

Leksykon IP

1. Podstawy IP

- **Adres IP** – numer nadawany urządzeniu pracującemu w sieci TCP/IP, dzięki któremu jest ono jednoznacznie identyfikowane. Adres IP w najpopularniejszej wersji czwartej zapisuje się w postaci czterech cyfr oddzielonych kropkami, np. 192.168.15.100. Każde urządzenie w danej sieci musi mieć inny adres IP.
- **Maska podsieci** – numer określający, która część adresu IP jest adresem sieci (część wspólna dla wszystkich urządzeń w sieci), a która jest adresem urządzenia (inne wartości dla każdego urządzenia w danej sieci). W najprostszym przypadku, pola adresu IP, którym w masce odpowiada liczba 255, są częścią adresu sieci, a pozostałe pola są adresem urządzenia. Np. dla adresu IP 192.168.15.100 i maski 255.255.255.0 adresem sieci jest 192.168.15.0, a adresem urządzenia jest 0.0.0.100. Wynika z tego, że wszystkie urządzenia w danej sieci muszą mieć ustawioną taką samą maskę, aby adres sieci był taki sam.
- **Brama** – urządzenie pracujące w danej sieci, które ma połączenie również z inną siecią. W sieciach TCP/IP jest to najczęściej jeden ruter, który zapewnia łączność z innymi podsieciami lub Internetem. Adres bramy jest parametrem konfiguracji urządzeń sieciowych, bez którego nie będzie możliwości komunikacji z innymi sieciami. Nie jest niezbędny, jeżeli cała komunikacja ma odbywać się w jednej sieci.
- **Adres MAC (sprzętowy, fizyczny)** – 48-bitowy, niepowtarzalny numer przydzielany przez producenta każdej karcie sieciowej. Jest on zapisywany w postaci sześciu liczb szesnastkowych, np.: 00-0C-6E-3D-5D-16.
- **IPv4, IPv6** – wersje protokołu IP, różniące się sposobem adresowania. Starsza, wciąż używana, wersja czwarta, używa do zapisania adresu 32 bitów. Adres najczęściej reprezentowany jest w postaci dziesiętnej jako cztery liczby ośmiobitowe (o wartościach od 0 do 255) oddzielone kropkami, np. 192.168.15.100. Obecnie ze względu na zbyt małą dostępną ilość adresów konieczne było utworzenie nowej wersji protokołu. IPv6 do zapisania adresu używa 128 bitów. Przedstawiany jest w postaci ośmiu liczb szesnastkowych np. 2001:0db8:0000:0000:0000:0000:1428:57ab.
- **Firewall (zapora sieciowa)** – oprogramowanie lub urządzenie sieciowe służące do zabezpieczania sieci przed atakami z zewnątrz np. z Internetu. Firewall nadzoruje ruch sieciowy i blokuje wychodzące lub przychodzące połączenia uznane za niebezpieczne.
- **PoE (Power over Ethernet)** – technologia zasilania urządzeń pracujących w sieci Ethernet za pomocą tego samego kabla, który jest używany do transmisji danych. Skrętka kat. 3 (lub wyższa) posiada nieużywaną parę przewodów, która może być wykorzystana do przesyłu energii elektrycznej. Napięcie w zależności od implementacji wynosi od 25 do 60 V, a maksymalny prąd to 400 mA.
- **Adres publiczny** – adres IP, który jest widziany bezpośrednio z sieci Internet. Dostęp do urządzenia o adresie publicznym jest możliwy z dowolnego miejsca.
- **Adres prywatny** – adres IP przydzielany wewnątrz podsieci, niedostępny i niewidoczny z zewnątrz. Adres ten można wybrać z następującej puli prywatnych adresów IP:
 - 10.0.0.0 – 10.255.255.255 (maska podsieci 255.0.0.0)
 - 192.168.0.0 – 192.168.255.255 (maska podsieci 255.255.0.0)

2. Rodzaje sieci IP

- **LAN** – ang. Local Area Network – sieć lokalna, najczęściej ograniczona do jednego budynku lub małej grupy budynków. Charakteryzuje się małą rozległością i dużą prędkością przesyłania danych, natomiast nie ma potrzeby dzierżawienia łączy telekomunikacyjnych. Wśród wielu standardów sieci lokalnych najpopularniejsze to Ethernet i Wi-Fi.
- **WAN** – ang. Wide Area Network – sieć rozległa, obejmująca obszar większy niż miasto. Przykładem sieci WAN jest Internet. Sieć taka wykorzystuje najczęściej łącza dzierżawione od operatorów telekomunikacyjnych i korzysta z ich usług w celu zestawiania połączeń.
- **Internet** – globalna sieć informatyczna
- **Ethernet** – standard budowy przewodowych sieci lokalnych. W najpopularniejszej wersji 100Base-TX o prędkości 100 Mbit/s do transmisji używany jest kabel miedziany – skrętka, dawniej stosowano także kable koncentryczne, a najszybsze obecnie wersje wykorzystują światłowody.
- **Wi-Fi** – standard budowy sieci bezprzewodowych, stosowany także do budowy sieci lokalnych. Najpopularniejsza wersja 802.11g osiąga prędkość 54 Mbit/s.
- **WiMAX** – technologia bezprzewodowego dostępu do Internetu o zasięgu 3-5 km w przypadku sygnału odbitego lub 10-30 km w przypadku bezpośredniej widoczności. Maksymalna przepustowość w praktyce wynosi do 4 Mbit/s.

3. Elementy sieci IP

Sieć może składać się tylko z dwóch komputerów wyposażonych w karty sieciowe, ale może być również tak złożona jak Internet. Zbudowany jest on z tysięcy podsieci połączonych ze sobą takimi urządzeniami jak koncentratory, mosty, przełączniki i rutery. Większość domowych sieci podłączona jest do Internetu za pomocą modemu.

- **Modem** – jest urządzeniem które tłumaczy dane cyfrowe na postać, która nadaje się do wysłania przez określone medium transmisyjne. Tym medium może być linia telefoniczna, sieć telewizji kablowej lub fale radiowe. Dzięki modemowi użytkownik może połączyć się z siecią dostawcy usług internetowych.
- **Koncentrator (Hub)** – jest urządzeniem sieciowym, którego zadanie polega na rozsyłaniu odebranego sygnału na wszystkie porty. Dzięki prostej budowie koncentrator jest bardzo szybki i tani, ale jego stosowanie powoduje częstsze powstawanie kolizji w sieci.
- **Przełącznik (Switch)** – tak jak koncentrator ma za zadania rozesłanie sygnału, różni się jednak tym, że potrafią wysyłać dane tylko na te porty, do których podłączony jest odbiorca. Dzięki temu koncentratory ograniczają liczbę kolizji w sieci.
- **Most (Bridge)** – zastosowaniem mostów jest łączenie segmentów sieci. Dzięki temu zmniejsza się obciążenie oraz liczba kolizji, ponieważ pakiety nigdy nie trafiają do segmentu sieci, do którego trafić nie powinny.

4. Protokoły komunikacyjne

- **HTTP** – protokół komunikacyjny używany powszechnie w sieci WWW. Zasada jego działania jest bardzo prosta: przeglądarka wysyła do serwera zapytanie, a serwer odpowiada odsyłając zawartość strony internetowej. Może się zdarzyć, że strona jest zabezpieczona przed niepowołanym dostępem, w tym przypadku serwer zażąda podania hasła.
- **FTP** – protokół komunikacyjny służący do dwukierunkowego przesyłania plików. Pliki przechowywane są na serwerze, a dostęp do nich może być chroniony hasłem. Serwery FTP pracują najczęściej na porcie TCP o numerze 21.
- **SMTP** – protokół wysyłania poczty elektronicznej. Wiadomość wysyłana jest najpierw na serwer, pracujący najczęściej na porcie TCP numer 25, a on przekazuje ją odbiorcy. W celu nawiązania połączenia z serwerem może być konieczne podanie nazwy użytkownika i hasła.
- **HTTPS** – bezpieczny protokół komunikacyjny, odmiana protokołu HTTP. Protokół ten jest zazwyczaj używany podczas połączeń ze stronami internetowymi banków, w celu zabezpieczenia wymiany poufnych informacji.
- **Unicast** – rodzaj połączenia, w którym pakiety wysyłane od jednego nadawcy trafiają do dokładnie jednego odbiorcy. W przypadku gdy nadawca komunikuje się z większą liczbą odbiorców, konieczne jest wysłanie oddzielnego pakietu do każdego z nich. W przypadku, gdy każdy z odbiorców żąda tych samych danych, metoda ta jest nieefektywna, ponieważ niepotrzebnie zwiększa ruch w sieci.
- **Multicast** – rodzaj połączenia, w którym pakiet wysyłany od jednego nadawcy jest powielany i rozsyłany do każdego z odbiorców, którzy zasygnalizowali wcześniej chęć odbierania tych danych. Rozwiązanie takie sprawdza się w przypadku, gdy każdy z odbiorców żąda tych samych danych (np. jednoczesny podgląd obrazu z kamery IP z wielu miejsc).
- **Broadcast** – rodzaj połączenia, w którym pakiet od jednego nadawcy jest powielany i trafia do wszystkich odbiorców. Od multICASTU różni się tym, że dane są wysyłane bez względu na to, czy odbiorca sygnalizował chęć ich odbierania.
- **TCP** – protokół komunikacyjny, który zapewnia bezbłędną wymianę danych między dwoma urządzeniami. Za pomocą tego protokołu nawiązywane jest połączenie, a wymiana danych realizowana jest w taki sposób, aby żadne informacje nie zostały zagubione i docierały do odbiorcy w odpowiedniej kolejności. Jest on wykorzystywany razem z IP przez protokoły znajdujące się wyżej w hierarchii, a adres IP wraz z numerem portu TCP określają urządzenie oraz usługę (aplikację, program) na nim uruchomioną, z którą ma zostać nawiązane połączenie. Domyślne numery portów TCP niektórych usług: HTTP – port 80, FTP – port 21, SMTP – port 25.
- **UDP** – protokół komunikacyjny, w którym nawiązanie połączenia nie jest wymagane, a informacja jest wysyłana do odbiorcy bez weryfikacji poprawności jej odbioru. Może się więc zdarzyć, że pakiet zostanie po drodze odrzucony i nie trafi do miejsca przeznaczenia. Oprócz tej oczywistej wady protokół ten ma też kilka zalet: jest przede wszystkim szybki oraz umożliwia transmisję danych do kilku odbiorców jednocześnie (patrz Multicast), dlatego często jest wykorzystywany do transmisji dźwięku lub obrazu w sieciach IP. Protokół UDP wymaga podania numeru portu, określającego usługę (aplikację, program), z którą ma być przeprowadzana wymiana pakietów.
- **DHCP** – protokół komunikacyjny, który umożliwia pobranie z serwera informacji o konfiguracji sieciowej: adresu IP, maski sieci, bramy i adresów serwerów DNS. Dzięki temu użytkownik podłączający urządzenie do sieci, w której jest uruchomiony serwer DHCP (najczęściej ruter posiadający taką funkcjonalność), nie musi wprowadzać żadnych parametrów.

5. NAT

Proces przesyłania pakietów danych przez ruter, związany ze zmianą adresów i numerów portów źródłowych lub docelowych (ang. Network Address Translation). W przypadku, gdy dysponuje się tylko jednym przydzielonym adresem IP, a trzeba podłączyć do Internetu więcej komputerów, należy do tego celu użyć rutera. Dzięki niemu, przy wykorzystaniu jednego zewnętrznego adresu IP, umożliwia się dostęp do Internetu wszystkim komputerom w sieci lokalnej. Podczas komunikacji ze światem zewnętrznym w pakietach wychodzących adresy IP komputerów w sieci lokalnej zamieniane są na adres zewnętrzny rutera, natomiast pakiety przychodzące na zewnętrzny adres IP rutera mają zamieniane adresy na wewnętrzne, zgodne z komputerem do którego mają trafić. Podobnie dzieje się z numerami portów.

Proces ten odbywa się automatycznie, ale działa tylko w przypadku połączeń wychodzących. W celu nawiązania połączenia z zewnątrz z urządzeniem w sieci lokalnej, trzeba ręcznie ustawić, na który adres wewnętrzny mają trafiać pakiety. Rozwiązanie takie nazywa się przekierowywaniem portów. Ręcznie definiowany jest wtedy numer portu zewnętrznego w routerze, z którego pakiety będą trafiały na określony adres IP w sieci wewnętrznej. Najczęściej w routerze można ustalić kilka numerów portów i przydzielić im różne wewnętrzne numery IP, dzięki czemu możliwe jest nawiązanie połączenia z każdym urządzeniem w sieci prywatnej.

6. DDNS

Usługa tzw. Dynamicznego DNS, czyli przydzielania nazw systemu DNS zmiennym publicznym adresom IP. Dzięki temu zdalny dostęp do urządzenia (rutera, komputera, rejestratora), którego IP jest przydzielane tymczasowo, jest możliwy poprzez jego stałą nazwę DNS. Usługa taka jest za darmo udostępniana przez serwis www.dyndns.com. Każdorazowo, po przydzieleniu nowego adresu IP, serwer Dynamicznego DNS jest o tej zmianie powiadamiany i od tej pory połączenia z urządzeniem o określonej nazwie DNS będą kierowane na nowy adres IP.