Część I
Usługi zorientowane połączeniowo i usługi bezpołączeniowe

Warstwy mogą oferować warstwom leżącym o jeden poziom wyżej, usługi bezpołączeniowe i usługi wymagające połączenia. W usługach sieciowych zorientowanych połączeniowo użytkownik usługi najpierw ustala połączenie, potem połączenia używa, a następnie przerywa połączenie. Ten rodzaj usług przypomina całkowicie połączenia w sieci telefonicznej.

Usługi bezpołączeniowe przypominają typowe usługi pocztowe. Każda wiadomość występująca w tego rodzaju usługach posiada pełny adres przeznaczenia i przesyłana jest przez sieć niezależnie od innych wiadomości. Może się więc zdarzyć, że wiadomość, przesłana jako pierwsza dotrze do adresata później, niż wiadomości o numerach większych. Taka sytuacja jest nie do pomyślenia w usługach zorientowanych połączeniowo.

Każda usługa cechuje się określoną jakością. Niektóre usługi są niezawodne w tym sensie, że nie powodują one nigdy utraty danych. Zwykle usługę niezawodną realizuje się w ten sposób, że adresat potwierdza odbiór każdej wiadomości, wobec czego nadawca ma pewność, że wysłana wiadomość osiągnęła cel. Procedura potwierdzeń wymaga kanału zwrotnego i wprowadza opóźnienia, co może być czasami niepożądane.

Typowym przykładem niezawodnej usługi zorientowanej połączeniowo, jest transfer pliku, kiedy wymaga się, by wszystkie bity były poprawnie odebrane w takiej kolejności, w jakiej zostały nadane.

Nie wszystkie zastosowania wymagają usług zorientowanych połączeniowo. Dotyczy to wiadomości, co do których wymaga się jedynie, by były przesłane do adresata z dużym prawdopodobieństwem doręczenia, ale bez gwarancji, że je doręczono. Przykładem tego typu usługi mogą być różnego rodzaju reklamy i oferty handlowe dostarczane przez pocztę. Taka usługa, na ogół tańsza od usługi zorientowanej połączeniowo, jest nazywana *usługą datagramową*, analogicznie do usług telegraficznych, przy wykonaniu których nie zawiadamia się nadawcy telegramu, że adresat telegram otrzymał.

Z innych usług bezpołączeniowch należy jeszcze wymienić *usługę datagramową z potwierdzeniem* oraz *usługę żądania odpowiedzi.*

Część II
Prymitywy usług

Usługi realizuje odpowiednie oprogramowanie, dlatego powinny one być precyzyjnie zdefiniowane. Usługę określa się zatem formalnie jako zestaw

tzw. prymitywów, będących do dyspozycji użytkownika, pragnącego skorzystać z danej usługi. Prymitywy te, pełniące podobną rolę w opisie usługi jak instrukcje i deklaracje języka programowania, powiadamiają usługę o konieczności podjęcia pewnego działania, lub informują o działaniu, podjętym przez stację równorzędną.

W modelu OSI prymitywy dzieli się na cztery klasy:

Tabela 1: Klasy prymitywów

Prymityw	**Znaczenie**
żądanie	żądanie od usługi wykonania pewnego działania
wskazanie	informowanie o pewnym zdarzeniu
odpowiedź	zgłoszenie chęci odpowiedzi na zdarzenie
potwierdzenie	informowanie o żądaniu usługi

Do pierwszej grupy należą prymitywy żądania, stosowane gdy wymaga się podjęcia jakiegoś działania, np. ustalenie połączenia lub przesłanie danych. Prymityw wskazania oznajmia jednostce związanej z żądaniem, że będzie wykonana pewna operacja, dotycząca tej jednostki, np. że ktoś żąda połączenia z daną jednostką. Jednostka, otrzymująca prymityw wskazania używa prymitywu odpowiedzi by powiadomić zainteresowaną jednostkę, iż jest w stanie przyjąć lub odrzucić określone działanie. Jednostka, która posługuje się prymitywem żądania może za pomocą prymitywu potwierdzenia dowiedzieć się, jakie działanie zostało podjęte na skutek prymitywu żądania.

Usługa może być potwierdzona – stosuje się wtedy prymitywy wszystkich czterech typów. Jeśli usługa nie jest potwierdzona, w użyciu są tylko prymitywy żądania i wskazania.

Część III
Przykłady sieci komputerowych

Na świecie działa obecnie wiele sieci komputerowych różnego typu. Istnieją sieci dokładnie zaprojektowane i zrealizowanie przez jedną organizację, a obok nich sieci budowane przez amatorów, stanowiące przypadkową kolekcję komputerów, łączonych ze sobą przez wiele lat bez nadzoru żadnej fachowej instytucji. Stąd też dostępne w sieciach usługi mogą dotyczyć, zarówno dowolnej komunikacji między procesami, jak i poczty elektronicznej, transferu plików, czy też zdalnej rejestracji użytkownika w sieci. Różniące się między sobą sieci mają też różne społeczności użytkowników. Warto więc poznać możliwości i historię kilku typowych sieci, aktualnie działających na świecie.

Część IV
Sieci publiczne

W wielu krajach administracje rządowe lub instytucje prywatne zaczęły oferować usługi sieciowe każdej organizacji lub osobie, zainteresowanej usługami tego typu. Na ogół proponuje się usługi komunikacyjne, polegające na łączeniu kanałami transmisyjnymi hostów i terminali potencjalnych klientów. Tak tworzone systemy, nazywają się sieciami publicznymi i są one podobne do sieci telekomunikacyjnej powszechnego użytku, a często stanowią nawet fragment takiej sieci.

Chociaż sieci publiczne w różnych krajach wyposażone są w różny sprzęt, wirtualnie są one podobne, ponieważ stosują one model OSI oraz znormalizowane protokoły CCITT lub ISO we wszystkich warstwach (tabela 3.1).

Dla najniższych trzech warstw sieci komputerowej CCITT wydało zalecenia, które są powszechnie respektowane na całym świecie. Protokół warstwy fizycznej (CCITT X.21) określa interfejs fizyczny, elektryczny i proceduralny między hostem a siecią. Aktualnie niewiele krajów respektuje tę normę, ponieważ dotyczy ona telefonii cyfrowej PCM, która funkcjonuje równolegle z powszechnie stosowanym starszym systemem telefonii analogowej. Oczekuje się jednak, że protokół X.21 będzie miał duże znaczenie w przyszłości, kiedy sieci telefoniczne w większości krajów zostaną zmodernizowane.

Norma warstwy łącza danych posiada kilka odmian, uwzględniających jednak problem korekcji błędów transmisji, powodowanych przez zakłócenia na liniach telefonicznych, łączących aparaturę użytkownika sieci komputerowej z publiczną podsiecią telekomunikacyjną.

Protokół warstwy sieci (CCITT X.25, warstwa 3) zajmuje się problemami adresowania, sterowania przepływem, potwierdzeniami odbioru, itp. Na świecie pracuje wiele terminali, które nie potrafią używać tego protokołu. Dlatego też takie terminale podłącza się do sieci za pomocą urządzenia do formowania i demontażu pakietów PAD (Packet Assembler Disassembler), którego funkcję opisano w zaleceniu CCITT X.3. Istnieje też znormalizowany protokół między terminalem a PAD-em (CCITT X.28) oraz między PAD-em a siecią (CCITT X.29).

Wyższe warstwy sieci publicznych cechuje znacznie mniejszy stopień uniformizacji. ISO opracowała normy definicji usługi bezpołączeniowej warstwy transportowej ISO 8072 i zorientowany połączeniowo protokół warstwy transportowej ISO 8073. Prawdopodobnie większość sieci publicznych te propozycje zaakceptuje.

ISO opracowała też normy dla zorientowanych połączeniowo usług warstwy sesji i protokołu warstwy sesji ISO 8326, ISO 8327 oraz normy dla usługi i protokołu warstwy prezentacji. Należy oczekiwać powszechnej akceptacji również i tych norm, chociaż potrzeby w tym zakresie nie są duże, gdyż wiele aplikacji nie wymaga wcale usług sesji i prezentacji.

Warstwa aplikacji zawiera zbiór protokołów dla różnych zastosowań. Należy tu wymienić:

- protokół dostępu i zarządzania systemem plików FTAM (File Transfer, Access and Management),
- protokół wirtualnego terminala VTP (Virtual Terminal Protocol),
- protokół zdalnego przetwarzania wsadowego JTM (Job Transfer and Manipulation), służący do przesyłania programów i plików.

Tabela 2: Kluczowe normy sieciowe CCITT i ISO

warstwa	**norma**	**opis**
1 – 7	ISO 7948	model odniesienia ISO/OSI
7	ISO 8571	usługa transferu plików
	ISO 8872	protokół transferu plików
	ISO 8831	usługa zdalnego przetwarzania wsadowego
	ISO 8832	protokół zdalnego przetwarzania wsadowego
	ISO 9040	usługa wirtualnego terminala
	ISO 9041	protokół wirtualnego terminala
	CCITT X.400	zalecenia dla poczty elektronicznej
6	ISO 8822	zorientowana połączeniowo usługa prezentacji
	ISO 8823	zorientowany połączeniowo protokół prezentacji
5	ISO 8326	zorientowana połączeniowo usługa sesji
	ISO 8327	zorientowany połączeniowo protokół sesji
4	ISO 8072	zorientowana połączeniowo usługa transportowa
	ISO 8073	zorientowany połączeniowo protokół transportowy
3	CCITT X.25	protokół X.25 warstwy 3.
2	ISO 8802	lokalne sieci komputerowe
	CCITT X.25	protokół warstwy łącza danych
1	CCITT X.21	cyfrowy interfejs warstwy fizycznej

Część V
Sieć ARPANET

Sieć ARPANET opracowała, zaprojektowała i zrealizowała instytucja DARPA (Defense Advanced Research Projects Agency), podległa ministerstwu obrony USA. Prace nad siecią rozpoczęto pod koniec lat 60., a pierwsze

eksperymenty techniczne przeprowadzono w grudniu 1969, po zbudowaniu sieci o 4 węzłach. W ciągu następnych lat sieć rozrosła się terytorialnie, łącząc kilkaset hostów na połowie globu ziemskiego, od Hawajów po Szwecję. Zastosowana w tej sieci technologia okazała się wysoce niezawodna, dlatego też wkrótce zbudowano w oparciu o tę technologię sieć wojskową MILNET, posiadającą swoje europejskie odgałęzienie o nazwie MINET. Obie te sieci są połączone z siecią ARPANET, ale przepływ informacji między siecią cywilną i wojskową jest ściśle kontrolowany. Następnie z siecią ARPANET połączono dwie sieci satelitarne SATNET i WIDEBAND. Wiele podłączonych do sieci ARPANET uniwersytetów amerykańskich i instytucji rządowych posiada własne sieci lokalne, co czyni z ARPANET-u sieć rozległą z tysiącami hostów i setkami tysięcy użytkowników.

Początkowo w węzłach sieci ARPANET pracowały minikomputery DDP-516 firmy Honeywell, o pamięci 12 tysięcy 16-bitowych słów, ale z upływem lat węzły te wielokrotnie modernizowano, wyposażając je w coraz to większe komputery, bez zmiany ich funkcji. Na początku węzły sieci były połączone za pomocą łączy transmisji danych, o szybkości 56000 bitów na sekundę, dzięki czemu każdy węzeł mógł obsłużyć od jednego do czterech hostów. Łącza takie pracują w tej sieci do dziś, ale aktualnie używa się też łączy o wiele szybszych, a do jednego węzła sieci można podłączyć maksymalnie 10 hostów z setkami terminali każdy.

ARPANET nie przestrzega zaleceń modelu OSI, ponieważ sieć ta jest starsza od tego modelu o 10 lat. W sieci ARPANET protokół międzywęzłowy stanowi mieszaninę protokołów warstw 2. i 3. modelu OSI, a warstwa 3. zawiera mechanizm doboru drogi dla wędrujących przez sieć pakietów, oraz weryfikuje poprawny odbiór każdego wysłanego w sieć pakietu, czego nie realizuje 3. warstwa modelu OSI. Protokół warstwy sieci, nazywany skrótowo IP (Internet Protocol), jest protokołem bezpołączeniowym, zaprojektowanym dla obsługi połączeń sieci ARPANET z licznymi sieciami lokalnymi i rozległymi. Protokół transportowy tej sieci, TCP (Transmission Control Protocol), jest protokołem zorientowanym połączeniowo i ogólnie przypomina protokół transportowy modelu OSI. W sieci ARPANET nie ma protokołów warstwy sesji i warstwy prezentacji, gdyż podczas wieloletniej eksploatacji sieci nie było potrzeby ich stosowania. Istnieją tu jednak różne protokoły warstwy aplikacji, które nie są podobne do ich odpowiedników w modelu OSI.

Sieć ARPANET świadczy swoim użytkownikom usługi typu transfer plików, poczta elektroniczna i zdalna rejestracja w sieci.

Część VI

Sieć ETHERNET

W roku 1973 pracujący w firmie Xerox Corporation Robert Metcalfe wraz z Dawidem Boggsem i grupą współpracowników rozpoczął realizację sieci lokalnej Ethernet, której koncepcję przedstawił w swojej pracy doktorskiej, obronionej w tym właśnie roku na renomowanym uniwersytecie MIT. Pracami tej grupy zainteresowała się firma Intel, opracowując dla tej sieci jednoczipowy sterownik, oraz przedsiębiorstwo General Motors (GM), konkurujące z japońskimi firmami samochodowymi, pragnące utworzyć jedną sieć komputerową dla wszystkich swoich biur, fabryk i przedstawicielstw handlowych i tym sposobem usprawnić proces produkcji i dystrybucji samochodów. Istotnym dla GM problemem była automatyzacja produkcji za pomocą lokalnej sieci komputerowej, pracującej w czasie rzeczywistym, łączącej wszystkie roboty na taśmie montażowej. Sieć ta miała minimalizować czas montażu, a w swej pierwotnej postaci Ethernet takiej możliwości nie posiadał.

Wszystkie połączone komputery sieci Ethernet znajdują się w stanie nasłuchu i badają, czy kablem są przesyłane dane. Jeśli w kablu nie ma sygnału, żaden komputer nie może danych nadawać. W przypadku gdy dwa komputery nadają w tym samym czasie, występuje stan kolizji, komputery przerywają nadawanie na krótki, losowo dobrany okres czasu, a następnie ponawiają próbę nadawania. W tym systemie trudno ustalić teoretycznie górną granicę czasu oczekiwania, podłączonej do sieci stacji na nadawanie, gdyż jest to wielkość statystyczna. Rozwiązanie to było nie do przyjęcia dla GM, gdyż firma ta potrzebowała systemu, w którym każdy komputer miałby wyznaczony deterministycznie cykliczny dostęp do sieci, z jednakowym dla każdego komputera czasem oczekiwania na nadawanie. Sieć lokalną o takiej własności nazwano siecią typu *token bus* (token - znak, bon, żeton, bus - szyna, magistrala). W międzyczasie firma IBM przyjęła jako normę podobny typ sieci lokalnej, o nazwie *token ring*, pracującej bardzo niezawodnie i posiadającej wiele innych zalet. Te trzy rozwiązania zostały wzięte pod uwagę przez największą światową organizację zawodową, zajmującą się normalizacją, IEEE (Institute of Electrical and Electronic Engineers), która opracowała normy IEEE 802.3 (Ethernet), IEEE 802.4 (token bus) i IEEE 802.5 (token ring), wychodząc z założenia, że lepiej mieć trzy normy niż jedną.

Poza tym GM i inne firmy zainteresowane automatyzacją produkcji dostrzegały potrzebę przyjęcia takich protokołów w każdej warstwie modelu OSI, które byłyby uniwersalne i brały pod uwagę przyszły rozwój technologii. W ten sposób powstał protokół MAP (Manufacturing Automation Protocol) dla sieci typu *token bus*, zaakceptowany przez wiele przedsiębiorstw.

W tym samym czasie firma Boeing była zainteresowana normami dla automatyzacji prac biurowych i nie miała wymagań związanych z automatyzacją czasu rzeczywistego (montaż samolotów 747 nie jest produkcją taśmową). Dla tych zastosowań sieć typu Ethernet była instalacją wystarczającą. Firma Boeing opracowała więc dla tej sieci zestaw protokołów TOP (Technical and Office Protocols), również zaakceptowany przez wiele firm, poszukujących wygodnego narzędzia tylko dla automatyzacji prac biurowych.

Firmy GM oraz Boeing starały się usilnie, by stosy protokołów MAP i TOP były jak najbardziej kompatybilne (tabela 3).

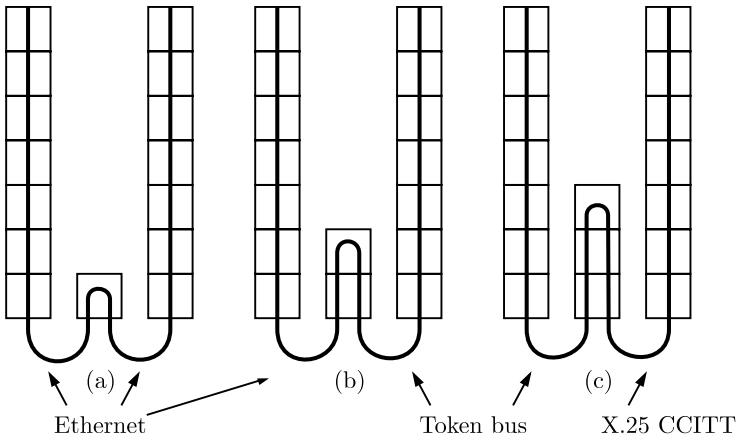
Tabela 3: Stosy protokołów MAP i TOP

warstwa	**protokół MAP**	**protokół TOP**
warstwa 7	FTAM, DS, MNS	FTAM, DS, VTP, MHS
warstwa 6	protokół prezentacji ISO 8823	protokół prezentacji ISO 8823
warstwa 5	protokół sesji ISO 8327	protokół sesji ISO 8327
warstwa 4	protokół transportowy ISO 8073	protokół transportowy ISO 8073
warstwa 3	protokół warstwy sieci ISO 8473	protokół warstwy sieci ISO 8473
warstwa 2	sterowanie łączem fizycznym ISO 8802/2	sterowanie łączem fizycznym ISO 8802/2
warstwa 1	token bus ISO 8802/4	Ethernet, token ring ISO 8802/3, ISO 8802/5

Obydwa stosy protokołów ściśle dostosowują się do modelu OSI, używając w warstwach 2 – 6 tych samych protokołów. W warstwie 4. zastosowano zorientowany połączeniowo protokół klasy 4, zakładający że warstwa sieci nie jest w pełni niezawodna i sama dokonuje procedur korekcji błędów oraz steruje przepływem danych. Przy tym założeniu możliwe są połączenia z każdą siecią, nawet o najgorszej jakości. Osiąga się to kosztem skomplikowania funkcji warstwy transportowej, która musi uwzględniać zawodną usługę sieciową.

Zestaw protokołów TOP rozpoznaje 4 typy systemów, które mogą istnieć

w sieci: system końcowy (end system, host), wzmacniak (repeater), most (bridge), urządzenie trasujące (router) oraz bramę (gateway). Systemy te różnią się między sobą liczbą warstw, użytych w połączeniu (rys. 1).



Rysunek 1: Repeater (a), most (b), router (c)

Repeater przekazuje transmitowane bity z jednej sieci do innej, dzięki czemu obie sieci tworzą logicznie jedną sieć. Jest to urządzenie dość proste, nie posiadające żadnego oprogramowania, służące jedynie do retransmisji bitów.

Most jest systemem, stosowanym do ustalania połączeń międzysieciowych, przebiegających przez dwie warstwy. System ten jest użyteczny np. wówczas, gdy sieci posiadają różne warstwy łącza danych przy tej samej warstwie sieci. Przypadek taki ma miejsce podczas łączenia sieci Ethernet i token ring, posiadających różne formaty ramek. Jest to urządzenie programowalne, dużo bardziej skomplikowane od repeatera i zawierające dość zaawansowane oprogramowanie.

Router jest wymagany wówczas, gdy dwie sieci stosują ten sam protokół warstwy transportowej przy różnych protokołach warstwy sieci. System ten jest niezbędny, np. przy połączeniu sieci typu token bus z siecią publiczną opartą na protokole X.25 CCITT.

Brama jest takim systemem, który stosuje się do wykonywania połączeń sieci nie stosujących modelu OSI. Często takie połączenie dotyczy warstwy aplikacji.

Podobne możliwości posiada stos protokołów MAP. Nie używa on natomiast repeaterów, stosując w zamian mosty, i dostosowany jest do pracy w czasie rzeczywistym.

Część VII

Sieci UUCP i USENET

W wyniku upowszechnienia się systemu operacyjnego UNIX, powstała pilna potrzeba kopiowania plików między różnymi komputerami, pracującymi pod nadzorem tego systemu. Problem ten rozwiązano, opracowując program **uucp** (UNIX to UNIX Copy Program). Systemy UNIX-owe były wyposażane w modemy i tzw. telefoniczne wzywaki automatyczne, co stwarzało możliwość automatycznego kopiowania plików między zdalnymi komputerami za pomocą programu uucp. Zaczęły więc powstawać sieci informacyjne, w których jeden komputer centralny z automatycznym wzywakiem, mógł łączyć się późno w nocy z całą grupą komputerów na raz i przekazywać im pliki oraz pocztę elektroniczną. Takie sieci rozwijały się szybko, ponieważ aby się stać ich użytkownikiem, wystarczyło mieć komputer z systemem UNIX-owym i modem. Dziś sieć tego typu, zwaną siecią UUCP, tworzą dziesiątki tysięcy komputerów i miliony użytkowników.

Sieć UUCP, w odróżnieniu od sieci publicznych czy sieci ARPANET, które są przeważnie centralnie zarządzane, nie podlega żadnym ograniczeniom. Chociaż w sieci UUCP panuje całkowita swoboda, granicząca z anarchią, to w społeczności użytkowników tej sieci znajdują się setki kompetentnych specjalistów, którzy dbają o to, aby sieć działała sprawnie mimo braku centralnego nadzoru. Europejski segment sieci UUCP posiada nawet swoją nazwę EUnet i jest bardziej zorganizowany. Każdy kraj europejski posiada jeden komputer centralny, pełniący rolę bramy (gateway), nadzorowany przez jednego administratora. Cały ruch międzynarodowy przechodzi przez takie bramy, które rozdzielają strumień danych między sieci narodowe. Europa i USA połączone są linią dzierżawioną między Amsterdamem a pewnym hostem w stanie Virginia, zwanym **uunet**, i połączonym też z siecią ARPANET. Segmenty sieci UUCP istnieją także w Australii, Korei, Japonii i innych państwach pozaeuropejskich.

Z siecią UUCP, świadczącą głównie usługę poczty elektronicznej, stowarzyszona jest sieć USENET, utworzona przez Duke University z Północnej Karoliny, oferująca nową usługę w postaci nowości sieciowych (network news). Prawie wszystkie UNIX-owe komputery w USA oraz wszystkie komputery sieci EUnet włączone są do sieci UUCP i USENET.

Nowości sieciowe są podzielone na setki grup tematycznych z różnych dziedzin. Obok grup dotyczących każdego popularnego języka programowania, czy też każdego systemu operacyjnego, istnieją np. grupy, poświęcone rekreacji. Użytkownicy sieci USENET mogą być subskrybentami tej usługi i deklarować swoje zainteresowania.

Część VIII
Sieć CSNET

Po uruchomieniu sieci ARPANET w latach 80-tych wiele uniwersytetów amerykańskich nie miało do niej dostępu, gdyż ta sieć była własnością departamentu obrony USA. Aby z usług sieciowych mogła korzystać cała społeczność amerykańskich informatyków, fundacja NSF (National Science Fundation) uruchomiła sieć CSNET, udostępniając ją wszystkim uniwersyteckim wydziałom informatyki (informatyka - Computer Science, stąd dwie pierwsze litery nazwy sieci CSNET). W rzeczywistości sieć CSNET nie jest siecią, jak ARPANET, ale tzw. metasiecią. Oznacza to, że CSNET używa środków transmisji, oferowanych przez inne sieci, ale na samej górze stosu protokołów dorzuca własną warstwę, dzięki czemu jest postrzegana przez swoich użytkowników jako sieć samodzielna. CSNET łączy około 150 środowisk akademickich i składa się z czterech komponentów w postaci podsieci, sterowanych centralnym komputerem o nazwie CSNET-RELAY. Komponentami tymi są:

- Sieć ARPANET, do której już są podłączone wydziały informatyki wielu uniwersytetów za pomocą łączy dzierżawionych o przepustowości 56 kbit/s.
- Sieć publiczna z protokołem X.25 CCITT. Za pomocą tej sieci można łączyć się z komputerem CSNET-RELAY.
- Sieć PHONENET, do której podłącza się te uniwersytety, które nie mają połączenia ani z ARPANET-em, ani z siecią X.25. Hosty sieci PHONENET mogą łączyć się bezpośrednio z komputerem CSNET-RELAY. Sieć PHONENET nie jest centralnie administrowana i jest w działaniu podobna do sieci USENET.
- Sieć CYPRESS, będąca repliką w mniejszej skali sieci ARPANET, posiadająca hosty oraz węzły, zwane IMPLET-ami.

Wszyscy użytkownicy sieci CSNET (z wyjątkiem tych, którzy są podłączeni do sieci PHONENET i mają do dyspozycji tylko pocztę elektroniczną), mogą korzystać z usług poczty elektronicznej, transferu plików i zdalnej rejestracji w sieci.

Sieć CSNET dostarczyła jej twórcom wielu pozytywnych doświadczeń i skłoniła fundację NSF do utworzenia w roku 1987 podobnej sieci, NSFNET, zapewniającej dostęp do superkomputerów, rozmieszczonych na całym terytorium USA. Używanie superkomputerów często wiąże się z transferem dużej ilości danych, dlatego też w sieci NSFNET do połączeń odległych zastosowano łącza mikrofalowe o przepustowości 1,5 Mbit/s. W sieci NSFNET, podobnie jak w sieciach ARPANET, CSNET i w sieciach UNIX-owych, stosuje się protokoły TCP/IP.

Część IX
Sieć BITNET

Innym interesującym przykładem sieci jest podobna do sieci CSNET, sieć łącząca wszystkie wydziały różnych uniwersytetów, nie tylko wydziału informatyki. Pod koniec lat 80. sieć ta łączyła ponad 175 stacji w USA, a jej europejski odpowiednik, zwany EARN (European Academic Research Network) obejmował 260 stacji. Cechą charakterystyczną sieci BITNET jest jej archaiczne oprogramowanie, które zostało przekazane twórcom sieci bezpłatnie przez IBM i było stosowane w czasach, gdy nośnikami informacji wprowadzanej do komputera były karty perforowane. Dlatego też protokoły tej sieci nie są podobne ani do protokołów OSI, ani do TCP/IP. Osobliwością tej sieci jest jej finansowanie, sprowadzające się zasadniczo tylko do opłat za dzierżawienie linii telefonicznej, za pomocą której uczelnia jest połączona z siecią.

Podstawową usługą sieci BITNET jest transfer plików, poczta elektroniczna, zdalne przetwarzanie wsadowe i w ograniczonym zakresie zdalna rejestracja w sieci. Zaawansowane są prace, mające na celu integrację sieci BITNET z sieciami ARPANET, USENET i CSNET.

Część X
Sieć SNA

Architektura sieci o nazwie SNA (Systems Network Architecture) została opracowana w firmie IBM i miała zapewnić klientom tej firmy możliwość budowy własnych, prywatnych sieci, łącznie z podsiecią komunikacyjną, której hostami byłyby komputery IBM. Ideą przewodnią tej koncepcji była próba połączenia kilku izolowanych komputerów IBM oraz wszystkich współpracujących z nimi terminali, zainstalowanych w jednym przedsiębiorstwie, w jeden spójny system. Na systemie SNA wzorowano w znacznym stopniu koncepcję modelu OSI.

Przed realizacją koncepcji SNA, firma IBM produkowała setki różnego rodzaju urządzeń, stosowanych do zdalnej komunikacji między komputerami, uwzględniających dziesiątki różnych metod zdalnego przetwarzania i różnorodne protokoły łącza transmisji danych. Idea SNA miała więc na celu opanowanie tego chaosu i stworzenie podstaw zwartej metody zdalnego przetwarzania danych, przez wyeliminowanie nie pasujących do siebie programów i protokołów.

Początki tej koncepcji sięgają roku 1974, kiedy sieć SNA posiadała strukturę drzewiastą z jednym hostem i podłączonymi do niego terminalami. Zasadniczo nie była to jeszcze sieć, ale w latach 1976 $\div$ 1985 stworzono możli-

wość łączenia ze sobą hostów na różne sposoby, dopuszczając ostatecznie do stosowania dowolne topologie hostów i sieci lokalnych.

Sieć SNA jest kolekcją komputerów, zwanych węzłami. Rozróżnia się 4 typy węzłów. Węzłami typu 1. są terminale. Rolę węzłów typu 2. pełnią komputery, sterujące pracą terminali i współpracujących z nimi urządzeń peryferyjnych. Węzłami typu 4. są tzw. komputery front-end, czyli komputery komunikacyjne, których moc obliczeniowa zaangażowana jest w realizację wszystkich funkcji, dotyczących obsługi transmisji danych. Odciążają one hosty, pełniące rolę węzłów typu 5., od tych zadań. W tym zestawie brakuje węzłów typu 3., który prawdopodobnie zarezerwowano na zapas.

Każdy węzeł posiada jeden lub więcej logicznych jednostek adresowalnych NAU (Network Adressable Unit), czyli modułów programowych, pozwalających procesom na korzystanie z sieci. Są to w istocie punkty wejściowe do sieci dla procesów użytkownika. Istnieją 3 rodzaje NAU:

- Jednostki logiczne LU (Logical Unit), czyli porty do sieci, za pomocą których użytkownik ma dostęp do zasobów sieciowych.

- Jednostki fizyczne PU (Physical Unit), rezydujące w każdym węźle. Te moduły programowe pozwalają na sterowanie łączem danych i zapewniają dostęp do różnych urządzeń fizycznych, bez precyzowania w jakim procesie te urządzenia będą użyte.

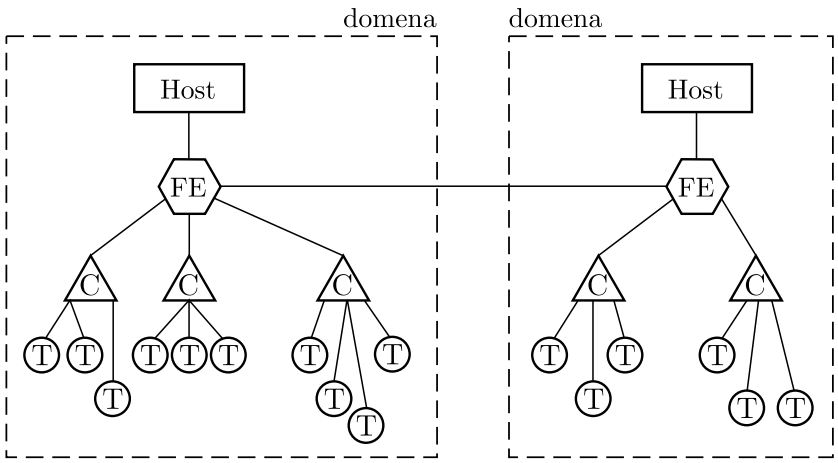
- Jednostki sterowania usługami systemowymi SSCP (System Services Control Point), instalowane tylko w hostach. SSCP musi posiadać dokładną wiedzę o wszystkich elementach sprzętowych, połączonych z hostem (komputer typu front-end oraz węzły typu 1. i 2.), ponieważ zadaniem tej jednostki jest sterowanie tym sprzętem. Sprzęt i oprogramowanie, którym steruje SSCP nazywa się domeną (rys. 2).

Warstwową strukturę logiczną sieci SNA pokazano na rys. 3. Jakkolwiek liczba warstw jest tu taka sama jak w modelu OSI, ich funkcje, poczynając od warstwy 3, znacznie różnią się od ich odpowiedników w tym modelu.

Najniższa warstwa SNA odpowiada za fizyczny transport bitów między połączonymi ze sobą komputerami, a zastosowane w niej protokoły odpowiadają ogólnie przyjętym normom.

Warstwa sterowania łączem danych, dzieli strumień bitów na ramki i realizuje procedury detekcji i korekcji błędów transmisji. Zastosowano tu protokół SDLC (Synchronous Data Link Control), który zasadniczo bez zmian przyjęty został przez ISO pod nazwą protokołu HDLC (High Level Data Link Control). Obie te warstwy są zasadniczo zgodne z modelem OSI i odpowiadają warstwom fizycznej i łącza danych w tym modelu.

Trzecia warstwa architektury SNA, zwana przez IBM warstwą sterowania ścieżką, ustanawia logiczną ścieżkę między porozumiewającymi się ze sobą jednostkami NAU. Składa się ona z trzech podwarstw. Podwarstwa

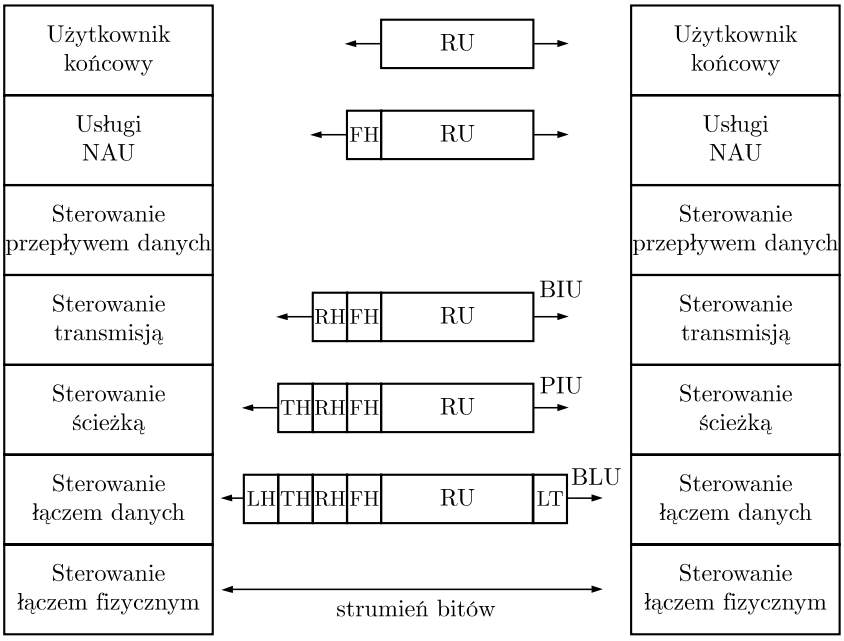


Rysunek 2: Domeny sieci SNA. FE – procesor front-end, C – węzeł typu 2., T – węzeł typu 1. (terminal)

najwyższa steruje globalnie ruchem pakietów, decydując przez jakie domeny powinny przechodzić pakiety na trasie od źródła do miejsca przeznaczenia. Podwarstwa ta dokonuje wyboru tzw. drogi wirtualnej, w odróżnieniu od podwarstwy drugiej, która decyduje o wyborze konkretnego środka komunikacji, za pomocą którego domeny mogą wymieniać dane (np. łącze satelitarne albo linia dzierżawiona od przedsiębiorstwa telekomunikacyjnego), czyli wybiera drogę absolutną. Najniższa podwarstwa tej warstwy rozdziela ruch pomiędzy kilka równoległych kanałów komunikacyjnych, dla uzyskania większej przepustowości i niezawodności.

Kolejną warstwą jest warstwa sterowania transmisją, której zadaniem jest tworzenie połączeń transportowych, używanie tych połączeń, a następnie ich kasowanie. Komunikacja w systemie SNA polega wyłącznie na stosowaniu tzw. sesji; system ten nie stosuje usług bezpołączeniowych. Zadaniem sesji jest dostarczanie warstwom wyższym niezawodnego środka wymiany danych, niezależnego od zmian technologii. Rozróżnia się tu 5 rodzajów sesji:

- SSCP – SSCP: sesja dla sterowania i obsługi wymiany wiadomości między domenami,
- SSCP – PU: sesja umożliwiająca jednostce sterowania usługami systemowymi zainicjowanie, sterowanie pracą lub zatrzymanie odpowiedniej jednostki fizycznej,
- SSCP – LU: sesja pozwalająca jednostce logicznej na zarządzanie innymi sesjami,
- LU – LU: sesja nadawania danych użytkownika,
- PU: sesja dla zarządzania siecią.



RU	- jednostka żądania/odpowiedzi
FH, RH, TH, LH	- nagłówki dodawane do RU przez kolejne warstwy
BIU	- podstawowa jednostka informacji - wiadomość (Basic Information Unit)
PIU	- jednostka informacyjna ścieżki - pakiet (Path Information Unit)
BLU	- podstawowa jednostka łącza - ramka (Basic Link Unit)

Rysunek 3: Hierarchia protokołów i wymiana danych między warstwami w sieci SNA

W modelu OSI każdy proces może wysłać wiadomość do innego procesu, żądając ustalenia połączenia sesji. Jeśli wzywany proces wyraża zgodę, wysyła zwrotnie odpowiedź, przez co połączenie między procesami jest zrealizowane. W sieci SNA sytuacja jest bardziej skomplikowana i zależy od typu sesji. Na przykład, dla sesji LU – LU, podczas której użytkownicy wymieniają dane między sobą, proces musi skontaktować się z jednostką sterowania sesją w swojej domenie. Jeśli procesy rezydują w tej samej domenie, sesja jest ustalana bezpośrednio. Jeśli jednak sesja ma być ustalana między procesami odległych domen, wówczas jednostka sterowania usługami systemowymi SSCP procesu inicjującego połączenie sesji musi powiadomić jednostkę SSCP procesu, znajdującego się w domenie odległej. Musi też zostać wybrana droga wirtualna i droga absolutna i w czasie trwania tych czynności, między komunikującymi się procesami wymienia się dziesiątki komunikatów w po-

staci wiadomości sterujących, niezbędnych przy ustalaniu połączenia sesji. Po ustaleniu sesji warstwa sterowania transmisją reguluje przepustowość łączy, steruje przydziałem buforów, ustala priorytety komunikatów, realizuje procedury szyfrowania i deszyfrowania, o ile takie usługi były wymagane, oraz wykonuje jeszcze cały szereg innych niezbędnych czynności.

Piątą warstwą jest warstwa sterowania przepływem danych, obsługująca wymianę komunikatów między procesami oraz realizująca procedury odzyskiwania danych odebranych błędnie. Osobliwością tej warstwy jest to, że do otrzymywanych do przesłania danych nie dołącza ona swojego nagłówka, lecz informację, które dane miałyby być umieszczone w nagłówku przekazuje warstwie niższej jako parametr.

Szósta warstwa architektury SNA, jest warstwą usług adresowalnych jednostek sieciowych NAU. Należy tu wymienić usługi prezentacji (np. kompresja tekstu), usługi sesji (np. ustalanie i zwalnianie połączenia) oraz usługi sieciowe, dotyczące działania sieci jako całości. Z tego bardzo pobieżnego opisu można wysnuć słuszny wniosek, że sieć SNA jest obiektem ogromnie skomplikowanym.