84. Protokoły z rodziny TCP/IP warstwy transportowej modelu ISO OSI (UDP, TCP).

UDP (ang. *User Datagram Protocol* - Datagramowy Protokół Użytkownika) – 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.

UDP udostępnia mechanizm identyfikacji różnych punktów końcowych (np. pracujących aplikacji, usług czy serwisów) na jednym hoście dzięki *portom*. 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 65536 różnych zakończeń. Z przyczyn historycznych, porty 0-1023 zarezerwowane są dla dobrze znanych usług sieciowych - dla aplikacji użytkownika przydziela się porty od 1024.

Struktura nagłówka UDP

+	Bity 0 - 7	8 - 15	16 - 23	24 - 31
0	Adres źródłowy			
32	Adres docelowy			
64	Zera	Protokół	Długość UDP	
96	Port źródłowy		Port docelowy	
128	Długość		Suma kontrolna	
160	Dane			

TCP (ang. *Transmission Control Protocol* - protokół kontroli transmisji) – 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.

Opis nagłówka TCP

<table>
<tr><th>+</th><th>Bity 0 - 3</th><th>4 - 9</th><th>10 - 15</th><th>16 - 31</th></tr>
<tr><td>0</td><td colspan="3">Port nadawcy</td><td>Port odbiorcy</td></tr>
<tr><td>32</td><td colspan="4">Numer sekwencyjny</td></tr>
<tr><td>64</td><td colspan="4">Numer potwierdzenia</td></tr>
<tr><td>96</td><td>Długość nagłówka</td><td>Zarezerwowane</td><td>Flagi</td><td>Szerokość okna</td></tr>
<tr><td>128</td><td colspan="3">Suma kontrolna</td><td>Wskaźnik priorytetu</td></tr>
<tr><td>160</td><td colspan="4">Opcje (opcjonalnie)</td></tr>
<tr><td>160/192+</td><td colspan="4">Dane</td></tr>
</table>

85. Usługa translacji adresów w sieci TCP/IP.

NAT (ang. ***N**etwork **A**ddress **T**ranslation*), nazywany też w jednej ze swych odmian **maskarada** (z ang. *masquerade*) - 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 maskarada, czyli 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.

86. Usługi nazewnicze sieci TCP/IP.

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.

Wewnątrz każdej domeny można tworzyć tzw. subdomeny - stąd mówimy, że system domen jest 'hierarchiczny'. Przykładowo wewnątrz domeny .pl utworzono wiele domen:

- regionalnych jak 'opole.pl', 'dzierzoniow.pl' czy 'warmia.pl'
- funkcjonalnych jak 'com.pl', 'gov.pl' czy 'org.pl'
- należących do firm, organizacji lub osób prywatnych jak 'onet.pl', 'zus.pl' czy 'olechowski.pl'

Nazwy domen i poszczególnych komputerów składają się z pewnej liczby nazw, oddzielonych kropkami. Ostatnia z tych nazw jest domeną najwyższego poziomu. Każda z tych nazw może zawierać litery, cyfry lub znak '-'. Od niedawna w nazwach niektórych domen można używać znaków narodowych (IDN) takich jak 'ą' czy 'ż', ale większość współczesnych programów nie przewiduje możliwości wykorzystania takich funkcji. Trwają prace nad nowymi standardami odpowiadającymi DNS, które będą obsługiwać kodowanie Unicode, co pozwoli na umieszczanie w nazwach domen dowolnych znaków np. polskich albo chińskich równocześnie. W Polsce domeny zawierające znaki diakrytyczne praktycznie nie występują. Wewnątrz każdej z poddomen można tworzyć dalsze poddomeny, np. w domenie 'wikipedia.org' można utworzyć domenę *pl.wikipedia.org*.

DNS, jako system organizacyjny, składa się z dwóch instytucji - IANA i ICANN. Nadzorują one ogólne zasady przyznawania nazw domen i adresów IP. Jednak te dwie instytucje nie są w stanie zajmować się całym światem i dlatego cedują swoje uprawnienia na szereg lokalnych instytucji i firm. W wielu krajach domena internetowa przyznana przez system DNS staje się własnością tego, kto pierwszy ją kupi. W Polsce jest ona tylko wynajmowana na określony czas. Jeżeli ktoś zrezygnuje ze swojej popularnej domeny i zwróci ją administratorowi DNS, to może się spodziewać, że trafi ona w niepowołane ręce.

87. Mosty i przełączniki w sieci Ethernet.

Most lub **mostek** (ang. *bridge*) to urządzenie warstwy łącza danych (ang. *Data Link Layer – DLL*) modelu OSI/ISO decydujące o przesyłaniu ramek danych (czyli pakietów danych warstwy 2) na podstawie stworzonej przez siebie tablicy forwardingu (ang. *Forwarding DataBase – FDB* lub *MAC DataBase*), zawierającej numery portów (interfejs E0/0, E0/1, itd...), do których przyłączone są urządzenia (każdy port to inny segment sieci), oraz adresy sprzętowe MAC urządzeń w segmencie sieci.

Mosty działają w trybie nasłuchu (ang. *promiscuous mode*) i odbierają dane krążące w medium transmisyjnym. Aby określić, jakie urządzenia znajdują się w poszczególnych segmentach sieci (skojarzonych z poszczególnymi portami), mosty odczytują źródłowe adresy MAC z ramek danych. Na tej podstawie tworzona jest tablica forwardingu (w wolnym tłumaczeniu "tablica mostowania"). Mosty, w przeciwieństwie do przełączników, mają

oprogramowanie w formie software'owej a nie hardware'owej, są więc od przełączników wolniejsze (switch używa układu scalonego ASIC wspomagającego podejmowanie decyzji o filtrowaniu). Mosty mogą mieć tylko jedną instancję drzewa rozpinającego przypadającą na jeden most, switche mogą mieć ich wiele. Podobnie mosty mogą mieć tylko do 16-tu portów, zaś przełączniki mogą mieć ich setki.

Kiedy mostek (lub analogicznie switch) odbierze ramkę, poszukuje jej adresu docelowego w swojej tablicy forwardingu.

- Jeśli go znajdzie, odczytuje port skojarzony z adresem docelowym, interpretując go teraz jako port docelowy. Następnie zajmuje się porównaniem. Jeśli port docelowy jest taki sam jak port, z którego przyszła ramka, mostek nic nie robi (nie przepuszcza na zewnątrz ruchu docelowo lokalnego). Jeśli port docelowy jest inny niż źródłowy, most przekazuje ramkę dalej, do portu docelowego – na zewnątrz.
- Jeśli mostek nie znajdzie adresu docelowego w FDB, zalewa (ang. flood) sieć, przekazując pakiet danych na wszystkie porty za wyjątkiem źródłowego.
- Jeśli natomiast adres docelowy jest typu multicast (grupowy), most przekazuje ramkę do grupy urządzeń, może więc służyć do tworzenia wirtualnych sieci lokalnych (VLAN).

Dzięki temu blokowane są pakiety, których nie trzeba przekazywać dalej poza lokalny segment sieci. Poprzez nieprzepuszczanie niepotrzebnych ramek, może się zmniejszyć obciążenie sieci.

Mimo, iż mosty są niewidoczne dla innych urządzeń (gdyż nie modyfikują ramek, jedynie je "podsłuchują"), użycie mostu powoduje zwiększenie opóźnienia w sieci o 10–30 procent (ale jednocześnie obciążenie sieci może się zmniejszyć). Wynika to z decyzji, jakie most musi podjąć przed przekazaniem pakietu.

Most jest uznawany za urządzenie zachowujące i przesyłające (ang. *store and forward*). Przed przesłaniem ramki dalej most analizuje pole zawierające adres odbiorcy i oblicza kod cyklicznej kontroli nadmiarowej CRC podany w polu kodu kontrolnego ramki. Jeśli port docelowy jest zajęty, most tymczasowo zachowuje ramkę do momentu, gdy będzie on wolny.

Można wyróżnić **mosty przeźroczyste**, **LSB** oraz **realizujące routing źródłowy**.

Mosty przezroczyste zwane też uczącymi się lub inteligentnymi, stosowane są w sieciach typu Ethernet. Tuż po zainstalowaniu urządzenie rozpoczyna proces poznawania topologii sieci. Tablica mostu jest stale aktualizowana. Mosty przezroczyste w rozległych sieciach działają w oparciu o algorytm STA (ang. *spanning tree algorithm*). Polega on na tworzeniu wielu alternatywnych dróg połączeń, ale pozostawieniu zawsze jednej trasy wolnej (zazwyczaj jest to jedna linia komutowana). Odblokowywana ona jest tylko w razie konieczności np. awarii innej drogi.

Mosty LSB (ang. *load-sharing bridges*) także stosowane są w sieciach Ethernet. Pozwalają na używanie tej rezerwowej linii, która jest nie wykorzystana w bridge'ach przezroczystych. Są więc przez to najwydajniejsze.

Mosty realizujące routing źródłowy działają w sieciach Token Ring. Poza informacją o miejscu docelowym pakietów, most w tym wypadku wie także którędy najlepiej je tam

przesłać. Przy czym to nie urządzenie wybiera optymalną trasę, lecz odczytuje je z danych zawartych w samych pakietach.

Switch (z ang., w jęz. polskim *przełącznik*, *przełącznica*, także *komutator*) – urządzenie łączące segmenty sieci komputerowej. Switch pracuje w warstwie drugiej modelu OSI (łącza danych), jego zadaniem jest przekazywanie ramek między segmentami.

Switche określa się też mianem wieloportowych mostów (ang. *bridge*) lub inteligentnych hubów – switch używa logiki podobnej jak w przypadku mostu do przekazywania ramek tylko do docelowego segmentu sieci (a nie do wszystkich segmentów jak hub), ale umożliwia połączenie wielu segmentów sieci w gwiazdę jak hub (nie jest ograniczony do łączenia dwóch segmentów jak most).

W celu ustalenia fizycznego adresata używają docelowego adresu MAC zawartego w nagłówku ramki Ethernet. Jeśli switch nie wie, do którego portu powinien wysłać konkretną ramkę, **zalewa** (*flooding*) wszystkie porty z wyjątkiem portu, z którego ramkę otrzymał. Switche utrzymują tablicę mapowań adres MAC<->port fizyczny, której pojemność jest zwykle określona na 4096, 8192 lub 16384 wpisów. Po przepełnieniu tej tablicy nowe wpisy nie są dodawane (chyba że któryś stary wygaśnie), a ramki 'zalewane' są do wszystkich portów (za wyjątkiem portu, którym ramka dotarła do switcha).

Switche ograniczają domenę kolizyjną do pojedynczego portu, dzięki czemu są w stanie zapewnić każdemu hostowi podłączonemu do portu osobny kanał transmisyjno-nadawczy, a nie współdzielony, tak jak huby.

Przekazywanie ramek przez switcha może się odbywać w różnych trybach. W przełącznikach zarządzalnych istnieje możliwość wyboru odpowiedniego trybu. Dostępne tryby to:

- Cut-through – wprowadza najmniejsze opóźnienie, brak sprawdzania poprawności ramek.
- Store and forward – wprowadza największe opóźnienie, sprawdza sumy kontrolne (CRC) ramek.
- Fragment free – rozwiązanie pośrednie sprawdzające tylko poprawność nagłówka ramki.
- Przełączanie adaptacyjne – na podstawie ruchu wybierany jest jeden z powyższych trybów.

88. Protokół DHCP.

DHCP (ang. ***D**ynamic **H**ost **C**onfiguration **P**rotocol* - protokół dynamicznego konfigurowania węzłów) to protokół komunikacyjny umożliwiający komputerom uzyskanie od serwera danych konfiguracyjnych, np. adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski sieci. Protokół DHCP jest zdefiniowany w RFC 2131 i jest następcą BOOTP. DHCP został opublikowany jako standard w roku 1993.

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 RFC 2136.

Nagłówek DHCP

00 - 07	08 - 15	16 - 23	24 - 31
operacja	typ sprzętu	długość adresu sprzętowego	ilość skoków
xid (identyfikator transakcji)			
ilość sekund		flagi	
adres IP klienta			
przydzielony adres IP klienta			
adres IP serwera			
adres IP bramki (rutera)			
adres sprzętowy klienta (16 oktetów)			
nazwa serwera (64 oktety)			
plik startowy (128 oktetów)			
opcje producenta (długość zmienna)			

Serwer DHCP może dostarczać swoim klientom dodatkowe dane pozwalające na konfigurację sieci. Zostały one opisane w specyfikacji RFC 2132.

Niektóre z dodatkowych opcji

- adres IP serwera DNS
- nazwa DNS
- adres IP bramy sieciowej (ang. *gateway*)
- adres broadcast
- maska podsieci
- maksymalny czas oczekiwania na odpowiedź w protokole ARP
- wartość MTU (maksymalny rozmiar pakietu)
- adresy serwerów NIS

- domena NIS
- adres IP serwera SMT
- adres serwera TFTP
- adres serwera nazw NetBIOS

89. Protokoły poczty elektronicznej w sieci TCP/IP (SMTP, POP, IMAP).

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. Demon SMTP działa najczęściej na porcie 25. Łatwo przetestować serwer SMTP przy użyciu programu telnet.

SMTP zaczęło być szeroko używane we wczesnych latach osiemdziesiątych dwudziestego wieku. W tamtym okresie było to uzupełnienie UUCP, który lepiej sprawdzał się przy przekazywaniu poczty między maszynami posiadającymi jedynie okresowe połączenie. SMTP natomiast lepiej działa, gdy zarówno maszyna nadająca jak odbierająca są na stałe przyłączone do sieci.

Jednym z pierwszych (jeśli nie pierwszym) z programów do przesyłania poczty, w którym zastosowano SMTP był sendmail. W roku 2001 istniało przynajmniej 50 (pięćdziesiąt) programów implementujących SMTP jako klient (nadawca) lub serwer (odbiorca wiadomości). Niektóre inne popularne programy serwerów SMTP to exim, Postfix, Qmail Bernsteina, GroupWise firmy Novell i Microsoft Exchange.

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

Post Office Protocol version 3 (**POP3**) to protokół internetowy z warstwy aplikacji pozwalający na odbiór poczty elektronicznej ze zdalnego serwera do lokalnego komputera poprzez połączenie TCP/IP. Ogromna większość współczesnych internautów korzysta z POP3 do odbioru poczty

Wcześniejsze wersje protokołu POP czyli, POP (czasami nazywany POP1), POP2 zostały całkowicie zastąpione przez POP3. Zwykle jeżeli ktoś mówi o protokole POP ma na myśli jego wersję 3.

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.

Programy odbierające pocztę najczęściej obsługują oba protokoły, ale POP3 jest bardziej popularny. Wysyłanie listów zawsze opiera się na protokole SMTP. Komunikacja POP3 może zostać zaszyfrowana z wykorzystaniem protokołu SSL. Jest to o tyle istotne, że w POP3 hasło przesyłane jest otwartym tekstem, o ile nie korzysta się z opcjonalnej komendy protokołu POP3, APOP.

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.

IMAP (*Internet Message Access Protocol*) to internetowy protokół pocztowy zaprojektowany jako następca POP3.

W przeciwieństwie do POP3, który umożliwia jedynie pobieranie i kasowanie poczty, IMAP pozwala na zarządzanie wieloma folderami pocztowymi oraz pobieranie i operowanie na listach znajdujących się na zdalnym serwerze.

IMAP pozwala na ściągnięcie nagłówków wiadomości i wybranie, które z wiadomości chcemy ściągnąć na komputer lokalny. Pozwala na wykonywanie wielu operacji, zarządzanie folderami i wiadomościami.

90. Protokoły transferu plików w sieci TCP/IP (TFTP, FTP).

TFTP to skrót od angielskiego *Trivial File Transfer Protocol*

Jest to względnie prosty protokół wykorzystywany do przesyłania plików, które są (zazwyczaj) małe i nie wymagają wiele fragmentacji.
Jest on implementowany na protokole UDP, chociaż jego definicja nie wyklucza stosowania innych protokołów datagramów.
Nie posiada większości funkcji protokołu FTP -np. nie może wyświetlać katalogów, ani uwierzytelniać użytkowników ,a jego jedynym zadaniem jest odczytywanie plików z komputera zdalnego i transmitowanie do niego plików. Protokół TFTP wykorzystywany jest przeważnie przez aplikacje poczty elektronicznej.

Przesył TFTP rozpoczyna się od żądania odczytu lub zapisu pliku, które żąda również połączenia. Plik wysyłany jest w blokach o stałej długości 512 bajtów. Każdy z pakietów musi być potwierdzony przez pakiet potwierdzający, zanim będzie mógł zostać wysłany następny pakiet.Pakiet danych mniejszy niż 512 bajtów wskazuje zakończenie przesyłu.
Jeżeli jakiś pakiet ulegnie zagubieniu, to u planowanego odbiorcy następuje przeterminowanie, a ten następnie żąda transmisji zagubionego pakietu. Pakiet retransmitowany w tym przypadku, to ostatni pakiet poprzedniej transmisji, więc nadawca musi zachować do retransmisji tylko jeden pakiet.
Poprzednie potwierdzenia gwarantują, że pakiety uprzednio wysłane zostały otrzymane.
Każdemu z pakietów danych towarzyszy numer bloku. Numery bloków są kolejne i zaczynają się od jeden, za wyjątkiem pozytywnej odpowiedzi na żądanie zapisu, która jest pakietem potwierdzającym o numerze bloku zero. Zazwyczaj pakiet potwierdzający zawiera numer bloku potwierdzanego pakietu danych.
Poza jednym wyjątkiem , błąd sprawia zakończenie połączenia. Błąd, sygnalizowany przez pakiet błędu, nie jest potwierdzany ani retransmitowany. Dlatego też, kiedy pakiet ulegnie zagubieniu, do wykrycia zakończenia wykorzystywane jest przeterminowanie.
Jeżeli port źródłowy otrzymanego pakietu jest niewłaściwy, to błąd nie powoduje zakończenia; do hosta, z którego pochodzi pakiet, zostaje wysłany pakiet błędu.

FTP (*ang. File Transfer Protocol*) jest protokołem typu klient-serwer, który umożliwia przesyłanie plików z i na serwer poprzez sieć TCP/IP. Protokół ten jest 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. Jedno z nich jest połączeniem kontrolnym za pomocą którego przesyłane są np. polecenia do serwera, drugie natomiast służy 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.

Jeżeli FTP pracuje 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. Jeżeli FTP pracuje w trybie pasywnym wykorzystuje port 21 do poleceń i port o numerze > 1024 do transmisji danych, gdzie obydwa połączenia zestawiane są przez klienta. W sieciach ukrytych za firewallem komunikacja z aktywnymi serwerami FTP jest możliwa, tylko pod warunkiem, jeżeli odpowiednie porty na firewallu (routerze) są zwolnione. Możliwe

jest zainstalowanie wielu serwerów FTP za jednym i tym samem routerem. Warunkiem jest rozdzielenie portów przez router dla każdego serwera.

Źródło Wikipedia.org