NAUKOWA I AKADEMICKA SIEĆ KOMPUTEROWA

POLSKIE KOLEJE PAŃSTWOWE

NETIA TELEKOM S.A.

MATERIAŁY SEMINARIUM „MIEDZESZYN '98" pt. „Sieć 2000"

12-14 maja 1998 r.

Warszawa 1998

netia

NAUKOWA I AKADEMICKA SIEĆ KOMPUTEROWA

POLSKIE KOLEJE PAŃSTWOWE

NETIA TELEKOM S.A.

MATERIAŁY SEMINARIUM „MIEDZESZYN '98" pt. „Sieć 2000"

12-14 maja 1998 r.

Warszawa 1998
ISBN 83-902314-7-6

Rada Programowa:

Stanisław Gago – PKP

Jan Guz – Netia Telekom S.A.

Mirosław Machalski – UOP

Mirosław Sadluk – Ericsson

Tomasz Ginał – Ericsson

Tomasz Hofmokl – NASK

Andrzej Zienkiewicz – NASK

Maciej Kozłowski – NASK

Wiktor Krzanowski – NASK

Roman Adamiec – NASK

Wstęp

To już po raz ósmy spotykamy się w Miedzeszynie. Konkurencja w zakresie usług teleinformatycznych staje się coraz silniejsza. W niektórych przypadkach wzmacniana jest celowymi działaniami administracyjnymi. Wymaga to od wszystkich uczestników tego rynku w mniejszym lub większym stopniu nowych form działania. NASK jest stosunkowo małą jednostką, której podstawowym atutem jest nieźle wyszkolona kadra stanowiąca zgrany i sprawny zespół. NASK nie posiada kapitału pozwalającego na konkurowanie z „rekinami rynku". Aby sprostać coraz większym wymaganiom musimy „uciekać do przodu"

Tym razem jednak nie pomogą już tylko proste usprawnienia techniczne. Nacisk wielkich operatorów telekomunikacyjnych jest na tyle duży, że konieczne jest wzmocnienie pozycji NASKu przez tworzenie wzajemnie korzystnych powiązań kooperacyjnych.

NASK postanowił odwrócić dotychczasową sytuację w sieciach teleinformatycznych, w tym w Internecie Zamiast dławić się na zbyt mało przepustowych połączeniach międzynarodowych i krajowych postanowiliśmy zbudować sieć, w której ograniczenia przepustowości występują przede wszystkim na portach przyłączenia abonentów.

W tym celu nawiązaliśmy współpracę z operatorem TELIA AB, jednym z głównych udziałowców systemu kablowego BALTICA.. Od niego wydzierżawiamy linię o przepustowości SDH STM-1, 155 Mb/s, na trasie Kołobrzeg - Sztokholm. W wyniku negocjacji Telia – TP S.A. ustalono, że w pierwszym okresie podłączenie NASK do tej linii nastąpi w Warszawie. Równolegle zawarliśmy umowę o współinwestowanie z PKP, od której wydzierżawimy w zamian za wkład inwestycyjny kanał SDH STM-1, 155 Mb/s w podwójnym pierścieniu obejmującym podstawowe miasta kraju. Po nałożeniu na pierścienie SDH naszej sieci ATM uzyskamy w całym kraju, jak to obecnie dzieje się w Warszawie i na trasie do Łodzi, sieć ATM o dużej przepływności. Spodziewamy się, że rozwiąże to problem przepełnienia sieci na okres roku, a może i półtora.

Od lat preferowana przez nas współpraca z TP S.A. nie przynosi spodziewanych rezultatów z przyczyn trudno dla nas zrozumiałych. Dobrze natomiast rozwija się współpraca z holdingiem Netia Telecom S.A., który dodatkowo powiązany z Telia AB pozwala mieć nadzieję na bardzo owocną i stabilną współpracę leżącą w interesie obu partnerów, tym bardziej, że wzajemnie oferowane usługi uzupełniają się nawzajem tworząc dla użytkownika bardzo atrakcyjną ofertę.

Zmiana koncepcji budowy sieci, do której dostęp decyduje o możliwościach abonenta, radykalne zwiększenie skali działań oraz liczby abonentów pozwalają na zmianę taryfikacji w sieci NASK. Po pierwsze, staje się możliwe odejście od zasady taryfikacji za ruch na rzecz ryczałtowej opłaty za port, po drugie staje się możliwe radykalne obniżenie cen jednostkowych. Zmiana zasady jaka leży u podstaw

Z PROBLEMATYKI PRAWA AUTORSKIEGO I PRASOWEGO W SIECIACH KOMPUTEROWYCH

mgr Sybilla Stanisławska

Instytut Wynalazczości i Ochrony Własności Intelektualnej
Uniwersytet Jagielloński

1. DOSTĘP DO ZASOBÓW INTERNETU

Internet jest źródłem upowszechniania wiedzy, kultury. Jest „narzędziem" dostępu do informacji – tak niezbędnej i ważnej w dzisiejszym świecie.

Jest nowym medium o zasięgu globalnym, zdecentralizowanym, nie podlegającym kontroli jakiegokolwiek instytucji państwowej czy prywatnej, jak i nie dającym się kontrolować, ze względu na zasięg i uwarunkowania techniczne. Stwarza on nowe możliwości partycypacji w przekazywaniu informacji, i to na pewno większe niż jakikolwiek inny środek masowego przekazu już istniejący, albowiem użytkownicy (odbiorcy) mogą być jednocześnie redaktorami i wpływać na przekazywaną treść.

Internet ułatwia komunikację, wymianę informacji, które stają się dostępne niemal na całym świecie, natychmiast po wprowadzeniu do pamięci jednego z komputerów podłączonych do Internetu.

Do tych wielu pozytywnych cech należy dodać to, iż jest stosunkowo tanim medium zarówno dla osób, które posiadają (utrzymują) swoje strony WWW jak i tych którzy tylko wędrują po zasobach Internetu. Coraz częściej wprowadzane są jednolite miesięczne opłaty abonamentowe. Umożliwia on korzystanie z informacji o każdej porze, w każdym miejscu na globie ziemskim, pozwala kontaktować się ludziom z odległych miejsc.

Oprócz tych niewątpliwych zalet, należy zwrócić uwagę na fakt, iż jest to bardzo niebezpieczne medium, dzięki któremu można małym kosztem:
– propagować treści szkodliwe, pornograficzne, obraźliwe, naruszające dobra osobiste osób trzecich,
– rozpowszechniać bez zgody autorów utwory, które podlegają ochronie przewidzianej w prawie autorskim.

Korzystanie z utworów wprowadzonych do Internetu jest możliwe głównie dzięki możliwościom jakie stworzył postęp techniczny, a szczególnie digitalizacji – która polega na transformowaniu utworów (materiałów) do formy zapisu cyfrowego, dzięki temu mogą one być przechowywane w jednej postaci i na jednym nośniku np. CD-ROM-ie.

Bardzo trudno poddać Internet kontroli prawnej, przede wszystkim ze względu na to, że jest to zdecentralizowane medium o zasięgu globalnym, nad którym nikt nie ma władzy. Jedna z pierwszych prób została przeprowadzona przez Amerykanów. Próbowali oni wprowadzić odrębną regulację prawną dotyczącą Internetu, a w szczególności wprowadzić kontrolę treści rozpowszechnianych za pomocą sieci komputerowych. W lutym 1995 r. Kongres USA rozpatrywał projekt ustawy – Prawo o przyzwoitości telekomunikacji (CDA – Communication Detency Act). Ustawa ta wprowadzałaby ograniczenie wolności wypowiedzi w mediach telekomunikacyjnych ze szczególnym uwzględnieniem sieci komputerowych. Ograniczenia takie nie są przewidziane w stosunku do innych form wypowiedzi, co powoduje że teksty które mogły być swobodnie rozpowszechniane w druku, nie zawsze mogłyby zostać wprowadzane do sieci komputerowej, gdyż musiałyby podlegać kontroli czy nie zawierają treści „nieprzyzwoitej, nieobyczajnej, gorszącej".

jednocześnie użytkownikami Internetu. Istniejące od 1995 r. Stowarzyszenie Polska Społeczność Internetu propaguje Internet jako powszechne medium komunikacyjne i jednocześnie zaproponowało opracowanie kodeksu postępowania dziennikarzy korzystających z sieci Internet w celach zawodowych.

Trzeba mieć na uwadze, że Internet to nie tylko czasopisma internetowe. Internet jest źródłem informacji udostępnianej przez instytucje rządowe, parlamenty, jak i podmioty prowadzące działalność komercyjną, w tym reklamową. Wśród sposobów wykorzystania sieci komputerowych do najbardziej rozpowszechnionych należą: poczta elektroniczna, grupy dyskusyjne, czy strony WWW (World Wide Web – ogólnoświatowa pajęczyna – dzięki której można skorzystać z informacji, materiałów zawartych w komputerach rozmieszczonych na całym świecie).

INTERNET W POLSCE – PODSTAWY PRAWNE FUNKCJONOWANIA

Funkcjonowanie Internetu w Polsce i świadczenie w jego ramach usług uregulowane zostało ustawie o łączności z dnia 23 XI 1990[5]. Po dokonanej w maja 1995 r. nowelizacji tej ustawy wprowadzono nową definicję usług telekomunikacyjnych, przez które rozumie się działalność gospodarczą polegająca na zapewnieniu przekazu informacji za pomocą sieci i linii telekomunikacyjnych (art. 3 ust.1 pkt.14)[6]. Na gruncie powołanej ustawy udostępnianie korzystania z Internetu przy wykorzystaniu sieci telekomunikacyjnej jest usługą z zakresu telekomunikacji i wymaga uzyskania koncesji.

Głównym operatorem sieci Internetu w Polsce jest NASK (Naukowe i Akademickie Sieci Komputerowe). NASK jest jednostka badawczo-rozwojową utworzoną zarządzeniem Przewodniczącego Komitetu Badań Naukowych i posiada osobowość prawną..

NASK posiada koncesję na świadczenie usług transmisji danych i poczty elektronicznej w ruchu krajowym i międzynarodowym.

OGRANICZENIA KORZYSTANIA Z MATERIAŁÓW DOSTĘPNYCH W INTERNECIE

Pierwsze i zarazem najbardziej znaczące ograniczenie potocznie rozumianej całkowitej swobody korzystania z materiałów wprowadzonych do sieci komputerowych może wynikać z przepisów prawa autorskiego. Odnosi się to zarówno do możliwości korzystania z już rozpowszechnionych w Internecie materiałów, jak i możliwości decydowania o udostępnieniu takich materiałów poprzez umieszczenie ich w ogólnie dostępnej sieci komputerowej.

Świadomie używam określenia „materiałów" znajdujących się w sieciach komputerowych, ponieważ tylko te materiały, które są utworami w rozumieniu prawa autorskiego korzystają z ochrony przewidzianej przepisami prawa autorskiego.

Utworem jest przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia (art. 1 pr. aut)[7]. Wytwór niematerialny musi spełniać łącznie trzy przesłanki aby można go było uznać za utwór:
– musi stanowić rezultat pracy człowieka, a nie maszyny,
– musi stanowić przejaw działalności twórczej, stanowić rezultat działalności o charakterze kreacyjnym – cecha ta jest określana jako oryginalność,
– mieć indywidualny charakter,

Przesłanka twórczości (oryginalności i indywidualności) może ujawniać się w doborze, układzie, wyborze, uporządkowaniu składników utworu (art.3 pr. aut.).

---

[5] Tekst jednolity ze zmianami: Dz.U. z 1995r., nr 117, poz 546.

[6] Wcześniejsza ustawa o łączności za usługi telekomunikacyjne uznawała tylko te, które polegały na zarobkowym zapewnianiu połączeń telefonicznych lub telegraficznych.

[7] Dz. U. z 1994 r.,nr 24, poz. 83.

Wyjątkowo ustawa przewiduje, iż prawo autorskie majątkowe przysługuje innej osobie niż twórca dzieła, np. art.74 ust.3 pracodawcy przysługują prawa majątkowe do utworu komputerowego stworzonego przez pracownika w ramach wykonywania obowiązków ze stosunku pracy, chyba że w umowie postanowiono inaczej.

W przypadku stworzenia dzieła przez kilku twórców przysługuje im prawo autorskie wspólnie (art.9 pr. aut.).

Autorskie prawa majątkowe do utworu zbiorowego, a w szczególności do encyklopedii lub publikacji periodycznej przysługują producentowi lub wydawcy, a do poszczególnych części mających samodzielne znaczenie – ich twórcom. Ponadto domniemywa się że producentowi lub wydawcy przysługuje prawo do tytułu (art. 11 pr. aut.).

Autorskie prawa osobiste (art. 16 pr. aut.) chronią nieograniczoną w czasie i nie podlegającą zrzeczeniu się lub zbyciu więź twórcy z utworem, a w szczególności prawo do:

– **autorstwa utworu** (żądanie aby osoby trzecie uznały, że on jest autorem),
– **oznaczenia utworu swoim nazwiskiem lub pseudonimem albo udostępnienia go anonimowo**,
– **decydowania o pierwszym udostępnieniu dzieła publiczności,**
– **nadzór nad sposobem korzystania z utworu,**
– **nienaruszalności treści i formy utworu i jego rzetelnego wykorzystania**,

Naruszenie prawa do integralności dzieła może przejawiać się w dokonywaniu zmian, pominięć, wprowadzeniach do utworu uzupełnień, dodatków.

Za naruszenie prawa do integralności utworu uznano w orzecznictwie polskim także[9]:

– opatrzenie tekstu ilustracjami niezgodnymi z jego charakterem,
– zniekształcenie dźwięku ilustracji muzycznej przy sporządzaniu kopii,
– sporządzenie kopii utworu, która ze względów technicznych ma gorszą jakość np. nieostre kontury, wyblakłe kolory,
– emitowanie koloryzowanej wersji filmu zrealizowanej pierwotnie w formie czarno-białej,
– przerywanie emisji utworu reklamami w miejscach przez twórców do tego nie przewidzianych

Do naruszenia rzetelności wykorzystania utworu dochodzi wtedy, gdy sposób prezentacji utworu fałszywie sugeruje oryginalny kształt dzieła, wprowadza w błąd odbiorców dzieła. Nierzetelnym wykorzystaniem dzieła może być opatrzenie zdjęcia dostarczonego przez fotografa dowolnym nieprawdziwym komentarzem[10], czy wybór małego fragmentu utworu i zaprezentowanie zawartej w nim tezy go jako reprezentatywnej dla całości poglądów autora,

Autorskie dobra osobiste nie są ograniczone w czasie.

Wraz z wprowadzaniem utworów do sieci komputerowej pojawia się niebezpieczeństwo częstego naruszania autorskich praw osobistych. Mam tu na myśli przede wszystkim pomijanie autorstwa utworu i naruszanie integralności utworu, o tyle niebezpieczne że trudne do stwierdzenia dla użytkowników, którzy nie są w stanie sprawdzić czy otrzymali dzieło w takiej formie w jakiej autor je ustalił.

Do uprawnień o charakterze majątkowym należy prawo:

– **do korzystania z utworu**,
– **rozporządzania utworem na wszystkich polach eksploatacji**,
– **do wynagrodzenia za korzystanie z utworu na każdym polu eksploatacji**.

Kategorycznie sformułowane są przepisy dotyczące umów autorskich i w szczególności wymóg wyraźnego wyliczenia pól eksploatacji w każdej umowie.

---

[9] J. Barta, R. Markiewicz, w(:) J. Barta, M. Czajkowska-Dąbrowska, Z. Ćwiąkalski, R. Markiewicz, E. Traple, Komentarz do ustawy o prawie autorskim i prawach pokrewnych, Dom Wydawniczy ABC, 1995, str. 143.

[10] Nie publikowane orzeczenie SN z 21 września 1963 r. I CR 734/62.

korzystania z sieci) będzie niemal na każdym kroku dochodziło do naruszenia prawa autorskiego i odpowiedzialności użytkownika lub operatora sieci. W związku z tym, iż nie doszło do wypracowania zadowalającego wszystkie strony stanowiska, artykuł ten został usunięty i nadal obowiązuje definicja reprodukcji zawarta w art. 9 konwencji berneńskiej[16]. Według M. Lehmana[17] czasowe przechowywanie utworu w pamięci komputera będzie dozwolone w świetle istniejącej regulacji. Jak zauważył on, postawa środowisk, które doprowadziły do usunięcia art.7, nie oznacza, iż dążą one do stworzenia „otwartego systemu" w którym dozwolone byłoby czasowe kopiowanie utworów znajdujących się np. w Internecie.

Ostatecznie w Konwencji I wprowadzono dwa uprawnienia nie znane w tym ujęciu konwencjom dotychczas obowiązującym. Pierwsze z nich, to prawo wprowadzania do obrotu (art. 6 – rights of distribution)[18], które zezwala autorowi utworu literackiego i artystycznego[19] na publiczne udostępnianie (making available) dzieła lub jego kopii poprzez sprzedaż lub inną formę przeniesienia własności.

Drugie uprawnienie to przewidziane w art. 8 prawo zezwalania na przewodowe lub bezprzewodowe (rozpowszechnianie) udostępnianie utworu publiczności (right of authorizing any communication to the public)[20].

Trzeba zauważyć, że w oświadczeniu dotyczącym konwencji I WIPO wyjaśniono znaczenie pojęć: „kopia" oraz „kopia i oryginał". Zgodnie z tym oświadczeniem za kopie należy uznać materialne przedmioty. W związku z tym w art. 6 konwencji zdefiniowano prawo wprowadzania do obrotu kopii utworu – utrwalonych w materialnej formie (tangible object).

W związku z tym „publikacja elektroniczna" mogłaby zostać uznana za formę rozpowszechniania utworu[21], a nie za publikacje[22] w rozumieniu prawa autorskiego, gdyż nie dochodzi tu do wytworzenia materialnych egzemplarzy.

---

[16] art. 9 ust. 1 kon. berneńskiej „ autorzy dzieł literackich i artystycznych chronionych przez niniejsza konwencję korzystają z wyłącznego prawa udzielania zezwolenia na reprodukcję tych dzieł, bez względu na sposób i formę, których miałaby ona nastąpić ."

[17] Artykuł bez podania autorstwa, WIPO Delegates Degree on Two Treaties, BNA's, 1997, vol.53, str.146.

[18] Tekst angielski w brzmieniu:

(1) Authors of literary and artistic works shall enjoy the exclusive right of authorizing the making available to the public the oryginal and copies of the work though sale or other transfer of ownership.

(2) Nothing in this Treaty shall affect the freedom of Contracting Parties to determine the conditions, if any, under which the exhaustion of the right in the paragraph (1) applies after the first sale or other transfer of ownership of the original of the work with the authorization of the author."

[19] W rozumieniu konwencji utworami są także programy komputerowe (art.4) i banki danych (compilation of data- art. 5).

[20] Tekst angielski w brzmieniu:

Without prejudice to the provision of Articles 11(1)(ii), 11bis (1)(i) and (ii), 11ter (1)(ii), 14(1)(ii) and 14 bis (1) of the Berne Convention, authors of literary and artistic works shall enjoy the exclusive right of the authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and a time individually chosen by them.

[21] Utworem rozpowszechnionym jest utwór, który został za zezwoleniem twórcy udostępniony publicznie- art. 6 pkt.3 pr. aut.

[22] Utworem opublikowanym jest utwór, który za zezwoleniem twórcy został publicznie zwielokrotniony i którego egzemplarze zostały udostępnione publicznie- art. 6 pkt. 1 pr. aut.

DOZWOLONY UŻYTEK UTWORÓW W SPOŁECZEŃSTWIE INFORMATYCZNYM

mgr Joanna Marcinkowska

Instytut Wynalazczości i Ochrony Własności Intelektualnej UJ

Postęp techniczny a przede wszystkim coraz szersze wykorzystywanie utworów spowodowały, iż obecnie funkcjonowanie prawa autorskiego uzyskało utartą już nazwę: **prawo autorskie w społeczeństwie informatycznym.**

Interesująca wydaje się kwestia na ile obowiązujące rozwiązania umów międzynarodowych a także ustaw krajowych pozwalają na korzystanie z utworów w środowisku digitalnym, bo przecież społeczeństwo przekazuje i czerpie informacje przede wszystkim dzięki rozbudowanym, autostradom ulokowanym w środowisku digitalnym. Nie będę tu wymieniać oczywistych zalet autostrad informatycznych, chociaż zalety te tracą czasami swoje walory, kiedy użytkownik chce dostać się do sieci pod określony adres i staje się to nie możliwe, bądź trwa zbyt długo. Sądzę jednak, że i tym niedogodnościom przyjdzie z pomocą postęp techniczny.

„Zadaniem prawa autorskiego jest nie tylko popieranie twórczości ale także zapewnienie odbiorcom jak najszerszego dostępu do jego rezultatów, czego wymaga postęp naukowy i kulturalny całej ludzkości; możemy zatem określić tę ideę prawa autorskiego **koncepcją systemu informacyjnego"** (prof. A. Kopff: Wpływ postępu techniki na prawo autorskie, ZN UJ, 1988r., s. 70).

Podobnie jak przed laty, tak i teraz wyłania się pytanie, czy w związku z łatwością korzystania z utworów bez odpowiedniej rekompensaty dla twórców, nie mówiąc już o uzyskaniu ich zgody, nie należałoby ustanowić prawa informatycznego, które zastąpiłoby uregulowania autorsko – prawne. Obserwując jednak poczynania na arenie międzynarodowej odpowiednie regulacje prawne (konwencje, dyrektywy, porozumienia) przede wszystkim idą w kierunku modyfikacji przepisów prawa autorskiego poprzez ich odpowiednią interpretację. Warto może podkreślić, iż wbrew wcześniejszym obawom nie mamy do czynienia z rewolucyjną zmianą zasad i utrwalonych reguł prawa autorskiego. Najnowsze bowiem postanowienia międzynarodowe zmierzają bardziej właśnie do interpretacji znanych rozwiązań, niż do ich całkowitej zmiany. Jest rzeczą oczywistą, że nawet takie interpretacje, czy wykładnie prawa zmieniają jego obraz ale nie można chyba mówić byśmy mieli do czynienia z przewrotem w tej dziedzinie.

Oprócz tego pojawiają się ustawy krajowe, które regulują ogólne zasady funkcjonowania usług informacyjnych i komunikacyjnych, jak np. tego rodzaju ustawa niemiecka z lipca ubiegłego roku, która jednak nie usuwa w cień postanowień prawa autorskiego a może jedynie w pewnym zakresie je uzupełnia. Tak więc można chyba powiedzieć, że regulacje prawne wymuszone przez postęp techniczny idą w dwóch kierunkach (wykładnia, dostosowanie prawa autorskiego, prawo przekazu informacji).

Nie można także pominąć faktu, iż nowe możliwości jakie stwarza środowisko digitalne wywołało szalone poruszenie zarówno w środowiskach twórczych, użytkowników jaki i dostawców informacji. To z kolei pociągnęło za sobą mobilizację wielu sił ludzkich dla rozważenia i rozwiązania w miarę możliwości powstałych wątpliwości. „Możliwości" te polegają przede wszystkim na osiągnięciu kompromisu miedzy podmiotami uprawnionymi z tytułu praw autorskich a żądnym wszelkiej informacji społeczeństwem. Należy także wskazać, że wszystkie opracowywane dokumenty za bazę wyjściową uznają postanowienia konwencji berneńskiej i zakładają, że nowe regulacje nie będą naruszać jej postanowień.

Pierwszą reakcją na rzeczywiste funkcjonowanie społeczeństwa informatycznego była Zielona Księga (Greenpaper, Grünbuch) Komisji Europejskiej z 1995r.(oprócz Białej Księgi

Porozumienie WIPO I przewiduje w art. 8, że podmioty prawa autorskiego mają wyłączne prawo zezwalania **publiczne rozpowszechnianie** ich dzieł łącznie z ich publicznym udostępnianiem drogą przewodową i bezprzewodową i że mogą oni także decydować o publicznym udostępnianiu utworów, które zachodzi także wtedy gdy odbiorca może mieć dostęp do dzieła w miejscu i w czasie przez siebie wybranym (online transmisssion). Wynika stąd zatem, że publiczne udostępnianie utworu nie musi być jednocześnie odbierane przez wiele osób. W ten sposób wskazane wcześniej niemieckie interpretacje muszą ulec modyfikacji. Treść art. 8 wskazuje, że zostało wyodrębnione nowe prawo, które polega na decydowaniu o samym **udostępnieniu** utworu w sieci. W ten sposób istotne dla prawa autorskiego staje się nie tylko przywołanie utworu ale już samo jego udostępnienie potencjalnym odbiorcom.

Ponadto wskazane wcześniej wątpliwości UE (zamieszczone Zielonej Księdze), czy wprowadzenie utworu do sieci objęte jest prawem wyłącznym również zostało wyjaśnione na korzyść podmiotów uprawnionych.

Także na podstawie porozumienia WIPO I artyści wykonawcy i producenci fonogramów uzyskują wyłączne prawo do decydowania o wprowadzeniu ich dóbr do środowiska sieci. Przyjęta jednak tutaj konstrukcja nie ma charakteru wyłącznego ale wiąże się z prawem do wynagrodzenia.

Z kolei wyjaśnienia do porozumienia WIPO I precyzują, że zagwarantowane w art. 9 konwencji berneńskiej prawo autorów dzieł literackich i artystycznych udzielania zezwolenia na **reprodukcję** dzieł, w pełni odnosi się także do środowiska cyfrowego. Oznacza to zatem, że wprowadzenie utworów do sieci stanowi ich reprodukcję (zwielokrotnienie), podobnie jak przechowywanie dzieła w stałej pamięci komputera (medium elektronicznego).
Jednakowe postanowienia w zakresie prawa reprodukcji zapisane zostały w drugim porozumieniu o ochronie artystów wykonawców i producentów fonogramów (WIPO II).

Przygotowany w listopadzie 1997r. przez komisję Europejską projekt dyrektywy dotyczącej prawa autorskiego w społeczeństwie informatycznym stanowi bezpośrednie następstwo Zielonej Księgi a także porozumień WIPO. Z uwagi na to, że UE była stroną porozumień WIPO, projekt wskazanej dyrektywy jest nie tylko chęcią dorównania regulacjom o zasięgu światowym ale i obowiązkiem Unii.

Art. 2 projektu stanowi, iż prawo **zwielokrotniania** obejmuje wyłączne prawo udzielania zezwalania lub nie, w pełnym zakresie lub częściowo na bezpośrednie, pośrednie, czasowe i trwałe zwielokrotnianie utworu bez względu na sposób i formę, w której miałoby ono nastąpić. To sformułowanie jest bliskie pojęciu zwielokrotniania zawartemu w dyrektywie z 1992r. dotyczącej prawa wynajmu i wypożyczania, które jednak ograniczało się tylko do bezpośredniego lub pośredniego zwielokrotniania, a także zawiera elementy zwielokrotniania przyjętego w dyrektywie o ochronie programów komputerowych z 1991r.i dyrektywie o ochronie baz danych z 1996r., które z kolei mówią o czasowym lub trwałym zwielokrotnianiu.

Przyjęte w projekcie rozwiązanie szerokiego rozumienia tego prawa (prawa zwielokrotniania) pozostaje w zgodzie z art. 9 ust. 2 konwencji berneńskiej, który stanowi, iż „ustawodawstwu państw należących do Związku zastrzega się możność zezwalania na reprodukcję tych dzieł w pewnych szczególnych przypadkach, pod warunkiem, że reprodukcja ta nie wyrządzi szkody normalnemu korzystaniu z dzieła ani nie przyniesie nieuzasadnionego uszczerbku prawowitym interesom autora". W przeciwnym razie pominięcie w tej definicji np. niektórych form czasowego zwielokrotniania mogłoby pozostać w sprzeczności z normalnym korzystaniem z dzieła lub z prawowitymi interesami autora.

Dyskutowane wielokrotnie i budzące wiele wątpliwości **prawo publicznego rozpowszechniania i udostępniania** utworów zostało sformułowane w art. 3 projektu identycznie jak we wcześniej wskazanych porozumieniach WIPO. Tak więc twórcom zagwarantowane zostało wyłączne prawo przewodowego lub bezprzewodowego rozpowszechniania utworów jak i wyłączne prawo udostępniania utworów według miejsca i czasu indywidualnie oznaczonego przez

Dlatego też to rozwiązanie powinno być wzmocnione odpowiednim systemem wynagradzania. Jakie jednak przyjęte zostanie rozwiązanie, pokaże ostateczna wersja dyrektywy.

Ponadto w projekcie zaznacza się, iż zwielokrotnianie w ramach **użytku prywatnego** może być dokonywane jedynie przez osoby fizyczne i dla celów niegospodarczych.

Wreszcie ustęp 3 art. 5 opisuje sytuacje dozwolonego korzystania z utworów:

- dla zobrazowania nauczania,
- badań naukowych,
- dla celów niekomercyjnych przez osoby upośledzone słuchowo i wzrokowo,
- korzystania z fragmentów utworów dla przekazywania informacji o bieżących wydarzeniach oraz
- korzystania z utworów dla celów bezpieczeństwa publicznego, postępowania sądowego i administracyjnego.

Dla potwierdzenia jak wiele wciąż wątpliwości budzi wykorzystywanie utworów w środowisku digitalnym, a przede wszystkim korzystanie z nich na podstawie licencji ustawowych, należy jeszcze wskazać, iż w październiku ubiegłego roku, a więc jeszcze przed opracowaniem projektu dyrektywy, odbyła się w Amsterdamie międzynarodowa konferencja pod patronatem Komisji Europejskiej. Uczestnikami tej konferencji była przede wszystkim Międzynarodowa Federacji Bibliotek (IFLA) oraz przedstawiciele z krajów Europy, St. Zjednoczonych, Australii, Japonii. Celem tej konferencji było m.in. przeanalizowanie problemów związanych z zastosowaniem ustawowych ograniczeń pr. autorskich do środowiska digitalnego oraz próba znalezienia konstruktywnych rozwiązań. Nie na wszystkie wątpliwości udało się znaleźć stosowne *remedium*, jednakże sama wymiana poglądów i doświadczeń pozwoliła ukierunkować plan dalszych prac, które posłużą opracowaniu kolejnej dyrektywy.

I tak można nadmienić, iż zgodnie ustalono, że:

- w zakresie ustawowych ograniczeń praw autorskich należy dokładnie przeanalizować ich racje, gdyż może się okazać, że w środowisku digitalnym nie znajdują one uzasadnienia; odnosi się to m.in. do usług bibliotecznych, gdyż obecnie ich forma i zasięg zdecydowanie odbiegają od dotychczasowych, chociaż biblioteki powinny nadal korzystać z uprzywilejowanej pozycji, lecz może zmodyfikowanej
- powinno zostać doprecyzowane, które akty zwielokrotniania są relewantne dla pr. autorskiego,
- korzystanie z utworów ulokowanych w środowisku digitalnym w ramach użytku prywatnego nie powinno korzystać z dotychczasowych przywilejów jednakże poszczególne akty takiego korzystania powinny znaleźć swoją regulację, np. jak osoby prywatne mogą wykorzystać legalnie otrzymane kopie utworów, w jakim zakresie mogą przekazywać taki materiał osobom trzecim, które akty prywatnego korzystania z utworów mogą być dozwolone,

Uwagi ogólne:

1) przedstawione działania i kierunki rozwiązań wskazują, iż społeczeństwo informatyczne nie jest tworem nietykalnym, funkcjonującym w oparciu o zasadę wolnego rynku lecz staje się coraz bardziej ujarzmione przez odpowiednie regulacje prawne,
2) ponadto wyraźnie widać, że mimo istnienia wielu możliwości technicznych wykorzystywania utworów, rozwiązania prawne zmierzają w kierunku poszanowania praw podmiotów prawa autorskiego i praw pokrewnych
3) jeśli chodzi o **użytek prywatny**, to okazuje się, że dotychczasowe rozwiązania, polegające na bezpłatnym korzystaniu z utworów a zwłaszcza ich zwielokrotnianiu, nie były szczególnym dobrodziejstwem ze strony ustawodawcy, z którym podmioty uprawnione musiały się pogodzić lecz swego rodzaju przymusowym rozwiązaniem, gdyż z powodu braku możliwości technicznych nie było jak ściągać od użytkowników odpowiedniego wynagrodzenia za

mamy do czynienia z publicznym udostępnieniem a nawet jego zwielokrotnieniem, to nie ma jasności jak należy rozumieć pojęcie **egzemplarze**. Tradycyjnie rozumie się przez to nośniki materialne. W porozumieniu WIPO zostało wyjaśnione, że takie pojęcia jak „kopie" i „oryginał" należy rozumieć jako utwory utrwalone w formie materialnej. Ale wyjaśnienie to odnosi się do aktów sprzedaży i dzierżawy egzemplarzy. Gdyby więc rozszerzyć zastosowanie tego wyjaśnienia, to nie można by mówić o publikacji utworów w środowisku elektronicznym a o ich rozpowszechnieniu.
Czy przy takim rozumowaniu nie można by korzystać z utworów w ramach art. 27? Czy trzymać się brzmienia ustawy, czy tez interpretować ją pod katem celu ustanowienia takiego przepisu.

Art. 28 tutaj analiza jest jeszcze trudniejsza
Można wyróżnić dwie sytuacje:

1) udostępnienie utworów w ramach zamkniętej sieci, ci by miało taki sam charakter jak normalne udostępnianie książek; w taki sam sposób można by odczytać ust. 2 tego artykułu, który zezwala na sporządzanie egzemplarzy niedostępnych w handlu. Mimo, iż obecnie ustawa nie daje podstaw aby sporządzać unikalne egzemplarze na mikrofilmach, to jednak przyjmuje się, że ze względu na interes publiczny jest to dopuszczalne, więc może w ten sam sposób można rozszerzyć wykładnię także na zamknięta sieć;
2) druga sytuacja to taka, czy biblioteka może przekazywać zawartość swoich zbiorów online – wg projektu dyrektywy nie;

wydaje się, że ten przepis jest ukierunkowany na korzystanie z utworów w ramach danej biblioteki jako zamkniętego budynku wyposażonego w określone zbiory; być może należałoby zmienić pojęcie biblioteki.
Wskazane regulacje polskiej ustawy i związane z nimi wątpliwości wskazują, że również należy podjąć odpowiednie kroki, uwzględniając regulacje międzynarodowe, w celu dokonania odpowiedniej wykładni przepisów, nie licząc na to, że rozstrzygnięcie wątpliwości zostanie dokonane orzecznictwem sądowym; stan niepewności co do interpretacji przepisów stwarza trudności w ich stosowaniu; chodzi o to, by z czasem nie okazało się, że biblioteki, czy inne instytucje wykorzystują utwory niezgodnie z prawem; podjęcie odpowiednich działań konieczne jest dla jasności i bezpieczeństwa prawnego

- w sieci kablowych linii światłowodowych powinny istnieć odpowiednie rezerwy eksploatacyjne, co umożliwiłoby rekonfigurację sieci teletransmisyjnej i świadczenie usług transmisyjnych nawet w sytuacjach awaryjnych.

Rezultatem tych założeń jest przyjęty dla sieci PKP plan budowy kablowych linii światłowodowych do 2005 r., który jest obecnie realizowany, przy czym wprowadzane są niewielkie jego modyfikacje, wynikające z aktualnych uwarunkowań eksploatacyjno-ekonomicznych. Budowanych jest około 600 – 700 km kabli światłowodowych rocznie, co jak do tej pory jest tempem wystarczającym w stosunku do innych poczynań w zakresie telekomunikacji na PKP.

Do roku 1997 ułożono na PKP około 5000 km kabli światłowodowych wzdłuż linii kolejowych, zapewniając co najmniej dwie, niezależne drogi światłowodowe 11 głównym węzłom telekomunikacyjnym PKP. Węzły te, to największe ośrodki gospodarcze Polski – Warszawa, Katowice, Kraków, Poznań, Wrocław, Łódź, Gdańsk, Szczecin, Lublin, Bydgoszcz, Olsztyn. Ponadto w węzłach tych, tam gdzie jest to uzasadnione, układane są pierścienie światłowodowe łączące duże skupiska abonentów kolejowych. Układane w węzłach kable mają z reguły więcej włókien światłowodowych niż kable światłowodowe szlakowe, które są z reguły kablami rozetowymi, 12-włóknowymi. Około 97 % tych kabli jest ułożonych w ziemi.

Budowa kablowych linii światłowodowych nie oznacza rezygnacji z kabli miedzianych typu TKD i TKM. Dla realizacji sieci dostępowych, włączania szeregu central końcowych będą one stanowiły jedyny środek realizacji połączeń cyfrowych przy wykorzystaniu systemów HDSL, ADSL lub połączeń analogowych realizowanych przy zastosowaniu urządzeń TFN.

3. Cyfrowa sieć teletransmisyjna PKP

3.1 Wprowadzenie

PKP na bazie własnych sieci telekomunikacyjnych linii kablowych posiada również własną sieć teletransmisyjną, obejmującą zasięgiem teren całego kraju.
Do niedawna sieć teletransmisyjna była budowana przy wykorzystaniu systemów analogowych. Sieć ta umożliwiała połączenie analogowe między węzłami komutacyjnymi, a jej rozwój był ściśle związany z zapewnieniem dostępu, głównie do usług typu telefonicznego.
Wzrost zapotrzebowania na zaawansowane usługi telekomunikacyjne, w tym zwłaszcza teleinformatyczne i szerokopasmowe wymusił nowe rozwiązania w zakresie sieci teletransmisyjnych.
Ważnym zagadnieniem przy tworzeniu cyfrowej sieci teletransmisyjnej PKP było określenie celów, które powinna ona spełniać. Założono, że sieć teletransmisyjnej PKP powinna charakteryzować się między innymi:

- szybką możliwością zestawienia dróg transmisyjnych,
- ciągłym nadzorem i oceną jakości transmisji,
- szybką rekonfiguracją w przypadku awarii,
- optymalnym wykorzystaniem przepustowości transmisji,
- możliwością współpracy z różnymi systemami teletransmisyjnymi,
- dużą niezawodnością,
- możliwością jej rozbudowy.

Stąd też przyjęto zasadę, że cyfrowa sieć teletransmisyjna PKP będzie realizowana głównie w oparciu o system SDH (w nielicznych przypadkach PDH), przy wykorzystaniu światłowodowych linii kablowych. Przyjęto również założenie, że istniejąca sieć analogowa nie będzie

System zarządzania elementami sieci wykonuje następujące funkcje:
– funkcje administracyjne,
– zarządzania konfiguracją elementów,
– zarządzania informacjami dotyczącymi uszkodzeń,
– zarządzania informacjami dotyczącymi jakości.

Natomiast system zarządzania na poziomie sieci (zarządca sieci) spełnia funkcje:
– obejmuje kontrolę nad wszystkimi połączeniami występującymi w sieci,
– daje możliwość zestawiania połączeń o wymaganej przepływności pomiędzy określonymi punktami,
– rejestruje zdarzenia oraz wydaje odpowiednie komunikaty dotyczące zdarzeń (połączenia),
– zapewnia graficzne przedstawianie alarmów na poziomie sieci tzn. dokonuje w sposób dynamiczny prezentacji uszkodzonych połączeń występujących w grafie sieci,

Ponadto system nadzoru sieci teletransmisyjnej SDH-PKP umożliwia zabezpieczenie jej przed rozmyślną lub przypadkową interwencją. Dokonywane jest to poprzez zabezpieczenie fizyczne, nadawanie praw dostępu poszczególnym użytkownikom, ochronę przechowywanych danych.

3.3 Topologia sieci SDH-PKP

Do podstawowych topologii sieci z urządzeniami SDH należy zaliczyć układy połączeniowe typu „pierścień", „punkt-punkt", „łańcuch" (szyna), „gwiazda", „krata".
Na to, która z topologii sieci byłaby najodpowiedniejsza dla PKP mają wpływ różne czynniki, jak np. wymagana niezawodność i jakość transmisji, przepływność transmisyjna, położenie geograficzne obiektów (central) oraz ich hierarchia ważności.
Struktura rzeczywistej cyfrowej sieci teletransmisyjnej SDH-PKP jest kombinacją podstawowych topologii (sieć o strukturze mieszanej), przy czym główną topologią występującą w tej sieci jest struktura pierścieniowa (pierścień dwukierunkowy).
Sieć złożona z tych pierścieni jest bardziej elastyczna i prostsza do zarządzania, stąd też wydaje się jako najodpowiedniejsza dla sieci SDH – PKP.

Konfiguracja sieci teletransmisyjnej SDH została opracowana na podstawie układu linii światłowodowych, analizy ruchu generowanego przez centrale w sieci ISDN PKP oraz zapotrzebowania na łącza 2 Mbit/s ze strony sieci transmisji danych Kolpak.
Przy wymiarowaniu przepływności systemów transmisyjnych przyjęto 50% narzut dla rezerw: eksploatacyjnej i rozwojowej.
W miarę rozwoju sieci zakłada się, że powstanie układ o topologii wielopierścieniowej, uzupełnionej strukturami łańcuchowymi (kablowe linie światłowodowe do innych zarządów kolejowych).

Już obecnie wiadomo, że ze względu na wielkość ruchu jaki jest obecnie generowany i uwzględnienia wszystkich potrzeb, zwłaszcza potrzeb komercyjnych i transmisji danych PKP (sieć Kolpak i sieć intranetowa PKP) należy się liczyć z koniecznością wydzielenia dla poszczególnych poziomów sieci oddzielnych warstw transmisyjnych.
Planuje się, że powstaną następujące warstwy:

- szkieletowa (STM-16),
- regionalna (pierścienie STM-4 i STM-1 obejmujące swoim zasięgiem obszar kilku Dyrekcji Okręgowych Kolei Państwowych),
- lokalna (pierścienie STM-4 i STM-1w dużych miastach).

Wszystkie te warstwy będą ze sobą połączone i nadzorowane przez jeden system.

Centrale końcowe przeznaczone do obsługi ruchu abonenckiego, pod względem technicznym będą mniej złożone niż centrale tranzytowe. (Należy nadmienić, że wszystkie centrale końcowe umożliwiają tranzytowanie określonego ruchu np. z sąsiedniej centrali w przypadku uszkodzenia drogi podstawowej). Przewiduje się zainstalowanie w sieci ISDN PKP ponad 160 central końcowych o minimalnej pojemności 150 NN. Mniejsze skupiska abonentów będą obsługiwane przez koncentratory lub systemy PCM z wydzielaniem i koncentracją kanałów.

4.3. Sygnalizacja

Sygnalizacja w przyszłej zintegrowanej sieci telekomunikacyjnej PKP powinna:
– zabezpieczać specyficzne wymagania PKP,
– być zgodna z zarządzeniami obowiązującymi w kraju a dotyczącymi współpracy systemów komutacyjnych świadczących usługi ISDN, należących do różnych operatorów,
– być zgodna z zaleceniami UIC dotyczącymi współpracy z sieciami ISDN należącymi do różnych zarządów kolejowych,
– mieć standardowe protokóły i procedury według ETSI, podlegające ciągłemu rozwojowi w zakresie nowych usług.

Analiza w/w warunków wykazuje, że najbardziej elastycznym rozwiązaniem jest zastosowanie sygnalizacji SS7. Dotyczyć to powinno wszystkich central pracujących w warstwie tranzytowej przy założeniu, że każda centrala tranzytowa będzie miała połączenie z operatorem publicznym, a niektóre centrale będą współpracowały za jej pomocą z sieciami innych zarządów kolejowych. Sygnalizacja zaimplementowana w centralach tranzytowych PKP powinna umożliwiać współpracę:
– z sieciami operatorów publicznych polską wersją sygnalizacji SS7,
– z sieciami innych zarządów kolejowych za pomocą Euro SS7,
– wewnętrzną pomiędzy centralami według własnej wersji SS7 (zabroniony tranzyt przez sieć ISDN PKP abonentów sieci TPSA, przenoszenie informacji o abonencie do central tranzytowych wchodzących w skład łańcucha połączeniowego itd.).

Poziom central końcowych będzie się łączył z poziomem tranzytowym przy pomocy sygnalizacji DSS-1.

4.4. Numeracja oraz punkty sygnalizacyjne

Zakłada się, że plan numeracyjny będzie planem ogólnokrajowym, obejmującym wszystkie centrale sieci ISDN PKP. W związku z tym, że Ministerstwo Łączności przyznało dla sieci telekomunikacyjnej PKP wyróżnik sieci (WST = AB= 28)) numer krajowy abonenta (KNA) powinien składać się z 9 cyfr: KNA = AB = SPQMCDU.
Połączenia abonentów PKP z abonentami sieci publicznych będą realizowane po wybraniu docelowej centrali tranzytowej i wybraniu cyfry „0". Połączenia tego typu mogliby realizować tylko abonenci uprawnieni.
Numery tranzytowe w ruchu międzynarodowym do sąsiednich Zarządów Kolejowych będą odpowiadać zaleceniom UIC. Według nich numery te są 4 cyfrowe, przy czym dwie pierwsze cyfry to „90" jako prefiks połączenia międzynarodowego, dwie pozostałe odpowiadają numerom kierunkowym danego kraju np. dostęp do sieci PKP z europejskiej sieci kolejowej jest przez numer „9048".
W ramach otrzymanej koncesji sieci telekomunikacyjnej PKP Ministerstwo Łączności przyznało ze swojej rezerwy grupę numerów krajowych punktów sygnalizacyjnych
NSCP = 111 ZZZ,
gdzie: 111 – oznacza numer obszaru sygnalizacji sieci krajowej (SAC– część NSCP),

- poziom pierwotnego(ych) zegara(ów) odniesienia – PRC,
- poziom zegarów podrzędnych w węzłach tranzytowych – SSU-T,
- poziom zegarów urządzeń (krotnic) – SEC,
- poziom zegarów central tranzytowych – CTG oraz CT,
- poziom zegarów central końcowych – CK.

Na wszystkich poziomach hierarchii powinna obowiązywać zasada, że parametry wtórnego źródła sygnałów synchronizacji wyższego poziomu są lepsze od parametrów wtórnego źródła synchronizacji niższego poziomu. Wszystkie elementy wewnątrz węzła powinny być synchronizowane do zegara o najwyższym stopniu hierarchii w węźle.

Zakłada się, że docelowa struktura cyfrowej sieci synchronizacyjnej PKP będzie zawierała jeden główny zegar odniesienia PRC, spełniający zalecenia ITU-T G.811 i zlokalizowany w węźle transmisyjnym Warszawa. Przyjmuje się także to, że zegar ten będzie wyposażony we własne wzorce cezowe, odbiornik GPS oraz w inne niezbędne zespoły pomocnicze. Do tego PRC powinien być także doprowadzony sygnał częstotliwości wzorcowej, np. z Głównego Urzędu Miar w Warszawie.

Taka lokalizacja zegara PRC (centralne położenie) umożliwi minimalizację długości dróg przesyłania sygnałów synchronizacyjnych. W przyszłości, przy rozbudowie cyfrowej sieci telekomunikacyjnej PKP nie wyklucza się możliwości budowy rezerwowego zegara PRC zlokalizowanego w węźle transmisyjnym w Poznaniu.

W wyniku analizy prawdopodobnej struktury cyfrowej sieci telekomunikacyjnej PKP planuje się, że docelowo w kilku węzłach cyfrowej sieci telekomunikacyjnej PKP, a mianowicie w Warszawie, Poznaniu Katowicach, Gdańsku i Lublinie będą zainstalowane zegary podrzędne, klasy SSU-T, spełniające zalecenia ITU-T G.812 i standardy ETSI (dokument DE/TM 3017-4). Zegary te powinny być wyposażone dodatkowo w odbiorniki sygnałów GPS.

Wszystkie krotnice SDH stanowiące węzły w cyfrowej sieci telekomunikacyjnej PKP będą wyposażone w zegary SEC spełniające zalecenia ITU-T G.813 oraz będą stanowiły węzły w sieci synchronizacyjnej.

Obecnie w cyfrowej sieci telekomunikacyjnej PKP, sieć synchronizacyjna jest wyposażona jedynie w trzy zegary SSU-T zlokalizowane w węzłach: Warszawa, Poznań, Katowice. Zegary te są wyposażone w odbiorniki sygnałów GPS. Tak skonfigurowane zegary SSU-T będą stanowić źródła sygnałów odniesienia klasy PRC, przy czym zespół SSU-T zlokalizowany w DG PKP w Warszawie będzie pełnił funkcje głównego zegara odniesienia, natomiast zegar SSU-T w węźle Poznań będzie pełnił funkcje zegara rezerwowego dla głównego zegara odniesienia. Sygnały synchronizacyjne z tych zegarów są rozprowadzane do krotnic SDH oraz dalej do central oraz innych elementów sieci wymagających synchronizacji.

Zakłada się, że w docelowej strukturze sieci synchronizacyjnej wszystkie zegary PRC i SSU będą koordynowane ze skalą czasu UTC.

Najważniejsze hierarchicznie warstwy sieci synchronizacyjnej PKP będą działały w oparciu o cyfrowe systemy transmisyjne SDH, a systemy z hierarchii plezjochronicznej będą pełniły rolę uzupełniającą.

W cyfrowej sieci teletransmisyjnej PKP, nośnikami sygnałów synchronizacyjnych będą głównie sygnały STM-N początkowo STM-1, a następnie po rozbudowie sieci STM-4 i STM-16, a w zakresie linii plezjochronicznych sygnały 2048 kbit/s.

Sygnały synchronizacyjne odtwarzane ze strumieni 2048 kbit/s, przesyłanych przez sieć transmisyjną SDH i wydzielanych na stykach dopływowych krotnic SDH nie będą wykorzystywane, jako sygnały odniesienia, do synchronizacji węzłów i central z uwagi na skażenie ich fluktuacjami fazy, wynikającymi z mechanizmu przetwarzania wskaźnika.

3. W zakresie zewnętrznych uwarunkowań prawnych, PKP mają koncesję Nr 213/07 na świadczenie usług telekomunikacyjnych i zezwolenie na zakładanie i używanie wydzielonej sieci telekomunikacyjnej. Zakres ten jest na obecnym etapie wystarczający do tego by już zarabiać na sieci telekomunikacyjnej PKP. W miarę nowelizacji aktów prawnych w zakresie telekomunikacji należy dbać o to, by te uprawnienia rozszerzać.

Obecnie PKP świadczy usługi przede wszystkim w postaci dzierżawy kanałów cyfrowych, między innymi naszymi klientami są: TPSA, NASK, operatorzy sieci komórkowych itd.

ZASADY BUDOWY SIECI TELEKOMUNIKACYJNYCH NETII

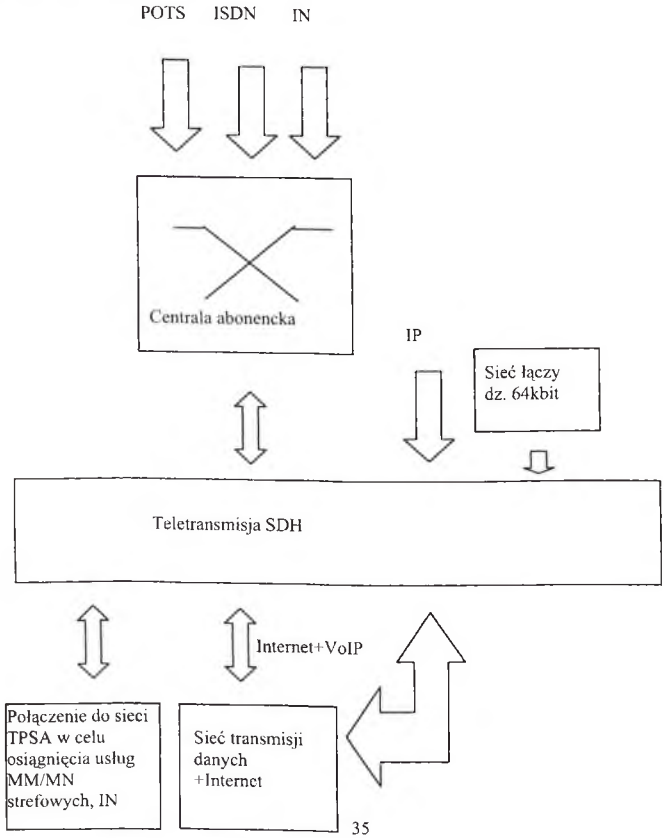
Andrzej Czerczak

Netia Telekom S.A., 02-822 Warszawa, ul. Poleczki 13
e-mail: Andrzej_Czerczak@netia.pl

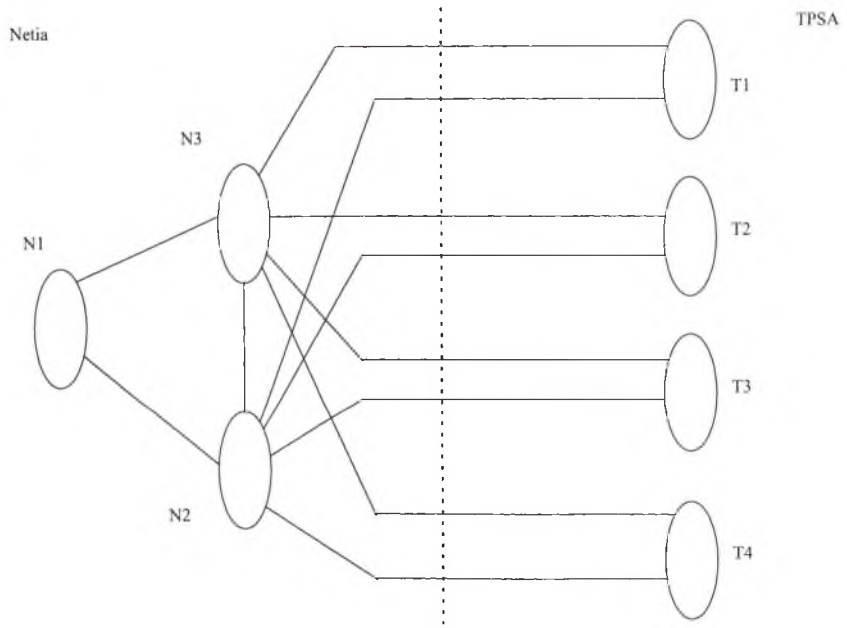
1. Wstęp.

Spółki operatorskie Netii Telekom posiadają koncesje Ministra Łączności na budowę sieci i świadczenie usług telekomunikacyjnych w obrębie strefy numeracyjnej, bez prawa skrośnego przesyłania ruchu do spółek siostrzanych. Fakt ten powoduje, że spółki w większości przypadków są w zasadzie „access providerem" dla podmiotów posiadających koncesje ogólnopolskie różnego rodzaju, czy to na świadczenie usług międzymiastowych przesyłu głosu, czy też danych.
Z drugiej strony, Polska jest jednym z nielicznych krajów, w których jest konkurencja w sieciach lokalnych i wydaje się, że posiadanie własnej infrastruktury będzie miało coraz większe znaczenie z punktu widzenia dochodów operatora.

2. Model usługowy sieci spółek Netii Telekom.



Wykorzystywane są także takie zalety jak możliwość scentralizowanego zarządzania i utrzymania elementów SDH: w każdym Regionie Netii istnieje centrum nadzoru nad elementami sieci, w szczególności SDH.
Kierowanie ruchu w sieciach Netii musi uwzględnić wymagania partnera, jak jest Telekomunikacja Polska S.A.: ponieważ we wszystkich obszarach Netii liczba abonentów TPSA jest większa niż liczba abonentów Netii, więc większość ruchu generowanego przez abonentów Netii jest ruchem wychodzącym do sieci Telekomunikacji Polskiej, przez uzgodnione punkty styku. Często architektura połączenia obu sieci jest dużo bardziej skomplikowana niż architektura wewnętrzna sieci Netii. Powoduje to problemy utrzymaniowe i w przypadku dużej liczby współpracujących węzłów komutacyjnych z obu stron, brak systematycznego podejścia do rozwiązania tego problemu mógłby spowodować, że strony nie byłyby w stanie zapanować na ruchem międzysieciowym, który jest rejestrowany dla celów statystycznych lub rozliczeniowych. Zastosowana została więc metoda maksymalnego rozdzielenia obu sieci, tzn. tylko ograniczona liczba central z obu stron widzi sieć drugiej strony. Zasada jest przedstawiona na rysunku niżej:



Ruch z centrali N1 jest kierowany do central „T" przez punkty styku central N1 i N2. Centrala N1 pracuje na łączach do central N2i N3 z tzw. podziałem ruchu 50%:50%.

uczą się dziedzin, które do tej pory były specjalnością klientów i podejmują z nimi realizację wspólnych projektów.

Drugim wyznacznikiem ewolucji są wewnętrzne zmiany organizacyjne operatorów, których celem jest tworzenie struktur zorientowanych na rynek i ich zróżnicowanie w zależności od segmentu rynku. Coraz ściślejsze związki z klientami umożliwiają gromadzenie szczegółowych informacji na temat ich potrzeb. Poszerzającej się ofercie i zróżnicowaniu organizacji pod kątem segmentów towarzyszy potrzeba coraz ściślejszej koordynacji i doskonalenia działań wewnątrz przedsiębiorstwa telekomunikacyjnego. Tempo, z jakim nowe technologie wprowadzane są na rynek wywiera ogromny wpływ na proces rozwoju usług. Zwiększa się presja na skracanie czasu wprowadzania usług na rynek, co jest oczywistym efektem globalizacji i deregulacji rynków telekomunikacyjnych. W przeszłości cykl rozwoju usługi trwał nawet kilka lat. Dziś czas ten trzeba mierzyć w miesiącach. Na przykład cykl opracowania i komercjalizacji usługi Frame Relay przez LDDS Worldcom trwał 9 miesięcy (marzec 1991).

Trzecim aspektem przemian są dokonywane przez operatorów inwestycje, dzięki którym mogą oni aspirować do strategicznej roli integratorów w stosunku do dużych klientów.

3. Warstwy oferty usługowej

Lakonicznie mówiąc można stwierdzić, że firmy telekomunikacyjne oferują dostęp do sieci telekomunikacyjnej. Występują tym samym w roli "integratora systemu" - łączą zasoby telekomunikacyjne funkcjonujące w różnych miejscach w spójną sieć wymiany danych. Integracja systemu przez dzisiejszego operatora telekomunikacyjnego jest widoczna na powierzchni - włączając wtyczkę telefonu do gniazdka uzyskiwany jest dostęp do usługi telefonicznej, podobnie jest w przypadku odbiornika telewizyjnego i sieci kablowej, czy tez modemu. Tradycyjny, pierwszy poziom integracji, widziany z perspektywy operatora, polega głównie na opisanym powyżej fizycznym podłączeniu do sieci takich urządzeń końcowych jak telefon tradycyjny lub komórkowy, komputer, fax, dostęp do Internetu lub połączenie przez modem.

Wyższym poziomem integracji jest integracja rozproszona. Niektóre typy połączeń wymagają zwiększonej szerokości pasma i większego zakresu opcji przenoszenia. Na tym poziomie integracji dostawcy usług muszą dysponować ofertą zróżnicowaną pod kątem szerokości pasma i stosowanego systemu billingu dla takich usług jak aplikacje dla grup roboczych, pasmo na życzenie, łączność z wykorzystaniem protokołu IP.

Najwyższy poziom integracji - integracja zastosowań - wymaga stworzenia różnych opcji oprogramowań i nośników, które dostosowane będą zarówno do potrzeb segmentu rynku jak również do zróżnicowanych potrzeb indywidualnych klientów. Na tym poziomie niezbędne stają się kompetencje, którymi dysponują różni aktorzy rynkowi - zarówno dostawcy usług telekomunikacyjnych jak i firmy softwarowe. Odpowiednikiem dzisiejszego sygnału telefonicznego stanie się usługa obejmująca połączenia i narzędzia potrzebne klientowi oraz zarządzanie danymi.

4. Nowy polski operator - TEL–ENERGO S.A.

Dynamiczny wzrost zapotrzebowania na nowoczesne usługi pociągnął za sobą pojawienie się w latach 90-tych nowych operatorów także na polskim rynku telekomunikacyjnym. Podobnie jak w innych krajach Europy, przedsiębiorstwa infrastrukturalne (energetyka, kolej, wodociągi, gazownictwo) stanowią dziś potencjalną konkurencję dla operatora narodowego, szczególnie w zakresie usług nie objętych monopolem. Obok rozbudowanej światłowodowej sieci TP S.A. powstały w ubiegłych kilku latach jeszcze dwie światłowodowe struktury telekomunikacyjne o zasięgu ogólnokrajowym – Energetyki i Kolei. Krajowa Sieć Telekomunikacyjna Energetyki

świadczyć usługi telekomunikacyjne, w tym wewnątrzstrefowe i międzystrefowe w ogólnokrajowej, wydzielonej sieci telekomunikacyjnej ograniczonemu zbiorowi użytkowników: Akcjonariuszom Spółki TEL–ENERGO oraz innym podmiotom związanym z wytwarzaniem lub dystrybucją energii elektrycznej i cieplnej;

dzierżawić łącza operatorom sieci telekomunikacyjnych oraz podmiotom gospodarczym wykorzystującym łącza i trakty telekomunikacyjne na własne potrzeby;

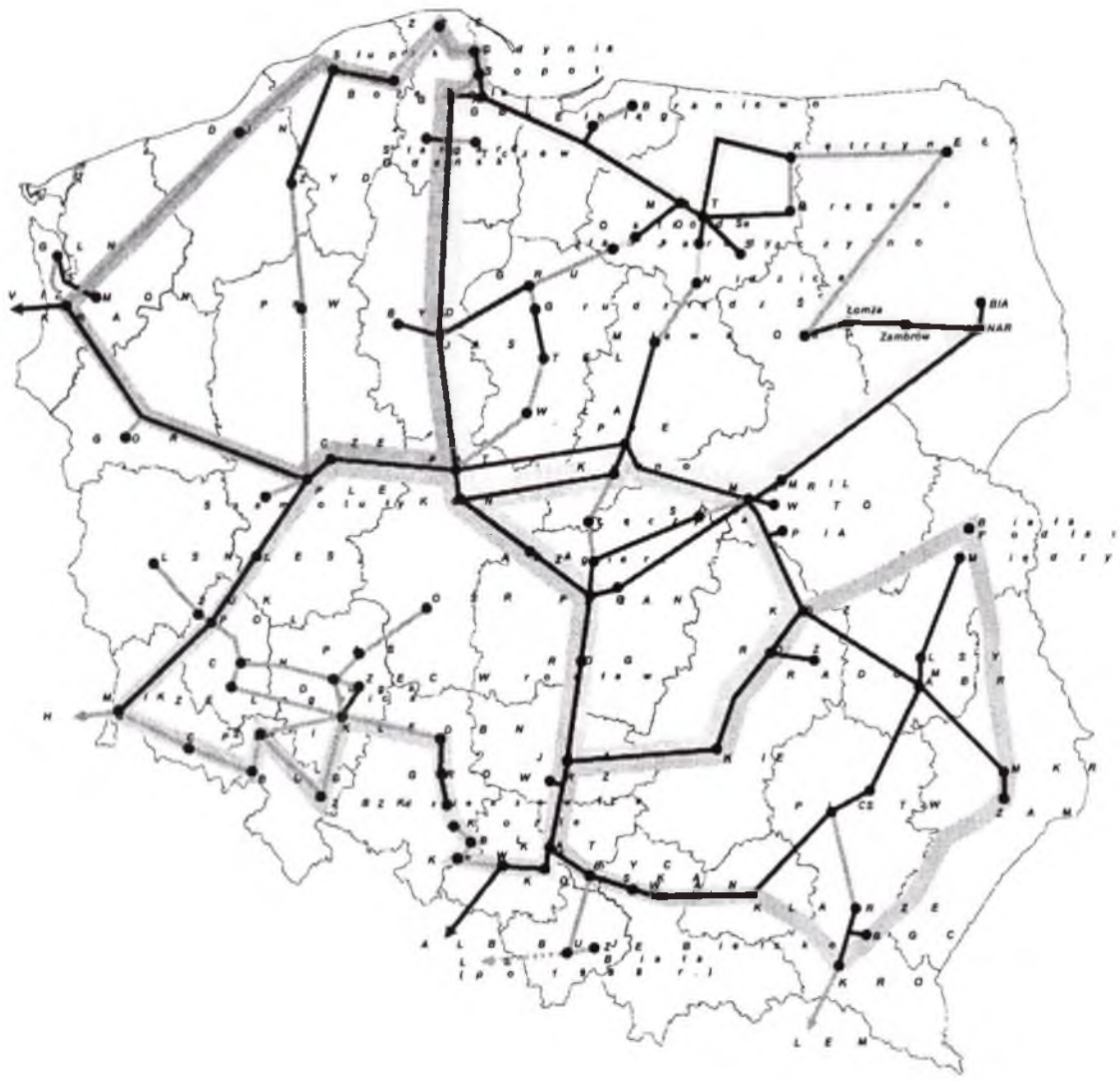
- Zatrudniona kadra;
- Szybko rosnąca baza klientów i związany z tym wzrost wartości sprzedanych usług dzierżawy łączy.

Próbkę możliwości technicznych sieci i kadry TEL–ENERGO można było zobaczyć na Targach INFOSYSTEM 98 w Poznaniu. Łącza TEL–ENERGO (155 Mb/s) zostały wykorzystane do stworzenia w ramach towarzyszącej targom konferencji Polman, sieci **POL-155** - rozproszonej sieci superszybkich komputerów, dzięki której naukowcy mogli prowadzić wspólne prace w kilku rozrzuconych po Polsce ośrodkach.

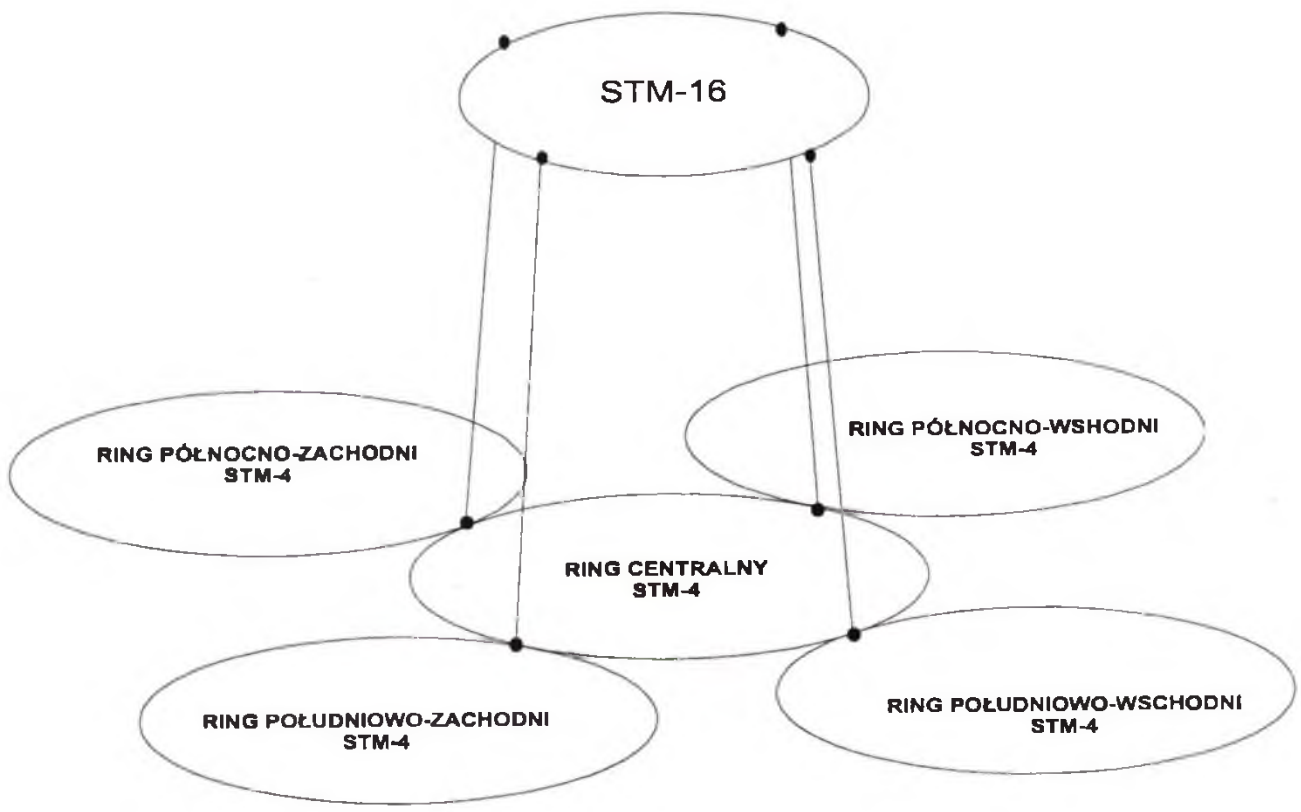
W jednym z pokazów trzy komputery w różnych miastach tworzyły razem film animowany - każdy z nich na podstawie danych tworzył inną klatkę filmu.

W innym eksperymencie stojąca w Poznaniu stacja robocza Silicon Graphics prowadziła skomplikowane obliczenia procesów chemicznych. Współpracujący z nią komputer Onyx2 zainstalowany w Gdańsku przedstawiał wynik tych obliczeń w postaci graficznej, pokazując obraz struktury cząsteczki chemicznej.

Wyniki tych wspólnych działań można było obserwować na zainstalowanych w Poznaniu monitorach.



Rys. 2. Bazowa Sieć Telekomunikacyjna na koniec 1998 r.



Rys. 3. Sieć SDH

Współpraca sieci MAN z innymi operatorami telekomunikacyjnymi na przykładzie MAN Kraków

Marian Noga

Akademickie Centrum Komputerowe CYFRONET – Kraków
e-mail: yymnoga@cyfronet.krakow.pl

MAN Kraków – sieć akademicka

a) historia sieci
b) hierarchia sieci (WAN, MAN, LANy)
c) uzależnienie od sieci rozległych
d) zadania MAN Kraków
(świadczenie usług sieciowych, eksploatacja sieci, rozbudowa sieci...)
e) usługi świadczone w sieci MAN Kraków
f) użytkownicy sieci

Historia i rozwój sieci MAN Kraków przebiegała w sposób analogiczny do innych sieci akademickich w dużych ośrodkach w Polsce. Równolegle z budową sieci lokalnych w jednostkach akademickich w Krakowie jest budowana i rozbudowywana infrastruktura telekomunikacyjna sieci MAN. W chwili obecnej infrastruktura obejmuje kilkadziesiąt kilometrów tras światłowodowych wraz z odpowiednimi urządzeniami aktywnymi w sieci. W MAN Kraków stosowane są równocześnie: starsza technologia FDDI z równoczesnym przechodzeniem do nowszej technologii – ATM.

W sposób naturalny w sieci MAN Kraków w zakresie możliwości świadczenia oczekiwanych przez użytkowników usług widać uzależnienie od sieci zewnętrznych. W początkowym okresie, jedynym bezpośrednim dostarczycielem usługi łączności zewnętrznej (krajowej i zagranicznej) była sieć rozległa NASK. Obecnie dzięki zwiększonej podaży usług innych operatorów telekomunikacyjnych, MAN Kraków może wykorzystywać usługi innych operatorów zewnętrznych w celu zwiększenia gamy świadczonych usług telekomunikacyjnych, jak też, co wydaje się **najważniejszym** podniesienie bezpieczeństwa i szeroko rozumianej niezawodności sieci MAN.

MAN Kraków jako jednostka wiodąca w zakresie **budowy i eksploatacji** sieci komputerowej musi równocześnie realizować kilka odrębnych zadań. Po pierwsze to bieżąca eksploatacja sieci MAN. Są to działania rutynowe, polegające na utrzymaniu w sprawności operacyjnej sieci oraz zapewnienie podstawowych usług telekomunikacyjnych dla wszystkich użytkowników. Następnym zadaniem jest realizacja wielorakich usług sieciowych dla całego środowiska krakowskiego (poczta elektroniczna, systemy informacyjne (www, usnet i inne), dostęp do sieci dla użytkowników poprzez łącza dzierżawione oraz łącza komutowane, zapewnienia bezpieczeństwa sieci i inne).

Kolejnym, niezmiernie istotnym zadaniem jakie musi wypełniać operator MAN Kraków jest dalsza rozbudowa infrastruktury sieciowej. Konieczność objęcia zakresem działania sieci wszystkich użytkowników ze sfery akademickiej w regionie nakłada na ACK CYFRONET obowiązek prowadzenia na stosunkową dużą skalę działań inwestycyjnych związanych z budową/rozbudową sieci komputerowej zarówno w obszarze Krakowa jak też w innych miejscowościach (Tarnów, Zakopane, Nowy Targ...)

c) możliwość sterowania wielkością ruchu wchodzącego i wychodzącego przez poszczególne łącza,
d) możliwości stosowania własnej polityki routingu.

W chwili obecnej są prowadzone prace inwestycyjne, które w efekcie doprowadzą do technicznej możliwości spięcia struktury sieci MAN Kraków z infrastrukturą Zakładów Energetycznych, a po doprowadzeniu sieci Telenergo do Krakowa dadzą w efekcie potencjalną możliwość połączenia sieci MAN Kraków z eksploatowaną w kraju siecią POL34.

Uwarunkowania organizacyjno prawne

a) model funkcjonowania i finansowani sieci komputerowej,
b) użytkownicy akademiccy
c) inni użytkownicy
d) prawo telekomunikacyjne

Zasadnicze poglądy na sieć komputerową w środowisku akademickim nie uległy w ostatnim okresie zmianom. Obserwuje się stały wzrost zainteresowania usługami w sieci oraz duże zainteresowanie zwiększaniem przepustowości sieci (w szczególności rozległej). Wiąże się to z coraz bardziej atrakcyjnymi usługami sieciowymi (usługi informacyjne WWW, duża ilość bibliotek i zasobów bibliotecznych, zwiększająca się atrakcyjność i dostępność baz danych itp.).

W modelowym działaniu sieci komputerowej, klasycznie wyróżnia się siedem warstw [2] funkcjonalnych sieci. W przypadku operatora (dostarczyciela usług sieciowych) istotne są cztery warstwy: pierwsza – łącza fizyczne (łącza galwaniczne, radiowe, światłowodowe i inne), druga i trzecia – łącza logiczne; tworzą ją zespoły specjalizowanych urządzeń sieciowych które są odpowiedzialne za odbieranie i wysyłanie informacji (pakietów danych) wraz z kontrolą poprawności. Warstwy pierwsza, druga i trzecia nie są związane z żadnym konkretnym użytkownikiem i jako takie muszą być zarządzane przez ogólnego operatora. Warstwa czwarta z formalnego modelu opisu sieci związana jest z usługami dla użytkowników.

Finansowanie akademickich sieci miejskich w ostatnich latach uległo zmianie. Decyzją Komitetu Badań Naukowych środki finansowe przeznaczone na utrzymanie sieci rozległej oraz utrzymanie sieci MANów zostały przekazane do poszczególnych MANów (a nie do NASK jak w latach ubiegłych). Mechanizm ten umożliwił poszukiwanie przez MANy dodatkowych lub alternatywnych rozwiązań w zakresie dostępu do sieci rozległej.

Poszukiwanie alternatywnych rozwiązań w zakresie sieci rozległych, zwłaszcza przy szczupłości środków finansowych przeznaczonych na eksploatację infrastruktury informatycznej dla nauki należy realizować z daleko idącą rozwagą i ostrożność. Sieć rozległa nie może funkcjonować w oderwaniu od innych już funkcjonujących sieci. Nierozważne działania, mogą doprowadzić do daleko idącej dezorganizacji sieci krajowej i w sumie pogorszenia jakości usług świadczonych dla całego środowiska. Nienajlepszym przykładem jest dosyć słaba współpraca operatorów (w sensie telekomunikacyjnym) sieci POL34 (opartej na łączach Telenergo) z istniejącą od kilku lat siecią NASK. Nie udało się w ciągu roku doprowadzić do harmonijnej współpracy tych sieci a zwłaszcza do konstruktywnych uzgodnień w zakresie obsługi ruchu międzynarodowego.

Akademickie sieci komputerowe, zwłaszcza większe MANy obsługujące dużą ilość użytkowników i świadczące szeroką gamę usług dla różnych abonentów muszą rozszerzyć swoją

[2] Model OSI ISO opisujący siedem współpracujących warstw, z których niższe świadczą usługi komunikacyjne dla warstw wyższych.

USŁUGI TELEKOMUNIKACYJNE DLA HANDLU

Wiesław Szypuła

Bankowe Przedsiębiorstwo Telekomunikacyjne „TELBANK" SA,
ul. Poligonowa 3, 04-051 Warszawa
e-mail: wieslaw.szypula@telbank.pl

Powszechność usług telekomunikacyjnych, rozwój technik wymiany informacji oraz rozwój systemów informatycznych doprowadził do realizacji transakcji handlowych drogą elektroniczną. Powstało pojęcie „rynek elektroniczny" (Electronic Commerce), które można zdefiniować jako system realizacji transakcji handlowych bez papieru, za pomocą Poczty Elektronicznej (E-mail), aplikacji Elektronicznej Wymiany Dokumentów (EDI Electronic Data Interchange), elektronicznego transferu pieniędzy (EFT – Electronic Found Transfer) i innych podobnych.

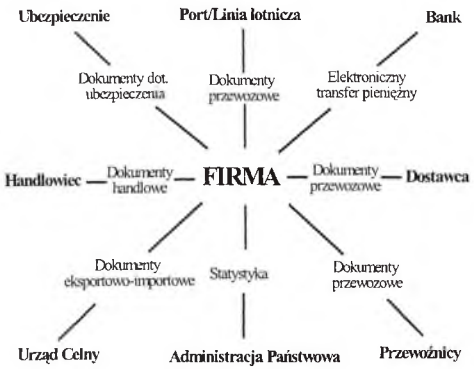
Istotne znaczenie dla rozwoju rynku elektronicznego ma dynamiczny przyrost użytkowników sieci INTERNET. Coraz więcej sklepów dopuszcza realizację zakupów poprzez tą sieć. Banki zaczynają wprowadzać na rynek nowe usługi polegające na umożliwieniu klientom dokonywania podstawowych operacji finansowych na kontach poprzez INTERNET (internet banking).

Dzięki nowym technologiom przesyłania informacji pojawiają się na rynku nowe usługi jak np. multimedialny przekaz na żądanie klienta (filmy video, gry komputerowe), usługi Call Center.

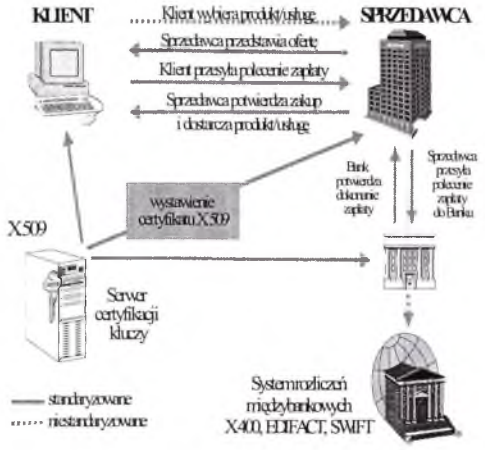
Techniki telekomunikacyjne dla elektronicznej wymiany dokumentów handlowych

Elektroniczny system wymiany dokumentów (EDI) jest już stosowany na świecie od przeszło 20 lat. Początkowo był on rozwijany w branży transportowej przez przewoźników morskich, kolejowych i powietrznych w wymianie dokumentów handlowych z magazynami, agencjami celnymi i bankami. Pierwszy zestaw standardów przemysłowych EDI został opracowany przez Komitet d/s Koordynacji Informacji Transportowych (TDCC). W oparciu o ten standard zostały opracowane standardy ANSII X.12 a następnie EDIFACT, który przyjęły państwa UE do prowadzenia korespondencji handlowej a także międzybankowej (SWIFT).

Rys. 1 Zakres stosowania standardów EDIFACT.



Pojawiły się już pierwsze aplikacje wykorzystujące ten standard w systemach sprzedaży poprzez INTERNET.



Rys. 3 Schemat realizacji transakcji wg standardu SET

Ze względu na konieczność zapewnienia wysokiego stopnia ochrony dokumentów elektronicznych w istniejących systemach EDI (np.: TRADACOMS, ODETTE, SWIFT, ELIXIR) eksploatowanych przez duże korporacje przemysłowe, transportowe, banki i administracje państwowe w wielu krajach, nie przewiduje się w najbliższym czasie wykorzystanie sieci INTERNET w tych systemach.

Rozwój usług realizowanych na bazie sieci INTERNET wymusza na operatorach sieci telekomunikacyjnych działania na rzecz:

- wzrostu przepustowości międzywęzłowych łączy telekomunikacyjnych z zastosowaniem najnowocześniejszych technik np. SDH, ATM,
- rozwoju sieci i usług dostępowych,
- rozszerzenia zakresu usług z tzw. wartością dodaną:
  - ⇒ serwisy informacyjne,
  - ⇒ zestawianie połączeń w oparciu o różne technologie sieci telekomunikacyjnych (VSAT, sieci naziemne, GSM),
  - ⇒ konwersja protokółów np.: EDIFACT, ANSI X.12, TRADACOM, ODETTE.

Call Center – Computer Telephony Integrator (CTI)

Jest to usługa umożliwiająca efektywniejsze prowadzenie transakcji handlowych i usługowych.

Z różnorodnych funkcji telefonii komputerowej z coraz większą popularnością wśród agencji handlowych i firm o dużym ruchu telekomunikacyjnym cieszą się najprostsze – funkcja

Wykaz najczęściej stosowanych technik telekomunikacyjnych w EC

Poniżej zestawiono najczęściej stosowane techniki telekomunikacyjne dla obsługi niektórych aplikacji związanych z elektronicznym rynkiem.

Rodzaj aplikacji	Rodzaj wykorzystywanego systemu telekomunikacyjnego
elektroniczna wymiana dokumentów handlowych EDI	X.400/X.500 pakietowe sieci transmisji danych, sieci telefoniczne oraz ISDN
bankomaty	pakietowe sieci transmisji danych (sieci naziemne i satelitarne), dzierżawione łącza i kanały cyfrowe o mniejszych szybkościach radiowe sieci do obsługi ruchu transakcyjnego
EFTPOS (czytniki kart płatniczych),	sieci telefoniczne, radiowe sieci do obsługi ruchu transakcyjnego, pakietowe sieci transmisji danych
samoobsługowe punkty sprzedaży	radiowe sieci do obsługi ruchu transakcyjnego, dzierżawione łącza i kanały cyfrowe
home banking dla klientów korporacyjnych	sieć telefoniczna, pakietowe sieci transmisji danych (zalecane)
home banking i elektroniczna sprzedaż dla klienta detalicznego	publiczna sieć telefoniczna, INTERNET, INTRANET
system rozliczeń wewnątrz i międzybankowych	EDIFACT, SWIFT, X.400/X.500 pakietowe sieci transmisji danych, ISDN, Frame Relay, ATM
usługi multimedialne	SDH, ATM, ISDN sieci światłowodowe i satelitarne

USŁUGI TELEKOMUNIKACYJNE ŚWIADCZONE PRZEZ BPT TELBANK S.A. 1998r

Dzierżawa kanałów cyfrowych o dużych przepustowościach

- cyfrowe kanały bitowo przezroczyste
- Frame Relay

Kanały cyfrowe o dużych szybkościach (powyżej 64 kb/s) zestawiane są w sieci podstawowej TELBANK-M.

- dostępne przepustowości kanałów cyfrowych: do 2 Mbit/s,
- protokoły transmisyjne:
  ⇒ kanały bitowo przezroczyste,

specjalne zamówienie.

Sieć satelitarna TELBANK-VSAT

W przypadku braku łączy naziemnych, a także ze względu na konieczność zapewnienia wysokiej niezawodności połączeń w systemie teleinformatycznym, BPT proponuje utworzenie połączeń w oparciu o sieć satelitarną TELBANK-VSAT.

Sieć TELBANK-VSAT jest w pełni zintegrowana z naziemną siecią pakietową TELBANK-P. Obie sieci są objęte wspólnym planem numeracji. Każdy abonent sieci TELBANK-VSAT może uzyskać połączenie z dowolnym abonentem sieci TELBANK-P i odwrotnie.

- dwa systemy zarządzania terminalami satelitarnymi (tzw. systemy HUB),
- obecnie w sieci pracuje ponad 1000 terminali VSAT,
- protokoły na portach: X.25, X.28, TC/IP (ETHERNET),
- prędkości nominalne na portach: do 64 kb/s,

Do końca bieżącego roku przewidywane jest uruchomienie szerokopasmowego systemu satelitarnego umożliwiającego zestawienie kanałów cyfrowych o przepustowości powyżej 64 kb/s.

Sieć z integracją usług ISDN

Kolejną usługą oferowaną przez BPT, dedykowaną dla banków i jednostek administracji państwowej, jest transmisja danych, głosu, obrazu wg protokołów stosowanych w ISDN. BPT proponuje utworzenie, w oparciu o sieć rozległą TEBANK-T, sieci korporacyjnej zgodnie z normami Euro-ISDN. Tak utworzona sieć korporacyjna jest chroniona przed dostępem abonentów sieci publicznej. Natomiast abonenci sieci korporacyjnej mają możliwość nawiązywania połączeń z abonentami sieci publicznej.

- obecna ilość węzłów w sieci TELBANK-T – 24,
- dostępne styki: 2B+D, 30B+D (QSIC),

System MOBITEX,
obsługa bankomatów, EFTPOSów, systemy alarmowania,
systemy śledzenia pojazdów.

W Warszawie, Zielonej Górze i Wrocławiu została uruchomiona, przez BPT, radiowa, komórkowa sieć transmisji danych dedykowana dla aplikacji generujących ruch o charakterze transakcyjnym np. dla:

- systemów obsługi EFTPOSów, bankomatów,
- systemów ochrony obiektów,
- realizowania transmisji pomiędzy obiektami ruchomymi,

BPT oferuje:

- sprzedaż oraz instalację oprogramowania: X.400, X.500, oprogramowanie narzędziowe dla systemów pracujących w standardzie EDIFACT.
- kompletne dołączanie węzłów pocztowych banków i instytucji do węzła pocztowego TELBANK400®,
- skrzynki pocztowe w węźle pocztowym TELBANK400®,
- transmisję wiadomości do abonentów krajowych i zagranicznych w standardzie X.400, lub poprzez INTERNET w standardzie SMTP/MIME.

Formy zamawiania zamówień

Usługui realizowane są na podstawie „Regulaminu i cennika usług telekomunikacyjnych świadczonych przez BPT TELBANK S.A.". Zamówienia składane są na formularzach BPT TELBANK S.A., ale możliwa jest również realizacja usług telekomunikacyjnych na podstawie odrębnych umów. Ta druga forma realizacji zamówień jest najczęściej stosowana gdy dotyczy wykonania dużych lub niestandardowych projektów telekomunikacyjnych.

Szczegółowe informacje można uzyskać:

- na stronie **Błąd! Nie zdefiniowano zakładki.**
- w zespole obsługi klienta tel. (22) 695-39-93
- w zespole marketingowym tel. (22) 695-39-16

Adres do korespondencji

Bankowe Przedsiębiorstwo Telekomunikacyjne „TELBANK" S.A.
ul. Poligonowa 3
04-052 Warszawa

email: marketing@telbank.pl

Powołanie zespołu kryzysowego na czas związany z:

- katastrofą;
- pożarem;
- włamaniem;
- klęską żywiołową

Zespół kryzysowy

- dysponuje pełną dokumentacją na określone sytuacje;
- zdefiniowany jest stan wyjątkowy i normalny sieci;
- zapewnia bezpieczeństwo sieci;
- autoryzacja selektywnego dostępu do fizycznych elementów sieci;
- protekcja przesyłanych danych
- alternatywne kierowanie ruchem;
- monitorowanie istotnych parametrów i zdarzeń występujących w sieci;
- redundancja krytycznych modułów i zbiorów systemowych(biling);
- elastyczne zarządzanie siecią w celu wyeliminowania przerw w połączeniach priorytetowych.

Absent Subscriber (Interception): The Absent Subscriber service allows providing special announcement (generated by the switch) if subscriber will be absent.

Call Forwarding if busy: The network will redirect, to another user, calls which are addressed to the served user and which meet busy.

Call Forwarding on No Reply: The network will redirect, to another user, calls which are addressed to the served user and which no reply.

Call Forwarding Unconditional: The network will redirect, to another user, calls which are addressed to the served user. The served user's ability to originate calls is unaffected.

Call Hold: This service allows users to put active call on hold. It can be used with 3PTY service as well.

Call Waiting: This supp. service allows a served user to be informed by the network of an incoming call even if he/she is busy. Served user can reject, accept or ignore the waiting call using the Call Hold service.

Changed Number (Interception): This service enables to switch incoming calls to a special announcement with information about new subscriber telephone number, etc.

Home Meter: The Home Meter supp. service provides the served analogue user with charging pulses information based on the number of units consumed. These informations are sent to the user's home meter during the call.

Hot Line Delayed: The Hot Line supp. service allows to the user to call to a predefined party without having to send destination address information to the network. The served user goes off-hook (and doesn't do anything else). The network fetches the fixed destination number linked to this access, waits a limited period of time before invoking the service and than establishes a call to the proper destination.

Hot Line Immediate: The Hot Line supp. service allows to the user to call to a predefined party without having to send destination address information to the network. The served user goes off-hook (and doesn't do anything else). The network fetches the fixed destination number linked to this access and immediately establishes a call to the proper destination.

Outgoing Calls Barring (total): The Outgoing Call Barring service enables the served user to prevent all/certain categories of outgoing calls from being made from his access.

Outgoing Calls Barring (code): The Outgoing Call Barring service enables the served user to prevent all/certain categories of outgoing calls from being made from his access. User can decide to activate or deactivate this facility.

Regular Alarm Call (Wake-up call regular): The Alarm Call allows the served user to order alarm calls to be made to his access at times specified in advance by himself regularly in many times.

Single Alarm Call (Wake-up call single): The Alarm Call allows the served user to order alarm calls to be made to his access at times specified in advance by himself once only.

this number is called there is the Voice Mail system that answer the phone and welcomes to leave a message. The virtual Voice Mail box owner can check his her messages using any telephone set or public phone available all over the network. The virtual Voice Mail box owner can also be automatically informed by the system about a new message. It can be performed, i.e. by paging.

Centrex: Customer does not need to buy any PABX or Key system, because he can use some of PABX facilities directly from public exchange. In Centrex group can be attendant, abbreviated numbers and public value added services like call waiting, call forwarding (on busy, on no reply, unconditional), three party conference, outgoing call barring, changed numbers. Most of features are available both for analog lines and for ISDN lines. In addition to conventional services on analog lines, user is also provided with all public ISDN services. In addition, Centrex group users have also access to services available within the group. There are services like operator access priority queue, call picks up, call picks up group, incoming general call forwarding on no reply, call transfer (when the connection has been already established).

Datacom services: Transferring of data from one point to another, X.25, Frame Relay. Netia has no license to provide these services today. Through partner who have a license this will become possible.

Internet (dial up or fixed connection): Customer must have telephone (analogue or ISDN), computer and modem. Connection with Internet server is established via modem through telephone line by choosing telephone number. When somebody makes calls for this number switch connects him to Internet server. Internet server has also modems and he takes care about data transmission from customer to any Internet server. By using fixed connection the customer also has possibility to use Internet without dialing for Internet number, without waiting for connecting and avoid possibility that network can be occupy. Netia has no license to provide these services today. Through partner who have a license this will become possible.

PABX offering incl. financial solutions: Through cooperation agreement with supplier of PABX equipment Netia will be able to provide business customers a PABX solution together with a financial solution (leasing).

Future services

What Netia will be offering to our customers in the future remains to be seen. Off course Netia will follow the market demand and in next year or maybe in a couple of years we will see Netia offering services like 700/800/900 numbers, Conference call, Video conference, Real time billing, Voice over IP and IN services.

Service Implementation

When there is a decision in Netia about a new service to be developed, to be packaged and commercial introduced, first thing that is done is to put one person responsible for this, a Project leader (PL) for this service. This PL is responsible for everything that is needed to be able to commercial introduces the service on the market. This includes tariff, promotion staff, choice of

ISDN - DOŚWIADCZENIA WE WPROWADZANIU USŁUGI

Ireneusz Klimczak

Netia Telekom S.A., 02-822 Warszawa, ul. Poleczki 13
e-mail: Ireneusz_Klimczak@netia.pl

W związku z koniecznością poszerzenia zakresu usług sprzedawanych w sieciach Netii, podjęto decyzję o wprowadzeniu ISDN. „Właścicielem" projektu został Dział Marketingu HQ Netia Telekom S. A. W obrębie działu nowymi usługami zajmuje się Grupa Produktowa. Za opracowanie strategii wprowadzania ISDN odpowiedzialna jest jedna osoba tzw. Lider Projektu. W zakres obowiązków Lidera Projektu ISDN weszły następujące problemy:

- pomysł na realizację zadania
- szacowanie potencjalnego rynku
- szacowanie przychodów
- szacowanie kosztów wprowadzenia ISDN
- koordynacja działań technicznych z marketingowymi
- przygotowanie Business Planu
- przygotowanie podręcznika ISDN dla pracowników Netii
- przygotowanie regulaminu i cennika
- koordynacja szkoleń
- koordynacja działań promocyjnych

1. Projekt Pilotowy ISDN w sieci Netia Telekom S.A.

W odpowiedzi na zapotrzebowanie klientów Netia Telekom S.A. postanowiła przeprowadzić Projekt Pilotowy ISDN. W okresie pilotowym Klientom Netii oferowany był jedynie dostęp podstawowy ISDN - BRA.

Zasady Projektu Pilotowego:

Klienci, którzy zgłosili chęć wzięcia udziału w Projekcie Pilotowym otrzymali, po wcześniejszych konsultacjach odpowiednie urządzenia końcowe ISDN (telefony cyfrowe, karty ISDN do PC, bridge/routery). Urządzenia określone we wcześniejszych ustaleniach, Netia Telekom S.A. oddawała Klientom na czas trwania projektu nieodpłatnie. Klienci nie wnosili opłaty abonamentowej, lecz pokrywali koszt związany z generowanym ruchem.

Projekt Pilotowy umożliwił przetestowanie możliwości central wykorzystywanych w sieciach Netii.

Uzyskano informacje od klientów o ich upodobaniach, potrzebach i możliwościach. Dane zawartych w ankietach wypełnianych przez klientów, posłużyły do stworzenia planu marketingowego umieszczonego w Business Planie.

W projekcie wzięło udział 15 klientów, którzy wykorzystali 25 dostępów BRA.

2. Testy przyłączeniowe sieci Netii do publicznej sieci ISDN TP S. A.

Za przeprowadzenie testów przyłączeniowych z operatorem narodowym i doprowadzenie do przenoszenia ruchu ISDN wychodzącego z sieci Netii do sieci publicznej, odpowiedzialny jest Departament Techniczny Netia Telekom S.A. oraz Departamenty Techniczne w regionach Netii.

Rozmowy dotyczące przeprowadzenia testów przyłączeniowych rozpoczęły się w 1997 roku. W lutym br. Uzgodniono listę osób z każdej ze stron, odpowiedzialnych za synchronizację i

2. Szkolenia.

W przygotowanie szkoleń ISDN zostało zaangażowanych kilkanaście osób z różnych działów Netii. Szkolenia są adresowane dla pracowników M&S wszystkich regionów, szczególnie dla specjalistów ISDN oraz Large Account Managers.

3. Promocja.

Za promocję jest odpowiedzialna Grupa promocyjna marketingu HQ. Ze względu na szereg istotnych informacji technicznych, które powinny się znajdować w broszurach i ulotkach oraz na internetowych stronach Netii. Nad przygotowaniem materiałów promocyjnych pracowały Grupy: produktowa oraz promocyjna.

Akcja promocyjna rozpocznie się przed rozpoczęciem sprzedaży komercyjnej ISDN w sieciach Netii.

Wszystkie wymienione wyżej działania, obrazujące najważniejsze problemy związane z wprowadzeniem nowej usługi a koordynowane przez Lidera Projektu ISDN powinny doprowadzić do jak najszybszego rozpoczęcia sprzedaży ISDN w obrębie sieci Netii.

Tym, co umożliwia integrację, jest rozwój technologii, natomiast to, co ten trend napędza, to oczywiście pieniądze – przekaz głosu w sieciach transmisji danych jest tańszy pozwalając wielu przedsiębiorstwom na redukcję kosztów.

Integracja głosu i danych jest tendencją powszechną. Stosuje się ją obecnie z powodzeniem w sieciach szkieletowych. Szybko zdobywa również popularność w warstwie dostępowej, a nawet komputerach osobistych poszczególnych użytkowników.

Bezpieczeństwo w technologii ATM

Andrzej Maciek Skrzeczkowski (NASK)
askrz@nask.pl

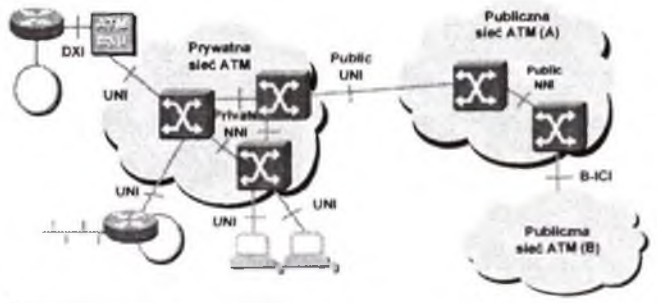
ATM - zintegrowane usługi

- Ekonomia integracji: dane, dźwięk i video
- zaszumienie przez wielość rodzajów danych

Podstawy ATM

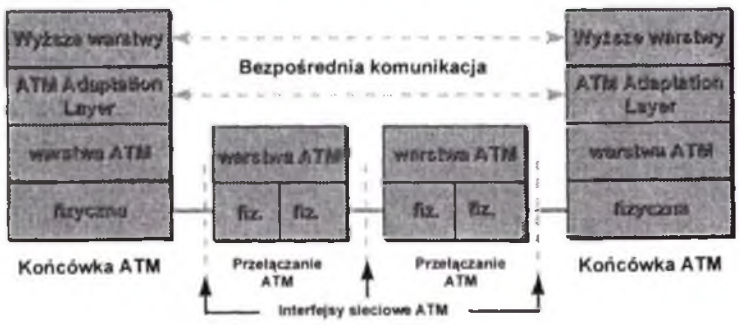
- Komórki o stałej, 53 - bajtowej, długości
- Ramki są dzielone, a następnie łączone na końcach połączenia
- Sprzętowe przełączanie komórek
- Komórki kierowane są w różnych kierunkach przez przełączniki ATM na podstawie zawartych w nich identyfikatorów
- Zorientowanie połączeniowo; połączenie od końca do końca nawiązywane przed rozpoczęciem transmisji
- Quality of Service (QoS) definiowane / negocjowane przy nawiązywaniu połączenia

interfejsy sieciwe ATM

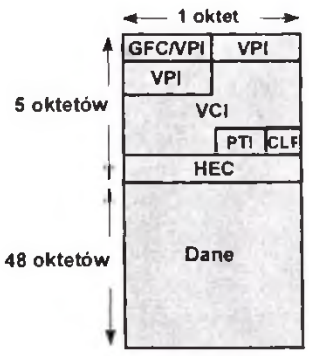


- User-Network Interface (UNI)
- Network-Node Interface (NNI)
- Broadband Inter-Carrier Interface (B-ICI)
- Data eXchange Interface (DXI)

ATM: architektura warstwowa

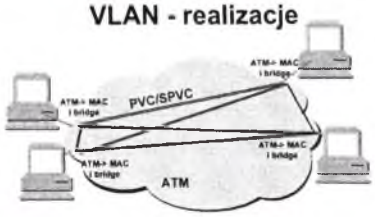


Format ramki ATM



- UNI
  - Generic Flow Control (GFC)
  - Virtual Path/Channel Identifier (VPI/VCI)
  - Payload Type Identifier (PTI)
    - Dane użytkownika lub ruchu utrzymaniowego
    - Wskaźnik przeciążenia
    - Koniec wiadomości (ramki AAL 5)
  - Cell Loss Priority (CLP)
  - Header Error Control (HEC)
- NNI
  - W miejscu GFC większe pole VPI

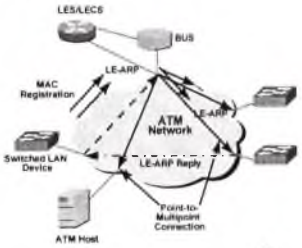
VLAN - realizacje



- najprostsza realizacja, dla niewielu punktów
- z punktu widzenia końcówek - jeden bridge
- enkapsulacja RFC 1483

Operacje LANE

- LAN Emulation Service (LES)
- LAN Emulation Configuration Server (LECS)
- Broadcast and Unknown Server (BUS)



Koncepcja ochrony łącz ATM

- Stan bezpieczeństwa
  - brak pełnej standaryzacji (+!)
  - dostępność standardów już opracowanych (-)
  - łączność światłowodowa (+?)
  - trudne szyfrowanie przy dużych prędkościach (-)
  - duże zaszumienie informacji (+)

Koncepcja ochrony łącz ATM

- Szyfrowanie na łączach
  - szyfrowanie całego strumienia informacji - drogie i wprowadzające opóźnienia
  - inteligentne szyfrowanie połączeń logicznych z wyminą kluczy przy ich zestawianiu

Koncepcja ochrony łącz ATM

- Szyfrowanie pomiędzy końcami połączenia
  - najbardziej skuteczne
  - przy łączeniu np. central poprzez bezpośredni interfejs ATM - problem miary szyfrowania szybkiego łącza

Koncepcja ochrony łącz ATM

- Problem synchronizacji
  - ATM nie widzi utraty komórki (uszkodzenia ramki) przy transporcie przez kolejne przełączniki
  - można stosować kody samosynchronizujące
  - można użyć informacji o końcu ramki AAL5 z nagłówka komórki
  - można użyć strumienia komórek OAM

BEZPIECZEŃSTWO W TECHNOLOGII FRAME RELAY

Maciej Szeptycki

NASK

Streszczenie

Wzrastająca liczba zastosowań technologii Frame Relay do budowy sieci rozległych karze zastanowić się nad bezpieczeństwem takiej sieci. Sama budowa protokołów związanych z Frame Relay oraz szybkość działania łącz jest powodem ogromnego zawikłania tego problemu.

Technologia Frame Relay

Frame Relay jest protokołem, który definiuje styk użytkownika z siecią na drugim poziomie modelu ISO OSI. Jego zadaniem jest stworzenie dla wyższych warstw przezroczystego, samorekonfigurującego się w wypadku awarii, jednak nie w pełni bezbłędnego medium transmisyjnego. Dane przenoszone są w ramkach o zmiennej długości. W nagłówku każdej ramki znajduje się adres DLCI, określający punkt docelowy dla przesyłanej informacji. Para adresów DLCI tworzy kanał logiczny (VC), który w sposób jednoznaczny określa drogę po której przesyłane są dane między dwoma portami użytkownika. Obecnie stosuje się tylko kanały permanentne PVC.

Frame Relay jest technologią, która może działać z szybkościami do 34Mb/s. Daje ona ogromną elastyczność w tworzeniu różnych topologii sieci. Na styku z użytkownikiem został zdefiniowany protokół LMI, raportujący dodanie, skasowanie i status poszczególnych PVC. Niektóre routery mają zaimplementowany protokół Inverse ARP pozwalający w sposób dynamiczny mapować adresy DLCI na odpowiadające im adresy warstwy trzeciej.

Zagrożenia w sieci Frame Relay.

Zagrożenia, związane ze stosowaniem technologii Frame Relay można podzielić na trzy zagadnienia. Pierwsze z nich dotyczy bezpieczeństwa przesyłanych informacji patrzą z punktu widzenia użytkownika. Chodzi tu o możliwość podsłuchania danych płynących w konkretnym kanale PVC, jak również o możliwość tworzenia nieautoryzowanych połączeń. Dostępne są już na rynku urządzenia umożliwiające szyfrowanie przesyłanych danych oraz ochronę typu firewall na styku użytkownika.

Drugie zagadnienie dotyczy popularnej, u zachodnich operatorów, usługi typu wirtualne sieci prywatne (VPN). Wiąże się to z podziałem przez operatora zasobów sieci na tzw. partycje i udostępnieniem użytkownikowi dostępu do zarządzania konkretną partycją. Tego typu rozwiązania wymagają od operatora bardzo ścisłej dyscypliny i uwagi w przydzielaniu uprawnień poszczególnym klientom.

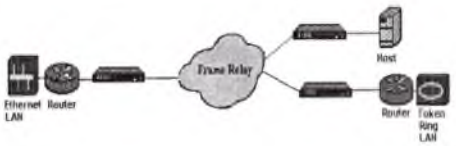
Trzecie zagadnienie dotyczy wreszcie zagrożeń związanych z dostępem do urządzeń sieci (przełączników) i systemu zarządzania siecią. Chodzi tu oczywiście o nieuprawniony dostęp osób trzecich, które mogły by podejmować próby dokonywania zmian w konfiguracji sieci. Całość zagadnień z tym związanych spoczywa na operatorze sieci Frame Relay.

Frame Relay: Zagrożenia

- połączenia wirtualne
- partycjonowanie sieci
- zarządzanie siecią (switch'ami) Frame Relay

Frame Relay: Ochrona kanałów wirtualnych

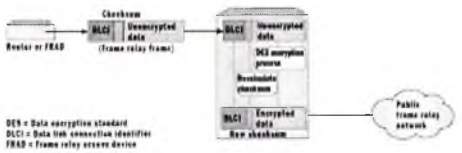
- szyfrowanie kanałów od końca do końca
- firewall: odrzucanie nieautoryzowanych połączeń



Frame Relay: Szyfrowanie danych

- oddzielenie nagłówka (adresu DLCI)
- separacja kanału LMI
- szyfrowanie danych
- ponowne naliczenie sumy kontrolnej (CRC)
- niezbędny jest dodatkowy czas na przetwarzanie

Frame Relay: Szyfrowanie danych



Frame Relay: Firewall

- definiowanie dopuszczalnych adresów DLCI
- odrzucanie uszkodzonych lub zmienionych ramek
- niezależny klucz dla każdego kanału wirtualnego

Frame Relay: Partycjonowanie

- operator zezwala klientowi na zarządzanie pewnymi zasobami sieci (VPN)
- klient używa protokołu SNMP do zbierania statystyk i rekofigurowania przydzielonych mu fragmentów sieci
- system partycji w sposób jednoznaczny oddziela uprawnienia klientów
- nadzór nad partycjami posiada wyłącznie operator sieci

OCHRONA ELEKTROMAGNETYCZNA WĘZŁÓW SIECI KOMPUTEROWYCH Z WYKORZYSTANIEM TECHNOLOGII ELASTYCZNYCH MATERIAŁÓW PRZEWODZĄCYCH

Andrzej Barczak

Zarząd Łączności i Informatyki MON, Warszawa
oraz NASK

Lesław Macherzyński, Tadeusz Szuszkiewicz, Piotr Wolski

Centrum Szkolenia Łączności i Informatyki, 05-131 Zegrze
E – mail: wsowl@atos.warman.com.pl
oraz NASK

Wstęp

W referacie rozważa się problematykę celowości oraz sposobów ochrony elektromagnetycznej węzłów sieci komputerowych. Przedstawiono możliwości wyboru istniejących technik ochrony, w tym nie znaną jeszcze powszechnie technologię elastycznych materiałów przewodzących. W oparciu o własne doświadczenia omówiono niektóre zagadnienia dotyczące projektowania i realizacji pomieszczeń ekranowanych elektromagnetycznie.

Węzeł sieci komputerowej jako zestaw złożonych urządzeń elektronicznych wytwarza promieniowanie elektromagnetyczne. Jest także wrażliwy na oddziaływanie promieniowania elektromagnetycznego zarówno pochodzenia zewnętrznego, jak i tego, które sam wytwarza. Sprzęt węzłów sieci komputerowych jest projektowany z uwzględnieniem określonych poziomów kompatybilności elektromagnetycznej (np. regulacje FCC I CE).

W wielu przypadkach nie stanowi to jednak w pełni zadowalającego rozwiązania problemów w odniesieniu do węzłów sieci komputerowych. Przykładowo typowe problemy mogą być następujące:

- Wzajemne oddziaływania poszczególnych składników sprzętu w zestawie są trudne do przewidzenia i prowadzą do przekroczenia zakładanych progów kompatybilności.
- Naprawy, rekonfiguracje i przemieszczenia sprzętu naruszają prawidłowy stan.
- Zmienia się niekorzystnie środowisko elektromagnetyczne węzła sieci komputerowej (np. telefony komórkowe, bliskie linie wysokiego napięcia, radiolokacja i radionawigacja, instalacje przemysłowe).
- Występują przypadki oddziaływania zewnętrznych pól elektromagnetycznych znacznie silniejszych niż te, dla których sprzęt był projektowany, w tym w sposób losowy (np. wyładowania atmosferyczne), jak również może mieć miejsce celowe zakłócanie pracy węzła łączności komputerowej (terroryzm EM, działania wojenne).
- Pozostaje do rozwiązania temat zabezpieczenia przed podsłuchem elektromagnetycznym.

- ograniczona przestrzeń możliwa do uzyskania w tej technologii „klatki Faradaya" to typowe budowane kabiny 2x3 m.

W związku z powyższym technologia ta może mieć zastosowanie do stosunkowo niewielkich ilości sprzętu węzła i na ogół narzuca potrzebę wydzielenia w ramach węzła podsystemu podlegającego szczególnej ochronie. Ponadto przy zastosowaniu rozwiązań opartych na kabinach metalowych należy uwzględnić wymogi konstrukcyjno – montażowe oraz konieczność zachowania w bezpośrednim otoczeniu kabiny określonej przestrzeni pomiarowo – technologicznej, co zwykle wiąże się z dużą stratą przestrzeni pomieszczenia, w którym instalowana jest kabina.

Stosowanie kabin metalowych wymaga także planowania instalacji takiej kabiny już na etapie projektowania budynku z uwagi na obciążenia stropów i technologię montażu kabin. W wieku przypadkach zastosowanie tej technologii w już istniejących budynkach jest niemożliwe. Praca personelu obsługującego węzeł zamkniętego w kabinie metalowej nie zapewnia podstawowych wymagań ergonomicznych. Może być też niebezpieczna z uwagi na fakt przebywania ludzi w zamknięciu i izolacji, niemożność natychmiastowej ewakuacji oraz natłok sprzętu i urządzeń. Kabina stwarza problemy utrzymania właściwej temperatury i wymiany powietrza. Tak nienaturalne otoczenie miejsca pracy może wywoływać i potęgować stresy psychiczne.

W odniesieniu do węzłów sieci komputerowych stosowanie rozwiązań w postaci kabin metalowych przy prawidłowym ich montażu i eksploatacji zapewnia ochronę elektromagnetyczną w bardzo wysokim stopniu. Z wymienionych powodów nie można jednak uznać, że może to być rozwiązanie przydatne do powszechnego stosowania.

Obecnie wydaje się, że być może w większości realnie istniejących potrzeb nie ma bezwzględnej konieczności uzyskiwania tłumienności rzędu 100÷120 dB. Większość powszechnie istniejących potrzeb ochrony elektromagnetycznej sprzętu komputerowego i innych urządzeń węzła wydaje się być możliwa do spełnienia przy uzyskaniu poziomu tłumienności około 60 dB. Stosowanie cieńszych powłok metalowych od powszechnie stosowanych w tradycyjnych kabinach jest problematyczne z uwagi na wymogi konstrukcyjne (np. proces spawania).

Przyjmując zasadę, że o skuteczności ochrony decyduje najsłabsze ogniwo w zastosowanym rozwiązaniu (np. otwory drzwiowe i okienne, doprowadzenia energetyczne, linie telefoniczne, kanalizacja, ogrzewanie itp.), poziom tłumienia elektromagnetycznego kabin może być znacznie niższy niż oczekiwane 100 (120 dB. Nie wydaje się, żeby mimo istnienia powszechnych potrzeb ochrony węzłów rozwiązanie w postaci kabin metalowych wyszło poza zastosowania militarne czy też specjalne.

Ochrona węzłów jest zagadnieniem znacznie szerszym niż tematyka dotycząca zjawisk promieniowania elektromagnetycznego. Zazwyczaj wprowadza się strefy ochrony fizycznej. W ten sposób ekranowanie na poziomie 60 dB (biorąc pod uwagę tłumienie murów i naturalne rozproszenie energii elektromagnetycznej) może oznaczać efekt 100 i więcej dB poza granicą strefy ochrony fizycznej, tzn. być taki, jakiego oczekuje się od tradycyjnych kabin metalowych.

Rozwiązanie w postaci ekranowania elektromagnetycznego całych pomieszczeń węzła stało się w ostatnim czasie nie tylko realne, lecz i atrakcyjne zarówno w aspekcie efektów, jak i kosztów. Jest tak z uwagi na zupełnie nowe perspektywy, jakie stwarzają nowe materiały (nie wykorzystywane dotychczas w kraju), które mogą być użyte jako osłona ekranująca.

Charakterystyczną cechą tych nowych materiałów jest:

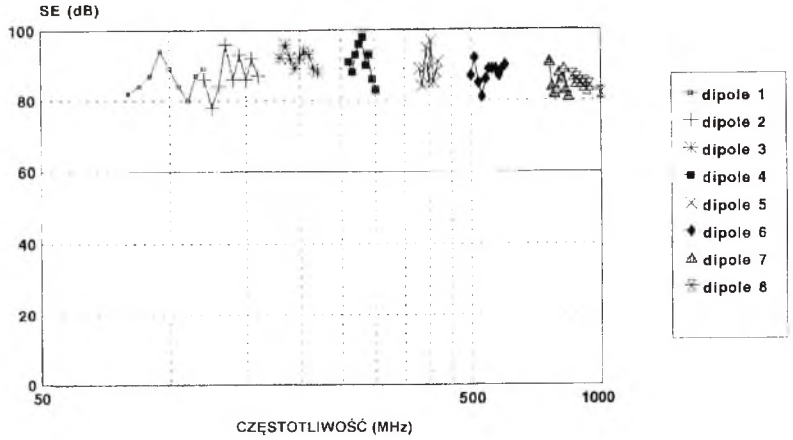
- Rozważono zagrożenia naruszeń ciągłości materiału ekranującego w wyniku przypadkowych bądź celowych uszkodzeń mechanicznych, lub chemicznych w powłoce tapety, uszczelnionych doprowadzeniach i otworach;
- Zapewniono możliwości odpowiedniego dostępu w celu konserwacji i serwisu;
- Przygotowano metodykę pomiarów skuteczności ekranowania elektromagnetycznego;
- Zapewniono zgodności z obowiązującymi normami budowlanymi, wymogami ppoż. i ergonomii pracy.

Realizacja pomieszczeń ekranowanych z wykorzystaniem elastycznych materiałów przewodzących wymaga rozważenia i rozwiązania całego wachlarza różnorodnych problemów znacznie wykraczających poza aspekty techniczne samego zjawiska propagacji fal elektromagnetycznych.

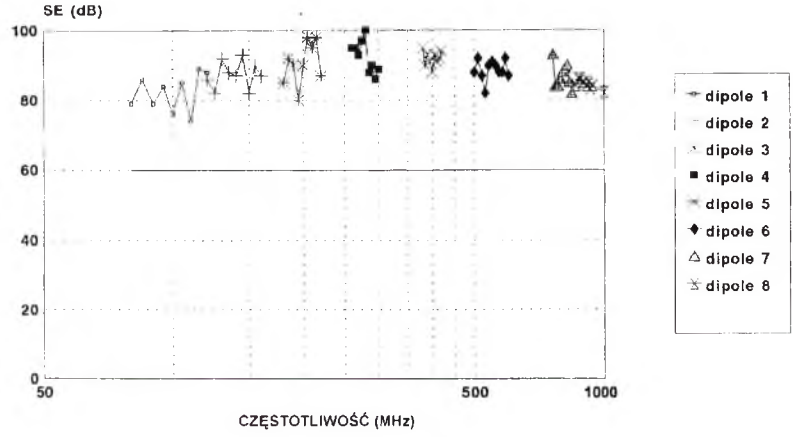
Warto również zaznaczyć, że jednym z istotnych zagadnień jest weryfikacja efektu szczelności elektromagnetycznej pomieszczenia, tj. jego pomiarów. Pochodząca z 1956 r. norma pomiarowa MIL-STD-285 odnosi się do tradycyjnych, stalowych osłon ekranujących, nie może być ściśle i bezpośrednio stosowana np. chociażby z uwagi na ograniczenia przestrzenne. Wszystkie liczące się narodowe normy z tego zakresu są tłumaczeniami ww. normy, która pozostaje normą najczęściej stosowaną. W praktyce odnosi się to nie tyle do samych pomiarów, co do wspólnego odniesienia dla porównania i interpretacji wyników. Należy jednocześnie zaznaczyć, że zmiany efektywności ekranowania elektromagnetycznego podawane zwykle w [dB] dla poszczególnych zakresów częstotliwości mogą pozostawać w dość luźnym związku w stosunku do potrzeb ochrony węzła. Wynik pomiaru według MIL-STD-285 nie powinien być ostateczną miarą w odniesieniu do oceny stopnia ochrony węzła sieci komputerowej. W każdym konkretnym przypadku przedsięwzięć zwiększających bezpieczeństwo węzła sieci komputerowej duże praktyczne znaczenie może mieć charakterystyka promieniowania systemu podlegającego ochronie, w tym zwłaszcza charakterystyka widmowa promieniowania będącego nośnikiem przetwarzanych danych, a także zakresów, które są szczególnie podatne na zakłócenia. Istotny jest fakt binarnej postaci tych danych oraz sposób modulacji i kodowania sygnału, redundancja i podobne zagadnienia sytuujące się w obszarze klasycznej teorii informacji. Z powyższego wynika potrzeba prowadzenia pomiarów oraz interpretacji uzyskanych wyników w sposób indywidualny dla każdego węzła sieci komputerowej.

Klasycznie efektywność ekranowania określana jest stosunkiem poziomów mocy fal elektromagnetycznych przed i za osłoną. Idealną miarą efektywności ekranowania w odniesieniu do problematyki ochrony sprzętu węzła w aspekcie poufności danych mógłby stanowić np. stosunek kosztu odbioru i dekodowania, tj. uzyskania danych komputerowych z fali elektromagnetycznej przed i za zasłoną ekranującą. W takim jednak ujęciu pomiary w aspekcie bezpiecznych węzłów wykraczają znacznie poza ramy stosowanego dotychczas modelu oraz norm, metod i technik pomiarowych.

Wydaje się, że obiecującymi kierunkami poszukiwań bardziej precyzyjnych metod wartościowania końcowego efektu ekranowania mogą być w pełni skomputeryzowane systemy pomiarowe wyposażone w samo adaptacyjne przetworniki analogowo – cyfrowe korelujące dane odbieranego sygnału z binarną postacią danych źródłowych z systemu komputerowego. Wykorzystywany może być dorobek i doświadczenie technik przesyłania danych cyfrowych w warunkach dużych zniekształceń i znacznych spadków mocy odbieranego sygnału.



Rys. 3. Wyniki pomiaru pomieszczenia w punkcie 3



Rys. 4. Wyniki pomiaru pomieszczenia w punkcie 6

Omawiane w niniejszym referacie rozwiązanie bazujące na opracowanej w ostatnich latach technologii elastycznych materiałów przewodzących dających efekt ekranowania pola elektromagnetycznego na poziomie 60 (70 dB może stanowić atrakcyjne uzupełnienie, a w niektórych przypadkach zastąpienie technologii kabin metalowych. Ekranowanie rzędu 60 dB wydaje się w zupełności rozwiązywać większość zagadnień ochrony przed promieniowaniem zewnętrznym. Odnośnie do aspektu zachowania poufności danych należy mieć na uwadze możliwości kompleksowego stosowania również innych środków (np. maskowania sygnału niosącego dane chronione w energii elektromagnetycznej wypromieniowanej przez analogiczny sprzęt komputerowy przetwarzający dane jawne i umieszczony na zewnątrz pomieszczeń ekranowanych).

ROZPRASZANIE ELEKTROMAGNETYCZNE WĘZŁÓW SIECI KOMPUTEROWYCH

Daniel J. Bem, Waldemar E. Grzebyk, Jarosław M. Janukiewicz

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

1. Wprowadzenie

W Zakładzie Naukowym Telekomunikacji NASK w ramach prac badawczych dotyczących rozpraszania elektromagnetycznego węzłów sieci komputerowych wykonano następujące prace:

- Przeprowadzono studia literaturowe na temat rozpraszania elektromagnetycznego urządzeń telekomunikacyjnych stosowanych w sieciach komputerowych.
- Zapoznano się z metodami pomiaru rozpraszania elektromagnetycznego urządzeń telekomunikacyjnych stosowanych w węzłach sieci komputerowych (normy i zalecenia).
- Przeprowadzono przy współpracy z Instytutem Telekomunikacji i Akustyki Politechniki Wrocławskiej (ITA PWr.) badania mające na celu sprawdzenie możliwości oraz opracowanie metodyki pomiarów charakterystyk częstotliwościowych odbicia materiałów tłumiących w komorze bezodbiciowej.
- Przeprowadzono przy współpracy z Instytutem Telekomunikacji i Akustyki Politechniki Wrocławskiej badania mające na celu opracowanie metody pomiaru skuteczności ekranowania szaf telekomunikacyjnych stosowanych w węzłach sieci komputerowych.

Wyniki tych badań zamieszczono w oddzielnym artykule.

2. Rozpraszanie elektromagnetyczne węzłów sieci komputerowych

Węzły sieci komputerowych składają się z elementów biernych i aktywnych. Do biernych elementów można zaliczyć: okablowanie, szafy telekomunikacyjne, krosownice itp.; do aktywnych natomiast: rutery, przełączniki, mosty, zasilacze awaryjne, konsole itp.

Znajomość wszystkich istotnych właściwości poszczególnych elementów składowych węzła sieci komputerowej umożliwia znalezienie możliwych dróg rozpraszania elektromagnetycznego

Zależnie od wymagań stosowanych norm lub specyfikacji odnoszących się do danego systemu telekomunikacyjnego właściwości emisyjne określane są za pomocą różnych metod pomiarowych elementów składowych systemu:

- pomiar prądów i napięć zakłócających,
- pomiar prądów i napięć zakłócających w czasie rzeczywistym,
- pomiar natężenia pola magnetycznego,
- pomiar natężenia pola elektrycznego,
- pomiar natężenia pola elektromagnetycznego,
- pomiar wielkości tłumienia ekranów obudów.

W wielu przypadkach wpływ okablowania systemu wraz z wszystkimi połączeniami rozłącznymi na rozpraszanie elektromagnetyczne węzła sieci komputerowej jest całkowicie niedoceniany. Nawet w małych węzłach okablowanie ma znaczną długość. Sprzężenia indukcyjne, pojemnościowe i przez promieniowanie między przewodami w wiązce kabli lub między wiązkami kabli, powodują często nieoczekiwany wzrost wielkości rozpraszania elektromagnetycznego,

Tabela 1. Normy EMC dla urządzeń informatycznych (ITE) dotyczące zakłóceń emitowanych

Normy międzynarodowe	Normy europejskie	Normy polskie	Normy niemieckie	Określenia norm
CISPR 22 & A1 (1993)	EN 55022 & A1 (1994)	PN-EN 55022 (1996)	VDE 0878, T.3 i T.22	Dopuszczalne poziomy i metody pomiaru zakłóceń radioelektrycznych wytwarzanych przez urządzenia informatyczne

Urządzenia tego typu obejmują m.in. urządzenia sieciowe i telekomunikacyjne stosowane w węzłach sieci komputerowych.

Urządzenia informatyczne klasy B według PN-EN 55022

Są to urządzenia, których poziom zakłóceń emitowanych (poziomy dopuszczalne zakłóceń radioelektrycznych) odpowiadają wymaganiom klasy B. Sprzęt klasy B jest przeznaczony przede wszystkim dla środowiska mieszkalnego i obejmuje m.in. urządzenia telekomunikacyjne zasilane z sieci telekomunikacyjnej, komputery indywidualne oraz przyłączone do nich urządzenia peryferyjne. Przez środowisko mieszkalne rozumie się środowisko w którym odbiorniki radiofoniczne i telewizyjne mogą być używane w odległości mniejszej niż 10 m od badanego urządzenia.

Urządzenia informatyczne klasy A według PN-EN 55022

Są to urządzenia informatyczne, których poziomy zakłóceń odpowiadają wymaganiom klasy A, ale nie spełniają wymagań klasy B. Urządzenia tego typu nie powinny podlegać żadnym ograniczeniom sprzedaży, jednak w instrukcji obsługi musi się znajdować informacja ostrzegawcza, że w mieszkaniach i domach aparat ten może powodować zakłócenia odbioru radiowego.

Tabela 2.

Klasa A		
Zakres częstotliwości	**Poziom dopuszczalny [dB (μV)]**	
[MHz]	**Wartość quasi-szczytowa**	**Wartość średnia**
0,15 ÷0,50	79	66
0,50 ÷30	73	60
• Na częstotliwości granicznej 0,50 MHz obowiązuje poziom niższy.		

3.1. Pomiar zakłóceń promieniowanych

Poziom zakłóceń promieniowanych do środowiska, podobnie jak przewodzonych, zależy nie tylko od parametrów urządzeń, ale również od dołączonych do nich linii zasilających, przewodów interfejsowych i kabli sterujących. W przypadku zakłóceń promieniowanych poziom ten określa wartość promieniowanego przez badane urządzenie natężenia pola elektromagnetycznego lub też promieniowanej mocy. Poziom zakłóceń przewodzonych do środowiska definiuje się przez określenie napięcia na dołączonych do badanego urządzenia przewodach lub też przewodzonego przez nie prądu.
Badania poziomu zakłóceń promieniowanych przez urządzenia przeprowadza się:

- na poligonach pomiarowych,
- w komorach bezodbiciowych,
- w komorach TEM typu Crawforda,
- komorach GTEM.

Bez względu na rodzaj stanowiska pomiarowego wyniki pomiarów w celu porównania odnosi się zawsze do pomiarów na poligonie pomiarowym. Właśnie dla pomiarów na poligonie pomiarowym w normach zdefiniowano dopuszczalne poziomy zakłóceń promieniowanych do środowiska. Aby mieć pewność, że badane obiekty spełniają wymagania stawiane przez normy w odniesieniu do poziomu natężenia promieniowanego pola elektromagnetycznego normy formułują również wymagania odnośnie: pola pomiarowego, konfiguracji układu pomiarowego, metod pomiaru oraz urządzeń pomiarowych.

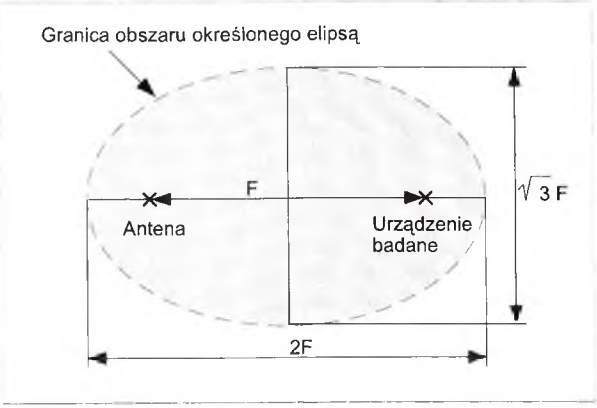
Norma PN-EN 55022 przyjmuje, że pomiary natężenia pola elektromagnetycznego powinny być wykonywane na otwartym poligonie pomiarowym. Stosowanie innych miejsc pomiarowych, uwarunkowane jest posiadaniem przez nie odpowiedniego atestu zgodności.

Pomiar emisyjności sprowadza się do określenia natężenia pola elektromagnetycznego na kierunku maksymalnego promieniowania. Większość norm zaleca układ pomiarowy, którego ideę zobrazowano na rysunku 1. Badany obiekt umieszcza się na izolowanej podstawie na wysokości h=1 m nad ziemią odniesienia (2 m przy odległości pomiarowej 30 m). Pomiaru natężenia pola elektromagnetycznego dokonuje się dla obu polaryzacji: poziomej i pionowej wyszukując kierunek maksymalnego promieniowania. Wyszukiwanie to odbywa się poprzez obrót badanego obiektu w płaszczyźnie poziomej w zakresie od 0° do 360° oraz zmianę wysokości zawieszenia anteny odbiorczej H w przedziale od 1 do 4 m (dla odległości pomiarowej D = 3 m i 10 m) oraz w przedziale od 2 do 6 m (dla odległości pomiarowej D = 30 m).

Przewody pomiarowe oraz zasilające powinny być tak poprowadzone, aby ich wpływ na wynik pomiarów natężenia pola elektromagnetycznego był jak najmniejszy.
Pomiar emisyjności na poligonie pomiarowym ma wiele niedogodności. Do najważniejszych należą:

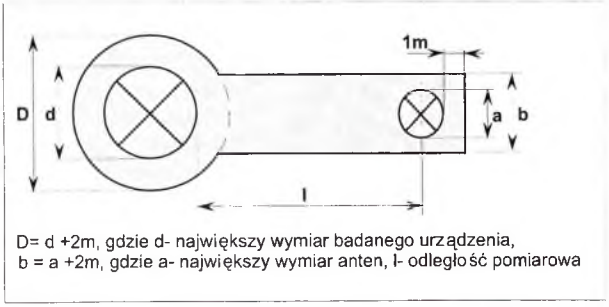
- wpływ czynników atmosferycznych na dostępność poligonu pomiarowego (przy złej pogodzie pomiar jest niemożliwy)
- wpływ otaczającego środowiska elektromagnetycznego, który zmusza do usytuowania poligonu w dużej odległości do potencjalnych zakłóceń.

odległość większą niż 3 m w stosunku do najwyżej położonych elementów układu pomiarowego. Zazwyczaj takie ograniczenie nasuwa najwyższe położenie anteny pomiarowej. Przy zalecanych przez normy wysokościach oznacza to, że nad płaszczyzną ziemi aż do wysokości 7 - 9 m nie powinno być żadnych elementów metalowych (związanych np. z konstrukcją dachu osłaniającego pole pomiarowe).



Rys 2. Poligon pomiarowy do pomiaru natężeń pól zakłóceń

Istotnym czynnikiem decydującym o poziomie mierzonego pola elektromagnetycznego jest nie tylko przewodność odbijającej płaszczyzny (ziemi odniesienia), ale również jej rozmiary. Oceny niezbędnych rozmiarów i kształtu ziemi odniesienia można dokonać korzystając z kryterium Fresnela. Tak zwana elipsa Fresnela określa najbardziej istotną część terenu, która warunkuje wartość mierzonego natężenia pola (rys. 2).



Rys. 3. Rozmiary płaszczyzny odniesienia wg PN-EN 55022

Pewna część elipsy Fresnela jest wyłożona metalową siatką lub płytą. Istotna jest odpowiedź na pytanie jaka to powinna być część. Oczywiście optymalnym rozwiązaniem z punktu widzenia przydatności byłoby pokrycie metalową płytą całej elipsy Fresnela. Jest to rozwiązanie optymalne,

$$r_a = \frac{2 \cdot D^2}{\lambda}$$

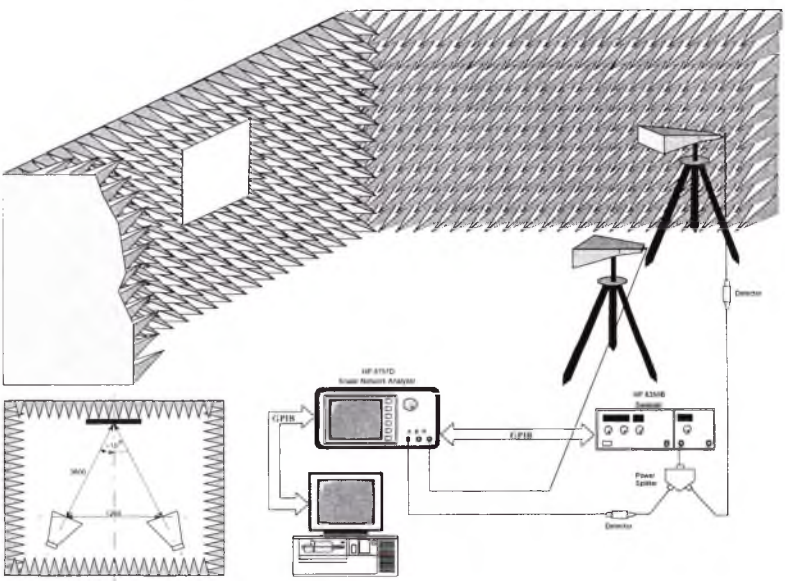
gdzie: r_a - suma odległości: antena nadawcza - płaszczyzna odbijająca i płaszczyzna odbijająca - antena odbiorcza. W „arch metod" promień łuku przyjmuje się jako 1/2 wartości r_a [m]. Jest to odległość dla której występuje strefa przejściowa pomiędzy polem bliskim (strefa Fresnela) a polem dalekim (strefa Fraunhofera) anten,

D - apertura anten [m]. Jako wartość współczynnika D przyjmuje się większy z wymiarów struktury anteny,

λ - długość fali dla najwyższej częstotliwości pomiarowej anteny [m].

4.2. Opis stanowiska pomiarowego

W komorze bezodbiciowej ITA PWr w oparciu o posiadany sprzęt pomiarowy (Scalar Network Analyzer HP 8757D, Sweeper Generator 8350B) oraz anteny pomiarowe (П6-23А) wykonano stanowisko do pomiaru charakterystyk częstotliwościowych współczynnika odbicia materiałów metodą łukową (ang. arch metod). Schemat układu pomiarowego i jego wymiary geometryczne przedstawiono na rysunku 5.



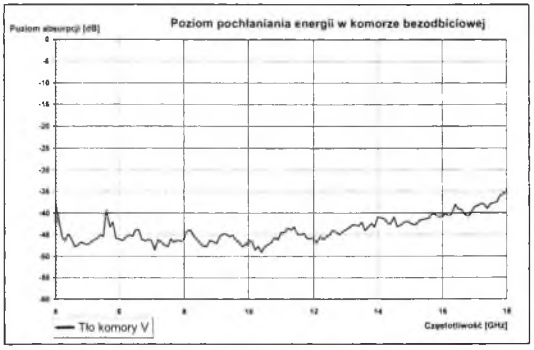
Rys. 5. Stanowisko do pomiaru charakterystyk częstotliwościowych absorpcji materiałów metodą łukową wykonane w komorze bezodbiciowej z wykorzystaniem aparatury pomiarowej ITiA

Kalibrację układu pomiarowego wykonywano na płytę odbijającą wykonaną z aluminium, na której montowane były badane próbki materiałów tłumiących. Kąt padania i odbicia fali wynosił 10 stopni, odległość próbki od anteny wynosiła 360 cm. Szerokość wiązki anteny nadawczej zmienia się od 15 stopni dla 4 GHz do 5 stopni dla 18 GHz. Odpowiada to oświetleniu powierzchni kołowej o średnicy 95 cm dla 4 GHz i 30 cm dla 18 GHz. Fala wypromieniowana przez antenę nadawczą jest spolaryzowana liniowo w płaszczyźnie elewacji. Minimalny rozmiar próbki, który

pozwoliłby na pomiar współczynnika absorbcji z dokładnością rzędu (1dB powinien wynosić 100x100 cm. Dokładnie zmierzono tło komory co pozwoliło określić czułość układu pomiarowego na około - 40 dB *(Rys. 6).*

4.3. Przykładowe wyniki pomiarów

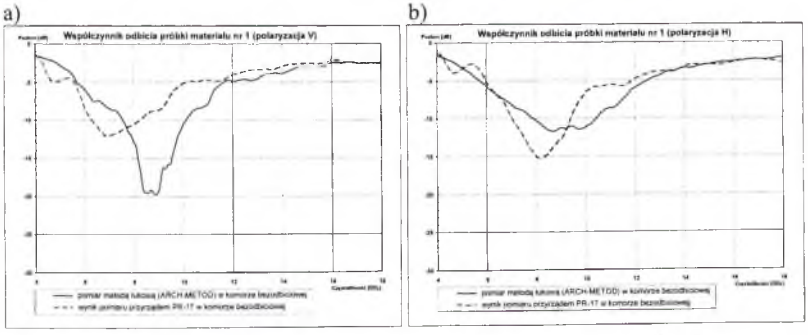
Podczas badań przeprowadzono pomiary kilku próbek materiałów tłumiących. Pomiary wykonano w paśmie częstotliwości od 4 do 18 GHz. W celu sprawdzenia dynamiki pomiaru wykonano pomiar tła komory bezodbiciowej (rys. 6).



Rys. 6. Charakterystyka tła komory bezodbiciowej

Na rysunkach 7 i 8 przedstawiono wyniki pomiarów charakterystyk współczynnika odbicia dwóch typów materiałów tłumiących oznaczonych numerami 1 i 2 dla dwóch polaryzacji anten (V- poziomej i H - pionowej), wykonanych metodą łukową w komorze bezodbiciowej.

Dla porównania, na wykresy naniesiono również (linią przerywaną) wyniki pomiaru charakterystyk częstotliwościowych współczynnika odbicia odpowiednich materiałów tłumiących wykonanych reflektometrem PR-17 CXKu w komorze bezodbiciowej. Zasada działania reflektometru PR-17 CXKu jest również oparta na metodzie łukowej.



Rys. 7. Charakterystyka częstotliwościowa współczynnika odbicia próbki materiału tłumiącego nr 1: a) polaryzacja V, b) polaryzacja H

BADANIA SKUTECZNOŚCI EKRANOWANIA SZAF TELEKOMUNIKACYJNYCH STOSOWANYCH W WĘZŁACH SIECI KOMPUTEROWYCH

Waldemar E. Grzebyk, Jarosław M. Janukiewicz, Jacek Skrzypczyński[*)]

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

1. Wprowadzenie

Podstawą zapewnienia niskiego poziomu rozpraszania elektromagnetycznego przez węzły sieci komputerowych jest znajomość wszystkich istotnych właściwości poszczególnych elementów składowych. Dla systemów prostych i przejrzystych, z kilkoma tylko elementami składowymi, niezbędna informacja może zostać ograniczona do przedstawienia parametrów podstawowych. Natomiast w wypadku większych systemów o złożonej strukturze, nawet informacje drugorzędne mogą stać się decydujące o jego jakości.

W zasadzie każda metoda pomiarowa dająca się technicznie zrealizować, może być zastosowana dla uzyskania wartości parametrów ważnych z punktu widzenia rozpraszania elektromagnetycznego węzła sieci.

Jednym z elementów węzłów sieci komputerowych decydujących o poziome rozpraszania elektromagnetycznego urządzeń aktywnych są szafy telekomunikacyjne. W szafach instalowany jest sprzęt sieciowy. Przy prawidłowym wykonaniu szafy i jej uszczelnieniu stanowi ona dobry ekran dla pola elektromagnetycznego.

W Zakładzie Naukowym Telekomunikacji NASK przy współpracy z Instytutem Telekomunikacji i Akustyki Politechniki Wrocławskiej (ITA PWr.) prowadzone są prace badawcze dotyczące rozpraszania elektromagnetycznego węzłów sieci komputerowych. W ramach tych prac w ITA wykonano badania mające na celu opracowanie metody pomiaru skuteczności ekranowania szaf telekomunikacyjnych stosowanych w węzłach sieci komputerowych.

2. Skuteczność ekranowania

Właściwości pola elektromagnetycznego są określone przez:

- źródło rozproszenia elektromagnetycznego,
- ośrodek otaczający źródło,
- odległość między źródłem a punktem obserwacji.

W przestrzeni wokół źródła rozpraszania elektromagnetycznego można wyróżnić trzy obszary [1] (*Rysunek 1*):

[*)] Instytut Telekomunikacji i Akustyki Politechniki Wrocławskiej
Wybrzeże St. Wyspiańskiego 27, 50-370 Wrocław

Podczas padania fali elektromagnetycznej na powierzchnię materiału ekranującego występują dwa rodzaje strat *(Rysunek 2)*:

- fala ulega odbiciu (R) od powierzchni, a jej część która nie ulega odbiciu jest tłumiona przy przechodzeniu przez materiał ekranujący,
- fala ulega pochłanianiu (A).

W przypadku cienkich materiałów ekranujących mogą występować wielokrotne odbicia (B) od obu płaszczyzn materiału.

Całkowitą wartość tłumienności ekranowania materiału ekranującego można zapisać jako [1]:

$$S\,[dB] = A + R + B \qquad (1)$$

gdzie: ***A*** - straty pochłaniania,
R - straty odbicia,
B - współczynnik korekcji uwzględniający wielokrotne odbicia w cienkich ekranach.

Wszystkie składniki sumy *(1)* są wyrażone w decybelach. Wartości poszczególnych rodzajów strat rozpraszania elektromagnetycznego, uzyskiwane przy zastosowaniu materiału ekranującego, można oszacować w oparciu o teoretyczne zależności.

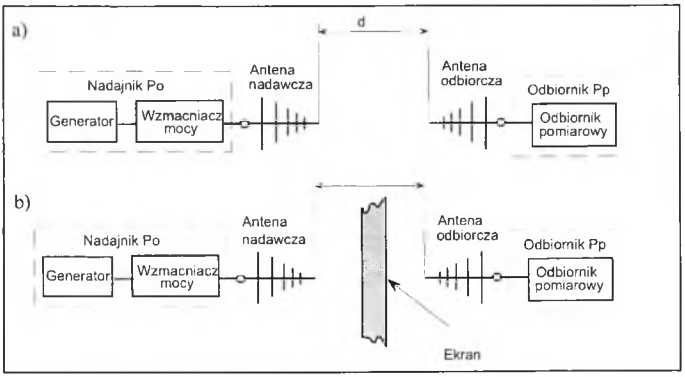
Oprócz rozważań teoretycznych prowadzone są pomiary skuteczności ekranowania różnych materiałów i ekranów o różnych rozwiązaniach konstrukcyjnych. Pomiary służą do weryfikowania teorii przez praktykę. Na ich podstawie opracowuje się wykresy i tablice ułatwiające zaprojektowanie ekranu o wymaganej jakości.

3.2. Metody pomiaru skuteczności ekranowania

Podczas pomiaru skuteczności ekranowania określa się tłumienność ekranowania badanego obiektu. Pomiar wykonujemy względem:

- poziomu mocy sygnału P_o - dla pola dalekiego,
- poziomu natężenia pola elektrycznego E_o, - dla składowej elektrycznej w polu bliskim,
- poziomu natężenia pola magnetycznego H_o - dla składowej magnetycznej w polu bliskim,

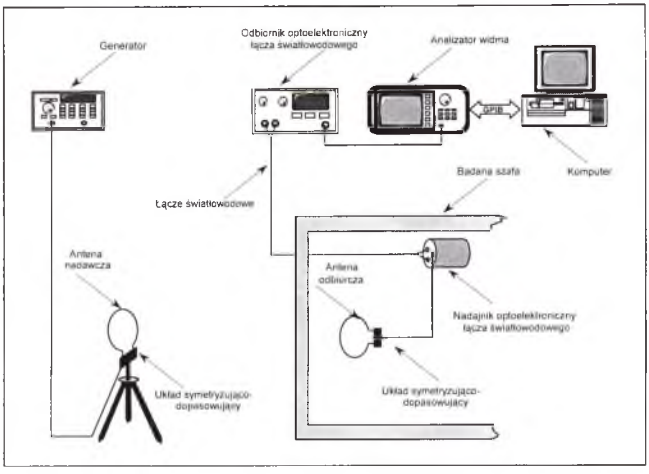
odebranego przez antenę podczas kalibracji bez obecności badanego ekranu (*Rysunek 3a*)



Rysunek 3. Metoda pomiaru skuteczności ekranowania
a) pomiar poziomu odniesienia
b) pomiar poziomu natężenia pola po stłumieniu przez ekran.

Poziom sygnału P_p, E_p lub H_p mierzony jest po wprowadzeniu ekranu (*Rysunek 3b*).

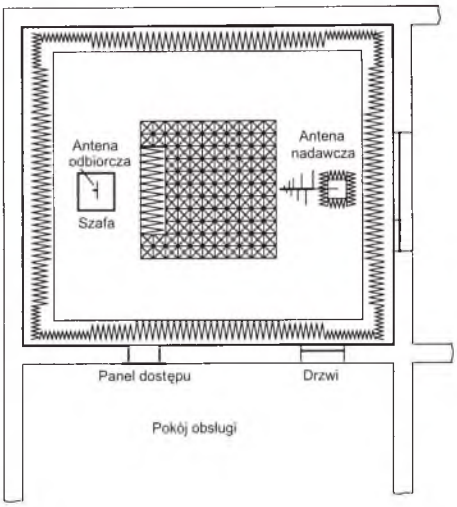
siebie w odległości 60 cm jedna od drugiej. Dla każdej częstotliwości wyznaczono skuteczność ekranowania poprzez porównanie poziomu sygnału z anteny odbiorczej na zewnątrz szafy z poziomem sygnału anteny w szafie.



Rysunek 4. Schemat układu pomiarowego do badania skuteczności ekranowania w polu bliskim dla pola magnetycznego, odległość anten od ściany szafy wynosi po 30 cm

Pomiar skuteczności ekranowania dla pola elektrycznego przeprowadzono w następujący sposób: antenę odbiorczą umieszczono symetrycznie względem środka szafy, a antenę nadawczą w odległości 3 m od szafy na tej samej wysokości co antena odbiorcza i ze zgodną polaryzacją (*Rysunek 5 i Rysunek 6*). Przy pomiarach poziomu odniesienia antenę odbiorczą ustawiono 30 cm przed ścianą szafy. Następnie wyznaczono skuteczność ekranowania. Zmieniając ustawienie anten można określać właściwości szafy dla różnych polaryzacji pola elektromagnetycznego. Pomiary przeprowadzono dla polaryzacji poziomej i pionowej. Dla poziomej polaryzacji pola elektrycznego zakres został zawężony do 30-100 MHz. Poziome rozmiary szafy są mniejsze od pionowych więc skrócono dipolową antenę odbiorczą co uniemożliwiło pomiar dla częstotliwości mniejszych od 30 MHz

przenikania energii pola elektromagnetycznego do środka szafy przez kabel łączący antenę odbiorczą z analizatorem widma.



Rysunek 7. Stanowisko pomiarowe w komorze bezechowej

Zakres mierzonych częstotliwości podzielono na 4 podzakresy kierując się optymalnym wykorzystaniem posiadanych anten w wymaganych warunkach pracy:

1) zakres 100 kHz do 30 MHz - anteny ramowe o średnicy 30 cm (pole magnetyczne w strefie bliskiej)
2) zakres 1 MHz do 100 MHz - dipole symetryczne typ AD160 (pole elektryczne w strefie bliskiej)
3) zakres 100 MHz do 300 MHz: antena nadawcza - biconical typ UNA-4, antena odbiorcza - dipol symetryczny typ AD160 (strefa pośrednia pola elektromagnetycznego).
4) zakres 300 MHz do 1 GHz: antena nadawcza - logarytmiczno-periodyczna typ INCO DLA, antena odbiorcza - biconical typ AD60 (strefa daleka pola elektromagnetycznego).

5. Przykładowe wyniki

Badana szafa miała konstrukcję szkieletową, spawaną. Drzwi przednie i tylne oraz osłony boczne były wykonane z blachy stalowej o grubości 1 mm. Między krawędziami blach a szkieletem były szczeliny bez kontaktu elektrycznego. Między dachem szafy a szkieletem był 15 mm odstęp, a w podstawie szafy był otwór o wymiarach 380x380 mm. Szafa nie stanowiła więc dla pola elektromagnetycznego obudowy zamkniętej. Poszczególne fragmenty obudowy sprzęgały się ze sobą bardziej lub mniej skutecznie dla różnych częstotliwości. Wynikiem tego jest występowanie na wykresach skuteczności ekranowania wyraźnych efektów rezonansowych, których charakter zależy od polaryzacji pola. Podczas badania szafy o poprawnej konstrukcji wybiera się częstotliwości pomiarowe leżące poza rezonansami własnymi szafy. Badana szafa ma tak wiele rezonansów, że nie sposób określić, które z nich są wynikiem rezonansów wewnętrznych szafy, a które są wywołane przez efekt antenowy szczelin (*Rysunek 8*).

długości uszczelki. Po pewnym czasie pogarszają się ich parametry z powodu trwałego odkształcenia jakiemu ulegają.

Uszczelki w formie sprężynujących pasków blachy zapewniają dobry styk elektryczny ocierając się o drzwi w czasie zamykania. Nie potrzebują więc dużej siły nacisku dla poprawnego działania i przez to nie odkształcają się w czasie eksploatacji. Są trwałe i chętnie stosowane.

Uszczelki z materiałów elastycznych (np. gumy czy silikonu) mają nieco gorsze parametry ekranujące. Ale niektóre z wykonań osiągają i 100 dB. Plusem jest duże bogactwo kształtów oraz łatwość montażu. Początkowo domieszkowanie materiałem przewodzącym stosowano w całej masie materiału elastycznego. W efekcie uzyskiwano uszczelki, których parametry silnie zależały od stopnia ściśnięcia i bardzo zmieniały się w procesie starzenia. Ani właściwości elastyczne ani przewodzące nie były zadowalające. Obecnie najczęściej są oferowane uszczelki o strukturze podwójnej: elastyczny rdzeń uszczelki jest pokryty cienką warstwą przewodzącą. Takie uszczelki mają dobre zarówno właściwości przewodzące jak i elastyczne. Skutecznie działają przy lekkim ściśnięciu (zmiana wymiaru o 10%) jak i przy dużym odkształceniu (80-90%). Gdy wewnętrzny rdzeń jest wykonany w formie gąbki to zapewnia poprawne działanie nawet przy bardzo małych siłach dociskających.

Niezależnie od rodzaju wybranych uszczelek należy zapewnić dobry kontakt elektryczny uszczelki z powierzchniami obu stykających się elementów, odpowiedni docisk, a również pamiętać o zgodności potencjałów elektrochemicznych.

Literatura

[1]. Ott H.W., "Metody redukcji zakłóceń i szumów w układach elektronicznych", WNT, Warszawa 1979.

[2]. MIL-STD-252, „Military Standard Attenuation Measurements for Enclosures, Electromagnetic Shielding for Electronic Test Purposes, Method of.", United States Government Printing Office, Washington 1956.

[3]. IEEE-STD-299-1991, IEEE Standard of measuring the Effectiveness of the Electromagnetic Shielding Enclosures, Institute of Electrical and Electronics Engineers, New York 1991

[4]. SPECIFICATION NSA NO. 65-6 „National Security Agency Specification for R.F. Shielded Enclosures for Communications Equipment: General Specification", 30 October 1964.

- ze względu na własność izolacji aktywne transakcje nie mogą przekazywać między sobą informacji.

Dlatego też zaproponowano szereg nowych, tak zwanych rozszerzonych modeli transakcji:

- *Transakcje zagnieżdżone [Moss 1985]* są sekwencją *podtransakcji*, które z kolei mogą rekurencyjnie zawierać kolejne podtransakcje, formując w ten sposób hierarchię podtransakcji. Podtransakcje są specyficznymi transakcjami o ograniczonej autonomii, obejmującymi wyodrębnione fragmenty transakcji zagnieżdżonej. Transakcje *potomne* mogą się rozpocząć się dopiero po rozpoczęciu transakcji *przodka*. Z kolei transakcja przodek może się zakończyć dopiero po zakończeniu wszystkich transakcji potomnych. Wycofanie transakcji przodka jest równoważne wycofaniu wszystkich transakcje potomnych. Mimo, że transakcje zagnieżdżone charakteryzują się pełną izolacją, to pozwalają zwiększyć modułowość długich transakcji oraz usprawnić obsługę błędów poprzez wycofywanie pojedynczych podtransakcji zamiast całej transakcji.

- *Transakcje zagnieżdżone otwarte [Weikum i Schek 1992]* są modyfikacją modelu transakcji zagnieżdżonych. Zwiększają one współbieżność długich transakcji w wyniku zmniejszenia izolacji transakcji przez udostępnianie rezultatów zatwierdzonych podtransakcji jednej transakcji zagnieżdżonej innym współbieżnie wykonywanym transakcjom. Rozwiązanie to przewiduje również możliwość modelowania operacji semantycznych i wykorzystanie tej semantyki dla określenia komutatywności operacji i dalszego zwiększenia współbieżności transakcji. Wiąże się to z potrzebą zdefiniowania nowego kryterium spójności dla współbieżnie wykonywanych transakcji.

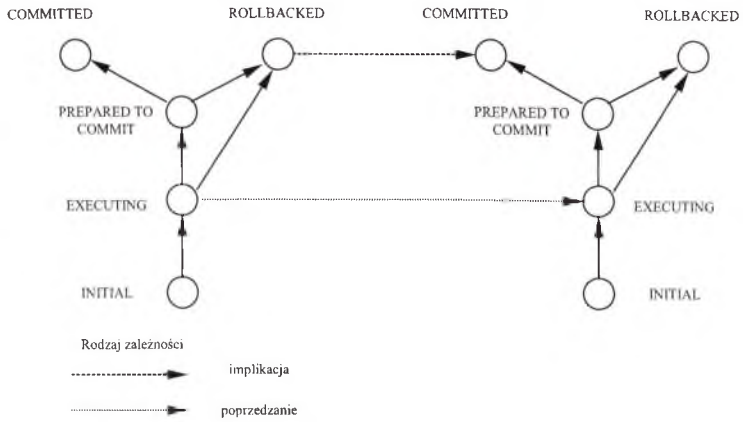
  Transakcje zagnieżdżone wymagają stosowania operacji kompensacyjnych. Zakończona podtransakcja zwalnia zasoby przed zakończeniem transakcji zagnieżdżonej. Późniejsze wycofanie transakcji zagnieżdżonej będzie wymagało wycofania rezultatu zakończonych podtransakcji przez wykonanie transakcji kompensacyjnych.

- *Sagi [Garcia-Molina i Salem 1987]* składają się ze zbioru podtransakcji $T_1,..,T_n$ o własnościach ACID i predefiniowanym porządku wykonywania oraz ze zbioru odpowiadających im podtransakcji kompensacyjnych $CT_1,..,CT_n$. Saga kończy się powodzeniem jeśli wszystkie jej podtransakcje zakończą się powodzeniem. Jeśli jedna z podtransakcji, na przykład T_k, nie powiedzie się, to zatwierdzone podtransakcje $T_1,..,T_{k-1}$ są wycofywane przez wykonywanie podtransakcji kompensacyjnych $CT_{k-1},..,T_1$. Saga rozluźnia własność izolacji przez udostępnienie wyników zatwierdzonych podtransakcji i zwiększa współbieżność transakcji (sag).

- *Transakcje rozdzielane i łączone [Pu 1988]* są przeznaczone dla przetwarzania charakteryzującego się długotrwałym, nieprzewidywalnym rozwojem i interakcją między różnymi wątkami przetwarzania. Transakcje takie mogą być dzielone w trakcie przetwarzania na odrębne transakcje, a później łączone z innymi transakcjami. Rozdzielanie i łączenie transakcji udostępnia mechanizm do bezpośredniego przenoszenia zasobów między różnymi transakcjami.

- *Transakcje elastyczne [Rusinkiewicz i Elmagarmid 1990]* zostały zaproponowane dla środowiska rozproszonych i heterogenicznych baz danych. Transakcja elastyczna obejmuje zbiór zadań, zbiór odpowiadających im podtransakcji oraz zbiór zależności wykonywania podtransakcji, zawierający zależności powodzenia, niepowodzenia i zależności zewnętrzne. W celu rozluźnienia własności izolacji, transakcje elastyczne używają kompensacji, a wymaganie atomowości transakcji jest zastąpione przez określenie akceptowalnego stanu końcowego.

- *Politransakcje [Shath 1992]* zostały zaproponowane jako mechanizm do utrzymywania zależności danych w środowisku rozproszonych i heterogenicznych baz danych. W modelu politransakcji więzy spójności między danymi należącymi do różnych baz danych są definiowane



Rys.2. Struktura transakcyjnego przepływu pracy.

W przypadku dynamicznej specyfikacji struktury przepływu pracy zależności między zadaniami powstają w trakcie wykonywania przepływów pracy, na podstawie wartościowania zdefiniowanego wcześniej zbioru zdarzeń i reguł.

Warunki poprawności przepływów pracy określają kryteria poprawności, które muszą zostać spełnione podczas wykonywania przepływów pracy. Jako warunki poprawności przyjmuje się najczęściej zmodyfikowane i zaadoptowane własności klasycznych lub rozszerzonych modeli transakcji. Określają one dopuszczalne sposoby interakcji między współbieżnie wykonywanymi przepływami pracy, własności procesu odtwarzania stanu i danych jednostek przetwarzania po awarii poszczególnych jednostek lub połączeń między nimi.

4. Realizacja transakcyjnych przepływów pracy

Środowiskiem wykonania transakcyjnych przepływów pracy jest system zarządzania przepływami. System ten musi umożliwiać realizację i koordynację przepływów pracy zgodnie z ich specyfikacją, w rozproszonym i heterogenicznym środowisku systemów baz danych. System zarządzania przepływami pracy musi realizować trzy podstawowe zadania: szeregowania przepływów pracy, synchronizacji współbieżnych przepływów pracy i odtwarzania stanu spójnego przepływów pracy w wypadku awarii systemu zarządzania.

Architektura systemu zarządzania przepływami pracy obejmuje dwa podstawowe moduły: zarządcy i agentów zadań. Agenci zadań nadzorują proces wykonywania poszczególnych zadań. Z każdym zadaniem skojarzony jest jeden nadzorujący go agent. Moduł zarządcy przetwarza przepływy pracy poprzez przedkładanie ich zadań agentom, monitorowanie zdarzeń występujących w ramach realizacji przepływów i analizę warunków związanych z zależnościami występującymi pomiędzy zadaniami.

Proponowane są trzy architektury systemu zarządzania przepływami pracy:

- scentralizowana, w której występuje tylko jeden moduł zarządcy koordynujący wszystkie współbieżnie wykonywane przepływy pracy;
- częściowo rozproszona, w której dla każdego realizowanego przepływu pracy jest generowane dedykowane wystąpienie modułu zarządcy;

Bibliografia

[1] Chrysanthis P., Ramamiritham K. ACTA: A Framework for Specifying and Reasoning about Transactions. *Proceedings of ACM-SIGMOD Conference on Management of Data*, 1990.

[2] Garcia-Molina H. And Salem K. SAGAS. *Proceedings of ACM-SIGMOD Conference on Management of Data*, 1987.

[3] Georgakopoulos D., Rusinkiewicz M. From Transactions to Transactional Workflows. ICDE-12 New Orleans, Feb. 26 1996.

[4] Kalichenko L. A Declarative Framework for Capturing Dynamic Behavior in Heterogeneous Interoperable Information Resource Enviroment. *Proceedings of the Thitd RIDE International Workshop on Interoperability in Multidatabase Systems*, 1993.

[5] Krychniak P., Rusinkiewicz M., Sheth A. and Thomas G. Boundingthe Effects of Compensatio Under Relaxed Multi-Level Serializability. Technical Report UH-CS-92-06, Dept. Of Computer Science, University of Houston, 1992.

[6] Moss J. E. B. Nested Transactions: Approach to Reliable Distributed Computing. Ph.D. thesis, MIT Press, Cambridge, Mass, 1985.

[7] Pu C. Superdatabases for Composition of Heterogeneous Databases. *IEEE Proceedings of the Fourth International Conference on Very Large Data Bases*, 1988.

[8] Reuter A. ConTracts: A Maens for Extending Control Beyond Transaction Boundaries. *Preceedings of the Third International Workshop on High Performance Transaction Systems,* 1989.

[9] Rusinkiewicz M., Elmagarmid A., Leu and Litwin W. Extending the Transaction Model to Capture More Meaning, *SIGMOD Record*, Vol. 19. 1990.

[10] Rusinkiewicz M., Sheth A. Specification and Execution of Transactional Workflows. In *Modern Database Systems*, editor Won Kim, Addison Wesley 1995.

[11] Sheth A. and Kalinichenko L. Information Modeling in Multidatabase Systems: Beyond Data Modeling. *Proceedings of the First International Conference on Information and Knowledge Management*, 1992.

[12] Sheth A., Rusinkiewicz M. and Karabatis G. Using Polytransactions to Manage Interdependent Data. In: *Transaction Models for Advance Database Aplications*. A. Elmagarmid, ed. Morgan-Kaufmann, Los Altos, Cal., 1992.

[13] Weikum G. And Schek H.-J. Concepts and Applications of Multilevel Transactions and Open Nested Transactions. In Transaction Models *for Advance Database Applications*. A. Elmagarmid, ed. Morgan-Kaufmann, Los Altos, Cal., 1992.

Ponieważ standard X.509 stosuje nazewnictwo zgodne z bazą X.500, baza ta jest naturalnym miejscem przechowywania informacji wymaganej dla sprawnego funkcjonowania PEM. Certyfikaty ze swojej natury są bezpieczne, a zatem przechowywanie ich nie wymaga, aby baza była dobrze zabezpieczona. Podmiana klucza jest wykluczona, możliwe jest jedynie jego skasowanie. Ta własność certyfikatów może być wykorzystana do zabezpieczenia samej bazy X.500, kiedy to certyfikaty, a nie hasła, są podstawą autentykacji użytkowników, korzystających z jej zasobów.

2. Założenia przyjęte w projekcie systemu

Podstawowym założeniem projektowym było wykorzystanie funkcjonującej w Polsce bazy X.500, po odpowiednim jej przygotowaniu, do wprowadzania certyfikatów kluczy publicznych o postaci zgodnej z zaleceniami standardu PEM oraz PGP. Mimo, że obecnie nasz system stosuje wyłącznie klucze PGP, zdecydowaliśmy, że w procesie generacji certyfikatów tworzone będą również certyfikaty zgodne z rekomendacją PEM. Zamierzamy udostępnić narzędzie translacji klucza prywatnego PGP na klucze systemów opartych o X.509, co pozwoliłoby na korzystanie z jednego tylko klucza w większości systemów. Opcjonalnie, na życzenie użytkownika przechowywać będzie można certyfikat X.509 nie mający związku z certyfikatem PGP.

W myśl PEMowskich zaleceń, przyjęliśmy, że zostanie powołana struktura administracyjna, pełniąca obowiązki urzędu poświadczającego klucze publiczne.

Duży nacisk został położony na wiarygodność wystawianych certyfikatów. Ten wymóg wymusił konieczność odseparowania komputera, na którym wystawiane są poświadczenia. Względy bezpieczeństwa z jednej strony i przewidywany pilotowy zasięg usługi zadecydowały o przyjęciu modelu centralnego urzędu certyfikacyjnego, obsługującego wszystkich użytkowników.

3. Implementacja systemu

Zadania implementacyjne objęły:

1. ustalenie mechanizmu certyfikacji kluczy przez wyznaczony urząd,
2. przygotowanie bazy X.500 do przechowywania danych dotyczących kluczy publicznych,
3. implementację programów narzędziowych do certyfikacji oraz wprowadzania informacji do X.500.

Wydawaniem poświadczeń zajmować się będzie specjalnie w tym celu powołany **Urząd Certyfikacyjny Polskiej Akademickiej Usługi Katalogowej** (w skrócie **UC**). Urząd ten poświadcza klucze publiczne otrzymywane ze wszystkich regionów Polski za pośrednictwem wyznaczonych Delegatur. W celu uproszczenia zarówno samego systemu, jak i ścieżki weryfikacji klucza przez użytkowników, jedynym zadaniem Delegatur jest umożliwienie użytkownikom bezpośredniego kontaktu z Urzędem Certyfikacyjnym. Kontakt taki jest niezbędny przy pierwszej weryfikacji tożsamości użytkownika. W utworzonej strukturze rolę UC pełni zespół administratorów polskiej usługi katalogowej X.500 w Toruniu, jako Delegatury występują administratorzy regionalni serwerów X.500.

Kolejnym składnikiem systemu jest **baza przechowująca certyfikaty**. Wykorzystana tu została funkcjonującą już w sieci Internet baza X.500. Baza została dostosowana do wprowadzania danych związanych z pocztą PGP oraz PEM, poprzez rozbudowę tablic dopuszczalnych typów obiektów i atrybutów. Standard X.500 definiuje postać wprowadzanego certyfikatu, uzupełnienia do standardu (publikowane w ramach *RFC* i *Internet-Drafts*) opisują, w jaki sposób należy gromadzić takie informacje jak np. klucze PGP. Dokumenty te określają również składnię atrybutów przechowujących dane związane z bezpieczną wymianą informacji.

W celu udostępnienia publicznie danych umożliwiających bezpieczną komunikację do bazy X.500 wprowadzane są następujące informacje:

- przygotowany zestaw skryptów w języku *Perl*, przeznaczonych do wprowadzania przez Delegatury modyfikacji do bazy X.500.

Użytkownik zainteresowany korzystaniem z opisanej usługi bezpiecznej poczty musi mieć dostęp do pakietu PGP, aby wygenerować klucze.

UC wykorzystuje do wystawiania certyfikatów stanowisko niezależne, odseparowane od sieci. Poświadczaniu podlegają klucze publiczne otrzymane w postaci *armor* od Delegatur, kluczowi towarzyszyć musi nazwa wyróżniona użytkownika w bazie X.500. Programy, z których korzysta system wystawiania certyfikatów to pgp oraz program pgp2cert, napisany w oparciu o biblioteki pakietu *SecuDE* (Security Development Environment) – jest to oprogramowanie rozwijane przez niemiecką organizację GMD, jako zestaw narzędzi programowych wspomagających tworzenie poufnych systemów. Całość została przygotowana w postaci interakcyjnego skryptu w języku *Perl*.

Polska bramka WWW-X.500 pozwala na wyszukiwanie kluczy PGP znajdujących się w internetowej gałęzi X.500, umożliwia on pobranie klucza w postaci tekstowej, bądź bezpośrednio do *keyringu* za pomocą odpowiedniego *plug-in* zdefiniowanego w przeglądarce Netscape.

5. Procedura generowania środowiska bezpiecznej wymiany informacji

W celu umieszczenia swoich danych dotyczących bezpieczeństwa w bazie X.500 niezbędne jest wykonanie następujących działań:

1. Użytkownik generuje samodzielnie klucze PGP (prywatny i publiczny).
2. Użytkownik zgłasza się do regionalnej delegatury, przekazuje swój klucz publiczny. Delegatura potwierdza tożsamość klienta (np. poprzez dowód osobisty). Użytkownik podpisuje również zgodę na umieszczenie danych w systemie X.500.
3. Delegatura przesyła (w środowisku bezpiecznej poczty) zlecenie certyfikacji do UC, dane zawierają klucz publiczny poprzedzony nazwą wyróżnioną DN identyfikującą użytkownika w hierarchii drzewa X.500.
4. UC usuwa z odebranego klucza wszystkie zbędne podpisy i sam poświadcza go własnym podpisem, następnie generuje na jego podstawie certyfikat PEMowski i przygotowuje plik w postaci poprawek do bazy X.500.
5. UC wysyła przygotowane dane do Delegatury za pośrednictwem bezpiecznej poczty.
6. Delegatura wprowadza dane do bazy X.500.

6. Zasady uczestnictwa w systemie bezpiecznej wymiany informacji

Docelowo przewidywane jest odpłatne korzystanie z usługi generacji certyfikatów. Użytkownik korzystający z systemu będzie zatem zobowiązany do usunięcia z bazy certyfikatu, za który nie opłacono abonamentu. Niezależnie od tego, ważność certyfikatu będzie zawsze ograniczona do okresu abonamentowego. (PGP nie korzysta z daty ważności certyfikatu, stąd możliwe jest korzystanie z certyfikatów przedawnionych i dlatego powinny one być fizycznie usuwane z bazy).

Uruchomienie serwisu komercyjnego miałoby sens dopiero po uzyskaniu odpowiedniej liczby użytkowników oraz wymagałoby uregulowania spraw związanych z licencjami na oprogramowanie. Z powodu publicznego charakteru usługi X.500 oraz licencji na wykorzystywane oprogramowanie serwerów, wydaje się, że niedopuszczalne jest branie pod uwagę możliwości pobierania opłat za przechowywanie kluczy w bazie. Opłatom podlegać może wyłącznie obsługa wystawiania certyfikatów.

Użytkownik, pragnący umieścić poświadczony klucz publiczny w bazie X.500 kontaktuje się ze swoją Delegaturą (administrator regionalny X.500). Delegatura potwierdza na podstawie odpo-

9. Wykorzystanie zasobów bazy X.500 do bezpiecznej wymiany informacji przez użytkowników

Wykonane do tej pory oprogramowanie ograniczone jest do platformy UNIX. Dostęp do zasobów X.500 jest realizowany za pośrednictwem protokołu LDAP. Zakładamy, że wraz ze wzrostem zainteresowania nową wersją protokołu LDAP pojawią się aplikacje, które będą wykorzystywały ten protokół do odnajdywania certyfikatów X.509. Tworzony przez nas system jest gotowy do tego typu pracy.

Dla użytkowników przygotowano szereg skryptów w języku *Perl* wspomagających pracę zaimplementowanego systemu. Podstawowym założeniem jest stosowanie pakietu PGP. Przyjmuje się, że osoby wykorzystujące nasz system mają w swoim środowisku programowym dostępny program PGP oraz wygenerowane własne klucze.

Jeżeli użytkownik *A* chce prowadzić bezpieczną korespondencję z użytkownikiem *B* musi wprowadzić do swojego *keyringu* jego klucz publiczny. Można tego dokonać za pomocą programu narzędziowego pgp-wrap, który sprawdza istnienie klucza publicznego dla użytkownika o podanym adresie e-mail w lokalnym *keyringu* i w przypadku, gdy klucza nie znaleziono wyszukuje go w zasobach bazy X.500. Funkcjonalność programu pgp-wrap została tak zaprojektowana, że może on być traktowany jako nadbudowa (*wrapper*) programu pgp. Przejmuje on wszystkie argumenty wywołania.

W przypadku, gdy w wywołaniu podano: opcje „-kv" i argument w polu użytkownika jest adresem poczty elektronicznej w postaci user@domain klucz publiczny jest poszukiwany najpierw w lokalnym *keyringu* (domyślne działanie programu pgp), a następnie w przypadku niepowodzenia w bazie X.500. pgp-wrap obsługuje również opcję „-f", oznaczającą przekazanie w standardowym strumieniu wejściowym danych dla programu pgp. W tej sytuacji *wrapper* pośredniczy w wywołaniu pgp, analizuje rezultat, jeżeli program pgp zgłosi się z komunikatem o braku klucza w *keyringu*, klucz ten jest poszukiwany w bazie X.500 (filtr wyszukania jest identyfikatorem klucza – KeyID), po czym następuje kolejne wywołanie pgp. W przypadku innych argumentów sterowanie jest przekazywane standardowemu pgp.

Po wpisaniu klucza publicznego wyszukanego w bazie X.500 do *keyringu*, należy pamiętać o okresowej kontroli poprawności klucza, który może stracić ważność na skutek upływu daty aktywności, czy jego kompromitacji. Program update-pgp umożliwia taką kontrolę, ponieważ porównuje klucz wskazanego użytkownika umieszczony w lokalnym *keyringu* z zawartością bazy X.500 (dokonywane jest porównanie tzw. *fingerprintów*) i zwraca odpowiednie komunikaty.

Użytkownik może również sprawdzić za pomocą programu ckkey, czy klucze umieszczone w jego lokalnym *keyringu*, poświadczone przez Urząd Certyfikacyjny są nadal aktualne. Ta kontrola odbywa się wyłącznie na podstawie daty certyfikacji poszczególnych kluczy, wykorzystuje tylko lokalny *keyring* i zakłada roczny okres ważności poświadczonych kluczy.

pgp-wrap może być wykorzystywany w miejsce programu pgp w automatyczny sposób, poprzez interfejsy e-mail. W takiej sytuacji pojawia się jednak dodatkowe utrudnienie związane z tym, że konieczne jest wykonanie dwóch prób pobrania klucza z *keyringu*. Brak klucza w lokalnym *keyringu* oznacza, ze konieczne jest odwołanie się do zasobów X.500, pobranie klucza, a następnie ponowne wywołanie pgp w celu sprawdzenia poprawności podpisu. W przypadku, gdy mamy do czynienia z pocztę jednocześnie szyfrowaną i podpisaną konieczna jest wstępna deszyfracja, a następnie dopiero weryfikacja podpisu. Wbudowanie funkcji współpracy z X.500 bezpośrednio w pakiet PGP byłoby najprostsze, użytkownicy PGP zgłosili jednak zastrzeżenie co do modyfikacji źródeł pakietu, jako podważających jego wiarygodność. Z tego powodu zdecydowaliśmy się na znacznie bardziej skomplikowaną obsługę poprzez zewnętrzną nakładkę. Komunikacja interakcyjna z programem PGP jest prowadzona za pośrednictwem programu expect. Niestety sposób wykorzystywania pgp przez pakiety obsługujące e-mail jest bardzo różny, stąd niemożliwe jest utworzenie

Literatura

[1] M. Górecka, T. Wolniewicz, *Obsługa zasobów informacyjno-adresowych za pomocą protokołu LDAP — przegląd dostępnych narzędzi i porównanie z technologią X.500*, maj 1998, materiały konferencyjne Miedzeszyn'98
[2] *Privacy Enhancements for Internet Electronic Mail*, RFC 1421-4

Specyfikacja X.500 jest bardzo obszerna, zdefiniowana w ramach siedmiowarstwowego sieciowego modelu OSI. Podstawowym założeniem jest brak uzależnienia od wykonywanego programu, czy środowiska sieciowego. Standard określa globalną, rozproszoną bazę danych opartą na hierarchicznym modelu nazywania obiektów, które mogą być wyszukiwane w zasobach lub przeglądane. X.500 funkcjonuje na zasadzie sieci serwerów (DSA), każdy ma utrzymywać porcję globalnej bazy danych. Użytkownik zasobów X.500 nie jest świadomy ich rozproszenia, ma wrażenie, że korzysta z jednej dużej bazy.

Kluczowe komponenty specyfikacji X.500 w wersji X.500 to:

1. DSA (*Directory System Agent*) – podstawowy serwer usługi, zarządzający fragmentem globalnej bazy.
2. DUA (*Directory User Agent*) – interfejs użytkownika, proces kliencki zgłaszający się do serwera w celu wyszukania informacji.
3. DAP (*Directory Access Protocol*) – protokół stosowany przez DUA dla uzyskania dostępu do serwerów DSA.
4. DSP (*Directory System Protocol*) – protokół stosowany do komunikowania się serwerów DSA między sobą.

Zastosowania usługi katalogowej opartej na standardzie X.500 są różnorodne. Przykładem jest światowa baza X.500 środowiska akademicko-naukowego rozwinięta w trakcie projektu PARIDISE i obecnie koordynowana przez organizację DANTE. Istnieje również sporo zastosowań w instytucjach, gdzie standard X.500 i odpowiednie oprogramowanie służy do zarządzania bazami pracowniczymi, czy systemami ewidencji zasobów różnego typu. W takich przypadkach w minimalnym stopniu, lub wcale nie jest wykorzystywana funkcja rozproszenia zasobów, stosowany jest model scentralizowanej bazy.

2. LDAP

Protokół LDAP wyrósł na bazie doświadczeń w rozwijaniu usługi katalogowej X.500 w latach 1989-91. Dwóch autorów interfejsów użytkowych do zasobów X.500, Marshall Rose i Tim Howes, rozwinęło „odchudzony" protokół pośredniczący w komunikacji programu klienckiego z serwerem X.500. Idea polegała na konstruowaniu przez stronę kliencką prostych zleceń, które przekazywane są serwerowi LDAP pełniącemu rolę bramki pośredniczącej między DUA a DSA i konwertującej zlecenia protokołu LDAP do postaci zleceń X.500 (DAP). Sposób komunikacji został zdefiniowany w standardzie LDAP, rozwijanym w grupie roboczej IEFT OSI-DS. Rezultatem były dokumenty RFC 1487 i aktualizacja w RFC 1777 ([6, 7]).

Porównując protokół LDAP w stosunku do standardu X.500 następujące elementy LDAP uznawane były za „lżejsze", określone w sposób bardziej przystępny:

1. Prostszy protokół kodowania.
2. Nazwy i atrybuty stosują tekstowe kodowanie (w X.500 używany jest standard ASN.1)
3. LDAP jest posadowiony bezpośrednio na protokole TCP/IP, ominięto specyfikację całości protokołu OSI.
4. Prosty interfejs programowania (API); w efekcie prac nad LDAPem grupy programistów z University of Michigan opublikowano RFC 1823 ([8]), dokument definiujący zasady konstruowania API (interfejs X/OPEN XDS, preferowane API X.500 jest znacznie bardziej skomplikowane)
5. LDAP opiera się na X.500 w zakresie definicji usługi i rozproszonych operacji, jest specyfikacją protokołu dostępowego, nie kompletnej usługi katalogowej.

4. Wprowadzono pojęcie obszaru administracyjnego w celu usprawnienia zarządzania danymi; dane mogą być grupowane, w ramach wspólnych obszarów można stosować atrybuty zbiorowe.

Dalsze działania standaryzacyjne doprowadziły do rozbudowania w zakresie obsługi wielojęzyczności zasobów informacyjnych. Wersja '97 zawiera pojęcie kontekstu atrybutu. Jednym z zastosowań kontekstu jest rozróżnianie języka atrybutu. Użytkownik specyfikuje język dostępu i system, w miarę możliwości, zapewnia mu odpowiednią interpretację wartości atrybutu. Przewidywane jest użycie kontekstu domyślnego, który stosowany jest w przypadku, kiedy niemożliwe jest dostarczenie wartości dla wyspecyfikowanego kontekstu.

5. Rozwój protokołu LDAP

Protokół LDAP również rozwijał się na bazie doświadczeń z pierwszą jego wersją. Od 1996 roku trwały, w ramach grupy roboczej IETF ASID, prace nad kolejną edycją, zwana LDAP version 3. Podstawowe elementy nowego protokołu to:

1. Dostęp do funkcjonalności X.500'93; celem jest umożliwienie oprogramowaniu klienckiemu LDAP korzystania z nowej usługi.
2. Komponenty w zakresie bezpieczeństwa systemu; uwierzytelnianie stron komunikujących się i poufność wymiany informacji dzięki zastosowaniu protokołu SSL (*Secure Socket Layer*).
3. Mechanizm rozszerzalności; taka organizacja bazowego protokołu, by możliwe było dodawanie nowych operacji bez zmian w podstawowych modułach.
4. Odsyłacze (*referrals*); wbudowanie technik przekierunkowania klienta LDAP do innego serwera w celu realizacji zlecenia.

LDAP v. 3 nie wymaga zasobów X.500 dla swojego istnienia. Może być stosowany na dwa sposoby:

- jako uproszczony sposób dostępu do bazy X.500,
- jako mechanizm tworzenia serwerów LDAP, nie będących oczywiście serwerami X.500, ale ze strony użytkowej traktowanych jako abstrakcja serwisu X.500.

Omówione cechy protokołu LDAP v. 3 pokazują, że znacznie wzrasta jego funkcjonalność, co przyczynia się do rosnącej popularności. Właśnie z implementacjami tej wersji protokołu świat Internetu wiąże największe oczekiwania. Niezbędne dla efektywności usługi są nowe elementy: dostępność technik bezpiecznej komunikacji oraz możliwość połączenia i współpracy serwerów LDAP za pomocą odsyłaczy.

Zakres rozbudowy protokołu LDAP w pierwszym etapie nie objął takich funkcji jak operacje rozproszone, czy replikacja. W efekcie pojawiające się implementacje stosują swoje własne mechanizmy, na ogół bardzo podobne do wykorzystywanych w produktach X.500. Takie rozwiązanie prowadzi do niekompatybilności serwisów bazujących na oprogramowaniu różnych firm. Obecnie kontynuowane są prace nad rozbudową specyfikacji LDAPa.

6. X.500 a LDAP

Historia standardu X.500 i protokołu LDAP pokazuje, że LDAP rozwinął się jako protokół dostępowy do X.500. Potrzeba takiej specyfikacji wynikała z kłopotów, jakie napotkali autorzy interfejsów użytkowych do zasobów X.500. Ich implementacja w oparciu o rodzimy protokół X.500 DAP została oceniona jako trudna, a produkty bazujące na DAPie wymagały zbyt wiele zasobów. Cały standard X.500, typowy przykład rekomendacji OSI, świat Internetu uznał za przeciążony, skomplikowany, intensywnie wykorzystujący zasoby komputerowe. Produktom

serwery: poziomu krajowego oraz serwer Uniwersytetu Mikołaja Kopernika w Toruniu. Doświadczenia zdobyte w trakcie eksperymentu można podsumować następująco:

1. Translacja zasobów w formacie `Quipu` do postaci wymaganej przez serwis X.500'93 nie sprawia większych kłopotów.
2. Uzyskana w wyniku konwersji baza najprawdopodobniej (sądząc po szybkości przeszukiwania zasobów) ma mało efektywnie ustawione prawa dostępu do encji.
3. Ustalanie praw dostępu wymaga dogłębnej znajomości problemu, nie jest łatwe.
4. Współpraca poprzez odsyłacze (*referrals*) i łańcuchowanie (*chaining*) funkcjonuje prawidłowo.
5. Realizacja mechanizmu replikacji jest uciążliwa, konieczne są wzajemne uzgodnienia stron oraz wymagane jest zatrzymanie serwera w trakcie rekonfiguracji.
6. System, w testowanej postaci, wykazywał małą efektywność, okres oczekiwania na wyniki zleceń był zdecydowanie zbyt długi (może to wynikać nie z cech oprogramowania, lecz postaci bazy, którę stosowaliśmy do testów).

Obecnie przewidujemy kontynuacje działań związanych z oprogramowaniem `IC`. Planowanie jest wykorzystanie pakietu w wersji `ICR4` i modelu X.500'93 w usłudze X.500 prowadzonej na Uniwersytecie Mikołaja Kopernika w Toruniu. W szczególności interesować nas będą problemy ustalania praw dostępu i tworzenia domen administracyjnych.

Warto wspomnieć, że autorzy najnowszej wersji pakietu `ICR4.0` twierdzą, że przeprowadzone testy efektywnościowe wskazują znaczne udoskonalenie oprogramowania. M.in. operacje odczytu i wyszukania są około trzy razy szybsze niż w poprzedniej wersji, bardziej wydajny jest również LDAP. Podawane są także porównania w stosunku do wyników publikowanych przez firmę Netscape dla `Directory Server`'a – około dwukrotnie większa wydajność.

8. Oprogramowanie implementujące protokół LDAP

Pakiet `ldap-3.3`

Najpopularniejszym oprogramowaniem implementującym LDAP jest udostępniany bezpłatnie pakiet LDAP, napisany przez grupę z University of Michigan. Ostatnia edycja to `ldap-3.3`. Jest on również częścią składową dystrybucji Isode (oprogramowanie X.500, obecna wersja to `ICR4`). Implementacja ta, mimo numeracji 3.3, opiera się na standardzie LDAP v. 2, ale posiada wbudowane elementy obsługi współpracy serwerów oraz realizacji replikacji pomiędzy serwerami. Oprogramowanie `ldap-3.3` dostarcza serwer `ldapd`, biblioteki wspomagające oraz programy klienckie, służące do przeglądania i modyfikacji zasobów. Jest również możliwe uruchomienie samodzielnego serwera, zwanego `slapd` (*stand-alone* LDAP *daemon*), który zarządza własną bazą danych, wzorowaną na modelu X.500. Zasoby wykorzystywane przez `slapd` mogą mieć następującą postać:

1. LDBM – efektywna baza dyskowa, oparta na czterobajtowych unikalnych identyfikatorach, stosowanych do wskazywania konkretnych encji w zasobach; dopuszcza się stosowanie indeksów wygenerowanych dla wybranych atrybutów (w celu optymalizacji operacji przeszukiwania bazy).
2. SHELL – interfejs bazy danych do komend UNIXa czy skryptów powłoki, po odebraniu zapytania wykonywana jest odpowiednia komenda, lub skrypt.
3. PASSWD – baza oparta na pliku haseł w systemie UNIX.

udostępnianych obecnie w oparciu o oprogramowanie firmy Isode ICR3.2 (realizuje ono standard X.500). Podstawowym celem eksperymentu było stwierdzenie na ile proste jest przeniesienie istniejącej usługi X.500 oraz ocena kompatybilności serwisów obu typów.

Sama instalacja pakietu Netscape Directory Server jest stosunkowo prosta. Następnie należy za pomocą SuiteSpot'a przeprowadzić konfigurację. Wymaga ona znajomości zagadnienia obsługi zasobów katalogowych (dostarczana jest bogata dokumentacja). Serwer administracyjny może współpracować na podstawie protokołu LDAP z serwerami ldapd lub kontaktować się z lokalnie uruchamianym serwerem ns-slapd, który jest eksploatowany w sposób bardzo podobny do tego, z czym mamy do czynienia w pakiecie ldap-3.3. Serwer ns-slapd powinien zostać skonfigurowany odpowiednio do potrzeb środowiska. Przede wszystkim można rozbudować obowiązującą postać informacji umieszczanej w zasobach bazy danych, rozszerzyć klasy obiektów, czy typy atrybutów. Ta operacja realizowana jest w serwerze za pomocą zestawu formularzy. W ten sposób dodawane są definicje tzw. „polskich" klas obiektów i atrybutów (podobna była procedura postępowania w przypadku pakietu Quipu). Temat projektu realizacji usługi X.500 dla potrzeb środowiska Polski omawiają prace [10, 11, 12]. Directory server stosuje, podobnie jak ldap-3.3, LDAP *Data Interchange Format* (LDIF) w celu przedstawiania encji w zasobach katalogowych. Dotyczy to zarówno encji wprowadzanych do zasobów jak i formy ich prezentacji. Format LDIF pozwala również na przygotowanie danych do modyfikacji zasobów. Pliki w formacie LDIF mogą zostać przygotowane w dowolny sposób, chodzi tu o utworzenie odpowiednich zbiorów tekstowych. Warto zauważyć fakt, że wszystkie dane katalogowe są zapamiętywane wewnętrznie przy użyciu kodowania UTF-8, co oznacza, że pliki LDIF stosują ten typ kodów. Usługa katalogowa uruchamiana w Polsce musi zakładać umieszczanie w zasobach danych polskojęzycznych. Do tego celu należy wykorzystać tzw. znaczniki językowe (*language tags*), które mogą wystąpić po typie konkretnego atrybutu w linii pliku LDIF określającego wskazaną atrybutem *dn* encję. Zabronione jest natomiast stosowanie znaczników językowych dla jednoznacznych nazw obiektów. Właściwa nazwa encji musi być przedstawiona, podobnie jak to miało miejsce w zasobach X.500, jako jedna konkretna nazwa, nie są możliwe wielowartościowe *dn*'y rozróżniane poprzez język (taka technika została wprowadzona w standardzie X.500'97). O konsekwencjach tak przyjętego modelu pisaliśmy w pracach [10, 11] i w efekcie została zaprojektowana odpowiednia postać systemu. Rozwiązanie zaprezentowane we wskazanych opracowaniach może zostać przeniesione na płaszczyznę Netscape Directory Server'a. Z punktu widzenia wewnętrznej organizacji zasobów wymaga ono rozbudowania tablic klas obiektów oraz atrybutów, następnie w fazie wprowadzania i modyfikacji zasobów należy pamiętać o umieszczaniu w opisie encji polskich atrybutów. Zgromadzenie informacji w rodzimym języku to nie wszystko. Należy dysponować interfejsami użytkownika, które przedstawią wyszukiwane w bazie informacje we właściwej postaci, czyli obsłużą polskie atrybuty. Sam serwer nie zawiera modułów przeglądania danych, które zadowoliłyby polskiego użytkownika, również przeglądarka Netscape, nie jest w stanie jako odpowiedź udostępnionej operacji „Directory Search" zaprezentować wyniki w odpowiedniej formie. Zaimplementowany przez nas program stanowiący bramkę pomiędzy X.500 a WWW („spolszczony" Web500gw F. Richtera z Politechniki w Chemnitz) wykorzystuje protokół LDAP jako warstwę pośrednią do zasobów X.500. Zasada działania tego programu jest zgodna z zaleceniami tworzenia aplikacji LDAPowskich, jest oparta o LDAP API. Wydaje się, że dostosowanie tego programu do współpracy z serwerem ns-slapd byłoby stosunkowo łatwe.

Jeżeli zakładać przeniesienie istniejącej usługi X.500 z oprogramowania Quipu na Netscape Directory Server konieczne jest przełożenie zasobów z postaci Quipu do formatu stosowanego przez ten serwer. Translacja taka jest bardzo prosta, należy ją dokonać dwustopniowo: najpierw konwertujemy drzewiasto zlokalizowane dane Quipu do postaci pliku

Literatura

[1] Data Networks and Open System Communications: *Directory*, ITU-T Recommendations X.500-X.525

[2] D. Chadwick, *Understanding X.500. The Directory.* Chapman & Hall 1994 (http://www.salford.ac.uk/its024/X500.htm)

[3] D. Goodman, C. Robbins, *Understanding LDAP and X.500* (http://www.eema.org./understanding_ldap.html)

[4] S. Kille, *LDAP and X.500*, First published i Messaging Magazine, September 1996

[5] Raporty i prace na temat projektu X.500 w Polsce: http://ocelot.uni.torun.pl/raporty_pl.html

[6] W. Yeong, T. Howes, S. Kille. *X.500 Lightweight Directory Access Protocol.* RFC1487

[7] W. Yeong, T. Howes, S. Kille, *Lightweight Directory Access Protocol*, RFC1777

[8] T. Howes, M. Smith, *The LDAP Application Program Interface,* RFC1823

[9] *The LDAP Data Interchange Format (LDIF)* – Technical Specification, Filename: draft-ietf-asid-ldif-02.txt, 30.07.1997

[10] M. Górecka, T. Wolniewicz, *Dostosowanie bazy X.500 do specyfiki języka lokalnego*, materiały konferencyjne, Miedzeszyn'96

[11] M. Górecka, T. Wolniewicz, *Nazewnictwo obiektów w rozproszonej międzynarodowej bazie X.500*, maj 1997, materiały konferencyjne Miedzeszyn'97.

[12] M. Górecka, T. Wolniewicz, *Use of national languages in X.500 Directory*, listopad 1996, materiały konferencyjne Bled, Słowenia, konferencja robocza n.t. standardu Unicode.

[13] M. Górecka, T. Wolniewicz, *Najnowsze tendencje w dostępie do zasobów adresowo-informacyjnych — protokół LDAP a X.500*, kwiecień 1998, Poznań, materiały konferencyjne POLMAN'98.

Idea single-sign-on (SSO)

Idea SSO (ang. single-sign-on) polega na tym aby w sposób bezpieczny zidentyfikować i zweryfikować użytkownika w pojedynczym procesie komunikacji z systemem w czasie pierwszego logowania do systemu w danej sesji a następnie automatycznie zezwolić na dostęp tego użytkownika do zasobów zdefiniowanych w centralnej bazie. W ten sposób użytkownik w zakresie posiadanych praw dostępu (zdefiniowanych przez np. administratora bezpieczeństwa) po pozytywnym uwierzytelnieniu w czasie zalogowania do sieci uzyskuje w danej sesji dostęp do określonych komputerów, aplikacji, baz danych itp.

Oczywistym faktem jest, że w takim scenariuszu krytyczne jest dobranie takich mechanizmów bezpieczeństwa, które zapewnią, że uwierzytelnianie i autoryzacja – mimo, ze dokonywana „w imieniu" użytkownika będą odporne na rozmaite zagrożenia (np. podszywanie się, przechwytywanie sesji). Jest to możliwe tylko i wyłącznie przy zastosowaniu nowoczesnych i mocnych mechanizmów kryptograficznych

Metody realizacji SSO

Istnieje kilka metod takiego czy innego zrealizowania idei SSO. Można więc wyróżnić metody polegające na wykorzystaniu:

1. Skryptów na stacjach roboczych
2. Skryptów uwierzytelniających na serwerach
3. Tokenów i/lub informacji uwierzytelniających (ang. credentials)

Ad.1

Najprostszą metodą jest zastosowanie skryptów do logowania (ang. logon) zainstalowanych na stacjach dostępowych. Użytkownik loguje się do stacji dostępowej (siedząc przy klawiaturze stacji) a następnie wybiera z menu komputery bądź aplikacje, z którymi zamierza pracować. Skrypt wysyła odpowiedni identyfikator użytkownika oraz jego hasło do docelowego komputera czy aplikacji. Taki system jest łatwy w użyciu, nie wymaga żadnych zmian w systemach czy aplikacjach jednak posiada wady z punktu widzenia bezpieczeństwa: wiele haseł użytkowników jest składowanych w stacji dostępowej (np. PC) – częstokroć w postaci jawnej lub słabo zabezpieczonej, nie istnieje centralne miejsce administrowania hasłami, skrypty wymagają modyfikacji w sytuacji okresowych zmian haseł użytkowników.

Ad.2

Produkty z drugiej grupy nie mają większości wad rozwiązań z grupy pierwszej poprzez zastosowanie centralnego serwera uwierzytelniającego. Użytkownicy uwierzytelniają się jedynie do serwera centralnego, który potem inicjuje proces identyfikacji i weryfikacji użytkownika na odległych maszynach i do określonych aplikacji. Niektóre systemy SSO po prostu inicjują zastępczy proces logowania (ang. „proxy") na podstawie zdefiniowanej tablicy identyfikatorów i haseł użytkowników zapisanych na serwerze. Dane te mogą być szyfrowane i prawdopodobnie lepiej zabezpieczone niż na stacji roboczej – natomiast w dalszym ciągu wprowadza się użytkowników oddzielnie dla każdego systemu – oraz dodatkowo do serwera uwierzytelniającego.

Prawa dostępu dla użytkowników / grup użytkowników są kontrolowane z jednego miejsca (konsola Managera Bezpieczeństwa) podobnie jak poziom bezpieczeństwa komputerów UNIXowych w całej sieci. Manager Bezpieczeństwa posiada swą replikę.

Serwer obsługuje zarządzanie strukturą klucza publicznego (ang. PKI – Public Key Infrastructure) służącą do wykorzystania certyfikatów kluczy publicznych użytkowników jako informacji uwierzytelniającej (ang. credentials) w procesie identyfikowania i uwierzytelniania użytkowników.

Certyfikaty użytkowników mogą być przechowywane na dyskietkach w postaci zaszyfrowanych plików bądź na kartach inteligentnych. Dostęp do kluczy prywatnych użytkowników jest chroniony hasłem: statycznym lub co jest rekomendowane, hasłem dynamicznym systemu OTP sprzężonym z Managerem Bezpieczeństwa.

Usługi katalogowe sprzężone z PKI zapewniają ułatwioną dystrybucję i zarządzanie certyfikatami. (Użytkownik powinien mieć możliwość łatwego uzyskania swych „credentials" przy pomocy swego komputera dostepowego do sieci -np. desktop PC– a administrator możliwość np. sprawnego centralnego unieważniania certyfikatów użytkowników.

Jeśli Manager Bezpieczeństwa posługuje się strukturą PKI – powinien mieć możliwość współpracowania z certyfikatami wydanymi przez inne Urzędy ds. Certyfikatów (ang. Certification Authority).

Moduły Współpracy – aby system SSO mógł być szeroko zastosowany systemy operacyjne i aplikacje na komputerach objętych technologią SSO muszą zostać wyposażone w pewien sprzęg pozwalający na komunikację z Managerem Bezpieczeństwa oraz komunikację z użytkownikiem. Możliwość praktycznego wdrożenia systemu tkwi niejednokrotnie w ilości standardowych modułów pozwalających na komunikację z wieloma systemami i aplikacjami różnych producentów (np. bazy danych Oracle,Informix, Sybase, protokoły HTTP, telnet, systemy operacyjne – np. rozmaite odmiany UNIX-a). Moduły współpracy powinny zapewniać mocne uwierzytelnienie (OTP, two factor authentication itp.) Moduły komunikacji pośredniczą we współpracy z Managerem Bezpieczeństwa w komunikacji użytkownika z zasobami, do których posiada on zdefiniowane w centralnej bazie prawa dostępu.

Oprogramowanie stacji użytkownika – pozwala na bezpieczne poruszanie się po systemie objętym SSO. W takim razie powinno zapewnić szyfrowanie sesji, zabezpieczenie przed nieuprawnionym wykorzystaniem cudzych certyfikatów i kluczy, wykorzystanie podpisu cyfrowego w celu uwierzytelnienia komunikujących się procesów. Podstawową funkcją jest zapewnienie dostępu do komputerów i aplikacji w rozproszonym, heterogenicznym środowisku przedsiębiorstwa czy organizacji.

Narzędzia dostosowujące – nie ma systemów, które obejmowały by swymi możliwościami wszystkie protokoły, aplikacje czy systemy operacyjne jakie są lub będą stworzone. Szanujący się system SSO powinien posiadać narzędzia programowe do wykonywania we własnym zakresie kolejnych modułów współpracy zapewniających mocne uwierzytelnienie przy próbie dostępu oraz sprzęg ze środowiskiem SSO.

WYBRANE ASPEKTY PRAWNE, INSTYTUCJONALNE I ORGANIZACYJNE BEZPIECZEŃSTWA KRYPTOGRAFICZNEGO w RZECZYPOSPOLITEJ POLSKIEJ
(kontynuacja rozważań Seminarium MIEDZESZYN '97)

Mirosław Machalski

Biuro Bezpieczeństwa Łączności i Informatyki
Urzędu Ochrony Państwa
02-517 Warszawa, ul. Rakowiecka 2b, tel. 6013268, fax. 6014270

„Okres po Zimnej Wojnie charakteryzuje się rozproszeniem sił, niepewnością geopolityczną i zmianami technologicznymi. Rewolucja informacyjna ogarnia cały świat, powodując zmiany tak radykalne, jak te spowodowane opracowaniem bomby atomowej. Tak jak panowanie nad technologiami przemysłowymi stanowiło klucz do potęgi ekonomicznej i militarnej przez dwa ostanie wieki, tak panowanie nad bezpieczeństwem technologii informacyjnych będzie kluczem do potęgi w 21 wieku".

Kenneth A. Minihan
porucznik generał USAF
Dyrektor NSA (USA)

1. Wstęp

Wiek Informacji wiąże się z ogromnymi wyzwaniami i zagrożeniami. Rdzeniem ich są technologie, służące niezawodnej eksploatacji systemów i ochronie informacji. Jednakże same technologie nie wystarczą - musimy zmienić nasze tradycyjne podejście do bezpieczeństwa systemów informacyjnych. Oczekiwanie na kompleksowe uregulowanie prawne tej dziedziny działalności nie może doprowadzić do celu – jakim jest bezpieczeństwo teleinformacyjnego – strategiczne zadanie naszego wieku. Nie oznacza to, że popieramy jakiekolwiek działania pozaprawne, oznacza natomiast popieranie wszelkich działań poprawiających skuteczność ochrony informacji w systemach teleinformacyjnych.
Szczególnymi prawami rządzi się jednak kryptografia – jedna z metod ochrony informacji – zaliczona przez większość państw (w tym Polskę) do technologii „podwójnego przeznaczenia", na równi wręcz z materiałami promieniotwórczymi. Nic więc dziwnego, że główne wysiłki legislacyjne RP w dziedzinie bezpieczeństwa teleinformacyjnego skierowane są na procedury obrotu i stosowania kryptografii. Pozostałe aspekty – bezpieczeństwo elektromagnetyczne, transmisyjne, komputerowe i organizacyjno-fizyczne – regulowane są niejako „przy okazji".

Bardzo „cenna" z punktu widzenia kryptograficznej ochrony informacji jest ustawa z dnia 3 kwietnia 1993 r. o badaniach i certyfikacji wraz z Rozporządzeniem Rady Ministrów w sprawie zakresu i trybu stosowania przepisów o badaniach i certyfikacji do wyrobów produkowanych w kraju i importowanych wyłącznie na potrzeby obronności i bezpieczeństwa państwa, a także właściwości tych organów (Dz. U. Nr 80, poz. 370). Upoważnia ona do prowadzenia badań i certyfikacji wyrobów istotnych dla obronności i bezpieczeństwa państwa organy ustawowo umocowane w tej sferze.

Funkcjonuje szereg innych aktów prawnych rangi ustawy, regulujących (z mniejszą lub większą skutecznością) bezpieczeństwo teleinformacyjne – w tym kryptograficzne w niektórych dziedzinach działalności państwa. Do ustaw tych zaliczyć można np. ustawę z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników (Dz. U. 95.142.702 z dnia 12 grudnia 1995 r.).
Artykuł 15 1. tej ustawy stanowi, że: urzędy skarbowe obowiązane są do zachowania tajemnicy odnośnie do danych zawartych w dokumentacji, o której mowa w art. 13 ust. 1 (Dokumentacja związana z nadaniem NIP oraz aktualizowaniem danych zawartych w zgłoszeniach identyfikacyjnych...). O ile jednak mi wiadomo, system teleinformacyjny projektowany i budowany dla potrzeb ewidencji podatników, nie uwzględnia jeszcze (!) ochrony kryptograficznej.

Dosyć obiecująco wygląda przepis zawarty w art. 45 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883) który stanowi, iż minister właściwy do spraw administracji określi, w drodze rozporządzenia... podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Wyrażam przekonanie, że rozporządzenie to – budowane przecież współcześnie i bez żadnych ograniczeń – ma dużą szansę kompleksowego (zgodnego ze standardami europejskimi) uregulowania procedur bezpieczeństwa teleinformacyjnego obszernej i ważnej sfery działania państwa.

2. 2. Regulacje międzynarodowe.

Najistotniejszym dokumentem międzynarodowym – skutkującym w sferze bezpieczeństwa teleinformacyjnego (w tym oczywiście kryptograficznego) jest podpisana dnia 3 listopada 1994 r. przez Rząd Rzeczypospolitej Polskiej Umowa o Bezpieczeństwie z Paktem Północno Atlantyckim (NATO). Stosownie do postanowień tej umowy – decyzją rządową Urząd Ochrony Państwa przyjął funkcję tzw. Krajowej Władzy Bezpieczeństwa sfery cywilnej[3] państwa.
Jednym z ważniejszych i odpowiedzialnych zadań Krajowej Władzy Bezpieczeństwa jest zorganizowanie i utrzymanie bezpiecznego systemu teleinformacyjnego dla potrzeb przetwarzania, przechowywania i przesyłania klasyfikowanych informacji NATO na terenie naszego państwa.
Wiedza, umiejętności i doświadczenia, jakie uzyskujemy od Paktu w trakcie procesu akcesyjnego w tej dziedzinie – pozwalają na wysunięcie tezy, iż będziemy w stanie skutecznie przeciwdziałać się ujawnianiu informacji w specjalnych systemach teleinformacyjnych.

2. 3. Akty prawne wykonawcze.

W trzecim już (i wyrażam przekonanie, że ostatnim) obiegu uzgodnień międzyresortowych jest od dwóch miesięcy projekt Rozporządzenia Prezesa Rady Ministrów w sprawie określenia

[3] z wyłączeniem sfery militarnej, która pozostaje pod kontrolą resortu obrony narodowej

i importowanych wyłącznie na potrzeby obronności i bezpieczeństwa państwa, a także właściwości organów w tych sprawach (Dz. U. z dnia 13 lipca 1994 r.) w § 3, ust. 2 stanowi, że:
2. Badania i certyfikacja wyrobów o przeznaczeniu specjalnym w jednostkach podległych Ministrom Obrony Narodowej i Spraw Wewnętrznych mogą być dokonywane przez laboratoria i jednostki certyfikujące wskazane przez Ministrów, w porozumieniu z dyrektorem Polskiego Centrum Badań i Certyfikacji.

Na tej podstawie Minister Spraw Wewnętrznych – w porozumieniu z dyrektorem PCBC - Decyzją nr 1842/96 z dnia 23 września 1996 r. powołał Jednostkę Certyfikującą Urządzeń i Systemów Kryptograficznych oraz Kompatybilności Elektromagnetycznej w Biurze Szyfrów UOP[7] a także Laboratoria Badawcze) i upoważnił je badań i certyfikacji wyrobów o przeznaczeniu specjalnym.
Podpisana jest również (aczkolwiek jeszcze nie opublikowana) nowelizacja przytoczonego wyżej Rozporządzenia Rady Ministrów nadająca (obok MSW i MON) stosowne uprawnienia Szefowi Urzędu Ochrony Państwa – organowi właściwemu w sprawach bezpieczeństwa państwa i ochrony jego porządku konstytucyjnego.
Prowadzone są równolegle prace zmierzające do uruchomienia w Biurze Bezpieczeństwa Łączności i Informatyki UOP komórki organizacyjnej prowadzącej proces „certyfikacji personelu bezpieczeństwa teleinformacyjnego".

3. 2. Cele, zadania i organizacja Jednostki Certyfikującej BBŁiI UOP.

Zadaniem Jednostki Certyfikującej jest dokonywanie w sposób rzetelny, bezstronny, kompleksowy i poufny niezależnej oceny wyrobów produkowanych w kraju oraz importowanych głównie na potrzeby obronności i bezpieczeństwa państwa.

Celem jest świadczenie usług na poziomie odpowiadającym uznanym standardom krajowym i międzynarodowym, a także zdobycie zaufania i uznania odbiorców usług zarówno w stosunku do certyfikowanych wyrobów jak i Jednostki.

Swoistym gwarantem rzetelności i bezstronności prowadzonych działań certyfikacyjnych jest niekwestionowany, przewidziany w ustawie „interes" Urzędu Ochrony Państwa, związany z przeciwdziałaniem i zapobieganiem ujawnianiu tajemnicy, a więc – wprowadzaniem do stosowania wyłącznie urządzeń i systemów
o najwyższej, potwierdzonej jakości.

Potwierdzeniem kompetencji Jednostki Certyfikującej BBŁiI UOP są realizowane dla potrzeb rządowych systemy kryptograficzne.

Certyfikacja i badania prowadzone są według kryteriów oceny zabezpieczeń teleinformatyki (ITSEC) lub/i na zgodność z normami i standardami (np. MIL STD).

Jednostka Certyfikująca funkcjonuje w strukturze Biura Bezpieczeństwa Łączności i Informatyki Urzędu Ochrony Państwa. Zorganizowana jest zgodnie z wymaganiami normy PN-EN 45011:1993 i przewodnika ISO/IEC 28.

Struktura organizacyjna Jednostki Certyfikującej BBŁiI UOP zaprezentowana jest na poniższym rysunku

[7] Obecnie - od 20 grudnia 1996 r. - Biuro Bezpieczeństwa Łączności i Informatyki UOP

Certyfikatu udziela się, jeżeli:

- oceniany podsystem, urządzenie lub oprogramowanie zabezpieczające odpowiada zatwierdzonym i powszechnie uznanym kryteriom bezpieczeństwa;
- Szef Urzędu Ochrony Państwa stwierdzi, że w udzieleniu certyfikatu nie stoją na przeszkodzie interesy państwowe, w szczególności interesy obronności i bezpieczeństwa państwa.

3. 4. Wyciąg z „Księgi Jakości" Jednostki Certyfikującej BBŁiI UOP.

Certyfikat jest urzędowym dokumentem potwierdzającym:

- rezultaty oceny dokonanej przez niezależne Laboratorium Badawcze;
- poprawność stosowania przez Laboratorium kryteriów oceny

Certyfikat typu jest urzędowym dokumentem gwarantującym, że oceniane przez Laboratorium Badawcze urządzenie lub oprogramowanie (Przedmiot Oceny – PO) spełnia wybrane parametry związane z zabezpieczeniem systemów teleinformacyjnych. Certyfikat typu może potwierdzać zgodność technicznych rozwiązań z innymi – wskazanymi przez Wnioskodawcę – standardami, kryteriami, patentami i opisami, które jednak jest on obowiązany dostarczyć do Jednostki Certyfikującej BBŁiI UOP, jeśli nie są one w jej posiadaniu.

Certyfikat akceptacji jest urzędowym dokumentem gwarantującym, że oceniane przez Laboratorium Badawcze urządzenie lub oprogramowanie (Przedmiot Oceny – PO) spełnia wybrane wymagania związane z zabezpieczeniem systemów teleinformacyjnych. Miarą tej oceny jest:

- przyznanie PO określonego poziomu oceny, potwierdzenie funkcjonalności i minimalnej siły mechanizmów zabezpieczających (zgodnie z normami i przepisami krajowymi, wewnętrznymi i europejską normą ITSEC lub MIL-STD)

oraz

- określenie potencjalnej przydatności PO do zabezpieczania informacji wrażliwych, nieklasyfikowanych lub klasyfikowanych z punktu widzenia:

- uniemożliwienie pracy urządzenia (systemu) bez włączonej ochrony kryptograficznej a przynajmniej sygnalizowanie (akustyczne, optyczne) pracy bez zabezpieczeń;

Z drugiej strony – biorąc pod uwagę podmiot ochrony – informacje wrażliwe (nieklasyfikowane), z dużym prawdopodobieństwem założyć można, że wymagają one ochrony w stosunkowo krótkim przedziale czasu (od kilku minut do kilku lat)[8]. Biorąc również pod uwagę wartość tych informacji a także konieczne nakłady intelektualne i techniczne potencjalnego intruza – można przyjąć, że nie będzie w tym przypadku konieczne stosowanie szczególnie wyrafinowanych (a więc bardzo drogich) środków ochrony.
Niewątpliwie „rozrzut" wymagań użytkownika będzie bardzo duży – jednak dotychczasowe nasze doświadczenia pozwalają na pewne uogólnienia.
Przyjęto, że systemy takie:

- mogą wykorzystywać krajowe rozwiązania kryptograficzne (cywilne) lub obce, na które producent (dostawca) może uzyskać certyfikat typu lub akceptacji w Jednostce Certyfikującej BBŁiI UOP;
- powinny być w wysokim stopniu odporne na penetrację i modyfikację (dotyczy rozwiązań programowych);
- powinny być w akceptowalnym stopniu odporne na dekonspirację kluczy;
- muszą posiadać bezpieczny mechanizm dystrybucji kluczy generowanych pseudolosowo wykorzystując np. algorytmy klucza publicznego o akceptowalnie wysokich parametrach;
- powinny być wyposażone (lub mieć możliwość utworzenia) zabezpieczonego stanowiska zarządzania kryptografią.

4. Uwagi końcowe.

Kształtowanie świadomości konieczności chronienia zasobów informacyjnych w systemach teleinformacyjnych jest procesem bardzo trudnym, a jednocześnie - z natury rzeczy - nie objętym żadnymi uregulowaniami. Enigmatyczne zapisy ustawowe, obligujące kierownika każdej organizacji do chronienia wiadomości klasyfikowanych nie są jednoznaczne (dają się wręcz dowolnie interpretować) w stosunku do bezpieczeństwa teleinformacyjnego.
Narasta natomiast pełna świadomość faktu, że dysponowanie wydajnym i bezpiecznym systemem teleinformacyjnym stanowi klucz do sukcesu (vide motto przytoczone na początku dokumentu).Świadomość ta zaczyna się kształtować najszybciej w organizacjach dla których utrata lub zniekształcenie informacji oznacza poważną stratę ekonomiczną, prestiżową lub wręcz bankructwo.

Kryptografia stanowi najskuteczniejsze (jeszcze raz podkreślam, że nie samodzielne) narzędzie umożliwiające chronienie informacji w systemach teleinformacyjnych. Już tylko z tego powodu powinna być stosowana powszechnie. Powszechność stosowania nie może jednak oznaczać nieskoordynowanego, żywiołowego wręcz jej wdrażania i eksploatowania.
Nie przypadkiem przecież uznano kryptografię jako technologię „*dual use*".
Z drugiej strony sztuka nie polega na krytykowaniu i zabranianiu a na kreowaniu i tworzeniu. Korzystając z zaproszenia Dyrekcji NASK staramy się przybliżać i propagować wybrane doświadczenia i metodykę systemowych zastosowań kryptografii.

[8] dla porównania – informacje TAJNE wymagają skutecznej ochrony przez okres co najmniej 20 lat

STRATEGIA ROZWOJU NETII POPRZEZ WSPÓŁPRACĘ Z INNYMI PODMIOTAMI

Roman Jarocki

Netia Telekom S.A., 02-822 Warszawa, ul. Poleczki 13
e-mail: Roman_Jarocki@netia.pl

Aktualną sytuację na rynku telekomunikacyjnym można opisać następująco:

- TPSA - silny monopolista (7,5 mln abonentów (98%), działalność we wszystkich segmentach rynku, ponad 90% generowanego przychodu z rynku, możliwość kros-subsydiowania usług)
- 48 lokalnych operatorów telefonicznych, 68 koncesji, łącznie 115 – 150 tys. abonentów (2% liczby wszystkich abonentów sieci stacjonarnych)
- 300 operatorów sieci transmisji danych i internetu
- trzech operatorów telefonii komórkowej
- w przyszłym roku przyznanie koncesji na świadczenie usług międzymiastowych
- do 2003 monopol TPSA na telefoniczne usługi międzynarodowe

Pytanie: kto, oprócz TPSA, może sobie pozwolić na samotne działanie na tym rynku?

W ciągu ostatnich lat daje się zauważyć szereg pozytywnych zjawisk:

- Postępująca konsolidacja rynku operatorów lokalnych (Netia, PTO, Telefonia Lokalna, Telefonia Polska Zachód, Elektrim)
- Postępująca współpraca operatorów internetu
- Współpraca operatorów z Polską Izbą Informatyki i Telekomunikacji

Netia wypracowała strategię współpracy, która opiera się na następujących filarach:

- współpraca z administracją państwową i samorządową
- współpraca z operatorami
- współpraca z producentami i dostawcami sprzętu
- współpraca z integratorami systemów
- współpraca z instytucjami badawczo-rozwojowymi
- współpraca z Polską Izbą Informatyki i Telekomunikacji
- współpraca ze strategicznym akcjonariuszem - Telią AB

dostępowymi i zorganizowaną profesjonalną organizacją sprzedaży. Z kolei liczni klienci Netii potrzebują profesjonalnych usług w zakresie transmisji danych i dostępu do internetu.

Istnieje również możliwość efektywniejszego wykorzystania posiadanej infrastruktury oraz realizacji wspólnych przedsięwzięć. Taka współpraca ma miejsce, w niektórych przypadkach już od kilku lat, ale potencjalne możliwości są dużo większe.

Operatorzy telefonii komórkowej

Zgodnie z podaną w prasie informacją o decyzji NSA operatorzy GSM mogą łączyć swoje sieci z operatorami lokalnymi bez pośrednictwa TPSA. Otwiera to różnorakie możliwości wspólnego promowania usług, kształtowania taryf za ruch itp.

Operatorzy telewizji kablowej

W Polsce, jak wszędzie na świecie, operatorzy telewizji kablowej są zainteresowani rozszerzaniem zakresu świadczonych usług o telefonię i dostęp do internetu. Możliwości w tym zakresie są w Polsce ograniczone ze względu na politykę przyznawania jednej koncesji na dany obszar. Ze względu na komplementarną pozycję na rynku operatorów telewizji kablowej w stosunku do operatorów telefonii lokalnej, pojawia się szereg możliwości współpracy:

- możliwość wzajemnego świadczenia usług
- możliwość wykorzystania posiadanej infrastruktury
- możliwość wspólnych przedsięwzięć

Współpraca z producentami i dostawcami sprzętu

Ze względu na gwałtowny rozwój technologii i liczne nowe możliwości techniczne i usługowe sprzętu oferowanego na rynku oraz demonopolizację rynków telekomunikacyjnych na świecie i pojawienie się wielu zupełnie nowych podmiotów (często nie mających doświadczenia) na rynku usług telekomunikacyjnych, zauważa się wyraźną ewolucję producentów różnych urządzeń i systemów telekomunikacyjnych w kierunku „od dostawców do doradców". Dzisiaj większość liczących się producentów różnych rozwiązań telekomunikacyjnych ma w swoich strukturach grupy zajmujące się doradztwem, zwłaszcza nowym operatorom, jak sobie radzić w warunkach silnej konkurencji. Znajomość kierunków rozwoju technologii jest dla operatorów niezbędna do zajęcia konkurencyjnej pozycji na rynku.

Współpraca z integratorami systemów

Jest rzeczą powszechnie znaną, że w warunkach silnej konkurencji największe szanse na osiągnięcie sukcesu mają te firmy, które najlepiej będą w stanie zaspokoić potrzeby klienta. Dzisiejszego klienta w coraz mniejszym stopniu interesuje usługa telekomunikacyjna jako taka, jest raczej zainteresowany sprawnym funkcjonowaniem aplikacji informatycznych wykorzystujących warstwę telekomunikacyjną. W związku ze zbieżnymi kierunkami rozwoju informatyki i telekomunikacji, coraz większą rolę w zaspokajaniu potrzeb telekomunikacyjnych klientów będą odgrywali ci integratorzy systemów, którzy będą w stanie kompleksowo zaoferować zintegrowane rozwiązania informatyczno-telekomunikacyjne.

Internet - projekt pilotowy w Otwocku

Marcin Rączkiewicz
Netia Telekom S.A. ul. Poleczki 13, 02-822 Warszawa
E-mail: Marcin_Rączkiewicz@netia.pl

WSTĘP

Polski rynek telekomunikacyjny powoli otwiera się na konkurencję, choć tempo to jest dalekie od oczekiwań zarówno klientów jaki i prywatnych operatorów. Nowopowstały operator telekomunikacyjny może torować sobie miejsce na rynku poprzez trzy kluczowe czynniki:

- Zakres świadczonych usług;
- Sposób obsługi klienta;
- Cena.

Wraz ze wzrostem Netii, z rozszerzeniem się obszaru działalności firmy, z budowaniem linii i przyłączaniem kolejnych klientów Netia stara się oddziaływać na wszystkie te czynniki. Jeśli chodzi o cenę to Netia wprowadziła już dość dawno możliwość wyboru taryfy dla swoich abonentów. W kwestii obsługi klienta Netia od samego początku przywiązywała wagę do tego zagadnienia. Abonenci mieszkaniowi są obsługiwani w biurach obsługi klienta, które znajdują się w miejscach, gdzie budowana jest sieć Netii, a więc w pobliżu instalowanych telefonów. Jest tam możliwość zawarcia umowy na abonament telefoniczny, można dowiedzieć się o dodatkowych usługach i promocjach czy zgłosić reklamacje. Abonenci biznesowi mogą te sprawy załatwić bezpośrednio w biurze obsługi klienta lub dowiedzieć się o nowych propozycjach firmy za pośrednictwem przedstawicieli handlowych, którzy zaproponują i doradzą rozwiązanie właściwe dla danej firmy.

W zakresie oferowania usług dodatkowych Netia świadczyła do tej pory głównie usługi związane z telefonią a więc:

- Dodatkowe usługi telefoniczne (oczekiwanie na połączenie, usługa „nie przeszkadzać", ograniczenie połączeń wychodzących, połączenie trójstronne, odczyt licznika, identyfikacja wywołań złośliwych, itd.);
- Gamę usług związanych z ISDN;
- Usługę CENTREX czyli usługi centrali abonenckiej dla klienta posiadającego klika lokalizacji na terenie danego miasta.

Świadczone są również usługi związane z zestawianiem linii dzierżawionych punkt- punkt.

W chwili obecnej Netia rozszerza zakres usług jaki świadczy poprzez współpracę z NASK. Za jego pośrednictwem Netia będzie zapewniała dostęp do sieci Internet oraz dostęp do sieci transmisji danych. Zakres oferowanych usług będzie obejmował wszystkie usługi świadczone dotąd przez NASK, są to w głównej mierze:

- dostęp do sieci Internet (włącznie z usługami obejmującymi konfigurację IP, DNS, rejestracja domen, przydział kont, tworzenie stron WWW, itp.);
- dostęp do sieci Frame Relay;
- dostęp do sieci X.25;
- instalacja i konfiguracja sieci u klienta (włącznie z dostawą sprzętu).

przedstawiciele handlowi. Informacja o uruchomieniu pilotowego dostępu do sieci Internet została przekazana listownie przez Netię wszystkim jej abonentom. Abonenci biznesowi z którymi regularny kontakt utrzymują nasi przedstawiciele handlowi zostali o tym poinformowani bezpośrednio. Dziennie podpisuje się kilka umów. Po podpisaniu umowy jest ona przekazywana do NASKu celem uruchomienia usługi: zestawienia sprzętu, skonfigurowania sieci, stworzenia konta. Równolegle Netia zestawia odpowiednie łącza dostępowe, jeśli zachodzi taka potrzeba. Po przetestowaniu możliwości poprawnego świadczenia usługi NASK wysyła do Biura Obsługi Klienta informację "Gotowe do usługi". Biuro Obsługi Klienta powiadamia abonenta o rozpoczęciu świadczenia usługi.

Istnienie nowoczesnej sieci limituje do minimum powody do reklamacji: gdyby jednak zaistniały powody do uzasadnionej reklamacji (z powodu złej jakości usługi, czy z powodu złego naliczenia rachunku) to zostaną one przyjęte przez lokalne biuro obsługi klienta Netii i załatwione na miejscu. W ten sposób klient nie musi kontaktować się bezpośrednio z NASK, który skoncentruje się na sprawach związanych z utrzymaniem i rozbudową swojej sieci oraz techniczną stroną obsługi klientów.

DALSZE KROKI

Projekt pilotowy w Otwocku po jego zakończeniu zostanie przekształcony w regularne świadczenie usług a następnie rozszerzany na tereny wszystkich obszarów licencyjnych Netii. Wraz z uruchomieniem działalności komercyjnej klientom zostanie zaproponowana możliwość skorzystania z pełnego wachlarza usług NASK na wszystkich obszarach licencyjnych Netii.

Okres trwania projektu pilotowego umożliwi obu firmom ostateczne dopracowanie procedur współpracy oraz nabycie przez strony doświadczeń potrzebnych do świadczenia usług na zasadach komercyjnych.

PODSUMOWANIE

Obecne duże i niesłabnące zainteresowanie siecią Internet w Polsce nadal nie jest odpowiednio zaspakajane. Wspólna oferta Netii i NASKu stanowi odpowiedź na istniejące zapotrzebowanie w dziedzinie dostępu do sieci Internet i transmisji danych.

MAN Łódź, RSK Śląsk), telenauczaniem (MAN Gdańsk). Eksperymenty te zaprezentowane były na konferencji i wystawie POLMAN'98.

2. Charakterystyka sieci POL-34

Budowę naukowej sieci ATM oparto na sieci telekomunikacyjnej TEL-ENERGO. TEL-ENERGO jest operatorem usług telekomunikacyjnych dla branży energetycznej, ale działa również na rynku komercyjnym. Sieć telekomunikacyjna TEL-ENERGO wykorzystuje podwieszone do linii wysokiego napięcia kable światłowodowe, zarówno w tak zwanej sieci bazowej energetyki (220kV oraz 400kV) jak i sieciach regionalnych budowanych przez zakłady energetyczne. Struktura tej sieci obejmuje systemy PDH 8 Mb/s i 34 Mb/s oraz systemy SDH 155 Mb/s i 622 Mb/s. Dostępne są również włókna światłowodowe. Istniejący aktualnie stan tej sieci i planowany na 1998 rok jej rozwój w zakresie światłowodów i urządzeń (tym SDH 2,4 Gb/s) stanowi realną możliwość obsługi wymagań całego środowiska naukowego.

Założono trzyetapową budowę sieci POL-34:

etap I (97.07.01 – 97.12.31) - testowej eksploatacji sieci,
etap II (98.01.01 – 98.08.31) - operacyjnego działania i rozbudowy sieci,
etap III (98.09.01 – 99.03.31) - docelowej struktury sieci.

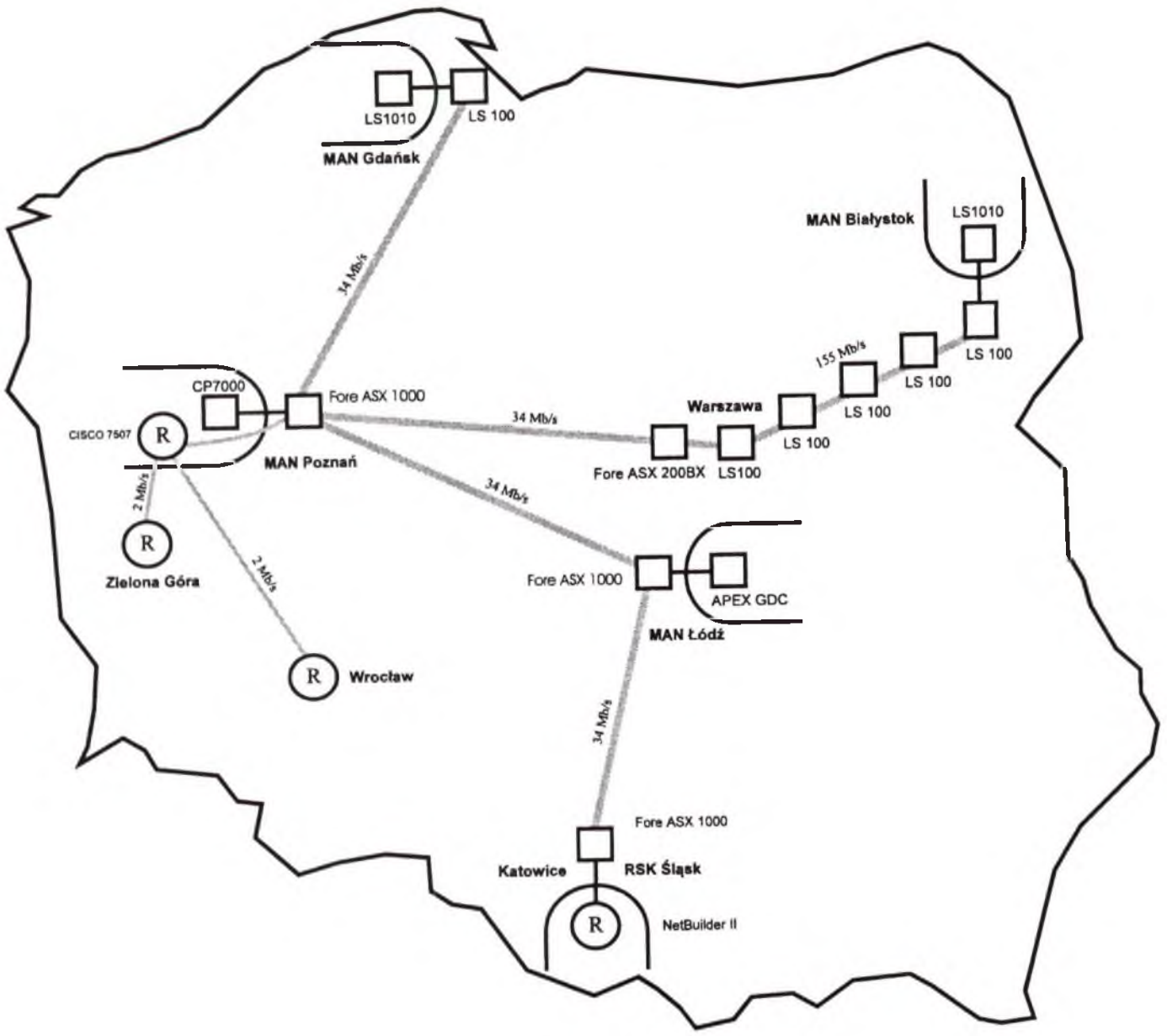
Zakończony w ubiegłym roku I etap budowy sieci POL-34 umożliwił połączenie następujących MAN-ów (rys.1 - stan aktualny na 30.03.98r.):

- Gdańska, Poznania, Warszawy, Łodzi i Katowic kanałami 34 Mb/s a także Białegostoku światłowodami i urządzeniami ATM 155Mb/s przez sieć TEL-ENERGO,
- Wrocławia kanałem 2 Mb/s przez sieć PKP,
- Zielonej Góry kanałem 2 Mb/s z CIR 64 Mb/s poprzez sieć POLPAK-T.

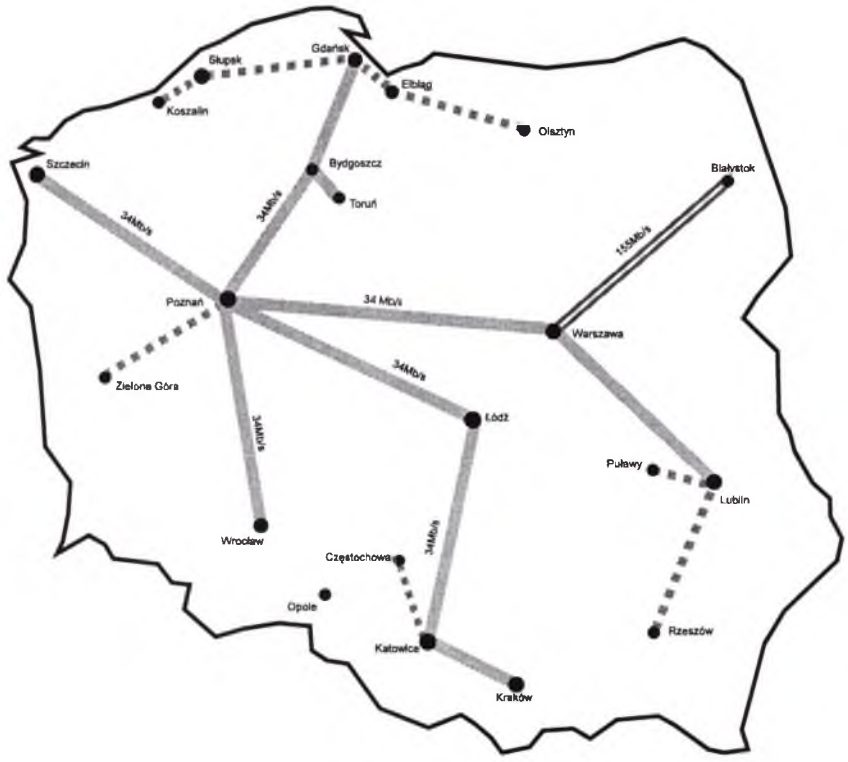
Zestawiona sieć posiada więc siedem węzłów zlokalizowanych w miastach biorących udział w projekcie. W każdym z węzłów zainstalowany jest brzegowy przełącznik ATM wyposażony w interfejsy do połączenia z innymi węzłami sieci krajowej i z siecią miejską. Urządzenia są zlokalizowane w obiektach Polskich Sieci Elektroenergetycznych. Wyjątkiem jest Wrocław i Zielona Góra, w których w związku z rodzajem przyłącza do sieci krajowej (kanał 2Mb/s) nie jest potrzebny przełącznik ATM.

W każdym z miast przełącznik ATM sieci krajowej jest połączony z przełącznikiem ATM sieci miejskiej łączem światłowodowym jednomodowym 155 Mb/s. Do przełączników sieci miejskiej dołączone są rutery sieci miejskich, superkomputery i serwery pracujące w tych sieciach. Uzyskano heterogeniczną strukturę sieci ATM (rys.2).

Początkowo jako węzły brzegowe sieci miejskich wykorzystano urządzenia z MAN-ów lub wypożyczone przez firmy ATM, Solidex, 3COM. W kręgosłupie sieci pracowały przełączniki: Fore ASX200BX, CISCO LS100 i 3COM Access Builder9600. Współpracowały one z różnymi przełącznikami sieci miejskich: CP7000 (3COM) APEX GDC, L1010 (CISCO). Mimo stabilnej pracy sieci, ze względu na ułatwienia w zarządzaniu oraz zwiększenie stopnia niezawodności, w końcu 1997 roku MAN-y biorące udział w inicjatywie POL-34 postanowiły zakupić jednolite wyposażenie brzegowe na stykach z innymi operatorami. W wyniku przetargu wybrano: przełączniki ATM Fore ASX1000 i rutery CISCO 7507. Urządzenia te zostały zainstalowane w Poznaniu, Łodzi i Katowicach.



Rys.2 Stan aktualny instalacji naukowej krajowej sieci ATM 34 Mb/s (etap I)



Połączenia 34 Mb/s w sieci SDH TEL-ENERGO

Połączenia światłowodowe dzierżawione od TEL-ENERGO

Połączenia 2 Mb/s w sieci TEL-ENERGO

Rys.4 Struktura połączeń fizycznych krajowej sieci ATM 34/155 Mb/s (etap II)

3. Usługi w sieci POL-34

Inicjatywa budowy sieci POL-34 jest integralnie związana z rozwojem nowych usług sieciowych dla środowiska naukowego. W ramach usług tradycyjnego dostępu do Internetu możliwe stało się uruchomienie procedur rozproszonego W3cache, wirtualnego serwera FTP, a także możliwe będzie stworzenie sieci serwerów bibliotecznych, sieci wideokonferencji, itp. W ramach usług szerokopasmowych możliwe staną się pilotowe realizacje usług związanych ze zdalnym nauczaniem, telediagnostyką (np. medyczną), dostępem do rozproszonego laboratorium obliczeń dużej mocy (np. metakomputer widziany jako klaster komputerów dla obliczeń wsadowych) i magazynów danych wraz z ich wizualizacją (np. GIS-owskich, meteorologicznych). Analiza wymagań komunikacyjnych zaawansowanych usług szeroko-pasmowych i przetwarzania rozproszonego nie pozostawia jednak wątpliwości, że w sieci ATM 34 Mb/s można co najwyżej przygotować i przetestować narzędzia i procedury. Natomiast wdrożenie i normalna eksploatacja tych usług w sieci wymagać będzie przepustowości i utrzymania określonych parametrów jakości usług, które mogą być spełnione przez łącza ATM 155 Mb/s, 622 Mb/s a nawet 2,4 Gb/s.

MAN-y dysponujące dostępem do sieci POL-34 postanowiły wykorzystać pasmo 34 Mb/s w pierwszym rzędzie dla:

- uzyskania światowego poziomu tradycyjnych usług Internetu, w ramach którego zorganizowano sieć połączeń krajowych i sieć dla połączeń zagranicznych,
- prowadzenia eksperymentów z usługami szerokopasmowymi i przetwa-rzaniem rozproszonym.

Poszczególne usługi sieci POL-34 dostępne z poziomu IP i ATM są zorganizowane w sieci wirtualne wykorzystujące kanały PVC o określonej przepustowości i kategorii usług. Wirtualna sieć połączeń krajowych do Internetu (krata, każdy z każdym o łącznej przepustowości z danego MAN-u
4 Mb/s) zbudowana jest na kanałach z usługą UBR. Wirtualna sieć połączeń zagranicznych (dedykowanych do punktu styku z operatorem między-narodowym o przepustowościach równych przepustowości w kanale zagranicznym dla danego MAN-u) zbudowana jest na kanałach z usługą CBR. Planowana wirtualna sieć dla połączeń multicastowych na kanałach 4-18 Mb/s z usługą VBR, natomiast sieć wirtualna połączeń między poszczególnymi komputerami SGI (Gdańsk, Łódź, Poznań, Wrocław, Szczecin), CRAY (Poznań, Warszawa), SP2 (Gdańsk, Poznań, Wrocław, Kraków) na kanałach o przepustowościach od 6-20 Mb/s z usługą VBR.

Prowadzone w sieci POL-34 eksperymenty z przetwarzaniem rozproszonym i zdalną wizualizacją obliczeń wykazały potrzebę dostępu do sieci o większej przepustowości. W celu przetestowania przygotowanych usług i sprawdzenia szybszych rozległych sieci ATM. MAN-y uczestniczące w inicjatywie POL-34 wspólnie z TEL-ENERGO zbudowany równolegle działającą sieć ATM 155 Mb/s prezentowaną na wystawie POLMAN'98. Jest ona opisana w dalszej części artykułu.

Środowiska naukowe dla prowadzenia właściwego, na poziomie światowym, procesu badawczego i dydaktycznego będą musiały więc dysponować podobną do światowej infrastrukturą. W warunkach polskich będzie ona jednak wynikiem kompromisu między potrzebami merytorycznymi a możliwościami finansowymi. Sieć POL-34 jest obecnie przykładem takiego kompromisowego rozwiązania.

7. Koncepcja sieci POL-34 zakłada stosowanie inżynierii ruchu w sieci, co zapewni efektywność i niezawodność jej działania.

Środowiska naukowe dla prowadzenia właściwego, na poziomie światowym, procesu badawczego i dydaktycznego będą musiały więc dysponować podobną do światowej infrastrukturą. W warunkach polskich będzie ona jednak wynikiem kompromisu między potrzebami merytorycznymi a możliwościami finansowymi. Sieć POL-34 jest obecnie przykładem takiego kompromisowego rozwiązania. Aktywność badawcza środowiska naukowego będzie jednak wymuszała użycie sieci o większych przepustowościach.

Kodowanie kanału wizyjnego dla celów wideokonferencyjnych w ISDN/LAN, zgodnie ze standardami H.320/H.323, opisane zostało w zaleceniach H.261/H.263. Dotyczą ono generalnie kodowania sygnału o standardach telewizyjnych w kanałach o przepływności (1÷30) x 64 kbit/s. Wejściowy obraz zmienia się z prędkością około 29,97 ramek na sekundę (30000/1001), kodowane są trzy komponenty: luminancja i dwie składowe różnicowe koloru (Y, C_B i C_R, czerni odpowiada wartość 16, bieli 235). Analogowy sygnał wizyjny próbkowany jest z założeniem utraty informacji w dwóch formatach:

- CIF (*Common Intermediate Format*), w którym liczba linii obrazu wynosi 288 dla luminancji i 144 chrominancji, przy 352 punktach w linii dla luminancji i 176 dla chrominancji;
- QCIF (*Quarter CIF*), w którym liczba linii obrazu wynosi 144 dla luminancji i 72 chrominancji, przy 176 punktach w linii dla luminancji i 88 dla chrominancji.

Stosuje się ustawienia, umożliwiające opuszczanie 0, 1, 2 lub 3 ramki. Kodek H.261 projektowany był z myślą o sieci ISDN, gdzie połączenia wykonywane są w trybie komutacji kanałów, tak że na jego wyjściu informacja przygotowana jest do transmisji o stałej przepływności binarnej (ang. *Constant Bit Rate*). W skład kodera wideo H.261/H.263 wchodzą bloki predykcji, transformacji i kwantyzacji. Ogólna zasada kodowania polega na redukcji redundancji przestrzennej informacji i przesyłaniu tylko różnic pomiędzy obrazami, pojawiającymi się w kolejnych ramkach. Operacja powyższa wykonywana jest w dwóch krokach:

- kompresja *intraframe* wewnątrz segmentów 8x8 z wykorzystaniem dwuwymiarowej transformacji kosinusowej. Wartości wyjściowe są następnie kwantowane, z możliwością zmian współczynnika kwantowania;
- kompresji *interframe* dotyczącej różnic pomiędzy makroblokami w kolejnych ramkach obrazu. W tym trybie wykonywana jest również opcjonalna kompensacja ruchu, która polega na przesyłaniu tylko różnic przesunięć danego makrobloku w poziomie i pionie.

Rozwinięciem powyższego jest schemat kodowania opisany w zaleceniu H.263, które bazuje na H.261, lecz wprowadza możliwość negocjacji czterech parametrów dla poprawienia wyników kompresji (ang. *unrestricted motion vestor, syntax-based arithmetic coding, advanced prediction, PB-frames*). Do wad powyższych technik kodowania można zaliczyć próbkowanie w stosunku 4:1:1 (luminancja:chrominancja:chrominancja) dla składowych luminancji i chrominancji (kodery M-JPEG i oparte o transformację falkową (ang. *wavelets*) wykorzystują stosunek 4:2:2 (luminancja:chrominancja:chrominancja)). Dodatkowo dzielenie obrazu na bloki i makrobloki, powoduje powstawanie charakterystycznych zakłóceń, które są łatwo wychwytywane przez oko ludzkie, szczególnie w przypadku powiększania obrazu. Również fakt, że obraz nie jest komprymowany w całości, lecz przy pomocy tworzonych ramek I (ang. *Intra frames*), P (ang. *Predictive*) i B (ang. *Bi-direction*), w ramach tworzonych bloków wewnątrz obrazu, powoduje, że utrata/opóźnienie pakietów podczas transmisji lub szybka zmiana ekspozycji obrazu objawia się znacznym pogorszeniem jakości. Powyższe błędy są odbierane w postaci skwantowanego obrazu w ramach bloków (*pixelization*) i pogorszenia ostrości.

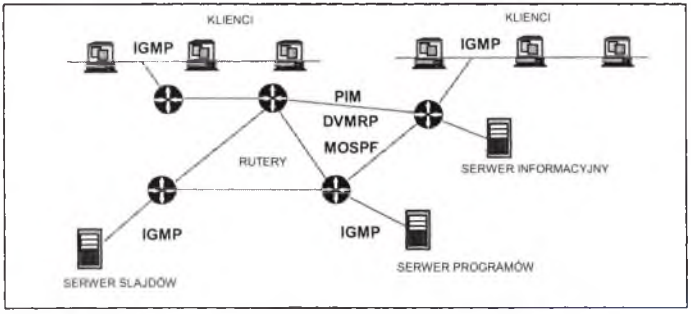
Do innych, często stosowanych, standardów kodowania sygnału wizyjnego dla potrzeb transmisji w sieciach LAN/WAN zaliczyć można:

- MPEG-1 Video, którego działanie jest podobne do kodeka H.261;
- M-JPEG, który w procesie komprymacji wykorzystuje dyskretną transformatę kosinusową (DCT), a jako informację wejściową wykorzystuje cały obraz. Dostrzegalne zakłócenia objawiają się w postaci linii i bloków;
- Indeo - standard zaproponowany przez firmę Intel;
- transformacja falkowa obrazu (ang. *wavelets*) - wykorzystująca bi-ortogonalną transformację całego obrazu. Ten schemat kompresji jest obecnie nowością i trudno znaleźć oprogramowanie realizujące funkcję kodera i dekodera.

podsieci a adres 224.0.0.2 oznacza wszystkie rutery w podsieci. Wykorzystanie adresów klasy D w transmisji rozsiewczej jest zdefiniowane w RFC 1112. Adres rozsiewczy pełni rolę kanału w systemach transmisji wizji i fonii. Zazwyczaj wizja i fonia nadawana jest na różnych adresach rozsiewczych. Rolę multipleksera różnych sygnałów wizji i fonii w jednym kanale pełni protokół UDP z różnymi numerami portów. Zasięg propagacji transmisji jest ograniczony parametrem TTL (*ang. Time To Live*) arbitralnie ustalanym dla każdego nadajnika. TTL jest zmniejszane po przejściu przez każdy z ruterów. TTL równe jeden oznacza, że transmisja jest ograniczona do lokalnego segmentu sieci. Dla systemów dynamicznie przydzielających adresy rozsiewcze zaleca się następujący podział:

- 224.0.1.0 - 238.255.255.255 mają nieograniczony zasięg (TTL = 255),
- 239.0.0.0 - 239.255.255.255 używane są na ograniczonym obszarze (np. jednego kraju),
- 239.192.0.0 - 239.252.255.255 mogą być używane na obszarze jednej organizacji,
- 239.253.0.0 - 239.255.255.255 mają zasięg lokalny.

W cytowanym dokumencie RFC 1112 zdefiniowany jest sposób odwzorowania adresów IP na adresy sieci Ethernet, FDDI i Token Ring. W sieci Ethernet przyjmuje się prefix adresu MAC równy 0x01005E i 23 najmłodsze bity adresu IP odwzorowuje się na 23 bity najmłodsze bity adresu MAC (np. 239.0.15.1 = 0xEF.0x00.0x0F.0x01 --> 0x01005E.000F01). Dzięki rozróżnieniu kanałów w warstwie drugiej możliwe jest sterowanie strumieniami również w sieciach lokalnych opartych o przełączniki Ethernet'u.



Rys. 2. Sieć z protokołami rozsiewczymi

W odróżnieniu od transmisji punkt-punkt w sieci pakietowej w transmisji rozsiewczej stroną inicjującą jest odbiorca informacji. Strumień danych jest wysyłany do klienta po złożeniu przez niego zamówienia na konkretny kanał rozsiewczy. Aby zamówienie zostało zrealizowane muszą być spełnione następujące warunki:

- klient musi znać parametry pożądanego kanału (adres rozsiewczy, port UDP, protokół SDR, serwer informacyjny),
- klient wysła do rutera informację o zapotrzebowaniu (protokół IGMP (ang. Internet Group Management Protocol)),
- w sieci musi być aktywny jeden z protokołów wyboru trasy (*ang. routing*) dla adresów rozsiewczych (DVMRP (*ang. Distance Vector Multicast Routing Protocol*), MOSPF (*ang. Multicast Open Shortest Path First*) lub PIM (*ang. Protocol Independent Multicast*)).

Schemat prostej sieci z zaznaczonymi protokołami stosowanymi w sieci rozsiewczej przedstawiono na rysunku 2.

Server i *IP/TV Viewer* mogą odpytywać tylko jeden podstawowy i zapasowy *IP/TV Program Guide*, o tyle jeden *IP/TV Program Guide* może obsługiwać wiele *IP/TV Server'ów*. Również użytkownicy pracujący z *IP/TV Viewer*, mogą oglądać treści pochodzące z wielu *IP/TV Server'ów*, które zostały wskazane przez skonfigurowany serwis *IP/TV Program Guide*. Dodatkowo w przypadku połączenia sieci lokalnej z usługami rozsiewczymi sieci MBone, możliwe jest skonfigurowanie *IP/TV Program Guide* tak, by możliwe było dołączanie do listy programowej sesji *Multicast Backbone*. Oprogramowanie *IP/TV* współpracuje ze standardami Lawrence Berkeley Labs (LBL) reprezentowanymi w postaci oprogramowania VIC 2.7, dla kodowania H.261 części wizyjnej w strumieniu rozsiewczym i VAT 4.0 dla części audio. Sesje MBone są anonsowane z wykorzystaniem narzędzia ***sdr***, pochodzącego z University College London (UCL), które po uruchomienie rozsyła zawiadomienia o sesji co około 5 minut.
Do podstawowych funkcji *IP/TV Program Guide* zaliczyć należy:

- definiowanie serwerów, które emitują programy z pamięci masowych lub na żywo z dołączonych kamer;
- zarządzania (towrzenie/edycja/kasowanie) kanałami telewizyjnymi, w ramach których emitowane są kolejne programy lub sygnał audio/wideo na żywo;
- zarządzanie programami (towrzenie/edycja/kasowanie), które emitowane są w określonym czasie i w pętli ciągłej w ramach zdefiniowanych kanałów;
- programowanie nagrań treści programów emitowanych na żywo na wskazanym serwerze IP/TV;
- konfigurowanie transferów FTP pomiędzy *IP/TV Program Guide* i *IP/TV Server*, które pozwalają na rozsyłanie programów pomiędzy serwerami, z wykorzystaniem protokołu ftp;
- programowanie sesji *SmallCasting IP/TV*, które umożliwiają rozsyłanie programów pomiędzy *IP/TV Server'ami*, w przypadku gdy są one dołączone do ruterów nie przenoszących *multicastów*;
- udostępnienie opcji *Question Manager*, pozwalającej na interakcje słuchaczy z prowadzącym wykład;

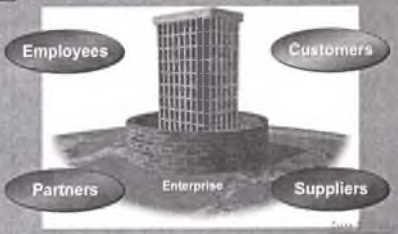
6. Podsumowanie

W ramach prac badawczych nad możliwością wdrożenia systemu multimedialnego we Wrocławskiej Akademickiej Sieci Komputerowej uruchomiono protokoły wyboru trasy dla adresów rozsiewczych IP (IGMP, PIM). Uruchomiono serwery wizyjne na bazie oprogramowania IP/TV i programów VAT , VIC (rozwiązania stosowane w MBONE). Podczas testów w nieobciążonym segmencie Ethernet'u możliwa była transmisja do czterech programów jednocześnie przy stosowaniu kompresji MPEG i H.261. Programy były transmitowane z prędkością 15 ramek/sek. Podstawowym celem prowadzonych prac była promocja rozwiązań multimedialnych w procesie kształcenia. Planuje się w najbliższej przyszłości utworzenie wirtualnej sieci do tramsmisji multimedialnych opartej o ATM'owy rdzeń sieci WASK. Pozwoli to wykorzystać dla rozbudowy systemów multimedialnych zasoby komputerowe, które obecnie są rozproszone na terenie Wrocławia.

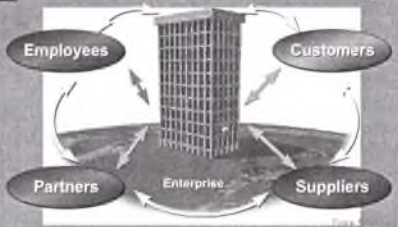
Global Networked Business- The new model of information technology

Open up Enterprise, internal systems and information to prospects, customers, partners, suppliers, employees

Traditional Business



The Global Networked Business



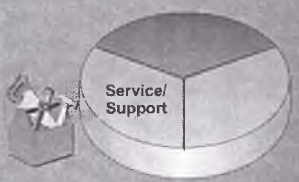
Global Networked Businesses Leverage Their Network to:

- Increase revenues
- Lower costs
- Improve productivity
- Enhance customer satisfaction and support

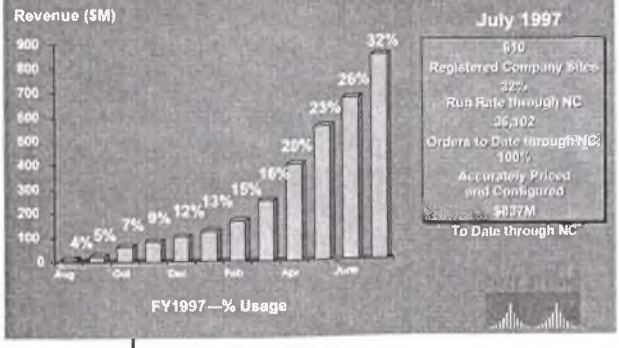
Cisco's History and Expertise

- $6.5 billion leader in networking
- 1,000%+ growth in 4 years
- 10,500 employees, 300 global offices
- The Internet runs on Cisco equipment
- Began using Internet as service and support tool in 1991
- Recognized leader in on-line customer support and commerce

Cisco Connection Online (CCO) Three Years Ago



Networked Commerce Ordering: Dramatic Results



Cisco's Networked Business Model Success

$125,000,000 Support
$8,400,000 Hiring
$85,000,000 Software
$50,000,000 Paperless

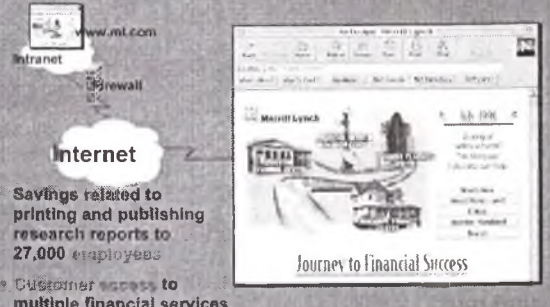
$250+M Savings/Year

$850+M Dollars To Date
30% Orders Online

Federal Express

- 500,000 customers using on line automated pickup, delivery, and invoicing services
- Introduced Internet-based package pickup, tracing and tracking functions in 1996
- Eliminating calls to its customer call centers saves $3 to $5 per call
- $1.5 million plus orders received via Internet

Merrill Lynch

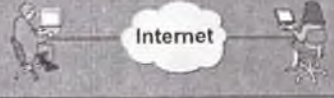


- Savings related to printing and publishing research reports to 27,000 employees
- Customer access to multiple financial services

First Union Bank

- Full-service home banking
- Substantial internal call center cost reduction
- Competitive advantage
- Investment training

The Promise of the Internet



"This year CIOs and network managers will stop focusing on technology and turn their full attention to applications and the business that the technology supports."

—Communications Week (1/6/97)

ZARZĄDZANIE TRANSAKCYJNYMI PRZEPŁYWAMI PRACY

Jerzy Brzeziński, Artur Grudzień, Tomasz Koszlajda

Naukowa i Akademicka Sieć Komputerowa

1. Wstęp

Pewne procesy przetwarzania danych w systemach informatycznych są kolekcjami powiązanych transakcji. Przykładem może być proces realizacji zamówienia w hurtowni, który obejmuje transakcje realizujące akcje przyjęcia zamówienia, wystawienia faktury, pobrania towaru z magazynu, wyekspediowania go oraz odebrania należności za towar. Transakcje te tworzą tak zwany transakcyjny przepływ pracy (ang. transactional workflow). Środowisko realizacji przepływów pracy ma zazwyczaj charakter rozproszony i heterogeniczny, a wykonanie transakcji wchodzących w skład pojedynczego przepływu pracy może być rozłożone w dłuższym odcinku czasu.

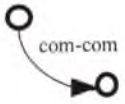
Na rynku informatycznym dostępne są narzędzia informatyczne, które wspomagają obsługę przepływów pracy. Jednak narzędzia te budowane w oparciu o standardowe systemy baz danych gwarantują poprawność wykonania poszczególnych transakcji, natomiast nie zapewniają globalnej poprawności przepływu pracy. Dlatego też, problem budowy systemów wspomagających poprawną obsługę transakcyjnych przepływów pracy jest wciąż intensywnie badany.

W niniejszym artykule opisano prototyp systemu zarządzania transakcyjnymi przepływami pracy oraz wstępne wyniki badań nad tym prototypem. Skonstruowany prototyp umożliwia:

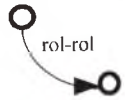
- definiowanie struktury transakcyjnych przepływów pracy,
- specyfikowanie parametrów wejściowych, z jakimi ma zostać uruchomione wystąpienie danego przepływu,
- efektywne wykonywanie określonych wystąpień transakcyjnych przepływów pracy w środowisku heterogenicznym i rozproszonym.

Zadania wchodzące w skład zarządzanych przepływów pracy muszą być aplikacjami systemów baz danych. Systemy te muszą umożliwiać realizację transakcji rozproszonych, za pomocą interfejsu XA. Ponadto, prototyp zarządza realizacją wystąpień przepływów pracy, w których zależności transakcyjne są ściśle określonego typu. Zależności te nadają się do modelowania transakcyjnych przepływów prac, w których między poszczególnymi zadaniami istnieją warunkowe zależności kolejnościowe oraz zależności typu zatwierdź/wycofaj.

Struktura artykułu jest następująca. W rozdziale drugim omówiono sposób modelowania struktury przepływów pracy. Dla ułatwienia zrozumienia poszczególnych elementów specyfikacji przepływów pracy, zilustrowano proces modelowania za pomocą prostego przykładu. W rozdziale trzecim przedstawiono architekturę prototypowego systemu zarządzania przepływami pracy oraz omówiono własności funkcjonalne poszczególnych modułów systemu. Rozdział czwarty zawiera opis współdziałania poszczególnych elementów systemu.



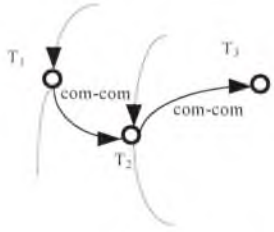
Zależność ***commit-commit*** oznacza, że jeśli zadanie T_1 może zakończyć się zatwierdzeniem, to zadanie T_2 musi też skończyć się zatwierdzeniem. Krawędzi tego typu są rozpoznawane przez zarządcę przepływu po wartości atrybutu *rodzaj_krawedzi* w relacji *WMR_kraw_mdl*, który w ich przypadku na wartość „com-com".



Zależność ***rollback-rollback*** oznacza, że jeśli zadanie T_1 musi zostać wycofane to zadanie T_2 też musi zostać wycofane. Krawędzi tego typu są rozpoznawane przez zarządcę przepływu po wartości atrybutu *rodzaj_krawedzi* w relacji *WMR_kraw_mdl*, który w ich przypadku na wartość „rol-rol".

Zależność ***rollback-commit*** oznacza, że jeśli zadanie T_1 musi zostać wycofane to zadanie T_2 musi skończyć się zatwierdzeniem. Krawędzi tego typu są rozpoznawane przez zarządcę przepływu po wartości atrybutu *rodzaj_krawedzi* w relacji *WMR_kraw_mdl*, który w ich przypadku na wartość „rol-com".

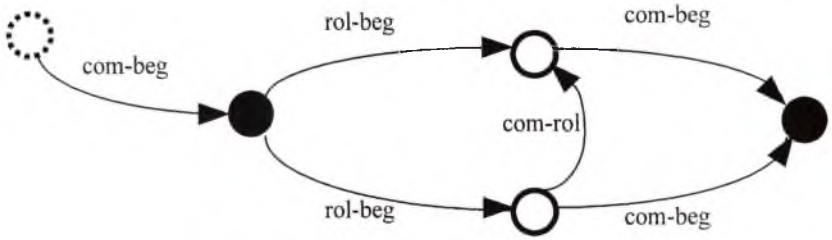
Konstruowana wersja prototypu nie posiada modułu analizy poprawności grafów. Modelowanie struktury przepływów pracy wymaga więc przestrzegania określonych reguł. Na przykład, krawędzie typu „com-rol", „com-com", „rol-rol", „rol-com" powodują opóźnienie rozpoczęcia wykonania zadań reprezentowanych przez wierzchołki znajdujące się na końcu krawędzi tych krawędzi, do momentu otrzymania przez zarządcę przepływów statusu wykonania zadań reprezentowanych przez wierzchołki znajdujące się na początku krawędzi. Dzieje się tak dlatego, ponieważ dany wierzchołek może zostać poddany analizie dopiero w momencie, kiedy wykonane zostaną wszystkie dochodzące do niego krawędzie. Ilustruje to przykład z Rys. 1, zadanie T_2 powinno zostać zatwierdzone, jeśli zostanie zatwierdzone T_1, ale wtedy powinno zostać też zatwierdzone zadanie T_3. Jeśli zadanie T_3 nie będzie mogło zostać zatwierdzone to zostaną unieważnione ścieżki przechodzące przez T_2, ale nie zostaną unieważnione ścieżki przechodzące przez T_1 (T_2 w dalszym ciągu jest przygotowane do zatwierdzenia). Jeśli chcemy aby w przypadku zatwierdzenia T_1 nastąpiło także zatwierdzenie T_3, to należy wyspecyfikować krawędź C-C między T_1 i T_3 w sposób jawny Rys. 2.



Rys. 1 Fragment grafu modelującego przepływ.

2) Rezerwacja miejsc w hotelach może mieć miejsce, jeśli nie jest możliwe zarezerwowanie przelotu z Poznania do Krakowa tego samego dnia co przylot ze Szczecina.

3) Rezerwacja przelotu z Poznania do Krakowa może mieć miejsce, jeśli możliwe jest zarezerwowanie miejsca w którymkolwiek z hoteli.



Rys. 4 Przykładowy graf struktury przepływu pracy

Poszczególne wierzchołki reprezentują zadania wykonujące następujące operacje:

T_1 - rezerwacja lotu ze Szczecina do Poznania w podanej klasie i na dany dzień,

T_2 - rezerwacja lotu z Poznania do Krakowa w podanej klasie i na dany dzień,

T_3 - rezerwacja miejsca o podanym standardzie w hotelu „Jowisz" i na dany dzień,

T_4 - rezerwacja miejsca o podanym standardzie w hotelu „Merkury" i na dany dzień,

T_5 - rezerwacja lotu z Poznania do Krakowa w podanej klasie i na następny dzień.

3. Architektura prototypu systemu

Prototyp systemu zarządzania przepływami transakcji ma architekturę częściowo rozproszoną. Dla każdego realizowanego przepływu pracy tworzony jest niezależny proces zarządcy przepływów. Moduł ten nadzoruje realizację poszczególnych zadań wchodzących w skład przepływu pracy za pomocą agentów dedykowanych dla każdego z zadań. Jest on uaktywniany na żądanie użytkownika poprzez dedykowany proces nasłuchujący (demon). Zadania mogą być wykonywane przez różne i w ogólności rozproszone i heterogeniczne systemy zarządzania bazami danych.

Poszczególne elementy systemu zarządzania komunikują się między sobą za pośrednictwem czterech typów interfejsów:

- interfejsu XA umożliwiającego atomowe zatwierdzanie transakcji rozproszonych;
- interfejsu SQL do zasobów systemów baz danych;
- interfejsu PVM do zarządzania procesami;
- interfejsu umożliwiającego przekazywanie parametrów.

Architektura systemu zarządzania przepływami pracy została przedstawiona na rysunku poniżej.

3.1.2 Demon zarządcy przepływów pracy

Zadaniem tego programu jest nasłuchiwanie, czy któryś z procesów nie zgłasza zapotrzebowania na współpracę z zarządcą przepływów. Po odebraniu takiego sygnału demon uruchamia program zarządcy przepływów, a jako parametr wejściowy podaje identyfikator procesu, który dla tego wystąpienia zarządcy przepływów jest programem do komunikacji z użytkownikiem.

3.1.3 Zarządca przepływów pracy

Proces zarządcy przepływów jest uruchamiany przez demona zarządcy przepływów na żądanie programu do komunikacji z użytkownikiem. Proces ten jest odpowiedzialny za prawidłowe wykonanie wystąpienia przepływu pracy, to znaczy zgodne z podaną specyfikacją przepływu pracy. W tym celu zarządca najpierw uruchamia agentów odpowiedzialnych za wykonanie zadań, a potem komunikuje się z nimi wydając polecenia dotyczące operacji wykonywanych na bazie danych i dotyczących zarządzania transakcjami lub danymi. Moduł ten jest też odpowiedzialny za konstruowanie odpowiednich identyfikatorów transakcji i nazw baz danych dla agentów zadań. Proces zarządcy odbiera komunikaty od agentów dotyczące stanu wykonania poszczególnych zadań i na tej podstawie podejmuje decyzje dotyczące dalszego wykonywania wystąpienia przepływu. Zarządca przepływu wykonując wystąpienie przepływu zapisuje odpowiednie informacje o stanie wystąpienia w bazie danych. Po wykonaniu przepływu proces zarządcy informuje program do komunikacji z użytkownikiem o zakończeniu przepływu pracy.

Proces zarządcy pełni jeszcze jedną ważną rolę, a mianowicie w przypadku stwierdzenia, że nie ma sensu uruchamiać niektórych zadań (bo i tak trzeba będzie je wycofać) nie wysyła do nich komunikatów nakazujących wykonanie operacji wchodzących w skład zadań, a zamiast tego wysyła sam do siebie komunikat o zakończeniu wykonywania danego zadania. Następnie odpowiada na komunikat wysyłany przez program do komunikacji z użytkownikiem (nakazujący podanie wyników wykonania wystąpienia przepływu) w imieniu agentów nadzorujących zadania, które nie zostały uruchomione. Cecha ta chroni przed „zagłodzeniem" procesów zarządcy przepływu i programu do komunikacji z użytkownikiem, które w trakcie wykonywania wystąpienia przepływu oczekują na określoną ilości komunikatów danego typu od wszystkich agentów.

3.1.4 Agenci zadań

Liczba agentów zadań jest równa liczbie wierzchołków w grafie struktury przepływu dla danego każdego wystąpienia. Nazwa programu, który należy uruchomić jako agenta danego zadania jest przechowywana w bazie danych wraz ze specyfikacją struktury przepływów. Każdy z agentów zadań oczekuje na komunikaty od zarządcy przepływu i na podstawie tych komunikatów wykonuje operacje na bazie danych. Po ich wykonaniu informuje zarządcę o wyniku ich wykonania (np.: dla polecenia wykonania zadania informuje zarządcę o tym, czy operacje wykonane na bazie danych mogą zostać zatwierdzone czy muszą zostać wycofane). Każdy z agentów odbiera także komunikat od programu do komunikacji z użytkownikiem zawierający parametry z jakimi musi zostać wykonane polecenie SQL wchodzące w skład zadania oraz odpowiada na żądanie podania wyników po zakończeniu wykonywania wystąpienia przepływu.

3.2 Interfejsy między komponentami systemu oraz narzędzia wykorzystane do ich tworzenia.

3.2.1 Interfejs XA zatwierdzania transakcji rozproszonych

Jest to zewnętrzny interfejs, który umożliwia koordynację rozproszonych transakcji przez koordynatora transakcji innego niż system zarządzania ORACLE wykorzystywany przez program

przekazywane między innymi identyfikatory PVM procesów, które dla nowo uruchamianego procesu oznaczają np. program do komunikacji z użytkownikiem.

4. Zasady współdziałania elementów systemu

Współdziałanie poszczególnych elementów systemu zarządzania przepływami pracy ma na celu stworzenie odpowiednich warunków do wykonania przepływu pracy. Z kolei po wykonaniu przepływu pracy współdziałanie komponentów systemu ma na celu przesłanie informacji o stanie poszczególnych zadań od programu do komunikacji z użytkownikiem oraz zakończenie pracy komponentów systemu uwikłanych w wykonywanie przepływu. Współdziałanie to opiera się w głównej mierze na przesyłaniu komunikatów między procesami komponentów systemu.

Przedstawiony poniżej diagram przedstawia algorytm wymiany komunikatów między komponentami systemu przed rozpoczęciem wykonywania przepływu i po jego zakończeniu.

Znaczenie użytych na diagramie symboli:

Symbol	Znaczenie
	czas w którym dany komponent systemu jest nieaktywny
	zdarzenie wysłania komunikatu do innego komponentu systemu (powyżej podana jest nazwa tego komunikatu)
	zdarzenie wysłania komunikatu rozgłoszeniowego do wszystkich członków grupy komunikacyjnej

Opis znaczenia komunikatów przedstawionych na powyższym diagramie:

1) Komunikat rozgłoszeniowy „MSG_WHO_IS_WMR" wysyłany przez program do komunikacji z użytkownikiem mający na celu nawiązanie kontaktu z zarządcą przepływu. Komunikat ten jest odbierany wyłącznie przez demona zarządcy przepływu. Demon po odebraniu komunikatu uruchamia nowy proces zarządcy przepływu i jako parametr uruchomienia przekazuje mu identyfikator aplikacji do komunikacji z użytkownikiem.
2) Proces zarządcy przepływu nawiązuje kontakt z aplikacją do komunikacji z użytkownikiem. Następnie przyłącza się do bazy danych.
3) Aplikacja do komunikacji z użytkownikiem przedkłada procesowi zarządcy przepływ do realizacji. W odpowiedzi proces zarządcy umieszcza w odpowiednich strukturach bazy danych dane, które będą wykorzystywane do zarządzania wykonaniem wystąpienia przepływu i będą zawierały informacje o stanie wykonania. Kolejną czynnością wykonywaną przez proces zarządcy jest uruchomienie agentów zadań. Każdy z uruchamianych agentów otrzymuje jako parametry uruchomienia: identyfikatory procesów programu do komunikacji z użytkownikiem i zarządcy przepływu oraz nazwę bazy danych. Każdy uruchomiony agent zadania przyłącza się do bazy danych wywołując funkcję *open* z interfejsu XA. W tym czasie użytkownik przy wykorzystaniu programu do komunikacji wprowadza parametry z jakimi będzie wykonywane wystąpienie przepływu.
4) Agent zadania informuje aplikację do komunikacji z użytkownikiem o swojej gotowości do pracy.
5) Agent zadania informuje zarządcę przepływu o swojej gotowości do pracy.
6) patrz punkt 4).
7) patrz punkt 5).
8) Program do komunikacji z użytkownikiem wysyła parametry wykonania zadania w ramach danego przepływu pracy.
9) patrz punkt 8).
10) Agent wysyła komunikat oznaczający gotowość do wykonania zadania.
11) patrz punkt 10).
12) Aplikacja do komunikacji z użytkownikiem wysyła komunikat nakazujący rozpoczęcie wykonywania wystąpienia przepływu pracy.

pracy i dokonania analizy wygenerowanych ścieżek przez zarządcę przepływu. Należy zwrócić uwagą, że czas blokowania zasobów zależy od wielkości struktury przepływu pracy i położenia wierzchołka symbolizującego dane zadanie. Im mniejszy graf lub im bliżej wierzchołka końcowego znajduje się dany wierzchołek, tym blokowanie zasobów trwa krócej.

Duże znaczenie dla działania zarządcy przepływów pracy ma fakt, że zadanie reprezentowane przez wierzchołek w grafie może zostać poddane analizie dopiero, kiedy zostaną wykorzystane wszystkie dochodzące do niego krawędzie. Rozwiązanie takie zostało zaproponowane, ponieważ z założenia zarządca przepływów ma realizować takie przepływy pracy, w których między zadaniami występują ograniczenia kolejnościowe (kolejne zadanie może zostać poddane analizie wtedy, kiedy poprzednie w grafie zostanie wykonane). Nawet jeśli użytkownik zdefiniuje taki graf przepływu pracy, w którym będą występowały same zależności typu zatwierdź/wycofaj, to nie zmieni to oczywiście działania zarządcy przepływu. Rozwiązanie to nie jest optymalne z punktu widzenia czasu wykonywania przepływów. Także możliwości zrównoleglenia wykonania przepływów jest stosunkowo ograniczona i zależna od struktury przepływów. Zaletą tego rozwiązania jest natomiast optymalizacja operacji wykonywanych na bazach danych pod względem liczby tych operacji. Jeśli bowiem okaże się, że już przed uruchomieniem danego zadania wiemy o potrzebie jej wycofania, to zadanie to nie jest uruchamiane. Takie rozwiązanie ma duże znaczenie w przypadku rozbudowanych struktur przepływów pracy, w których już po analizie kilku początkowych wierzchołków wiadomo, że nie uda się znaleźć rozwiązania, bo na przykład nie jest możliwa dalsza realizacja wykonania przepływu pracy, a wszystkie krawędzie grafu wykorzystywane są w sposób nieaktywny. W takiej sytuacji wszystkie zadania symbolizowane przez kolejne wierzchołki w grafie w ogóle nie będą uruchamiane.

Alternatywnym podejściem do rozważanego problemu jest uruchamianie wszystkich zadań równolegle, a następnie po otrzymaniu wyników ich wykonania analiza zależności między zadaniami przeprowadzona na podstawie struktury przepływu pracy. Takie rozwiązanie mogłoby spowodować skrócenie czasu wykonywania wystąpienia przepływu, ale z drugiej strony powodowałoby też blokadę zasobów, na których operują zadania. Mogłoby one ponadto znacznie obciążyć systemy zarządzania bazami danych. Podejście to byłoby możliwe tylko dla przepływów pracy, w których między zadaniami nie występują ograniczenia kolejnościowe.

Inną zaletą prototypu systemu jest wykonywanie operacji wprowadzania parametrów dla konkretnego przepływu pracy i przyłączanie się poszczególnych agentów zadań do odpowiednich baz danych w tym samym czasie. W ten sposób dwie najdłużej trwające operacje inicjowane są równolegle, w momencie kiedy użytkownik wprowadzi ostatni parametr dla wystąpienia przepływu. Jest to możliwe, ponieważ wszystkie komponenty systemu konieczne dla wykonania przepływu są już gotowe do pracy.

Bibliografia

[1] Georgakopoulos D., Rusinkiewicz M. From Transactions to Transactional Workflows. ICDE-12 New Orleans, Feb. 26 1996.

[2] Moss J. E. B. Nested Transactions: Approach to Reliable Distributed Computing. Ph.D. thesis, MIT Press, Cambridge, Mass, 1985.

[3] Rusinkiewicz M., Sheth A. Specification and Execution of Transactional Workflows. In *Modern Database Systems*, editor Won Kim, Addison Wesley 1995.

[4] Oracle7 Server Distributed Systems Administration Tools, Vol I: Distributed Data

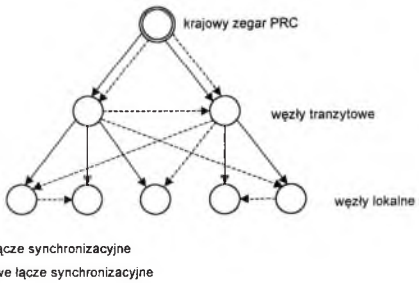
[5] Pro*C Oracle™ Precompilers Guide

[6] X/Open Snapshot Distributed Transaction Processing: The XA+ Specification Version 2 X/Open Company Ltd., U.K.

(zalecenie ITU-T G.811). Taki sposób synchronizacji oznaczał, że teoretycznie poślizgi mogły występować sporadycznie (raz na kilkadziesiąt dni) i tylko na połączeniach międzynarodowych. Uzgodnione zostały również wymagania na parametry zegarów podległych sieci synchronizacyjnej. Zegary takie występowały praktycznie tylko w centralach telefonicznych i stanowiły ich integralną część. Ich parametry zostały dobrane tak, żeby utrata sygnału synchronizacyjnego z zegara nadrzędnego, nie powodowała przekroczenia dopuszczalnej częstotliwości występowania poślizgów.

Konstrukcje ówcześnie stosowanych zegarów PRC bazowały na wzorcach cezowch. Z uwagi na ich krótką żywotność stosowano zwykle konstrukcje potrójne zapewniające wysoki stopień niezawodności. Wiele krajowych zegarów PRC było instalowanych przy wybranych cyfrowych centralach telefonicznych (np. międzynarodowych). W innych przypadkach zegary te funkcjonują w specjalnych laboratoriach.

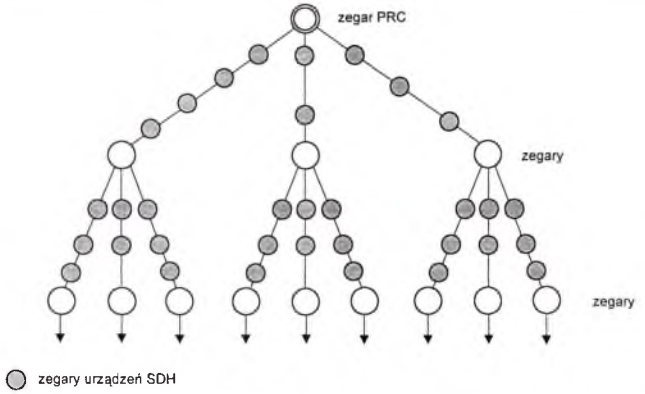
Najczęściej struktura krajowych sieci synchronizacyjnych miała charakter hierarchiczny. Zegary w danej warstwie charakteryzują się takimi samymi parametrami jakościowymi. Pomiędzy warstwami zachowana jest zależność nadrzędny-podległy (*master-slave*), polegająca na tym, że pewne zegary są synchronizowane do zegarów wyższego rzędu i są one jednocześnie zegarami nadrzędnymi w stosunku do zegarów niższego rzędu. Najwyższą warstwą jest warstwa zegara PRC.
Wykorzystywana była również metoda synchronizacji wzajemnej, w której wszystkie zegary są ze sobą połączone i każdy z nich ma, do pewnego stopnia, wpływ na pozostałe zegary.
Dystrybucja sygnałów synchronizacyjnych oparta była o systemy PDH, których charakterystyczną cechą są połączenia punkt-punkt. Sieci takie są z natury statyczne i sposób dystrybucji sygnałów synchronizacji nie ulega częstym rekonfiguracjom. Niezawodność w sieci synchronizacyjnej osiągano przez doprowadzanie do zegarów węzłowych sygnałów poprzez fizycznie niezależne połączenia teletransmisyjne. Przykładowy sposób realizacji sieci synchronizacyjnej w oparciu o metodę master-slave został przedstawiony na rys. 1.



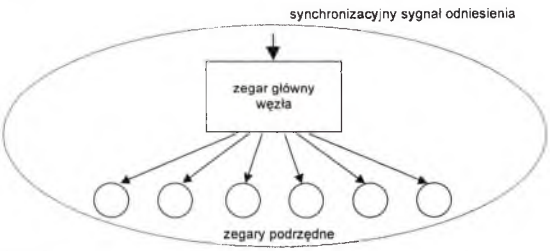
Rys. 1. Synchronizacja sieci w oparciu o metodę master-slave

Do dystrybucji sygnałów synchronizacyjnych najczęściej wykorzystywano strumienie danych o przepływności 2.048kbit/s. Urządzenia PDH są źródłem głównie szybkozmiennych fluktuacji fazy (*jitter*), które są łatwe do odfiltrowania przez zegary podległe (centralowe). Wolnozmienne fluktuacje fazy (*wander*) pochodzące z systemów liniowych PDH oscylują tak wolno, że zegary podległe są w stanie nadążać za nimi. Daje to zakres częstotliwości pomiędzy fluktuacjami dobowymi oraz jitterem pochodzącym od krotnic i regeneratorów PDH, w obrębie którego

podrzędnym. Połączenie wielu zegarów w kaskadzie prowadzi do kumulowania fluktuacji fazowych. Dlatego bardzo istotne jest określenie parametrów układów zegarowych urządzeń SDH oraz dopuszczalnych ilości zegarów połączonych w kaskadzie.
Obydwa powyższe zagadnienia zostały poddane analizie i organizacje standaryzacyjne (ITU-T i ETSI) opracowały odpowiednie zalecenia definiujące parametry zegarów SDH, dopuszczalne długości łańcuchów synchronizacyjnych oraz dopuszczalne poziomy fluktuacji fazowych dla styków synchronizacyjnych na poziomie sieciowym. Do dystrybucji synchronizacji pomiędzy węzłami zaleca się stosowanie metody typy nadrzędny-podległy (rys. 2.). W obrębie węzła sygnały synchronizacyjne powinny być rozprowadzane w strukturze gwiaździstej (rys. 3).



Rys. 2. Ogólna topologia sieci synchronizacyjnej z wykorzystaniem urządzeń SDH



Rys. 3. Sposób rozprowadzania sygnałów synchronizacyjnych w obrębie węzła

Źródła sygnałów odniesienia

W dalszym ciągu za podstawowe źródło odniesienia dla zegarów PRC uważa się wzorce cezowe. Pojawiła się jednak alternatywa w postaci radiowych systemów przesyłania sygnałów synchronizacyjnych. Spośród nich najbardziej znanym jest satelitarny system pozycyjny GPS będący własnością Departamentu Obrony USA. Jego głównym przeznaczeniem jest precyzyjne określanie położenia obiektów w przestrzeni trójwymiarowej. Dla zastosowań cywilnych udostępniany jest sygnał o celowo obniżonej dokładności. Mimo tego odebrany sygnał może być wykorzystany do synchronizowania SSU, tworząc w ten sposób zegar o dokładności równoważnej

identyfikatora ścieżki synchronizacyjnej – mechanizmu pozwalającego na rozpoznawanie czy sygnał synchronizacyjny odbierany w danym urządzeniu SDH nie pochodzi właśnie od niego.
Obecnie w większości przypadków urządzenia zegarowe SDH oraz SSU do celów synchronizacji używają sygnałów 2MHz. W takim przypadku informacja o jakości synchronizacji jest tracona.
W systemach SDH komunikaty SSM są kodowane w nagłówku sygnału STM-N. Wykorzystanie komunikatów o jakości synchronizacji przewidziano również dla systemach PDH. Zdefiniowane zostały komunikaty dla sygnałów 2, 34 i 140 Mbit/s. Spośród nich tylko dla sygnałów o przepływności 2Mbit/s można oczekiwać praktycznych implementacji.

Przekazywanie sygnałów synchronizacji między operatorami

Postępująca demonopolizacja rynku telekomunikacyjnego powoduje powstanie nowych firm operatorskich, zwiększenie ilości punktów styku pomiędzy operatorami oraz dużą różnorodnością urządzeń i systemów poprzez które realizowane są usługi. Oznacza to również powstanie nowego rodzaju usługi: dostarczanie sygnałów synchronizacji (w przyszłości być może to rozszerzone o dostarczanie sygnałów czasu).
W przypadku przekazywania sygnałów synchronizacyjnych pomiędzy operatorami odbiorca nie posiada własnego zegara PRC, a jego sieć jest synchronizowana przez sieć dostawcy. Z punktu widzenia sieci synchronizacyjnej sieć odbiorcy staje się częścią sieci synchronizacyjnej dostawcy. Na punktach pomiędzy operatorami nie występują więc poślizgi. Jednakże oznacza to całkowitą zależność jakości synchronizacji sieci odbiorcy synchronizacji od jakości dostarczanego sygnału synchronizacyjnego.
Na jakość dostarczanego sygnału synchronizacyjnego mają wpływ następujące czynniki:

- jakość zegara PRC używanego przez dostawcę synchronizacji
- jakość dystrybucji sygnału synchronizacyjnego w sieci dostawcy synchronizacji.

Konieczne jest więc określenie precyzyjnych zasad przekazywania sygnałów synchronizacyjnych oraz parametrów sygnałów synchronizacyjnych. Zmiany w konfiguracji sieci synchronizacyjnej operatora „dostawcy" mogą mieć istotny wpływ na sieć synchronizacyjną operatora „odbiorcy". Zatem zmiany takie powinny być wzajemnie koordynowane, by uniknąć powstania pętli synchronizacyjnych.
Przykładowe sposoby współpracy sieci synchronizacyjnych pomiędzy operatorami przedstawiono na rys. 4.

Nowa struktura sieci NASK

Wiktor Krzanowski

Naukowa i Akademicka Sieć Komputerowa

Już we wstępie do tegorocznej konferencji przedstawiliśmy informacje o zasadniczych zmianach dotyczących struktury sieci NASK. Tradycją tych konferencji stało się już informowanie o kolejnych przeobrażeniach sieci, przeobrażeniach bardzo istotnych i następujących z roku na rok. Szybkość tych zmian odpowiada tempu rozwoju technologii sieciowych na świecie - i takie zmiany dominowały w pierwszych latach budowy sieci NASK - oraz gwałtownemu rozwojowi rynku teleinformacyjnego, a co za tym idzie zmianom w naszej sieci struktury organizacyjnej, obsługi abonentów, kooperacji etc. - co obserwujemy w ostatnich latach.

O ile wprowadzenie zmian w technologiach sieciowych związane było i jest w dalszym ciągu z znajomością tego co jest dostępne, posiadaniem wysoko kwalifikowanej kadry zdolnej do opanowania nowości i ich wdrożenia i oczywiście podejmowaniem ryzyka bycia pierwszym, o tyle zmiany związane z rozwojem rynku (w tym jego konkurencyjności) wymagają umiejętności prowadzenia często trudnych i żmudnych rozmów mających na celu znalezienie z potencjalnymi partnerami płaszczyzny współpracy korzystnej dla obu stron.

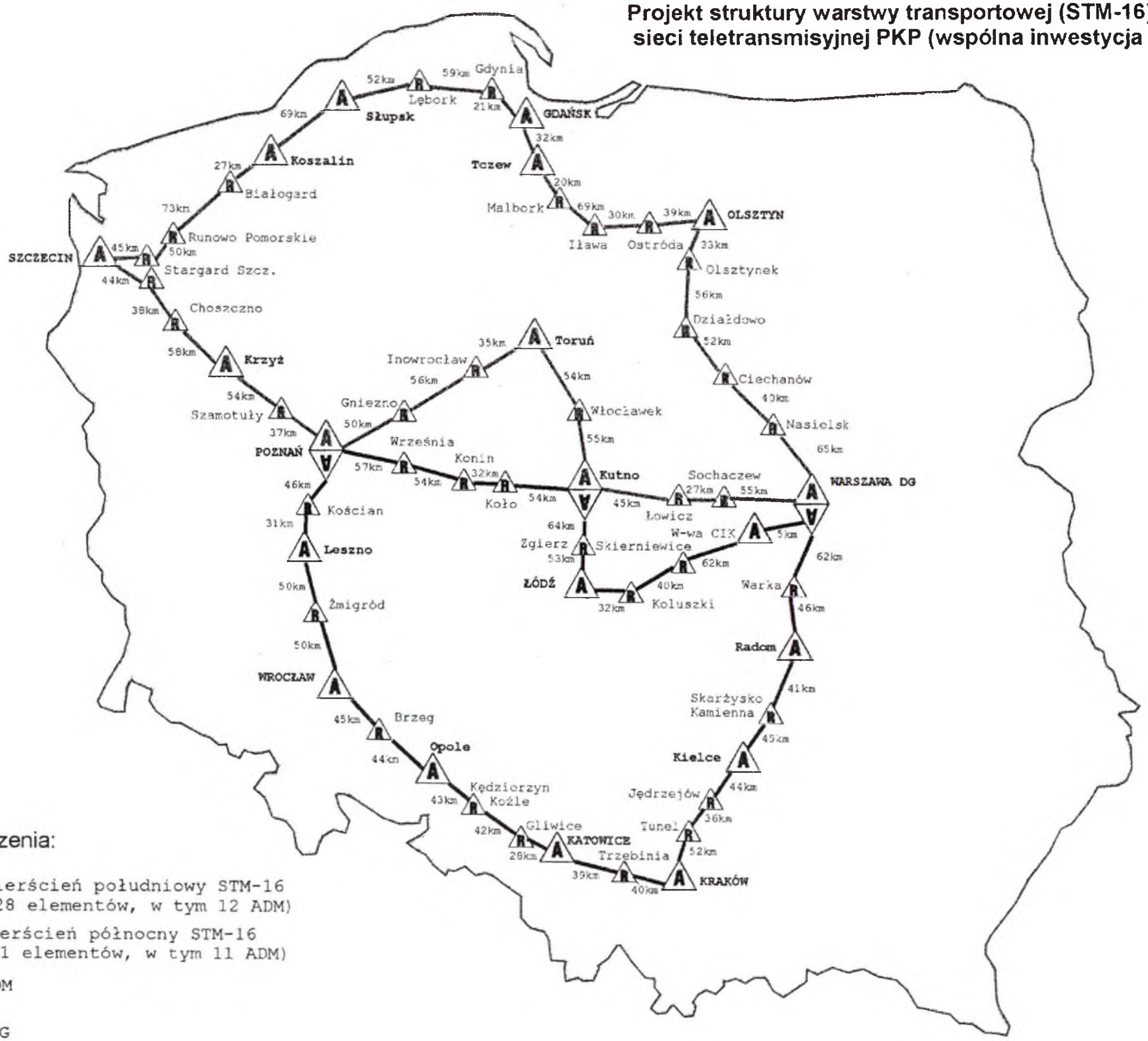
Podobnie jak w całej branży technologii informatycznych także w działalności sieciowej zachodzi proces konsolidacji. Wynika to konieczności sprostania gwałtownie rozwijającym się potrzebom rynku, rosnącą złożonością i zakresem dziedzin technologii teleinformacyjnych i informatycznych oraz koniecznością coraz bardziej kompleksowego podejścia do klienta. Nasze obserwacje i doświadczenia jako pioniera tego rynku w Polsce, skłaniają nas do kolejnej ucieczki " do przodu ". Podstawowe założenia obecnie dokonywanych i planowanych przez nas zmian są następujące:

- istnieją warunki techniczne i ekonomiczne do odwrócenia dotychczasowej sytuacji w sieci gdzie podstawowe problemy są z jej wydolnością w relacjach międzynarodowych i krajowych na strukturę gdzie ograniczenia przepustowości występują przede wszystkim na portach przyłączających abonentów,
- możliwe jest świadczenie w związku z powyższym, i jest na to zapotrzebowanie ze strony rynku, usług sieciowych o znacznie lepszej jakości niż obecnie dostępne,
- podaż odpowiedniej jakości usług sieciowych umożliwi efektywne rozwijanie i co za tym idzie rosnące zapotrzebowanie na zaawansowane usługi np. handel poprzez sieć, telepraca itp.
- istnieją warunki i rzeczywista potrzeba współpracy z innymi podmiotami na zasadzie stabilnych i długotrwałych powiązań kooperacyjnych.

Przesłanki te zaowocowały nawiązaniem współpracy z operatorem szwedzkim Telia AB – jednym z głównych udziałowców systemu kablowego BALTICA. W ramach podpisanej umowy dzierżawimy linię w technologii SDH o przepływności 155Mb/s w relacji Sztokholm Kołobrzeg. W wyniku negocjacji z TP S.A. przyjęto, że czasowo podłączenie NASK do tej linii nastąpi w Warszawie w ramach umowy z Telia AB. Linia ta z punktu widzenia zainstalowanych na obu końcach urządzeń pracuje w technologii ATM co ma istotne znaczenie ze względu na możliwość świadczenia różnych usług. I tak:

- wydzielony kanał wirtualny będzie obsługiwał ruch Internetowy i umowa na tranzyt ruchu Internetowego z Telia AB gwarantuje wysoką jakość tej usługi,

Projekt struktury warstwy transportowej (STM-16)
sieci teletransmisyjnej PKP (wspólna inwestycja PKP i NASK)



teleinformatycznych w postaci kanałów logicznych w sieci NASK, zestawienie i utrzymanie linii dostępowych, wyposażenie abonenta w urządzenia dla połączenia jego sieci LAN oraz usługi związane z uruchomieniem i konserwacją części telekomunikacyjnej abonenta.

5.

W cenniku podano ceny nowych usług w sieci NASK obecnie śladowo świadczonych, na które jednak jest zapotrzebowanie zgłaszane pod adresem NASK.

Dla abonentów posiadających skrzynki na serwerze NASK (kod usługi W), poprzez które można realizować wszystkie funkcje Internetu, zniesiono limit czasowy oraz dodatkową opłatę za godziny ponad limit. Jednocześnie dla abonentów prowadzących działalność publiczną wprowadzono możliwość posiadania własnego adresu domenowego tak samo jak dla abonentów podłączonych przez łącze stałe. Tym samym ci abonenci widziani są w sieci co najmniej tak samo dobrze jak inni, a często lepiej ze względu na umieszczenie informacji na serwerze NASK mającym szybkie połączenie ze szkieletem sieci. Oferta ta wiąże się z coraz popularniejszym traktowaniem adresu domenowego w sieci podobnie jak znaku firmowego w innego rodzaju publikatorach.

Dla abonentów łączących się poprzez sieć komutowaną zaproponowano możliwość i cenę podłączenia się poprzez ISDN. Liczymy, że po długim okresie rozruchu usługa ta będzie szerzej oferowana i dla części abonentów obecnie pracujących poprzez łącza dzierżawione, będzie korzystną ekonomicznie i usługowo ofertą.

Wprowadzamy dzierżawę międzynarodowego kanału Internetowego o gwarantowanej przepustowości (kod usługi Z) dla abonentów, przede wszystkim operatorów, dla których będzie to bardziej opłacalne. Dzierżawa kanału w połączeniu naziemnym ma również zalety w postaci większej odporności na zakłócenia w porównaniu z łączem satelitarnym oraz likwidacji opóźnienia wywołanego długą drogą do satelity i z powrotem na ziemię.

W sieci szerokopasmowej NASK obejmującej cały kraj proponujemy również wynajem portów (kod usługi P) z możliwością zestawiania kanałów logicznych pomiędzy punktami określonymi przez abonenta. Mogą to być również kanały do węzłów NASK, na przykład do węzłów Internetu. Ilość kanałów zestawianych na portach nie jest ograniczona, a gwarantowana przepływność portu wynosi w sumie 50% jego chwilowej przepustowości.

Wreszcie wobec coraz powszechniejszego rozwijania się tej usługi na świecie proponujemy transmisję głosu (kod usługi GT) pomiędzy urządzeniami abonentów lub partnerów NASK. Usługa ta od dawna jest w sieci realizowana, ale bez informowania o tym operatorów. W połączeniu z transmisją innego rodzaju danych, zwłaszcza w sieci korporacyjnej lub w zamkniętej grupie użytkowników jest ekonomicznie wysoce efektywna.

6.

Wreszcie w cenniku zaproponowano ceny za usługi nazwane eksperymentalnymi. Są to usługi ogólnie nazywane szerokopasmowymi (kod usługi V) oraz telefon internetowy (kod usługi T).

Pierwsza obejmuje przede wszystkim różnego rodzaju usługi videokonferenycyjne świadczone chwilowo, stale oraz na sprzęcie NASK lub sprzęcie abonenta. NASK dysponuje odpowiednim wyposażeniem i wiedzą, jednak rynek w tym zakresie jest uśpiony. Spodziewamy się, że jednoznaczne umieszczenie tych usług w cenniku spowoduje ich powszechniejsze zastosowanie.

Do cennika wprowadziliśmy już cenę za telefon internetowy, to znaczy specjalny telefon dodatkowo wyposażony w ekran oraz funkcje umożliwiające korzystanie z usług WWW bez posiadania komputera lub podobnego urządzenia. W cenniku NASK proponuje się wydzierżawianie abonentowi odpowiednich urządzeń oraz utrzymanie koniecznego pomocniczego konta na serwerze NASK, na którym informacja nadchodząca i wychodząca z telefonu jest odpowiednio przetwarzana stosownie do możliwości urządzenia oraz małego ekranu.

ZMIANY W ADMINISTROWANIU ŚWIATOWYM INTERNETEM

Maciej Kozłowski

Naukowa i Akademicka Sieć Komputerowa

Niniejsze opracowanie jest bardzo skrótowe. Jego celem jest jedynie zaznaczenie tematyki dotyczącej generaliów rozwoju Internetu.

1. Wzrost Internetu.

Podług opracowania „Internet Demographic Survey" wykorzystanie Internetu potroiło się w ciągu ostatnich 2 lat, co oznacza wzrost w tempie 70% rocznie. Ostrożne oceny, dotyczące ilości użytkowników Internetu w Stanach Zjednoczonych, podają wzrost w ciągu ostatniego roku o 46%, co ciągle jest bardzo interesujące, zważywszy na bliskość granicy nasycenia pod tym względem. Ocenia się, że pod koniec 1997 r. z Internetu korzystało 58 milionów dorosłych Amerykanów (w wieku ponad 15 lat), w tym 42 miliony określiło się jako „aktywni użytkownicy". Ocenia się, że w 1998 r. światowa ilość użytkowników Internetu przekroczy liczbę 100 mln.

Podług danych „Network Wizzards", w styczniu 1998r. było zarejestrowanych 29.670.000 „hostów" w Internecie, co oznacza wzrost o 83% w porównaniu z liczbą 19.540.000 w styczniu 1996 r. Najliczniejsze domeny to:

Domena	Liczba „hostów"
com	8.201.000
net	5.283.000
edu	3.945.000
jp	1.169.000
mil	1.099.000
us	1.076.000
de	994.000
uk	987.000
ca	839.000
au	665.000
org	519.000
gov	497.000
fi	450.000
nl	381.000
fr	333.000
se	319.000

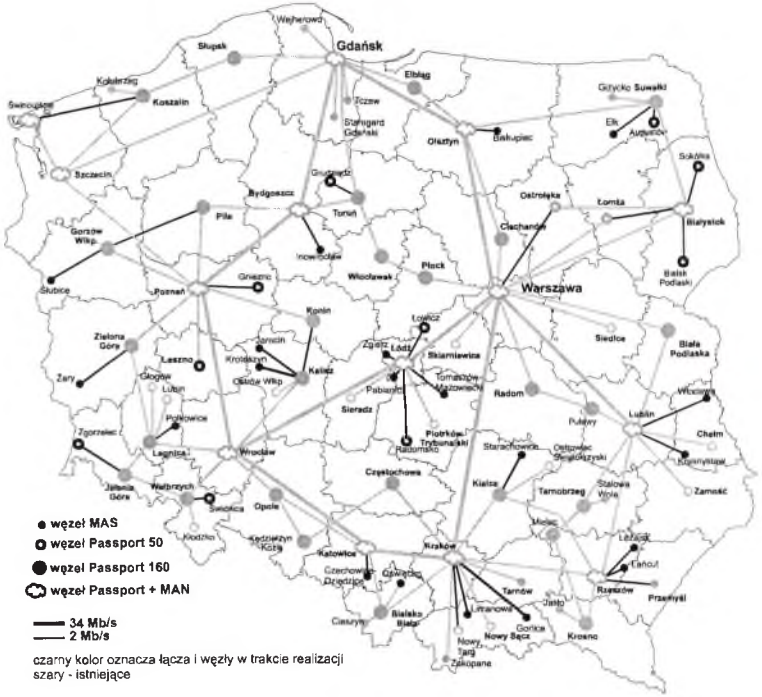
2. Komercyjne wykorzystanie Internetu

Wzrost komercyjnego wykorzystania Internetu jest nawet szybszy, niż wzrost ilości użytkowników. Podług sondażu wykonanego przez „Media Dialogue", 27% amerykańskich użytkowników „web" dokonało w 1997 r. zakupów za pośrednictwem Internetu, podczas gdy w

Była propozycja, aby grupa ta składała się z 9 osób wyłonionych podług schematu 2+2+2+3, ale dyskutowane są także inne możliwości, np. szersze ciało z wybieranym prezydium. Są pomysły utworzenia dodatkowo szerokiego komitetu przedstawicieli różnych organizacji przy oczekiwaniu od nich wkładu na poziomie $5.000 rocznie. Celem nadrzędnym jest dobre umocowanie formalne nowej organizacji, bez angażowania w nią rządu USA.

Rozwiązanie ma zapewnić rejestrację i utrzymanie nazw na bazie konkurencyjności. Punkt ten wydaje się kontrowersyjny, bowiem zakłada się wielość organizacji operujących na wspólnej bazie danych ale nie ulega wątpliwości, że są to kontrowersje rozwiązywalne. Proponuje się zwiększenie ilości domen poziomu "generic" (takich jak .com, .edu) w kierunku propozycji zgłoszonych przez działający w 1997 r. Internet Ad Hoc Committe (IAHC).

Z punktu widzenia Europy kontrowersyjny jest pomysł wprowadzenia do ciała sterującego nową organizacją przedstawicieli "użytkowników" oraz "przemysłu", bowiem paradoksalnie może to utrwalić, a nawet nasilić dominację USA względem Internetu. Zdaniem Christophera Wilkinsona z Dyrektoriatu Generalnego XIII Komisji Wspólnot Europejskich zamiast "nie mieszania się rządu USA" warto rozważyć "mieszanie się innych rządów". Dyskusja na temat nowej struktury IANA trwa. Europę - oprócz DG XIII - reprezentuje w niej RIPE



Rys 1. Schemat sieci POLPAK-T w marcu 1998 r.

Na przełomie 1996/1997 r uruchomiony został protokół ATM w relacji Gdańsk -Warszawa-Łódź. w oparciu o trakty 34 Mb/s. Dało to poczętek szkieletowi sieci ATM dla połączeń międzywęzłowych.Szkielet ten tworzą połączone traktami ATM o przepływności 34 Mb/s miasta Wrocław, Katowice, Kraków, Poznań, Warszawa, Lublin, Łódź, Poznań, Olsztyn. Obecnie węzły sieci POLPAK-T zainstalowane są we wszystkich miastach wojewódzkich i niektórych rejonowych. Całkowita liczba portów mogących pracować z protokółem frame relay o szybkościach z zakresu 64 kb/s do 2048 kbs. Pojedynczy port fizyczny pozwala na stworzenie do 992 stałych łączy wirtualnych. W końcu marca 1998 roku całkowita liczba portów dostępna w sieci wynosiła ok. 3500. Potencjalnie obecna struktura sieci pozwala na uruchomienie 12000 portów.

Zainteresowanie ze strony Klientów jest również usługami dostępnymi jednocześnie w technologiach frame relay i X25. Spowodowane jest to eksploatowaniem dobrze pracujących sieci i aplikacji X.25 i migracją w kierunku nowych rozwiązań sieciowych. W tym celu w sieci POLPAK-T zainstalowanych zostały węzły z rodziny DPN 100 i węzły typu MAS (Magellan Acces Switch). Pozwalają one udostępnienie Klientom portów frame relay lub X.25 Zainstalowanych zostało w sieci 64 tego typu urządzeń. o łącznej liczbie portów wynoszącej ok. 1500. Ze względu na swe małe rozmiary i niewielką moc zasilania i cenę instalowane są tam, gdzie występują pojedynczy Klienci.

Dostęp do sieci Internet z sieci PSTN.

Intensywnie rozbudowywana była część struktury sieci przeznaczona do realizacji dostępu do Internetu z sieci telefonicznej Źródłem tej rozbudowy było z jednej strony dążenie do objęcia taryfą lokalną obszaru całego kraju, z drugiej zaś zwiększenie liczby modemów dostępowych. Pierwszą powód został rozwiązany poprzez budowę węzłów sieci POLPAK- T w każdej strefie numeracyjnej. Dla zwiększenia liczby modemów dostępowych wybrano inne rozwiązanie niż podstawowe -podręcznikowe, stosowane w początkowym okresie eksploatacji sieci. To rozwiązanie polegało na użyciu wiązki analogowych linii telefonicznych na końcu których podłączone zostały modemy. Z tych modemów poprzez szeregowe porty routera dane przesyłane były do portu frame relay seci POLPAK-T. W ten sposób dla całego kraju utworzono ok 800 linii dostępu do Internetu. Dalsze zwiększanie liczby modemów w ten sposób było technicznie możliwe ale trudne do opanowania w eksploatacji. Wybrano inne rozwiązanie przy wykorzystaniu urządzeń dostępowych typu Rapport 112. Zawiera ono 60 modemów analogowych i 60 modemów ISDN.Dołączone jest ono do centrali telefonicznej poprzez interfejs PRI.. Na koniec marca 1998 roku zainstalowanych było 50 takich urządzeń w sieci TP S.A. Obecnie uruchomionych na terenie całego kraju jest ponad 4100 linii dostępowych dla abonentów posiadających modemy analogowe i 1700 linii dla posiadaczy modemów ISDN.

Stosowane techniki dostępowe.

Telekomunikacja Polska S.A. udostępniając usługi transmisji danych dla szerokiej rzeszy Klientów musiała rozwiązać problem połączenia lokalizacji Klienta z węzłem sieci PPOLPAK-T. Znane rozwiązania techniczne o wysokiej jakości połączeń wykorzystujące trakty cyfrowe czy włókna światłowodowe nie mogły być brane pod uwagę z powodu, poza nowymi inwestycjami, ich powszechnego braku. W realiach polskim jedynym rozwiązaniem było wykorzystanie do tego celu istniejących kabli miedzianych. Występuje tu kilka barier z których decydujące znaczenie mają:

1. Odległość od węzła do klienta,
2. Koszt urządzeń dostępowych,
3. Możliwość zdalnego zarządzania urządzeniami dostępowymi,
4. Różnorodność interfejsów od strony linii.

Wybór padł na modemy HDSL. Pozwalają one na kablach o średnicy 0,5 mm osiągnąć szybkość do 1 Mb/s przy zasięgu do 5 km na jednej parze. Dla szybkości do 2 Mb/s stosowane są połączenia dwuparowe. Dotychczasowe doświadczenia wskazują na to, że nowe kable gwarantują dobrą i stałą jakość transmisji. Gorzej jest w przypadku starych kabli o zmiennej w czasie pracy impedancji. Trudno jest wtedy osiągnąć dobrą jakość transmisji szczególnie dla dwuparowych połączeń. Przy większych odległościach ok. 10 km zastosowanie mają modemy N x 64 kb/s. Tam gdzie występuje znaczący popyt na usługi a odległość stanowi barierę dla modemów HDSL, eliminuje się ją przez uruchomienie nowego węzła. Przy odległościach sięgających kilkudziesięciu kilometrów proponowanym i stosowanym przez TP S.A rozwiązaniem jest wykorzystanie modemów V.34 i praca z protokołem PPP lub HDLC. Uzyskiwane przepływności nie przekraczają 28,8 kb/s. Innym sposobem jest przedłużenie połączenia traktem cyfrowym. Rozwiązanie to przy obowiązujących taryfach jest kosztowne zwłaszcza dla większych szybkości transmisji. Stosowane jest ono zawsze w przypadkach gdy łącza cyfrowe lub światłowody są własnością Klienta.

TP S.A. w ramach abonamentu udostępnia modemy Klientom i zapewnia ich serwis. Dlatego też ograniczono liczbę typów stosowanych urządzeń. Obecnie stosowane są modemy HDSL serii Crokus firmy Telindus i modemów V. 34 firmy Motorola. Przy realizacji dostępu do Internetu z sieci telefonicznej modemem analogowym wykorzystywany jest standard V.34 o maksymalnej szybkości 28,8 kb/s. Urządzenia Rapport 112 powalają na realizację standardu K56Flex o

Istotnym elementem decydującym o sprzedaży usług jest ich jakość. Dla Klientów wielkie znaczenie oprócz udostępnionych parametrów ma ciągłość dostępu do usług sieci transmisji danych. Przy istniejącej architekturze sieci najbardziej wrażliwym elementem jest łącze dostępowe. Usunięcie jego awarii a czasem nawet konieczność jego odbudowy może być powodem strat trudnych do odrobienia. Sposobem na ominięcie tego problemu jest stosowanie łączy backupowych. Z istniejących metod najbardziej obiecująca jest technika radiodostępu, zarówno łączy punkt - punkt jak i punkt - wielopunkt. Łącza radiowe pozwalają również na dostęp do Klientów tam gdzie nie ma sieci przewodowej. W tej chwili Centrum Systemów Teleinformatycznych prowadzi prace nad wyborem systemu radiodostępu, którego parametry techniczne i ekonomiczne pozwoliłyby na wprowadzenie go do eksploatacji w sieci POLPAK-T.

Literatura:

1. Informacja o sieci POLPAK-T, Telekomunikacja Polska S.A. - Centrum Systemów Teleinformatycznych

Art. 2.: 28 definicji, w tym:

„6) operator – uprawniony podmiot, który świadczy usługi telekomunikacyjne,
16) sprzedawca usług – uprawniony podmiot, który sprzedaje usługi telekomunikacyjne świadczone przez operatorów,
18) telekomunikacja – nadawanie, odbiór oraz transmisja pomiędzy zakończeniami sieci wybranymi przez użytkownika informacji jakiejkolwiek natury, a w szczególności znaków, pisma, obrazów i dźwięków, za pomocą fal radiowych bądź optycznych lub urządzeń wykorzystujących energię elektromagnetyczną,
21) usługa (telekomunikacyjna) – działalność gospodarcza polegająca na zapewnianiu telekomunikacji,
28) zakończenie sieci – punkt sieci praeznaczony do dołączenia urządzenia końcowego,
20) urządzenie końcowe – urządzenie przeznaczone do dołączenia do zakończenia sieci w celu korzystania z usług lub ich świadczenia."
Dział II: Uprawnienia do prowadzenia działalności telekomunikacyjnej

„Art. 3.

1. Jeżeli ustawa nie stanowi inaczej, prowadzenie działalności polegającej na świadczeniu lub sprzedaży usług telekomunikacyjnych, a także zakładaniu lub używaniu sieci lub urządzeń, z wyłączeniem zakładania lub używania urządzeń radiowych, wymaga posiadania uprawnień określonych ustawą, zwanych dalej „uprawnieniami telekomunikacyjnymi".

...

Art. 4.

1. Nabycie uprawnień do działalności telekomunikacyjnej następuje z mocy ustawy albo na podstawie:
   1) koncesji na świadczenie usług, zwanej dalej „koncesją",
   2) zezwolenia na zakładanie sieci lub urządzeń,
   3) zezwolenia na używanie sieci lub urządzeń,
   zwanych dalej „uprawnieniami telekomunikacyjnymi", albo na podstawie rejestracji działalności.

...

Art. 6.

1. Nie wymaga koncesji świadczenie usług za pomocą urządzeń końcowych dołączonych do zakończeń sieci operatora.
2. Nie wymaga zezwolenia zakładanie lub używanie sieci wewnętrznych oraz urządzeń końcowych.
3. Minister może określić, w drodze rozporządzenia, warunki prowadzenia działalności, o której mowa w ust.2, w szczególności dotyczące jakości świadczenia usług oraz ochrony interesu użytkowników.

..."

„Art. 8.

1. Organem właściwym w sprawach koncesji i zezwoleń jest Prezes Urzędu Regukacji Telekomunikacji, zwany dalej „Prezesem URT"....

Dział III. Świadczenie usług telekomunikacyjnych

„Art. 40.

2. Świadczenie usług odbywa się na podstawie umowy o świadczenie usług. Przy zawieraniu umów o świadczenie usług przestrzega się zasad bezstronności, jawności i niedyskryminacji.
3. Operator nie może uzależniać świadczenia określonej usługi od:
   1) zawarcia przez użytkownika umowy o świadczenie innych usług,
   2) nie zawierania z innym operatorem umowy o świadczeniu usług,
   3) udzielania informacji nie mającej bezpośrednio znaczenia dla należytego świadczenia usługi,
   4) nabycia urządzeń końcowych u określonego dostawcy.
4. Warunki świadczenia usług oraz tryb reklamacyjny określa operator, o ile ustawa nie stanowi inaczej.
5. Minister może określić, w drodze rozporządzenia, wykaz usług oraz zasady ich świadczenia i sprzedaży, a w szczególności wymagania dotyczące:
   1) ogólnych warunków świadczenia usług, w tym – zawierania umów pomiędzy użytkownikiem a operatorem o świadczenie określonych rodzajów usług oraz obowiązkowych składników tych umów,
   2) zawierania umów pomiędzy użytkownikiem a sprzedawcami usług, w tym – obligatoryjnych składników tych umów, zakresu odpowiedzialności sprzedawcy usług wobec użytkownika oraz przypadków, w których zawieranie takich umów jest dopuszczalne,
   3) jakości świadczenia usług,...

Art. 41.

1. Działalność telekomunikacyjna prowadzona w sieciach wewnętrznych nie jest świadczeniem usług.

...”

„Art. 42.

1. Operator jest zobowiązany do rejestracji danych zawierających szczegółowy wykaz usług świadczonych każdemu użytkownikowi, w zakresie umożliwiającym sporządzenie rachunku oraz rozpatrzenie reklamacji.
2. Operator jest zobowiązany do dostarczania użytkownikowi rachunków za wykonane usługi w formie uniemożliwiającej osobom trzecim bezpośredni dostęp do informacji w nich zawartych.
3. ...
4. Operator przechowuje dane, o których mowa w ust.1,

przez co najmniej 12 miesięcy, a w przypadku wniesienia reklamacji przez użytkownika – przez okres niezbędny do rozstrzygnięcia sporu o niewykonanie lub nienależyte wykonanie usługi.

Art. 43.

Właściciel, użytkownik wieczysty, osoba wykonująca zarząd lub użytkowanie oraz samoistny posiadacz nieruchomości mają obowiązek umożliwić osobom, mającym tytuł prawny do korzystania z nieruchomości lub jej części, dostęp do usług świadczonych uzytkownikom sieci publicznych.

Art. 44.

1. Użytkownik ma prawo do zmiany operatora świadczącego usługi. Warunki umów o świadczenie usług nie mogą ograniczać prawa użytkownika do korzystania z tego uprawnienia.

2. Operatorowi nie przysługuje roszczenie od użytkownika z tytułu zmiany operatora przez użytkownika.

...

Art. 48.

1. Operator może zaprzestać świadczenia usługi w drodze jednostronnego rozwiązania umowy, jeżeli użytkownik:
   1) pozostaje w zwłoce z płatnością należności za wykonane usługi, przy czym w przypadku płatności okresowych minimalny okres zwłoki uprawniający do rozwiązania umowy wynosi 30 dni, z zastrz. Art. 55,
   2) uporczywie narusza warunki regulaminu lub umowy,
   3) podejmuje działania utrudniające lub uniemożliwiające świadczenie usług, w szczególności działania wymienione w art. 47 (dołączanie urządzeń zabronionych, zakłócanie pracy sieci, blokowanie łączy lub urządzeń końcowych innego użytkownika przez przesyłanie nie zamówionych przez niego informacji).
2. Rozwiązanie umowy na podstawie ust.1 powinno być poprzedzone wezwaniem do:
   1) zapłaty – z terminem nie krótszym niż 30 dni,
   2) usunięcia innych naruszeń – z terminem nie krótszym niż 7 dni.

Art. 49.

1. Operatorzy mają prawo do swobodnego ustalania cen usług, z uwzględnieniem wymogów określonych ustawą oraz innymi przepisami.

...

Art. 55.

1. Rozwiązanie umowy o świadczenie usług podstawowych z przyczyn określonych w art. 48 ust.1 pkt. 1 następuje po okresie zwłoki nie mniejszym niż 60 dni. W tym okresie operator:
   1) może ograniczyć świadczenie usług, w miarę możliwości stopniowo, w pierwszym rzędzie - –usług nie będących usługami telefonicznymi, usług międzynarodowych oraz usług międzystrefowych,
   2) świadczy usługi, które nie powiększą zadłużenia użytkownika, w tym zapewnia przekazywanie połączeń do użytkownika,
   3) ma obowiązek zapewnienia użytkownikowi bezpłatnych połączeń z jednostkami powołanymi ustawowo do niesienia pomocy oraz innych połączeń bezpłatnych,...

Art. 50.

1. Cena usługi powinna uwzględniać koszty jej świadczenia.
2. Podmiotom posiadającym pozycję dominującą, w rozumieniu art. 52 ust.1 (Prezes URT w porozumieniu z UOKiK ustala wykaz operatorów dominujących), lub których roczny przychód za poprzedni rok kalendarzowy przekroczył 5 milionów ECU, nie wolno:
   1) ustalać ceny usług poniżej uzasadnionych kosztów ich świadczenia,
   2) dotować usługi w jakiejkolwiek formie, w szczególności – przekazywać na ten cel dochody ze świadczenia innych rodzajów usług,
   3) wliczać w ceny usłuh narzuty, nie związane ze świadczeniem tych usług.

...

Art. 9. – patrz obecne przepisy art. 16 ustawy o łączności

„Art. 10.

1. Minister określa w drodze rozporządzenia rodzaje usług lub sieci, dla których liczba koncesji lub zezwoleń jest ograniczana, kierując się zasadą zmniejszania liczby takich usług lub sieci do niezbędnego minimum.

2. Koncesje lub zezwolenia na usługi lub sieci, o których mowa w ust.1, udziela się po przeprowadzeniu przetargu. Przetargi ogłasza i przeprowadza Prezes URT.

6. Prezes URT ustala harmonogram przetargów na każdy rok kalendarzowy, nie później jednak niż do dnia 30 września roku poprzedzającego. Harmonogram może być uzupełniany o dodatkowy przetarg nie później niż 3 miesiące przed ogłoszeniem przetargu.

...

Art. 19.

1. Świadczenie usług, o których mowa w art. 6 ust. 1 i 4, a także działalność prowadzona przez sprzedawców usług podlega rejestracji.

2. Rejestracji działalności, o której mowa w ust. 1, dokonuje Prezes URT w drodze wpisu do rejestru, zwanego „rejestrem telekomunikacyjnym". Rejestr jest jawny.

..."

Pozwolenia, przydziały częstotliwości i promesy

Pozwolenia (art. 22 – 28) dotyczą uprawnień do zakładania i używania urządzeń radiowych (patrz art. 12 ust.1 p. 2 obecnej ustawy o łączności).

Pozwolenie określa (art.24):

1) osobę uprawnioną oraz jej siedzibę,
2) rodzaj urządzenia radiowego,
3) okres ważności.

Może określać ponadto warunki używania urządzenia radiowego. Zawiera także przydział częstotliwości, kanałów lub zakresów częstotliwości, zwany „przydziałem częstotliwości".
Organem właściwym w sprawach pozwoleń jest Prezes Państwowej Agencji Radiokomunikacyjnej (PAR), który w pozwoleniu udziela także przydziału częstotliwości (art. 29).

Prezes URT oraz Przewodniczący KRRiTV mogą udzielić promesy przydziału częstotliwości (art. 32 – 33) odpowiednio w zezwoleniu na używanie sieci lub urządzeń, udzielonym wraz z koncesją, jeżeli charakter usług świadczonych w tej sieci wymaga wykorzystywania częstotliwości (Prezes URT), lub w koncesji na rozpowszechnianie lub rozprowadzanie programów radiofonicznych lub telewizyjnych (Przewodniczący KRRiTV).

SIEĆ 2000

Seminarium „Miedzeszyn'98"
12 – 14 maja 1998r.
„Nowe prawo telekomunikacyjne"

Wojciech Hałka

Harmonogram prac:

1. Rezolucja Sejmu R.P. (marzec 1996 r.):

Rząd przedstawi projekt nowej ustawy o łączności do końca 1997 r.

2. Ministerstwo Łączności:

- Decyzja o opracowaniu projektów odrębnych ustaw „Prawo telekomunikacyjne" i „Prawo pocztowe"
- Powołanie Zespołów Sterujących i zlecenie prac do Instytutu Łączności (czerwiec 1996r.)

3. Dwa autorskie projekty „Prawa telekomunikacyjnego":
- prof. dr hab. Stanisława Piątka (UW)
- zespołu mgr Marcina Jakubowskiego, mgr Andrzeja Kaczorowskiego i mgr inż. Piotra Rutkowskiego

4. Projekt jednolity przedłożony do publicznej konsultacji:
15 marca 1998r. (www@ ml.gov.pl)

5. Zgłaszanie uwag: do 15 kwietnia 1998 r.

6. Opracowanie uwag i uzgodnienie międzyresortowe projektu: czerwiec 1998 r. (?)

7. Przedłożenie projektu do Sejmu: lipiec – sierpień 1998r. (?)

8. Uchwalenie projektu przez Sejm: (?)

Dział I: Przepisy ogólne

„Art. 1.

1. Ustawa określa zasady prowadzenia, regulacji i kontroli działalności w dziedzinie telekomunikacji.
2. Celem ustawy jest stworzenie warunków dla zwiększenia dostępności usług telekomunikacyjnych przez równomierny rozwój infrastruktury telekomunikacyjnej oraz stworzenie konkurencyjnego rynku tych usług, przy uwzględnieniu ochrony interesów użytkownika, uzasadnionych potrzeb gospodarki, a także bezpieczeństwa i obronności gospodarki."

maksymalnej szybkości do 56 kb/s i transmisja w tym standardzie uruchomiona została w lutym dla warszawskiej strefy numeracyjnej.

Koszty eksploatacji sieci POLPAK-T i zasady taryfikacji.

Zasadniczymi pozycjami kosztów eksploatacji sieci POLPAK-T są:
1. Amortyzacja węzłów sieci., ok. 50 %
2.Opłaty za łącza międzywęzłowe i międzynarodowe, ok. 20 %
3. Wynagrodzenia 20%,
4. Inne koszty 10 %

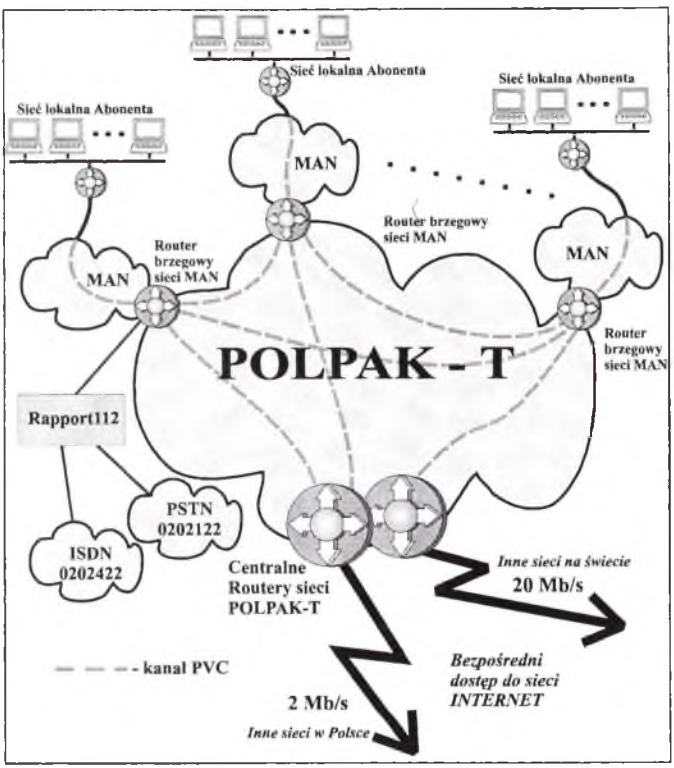
Struktura kosztów wskazuje na konieczność optymalnego planowania topologii i wymiarów sieci. Założeniem przyjętym od początku realizacji inwestycji była jej opłacalność. Z tego powodu bardzo ostrożnie zwiększano przepływności łączy międzywęzłowych. Zainstalowane węzły mogą pracować z łączami 155 Mb/s. Od strony ekonomicznej było by to nieuzasadnione.
Konstrukcję cennika oparto o koszty eksploatacji sieci przy założeniu, że Klient otrzymuje do wykorzystania zasoby sieci i za nie ponosi opłaty. Płaci więc przede wszystkim za wykorzystane zasoby sprzętowe: porty, modemy, łącza dostępowe i udział w przepływnościach łączy międzywęzłowych oraz międzynarodowych. Nie płaci zaś, za ilość przesłanej informacji. W cenniku znajduje to odzwierciedlenie w postaci opłat abonamentowych za uzyskanie szybkości transmisji i opłaty za gwarantowaną przepływność (CIR) dla utworzonych stałych połączeń wirtualnych, które są wprost proporcjonalne do długości utworzonego kanału. Górną barierą ograniczającą wysokość opłat ponoszonych przez Klienta jest opłata za łącza dzierżawione. Od dołu wysokość opłat określa opłacalność przedsięwzięcia. Cennik dla usług sieci POLPAK-T wprowadzony został w grudniu 1995 roku i obowiązuje nadal. Mając na uwadze inflację, można stwierdzić że opłaty za usługi transmisji danych w sieci POLPAK-T są coraz niższe.

Nowe usługi.

Telekomunikacja Polska S.A. jest firmą komercyjną i udostępnia te usługi, które mieszczą się w obrębie zainteresowań Klientów. Poza instalacjami pilotowymi w ofercie TP S.A. nie ma technicznych rozwiązań znacznie wyprzedzających chłonność rynku. Bacznie analizowane są poczynania producentów sprzętu, operatorów, dostawców usług transmisji danych i potrzeby Klientów. W 1998 w ofercie Centrum Systemów Teleinformatycznych znajdą się usługi w technologii ATM. Usługi te oparte będą o styk E3 i AAL 3/4 i AAL 5. Sieć POLPAK-T jest technicznie gotowa do świadczenia usługi transmisji wysokiej jakości głosu i obrazu.. Takie możliwości daje również protokół frame relay. Dobrej jakości przesyłanie głosu w sieci transmisji danych jest zadaniem realnym i dla operatora telekomunikacyjnego dysponującego siecią POLPAK-T, którego podstawowym zadaniem jest telefonia głosowa powoduje problemy natury nie technicznej. Dla uniknięcia wewnętrznej konkurencji między usługami o porównywalnej jakości transmisja głosu za pomocą sieci transmisji danych możliwa jest w pakiecie usług telekomunikacyjnych dostarczanych Klientowi np. w celu budowy korporacyjnej sieci telekomunikacyjnej obejmującej całość usług. Wprowadzenie do sprzedaży tej usługi planowane jest na koniec 1998 r. Barierą w rozpowszechnieniu usług szerokopasmowych w tym i ATM jest sieć dostępowa. Wymagana ona istnienia traktów światłowodowych do siedziby Klienta. Innym rozwiązaniem jest stosowanie modemów ADSL, VDSL. Zasięg w tej technologii ograniczony jest do ok. 1-3 km, oraz początkowe stadium rozwoju tych technologii co może stanowić przeszkodę w ich upowszechnieniu..

Dostęp do sieci Internet.

Usługą, której dostępność wywołuje olbrzymie zainteresowanie jest dostęp do sieci Internet. Udostępnienie jej było możliwe po nałożeniu na sieć frame relay warstwy routerowej. Schemat warstwy routerowej przedstawiony jest na rys 2.



Rys 2. Schemat warstwy routerowej sieci POLPAk-T.

Zasadniczymi elementami tej warstwy są ruotery brzegowe zainstalowane w sieciach MAN i routery centralne w Warszawie. Routery te są połączone między sobą stałymi łączami wirtualnymi (PVC) sieci frame relay. Routery centralne dołączone są do międzynarodowej sieci Internet. Telekomunikacja Polska S.A. ma płączenie 2x 2 Mb/s poprzez MCI i 8 x 2 Mb/s porzez Teleglob do USA. Dla ruchu krajowego do sieci NASK eksploatowane jest połączenie o przepływności 2 Mb/s.

Dostęp Klienta do sieci Internet może być zrealizowany przy pomocy łącza stałego i standardowy port frame relay i PVC do routera brzegowego lub z sieci telefonicznej wg protokołu PPP. Do tego celu służą przedstawione na rys 4 urządzenia Rapport 112.

TP S.A. jest zarejestrowanym w RIPE NCC providerem Internetu. Administruje adresami w dwóch domenach tpsa.pl i tpnet.pl.

SIEĆ TRANSMISJI DANYCH DLA POTRZEB KOMERCYJNYCH OFEROWANA PRZEZ TELEKOMUNIKACJĘ POLSKĄ S.A.

Euzebiusz Sowa

Telekomunikacja Polska S.A.- Centrum Systemów Teleinformatycznych
ul Nowogrodzka 47 a. 00 -695 Warszawa

Wprowadzenie

Dziś nikogo już nie trzeba przekonywać, że szybka i niezawodna wymiana informacji, za pomocą sieci transmisji danych stanowi podstawę sukcesu organizacji gospodarczych, naukowych i różnego rodzaju administracji. Wewnętrzne sieci komputerowe LAN stały się nieodzowne dla normalnego funkcjonowania organizacji. Wymiana informacji między jednostkami rozrzuconymi po terenie całego kraju a nierzadko i poza jego granicami zmusza do korzystania z sieci rozległych. Jedną z takich sieci, dających podstawę dla budowy sieci korporacyjnych jest sieć POLPAK-T zbudowana i eksploatowana przez Telekomunikację Polską S.A.,
W wyniku przetargu rozstrzygniętego w połowie września 1995 roku wyłoniono firmę Nortel jako dostawcę sprzętu sieciowego. Podstawowym węzłem komutacyjnym dla sieci wybrano Passport 160. Pozwala on na pracę z protokołem frame realay przy szybkościach od 64 kb/s do 2 Mb/s i ATM z 34 Mb/s, 155 Mb/s Do końca 1995 r zainstalowane zostały 51 węzły typu Passport 160. Wszystkie łącza międzywęzłowe zostały zestawione w oparciu o cyfrowe strumienie o przepływności 2 Mb/s. Budowę a następnie eksploatację sieci POLPAK-T powierzono Centrum Systemów Teleinformatycznych TP S.A.
Usługi które były dostępne w sieci POLPAK-T, to połączenia PVC z protokołem frame relay, i dostęp do Internetu zarówno w oparciu o łącza stałe i komutowane z sieci PSTN poprzez nr 0- 20-21-22. Docelowo taryfą dla dostępu do Internetu miała być taryfa lokalna.
Pierwszych abonentów włączono do sieci w kwietniu 1996 r. Dostęp do Intrnetu przez jednolity numer telefoniczny dla całej Polski uruchomiony został w czerwcu 1996 r.

Sieć POLPAK-T -stan istniejący.

Zainteresowanie usługami sieci frame relay i dostępem do Internetu okazało się tak duże, że w 1996 roku rozpoczęto rozbudowę sieci POLPAK -T do stanu przedstawionego na rys. 1.

1995 r. tylko 19% spośród nich. Około 25% amerykańskich przedsiębiorstw typu „small business" ustanowiło już swą „obecność" w internecie. Podług szacunków IBM, jeszcze w tym wieku ok. 40% amerykańskich przedsiębiorstw będzie prowadzić sprzedaż za pośrednictwem Internetu. Szczególnie istotny jest handel „business-to-business", który w Ameryce w 1997 r. osiągnął wartość 8 mld. dolarów. Opracowanie firmy „Arthur Andersen" przewiduje, że w roku 2000 obroty za pośrednictwem Internetu osiągną wartość 150-600 mld. dolarów.

Podług danych przytoczonych przez Prezydenta Clintona w przemówieniu wygłoszonym 26.02.1998 r., każdego dnia powstaje 1.500.000 stron www - 65.000 na godzinę. Jako przykład gwałtownego wzrostu przedsiębiorstwa Clinton podał księgarnię internetową Amazon.com, która w ciągu 1997 r. sprzedała 6.500.000 książek, zwiększając sprzedaż 10-krotnie. Przytoczył on także szacunki, że w roku 2000 sprzedaż biletów lotniczych poprzez Internet osiągnie wartość 5 mld dolarów, zaś w roku 2002 wartość handlu za pośrednictwem Internetu osiągnie w USA wartość 300 mld. dolarów. Jako kluczowe dla tego - generującego ogólne ożywienie ekonomiczne - rozwoju, uznał Clinton powstrzymanie się od nakładania dyskryminujących podatków na dostęp do Internetu i na handel w Internecie, oraz zapowiedział swoje poparcie dla wdrażania tej idei w skali światowej. Obecnie w Ameryce toczy się batalia o wycofanie podatków stosowanych do Internetu przez analogię z podatkami tyczącymi się tradycyjnej telekomunikacji.

3. Zmiany w IANA.

IANA - Internet Assigned Numbers Authority - pełni rolę centralnego koordynatora Internetu w zakresie wyznaczania parametrów istotnych dla transmisji. Jest utrzymywana przez Information Sciences Institute (ISI) Uniwersytetu Południowej Kalifornii (USC). Wobec organizacji takich jak Internet Society (ISOC) oraz Federal Network Council (FNC) IANA pełni rolę "clearinghouse" w zakresie koordynacji wyznaczania i stosowania parametrów sieciowych, opierając się przy tym na propozycjach Internet Engineering Task Force (IETF). Współpracuje także z regionalnymi organizacjami zajmującymi się koordynacją Internetu takimi jak ARIN w Ameryce, APNIC w rejonie dalekiej Azji i Pacyfiku oraz RIPE w Europie, bliskiej Azji i północnej Afryki. Kieruje nią John Postel.

Jest zrozumiałe, że zmiana charakteru Internetu z sieci „akademickiej" na podstawowe medium służące komercji, wymusi zmiany w strukturze IANA - o rodowodzie silnie „akademickim". Ideą, która przyświeca zapowiedzianym zmianom, jest pełna komercjalizacja Internetu, co wyklucza utrzymywanie organizacji takiej jak IANA przez rząd USA. Punktem wyjścia jest plan opracowany przez Johna Postela, a także idee, które wyraża Ira Magaziner - doradca Prezydenta Clintona w zakresie polityki wobec Internetu - "A Proposal to Improve Technical Management of Internet Names and Adresses"; discussion draft 1/30/98.

Plan przewiduje powołanie organizacji o charakterze "non-profit", która zachowałaby nazwę IANA, a roboczo nawet dotychczasowy zespół techniczny IANA. Ma ona być kontrolowana przez grupę desygnowaną przez:

(a) organizacje regionalne rejestrujące numery IP (aktualnie ARIN, APNIC, RIPE),

(b) organizacje regionalne rejestrujące nazwy domenowe "top level" (aktualnie Network Solutions Inc. w USA w zakresie domeny .com; organizacja ta została wyznaczona przez rząd USA na zasadzie kontraktu, który kończy się w 1998 r.)

(c) organizacje zajmujące się rozwiązaniami technicznymi Internetu (aktualnie IETF)

(d) "użytkownicy" oraz "przemysł"

7.

Cennik NASK przewiduje usługi w zakresie bezpieczeństwa sieci. Realizacja tych usług z przyczyn oczywistych nie jest publicznie rozgłaśniana, tym nie mniej coraz więcej użytkowników i abonentów z niej korzysta. Spodziewamy się, że nadchodząca era handlu poprzez Internet szybko powiększy zapotrzebowanie na te usługi.

8.

Wreszcie w cenniku wprowadzono opłatę za utrzymanie domen. Bardzo szybko rozwijająca się usługa oraz coraz większe koszty związane z utrzymaniem adresów domenowych oraz coraz większy ruch związany z obsługą zapytań o adresy fizyczne skłaniają do wydzielenia tej grupy kosztów.

Warszawa maj 1998 rok.

Nowy cennik i regulamin NASK

Andrzej Zienkiewicz

Naukowa i Akademicka Sieć Komputerowa

1.

Podstawową zmianą w nowym cenniku w stosunku do starego jest wprowadzenie jako podstawowej zasady opłaty zryczałtowanej (kod usługi I). W zasadzie w sieci NASK od wejścia w życie nowego cennika nie będzie mierzyć się ruchu do i od abonenta w celu obliczenia należności za usługi telekomunikacyjne w Internecie. Jak łatwo zauważyć nie będzie się również odróżniać kierunku i miejsca do i z którego ruch przychodzi. Tego rodzaju zmiana wydaje się możliwa po zmianie struktury sieci do czego NASK się od dawna przygotowywał.

Zmiana cennika i zaniechanie pomiarów ruchu Internetowego pozwoli uniknąć wielu sporów i reklamacji, które zwłaszcza w Internecie są trudne do jednoznacznego rozstrzygnięcia. Tak jak cały Internet zasady pomiarów ruchu opierają się na swoistym „gentleman agreement". Wystarczy, że któraś ze stron nie ma zamiaru stosować zasad, mamy do czynienia z przykrymi dla obu stron sporami.

Zmiana zasad naliczania i rozliczania ruchu Internetowego pozwoli rozstrzygnąć jeden z podstawowych dylematów jakim jest rozliczanie międzyoperatorskie. Przy pobieraniu opłat za porty o określonych przepływnościach każdy z operatorów pobiera pełne opłaty za utrzymanie swojej sieci i wobec tego rozliczenia międzyoperatorskie stają się bezprzedmiotowe o ile mamy do czynienia tylko z ruchem do i od abonentów sieci. Tylko w przypadku tranzytu przez sieć NASK do innych operatorów pobierane będą opłaty o charakterze zryczałtowanym.

2.

Jednak rzeczywistość nie pozwala na całkowite odejście od opłat za ruch w Internecie. Dla części abonentów nastawionych na dokładniejszy rachunek opłata za ruch była i jest korzystniejsza. Są również abonenci, dla których przepustowość portu ma istotne znaczenie, a ruch generowany przez nich jest mały. Są wreszcie abonenci korzystający tylko z ruchu lokalnego lub krajowego. Dla tych abonentów średnie traktowanie w ramach ryczałtu jest niekorzystne. Mimo radykalnej obniżki cen abonenci ci mogą według nowego cennika zapłacić więcej. Dla tych abonentów NASK przygotował działania osłonowe.

3.

Prawie równolegle z nowym cennikiem NASK wprowadza nowy regulamin świadczenia usług telekomunikacyjnych. Ten regulamin w stosunku do poprzedniego jest odchudzony w ten sposób, że usunięto z niego szereg regulacji dotyczących w istocie spraw wewnętrznych NASK. Jednocześnie rozwinięto regulacje związane z załatwianiem reklamacji abonenckich oraz dokonano szeregu poprawek kosmetycznych związanych ze zmianami przepisów.

Nadal dużą część regulaminu zajmują definicje potrzebne dla poprawienia jednoznaczności porozumiewania się z klientami, abonentami oraz partnerami NASK.

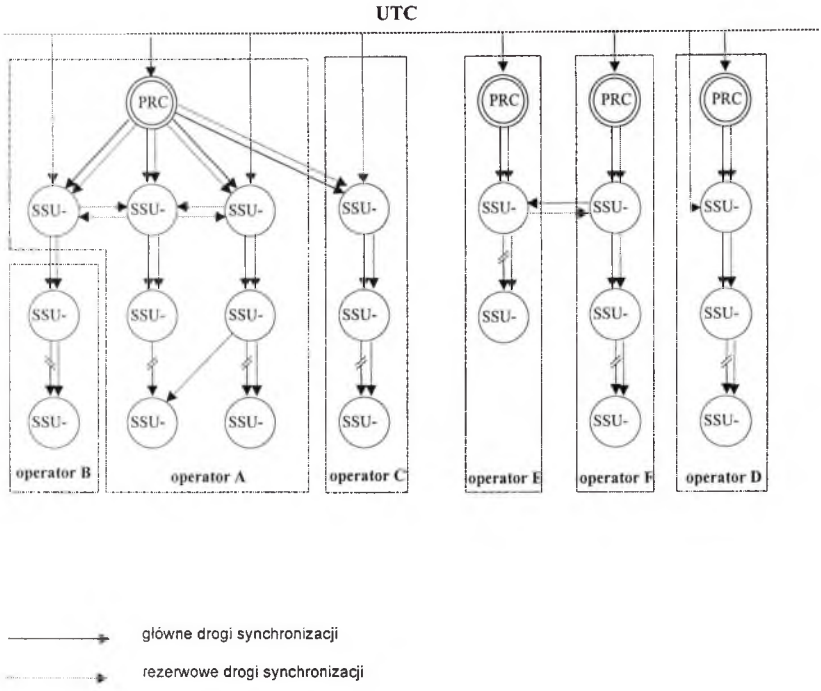
4.

W cenniku umieszczono opłaty za usługi obecnie realizowane na podstawie odrębnych umów z partnerami zagranicznymi (kody usług L, F, S). Zdobyte doświadczenie oraz rozwój tych usług pozwalają na powszechne ich oferowanie. Usługi te obejmują kompleksowe świadczenie usługi dla kooperacji krajowych i zagranicznych. Podane ceny obejmują tworzenie sieci połączeń

- kolejny kanał wirtualny będzie obsługiwał ruch Internetowy akademicki do naszego tradycyjnego partnera NORDUNET'u co wiążę się z mniejszymi kosztami tranzytu i tym samym tańszą oferta dla środowiska naukowo-akademickiego,
- odrębnym kanałem obsługiwani są klienci korporacyjni w ramach usługi FR realizowanej wspólnie z UBN,
- możliwe jest elastyczne tworzenie wydzielonych kanałów stałych lub czasowych dedykowanych dla specyficznych usług bądź grup użytkowników.

Kolejnym elementem jest współpraca z PKP w zakresie współinwestowania w budowę struktury SDH STM-16 (o przepływności 2.4Gb/s). W zamian za wkład inwestycyjny otrzymamy kanał SDH STM-1 (155 Mb/s) w podwójnym pierścieniu przedstawionym na załączonym rysunku. Na taką strukturę transmisyjną nałożona będzie sieć ATM podobnie jak ma to miejsce w relacji Warszawa – Łódź (łącze 34Mb/s). Podobnie jak ma to miejsce w relacji międzynarodowej sieć o takiej technologii umożliwia świadczenie wielu zaawansowanych usług – co więcej jest to jednolita sieć ATM obejmująca swoim zasięgiem sieć metropolitarna w Warszawie, połączenia krajowe i międzynarodowe.

I w końcu następnym istotnym elementem całej struktury jest współpraca z holdingiem NETIA na obszarze działania poszczególnych spółek NETII. Partner ten budujący od podstaw nowoczesną infrastrukturę telekomunikacyjną i świadczący usługi w tym zakresie jest zainteresowany i ma możliwości uzupełnienia wyżej wymienionej struktury szkieletowej w część dostępową wysokiej jakości a przecież w końcowym efekcie usługa sieciowa musi dotrzeć i być realizowana u masowego końcowego użytkownika.



Rys. 4. Przykładowe realizacje sieci synchronizacyjnych

Literatura

1. Dobrogowski A., Jessa M., Kasznia M.: *Podstawy pomiarów parametrów sygnałów i urządzeń synchronizacji sieci telekomunikacyjnej*, Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne nr 6, 1997

2. ITU-T Recommendation: G.803

3. Sexton M., Reid A.: *Broadband Networking: ATM, SDH and SONET*, Artech House, Boston 1997

4. Smith R., Millott L.J.: *Synchronisation and Slip Performance in a Digital Network*, British Telecommunications Engineering, vol. 3, 1984.

5. Instytut Telekomunikacji Politechniki Warszawskiej: *Strategia synchronizacji sieci telekomunikacyjnych na terenie Polski*, 1996

zegarowi PRC. Ponieważ rozwiązanie to jest stosunkowo tanie i proste, to wielu operatorów decyduje się na synchronizowanie swoich sieci w taki w sposób.
System GPS oferuje jeszcze jedną niezwykle istotną cechę z punktu widzenia synchronizacji. Wszystkie satelity wyposażone są we wzorce cezowe, których praca jest koordynowana ze skalą UTC. Wykorzystanie systemu GPS do celów synchronizacji sieci pozwala na zminimalizowanie długości łańcuchów synchronizacyjnych przez co struktura sieci synchronizacyjnej ulega „spłaszczeniu". Relacje fazowe zegarów nawet pomiędzy znacznie od siebie oddalonymi węzłami zostają zachowane na podobnym poziomie. Czynnikiem, który powinien być wzięty pod uwagę przy stosowaniu systemu GPS jest jego podatność na zakłócenia sygnału radiowego.

Dystrybucja sygnałów synchronizacyjnych poprzez sieć SDH

Dla synchronizacji sieci telekomunikacyjnych wykorzystujących systemy teletransmisyjne SDH przyjęto następujące zasady:

- sygnały taktowania są przenoszone pomiędzy urządzeniami poprzez styki STM-N
- sygnały taktowania powinny być odtwarzane bezpośrednio z interfejsu liniowego SDH STM-N
- do synchronizacji powinna być stosowana metoda typu master-slave
- pomiędzy urządzeniami zegarowymi SDH powinny być stosowane zegary SSU w celu odfiltrowania fluktuacji fazy
- liczba elementów SDH oraz liczba zegarów SSU w łańcuchach synchronizacyjnych powinna być ograniczona.

Pętle synchronizacyjne

Pętle synchronizacyjne polegających na tym, że zegar synchronizuje się do własnego sygnału wyjściowego. Takie zjawisko najczęściej może powstać w sytuacji gdy w sieci transmisyjnej następuje uszkodzenie łącza, np. w sieci SDH. Efektem pętli synchronizacyjnej jest powstanie dużej odchyłki częstotliwości zegara (w tym przypadku zegara urządzenia SDH) prowadzącej do wystąpienia dużej ilości operacji wskaźnikowych (a w konsekwencji mogącej doprowadzić do generacji poślizgów). Podobna sytuacja będzie miała miejsce nawet w przypadku, kiedy zegar urządzenia SDH będącego w stanie pętli synchronizacyjnej współpracuje z SSU. Zegar SSU będzie wówczas podążał za zmianami częstotliwości wyjściowej zegara SDH do czasu przekroczenia zakresu chwytania zegara SSU.
Pętle synchronizacyjne są trudne do zlokalizowania, gdyż ich powstanie nie wiąże się z generacją jakiegokolwiek alarmu. Dlatego takie istotne jest zabezpieczenie się przed ich powstawaniem. Następujące sposoby pozwalają zmniejszyć ryzyko powstania pętli synchronizacyjnych:

- dokładne planowanie sieci synchronizacyjnej;
- stosowanie rozproszonej architektury sieci synchronizacyjnej z wieloma głównymi zegarami odniesienia;
- wykorzystanie komunikatów o jakości sygnałów synchronizacyjnych (SSM).

Komunikaty o statusie synchronizacji

Mechanizm SSM jest odpowiednim sposobem zabezpieczania się przed pętlami synchronizacyjnymi w układach pierścieniowych sieci SDH. W sieciach o skomplikowanej strukturze połączeń (np. w sieciach kratowych) SSM nie jest rozwiązaniem całkowicie zabezpieczającym przed pętlami synchronizacyjnymi. Wynika to z braku implementacji tzw.

występują niewielkie fluktuacje fazy. Właśnie w tym zakresie częstotliwości przewidziano pracę dla zegarów podległych.

Synchronizacja sieci szerokopasmowych

Jeżeli do przenoszenia sygnału 2Mbit/s wykorzystywane zostaną systemy SDH to sygnał taki będzie poddany znaczącemu kwantowaniu fazy. Ponadto zawartość harmoniczna fluktuacji fazy wynikających z operacji wskaźnikowych jest usytuowana dokładnie w obszarze, który dotąd był wolny od fluktuacji fazy. Jeszcze gorzej sytuacja wygląda jeżeli do przenoszenia sygnału 2Mbit/s zostaną wykorzystane systemy ATM. Występująca w systemach ATM kwantyzacja fazy o wartości 376 bitów powoduje, że wytwarzane fluktuacje fazy przekraczają o kilka rzędów dopuszczalne wartości dla sygnałów synchronizacyjnych. Dlatego powstała konieczność zdefiniowania na nowo sieci synchronizacyjnej obejmującej wymagania dla sieci PSTN/ISDN, sieci ATM oraz sieci SDH.
Uwzględnione zostały następujące czynniki:

- funkcjonalność wielu sieci oraz wielu nowych elementów sieciowych wymaga wysokiej jakości sieci synchronizacyjnej
- parametry zegarów w trybie podtrzymania, poziom szumów zegarów, wolnozmienne fluktuacje fazy oraz poślizgi są ważnymi parametrami, które powinny być kontrolowane w sieci synchronizacyjnej
- wzrost liczby operatorów w jednym kraju, poza tym ci sami operatorzy działają w kilku krajach
- dystrybucja synchronizacji powinna zapewniać możliwość monitorowania jakości we wszystkich węzłach sieci.

Doprowadziło to do zdefiniowania nowych funkcji w elementach sieci synchronizacyjnej. W nowych sieciach synchronizacyjnych kluczową rolę odgrywają urządzenia zwane wtórnymi źródłami synchronizacji (SSU).
SSU spełniają następujące funkcje:

- wybór synchronizacyjnego źródła odniesienia – wybór źródła jest dokonywany na podstawie analizy jakości sygnału odniesienia doprowadzonego do SSU (w automatycznym trybie pracy wybór wejścia synchronizacyjnego zależy od zdefiniowanych priorytetów, SSU dopuszczają również tryb wymuszonego wyboru wejścia)
- redukcja składników szumu o wysokiej częstotliwości wywołanych fluktuacjami fazowymi i skokami fazy (np. w wyniku przełączania na rezerwę w warstwie transportowej sieci)
- praca w trybie podtrzymania – zapewnienie dostarczania wyjściowych sygnałów synchronizacyjnych w sytuacji utraty wejściowych sygnałów synchronizacyjnych
- dystrybucja sygnałów synchronizacyjnych
- kontrola jakości wejściowych sygnałów synchronizacyjnych
- funkcje zarządzania – zmiany wejść synchronizacyjnych, zmiana konfiguracji, rejestrowanie zdarzeń.

Wymagania na parametry zegarów SSU zostały zdefiniowane przez ETSI oraz przez ITU-T (rewizja rekomendacji G.812).
Sieci SDH z ich naturalnymi mechanizmami zabezpieczeń sieciowych charakteryzują się znacznie większym dynamizmem w porównaniu z systemami PDH. Jeżeli sieć SDH jest wykorzystywana do dystrybucji synchronizacji to rekonfiguracja wynikająca z odtwarzania połączeń w warstwie transportowej może jednocześnie prowadzić do rekonfiguracja połączeń synchronizacyjnych. W skomplikowanych strukturach teletransmisyjnych mogą wystąpić znaczące różnice w długościach połączeń synchronizacyjnych podstawowych i rezerwowych między zegarem nadrzędnym i

SYNCHRONIZACJA SIECI TELEKOMUNIKACYJNYCH

Roman Kowalski

Netia Telekom S.A., 02-822 Warszawa, ul. Połeczki 13
e-mail: Roman_Kowalski@netia.pl

Artykuł opisuje podstawowe zagadnienia związane z synchronizacją sieci telekomunikacyjnych uwzględniając ewolucję jaka zaszła po wprowadzeniu do sieci teletransmisyjnych systemów SDH.

Wprowadzenie

W przypadku sieci telekomunikacyjnych synchronizacja polega na zapewnieniu zgodności taktowania zegarów znajdujących się w elementach tworzących sieć. Utrzymywanie sieci w stanie synchronizacji jest wymagane ze względu na konieczność zabezpieczenia się przed utratą bądź zniekształceniem informacji.

Ewolucja synchronizacji sieci telekomunikacyjnych

W sieciach analogowych nie było potrzeby zapewniania synchronizacji. Pierwsze systemy teletransmisyjne PCM były używane w sieciach z centralami analogowymi. Każdy system PCM posiadał własny zegar, a jedynym wymaganiem było utrzymywanie poziomu fluktuacji fazowych na tak niskim poziomie by nie doprowadzić do powstania wysokiego poziomu szumów kwantyzacji lub przepełnienia buforów. Wymagania te mogły być spełnione przez proste układy zegarowe.

Poważne zmiany nastąpiły po wprowadzeniu central cyfrowych wykorzystujących komutację kanałów cyfrowych 64kbit/s. Jedyną metodą absorbowania długookresowych różnic częstotliwości pomiędzy zegarami w różnych węzłach takiej sieci jest generowanie poślizgów kontrolowanych, czyli utrata bądź powtórzenie jednego bajtu informacji. Poślizgi nie stanowią dużego problemu dla telefonii analogowej, gdyż kodery mowy nie są czułe na poślizgi w strumieniu danych o ile sprowadzają się one do całych bajtów. Efekt poślizgu jest w takim przypadku słabo zauważalny.
Dla usługi transmisji danych natomiast, skutki poślizgów są o wiele poważniejsze (utrata danych, konieczność powtórzenia transmisji, itd.).
W celu uniknięcia występowania poślizgów należało doprowadzić do sytuacji, w której wszystkie węzły były synchronizowane do tego samego zegara nadrzędnego. Pożądane było również, aby takt zegarowy strumieni 2Mbit/s łączących ze sobą centrale był uniezależniony od zegara urządzenia teletransmisyjnego.
Czynniki te doprowadziły do opracowania wymagań na architekturę sieci synchronizacyjnej oraz metod zwielokrotniania wykorzystywanych w urządzeniach teletransmisyjnych hierarchii plezjochronicznej (PDH).

Na forum międzynarodowym uznano, że wybudowanie jednolitej sieci synchronizacyjnej, w której wszystkie zegary na świecie są synchronizowane do jednego zegara nadrzędnego, jest zadaniem bardzo trudnym do wykonania. Dlatego przyjęto zalecenie określające, że każdy operator narodowy powinien stosować do synchronizacji swojej sieci zegar nadrzędny, tzw. główny zegar odniesienia (*Primary Reference Clock – PRC*), o dużej stabilności częstotliwości i niskim poziomie szumów

13) Po wykonaniu wystąpienia przepływu zarządca informuje o tym fakcie aplikację do komunikacji z użytkownikiem.

14) Aplikacja do komunikacji z użytkownikiem wysyła komunikat rozgłoszeniowy nakazujący przesłanie do niej wyników wykonania zadań.

15) Agent wysyła wynik wykonania zadania do programu do komunikacji z użytkownikiem. Jeśli dane zadanie nie było uruchomiane to odpowiedzi na komunikat „MSG_GIVE_ME_RESULT" w imieniu agenta zadania udziela zarządca przepływu.

16) patrz punkt 15).

17) Po odebraniu wyników wykonania wystąpienia przepływu pracy od wszystkich agentów zadań program do komunikacji z użytkownikiem wysyła do zarządcy przepływu komunikat nakazujący zakończenie pracy i sam kończy pracę odłączając się od grupy komunikacyjnej PVM.

18) i 19) Zarządca przepływu pracy wysyła komunikat nakazujący zakończenie pracy do wszystkich agentów zadań i sam kończy pracę odłączając się od bazy danych i grupy komunikacyjnej PVM. Każdy z agentów po odebraniu tego komunikatu również odłącza się od bazy danych (wywołując funkcję *close* z biblioteki XA).

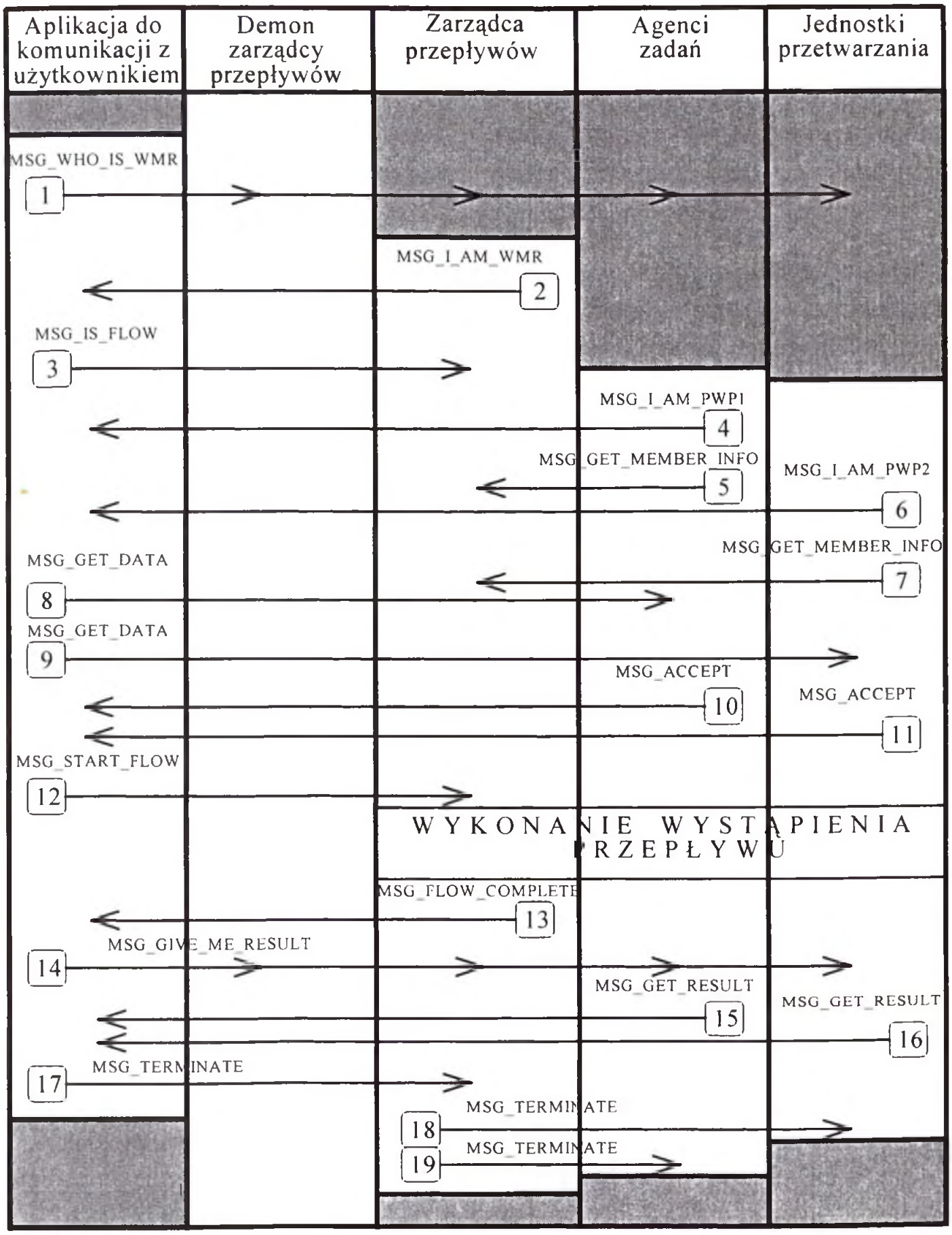
Na uwagę zasługuje zachowanie zarządcy przepływu pracy po odebraniu komunikatu „MSG_IS_FLOW" (opisane w punkcie 3)). Przyjęcie takiego rozwiązania ma bardzo istotną zaletę, a mianowicie najdłużej trwające operacje: przyłączanie się do bazy danych i wprowadzanie parametrów wystąpienia przepływu przez użytkownika, wykonywane są w tym samym czasie. Skraca to czas od momentu wprowadzenia przez użytkownika parametrów do momentu otrzymania wyników wykonania wystąpienia przepływu pracy.

5. Podsumowanie.

W pracy przedstawiono prototyp systemu, którego architektura umożliwia wykonywanie wystąpień przepływów określonych typów i spełnia podane na wstępie założenia. Oceniając jakość zarządzania wykonywaniem przepływów można mieć na uwadze dwa jej aspekty. Pierwszy to ograniczenia wynikające z architektury aplikacji, a drugi to ograniczenia wynikające z zasad działania zarządcy przepływów pracy.

Odnośnie ograniczeń wynikających z architektury aplikacji to głównym powodem rezygnacji z rozwiązania alternatywnego był fakt, że rozwiązanie to powodowałoby zbyt duże obciążenie zarządcy przepływu pracy, który pełniłby funkcję nie tylko zarządcę wykonywanych przepływów, ale byłby też bezpośrednio uwikłany w wykonanie każdej instrukcji SQL wchodzącej w skład jakiegokolwiek zadania. Ponadto, przyjęcie tego rozwiązania uniemożliwiałoby współbieżne wykonywanie operacji wchodzących w skład kilku zadań. W zaimplementowanym rozwiązaniu możliwość współbieżnego wykonania operacji wchodzących w skład kilku zadań zależy tylko od struktury przepływu pracy i o ile struktura nie ogranicza takiego wykonania, to operacje wchodzące w skład kilku zadań mogą wykonywać się współbieżnie. Wprawdzie zaimplementowane rozwiązanie zwiększa ilość komunikatów w systemie, ale liczba ta jest liniowo zależna od liczby zadań. Z drugiej strony proponowane w rozwiązaniu alternatywnym przesyłanie instrukcji SQL między dwoma komponentami systemu mogłoby być bardziej uciążliwe dla systemu, w związku z dużą liczbą i długością tych instrukcji, niż przesłanie kilku krótkich komunikatów, jak ma to miejsce w zaimplementowanym rozwiązaniu.

Ograniczeniem algorytmu zarządcy przepływów pracy może być stosunkowo długie blokowanie zasobów. Wynika to z faktu, że każde z uruchomionych zadań oczekuje na sygnał zatwierdzenia lub odrzucenia operacji wchodzących w skład zadania do momentu zakończenia wykonywania przepływu



Rys. 6 Zasady współdziałania elementów systemu

zarządcy przepływów. Pozwala to na wykonywanie przepływów pracy w środowisku heterogenicznym i rozproszonym.

Interfejs XA jest dwukierunkowym interfejsem pomiędzy koordynatorem transakcji a koordynatorem zasobów. Nie jest to zwykły interfejs API (ang. Application Programming Interface), ale interfejs na poziomie systemowym pomiędzy programowymi komponentami modelu DTP (ang. Distributed Transactional Processing). Model DTP definiuje programową architekturę, która pozwala różnym programom aplikacyjnym współdzielić zasoby dostarczane przez różnych koordynatorów zasobów i pozwala na to by wykonywane przez nich zadania były koordynowane w rozproszonej transakcji.

Interfejs XA w aplikacji zarządzającej wykonaniem transakcji powiązanych został wykorzystany do:

- otwierania i zamykania zasobów bazy danych;
- informowania koordynatora zasobów o rozpoczynaniu i kończeniu wykonywania operacji wchodzących w skład zadań;
- zatwierdzania lub wycofywania zadań wchodzących w skład wykonywanego przepływu pracy.

3.2.2 Interfejs do obsługi procesów PVM

PVM jest rozproszonym systemem operacyjnym, który umożliwia zarządzanie zasobami wielu heterogenicznych systemów komputerowych. Na każdym z wykorzystywanych komputerów można uruchamiać posiadać wiele procesorów ze współdzieloną pamięcią. Komputery te mogą być połączone za pośrednictwem różnych typów sieci, na przykład Ethernet czy FDDI. W strukturze prototypu systemu zarządzania przepływami pracy PVM wykorzystany został do zapewnienia komunikacji między poszczególnymi komponentami systemu. Komunikacja ta ma na celu:

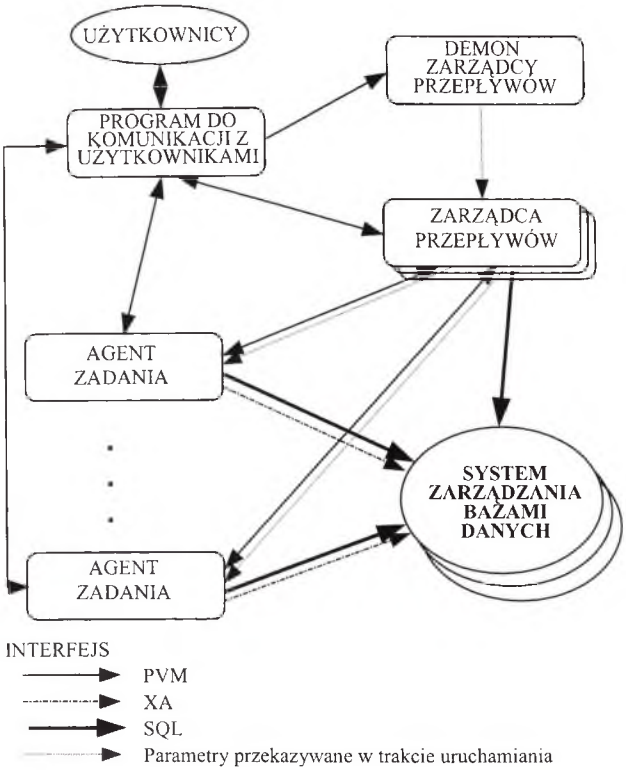
- przekazywanie parametrów istotnych dla prawidłowego wykonania wystąpienia przepływu (na przykład dane dla agentów zadań);
- przekazywanie informacji służących do zarządzania transakcjami (polecenia wydawane przez zarządcę przepływu do agentów zadań);
- zapewnienie synchronizacji i odpowiedniej kolejności wykonywania operacji związanych z wykonaniem wystąpienia przepływu, np.: komunikaty związane z wykonywaniem na bazie danych operacji wchodzących w skład zadań mogą zostać nadane dopiero po otrzymaniu przez agentów zadań parametrów związanych z danym wystąpieniem przepływu.

3.2.3 Interfejs do zasobów informacyjnych baz danych

Interfejs ten jest programowym interfejsem języka dostępu da bazy danych SQL. Instrukcje języka SQL są *zanurzane* w programie źródłowym napisanym za pomocą klasycznego języka programowania, takiego jak Pascal lub C. Interfejs pozwala na przedkładanie instrukcji SQL systemom zarządzania bazami danych: ich analizę składniową, wykonanie i odbierania wyników zapytań.

3.2.4 Przekazywanie parametrów w trakcie uruchamiania programu

Przekazywanie parametrów w trakcie uruchamiania programu polega na stworzeniu procesu potomnego przez program przekazujący parametry i uruchomieniu w ramach tego procesu odpowiedniego programu z odpowiednią ilością i wartością parametrów. W ten sposób są



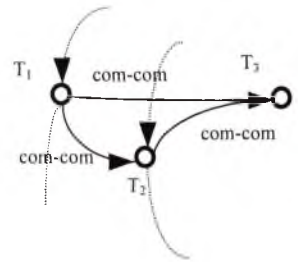
Rys. 5 Architektura systemu zarządzania przepływami pracy

3.1 Zadania poszczególnych elementów systemu

3.1.1 Program do komunikacji z użytkownikami

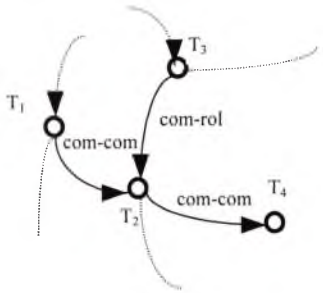
Jest to element systemu odpowiedzialny za interakcję z użytkownikami. Interakcja z użytkownikiem w trakcie wykonania jednego wystąpienia przepływu pracy przebiega w następujący sposób:

1) program do komunikacji oczekuje na sygnał od użytkownika oznaczający przedłożenie przepływu do realizacji (ten punkt można pominąć - takim sygnałem może być samo uruchomienie tego programu);
2) program oczekuje na wprowadzenie parametrów wejściowych dla danego przepływu;
3) po wykonaniu wystąpienia przepływu i odebraniu za pośrednictwem agentów zadań przekazanych przez nie wyników, program informuje użytkownika o wynikach wykonania wystąpienia przepływu pracy.



Rys. 2 Fragment B grafu modelującego przepływ.

W trakcie modelowania struktury przepływów pracy należy zwrócić również uwagę na to, żeby do jednego wierzchołka w grafie nie dochodziły z jednej strony krawędzie nakazujące wycofanie zadania przypisanego do tego wierzchołka („com-rol" i „rol-rol"), a z drugiej strony krawędzie nakazujące zatwierdzenie zadania przypisanego do tego wierzchołka („com-com" i „rol-com"). Fragment grafu przedstawiającego taką błędną sytuację przedstawiono na rysunku poniżej.



Rys. 3 Fragment B błędnego grafu modelu przepływu.

2.2 Przykład modelowania struktury przepływu pracy

Przedstawiony poniżej graf modeluje strukturę przepływu pracy, którego celem jest zarezerwowanie przelotu samolotem ze Szczecina do Krakowa, z przesiadką w Poznaniu z zachowaniem poniższych założeń:

Wylot z Poznania do Krakowa powinien nastąpić tego samego dnia co przylot do Poznania.

1) Jeśli odlot tego samego dnia nie jest możliwy, to należy zarezerwować miejsce w jednym z dwóch dostępnych hoteli („Jowisz" lub „Merkury").
2) Jeśli możliwa jest rezerwacja miejsca w obydwu hotelach, to należy dokonać rezerwacji w hotelu „Jowisz".
3) Jeśli udało się dokonać rezerwacji miejsca w hotelu, to odlot z Poznania do Krakowa powinien nastąpić następnego dnia.

Dodatkowo na zadania wchodzące w skład tego przepływu nałożone są następujące ograniczenia:

1) Rezerwacja odlotu z Poznania do Krakowa na ten sam dzień co przylot może mieć miejsce, jeśli jest możliwe dokonanie rezerwacji ze Szczecina do Poznania.

2. Modelowanie struktury przepływów pracy

2.1 Elementy specyfikacji struktury przepływów pracy

Struktura przepływu pracy jest definiowana za pomocą acyklicznego grafu skierowanego. Graf ten jest zapisywany w bazie danych systemu zarządzania przepływami pracy i jest wykorzystywany przez moduł zarządcy przepływów w czasie realizacji konkretnych wystąpień przepływów. Graf struktury przepływów składa się z wierzchołków, które symbolizują zadania (podtransakcje) wchodzące w skład przepływu oraz krawędzi, które symbolizują zależności między poszczególnymi zadaniami.

2.1.1 Rodzaje wierzchołków w grafie struktury przepływów pracy

Możemy wyróżnić trzy rodzaje wierzchołków:

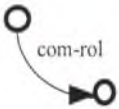
1) Wierzchołki startowe oznaczane na diagramach ⋱ są to wierzchołki, od których rozpoczyna się wykonywanie przepływu. Charakteryzują się one tym, że nie istnieją w grafie krawędzie dochodzące do tych wierzchołków. Przyjęto założenie, że w danym grafie może istnieć co najwyżej jeden wierzchołek startowy.
2) Wierzchołki końcowy, oznaczane na wykresach ○ opisują akceptowalne stany zakończenia przepływów pracy. Jeśli w tym stanie możliwe jest zatwierdzenie przepływu pracy i dochodzi do niego ważna ścieżka to oznacza, że znaleziona została poprawna realizacja przepływu. Jeśli z wierzchołka końcowego wychodzą krawędzie to zarządca przepływu będzie kontynuował wykonywanie wystąpienia aż do wyczerpania możliwości dalszej realizacji.
3) Wierzchołki pośrednie, oznaczane na wykresach ◯ to wierzchołki, które nie są ani końcowe ani początkowe. Oznacza to, że istnieją w grafie takie krawędzie dla których dany wierzchołek jest początkiem oraz istnieją takie krawędzie dla których dany wierzchołek jest końcem.

2.1.2 Rodzaje krawędzi w grafie modelu przepływu

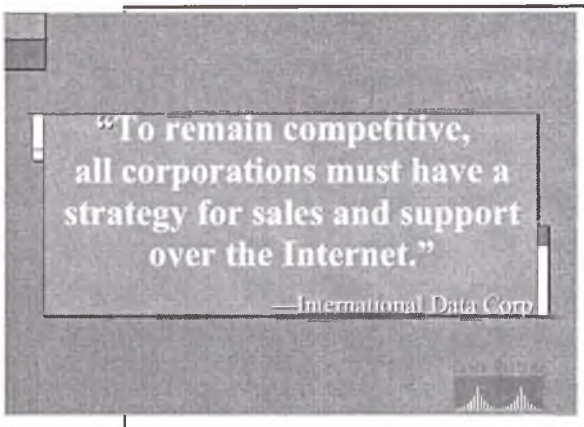
Rodzaje krawędzi symbolizujących zależności między zadaniami:

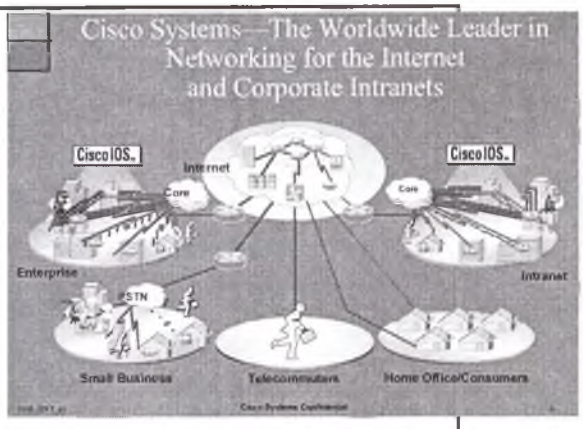
Zależność typu ***commit-begin*** oznacza, że zadanie T_2 może się zacząć, jeśli T_1 może zakończyć się zatwierdzeniem. Krawędzi tego typu są rozpoznawane przez zarządcę przepływu po wartości atrybutu *rodzaj_krawedzi* w relacji *WMR_kraw_mdl*, który w ich przypadku na wartość „com-beg".

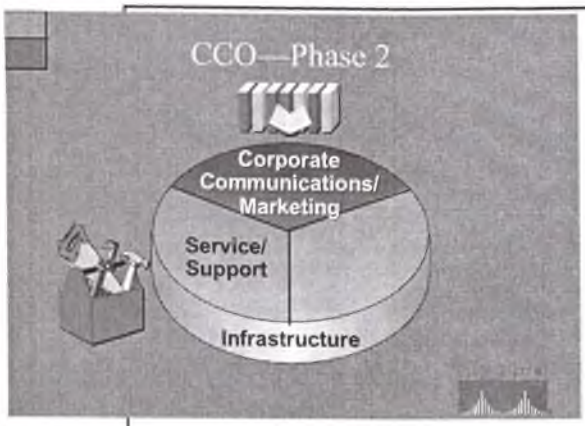
Zależność ***rollback-begin*** oznacza, że zadanie T_2 może się zacząć, jeśli T_1 musi skończyć się wycofaniem. Krawędzi tego typu są rozpoznawane przez zarządcę przepływu po wartości atrybutu *rodzaj_krawedzi* w relacji *WMR_kraw_mdl*, który w ich przypadku na wartość „rol-beg".

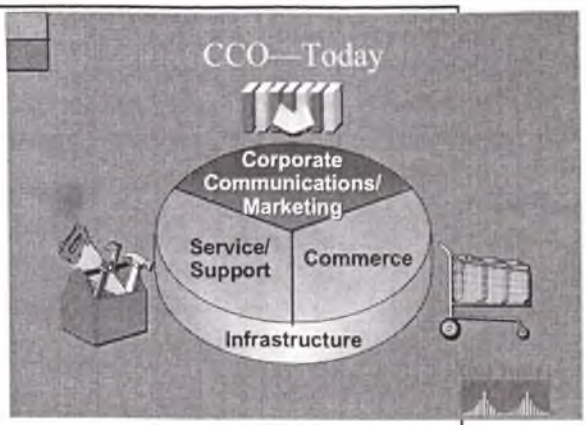


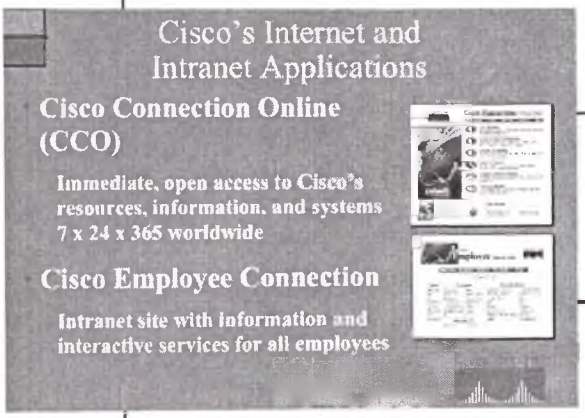
Zależność ***commit-rollback*** oznacza, że jeśli zadanie T_1 może zakończyć się zatwierdzeniem, to zadanie T_2 musi zostać wycofane. Krawędzi tego typu są rozpoznawane przez zarządcę przepływu po wartości atrybutu *rodzaj_krawędzi* w relacji *WMR_kraw_mdl*, który w ich przypadku na wartość „com-rol".

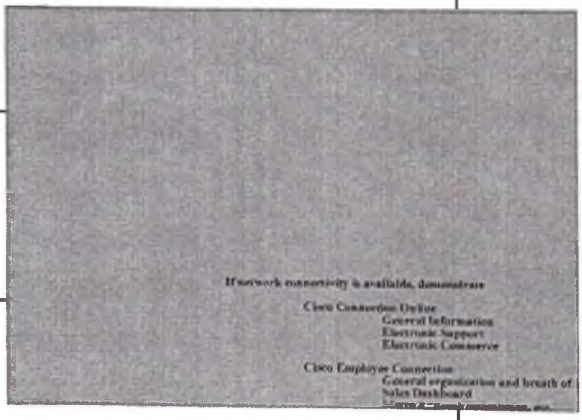

"To remain competitive, all corporations must have a strategy for sales and support over the Internet."
—International Data Corp

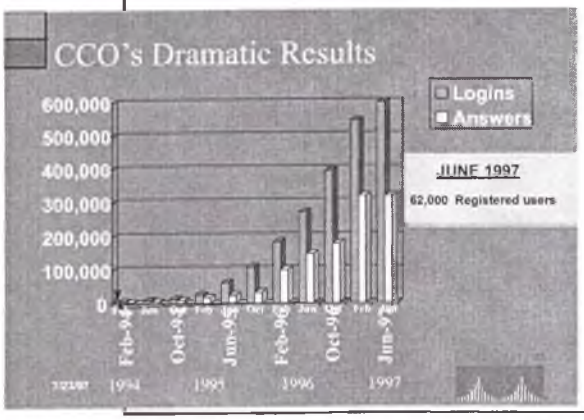

Cisco Systems—The Worldwide Leader in Networking for the Internet and Corporate Intranets
Cisco IOS
Internet
Core
Cisco IOS
Core
Enterprise
Intranet
PSTN
Small Business
Telecommuters
Home Office/Consumers

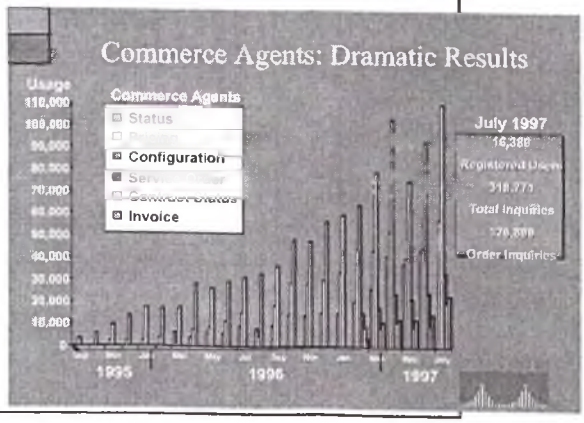

CCO—Phase 2
Corporate Communications/ Marketing
Service/ Support
Infrastructure

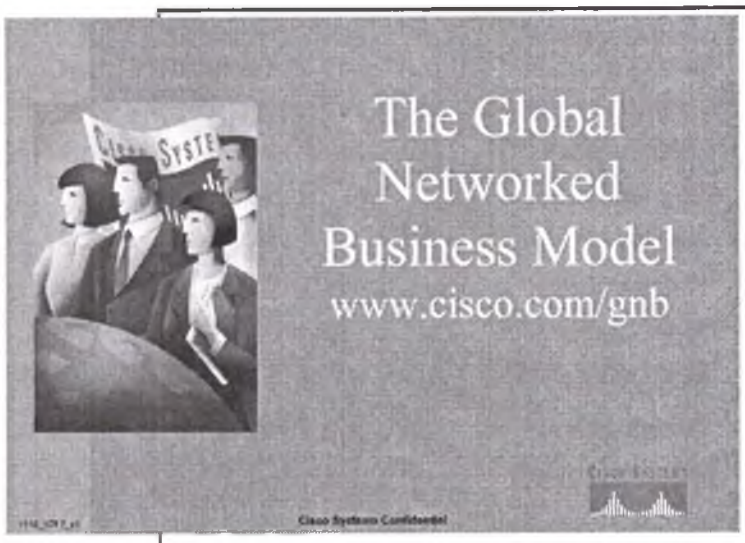

CCO—Today
Corporate Communications/ Marketing
Service/ Support
Commerce
Infrastructure


Cisco's Internet and Intranet Applications
Cisco Connection Online (CCO)
Immediate, open access to Cisco's resources, information, and systems 7 x 24 x 365 worldwide
Cisco Employee Connection
Intranet site with information and interactive services for all employees

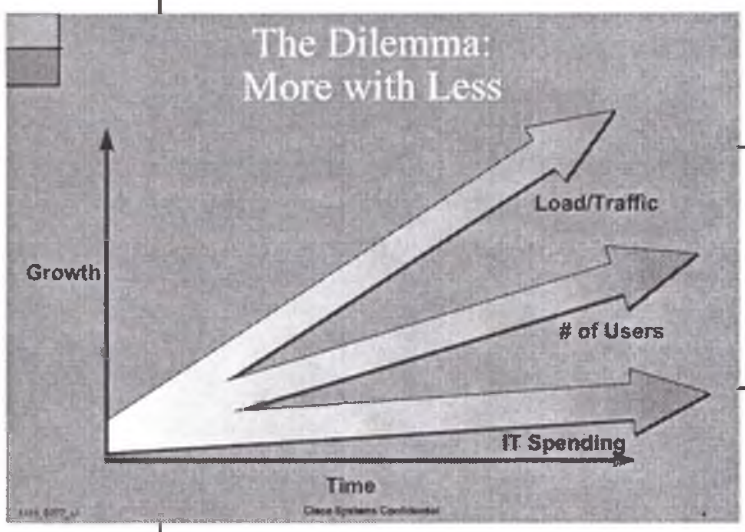


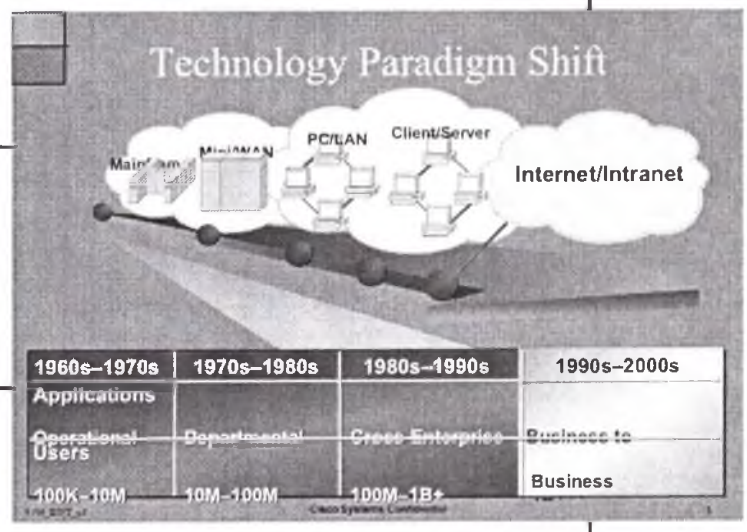

CCO's Dramatic Results
Logins
Answers
600,000
500,000
400,000
300,000
200,000
100,000
0
Feb-94
Oct-94
Jun-95
Feb-96
Oct-96
Jun-97
1994
1995
1996
1997
JUNE 1997
62,000 Registered users

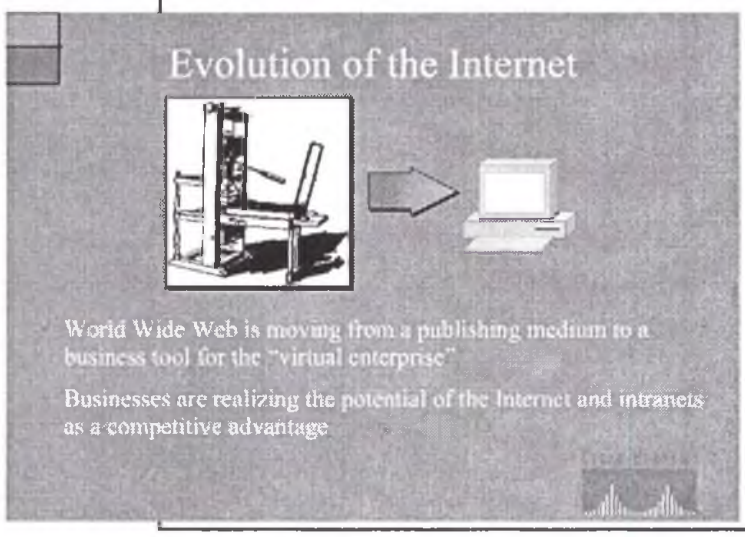

Commerce Agents: Dramatic Results
Usage
Commerce Agents
Status
Configuration
Invoice
July 1997
16,380
Total Inquiries
Order Inquiries
1995
1996
1997

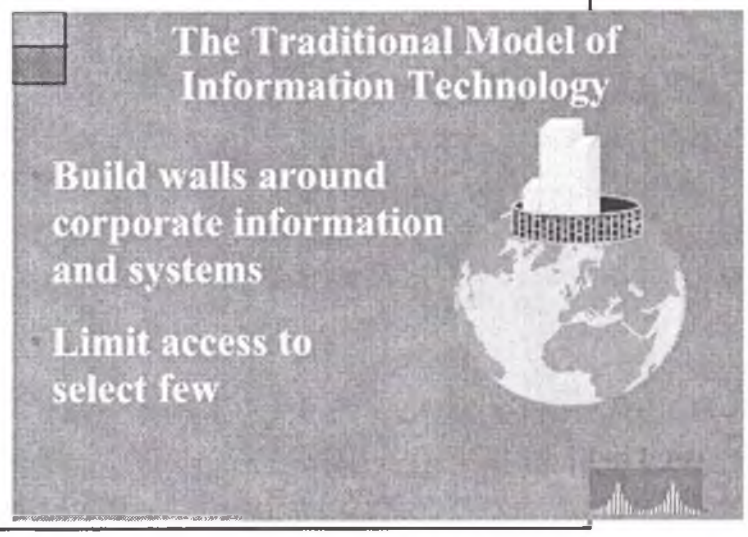

The Global
Networked
Business Model
www.cisco.com/gnb
Cisco Systems Confidential


Businesses Face New Challenges
Global competition
Accelerating pace
Access to information


The Dilemma:
More with Less
Load/Traffic
Growth
# of Users
IT Spending
Time

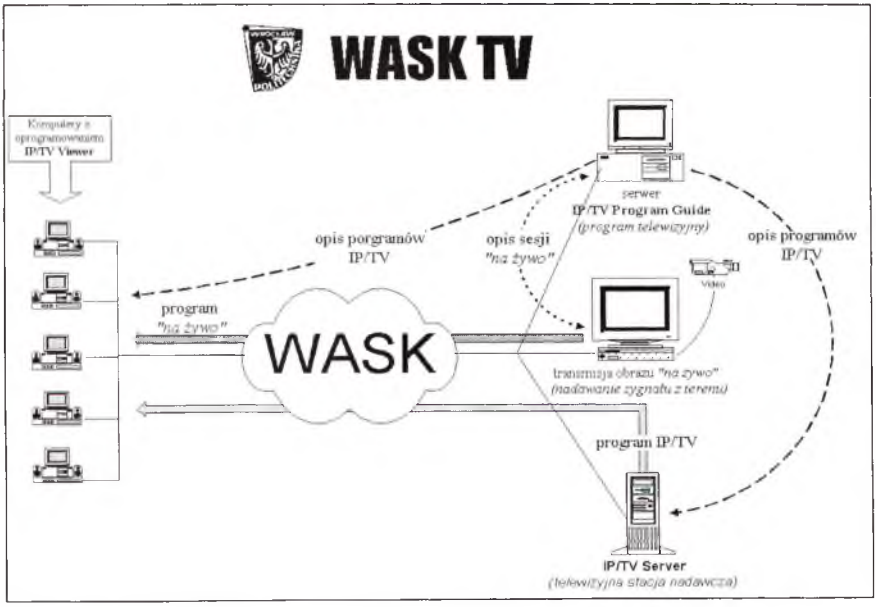

Technology Paradigm Shift
PC/LAN
Client/Server
Internet/Intranet
1960s–1970s
1970s–1980s
1980s–1990s
1990s–2000s
Applications
Operational
Departmental
Cross-Enterprise
Business to
Users
Business
100K–10M
10M–100M
100M–1B+


Evolution of the Internet
World Wide Web is moving from a publishing medium to a business tool for the "virtual enterprise"
Businesses are realizing the potential of the Internet and intranets as a competitive advantage


The Traditional Model of
Information Technology
Build walls around corporate information and systems
Limit access to select few

5. System wideo prawie na życzenie na przykładzie IP/TV

We Wrocławskiej Akademickiej Sieci Komputerowej wdrożono system IP/TV firmy Precept. System ten w założeniach miał być pilotową instalacją w której testowana jest możliwość budowy systemów teleedukacyjnych na bazie sprzętu i stosowanych protokołów w sieci WASK. Podstawowym problemem w realizacji systemów edukacyjnych jest sprawa wykorzystania komputerów o różnych możliwościach i systemach. W testowanym przez nas systemie udało się połączyć w jeden system oprogramowanie stosowane dla celów wideokonferencyjnych w sieci MBONE (VIC i VAT) z oprogramowaniem zaprojektowanym dla komputerów klasy PC z systemem Windows. Obydwa systemy korzystają z tych samych protokołów sieciowych czasu rzeczywistego (RTP). Wspólnym dla obu systemów jest protokół H.261 stosowany do komprymowania sygnałów wizji. W systemie tym transmisja sygnałów na żywo jest realizowana na stacji roboczej Sun ULTRA 1. Serwer programów jest zrealizowany na komputerze z procesorem PENTIUM. Schemat środowiska do realizacji przekazów audiowizualnych z wykorzystaniem techniki transmisji rozsiewczej zaprezentowany został na rysunku 3.



Rys. 3. Struktura systemu IP/TV pracującego w strukturze sieci WASK na Politechnice Wrocławskiej

Sercem systemu jest serwer WWW wyposażony w skrypty napisane w języku Perl wraz ze stronami HTML i grafiką. W przypadku instalacji WASK TV, oprogramowanie *IP/TV Program Guide* pracuje na komputerze Intel Pentium 60 MHz z systemem operacyjnym Linux 2.0.30, wyposażonym w serwer WWW Apache wersji 1.2. i kompilator Perl wersji 5.0. Serwer *IP/TV Program Guide* udostępnia dane o programie w protokole *http* zarówno stacjom będącym serwerami programów (*IP/TV Server*), jak również przeglądarkom (*IP/TV Viewer*), które odpytują serwer WWW zgodnie z zaprogramowanym odstępem czasu. Należy dodać, że o ile jeden *IP/TV*

3. Standardy kodowania sygnału audio

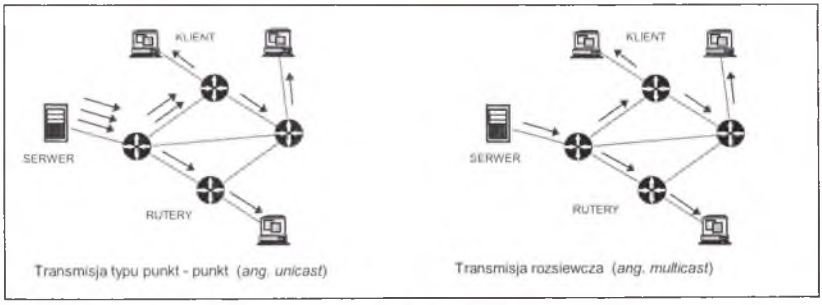
Sygnał audio kodowany jest zgodnie z zaleceniami ITU:

- G.711 - kodowanie sygnału audio w paśmie telefonicznym, 8 bit PCM z krzywą kodowania μ lub A i częstotliwością próbkowania 8 kHz;
- G.722 - kodowanie sygnału audio o paśmie 7 kHz, z wykorzystaniem metody podpasmowego kodowania ADPCM (SB-ADPCM) dla potrzeb transmisji z prędkością 64 kbit/s;
- G.728 - kodowanie sygnału audio w paśmie telefonicznym, dla potrzeb transmisji z prędkością 16 kbit/s z wykorzystaniem kodera LD-CELP (*low-delay code excited linear prediction*);
- G.729 - kodowanie sygnału audio w paśmie telefonicznym, dla potrzeb transmisji z prędkością 8 kbit/s z wykorzystaniem kodera CS-ACELP (*conjugate structure algebraic-code-excited linear-prediction*);
- GSM - schemat kodowania sygnału wykorzystywany w telefonii ruchomej GSM, z wykorzystaniem kodera RPE-LTP (*Regular Pulse Excited LPC with Long Term Predictor*), ze średnią prędkością transmisji 13 kbit/s;
- MPEG Audio - schemat kodowania .

4. Techniki transmisji sygnałów wizji przez sieć z protokołem IP

Przenoszenie sygnałów wizji i dźwięku w sieciach z protokołem IP (*ang. Internet Protocol*) zazwyczaj jest realizowane z wykorzystaniem warstwy transportowej TCP (*ang. Transport Control Protocol*) lub UDP (*ang. User Datagram Protocol*).

Sygnał wizji generuje ruch pakietów o stałym - w trakcie transmisji - natężeniu. Na przykład transmisja programu telewizyjnego o jakości zbliżonej do VHS przy 15 ramkach na sekundę generuje ruch rzędu 1,5 Mb/s. Oznacza to, że o 1,5 Mb/s zmniejsza się przepustowość segmentu sieci w trakcie nadawania programu telewizyjnego. W typowych sieciach lokalnych z protokołem. Ethernet w praktyce możemy wygenerować dwa do trzech strumieni 1,5 Mb/s bez poważnego ograniczenia w ruchu urządzeń realizujących tradycyjną wymianę danych.



Rys. 1. Realizacja transmisji rozsiewczej w sieci pakietowej

Aby informacja, która jest nadawana jednokierunkowo nie była powielana w nowych strumieniach generowanych przez nadajnik stosuje się technikę transmisji rozsiewczej (*ang. multicasting*) (rys. 1). W tym celu wykorzystywana jest klasa D adresów IP. Są to adresy z zakresu od 224.0.0.0 do 239.255.255.255, w których trzy najstarsze bity są ustawione na 1. Adresy z zakresu od 224.0.0.1 do 224.0.0.255 są zarezerwowane jako „dobrze znane" (*ang. well known*) dla realizacji specyficznych usług. Na przykład adres 224.0.0.1 oznacza wszystkie systemy rozsiewcze lub

MOŻLIWOŚCI WDROŻENIA ZDALNYCH SYSTEMÓW EDUKACYJNYCH PRACUJĄCYCH W TRYBIE ON-LINE W SIECIACH MIEJSKICH

Waldemar E. Grzebyk, Jarosław M. Janukiewicz, Tomasz M. Rutkowski *

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

1. Wstęp

Pośród wielu aplikacji określanych przymiotnikiem multimedialne można wyróżnić te, które pozwalają lub są przygotowane do realizacji usług transmisji sygnału wizji i fonii. Oczekiwane zastosowania aplikacji multimedialnych w sieciach komputerowych to:

- telewizja i radio na komputerze biurkowym użytkownika sieci,
- teleedukacja i szkolenia pracowników,
- wideo i audiokonferencje,
- prowadzenie dyskusji z wymianą odręcznych rysunków (*ang. whiteboard*),
- wideo na życzenie,
- dostarczanie danych czasu rzeczywistego (notowania giełdowe).

Można mnożyć zastosowania lecz cechą wspólną aplikacji multimedialnych pracujących w sieciach komputerowych będzie możliwość przesyłania ruchomych obrazów i dźwięku. Systemy multimedialne muszą być zintegrowane z sieciami, które nie były projektowane do przenoszenia ruchu izochronicznego. Wreszcie powinny się charakteryzować możliwością współpracy z innymi systemami. W obecnym stanie rozwoju systemów multimedialnych istnieje wiele programów, które poprawnie realizują usługi multimedialne lecz nie są kompatybilne pomiędzy sobą. Oznacza to, że system wideokonferencyjny pracujący na platformie UNIX'a nie będzie współpracował z aplikacjami pracującymi w systemie Windows'95. Podstawowym problemem nie są protokoły sieciowe lecz sposoby komprymowania sygnału. W niniejszym artykule autorzy przedstawiają wybrane problemy związane z transmisją informacji multimedialnej przez sieci pracujące z protokołem IP. Jako punkt wyjścia przyjmuje się aktualny stan standaryzacji w zakresie wideokonferencji. Jako przykład zdalnego systemu edukacyjnego w sieci Internet lub Intranet przedstawiono w artykule wdrożony we Wrocławskiej Akademickiej Sieci Komputerowej system IP/TV firmy Precept.

2. Standardy kodowania sygnału wideo

Idea połączeń wideokonferencyjnych znalazła swoje odbicie w standardach ITU przygotowanych głównie dla sieci ISDN, która to jako pierwsza pozwalała na przeprowadzanie połączeń wideokonfernecyjnych z wykorzystaniem publicznej sieci telefonicznej (w tym wypadku cyfrowej z integracją usług), wąskie pasmo transmisyjne wymusiło utworzenie algorytmów dobrze komprymujących informację związaną z obrazem przy założeniu pogorszenia jakości. Później standardy te zostały przeniesione do sieci LAN/WAN, gdzie mimo swoich wad są najczęściej wykorzystywane ze względu na niewielkie wymagania i łatwość implementacji. Podstawowym dokumentem opisującym techniczne aspekty przeprowadzania wideokonferencji w sieci ISDN jest zalecenie H.320, które to zostało później rozwinięte do zalecenia H.323, specyfikującego tryb wideokonferencji w sieciach LAN. Połączenie wideo nawiązywane jest bądź bezpośrednio między dwoma terminalami (w przypadku połączenia punkt-punkt) bądź za pośrednictwem serwera MCU (*ang. Multipoint Control Unit*), gdy liczba uczestników konferencji jest większa niż dwa.

* *Instytut Telekomunikacji i Akustyki, Politechniki Wrocławskiej, Wybrzeże Wyspiańskiego 27, 50-327 Wrocław*

4. Zarządzanie w sieci POL-34

Sieć POL-34 jest zarządzana domenowo. Domeny związane są z poszczególnymi grupami usług, np. Internet krajowy, dostęp do kanału zagranicznego, połączenia serwerów bibliotecznych, eksperymenty telematyczne, które budowane są na sieciach wirtualnych. Sieci wirtualne mogą być dedykowane również do obsługi poszczególnych grup badawczych czy rozwiązywanych problemów. Oznacza to, że poszczególne domeny mogą być zarządzane przez różne zespoły. W tym sensie zarządzanie domenowe ma charakter rozproszony. Odnosząc to do sieci POL-34 można wskazać, że zarządzanie siecią podkładową ATM realizuje PCSS, zarządzanie usługami Internetu – MAN Łódź itd.

Urządzenia brzegowe sieci POL-34: węzły ATM Fore ASX1000 i węzły międzysieciowe CISCO 7507 są punktami wymiany między-narodowej. W punktach tych użytkownicy końcowi poprzez sieć miejską (ATM 155/622 Mb/s) maja dostęp do „świata zewnętrznego", tj. wszystkich domen. Z tego punktu widzenia miejskie sieci komputerowe wraz z urządzeniami brzegowymi stanowią odpowiedniki rozproszonych gigaPOP-ów w Internecie2.

Zarządzanie siecią podkładową realizowane jest na bazie platformy zarządzania NetView 6000 i oprogramowania firmowego: NetView 6000 oraz własnych aplikacji do wizualizacji i zarządzania sprzężonych z bazą danych DB2.

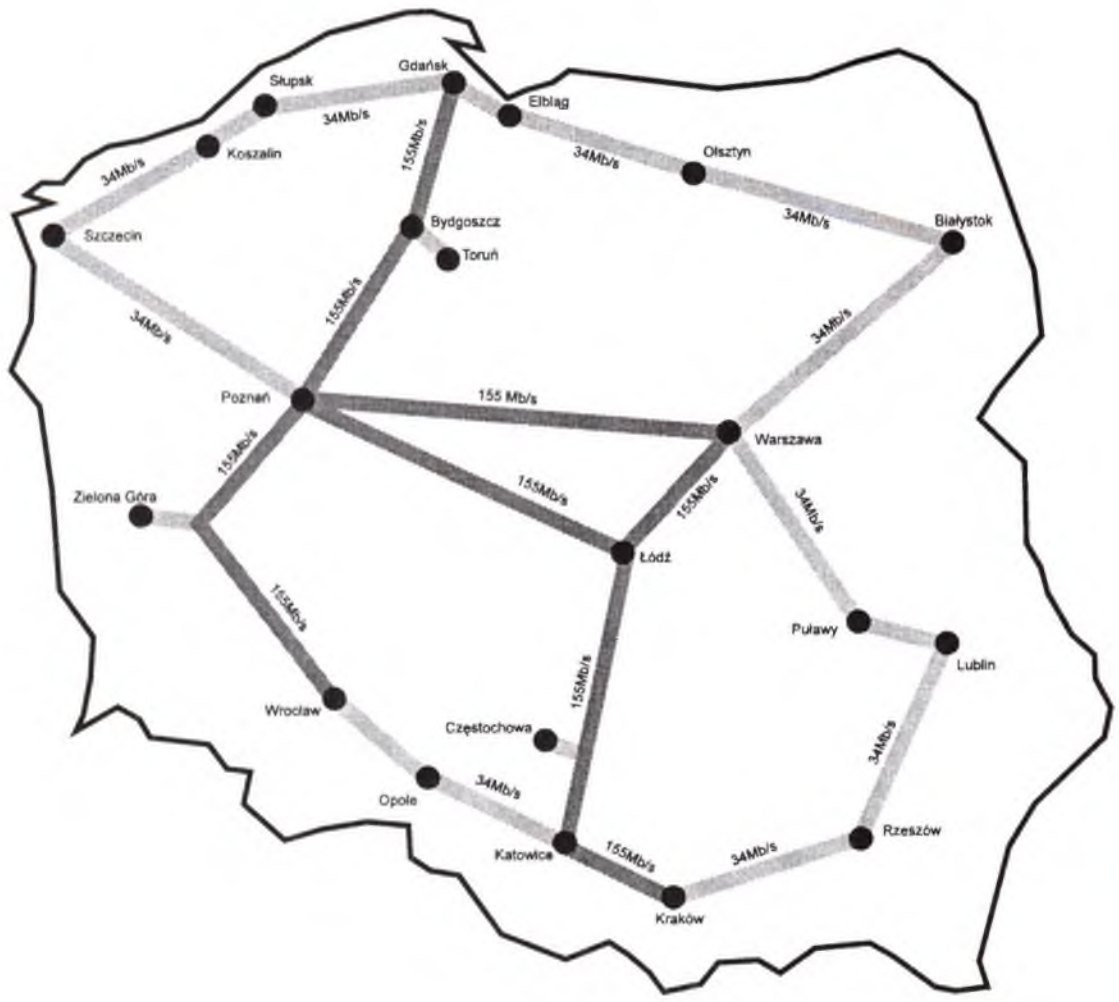
5. Wnioski

Na podstawie dotychczasowych doświadczeń z pracy sieci POL-34 oraz eksperymentów z POL-155 sformułować można kilka wskazówek dla dalszego rozwoju sieci.

1. Dostęp do sieci realizowany będzie w dwóch trybach umownie zwanych: dostępem krajowym ATM (o przepustowościach: 34 Mb/s, 155 Mb/s) i dostępem regionalnym (o przepustowości 2-8 Mb/s) do najbliższego węzła brzegowego MAN-u mającego dostęp krajowy. Docelowo wszystkie MAN-y będą posiadały dostęp krajowy.
   W dostępie do sieci krajowej, po stronie urządzeń ATM, zastosowane są dwa typy interfejsów. Na łączach 34 Mb/s zainstalowane są interfejsy galwaniczne E3, na łączach 155Mb/s interfejsy światłowodowe jednomodowe OC3. Każdy z przyłączy ATM powinien posiadać co najmniej jeden interfejs światłowodowy jednomodowy OC3 do połączenia z przełącznikiem ATM (lub ewentualnie ruterem) odpowiedniej sieci miejskiej.

2. W celu efektywnego wykorzystania budowanej sieci dla usług tradycyjnych oraz eksperymentów z metaprzetwarzaniem i multimediami w sieci POL-34 utworzone zostały sieci wirtualne dedykowane dla tych usług. Uważamy za celowe, utrzymanie sieci wirtualnych. Umożliwi to świadome i dynamiczne alokowanie pasma dla poszczególnych usług sieci. Możliwe jest również precyzyjne określenie kosztu komunikacji w danej usłudze. Aktualnie zestawiono sieci dla trzech rodzajów usług: połączenia w ramach Internetu krajowego, połączenia do Internetu zagranicznego i połączenia dla aplikacji badawczych: multimedialnych i metaprzetwarzania.

4. Sieć POL-34 jest zarządzana domenowo. Zarządzanie domenowe wydaje się najlepszym sposobem na zarządzanie poszczególnymi sieciami wirtualnymi.



Rys.4 Struktura połączeń fizycznych krajowej sieci ATM 34 /155 Mb/s (etap III)

Sieć POL-34 jest połączona z sieciami innych operatorów. Aktualnie zrealizowano połączenie ATM w Warszawie między przełącznikami POL-34 i NASK. Na tym połączeniu wykorzystuje się kanał 4 Mb/s (2 Mb/s dla połączeń krajowych i 2 Mb/s dla połączeń zagranicznych) dla wymiany danych między tymi dwiema sieciami.

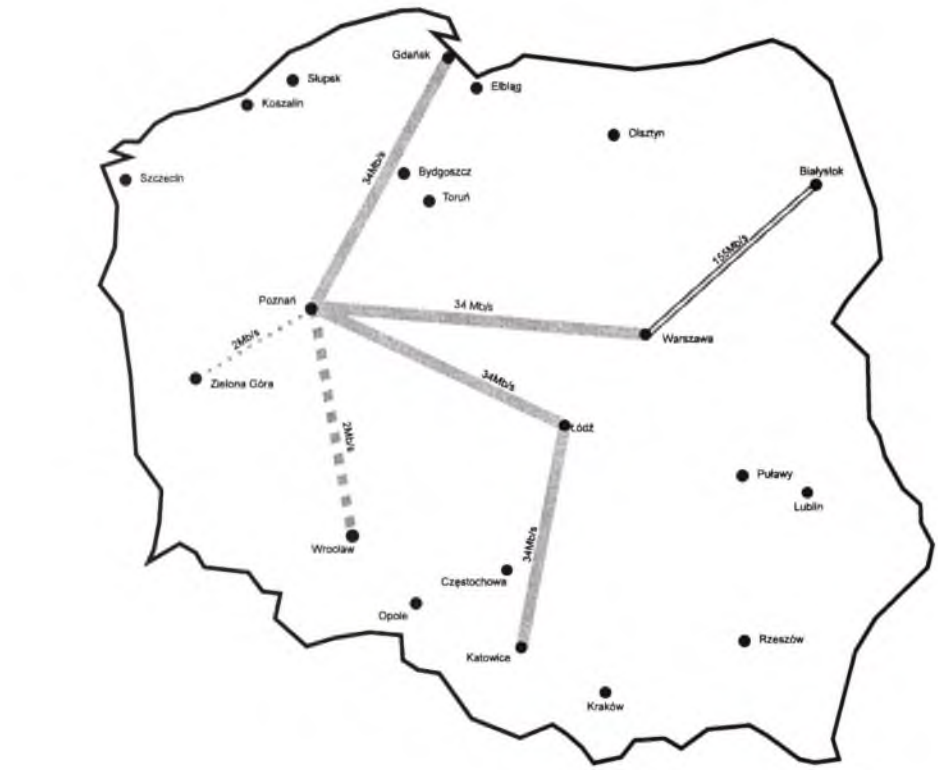
Sieć POL-34 będzie posiadała również niezależne połączenia zagraniczne. Aktualnie trwa instalacja łącza zagranicznego do Internetu światowego o przepustowości: 3 Mb/s do Polski i 1 Mb/s z Polski oraz analogicznego połączenia do krajowego węzła TPNET-u.. Planuje się możliwość skalowania tego połączenia do przepustowości odpowiednio: 6 Mb/s i 2 Mb/s. Rozważane jest także zwiększenie liczby połączeń zagranicznych i dostęp w technice ATM. Punkt dołączenia zlokalizowano w Łodzi. Trwają równocześnie przygotowania do połączenia POL-34 z siecią europejską TEN-34 oraz z sieciami krajów sąsiedzkich.

Szerokie zainteresowanie środowiska naukowego inicjatywą POL-34 i otwartość tej inicjatywy dla nowych uczestników sprawiły, że aktualnie trwają prace zmierzające do rozbudowania sieci w ramach II etapu (rys.3). W tym etapie planuje się przyłączenie do sieci: Krakowa (34 Mb/s), Szczecina (34 Mb/s), Lublina (34 Mb/s), oraz Torunia wraz z Bydgoszczą (34 Mb/s). Połączenie 34 Mb/s otrzyma również Wrocław. Szereg miast uzyska dostęp regionalny: Zielona Góra do Poznania łączem TEL-ENERGO (2 Mb/s), Rzeszów i Puławy do Lublina (2 Mb/s), Olsztyn i Koszalin do Gdańska (2 Mb/s), Częstochowa do Katowic (2 Mb/s).

W 1999 roku planowane jest zakończenie budowy etapu III docelowej struktury sieci POL-34 (rys.4). Podstawą sieci będzie trójkąt połączeń ATM:
Poznań – Warszawa – Łódź z przyłączami do Gdańska, Krakowa i Wrocławia wszystkie o przepustowości 155 Mb/s. Do tego trójkąta będą przylegały cztery pętle ATM pracujące z przepustowością 34 Mb/s:

* Gdańsk – Szczecin – Poznań,
* Wrocław – Opole – Katowice,
* Warszawa – Białystok – Olsztyn – Gdańsk,
* Warszawa – Lublin – Rzeszów – Kraków.

W efekcie realizacji tego etapu wszystkie MAN-y biorące udział w inicjatywie POL-34 otrzymają dostęp ATM do sieci krajowej.



Połączenia w sieci SDH TEL-ENERGO

Połączenia światłowodowe dzierżawione od TEL-ENERGO

Połączenia w sieci SDH PKP

Połączenia w sieci POLPAK-T

Rys.1 Struktura połączeń fizycznych krajowej sieci ATM 34Mb/s (etap I)

SIEĆ POL-34 *

Mścisław Nakonieczny[1], Stanisław Starzak[2], Maciej Stroiński[3], Jan Węglarz[3]

1. Wstęp

Powstała w ostatnich pięciu latach w Polsce nowoczesna infrastruktura informatyczna nauki obejmująca miejskie sieci komputerowe w 20 miastach, zbudowane na własnych kablach światłowodowych i pracujące w technologiach: FDDI (100Mb/s), ATM (155/622 Mb/s) oraz centra komputerów dużej mocy (Gdańsk, Kraków, Poznań, Warszawa, Wrocław) wymaga odpowiedniej infrastruktury połączeń krajowych.

Zakończony sukcesem eksperyment zaprezentowany na między-narodowych targach Informatyki i Telekomunikacji INFOSYSTEM'97 w Poznaniu podczas stowarzyszonej konferencji POLMAN'97 polegający na zbudowaniu heterogenicznej rozległej sieci ATM 34 Mb/s w środowisku telekomunikacyjnym SDH 622 Mb/s operatora TEL-ENERGO, stanowił impuls dla środowiska naukowego oczekującego na możliwość poprawy komunikacji między miejskimi sieciami komputerowymi. Przedstawiona możliwość powiązania nowoczesnej infrastruktury informatycznej nauki z infrastrukturą telekomunikacyjną energetyki uświadomiła równocześnie partnerom z obu tych sfer znaczenie ich współpracy dla rozwoju zastosowań informatyki i telekomunikacji. Stanowiło to podstawę do porozumienia między TEL-ENEGRO a jednostkami wiodącymi-operatorami MAN-ów akademickich w zakresie budowy krajowej, naukowej sieci ATM 34 Mb/s. Sieć ta otrzymała nazwę POL-34. Aktualnie w inicjatywie POL-34 biorą udział następujące MAN-y: MAN Gdańsk, MAN Kraków, MAN Łódź, MAN Poznań, RSK Śląsk, MAN Białystok, MAN Wrocław, MAN Zielona Góra oraz MAN Olsztyn. Oczekiwane jest dołączenie sieci naukowych w Warszawie, MAN Lublin wraz z MAN Puławy i MAN Rzeszów, MAN Toruń wraz z MAN Bydgoszcz oraz MAN Częstochowa.

Sieć POL-34 rozwijana jest z inicjatywy MAN-ów, przy dużym entuzjazmie ich zespołów projektowych i naukowych. Celem tej inicjatywy jest stworzenie nowych możliwości rozwoju powszechnego Internetu, takich jak: połączenie serwerów bibliotecznych, dostęp do krajowych baz danych i krajowych serwerów licencyjnych oraz wytworzenie nowej klasy usług dla nauki, związanych z zastosowaniem multimediów i metaprzetwarzania. Powyższe działania są zgodne koncepcyjnie z inicjatywą amerykańskich uniwersytetów znaną pod nazwą Internet2. Można więc uznać, że jest to polska wersja Internet2.

Półroczna eksploatacja sieci POL-34 nie tylko znacznie poprawiła łączność między MAN-ami, ale pozwoliła rozpocząć eksperymenty z nowymi aplikacjami, np. zdalne rozdzielanie zadań wsadowych systemem LSF (MAN Poznań i MAN Łódź), rozproszony rendering (MAN Gdańsk, MAN Poznań i MAN Łódź). Wspólnie z TEL- ENERGO podjęto również prace wdroże-niowe dla krajowej sieci ATM 155 Mb/s o typologii trójkąta: Gdańsk – Łódź – Poznań z doprowadzeniem do Katowic. W tej sieci trwają aktualnie eksperymenty ze zdalną wizualizacją obliczeń KDM (MAN Gdańsk i MAN Poznań), metaprzetwarzaniem z pakietem GAMESS (MAN Gdańsk, MAN Poznań,

---

* Opracowano na podstawie referatu przygotowanego na konferencj ę POLMAN'98

[1] Centrum Informatyczne TASK, Gdańsk (e-mail: mnak@task.gda.pl)
[2] Centrum Komputerowe, Łódź (e-mail: starzak@man.lodz.pl)
[3] Poznańskie Centrum Superkomputerowo-Sieciowe (stroins | weglarz@man.poznan.pl)

MOŻLIWOŚCI WSPOŁPRACY NETIA - NASK

Koncesje przyznane przez Ministra Łączności limitują zakres działalności Netii do obszarów lokalnych. Oznacza to że Netia ma nowoczesną sieć na obszarach koncesyjnych bez możliwości połączenia tych obszarów ze sobą. NASK jest operatorem transmisji danych i sieci Internet i jego główną bolączką jest sprawa łączy dostępowych do klienta. W pewnej ilości wypadków NASK musiał rezygnować z zestawiania połączenia kablowego do klienta gdyż nie było możliwości uzyskania odpowiedniej jakości przewodów miedzianych. Alternatywą w tym przypadku są drogie rozwiązania radiowe.

Bazując na tych założeniach, podjęliśmy współpracę w zakresie wspólnego świadczenia usług oferowanych przez NASK. Korzyści jakie obie firmy widzą we wzajemnej współpracy to wykorzystanie silnych stron obu firm: ze strony Netii sieci dostępowej i sieci biur obsługi klienta; ze strony NASK infrastruktury szkieletowej oraz wiedzy i doświadczenia. Naszym celem jest kompleksowa obsługa klienta w jak najszerszym zakresie usług teleinformatycznych.

ZAŁOŻENIA PRZYJĘTE PRZY URUCHAMIANIU PROJEKTU PILOTOWEGO W OTWOCKU

Rozpoczęcie współpracy Netia – NASK nastąpiło na początku kwietnia b.r. od próbnego uruchomienia usługi NASKu dostępu do sieci Internet poprzez sieć telefoniczną Netii. Celem tej współpracy jest sprawdzenie, skorygowanie bądź wypracowanie nowych zasad współpracy w zakresie wspólnego świadczenia usług.

Obszar objęty projektem pilotowym to Otwock, Karczew i Celestynów. W obszarze tym mamy ponad 3 000 abonentów z tego około 10% to abonenci biznesowi. W projekcie pilotowym weźmie udział około 50 abonentów Netii którym zapewniona zostanie możliwość korzystania z usługi dostępu do sieci Internet poprzez łącza analogowe, łącza cyfrowe ISDN i łącza stałe. W czasie trwania projektu opłaty pobierane będą jedynie za generowany ruch lokalny z pominięciem opłat instalacyjnych i opłat abonamentowych za dostęp do sieci Internet. Sprzęt potrzebny do podłączenia u abonenta (modemy analogowe 56 kbit/s, karty ISDN, rutery) są wypożyczane bezpłatnie na okres trwania projektu pilotowego. W ramach dostępu do sieci abonent dostaje konto.

Netia i NASK gwarantują wysoki poziom obsługi klienta oraz odpowiednie parametry jakościowe dostępu do sieci Internet:

- odpowiednia ilość abonentów przypadających na jeden port;
- cyfrowe lub analogowe wysokiej jakości łącza dostępowe;
- dużej przepływności łącza szkieletowe i połączenie ze światem.

Biuro Obsługi Klienta w Otwocku przyjmuje i obsługuje zgłoszenia od klientów zainteresowanych uzyskaniem usługi dostępu do sieci Internet. Na miejscu można uzyskać wszystkie informacje dotyczące tej usługi oraz próbnie z niej skorzystać przy pomocy przeznaczonego do tego celów komputera podłączonego do sieci Internet przez ISDN. Wsparcie dla pracowników Biura Obsługi Klienta Netii stanowią pracownicy NASK. Innym sposobem kontaktowania się z klientem są bezpośrednie spotkania w których ze strony operatora biorą udział

Współpraca z instytucjami badawczo-rozwojowymi

Netia widzi możliwość i potrzebę współpracy ze środowiskiem naukowym i akademickim. W trakcie planowania i budowy sieci Netii pojawiają się problemy, które wymagają odpowiednich analiz i opracowań. Większość z tych problemów jesteśmy w stanie rozwiązywać sami lub we współpracy z ekspertami z Telii. Niektóre jednak wymagają pogłębionych studiów i tutaj pojawia się możliwość współpracy z instytucjami naukowymi. Bardzo dobrym przykładem takiej współpracy jest zlecone przez Netię Instytutowi Telekomunikacji Politechniki Warszawskiej opracowanie dotyczące synchronizacji sieci telekomunikacyjnych w Polsce.

Netia w różnym zakresie współpracuje z szeregiem uczelni i instytucji naukowych w Polsce.

Współpraca z Polską Izbą Informatyki i Telekomunikacji

Polska Izba Informatyki i Telekomunikacji zrzesza większość działających w Polsce niezależnych operatorów telekomunikacyjnych. Ostatnio PIIiT aktywnie zajęła się udostępnionym przez Ministra Łączności do publicznej konsultacji projektem ustawy „Prawo telekomunikacyjne". Ze względu na znaczący wpływ obowiązujących uregulowań prawnych na opłacalność i sprawność budowy sieci telekomunikacyjnych wszyscy operatorzy są zainteresowani kształtem nowej ustawy, a PIIiT stała się naturalnym „pośrednikiem" pomiędzy twórcami projektu ustawy i operatorami. Rada PIIiT powołała zespół specjalistów którego zadaniem było wypracowanie opinii nt. projektu ustawy na podstawie uwag zgłoszonych przez poszczególnych jej członków oraz opracowanie propozycji zmian projektu. Praca ta zastała wykonana i przesłana Ministrowi Łączności. Efektem wspólnych działań jest zaproszenie na spotkanie i dyskusję z twórcami projektu ustawy.

Współpraca ze strategicznym akcjonariuszem - Telią AB

Netia w szerokim zakresie współpracuje ze swoim strategicznym akcjonariuszem – szwedzkim operatorem narodowym Telią A.B. Szwecja jest jednym z najlepiej stelefonizowanych krajów na świecie (ponad 70 telefonów stacjonarnych i 30 telefonów komórkowych na 100 mieszkańców). Również wskaźniki jakościowe są na najwyższym światowym poziomie. Telia zatrudnia wielu wysokiej klasy specjalistów mających międzynarodowe doświadczenie. Kadry kierownicze Netii odbywają liczne szkolenia w Szwecji, również liczna grupa ekspertów szwedzkich jest na stałe obecna w Polsce. Współpraca z Telią odbywa się na podstawie wieloletniej umowy o transferze know-how i wsparciu operacyjnym.

Współpraca z administracją państwową i samorządową

Podstawowym organem administracji państwowej z którym współpracuje Netia jest regulator rynku telekomunikacyjnego Minister Łączności. Netia aktywnie stara się uczestniczyć w pracach Ministerstwa Łączności, zarówno w zespołach problemowych (np. w pracach zespołu ds. synchronizacji sieci telekomunikacyjnych) jak i w innych działaniach (np. Netia przedstawiła obszerne uwagi do projektu nowego prawa telekomunikacyjnego).

Netia aktywnie współpracuje z MON i MSWiA w zakresie zarówno świadczenia usług na rzecz wszystkich operatorów specjalnych jak i w zakresie zarządzania systemem telekomunikacyjnym Państwa w sytuacjach kryzysowych.

Większość spółek operatorskich grupy Netia została utworzona przy aktywnym współudziale samorządów lokalnych. Z tego względu Netia ma silne poparcie miast i gmin na obszarach działania spółek operatorskich.

Współpraca z operatorami

TPSA

Spółki operatorskie grupy Netia, podobnie jak i wszyscy inni operatorzy lokalni, z ekonomicznego punktu widzenia są dla TPSA zbiorowym klientem, zapewniającym duże przychody z generowanego ruchu bez konieczności ponoszenia nakładów na budowę sieci oraz jej utrzymanie (czyli praktycznie bezinwestycyjnie).

Wszystkie spółki grupy Netia mają zawarte umowy o współpracy z TPSA. Trzeba stwierdzić, że współpraca w tym zakresie, chociaż nie jest bezproblemowa, układa się coraz lepiej.

Oczywiście istnieje ogromny obszar możliwej (a nawet koniecznej) współpracy TPSA z innymi operatorami. Dotyczy to m.in. standardów technicznych, wdrażania nowych usług i technologii, aparatów publicznych itp. Bardzo cenna byłaby również wymiana doświadczeń w zakresie wdrażania nowych technologii czy nowych usług.

Operatorzy lokalni

Operatorzy lokalni są dla siebie konkurencją w trakcie ubiegania się o nowe koncesje; poza tym są spółkami siostrzanymi borykającymi się z tymi samymi problemami. Podstawową płaszczyzną współpracy powinna być systematyczna wymiana informacji. Powinno zostać wypracowane wspólne stanowisko w sprawie nowego prawa telekomunikacyjnego. Możliwa jest również współpraca organizacyjna i kapitałowa. Prawa rynku doprowadzą do konsolidacji tego segmentu rynku usług telekomunikacyjnych. Pewne zwiastuny tego pozytywnego trendu są już zauważalne.

Operatorzy usług internetowych i transmisji danych

Rynek usług internetowych i transmisji danych rozwija się w Polsce bardzo żywiołowo. Jest już ok. 300 operatorów w tym segmencie rynku. Ze względu na rozdrobnienie, dużą konkurencję, ograniczoną współpracę (zwłaszcza z operatorami działającymi w innych segmentach rynku telekomunikacyjnego) oraz brak niezależnej pełnej infrastruktury technicznej, liczni operatorzy nie mogą w pełni wykorzystać swoich możliwości (dotyczy to głównie operatorów takich jak PKP, Tel-Energo, Telbank czy NASK).

Netia zajmuje komplementarną pozycję w stosunku do tych operatorów: jest mocna tam, gdzie operatorzy rynku danych są najsłabsi, tzn. dysponuje stale rozbudowywanymi sieciami

Literatura

[1] Dorothy Elizabeth Robling Denning „Kryptografia i ochrona danych" WNT 1996
[2] Jerzy Berger „Technologia i technika kryptograficzna" materiały WKTiI 1997
[3] Mirosław Tkaczyk, Marek Protekta „Księga Jakości Jednostki Certyfikującej" BBŁiI UOP 1998,
[4] Mirosław Machalski „Polityka bezpieczeństwa teleinformacyjnego w Rzeczypospolitej Polskiej" Agencja Unia Press, styczeń 1998.

- mocy rozwiązań kryptograficznych;
- skuteczności ochrony elektromagnetycznej;
- tłumienności;
- odporności na nieautoryzowaną penetrację

Certyfikat dopuszczenia jest urzędowym dokumentem gwarantującym, że oceniany przez Laboratorium Badawcze podsystem zabezpieczenia systemu TI odpowiada określonym wymaganiom związanym z zabezpieczeniem systemów teleinformacyjnych w których jest gromadzona, przetwarzana i przesyłana informacja. Wydanie certyfikatu jest uzależnione od uzyskania wcześniej certyfikatów akceptacji na stosowane w systemie urządzenia i oprogramowanie zabezpieczające oraz od pozytywnej oceny polityki zabezpieczeń i jej realizacji w postaci kompleksu metod i środków zabezpieczeń (kryptograficznych, administracyjno-fizycznych, logiczno-komputerowych, emisyjnych i transmisyjnych).

Dodatkowo – wydany certyfikat potwierdza poprawność stosowanych przez Laboratorium metod badawczych i pomiarowych oraz kryteriów oceny.

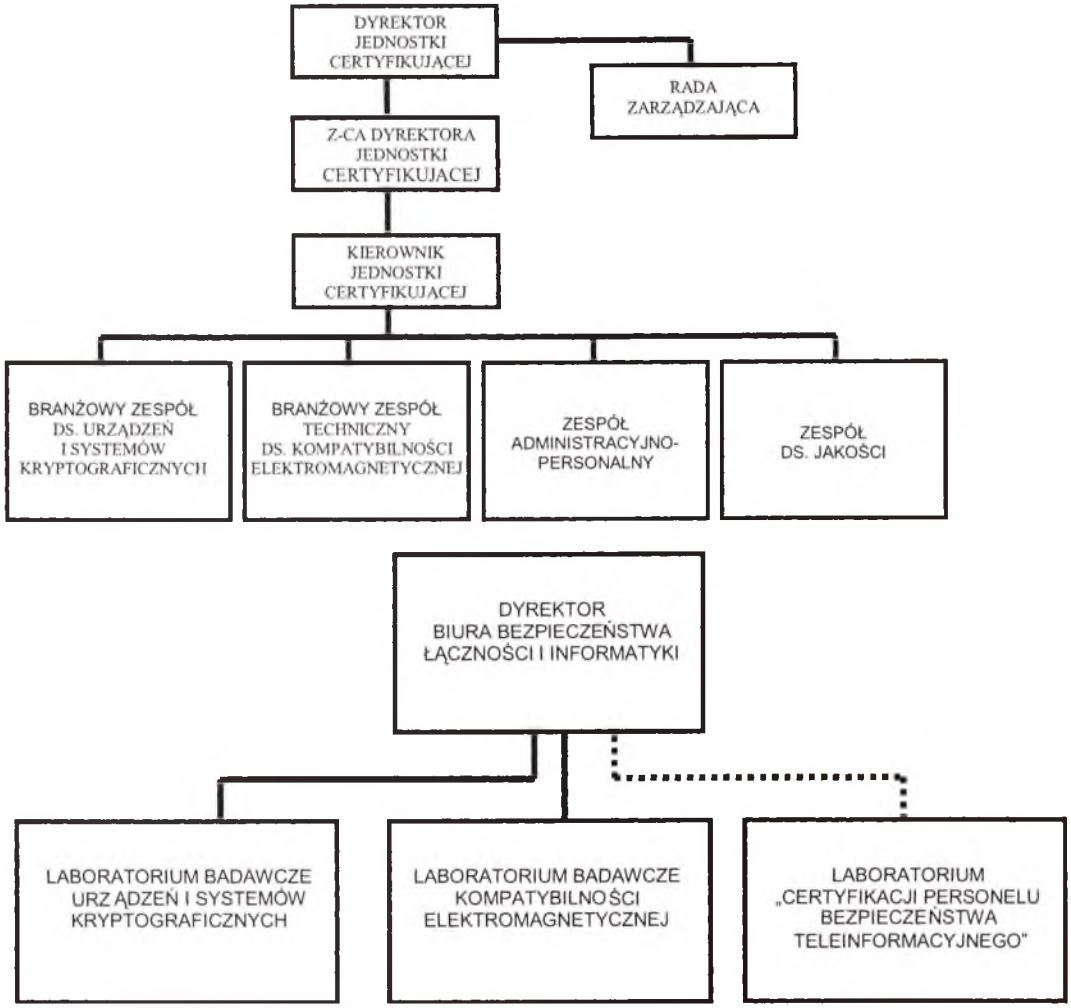
3. 5. Wybrane wymagania stawiane systemom i urządzeniom kryptograficznym (na poziomie informacji „wrażliwych")

Kryptografowie najczęściej uznają wyższość rozwiązań sprzętowych nad programowymi ze względu na większą odporność tych pierwszych na nieuprawnioną penetrację i znacznie wyższą szybkość realizacji funkcji kryptograficznych (możliwość zrealizowania algorytmów na układach ASIC *Application Specific Integrated Circuit*).
Z drugiej strony – rozwiązania programowe są tańsze i łatwiej je modyfikować (co – w konkretnych sytuacjach może być wadą lub zaletą).
Jak zwykle w życiu, optimum należy poszukiwać w okolicy „środka" – najskuteczniejsze są rozwiązania sprzętowo-programowe, łączące zalety obydwu sposobów.
Nie jest to jednak zalecenie uniwersalne, gdyż system kryptograficzny musi być zawsze rozpatrywany i projektowany jako element systemu zabezpieczeń dla konkretnego środowiska teleinformacyjnego.

Rozważając wymagania na system kryptograficzny należy brać pod uwagę:
1. aspekty zabezpieczeń
- odpowiednią do potrzeb moc kryptograficzną;
- bezpieczeństwo i sprawność systemu generacji i dystrybucji kluczy;
- efektywność realizacji gamy funkcji kryptograficznych (poufność, integralność, uwierzytelnienie);
- efektywność realizacji funkcji zabezpieczających prawidłowe funkcjonowanie systemów (identyfikacja i uwierzytelnienie użytkownika, kontrola dostępu, rozliczalność, audyt, itp.);

2. aspekty techniczne
- możliwość dopasowania parametrów urządzenia (systemu) do parametrów urządzeń współpracujących i parametrów toru transmisyjnego;
- odporność fizyczną (np. mechaniczną) i i istnienie mechanizmów przeciwstawiających się nieuprawnionej penetracji;
- zapewnienie możliwie najniższego (akceptowalnego) poziomu ulotu elektromagnetycznego

3. aspekty eksploatacyjne
- prostota i bezpieczeństwo obsługi, minimalizujące możliwość popełnienia błędu przez operatora (użytkownika);



natomiast podporządkowanie laboratoriów badawczych obrazuje schemat

3. 3. Procedury certyfikacji.

Proces certyfikacji rozpoczyna się w momencie złożenia przez Wnioskodawcę w Jednostce Certyfikującej wniosku o badania i/lub certyfikację urządzeń, oprogramowania lub systemów kryptograficznych (bezpieczeństwa teleinformacyjnego).

Wniosek taki stanowi pierwszy „Fire Wall" procesu certyfikacji, przy czym celem nie jest tu eliminowanie jakiejś kategorii urządzeń lub systemów kryptograficznych. Wprost przeciwnie – stosując zasadę równouprawnienia prowadzimy badania wszystkich systemów, jednakże według zasad, do których muszą się stosować obydwie strony.

Skrócona procedura certyfikacji wyrobów zaprezentowana jest na schemacie:

organów i instytucji oraz zakresu i trybu wykonywania przez nie obowiązków niezbędnych do realizacji kryptograficznej ochrony wiadomości stanowiących tajemnicę państwową i służbową. Projekt ten – przygotowany w Biurze Bezpieczeństwa Łączności i Informatyki UOP na podstawie delegacji ustawowej [4] - uwzględnia wszystkie zgłoszone wcześniej uwagi i sugestie i przewiduje między innymi, że[5]:

- informacje klasyfikowane (stanowiące tajemnicę państwową i służbową) mogą być przekazywane tylko za pomocą specjalnych systemów teleinformacyjnych, zapewniających skuteczną ochronę informacji przed ujawnieniem, nieautoryzowaną modyfikacją lub zniszczeniem;
- specjalne systemy teleinformacyjne są to techniczne środki łączności i informatyki służące do bezpiecznego przekazywania informacji klasyfikowanych z wykorzystaniem środków ochrony kryptograficznej;
- środki ochrony kryptograficznej są to systemy i urządzenia kryptograficzne a także dokumenty szyfrowe, przepisy dotyczące kryptograficznej ochrony systemów teleinformacyjnych oraz dokumentacja organizacyjna, techniczna i ewidencyjna urządzeń i systemów kryptograficznych;
- za bezpieczeństwo informacji klasyfikowanych w czasie ich przekazywania specjalnymi systemami teleinformacyjnymi odpowiada Szef Urzędu Ochrony Państwa (osobny przepis ogranicza tą odpowiedzialność do przypadków, w których przestrzegane są zalecenia i wytyczne Szefa UOP);
- procedury projektowania, budowy i eksploatowania specjalnych systemów teleinformacyjnych opisywane są w dokumencie „Program Organizacyjno-Użytkowy" uzgadnianym z Szefem UOP;
- podmioty budujące specjalne systemy teleinformacyjne zobowiązane są do zorganizowania Służby Bezpieczeństwa Teleinformacyjnego;
- w skład Służby Bezpieczeństwa Teleinformacyjnego mogą wchodzić wyłącznie osoby, które ukończyły specjalistyczne szkolenie w tym zakresie w UOP (potwierdzone zaświadczeniem – certyfikatem) i posiadają dopuszczenie do tajemnicy państwowej;
- Szef UOP dopuszcza do eksploatacji specjalne systemy teleinformacyjne oraz decyduje o ich wycofaniu a także sprawuje kontrolę nad ich organizacją, bezpieczeństwem i funkcjonowaniem.

Dokument ten – po jego uzgodnieniu, podpisaniu i wejściu w życie – stanowił będzie istotny krok „uzdrawiający" stan bezpieczeństwa teleinformacyjnego naszego państwa.
Jednakże – jak zapewne dostrzeże uważny Czytelnik - projektodawcy poruszali się w granicach upoważnienia ustawowego. Tym samym niemożliwe było – w ramach tego aktu - uporządkowanie kompleksu spraw związanych z ochroną kryptograficzną informacji „nieklasyfikowanych".
Pełnych – zbliżonych do rozwiązań „Zachodu" – regulacji w tym zakresie, można spodziewać się dopiero w ramach nowelizacji ustawy o ochronie tajemnicy (chyba już nie tylko państwowej i służbowej).

3. Certyfikacja urządzeń i systemów kryptograficznych[6].

3. 1. „Ścieżka" prawna.

Rozporządzenie Rady Ministrów z dnia 21 czerwca 1994 r w sprawie zakresu i trybu stosowania przepisów ustawy o badaniach i certyfikacji do wyrobów produkowanych w kraju

[4] Art. 1 ust. 5 ustawy z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa
[5] poniższe zapisy nie stanowią cytatów – oddają jednak obraz projektowanych przepisów
[6] oczywiście w kompleksie bezpieczeństwa teleinformacyjnego

Stan formalno-prawny w Rzeczypospolitej

2. 1. Regulacje ustawowe

Podstawowym aktem prawnym, regulującym procedury bezpieczeństwa kryptograficznego w RP jest ustawa z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa. Nakłada ona na Szefa Urzędu Ochrony Państwa (art. 1. 2. pkt. 7) obowiązek kryptograficznej ochrony wiadomości stanowiących tajemnicę państwową i służbową, przekazywanych przez techniczne środki łączności na potrzeby organów administracji państwowej i państwowych instytucji finansowych i gospodarczych.

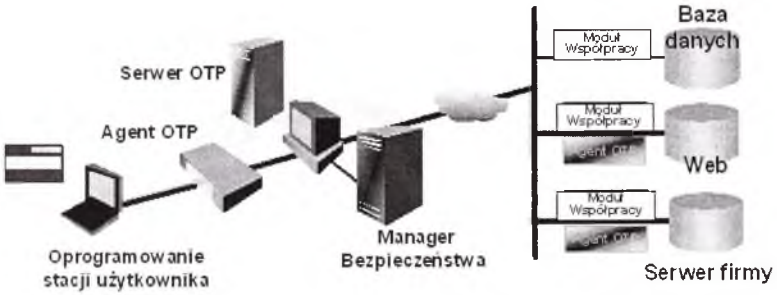
Tak określone zadanie powoduje szereg rozbieżności interpretacyjnych wśród znawców prawa, a także – co gorsza – jego adresatów. Rozbieżności te i krytyka dotyczą najczęściej:

- nie objęcia przepisem aspektów bezpieczeństwa transmisyjnego, elektromagnetycznego, fizycznego i logicznego - regulowane jest wyłącznie bezpieczeństwo kryptograficzne[1];
- regulacja obejmuje ograniczony katalog informacji klasyfikowanych (stanowiących tajemnicę państwową i służbową) do informacji funkcjonujących „na potrzeby organów administracji państwowej i państwowych instytucji finansowych i gospodarczych";
- brak regulacji prawnych ochrony kryptograficznej procesów przetwarzania, przechowywania i przesyłania informacji wrażliwych (chronionych na podstawie innych niż ustawa o ochronie tajemnicy państwowej i służbowej przepisów - np. prawo bankowe, dane osobowe lub własnych potrzeb konkretnej jednostki organizacyjnej).
- nie objęcie regulacjami ochrony kryptograficznej procesów przetwarzania i przechowywania informacji w systemach - regulowany jest wyłącznie proces przesyłania informacji klasyfikowanych;

Nie ułatwia sytuacji – funkcjonująca równolegle – ustawa z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej (Dz. U. Nr 40, poz. 271). Ustawa ta - mimo, że niektóre jej przepisy można (i trzeba) stosować do procedur ochrony informacji w systemach teleinformacyjnych – również nie odpowiada współczesnym standardom[2].

Innym aktem prawnym związanym z kryptograficzną ochroną informacji jest ustawa z dnia 2 grudnia 1993 r. o zasadach szczególnej kontroli obrotu z zagranicą towarami i technologiami w związku z porozumieniami i zobowiązaniami międzynarodowymi. Ustawa ta nakłada na importerów, eksporterów i dealerów urządzeń i systemów kryptograficznych obowiązek uzyskiwania zgody Ministra Gospodarki na obrót i stosowanie tej technologii „podwójnego przeznaczenia".
Przepisem wydanym na podstawie tej ustawy jest Zarządzenie Ministra Współpracy Gospodarczej z Zagranicą z dnia 20 grudnia 1996 r. w sprawie ustalenia wykazu towarów i technologii objętych szczególną kontrolą obrotu z zagranicą (kategoria 5 - komputery, telekomunikacja i ochrona informacji).
W pracach specjalnej komisji powołanej na podstawie powyższych aktów prawnych biorą aktywny udział eksperci Urzędu Ochrony Państwa.

[1] tylko konsekwentne wdrożenie i stosowanie kompleksu procedur bezpieczeństwa teleinformacyjnego może doprowadzić do uzyskania i utrzymania wymaganego poziomu bezpieczeństwa informacji.
[2] zainteresowanych szczegółami odsyłam do referatu programowego Seminarium MIEDZESZYN '97 gdzie opisano szerzej ten problem



Rys. Przykładowa topologia systemu SSSO (Secure Single Sign On)

Ad.3

Bardziej zaawansowane centralne serwisy uwierzytelniające oparte są o tzw. tokeny czyli potwierdzone kryptograficznie dane uwierzytelniające. Przykładem może być sławny Kerberos opracowany w MIT gdzie użytkownik po pozytywnym zidentyfikowaniu otrzymuje od systemu niepowtarzalny bilet, który w danej sesji służy do automatycznego dalszego uwierzytelniania się i autoryzacji. Pierwsze zalogowanie się musi być oczywiście precyzyjnie kontrolowane np. za pomocą techniki OTP – od niego bowiem zależy cały dalszy proces „wędrowania" po systemie objętym SSO.

W tego typu systemach każdy komputer czy aplikacja musi być w odpowiedni sposób dostosowana do uwierzytelniania za pomocą tokenów zamiast tradycyjnego systemu haseł.

W dalszej części referatu zostanie przedstawiony przykładowy system, w którym SSO stanowi jeden z najistotniejszych elementów zarządzania bezpieczeństwem rozproszonej struktury serwerów i stacji roboczych UNIX oraz komputerów dostępowych typu PC.

Wcześniej jednak należy zaznaczyć, że zapewnienie niezawodności i bezpieczeństwa systemów wyposażonych w technologię SSO stanowi wyzwanie o szczególnym wymiarze.

Niezawodność i bezpieczeństwo

W systemach SSO kluczową sprawą jest zapewnienie mocnego uwierzytelnienia na etapie dostępu do uprawnień. Hasło, które jest kluczem do wielu systemów i/lub aplikacji nie może być statyczne a sesja użytkownika z serwerem powinna być szyfrowana algorytmem o odpowiedniej mocy kryptograficznej. Centralny serwer uwierzytelniający jest w systemach SSO czułym miejscem: może stanowić obiekt ataków a także nie było by dobrze gdyby stał się pojedynczym punktem awarii (ang. single point of failure). Serwery SSO muszą zapewniać redundancję (mirrory, repliki itd.)

Centralne administrowanie

Tak naprawdę, systemy SSO oprócz wygody dla użytkowników mają do spełnienia jeszcze jedną ważną misję: dostarczyć administratorowi bezpieczeństwa danego systemu oręża w postaci możliwości zarządzania użytkownikami, ich prawami a także zarządzania i monitorowania bezpieczeństwa wielu rozproszonych systemów komputerowych i aplikacji na nich zainstalowanych – wszystko to centralnie, z jednego miejsca (które na dodatek może być w sytuacji kryzysowej zastąpione przez swą replikę). To zadanie jest niewątpliwie najtrudniejsze do osiągnięcia.

Przykładowy system wykorzystujący ideę bezpiecznego SSO

Jak to było wcześniej zapowiedziane zostanie pokrótce omówiony przykładowy system zapewniający kontrolę dostępu oraz zarządzanie bezpieczeństwem w środowisku rozproszonych komputerów pod systemem operacyjnym UNIX w oparciu o ideę single-sign-on.

System aby zrealizować maksymalnie wiele funkcji związanych z zapewnieniem bezpieczeństwa powinien składać się z wielu komponentów a mianowicie:

Manager Bezpieczeństwa – Serwer zapewniający mocne uwierzytelnienie, kontrole dostepu, scentralizowane zarządzanie profilami bezpieczeństwa, monitorowanie i audyt całej sieci komputerów oraz aplikacji na nich posadowionych.

ZARZĄDZANIE BEZPIECZEŃSTWEM ROZPROSZONYCH SYSTEMÓW KOMPUTEROWYCH Z WYKORZYSTANIEM IDEI SINGLE-SIGN-ON

Krzysztof Silicki

Wprowadzenie

W środowisku sieci komputerowych łączących w jednej firmie kilkanaście, kilkadziesiąt i więcej systemów komputerowych (serwerów, stacji roboczych, terminali dostępowych) zapewnienie bezpieczeństwa na satysfakcjonującym poziomie łączy się z umiejętnym zarządzaniem i kontrolą praw dostępu użytkowników do urządzeń, systemów, aplikacji, katalogów, stron WWW itp. W rozbudowanych, rozproszonych systemach problem spójnego wdrożenia i utrzymania w działaniu programu bezpieczeństwa (security policy) w zakresie praw dostępu, uwierzytelniania i autoryzacji staje się kluczowym zadaniem organizacyjno-technicznym. W niniejszym referacie zostaną zarysowane praktyczne możliwości wykorzystania idei single-sign-on wraz z innymi dokonaniami współczesnej kryptografii (np. kryptografia asymetryczna, podpis cyfrowy, szyfracja komunikacji) w celu zapewnienia mocnego uwierzytelniania i autoryzacji użytkowników systemu oraz wdrażania i centralnego egzekwowania kontroli praw dostępu.

Problem zarządzania hasłami dostępu

W każdym systemie wielodostępnym istnieje problem zapewnienia skutecznej identyfikacji i weryfikacji użytkownika na etapie zezwalania dostępu do określonych zasobów (np.logowanie do sieci, logowanie do systemu operacyjnego komputera, dostęp do aplikacji, dostęp do plików i katalogów np. WWW).

Sieci lokalne, korporacyjne, intranety, extranety, VPN-y i inne typy sieci obfitują w systemy o różnym przeznaczeniu gdzie niezwykle istotne jest rozgraniczenie praw dostępu (np. blokowanie dostępu z zewnątrz do serwerów intranetowych, ograniczenie dostępu do niektórych aplikacji.

Tradycyjne systemy haseł nie są już obecnie traktowane jako wystarczające ze względu na powszechnie występujące przypadki podsłuchiwania, podpatrywania, wykradania, łamania haseł. Coraz częściej wykorzystywane są metody typu OTP (One Time Password), w których w sposób programowy lub sprzętowy (użytkownik zostaje wyposażony w kartę/token generujący hasła ważne tylko jeden raz) realizowana jest zasada jednorazowego hasła dostępu: hasło raz użyte jest „zużyte". Co pod względem bezpieczeństwa jest do zaakceptowania to ze względów użytkowych może posiadać pewne wady. W tym wypadku użytkownik, który miałby mieć precyzyjnie określone i egzekwowane prawa dostępu do wielu systemów, aplikacji w środowisku pracy w sieci musiałby za każdym razem, kiedy stara się uzyskać dostęp do określonego zasobu – podawać hasło. Jeśli system haseł dostępu jest tradycyjny – użytkownika zmusza się do pamiętania kilku, kilkunastu czy kilkudziesięciu różnych haseł – co jest trudne i zazwyczaj powoduje zagrożenia bezpieczeństwa (jedno hasło do wszystkich zasobów, hasła zbyt proste, hasła zapisywane w widocznych miejscach). Jeśli system haseł dostępu jest dynamiczny (OTP) użytkownik haseł pamiętać nie musi – jednak częste wprowadzanie haseł w czasie pracy może być uciążliwe.

Administrowanie skomplikowanym układem haseł również może powodować problemy.

Wprowadzanie nowych użytkowników oznacza zmiany w kilku/kilkunastu/kilkudziesięciu plikach na różnych urządzeniach, z reguły przy użyciu zupełnie różnych narzędzi programowych. Nawet proste sprawdzenie w takim środowisku, do czego użytkownik ma dostęp nastręcza administratorowi sporo problemu. Obsługa użytkownika, która posiada już więcej niż 3 hasła wprowadza całkiem spory narzut administracyjny.

LDIF. Ponieważ dane w X.500 stosują kody T.61 należy zastosować przekodowanie do UTF-8. Tak przygotowane zasoby umieszczone w pliku LDIF mogą już zostać przekazane odpowiednim modułom odpowiedzialnym za dodawanie encji. Narzędzia stosowane przy translacji zasobów nie są dostępne, administrator musi przygotować skrypty wykonujące potrzebne operacje. Można tu również wykorzystać oferowane w pakiecie `ldap-3.3` programy obsługi zasobów.

Serwis katalogowy oparty na pakiecie `Netscape Directory Server` musi nadal funkcjonować jako fragment globalnej usługi. Oznacza to możliwość komunikowania się z innymi serwerami oferującymi dane informacyjno-adresowe. W ramach serwera `ns-slapd` jest to realizowane za pomocą odsyłaczy (*refferals*). Po pierwsze stosowany jest odsyłacz określony w pliku konfiguracyjnym jako punkt kontaktowy, w przypadku, gdy zadano pytanie dotyczące encji nie rezydującej na serwerze, jest on przekazywany stronie klienckiej, która odpowiednio wykorzystuje informacje. Poza tym, gdy strona kliencka poszukuje określonej encji, lub pragnie ją modyfikować może zostać zwrócony odsyłacz, który został wprowadzony do bazy danych jako encja klasy obiektów `referral` (*smart refferal*).

Oprogramowanie `Netscape Directory Server` przewiduje również replikacje wskazanych części drzewa informacyjnego. Mechanizm ten funkcjonuje na podstawie wzajemnych uzgodnień i stosuje model podobny do X.500.

Wnioski z przeprowadzonych testów

Przeprowadzone prace testowe pokazały, że przeniesienie obecnie eksploatowanej bazy X.500 na platformę opartą na protokole LDAP nie powinno napotkać większych problemów. Jeśli założyć, że kierunek w jakim zmierzają obecnie aplikacje sieciowe będzie kontynuowany, czyli rozwijane będą systemy zintegrowane z protokołem LDAP świadczenie usługi katalogowej w tej postaci stanie się niezbędne. Oczywiście można stosować serwer `ldapd` jako pośredniczący między klientem i serwerem X.500, ale z drugiej strony, jeśli fakty pokażą, że stosowanie LDAPa do zarządzania bazą danych jest efektywniejsze będzie trzeba pójść w tym kierunku. Zasadniczą przyczyną problemów, jakąkolwiek drogę wybierzemy, może być prawdopodobnie pozyskanie odpowiedniego oprogramowania. Tendencje panujące na rynku wskazują, że zabraknie firm, czy grup programistów oferujących swoje produkty za darmo. Ostatnia wersja pakietu `ldap-3.3` pochodzi z 1996, jeden z głównych programistów, Tim Howes, przeszedł do firmy Netscape, która dostarcza pakiet bezpłatnie na okres 60 dni, a w celu uzyskania licencji pełnej należy wnieść odpowiednie opłaty.

9. Podsumowanie

Wyniki doświadczeń zdobytych w trakcie przeprowadzonych prac będą wykorzystywane dla potrzeb polskiego projektu X.500. Nie można przeoczyć szansy jaka pojawia się obecnie, gdy większość produktów zmierza do integracji z usługą katalogową. Te okoliczności sprzyjają tworzeniu dobrych narzędzi, dzięki którym będzie znacznie łatwiejsze tworzenie interfejsów użytkownika. Godne uwagi są dostępne już pakiety `Netscape Directory SDK` i `Netscape LDAP Java SDK`. Pierwsze próby implementacji w oparciu te biblioteki pokazały, że są to narzędzia bardzo wygodne. Nie można również pominąć inicjatywy o nazwie `Java Naming and directory interface - JNDI (http://jaca.sun.com/products/jndi)`. Jest to specyfikacja rozwinięta przez *JavaSoft* w celu wbudowania w aplikacje Javy interfejsu dostępu do zasobów katalogowych.

W skład pakietu wchodzi również serwer replikacji – `slurpd`, uruchamiany na tej samej stacji co `slapd` i odpowiedzialny za propagowanie zmian do podporządkowanych (na zasadzie wzajemnych uzgodnień) serwerów.

Usługa katalogowa wykorzystująca pakiet `ldap-3.3` może być zrealizowana na różne sposoby:

1. LDAP jako serwis lokalny. Oznacza to, że uruchamiany jest serwer `slapd`, który zarządza lokalną bazą danych, nie kontaktuje się z innymi serwerami. Jest to postać usługi zalecana w fazie testowej, czy eksperymentalnej, lub w przypadku, gdy celem jest oferowanie dostępu do lokalnych zasobów.
2. LDAP jako serwis lokalny z możliwością kontaktu z innymi serwerami. W tej konfiguracji uruchamiany jest zarówno serwer `slapd` jak i `ldapd`. Serwer `ldapd` daje dostęp do świata X.500. Możliwe jest również zrezygnowanie ze stosowania własnego serwera, w sytuacji, gdy jest znany odpowiedni serwer `ldapd`, który może zostać wskazany jako usługodawca w zakresie X.500.
3. LDAP jako interfejs dostępowy (*front-end*) do X.500. Jest to jedno z typowych zastosowań LDAPa, polegające na stosowaniu serwera `ldapd` jako pośrednika translującego zapytania klienta LDAP do postaci X.500.
4. Replikowana usługa `slapd`. Oznacza stosowanie serwera `slurpd` do propagowania zmian do jednego lub więcej serwerów `slapd` (technika *master-slave*). Ten typ usługi może być stosowany w połączeniu z dwiema pierwszymi konfiguracjami.

Zarządzanie bazą danych `slapd` może odbywać się poprzez interfejsy klienckie, jest to dobra metoda w przypadku małych modyfikacji zasobów. Istnieją również narzędzia przeznaczone do operowania bezpośrednio na bazie, *off-line*. Do reprezentacji encji (*entries*) w prostej postaci tekstowej stosowany jest format LDIF (LDAP *Data Interchange Format*), zdefiniowany w dokumencie Internet-Draft [9]. W pakiecie `ldap-3.3` istnieją programy translacji tego formatu do postaci DBM, czy tworzenia na ich podstawie plików zawierających indeksy atrybutów. Opracowano także narzędzia do konwersji plików EDB, stosowanych w serwisie X.500 opartym na `Quipu`, do plików LDIF. Baza danych `slapd` może być wystarczająca tylko w przypadku stosowania odseparowanych zasobów informacyjnych.

Jeżeli wymagana jest komunikacja z innymi serwerami `slapd` tworzone są tzw. *referral entries*, czyli encje będące odesłaniem do innego serwera. Muszą one zawierać atrybut *ref*, któremu jest przypisywany identyfikator URL odpowiedniego serwera.

Netscape Directory Server

Firma Netscape dostarcza wśród swoich produktów wiele typów serwerów, m.in. `Messaging Server`, `Collabra Server`, `Proxy Server`, `Certificate Server`, a również `Directory Server`. Integralną częścią serwera każdego typu jest serwer administracyjny – `Netscape SuiteSpot`, wspomagający proces zarządzania. Produkt ten jest tak zaprojektowany, że większość operacji odbywa się poprzez zestaw odpowiednich formularzy i programów wykonywanych w odpowiedzi na zlecenie. Niewielka ilość funkcji dostępna jest spoza przeglądarki. Obecnie firma Netscape umożliwia pozyskanie wersji `Directory Server 3.1`. Ponieważ ukazała się ona w ostatnich dniach nasze doświadczenia dotyczą edycji 3.0. Oprogramowanie jest oferowane na okres 60 dni, w formie wersji eksperymentalnej. Istnieją implementacje na większość popularnych platform systemowych, m.in. Solaris, Digital-Unix, HP-UX, AIX, IRIX, Windows NT.

Testowa instalacja pakietu `Netscape Directory Server 3.0`, posłużyła nam jako platforma oceny możliwości przejęcia przez ten system obsługi zasobów katalogowych,

opartym na X.500 zarzucano niedojrzałość i duży stopień trudności w trakcie instalacji i konfiguracji. Jednocześnie prace nad modyfikacją standardu postępowały wolno, istotną przeszkodą był długi czas ratyfikacji wszelkich dokumentów ukazujących się pod szyldem OSI. Technologia „*top-down*" stosowana w rekomendacjach OSI wychodziła pokonana w konkurencji ze specyfikacjami pojawiającymi się w Internecie, gdzie krok po kroku, metodą „*bottom-up*" konstruowano kolejne składniki systemów, by w efekcie uzyskać sprawny i wydajny system w czasie zdecydowanie krótszym.

Rozwój LDAPa z jednej strony zmierza w kierunku, który wskazuje na dążenie do odcięcia się od standardu X.500, a dokładnie od implementacji opartych na X.500 – dodefiniowywane są elementy, które obecnie są realizowane przez X.500 (zdalne operacje, replikacja). Z drugiej strony wszelkie działania realizowane są na wzór doświadczeń uzyskanych w fazie eksploatacji X.500 i nie przewiduje się definitywnego zerwania z produktami X.500.

W dziedzinie systemów informatycznych ważna jest zawsze dobra specyfikacja zagadnienia, nie ma jednak pożytku z modelu i projektu, jeśli nie powstanie odpowiednie oprogramowanie. „Odpowiednie" nie znaczy wyłącznie dobrze przygotowane i wiernie implementujące projekt. Musi być ono również łatwo dostępne, co, w środowisku akademicko-naukowym, oznacza na ogół bezpłatne. Tylko dzięki temu, że pakiet `Quipu` dostępny był za darmo możliwe było uruchomienie projektu X.500 w Polsce. Obecnie, ośrodki pragnące posiadać produkt implementujący standard X.500'93 muszą za takie oprogramowanie zapłacić. Ogranicza to bardzo zasięg usługi i wprowadza znaczne ograniczenia w jej rozwoju. Nadal dostępne bezpłatne oprogramowanie `Quipu` (X.500'88) nie jest rozwijane od 1992 roku i brakuje wersji na aktualne platformy systemowe. Pakiet LDAP zrealizowany przez programistów University of Michigan jest ogólnodostępny, niestety, nie jest zgodny z aktualną wersją standardu.

To jak rozwijać się będzie oprogramowanie będzie w znacznym stopniu decydować w jakim kierunku toczyć się będą losy usługi katalogowej.

7. Oprogramowanie X.500

W trakcie prac w dziedzinie serwisu X.500 mieliśmy do czynienia z oprogramowaniem `Quipu` w wersji ogólnodostępnej (pakiet `Isode-8.0`), następnie wykorzystywaliśmy produkt firmy Isode, `IC`. Obecnie Isode wymaga opłaty subskrypcji, która pozwala na otrzymywanie w ciągu roku dostępu do kolejnych edycji oprogramowania. Najnowsza, ogłoszona ostatnio wersja to `ICR4`. Ostatnią edycją, nad którą pracowaliśmy było `ICR3.2`. Nasze doświadczenia z eksploatacji pakietu są duże, tym bardziej, że wielokrotnie w pracach rozwojowych niezbędne było zrozumienie fragmentów kodu źródłowego. Oceniamy, że faza kompilacji, instalacji i konfiguracji nie powinna przynieść większych trudności osobom mającym związek ze środowiskiem Unix i z technikami adaptacji oprogramowania.

Począwszy od wersji R3 pakiet `IC` implementuje standard X.500'93. Wnosi to sporo istotnych zmian w samą usługę i sposoby zarządzania. W tym celu zostały znacznie rozbudowane moduły zarządzania systemem – wszystkie działania odbywają się poprzez interfejsy graficzne. Pakiet `IC` bardzo się rozrasta, zwiększają się też wymagania sprzętowe. W celu kompilacji oprogramowania potrzebna jest instalacja innych pakietów, przede wszystkim graficznych. Począwszy od wersji R4 zapowiadana jest możliwość uzyskania binariów na popularne platformy.

W maju 1997 roku wzięliśmy udział w międzynarodowych testach oprogramowania X.500'93, prowadzonych przez organizację DANTE, nadzorującą usługę X.500 w Europie (projekt NameFLOW-Paradise). W kilku instytucjach na świecie zostały wystartowane serwery pracujące na oprogramowaniu implementującym X.500'93 oferowanym przez różnych producentów. Serwery te kontaktowały się między sobą oraz ze światem zewnętrznym. W Toruniu uruchomiono dwa

Celem, do którego zmierzali autorzy standardu LDAP było powstanie narzędzi wspomagających rozwój interfejsów użytkowych do zasobów X.500 i rozszerzenie zasięgu tych aplikacji. M.in. użyto LDAPa do zaimplementowania programów współpracujących z usługą `gopher`, `finger`, czy interfejsy poczty elektronicznej, a gdy najpopularniejszą formą dostępu do zasobów informacyjnych stało się WWW w oparciu o LDAP powstała bramka X.500-WWW. Popularność protokołu LDAP rosła, bez wątpliwości dzięki niemu X.500 stało się jedną z istotnych usług sieci Internet.

Skalę popularności LDAP podsumowało ogłoszenie w 1996 roku przez firmę Netscape oraz czterdzieści innych firm integracji swoich produktów z protokołem LDAP. Konsekwencją stał się zataczający coraz szersze kręgi się pogląd, że LDAP jest synonimem „**`Internet Directory`**".

3. Cechy wspólne standardu X.500 i protokołu LDAP

Analizując rekomendacje X.500 oraz protokół LDAP nie trudno zauważyć, że specyfikacje te mają więcej elementów wspólnych niż różnic. Główne punkty styczności dotyczą modelu informacyjnego i standardowych usług. Podstawowa definicja obu produktów zawiera:

1. **Hierarchiczne nazewnictwo**. LDAP na wzór X.500 definiuje hierarchiczną strukturę samej bazy oraz nazw encji umieszczanych w bazie danych, cały model informacyjny LDAPa opiera się na specyfikacji X.500.
2. **Składniki nazw o określonych typach**. Nazwa wyróżniona na każdym poziomie drzewa informacji opisana jest typem atrybutu oraz jego wartością.
3. **Obiekty o określonych typach**. Obiekty reprezentowane są w zasobach X.500 i LDAP jako encje, posiadające typ, zwany klasą obiektów. Typ obiektu jest określany atrybutem „klasa obiektu" (*object class*). X.500 i LDAP stosują wspólną definicję podstawowych klas obiektów.
4. **Atrybuty o określonych typach**. Informacja na temat obiektu jest utrzymywana w postaci zbioru atrybutów, posiadających określone typy. X.500 i LDAP stosują wspólną definicję podstawowych atrybutów.
5. **Operacje bazy danych**. X.500 i LDAP mają wspólny podstawowy zakres operacji dostępu i zarządzania danymi w bazie (`read`, `compare`, `search`, `add`, `delete`, `modify`).

4. Rozwój standardu X.500 (1993)

Prace nad specyfikacjami standardu X.500 nie zakończyły się w 1988 roku. Definicję niektórych elementów celowo odłożono na późniejszy okres. Autorzy rekomendacji zdobywali spore doświadczenie obserwując jak rozwijają się produkty programowe implementujące X.500, śledząc problemy dotyczące współpracy pakietów różnych producentów. W efekcie, z opóźnieniem, bo w 1995 roku ukazał się standard tytułowany X.500'93, znacznie wzbogacający możliwości. Najistotniejsze własności nowego standardu to:

1. Technika replikacji oparta na protokole DISP (*Directory Information Shadowing Protocol*); replikacja umożliwia znaczną elastyczność i zwiększa efektywność usługi.
2. Sterowanie dostępem (*Access Control*); opracowano standard określania praw dostępu do wybranych danych.
3. Usprawnienie modelu informacyjnego; wprowadzono podtypy atrybutów, wydzielono atrybuty operacyjne, co pozwala rozróżnić dane użytkowe od informacji wspomagających usługę.

OBSŁUGA ZASOBÓW INFORMACYJNO-ADRESOWYCH ZA POMOCĄ PROTOKOŁU LDAP

PRZEGLĄD DOSTĘPNYCH NARZĘDZI I PORÓWNANIE Z TECHNOLOGIĄ X.500

Maja Górecka *Maja.Gorecka@cc.uni.torun.pl*

Tomasz Wolniewicz *twoln@hpc.uni.torun.pl*

Naukowa Akademicka Sieć Komputerowa NASK
Zakład Rozproszonych Systemów Informacyjnych

Referat odnosi się do najnowszych tendencji w sieci Internet dotyczących obsługi zasobów informacyjno-adresowych, zwanych katalogowymi bazami danych (**`Directory Services`**). Punktem odniesienia przeprowadzonej analizy zagadnienia jest standard X.500. Autorzy pracy od 1992 roku zajmują się tą tematyką i kierują rozwojem usługi X.500 na terenie Polski. Referat omawia zyskujący coraz większą popularność protokół LDAP (*Lightweight Directory Access Protocol*) na tle historii standardu X.500. Następnie prezentujemy konkretne narzędzia do obsługi baz katalogowych za pomocą protokołu LDAP. W zakończeniu oceniliśmy efekty przeprowadzonych testów polegających na uruchomieniu usługi katalogowej pracującej na oprogramowaniu LDAP.

Tematyka panujących obecnie tendencji w dziedzinie usług katalogowych była również przedmiotem naszego opracowania [13]. Lektura pozycji [3, 4] pozwala zapoznać się z poglądami osób intensywnie zaangażowanych w rozwój światowej usługi X.500.

Opracowanie podsumowuje działania zmierzające do przygotowania się do prac rozwojowych na nowych platformach.

1. Standard X.500

Pełną wersję międzynarodowych rekomendacji ITU-T dotyczących standardu X.500 można znaleźć w odpowiednich dokumentach ([1]). Jest to zestaw zaleceń (X.500-X.521) obejmujący m.in. definicję struktury bazy, opis modelu informacyjnego i funkcjonalnego, definicję protokołu komunikacji między współpracującymi systemami, specyfikację bazowych własności zasobów: typów obiektów oraz atrybutów. Standard X.509 precyzuje zasady komunikacji w ramach bezpiecznych systemów informacyjnych, określa metody uwierzytelniania użytkowników systemu. Tematykę X.500 przybliża w sposób przystępny, a jednocześnie wyczerpujący pozycja [2]. Prezentowane przez nas w ubiegłych latach referaty ([5]) były z jednej strony opisem cech i funkcjonalności X.500, z drugiej stanowiły podsumowanie prowadzonych przez nas prac rozwojowych w tym zakresie.

Pierwsza wersja standardu ukazała się w 1988 roku. Potrzeba tego typu specyfikacji wynikła z charakteru usługi X.400 (poczta elektroniczna), która stosowała skomplikowane łańcuchy do identyfikacji stron komunikujących się. Poczta elektroniczna oparta o protokół X.400 nie przyjęła się, natomiast funkcjonalność X.500 rozszerzono z zamiarem stosowania tej technologii do zarządzania rozproszonymi zasobami informacyjno-adresowymi, gromadzącymi adresy, telefony, opisy itp. osób, jednostek organizacyjnych, instytucji.

Tuż po ukazaniu się standardu X.500 zaczęły pojawiać się pierwsze jego implementacje. W środowisku akademicko-naukowym najpopularniejszy stał się pakiet `Quipu`, autorstwa Collina Robinsa, który szybko zdominował światowy rynek i stał się podstawą późniejszych komercyjnych implementacji sprzedawanych m.in. przez firmy Isode Ltd, NEXOR, czy ISOCOR.

interfejsu obsługującego wszelkie takie programy. Nasz system został sprawdzony z programami elm, pine i emacs.

10. Planowane prace rozwojowe

Nadzwyczaj duża dynamika prac w dziedzinie usługi katalogowej powoduje, że w najbliższym czasie oczekujemy pojawienia się aplikacji wykorzystujących bezpośrednio protokół LDAP.

PGP 5.5, który pojawił się w ostatnich dniach, pozwala korzystać z LDAPv3 w celu dokonywania „ręcznego" odszukiwania kluczy. Przetestowana zostanie współpraca tego pakietu z serverem LDAPv3 Netscape oraz bramką LDAVv3 - X.500 zawartą w najnowszym pakiecie Isode.

Do upowszechnienia usługi niezbędne będzie wsparcie systemów poczty działających pod systemami Windows95 i Windows NT. PGP 5.5 powinno dostarczyć przynajmniej części oczekiwanej funkcjonalności.

Rozbudowane zostanie wparcie dla systemów korzystających z certyfikatów X.509.

11. Zestawienie programów wspomagających system bezpiecznej wymiany informacji

pgp2cert – program w języku C, aplikacja pakietu SecuDE, funkcja: wystawienie certyfikatu PGP i PEM na podstawie klucza publicznego, do wykorzystywania przez Urząd Certyfikacyjny,
cuc-check – skrypt w języku *Perl*, wykorzystuje program pakietu SecuDE psemaint, kontroluje dziennik pracy i buduje listę przedawnionych certyfikatów, do wykorzystywania przez Urząd Certyfikacyjny,
newattr – skrypt w języku *Perl*, wykorzystuje programy dostępowe do zasobów X.500 (showentry, modify), wprowadza do bazy X.500 atrybuty dotyczące kluczy PGP i PEM (pGPKey, pGPKeyID, pGPUserID, userCertificate), do wykorzystywania przez administratorów regionalnych – delegatury,
delkey – skrypt w języku *Perl*, wykorzystuje programy dostępowe do zasobów X.500 (showentry, modify), kasuje w bazie X.500 klucze PGP i PEM dla wskazanych obiektów, do wykorzystywania przez administratorów regionalnych – delegatury,
pgp-wrap – skrypt w języku *Perl* obudowany *wrapperem*, wykorzystuje program pgp oraz program dostępowy do zasobów X.500 ldapsearch; do wykorzystania przez użytkowników systemu; rozszerza funkcje programu pgp:

- w przypadku zlecenia wyświetlenia klucza publicznego użytkownika o podanym adresie e-mail, gdy klucz nie istnieje w lokalnym *keyringu* wyszukuje go w zasobach X.500,
- pośredniczy w wywołaniu komendy pgp w przypadku podania opcji „-f" (tzw. *filter mode*), analizuje komunikaty i gdy nie został znaleziony potrzebny klucz w lokalnym *keyringu*, próbuje wyszukać go w zasobach X.500 i dopisać do *keyringu*

ckkey – skrypt w języku *Perl*, wykorzystuje program pgp, dla kluczy poświadczonych przez Urząd Certyfi kontroluje datę wystawienia certyfikatu i informuje o przedawnieniu kluczy,
update-pgp – skrypt w języku *Perl*, wykorzystuje program pgp oraz program dostępowy do zasobów X.500 — ldapsearch do sprawdzenia zgodności klucza umieszczonego w lokalnym *keyringu* i w bazie X.500, w przypadku niezgodności pozwala zaktualizować zawartość *keyringu*.

Przygotowany został również pakiet zawierający powyższe programy i prekompilowane (na Solaris 2) programy ldapsearch i expect.

wiedniego dokumentu tożsamość osoby zgłaszającej się. Ważność certyfikatów mija po upływie roku od daty wystawienia.

7. Zadania Urzędu Certyfikacyjnego

Specjalnie powołany do poświadczania kluczy publicznych Urząd Certyfikacyjny Polskiej Akademickiej Usługi Katalogowej udostępnia w zasobach X.500 swój klucz publiczny. Urząd występuje w X.500 pod nazwą wyróżnioną:

c=PL@ou=Polska Akademicka Usługa Katalogowa

Klucz, umieszczony pod atrybutem pGPKey można odnaleźć za pomocą dowolnego interfejsu użytkowego X.500, np. bramki WWW-X.500.

Do obowiązków Urzędu Certyfikacyjnego należy:

1. poświadczanie przesyłanych z Delegatur kluczy na specjalnie dedykowanej, odseparowanej od sieci komputerowej, bezpiecznej stacji,
2. przesyłanie poświadczonych kluczy w odpowiedniej postaci do Delegatur,
3. aktualizacja gałęzi identyfikatorów kluczy publicznych, poprzez dodawanie lub usuwanie aliasów,
4. utrzymywanie dziennika pracy systemu,
5. okresowa kontrola aktualności kluczy i wysyłanie informacji do Delegatur o konieczności usunięcia kluczy z zasobów X.500.

Ponadto zakłada się, że Urząd Certyfikacyjny koordynuje działania w zakresie eksplotacji systemu i dostarcza jednorodne narzędzia pracy administratorom pełniącym rolę Delegatury oraz użytkownikom.

8. Zadania administratorów regionalnych

Zgodnie z tym, co zostało wcześniej opisane, regionalni administratorzy bazy X.500 występują jako delegatury Urzędu Certyfikacyjnego. Ich zadania to:

1. zaświadczanie wiarygodności kluczy przesyłanych do Urzędu Certyfikacyjnego,
2. przesyłanie w postaci bezpiecznej kluczy do Urzędu Certyfikacyjnego,
3. odbiór oraz umieszczanie poświadczonych kluczy w bazie X.500,
4. kasowanie kluczy przedawnionych, po otrzymaniu zlecenia z Urzędu Certyfikacyjnego.

Administratorzy otrzymują zestaw narzędzi do obsługi zasobów X.500 w aspekcie danych dotyczących bezpiecznej wymiany informacji. Są to skrypty w języku *Perl*, wykorzystujące programy współpracujące z bazą X.500, typu search, showentry, czy ldapsearch i przeznaczone do automatyzacji procesu wprowadzania lub kasowania odpowiednich danych.

Skrypt newattr dokonuje odpowiedniej aktualizacji bazy X.500 na podstawie przesłanego przez Urząd Centralny pliku, zawierającego poświadczony klucz publiczny. Dystrybuowana wersja skryptu wymaga konfiguracji do bieżącego środowiska pracy poprzez podanie odpowiednich ścieżek dostępu do programów oraz nazwy administratora danych X.500. W skrypcie realizowana jest kontrola dostępu poprzez sprawdzenie hasła. Efektem pracy skryptu jest modyfikacja zawartości bazy X.500 w zakresie wskazanych obiektów i wpisanie kluczy publicznych.

Skrypt delkey modyfikuje zasoby na podstawie listy nazw użytkowników, których klucze publiczne (PGP oraz certyfikat PEM) należy usunąć (lista ta przesyłana jest okresowo do delegatur przez Urząd Centralny).

- klucz publiczny PGP w postaci tekstowej, poświadczony przez Urząd Certyfikacyjny (atrybut pGPKey),
- identyfikator klucza publicznego PGP (atrybut pGPKeyId),
- identyfikator użytkownika klucza publicznego PGP (atrybut pGPUserId),
- certyfikat w standardzie PEM (X.509) (atrybut userCertificate).

UC po wystawieniu certyfikatów przesyła je zwrotnie wraz z pozostałymi informacjami odpowiednim Delegaturom, których zadaniem jest wprowadzenie ich do bazy X.500.

W ramach realizacji systemu ustalono zasady wprowadzania do bazy X.500 danych związanych z bezpieczną wymianą informacji. Powstały programy służące do poświadczania dostarczonych przez użytkowników kluczy publicznych oraz narzędzia wspomagające umieszczenie tych danych w bazie X.500.

Certyfikaty PEM i PGP korzystają z różnych sposobów identyfikacji użytkownika. W PEM jest to *Distingushed Name*, w PGP przyjęto stosowanie adresu RFC-822. W typowym przypadku użytkownik powinien występować w bazie danych X.500 w ramach instytucji, a zatem posiadać DN, dopuszcza się jednak udostępnianie usługi użytkownikom, którzy nie mogą być w naturalny sposób wprowadzeni do drzewa instytucji. W tym przypadku użytkownikowi nadany zostanie DN będący naturalną transformacją jego adresu *e-mail*.

Na przykład:

twoln@hpc.uni.torun.pl

podlega transformacji na pełną nazwę wyróżnioną (DN):

c=PL@o=Internet@dc=pl@dc=torun@dc=uni@dc=hpc@uid=twoln

System przewiduje stopniowe budowanie oddzielnego poddrzewa w bazie X.500, reprezentującego domeny internetowe — **gałęzi internetowej**. Wydaje się, że najpopularniejszą metodą wyszukiwania kluczy publicznych PGP będzie podawanie adresów *e-mail*. Dlatego najbardziej efektywne jest wprowadzenie gałęzi ustrukturalizowanej zgodnie z domenową postacią Internetu, w której znajdują się wskaźniki do odpowiednich haseł (aliasy). Umożliwi to łatwą transformację adresu *e-mail* na odpowiedni DN w X.500. Gałąź ta może być jednocześnie wykorzystywana do umieszczania w niej użytkowników, którzy nie mogą zostać zlokalizowani w poddrzewach instytucji.

Ponieważ system PGP stosuje w operacjach podpisywania elektronicznego identyfikatora klucza publicznego (KeyID) bez identyfikatora właściciela klucza, konieczne było utworzenie rodzaju indeksu tych kluczy.

Na serwerze poziomu kraju w gałęzi c=PL@o=Internet@ou=PGP KeyID są umieszczane pod atrybutem PGPKeyID odesłania do właściwych obiektów. Istnienie tych odsyłaczy znacznie poprawia efektywność wyszukiwania. Aktualizacja listy aktywnych identyfikatorów kluczy i budowanie odpowiednich aliasów należy do UC i podlegającego mu administratora krajowego DSA.

4. Moduły składowe systemu

Funkcjonowanie systemu bazuje na następujących programach:

- pakiet PGP – musi nim dysponować osoba generująca swój zestaw kluczy,
- program pgp2cert oraz zestaw specjalnych skryptów w języku *Perl* przeznaczonych do generowania certyfikatów i przygotowania pliku modyfikacji bazy X.500 – z tego zestawu narzędzi korzysta Urząd Certyfikacyjny,

SYSTEM BEZPIECZNEJ WYMIANY INFORMACJI W POLSKIEJ SIECI INTERNET WYKORZYSTUJĄCY ADRESOWO-INFORMACYJNĄ BAZĘ X.500

Maja Górecka *Maja.Gorecka@cc.uni.torun.pl*

Tomasz Wolniewicz *twoln@hpc.uni.torun.pl.*

Naukowa Akademicka Sieć Komputerowa NASK
Zakład Rozproszonych Systemów Informacyjnych

Niniejszy raport podsumowuje prace projektowe i implementacyjne mające na celu wykorzystanie bazy X.500 jako zaplecza bezpiecznej komunikacji w sieci Internet. Główny nacisk położono na wsparcie systemu PGP.

Rosnąca popularność wykorzystywania certyfikatów X.509 sprawia, że celowe będzie rozbudowanie systemu o interfejsy automatycznie pobierające certyfikaty X.509 oraz przeprowadzenie ewentualnych prac dostosowawczych związanych z pojawiającymi się ostatnio rozwiązaniami bazującymi na nowej wersji protokołu LDAP.

Podstawowe informacje na temat usługi katalogowej X.500 są dostępne, między innymi w naszym referacie [1] oraz w archiwum polskiej usługi katalogowej http://ocelot.uni.torun.pl.

1. Standard X.500 a systemy bezpiecznej wymiany informacji

Zaimplementowany system stanowi podstawę dla bezpiecznej wymiany informacji w sieci Internet poprzez udostępnianie bazy poświadczonych kluczy publicznych. System wykorzystuje funkcjonującą w Polsce bazę X.500, gromadzącą dane adresowo-informacyjne środowiska akademicko-naukowego.

System X.500 od początku był pomyślany jako wsparcie technik bezpiecznej wymiany informacji i autentykacji obiektów, podstawy strukturalne i funkcjonalne dotyczące tego zakresu opisuje standard X.509. W ramach rekomendacji X.509 wprowadza się określenie ***certyfikatu***. Certyfikatem nazywa się klucz publiczny obiektu (osoby, systemu komputerowego, instytucji itp.) zaopatrzony atrybutami daty wystawienia i okresu ważności i następnie podpisany elektronicznie przez inny, wiarygodny obiekt. Podstawowy związek pomiędzy X.509 a definicją bazy X.500 polega na nazewnictwie obiektów. Wszelkie podmioty, zarówno certyfikowane jak i certyfikujące, są identyfikowane za pomocą ***nazw wyróżnionych*** tworzonych zgodnie z hierarchiczną strukturą X.500.

W oparciu o standard X.509 określono standard PEM (Privacy Enhanced Mail)[2]. PEM poza formatem wymienianej informacji definiuje strukturę instytucji wystawiających certyfikaty. Właśnie struktura wzajemnie poświadczających się urzędów ma podstawowe znaczenie w systemie bezpieczeństwa opartego o certyfikaty. Na to, aby system taki jak PEM działał sprawnie potrzebne jest spełnienie dwóch warunków:

1. klucze publiczne identyfikujące podmioty biorące udział w wymianie informacji, muszą być powszechnie i łatwo dostępne,
2. musi istnieć absolutna pewność, że klucze są istotnie związane z podmiotami, które je wykorzystują.

Drugi warunek zapewnić może tylko system urzędów certyfikacji, pierwszy wymaga utworzenia szeroko dostępnych baz danych.

Certyfikaty X.509 są coraz powszechniej wykorzystywane w systemach WWW. Pojawia się również coraz więcej oprogramowania pozwalającego na generowanie kluczy i certyfikatów oraz zarządzanie urzędami certyfikacji.

- całkowicie rozproszona, w której moduł zarządcy w ogóle nie występuje, a proces zarządzania realizowany jest przez zbiór rozproszonych, wzajemnie komunikujących się agentów zadań.

4.1 Szeregowanie przepływów pracy

Celem szeregowania przepływów pracy jest zapewnienie poprawności realizacji przepływów pracy zgodnie z ich specyfikacją, zagwarantowanie osiągnięcia przez przepływy akceptowalnych stanów końcowych, optymalizacja realizacji przepływów oraz obsługa błędów powstałych w trakcie realizacji. Algorytmy szeregowania przepływów mogą być konstruowane w oparciu o Sieci Petriego, automaty skończone, logikę temporalną, model aktywności ECA, itp.

4.2 Synchronizacji współbieżnych przepływów pracy

Poszczególne zadania transakcyjnych przepływów pracy są wykonywane w środowisku pojedynczych jednostek przetwarzania (systemów zarządzania bazami danych). Systemy te poprzez lokalne zarządzanie współbieżnością gwarantują uszeregowalność pojedynczych zadań. Każdy z tych systemów po zakończeniu realizacji danego zdania pozostaje w stanie spójnym. Problemem pozostaje zagwarantowanie globalnej uszeregowalności całych przepływów pracy.

Przy założeniu, że każdy z przepływów pracy jest wykonany poprawnie, to współbieżna realizacja zbioru przepływów pracy jest poprawna jeżeli jest ona równoważna dowolnej sekwencyjnej realizacji tych przepływów pracy. Przy braku dodatkowych informacji o własnościach poszczególnych przepływów pracy zapewnienie powyższej równoważności wymaga zapewnienia globalnej uszeregowalności wszystkich zadań należących do współbieżnie wykonywanych przepływów pracy.

Globalne uszeregowanie zadań należących do różnych przepływów pracy wymaga takiej samej kolejności realizacji tych zadań na wszystkich jednostkach przetwarzania. Dla weryfikacji poprawności globalnego uszeregowania zadań system zarządzania przepływami pracy musi mieć dostęp do informacji o lokalnym uporządkowaniu zadań na poszczególnych jednostkach przetwarzania.

4.3 Odtwarzania przepływów pracy

Celem odtwarzania stanu spójnego przepływów pracy jest zapewnienie, że mimo wystąpienia awarii jednego z modułów zarządzania, po ich powtórnym uruchomieniu, nie zakończone przepływy pracy zostaną ostatecznie przeprowadzone przez system zarządzania do jednego z akceptowalnych stanów końcowych, zgodnie z ich specyfikacją. Przyjmuje się, że awarie poszczególnych jednostek przetwarzania i połączeń między nimi będą obsługiwane przez lokalne mechanizmy odtwarzania stanu spójnego poszczególnych jednostek.

5. Podsumowanie

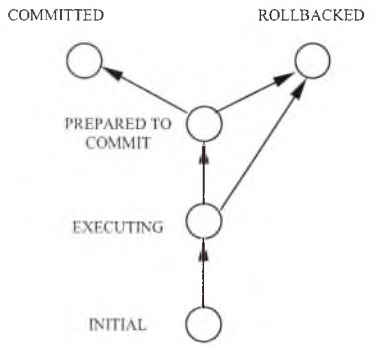
Na rynku informatycznym dostępne są narzędzia informatyczne, które wspomagają obsługę przepływów pracy. Jednak narzędzia te są budowane w oparciu o standardowe systemy baz danych i ograniczone do jednorodnych środowisk programowych, co powoduje, że gwarantują one poprawność wykonania jedynie poszczególnych transakcji, natomiast nie zapewniają globalnej poprawności transakcyjnego przepływu pracy. Również ich możliwości co do specyfikacji struktury zadań, struktury przepływu pracy i warunków poprawności realizacji przepływu, są bardzo ograniczone. W związku z tym problem budowy systemów zarządzających transakcyjnymi przepływami pracy jest ciągle otwartym i silnie eksplorowanym problemem badawczym.

jako kolekcja deskryptorów zależności danych (D^3). Każde deskryptor zawiera opis wzajemnych zależności między poszczególnymi danymi, łącznie z wymaganiami spójności danych i procedurami przywracania spójności. Politransakcja $\mathbf{T}^-$ jest domknięciem przechodnim transakcji T ze względu na wszystkie deskryptory D^3.

3. Specyfikacja transakcyjnych przepływów pracy

Specyfikacja transakcyjnych przepływów pracy obejmuje specyfikację zadań, struktury przepływu pracy i warunki poprawności.

Specyfikacja zadań określa strukturę realizacji każdego zadania. Struktura zadań jest zdefiniowana przez zbiór widocznych z zewnątrz stanów realizacji zadań, zbiór przejść między stanami oraz zbiór warunków, które muszą być spełnione dla realizacji tych przejść. Dodatkowo specyfikacja zadań może obejmować wymagania co do niezbędnych własności funkcjonalnych jednostek przetwarzania. Do specyfikacji zadań wykorzystuje się najczęściej diagramy przepływu stanów. Przykład specyfikacji zadania przedstawiono na Rys. 1.



Rys. 1. Specyfikacja zadania

Struktura przepływów pracy jest określona przez zależności między zadaniami wchodzącymi w skład danego przepływu pracy, przepływy danych między zadaniami i warunki zakończenia przepływu pracy. Struktura przepływu pracy może być definiowana w sposób statyczny lub dynamiczny.

W przypadku statycznej specyfikacji struktury przepływu pracy, wszystkie zadania i zależności między nimi muszą być znane przed jego uruchomieniem. Dla każdego zadania muszą być określone warunki wstępne jego realizacji. Warunki te mogą dotyczyć:

- stanu zadań - np. zadanie T_1 nie może wystartować zanim zadanie T_2 nie zostanie zakończone;
- wartości wyjściowych zadań - np. zadanie T_1 może wystartować jeżeli zadnie T_2 zwróciło wartość większą niż 125;
- zmiennych i zdarzeń zewnętrznych - np. zadanie T_1 nie może być wystartowane przed godziną 9.25 lub nie wcześniej niż dwie godziny po zakończeniu zadania T_2.

Przykład statycznej specyfikacji struktury przepływu pracy zilustrowano na rysunku 2.

WPROWADZENIE DO TRANSAKCYJNYCH PRZEPŁYWÓW PRACY

Jerzy Brzeziński, Tomasz Koszlajda

Naukowa i Akademicka Sieć Komputerowa

1. Wstęp.

Przez *przepływ pracy* rozumiemy zbiór powiązanych zadań wykonywanych na różnych jednostkach przetwarzania. Zadania definiują pewną pracą do wykonania i mogą być wyspecyfikowane w postaci luźnego tekstu, formatki lub programu komputerowego. Jednostkami przetwarzania, na których realizowane są zadania mogą być osoby, maszyny lub systemy komputerowe takie jak, programy do obsługi poczty elektronicznej, programy aplikacyjne lub systemy zarządzania bazami danych.

Transakcyjny przepływ pracy jest przepływem realizowanym w środowisku rozproszonych i heterogenicznych systemów baz danych, na który nałożono dodatkowe wymagania poprawności wykonania przepływu pracy, bazujące na własnościach transakcji znanych powszechnie jako ACID: atomowość, spójność, izolacja i trwałość. Koordynacja zadań składających się na przepływy pracy spełniająca określone wymagania poprawności może być realizowana ręcznie przez operatorów systemu bazy danych lub przez programy komputerowe tworzące *system zarządzania przepływami pracy*.

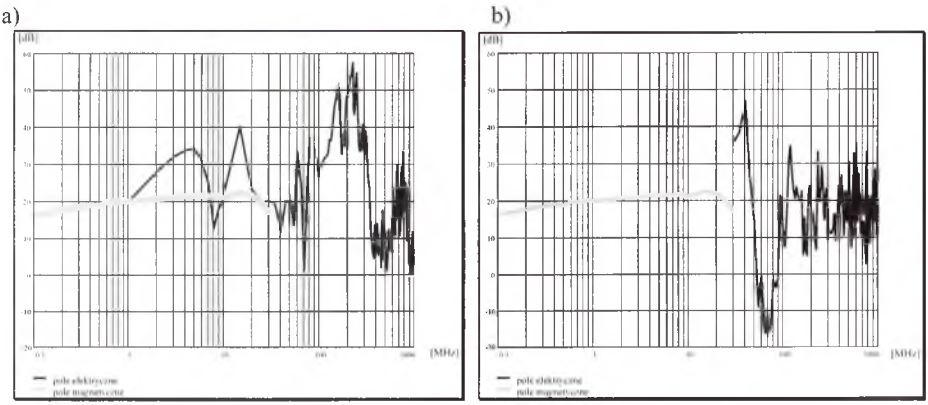
Przykładem transakcyjnego przepływu pracy może być proces realizacji zamówienia w hurtowni. Obejmuje on transakcje realizujące zadania: przyjęcia zamówienia, wystawienia faktury, pobrania towaru z magazynu, wyekspediowania go oraz odebrania należności za towar. Transakcyjnym przepływem pracy jest też obsługa żądań klientów, obejmująca rezerwację biletów lotniczych, miejsc hotelach oraz wynajem samochodów. Poszczególne zadania składające się na powyższe przepływy pracy wykonywane są w ogólności przez różne programy komputerowe, działające na różnych platformach programowo-sprzętowych, o różnych własnościach funkcjonalnych.

W niniejszym artykule przedstawiono podstawowe problemy związane ze specyfikacją i zarządzaniem transakcyjnymi przepływami pracy. W rozdziale drugim przedstawiono nowe modele transakcji, wykorzystywane do zarządzania współbieżnością w systemach zarządzania transakcyjnymi przepływami pracy. W rozdziale trzecim omówiono elementy specyfikacji przepływów pracy, a w rozdziale czwartym własności systemów zarządzania transakcyjnymi przepływami pracy.

2. Nowe modele transakcji

Klasyczny model transakcji często okazuje się niewystarczający dla nowych zastosowań systemów baz danych. Nie jest on odpowiedni dla bardzo długich transakcji (rzędu dni lub tygodni) (ang. *long-running activities*), charakteryzujących się ponadto potrzebą współdziałania (ang. *cooperating transaction*). Stosowanie w takich sytuacjach klasycznych transakcji o własnościach ACID wiąże się z szeregiem niedogodności:

- w wypadku wycofywania długiej transakcji wymagane jest wycofanie wszystkich wprowadzonych przez nią zmian, które są wynikiem tysięcy operacji;
- dla długotrwałych transakcji algorytmy zarządzania współbieżnością blokują znaczne ilości danych, co ogranicza współbieżność transakcji i może prowadzić do zablokowania całego systemu;



Rysunek 8. Skuteczność ekranowania szafy zmierzona dla pola elektromagnetycznego
a) polaryzacja pionowa
b) polaryzacja pozioma

Z wyników pomiarów wynika, że szafa ma słabe właściwości ekranujące. Można je poprawić zapewniając dobry kontakt elektryczny na wszystkich szczelinach i ekranując odpowiednio otwory wentylacyjne.

6. Podsumowanie

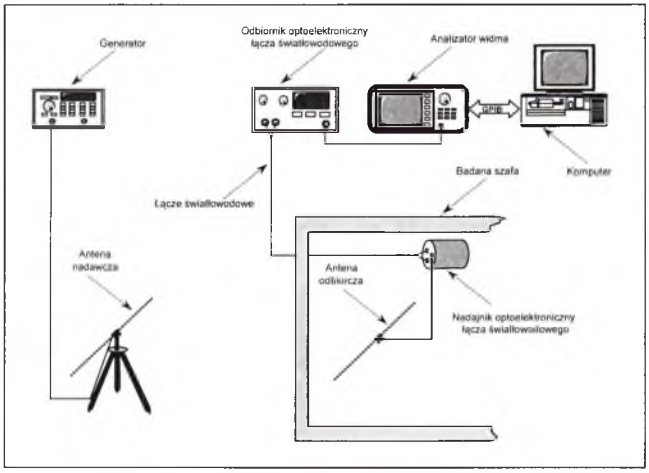
Idealna obudowa z punktu widzenia skuteczności ekranowania powinna być wykonana z grubej blachy i nie mieć żadnych szczelin ani otworów. W praktyce potrzebny jest dostęp do wnętrza obudowy w celu obsługi lub naprawy, a konieczność wyprowadzenia na zewnątrz przełączników, pokręteł, gniazd przyłączeniowych itp. wymaga wykonania otworów. Obudowa składa się więc zwykle z kilku połączonych ze sobą elementów, a w niektórych z nich są wykonane otwory. Rezystancje styku pomiędzy poszczególnymi częściami obudowy muszą być jak najmniejsze, otwory w obudowie małe w stosunku do długości fali, a jeżeli konieczne są duże to muszą być odpowiednio zabezpieczone. Przewody wychodzące na zewnątrz i wchodzące do środka muszą być odpowiednio ekranowane i filtrowane.

Obowiązuje zasada, że im większe są rezystancje styku elementów ekranu tym gorsze jego właściwości ekranujące. Stykające się powierzchnie muszą być zatem zabezpieczone przed korozją czy utlenianiem, a dla dobrego styku elektrycznego muszą być dociśnięte do siebie z odpowiednią siłą. Nie może być mowy o malowaniu farbami o ile nie są to odpowiednie farby przewodzące. Przy konstruowaniu ekranu z kilku rodzajów materiałów należy materiały tak dobrać aby nie występowały między nimi efekty elektrochemiczne pogarszające z czasem jakość styku. Drzwi i otwierane ścianki boczne powinny być zabezpieczone elektromagnetycznie za pomocą odpowiednich "uszczelek" (ang. *gaskets*).

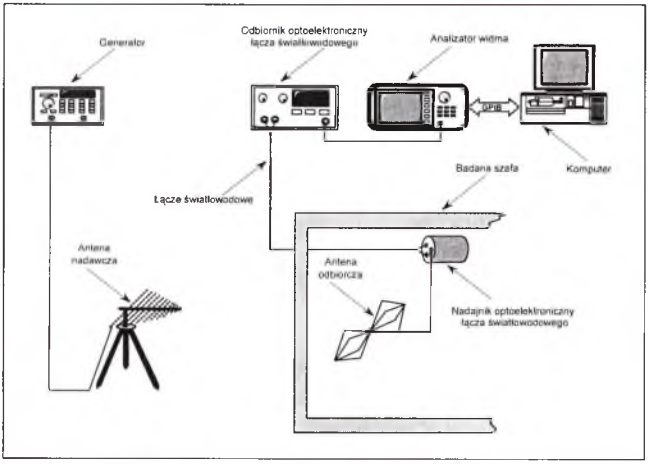
Produkowany jest cały szereg uszczelek do różnych zastosowań. Najbardziej rozpowszechnione rodzaje to:

- uszczelki w postaci siatki drucianej z elastycznym rdzeniem lub bez niego
- uszczelki w postaci zwiniętej sprężyny
- uszczelki składające się ze sprężynujących pasków
- uszczelki z materiałów elastycznych domieszkowanych materiałami przewodzącymi.

Dwa pierwsze rodzaje uszczelek mają bardzo dobre właściwości ekranujące, ale dla poprawnego działania wymagają dużej siły ściskającej i to równomiernie rozłożonej na całej



Rysunek 5. Schemat układu pomiarowego do badania skuteczności ekranowania w polu bliskim dla pola elektrycznego (zgodnie z zaleceniem IEEE-STD-299-1991), odległość anteny nadawczej ściany szafy wynosi 3 m, a antena odbiorcza jest umieszczona symetrycznie w środku



Rysunek 6. Schemat układu pomiarowego do badania skuteczności ekranowania w polu dalekim (zgodnie z zaleceniem IEEE-STD-299-1991), odległość anteny nadawczej ściany szafy wynosi 3 m, a antena odbiorcza jest umieszczona symetrycznie w środku szafy

Stanowiska pomiarowe zestawiano w komorze bezechowej. Konfigurację stanowiska przedstawiono na rysunku (*Rysunek* 7). Anteny nadawcze są pobudzane za pomocą generatora sygnałowego, znajdującego się na zewnątrz komory. Sygnał z anten odbiorczych jest przesyłany za pomocą łącza optoelektronicznego do analizatora widma znajdującego się również na zewnątrz komory bezechowej. Łącze optoelektroniczne zostało wykorzystane w celu uniemożliwienia

Skuteczność ekranowania badanego materiału S wyrażona w decybelach, wyznaczana jest z jednej z następujących zależności:

$$S = 10 * log(P_0 / P_p), \quad S = 20 * log(E_0 / E_p), \quad S = 20 * log(H_0 / H_p)\ [dB] \quad (2)$$

Dla prawidłowego przeprowadzenia pomiaru, ekran powinien rozciągać się w nieskończoność. Przy badaniu pomieszczenia ekranowanego lub obudowy problemem jest występowanie szeregu częstotliwości rezonansowych zależnych od rozmiarów geometrycznych badanego obiektu. Na wyniki pomiaru ma wpływ rodzaj użytej anteny i sposób jej umieszczenia, gdyż każda przewodząca płaszczyzna znajdująca się w pobliżu anteny zmienia jej parametry. Dla pomieszczeń ekranowanych opracowano odpowiednie procedury pomiarowe eliminujące efekty rezonansów oraz normujące rodzaje anten i sposoby ich umieszczenia. Częstotliwości pomiarowe dobierane są poniżej i powyżej częstotliwości głównych rezonansów komory.

W większości metod pomiaru skuteczności ekranowania pomieszczeń ekranowanych wykorzystuje się takie same ogólne zasady. Metody różnią się jedynie szczegółami związanymi z aparaturą pomiarową, częstotliwościami pomiarowymi, sposobem ustawienia anten itp. Najczęściej wykorzystuje się metody opisane w standardzie MIL-STD-285 lub w IEEE-STD-299-1991.

MIL-STD-285 [2] opracowano w USA dla potrzeb wojskowych i opublikowano w 1956 roku. Stała się ona najbardziej popularną normą ujednolicającą sposoby pomiaru charakterystyki tłumienia pola elektromagnetycznego przez pomieszczenia ekranowane w zakresie od 100 kHz do 10 GHz. Standard podaje częstotliwości i pola będące przedmiotem pomiaru, specyfikuje przyrządy potrzebne do przeprowadzenia pomiaru, opisuje konfigurację anten. Źródło sygnału umieszcza się wewnątrz badanego pomieszczenia, a odbiornik na zewnątrz. Pomiar charakterystyki tłumienia jest wykonywany tylko dla pięciu częstotliwości, pomimo że wymagania standardu odnoszą się do stosunkowo szerokiego zakresu częstotliwości.

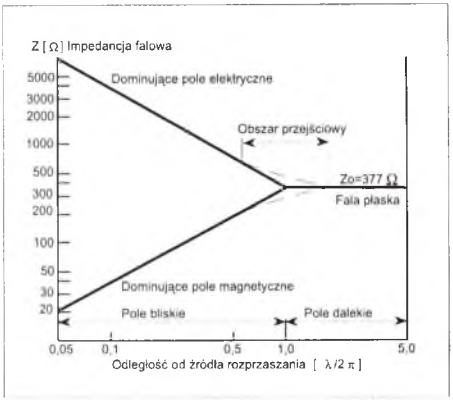
IEEE-STD-299-1991 [3] opublikowano w roku 1991 z zamiarem uaktualniania normy MIL-STD-285. Poszerzono zakres częstotliwości pomiarowych do 14 kHz - 18 GHz, a pomiary wykonuje się dla 7 częstotliwości wybieranych z podanych w normie podzakresów. Źródło sygnału umieszcza się na zewnątrz badanego pomieszczenia, a odbiornik wewnątrz. Norma podaje również zalecane rodzaje anten i sposób ich umieszczenia. W zakresie niskich częstotliwości przewiduje się pomiary jedynie dla pola magnetycznego przez co wyeliminowano, wymagane w normie MIL-STD-285, kłopotliwe pomiary pola elektrycznego w polu bliskim za pomocą anten prętowych (wyniki pomiarów silnie zależą od wpływów otoczenia przez co trudno uzyskać ich powtarzalność).

4. Opis przyjętej metody i stanowiska pomiarowego skuteczności ekranowania szafy

Metodę pomiaru skuteczności ekranowania szafy opracowano na podstawie procedur pomiarowych i zaleceń zawartych w normie IEEE-STD-299-1991.

Odstępstwem od zaleceń normy jest prowadzanie pomiarów dla jak najgęstszego rastra częstotliwości, gdyż badana szafa, ze względu na brak kontaktu elektrycznego na krawędziach pomiędzy poszczególnymi elementami, musi mieć silne właściwości rezonansowe dla wielu częstotliwości. Te częstotliwości rezonansowe charakteryzują szafę, podkreślając jej właściwości, które nie zostałyby zauważone przy pomiarze tylko dla 7 częstotliwości jak zaleca norma IEEE-STD-299-1991.

Pomiar skuteczności ekranowania dla pola magnetycznego przeprowadzono za pomocą anten ramowych ustawionych równolegle do ściany szafy w odległościach równych 30 cm (*Rysunek 4*). Antenę odbiorczą umieszczono wewnątrz szafy, w środku jej wysokości, a antenę nadawczą na zewnątrz. Przy pomiarach poziomu odniesienia anteny ustawiono równolegle do



Rysunek 1. Zależność impedancji falowej od odległości od źródła i rodzaju pola

- pole bliskie (indukcyjne) występujące w pobliżu źródła w odległości $r < \lambda/2\pi$ - właściwości pola określone są przez właściwości źródła,
- pole dalekie (promieniowania) w odległości $r > \lambda/2\pi$ (w przybliżeniu 1/6 długości fali), - właściwości pola zależą głównie od ośrodka, w którym odbywa się propagacja,
- obszar przejściowy wokół granicy pomiędzy tymi obszarami $r \approx \lambda/2\pi$.

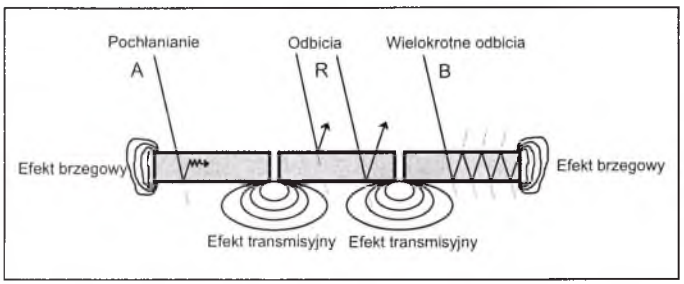
W praktyce za pole dalekie przyjmuje się obszar w odległości $r > 5\lambda/2\pi$.

Dla pola dalekiego stosunek natężenia pola elektrycznego E do natężenia pola magnetycznego H (impedancja falowa) równa się impedancji charakterystycznej (dla wolnej przestrzeni $E/H = Z_o = 377\ \Omega$). W polu bliskim stosunek E/H określony jest przez właściwości źródła rozpraszania elektromagnetycznego i odległość od źródła:

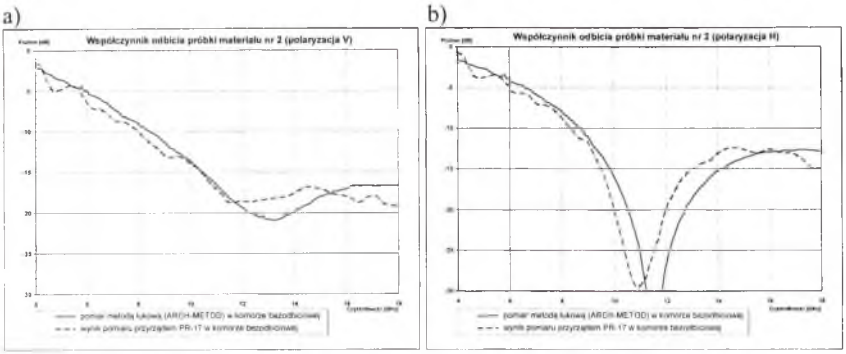
- w przypadku gdy źródło ma duży prąd i małe napięcie wtedy stosunek $E/H < 377\ \Omega$ a w polu bliskim przeważa pole magnetyczne,
- w przypadku gdy źródło ma mały prąd i duże napięcie wtedy stosunek $E/H > 377\ \Omega$ a w polu bliskim przeważa pole elektryczne.

Z tego względu w polu bliskim pola elektryczne i magnetyczne są rozpatrywane oddzielnie. W polu dalekim ulegają one kombinacji tworząc falę płaską o stosunku E/H równym 377 Ω.

Podstawowym parametrem ekranów jest charakterystyka skuteczności ekranowania S_s (dB) w funkcji częstotliwości. Miarą skuteczności ekranowania jest tłumienność określająca zmniejszenie natężenia pola magnetycznego i (lub) pola elektrycznego po przejściu przez ekran. Skuteczność danego ekranu przy określonej częstotliwości zależy od materiału, grubości ścianek konstrukcji ekranującej i odległości między powierzchnią ekranująca a źródłem promieniowania. Skuteczność ekranów idealnych (czyli w pełni jednorodnych, bez złącz, szczelin i otworów) można obliczyć przy pomocy zależności matematycznych. Rzeczywiste ekrany mają skuteczność ekranowania znacznie mniejszą z powodu niejednorodności i przerw w powierzchni ekranującej. Charakterystyki ekranów rzeczywistych najłatwiej wyznaczyć na drodze pomiarów.



Rysunek 2. Oddziaływanie materiału ekranującego na pole elektromagnetyczne



Rys. 8. Charakterystyka częstotliwościowa współczynnika odbicia próbki materiału tłumiącego nr 2: a) polaryzacja V, b) polaryzacja H

4.4. Wnioski

Przeprowadzone badania miały na celu sprawdzenie możliwości wdrożenia metody łukowej do pomiaru współczynnika odbicia materiałów tłumiących w komorze bezodbiciowej ITA PWr.

Układ pomiarowy zestawiony z przyrządów zalecanych przy metodzie łukowej umożliwił wykonanie wstępnych pomiarów współczynnika odbicia. Dla wykonanego układu pomiarowego minimalne rozmiary próbek w badanym zakresie częstotliwości powinny wynosić 100x100 cm Ponieważ posiadane próbki miały mniejsze rozmiary (50x50 cm, 30x30 cm, 20x20 cm), to wykonane pomiary należy traktować jako orientacyjne i obarczone błędem metody. Dokładnie natomiast zmierzono tło komory, co pozwoliło określić czułość układu pomiarowego na około -40 dB. Uzyskane wyniki pomiarów i wyniki z pomiarów reflektometrem PR-17 CXKu wykazują dużą zbieżność.

Dalsze badania powinny być kontynuowane w komorze bezodbiciowej. Wdrożone w wyniku badań stanowisko pomiarowe umożliwi precyzyjne pomiary współczynnika odbicia materiałów tłumiących.

5. LITERATURA

[1]. W. E. Grzebyk, J. M. Janukiewicz, „Detekcja informacji użytecznej w sieciach komputerowych", Materiały Seminarium MIEDZESZYN'97, 21-23 Maj 1998, str. 151-165.

[2]. Draft IEEE Standard PAR-1128, "IEEE Recommended practice for RF absorber evaluation in the range 30 MHz to 5 GHz", March, 1995.

[3]. MIL-STD-252, „Military Standard Attenuation Measurements for Enclosures, Electromagnetics Shielding for Electronic Test Purposes, Method of.", United States Goverment Printing Office, Washington 1956.

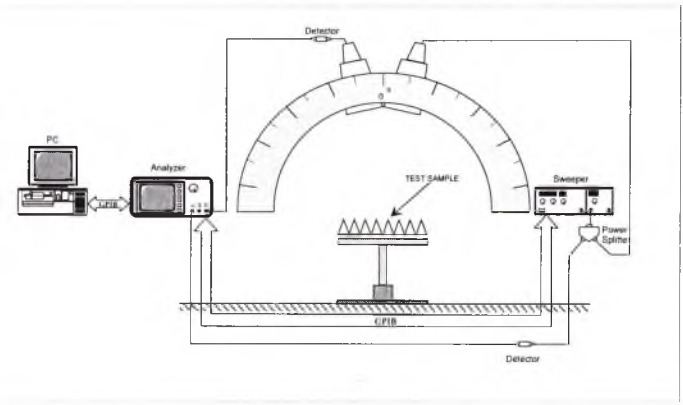
[4]. „Reflectometer Operating and Maintenance Manual", Millimeter Wave Technology, Inc., Revision B, 15 August 1996.

Czwarta z metod, będąca modyfikacją trzeciej metody. różni się od niej zastosowaniem zamiast falowodu linii współosiowej o odpowiednim przekroju i długości. Współczynnik odbicia jest obliczany z mierzonego na wejściu układu sygnału.

Podczas pomiarów prowadzonych w ITA PWr zmierzono próbki materiałów tłumiących stosując układ pomiarowy zmontowany w komorze bezodbiciowej. Stosowana była metoda łukowa (ang. arch metod) pomiaru współczynnika odbicia.

4.1. Opis metody łukowej

Klasyczną metodą pomiaru charakterystyk częstotliwościowych współczynnika odbicia materiałów jest metoda łukowa.



Rys. 4. Metoda łukowa - konfiguracja stanowiska pomiarowego

Charakteryzuje się ona tym, że anteny nadawcza i odbiorcza montowane są na platformie w kształcie półokręgu ponad stołem pomiarowym na którym umieszczany jest badany materiał tłumiący [2]. Antena nadawcza oświeca badany materiał i odbita wiązka powraca do anteny odbiorczej (rys. 4).

Współczynnik odbicia materiału wyznacza się metodą porównawczą. Porównywane są dwie mierzone wielkości:

- sygnał odbity od dobrze przewodzącej powierzchni umieszczonej w miejscu pomiaru materiału tłumiącego,
- sygnał odbity od materiału tłumiącego umieszczonego na wcześniej mierzonej powierzchni przewodzącej.

W przypadku gdy materiał wykazuje zmiany poziomu odbicia w zależności od polaryzacji pola elektromagnetycznego, pomiar należy wykonywać dla różnych polaryzacji anten. Natomiast jeżeli materiał wykazuje właściwości kierunkowe odbicia, należy zmieniać kąt ustawienia anten przesuwając je po łuku platformy pomiarowej, w celu wyznaczenia zależności poziomu odbicia od kierunku rozchodzenia się promieniowania pola elektromagnetycznego. Teoretycznie „arch metod" nie ma ograniczeń częstotliwościowych, W praktyce nie jest ona jednak stosowana poniżej 1 GHz [2]. Wynika to z faktu, że badana próbka musi się znajdować w polu dalekim anten pomiarowych, co zazwyczaj wymaga dużych rozmiarów platformy pomiarowej oraz badanej próbki. Warunkiem poprawności metody pomiarowej jest zachowanie minimalnej odległości anten od badanej próbki określonej zależnością [2]:

niestety kosztowne. Taki poligon pomiarowy może wówczas być wykorzystywany nie tylko przy pomiarach emisyjności, ale także do innych celów, np. cechowania anten pomiarowych.

W normie PN-EN 55022 określono nie tylko minimalne rozmiary przewodzącej płaszczyzny, ale również jej kształt. Przykład takiej płaszczyzny odniesienia zobrazowano na rysunku 3.

Sprawdzenie miejsca, w którym są wykonywane pomiary jest w każdym przypadku konieczne, nawet wtedy gdy spełnione są wymagania normy odnośnie wielkości wolnej od przeszkód powierzchni, oraz minimalnych rozmiarów ziemi odniesienia. W załączniku do normy EN 55022 podano również sposoby sprawdzania tzw. alternatywnych stanowisk pomiarowych.

W pojęciu tym mieszczą się wszystkie ekranowane i wyłożone materiałem pochłaniającym (absorberem) hale pomiarowe. Sprawdzenie przydatności alternatywnych stanowisk pomiarowych jest procesem złożonym i trudnym. W zamkniętych pomieszczeniach nie jest możliwe całkowite wyeliminowanie wpływu odbić od ścian.

4. Pomiary charakterystyk częstotliwościowych odbicia materiałów tłumiących w komorze bezodbiciowej

Wpływ pola elektromagnetycznego emitowanego przez urządzenia można ograniczyć stosując ekranowanie pomieszczeń lub wykładziny z materiałów tłumiących pole elektromagnetyczne. Dla zachowania kompatybilności wewnętrznej systemu lub realizacji alternatywnych stanowisk pomiarowych emisyjności istotny jest poziom absorpcji fali elektromagnetycznej przez materiały tłumiące. Opis stanowiska pomiarowego umożliwiającego pomiar skuteczności ekranowania materiałów lub pomieszczeń jest przedstawiony w pracy [1]. W niniejszym rozdziale zostanie przedstawiona metodyka pomiarów charakterystyk częstotliwościowych współczynnika odbicia materiałów tłumiących. Materiały tłumiące, podobnie jak materiały ekranujące, mogą być stosowane jako element redukujący poziom rozpraszania elektromagnetycznego.

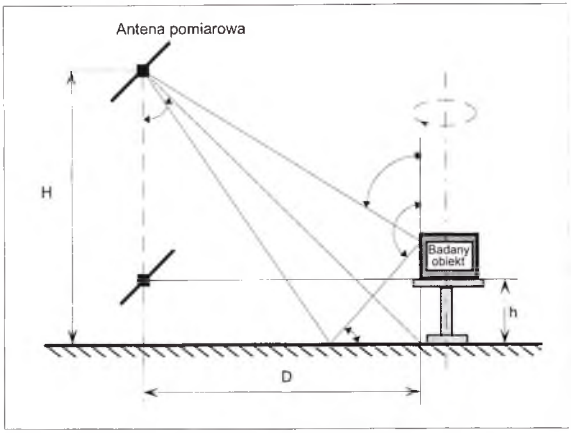
W ramach badań mających na celu sprawdzenie możliwości oraz opracowanie metodyki pomiarów charakterystyk częstotliwościowych odbicia materiałów tłumiących w komorze bezodbiciowej przeprowadzono pomiary kilku próbek materiałów tłumiących.

Obecnie używane są cztery techniki pomiarowe do wyznaczenia wartości współczynnika odbicia dla materiałów tłumiących (absorberów).

W pierwszej z nich nazywanej metodą łukową (ang. arch metod) używa się anten nadawczej i odbiorczej umieszczonych na łuku koła, ustawionych w kierunku powierzchni materiału tłumiącego (rys. 4) umieszczonego w środku koła. Antena nadawcza oświetla materiał, fala odbita jest mierzona przez antenę odbiorczą. W metodzie tej kąt padania i odbicia fali jest regulowany przez przemieszczenie anten po łuku koła. Polaryzacja fali jest zależna od typu anten i odpowiedniego ich ustawienia.

Druga z metod nazywana jest metodą czasową (ang. time-domain metod). Badany materiał jest montowany na dowolnej ścianie w pomieszczeniu zamkniętym. Antena nadawcza oświetla absorber krótkim impulsem elektromagnetycznym. Fala odbita jest mierzona przez antenę odbiorczą. Po wykonaniu przekształceń matematycznych odebranego sygnału można wyznaczyć współczynnik odbicia w funkcji częstotliwości. Wpływ odbić od ścian, podłogi, sufitu może być wyeliminowany poprzez użycie odpowiedniego okna czasowego i przekształcenia matematyczne odebranego sygnału.

Trzecia metoda wykorzystuje falowód o odpowiednio dużym przekroju i długości. Przez układ dopasowujący falowód jest dołączony do miernika współczynnika odbicia. Koniec falowodu jest przesłonięty badanym materiałem. Wartość współczynnika odbicia jest wyznaczana na podstawie zmierzonego na wejściu do falowodu sygnału.



Rys 1. Zasada pomiaru zakłóceń promieniowanych

Tak więc jeśli kombinacja zakłóceń zewnętrznych i zakłóceń od badanego urządzenia nie przekracza dopuszczalnych poziomów, to nie trzeba redukować wpływu zakłóceń zewnętrznych. Uznaje się wówczas, że badane urządzenie spełnia wymagania. W przypadku, gdy wymieniona kombinacja sygnałów przekracza dopuszczalne poziomy, to aby uznać urządzenie za spełniające wymagania, należy dla każdej częstotliwości pomiarowej wykazać, że poziom zakłóceń zewnętrznych jest co najmniej o 6 dB niższy od wypadkowego poziomu zakłóceń badanego urządzenia i zakłóceń zewnętrznych. Wspomniane niedogodności doprowadziły do nowego podejścia w projektowaniu stanowisk pomiarowych na poligonach. Pierwszym krokiem było umieszczenie ich w specjalnych warunkach terenowych, które zapewniały:

- niski poziom pól elektromagnetycznych środowiska,
- oddalenie od urządzeń, na które wpływałyby pola wytwarzane podczas pomiarów,
- odpowiednie warunki do testowania nawet dużych urządzeń.

Drugim krokiem było uniezależnienie się od warunków atmosferycznych oraz zabezpieczenie stanowisk pomiarowych podczas przerw w pomiarach.

Poligon pomiarowy

Poligon pomiarowy stanowi płaska powierzchnia o odpowiednio przygotowanej ziemi (tzw. ziemia odniesienia), z doprowadzoną energią zasilania, stołem pomiarowym (najczęściej obrotowym), masztem antenowym z odpowiednim zestawem anten oraz odpowiednimi osłonami pogodowymi.

Poligon pomiarowy powinien być umieszczony na odpowiednio rozległym i płaskim terenie. W pobliżu nie powinny znajdować się budynki lub jakiekolwiek konstrukcje stalowe powodujące niekontrolowane odbicia fal elektromagnetycznych. Nad poligonem nie powinny przebiegać napowietrzne linie energetyczne. Najlepiej jeśli znajduje się on w terenie osłoniętym, np. w kotlinach, co może być dodatkową osłoną przed obcymi źródłami zakłóceń. Jako osłony mogą być wykorzystane ściany budynków. Muszą one jednak znajdować się wystarczająco daleko, aby ewentualne odbicia od nich nie wpływały na wynik pomiarów natężenia pola elektromagnetycznego. Z doświadczenia wynika, że odległość około 20 m gwarantuje takie warunki. Należy także pamiętać o zapewnieniu odpowiedniej odległości od przedmiotów odbijających znajdujących się nad wybranym terenem. Ogólnie zakłada się, że wystarczy zapewnić

Tabela 3.

Klasa B		
Zakres częstotliwości [MHz]	**Poziom dopuszczalny [dB (μV)]**	
	Wartość quasi-szczytowa	**Wartość średnia**
0,15 ÷ 0,50	66 ÷56	56 ÷46
0,50 ÷ 5	56	46
5 ÷ 30	60	50
• Na częstotliwościach granicznych 0,50 MHz i 5 MHz obowiązuje poziom niższy. • W zakresie częstotliwości 0,15 - 0,50 MHz poziom opada liniowo w funkcji częstotliwości podane w skali logarytmicznej		

Poziomy dopuszczalne zakłóceń przewodzonych (napięcie zakłóceń radioelektrycznych) na zaciskach zasilania sieciowego dla urządzeń klasy A i B według PN-EN 55022 przedstawiono w tabelach 2 i 3.

Poziomy dopuszczalnych zakłóceń promieniowanych (natężenie zakłócających pól radioelektrycznych) dla urządzeń klasy A i B przy odległości pomiarowej 10 m według PN-EN 55022 przedstawiono w tabelach 4 i 5.

Tabela 4.

Klasa A	
Zakres częstotliwości [MHz]	**Poziom dopuszczalny quasi-szczytowy [dB (μV/m)]**
30 ÷ 230	40
230 ÷1000	47
• Na częstotliwości granicznej 230 MHz obowiązuje poziom niższy. • Jeśli podczas pomiarów występują zakłócenia powodowane przez sygnały obce, to konieczne mogą okazać się dodatkowe środki ochrony	

Tabela 5.

Klasa B	
Zakres częstotliwości [MHz]	**Poziom dopuszczalny quasi-szczytowy [dB (μV/m)]**
30 ÷ 230	30
230 ÷1000	37
• Na częstotliwości granicznej 230 MHz obowiązuje poziom niższy. • Jeśli podczas pomiarów występują zakłócenia powodowane przez sygnały obce, to konieczne mogą okazać się dodatkowe środki ochrony	

powyżej poziomu odporności urządzeń aktywnych. Skutkiem tego są zakłócenia działania pracy węzła.

Właściwości elektromagnetyczne kabli wraz z połączeniami rozłącznymi mogą być określane za pomocą następujących pomiarów:

- pomiar tłumienia ekranów i połączeń ekranów kabla,
- pomiar tłumienia ekranu obudowy i impedancji sprzężenia ekranowanych połączeń rozłącznych
- pomiar tłumienia sprzężenia między różnymi przewodami i kablami

Struktura, wielkość, forma, materiał oraz inne elementy konstrukcji mechanicznej węzła mogą mieć wiele postaci. Konieczna jest więc znajomość właściwości emisyjnych poszczególnych elementów. Do określenia tych właściwości wykonuje się następujące badania:

- pomiar odporności obiektów na sprzężenia,
- pomiar skuteczności ekranowania metodą „środkowego punktu przestrzeni",
- pomiar wielkości tłumienia ekranu w miejscach nieciągłości konstrukcji mechanicznych.

W węźle sieci są zazwyczaj instalowane urządzenia, okablowanie, szafy telekomunikacyjne. Ponadto w węźle stosuje się filtry, elementy ochrony przepięciowej i elementy dopasowujące złączy. Elementy te występują głównie w złączach urządzeń dlatego konieczna jest znajomość ich właściwości kompatybilnościowych.

Podstawowym problemem w badaniach systemów pod względem kompatybilności elektromagnetycznej jest brak wiążących norm dla jej oceny i norm dotyczących badań systemów. Znana jest niemiecka norma VG 95372 i pochodne opisujące zagadnienia związane z EMC na poziomie systemów i instalacji. Pozostałe normy dotyczą elementów składowych systemów. Dotyczy to również sieci komputerowych, a w szczególności węzłów sieci. Jeżeli rozmiary węzła nie są zbyt duże, to istniejące normy - dotyczące pojedynczych urządzeń - mogą być stosowane również do badania całego węzła. Jeżeli rozmiary węzła przekraczają dopuszczalne gabaryty, określone w normach, to węzeł sieci należy rozłożyć na mniejsze części. Należy przy tym pamiętać, by połączenia pomiędzy urządzeniami były prawidłowo rozdzielone.

Pojedyncze urządzenia sprawdzone pod względem kompatybilności elektromagnetycznej - połączone w węźle sieci komputerowej w jeden system - nie zawsze spełniają warunki kompatybilności elektromagnetycznej dla całego systemu.

3. Metody pomiaru rozpraszania elektromagnetycznego urządzeń telekomunikacyjnych stosowanych w węzłach sieci komputerowych (normy i zalecenia)

Urządzenia informatyczne i telekomunikacyjne są objęte wspólnymi normami dotyczącymi kompatybilności elektromagnetycznej. Obecnie opracowuje się niezależne normy dla urządzeń informatycznych i urządzeń telekomunikacyjnych. W Polsce dla urządzeń techniki informatycznej (ITE) podstawową w zakresie emisyjności jest norma PN-EN 550022 - „Dopuszczalne poziomy i metody pomiaru zakłóceń radioelektrycznych wytwarzanych przez urządzenia informatyczne (CISPR 22:1993) - odpowiednik EN550022 (1994)" (*Tabela 1*).

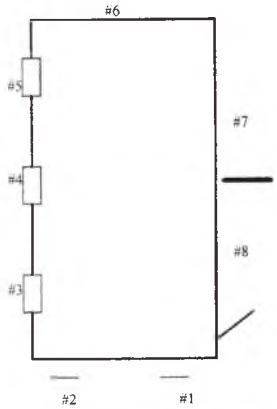
Zgodnie z wymienioną normą urządzenia informatyczne (ITE) są zasilane napięciem niższym niż 600 V, a ich zadaniem jest szeroko rozumiane przetwarzanie informacji. Urządzenia informatyczne służą do wyświetlania, transmisji, przetwarzania, przełączania lub sterowania danymi i informacjami telekomunikacyjnymi. Zazwyczaj są one wyposażone w jedno lub więcej złącz służących do przesyłania informacji.

Szczególną wagę posiada zagadnienie weryfikacji osiągnięcia celu, tj. szczelności elektromagnetycznej wykonanego ekranu. Między innymi wiąże się to z doborem odpowiedniej metodyki pomiarowej, tak aby wyniki mogły być możliwie „obiektywne", osadzone w standardach i porównywalne. Z tego względu pomiarów dokonano przy współudziale uznanych autorytetów w tej dziedzinie.

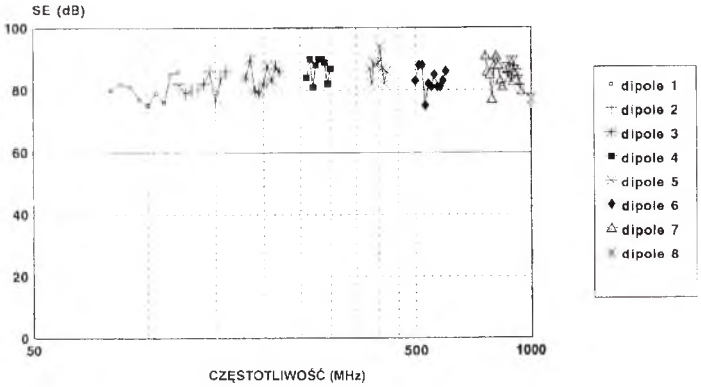
Wyniki pomiarów w pełni potwierdzają uzyskanie zakładanych celów w technologii elastycznych materiałów przewodzących. Przykładowe wyniki pomiarów przedstawiono na rys. 1 (4.

LITERATURA

1. Barczak A.: Analiza norm pomiarowych w aspekcie potrzeb bezpieczeństwa sieci komputerowych. Praca zbiorowa, Zegrze 1996.
2. Barczak A., Macherzyński L., Szuszkiewicz T., Wolski P.: Wybrane problemy ekranowania elektromagnetycznego pomieszczeń przy użyciu elastycznych materiałów przewodzących. V Krajowa Konferencja Naukowa KNSŁ – 96. Systemy Łączności i Informatyki na potrzeby ochrony i bezpieczeństwa RP. Zegrze, 02-04 października 1996.
3. Barczak A., Macherzyński L., Szuszkiewicz T., Wolski P., Silicki K.: Problemy ochrony informacji w sieciach komputerowych. Opracowanie: Wyższa Szkoła Oficerska Wojsk Łączności. Naukowa i Akademicka Sieć Komputerowa NASK Zeszyty Naukowe Politechniki Śląskiej. Seria Informatyka z. 32, Gliwice 1997.
4. Barczak A., Macherzyński L., Szuszkiewicz T., Wolski P.: Zapoznanie z metodyką i praktycznym wykonywaniem pomiarów tłumienności elektromagnetycznej w oparciu o normę MIL-STD 285. Materiały z seminarium, Zegrze, 11-13 maja 1997.



Rys. 1. Lokalizacja punktów pomiarowych w pomieszczeniu ekranowanym elektromagnetycznie węzła sieci komputerowej



Rys. 2. Wyniki pomiaru pomieszczenia w punkcie 1

- efektywność ekranowania ponad 60 dB przy dominowaniu efektu odbicia fali nad efektem tłumienia;
- duża różnorodność struktur i właściwości fizycznych, a zatem również duża swoboda konstrukcyjna;
- mały ciężar właściwy, cienkie warstwy, wiotkość i elastyczność, dzięki czemu można formować dowolne kształty;
- wysoka odporność na korozję i tzw. efekty starzenia.

Te cechy materiałów określanych często jako elastyczne materiały przewodzące tworzą zupełnie nowe możliwości konstrukcyjne.

Ekranowanie pomieszczeń węzła z użyciem elastycznych materiałów przewodzących dokonuje się przez tapetowanie, tzn. wykłada się nimi ściany, sufit, podłogę i pokrywa się następnie normalną tapetą i wykładziną. Oprócz roli dekoracyjnej normalna tapeta pełni rolę warstwy ochronnej. Technologia ta może być zatem zastosowana w każdym pomieszczeniu, które można wytapetować, a podłogę pokryć wykładziną bądź z wykorzystaniem podwójnej podłogi. Okna są ekranowane poprzez system rolet z elastycznego materiału przewodzącego odpowiedniego na roletę. Tapetuje się również drzwi i uszczelnia odpowiednimi uszczelkami, podobnie rury grzewcze, gazowe, wodociągowe i kanalizacyjne.

Pozostałe elementy węzła sieci komputerowej (energetyka, klimatyzacja, linie telefoniczne, kable sieci komputerowej itp.) mogą być filtrowane w sposób tradycyjnie stosowany. Ponieważ nie potrzeba i nie ma uzasadnienia stosowania rozwiązań dających parametry znacznie ponad 60 dB, ponoszone koszty komponentów uzupełniających mogą być znacznie obniżone w porównaniu z rozwiązaniami stosowanymi w kabinach metalowych.

W rezultacie powstałe pomieszczenie ekranowane jest normalnie wyglądającym pomieszczeniem. Nie istnieje potrzeba spełniania żadnych szczególnych wymogów budowlanych, konstrukcyjnych i montażowych. Fakt, że pomieszczenie nie wyróżnia się szczególnie spośród innych, ma również ważne aspekty dla bezpieczeństwa węzłów sieci komputerowych.

Zaprojektowano i wykonano pomieszczenie ekranowane elektromagnetycznie w technologii elastycznych materiałów przewodzących o powierzchni użytkowej 48 m^2. Zespół autorski rozwiązał szereg zagadnień, a w szczególności:

- Rozpoznano i dokonano wyboru z szerokiej gamy oferowanych na rynkach światowych produktów elastycznych materiałów przewodzących takich, które charakteryzował zarówno odpowiedni współczynnik ekranowania, jak i cechy fizyczno-konstrukcyjne umożliwiające ich użycie w postaci tapety;
- Opracowano technologię odpowiedniego przygotowania podłoża oraz montażu materiału jako tapety, w tym uszczelniania, zakładek, doboru odpowiednich klejów itp.;
- Dokonano analiz podatności materiału na utraty własności ekranujących na skutek zjawiska korozji i innych procesów fizykotechnicznych związanych ze starzeniem;
- Opracowano odpowiednie rozwiązania dla otworów okiennych, drzwi, kanałów wentylacyjnych, ogrzewania, zasileń energetycznych, linii telekomunikacyjnych oraz elementów konstrukcyjnych, takich jak mocowanie oświetlenia, elementy wystroju itp.;

Węzły sieci komputerowych powinny być chronione elektromagnetycznie w sposób szczególny, zaś w praktyce konkretna realizacja sposobu ochrony wymaga analizy i oceny ryzyka, zwymiarowania potencjalnych strat oraz kosztów tej ochrony.

Zjawisko promieniowania elektromagnetycznego – a zatem i potrzeby ekranowania w odniesieniu do bezpieczeństwa sieci i węzłów systemów komputerowych ma co najmniej dwa aspekty:

- Sprzęt elektroniczny będący na wyposażeniu węzła sieci komputerowej nie powinien być podatny na promieniowanie elektromagnetyczne występujące w jego otoczeniu. Jest to podstawowy warunek uzyskania stabilności i niezawodności pracy węzła. Należy przy tym mieć na uwadze, że tak zwane „normalne" środowisko pracy jest w coraz większym stopniu „zaśmiecane" elektromagnetycznie zarówno przez typowe nadajniki (np. telefony komórkowe), jak również urządzenia przemysłowe i sprzęt powszechnego użytku. W stosunku do niektórych węzłów może istnieć potrzeba przeciwdziałania celowym próbom zakłócania na drodze elektromagnetycznej.
- Promieniowanie elektromagnetyczne emitowane przez sprzęt pracujący w węźle jest nośnikiem przetwarzanych danych, w tym takich, które powinny pozostać poufne, tajne lub ściśle tajne ze swej natury lub z uwagi na potrzeby zapewnienia bezpieczeństwa funkcjonowania węzła.

Znane są trzy podstawowe kierunki poszukiwań rozwiązań problemu bezpieczeństwa systemów w aspekcie promieniowania elektromagnetycznego.

Jest to:

- Stosowanie wydzielonych stref na tyle przestrzennie rozległych, aby wypromieniowana energia elektromagnetyczna uległa naturalnemu rozproszeniu w ich obrębie do poziomu uznanego za bezpieczny, bądź aby docierające promieniowanie spoza strefy zostało wystarczająco rozproszone i wytłumione.
- Konstruowanie sprzętu, którego poziom emisji elektromagnetycznej byłby na tyle mały, że przechwycenie tą drogą przetwarzanych danych można by było uznać za praktycznie niemożliwe w sensie technologicznym lub też wymaganych nakładów. Powyższe rozumowanie odnosi się także do odporności sprzętu na zakłócenia.
- Ekranowanie, tj. konstruowanie hermetycznych osłon z materiałów charakteryzujących się dobra tłumiennością i/lub współczynnikiem odbicia.

Osłona może mieć postać różnego rodzaju obudów. Najwygodniejszym i radykalnym rozwiązaniem w warunkach stacjonarnych węzła sieci komputerowej jest w szczególności pomieszczenie ekranowane elektromagnetycznie.

Zespół autorski zajął się zagadnieniem zapewnienia bezpieczeństwa węzłów sieci komputerowych poprzez ekranowanie.

Tradycyjne rozwiązanie ekranowania elektromagnetycznego polega na zamykaniu sprzętu i osprzętu węzła wraz z obsługą w tzw. „klatce Faradaya", to jest elektromagnetycznie hermetycznej przestrzeni w postaci kabiny obudowanej ze wszystkich stron blachą stalową.

Podstawowymi wadami tego typu technologii jest:

- uciążliwość realizacji projektu z uwagi na ciężar elementów konstrukcyjnych oraz potrzebę bardzo precyzyjnego połączenia poprzez spawanie i/lub skręcanie, stosowanie specjalnych uszczelek elektromagnetycznych, potrzebę stałego diagnozowania szczelności elektromagnetycznej na skutek niebezpieczeństwa przemieszczania się elementów;

Frame Relay: Ochrona sieci

- pełna separacja funkcji zarządzania od przełączania wewnątrz switch'a
- oddzielne kanały PVC dla zarządzania
- używane protokoły to stos TCP/IP + SNMP
- sieci zarządzania są wydzielone na poziomie trzecim modelu ISO (niedostępne ze "świata")

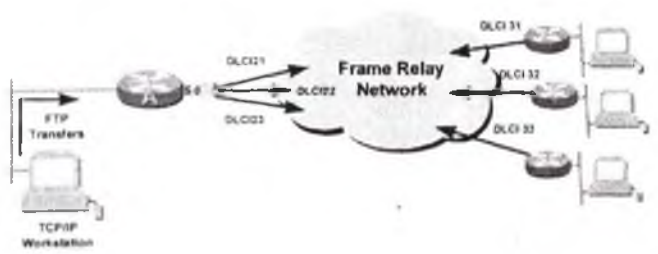
Bezpieczeństwo w technologii Frame Relay

Maciej Szeptycki (NASK)
marias@nask.pl

Frame Relay: Przegląd

- Sieci wirtualne
- Kanały logiczne PVC (*Permanent Virtual Circuit*) określane przez parę DLCI
- Możliwość tworzenia różnych topologii
- Separacja transportu dla protokołów wyższych warstw (TCP/IP, IPX, Apple Talk, DECnet, ...)
- Przezroczystość sieci Frame Relay
- Bezpieczeństwo - pełne oddzielenie ruchu użytkowników na poziomie warstwy 2 modelu ISO OSI

Frame Relay: Przegląd



Frame Relay: Przegląd

- typowo 56/64 Kbps do T1/E1
- zaimplementowane tylko PVCs (SVCs planowane)
- Format ramki:

Flag	Address	Info Field	FCS	Flag
1	2–4	n	2	1

DLCI (High Order)						C/R	EA0	Byte 0
DLCI (Low Order)			FECN	BECN		DE	EA1	Byte 1
8	7	6	5	4	3	2	1	Bits

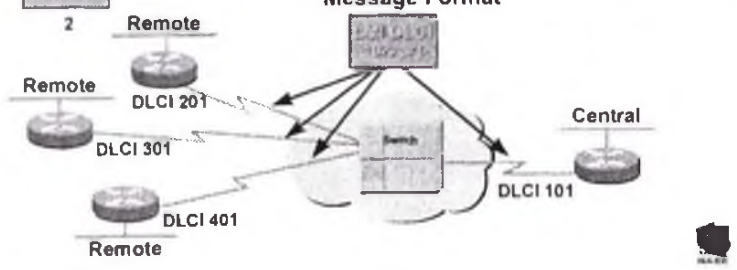
- DLCI: Data Link Connection Identifier
- C/R: Command/Response Field
- FECN: Forward Explicit Congestion Notify
- BECN: Backward Explicit Congestion Notify
- DE: Discard Eligible
- EA: Address Field Extension

Frame Relay: Przegląd

- Link Management Interface (LMI)
  - Raportuje dodanie/skasowanie PVC
  - Raportuje status PVC

1	1	1	1	1	Variable	2	1
Flag	LMI DLCI	U I Field	Call Ref	Message Type	Info Elements	Frame Check Sequence	Flag
	2						

Message Format



Frame Relay: Przegląd

- Inverse ARP (RARP)
  - Nie jest wymagane statyczne mapowanie
  - Używa LMI do wykrycia aktywnych DLCI

Router A: Hello, Who are you? (I am 131.108.25.5) — DLCI 14 → Router B: I can now map DLCI 18 with network 131.108.25.5

Router A: I can now map DLCI 14 with network 131.108.25.1 ← DLCI 18 — Router B: Hello, I'm 131.108.25.1

Ochrona zarządzania i protokołów kontrolnych

- Bezpieczeństwo zestawiania połączenia
  - użycie styku z odpowiednią gamą uprawnień
  - odseparowanie routingu i kanałów nim zarządzających od użytkownika
  - ochrona serwerów mających znaczenie dla protokołu
  - ochrona SNMP - używana v.1 (!)

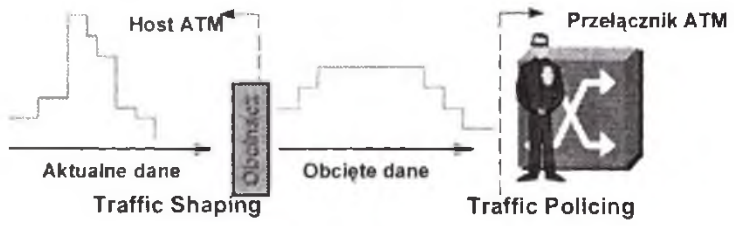
Ochrona zarządzania i protokołów kontrolnych

- Bezpieczeństwo użytkowania połączenia
  - konieczność zarządzania ruchem
  - ochrona przed zerwaniem połączenia (sposoby jak przy zestawianiu)
  - monitoring sieci - wychwytywanie informacji o "dziwnym działaniu" połączenia

ATM - podsumowanie

- pierwszy oficjalny dokument ATM Forum dotyczący bezpieczeństwa - lipiec '97
- koszt urządzenia do podsłuchu światłowodu - ok. 2000$
- wzrastająca ilość zastosowań ATM do budowy sieci rozległych

Traffic Shaping i Traffic Policing
Generic Cell Rate Algorithm (GCRA)



- "Leaky Bucket Algorithm"
- Ogranicza szczytową prędkość transmisji ramek
- Ogranicza czas dociążenia
- Ogranicza Jitter transmitowanych ramek

Czy otrzymywany ruch spełnia kontrakt?

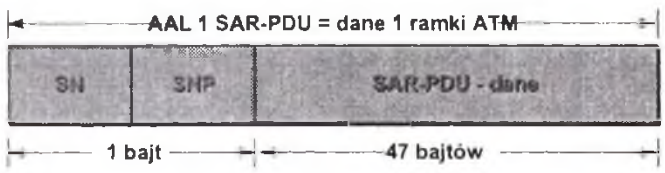
- Jeżeli nie:
  mogę odrzucić ramki z CLP = 1
  mogę ustawić w ramkach CLP = 0+1

Kategorie usług warstwy ATM

	CBR	VBR		ABR	UBR
		Real-Time (RT)	Non RT (NRT)		
Gwarancja	pasma i opóźnienia	minimalnego pasma i opóźnienia		małe/brak strat ramek ATM	"wyślij i się módl"
Adaptacja do zwrotnej kontroli przeciążeń	Nie	odmiana		Tak	Nie, sieć może odrzucić ruch UBR
Cell Delay Variation (Jitter)	Określony	Określony	Nie określony	Określony*	Nie określony
Max Cell Transit Delay (opóźnienie)	Nie	Określone	tylko średn CTD	Tak*	Nie określone
poziom utraty / błędów ramek	Określony	Określony		Określony*	Nie określony

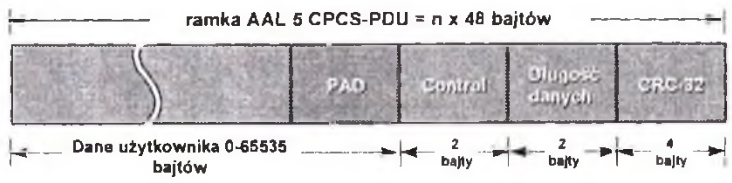
* powinno być już określone na poziomie produkowanego sprzętu

AAL 1



SN = Sequence Number
SNP = Sequence Number Protection

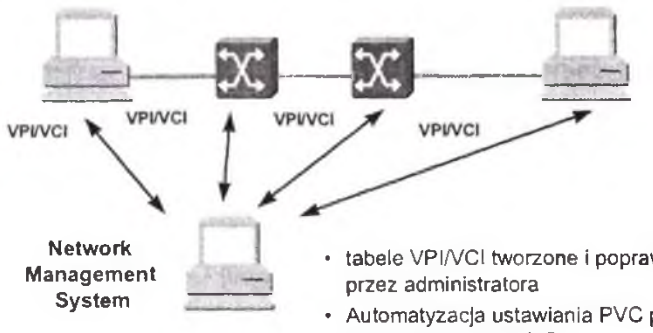
AAL 5



pole PTI w nagłówku ramki ATM sygnalizuje:

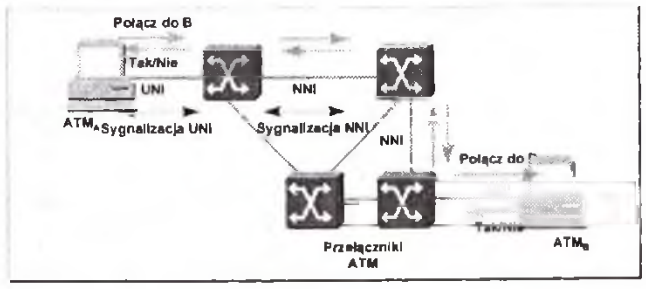
- brak danych
- dane AAL 5 z wnętrza ramki AAL 5 PDU
- dane AAL 5 kończące ramkę AAL 5 PDU (koniec ramki)

Permanent Virtual Connections (PVC)



- tabele VPI/VCI tworzone i poprawiane przez administratora
- Automatyzacja ustawiania PVC przez oprogramowanie NMS

Switched Virtual Connections (SVC)



- Połączenia dynamicznie ustanawiane poprzez sygnalizację
- Adresacja ATM w sygnalizacji nawiązującej połączenie określa urządzenie wołane i wywołujące
- Kanał sygnaliacji UNI (VPI/VCI = 0/5)

BEZPIECZEŃSTWO W TECHNOLOGII ATM

Andrzej Maciej Skrzeczkowski

NASK

Streszczenie

Wzrastająca liczba zastosowań technologii ATM do budowy sieci rozległych karze zastanowić się nad bezpieczeństwem takiej sieci. Sama budowa protokołów związanych z ATM oraz szybkość działania łącz jest powodem ogromnego zawikłania tego problemu.

Technologia ATM

ATM jest technologią, która ma za zadanie integrować wszystkie rodzaje przesyłanych danych - od dźwięku i video do danych Internetowych. Realizuje to zadanie przez określenie jako jednostki przesyłowej małej, 53 bajtowej komórki. Większe porcje informacji dzielone są na takie właśnie części. W nagłówku znajdują się identyfikatory, pozwalające na ustalenie przez urządzenie ATM - przełącznik - drogi, którą dana komórka ma być transmitowana.

W ATM transmisja odbywa się przez zestawianie wirtualnych połączeń (VC) - rozesłanie zestawów danych które instruują przełączniki jak mają się zachować wobec przybycia do portu komórki ATM o określonym identyfikatorze. W skład informacji konfiguracyjnej wchodzą dane o porcie docelowym w przełączniku, docelowych identyfikatorach (które przełącznik może zmieniać) i parametrach połączenia, które przełącznik musi zagwarantować. Następnym etapem jest wysyłanie komórek o odpowiednich identyfikatorach do portu wejściowego i ich odbiór na wyjściu. Automatyczne zestawianie VC to SVC, a ręczne to PVC.

Do celów zestawiania połączeń i późniejszego ich utrzymania zdefiniowano różne protokoły, posługujące się własnymi VC.

Bezpieczeństwo sieci ATM.

Problem bezpieczeństwa w sieciach ATM można podzielić na ochronę łącz (fizycznych i wirtualnych) oraz ochronę protokołów kontrolnych.

W przypadku łącz ochrona może odbywać się przez szyfrowanie (co ze względu na duże przepustowości łącz jest trudne i drogie) bądź przez szyfrowanie „end-to-end" (gdy łatwy jest dostęp do urządzeń końcowych). Dla ATM pojawia się przy tym rodzaju ochrony problem z synchronizacją - ustaleniem początków ramek lub bloków informacji. Rozwiązaniem jest tutaj zastosowanie kodów samosynchronizujących, mechanizmów oznaczania końca ramki AAL5 w nagłówku komórki lub ruchu utrzymaniowego OAM.

Dużo bardziej złożonym problemem jest ochrona protokołów kontrolnych. Pierwszą przeszkodą jest ich nie zawsze precyzyjne zdefiniowanie (zależne od producenta). Następną - ich duża różnorodność. Podstawowym rozwiązaniem jakie się tu stosuje jest udostępnienie użytkownikowi tylko niezbędnych dla niego protokołów i ścisły monitoring sieci. Odbiorca końcowy ma więc zazwyczaj zablokowane kanały służące do przesyłania informacji o konfiguracji sieci operatora, a zestawiane są tylko kanały PVC, PVP i odpowiednio SPVC i SPVP.

Podsumowując ATM jako technologia dynamicznie zdobywająca rynek wymaga dużej uwagi ze względu na problemy bezpieczeństwa. Znalazło to wyraz w opracowaniu w lipcu '97 roku przez ATM Forum zaleceń dotyczących bezpieczeństwa sieci ATM. Musi to też być brane pod uwagę przy projektowaniu takich sieci.

NOWE TRENDY W WARSTWIE DOSTĘPOWEJ – INTEGRACJA GŁOSU I DANYCH

Marcin Fryzik

Ericsson Sp. z o.o.

Zjawisko integrowania transmisji głosu i danych pojawiło się w telekomunikacji wraz z szybko rosnącym zapotrzebowaniem na przesyłanie danych. Rozwijane były techniki umożliwiające wykorzystanie do tego celu łącz telefonicznych – największej infrastruktury sieciowej na świecie. Odpowiedzią ze strony dostawców usług telefonicznych na potrzebę połączenia transmisji głosu i danych była sieć ISDN. Gwałtowny rozwój technologii sprawia jednak, że telefoniczni operatorzy publiczni mogą stawać w obliczu coraz silniejszej konkurencji ze strony przemysłu sieciowego – operatorów Internetu, dostawców usług, producentów sprzętu i oprogramowania. Coraz częściej pojawia się pytanie czy Internet zastąpi telefon. Dzisiejsza technologia na to pozwala. Gwałtowny wzrost transmisji głosu może jednak spowodować zbyt duże obciążenie sieci. Istnieje więc konieczność wdrożenia mechanizmów pozwalających na rezerwację pasma, zapewnienie określonego poziomu usług, a co za tym idzie umożliwienie pobierania za nie zróżnicowanych opłat.

Obecnie integracja głosu stosowana jest przede wszystkim w sieciach opartych o ATM, czy adaptowaną do tego celu technologię Frame Relay. Dla sieci IP natomiast opracowano protokół RSVP (*Resource Reservation Protocol*) pozwalający na rezerwację zasobów, co przy jednoczesnym rozwoju mechanizmów kolejkowania ruchu, kontroli przeciążeń sieci, czy zastosowaniu kodeków i procesorów sygnałowych pozwala na implementację telefonii oraz transmisji multimedialnych.

Aby stworzyć system dla zastosowań profesjonalnych należy brać pod uwagę takie aspekty jak bezpieczeństwo, kontrola dostępu, niezawodność czy możliwość rozbudowy. Powszechna akceptacja standardu H.323 dała możliwość powstania współpracujących ze sobą produktów telefonii IP pochodzących od różnych producentów. Naturalną konsekwencją techniki przesyłania głosu przez IP stała się konieczność stworzenia połączenia z tradycyjną siecią telefoniczną PSTN lub ISDN – *IP telephony gateway*. Biorąc pod uwagę obecne ceny usług telefonicznych może to spowodować popularyzację rozmów telefonicznych przez IP zwłaszcza na duże odległości, natomiast stworzenie oprogramowania realizującego usługi central abonenckich PBX i pozwalającego na powstanie w pełni zintegrowanej sieci telefonicznej i komputerowej przedsiębiorstwa może być tylko kwestią czasu.

Multimedia Telephone System firmy Ericsson jest kompletnym rozwiązaniem pozwalającym na transmisje multimedialne oparte o IP. Składa się z aplikacji video klienta oraz *gateway'a* do sieci PSTN lub ISDN, *Multipoint Conference Unit* pozwalającego na konferencje z udziałem więcej niż dwóch użytkowników oraz *Gatekeeper'a* – serwera pośredniczącego w połączeniach, a umożliwiającego między innymi kontrolę dostępu i adresowanie.

Użytkownik komputera PC wyposażony w modem i dołączony do Internetu przez łącze telefoniczne dotychczas mógł transmitować dane bez możliwości jednoczesnego wykonania rozmowy telefonicznej. Phone Doubler firmy Ericsson pozwala na prowadzenie rozmowy telefonicznej bez zerwania połączenia z Internetem wykorzystując transmisję głosu przez IP. Jest to więc rozwiązanie korzystne zarówno dla użytkownika, jak i dla operatora pozwalając mu na wzbogacenie oferty o dodatkową usługę.

przeprowadzenie testów. 28.04.1998 rozpoczęły się pierwsze testy przeprowadzane zgodnie z wcześniej ustalonymi procedurami.

3. Opracowanie strategii – Business Plan.

Business Plan został stworzony tylko na potrzeby wewnętrzne. Do uruchomienia usługi Netia nie musi wykorzystywać zewnętrznych źródeł finansowania.

Do tworzenia dokumentu zostały zaproszone osoby z różnych działów Netii (technicznego, finansowego i marketingu). Osoby biorące udział w pracach tworzyły „wirtualny" zespół zadaniowy, który rozwiązano po realizacji zadania.

W dokumencie zostały opisane i analizowane następujące bloki tematyczne:

- analiza konkurencji
- analiza wewnętrzna
  - zasoby ludzkie
  - billing
  - zasoby techniczne (w tym testy)
- plan marketingowy
- plan organizacyjny
- plan finansowy

Pod koniec lutego 1998 Business Plan został zaakceptowany, co było jednoznaczne z wyrażeniem zgody na wprowadzenie ISDN w sposób zaproponowany przez Lidera Projektu i zespół.

1. Podręcznik ISDN dla pracowników Netii.

Wprowadzenie nowego produktu wymaga przygotowania dokumentacji zawierającej:

- opis produktu
- zalety i korzyści wynikające ze stosowania ISDN
- opis procesu sprzedaży
  - docelowy segment
  - organizacja sprzedaży
  - procedury przyjmowania wniosków i podpisywania umów
  - procedury rejestracji klienta w systemie billingowym
- reklamacje
- zakres obowiązków osób odpowiedzialnych za ISDN w regionach – specjalistów ISDN
- cennik
- skróty i terminologię ISDN
- wzory dokumentów

Podręcznik zostanie dostarczony do wszystkich Biur Obsługi Klienta Netii.

1. Regulamin świadczenia usług ISDN, Cennik ISDN.

Regulamin i cennik, które nie zostały zatwierdzone przez Zarząd Netia Telekom S.A., zostały oparte na założeniach dokonanych w planach organizacyjnym i finansowym stworzonych na potrzeby Business Planu. Dokumenty zostaną wprowadzone w dniu rozpoczęcia świadczenia usługi ISDN w sieciach Netii.

vendor, education package, etc. The PL creates a project group inside the company with all-necessary knowledge and skills. These people are technical, marketing, sales, legal, billing, etc. These people are both from HQ and from local units. Together with this group, the PL will then create, develop and pack the service.

When the service is ready to be introduced on the market, the project is finished. This project for the service becomes a real product (service) in Netia's product portfolio. At the same time the PL is ready with his job. This new service is then handled over to a Product Manager (PM). Very often the PL becomes the PM. From now on this PM is responsible for everything concerning this service (product). This also contains follow up during the product's life cycle. All services in Netia have a PM. One PM can be responsible for more than one service.

Subscriber Counter Reading: This service allows the user to "read" directly the real value of their own counter in S12 switch.

Three-party Service: The 3PTY service enables a served user who is involved in at last two calls (one active and one on hold) to request these calls to be joined in a three-way conversation.

Service under development

Netia Product Portfolio as of today is not good enough to satisfy the needs from the market. To be able to meet this rapidly growing demand, Netia is now developing new services that will be introduced on the market during 1998. These services are described here below.

ISDN (Integrated Services Digital Network): ISDN is an extension of the public telephone network, designed to carry digitized voice calls, or data, from one subscriber to another. Its main advantages over the conventional telephone network is better voice quality, higher data speeds, lower error rate, faster call setup times and greater flexibility. ISDN call charges are similar to conventional telephone calls. In ISDN, a 64 kbit/s digital data stream, called a B channel replaces the conventional analog telephone signal. In an ISDN voice call this B channel carries the digitized speech, in internetworking applications we use it to carry data. To make, receive and generally control calls, an additional signaling channel, called D channel is used. ISDN is available on two main types of interface. First we have a basic rate interface (BRI) with two independent B channels and one D channel. Then we have Primary Rate Interface (PRI) with up to 30 independent B channels and one D channel.

Voice Mail: The Voice Mail system has following functionality:
Call answering: This function enables completing the call when the subscriber does not answer or the line is busy. In this case the Voice Mail system answer the call by playing a greeting message and inviting the caller to leave his/her message. Call answering makes sure your subscriber can get the message even if they cannot take the call.
Fax answering: This function enables to receive and store faxes when certain fax number is busy or does not respond.
Message delivery: This function enables to store all incoming messages into the Voice Mail system.
Message retrieval: This function permits the Voice Mail subscriber to retrieve any voice or fax message from the Voice Mail box. The subscriber can hear, delete or skip messages previously recorded in his/her Voice Mail box.
New message notification: This function permits the subscriber to notify if there is any new message in his/her Voice Mail box. This notification is realized by sending special modulated signal in the same time as the exchange's greeting signal when the subscriber picks up his/her handset. The new message notification can also be realized by calling subscribers having any new message. The Voice Mail system can then call all subscribers every 30 minutes saying: "There is a new message in your Voice Mail box. Please enter your password to check your messages." When the system is calling and the subscriber is busy or does not answer his/her phone, the system does not leave any new message, but it try's to call later (in 30 minutes).
Virtual fax feature: This function enables to store all incoming faxes in the fax box, because physically there is no fax machine and all fax calls are forwarding to the system. After that, the subscriber can retrieve his/her faxes using any fax machine available over the telephone network.
Virtual telephony solution: This function provides to subscriber the virtual Voice Mail box. The subscriber does not have his/her physical telephone line, but only the telephone number. Every time

PRODUCT PORTFOLIO AND SERVICE IMPLEMENTATION

Stefan Albertsson

Netia Telekom S.A., 02-822 Warszawa, ul. Poleczki 13
e-mail: Stefan_ Albertsson@netia.pl

Product Portfolio

Without license for Long distance, international and datacom traffic, Netia is today limited to provide service to our customers. Services available in Netia Network as of today are described here below.

Access connection: Access connection is always sold together with telephone line subscription. Netia provides two different subscriptions of telephone line. One with lower monthly fee (today 11 PLN per month plus VAT) and higher price per pulse (18 gr. per pulse plus VAT). The other with higher monthly fee (today 14 PLN per month plus VAT) and lower price per pulse (17 gr. per pulse plus VAT).

Calls local and Zone I (<25 km): Could be done through our own network between two Netia customers. Could also be done from a Netia customer first part through our network and then through other operator to a non-Netia customer.

Calls local and Zone II (25 km – 100 km): These calls will be done to or through other operator's network.

Calls Long Distance Zone III (>100 km): These calls will be done to or through other operator's network.

Calls to Mobile or Komertel: These calls will be done to or through other operator's network.

Calls International: These calls will be done to or through other operator's network.

Calls to 700 and 800 numbers: This is just the possibility for Netia customers to call to TPSA customers.

Leased local and zone areas line: We lease digital lines 2Mbit/s or 64kbit/s and analog lines. Customer can define interfaces for digital line: V.35, G.703, V.24, which we will give him in price leased, line from our tariff. This is connection from point to point and our customer receives "black boxes" with proper interfaces.

There are also some additional services that are described here below.

Abbreviated Address: The Abbreviated Address supplementary service allows the served user to set-up calls towards certain destinations by dialling short codes only (e.g. #1 as short number for 056 6435467). Served user himself can define short codes.

NETIA JAKO OPERATOR ŚWIADCZĄCY USŁUGI NA RZECZ UŻYTKOWNIKÓW NIEPUBLICZNYCH (z uwzględnieniem zarządzania systemami telekomunikacyjnym w stanach kryzysowych)

Ryszard Treider

Netia Telekom S.A., 02-822 Warszawa, ul. Poleczki 13
e-mail: Ryszard_Treider@netia.pl

Podstawy prawne działalności

- Zezwolenie lub koncesja na działalność operatorską;
- Ustawa o Łączności;
- Ustawa o Policji;
- Ustawa o ochronie tajemnicy państwowej i służbowej;
- Rozporządzenie Rady Ministrów w sprawie reklamowania osób od pełnienia obowiązków czynnej służby wojskowej w stanie ogłoszenia mobilizacji;

Informowanie użytkowników niepublicznych o przewidywanych:

- kierunkach działania;
- planowaniu i projektowaniu sieci;
- budowy i eksploatacji światłowodowych systemów transmisyjnych;
- budowy i eksploatacji kanalizacji kablowej;

Spełnienie wymogów prawnych wynikających ze świadczenia usług na rzecz obronności i bezpieczeństwa państwa

- utworzenie kancelarii tajnej
- zatrudnienie do prowadzenia i korzystania z jej zasobów osób uprawnionych spełniających wymogi wynikające z ustawy o ochronie tajemnicy państwowej i służbowej;

Netia jest przygotowana do zawarcia strategicznych umów z resortami obrony i spraw wewnętrznych oraz umów szczegółowych z poszczególnymi formacjami tych resortów w następujących obszarach:

- rodzaj i zakres świadczonych usług;
- wymagań organizacyjno technicznych;
- procedur współpracy;
- odpłatność za usługi;

Określenie procedur ochrony systemu i odpowiedzialności poszczególnych osób

- systemów alarmowania o zagrożeniach i skażeniach ekologicznych,
- systemów telemetrycznych.

Eksploatacja ww. aplikacji w tej sieci jest znacznie bardziej efektywna niż zastosowanie innych sieci np: radiowych sieci trankingowych, sieci komutowanych, sieci GSM.

Kolejne węzły tej sieci będą instalowane w pozostałych miejscowościach zależnie od zainteresowania poszczególnych abonentów.

Sieć radiowa

Do połowy br. w Warszawie zostanie uruchomiony nowy system transmisji radiowej z kanałami przezroczystymi o szybkościach 64-128 kbit/s., umożliwiający dostęp do wszystkich usług oferowanych przez BPT: sieć pakietowa X.25, Frame Relay, sieć multiplekserowa (kanały przezroczyste), Internet, poczta elektroniczna.

Wdrażany system pracuje w trybie punkt-wielopunkt, ze stacją bazową w węźle BPT i stacjami terminalowymi umiejscowionymi u klientów. Stacja terminalowa wyposażona jest w interface V.35 i dostarcza jeden kanał 128 kb/s lub 2 kanały 64 kb/s. W odróżnieniu od innych systemów, w sprzyjających warunkach nie musi być zapewniona bezpośrednia widoczność anten. Część zewnętrzna stacji terminalowej może być instalowana na ścianach budynków drewnianych, ceglanych i otynkowanych, oraz masztach metalowych i drewnianych.

Po przeprowadzeniu testów planowane jest sukcesywne uruchamianie dalszych stacji bazowych w Warszawie (rozszerzenie zasięgu) oraz w węzłach BPT w innych miastach.

Poczta elektroniczna wg standardu X.400/ X.500, oprogramowanie

BPT TELBANK SA jest administratorem systemu pocztowego w domenie ADMD TELBANK400®. Jest także bezpośrednim dystrybutorem oprogramowania firmy ISOCOR.

Od dwóch lat pracują dwa węzły pocztowe:

- Open Mail (Hewlett Packard),
- ISOPLEX (ISOCOR).

Uruchomione i eksploatowane są moduły typu gateway umożliwiające dołączenie następujących węzłów pocztowych abonentów:

- cc: Mail,
- Open Mail,
- Microsoft Mail.

Serwer X.500 pozwala na rozgłaszanie adresów, a także innych danych, użytkowników systemu X.400.

⇒ Frame Relay:
- port 64 kb/s – 512 kb/s,
- CIR 16 kb/s – 256 kb/s,
- EIR 8 kb/s – 256 kb/s.

Istnieje możliwość zwiększenia przepustowości dla FR (do 2 Mbit/s włącznie) w większości relacji w terminie do trzech miesięcy od daty złożenia zamówienia.

W 1998r. będzie kontynuowany, proces zwiększania przepustowości kanałów międzywęzłowych do 34 Mbit/s. Stopniowo będą wprowadzane usługi ATM.

Warszawska sieć światłowodowa SDH

Warszawska sieć światłowodowa SDH została uruchomiona w grudniu 1996 r. Składa się z czterech węzłów SDH (Synchronous Digital Hierarchy) połączonych światłowodowymi kanałami cyfrowymi o przepustowości 622 Mbit/s.

Sieć umożliwia zestawianie kanałów cyfrowych m.in. dla połączenia:

- sieci lokalnych,
- telefonicznych central cyfrowych,
- podstawowych i rezerwowych ośrodków obliczeniowych.

Łączna długość wybudowanych przez BPT TELBANK SA łączy światłowodowych w Warszawie przekracza 80 km.

BPT oferuje:
- zestawianie kanałów cyfrowych bitowo przezroczystych o szybkościach od 64 kb/s do 34/155 Mbit/s,
- budowanie przyłączy światłowodowych,
- opracowanie i realizację projektów technicznych sieci korporacyjnych banków na terenie Warszawy (wraz z dostawą i uruchomieniem niezbędnych urządzeń telekomunikacyjnych).

Biorąc pod uwagę opracowywane projekty rozbudowy tych sieci o nowe relacje światłowodowe, istnieje możliwość wybudowania dla klientów łączy światłowodowych w wielu relacjach po znacznie niższych kosztach w porównaniu z kosztami samodzielnej inwestycji.

Transmisja danych w sieci pakietowej TELBANK-P

Połączenia telekomunikacyjne krajowe i międzynarodowe są realizowane w sieci pakietowej TELBANK-P. Obecnie sieć charakteryzują następujące parametry:
- dostępne prędkości na portach: standardowo do 64 kb/s, opcjonalnie do 512 kb/s.
- przepustowość międzywęzłowa w 24 relacjach – 256 kb/s, w pozostałych 64 kb/s.

Dostępne protokoły transmisji: X.28, X.25, SDLC.

Istnieje możliwość zwiększenia zarówno ilości węzłów, jak i prędkości na portach – na

integracji telefonu z komputerem CTI – znana jako Call Center, a umożliwiająca efektywniejsze prowadzenie transakcji handlowych i usługowych.

Integracja telefonu z komputerem CTI jest technologią łączenia funkcji telefonu i terminala PC przez integrację głosu, obrazu i danych w celu tworzenia nowych zautomatyzowanych usług komercyjnych.

Podstawowymi usługami realizowanymi w sposób automatyczny przez Call Center:

- przyjęcie rozmowy i identyfikacja potrzeb użytkownika
- zestawienie połączenia do właściwego serwera informacyjnego realizującego usługę lub ewentualnie osoby (agenta)
- realizacja transmisji danych z serwerów informacyjnych
- umożliwienie połączenia i tworzenie danych do bilingu

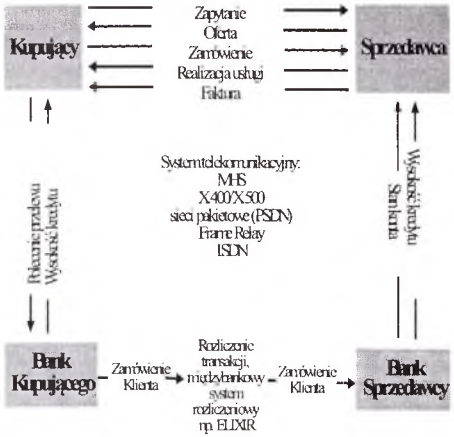
Europejskie projekty multimedialne

Na ostatniej wystawie IFA (Internationale Funkausstellung) – największej europejskiej imprezie w dziedzinie radiofonii, telewizji i elektroniki powszechnego użytku zostało przedstawionych szereg telekomunikacyjnych programów badawczo – wdrożeniowych wspieranych przez WE zaprezentowanych pod hasłem:

„multimedia w technice rozsiewczej i telekomunikacji"

Należy przypuszczać, że wiele z nich będzie miało wpływ na rozwój usług telekomunikacyjnych. Najciekawsze z nich to:

1. Cyfrowa radiofonia DAB (Digital Audio Broadcasting) – system umożliwiający przekazywanie głosu, obrazu, grafiki i tekstu przez radiowy system rozsiewczy.
   Umożliwia on m.in. przesyłanie multimedialnej informacji dotyczącej m.in.:
   - rozkładu jazdy pociągów i autobusów
   - ważniejszych informacji i gazet
   - repertuaru teatrów i kin
   - komunikatów zarządu miasta
   - informacji o ruchu drogowym
   - reklam.
1. Mobile Multimedia – MAVT
   Program MVAT (Mobile Audio Visual Terminal) stanowi część programu RACE II (Research and Techology Development in Advanced Communication Technologies in Europe). Konsorcjum MAVT utworzone w 1992r. Łączy 18 partnerów z przemysłu, operatorów sieci i europejskich ośrodków badawczych telekomunikacji. Celem projektu jest opracowanie i budowa terminala do odbioru ruchomego obrazów i dźwięków przekazywanych w rozsiewczym kanale wysokopasmowym.



Rys. 2 Schemat przekazywania dokumentów elektronicznych w typowym systemie EDI

Początkowo w systemach EDI wykorzystywano do transmisji dokumentów publiczne sieci telefoniczne. Obecnie zalecaną, przez organizacje standaryzacyjne państw UE, platformą przekazywania dokumentów jest system poczty elektronicznej o standardzie X.400/X.500 zbudowany w oparciu o pakietowe sieci transmisji danych (PSDN).

W Polsce standard EDIFACT stosowany jest w wewnątrz-bankowych i między-bankowych systemach przekazywania dokumentów finansowych i sprawozdawczych m.in. w aplikacjach:

- ELIXIR – Krajowej Izby Rozliczeniowej,
- BIS, SORBNET – Narodowego Banku Polskiego,

które zbudowane są w oparciu o platformę X.400 w systemie TELBANK400® Bankowego Przedsiębiorstwa Telekomunikacyjnego „TELBANK" SA.

Systemy EDI stosowane są również przez największych producentów samochodów i ich kooperantów produkujących w Polsce.

Na świecie systemy EDI używane są przez kilkaset tysięcy firm (w tym 50 000 firm z sektora prywatnego w USA). Stosowane są przede wszystkim w sektorach produkcji, dystrybucji, magazynowania, usług publicznych, farmacji, budownictwa, petrochemii, metalurgii, produkcji żywności, bankowości, ubezpieczeń, zarządzania, ochrony zdrowia i produkcji tekstylnej.

Zgodnie z najnowszymi badaniami liczba firm używających EDI zwiększy się czterokrotnie w ciągu najbliższych 6 lat.

Wykorzystanie sieci Internet

Sieć INTERNET w coraz większym stopniu jest wykorzystywana przez przedsiębiorstwa handlowe, usługowe oraz producentów w celach nie tylko marketingowych, ale także do realizacji transakcji handlowych. Wzrasta również zainteresowanie banków możliwościami jej wykorzystania do świadczenia usług bankowych przede wszystkim dla transakcji detalicznych.

W tym celu został opracowany standard SET (Secure Electronic Transaction), który definiuje zasady realizacji płatności poprzez sieć INTERNET.

ofertę poza środowisko akademickie. Koniec XX wieku jest dobrą okazją aby ze środowiska naukowego wypromować elementy Globalnego Społeczeństwa Informacyjnego.

„ Należy myśleć w najbliższej przyszłości o wprowadzeniu cenników za użytkowanie, za korzystanie z miejskich sieci komputerowych. Trzeba myśleć o wprowadzeniu zasady gospodarki rynkowej kiedy użytkownicy płaca za usługę a usługa powinna być postawiona na bardzo wysokim poziomie i jednocześnie jest to szansa dla nauki, dla państwa prowadzących miejskie sieci w poszczególnych regionach aby rozwijać zakres usług i świadczyć je na takim poziomie aby administracja i gospodarka były zainteresowane ich wykorzystywaniem..... Jest to niezmiernie ważne w procesie przystąpienia do negocjacji z Unia Europejska gdzie jednym z obszarów w których nie jesteśmy z tyłu, jesteśmy na równi z krajami Unii Europejskiej jest obszar – Globalne Społeczeństwo Informacyjne."[3]

Tego typu myślenie, a co ważniejsze działanie jest zgodne z duchem potrzeb cywilizacyjnych i zgodne z propozycjami nowego prawa telekomunikacyjnego [4].

Modele współpracy sieci MAN (operatorów)

a) współistnienie (wzajemne tolerowanie),
b) współpraca,
c) konkurencja,
d) ??????

Współpraca operatorów telekomunikacyjnych w sieciach komputerowych (powszechnie dostępnych) może być realizowana na wiele sposobów.
Najprostszy i chyba najmniej dojrzały a społecznie najbardziej kosztowny to model wzajemnego tolerowania. Polega to na „udawaniu", że operatorzy nie widzą się nawzajem. Efektem takiego działania jest potencjalna możliwość istnienia równolegle obok siebie niezależnych kosztownych infrastruktur informatycznych. Brak możliwości transferu informacji pomiędzy sieciami (ogólnie niezgodne z propozycjami nowego prawa telekomunikacyjnego). Tego typu sytuacja jest ewentualnie do przyjęcia w sieciach specjalnego znaczenia (sieci zamknięte).
Model współpracy, model najbardziej naturalny, oparty o klarowne umowy międzyoperatorskie. Wydaje się, że model współpracy operatorów z uregulowanymi kwestiami wzajemnych usług, transferu ruchu, uzgadnionej technologii itp. jest modelem najbardziej poprawnym, a w zakresie sieci finansowanych z budżetu państwa **jedynym dopuszczalnym**.

Sieć MAN Kraków realizuje jak się wydaje w obecnych kontaktach z innymi operatorami telekomunikacyjnymi (NASK, TP S.A, Telbank) model oparty na współpracy z ograniczoną konkurencją.

[3] Wypowiedź minister Małgorzaty Kozłowskiej w trakcie konferencji POLMAN 98

[4] Por. udostępniony projekt prawa telekomunikacyjnego http://www.ml.gov.pl/prasa.htm

Użytkownikami sieci MAN Kraków są przede wszystkim użytkownicy instytucjonalni ze środowiska akademickiego. Praktycznie każda uczelnia czy instytut naukowy w Krakowie jest bezpośrednim użytkownikiem/abonentem miejskiej sieci. MAN Kraków dla tego typu użytkowników świadczy podstawową usługę jaką jest transmisja danych zarówno w obszarze sieci miejskiej jak też zapewnienia połączenia sieci ze światem zewnętrznym. Oprócz użytkowników akademickich MAN Kraków obsługuje innych użytkowników instytucjonalnych (na zasadach komercyjnych) oraz kilka tysięcy użytkowników indywidualnych utrzymując na swoich serwerach indywidualne konta użytkowników. Naturalnym jest oczekiwanie przez wszystkich abonentów sieci (zarówno bezpośrednich jak też pośrednich[1]) aby szeroko pojęta usługa sieciowa świadczona przez MAN była usługą na wysokim poziomie. Oczekiwaniem użytkowników jest sprawne działanie sieci a zwłaszcza pewne i szybkie połączenia ze światem zewnętrznym w szczególności z sieciami zagranicznymi.

Styk sieci MAN Kraków z innymi sieciami

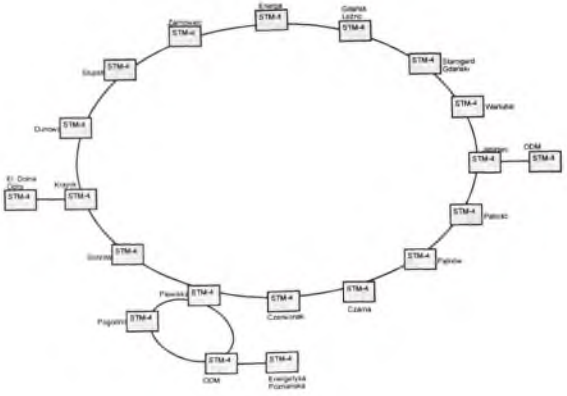
a) NASK
b) TP S.A
c) TELBANK
d) inni operatorzy

Struktura sieci MAN Kraków zbudowana w dwu uzupełniających się technologiach (FDDI oraz ATM) cechuje wysoka niezawodność. Istotą sprawnego funkcjonowania sieci MAN, oraz oczywiste oczekiwania użytkowników jest sprawne i niezawodne połączenie sieci miejskiej z innymi sieciami. Dotychczas wszystkie krajowe sieci MAN (akademickie) posiadały wyłącznie jedno wyjście zewnętrzne. Pojawienie się dodatkowej oferty oferowanej przez Telekomunikację Polską S.A. usługi podobnej jaką świadczy NASK umożliwiło podnoszenie stopnia niezawodności sieci miejskiej drogą uruchomienia niezależnych połączeń zewnętrznych.
Miejska Sieć Komputerowa w Krakowie od roku 1994 posiada łącze o przepustowości 2 Mb/s do sieci rozległej NASK. Łącze to, praktycznie od samego początku, jest bardzo przeciążone, co stawiało pod znakiem zapytania sensowność dalszego rozwoju usług w miejskiej sieci. Od listopada 1997 jest eksploatowane drugie, alternatywne łącze o przepustowości 2 Mb/s do sieci TP S.A. Na styku z obydwoma sieciami (NASK, TP S.A) uruchomiono routing oparty o protokół BGP, który w przypadku sprawności obydwu połączeń rozkłada obciążenie, a w przypadku awarii jednego z nich w płynny sposób kieruje cały ruch poprzez sprawne łącze. W lutym 1998 roku dodatkowo połączono przy użyciu protokołu BGP MAN w Krakowie z siecią Telbank (wyłącznie dla ruchu krajowego). Dzięki takiemu rozwiązaniu ruch pomiędzy sieciami nie obciąża połączeń z siecią NASK oraz TP S.A.

Zastosowanie protokołu BGP pomiędzy siecią MAN Kraków a sieciami NASK oraz TPNET daje wymierne efekty w postaci:

a) zwiększenia niezawodności i bezpieczeństwa sieci MAN. Awaria jednego z łącz powoduje automatyczne przestawienie routingu na łącze alternatywne w sposób praktycznie niewidoczny dla użytkownika końcowego,
b) zwiększenie efektywności przepustowości łącz w relacji Kraków – Świat,

[1] Użytkownikami pośrednimi są użytkownicy wykorzystujący sieć MAN ze swoich lokalnych sieci. Nie posiadają oni bezpośrednio kont w ACK CYFRONET, natomiast wykorzystują zasoby i usługi sieci miejskiej



Rys. 4. *Konfiguracja jednego z pierścieni – Ring Północno – Zachodni*

6. Planowana oferta usługowa

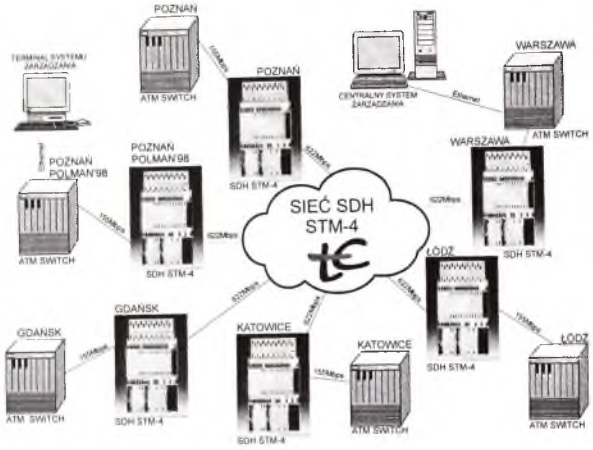
TEL–ENERGO przygotowuje się do stworzenia na bazie istniejącej sieci szkieletowej SDH/PDH warstwy transmisji danych z komutacją pakietów. Planowana platforma ATM/FR/IP umożliwiająca dynamiczny przydział pasma oraz dynamiczne przekierowywanie ruchu w przypadku przeciążenia lub uszkodzenia łącza będzie atrakcyjna zarówno dla klientów (opłata tylko za rzeczywisty ruch) jak i dostawcy usług (ekonomicznie wykorzystanie pasma).

W niedalekiej przyszłości możliwe będzie świadczenie w sieci TEL–ENERGO takich grup usług jak: dostęp do przezroczystych kanałów transmisji danych PDH i SDH (2, 34, 155 Mbit/s); bezpośrednie podłączenie ATM; protokoły zgodne z zaleceniami CCITT; protokoły IBM; dostęp do usług ISDN; łączenie sieci LAN (Ethernet, TCP/IP, IPX, DECNet, Appletalk); zdalny dostęp do sieci LAN; dostęp do Internetu; zarządzanie siecią.

Celem TEL–ENERGO jest zaspokajanie potrzeb klientów (zarówno aktualnych jak i nowych). Bardzo istotne stanie się więc prognozowanie zapotrzebowania na usługi i współpraca z klientem na wszystkich etapach opracowywania usługi. Ze względu na wymaganą konkurencyjność ważne stanie się skracanie czasu wprowadzenia usługi i zapewnienie wymaganych standardów. TEL–ENERGO jest obecnie na etapie tworzenia zasobów, procesów, infrastruktury, systemu zarządzania usługami.

Wśród usług, które mogą być uruchomione w pierwszej kolejności spodziewać się można Wirtualnych Sieci Prywatnych, połączeń sieci LAN, usług Frame Relay i ATM.

Ambicją TEL–ENERGO jest w najbliższej przyszłości wyróżnić się na rynku jako partner, któremu klient może z pełnym zaufaniem powierzyć kompleksowe rozwiązywanie problemów z zakresu teleinformatyki.



Rys. 1. Eksperymentalna sieć POL–155

5. Rozbudowa sieci bazowej TEL-ENERGO

Na słupach linii energetycznych zainstalowano w ciągu ubiegłych pięciu lat ponad 7 000 km kabli światłowodowych. Są one odporne na uszkodzenia, zakłócenia elektromagnetyczne i zmienność warunków atmosferycznych.

W 1998 r. zakończone zostaną prace prowadzące do zamknięcia pętli transmisyjnych. Docelowy stan sieci przedstawiony jest na poniższych rysunkach.

Dzięki strukturze pierścieniowej (pięć ringów STM–4) sieć TEL–ENERGO posiada wysoką niezawodność. Tranzytowy ring STM–16 minimalizuje ruch pomiędzy pierścieniami, przyczyniając się w ten sposób do maksymalizacji przepustowości sieci.

Wszystkie elementy sieci są monitorowane i zarządzanie z punktu centralnego.

powstała i była modernizowana ponieważ analogowa łączność jaka wcześniej była do dyspozycji sektora okazała się przestarzała i niewystarczająca dla jego potrzeb.

Wybór technologii światłowodowej wynikał z relatywnie niskich kosztów umieszczenia włókien w linie odgromowej sieci energetycznych w stosunku do całkowitego kosztu zakupu i wymiany linki odgromowej. Za światłowodami przemawiała też ich duża odporność na zakłócenia elektryczne i zmienność warunków atmosferycznych. Sektor Energetyczny wykorzystuje na swoje potrzeby tylko niewielki procent pojemności sieci. Niewykorzystana przez Energetykę pojemności mogą być wykorzystywane przez klientów zewnętrznych.

TEL–ENERGO S.A. utworzone w styczniu 1993 r. jest operatorem telekomunikacyjnym działającym na bazie światłowodowej Krajowej Sieci Telekomunikacyjnej Energetyki. Właścicielami Spółki są firmy zajmujące się wytwarzaniem, przesyłem i dystrybucją energii elektrycznej i cieplnej: Polskie Sieci Elektroenergetyczne S.A., 31 Spółek Dystrybucyjnych oraz Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej.

Misją TEL–ENERGO jest:

- świadczyć kompleksowe usługi teleinformatyczne dla klientów biznesowych i administracji;
- pełnić funkcję głównego dostawcy i integratora usług telekomunikacyjnych dla energetyki;
- świadczyć międzymiastowe i międzynarodowe usługi powszechne;
- dostarczać usługi transmisji innym operatorom;
- przyczyniać się do rozwoju operatorów telefonii lokalnej.
- Silnymi stronami firmy są:
- Ogólnokrajowy zasięg i parametry techniczne istniejącej infrastruktury telekomunikacyjnej:

  energetyczne linie przesyłowe (i poprowadzone wzdłuż nich międzymiastowe linie światłowodowe) łączą wielkie aglomeracje miejskie i obszary wysoko uprzemysłowione - w większości przypadków pokrywają się one z trasami komunikacyjnymi;

  teletransmisyjna sieć energetyki jest zbudowana wzdłuż linii energetycznych, z wykorzystaniem "prawa drogi"; atutem sektora jest jego infrastruktura (słupy energetycznych linii wysokiego i średniego napięcia) - w procesie inwestycyjnym zbędne jest postępowanie prawne, aby uzyskać zgodę właścicieli gruntów;

  obecnie stosowane urządzenia realizują łącza o przepustowości 155 Mbit/s i 622 Mbit/s, w najbliższej przyszłości przepustowość wzrośnie do co najmniej 2.5 Gbit/s;

  systemy światłowodowe są powiązane ze stale monitorowanymi liniami energetycznymi, co umożliwia natychmiastowe usługi serwisowe w przypadku usterek;

  docelowa pierścieniowa architektura sieci charakteryzować się będzie wysoką niezawodnością, możliwe stanie się świadczenie szerokiego zakresu zintegrowanych usług o najwyższej jakości

- Zaplecze kapitałowe;
- Posiadane koncesja i zezwolenie pozwalające obsłużyć kluczowych klientów, w tym w szczególności:

  zakładać i używać urządzenia, linie i sieci telekomunikacyjne, umożliwiające stworzenie ogólnokrajowego systemu nadzoru sterowania dyspozytorskiego Krajowym Systemem Elektroenergetycznym;

TEL–ENERGO S.A.
OPERATOR SIECI I DOSTAWCA USŁUG

Hanna Kontkiewicz–Chachulska

1. Wstęp

Celem prezentacji jest przedstawienie TEL–ENERGO w kontekście obserwowanej ewolucji sektora telekomunikacyjnego.

Pojawienie się na polskim rynku nowego operatora, jakim jest TEL–ENERGO i jego dzisiejsza pozycja są wynikiem zmian, jakie zaszły w sektorze telekomunikacji w latach 90-tych. Realizowane przez firmę plany rozwojowe są dostosowane do potrzeb miejscowych klientów, biorą jednak pod uwagę także trendy rynkowe obserwowane poza granicami kraju.

2. Otoczenie zewnętrzne telekomunikacji w Europie, ewolucja rynku i operatorów

Postęp w dziedzinie nowych technik telekomunikacyjnych i informacyjnych doprowadził na przestrzeni ostatnich 50 lat do znacznego obniżenia kosztu gromadzenia i przetwarzania informacji. Obecnie jesteśmy świadkami podobnego spadku kosztu transmisji danych, co łącznie ze zjawiskiem konwergencji sektorów telekomunikacji, przemysłu komputerowego i elektroniki wywiera silny wpływ na organizacje warsztatów pracy, przedsiębiorstw a nawet społeczeństw. Przedsiębiorstwa przekształcają się ze złożonych, hierarchicznych struktur w zdecentralizowane organizacje, funkcjonujące na zasadzie sieci.

W krajach Unii Europejskiej już w latach 80-tych zaczęły ulegać rozmyciu granice narodowych monopoli telekomunikacyjnych, co było skutkiem wysiłków zmierzających do stworzenia wspólnego rynku, w ramach którego telekomunikacja traktowana byłaby na równi z innymi sektorami. Przed dotychczasowymi państwowymi przedsiębiorstwami Poczty, Telefonu i Telegrafu (PTT) stanęły nowe wyzwania takie jak walka konkurencyjna, tworzenie międzynarodowych konsorcjów, opracowywanie nowych generacji technologii i usług. Na rynkach pojawiają się konkurenci operatorów historycznych, koncentrujący się na wybranych segmentach rynku, zatrudniający relatywnie mniejszy personel i proponujący usługi niejednokrotnie o wyższej jakości. Firmy te wyróżniają się często dużą efektywnością (porównanie Energis i British Telecom), korzystają z różnych kanałów dystrybucji usług, zlecają część prac do wykonania na zewnątrz. Operatorzy rozszerzają działanie na nowe, szybko rozwijające się dziedziny, które być może w przyszłości będą odgrywały większą rolę niż tradycyjne usługi telefoniczne.

Cechami charakterystycznymi dzisiejszego rynku telekomunikacyjnego są: szybka ewolucja potrzeb użytkowników i proponowanych usług, zmiana w relacjach klient/dostawca, zwiększająca się liczba konkurentów i co za tym idzie obniżające się taryfy.

Po stronie operatorów i dostawców usług obserwuje się bardzo częste operacje fuzji firm, przejęć, tworzenie aliansów, łączenie firm z branży telekomunikacji, mediów, elektroniki, komputerów, jak również powstawanie nowych firm.

Operatorzy doskonalą swój sposób działania w kilku wymiarach.

Pierwszym z nich jest sposób odpowiedzi na zmieniające się wymagania otoczenia, wyrażający się nową ofertą i strategią międzynarodową. Kluczową rolę odgrywają tu klienci - duże przedsiębiorstwa, pod wpływem których operatorzy wzbogacają swoją ofertę, a także stopniowo

W przedstawionym modelu usługowym dla abonentów centrali lokalnej świadczone są usługi POTS/ISDN, sieci inteligentnej, cyfrowych linii dzierżawionych 64kbit/s oraz usługi transmisji danych i dostępu do internetu.
Szczególna uwaga zostanie poświęcona problemowi obsługi ruchu do Internetu.
Wydzielenie strumienia połączeń do sieci transmisji danych powinno odbywać się w dolnej warstwie sieci, ze względu na inną charakterystykę ruchu połączeń do sieci transmisji danych: średni czas połączenia jest znacznie dłuższy niż rozmowa telefoniczna. Wydzielenie ruchu do sieci transmisji danych może odbywać się poprzez
W ostatnich latach Internet stał się globalną siecią transmisji danych przyciągającą użytkowników różnorodnością zawartych informacji dostępnych on-line. PSTN/Internet „gateways" (Point of Presence – PoP) w chwili obecnej są przyłączane do wybranych central poprzez interfejs ISDN PRI, analogowy lub ISDN BA. Operator sieci telekomunikacyjnej jednak w tym przypadku ma problem związany z inna charakterystyka ruchu niż zakładany dla telefonii:

- Dłuższe czasy połączeń komutowanych do sieci Internet;
- Wiele połączeń posiada jednakowe przeznaczenie, co wprowadza nierównowagę ruchu w sieci;

Rozpatrywane są dwa rozwiązania:

- Implementacja w centrali routera, który przeprowadzi pakietyzację połączenia komutowanego do interfejsu z protokołem IP. Technicznie oznacza to, że centrala będzie posiadała zintegrowany PoP składający się z następujących komponentów:
  - handlerów protokołów UDP, TCP-IP oraz protokołów warstwy niżej np. ATM lub Frame Relay.
  - router IP and serwer domeny.
- Prostsze oddzielenie strumienia danych od głosu albo poprzez integrację modemów w centrali lub poprzez użycie xDSL i tzw. wskaźnika usługi (jeszcze nie jest ustandaryzowany).

Oba podejścia są badane przez dostawców sprzętu komutacyjnego.
Inne ciekawym podejściem są urządzenia dostępowe, które umożliwiają przesłanie ruchu IP bezpośrednio po SDH: niestety proces standaryzacyjny dopiero został rozpoczęty, a ponadto, opracowanie nowych kart jest do SDH, które będą posiadały odpowiednie interfejsy jest konieczne, co zapewne wydłuży cały proces.

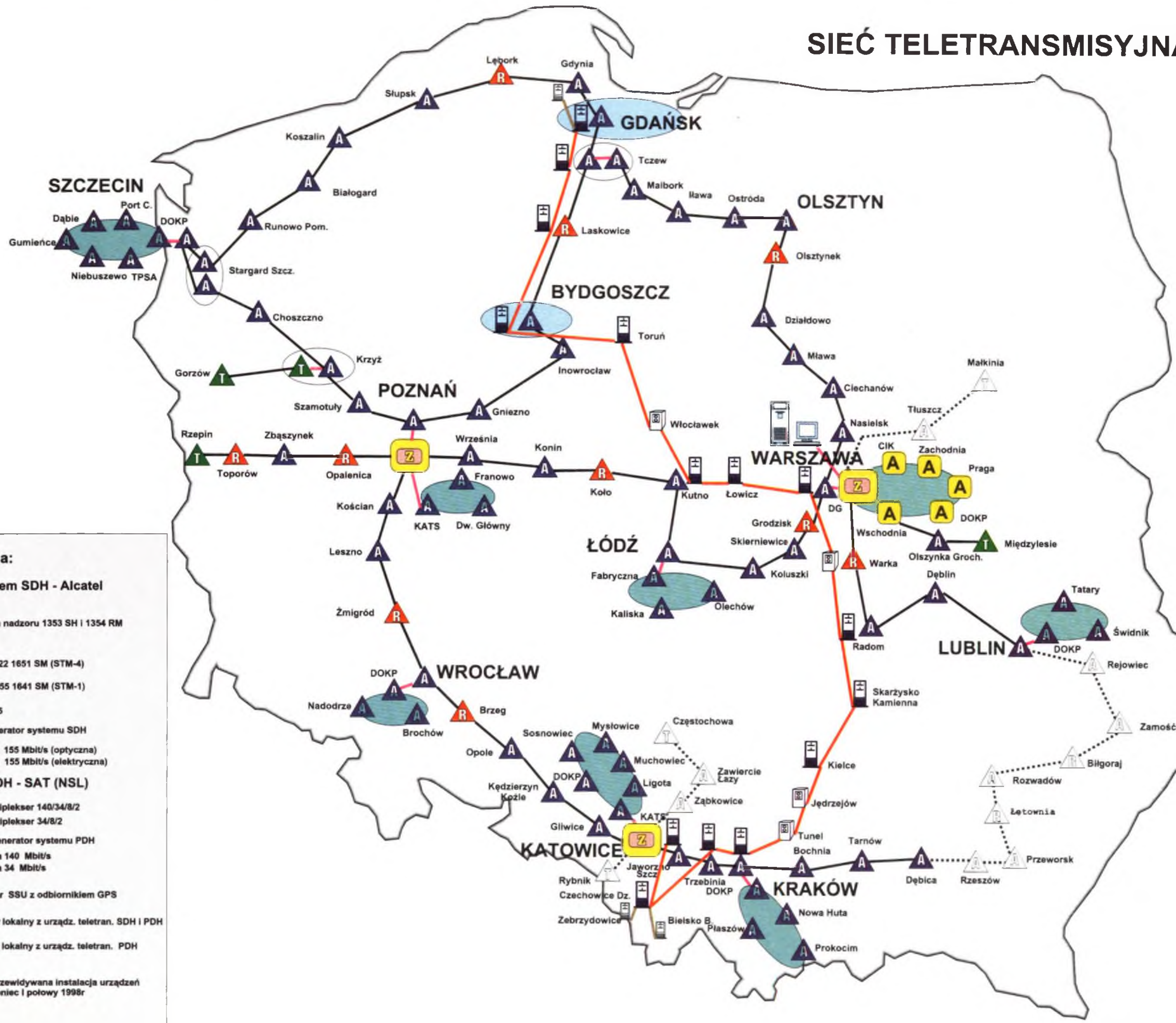
1. Zasady budowy sieci komutacyjnych/teletransmisyjnych.

Trzy podstawowe czynniki posiadają zasadniczy wpływ na strukturę budowanej sieci telekomunikacyjnej przez spółki operatorskie Netii:

- Brak istniejącej infrastruktury tj. central ręcznych lub elektromechanicznych;
- Minimalizacja długości odcinka miedzianego do abonenta;
- Zastosowanie wyłącznie technologii SDH jako środka teletransmisyjnego.

Minimalizacja długości odcinka miedzianego w konsekwencji oznacza bliskie podejście światłowodem do abonenta, co ma zapewnić w przyszłości usług szerokopasmowych, ma też jednak bezpośredni wpływ na strukturę sieci komutacyjnej: budowana sieć komutacyjna składa się z relatywnie dużej liczby jednostek wyniesionych i małej liczby linii bezpośrednio podłączonych do hosta. Największa liczba linii bezpośrednio obsługiwanych przez hosta w sieci Netii nie przekracza 4,000 linii. Rozważane jest także użycie technologii dostępowych FITL, jednak praktycznym ograniczeniem jest brak, na dzień dzisiejszy, interfejsu skoncentrowanego V5.2 u dostawców sprzętu komutacyjnego.
Jednostki wyniesione są podłączone do hosta przy pomocy teletransmisji SDH STM-1, więc naturalne jest też tworzenie struktur pierścieniowych w sieci dostępowej, w celu zapewnienia odporności sieci na przecięcia kabla i przez to zapewnienia stałej dostępności usług dla abonentów Netii. W sieci szkieletowej, łączącej węzły komutacyjne stosowane są urządzenia SDH typu STM-4 lub STM-16.

SIEĆ TELETRANSMISYJNA PKP



Oznaczenia:

System SDH - Alcatel

- System nadzoru 1353 SH i 1354 RM
- ADM 622 1651 SM (STM-4)
- ADM 155 1641 SM (STM-1)
- TM 155
- Regenerator systemu SDH
- Linia 155 Mbit/s (optyczna)
- Linia 155 Mbit/s (elektryczna)

System PDH - SAT (NSL)

- Multiplekser 140/34/8/2
- Multiplekser 34/8/2
- Regenerator systemu PDH
- Linia 140 Mbit/s
- Linia 34 Mbit/s
- Zegar SSU z odbiornikiem GPS
- Węzeł lokalny z urządz. teletran. SDH i PDH
- Węzeł lokalny z urządz. teletran. PDH
- Przewidywana instalacja urządzeń koniec I połowy 1998r

Rys. 1

Ze względu na kumulowanie się fluktuacji fazy, łańcuch odniesienia sieci synchronizacyjnej PKP nie będzie zawierał więcej niż 10 zegarów SSU (zalecane 5) oraz między nimi, nie więcej niż 20 (zalecane 10) zegarów SEC.
Całkowita liczba zegarów SEC w łańcuchu nie będzie przekraczać 60-ciu. Powyższe ustalenia wynikają z zaleceń ITU-T i standardów ETSI oraz z faktu, że im liczba zegarów w łańcuchu synchronizacyjnym jest większa, tym jakość sygnału taktowania docierającego do ostatniego elementu w łańcuchu jest niższa.
Jeżeli struktura cyfrowej sieci teletransmisyjnej PKP umożliwi, to sygnały synchronizacyjne do każdego węzła sieci będą doprowadzone co najmniej dwiema rozłącznymi drogami tzn. drogą podstawową i rezerwową.
Drogi doprowadzające sygnały synchronizacyjne powinny być możliwie krótkie, o dużej pewności działania (niezawodne).
W sytuacjach, kiedy nie można będzie zapewnić dróg rezerwowych dla sygnałów synchronizacyjnych doprowadzanych do węzłów, aby nie utworzyć pętli, zegary tych węzłów będą pracować w trybie pracy z podtrzymaniem.

Zakłada się, że sieć synchronizacyjna PKP będzie współpracować z sieciami innych operatorów w tym z siecią TP S.A. na zasadach pracy pseudosynchronicznej. Na poziomie współpracy międzynarodowej, z sieciami innych zarządów kolejowych dopuszczamy pracę w trybie plezjochronicznym.

6. Perspektywa rozwoju sieci telekomunikacyjnej PKP

Sieć telekomunikacyjna PKP powinna świadczyć zarówno dotychczasowe jak i nowe usługi telekomunikacyjne, które będą przyczyniać się do podnoszenia konkurencyjności PKP jako przedsiębiorstwa transportowego i docelowo, poprzez świadczenie usług telekomunikacyjnych i teleinformatycznych innym klientom, stać się siecią samofinansującą zarówno w zakresie utrzymania jak i dalszego rozwoju. Samofinansowanie jest warunkiem koniecznym do tego by sieć telekomunikacyjna była sukcesywnie modernizowana i świadczyła usługi telekomunikacyjne, zarówno dla PKP jak i innych instytucji na najwyższym poziomie.
Warunkami koniecznymi do realizacji tych celów jest:
– cyfryzacja sieci telekomunikacyjnej,
– zmiany organizacyjno-prawne w otoczeniu i w samej telekomunikacji na PKP,
– zewnętrzne uwarunkowania prawne zezwalające na podjęcie działalności zarobkowej.
Warunki te są wypełniane w różnym stopniu i tak:

1. W zakresie cyfryzacji sieci telekomunikacyjnej należy stwierdzić, że proces ten jest rozpoczęty poprzez układanie kabli światłowodowych, wprowadzanie cyfrowych urządzeń teletransmisyjnych i wprowadzanie cyfrowych central telefonicznych. Proces ten nabiera odpowiedniej dynamiki i ma być kontynuowany w najbliższych latach.
   Obecnie głównymi zadaniami przed którymi stoją PKP są:
   - rozbudowa sieci teletransmisyjnej (warstwa szkieletowa),
   - budowa central tranzytowych sieci ISDN-PKP.
2. W zakresie zmian organizacyjno-prawnych na PKP, dokonywane są obecnie zmiany restrukturyzacyjne PKP a szczególnie zmiany restrukturyzacyjne infrastruktury PKP.
   Zmiany te powinny wykreować powstanie samodzielnego pionu telekomunikacji PKP. Pozwoliłoby to na uruchomienie procesu takich zmian organizacyjno – prawnych, które stałyby się początkiem prywatyzacji tej części struktury PKP. Szczególnie ważnym czynnikiem, o którym należy pamiętać w tym procesie jest stworzenie atmosfery akceptacji (pracownicy, związki zawodowe) dla wszystkich zmian restrukturyzacyjnych.

ZZZ – oznacza trzy cyfry (w zapisie dziesiętnym od 000 do 127) identyfikujące punkt sygnalizacyjny w ramach SAC, które są w dyspozycji PKP.

4.5. Aktualna sytuacja w PKP w dziedzinie komutacji

W ogólnoeksploatacyjnej sieci telekomunikacyjnej PKP (około 120 tyś. abonentów, 1181 central) prawie w 90% są zainstalowane i pracują elektromechaniczne centrale biegowego systemu Eb5 Siemens lub centrale krzyżowe typu CK-20/30/60. Jest to sprzęt stary, mający za sobą kilkadziesiąt lat pracy. PKP ogłosiły przetarg na dostawę nowoczesnych, cyfrowych central ISDN'owych.

W efekcie sytuacja na dzisiaj wygląda następująco:

1. w węźle katowickim eksploatowanych jest 9 central systemu Meridian1 firmy Kapsch
2. w pozostałych 10 węzłach (Warszawa, Lublin, Kraków, Gdańsk, Poznań, Łódź, Bydgoszcz, Olsztyn, Wrocław, Szczecin) centrale systemu Meridian1 są już zainstalowane i obecnie trwają prace uruchomieniowe.

Należy jednak zaznaczyć, ze centrale Meridian 1 są centralami typu abonenckiego.

5. Synchronizacja sieci telekomunikacyjnej PKP

Powszechna cyfryzacja systemów komutacyjnych i teletransmisyjnych, zwłaszcza zaś wprowadzanie do sieci telekomunikacyjnej PKP synchronicznej hierarchii cyfrowych systemów transmisyjnych (SDH) oraz potrzeba świadczenia nowych usług telekomunikacyjnych, opartych o technikę cyfrową, wymagają stosowania kompleksowej i sprawnej synchronizacji całej cyfrowej sieci telekomunikacyjnej PKP.

Brak synchronizacji sieci będzie powodować nie tylko pogorszenie jakości świadczonych usług ale także, w skrajnych przypadkach, uniemożliwi poprawne funkcjonowanie sieci. Główną przyczyną degradacji jakości oferowanych usług są zjawiska krótko– i długoterminowych fluktuacji fazy oraz poślizgów fazy wynikających z różnic w częstotliwościach sygnałów taktowania zegarów stosowanych w węzłach (centralach) sieci telekomunikacyjnej. O ile w powszechnej usłudze telefonicznej występowanie poślizgów nie wpływa znacząco na jej jakość (poślizgi mogą objawiać się krótkotrwałymi trzaskami), o tyle w przypadku usług wymagających precyzyjnego taktowania (np. transmisja danych i obrazów) skutki poślizgów są bardzo odczuwalne. W najlepszym przypadku może to być wydłużenie czasu transmisji informacji, w najgorszym zaś zniekształcenia tekstów i obrazów aż do zerwania połączenia.

Synchronizacja nabiera szczególnego znaczenia w przypadku stosowania w cyfrowej sieci telekomunikacyjnej urządzeń SDH, których zegary z założenia powinny być synchronizowane do centralnego zegara (zegarów) odniesienia.

Powyższe aspekty wskazują, jak bardzo ważnym problemem jest stworzenie w sieci telekomunikacyjnej PKP niezawodnej i efektywnej sieci synchronizacyjnej.

Struktura sieci synchronizacyjnej PKP będzie stanowiła sieć wielopoziomową, w której zegary, stanowiące źródła sygnałów synchronizacyjnych, będą działały w oparciu o metodę synchronizacji „nadrzędny-podrzędny" (master-salve).

W sieci synchronizacyjnej PKP nie zakłada się stosowania wydzielonych mediów transmisyjnych czy też systemów do przesyłania sygnałów synchronizacyjnych. Nie wynika to z przyczyn technicznych lecz ekonomicznych oraz z trudności objęcia np. wydzielonych linii kablowych, jednolitym systemem zarządzania.

Planuje się, że w cyfrowej sieci telekomunikacyjnej PKP, opartej głównie na systemach transmisyjnych SDH oraz synchronizowanej zgodnie z metodą nadrzędny-podrzędny, będą następujące poziomy hierarchii zegarów:

4. Komutacja

4.1. Założenia dla sieci ISDN PKP

Podstawowym założeniem koncepcji modernizacyjnej sieci telekomunikacyjnej PKP jest to, że będzie ona zintegrowaną siecią wielousługową odpowiadającą standardom ISDN.
Sieć ta powinna:
- umożliwiać łatwe wprowadzenie standardowych usług telekomunikacyjnych zarówno o zasięgu lokalnym jak i ogólnosieciowym,
- świadczyć usługi sieci inteligentnych,
- umożliwiać w sposób standardowy współpracę z siecią TPSA i sieciami innych operatorów publicznych, sieciami innych Zarządów Kolejowych, siecią Kolpak, sieciami radiowymi trankingowymi i/lub sieciami komórkowymi (GSM),
- stosować standardową sygnalizację abonencką i międzycentralową (standardy ITU-T, ETSI) umożliwiającą m.in przenoszenie wszelkich informacji o abonencie między centralami np. czy abonent ma prawo łączenia się z centralą TPSA w innym mieście (innej strefie numerycznej) itd,
- funkcjonalnie obejmować oprócz sieci ogólnoeksplatacyjnej sieć dyspozytorską (zamknięte grupy abonentów) sieć telekonferencyjną, a być może, że i niektóre sieci technologiczne,
- obejmować oprócz central głównych także centrale węzłowe,

Sieć ta powinna być otwarta na modernizację wynikającą z postępu technicznego np. dołączenie do węzłów ATM. W sieci powinny być stosowane standardowe styki umożliwiające dołączanie do nich aparatów analogowych i cyfrowych różnych producentów spełniających międzynarodowe standardy.
Aby sieć ISDN prawidłowo działała musi być zbudowana zarówno sieć sygnalizacyjna jak i synchronizacyjna. Ponadto powinno być zbudowane centrum nadzoru i zarządzania węzłami komutacyjnymi. Centrum to powinno być przygotowane do współdziałania z centrum zarządzania siecią teletransmisyjną poprzez nadrzędne centrum zarządzania siecią telekomunikacyjną (TMN – Telecommunications Managment Network). Centrale ISDN powinny mieć możliwość wysyłania impulsów taryfikacyjnych przynajmniej z dwóch powodów:
1. do rozliczeń z operatorem publicznym TPSA, a być może, że i innymi operatorami,
2. do rozliczenia z abonentami niekolejowymi.
Taryfikacja jest niezbędnym warunkiem rozliczania się wewnątrz przedsiębiorstwa PKP jak i do prowadzenia działalności zarobkowej przez sieć telekomunikacyjną tym bardziej, że już obecnie są próby stosowania systemów bilingowych nadzorujących ruch z sieci kolejowej do sieci publicznej.

4.2. Poziomy central

Docelowa sieć ISDN PKP powinna być siecią o dwupoziomowej, wielobocznej strukturze hierarchicznej, składającej się z dwóch kategorii central
- tranzytowych
- końcowych.

Centrale tranzytowe powinny realizować połączenia pomiędzy poszczególnymi obszarami sieci ISDN PKP, połączenia do i z sieci TPSA oraz połączenia do innych Zarządów Kolejowych. Powinny być wyposażone w stanowiska informacyjno – połączeniowe i w systemy taryfikacyjne. Ze względu na taryfikację, komplikację układu sieci na styku sieci ISDN PKP z siecią TPSA, posiadane koncesję i zezwolenie telekomunikacyjne, sygnalizację, synchronizację itd. przewiduje się, że central tranzytowych w sieci ISDN PKP będzie nie więcej niż stref numeracyjnych w sieci TPSA tj. ponad 40 (obecnie jest 49 stref numeracyjnych w sieci TPSA).

rozbudowywana, przewidując jej stopniową likwidację, w miarę wycofywania z sieci telekomunikacyjnej PKP central analogowych.

3.2. Aktualny stan wyposażenia cyfrowej sieci teletransmisyjnej PKP

Na początku lat 90-tych PKP, zgodnie z kierunkami rozwoju światowej techniki telekomunikacyjnej zaczęły wprowadzać do swojej sieci cyfrowe systemy teletransmisyjne.
Na zbudowanej światłowodowej linii kablowej NSL (Północ – Południe) o długości ok. 1200 km. zastosowano cyfrowe urządzenia teletransmisyjne PDH firmy SAT (Francja) o przepływności 140 Mbit/s (1920 kanałów cyfrowych) na odcinku Gdańsk – Bydgoszcz – Warszawa – Kraków – Katowice oraz urządzenia teletransmisyjne o przepływności 34 Mbit/s (480 kanałów cyfrowych) na odcinkach Czechowice – Bielsko Biała i Czechowice – Zebrzydowice.

Dzięki zastosowaniu krotnic PCM-30 można było już w początkowym okresie (większość urządzeń końcowych pracowało w technice analogowej) eksploatować łącza 2 Mbit/s (30 kanałów cyfrowych) wykorzystując je dla potrzeb sieci ogólnoeksploatacyjnej, transmisji danych (łącza pomiędzy węzłami sieci Kolpak) oraz dla innych połączeń np. telekonferencji, łączy dyspozytorskich itp.

Jak już wcześniej zostało wspomniane PKP przyjęły strategię budowy swojej cyfrowej sieci teletransmisyjnej w oparciu o systemy hierarchii synchronicznej SDH. W 1995r został rozstrzygnięty przetarg na dostawę urządzeń SDH dla sieci PKP i podpisano wówczas kontrakt z firmą Alcatel Polska S.A. obejmujący dostawę i instalację urządzeń SDH i PDH (wyposażenie uzupełniające dla węzłów lokalnych) dla 11 linii (Warszawa – Łódź, Łódź – Kutno, Kutno – Poznań, Poznań – Szczecin, Poznań – Wrocław, Poznań – Rzepin, Poznań – Inowrocław, Szczecin – Gdańsk, Gdańsk – Olsztyn, Wrocław – Katowice, Radom – Lublin) oraz 11 węzłów (Katowice, Warszawa, Poznań, Szczecin, Wrocław, Łódź, Kraków, Lublin Gdańsk, Bydgoszcz, Olsztyn).
Kontrakt ten przewidywał, że podstawowe linie kablowe będą wyposażane w cyfrowe urządzenia transmisyjne SDH o przepływności binarnej 155,520 Mbit/s (STM-1), natomiast w Warszawskim Węźle Kolejowym, ze względu na rozbudowę sieci Kolpak zostaną zainstalowane urządzenia teletransmisyjne o przepływności 622,080Mbit/s (STM-4).
Wraz ze sprzętem teletransmisyjnym zakupiono wówczas także od firmy Alcatel Polska S.A. system centralnego nadzoru i zarządzania dla całej sieci SDH – PKP. Była to najnowsza wersja systemu zarządzania tej firmy (1353 SH i 1354 RM) oparta na platformie sprzętowej firmy Hewlett Packard (HP-9000). Przyjęto, że system ten będzie zainstalowany w Warszawie.
Pierwsze instalacje urządzeń teletransmisyjnych SDH na PKP rozpoczęto w węźle Katowice, ze względu na instalację cyfrowych central Merdian 1 firmy Kapsch.
W miarę budowy nowych kablowych linii światłowodowych w/w kontrakt był rozszerzany o dostawę i instalację urządzeń teletransmisyjnych SDH dla tych linii.

Obecnie PKP jest w końcowym etapie instalacji i uruchomiania urządzeń teletransmisyjnych SDH na podstawowych liniach i w głównych węzłach sieci teletransmisyjnej PKP. Konfiguracja tej sieci wraz z urządzeniami PDH linii NSL jest przedstawiona na rysunku 1.
Cyfrowa sieć teletransmisyjna PKP jest budowana w oparciu o dwa typy urządzeń teletransmisyjnych SDH firmy Alcatel: krotnice A 1641SM (STM-1), A 1651 SM (STM-4). Obecnie jest już zainstalowanych około 110 krotnic w/w typu.

Wydaje się jednak, że największym osiągnięciem w dziedzinie teletransmisji było uruchomienie w I kwartale br. roku, w Warszawie systemu centralnego zarządzania siecią SDH – PKP. System zarządzania urządzeniami SDH jest realizowany w postaci dwóch aplikacji:
– systemu zarządzania elementami sieci (1353 SH V1.2),
– systemu zarządzania siecią (1354 RM V.2.2).
Z założenia system zarządzania działa automatycznie, ale wymaga nadzoru, a w pewnych przypadkach również sterowania ze strony personelu obsługującego ten system.

MODERNIZACJA SIECI TELEKOMUNIKACYJNEJ PKP

Stanisław Gago, Dariusz Zagrajek

Polskie Koleje Państwowe, Dyrekcja Generalna, Naczelny Zarząd Automatyki i Telekomunikacji, ul. Chałubińskiego 4, 00-928 Warszawa

1. Wprowadzenie

Rozwój telekomunikacji oraz rozwój sieci komputerowych wykreowały nowe rodzaje usług. Usługi takie, jak: poczta elektroniczna, transfer plików, powszechny dostęp do baz danych (INTERNET), usługi sieci ISDN stały się ważnym składnikiem codzienności w wielu grupach zawodowych (administracje, firmy handlowe) w wielu krajach świata. Zasięg tych usług już dzisiaj jest ogromny

Jest rzeczą oczywistą, że do realizacji tych usług jest potrzebna odpowiednia infrastruktura telekomunikacyjna. Niezawodność i jakość usług, a także odpowiedni poziom bezpieczeństwa i poufności stanowi warunek powszechnej akceptacji usług teleinformatycznych. Stąd też jednym z najważniejszych zadań, przed którymi stoją operatorzy sieci telekomunikacyjnych jest modernizacja swoich sieci.

W tym procesie biorą udział również duże przedsiębiorstwa transportowe tj. Zarządy Kolejowe, a w tym także i Polskie Koleje Państwowe (PKP).

Ze względu na wielkość sieci, zakres świadczonych usług jak i rozległość (cały kraj), sieć telekomunikacyjna PKP powinna przyjmować rozwiązania techniczne stosowane w publicznych sieciach telekomunikacyjnych (zarządzanie, synchronizacja, sygnalizacja, numeracja, taryfikacja). Taki kierunek rozwoju tej sieci gwarantuje, że będzie ona otwarta zarówno na rozbudowę ilościową jak i przyjęcie nowych rozwiązań wynikających z postępu technicznego.

2. Kablowe linie światłowodowe w sieci telekomunikacyjnej PKP

PKP, podobnie jak większość zarządów kolejowych w Europie, dysponuje własną siecią telekomunikacyjnych linii kablowych (łączna długość około 40.000 km) oraz linii napowietrznych (około 7500 km). Linie kablowe do niedawna były budowane głównie w oparciu o klasyczne kable TKD (telekomunikacyjne kable dalekosiężne) i TKM (telekomunikacyjne kable miejscowe).

Obecnie dominującym kierunkiem w budowie cyfrowych sieci teletransmisyjnych jest szerokie zastosowanie światłowodów jako podstawowego środka do transmisji sygnałów.

Przy tworzeniu sieci optotelekomunikacyjnych PKP przyjęły następujące założenia:

- trasy przebiegu kablowych linii światłowodowych będą odpowiadać geograficznemu układowi linii kolejowych w sieci PKP,
- kolejność budowy kablowych linii światłowodowych powinna wynikać z hierarchii ich ważności w realizacji struktur pierścieniowych sieci teletransmisyjnej SDH oraz potrzeb tworzenia wiązek łączy cyfrowych pomiędzy budowanymi centralami cyfrowymi,
- budowane linie światłowodowe powinny umożliwiać stworzenie takiej struktury sieci teletransmisyjnej, w której do każdego węzła teletransmisyjnego istnieją co najmniej dwie niezależne drogi transmisyjne,

korzystanie z utworów (oprócz opłat od urządzeń reprograficznych i nośników dźwięku i obrazu); teraz kiedy pojawiły się możliwości techniczne, rozważa się możliwość wprowadzenia opłat za zwielokrotnianie utworów dla użytku osobistego.

4) na tle tych wszystkich podejmowanych działań pojawiają się głosy, iż tworzenie zasad i rozwiązań „pod" najnowsze osiągnięcia techniczne zarówno na gruncie prawa autorskiego jak i poza jego ramami może okazać się w niedługim czasie przestarzałe, niedostosowane do nowych potrzeb; ponadto wskazuje się, że istniejące jeszcze różnorodne rodzaje utworów, mediów i technologii zostaną włączone w jednolite środowisko multimedialne i w ten sposób dające się obecnie wychwycić istniejące między nim różnice ulegną zatarciu.

Uwagi dotyczące prawa polskiego (wcale do tych uwag nie mam pewności)

Chciałam przedstawić wątpliwości jakie rysują się na gruncie polskiej ustawy na podstawie trzech wybranych przepisów. I tak nie sposób omówić wszystkich licencji w aspekcie zapisu digitalnego i sieciowego przekazu informacji.

I tak **art. 25**, który jest jednym z tych które najbardziej wiążą się z przekazem informacji. W treści tego przepisu istotne są dwa pojęcia: **rozpowszechnianie i prasa**.

Jak wiadomo, zgodnie z art. 6 ust. 3 **rozpowszechnianie** to udostępnienie utworu publicznie w ten sposób, że odbiorca może zaznajomić się z dziełem w postaci zdatnej do percepcji; udostępnienie utworu może nastąpić w każdej formie, czyli nie tylko poprzez udostępnienie jego egzemplarzy. Takie pojęcie rozpowszechniania zgodne jest z przyjętymi rozwiązaniami zarówno w porozumieniach WIPO jak i projekcie dyrektywy.

Nie spotkałam się z polskimi komentarzami, które by precyzowały pojęcie „**publicznie**". Stąd też należy ten termin rozumieć chyba jako udostępnienie utworu większej liczbie osób w przeciwieństwie do kręgu osób wyznaczonego w art. 23 dot. dozwolonego użytku osobistego. Tak więc można chyba przyjąć, że umożliwienie dostępu do utworu poprzez wprowadzenie go do sieci jest udostępnieniem publicznym wg art. 6 ust. 3.

Dalej, można udostępnić w sieci „**już rozpowszechnione** „ sprawozdania, aktualne artykuły i zdjęcia reporterskie; czyli można chyba wyróżnić, że zostały one wcześniej rozpowszechnione w sieci albo w inny sposób.

Pojęcie **prasy**: do tego terminu należy posłużyć się definicją zawartą w ustawie pr. prasowe. Ponieważ daje ona możliwość zaliczenia do prasy powstające w wyniku postępu technicznego środki masowego przekazywania, dlatego za prasę internetową uznać można te publikacje, które nie tworzą zamkniętej całości, ukazują się w sieci nie rzadziej niż raz do roku i zaopatrzone są w odpowiednie dane: tytuł, numer bieżący, datę.

Fakt, że ustawodawca posłużył się w tym przepisie właśnie określeniem „prasa", można powiedzieć, że stawia nas to w lepszej sytuacji np. w stosunku do Niemców. Tam bowiem w analogicznym przepisie posłużono się określeniem „gazeta" a nie „prasa". Jest to więc pojęcie węższe i nie ma całkowitej jasności, czy gazetę dostępną online można nadal uznać za gazetę w rozumieniu przepisu ustawy (par. 49), zważywszy, że ten przepis jako wyjątek należy interpretować zwężająco. Pytanie więc, czy ma znaczenie w jakim medium udostępniane są informacje.

Tak więc można uznać, że przekazywanie informacji w granicach wyznaczonych art. 25 jest dozwolone także w środowisku sieciowym. Ponadto można jeszcze wskazać, że generalnie ten rodzaj licencji został przewidziany jako dozwolony i w porozumieniach WIPO i w proj. dyr.

Art. 27 (przeczytać)

W przypadku tego przepisu, pojęcia, które budzą wątpliwości, to: utwory opublikowane, egzemplarze utworów.

Jeśli chodzi o **utwory opublikowane**, to ani porozumienie WIPO ani projekt dyr. nie zajmują się tym terminem. Według naszej ustawy utwór opublikowany to taki, który został zwielokrotniony i którego egzemplarze zostały udostępnione publicznie. O ile w przypadku sieci

odbiorców. W ten sposób i w tym dokumencie objęte zostało ważne wykorzystywanie utworów w środowisku sieciowym.

Jeśli chodzi o **ograniczenia wyłącznych** praw autorskich, to art. 5 projektowanej dyrektywy zawiera zamkniętą regulację tej instytucji. Przede wszystkim stanowi, iż państwa członkowskie nie mogą wyjść poza ustanowione w tym przepisie granice dozwolonego zwielokrotniania i rozpowszechniania utworów. Ponadto wszystkie wymienione w ust. 1-3 dozwolone formy wykorzystywania utworów muszą spełniać wymogi znanego tzw. trzystopniowego testu, który wywodzi się z art. 9 ust. 2 konwencji berneńskiej i znalazł swoją kontynuację zarówno w postanowieniach TRIPs (art.. 13) jak i porozumień WIPO (art. 10, 16), a zatem ograniczenia te:

⇒ mogą być przewidziane tylko w przypadkach szczególnych,

⇒ nie mogą być sprzeczne z normalnym korzystaniem z utworu i

⇒ nie mogą przynieść nieuzasadnionego uszczerbku prawowitym interesom podmiotów uprawnionych.

Ust. 1 art. 5 stanowi jedyny przymusowy wyjątek, który polega na wyłączeniu spod wyłącznego prawa zwielokrotniania **czasowych aktów** zwielokrotniania, które mają miejsce w przekazie online, a które nie są dostrzegalne dla użytkownika. W ustępie tym sprecyzowane są więc przesłanki jakie muszą zaistnieć aby czasowe zwielokrotnianie mogło być wyjęte spod wyłącznego prawa.

Przede wszystkim takie zwielokrotnienie musi być:

⇒ częścią procesu technicznego a więc nie wywołanego bezpośrednio przez człowieka,

⇒ wywołane tylko dlatego, by można było skorzystać z utworu,

⇒ nie może mieć takie zwielokrotnianie samodzielnego gospodarczego znaczenia.

Wyodrębnienie tych przesłanek pozwala wyróżnić takie czasowe przechowanie materiału, które nie wpływa na intensywność korzystania z niego, od takiego, które może przyspieszyć czas jego przekazu, przez co ujawnia się jego samodzielne znaczenie ekonomiczne. To rozwiązanie nie jest ostateczne i może być jeszcze wzmocnione na korzyść podmiotów uprawnionych poprawką zaproponowaną przez Parlament lub Radę.

Ustęp 2 z kolei przewiduje wyjątki w zakresie reprografii, zwielokrotniania dźwięku i obrazu dla użytku osobistego oraz zwielokrotniania utworów przez biblioteki dla niegospodarczych i niekomercyjnych celów. Jeśli chodzi o uprzywilejowanie bibliotek publicznych i innych tego rodzaju instytucji, to projekt wyraźnie przewiduje wyłączenie w stosunku do tych podmiotów możliwości korzystania z utworów w zakresie przekazu online. To rozwiązanie jest odmienne od założeń przewidywanych w Zielonej Księdze, gdyż tam sugerowano aby biblioteki publiczne mogły korzystać z odczytu online na zasadzie wypożyczania egzemplarzy utworów.

Można powiedzieć, iż zgodnie z przewidywaniami, wcześniej cytowanego prof. Kopffa dotąd na ogół nieodpłatne korzystanie z utworów w ramach **użytku prywatnego**, z czasem w „związku z nowymi środkami technicznymi zwielokrotniania i rozpowszechniania dzieł w ramach użytku prywatnego będzie mieć charakter szeroki, a zarazem odpłatny"(Tamże, s.66). Omawiany bowiem projekt dyrektywy w art. 5 ust. 4 przewiduje obowiązek wprowadzenia przez kraje członkowskie roszczenia o stosowne wynagrodzenie za prywatne zwielokrotnianie. Ta kwestia, czyli prawa do wynagrodzenia nie jest jednak jeszcze całkiem przesądzona. Komisja Europejska przewiduje bowiem, zająć się w szerszym zakresie problemem dozwolonego użytku prywatnego utworów w środowisku digitalnym w bieżącym roku i przedstawić odpowiednią dyrektywę.

Dlatego też nie wiadomo jeszcze, czy faktycznie możliwe jest utrzymanie różnicy między granicami wyznaczonymi dla możliwości sporządzania kopii dla użytku prywatnego tradycyjnymi metodami a granicami wyznaczonymi dla digitalnego zwielokrotniania.

Wydaje się, że utrzymanie w przyszłej dyrektywie jedynie wyłącznego prawa podmiotów prawa autorskiego do udzielania zezwolenia na sporządzanie w ramach użytku prywatnego digitalnych kopii spowoduje, że podmioty uprawnione uzyskają *de facto* niewielką ochronę.

wydanej prze rząd USA również w 1995r.), która jedynie stanowi swego rodzaju analizę problemu w aspekcie dążenia krajów Unii do wspólnego rynku i zaznacza kwestie, które powinny być przedefiniowane bądź w inny sposób jasno określone.

Zasadniczymi pojęciami w zakresie licencji ustawowych są **„zwielokrotnianie"** i **„rozpowszechnianie"**. Dlatego też jako najistotniejsze wskazano, potrzebę zmiany tych pojęć. Uznano więc potrzebę przyjęcia wspólnego rozwiązania zagadnienia, czy digitalizacja stanowi **zwielokrotnienie** utworu, czy też nie (proponowano aby tu oprzeć się na rozwiązaniu przyjętym w dyrektywie UE o ochronie programów komputerowych, że wprowadzenie utworu do pamięci komp. stanowi jego zwielokrotnienie). Innym problemem było określenie, czy przewidziane w konwencji berneńskiej **wyjątki** od wyłącznych praw autorskich mają także zastosowanie do środowiska digitalnego. Otwarta pozostała także kwestia poddania bądź nie, dzięki pojawiającym się możliwościom technicznym, kontrolowania sporządzania kopii utworów dokonywanych w ramach użytku prywatnego (osobistego).

Jeśli chodzi o termin **„rozpowszechnianie"** to ma on centralne znaczenie dla wielu form wykorzystywania utworów (obok pojęcia „opublikowania utworu" często występującego w naszej ustawie). Rozpowszechnienie, to udostępnienie utworu publiczności. Jak więc dalece i swobodnie można korzystać w społeczeństwie informatycznym z materiałów przekazywanych autostradami informatycznymi. Doprecyzowanie tego pojęcia pozwoliłoby rozróżnić i ustanowić w wyważony sposób granice między możliwymi sposobami korzystania z utworów, tak by z jednej strony nie odstraszać twórców od udostępniania swych dzieł w sieci, z drugiej zaś by autostrady informatyczne spełniały swoją funkcję.

W rzeczywistości dotychczasowe międzynarodowe uregulowania nie precyzują tego pojęcia. Nie ma też żadnych wskazówek w obowiązujących dyrektywach UE. W Niemczech komentuje się np. iż rozpowszechnianie utworu zachodzi gdy skierowane jest **jednocześnie** do większej liczby osób, co nie zachodzi przy elektronicznej komunikacji tekstu, gdyż każdy odbiorca indywidualnie określa moment w którym zaznajamia się z danym tekstem. Dlatego też przyjęto w Niemczech rozwiązanie, iż elektroniczne przekazywanie tekstu jest aktem jego opublikowania. Wydaje się, że takie rozwiązanie nie jest precyzyjne, gdyż publikacja dotyczy egzemplarza utworu, a w przypadku elektronicznego przekazu nie mamy do czynienia z egzemplarzem.
Sprecyzowanie pojęcia publicznego odtwarzania utworu pozwoliłoby także na ustanowienie granicy między użytkiem publicznym i prywatnym w aspekcie korzystania z utworów w środowisku digitalnym. W związku z tym pozostawało także wątpliwe, czy wprowadzenie utworu do sieci ma być uznane za prawo wyłączne twórcy, czy też pozostające poza jego domeną.

Innym problemem jaki zasygnalizowano w Zielonej Księdze było określenie zakresu digitalnego **rozpowszechniania** i przekazywania utworów. Uznano, iż możliwe są tutaj dwa rozwiązania. Jedno: szerokie ujęcie prawa rozpowszechniania, które polegałoby na tym, że każde wprowadzenie utworu do sieci oznaczałoby jego rozpowszechnienie niezależnie od tego, czy przekazanie utworu odbyłoby się z jednego punku do innego, czy do wielu. Wąskie natomiast ujęcie oznaczałoby jedynie przekazywanie utworu od punktu do punku. Ponieważ takie przekazywanie różni się od nadań radiowych i telewizyjnych tym, że odbiorca może dokonywać zmian w przekazywanym materiale jak i tym, że ma do niego bezpośredni dostęp, należałoby zatem tego rodzaju przekaz digitalny poddać oddzielnemu reżimowi prawnemu. Ponadto pozostało pytanie jakie prawa powinny się wiązać z tego rodzaju działaniami, tzn. czy powinny one podlegać prawu wyłącznemu, czy powinno przysługiwać wynagrodzenie.

Chronologicznie następnym krokiem podjętym przez Światową Organizację Własności Intelektualnej (WIPO) były dwa porozumienia z grudnia 1996 jedno: o ochronie praw autorskich (WIPO I) i o ochronie artystów wykonawców, producentów fonogramów oraz stacji nadawczych (WIPO II). Celem tych porozumień było sprecyzowanie pojęć prawa autorskiego w aspekcie wykorzystywania utworów w środowisku digitalnym.

ODPOWIEDZIALNOŚĆ ZA NARUSZENIE PRAWA AUTORSKIEGO W SIECIACH KOMPUTEROWYCH.

I. Najważniejszą kwestią dla problematyki odpowiedzialności za naruszenie prawa autorskiego, gdy np. w sposób bezprawny zostaną umieszczone w Internecie utwory chronione prawem autorskim jest wyróżnienie podmiotów, które prowadzą działalność w Internecie i ustalenie w jakim zakresie i na jakiej podstawie każdy z nich mógłby ponosić odpowiedzialność. Do podmiotów tych należą:
– dysponenci i operatorzy sieci telekomunikacyjnej np. Telekomunikacja Polska S.A.
– dostawcy dostępu do sieci, te podmioty które umożliwiają dostęp do sieci, nie posiadając żadnego wpływu na treść przekazywanych materiałów, w Polsce np. NASK
– producenci i dostawcy materiałów do sieci – information provides, określa się tym mianen osoby które wprowadzają do sieci własne materiały i udostępniają innym, np. twórcy stron WWW
– dostawcy usług internetowych– service provider, którzy dostarczają własny materiał oraz dostęp do Internetu
– końcowi użytkownicy sieci

Najwięcej wątpliwości budzi kwestia odpowiedzialności service provider. Przedstawia się zarówno argumenty za wprowadzeniem takiej odpowiedzialności jak i przeciw.

Przeciwnicy wprowadzenia takiej odpowiedzialności podnoszą iż:
– w związku z ilością informacji jaka jest udostępniana nie ma praktycznych możliwości sprawdzania treści (zawartości) tych informacji,
– service providerzy nie są upoważnieni do oceny czy coś podlega i jakiej ochronie,
– wymaga to zatrudnienia dodatkowych pracowników/ludzi

Ponadto wprowadzenie takiej odpowiedzialności spowodowałoby ograniczenie działalności service providerów, gdyż ryzyko z nią związane byłoby zbyt duże i działalność taka nie byłaby opłacalna. Spowodowałoby to także zahamowanie rozwoju sieci komputerowych i przepływu informacji.

II. Odpowiedzialność za naruszenie prawa w świetle orzecznictwa zagranicznego.

III. Rozwiązania prawne proponowane w Niemczech i USA.

Dlatego tez w art. 50 pr. aut. dokonano przykładowego wyliczenia pól eksploatacji. Podział ten opiera się na zróżnicowaniu sposobów zwielokrotniania i rozpowszechniania utworów[11]. Do pól tych zaliczamy między innymi: utrwalenie, zwielokrotnienie, wprowadzenie do obrotu, wprowadzanie do pamięci komputera, wyświetlenie, nadanie za pomocą wizji i fonii, nadanie za pośrednictwem satelity. Obok kryterium form eksploatacji przy wyodrębnianiu nowego pola eksploatacji duże znaczenie ma kryterium nowego kręgu odbiorców (terytorialny zasięg użytkowników) oraz możliwości osiągnięcia dodatkowych korzyści majątkowych.

W orzeczeniu[12] z 1992 r. Sąd Najwyższy wyraził pogląd, iż „rozpowszechnianie filmów na kasetach video odbiega w zasadniczy sposób od rozpowszechniania na poprzednio znanych polach eksploatacji, tj. w kinach, w telewizji, a przede wszystkim z punktu widzenia komercyjnego, bowiem utwór powielony jest w nieporównywalnie większej ilości kopii i odtwarzany znacznie częściej".

Niewątpliwie Internet (sieć komputerowa) jest nowym polem eksploatacji, dlatego na wprowadzenie utworu do Internetu należy uzyskać zgodę podmiotu praw autorskich np. w postaci licencji zezwalające na wykorzystanie utworu na nowym polu eksploatacji.

Autorskie prawa majątkowe są ograniczone w czasie. Gasną z upływem 50 lat od:
– śmierci twórcy,
– jeżeli twórca jest nieznany od chwili pierwszej publikacji, a gdy utwór nie został opublikowany od chwili jego ustalenia,
– momentu pierwszej publikacji, jeżeli prawa autorskie z mocy ustawy przysługują innej osobie niż twórca.

Twórcy obawiają się także tego, iż rozpowszechnianie zdigitalizowanej postaci utworów doprowadzi do ich eksploatacji poza kontrolą twórców. Ograniczy to możliwości czerpania korzyści z eksploatacji utworów dostępnych w tradycyjnych formach i nie zapewni odpowiedniego wynagrodzenia autorom. Daje natomiast użytkownikom możliwość zwielokrotniania utworów bez obniżania jakości kopii. Ponadto w związku z możliwościami utrwalania na jednym nośniku różnych kategorii utworów traci na znaczeniu fakt kategoryzacji utworów.

Podczas konferencji zorganizowanej przez Światową Organizację Własności Intelektualnej w Genewie w grudniu 1996 r. zwrócono uwagę na konieczność dostosowania istniejących uregulowań prawnych do zmian jakie zachodzą w związku z powstaniem technologii cyfrowej, szczególnie w związku z możliwościami przechowywania i transmisji utworów w Internecie lub przy wykorzystaniu podobnych systemów elektronicznych. Jednak z uwagi na to, aby nie posługiwać się językiem za bardzo technicznym, nie zdecydowano się w tekście użyć słów „Internet" czy „cyfrowy"[13].

Na konferencji tej przyjęto dwie konwencje. Konwencja I [14] dotyczy ochrony dzieł literackich i artystycznych oraz nagrań dźwiękowych w erze elektronicznej, natomiast Konwencja II[15] zawiera regulacje dotyczącą ochrony praw artystów wykonawców i producentów fonogramów.

Najwięcej kontrowersji wzbudził projekt konwencji I, szczególnie w środowisku amerykańskich biznesmenów, użytkowników Internetu i firm zajmujących się usługami telekomunikacyjnymi. Szczególnie krytykowano rozwiązania dotyczące czasowej reprodukcji utworów (art. 7 proj.), albowiem obawiano się, iż w przypadku uznania relewantności „krótkotrwałych " kopii (których powstanie w pamięci komputera jest nieodłączne w przypadku

[11] E. Traple, w: Komentarz do....., str.248.
[12] Orzecznie nie publikowane, I A CR 296/92.
[13] Artykuł bez podania autorstwa, WIPO Annexes to Draft Treaties on Literary and Artistic Works, Performers works and Databases, opublikowany w BNA's Patent, Trademark & Copyright Journal 1996, vol. 52, str. 510.
[14] Tekst oryginalny w j. angielskim - WIPO Treaty on the Protection of Literary and Artistic Works and Sound Recording Rights in the Electronic Age, opublikowany w BNA's 1997, vol. 11, str. 64-67.
[15] Tekst oryginalny w języku angielskim, WIPO Performance and Phonograms Treaty, opublikowany w BNA's 1997, vol. 11, str.68-73.

Dla uznania wytworu intelektualnego za utwór w rozumieniu prawa autorskiego nie mają znaczenia takie okoliczności jak:
– wiek twórcy, jego stan psychiczny, stopień zdolności do czynności prawnych,
– zamiar stworzenia dzieła,
– przeznaczenie utworu np. cel naukowy, praktyczny,
– sprzeczność rozpowszechniania utworu z prawem – w przypadku dzieł pornograficznych lub fakt, iż dzieło powstało ono naruszeniem dóbr osobistych prawa powszechnego,
– wartość utworu – związana z poziomem estetycznym, naukowym, artystycznym,
– rozmiar utworu, bez względu czy jest to krótki kilku wersowy wiersz czy kilkuset stronicowa powieść.

Ochrona oparta na przepisach prawa autorskiego powstaje z chwilą ustalenia utworu umożliwiającego jakąkolwiek percepcję przez inne niż twórca osoby. Sama czynność ustalenia nie jest tożsama z czynnością utrwalenia na materialnym nośniku. Wystarczy zatem samo wykonanie utworu, zagranie. W nadal aktualnym orzeczeniu SN z 1973[8] uznano iż przez ustalenie należy rozumieć przybranie przez utwór jakiejkolwiek postaci, chociażby nietrwałej, ale na tyle stabilnej żeby cechy i treść utworu wywierały efekt artystyczny.

Ponadto powstanie ochrony nie jest uzależnione od spełnienia jakichkolwiek formalności umieszczenia adnotacji o zastrzeżeniu praw, znaku C, czy noty copyright`owej. Umieszczenie takiego zastrzeżenia służy często celom dowodowym, ułatwia dochodzenie ochrony, a także ułatwia nawiązanie kontaktu z twórcą lub podmiotem praw autorskich, ponieważ zawiera informacje o podmiocie tych praw – np. nazwisko autora lub nazwę wydawnictwa.

Ustęp 2 art.1 pr. aut. precyzuje, iż przedmiotem prawa autorskiego są w szczególności utwory:
– wyrażone słowem, symbolami matematycznymi, znakami graficznymi(literackie publicystyczne, naukowe, kartograficzne, oraz programy komputerowe)
– plastyczne,
– fotograficzne,
– wzornictwa przemysłowego,
– architektoniczne,
– muzyczne, słowno-muzyczne,
– sceniczne,
– audiowizualne.

Katalog utworów wymienionych w ustawie jest otwarty.

Artykuł 3 pr. autorskiego przewiduje, iż przedmiotem prawa autorskiego mogą być

zbiory – antologie-wybory – bazy danych, nawet jeżeli zawierają nie chronione materiały, o ile przyjęty w nich dobór, układ lub zestawienie ma charakter twórczy, bez uszczerbku dla praw do wykorzystanych utworów.

Natomiast nie stanowią przedmiotu prawa autorskiego, a więc mogą być dowolnie wykorzystywane bez względu na to czy są dostępne w Internecie, na serwerze np. Sejmu czy też zostały opublikowane w prasie:
– akty normatywne (ustawy, rozporządzenia, zarządzenia) lub ich urzędowe projekty,
– urzędowe dokumenty, materiały, znaki i symbole,
– opublikowane opisy patentowe lub ochronne,
– proste informacje prasowe.

Osoba, która stworzyła dzieło jest podmiotem praw autorskich majątkowych i osobistych.

[8] Opublikowane w OSN z 1974 r., poz.50.

Pojęcia, według których należałoby dokonywać oceny są bardzo nieostre i niejasne. Należy pamiętać, że zgodnie z tradycyjną doktryną Sądu Najwyższego ustawy ograniczające wolność słowa muszą posługiwać się terminami bardzo precyzyjnymi tak, aby nie stwarzać niepewności co do tego czy wypowiedzi te są dopuszczalne. Niepewność taka stanowi bowiem zagrożenie wolności albowiem ludzie nie mogą świadomie dokonywać wyboru – autocenzury aby unikną kary[1].

Ponadto zwrócono uwagę na jeden bardzo ważny aspekt związany z wprowadzaniem regulacji prawnej Internetu– wprowadzenie przepisów w jednym kraju nie rozwiąże problemu w skali całego świata. Jako przykład powoływano, iż ustawa ta nie osiągnie jednego ze swoich celów – nie uchroni dzieci przed pornografią, gdyż duża część przekazów internetowych pochodzi spoza USA, a CDA mogłaby być stosowana tylko do tych materiałów które były by wprowadzane do sieci w USA.

Ustawa CDA została zaskarżona do sądu, który uznał, iż jest ona sprzeczna z postanowieniami I i IV poprawki do konstytucji USA[2]. Ponadto w orzeczeniu swym sąd wyraził pogląd, iż Internet jest jedynym medium, w którym możliwa jest realizacja idei wolnego rynku informacji, w sposób dostępny dla każdego obywatela. Natomiast z uwagi na sam charakter Internetu uznać należy, że niedopuszczalne jest jakiekolwiek ograniczenie wolności wypowiedzi w tym medium.

Nie oznacza to, że w ogóle odstąpiono od zamiaru stworzenia ram prawnych dla działalności w Internecie. Poza tym już istniejące przepisy prawa mogą być stosowane wprost lub odpowiednio do nowych sytuacji.

INTERNET A PRAWO PRASOWE

Jedną z pierwszych wątpliwości jaka powstają w związku z funkcjonowaniem Internetu i potocznym określaniem go jako środka masowego komunikowania jest to czy można uznać Internet za środek masowego komunikowania (przekazu) podlegający regulacji polskiego prawa prasowego.

Pierwotnie prawo prasowe regulowało działalność wydawniczą odnoszącą się do pism drukowanych. Następnie wraz z pojawieniem się nowych rozwiązań technicznych i nowych form masowego przekazu informacji przedmiotowy zakres regulacji prawa prasowego uległ rozszerzeniu obejmując: radio, telewizję, film. Prawo prasowe[3] nie wyjaśnia pojęcia środki masowego przekazu. Posługując się potocznym znaczeniem tego terminu za "środki masowego przekazu" należy uznać: prasę periodyczną, radio, telewizję, film, ulotki, plakaty. Do tak szeroko rozumianych mass mediów z całą pewnością można zaliczyć Internet, co jednak nie przesądza jego kwalifikacji prawnej jako środka masowego przekazu. Natomiast w literaturze prawniczej jako mass media kwalifikuje się prasę periodyczna, radio, telewizje, a także film w zakresie w jakim przekazuje on informację prasowa i publicystykę[4].

Ustawa prawo prasowe zawiera definicję prasy, są nią publikacje nie tworzące zamkniętej całości, ukazujące się nie rzadziej niż raz w roku, opatrzone stałym tytułem lub nazwą, numerem bieżącym lub datą. W ustawie wymieniono przykładowo pewne rodzaje prasy, dzienniki, czasopisma, serwisy informacyjne, programy radiowe i telewizyjne oraz kroniki filmowe. Drugi człon tej definicji zawiera postanowienie umożliwiające zaliczenie do prasy także takich środków masowego przekazu, które mogą powstać w przyszłości w wyniku postępu technicznego. Na podstawie tej definicji za prasę internetową można uznać te publikacje, które nie tworzą zamkniętej całości, ukazują się w Internecie nie rzadziej niż raz w roku i posiadają stały tytuł, numer bieżący i datę. Zaletą czasopism internetowych jest to, że szybko docierają do czytelników, którzy są

---

[1] W. Sandurski, Śmiecie w Internecie, Rzeczpospolita nr 12 z dnia 15 stycznia 1997.
[2] Orzeczenie to jest dostępne w internecie pod adresem: http://www.vtw.prg/seech/decision.htm/.
[3] Dz.U. z 1994 r., nr 5, poz.24 z późn. zm.
[4] J. Barta, I. Dobosz: Prawo rasowe, Skrypty Uczelniane, Kraków 1989, str.12-13.

Spis treści

konstrukcji cennika może w niektórych szczególnych przypadkach wzbudzać wątpliwości. Część obecnych abonentów, ze względu na specyficzny charakter wykorzystania sieci preferuje zasadę taryfikacji za ruch i dla nich opłata ryczałtowa mogłaby się okazać mniej korzystna. Z myślą o tej grupie abonentów pozostawiono możliwość utrzymania uproszczonej taryfikacji za ruch na porcie przyłączeniowym. Zmiana cennika niesie również pewne ryzyko dla NASKu, ponieważ wystąpi okres zmniejszenia wpływów przy nieco wyższych kosztach. Mamy nadzieję, że okres ten będzie krótki.

NASK nie opuszcza swoich podstawowych partnerów. W dalszym ciągu specjalnie będziemy preferować abonentów z obszaru nauki, a również szeroko pojętej edukacji, dla których cennik przewiduje specjalne niższe taryfy. Możemy to zrobić bowiem współpracujemy również z akademickim operatorem zagranicznym transferującym ruch „akademicki" po niższej cenie. Rozszerzamy obecnie preferowane środowisko naukowe i akademickie na całą sferę nauki i edukacji (a więc i szkoły). Nadal będziemy realizować przedsięwzięcia w ramach porozumienia pomiędzy Ministrem Spraw Wewnętrznych i Administracji i NASK, jakkolwiek nasza rola w tym porozumieniu jest w naturalny sposób ograniczona. Spodziewamy się, że wobec nowych wyzwań związanych z reformą administracji kraju oraz dążeniami do NATO i UE współpraca ta ulegnie rozszerzeniu

Warto również wspomnieć, że NASK opiera się skutecznie zagrożeniom kadrowym wynikającym z „ssania rynkowego" związanego z pojawieniem się nowych operatorów telekomunikacyjnych. Podstawowy zespół NASK rozumie, że w całości reprezentuje potencjał znacznie większy niż suma indywidualnych potencjałów członków zespołu. Za to zrozumienie i wytrwałość należy się naszym kolegom szczególne uznanie.

Rozwijamy również współpracę z innymi jednostkami działającymi w tym obszarze. Pozwala to na lepszą obsługę klienta zapewniając mu usługę kompleksową jakiej NASK sam nie oferuję. W miarę upływu czasu coraz bardziej oczywisty staje się podział prac pomiędzy operatorem jakim jest NASK, a jednostką wspomagającą w zakresie prac nietypowych, dostaw sprzętu oraz obsługi klienta. Przykładem jest współpraca NASK z NASK SERVICE przy obsłudze dwóch umów kooperacyjnych z Unisource Business Network w Szwecji w zakresie międzynarodowych sieci korporacyjnych oraz Saturn Global Network z Australii w zakresie obsługi specjalnych usług bankowych.

Stoimy na stanowisku, że warunkiem rozwoju sieci w Polsce i uczynienia ich dostępnymi dla całego społeczeństwa jest jak najszersza współpraca operatorów sieciowych.