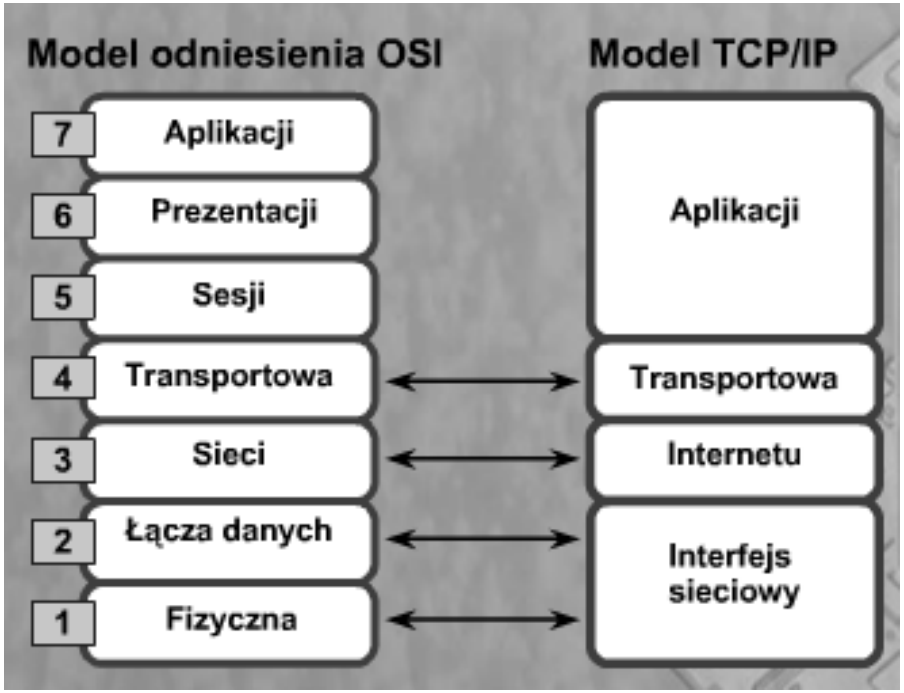
PODSTAWY SIECI KOMPUTEROWYCH

Modele warstwowe

- Model OSI - warstwa aplikacji.

Funkcje warstwy

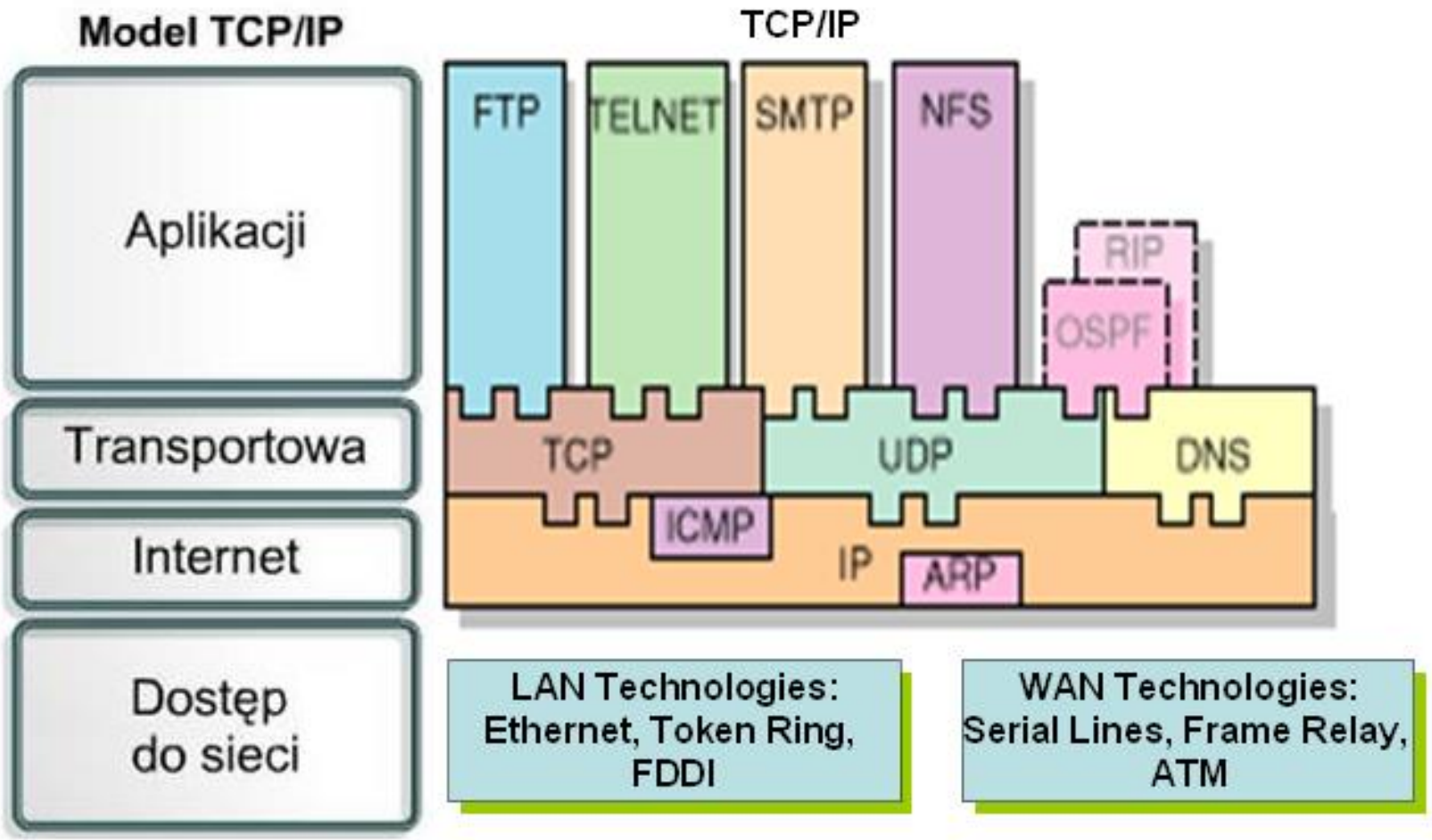
- Aplikacji (programów użytkowych) – klient pocztowy, przeglądarka WWW ... korzystają z usług protokołów warstwy transportowej.



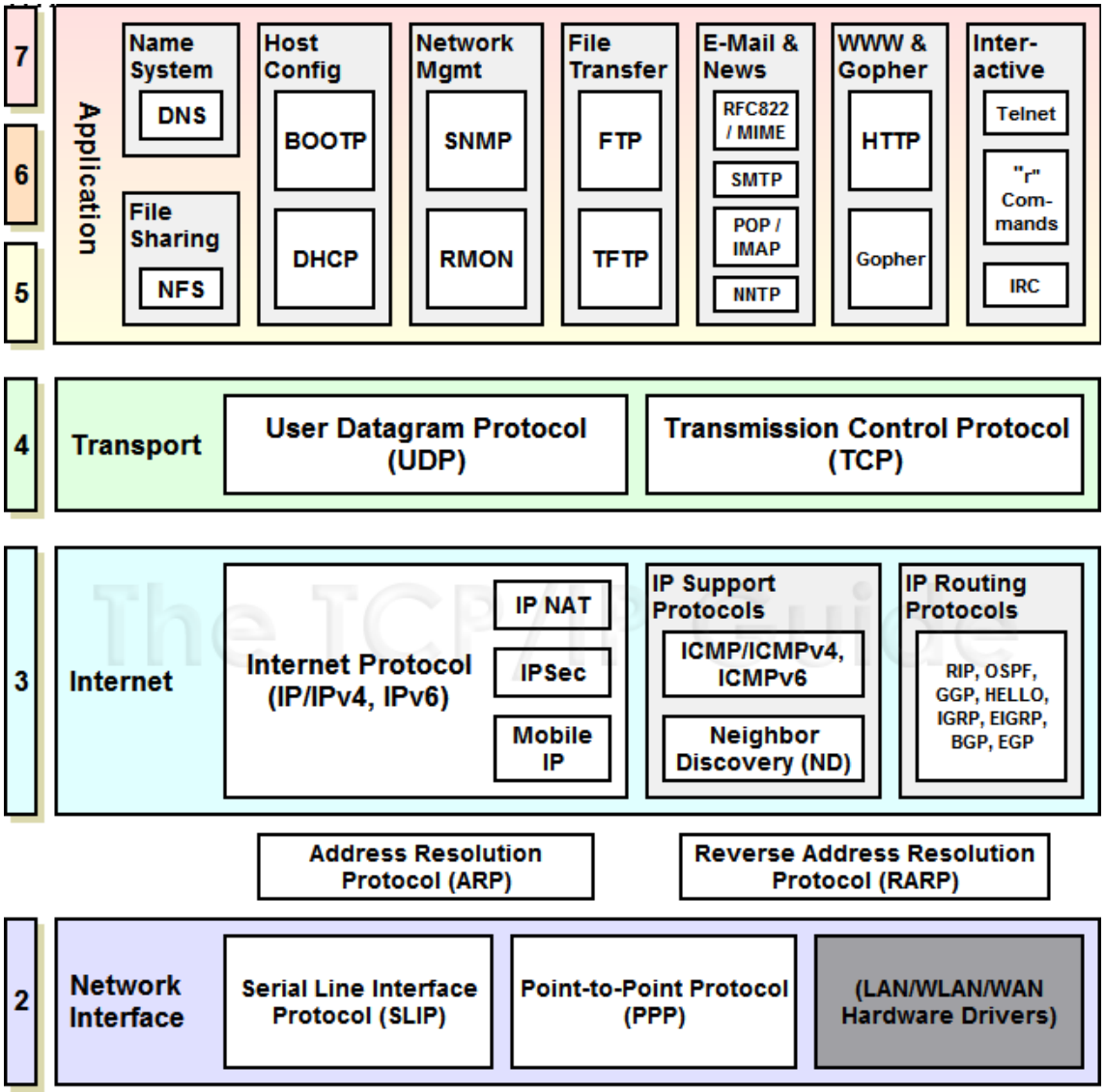
Pakiet protokołów TCP/IP

- najbardziej rozpowszechniony pakiet protokołów sieciowych,
- stanowi podstawę współczesnego Internetu,
- jest standardem otwartym - istnieje możliwość komunikacji między dowolnymi typami urządzeń,
- umożliwia dodawanie nowych sieci bez przerywania pracy istniejących,
- posiada wysoki współczynnik korekcji błędów,
- dobra odtwarzalność protokołu,
- duża wydajność.

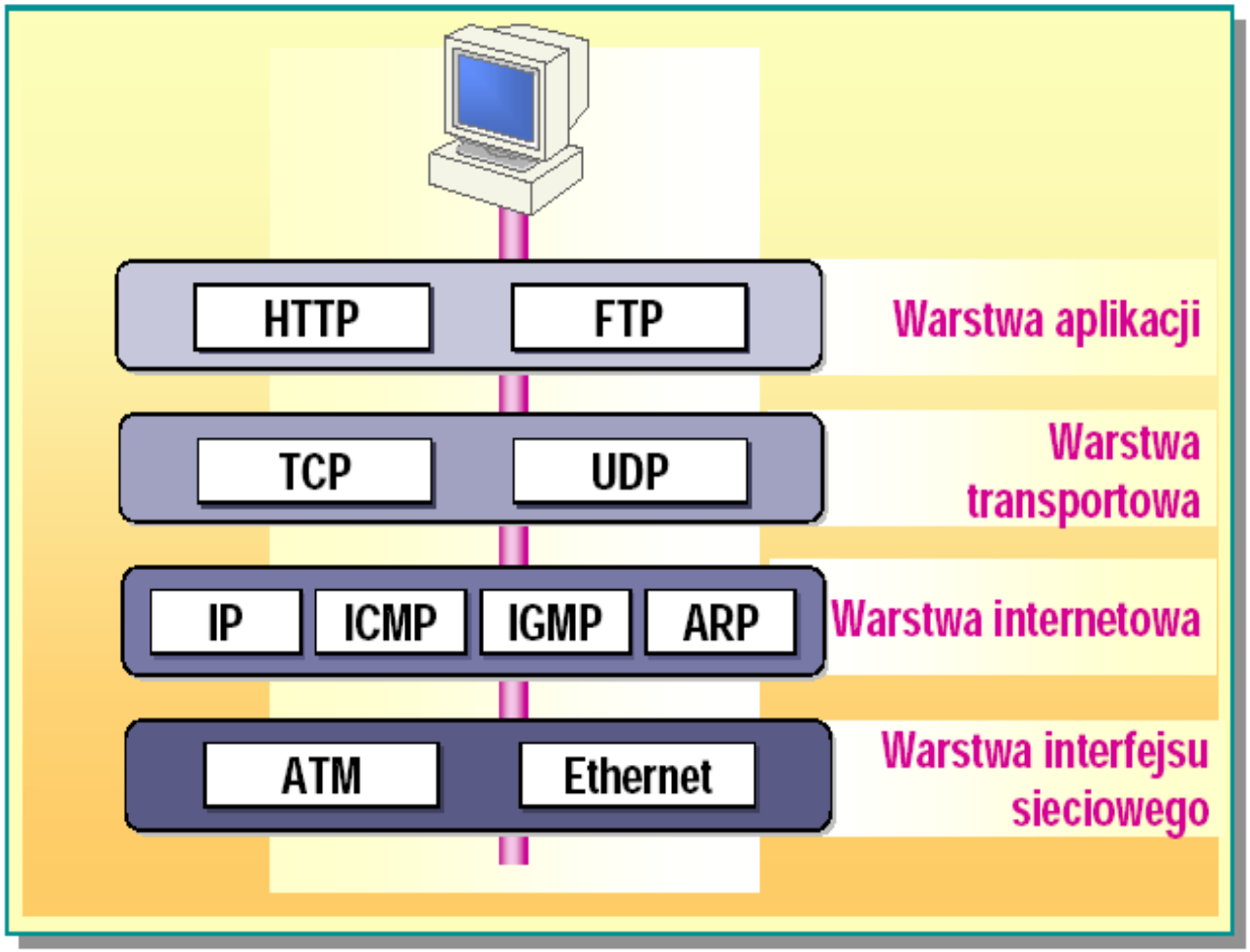
TCP/IP / stos protokołów TCP/IP / protokoły dostępu



Stos protokołów TCP/IP / protokoły dostępu



Warstwy TCP/IP



Warstwa aplikacji

- Jest to najbardziej ogólny poziom obsługi sieci, zapewniający interfejs pomiędzy aplikacjami użytkowymi, a usługami sieciowymi. Działania w warstwie są widoczne dla użytkownika, ponieważ działają standardowe aplikacje TCP/IP, np.: telnet, HTTP, FTP, POP3, SMTP.

  To warstwa aplikacji jest bezpośrednio wykorzystywana przez oprogramowanie użytkowe - przeglądarki WWW, programy pocztowe, instant messengers, chat itd.

Protokoły warstw wyższych:

- DHCP - Dynamic Host Configuration Protocol
- SLIP - Serial Line Interface Protocol
- PPP - Point-to-Point Protocol
- SNMP - Simple Network Management Protocol
- FTP, Telnet, SMTP, WWW

Protokół DHCP

- Protokół DHCP (Dynamic Host Configuration Protocol) zdefiniowany w RFC 2131 umożliwia automatyczną konfigurację adresów IP oraz innych parametrów klientów (np. brama, maska) przy użyciu jednego lub kilku serwerów DHCP
- DHCP wykorzystuje protokół IP
- Serwer DHCP przechowuje bazę danych o dostępnych adresach IP
- Podobne funkcje do DHCP pełnią również starsze protokoły RARP (Reverse Address Resolution Protocol) oraz BOOTP

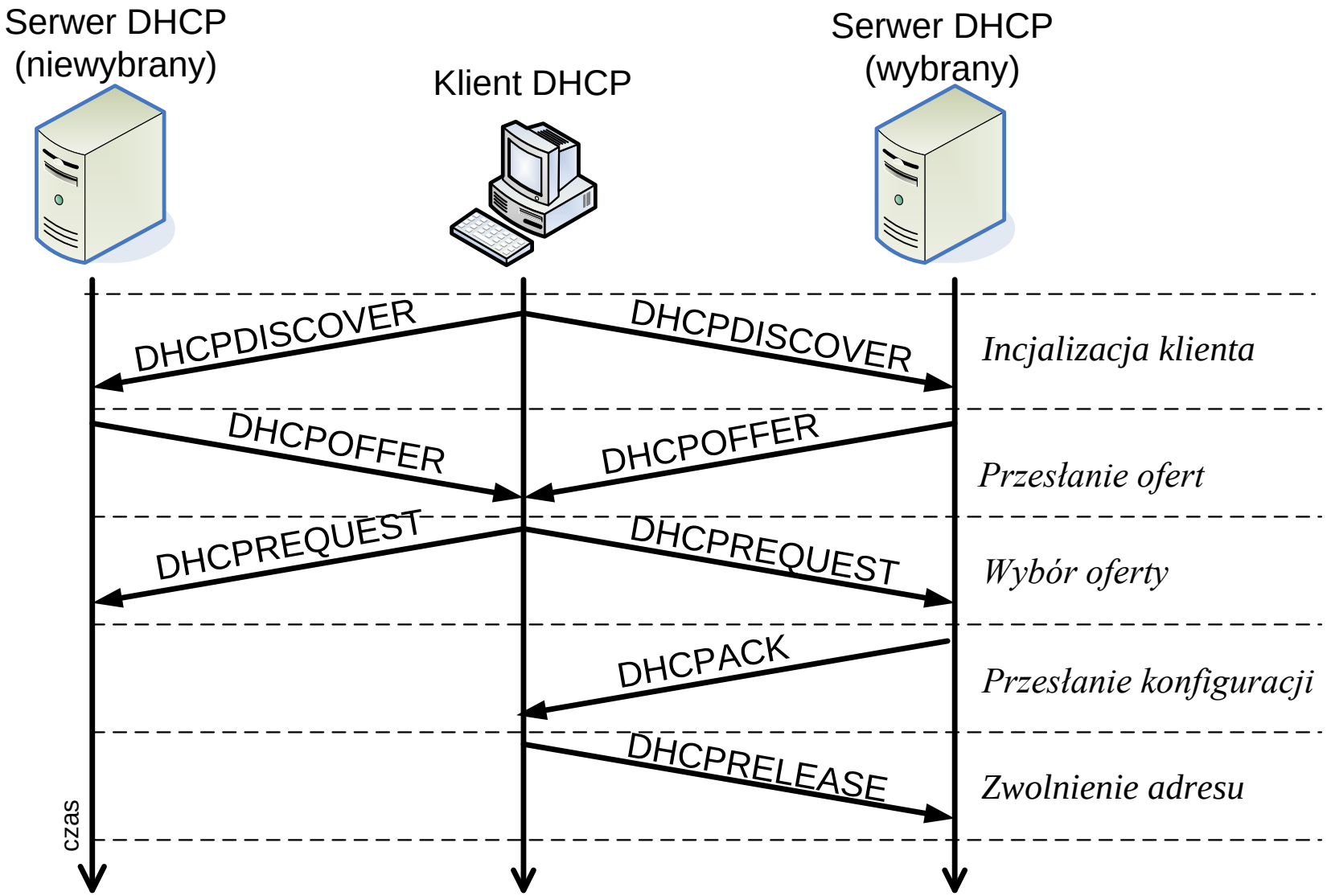
Komunikaty DHCP

- DHCPDISCOVER – klient wysyła rozgłoszeniowy komunikat w celu znalezienia serwera DHCP
- DHCPOFFER – serwer wysyła odpowiedź (unicast) zawierającą propozycję parametrów konfiguracyjnych
- DHCPREQUEST – klient wysyła wiadomość rozgłoszeniową do serwerów DHCP w celu (a) pobrania parametrów z jednego z serwerów i odrzucenia oferty innych serwerów, (b) potwierdzenia poprzednio pobranego adresu lub (c) rozszerzając dzierżawę konkretnego adresu

Komunikaty DHCP

- DHCPACK – serwer wysyła do klienta odpowiedź z parametrami zawierającymi adres IP
- DHCPNAK – serwer wysyła do klienta informację o błędzie w adresie
- DHCPDECLINE – klient do serwera, że adres jest już w użyciu
- DHCPRELEASE – klient kończy dzierżawę adresu
- DHCPINFORM – klient prosi serwer DHCP o lokalną konfigurację

Przesyłanie komunikatów DHCP



Podsumowanie DHCP

- Serwer DHCP może przyznawać adresy IP według adresu MAC klienta – ważne dla stacji wymagającego stałego IP np. ze względu na rejestrację w DNS
- Klient może pominąć komunikat DHCPDISCOVER jeśli zna adres serwera DHCP
- Czas dzierżawy adresu jest ustalany między klientem i serwerem, który zobowiązuje się nie udostępniać przydzielonego adresu nikomu na wyznaczony czas
- Klient może prosić serwer o wydłużenie czasu dzierżawy

Simple Mail Transfer Protocol (SMTP)

SMTP to tekstowy protokół, w którym określa się co najmniej jednego odbiorcę wiadomości (w większości przypadków weryfikowane jest jego istnienie), a następnie przekazuje treść wiadomości.

SMTP zaczęło być szeroko używane we wczesnych latach osiemdziesiątych dwudziestego wieku.

Początkowo 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.
Większość serwerów SMTP obsługuje rozszerzenie 8BITMIME pozwalające przesyłać pliki binarne równie łatwo jak tekst.

Simple Mail Transfer Protocol (SMTP)

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).

Rozszerzenie SMTP-AUTH, jest częściowym rozwiązaniem problemu - ogranicza wykorzystanie serwera wymagającego autoryzacji do zwielokrotniania poczty.

Nie istnieje metoda, dzięki której odbiorca autoryzowałby nadawcę - nadawca może "udawać" serwer i wysłać dowolny komunikat do dowolnego odbiorcy.

Domain Name System (DNS)

System serwerów oraz protokół komunikacyjny zapewniający zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową.

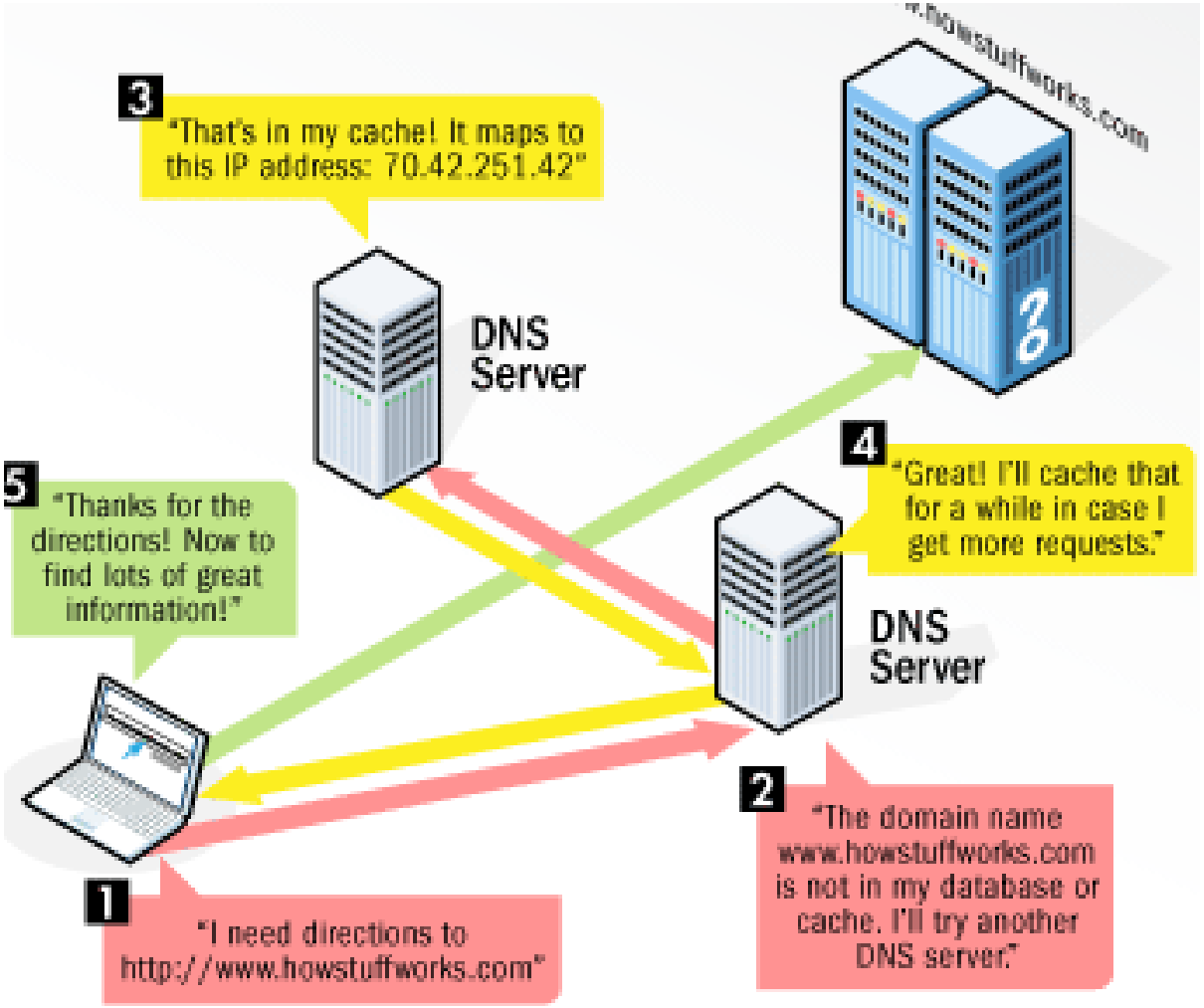
Dzięki wykorzystaniu DNS nazwa mnemoniczna, np. www.zsl.gda.pl jest zamieniona na odpowiadający jej adres IP, czyli 153.19.157.1.

Adresy DNS składają się z domen internetowych rozdzielonych kropkami. Dla przykładu w adresie zsl.gda.pl oznacza domenę funkcjonalną organizacji, zsl domenę należącą do ZSŁ, gda oznacza lokalizację, a pl polską domenę w sieci.
W ten sposób możliwe jest budowanie hierarchii nazw, które porządkują Internet.

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

Podstawy protokołu DNS zostały opisane w 1982 roku w dokumencie IETF - RFC 819

Domain Name System (DNS)



Hypertext Transfer Protocol (HTTP)

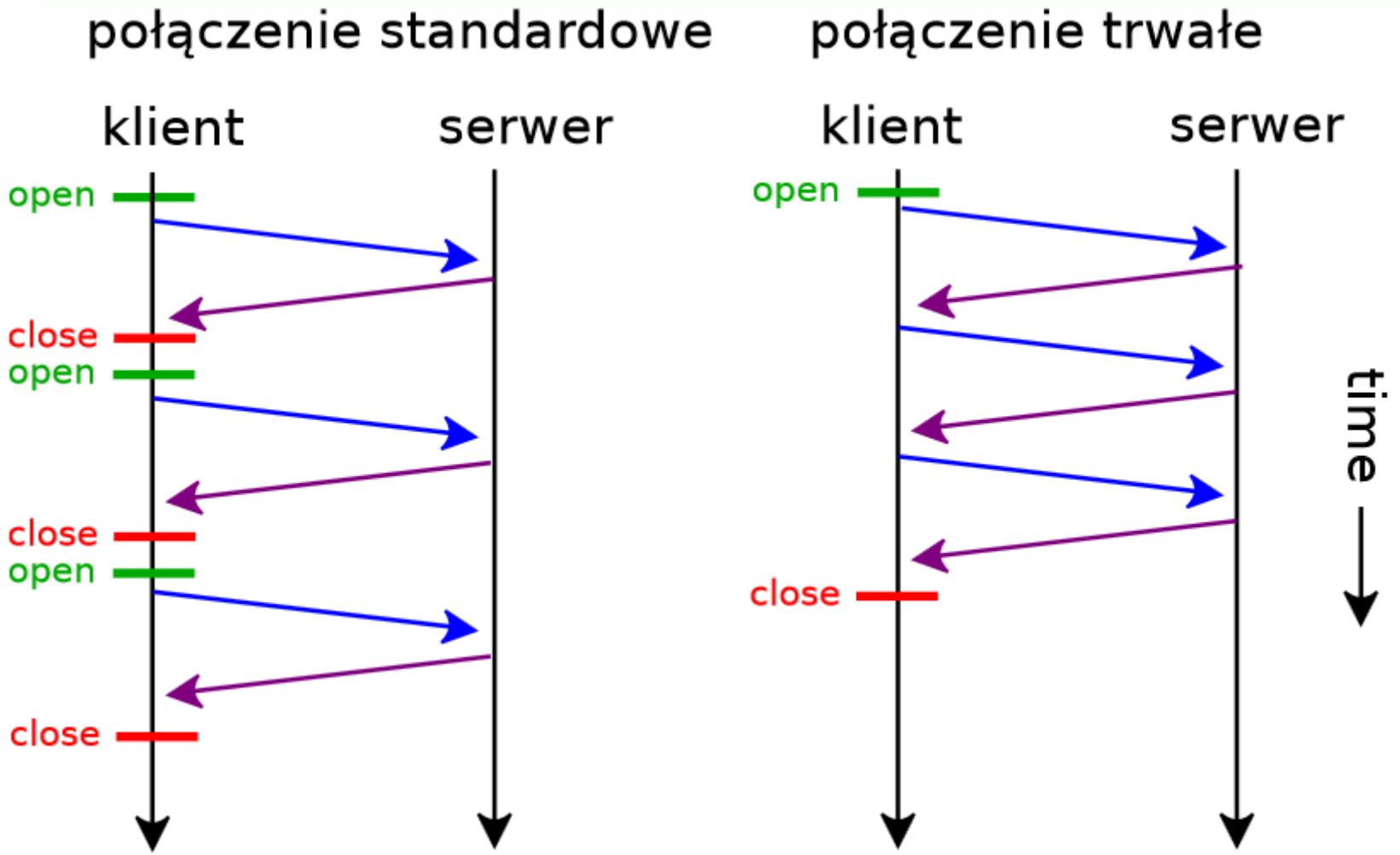
Protokół sieci WWW (World Wide Web). Definicję HTTP stanowi RFC 2616. Za pomocą protokołu HTTP przesyła się żądania udostępnienia dokumentów WWW i informacje o kliknięciu odnośnika oraz informacje z formularzy.

Zadaniem stron WWW jest publikowanie informacji - protokół HTTP to umożliwia.

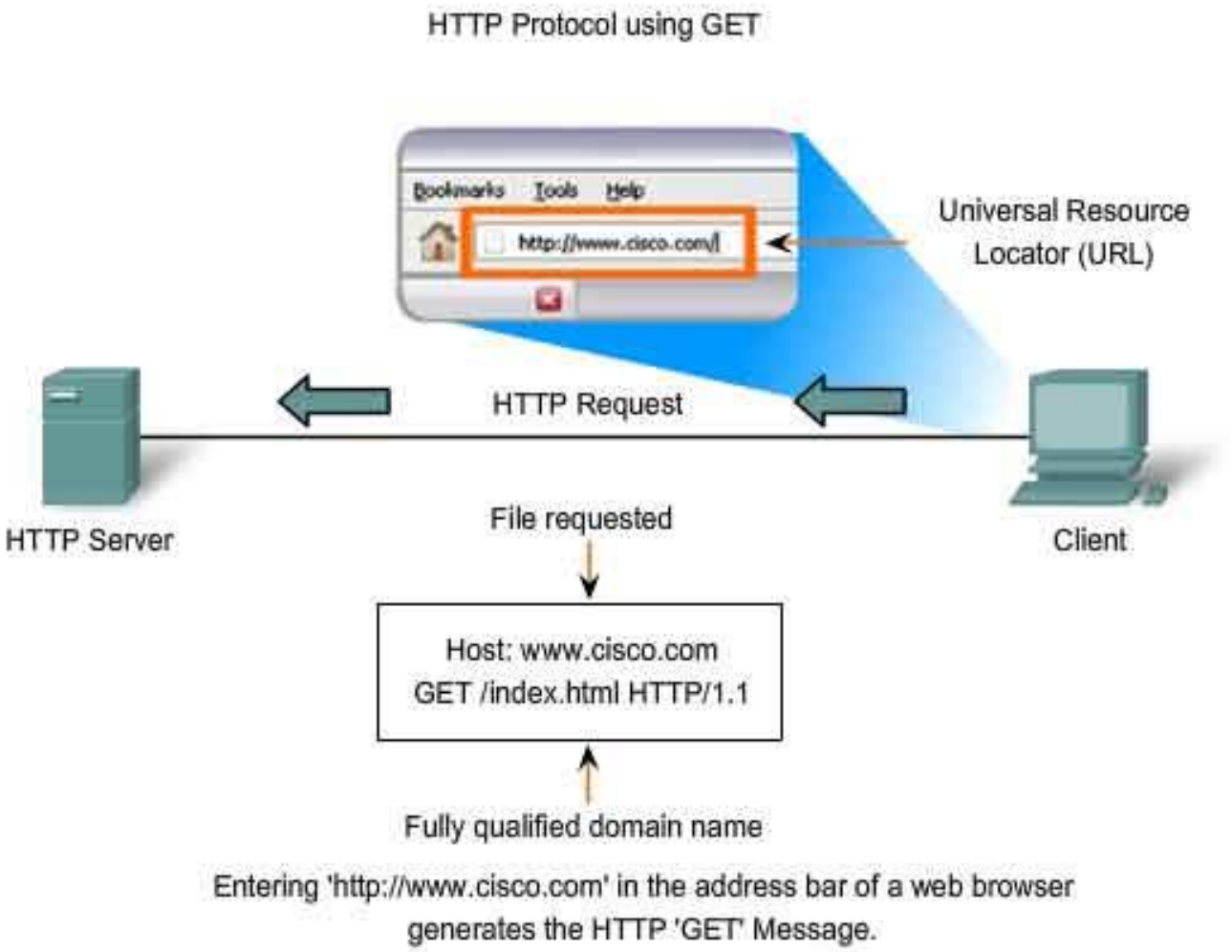
Protokół HTTP udostępnia znormalizowany sposób komunikowania się komputerów ze sobą. Określa on formę żądań klienta dotyczących danych oraz formę odpowiedzi serwera na te żądania. Jest zaliczany do protokołów stateless (bezstanowy), nie zachowuje żadnych informacji o poprzednich transakcjach z klientem,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

HTTP korzysta z portu nr 80.

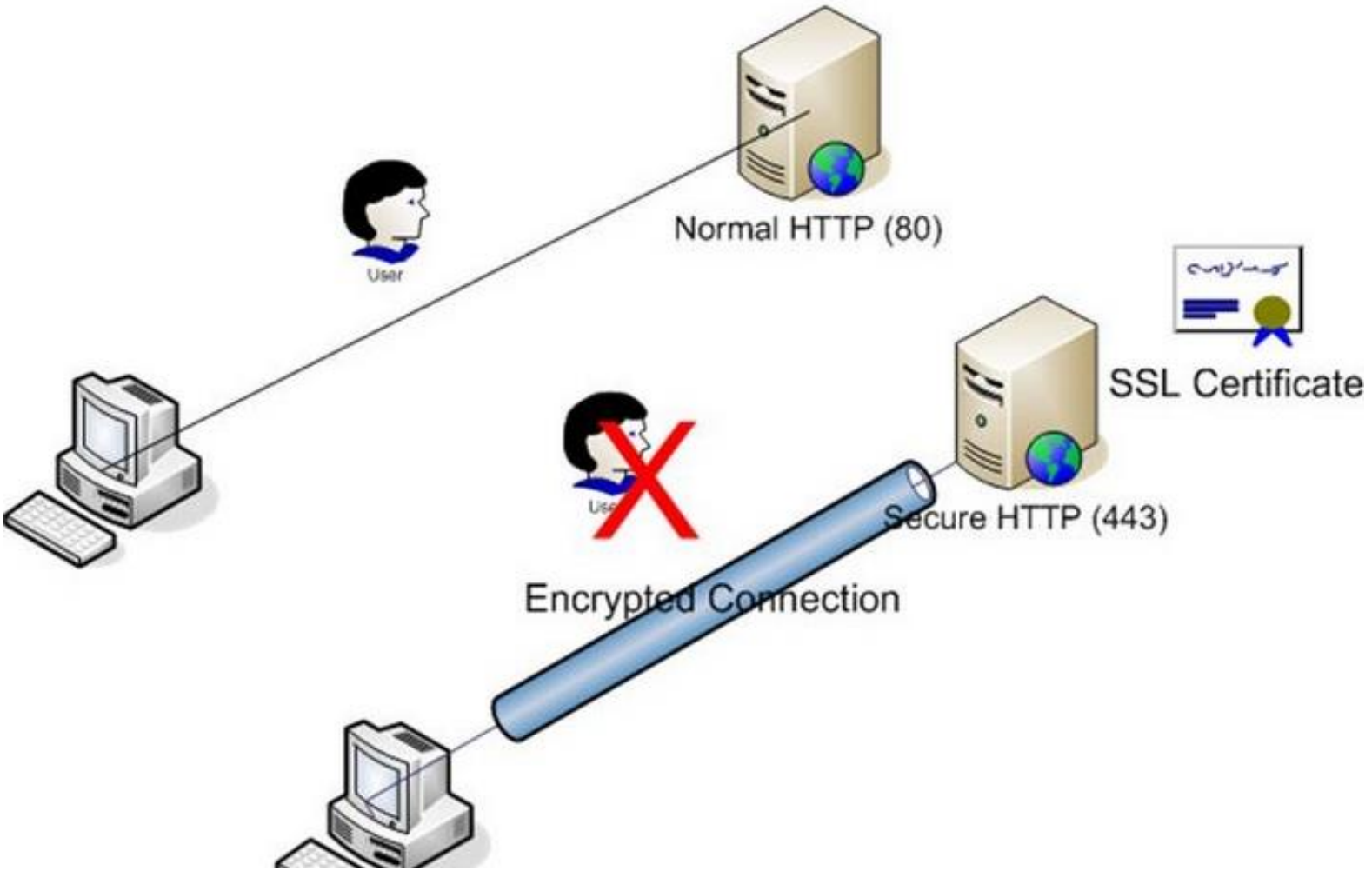
Hypertext Transfer Protocol (HTTP)



Hypertext Transfer Protocol (HTTP)



HTTP v HTTPS


Normal HTTP (80)
User
SSL Certificate
Secure HTTP (443)
Encrypted Connection

TELNET (przestarzały, niebezpieczny)

Telnet jest usługą (programem) pozwalającą na zdalne połączenie się komputera (terminala) z oddalonym od niego komputerem (serwerem) przy użyciu sieci, wykorzystując do tego celu protokół TCP-IP oraz standardowo przypisany port 23.

Umożliwia ustanowienie użytkownikowi zdalnej sesji na serwerze tak jak gdyby siedział tuż przed nim.

Protokół obsługuje tylko terminalne alfanumeryczne, nie obsługuje myszy ani innych urządzeń wskazujących.

Nie obsługuje także graficznych interfejsów użytkownika.

Wszystkie polecenia muszą być wprowadzane w trybie znakowym w wierszu poleceń.

TELNET (przestarzały, niebezpieczny)

Polecenia wydawane za pomocą naszego komputera przysłane są poprzez sieć serwera, na którym zainstalowane jest oprogramowanie serwera telnetu.

W odpowiedzi serwer odsyła nam komunikaty, które następnie wyświetlane są na naszym ekranie.

Bardzo często usługa telnet implementowana jest do urządzeń aktywnych sieci (switche, routery) w celu ułatwienia konfiguracji tychże urządzeń.

Telnet jest najstarszą i najbardziej elementarną usługą internetową. Został opisany w dokumentach RFC numer RFC 854 i RFC 855.

SSH

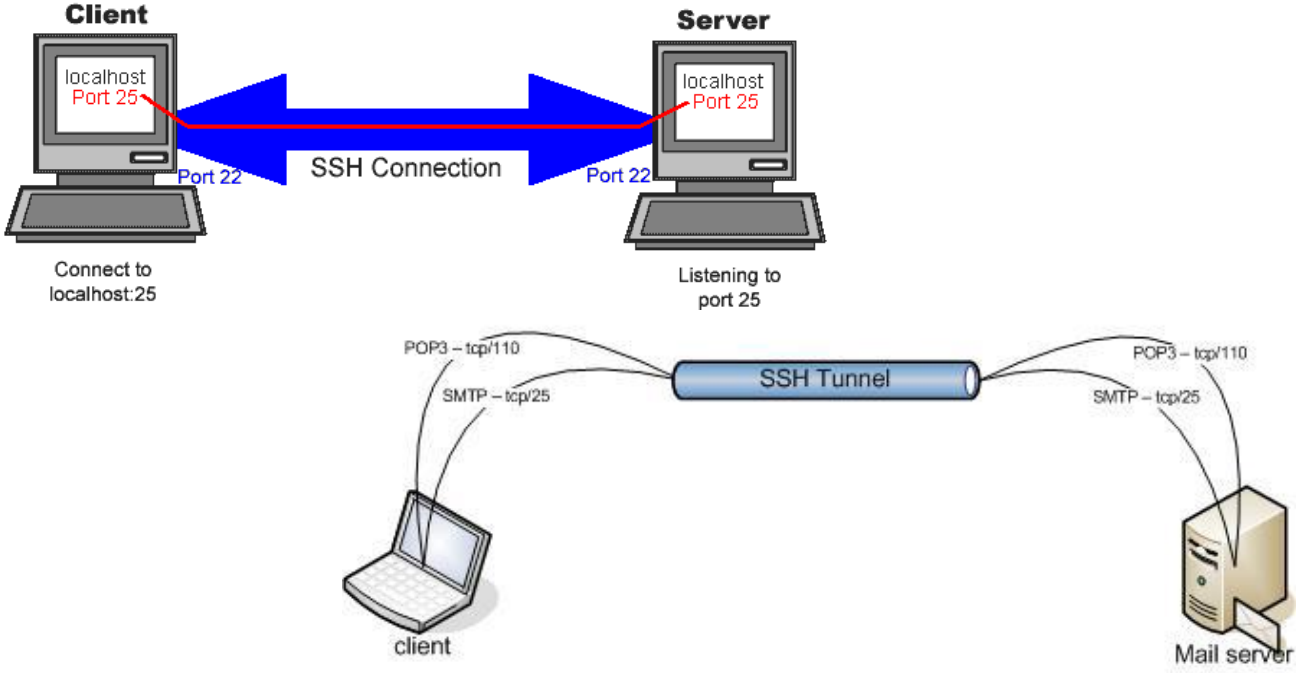
- SSH to tylko następca protokołu Telnet,
  różni się od Telnetu tym, że transfer danych jest zaszyfrowany oraz możliwe jest rozpoznawanie użytkownika na wiele różnych sposobów.

- W szerszym znaczeniu SSH to wspólna nazwa dla całej rodziny protokołów, nie tylko terminalowych, lecz także służących do przesyłania plików (SCP, SFTP), zdalnej kontroli zasobów, tunelowania i wielu innych zastosowań.
  Wspólną cechą wszystkich protokołów jest identyczna z SSH technika szyfrowania danych i rozpoznawania użytkownika.
  Protokoły z rodziny SSH praktycznie wyparły wszystkie inne mniej bezpieczne protokoły, takie, jak np. rlogin czy RSH.

- RFC 4250 RFC 4251 RFC 4252 RFC 4253 RFC 4254

SSH

- Najczęściej stosowany sposób szyfrowania to AES, część serwerów używa szyfrowania Blowfish i technik z rodziny DES.
- Uwierzytelnienie użytkownika może się opierać na haśle, kluczu (RSA, DSA) lub protokole Kerberos.
- Dwie najbardziej znane implementacje SSH to zamknięte ssh.com i otwarte OpenSSH. Znaną implementacją klienta ssh jest PuTTY.



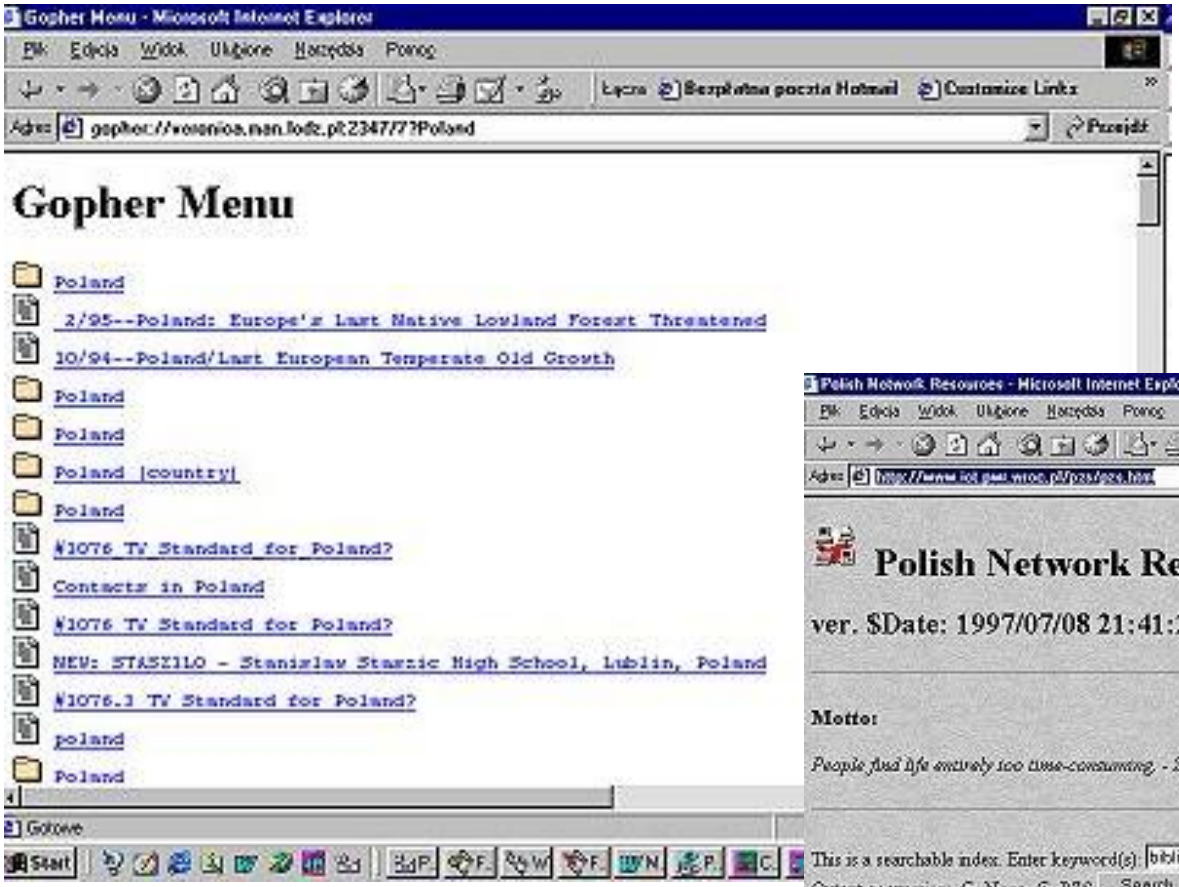
Gopher (przestarzały, niebezpieczny)

Powstał w kwietniu 1991 roku na University of Minnesota Microcomputer, Workstation, Networks Center w celu dystrybucji informacji wewnątrzwydziałowej.

Był pierwszym rozpowszechnionym systemem informacyjnym w sieci integrującym różne protokoły: FTP, telnet, WAIS własne struktury danych z możliwością dostępu do różnych typów danych, tak czysto tekstowych, jak i grafik i danych czysto binarnych (archiwów wszelkiego rodzaju).

Odchodzi w zapomnienie (dogorywają jeszcze resztki dawnej jego świetności) z powodu sztywnej, hierarchicznej struktury (gdzie jednym z elementów ścieżki dostępu był typ pliku), niewygodnych metod tworzenia serwisów, braku pełnej "multimedialności" czy wreszcie dlatego, że WWW zyskał większe wsparcie tak producentów jak i środowisk akademickich.

Gopher / WAIS (przestarzały, niebezpieczny)



File Transfer Protocol (FTP)

Protokół transmisji plików.
Protokół typu klient-serwer, który umożliwia przesyłanie plików z i na serwer poprzez sieć TCP/IP, zdefiniowany przez IETF w RFC 959.

FTP jest protokołem 8-bitowym, dlatego nie wymaga specjalnego kodowania danych na postać 7-bitową, tak jak ma to miejsce w przypadku poczty elektronicznej.

Do komunikacji wykorzystywane są dwa połączenia TCP.

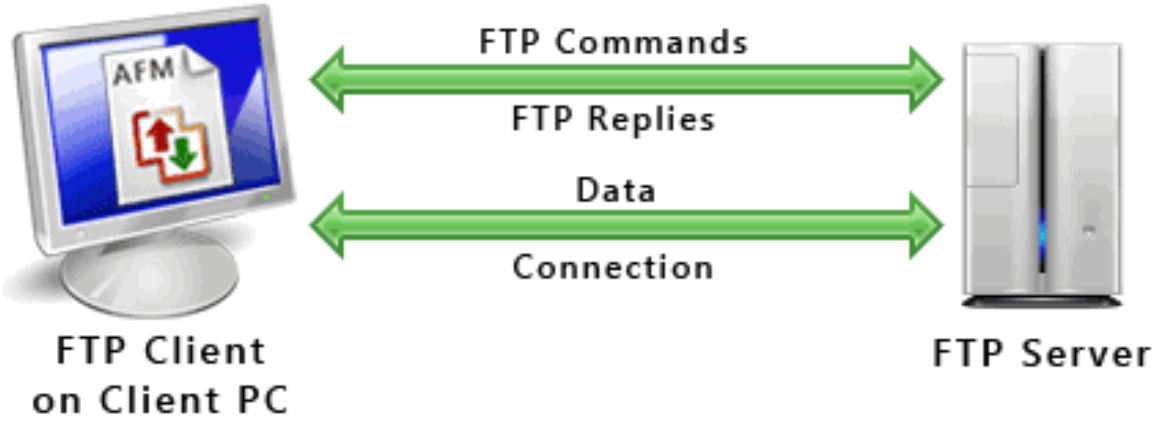
- kontrolne za pomocą którego przesyłane są np. polecenia do serwera,
- do transmisji danych m.in. plików.

FTP działa w dwóch trybach: aktywnym i pasywnym, w zależności od tego, w jakim jest trybie, używa innych portów do komunikacji.

File Transfer Protocol (FTP)

Pracując w trybie aktywnym, korzysta z portów: 21 dla poleceń (połączenie to jest zestawiane przez klienta) oraz 20 do przesyłu danych. Połączenie nawiązywane jest wówczas przez serwer.

Pracując w trybie pasywnym wykorzystuje port 21 do poleceń i port o numerze większy od 1024 do transmisji danych, gdzie obydwa połączenia zestawiane są przez klienta.



Network News Transport Protocol (NNTP)

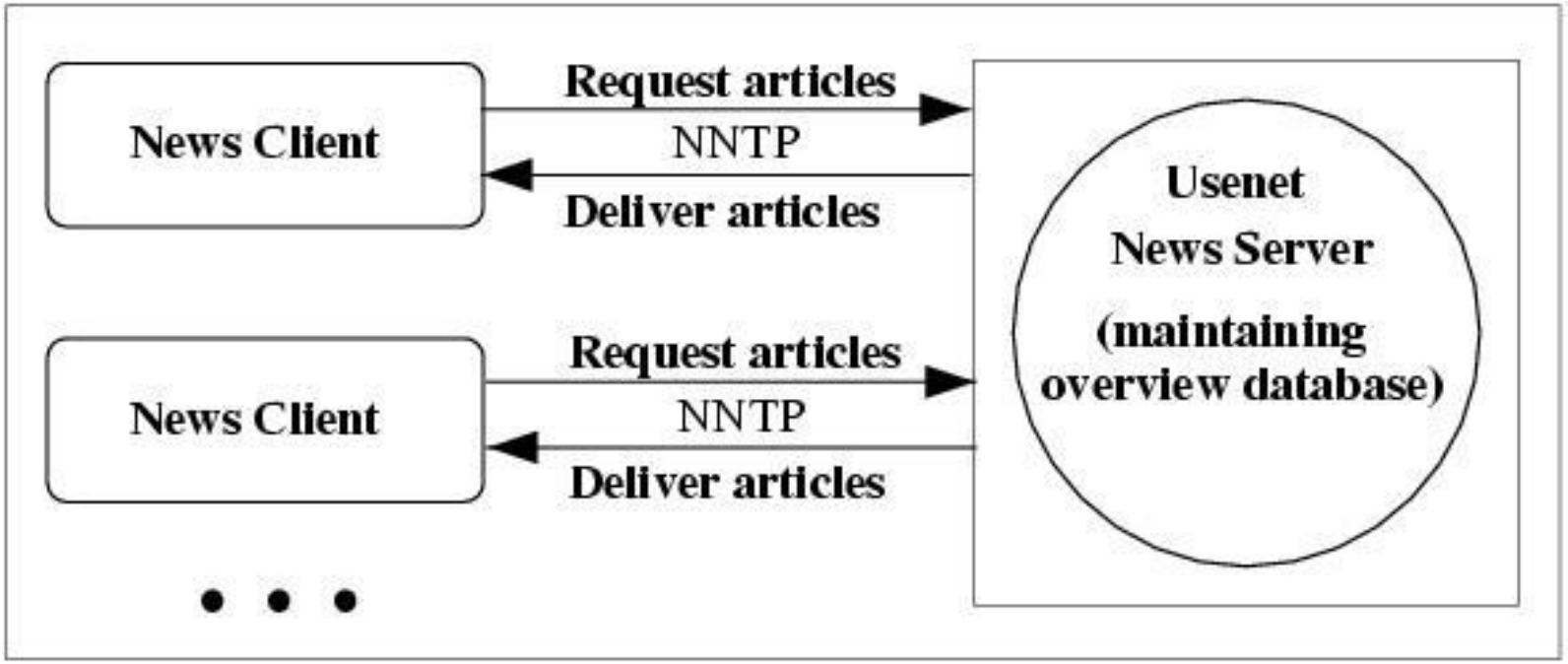
Oparty o TCP/IP protokół polegający na przesyłaniu ciągów tekstowych przez siedmiobitowe kanały ASCII.
Używany zarówno do przesyłania tekstów między serwerami, jak również do czytania i wysyłania artykułów.

NNTP zdefiniowano w RFC 977 w roku 1986.

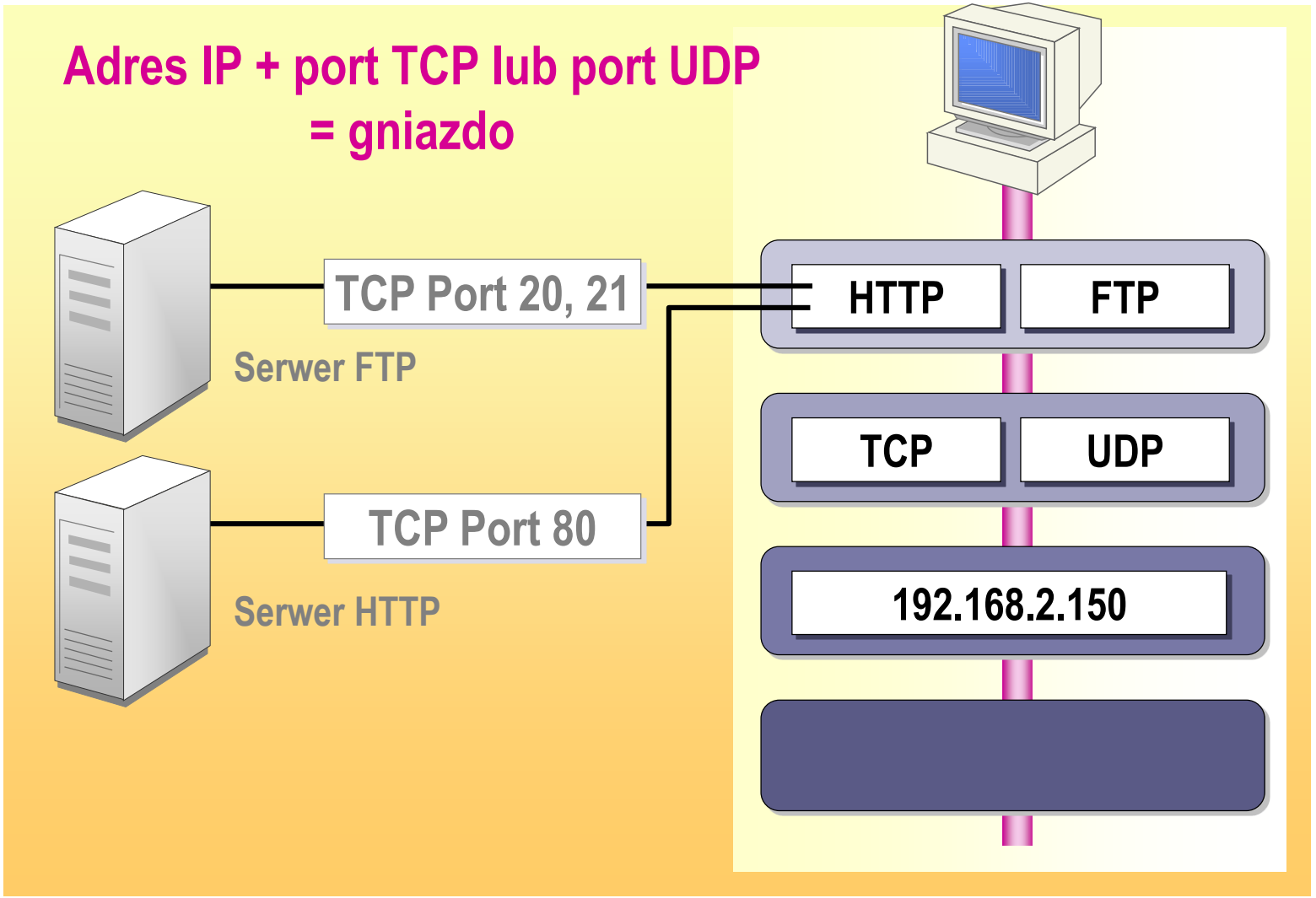
W roku 2000 w RFC 2980 został on rozszerzony o nowe możliwości.
Format wiadomości opisuje RFC 1036.

Na protokole tym oparte jest działanie usługi Usenet.
NNTP działa standardowo na porcie nr 119.

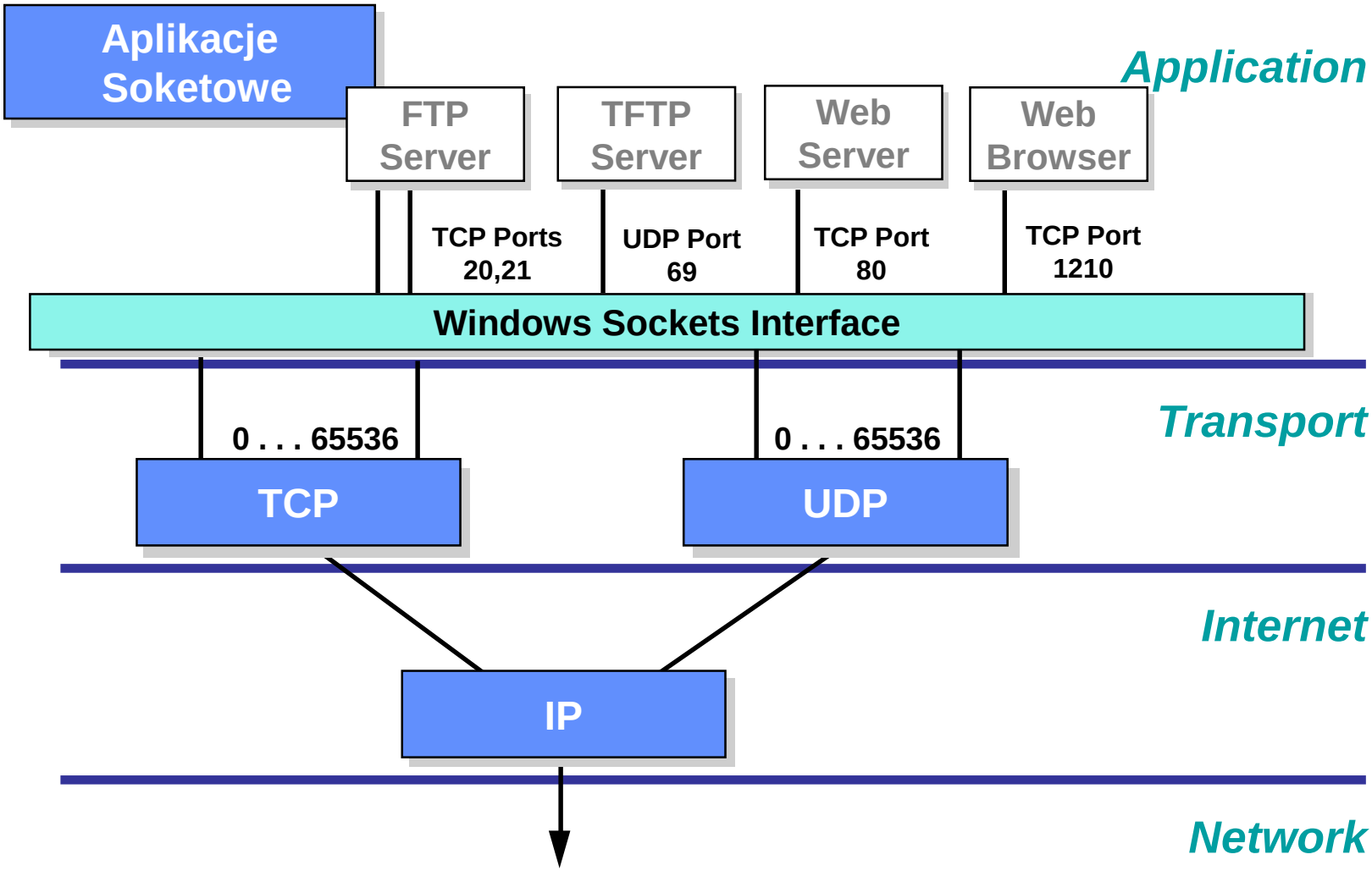
Network News Transport Protocol (NNTP)



Identyfikacja aplikacji



Porty i Gniazda



Porty i Gniazda

Porty i Gniazda

Dodatkowe pojęcia związane z TCP/IP

Porty - każda usługa w sieci ma przypisany sobie adres, zwany portem.

Najczęściej używane usługi otrzymały następujące porty

- File Transfer Protocol (FTP) **21**
- Telnet **23**
- SSH **22**
- Simple Mail Transfer Protocol (SMTP) **25**
- Gopher **70**
- Finger **79**
- Hypertext Transfer Protocol (HTTP) **80**
- HyperText Transfer Protocol Secure **443**
- Network News Transfer Protocol **119**

znane porty 0-1023

http://www.iana.org/assignments/port-numbers

...
ftp 21/tcp File Transfer [Control]
ftp 21/udp File Transfer [Control] # Jon Postel postel@isi.edu
ssh 22/tcp SSH Remote Login Protocol
ssh 22/udp SSH Remote Login Protocol # Tatu Ylonen ylo@cs.hut.fi
telnet 23/tcp Telnet telnet 23/udp Telnet # Jon Postel postel@isi.edu
24/tcp any private mail system
24/udp any private mail system # Rick Adams <rick@UUNET.UU.NET>
smtp 25/tcp Simple Mail Transfer
smtp 25/udp Simple Mail Transfer
...

Terminologia pakietów

Przykład współpracy protokołów TCP oraz IP podczas pobierania strony WWW:

1. Użytkownik wpisuje w przeglądarce adres strony na serwerze WWW

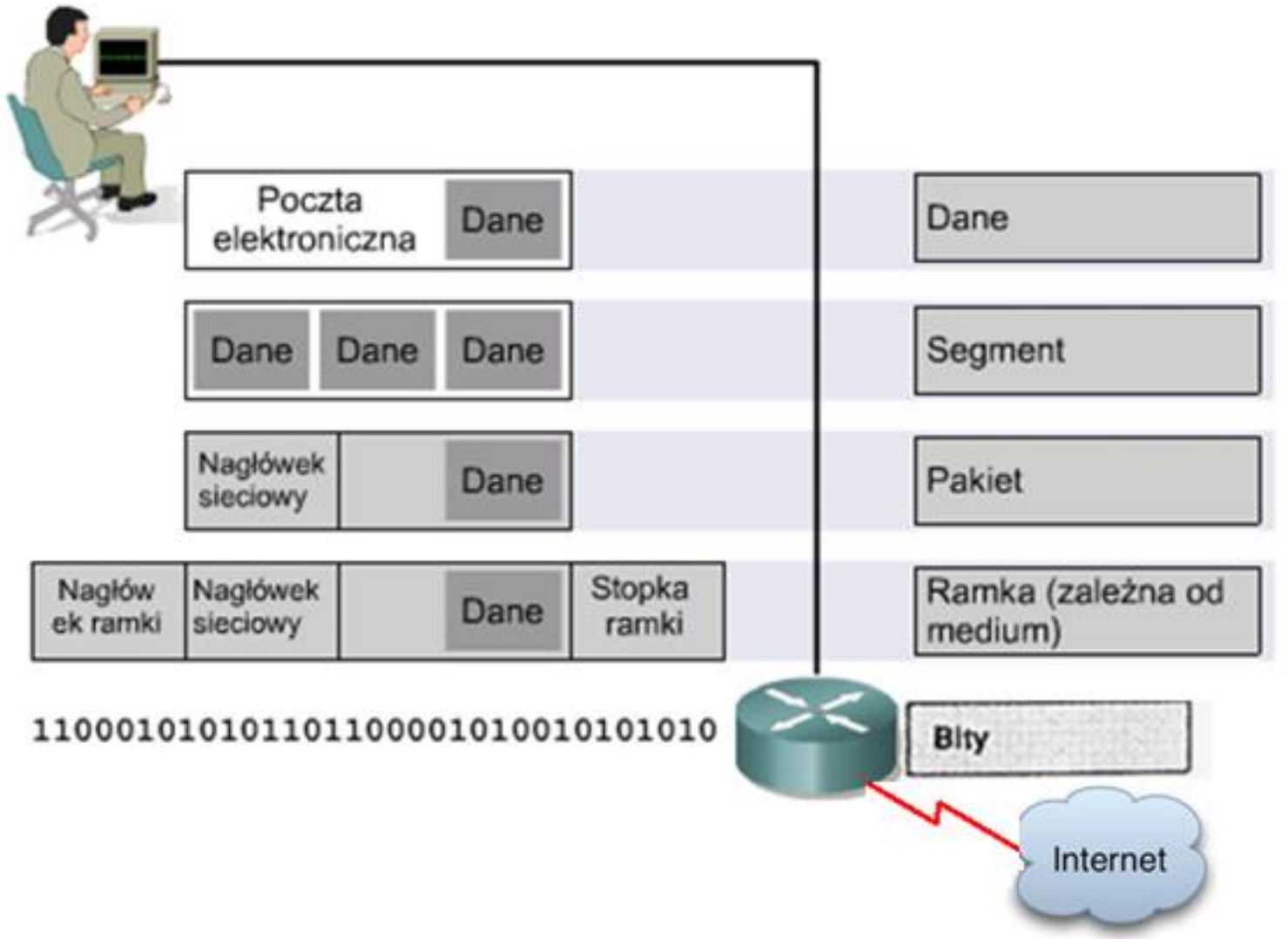
2. Mechanizm protokołu TCP serwera dzieli dokument HTML na odpowiednią liczbę pakietów

3. Następuje przekazanie pakietów do warstwy protokołu IP, który dołącza do każdego z nich adres komputera użytkownika (dostarczany przez przeglądarkę) i wysyła pakiety.

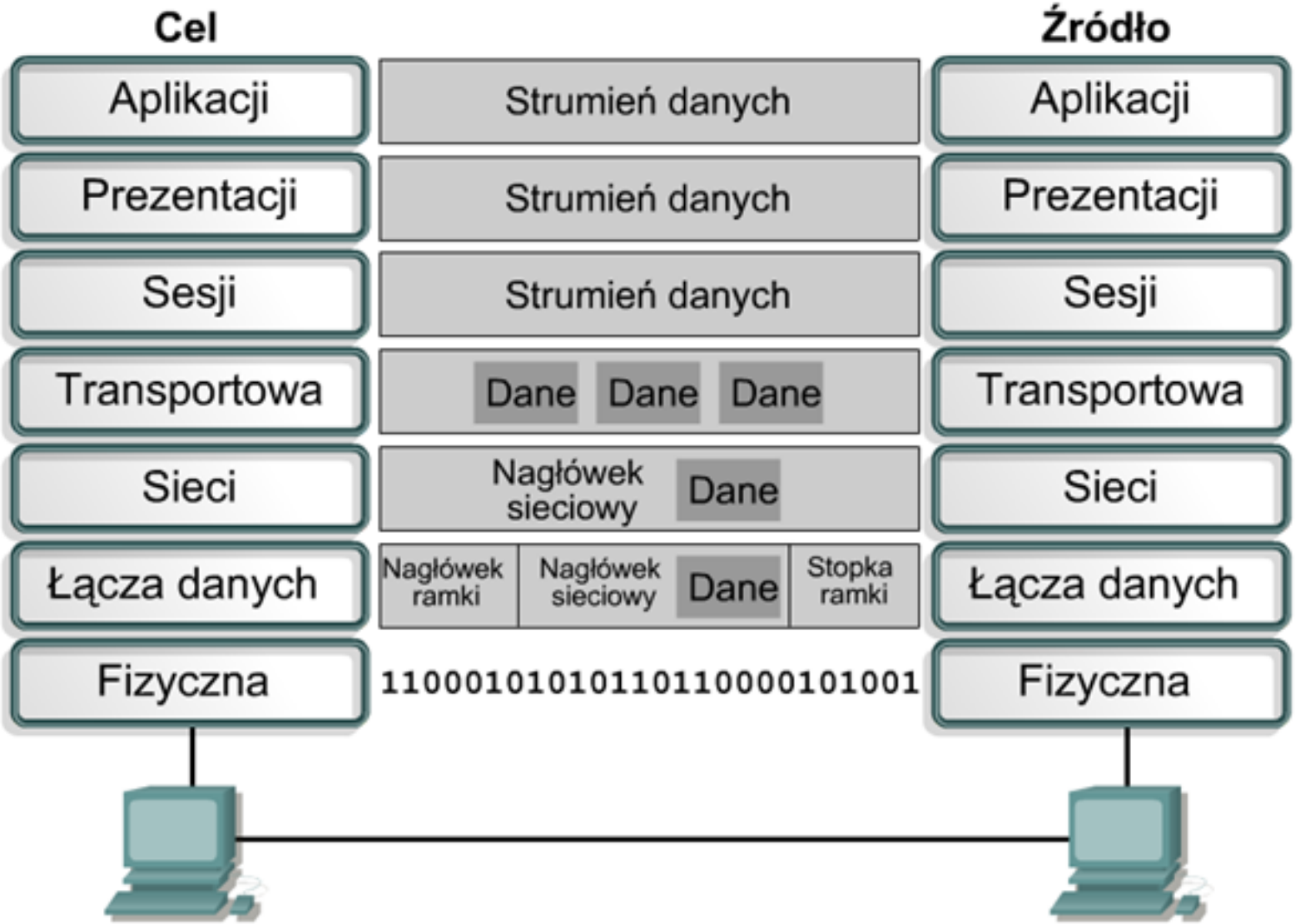
4. W sieci pakiety poruszają się niezależnie od siebie, przerzucane przez routery do kolejnych punktów pośrednich. W zależności od stanu połączeń ich trasy mogą różnić się od siebie, mogą w różnej kolejności osiągać cel.

5. Po dotarciu do komputera użytkownika, warstwa TCP rozpoznaje pakiety składające na ten sam plik i łączy je ze sobą. Przekazuje je następnie przeglądarce, która wyświetla stronę WWW na monitorze użytkownika.

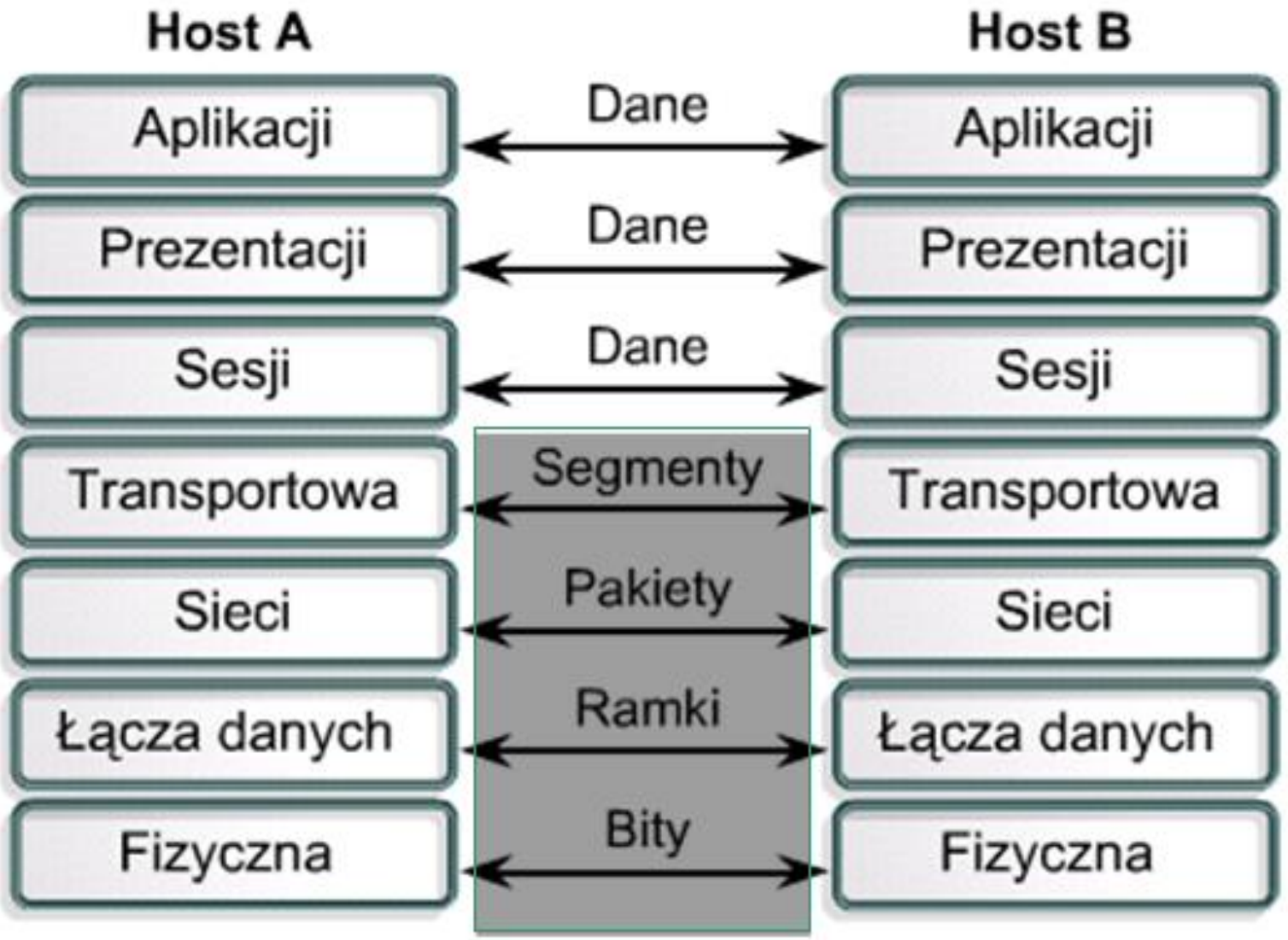
Mechanizm eknapsulacji



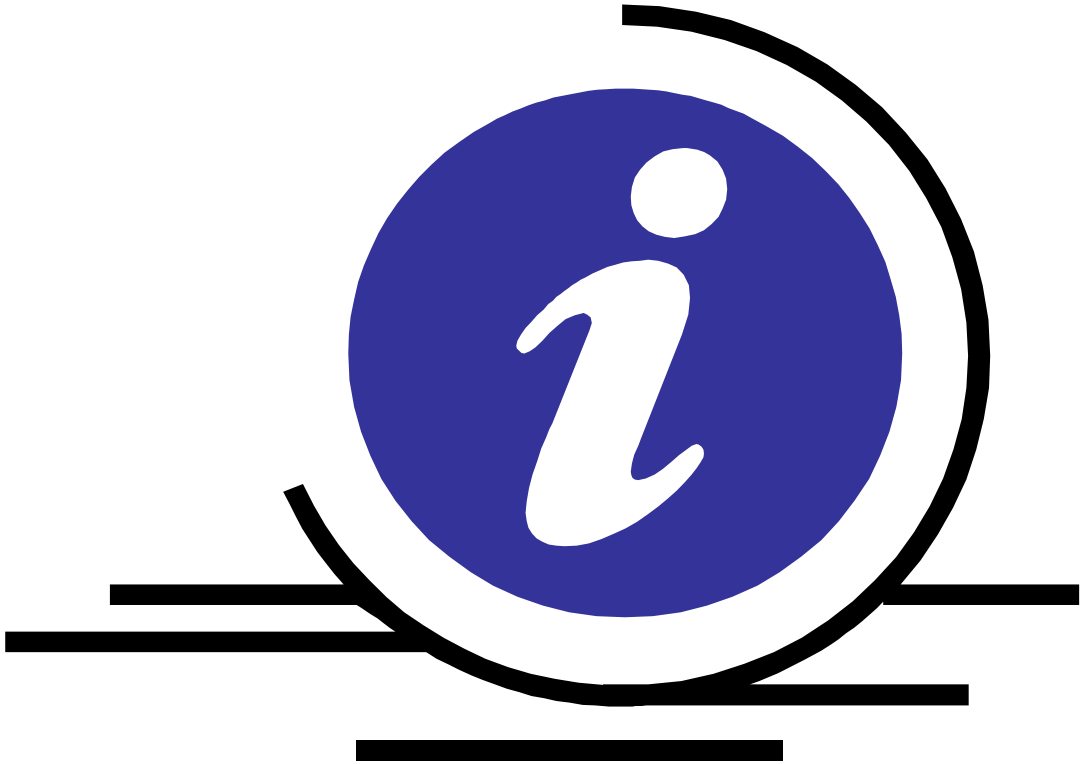
Mechanizm eknapsulacji



Mechanizm eknapsulacji



Pytania



Mechanizm eknapsulacji

http://www.linux-tutorial.info/Linux_Tutorial/Networking/TCP-IP//encapsula.gif /