

IPX/SPX

Autor: Kwaśny Piotr IVFDS

STRESZCZENIE

Tematem tego projektu jest stos protokołów IPX/SPX. W kolejnych rozdziałach pracy przedstawione zostały protokoły IPX oraz SPX firmy Novell. Pierwszy rozdział dotyczy samego pojęcia protokołu a następnie przedstawiono pokrótce charakterystykę modelu warstwowego ISO/OSI oraz przeprowadzono jego porównanie z modelem IPX/SPX. Kolejne rozdziały omawiają bardziej szczegółowo protokoły IPX oraz SPX, zaczynając od przedstawienia i opisu warstw modelu IPX/SPX, przedstawiając również wady i zalety tychże protokołów, a także strukturę nagłówek, ramki oraz format adresu IPX. W dalszej części mowa jest również o zastosowaniu tych protokołów głównie w sieciach lokalnych oraz rozwój i ewolucja (IPv6) w obliczu konkurencji ze strony innych protokołów, jak się okaże bardziej elastycznych.

SPIS TREŚCI

Streszczenie.....	1
1. Pojęcie protokołu	3
2. Charakterystyka Modelu ISO/OSI.....	3
2.1 Porównanie modelu OSI z modelem IPX/SPX	4
3. Warstwy w IPX/SPX	5
4. Protokół IPX	6
4.1. Zalety i wady.....	7
4.2. Pakiety.....	7
5. Protokół SPX	7
6. Pakiety w IPX/SPX.....	8
7. IPX w praktyce	9
8. IPX/SPX – jak to działa?	10
8.1. Struktura ramki Ethernet 802.3, zawierającej nagłówki IPX/SPX	10
9. IPX/SPX a sieci rozległe.....	10
10. Rola ‘MAC’ w Adresie IPX	11
11. Rozwój IPX/SPX	11
12. Podsumowanie	12
Literatura.....	13

1. POJĘCIE PROTOKOŁU

Protokołem nazywamy formalną specyfikację formatu przesyłanych komunikatów oraz reguł, które muszą realizować komunikujące się ze sobą komputery. Pewne protokoły służą do sterowania ruchem wiadomości, inne zaś do sprawdzania poprawności przesyłanych danych, jeszcze inne przekształcają dane z jednego formatu na inny. Protokoły nie są widoczne dla użytkownika. Zadanie przesyłania wiadomości zgodnie z protokołami wykonywane jest przez komputery podłączone do sieci. Termin protokoły sieciowe odnosi się przede wszystkim do protokołów warstwy 3 modelu OSI. Zapewniają one adresowanie, dzięki któremu dane mogą być dostarczane na nieokreślone odległości, poza domenę sieci lokalnej nadawcy. Przeważnie protokoły warstwy 3 wykorzystują do transportu danych strukturę znaną jako pakiet. Choć protokoły warstwy 3 dostarczają mechanizmów niezbędnych do wysyłania pakietów, nie są na tyle wyszukane, aby mieć pewność, że pakiety zostały rzeczywiście odebrane i to we właściwym porządku. Zadania te pozostawiono protokołom transportowym warstwy 4. Protokoły te przyjmują dane z wyższych warstw i osadzają je w segmentach, które przekazują warstwie 3.

2. CHARAKTERYSTYKA MODELU ISO/OSI

Organizacja ISO (ang. International Organization for Standardization) Międzynarodowa Organizacja Normalizacyjna opracowała Model Referencyjny Połączonych Systemów Otwartych (czyli model OSI) w celu ułatwienia realizacji otwartych połączeń systemów komputerowych. Połączenia otwarte to takie, które mogą być obsługiwane w środowiskach wielosystemowych. Model referencyjny OSI dzieli procesy zachodzące podczas sesji komunikacyjnej na siedem warstw funkcjonalnych, które zorganizowane są według naturalnej sekwencji zdarzeń zachodzących podczas sesji komunikacyjnej.

Tabela 1.

Nazwa warstwy	Numer warstwy
Aplikacji	7
Prezentacji	6
Sesji	5
Transportowa	4
Sieci	3
Łączy danych	2
Fizyczna	1

- Warstwa pierwsza – fizyczna, jest odpowiedzialna za przesyłanie strumieni bitów. Odbiera ramki danych z warstw 2, czyli warstwy łącza danych, i przesyła szeregowo, bit po bicie, całą strukturę oraz zawartość.
- Warstwa druga - łącza danych, pełni funkcje nadawania i odbierania. Jest odpowiedzialna za końcową zgodność przesyłanych danych.
- Warstwa trzecia – sieci, jest odpowiedzialna za określanie trasy transmisji między komputerem nadawcy a komputerem odbiorcy.

- Warstwa czwarta – transportu, pełni funkcje podobną do funkcji warstwy łączy, w tym sensie, że jest odpowiedzialna za końcową integralność transmisji.
- Warstwa piąta – sesji, ma za zadanie zarządzanie przebiegiem komunikacji podczas połączenia między dwoma komputerami.
- Warstwa szósta – prezentacji, odpowiada za zarządzanie sposobem kodowania wszelkich danych. Nie każdy komputer korzysta z tych samych schematów kodowania danych, więc warstwa prezentacji odpowiedzialna jest za translacje między niezgodnymi schematami kodowania np. ASCII (American Standard Code for Information Interchange) i EBCDIC (Extended Binary Coded Decimal Interchange Code).
- Warstwa siódma – aplikacji, pełni rolę interfejsu pomiędzy tą aplikacją a usługami sieci.

Chociaż model ten składa się z siedmiu warstw, to określona sesja komunikacyjna nie musi wykorzystywać wszystkich siedmiu, lecz tylko niektóre z nich.

Zestaw protokołów firmy Novell bierze nazwę od swoich dwóch głównych protokołów: międzysieciowej wymiany pakietów (ang. Internet Packet Exchange) i sekwencyjnej wymiany pakietów (Sequenced Packed Exchange). Ten firmowy stos protokołów został oparty na protokole systemów sieciowych firmy Xerox (ang. Xerox's Network System), wykorzystywanym w pierwszej generacji sieci Ethernet. Wymiana IPX/SPX zyskała na znaczeniu we wczesnych latach 80. Jako integralna część systemu Novell Netware. Netware stał się faktycznym standardem sieciowego systemu operacyjnego (ang. Network Operating System) dla sieci lokalnych pierwszej generacji. Protokół IPX w dużym stopniu przypomina IP. Jest bezpołączeniowym protokołem datagramowym, który nie wymaga ani nie zapewnia potwierdzenia każdego transmitowanego pakietu. Protokół IPX polega na SPX w taki sam sposób, w jaki protokół IP polega na TCP w zakresie porządkowania kolejności i innych usług połączeniowych warstwy 4. Protokoły IPX i SPX Novella są funkcjonalnym ekwiwalentem warstw modelu OSI, odpowiednio warstw 3 i 4. [1]

2.1 Porównanie modelu OSI z modelem IPX/SPX

Tabela 2.

Nazwa warstwy modelu referencyjnego OSI	Numer warstwy OSI	Opis równoważnej warstwy IPX/SPX				
Aplikacji	7	RIP	SAP	NCP	NLSP	Różne protokoły
Prezentacji	6					
Sesji	5					
Transportu	4					
Sieci	3	Międzysieciowa wymiana pakietów				
Łącza danych	2	Interfejs otwartego łącza danych				
Fizyczna	1	Dostęp do nośnika				

3. WARSTWY W IPX/SPX

Stos protokołów IPX/SPX obejmuje cztery warstwy funkcjonalne: dostęp do nośnika, łącza danych, Internetu i aplikacji. Te cztery warstwy luźno nawiązują do siedmiu warstw modelu referencyjnego OSI, nie tracąc na funkcjonalności.

➤ Warstwa aplikacji

Warstwa aplikacji Novella obejmuje trzy warstwy - aplikacji, prezentacji i sesji - modelu OSI, choć niektóre z jej protokołów aplikacyjnych rozciągają ten stos w dół, aż do warstwy sieci. Głównym protokołem warstwy aplikacji w tym stosie jest protokół rdzenia NetWare (ang. NCP - NetWare Core Protocol). Protokół ten można bezpośrednio sprzęgać zarówno z protokołem SPX, jak i IPX. Jest wykorzystywany do drukowania, współdzielenia plików, poczty elektronicznej i dostępu do katalogów. IPX jest protokołem usługowym, realizującym transmisję. NCP jest natomiast protokołem sieci lokalnej, zaprojektowanym przy założeniu, że serwer i stacje robocze będą zlokalizowane blisko siebie. Wobec zastosowania routerów oraz wzrostu oddalenia połączeń - NCP staje się przyczyną powstawania spięrzeń w sieci. Dla zarządzania komunikacją pomiędzy serwerem a stacją korzysta on z procedury "pytanie/odpowiedź" (request/response). Kiedy stacja zgłosi jakieś żądanie (request), musi czekać na odpowiedź i dopiero potem może zgłaszać następne żądanie. Ta procedura potwierdzania generuje w sieci niepotrzebny dodatkowy ruch.

Innymi protokołami warstwy aplikacji są m.in. :

- Protokół Informacyjny Trasowania (ang. RIP Routing Information Protocol). Jest on wykorzystywany do informowania routerów o zmianach dróg routingu (transmisji) w sieci. Serwery NetWare mogą pracować także jako routery. Dla określenia optymalnych dróg routingu, RIP korzysta z algorytmów wektora odległości (DVA). W algorytmach DVA, decyzja o wyborze drogi zapada na podstawie minimalizacji liczby tzw. hop-ów (przejsć przez router), koniecznych do osiągnięcia miejsca przeznaczenia. RIP w wersji Novella dysponuje ponadto polem, gdzie zapisywana jest informacja o prędkości łącza, co pozwala na modyfikację drogi przekazu pakietów. Tabele routingu RIP wymieniane są pomiędzy routerami co 60 sekund. Na podstawie tej informacji - każdy z routerów przebudowuje własną tabelę. Problemy zaczynają się w momencie, kiedy któryś z routerów spóźnia się z modyfikacją swojej tabeli, co może mieć miejsce, kiedy jest on przyłączony za pośrednictwem zbyt wolnego łącza. Ponadto, wymiana tablic routingu może spowodować przeciążenie sieci i dalsze opóźnienie aktualizacji tabel. Po awarii jednej z dróg routingu, ustanowienie nowej drogi może przeciągnąć się do momentu odbudowania tabel routingu.
- Firmowy Protokół Ogłoszeniowy Usługi (ang. SAP Service Advertisement Protocol). Serwery i routery w sieci NetWare korzystają z protokołu SAP, aby co 60 sekund rozprowadzać informację o rodzajach realizowanych przez siebie usług. Generowany przez niego ruch bywa zbędny, jeżeli informacja dotyczy usług mało istotnych, albo dostarczana jest przez łącza rozległe do miejsc, gdzie nikt nie wykazuje nią zainteresowania. Nadmierny ruch może być zredukowany zmniejszeniem częstotliwości wysyłania komunikatów przez SAP, natomiast do wyeliminowania transmisji (komunikatów) poprzez łącza sieci rozległej dochodzi w rezultacie zastosowania specjalnych filtrów, dostarczonych przez firmę Novell.
- Protokół Obsługi Łącza systemu Netware (ang. NLSP Netware Link Services Protocol). Jest to najnowszy protokół warstwy aplikacji. Jest to protokół trasowania w zależności od stanu łącza, którym Novell zamierza zastąpić starzejące się protokoły RIP i SAP.

Protokół NLSP aktualizuje trasy tylko wtedy, gdy zaszły jakieś zmiany. Protokół ten rozwiązuje wszystkie problemy, z którymi borykały się protokoły RIP i SAP

➤ Warstwy łącza danych i dostępu do nośnika

W systemie NetWare odpowiednikami warstw fizycznej i łącza danych OSI są warstwy dostępu do nośnika i łącza danych. Warstwa łącza danych jest bezpośrednio kompatybilna ze standardem interfejsu otwartego łącza danych (ODI). Podobnie warstwa dostępu do nośnika jest bezpośrednio kompatybilna ze wszystkimi popularnymi, znormalizowanymi protokołami dostępu do nośnika. Ta niskopoziomowa zgodność z przemysłowymi standardami otwartymi sprawia, że system NetWare ze stosem protokołów IPX/SPX może być implementowany niemal wszędzie.

➤ Protokoły warstw internetu

Warstwa Internetu wymiany IPX/SPX luźno nawiązuje do warstwy sieci i transportu modelu referencyjnego OSI. IPX jest w przeważającej części protokołem warstwy 3 (sieci), choć może też być bezpośrednio sprzęgany z warstwą aplikacji. SPX jest wyłącznie protokołem warstwy 4 (transportu) i nie może być bezpośrednio sprzęgnięty z interfejsem ODI warstwy łącza danych. Musi przekazywać dane poprzez protokół IPX sprzęgnięty z ODI. IPX i SPX funkcjonują jako protokoły podwarstw we wspólnej warstwie Internetu. SPX jest protokołem połączeniowym i może być wykorzystywany do przesyłania danych między klientem serwerem, dwoma serwerami, czy nawet dwoma klientami. Tak jak w przypadku TCP, protokół SPX zapewnia niezawodność transmisjom IPX, zarządzając (administrując) połączeniem i udostępniając sterowanie strumieniem danych, kontrolę błędów i porządkowanie kolejności pakietów. [1], [2]

4. PROTOKÓŁ IPX

Protokół IPX (Internetwork Packet Exchange) został adaptowany przez firmę Novell z protokołu Xerox Network System's Internet Datagram Protocol jako protokół sieci typu peer-to-peer (równy z równym). IPX jest protokołem bezpołączeniowym lub datagramowym, który nie wymaga potwierdzenia każdego wysłanego pakietu. Potwierdzenie i kontrola połączenia muszą być realizowane przez protokoły mieszczące się nad IPX. Określenie bezpołączeniowy oznacza, że gdy aplikacja na jednej stacji używa protokołu IPX do komunikacji z drugą stacją, pomiędzy stacjami nie tworzy się potok czy też połączenie. Choć pakiety IPX są adresowane i rozsyłane do stacji docelowych, nie ma weryfikacji i gwarancji pomyślnego ich dostarczenia. Słowo datagramowy znaczy, że każdy pakiet traktowany jest jako osobna całość, nie mająca logicznej lub sekwencyjnej relacji z jakimkolwiek innym pakietem. IPX definiuje schematy adresowe międzysieciowe i wewnątrz podsieci, pozostawiając sprzętowi sieciowemu adresowanie poszczególnych węzłów. IPX wykonuje zadania tylko warstwy sieciowej modelu OSI, w tym adresowanie, routing i przekazywanie pakietów informacji z jednego miejsca w sieci do drugiego. IPX jest wbudowany, w system operacyjny NovelNetWare. NetWare jest systemem operacyjnym dla architektury klient-server i umożliwia użytkownikom (klientom) wspólny dostęp do plików, drukarek, aplikacji, faksów, usług komunikacyjnych, poczty elektronicznej. IPX jest podstawowym środkiem realizacji wymienionych usług. [1], [2]

4.1. Zalety i wady

IPX spełnia zadanie tylko warstwy sieciowej w modelu OSI, więc oferuje zysk szybkości działania. Jakkolwiek usługi IPX są niewystarczające, jeśli są wymagane gwarancje warstwy transportowej. Programiści muszą rozstrzygnąć, który z protokołów: IPX czy SPX ma zostać zastosowany w zależności od indywidualnego problemu. Rozważyć można następujące wady i zalety:

- Jednoczesna dostępność nadajnika i odbiornika nie jest wymagana, ponieważ nie istnieje ściśle określone połączenie. Jednak nadajnik nie otrzymuje weryfikacji ani gwarancji dostarczenia wysłanego pakietu.
- Elastyczność w przekazywaniu (routing) pakietów jest większa, gdyż nie jest konieczne wstępne określenie trasy przekazu. Wadę stanowi fakt, że pakiety mogą docierać w przypadkowej kolejności.
- Pakiety mogą być wysyłane do wielu miejsc za pomocą powielania pakietów i zmiany adresu docelowego. [2]

4.2. Pakiety

Pakiem jest zbiór bitów, w którym można wyróżnić przesyłane dane ("ładunek"-payload) o rozmiarze od 0 do 546 bajtów oraz informacje nagłówkowe ("pilot") o 30 bajtowym rozmiarze. Zatem minimalna długość pakietu wynosi 30 bajtów, a maksymalna 576 bajtów. W nagłówku zapisane są adresy miejsca nadania i miejsca przeznaczenia przesyłki, a także informacje kontrolne, pozwalające na wykrycie błędów oraz utrzymanie właściwej kolejności pakietów. Pakiety przesyłane są do miejsca przeznaczenia, poprzez kanały komunikacyjne (jako strumień bitów). Każdy pakiet jest oddzielnym blokiem danych i ogólnie rzecz biorąc, może mieć inny adres niż pozostałe pakiety, przesyłane w danym momencie przez sieć. Dane w pakiecie mogą zawierać sformułowane przez klienta żądanie dostępu do usługi, albo odpowiedź od serwera. Danymi mogą być również informacje tekstowe, przesyłane pomiędzy systemami. Typowy pakiet ma rozmiar od 512 do 6500 bajtów, tak więc - przesłanie dużego pliku może oznaczać wykorzystanie wielu pakietów. Mimo to skuteczność dostarczania pakietów za pomocą IPX ocenia się na ok. 95%

5. PROTOKÓŁ SPX

W odróżnieniu od IPX, jego siostrzany protokół - SPX (Sequenced Packet Exchange) jest protokołem połączeniowym, lokującym się w warstwie transportowej modelu OSI. Połączeniowość protokołu oznacza, że dla potrzeb przeprowadzenia transmisji pomiędzy dwoma urządzeniami ustanawiana jest tzw. sesja, co pozwala kontrolować przepływ pakietu. Cecha połączeniowości protokołu SPX powoduje wprawdzie, że na ustanowienie sesji zużywa się trochę czasu, ale daje za to gwarancje poprawnego przekazu danych wrażliwych na opóźnienie. Ponadto, pakiety są w tym przypadku mniejsze, gdyż nie jest potrzebne pełne adresowanie. Przekaz bezpołączeniowy jest szybki i efektywny, ale pakiety są większe, gdyż - aby dotarły na miejsce przeznaczenia, muszą zawierać pełny adres.

W większości przypadków, w powodujących stosunkowo niewiele błędów sieciach lokalnych preferuje się stosowanie metod bezpołączeniowych. Okazują się one być bardziej efektywne i szybsze przy przekazywaniu danych, jakie na ogół są wymieniane poprzez sieć. Dane te transmitowane są zwykle w nieregularnych fragmentach i byłoby niecelowe dla każdego z tych fragmentów nawiązywać oddzielną sesję. Inaczej jest w przypadku zdalnej konsoli (Remote Console) w systemie NetWare; tutaj preferuje się technikę połączeniową. W tym przypadku

ustanawia się, za pomocą protokołu SPX, względnie stale połączenie pomiędzy stacją zarządcy a serwerem, co pozwala na ciągłą kontrolę stanu serwera w czasie rzeczywistym. Zastosowanie SPX jest tu celowe, gdyż pakiety przekazywane są regularnie, a połączenie jest stale wykorzystywane. [1], [2]

6. PAKIETY W IPX/SPX

Nagłówek SPX ma następujący rozmiar i strukturę:

- Sterowanie połączeniem: Pierwszy oktet (8 bitów) nagłówka SPX zawiera cztery 2-bitowe flagi, sterujące dwukierunkowym przepływem danych przez połączenie SPX.
- Typ strumienia danych: Następnym osiem bitów nagłówka definiuje typ strumienia danych.
- Identyfikacja połączenia źródłowego: 16-bitowe pole identyfikacji połączenia źródłowego identyfikuje proces odpowiedzialny za inicjowanie połączenia.
- Identyfikacja połączenia docelowego: 16-bitowe pole identyfikacji połączenia docelowego służy do identyfikowania procesu, który zaakceptował żądanie (zgłoszenie) połączenia SPX.
- Numer sekwencji: 16-bitowe pole numeru sekwencji dostarcza protokołowi SPX hosta docelowego informację o liczbie wysłanych pakietów. To sekwencyjne numerowanie może być wykorzystywane do zmiany kolejności odebranych pakietów, gdyby przybyły w niewłaściwej kolejności.
- Numer potwierdzenia: 16-bitowe pole numeru potwierdzenia wskazuje następny oczekiwany segment.
- Liczba alokacji: 16-bitowe pole liczby alokacji jest wykorzystywane do śledzenia liczby pakietów wysłanych, ale nie potwierdzonych przez odbiorcę.
- Dane: Ostatnie pole nagłówka SPX zawiera dane. W jednym pakiecie SPX można przesłać do 534 oktetów danych.

Protokołem warstwy sieci dla sieci Novell jest IPX. Protokół ten zapewnia bezpołączeniowe usługi dostarczania datagramów. Przygotowuje pakiety protokołu SPX (lub pakiety innych protokołów) do dostarczenia przez wiele sieci, dołączając do nich nagłówki IPX. W ten sposób powstaje struktura zwana datagramem IPX. Nagłówek tego datagramu zawiera wszystkie informacje niezbędne do skierowania pakietów do miejsca przeznaczenia, niezależnie od tego, gdzie mogłoby się ono znajdować.

Długość nagłówka IPX wynosi 11 oktetów. Jego struktura obejmuje następujące pola:

- Suma kontrolna: Nagłówek IPX zaczyna się do 16-bitowego pola dziedziczenia, które istnieje tylko po to, aby zapewnić kompatybilność wsteczną z protokołem XNS. Protokół XNS wykorzystywał to pole do kontrolowania błędów, ale IPX domyślnie ustawia to pole na FFFFH, a wykrywanie (i korekcję) błędów transmisji pozostawia protokołom wyższego poziomu.

- Długość pakietu: 16-bitowe pole określające długość datagramu IPX, wliczając nagłówek i dane. Pole to jest sprawdzane w celu weryfikacji integralności pakietu.
- Sterowanie transportem: 8-bitowe pole wykorzystywane przez routery podczas przesyłania datagramu. Przed wysłaniem IPX ustawia to pole na "0". Każdy router, który odbiera i przesyła dalej datagram, zwiększa wartość pola o jeden.
- Typ pakietu: 8-bitowe pole identyfikujące typ pakietu zawartego w datagramie IPX. Pole to umożliwia hostowi docelowemu przekazanie zawartości do następnej, odpowiedniej warstwy protokołów. Typy mogą obejmować RIP, NCP, SPX, błąd itd.
- Numer sieci docelowej: 32-bitowe pole określające numer sieci, w której znajduje się węzeł docelowy.
- Węzeł docelowy: 48-bitowe pole zawierające numer węzła, w którym znajduje się komputer docelowy.
- Numer gniazda docelowego: Ponieważ IPX umożliwia wiele jednoczesnych połączeń z jednym systemem, istotne jest określenie numeru gniazda procesu lub programu odbierającego pakiety. Informacji takiej dostarcza to 16-bitowe pole.
- Numer sieci źródłowej: 32-bitowe pole określające numer sieci, w której znajduje się węzeł źródłowy.
- Adres węzła źródłowego: 48-bitowe pole zawierające numer węzła, w którym znajduje się komputer źródłowy.
- Numer gniazda źródłowego: 16-bitowe pole, określające numer gniazda procesu lub programu wysyłającego pakiety. [1]

7. IPX W PRAKTYCE

IPX jest wbudowany w system operacyjny NetWare, toteż stacja robocza, aby komunikować się z serwerem, wymaga jedynie zainstalowania protokołu i uruchomienie klienta. IPX nie jest raczej używany w środowiskach innych niż NetWare, wywołując jednak zainteresowanie jako sposób na dostęp do internetu. Obsługa IPX instalowana jest na stacji roboczej, razem z oprogramowaniem requestera (analizatora poleceń), jak np. DOS Requester czy OS/2 Requester. Aktualna wersja oprogramowania zawiera interfejs ODI-Open Data Link Interface firmy Novell, który pozwala na jednoczesne ładowanie wielu warstw protokołów, jak IPX i TCP/IP. Oprogramowanie requestera jest dyspozytorem (redirection utility) poleceń użytkownika; analizuje je i przesyła - albo do lokalnego systemu operacyjnego, albo do innego systemu w sieci. W przypadku, gdy polecenie odnosi się do sieci - oprogramowanie requestera pakietuje polecenie - jako pakiet IPX i udostępnia karcie sieciowej, która z kolei "wpuszcza" pakiet do sieci, jako strumień bitów. Miejsc przeznaczenia może być wiele:

- Serwer w tym samym segmencie sieci lokalnej (LAN)
- Stacja robocza w tym samym segmencie sieci lokalnej
- Stacja robocza lub serwer w innym segmencie sieci

Nagłówek pakietu zawiera adres segmentu sieci lokalnej - miejsce przeznaczenia pakietu. Podczas przechodzenia przez sieć, informacja ta odczytywana jest przez router, który kieruje potem

pakiet do właściwego segmentu. [2]

8. IPX/SPX – JAK TO DZIAŁA?

Protokół SPX tworzy i utrzymuje połączeniowy strumień bitów między dwoma przyłączonymi do sieci urządzeniami. Protokół przyjmuje duże bloki danych z protokołów wyższych warstw i dzieli je na łatwiejsze w kierowaniu kawałki, nie przekraczające długości 534 oktetów. Do danych dołączany jest nagłówek SPX i w ten sposób powstają segmenty danych SPX. Segmenty przekazywane są protokołowi warstwy internetu, czyli protokołowi IPX. IPX umieszcza segmenty w polu danych swoich pakietów i wypełnia wszystkie pola nagłówka IPX. Pola nagłówka IPX obejmują adresowanie sieci, długość, sumę kontrolną i inne informacje nagłówkowe. Następnie pakiet przekazywany jest warstwie łącza danych.

8.1. Struktura ramki Ethernet 802.3, zawierającej nagłówki IPX/SPX

Tabela 3.

7 - oktetowa Preambuła	1 - oktetowy Ogranicznik początku ramki	6 - oktetowy Adres odbiorcy	6 - oktetowy Adres nadawcy	2 - oktetowe pole Długości	30 - oktetowy nagłówek IPX	Nagłówek SPX o zmiennej długości	Pole Dane o zmiennej długości od 46 do 1482 oktetów	4 - oktetowa Sekwencja kontrolna ramki
------------------------	---	-----------------------------	----------------------------	----------------------------	----------------------------	----------------------------------	---	--

Komputer docelowy odwraca opisane wyżej działania. Odbiera pakiety i przekazuje je własnemu protokołowi SPX do ponownego złożenia. Jeśli to konieczne, pakiety są ponownie grupowane w segmenty danych, przekazywane odpowiedniej aplikacji. [1]

9. IPX/SPX A SIECI ROZLEGŁE

W przeszłości - system Novell NetWare, wraz z protokołem IPX - nie były najlepszymi środkami do realizacji sieci rozległych, co wynikało z nieefektywności zarówno systemu operacyjnego, jak i protokołu. Braki te wyglądały następująco z uwzględnieniem korekt, wprowadzonych przez firmę Novell w protokole IPX.

- Tryb burst - monopolizujący. Konieczność potwierdzania odbioru pakietów IPX może doprowadzić do tzw. efektu "pingpongowego", czyli wysyłania potwierdzenia po każdym nadanym pakiecie, co prowadzi do obniżenia wydolności sieci rozległej. W unowocześnionym trybie pracy IPX - burst mode - potwierdzenie przesyłane jest po odebraniu max. 128 pakietów. Pozwala to zwiększyć przepustowość sieci nawet o 50%. Z drugiej strony, przy pracy wieloprotokołowej, taki tryb pracy może być przyczyną zablokowania ruchu innych protokołów. IPX może zmonopolizować router, wówczas

ruch (generowany przez TCP/IP) zostaje wstrzymany do momentu przerwy. Istnieją routery umożliwiające nadanie priorytetu określonej rodzajowi ruchu.

- Ramki o dużym rozmiarze - Początkowo, aby uniknąć spiętrzeń - dane przechodzące przez router dzielone były na pakiety 512 - bajtowe. Oprogramowanie firmy Novell umożliwia przesyłanie przez router dużych pakietów, co pozwala poprawić wymianę pakietów w sieci. Rozmiar pakietu negocjowany jest podczas nawiązywania połączenia. [2]

10. ROLA 'MAC' W ADRESIE IPX

Adresy IPX mają długość 10 oktetów (80 bitów). Jest to znacznie więcej niż 32 bity adresu IPv4, ale mniej niż 128 bitów adresu IPv6. Każdy adres składa się z dwóch części składowych: numeru sieci o maksymalnej długości 32 bitów oraz 48-bitowego numeru węzła. Numery te są wyrażane w notacji kropkowo-szesnastkowej. Na przykład, 1a2b.0000.3c4d.5e6d mogłoby być prawidłowym adresem IPX, w którym "1a2b" reprezentuje numer sieci, a "0000.3c4d.5e.6d" jest numerem węzła. Adresy IPX mogą być tworzone przez administratora sieci. Jednak tak utworzone po znalezieniu się w sieci mogą spowodować pojawienie się konfliktów adresów. Wymyślanie numerów sieci obciąża administratora obowiązkiem ich utrzymania i administrowania nimi. Lepszym rozwiązaniem jest więc pozyskanie zarejestrowanych adresów sieci IPX Novell. Jako numer hosta IPX wykorzystuje się zwykle powszechnie przypisywany adres (adres MAC) karty sieciowej (NIC). Ponieważ adresy te są unikatowe, przynajmniej w teorii i w stopniu zależnym od zapewnienia jakości przez producenta, oferują wygodną i unikatową numerację hostów. Podobnie jak IP, protokół IPX może obsługiwać wiele jednoczesnych sesji. Stwarza to potrzebę identyfikowania określonego procesu lub programu, który bierze udział w danej sesji. Identyfikację osiąga się dzięki stosowaniu 16-bitowego numeru "gniazda" w nagłówku IPX. Numer gniazda jest analogiczny do numeru portu w protokole TCP/IP. [1]

11. ROZWÓJ IPX/SPX

Następcą protokołu IPX jest NetWare Link Services Protocol - NLSP. Jego zastosowanie poprawia parametry sieci, dzięki zastąpieniu protokołów SAP oraz RIP - algorytmem routingu adaptacyjnego (link-state). Metody routingu adaptacyjnego umożliwiają lepsze sterowanie procesem routingu i szybciej reagują --zestawieniem innej drogi transportu - na uszkodzenie łącza. Decyzja o wyborze drogi może być podejmowana na podstawie danych o obciążeniu poszczególnych łączy, prędkości linii, kosztach przekazu itp. NLSP korzysta z protokołów Open Shortest Path First (otwieraj najpierw krótszą ścieżkę) albo IS-IS (system pośredniczący do systemu pośredniczącego). Novell unowocześnił także protokół SPX - poprzez wprowadzenie zmiennej wielkości ramki (sliding windows), trybu monopolizującego (burst mode) oraz obsługi dużych pakietów. Ponadto, dostępna jest nowa powłoka stacji roboczej (workstation shell), wyszukująca w sieci alternatywną drogę w momencie uszkodzenia dotychczasowej. [1], [2]

12. PODSUMOWANIE

Firma Novell Inc. zaobserwowała, jak pozycja rynkowa będącego jej własnością stosu protokołów IPX/SPX słabnie pod naporem konkurencji. Gdy dostępne stały się stosy protokołów otwartych, takich jak OSI, IP i inne, pozycja IPX/SPX bardzo na tym ucierpiała. Dostępne w handlu pakiety oprogramowania wspomagającego prace biurowe również wpłynęły na sprzedaż produktów firmy Novell. Będąc jej własnością, ściśle połączone ze sobą serie produktów zapewniły początkowy sukces, ale stały się ciężarem w warunkach rynku ceniącego otwartość i współoperacyjność. Novell zademonstrował swoje zaangażowanie w staraniach o odzyskanie utraconej pozycji, czyniąc IPv6 domyślnym protokołem przyszłych wersji systemu NetWare. Aby pomyślnie wprowadzić tę zmianę strategii, Novell musi zapewnić kompatybilność między protokołami IPv6 i IPX/SPX. By osiągnąć ten cel, Novell blisko współpracował z grupą roboczą ds. Technicznych Internetu podczas projektowania IPv6. Dzięki temu wiele usług IPX stało się integralną częścią IPv6. Przygotowawszy grunt pod przyszłość, Novell musi teraz umożliwić bezbolesną migrację obecnego stosu protokołów i zestawu aplikacji do nowego środowiska. Co więcej, powinien także dostarczyć produkty i usługi podnoszące wartość wykorzystywania platformy sieciowej otwartej. Dla firmy Novell wizją na przyszłość jest dostarczenie usługi katalogów sieciowych (ang. NDS - Network Directory Service) i powiązanych produktów dla dwóch grup użytkowników: środowiska internetu i korporacyjnych internetów. Usługa NDS oferuje jeden, globalny, logiczny widok na wszystkie usługi i zasoby sieciowe. Umożliwia to użytkownikom dostęp do tych usług i zasobów po wykonaniu pojedynczego logowania, niezależnie od lokalizacji użytkownika czy zasobów. [1], [2]

LITERATURA

- [1] Mark Sportack „Sieci Komputerowe Księga Eksperta” Wydawnictwo Helion, Gliwice 1999
- [2] Kelly J.P. Lindberg „Novell Netware5 Podręcznik Administratora“ Wydawnictwo PLJ, Warszawa 1999