informatyka+

Algorytmika i programowanie

Bazy danych

Multimedia, grafika i technologie internetowe

Sieci komputerowe

Tendencje w rozwoju informatyki i jej zastosowań

Człowiek – najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

informatyka+

Kuźnia Talentów: Sieci komputerowe

Zarządzanie sieciami WAN

Dariusz Chaładyniak

Józef Wacnik

Człowiek – najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Zarządzanie sieciami WAN

Rodzaj zajęć: Kuźnia Talentów
Tytuł: Zarządzanie sieciami WAN
Autor: dr inż. Dariusz Chaładyniak, mgr inż. Józef Wacnik

Redaktor merytoryczny: prof. dr hab. Maciej M Sysło

Zeszyt dydaktyczny opracowany w ramach projektu edukacyjnego **Informatyka+** — ponadregionalny program rozwijania kompetencji uczniów szkół ponadgimnazjalnych w zakresie technologii informacyjno-komunikacyjnych (ICT).
www.informatykaplus.edu.pl
kontakt@informatykaplus.edu.pl

Wydawca: Warszawska Wyższa Szkoła Informatyki
ul. Lewartowskiego 17, 00-169 Warszawa
www.wwsi.edu.pl
rektorat@wwsi.edu.pl

Projekt graficzny: FRYCZ I WICHA

Warszawa 2010

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Zarządzanie sieciami WAN

Dariusz Chaładyniak
Warszawska Wyższa Szkoła Informatyki
dchalad@wwsi.edu.pl

Józef Wacnik
Warszawska Wyższa Szkoła Informatyki
j_wacnik@poczta.wwsi.edu.plx

Streszczenie

Wraz ze wzrostem działalności związanej z przesyłaniem informacji oraz zwiększaniem się ilości usług sieciowych, konieczna stała się komunikacja pomiędzy sieciami odległymi od siebie i korzystającymi z różnych protokołów. Wykład przedstawia wybrane technologie spotykane w sieciach rozległych. Wyjaśnia ich budowę, działanie oraz zastosowanie. Skupiono się głównie na technologiach mających najistotniejsze znaczenie w transmisji danych we współczesnych sieciach teleinformatycznych (PSTN, ISDN, xDSL, ATM, Frame Relay). Wykład omawia ponadto trzy wybrane usługi sieciowe, których zrozumienie opiera się na podstawowej wiedzy związanej z adresowaniem IP. Aby móc skorzystać z dowolnych zasobów WWW musimy mieć publiczny adres IP, który może być współdzielony przez wiele komputerów z zastosowaniem translacji NAT (statycznej lub dynamicznej) lub translacji z przeciążeniem PAT. Adres IP dla naszego komputera może być przypisany ręcznie lub przydzielony dynamicznie poprzez usługę DHCP. Aby przeglądarka internetowa właściwe zinterpretowała adres domenowy musi być dostępna usługa odwzorowująca ten adres na adres IP zrozumiały dla oprogramowania sieciowego.

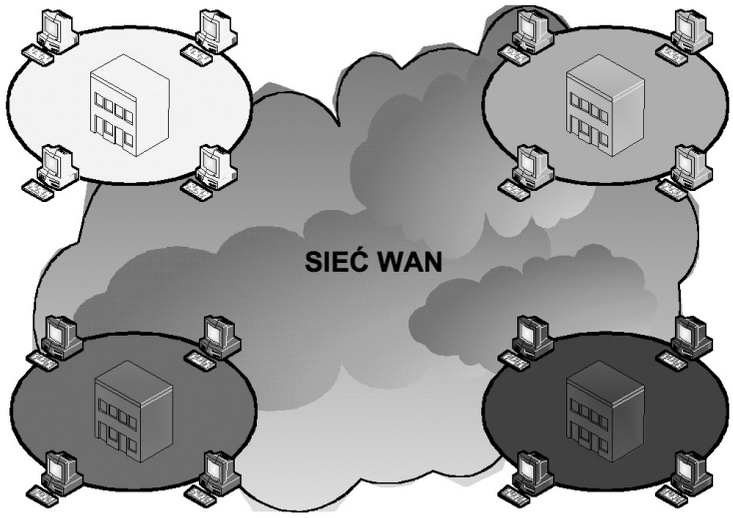
Warsztaty będą okazją do praktycznego przećwiczenia materiału z wykładu.

Spis treści

Warsztaty

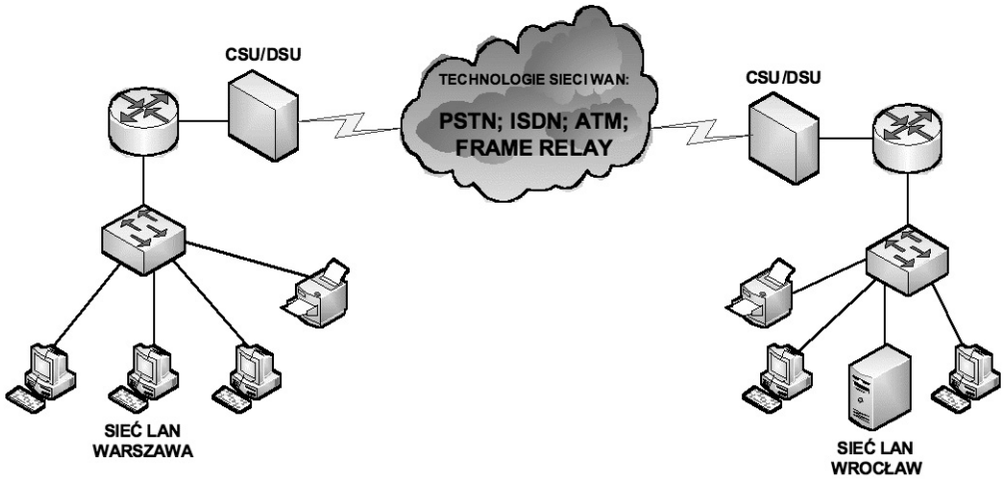
1 TECHNOLOGIE W SIECIACH ROZLEGŁYCH

Sieć **rozległa WAN** (ang. *Wide Area Network*) jest to sieć o zasięgu globalnym. Łączy ona sieci w obrębie dużych obszarów, obejmujących miasta, kraje a nawet kontynenty.



Rysunek 1.
Przykład sieci WAN

Sieci WAN są grupami sieci LAN połączonych łączami komunikacyjnymi udostępnianymi przez dostawcę usług. Ponieważ jednak łączy komunikacyjnych nie można podłączać bezpośrednio do sieci LAN, konieczne jest użycie różnych urządzeń pełniących rolę interfejsów (patrz rys. 2).



Rysunek 2.
Przykład połączenia dwóch sieci LAN za pomocą infrastruktury sieci WAN

Komputery w sieci LAN przesyłają dane do routera, który jest wyposażony zarówno w interfejs LAN, jak i WAN. Router ten na podstawie adresu warstwy sieci dostarcza dane do określonego interfejsu WAN. Dzięki temu, że routery są aktywnymi i inteligentnymi urządzeniami sieciowymi, mogą aktywnie uczestniczyć w zarządzaniu siecią. Routery zarządzają sieciami poprzez dynamiczne sterowanie zasobami i wspomaganie realizacji celów stawianych sieciom. Niektóre z tych celów to zapewnienie łączności, niezawodność, wydajność, możliwość zarządzania i elastyczność.

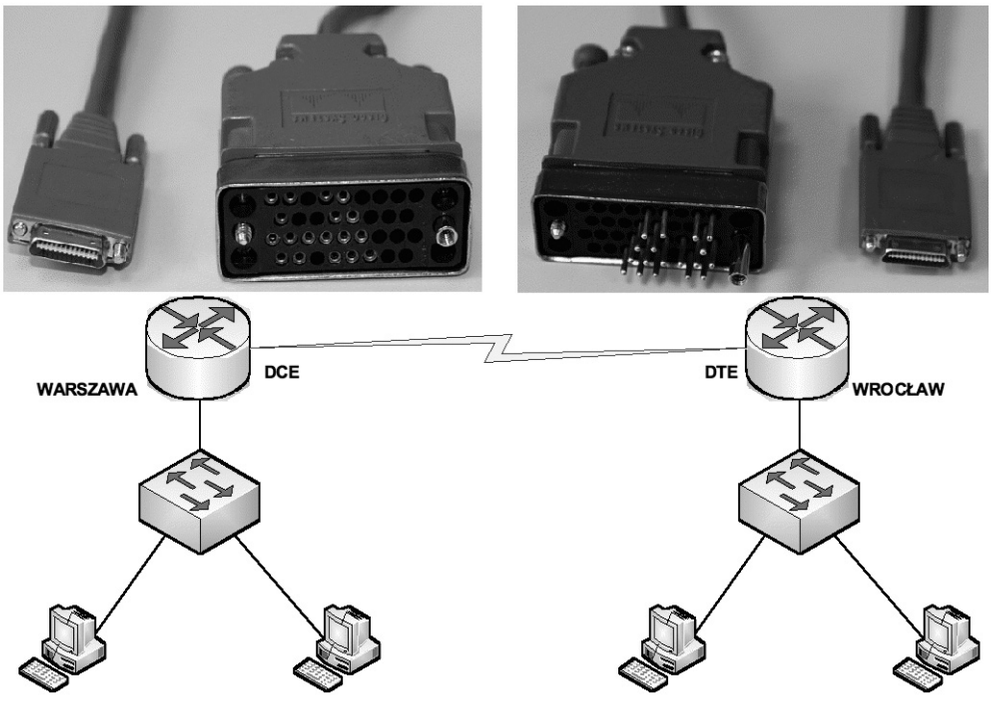
Linia komunikacyjna wymaga, aby sygnały były przesyłane w odpowiednim formacie. W przypadku linii cyfrowych potrzebna jest jednostka obsługi kanału **CSU** (ang. *Channel Service Unit*) i jednostka obsługi danych **DSU** (ang. *Data Service Unit*). Często stanowią one jedno urządzenie CSU/DSU. Urządzenie CSU/DSU może także być wbudowane w kartę interfejsu routera.

Jeśli używana jest pętla lokalna analogowa, a nie cyfrowa, potrzebny jest modem. Modemy przesyłają dane przez głosowe linie telefoniczne, stosując technikę modulacji i demodulacji sygnału. Sygnały cyfrowe nakłada się na sygnał analogowy modulowany w celu przesłania go po łączu. Po włączeniu głośnika modemu można usłyszeć zmodulowany sygnał, który przypomina serię pisków. U celu sygnały analogowe są demodulowane, czyli przekształcane ponownie na postać cyfrową.

Jeśli używana jest linia komunikacyjna ISDN, sprzęt do niej podłączony musi być zgodny z tym standardem. Zgodność tę zapewnia interfejs komputera (w przypadku bezpośrednich połączeń dodzwanianych) lub interfejs routera (w przypadku połączeń między sieciami LAN i WAN).

Połączenia w sieciach WAN

Sieci WAN korzystają z wielu różnych technologii do realizowania połączeń danych na dużych obszarach geograficznych. Usługi komunikacji WAN są zazwyczaj dzierżawione od dostawców usług. Typy połączeń WAN obejmują linie dzierżawione, połączenia z komutacją łączy oraz połączenia z komutacją pakietów. Dla każdego typu usługi **WAN CPE** (ang. *Customer Premises Equipment* – urządzenie końcowe użytkownika), stanowi urządzenie DTE. Ono z kolei jest połączone z dostawcą usług za pomocą urządzenia DCE, które jest zwykle modemem lub jednostką CSU/DSU. Urządzenie to służy do konwersji danych z urządzenia DTE do postaci akceptowanej przez dostawcę usług WAN.



Rysunek 3.
Przykład połączeń WAN w warunkach laboratoryjnych

W laboratorium wszystkie sieci będą połączone kablami szeregowymi (patrz rys. 3) lub Ethernet. W przeciwieństwie do instalacji w laboratorium, w rzeczywistości kable szeregowe nie łączą urządzeń bezpośrednio ze sobą. W rzeczywistości jeden router może znajdować się w Warszawie, podczas gdy inny może znajdować się we Wrocławiu.

Popularne standardy WAN warstwy fizycznej

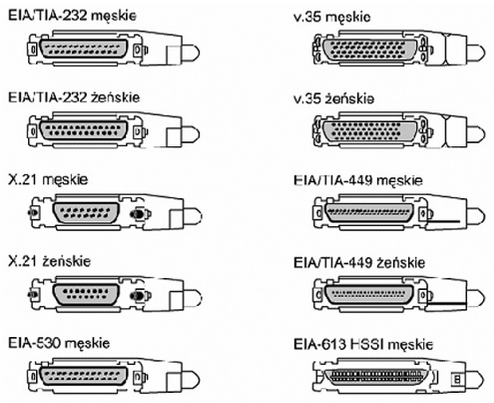
EIA/TIA-232 – umożliwia połączenia z szybkością do 64 kbps. Używa 25-pinowe złącze typu D.

EIA/TIA-449/530 – umożliwia połączenia do 2 Mbps. Używa 36-pinowe złącze typu D.

EIA/TIA-612/613 – zapewnia dostęp do usług z szybkością do 52 Mbps przez interfejs **HSSI** (ang. *High Speed Serial Interface*). Używa 60-pinowe złącze typu D.

V.35 – standard ITU-T dla synchronicznej komunikacji z szybkością od 48 kbps do 2 Mbps. Używa 34-pinowe złącze prostokątne.

X.21 – standard ITU-T dla synchronicznej komunikacji cyfrowej. Używa 15-pinowe złącze typu D.

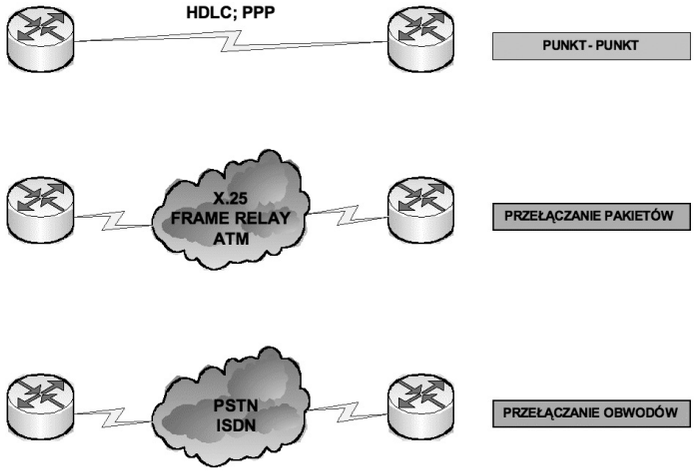


Rysunek 4.
Przykłady złączy stosowanych w sieciach WAN

Popularne standardy WAN warstwy łącza danych

Dane warstwy sieci są enkapsulowane w ramki w warstwie łącza danych. Konkretny typ enkapsulacji zależy od typu stosowanej na łączu technologii i trzeba go skonfigurować na interfejsie szeregowym. Istnieją trzy rodzaje połączeń w sieciach rozległych (patrz rys. 5):

1. Połączenie punkt-punkt (np. protokół HDLC, protokół PPP);
2. Przełączanie pakietów (np. technologia X.25, technologia Frame Relay, technologia ATM);
3. Przełączanie obwodów (np. technologia PSTN, technologia ISDN).



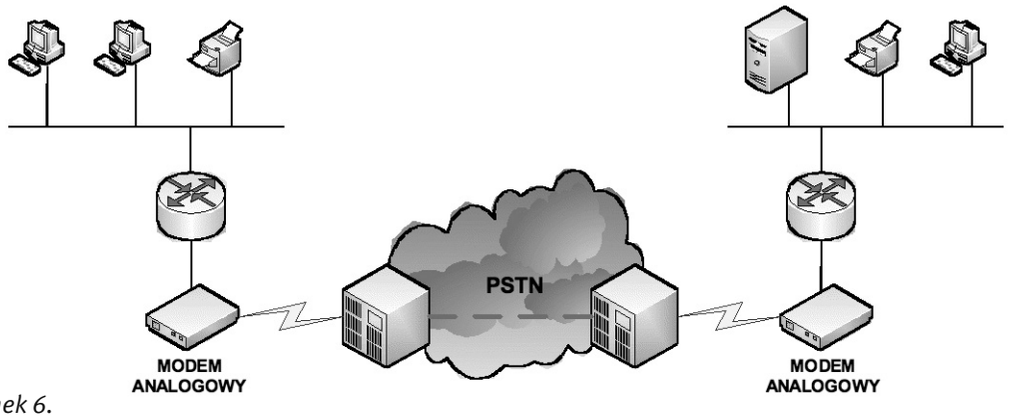
Rysunek 5.
Przykłady połączeń w sieciach WAN

2 TECHNOLOGIA PSTN

Publiczna sieć telefoniczna PSTN

Najstarsza, nadal jeszcze funkcjonująca infrastruktura telekomunikacyjna o charakterze publicznym **PSTN** (ang. *Public Switched Telephone Network*) jest oparta na komutacji łączy (linii telefonicznych), patrz rys. 6. Podstawowa oferta usług w sieci PSTN, a obejmująca tylko automatyczną komutację kanałów rozmównych, jest stopniowo powiększana o usługi rozszerzone i dodatkowe – związane z wprowadzaniem bardziej inteligentnych cyfrowych systemów komutacji. Należą do nich:

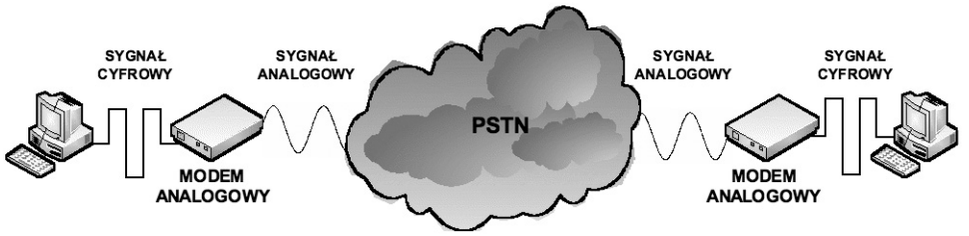
- usługi podstawowe (zestawianie połączeń za pomocą aparatów z tarczą cyfrową lub tonową, restrykcje zestawień, taryfikacja);
- usługi rozszerzone (rozmowy trójstronne, telekonferencje, przekierowanie rozmów, gorąca linia);
- usługi dodatkowe (poczta głosowa, poczta elektroniczna, usługi ISDN).



Rysunek 6.
Wykorzystanie publicznej sieci telefonicznej do przesyłu danych w postaci analogowej w sieciach WAN

Usługi podstawowe związane z transmisją głosu, funkcjonujące od czasu udostępnienia sieci publicznej głównie w centralach analogowych, nazwano usługami **POTS** (ang. *Plain Old Telephone Services*). Transmisje oparte na komutacji pakietów przeprowadza się w publicznych sieciach pakietowych **PDN** (ang. *Packet Data Network*).

Modem analogowy



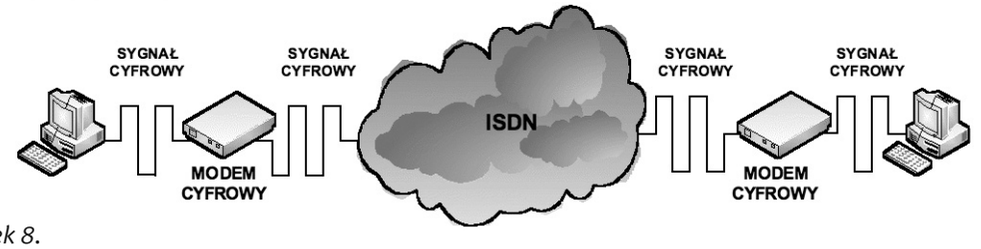
Rysunek 7.
Przykład zastosowania modemu analogowego

Modem to skrót od słów **MO**dulacja **DEM**odulacja. Jest to urządzenie służące do transmisji danych przez zwykłą linię telefoniczną (patrz rys. 7). Informacje przetwarzane przez komputer mają postać cyfrową (bity), podczas gdy przez linię telefoniczną są przesyłane dane analogowe. Modem jest specyficznym konwerterem, który zamienia sygnały cyfrowe na analogowe (modulacja) i analogowe na cyfrowe (demodulacja). Sygnał analogowy jest przesyłany przez linię telefoniczną dysponującą pasmem przenoszenia o szerokości 3 kHz. Dane mogą być transmitowane w obie strony jednocześnie (pełny dupleks) lub naprzemiennie (półdupleks).

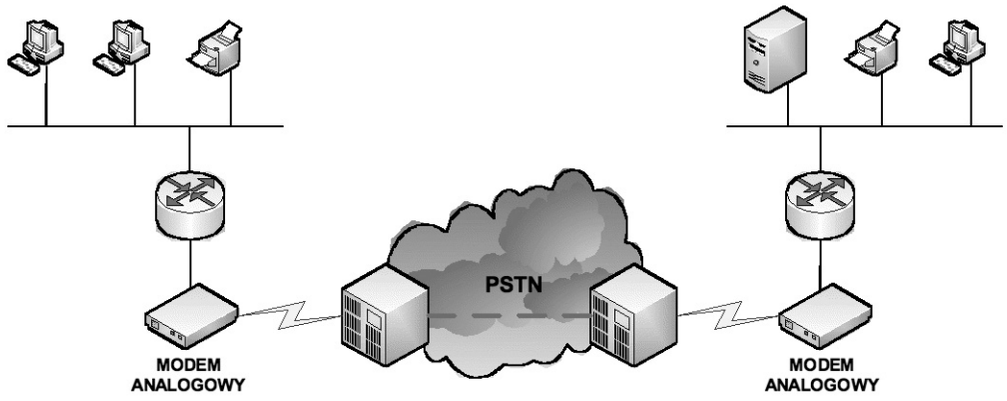
Szybkość pracy modemów jest podawana w **bodach** (ang. *baud*). Bod to liczba zmian sygnału, jaką modem może wygenerować w ciągu określonego czasu (np. jednej sekundy). Jeśli stan linii może się zmienić w czasie jednej sekundy (z logicznego „0" na „1" i odwrotnie) sto razy, to urządzenie może pracować z szybkością 100 bodów.

Szybkość pracy modemu i szybkość transmisji danych (która jest zdefiniowana w bitach na sekundę) to dwie różne sprawy. Chodzi o to, że modem może wyekspediować w sieć w momencie zmiany sygnału z jednego stanu logicznego na drugi więcej niż jeden bit. I tak modem pracujący z szybkością 1200 bodów może np. (zależnie od zastosowanej technologii) transmitować dane z szybkością 14400 bitów na sekundę.

3 TECHNOLOGIA ISDN



Rysunek 8.
Przykład zastosowania modemu cyfrowego



Rysunek 9.
Wykorzystanie publicznej sieci telefonicznej do przesyłu danych w postaci cyfrowej w sieciach WAN

Sieci ISDN, stosowane początkowo w prywatnych, a następnie publicznych cyfrowych sieciach telekomunikacyjnych, umożliwiają nie tylko przekaz głosu, tekstu, grafiki i obrazów ruchomych, ale mają zdolność współpracy zarówno z sieciami komputerowymi LAN, jak i z różnymi typami sieci rozległych. Wyróżnia się trzy czynniki leżące u podstaw rozwoju sieci cyfrowej z integracją usług ISDN, odróżniające je od tradycyjnych sieci analogowych:

- opanowanie techniki przekazu cyfrowego na wszystkich etapach łączności od abonenta (telefony, telefaksy, terminale, komputery, przełącznice, krotnice) do cyfrowej centrali abonenckiej i systemu komutacyjnego włącznie (patrz rys. 9);
- wzrost zainteresowania abonentów usługami niefonicznymi (przekazy cyfrowe, dostęp do baz danych, grafika, obrazy ruchome), wymagającymi połączeń z sieciami LAN o znacznie wyższych przepływnościach, praktycznie niedostępnych przez łącza analogowe (znacznie powyżej 100 Kb/s);
- wykorzystanie istniejącej miedzianej infrastruktury okablowania na najniższym poziomie w otoczeniu abonenta, bez ponoszenia wydatków na wymianę lokalnych instalacji, co w istotny sposób wpływa na obniżenie kosztów wdrażania techniki ISDN.

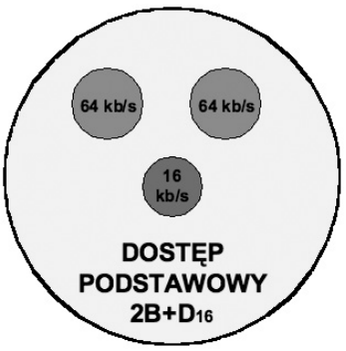
Podstawowe cechy ISDN

Podstawowe cechy technologii ISDN:

- przekaz cyfrowy z gwarantowaną przepływnością 64 kb/s bez względu na odległość dzielącą abonentów, z możliwością zastosowania dwóch kanałów typu B udostępniających gwarantowaną przepływność 128 kb/s;
- krótki czas zestawiania połączeń i możliwość ich likwidacji natychmiast po zrealizowaniu sesji komunikacyjnej;
- szeroki zakres usług z równoczesnym przekazem głosu i danych (wideotelefonia);
- deklarowana szerokość pasma (Nx64 kb/s), agregowanie kanałów;
- sygnalizacja pozapasmowa (kanał D);
- automatyczna identyfikacja numeru (ANI);
- identyfikacja abonenta wywołującego (CLI);
- współdziałanie z innymi sieciami (X.25, Frame Relay, ATM i in.);
- korzystanie ze standardowych (istniejących i komutowanych) linii telefonicznych dla dostępu podstawowego;
- identyczna lub zbliżona taryfikacja jak dla usług podstawowych POTS.

Dostęp BRI

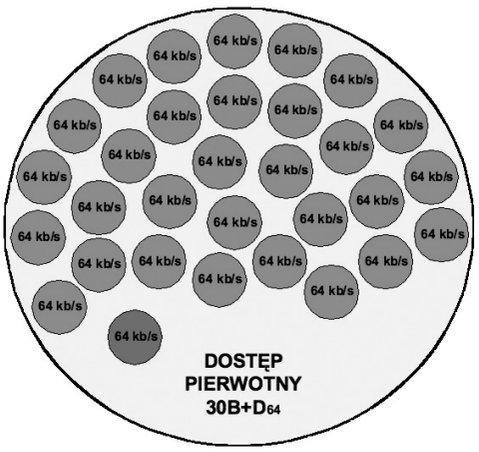
W dostępie podstawowym **BRI** (ang. *Basic Rate Interface*), oznaczanym 2B+D16, maksymalna przepływność 144 kb/s (2x64 kb/s + 16 kb/s) jest oferowana przez dwa kanały B (Bearer) po 64 kb/s w każdym oraz jeden kanał D (Delta) z przepływnością 16 kb/s (patrz rys. 10). Kanałami informacyjnymi B przesyła się głos w postaci cyfrowej, telekopie (faks G4) i dane cyfrowe, natomiast kanałem D sekwencje sygnalizacyjne stosowane przy konfigurowaniu komunikacji, nadzór nad przebiegiem transmisji w kanałach B i inne informacje serwisowe. Kanały B można wykorzystywać pojedynczo (po 64 kb/s) lub łącznie (128 kb/s), bądź z integracją



Rysunek 10.
Dostęp podstawowy BRI

kanału D (razem 144 kb/s), jeśli nie jest on zajęty sygnalizacją połączenia. W niektórych sytuacjach wydzielony kanał D (16 kb/s) może być używany jako kanał informacyjny użytkownika do prowadzenia transmisji pakietowej.

Dostęp PRI

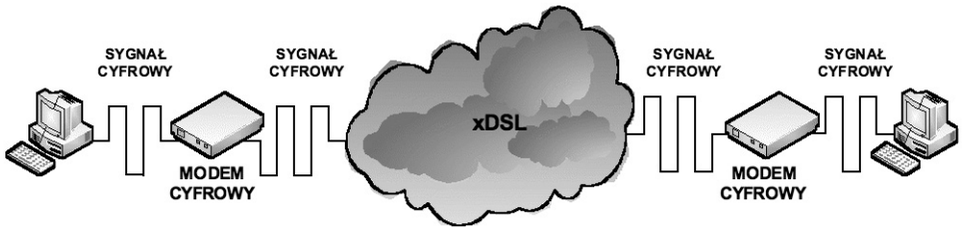


Rysunek 11.
Dostęp pierwotny PRI

W dostępie pierwotnym **PRI** (ang. *Primary Rate Interface*), oznaczanym 30B+D64, istnieje 30 kanałów B (po 64 kb/s) oraz 1 kanał D (64 kb/s), a maksymalna przepływność wynosi 1984 kb/s (30x64 kb/s + 64 kb/s). W systemie amerykańskim i japońskim (23B+D64) przepływność wynosi tylko 1536 kb/s (23x64 kb/s + 64 kb/s). Łączem fizycznym (medium transportowym) w dostępie pierwotnym PRI jest zwykle skrętka miedziana wykonana w technologii HDSL (2048 kb/s), także kanał radiowy bądź światłowód o podobnych własnościach.

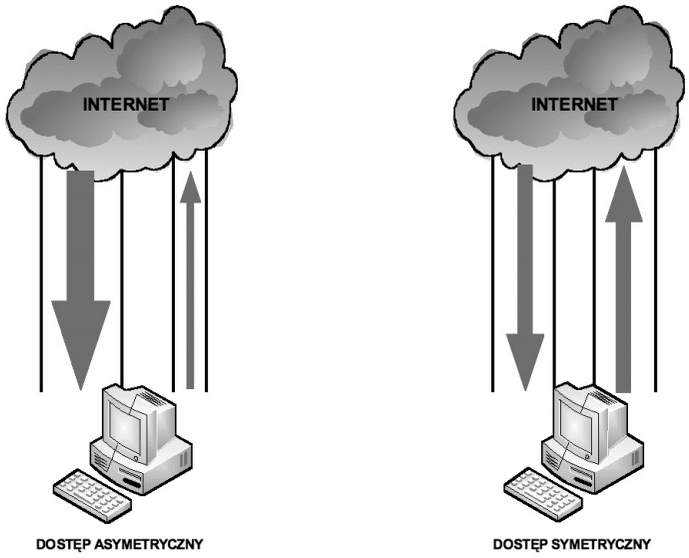
4 TECHNOLOGIA XDSL

Technologia xDSL (ang. *Digital Subscriber Line*) oznacza cyfrową linię abonencką. xDSL jest określeniem całej rodziny technologii zapewniających połączenia z wykorzystaniem istniejących sieci telefonicznych, bez potrzeby ich przebudowy. Modemy DSL wymagają wydzielonej linii kabli miedzianych na swoje potrzeby, najczęściej konieczna jest dzierżawa odpowiedniego łącza od operatora telekomunikacyjnego (patrz rys. 12). Większość łączy stałych o większej przepustowości powyżej 512 kb/s w Polsce realizowana jest za pomocą technologii z rodziny DSL. Korzystając z istniejącej infrastruktury telekomunikacyjnej, technologie te pozwalają uzyskać przepustowość nawet do 50 Mb/s. Ponieważ cały czas powstają nowe protokoły wykorzystujące coraz bardziej zaawansowane metody transmisji, więc możliwości oferowane przez technologię xDSL ciągle wzrastają.



Rysunek 12.
Wykorzystanie publicznej sieci telefonicznej do przesyłu danych w postaci cyfrowej

Dostęp symetryczny i asymetryczny



Rysunek 13.
Różnice w przepływie danych w dostępie symetrycznym i asymetrycznym

Ważnym pojęciem z zakresu technologii xDSL jest symetria łącza. Ponieważ typowy użytkownik Internetu generuje dużo większy ruch do siebie niż od siebie, powstały technologie niesymetrycznego dostępu, zapewniające dużo większe pasmo podczas ściągania danych z Internetu, a mniejsze przy wysyłaniu. Modemy DSL możemy podzielić na dwie grupy:

1. Modemy teletransmisyjne – zapewniające transmisje symetryczne, służące do zapewnienia dostępu dla firm posiadających własne serwery, które udostępniają informacje do Internetu.
2. Szerokopasmowe modemy dostępowe – urządzenia asymetryczne używane przez klientów chcących zapewnić sobie wygodny i tani dostęp do Internetu.

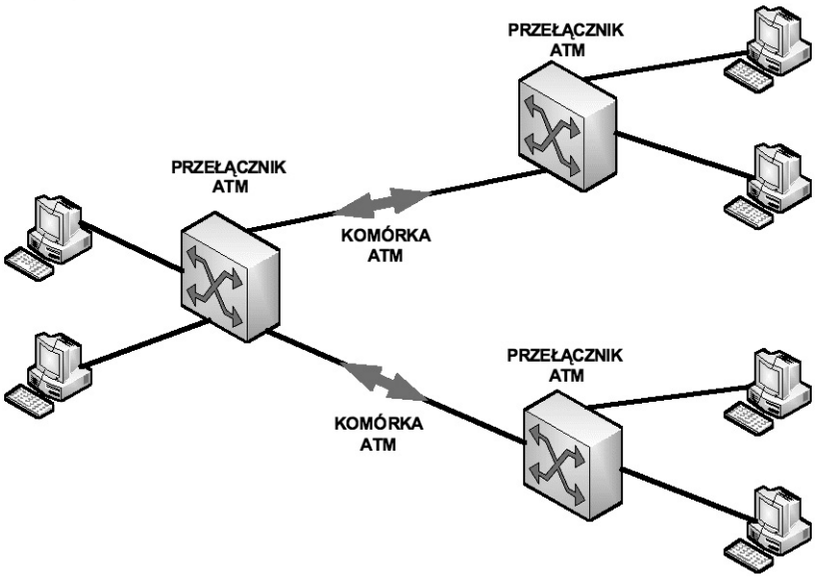
Technologie DSL możemy podzielić na dwie grupy, które są uwarunkowane symetrią transmisji.

1. Asymetryczne:
   ADSL (ang. *Asymmetric Digital Subscriber Line*),
   G. Lite ADSL,
   RADSL (ang. *Rate Adaptive Digital Subscriber Line*),
   VDSL (ang. *Very high Digital Subscriber Line*).
2. Symetryczne:
   SDSL (ang. *Symmetric Digital Subscriber Line*),
   HDSL (ang. *High bit rate Digital Subscriber Line*),
   HDSL2,
   IDSL (ang. *ISDN Digital Subscriber Line*).

Najbardziej znaną technologią xDSL z dostępem asymetrycznym jest Neostrada.

5 TECHNOLOGIA ATM

Sieci asynchroniczne ATM



Rysunek 14.
Przełączanie komórek w sieciach ATM

Sieci **ATM** (ang. *Asynchronous Transfer Mode*) oferują *a*synchroniczną i szerokopasmową technologię komunikacyjną przeznaczoną do przesyłania usług multimedialnych (głosu, dźwięku, obrazu, danych). Technika ATM łączy zalety transmisji synchronicznej **STM** (ang. *Synchronous Transfer Mode*) i transmisji pakietowej **PTM** (ang. *Packet Transfer Mode*), eliminując większość wad każdego z tych systemów. Cechy sieci asynchronicznych ATM:

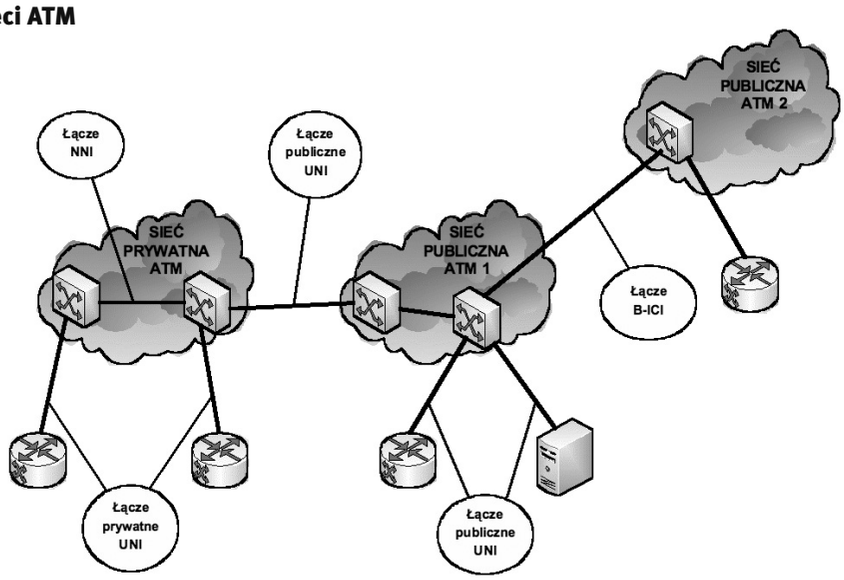
- przesyłanie stałych porcji informacji o pojemności 53 bajty (w tym 48 bajtów informacji użytecznej);
- ustalanie indywidualnych połączeń o dowolnej szybkości w obrębie przyjętych lub istniejących standardów (25 Mb/s, 100 Mb/s, 155 Mb/s, 622 Mb/s, 2,5 Gb/s, 10 Gb/s, 40 Gb/s), dzięki przyporządkowaniu dowolnej liczby komórek do konkretnego połączenia użytkownika;
- obsługa transmisji izochronicznych (głos, obraz ruchomy) z opóźnieniem nie większym niż 10 ms, przez zastosowanie przełączników ATM z szybkim przełączaniem komórek i połączeń;
- skalowanie przepływności ścieżek i węzłów ATM, dzięki czemu wykorzystuje się w pełni maksymalną przepływność dowolnego medium transportowego.
- tworzenie przekazów głównie w trybie połączeniowym, co oznacza, że przed wysłaniem informacji właściwej występuje faza zestawienia łącza – według parametrów deklarowanych przez abonenta (typ usługi, przewidywana przepływność, deklarowany adres), a po zakończeniu przekazu – jego likwidacja.
- tworzenie wirtualnych połączeń przez sieć zarówno dla pojedynczych kanałów, jak i definiowanych grup kanałów zwanych ścieżkami – jest to możliwe dzięki istnieniu odpowiednich identyfikatorów **VCI** (ang. *Virtual Channel Identifier*) dla kanałów oraz identyfikatorów **VPI** (ang. *Virtual Path Identifier*) dla ścieżek wirtualnych; pola tych identyfikatorów znajdują się w nagłówku każdej komórki ATM przesyłanej przez sieć.
- przypisanie komórkom ATM (kanałowi, ścieżce, połączeniu między użytkownikami) konkretnej usługi, której parametry mogą być dynamicznie zmieniane zarówno w fazie nawiązywania łącza, jak i w trakcie działania usługi komunikacyjnej.

Duża szybkość multipleksowania portów i strumieni w rozbudowanych przełącznikach ATM klasy high-end, sięgająca 40 Gb/s (znane są już rozwiązania działające z szybkością 160 Gb/s), wynika ze sprzętowej realizacji procesu przełączania opartej na dynamicznie wymienianych tablicach routingu, przekazywanych kanałami sygnalizacyjnymi ATM.

Dla optymalizacji szybkości przekazu komórek przełączniki ATM nie mają warstwy sieciowej modelu odniesienia OSI, nie prowadzą kontroli błędów transmisyjnych, a stacja odbiorcza sama musi sprawdzić, czy odebrany przekaz jest kompletny i poprawny.

Sieć ATM, inaczej niż sieć X.25, nie odpowiada za błędnie przesłane komórki, nie inicjuje retransmisji i powtórzeń, ale wykorzystując media o bardzo dobrej jakości, jest szybką i nowoczesną siecią transportową.

Działanie sieci ATM



Rysunek 15.
Rodzaje łączy w sieciach asynchronicznych ATM

Sieć ATM składa się ze zbioru central ATM połączonych ze sobą za pomocą łączy punkt-punkt. Centrale ATM są obsługiwane głównie za pomocą trzech rodzajów interfejsów (patrz rys. 15):

- **UNI** (ang. *user to network interface*),
- **NNI** (ang. *network to network interface*),
- **B-ICI** (ang. *broadband inter carrier interface*).

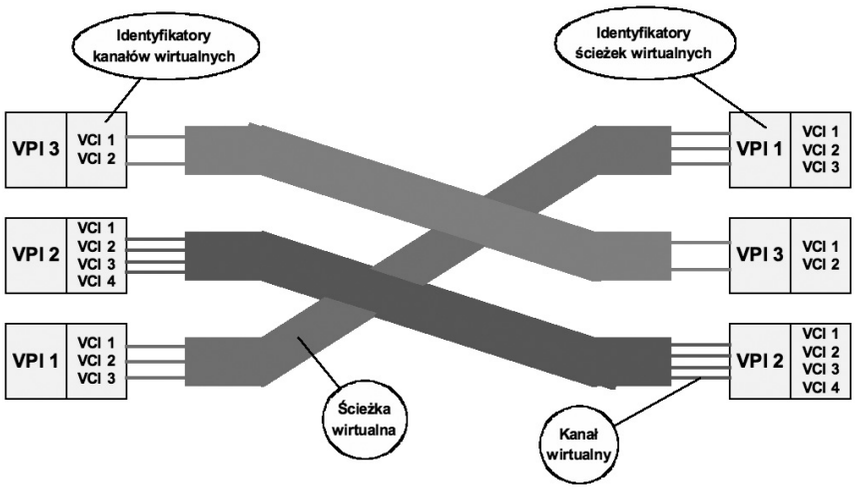
UNI łączy punkty końcowe ATM takie jak hosty, routery, centrale LAN z centralą ATM.

NNI łączy dwie centrale ATM w ramach tej samej organizacji.

W zależności od tego czy centrala znajduje się w posiadaniu prywatnym czy jest publiczna, UNI i NNI można sklasyfikować odpowiednio jako prywatne lub publiczne. Prywatny UNI to punkt referencyjny pomiędzy punktem końcowym ATM i prywatną centralą ATM. Publiczny UNI znajduje się pomiędzy punktem końcowym ATM i centralą publiczną lub pomiędzy centralą prywatną a centralą publiczną. Prywatny NNI (PNNI) określa punkty referencyjne pomiędzy dwiema centralami ATM w tej samej organizacji prywatnej.

B-ICI znajduje się pomiędzy dwiema centralami publicznymi różnych dostawców usług.

Ścieżki i kanały wirtualne ATM



Rysunek 16.
Identyfikatory ścieżek i kanałów wirtualnych

Połączenia w sieci ATM nie odwzorowują jej fizycznej struktury – a są to jedynie wirtualne połączenia logiczne. Wyróżniamy dwa typy połączeń wirtualnych (patrz rys. 16):

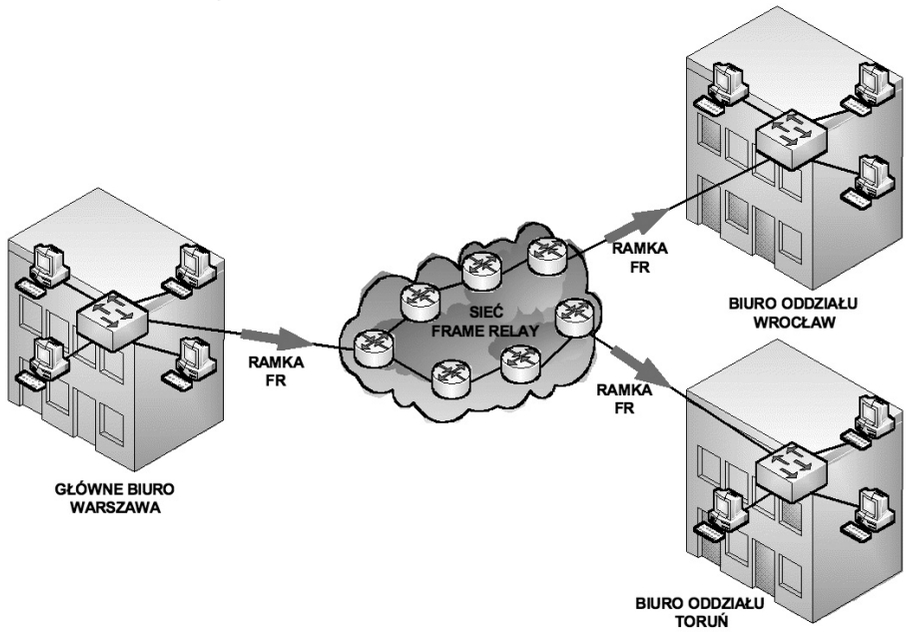
- Kanał wirtualny **VC** (ang. *Virtual Channel*) – jako jednokierunkowe połączenie logiczne przez sieć pomiędzy dwoma stacjami końcowymi, ustanawiane i przełączane dynamicznie przez węzły pośredniczące sieci (fizyczne przełączniki ATM);
- Ścieżki wirtualne **VP** (ang. *Virtual Path*) – jako wiązka kanałów przebiegająca tą samą trasą co kanały wirtualne i łącząca dwóch użytkowników lub grupę abonentów końcowych zainstalowanych w tych samych węzłach dostępu.

Realizacja połączeń za pomocą ścieżek i kanałów wirtualnych w sieciach ATM zapewniona jest przez przydzielenie im odpowiednich identyfikatorów ścieżki wirtualnej VPI oraz kanałów wirtualnych VCI w obrębie każdej ścieżki. Pola identyfikatorów VPI i VCI znajdują się w nagłówku każdego pakietu przesyłanego przez sieć ATM, są zwykle kasowane i wypełniane w węzłach dostępowych sieci oraz modyfikowane przez węzły pośredniczące. Tak zdefiniowana sieć połączeń umożliwia dowolne konfigurowanie struktury, niezależnie od topologii sieci z uwzględnieniem relacji:

- użytkownik – użytkownik: połączenia wirtualne są zakończone u abonentów zapewniając dużą przepływność magistralową przez sieć;
- użytkownik – sieć: odpowiednik centrali abonenckiej PABX w strukturach klasycznych.
- sieć – sieć: zakończenia ścieżek wirtualnych znajdują się w węzłach dostępowych sieci ATM lub w węzłach sieci współpracujących.

6 TECHNOLOGIA FRAME RELAY

Wprowadzenie do Frame Relay



Rysunek 17.
Połączenia pomiędzy oddziałami firmy za pomocą sieci Frame Relay

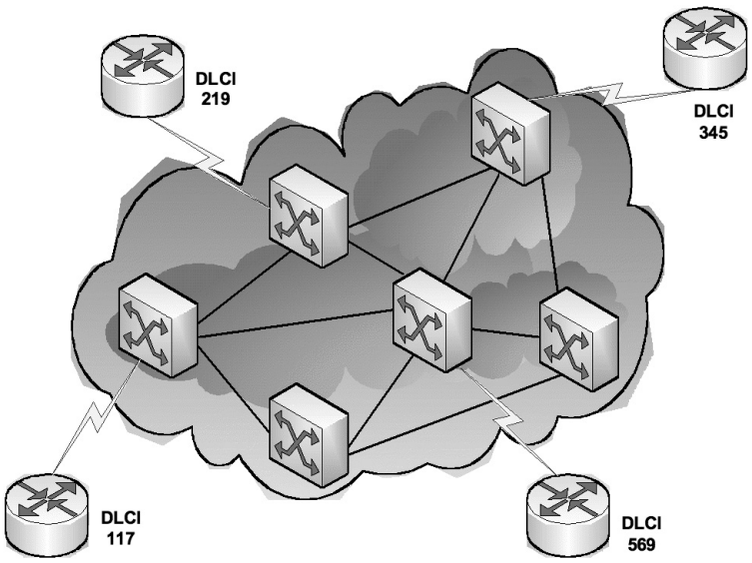
Frame Relay to standard **ITU-T** (ang. *International Telecommunication Union Telecommunication Standardization Sector*) i **ANSI** (ang. *American National Standards Institute*).

Pierwsze propozycje normalizacji Frame Relay przedstawiono organizacji **CCITT** (ang. *Consultative Committee on International Telephone and Telegraph*) w roku 1984. Jednak z uwagi na brak pełnej normalizacji i współpracy w latach 80 ubiegłego wieku technologii Frame Relay nie stosowano na wielką skalę. W 1990 roku firmy Cisco, DEC, Northern Telecom i StrataCom utworzyły konsorcjum do prac nad rozwojem technologii FR. Specyfikacje będące dziełem tego konsorcjum poszerzyły protokół Frame Relay o dodatkowe możliwo-

ści dla złożonych środowisk sieciowych. Rozszerzenia te znane są pod zbiorczą nazwą **LMI** (ang. *Local Management Interface*).

Technologia **FR** (ang. *Frame Relay*) stała się dosyć powszechnym standardem sieciowym zwłaszcza w regionach, gdzie nie dotarła wcześniej technologia X.25. Sieć FR jest znacznie szybsza od X.25 i tańsza niż ATM. Frame Relay działa podobnie jak X.25, operuje jednak na pakietach o zmiennej długości i pozwala na zwiększenie szybkości tworzonych połączeń. Wnosi niewielkie opóźnienia i zapewnia sprawiedliwy dostęp do pasma wszystkim użytkownikom. Na taką właśnie technologię czekali administratorzy sieciowi średnich i wielkich przedsiębiorstw. Protokół Frame Relay funkcjonuje w dwu pierwszych warstwach modelu ISO/OSI.

Identyfikatory DLCI



Rysunek 18.
Identyfikatory DLCI

Sieć FR składa się z przełączników połączonych kanałami fizycznymi, w których są multipleksowane obwody wirtualne rozpoznawane po niepowtarzalnych numerach **DLCI** (ang. *Data Link Connection Identifier*), i z urządzeń dostępowych (patrz rys. 18). Połączenie zrealizowane w sieci Frame Relay między dwoma urządzeniami DTE jest określane jako obwód wirtualny **VC** (ang. *Virtual Circuit*). Obwody wirtualne mogą być ustanawiane dynamicznie poprzez wysłanie do sieci odpowiednich komunikatów sygnalizacyjnych. Takie obwody określane są jako przełączane obwody wirtualne **SVC** (ang. *Switched Virtual Circuit*).Zwykle używane są stałe obwody wirtualne **PVC** (ang. *Permanent Virtual Circuit*) skonfigurowane wstępnie przez operatora. Obwód wirtualny tworzony jest poprzez zapisanie w pamięci każdego przełącznika odwzorowania między portem wejściowym a portem wyjściowym. W wyniku tej operacji oba przełączniki pozostają połączone tak długo, jak zdefiniowana jest ciągła ścieżka między dwoma końcami określonego obwodu.

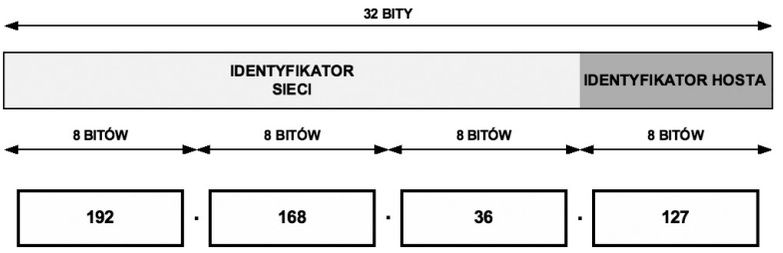
Istnieje możliwość rozróżnienia wielu obwodów wirtualnych występujących w pojedynczym łączu dostępowym, ponieważ z każdym obwodem wirtualnym jest związany unikalny identyfikator DLCI. Identyfikator DLCI jest zapisany w polu adresu każdej przesyłanej ramki. Identyfikator DLCI jest zazwyczaj zdefiniowany lokalnie i może być różny na każdym końcu obwodu wirtualnego.

7 WYBRANE USŁUGI SIECIOWE

7.1 PODSTAWY ADRESOWANIA IPV4

Format adresu IPv4

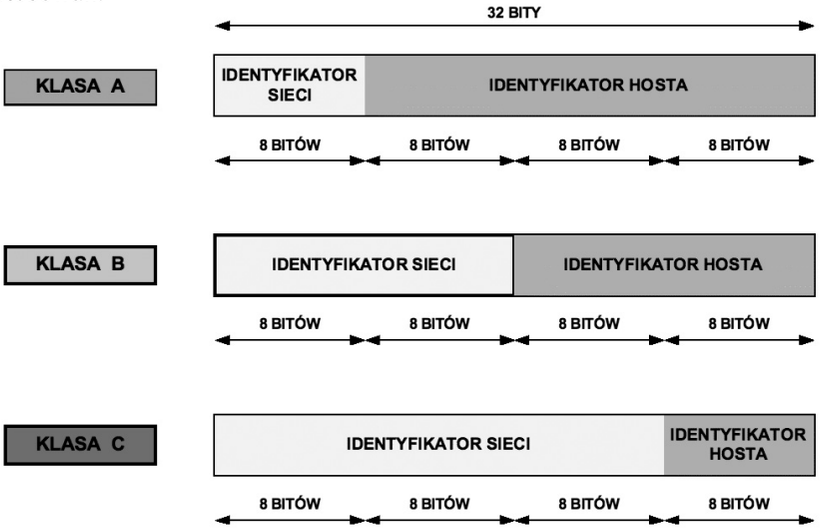
Adres IPv4 jest 32-bitową liczbą binarną konwertowaną do notacji kropkowo-dziesiętnej. Składa się z identyfikatora sieci przydzielonego przez odpowiedni **RIR** (ang. *Regional Internet Registries*) oraz identyfikatora hosta (zarządzanego przez administratora sieciowego).



Rysunek 19.
Format adresu IP w wersji 4

Klasy adresów IPv4

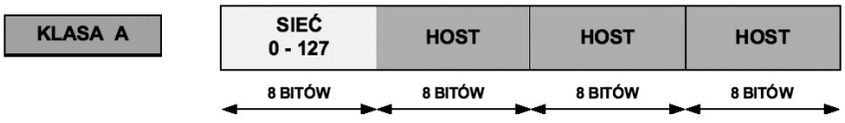
W **adresowaniu klasowym** wyróżniono pięć klas adresowych – A, B, C, D i E. Trzy pierwsze klasy A, B i C wykorzystuje się do adresacji hostów w sieciach komputerowych, natomiast klasy D i E są przeznaczone dla specyficznych zastosowań.



Rysunek 20.
Klasy adresów IP w wersji 4

Klasa A

klasa A – pierwszy bit adresu jest równy 0, a następne 7 bitów określa sieć. Kolejne 24 bity wskazują komputer w tych sieciach. Adres rozpoczyna się liczbą między 1 i 127. Można zaadresować 126 sieci (adres 127.x.y.z został zarezerwowany dla celów diagnostycznych jako adres loopback) po 16 777 214 ($2^{24} – 2$) komputerów.



Rysunek 21.
Klasa A

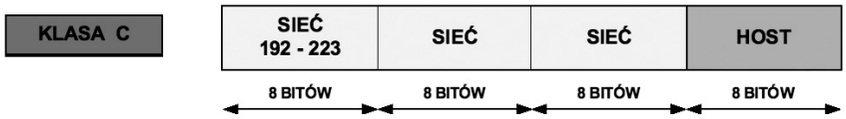
Klasa B

klasa B – dwa pierwsze bity adresu to 1 i 0, a następne 14 bitów określa sieć. Kolejne 16 bitów identyfikuje komputer. Adres rozpoczyna się liczbą między 128 i 191. Można zaadresować 16 384 (2^{14}) sieci po 65 534 ($2^{16} – 2$) komputery.

Rysunek 22.
Klasa B

Klasa C

klasa C – trzy pierwsze bity adresu to 1, 1 i 0, a następnych 21 bitów identyfikuje adresy sieci. Ostatnie 8 bitów służy do określenia numeru komputerów w tych sieciach. Adres rozpoczyna się liczbą między 192 i 223. Może zaadresować 2 097 152 (2^{21}) sieci po 254 (2^8 – 2) komputery.

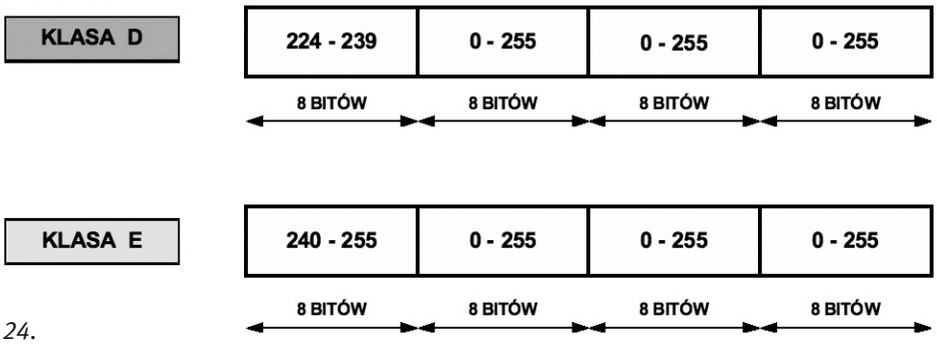


Rysunek 23.
Klasa C

Klasa D i E

klasa D – cztery pierwsze bity adresu to 1110. Adres rozpoczyna się liczbą między 224 i 239. Adresy tej klasy są stosowane do wysyłania rozgłoszeń typu multicast.

klasa E – cztery pierwsze bity adresu to 1111. Adres rozpoczyna się liczbą między 240 i 255 (adres 255.255.255.255 został zarezerwowany dla celów rozgłoszeniowych). Adresy tej klasy są zarezerwowane dla przyszłych zastosowań.



Rysunek 24.
Klasa D i E

7.2 USŁUGI NAT I PAT

Adresy prywatne

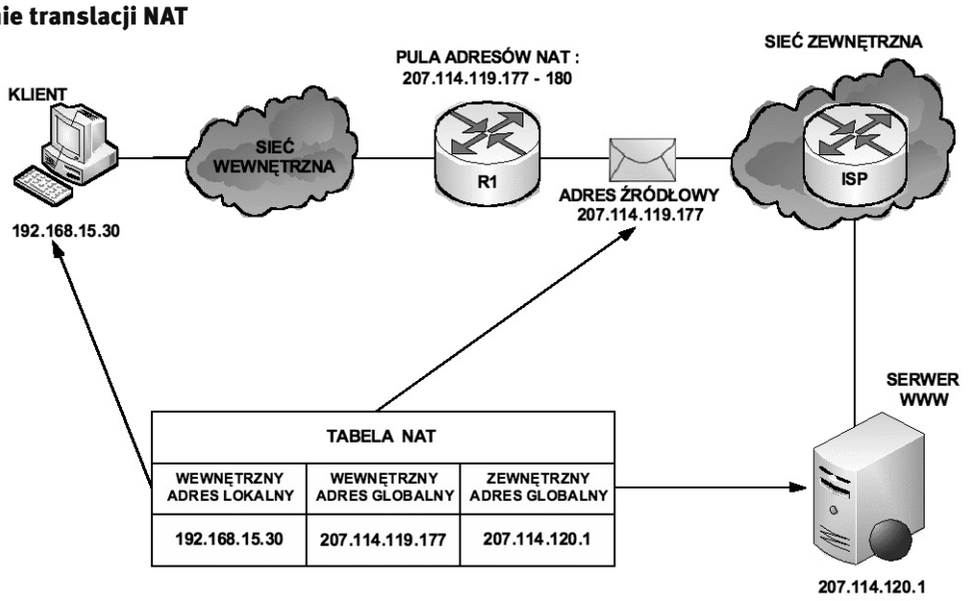
Tabela 1.
Dostępne zakresy prywatnych adresów IP

KLASA	ZAKRES ADRESÓW PRYWATNYCH RFC 1918	STANDARDOWA MASKA PODSIECI	ILOŚĆ SIECI	ILOŚĆ HOSTÓW NA SIEĆ	CAŁKOWITA ILOŚĆ HOSTÓW
A	10.0.0.0 – 10.255.255.255	255.0.0.0	1	16 777 214	16 777 214
B	172.16.0.0 – 172.31.255.255	255.255.0.0	16	65 534	1 048 544
C	192.168.0.0 – 192.168.255.255	255.255.255.0	256	254	65 024

W dokumencie RFC 1918 wyróżniono trzy pule adresów IP przeznaczonych tylko do użytku prywatnego. Adresy te mogą być stosowane tylko i wyłącznie w sieci wewnętrznej. W zależności od tego, jak dużą sieć zamierzamy skonfigurować, wybieramy jedną z klas adresów (A, B lub C). Pakiety z takimi adresami nie są routowane przez Internet.

Prywatne adresy IP są zarezerwowane i mogą zostać wykorzystane przez dowolnego użytkownika. Oznacza to, że ten sam adres prywatny może zostać wykorzystany w wielu różnych sieciach prywatnych. Router nie powinien nigdy routować adresów wymienionych w dokumencie RFC 1918. Dostawcy usług internetowych zazwyczaj konfigurują routery brzegowe tak, aby zapobiec przekazywaniu ruchu przeznaczonego dla adresów prywatnych. Zastosowanie mechanizmu NAT zapewnia wiele korzyści dla poszczególnych przedsiębiorstw i dla całego Internetu. Zanim opracowano technologię NAT, host z adresem prywatnym nie mógł uzyskać dostępu do Internetu. Wykorzystując mechanizm NAT, poszczególne przedsiębiorstwa mogą określić adresy prywatne dla niektórych lub wszystkich swoich hostów i zapewnić im dostęp do Internetu.

Działanie translacji NAT

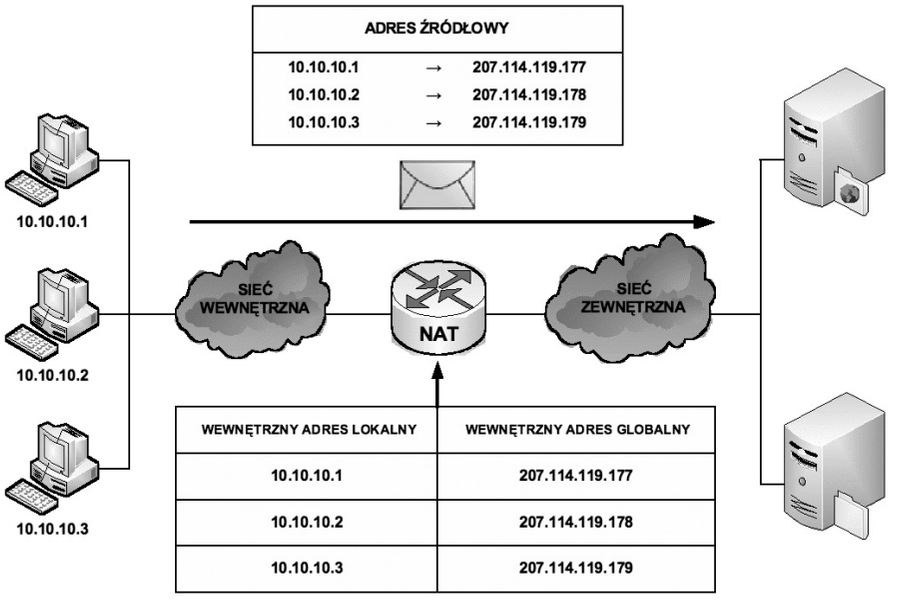


Rysunek 25.
Działanie translacji NAT

Na rysunku 25 wyjaśnione jest działanie usługi **NAT** (ang. *Network Address Translation*):

- Klient o adresie prywatnym 192.168.15.30 (wewnętrzny adres lokalny) zamierza otworzyć stronę WWW przechowywaną na serwerze o adresie publicznym 207.114.120.1 (zewnętrzny adres globalny).
- Komputer kliencki otrzymuje z puli adresów przechowywanych na routerze R1 publiczny adres IP (wewnętrzny adres globalny) 207.114.119.177.
- Następnie router ten wysyła pakiet o zmienionym adresie źródłowym do sieci zewnętrznej (router ISP), z której trafia do serwera WWW.
- Kiedy serwer WWW odpowiada na przypisany przez usługę NAT adres IP 207.114.119.177, pakiet powraca do routera R1, który na podstawie wpisów w tabeli NAT ustala, że jest to uprzednio przekształcony adres IP.
- Następuje translacja wewnętrznego adresu globalnego 207.114.119.177 na wewnętrzny adres lokalny 192.168.15.30, a pakiet przekazywany jest do stacji klienckiej.

Statyczna translacja NAT

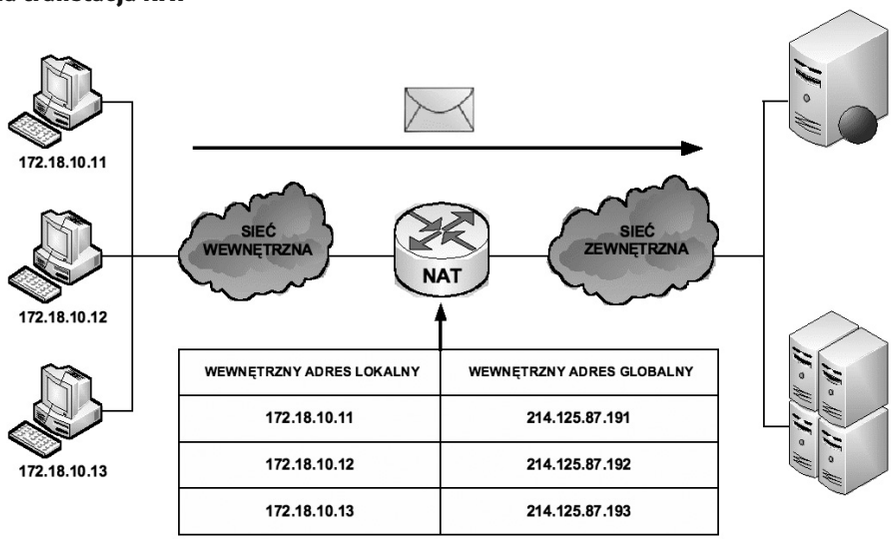


Rysunek 26.
Statyczna translacja NAT

Statyczna translacja NAT (ang. *static NAT*) umożliwia utworzenie odwzorowania typu jeden-do-jednego pomiędzy adresami lokalnymi i globalnymi pomiędzy sieciami wewnętrzną i zewnętrzną. Jest to szczególnie przydatne w wypadku hostów, które muszą mieć stały adres dostępny z Internetu. Takimi wewnętrznymi hostami mogą być serwery lub urządzenia sieciowe w przedsiębiorstwie. W tym rozwiązaniu administrator ręcznie konfiguruje predefiniowane skojarzenia adresów IP. Ten typ translacji tak naprawdę nie ma nic wspólnego z oszczędzaniem przestrzeni adresowej IP, gdyż każdemu prywatnemu adresowi w sieci wewnętrznej trzeba przypisać adres publiczny w sieci zewnętrznej. Jednakże takie odwzorowanie daje gwarancję, że żaden przesyłany pakiet nie zostanie odrzucony z powodu braku dostępnej przestrzeni adresowej.

Na rys. 26 widzimy, że trzem adresom prywatnym (10.10.10.1, 10.10.10.2, 10.10.10.3) zamapowano trzy adresy publiczne (odpowiednio 207.114.119.177, 207.114.119.178, 207.114.119.179).

Dynamiczna translacja NAT

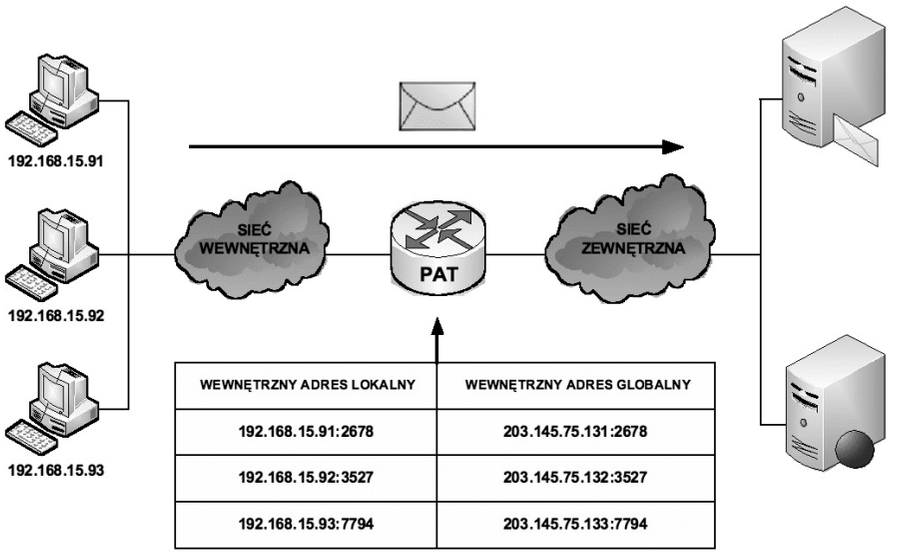


Rysunek 27.
Dynamiczna translacja NAT

Dynamiczna translacja NAT (ang. *dynamic NAT*), patrz rys. 27, służy do odwzorowania prywatnego adresu IP na dowolny adres publiczny (z uprzednio zdefiniowanej puli). W translacji dynamicznej unikamy stosowania dokładnie takiej samej puli adresów publicznych co prywatnych. Oznacza to, że z jednej strony możemy zaoszczędzić dostępną przestrzeń adresową ale istnieje ryzyko braku gwarancji zamiany adresów w przypadku wyczerpania się puli adresów routowalnych. Z tego powodu na administratora sieci spoczywa obowiązek zadbania o odpowiedni zakres puli adresów publicznych, aby możliwa była obsługa wszystkich możliwych translacji. Ponieważ nie wszyscy użytkownicy sieci komputerowej potrzebują jednoczesnego dostępu do zasobów zewnętrznych, można skonfigurować pulę adresów publicznych mniejszą od liczby adresów prywatnych. Dlatego w tym przypadku unikamy przypisywania wszystkim użytkownikom adresów routowalnych jak w usłudze translacji statycznej NAT.

Translacja PAT

Translacja **PAT** (ang. *Port Address Translation*), patrz rys. 28, służy do odwzorowania wielu prywatnych adresów IP na jeden publiczny adres IP. Istnieje możliwość odwzorowania wielu adresów na jeden adres IP, ponieważ z każdym adresem prywatnym związany jest inny numer portu. W technologii PAT tłumaczone adresy są rozróżniane przy użyciu unikatowych numerów portów źródłowych powiązanych z globalnym adresem IP. Numer portu zakodowany jest na 16 bitach. Całkowita liczba adresów wewnętrznych, które mogą być przetłumaczone na jeden adres zewnętrzny, może teoretycznie wynosić nawet 65 536. W rzeczywistości do jednego adresu IP może zostać przypisanych około 4000 portów. W mechanizmie PAT podejmowana jest zawsze próba zachowania pierwotnego portu źródłowego. Jeśli określony port źródłowy jest już używany, funkcja PAT przypisuje pierwszy dostępny numer portu, licząc od początku zbioru numerów odpowiedniej grupy portów (0–511, 512–1023 lub 1024–65535). Gdy zabraknie dostępnych portów, a skonfigurowanych jest wiele zewnętrznych adresów IP, mechanizm PAT przechodzi do następnego adresu IP w celu podjęcia kolejnej próby



Rysunek 28.
Translacja PAT

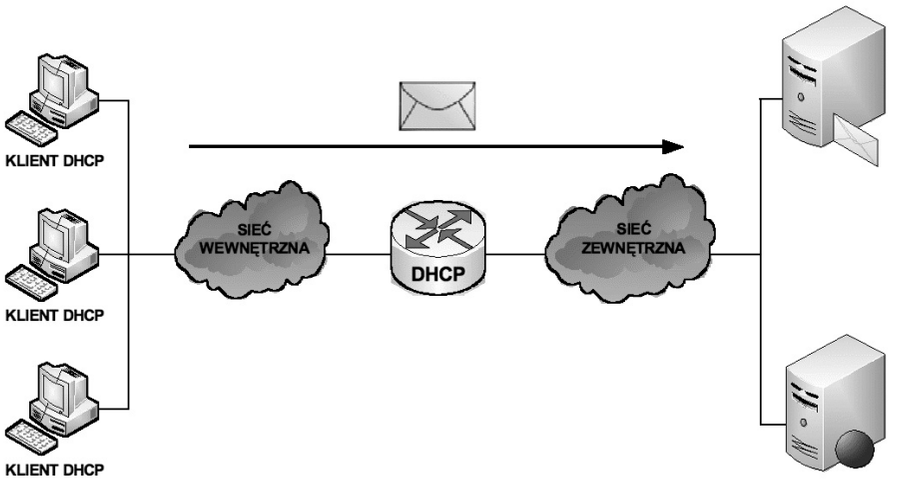
przydzielenia pierwotnego portu źródłowego. Ten proces jest kontynuowany aż do wyczerpania wszystkich dostępnych numerów portów i zewnętrznych adresów IP.

Zalety translacji NAT i PAT

Do głównych zalet translacji adresów prywatnych na publiczne należą:

1. Eliminacja konieczności ponownego przypisania adresów IP do każdego hosta po zmianie dostawcy usług internetowych (ISP). Użycie mechanizmu NAT umożliwia uniknięcie zmiany adresów wszystkich hostów, dla których wymagany jest dostęp zewnętrzny, a to wiąże się z oszczędnościami czasowymi i finansowymi.
2. Zmniejszenie liczby adresów przy użyciu dostępnej w aplikacji funkcji multipleksowania na poziomie portów. Gdy wykorzystywany jest mechanizm PAT, hosty wewnętrzne mogą współużytkować pojedynczy publiczny adres IP podczas realizacji wszystkich operacji wymagających komunikacji zewnętrznej. W takiej konfiguracji do obsługi wielu hostów wewnętrznych wymagana jest bardzo niewielka liczba adresów zewnętrznych. Prowadzi to do oszczędności adresó IP.
3. Zwiększenie poziomu bezpieczeństwa w sieci. Ponieważ w wypadku sieci prywatnej nie są rozgłaszane wewnętrzne adresy ani informacje o wewnętrznej topologii, sieć taka pozostaje wystarczająco zabezpieczona, gdy dostęp zewnętrzny odbywa się z wykorzystaniem translacji NAT.

7.3 USŁUGA DHCP



Rysunek 29.
Działanie usługi dynamicznego przydzielania adresów IP

Usługa **DHCP** (ang. *Dynamic Host Configuration Protocol*) działa w trybie klient-serwer i została opisana w dokumencie RFC 2131. Umożliwia ona klientom DHCP w sieciach IP uzyskiwanie informacji o ich konfiguracji z serwera DHCP. Użycie usługi DHCP zmniejsza nakład pracy wymagany przy zarządzaniu siecią IP. Najważniejszym elementem konfiguracji odbieranym przez klienta od serwera jest adres IP klienta. Klient DHCP wchodzi w skład większości nowoczesnych systemów operacyjnych, takich jak systemy Windows, Sun Solaris, Linux i MAC OS. Klient żąda uzyskania danych adresowych z sieciowego serwera DHCP, który zarządza przydzielaniem adresów IP i odpowiada na żądania konfiguracyjne klientów.

Serwer DHCP może odpowiadać na żądania pochodzące z wielu podsieci. Protokół DHCP działa jako proces serwera służący do przydzielania danych adresowych IP dla klientów. Klienci dzierżawią informacje pobrane z serwera na czas ustalony przez administratora. Gdy okres ten dobiega końca, klient musi zażądać nowego adresu. Zazwyczaj klient uzyskuje ten sam adres.

Administratorzy na ogół preferują serwery sieciowe z usługą DHCP, ponieważ takie rozwiązanie jest skalowalne i łatwo nim zarządzać. Konfigurują oni serwery DHCP tak, aby przydzielane były adresy ze zdefiniowanych pul adresów. Na serwerach DHCP mogą być dostępne także inne informacje, takie jak adresy serwerów DNS, adresy serwerów WINS i nazwy domen. W wypadku większości serwerów DHCP administratorzy mogą także zdefiniować adresy MAC obsługiwanych klientów i automatycznie przypisywać dla tych klientów zawsze te same adresy IP.

Protokołem transportowym wykorzystywanym przez protokół DHCP jest **UDP** (ang. *User Datagram Protocol*). Klient wysyła komunikaty do serwera na port 67. Serwer wysyła komunikaty do klienta na port 68.

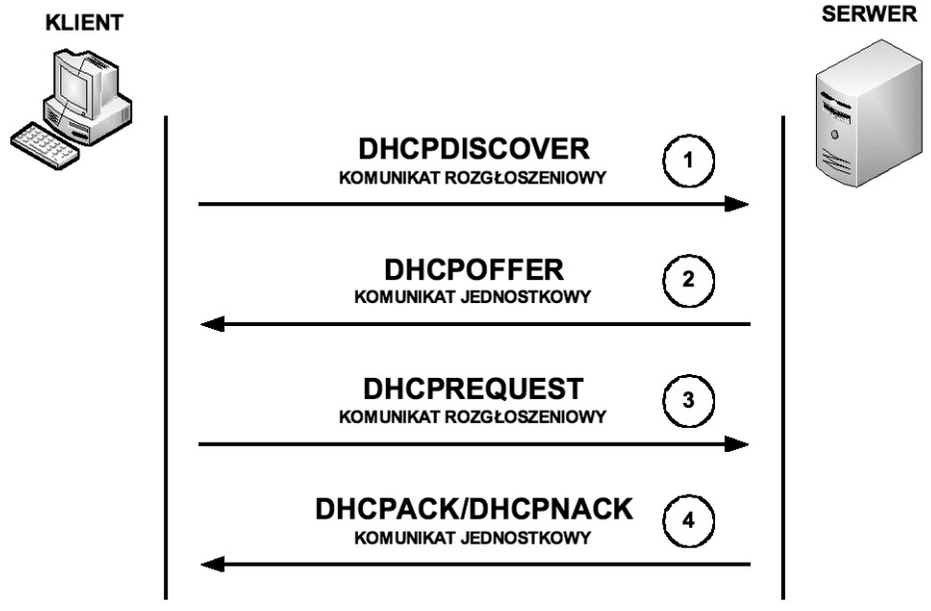
Sposoby przydzielania adresów IP

Istnieją trzy mechanizmy przydzielania adresów IP dla klientów:

1. **Alokacja automatyczna** – serwer DHCP przypisuje klientowi stały adres IP.
2. **Alokacja ręczna** – adres IP dla klienta jest przydzielany przez administratora. Serwer DHCP przesyła adres do klienta.
3. **Alokacja dynamiczna** – serwer DHCP dzierżawi klientowi adres IP na pewien ograniczony odcinek czasu.

Serwer DHCP tworzy pule adresów IP i skojarzonych z nimi parametrów. Pule przeznaczone są dla poszczególnych logicznych podsieci IP. Dzięki temu jeden klient IP może uzyskiwać adresy od wielu serwerów DHCP i może być przenoszony. Jeśli klient uzyska odpowiedź od wielu serwerów, może wybrać tylko jedną z ofert.

Wymiana komunikatów protokołu DHCP



Rysunek 30.
Wymiana komunikatów protokołu DHCP

W procesie konfiguracyjnym klienta DHCP wykonywane są następujące działania (patrz rys. 30):

1. Na kliencie, który uzyskuje członkostwo w sieci, musi być skonfigurowany protokół DHCP. Klient wysyła do serwera żądanie uzyskania konfiguracji IP. Czasami klient może zaproponować adres IP, na przykład wówczas, gdy żądanie dotyczy przedłużenia okresu dzierżawy adresu uzyskanego wcześniej od serwera DHCP. Klient wyszukuje serwer DHCP, wysyłając komunikat rozgłoszeniowy DHCPDISCOVER.
2. Po odebraniu tego komunikatu serwer określa, czy może obsłużyć określone żądanie przy użyciu własnej bazy danych. Jeśli żądanie nie może zostać obsłużone, serwer może przekazać odebrane żądanie dalej, do innego serwera DHCP. Jeśli serwer DHCP może obsłużyć żądanie, do klienta wysyłana jest oferta z konfiguracją IP w formie komunikatu transmisji pojedynczej (unicast) DHCPOFFER. Komunikat DHCPOFFER zawiera propozycję konfiguracji, która może obejmować adres IP, adres serwera DNS i okres dzierżawy.
3. Jeśli określona oferta jest odpowiednia dla klienta, wysyła on inny komunikat rozgłoszeniowy, DHCPREQUEST, z żądaniem uzyskania tych konkretnych parametrów IP. Wykorzystywany jest komunikat rozgłoszeniowy, ponieważ pierwszy komunikat, DHCPDISCOVER mógł zostać odebrany przez wiele serwerów DHCP. Jeśli wiele serwerów wyśle do klienta swoje oferty, dzięki komunikatowi rozgłoszeniowemu DHCPREQUEST serwery te będą mogły poznać ofertę, która została zaakceptowana. Zazwyczaj akceptowana jest pierwsza odebrana oferta.
4. Serwer, który odbierze sygnał DHCPREQUEST, publikuje określoną konfigurację, wysyłając potwierdzenie w formie komunikatu transmisji pojedynczej DHCPACK. Istnieje możliwość (choć jest to bardzo mało prawdopodobne), że serwer nie wyśle komunikatu DHCPACK. Taka sytuacja może wystąpić wówczas, gdy serwer wydzierżawi w międzyczasie określoną konfigurację innemu klientowi. Odebranie komunikatu DHCPACK upoważnia klienta do natychmiastowego użycia przypisanego adresu.

Jeśli klient wykryje, że określony adres jest już używany w lokalnym segmencie, wysyła komunikat DHCPDECLINE i cały proces zaczyna się od początku. Jeśli po wysłaniu komunikatu DHCPREQUEST klient otrzyma od serwera komunikat DHCPNACK, proces rozpocznie się od początku. Gdy klient nie potrzebuje już adresu IP, wysyła do serwera komunikat DHCPRELEASE.

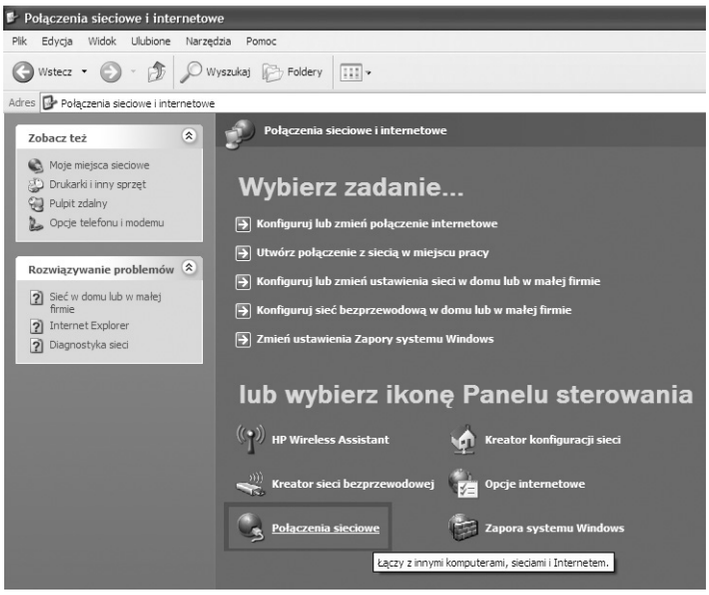
Zależnie od reguł obowiązujących w przedsiębiorstwie, użytkownik końcowy lub administrator może przypisać dla hosta statyczny adres IP dostępny w puli adresów na serwerze DHCP.

Automatyczna konfiguracja adresów IP

Aby automatycznie skonfigurować adresy IP (adres hosta, maska podsieci, brama domyślna, główny serwer DNS, zapasowy serwer DNS) w systemie Windows XP należy wykonać kolejne kroki:

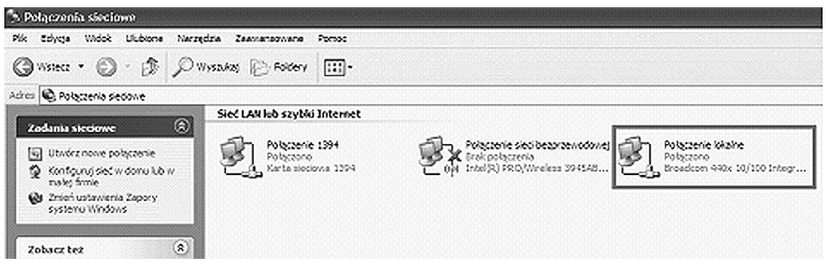
Klikamy przycisk Start a następnie wybieramy zakładkę Panel sterowania. W oknie, które się pojawi (rys. 31), klikamy w kategorię Połączenia sieciowe i internetowe. Z kategorii Połączenia sieciowe i internetowe wybieramy Połączenia sieciowe (patrz rys. 32).

Rysunek 31.
Początek automatycznego konfigurowania adresów IP



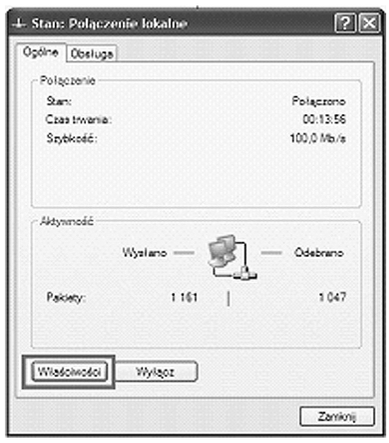
Rysunek 32.
Wybór wśród połączeń sieciowych i internetowych

W kategorii Połączenia sieciowe wybieramy Połączenie lokalne (patrz rys. 33).



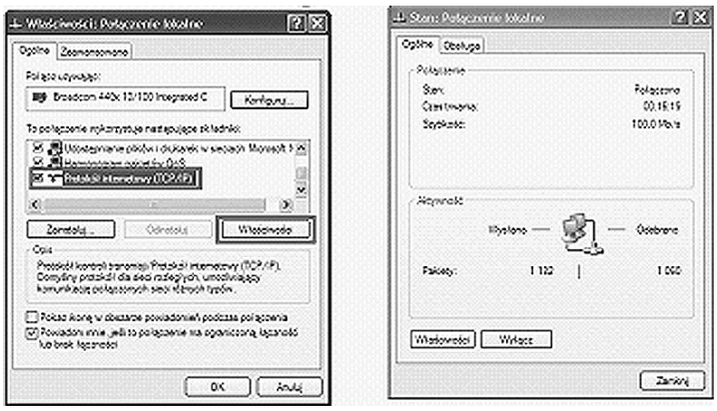
Rysunek 33.
Wybór połączenia lokalnego wśród połączeń sieciowych

W oknie na rys. 34 jest ukazany podgląd stanu Połączenia lokalnego z którego możemy odczytać: stan połączenia, czas trwania połączenia, szybkość połączenia a także jego aktywność (ilość pakietów wysłanych i odebranych). W oknie tym klikamy na zakładkę Właściwości.



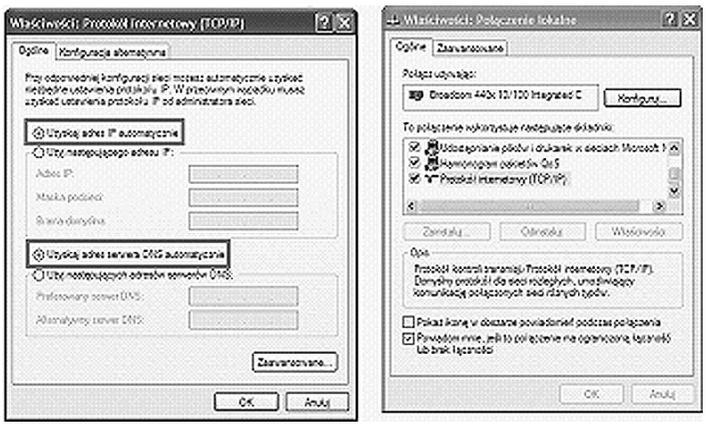
Rysunek 34.
Okno ukazujące stan połączenia lokalnego

Po wybraniu zakładki Właściwości ukazuje nam się kolejne okno (rys. 35), w którym wybieramy składnik Protokół internetowy (TCP/IP) a następnie klikamy w zakładkę Właściwości.



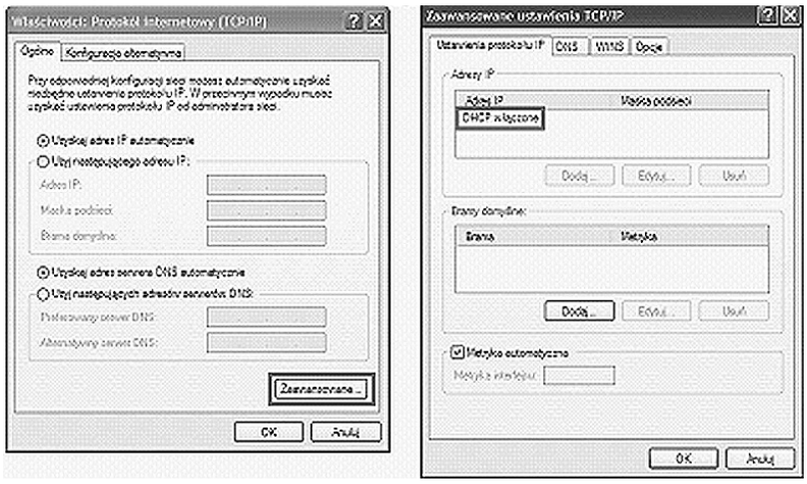
Rysunek 35.
Okno z właściwościami połączenia lokalnego

Po wybraniu składnika Protokół internetowy (TCP/IP) i kliknięciu w zakładkę Właściwości otwiera się okno (rys. 36), w którym wybieramy następujące opcje: Uzyskaj adres IP automatycznie oraz Uzyskaj adres serwera DNS automatycznie. Po wybraniu tych opcji zostaną nadane automatycznie następujące adresy IP: adres IP hosta, jego maska podsieci, adres IP bramy domyślnej, adres IP preferowanego serwera DNS oraz adres IP alternatywnego serwera DNS.



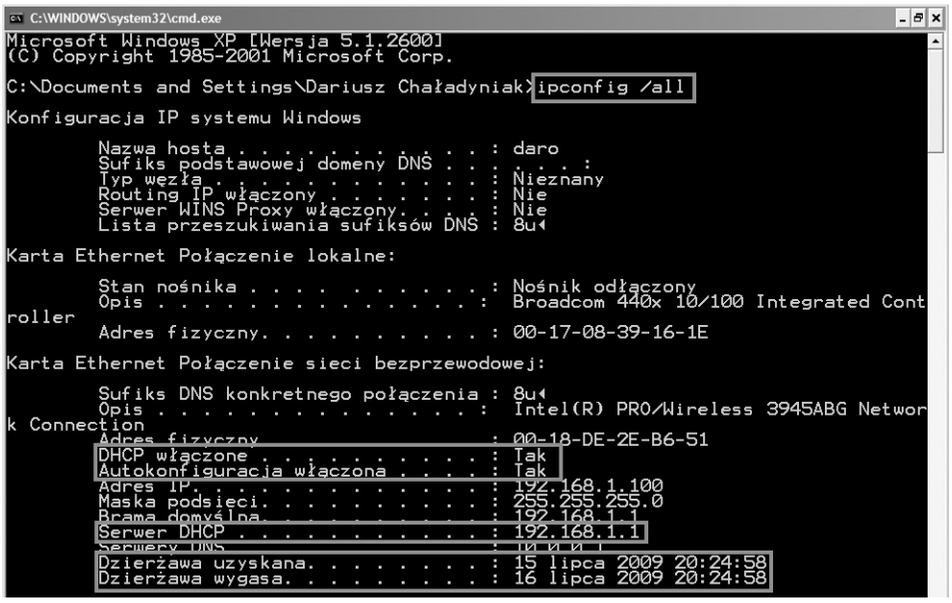
Rysunek 36.
Odznaczenie automatycznych wyborów adresów IP

Po kliknięciu w zakładkę Zaawansowane w oknie Właściwości: Protokół internetowy (TCP/IP) otrzymujemy podgląd w zaawansowane ustawienia stosu protokołów TCP/IP, w którym możemy zauważyć, że jest włączony serwer DHCP (patrz rys. 37).



Rysunek 37.
Efekt wybrania zakładki Zaawansowane w oknie Właściwości Protokołu Internetowego TCP/IP

Testowanie konfiguracji usługi DHCP



Rysunek 38.
Testowanie konfiguracji usługi DHCP

Aby przetestować konfigurację usługi DHCP wydajemy polecenie ipconfig z opcją all. W wyniku jego wykonania otrzymujemy informację, czy usługa DHCP jest włączona i czy włączona jest jej autokonfiguracja. Ponadto otrzymujemy informację o adresie IP serwera DHCP (w tym przypadku – 192.168.1.1) oraz daty: uzyskania dzierżawy usługi DHCP i jej wygaśnięcia (patrz rys. 38).

7.4 USŁUGA DNS

Adresy domenowe

Posługiwanie się adresami IP jest bardzo niewygodne dla człowieka, ale niestety oprogramowanie sieciowe wykorzystuje je do przesyłania pakietów z danymi. Aby ułatwić użytkownikom sieci komputerowych korzystanie z usług sieciowych, obok adresów IP wprowadzono tzw. **adresy domenowe** (symboliczne). Nie każdy komputer musi mieć taki adres. Są one z reguły przypisywane tylko komputerom udostępniającym w Internecie jakieś usługi. Umożliwia to użytkownikom chcącym z nich skorzystać łatwiejsze wskazanie konkretnego serwera. Adres symboliczny zapisywany jest w postaci ciągu nazw, tzw. **domen**, które są rozdzielone kropkami, podobnie jak w przypadku adresu IP. Części adresu domenowego nie mają jednak żadnego związku z poszczególnymi fragmentami adresu IP – chociażby ze względu na fakt, że o ile adres IP składa się zawsze z czterech części, o tyle adres domenowy może ich mieć różną liczbę – od dwóch do siedmiu lub jeszcze więcej. Kilka przykładowych adresów domenowych przedstawiono poniżej:

http://www.wwsi.edu.pl
http://www.onet.pl
http://www.microsoft.com
ftp://public.wwsi.edu.pl
http://www.nask.pl
http://www.mf.gov.pl/

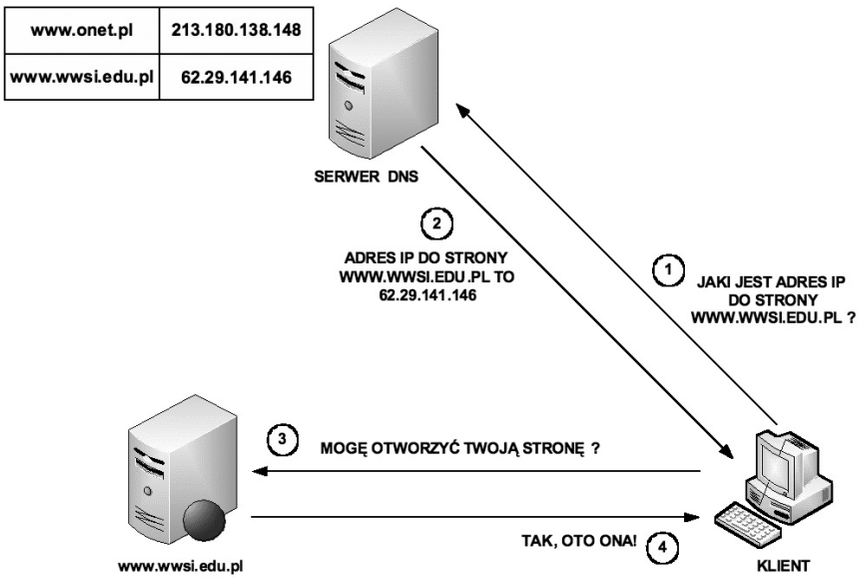
Domeny

Odwrotnie niż adres IP, adres domenowy czyta się od tyłu. Ostatni jego fragment, tzw. **domena najwyższego poziomu** (ang. *top-level domain*), jest z reguły dwuliterowym oznaczeniem kraju (np. .pl, .de). Jedynie w USA dopuszcza się istnienie adresów bez oznaczenia kraju na końcu. W tym przypadku domena najwyższego poziomu opisuje „branżową" przynależność instytucji, do której należy dany komputer. Może to być:

com/co – firmy komercyjne (np. Microsoft, IBM, Intel);
edu/ac – instytucje naukowe i edukacyjne (np. uczelnie);

gov – instytucje rządowe (np. Biały Dom, Biblioteka Kongresu, NASA, Sejm RP);
mil – instytucje wojskowe (np. MON);
org – wszelkie organizacje społeczne i inne instytucje typu *non-profit*;
int – organizacje międzynarodowe nie dające się zlokalizować w konkretnym państwie (np. NATO);
net – firmy i organizacje zajmujące się administrowaniem i utrzymywaniem sieci komputerowych (np. EARN);
biz – biznes;
info – informacje;
name – nazwy indywidualne;
pro – zawody.

Działanie usługi DNS



Rysunek 39.
Przykład działania usługi DNS

Działanie usługi DNS sprowadza się do następujących kolejnych czynności (patrz rys. 39):
1. Klient z przeglądarką internetową pragnie otworzyć stronę www.wwsi.edu.pl przechowywaną na serwerze WWW. Z uwagi, że oprogramowanie sieciowe wymaga adresu IP, klient wysyła zapytanie do serwera DNS o adres IP dla żądanej strony WWW.
2. Serwer DNS na podstawie odpowiednich wpisów w swojej tablicy DNS odsyła klientowi odpowiedź, że dla strony www.wwsi.edu.pl odpowiada adres IP o wartości 62.29.141.146.
3. Klient po otrzymaniu właściwego adresu IP wysyła do serwera WWW zapytanie o możliwość otwarcia strony www.wwsi.edu.pl.
4. Serwer WWW po zweryfikowaniu właściwego skojarzenia strony WWW z adresem IP odsyła klientowi zgodę na otwarcie żądanej strony internetowej.

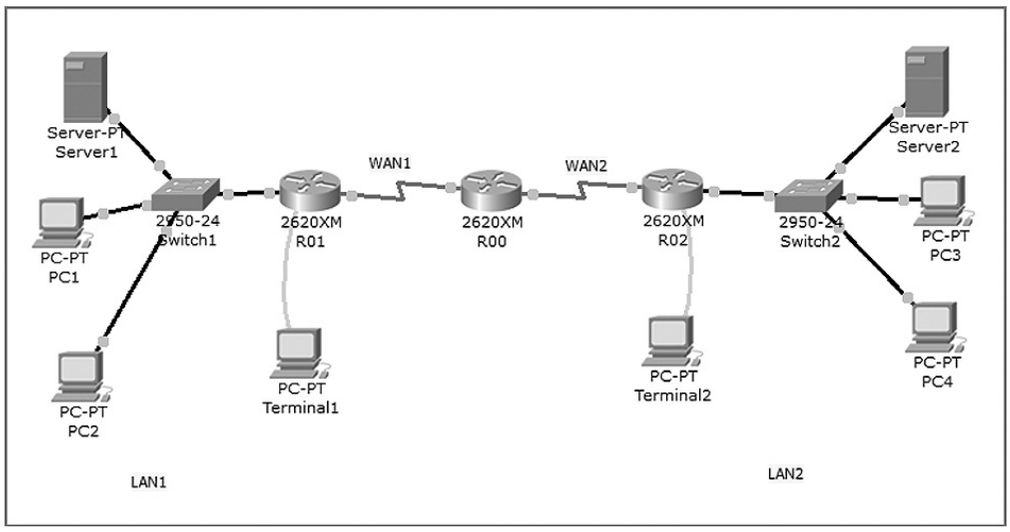
LITERATURA

1. Dye M.A., McDonald R., Rufi A.W., *Akademia sieci Cisco. CCNA Exploration. Semestr 1*, WN PWN, Warszawa 2008
2. Graziani R., Vachon B., *Akademia sieci Cisco. CCNA Exploration. Semestr 4*, WN PWN, Warszawa 2009
3. Krysiak K., *Sieci komputerowe. Kompendium*, Helion, Gliwice 2005
4. Reid A., *CCNA semestr 4. Sieci rozległe – technologie WAN*, WN PWN, Warszawa 2007
5. *Vademecum teleinformatyka*, IDG Poland SA, Warszawa 1999

WARSZTATY

1 PRAKTYCZNE ASPEKTY IMPLEMENTACJI PROTOKOŁÓW WAN NA URZĄDZENIACH SIECIOWYCH

Ćwiczenie 1. Interaktywny model stworzony indywidualnie przez uczestników z wykorzystaniem oprogramowania Packet Tracer (firmy Cisco Systems).



Rysunek 40.
Model topologii sieci

Ćwiczenie 2. Konfiguracja protokołu HDLC.

```
INFORMATYKA+_00(config)#interface serial 0/0
INFORMATYKA+_00(config-if)#encapsulation HDLC

INFORMATYKA+_00#show interfaces s0/0 (sprawdzenie stanu interfejsu)
Serial0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 10.10.10.2/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of „show interface” counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 68 bits/sec, 0 packets/sec
  5 minute output rate 69 bits/sec, 0 packets/sec
     203 packets input, 16384 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     210 packets output, 16836 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up DSR=up DTR=up RTS=up CTS=up
```

Ćwiczenie 3. Konfiguracja protokołu PPP (pomiędzy routerami R00 i R01).

INFORMATYKA+_00(config)#interface serial 0/0
INFORMATYKA+_00(config-if)#encapsulation ppp (włączenie enkapsulacji PPP)

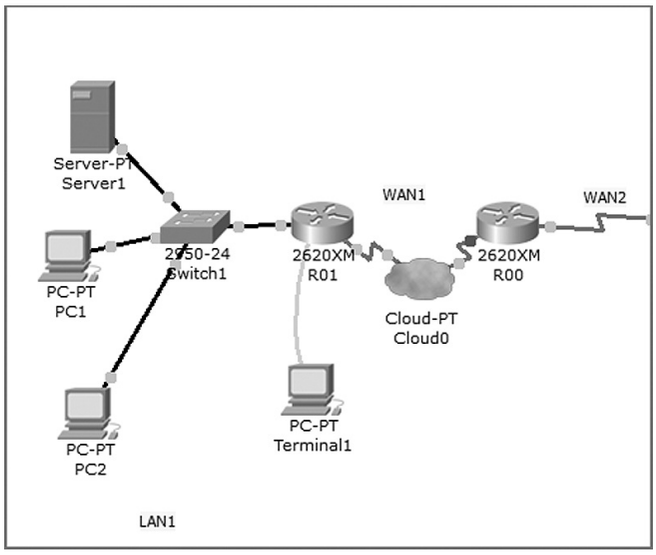
Serial0/0 PPP: Using default call direction
Serial0/0 PPP: Treating connection as a dedicated line
Serial0/0 PPP: Phase is ESTABLISHING, Active OpenINFORMATYKA+_00(config-if)#
Serial0/0 LCP: State is Open
Serial0/0 PPP: Phase is FORWARDING, Attempting Forward
Serial0/0 Phase is ESTABLISHING, Finish LCP
Serial0/0 Phase is UP
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
00:12:49: %OSPF-5-ADJCHG: Process 200, Nbr 192.168.1.1 on Serial0/0 from EXCHANGE to FULL, Exchange Done

INFORMATYKA+_01(config-if)#encapsulation ppp (włączenie enkapsulacji PPP na drugim interfejsie)

Serial0/0 PPP: Using default call direction
Serial0/0 PPP: Treating connection as a dedicated line
Serial0/0 PPP: Phase is ESTABLISHING, Active OpenINFORMATYKA+_01(config-if)#
Serial0/0 LCP: State is Open
Serial0/0 PPP: Phase is FORWARDING, Attempting Forward
Serial0/0 Phase is ESTABLISHING, Finish LCP
Serial0/0 Phase is UP
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
00:12:49: %OSPF-5-ADJCHG: Process 200, Nbr 10.10.10.5 on Serial0/0 from EXCHANGE to FULL, Exchange Done

INFORMATYKA+_00#show interfaces s0/0 (sprawdzenie stanu interfejsu)
Serial0/0 is up, line protocol is up (connected)
 Hardware is HD64570
 Internet address is 10.10.10.2/30
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
 Encapsulation PPP, loopback not set, keepalive set (10 sec)
 LCP Open
 Open: IPCP, CDPCP
 Last input never, output never, output hang never
 Last clearing of „show interface” counters never
 Input queue: 0/75/0 (size/max/drops); Total output drops: 0
 Queueing strategy: weighted fair
 Output queue: 0/1000/64/0 (size/max total/threshold/drops)
   Conversations 0/0/256 (active/max active/max total)
   Reserved Conversations 0/0 (allocated/max allocated)
 5 minute input rate 64 bits/sec, 0 packets/sec
 5 minute output rate 61 bits/sec, 0 packets/sec
   99 packets input, 8032 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   98 packets output, 7840 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 output buffer failures, 0 output buffers swapped out
   0 carrier transitions
   DCD=up DSR=up DTR=up RTS=up CTS=up

Ćwiczenie 4. Konfiguracja protokołu Frame Relay.



Rysunek 41.
Topologia sieci dla Frame Relay

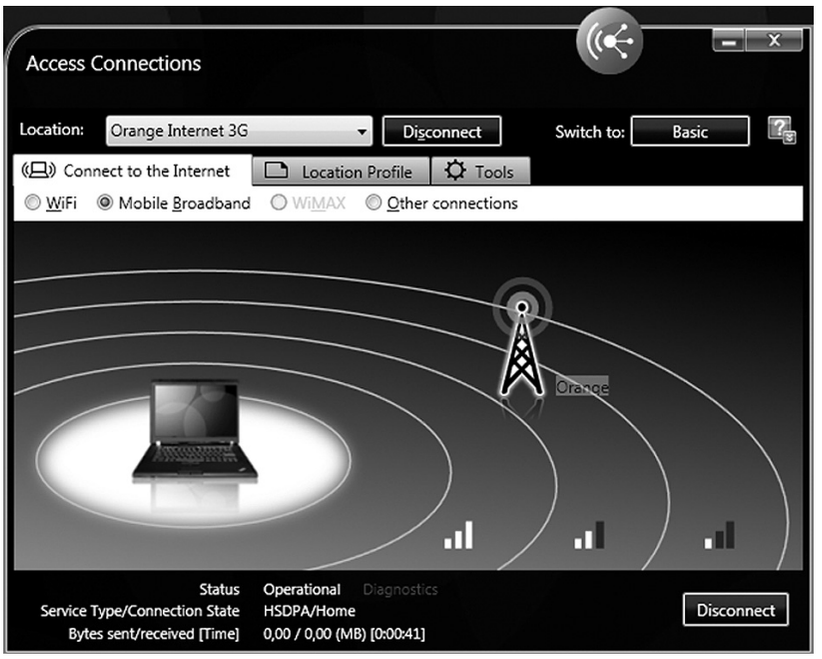
```
INFORMATYKA+_00#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
INFORMATYKA+_00(config)#interface s0/0
INFORMATYKA+_00(config-if)#encapsulation frame-relay
INFORMATYKA+_00(config-if)#end

INFORMATYKA+_01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
INFORMATYKA+_01(config)#interface s0/0
INFORMATYKA+_01(config-if)#encapsulation frame-relay
INFORMATYKA+_01(config-if)#end

INFORMATYKA+_00#show int s 0/0
Serial0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 10.10.10.2/30
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation Frame Relay, loopback not set, keepalive set (10 sec)
  LMI enq sent  91, LMI stat recvd 89, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  Broadcast queue 0/64, broadcasts sent/dropped 0/0, interface broadcasts 0
  Last input never, output never, output hang never
  Last clearing of „show interface” counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     34 packets input, 2780 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
33 packets output, 2604 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

2 MOBILNE SIECI WAN

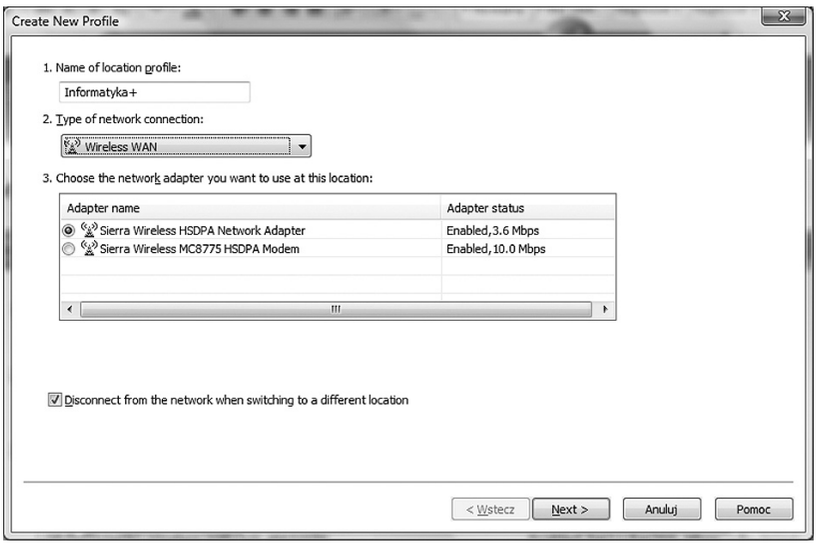
Ćwiczenie 5. Konfiguracja sieci WWAN w notebooku.

Krok 1. Uruchamiamy narzędzie do zarządzania komunikacją i połączeniami (rys. 42).



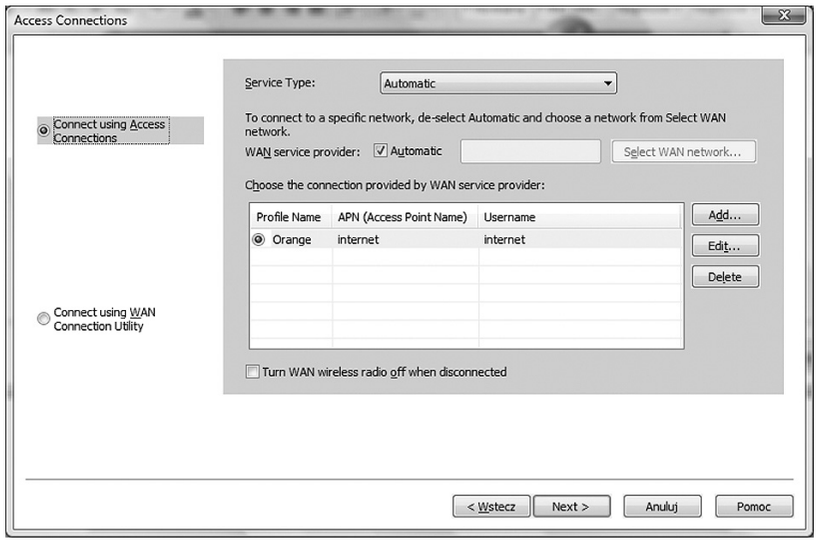
Rysunek 42.
Okno aplikacji do zarządzania połączeniami (Lenovo ThinkPad)

Krok 2. Tworzymy nowy profil (rys. 43).



Rysunek 43.
Tworzenie nowego profilu

Krok 3. Wybieramy operatora (rys. 44).

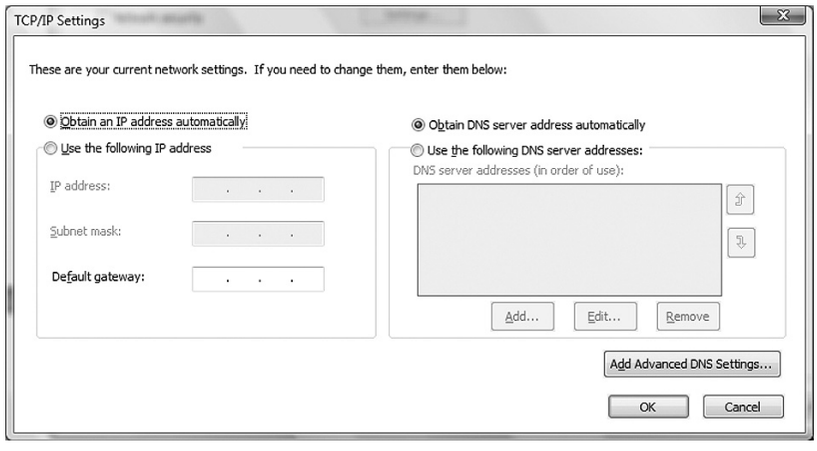


Rysunek 44.
Wybór operatora

Krok 4. Edytujemy parametry profilu (rys. 45).

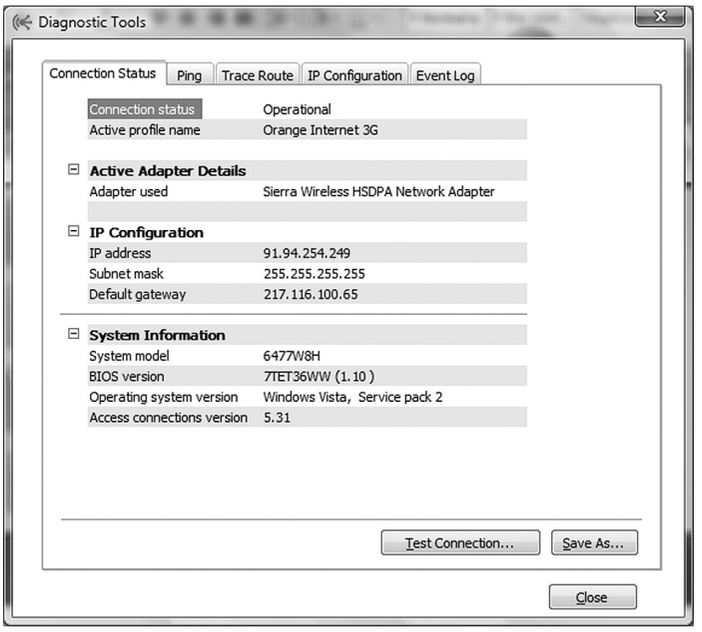
Rysunek 45.
Ustawianie parametrów profilu

Krok 5. Konfigurujemy parametry protokołu TCP/IP (rys. 46).



Rysunek 46.
Konfiguracja parametrów protokołu TCP/IP

Krok 6. Diagnostyka połączenia (rys. 47).



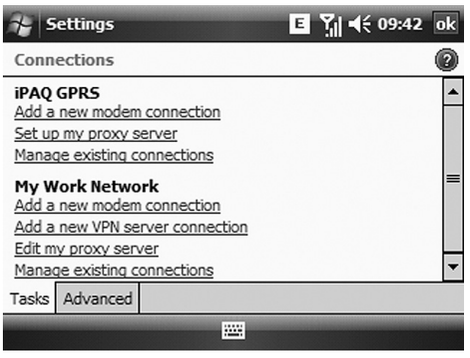
Rysunek 47.
Diagnostyka konfiguracji

Ćwiczenie 6. Konfiguracja sieci WWAN w telefonie komórkowym (Windows Mobile Professional 6.1).

Krok 1. W panelu ustawień przechodzimy do zakładki połączenia (rys. 48).

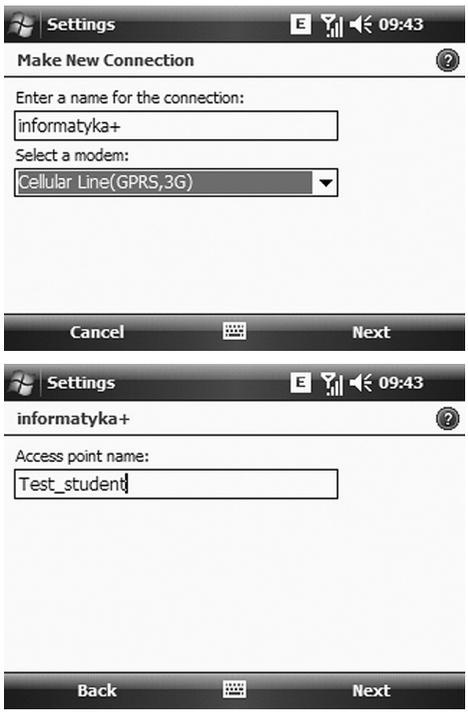
Rysunek 48.
Wybór rodzaju połączenia

Krok 2. Wybieramy dodaj nowe połączenie modemowe (rys. 49).



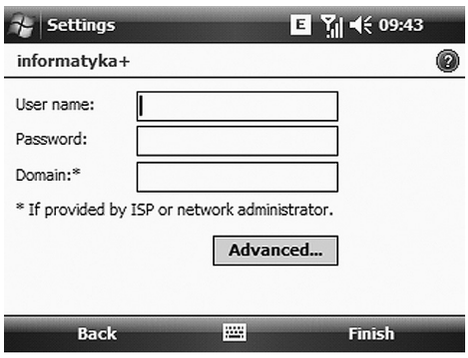
Rysunek 49.
Dodanie nowego połączenia

Krok 3. Tworzymy nowe połączenie wraz z nowym punktem dostępowym (rys. 50).



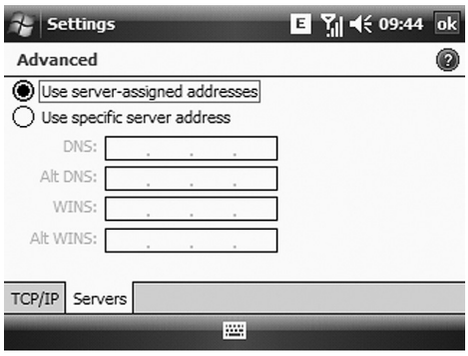
Rysunek 50.
Tworzenie nowego połączenia

Krok 4. Wpisujemy parametry konta (rys. 51).



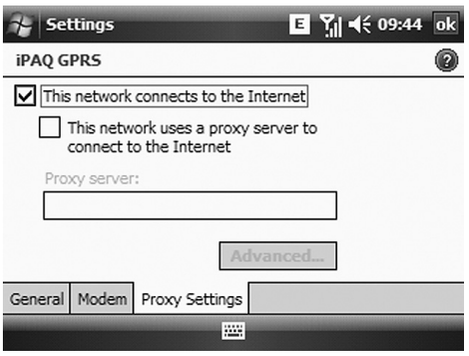
Rysunek 51.
Parametryzacja konta użytkownika

Krok 5. Konfigurujemy parametry protokołu IP oraz serwera DNS (rys. 52).

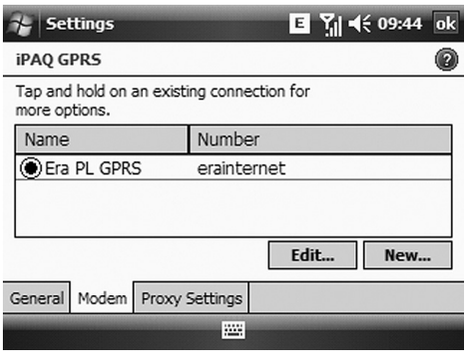


Rysunek 52.
Konfiguracja parametrów protokołu IP

Krok 6. Ustawiamy parametry dodatkowe połączenia (rys. 53, 54).



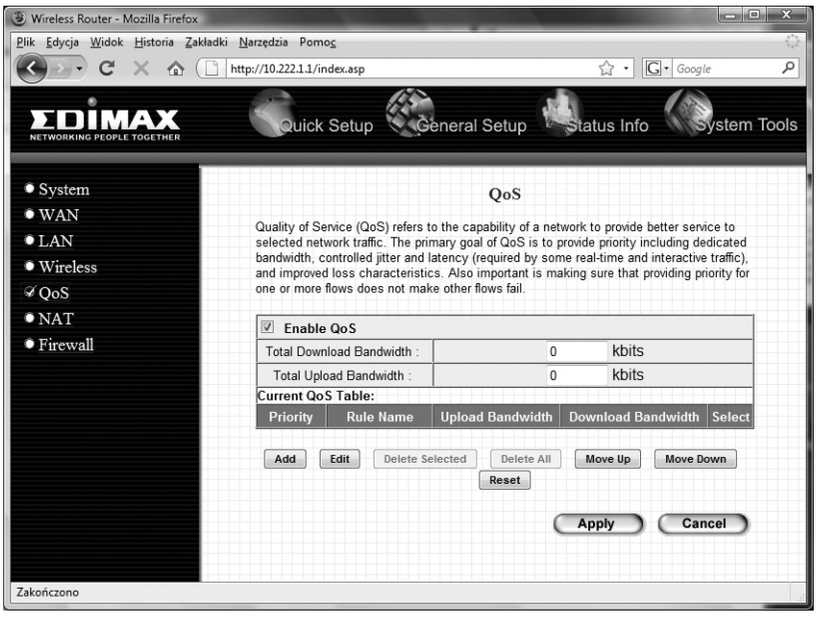
Rysunek 53.
Finalizacja tworzenia połączenia



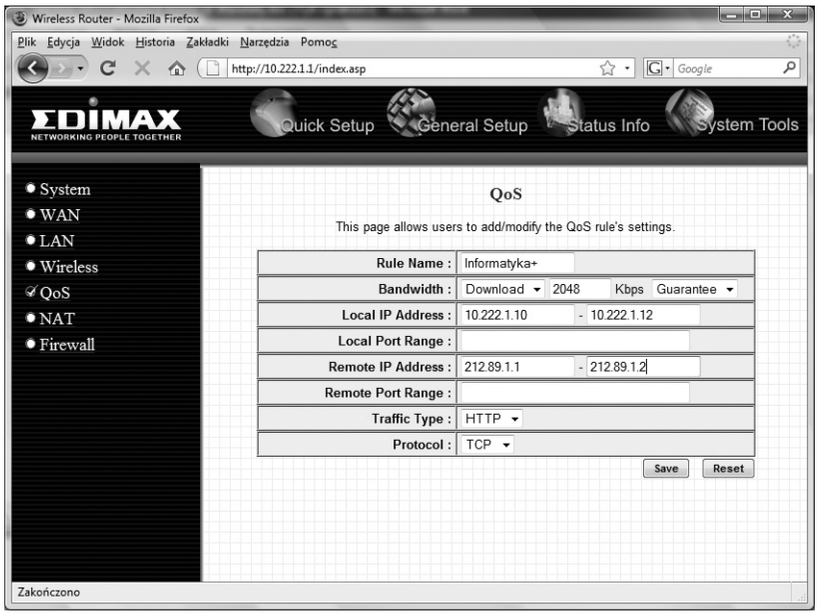
Rysunek 54.
Finalizacja parametryzacji połączenia

3 STEROWANIE RUCHEM W SIECIACH KOMPUTEROWYCH. ZAPEWNIENIE GWARANTOWANEJ JAKOŚCI USŁUG.

Ćwiczenie 7. Konfiguracja **QoS** (ang. *Quality of Service*) na aktywnym urządzeniu sieciowym (rys. 55, 56).



Rysunek 55.
Okno konfiguracji routera bezprzewodowego



Rysunek 56.
Dodanie tablicy QoS

4 LISTY DOSTĘPU ACL

Ćwiczenie 8. Utworzenie listy ACL (ang. *Access Control List*).

INFORMATYKA+_01#**ip access-list extended test**

INFORMATYKA+_01#(config-ext-nacl)#**permit ip any host 192.168.1.101**
INFORMATYKA+_01#(config-ext-nacl)#**permit ip any host 192.168.1.11**
INFORMATYKA+_01#(config-ext-nacl)#**permit ip any host 192.168.1.12**

Ćwiczenie 9. Sprawdzenie listy ACL.

INFORMATYKA+_01#**sh ip access-lists**
Extended IPaccess list test
permit ip any host **192.168.1.101**
permit ip any host **192.168.1.11**
permit ip any host **192.168.1.12**

Usunięcie linii drugiej:

INFORMATYKA+_01#ip access-list extended test
INFORMATYKA+_01#(config-ext-nacl)#no permit ip any host **192.168.1.11**

Ponowne sprawdzenie zawartości listy:

INFORMATYKA+_01#sh ip access-lists
Extended IPaccess list test
permit ip any host **192.168.1.101**
permit ip any host **192.168.1.12**

Dostęp do linii wirtualnych routera
Omawiane do tej pory listy dostępu służyły do filtrowania ruchu przechodzącego przez router. Istnieje jednak

możliwość filtrowania ruchu przychodzącego do samego routera (np. telnet na linie wirtualne). Dla tego typu ruchu mogą byc zastosowane tylko standardowe listy dostęp. Aby zezwolic na połączenie telnet tylko ze stacji o IP 192.168.14.2 na RouterA, konfiguracja listy będzie wyglądać następująco:

Ćwiczenie 10. Konfiguracja listy ACL.

INFORMATYKA+_01#(config)#**access-list 2 permit 192.168.1.11**

INFORMATYKA+_01#**line vty 0 4**
INFORMATYKA+_01#**access-class 2 in**

5 IMPLEMENTACJA MECHANIZMÓW BEZPIECZEŃSTWA

Ćwiczenie 11. Konfiguracja protokołu SSH dla konsoli wirtualnego terminala routera.

INFORMATYKA+_01(config)#ip domain-name wwsi.pl
INFORMATYKA+_01(config)#crypto key generate rsa
The name for the keys will be: INFORMATYKA+_01.wwsi.pl
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

INFORMATYKA+_01(config)#username student password 12345678
INFORMATYKA+_01(config)#line vty 0 4
INFORMATYKA+_01(config-line)#transport input ssh
INFORMATYKA+_01(config-line)#login local
INFORMATYKA+_01(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
Konfiguracja protokołu PPP z autentykacją PAP (pomiędzy routerami R00 i R01)
INFORMATYKA+_00(config)#interface serial 0/0
INFORMATYKA+_00(config-if)#encapsulation ppp (włączenie enkapsulacji PPP)
INFORMATYKA+_00(config-if)#ppp authentication pap
INFORMATYKA+_00(config-if)# ppp sent-username I_00 password test
INFORMATYKA+_00(config-if)#end

INFORMATYKA+_01(config)#interface serial 0/0
INFORMATYKA+_01(config-if)#encapsulation ppp (włączenie enkapsulacji PPP)
INFORMATYKA+_01(config-if)#ppp authentication pap
INFORMATYKA+_01(config-if)# ppp sent-username I_01 password test
INFORMATYKA+_01(config-if)#end

6 KONFIGURACJA PROTOKOŁU PPP Z AUTENTYKACJĄ CHAP

CHAP (ang. *Challenge Handshake Authentication Protocol*) – to jeden z dwóch (obok PAP) sposobów uwierzytelniania w PPP. CHAP zapewnia węzłom zgłaszanie swojej tożsamości za pomocą trójfazowego uzgadniania. CHAP jest bezpiecznym protokołem uwierzytelniania, zapewnia ochronę przed atakami wykorzystującymi podsłuch transmisji, wykorzystuje MD5. Jest preferowany jako uwierzytelnianie w PPP

Ćwiczenie 12. Konfiguracja protokołu PPP.

INFORMATYKA+_00(config)#username INFORMATYKA+_02 password 12345678

```
INFORMATYKA+_00(config)#interface serial 0/1
INFORMATYKA+_00(config-if)#encapsulation ppp (włączenie enkapsulacji PPP)
INFORMATYKA+_00(config-if)#ppp authentication chap
INFORMATYKA+_00(config-if)#end

INFORMATYKA+_02(config)#username INFORMATYKA+_00 password 12345678
INFORMATYKA+_02(config)#interface serial 0/1
INFORMATYKA+_02(config-if)#encapsulation ppp (włączenie enkapsulacji PPP)
INFORMATYKA+_02(config-if)#ppp authentication chap
INFORMATYKA+_02(config-if)#end
```

W projekcie **Informatyka +**, poza wykładami i warsztatami, przewidziano następujące działania:

- 24-godzinne kursy dla uczniów w ramach modułów tematycznych
- 24-godzinne kursy metodyczne dla nauczycieli, przygotowujące do pracy z uczniem zdolnym
- nagrania 60 wykładów informatycznych, prowadzonych przez wybitnych specjalistów i nauczycieli akademickich
- konkursy dla uczniów, trzy w ciągu roku
- udział uczniów w pracach kół naukowych
- udział uczniów w konferencjach naukowych
- obozy wypoczynkowo-naukowe.

Szczegółowe informacje znajdują się na stronie projektu

www.informatykaplus.edu.pl