Ćwiczenie 3 Sieć TCP/IP w Windows XP Pro

Cel ćwiczenia:

Zapoznanie się z konfiguracją sieci w Windows XP. Poznanie konfiguracji protokołu TCP/IP.

Przed przystąpieniem do ćwiczenia uczeń powinien umieć:

- poruszać się po systemie Windows XP,
- zarządzać kontami użytkowników i grup,
- zarządzać zabezpieczeniami folderów i plików.

Po wykonaniu ćwiczenia uczeń będzie umiał:

- omówić model ISO/OSI, zastosowanie sprzętu sieciowego, adresację w protokole TCP/IP,
- zainstalować protokół TCP/IP,
- skonfigurować adresację i rozpoznawanie nazw TCP/IP,
- skonfigurować host wieloadresowy,
- skonfigurować protokół IPSec,
- rozwiązywać problemy z protokołem TCP/IP,
- udostępniać zasoby dyskowe w grupie roboczej,
- dołączyć się do domeny.

Uwagi o realizacji ćwiczenia:

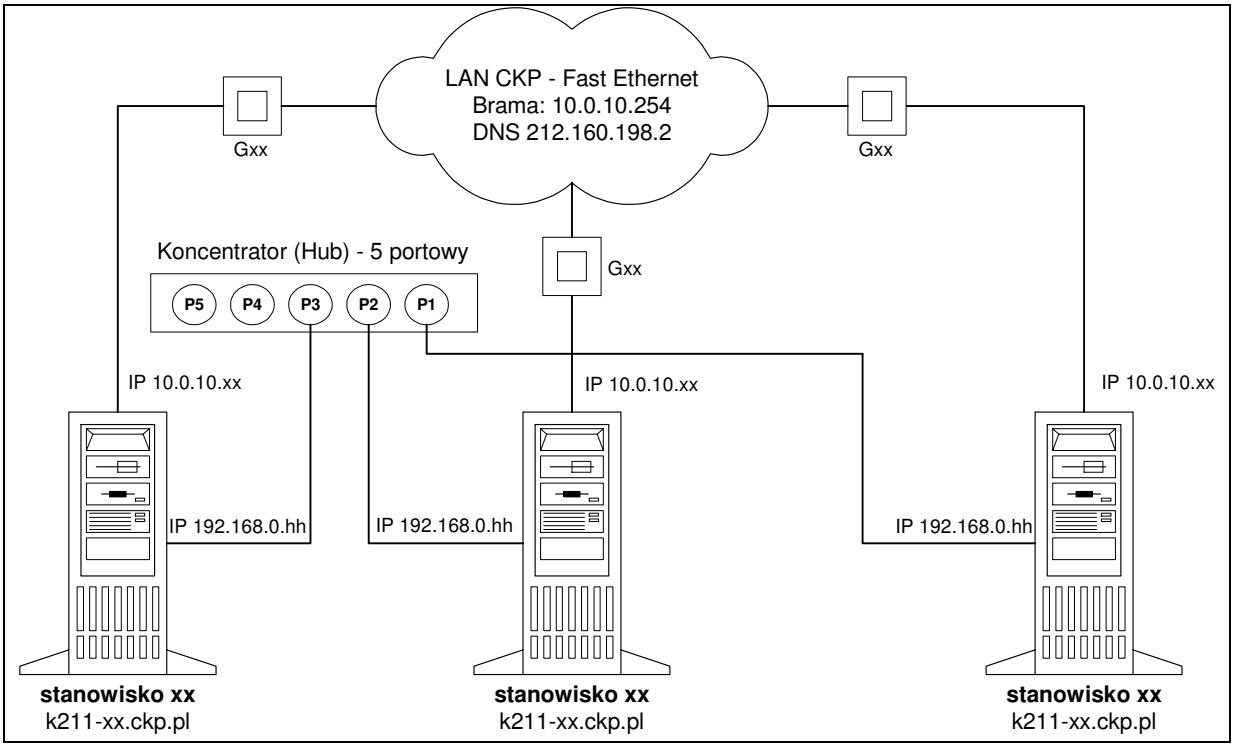
Ćwiczenie podzielone jest na rozdziały. Rozdział zbudowany jest z opisu teoretycznego omawiającego wybrane zagadnienie i zadania do wykonania. Zadania umieszczone są w ramkach. Po wykonaniu zadania uczeń zobowiązany jest do przeprowadzenia samooceny, korzystając z punktacji 1-5. Nauczyciel może skorygować ocenę ucznia. Na końcu ćwiczenia znajduje się spis zadań.

W czasie tego ćwiczenia uczniowie pracują na oddzielnych komputerach wyposażonych w dwie karty sieciowe firmy. Jedna z kart powinna być podłączona do sieci LAN CKP, druga do koncentratora (huba) łączącego 3 sąsiednie komputery. Dokładną konfigurację stanowisk przedstawia rysunek 3.1

Przed przystąpieniem do ćwiczenia uczeń powinien odświeżyć swój komputer z obrazu Windows XP Pro PL.

W czasie ćwiczenia uczeń ma do dyspozycji:

- płytę z obrazem Windows XP Pro PL.



Rys. 3.1 Konfiguracja stanowisk (xx to numer komputera, hh to numer portu huba)

3.1 Wstęp

3.1.a Sieć LAN i WAN

Najprościej mówiąc, sieć to grupa połączonych ze sobą komputerów lub innych urządzeń peryferyjnych. Przy definicji sieci często mówi się o łączeniu stacji (host). Host to nie tylko komputer umożliwiający pracę interaktywną, ale także urządzenie udostępniające usługi: np. serwery druku czy serwery plików.

Ze względu na rozmiar i rodzaje połączeń, sieci dzielimy na sieci lokalne (LAN – Local Area Network) i rozległe (WAN- Wide Area Network).

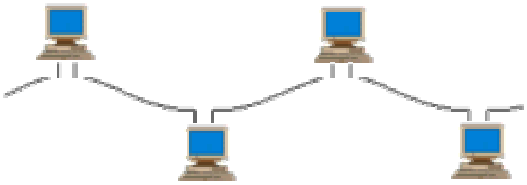
Sieci LAN łączą użytkowników na niewielkim obszarze (pomieszczenie, piętro, budynek). Zasięg ograniczony jest to kilku kilometrów. Sieci te charakteryzują się przede wszystkim małym kosztem, prostym oprogramowaniem komunikacyjnym i łatwością rozbudowy. Jest kilka specyfikacji określających charakterystykę sieci lokalnych. Do najpopularniejszych należą Ethernet i Fast Ethernet.

WAN **-** jest to sieć, która przekracza granice miast, państw, kontynentów (największą siecią rozległą jest sieć Internet). Sieć taka składa się z węzłów i łączących je łączy transmisyjnych. Dostęp do sieci rozległej uzyskuje się poprzez dołączenie systemów użytkownika do węzłów sieci. W węzłach znajdują się urządzenia umożliwiające przesyłanie danych między różnymi użytkownikami. Łączność pomiędzy węzłami realizowana jest za pomocą publicznej sieci telefonicznej, specjalnie zestawionych łączy, kanałów satelitarnych, radiowych lub innych.

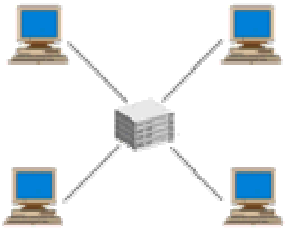
3.1.b Topologie sieci

- Topologia magistrali (szynowa)

Topologie magistrali wyróżnia to, że wszystkie węzły sieci połączone są ze sobą za pomocą pojedynczego, otwartego (umożliwiającego przyłączenie kolejnych urządzeń) kabla. Kabel ten obsługuje tylko jeden kanał i nosi on nazwę magistrali. Oba końce magistrali muszą być zakończone opornikami ograniczającymi, zwanymi również często terminatorami. W przypadku uszkodzenia kabla, przestaje działać cała sieć.



Rys. 3.2 Sieć połączona w magistralę



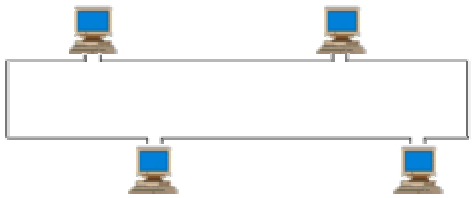
Rys. 3.3 Sieć połączona w gwiazdę

- Topologia gwiazdy

Połączenie sieci LAN o topologii gwiazdy, z przyłączonymi do niej urządzeniami, rozchodzą się z jednego, wspólnego punktu, którym jest koncentrator (hub).W przypadku uszkodzenia jednego z kabli, tylko jeden komputer przestaje działać. W przypadku awarii huba, nie działa cała sieć. Topologie gwiazdy stały się dominującym we współczesnych sieciach LAN rodzajem topologii. Są one elastyczne, skalowalne i stosunkowo tanie.

- Topologia pierścienia

Każda przyłączona do sieci stacja robocza ma w ramach takiej topologii dwa połączenia, po jednym dla każdego ze swoich najbliższych sąsiadów. Połączenie takie musiało tworzyć fizyczną pętlę, czyli pierścień. Dane przesyłane były, wokół pierścienia, w jednym kierunku. Każda stacja robocza pobiera i odpowiada na pakiety do nich zaadresowane, a także przesyła dalej pozostałe pakiety do następnej stacji roboczej, wchodzącej w skład sieci.



Rys. 3.4 Sieć połączona w pierścień

3.1.c Ethernet

Obecnie najbardziej popularnym rodzajem sieci lokalnych są sieci Ethernet i Fast Ethernet. Są one zbliżone pod względem sposobu definiowania założeń działania sieci, a dzieli je bardzo istotny parametr – szybkość transmisji. Ethernet może przesyłać dane z prędkością do 10Mb/s, a Fast Ethernet do 100 Mb/s.

W sieciach typu Ethernet stacje robocze wysyłają dane w trybie rozgłoszeniowym (broadcastowym). Inne stacje wsłuchują się w rozsyłane dane, i odbierają tylko pakiety przeznaczone dla siebie. Gdy jeden użytkownik nadaje komunikat do innego użytkownika, jest on rozsyłany rozgłoszeniowo do wszystkich stacji.

Ethernet jest siecią typu rywalizującego, gdzie wszystkie węzły w danym segmencie rywalizują ze sobą o dostęp do sieci - w przypadku, gdy dwa komputery próbują komunikować się w tym samym czasie, następuje kolizja, komputery muszą się wycofać i zaprzestać transmisji. Sieć ta korzysta przy tym z protokołu CSMA/CD (Carrier-Sense Multiple Access with Collision Detection).

Stacje robocze monitorują aktywność sieci (nasłuchują) w celu ustalenia, czy mogą transmitować dane, czy nie. Jeśli w danej chwili żaden z komputerów nie przesyła informacji, wybrana stacja może rozpocząć nadawanie, nikomu nie przeszkadzając. Gdy dwie stacje próbują przesyłać dane jednocześnie, dochodzi do kolizji, co powoduje chwilowe zatrzymanie transmisji. Po określonym czasie transmisja jest wznawiana. Za czas wstrzymania wysyłki odpowiedzialna jest każda stacja robocza, wobec tego wystąpienie powtórnej kolizji jest mało prawdopodobne.

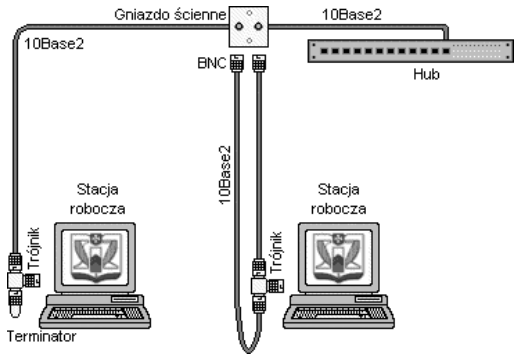
Informacje są przesyłane w postaci impulsów cyfrowych. Zbiór impulsów nazywamy ramką. Ramka sieci Ethernet może mieć wielkość od 64 do 1518 bajtów. Każdy przesyłany siecią pakiet zawiera pole z adresem odbiorcy i adresem nadawcy. Pozwala to na zlokalizowanie komputera, dla którego informacja jest przeznaczona, oraz prawidłowe doręczenie tej informacji. Wszystkie karty sieciowe mają 12-cyfrowy (6-bajtowy), unikatowy w skali światowej adres, co wyklucza możliwość błędnego dostarczenia wysyłanych pakietów. Adres ten zwany jest adresem sprzętowym MAC (Media Access Control). Adresy komunikujących się stacji składają się z dwóch części: pola opisującego producenta oraz numeru seryjnego (np. 00-01-02-DB-61-A9). W każdej ramce poza sekcją zawierającą identyfikator nadawcy i odbiorcy, znajduje się sekcja zawierająca przesyłane dane. Jej wielkość waha się od 46 do 1500 bajtów.

3.1.d Okablowanie

Medium transportowym w sieciach Ethernet jest kabel koncentryczny (mniejsze szybkości transmisji), skrętka oraz światłowód. Podstawowym typem topologii jest magistrala oraz gwiazda (obecnie najczęściej stosowana).

- Kabel koncentryczny

Kabel współosiowy zbudowany jest z pojedynczego, centralnego przewodu miedzianego, otoczonego warstwą izolacyjną. Kabel ten jest ekranowany. W celu odizolowania od zewnętrznych pól elektromagnetycznych stosuje się cienką siatkę miedzianą. W użyciu znajdują się dwa rodzaje kabli koncentrycznych: o oporności falowej 50 Ω (w sieciach komputerowych) i 75 Ω (wykorzystywany w TV-SAT). Sieć Ethernet definiuje dwie specyfikacje:



Rys. 3.5 Przykładowe połączenie dla kabla koncentrycznego – topologia: magistrala

- 10BASE-2 zwany jest cienkim koncentrykiem. Grubość: 0.25", impedancja: 50 Ω, przepustowość: 10 Mb/s, maksymalna długość jednego segmentu sieci to 185 m, a przyłączonych do niego może być 30 komputerów.
- 10BASE-5 zwany jest grubym koncentrykiem. Grubość: 10 mm, impedancja: 50 Ω, przepustowość: 10 Mb/s, maksymalna długość jednego segmentu sieci to 500 m, a przyłączonych do niego może być 100 komputerów

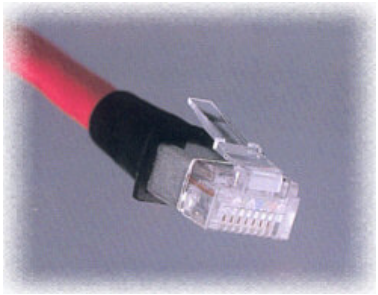
- Skrętka

Skrętka, zwana też w zależności od przepustowości 10BASE-T, 100BASE-T lub 1000BASE-T, to obecnie najpopularniejsze medium transmisyjne. Używana jest także w telefonii. Wyróżnia się dużą niezawodnością i niewielkimi kosztami realizacji sieci. Składa się z: od 2 do nawet kilku tysięcy par skręconych przewodów, umieszczonych we wspólnej osłonie. Istnieją 2 rodzaje tego typu kabla: ekranowany (STP, FTP) i nieekranowany (UTP). Różnią się one tym, iż ekranowany posiada folię ekranującą, a pokrycie ochronne jest lepszej jakości, więc w efekcie zapewnia mniejsze straty transmisji i większą odporność na zakłócenia. Mimo to, powszechnie stosuje się skrętkę UTP.

Przepustowość skrętki zależna jest od tzw. kategorii. Skrętka kategorii 1 to kabel telefoniczny, natomiast kategorii 2 przeznaczona jest do transmisji danych z szybkością 4 Mb/s, kategorii 3 do transmisji o przepustowości do 10 Mb/s, kategorii 4 do 16 Mb/s, kategorii 5 do ponad 100 Mb/s - ten typ ma zastosowanie w szybkich sieciach np. Fast Ethernet. Natomiast skrętka kategorii 6 - 622 Mb/s przeznaczona jest dla sieci ATM.

Maksymalna długość połączeń dla UTP wynosi 100 m, natomiast dla STP 250 m. Limit ten można przekroczyć, używając repeatera. Obydwa rodzaje skrętki posiadają impedancję 100 ohmów. Do karty sieciowej skrętkę przyłączą się za pomocą złącza RJ-45. Skrętkę stosuje się przede wszystkim w sieciach o topologii gwiazdy, więc uszkodzenie jednego połączenia z zasady nie wpływa na pracę całej sieci.

Rys. 3.6 Sieć oparta na skrętce z odległą stacją – topologia: gwiazda



Rys. 3.7 Złącze RJ-45

- Światłowód

W światłowodach, do transmisji informacji, wykorzystywana jest wiązka światła, która jest odpowiednikiem prądu w innych kablach. Wiązka ta jest modulowana zgodnie z treścią przekazywanych informacji. To rozwiązanie otworzyło nowe możliwości w dziedzinie tworzenia szybkich i niezawodnych sieci komputerowych. Właściwie dobrany

kabel może przebiegać w każdym środowisku. Szybkość transmisji może wynosić nawet 3 Tb/s. Sieci oparte na światłowodach zwane są FDDI. Światłowód wykonany ze szkła kwarcowego, składa się z rdzenia (złożonego z jednego lub wielu włókien), okrywającego go płaszcza oraz warstwy ochronnej. Dielektryczny kanał informatyczny eliminuje konieczność ekranowania.

Budując sieć Ethernet, można korzystać, ze światłowodu. Niezbędny będzie wówczas Tranceiver, który pobiera dane ze światłowodu i zamienia je na sygnały elektryczne. Długość połączeń może wzrosnąć aż do 20 km.

3.1.e Sprzęt sieciowy

- Karta sieciowa

Nazywana jest również adapterem sieciowym (NIC – Network Interface Adapter) Jest to urządzenie wymagane we wszystkich stacjach roboczych przyłączonych do sieci. Każda karta jest przystosowana tylko do jednego typu sieci i posiada niepowtarzalny numer, który identyfikuje zawierający ją komputer (adres MAC). Istnieją karty sieciowe przystosowane zarówno do magistrali ISA, jak i PCI. Karty pod PCI wyróżniają się wyższą wydajnością i mniejszym obciążeniem procesora stacji. Obecnie karty sieciowe posiadają własny procesor i pamięć RAM. Procesor pozwala przetwarzać dane bez angażowania w to głównego procesora komputera, a pamięć pełni rolę bufora w sytuacji, gdy karta nie jest w stanie przetworzyć napływających z sieci dużych ilości danych. Są one wtedy tymczasowo umieszczane w pamięci.

Na karcie sieciowej znajduje się złącze dla medium transmisyjnego. Często, aby zapewnić zgodność karty z różnymi standardami okablowania producenci umieszczają 2 lub 3 typy takich złącz. Obecnie najpopularniejsze są RJ-45 i BNC**.**

Rys. 3.8 Złącza na karcie sieciowej.

Głównym zadaniem karty sieciowej jest transmisja i rozszyfrowywanie informacji biegnących łączami komunikacyjnymi. Przesyłanie danych rozpoczyna się od uzgodnienia parametrów transmisji pomiędzy stacjami (np. prędkość, rozmiar pakietów). Następnie dane są przekształcane na sygnały elektryczne, kodowane, kompresowane i wysyłane do odbiorcy. Tak więc karta odbiera i zamienia pakiety na bajty zrozumiałe dla procesora stacji roboczej.

- Koncentrator (Hub)

Jest to urządzenie posiadające wiele portów, służących do przyłączania stacji roboczych zestawionych przede wszystkim w topologii gwiazdy. W zależności od liczby komputerów przyłączonych do sieci, może się okazać konieczne użycie wielu hubów. W sieci takiej nie ma bezpośrednich połączeń pomiędzy stacjami . Komputery podłączone są przy pomocy jednego kabla do centralnego huba, który po nadejściu sygnału rozprowadza go do wszystkich linii wyjściowych.

Dużą zaletą takiego rozwiązania jest fakt, iż przerwanie komunikacji między jednym komputerem a hubem nie powoduje awarii całej sieci, ponieważ każda stacja posiada z nim oddzielne połączenie. Ponadto każdy pakiet musi przejść przez hub, więc możliwa jest kontrola stanu poszczególnych odcinków sieci. Jednak uszkodzenia huba unieruchomi całą sieć.

Można wyróżnić huby pasywne i aktywne. Hub pasywny jest tanim urządzeniem, pełniącym funkcję skrzynki łączeniowej, nie wymaga zasilania. Hub aktywny, dodatkowo wzmacnia sygnały ze stacji roboczej i pozwala na wydłużenie połączenia z nią. Zasilanie jest wymagane.

Najczęstszym rodzajem kabla łączącego komputer i hub jest skrętka . Huby potrafią jednak dokonać konwersji sygnału pochodzącego z różnych mediów transmisyjnych. Huby są na ogół przyłączane do innych hubów.

- Przełącznik (switch), hab przełączający.

Ogólnie przełącznik jest urządzeniem sieciowym odbierającym przychodzące pakiety, tymczasowo je przechowujący i wysyłający do odpowiedniego portu. Przełączniki są zbliżone wyglądem do koncentratorów. W przeciwieństwie do nich analizują otrzymane ramki, aby kontrolować ruch w sieci. Uczą się, do którego z portów podłączeni są adresaci informacji, a następnie kierują przesyłanie danych wyłącznie do wskazanych odbiorców. Stosowanie ich w sieci poważnie ogranicza niepotrzebny ruch, gdyż dane nie są rozsyłane do wszystkich portów urządzenia.

Potencjalna przepustowość przełącznika jest określana przez sumaryczną przepustowość każdego z portów. Na przykład 16-portowy przełącznik Fast Ethernet posiada zagregowaną przepustowość 1,6 Gb/s (przy założeniu działania w trybie pół-dupleksu i bez innych ograniczeń związanych z architekturą), podczas gdy 16-portowy koncentrator Fast Ethernet posiada przepustowość tylko 100 Mb/s. Przełącznik może być jednak ograniczony przez swoją architekturę.

Przełączniki są bardzo użyteczne do budowania dużych i niezawodnych sieci LAN, ponieważ oferują one najniższą cenę za megabajt przepustowości ze wszystkich istniejących komponentów sieciowych. Przełączniki Ethernet i Fast Ethernet są także użyteczne w zapewnianiu stałych transferów w sieci takich, jak na przykład transmisje obrazu. Jest tak dzięki temu, że zapewniają one każdemu portowi stałą przepustowość.

- Repeater (wzmacniak)

Wzmacniak, to zazwyczaj niewielkie, posiadające dwa porty, urządzenie elektroniczne służące do łączenia dwóch segmentów kabla sieciowego. Urządzenie to regeneruje (wzmacnia) sygnały cyfrowe transmitowane w kablu. Po wykonaniu tej czynności, przesyła już wzmocniony sygnał do następnego segmentu sieci lokalnej. Dzięki temu możliwe jest powiększenie zasięgu sieci. W standardzie Ethernet, w pojedynczym segmencie sieci, sygnały możemy przesyłać na odległość do 500 metrów. Po zastosowaniu repeatera, odległość zostaje zwiększona do 1000 metrów. Niestety wzmacniaki wprowadzają pewne opóźnienia sygnału i nie można stosować ich w nieskończoność. Wiąże się to między innymi z mechanizmem wykrywania kolizji. Jeżeli opóźnienie sygnału będzie zbyt duże, mechanizm ten nie będzie w stanie prawidłowo działać. Repeatery mogą łączyć segmenty sieci opartych na różnych nośnikach fizycznych. Na przykład, do jednego z portów koncentratora możemy podłączyć kabel koncentryczny sieci Ethernet, natomiast do drugiego światłowód.

- Most (bridge)

Mosty są urządzeniami możliwościami przypominające wzmacniaki. Tak samo jak one, pośredniczą pomiędzy dwoma segmentami sieci. Jednak mosty posiadają dużo większe możliwości. Największą ich zaletą jest zdolność do filtrowania pakietów, przesyłając je z jednego segmentu sieci do drugiego jeżeli zachodzi taka potrzeba, przez co uzyskujemy zmniejszenie niepotrzebnego ruchu w segmencie. Na przykład, jeżeli występuje komunikacja między stacjami znajdującymi się w tym samym segmencie, most nie wysyła pakietów do innego segmentu. Most analizuje adresy fizyczne kart sieciowych i na tej podstawie decyduje, czy dany pakiet powinien zostać przesłany do innego segmentu, czy nie. Mosty miały szerokie zastosowanie w sieciach o topologii magistrali. Most jest ewolucyjnym poprzednikiem przełącznika, obecnie jest rzadko stosowany, zastępują go szybkie przełączniki.

- Router

Zadaniem routerów jest rozsyłanie informacji. Decyzja, gdzie przesłać ramkę, oparta jest na analizie protokołu i adresu sieci. Dokładniej mówiąc, routery łączą co najmniej dwa logiczne segmenty sieci. Router może wykonywać wszystkie funkcje mostu i więcej, co pozwala na używanie go w wielu różnych aplikacjach. Router różni się od mostu możliwością analizy nagłówka protokołu. To umożliwia routerowi podział sieci w oparciu o adresy sieci i hosta. Ta właściwość pozwala używać routera do trzech funkcji:

- Zwiększania segmentacji sieci

Routery były od początku wykorzystywane do segmentowania sieci na podsieci. To umożliwia im filtrowanie ramek rozgłoszeniowych i utrzymuje w odizolowaniu mniejszą liczbę użytkowników, co poprawia wydajność tych segmentów.

- Routowania pomiędzy różnymi sieciami LAN

Kolejną zaletą routerów jest możliwość łączenia różnych sieci opartych na pakietach. Routery są zwykle używane do łączenia sieci Ethernet i Token Ring. Router przyjmuje nadchodzącą ramkę i przechowuje ją w pamięci. Następnie usuwa on z ramki wszystko, poza polem danych i opakowuje te dane w ramkę innego standardu sieciowego. Następnie wysyła ją do właściwego portu. Routery w takiej konfiguracji nie są przeźroczyste dla sieci, ale muszę być jawnie adresowane. Dlatego, jeżeli użytkownik sieci Ethernet będzie chciał wysłać dane do użytkownika sieci Token Ring, będzie musiał wysłać je do routera, który łączy dwie sieci LAN.

- Łączenie z sieciami WAN

Routery odgrywają także ważną rolę w połączeniach WAN. Łącza WAN mają zwykle mniejszą przepustowość niż sieć lokalna ze względu na to, że koszt uzyskania tej przepustowości jest tutaj znacznie wyższy. Ponieważ routery najlepiej filtrują pakiety, są one najlepszymi urządzeniami pełniącymi rolę bram. Routery WAN mogą także wykonywać takie funkcje, jak kompresja, czy szyfrowanie. Czasami routery w takiej konfiguracji nazywa się bramami.

3.1.f Model ISO/OSI

Organizacja ISO opracowała Model Referencyjny Połączonych Systemów Otwartych (model OSI – Open System Interconection) w celu ułatwienia realizacji otwartych połączeń systemów komputerowych. Organizacja przepływu danych podlega siedmiowarstwowemu modelowi łączenia systemów otwartych, który zakłada przesyłanie danych z aplikacji (programu) na jednym komputerze do aplikacji na drugim komputerze przez medium transmisyjne. Open oznacza, iż dwa dowolne systemy spełniające warunki standardu ISO mogą wzajemnie się komunikować przy pomocy dowolnego medium transmisyjnego np. kabel miedziany, światłowód, droga radiowa, system satelitarny lub inny. Każda warstwa definiuje funkcję wykonywaną podczas przekazywania danych za pośrednictwem sieci między współpracującymi ze sobą aplikacjami. Inaczej mówiąc, model OSI dzieli zadanie przesyłania informacji między stacjami sieciowymi na siedem mniejszych zadań, składających się na poszczególne warstwy. Zadania te nie definiują konkretnego protokołu, czyli nie precyzują one dokładnie, jak dany fragment oprogramowania pełniący zadania jednej z warstw ma działać, ale tylko co - ma wykonywać.

Nazwa warstwy modelu OSI	Numer warstwy
Aplikacji	7
Prezentacji	6
Sesji	5
Transportu	4
Sieci	3
Łącza danych	2
Fizyczna	1

- *Warstwa fizyczna*

Warstwa najniższa nazywana jest warstwą fizyczną. Jest ona odpowiedzialna za przesyłanie strumieni bitów. Odbiera ramki danych z warstwy 2, czyli warstwy łącza danych, i przesyła szeregowo, bit po bicie, całą ich strukturę oraz zawartość przez medium transmisyjne. Jest ona również odpowiedzialna za odbiór kolejnych bitów przychodzących strumieni danych. Strumienie te są następnie przesyłane do warstwy łącza danych w celu ich ponownego ukształtowania. W warstwie tej działają karty sieciowe, koncentratory (huby), wzmacniaki (repeatery) i tranceivery.

- *Warstwa łącza danych*

Druga warstwa modelu OSI nazywana jest warstwą łącza danych. Jak każda z warstw, pełni ona dwie zasadnicze funkcje: odbierania i nadawania. Warstwa ta jest odpowiedzialna za upakowanie strumienia danych przychodzącego z warstwy fizycznej w tzw. ramki. Każda ramka zawiera adres nadawcy i odbiorcy. Pozwala to na zlokalizowanie komputera, dla którego informacja jest przeznaczona. Dodatkowo zapewnia niezawodność łącza danych. Definiuje mechanizmy kontroli błędów

w przesyłanych ramkach - CRC (*Cyclic Redundancy Check*). Jest ona ściśle powiązana z warstwą fizyczną, która narzuca topologię np. Ethernet. W warstwie tej działają sterowniki (*drivery*) kart sieciowych oraz mosty (*bridge*) i przełączniki (*switche*).

- *Warstwa sieci*

Warstwa sieci jest odpowiedzialna za określenie trasy transmisji między nadawcą, a odbiorcą. Warstwa ta nie ma żadnych wbudowanych mechanizmów korekcji błędów i w związku z tym musi polegać na wiarygodnej transmisji końcowej warstwy łącza danych. Warstwa sieci używana jest do komunikowania się z komputerami znajdującymi się poza lokalnym segmentem sieci LAN (np. przez sieć rozległą WAN). Ramki przychodzące z warstwy drugiej otrzymują unikalny adres w całej sieci, dzięki czemu mogą zostać dostarczone do odległych systemów. Warstwa ta przetwarza informacje w porcjach zwanych pakietami. Ponadto odpowiedzialna jest za trasowanie (*routing*) pakietów w sieci, czyli wyznaczenie optymalnej trasy dla połączenia. W tej warstwie działa protokół IP wykorzystywany przez największą sieć WAN – Internet. W warstwie sieciowej działają routery i zarządzalne przełączniki.

- *Warstwa transportu*

Warstwa ta pełni funkcję podobną do funkcji warstwy łącza w tym sensie, że jest odpowiedzialna za końcową integralność transmisji. Jednak w odróżnieniu od warstwy łącza danych - warstwa transportu umożliwia tę usługę również poza lokalnymi segmentami sieci LAN. Potrafi bowiem wykrywać pakiety, które zostały przez routery odrzucone i automatycznie generować żądanie ich ponownej transmisji. Warstwa transportu identyfikuje oryginalną sekwencję pakietów i ustawia je w oryginalnej kolejności przed wysłaniem ich zawartości do warstwy sesji. W tej warstwie działa protokół TCP.

- *Warstwa sesji*

Piątą warstwą modelu OSI jest warstwa sesji. Jest ona rzadko używana; wiele protokołów funkcje tej warstwy dołącza do swoich warstw transportowych. Zadaniem warstwy sesji modelu OSI jest zarządzanie przebiegiem komunikacji, podczas połączenia miedzy dwoma komputerami. Przepływ tej komunikacji nazywany jest sesją. Warstwa ta określa, czy komunikacja może zachodzić w jednym, czy obu kierunkach. Gwarantuje również zakończenie wykonywania bieżącego żądania przed przyjęciem kolejnego.

- *Warstwa prezentacji*

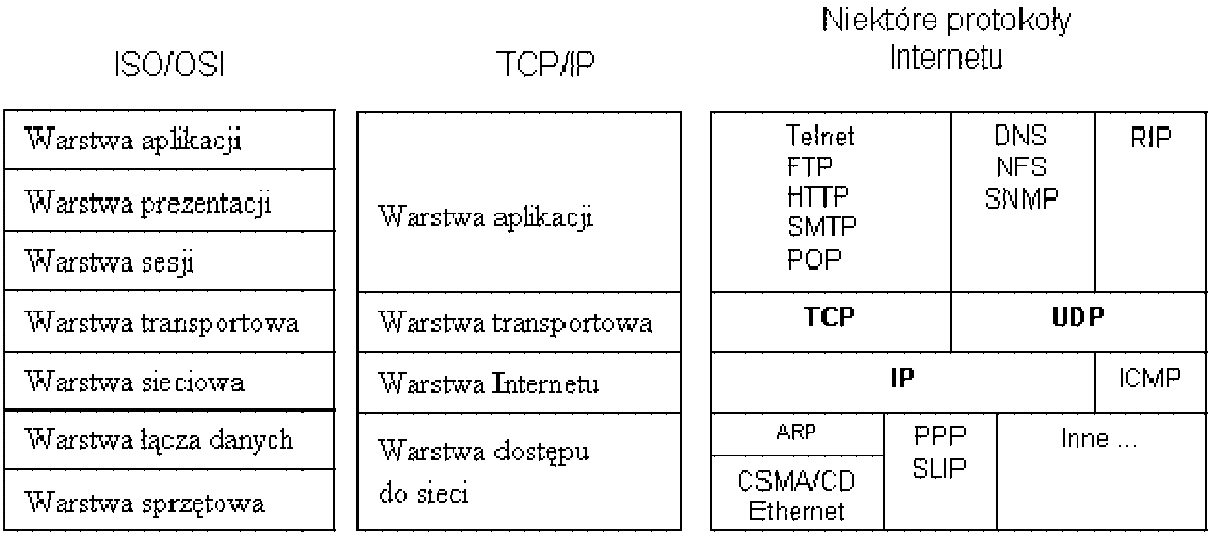
Zapewnia tłumaczenie danych, definiowanie ich formatu oraz odpowiednią składnię. Umożliwia przekształcenie danych na postać standardową, niezależną od aplikacji. Rozwiązuje takie problemy, jak niezgodność reprezentacji liczb, znaków końca wiersza, liter narodowych itp. Odpowiada także za kompresję i szyfrowanie.

- *Warstwa aplikacji*

Najwyższą warstwą modelu OSI jest warstwa aplikacji. Pełni ona rolę interfejsu pomiędzy aplikacjami użytkownika a usługami sieci. Warstwę tę można uważać za inicjującą sesje komunikacyjne. W warstwie tej działają protokoły HTTP, FTP, NNTP, TELNET, SMTP, POP3.

3.1.g Protokół TCP/IP

Protokół, z którego korzysta Internet - TCP/IP można opisać za pomocą siedmio-warstwowego modelu ISO/OSI. Lepiej jednak funkcje i właściwości protokołu TCP/IP oddaje uproszczony model cztero-warstwowy. W modelu tym najważniejsze są warstwy *sieciowa* i *transportowa*, pozostałe są połączone i tworzą dwie warstwy zwane *warstwą dostępu do sieci* oraz *warstwą aplikacji*. Funkcje tych warstw pokrywają się z zadaniami odpowiadających im warstw w modelu ISO/OSI.



Rys. 3.9 Porównanie modelu ISO/OSI i modelu TCP/IP

Podobnie jak w modelu OSI kolejne warstwy dołączają bądź usuwają (w zależności w którą stronę przesuwają się dane na stosie protokołów) własne nagłówki. Taki proces nazywa się enkapsulacją danych. Jednak model czterowarstwowy, poprzez zintegrowanie funkcjonalne niektórych warstw, o wiele lepiej obrazuje ten proces dla protokołu TCP/IP. Każda warstwa ma swoją terminologię, określającą dane aktualnie przez nią obrabiane. Ponieważ protokół TCP/IP składa się z dwóch głównych protokołów warstwy transportowej TCP i UDP, więc również w nazewnictwie wprowadzony został podział.

Warstwa	**TCP**	**UDP**
Aplikacji	strumień	wiadomość
Transportowa	segment	pakiet
Internetu	datagram	
Dostępu do sieci	ramka	

3.1.h Adresacja IP

Adresy wszystkich komputerów w Internecie są wyznaczane przez właściwości protokołu IP. Adres IP składa się z czterech liczb dziesiętnych z zakresu 0-255 przedzielonych kropkami (np. 212.160.198.1). Można go również zapisać jako jeden ciąg 32 bitów lub też cztery ciągi po osiem bitów każdy, przedzielone kropkami.

Każdy taki adres można podzielić na dwie części:
- część identyfikującą daną sieć w Internecie,
- część identyfikującą konkretny komputer w tej sieci.

Podział ten wynika z faktu, że każde przedsiębiorstwo, które otrzymuje adresy Internetowe do własnego wykorzystania, otrzymuje tylko jakiś wydzielony zakres tych adresów, określany mianem: przestrzeń adresowa.

- Klasy adresów w TCP/IP

Pierwotnie bity określające sieć i bity wyznaczające komputer były rozróżniane za pomocą tzw. klas adresów IP. Klasy były definiowane za pomocą kilku pierwszych bitów adresu. Na podstawie ich wartości oprogramowanie określało klasę adresu, a tym samym, które bity odpowiadają za adres podsieci, a które za adres hosta.

```
0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh  –  klasa A
10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh  –  klasa B
110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh  –  klasa C
1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx  –  multicast
1111xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx  –  adresy zarezerwowane
n – bit należący do adresu sieci,
h – bit należący do adresu hosta.
```

W ten sposób, na podstawie wartości N pierwszego bajtu adresu IP możemy zdefiniować, do jakiej klasy należy dany adres:

N < 128 – klasa A
128 < N < 191 – klasa B
192 < N < 223 – klasa C
224 < N < 239 – multicast (transmisja grupowa, wykorzystywana przy np.: wideo-konferencjach)
N > 239 – adresy zarezerwowane

W pewnym momencie rozwoju Internetu okazało się, że ten sposób przydzielania adresów sieci jest bardzo nieekonomiczny. Dostępne klasy adresów zaczęły się bardzo szybko kurczyć. Wprowadzono system zwany: bezklasowym routowaniem międzydomenowym CIDR (*Classless Inter-Domain Routing*). Pojawiło się pojęcie maski sieci. Maska sieci składa się podobnie jak adres IP z 4 bajtów. Używana jest do wydzielenia części adresu odpowiadającej za identyfikację sieci i części odpowiadającej za identyfikację komputera z adresu IP.

```
Adres IP:    212.51.219.50
Maska sieci: 255.255.255.192
Adres IP:    11010100.00110011.11011011.00110010
Maska:       11111111.11111111.11111111.11000000
Adres sieci: 11010100.00110011.11011011.00000000
Broadcast:   11010100.00110011.11011011.00111111
Adres sieci: 212.51.219.0
Broadcast:   212.51.219.63
```

Adres sieci tworzymy, przepisując niezmienione wszystkie bity adresu IP, dla których odpowiednie bity maski mają wartość jeden. Resztę uzupełniamy zerami. Adres broadcast jest adresem rozgłoszeniowym sieci. Używa się go do jednoczesnego

zaadresowania wszystkich komputerów w danej sieci (jest przetwarzany przez wszystkie komputery w sieci). Tworzymy go podobnie do adresu sieci, jednak dopełniamy jedynkami zamiast zerami.

Mając adres sieci i adres broadcast możemy łatwo wyznaczyć możliwy zakres numerów IP komputerów w danej sieci. Dla podanych powyżej adresów sieci i broadcast, komputerów w sieci mogą przyjmować adresy IP od numeru: 212.51.219.1 do 212.51.219.62.

Adres 212.51.219.50 z maską 255.255.255.192 możemy w skrócie zapisać 212.51.219.50/26. W tym przypadku ostatnia liczba oznacza ilość bitów o wartości jeden w masce.

- Adresy specjalne, klasy nieroutowalne

Istnieją pewne adresy, których nie można wykorzystać do normalnych zastosowań (przydzielić ich komputerom). Dla danej sieci (przestrzeni adresowej) takim adresem jest adres sieci. W omawianym przykładzie tym adresem jest 212.51.219.0; adres ten symbolizuje całą sieć. Drugim takim adresem jest wyznaczony powyżej broadcast, czyli adres rozgłoszeniowy. Każdy datagram IP o tym adresie zostanie odczytany i przetworzony przez wszystkie komputery danej sieci. Adres sieci i broadcast zmieniają się w zależności od aktualnej przestrzeni adresowej.

Ponadto adresem specjalnego przeznaczenia jest adres: 0.0.0.0. Oznacza on wszystkie komputery w Internecie. Często podczas odczytywania tablicy routingu zastępowany jest on słowem: „*default*".

Następnym adresem specjalnym jest 127.0.0.1. Jest to adres pętli (*loop-back address*). Adres ten służy do komunikacji z wykorzystaniem protokołu IP z lokalnym komputerem (*localhost*). Jest on zawsze przypisany komputerowi, na którym właśnie pracujemy. Ponieważ pakiety z takimi adresami nie powinny wydostawać się na zewnątrz komputera, nie powoduje to żadnych konfliktów.

Należy również pamiętać o adresach, klasach adresów multicast i zarezerwowanych, których też nie możemy wykorzystać do normalnych zastosowań.

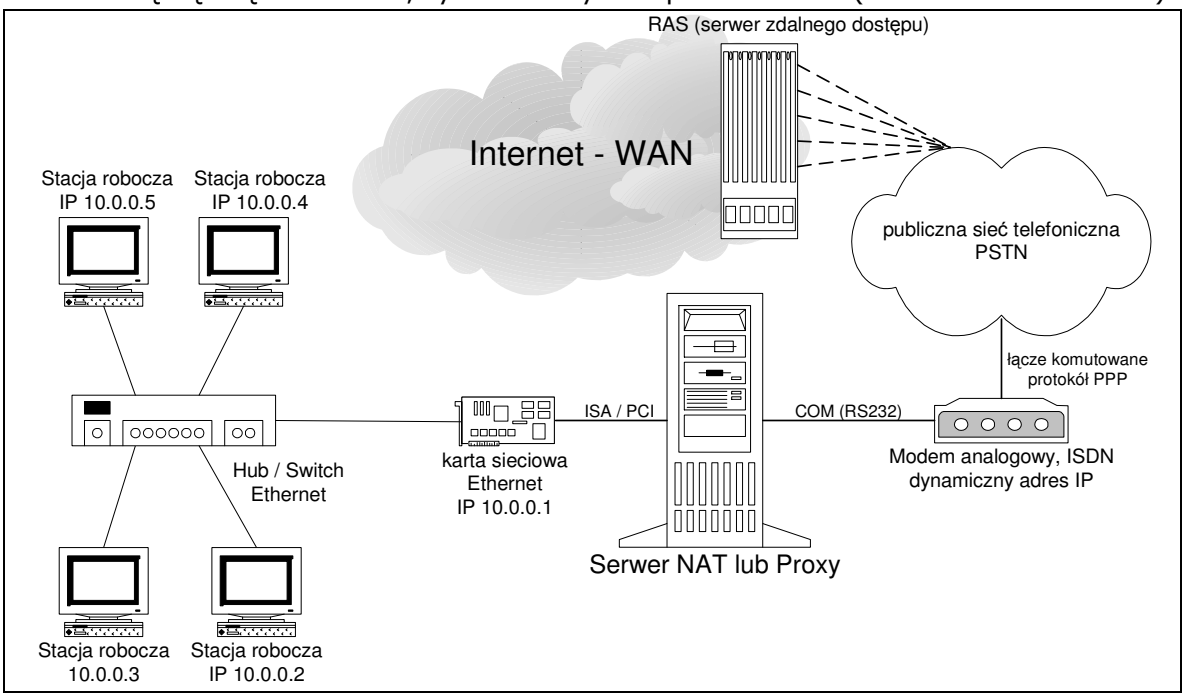
Pewna grupa adresów została zarezerwowana do powszechnego wykorzystania. Można z wykorzystaniem tych adresów budować lokalne intranety (sieci IP świadczące takie same usługi jak Internet, ale dla pojedynczego przedsiębiorstwa). Adresy te czasem nazywane są adresami nieroutowalnymi. Nazwa ta powstała, ponieważ pakiety z takich sieci nie powinny być przekazywane przez routery. Wynika stąd, że możemy założyć sobie sieć przestrzenią adresową z takiego zakresu i sieć ta nie będzie widziana na zewnątrz w Internecie.

```
A   255.0.0.0         10.  0.0.0 –  10.255.255.255
B   255.255.0.0      172. 16.0.0 – 172. 31.255.255
C   255.255.255.0    192.168.0.0 – 192.168.255.255
```

3.1.i Dostęp do Internetu

Najprostszą metodą dostępu do Internetu jest wykorzystanie modemu analogowego lub cyfrowego ISDN i połączenie się z dostawcą Internetu (np. TP S.A., Dialog) przez publiczną sieć telefoniczną PSTN (Public Switched Telephony Network). Tego typu dostęp nazywany jest dostępem komutowanym.

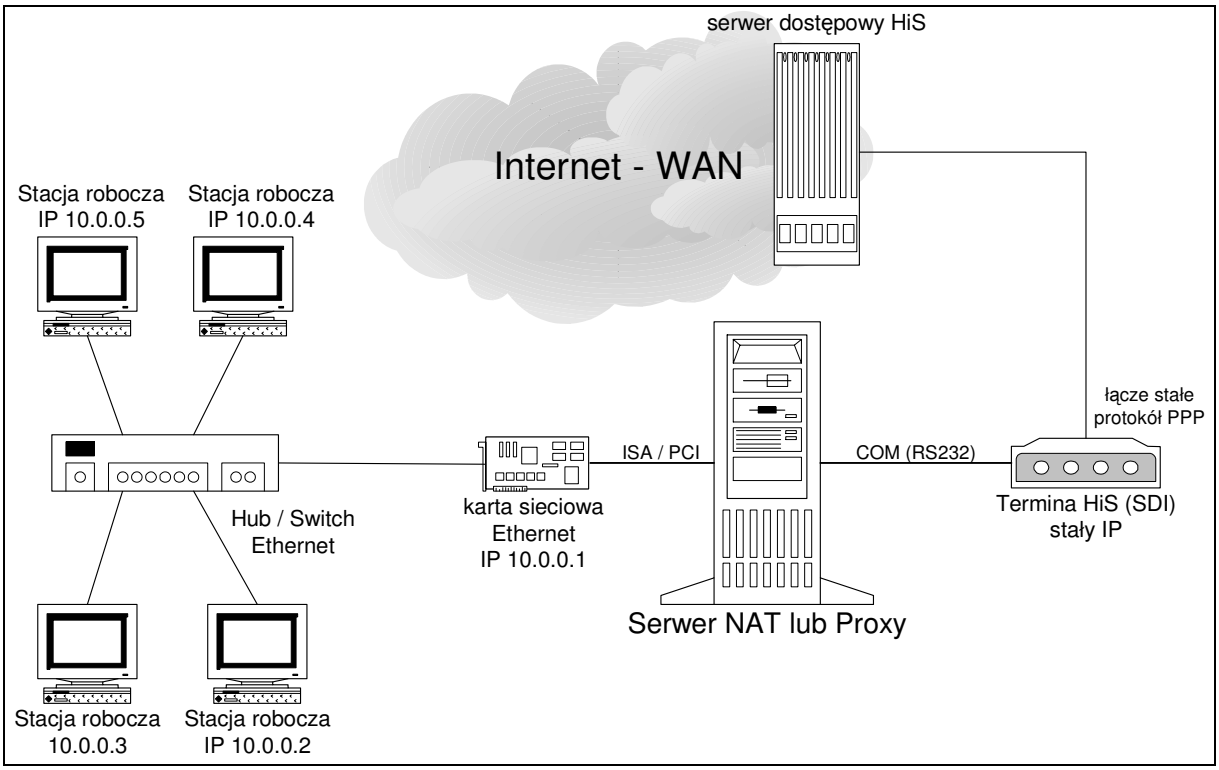
Dzwoniąc na odpowiedni numer, można połączyć komputer z Internetem (dla TP S.A. i modemu analogowego to 0202122, dla modemu ISDN – 0202422). Po nawiązaniu połączenia, serwer zdalnego dostępu automatycznie konfiguruje połączenie sieciowe, dynamicznie przypisuje adres IP. Dlatego też po rozłączeniu i ponownym połączeniu przypisany adres IP jest innym. Brak stałego adresu uniemożliwia podłączenie w ten sposób serwera udostępniającego usługi internetowe, którego działanie wymaga stałego adresu IP. Łącząc się modemem, system korzysta z protokołu PPP (Point To Point Protocol).



Rys. 3.10 Dostęp komutowany do Internetu

Chcąc udostępnić połączenie z Internetem sieci lokalnej, komputer z podłączonym modemem musi pełnić rolę serwera NAT (Network Address Translation) lub Proxy. Serwer NAT zamienia adresy pakietów IP kierowanych do Internetu, z adresów lokalnych na adres IP, wykorzystywany przez połączenie modemowe. W momencie przyjścia odpowiedzi dokonuje odwrotnej translacji. NAT obsługiwany jest przez usługę udostępniania połączenia internetowego (ICS - Internet Connection Sharing) dostępną w systemach Windows 98SE/ME/2000/XP, a także w serwerach Windows 2000/2003, Linux. Inna metoda udostępnienia Internetu wykorzystywana w Windows NT to oprogramowanie Proxy Server instalowane na serwerze i Client Proxy Server instalowany na stacjach roboczych.

Najprostszym stałym połączeniem z Internetem jest usługa SDI TP S.A. wykorzystująca system HiS (Home internet Solution) firmy Ericsson. Terminal HiS podłączony jest na stałe parą kabli miedzianych z systemem dostępowym operatora. W połączeniu SDI wykorzystywany jest protokół PPP i jeden stały adres IP, dzięki czemu przez SDI można podłączyć serwer internetowy.



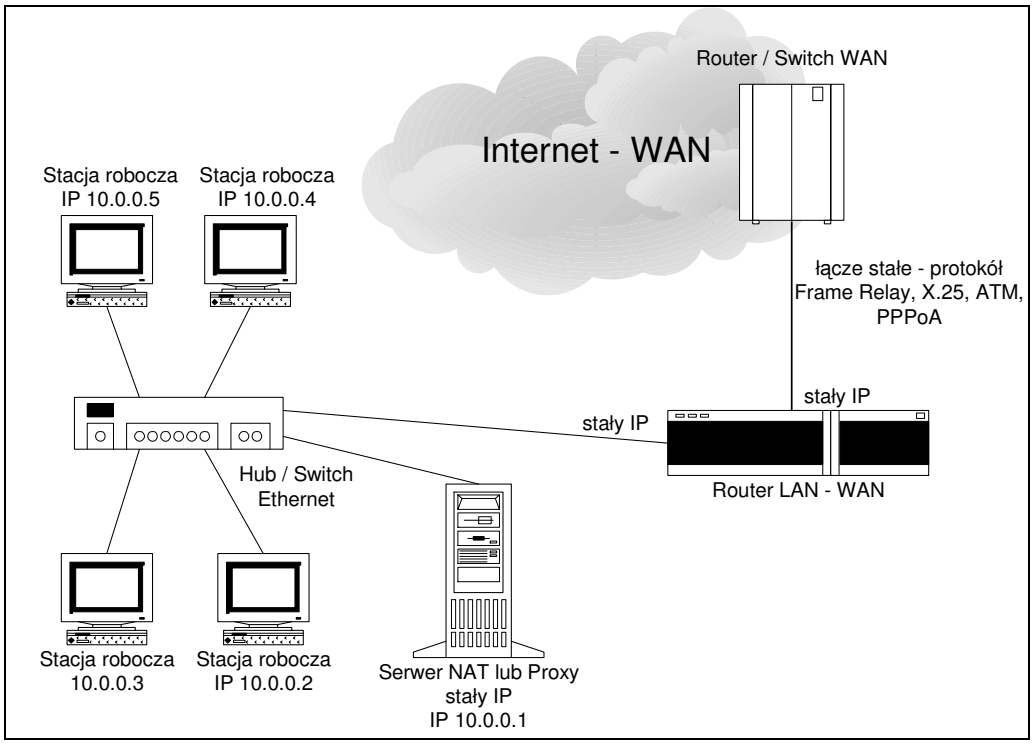
Rys. 3.11 Dostęp stały do Internetu przez usługę SDI

Od kilku lat na świecie, a także w Polsce, dużą popularnością cieszą się usługi DLS (Digital Subscriber Line - cyfrowe łącze abonenckie), a w szczególności ADSL - asymetryczne cyfrowe łącze abonenckie. Asymetryczność polega na tym, że szybkość transmisji z Internetu do komputera klienta jest większa niż przesyłu danych z komputera klienta do Internetu. Rozwiązanie to stało się bardzo popularne, gdyż nie ingeruje w istniejącą infrastrukturę telefoniczną. Pod zakończenie kabla miedzianego (idącego z centrali telefonicznej, wykorzystywanego przez linię telefoniczną), podłącza się modem ADSL, który przez port Ethernet lub USB łączony jest z komputerem.

Telekomunikacja Polska udostępnia dwie usługi ADSL:

- Neostrada Plus – usługa ta kierowana jest do klientów indywidualnych i małych firm. Za pomocą specjalnego modemu ADSL uzyskujemy szybkie połączenie z Internetem.
- DSL TP – usługa kierowana do małych i średnich firm. Za pomocą łącza ADSL i routera możemy podłączyć nie tylko jeden komputer, ale także sieć lokalną, z serwerem internetowym.

Inna metoda dostępu do Internetu (profesjonalna) to skorzystanie z sieci WAN operatora (np. Polpak-T TP S.A.), wykorzystującej protokół Frame Relay. Aby podłączyć sieć lokalną, należy zainstalować router, który połączy sieć Ethernet z siecią Frame Relay. Od operatora otrzymuje się wówczas pulę stałych adresów, z których mogą korzystać komputery sieci lokalnej. Zazwyczaj z adresów tych korzystają serwery, natomiast stacje robocze tworzą podsieć, która łączy się z Internetem przez serwer NAT lub Proxy.



Rys. 3.12 Dostęp stały do Internetu np. przez sieć Polpak-T lub DSL TP

3.2 Protokół TCP/IP w Windows XP

3.2.a Instalacja protokołu

Aby system operacyjny mógł komunikować się przez sieć z innymi urządzeniami, konieczne jest skonfigurowanie odpowiedniego protokołu transportowego wykorzystywanego w danej sieci.

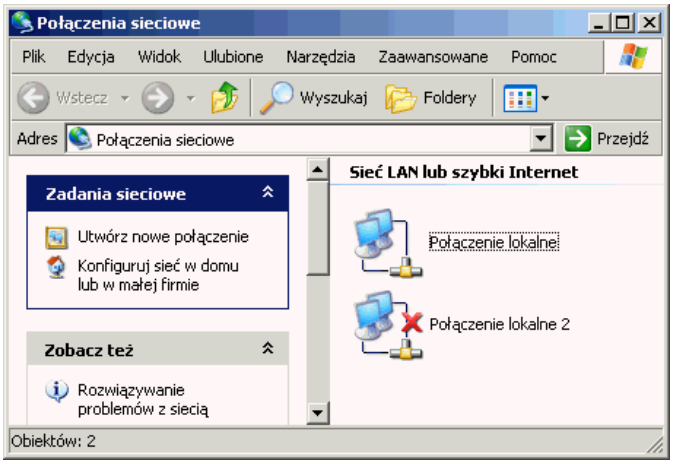
Obecnie najczęściej wykorzystywanym protokołem jest TCP/IP. Z protokołu tego korzysta sieć Internet, zatem zbudowanie sieci lokalnej w oparciu o TCP/IP umożliwi komputerom bezproblemowy dostęp do Internetu. TCP/IP dzięki routingowi pakietów daje możliwość podziału sieci na podsieci, w celu optymalizacji wydajności i zwiększenia efektywności zarządzania.

Jeżeli niewielka sieć lokalna (do 200 komputerów), zbudowana z jednej podsieci, nie jest podłączona do Internetu, to można wykorzystać protokół NetBEUI. Jest on bardzo prosty w instalacji, gdyż nie wymaga żadnej konfiguracji.

Windows 2000/XP potrafi także obsługiwać protokół IPX/SPX wykorzystywany w sieciach korzystających z serwera firmy Novell wersji 3.x lub 4.x.

Program instalacyjny systemu Windows 2000/XP, po zaakceptowaniu opcji domyślnych, automatycznie instaluje protokół TCP/IP. Jeżeli po instalacji zachodzi potrzeba dodania lub skonfigurowania protokołu, wówczas z ***Panelu sterowania*** należy wybrać ***Połączenia sieciowe***, następnie ***Właściwości połączenia lokalnego***. Jeżeli w komputerze znajdują się dwie karty sieciowe, wówczas każda z nich będzie tworzyć osobne połączenie.

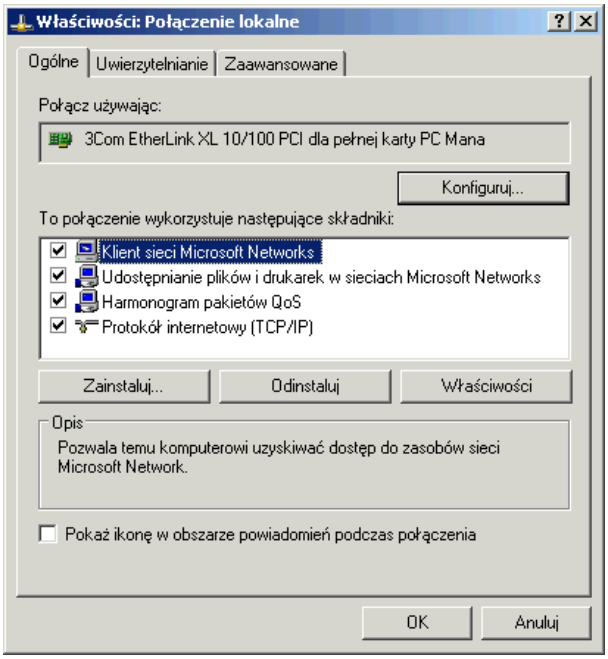
Jeżeli przy ikonie ***Połączenie lokalne*** widnieje czerwony **x** oznacza to, iż urządzenie nie jest aktywne np. z powodu odłączenia kabla sieciowego. Po dwukrotnym kliknięciu na ikonę połączenia, można uzyskać informację o stanie połączenia.



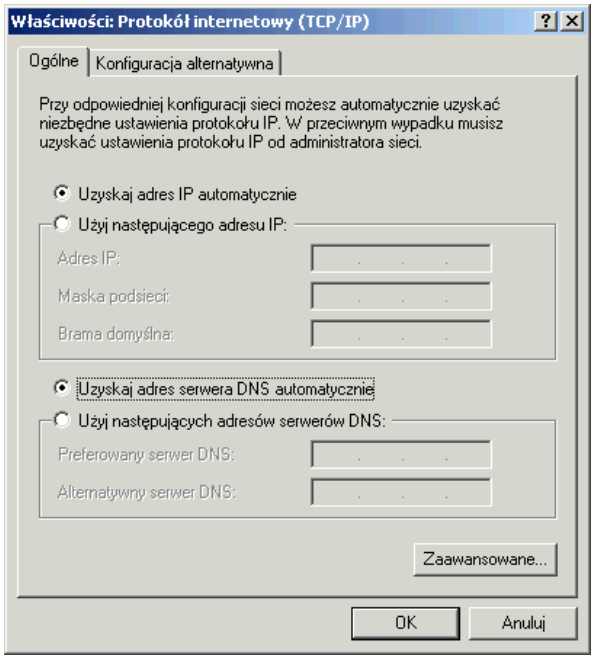
Rys. 3.13 Połączenia sieciowe i telefoniczne

Rys. 3.14 Stan połączenia

Jeżeli zachodzi potrzeba dodania protokołu, należy wybrać przycisk ***Zainstaluj***. Dodatkowo protokół musi być załączony (haczyk przy protokole).



Rys. 3.15 Właściwości połączenia



Rys. 3.16 Właściwości protokołu TCP/IP

Zadanie 3.2.a

1. Zmień nazwę połączenia: ***Połączenie lokalne*** na ***CKP*** i ***Połączenie lokalne 2*** na ***LAN***.

3.2.b Konfigurowanie adresacji TCP/IP

System Windows 2000/XP daje możliwość wykorzystania jednej z trzech metod adresacji.

1. Wykorzystanie protokołu DHCP. Jeżeli w sieci znajduje się serwer DHCP, wówczas przy pomocy protokołu DHCP (Dynamic Host Configuration Protocol) może automatycznie konfigurować ustawienia TCP/IP innych hostów (urządzeń sieciowych). Centralne zarządzanie konfiguracją TCP/IP znacznie upraszcza administrację siecią. Administrator DHCP może przydzielić pulę adresów, z której dzierżawione są adresy na określony czas (zazwyczaj kilka dni). Może także wybranym urządzeniom (np. kartą sieciowym) zarezerwować konkretny adres.
2. Automatyczne prywatne adresowanie IP (APIPA - Automatic Private IP Addressing) jest dobrym rozwiązaniem w niewielkich sieciach zbudowanych z jednej podsieci. Jeżeli serwer DHCP nie jest dostępny, wówczas komputer pracujący pod systemem Windows 2000/XP automatycznie przypisuje sobie adres z zakresu 169.254.x.x Przed przydzieleniem adresu, system sprawdza czy wybrany adres nie jest już zajęty przez inny komputer. Po przydzieleniu adresu co 5 min. sprawdzana jest obecność serwera DHCP. Jeżeli odpowie, pobierana jest konfiguracja TCP/IP.
3. Statyczne adresowanie IP wymaga ręcznego określenia adresów IP dla każdego komputera. Zalecana jest jedynie w małych sieciach, gdy adresowanie DHCP lub APIPA nie jest możliwe.

Jeżeli komputer ma kontaktować się z innymi podsieciami, oprócz adresu IP oraz maski, musi znać domyślną bramę, przez którą może przejść do innych podsieci, czy skontaktować się z Internetem.

Aby system korzystał z automatycznego adresowania DHCP lub APIPA, we właściwościach protokołu TCP/IP należy wybrać ***Uzyskaj adres IP automatycznie***. Natomiast przy adresowaniu statycznym, załączyć opcję ***Użyj następującego adresu IP*** i podać adres, maskę oraz domyślną bramę.

Przy adresowaniu automatycznym istnieje możliwość ustawienia ***Konfiguracji alternatywnej***. Jeżeli system nie otrzyma danych z DHCP, wówczas wykorzysta ustawienia alternatywne. Metodę tą można wykorzystać np. w komputerach przenośnych pracujących w dwóch sieciach: z serwerem DHCP i bez.

Aby sprawdzić, jaki adres IP jest aktualnie wykorzystywany, można wywołać z ***wiersza poleceń*** komendę ***ipconfig***.

```
Karta Ethernet  Połączenie lokalne 2:

        Sufiks DNS konkretnego połączenia:
        Adres IP autokonfiguracji . . . . : 169.254.55.81
        Maska podsieci. . . . . . . . . . : 255.255.0.0
        Brama domyślna. . . . . . . . . . :

Karta Ethernet  Połączenie lokalne:

        Sufiks DNS konkretnego połączenia:ckp.pl
        Adres IP. . . . . . . . . . . . . : 10.0.10.1
        Maska podsieci. . . . . . . . . . : 255.255.255.0
        Brama domyślna. . . . . . . . . . : 10.0.10.100
```

Rys. 3.17 Użycie polecenia ipconfig

Aby sprawdzić, czy system może skomunikować się przez protokół TCP/IP z innym hostem, można skorzystać z polecenia ***ping***.

```
C:\>ping 192.168.0.2

Badanie 192.168.0.2 z użyciem 32 bajtów danych:

Odpowiedź z 192.168.0.2: bajtów=32 czas<10ms TTL=128
Odpowiedź z 192.168.0.2: bajtów=32 czas<10ms TTL=128
Odpowiedź z 192.168.0.2: bajtów=32 czas<10ms TTL=128
Odpowiedź z 192.168.0.2: bajtów=32 czas<10ms TTL=128

Statystyka badania dla 192.168.0.2:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% utraconych),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 0ms, Maksimum =  0ms, Średnia =  0ms
```

Rys. 3.18 Użycie polecenia ping

Zadanie 3.2.b – Konfiguracja protokołu TCP/IP

1. Ustaw automatyczną adresację IP. Sprawdź z jakich adresów i maski podsieci korzysta twój komputer. Określ, czy twój komputer skorzystał z serwera DHCP i APIPA.
2. Ustaw adresowanie statyczne:
   - połączeniu ***CKP*** w przypisz adres ***10.0.10.xx*** (xx to numer twojego komputera) i maskę podsieci ***255.255.255.0***
   - połączeniu ***LAN*** przypisz adres ***192.168.0.hh*** (gdzie hh to numer portu huba, do którego jesteś przyłączony - nr komputera w twojej sieci LAN) i maskę podsieci ***255.255.255.0***
3. Sprawdź, czy możesz skontaktować się z sąsiednim komputerem. Sprawdź, czy odpowiadają obie karty sieciowe.
4. Spróbuj skontaktować się z serwerem CKP o adresie ***212.160.198.2.*** Jeżeli połączenie nie jest możliwe określ dlaczego.
5. W ustaw domyślną bramę na ***10.0.10.254*** i sprawdź czy odpowiada adres ***212.160.198.2***

3.2.c Konfigurowanie rozpoznawania nazw TCP/IP

Usługi korzystające z protokołu TCP/IP do identyfikowania, używają adresów IP, natomiast użytkownicy i aplikacje korzystają zazwyczaj z nazw. Aby nazwy mogły być przetłumaczone na adresy, dostępny musi być mechanizm rozpoznawania nazw.

System Windows 2000/XP, żądanie przetłumaczenia nazwy wysyła, w pierwszej kolejności, do systemu DNS (Domain Name System). Jeżeli nie otrzyma odpowiedzi, a nazwa ma do 15 znaków wówczas system korzysta z rozpoznawania nazw NetBIOS (przy założeniu, że protokół ten działa). Protokół NetBIOS wykorzystywany jest w sieciach Microsoft Networks przez protokół TCP/IP. Jeżeli i w tym wypadku nie powiedzie się rozpoznawanie, to proces kończy się niepowodzeniem.

- ***System DNS***

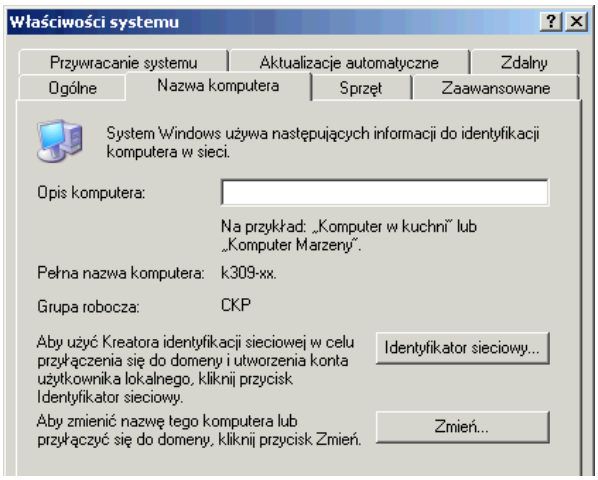
System DNS jest globalną, rozproszoną bazą danych, opartą na hierarchicznym systemie nazw. Z systemu DNS korzysta sieć Internet. Nazwy składają się ze skrótów rozdzielanych kropkami, zapisywane są małymi literami i nie zawierają polskich znaków. Skróty te tworzą domeny nazewnicze. Domeny obsługiwane są przez odpowiednie organizacje. Pierwszy poziom nazwy, to skrót kraju, w którym zarejestrowana jest nazwa np. pl – to Polska, ru – Rosja, de – Niemcy, uk – Wielka Brytania (tylko Stany Zjednoczone nie korzystają z domeny pierwszego poziomu). Drugi poziom, to skróty rodzaju organizacji np. com – komercyjne, edu – edukacyjne, gov – rządowe,

org – organizacje niekomercyjne lub nazwy regionalne np. wroc – Wrocław, waw – Warszawa. Drugi poziom nie jest wymagany podczas rejestracji. W Polsce za obsługę domeny pl odpowiedzialny jest NASK (Naukowa Akademicka Sieć Komputerowa), a za obsługę domeny wroc.pl WCSS (Wrocławskie Centrum Sieciowo-Superkomputerowe przy Politechnice Wrocławskiej).

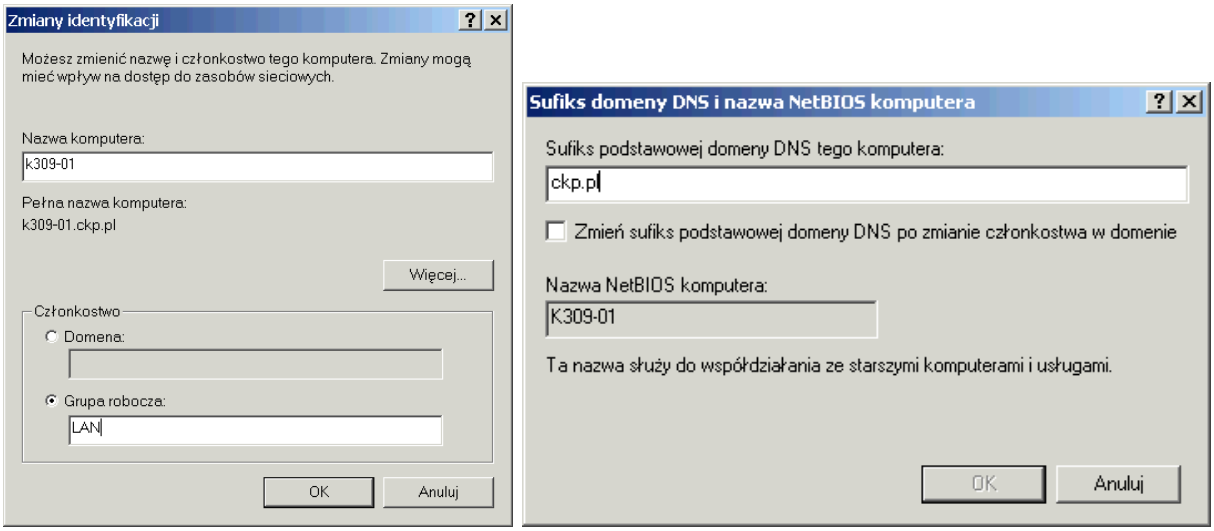
Firma, chcąc obsługiwać własną domenę zarejestrowaną np. w NASK, musi posiadać serwer DNS. W serwerze tym powinny być zarejestrowane wszystkie wykorzystywane nazwy.

Pełna nazwa każdego komputera z Windows 2000/XP składa się z nazwy komputera i domeny DNS. Aby sieć podłączona na stałe do Internetu była widoczna z Internetu, wówczas nazwa domeny musi być zarejestrowana w systemie DNS.

Aby zdefiniować pełną nazwę komputera, z ***panelu sterowania*** należy wybrać ***System*** i zakładkę ***Nazwa komputera***. W oknie znajduje się pole ***Pełna nazwa komputera*** i przycisk ***Zmień***. Przy jego pomocy można dostać się do okna umożliwiającego zdefiniowanie ***nazwy komputera***. Po wybraniu ***Więcej*** także domeny, podawanej w polu edycji ***Sufiks podstawowej nazwy domeny DNS dla tego komputera.***



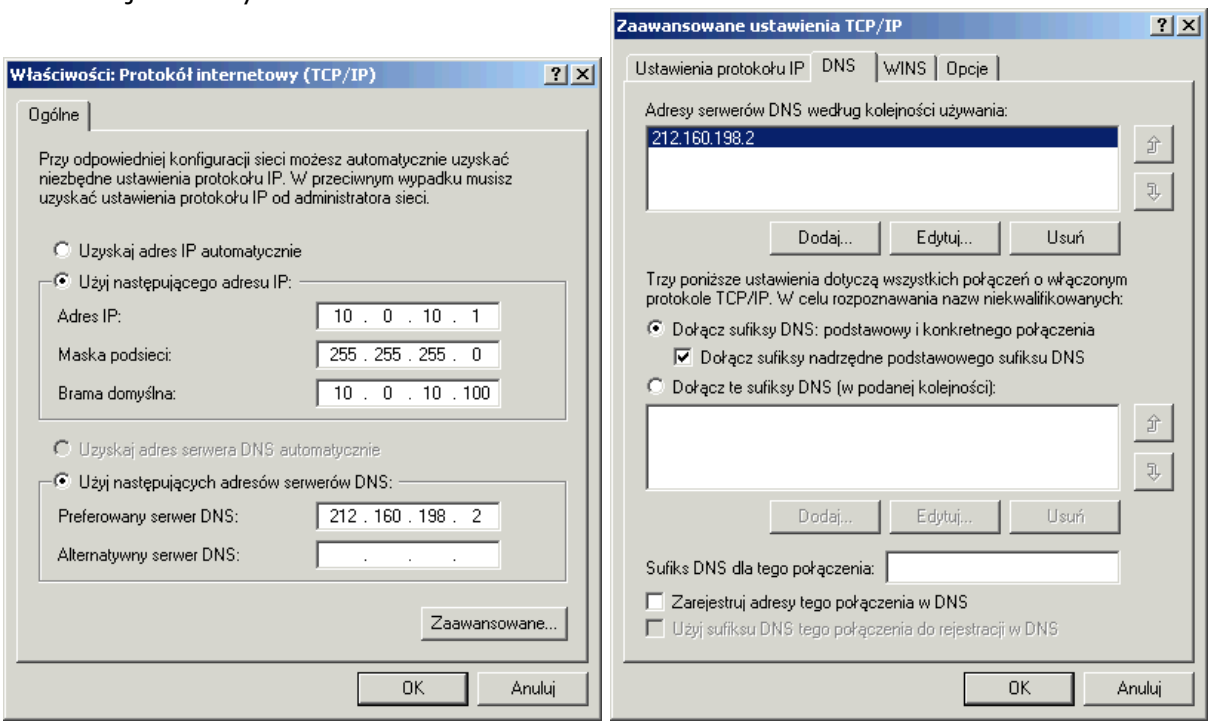
Rys. 3.19 Identyfikacja sieciowa



Rys. 3.20 Definiowanie pełnej nazwy domeny

Jeżeli komputer pracuje w domenie Windows 2000/2003 Active Directory i/lub ma mieć dostęp do Internetu, wówczas musi korzystać z serwera DNS. Usługa Active Directory Windows 2000/2003 Server jest ściśle zintegrowana z DNS. W sieciach lokalnych posiadających stałe złącze z Internetem, powinien działać serwer DNS. Jeżeli go nie ma, można skorzystać z serwera DNS operatora Internetu.

W systemie Windows 2000/XP lokalizację serwera DNS podaje się we właściwościach protokołu TCP/IP, w sekcji ***Użyj następujących adresów serwerów DNS***. Można podać adres serwera ***preferowanego*** i ***alternatywnego***. Jeżeli w sieci znajduje się serwer DHCP, powinien konfigurować automatycznie ustawienia serwera DNS stacji roboczych.



Rys. 3.21 Ustawienia serwera DNS

Jeżeli zachodzi potrzeba zdefiniowania dodatkowych serwerów, wówczas po wybraniu opcji ***Zaawansowanych*** na zakładce ***DNS,*** można podać je, wybierając przycisk ***Dodaj***. Następnie za pomocą przycisków ↑ ↓ określa się kolejność przepytywania. Jeżeli w komputerze zainstalowanych jest kilka adapterów sieciowych, wystarczy, aby tylko jeden z nich miał zdefiniowane ustawienia DNS.

System Windows 2000/XP zezwala na ustawienie tylko jednej nazwy komputera, nawet jeżeli korzysta z kilku kart sieciowych. Inaczej wygląda w takim przypadku nazwa domeny. Każde połączenie może mieć zdefiniowaną inną domenę, wystarczy podać je w polach ***Sufiks DNS dla tego połączenia.***

Jeżeli Windows 2000/XP współpracuje z dynamicznym DNS (np. pracuje w domenie AD 2000/2003), wówczas może automatycznie rejestrować adresy połączeń, po wybraniu opcji ***Zarejestruj adresy tego połączenia w DNS***.

W sytuacji, gdy rozpoznawana nazwa składa się z jednej etykiety i nie jest nazwą pełną (nazwa hosta plus domena) lub składa się z kilku etykiet (nazwy rozdzielone kropkami), a składnik rozpoznawania nie potrafi jej sprawdzić, wówczas dołączany jest sufiks DNS podstawowy i konkretnego połączenia. Przy założeniu, że wybrana jest opcja ***Dołącz sufiksy DNS***.

Przykładowo jeżeli domena to ***sala211.ckp.pl,*** wówczas przy zapytaniu o adres ***k211-01*** system zapyta się o ***k211-01.sala211.ckp.pl***. Jeżeli dodatkowo będzie załączona opcja ***Dołącz sufiksy nadrzędne podstawowego sufiksu DNS*** wówczas, jeżeli we wcześniejszym zapytaniu system nie znajdzie ***k211-01.sala211.ckp.pl*** zapyta się o nazwę ***k211-01.ckp.pl***.

Na zakładce ***DNS*** właściwości protokołu TCP/IP można wybrać opcję ***Dołącz te sufiksy DNS (w podanej kolejności)*** i podać listę domen, które mają być odpytywane.

System rozpoznawania nazw systemu Windows 2000/XP korzysta z pamięci podręcznej. Aby zobaczyć zawartość bufora nazw, można skorzystać z polecenia ***ipconfig*** z parametrem ***/displaydns***. Wykorzystanie przełącznika ***/flushdns*** wyczyści cache systemy rozpoznawania nazw.

- ***Plik hosts***

W przypadku sieci nie posiadających dostępu do serwera nazw DNS, utworzenie pliku ***hosts*** pozwala na rozpoznawanie nazw hostów przez aplikacje i usługi. Plik ten może być używany także w środowiskach, w których serwery nazw są dostępne, ale nie wszystkie hosty zostały w nich zarejestrowane. Przykładem takiego hosta może być serwer, który nie jest dostępny na publiczny użytek i z którego może korzystać jedynie ograniczona liczba klientów. Plik ***hosts*** musi zostać utworzony ręcznie, należy też ręcznie wprowadzać do niego zmiany za każdym razem, gdy zmieniają się nazwy lub adresy hostów. Plik ***host*** jest ładowany do bufora składnika rozpoznawania nazw. Przykładowy plik znajduje się w katalogu ***%SystemRoot%\System32\Drivers\Etc***. Do tego pliku można wpisać nazwy wszystkich komputerów, z którymi ma być nawiązywana komunikacja.

- ***Rozpoznawanie nazw NetBIOS***

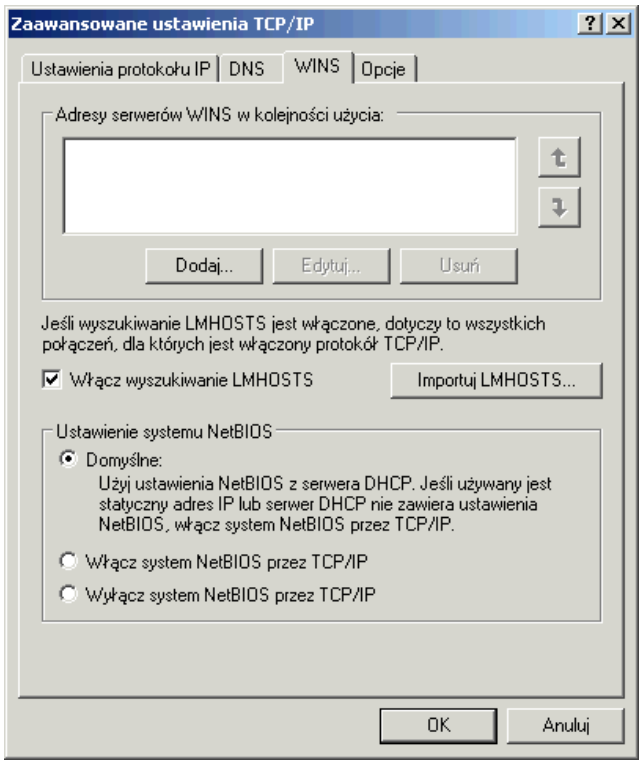
Implementacja TCP/IP firmy Microsoft korzysta z protokołu NetBIOS przez TCP/IP (NetBT). W systemie Windows 2000/XP domyślną metodą jest rozpoznawanie nazw DNS, jednak system ten umożliwia rozpoznawanie NetBIOS. W wcześniejszych systemach Microsoft (9x/ME/NT) to rozpoznawanie NetBIOS było domyślne.

System rozpoznawania NetBIOS korzysta z czterech metod rozpoznawania, określanych jako typ węzła:

- ***B-węzeł*** - korzysta z rozgłoszeń.
- ***P-węzeł*** - korzysta z komunikacji typu punkt-punkt z serwerem NetBIOS - WINS.
- ***M-węzeł*** - korzysta najpierw z rozgłoszeń (b-węzeł), a następnie, jeżeli nie otrzyma odpowiedzi, ze skierowanych zapytań (p-węzeł).
- ***H-węzeł*** - korzysta najpierw z zapytań (p-węzeł), a następnie, jeżeli serwer nazw jest niedostępny lub nazwa nie jest zarejestrowana w bazie danych WINS, z rozgłoszeń.
- Dodatkowym typem węzła jest rozszerzony węzeł Microsoft. Korzysta on, poza standardowymi metodami, z lokalnego pliku ***lmhosts*** oraz z wywołań korzystających z DNS i lokalnego pliku ***hosts***.

Wykorzystanie serwera WINS redukuje konieczność korzystania z lokalnych rozgłoszeń, w celu rozpoznawania nazw, co podnosi wydajność sieci i pozwala użytkownikom na wyszukiwanie komputerów znajdujących się w odległych sieciach. Administrator sieci nie musi dokonywać ręcznie zmian w systemie rozpoznawania nazw, serwer WINS sam dynamicznie buduje bazę adresową.

Serwer WINS można zdefiniować we właściwościach TCP/IP na zakładce ***WINS***, oddzielnie dla każdego adaptera sieciowego. Typ węzła można zobaczyć za pomocą polecenia ***ipconfig*** z parametrem ***/all***.



Rys. 3.22 Ustawienia WINS

```
        Nazwa hosta . . . . . . . . . . . . : k309-01
        Sufiks podstawowej domeny DNS:ckp.pl
        Typ węzła . . . . . . . . . . . . . : Hybrydowa
        Routing IP włączony . . . . . . . . : Nie
        Serwer proxy WINS włączony. . . . . : Nie
        Lista przeszukiwania sufiksów DNS : ckp.pl
```

Rys. 3.23 Typ węzła

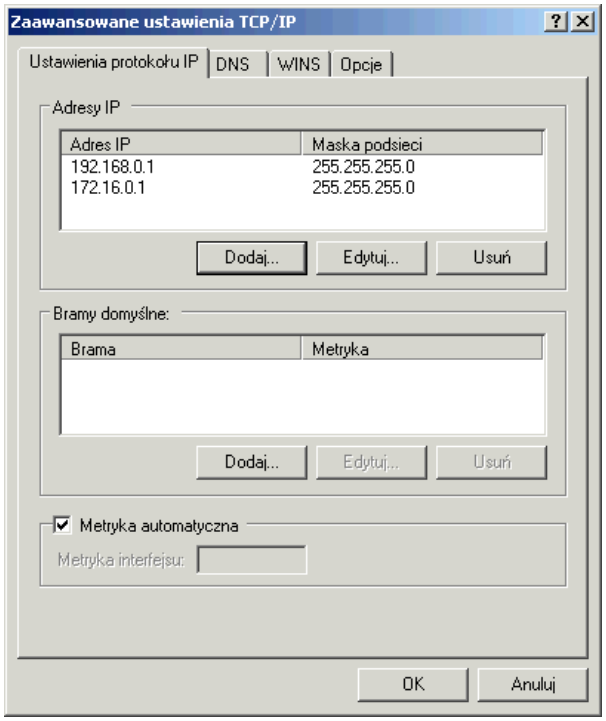
Zadanie 3.2.c – Rozwiązywanie nazw

1. Ustaw serwer DNS na ***212.160.198.2***
2. Sprawdź za pomocą ***ipconfig*** z parametrem ***/all,*** czy system korzysta już z DNS.
3. Sprawdź, czy działa DNS, przez wysłanie pinga na ***wp.pl***
4. Ustaw sufiks podstawowej domeny DNS na ***ckp.pl***
5. W ustaw nazwę komputera na ***k211-xx***, gdzie xx to numer twojego komputera.
6. Sprawdź, czy działa dołączanie sufiksu DNS przez wysłanie pinga na ***alpha***
7. Ustaw serwer WINS dla połączenie ***CKP*** na ***212.160.198.2***

3.2.d Konfigurowanie hostów wieloadresowych

System Windows 2000/XP nie ma ograniczeń co do ilości obsługiwanych adapterów. Każdy adapter musi mieć przypisany adres IP. Domyślnie ustawiana jest adresacja automatyczna. Dodatkowo jeden adapter może mieć przypisanych kilka adresów IP z odpowiednimi maskami. Dzięki przypisaniu kilku adresów IP, system może mieć dostęp do kilku podsieci jednocześnie.

Dodatkowe adresy IP przypisuje się we właściwościach TCP/IP na zakładce ***Ustawienia protokołu IP,*** po wybraniu ***Dodaj***.



Rys. 3.24 Ustawienia protokołu IP

Zadanie 3.2.d – Konfigurowanie hostów wieloadresowych

1. Połączeniu ***LAN*** przypisz dodatkowy adres ***172.16.0.hh*** z maską ***255.255.255.0***, gdzie ***hh*** to numer portu huba, do którego jesteś podłączony – nr komputera w twojej sieci LAN.
2. Sprawdź, czy odpowiadają inne komputery twojej nowej podsieci.

3.2.e Konfigurowanie routingu TCP/IP

Sieci TCP/IP mogą być łączone za pomocą routerów, których zadaniem jest przekazywanie pakietów IP między podsieciami. Pakiet IP w nagłówku posiada adres źródłowy (lokalny) i docelowy. Przed wysłaniem, system porównuje adres docelowy z lokalną tablicą routingu i na jej podstawie podejmuje odpowiednie działanie. Może przekazać pakiet do warstwy IP na lokalnym komputerze, przesłać przez jeden z adapterów sieciowych lub pakiet odrzucić.

Wyszukując trasy w lokalnej tabeli routingu, system na wstępie szuka trasy do konkretnego hosta (dokładny odpowiednik), następnie trasy do podsieci (lokalnie dołączone podsieci) i jeżeli nie znajdzie trasy domyślnej (brama domyślna), pakiet jest odrzucany.

Lokalna tabela routingu może być konfigurowana:

- ręcznie,
- automatycznie za pomocą rozgłoszeń protokołu RIP od routerów lokalnej podsieci,
- przez ręczne ustawienie domyślnej bramy,
- przez automatyczne ustawienie domyślnej bramy przez DHCP lub wykrywanie routerów ICMP.

W przypadku systemów wieloadresowych, bramy domyślne wykorzystywane są przez wszystkie adaptery. Dodatkowo system Windows 2000/XP umożliwia zdefiniowanie kilku bram domyślnych w określonej kolejności związanej z dostępnością, obciążeniem. Każdej bramie można przypisać metrykę (im niższa wartość tym bardziej preferowana).

Bramy domyślne można zdefiniować na zakładce ***Ustawienia protokołu IP*** okna właściwości protokołu TCP/IP.

Za pomocą polecenia ***route*** można zarządzać lokalną tabelą routingu. Parametr ***print*** umożliwia wyświetlenie lokalnej tabeli.

```
C:\>route print
===========================================================================
Lista interfejsów
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 04 76 9f f2 77 ...... 3Com EtherLink PCI
0x1000004 ...00 a0 24 51 ee 1a ...... ELNK3 Ethernet Adapter
===========================================================================
===========================================================================
Aktywne trasy:
Miejsce docelowe w sieci      Maska sieci      Brama       Interfejs       Metryka

          0.0.0.0          0.0.0.0      10.0.10.100       10.0.10.1        1
        10.0.10.0    255.255.255.0        10.0.10.1       10.0.10.1        1
        10.0.10.1  255.255.255.255        127.0.0.1       127.0.0.1        1
   10.255.255.255  255.255.255.255        10.0.10.1       10.0.10.1        1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1        1
      172.16.0.0    255.255.255.0       172.16.0.1     192.168.0.1        1
      172.16.0.1  255.255.255.255        127.0.0.1       127.0.0.1        1
   172.16.255.255  255.255.255.255      192.168.0.1     192.168.0.1        1
     192.168.0.0    255.255.255.0      192.168.0.1     192.168.0.1        1
     192.168.0.1  255.255.255.255        127.0.0.1       127.0.0.1        1
   192.168.0.255  255.255.255.255      192.168.0.1     192.168.0.1        1
        224.0.0.0        224.0.0.0        10.0.10.1       10.0.10.1        1
        224.0.0.0        224.0.0.0      192.168.0.1     192.168.0.1        1
  255.255.255.255  255.255.255.255        10.0.10.1       10.0.10.1        1
Domyślna brama:       10.0.10.100.
===========================================================================
Trasy trwałe:
  Brak
```

Rys. 3.25 Lokalna tabela routingu

Zadanie 3.2.e – Routing TCP/IP

1. Wyświetl i przeanalizuj lokalną tabelę routingu.

3.2.f Konfigurowanie protokołu IPSec

Obecnie coraz częściej przez sieć Internet przesyłane są bardzo ważne informacje, co za tym idzie pojawiła się potrzeba zabezpieczenia ruchu IP. Zadaniem administratorów sieci jest zagwarantowanie, aby ruch sieciowy był:

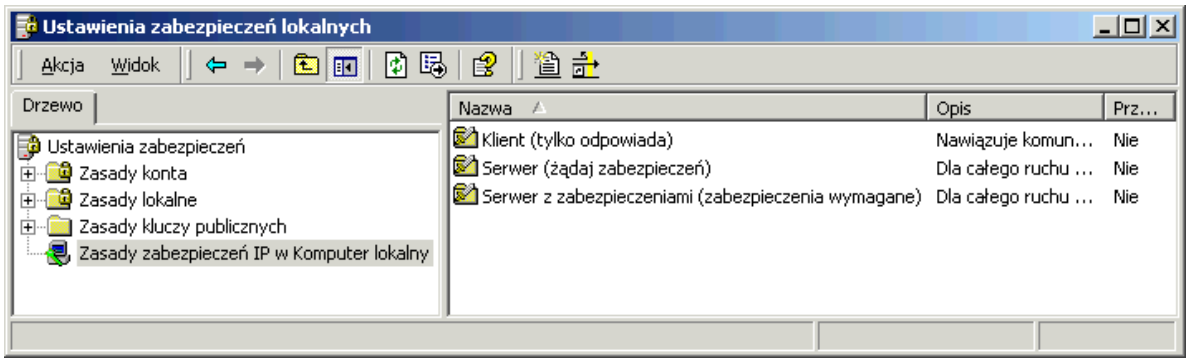
- niemożliwy do zmodyfikowania podczas przesyłania,
- niemożliwy do przechwycenia, przejrzenia lub skopiowania,
- niedostępny dla nieautoryzowanych stron.

Powyższe wymagania spowodowały, że organizacja IETF zaprojektowała protokół IPSec. Protokół IPSec korzysta ze standardowych algorytmów szyfrowania i kompleksowo zarządza zabezpieczeniami, umożliwiając ochronę całej komunikacji TCP/IP.

Protokół IPSec jest implementowany poniżej warstwy transportowej, dzięki czemu administratorzy sieci i producenci oprogramowania nie muszą ponosić wydatków i trudności związanych z zapewnianiem i koordynowaniem zabezpieczeń dla poszczególnych aplikacji. W prosty sposób włączając protokół IPSec w systemie Windows 2000/XP, administrator sieci może utworzyć warstwę mocnych zabezpieczeń dla całej sieci. Aplikacje automatycznie i w sposób przezroczysty dziedziczą funkcje zabezpieczeń od serwerów i klientów korzystających z IPSec.

Protokół IPSec może zostać uaktywniony w domenie Active Directory lub za pomocą zasad lokalnych.

Po wybraniu z ***narzędzi administracyjnych*** można dostać się do ***Zasad zabezpieczeń lokalnych***, a w nich dostępne są ***Zasady zabezpieczeń IP***.



Rys. 3.26 Zasady zabezpieczeń IP

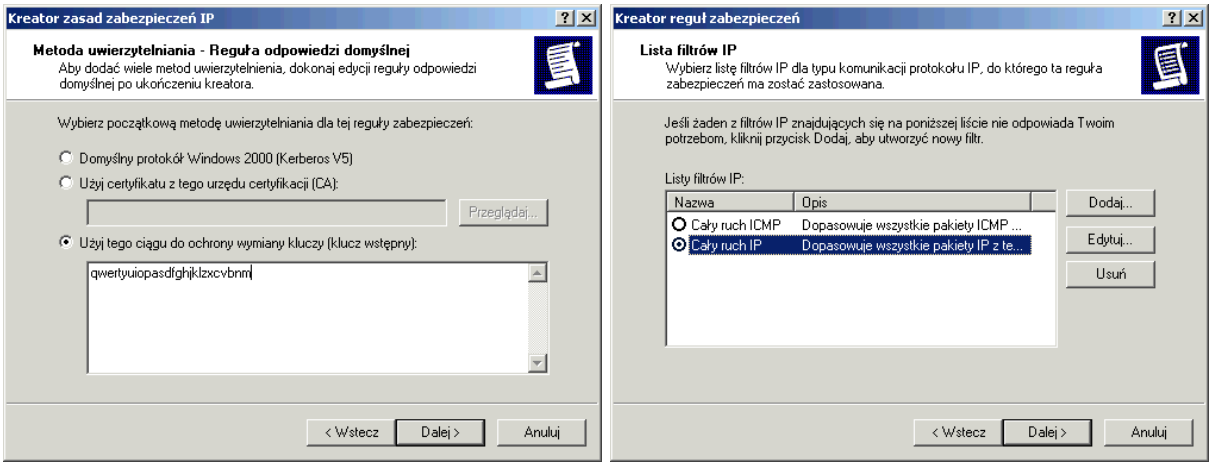
Domyślnie zdefiniowane są trzy zasady:

- ***Klient*** (tylko odpowiada) – niski poziom zabezpieczeń. Ta zasada umożliwia komputerom, które nie wymagają bezpiecznej komunikacji, odpowiadanie na żądania komunikacji zabezpieczonej. Możliwa jest w dalszym ciągu niezabezpieczona komunikacja z hostami nie używającymi protokołu IPSec.
- ***Serwer*** (żądaj zabezpieczeń) - średni poziom zabezpieczeń. Umożliwia akceptowanie niezabezpieczonych połączeń i podejmowanie prób nawiązywania bezpiecznych kanałów. Komunikacja nie jest zabezpieczona, gdy drugi host nie obsługuje protokołu IPSec.
- ***Serwer z zabezpieczeniami*** (wymagane) - wysoki poziom zabezpieczeń. Wymaga, aby cała prowadzona komunikacja była zabezpieczana.

Wszystkie te zasady do uwierzytelniania wykorzystują protokół Kerberos V5, który wymaga pracy w domenie Windows Server 2000/2003.

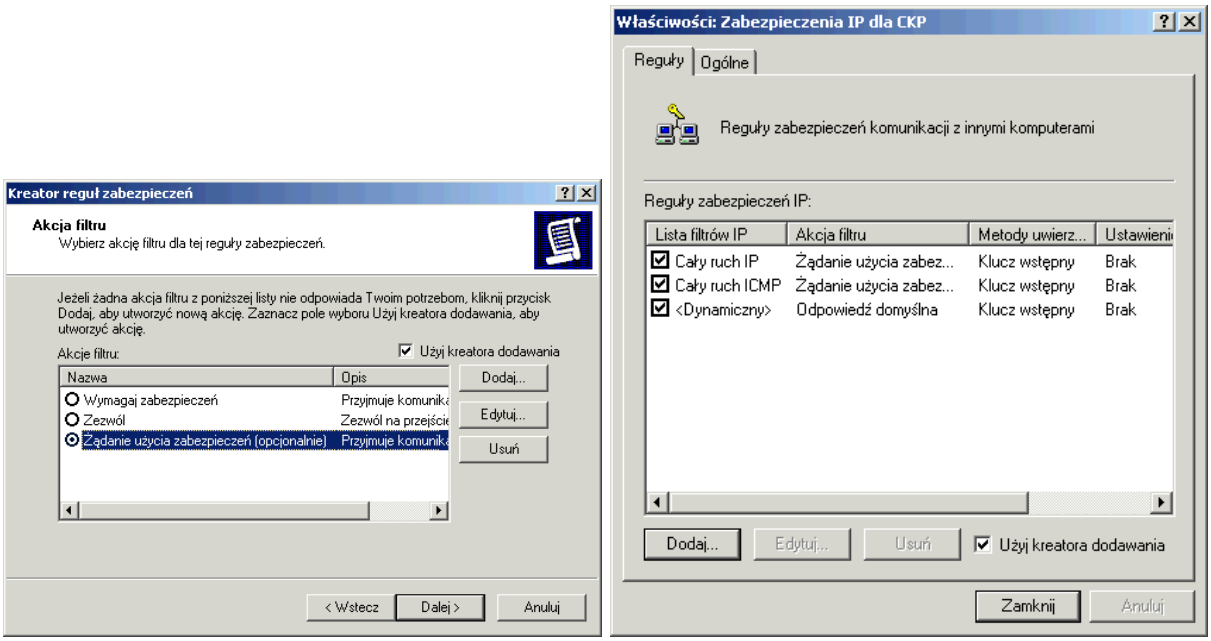
Jeżeli zabezpieczona komunikacja ma być zrealizowana przy braku domeny 2000/2003, wówczas należy zdefiniować nową zasadę z odpowiednimi ustawieniami. W tym celu w oknie zasad lokalnych po kliknięciu prawym przyciskiem myszy na ***Zasady zabezpieczeń IP*** należy wybrać ***Utwórz zasadę zabezpieczeń IP.***

1. W początkowych krokach kreatora należy podać ***nazwę*** zasady zabezpieczeń IP i włączyć ***regułę odpowiedzi domyślnej***. Odpowiedzialna jest ona za odpowiadanie komputerom żądającym użycia zabezpieczeń, w przypadku, gdy nie jest użyta żadna reguła.
2. Kolejny krok to wybór ***metody uwierzytelniania***. Należy podać dowolny ***klucz wstępny.*** Następnie zdecydować się na ***edytowanie właściwości***.



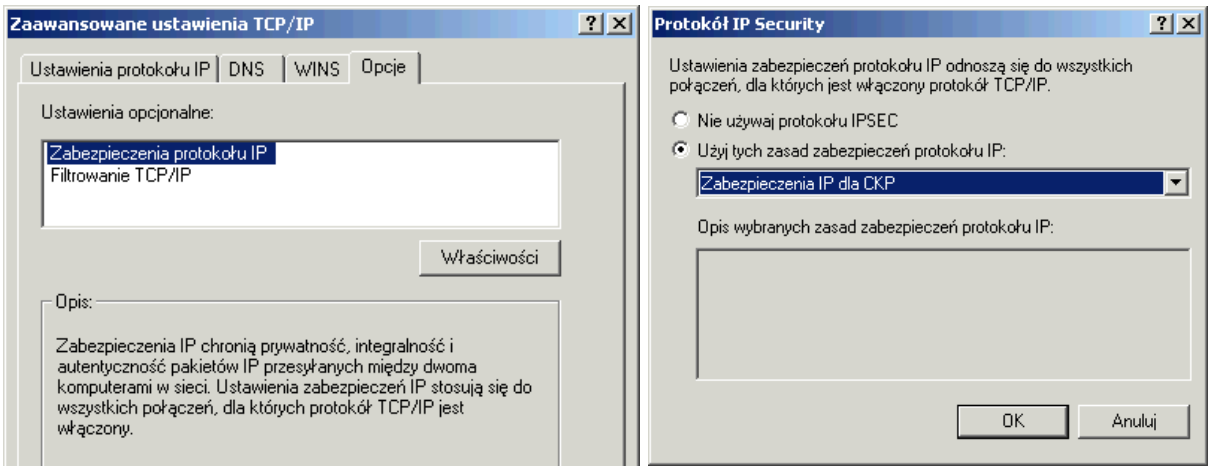
Rys. 3.27 Wybór metody uwierzytelniania i filtru IP

3. W oknie ***Właściwości*** należy wybrać ***Dodaj,*** w celu dodania reguły zabezpieczeń.
4. Początkowe okno kreatora zezwala na zdefiniowanie tunelu protokołu IPSec umożliwiającego przesyłanie pakietów między sieciami prywatnymi i publicznymi przy zachowaniu poziomu zabezpieczeń zbliżonego do takiego, jaki istnieje w przypadku bezpośredniego połączenia dwóch komputerów.
5. Kolejne okno to wybór typu sieci, w której ma zostać zastosowane zabezpieczenie. Do wyboru są: wszystkie połączenia sieciowe, sieć lokalna lub zdalny dostęp.
6. Następny krok to wybór metody uwierzytelniania i wybranie filtru IP określającego ruch IP. Domyślnie można wybrać ***Cały ruch ICMP*** lub ***Cały ruch IP***. Jeżeli zachodzi potrzeba zdefiniowania tylko części ruchu IP (np. z wybranej podsieci) można utworzyć nowy filtr po wybraniu ***Dodaj***.
7. Kolejne okno to wybór typu akcji, standardowo można wybrać:
   - ***Wymagaj zabezpieczeń.*** Przyjmuje komunikację niezabezpieczoną, lecz zawsze wysyła do klientów żądanie wprowadzenia mechanizmów potwierdzania zaufania i zabezpieczeń. Nie nawiąże komunikacji z klientami innymi niż zaufani.
   - ***Zezwól***. Zezwól na przejście niezabezpieczonych pakietów IP.
   - ***Żądanie użycia zabezpieczeń (opcjonalnie)*** Przyjmuje komunikację niezabezpieczoną, lecz wysyła do klientów żądanie wprowadzenia mechanizmów potwierdzania zaufania i zabezpieczeń. Jeśli klient nie odpowie na żądanie, nawiązana zostanie komunikacja bez zabezpieczeń.



Rys. 3.28 Wybór akcji filtru i właściwości zabezpieczeń

Aby uaktywnić zabezpieczenia protokołu IP w opcjach zaawansowanych właściwości protokołu TCP/IP na zakładce ***Opcje*** należy wybrać ***Właściwości Zabezpieczenia protokołu TCP/IP***.

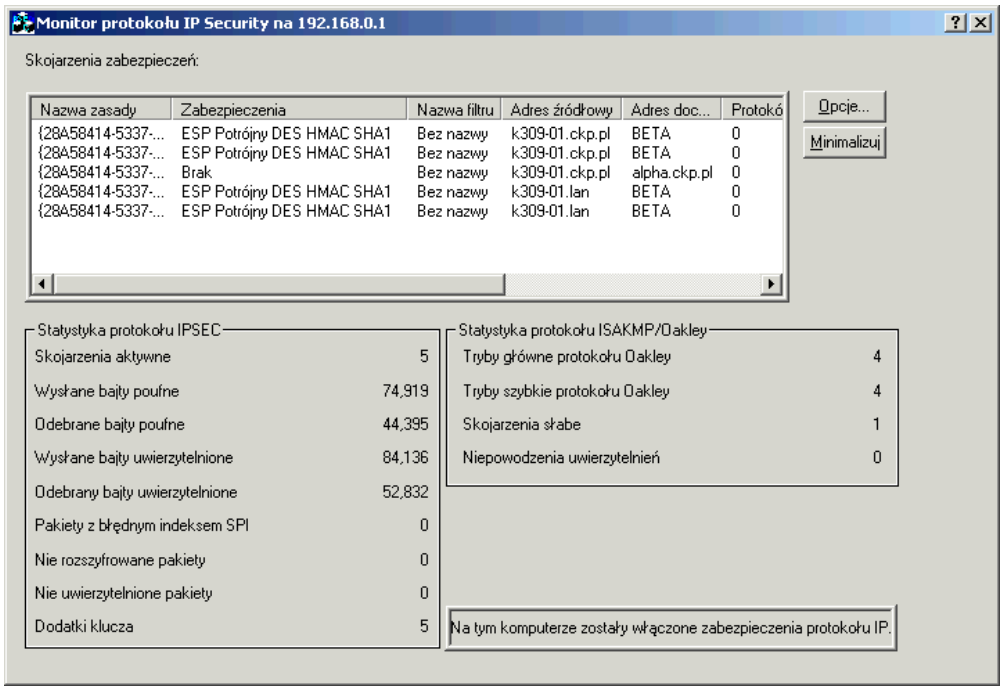


Rys. 3.29 Załączenie zabezpieczenia protokołu IP

Aby zobaczyć aktualne zabezpieczone połączenia można skorzystać z programu ***ipsecmon*** podając w parametrach adres IP kontrolowanego hosta.

Zadanie 3.2.f – Konfiguracja IPSec

1. Zmodyfikuj zasadę zabezpieczeń (serwer) przez ustawienie klucza wstępnego ***qwertyuiopasdfghjklzxcvbnm*** zarówno dla protokołu ***ICMP***, jaki i ***IP***. W akcji filtru wybierz ***Żądanie użycia zabezpieczeń***.
2. Załącz zabezpieczenia protokołu IP.
3. Nawiąż połączenie z innym komputerem, który korzysta z protokołu IPSec za pomocą polecenia ***ping*** i przez ***Moje miejsce sieciowe.***
4. Sprawdź czy udało ci się nawiązać zabezpieczone połączenie.



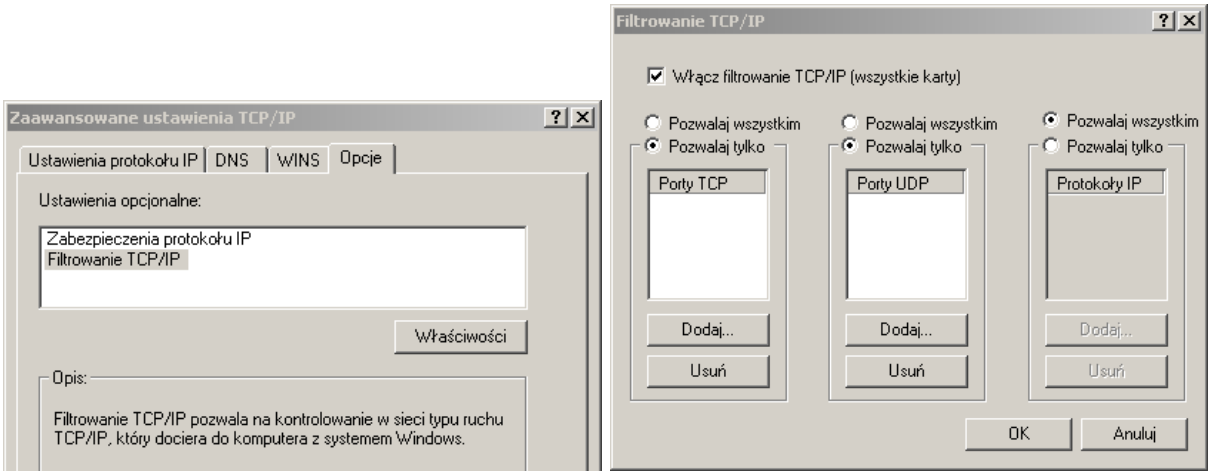
Rys. 3.30 Monitor protokołu IPSec

3.2.g Filtrowanie protokołu TPC/IP

Filtrowanie TCP/IP umożliwia precyzyjne określenie ruchu przychodzącego TCP/IP, przetwarzanego przez poszczególne interfejsy. Załączenie filtrowania TCP/IP umożliwia mocne zabezpieczenie komputera w sytuacji, gdy filtrowanie TCP/IP nie jest załączone w bramie łączącej z innymi sieciami (np. Internetem). Filtrowanie TCP/IP jest domyślnie wyłączone. Dotyczy jedynie ruchu nietranzytowego (przetwarzanego przez hosta). Filtrowanie TCP/IP umożliwia ograniczenie ruchu w oparciu o docelowy port TCP, docelowy port UDP i protokół IP.

Poprawne skonfigurowanie filtrowania TCP/IP nie jest prostą czynnością, gdyż zbyt restrykcyjne filtry mogą nie pozwolić na nawiązanie wymaganych połączeń.

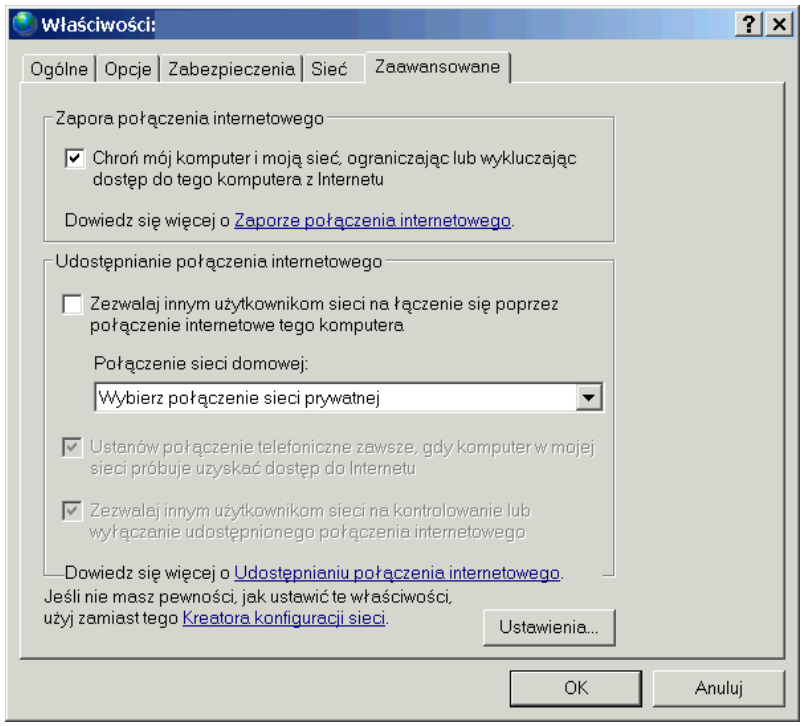
Filtrowanie TCP/IP załącza się we właściwościach protokołu TCP/IP na zakładce ***Opcje*** po wybraniu ***Właściwości Filtrowania TCP/IP***.



Rys. 3.31 Filtrowanie TCP/IP

3.2.h Zabezpieczenie połączeń internetowych

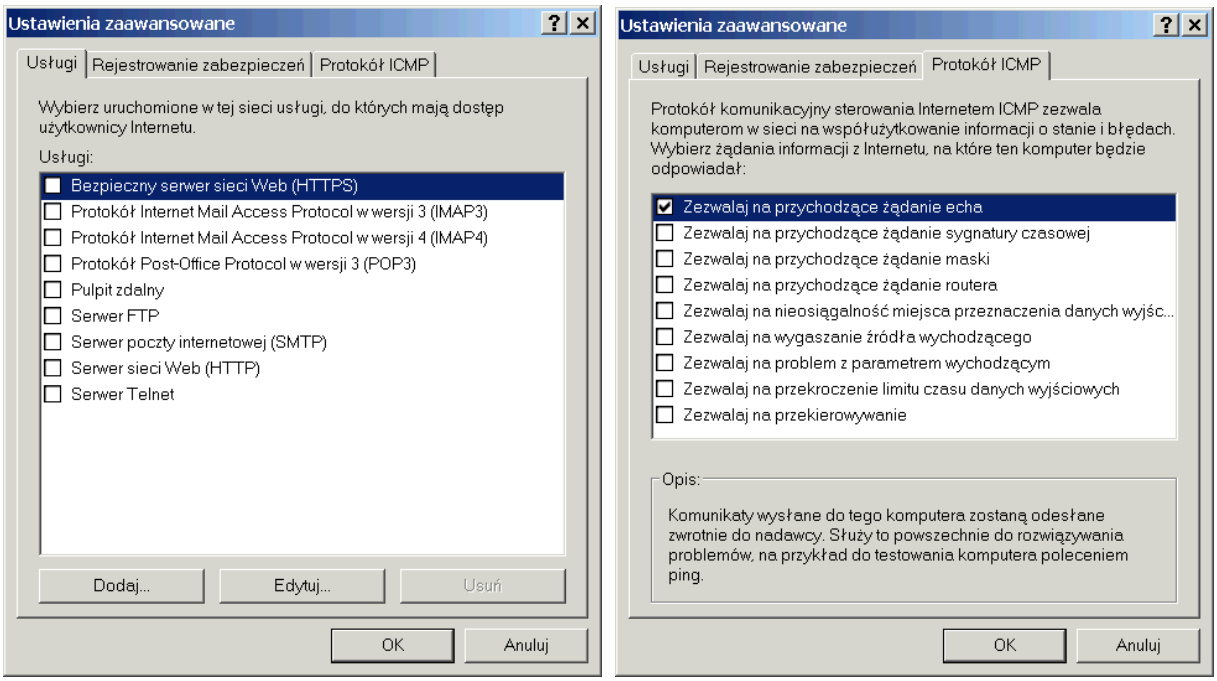
System Windows XP umożliwia zabezpieczenie połączeń internetowych za pomocą zapory ogniowej - firewall (Internet Connection Firewall, ICF). Jej działanie polega na tym, że firewall pamięta każde połączenie, jakie zostało nawiązane i śledzi jego stan. Jeżeli do komputera docierają pakiety odpowiedzi, są one wpuszczane, inne pakiety system blokuje. Domyślnie zapora jest wyłączona. Aby ją załączyć, należy we właściwościach połączenia sieciowego, na zakładce ***Zaawansowane,*** włączyć ***Chroń mój komputer i moją sieć ograniczając lub wykluczając dostęp do tego komputera z Internetu.***



Rys. 3.32 Załączenie ochrony połączenia internetowego

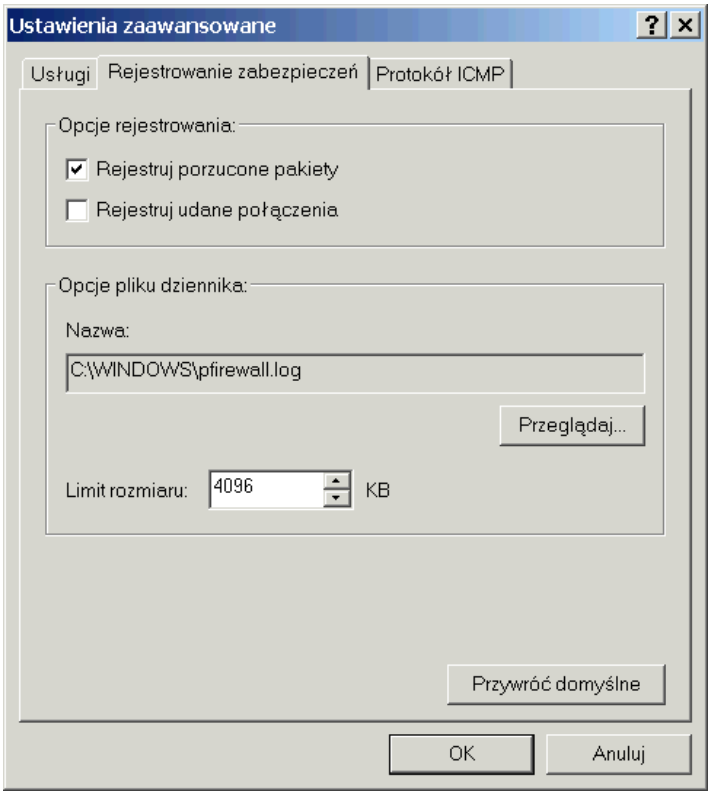
Domyślnie blokowane są wszystkie połączenia przychodzące i w sytuacji, gdy komputer nie udostępnia żadnych usług w sieci, jest to bardzo dobre rozwiązanie. Jednak, gdy komputer ma udostępniać usługi, wówczas trzeba wpuścić określony ruch. W tym przypadku pomocne będą ***Ustawienia*** ICF. Na zakładce ***Usługi*** można zaznaczyć, które usługi chcemy odblokować. Jeżeli na liście nie ma potrzebnej usługi, można ją dodać po wybraniu przycisku ***Dodaj***.

W Internecie, do kontroli połączenia, wykorzystywany jest protokół **ICMP** (ang. *Internet Control Message Protocol* - protokół komunikatów kontrolnych Internetu). Załączenie ochrony połączenia blokuje wszystkie komunikaty docierające do komputera. Jeżeli zachodzi potrzeba wpuszczenia niektórych z nich, można wprowadzić odpowiednie ustawienia na zakładce ***Protokół ICMP***, np. jeżeli komputer ma odpowiadać na polecenie ping, należy załączyć ***Zezwalaj na przychodzące żądanie echa***.



Rys. 3.33 Okna ustawień zapory firewall

Dodatkowo, w ustawieniach ICF, można załączyć rejestrowanie pakietów porzuconych, a także rejestrowanie udanych połączeń. Analiza plików dziennika może być bardzo pomocna przy rozwiązywaniu problemów, a także przy wykrywaniu włamań. Odpowiednie opcje można załączyć na zakładce ***Rejestrowanie zabezpieczeń.***



Rys. 3.34 Opcje rejestrowania

3.2.i Rozwiązywanie problemów z protokołem TCP/IP

W sytuacji, gdy wystąpi problem z protokołem TCP/IP, na wstępie należy skontrolować konfigurację, za pomocą polecenia ***ipconfig*** z parametrem ***/all***. ***Ipconfig*** oprócz wyświetlenia aktualnych ustawień sieciowych, dodatkowo testuje adres interfejsu zwrotnego (127.0.0.1) oraz własne adresy IP za pomocą polecenia ***ping.***

Ping wysyła komunikat do określonego hosta TCP/IP, a host przeznaczenia zwraca ów komunikat jako odpowiedź. Brak odpowiedzi oznacza, że sieć lub host nie działają albo, że pakiet został zgubiony, podczas transmisji. Polecenie ***PING*** powtarza test określoną ilość razy. Polecenie to ma szereg parametrów, między innymi umożliwiające zwiększenie długości pakietów (-l), ilości wysyłanych pakietów (-n) czy wysyłanie komunikatów w sposób ciągły (-n).

Jeżeli konfiguracja jest poprawna można za pomocą polecenia ***ping*** sprawdzić, czy odpowiada brama domyślna. Gdy brama nie istnieje, sprawdzić połączenie z innym komputerem w sieci.

Jeżeli brama odpowiada, wówczas za pomocą ***tracert*** lub ***pathping*** należy sprawdzić, czy przez bramę można wydostać się do innej sieci. Jako parametr podajemy adres komputera poza naszą siecią.

Kolejny krok sprawdzania, to określenie, czy działa system rozpoznawania nazw. W tym celu polecenie ***ping***, ***tracert*** lub ***pathping*** należy wywołać z nazwą, z którą występuje problem.

```
C:\>pathping www.onet.pl

Śledzenie trasy do www.onet.pl [213.180.130.200]
z maksymalną liczbą 30 przeskoków:
  0  k211-01.ckp.pl [10.0.10.1]
  1  ALPHA [10.0.10.254]
  2  router.ckp.pl [212.160.198.1]
  3  194.204.168.133
  4  z.wro-ar2.do.wro-r1.tpnet.pl [195.205.0.129]
  5  z.kat-r1.do.wro-r1.tpnet.pl [194.204.175.177]
  6  z.kra-r1.do.kat-r1.tpnet.pl [194.204.175.132]
  7  do.kra-ar2.z.kra-r1.tpnet.pl [213.25.5.82]
  8  z-tpnet1.onet.pl [194.204.130.130]
  9  pok1-v62.onet.pl [213.180.131.197]
 10  f1virt.onet.pl [213.180.130.200]

Wyliczanie statystyk dla 250 sekund...
Przeskok RTT Zgubione/wysłane = Pct Zgubione/wysłane = adres Pct
  0                                           k211-01.ckp.pl [10.0.10.1]
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  ALPHA [10.0.10.254]
  2    2ms     0/ 100 =  0%     0/ 100 =  0%  router.ckp.pl [212.160.198.1]

  3   34ms     0/ 100 =  0%     0/ 100 =  0%  194.204.168.133
  4   35ms     0/ 100 =  0%     0/ 100 =  0%  z.wro-ar2.do.wro-r1.tpnet.pl [195.205.0.129]
  5   45ms     1/ 100 =  1%     1/ 100 =  1%  z.kat-r1.do.wro-r1.tpnet.pl [194.204.175.177]
  6   48ms     0/ 100 =  0%     0/ 100 =  0%  z.kra-r1.do.kat-r1.tpnet.pl [194.204.175.132]
  7   48ms     0/ 100 =  0%     0/ 100 =  0%  do.kra-ar2.z.kra-r1.tpnet.pl [213.25.5.82]
  8   61ms     1/ 100 =  1%     1/ 100 =  1%  z-tpnet1.onet.pl [194.204.130.130]
  9   ---    100/ 100 = 100%  100/ 100 = 100% pok1-v62.onet.pl [213.180.131.197]
 10   48ms     0/ 100 =  0%     0/ 100 =  0%  f1virt.onet.pl [213.180.130.200]
Śledzenie zakończone.
```

Zadanie 3.2.g – Rozwiązywanie problemów z protokołem TCP/IP

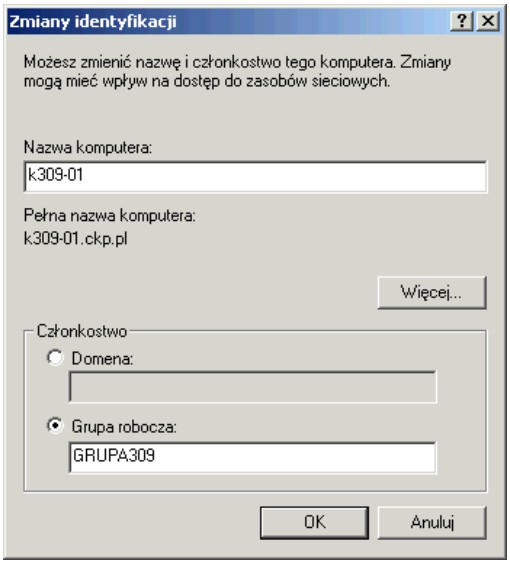
1. Sprawdź konfigurację sieciową za pomocą ***ipconfig***.
2. Wyślij pinga na bramę domyślną.
3. Za pomocą ***pathping*** i ***tracert*** sprawdź trasę do ***wp.pl***

3.3 Windows XP w sieci lokalnej

3.3.a Grupa robocza

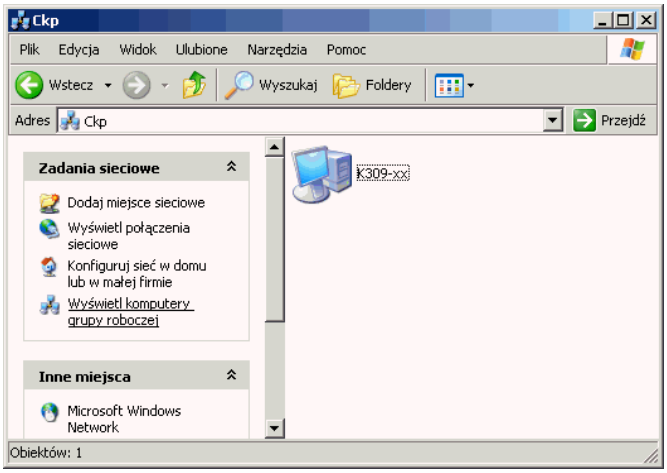
Sieć peer-to-peer zwana grupą roboczą jest siecią składającą się z jednej podsieci, korzystającą ze wspólnego protokołu sieciowego. Obecnie najpopularniejszy jest TCP/IP. Tego typu sieć wykorzystywana jest do łączenia niewielkiej liczby komputerów korzystających ze wspólnych zasobów (od 2 do 10). Uwierzytelnianie użytkowników jest zdecentralizowane, na każdym kliencie umieszczona jest lokalna baza użytkowników. Chcąc korzystać z zasobów innego komputera, użytkownik musi posiadać konto na tym komputerze.

Aby dołączyć się do grupy roboczej, we ***właściwościach systemu,*** na zakładce ***Nazwa komputera*** należy wybrać ***Zmień*** i w polu ***Grupa robocza*** podać nazwę grupy.



Rys. 3.35 Określenie grupy roboczej

Aby dostać się do zasobów innego komputera, korzysta się z ikony ***Moje miejsce sieciowe*** znajdującej się na pulpicie. Po kliknięciu na ***Wyświetl komputery grupy roboczej***, można dostać się do komputerów w grupie roboczej. Wybierając ***Microsoft Windows Network*** do komputerów poza grupą roboczą.



Rys. 3.36 Moje miejsce sieciowe

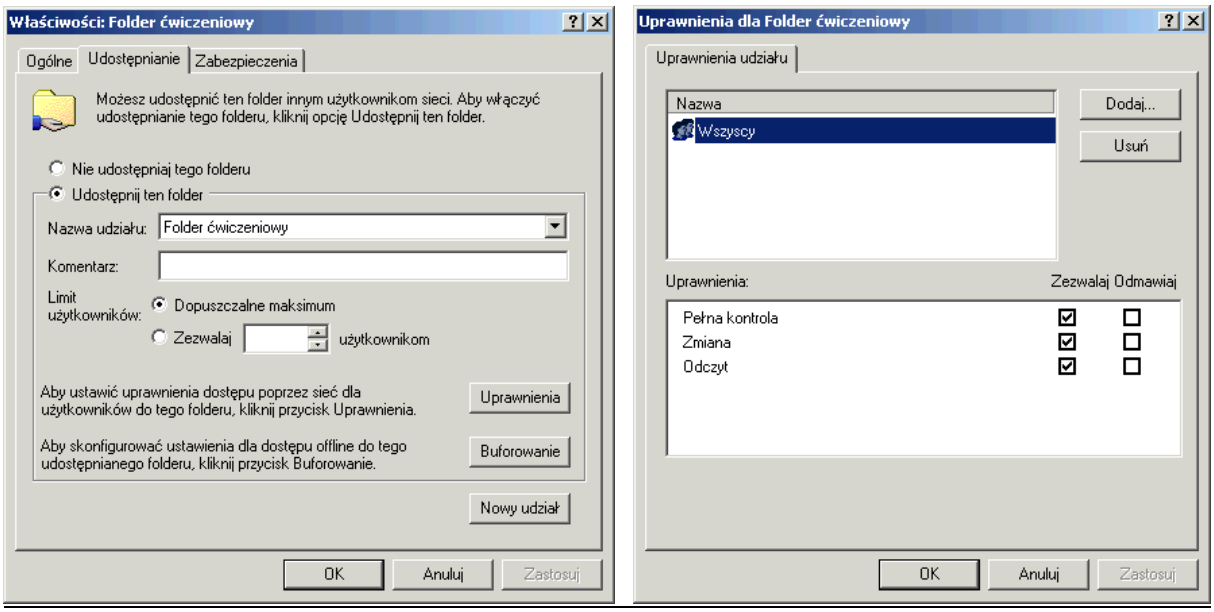
3.3.b Udostępnianie folderów

Jeżeli we właściwościach ***połączenia lokalnego*** zainstalowany jest ***Klient sieci Microsoft Networks*** i załączone jest ***Udostępnianie plików i drukarek w sieciach Microsoft Networks,*** wówczas administratorzy i użytkownicy zaawansowani mogą udostępniać foldery. Dodatkowo muszą posiadać uprawnienie ***Wyświetlenie zawartości folderu***.

W celu udostępnienia folderu, należy prawym przyciskiem myszy kliknąć na określonym folderze i wybrać ***Udostępnianie i Zabezpieczenia.***

Następnie na zakładce ***Udostępnianie*** wybrać ***Udostępnij ten folder*** i podać nazwę udziału (uwaga: jeżeli z folderu mają korzystać użytkownicy pracujący pod systemem MS-DOS, nazwa udziału nie może być dłuższa niż 8 znaków, dla klienta Windows 9x/ME ograniczenie, to 12 znaków).

Udostępniany zasób można opisać ***komentarzem*** i zdefiniować limit użytkowników mogących jednocześnie podłączyć się do zasobu (rzadko wykorzystywany). W systemie Windows 2000/XP Professional maksymalny limit to 10, niezależnie od wpisanej wartości.



Rys. 3.37 Udostępnianie folderu

Udostępnianym zasobom można definiować uprawnienia, po wybraniu przycisku ***Uprawnienia.*** Domyślnie grupa ***Wszyscy*** otrzymuje uprawnienie ***pełnej kontroli. UWAGA: w systemie Windows 2003 Server domyślnym uprawnieniem jest Odczyt dla grupy Wszyscy***.

W sytuacji, gdy korzysta się z systemu plików NTFS, nie powinno się definiować tych uprawnień, a dostęp do folderów ograniczać przez ***Zabezpieczenia*** NTFS. Jeżeli dysk sformatowany jest na FAT, uprawnienia do udostępnianego folderu są jedyną metodą ochrony zasobów sieciowych.

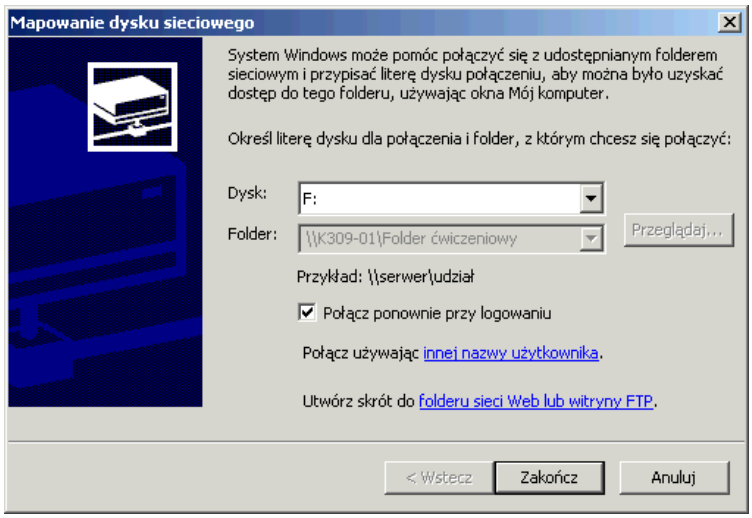
Definiując uprawnienia można zezwolić lub odmówić ***pełnej kontroli***, ***zmiany*** lub ***odczytu.***

Udostępniany folder można ukryć tak, aby nie był dostępny podczas przeglądania sieci. Wystarczy po ***nazwie udziału*** podać znak ***$***. Do takiego zasobu można dostać się przez podanie adresu zasobu postaci ***\\nazwa_komputera\nazwa_zasobu,*** np. po wybraniu ***Start - Uruchom***.

UWAGA: domyślnie wszystkie woluminy udostępniane są dla Administratora jako <litera_dysku$>

Jeżeli użytkownik często korzysta z zasobu sieciowego może podmapować go pod wybraną, wolną literkę dysku. W tym celu, należy prawym przyciskiem myszy kliknąć na udostępnianym folderze i wybrać ***Mapuj dysk sieciowy***.

W oknie ***Mapowanie dysku sieciowego*** można wybrać literkę dysku. Jeżeli zawsze po zalogowaniu mapowanie ma być wykonywane, należy załączyć opcję ***Połącz ponownie przy logowaniu***. Domyślnie system próbuje dokonać autoryzacji, korzystając z nazwy i hasła zalogowanego użytkownika. Podczas mapowania może jednak wykorzystać inne dane do uwierzytelnienia. Trzeba je podać po wybraniu ***Podłącz używając innej nazwy użytkownika***.



Rys. 3.38 Mapowanie dysku

Zadanie 3.3.a – Udostępnianie folderów

1. Ustaw grupę roboczą na ***LAN***.
2. Przez ***Moje miejsce sieciowe*** wejdź na swój komputer.
3. Wejdź na sąsiednie komputery.
4. Załóż konto ***jkowalskixx*** z hasłem ***jk***, przypisz do grupy użytkownicy, gdzie ***xx*** to numer twojego komputera.
5. Załóż folder <***C:\Folder ćwiczeniowy***> i udostępnij go.
6. Ogranicz dostęp do <***C:\Folder ćwiczeniowy***> tak, aby tylko użytkownik ***jkowalskixx*** miał uprawnienie ***Pełna kontrola***.
7. Wejdź do zasobu sieciowego ***Folder ćwiczeniowy*** udostępnianego na sąsiednim komputerze. Utwórz plik lub folder.
8. Załóż folder <***C:\Folder ukryty***> i udostępnij go jako zasób ukryty o nazwie ***ukryty$***. Ustaw zabezpieczenia NTFS tak, aby tylko ***Administrator*** miał dostęp do udostępnianego folderu.

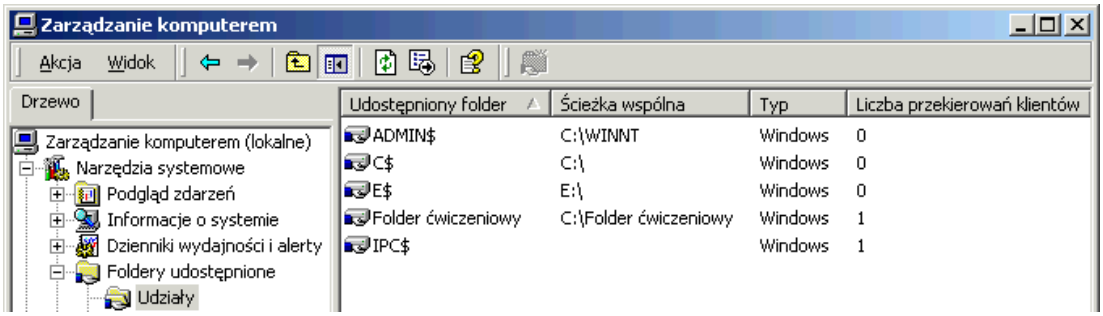
9. Podłącz się do sąsiedniego komputera do zasobu ukrytego ***\\k211-xx\ukryty$***.
10. Podmapuj pod literkę F: udział ***Folder ćwiczeniowy*** sąsiedniego komputera.
11. Podmapuj pod literkę U: udział ***ukryty$*** sąsiedniego komputera.
12. Wejdź na dysk sąsiedniego komputera przez udział sieciowy ***\\k211-xx\c$***

3.3.c Monitorowanie udostępnianych folderów

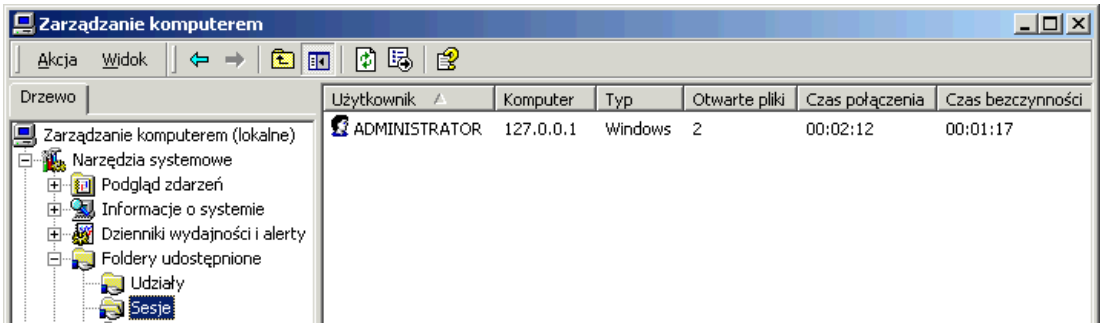
W ***narzędziach administracyjnych*** dostępna jest przystawka konsoli MMC ***zarządzanie komputerem***. W gałęzi ***Narzędzia systemowe – Foldery udostępniane*** można zobaczyć, jakie foldery udostępnione są w systemie i ile osób aktualnie z nich korzysta. Informacje te dostępne są w gałęzi ***Udziały.***

Wybierając ***Sesje,*** można dowiedzieć się, kto podłączony jest do komputera. A po kliknięciu prawym przyciskiem myszy na wybranej osobie, można odłączyć użytkownika przez wybranie ***Zamknij sesję.***

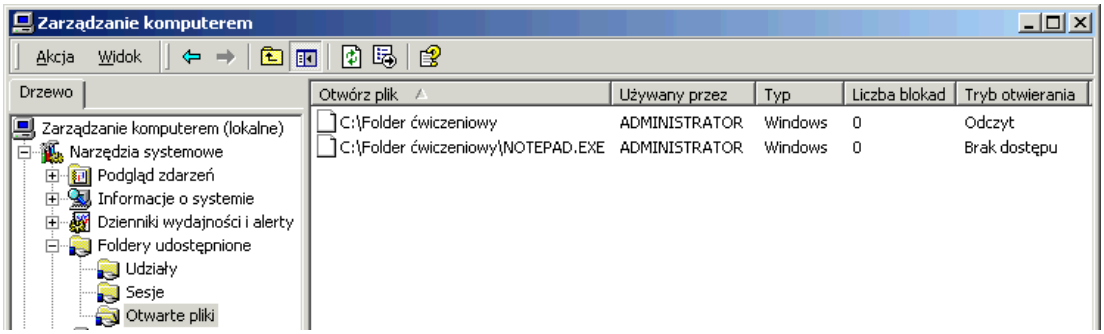
Dostępna jest także gałąź ***Otwarte pliki***, gdzie zobaczymy jakie pliki otwarte są w połączeniach sieciowych. A w menu prawego przycisku myszy można wywołać funkcję ***Zamknij otwarty plik.***



Rys. 3.39 Lista udostępnianych folderów



Rys. 3.40 Lista otwartych sesji



Rys. 3.41 Lista otwartych plików

Zadanie 3.3.b – Monitorowanie zasobów sieciowych

1. Do katalogu <***C:\Folder ćwiczeniowy***> skopiuj ***notepad.exe***.
2. Poproś sąsiada o uruchomienie notatnika z udostępnianego katalogu.
3. Przeglądnij listę otwartych sesji i plików.

3.3.d Domena

Domena jest logiczną grupą komputerów sieciowych, współdzielących centralną katalogową bazę danych, zawierającą konta użytkowników i informacje o zabezpieczeniach obiektów znajdujących się w domenie. Baza ta w systemie Windows 2000/2003 nazywana jest Active Directory (AD). Katalogowa baza znajduje się na serwerach skonfigurowanych jako kontrolery. Jeżeli w sieci znajduje się kilka kontrolerów,
baza replikowana jest między nim, co pozwala zachować większą odporność na awarie.

Obiektami w Active Directory są użytkownicy, grupy, komputery i zasoby, z których mają korzystać. Każdy obiekt opisany jest zbiorem atrybutów, definiowanych przez zestaw reguł zwanych schematem. Obiekty AD mogą być umieszczane w jednostkach organizacyjnych reprezentujących zazwyczaj jednostki administracyjne przedsiębiorstwa np. marketing, produkcja. Mogą także grupować obiekty tego samego typu np. komputery, drukarki. Jednostki organizacyjne i obiekty AD tworzą strukturę drzewiastą. Jednostki organizacyjne i obiekty AD mogą być tworzone na kontrolerze domeny przez administratora, a także ze stacji Windows 2000/XP przez osoby z odpowiednimi uprawnieniami.

Podczas zakładania konta użytkownika, grupy, czy komputera tworzony jest identyfikator zabezpieczenia (SID – security identifier). Identyfikator ten wykorzystywany jest podczas tworzenia list kontroli dostępu do obiektów.

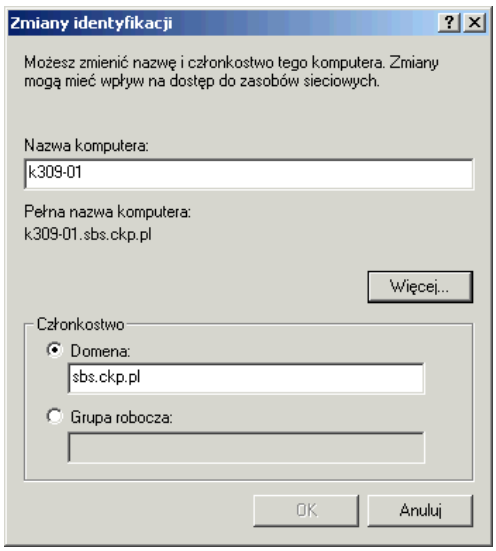
Usługa Active Directory ściśle związana jest z systemem DNS. Nazwy domen Windows 2000/2003 tworzone są w oparciu o hierarchiczną strukturę nazewnictwa DNS. Przypomina ona odwrócone drzewo. Na górze znajduje się korzeń (pojedyncza domena główna), pod którą znajdują się domeny nadrzędne i podrzędne (gałęzie i liście). Każdy komputer w domenie identyfikowany jest przez pełną nazwę (FQDN), składającą się z nazwy komputera i domeny, do której należy. Aby dołączyć się do domeny, konieczne jest podanie pełnej nazwy FQDN. Przykładowa domena może wyglądać, jak na poniższym rysunku.

Jednym z ważniejszych zadań kontrolera domeny jest potwierdzanie tożsamości użytkowników. Chcąc dostać się do stacji roboczej pracującej w domenie, należy podać nazwę konta w domenie i hasło. Po poprawnej autoryzacji, użytkownik otrzymuje dostęp do zasobów, zgodnie z listami kontroli dostępu do obiektów.

Podczas logowania do domeny, system przetwarza także zasady grup użytkownika i komputera, zdefiniowane na kontrolerze domeny.

Aby dołączyć się do domeny, we ***właściwościach systemu,*** na zakładce ***Identyfikacja sieciowa*** należy wybrać ***Właściwości***, następnie podać nazwę komputera i domeny.

Komputer powinien posiadać konto w domenie. Jeżeli takiego konta nie ma, to przy podłączaniu do domeny można podać nazwę użytkownika z prawem dodawania komputerów do domeny. Wówczas system automatycznie utworzy konto dla komputera. Standardowo każdy użytkownik domeny, posiadający konto w Active Directory, otrzymuje prawo dodania komputera do domeny.



Rys. 3.42 Dołączenie komputera do domeny

3.4 Literatura

[1] Windows XP Professional Training Kit, Microsoft Press.

[2] Windows XP Professional Resource Kit, Microsoft Press.

[3] http://www.microsoft.com/poland/windows2000/win2000prof/default.asp

3.5 Lista zadań do wykonania i samoocena

Nr zadania	Temat	Ocena (1 – 5 pt.)
3.2.a	Konfigurowanie protokołu TCP/IP	
3.2.b	Rozwiązywanie nazw	
3.2.c	Konfigurowanie hostów wieloadresowych	
3.2.d	Routing TCP/IP	
3.2.e	Konfiguracja IPSec	
3.2.f	Rozwiązywanie problemów z protokołem TCP/IP	
3.3.a	Udostępnianie folderów	
3.3.b	Monitorowanie zasobów sieciowych	