

## Porty protokołów i gniazda w komunikacji sieciowej

### Cel stosowania portów protokołów

Łączenie danych pochodzących z różnych źródeł w pojedynczy strumień danych określa się mianem multipleksingu. Protokół internetowy (IP) musi zdemultipleksować dane przychodzące z Internetu. W tym celu IP oznacza protokoły transportowe numerami. Z kolei same **protokoły transportowe wykorzystują numery portów do identyfikacji aplikacji**.

### Pojęcia gniazda

**Kombinacja adresu IP i numeru portu nosi nazwę gniazda.** W ten sposób możliwa jest jednoznaczna identyfikacja pojedynczego procesu sieciowego w całym Internecie. Zapis wygląda następująco: **adres IP:numer portu**, na przykład 62.96.227.70:80. Dwa gniazda definiują połączenie - jedno dla komputera-nadawcy, drugie dla odbiorcy.

TCP i UDP mogą nadawać te same numery portów. Dopiero kombinacja protokołu i numeru portu jest jednoznaczna. Tak więc port numer 53 w protokole TCP nie jest identyczny z portem numer 53 w protokole UDP.

### Rodzaje portów

Do dyspozycji jest ogółem **65 535** portów TCP i UDP. Aby zachować nad nimi kontrolę, a także by móc przydzielać aplikacjom stałe numery, podzielono je na trzy grupy.

1. **Dobrze znane porty** (*well known ports*) - zarezerwowane, standardowe numery portów od 1 do 1023. Ułatwiają nawiązanie połączenia, ponieważ zarówno nadawca, jak i odbiorca z góry wiedzą, że dane muszą być przesłane dla określonego procesu pod określony numer portu.

Dobrze znane porty umożliwiają klientom nawiązywanie połączeń z serwerami bez dodatkowej konfiguracji. Zarządzaniem tymi portami zajmuje się Internet Assigned Numbers Authority (IANA). Listę aktualnie przydzielonych numerów portów można znaleźć pod adresem [www.iana.org/assignments/port-numbers](http://www.iana.org/assignments/port-numbers). Do roku 1992 dobrze znane porty ograniczały się do zakresu 1 do 255. Porty o numerach od 256 do 1023 były stosowane do usług uniksowych.

2. **Zarejestrowane porty** (*registered ports*) - porty o numerach od 1024 do 49.151 przewidziane są dla usług, które zwyczajowo korzystają z określonych portów. Przykładem może być port 3128, często wykorzystywany przez serwery proxy jako alternatywny port HTTP.
3. **Porty przydzielane dynamicznie** (*dynamically allocated ports, również ephemeral ports*) - jak wskazuje nazwa, zawsze przydzielane dynamicznie. Są to porty o numerach od 49.152 do 65.535. Każdy klient może korzystać z nich tak długo, jak długo

kombinacja protokołu transportowego, adresu IP i numeru portu jest jednoznaczna. Proces, który potrzebuje dostępu do portu, żąda go od swojego hosta.

Porty TCP i UDP są potencjalnym źródłem zagrożeń. Za ich pośrednictwem robaki i trojany ingerują w systemy lokalne lub tworzą połączenia internetowe. Dlatego też zaleca się stosowanie firewalli, szczególnie w systemach windowsowych.

Wiedza o portach jest nieodzowna do konfiguracji firewalla. Należy określić, które porty mogą być wykorzystywane do połączeń wychodzących i przychodzących. Jednak często nie wiadomo, z których portów korzysta dana aplikacja. Nieraz dobrze byłoby też wiedzieć, który z portów został już losowo przydzielony aplikacji na komputerze-kliencie.

W celu zdobycia tej wiedzy można się posłużyć się narzędziem Windows - **Netstat**. Niestety, jego funkcjonalność jest bardzo ograniczona. Nie podaje ono na przykład informacji o tym, jakie aplikacje używają poszczególnych połączeń.

### Dobrze znane porty i protokoły

- **20** FTP – przesyłanie danych
- **21** FTP – przesyłanie poleceń
- **22** SSH
- **23** Telnet
- **25** SMTP
- **53** DNS
- **69** TFTP
- **80** HTTP
- **110** POP3
- **143** IMAP
- **443** HTTPS (HTTP na SSL)
- **995** POP3S (POP3 na SSL)
- **3306** MySQL
- **5432** PostgreSQL