HTTP (ang. Hypertext Transfer Protocol) – protokół przesyłania dokumentów hipertekstowych) to protokół sieci WWW (ang. World Wide Web). 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 użyteczny, ponieważ udostępnia znormalizowany sposób komunikowania się komputerów ze sobą. Określa on formę żądań klienta (tj. np. przeglądarki www) dotyczących danych oraz formę odpowiedzi serwera na te żądania. Jest zaliczany do protokołów bezstanowych (ang. stateless) z racji tego, że nie zachowuje żadnych informacji o poprzednich transakcjach z klientem (po zakończeniu transakcji wszystko "przepada"). Pozwala to znacznie zmniejszyć obciążenie serwera, jednak jest kłopotliwe w sytuacji, gdy np. trzeba zapamiętać konkretny stan dla użytkownika, który wcześniej łączył się już z serwerem.

Model **TCP/IP**. Podstawowym założeniem modelu TCP/IP jest podział całego zagadnienia komunikacji sieciowej na szereg współpracujących ze sobą warstw (ang. layers). Każda z nich może być tworzona przez programistów zupełnie niezależnie, jeżeli narzucimy pewne protokoły według których wymieniają się one informacjami. Założenia modelu TCP/IP są pod względem organizacji warstw zbliżone do modelu OSI. Jednak liczba warstw jest mniejsza i bardziej odzwierciedla prawdziwą strukturę Internetu. Model TCP/IP składa się z czterech warstw: aplikacji, transportowej, internetu, dostępu do sieci.

IPv4

Pod koniec lat siedemdziesiątych ubiegłego wieku opracowano ten protokół na zlecenie Departamentu Obrony Stanów Zjednoczonych. IPv4 miał za zadanie połączyć ze sobą rozsiane po całym kraju wojskowe sieci WAN, w pojedynczą zunifikowaną sieć ARPANET. Następne lata przyniosły jego akceptację jako głównego protokołu warstwy sieci dla Internetu, a także dla sieci lokalnych. IP odpowiada za dostarczanie procedur, które wystarczają do przesyłania danych pomiędzy maszynami, które znajdują się w połączonych ze sobą sieciach.
Definiowany jest format pakietów oraz metody ich adresowania. Nie odpowiada on jednak za realizację żadnych funkcji, które są związane z poprawnością transmisji. Nie identyfikuje on pakietów, które wymagają ponownego przesłania. Nie jest w stanie również wykonać wielu innych procesów, które są związane z odtworzeniem prawidłowej sekwencji pakietów, ponieważ pakiety mogą podróżować do celu różnymi drogami i przez to kolejność ich odbierania może się różnić od kolejności nadawania. Jest to więc protokół bezpołączeniowy, który nie zapewnia stałego kanału do komunikacji. Dopiero dzięki współpracy protokołu IP, a także jednego z protokołów wyższej warstwy transportu możliwe jest wygodne i prawidłowe przesyłanie danych na większe odległości. Przykłady protokołów, które korzystają w czasie transmisji z protokołu IP to UDP oraz TCP. W tego rodzaju przypadkach, dzięki określeniu dwóch współdziałających ze sobą protokołów, możliwe jest używanie rozdzielonych ukośnikiem nazw, takich jak TCP / IP oraz UDP / IP. Analizując TCP komunikacja połączeniowa jest symulowana w bezpołączeniowym kanale na drodze wymiany pakietów oraz potwierdzeń ich odbioru. Aby zidentyfikować sieć, urządzenia sieciowe oraz hosty protokołów IP, wykorzystywany jest binarny system adresowania. IPv4 zakłada 32 bitowy adres, który składa się z czterech sekcji liczb ośmiobitowych,

oddzielonych od siebie kropkami, przykładowo 192.168.1.10. Ponieważ ARPANET miał za zadanie łączyć maksymalnie kilkadziesiąt instytucji, przyjęcie 32 - bitowej przestrzeni adresowej wydawało się być bardzo nowoczesnym i przyszłościowym rozwiązaniem. W dzisiejszych czasach rozwój Internetu przekroczył jednak najśmielsze oczekiwania ich twórców. W pewnym momencie liczba wolnych adresów IP zaczęła w sposób drastyczny maleć. Z tego powodu koniecznym stało się opracowanie zupełnie nowej wersji protokołu IP. Następcą protokołu IPv4 stał się protokół IPv6, który jest również nazywany protokołem IP nowej generacji IP NG.

IPv6

Następca protokołu IP wyróżnia się między innymi unowocześnionym schematem adresacji urządzeń podpiętych do sieci Internet. Poszerzenie standardu stosowanego dotychczas stanowi odpowiedź na dynamiczny rozwój Internetu, jaki dokonał się w ostatnich latach. Na skutek gwałtownego wzrostu liczby komputerów podłączonych do sieci, zaczęła ona pękać w szwach, a pula wolnych adresów IPv4 znalazła się na wyczerpaniu. Chociaż trudno to sobie wyobrazić, ale zapotrzebowania na adresy IP przewyższają 4 miliardy kombinacji cyfr, które można ułożyć z 32 bitowego kodu. Na skutek podzielenia puli adresów na klasy adresów doprowadzono do roztrwonienia tego jakże wielkiego zasobu. Również zadania, jakim muszą sprostać współczesne łącza internetowe wyglądają zupełnie inaczej niż przed dwudziestoma laty, kiedy standard IP był projektowany. Rosnący w siłę biznes elektroniczny zaczął się z kolei domagać poprawienia bezpieczeństwa przesyłanych siecią danych. Aby możliwe było nadążenie za szybką ekspansją Internetu musiano wyeliminować każdą pojawiającą się w protokole IPv4 słabość oraz uwzględnić rozsądny zapas puli adresowej na przyszłość. IPv6 stanowi rozwiązanie wymienionych wcześniej problemów, dostarcza ona również zupełnie nowych możliwości. Poniżej przedstawione są najważniejsze zmiany, które dotyczą protokołu IPv6:

Dłuższe adresy internetowe. Dotychczas stosowane adresy 32 bitowe zostały zastąpione adresami 128 - bitowymi. Pula możliwych do wykorzystania adresów internetowych została więc w sposób niewyobrażalny powiększona. W chwili obecnej nie ma żadnych przeszkód, by indywidualne adresy IP przypisywać wszystkim urządzeniom, nawet takim jak pagery i komputery pokładowe montowane w nowoczesnych samochodach. Przestrzeń adresowa protokołu IPv6 wygląda w nieco inny sposób od jej czwartej wersji. Pełny adres IPv6 składa się bowiem z ośmiu 16 bitowych części oddzielonych dwukropkami. Przykładowy adres może więc wyglądać w ten sposób: 234A:BD89:FEA8:8762:1235:DC98:11AA:FFFF.

Zwiększona elastyczność, a także zupełnie nowe struktury adresowe. W nowym protokole nastąpiło odejście od sposobu adresowania, które bazowało na klasach, protokół IPv4 rozróżniał bowiem pięć rodzajów klas adresów, które przeznaczone były dla różnej wielkości sieci.

Prostszy oraz bardziej elastyczny format nagłówków krążących po sieci pakietów.

Większe bezpieczeństwo przesyłanych pakietów. Wprowadzone zostały elementy zapobiegające najczęściej spotykanym atakom, a także wbudowano opcje ich szyfrowania oraz identyfikacji poszczególnych hostów, przy pomocy towarzyszącego protokołu Ipsec. Tym samym na całej długości połączenia zostało zapewnione bezpieczeństwo.
Zapewniona przestrzeń dla ewentualnych przyszłych rozszerzeń tego protokołu.

Rozpoznawane są trzy rodzaje adresów:

Unicast - standardowy tryb adresacji pakietów, który pozwala na transmisję danych pomiędzy hostem, a nadawcą oraz pomiędzy hostem, a odbiorcą.

Multicast - podobnie jak powyższy sposób adresacji posiada on swój odpowiednik w IPv4.

Anycast - nowy sposób adresacji, którego wprowadzono w protokole IPv6. Przewiduje on możliwość transmisji danych do bramy znajdującej się najbliżej, spośród tych znajdujących się w obrębie danej lokalizacji, z zamiarem powierzenia tej bramie zadania dalszego przekierowania wysyłanego pakietu.

W ciągu ostatnich kilku lat protokół IPv6 poddawano intensywnym testom. W chwili obecnej zachodzi jego stopniowe wdrażanie. Pierwsze pule adresów IPv6 zostały przekazane regionalnym organizacjom zajmującym się przydzielaniem adresów IP w lipcu roku 1999. Poprzez wprowadzenie IPv6 zaszła konieczność modyfikacji wszystkich standardów oraz usług spotykanych w sieci, takich jak chociażby DNS. Usługi te muszą w tym momencie współpracować z obiema wersjami protokołu IP oraz obsługiwać poprawnie 128 bitowe adresy urządzeń. W samym protokole IPv6 zawarte są mechanizmy, które umożliwiają ich współistnienie ze starszymi wersjami IP, przykładem jest tutaj mechanizm translacji adresu IPv4 na adres IPv6. Obsługę IPv6 wprowadza się obecnie w każdych routerach produkowanych w dzisiejszych czasach. Na pewno pełne przejście do nowego procesu będzie procesem bardzo powolnym. Należy się spodziewać, że przez najbliższe lata obie wersje protokołu IP będą musiały koegzystować ze sobą.

HTTPS (ang. HyperText Transfer Protocol Secure) to szyfrowana wersja protokołu HTTP. Zamiast używać w komunikacji klient-serwer niezaszyfrowanego tekstu, szyfruje go za pomocą protokołu SSL. Zapobiega to przechwytywaniu i zmienianiu przesyłanych danych.
HTTPS działa domyślnie na porcie nr 443 w protokole TCP.

FTP (File Transfer Protocol) – protokół transferu plików – protokół komunikacyjny typu klient-serwer wykorzystujący protokół TCP według modelu TCP/IP (krótko: połączenie TCP), umożliwiający dwukierunkowy transfer plików w układzie serwer FTP – klient FTP.

SMTP (Simple Mail Transfer Protocol) – protokół komunikacyjny opisujący sposób przekazywania poczty elektronicznej w Internecie

POP (Post Office Protocol) - 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.

IPX/SPX (ang. Internetwork Packet EXchange/Sequential Packet EXchange) – zestaw protokołów sieciowych firmy Novell (protokół warstwy sieciowej IPX i warstwy transportowej SPX). Użytkowany w różnych sieciach lokalnych (od PC LAN do sieci branżowych). Rozwiązanie to jako implementacja protokołów XNS (ang. Xerox Network Service) warstwy transportu i sieciowej dostępne jest w systemach: NetWare, MS-DOS, MS Windows i OS/2. Obecnie protokoły te są wycofywane i zastępowane zestawem protokołów TCP/IP.

Źródła:

http://pl.wikipedia.org/wiki/Hypertext_Transfer_Protocol
http://pl.wikipedia.org/wiki/Model_TCP/IP#Warstwa_aplikacji
http://pl.wikipedia.org/wiki/HTTP