Sieć komputerowa Instytutu Łączności

Grzegorz Wójcik

Omówiono prace nad budową sieci komputerowej Instytutu Łączności. Szczególną uwagę poświęcono zagadnieniom związanym z wyborem technologii sieciowej, konfiguracji szkieletu sieci oraz doborem urządzeń sieciowych. Opisano również podstawowe usługi sieciowe uruchomione w sieci komputerowej IŁ, system zarządzania siecią oraz wybrane aspekty systemu ochrony informacji.

sieć komputerowa, intranet, usługi sieciowe, urządzenia sieci komputerowej, ATM

Wstęp

Sieć komputerowa Instytutu Łączności powstawała etapami. Początkowo, jak wszędzie w naszym kraju, był to zespół niepołączonych ze sobą lokalnych sieci Ethernet. W tym okresie nie było jeszcze właściwie możliwości wyboru innej technologii – dominował Ethernet wykorzystujący tzw. „cienki" kabel koncentryczny. Technologia ta miała wiele zalet. Przede wszystkim sieci na niej oparte tworzyło się łatwo, szybko i w miarę tanio. Jej piętą achillesową była jednak niezawodność – gdy rosły rozmiary sieci, zwiększała się też jej podatność na awarie, a pojedyncze uszkodzenie powodowało od razu wyeliminowanie z działania całego segmentu sieci. Przy rozbudowie dosyć szybko można było natrafić na poważne bariery: ograniczony zasięg i niewielką całkowitą przepustowość sieci.

Wady te oraz potrzeby Instytutu Łączności w zakresie możliwości korzystania z nowoczesnych usług sieciowych spowodowały, że w połowie 1996 r. zapadła decyzja o utworzeniu od podstaw strukturalnej sieci komputerowej w IŁ. Taka sieć nie tylko objęłaby swoim zasięgiem cały Instytut, ale zapewniłaby również wszystkim pracownikom dostęp do sieci rozległej i do wszystkich oferowanych przez nią usług. W trakcie przygotowywania tego projektu pamiętano, że tworzona sieć i zastosowane w niej rozwiązania, powinny służyć pracownikom Instytutu przez wiele lat. Starano się zatem, by kompromisy, na które – jak przy każdym większym projekcie – musiano się decydować, w jak najmniejszym stopniu dotyczyły najistotniejszych jej elementów.

Fizyczna konfiguracja sieci komputerowej IŁ

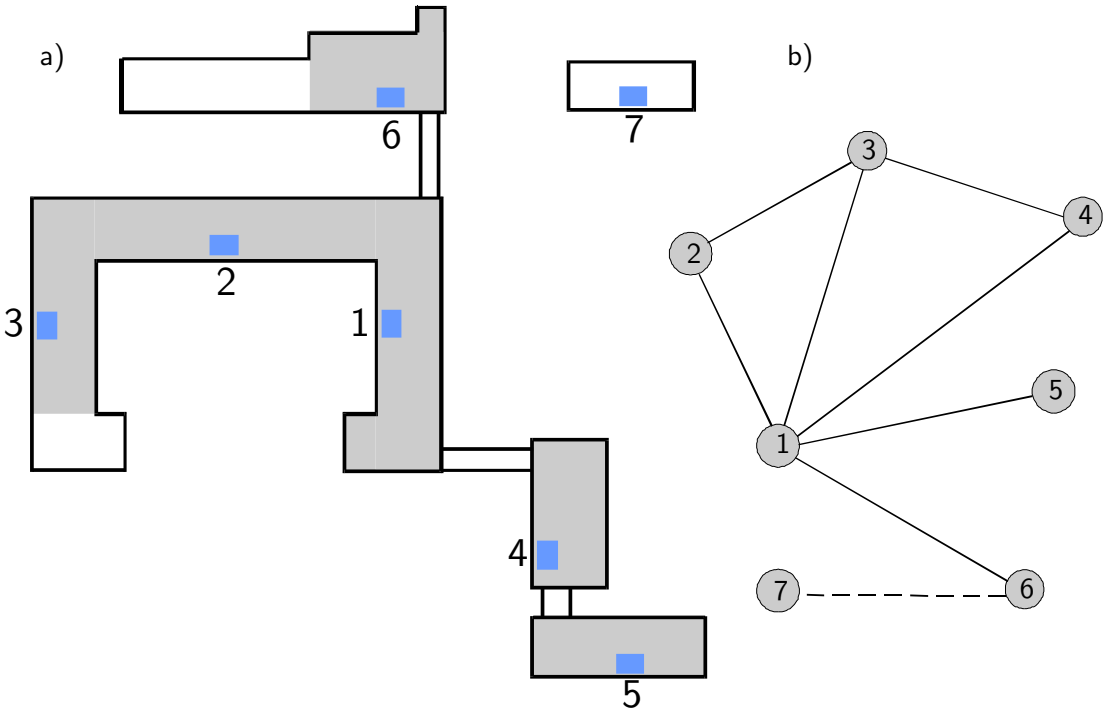
Szkielet sieci

Centrala Instytutu Łączności w Warszawie mieści się w kilku oddzielnych budynkach. Tworzona sieć musiała mieć zatem charakter sieci kampusowej, składającej się z pewnej liczby oddalonych od siebie węzłów, w których koncentrowałoby się okablowanie oraz znajdował się aktywny sprzęt sieciowy. Ze względu na wielkość głównego budynku IŁ, musiano dodatkowo podzielić tworzoną tam sieć na trzy niezależne części – z trzema dużymi węzłami (rys. 1).

Odległości między węzłami nie przekraczają 400 m, dlatego też poszczególne centra można było połączyć między sobą wielomodowymi łączami światłowodowymi. Aby umożliwić w przyszłości

światłowodowe połączenia z siecią rozległą, dwa węzły sieci zostały dodatkowo połączone łączami jednomodowymi z pomieszczeniem centrali telefonicznej, w której znajdują się zakończenia kabla światłowodowego łączącego Instytut z siecią publiczną.

Liczba włókien światłowodowych, w połączeniach między węzłami była oczywiście kompromisem między możliwościami przyszłej rozbudowy a ceną (w której główną rolę odgrywały koszty spawów, nie zaś koszty samego materiału czy nawet koszty ułożenia światłowodów). Zastosowano zatem kable sześciowłóknowe. W 1996 r. ta liczba światłowodów mogła wydawać się nadmiarowa, jednak dalszy rozwój sieci IŁ wykazał, że przyjęte rozwiązanie było słuszne.



Rys. 1. *Węzły sieci komputerowej Instytutu Łączności: a) rzut z zaznaczonymi węzłami sieci komputerowej (1÷7) i obecnym zasięgiem okablowania strukturalnego; b) istniejące połączenia światłowodowe między poszczególnymi węzłami sieci*

Wybór technologii sieci szkieletowej

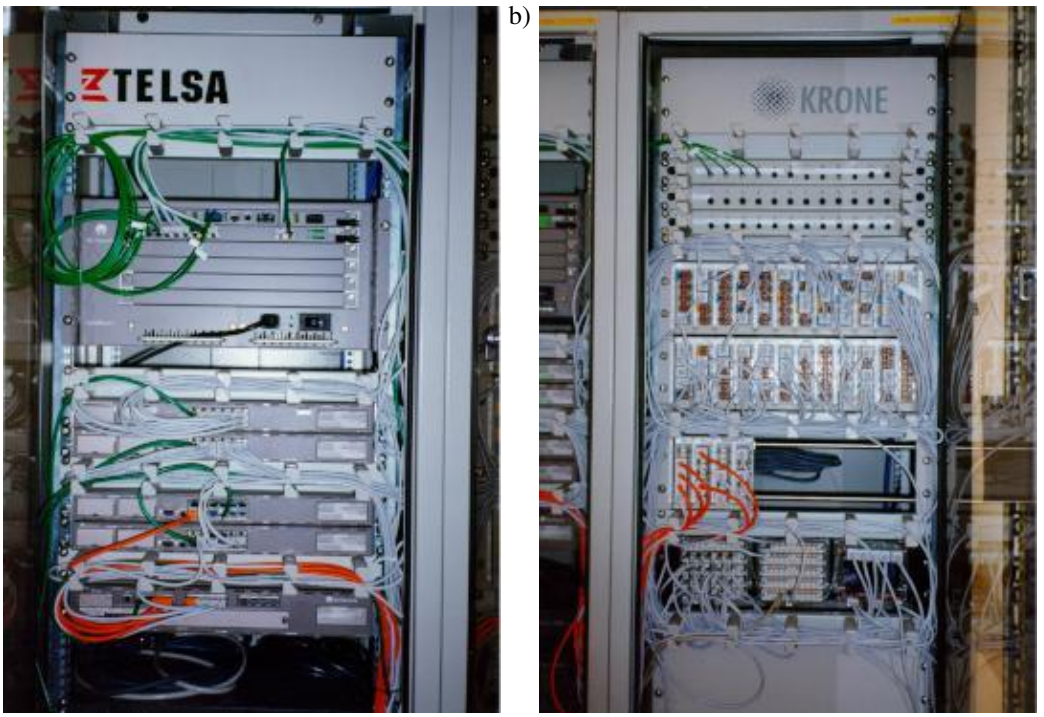
Wybór rozwiązania szkieletu sieci był jedną z najbardziej istotnych decyzji dla całego projektu. W tamtym okresie w praktyce można było wybierać tylko między dwiema technologiami – sieciami Fast Ethernet i ATM[①] (*Asynchronous Transfer Mode*). Wybór musiał być zatem kompromisem między możliwościami (uwzględniającymi poźniejszą rozbudowę) a ceną.

① *Warto zauważyć, że choć w technologii urządzeń sieciowych i sprzętu komputerowego upłynęła nieomal generacja – to przed podjęciem decyzji o budowie sieci szkieletowej wciąż dokonuje się wyboru między sieciami Ethernet (tym razem w ich najnowszym wcieleniu – Gigabit Ethernet) a ATM. Wprawdzie wzrosły znacznie przepustowości tych sieci, jednak zasadnicze argumenty za i przeciw każdej z technologii pozostają niezmienione.*

Sprzęt sieciowy kupowano z przetargu. Paradoksalnie – niezależnie od wyboru technologii – oferowane IŁ przez sprzedawców rozwiązania cechowała zawsze ta sama topologia sieci. Składały się na nią: centralny przełącznik (ATM lub Fast Ethernet), podłączone do niego łączami światłowodowymi przełączniki brzegowe, do których z kolei były podłączone koncentratory Ethernet. Rozwiązanie takie, choć narzucające się w przypadku sieci Ethernet, miało wiele wad – przede wszystkim ograniczoną przepustowość szkieletu sieci (pojedyncze łącza między przełącznikami) oraz podatność na awarie (uszkodzenie jednego łącza może spowodować odcięcie od reszty sieci dużej liczby komputerów). Istotną wadą była też wysoka cena centralnych przełączników.

Jednak w przetargu pojawiło się również inne rozwiązanie, które ostatecznie zostało wybrane ze względu na niezbyt wysoką cenę (w stosunku do innych tego typu urządzeń) oraz znacznie wyższe możliwości techniczne. Zdecydowano się na przełączniki ATM Centillion 100 firmy Bay Networks (obecnie Nortel Networks). Były to jedne z pierwszych przełączników, które mogły pełnić zarówno rolę przełącznika szkieletowego, jak i urządzenia brzegowego ATM. Mają one budowę modułową. Mogą być wyposażone w moduły z portami ATM (155 Mbit/s OC-3, 622 Mbit/s OC-12), Fast Ethernet (100 Base-TX, 100 Base-FX), Ethernet (10 Base-T) i Token Ring.

a) b)



Rys. 2. *Szafy dystrybucyjne jednego z węzłów sieci komputerowej Instytutu Łączności: a) urządzenia sieciowe; b) panele krosujące*

W każdym węźle sieci komputerowej IŁ został zainstalowany tego typu przełącznik (rys. 2). Jest on połączony, łączami ATM OC-3 o przepustowości 155 Mbit/s, z co najmniej dwoma przełącznikami, znajdującymi się w innych węzłach sieci. Dzięki temu awaria pojedynczego łącza nie powoduje odcięcia węzła od reszty sieci. Co więcej, te nadmiarowe połączenia są wykorzystywane w trakcie normalnej eksploatacji – ruch danych jest automatycznie rozdzielany między wszystkie możliwe trasy,

wzrasta zatem efektywna przepustowość całej sieci. W razie gdyby w jakiejś części sieci istniejące połączenia okazały się niewystarczające, można łatwo zwiększyć przepustowość, dodając kolejne połączenie między przełącznikami.

Konfiguracja sieci szkieletowej ATM opiera się na PVP (*Permanent Virtual Path*). Oznacza to, że każdy z przełączników ma pełną informację o wszystkich połączeniach między nim a pozostałymi przełącznikami (przypomina to nieco tworzenie statycznej tablicy rutingu dla klasycznych sieci TCP/IP). Ten sposób konfiguracji, choć bardzo pracochłonny, ma jednak jedną podstawową zaletę: awaria któregokolwiek z przełączników nie powoduje zakłóceń w działaniu reszty sieci. Umożliwia on również osiągnięcie maksymalnej przepustowości (w tym przypadku w przełącznikach nie odbywa się praktycznie żadne przetwarzanie danych).

Niektóre, najistotniejsze dla działania sieci lokalnej Instytutu, serwery zostały dołączone bezpośrednio do sieci ATM. Aby było to możliwe, należało również uruchomić obsługę standardu LANE 1.0 (*LAN Emulation*). Dla zwiększenia niezawodności sieci opartych na tym standardzie, producent stosowanych w IŁ urządzeń, przewidział możliwość zdefiniowania na przełącznikach ATM podstawowych dla działania sieci serwerów: LECS (*LAN Emulation Configuration Server*) i LES/BUS (*LAN Emulation Server/Broadcast Unknown Server*) – zostało to wykorzystane w konfiguracji sieci IŁ.

Oczywiście, zbudowana w ten sposób sieć komputerowa IŁ charakteryzuje się także innymi zaletami, np. łatwym tworzeniem sieci wirtualnych, czy też możliwościami transmisji ruchu multimedialnego. Nie wszystkie z tych właściwości sieci ATM są obecnie wykorzystywane, ale fakt, że sieć Instytutu można łatwo rozbudować, na wiele różnych sposobów, stanowi jej niewątpliwą zaletę.

Okablowanie strukturalne

Okablowanie strukturalne w Instytucie Łączności wykonano z zastosowaniem technologii Krone. Ogółem zainstalowano ok. 1200 gniazd RJ-45. Mogą być one wykorzystane jako punkty podłączeniowe do sieci informatycznej, ale także jako gniazdka telefoniczne. Do węzłów sieci doprowadzono bowiem wieloparowe kable z centrali telefonicznej. Dzięki temu łatwo można tworzyć połączenia między pokojami pracowników a centralą (zestawiając odpowiednie połączenia w szafach dystrybucyjnych węzłów). Większość okablowania spełnia wymogi kategorii 5. W niektórych przypadkach, gdy planowano wykorzystanie większych przepustowości niż 100 Mbit/s, instalowano okablowanie kategorii 5+. Ważniejsze serwery podłączono bezpośrednio do przełączników sieci szkieletowej przez światłowodowe łącza ATM.

Łącznie z budową strukturalnej sieci teleinformatycznej tworzono również wydzieloną sieć elektryczną dla urządzeń komputerowych. Zapewnia ona bardziej stabilną pracę tych urządzeń – uniezależnia od wahań napięcia w ogólnej sieci zasilającej oraz umożliwia odseparowanie ewentualnych sygnałów zakłócających pracę precyzyjnych urządzeń pomiarowych, znajdujących się w laboratoriach badawczych.

Urządzenia sieciowe

W pierwszym etapie budowy sieci, jako urządzenia dostępowe, instalowano koncentratory Ethernet 10 Base-T. Z punktu widzenia użytkowników, przepustowość sieci opartej na takich koncentratorach niewiele różni się od przepustowości sieci zbudowanej przy użyciu kabla koncentrycznego. Podział sieci na mniejsze segmenty[①], odpowiadający podziałowi organizacyjnemu w Instytucie, oraz podłączenie tych segmentów do przełączników umożliwiły i w tym przypadku uzyskanie większej przepustowości

① *Każdy z koncentratorów Ethernet można traktować jak niezależny segment sieci.*

sieci. Skończyły się również problemy z częstymi awariami – rozłączenie jednego przewodu nie powoduje już unieruchomienia całego segmentu sieci.

Jednak nowe, wymagające coraz szybszych sieci aplikacje, wzrost zainteresowania usługami internetowymi oraz powstający intranet, powodują, że stale rosną wymagania dotyczące przepustowości sieci lokalnej. W ciągu ostatnich lat radykalnie zmienił się sposób przetwarzania danych i korzystania z sieci. Dawniej większość informacji tworzono lokalnie, a wymiana informacji następowała głównie w obrębie jednego działu, teraz zaś większość informacji pobiera się z centralnych serwerów i Internetu, jedynie niewielkie ilości informacji wymienia się w grupach roboczych. Poza tym, rozpowszechnienie się nowoczesnych aplikacji, umożliwiających w łatwy sposób tworzenie rozbudowanych dokumentów multimedialnych oraz wielka rewolucja związana z WWW, spowodowały, że przez sieć przesyła się po prostu znacznie więcej danych.

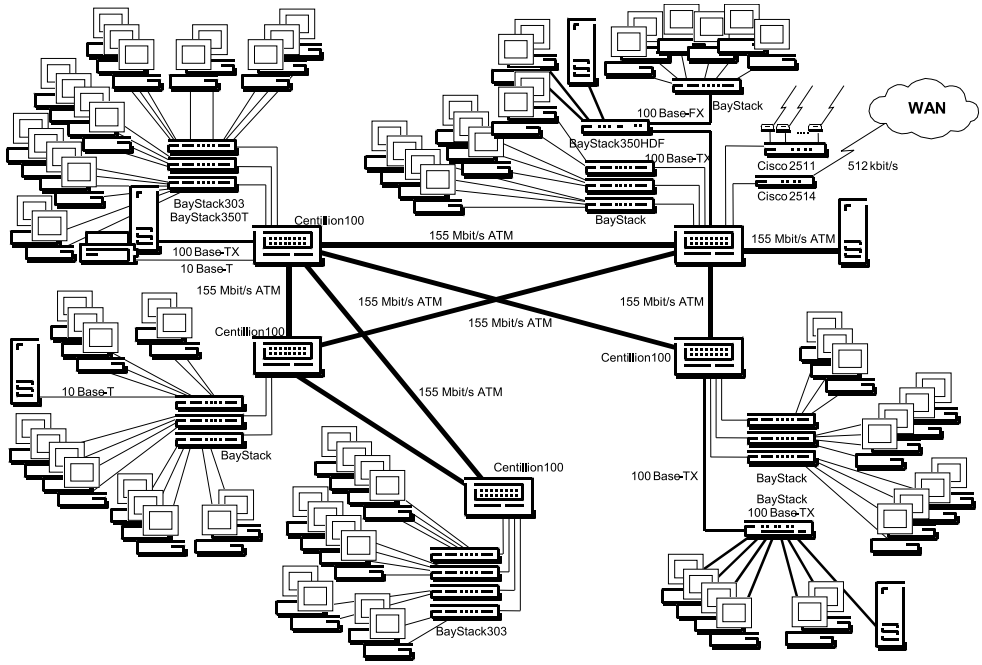
Te zmiany w zasadach korzystania z sieci komputerowej muszą pociągać za sobą zmiany w sposobach ich projektowania. Należy przede wszystkim uwzględnić to, że znacznie więcej danych będzie przesyłanych przez sieć szkieletową oraz że urządzenia brzegowe powinny zapewniać jak najlepsze do niej dołączenia. Dlatego też, począwszy od 1998 roku, zamiast koncentratorów (w nowych częściach sieci) są stosowane przełączniki. Tam, gdzie ruch jest mniejszy zastosowano przełączniki Ethernet, natomiast tam, gdzie wymienia się duże ilości danych użyto przełączników Fast Ethernet. W przypadku koncentratora wszyscy użytkownicy, których komputery są do niego podłączone, muszą dzielić się dostępnym pasmem. Co więcej, ze względu na kolizje pakietów w sieci (wynikające ze sposobu działania Ethernetu), nie ma możliwości pełnego wykorzystania dostępnej przepustowości. Szacuje się, że całkowity ruch w pojedynczym segmencie sieci nie powinien przekraczać 60–80% dostępnego teoretycznie pasma, bowiem przy dalszym wzroście ilości przesyłanych danych, lawinowo rośnie też liczba kolizji i dochodzi do całkowitego zablokowania sieci.

W przypadku przełącznika każdy z użytkowników dysponuje dedykowanym pasmem (10 lub 100 Mbit/s), które może wykorzystać w całości. Żaden z użytkowników nie może też zmonopolizować pasma. Dodatkową zaletą jest możliwość tworzenia sieci wirtualnych i filtracji ruchu.

Przełączniki podłączono do urządzeń szkieletowych łączami 100 Base-TX pracującymi w trybie *full-duplex*. Przepustowość szkieletu sieci wystarcza do obsługi ruchu generowanego przez te przełączniki (rys. 3).

Dołączenie do sieci rozległej

Ze względu na położenie Instytutu (ok. 20 km od centrum Warszawy i ok. 8 km od najbliższego węzła miejskiej sieci komputerowej) oraz fatalną jakość istniejących linii telefonicznych wynikły spore trudności przy doborze sprzętu do podłączenia Instytutu do sieci rozległej. Pierwotnie zdecydowano się na zastosowanie modemów synchronicznych RAD ASM 31. Sieć komputerowa IŁ była podłączona do węzła sieci Warman łączem synchronicznym o przepustowości 128 kbit/s. Obecnie przepustowość tego łącza została zwiększona do 512 kbit/s przez zastosowanie urządzeń nowej generacji: RAD ASM 51. W przyszłości planuje się uruchomienie połączenia światłowodowego między Instytutem Łączności a jedną z central TP SA, będącą równocześnie węzłem sieci Warman. Umożliwiłoby to zmianę istniejących połączeń telekomunikacyjnych i informatycznych, m.in. zestawienie na potrzeby łączności internetowej kanału cyfrowego o przepustowości 2 Mbit/s.



Rys. 3. *Uproszczony schemat lokalnej sieci komputerowej Instytutu Łączności*

Serwery sieci

Praktycznie wszystkie komputery w Instytucie są to komputery klasy PC, pracujące pod kontrolą którejś z wersji systemu operacyjnego Microsoft Windows. Natomiast nieomal wszystkie serwery to komputery Sun, wykorzystujące oparty na Unixie system operacyjny – Solaris. Wbrew „świętym wojnom" toczonym przez zwolenników obu systemów, jest możliwa ich znakomita współpraca.

Komputery firmy Sun Microsystems od lat cieszą się opinią bardzo wydajnych, stabilnych i niezawodnych serwerów. Stosowane są przede wszystkim jako serwery plików, baz danych oraz serwery usług sieciowych. Ich początkowa, dosyć wysoka cena, jest z powodzeniem rekompensowana olbrzymimi zasobami publicznie dostępnego, darmowego oprogramowania, które może być na nich uruchomione. Programy te mogą bardzo dobrze zastąpić wiele systemów komercyjnych i niejednokrotnie są od nich znacznie efektywniejsze w działaniu.

Usługi w sieci komputerowej IŁ

Sieć komputerowa bez dostępu do usług jest tylko nikomu nie potrzebną plątaniną drutów. Dopiero usługi, które oferuje, stwarzające zupełnie nowe możliwości wykorzystania sprzętu komputerowego, decydują o sensie jej tworzenia.

Początkowo, najbardziej oczekiwanym efektem pojawienia się sieci komputerowej w Instytucie Łączności była możliwość dostępu do sieci Internet. W miarę upływu czasu rosło również zapotrzebowanie i na inne usługi.

Serwer plików

Rolę serwera plików pełni w Instytucie dwuprocesorowy komputer Sun Ultra 2/170 wyposażony w macierz dyskową. Zasoby dyskowe serwera są dostępne przez sieć nie tylko dla maszyn unixowych (przez NFS – *Network File System*), ale również dla komputerów, na których działa system MS-Windows 3.11 i 95/NT. Udostępnianie wybranych dysków, zgodnie ze standardem Microsoft LAN Manager, umożliwia *Samba*. Jest to oprogramowanie *public domain*, dostępne dla praktycznie wszystkich wersji systemu Unix.

Umożliwia to nie tylko dystrybucję z jednego serwera praktycznie każdego rodzaju oprogramowania dostępnego w Instytucie, ale także znakomicie ułatwia pracę użytkownikom. Dzięki takiej konfiguracji mają oni możliwość korzystania z tych samych danych zarówno na komputerach PC, jak i na stacjach roboczych Sun Microsystems (wyniki obliczeń na silnych komputerach unixowych mogą być dalej przetwarzane na komputerach PC, np. przy użyciu standardowych arkuszy kalkulacyjnych).

Ponieważ serwer jest komputerem, na którym może pracować jednocześnie kilka osób, jest możliwe korzystanie z zasobów oprogramowania unixowego również i przez tych użytkowników, którzy nie mają stacji roboczych. Zdalna praca może odbywać się zarówno w trybie terminalowym (przez `telnet`, `rlogin` i `ssh`), jak i przez X-server.

Poczta elektroniczna

Poczta elektroniczna w Instytucie opiera się na protokołach SMTP (*Simple Mail Transfer Protocol*) i POP3 (*Post Office Protocol*). Serwerem pocztowym jest również komputer unixowy, natomiast odbierać listy można z dowolnego komputera dołączonego do naszej sieci lokalnej. Najczęściej wykorzystuje się do tego takie programy, jak: *Netscape Navigator* i *Microsoft Internet Explorer*.

W Instytucie działają też pocztowe listy dystrybucyjne, za pomocą których przesyła się np. informacje o zmianach zachodzących w sieci komputerowej czy korespondencję wewnątrz grup roboczych.

Możliwe jest również szyfrowanie poczty i opatrywanie jej podpisem cyfrowym. Służy do tego oprogramowanie PGP (*Pretty Good Privacy*). Odpowiednie wersje tego systemu są dostępne zarówno na maszynach unixowych, jak i na komputerach PC.

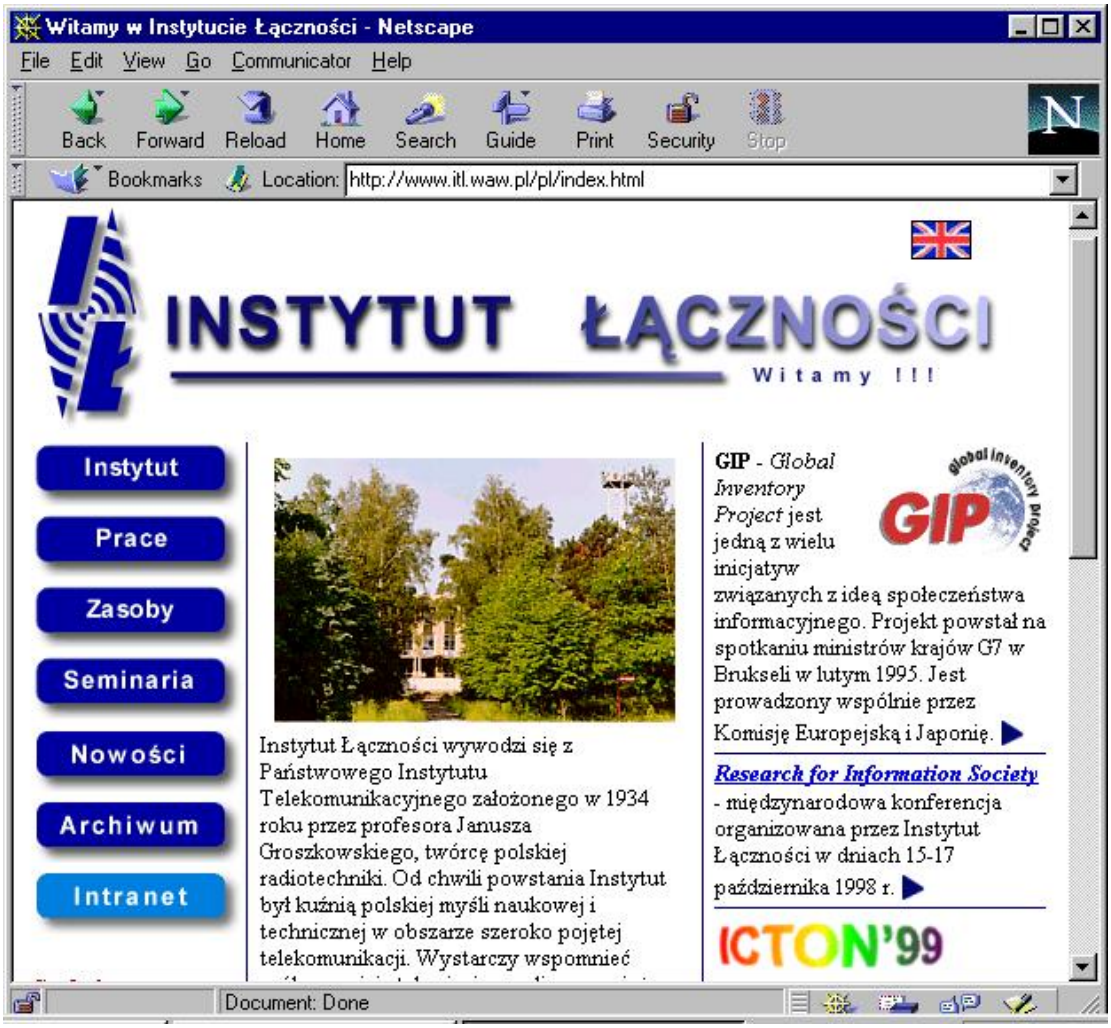
Serwer WWW

Stworzony w IŁ serwer WWW udostępnia nie tylko podstawowe informacje o Instytucie, ale także – dzięki wykorzystaniu możliwości tworzenia dynamicznych stron WWW – umożliwia dostęp do gromadzonych w IŁ zasobów oprogramowania i dokumentacji (rys. 4). Wprost ze stron WWW można również skorzystać z baz danych organizacji standaryzacyjnych ETSI, ITU, IEC, bazy publikacji IŁ itp.

W przyszłości można tam będzie również znaleźć niektóre z programów tworzonych w Instytucie oraz dokumentację wybranych urządzeń i oprogramowania.

Serwer w3cache

W3cache jest serwerem pośredniczącym w wymianie danych między odległymi serwerami WWW a przeglądarkami znajdującymi się w sieci lokalnej, takimi jak Netscape czy Internet Explorer. Idea działania w3cache jest prosta – przechowuje w pamięci (lub na dysku) ostatnio odwiedzane strony WWW. Im częściej dana strona jest odwiedzana, tym dłużej pozostaje w pamięci serwera. Oczywiście w momencie, gdy strona znajduje się już na lokalnym serwerze w3cache, nie ma potrzeby łączenia



Rys. 4. *Główna strona serwera WWW IŁ*

się z odległym serwerem WWW – stronę pobiera się z pamięci podręcznej (do odległego serwera jest wysyłane jedynie krótkie zapytanie na temat daty ostatniej modyfikacji strony, aby upewnić się, że w pamięci znajduje się jej najbardziej aktualna wersja). Uruchomiony w Instytucie Łączności serwer w3cache opiera się na oprogramowaniu *public domain* (`squid` 2.2.5). Ma on dwa zadania: po pierwsze, odciążenie łącza do sieci rozległej (a co się z tym wiąże zmniejszenie kosztów jego utrzymania), a po drugie – przyspieszenie dostępu do najczęściej odwiedzanych stron WWW.

Serwer FTP

Powody utworzenia w sieci Instytutu Łączności serwera FTP (*File Transfer Protocol*) były podobne, jak w przypadku serwera w3cache. Przede wszystkim należało stworzyć w sieci lokalnej Instytutu miejsce, w którym byłoby przechowywane najczęściej wykorzystywane oprogramowanie *public*

domain i dokumentacja sieciowa, tak aby użytkownicy naszej sieci nie byli zmuszeni do korzystania z odległych archiwów sieciowych. Serwer FTP uruchomiono na oprogramowaniu komercyjnym (udostępnionym jednak Instytutowi nieodpłatnie) – *ncftpd*. Dodatkowo na serwerze tym działa oprogramowanie umożliwiające tworzenie lustrzanych kopii wybranych katalogów z innych serwerów w sieci Internet. Dzięki temu na serwerze IŁ zawsze znajdują się najbardziej aktualne wersje kilku najczęściej wykorzystywanych pakietów, natychmiast bowiem nadąża on za zmianami, które zachodzą w miejscach ich powstawania.

Archiwum to daje również pracownikom Instytutu możliwość udostępniania własnego oprogramowania innym użytkownikom sieci.

Usenet News

Usenet News jest to jedna z najstarszych usług Internetu. Gromadzi ona wiele tysięcy, zorganizowanych hierarchicznie, grup dyskusyjnych, poruszających problemy z praktycznie wszystkich dziedzin życia. Wypowiadają się zarówno laicy, jak i wybitni eksperci w danej dziedzinie. Szczególnie liczne są grupy zajmujące się nauką i techniką (np. `sci.*`, `comp.*`). Dużą aktywność wykazują polskojęzyczne grupy dyskusyjne (`pl.*`).

W Instytucie Łączności uruchomiono własny serwer Usenet News (`news.itl.waw.pl`), mający bezpośrednie połączenie z największym polskim serwerem tego typu, znajdującym się w Interdyscyplinarnym Centrum Modelowania Uniwersytetu Warszawskiego. Serwer wykorzystuje oprogramowanie *public domain*: `inn`. Zapewnia przechowywanie artykułów i dostęp do najważniejszych grup dyskusyjnych Usenetu.

Intranet

Mianem intranet określa się zwykle sposób dostępu do zasobów sieci lokalnej – analogiczny do tego internetowego. Podstawową rolę odgrywa tu wewnętrzny serwer WWW. Uruchomienie takiego serwera było więc pierwszym etapem tworzenia intranetu w Instytucie. Jest on dostępny wyłącznie z sieci lokalnej i widziany pod nazwą `intranet` (rys. 5). Ponieważ serwer ten ma służyć nie tylko do prezentowania informacji, ale także do wprowadzania danych, uruchomiono bezpieczną wersję serwera opartą na protokole SSL (*Secure Socket Layer*). Protokół ten umożliwia szyfrowanie danych przesyłanych między serwerem WWW a przeglądarką, a także wzajemne uwierzytelnianie stron biorących udział w sesji transmisji danych.

Na intranetowym serwerze WWW Instytutu Łączności umieszcza się dane najczęściej potrzebne i wykorzystywane w codziennej pracy. Są to: bazy danych aktów prawnych, z których korzysta Instytut, formularze najczęściej używanych dokumentów (sprawozdania i wnioski), dane finansowe, wewnętrzne ogłoszenia Instytutu oraz dane na temat sieci komputerowej (informacje o zachodzących w niej zmianach, zainstalowanym oprogramowaniu, sposobach korzystania z podstawowych programów, statystyki ruchu).

Komunikacja modemowa

W sieci komputerowej Instytutu Łączności został uruchomiony również serwer komunikacyjny. Dla pracowników Instytutu jest dostępnych 8 modemów Microcom IS Porte, pracujących z szybkością 33,6 kbit/s. Serwer zapewnia możliwość pracy w protokołach PPP (*Point-to-Point Protocol*) i SLIP (*Serial Line Internet Protocol*). Serwer komunikacyjny został tak skonfigurowany, że komputer dołączony do niego przez łącze telefoniczne staje się jakby jeszcze jedną końcówką sieci lokalnej z własnym

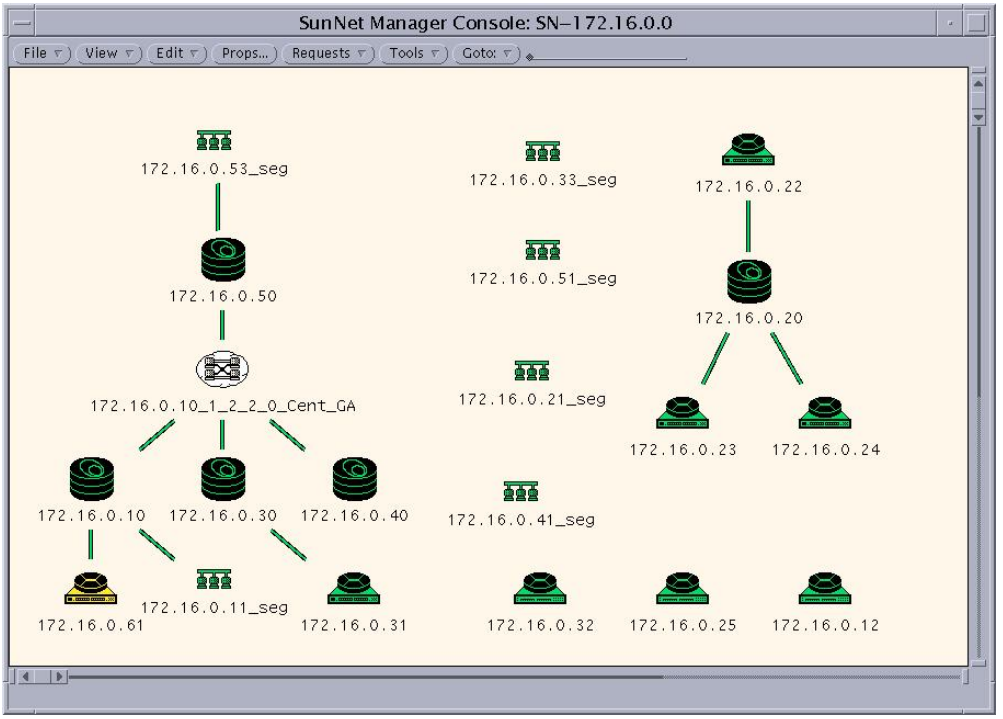
Rys. 5. *Pierwsza strona serwera intranetowego IŁ*

adresem IP i możliwością korzystania ze wszystkich usług lokalnej sieci komputerowej (w tym intranetu). Dostępna jest również możliwość zdalnego zalogowania się z serwera komunikacyjnego na wybrany komputer sieci lokalnej, np. przez `telnet`. Autoryzacja użytkowników próbujących dostać się do sieci Instytutu odbywa się przez osobny serwer TACACS.

Zarządzanie siecią

Sieć komputerowa Instytutu staje się coraz bardziej złożona. Od jej właściwej pracy coraz częściej zależy sprawne działanie wielu działów. Dlatego też jest konieczne stosowanie narzędzi, które umożliwią analizowanie zjawisk zachodzących w sieci, szybkie alarmowanie o zaistniałych awariach oraz zdalną konfigurację urządzeń sieciowych.

Do zarządzania siecią jest wykorzystywany protokół SNMP (*Simple Network Management Protocol*). Praktycznie wszystkie urządzenia sieciowe sieci lokalnej IŁ mogą być monitorowane i konfigurowane przy jego użyciu. Podstawowym stosowanym oprogramowaniem jest *Sun Domain Manager* (rys. 6). Na nim opierają się działające aplikacje charakterystyczne dla posiadanego przez IŁ sprzętu sieciowego firmy Bay Networks: *Optivity Network Management System* (zarządzanie koncentratorami, przełączni-



Rys. 6. *Niektóre urządzenia sieciowe IŁ przedstawione na konsoli SunNet Managera*

kami i ruterami), *Optivity Analysis* (analiza ruchu w sieci, statystyki na podstawie sond RMON) oraz *Optivity Planning* (agregacja statystyk, raporty z działania sieci).

Bezpieczeństwo

Wprawdzie sieć komputerowa Instytutu Łączności jest typową siecią jednostki naukowo-badawczej – przesyła się przez nią i przechowuje na serwerach dane, które w większości nie są informacjami o charakterze poufnym – ale jednak dla komfortu pracy badawczej ważne jest, aby nie można było ingerować w działanie sieci i przesyłane przez nią dane.

Od strony sieci rozległej sieć lokalna jest chroniona przez odpowiednio skonfigurowane rutery i „zaporę ogniową" (*firewall*). Zapewniają one m.in. filtrację ruchu, tj. do sieci wewnętrznej IŁ przepuszcza się tylko te pakiety, które spełniają warunki bezpieczeństwa (np. stanowią odpowiedź na próbę połączenia z sieci wewnętrznej, są skierowane do serwera WWW, FTP lub do serwera pocztowego itd.). Na komputerze pełniącym rolę „zapory ogniowej" stworzono tzw. *proxy server* dla wielu podstawowych usług sieciowych. Połączenia kierowane do serwera pocztowego, serwera FTP, czy np. realizowane w protokole telnet, są przechwytywane przez *firewall*, który po sprawdzeniu, że mogą one być skierowane do sieci lokalnej, sam łączy się z odpowiednimi serwerami. Dzięki temu nawet jeśli w oprogramowaniu serwerów znalazłby się jakiś błąd mogący naruszyć zasady bezpieczeństwa sieci, to nie można go wykorzystać z sieci zewnętrznej. W tej sieci te serwery są po prostu niewidoczne.

Dodatkowym utrudnieniem dla ewentualnego intruza jest dynamiczny przydział adresów, pod którymi komputery IŁ są widziane w sieci zewnętrznej (NAT – *Network Address Translation*). Lokalnie są używane adresy prywatne z grupy numerowej 172.16.0.0. W momencie gdy którykolwiek z komputerów znajdujących się w sieci wewnętrznej nawiązuje połączenie z maszyną spoza Instytutu, przyznaje mu się adres IP z puli oficjalnych adresów IŁ. Ponieważ adresy przyznawane dynamicznie stale się zmieniają (a co więcej, jeden adres zewnętrzny może odpowiadać wielu komputerom z sieci wewnętrznej), bardzo trudno jest komuś z zewnątrz zidentyfikować konkretny komputer pracujący w sieci IŁ.

Podsumowanie

Sieć Instytutu podlega ciągłym zmianom. Nieustanny postęp technologiczny oraz wzrastające wymagania stawiane urządzeniom i oprogramowaniu wymuszają ich stały rozwój. W najbliższej przyszłości planuje się np. wprowadzenie do sieci standardów PNNI (*Private Network-Node Interface*) i MPOA (*MultiProtocol Over ATM*). Cały czas są rozwijane usługi intranetowe.

W niniejszym artykule omówiono zasady, jakimi kierowano się przy budowie utworzonej w latach 1996–98 sieci komputerowej Instytutu Łączności. Pomimo że jest to sieć powstająca na potrzeby jednostki naukowo-badawczej, to doświadczenia – zdobyte przy jej planowaniu, budowie i bieżącej eksploatacji – mogą być wykorzystane przy tworzeniu dowolnej, dużej sieci komputerowej.

Grzegorz Wójcik

Mgr inż. Grzegorz Wójcik (1970) – absolwent Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej (1994); nauczyciel akademicki oraz administrator sieci komputerowej na tym Wydziale (od 1994), kierownik Laboratorium Sieci Komputerowych oraz Laboratorium Obliczeń Równoległych i Rozproszonych Instytutu Automatyki i Informatyki Stosowanej Politechniki Warszawskiej (od 1996); kierownik Ośrodka Informatyki w Instytucie Łączności w Warszawie (od 1997); zainteresowania naukowe: projektowanie i zarządzanie sieciami komputerowymi, sieciowe systemy informacyjne.
e-mail: G.Wojcik@itl.waw.pl