Bezpieczeństwo
Sieci Komputerowych

Część 3.
Charakterystyka sieci komputerowych, infrastruktury sieciowej oraz informatycznych technologii komunikacyjnych (c.d.).

Praktyczny Pedagog

Bezpieczeństwo Sieci Komputerowych

PROGRAM ZAJĘĆ cz. 3

Cechy sieci bezprzewodowych.
Dostępność danych w sieciach – jak ją zmierzyć. Pojęcia: przepustowość, opóźnienie, szerokość pasma.
Protokoły sieciowe warstwy łącza danych – MAC, ARP, IP.
Protokoły warstwy transportowej – TCP, UDP.
Protokoły warstwy aplikacji – FTP, HTTP, SMTP, POP3, DNS.
Termin: porty.
Najpopularniejsze usługi spotykane w sieciach, ich protokoły i porty.
Pojęcia: brama sieciowa, maska podsieci, DHCP.
Wyznaczenie drogi dla pakietów – routing.
Konfiguracja interfejsu sieciowego.

Sieci bezprzewodowe

Punkt dostępowy jak każde urządzenie sieci bezprzewodowych ma ograniczony zasięg, który w przypadku niektórych modeli możemy zwiększać za pomocą zewnętrznych konfigurowalnych anten. Na zasięg punktu dostępowego poza rodzajem użytej anteny ma wpływ także umiejscowienie (wewnątrz lub na zewnątrz budynku), inne elektroniczne urządzenia działające na tej samej częstotliwości a dla urządzeń znajdujących się na otwartej przestrzeni także warunki pogodowe.

Standard	Przepustowość	Częstotliwość	Zasięg
802.11a	6, 9, 12, 18, 24, 36, 48, 54 Mbit/s	5 GHz	18m
802.11b	1, 2, 5.5, 11, (22 i 44)[1] Mbit/s	2,4 GHz	45m
802.11g	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbit/s	2,4 GHz	40m
802.11n	100, 250, 540 Mbit/s	2,4 lub 5.0 GHz	40m

Tabela 1. Parametry zawarte w standardach rodziny 802.11.

Dostępność danych w sieciach – jak ją zmierzyć*

• **Przepustowość** (ang. throughput) jest szybkością z jaką system komputerowy wysyła lub otrzymuje dane, mierzoną w bitach na sekundę (bps). Dla określonych technologii sieciowych podaje się maksymalną teoretyczną przepustowość (na przykład dla standardu fast ethernet wynosi ona 100 Mbps).

• **Opóźnienie** (ang. latency) jest definiowane jako czas, który upłynął pomiędzy rozpoczęciem nadawania pakietu przez stację wysyłającą, a rozpoczęciem odbierania go przez stację odbiorczcą (tzw. opóźnienie jednostronne).
Jako miernika opóźnienia w rzeczywistych sieciach używa się często wskaźnika RTT (ang. Round Trip Time) – czasu jaki upływa od wysłania pakietu do otrzymania odpowiedzi nań (polecenie *ping)*.

*http://en.wikipedia.org Wikipedia Wolna Encyklopedia, wersja anglojęzyczna, hasła bandwidth, Measuring_data_throughput , throughput

Dostępność danych w sieciach – jak ją zmierzyć

• **Szerokość pasma transmisyjnego** (ang. bandwidth) wyrażona w Hz jest dla sygnału analogowego różnicą częstotliwości sygnału, dla których transformanta Fouriera jest różna od zera. Dla sygnału cyfrowego często używa się zamiennie pojęć „szerokość pasma" i „przepustowość".

• **Rzeczywista szybkość** (albo mniej dokładnie: prędkość) transmisji (ang. bitrate) jest rzeczywistą prędkością – mierzoną w bitach na sekundę lub czasem w ramkach lub pakietach na sekundę – z jaką system komputerowy wysyła lub otrzymuje dane. Z oczywistych względów prędkość transmisji nie jest większa od przepustowości jaką oferuje dana sieć.

Szerokość pasma

Szerokość pasma jest skończona. Innymi słowy, niezależnie od medium użytego do budowy sieci ilość informacji przenoszonych przez tę sieć jest ograniczona. Szerokość pasma jest ograniczona prawami fizyki i technologiami umieszczania informacji w medium.

Im większa szerokość pasma, tym większy koszt. Można kupić sprzęt dla sieci LAN, który zapewni niemal nieograniczoną szerokość pasma przez długi czas. W przypadku połączeń WAN prawie zawsze trzeba kupić szerokość pasma od dostawcy usług.

Popyt na szerokość pasma nieustannie rośnie. Wraz z powstaniem technologii i infrastruktur sieciowych zapewniających szersze pasmo tworzone są aplikacje korzystające z tych możliwości.

Szerokość pasma

Szerokość pasma zależy od typu użytego medium oraz od użytej technologii sieci LAN lub WAN. Niektóre różnice wynikają z fizycznych właściwości medium. Sygnały są przesyłane miedzianą skrętką, kablem koncentrycznym, światłowodem lub za pomocą łącza bezprzewodowego.

Rzeczywista szerokość pasma jest określana również poprzez wybrane metody sygnalizacji, rodzaje kart sieciowych i inne elementy sieci.

Szerokość pasma

Typowa sieć LAN może być tak skonstruowana, aby zapewniała pasmo 100 Mb/s dla każdej stacji roboczej, ale to nie znaczy, że dowolny użytkownik będzie mógł w rzeczywistości przesłać siecią sto megabitów danych w każdej sekundzie korzystania z niej.

Przepustowość oznacza rzeczywistą szerokość pasma zmierzoną o określonej porze dnia, przy użyciu określonych tras internetowych i podczas transmisji siecią określonych zbiorów danych.

Szerokość pasma

Niestety z wielu powodów przepustowość jest często znacznie mniejsza niż maksymalna możliwa szerokość pasma cyfrowego używanego medium. Niektórymi spośród czynników mających wpływ na przepustowość są:

- urządzenia intersieciowe
- typ przesyłanych danych
- topologia sieci
- liczba użytkowników sieci
- komputer użytkownika
- komputer pracujący jako serwer
- warunki zasilania

Dzięki okresowym pomiarom przepustowości administrator sieci będzie miał świadomość zmian wydajności sieci i potrzeb jej użytkowników.
Sieć można dzięki temu dostosowywać do aktualnych wymagań.

Protokoły sieciowe

W celu wymiany informacji różne urządzenia sieciowe i rozmaite systemy operacyjne posługują się **protokołami** — zbiorami reguł, jakich musza przestrzegać pakiety krążące w sieci, by mogły być przyjęte, zrozumiane i przetworzone. Protokoły odpowiadają również za prawidłowe tworzenie pakietów.

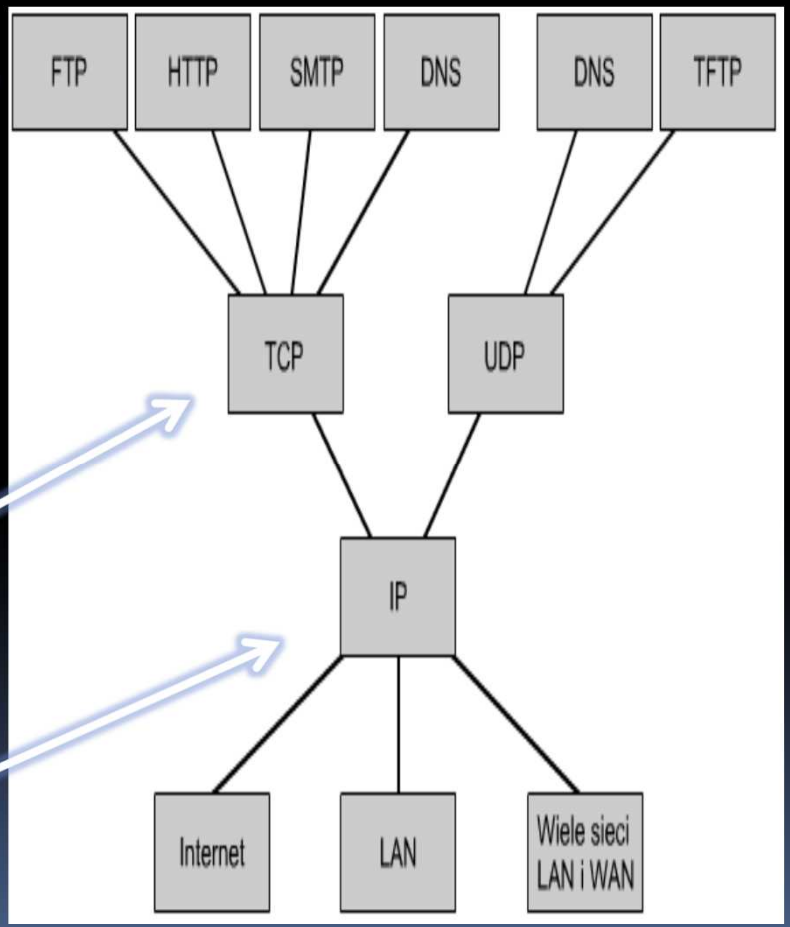
Protokoły sieciowe

Na rysunku przedstawiono niektóre spośród popularnych protokołów zdefiniowanych przy użyciu warstw modelu odniesienia TCP/IP.

Najczęściej stosowane protokoły warstwy aplikacji to:
protokół FTP (ang. *File Transfer Protocol*)
protokół HTTP (ang. *Hypertext Transfer Protocol*)
protokół SMTP (ang. *Simple Mail Transfer Protocol*)
protokół DNS (ang. *Domain Name System*)
protokół TFTP (ang. *Trivial File Transfer Protocol*)

Najczęściej stosowane protokoły warstwy transportowej:
protokół TCP (ang. *Transport Control Protocol*)
protokół UDP (ang. *User Datagram Protocol*)

Główny protokół warstwy internetowej to protokół IP (ang. *Internet Protocol*)



MAC, IP oraz ARP – protokół warstwy łącza danych

Adres MAC (*Media Access Control*) to unikalny sprzętowy numer urządzenia sieciowego, nadawany w procesie produkcji na stałe (chociaż metodami programowymi można go zmieniać).

Listę kodów przypisanych do producentów (pierwsze 24 bity adresu MAC) można znaleźć pod adresem
http://standards.ieee.org/regauth/oui/oui.txt

Gdy docelowy adres MAC ma wartość FF-FF-FF-FF-FF-FF, wówczas następuje rozgłaszanie (*broadcast*).

MAC, IP oraz ARP – protokół warstwy łącza danych

Adres IP (*Internet Protocol*) to numer przypisywany urządzeniom sieciowym, zarówno w sieciach lokalnych, jak i Internecie. Najczęściej IP zapisuje się w postaci dziesiętnej, łatwiejszej do zapamiętania. Przykładowy adres IP w zapisie dziesiętnym: **156.17.1.38**.

Adres IP składa się z **części sieciowej** oraz **części hosta**. W różnych adresach IP występują one w różnych „proporcjach", a do ich oddzielenia
stworzono pojęcie **maski podsieci** (*subnet mask*). Cała 32-bitowa przestrzeń adresowa jest podzielona pulę publiczną oraz prywatną.

MAC, IP oraz ARP – protokół warstwy łącza danych

Trzy następujące pule adresów IP zostały zarezerwowane do użytku w sieciach lokalnych:

od 10.0.0.0 do 10.255.255.255
od 172.16.0.0 do 172.31.255.255
od 192.168.0.0 do 192.168.255.255

Sieci LAN z adresacją prywatną mogą łączyć się z internetem z wykorzystaniem usługi NAT.

Adresy NAT mogą być wykorzystywane wyłącznie za zaporami firewall albo serwerami proxy, które ukrywają przed Internetem własne schematy adresowania. Utrudnia to dostęp do sieci osobom nieuprawnionym i umożliwia współużytkowania jednego adresu publicznego przez wiele stacji

MAC, IP oraz ARP – protokół warstwy łącza danych

ARP (*Address Resolution Protocol*) to protokół wykorzystywany do zamieniania adresów **logicznych** (IP) na adresy **fizyczne** (MAC) urządzeń sieciowych. **ARP ma zastosowanie tylko w sieciach LAN**. Operuje w warstwie łącza danych (druga warstwa modelu OSI).

Tablica ARP zawiera pary IP-MAC dla konkretnych urządzeń. Każde „inteligentne" urządzenie sieciowe posiada taka tablice, dzięki czemu może lokalizować inne urządzenia w sieci na podstawie ich adresów sprzętowych. Jeśli informacja ma być wysłana poza siec lokalna (ewentualnie podsieć), to adres MAC jest zastępowany adresem IP.

Protokoły warstwy transportowej TCP/UDP

Protokoły warstwy czwartej ISO/OSI

Zapewniają rozszerzoną adresację (w obrębie pojedynczego hosta)

65535 wartości (dwa bajty oprócz 0) dla każdego z protokołów

Pozwalają na kierowanie strumienia danych do odpowiedniej aplikacji

Protokoły warstwy transportowej TCP/UDP

Cecha różniąca rodziny TCP i UDP jest **sposób dostarczania informacji** do celu. Protokół TCP posiada mechanizmy sprawdzania poprawności transmisji, obliczania sum kontrolnych pakietów oraz wykrywania i korekcji błędów. Stosuje sie go w usługach, które musza być **niezawodne**, np. w poczcie elektronicznej, protokole HTTP czy SSH.

Protokół UDP natomiast jest protokołem **bezpołączeniowym**, mającym bardzo ograniczona kontrole poprawności transmisji. Wymaga mniej „wysiłku" zarówno ze strony systemu źródłowego, jak i docelowego na stworzenie i przetworzenie pakietu. Ma zastosowanie w usługach, które maja mniejsze wymagania co do poprawności transmisji, np. przekaz dźwięku lub obrazu (usługi *Voice over IP*, strumienie wideo, połączenia telekonferencyjne) bądź nie mogą „pozwolić" sobie na zbędny narzut na kontrole poprawności, np. DNS czy NFS (*Network File System*).

Porty

Gdyby nie było portów, komunikacja za pośrednictwem standardowych protokołów internetowych TCP i UDP byłaby niemożliwa. To dzięki portom wiele aplikacji może jednocześnie wymieniać dane, wykorzystując jedno łącze internetowe

Numery portów stanowią jeden z podstawowych elementów stosowania protokołów TCP i UDP. Gdy dane docierają do komputera docelowego, muszą jeszcze zostać dostarczone do właściwej aplikacji. Podczas transportu informacji przez warstwy sieci potrzebny jest mechanizm, który najpierw gwarantuje przekazanie danych do właściwego w danym wypadku protokołu.

Porty

Łączenie danych z wielu źródeł w jeden strumień danych nosi nazwę multipleksowania. Protokół internetowy (IP) musi zatem poddać dane nadchodzące z sieci procesowi demultipleksowania. W tym celu IP oznacza protokoły transportowe numerami protokołów. Same protokoły transportowe wykorzystują z kolei numery portów do identyfikacji aplikacji.

Numer protokołu IP zawarty jest w jednym bajcie, w trzecim słowie nagłówka datagramu. Wartość ta determinuje przekazanie do odnośnego protokołu w warstwie transportowej; przykładowo 6 to TCP, 17 to UDP. Protokół transportowy musi przekazać otrzymane dane do właściwego procesu aplikacji.

Aplikacje identyfikowane są na podstawie numerów portów o długości 16 bitów, do których dane kierowane są po nadejściu do komputera docelowego. W pierwszym słowie każdego nagłówka TCP czy UDP zapisany jest też numer portu źródłowego i numer portu docelowego. Jeżeli aplikacja ma być dostępna pod określonym numerem portu, musi przekazać tę informację do stosu protokółu TCP/IP.

Porty

Porty są nierozłącznie związane z protokołami. Niektóre porty są uznawane za standardowe, inne można dowolnie zmieniać. Porty przyjmują wartości z zakresu 0. . . 65535, a ich umowny podział jest następujący:
dobrze znane (systemowe, *well known*): 0-1023
zarezerwowane: 1024-49151
prywatne (dynamiczne): 49152-65535

Porty

FTP (*File Transfer Protocol*) — 20 i 21 (TCP)
SSH (*Secure SHell*) — 22 (TCP)
SMTP (*Simple Mail Transport Protocol*) — 22 (TCP)
DNS (*Domain Name Service*) — 53 (UDP)
TFTP (*Trivial File Transfer Protocol*) — 69 (UDP)
HTTP (*Hyper Text Transfer Protocol*) — 80 i 8080 (TCP)
POP3 (*Post Office Protocol*) — 110 (TCP) (może się różnić)
NNTP (*Network News Transfer Protocol*) — 119 (TCP)
SNMP (*Simple Network Management Protocol*) — 161 (UDP)
HTTPS (*HTTP over TLS/SSL*) — 443 (TCP)
NFS (*Network File System*) — 2049 (UDP i TCP)

Zasoby współdzielone w sieci

Zasoby współdzielone przez urządzenia sieciowe i ich użytkowników można rozumieć wielopłaszczyznowo, miedzy innymi jako:

- sprzęt, np. drukarki i skanery
- pojedyncze pliki lub ich zbiory
- programy
- bazy danych
- moc obliczeniowa
- przestrzeń dyskowa

Usługi w sieciach

WWW
FTP
E-mail
Bazy danych
Pulpit zdalny

DNS – nazwy zamiast liczb

Urządzenia sieciowe komunikując się ze sobą posługują się adresami IP (ewentualnie adresami MAC). Dla człowieka łatwiejsze do zapamiętania są słowa, dlatego opracowano protokół tłumaczący tzw. **nazwy domenowe** na adresy IP. Protokół ten nosi nazwę **usługi nazw domenowych** (*Domain Name Service*, DNS).
DNS jest jednym z filarów Internetu. Jest to usługa rozproszona i hierarchiczna. Tzw. domeny najwyższego poziomu dzielą się na domeny niższych poziomów i tworzą strukturę drzewiasta. Przykłady „tradycyjnych" domen najwyższego poziomu: com, edu, gov, net, org. Szczególnym rodzajem domen najwyższego poziomu sa **domeny narodowe**, np. pl, ca, ru, br.
Przyznawaniem nazw domenowych zajmuje sie IANA i jej regionalne przedstawicielstwa, którzy z kolei udzielają odpowiednich uprawnień lokalnym dostawcom Internetu.

Brama sieciowa

Maszyna podłączona do sieci komputerowej, za pośrednictwem której komputery z sieci lokalnej komunikują się z komputerami w innych sieciach.

W sieci TCP/IP domyślna brama (sieciowa) (ang. default gateway) oznacza router, do którego komputery sieci lokalnej mają wysyłać pakiety o ile nie powinny być one kierowane w sieć lokalną lub do innych, znanych im routerów. W typowej konfiguracji sieci lokalnej TCP/IP wszystkie komputery korzystają z jednej domyślnej bramy, która zapewnia im łączność z innymi podsieciami lub z Internetem. Ustawienie adresu bramy domyślnej jest – oprócz nadania maszynie adresu IP i maski podsieci – podstawowym elementem konfiguracji sieci TCP/IP. Maszyna bez podanego adresu bramy domyślnej może wymieniać pakiety tylko z komputerami w tej samej sieci lokalnej.

Maska podsieci

(ang. subnetwork mask, address mask) – liczba służąca do wyodrębnienia w adresie IP części sieciowej od części hosta.

Po wykonaniu iloczynu bitowego maski i adresu IP komputera otrzymujemy adres IP całej sieci, do której należy ten komputer.

Model adresowania w oparciu o maski adresów wprowadzono w odpowiedzi na niewystarczający, sztywny podział adresów na klasy A, B i C. Pozwala on w elastyczny sposób dzielić duże dowolne sieci (zwłaszcza te o ograniczonej puli adresów IP) na mniejsze podsieci.

Maska podsieci

Maski podsieci w obrębie jednej klasy:

CIDR	Maska	Liczba dostępnych adresów hostów
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/29	255.255.255.248	6
/30	255.255.255.252	2

Liczba dostępnych adresów hostów jest o 2 mniejsza, ponieważ odpadają na adres sieci (pierwszy z zakresu) i broadcast (ostatni z zakresu).

DHCP

(ang. Dynamic Host Configuration Protocol – protokół dynamicznego konfigurowania węzłów) – protokół komunikacyjny umożliwiający komputerom uzyskanie od serwera danych konfiguracyjnych, np. adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski podsieci.

DHCP

Protokół DHCP opisuje trzy techniki przydzielania adresów IP:

- **przydzielanie ręczne** oparte na tablicy adresów MAC oraz odpowiednich dla nich adresów IP. Jest ona tworzona przez administratora serwera DHCP. W takiej sytuacji prawo do pracy w sieci mają tylko komputery zarejestrowane wcześniej przez obsługę systemu.
- **przydzielanie automatyczne**, gdzie wolne adresy IP z zakresu ustalonego przez administratora są przydzielane kolejnym zgłaszającym się po nie klientom.
- **przydzielanie dynamiczne**, pozwalające na ponowne użycie adresów IP. Administrator sieci nadaje zakres adresów IP do rozdzielenia. Wszyscy klienci mają tak skonfigurowane interfejsy sieciowe, że po starcie systemu automatycznie pobierają swoje adresy. Każdy adres przydzielany jest na pewien czas. Taka konfiguracja powoduje, że zwykły użytkownik ma ułatwioną pracę z siecią.

Niektóre serwery DHCP dodatkowo przydzielają każdemu klientowi własny adres DNS, przekazywany na serwer nazw protokołem zgodnym ze specyfikacją.

Routing

Wyznaczaniem drogi dla pakietów przeznaczonych dla odległych systemów zajmują się *routery*. Określenie, czy pakiet jest przeznaczony dla urządzenia w sieci lokalnej czy poza nią opiera się na masce sieci urządzenia, które jest źródłem pakietu. Jeśli maska sieci celu jest identyczna z maska sieci źródła pakietu, to rozpoznanie urządzenia docelowego odbywa się za pomocą protokołu ARP. Jeśli maski urządzenia źródłowego i docelowego są różne — pakiet jest kierowany do urządzenia trasującego. Przechodząc przez kolejne *routery* pakiet dociera do urządzenia docelowego.

Trasę pakietu do zdalnego systemu można sprawdzić za pomocą polecenia *traceroute* (Linux) lub *tracert* (Windows). Różne ciekawe informacje o odległych hostach można również uzyskać komenda ping, która posługuje się protokołem ICMP (*Internet Control Message Protocol*).

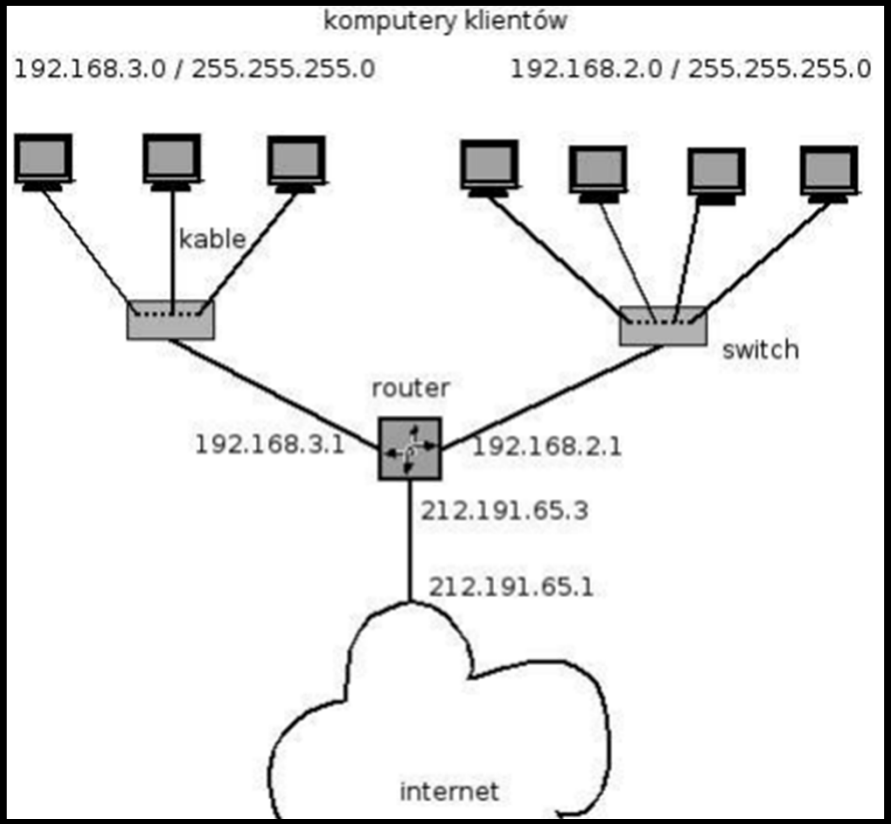
Routing

Trasowanie musi zachodzić między co najmniej dwiema podsieciami, które można wydzielić w ramach jednej sieci komputerowej. Urządzenie tworzy i utrzymuje tablicę trasowania, która przechowuje ścieżki do konkretnych obszarów sieci oraz metryki z nimi związane (odległości od siebie licząc kolejne routery).

Skuteczne działanie routera wymaga wiedzy na temat otaczających go urządzeń, przede wszystkim innych routerów oraz przełączników. Może być ona dostarczona w sposób statyczny przez administratora, wówczas nosi ona nazwę tablicy statycznej lub może być pozyskana przez sam router od sąsiadujących urządzeń pracujących w trzeciej warstwie, tablice tak konstruowane nazywane są dynamicznymi.

Podczas wyznaczania tras dynamicznych router korzysta z różnego rodzaju protokołów trasowania i polega przede wszystkim na odpytywaniu sąsiednich urządzeń o ich tablice trasowania, a następnie kolejnych w zależności od zapotrzebowań ruchu, który urządzenie obsługuje.

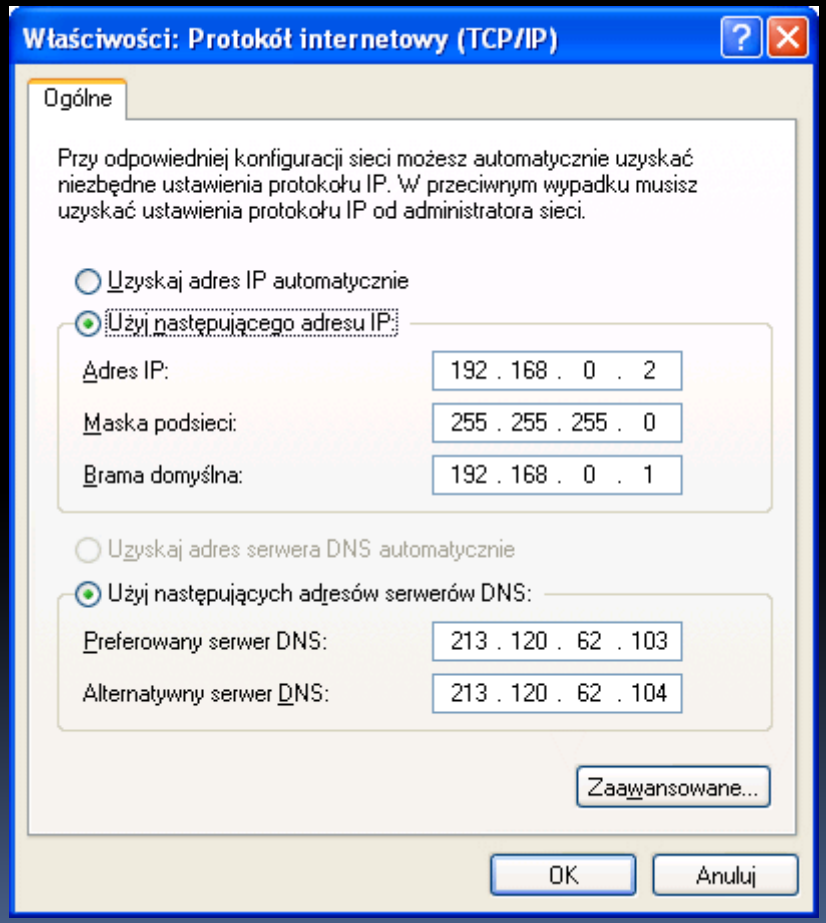
Routing



W takiej sieci komputery z podsieci 192.168.3.0 ustawią adres swojej domyślnej bramy na 192.168.3.1, komputery z podsieci 192.168.2.0 ustawią adres 192.168.2.1. Na powyższym rysunku widzimy że router posiada 3 karty sieciowe po jednej w obsługiwanych podsieciach oraz jedną łączącą go z internetem za pośrednictwem jego routera dostępowego. Tak więc router posiadałby wpisy przekierowujące pakiety pomiędzy dwoma podsieciami oraz domyślną bramę pod adresem 212.191.65.1

Konfiguracja interfejsu sieciowego

Konfiguracja Windows:
graficzna



Konfiguracja interfejsu sieciowego

Konfiguracja Windows:
netsh

Komenda NETSH służy do wszechstronnego konfigurowania sieci. Działa ona w wierszu poleceń i przez to może niektórym się wydawać niewygodna. Niepodważalną zaletą tej komendy jest możliwość szybkiej zmiany konfiguracji sieci poprzez proste skrypty wsadowe. Pozwala to używać szybkiego przełączania miedzy wieloma konfiguracjami sieci zrzuconymi do pliku. Wpierw należy zrzucić obecną konfiguracje sieci poprzez komendę:

netsh interface dump > siec1.txt

W pliku siec1.txt znajdzie się cała konfiguracja obecna naszej sieci na komputerze.

Następnie można przekonfigurować sieć na inny wariant, zrzucić ją analogicznie zapisując do pliku np. siec2.txt. Odtwarzanie konfiguracji sieci z pliku odbywa się poprzez poniższą komendę:
netsh -f siec1.txt

Koniec części 3.