz działające lokalnie sieci akademickie, np. BARRnet, CA*net, CERFnet, CICnet, CSUnet, Michnet, PREPnet, Morenet, NevadaNet, NYSERnet, SURAnet, THEnet etc.

Dobrym kryterium efektywności dokonujących się zmian są ceny. Przytoczymy przykłady cen w zakresie dostępu do Network Access Points:

Pacific Bell (San Francisco); ceny miesięczne

			przy kontrakcie 3-letnim	
	miesięcznie	instalacja	miesięcznie	instalacja
1.5 Mbps FR	500 $	375 $	475 $	375 $
45 Mbps ATM	4850 $	5000 $	3541 $	1500 $
155 Mbps ATM	7900 $	8500 $	7900 $	1500 $

MFS (Waszyngton) - ceny miesięczne

	kontrakt roczny	kontrakt 3-letni	kontrakt 5-letni
Ethernet 1.5 Mbps	1680 $	1520 $	1400 $
Ethernet 10 Mbps	2280 $	2050 $	1900 $
FDDI 45 Mbps	4080 $	3650 $	3400 $
FDDI 100 Mbps	8400 $	7560 $	7000 $

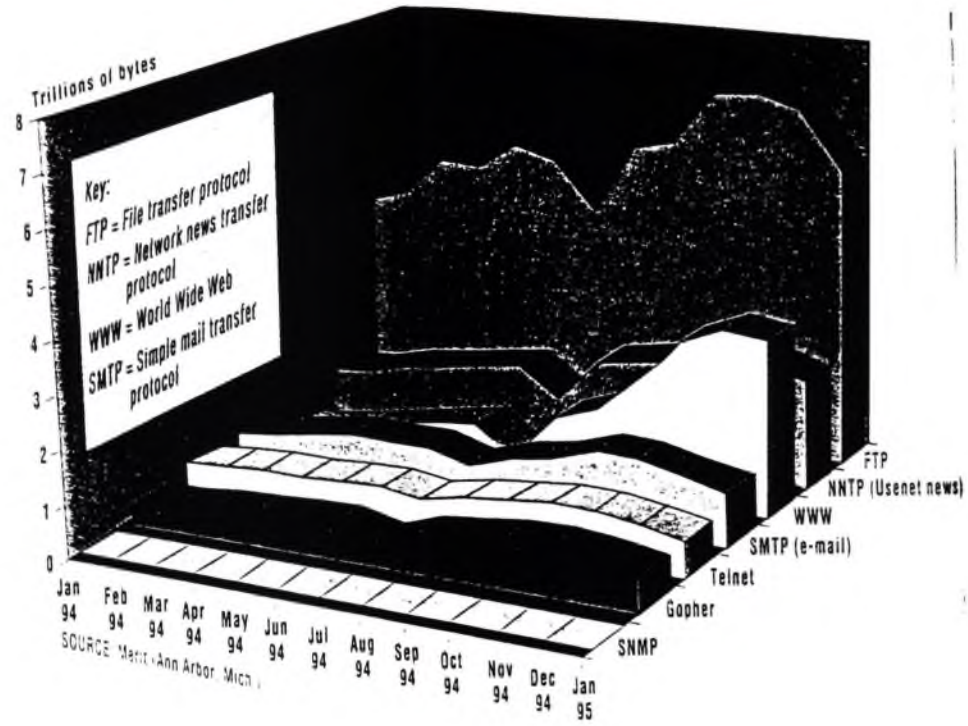
Ameritech (Chicago) - ceny miesięczne

	kontrakt roczny	kontrakt 3-letni	kontrakt 5-letni
DS3 45 Mbps ATM	5900 $	4750 $	4000 $
OC3 155 Mbps ATM	cena umowna	cena umowna	cena umowna
instalacja:	2000 $	2000 $	2000 $

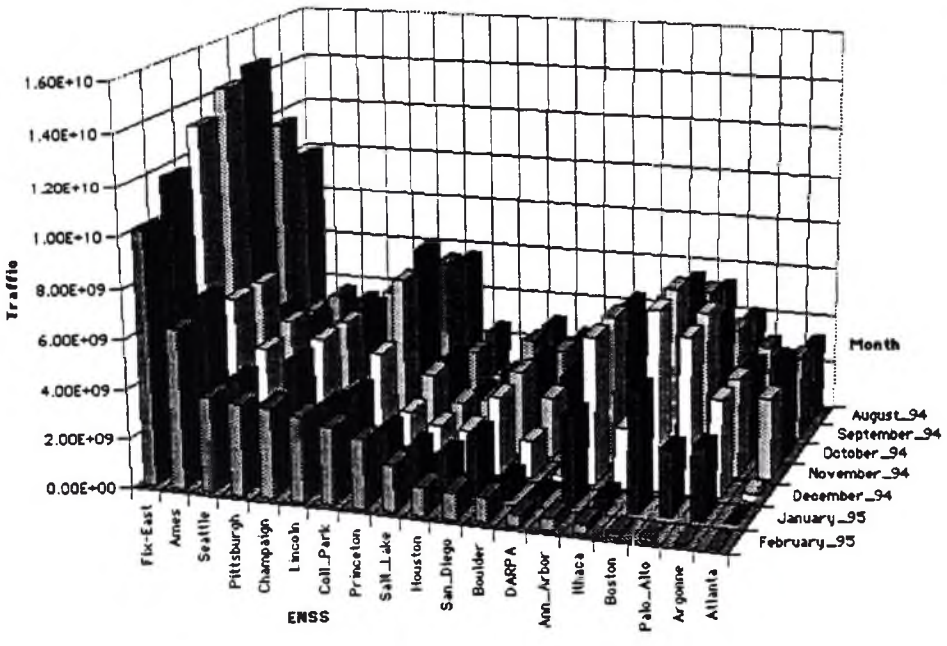
Dla przykładu, wymienimy niektóre połączenia w Chicago do NAP, obsługiwanego przez Ameritech (Jako switch ATM zastosowano Globeview 2000 firmy AT&T z interfejsami DS-3 (45 Mbps) HSSI, DS-3 ATM, OC3c 155 Mbps SONET/ATM).

Alpha Net (połączenie do Milawaukee)	DS3 45 Mbps ATM
Argonne National Laboratory	DS3 45 Mbps ATM (plan: OC3c ATM)
Fermi National Laboratory	DS3 45 Mbps ATM, FDDI 100 Mbps
MCI Internet	DS3 45 Mbps ATM, FDDI 100 Mbps
NETCOM On-line	DS3 ATM
Sprint	DS3 ATM
University of Chicago	DS3 ATM (plan: OC3c 155 Mbps ATM)

Przedstawimy także dwa diagramy ilustujące zmniejszanie się ruchu w szkielecie sieci NSFnet w okresie czerwiec 1994 - luty 1995.



Rys. 2. Statystyka ruchu w szkielecie sieci NSFnet w okresie styczeń 1994 r. - styczeń 1995 r. Dominującą aplikacją jest FTP. Od połowy 1994 r. Następuje gwałtowny wzrost transmisji WWW. Minimum w połowie 1994 r. jest spowodowane okresem wakacyjnym. Końcowe minimum jest związane ze stopniowym wyłączaniem sieci.



Rys. 3. Statystyki ruchu na różnych liniach dostępowych do szkieletu sieci NSFnet przeprowadzone w okresie lipiec 1994 - luty 1995. Rysunek obrazuje proces stopniowego wyłączania sieci NSFnet.

EuropaNET

Jest to - obok EBONE - główna sieć szkieletowa w Europie. Wywodzi się z programu COSINE *(Cooperation for Open Systems Networking in Europe)*. Została powołana z myślą o obsłudze środowiska naukowego i akademickiego. Początkowo nie obsługiwała ruchu pozaakademickiego; obecnie zdecydowała się na jego transmisję. Właścicielem EUROPANet jest DANTE - spółka narodowych sieci akademickich kilku krajów, zarejestrowana w Cambridge (UK). Operatorem jest Unisource Business Network (Haga, Holandia). Wymienimy wszystkie sieci dołączone bezpośrednio do EuropaNET'u (stan z marca 1995 r.)

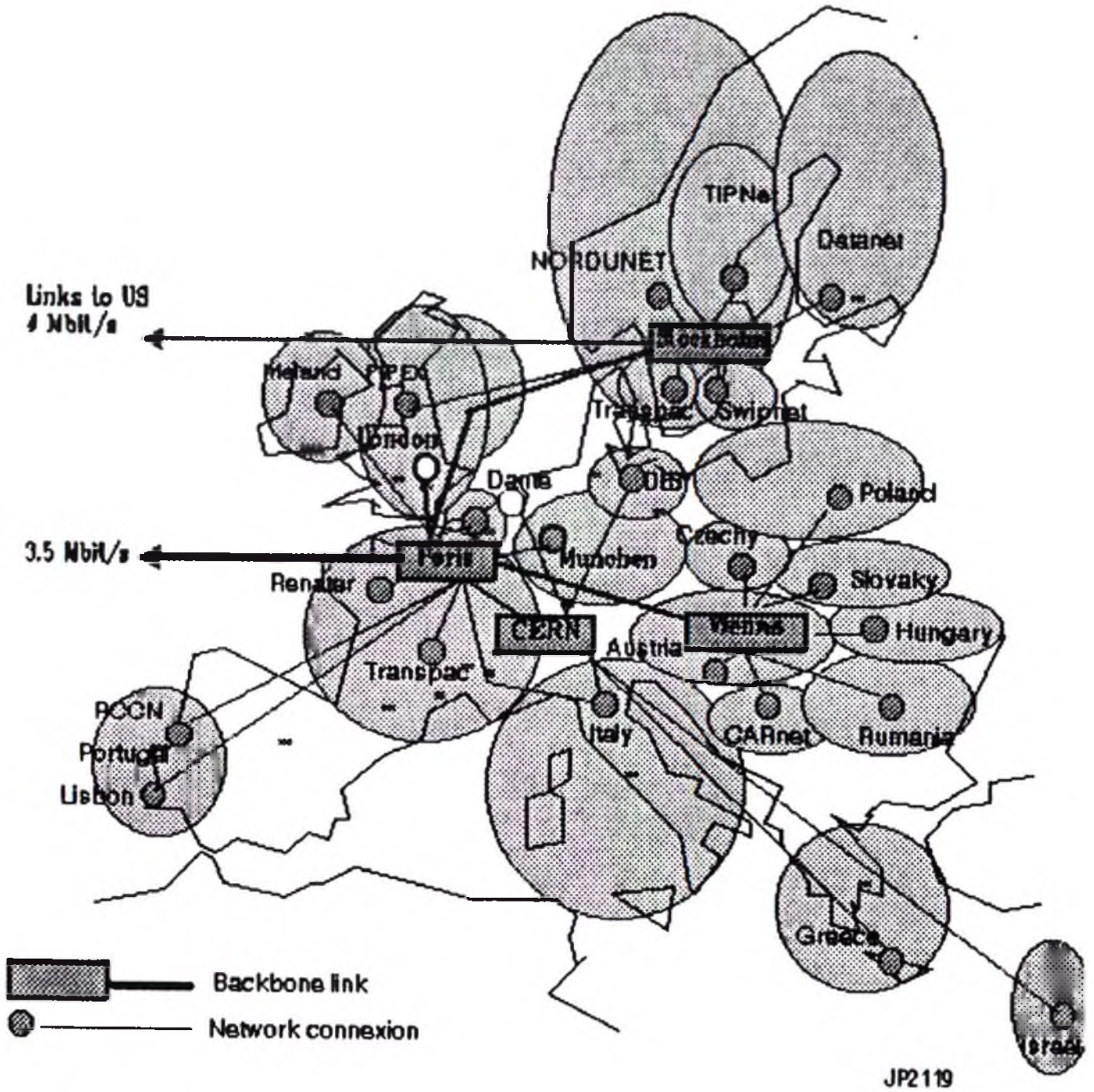
		łącze (Kbps)	protokoły
Belgia	BELNET-IP	1984	IP
	CEC	64	X.25
	JRC-GEEL	64	X.25
Czechy	CESNET	512	IP
Niemcy	WIN	2048	X.25, IP, CLNS
Grecja	ARIADNET	64	X.25, IP, CLNS
	NTUA	64	IP
Węgry	HUNGARNET	128	IP
	BMENET	64	IP
Irlandia	HEANET	64	X.25, IP
Włochy	GARR-IP	2048	IP
	GARR	64	X.25
	JRC/ISPRA	64	X.25
Luksemburg	RESTENA	128	X.25, IP
Holandia	SURFNET-IP	1984	IP
	SURFNET	64	X.25, CLNS
	AMS-GWY	1984	IP
	DN1	64	X.25
	ESAPAC	64	X.25
Portugalia	RCCN-IP	64	IP
	RCCN	64	X.25,IP,CLNS
Rumunia	ICI	9.6	X.25, IP
	PUB	9.6	X.25, IP
Słowenia	ARNES	512	X.25, IP
Hiszpania	RedIRIS	2048	X.25, IP, CLNS
Skandynawia	NORDUNET	1984	IP
	NORUNET	64	X.25, CLNS
Szwajcaria	SWITCH-IP	1024	X.25
	SWITCH	128	X.25, IP, CLNS
	CERN	1024	IP
Wielka Bryt	JANET-IP	2048	IP
	JANET	64	X.25

EuropaNET dysponuje dwoma łączami transatlantyckimi o łącznej przepustowości 5 Mbps oraz łączamio do EBONE (Genewa, 1.5 Mbps) i do Korei (64 Kbps).

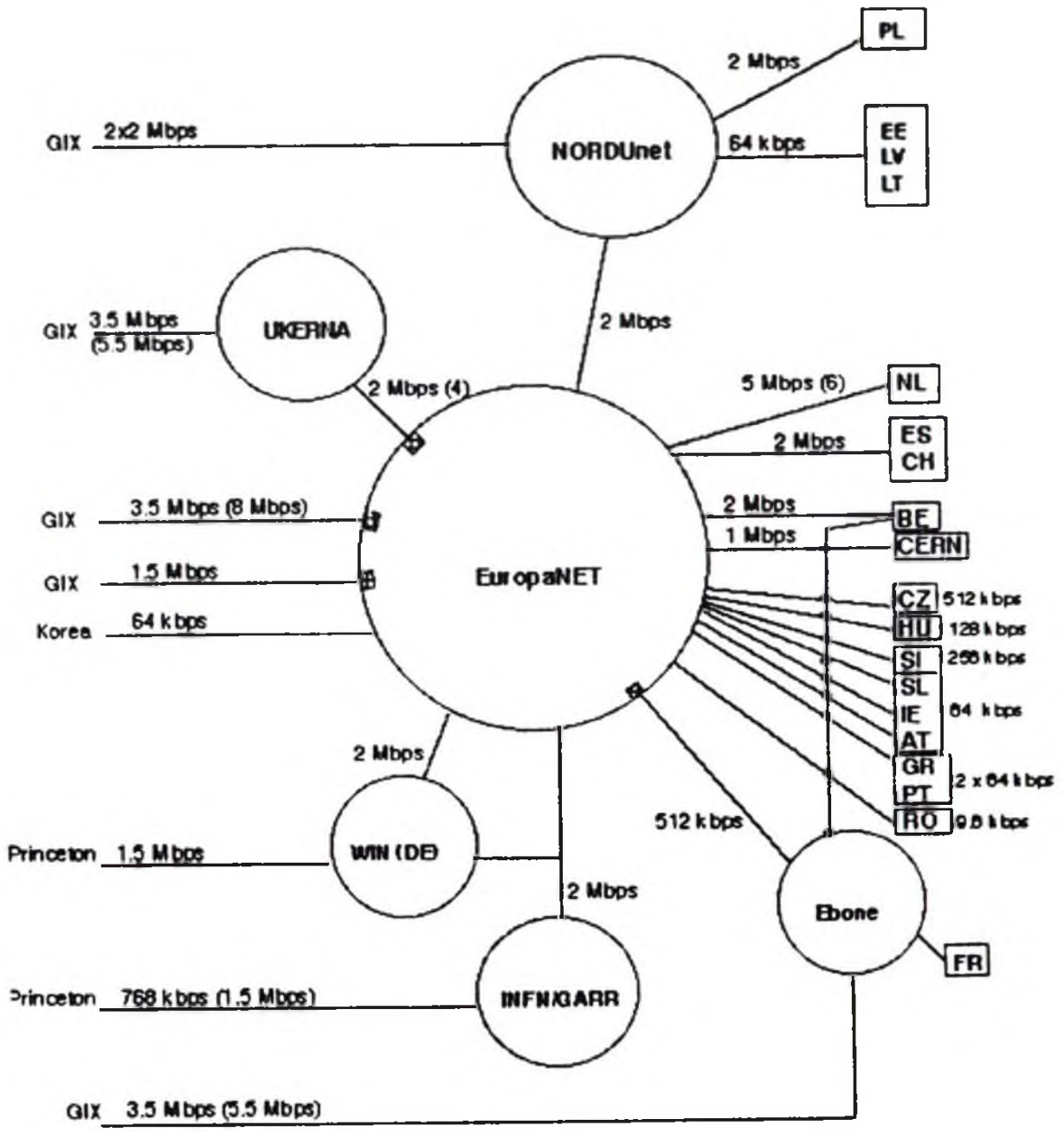
EBONE

Jest to jedna z głównych szkieletowych struktur sieciowych w Europie, zarejestrowana w Paryżu jako konsorcjum organizacji członkowskich. Na początku 1995 r. szkielet tej sieci tworzyły łącza Paryż-Monachium (2 Mbps), Paryż-Genewa (2 Mbps), Paryż-Wiedeń (1.5 Mbps), Paryż-USA (3.5 Mbps) i Monachium-USA (2 Mbps) oraz połączenia do EBONE i NORDUNETu. Członkami lub klientami EBONE są:

ACONET - Austria
BELNET - Belgia
CARNET - Chorwacja
Sieć akademicka Cypru
CESNET - Czechy
FRCU - Egipt
CERN
DATANET - Finlandia
RENATER - Francja
Internet Way - Francja
OLEANE - Francja
TRANSPAC - Francja
ECRC - Niemcy
FORTH - Grecja
HUNGARNET - Węgry
HEANET - Irlandia
ILAN - Izrael
CINECA - Włochy
GARR - Włochy
NASK - Polska
RCCN - Portugalia
Sieć akademicka Rumunii
TRANSPAC - Skandynawia
SANET - Słowacja
SWIPNET - Szwecja
TIPNET - Szwecja
JANET - Wielka Brytania
British Telecom (sieć IP)



Rys. 4 Schemat połączeń w sieci szkieletowej **EBONE**



Rys. 5 Schemat połączeń w sieci szkieletowej **EUROPAnet**

Na początku 1994 r. sieć EBONE przeszła kryzys organizacyjny, po tym jak kilka dużych sieci krajowych zdecydowało się na partnerstwo w oparciu raczej o sieć szkieletową EuropaNET, niż EBONE. Trzeba jednak powiedzieć, że EBONE rozwija się bardzo dobrze; w ciągu drugiego półrocza 1994 r. przepustowość głównych łącz wzrosła średnio o 75% i rośnie w tym tempie nadal.

Europejska instalacja pilotowa ATM

W listopadzie 1994 r. został uruchomiony pierwszy fragment (Bruksela, Dublin) europejskiej sieci pilotowej ATM. Jest to wspólne przedsięwzięcie 16 krajowych operatorów telekomunikacyjnych: PTT-Austria, BELGACOM, Tele-Dania, ATC-Finlandia, Telecom-Finlandia, France Telecom, TELEFONICA-Hiszpania, PTT Telecom-Holandia, Eireann-Irlandia, DBP-Niemcy, Telecom-Norwegia, Telecom-Portugalia, PTT Telecom-Szwajcaria, Telia AB-Szwecja, Britich Telecom, Telecom-Włochy. Projekt zakłada uruchomienie w każdym kraju co najmniej jednego węzła ATM, przy wykorzystaniu połączeń PDH 34 Mbps, a w perspektywie SDH 155 Mbps. Celem projektu jest test technologii ATM w zakresie sieci rozległych i usług, które w oparciu o nią mogą być oferowane. Środowisko naukowe i akademickie zostało zaproszone do korzystania z instalacji w ramach programu DG XIII ACTS - Advanced Communications Technologies & Services. Planuje się utrzymanie instalacji pilotowej ATM co najmniej do końca 1995 r.

Należy odnotować, że nie jest to jedyna w Europie sieć pilotowa ATM przekraczająca granicę krajów. Jako przykład innych inicjatyw tego typu należy wymienić projekt ATLAS, angażujący DBP, France Telecom i Sprint (USA).

Sieć EARN - Bitnet

Sieć Bitnet (w Europie EARN) to najstarsza obecnie akademicka sieć komputerowa. Ma ona hierarchiczną strukturę; dane są przesyłane na zasadzie "store and forward" pod nadzorem protokołu NJE - Network Job Entry. Połączenia Bitnetu na ogół przeszły ewolucję wykorzystując IP jako medium transmisyjne, a więc odbywa się ona najczęściej na "normalnych" łaczach Internetu. Większość węzłów Bitnetu jest także (a nawet przede wszystkim) węzłami Internetu. Zmiany te spowodowały, że sieć Bitnet zanika wolniej, niż można się było tego spodziewać - ciągle działa ponad 2000 węzłów tej sieci. W niektórych krajach (Hiszpania, Anglia, Norwegia) sieć bitnet/EARN zanikła zupełnie; niektóre zapowiedziały likwidację węzłów krajowych. Nie został dotychczas opracowany plan likwidacji tej sieci, ale należy wątpić, aby przetrwała ona poza koniec 1995 r.

EARN, RARE

W październiku 1994 r. nastąpiła fuzja EARN (European Academic and Research Network) i RARE (Resaux Asocies pour la Recherche Europeenne) - organizacji mających na celu promocję sieci komputerowych dla potrzeb środowiska naukowego i akademickiego w Europie. Nowa organizacja przyjęła nazwę TERENA - Trans-European Research and Education Networking Association. Stawia sobie ona na celu wspieranie działań i udział w rozwoju międzynarodowej struktury telekomunikacyjnej dla potrzeb środowiska naukowego i akademickiego oraz popieranie rozwoju technologii służącej międzynarodowej wymianie informacji. Cele te zamierza realizować przez:

- działania zmierzające do eliminacji barier technicznych, takie jak koordynacja prac standaryzacyjnych, procedur operacyjnych i promowanie swobodnej wymiany informacji technicznej,
- edukację, dokumentację i utrzymywanie serwisów informacyjnych dla użytkowników sieci,
- koordynację w zakresie ruchu sieciowego w skali międzynarodowej,
- organizację konferencji i spotkań warsztatowych mających na celu promocję sieci komputerowych, wymianę i udostępnianie informacji,
- podejmowanie dyskusji z ciałami rządowymi, organizacjami standaryzacyjnymi, operatorami telekomunikacyjnymi i przemysłem,
- udział w projektach serwisów pan-Europejskich, stosownie do woli organizacji członkowskich.

Członkami TERENy są organizacje reprezentujące akademickie i naukowe społeczności sieciowe - po jednej z każdego kraju. Aktualnie reprezentowane są prawie wszystkie kraje Europy (oprócz Jugosławii i Bośni), a także kraje Bliskiego Wschodu i północnej Afryki.

Kraje Europy Zachodniej i Skandynawia

Zamiast omawiania ciekawszych instalacji lub inicjatyw sieciowych w poszczególnych krajach przytoczymy zbiorcze zestawienie z opracowania *Connecting the User to the European Infostructure* przygotowanego dla celów programu ACTS *(Advanced Communications Technologies & Services)*. Program ACTS zakłada on, że kraje w nim uczestniczące będą działać poprzez wytypowane organizacje - w użytej tu terminologii *National Hosts*. Uważny czytelnik znajdzie w nim wiele ciekawych danych świadczących o tym, że Europa niekoniecznie jest opóźniona sieciowo stosunku do USA tak bardzo, jak wskazywałby na to stan sieci szkieletowych lub taryfy telekomunikacyjne.

Country	Characteristics	Services offered	User Population
Austria	Public: SDH, PDH, MAN, B-ISDN (ATM), ISDN, Frame Relay local networks: LAN, local ATM; Connects eight Austrian Cities	Service support environment based on ODP, IN, TMN, TINA-C DPE	Users in: Social and environmental areas, Electronic Publishing, Banking, Culture, Research/Education, etc.
Belgium	Host based on ATM Telecom Network	LAN Interconnect, Frame relay, ATM Connections, DQDB MAN Access	Experimental business and professional users linked to the ATM pilot
	Host based on CATV Networks	Testbed for video-telephony; Video on demand	3.85 million households
	Host based on TITAN Project	Audio-visual services, Public digital MM applications	10000 Users of digital MM terminals in southern Belgium
Denmark	TELE DENMARK DATACOM Host: LANlink interconnection by Frame Relay; connecting ten Danish Cities, ATM Services	Switched or point-to-point up to 34Mb/s	
Finland	Mobile National Host - UMTS	GSM and ATM Services Access, Experimental UMTS service	Campus of several Universities and research institutes
France	Public ATM and ISDN; Cable TV; DAB networks; RDS; Telecom 1-2 satellites; Digital Visiopass; Machine translation server; ATM pilot network between 3 cities; ATM commercial network; Private research network - RENATER	Video on demand; Audio on Demand; News on demand; Broadband interactive retrieval services; Interactive TV and radio; Teleshopping; Teleworking; Videoconferencing; Speech synthesis/recognition	Domestic users of Cable TV; News publishers; A/V program societies; Information providers; Manufacturers; Voice processing for ACTS projects; Education, research user groups; Health; SMEs
Germany	Deutsche Bundespost Telekom. German ATM network, connecting eight cities including Metropolitan Networks and Local Networks; German DATEX-M connecting twelve cities; ISDN, B-ISDN, Ethernet, Token Ring, FDDI, DQDB, ATM, etc.	Teleservices: Multi-media Archiving; Multimedia Mail; Multi-media Collaboration; Transport Services: PC-Protocol, TCP/IP, ISO-TP, XTP/ST2; Telemedicine; Telepublishing; Teleworking	Experimental users organised by German National Host Users Board

Greece	HESTIA: 13 Sites connected by 2Mb/s/s switched on demand; Each site is a broadband island; N-ISDN; ATM LAN; FDDI LAN; Satcom Links; Multimedia Server	Many services in the different HESTIA nodes; Multimedia mail; Multimedia authoring; Voice conferencing; Remote delivery of expertise; Distributed documenting; Telepublishing; Computer aided design; Teletraining	Greek shipping construction companies; Publishing companies; Hellenic Aerospace Industry; Greek Industry; Remote and isolated communities; Academic and Research Communities; Local SMEs; Hospitals (8 major hospitals in the Thessaloniki area); Emphasis on shipping, Tourism and Culture
Iceland	FO Network to all cities: 565 Mb/s PDH, 155 Mb/s SDH; FTTC Pilot; SDMS: 2Mb/s; CANTAT-3; Digital Exchanges, IN, Euro-ISDN; INTELSAT; EUTELSAT; INMARSAT; VSAT.	Interactive Multimedia; Tourism Information Network; MM Mail; Video telephony	Ministry of Health and Hospitals; Universities; Ministry of Tourism and Hotels; Publishers; SMEs; PSN; Public Administration
Ireland	Broadband Services	SMDS	Commercial Users
	NW Host	CATV - 2 way video services; MMDS digital TV/HDTV; ATM demonstrator;	Commercial and domestic users; end-users; SMEs
Italy	Torino ATM Laboratory Testbed	BB Video-telephony; Audio Conferencing; Digital HDTV; Virtual Path + VC Connections; Connection Less Server; Multicast; ATM-Virtual Private Network	
	Napoli, ATM Digital Cross Connect	Virtual Path	Universities, Research Institutes
	Aosta Valley, Digital Broadcasting Testbed		RAI Research Center
	Toscana; MAN Field trial	SMDS	Hospitals; Museums; Universities; Research Centres
Netherlands	National ATM Pilot; Specialised Broadband testing facilities	B-ISDN (Q.2931); TCP/IP over ATM; Desktop Conferencing; JVTOS; MMMS; Video Applications	Dutch Universities; Eindhoven City Administration; Research Institutes
Norway	Five islands interconnected via Supernett (ATM cross connect network): Oslo, Kjeller, Bergen, Trondheim, Tromso. Mix of ATM cross connects, FDDI, Ethernet in the islands; Connected to the ATM Pilot; Possibility of interconnection via satellite.	MM Services (mailing, archiving, ...); Telemedicine; Distance Education; MM Conferencing;	Health care (doctors); Distance education (teachers and students); Publishers and journalists; Researchers.

Portugal	RIA National Host including sites: Aveiro, Coimbra, Porto, Lisboa, Braga, Santa Maria da Feria, Mangualde; ATM cross connect, Ethernet, FDDI, PONs, X25, N-ISDN, DQDB MAN; Connected to the ATM pilot; Possibility of interconnection via satellite.	Distributed Case Handling, MM Interpersonal Communications, Remote delivery of Expertise, Distributed Learning / Training / Entertainment / Leisure, Monitoring and surveillance, Telemarket placeVideo; Switched 2 Mb/s circuit provision.	Public administration; SMEs and Technological parks; Tourism; Schools and training centres; Hospitals; Universities; Large business; Social care Centers; Museums; Residential Users
Spain	Spanish National Host based on RECIBA island (Madrid); Complementary Facilities (PLANBA, ETSIT-UPM); ATM cross connect, FDDI; Connected to the ATM Pilot.	MM and multi-point conference; MM messaging; MM CSCW; Video-retrieval; B-ISDN Supplementary Services; LAN-to-LAN interconection	Tourism (Hotels, Travel Agencies, Spanish Paradores); Health Care (Hospitals); Educational (Universities); Scientific (Public Research Institutions); Financial (Banks); Industry (Telecom, Aerospace); People with Special Needs; Public Administrations; Residential Users
Sweden	Stockolm Gigabit Netswork; Optical Fiber Network for precompetitive research; 10Gb/s experimentation	Open to negotiations with partners	Open to negotiations with partners
	Lund University; ATM Platform; Radio LAN	Interactive Digital MM; Mobility and Personal Communications	Research population; SMEs
	C&C National Host: including access to Stockholm Gigabit Network, Swipnet, Tipnet and Stockolm City Network; SDH, ATM, PSTN, ISDN, CATV,Wireless networks (NMT, GSM and Mobitex).	Education, Teleworking, Trade, Home services, Control Centers	SMEs; Public authorities (National and Local); Education Sector (Upper secondary schools and comprehensive schools)
Switzerland	ATM Testbed in Basel, based on EXPLOIT project; Connected to the ATM Pilot.	Managed broadband network services on international scale (Frame Relay, , Virtual Leased Lines, ISDN, CATV)	Swiss Scientific / Academic community; Researchers; Hospitals; Commercial Organizations; Public Services
UK	SUPERJANET Research Network (60 sites connected, 53 + during the next three years); Broadcasting (Testing facilities offered: experimental TV, HDTV production); ATM/CPN , ATM LANs, N-ISDN; Cable Networks; Long distance dark fibre	IP at 2/34 Mbit/s; Digital audio by satellite; Interactive Mobile video; Digital Terrestrial Broadcasting; SMDS 34 Mbits/s; MM CSCW	Researchers; Education and Tourist enterprises; Local business; Health care; Local authorities; Publishing; Residential users
ESA	Satellite based infrastructure (VSAT)	Digitally compressed video mixed services; LAN interconnection; Video Conferencing; Mobile applications; Data collection and monitoring.	User group (FOCUS)

CEENet

Stowarzyszenie CEENet (Central and Eastern European Networking Association) zostało ustanowione w Warszawie w dniach 14-15 lutego 1994 r. w wyniku porozumienia organizacji mających na celu budowę i utrzymanie naukowych i akademickich sieci komputerowych w poszczególnych krajach Europy Środkowej i Wschodniej. Obecnie są w nim reprezentowane wszystkie kraje tego regionu (oprócz Jugosławii i Bośni). Przewodniczącym CEENet'u jest prof. Hofmokl; sekretariat tej organizacji znajduje się w Warszawie. Głównym zadaniem CEENet'u jest koordynacja międzynarodowych aspektów tyczących się krajów Europy Środkowej i Wschodniej; w szczególności:

- promocja i wspieranie technicznej i organizacyjnej współpracy pomiędzy krajowymi sieciami komputerowymi,
- wymiana informacji technicznej i udostępnianie procedur operacyjnych,
- w miarę potrzeb i możliwości ustanowienie wspólnych serwisów technicznych,
- utworzenie tematycznych grup roboczych
- organizacja konferencji i spotkań warsztatowych
- publikacja i rozpowszechnianie dokumentów, wydawnictw periodycznych i innych,
- wspieranie rozwoju usług sieciowych
- wspólne przygotowywanie wystąpień do europejskich i międzynarodowych organizacji mających na celu promocję sieci komputerowych i serwisów informacyjnych,

Głównym dotychczasowym sukcesem CEENetu stało się postrzeganie tej organizacji przez Komisję Wspólnot Europejskich jako forum współpracy krajów członkowskich w zakresie koordynacji działań sieciowych. W szczególności nastąpiła racjonalizacja pomocy w ramach programu PHARE - do niedawna rozproszonej i niekoniecznie skutecznej. W ramch współpracy organizacji członkowskich nastąpiła także racjonalizacja niektórych połączeń międzynarodowych.
Wymienimy wszystkie organizacje członkowskie CEENETu oraz osoby je reprezentujące.

kraj	Organizacja	Reprezentant krajowy	e-mail
Albania	INIMA	Gudar Bequiraj	inima@santel.it
Austria	ACOnet	Peter Rastl	rast@cc.univie.ac.at
Białoruć	UNIBEL	Andrey Ivanov	ivanov@ok.minsk.by
Bułgaria	UNICOM	Kiril Boyanov	boyanov@bgcict.bitnet
Chorwacja	CARNet	Predrag Pale	predrag.pale@carnet.hr
Czechy	CESNet	Jan Gruntorad	tkgj@sci.cvut.cz
Estonia	EENet	Enok Sein	enok@eenet.ee
Gruzja	ICM	Levan Kiknadze	kiknadze@compmath.acnet.ge
Litwa	LITNet	Laimutis Telksnys	telksnys@mii.lt
Łotwa	LATNet	Janis Kikuts	kikuts@mii.lu.lv
Macedonia	MARNet	Oliver Popov	oliver@soros.mk
Mołdawia	NIC	Valerian Levinski	levinsky@mdearu.cri.md
Polska	NASK	Tomasz Hofmokl	FDL50@plearn.edu.pl
Rosja	FREENet	Andrej Mendkovich	asm@free.net
Rumunia	RNC	Adrian Toia	atoia@roearn.ici.ro
Słowacja	SANET	Pavol Horvath	horvath@cvt.stuba.sk
Słowenia	ARNES	Marco Bonac	bonac@arnes.si
Ukraina	UARNET	Alexander Saban	saban@icmp.lviv.ua
Węgry	HUNGARNet	Laszlo Csaba	h26csa@ella.hu

Kraje Europy Środkowej i Wschodniej (oprócz Austrii)

Nie miejsce tu na szczegółowe prezentacje sieci komputerowych w poszczególnych krajach, ani na głębszą analizę zjawisk tyczących się ich rozwoju. Odnotujmy tylko, że rozwój sieci w skali zbliżonej do Polski osiągnęły tylko Węgry, Czechy, Słowacja i Słowenia. Bardzo zagmatwana jest sytuacja w Rosji, gdzie pojawiło się wiele inicjatyw sieciowych, a nawet ustanowiono kilka wydajnych łącz międzynarodowych; różnorodne działania wydają się być nie skoordynowane. Jak dotychczas, główną siecią Rosji pozostaje RELCOM - prywatna sieć UUCP opierająca się na łączach komutowanych.

Piotr Wiench
Zakład Teorii Kultury IFiS PAN

Internet jako laboratorium nowych zjawisk społecznych

Zmiany w sposobach komunikowania między ludźmi które wiążą się z upowszechnieniem rozległych sieci komputerowych mogą być zjawiskiem porównywalnym do tych, które przyniosło pismo, wynalezione 3000 lat p. n. e., druk, wynaleziony w 1450 r., czy telegraf i telefon, wynalezione pod koniec XIX w.

Warto więc zwracać uwagę na zachodzące już teraz w zjawiska, które spotęgują się po upowszechnieniu tego nowego środka masowego przekazu. Sformułowania "środek masowego przekazu" używam nieprzypadkowo. Internet ze środka komunikacji środowiska naukowego staje się coraz powszechniejszą techniką rozpowszechniania informacji, przybierając masowy charakter. Warto także poświęcić nieco uwagi innym sieciom, które mogą być uzupełnieniem tego, co oferuje Internet.

Chciałbym zasygnalizować zatem kilka zjawisk społecznych, które powstają w wyniku rozwoju sieci. Jest to przegląd niepełny, a każde z poruszanych zagadnień wymagałoby bardziej wnikliwego przedstawienia. Mam nadzieję, że wszystkie te wątki będę mógł z czasem rozwinąć w ramach planowanego projektu badawczego.

Ekspansja nowej technologii powoduje zmiany w ludzkich zachowaniach. Poczta elektroniczna spowodowała w Stanach Zjednoczonych nawrót do pisania listów w skali nie spotykanej od XIX w. W miarę upowszechniania się Internetu, podobnego zjawiska można się spodziewać również i w Polsce. Barierą, która utrudnia rozwój tej formy kontaktu jest jednak brak kompletnych i łatwych w obsłudze baz danych o użytkownikach sieci.

Jakościową zmianę, którą przynoszą sieci komputerowe, jest możliwość komunikacji z wieloma odbiorcami w postaci list dyskusyjnych czy grup Usenetu. Łączenie się ludzi o podobnych zainteresowaniach niezależnie od dzielących ich odległości może być czynnikiem silnie wzmacniającym więzi społeczne.

Wreszcie należy wymienić periodyki sieciowe, które mogą odegrać niezwykle istotną rolę. Pionierskim przedsięwzięciem tego rodzaju są warszawskie "Donosy". Dostęp do sieci ma obecnie w Polsce kilkadziesiąt tysięcy ludzi, czyli więcej, niż liczba czytelników niejednego czasopisma. Liczba ta będzie wzrastać, co za tym idzie - zwiększać się będzie krąg odbiorców tego typu publikacji. Szczególne znaczenie ma tu fakt, że w momencie, kiedy ta infrastruktura komunikacyjna się rozwinie, nakłady niezbędne do rozpowszechniania tego typu publikacji będą dla autorów minimalne. Co za tym idzie, zdemokratyzuje się możliwość upowszechniania

informacji, dziś dostępna tylko dla tych, których stać na inwestycję w druk czasopisma, jego kolportaż i reklamę.

Powstaje pytanie o granice wolności słowa w tym środku przekazu. Jak skomplikowane są to problemy dowodzi trwająca w Stanach Zjednoczonych dyskusja, czy w przypadku sieci komputerowych za rozpowszechnianie treści o charakterze np. obscenicznym, oszczerczym lub służącym celom przestępczym odpowiedzialny jest tylko autor, czy również dysponent kanału rozpowszechniania, np. administrator węzła lub BBSu.

Tego typu problemy zaczynają się pojawiać także i w Polsce. Przypomnijmy choćby sprawę rozesłanych na liście CIUW-L życzeń świątecznych dla muzułmanów. Złośliwy komentarz jednego z subskrybentów wywołał bardzo gwałtowną reakcję obrażonego autora, włącznie z groźbą procesu sądowego. Jest to zatem materia bardzo delikatna. Potrzebne są tu zatem precyzyjne regulacje prawne: tak jak w przypadku każdego konfliktu powinny istnieć mechanizmy, które zapobiegają jego eskalacji i umożliwiają jego rozwiązanie poprzez odwołanie się do powszechnie akceptowanych norm.

Warto sobie uświadomić, że obok rozwiązań opartych o demokratyczną kulturę prawną możliwe są także i inne regulacje. W Rosji powołano niedawno specjalny urząd o policyjnym charakterze i bardzo rozbudowanych prerogatywach, którego celem jest kontrola sieci komputerowych.

Na tym tle warto zastanowić się, w którym kierunku pójdzie rozwój sieci w Polsce: nie do przyjęcia jest model, w którym ludzie mogą się komunikować tylko za przyzwoleniem władzy. Należy się spodziewać, że sieć w Polsce będzie miała cechy nieco anarchicznego i czasem uciążliwego sejmiku, na którym jednak swobodnie i bez cenzury wolni obywatele uczą się demokracji.

Na uwagę zasługuje potencjalna rola sieci w rozwoju społeczeństwa obywatelskiego - ruchu stowarzyszeniowego, wszelkich form uczestnictwa w sprawach publicznych, uczestnictwa w różnych grupach. Przez ostatnie 200 lat w Polsce tylko przez lat 25 istniały nieograniczone możliwości zrzeszania się obywateli. Szczególnie ważnym problemem z tego punktu widzenia jest uregulowanie dostępu do sieci dla organizacji pozarządowych, takich jak np. ruchy ekologiczne i inne stowarzyszenia wyższej użyteczności. Jako organizacje nie nastawione na zysk (non-profit), utrzymujące się często z niewielkich dotacji budżetowych nie są one w stanie ponosić wysokich kosztów dostępu do sieci na takich zasadach, jak firmy komercyjne. Tym niemniej zainteresowanie dostępem do Internetu jest w tych środowiskach duże.

To właśnie w aktywności tych grup, dla których sieć jest znakomitym środkiem komunikacji widzę wielki potencjał, który może być z ogromnym pożytkiem wykorzystany. Przy tym wsparcie tego typu stowarzyszeń poprzez udostępnienie im sieci należy widzieć w szerszym kontekście: jako inwestowanie niewielkich w sumie środków w aktywność społeczną, która przynosi znaczne korzyści całemu społeczeństwu.

Sam proces asymilacji Internetu jako nowej formy komunikowania się jest niezwykle interesującym zjawiskiem społecznym.

Przywołując porównanie Internetu do wynalazku druku, można się spodziewać, że procent społeczeństwa mający dostęp do sieci będzie za pewien czas wskaźnikiem precyzyjniej mierzącym stopień rozwoju kraju niż obecnie procent ludności umiejącej czytać i pisać.

Tym większe znaczenie ma rozszerzanie sieci na coraz nowe grupy społeczne. Warto tu więc wspomnieć o paru przełomowych wydarzeniach, które w Polsce wyprowadziły Internet poza mury wyższych uczelni.

Mimo wielu wątpliwości, jakie towarzyszyły utworzeniu w Pałacu Młodzieży w Warszawie bramki między Internetem i amatorską siecią BBSów FIDONET bramka ta powstała. Sieć FIDO jest finansowana z własnych środków właścicieli BBSów i jest wielkim osiągnięciem spontanicznie tworzącego się amatorskiego ruchu. Zapewniając możliwość - jakkolwiek ze sporym opóźnieniem - wymiany poczty z Internetem, FIDO dla wielu ludzi jest pierwszym kontaktem ze światem sieci komputerowych. Oprócz poczty sieć ta pozwala korzystać z konferencji - odpowiedników Internetowych list dyskusyjnych. Sieć ta funkcjonowała w Polsce wcześniej, niż EARN i Internet, dociera ona przy tym do małych ośrodków, gdzie sieci oparte na protokole internetowym pojawią się nieprędko.

Kolejnym istotnym przełomem było powstanie "Maloka BBS", powszechnie dostępnego BBSu komercyjnego w Warszawie. Nie wdając się w rozważania o jakości tych usług warto zauważyć, że otwarcie możliwości korzystania z nich jest przedsięwzięciem o pionierskim znaczeniu.

Wreszcie bardzo istotnym zjawiskiem jest dotarcie Internetu do szkół - początkowo w formie kont, udostępnianych uczniom w niektórych węzłach sieci, później zaś w ramach akcji "Internet dla szkół", zainicjowanej na Wydziale Fizyki Uniwersytetu Warszawskiego. Jest to otwarcie na nowy krąg użytkowników sieci, który w perspektywie kilku lat wchodząc na wyższe uczelnie będzie już w pełni przygotowany do wykorzystania tkwiącego w Internecie potencjału.

Ten proces powiększania kręgu użytkowników sieci mógłby być kontynuowany. W Polsce istnieją techniczne możliwości budowy powiązanych z Internetem sieci komputerowych opartych na istniejących sieciach telewizji kablowej, o czym była mowa na tegorocznym seminarium "Polman". To rozwiązanie techniczne mogłoby być rzeczywistym przełomem w upowszechnieniu sieci w Polsce i zbliżyć nasz kraj do światowej czołówki. Oznaczałoby dotarcie sieci bezpośrednio do domów jej użytkowników.

Niestety restrykcyjne ustawodawstwo wciąż jeszcze uniemożliwia taką działalność. Dopiero jednak próba wykorzystania tych możliwości, chociażby na prawach ograniczonego w skali i w czasie eksperymentu, mogłaby ukazać nowe zastosowania sieci i być przekonującym świadectwem jej ogromnego znaczenia dla awansu cywilizacyjnego Polski.

Wobec istnienia bardzo licznej polskiej diaspory ogromne znaczenie może mieć ułatwienie przepływu informacji między Polakami w kraju i za granicą. Bardzo obiecującym przedsięwzięciem wydaje się tworzony z inicjatywy redakcji polskiej "Głosu Ameryki" bank danych adresowych Polonii amerykańskiej. W ostatnich latach Polska przeżyła intensywny drenaż mózgów i znaczący odpływ wykwalifikowanej kadry do krajów zachodnich. Internet umożliwia wykorzystanie chociaż w części tego utraconego potencjału poprzez skrócenie obiegu informacji, a w przyszłości być może także poprzez wideokonferencje.

Wreszcie bardzo ciekawym zjawiskiem jest spełnianie się prognoz wybitnej amerykańskiej uczonej, klasyka etnologii, Margaret Mead. Zwróciła ona uwagę na to, że cała dotychczasowa historia ludzkości opierała się na tradycji, funkcjonującej w formie przekazywania swoich doświadczeń życiowych przez starszą generację młodszej. Jednak model ten współcześnie uległ załamaniu. Oto tempo zmian zachodzących w życiu uległo takiemu przyspieszeniu, że tradycyjne wzorce zachowania i postępowania w przekształcającym się świecie stają się bezużyteczne. Zachodzi wtedy zjawisko wypracowywania nowych sposobów radzenia sobie z

rzeczywistością w ramach jednego pokolenia. Ale na tym nie koniec. Mead w latach siedemdziesiątych prorokowała nadejście chwili, kiedy tempo zmian technologicznych będzie tak duże, że nadążać za nim będzie tylko młodsze pokolenie. Odwróceniu ulegnie kierunek zdobywania wiedzy: starsi zaczną uczyć się od młodszych.

Ten moment już nadszedł. Daje się zauważyć nie tylko w procesie przyswajania sobie ulegającej szybkim przemianom wiedzy technicznej związanej z obsługą komputera; przyglądając się scenie hackerskiej w Polsce można zauważyć, że dużym prestiżem w tych środowiskach cieszą się właśnie najmłodsi sprawcy włamań do sieci i to oni są nierzadko autorami nowych sposobów pokonywania zabezpieczeń.

Sieć obrasta także specyficzną młodzieżową subkulturą. W czasie moich wstępnych badań nad takimi grupami na europejskim zlocie hackerów k. Lelystad w Holandii w 1993 r. i nad sceną hackerską w Warszawie i w Lublinie czynnikiem, który był najbardziej interesujący w omawianych grupach było ich podobieństwo, wynikające z wyznawanych specyficznych kodeksów, obowiązujących w tym środowisku, jak i używanego w nich żargonu.

Przejawy organizowania się ludzi wokół Inernetu mają miejsce także w postaci aktywności użytkowników, zainteresowanych dalszymi losami sieci. Przykładem takiej działalności są próby utworzenia polskiego odpowiednika "The Internet Society".

Wreszcie warto zasygnalizować fakt zaistnienia wraz z siecią całej gamy zjawisk, zwiazanych z charakterystyczną dla tego środka przekazu anonimowością przekazu, czy też nieoczekiwane konsekwencje rozwoju Internetu, jak np. nałogowe uzależnienie od sieci, które doczekało się już poważnej analizy w Katedrze Etnologii i Antropologii UW. Bogactwa zjawisk, jakie przynosi sieć, nie sposób zawrzeć w ramach krótkiego opracowania.

WWW jako wszechstronne narzędzie w sieci Internet

Łukasz Płoszajski

1. Historia systemu WWW

Jedną z głównych przyczyn popularności sieci Internet jest ogromna ilość zgromadzonych w niej, dostępnych publicznie zasobów. Zasoby te, to różnego rodzaju oprogramowanie, bazy danych, publikacje, listy dyskusyjne, biblioteki obrazów itp. Korzystanie z tego bogactwa informacji utrudnia fakt, że nie istnieje dla niego żaden globalny schemat dostępu. Aby dostać się do jakichkolwiek zasobów, trzeba znać miejsce w sieci, gdzie są przechowywane. Użytkownik sieci, poszukujący informacji na jakiś temat, zmuszony jest często szukać na oślep, korzystając ze znanych mu archiwów danych. Dużym utrudnieniem jest sposób dostępu do źródła informacji. Różne organizacje, gromadząc dane, udostępniają je na różne sposoby. Dostęp do nich możliwy jest przeważnie przy pomocy prymitywnych usług sieciowych, takich jak protokół transmisji plików *ftp*, czy dostęp terminalowy. Korzystanie z mało przyjaznych komend protokołów typu *ftp*, czy też uczenie się różnych sposobów dostępu do każdej bazy danych jest dla przeciętnego użytkownika dużym utrudnieniem.

Aby ułatwić dostęp do gromadzonych danych zaczęto opracowywać różne „systemy informacyjne". Ich głównym celem było stworzenie dla użytkownika wygodnego interfejsu dostępu do informacji, ukrycie miejsca przechowywania zasobów i możliwość wyszukiwania informacji na zadany temat. Jednym z pierwszych tego typu systemów, który zyskał szeroką popularność, był *gopher*. Oferował on użytkownikowi dostęp do informacji w formie menu, gdzie pozycjami mogły być inne menu, dokumenty, odnośniki do innych serwerów *gophera* lub też do innych systemów informacyjnych, np. do baz danych. Informacja dostępna była tylko w trybie tekstowym.

System World Wide Web pojawił się w sieci w marcu 1989 roku, gdy wprowadzono go jako narzędzie do przedstawiania informacji gromadzonej w CERN-ie. Wkrótce system zaczął być wykorzystywany w innych miejscach, a prawdziwa eksplozja jego popularności nastąpiła po opracowaniu dostępnego publicznie oprogramowania WWW działającego w trybie graficznym i wykorzystującym w pełni multimedialne zdolności komputerów. Dzięki temu z gromadzonych w WWW zasobów zaczęła korzystać ogromna liczba osób, których do tej pory odstraszał siermiężny tryb pracy w sieci. Jednocześnie stało się to zachętą do udostępniania informacji w tym systemie na szerszą skalę.

Na popularność WWW składa się wiele elementów:

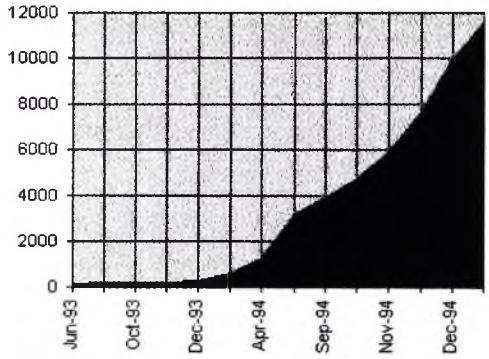
- Możliwość tworzenia dokumentów z włączoną grafiką, z odsyłaczami do innych dokumentów czy też plików z grafiką, dźwiękiem lub filmami; przy czym każdy z tych dokumentów może się znajdować na innym komputerze w sieci,

- Prosty język opisu dokumentów - nawet nie znający systemu użytkownik szybko nauczy się tworzyć własne dokumenty,

- Dostępne nieodpłatnie oprogramowanie WWW (zarówno serwerów, jak i klientów - przeglądarek) dla praktycznie każdego systemu operacyjnego,

- Możliwość wiązania dokumentów z programami, umożliwiającymi interakcję z użytkownikiem oraz możliwość tworzenia interfejsów do innych systemów, np. do baz danych.

Poniższy wykres, opracowany przez Matthew Graya, przedstawia szacunkową liczbę serwerów WWW w sieci Internet. Widać wyraźnie gwałtowny wzrost liczby tych serwerów, postępujący od czasu napisania pierwszej graficznej przeglądarki systemu.



Rys 1. Liczba serwerów WWW od czerwca 1993 do stycznia 1995.

2. Zasada działania systemu

System World Wide Web, tak jak większość systemów sieciowych, działa zgodnie z architekturą klient - serwer. Oprogramowanie serwera WWW uruchamiane jest na maszynie, na której gromadzi się informacje. Zajmuje się ono udostępnianiem zgromadzonych lokalnie dokumentów, ochroną dostępu do wybranych informacji, uruchamianiem programów pomocniczych, a ostatnio także kodowaniem przesyłanych danych. Oczywiście możliwości serwera zależą od konkretnego oprogramowania i systemu operacyjnego, na którym to oprogramowanie pracuje.

Klient WWW to aplikacja, którą posługuje się użytkownik, umożliwiająca przeglądanie dokumentów. Oprogramowanie to łączy się ze wskazanym (bądź domyślnym) serwerem WWW, zgłasza żądanie przesłania dokumentu, odczytuje przesyłane dane i wyświetla je lub też uruchamia oprogramowanie pomocnicze, np. do odtwarzania dźwięków. Istnieją proste przeglądarki działające tylko w trybie tekstowym, dla osób z terminalowym dostępem do sieci.

Jest też oprogramowanie działające w różnych środowiskach graficznych, w tym w najbardziej popularnych MS-Windows i X Window. Najczęściej używane, dostępne w sieci Internet, to Mosaic, napisany w National Center for Supercomputing Applications (NCSA) oraz Netscape, opracowany przez Netscape Communications Corporation. Ta ostatnia firma produkuje oprogramowanie serwera i klienta, które mogą kodować przesyłane dane (wykorzystując protokół HTTPS). Jest to istotne przy przesyłaniu poufnych informacji, np. haseł czy kodów do kart kredytowych. Jeżeli nasz komputer ma takie możliwości, to po odpowiednim skonfigurowaniu klient będzie umożliwiał odtwarzenie dźwięków i filmów. Zastosowanie graficznych klientów umożliwia też wykorzystanie bardziej zaawansowanych możliwości systemu WWW, takich jak wypełnianie formularzy i wysyłanie informacji zwrotnych do serwera, czy też „interakcyjną grafikę", gdzie w zależności od wskazanego myszką miejsca na rysunku otrzymujemy różne rezultaty.

Dokumenty tworzone są w języku zwanym hipertekstem (HTML - HyperText Markup Language), który zostanie krótko opisany poniżej. Klient WWW komunikuje się z serwerem przy pomocy protokołu HTTP (HyperText Transmission Protocol). Istnieją standardy HTML i HTTP, jednak prace nad ich rozszerzeniem trwają cały czas, a programiści tworzący aplikacje WWW dodają często własne rozszerzenia. Jeżeli przeglądarka WWW napotka polecenie, którego nie rozumie, to po prostu ignoruje je.

3. HTML - język opisu stron.

Dokumenty umieszczane w WWW są pisane w języku opisu stron - HTML. Prostota tego języka i jego możliwości są jedną z przyczyn popularności całego systemu. Dokumenty w hipertekście można tworzyć przy pomocy specjalnie napisanych do tego programów lub też używając dowolnego edytora, który potrafi zapisać „czysty" tekst, bez własnych znaków sterujących. Istnieje wiele filtrów, które umożliwiają konwersję dokumentów napisanych w innych formatach do HTML.

HTML definiuje format tekstu: podział na paragrafy, występowanie tytułów i wyróżnień tekstu, tworzenie list, dołączanie grafiki. Ostateczna postać wyświetlonego dokumentu zależy jednak od używanej przez nas przeglądarki.

Kluczowym elementem języka jest definicja łącznika - wskazania na inny dokument czy usługę sieciową. W każdym odnośniku możemy wyróżnić tekst bądź obrazek, którego uaktywnienie (poprzez wciśniecie odpowiedniego klawisza w przeglądarce tekstowej bądź wybranie myszką łącznika w przeglądarce graficznej) powoduje rozwinięcie odnośnika, np. wczytanie podanego tam dokumentu. Wskazania takie definiuje się w formacie URL (Universal Resource Locator), podając rodzaj usługi, adres komputera w sieci oraz ścieżkę dostępu do dokumentu, który chcemy odczytać. Czasami dodatkowo podaje się numer portu, na który należy się połączyć - jeżeli nie jest to numer standardowy. Przykładowo strona główna Polski, umieszczona na serwerze WWW pracującym na maszynie info.fuw.edu.pl, znajdująca się w pliku PolandHome.html w katalogu pl, będzie miała wskazanie:

http://info.fuw.edu.pl/pl/PolandHome.html

Poza wskazaniami do hipertekstowych dokumentów istnieją łączniki do innych „usług", np. ftp dla plików dostępnych w publicznych archiwach, gopher do systemu gopher, news do list dyskusyjnch Usenet.

W hipertekstowych dokumentach jako komend formatujących używa się słów kluczowych objętych znakami < oraz >. Każdy tryb formatowania (np. zmianę czcionki na kursywę) trzeba odpowiednią komendą włączyć, a następnie wyłączyć taką samą komendą ze słowem kluczowym poprzedzonym ukośnikiem.

Przykładowy dokument, zawierający jeden paragraf ze wskazaniem do strony tytułowej serwera NASK, ze słowem NASK wyróżnionym kursywą, może wyglądać następująco:

```
<HTML>
<HEAD>
<TITLE>Strona Próbna</TITLE>
</HEAD> <BODY>
<H1> Tytuł strony </H1>
<P> Aby dostać się do serwera <I>NASK</I> naciśnij
<A HREF="http://www.nask.org.pl/Welcome.html"> ten łącznik. </A>
</P>
</BODY>
</HTML>
```

Należy zauważyć, że użytkownik nie widzi całości tego wskazania: nie musi wiedzieć, gdzie się dany dokument znajduje i jak się nazywa.

Podręczniki pisania w HTML-u można oczywiście znaleźć w samym systemie WWW.

4. Zastosowania WWW

W chwili obecnej system WWW to narzędzie, które umożliwia przesyłanie multimedialnych dokumentów, interakcję z użytkownikiem za pośrednictwem formularzy i grafiki, a wszystko to działa w sieci na różnych systemach operacyjnych. Uniwersalność i możliwości systemu oraz przyjazny dla użytkownika interfejs powodują, że niektórzy nazywają oprogramowanie klientów WWW „przeglądarkami do sieci Internet". Przeciętnemu użytkownikowi system ten umożliwia proste dotarcie do wszystkich interesujących go zasobów sieci.

Warto też zauważyć, że oprogramowanie serwera może być w rzeczywistości bramką, umożliwiającą dostęp do innego systemu informacyjnego, tłumaczącą dane z tego systemu na hipertekst. Tego typu zastosowania znajdują coraz szerszą aprobatę wśród twórców oprogramowania komercyjnego. Dla przykładu producenci systemu baz danych Oracle zapowiadają wzbogacenie go o interfejs użytkownika zgodny z HTTP/HTML. Umożliwi to zarówno przeszukiwanie, jak i wprowadzanie informacji do baz danych przy pomocy klientów WWW.

World Wide Web znalazł zastosowanie w ośrodkach uniwersyteckich, do prezentacji lokalnych informacji i publikacji prac naukowych. Wykorzystuje się go do reklamy i „zdalnych zakupów", do obsługi użytkowników (*user support*). Coraz powszechniejsze stają się elektroniczne wydania różnych czasopism. Tworzone są galerie zdjęć i obrazów oraz centra informacji turystycznej. Jedną z najbardziej spektakularnych prób wykorzystania systemu WWW była prezentacja na bieżąco informacji otrzymywanych z sondy kosmicznej.

Wszechstronność systemu najprościej jest pokazać na przykładach. Każdy przykład oprócz opisu zawiera wskazanie, które można wypróbować samemu.

Wykorzystanie serwera WWW jako bazy danych.

Firma PETEX z Bielska-Białej uruchomiła serwer, w którym publikowane są dane dotyczące warunków narciarskich w okolicznych ośrodkach turystycznych. Zbierane systematycznie dane zapisywane są w postaci plików HTML (czyli serwer jest wykorzystywany jako baza danych).

URL: http://www.petex.bielsko.pl/

WWW jako interfejs do innego systemu informacyjnego

Na uniwersytecie w Toruniu uruchomiony jest serwis X.500, z informacjami o instytucjach i osobach ze środowiska naukowego. Informacje te obejrzeć można również przy pomocy WWW, pod następującym wskazaniem:

URL: http://jaguar.cc.uni.torun.pl:8888/Mc=PL

Zastosowania reklamowe

Firma Volvo stworzyła serwer, w którym znaleźć można informacje o najnowszych samochodach tej firmy, opisy systemów bezpieczeństwa, a także listę dealerów w Stanach Zjednoczonych. Całość wzbogacona jest dużą ilością zdjęć i rysunków.

URL: http://www.volvocars.com/

Prognozy meteorologiczne

Interakcyjna mapa pogody Stanów Zjednoczonych. Po wybraniu myszką dowolnego punktu na mapie otrzymujemy szczegółową prognozę dla tego rejonu:

URL: http://www.mit.edu:8001/usa.html

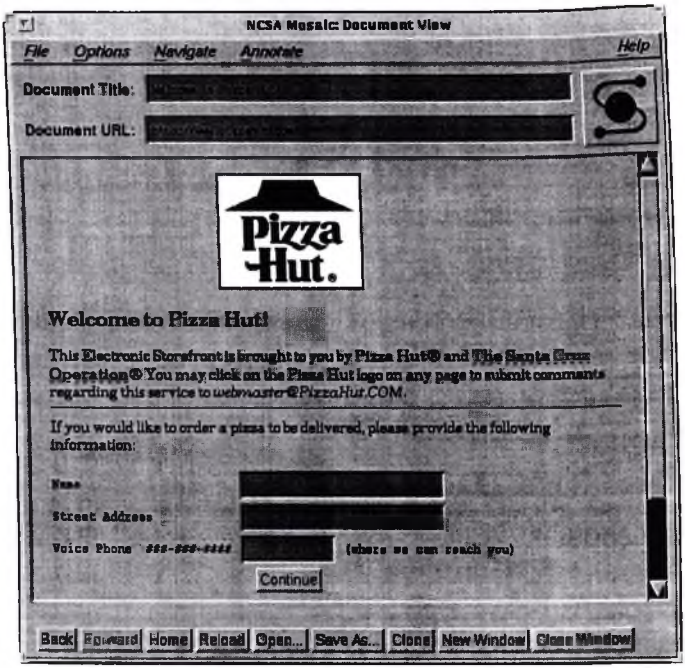
W sieci można też znaleźć zdjęcia i filmy, przesyłane na bieżąco z satelity meteorologicznego:

URL: http://wxweb.msu.edu/weather/

Zdalne zakupy

Coraz więcej firm oferuje możliwość robienia zakupów bez wstawania od biurka. Przykładem tego jest serwer znanej sieci Pizza Hut, przy użyciu którego można zamówić pizzę do domu (niestety, Polska nie jest objęta siecią dostaw...):

URL: http://www.pizzahut.com/



Rys. 2: Strona WWW serwera Pizza Hut, umożliwiająca zamówienie pizzy (wykorzystująca formularze, które wypełnia użytkownik).

Komputerowe czasopisma

Wiele redakcji decyduje się na publikacje elektronicznych wersji swoich czasopism. Są to głównie magazyny komputerowe, ale liczba różnych dostępnych w ten sposób tytułów stale rośnie. Przykładem może być elektroniczne wydanie PC Magazine:

URL: http://zcias3.ziff.com/%7Epcmag/

Sztuka i kultura w WWW

Jeden z najbardziej znanych serwerów, w których można znaleźć coś dla ducha, prezentuje galerię obrazów w Luwrze. Można tam też odbyć wirtualną wycieczkę po Paryżu, oglądając zdjęcia miasta i czytając opisy historyczne. Są tam też wskazania do innych galerii:

URL: http://www.cnam.fr/louvre/

Przykład lokalny to Muzeum Sztuki Współczesnej w Warszawie:

URL: http://www.pap.waw.pl/~martad/

5. Jak znaleźć potrzebną informację?

Problemem, którego nie udało się do końca rozwiązać jest fakt, że użytkownik musi znać „namiar" na każdą informację. Dlatego tworzy się serwery, gdzie gromadzone są wskazania pogrupowane na różne sposoby: tematycznie, geograficznie, alfabetycznie itp. Informacje do takich serwerów też zbiera się rozmaicie, najprostszym sposobem jest namawianie użytkowników, żeby sami uzupełniali bazę. Najbardziej zaawansowane i skuteczne mechanizmy, to programy, które „wędrują" po sieci i kolekcjonują tytuły stron, zbierane następnie w bazie. Są to tak zwane roboty bądź robaki WWW (WWW Worms). Użytkownik może wyszukać wszystkie odnośniki, zawierające podane przez niego słowo kluczowe.

Jeden z serwerów gromadzących w ten sposób dane można znaleźć pod wskazaniem:

http://js.stir.ac.uk/jsbin/js

Przy wyszukiwaniu informacji można też skorzystać z koncepcji stron głównych. Każdy serwer ma swoją stronę główną, są strony główne różnych organizacji, krajów, istnieje strona główna systemu WWW, a nawet strona główna Ziemi. Strony takie są dobrymi punktami startowymi przy wyszukiwaniu wszelkich informacji. Strona główna systemu WWW, wraz z różnymi listami dostępnych serwerów, opisem historii systemu World Wide Web i wieloma innymi wskazówkami znajduje się na serwerze w CERN-ie:

http://info.cern.ch/

Andrzej Adamski
Katedra Prawa Karnego i Polityki
Kryminalnej UMK w Toruniu

ODPOWIEDZIALNOŚĆ OPERATORA SIECI KOMPUTEROWEJ I BBS-u ZA PRZESYŁANĄ INFORMACJĘ: AKTUALNY STANU PRAWNY W POLSCE NA TLE TENDENCJI ŚWIATOWYCH (*wybrane aspekty*)

1. Wstęp

Rozwój regulacji prawnych związanych z elektronicznym przetwarzaniem danych jest równie szybki i nieprzewidywalny jak rozwój nowoczesnych technologii informatycznych. Mowa oczywiście o sytuacji na świecie, w jego cywilizacyjnie najbardziej rozwiniętych regionach. W Polsce, przeżywającej od kilku lat okres prawdziwego boomu informatycznego, proces stanowienia "prawa komputerowego" przebiega tak wolno, że już wkrótce może okazać się jednym z hamulców wkraczania naszego kraju w erę społeczeństwa informatycznego.

Powstanie "infostrad" spowoduje totalną uniformizację przekazu informacji: gazety, programy telewizyjne, rozmowy telefoniczne, usługi bankowe, pocztowe i sklepowe oraz inne formy komunikowania się zostaną zredukowane do tego samego formatu - bitów numerycznych, przesyłanych przy pomocy światłowodów. Jeżeli prognozy te okażą się trafne, to budowa globalnych sieci komputerowych wywoła wiele nowych problemów prawnych. Pojawią się one nieomal w każdej dziedzinie prawa, poczynając od autorskiego i karnego, poprzez telekomunikacyjne i handlowe, na konstytucyjnym i międzynarodowym kończąc. Już dziś wiele krajów i organizacji międzynarodowych przygotowuje się do ich rozwiązania.

W USA, grupy prawników na Cornell University i Chicago-Kent College of Law opracowują projekt modelowej (dla USA) regulacji prawnej w zakresie prawa "internetowego". Powołany z inicjatywy Białego Domu Zespół ds. Infrastruktury Informatycznej, próbuje stworzyć całkowicie nową definicję prawa autorskiego na potrzeby globalnych autostrad informatycznych. Standardy prawne związane z elektroniczną wymianą danych (EDI) w dziedzinie obrotu bankowego i handlu międzynarodowego, opracowuje wyspecjalizowana agenda ONZ (UNCITRAL). Zespół Ekspertów Rady Europy przyjął właśnie projekt zalecenia określającego kierunki nowelizacji procedury karnej krajów członkowskich tej organizacji, w związku z koniecznością dostosowania przepisów prawa karnego procesowego do specyfiki zdigitalizowanej informacji i realiów społeczeństwa informatycznego.

Powołane przykłady to przysłowiowy "wierzchołek góry lodowej" aktualnie prowadzonych za granicą prac legislacyjnych w zakresie tzw. prawa informacyjnego (ius informationis). Mogą one wywoływać wrażenie, że ekspansja prawa w dziedzinę nowoczesnych technologii informatycznych dopiero się zaczyna i z tego względu nasz rodzimy system prawny wcale nie jest anachroniczny i zapóźniony, nie ma więc powodów do narzekań i kompleksów.

Wrażenie to jest niestety całkowicie błędne. Kraje rozwinięte, w ciągu ostatnich 20 lat zdołały bowiem nie tylko stworzyć podstawy prawa informacyjnego, ale co ważniejsze - wykształcić wykwalifikowane kadry i powołać do życia liczne instytucje zajmujące się jego stosowaniem. Aktualnie obserwowana aktywność prawotórcza w tych krajach związana jest z kolejnym etapem rozwoju prawa informacyjnego, które w Polsce w zasadzie jeszcze nie istnieje. Można się o tym przekonać dokonując krótkiego bilansu polskich dokonań legislacyjnych w omawianej dziedzinie na tle sytuacji panującej w krajach Europy Zachodniej.

2. Próba bilansu polskich dokonań legislacyjnych w zakresie ochrony informacji przetwarzanej elektronicznie.

W Polsce z wyjątkiem dwóch ustaw: nowego prawa autorskiego i obowiązującej od 1 stycznia 1995 r. ustawy o rachunkowości (Dz.U. z 1994 r. Nr 121, poz. 591) nie ma w zasadzie innych aktów ustawodawczych, które uwzględniałyby fakt istnienia komputera, dostrzegały z tym związane implikacje prawne i starałyby się je wyartykułować. Można więc stwierdzić, że na razie USTAWODAWCA urządzenie zwane komputerem kojarzy przede wszystkim z jego pierwotną funkcją - maszyny liczącej!

Oczywiście myślenie w tych kategoriach przestało być dominujące w krajach o bardziej od Polski rozwiniętej infrastrukturze informatycznej. Jest to jednak wynikiem innej historii oraz - co się z nią wiąże - ewolucyjnego rozwoju ustawodawstwa w tych krajach. Prawo starało się tam nadążać za postępem technicznym i chroniło w pierwszym rzędzie te dobra, dla których nowe technologie oznaczały nowe zagrożenia. Chodziło więc w szczególności o ochronę praw człowieka i takich jego dóbr osobistych, jak wolność, prywatność oraz o ochronę swobód obywatelskich.

* Pierwsza fala reform ustawodawczych związanych ze zjawiskiem komputeryzacji ogarnęła kraje Europy Zachodniej w latach 70-tych. Stanowiła ona reakcję na potencjalne zagrożenia dla prywatności człowieka związane z technologią elektronicznego przetwarzania danych. "Fenomenalna" pamięć systemów komputerowych, błyskawiczny dostęp do przechowywanych w niej informacji, możliwość transmisji i kompilacji danych sprawiły, że poczucie zagrożenia okazało się silniejsze od fascynacji nowoczesną technologią. W ślad za Szwecją, która jako pierwsze państwo na świecie uczyniła to w 1973 r., większość rozwiniętych gospodarczo krajów zachodnich uchwaliła i wprowadziła wówczas w życie ustawy o ochronie danych osobowych.[1]

** Polska ma od połowy lat 70-tych system PESEL, nie ma natomiast ustawy o ochronie danych osobowych. Istniejący projekt takiej ustawy, mimo iż zawiera poważne wady [2], został ostatnio pozytywnie oceniony przez Komitet Społeczny Rady Ministrów.

* W dekadzie lat osiemdziesiątych przedmiotem reglamentacji prawnej stały się nadużycia popełnianie z wykorzystaniem elektronicznych systemów przetwarzania danych oraz zamachy skierowanie przeciwko tym systemom. W ustawodawstwie karnym wielu krajów pojawiły tzw. "przestępstwa komputerowe". Przedmiotem ich ochrony oprócz tradycyjnych wartości materialnych (mienie) stał się także niematerialny - ze swej natury - komputerowy zapis informacji.

** W Polsce zamachy na dane i systemy komputerowe nie są prawnie zabronione. Zakazy takie zawiera projekt nowego kodeksu karnego. Przewiduje on następujące rodzaje przestępstw komputerowych: oszustwo, sabotaż, podsłuch komputerowy, hacking, bezprawne zacieranie lub modyfikowanie danych komputerowych oraz kradzież i paserstwo programu komputerowego.[3]

* Trzecia z kolei tendencja legislacyjna związana z rewolucją informacyjną polegała na wzmocnieniu ochrony własności intelektualnej w zakresie oprogramowania komputerowego. Kraje, które w ciągu lat 70-tych przyjęły prawnopatentowy model ochrony programów komputerowych, w większości zrezygnowały z niego w latach osiemdziesiątych na rzecz ochrony prawnoautorskiej.[4]

** W Polsce od 23 maja 1994 r. obowiązuje ustawa o prawie autorskim i prawach pokrewnych, która przewiduje ochronę programów komputerowych i baz danych.

* Lata 90-te to początek ery globalnego społeczeństwa informatycznego i poszukiwania prawnych rozwiązań problemów związanych z eksploatacją sieci teleinformatycznych. Zapewnienie im odpowiedniego poziomu bezpieczeństwa przy pomocy środkow prawnych napotyka w Polsce na poważne problemy. Powodem tego są wskazane

luki prawne w zakresie prawnokarnej ochrony danych i systemów komputerowych, a także ogólne niedostosowanie polskiego ustawodawstwa do wspierania rynkowego modelu rozwoju usług teleinformatycznych.[5]

Z myślą o wzmocnieniu ochrony prawnej sieci teleinformatycznych Komitet Ekspertów Rady Europy ds. Problemów Karnoprocesowych Związanych z Technologią Informatyczną wzywa kraje członkowskie do zrewidowania ustawodawstwa wewnętrznego, tak aby pozwalało ono organom ścigania na stosowanie podsłuchu (interception) w trakcie prowadzonych postępowań karnych w sprawach poważnych przestępstw przeciwko poufności, integralności i dostępności systemów telekomunikacyjnych i komputerowych. Dokument ten zawiera ponadto kilkanaście innych szczegółowych zaleceń wskazujących kierunki nowelizacji procedury karnej "na progu społeczeństwa informatycznego".

** Niestety, projekt nowego polskiego kodeksu postępowania karnego większości tych zaleceń nie uwzględnia.

Jak pokazuje powyższa analiza - w porównaniu z Europą Zachodnią - Polska buduje obecnie zręby prawa informacyjnego. Nasze zapóźnienie w tej dziedzinie jest przy tym największe, bo co najmniej kilkunastoletnie, w przypadku ochrony danych osobowych. Gdy chodzi o prawnokarną reglamentację nadużyć komputerowych, dystans dzielący nas od krajów Europy Zachodniej szacować można na ok. 10 lat. Z drugiej strony, są w naszym prawie również takie unormowania, które ze względu na swój tradycjonalizm i przywiązanie do klasycznych zasad odpowiedzialności (opartej na indywidualnym zawinieniu), wydają się być "postępowe" na tle aktualnie zgłaszanych przez niektórych konserwatywnych polityków zachodnich projektów poddania rygorystycznej kontroli informacji cyrkulującej w sieciach komputerowych. Paradoksalnie, dzięki "staremu" prawu mamy realną szansę stać się prawdziwą enklawą liberalizmu i wolności słowa w cyberprzestrzeni.

3. **Aktualne tendencje legislacyjne do ograniczenia swobodnego przepływu informacji w cyberprzestrzeni.**

W Stanach Zjednoczonych, Australii, ale także w Europie Zachodniej pojawiła się silna presja polityczna na ograniczenie swobodnego przepływu informacji w cyberprzestrzeni. Do bardziej widocznych tendencji w tym zakresie należy zaliczyć inicjatywy ustawodawcze zmierzające do obarczenia operatorów systemów odpowiedzialnością za treść przesyłanych przez nich informacji, oraz planowane restrykcje dotyczące stosowania kryptografii.

W Australii rozważa się możliwość wprowadzenia odpowiedzialności karnej za wykorzystywanie BBS-ów do przesyłania, reklamowania lub posiadania w celu udostępnienia materiałów, które dotyczą takich tematów jak seks, używanie narkotyków,przestępstwa, okrucieństwo, przemoc, działalność wywrotowa i przedstawiają je w taki sposób, który może "urazić przeciętnego dorosłego człowieka".[6]

W Stanach Zjednoczonych tzw. "projekt Exona" - senatora z Nebraski, idzie jeszcze dalej.[7] Proponuje bowiem obarczenie odpowiedzialnością wszystkie podmioty świadczące usługi telekomunikacyjne (począwszy do dużych kompanii telekomunikacyjnych, i komercyjnych serwisów informacyjnych, a na BBs-ach kończąc) za treść każdej świadomie przesłanej przy pomocy mediów elektronicznych informacji. Oficjalnie, obie te inicjatywy ustawodawcze (australijska i amerykańska) skierowane są przede wszystkim przeciwko rozpowszechnianiu za pomocą sieci teleinformatycznych materiałów obscenicznych, w szczególności tzw. pornografii dziecięcej.

Podobne propozycje wysuwane są w Europie. Chodzi o ściganie tzw. "wydawców elektronicznych" za świadomie rozpowszechniane w sieciach teleinformatycznych informacji zabronionych przez prawo. Mówi o tym cytowany wyżej projekt najnowszego Zalecenia Rady Europy.

Nie są to bynajmniej problemy kulturowo czy cywilizacyjnie nam odległe. Wręcz przeciwnie. Niedawny incydent z tzw. *."książką kucharską, czyli poradnikiem z sieci komputerowej Stana Tymińskiego, jak domowym*

sposobem otrzymać napalm, nitroglicerynę lub LSD" [8] wskazuje, że wraz z rozwojem telematyki dotarły one także do Polski i wymagają oceny prawnej.

4. Odpowiedzialność operatora sieci komputerowej za treść przesyłanej informacji a tajemnica korespondencji

W świetle obowiązującego w Polsce prawa operatorzy sieci komputerowych, którzy świadczą usługi telekomunikacyjne w zakresie transmisji danych i poczty elektronicznej, w zasadzie nie ponoszą odpowiedzialność za treść informacji przesyłanej siecią przez klienta (abonenta). Analogia do sytuacji prawnej operatorów świadczących usługi telefoniczne jest tu wyraźna, aczkolwiek chyba nie całkowita. Nie można byłoby bowiem zwolnić z odpowiedzialności karnej operatora, który wiedząc, iż jego klient rozpowszechnia informacje chronione prawem lub objęte zakazem rozpowszechniania, nie odmawia mu świadczenia swych usług, lub zawiera umowę o ich świadczenie godząc się z tym, iż w ten sposób ułatwia innej osobie popełnienie czynu zabronionego (art.18 § 2 kk).

Teza, iż operator sieci komputerowej nie ponosi odpowiedzialności za treść informacji przesyłanej przez swego klienta ma również inne uzasadnienie. Wiąże się ono z faktem, iż treść tej informacji objęta jest tajemnicą korespondencji, do przestrzegania której zobowiązany jest także operator sieci. Argument ten, na pierwszy rzut oka przekonywający, traci na znaczeniu po przeanalizowaniu obowiązujacych w Polsce przepisów prawa odnoszących się do ochrony tajemnicy korespondencji.

Tajemnica korespondencji, podobnie jak inne postaci wolności człowieka, objęta jest ochroną konstytucji (art.87 ust.2). Kodeks cywilny zalicza ją do dóbr osobistych jednostki (art.23 k.c.), a ustawa o prawie autorskim i prawach pokrewnych reglamentuje dopuszczalność rozpowszechniania cudzej korespondencji (art.82 i 83). Wreszcie kodeks karny przewiduje sankcje za naruszenie tajemnicy korespondencji (art.172 k.k.).

Jeżeli jednak postawimy pytanie: czy w świetle polskiego ustawodawstwa czytanie cudzej korespondencji elektronicznej, ujawnianie lub rozpowszechnianie jej treści bez wiedzy i zgody adresata jest naruszeniem tajemnicy cudzej korespondencji, to odpowiedź na to pytanie wcale nie jest prosta i jednoznaczna.

Problem ma przede wszystkim charakter definicyjny, gdyż żadna z obowiązujących w Polsce ustaw nie wyjaśnia pojęcia "korespondencji". Termin "korespondencja pisemna", zawarty w ordynacji pocztowej [9] został tam zdefiniowany jako " informacje pisemne o charakterze bieżącym i osobistym, mające walor niepowtarzalności, przesyłane w listach lub na kartkach pocztowych" (§ 4 ordynacji). Jest to więc ujęcie tradycyjne, łączące pojęcie korespondencji z jej materialnym substratem (list, kartka pocztowa). Z równie wąskim i tradycyjnym sposobem rozumienia pojęcia "tajemnica korespondencji" spotykamy się na gruncie kodeksu cywilnego, który w art. 23 chroni dobra osobiste człowieka, m.in. zdrowie, wolność, cześć, swobodę sumienia, nazwisko, wizerunek, a także tajemnicę korespondencji. Gdy chodzi o wykładnię tego przepisu, to w doktrynie prawa cywilnego reprezentowany jest pogląd, że pojęcie "korespondencji" odnosi się do tej formy interpersonalnego porozumiewania się ("komunikowania się"), która posługuje się nośnikiem fizycznym (listem).[10] Jest to zatem interpretacja wyłączająca z zakresu cywilnoprawnej ochrony tajemnicy korespondencji nawet poufność rozmów telefonicznych.

Ochrona tajemnicy korespondencji na gruncie przepisów kodeksu karnego (art.172 kk) obejmuje natomiast zarówno rozmowy telefoniczne, jak i inne formy interpersonalnego przekazu informacji przy wykorzystaniu środków telekomunikacyjnych. W świetle definicji tego ostatniego pojęcia na gruncie ustawy z dnia 23 listopada 1990 r. o łączności (art.2 ust.1 pkt.3), nie ulega wątpliwości, że tajemnica korespondencji, chroniona przez przepis art. 172 kk, obejmuje także treść informacji przesyłanych pocztą elektroniczną. Karalne jest jednak tylko takie naruszenie tajemnicy przesyłanej pocztą elektroniczną, które ma charakter "podstępny". Zakres znaczeniowy tego określenia wywołuje w literaturze prawniczej różnice zdań i nie jest bynajmniej utożsamiany wyłącznie z brakiem zgody osób uprawnionych (nadawcy i adresata) na zapoznanie się przez osobę trzecią z treścią korespondencji dla niej nie przeznaczonej.

Nie ulega natomiast wątpliwości, iż w przeciwieństwie do funcjonariuszy organów ścigania (art.198 kpk), operatorzy sieci komputerowych nie mają aktualnie żadnych szczególnych uprawnień ustawowych do naruszania

tajemnicy cudzej korespondencji. Nie mogą w związku z tym w żadnym wypadku spełniać funkcji cenzorów i delatorów.

Należy jednak postulować, aby wzorem niektórych ustawodawstw obcych, zwolnić operatorów sieci komputerowych z przestrzegania tajemnicy cudzej korespondencji w ściśle określonych okolicznościach podyktowanych względami natury technicznej. Odpowiednią klauzulę w tym zakresie mogłaby zawierać np. nowa ustawa o łączności.

5. Odpowiedzialność operatora elektronicznej tablicy ogłoszeniowej

Zakres odpowiedzialności operatora za treść przesyłanej informacji będzie o wiele szerszy, gdy poza właściwą mu funkcją "przekaźnika" informacji, zajmie się on także jej nadawaniem i rozpowszechnianiem za pomocą np. założonego w tym celu BBS-u.

Komitet Ekspertów Rady Europy postuluje wręcz, aby do tzw. "wydawców elektronicznych" stosować te same zasady odpowiedzialności, które aktualnie obowiązują wydawców książek lub prasy. Zagadnienie jest jednak nieco bardziej skomplikowane. Operator BBS-u, w odróżnieniu od redaktora konwencjonalnej gazety, nie ma bowiem na ogół wpływu na to, co za pośrednictwem jego tablicy elektronicznej zechcą opublikować jej użytkownicy. Ponieważ klasyczne zasady odpowiedzialności karnej opierają się na zasadzie winy za własne, nie zaś cudze czyny, obarczanie odpowiedzialnością operatora za działanie innej osoby nie wchodzi w grę. Pozostaje natomiast alternatywa w postaci przypisania operatorowi odpowiedzialności za zaniechanie usunięcia z tablicy zabronionej przez prawo informacji. Jednakże warunkiem takiej odpowiedzialności musi być ciążący na operatorze obowiązek do sprawowania de facto cenzury represyjnej, eliminowania "nielegalnych" materiałów w strefie buforowej BBS-u i udostępniania skontrolowanych merytorycznie przez siebie plików do obszaru dostępnego dla użytkowników. Należy zaznaczyć, że jest to tylko hipoteza dotycząca możliwego kierunku ewolucji ustawodawstwa reglamentującego zasady opowiedzialności "wydawców elektronicznych". W chwili obecnej prawne źródła wyżej wspomianych obowiązków w systemie prawa polskiego nie istnieją, a odpowiednie stosowanie przepisów ustawy z dnia 28 stycznia 1984 r. prawo prasowe wydaje się być wykluczone, ze względu na nieadekwatność ustawowego pojęcia "prasy" (art. 7 ust.2 pkt.1 prawa prasowego) do takiego medium przekazu informacji, jakim jest elektroniczna tablica ogłoszeniowa (chyba, że chodzi o wydawaną za jej pośrednictwem gazetę lub inną publikację periodyczną). Z tych powodów operatorowi BBS-u nie można obecnie przypisać odpowiedzialności za przestępne zaniechanie (także w postaci pomocnictwa) usunięcia z tablicy elektronicznej informacji naruszających prawo. Nie ma on także, z pewnymi wyjątkami, prawnego obowiązku zawiadomienia organów ścigania o naruszeniu przepisów prawa karnego przez użytkowników BBS-u.

6. Obowiązek zawiadomienia o przestępstwie

Polskie prawo nie zna powszechnego obowiązku prawnego zawiadamiania organów ścigania o znanym komuś fakcie popełnienia przestępstwa. Obowiązek taki mają jedynie instytucje państwowe i społeczne (a więc kierujące nimi osoby), które w związku ze swą działalnością dowiedziały się o popełnieniu przestępstwa ściganego z urzędu (art.256 § 2 kpk). Kierownicy tych instytucji lub samodzielnych jednostek organizacyjnych są nie tylko obowiązani do niezwłocznego zawiadomienia prokuratora lub policji o takim przestępstwie, lecz także do przedsięwzięcia czynności nie cierpiących zwłoki, aby nie dopuścić do zatarcia śladów i dowodów przestępstwa.
Wszyscy pozostali obywatele mają tylko społeczny (a więc nie wywołujący żadnych skutków prawnych w razie jego zaniedbania) obowiązek zawiadomienia o przestępstwie.[11]

Wyjątek od tej ogólnej zasady stwarza art. 254 kk, który zobowiązuje pod groźbą odpowiedzialności karnej, do niezwłocznego zawiadamiania organów ścigania o popełnieniu przestępstw przeciwko podstawowym interesom politycznym i gospodarczym państwa (zdrada Ojczyzny, spisek antypaństwowy, szpiegostwo, zamach terrorystyczny, dywersja i sabotaż oraz zbrodni zabójstwa. Obowiązek zawiadomienia powstaje tylko wtedy, gdy wiadomość o popełnieniu jednego z wymienionych przestępstw jest wiarygodna. Obowiązek zawiadamienia, przewidziany w art.

254 kk, powoduje uchylenie tajemnicy dziennikarskiej (art.15 prawa prasowego) i tajemnicy lekarskiej (art.14 ust. 2 ustawy o zaw. lekarza z 1950r.).

Zaniechanie obowiązku prawnego (art.256 § 1 kpk) zawiadomienia o przestępstwie pociąga za sobą odpowiedzialność karną z art. 246 § 1 lub 2 kk.

7. Pornografia w sieci

Polskie prawo karne (art.173 kk) penalizuje w zasadzie tylko rozpowszechnianie pornografii, a więc przekazywanie jej szerszemu kręgowi odbiorców. Kupowanie, posiadanie, oglądanie, a nawet pokazywanie tego rodzaju dzieł nie jest zabronione. Przepis mówi o pismach, drukach, fotografiach lub innych przedmiotach mających charakter pornograficzny. Chodzi więc o rozpowszechnianie przedmiotów o charakterze materialnym, np. w drodze sprzedaży lub wypożyczenia pism, kaset, zdjęć. "Pornografia w sieci" nie ma natomiast atrybutu przedmiotu materialnego. Żadna więc elektroniczna kolekcja pornografii, nawet największa i dostępna każdemu użytkownikowi sieci, nie narusza dyspozycji art. 173 §2 kk, który przewiduje karę za "sporządzanie, przechowywanie, przenoszenie, przesyłanie lub przewożenie w celu rozpowszechnienia" pism, druków fotografii lub innych przedmiotów mających charakter pornograficzny. Odkrycie istnienia takiej kolekcji przez operatora sieci (instytucję państwową lub społeczną) nie obliguje go zatem do zawiadomienia organow ścigania o tym odkryciu. Tym bardziej nie ma on takiego obowiązku gdy chodzi o przypadki ściągania plików (porno)graficznych, gdyż czyn taki nie mieści się w pojęciu rozpowszechniania, jakim posługuje się art. 172 § 1 kk. Potwierdza to sformułowaną na wstępie tezę o liberalnym, aczkolwiek w sposób całkowicie niezamierzony, charakterze "starego" prawa w warunkach rewolucji informacyjnej.

8. Podsumowanie

Obserwowane w innych krajach, bardziej od Polski zaawansowanych pod względem rozwoju teleinformatyki, tendencje legislacyjne będą miały prawdopodobnie charakter uniwersalny. Wszak wiążą się one z stopniowo już urzeczywistnianą wizją informatycznego społeczeństwa bez granic. Warto więc śledzić zachodzącą w tym zakresie ewolucję. Nawet jeżeli dziś nie jesteśmy jeszcze w stanie przewidzieć ostatecznego kształtu nowych instytucji prawnych, pewne jest to, że w najbliższym czasie zostaną one wprowadzone do ustawodawstwa wewnętrznego wielu państw.

CYTOWANE ŹRÓDŁA

[1] A.Mrózek, Ustawowe prawo ochrony danych, Wyd. UMK, Toruń 1981.

[2] Chrońmy nasze dane, "PCKurier" nr 6/1995.

[3] K.Buchała, Reforma polskiego prawa karnego materialnego.Przestępstwa przeciwko ochronie informacjii oszustwo komputerowe; A.Adamski, Przestępstwa komputerowe w projekcie kodeksu karnego na tle europejskich standardów normatywnych (w:) Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Materiały z konferencji naukowej (Poznań, 20-22 kwietnia 1994), Wyd. "Dom Organizatora", Toruń 1994.

[4] U.Siebier, Information Technology Crime and Criminal Information Law (w:) U.Sieber (red.) Information Technology Crime, vol. 6, Cologne 1994.

[5] A.Adamski, Aspekty prawne ochrony sieci komputerowych w Polsce,"Net Forum" nr 3/1995 (w druku).

[6] Australian Task Force Report on Computer Bulletin Board Systems, Attorney General's Department, 8 August 1994.

[7] Snuffy Porn on the Net, "Time", February 20,1995.

[8] L.Kraskowski, >>Książka kucharska<< dla terrorysty, "Życie Warszawy" z 06.03.1995 r.

[9] Rozporządzenie Ministra Łączności z dnia 7 X 1991 r.(Dz.U. Nr 96, poz.427).

[10] I.Dobosz, Tajemnica korespondencji jako dobro osobiste i jego ochrona w prawie cywilnym, Kraków 1989.

[11] L.Gardocki, Prawo karne, Warszawa 1994.

dr Jerzy Gospodarek
Szkoła Główna Handlowa
w Warszawie
Katedra Prawa Gospodarczego

WYDAWANIE KONCESJI I ZEZWOLEŃ W DZIEDZINIE TELEKOMUNIKACJI W ŚWIETLE ZMIAN USTAWY O ŁĄCZNOŚCI

1. Uwagi ogólne

Budowa i eksploatacja sieci komputerowych jest działalnością w dziedzinie telekomunikacji. Konsekwencją tego stanu rzeczy jest konieczność przestrzegania przepisów ustawy z dnia 23 listopada 1990 r. o łączności /Dz. U. Nr 86, poz. 504, z 1991 r. Nr 69, poz. 293 i Nr 105, poz. 451 oraz z 1993 r. Nr 7, poz.34/. Na podstawie art. 14 tej ustawy oraz w związku z jej art. 12 i 17 jednostka badawczo-rozwojowa pod nazwą Naukowa i Akademicka Sieć Komputerowa w Warszawie otrzymała zezwolenie nr 127/94 na działalność w dziedzinie telekomunikacji, wydane przez Ministra Łączności w dniu 9 grudnia 1994 r. Należy oczekiwać powstawania innych sieci tego typu i świadczenia usług przez ich operatorów. Jest więc celowe przedstawienie, jakie nowe uregulowania prawne dotyczące procesu wydawania dotychczasowych zezwoleń telekomunikacyjnych, są zawarte w uchwalonej w dniu 21 kwietnia 1995 r. ustawie o zmianie ustawy o łączności oraz niektórych innych ustaw.

Trzeba zaznaczyć, że w chwili zakończenia pisania niniejszego referatu proces ustawodawczy związany z nowelizacją ustawy o łączności nie był jeszcze zamknięty. Do uchwalonej bowiem ustawy musi jeszcze ustosunkować się Senat i ewentualne jego poprawki Sejm może przyjąć lub odrzucić. Z kolei Prezydent zgodnie z Małą Konstytucją może zgłosić tzw. weto zawieszające, które może być odrzucone przez Sejm większością 2/3 głosów. Ponadto Prezydent może wystąpić do Trybunału Konstytucyjnego z wnioskiem o stwierdzenie zgodności ustawy z Konstytucją. Trudno więc jeszcze stwierdzić, jakie będą dalsze losy tej nowelizacji ustawy o łączności dokonanej przez Sejm w trybie pilnym. Można jednak z dosyć dużym prawdopodobieństwem oczekiwać, że pod koniec maja br. Prezydent podpisze ustawę o zmianie ustawy o łączności oraz niektórych innych ustaw i następnie akt ten zostanie opublikowany w Dzienniku Ustaw. Wówczas zmiany do ustawy o łączności weszłyby w życie po upływie 30 dni od dnia ogłoszenia ustawy nowelizującej tj. najprawdopodobniej na początku lipca br. Takie oczekiwanie ma swoje uzasadnienie m.in. w tym, że ustawa ta została przyjęta zdecydowaną większością głosów, przekraczającą 2/3 liczby posłów biorących udział w głosowaniu. Aż 247 posłów było za przyjęciem omawianego pilnego, rządowego projektu ustawy, a tylko 41 przeciw, przy 69 wstrzymujących się od głosu.1/

2. Koncesje a zezwolenia

Dotychczasowe zezwolenia telekomunikacyjne były udzielane na zakładanie i używanie urządzeń, linii i sieci telekomunikacyjnych oraz na świadczenie usług za pomocą tych urządzeń, linii lub sieci. Omawiana nowelizacja zmierza do wprowadzenia rozwiązania odróżniającego koncesje wydawane na świadczenie usług telekomunikacyjnych od zezwoleń udzielanych na zakładanie i używanie radiokomunikacyjnych urządzeń nadawczych lub nadawczo-odbiorczych bądź urządzeń lub sieci telekomunikacyjnych. Nie jest to tylko zmiana terminologiczna, gdyż ma ona merytoryczne przyczyny oraz skutki i wprowadza podział podmiotów wykonujących działalność w dziedzinie telekomunikacji na działające na podstawie koncesji oraz działające na podstawie zezwoleń.2/ Oczywiście zostają przy tym zachowane ustawowe podstawy działalności w tej dziedzinie Telekomunikacji Polskiej S.A. oraz jednostek organizacyjnych podległych MON, MSW i MSZ.

Warto dodać, że stworzona została możliwość wydawania omawianych koncesji łącznie z odpowiednim zezwoleniem na zakładanie i używanie radiokomunikacyjnych urządzeń nadawczych lub nadawczo-odbiorczych, innych urządzeń telekomunikacyjnych lub sieci telekomunikacyjnych. Nie będzie więc potrzeby dublowania procesu decyzyjnego w tych sprawach, jeśli jeden podmiot zechce wystąpić zarazem o koncesję i zezwolenie.

Należy też zaznaczyć, że koncesje i zezwolenia na działalność w dziedzinie telekomunikacji w pewnych wypadkach nie będą wymagane. Zostało to pozostawione uznaniu Ministra Łączności, który w drodze rozporządzenia ma możliwość określenia usług telekomunikacyjnych, rodzajów urządzeń telekomunikacyjnych /w tym radiokomunikacyjnych/ oraz rodzajów wewnętrznych i wydzielonych sieci telekomunikacyjnych podlegających temu wyłączeniu. Chociaż wskazane rozporządzenie ma charakter fakultatywny, to należy oczekiwać, że na podstawie tej zmienionej delegacji ustawowej zawartej w art. 13 ustawy o łączności zostanie wydany nowy akt wykonawczy, uchylający rozporządzenie Ministra Łączności z dnia 30 czerwca 1993 r. w sprawie urządzeń, linii i sieci telekomunikacyjnych, których zakładanie i używanie nie wymaga zezwolenia /Dz. U. Nr 63, poz. 303/.

3. Procedura wydawania koncesji i zezwoleń

Dotychczas jedynym organem ustawowo upoważnionym do wydawania zezwoleń telekomunikacyjnych był Minister Łączności. Na podstawie upoważnienia zawartego w decyzji nr 8 Ministra Łączności z dnia 18 lutego 1994 r. w sprawie upoważnienia Państwowej Agencji Radiokomunikacyjnej do wydawania zezwoleń i wykonywania innych czynności i zadań z zakresu administracji państwowej /Dz. Urz. Ministerstwa Łączności Nr 1, poz. 3/ takie zezwolenia dotyczące zakładania i używania określonych urządzeń radiokomunikacyjnych oraz wewnętrznych sieci radiokomunikacyjnych otrzymała PAR. Obecnie nowe brzmienie art. 14 ustawy o łączności przewiduje, że wydawanie omawianych koncesji należy do Ministra Łączności, a wydawanie zezwoleń nie tylko do tego naczelnego organu administracji państwowej ale również do PAR w zakresie określonym

przez Ministra Łączności. Stanowi to niewątpliwie swego rodzaju dowartościowanie PAR kosztem pewnego ograniczenia kompetencji Ministra Łączności.3/

Omawiane kompetencje odnoszą się nie tylko do wydania koncesji lub zezwolenia ale również do odmowy ich wydania i cofnięcia, jak również do ewentualnego ograniczenia przedmiotu, zakresu lub obszaru działalności. To ostatnie sformułowanie o możliwości ograniczenia przedmiotu, zakresu lub obszaru działalności stanowi istotne novum wzorowane na postanowieniach ustawy z dnia 23 grudnia 1988 r. o działalności gospodarczej /Dz. U. Nr 41, poz. 324 ze zmianami/.

Każde takie rozstrzygnięcie musi nastąpić w drodze decyzji administracyjnej. W tym zakresie nowelizacja nie wprowadza żadnej zmiany do ustawy o łączności z 1990 r. Mamy więc tutaj do czynienia z tzw. ogólnym postępowaniem administracyjnym, które jest unormowane w dziale I, II i IX kodeksu postępowania administracyjnego z dnia 14 czerwca 1960 r. /tekst jednolity Dz. U. z 1980 r. Nr 9, poz. 26 ze zmianami/. Przepisy tego kodeksu są więc stosowane w omawianym zakresie, chyba że w samej ustawie o łączności są zawarte w danej kwestii przepisy szczególne.4/

Wydanie koncesji lub zezwolenia następuje na pisemny wniosek podmiotu występującego o tego rodzaju decyzję administracyjną. Nowością jest, że po zmianach ustawa o łączności będzie wreszcie szczegółowo określać, jakie wymagania musi spełniać taki wniosek. Dotychczas te podstawowe kwestie w ogóle nie były unormowane w ustawie o łączności, co w konsekwencji powodowało wiele dowolności w postępowaniu o wydanie zezwolenia oraz konflikty w stosunkach z wnioskodawcami.5/

Zgodnie z nowym brzmieniem art. 14 ust. 3 ustawy o łączności pisemny wniosek o wydanie koncesji lub zezwolenia powinien zawierać w szczególności oznaczenie wnioskodawcy i jego siedziby, określenie przedmiotu działalności i obszaru działania oraz przewidywaną datę rozpoczęcia działalnosci. Oczywiście takim wnioskodawcą może być również osoba fizyczna i wówczas należałoby podać jej miejsce zamieszkania. Wskazane informacje stanowią minimum danych, które powinien w swym wniosku sformułować wnioskodawca. Niewątpliwie może on we wniosku lub załączonych doń dokumentach podać szereg innych informacji, które jego zdaniem mają znaczenie dla rozstrzygnięcia sprawy. Najczęściej tak zresztą było dotychczas i tym bardziej będzie w przyszłości.

Ważną nowością jest przyznanie Ministrowi Łączności kompetencji do żądania od wnioskodawcy dodatkowych dokumentów istotnych dla sprawy wydania koncesji lub zezwolenia. Ta możliwość dotyczy przedstawienia w wyznaczonym terminie składu kapitałowego wnioskodawcy oraz dokumentów i informacji mogących uprawdopodobnić, że spełni on warunki, które zostaną określone w koncesji lub zezwoleniu, oraz wynikające z odrębnych przepisów. Tym samym zostają stworzone podstawy prawne weryfikacji potencjalnych możliwości wnioskodawcy spełnienia wskazanych warunków.6/

Dodatkowo organ koncesyjny będzie mógł teraz uzależnić wydanie

koncesji od złożenia zabezpieczenia majątkowego roszczeń osob trzecich do wnioskodawcy z tytułu prowadzenia działalności gospodarczej. Jest to rozwiązanie wzorowane na postanowieniach art. 20 ust. 4a powołanej ustawy o działalności gospodarczej z 1988 r. Rada Ministrów została przy tym upoważniona do określenia w drodze rozporządzenia sposobu realizacji owej czynności zabezpieczającej. Wymowę tej regulacji ustawowej znacznie zmniejsza jednak fakt, że analogiczne rozporządzenie Rady Ministrów przewidziane przez ustawę o działalności gospodarczej nie zostało do dzisiaj wydane. Uzasadnione wydają się więc obawy co do wydania w nieodległej przyszłości na podstawie art. 14 ust. 6 ustawy o łączności wskazanego rozporządzenia.

Jeszcze więcej wątpliwości w zakresie procedury wydawania koncesji na świadczenie usług telekomunikacyjnych wywołują dodane w ostatniej chwili ustalenia art. 14a ustawy o łączności, przewidujące jako zasadę przeprowadzenie przetargu w celu wyboru podmiotu, któremu zostanie wydana koncesja. Minister będzie mógł odstąpić od przetargu tylko w 2 sytuacjach: gdy po odpowiednim ogłoszeniu prasowym do przetargu zgłosi się mniej niż dwóch zainteresowanych, spełniających warunki do otrzymania koncesji, bądź gdy o koncesję na świadczenie usług na danym obszarze wystąpi podmiot, który otrzymał już zezwolenie na zakładanie lub używanie urządzeń przeznaczonych do świadczenia tych usług na tym obszarze. Tej treści tzw. wniosek mniejszości został przegłosowany prawie jednomyślnie, bo 342 głosami przy zaledwie 5 przeciwnych i 8 wstrzymujących się.7/ Nastąpiło to w skądinąd słusznym przekonaniu, że przetarg jest najlepszą metodą przeciwdziałania korupcji i dowolności przy przyznawaniu koncesji. Jednakże nie zawsze ta właśnie metoda prowadzi ostatecznie do najlepszych rezultatów: jest ona dosyć kosztowna, długotrwała, w drobnych sprawach wręcz zbędna i może powodować, że ktoś, kto ma jakiś nowy pomysł na świadczenie określonych usług telekomunikacyjnych, straci go na rzecz innego uczestnika przetargu. Wydaje się więc, że znacznie lepszym rozwiązaniem była odrzucona propozycja przewidująca możliwość zarządzenia przez Ministra Łączności przeprowadzenia przetargu w celu wyboru podmiotu, któremu wyda koncesję. Zamiast możliwości wprowadzono obowiązek ogłaszania przetargów, chociaż nikt nie przemyślał do końca skutków tej zmiany dla procedury wydawania koncesji na świadczenie usług telekomunikacyjnych.

4. Treść koncesji lub zezwolenia

W porównaniu z dotychczasowym brzmieniem art. 17 ustawy o łączności zmiany co do treści koncesji lub zezwolenia sprowadzają się przede wszystkim do ustawowego przesądzenia koniecznych składników tego rodzaju decyzji oraz wyznaczenia takich danych, które mogą lecz nie zawsze muszą znaleźć się w niej. Do pierwszej grupy należy określenie osoby upoważnionej i jej siedziby, przedmiotu, zakresu i obszaru wykonywanej działalności, daty rozpoczęcia działalności oraz czasu trwania koncesji lub zezwolenia. Poza tym w każdej koncesji powinien być określony sposób wykonywania obowiązków na rzecz bezpieczeństwa i

obronności państwa. Jest to niewątpliwie istotne novum.

W zależności od konkretnego przypadku w koncesji i zezwoleniu mogą być ponadto określone warunki wykonywania działalności /tj. w szczególności co do formy świadczenia usług, wymagań technicznych dotyczących urządzeń telekomunikacyjnych, rodzaju i rozmiaru sieci telekomunikacyjnej/, założenia i warunki współpracy z sieciami telekomunikacyjnymi użytku publicznego, podstawowe parametry techniczne, przyznane numeracje, częstotliwości i zakresy częstotliwości oraz techniczne warunki ich wykorzystania, sygnały identyfikacyjne, znaki wywoławcze, sposoby uiszczania opłat za udzielenie koncesji oraz za używanie linii, urządzeń lub sieci telekomunikacyjnej, zasady działania w razie klęsk żywiołowych, jak również skład kapitałowy podmiotu, któremu została wydana koncesja lub zezwolenie. Poza tym w zezwoleniu może być określony sposób wykonywania obowiązków na rzecz bezpieczeństwa i obronności państwa. Osobnego podkreślenia wymaga, że obecnie będą mogły być w koncesji lub zezwoleniu nałożone obowiązki w zakresie informowania Ministra Łączności o przypadkach posiadania ponad 10 % akcji, udziałów lub praw z udziałów w podmiotach posiadających koncesje lub zezwolenia, a także co do występowania w takich sytuacjach o stosowną zgodę Ministra Łączności. Oczywiście nie będzie to dotyczyło wszystkich podmiotów otrzymujących koncesje i zezwolenia.

5. Zakazy i ograniczenia w zakresie wydawania koncesji i zezwoleń

Chociaż oficjalnie zaostrzenie zakazów i ograniczeń w zakresie wydawania koncesji i zezwoleń na działalność w dziedzinie telekomunikacji nie było celem omawianej nowelizacji ustawy o łączności, to jednak ostateczny rezultat tej noweli uwzględniający zmiany dokonane w toku prac komisji sejmowych jawi się jako zdecydowanie restrykcyjny. Brak czasu i miejsca nie pozwala na pełną analizę przypadków tych restrykcyjnych zmian. Toteż z konieczności zostaną wskazane tylko najważniejsze płaszczyzny, w których one występują. I tak przykładów takich dostarcza nowe, niezmiernie skomplikowane brzmienie art. 16 ustawy o łączności. W konsekwencji będzie teraz znacznie więcej takich sytuacji, gdy podmiotowi zagranicznemu lub spółce z udziałem podmiotów zagranicznych nie będzie można wydać koncesji lub zezwolenia na działalność w dziedzinie telekomunikacji. Restrykcje poszły tutaj - przy utrzymaniu jako zasady maksimum 33 % lub 49 % udziału podmiotów zagranicznych w kapitale zakładowym lub akcyjnym spółki - zwłaszcza w kierunku ograniczenia członkostwa obywateli obcych w zarządach i radach nadzorczych spółek oraz dopuszczalnej liczby głosów podmiotów zagranicznych i podmiotów kontrolowanych przez podmioty zagraniczne w zgromadzeniu wspólników lub walnym zgromadzeniu akcjonariuszy.

Drugą płaszczyznę, w której przejawiają się omawiane tendencje restrykcyjne, stanowią sytuacje odmowy wydania koncesji lub zezwolenia określone w art. 18 ustawy o łączności. Obecnie podstawę prawną takiej odmowy będzie mogło stanowić także m.in. zagrożenie interesu gospodarki narodowej czy brak rękojmii

należytego wykonywania działalności. Sa to pojęcia nader ogólne, przejęte z ustawy o działalności gospodarczej, które niewątpliwie będą mogły być różnie interpretowane. Należy więc zgodzić się ze zdaniem A. Kemplińskiego o celowości wydania przez Trybunał Konstytucyjny orzeczenia uściślającego zakres tych pojęć będących podstawą wydawania negatywnych decyzji administracyjnych co do podjęcia określonego rodzaju działalności gospodarczej.8/

Trzecią płaszczyzną restrykcyjnych nowych ustaleń ustawy o łączności są przypadki cofnięcia koncesji lub zezwolenia ujęte w nowym brzmieniu art. 19 tej ustawy. Celem tych unormowań było wyeliminowanie możliwości odsprzedawania koncesji podmiotom zagranicznym lub omijania zapisów omawianej ustawy przy pomocy fikcyjnych podmiotów.9/ Z takim uzasadnieniem wskazanych ustaleń trzeba się generalnie zgodzić, co oczywiście nie zmienia ich restrykcyjnego charakteru.

6. Dostosowanie wydanych zezwoleń telekomunikacyjnych do zmian ustawy o łączności

Wydane do czasu wejścia w życie nowelizacji ustawy o łączności zezwolenia telekomunikacyjne będą w większości w pewnym zakresie pozostawać w sprzeczności z nowymi regulacjami ustawowymi dotyczącymi koncesji i zezwoleń na działalność w dziedzinie telekomunikacji. Toteż Minister Łączności został zobowiązany do dostosowania tych zezwoleń do obowiązującego brzmienia przepisów ustawy o łączności. Powinno to nastąpić w terminie dwóch lat od dnia wejścia w życie ustawy o zmianie ustawy o łączności oraz niektórych innych ustaw. Jest to okres wystarczająco długi, żeby w tym czasie bez zbędnego pośpiechu i dezorganizacji funkcjonowania podmiotów, które prowadzą działalność na podstawie takich zezwoleń, dokonać odpowiednich zmian dostosowujących.

Przypisy:

1/ Zob. Diariusz Sejmowy z 47. posiedzenia w dniu 21 kwietnia 1995 r., Warszawa 1995, s. 6 oraz załącznik nr 1 zawierający wyniki głosowania nr 12.
2/ R. Długołęcka, A. Żytowiecka: Polskie prawo w dziedzinie telekomunikacji a wymogi Wspólnot Europejskich, Warszawa 1994, s. 65.
3/ Por. J. Gospodarek: Aspekty prawne wydawania zezwoleń telekomunikacyjnych /Praca zlecona przez Ministerstwo Łączności/, Warszawa grudzień 1991, s. 6.
4/ Zob. tamże, s. 14 i nast.
5/ J. Gospodarek: Remont po czterech latach, Świat Telekomunikacji nr 2/1994, s. 10.
6/ Zob. uzasadnienie rządowego projektu zmiany ustawy o łączności oraz niektórych innych ustaw, druk sejmowy nr 863, s. 15.
7/ Zob. cyt. Diariusz Sejmowy, s. 6 oraz załącznik zawierający wyniki głosowania nr 10.
8/ A. Kempliński: Prawo do podjęcia negatywnej decyzji administracyjnej - udzielenia koncesji lub zezwolenia na prowadzenie działalności gospodarczej, Przegląd Ustwodawstwa Gospodarczego nr 12/1994, s. 15.

9/ Zob. uzasadnienie rządowego projektu zmiany ustawy o łączności oraz niektórych innych ustaw, druk sejmowy nr 863, s. 17.

Bezpieczeństwo w sieci NASK

Krzysztof Silicki

Naukowa i Akademicka Sieć Komputerowa prowadzi zdefiniowaną politykę bezpieczeństwa sieci stawiającą jako główny cel zapewnienie niezawodnej pracy sieci na odpowiednim poziomie wynikającym z Regulaminu Świadczenia Usług przez NASK. Niezawodność pracy sieci należy w tym wypadku rozumieć w sposób bardzo szeroki. Zarówno bowiem aspekty związane z bezawaryjnością sprzętu jak i apekty związane z ochroną przed nieuprawnionym dostępem są tematem i przedmiotem działań w zakresie bezpieczeństwa sieci. Na niezawodność wpływa więc poziom świadczenia wszelkich usług na rzecz abonenta. Zarówno więc awaria routera czy atak hackera zaburzając normalną dostępność usług gwarantowanych abonentowi jest przedmiotem troski polityki bezpieczeństwa sieci NASK.

Należy jednak już na wstępie zaznaczyć ,iż NASK jako operator nie ma prawa i możliwości klasyfikowania informacji przesyłanych w sieci NASK przez jej abonentów. Każdy użytkownik jest odpowiedzialny za przedsięwzięcie stosownych środków ostrożności (np. szyfrowania wiadomości) w zależności od istoty i wagi wiadomości. Rolą operatora natomiast jest niejako przezroczyste przesłanie wiadomości powierzonej - od nadawcy do odbiorcy. NASK na życzenie użytkownika może jednak zaproponować zastosowanie odpowiednich rozwiązań techniczno-organizacyjnych dla zapewnienia transmisji o podwyższonych walorach bezpieczeństwa.

Program Bezpieczeństwa Sieci NASK

Problematyka bezpieczeństwa uzyskała w NASK wysoką rangę. We wspomnianyn już Regulaminie Świadczenia Usług przez NASK jeden z rozdziałów jest w całości poświęcony ochronie sieci NASK natomiast w wielu innych miejscach znajdujemy punkty związane z problematyką bezpieczeństwa. Każdy abonent NASK otrzymuje egzemplarz regulaminu wraz z umową.

Zarządzeniem Dyrekcji został powołany zespół koordynujący realizowanie polityki bezpieczeństwa sieci NASK, w skład którego obok przedstwaicieli Dyrekcji wchodzą specjaliści NASK, członkowie Zespołu Ochrony Sieci oraz mogą być zapraszani eksperci z zewnątrz. NASK korzysta m.in z ekspertyz specjalistow z zewnątrz służących zdefiniowaniu aspektów prawnych, organizacyjnych, technicznych i innych związanych z problematyką bezpieczeństwa w sieci. Przykładem jest tu współpraca z Wyższą Szkołą Oficerską Wojsk Łączności. Z zewnętrznych opracowań wynika m.in, iż prace prowadzone w NASK w dziedzinie bezpieczeństwa sieci są niejednokrotnie pionierskie w skali kraju. I tak powstał w NASK pakiet dokumentów nazwany Programem Bezpieczeństwa Sieci NASK, którego dokument główny został zatwierdzony przez Dyrekcję jako oficjalny zapis polityki bezpieczeństwa. Dokument ten powstał zgodnie z regułami obowiązującymi przy opracowywaniu tzw. security policy - szeroko na świecie stosowanej przez poważne organizacje formy zapisu reguł i zadań do zrealizowania na poziomie całej organizacji i poszczególnych wycinków działalności.

Program bezpieczenstwa zakłada, iż każdy z pracowników ale też i użytkowników (abonentów) ma wpływ na bezpieczeństwo pracy w sieci a konsekwencje zaniedbania reguł właściwego postępowania są trudne do przecenienia. Hierarchiczny układ Programu, w którym dokument główny obejmując całościowo problematykę uzyskuje dopełnienie w dokumentach związanych (np. instrukcjach, zaleceniach itp.) wyraża się jednocześnie w tym, iż każdy z dokumentów jest adresowany do odpowiedniej grupy osób w zależności od rodzaju wykonywanej przez nich pracy.

Program bezpieczeństwa sieci zakłada mówiąc ogólnie projektowanie, wdrażanie, utrzymanie i rozwój systemu bezpieczeństwa sieci NASK we wszelkich związanych z tą problematyką aspektach.
Reguły bezpieczeństwa sieci mogą dotyczyć całej organizacji, określonej lokalizacji, oraz zastosowanego systemu komputerowego (lub technologii). Dokument ogólny zajmuje się bezpieczeństwem na poziomie całej organizacji. Dokumenty szczegółowe opisują reguły specyficzne dla określonych lokalizacji i systemów komputerowych.

Bezpieczeństwo sieci zależy od dwóch kardynalnych aspektów: fizycznego i technicznego. Aspekt techniczny wymaga zastosowania odpowiednich rozwiązań technicznych ochrony sieci. Aspekt fizyczny jest ściśle związany z:

- świadomością potrzeby i obowiązku bezpiecznego operowania zasobami sieci przez wszystkich użytkowników (niezależnie od posiadanych uprawnień) ,
- ochroną fizyczną dostępu do sieci,
- ochroną fizyczną nośników informacji (kopie zapasowe, dokumentacja).

Program Bezpieczeństwa Sieci NASK obejmuje zagadnienia związane z:

- zaplanowaniem,
- zaprojektowaniem,
- zaimplementowaniem,
- zarządzaniem

systemu bezpieczeństwa sieci NASK.
Powiązaniem obu aspektów jest aspekt organizacyjny - również obecny w Programie.

NASK jest rozległą siecią międzymiastową oraz miejską siecią w Warszawie, która pracuje w oparciu o łącza własne lub dzierżawione od innych operatorów bądź. Do urządzeń sieci NASK należą głównie urządzenia specjalistyczne wyposażenia łączy jak: modemy, routery, węzły , switche, huby oraz serwery ale także sprzęt komputerowy powszechnego użytku do obsługi pracy NASK.Urządzenia specjalistyczne w węzłach NASK są urządzeniami podlegającymi specjalnej ochronie ze względu na swą kluczową rolę w niezawodnej pracy sieci.

Wysoki założony poziom niezawodności sieci powoduje, że podstawowym zagrożeniem jest nierealizowanie usługi dla abonenta (brak połączenia fizycznego, brak połączenia logicznego).
Zagrożenia dla prawidłowej pracy sieci mogą wynikać z:

- przerwania linii na poziomie łącza fizycznego,
- problemów konfiguracyjnych (administrowanie ciągłe)
- problemów z oprogramowaniem działającym na urządzeniach
- awarią sprzętu należącego do NASK,
- ataków intruzów,

- katastrof (zniszczenia sprzętu)

Czynników powodujących zagrożenia dla normalnej pracy użytkownika w sieci jest niesłychanie wiele. Tym ważniejsze jest ciągłe inwentaryzowanie możliwych niebezpieczeństw i bieżące przeciwdziałanie.

Częstokroć przywoływanymi zagrożeniami są np. ataki intruzów czyli próby sforsowania zabezpieczeń sieci i wdarcia się w obszary niedozwolone. Wśród sposobów ataku można wymienić:

- atak na zbiory z hasłami użytkowników,
- wirusy, konie trjańskie itp,
- wykorzystanie dostępu przez publiczne sieci w celu dokonania prób ataku,
- nielegalne dołączenie się do sieci (np. podszywanie się).

Mówiąc więc o atakach intruzów trzeba mieć świadomość, iż praktycznie każda sieć lokalna abonenta dołączona do sieci NASK może stwarzać potencjalne zagrożenie dla bezpieczeństwa - tym trudniejsze do oszacowania, iż nie jest to obszar administrowania przez NASK. Nielegalne stacje w sieciach abonentów lub niekontrolowane konta użytkowników - jeśli istnieją- stanowią poważna groźbę dla całego organizmu sieci rozległej NASK. Częstokroć do jednego konta ma dostęp wiele osób co jest przeciwko zasadom bezpieczeństwa podobnie jak odstępowanie uprawnień (związanych z konkretnym identyfikatorem) innym osobom co jest sprzeczne z Regulaminem NASK.

Dokumenty programu bezpieczeństwa zawierają zatem reguły, procedury, zakresy odpowiedzialności, wskazówki dla pracowników NASK tak aby zdefiniować zadania stojące przed pracownikami w celu zapewnienia założonego poziomu bezpieczeństwa sieci NASK. Program bezpieczeństwa ma też na celu wypracowanie standardów dla całej organizacji w aspekcie bezpieczeństwa (np. dotyczących elektronicznej korespondencji czy archiwizowania)

Bezpieczny system rządzi się kilkoma zasadami:

- ścisłym zdefiniowaniem uprawnień użytkowników do zasobów w sieci
- związaną z powyższym zasadą niedostępności danych określonych kategorii dla nieuprawnionych użytkowników.
- zapewnieniem integralności danych (konfiguracyjnych lub użytkownika) - czyli zabezpieczeniem przed nieuprawnionymi zmianami,
- zapewnieniem dostępności danych i usług zgodnie z założonym poziomem niezawodności usług,
- kontrolą dostępu do zasobów i pomieszczeń,
- zdolnością oceny stanu bezpieczeństwa systemu

Wszystkie zbiory konfiguracyjne (np. serwerów, routerów, węzłów) są traktowane jako "specjalnie chronione" i podlegają specjalnej ochronie. Informacje zakwalifikowane jako "poufne" są przesyłane (dostępne) poprzez sieć tylko w postaci zaszyfrowanej.

Strumienie danych płynące w liniach NASK nie są domyślnie szyfrowane na poziomie łącza. Jest kwestią aplikacji użytkownika zastosowanie szyfracji w przypadkach koniecznych z punktu widzenia abonenta. W drodze indywidualnych uzgodnień jest możliwe zapewnienie przez NASK dodatkowej ochrony strumieniom danych abonenta.

Strumienie danych różnych abonentów i ich sieci (o różnych protokołach) są "wymieszane" w sieci szkieletowej NASK.

Na wszelkich serwerach, gateway'ach, routerach itp. jeśli istnieją techniczne możliwości są uruchomione mechanizmy rozłączające sesję użytkownika (time-out) w przypadku nieaktywności ponad pewien dopuszczalny czas. Jest to w interesie innych abonentów aby nie blokować dostępu do sieci. Są również zaimplementowane mechanizmy zabezpieczające przed "przechwytywaniem" (celowym lub nieświadomym) sesji innego abonenta.

Wszelkie zasoby zgromadzone na komputerach NASK muszą być regularnie poddawane archiwizacji . Każde urządzenie dyskowe podlega planowi archiwizacji zasobów realizowanemu przez administratrującego danym urządzeniem. Urządzenia te mają opisany harmonogram i procedurę archiwizacji gdzie podane są podstawowe dane (typ urządzenia archiwizującego, oznaczenia pustych i zapisanych nośników oraz miejsce przechowywania kopii zapasowych). Kopie zapasowe przechowywane są w zamkniętych sejfach w odległości gwarantującej maksymalne bezpieczeństwo a także założony czas odtworzenia.

Zaplanowana i przestrzegana kontrola dostępu jest kardynalnym wymogiem ochrony. Obejmuje ona:

- przyznawanie użytkownikom takich praw do zasobów jakie są wymagane do prawidłowego wykonywania ich pracy lecz nie więcej niż jest to wymagane.
- przestrzeganie zasady , iż dostęp do pomieszczeń jest możliwy jedynie dla osób do tego uprawnionych .

Aby system był bezpieczny muszą istnieć metody i procedury uzyskiwania danych o zdarzeniach w sieci. W chwili obecnej jest wdrażanay system informowania abonentów o zdarzeniach typu awaryjnego, który docelowo będzie obejmował wszystkich abonentów oraz system przesyłania informacji o problemach abonentów dotyczących korzystania z usług sieci NASK.

Zdarzenia w sieci NASK są rejestrowane i zapamiętywane w celu późniejszego ich wykorzystania.

Program Bezpieczeństwa Sieci NASK przewiduje także dokonywanie okresowych przeglądów stanu bezpieczeństwa (tzw. audits) wg. schematów dostosowanych do jednostki takiej jak NASK, w których to przeglądach dokonuje się analizy działania wszelkich parametrów mających wpływ na bezpieczeństwo a więc np.:

- elementów umownych (umowy międzyoperatorskie, umowy serwisowe, gwarancyjne itp),
- elementów organizacyjnych (np. funkcjonowanie systemu reagowania na zdarzenia, gromadzenia pamiętników zdarzeń)
- elementów technicznych (przegląd stanu bezpieczeństwa urządzeń)
- innych (wszelkie nowo pojawiające się aspekty)

konsekwencją czego powstają konkretne propozycje usprawnienia systemu.

Bezpieczna poczta elektroniczna

W NASKu funkcjonuje tzw. bezpieczna poczta elektroniczna wg. Internetowej normy PEM (Privacy Enhanced Mail). Jest to system pocztowy działający w sieci Internet na poziomie aplikacji użytkownika powstały - w wyniku świadomości braku zabezpieczeń w poczcie elektronicznej standardu SMTP - na zamówienie NASK. W systemie pocztowym PEM-HEART zastosowano nowoczesne metody kryptograficzne pozwalające np. na szyfrowanie treści wiadomości oraz tzw. podpis elektroniczny (cyfrowy).

Potrzeba zastosowania tego typu systemu jest oczywista jeśli mamy świadomość, że zwykła poczta internetowa jest narażona na szereg ataków, (które nota bene nie są li tylko teoretycznymi możliwościami lecz w niezbyt trudny sposób intruz jest w stanie je zastosować) sprawiających, że nigdy nie ma pewności, iż :

-dany list pochodzi od tego nadawcy, który się pod korespondencją podpisał (nawet adres nadawcy widniejący w nagłówku nie może być dowodem),
- treść listu nie została przeczytana przez osobę trzecią,
- treść listu nie została zmodyfikowana (przypadkowo lub intencjonalnie).

Specyfikacja standardu poczty elektronicznej w sieciach typu Internet, opisana w dokumencie RFC 822, zawiera wprawdzie opcjonalne pole ENCRYPTED w nagłówku wiadomości, które pozwala sprecyzować nazwę (zarejestrowany w Network Information Centre identyfikator) programu użytego do szyfrowania i wskazać użyty klucz. To podejście nie uzyskało jednak popularności i IESG, ciało odpowiedzialne za normalizację protokołów w Internecie, podj ęł o decyzj ę o opracowaniu odrębnego protokołu zabezpieczania informacji przesyłanych pocztą elektroniczną , jednakowego dla wszystkich zainteresowanych użytkowników Internetu. Pierwsza wersja specyfikacji takiego protokoł u pojawiła się w 1987 roku w dokumencie RFC 989. Kolejne modyfikacje i rozszerzenia tego protokołu by y publikowane w dokumentach RFC 1040, RFC 1113-1115. Aktualna wersja, zamieszczona w dokumentach RFC 1421-1424 .

PEM-HEART realizuje nastę puj ące usługi ochrony informacji:

- poufność
- kontrola integralności wiadomości
- uwierzytelnienie
- niezaprzeczalność nadania wiadomości (podpis cyfrowy)

Jedn z wa niejszych cech PEM-a jest to, że jego realizacja nie wymaga żadnej ingerencji w wewnętrzne mechanizmy poczty elektronicznej sieci Internet. Oznacza to, że oprogramowanie realizuj ce usługi bezpiecznej poczty jest uruchamiane na poziomie aplikacji użytkownika.

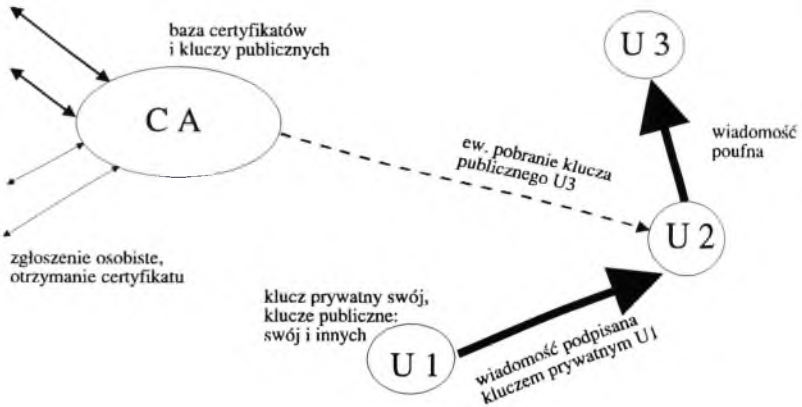
Tak więc w łatwy sposób można wykorzystywać popularne programy obsługi poczty elektronicznej takie jak ELM czy PINE. Użytkownicy nie muszą więc zmieniać swych przyzwyczajeń wkładając jednak minimum wysiłku w użytkowanie dodatkowych funkcji jakie daje PEM. Co więcej w normie PEM realizacja usług ochrony informacji nie jest związana z żadną platformą sprzętową ani programową. Oznacza to, że implementacje PEM-a mogą być uruchamiane na dowolnym komputerze z dowolnym systemem operacyjnym (np. IBM PC). Otwiera to również drogę do wykorzystania w PEM-ie sprzętowych realizacji niektórych algorytmów np. DES-a, RSA czy generatora liczb losowych.

Od strony kryptograficznej norma (a więc także implementacja działająca w NASK) ma następujące cechy: podpis cyfrowy realizowany jest za pomoc algorytmu RSA o długości

klucza od 512 do 1024 bitów, natomiast szyfrowanie odbywa się za pomoc DES-a. Zarządzanie kluczami zrealizowano w oparciu o certyfikaty kluczy wystawiane przez urzędy do spraw certyfikatów (ang. certification authority).

Użytkownicy zgłaszają się do tzw. urzędu ds. certyfikatów (który de facto składa się z obsługi komputera PC z odpowiednim oprogramowaniem) i otrzymują parę kluczy : prywatny i publiczny a także certyfikat stwierdzający autentyczność klucza publicznego. Klucze i certyfikat są w istocie zbiorami binarnymi na dyskietce użytkownika. Klucz prywatny użytkownika podlega specjalnej ochronie - to jest zadanie samego użytkownika. Klucz publiczny jest zawarty w certyfikacie i podlega szerokiemu rozprzestrzenieniu wśród użytkowników bezpiecznej poczty bez obawy utraty bezpieczeństwa. Kiedy użytkownikowi U1 zależy aby wysłać do U2 wiadomość o treści jawnej lecz opatrzonej jego (U1) podpisem (oczywiście elektronicznym) używa swego klucza prywatnego do obliczenia podpisu, który potem jest dołączany do wiadomości. U2 weryfikuje nadawcę wiadomości używając klucza publicznego U1, który otrzymał w postaci certyfikatu np. z bazy danych urzędu (ang. Certification Authority).

Mechanizmy szyfrowania asymetrycznego i klucza publicznego

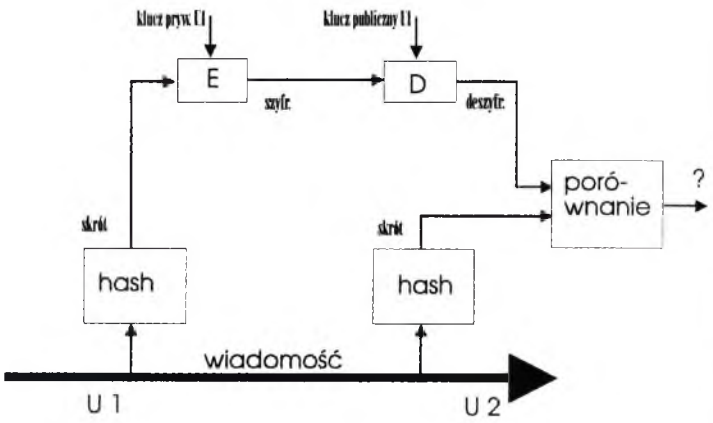


C A -urząd d/s certyfikatów
U1, U2, U3 - użytkownicy

Mechanizm działania podpisu cyfrowego jest przedstawiony na kolejnym rysunku. U1 a właściwie oprogramowanie pakietu PEM-HEART dokonuje skrótu wiadomości za pomocą specjalnej funkcji matematycznej (ang. hash function) , która następnie jest szyfrowana. U2 dokonuje:

- deszyfracji przy pomocy klucza publicznego U1,
- obliczenia skrótu przychodzącej wiadomości za pomocą tej samej funkcji hash,
- porównania obliczonego skrótu ze skrótem otrzymanym (po zdeszyfrowaniu) od U1.

Podpis elektroniczny (cyfrowy)



U 1, U 2 - użytkownicy

Jeśli wynik porównania jest ujemny nie jest wskazane traktować otrzymanej wiadomości jako wiarygodnej.

Tu ujawnia się pewna przewaga podpisu elektronicznego nad podpisem ręcznym : podpis elektroniczny nie tylko uwierzytelnia nadacę wiadomości ale jest także strażnikiem integralności treści wiadomości tzn. że jeśli choćby jeden bit w treści wiadomości ulegnie zmianie weryfikacja podpisu będzie ujemna.

Kiedy zaś np. użytkownik U2 zechce wysłać wiadomość poufną (tzn. zaszyfrowaną) do użytkownika U3 posłuży się jego (U3) kluczem publicznym zawartym w certyfikacie, który może otrzymać bezpośrednio od U3 lub pobrać z bazy. U3 z kolei odszyfruje wiadomość posługując się sobie jedynie znanym kluczem prywatnym (nikt inny nie jest w stanie odczytać tak zaszyfrowanej wiadomości do czasu kiedy klucz prywatny U3 jest dobrze strzeżony).

Tak skonstruowany system nazuwa się systemem klucza publicznego lub asymertycznym. Urząd ds. certyfikatów jest gwarancją, że dany certyfikat jest autentyczny. Certyfikaty są praktycznie niepodrabialne.

W NASK urząd ds. certyfikatów podlega ostremu reżimowi opisanemu w regulaminie urzędu i innych instrukcjach, każdy użytkownik otrzymuje też regulamin przeznaczony dla uczestnika bezpiecznej poczty.

Zarządzanie

System bezpieczeństwa opiera się na zarządzaniu. Zarządzanie także jest postrzegane w sposób szeroki i dotyczy zarządzania siecią w oparciu o wykorzystywane oprogramowanie ale także bieżące zarządzanie wyposażeniem sieci (inwentaryzacja ciągła) oraz zarządzanie w szerszym kontekście rozumianyn jako opieka nad Programem Bezpieczeństwa a więc chociażby bieżące ewaluacje stanu bezpieczeństwa posczególnych urządzeń, stosowanie upgradów oprogramowania poprawiających bezpieczeństwo itd.

Zarządzanie siecią NASK jest przeprowadzane centralnie z jednego miejsca zarówno w przypadku Internetu jak X.25 a także Frame Relay. W przypadku Internetu stosowany jest system SNMP i oprogramowanie Cisco Works na bazie SUNnet Managera. System zarządzania rejestruje zdarzenia w sieci (np. zmiany stanu linii transmisyjnych, zmiany konfiguracji routerów). Konfiguracje routerów gromadzone są też w centralnej bazie. System pozwala także na:

-monitorowanie podstawowych parametrów urządzeń ,
- ustawianie pułapek informujących centrum o przekroczeniu określonej wartości danego parametru w zarządzanym urządzeniu,
- zdalne konfigurowanie urządzeń,
- prowadzenie statystyk natężenia ruchu na najważniejszych liniach.

Oprócz oprogramowania firmowego specjaliści NASK stosują wiele narzędzi (skryptów) wspomagających zarządzanie siecią i informowanie o stanie sieci pod wybranym kątem.

NASK jest w trakcie dokonywania upgrade'u oprogramowania zarządzającego do wersji spełniającej standard SNMP v2 co podniesie bezpieczeństwo zarządzania syetmem. SNMP v2 definiuje bowiem (i jest to nowość w stosunku do wersji 1) dwa protokoły związane z bezpieczeństwem:

- realizujący usługę uwierzytelnienia ale także kontrolę integralności Digest Authentication Protocol (DAP),
- realizujący usługę poufności Symmetric Privacy Protocol.

Kontrola integralności obsługiwana przez DAP oznacza sprawdzenie, czy informacja dotarła w nie zmienionej postaci do adresata. DAP posługuje się mechanizmem skrótu wiadomości, który obliczany jest przy pomocy standardowej funkcji matematycznej MD-5. Skrót dołączany jest do wiadomości i służy do weryfikacji po stronie odbiorczej. Przy pomocy tajnego klucza znanego jedynie nadawcy i odbiorcy dokonywane także jest uwierzytelnienie nadawcy (czy jest tym za kogo się podaje).

Drugi z protokołów zapewniający z kolei poufność to symetryczny algorytm szyfrujący DES.

Wspomniane mechanizmy bezpieczeństwa dotyczą oczywiście wszelkich zapytań i zleceń jakie są przesyłane siecią pomiędzy zarządzanymi urządzeniami a centrum.

Ważną częścią bezpieczeństwa całego systemu pracującej sieci NASK są także bazy danych samego sprzętu uzupełniane na bieżąco w procesie ciągłej inwentaryzacji. Trudno bowiem zarządzać siecią nie mając bieżącej pełnej informacji czyli:

- wszelkich danych o zainstalowanych urządzeniach,

- danych na temat lokalizacji sprzętu, osób odpowiedzialnych, adresów, telefonów itp,
- innych danych związanych z gospodarką środkami trwałymi.

W codziennej pracy specjaliści NASK korzystają z dostępnych informacji jakie generują światowe centra doradcze w zakresie bezpieczeństwa sieci Internet (np. CERT) oraz stosują półautomatyczne metody ewaluacji bezpieczeństwa ssystemów komputerowych (sprawdzone i rekomendowane pakiety -np. COPS)

NASK jest obecnie w trakcie realizacji programu wyposażenia urządzeń sieci szkieletowej (routerów) w mechanizmy kryptograficzne uwierzytelnienia dostępu oraz przesyłania a także opcjonalnego szyfrowania transmisji.

O pewnych problemach Autentyzacji i Autoryzacji we współczesnych sieciach

Piotr WOLSKI, Tadeusz SZUSZKIEWICZ,
Lesław MACHARZYŃSKI

Autentyzacja w uproszczeniu pozwala administratorowi sieci odgrodzić się od osób niepożądanych umożliwiając zarazem normalne funkcjonowanie tym, którzy mają do tego prawo; zwykle czyni się to przy użyciu haseł, ale jest to wysoce nieskuteczne. Hasła można łatwo odgadnąć lub wejść w ich posiadanie. Nawet dysponowanie pojedynczym hasłem (administratora) można naruszyć integralność sieci.

Jednokrotne hasła generowane przez inteligentne karty autentyzacyjne (ang. token) IKA weryfikowane na serwerze sieci są rozwiązaniem bezpieczniejszym. IKA są zwykle wielkości karty kredytowej. Generacja jednokrotnego hasła oraz funkcjonowanie IKA są oparte na dwóch podstawowych zasadach:

1. Synchronizacja czasu (ang. Time synchronization),
2. Pytanie - odpowiedź (ang. Challange -responze).

Autoryzacja to realizacja ustalonych przez administratora sieci zasad udostępniania zasobów użytkownikom.

Bezpieczne jednokrotne logowanie (ang. secure single sign-on) oznacza, że użytkownik po pojedyńczym zalogowaniu ma dostęp do tego, do czego powinien, w ramach wszystkich przyznanych zasobów w całej sieci. Ogólnie systemy autoryzacji bazują na złożonych pakietach softwarowych, instalowanych na wszystkich komputerach zabezpieczonych w sieci. Jednym z najbardziej znanych jest KERBEROS sprzedawany w różnych wariantach. Podstawowym problemem jest dostosowanie procedur logowania do poszczególnych platform softwarowych.

Z systemem autoryzacji łączy się użycie IKA . Popularne stają się produkty bazujące na IKA. Jest to bardziej bezpieczne niż prosty system haseł i bardziej wygodne niż inne rozwiązania typu np. DNA print. IKA mogą służyć do weryfikacji użytkowników w systemach "diał - up", sieciach LAN lub w INTERNECIE, czy systemach FAX. IKA generują hasło przekazywane do systemu weryfikacji punktów dostępu do sieci. Serwer autentyzacji weryfikuje hasło umożliwiając logowanie użytkownika . Serwerem autentyzacji może być wydzielone urządzenie - router, dedykowany komputer pod systemem UNIX lub innej platformy pakiet softwarowy na serwerze, bądź inaczej, zwykle w zależności od tego, ilu użytkowników ma obejmować system. Szczegóły realizacji mechanizmów autentyzacji zależą od producenta. Najbardziej popularna technika to opracowana przez Security Dynamic synchronizacja czasowa. Przykładami są : KERBEROS, IBM-owski NetSP, ICL Lan Manager.

Synchronizacja czasowa polega na algorytmie i kluczu 64-bitowym do generowania liczby losowej co minutę, przy czym czas może być zmieniany przez administratora sieci. Każdy użytkownik ma przydzielony unikalny Klucz pamiętany w IKA, jak i w bazie danych serwera autentyzacji. W czasie próby logowania użytkownik podaje cztero-cyfrowy osobisty numer identyfikacyjny (ang. PIN), a następnie sześcio-cyfrową liczbę wygenerowaną przez IKA. PIN określa serwerowi, jakiego tajnego klucza użyć. Serwer znajduje odpowiedni klucz, wykonuje

algorytm i sprawdza, czy otrzymana (wygenerowana) liczba jest taka sama, jak podana przez użytkownika. W wypadku zgodności następuje logowanie.

Pytanie - odpowiedź jest innym schematem bazującym na DES-ie. Gdy użytkownik próbuje się logować serwer autentyzacji wysyła liczbę losową. IKA szyfruje tę liczbę przy użyciu tajnego klucza użytkownika i wysyła z powrotem do serwera autentyzacji. Identyczny algorytm jest wykonywany na serwerze, a rezultaty porównywanie.

Podstawowym problemem w synchronizacji czasowej jest synchronizacja czasu na IKA, zwłaszcza o ile IKA mają być używane przez kilka lat. Stosowana może być metoda kompensacji powstających rozbieżności czasu. Zastrzeżenie może budzić fakt ważności hasła przez okres do 60 sek, co teoretycznie jest czasem, który może wystarczać hackerowi włamanie do sieci po przechwyceniu hasła. Mechanizm "pytanie - odpowiedź" wymaga użycia komputera po obu stronach.

Metoda "Synchronizacji - czasu " może być użyta przy wykorzystaniu "ślepych" terminali Faxów, a także "poczty głosem", "voice mail" - spr. konta w banku.

Metoda "pytanie - odpowiedź" daje szersze możliwości implementacji. Np. może być w pełni zautomatyzowana poprzez włączenie odpowiednich urządzeń do PC w miejsce stacji dyskowych, co też jest dyskusyjne, ponieważ użytkownicy mogą je zostawiać w stacji po zakończeniu pracy.

Metoda "synchronizacji - czasu " wymaga wprowadzenia 10-ciu cyfr, zaś metoda "pytanie - odpowiedź" jest jednak bardziej uciążliwa ponieważ użytkownik musi podać do IKA np. w przypadku łączy "dial up" liczbę losową, a potem rezultat szyfracji, a niekiedy musi się ponownie logować do serwera. Nawet w przypadku softwarowych IKA, programów wykonywanych na PC-cie lub laptopie, jest wiele opinii, że proces logowania jest zbyt wolny i zbyt uciążliwy. Problem stanowi także połączenie serwerów komunikacyjnych z serwerem autentyzacji. Metoda "pytanie - odpowiedź" umożliwia zwykle samodzielne konfigurowanie IKA. Jest to oczywiście dodatkowa praca , ale wtedy tylko administrator, poza użytkownikiem, ma dostęp do klucza. Metody inicjalizacji IKA są różne w zależności od dostawcy, niekiedy np. Security - Dynamic inicjacja jest fabryczna. Problemem jest także wymiana baterii w IKA, (koszt około 100$ na stanowisko, na wymianę i rekonfigurację bazy). Synchronizacja bazy i IKA w przypadku dużej sieci stanowi problem bywa kosztowna. Z drugiej strony stosowanie tego typu mechanizmów w małych sieciach jest niecelowe. Zwykle przyjmuje się jako granicę sieć powyżej 500 stanowisk (użytkowników).

Autoryzacja.

Są dwie podstawowe architektury bazujące na serwerze i stacjach roboczych (stacji roboczej). Metoda na serwerze polega na tym, że serwer kontroluje co użytkownikowi może być udostępnione. Metoda stacji roboczej polega na tym, iż stacja kontroluje co użytkownikowi może być udostępnione. Przykładami rozwiązań dla metody na serwerze jest KERBEROS, IBM-owski NetSP i ICL Access Manager. Przykładami rozwiązań dla metody na stacji roboczej jest SSO/DACS (Secure Sign On/Data Access Control System). W tym przypadku same stacje robocze muszą być chronione. Niezależnie od sposobu rozwiązań celem jest, przy pojedyńczym (jednokrotnym) logowaniu, dostęp do wszystkich zasobów sieci do których użytkownik jest upoważniony. System autoryzacji wymaga szczególnej ochrony haseł użytkownika. Dlatego też

systemy autoryzacji powinny być łączone z systemami autentyzacji. Aplikacje muszą być odpowiednio dostosowane, aby mogły się komunikować z procesem autoryzacji. W większości stosowanych aplikacji, z uwagi na brak dostępu do kodu źródłowego, nie da się tego zrobić.
Dla kerberosa, o ile użytkownik dysponuje kodem źródłowym, tak zwana " kerberyzacja aplikacji " nie stanowi na ogół problemu. Jak narazie aplikacje w postaci kerberyzowanej nie są jaszcze powszechnie dostępne.

Jedną z rzeczy, która wyróżnia NetSP od Kerberosa jest fakt szerokiego wspierania aplikacji szczególnie pod NetWare Novell. Należy oczekiwać, że coraz więcej produktów będzie wyposażone w tzw. GSS-API to jest (generic security service- application program interface), specyfikacja rozwinięta przez X-OPEN i zaaprobowana przez IETF (Internet Engineeri Task Force). Specyfikacja jest podana w RFC (Request for Comment) 1503 - 1509.

Poblemy ochrony kryptograficznej informacji przetwarzanych i przekazywanych we współczesnych sieciach informatycznych i systemach komputerowych.

1. Ochrona kryptograficzna przestaje być domeną wojska i "służb".

2. Konieczność kodowania masowych danych zarówno w systemach łączności, sieciach informatycznych i systemach komputerowych.

3. Konieczność standaryzacji w skali globalnej (konieczność standaryzacji wynika z masowości).

Uzasadnienie :

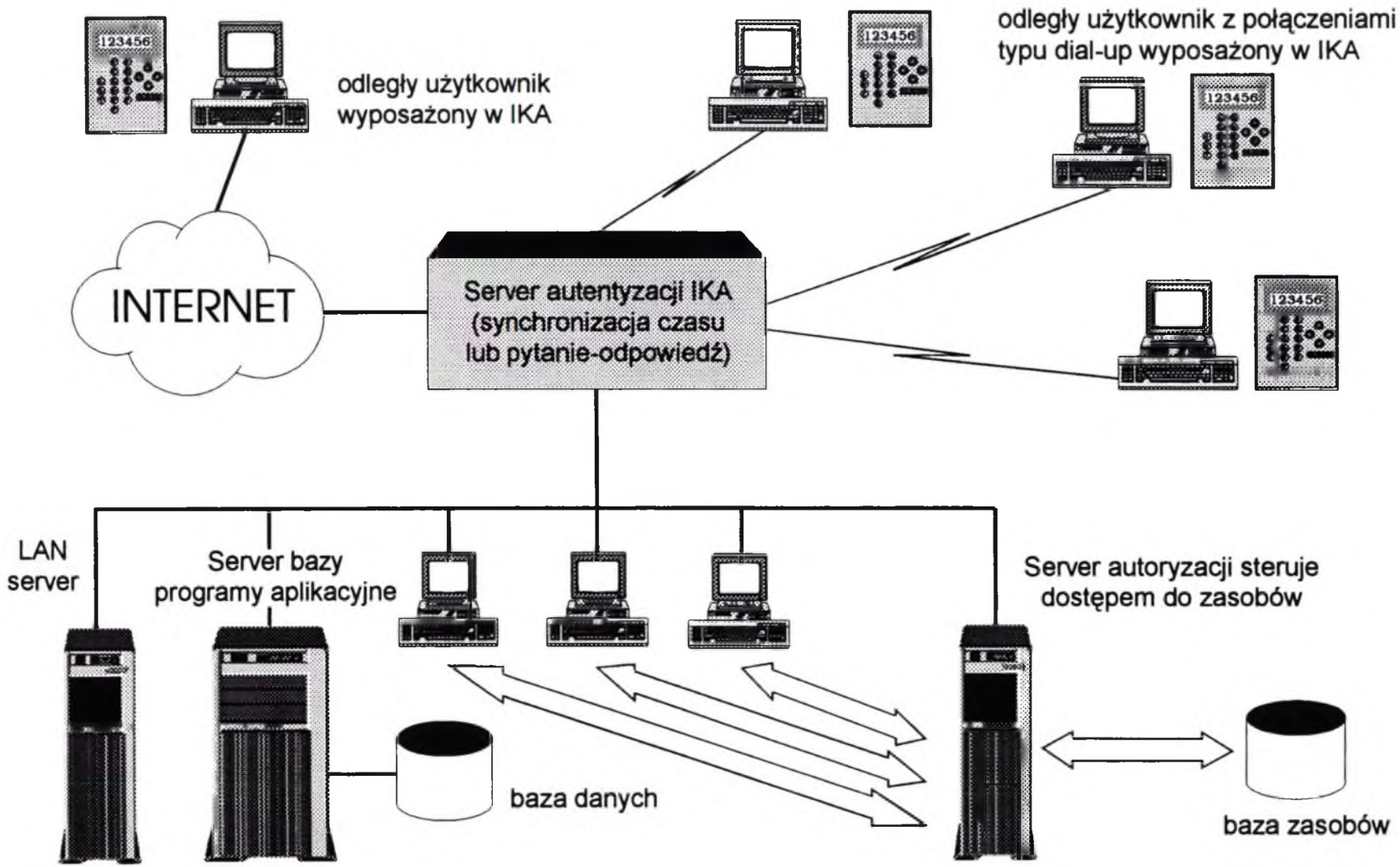
- Tradycyjne systemy kryptograficzne dotyczyły zwykle krótkiej informacji tekstowej;
- Obecnie coraz powszechniejsze stają się systemy multimedialne z pojemnościami rzędu Gigabajtów;
- Stosowanie kryptografii w biznesie, medycynie, bankach z nowymi zagadnieniami takimi jak : ochrona prywatności, elektroniczny pieniądz; to zapewnienie bezpieczeństwa informacji w Europie oraz na skalę międzynarodową, tam gdzie to możliwe.
- Dystrybucja kluczy musi być efektywna na skalę masową, kierunek ten reprezentuje np. RSA, musi istnieć identyfikacja nadawcy i odbiorcy;

- Współczesna rola kryptografii to :

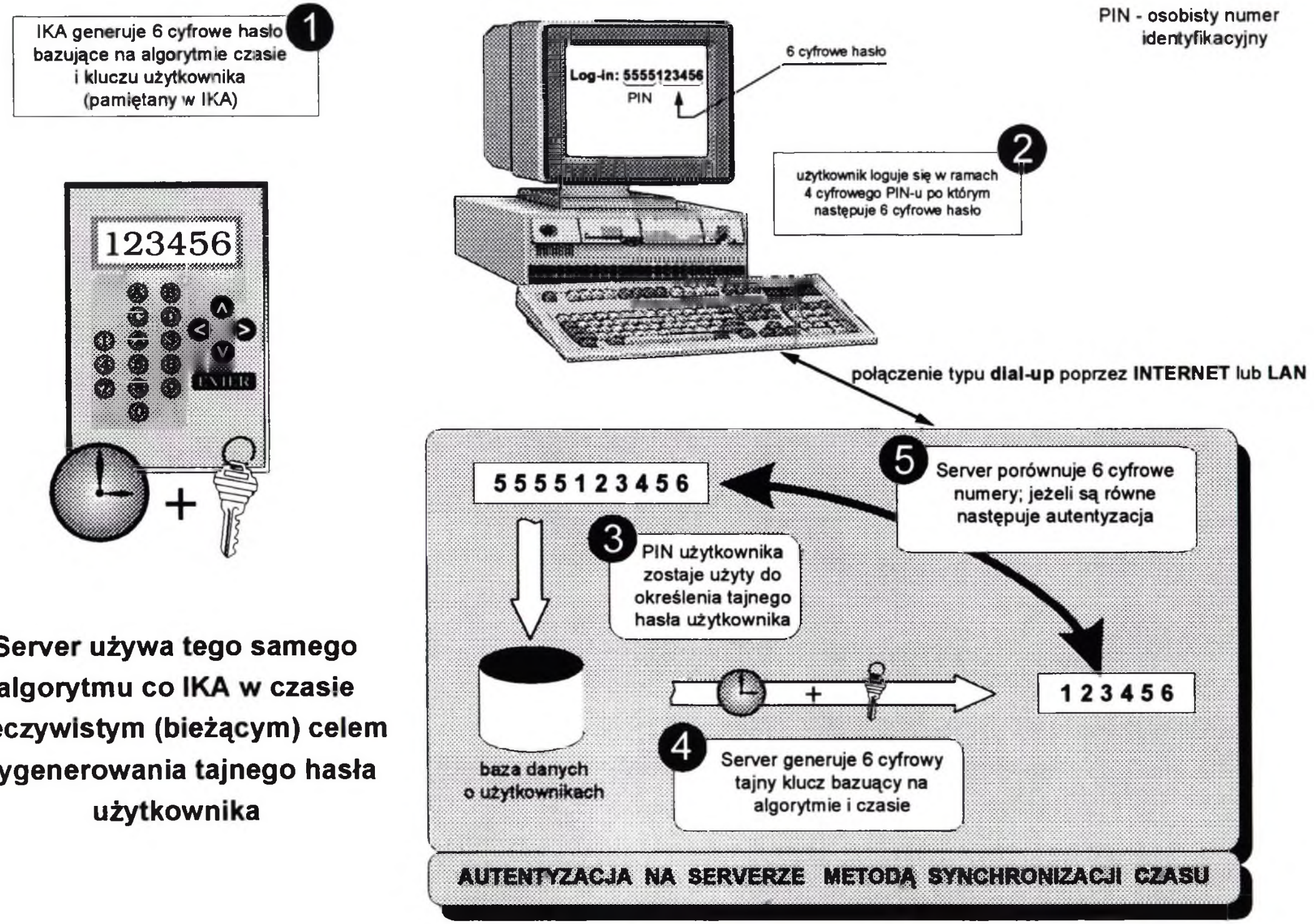
I autentyzacja nadawcy i odbiorcy
II zapewnienie niezmienności informacji
III tradycyjna ochrona tajności i poufności.

Realizacja: możliwa jedynie poprzez " SECURITY ON SILICON ".
Układy produkowane masowo; np. program szwajcarski IDEA, czy amerykański z kontrolą kluczy znany pod nazwą " CLIPER CHIP ".
Potrzeba standaryzacji i dopasowania się do świata nie oznacza rezygnacji z tożsamości narodowej, a więc z troski o narodowy interes; przykład w Ameryce " Pomarańczowa Księga ", w Niemczech " Zielona ", a mając na uwadze nasze tradycje być może Książka " Biało - Czerwona ".

Autentyzacja z użyciem IKA do generowania jednokrotnych haseł weryfikowanych na serwerze ochrony pozwala odciąć dostęp do sieci osobom niepożądanym Autentyzacja zaś to sposób w jaki administrator sieci może sterować jakie zasoby komputera i na jakiej zasadzie udostępniać. Systemy autentyzacji powinny być stosowane łącznie z systemami autoryzacji

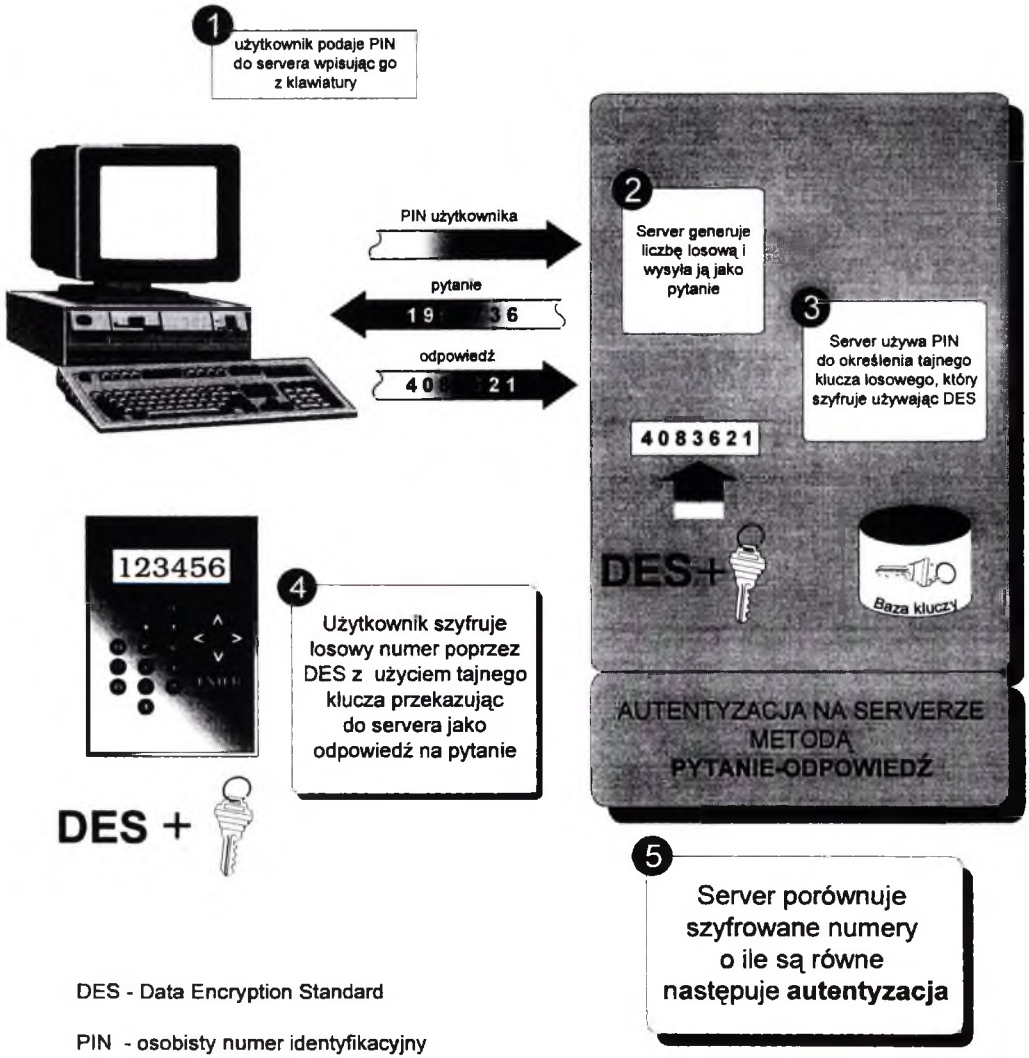


AUTENTYZACJA METODĄ SYNCHRONIZACJI CZASU



Server używa tego samego algorytmu co IKA w czasie rzeczywistym (bieżącym) celem wygenerowania tajnego hasła użytkownika

AUTENTYZACJA METODĄ PYTANIE-ODPOWIEDŹ



DES - Data Encryption Standard

PIN - osobisty numer identyfikacyjny

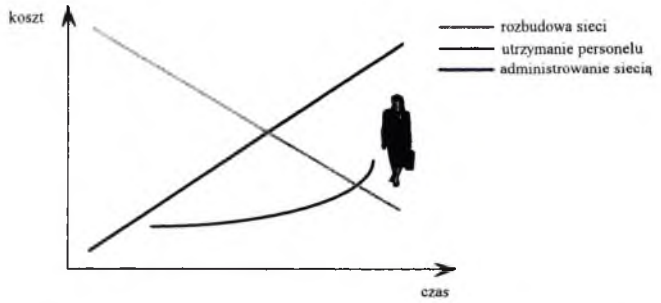
PORÓWNANIE PLATFORM ZARZĄDZAJĄCYCH SunNet Manager i HP OpenView

Waldemar E. Grzebyk, Jarosław M. Janukiewicz, Tomasz Banyś[*)]

Naukowa i Akademicka Sieć Komputerowa
Zakład Telekomunikacji
50-327 Wrocław, ul. Janiszewskiego 7/9, tel./fax: 219529

1.Wprowadzenie

Jednym z podstawowych problemów utrzymania sieci komputerowej jest jej administrowanie. Każda sieć komputerowa na pewnym etapie rozwoju i eksploatacji wymaga od operatora rzeczywistej organizacji zarządzania. Zarządzanie siecią składa się z dwóch podstawowych elementów: zarządzania systemem komunikacyjnym i systemami operacyjnymi. Dla administratorów sieci lokalnych LAN (ang. Local Area Network) najistotniejszym elementem jest zarządzanie systemami operacyjnymi dla operatorów sieci miejskich MAN (ang. Metropolitan Area Network) i rozległych WAN (ang. Wide Area Network) zarządzanie systemem komunikacyjnym. Wraz z rozwojem sieci koszty jej rozbudowy maleją, ilość personelu potrzebna do obsługi sieci i koszty administrowania siecią rosną (Rysunek 1). Czy tzw. „platformy zarządzające" NMP (ang. Network Menagement Platform) są w stanie wpłynąć na zmniejszenie tempa wzrostu kosztów administrowania siecią ?. Chyba tak. NMP napewno nie rozwiązują wszystkich problemów związanych z administrowaniem siecią. Mogą natomiast stanowić pomocne narzędzie do wspomagania procesu zarządzania.



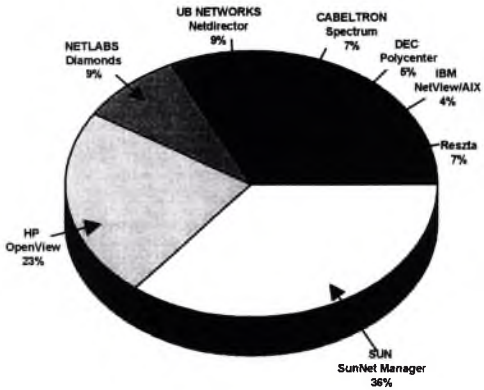
Rysunek 1. Tendencje w rozkładzie kosztów eksploatacji i rozbudowy sieci

Jednym z kryteriów klasyfikacji platform zarządzających przyjmowany jest system operacyjny w jakim pracują: Unix i Windows. Platformy Unix-owe są znacznie droższe i są dedykowane dla administratorów dużych sieci heterogenicznych MAN lub WAN, którzy potrzebują integracji zarządzania wieloma protokołami. Wybór odpowiedniej platformy zależy od charakteru zarządzanego środowiska:

[*)] Instytut Telekomunikacji i Akustyki Politechniki Wrocławskiej

- rodzaju i ilości urządzeń;
- oprogramowania systemowego urządzeń;
- stosowanych w sieci protokołów komunikacyjnych.

W artykule skupiono się na porównaniu platform Unix-owych a ściślej mówiąc dwóch które w roku ubiegłym wg. IDC (ang. International Data Corporation) posiadały 59% rynku platform zarządzających (Rysunek 2): SunNet Manager firmy SunConnect i HP OpenView firmy Hewlett Packard.



Rysunek 2. Podział rynku platform zarządzających sieci Uinx-owych w 1994 (wg.IDC)

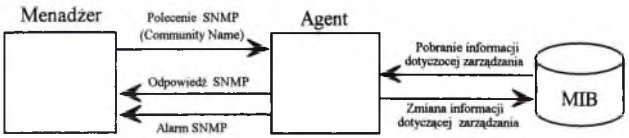
2. Ogólna zasada działania platform zarządzających

Idealnym rozwiązaniem w administrowaniu siecią byłby taki system zarządzania, przy pomocy którego operator korzystając z jednej stacji roboczej mógłby kontrolować wszystkie zasoby sieci. Platforma do zarządzania (ang. Network Menagement Platform) może być podstawą takiego systemu. Nowoczesne platformy do zarządzania oferują wspólne środowisko dla integracji aplikacji realizujących różne aspekty zarządzania, z których jedne służą do obsługi urządzeń sieciowych a inne wykonują funkcje administracyjne takie jak kontrola urządzeń czy obsługa awarii sieci. Umożliwiają one korzystanie ze wspólnych danych o sieci komputerowej a zarazem wymianę informacji pomiędzy poszczególnymi aplikacjami. Platforma zapewnia zbiór funkcji oferowanych dla aplikacji API (ang. Application Programming Interface).

Działanie platform zarządzających opiera się na architekturze klient/serwer. Przez klienta rozumiemy stacje zarządzające (ang. management station). Serwer dostarczający informacji o stanie urządzeń nazywany jest agentem. Węzeł sieci komputerowej może spełniać obydwie funkcje.

Menedżer zainstalowany w stacji zarządzającej wysyła zapytania i polecenia adresowane do poszczególnych agentów. Gromadzi informacje niezbędne dla procesu zarządzania. Agent jest pośrednikiem pomiędzy poszczególnymi urządzeniami i menedżerem (Rysunek 3). Komunikacja pomiędzy menedżerem i agentem jest realizowana poprzez protokół SNMP (ang. Simple Network Management Protocol). Protokół SNMP został stworzony do zarządzania sieciami

TCP/IP. Pozwala na monitorowanie różnych urządzeń za pomocą specjalnej bazy danych MIB (ang. Management Information Base).



Rysunek 3. Komunikacja pomiędzy menedżerem i agentem poprzez protokół SNMP

3. Kryteria porównawcze platform zarządzających

Analiza porównawcza platform zarządzających prezentowana w artykule została przeprowadzona na dwa sposoby. Pierwsze porównanie wykonano w oparciu o dokumentację dostarczaną przez producenta, drugie porównanie jest wynikiem doświadczeń zebranych podczas eksploatacji systemów zarządzania we Wrocławskiej Akademickiej Sieci Komputerowej (WASK).

Wykorzystując dokumentację dostarczaną przez producentów dokonano porównania platform zarządzających według następujących kryteriów:

1. Konfiguracja platformy zarządzającej;
2. Interfejsy do programu użytkownika APIs;
3. Współpraca z siecią (zakres realizowanych funkcji, obsługa protokołów sieciowych);
4. Właściwości interfejsu użytkownika.

W oparciu o doświadczenia zebrane podczas eksploatacji systemów zarządzania dokonano porównania platform zarządzających według następujących kryteriów:

1. Praca wielu niezależnych administratorów;
2. Baza danych systemu zarządzania;
3. Automatyczne odpytywanie urządzeń - synchronizacja bazy danych z aktualnym stanem sieci;
4. Organizacja menu;
5. Reprezentacja graficzna elementów sieci;
6. Okna;
7. Dostępność podstawowych operacji protokołu SNMP z linii komend systemu UNIX;
8. Reprezentacja i dostęp do obiektów baz MIB;
9. System wspomagania użytkownika;
10. Inne właściwości.

4. Porównanie platform zarządzających

Porównano dwie platformy SunNet Manager 2.0 firmy SunConnect (SNM) i OpenView SNMP Menagment Platform z aplikacją Network Node Menager firmy Hewlett Packard (HP OpenView) wykorzystywane do zarządzania siecią kręgosłupową WASK we Wrocławiu. W pierwszym zestawieniu (Tabela 1) zamieszczono ogólne dane o porównywanych platformach. Tabela 2 zawiera porównanie parametrów technicznych w oparciu o dane katalogowe.

Tabela 1

Produkt (platforma zarządzająca)	**Platforma sprzętowa i systemowa**	**Popularne aplikacje na platformę zarządzającą**
SunNet Manager 2.0	- Sun Sparc z SunOS	- SunOptics Optivity (SynOptics Communications), - CiscoWorks (Cisco Systems)
OpenView SNMP Menagment Platform z aplikacją Network Node Menager	- HP 900 serii 300, 400, 700 z HP-UX, - Sun Sparc z SunOS	- SunOptics Optivity (SynOptics Communications), - CiscoWorks (Cisco Systems),

Tabela 2

	SNM	**HP OpenView**
1. Konfiguracja platformy zarządzającej		
Wybór sposobu selekcji alarmów	W	W
Selekcja monitorowanych zdarzeń	W	W
Edytowanie filtrów	N	W
2. Interfejsy do programu użytkownika APIs		
Do bazy danych	W	W
Do tworzenia aplikacji zintegrowanych z systemem	W	W
Do opisu stosowanej bazy danych	O	W
Do zarządzania poprzez „proxy" agentów	W	W
3. Współpraca z siecią (zakres realizowanych funkcji, obsługa protokołów sieciowych):		
IP:		
- SNMP:		
• MIB I, MIB II	W	W
• RMON	O	D
• MIB kompilator/zarządca	O	W
• „przeglądarka" bazy MIB	O	W
• automatyczne wyszukiwanie urządzeń z SNMP	W	W
- automatyczne wyszukiwanie urządzeń bez SNMP (ping)	W	D/O
NetWare/IPX:		
- automatyczne wyszukiwanie serwerów	O	D
- automatyczne wyszukiwanie węzłów sieci	O	D
- diagnostyka IPX	O	D
AppleTalk	O	N
NetBEUI	W	O
Vines/IP	W	O
SNA	W/O	D
DECnet	W	O
Diagnostyka pakietów:		
- dekodowanie pakietów	D	O
- analiza pakietów	D	O

gdzie: W - Wbudowane w podstawową wersję pakietu platformy zarządzającej;
D - Dołączane za dodatkową opłatą przez producenta;
O - Oferowane jako dodatkowe opcje przez innych producentów;
N - Nie implementowane.

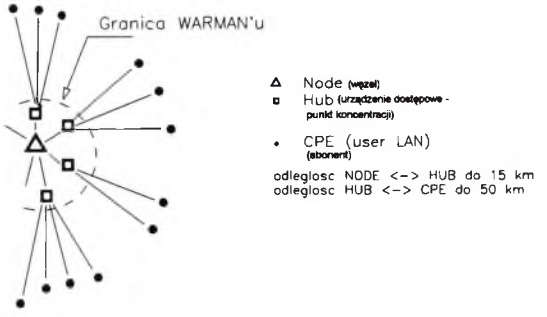
WARMAN - doświadczenia eksploatacji

Maciej Kozłowski, Roman Adamiec

Informacje ogólne

Budowana w Warszawie metropolitalna sieć komputerowa WARMAN ma objąć swoim zasięgiem wszystkie dzielnice Warszawy, tak by umożliwić dostęp do sieci placówkom naukowym i akademickim oraz innym abonentom, w tym administracji państwowej. Formalną podstawą do jej budowy jest porozumienie środowiskowe, podpisane przez rektorów pięciu największych uczelni Warszawy, Prezesa Polskiej Akademii Nauk i Prezesa Państwowej Agencji Atomistyki, działających w imieniu ponad 200 ulokowanych w Warszawie placówek naukowych i akademickich. Sygnatariusze porozumienia powołali 10-osobową Radę Użytkowników, która opiniuje działania prowadzone w zakresie budowy i eksploatacji sieci (a także w zakresie funkcjonowania centrów superkomputerowych w Uniwersytecie Warszawskim i Politechnice Warszawskiej). Wyznaczyli także NASK j.b.r. jako jednostkę wiodącą, tzn. prowadzącą budowę i eksploatację sieci. Ten tryb powołania NASK j.b.r. jako wykonawcy i administratora przedsięwzięcia nie umniejsza jego prawa do zawierania porozumień z innymi podmiotami w zakresie budowy i eksploatacji sieci.

Szkielet sieci sieci bazuje na 10 węzłach oraz ponad 20 punktach koncentracji dołączonych do tych węzłów. Punkty koncentracji stanowią zestawy urządzeń, realizujących wymagane w danym rejonie funkcje. Idea struktury węzła została przedstawiona na rys. 1.



1

Technologia

W wyniku trójstopniowego konkursu na dostawę technologii i urządzeń dla sieci WARMAN zdecydowano o wyborze technologii ATM (Asynchronous Transfer Mode). Decyzję tę podjęto przy pełnej świadomości, że technologia ATM nie jest jeszcze ostatecznie wystandaryzowana, a rozwiązania firmowe różnych producentów nie zawsze są dopracowane na tyle, by gwarantować realizacje różnorodnych możliwości, które ta technologia przynosi, czy też ma przynieść w przyszłości. Rozważenie wariantów alternatywnych pokazało, że w każdym przypadku należy przewidzieć migrację rozwiązań - od rozwiązania wstępnego ku rozwiązaniu docelowemu, zaś wiele okoliczności wskazywało, że rozwiązaniem docelowym stanie się ATM. Wybrano więc migrację najprostszą - od ATM w postaci tylko częściowo wystandaryzowanej do pełnego standardu w przyszłości. Oczywiście, taka ewolucja rozwiązań jest możliwa tylko przy gwarancjach dostawcy odnośnie wymiany urządzeń w miarę rozwoju technologii ATM; niezbędna jest zatem długofalowa współpraca z dostawcą technologii.

1 lipca 1994 r. zawarto kontrakt z firmą Schrack Ericsson na dostawę urządzeń i technologii dla sieci WARMAN. W szkielecie sieci zastosowano urządzenia firmy General DataComm (GDC).

W pierwszej połowie sierpnia 1994 r. do Warszawy została dostarczona instalacja pilotowa ATM, składająca się z trzech switchów GDC APEX DV2. Posłużyła ona do zapoznania się z technologią ATM oraz do wstępnego przeszkolenia podstawowej kadry technicznej. Część tej instalacji była prezentowana w ramach ekspozycji towarzyszącej seminariun NASK Miedzeszyn'94.

W grudniu 1994 r. i styczniu 1995 r. nastąpiła dostawa urządzeń eksploatacyjnych. Urządzenia te są sukcesywnie testowane i instalowane na docelowych stanowiskach.

Komunikacja pomiędzy węzłami, a także pomiędzy węzłami i koncentratorami sieci odbywa się na dedykowanych liniach światłowodowych z szybkością 155 Mbps w oparciu o protokoł SDH/STM-1. Protokołem sieciowym, obejmującym switche i koncentratory, jest ATM.

Technologia ATM umożliwia, przy wykorzystaniu tej samej struktury fizycznych połączeń szkieletu sieci, stworzenie wirtualnych sieci logicznych, rozłącznych z punktu wudzenia zarządzania i dostępu do zasobów. Np. mogą to być sieci wirtualne uczelni, administracji państwowej oraz innych abonentów. Do chwili przygotowania niniejszego opracowania możliwości te zostały przetestowane laboratoryjnie, lecz nie zostały jeszcze zrealizowane eksploatacyjnie.

technologii ATM umożliwia także, przy wykorzystaniu tej samej struktury fizycznych połączeń szkieletu sieci, stworzenie wirtualnych sieci logicznych, rozłącznych z punktu widzenia zarządzania, dostępu do zasobów itd, dla różnych podmiotów. Np. mogą to być sieci wirtualne uczelni, administracji państwowej oraz innych abonentów.

Technologia ATM umożliwia także przekazywanie obrazu i głosu na potrzeby wideokonferencji oraz łączenie central telefonicznych. Przeprowadzone dotychczas testy i eksperymenty wykazują pełną przydatność urządzeń WARMANu do tych celów.

17 stycznia 1995 r. nastąpiło przekazanie do eksploatacji pierwszej linii ATM na trasie Politechnika Warszawska - Uniwersytet Warszawski (Krakowskie Przedmieście). począwszy od kwietnia 1995 r. są uruchamiane następne linie transmisyjne ATM.

Zgodnie z projektem oraz przyjętym harmonogramem, w pierwszej połowie 1995 r. nastąpi uruchomienie sześciu węzłów:

- UW - Krak. Przedmieście (uruchomiony),
- PW - Pl. Politechniki 1 (uruchomiony),
- Zgrupowanie naukowe Ochota
- SGGW
- CUP - Żurawia 4 - termin do uzgodnienia (światłowód został zainstalowany)
- URM - do uzgodnienia (j.w.),

Planowane jest także uruchomienie punktów koncentracji w CRiT przy ul. Barbary 2, Centrali Telefonicznej przy ul. Pięknej oraz PKiN.

Węzły planowane w drugiej połowie tego roku, to:

- Wola - Instytuty PAN przy ul. Kasprzaka,
- Mokotów - Instytut Fizyki w Al. Lotników,
- Praga - prawdopodobnie Instytut Transportu Samochodowego,ul. Jagiellońska,
- Żoliborz - IMGW i/lub Instytuty przy ul. Rydygiera.

Ponadto wykorzystując fakt położenia "na drodze" naszej inwestycji obiektów administracji państwowej, infrastruktura światłowodowa została wprowadzona do:

- Ministerstwa Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa,
- Ministerstwa Łączności,
- Ministerstwa Transportu,
- Ministerstwa Finansów,
- GUSu.

Planowane w bieżącym roku jest uwzględnienie także Komitetu Badań Naukowych.

Warman jest dołączony do sieci szkieletowej NASK za pomocą łącza o przepustowości 2 Mbps; planuje się uruchomienie drugiego takiego łącza w drugiej połowie 1995 r.

Ponieważ WARMAN jest jednym z przedsięwzięć realizowanych przez NASK, dziedziczy on usługi oferowane dotychczas przez NASK na terenie Warszawy. W pierwszym etapie następuje relokacja użytkowników w ramach nowo uruchomionej struktury. W drugiej kolejności następuje przyłączanie nowych użytkowników.

Z punktu widzenia podłączenia użytkownika (a dokładniej sieci użytkownika - abonenta) istotne są następujące informacje:

- położenie najbliższego punktu koncentracji (urządzeń dostępowych),
- wybór technologii podłączenia (światłowodów, kabel dedykowany,...)
- protokół i interface wymagany w punkcie koncentracji WARMANA,
- wymagane urządzenia, np. modemy, konwertery, itp

Podłączenie abonenta (użytkownika) następuje po zawarciu z nim umowy. Przedmiot umowy podlega wycenie, stosownie do cennika NASK'u. Należy zauważyć, że z użytkownikami naukowymi i akademickimi są również zawierane regulamie umowy finansowe. Jednostki naukowe i akademickie mogą uzyskac zwolnienie od wniesienia opłat, w zależności od wysokości funduszy przekazanych w danym roku przez Komitet Badań naukowych na utrzymanie sieci w ruchu oraz amortyzację jej urządzeń.

Z punktu widzenia abonenta WARMAN oferuje trzy typy podłączeń:

- pomiędzy prywatnymi sieciami LAN abonenta,
- przyłączenie sieci LAN użytkownika do sieci WARMAN
- przyłączenie indywidualnego użytkownika do sieci WARMAN.

Cennik WARMANu rozróżnia również abonentów świadczących usługi na rzecz osób trzecich.

Charakterystyka urządzeń w sieci WARMAN

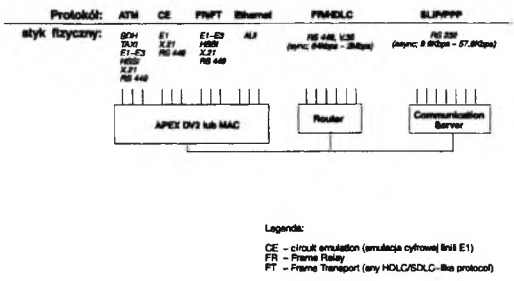
Podstawową strukturę węzłów stanowią *switche* GDC APEX-DV2 firmy General DataComm.

Dostępne są następujące styki fizyczne:

- E1 - styk cyfrowy G703 o szybkości 2.048 Mbps, dwa porty na karcie,
- E2 - styk cyfrowy G703 o szybkości 8.448 Mbps, dwa porty na karcie,
- E3 - styk cyfrowy G703 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.

Na rys. 2 przedstawiono w sposób syntetyczny możliwości dołączania urządzeń użytkownika punktu koncentracji WARMANA.



Rys. 2

Odwołując się do powyższego zestawienia oraz rys. 2, zauważmy, że abonent może podłączyć się do sieci WARMAN wykorzystując różnorodne protokoły oraz nośniki w zależności od swoich potrzeb (aplikacji). Przykładowo, abonent, który dysponuje komputerami z aplikacjami typu videokonferencja oraz kartami sieciowym z protokołem ATM, powinien wykorzystać też taki sposób włączenia się do sieci WARMAN. Synchroniczne styki szeregowe X.21, RS449, HSSI i cyfrowe E1, E2, E3 dają szerokie możliwości optymalnego doboru podłączenia sieci odległej, wykorzystując protokoły transportowe HDLC, Frame Relay. Styk typu CE - Circuit Emulation - daje ponadto możliwość podłączenia centrali telefonicznej z wykorzystaniem kanału cyfrowego E1. Z kolei asynchroniczne styki szeregowe dają możliwość zestawienia popularnych połączeń poprzez SLIP. Możliwe jest również, zachowując wymagania odległościowe do punktu koncentracji, wykorzystanie styku Ethernet.

W maksymalnie rozbudowej konfiguracji, w zależności od potrzeb, punkt koncentracji składać się może 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.

Zarządzanie siecią wymaga zarówno specjalistycznych narzędzi jak i wykwalifikowanej kadry. W sieci WARMAN zadaniem tym zajmuje się zespół operatorów. Praca zespołu jest zorganizowana tak, abvy każdy jego uczestnik mógł podnosić swoje kwalifikacje przez bezpośredni udział w rozwiązywaniu wszelkich problemów związanych z przyłączaniem abonentow i zarządzaniem siecią.

Jako narzędzie do zarządzania siecią został zastosowany system NMS 3000. Posiada on między innymi następujące możliwości:

- możliwość automatycznego rozpoznawania topologii sieci w części związanej z ATM; możliwość konfigurowania parametrów sieci ATM.
- możliwość wykonywania kopii zapasowych konfiguracji poszczególnych urządzeń bez interwencji operatora,
- możliwość dodawania modyłów do celów nie przewidzianych przzez autorów tego ssytemu,
- możliwość tworzenia "przekrojów" sieci, będących obrazem różnych sposobów patrzenia na nią

Sieć kampusowa w zgrupowaniu Ochota

Zgrupowanie naukowe w rejonie ulic Banacha, Pasteura, pawińskiego, Żwirki i Wigury obejmuje szereg jednostek Uniwersytetu Warszawskiego, Akademii medycznej, Polskiej Akademii Nauk i innych, tworzących zwarty zespół o rozmiarach rzędu 2 km. Zdecydowano się na wyodrębnienie tego rejonu ze struktury WARMANu w postaci siecimkampusowej. Jest ona również oparta o rozwiązania ATM. Zastosowano w niej urządzenia firmy Fore Systems: centralny switch ASX-200 oraz koncentratory LAX-20, połączone z centralnym switchem światłowodami wielomodowymi przy użyciu protokołu SDH/STM-1 (155 Mbps). W początku maja 1995 r. rozpoczęto montowanie tych urządzeń w docelowych miejscach pracy.

Kierunki rozwoju

Zastosowanie ATM w sieci miejskiej daje szerokie możliwości, Jedną z nich jest możliwość podziału sieci ATM na regiony (obszary) realizujące różne funkcje. Dzięki temu możliwe jest lepsze wykorzystanie zasobów sieci przez oddzielenie od siebie strumieni danych należących do użytkowników wymagających innego sposobu obsługi. Obecnie jest to możliwe jedynie w ograniczonym zakresie, wykorzystując *Virtual Path Switching*.

Następny etap jesat związany z ukończeniem prze ATM Forum prac standaryzujących SVC *(Switched Virtual Circuit)*. Zastosowanie SVC umożliwi takie funkcje jak automatyczna rekonfiguracja fragmentów sieci w przypadku awarii czy lepsze wykorzystanie sieci o możliwości wielu dróg obejściowych.

Istotne będzie również zakończenie prac nad *LAN emulation*. Jest to usługa w sieci ATM, polegająca na integracji urządzeń wykorzystujących interfejsy Ethernet i ATM w jedną sieć lokalną. Dzięki temu moiżliwe będzie np. włączaie szybkich serwerów lub centralnych routerów do sieci komputerowych przy użyciu interfejsów ATM. W przyszłości jest planowana możliwość tworzenia wielu sieci wirtualnych , wykorzystujących *LAN emulation* w sieci ATM.

Korzystając z dotychczasowych doświadczeń eksploatacyjnych, obserwując gwałtowny popyt światowy na rządzenia ATM oraz pozytywnie oceniając współpracę z dostawcą instalacji (tzn. z firmą Schrack Ericsson, ale także z firmą GDC) należy ocenić wybór technologii i sposób jej opanowywania jako udany.

Technologia ATM w praktyce

Andrzej Skrzeczkowski

I. Wstęp teoretyczny.

ATM jest obecnie najszybciej rozwijającą się technologią sieciową. Aby stwierdzić, dlaczego tak się dzieje należy najpierw zauważyć jej wielką atrakcyjność. Oferuje ona ogromną funkcjonalność, jest bardzo uniwersalna, a przy tym sieci zbudowane w oparciu o nią łatwo jest rozbudowywać.

Łączność między urządzeniami ATM zapewniają głównie łącza SDH (optyczne i galwaniczne). Za łączność z aplikacjami odpowiada warstwa adaptacyjna AAL1,..., AAL5 (*ATM Adaptation Layer)*. Umożliwiają one przesyłanie za pomocą ATM na przykład głosu (AAL1), HDTV (AAL2), danych transportowanych przy pomocy Frame Relay (AAL3/4), Ethernetu (AAL5) itp.

Ramka ATM zbudowana jest z 53 bajtów (rys. 1).

	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
1	Generic Flow Control				Virtual Path Identifier (VPI)			
2	Virtual Path Identifier (VPI)				Virtual Channel Identifier (VCI)			
3	Virtual Channel Identifier (VCI)							
4	Virtual Channel Identifier (VCI)				Payload Type Identifier			CLP
5	Header Error Check							
od 7 do 53	Payload (48 bytes)							

Rysunek 1. Struktura ramki ATM

Przy przejściu transmisji przez jeden z podstawowych elementów sieci - switch ATM może ulec zmianie albo VPI (VP switching), albo zarówno VPI jak i VCI (VC switching).

Zestawienie połączenia może mieć albo charakter stały ze stałą drogą (PVC), może być nawiązywane na życzenie (SVC) albo mieć charakter stały ze zmienną drogą (SPVC).

II. Źródła wiedzy praktycznej

Od ok. 9 miesięcy zespół WARMANa testuje sprzęt firmy GDC APEX-DV2 i APEX-MAC. Są to uniwersalne switch'e ATM umożliwiające wykorzystywanie zarówno kart z interfejsem SDH jak i kart adaptacyjnych.

Nasza droga przez technologię ATM wiodła od poznania podstawowych zasad obsługi sprzętu, przez doświadczenia z różnymi konfiguracjami, aż do organizacji złożonych testów i diagnostyki specyficznych błędów.

Dużo czasu zajęło nam również praktyczne zrozumienie zasad rządzących tworzeniem i używaniem sieci ATM. Przy próbach zestawiania logicznych połączeń okazywało się, że nasze

projekty przypominają raczej sieci z którymi mieliśmy dotychczas do czynienia (co było możliwe dzięki uniwersalności ATM). Gdybyśmy na tym poprzestali, to ATM wydawałby się ograniczony i mało atrakcyjny. Dopiero po nabraniu doświadczenia nasze projekty zaczęły wykorzystywać specyficzne właściwości ATM, w pełni potwierdzając zalety tej technologii.

III. O sprzęcie - obserwacje fizyczne

Elastyczność ATM wymusza elastyczność sprzętu. Przykładem są tu posiadane przez nas switch'e firmy GDC. Składają się one z obudowy, zasilaczy i kart. Do każdej obudowy APEX-DV2 można włożyć do 4 zasilaczy i 18 kart. Dostępne są różne typy kart, co powoduje, że można na ich bazie złożyć na przykład switch dostępowy (to znaczy umożliwiający dostęp użytkownikom), switch pracujący w szkielecie sieci (np. złożony jedynie z kart SDH) oraz, w razie potrzeby, switch mieszany (pracujący w szkielecie sieci z możliwością podłączania użytkowników).

Główne elementy switch'a mogą być dublowane. Do zasilania wystarczają 3 zasilacze (przy maksymalnej liczbie kart). Czwarty przewidziany jest do pracy w razie awarii. W ten sposób switch pracuje z trzema zasilaczami jedynie do czasu wymiany (oczywiście bez wyłączania całego urządzenia) popsutego modułu. Zdublowany jest także podstawowy element switch'a - karta odpowiedzialna za przełączanie połączeń. W czasie normalnej pracy pracuje tylko jedna z nich. Druga jest uaktywniana w razie awarii. Pozostałe karty mogą także pracować w reżimie podwyższonej niezawodności (przez dublowanie samych kart oraz/lub połączeń w sieci).

Tak pomyślane zabezpieczenia, aby mogły być w pełni wykorzystane wymagają, jak się okazuje, nie tylko zwiększonych nakładów na dublujący się sprzęt. Dla zasilaczy potrzebne są specjalne sieci elektryczne z urządzeniami podtrzymującymi (podwójna instalacja). Dodatkowo wydaje się konieczne utrzymywanie zespołu operatorskiego z pełnym zestawem części zamiennych, mobilnego i pracującego 24 godziny na dobę. Jak widać cena bezprzerwowego działania sieci jest bardzo wysoka. Warto jednak ponieść te koszty, gdyż jedynie w ten sposób jesteśmy w stanie zapewnić (z prawie 100% pewnością) dotarcie ważnych, potrzebnych i cennych danych w określone miejsce w określonym czasie.

Ważnym zadaniem jest realizacja synchronizacji w switch'u i w całej sieci. Można je zrealizować na różne sposoby. Najprostszym jest zastosowanie oscylatorów lokalnych dla każdej karty. Z naszych doświadczeń wynika, że w testowanym sprzęcie jest to rozwiązanie wystarczające. Jedyne błędy w pracy (niewielkie) zaobserwowaliśmy w raczej ekstremalnych warunkach: duża temperatura zewnętrzna, duża ilość działających kart, awaria głównego, zewnętrznego systemu chłodzenia i nadmiarowego zasilacza (sytuacja ta była symulowana w laboratorium).

Istnieją także inne, alternatywne sposoby synchronizacji. Sygnał synchronizacyjny może być na przykład pobierany z jednej z kart.Może być to albo dowolna działająca karta, albo specjalna karta zegara z dodatkowymi systemami kontrolnymi i wejściem zewnętrznych alarmów. Sygnał synchronizacyjny może być także pobierany z interfejsu SDH, co umożliwia synchronizację jednym zegarem całej sieci.

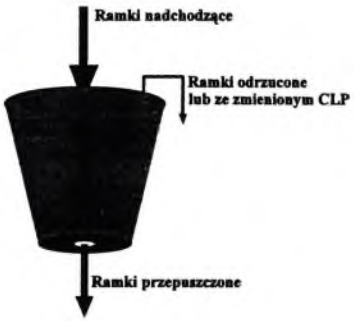
IV. Konfiguracja sprzętu ATM.

Konfiguracja sieci ATM wymaga dość specyficznego podejścia. Łatwo jest popełnić błędy ograniczające zalety technologii ATM. Najprostszy przykład: należy przyporządkować numery VPI/VCI w sieci złożonej z 5 węzłów, przy założeniu, że między dwoma węzłami nie będzie wykorzystywanych na raz więcej niż 10 połączeń. Najbardziej narzucającym się rozwiązaniem jest przyznanie oddzielnej, jednej pary numerów VPI/VCI dla każdej pary węzłów. Rozwiązanie takie

jest możliwe do realizacji, ale nie uwzględnia możliwości wzrostu liczby węzłów. Gdyby podobne rozwiązanie zastosować dla np. 40 węzłów, to należałoby przyznać 10*40*39/2=7800 oddzielnych par numerów VPI/VCI. Każdy switch musiałby tyle kanałów obsługiwać. Tu napotykamy na ograniczenie tej liczby w oprogramowaniu switch'a. Wraz ze wzrostem liczby węzłów napotykamy więc na barierę, która niszczy porządek, a więc i bezpieczeństwo sieci. Rozwiązanie jest w tym przypadku proste: należy stosować zmiany VPI i/lub VCI na drodze między dwoma punktami końcowymi (przy przechodzeniu przez kolejne switch'e).

Oddzielnym zagadnieniem przy konfiguracji jest kontrola ruchu. Realizowana jest ona za pomocą algorytmu "cieknących wiader". Dane "wpływają" do wiadra w przypadkowych odstępach czasu, a "wyciekają" w określonym tempie. Wiadro mając odpowiednią wielkość wypełnia się, gdy ramki przychodzą zbyt często. Po przekroczeniu odpowiedniego poziomu, zbyt często nadchodzące ramki są odrzucane (lub, zależnie od konfiguracji, zmieniany jest im bit CLP=0 na CLP=1). Zasadę działania tego algorytmu ilustruje rysunek 2.

Ustawienie parametrów tak skonstruowanego algorytmu (a zazwyczaj mamy do czynienia z dwoma wiadrami) wymaga znajomości ruchu i pewnego doświadczenia. Można na przykład wyobrazić sobie, że zamierzamy przesłać przez sieć ATM ramki Ethernetu. Wybranie nieodpowiednich wartości parametrów algorytmu może spowodować odrzucenie, powiedzmy, co 20 ramki ATM. Przy transmisji wyłącznie ATM nie musi mieć to, poza spowolnieniem faktycznej szybkości transmisji, wpływu na jakość połączenia. Przy transmisji ramek Ethernetu tak ustawione parametry praktycznie uniemożliwią transmisję. W takich warunkach ramka o długości 19*47+1=894 bajtów lub większej nie może być prawidłowa transportowana. Wysłanie takiej ramki spowoduje konieczność wielokrotnego - bezskutecznego - powtarzania jej przez nadawcę, a to z kolei zawiesi transmisję.



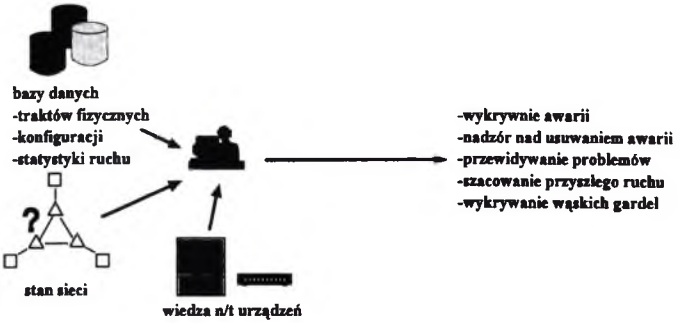
Rysunek 2. Zasada działania algorytmu cieknących wiader.

Przytoczone wyżej stosunkowo przecież proste przykłady dowodzą, że konfiguracja sieci ATM wymaga pewnego doświadczenia, które można zdobyć jedynie przy pracy nad konfiguracją sieci ATM.

V. Administracja sieci ATM.

Technologia ATM zapewnia duże bezpieczeństwo przesyłanych danych. Po pierwsze nie jest możliwe (bez zastosowania bardzo niekonwencjonalnych środków do analizy danych transmitowanych przez światłowody) śledzenie przesyłanych danych. Po drugie praca sieci może być administrowana centralnie. Może być zdefiniowany na przykład tylko jeden punkt w całej sieci, z którego administracja taka byłaby możliwa. Można także określić, jakie uprawnienia mają administratorzy różnych poziomów (w celu zabezpieczenia ważnych danych konfiguracyjnych). Po

trzecie wreszcie, możliwy jest centralny monitoring pracy sieci z graficzną prezentacją jej struktury, ważnych parametrów i danych dotyczących ruchu w poszczególnych połączeniach fizycznych i logicznych (rys 3).



Rysunek 3. Zalety centralnego zarządzania siecią ATM

Graficzny system administrowania siecią służy nie tylko do monitoringu, ale także do zarządzania siecią. W naszej pracy stosujemy system NMS3000 firmy GDC, umożliwiający kontrolę i zarządzanie wszelkimi urządzeniami sieciowymi posługującymi się protokołem SNMP, a do takich zaliczają się switch'e ATM APEX. System ten oprócz graficznej prezentacji urządzeń i połączeń między nimi może wyświetlać dowolne parametry, reagować na ich zmiany, informując operatora o przekroczeniu przez nie wartości alarmowych. Przy jego pomocy można także zmieniać konfigurację sprzętu.

Takie zarządzanie siecią ma swoje ogromne zalety. Po pierwsze, mając do dyspozycji narzędzie do diagnostyki i usuwania niektórych awarii, operator może szybko reagować na awarie zgłaszane przez użytkowników. Po drugie może on sam dostrzegać nieprawidłowości w działaniu sieci (awarie redundantnych urządzeń, uszkodzenie fizyczne połączenia itp.). Po trzecie może on wykrywać słabe punkty sieci (punkty koncentracji ruchu, nieoptymalne wykorzystanie połączeń fizycznych itp.), co może stanowić podstawę do planów jej dalszej rozbudowy.

Administrator sieci ATM ze switch'ami APEX ma do dyspozycji jeszcze jedno bardzo silne narzędzie - programy PSI. Można je napisać i uruchomić na switch'u w celu realizacji przez niego niestandardowych zadań. Jednym z nich jest okresowe przełączanie redundantnych elementów sieci. Jest to konieczne, jeżeli chcemy mieć pewność, że urządzenia te gotowe są do podjęcia swoich funkcji w razie awarii. W praktyce stosowaliśmy także programy PSI do testowania - wyświetlania na konsoli niestandardowych parametrów (po przeliczeniu) oraz automatycznego wykonywania różnych czynności w reakcji na określone parametry przechodzącego przez switch ruchu. Wydaje się wskazane napisanie biblioteki programów PSI do wykonywania pewnych rutynowych zadań występujących przy konfigurowaniu i testowaniu switch'y.

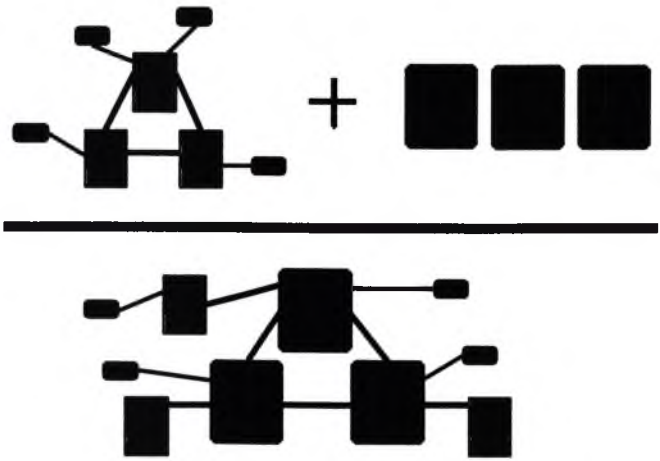
Rozbudowa sieci ATM częściowo wynika także z zadań administratora. Sieć ATM jest skalowalna. Możliwa jest jej rozbudowa w praktycznie dowolnym miejscu i na dowolną skalę. Wynika z tego, że sposób rozbudowy sieci będzie zależał prawie wyłącznie od potrzeb i nie jest w żaden sposób ograniczany przez technologię (tak jak ma to miejsce np. w przypadku sieci FDDI).

Dlatego przed administratorem stoją dodatkowe, ważne zadania obserwacji zachowania się sieci, przewidywania niebezpieczeństw i wskazywania wrażliwych punktów. Dopiero po takiej analizie możliwe jest planowanie dalszej jej rozbudowy.

VI. Ekonomia ATM

Sprzęt ATM jest ciągle nowością. W związku z tym ceny są jeszcze wysokie. Tym niemniej wszystkie większe firmy produkujące sprzęt sieciowy już zapowiedziały przejście na tą technologię. Dlaczego tak się dzieje? Przyczyna leży w cechach ATM. W przypadku używanych przez nas switch'y można na przykład bardzo łatwo zmieniać konfiguracją (przez wymianę lub dokładanie nowych kart), a przez to nadążać za rosnącymi potrzebami użytkowników. Nie jest także wielkim problemem zaadoptowanie sieci ATM do przesyłania nowego rodzaju danych. W sieci tej mogą być transportowane zarówno różne protokoły jak i wymagające transmisji izochronicznych sygnały dźwięku i obrazu.

Przy ocenie opłacalności sieci ATM należy także zwrócić uwagę na amortyzację sprzętu. Nie byłoby dobrze gdyby okazało się, że urządzenia, które się jeszcze nie zamortyzowały, nie spełniają rosnących wymagań. W technologii ATM możliwa jest migracja takiego sprzętu w punkty, gdzie wymagania są mniejsze (rys. 4). Takie podejście powoduje, że starszy sprzęt może się w pełni zamortyzować, pracując tam, gdzie jego zdolności przetwarzania są wystarczające.



Rysunek 4. Skalowalność ATM

Sam standard nie stanowi także ograniczenia. Definiowane są ciągle nowe protokoły, szybkości i sposoby fizycznego połączenia. Z technologią ATM można więc patrzeć w przyszłość bez strachu.

VII. Kadra ATM

Z przedstawionych powyżej doświadczeniach praktycznych wynika jeszcze jeden ogólny wniosek. Aby prawidłowo uruchomić i utrzymać dużą sieć ATM należy skompletować zespół specjalistów, bardzo dobrze znających niuanse używania tej technologii, jej możliwości, zalety i ograniczenia. Taki zakres wiedzy może zostać zdobyty jedynie przez bezpośrednie doświadczenie. Wniosek nasuwa się więc sam. Jeżeli myśli się o ATM w przyszłości należy już teraz, mimo że niektóre standardy są dopiero ustalane, zacząć stosować sprzęt pracujący z wykorzystaniem tej technologii.

Protokoły wyboru trasy w sieci ATM

Jarosław M. Janukiewicz, Waldemar E. Grzebyk

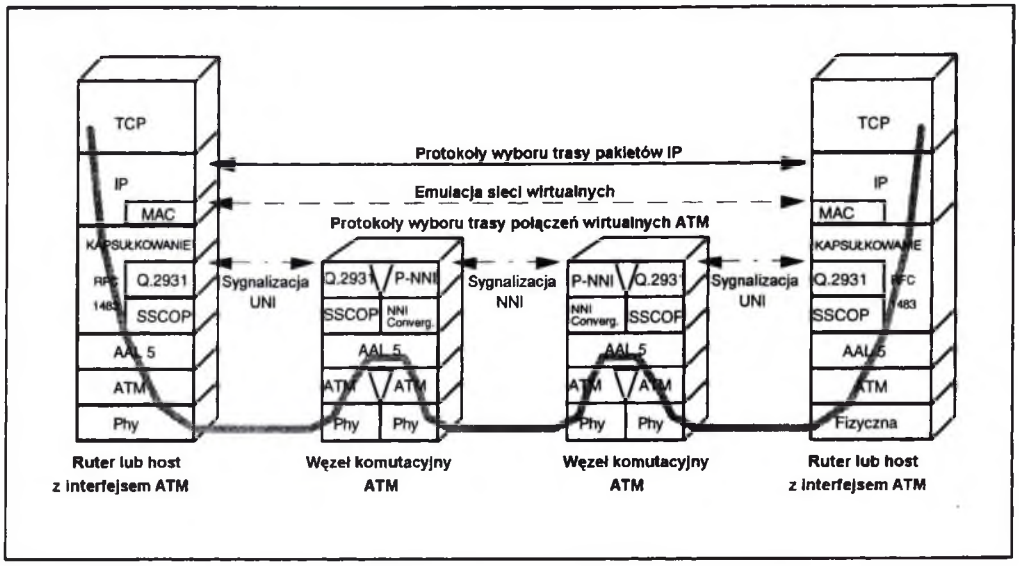
Naukowa i Akademicka Sieć Komputerowa
Zakład Telekomunikacji
50-327 Wrocław, ul. Janiszewskiego 7/9, tel./fax: 219529

1. Wstęp

Wśród wielu usług, które mogą być realizowane przez sieć ATM (ang. Asynchronous Transfer Mode) najszybciej rozwijane są usługi transmisji danych. W większości działających węzłów ATM implementowane są warstwy adaptacyjne 3,4, i 5. przeznaczone do realizacji transmisji danych w trybie połączeniowym i bezpołączeniowym. Najczęściej używanym jest protokół IP (ang. Internet Protocol). Równolegle z pojawieniem się pierwszych specyfikacji określających UNI (ang. User Network Interface) dla sieci ATM pojawiły się dokumenty RFC (ang. Request for Comments) przedstawiające sposób transmitowania różnych protokołów przez sieć ATM. Podstawowym nie mającym jeszcze ostatecznego rozwiązania jest problem wytyczania trasy, po której przesyłana jest informacja pomiędzy węzłami sieci. Wybór trasy (ang. routing) w przypadku sieci ATM rozpatrywany jest w dwóch aspektach. Jako metoda znajdowania drogi dla pakietów warstwy trzeciej przez zestawione trwałe połączenia wirtualne PVC (ang. Permament Virtual Circuit) lub jako zestawianie przełączanych połączeń wirtualnych SVC (ang Switched Virtual Circuit). Połączenia przełączane są zestawiane na życzenie w sposób dynamiczny z wykorzystaniem sygnalizacji definiowanej dla ATM-u.
W artykule skupiono się na przedstawieniu sposobu transmisji pakietów IP poprzez sieć ATM. Na przykładzie urządzeń - rutery C7000 i węzeł komutacyjny ATM HyperSwitch 100 firmy Cisco - pracujących we Wrocławskiej Akademickiej Sieci Komputerowej przedstawiono stosowane protokoły wyboru trasy zarówno dla sieci IP poprzez ATM jak i dla tworzenia połączeń wirtualnych.

2. Transmisja z protokołem IP przez sieć ATM.

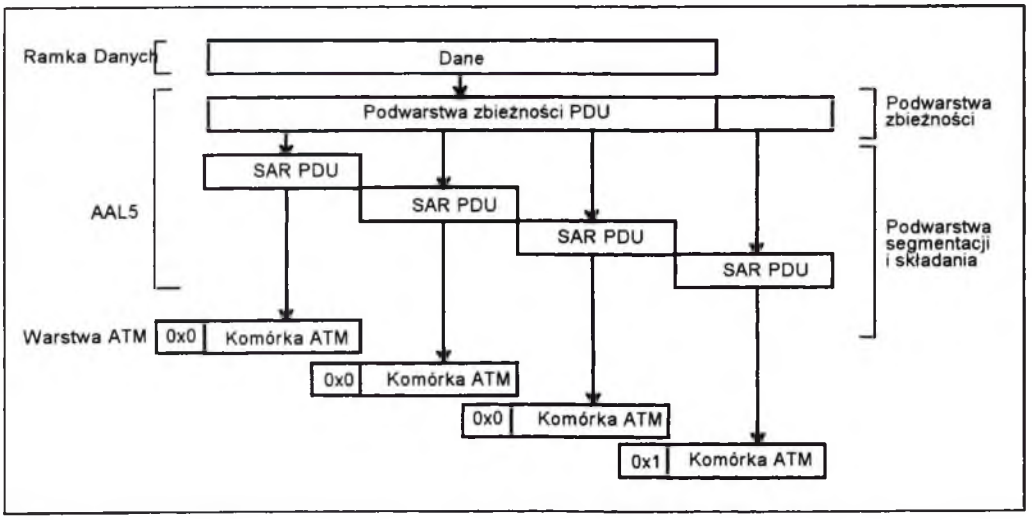
Transmisja pakietów IP przez sieć ATM może być realizowana na kilka sposobów. Różnice wynikają ze sposobu kapsułkowania pakietów IP i przyjętego protokołu wyboru trasy. Proponowane rozwiązania wykorzystują warstwę adaptacyjną typu piątego ATM-u (AAL 5) do przeniesienia pakietów IP. W procesie transmisji pakietów mogą brać udział dwa różne protokoły wyboru trasy. Pierwszy z nich jest jednym z protokołów typowych dla sieci IP statyczny lub dynamiczny, drugi jest protokołem związanym z wytyczaniem trasy kanału wirtualnego obecnie statyczny. Na rysunku 1 przedstawiono model systemu transmisji IP przez sieć ATM. Sposób kapsułkowania ramek protokołów wyższych warstw przedstawiony jest w dokumencie RFC-1483. W opracowaniu tym przedstawiono dwie metody kapsułkowania. W pierwszym przypadku transmisja ramek odbywa się poprzez jedno łącze wirtualne. Każda ramka posiada nagłówek LLC (ang. Link Layer Control) zgodny ze specyfikacją IEEE 802.2. W drugim przypadku pakiety każdego z protokołów przesyłane są odrębnymi kanałami wirtualnymi. Preferowana jest jako szybsza i bardziej wydajna druga metoda bazująca na multipleksacji połączeń wirtualnych (ang. VC based multiplexing).
W obydwu przypadkach transport przez sieć ATM realizowany jest z wykorzystaniem warstwy adaptacyjnej ATM-u typu piątego (AAL 5). Schemat procesu segmentacji i składania pakietu i sposób upakowania w komórkach ATM został przedstawiony na rysunku 2.



Rys. 1. Model transmisji IP przez sieć ATM

Skróty: TCP - Transport Control Protocol
IP - Internet Protocol
MAC - Medium Access Control
SSCOP - Service Specific Connected Oriented Protocol
AAL - ATM Adaptation Layer
UNI - User-Network Interface
NNI - Network-Network Interface
P-NNI - Private Network-Network Interface

W AAL 5 maksymalna długość jednostki protokołu PDU (ang. Protocol Data Unit) może wynosić 65535 oktetów. W przypadku protokołu IP maksymalna długość PDU została określona w RFC-1626 na 9180 oktetów i jest wystarczająca do obsłużenia bez dodatkowej segmentacji w warstwie IP wszystkich protokołów warstw wyższych.

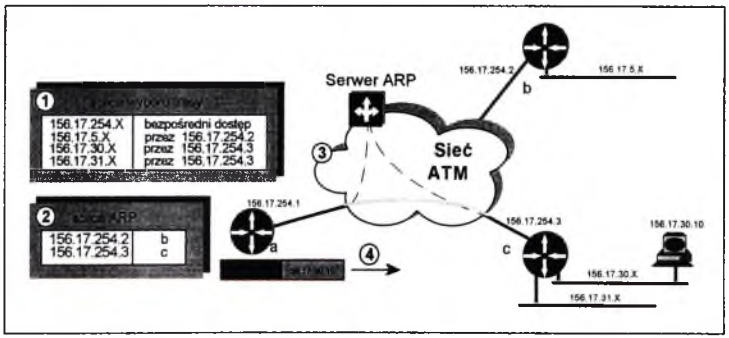


Rys. 2. Sposób upakowania pakietów protokołów warstw wyższych w komórkach ATM

Komórki zgodne ze specyfikacją AAL 5 mogą znajdować się w jednym z trzech stanów:

- komórka pusta,
- ostatnia komórka zawierająca fragment PDU,
- kolejna komórka zawierająca fragment PDU.

Do oznakowania komórek wykorzystuje się jeden z bitów w nagłówku komórki. Ostatnia komórka w sekwencji ma ten bit ustawiony na jedynkę w pozostałych bit jest ustawiony na zero. Wybór trasy dla pakietów IP związany jest z procesem skojarzenia adresu IP z adresem warstwy drugiej wykorzystywanego systemu połączeń. W sieci ATM stosuje się dwa systemy adresacji zgodny ze stosowanym w sieciach publicznych i zalecany przez ITU-T w E.164 lub jedną z implementacji adresacji ISO NSAP (ang. Network Service Access Point). W typowych sieciach lokalnych (Ethernet, Token Ring, FDDI) informacja o związku adresów IP z adresami warstwy drugiej jest przekazywana zgodnie z protokołem ARP (ang. Address Resolution Protocol). Protokół ten korzysta z mechanizmu rozgłaszania (ang. broadcast) do wymiany informacji. W wyniku działania tego protokołu urządzenie sieciowe tworzy tablicę z parami adresów IP i adresu warstwy drugiej zgodnie z ISO OSI. W dokumencie RFC-1577 przedstawiono sposób realizacji klasycznej sieci IP i implementacji protokołu ARP w sieci ATM. Scenariusz działania protokołu wyboru trasy zgodny z cytowanym dokumentem został przedstawiony na rysunku 3.



Rys. 3. Wybór trasy pakietów IP w sieci ATM.

Przesłanie pakietu IP przez sieć ATM (w naszym przykładzie przeznaczonego dla hosta o adresie 156.17.30.10) jest realizowane w czterech krokach:

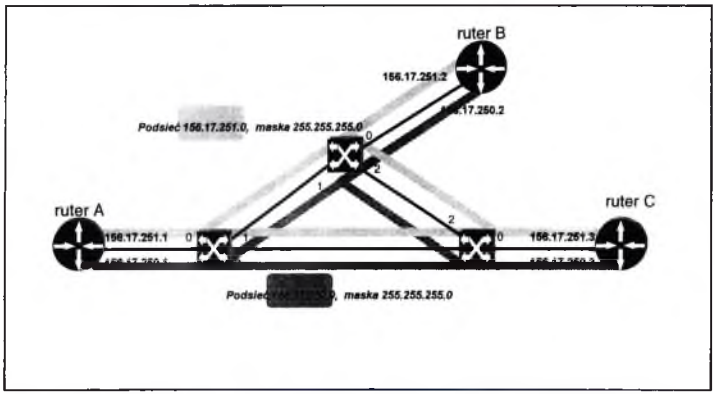
1. Z tablicy wyboru trasy pobrany jest adres IP następnego rutera na drodze do odbiorcy pakietów (156.17.254.3) znajdującego się w podsieci 156.17.31.X;
2. Na podstawie tablicy ARP odwzorowywany jest adres IP (156.17.254.3) na adres rutera w sieci ATM (c);
3. Przy użyciu sygnalizacji UNI (ITU-T Q-2931) na żądanie rutera kreowane jest połączenie wirtualne pomiędzy węzłami a i c;
4. Przez zestawione połączenie przesyłane są pakiety do odbiorcy.

W przypadku małych sieci tablica wyboru trasy i tablica ARP mogą być wypełnione ręcznie przez administratora systemu. W dużych systemach operacja taka jest staje się bardzo skomplikowana i kłopotliwa w przypadku zmiany konfiguracji. Jednym z rozwiązań dynamicznego uzupełniania zawartości tablicy polega na zastosowaniu serwera ARP o znanym

adresie ATM [RFC1577]. W serwerze rejestrowane są zgłoszenia od wszystkich ruterów. Serwer przechowuje tablice ARP i na zapytanie rutera podaje adres ATM związany z adresem IP. Obecnie opracowywany protokół NHRP (ang. Next Hop Resolution Protocol) [NHRP03] będący rozwinięciem idei wykorzystania serwera ARP.

3. Realizacja sieci IP z wykorzystaniem trwałych kanałów wirtualnych

Trwałe połączenia wirtualne PVC są odpowiednikiem połączeń punkt-punkt na tradycyjnych łączach dedykowanych. Na jednym fizycznym połączeniu można zdefiniować wiele połączeń wirtualnych. Rutery można skonfigurować z dowolnym protokołem wyboru trasy (np. RIP, IGRP, OSPF, "Hello"). W celu zwiększenia niezawodności sieci możemy utworzyć różne podsieci związane z różnymi połączeniami wirtualnymi. Na rysunku 4 przedstawiono przykład takiej konfiguracji.



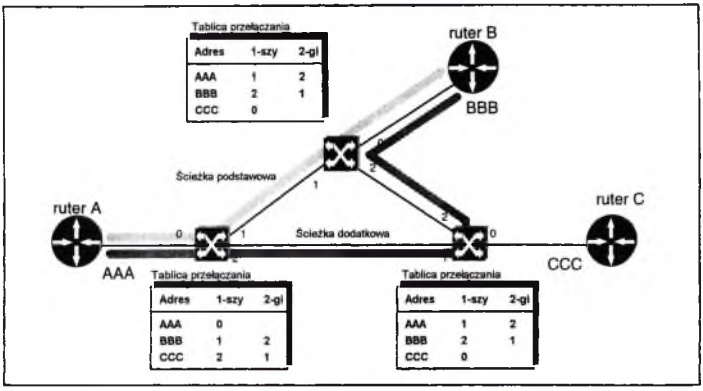
Rys. 4. Dwie podsieci IP realizowane na dedykowanych PVC.

Kazdy z ruterów jest dołączony do dwóch podsieci IP. Połączenia wirtualne zrealizowane są w strukturze typu "mesh". Uszkodzenie dowolnej z linii fizycznych pomiędzy węzłami komutacyjnymi nie powoduje przerwy w transmisji. Użycie dynamicznego protokołu wyboru trasy w warstwie IP wystarcza do znalezienia alternatywnej trasy transmisji pakietów. Tak skonstruowana sieć jest odporna na uszkodzenia.

4. Realizacja sieci IP z wykorzystaniem przełączanych kanałów wirtualnych

Przełączane połączenia wirtualne wymagają implementacji w węzłach komutacyjnych sygnalizacji pomiędzy użytkownikiem i siecią a także sygnalizacji międzysieciowej. Obecnie znane są definicje sygnalizacji typu użytkownik - sieć (sygnalizacja UNI). Implementowana jest sygnalizacja typu P-NNI zgodna ze specyfikacją UNI-3.0. Charakteryzuje się ona realizacją statycznego wyboru trasy, nie zawiera mechanizmów pozwalających na wykrywanie zapętleń w sieci. Ten system sygnalizacji używany jest w węzłach komutacyjnych HS A-100 firmy Cisco. Na rysunku 5 został przedstawiony schemat sieci ATM w którym zastosowano sygnalizację typu P-NNI Phase 0 do realizacji alternatywnej trasy połączenia pomiędzy dwoma

ruterami. W przypadku uszkodzenia podstawowego połączenia generowany jest pakiet sygnalizacyjny. Każdy z węzłów ma zdefiniowane w tablicy przełączania dwie drogi. W przypadku niedostępności drogi podstawowej aktywowana jest droga rezerwowa.



Rys. 5. Realizacja alternatywnego połączenia wirtualnego z wykorzystaniem SVC

Nowa trasa używana jest do chwili odzyskania połączenia na podstawowej trasie. Tablice przełączania w węzłach komutacyjnych ATM są wypełniane przez administratora podczas konfiguracji.

5. ATM w sieci WASK

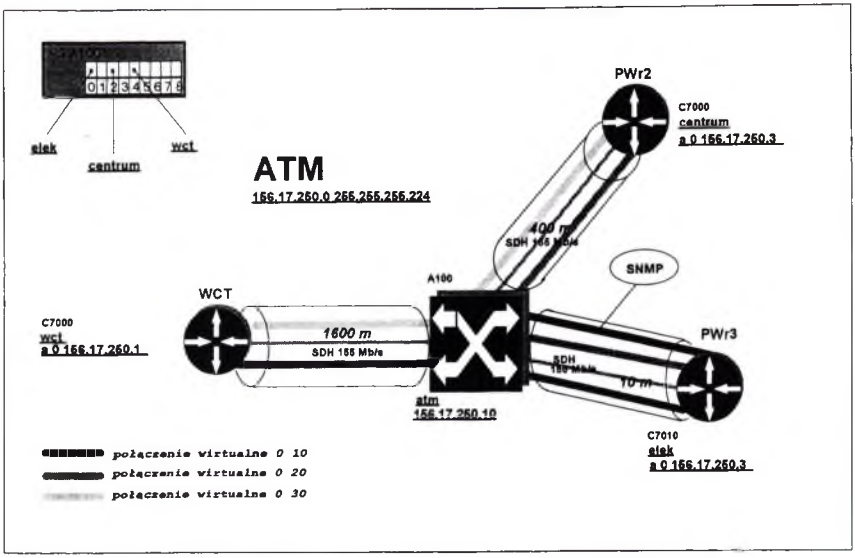
Fragment sieci wykonany w technologii ATM został uruchomiony we Wrocławskiej Akademickiej Sieci Komputerowej WASK na początku 1995 r. Ma on charakter eksperymentalny. Sieć ATM wykonano w oparciu o HyperSwitch A100 i trzy rutery C7000 z interfejsami ATM SDH 155 Mb/s firmy Cisco Systems Inc. Topologię sieci przedstawiono na rysunku 6. Sieć ATM skonfigurowano definiując trwałe połączenia wirtualne PVC.

Do konfiguracji węzła komutacyjnego A100 wykorzystano dwie podstawowe komendy:

- komendę **set**:

  a100# set interface P1 P2 P3 P4 P5

  gdzie: **P1:** Numer linii (0÷15)
  P2: Typ interfejsu:
  0: UNI - domyślnie
  1: NNI
  P3: Standard
  0: ATM Forum - domyślnie
  1: ITU
  P4: ilość bitów znaczących w VPI (0÷7; domyślnie - 4)
  ilość bitów znaczących w VCI (5÷12, domyślnie - 8)



Rys. 6. Schemat fragmentu sieci WASK zrealizowanego w technologii ATM

- komendę **pvc**

  a100# pvc P1 P2 P3 P4 P5 P6 P7 P8 P9 P10 P11 P12 P13

  gdzie: **P1:** Typ połączenia
  0: jednokierunkowy
  1: dwukierunkowa
  2: punkt-wiele punktów

  P2: Jakość transmisji
  0: gwarantowana
  1: niegwarantowana

  P3: Szybkość transmisji (podawana w Mb/s, jeżeli P2=1 podać P3=0)

  P4: Dolny numer linii (0÷15, odpowiadający numerowi slotu)

  P5: Dolne VPI (0÷4095)

  P6: Dolne VCI (0÷4095)

  P7: Dolne UPVP (0÷512)

  P8: Dolne COOP używane w przypadku zgubienia komórki
  0: zapamiętywane
  1: odrzucane

  P9: Górny numer linii (0÷15, odpowiadający numerowi slotu)

  P10: Górne VPI (0÷4095)

  P11: Górne VCI (0÷4095)

  P12: Górne UPVP (0÷512) (jeżeli P1=0 podać P12=0)

  P13: Górne COOP używane w przypadku zgubienia komórki
  0: zapamiętywane
  1: odrzucane (jeżeli P1=0, ustawić P13=0)

Sposób konfigurowania trwałych połączeń wirtualnych w węźle **A100** jest przedstawiony poniżej:

```
a100# set interface 0 0
a100# set interface 2 0
a100# set interface 4 0
a100# pvc establish 1 1 0 0 0 10 512 1 4 0 10 512 1
a100# pvc establish 1 1 0 0 0 20 512 1 2 0 20 512 1
a100# pvc establish 1 1 0 2 0 30 512 1 4 0 30 512 1
a100# pvc establish 1 0 1 0 0 1 512 1
```

Wytłuszczoną czcionką zaznaczono numery linii, wytłuszczoną kursywą oznaczono adresy VPI i VCI. Fragmenty zbiorów konfiguracyjnych dotyczące interfejsów ATM w ruterach C7000 zostały przedstawione w tabeli 1.

Tabela 1

Konfiguracja rutera **elek**	Konfiguracja rutera **centrum**	Konfiguracja rutera **wct**

TECHNOLOGIA FRAME RELAY

Dariusz Piotrowski

Wstęp.

Rozwój sieci teleinformatycznych zmierza w kierunku zwiększania przepustowości i szybkości transmisji danych. Proces ewolucji jest zależny przede wszystkim od wymagań użytkowników, którzy tworzą rynek silnie osadzony w realiach ekonomicznych. Najczęściej o wyborze technologii decydują następujące czynniki:

- maksymalna efektywność,
- elastyczność rozwiązań,
- minimalizacja kosztów.

Tytułowa technologia frame relay powstała w wyniku zmian jakie dokonały się w technologiach przekazywania danych.

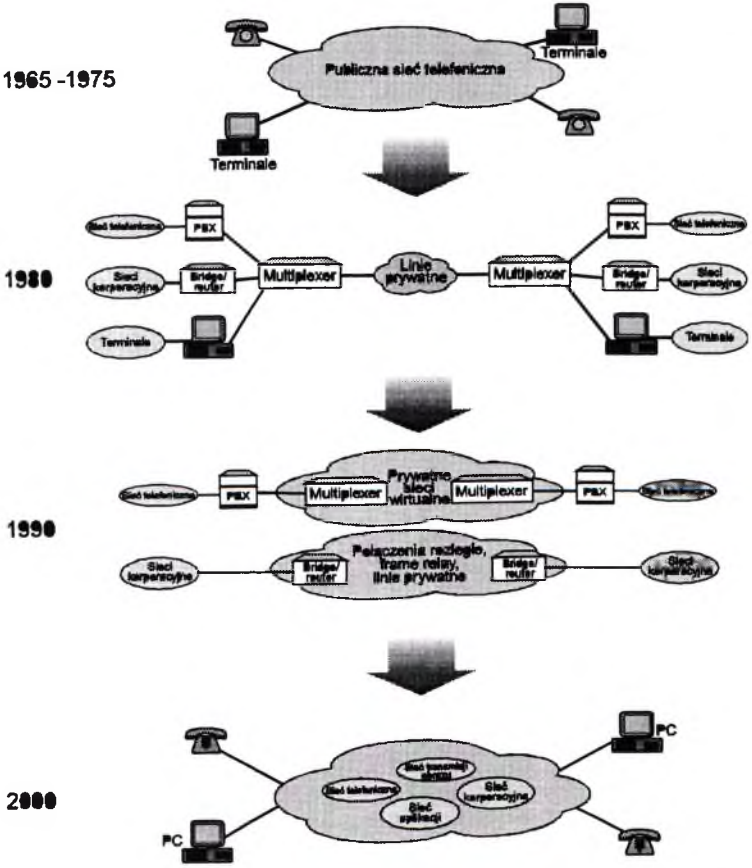
W połowie lat sześćdziesiątych i siedemdziesiątych dominował dostęp terminałowy. Użytkownicy zaopatrzeni w terminale, czyli komputery służące praktycznie do wprowadzania danych i odczytywania wyników, łączyli się poprzez publiczną sieć telefoniczną z ośrodkami komputerowymi umożliwiającymi dokonywanie obliczeń. Z punktu widzenia sieci telefonicznych przesyłanie danych było traktowane dokładnie tak, jak przesyłanie głosu. Jednak była to znikoma część - około 2 procent ogólnej transmisji. Dominującym i właściwie jedynym standardem w sieciach rozległych, nie licząc doświadczeń laboratoryjnych, był standard X.25.

Kolejnym krokiem zapoczątkowanym przez duże firmy i korporacje było tworzenie własnych sieci opartych na prywatnych łączach. Wysokie opłaty za rozmowy telefoniczne przy jednoczesnym obniżeniu kosztów dzierżawy linii spowodowały, iż wiele firm zbudowało własne sieci integrujące transmisję danych (różne protokoły) i głosu. Jako rozwiązanie techniczne stosowano multipleksery wielokanałowe na liniach dzierżawionych. Był to okres lat osiemdziesiątych.

Jednak szybki rozwój sieci rozległych opartych na protokole TCP/IP oraz usług dostępnych na całym świecie: e-mail, bazy danych, etc. wyznaczył nowy etap, który trwa do dziś. Technologia oparta na multiplekserach okazała niewystarczająca i mało elastyczna jeśli chodzi o przesyłanie danych. Równocześnie obniżono koszty rozmów telefonicznych do poziomu, który zahamował trend integracji danych i głosu. Nie oznaczało to oczywiście natychmiastowego powrotu do wcześniejszych rozwiązań lecz pozwoliło wykreować zupełnie nowe pomysły. Obok multiplekserów i sieci prywatnych pojawiła się koncepcja sieci wirtualnych. Sieci wirtulane są sieciami logicznymi, niezależnymi od struktury połączeń fizycznych. Użytkownik dołącza się do najbliższego węzła sieci operatora i określa punkty, z którymi chce utrzymywać łączność. Sposób realizacji tej usługi wewnątrz sieci, obrazowo przedstawianej w postaci chmurki, leży całkowicie w gestii operatora. Dla użytkownika zanika pojęcie fizycznej linii dzierżawionej zestawianej na zasadzie punkt-punkt. Równocześnie dokonał się olbrzymi postęp w dziedzinie mediów transmisyjnych. Światłowody stworzyły perspektywę niemal bezbłędnej transmisji z prędkościami dziesiątek, setek, a nawet tysięcy mega bitów na sekundę. Właśnie te nowe możliwości i zapotrzebowanie ze strony rynku doprowadziło do przyspieszenia prac nad nowymi technologiami bazującymi na *szybkim przełączaniu pakietów*. Zgodnie z przewidywaniami właśnie te technologie mają zdominować rynek sieci rozległych w drugiej połowie lat dziewięćdziesiątych.

Przyszłość, czyli początek XXI wieku może paradoksalnie okazać się powrotem do modelu, od którego wszystko się zaczęło. Zgodnie z działaniami operatorów publicznych

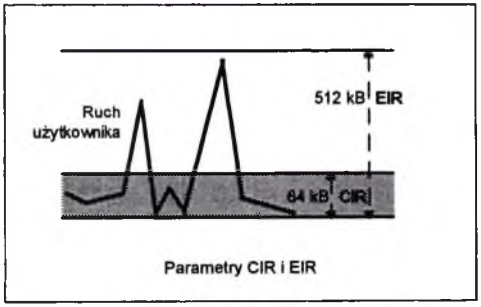
powstanie jedna, ogólna sieć integrująca wszelkie rodzaje transmisji począwszy od danych, a skończywszy na telewizji wysokiej rozdzielczości. I podobnie jak w latach siedemdziesiątych użytkownik będzie dołączał się do niej w celu uzyskania określonej usługi. Oczywiście komputer użytkownika będzie posiadał bardzo szybkie interfejsy i nieporównywalnie większą inteligencję, niż terminale i modemy z lat sześćdziesiątych. Prawdopodobnie na bazie tej supersieci powstaną wirtualne sieci korporacyjne, bankowe, transmisji głosu, obrazu, a także sieci serwerów konkretnych aplikacji np. popularnego obecnie serwisu informacyjnego WWW (World Wide Web). Kolejne etapy zostały przedstawione na rysunku poniżej.



1. Podstawowe elementy technologii Frame relay

Technologia frame relay była projektowana z myślą o transmisji danych. Cechuje ją *szybkie przełączanie pakietów* czyli wprowadzanie minimalnych opóźnień w węzłach sieci. Jej efektywność w stosunku do tradycyjnych sieci bazujących na przełączaniu pakietów widać najlepiej przy szybkich łączach 2MB. Właśnie wtedy opóźnienia na węzłach zaczynają znacząco wpływać na całkowity czas transmisji.

Jedną z podstawowych zalet jest elastyczność frame relay w przypadku przenoszenia ruchu o zmiennym natężeniu. Większość współczesnych aplikacji generuje bardzo duży ruch chwilowy. Oprogramowanie działające w oparciu o zasadę klient - serwer nie obciąża pasma w sposób ciągły, gdyż bazuje na asynchronicznych zapytaniach i odpowiedziach. Podobnie można opisać ruch generowany przez sieci lokalne. Technologia frame relay udostępnia mechanizm pasma na żądanie, który pozwala przenosić ruch chwilowy większy niż wartość pasma, za które płaci użytkownik. Multipleksowanie statystyczne ramek umożliwia zajęcie przez użytkownika większego niż ma zagwarantowane lub nawet całego pasma, pod warunkiem, że inni użytkownicy w tym momencie nic nie transmitują. W rzeczywistości opisaną powyżej funkcję realizuje się za pomocą parametru CIR (Commited Information Rate). Jest to parametr określający ilość bitów jaką użytkownik może przesłać w zadanym przedziale czasu. Charakteryzuje on każdy kanał wirtualny użytkownika. Natomiast przy przekroczeniu limitu określanego przez CIR sieć Frame Relay podejmuje próbę przesłania danych bez gwarancji dostarczenia ich do adresata. Jednak taka zasada skalkulowanego ryzyka opłaca się, gdyż praktycznie nie zdarzają się takie sytuacje, w których wszyscy użytkownicy nadają jednocześnie. Wielkość ruchu jaką użytkownik może próbować przesłać przekraczając CIR określa parametr EIR (Excess Information Rate).

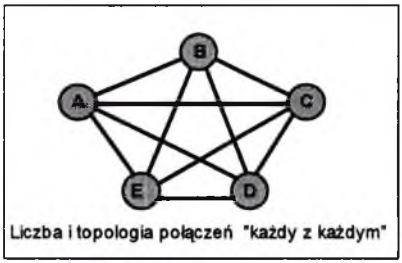


Parametry CIR i EIR

Przykładowo, jeśli mamy połączenie fizyczne 2 MB do switch'a frame relay i opłacony kanał wirtualny z parametrem CIR 64 kbps oraz EIR 512 kbps to sieć podejmie próbę przeniesienia naszego chwilowego ruchu do wartości 512 kbps. Jednak należy pamiętać, że jest to próba i normalny, średni ruch generowany przez użytkownika powinien mieścić się w zakresie pasma określonego CIR'em czyli 64 kbps.

W przypadku istniejącej sieci szkieletowej frame-relay jedynym kosztem jest opłata za dołączenie do portu najbliższego węzła sieci. Takie sieci szkieletowe są budowane na świecie najczęściej przez operatorów publicznych.

Frame relay stanowi konkurencję zarówno dla obecnie stosowanych rozwiązań jak i dla technologii zdobywających rynek. W chwili obecnej aby, uzyskać w sieci pełny graf połączeń wszystkich węzłów należy zestawić N*(N-1)/2 połączeń dzierżawionych, co w wielu wypadkach przekracza możliwości finansowe firm. Przykładowe połączenie pięciu lokalizacji wymaga dziesięciu linii.



Liczba i topologia połączeń "każdy z każdym"

Jeśli chodzi o nowe rozwiązania np. ATM, SMDS istotnym elementem jest stan standaryzacji protokółu i stopień jego wdrożenia w skali całego świata. Jednak nawet w przypadku szybkiego rozwiązania wielu problemów implementacyjnych pozostanie problem prędkości łącz. W chwili obecnej operatorzy publiczni nie są przygotowani do udostępniania powszechnie traktów 155 i 622 czy nawet 34 MB. Również ceny takich łącz, biorąc jako odniesienie obecne koszty linii 2 MB wydają się astronomiczne.
Biorąc pod uwagę powyższe fakty, frame relay znacznie wyprzedza konkurencyjne rozwiązania co potwierdzają zestawienia określające kierunki rozwoju w sieciach komputerowych. O dynamice rozwoju świadczą dwa czynniki: wielkość inwestycji finansowych i zainteresowanie ze strony rynku czyli popyt. Jeśli chodzi o inwestycje na frame relay to przekraczają one zdecydowanie nakłady na tworzenie sieci ATM, natomiast o popycie świadczyć może fakt, że najwięksi operatorzy w Stanach i Europie szacują czas oczekiwania na port frame relay od 2 do 6 miesięcy.

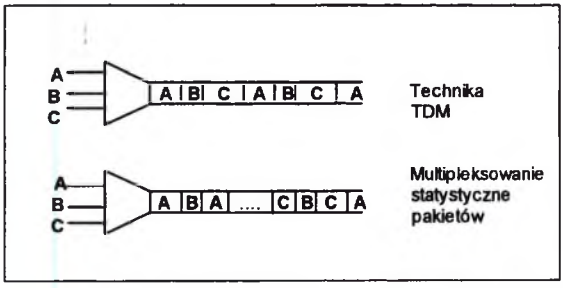
Reasumując, elastyczność w przenoszeniu silnie zmiennego ruchu i konkurencyjność cenowa w stosunku do sieci opartych na połączeniach dzierżawionych stawiają frame relay na jednym z pierwszych miejsc wśród technologii połowy lat dziewięćdziesiątych

2. Porównanie technologii przełączania pakietów i TDM (Time Division Multiplexing)

Technologie oparte na przełączaniu pakietów wykorzystują statystyczne multipleksowanie wielu strumieni pakietów w jedno łącze fizyczne. Oznacza to, że każdy kolejny pakiet jest przekazywany natychmiast jeśli pojawi się wolne pasmo. Obowiązuje zasada "składuj i przekazuj dalej", realizowana przez zaawansowane metody buforowanie. To rozwiązanie pozwala na chwilowe przepełnienie na liniach wejściowych. Sumaryczna liczba pakietów na wszystkich wejściach może chwilowo przekroczyć liczbę pakietów wychodzących. Strumienie pakietów nie mają przypisanych konkretnych szczelin czasowych. Pakiety z jednego strumienia mogą być wysyłane dalej niemal tak szybko jak są otrzymywane pod warunkiem braku obciążenia

generowanego przez inne strumienie. Przełączanie pakietów między portami odbywa się na poziomie warstwy drugiej modelu ISO OSI. Zapewnia to przyspieszenie transmisji i bardzo elastyczne wykorzystanie pasma.

Powszechnie wykorzystywana technika TDM zakłada ścisły podział pasma między przychodzące strumienie pakietów. Całe pasmo jest dzielone na szczeliny czasowe. Użytkownik w zależności od prędkości ma przyznaną odpowiednią ilość szczelin czasowych. Ilość pakietów wejściowych jest równa ilości pakietów wyjściowych. Między portami dwóch urządzeń końcowych jest tworzony kanał logiczny z reguły odpowiadający danemu użytkownikowi czy wręcz protokołowi sieciowemu. W takiej sytuacji pakiet musi oczekiwać na swoje miejsce, nawet wtedy, gdy w danym momencie pojawia się wolna szczelina. Takie podejście nie pozwala na efektywne wykorzystanie dostępnego pasma. Z drugiej strony, ścisłe przypisanie użytkownikowi pasma ma również swoje zalety. Pozwala na deterministyczne określenie maksymalnego opóźnienia związanego z zadaną transmisją. Jest to szczególnie ważne w przypadku transmisji głosu i obrazu, gdzie zmienne opóźnienia są niedopuszczalne. Sieci wykorzystujące technikę TDM są prostsze, łatwo konfigurowalne i nie wymagające stałego nadzoru. Jednak są one zestawiane na stałe bez możliwości dynamicznego dostosowywania się do zmieniającego się natężenia ruchu i rekonfiguracji w przypadku awarii połączeń. Poniżej przedstawiono schematycznie obie techniki wykorzystywania pasma.



Podsumowując, technika TDM nie zapewnia wykorzystania w elastyczny sposób całego dostępnego pasma, a co za tym idzie nie nadaje się do przenoszenia ruchu o silnie zmiennym natężeniu. Nie istnieją mechanizmy umożliwiające zlikwidowanie dużych kolejek na pojedynczych, chwilowo przeciążonych kanałach TDM. Jednocześnie użytkownik musi ponosić koszty dzierżawienia kanału nawet wtedy, gdy nie wykorzystuje go do transmisji danych. Warto zaznaczyć, że względy ekonomiczne odgrywają w takiej sytuacji bardzo ważną rolę.

Multipleksowanie statystyczne kanałów logicznych w jedno łącze fizyczne pozwala na udostępnianie tanich sieci wirtualnych przy użyciu tych samych linii. Są one niezależne od połączeń fizycznych co pozwala radykalnie obniżyć koszty. W trakcie eksploatacji możliwe jest przenoszenie silnie zmiennego ruchu, który w swoich ekstremach może przekraczać wielkość pasma, za które płaci użytkownik. Jednak ta technika wymaga medium transmisyjnego o minimalnej stopie błędów i inwestycji związanych ze sprzętem sieciowym.

3. Frame Relay - jedna z technologii przełączania pakietów

Frame-relay należy do grupy technologii, które opierają się na koncepcji przełączania pakietów. Pod pojęciem pakietu rozumiemy jednostkową porcję informacji przesyłaną przez sieć. Do tej rodziny należy zarówno: najstarsza i najlepiej udokumentowana technologia X.25, jak i najnowsza ATM (Asynchronous Transfer Mode). Często dla odróżnienia od X.25, frame-relay i ATM określa się mianem technologii *szybkiego przełączania pakietów*. Podstawowe różnice między nimi dotyczą:

- podejścia do problemu korekcji błędów;
- wymagań nakładanych na medium transmisyjne;
- długości jednostkowej porcji informacji przesyłanej przez sieć;
- stopnia wdrożenia.

Głównym celem projektantów technologii X.25 było zdefiniowanie protokółu umożliwiającego transmisję danych poprzez sieć publiczną, używaną do tej pory tylko do transmisji głosu. Poziom techniki teletransmisyjnej, a także jakość fizycznego medium z definicji zakładały wysoką stopę błędów i niskie prędkości (9600 kbps) przy transmisji danych. Wymagało to stworzenia wewnątrz protokołu mechanizmów korekcji i retransmisji pakietów. Komunikacja między użytkownikami odbywa się na zasadach nawiązywania połączenia i zestawiania sesji, podczas której wymieniane są informacje. Niezawodność transmisji realizowana jest za pomocą mechanizmów potwierdzeń między kolejnymi węzłami. W przypadku frame relay i ATM założeniem podstawowym jest zmniejszenie stopy błędów do poziomu: 10^{-10}. Co za tym idzie, nie wprowadzono mechanizmów korekcji i retransmisji na poziomie protokółu sieciowego. W stosunku do X.25, frame relay całkowicie rezygnuje z kontroli przepływu danych. Te zadania pozostawiono wyższym "inteligentnym" warstwom modelu ISO OSI. Obie technologie mają zastosowanie na szybkich łączach. W przypadku frame relay jest to prędkość podstawowa 2MB, a w przypadku ATM 155 i 655MB. Warto zaznaczyć, iż teoretycznie przy wykorzystaniu ATM możliwa jest transmisja z prędkościami Gigabitów na sekundę .

Zmienna długość ramki charakteryzuje zarówno X.25 jak i frame relay. Protokół frame relay nie specyfikuje ograniczeń, jednak w praktyce implementuje się jako maksymalną długość 1600 bajtów. W X.25 administrator sieci określa maksymalną długość pakietu. W standardzie ATM długość podstawowej porcji informacji tzw. celki jest stała i wynosi 53 bajty. Pozwala to określić wielkość i niezmienność opóźnień na poziomie, który umożliwia transmisję głosu i obrazu.

Protokół X.25 definiuje styk użytkownika z urządzeniami sieciowymi poprzez trzy pierwsze warstwy modelu ISO OSI, frame relay koncentruje się na pierwszych dwóch, natomiast ATM wprowadza własny czteropoziomowy model odniesienia.

Frame relay w swoich generalnych założeniach jest podobne do X.25. Zakłada tworzenie połączeń logicznych czyli tzw. kanałów wirtualnych (Virtual Circuit). Dotychczas zostały zaimplementowane tylko stałe kanały logiczne (Permanent Virtual Circuit), natomiast prace nad przełączanymi kanałami wirtualnymi (Switched Virtual Circuit) trwają nadal. Podobnie jak w X.25 definiuje styk między użytkownikiem a siecią na zasadach na DTE /DCE (Data Teminal Equipment/Data Circiut-terminating Equipment). Natomiast w technologii ATM możliwe jest wykorzystanie zarówno trybu bezpołączeniowego jak i połączeniowego.

Ostatnim aspektem jest stopień wdrożenia omawianych technologii. X.25 jest od wielu lat ogólnoświatowym standardem, używanym w wielu sieciach publicznych. ATM jest bardzo młodą technologią i pozostaje jeszcze wiele problemów związanych z procesem standaryzacji i implementacji. Z tego powodu na razie ATM jest w początkowym etapie wdrażania i upłynie co najmniej kilka lat zanim stanie się stabilnym, ogólnoświatowym standardem. Technologia frame

relay jest zestandaryzowana i od kilku lat z powodzeniem wykorzystywana. Miniony rok - 1994 był okresem niezwykłego rozwoju sieci frame relay. Zainteresowanie tą technologia spowodowały dwa czynniki :
- konkurencyjność cenowa
- wysoka efektywność transmisji dla prędkości do 2MB.

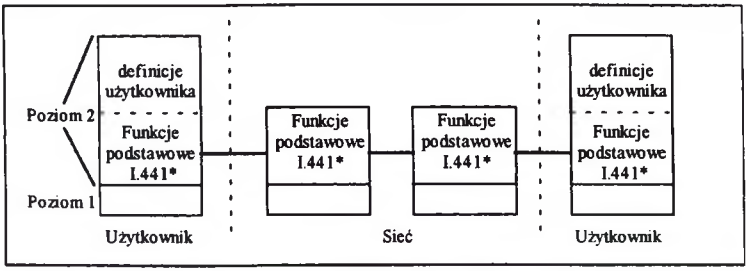
Podsumowując, Frame-relay znajduje się na drodze pomiędzy obecną epoką X.25, a nową wizją sieci kreowaną przez technologię ATM. Zapewnia najlepsze rozwiązanie na dziś i łatwą migrację do przyszłych technologii.

4. Przebieg procesu standaryzacji Frame-relay

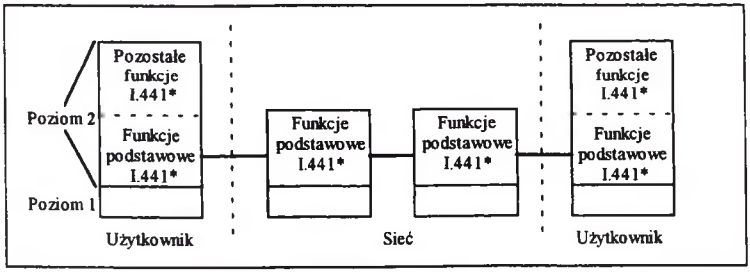
Najważniejszymi organizacjami, które zajmują się tworzeniem oficjalnych, międzynarodowych standardów w dziedzinie teleinformatyki są:
- CCITT (Comité Consultatif International Télegraphique et Télephonique), a dokładnie
- ANSI (American National Standards Institute)
Podstawowe dokumenty, z których wywodzi się współczesny kształt technologii frame relay powstały właśnie w tych organizacjach. Frame-relay nie powstało jako samodzielna, niezależna technologia. Pierwsze opracowania zostały zawarte w grupie dokumentów definiujących standard ISDN. Dotyczyły protokołu transmisji danych charakteryzującego się:
- wysoką efektywnością,
- ograniczonymi mechanizmami korekcji błędów,
- niskimi opóźnieniami transmisji
Jednak pod wpływem presji producentów zdecydowano się na wyodrębnienie powyższego protokołu i stworzenie standardu, który miałby zastosowanie również poza siecią ISDN. Komitet standaryzacyjny CCITT zdefiniował w 1988 roku specyfikację I.122. Zawiera ona definicję czterech różnych trybów przesyłania pakietów:
- Frame relaying 1
- Frame relaying 2
- Frame switching
- X.25-based packet mode

Pomijając tryb oparty na protokole X.25, pozostałe trzy specyfikują sposób implementacji podstawowych funkcji dotyczących transportu ramek. Wszystkie bazują na zaleceniu I.441* opisującym procedury kontroli łącza. I.441* składa się z podzbioru protokołu I.441 i jednocześnie jest rozszerzeniem protokołu LAPD.
Definiuje następujące funkcje podstawowe:
- rozmiar i strukturę ramek
- technikę oznaczania końców ramki
- sposób multipleksowania/demultipleksowania ramek na podstawie adresów
- sprawdzanie długości ramki
- detekcje błędów transmisji
Zgodnie z założeniami protokołu frame-relay nie znajdujemy w nim procedur kontroli przepływu danych, kolejności ramek, odtwarzania ramek. Te problemy zostały przeniesione na poziom wyższych warstw, upraszczając i przyspieszając sam proces przekazywania ramek. Jedyną akcją spowodowaną wykryciem błędnego bitu jest porzucenie całej ramki. Problem retransmisji należy do urządzeń końcowych, a konkretnie aplikacji użytkownika. Sieć w porównaniu do wcześniejszych rozwiązań "traci" swoją inteligencję na rzecz urządzeń końcowych użytkownika. Ta pozorna "strata" procentuje w postaci minimalnych opóźnień przełączania.

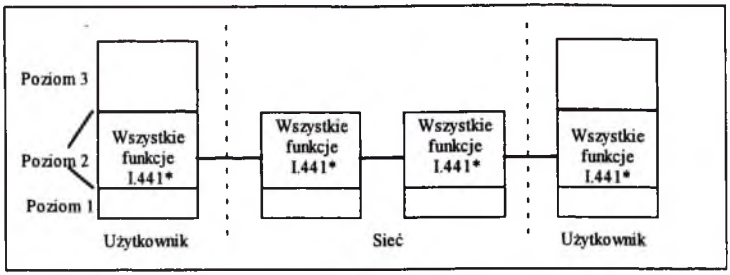
Pierwszy z trybów (frame relaying 1) przekazywania ramek pozostawia użytkownikowi swobodę implementacji wyższych warstw łącznie z częścią warstwy drugiej czyli procedur kontroli przepływu itd. Obowiązkowe są tylko procedury podstawowe zalecenia I.441*. Warto zwrócić uwagę, że są one realizowane przez urządzenia końcowe. W przypadku drugiego trybu (frame relaying 2), cała warstwa druga czyli zarówno funkcje podstawowe, jak i inne są realizowane przez zalecenie I.441*. Ponownie całość działa w oparciu o urządzenia użytkownika. Inne podejście do problemu przedstawia tryb transmisji oparty na przełączaniu ramek. (frame switching). Całość zalecenia I.441* jest implementowana w warstwie drugiej jednak w oparciu o urządzenia należące do sieci. Omówione tryby przesyłania pakietów przedstawiono schematycznie na rysunkach.



Frame relaying 1



Frame relaying 2



Frame switching

5. Frame Relay Forum

Podstawowe dokumenty CCITT i ANSI określiły ramy protokołu, jednak pozostało wiele zagadnień szczegółowych wymagających dodatkowych regulacji. Firmy zajmujące się konstrukcją urządzeń sieciowych i upowszechnianiem technologii frame-relay postanowiły przyspieszyć proces standaryzacji. Podjęły aktywne działania mające na celu stworzenie organizacji, której zadaniem byłoby kreowanie i rozpowszechnianie rozwiązań technicznych. W ten sposób pewne zalecenia stawałyby się "de facto" standardem jeszcze przed oficjalnym ich zatwierdzeniem przez komitety CCITT i ANSI. Założycielami i inicjatorami całej akcji były cztery firmy:

- Digital Equipment Corporation (DEC)
- Northern Telecom
- Cisco
- Stratacom

Pierwszym krokiem "grupy czterech" - taką bowiem nazwę przyjęła organizacja, było opracowanie na podstawie zaleceń komitetu ANSI i CCITT dokumentu zawierającego istotne rozszerzenia specyfikacji frame-relay. Ułatwiło to współpracę między urządzeniami i zapewniło zgodność na poziomie protokołu. Inne firmy bazując na wprowadzonych rozszerzeniach zaczęły dostosowywać swoje urządzenia i programy akceptując podane zalecenia "grupy czterech". Z powodu rosnącej liczby korporacji, które chciały korzystać z powstających rekomendacji a także mieć wpływ na ich przyszły kształt, zdecydowano się na utworzenie Frame Relay Forum. W tej chwili czyli na początku 1995 roku organizacja skupia blisko 100 firm, korporacji. Dla porównania w momencie powstania 16 listopada 1990 roku liczyła sobie 21 członków. Oprócz firm produkujących urządzenia sieciowe, dostępowe i monitorujące, w pracach Frame Relay Forum biorą udział przedstawiciele dużych operatorów publicznych.
Struktura Frame Relay Forum przedstawia się w następujący sposób:

- Komitet techniczny zajmuje się uzgadnianiem standardów implementacyjnych. Uwzględnia zarówno uwagi sprzedawców jak również użytkowników sprzętu. Dba o zgodność interfejsów różnych firm, tak aby zapewnić ich funkcjonowanie w obrębie jednej sieci. Drugim istotnym elementem jest współpraca z międzynarodowymi organizacjami standaryzacyjnymi.

- Komitet promocji stawia sobie jako główne zadanie - rozpowszechnianie technologii frame-relay. Promuje rozwiązania techniczne za pomocą pokazów i szkoleń kreując zainteresowanie oraz popyt ze strony rynku. Organizuje konferencje, seminaria, a także prezentacje na wszystkich większych targach międzynarodowych.

- Komitet normalizacyjny jest odpowiedzialny za przeprowadzanie testów i prób. Koncentruje się na weryfikacji zaimplementowanych standardów pod kątem ich zgodności z innymi urządzeniami. Dba o to, by rozwiązania zaproponowane przez różnych sprzedawców w warunkach rzeczywistych współpracowały ze sobą.

Tadeusz Wiśniewski

Urządzenia sieci szkieletowej frame relay.

W wyniku przeprowadzenia przetargu na dostawę urządzeń dla utworzenia szkieletowej sieci frame relay została wybrana firma Ascom Timeplex. W ofercie tej firmy znalazły się urządzenia typu Enterprise Router (ER) oraz Integrated Access Node (IAN), które mogą pełnić funkcje węzłów i koncentratorów sieci frame relay.

1. Urządzenia typu Enterprise Router

Obecnie dostępne są dwie wersje urządzeń typu Enterprise Router, umożliwiające instalację 15-tu lub 5-ciu kart typu IRP (Independent Routing Processor) w jednej obudowie. Karty te mogą komunikować się ze sobą poprzez magistralę danych o łącznej przepustowości 1.9Gbps, dodatkowo podzieloną na 3 segmenty w celu zapewnienia ciągłości komunikacji pomiędzy kartami IRP w przypadku uszkodzenia jednego z segmentów magistrali. Zdublowana jest także szyna sterująca magistralą danych. Istnieje możliwość instalacji w systemie dwóch niezależnych elementów zarządzających pracą magistali systemowej. W przypadku konieczności wymiany kart IRP, operacja ta może być wykonana bez konieczności wyłączenia napięcia zasilającego. Ponadto konstrukcja urządzeń typu Enterprise Router zapewnia możliwość instalacji dodatkowego zasilacza, mogącego w przypadku awarii przejąć funkcje jednego z zasilaczy podstawowych.

Karty IRP mogą być wyposażone w następujące interfejsy fizyczne :
- 4 porty Ethernet (AUI)
- 2 porty Token Ring
- 1 port FDDI
- 4 porty V.35
- 4 porty V.11/X.21/RS-449
- 1 port ISDN BRI (2B+D) wraz z 1 portem V.35 lub V.11

W planach produkcyjnych firmy Ascom Timeplex znajdują się karty IRP pełniące funkcje styku z siecią ATM (Asynchronous Transfer Mode) oraz koncentratora frame relay (funkcje karty Branch Nodal Processor zostaną opisane w części poświęconej urządzeniu typu Integrated Access Node). Podstawową funkcją urządzenia typu Enterprise Router jest praca jako węzeł sieci frame relay. Firma Ascom Timeplex zaimplementowała system adresowania globalnego oznaczający, że każde urządzenie użytkownika dołączone do tej sieci posiada swój unikalny numer - tzw. adres DLCI (Data Link Connection Identifier). Dla danego urządzenia końcowego definiowane są na węźle frame relay parametry transmisyjne takie jak : CIR (Committed Information Rate), EIR (Excess Information Rate) oraz możliwy jest wybór wartości priorytetów transmisji. Firma Ascom Timeplex zaimplementowała w wewnętrznej sieci frame relay protokół routingu Express Routing przełączający ramki na poziomie drugim (w modelu odniesienia ISO/OSI) bez komentowania zawartości w polu informacyjnym tych ramek. W przypadku połączenia sieci frame relay zbudowanej w oparciu o produkty firmy Ascom Timeplex z siecią frame relay innego operatora dostępny jest protokół Network-To-Network Interface (NNI).
Oprócz podstawowej funkcji przełączania ramek frame relay urządzenie Enterprise Router może także pełnić funkcję routera następujących protokołów :

- IP, IPX, XeroxXNS, DECnet, AppleTalk

wraz z następującymi protokołami routingowymi :

- OSPF, RIP, EGP, Remote IPX RIP, AppleTalk RMTP, DECnet phase IV.

Urządzenia Enterprise Router pracujące jako routery mogą być połączone ze sobą za pomocą następujących protokołów :

- LAPB, PPP, X.25, ISDN-BRI, SMDS, Frame Relay.

Możliwe jest także utworzenie sieci frame relay o oparciu o urzadzenia Enterprise Router i równoczesne wykorzystywanie ich jako routerów wyższych warstw komunikujących się ze sobą przez sieć frame relay.
Urządzenia te mogą być zarządzane za pośrednictwem lokalnej konsoli dołączanej do kart IRP lub też za pomocą systemu zarządzania opartego o protokół SNMP.

2. Urządzenia typu Integrated Access Node.

Urządzenia typu Integrated Access Node składają się zasadniczo z dwóch oddzielnych bloków funkcjonalnych : modułu Access Router (AR) oraz modułu Branch Nodal Processor (BNP). W module Access Router mogą być zainstalowane maksymalnie 2 karty wyposażone w następujące interfejsy fizyczne :

- 2 porty Ethernet (AUI)
- 24 porty Ethernet (10baseT)
- 1 port Token Ring
- 2 porty V.35
- 2 porty V.11/X.21/RS-449
- ISDN BRI (2B+D)

Od strony funkcjonalnej moduł Access Router w urządzeniu typu Integrated Access Node może pełnić takie same funkcje jak poszczególne karty IRP w urządzeniach typu Enterprise Router tzn. wchodzić w skład sieci frame relay oraz pełnić funkcje węzła frame relay i/lub pracować jako router protokołów wyższych warstw.
Kolejnym blokiem funkcjonalnym wchodzącym w skład urządzenia Integrated Access Node jest Branch Nodal Processor. Może być on wyposażony w maksymalnie 5 dwuportowych kart posiadających następujące interfejsy fizyczne :

- V.28 oraz V.35.

Moduł Branch Nodal Processor może pracować jako węzeł sieci X.25 umożliwiając dołączanie użytkowników pracujących za pomocą protokołu X.25 oraz jako PAD (Packet Assembler Disassembler) dla użytkowników asynchronicznych dołączających się za pomocą protokołu X.28. Możliwa jest także praca według protokołów SNA/SDLC , 3270 Bisync, Burroughs Poll Select, tunelowanie protokołów typu BOP (Bit Oriented Protocol) oraz praca transparentna w trybie asynchronicznym z pominięciem bloku X.25. Moduł Branch Nodal Processor jest połączony z modułem Access Router za pomocą wewnętrznego łącza synchronicznego. Urządzenie typu Integrated Access Node może być zarządzane za pośrednictwem lokalnej konsoli lub też za pomocą systemu zarządzania opartego o protokół SNMP.

3. System zarządzania Enterprise Vision

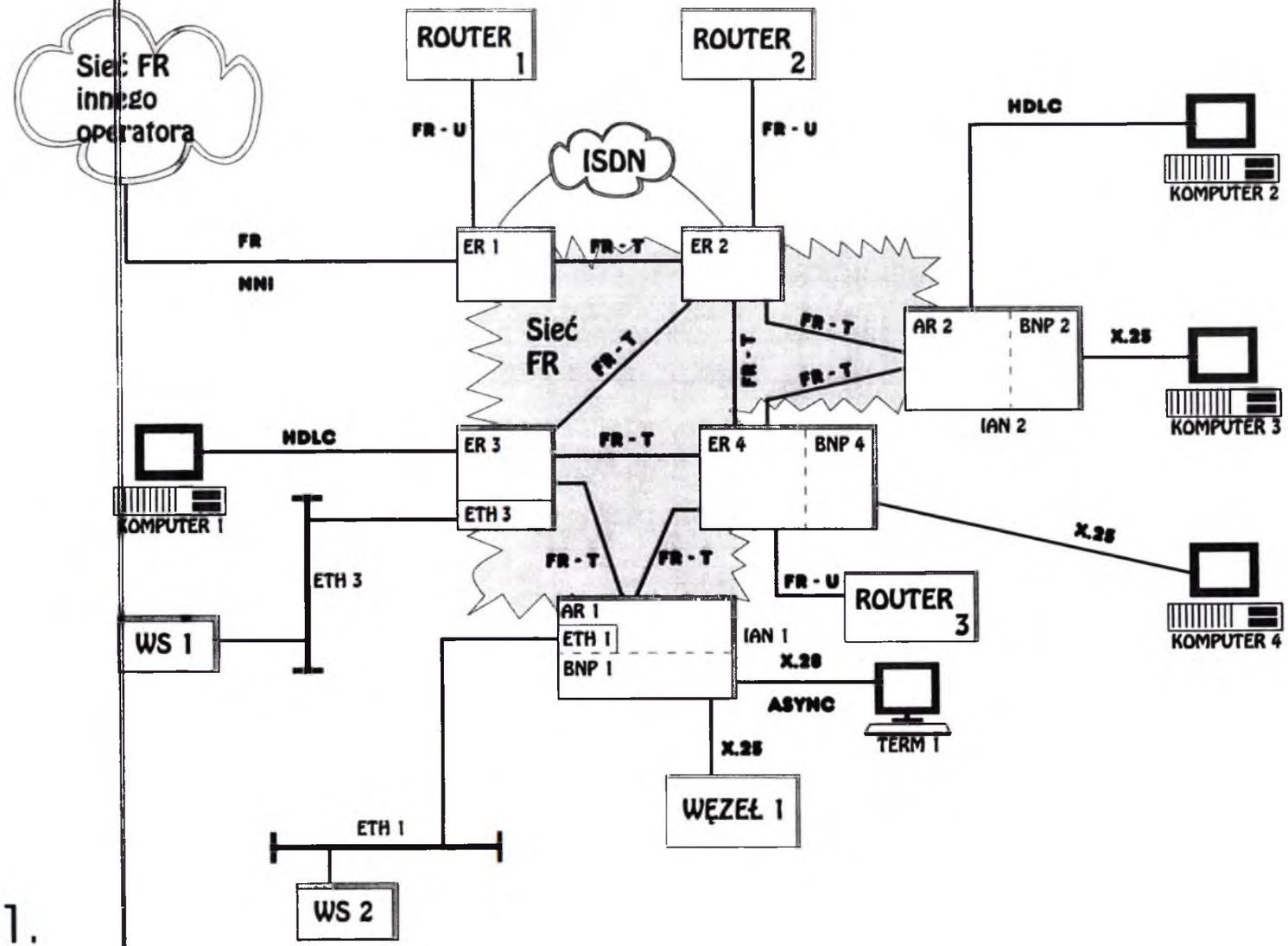
System zarządzania Enterprise Vision jest przeznaczony do zarządzania produktami firmy Ascom Timeplex. Wykorzystuje on jako platformę programową system OpenView firmy Hewlett-Packard. System Enterprise Vision dysponuje wygodnym interfejsem graficznym użytkownika z możliwościa graficznej reprezentacji topologii sieci, prezentacji pojedynczego urządzenia oraz wyświetlenia statusu poszczególnych modułów składowych. Automatyczna procedura umożliwia generację topologii sieci (np. frame relay) i prezentację dołączonych do niej urządzeń. Inne cechy systemu zarządzania to zbieranie danych statystycznych, monitorowanie wykorzystania zasobów sieci i urzadzeń wchodzących w jej skład, automatyczne śledzenie topologii sieci, dokonywanie zmian konfiguracyjnych i śledzenie procesu przeprowadzania zmian, utrzymywanie informacji o konfiguracji urządzeń w bazie danych, wyświetlanie statusu połączeń sieci i stanu poszczególnych urządzeń, monitorowanie i wizualizację zdarzeń zachodzących w sieci, możliwość definicji dopuszczalnych wartości parametrów sieci wraz z generowaniem alarmów w przypadku ich przekroczenia, diagnostykę węzłów i dokumentowanie topologii sieci.

4. Przykładowa konfiguracja sieci zbudowanej w oparciu o urządzenia typu Enterprise Router i Integrated Access Node

Na rysunku 1 przedstawiono przykład wykorzystania części możliwości funkcjonalnych urządzeń typu Enterprise Router oraz Integrated Access Node. W tym przypadku pełnią one funkcje węzłów i koncentratorów sieci frame relay oraz routerów sieci opartej o protokół TCP/IP. Urządzenia ER1-4 oraz IAN1 i IAN2 są połączone ze sobą za pomocą wewnętrznego protokołu frame relay (na rysunku połączenia te oznaczono jako FR-T) tworząc sieć bazową. Wybór drogi podstawowej oraz drogi zapasowej pomiędzy tymi urządzeniami jest dokonywany przez firmowy protokół Express Routing. Do ER1 została dołączona za pomocą protokołu Network-To-Network Interface sieć frame relay zarządzana przez innego operatora. Sieć frame relay przedstawiona na rysunku 1 tworzy między innymi szkielet dla sieci TCP/IP zbudowanej o oparciu o routery 1, 2 i 3 oraz moduły routerów IP ETH1 i ETH3 wchodzące w skład urządzeń odpowiednio ER3 i IAN1. Routery te mogą być ze sobą logicznie połączone na zasadzie kazdy z każdym (w sieci frame relay zdefiniowane są stałe kanały wirtualne PVC pomiędzy każdą parą routerów) nie zależnie od fizycznej struktury połączeń w wewnętrznej sieci bazowej frame relay. Ewentualne uszkodzenie linii łączącej ze sobą urządzenia ER lub IAN i związany z tym wybór linii obejściowej jest dokonywany na poziomie sieci frame relay, a nie przez routery IP. Dodatkowo w przypadku awarii linii łączącej urządzenia ER1 i ER2 następuje automatyczne odtworzenie połączenia przez sieć ISDN. Do urządzeń ER3 oraz IAN2 dołączone są za pomocą protokołu HDLC komputery 1 i 2. Protokół HDLC jest w tym przypadku tunelowany przez sieć frame relay tworząc połącznie typu punkt-punkt pomiędzy komputerami 1 i 2. Moduły Branch Nodal Processor (BNP) zainstalowane w urządzeniach ER4, IAN1 oraz IAN2 pełnią funkcje koncentratorów frame relay. Wewnętrzne połączenie pomiędzy modułami BNP i AR zrealizowane jest za pomocą protokołu frame relay. Sieć X.25 składa się w tym przykładzie z węzłów X.25 - bloków funkcjonalnych w modułach BNP2 i BNP4 oraz zewnętrznego węzła 1. Terminal 1 umożliwia asynchroniczny dostęp do np. komputera 3 lub 4 dołączonych bezpośrednio do sieci X.25.

Rys. 2.

W tworzonej sieci szkieletowej frame relay urządzenia typu Enterprise Router będą pełniły funkcje węzłów frame relay oraz urzadzeń dostępowych dla użytkowników dołączających się do sieci szkieletowej za pomocą protokołu frame relay. W przyszłości planuje się wyposażenie tych urządzeń w karty IRP typu BNP. Urządzenia typu Integrated Access Node będa również pełniły funkcję węzłów sieci frame relay oraz routera IP. Moduł funkcjonalny Branch Nodal Procesor umożliwi dołączanie użytkowników niedysponujących urządzeniami z protokołem frame relay. Schemat planowanych połączeń wewnątrz sieci szkieletowej frame relay oraz lokalizacji urzadzeń pokazano na rysunku 2. Do sieci szkieletowej frame relay zostaną dołączone obecnie eksploatowane w NASK sieci TCP/IP (Internet) oraz sieć X.25, które tym samym będa tworzyły sieci wirtualne nałożone na sieć bazową.


Sieć FR innego operatora
ROUTER 1
ROUTER 2
FR - U
FR - U
ISDN
HDLC
KOMPUTER 2
FR
NNI
ER 1
FR - T
ER 2
Sieć FR
FR - T
FR - T
FR - T
AR 2
BNP 2
X.25
KOMPUTER 3
IAN 2
HDLC
ER 3
FR - T
ER 4
BNP 4
KOMPUTER 1
ETH 3
X.25
ETH 3
FR - T
FR - T
FR - U
ROUTER 3
AR 1
ETH 1
BNP 1
IAN 1
KOMPUTER 4
WS 1
X.28
ASYNC
TERM 1
X.25
WĘZEŁ 1
ETH 1
WS 2

Rys. 1.

Bogusław Lisiecki
Telekomunikacja Polska SA

Problemy rozwoju cyfrowej sieci dalekosiężnej TP SA

Sieć telekomunikacyjna będąca obecnie własnością TP SA była budowana i modernizowana przez dziesiątki lat. Stosowano coraz sprawniejsze urządzenia komutacyjne (centrale) i coraz pojemniejsze urządzenia transmisyjne (linie kablowe i radiowe). Rozwój ilościowy i jakościowy był jednak powolny. Przyczyn tego stanu należy szukać w priorytetach rozwoju gospodarczego Polski w tym czasie. Telekomunikacja prawie nigdy nie zaliczała się do gałęzi gospodarki objętych priorytetem.

Na początku bieżącej dekady nastąpił przełom w rozwoju telekomunikacji w Polsce, którego przyczynami było m.in.

- otwarcie możliwości uzyskiwania kredytów z zagranicy, przede wszystkim z Banku Światowego;
- zdjęcie większości restrykcji eksportowych na sprzedaż nowoczesnych technologii;
- wdrożenie nowych technologii w telekomunikacji; systemów cyfrowych i światłowodów.

Zaistnienie pierwszych dwóch czynników było skutkiem zmian politycznych i ekonomicznych w polskiej gospodarce. Natomiast czynnik technologiczny spowodował przewartościowanie wielu pojęć, które dotychczas były w telekomunikacji prawie dogmatami. Przede wszystkim została podważona struktura sieci w postaci piramidy i kompleks zagadnień związanych z tą strukturą. Powstało zapotrzebowanie na zupełnie nowe zaplecze techniczno-rozwojowe TP SA. Zaistniała konieczność zmiany kwalifikacji służb technicznych i zarządzających. Spróbujemy przedstawić ewolucję techniczną dla sieci dalekosiężnej, co pozwoli na przybliżenie pojawiających sie problemów.

Sieć analogowa; początki sieci cyfrowej

Do końca lat osiemdziesiątych dominującymi systemami w sieci dalekosiężnej były komutacyjne systemy elektromechaniczne i elektroniczne oraz transmisyjne systemy analogowe realizowane na kablach współosiowych (systemy o krotnościach 300, 960, 1920 i 2700 kanałów) oraz na liniach radiowych (krotności 960 i 1800 kanałów). Uzupełnieniem linii wsółosiowych i radiowych były kablowe linie symetryczne uwielokrotnione systemami o krotnościach 120 i 60 kanałów.

W sieciach miejscowych dominowały systemy naturalne (łącza na przewodach fizycznych) oraz nieliczne systemy cyfrowe, głównie TCK-30.

Szybki wzrost zapotrzebowania na połączenia międzymiastowe i międzynarodowe oraz wprowadzanie cyfrowych central telefonicznych spowodowały, że sieć oparta o linie analogowe stała się niewydolna, kosztowna i trudna w rozbudowie, nie zapewniająca właściwej odporności i żywotności.

Pierwszymi telefonicznymi centralami cyfrowymi były centrala międzynarodowa w Warszawie i centrala zespolona w Katowicach i 12 central międzymiastowych w ważniejszych miastach w Polsce

Pierwszymi transmisyjnymi systemami cyfrowymi zbudowanymi w sieci magistralnej TP SA były:

- podmorski kabel optotelekomunikacyjny z Koszalina do Danii (Bornholm), wyposażony w system transmisji plezjochronicznej roboczy i rezerwowy, każdy o przepływności 140 Mbit/s;
- cyfrowa linia radiowa Koszalin - Warszawa (również 140 Mbit/s);
- cyfrowy system łączności satelitarnej Intelsat na region Oceanu Atlantyckiego.

Ponadto rozpoczęto w tym czasie budowę kilku linii optotelekomunikacyjnych o znaczeniu lokalnym, głównie w rejonach wschodnim i południowo-zachodnim.

Kompleksowa budowa sieci cyfrowej

Na początku bieżącej dekady podjęto kilka strategicznych decyzji dotyczących rozbudowy sieci telekomunikacyjnej w Polsce, w tym przede wszystkim budowy cyfrowych central międzymiastowych i transmisyjnej sieci dalekosiężnej. Decyzje te mogły być podjęte dzięki pojawieniu się nowych możliwości finansowania rozwoju i złagodzeniu restrykcji eksportowych ze strony COCOM.

W rezultacie pojawienia się nowych możliwości wybudowano prawie 40 cyfrowych central międzymiastowych.

Zdecydowano o przerwaniu budowy linii analogowych i rozpoczęto budowę dalszych linii cyfrowych wyposażonych w urządzenia systemów plezjochronicznych (PDH). W tym okresie wybudowano:

- linię optotelekomunikacyjną łączącą Wybrzeże z południową granicą Polski - Koszalin - Gdańsk - Bydgoszcz - Toruń - Włocławek - Warszawa - Radom - Kielce - Kraków - Cieszyn, z odgałęzieniami do Płocka, stacji satelitarnej w Psarach, Katowic i Bielska Białej. Długość linii wynosi około 1500 km. Wyposażona jest w urządzenia o przepływności 140 Mbit/s produkcji duńskiej firmy NKT;
- linię optotelekomunikacyjną od granicy zachodniej do Olsztyna przez Zgorzelec - Wrocław - Sieradz - Łódź - Warszawę, z odgałęzieniem z Sieradza do Poznania i Bydgoszczy. Budowa była możliwa dzięki pożyczce udzielonej przez Bank Światowy. Długość linii wynosi ok. 1300 km. Wyposażona jest w urządzenia 140 Mbit/s produkcji AT&T;

- szesnaście cyfrowych linii radiowych 140 Mbit/s produkcji NEC (Japonia), budowa również była finansowana z kredytów Banku Światowego. Łączna długość linii wynosi ponad 3000 km.

Cezurą w rozwoju sieci cyfrowej w Polsce był przełom lat 1993-1994, kiedy przekazano do eksploatacji większość z wyżej wymienionych linii. Sieć tych linii zapewniła cyfrowe wiązki łączy dla nowych cyfrowych central międzymiastowych włączanych do eksploatacji w tym samym okresie.

W tym samym czasie mieliśmy połączenia trzech central międzynarodowych w Warszawie, Katowicach i Poznaniu z siecią europejską i światową poprzez linie optotelekomunikacyjne:

- Koszalin - Kopenhaga;
- Zgorzelec - Frankfurt nad Menem;
- Cieszyn - Praga;
- Suwałki - Kowno;

oraz z siecią światową poprzez systemy satelitarne ze stacji naziemnej w Psarach.

Najbliższe plany

W roku bieżącym wybudowane zostaną cyfrowe centrale telefoniczne we wszystkich miastach wojewódzkich.

Do roku 1998 przewidziana jest dalsza rozbudowa transmisyjnej sieci dalekosiężnej (rys. 1), realizowana, ze względów finansowych w dwóch fazach.

W pierwszej fazie, której zakończenie przewidziane jest na przełomie lat 1996/97, zbudowane zostanie około 2600 km linii optotelekomunikacyjnych, co zapewni doprowadzenie cyfrowych wiązek łączy do wszystkich 49 central międzymiastowych w Polsce. W tej fazie zostanie rozpoczęta zmiana struktury sieci transmisyjnej poprzez wprowadzanie systemów synchronicznych (SDH). Nowo budowane linie rozpoczną budowę dwuwarstwowej sieci transmisyjnej:

- warstwa tranzytowa (rys. 3) zapewniająca połączenie 10 z 12 central węzłowych sieci. Przęsła tej warstwy będą wykorzystywać moduły STM-16 (przepływność 2.4 Gbit/s). Warstwa będzie mieć strukturę kratową. Pozostałe dwa węzły będą dołączone poprzez sieć warstwy regionalnej;
- warstwa regionalna (rys. 2) obejmująca 32 z 49 central międzymiastowych tranzytowych. Przęsłą tej sieci będą wykorzystywać moduły STM-4 lub STM-1 (przepływność 622 Mbit/s lub 155 Mbit/s). Warstwa będzie miała strukturę pierścieniową. Pozostałe 17 central będzie dołączone poprzez odgałęzienia (ostrogi),

W tej fazie część linii optotelekomunikacyjnych wybudowanych wcześniej zostanie wyposażona w urządzenia SDH.

W drugiej fazie przewidziane jest wybudowanie około 1700 km linii optotelekomunikacyjnych i osiągnięcie docelowej struktury sieci synchronicznej w obu

warstwach - tranzytowej i regionalnej. Warstwa tranzytowa obejmie wówczas wszystkie 12 central węzłowych. Warstwa regionalna złożona będzie z 12 pierścieni obejmujących 49 central tranzytowych.

Sieć międzynarodowa

Poza wzmiankowanymi wyżej połączeniami optotelekomunikacyjnymi do Danii, Niemiec, Czech i Litwy przygotowywane są budowy innych linii międzynarodowych.

Porozumienie podpisane przez TP SA z Ministerstwem Informatyki i Łączności Białorusi przewiduje budowę w roku 1995 linii optotelekomunikacyjnej z Warszawy do Mińska via Terespol i Brześć.

Analogiczne porozumienie podpisane z operatorem ukraińskim Ukrelektrozwiazok okresla, że w roku 1995 wybudujemy linię optotelekomunikacyjną z Rzeszowa do Lwowa przez Radymno, Jaworów, a w roku 1996 przedłużymy ją do Krakowa.

Podpisano listy intencyjne i podjęto przygotowania do budowy linii:

- do Słowacji z Krakowa przez Chyżne, z terminem zakończenia w 1995 roku;
- drugiej linii do Niemiec - z Bydgoszczy przez Kostrzyń do Berlina; planowane przekazanie do eksploatacji w 1966 roku.

Wybudowanie powyższych linii stworzy warunki dla osiągnięcia dobrej jakości ruchu końcowego i korzystnych tranzytów transmisyjnych. Są to jednocześnie działania w ramach projektu o nazwie Trans Europe Line (TEL), którego inicjatorami były przedsiebiorstwa telekomunikacyjne Polski, Niemiec, Czechosłowacji i Węgier. Obecnie członkami tego projektu są również inni operatorzy telekomunikacyjni z regionu Europy Centralnej i Wschodniej - Austria, Białoruś, Ukraina, Litwa, Słowenia, Chorwacja, Mołdawia i Rumunia. Zainteresowanie przystąpieniem do projektu wyrazili operatorzy z Finlandii, Łotwy i Estonii. Stałymi obserwatorami są Grecja i Turcja. Celem projektu TEL jest zbudowanie sieci linii optotelekomunikacyjnych i wspólna polityka w zakresie wykorzystywania tych linii. Otwarcie pierwszego fragmentu TEL nastąpiło na początku bieżącego roku.

Jedyną drogą cyfrową z Polski do Rosji jest kabel podmorski z Danii do Rosji. Od kilku lat trwają rozmowy w sprawie przedłużenia projektu TEL z Mińska (Białoruś) do Moskwy, ale dotychczas nie dały zadowalających rezultatów.

W połowie bieżącego roku podjęte zostały prace, które określą celowość i możliwość budowy połączenia pomorskim kablem optotelekomunikacyjnym Polski i Szwecji. Prawdopodobnym punktem lądowania kabla w Polsce byłby Kołobrzeg, a w Szwecji Ystad. W przypadku pomyślnego rezultatu negocjacji przekazanie linii do eksploatacji byłoby możliwe w końcu 1996 lub na początku 1997 roku.

Zakończenie

Przedstawione zostały niektóre dokonania i plany w zakresie budowy sieci dalekosiężnej. Równolegle z tą budową prowadzone są działania przy konstrukcji sieci cyfrowych na niższych poziomach, aż do abonenta. Prezentacja przedsięwzięć realizowanych w poszczególnych województwach wymagałaby oddzielnych opracowań - w wielu przypadkach
są to wielkie wysiłki i duże pieniądze.

Rezultatem tych działań będzie osiągnięcie ilościowego rozwoju telekomunikacji w Polsce na poziomie nie odbiegającym od poziomu średnio rozwiniętych krajów europejskich.

Utworzona zostanie sieć podstawowa, która będzie bazą dla tworzenia sieci wtórnych powszechnego użytku (telefonia), sieci teleinformatycznych, sieci telewizji kablowej i innych - organizowanych zarówno przez TP SA jak też przez innych operatorów, którzy nie będą w stanie ponosić kosztów budowy własnej sieci.

Zadaniem Centrum TP SA jest koordynacja działań i organizowanie warunków dla restrukturyzacji zaplecza technicznego i kadrowego firmy.

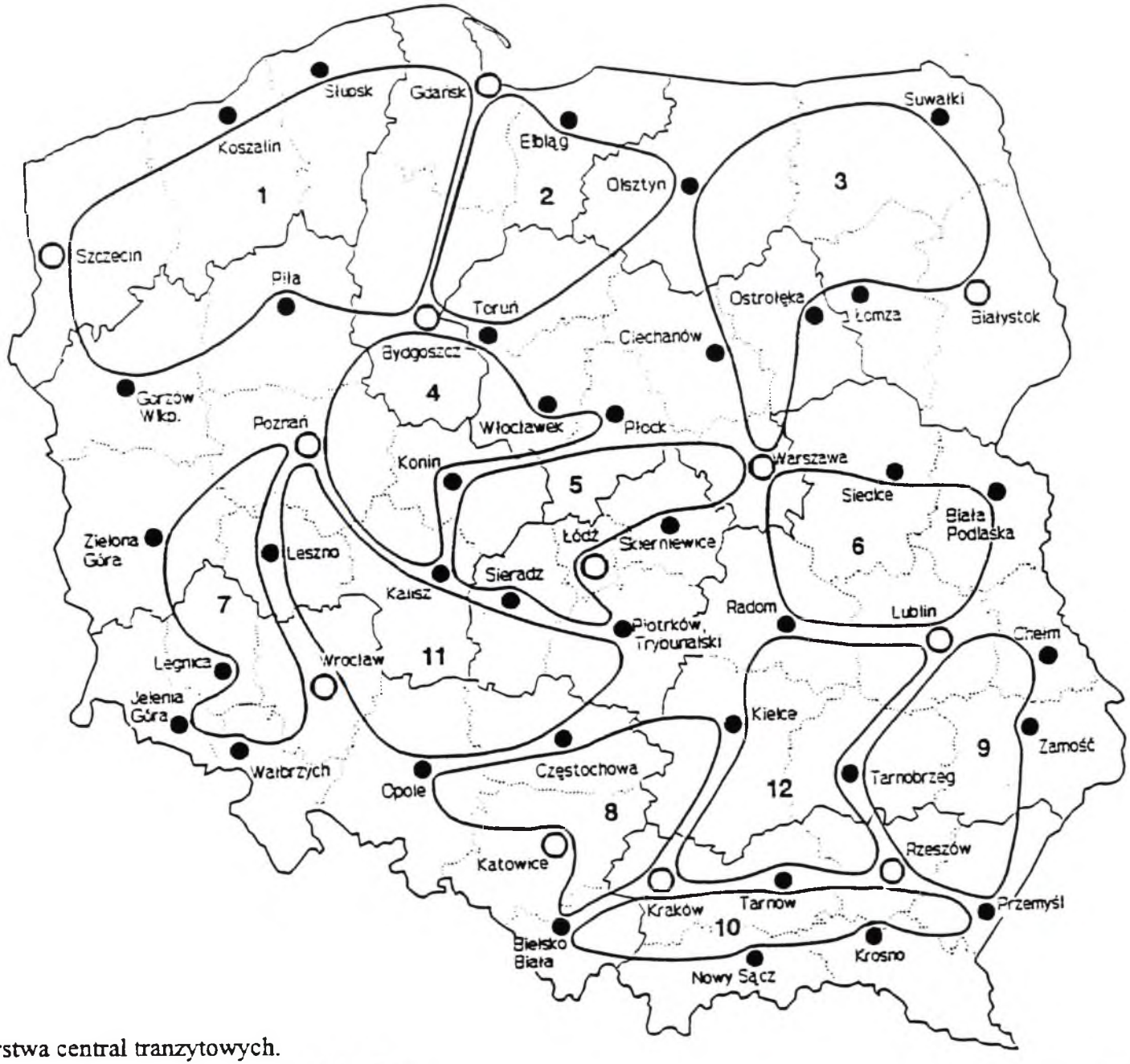
W niniejszym artykule wykorzystano opracowania
Instytutu Telekomunikacji Politechniki Warszawskiej
i Instytutu Łączności w Warszawie.

Rys.1. Sieć pierwotna TP S.A.

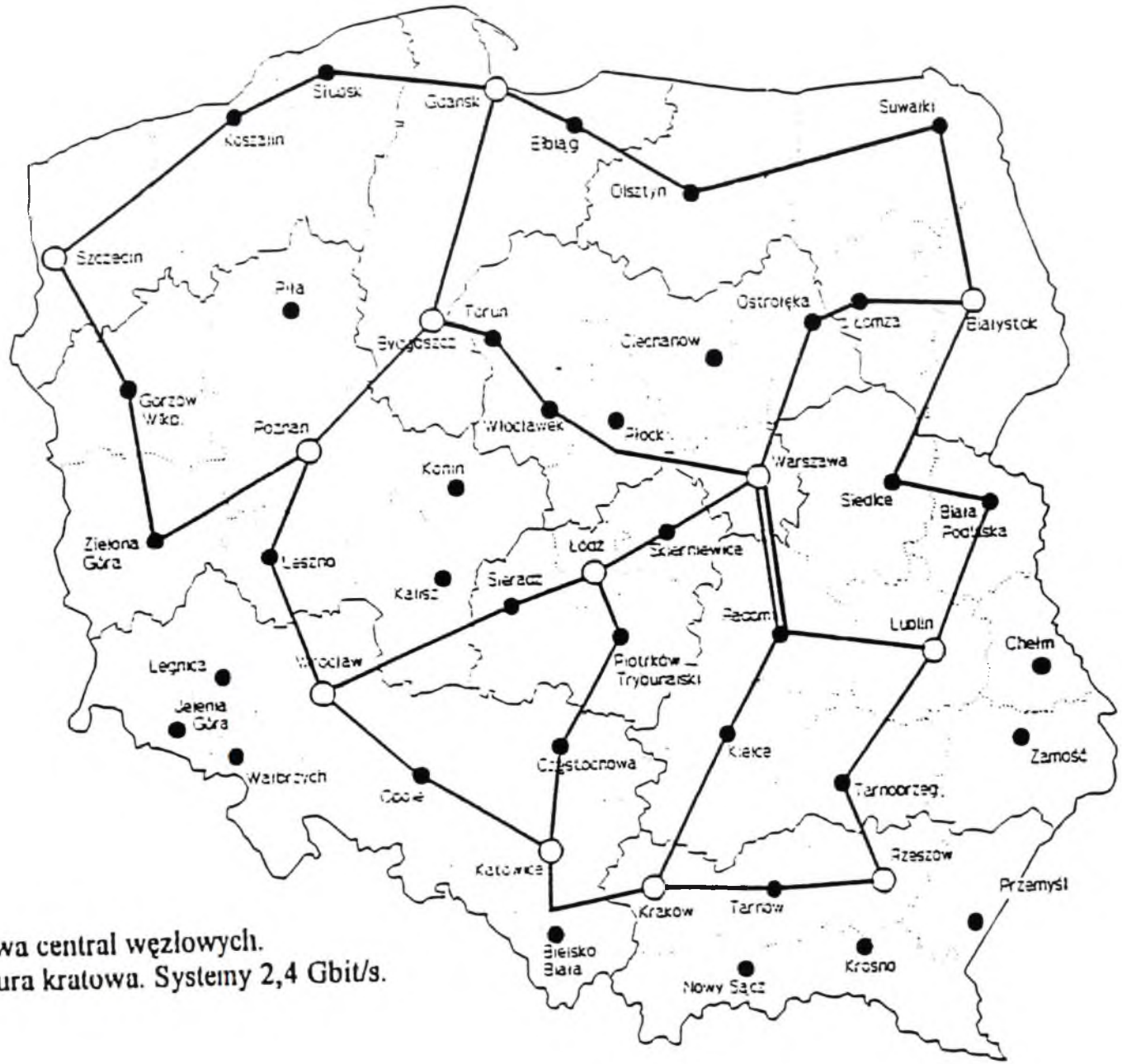
- - - - - - - cyfrowe linie radiowe

——————— linie światłowodowe w eksploatacji

——————— linie światłowodowe planowane do 1996 r.



Rys 2. Warstwa central tranzytowych.
Struktura pierścieniowa. Systemy 622 Mbit/s.



Rys.3. Warstwa central węzłowych.
Struktura kratowa. Systemy 2,4 Gbit/s.

Multimedialna poczta elektroniczna w środowisku SMTP/MIME i X400 w sieci NASK

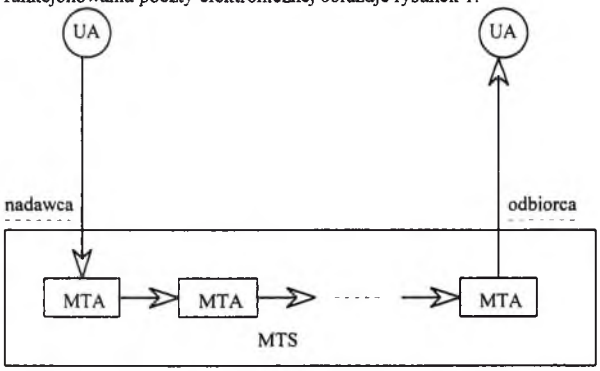
Józef Janyszek

1. Wstęp

W Polsce występują dwa rodzaje sieci rozległych. Jedną z nich jest sieć Internet działająca według protokołu TCP/IP. Obejmuje ona swym zasięgiem głównie środowisko naukowo - akademickie. Ostatnio coraz większe zainteresowanie dostępem do Internetu przejawia również środowisko komercyjne, administracja państwowa, służba zdrowia, szkolnictwo średnie.

Drugi rodzaj sieci rozległych w Polsce tworzą sieci budowane wg protokołu X25. Do największych sieci tego typu należą KOLPAK - sieć komputerowa Polskich Kolei Państwowych, TELBANK - sieć banków polskich, POLPAK - sieć publiczna Telekomunikacji Polskiej SA.

W każdej sieci komputerowej, obok usługi zdalnego dostępu i przesyłania zbiorów, istnieje usługa poczty elektronicznej. Polega ona na przesyłaniu wiadomości (listów) między użytkownikami różnych komputerów lub między różnymi użytkownikami tego samego komputera. Użytkownik wysyłający list korzysta ze specjalnego oprogramowania, które w zależności od środowiska nazywamy User Agent (X400), Klient (SMTP). Oprogramowanie typu User Agent (UA) lub Klient (K) łączy się z innym produktem software'owym, zwanym Message Transport Agent (MTA) w przypadku poczty X400 lub serwerem (S) w przypadku poczty w sieci Internet. Zanim list dotrze do końcowego MTA lub serwera przechodzi przez MTA lub serwery pośrednie. Ciąg MTA lub serwerów uczestniczący w przesyłaniu wiadomości nazywamy systemem przesyłania wiadomości (Message Transport System - MTS). Odbiorca listu korzystając z oprogramowania typu UA lub Klient może list przeczytać. Opisaną powyżej zasadę funkcjonowania poczty elektronicznej obrazuje rysunek 1.



Rys. 1

2. Mulitimedialna poczta elektroniczna w sieci Internet

Poczta elektroniczna jest ciągle rozwijana. Początkowo usługa ta stwarzała możliwość przesyłania informacji alfanumerycznych. Repertuar znaków był ograniczony tylko do kodów ASCII.

Zasady funkcjonowania takiej poczty określa protokoł Simple Mail Transport Protocol (SMTP) opisany w dokumencie RFC 821 (Request For Comments). Obecnie usługa poczty elektronicznej pozwala przesyłać pliki tekstowe, pliki graficzne, pliki typu video, pliki dźwiękowe, pliki związane z konkretną aplikacją, np. postscript. Zasady funkcjonowania rozszerzonej poczty internetowej przedstawia dokument Multipurpose Internet Mail Extensions (MIME) znany jako RFC 1521.

Bardzo często ten rodzaj poczty nazywany jest pocztą multimedialną. Idea tej poczty została wzięta z właściwości systemów operacyjnych Unix. Każdy system Unix posiada komendy: **uuencode** i **uudecode**. Komenda **uuencode** pozwala dowolny zbiór binarny (nie składający się ze znaków ASCII) zamienić na zbiór ASCII. Z kolei komenda **uudecode** pozwala przywrócić zbiór powstały w wyniku działania komendy **uuencode** do pierwotnej postaci. Wykorzystując w/w właściwość systemów operacyjnych Unix zyskuje się możliwość przesyłania zbiorów binarnych, będących np. zdjęciami, zapisami dźwięku i obrazu. Zakodowany zbiór można wstawić do treści listu i przesłać. Odbiorca może zakodowany list przywrócić do postaci pierwotnej. Idea poczty typu MIME wykorzystuje taką samą zasadę ale kodowanie i rozkodowywanie odbywa się automatycznie. Istnieją specjalne techniki kodowania, takie jak: 7bit (siedmiobitowa), quoted-printable, base64, 8bit (ośmiobitowa) i inne. Treść listu może składać się z kilku części. Jest to określone przez typ listu - multipart. Z kolei każda część może być określona poprzez podtyp (subtyp). Występują następujące podtypy: message (informacja), text, image (obraz), audio (dźwięk), video, application (zastosowanie). Każdy podtyp może być jeszcze następnie podzielony na podtypy, czasem zwane parametrami. Przykładowo można podać sekwencję: type/multipart, subtype text/richtext lub type multipart/image/gif.

Podane wyżej informacje o zawartości listu poczty multimedialnej są umieszczone w nagłówku (header). W nagłówku znajduje się też informacja w jaki sposób treść listu (body letter) została zakodowana. Informacje te po stronie odbiorcy służą do odtworzenia treści listu. Dla każdego podtypu określającego rodzaj danych są przypisane dopuszczalne formaty. Określa to tabela 1:

Typ danych	**Dopuszczalne formaty**
text	plain/richtext
image	gif/jpeg
audio	basic
video	mpeg
application	postscript/ODA/ODIF/octet stream

Tabela 1.

Powyższy opis nie zawiera wszystkich możliwości poczty multimedialnej w sieci Internet. Możliwa jest np. kontrola treści listu pod względem nienaruszalności (integrity) wg protokołu MD5, przesyłanie listu częściami (partial) lub dołączenie do treści listu treści zewnętrznej (external body) za pomocą np. usługi ftp. Rozwinęły się też inne protokoły poczty elektronicznej, np. POP3 (Post Office Protocol), które również posiadają możliwości przesyłania danych w różnych formatach.

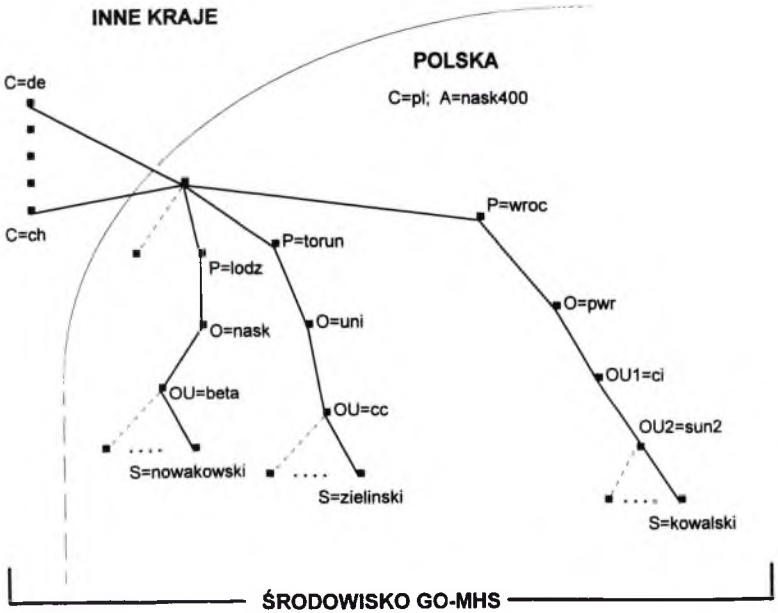
3. Poczta multimedialna w środowisku X400

Poczta elektroniczna w środowisku X400 jest dostępna już w wersji X400(84) i daje możliwości przesyłania zbiorów zapisanych w kilku formatach. Oprócz formatu tekstowego wykorzystującego zbiór znaków IA5 (International Alphabet No5) istnieje możliwość przesyłania zbiorów w formacie teletext, videotext, TIF0. Użytkownik może, korzystać z usługi poczty elektronicznej w środowisku x400 posługując się oprogramowaniem zwanym User Agent

(UA). Format listu zależy od możliwości tego oprogramowania. Oprogramowanie UA formuje list, tworzy nagłówek i jego treść i przekazuje go do węzła poczty X400 zwanego MTA. Schemat przesyłania listów pokazuje rys. 1. Użytkownicy poczty X400 mają również możliwość korzystania z takich usług jak telex, fax, chociaż wersja X400(88) nie posiada już możliwości korzystania z telexu.

4. Poczta X400 w sieci NASK

Usługa poczty X400 w sieci NASK jest realizowana przez jeden węzeł wejściowy MTA - Relay i trzy węzły MTA. Miejsca rozmieszczenia tych węzłów pokazuje rys. 2.



Rys. 2.

Poczta X400 sieci NASK funkcjonuje w środowisku GO-MHS (Global - Message Handle Service). Środowisko to opisuje tabela 2.

Kraj	Nazwa sieci	RELAY-MTA	Sposób podłączenia			
			Internet	Public X.25	Europa-NET X.25	R&D CLNS
Austria	ACONET	1	x	x		
Belgia	BELNET	1	x	x	x	
Chiny	CRN	2		x		
Chorwacja	CARNET	0				
Dania	DENET	2	x	x	x	
Dania	DKNET	1	x	x	x	
Dania	MINERVA	0				
Finlandia	FUNET	1	x	x		
Francja	RED	2	x	x		
Grecja	ARIADNET	1	x	x	x	
Hiszpania	IRIS	1	x	x	x	
Holandia	SURFNET	1	x	x	x	
Indie	ERNET	1	x			
Irlandia	INCIP	1	x	x	x	
Kanada	CDNNET	1	x	x		
Litwa	LITNET	0				
Luksemburg	RESTENA	1		x	x	
Niemcy	DFN	1	x	x	x	
Norwegia	UNINETT	1	x	x	x	
Polska	**NASK**	**1**	**x**	**x**		
Portugalia	INESC	2	x	x	x	
Słowenia	ARNES	2	x	x	x	
Szwajcaria	SWITCH	2	x	x	x	x
Szwecja	SUNET	1	x	x		
Tunezja	IRSINET	1		x		
USA	SNET	2	x			x
USA	XNREN	1	x			
Węgry	HUNGARNET	1	x			
Wielka Brytania	JANET	1	x	x	x	
Włochy	GARR	2		x	x	

Tabela 2

Uruchomiona w sieci NASK usługa poczty realizuje wersję X400(84). Wykorzystuje ona oprogramowanie ISODE/PP.
Dostępne oprogramowanie UA daje możliwość tylko pisania listów w formacie tekstowym.

5. Atrybuty adresowe poczty X400 w sieci NASK

W sieci NASK przyjęto następujące atrybuty adresowe:

G - imię
I - inicjały
S - nazwisko
OU1 - jednostka organizacyjna 1

.
.
.

OU4 - jednostka organizacyjna 4
P - prywatna domena zarządzania
A - administracyjna domena zarządzania
C - kraj

W sieci NASK przyjęto następujące wartości wyżej wymienionych atrybutów:

Atrybut C = pl

Atrybut A = nask400 - wartość tego atrybutu przyjęto arbitralnie z powodu braku ustaleń, kto w kraju i w jakim trybie ten atrybut ma przydzielać

Atrybut P - w sieci NASK wartości atrybutu P korespondują do regionów NASK. Przyjęto zasadę, że wartość atrybutu odpowiada zarejestrowanej, regionalnej domenie internetowej, a więc P może mieć wartości:
P = wroc; P = waw; P = poznan; P = lodz; P = torun; P = gda; itp

Atrybut O - atrybut będzie przyjmował skrócone nazwy istytucji korzystających z usługi poczty X400, np.
O = pwr dla Politechniki Wrocławskiej
O = nask dla JBR NASK
O = uni dla UMK Toruń

Atrybuty OU1 ÷ OU4 - wartościami tych atrybutów w sieci NASK są skrócone nazwy jednostek organizacyjnych organizacji określonych przez atrybut O, np.OU1 = ci dla O = pwr.
Atrybutom OU w sieci NASK przypisano też nazwy komputerów, w przypadku ich występowania w adresach sieci Internet, np.:
OU2 = sun2, OU1 = ci dla P = pwr
OU1 = beta dla P = nask

6. Adaptery (gateways) międzysieciowe dla usługi poczty elektronicznej w sieci NASK

W sieci NASK po wdrożeniu poczty X400, występują trzy różne systemy poczty X400, SMTP (Internet), RSCS (Remote Spooling Communication Subsystem) dla sieci EARN/Bitnet. Konieczne było zapewnienie przesyłania wiadomości między tymi systemami. Dla realizacji tego celu możliwe są trzy rozwiązania konwersji adresów z jednego systemu na drugi:

- konwersja domyślna - kolejne atrybuty adresu X400 opisywane są poddomenami adresu w/g RFC-822 i odwrotnie
- konwersja poprzez tablice (mapping)
- konwersja poprzez wprowadzenie własnego atrybutu tzw. DDA (Domain Defined Attribute).

Ze względu na występujące różnorodne systemy adresowania w polskiej części sieci Internet oraz trudności w konstruowaniu tablic konwersji, zastosowano konwersję poprzez wprowadzenie własnego atrybutu. Wprowadzono prywatną domenę zarządzania P = internet oraz zdefiniowano własne atrybuty:

DD RFC - 822 = internet adres
DD FRC - 822 = bitnet adres.bitnet

Adresy X400 z powyższymi atrybutami zawierają pełne adresy w sieci Internet i Bitnet. Zadaniem gateway'a między pocztą X400 a pocztą SMTP jest odrzucenie części X400 i wysłanie wiadomości pod adres, który zawiera atrybut DD RFC - 822. Z kolei przesyłając wiadomość (list) ze środowiska SMTP do środowiska X400, należy średniki oddzielające poszczególne atrybuty zastąpić kropkami, tak aby kod kraju był na końcu adresu.

7. Usługa poczty multimedialnej w środowisku X400.NASK

Usługa takiej poczty będzie wiązać się z uruchomieniem nowej wersji oprogramowania X400(88) IC 2.1.v2 wytworzonego przez ISODE Consortium. Dostęp do tego oprogramowania jest ograniczony koniecznością płatnego przystąpienia do konsorcjum. Dotyczy to organizacji, które zajmują się udostępnieniem usług sieciowych. Uczelnie mogą otrzymać wymienione oprogramowanie bezpłatnie w ramach tak zwanej licencji bezkosztowej.

IC 2.1.v2 jest wieloprotokołowym węzłem poczty X400 (MTA), który posiada możliwość współpracy z innymi systemami poczty elektronicznej, takimi jak: SMTP (Internet), DECnet Mail (DECnet), UUCP (Unix). Wyposażony jest również w interfejs dostępowy (tylko wyjście) dla modemów współpracujących z faksami. Może współpracować z innymi MTA pracującymi z protokołem P1-1984 jak i z protokołem P1-1988. Wyposażony jest także we wszelkie mechanizmy konwersji, jak: konwersja treści listu (body-part), konwersja typu zawartości (Content-type) oraz konwersja MIME-MHS.

Węzeł poczty X400 zbudowany w oparciu o oprogramowanie IC 2.1.v2 daje możliwość wysyłania poczty multimedialnej (treść listu może być zapisana w różnych formatach), a także stwarza możliwości przesyłania poczty multimedialnej między środowiskami MIME (Internet) i MHS (X400).

Format przesyłanej informacji zależy od możliwości oprogramowania typu UA.

W 1995 roku w sieci NASK planuje się wdrożenie węzłów MTA z IC 2.1.v2 jak i UA pracujących w środowisku MS-Windows i XT-Windows.

8. Uwagi końcowe

Poczta multimedialna możliwa jest zarówno w środowisku SMTP/MIME jak i X400. W sieci Internet istnieje szereg edytorów poczty, które umożliwiają przesyłanie informacji w różnych formatach. Można tutaj wymienić takie edytory, jak: PINE, POP, ELM.

Edytory mogą być wdrażane na różnych platformach sprzętowych (np. SUN, HP, itp). Powszechne użycie poczty multimedialnej (w tym także tekstów z polskimi znakami) wymaga wielu prac organizacyjnych i wdrożeniowych modyfikujących istniejące oprogramowanie na poszczególnych komputerach.

Możliwe jest także wdrożenie poczty multimedialnej w środowisku X400. W sieci NASK prace z tego zakresu zamierza się prowadzić w 1995 roku. Zakłada się, że w 1996 roku będą prowadzone prace z zakresu przesyłania poczty multimedialnej między środowiskami MIME i MHS (X400(88) i ewentualnie X400(92)).

Kompleksowe prace z tego zakresu będą prowadzone we Wspólnocie Europejskiej w ramach projektu PANTOMIME (Advanced Multimedia Elektronic Mail Service in Europe). Zadaniem tego projektu będzie zbudowanie takiej infrastruktury poczty elektronicznej, która umożliwia przesyłanie zbiorów tekstowych oraz zbiorów typu non-ASCII, non IA5, sformatowanych tekstów (Word Perfect, Word, EDI), obrazów, grafów, zdjęć, arkuszów kalkulacyjnych, programów binarnych, bibliotek programów, zbiorów typu audio i video, itp.

Taka kompleksowa usługa poczty elektronicznej powinna również posiadać adaptery do innych serwisów (np. fax) oraz zapewniać oszczędne wykorzystywanie sieci poprzez użycie mechanizmów kompresji. Powinna być jednocześnie powiązana z usługą Directory Service (X500).

KONCEPCJA REALIZACJI POCZTY ELEKTRONICZNEJ X.400 w TPS.A.

Sławomir Michalski
Marian Suskiewicz
Telekomunikacja Polska S.A.

1.Wstęp

Poczta elektroniczna (ang. e-mail) jest popularną nazwą usług zaliczanych do usług dodanych. Usługa ta oferuje użytkownikom szybką wymianę informacji zwanych wiadomościami z wykorzystaniem komputerów i mediów teletransmisyjnych.
Poczta elektroniczna oferuje dużo większe możliwości niż tradycyjne formy międzyludzkiej komunikacji:
- jest usługa asynchroniczną , tzn. nie jest wymagane, aby odbiorca wiadomosci był aktywny (online) wtedy, gdy wiadomość przychodzi;
- jest usługą wieloadresową , pozwala zaadresować wiadomość do wielu odbiorców i przekazać tę wiadomość jednocześnie do wskazanych adresatów;
- jest usługą otwartą, pozwala na wymianę informacji z różnymi innymi systemami przesyłania np. teleksem, telefaksem, itp.
Telekomunikacja Polska S.A. - największy publiczny operator telekomunikacyjny w Polsce - postanowiła rozszerzyć swoje usługi właśnie o elektroniczną wymianę informacji opartą na standardzie X.400.
Po przeprowadzeniu działań marketingowych stwierdzono coraz większe zainteresowanie taką usługą w Polsce i postanowiono zakupić odpowiedni system komputerowy realizujący tę usługę.

Publiczny System Wymiany Wiadomości MHS (*Message Handling System*) otrzymał nazwę POLKOM/400, historycznie nawiązując do eksploatowanego wcześniej w telekomunikacji Systemu Retransmisji Faksów, Teleksów i Telegramów - POLKOM. W stosunku do swego poprzednika, obecny system posiada całkowicie nową jakość realizacji usług publicznych i poza nazwą niewiele ma z dawnym POLKOM'em wspólnego.
W wyniku przeprowadzonego przetargu na Publiczny System Wymiany Wiadomości MHS, oparty na standardzie X.400, TP S.A. wybrała jako integratora i dostawcę, francuską firmę SYSECA. System POLKOM/400 zaproponowany przez tę firmę bazuje na produktach znanego na świecie dostawcy systemów wymiany informacji - firmy ISOCOR. System ten stanowi kompletne rozwiązanie zarówno dla operatora publicznego jak i dla użytkownika końcowego.

2. Ogólne informacje o systemie POLKOM/400

System POLKOM/400 oparty jest generalnie o standard X.400 (84/88/92), który definiuje Publiczny System Wymiany Wiadomości MHS i protokoły wymiany przesyłek:

- Protokół P1 między węzłami pocztowymi MTA (*Message Transfer Agent*)
- Protokół P2 między modułami obsługi użytkowników UA (*User Agent*)
- Protokół P3 między użytkownikami, a węzłami pocztowymi MTA

- Protokół P7 między użytkownikami, a pamięcią wiadomości MS (*Message Store*), w której przechowywane są skierowane do nich przesyłki

Określa on także sposób dostępu najbardziej rozpowszechnionej usługi realizowanej w sieciach komputerowych - poczty elektronicznej, do innych systemów przesyłania wiadomości. Ponadto opisuje elementy koperty elektronicznej, na której umieszczony jest znormalizowany adres nadawcy i odbiorcy oraz takie cechy jak np. pilność, stopień poufności, termin ważności, zawiadomienie o dostarczeniu bądź niedostarczeniu wiadomości itp.
W kolejnej wersji standard X.400 został wzbogacony o elementy bezpieczeństwa zapewniające między innymi: uwiarygodnienie nadawcy i odbiorcy oraz bezbłędne przesyłanie. Ponadto zdefiniowano w nim sposób dołączenia do systemu X.400 takich usług, jak usługa teleksowa, faxowa czy fizyczne doręczenie, polegające na wydrukowaniu i dostarczeniu przesyłki adresatowi, do którego dotarcie inną drogą nie jest możliwe.

3.Architektura systemu POLKOM/400

System POLKOM/400 zostanie dostarczony w przedstawionej na rys. 1 następującej konfiguracji sprzętowej:

-Serwer główny:
- Stratus R5 Risc Fault Tolerant Computer - z dwoma procesorami
- 2 x 64 MB RAM
- 4 x 1.4 GB HDD (disk duplexing)
- 2 Gb DAT (backup cartridge)
- 4 x K118-D12 (64 Kb/s)
- 2 x K124 (2 Mb/s)
- 32 porty asynchroniczne (19.2 Kb/s)

- Serwer komunikacyjny do innych systemów wymiany informacji (PC UNIX/SCO)

- Stanowisko zarządzania systemem (PC/Windows)

- Podsystemy współpracy z abonentami sieci teleksowej i faksowej (DISTEL)

- Moduły obsługi użytkowników (RUA/P7)

- Interfejsy dostępowe (X.25, ASYNC, PAD, ISDN)

4. Podstawowe moduły systemu POLKOM/400

System POLKOM/400 oparty na oprogramowaniu firmy ISOCOR ma budowę modularną. W jego skład wchodzą następujące moduły podstawowe:

- MTA ISOPLEX ADMD

- MS ISOPLEX MS
- X.500 ISOPLEX DS
- ISOGATE (cc:Mail, Ms:Mail, Novell-MHS, Lotus Notes, SMTP)
- ISOTRADE (moduł EDI - *Electronic Data Interchange*)
- ISOMAN (moduł administracji i zarządzania)
- AU (ISOTELEX, ISOFAX, ISOROUTE)
- UA (LUA, RUA, Sec RUA)
- API (MAPI, SSAPI, XOPEN, XDS, FPI)
- ACCOUNTING, BILLING, STATISTICS, ALARMS

Struktura funkcjonalna systemu POLKOM/400 została przedstawiona na rys.2.

5. Opis modułu MTA Isoplex 800

Moduł przekazywania wiadomości MTA odpowiada za transport komunikatów pomiędzy węzłami systemu X.400. Jest on odpowiednikiem urzędu pocztowego sortującego korespondencję. Korespondencja wychodząca jest umieszczana w odpowiedniej skrytce pocztowej jeśli odbiorca jest obsługiwany przez dany moduł, w przeciwnym wypadku, jeżeli adresat nie jest lokalny, wiadomość jest transportowana do innych MTA. Głównym środkiem transportu jest sieć transportowa, a punktem docelowym - zdalny MTA, właściwy dla adresata.
W systemie POLKOM/400 wiadomości mogą być przesyłane po sieci za pomocą następujących protokołów komunikacyjnych:

- RFC 1006 on TCP/IP
- ISO CLNS on 802.3
- ISO CONS on X.25
- Asynchronous with calling mode on PAD X.3/X.28/X.29
- APS on asynchrone connections
- Frame relay

Moduł MTA Isoplex 800 jest całkowicie obsługiwany przez administratora systemu.

6. Opis modułu obsługi użytkownika - UA

Moduł obsługi użytkownika działa jak skrzynka pocztowa rozumiana w/g zasad amerykańskich, tzn. podobnie jak w Europie poczta przychodząca jest przechowywana do momentu jej odebrania przez adresata i odmiennie jak w Europie, w tej samej skrzynce można umieszczać korespondencję do wysłania.
Użytkownik systemu POLKOM/400 postrzega moduł UA poprzez jego oprogramowanie obsługujące dialog. Moduł użytkownika UA wykonuje wszystkie funkcje związane z przygotowaniem, wysłaniem i odbiorem wiadomości. Obejmuje to takie funkcje jak przypomnienie wypełnienia pól adresu, tematu i treści wiadomości oraz np. funkcje redakcji tekstu. Do zadań UA należy również ułatwienie użytkownikowi manipulacji wiadomościami odebranymi z MTA.

W systemie POLKOM/400, poza dowolnymi UA komunikującymi się z MTA za pomocą protokołu P7, posiadamy dwa dodatkowe UA firmy ISOCOR:
- graficzny ISOPRO (GUI for Windows 3.1 and NT)
- znakowy ISOMAIL 800 (for DOS)

7. Opis modułu pamięć wiadomości -MS

Pamięć wiadomości MS jest dodatkową uniwersalną funkcją MHS, która działa jako pośrednik pomiędzy UA i MTA. MS może uzupełniać zaimplementowany na komputerze osobistym moduł użytkownika UA, zapewniając bezpieczny, stale dostępny mechanizm pamięciowy, działający na rzecz UA. UA jest informowany o napłynięciu wiadomości do MS i może ją stamtąd pobrać. Wysyłanie wiadomości przez UA współpracujące z MS polega na przekazaniu wiadomości do MS, która bezwłocznie przekazuje wiadomość do MTA. Na żądanie UA możliwe jest wysyłanie wiadomości przechowywanej w MS.

W systemie POLKOM/400 zaimplementowano następujące sposoby dostępu do MS:

- P7 on X.25
- P7 on X.28 and X..29 (PAD)
- P7 on TCP/IP
- P7 on APS asynchronous connections

W systemie POLKOM/400 usługę X.400 MS realizuje moduł ISOPLEX MS.

8. Opis modułu dostępowego ISOGATE

W systemie POLKOM/400 zaimplementowano współpracę z wieloma popularnymi systemami pocztowymi różnych dostawców, takimi jak:

- MS-Mail
- cc:MAil
- Lotus Notes
- Novell MHS Server
- Internet based on SMTP product
- QuickMail
- DEC ALL-IN-1
- IBM PROFS/Office Vision
- HP Desk Manager
- Banyan Mail
- Wang Office

Komunikacja ze światem internetowym zapewniona jest za pomocą protokołu SMTP (*Simple Mail Transfer Protocol*). Protokół ten określa format wiadomości wysyłanych przez proces klienta w komputerze źródłowym do procesu serwera w komputerze docelowym. Komunikacja

pomiędzy nadawcą i odbiorcą odbywa się w czytelnej formie, za pomocą rozkazów i odpowiedzi reprezentowanych tekstowo. Protokół SMTP jest więc protokołem typu klient-serwer. Pełny opis SMTP można znaleźć w dokumencie RFC 822. Natomiast w dokumencie RFC 1090 opisany jest standard stosowania protokołu SMTP w sieciach X.25, a w dokumencie RFC 1006 w sieciach TCP/IP. Wszystkie te dokumenty zostały między innymi zaimplementowane w module ISOGATE systemu POLKOM/400.

9. Opis modułów ISOTELEX i ISOFAX

Od wielu lat używane są dwa tradycyjne systemy elektronicznego przesyłania informacji: telex i fax. Telex działa jako autonomiczna sieć z własnymi centralami umożliwiająca przekazywanie informacji reprezentowanej w bardzo ograniczonym zbiorze znaków i z małą szybkością (standardowo 50 bodów). Fax natomiast wykorzystuje do przesyłania dokumentów normalną publiczną komutowaną sieć telefoniczną. Usługa ta ma także bardzo istotne ograniczenia.
W systemie POLKOM/400 zaimplementowano dostęp zarówno do sieci telexowej jak i faxowej.

10. Interfejsy programowe - APIs

W systemie POLKOM/400 dostępne są następujące interfejsy programowe APIs (*Application Programming Interface*):

- API ISOPLEX 800 - interfejs programowy MTA
- API XDS++ - interfejs programowy X.500
- ISOTRADE - interfejs programowy EDI
- API X/Open - interfejs programowy UA
- MAPI - interfejs programowy firmy Microsoft
- SSAPI - Security profile provider, Key store provider, Algorithm provider

11. Elektroniczny spis abonentów - X.500

Aby MHS X.400 mógł się stać systemem o zasięgu globalnym konieczne było rozwiązanie problemu implementacji i utrzymania elektronicznego spisu użytkowników. Zagadnienie to jest przedmiotem zaleceń serii X.500, definiujących model funkcjonalny spisu abonentów.
Spis jest zbiorem otwartych systemów współpracujących przy utrzymywaniu logicznej bazy danych o zbiorze obiektów realnego świata. Użytkownicy spisu, którymi mogą być osoby lub programy, mają możliwość odczytu i modyfikacji informacji, pod warunkiem posiadania uprawnień. Podczas dostępu do spisu każdy użytkownik jest reprezentowany przez moduł dostępu do spisu DUA (*Directory User Agent*). Moduł ten jest procesem aplikacyjnym w sensie modelu OSI.

W systemie POLKOM/400 usługę X.500 realizuje moduł ISOPLEX DS.

12. Elektroniczna wymiana danych - ISOTRADE

W oparciu o standard X.400 powstały systemy EDI (Electronic Data Interchange), które pozwalają na przesyłanie gotowych dokumentów wprost między programami przetwarzającymi te dokumenty u różnych użytkowników. Termin EDI oznacza systemy elektronicznego przesyłania dokumentów handlowych takich jak zamówienia, faktury, płatności. Głównymi standardami w dziedzinie EDI są: ANSI X.12 w Stanach Zjednoczonych i EDIFACT (*Electronic Data Interchange for Administration, Commerce and Trade*) w Europie. Oba są zgodne z nowym zaleceniem CCITT X.435 definiującym między innymi sposób wykorzystania systemu X.400 do transportu komunikatów EDIFACT'owych i X.12.

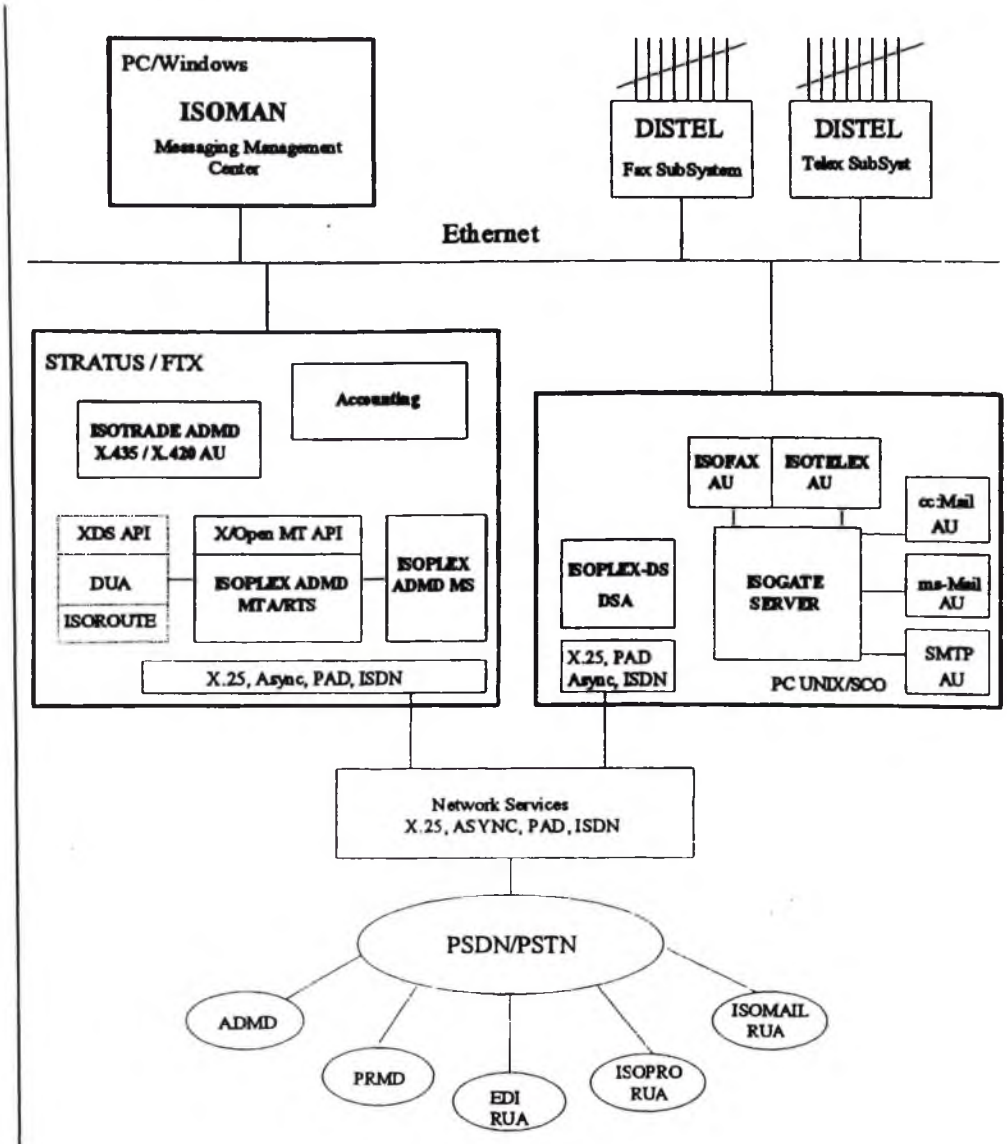
13. Standardy i profile systemu POLKOM/400

Funkcjonowanie systemu POLKOM/400 będzie zgodne z następującymi zaleceniami:

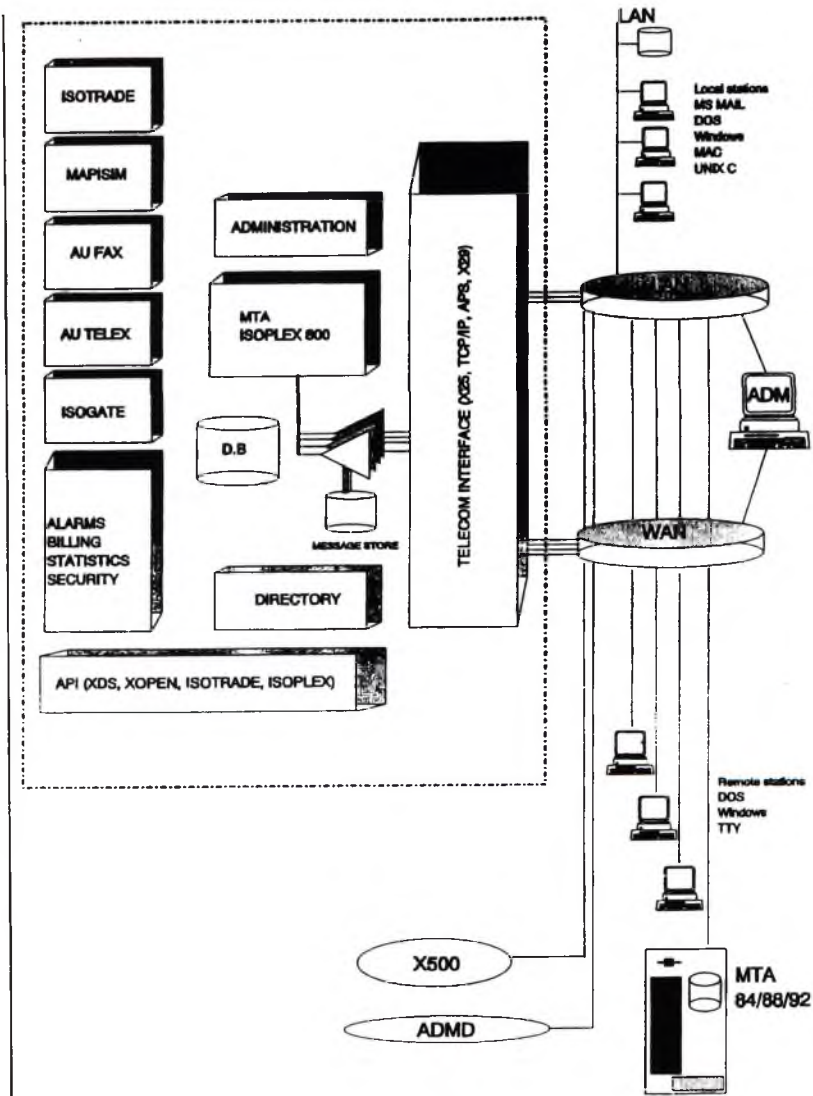
- CCITT X.200 Model odniesienia OSI, X.213, X.214, X.215, X.224, X.225
- CCITT X.400 Model funkcjonalny X.400, X.401, X.409, X.410, X.411 i X.420
- CCITT X.435 Elektroniczna Wymiana Dokumentów - EDI
- CCITT X.500 Spis abonentów X.500, X.509, X.518, X.519, X.520 i X.521
- ISO 7498, 8072, 8073, 8073/AD2, 8326, 8327, 8348/AD1, 8348/AD2, 8473, 8802-2, 8880 i 9542
- ENV 41201 (CEN/CENELEC A/3211)
- ENV 41202 (CEPT A/311)
- NIST SP 500-183
- Australian GOSIP v 2.0
- NORDIC GOSIP
- UK GOSIP v 4.0 i 4.1
- US GOSIP v 1 i 2 (FIPS 146-1)
- OSTC
- TOP 3.0

14. Użytkownicy systemu POLKOM/400

Użytkownikiem systemu POLKOM/400 może zostać każdy, kto posiada zapotrzebowanie na usługi poczty elektronicznej. Z systemu POLKOM/400 może korzystać zarówno indywidualny użytkownik komputera wolnostojącego lub pracującego w sieci lokalnej, jak też serwer sieci lokalnej, abonenci sieci teleksowej, abonenci firmowych systemów pocztowych typu np. cc:mail, abonenci sieci POLPAK lub innych sieci rozległych.
Aby zostać abonentem systemu POLKOM/400 (z chwilą jego uruchomienia) należy zgłaszać swoje zapotrzebowanie do CST -TPSA, administratora systemu POLKOM/400, gdzie będzie można uzyskiwać fachową poradę odnośnie technicznych możliwości dołączania się do systemu i udostępnianych usług.



Rys. 1. : Konfiguracja sprzętowa systemu POLKOM/400



Rys. 2. : Struktura funkcjonalna systemu POLKOM/400

Bogumiła Rykaczewska-Wiorogórska
Uniwersytet Warszawski, Centrum Informatyczne
e-mail: osk06@plearn.edu.pl

NOWE USLUGI INFORMACYJNE W SIECI INTERNET

1. WPROWADZENIE

Pod pojęciem „nowe usługi informacyjne w Internecie" rozumieć będziemy ofertę usług dla użytkowników sieci ze strony firm, które zajmują się profesjonalnie kształceniem, tworzeniem baz danych, promocją oraz wydawnictwami w dziedzinie informacji i bibliotekoznawstwa, a także ze strony zespołów naukowych o podobnym profilu.
Atrakcyjność takiej oferty dla przedstawicieli różnych dyscyplin zawodowych i badawczych jest bezsporna.
Formalnie nowe usługi są świadczone w komercyjnej („com") domenie Internetu, ale zdarza się, że również w narodowych sieciach naukowo-akademickich ([3]). Kwestie płatności za informację są rozwiązywane bardzo różnie. Zakres usług rozciąga się od wyszukiwań bibliograficznych, wyciągów prasowych, po zamawianie szkoleń, rejestrację na konferencjach, prenumeratę czasopism papierowych lub elektronicznych, rekomendację produktów. Cechą charakterystyczną jest dążenie każdego usługodawcy do maksymalnej interakcji z użytkownikiem - klientem i realizowanie jego zindywidualizowanych potrzeb.

Dostrzeżenie korzyści płynących wyłącznie dla odbiorców usług, byłoby tylko przedstawieniem jednej strony zagadnienia. Firmy i zespoły ekspertów są również świadome tego, co osiągają przez „bycie w Internecie".

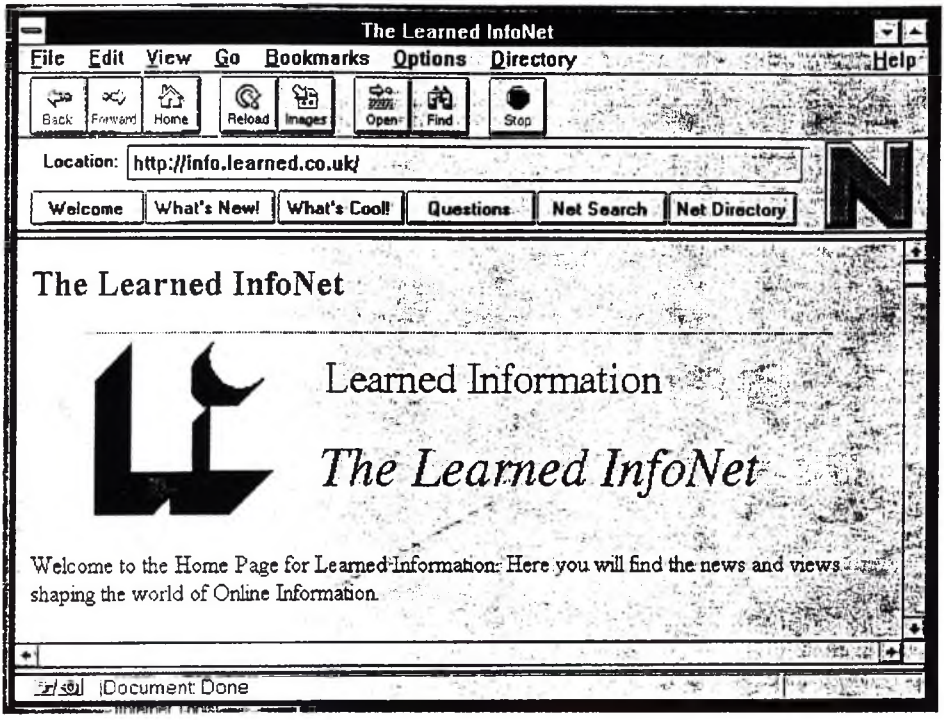
Mary J. Cronin, autorka książki (ubiegłorocznego bestselleru zresztą) pt. „Doing Business on the Internet - How the Electronic Highway is Transforming American Companies" [4] przebadała około 100 amerykańskich i międzynarodowych przedsiębiorstw, pokazując znaczenie włączenia się do Internetu dla ich rozwoju i kokurencyjności.
Najczęściej wymieniane pozytywy, to:
- możliwość kontaktów za pomocą e-mail z konsumentami i kolegami,
- śledzenie standardów,
- wyszukiwanie parametrów towarów,
- łatwy przegląd dostępnych technologii,
- możność stawiania pytań i udzielania odpowiedzi,
- prosty obieg dokumentów,
- szybkie zaznajamianie się z nowymi technikami,
- łatwiejsze realizowanie interesów jak: zakupy i składanie różnych zamówień (tu proponuję zajrzeć do jednego z wcześniejszych moich artykułów [5], w którym jest przykład, jak kupować i wybierać książki za pośrednictwem GOPHERa oficyny wydawniczej).

Funkcjonowanie firmy w Internecie rozpoczyna się zazwyczaj od założenia własnego MAILERA, obsługującego pocztę i serwera WWW, organizującego hipertekstowa, wielopoziomową informację z wyróżniającą się pośród innych „stroną wstępną" ("home page").

Poniższe przykłady pokażą kilka typów nowych usług informacyjnych.

2. PRZYKLADY

I. The Learned InfoNet



Rys. 1

Serwery: <URL: http://info.learned.co.uk>
<URL: gopher://info.learned.ac.uk>

Sieć „Learned InfoNet" została utworzona przez anglo-amerykańską spółkę Learned Information Ltd, znaną przede wszystkim jako organizator dużych konferencji branżowych, specjalistycznych kursów i jako wydawca 8-miu magazynów: „Information World Review", „School Library 2000", „Library Manager", „Online CD-ROM Review", „The Electronic Library", „Monitor", „Expert Systems", „Electronic Documents". Sieć „Learned InfoNet" będzie włączona do katalogu „MATRIX" Johna Quartermana*).

* MATRIX jest to wydawany od 1990 r spis światowych sieci, sewisów i telekonferencji, widzianych od strony świadczonych usług, a nie struktury komunikacyjnej, co jakiś czas aktualizowany przez autora. Można zobaczyć w tym spisie EARN, SURFNet, ale również DIALOG.

The Learned InfoNet

Welcome to the Home Page for Learned Information. Here you will find the news and views shaping the world of Online Information.

Learned NewsWire

The news and views shaping the world of online information, electronic documentation, and library information systems.

Library Manager

Library Manager, the UK manager magazine for librarians aims to engage, inform and at times infuriate, on a wide range of topics from coping with change, coming to grips with technology, and making the most of information resources.

Publications

Information about Learned Information's newspapers, journals and magazines are kept here. Sample copies and subscription information can be obtained.

Conferences

A roundup of conferences focusing on online information, with information, call-for-papers, and registration, with particular focus on the upcoming **Internet World 95**.

Internet Training

This section outlines Learned Information's Internet training courses and activities, and contains registration forms and information.

Who is Learned Information?
Search all menus on the Learned Information server

This searches all document menus on the Learned InfoNet, but is not a full-text full-article database engine. Searches are not case-sensitive.

Feedback about the Learned InfoNet (uses forms)

ben_jeapes@learned.co.uk

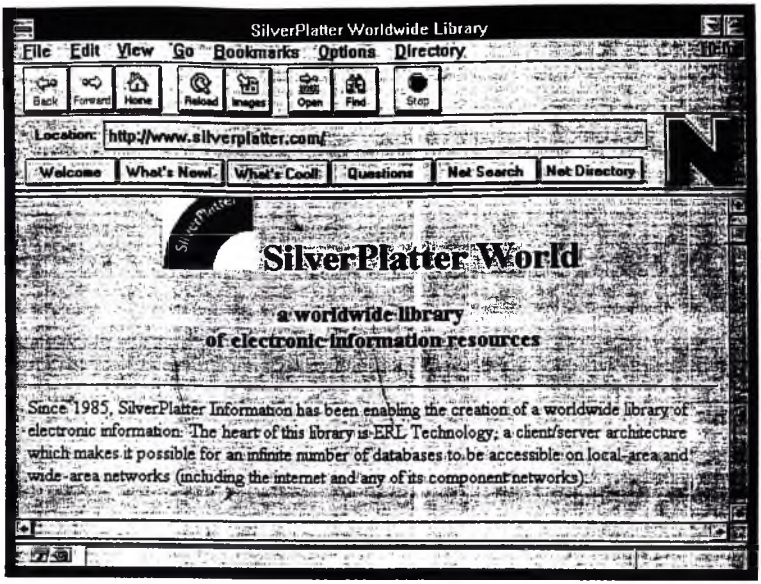
Usługi firmowego serwera WWW zorganizowane są działami, uwidocznionymi na stronie wstępnej - rys.2.

* Learned NewsWire - zawiera informacje o projektach, artykuły z czasopism.
* Library Manager - pełne teksty artykułów z tego czasopisma, listę dyskusyjną „opiniotwórczą" dla jego czytelników, formularz zamówienia prenumeraty przez e-mail.
* Publications - dane o pozostałych publikacjach z możliwością zamówienia i zakupu.
* Conferences - wszystko, co dotyczy licznych, organizowanych przez spółkę konferencji (zgłaszanie prac, rejestracja, i.t.d.).
* Internet Training - wykaz szkoleń, kursów z możliwością zgłoszenia się na nie.
* Inne informacje o spółce -

Dodatkowo uruchomione są 3 serwisy pocztowe:
conferences@learned.co.uk
subscriptions@learned.co.uk
registrations@learned.co.uk
dla tych, którzy nie mogą korzystać z serwerów.

II. Silver Platter World

Firma Silver Platter Information jest producentem około 200 baz, udostepnianych na CD-ROMach oraz tzw. Electronic Reference Library (w skrócie ERL), czyli serwera, umożliwiającego poprzez sieć Internet, jednoczesną pracę wielu użytkowników z kilkudziesięcioma bazami firmy, przeniesionymi na twardy dysk serwera [7]. Opracowany jest program, który ma pozwolić innym twórcom baz wykorzystywać technologię ERL. Może ona mieć szersze zastosowanie w sieciach kampusowych, branżowych albo miejskich.
Serwer nie wymaga odrębnego administratora.



Rys. 3

Serwer infomacyjny WWW:
<URL:http://www.silverplatter.com>
na codzień rozpowszechnia produkty i technologię firmy - patrz „Home Page" (Rys. 4), a podczas promocyjnych imprez czy konferencji może organizować również wolny, zdalny dostęp przez Internet do jakiegoś ERL (od niedawna w taki sposób reklamuje swoje produkty coraz więcej firm). Dodatkowo Silver Platter dysponuje serwisem e-mail (patrz Rys.4).

SilverPlatter World

a worldwide library
of electronic information resources

Since 1985, SilverPlatter Information has been enabling the creation of a worldwide library of electronic information. The heart of this library is ERL Technology, a client/server architecture which makes it possible for an infinite number of databases to be accessible on local-area and wide-area networks (including the internet and any of its component networks).

What's New at SilverPlatter World

Products and Partnerships

Available Information Products | **Products available over the Internet** | **Participating Data Providers** | **Technology Partners**

Technology

ERL | **Client Software** | **Test the Technology**

Training, Support, and Services

Technical Support Frequently Asked Questions | **SPIN-L, an electronic discussion list**

Related Information

Articles | **Press Releases** | **Electronic discussion lists hosted by SilverPlatter**

IntIndex: an index of Internet Resources

Alphabetical | **Subject** | **Contributing to IntIndex**

SilverPlatter World for Physicians

How to contact SilverPlatter | Our FTP Site | Do you have any comments? | This page has been accessed  times since SilverPlatter started offering world wide web access.

If you would like to send us e-mail:

About SilverPlatter World: editor@silverplatter.com | For Technical Support: support@silverplatter.com | About Products and Partnerships: info@silverplatter.com

III. Serwis Informacyjny Londyńskiej Szkoły Businessu (London Business School Information Service - Research Service)

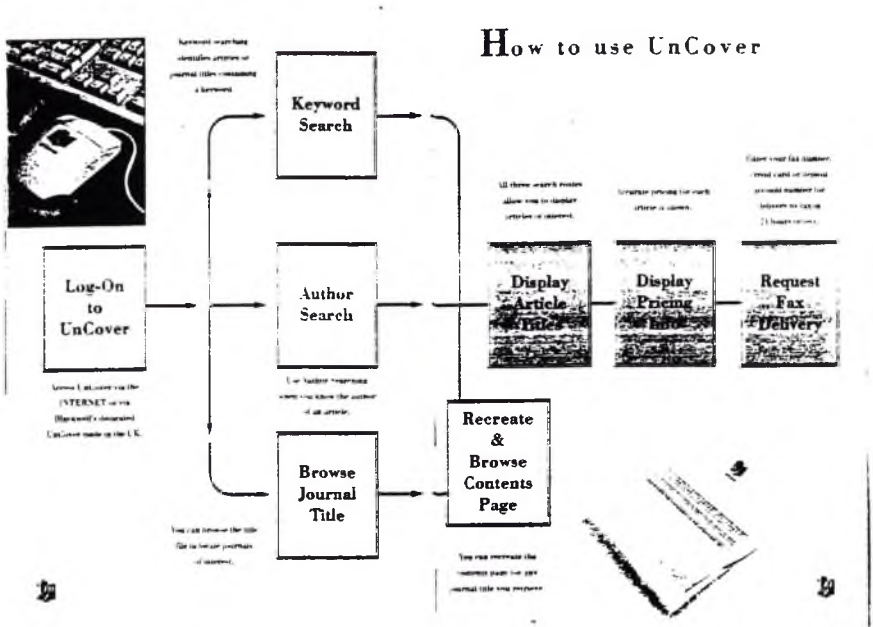
Opisywana teraz usługa zdecydowanie różni się od poprzednich, ponieważ nie wymaga od oferenta posiadania własnego serwera w sieci. Użytkownik przesyła zespołowi konsultantów zlecenie za pomocą e-mail ([8]). Jest to styl świadczenia usług do realizacji przy najprostszym podłączeniu do Internetu, do zaadaptowania szeroko również w Polsce.
Kontakt z konsultantami, pracownikami wyższej uczelni, jest nie tylko przez pocztę elektroniczną, ale też przez fax i telefon. Zespół dysponuje dostepem do około 1000 baz online różnych serwisów i firm światowych oraz do zasobów bibliotecznych uczelni. Podane są wysokości opłat za przekazywane dokumenty i wyszukania on-line. Można być stałym abonentem usług. Wyniki kwerendy przekazywane są na biurko zleceniodawcy.
/e-mail: Infoserve@lbs.lon.ac.uk/.

IV. System IBSS Online

Usługa „International Bibliography of the Social Sciences Online" (w skrócie IBSS) była prezentowana podczas konferencji NSC'94 ([3]). IBSS jest multijęzykową i międzynarodową bibliografią z dziedziny nauk społecznych, dawniej dostępną tylko w formie książkowej, a od stycznia br udostępnioną on-line i jednocześnie powiększoną z około 30 tys. rekordów w książce do 500 tys. w wersji elektronicznej (planowany przyrost roczny - 100 tys. rekordów). Dostęp bezpłatny i nieograniczony do bazy IBSS, posadowionej na SUN SPARK serwerze, mają tylko użytkowncy z placówek akademickich w Wielkiej Brytanii za pośrednictwem centrum BIDS. Pozostali mogą z niej korzystać pod warunkiem wykupienia przez ich instytucję licencji, ewentualnie dotrzeć do IBSS w wersji CD-ROMowej, sprzedawanej przez firmę Silver Platter Information Ltd.
Interesującą organizacją w aspekcie świadczenia usług jest BIDS - Bath Information Data Services, zlokalizowana przy Uniwersytecie w Bath.
Serwer BIDS: <URL: http://www.bids.ac.uk/>
Od kilku lat BIDS ma rangę narodowego punktu dostępu do baz on-line, głównie bibliograficznych i komercyjnych. Finansowane jest z funduszy rządowych oraz ze składek instytucji. Prowadzi również szkolenia, konsultacje i działalność edytorską.

V. Serwis UnCover

Serwis UnCover jest wspólnym przedsięwzięciem dwóch firm, zajmujących się technologiami informacyjnymi i bibliotecznymi: angielskiej - Blackwell Group i amerykańskiej CARL Systems Inc, występujących pod nazwą UnCover Inc. (Rys. 5).



Rys. 5

Serwis daje użytkownikom dostęp do około 5 milionów artykułów z 16 tys. czasopism w języku angielskim bez odchodzenia od biurka. Reklamowany jest jako największy na świecie, codziennie aktualizowany zbiór indeksowanych dokumentów. Obejmuje czasoipsma z zakresu sztuki, humanistyki, nauk ścisłych i społecznych, techniki, medycyny, ekonomii i zarządzania. Wybrany i zamówiony artykuł w ciągu maksymalnie 24 godzin przesyłany jest faxem na biurko (tak było dotąd). Przeglądanie UnCover, tzn. bazy spisów treści czasopism i cytowań artykułów jest darmowe. Płaci się (pokazaną uprzednio cenę) tylko za zamówione teksty. Podsystem „UnCover Reveal" czyli „Odsłaniacz Tytułów" pozwala użytkownikowi wybrać zestaw czasopism i otrzymywać następnie spisy treści kolejnych numerów za pośrednictwem e-mail.

Dostęp do UnCover jest przez Internet i metodą dial-up. Adres do zasięgania informacji:

uncover@blackwell.co.uk

Historia wdrażania sieciowego systemu UnCover opisana jest w książce Mary J. Cronin ([4], 195-201, „... without the distribution power of the Internet, UnCover would never get off the ground.").

3. UWAGI KOŃCOWE

Kilka powyższych przykładów miało wyjaśnić, czym są nowe usługi informacyjne w Internecie. Stanowią one alternatywę dla znanych od dawna serwisów on-line (np. DIALOG czy DATA-STAR) i kompensują braki zasobów, udostępnianych przez klasyczne serwisy (WWW, GOPHER, WAIS, FTP,...) i metaserwisy (VERONICA, JUGHEAD, ARCHIE,...) Internetu - patrz ([1], [2], [6]).

Znane od lat serwisy on-line powstały jeszcze przed epoką burzliwego rozwoju Internetu i można uważać ich stan za stabilny. Nowe usługi natomiast, to efekt konstruowania aplikacji techniką klient/serwer, ułatwiającą udostępnianie ich później interakcyjnie w sieci. Ten kierunek usług będzie rozwijał się bardzo intensywnie na świecie i w Polsce. Przytoczone przykłady pokazały też, że bardzo trudno jest rozróżnić, co jest informacją naukową, a co komercyjną.

Dla środowiska akademickiego i badawczego informacja jest albo wartościowa i przydatna, albo nic nie wnosząca, nawet gdy formalnie traktuje się ją jako naukową. Tradycyjnie środowisko akademickie zawsze korzystało bezpłatnie z bibliotek i centrów INTE, a potem z sieci rozległej NASK. Światowe zasoby informacyjne i usługi dostępne przez sieć współistnieją z konwencjonalnie gromadzonymi zasobami. W sytuacji, gdy prawie wszystkie instytucje naukowe są skomunikowane przez NASK i wzrasta rola kwalifikowanych, nowych serwisów informacyjnych, uważam za bardzo ważną sprawę podjęcie decyzji o promocyjnych zasadach udostępniania informacji naukowej użytkownikom NASK i regułach świadczenia usług, (na przykład konsultacji informacyjnych) z wykorzystaniem NASK.

Bibliografia

[1] B. Rykaczewska-Wiorogórska: Usługi i zasoby sieci naukowo-badawczych (część 3: Nowe usługi informacyjne w Internecie (1)), Praktyka i Teoria Informacji Naukowej i Technicznej, nr 2/1995, ISSN 1230-5529 (kwartalnik).

[2] M. Farbert: The Quality of Information on Internet, Computer Networks for Research in Europe and ISDN Systems, vol 26 (1994), suppl. 2,3, 375-378, ISSN 0169-7552

[3] Ch. Doutney: IBSS Online, czasopismo jak w [2], s79-s93.

[4] M.J. Cronin: Doing Business on the Internet, Van Nostrand Reinhold, New York 1994, ISBN 0-442-01770-7.

[5] B. Rykaczewska-Wiorogórska, E. Kuczyńska: Problematyka chemiczna w sieci Internet, PTINT, nr 2/1994, str. 24-27, ISSN 1230-5529.

[6] B. Rykaczewska-Wiorogórska: Jeszcze raz o problematyce chemicznej w sieci Internet,. PTINT, nr 1/1995.

[7] P. Płóciennik: Electronic Reference Library, Informacja Profesjonalna, nr 1/1994, str.20-22, ISSN 1233-0329.

[8] Folder - „London Business School Information Service", oferta na 1994 rok.

[9] UnCover - Blackwell, in: Information World Review, nr 98, Dec 1994, p.21, ISSN 0950-9879.

[10] Folder - „UnCover - a world of information at your fingertips", wyd. Blackwell.

Analiza związków modelu zarządzania OSI z systemami obiektowych baz danych

Jerzy Brzeziński i Tomasz Koszlajda
Naukowa i Akademicka Sieć Komputerowa JBR

1. Wprowadzenie

Współcześnie konstruowane sieci komputerowe stają się coraz bardziej złożone i w konsekwencji nabiera znaczenia problem efektywnego zarządzania nimi. Zarządzanie sieciami komputerowymi obejmuje problemy obsługi awarii, rekonfiguracji, zagwarantowania odpowiedniego poziomu efektywności działania, rozliczania klientów, ochronę dostępu, itp. Poprawne zarządzanie siecią komputerową wymaga zapewnienia szybkiego dostępu do rzetelnych informacji o bieżącym i historycznych stanach sieci. Wiąże się to z koniecznością gromadzenia danych opisujących globalny stan sieci i związanych z różnymi aspektami procesu zarządzania oraz rozszerzenia systemu zarządzania o funkcje efektywnego składowania i dostępu do tych danych ([Bapa91], [Valt91], [Terp92]). Funkcje te tworzą system bazy danych procesu zarządzania.

Kluczowy dla jakości procesu zarządzania jest wybór właściwego systemu bazy danych do przechowywania danych opisujących stan zasobów sieci, zwanych danymi zarządzania. Po pierwsze, system ten powinien posiadać model danych pozwalający na naturalny i pełny opis różnych aspektów aktualnego i historycznych stanów sieci. Zaproponowany przez komitet standaryzacyjny ISO model zarządzania OSI obejmuje propozycję modelu danych zarządzania. Bazuje ona na obiektowo-zorientowanym modelu danych. Stąd wzięło się zainteresowanie wykorzystaniem do składowania i przetwarzania danych zarządzania obiektowych baz danych.

Drugą wymaganą własnością systemu bazy danych jest zapewnienie poprawności danych zarządzania polegającej na zgodności tych danych z faktycznym stanem sieci. Ponadto, system bazy danych powinien gwarantować efektywne zarządzanie danymi zarządzania uwzględniające istotne ograniczenia czasowe procesu zarządzania.

Niniejszy artykuł zawiera analizę możliwości zastosowania obiektowego systemu bazy danych do implementacji systemów zarządzania sieciami komputerowymi. Jego struktura jest następująca. W rozdziale drugim przedstawiono klasyfikację i charakterystykę danych zarządzania oraz charakterystykę modelu przetwarzania tych danych. Rozdział trzeci zawiera porównanie tych charakterystyk z własnościami obiektowych systemów baz danych. Rozdział czwarty jest podsumowaniem artykułu.

2 Rola systemów baz danych w zarządzaniu sieciami komputerowymi

Podstawą poprawnego i efektywnego zarządzania siecią jest pełna i rzetelna informacja o bieżącym stanie sieci i zachodzących w niej procesach. Efektywny dostęp do informacji o wszystkich komponentach sieci wymaga ich gromadzenia w systemie bazy danych. Jakość zarządzania jest zależna od wierności i pełności opisu zasobów sieci komputerowej przez dane w bazie danych oraz poprawności i efektywności mechanizmów gromadzenia i dostępu do tych danych. Dlatego technologia zarządzania sieciami komputerowymi powinna bazować na dorobku teorii systemów zarządzania bazami danych.

2.1 Model zarządzania sieciami komputerowymi OSI

Przed systemami zarządzania sieciami komputerowymi są stawiane różne cele. Komitet standaryzacyjny ISO/ANSI [Cher87] wyróżnił w modelu zarządzania sieciami komputerowymi sześć dziedzin zarządzania:

1. *zarządzanie konfiguracją systemu* (ang. *Configuration Management*) - umożliwiające reorganizację topologii sieci lub modyfikacje funkcji węzłów sieci;
2. *obsługę awarii* (ang. *Fault Management*) - mającą na celu wykrywanie i lokalizację awarii, informowanie o wykrytych awariach operatorów sieci oraz automatyczne podejmowanie niezbędnych akcji przeciwdziałających skutkom awarii;
3. *optymalizację pracy systemu* (ang. *Performence Management*) - polegającą na wyznaczaniu agregatów opisujących stan sieci i przekazywanie ich operatorom sieci, wspomaganie operatorów sieci w wyborze optymalnych nastaw parametrów sieci oraz automatyczna modyfikacja tych parametrów;
4. *autoryzację i kontrolę dostępu* (ang. *Security Management*), której celem jest zapewnienie bezpieczeństwa zasobów sieci przed niepowołanym dostępem;
5. *rozliczanie klientów* (ang. *Accounting Management*), której celem jest zbieranie i udostępnianie danych umożliwiających obciążanie użytkowników sieci kosztami jej użytkowania;
6. *zarządzanie usługami sieciowymi* (ang. *Directory Management*) - mające na celu ułatwienie poszukiwania przez użytkowników sieci usług sieciowych zlokalizowanych na nieokreślonych węzłach sieci.

Powyższy podział upraszcza funkcjonalną architekturę systemów zarządzania sieciami komputerowymi i umożliwia modularne podejście do projektowania takich systemów. Jednakże, poszczególne dziedziny zarządzania częściowo pokrywają się, co pociąga za sobą konieczność wzajemnej interakcji między podsystemami odpowiadającymi za różne dziedziny zarządzania. Przykładowo dziedziny obsługi awarii i optymalizacji pracy systemu są ze sobą ściśle powiązane, ponieważ niska efektywność sieci jest często jedynym widzialnym symptomem lokalnych awarii o ograniczonych skutkach ukrytych głęboko w systemie. Z kolei, izolacja uszkodzonych fragmentów sieci jest związana z dziedzinami obsługi awarii i zarządzania konfiguracją systemu. Sposobem na koordynację działań modułów programowych związanych z różnymi dziedzinami zarządzania jest wspólna baza danych. Baza ta pełni rolę zbioru informacji o stanie zasobów sieci komputerowej [Kler88], informacji, które są podstawą do poprawnego zarządzania daną siecią komputerową. Z tego powodu baza ta jest nazywana *bazą informacji zarządzania*, w skrócie *MIB* (ang. *Management Information Base*).

2.2 Baza informacji zarządzania

Baza informacji zarządzania (MIB) zawiera dane opisujące stan oraz stałe i modyfikowalne parametry zasobów sieciowych podlegających procesowi zarządzania. Na bazę tę składają się dane związane z poszczególnymi elementami sieci, przeznaczone do lokalnego zarządzania tymi elementami, oraz dane zawierające sumaryczne informacje o globalnym stanie sieci. Można wyróżnić trzy kategorie danych przechowywanych w MIB: dane konfiguracyjne, dane sterujące i dane pomiarowe.

- *Dane konfiguracyjne* są kolekcją statycznych lub rzadko modyfikowanych informacji o bieżącej konfiguracji sieci. Opisują one na przykład: topologię sieci, łącza (ang. trunks), przełącznice (ang. switches), usługi sieciowe (ang. network services) lub klucze kodowania danych. Ze względu na złożoną strukturę sieci dane konfiguracyjne również charakteryzują się dużą złożonością strukturalną. Ta kategoria danych jest podstawą dla zarządzania konfiguracją sieci, kontrolą dostępu i usługami sieciowymi.

  Dla rozbudowanych rozległych sieci komputerowych wolumen danych konfiguracyjnych może osiągać rozmiar do kilku gigabajtów. Większość danych konfiguracyjnych jest składowana w MIB w momencie inicjacji systemu i jest modyfikowana w odpowiedzi na takie zdarzenia jak dodanie (lub usunięcie) nowego węzła sieci, połączenia lub usługi sieciowej.

- *Dane sterujące* są kolekcją danych opisujących bieżące nastawy parametrów umożliwiających strojenie sieci. Do tej grupy danych należą na przykład parametry określające maksymalne przepływy dla poszczególnych łączach, proporcje podziału obciążenia sieci na wyjściach przełącznic lub tablice marszrutyzacji. Oprócz bieżących nastaw parametrów, ta kategoria danych obejmuje również alternatywne zestawy nastaw dla różnych obciążeń i konfiguracji sieci. Na przykład MIB może zawierać dwa zestawy nastaw: dla obciążenia dziennego i nocnego.

  Dane sterujące są wykorzystywane do zarządzania wydajnością pracy i obsługą awarii sieci. W związku z tym, dane te mogą być modyfikowane wielokrotnie w ciągu dnia w celu uwzględnienia charakteru *ruchu* w sieci lub występujących awarii.

- *Dane pomiarowe* opisują dynamicznie zmieniający się stan sieci. Przykładem takich danych są długości kolejek na poszczególnych węzłach sieci, stany łączy lub współczynniki retransmisji danych. Wszystkie te dane są zbierane przez procesy monitorowania sieci. Są one podstawą do określenia stopnia wykorzystania i operacyjnej jakości sieci. Dane pomiarowe są podstawowymi danymi wejściowymi dla modułów zarządzania wydajnością pracy sieci, obsługą awarii i rozliczaniem obsługi klientów sieci. Szacuje się, że w rozbudowanych sieciach wolumen danych pomiarowych może przyrastać o 20 do 30 gigabajtów dziennie [Spri92].

  Dane pomiarowe można podzielić na dwie grupy ze względu na czas ich utrzymywania w bazie danych. Do danych trwałych, to jest danych utrzymywanych przez okres wielu tygodni lub miesięcy, należą informacje o sumarycznym obciążaniu sieci przez poszczególnych klientów, o próbach naruszenia autoryzacji dostępu lub innych sytuacjach alarmowych. Z kolei do danych krótkotrwałych, to jest utrzymywanych w ciągu godzin lub pojedynczych dni, należą dane opisujące dynamiczną charakterystykę pracy sieci. W danym momencie oprócz bieżącego zbioru danych pomiarowych utrzymywane są również historyczne wersje tych danych, dla celów analizy efektywności pracy systemu i występujących w nim awarii.

Mimo daleko posuniętej standaryzacji, rozległe sieci komputerowe są zazwyczaj systemami heterogenicznymi. Elementy składowe poszczególnych podsieci pochodzą często od różnych

dostawców, co powoduje, że różnią się one często protokołami komunikacyjnymi, architekturą i implementacją poszczególnych warstw lokalnego systemu zarządzania. W związku z tym, dla uproszczenia architektury globalnego systemu zarządzania postuluje się wprowadzenie wspólnego modelu danych dla opisu danych zarządzania. Szerzej rozpowszechnione są dwie propozycje takiego standardu. Bazują one na pojęciu tak zwanych *obiektów zarządzania*, które są abstrakcyjną reprezentacją fizycznych zasobów sieci komputerowej. Pierwszy z proponowanych modeli został opracowany przez komitet standaryzacyjny *ISO*. Model ten jest w pełni obiektowo-zorientowany. Obiekty zarządzania są w nim obiektami w rozumieniu paradygmatu obiektowego. Drugi model został opracowany przez *Internet Activity Board* (*IAB*). W modelu tym obiekty zarządzania są implementowane przez zmienne atomowe lub strukturalne, takie jak listy lub tablice.

2.3 System zarządzania bazą danych MIB

Poprawne i efektywne operowanie na wszystkich opisanych powyżej kategoriach danych, wymaga właściwego zarządzania bazą danych MIB. W tym celu należy zastosować odpowiednie oprogramowanie, realizujące funkcje systemu zarządzania bazą danych - DBMS (ang. Database Management System). DBMS bazy MIB powinien spełniać następujące wymagania funkcjonalne:

1. **Praca w czasie rzeczywistym**: Poprawne zarządzanie siecią komputerową wiąże się z dostępem do danych zarządzania zgodnych z bieżącym stanem sieci. Jeżeli stan bazy danych w pełni odzwierciedla stan modelowanej przez nią rzeczywistości to mówimy o spójnym stanie bazy danych. Zapewnienie spójności bazy danych MIB wymaga nieustannego nadążania jej stanu za zmieniającym się rzeczywistym stanem sieci. W asynchronicznym systemie rozproszonym, jakim jest system zarządzania siecią komputerową, niemożliwe jest zapewnienie całkowitej spójności stanu bazy danych. Do takich zastosowań niezbędne jest użycie systemu zarządzania bazą danych czasu rzeczywistego, który umożliwi nałożenie istotnych ograniczeń na stopień niezgodności bazy danych ze stanem rzeczywistym i pozwoli na określenie wiarygodności wartości poszczególnych danych zarządzania. System czasu rzeczywistego umożliwi również nałożenie określonych ograniczeń czasowych na operacje zarządzania siecią, co jest niezbędne na przykład w obsłudze awarii sieci.

2. **Przetwarzanie transakcyjne**: DBMS musi gwarantować transakcyjne przetwarzanie wszystkich kategorii danych. To znaczy musi gwarantować niepodzielność pewnych operacji wykonywanych na danych MIB, oraz spójność i trwałość tych danych. Dla przykładu, zbiór modyfikacji parametrów sterowania siecią w związku ze zmianą obciążenia sieci z dziennego na nocny, lub zbiór modyfikacji konfiguracji sieci w związku z awarią jednego z elementów sieci musi stanowić operację atomową, ponieważ operacje to mają sens tylko wtedy kiedy są wykonane wszystkie razem. W innym wypadku dane MIB mogłyby stać się niespójne. Potrzeba trwałość danych dotyczy w szczególności danych konfiguracyjnych i sterujących, aby po ewentualnej awarii systemu można było powrócić do stanu wyjściowego. Efektywność operacji odtwarzania spójnego stanu danych po awarii ma podstawowe znaczenie dla ciągłości pracy sieci.
   Zapewnienie trwałości danych nie jest natomiast krytyczne dla danych pomiarowych. Utracenie określonej liczby próbek pomiarowych jedynie przejściowo i w niewielkim stopniu może wpłynąć na jakość procesu zarządzania. Natomiast rozmiar wolumenu danych pomiarowych w istotny sposób wpłynąłby na długotrwałość procesu odtwarzania bazy danych.

3. **Zarządzanie współbieżnością transakcji**: Ponieważ na system zarządzania siecią może składać się wiele procesów zarządzania, w danym momencie, w systemie może być inicjowanych wiele transakcji. Z drugiej strony, dane zarządzania mogą być składowane w wielu rozproszonych bazach danych. Wynika stąd, że DBMS musi gwarantować uszeregowalność realizacji rozproszonych transakcji.
   Model przetwarzanie danych pomiarowych posiada wyróżniającą go specyfikę, która może być przesłanką dla modyfikacji mechanizmu synchronizacji transakcji. Źródłem modyfikacji tych danych są narzędzia monitorujące stan sieci. Każda z danych pomiarowych jest modyfikowana tylko przez jeden proces monitorujący. Dzięki temu dla tego typu danych nie występują konflikty typy *zapis-zapis*. Modyfikacje tego typu danych są zazwyczaj niezależne od ich aktualnego stanu. Są to tak zwane modyfikacje typu *blind-writes* [Bern87]. Dodatkowo, dla umożliwienia dostępu do informacji o historii stanów sieci komputerowej dane pomiarowe opisujące charakterystykę pracy sieci powinny być wersjowane. W związku z tym, dane te nie są modyfikowane, a jedynie tworzone są ich nowe wersje. Te specyficzne własności modelu przetwarzania danych pomiarowych, pozwalają na uproszczenie klasycznych mechanizmów synchronizacji transakcji dla tej kategorii danych, co zmniejsza narzut systemowy i może przyczynić się do podniesienia efektywności pracy systemu.

4. **Aktywność systemu bazy danych**: Duża złożoność rozległych sieci komputerowych oraz wymaganie natychmiastowych reakcji na niektóre zdarzenia występujące w sieci, wiążą się z koniecznością wprowadzenia automatyzacji procesu zarządzania. Zapewnienie odpowiedniej efektywności procesu automatycznego wyzwalania procedur obsługi błędów lub zmiany nastaw parametrów sieci w wyniku zajścia pewnych złożonych zdarzeń w sieci komputerowej wymaga z kolei zastosowania aktywnej bazy danych. Bardziej precyzyjne określenie wymagań co do modelu aktywności DBMS wymaga przeprowadzenia dalszych badań (literatura przedmiotu nie zawiera żadnych informacji na ten temat).

5. **Zarządzanie rozproszoną bazą danych**: W heterogenicznej i rozległej sieci komputerowej MIB jest zazwyczaj fizycznie i logicznie rozproszony. DBMS musi zagwarantować efektywny dostęp do danych MIB niezależnie od ich lokalizacji. Wymaga to zastosowania technik fragmentaryzacji i replikacji danych. Zbieranie sumarycznych informacji o stanie sieci wymaga ponadto zastosowania efektywnych algorytmów optymalizacji zapytań rozproszonych.

6. **Wysoka efektywność**: Wymaganie pracy w czasie rzeczywistym w połączeniu z wielkością wolumenu przetwarzanych danych nakładają na DBMS duże wymagania co do efektywności przetwarzania danych. Wiąże się to z koniecznością zastosowania w DBMS efektywnych struktur danych, metod dostępu oraz technik optymalizacji zapytań. Mechanizmy te powinny ponadto uwzględniać semantykę związaną z możliwością wersjowania niektórych danych.

7. **Fault-tolerance**: Ponieważ MIB jest jądrem systemów zarządzania sieciami komputerowymi, DBMS musi zagwarantować bezustanną dostępność danych MIB. Wymaga to zastosowania odpowiedniej architektury systemu i rozszerzenia DBMS o mechanizmy zwiększające odporność systemu na sytuacje awaryjne.

8. **Wspomaganie decyzji**: Systemy zarządzania sieciami komputerowymi powinny wspomagać operatorów systemu w wyborze optymalnych nastaw parametrów sieci, przez udzielanie odpowiedzi na pytania jak zmieni się stan sieci w wyniku zmiany jego

określonych parametrów. Wymaga to rozbudowy DBMS o warstwę oprogramowania systemu wspomagania decyzji. Takie systemy są nazywane dedukcyjnymi bazami danych.

3. Wykorzystanie obiektowej bazy danych do implementacji MIB

Wybór odpowiedniego DBMS do zarządzania MIB ma zasadnicze znaczenie dla jakości procesu zarządzania sieciami komputerowymi. Wymagany w tym wypadku DBMS powinien umożliwiać naturalne modelowanie obiektów zarządzania i jednocześnie powinien spełniać postulowane w punkcie 2.3 wymagania funkcjonalne. Z analizy oferty rynku systemów baz danych wynika, że nie ma obecnie komercyjnego produktu, który spełniałby wszystkie postulowane wymagania funkcjonalne. Jednakże, z drugiej strony ze względu bardzo dużą złożoność tych wymagań niecelowe jest budowanie odpowiedniego DBMS od podstaw dla poszczególnych systemów zarządzania siecią. Racjonalne wydaje się natomiast rozwiązanie polegające na wykorzystaniu istniejącego DBMS o własnościach maksymalnie zbliżonych do tych postulowanych i rozszerzenie go o brakujące własności.

Ze względu na szerokie rozpowszechnienie się zaproponowanego przez ISO obiektowo-zorientowanego podejścia do modelowania danych zarządzania, naturalne wydaje się wykorzystanie jako MIB DBMS obiektowej bazy danych. Poniżej przedstawiono pogłębioną analizę takiego rozwiązania.

3.1 Model danych

Obiektowo-zorientowany model danych wyróżnia się spośród innych modeli dużą siłą ekspresji składających się na niego pojęć. Dzięki temu jest on predestynowany do modelowania złożonej semantyki obiektów świata rzeczywistego. Model ten umożliwia definiowanie dowolnie złożonych struktur danych, licznych typów związków między danymi, własności behawioralnych oraz definiowanie niestandardowych typów danych, takich jak teksty, obrazy lub dźwięki.

Złożoność strukturalna danych zarządzania uzasadnia wykorzystanie do ich modelowania obiektowo-zorientowanego modelu danych. Pozwala to na naturalne wykorzystanie standardu modelowania danych zarządzania zaproponowanego przez komitet standaryzacyjny ISO. Rozwiązanie takie upraszcza proces implementacji przez uniknięcie etapu konwersji modelu obiektów zarządzania do modelu danych bazy danych.

Z drugiej strony semantyka danych zarządzania nie jest na tyle złożona, by wykluczyć wykorzystanie do implementacji MIB systemu bazy danych o innym niż obiektowy modelu danych. Złożoność strukturalna danych zarządzania jest nieporównanie mniejsza niż na przykład złożoność danych w typowych systemach wspomagania projektowania. Ponadto, wedle najlepszej wiedzy autorów, dane zarządzania nie charakteryzują się również dużą złożonością własności behawioralnych, bogatą semantyką łączących je związków lub przynależnością do niestandardowych typów danych, które uzasadniałyby konieczność zastosowania obiektowego modelu danych.

Model danych użyty do implementacji MIB powinien posiadać własność wersjowania danych. Model wersjowania powinien umożliwiać tworzenie zarówno wersji historycznych i alternatywnych. Historyczne wersje niektórych danych pomiarowych pozwalałyby na pamiętanie nie tylko aktualnego stanu sieci, ale również stanów poprzednich w celu umożliwienia łatwiejszego wykrywania trendów zmian w pracy sieci. Alternatywne wersje danych kontrolnych umożliwiałyby przechowywanie w systemie alternatywnych zbiorów nastaw dla różnych charakterystyk pracy sieci. Przyjęty model wersjowania powinien umożliwiać ponadto, definiowanie spójnych zbiorów alternatywnych wersji danych kontrolnych.

Należy zaznaczyć, że własność wersjowania danych jest niezależna od innych własności modelu, to znaczy, że wielowersyjny może być zarówno model obiektowy jak i relacyjny. Wśród znanych komercyjnych i prototypowych obiektowych systemów baz danych, własność wielowersyjności posiadają systemy: Ode [Agra89] i ObjectStore [Lamb91], przy czym ze względu na mechanizm ustalania konfiguracji odpowiadających sobie wersji danych, do wykorzystania w implementacji MIB, bardziej nadaje się model wielowersyjności systemu ObjectStore.

3.2 Funkcje systemu zarządzania bazą danych

Model transakcji: Głównym zastosowaniem obiektowych baz danych są systemy wspomagania projektowania. Dlatego związany z obiektowymi bazami danych model transakcji uwzględnia specyfikę takich systemów, polegającą na długim trwaniu i hierarchicznej strukturze transakcji, bogatej semantyce synchronizowanych operacji oraz konieczności uwzględnienia specyficznych związków łączących obiekty, takich jak kompozycja lub generalizacja. Specyfika modelu transakcji systemów zarządzania sieciami komputerowymi jest całkowicie odmienna. Jest ona za to na tyle bliska klasycznemu modelowi transakcji z zastosowań administracyjno-finasowych, że niecelowe jest wprowadzenia nowego modelu transakcji. Zatem, z punktu widzenia modelu transakcji bardziej racjonalne jest wykorzystanie jako DBMS MIB relacyjnego systemu zarządzania bazą danych: z klasycznymi mechanizmami synchronizacji transakcji i odtwarzania spójności bazy danych po awarii systemu.

- **Zarządzania współbieżnością transakcji**: Dla synchronizacji transakcji w systemach zarządzania sieciami komputerowymi zupełnie wystarczający jest klasyczny algorytm blokowania dwufazowego. Jak już wspomniano w punkcie 2.3, model przetwarzania danych pomiarowych jest pewnym szczególnym przypadkiem ogólnego modelu przetwarzania przez brak występowania w nim konfliktów typu zapis-zapis. Dlatego autorzy niektórych prac, na przykład [Har93], proponują wprowadzenie do DBMS obok algorytmu blokowania dwufazowego, uproszczonego algorytmu dla synchronizacji przetwarzania danych pomiarowych. Takie podejście wymagałoby wykorzystania specjalnej architektury tak zwanego rozszerzalnego DBMS (ang. extensible database system) [Car91].

  Ze względu na ograniczenia czasowe celowe byłoby również usunięcie w przetwarzaniu danych pomiarowych konfliktów typu odczyt-zapis. Można by to osiągnąć przez zastosowanie K-wersyjnego algorytmu synchronizacji transakcji [Morz92].

- **Odtwarzanie spójności danych**: W pracy [Har93], ze względu na konieczność ograniczenia do minimum czasu restartowania systemu po awarii, zaproponowano ograniczenie mechanizmu odtwarzania spójności bazy danych jedynie do danych konfiguracyjnych i kontrolnych. Natomiast, dane pomiarowe mogłyby po restarcie systemu przez pewien czas (to jest do momentu ich okresowej modyfikacji) pozostawać w stanie niespójnym. Również to rozwiązanie wymagałoby zastosowania specjalnej architektury DBMS.

Aktywność bazy danych: Mechanizm aktywności bazy danych nie jest immanentną cechą obiektowego modelu danych. Mechanizm ten jest w ogólności niezależny od przyjętego modelu danych. Może stanowić on rozszerzenie zarówno do obiektowych jak i relacyjnych DBMS. Powstało wiele prac [HiPAC], [Ode] opisujących sposób rozszerzenia obiektowej bazy danych o mechanizm aktywności. Istnieją również pewne prototypowe systemy aktywnych obiektowych baz danych, na przykład systemy Ode lub Postgres. Własności obiektowego modelu danych przyczyniły się do powstania pewnych specyficznych cech związanego z nim modelu aktywności. Na przykład, dzięki własności tożsamości obiektów zdarzenia wyzwalające określone akcje w systemie mogą być definiowane dla pojedynczych obiektów, a zbiór zdarzeń może być rozszerzony o zdarzenia związane z wywoływaniem metod. Jednak brak dogłębniejszej analizy

modelu aktywności wymaganego w systemach zarządzania sieciami komputerowymi utrudnia określenie czy któryś z proponowanych dla obiektowych baz danych modeli aktywności jest odpowiedni dla tej klasy zastosowań.

Praca w czasie rzeczywistym: Rozszerzenie DBMS o możliwość pracy w czasie rzeczywistym podobnie jak w przypadku mechanizmu aktywności bazy danych jest niezależne od przyjętego modelu danych. I podobnie jak w poprzednim przypadku, brak dogłębniejszej analizy wymaganego modelu pracy w czasie rzeczywistym uniemożliwia stwierdzenie przydatności proponowanych w literaturze modeli baz danych czasu rzeczywistego [Grah92, Kort90].

4. Podsumowanie

Niniejszy artykuł jest próbą odpowiedzi na pytanie, czy obiektowe bazy danych są odpowiednim narzędziem do implementacji systemu zarządzania sieciami komputerowymi zgodnie z wymaganiami standardu OSI. Odpowiedzi na to pytanie poszukiwano w dwóch obszarach: możliwości przechowywania danych zarządzania w obiektowej bazie danych oraz przydatności obiektowego DBMS do zarządzania tymi danymi.

Implementacja bazy danych zarządzania MIB za pomocą obiektowej bazy danych pozwala na naturalne wykorzystanie standardu modelowania danych zarządzania zaproponowanego przez komitet standaryzacyjny ISO. Rozwiązanie takie upraszcza proces implementacji przez uniknięcie etapu konwersji modelu obiektów zarządzania do modelu danych bazy danych. Z drugiej strony semantyka danych zarządzania nie jest na tyle złożona, by wykluczyć wykorzystanie do implementacji MIB prostszego modelu danych, na przykład relacyjnego.

Z kolei, analiza wymagań dotyczących zarządzania danymi MIB nie uzasadnia jednoznacznie wyboru obiektowego DBMS do zarządzania tymi danymi. Wymagania te adresują najświeższe osiągnięcia technologii baz danych, które są jednak w znacznej mierze niezależne od przyjętego modelu danych. Jednakże wykorzystanie do implementacji konkretnego systemu zarządzania siecią komputerową komercyjnego DBMS, wskazuje jednoznacznie na relacyjne systemy baz danych, ze względu na większą dojrzałość tych produktów, która wyraża się ich większą efektywnością i niezawodnością. Należy przy tym jednak wyraźnie podkreślić, że na razie nie istnieje żaden komercyjnie dostępny DBMS, który spełniałby wszystkie wymienione wymagania.

W artykule przedstawiono podstawowe problemy konstrukcji systemów zarządzania sieciami komputerowymi, oraz rozwiązania niektórych z tych problemów z użyciem systemów zarządzania obiektowymi i relacyjnymi bazami danych. Niestety pewne problemy zwłaszcza dotyczące pewnych aspektów synchronizacji, aktywności i pracy w czasie rzeczywistym nie znalazły dotychczas zadowalających rozwiązań. Stąd wynika konieczność dalszych badań w tym zakresie.

Bibliografia

[Agra89] 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.

[Bapa91] Bapat, S., *OSI Management Information Base Implementation*, Integrated Network Management, II, eds. I. Krishnan i W. Zimmer, Elsevier Science Publishers B.V. (North-Holland), 1991.

[Bern87] Bernstein, P., Hadzilacos, V., Goodman, N., *Concurrency Control and Recovery in Database Systems*, Adison-Wesley, 1987.

[Car91] Carey, M., et al, *The of the Exodus Extensible DBMS*, in *Object-Oriented Database System*, K.Dietrich, U.Dayal and A.Buchmann, eds.Spring-Verlag, Berlin.

[Cher87] Chernick, M., et al, *A survey of OSI network management standards activities*, Tech. Report NMSIg87/16 ICST-SNA-87-01, National Bureau of Standards, 1987.

[Day94] Dayal, U., Hanson, E., Widom, J., *Active Database Systems*, in *Modern Database Systems* W.Kim, ACM Press New York, 1994.

[Grah92] Graham, M.H., *Issues in Real-Time Data Management*, in *The Journal of Real-Time Systems*, **4**, 185-202 (1992).

[Har93] Haritsa J., et al, *Design of the MANDATE MIB*, Integrated Network Management, III, eds. H. Hegering i Y. Yemini, Elsevier Science Publishers B.V. (North-Holland), 1993.

[Kort90] Korth, H., Soparkar, N., Silberschatz, A., *Triggered Real-Time Databases with Consistency Constraints*, Proceedings of 16th VLDB Brisbane, Australia 1990.

[Kler88] Klerer, S., *The OSI Management Architecture: an Overview*, IEEE Network Magazine, 2(2), March 1988.

[Lamb91] Lamb C., G.Landis, J.Orenstein, D. Weinreb, *The ObjectStore Database System*, Communications of the ACM, Vol.34, No.10, pp. 34-50, October 1991.

[Morz92] Morzy T. *Zarządzanie współbieżnym wykonywaniem transakcji w systemach wielowersyjnych baz danych*, rozprawa habilitacyjna, Politechnika Poznańska - Rozprawy nr. 273, 1992.

[Nak93] Nakai S., *MIB Design for Network Management Transaction Processing*, Integrated Network Management, III, eds. H. Hegering i Y. Yemini, Elsevier Science Publishers B.V. (North-Holland), 1993.

[Spri92] SPRINT Network Management Center, Virginia, Site Visit, April 1992.

[Terp92] Terplan, K., *Communications Network Management*, Prentice-Hall, 1992.

[Valt91] Valta, R., *Design concepts for a Global Network Management Database*, ntegrated Network Management, II, eds. I. Krishnan i W. Zimmer, Elsevier Science Publishers B.V. (North-Holland), 1991.

X.500 — usługa katalogowa w sieci Internet

Maja Górecka
mgorecka@cc.uni.torun.pl

Tomasz Wolniewicz
twoln@mat.uni.torun.pl

Jerzy Żenkiewicz
jezenk@cc.uni.torun.pl

Uniwersytet Mikołaja Kopernika w Toruniu

1 X.500 — standard i jego realizacja

Zgodnie z założeniami, standard X.500 został opracowany dla celów szeroko rozumianej informacji katalogowej wspierającej procesy warstwy aplikacji OSI, jak też procesy zarządzające sieciami zgodnymi z OSI. Jednocześnie chciano wyjść naprzeciw rosnącemu zapotrzebowaniu na dostęp do światowej książki telefoniczno-adresowej — „White Pages".

Dwie organizacje: CCITT (obecnie ITU-T) oraz ISO równolegle prowadziły od roku 1984 prace standaryzacyjne. CCITT definiowało usługę informacji adresowej, a ISO opracowywało zasady nazewnictwa zasobów i usług komputerowych. W 1986 roku nastąpiło połączenie obu grup. Efektem działań było opublikowanie niezależnych standardów CCITT [1] i ISO/IEC 9594 [2], zwanych standardem X.500 '88. Prace nad rozwojem X.500 trwają, tym bardziej, że implementacje usługi według standardu '88 ujawniły wiele słabości i niedociągnięć protokołu. Ostatnio została oficjalnie opublikowana kolejna wersja, oznaczona jako X.500 '93. Jej obszerne fragmenty są już od roku ogólnie znane i dyskutowane, rozpoczęły się też prace nad wdrożeniem nowych cech standardu do programów.

Najbardziej popularnym oprogramowaniem realizującym funkcje X.500 Directory jest QUIPU. Pakiet ten został zaimplementowany przez grupę związaną z University College London w celu utworzenia narzędzia badawczego, demonstrującego możliwości działania rozproszonej bazy X.500 w sieciach rozległych. Początkowo oprogramowanie QUIPU było dostępne ogólnie, od 1993 roku jest ono w gestii organizacji ISODE Consortium, która udziela nieodpłatnej licencji ośrodkom akademickim. Jednocześnie powstały i są nadal tworzone inne implementacje, m.in. NEXOR QUIPU, DEC, UCOM, Siemens.

Rozwój usługi X.500 wiąże się z uruchomieniem serwisu pracującego na wybranym oprogramowaniu i załadować dane. Pierwsze lata działania X.500 były w zdecydowanej większości oparte na entuzjastycznych działaniach i dobrej woli zainteresowanych grup. W 1989 roku wystartowały dwa programy pilotowe: europejski, koordynowany przez Uniwersytet Londyński oraz amerykański, sponsorowany przez US DARPA. Następnie w ramach Europy zainicjowano projekt PARADISE, którego celem była międzynarodowa koordynacja rozwoju X.500 oraz połączenie pilotów europejskich i amerykańskich. W kwietniu 1994 został zakończony projekt PARADISE i opiekę nad usługą X.500 przejęła organizacja DANTE z zamiarem dostarczania na podstawie dotychczasowego pilota niezawodnego, samofinansującego się serwisu. Aktualnie w ramach X.500 oferuje swoje dane 35 krajów a łączną ilość haseł ocenia się na ponad 1.5 mln.

Pod nazwą „White Pages" rozumiemy obecnie międzynarodowy program rozwoju usługi (połącznienie europejskiego programu PARADISE i amerykańskiego „White Pages"). Jednocześnie działa kilka programów zamkniętych, inicjowanych między innymi przez dostawców usług telefonicznych. Programy takie stosują zwykle X.500 w zawężonym zakresie, np. umieszczając w bazach danych wyłącznie dane dotyczące numerów telefonów, miejsca zatrudnienia lub zamieszkania. Ta tendencja powoduje, że ogólnoświatowa rozproszona baza informacyjna X.500, zbudowana zgodnie ze standardem jako struktura hierarchiczna i składająca się, jak dotychczas, z jednego drzewa danych (DIT), będzie musiała uwzględnić możliwość istnienia wielu niezależnych drzew informacyjnych, tworzonych przez odrębne domeny administracyjne.

Jak już wspomniano, w swoim założeniu X.500 miało być stosowane jako usługa „White Pages" (informacja adresowa), przeznaczona zarówno dla celów ogólnych, jak przesyłania poczty elektronicznej w standardzie X.400. „White Pages" ma za zadanie wyszukiwanie osób ze względu na dane osobowe, miejsce pracy lub zamieszkania. W odróżnieniu od „Yellow Pages" nie zakłada się rozległego wyszukiwania według specjalności zawodowej, zainteresowań, czy innych cech charakterystycznych.

Internet zaadoptował standard X.500 jako podstawę usługi katalogowej, mimo że większość środowiska była zdecydowanie przeciwna protokołom CCITT/OSI. Nie było jednak żadnej rozsądnej alternatywy, a X.500 może być eksploatowane na bazie różnych infrastruktur sieciowych. Tempo rozwoju zasobów bazy obsługiwanej przez X.500 nie nadąża za dynamiką Internetu. Jednym z powodów takiej sytuacji była dominacja aspektu protokołu w pracach aktywistów X.500, często prowadząca do oderwania od zadania docelowego — zbudowania niezawodnego serwisu. Internet stosuje metodę tworzenia aplikacji poprzez szybką realizację w jak najprostszy sposób zamierzonego celu, środowisko OSI najpierw przygotowuje jednoznacznie zdefiniowaną i wszechstronną infractrukturę, a dopiero na jej podstawie aplikacje użytkowe.

Obecnie X.500 posiada konkurentów w postaci innych technologii. Coraz szerzej mówi się o niezbędności realizacji w ramach usług katalogowych indeksacji zasobów sieciowych. Planowany protokół wspierający tę funkcję nosi nazwe WHOIS++ i jest dokładniej opisany poniżej.

Jednocześnie jednak X.500 pozostaje funkcjonalnym, elastycznym i wieloplatformowym standardem. Jego nowa wersja '93 pozwala przypuszczać, że kolejne implementacje będą efektywniejsze, a dodanie protokołu replikacji daje prosty mechanizm wbudowania serwerów indeksowych w model strukturalny X.500.

2 Możliwości wykorzystania X.500

Standard X.500 przewiduje w swoim założeniu możliwość zupełnie dowolnego rozszerzania rodzaju przechowywanych w bazie obiektów, co pozwala umieszczać w niej różnego typu informacje. Opierając się na architekturze X.500 można utworzyć bazę gromadzącą np. zbiory biblioteczne, dokumenty itp.

Ogromną zaletą bazy X.500 jest jej rozproszony charakter. Zarządzanie dużą, centralną bazą danych prowadzi na ogół do znacznego pogorszenia jakości utrzymywanych w niej informacji. W X.500 uprawnienia do modyfikacji zasobów ma każdy administrator domeny (tzw. *naming context*). Poprzez powiązanie z danymi odpowiedniej autoryzacji dostępu do nich można zgodnie z potrzebą rozszerzyć zezwolenie na modyfikacje danych, albo oddele-

gować zarządzanie fragmentem drzewa informacji wybranemu administratorowi w ramach organizacji czy instytutu.

Autoryzacja dostępu pozwala również wskazać właściwych odbiorców danych. Dopuszcza się ograniczanie uprawnień do odczytu niektórych haseł, przeszukiwania czy listowania fragmentów drzewa informacyjnego.

Autoryzacja jest możliwa w oparciu o konieczność poświadczania tożsamości przy łączeniu się z bazą X.500, dopuszcza się wprowadzanie różnych poziomów identyfikacji zgłaszającego (*simple*, *strong*).

Standard X.500, pomimo swojego rozproszonego charakteru, używany bywa również jako scentralizowana baza danych, tam gdzie jej hierarchiczna specyfika szczególnie dobrze nadaje sie do wiernego odwzorowywania struktury organizacji instytucji. Wspomiana modyfikowalność rodzaju przechowywanych zasobów jest tu dużym atutem, ponieważ zapewnia prostą skalowalność aplikacji.

Ważną dziedziną zastosowania X.500 jest poczta elektroniczna. Istnieją już pierwsze próby integracji programów obsługi e-mail z dostępem do X.500. Baza X.500 jest naturalnym miejscem przechowywania kluczy publicznych dla celów „bezpiecznej" poczty prywatnej (PEM). Technologia PEM opiera się na koncepcji certyfikatów kluczy publicznych według rekomendacji X.509, dotyczącej aspektu poświadczania w ramach X.500.

W RFC 1491 [4] można znaleźć listę rożnorodnych zaawansowanych zastosowań X.500.

3 X.500 na tle innych usług przechowywania i wyszukiwania informacji

Mówiąc o X.500, bardzo często identyfikuje się ten termin z usługą „White Pages". Krytyka, która wielokrotnie kierowana jest pod adresem X.500 dotyczy w zasadzie samej służby katalogowej.

Naszym zdaniem, kilka powodów decyduje o tym, że „White Pages" jest usługą, którą należy traktować odmiennie od innych serwisów:

- **Typ użytkownika** — użytkownik usługi katalogowej bardzo rzadko jest typem szperacza. Wymaga usługi sprawnej i szybkiej i co najważniejsze niezawodnej. Zawodność usługi może być spowodowana np. niedostępnością określonego serwera, niekompletnością informacji, czy faktem, że pewne instytucje nie wprowadziły swoich danych, albo że format danych jest niejednorodny.

- **Niezbędność usługi** — pomimo, że usługa katalogowa jest jedną z najbardziej pożądanych, wiekszość użytkowników zakłada, że jest ona po prostu niemożliwa do realizacji i, co za tym idzie, nie wymaga jej zainstalowania. Każdy oczekuje sprawnie działającej poczty elektronicznej, FTP, telneta, a więc niezawodnego serwisu DNS. Administrowanie DNS jest przykrą koniecznością, przed którą nie uchyla się żaden administrator — bez tego nic nie działa. X.500 nie ma jeszcze charakteru usługi koniecznej.

- **Koordynacja** — usługa katalogowa musi być częściowo scentralizowana, aby zapewnić minimalną przynajmniej spójność danych. Chodzi tu o koordynację na szczeblu krajowym oraz dostosowywanie się do wzorców światowych. Potrzeba ta jest kosztowna, wymaga spotkań administratorów na szczeblach międzynarodowych i krajowych. W ramach kierowania programem krajowym X.500 konieczne jest rozpoznanie zapotrzebowań użytkowników na usługę i dążenie do udostępniania danych, które są pożądane,

dotyczy to zarówno rodzaju, czy jakości informacji, jak i jej rozległości. Niezbędne jest prowadzenie działalności popularyzacyjnej i zachęcanie środowisk do współtworzenia serwisu.

- **Administrowanie** — „White Pages" musi zawierać aktualne i pełne informacje. Ze względu na dynamikę zmian danych gromadzonych w X.500 Directory oznacza to, że administrowanie jest w zasadzie zadaniem ciągłym, uciążliwym i kosztownym. Specyfika postaci danych w X.500 wymaga przygotowania odpowiednich narzędzi programowych, zapewniających w miarę automatyczne dokonywanie konwersji danych do właściwej postaci, a także sprawdzanie poprawności danych. Z drugiej strony uruchomienie uniwersalnych metod ładowania bazy może w znacznym stopniu poprawić jakość X.500 i wpłynąć na zwiększanie zasobów.

- **Łatwość instalacji** — utarta opinia głosi, że X.500 jest trudne w instalacji i administrowaniu. Wydaje się nam, ze opinia ta nie jest słuszna i przy odpowiednio dostosowanych narzędziach X.500 może uruchomić każdy kompetentny administrator UNIXa. Również utrzymanie podstawowego serwisu nie nastręcza na ogół problemów. Trudności pojawiają się często przy eksploatowaniu rozbudowanej bazy, kiedy trzeba podejmować decyzje wpływające na efektywność działania systemu i gdy bardzo przydatna jest znajomość szczegółów. Tego typu sytuacje powinny być regulowane poprzez działania odpowiednich służb typu *HelpDesk*. Administrowanie szczeblem krajowym jest pod tym względem mocno wyróżnione.

  Z drugiej strony wystartowanie usługi X.500 nie jest zadaniem tak prostym jak uruchomienie *gophera*, czy *WWW*. Wymaga kompilacji całego, rozbudowanego oprogramowania, a następnie odpowiedniej konfiguracji. Udostępnienie danych w ramach X.500 nie może być również porównywane z DNS, czy gopherem, nie tylko ze względu na ilość danych, ale przede wszystkim dlatego, że trzeba, przynajmniej pobieżnie znać dopuszczalną strukturę bazy (typy obiektów, atrybuty opisujące obiekt), by właściwie załadować informacje.

- **Dostępność informacji** — baza danych jest zawsze postrzegana jako potencjalne źródło dochodów, jak również zagrożenie dla prywatności. Z faktów tych wynika, że zdarzają się problemy zarówno z pozyskiwaniem danych jak i ich publicznym udostępnianiem. Docelowo zatem, baza musi być wyposażona w mechanizmy identyfikacyjne, ograniczenia dostępu itp. Przykładowym zabezpieczeniem może być zezwolenie na odczytywanie poszczególnych obiektów bazy z równoczesną blokadą operacji przeszukiwania.

- **Modyfikowanie informacji** — typowe służby informacyjne, funkcjonujące w Internecie są albo bardzo ograniczone odnośnie możliwości przechowywania rozbudowanej informacji (np. DNS), albo dają całkowitą dowolność co do organizacji i zawartości. Skrajnym przykładem jest WWW, które przy swoim lawinowym rozwoju doprowadza do totalnego zamętu i niemożliwości oddzielenia użytecznej informacji od szumu. Usługa „White Pages" nie może zezwalać na tego typu dowolność, musi zawierać informację bogatą, o odpowiedniej jakości, zwartą, tak by np. mogła być wykorzystana do automatycznego tworzenia wyciągów drukowanych. Jednocześnie należy implementować metody wpływania użytkowników na zawartość bazy (np. korygowanie błędów). Administrator domeny musi być odpowiedzialny za jakość informacji w ramach zarządzanego przez siebie poddrzewa. Bardzo istotne jest podejmowanie decyzji

odnośnie rozszerzania zezwoleń na modyfikacje danych w X.500. Istnienie wbudowanych metod poświadczania tożsamości częściowo zabezpiecza bazę. Dodatkowo jednak niezbędne byłyby odpowiednie interfejsy użytkowe, umożliwiające wprowadzanie danych według odpowiedniego schematu, tak aby nie została naruszona spójność formatu (w ramach ogólnych mechanizmów jest ona kontrolowana tylko na zasadzie sprawdzania poprawności składni). Użytkownik powinien móc decydować o zawartości swojego hasła w sposób pośredni, np. poprzez przesyłanie odpowiedniego formularza.

4 Inne technologie realizujące usługę informacyjną

4.1 WHOIS++

Historia protokołu WHOIS++ wykazuje w jak szybkim tempie tworzone są aplikacje internetowe. Prace zainicjowano w połowie 1992, po 15 miesiącach istniały już trzy pracujące implementacje *„public domain"*, trzy kolejne były przygotowywane, powstał również procesor czołowy (*gateway*), łączący WHOIS++ i X.500.

Protokół WHOIS++ rozwinął się jako kontynuacja zdefiniowanego w 1982 roku w ramach Network Information Center (NIC) NICNAME/WHOIS ([5]). Usługa WHOIS umożliwia dostęp do danych o użytkownikach, organizacjach, zasobach sprzętowych i programowych w sieci Internet. Jest ona oparta na scentralizowanej bazie danych, co w dużym stopniu utrudnia jej aktualizację, a przy istniejącym ogromnym rozbudowaniu zasobów internetowych (sprzętowych i „osobowych") utrzymanie centralnej bazy staje się wręcz niemożliwe.

WHOIS++ miał uporać się z problemami hamującymi popularyzację usługi „White Pages", takimi jak:

- utrudnione przeszukiwanie w szerokim zakresie poddrzewa danych,
- brak ogólnie dostępnych, łatwych w instalacji i zarządzaniu implementacji,
- duży balast, jaki niesie z sobą pełna implementacja X.500, obarczona koniecznością obsługi protokołów OSI,
- nieadekwatność wielkości przedsięwzięcia związanego z instalacją do potrzeb, w przypadku tworzenia katalogów informacyjnych małych organizacji.

Model danych WHOIS jest bardzo prosty, baza składa się z rekordów o przypisanych jednoznacznych identyfikatorach (tzw. *handles*). Rekordy mogą zawierać dowolne dane.

W modelu WHOIS++, opisanym w dokumentach Internet–Draft [6] i [7], rekord jest nadal oznaczany poprzez *handle*, ale informacji w bazie została nadana struktura. Każdy rekord jest uporządkowanym zbiorem elementów będących parami (atrybut,wartość). Poza tym wprowadzono pojęcie typu rekordu, który specyfikuje postać występujących w nim elementów danych. Zestaw dopuszczalnych typów (zwanych *template*) określa wszystkie akceptowane postaci danych umieszczanych w bazie. Istnienie typów rekordów uznano za niezbędne w celu umożliwienia prostego sposobu ograniczania zakresu przeszukiwań do określonego zbioru informacji (np. wyłącznie osoby, usługi czy dokumenty). Mechanizm przeszukiwania bazy WHOIS++ opiera się na podanym wzorcu oraz opcjonalnym zbiorze globalnych ograniczeń, sterujących wykonaniem operacji. We wzorcu może zostać wyspecyfikowany typ rekordu (*template*), atrybut, wartość lub identyfikator (*handle*), dodatkowo dopuszcza się podanie metody wyszukania (dokładne, podłańcucha, według wyrażenia regularnego itp.), sprawdzania zgodności duże/małe litery, stosowanej tablicy kodowej itd.

WHOIS++ charakteryzuje się również prostą architekturą. Została on podzielona pomiędzy dwa komponenty: serwer poziomu podstawowego oraz indeksujący. W praktyce jeden serwer fizyczny może spełniać obie funkcje.

Serwer podstawowy gromadzi dane według ustalonego schematu. Serwer indeksowy utrzymuje informacje pomocne w wyborze właściwego miejsca odbioru danych (*forward knowledge*) i zawiera wskazania do innych serwerów indeksowych i podstawowych.

Stosowana zasada indeksowania polega na tworzeniu na podstawie informacji zawartej w ramach serwerów odwzorowania w ogromne rekordy zwane *centroidami*, które dla każdego dozwolonego typu *template* gromadzą zestawy: (atrybut,wszystkie wartości w danej bazie). Informacje te są zarządzane przez serwery indeksujące, zbierające centroidy własne oraz wybranych innych serwerów indeksujących.

Równie nieskomplikowany jest model interakcji, czyli protokół, według którego WHOIS++ kontaktuje się z innymi serwerami lub aplikacjami klienckimi. Serwer WHOIS++ oczekuje na określonym porcie na połączenia TCP, a po nawiązaniu łączności przetwarza otrzymane komendy i wysyła wyniki. Rozróżnia się komendy systemowe, stosowane do celów informacyjnych, bądź sterowania pracą oraz komendę przeszukiwania, której dodatkowe argumenty specyfikują lokalne ograniczenia odnośnie zakresu.

Trudno nie zauważyć, że podstawowa struktura danych WHOIS++ jest wzorowana na bazie X.500, znajdujemy w niej odpowiedniki klas obiektów, typów i wartości atrybutów. Twórcy tego standardu w dużej mierze korzystali z doświadczeń zebranych przy implementacji i eksploatacji X.500. WHOIS++ uwzględnia również rozproszone zarządzanie bazą danych. Jego architektura jest natomiast nastawiona na optymalizację przeszukiwania rozproszonej bazy danych.

WHOIS++ jest dobrym rozwiązaniem dla zapewnienia lokalnej usługi katalogowej. Jego implementacje są małe, łatwe w instalacji, a interakcje pomiędzy klientem i serwerem bardzo proste, co nie stwarza problemów przy konstruowaniu interfejsów użytkowych. Dodatkowo WHOIS++ może pracować jako lokalny serwis zintegrowany z globalną infrastrukturą.

WHOIS++ nie jest, jak dotychczas, w pełni funkcjonalną usługą „White Pages". Nie zapewnia właściwego poziomu ochrony danach w ramach bazy, opcjonalnie dopuszcza bardzo prostą identyfikację pytającego poprzez hasło. Nie zdefiniowano także istotnego elementu obsługi baz rozproszonych — zasad replikacji danych. System oparty o WHOIS++ jest w zasadzie mało elastyczny. Wymienione wady są konsekwencją zamierzonego podążania do celu najprostszą drogą. Tego typu implementacje dają szybki efekt, jednak na ogół wkrótce ujawniają się wszelkie niedociągnięcia i braki, szczególnie gdy należy zadowolić zapotrzebowania i upodobania szerokiej rzeszy użytkowników.

4.2 SOLO

SOLO (Simple Object Look-up Protocol) to kolejna próba specyfikacji usługi zwanej *directory service* ([8]). Protokół ten jest rozwijany we Francji (INRIA), jego autorzy bazują na doświadczeniach związanych z X.500, wykorzystują zainicjowane w ramach X.500 „przyjazne" nazewnictwo obiektów (*user friendly naming*) oraz koncepcje indeksowania (*centroidy*) stosowaną w WHOIS++. Podstawowym motywem przy defincji tego standardu było powstanie systemu dostarczającego z jednej strony mechanizmy prostego tworzenia oprogramowania typu serwer-klient dla usługi katalogowej oraz dającego dostęp do serwerów pracujących według innych protokołów — WHOIS czy X.500, tj. oprogramowania pośredniczącego pomiędzy tymi protokołami (typu *gateway*).

SOLO oparte jest na prostym protokole tekstowym, pracującym na platformie połączeń TCP/IP i składającym się z dwóch podstawowych operacji:

- przeszukiwania — w celu odzyskania informacji o określonym obiekcie,
- transferu strefy — operacji wykonywanej dla aktualizacji indeksów w ramach serwera; indeksowanie odbywa się analogicznie jak w protokole WHOIS++ poprzez tworzenie tzw. *centroidu*, czyli jednego ogromnego hasła (*entry*), zawierającego wartości atrybutów dla wszystkich indeksowanych typów atrybutów opisujących obiekty.

Implementacje protokołu SOLO są najpopularniejsze we Francji. Uruchomiono tam również wiele programów pośredniczących pomiędzy serwerami według protokołu SOLO i X.500 a usługą informacyjną World Wide Web.

4.3 DNS

Domain Name Service to podstawowa usługa informacyjna Internetu, pozwalająca identyfikować najistotniejsze zasoby typu: domena sieci, komputer, mailhost, adres IP, dla potrzeb niezawodnej pracy aplikacji aplikacji sieciowych. Serwis DNS jest niezbędny w każdej większej sieci komputerowej, jego realizacja jest wbudowana w system operacyjny, a zarządzanie sprowadza się do odpowiedniej konfiguracji tablic gromadzących dane własnej domeny.

4.4 NETFIND

Wielu użytkowników traktuje serwis zwany Netfind jako internetową usługę „White Pages".

Netfind działa w dwóch etapach. Najpierw zostaje wyszukane miejsce, do którego należy skierować żądanie, w tym celu wykorzystuje się bazy artykułów News, mapy UUCP, bazy NIC WHOIS oraz wskazania DNS. Następnie rozpoczyna się faza wysyłania zapytań, realizowana poprzez komendę *finger*, zapytania Whois, komendy SMTP (*expns*, *vrfys*) oraz polecenia do serwisu DNS.

Podstawową zaletą usługi Netfind jest jej samotworzenie. Nie wymaga ona uruchamiania specjalnych serwerów, administracji, ładowania danych, aktualizacji itp. Bazuje na istniejących zasobach informacyjnych.

Zasada działania Netfind, wiążąca efekt końcowy z wynikami pośrednimi pochodzącymi z różnych źródeł, powoduje, że często otrzymane rezultaty nie są zadawalające. W uzyskaniu prawidłowego wyniku może przeszkodzić zawodna usługa DNS, niedostępna komenda *finger*, zdezaktualizowana baza WHOIS. Dużą przeszkodą jest również fakt, że wiele ośrodków internetowych instaluje w postaci zabezpieczenia zakazy zgłaszania się z określonymi komendami.

Najpopularniejszą aktualnie formą wykorzystania usługi Netfind jest poszukiwanie użytkowników sieci komputerowych. W istniejącej postaci Netfind nie może zadowolić odbiorcy, uzyskana informacja jest uboga, pozbawiona określonej struktury, a serwis zawodny. Z drugiej strony usługa ta jest bardzo wygodna, gdy trzeba ustalić umiejscowienie domeny, aplikacji, serwera. Netfind może być w znakomity sposób stosowany do wyszukiwania właściwego serwera usługi katalogowej w danej domenie, czy organizacji.

Istnieją propozycje, aby Netfind dołączył bazy X.500 jako jedno z miejsc poszukiwania danych dotyczących organizacji i osób. Mówi się również o możliwości pozyskiwania danych do X.500 poprzez wysyłanie odpowiednich zapytań typu Netfind.

Ogólnie, wydaje się, że Netfind nie jest ani alternatywą, ani konkurentem X.500. Jego funkcjonalność jest bardzo ograniczona, a rozwój na istniejącej bazie, nie może spowodować takiej poprawy, by mógł być traktowany jako pełna usługa katalogowa.

4.5 Gopher i Veronica

Gopher to jeden z popularniejszych systemów naprowadzania i udostępniania informacji na bazie wielopoziomowych menu. Pozwala gromadzić różnego typu informacje oraz docierać do danych oferowanych przez inne serwery. Również dane X.500 mogą być widoczne z menu gophera, zapewnia to odpowiednie oprogramowanie typu *gateway*. Ilość informacji proponowana w ramach usługi gopher jest ogromna. Doprowadza to bardzo często do kłopotów z dotarciem do poszukiwanego celu.

Systemem upraszczającym zarządzanie dostępem do informacji zawartej w światowych zasobach gophera jest Veronica. Veronica zawiera odesłania do odpowiednich serwerów gopher, a także innych serwerów informacyjnych, typu WWW, archiwa Usenet itp. Tworzony indeks zasobów bazuje na słowach kluczowych tytułów zasobów informacyjnych.

W styczniu 1995 roku w indeks Veronica włączonych było 5057 serwerów gopher i 5000 innych serwerów, a ilość elementów informacji udostępnianej w ten sposób ocenia się na 15 milionów.

Z usługi Veronica można korzystać poprzez zwykły kliencki interfejs gophera.

4.6 WWW

World Wide Web to w chwili obecnej najczęściej stosowana usługa informacyjna Internetu. Oferuje prostą w obsłudze metodę wyszukiwania danych, zgromadzonych w bazach udostępnianych przez różne usługi informacyjne. WWW wprowadził jednorodne nazewnictwo zasobów komputerowych za pomocą tzw. Universal Resource Locators (URL). Nazwa taka zawiera rodzaj i lokalizację zasobu, łącznie z formą dostępu do niego.

X.500 może zostać zintegrowane z usługą WWW poprzez stosowanie odpowiedniego oprogramowania pełniącego funkcję *gateway* pomiędzy serwerem X.500 a WWW. Baza X.500 dopuszcza umieszczanie w niej danych typu URL, tak by można charakteryzując obiekty wskazać położenie dodatkowych opisów (np. zdjęć, dźwięku) w przestrzeni informacyjnej Internet.

5 Proponowane usprawnienia wykorzystania X.500

Przeciwnicy X.500 wymieniają jako jeden z podstawowych zarzutów zawodność oprogramowania zrealizowanego na podstawie standardu '88. Jest ono określane jako rozbudowane, trudne w instalacji i modyfikacji, a tworzenie nowych interfejsów użytkowych wymaga dokładnej znajomości szczegółów protokołu i zaimplementowanych funkcji bibliotecznych. Dodatkowo, w ramach konkretnych pakietów niezbędne było wprowadzenie pozastandardowych rozszerzeń, by zapewnienić funkcjonalność systemu. Oczywiście tego typu działania prowadzą do występowania niekompatybilności pomiędzy implementacjami. M.in. w oprogramowaniu QUIPU została dodana obsługa operacji replikacji danych pomiędzy serwerami (wg. RFC1276 [3]).

Prace nad protokołem X.500 były kontynuowane i zaowocowały nowym standardem, zwanym X.500 '93.

Jego najistotniejsze cechy to:

- dodany protokół replikacji informacji, tzw. *shadowing* z możliwościami:
  - utrzymywania kopii całego poddrzewa lub jego fragmentów,
  - wyboru atrybutów replikowanych,
  - wykonania replikacji na własne żądanie lub z inicjatywy wysyłającego kopię,
  - dokonywania pełnej kopii lub ograniczenie do fragmentów, które uległy zmianie (*incremental*),
- wbudowanie schematu danych w bazę X.500:
  - „formularze" zawartości haseł, reguły nazewnictwa,
  - powiązanie zasady dopasowywania z zawartością hasła,
  - wyodrębnienie atrybutów operacyjnych — dotychczas wszystkie traktowano jako użytkowe,
- zdefiniowanie zasad kontroli dostępu (*access control*),
- modyfikacja operacji protokołu między DUA a DSA, m.in. wprowadzenie stronicowania wyników operacji listowania i przeszukiwania.

Nowe implementacje według standardu '93 są w trakcie opracowywania, przewiduje się stopniowe przejście do pełnej zgodności. Standard '93 otwiera możliwości zwiększenia funkcjonalności X.500, przede wszystkim dzięki rozbudowanemu protokołowi replikacji.

Trwająca już 5 lat eksploatacja X.500 pokazała, jaki rodzaj informacji jest najczęściej poszukiwany poprzez „White Pages" i w jaki sposób użytkownicy generują swoje zapytania.

Badania statystyczne najpopularniejszego interfejsu X.500 — programu de, wykazują, że na ogół użytkownik w zapytaniu nie podaje nazwy organizacji, w ramach której ma nastąpić przeszukanie, lub podaje niedokładną nazwę. Poza tym często wykorzystywany jest tryb de zwany *power search*, w którym następuje równoległe wyszukiwanie w domenach administracyjnych wszystkich organizacji danego kraju.

Hierarchiczność bazy X.500 pozwala łatwo dokonywać przeszukiwań w obszarach poddrzew (*naming context*). Jeden z podstawowych wymogów funkcjonalnych — operacje znalezienia informacji w przypadku mało precyzyjnego sformułowania miejsca poszukiwania są w X.500 bardzo uciążliwe lub niemożliwe. Oznacza to w obecnej sytuacji konieczność przeglądania rozległych obszarów, a nawet całego drzewa danych DIT i wymaga łaczenia z dużą ilością serwerów. Jest to często niemożliwe (poprzez ustalenie administracyjnego zakazu), a przede wszystkim niepraktyczne.

Tego typu problemy są charakterystyczne dla wszelkiego rodzaju baz rozproszonych, zawsze też są rozwiązywane jedną metodą — poprzez stosowanie techniki indeksowania. Podobne potrzeby spowodowały utworzenie usługi archie dla FTP, czy Veronica dla przestrzeni gopher.

Został już sprecyzowany niezbędny opis funkcjonalny serwerów indeksowych w ramach X.500 ([9]). Serwery takie nastawione na gromadzenie haseł pochodzących z różnych obszarów DIT i zawierałyby odsyłacze do miejsc zarządzania danym fragmentem poddrzewa, lub do serwerów dysponujących kopią pożądanej informacji.

Wprowadzenie indeksowych DSA jest z punktu widzenia użytkowego rzeczą naturalną, jednak realizacja tego przedsięwzięcia była niemożliwa przy braku jednoznacznej definicji operacji replikacji pomiędzy serwerami X.500; standard '93 tę barierę przełamuje.

Indeksowe serwery X.500 miałyby docelowo zostać zintegrowane jako wskazania w usłudze WWW, bierze się również pod uwagę konieczność umieszczania w ramach indeksów wskazań do serwerów „White Pages" pracujących według innej technologii (WHOIS++, SOLO).

Implementacje według standardu '93 są w stanie zapewnić szybszy dostęp do danych nawet bez stosowania indeksowych DSA, jeżeli zostanie właściwie wykorzystana technika replikacji danych. Administrator serwera X.500 może wówczas odpowiednio do potrzeb środowiska skonfigurować DSA tak, aby pobierać i utrzymywać lokalnie kopie pożądanych informacji.

Kolejnym problemem wymagającym rozwiązania w X.500 jest zapewnienie możliwości zawężonego przeszukiwania poddrzewa. Taka potrzeba pojawia się, gdy poszukiwany jest obiekt o określonym typie, np. organizacja i wiadomo, że nie jest wymagane przeglądanie haseł występujących najniżej w hierarchii drzewa (*leaf entries*).

Bibliografia

[1] Data Communication Networks: Directory, Recommendations X500-X.521, CCITT, Fascile VIII.8 of Blue Book

[2] The Directory — Overview of Concepts, Models and Service, ISO/IEC 9594

[3] S. E. Hardcastle-Kille (1991) *Replication and distributed operation extentions to provide an Internet Directory using X.500, Request for Comments RFC1276*
URL=<ftp://ds.internic.net/rfc/rfc1276.txt>

[4] C. Weider, R. Wright *A Survey of Advanced Usages of X.500* Request for Comments RFC1491
URL=<ftp://ds.internic.net/rfc/rfc1491.txt>

[5] E. Finler, K. Harrenstien, M. Stahl (1985) *NICNAME/WHOIS*, Request for Comments RFC954
URL=<ftp://ds.internic.net/rfc/rfc954.txt>

[6] P. Deutsch, R. Schoultz, P. Faltstrom, C. Weider (1995) *Architecture of the WHOIS++ service*, Internet Draft
URL=<ftp://ds.internic.net/internet-drafts/drafts-ietf-wnils-whois-arc h-03.txt>

[7] C. Weider, J. Fullton, S. Spero (1994) *Architecture of the WHOIS++ Index Service*, Internet Draft
URL=<ftp://ds.internic.net/internet-drafts/drafts-ietf-wnils-whois-04. txt>

[8] C. Huitema, P-A. Pays, A. Zahm, A. Woermann (1994) *Simple Object Look-up protocol (SOLO)*, Internet Draft
URL=<ftp://ds.internic.net/internet-drafts/drafts-huitema-solo-01.txt>

[9] P. Barker (1995) *X.500 Index DSAs*

Optymalizacja działania rozproszonej bazy danych na podstawie badań efektywnościowych X.500*

Maja Górecka
mgorecka@cc.uni.torun.pl

Tomasz Wolniewicz
twoln@mat.uni.torun.pl

Uniwersytet Mikołaja Kopernika w Toruniu

1 Wstęp

Celem niniejszego opracowania jest przedstawienie wniosków z badań efektywnościowych X.500 Directory, a dokładniej konkretnej implementacji standardu — oprogramowania QUIPU wersja 12.0.

Bazą dla pracy był nasz wstępny raport [4], w którym przedstawiliśmy rozważania teoretyczne nad czynnikami mającymi wpływ na sprawność działania rozproszonej bazy danych, jaką jest X.500. Zapoznanie się z tym raportem byłoby niewątpliwie pomocne przy czytaniu przedstawianego tutaj opracowania.

Obecnie chcemy podsumować wyniki testów i skonfrontować je z wcześniejszymi przewidywaniami. Od razu możemy nadmienić, że nie wszystkie testy dały oczekiwane wyniki. Głębsza analiza tych rozbieżności wykazała, że niektóre zaimplementowane w badanym oprogramowaniu metody nie działają zgodne z ich opisem, w pewnych sytuacjach natomiast wpływ niektórych czynników na działanie bazy jest tak silny, że uniemożliwia ocenę znaczenia elementu badanego.

Nasz raport opisuje, często dość szczegółowo, mechanizmy działania bazy X.500 w implementacji QUIPU. Wydaje się nam, że taka głębsza wiedza może być bardzo przydatna administratorom serwisu X.500, a nie spotkaliśmy dotychczas opracowań, które przybliżałyby rozważane przez nas tematy dostatecznie wyczerpująco.

Nie będziemy omawiali samego schematu bazy X.500. Powiemy tylko, że analizujemy rozproszoną bazę danych opartą na serwerach (DSA), do której dostęp zapewnia oprogramowanie klienta (DUA). Dokładny opis funkcjonowania bazy i używanej terminologii można znaleźć między innymi w naszych raportach [4], [5], [6], a także w [2] i [1], natomiast opis użytkowy oprogramowania QUIPU zawarty jest w [3].

W raporcie zamieszczamy też wyniki pomiarów działania polskiej bazy X.500, które zebraliśmy za pomocą specjalnie do tego celu napisanego oprogramowania. Niektóre pomiary dokonywane były również na testowo uruchamianych instalacjach, robiliśmy to w przypadkach, gdy konieczne było dokładne wydzielenie wpływu jednego badanego czynnika na zachowanie serwera bazy.

*Praca wykonana w ramach statutowej działalności NASK

2 Obsługa operacji rozproszonych

System rozproszony (jakim jest X.500) przechowuje gromadzoną informację na wielu serwerach (DSA). Dostęp klienta (DUA) do bazy rozpoczyna się od dowiązania do wybranego DSA i zadania pierwszego zapytania. W zależności od tego, czy realizacja odpowiedzi może być dokonana lokalnie, czy też niezbędne jest odwołanie do innych serwerów będziemy mieli do czynienia z występowaniem operacji rozproszonego dostępu lub nie. Do wymiany informacji pomiędzy DUA a DSA służy protokół DAP (*Directory Access Protocol*), serwery DSA komunikują się w ramach protokołu DSP (*Directory System Protocol*).

W części tej opisujemy jak oprogramowanie QUIPU podejmuje decyzje o nawiązaniu kolejnych połączeń i jaki ma to wpływ na efektywność działania całej bazy.

2.1 Wybór serwera

DSA obsługujący zlecenie nie dające się zrealizować lokalnie może albo przekazać je kolejnemu serwerowi poprzez tworzenie łańcucha (*chaining*), albo zwrócić DUA odesłanie do innego serwera DSA (*referral*). Identyczny protokół komunikacyjny obowiązuje również w trakcie wymiany informacji pomiędzy serwerami.

Wybór właściwego DSA jest bardzo istotny z punktu widzenia efektywności pracy X.500. Na ogół istnieje kilka serwerów, które prawdopodobnie są w stanie obsłużyć zlecenie. QUIPU DSA w tej sytuacji dokonuje uporządkowania listy serwerów według jakości operacyjnej i następnie przekazuje żądanie do DSA uznanego jako najlepsze, w przypadku niepowodzenia, wybiera kolejny serwer z listy itd.

Sposób postępowania przy ocenie serwerów jest określony w implementacji QUIPU w ramach algorytmu, który bazuje na informacjach o parametrach własnych DSA oraz zapamiętanych danych, dotyczących aktywności serwerów. Dodatkowo umożliwia się administracyjny wpływ na wybór serwera docelowego poprzez podanie w zbiorze konfiguracyjnym QUIPU wartości tzw. `preferDSA`.

Algorytm ustala następujące uporządkowanie elementów decydujących o wyborze DSA:

1. Istnienie nawiązanego połączenia z odpowiednim serwerem.

2. Docelowe DSA jest QUIPU DSA, czyli w `objectClass` znaleziono wartość `quipuDSA`. Dodatkowo sprawdzany jest atrybut specyfikujący akceptowane typy protokołów, zwane kontekstem aplikacji (`SupportedApplicationContext`), tzn. te wszystkie elementy warstwy aplikacji (ASE — Application Service Element), które serwer implementuje. Pierwszeństwo otrzymuje DSA z kontekstem QUIPU, następnie DSA według protokołu Internet, wszystkie pozostałe traktowane są jednakowo, z wyjątkiem serwera DSA, który podtrzymuje wyłącznie protokół DAP.

3. Docelowe DSA zostało uznane jako bardziej niezawodne. Ocena ta bazuje na śledzeniu informacji o czasie ostatniej próby dostępu do DSA oraz jej efekcie, tzn. czy połączenie zakończyło się sukcesem oraz czy wystąpiły błędy. W ten sposób preferowany jest np. ten serwer, który nie był ostatnio aktywny w sytuacji, gdy konkurencyjny miał nawiązane połączenie, ale w trakcie dostępu zawiódł. Z kolei w przypadku, gdy dwa serwery były aktywne, zwycięża ten, który nie zawiódł, a jeżeli oba miały błędy — serwer, dla którego nie minął czas między kolejnymi próbami nawiązania połączenia (*retrytime*). Wiele przypadków traktowanych jest jako nierozstrzygalnych, m.in. gdy oba serwery nie były aktywne, gdy oba były, jeden zawiódł, ale dla obu upłynął czas *retrytime*, gdy jeden był aktywny, ale zawiódł i upłynął czas ponowienia próby połączenia.

4. DSA dostępne jest we właściwej kategorii protokołu sieciowego (*community*), a w przypadku, gdy dwa DSA znajdują się w tej samej kategorii, wybierany jest serwer uznany za lokalny na bazie analizy wyróżnionej nazwy DSA (*Distinguished Name*).

5. DSA jest uprzywilejowany na podstawie listy `preferDSA`.

Jak widać algorytm wyboru DSA nie jest rozbudowany. W minimalnym stopniu wykorzystuje „historię" połaczeń, ogranicza się wyłącznie do sprawdzania, czy DSA był aktywny i czy wystąpiły błędy w trakcie pracy. Nie jest zapamiętywany czas niezbędny do nawiązania łączności, czy średni czas połączenia. Oczywiście może to prowadzić do częstego korzystania z serwerów, które spełniają warunki kwalifikacyjne, natomiast kontakt z nimi jest czasochłonny.

Wątpliwości budzi określona kolejność czynników decydujących o doborze DSA. Małą rolę odgrywa administracyjne ustalenie listy uprzywilejowanych serwerów; jedynie w przypadku niemożliwości rozstrzygnięcia na podstawie niezawodności i lokalizacji DSA wybierany jest serwer wskazany przez administratora. W przypadku zapytań pochodzących np. z polskich serwerów regionalnych zapewnienie wysokiego priorytetu wyborowi DSA według listy wskazanej przez `preferDSA`, na której znajdowałby się serwer krajowy, miałoby zdecydowanie korzystny wpływ na obsługę zapytań dotyczących danych replikowanych przez DSA Polski. Typowym rozwiązaniem mającym na celu usprawnienie działania bazy jest replikowanie fragmentów drzewa geograficznie odległych. Na przykład lista instytucji polskich jest replikowana przez krajowy serwer australijski. Fakt ten oznacza jednak, że serwer australijski może być wybierany jako źródło informacji o Polsce przez inne serwery europejskie (a nawet polskie (!)).

QUIPU daje najwyższy priorytet DSA, do którego jest już aktualnie nawiązane połączenie. Intencja autorów oprogramowania jest łatwo zrozumiała, gdy uświadomimy sobie, że nawiązanie nowego kontaktu jest zawsze kosztowne czasowo (potwierdzają to wyraźnie wyniki wykonanych przez nas testów). Rozumiejąc to zauważamy jednocześnie negatywny wpływ takiego rozwiązania. Może się zdażyć, że nawiązane połaczenie z odległym serwerem w celu uzyskania od niego informacji dla niego lokalnej przesądzi o pobieraniu z tego miejsca danych, które, gdyby nie otwarte połączenie, mogłyby zostać udostępnione z bliższego, a nawet lokalnego serwera.

2.2 Obsługa zlecania — tworzenie łańcucha lub przekazywanie odesłania do serwera

QUIPU DSA realizując zlecenie musi podjąć decyzję, w jaki sposób ma ono zostać obsłużone. Jeżeli polecenie otrzymane od DUA lub innego DSA nie może być rozstrzygnięte lokalnie jest ono albo przekazywane innemu serwerowi poprzez formowanie łańcucha zleceń (*chaining*), albo DSA zwraca DUA odesłanie do innego serwera (*referral*) i DUA samodzielnie kontynuuje zapytania.

Wybór metody może mieć istotny wpływ na efektywność pracy X.500. Decyzja *chaining* lub *referral* jest podejmowana po ustaleniu listy możliwych serwerów oraz uporządkowaniu jej zgodnie z algorytmem opisanym w rozdziale 2.1 i odbywa się w następujących krokach:

- W przypadku, gdy zgłaszająca się do DSA aplikacja legitymuje się jako proces używający protokołu DAP — służący do wymiany informacji pomiędzy DUA i DSA) zakłada się, że stosowana będzie obsługa poprzez tworzenie łańcucha zleceń, druga

forma — zwrot odesłania pozostaje również w mocy. Uporządkowanie listy serwerów nie ulega zmianie. Na bazie tej listy tworzone są odpowiednie parametry dla operacji, tzw. *continuation references*, czyli wskazania dokąd kierować zlecenie po wystąpieniu błędów. Następnie sprawdzane są argumenty związane z obsługą operacji (*service control*). Jeżeli proces zgłosił się z zaleceniem, by nie przekazywać zadania do wykonania innym serwerom (*chainingprohibited*), lub by ograniczyć przeszukiwania do bazy lokalnej (*localscope*), zostaje wybrana metoda zwrotu odesłania do DUA, w przeciwnym razie stosowana jest metoda tworzenia łańcuchów zleceń.

- Jeżeli do DSA zwraca się proces o protokole DSP, wówczas następuje wybór serwera DSA priorytetowego przy wskazywaniu odesłania. Odbywa się to przez określenie czy proces wysyłający zlecenie i docelowy serwer należą do tej samej kategorii sieciowej — *community*. Oczywiście jest to możliwe jedynie w sytuacji, gdy lokalnie można zdobyć informację, jaki adres prezentacyjny posiada zlecający. Pierwszy serwer z listy dopuszczalnych DSA o *community* zgodnej z aplikacją zlecającą jest wybierany jako najlepszy. Jeżeli żaden serwer nie znajduje się w tej samej sieci, blokowana jest możliwość zwracania odesłania. W przypadku, gdy DSA nie jest w stanie ustalić adresu zgłaszającego, pierwszy serwer z listy delegowany jest jako adres ewentualnego odesłania.

  Po ustaleniu listy DSA sprawdzana jest możliwość wykonywania operacji *chaining* w ramach obsługi zlecenia według protokołu DSP. Jeżeli wystąpił jeden z następujących przypadków:

  - *chaining* został zakazany administracyjnie przez ustawienie parametru konfiguracyjnego `dspchaining` jako `off` lub `WhenNeeded`,
  - proces zgłaszający wymusza obsługę bez łańcuchowania (*chainingprohibited* lub *localscope*)

  DSA będzie obsługiwało zlecenia przez zwrot odesłania, chyba że wcześniej zablokowano stosowanie tej metody — w tym przypadku operacja zakończy się niepomyślnie z powodu zakazu tworzenia łańcucha do innych DSA i niemożliwości wysłania wskazania innego serwera.

  W pozostałych sytuacjach stosowane jest przekazywanie niezrealizowanych żądań do kolejnych DSA.

Jak wynika z opisu, decyzja o metodzie obsługi zlecenia zależy od takich czynników jak:

- środowisko pracy serwera i możliwość współpracy z innymi DSA,
- parametry konfiguracyjne serwera,
- otrzymane razem ze zleceniem argumenty operacji.

Dla zapytań od DUA typowo stosowana jest metoda budowania łańcucha, jednak interfejs użytkowy może wymusić obsługę poprzez wskazania za pomocą odpowiednich argumentów.

Jeżeli DSA pośredniczy w realizacji zlecenia, *chaining* dokonywany jest do kolejnych DSA z listy, stąd większe prawdopodobieństwo sukcesu. Dodatkowo DSA jest w posiadaniu informacji statystycznej, na podstawie której będzie w stanie podejmować kolejne akcje w imieniu DUA, samo DUA skazane jest na ścisłe podążanie za podawanymi mu odesłaniami.

Widać z tego, że tworzenia łańcucha ma szereg zalet. Niewątpliwie jest to najwłaściwszą metodą dla obsługi połączenia realizowanego w protokole DAP (inicjowanego przez DUA), a operacje według protokołu DSP (pomiędzy DSA) powinny mieć zablokowanie łańcuchowanie zgłoszeń. Aby to uzasadnić przyjmijmy najbardziej typową sytuację, w której DUA łączy się z bliskim sobie (w sensie geograficznym) DSA. DSA to posiada lokalną wiedzę o możliwości nawiązywania sprawnych połączeń z innymi DSA, które poprzednio wykorzystywało, może też preferować pewne DSA zgodnie z ustawieniami administracyjnymi. Pytania zadawane przez DUA obsługiwane są zatem zawsze w optymalny dla tego DUA sposób. Przekazanie DUA odesłania spowoduje, że nastąpi dowiązanie do obcego (być może odległego) DSA, który będzie stosował swoje mechanizmy doboru najwłaściwszych DSA, sam będzie podejmował decyzje o tym, czy tworzyć łańcuchy czy nie i w efekcie może doprowadzić do tego, ze DUA będzie korzystało z niego do końca nawiązanej sesji. Utworzenie łańcucha zawierającego więcej niż jedno DSA powoduje, że kolejne DSA nie mają właściwej informacji o tym skąd pochodzi zapytanie i mogą przekazywać nieoptymalne adresy kolejnych DSA. Towarzyszy temu oczywiście niepotrzebny transfer danych przez kilka serwerów.

Oczywiście tworzenie łańcuchów protokołu DSP daje większe prawdopodobieństwo powodzenia operacji, ale równocześnie obniża sprawność całej bazy i dlatego, naszym zdaniem, nie powinno mieć miejsca. Z tego powodu wydaje się korzystne wymuszanie administracyjnego zakazu tworzenia łańcuchów dla protokołu DSP. W sytuacji podłaczenia DSA tylko do jednego *community*, całkowicie zbędna jest funkcja łańcuchowania protokołu DSP, funkcja ta ma sens, gdy serwer jest podłączony do kilku *communities* i może działać jako most (*relay DSA*). W takiej sytuacji włączenie lub wyłączenie opcji zezwalającej na łańcuchowanie może być podyktowane np. argumentami finansowymi (routowanie obcego ruchu).

Wydaje się nam, że najwłaściwsze w sytuacji polskiego X.500 byłoby zmodyfikowanie algorytmu generowania odesłań, tak aby polskie DSA zwracały się do polskiego serwera krajowego, zawsze wtedy gdy serwer ten posiada poszukiwaną przez nie informację, z kolei serwer krajowy powinien blokować łańcuchowanie protokołu DSP, tak aby promować obsługiwanie lokalnych DUA, przez ich lokalne DSA.

3 Wpływ wielkości bazy na pracę serwera

Serwer DSA w implementacji QUIPU w swojej podstawowej konfiguracji ładuje do pamięci operacyjnej całą lokalną bazę danych, łącznie z wszystkimi replikacjami. Przy dużej ilości haseł prowadzi to do tworzenia bardzo pamięciochłonnego procesu.

Rozmiar bazy danych w pamięci zależy od ilości i wielkości haseł. Średnio określa się, że jedno hasło potrzebuje około 2KB pamięci.

Przeprowadzone testy wykazały m.in., że:

- Baza o ilości haseł 3500, większość haseł rozbudowana — wymaga ok. 6.5MB pamięci operacyjnej (na dysku zajmuje ok. 14MB), czyli średnio na jedno hasło przypada 1.8MB.
- Baza o ilości haseł ok. 30000, hasła o małej ilości atrybutów — wymaga ok. 33MB pamięci operacyjnej (na dysku — 27MB), czyli średnio jedno hasło zajmuje 1.1MB.
- Baza o 20000 małych haseł zajmuje 24MB pamięci operacyjnej (ok. 1.2MB na hasło), po rozbudowanu haseł — 34MB (ok. 1.7MB na hasło).

Pamięć zajmowana przez serwer, to suma wielkości samego procesu DSA i rozmiaru bazy danych powiększana przez bieżącą alokację dla potrzeb buforowania, czy wykonywania operacji replikacji danych. Zarządzanie pamięcią nie jest mocną stroną oprogramowania QUIPU. Wszystkie wersje, na bazie których pracujemy już od 3 lat m.in. nie wykonują prawidłowo zwalniania pamięci, co powoduje, że rozmiar długo pracującego serwera znacznie wzrasta.

Jeżeli proces serwera nie mieści się w całości w wolnej pamięci komputera stosowana jest metoda tworzenia pamięci wirtualnej poprzez przenoszenie części procesu na dysk (stronicowanie pamięci). W tej sytuacji istotnie obniża się efektywność pracy serwera, gdyż większość operacji wiąże się z koniecznością kontaktu z dyskiem w celu pobrania właściwego fragmentu procesu.

Z powyższych ustaleń wynika, że serwery QUIPU obsługujące duże bazy lokalne, dla zapewnienia sprawności działania wymagają odpowiedniej wielkości pamięci operacyjnej, tak by cały proces mógł rezydować w pamięci. W przeciwnym razie doprowadza się do bardzo dużych opóźnień czasowych w realizacji zapytań. Testy wykazały, że operacja przeszukiwania lokalnej bazy zawierającej 20000 haseł, obsługiwana przez serwer o pamięci operacyjnej 64MB jest wykonywana w przeciągu 1-2 sekundy, podczas gdy w przypadku uruchomienia tego serwera na tym samym komputerze, ale przy rozmiarze pamięci 32MB oczekiwanie na rezultat trwa ok. 1.5 minuty.

W pakiecie oprogramowania Isode Consortium począwszy od wersji IC R2.0 istnieje możliwość przechowywania części bazy X.500 na dysku w trakcie pracy serwera. Wydzielony fragment drzewa informacji DIT jest zarządzany przez specjalny proces zwany *delegate DSA*. Baza dyskowa posiada szereg dodatkowych zbiorów indeksowych, pomocnych przy operacjach przeszukiwania i listowania.

Stosowanie bazy dyskowej jest zalecane przy przechowywaniu dużych poddrzew, autorzy oprogramowania zapewniają sprawne działanie przy ilości haseł do jednego miliona. Korzystanie z dysku zacznie skraca czas ładowania procesu i istotnie ogranicza wymagania odnośnie pamięci operacyjnej. Usprawnienie to odbywa się jednak kosztem zwiększenia zapotrzebowania na pamięć dyskową. Bardzo czasochłonny jest też proces budowania baz indeksowych.

Testowanie wersji serwera z obsługą dyskową dla bazy gromadzącej w „delegowanym" poddrzewie ok. 3500 haseł wykazało blisko dwukrotne powiększenie zużycia obszaru dyskowego, zapotrzebowanie na pamięć spadło o ok. 3MB, przy czym w trakcie pracy rozmiar serwera w pamięci rósł stosunkowo szybko (buforowanie wyników). Sprawność reakcji przy realizacji zleceń dotyczących lokalnych zasobów w sposób zauważalny maleje, w porównaniu z sytuacją, gdy cała baza rezyduje w pamięci (opóźnienie rzędu 3-5 sekund).

W przypadku, gdy serwer ma obsługiwać rozbudowane poddrzewo danych i wiadomo, że proces serwera nie będzie dysponował wystarczającą pamięcią operacyjną, podejście dyskowe powinno znacznie podnieść efektywność.

4 Indeksowanie a wielkość bazy i sprawność jej działania

Oprogramowanie QUIPU dopuszcza indeksowanie bazy X.500 według zadanych atrybutów `optimized_attr` w ramach wskazanych obszarów drzewa danych (poddrzewo — *subtree* lub jeden poziom — *siblings*). Tworzenie indeksu odbywa się w pamięci operacyjnej, podczas

ładowania bazy danych serwera. Indeks zawiera dla każdego optymalizowanego atrybutu wskazania miejsc rezydowania w pamięci haseł mających przypisane tym atrybutom wartości.

W celu przyspieszenia realizacji zapytań QUIPU używa do zapamiętywania haseł w pamięci struktur wyważonego drzewa binarnego, zwany AVL[1]. Obsługa takiej struktury jest optymalna — przy N hasłach średnio potrzeba nie więcej niż $logN$ operacji, by odnaleźć hasło szukane. Odpowiednie algorytmy dokonują wyrównania drzewa po dodaniu lub usunięciu węzłów. Również indeksy budowane są na bazie struktur AVL.

Wprowadzenie indeksowania w bazie prowadzi do dodatkowego zapotrzebowania na pamięć operacyjną. Nie jest to wprawdzie drastyczny wzrost (np. dla indeksacji według dwóch atrybutów, względem jednego poddrzewa przy ilości haseł 3500 zaobserwowano przyrost ok. 500KB, przy zwiększeniu ilości atrybutów do 6 — ok. 1.8MB), jednak w niektórych sytuacjach można indeksując przekroczyć barierę dostępnej pamięci i w efekcie spowodować znaczne pogorszenie efektywności.

Wykonane testy wykazały, że wprowadzenie indeksu nie wpływa zauważalnie na przyspieszenie operacji na bazie lokalnej. Krytycznym elementem pozostaje pamięć, jaką dysponuje serwer. Jeżeli proces serwera nie musi korzystać z technik stronicowania i *swapowania*, jego reakcja, jest zadawalająca, nawet przy przeglądaniu dużego poddrzewa i stosowaniu rozbudowanych filtrów przeszukania. Niewystarczająca pamięć wprowadza długi czas odpowiedzi, a dodanie metody indeksacji nie wnosi istotnych zmian.

Przeprowadzone próby z nowym mechanizmem bazy opartej na dysku pokazują, że stosowanie jego wydaje się bardzo ograniczać możliwości przeszukań całych gałęzi bazy. Serwer nie zezwala na dokonywanie przeszukań ze względu na atrybuty nieindeksowane. Mechamizm działania serwera z tą dodatkową opcją nie jest dostatecznie dobrze opisany w dokumentacji i prawidłowe zrozumienie algorytmów możliwe będzie dopiero po analizie kodu źródłowego.

5 Wpływ na efektywność poprzez stosowanie techniki buforowania resultatów operacji

QUIPU DSA pozwala utrzymywać w „podręcznej pamięci" typu *cache* otrzymane dane z innych serwerów DSA. Technika *„cachowania"* jest stosowana zarówno po stronie DSA jak i DUA. W trakcie pracy serwera w pamięci *cache* gromadzone są przeczytane hasła, tj. nazwa (DN — *Distinguished Name*) oraz wartości tych atrybutów, które zostały przekazane pytającemu. DSA implementuje, niezbędne dla wiarygodnej pracy serwera, algorytmy przedawniania danych w pamięci podręcznej oraz decydowania, czy informacja ta może zadowolić odbiorcę. W tym celu wprowadzane są odpowiednie interwały czasowe, w ramach których zakładana jest poprawność danych z pamięci typu *cache*. Dodatkowo zlecający razem z typem wykonywanej operacji może ustalić warunki obsługi (*service control*) i m.in. zażądać nie używania kopii przy przekazywaniu wyników.

Stosowanie techniki buforowania znacznie przyspiesza wszelkie operacje związane z ponownym odczytem informacji z bazy X.500. Z punktu widzenia serwera wprowadza jednak dodatkowe zapotrzebowanie na pamięć operacyjną i wymaga poprawnych algorytmów przedawniania informacji oraz prawidłowego administracyjnego ustalenia interwałów czasowych dotyczących czasu życia danych.

Należy podkreślić, że niezbędne jest również korzystanie z dobrze przygotowanych in-

[1] Adelson-Velskii i Landis zdefiniowali tę strukturę jako takie drzewo, w którym dla każdego węzła wysokości dwóch jego poddrzew różnią się co najwyżej o 1.

terfejsów użytkowych — DUA. DSA implementuje utrzymywanie kopii rezultatu operacji listowania tylko dla poleceń według protokołu DSP (czyli pomiędzy serwerami), poza tym w pamięci podręcznej umieszczane są odczytane hasła. Uzyskane wyniki listingu powinny więc być *cachowane* w ramach DUA. Dzięki temu można np. dodatkowo, przed zapamiętaniem w pamięci podręcznej przeprowadzić uporządkowanie. DUA działające w oparciu o prawidłowo zrealizowaną technikę korzystania z pamięci *cache* mogą znacznie podnieść efektywność pracy serwisu postrzeganą przez użytkowników. Jednocześnie, w przypadku interfejsów DUA, będących procesami krótkotrwałymi, niebezpieczeństwo przekazywania odbiorcy nieaktualnej informacji, wnoszone przez buforowanie danych jest niewielkie.

Nasze dotychczasowe doświadczenia związane z realizacją programów użytkowych opierają się na pracach nad modyfikacjami w celu dostosowania do korzystania z zapamiętanych w bazie X.500 poprawnych polskich danych. Przy obsłudze zlecenia odczytu uzyskiwana jest wyróżniona nazwa konkretnego obiektu w przeszukiwanym drzewie. Nazwa ta składa się z szeregu relatywnych nazw wyróżnionych, które pozbawione są polskich znaków narodowych. Aby uzyskać pełną, poprawną polską nazwę należy odczytać odpowiednie atrybuty każdego obiektu występującego w gałęzi prowadzącej do otrzymanego wyniku. Oczywiście, tego typu działania mogą powodować istotne opóźnienia w odbiorze rezultatu. Technika buforowania polskich nazw wyróżnionych może w opisanym przypadku istotnie poprawić efektywność.

W ramach opisywanych prac dokonaliśmy modyfikacji atrakcyjnego interfejsu POD poprzez wprowadzenie funkcji buforowania wyników i poprawę algorytmu sortowania list. Zmiana sposobu sortowania przyspieszyła działanie tego interfejsu o ok. 100 razy. Zwracamy na to uwagę, aby podkreślić jak zupełnie prosty błąd w realizacji końcowego interfejsu może osłabić działanie całego systemu.

6 Wyniki pomiarów sprawności polskiej bazy X.500

W ramach badania efektywności bazy X.500 przeprowadzilismy szereg pomiarów funkcjonowania polskiej bazy. W tym celu napisane zostało oprogramowanie monitorujące bazę o następujących funkcjach:

1. sprawdzenie średnigo czasu dostępu do komputera, na którym działa DSA (za pomocą internetowego `ping`),
2. dowiązanie do DSA (bind),
3. dokonanie kilku wyszukań lokalnych dla serwera, z którym się połączyliśmy,
4. dokonanie kilku wyszukań nielokalnych,
5. wyświetlenie wartości odszukanych haseł lokalnych,
6. wyświetlenie wartości wyszukanych haseł nielokalnych.

Oprogramowanie monitorujące oparte jest na wersji DUA o nazwie `dish`, które pozwala na wydawanie dowolnych komend DUA bezpośrednio z linii komend systemu operacyjnego. Interfejs ten jest bardzo wygodny do oprogramowania, obarczony jednak pewnym opóźnieniem uruchomienia każdej komendy (oceniamy ją na ok. 0.5s). Pomiary czasów prowadzone były z dokładnością ok. 0.1 s. Trzeba podkreślić, że toruński serwer centralny ma

jeszcze obecnie połaczenie satelitarne z Warszawą, co wprowadza opóźnienia sieciowe. Sytuacja ta jest w zasadzie sprzyjająca pomiarom efektywności, gdyż pozwala łatwiej mierzyć wpływ opóźnień sieciowych na zachowanie się bazy.

Pomiar był dokonywany według następującego algorytmu:

1. dowiązanie do mierzonego serwera,
2. wydanie komendy przeszukania (typowo dwa do trzech przeszukań zwracających niekiedy pojedyncze, a niekiedy wielokrotne trafienia), czasy przeszukań były dodawane, a następnie uśredniane,
3. wydanie komendy wypisania wybranych atrybutów znalezionych haseł poprzez wielokrotne wydanie rozkazu **showentry** odpowiadającemu protokołowemu **read**, czasy były dodawane, a następnie uśredniane; ponieważ wyników operacji przeszukania było z reguły więcej niż samych operacji przeszukania, dla operacji czytania mieliśmy większą próbkę statystyczną,
4. wydanie komendy przeszukania w zakresie organizacji obługiwanej przez inny serwer (dla wszystkich przypadków były to te same dwa hasła znajdujące się na serwerze warszawskim),
5. wydanie komendy wypisania atrybutów tych haseł.

Operacja ta wykonywana jest 7 razy. Z każdego ciągu wyników odrzucany jest wynik najlepszy i najgorszy, pozostałe są uśredniane. Dodatkowo odnotowywane są również wyniki skrajne, jak też czas pierwszego dowiązania do serwera.

Dowiązanie do serwera prowadzone było zarówno w trybie anonimowym jak i ze sprawdzeniem tożsmości. Ta druga sytuacja zmusza serwery do dokonania poświadczania (*authentication*), a zatem przesłania dodatkowej informacji (co oczywiście musi opóźnić operację dowiązania).

Poza możliwościa przeprowadzenia pojedynczego cyklu prób, napisane przez nas oprogramowanie (po ewentualnym rozbudowaniu) będzie służyło jako system ciągłego monitorowania polskiego projektu X.500.

Wyniki przeprowadzonych pomiarów wykazują generalnie dobre zachowanie się bazy. Spodziewaliśmy się uzyskania odpowiedzi na następujące pytania:

1. Jaki jest czas startu bazy (czy pierwsze dowiazanie jest wolniejsze od następnych)?
2. Jaka jest różnica pomiędzy wykonaniem dowiązania anonimowego i autoryzowanego?
3. Jaka jest róznica pomiędzy otrzymaniem wyniku przeszukania instytucji, której dane są dostępne lokalnie od tych, których pozyskanie wymaga nawiązania dodatkowego połączenia?
4. Jakie składowe typowego zapytania mają szczególny wpływ na czas trwania operacji?
5. Czy rozpraszanie bazy na wiele serwerów jest korzystne i w jakich warunkach?

W wyniku testów otrzymaliśmy:

ad. 1 W przypadku polskiego systemu serwerów regionalnych czas pierwszego dowiązania nie jest zauważalnie dłuższy od następnych. Z doświadczeń lokalnych wiemy, że serwer bardzo rzadko eksploatowany ma dłuższy czas rozruchu (konieczność załadowania do pamięci operacyjnej znacznej ilości danych z dysku). Serwery regionalme są jednak eksploatowane stosunkowo intensywnie.

ad. 2 Opóźnienie powodowane poświadczaniem jest sumą operacji dowiązania do DSA przechowującego dane dowiązującego się, przesłania podanego hasła i wykonanie porównania z przechowywanym w bazie, przesłania wyniku operacji. Na wszystko to nakładają się oczywiście opóźnienia sieciowe. W niekorzystnych sytuacjach może to oczywiście prowadzić do zauważalnego pogorszenia działania bazy, typowo jednak poświadczanie dokonywane jest przez DSA bliskie DUA, a następne operacje rozproszone oparte są na wzajemnym zaufaniu DSA (ta ewidentna luka w bezpieczeństwie może być usuwana przy stosowaniu wyższych poziomomów zabezpieczeń). Przy okazji warto wspomnieć, że istnieje możliwość dowiązania z podaniem nazwy, ale bez poświadczania. Takie dowiązanie ma charakter jedynie informacyjny. Serwer dokonuje jedynie bardzo pobieżnej weryfikacji, jeżeli dowiązujący się powinien występować w bazie lokalnej danego serwera, to sprawdzane jest istnienie takiego obiektu i w przypadku stwierdzenia fałszu połączenie jest blokowane, nie sprawdza sie jednak danych nielokalnych, aby nie przedłużać operacji. Ten rodzaj dowiązania nie pozwala oczywiście na dokonywanie żadnych modyfikacji bazy, ani na czytanie zastrzeżonych danych.

ad. 3 Zgodnie z przewidywaniami, dostęp do danych lokalnych jest na ogół szybszy, chociaż w przypadku serwera krakowskiego, w pewnych okresach dane nielokalne były dostępne znacznie szybciej. Musi to być związane z obciążeniem maszyny. Dostęp do danych nielokalnych był jednak w sumie bardzo szybki (średnio przeszukanie lokalne trwa 2–3 sekund, nielokane o 1 do 2 sekund dłużej).

ad. 4 Jak wynika z załączonych wyników testów, najdłuższą operacją jest dokonanie początkowego dowiązania do serwera (zwłaszcza autoryzowanego na znaczną odległość). Operacje przeszukania są stosunko sprawne. Należy przyjąć kryterium, że operacja przeszukania bazy nie powinna przekraczać 3 sekund. Dłuższy czas wskazuje na nadmierne obciążenie serwera, bądź tą samą bazą X.500, bądź innymi procesami. Najszybsza (zgodnie z przewidywaniem) jest operacja czytania. Przy konstrukcji DUA należy zwracać uwagę na to, aby prosić o przesłanie jedynie tych atrybutów, które nasze DUA jest w stanie obrabiać, w szczególności nie ma sensu robić transferu obrazu dla DUA tekstowego. Jednocześnie prawidłowo realizowane buforowanie tego typu danych może bardzo znacznie przyspieszyć funkcjonowanie systemu.

ad. 5 Stosunkowo szybki dostęp do danych nielokalnych wydaje się wskazywać na celowość rozpraszania bazy. Jednocześnie jednak rozpraszanie pojedynczych instytucji, w ramach których dokonywane jest przeszukiwanie, wyraźnie osłabia funkcjonowanie systemu i należy go unikać. Wydaje się zatem, że właściwym modelem jest rozproszone zarządzanie danymi skupionymi na jednym serwerze. Zarządzanie takie polega na powierzeniu pieczy nad wybranymi domenami określonym zarządcom. Mogą oni dokonywać modyfikacji danych po autoryzowanym dowiązaniu do bazy. Zarządzanie takie może być dokonywane jedynie w czasie pracy serwera i nie może dotyczyć modyfikacji danych bezpośrednio na dysku.

Bibliografia

[1] Data Communication Networks: Directory, Recommendations X500-X.521, CCITT, Fascile VIII.8 of Blue Book

[2] Marshall T. Rose (1992) *The Little Black Book: Mail Bounding with OSI Directory Services*

[3] C.J. Robbins, S.E. Kille (1992) *The ISO Development Environment: User's Manual, Volume 5: QUIPU*

[4] M. Górecka, T. Wolniewicz (1994) *Ocena efektywności rozproszonej bazy danych na podstawie X.500 Directory*, Raport NASK

[5] M. Górecka, T. Wolniewicz (1994) *Stosowanie znaków diakrytycznych w systemach baz danych X.500*, Raport NASK

[6] M. Górecka, T. Wolniewicz (1995) *X.500 — standard i usługi katalogowe*, Materiały konferencyjne, POLMAN '95