**PROTOKOŁY INTERNETOWE**

Protokół stanowi zestaw zasad i standardów, które umożliwiają komunikację pomiędzy komputerami w sieci. Protokół internetowy jest to podzbiór protokołów komunikacyjnych, mający zastosowanie w środowisku Internetu.

Protokół ARP (Address Resolution Protocol) na styku między warstwą internetową i warstwą dostępu do sieci, pozwala na ustalenie adresu sprzętowego MAC hosta, gdy dany jest adres warstwy sieciowej IP. Protokół odwrotny RARP (Reverse Address Resolution Protocol) pozwala na ustalenie adresu IP na podstawie adresu fizycznego MAC.

DHCP (Dynamic Host Configuration Protocol — protokół dynamicznego konfigurowania węzłów) to standardowy protokół warstwy sieciowej przydzielający adresy IP poszczególnym komputerom. Przydział adresów IP jest realizowany poprzez serwer DHCP, który obsługuje daną podsieć.

Protokół warstwy sieciowej ICMP (Internet Control Message Protocol) umożliwia przesyłanie między komputerami lub routerami informacji o błędach występujących w funkcjonowaniu sieci IP. Najczęściej używanymi poleceniami korzystającymi w protokołu ICMP są ping i tracert.

IP (Internet Protocol – Protokół IP) to protokół komunikacyjny działający w warstwie sieciowej modelu OSI lub internetowej stosu TCP/IP. Protokół IP jest odpowiedzialny za przesyłanie pakietów między użytkownikami sieci. Jest protokołem bezpołączeniowym, co oznacza, że w trakcie transmisji nie sprawdza się poprawności pakietów przesyłanych przez sieć.

Protokół TCP (Transmission Control Protocol) działa w warstwie transportowej w trybie połączeniowym. Korzystanie z trybu połączeniowego umożliwia zagwarantowanie dostarczenia danych do odbiorcy. Połączenia TCP są połączeniami wirtualnymi, rozpoznawanymi po adresach i portach urządzeń docelowych i źródłowych. Aplikacje, w których jest wykorzystywany protokół TCP to: http, FTP, SSH, IMAP, SMTP, POP3.

Protokół UDP (User Datagram Protocol) działa w warstwie transportowej w trybie bezpołączeniowym. Protokół ten nie gwarantuje dostarczenia danych do odbiorcy. Protokół jest wykorzystywany do szybkiego przesyłania danych w niezawodnych sieciach.

DNS (Domain Name Service) to protokół warstwy aplikacji obsługujący system nazywania domen. Umożliwia on nadawanie nazw domenowych — które są zrozumiałe i łatwe do zapamiętania dla człowieka — tłumacząc je na adresy IP. Protokół DNS posługuje się do komunikacji serwer-klient głównie protokołem UDP, serwer pracuje na porcie numer 53.

Protokół NetBEUI (NetBIOS Extended User Interface) jest małym, ale wydajnym protokołem komunikacyjnym (warstwa sesji). Nie wymaga wprowadzania żadnych informacji podczas konfiguracji, a stacje wyszukują obecne w sieci komputery za pomocą komunikatów rozgłoszeniowych. Jego zastosowanie ogranicza się do sieci lokalnych, w których pracują komputery wykorzystujące systemy operacyjne firmy Microsoft. Protokół ten do identyfikowania komputerów w sieci używa ich nazw i nie umożliwia wyznaczania tras.

FTP (File Transfer Protocol — protokół transferu plików) to protokół warstwy aplikacji typu klient-serwer, który umożliwia przesyłanie plików z serwera i na serwer poprzez sieć TCP/IP. Do komunikacji wykorzystywane są dwa połączenia TCP. Jedno z nich jest połączeniem kontrolnym, za pomocą którego przesyłane są polecenia do serwera, drugie służy do transmisji danych. FTP domyślnie wykorzystuje do transmisji danych port 20., natomiast do kontroli transmisji — port 21.

SFTP (Secure File Transfer Protocol — protokół bezpiecznego przesyłania plików). Przesyła on pliki z danymi z serwera i na serwer, szyfrując nie tylko dane, ale i hasło dostępu do serwera. Protokół ten zapewnia szyfrowanie połączenia, przesyłu danych oraz rozpoznawanie użytkownika.

HTTP (Hypertext Transfer Protocol — protokół przesyłania dokumentów hipertekstowych) to protokół warstwy aplikacji dla sieci WWW. Za jego pomocą przesyła się żądania udostępnienia dokumentów WWW. Zadaniem stron WWW jest publikowanie informacji, natomiast protokół HTTP umożliwia ich udostępnianie. Jest zaliczany do protokołów bezstanowych (ang. stateless), ponieważ nie zachowuje żadnych informacji o poprzednich transakcjach z klientem (po zakończeniu transakcji wszystko przepada). HTTP standardowo korzysta z portu nr 80.

HTTPS (HyperText Transfer Protocol Secure — protokół przesyłania zaszyfrowanych dokumentów hipertekstowych) różni się od zwykłego protokołu HTTP po prostu tym, że tekst w komunikacji jest szyfrowany za pomocą protokołu SSL. HTTPS korzysta z portu 443 (na którym nasłuchuje SSL).

SSL (Secure Socket Layer — protokół bezpiecznych połączeń) - protokół zapewniający integralność i poufność transmisji danych oraz uwierzytelnianie. Opiera się na szyfrach asymetrycznych oraz certyfikatach. Ponieważ ten protokół działa w warstwie transportu można stosować go do zabezpieczenia protokołów warstwy aplikacji.

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 jest przeznaczony do pracy offline.

SMTP (Simple Mail Transfer Protocol) to protokół komunikacyjny warstwy aplikacji opisujący sposób wysyłania poczty elektronicznej w internecie. SMTP działa najczęściej na porcie 25.

Telnet (warstwa aplikacji) jest usługą (programem) pozwalającą na zdalne połączenie się komputera (terminala) z oddalonym od niego komputerem (serwerem) przy użyciu sieci. Wykorzystuje do tego celu protokół TCP/IP oraz standardowo przypisany port 23. Telnet umożliwia zatem użytkownikowi ustanowienie zdalnej sesji na serwerze.

SSH (secure shell — bezpieczna powłoka) jest następcą protokołu telnet (warstwa aplikacji). SSH, podobnie jak telnet, służy do łączenia się ze zdalnym komputerem (terminalem). Jednakże SSH zapewnia szyfrowanie oraz umożliwia rozpoznawanie użytkownika. Zazwyczaj SSH korzysta z portu 22.