# TCP/IP

**TCP** (ang. Transmission Control Protocol) – strumieniowy protokół komunikacji między dwoma komputerami. Został stworzony przez Vintona Cerfa i Roberta Kahna. Jest on częścią większej całości określanej jako stos TCP/IP. W modelu OSI TCP odpowiada warstwie Transportowej.

W przeciwieństwie do UDP, TCP zapewnia wiarygodne połączenie dla wyższych warstw komunikacyjnych przy pomocy sum kontrolnych i numerów sekwencyjnych pakietów, w celu weryfikacji wysyłki i odbioru. Brakujące pakiety są obsługiwane przez żądania retransmisji. Host odbierający pakiety TCP porządkuje je według numerów sekwencyjnych tak, by przekazać wyższym warstwom modelu OSI pełen, złożony segment.

Chociaż protokół definiuje pakiet TCP, to z punktu widzenia wyższej warstwy oprogramowania, dane płynące połączeniem TCP należy traktować jako ciąg oktetów. W szczególności – jednemu wywołaniu funkcji API (np. send()) nie musi odpowiadać wysłanie jednego pakietu. Dane z jednego wywołania mogą zostać podzielone na kilka pakietów lub odwrotnie – dane z kilku wywołań mogą zostać połączone i wysłane jako jeden pakiet (dzięki użyciu algorytmu Nagle'a). Również funkcje odbierające dane (recv()) w praktyce odbierają nie konkretne pakiety, ale zawartość bufora stosu TCP/IP, wypełnianego sukcesywnie danymi z przychodzących pakietów.

Charakterystyczny dla TCP jest moment nawiązania połączenia, nazywany ang. *three-way handshake*. Host inicjujący połączenie wysyła pakiet zawierający segment TCP z ustawioną flagą SYN (synchronize). Host odbierający połączenie, jeśli zechce je obsłużyć, odsyła pakiet z ustawionymi flagami SYN i ACK (acknowledge – potwierdzenie). Inicjujący host powinien teraz wysłać pierwszą porcję danych, ustawiając już tylko flagę ACK (gasząc SYN). Jeśli host odbierający połączenie nie chce lub nie może odebrać połączenia, powinien odpowiedzieć pakietem z ustawioną flagą RST (Reset). Prawidłowe zakończenie połączenia polega na wysłaniu flagi FIN.

Aplikacje, w których zalety TCP przeważają nad wadami (większy koszt związany z utrzymaniem sesji TCP przez stos sieciowy) to m.in. HTTP, SSH, FTP czy SMTP/POP3 i IMAP4.

| + | Bity 0 - 3 | 4 - 9 | 10 - 15 | 16 - 31 |
|---|---|---|---|---|
| 0 | Port nadawcy | | | Port odbiorcy |
| 32 | Numer sekwencyjny | | | |
| 64 | Numer potwierdzenia | | | |
| 96 | Przesunięcie danych | Zarezerwowane | Flagi | Szerokość okna |
| 128 | Suma kontrolna | | | Wskaźnik priorytetu |
| 160 | Opcje (opcjonalnie) | | | |
| 160/192+ | Dane | | | |

*Nagłówek TCP*

***

**IP (protokół)** (ang. Internet Protocol) to protokół komunikacyjny warstwy sieciowej modelu OSI (warstwy internet w modelu TCP/IP). Używany powszechnie w Internecie i sieciach lokalnych.

Dane w sieciach IP są wysyłane w formie bloków określanych mianem pakietów. W przypadku protokołu IP, przed rozpoczęciem transmisji nie jest zestawiana wirtualna sesja komunikacyjna pomiędzy dwoma hostami, które nie komunikowały się ze sobą wcześniej.

Protokół IP jest protokołem zawodnym - nie gwarantuje, że pakiety dotrą do adresata, nie zostaną sfragmentowane, czy też zdublowane, a ponadto mogą dotrzeć do odbiorcy w innej kolejności niż zostały nadane. Niezawodność transmisji danych jest zapewniana przez protokoły warstw wyższych (np. TCP), znajdujących się w hierarchii powyżej warstwy sieciowej.

**IPv4** (ang. Internet Protocol version 4) - czwarta wersja protokołu komunikacyjnego IP przeznaczonego dla Internetu. Identyfikacja hostów w IPv4 opiera się na adresach IP. Dane przesyłane są w postaci standardowych datagramów. Wykorzystanie IPv4 jest możliwe niezależnie od technologii łączącej urządzenia sieciowe – sieć telefoniczna, kablowa, radiowa, itp. IPv4 znajduje się obecnie w powszechnym użyciu. Dostępna jest również nowsza wersja - IPv6. Dokładny opis czwartej wersji protokołu IP znajduje się w RFC 791. W modelu DoD protokół IPv4 znajduje się w warstwie sieciowej.

<table>
<tr><th>+</th><th>Bity 0 - 3</th><th>4 - 7</th><th>8 - 15</th><th>16 - 18</th><th>19 - 31</th></tr>
<tr><td>0</td><td>Wersja</td><td>Długość nagłówka</td><td>Typ usługi</td><td colspan="2">Całkowita długość</td></tr>
<tr><td>32</td><td colspan="3">Numer identyfikacyjny</td><td>Flagi</td><td>Kontrola przesunięcia</td></tr>
<tr><td>64</td><td colspan="2">Czas życia pakietu (TTL)</td><td>Protokół warstwy wyższej</td><td colspan="2">Suma kontrolna nagłówka</td></tr>
<tr><td>96</td><td colspan="5">Adres źródłowy</td></tr>
<tr><td>128</td><td colspan="5">Adres docelowy</td></tr>
<tr><td>160</td><td colspan="5">Opcje</td></tr>
<tr><td>192</td><td colspan="5">Dane</td></tr>
</table>

*Budowa datagramu*

Pierwsze, 4-bitowe pole zawiera numer wersji protokołu IP (dla IPv4 jest to 4).

Kolejne 4-bitowe pole zawiera długość samego nagłówka protokołu (bez danych).

Następne 8 bitów prezentuje tzw. "typ usługi" (ang. Type of Service). Jest to najbardziej podstawowy sposób wyznaczania priorytetu danego datagramu. Na podstawie ToS routery mogą szybciej (np. dla sesji SSH), lub wolniej (np. dla przesyłania danych) przepuszczać przez siebie dane datagramy, zwiększając bądź też zmniejszając w ten sposób interaktywność transmisji.

Kolejnym 16-bitowym polem jest całkowita długość pakietu (razem z danymi). Jego długość (wynosząca 2^16) umożliwia ustawienie rozmiaru pakietu na 65536 bajtów. Warto dodać, że minimalny rozmiar pakietu to 20 bajtów.

Kolejne 16-bitowe pole to numer identyfikacyjny, potrzebny między innymi do fragmentacji i defragmentacji pakietów.

Kolejnym 3-bitowym polem są flagi, które są używane przy fragmentacji pakietów.

Następne 13-bitowe pole służy do odpowiedniego "poukładania" pofragmentowanych pakietów w taki sposób, aby dane zawarte w tych pakietach miały taki sam układ, jak w pakiecie przed fragmentacją.

Pole TTL (8 bitów) to czas życia pakietów (ang. time to live). Jest to liczba z zakresu 0-255. Przy przechodzeniu pakietu przez router jest ona zmniejszana o jeden. W momencie osiągnięcia przez TTL zera, router zatrzymuje i "zabija" pakiet.

Kolejne, 8-bitowe pole to numer protokołu warstwy wyższej, takimi jak ICMP (1), TCP (6) czy UDP (17).

Następnym polem jest suma kontrolna pakietu. Służy ona kontroli, czy wszystkie dane zostały przetransmitowane. Przy każdej zmianie zawartości pakietu, router oblicza sumę kontrolną dla pakietu i zapisuje ją w odpowiednim polu.

Dalsze pola zawierają adres źródłowy i docelowy. To właśnie na podstawie nich można określić pochodzenie i miejsce docelowe pakietu w sieci.

Ostatnim, 32-bitowym polem są opcje, które w normalnej transmisji zwykle nie są używane.

**Adres IP dla Protokołu IPv4 -** aby możliwa była komunikacja w protokole IP konieczne jest nadanie każdemu hostowi adresu IP czyli unikalnego identyfikatora, który pozwoli na wzajemne rozpoznawanie się poszczególnych uczestników komunikacji. Ma on postać 32-bitowej liczby, którą zwyczajowo zapisuje się jako cztery liczby dziesiętne (oktety) oddzielone kropkami. Np. 207.142.131.236. Użytkownicy Internetu nie muszą znać adresów IP. Nazwa www.wikipedia.org jest tłumaczona na adres IP dzięki wykorzystaniu protokołu DNS. Adres IP jest dostarczany każdemu użytkownikowi przez dostawcę internetu (ISP). Może być przydzielany statycznie lub dynamicznie. Zapotrzebowanie na adresy IP jest tak duże, że pula nieprzydzielonych adresów zaczyna się wyczerpywać.

Aby możliwa była komunikacja między wieloma sieciami połączonymi systemem routerów, konieczne jest zdefiniowanie dla każdej z nich maski sieciowej oraz adresu podsieci. Maska zapisywana jest analogicznie do adresu IP: 255.255.255.0

Maska o takiej postaci pojawi się w podsieci, dla której ostatni oktet może się zmieniać dla poszczególnych hostów. Pula adresów podzielona jest na odpowiednie zakresy, które ułatwiają konfigurację routerów i pozwalają na łatwe kierowanie ruchem w sieci. Wadą tego systemu jest bardzo rozrzutne dysponowanie pulą adresów, co doprowadziło do ich niedoboru. Protokół NAT pozwala na wykorzystanie jednego publicznego adresu IP do obsługi wielu hostów pracujących w sieci prywatnej.

Metody adresowania: http://pl.wikipedia.org/wiki/Adres_IP

**IPv6 -** IPv6 / IPNG (ang. Internet Protocol version 6 / Internet Protocol Next Generation) - najnowsza wersja protokołu IP, będąca następcą IPv4, do którego stworzenia przyczynił się w głównej mierze problem małej ilości adresów IPv4. Dodatkowymi zamierzeniami było udoskonalenie protokołu IP: eliminacja wad starszej wersji, wprowadzenie nowych rozszerzeń (uwierzytelnienie, kompresja i inne), zminimalizowanie czynności wymaganych do podłączenia nowego węzła do Internetu (autokonfiguracja).

Warto zaznaczyć, iż IPv6 to tylko jedna warstwa w modelu OSI - nie ingeruje on w inne warstwy, np. aplikacyjną, co pozwala działać istniejącym już protokołom zasadniczo "bezboleśnie".

IPv6 jest protokołem wdrażanym w infrastrukturę Internetu od 2000 roku. Niektórzy dostawcy usług internetowych (ISP) dostarczają już IPv6 "w kabelku" tak samo jak obecnie IPv4; jednak aktualnie ogromna część sieci opiera się na tunelach wykorzystujących poprzednią wersję protokołu (tzw. IPv6-in-IPv4). Najprostszą metodą zestawienia takiego tunelu jest obecnie mechanizm 6to4.

<table>
<tr><th>Bity</th><th>0-3</th><th>4-7</th><th>8-11</th><th>12-15</th><th>16-19</th><th>20-23</th><th>24-27</th><th>28-31</th></tr>
<tr><td>0</td><td>Wersja</td><td colspan="2">Priorytet</td><td colspan="5">Etykieta przepływu</td></tr>
<tr><td>32</td><td colspan="4">Długość danych</td><td colspan="2">Następny nagłówek</td><td colspan="2">Limit przeskoków</td></tr>
<tr><td>64</td><td colspan="8" rowspan="4">Adres źródłowy (128 bitów)</td></tr>
<tr><td>96</td></tr>
<tr><td>128</td></tr>
<tr><td>160</td></tr>
<tr><td>192</td><td colspan="8" rowspan="4">Adres docelowy (128 bitów)</td></tr>
<tr><td>224</td></tr>
<tr><td>256</td></tr>
<tr><td>288</td></tr>
</table>

*Budowa datagramu*

Dla podsieci będących LAN-em przydzielana jest pula adresów z maską /64 co umożliwia tworzenie unikalnych numerów IP w oparciu o (niepowtarzalne) numery sprzętowe MAC; adres taki (dla adresu MAC 11:22:33:44:55:66) będzie miał postać: 64bitowy_prefiks_sieci:1322:33FF:FE44:5566 (pierwsza część adresu MAC zwiększana jest o 2, w środku wstawiane jest FFFE). 64 bitowy prefiks sieci jest informacją rozgłaszaną przy pomocy ICMPv6 przez routery; natomiast jeżeli host nie uzyskał wspomnianego prefiksu w jego miejsce wstawiane jest fe80:: (czyli fe80:0000:0000:0000) - taki adres nazywa się "link-local" (nie jest on routowany do sieci zewnętrznych, jednak zawsze (także gdy prefiks został uzyskany) może być używany wewnątrz sieci lokalnej). Oczywiście nadal możemy korzystać z przydziału IP przez DHCP oraz ręcznego przydziału IP.

***

**ARP** (ang. Address Resolution Protocol) - protokół komunikacyjny przekształcania adresów IP (ustalanych autorytarnie przez użytkownika/administratora) na fizyczne, 48-bitowe adresy MAC (przypisane fizycznie m.in. do kart sieciowych) w komputerowych sieciach lokalnych typu Ethernet. Każdy komputer w sieci powinien posiadać tzw. tablicę ARP. Znajduje się w niej adres IP i przypisany do niego adres MAC. Dzięki temu komputery mogą się ze sobą komunikować za pośrednictwem adresu MAC, ale tylko w obrębie danej sieci LAN. Jeśli jakieś informacje mają być przesłane do innej sieci (lub podsieci w sieci złożonej, sieci oddzielonej routerem, itp.), to adres MAC musi być zastąpiony adresem IP.

ARP jest protokołem pracującym na drugiej warstwie modelu ISO/OSI, czyli warstwie łącza danych, ponieważ pracuje ona na ramkach i może je analizować tzn. np. sprawdzać ich poprawność.

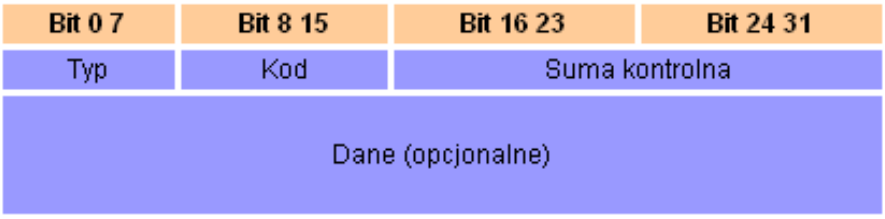
ARP działa w następujący sposób:

- Utworzenie pakietu z szukanym adresem IP.
- Wysłanie pakietu w obrębie danej sieci.
- Wysłany pakiet odbierają wszystkie hosty podłączone do sieci. Jako jedyny odpowiada host o szukanym IP - przesyła pakiet z odpowiedzią zawierającą adres MAC.

- Host szukający po odebraniu pakietu z szukanym adresem MAC zapisuje go w pamięci podręcznej, dzięki czemu nie musi później szukać jeszcze raz tego samego adresu.

***

**ICMP** (ang. Internet Control Message Protocol, internetowy protokół komunikatów kontrolnych) – protokół wykorzystywany w diagnostyce sieci oraz routingu. Najpopularniejszymi programami użytkowymi wykorzystującymi protokół ICMP są *ping* oraz *traceroute.*




*Ramka ICMP*

***

**IGMP** (ang. Internet Group Management Protocol) - jeden z rodziny protokołów TCP/IP. IGMP służy do zarządzania grupami multicastowymi w sieciach opartych na protokole IP. Komputery wykorzystują komunikaty IGMP do powiadamiania routerów w swojej sieci o chęci przyłączenia się do lub odejścia z określonej grupy multicastowej.

*(Multicast to sposób dystrybucji informacji, w którym istnieje więcej niż jeden odbiorca)*

***

**UDP** (ang. User Datagram Protocol - Datagramowy Protokół Użytkownika) to jeden z podstawowych protokołów internetowych. Umieszcza się go w warstwie czwartej (transportu) modelu OSI. Jest to protokół bezpołączeniowy, więc nie ma narzutu na nawiązywanie połączenia i śledzenie sesji (w przeciwieństwie do TCP). Nie ma też mechanizmów kontroli przepływu i retransmisji. Korzyścią płynącą z takiego uproszczenia budowy jest większa szybkość transmisji danych i brak dodatkowych zadań, którymi musi zajmować się host posługujący się tym protokołem. Z tych względów UDP jest często używany w takich zastosowaniach jak wideokonferencje, strumienie dźwięku w Internecie i gry sieciowe, gdzie dane muszą być przesyłane możliwie szybko, a poprawianiem błędów zajmują się inne warstwy modelu OSI. Innym przykładem może być protokół DNS lub VoIP.

UDP udostępnia mechanizm identyfikacji różnych punktów końcowych (np. pracujących aplikacji, usług czy serwisów) na jednym hoście dzięki portom (porównaj: socket). UDP zajmuje się dostarczaniem pojedynczych pakietów, udostępnionych przez IP, na którym się opiera. Kolejną cechą odróżniającą UDP od TCP jest możliwość transmisji do kilku adresów docelowych na raz (tzw. multicast).

Pakiety UDP (zwane też datagramami) zawierają oprócz nagłówków niższego poziomu nagłówek UDP. Składa się on z pól zawierających sumę kontrolną, długość pakietu oraz porty: źródłowy i docelowy.

Podobnie jak w TCP, porty UDP zapisywane są na dwóch bajtach (szesnastu bitach), więc każdy adres IP może mieć przypisanych 65535 różnych zakończeń. Z przyczyn

historycznych, porty 0-1023 zarezerwowane są dla dobrze znanych usług sieciowych - dla aplikacji użytkownika przydziela się porty od 1024.

| + | Bity 0 - 15 | 16 - 31 |
|---|---|---|
| 0 | Port nadawcy | Port odbiorcy |
| 32 | Długość | Suma kontrolna |
| 64 | Dane | |

*Struktura nagłówka UDP*

***

**SMTP** (ang. Simple Mail Transfer Protocol) - protokół komunikacyjny opisujący sposób przekazywania poczty elektronicznej w internecie.

SMTP to względnie prosty, tekstowy protokół, w którym określa się co najmniej jednego odbiorcę wiadomości (w większości przypadków weryfikowane jest jego istnienie), a następnie przekazuje treść wiadomości. Łatwo przetestować serwer SMTP przy użyciu programu telnet.

Protokół ten nie radził sobie dobrze z plikami binarnymi, ponieważ stworzony był w oparciu o czysty tekst ASCII. W celu kodowania plików binarnych do przesyłu przez SMTP stworzono standardy takie jak MIME. W dzisiejszych czasach większość serwerów SMTP obsługuje rozszerzenie 8BITMIME pozwalające przesyłać pliki binarne równie łatwo jak tekst.

SMTP nie pozwala na pobieranie wiadomości ze zdalnego serwera. Do tego celu służą POP3 lub IMAP.

Jednym z ograniczeń pierwotnego SMTP jest brak mechanizmu weryfikacji nadawcy, co ułatwia rozpowszechnianie niepożądanych treści poprzez pocztę elektroniczną (wirusy, spam). Żeby temu zaradzić stworzono rozszerzenie SMTP-AUTH, które jednak jest tylko częściowym rozwiązaniem problemu - ogranicza wykorzystanie serwera wymagającego autoryzacji do zwielokratniania poczty. Nadal nie istnieje metoda, dzięki której odbiorca autoryzowałby nadawcę - nadawca może "udawać" serwer i wysłać dowolny komunikat do dowolnego odbiorcy.

***

**POP3** (Post Office Protocol version 3) to protokół internetowy z warstwy aplikacji pozwalający na odbiór poczty elektronicznej ze zdalnego serwera do lokalnego komputera poprzez połączenie TCP/IP.
Protokół POP3 powstał dla użytkowników, którzy nie są cały czas obecni w Internecie. Jeżeli ktoś łączy się z siecią tylko na chwilę, to poczta nie może dotrzeć do niego protokołem SMTP. W takiej sytuacji w sieci istnieje specjalny serwer, który przez SMTP odbiera przychodzącą pocztę i ustawia ją w kolejce.

Kiedy użytkownik połączy się z siecią, to korzystając z POP3 może pobrać czekające na niego listy do lokalnego komputera. Jednak protokół ten ma wiele ograniczeń:

- połączenie trwa tylko, jeżeli użytkownik pobiera pocztę i nie może pozostać uśpione,
- do jednej skrzynki może podłączyć się tylko jeden klient równocześnie,

- każdy list musi być pobierany razem z załącznikami i żadnej jego części nie można w łatwy sposób pominąć - istnieje co prawda komenda top, ale pozwala ona jedynie określić przesyłaną liczbę linii od początku wiadomości,
- wszystkie odbierane listy trafiają do jednej skrzynki, nie da się utworzyć ich kilku,
- serwer POP3 nie potrafi sam przeszukiwać czekających w kolejce listów.

Istnieje bardziej zaawansowany protokół IMAP, który pozwala na przeglądanie czekających listów nie po kolei na podobieństwo plików w katalogach i posiada niektóre funkcje pominięte w POP3.

Protokół POP3, podobnie, jak inne protokoły internetowe (np. SMTP, HTTP) jest protokołem tekstowym, czyli w odróżnieniu od protokołu binarnego, czytelnym dla człowieka. Komunikacja między klientem pocztowym, a serwerem odbywa się za pomocą czteroliterowych poleceń.

***

**HTTP** (ang. Hypertext Transfer Protocol) to protokół sieci WWW (World Wide Web). Obecną definicję HTTP stanowi RFC 2616. Właśnie za pomocą protokołu HTTP przesyła się żądania udostępnienia dokumentów WWW i informacje o kliknięciu odnośnika oraz informacje z formularzy. Zadaniem stron WWW jest publikowanie informacji - natomiast protokół HTTP właśnie to umożliwia.

Protokół HTTP jest tak użyteczny, ponieważ udostępnia znormalizowany sposób komunikowania się komputerów ze sobą. Określa on formę żądań klienta dotyczących danych oraz formę odpowiedzi serwera na te żądania. Jest zaliczany do protokołów ***stateless*** (bezstanowy), z racji tego, że nie zachowuje żadnych informacji o poprzednich transakcjach z klientem, po zakończeniu transakcji wszystko "przepada" - z tego powodu tak bardzo spopularyzowały się *cookies*.

HTTP korzysta z portu nr 80.

Metody HTTP:

- GET - pobranie zasobu wskazanego przez URI, może mieć postać warunkową jeśli w nagłówku występują pola warunkowe takie jak "If-Modified-Since"
- HEAD - pobiera informacje o zasobie, stosowane do sprawdzania dostępności zasobu
- PUT - przyjęcie danych przesyłanych od klienta do serwera
- POST - przyjęcie danych przesyłanych od klienta do serwera (np. wysyłanie zawartości formularzy)
- DELETE - żądanie usunięcia zasobu, włączone dla uprawnionych użytkowników
- OPTIONS - informacje o opcjach i wymaganiach istniejących w kanale komunikacyjnym
- TRACE - diagnostyka, analiza kanału komunikacyjnego
- CONNECT - żądanie przeznaczone dla serwerów proxy pełniących funkcje tunelowania

***

**SMB (**Server Message Block) to protokół służący udostępnianiu zasobów komputerowych, m.in. drukarek czy plików.
SMB jest protokołem typu klient-serwer, a więc opiera się na systemie zapytań generowanych przez klienta i odpowiedzi od serwera. Wyjątkiem od tej zasady jest mechanizm tzw. *oplocków* (*opportunistic lock*), w którym to serwer może wygenerować "nieproszony" przez klienta sygnał informujący o zerwaniu wcześniej założonego *oplocka* (blokady).

Niemniej jednak, chociaż sam protokół ma charakter klient-serwer, to z racji tego, że najczęściej maszyny klienckie dysponują także funkcjami serwerowymi (udostępnianie plików) to sieci SMB nabierają charakteru sieci peer-to-peer.

Identyfikacja komputerów w sieciach SMB odbywa się za pomocą ich nazw NetBIOS (nazwą jest ciąg znaków, nie dłuższy niż 15 znaków) lub za pomocą mechanizmów protokołów "podległych" SMB, np. poprzez adres IP czy nazw DNS, gdy SMB wykorzystuje protokół TCP do transportu danych.

**CIFS** (Common Internet File System) to nowa wersja protokołu SMB opracowywana przez Microsoft i kilka innych firm. Szkic protokołu został przesłany do IETF, jednak z powodu wielu niedoskonałości nie został zatwierdzony. CIFS został zaimplementowany m.in. w Windows 2000/XP/2003 oraz Samba 3.0.

***

**Tablica routingu** - w protokołach routingu sieci komputerowych spis wskazujący, przez które sąsiadujące z routerem węzły sieci prowadzi trasa do węzłów oddalonych. Tablica routingu jest utrzymywana niezależnie przez każdy router.

W sieciach rozległych dane przesyłane są z jednego węzła do konkretnego drugiego, a nie do wszystkich. Po drodze napotykają na wiele węzłów pośredniczących, mogą też być transmitowane wieloma różnymi trasami. Router jest jednym z tych węzłów, który ma za zadanie przesłać dane najlepszą (najszybszą) trasą.

Do kierowania danych routery używają tablic routingu, zawierającą informacje o sąsiadujących routerach i sieciach lokalnych. Służy ona do wyszukania optymalnej drogi od obecnego położenia pakietu do innego miejsca w sieci. Tablica routingu może być statyczna lub dynamiczna, zależy to od postawionych wymagań. Statyczna tablica routingu musi być aktualizowana ręcznie przez administratora sieci, dynamiczna natomiast jest aktualizowana automatycznie przez oprogramowanie sieciowe.

**Routowanie** polega na wyszukiwaniu w tablicy odpowiedniej informacji dot. miejsca docelowego pakietu, tzn. trasy jaką ma przebyć dany pakiet, aby dotrzeć do celu. Każdy wpis trasy musi zawierać dwie informacje:

- adres docelowy – to jest adres sieci, z jaką router jest bezpośrednio połączony; czasem może się zdarzyć, ze urządzenie zna kilka tras dojścia do danej sieci (w takim przypadku wyboru tej najwłaściwszej dokonuje się za pomocą metryk, ale to już temat dotyczący protokołów routingu);
- wskaźnik do celu – informacja, czy router jest bezpośrednio podłączony do sieci docelowej, lub adres innego routera bezpośrednio połączonego z szukaną siecią (tzw. "next-hop router");

Istnieją dwa sposoby dobierania trasy: klasowy (protokół RIP) oraz bezklasowy (protokoły: RIPv2, RIPng, Classless Routing).

Protokoły routingu dynamicznego: **RIP, IGRP, EIGRP, OSPF, BGP, IS-IS**

***

**DNS** - (ang. Domain Name System, system nazw domenowych) to system serwerów oraz protokół komunikacyjny zapewniający zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową. Dzięki wykorzystaniu DNS

nazwa mnemoniczna, np. pl.wikipedia.org, może zostać zamieniona na odpowiadający jej adres IP, czyli 145.97.39.135.

Adresy DNS składają się z domen internetowych rozdzielonych kropkami. Dla przykładu w adresie Wikipedii org oznacza domenę funkcjonalną organizacji, wikipedia domenę należącą do fundacji Wikimedia, a pl polską domenę w sieci tej instytucji. W ten sposób możliwe jest budowanie hierarchii nazw, które porządkują Internet.

DNS to złożony system komputerowy oraz prawny. Zapewnia z jednej strony rejestrację nazw domen internetowych i ich powiązanie z numerami IP. Z drugiej strony realizuje bieżącą obsługę komputerów odnajdujących adresy IP odpowiadające poszczególnym nazwom.

***

**IPTables** jest filtrem pakietów (głównie używanym jako firewall bądź router) dla systemu operacyjnego GNU/Linux. Został napisany w 1999 roku przez Rusty'ego Russella w języku C i jest to program, będący zarówno filtrem pakietów jak i tzw. firewallem stanowym dla systemów z jądrem począwszy od serii 2.4.x, kontrolujący linki wchodzące i wychodzące do sieci komputerowej lub stacji roboczej.

Firewall, uruchamiany najczęściej na hostach pełniących rolę routerów. Działanie opiera się na trzech podstawowych regułach opisujących działania mające zostać podjęte w odpowiednich sytuacjach. Reguła INPUT opisuje działania dla pakietów przychodzących, reguła OUTPUT dla wychodzących i FORWARD dla pakietów przechodzących pomiędzy kilkoma interfejsami. Możliwe do wykonania działania to ACCEPT (zaakceptowanie pakietu), DROP (usunięcie) i REJECT (odrzucenie z powiadomieniem nadawcy). Reguły iptables pozwalają na dokładniejsze określenie rodzaju i przeznaczenia pakietu, z uwagi na np. port lub host zródłowy/docelowy, wykorzystany protokół, czas życia.

Przykład użycia: http://pl.wikipedia.org/wiki/Iptables

***

**NAT** (ang. Network Address Translation, także maskarada (ang. masquerading)) - technika translacji adresów sieciowych.

Wraz ze wzrostem ilości komputerów w Internecie, zaczęła zbliżać się groźba wyczerpania puli dostępnych adresów internetowych IPv4. Aby temu zaradzić, lokalne sieci komputerowe, korzystające z tzw. adresów prywatnych (specjalna pula adresów tylko dla sieci lokalnych), mogą zostać podłączone do Internetu przez jeden komputer (lub router), posiadający mniej adresów internetowych niż komputerów w tej sieci.

Router ten, gdy komputery z sieci lokalnej komunikują się ze światem, dynamicznie tłumaczy adresy prywatne na adresy zewnętrzne, umożliwiając użytkowanie Internetu przez większą liczbę komputerów niż posiadana liczba adresów zewnętrznych.

Z korzystaniem z Internetu poprzez NAT wiążą się wady:

- nie można na własnym komputerze uruchomić serwera dostępnego w Internecie bez zmian wymagających interwencji administratora;
- utrudnione korzystanie z programów P2P i bezpośredniego wysyłania plików.

Zaletą takiego systemu jest większe bezpieczeństwo komputerów znajdujących się za NAT-em.

NAT jest często stosowany w sieciach korporacyjnych (w połączeniu z proxy) oraz sieciach osiedlowych. Można wyróżnić 2 podstawowe typy NAT:
**SNAT** (Source Network Address Translation) to technika polegająca na zmianie adresu źródłowego pakietu IP na jakiś inny. Stosowana często w przypadku podłączenia sieci dysponującej adresami prywatnymi do sieci Internet. Wtedy router, przez który podłączono sieć, podmienia adres źródłowy prywatny na adres publiczny (najczęściej swój własny).
**DNAT** (Destination Network Address Translation) to technika polegająca na zmianie adresu docelowego pakietu IP na jakiś inny. Stosowana często w przypadku, gdy serwer, który ma być dostępny z Internetu ma tylko adres prywatny. W tym przypadku router dokonuje translacji adresu docelowego pakietów IP z Internetu na adres tego serwera.

Szczególnym przypadkiem SNAT jest sytuacja, gdy router ma zmienny adres IP (np. otrzymuje go w przypadku połączenia modemowego dodzwanianego). Wtedy router zmienia adres źródłowy na taki, jak adres interfejsu, przez który pakiet opuszcza router.

W przypadku systemu operacyjnego Linux funkcje NAT definiowane są za pomocą programów iptables lub ipchains, a w przypadku FreeBSD ipfw (IP firewall), ipf (IP filter) lub pf (OpenBSD Packet Filter)

***

**ifconfig** - polecenie konfigurujące interfejsy sieciowe w systemach Unix i Linux (ifconfig eth0, ifconfig –a)

**ipconfig -** wyświetla wszystkie bieżące wartości konfiguracji sieci protokołu TCP/IP oraz odświeża ustawienia protokołu dynamicznej konfiguracji hosta (DHCP, Dynamic Host Configuration Protocol) i systemu DNS (Domain Name System). Polecenie ipconfig użyte bez parametrów powoduje wyświetlenie adresów IPv6 lub adresu IPv4, maski podsieci i bramy domyślnej dla wszystkich kart.

Składnia:

ipconfig [/all] [/renew[karta]] [/release [karta]] [/flushdns] [/displaydns] [/registerdns] [/showclassidkarta] [/setclassidkarta [identyfikator_klasy]]

**ping -** weryfikuje łączność na poziomie protokołu IP z innym komputerem obsługującym protokół TCP/IP, wysyłając komunikaty żądania echa protokołu ICMP (Internet Control Message Protocol). Potwierdzenia odpowiednich komunikatów odpowiedzi echa są wyświetlane razem z czasami opóźnienia. Polecenie ping to podstawowe polecenie protokołu TCP/IP używane do rozwiązywania problemów z łącznością, dostępnością i rozpoznawaniem nazw. Polecenie ping użyte bez parametrów powoduje wyświetlenie Pomocy.

Składnia:

ping[-t ] [-a ] [-n liczba] [-l rozmiar] [-f ] [-i TTL] [-v TOS] [-r liczba] [-s liczba] [{-j lista_hostów | -k lista_hostów}] [-w limit_czasu] [-R ] [-S adres_źródłowy] [-4] [-6] nazwa_obiektu_docelowego

**tracert - u**stala ścieżkę do lokalizacji docelowej przez wysłanie komunikatów protokołu ICMP (Internet Control Message Protocol) typu Echo Request lub komunikatów ICMPv6 do lokalizacji docelowej, stopniowo zwiększając wartości pola czasu wygaśnięcia (TTL, Time to Live). Wyświetlana ścieżka jest listą bliskich interfejsów routerów znajdujących się na ścieżce między hostem źródłowym a lokalizacją docelową. Interfejs bliski jest interfejsem routera znajdującym się na ścieżce najbliżej hosta wysyłającego komunikat. Polecenie tracert bez parametrów powoduje wyświetlenie Pomocy.

Składnia:

tracert [-d ] [-h maksymalna_liczba_przeskoków] [-j lista_hostów] [-w limit_czasu] [-R ] [-S adres_źródłowy] [-4][-6] nazwa_obiektu_docelowego

**hostname -** wyświetla część nazwy hosta pełnej nazwy komputera.

**route** - wyświetla i modyfikuje wpisy w lokalnej tabeli routingu protokołu IP. Polecenie route użyte bez parametrów powoduje wyświetlenie Pomocy.

Składnia:

route [-f ] [-p ] [polecenie [lokalizacja_docelowa] [mask maska_sieci] [brama] [metric metryka]] [if interfejs]]

**nslookup** - yyświetla informacje, które można wykorzystywać do diagnozowania infrastruktury systemu DNS (Domain Name System). Przed użyciem tego narzędzia należy zapoznać się z zasadami działania systemu DNS. Narzędzie Nslookup jest dostępne w wierszu polecenia tylko wtedy, gdy zainstalowano protokół TCP/IP.

Składnia:

nslookup [-podpolecenie...] [{poszukiwany_komputer | -serwer}]
**traceroute** - program służący do badania trasy w sieci IP pomiędzy hostami, wywodzący się z Uniksa. Brak odpowiedzi na zadany pakiet sygnalizowany jest znakiem gwiazdki "*" i może wynikać z przeciążenia sieci, routera bądź z celowej konfiguracji urządzeń (ustawienia firewalla).

**net** - net accounts, net computer, net config, net continue, net file, net group, net help, net helpmsg, net localgroup, net name, net pause, net print, net send, net session, net share, net start, net statistics, net stop, net time, net use, net user, net view

**host** - konwersjia nazw DNS na adresy IP i vice-versa (UNIX / Linux)

**dig -** porównywanie czasów wykonania dwóch zapytań DNS (?)

Składnia:

dig <nazwa_komputera>