Lokalne sieci komputerowe

http://pkosla.kis.p.lodz.pl/fl/sk1.pdf

Tomasz Fitzermann

tomax13@wp.pl

Rozkład materiału

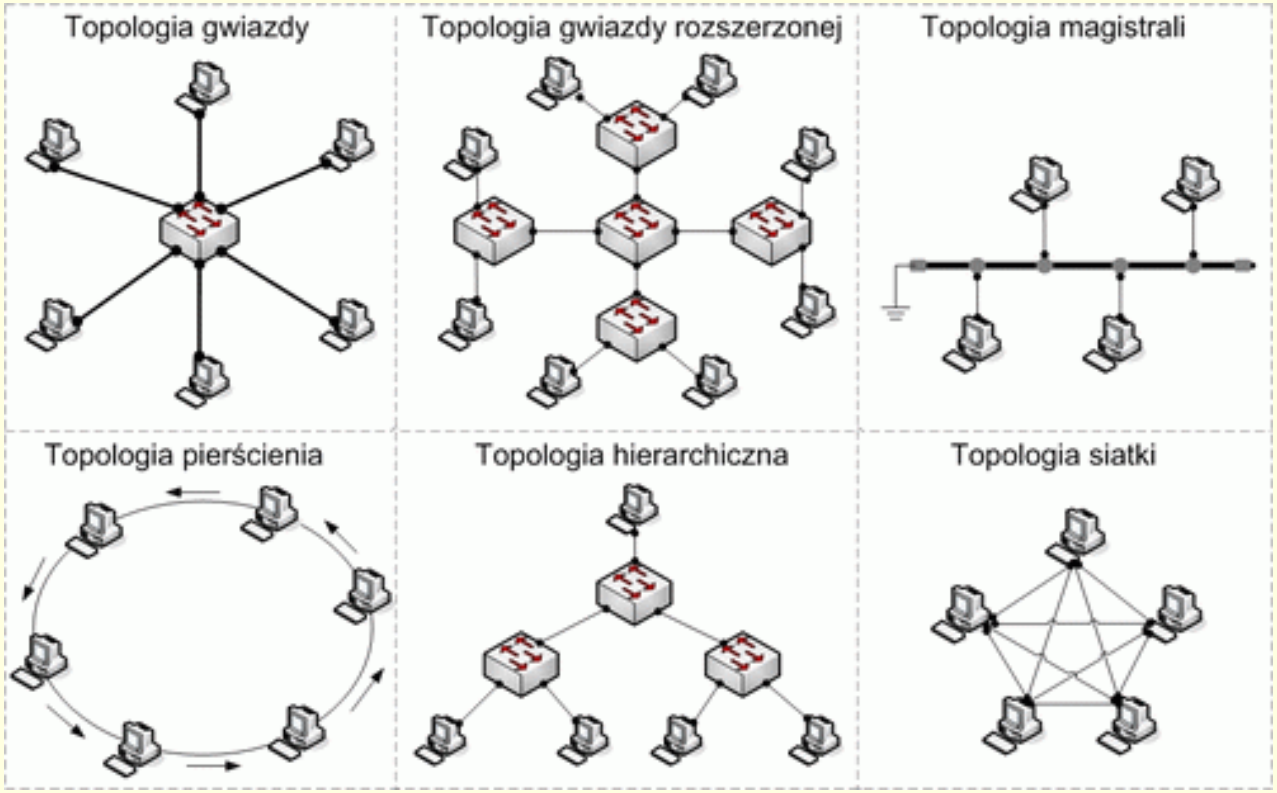
- Podstawy sieci komputerowych (12) – topologie, protokoły, programy sieciowe
- Standardy i urządzenia sieciowe (12) – standardy i urządzenia sieciowe
- Adresacja IP (12) – maski, adresy
- Sieci przewodowe LAN (15) – Ethernet 802.3
- Sieci bezprzewodowe WLAN (15) – WIFI 802.11
- Sieci wirtualne VLAN i VPN (12)
- Routing (9) – Algorytmy routingu, routery
- Usługi sieciowe (9) - Usługi sieciowe i serwerowe

Temat: Pojęcia podstawowe

- **Sieć komputerowa** – zbiór komputerów i innych urządzeń połączonych ze sobą kanałami komunikacyjnymi oraz oprogramowanie wykorzystywane do przekazywania informacji w tej sieci.
- **Intersieć** - to środowisko sprzętowo-programowe zapewniające jednolite usługi w niejednorodnym środowisku sieciowym („różne technologie sieciowe”)
- **LAN** (ang. Local Area Network) – Lokalna sieć komputerowa. Sieć komputerowa łącząca komputery na określonym obszarze (blok, szkoła, laboratorium, biuro)
- **MAN** (ang. Metropolitan Area Network) – duża sieć komputerowa, której zasięg obejmuje aglomerację lub miasto.
- **WAN** (ang. Wide Area Network) - rozległa sieć komputerowa
- **Protokół** - jest zbiorem reguł definiujących sposób przesyłania danych między aplikacjami/urządzeniami. Reguły te określają między innymi format przesyłanych danych. Przykłady protokołów: Token Ring, IP, TCP, FTP.
- **Aplikacje sieciowe** - program komputerowy, który pracuje na serwerze i komunikuje się poprzez sieć komputerową z hostem użytkownika komputera. Przykłady: poczta elektroniczna, transmisja danych, usługi terminalowe, serwisy informacyjne, synchronizacja czasu, dostęp do informacji o użytkownikach.

Topologie sieciowe

Topologia sieci komputerowej – model układu połączeń różnych elementów sieci komputerowej. Określenie topologia sieci może odnosić się do konstrukcji fizycznej albo logicznej sieci.



Topologie logiczne

Topologia logiczna opisuje sposoby komunikowania się hostów za pomocą urządzeń topologii fizycznej. Topologię logiczną można podzielić na:

- **Topologia rozgłaszania** – polega na tym, że host wysyła dane do wszystkich hostów podłączonych do medium. Kolejność korzystania z medium wg reguły kto pierwszy wyśle, pierwszy zostanie obsłużony. Przykładem są tutaj sieci Ethernet.

- **Topologia przekazywania tokenu** (żetonu) – polega na kontrolowaniu dostępu do sieci poprzez przekazywanie tokenu. Host, który w danym momencie posiada token może skorzystać z medium. W przypadku gdy nie ma zadań przekazuje token kolejnemu hostowi i cykl się powtarza. Przykładem są tutaj sieci Token Ring.

Przełączanie pakietów

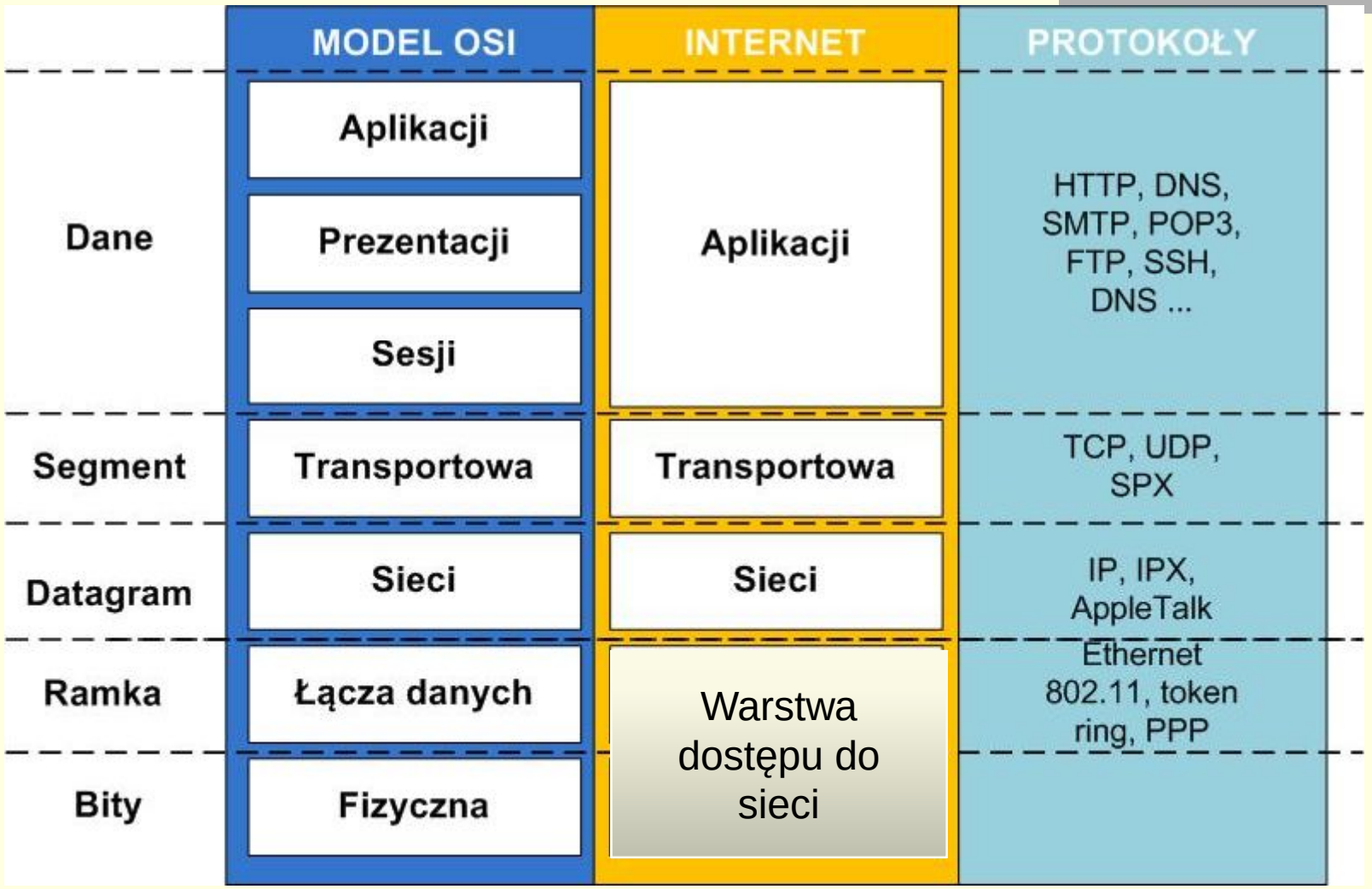
Pierwsze sieci do utworzenia kanału komunikacyjnego wykorzystywały fizyczne połączenie urządzeń końcowych za pomocą pary przewodów.

Komutacja, przełączanie pakietów

- W telekomunikacji sposób transmisji danych polegający na dzieleniu strumienia danych na kawałki (pakiety), a następnie wysyłaniu ich za pomocą łączy komunikacyjnych pomiędzy węzłami sieci.
- Do pakietów dołącza się identyfikator odbiorcy i nadawcy.
- Każdy pakiet podlega osobnemu trasowaniu – może podążać do celu ścieżką niezależną od wcześniejszych pakietów.
- Dane pochodzące od wielu użytkowników i usług są przekazywane w ramach wspólnych połączeń sieciowych.

- **Powody przesyłania danych w pakietach:**
  - odporność na uszkodzenia sieci (uszkodzone urządzenia są po prostu omijane)
  - możliwość docierania pakietów w przypadkowej kolejności (ze względu na różne ścieżki transmisji)
  - opóźnienia związane z buforowaniem pakietów w routerach
  - duża przepustowość efektywna sieci
  - wysyłanie danych w pakietach umożliwia dzielenie dostępu do łącza pomiędzy wieloma komputerami (jeden komputer nie blokuje łącza)
  - w przypadku ewentualnego błędu transmisji powtórzyć należy transmisję tylko wadliwie przesłanego pakietu, a nie całego komunikatu

Modele odniesienia OSI, TCP/IP



Protokół IP

- **IP** (*ang. Internet Protocol*) – protokół komunikacyjny warstwy sieciowej modelu OSI (warstwy internetu w modelu TCP/IP). Umożliwia trasowanie, określanie ścieżek którymi wędrują pakiety (rutery, algorytmy rutingu). Aby zapewnić pomyślność komunikacji w tym protokole konieczne jest przyporządkowanie adresów IP interfejsom sieciowym urządzeń.

+	Bity 0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Wersja	Długość nagłówka	Typ usługi	Całkowita długość	
32	Numer identyfikacyjny			Flagi	Kontrola przesunięcia
64	Czas życia pakietu (TTL)		Protokół warstwy wyższej	Suma kontrolna nagłówka	
96	Adres źródłowy IP				
128	Adres docelowy IP				
160	Opcje IP				Uzupełnienie
192	Dane				

Protokoły warstwy sieciowej

- **ARP** (*ang. Adres Resolution Protocol*) - informuje warstwę trzecią o adresie sprzętowym urządzenia (na podstawie IP → pyta o MAC)
- **RARP** (*ang. Reverse Adres Resolution Protocol*) - umożliwia wskazanie adresu IP urządzenia przy znajomości adresu sprzętowego (na podstawie MAC → pyta o IP).
- **ICMP** (*ang. Internet Control Message Protocol*) – internetowy protokół komunikatów kontrolnych. Protokół warstwy sieciowej modelu OSI, wykorzystywany w diagnostyce sieci oraz trasowaniu. Pełni przede wszystkim funkcję kontroli transmisji w sieci. Jest wykorzystywany w programach **ping** oraz **traceroute**.
- **IGMP** (*ang. Internet Group Management Protocol*) – jeden z rodziny protokołów TCP/IP. IGMP służy do zarządzania grupami multicastowymi w sieciach opartych na protokole IP. Komputery wykorzystują komunikaty IGMP do powiadamiania routerów w swojej sieci o chęci przyłączenia się do lub odejścia z określonej grupy multicastowej.

Protokoły warstwy transportowej

Warstwa transportowa jest odpowiedzialna za:

- prawidłowy przebieg komunikacji oraz jej niezawodność.
- sposób segmentacji danych (zasady dzielenia ich na możliwe do zarządzania części) oraz późniejszego ich scalania,
- identyfikuje dane pochodzące z różnych aplikacji (poprzez numery portów).

TCP (*ang. Transmission Control Protocol*) – Protokół sterowania transmisją. Niezawodny, strumieniowy protokół komunikacyjny stosowany do przesyłania danych między procesami uruchomionymi na różnych maszynach, będący częścią szeroko wykorzystywanego obecnie stosu TCP/IP. TCP jest protokołem połączeniowym. Z tego protokołu korzystają wszystkie aplikacje wymagające niezawodnej transmisji np. FTP.

UDP (*ang. User Datagram Protocol*) – jeden z protokołów internetowych. UDP stosowany jest w warstwie transportowej modelu OSI. Nie gwarantuje dostarczenia datagramu. 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. Aplikacje które używają UDP to DNS, VoIP.

UDP vs TCP

TCP Segment Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset	Res	Flags	Window Size
128	Header and Data Checksum		Urgent Pointer	
160...	Options			

UDP Datagram Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Length		Header and Data Checksum	

Protokoły warstwy aplikacji

- **FTP** (*ang. File Transfer Protocol*) – protokół przesyłania plików przez sieć
- **DNS** (*ang. Domain Name Service*) – system serwerów, protokół komunikacyjny oraz usługa obsługująca rozproszoną bazę danych adresów sieciowych. Pozwala na zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową. Dzięki DNS nazwa mnemoniczna, np. pl.wikipedia.org jest tłumaczona na odpowiadający jej adres IP, czyli 91.198.174.192.
- **HTTP** (*ang. Hypertext Transfer Protocol*) – protokół przesyłania dokumentów hipertekstowych to protokół sieci WWW (ang. World Wide Web).
- **HTTPS** (*ang. Hypertext Transfer Protocol Secure*) – szyfrowana wersja protokołu HTTP. W przeciwieństwie do komunikacji niezaszyfrowanego tekstu w HTTP klient-serwer, HTTPS szyfrował dane przy pomocy protokołu SSL, natomiast obecnie używany jest do tego celu protokół TLS. Zapobiega to przechwytywaniu i zmienianiu przesyłanych danych.
- **NTP** (*ang. Network Time Protocol*)
- **SNMP** (*ang. Simple Network Management Protocol*)

  - prosty protokół zarządzania urządzeniami w sieci

TCP		UDP	
FTP	20,21	DNS	53
SSH	22	BooTPS/DHCP	67
Telnet	23	TFTP	69
SMTP	25	SNMP	161
DNS	53		
HTTP	80		
POP3	110		
NTP	123		
IMAP4	143		
HTTPS	443		

numery portów

Protokoły warstwy aplikacji

Terminalowe (tekstowe) protokoły połączenia ze zdalnymi komputerami (hostami).

- **Telnet** - usługę telnet czasami wykorzystują (przełączniki, routery) w celu ułatwienia zdalnej konfiguracji. Użytkownik za pomocą polecenia telnet oraz podaniu adresu danego urządzenia loguje się do niego i w trybie znakowym wykonuje konfiguracje VLAN-ów, adresów IP, NAT-a itd. Połączenie tego typu nie jest szyfrowane, a więc istnieje możliwość przechwycenia przesyłanych danych. Z tego powodu częściej stosuje się następcę Telnetu, czyli SSH.
- **SSH** (*ang. Secure SHell*) – nastepca Telnet (szyfrowany → bezpieczny)

Poczta

- **SMTP** (*ang. Simple Mailt Transfer Protocol*) - – protokół komunikacyjny opisujący sposób przekazywania poczty elektronicznej w Internecie.
- **POP3** (ang. Post Office Protocol) – protokół internetowy z warstwy aplikacji pozwalający na odbiór poczty elektronicznej.
- **IMAP4** (*ang. Internet Message Access Protocol*) - protokół odbioru poczty

TCP		UDP	
FTP	20,21	DNS	53
SSH	22	BooTPS/DHCP	67
Telnet	23	TFTP	69
SMTP	25	SNMP	161
DNS	53		
HTTP	80		
POP3	110		
NTP	123		
IMAP4	143		
HTTPS	443		

numery portów

Sieci rozległe - WAN

Sieć **WAN** (*ang. Wide Area Network*) – rozległa sieć komputerowa znajdująca się na obszarze wykraczającym poza miasto, kraj, kontynent.

- Korzystają z usług operatorów telekomunikacyjnych, np. Netia, TP S.A.
- Wykorzystują różne odmiany transmisji szeregowej.
- Sieć WAN działa w warstwie fizycznej oraz warstwie łącza danych modelu odniesienia OSI.
- Łączy ona ze sobą sieci lokalne, które są zazwyczaj rozproszone na dużych obszarach geograficznych.
- Umożliwiają wymianę ramek i pakietów danych pomiędzy routerami i przełącznikami oraz obsługiwanymi sieciami LAN.

Protokoły WAN, techniki przełącznia:

- komutacja kanałów (*ang. circuit-switched*) – **PPP, ISDN**
- łącza dzierżawione (trwałe, dedykowane) (*ang. dedicated-switched*)
- komutacja komórek (*ang. cell-switched*) – **ATM, SMDS**
- komutacja pakietów (*ang. packet-switched*) – **Frame Relay, X.25**.

ISP (*ang. Internet Service Provider*) – dostawca usług internetowych poprzez linie telefoniczne, instalację telewizji kablowej.

ADSL (*ang. Asymmetric Digital Subscriber Line*) – asymetryczna cyfrowa linia abonencka, technologia umożliwiająca szerokopasmowy asymetryczny dostęp do sieci teleinformatycznych. Asymetria polega tutaj na tym, iż przesyłanie danych z sieci do użytkownika jest szybsze niż w drugą stronę.

DSL (*ang. Digital Subscriber Line*) – cyfrowa linia abonencka, technologia cyfrowego szerokopasmowego dostępu do Internetu[1]. Standardowa maksymalna prędkość odbierania danych waha się od 8Mb/s do 52 Mb/s oraz od 1Mb/s do 5Mb/s dla prędkości wysyłania w zależności od stosowanej w danym kraju technologii DSL.

IEEE 802

IEEE 802 – grupa standardów IEEE stosowanych w lokalnych sieciach komputerowych (LAN) oraz miejskich sieciach komputerowych (MAN) przesyłających dane w systemie pakietowym. Usługi i protokoły wyszczególnione w IEEE 802 nawiązują do warstwy fizycznej i łącza danych modelu OSI.

Popularne standardy:

- IEEE 802.1 - higher layer LAN protocols (802.1Q wirtualna sieć lokalna)
- IEEE 802.3 - Ethernet
- IEEE 802.5 - Token Ring
- IEEE 802.11 - bezprzewodowa sieć lokalna (Wi-Fi certification)
- IEEE 802.15 Wireless PAN
  - IEEE 802.15.1 (Bluetooth certification)
  - IEEE 802.15.4 (ZigBee certification)
- IEEE 802.16 - Broadband Wireless Access (WiMAX certification)

IEEE 802 dzieli warstwę łącza danych na dwie podwarstwy: **LLC** i **adres MAC**.

LLC (*ang Logical Link Control)* – wyższa podwarstwa warstwy łącza danych w modelu OSI według rodziny standardów IEEE 802. Warstwa LLC jest identyczna dla różnych fizycznych mediów wymiany danych (jak np. ethernet, token ring, WLAN). Podwarstwa LLC jest przede wszystkim odpowiedzialna za:

- rozdzielanie, zwielokrotnianie danych transmitowanych przez podwarstwę MAC (podczas transmitowania) oraz łączenie ich (podczas odbierania),
- jeżeli zachodzi taka potrzeba, sterowanie przepływem, detekcję i retransmisję zgubionych pakietów.

Adres fizyczny MAC

Adres MAC (*ang. medium access control address*) – termin o dwóch znaczeniach:

- sprzętowy adres karty sieciowej Ethernet i Token Ring, unikatowy w skali światowej, nadawany przez producenta danej karty podczas produkcji.
- warstwa sterowania dostępem do medium transmisyjnego w modelu OSI

Cechy adresu MAC:

- 48-bitowy
- zapisywany jest heksadecymalnie (szesnastkowo za pomocą 12 znaków) np. 00:0A:E6:3E:FD:E1
- Pierwsze 24 bity oznaczają producenta karty sieciowej (vendor code), pozostałe 24 bity są unikatowym identyfikatorem danego egzemplarza karty.
- Można się spotkać z określeniem, że adres MAC jest 6-bajtowy. Ponieważ 1 bajt to 8 bitów, więc 6 bajtów odpowiada 48 bitom. Pierwsze 3 bajty (vendor code) oznaczają producenta, pozostałe 3 bajty oznaczają kolejny (unikatowy) egzemplarz karty.
- Nowsze karty sieciowe pozwalają na zmianę nadanego im adresu MAC. W przypadku blokowania dostępu przez ISP dla danego urządzenia za pomocą adresu MAC routery WiFi posiadają funkcję klonowania adresu MAC karty sieciowej i obejście tego ograniczenia.
- Adresy MAC wykorzystuje się np. na routerach do ograniczenia dostępu do sieci tylko urządzeń o określonych adresach fizycznych - filtrowanie adresów MAC.

Przykład:

MAC = 00:0A:E6:3E:FD:E1

- karta została wyprodukowana przez Elitegroup Computer System Co. (ECS)
- producent nadał jej numer 3E:FD:E1.

Uwaga: Adres MAC karty sieciowej można odczytać za pomocą polecenia ipconfig /all

IEEE 802.3 - Ethernet

- **CSMA/CD** *(ang. Carrier Sense Multiple Access / with Collision Detection*) – protokół wielodostępu **CSMA** z badaniem stanu kanału i wykrywaniem kolizji.
- **PoE** (*ang. power over ethernet*) – standard zasilania urządzeń poprzez wolne pary skrętki.

standard	predkość	medium	uwagi
802.3a	**10BASE2** 10 Mbit/s	Cienki przewód koncentryczny	
802.3i	**10BASE-T** 10 Mbit/s	Skrętka (twisted pair)	2 pary przewodów
802.3j	**10BASE-F** 10 Mbit/s	światłowód (Fiber -Optic)	
802.3u **(Fast Ethernet)**	100 Mbit/s **100BASE-TX** **100BASE-T4** **100BASE-FX**	 skrętka kategorii >=5 skrętka kategorii >=3 światłowód	 2 pary przewodów 4 pary przewodów
802.3z **(Gigabit ethernet)**	**1000BASE-FX** 1 Gbit/s	światłówód	
802.3ab **(Gigabit ethernet)**	**1000BASE-T** 1 Gbit/s (125 MB/s)	skrętka kategorii >=5 (5e,6, 7)	4 pary (TX – 2 pary)

Uwaga: prędkości w sieciach podaje się w Mbit/s lub Mbps (mega bits per second)

Gigabit Ethernet

- Standard IEEE 802.3z zawiera 1000BASE-SX dla transmisji przez światłowód wielomodowy, 1000BASE-LX dla transmisji światłowodem jednomodowym i praktycznie wycofany z użycia 1000BASE-CX, który używa kabla koncentrycznego.

nazwa	medium	zasięg
1000BASE-CX	specjalny kabel miedziany	25 metrów
1000BASE-LX	jednomodowy, wielomodowy światłowód	5 km
1000BASE-SX	wielomodowy światłowód (długość fali: 850 nm)	500 metrów
1000BASE-LH	jednomodowy, wielomodowy światłowód (1310 nm)	10km
1000BASE-ZX	jednomodowy światłowód (1550 nm)	~ 70 km
1000BASE-LX10	jednomodowy światłowód (1310 nm)	10 km
1000BASE-BX10	jednomodowy światłowód (1490 nm w dół, 1310 nm w górę)	10 km
1000BASE-T	skrętka (CAT-5, CAT-5e, CAT-6, lub CAT-7)	100 metrów
1000BASE-TX	skrętka (CAT-6, CAT-7)	100 metrów

802.5 – Token Ring, FDDI

Token ring – metoda tworzenia sieci LAN opracowana przez firmę IBM w latach 70., dziś wypierana przez technologię Ethernetu. Szybkość przesyłania informacji w sieciach Token Ring wynosi 4 lub 16 Mb/s.

- Topologia fizyczna: dowolna, np. pierścień
- Topologia logiczna: przekazywania żetonu
- Wykorzystuje technikę przekazywania tzw. "żetonu" (ang. token passing), stosowaną również w technologii FDDI. Stacja, która ma wiadomość do nadania, czeka na wolny żeton. Kiedy go otrzyma, zmienia go na żeton zajęty i wysyła go do sieci, a zaraz za nim blok danych zwany ramką (frame). Ramka zawiera część komunikatu (lub cały komunikat), który miała wysłać stacja.
- Zastosowanie systemu sterowania dostępem do nośnika za pomocą przekazywania żetonu zapobiega wzajemnemu zakłócaniu się przesyłanych wiadomości i gwarantuje, że w danej chwili tylko jedna stacja może nadawać dane.

FDDI – *(ang. Fiber Distributed Data Interface*) – standard transmisji danych, jest oparty na technologii światłowodowej. Transfer w tych sieciach wynosi 100 Mb/s. Sieć ta zbudowana jest z dwóch pierścieni – pierścień pierwotny i pierścień zapasowy (wtórny).

- Przepustowość: **100 Mb/s**
- Metoda dostępu: **Token Passing**
- Medium transmisyjne: **kabel światłowodowy (jedno- i wielomodowy)**
- Topologia: podwójny **pierścień (ang. Dual Ring)**

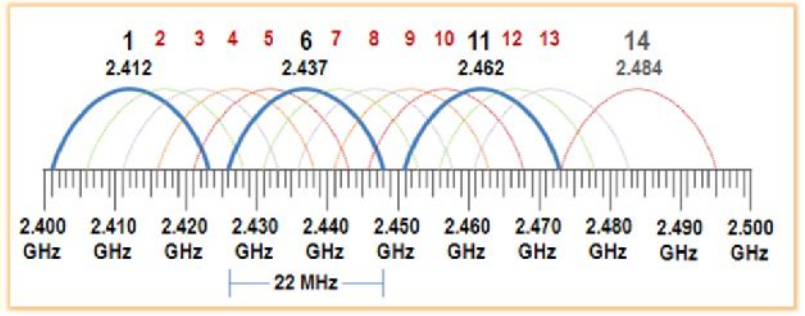
IEEE 802.11 - WiFi

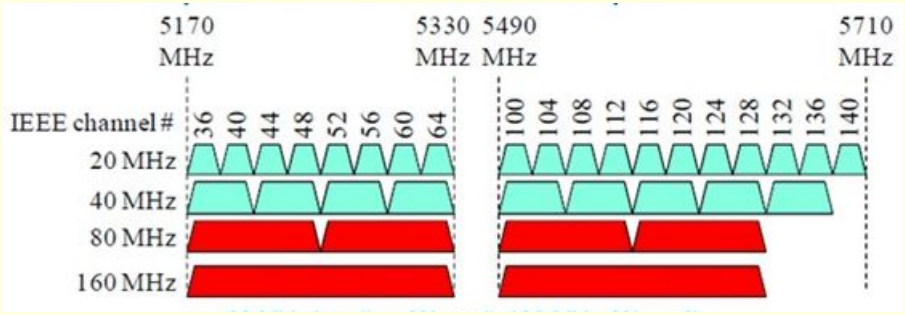
IEEE 802.11 – podgrupa standardów IEEE 802, opisujących warstwę fizyczną i podwarstwę MAC bezprzewodowych sieci lokalnych.

standard	Predkość max	zasięg	uwagi
802.11a	54 Mbit/s	35m (120m - outdoor)	f=5Ghz
802.11b	11 Mbit/s	35m (140m - outdoor)	f=2.4Ghz
802.11g	54 Mbit/s	38m (140m - outdoor)	f=2.4Ghz
802.11n	150 Mbit/s teoretycznie do 600 Mbit/s	70m (250m - outdoor)	f=2.4Ghz, 5Ghz MIMO – Multiple Input Multiple Output (kilka anten)
802.11ac	600 Mbit/s	35m	f = 5Ghz MIMO – Multiple Input Multiple Output (kilka anten)

WiFi - Częstotliwości, kanały

- Zakres częstotliwości dla sieci Wi-Fi na paśmie 2,4 GHz podzielono na 13 kanałów. Niestety, większość kanałów zachodzi na siebie, co powoduje wzajemne zakłócanie się sygnałów. W tej samej okolicy mogą więc działać co najwyżej trzy sieci wzajemnie niezakłócające się - na kanałach 1, 6 oraz 11.





- Na paśmie 5 GHz nie ma tylu zakłóceń. Zakres ten podzielony jest na 19 kanałów przeznaczonych dla sieci Wi-Fi i, co najważniejsze, nie zachodzą one na siebie. Działające na różnych kanałach sieci nawet w bardzo bliskim sąsiedztwie nie zakłócają się więc, jak ma to miejsce w wypadku częstotliwości 2,4 GHz.

Uwaga: O ile zakłócenia w sieciach 2.4 GHz są większe, a przepustowość potencjalnie mniejsza, o tyle pasmo 2.4GHz ma jeden plus - większy zasięg. Długie fale lepiej przebijają się np. przez ściany, dzięki czemu zasięg naszej sieci jest większy i nie ograniczają go tak mocno stałe obiekty.

IEEE 802.11- Koncepcje zabezpieczeń

- **Rozgłaszanie sieci SSID** (*ang. service set identifier*) przez AP (*ang. Access Point*). Miało to zabezpieczyć przed wykryciem obecności sieci, a atakujący, bez znajomości SSID, nie mógłby się do niej podłączyć.
- **Filtrowanie dostępu -** autoryzowanie tylko wybranych adresów MAC. Problem jednak ponownie tkwi we współdzielonym medium, ponieważ adresy MAC są publicznie widoczne w najniższej warstwie komunikacji sieciowej.
- **Izolacja.** Istnieją także rozwiązania mające na celu izolację użytkowników sieci pomiędzy sobą czyli tzw. „wireless client isolation". Dzięki niemu poszczególne urządzenia, już podłączone do AP, nie mogą się między sobą komunikować, jeśli AP im na to nie zezwoli.
- **Szyfrowanie.** Rozwiązania, które wymagają podania hasła w celu podłączenia się do sieci, a wszystkie dane są następnie szyfrowane. Pierwszym takim mechanizmem był WEP, który, jak się okazało, miał niestety bardzo poważne wady kryptograficzne. W związku z tym w kolejnych latach wprowadzono WPA mające naprawić słabość zabezpieczeń oferowanych przez WEP, a następnie WPA2
- **802.1X -** Zastosowanie infrastruktury bazującej na tym standardzie . W tym przypadku każdy użytkownik ma możliwość uwierzytelnić punkt dostępowy, do którego się podłącza, przesłać login i hasło w bezpieczny sposób i uzyskać indywidualny klucz do szyfrowania transmisji. W tym przypadku nie ma też możliwości instalacji fałszywego AP ani złamania szyfrowania transmisji, ponieważ możliwe jest zastosowanie wielu zaawansowanych metod uwierzytelniania użytkownika, takich jak np. klucze prywatne.

IEEE 802.11- szyfrowanie

- **WEP, 802.1X, WPA, WPA2**
- **WEP (*ang. Wired Equivalent Privacy*)** został wprowadzony w 1999 roku jako część oryginalnego standardu 802.11. Miało to na celu zapewnienie poufności na poziomie zbliżonym do sieci kablowych. Szyfrowanie występuje w dwóch wersjach z różną długością klucza RC4: 64 i 128 bitów. Tekst jawny jest szyfrowany przy pomocy operacji XOR ze strumieniem klucza, tworząc szyfrogram.
- **WPA (*ang. Wi-Fi Protected Access*).** WPA jest następcą mniej bezpiecznego standardu WEP. Pierwsza wersja profilu WPA została wprowadzona w kwietniu 2003 roku. WPA wykorzystuje protokoły **TKIP** (***ang. Temporal Key Integrity Protocol***), 802.1x oraz uwierzytelnienie EAP. WPA został wprowadzony jako standard przejściowy pomiędzy WEP a zabezpieczeniem WPA2 w celu zwiększenia bezpieczeństwa użytkowników sprzętu mającego na stałe zaimplementowany WEP bez konieczności ich wymiany. Osiągnięto to przez cykliczną zmianę klucza szyfrującego WEP, co przy odpowiedniej częstotliwości zmian uniemożliwia jego złamanie pomimo istniejących podatności.
- **WPA2** (*ang. Wi-Fi Protected Access 2 - 802.11i*). W 2006 r. algorytm WPA został oficjalnie wyparty przez WPA2. Jedną ze znaczących zmian było obowiązkowe użycie **AES (*ang. Advanced Encryption Standard*)** jako zamiennika dla TKIP (nadal zachowany w WPA2 jako rezerwowy system dla kompatybilności z WPA).

TKIP lub AES używają Pre-Shared Key (PSK) od 8 znaków do maksymalnie 63.

Uwaga: Niestety, podobnie jak w WPA, duża dziura istnieje w ataku wektorowym poprzez WPS (Wi-Fi Protected Setup), czyli tym łatwym łączeniem z siecią. Pomimo faktu, że włamanie do sieci WPA/WPA2 z włączonym WPS-em wymaga od 2 do 14 godzin ciągłej pracy komputera hakera, nie zwalnia nas to z wyłączenia WPS-a dla naszego bezpieczeństwa. Jeśli to możliwe, najlepiej, aby opcję WPS w ogóle usunąć z oprogramowania na naszym routerze/access poincie.

IEEE 802.16 - WiMAX

- **WiMAX** (*ang. World Interoperability for Microwave Access*) **IEEE 802.16** – grupa standardów bezprzewodowej, szerokopasmowej transmisji danych.
- Zasięg obszaru usługowego wynosi maksymalnie 50 km, natomiast prędkość transmisji może osiągnąć 70 Mbit/s. Określa się, iż maksymalna przepustowość technologii WiMAX zbliżona jest do 175 Mb/s.
- WiMAX stanowi alternatywę dla stałych łączy typu xDSL, zapewniając porównywalne przepływności.
- **WiMAX** jest technologią umożliwiającą budowę bezprzewodowych miejskich sieci komputerowych (MAN), a także rozległych obszarów usługowych, wykorzystywanych na przykład do świadczenia usług szerokopasmowych. Aktualnie (od wersji 802.16e) standard zapewnia mobilność dostępu.

Okablowanie strukturalne

Rodzaje okablowania:

- **10BASE2** - kabel koncentryczny (tzw. "cienki Ethernet"). Odległość 185 m, przepustowość 10 Mbit/s
- **10BASE5** - kabel koncentryczny (tzw. "gruby Ethernet"). Odległość 500 m, przepustowość 10 Mbit/s
- **10Base-T** - "skrętka", odległość 100 m, przepustowość 10 Mbit/s
- **100BASE-TX** - "skrętka", odległość 100 m, przepustowość 100 Mbit/s
- **1000BASE-T** - "skrętka", aby przesłać strumień danych z przepustowością 1000 Mbit/s przez okablowanie kategorii 5

Rodzaje okablowania wykorzystującego światłowody:

- **10BASE-F** - światłowód, przepustowość 10 Mbit/s
- **100BASE-FX** - światłowód, przepustowość 100 Mbit/s
- **1000BASE-FX/LX/SX** - światłowód, przepustowość 1000 Mbit/s

Okablowanie strukturalne

Normy okablowania strukturalnego:

- **EN 50167** „Okablowanie poziome”
- **EN 50168** „Okablowanie pionowe”
- **EN 50169** „Okablowanie krosowe i stacyjne”

Najważniejsze zalecenia wynikające z powyższych norm:

- Okablowanie poziome powinno tworzyć nieprzerwane połączenie od punktu dystrybucyjnego do punktu abonenckiego.
- Należy umieścić jeden punkt abonencki (2xRJ-45) na każde 10 m2 powierzchni biurowej.
- Na każdym piętrze budynku powinien być punkt dystrybucyjny (w przypadku małej liczby punktów abonenckich możliwe jest ich przyłączenie do punktu dystrybucyjnego na innym piętrze).
- Wszystkie kable muszą być zakończone w gniazdach abonenckich i szafach dystrybucyjnych.
- W obrębie całej sieci powinno się stosować jednakowe przewody (kable miedziane o jednakowej impedancji i średnicy, a kable światłowodowe o jednakowych włóknach).
- Rozplot kabla UTP nie powinien być większy niż 13 mm.
- Każdy element systemu powinien być czytelnie oznaczony (jednakowe oznaczenie na obu końcach kabla).
- Sieć musi posiadać pełną dokumentację.

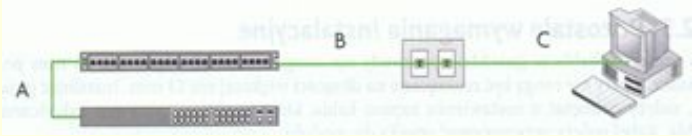
Panele krosownicze

Panel krosowniczy lub panel krosowy, panel rozdzielczy (***ang. patch panel***) – pasywny element sieci komputerowych i telekomunikacyjnych.

- Stanowi on zakończenie okablowania strukturalnego.
- Montowany jest w szafach rackowych i składa się z szeregu (najczęściej 12, 16, 24 lub 48) gniazd 8P8C.
- Z tyłu na stałe przyłączane są do niego przewody prowadzące do gniazdek 8P8C w budynku.
- Z przodu przy pomocy kabli krosowych gniazda te (a przez to i urządzenia będące na drugim końcu kabla) przyłączane są najczęściej do aktywnych urządzeń sieciowych.
- Jest to ważny element sieci strukturalnej. Zastosowanie paneli krosowniczych ułatwia zarządzanie architekturą sieci.

Kabel krosowy (*ang. patch cord*)

- krótki przewód służący do przesyłania sygnałów elektrycznych lub optycznych.
- Najczęściej jest on kojarzony z sieciami komputerowymi – skrętką. Wtedy jest to przewód połączony według specyfikacji 100BASE-T568A lub 100BASE-T568B.
- Są także kable krosowe służące do łączenia osprzętu optycznego (przewód krosowy optyczny – światłowód) oraz do łączenia osprzętu wideo.
- Zwykle kablem krosowym określa się gotowy przewód o znormalizowanej długości (1, 2, 3, 5 m) zakończony z obu stron końcówkami zgodnymi z technologią, dla której został przygotowany (skrętka RJ45, światłowód: SC, FC, ST, LC, E2000).
- Kable krosowe wykorzystywane są w szafach krosowniczych do łączenia elementów aktywnych (przełączników, routerów) i pasywnych (koncentratorów, panele krosownicze) sieci komputerowej oraz do podłączania stacji roboczych (PC) do gniazd sieci lokalnej.



Okablowanie poziome

Zalecenia dotyczące kabli w przebiegach poziomych:

- Normy zalecają stosowanie 4-parowego symetrycznego kabla STP lub UTP kategorii co najmniej 5e dla wszystkich kanałów poziomych.
- Całkowita długość kanału nie może przekroczyć 100 m.
- B<=90m (maksymalna długość przebiegu kabla poziomego pomiędzy punktem abonenckim a punktem dystrybucyjnym w panelu krosowym (patch panel).
- A <= 6m
- A+C <=10m (łączna długość kabla stacyjnego i krosowego)

Podczas układania kabla w przebiegach poziomych należy przestrzegać następujących zasad:

- kable biegnące ponad sufitem podwieszanym nie powinny być mocowane do konstrukcji sufitu;
- odległości pomiędzy punktami mocowania kabli poziomych nie powinny być większe niż 1,2 -1,5 m;
- kable wchodzące i wychodzące do/z pomieszczeń (pod kątem 90°) powinny skręcać łagodnie (minimalny promień skrętu = 8 średnic kabla);
- nie można rozdzielać par przewodów na dwa kanały komunikacyjne;
- kable, na całej długości od gniazda abonenckiego do punktu dystrybucyjnego, powinny być wolne od sztukowań, zagnieceń i nacięć lub złamań;
- kable powinny być wyprowadzane i wprowadzane z głównych tras przebiegu pod kątem 90°, zaś promień ich zagięć w kanałach powinien być zgodny z zaleceniami producenta kabla. Jeżeli producent nie zaleci inaczej, przyjmuje się minimalny promień zgięcia: (UTP - 4 średnice kabla, STP - 6 średnic kabla, kabel światłowodowy od 10 do 20 średnic w zależności od sposobu wykonania)

Ustalając trasę przebiegu kabla, należy zachować następujące odległości od źródeł zasilania:

- 30 cm od wysokonapięciowego oświetlenia (świetlówki),
- 90 cm od przewodów elektrycznych 5 KVA lub więcej,
- 100 cm od transformatorów i silników.

EN 50167 „Okablowanie poziome”

Okablowanie pionowe

Wymagania instalacyjne dla przebiegów pionowych

- Do budowy przebiegów pionowych zalecane jest używanie kabli światłowodowych lub - w wyjątkowych przypadkach - skrętki.
- Do prowadzenia kabli między piętrami stosowany jest rękaw lub szyb. Zaleca się rękawy o średnicy co najmniej 10 cm (mogą one wystawać od 2,5 cm do 10 cm powyżej płaszczyzny podłogi) lub prostokątne szyby o minimalnym wymiarze 15 cm x 22,5 cm.
- Jeżeli trasa przebiegu kabli pionowych obejmuje więcej niż dwa piętra lub gdy kable są wyjątkowo ciężkie (np. wieloparowe kable miedziane), muszą być one mocowane. Mocowanie można wykonać np. za pomocą specjalnej żyły podtrzymującej, ułożonej po całej trasie kabla między najwyższym piętrem i piwnicą. Kabel należy połączyć z żyłą podtrzymującą co 90 cm, przy czym na jedno piętro powinny przypadać minimum trzy punkty wiązania. Dla dużych ilości kabli lub dla kabli wyjątkowo ciężkich powinna być użyta obejma lub osłona dla grupy kabli z każdego piętra.
- Ze względu na ochronę przeciwpożarową przejścia pomiędzy piętrami powinny być uszczelnione za pomocą specjalnych uszczelniaczy, powłoki przeciwpożarowej, pianki, kitu itp.

EN 50168 „Okablowanie pionowe”

Media transmisyjne

- Przewód koncentryczny

RG-58 to kabel koncentryczny o impedancji falowej 50 Ω i średnicy zewnętrznej 5 mm.

- **BNC -** złącze stosowane do łączenia sieci komputerowych zbudowanych z kabli koncentrycznych (np. 10BASE2), a także w aparaturze pomiarowej, systemach telewizji analogowej i cyfrowej oraz radiotelekomunikacji. Złącza BNC występują w dwóch wersjach: 50- i 75-omowej.

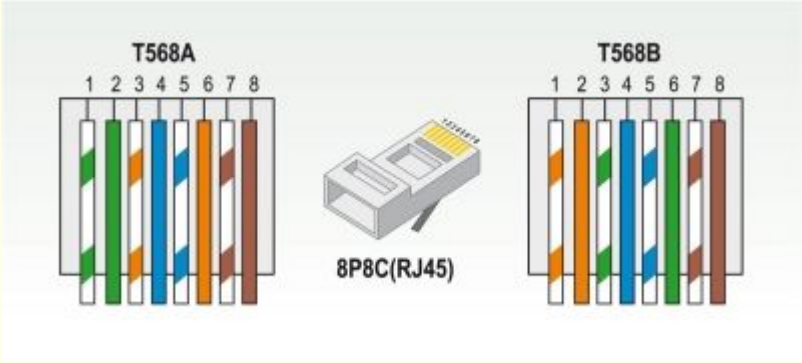
Wtyk BNC

Trójnik BNC

Terminator BNC – element w sieciach komputerowych opartych na kablu koncentrycznym służący do zakończenia linii. Terminator jest specjalnie dobranym rezystorem symulującym nieskończenie długi kabel i eliminującym w ten sposób odbicia sygnału od końca kabla mogące zakłócić pracę odbiorników.

Media transmisyjne

- **Skrętka** – rodzaj kabla sygnałowego służącego do przesyłania informacji, który zbudowany jest z jednej lub więcej par skręconych ze sobą żył w celu eliminacji wpływu zakłóceń elektromagnetycznych oraz zakłóceń wzajemnych, zwanych przesłuchami**.**
- **Złącze 8P8C** (ang. 8 Position 8 Contact; bardzo popularnie ale błędnie nazywane **RJ-45**) – rodzaj ośmiostykowego złącza (gniazdo i wtyk) Wykorzystywane w różnego rodzaju sprzęcie telekomunikacyjnym i komputerowym. Najbardziej rozpowszechnione jako podstawowe złącze do budowy przewodowych sieci komputerowych w standardzie Ethernet.



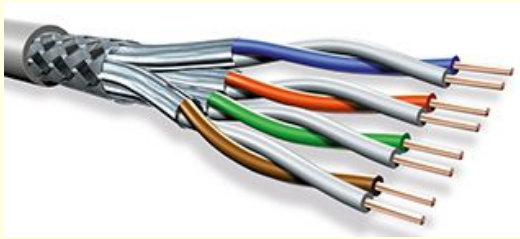
Standardy połączeń T568A,B

Zaciskarka RJ45(8P), RJ11(6P)

Rodzaje skrętek

- Dla większej ochrony przed zakłóceniami stosuje się **ekran** w postaci folii, w którą zawinięte są pary żył oraz uziemienie. Folia może być owinięta wokół pojedynczych par lub wszystkich żył.
- **Impedancja** typowej skrętki wynosi 100Ω, a maksymalna prędkość transmisji wynosi 1 Gbit/s.
- **Maksymalna odległość** pomiędzy urządzeniami połączonymi skrętką nie powinna przekraczać **100 m**.
- **Rodzaje skrętek:** (**T**wisted pair, **U**nshielded, **S**hielded, **F**olied)

U/UTP (*ang. Unshielded Twisted Pair*) – skretka nieekranowana



S/FTP (*ang. Shielded/ Foiled Twisted Pair*) - folia aluminiowa na każdej pojedynczej parze przewodów, ekran miedziany na czterech parach przewodów.

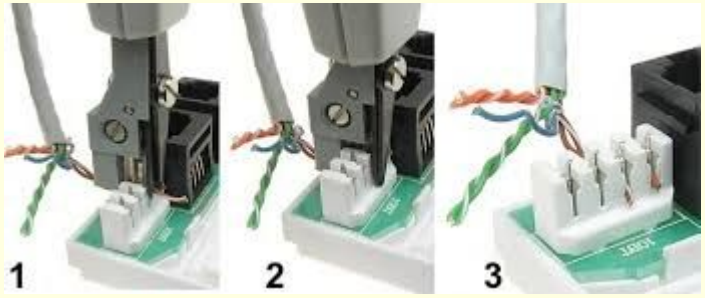
F/UTP (*ang. Foiled/Unshielded Twisted Pair*)- folia aluminiowa na czterech parach przewodów.

SF/UTP (*ang. Shielded/Foiled Twisted Pair*) — kabel skręcany z podwójnym zewnętrznym ekranem w postaci foliowego oplotu i siatki.

Moduły Keystone, złącza LSA

MODUŁ KEYSTONE JACK 1XRJ45 8P8C UTP CAT5E LSA

NARZĘDZIE UDERZENIOWE NÓŻ KROSOWNICZY KRONE LSA



Światłowód

- **Światłowód** – przezroczysta zamknięta struktura z włókna szklanego wykorzystywana do propagacji światła jako nośnika informacji
- **Zaleta -** Światłowody nie powodują interferencji elektrycznej w innych kablach ani też nie są na nią podatne. Impulsy świetlne mogą docierać na znacznie większe odległości niż to jest w przypadku sygnału w kablu miedzianym.
- **Wada** – przy instalowaniu światłowodów konieczny jest specjalny sprzęt do ich łączenia, który wygładza końce włókien w celu umożliwienia przechodzenia przez nie światła (spawarki światłowodowe).

Wtyk złącza ST

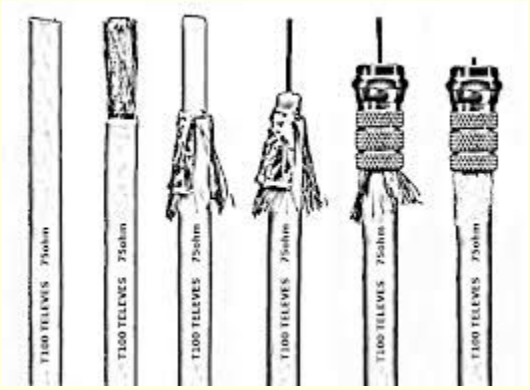
Wtyk złącza SC

Typy złącz: ST, SC, FC, LC

Złącze SMA, typu F

- Złącza anten WiFi, [1x złącze męskie RP-**SMA** - 1x złącze żeńskie RP-**SMA**]

- Złącze (wtyk) typu F – stosowany w instalacjach modemów kablowych (zakończenie przewodu antenowego)



Testery okablowania

Tester Diodowy
(Porty RJ45)

Tester kabli MicroScanner2, MS2-100, FLUKE networks

- **Funkcje:** Sprawdzanie układu żył, długości par, odległości do usterki,
- **Porty:** skrętka – UTP, FTP, SSTP, 8-stykowe wkładki modułowe typu RJ-45 i RJ-11; kabel koncentryczny – wkładki typu F kabli o impedancji 75/50/93 Ohm

Reflektometr optyczny FLX, OFL, CS

- opracowane z myślą o monterach nie posiadających dużego doświadczenia w dziedzinie techniki światłowodowej
- reflektometr
- źródło światła
- miernik mocy

Urządzenia sieciowe

Urządzenia warstwy fizycznej

- **Wzmacniak** (ang. Repeater)
- **Koncentrator** (ang. Hub)
- **Konwerter** (*ang. converter, transceiver*)

Interfejs sieciowy (ang. NIC – network interface connector)

Modem

Urządzenia warstwy łącza danych

- **Przełącznik** (ang. Switch)
- **Punkt dostępowy** (ang. Acces Point)
- **Most** (ang. Bridge)

Urządzenia warstwy sieciowej

- **Ruter** (ang. Ruter)
- Przełączniki warstwy 3

Symbole urządzeń sieciowych

Koncentrator

Przełącznik

Most

Modem

Ruter

Zapora sieciowa

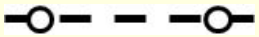
Punkt dostępowy

Stacja robocza

Rodzaje połączeń

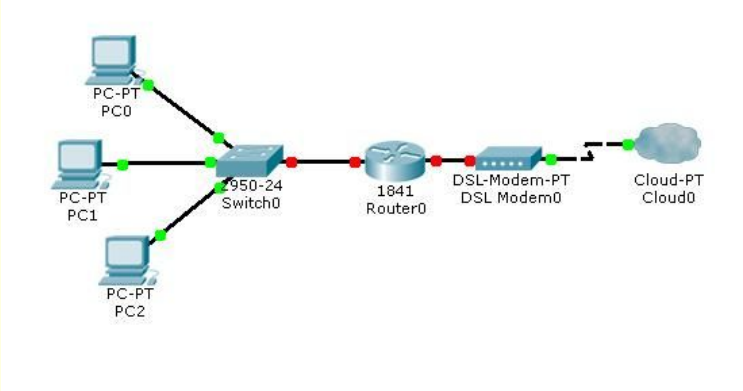
kabel Ethernet prosty

kabel swiatłwodowy



kabel Ethernet skrosowany

kabel szeregowy



Schemat połączeń przykładowej sieci w programie Cisco PacketTracer

Urządzenia warstwy fizycznej

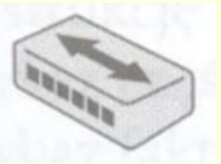
Urządzenia warstwy fizycznej stanowią grupę urządzeń transmisyjnych nie dokonujących analizy przesyłanych danych. Ich podstawowym zadaniem jest retransmisja danych pozyskanych na jednym z portów komunikacyjnych na wszystkie pozostałe. Warstwa fizyczna definiująca niskopoziomowe standardy komunikacyjne w aspektach mechanicznym, elektrycznym, funkcjonalnym, umożliwia jedynie (re-) transmisję strumienia bitów w różnych standardach.

Urządzenia pracujące w tej warstwie

- **Wzmacniak** (*ang. repeater*) jest urządzeniem, którego podstawowym zadaniem jest regeneracja sygnałów w sieci. Regeneracja, realizowana w drodze wzmocnienia umożliwia wydłużenie rozmiarów sieci.
- **Koncentrator** (*ang. HUB*) jest urządzeniem, którego podstawową funkcją jest retransmisja sygnału otrzymanego na jednym porcie na wszystkie pozostałe porty, umożliwiając utworzenie topologii gwiazdy. Wyróżnia się koncentratory aktywne oraz pasywne.
- **Konwerter** (*ang. converter, transceiver*) jest urządzeniem umożliwiającym konwersję standardu transmitowanego sygnału.

Wszystkie urządzenia warstwy pierwszej rozszerzają domenę kolizyjną i rozgłoszeniową, stąd ich stosowanie winno być szczególnie przemyślane już podczas projektowania sieci komunikacyjnej.

Koncentrator



Koncentrator pracuje w warstwie pierwszej modelu ISO/OSI, przesyłając sygnał z jednego portu na wszystkie pozostałe.

- Nie analizuje ramki pod kątem adresu MAC oraz IP.
- Koncentrator powtarza każdy sygnał elektroniczny, tworząc jedną domenę kolizyjną. Wadą sieci korzystających z koncentratorów jest duża liczba kolizji. Zaletą małe opóźnienia.

Modem

Modem (*ang. Modem – **Mod**ulator/**Dem**odulator*) – urządzenie elektroniczne, którego zadaniem jest zamiana danych cyfrowych na analogowe sygnały elektryczne (modulacja) i na odwrót (demodulacja) tak, aby mogły być przesyłane i odbierane poprzez linię telefoniczną, łącze telewizji kablowej lub fale radiowe.

Rodzaje:

- **Zewnętrzny -** występujący w postaci oddzielnego urządzenia, znajdującego się poza komputerem i połączony z nim (lub z innym odbiornikiem) przy użyciu przewodu (interfejs: RS-232, USB, LPT, ethernet) oraz charakteryzujący się pełną samodzielnością sprzętową.
- **Wewnętrzny -** zbudowany w postaci specjalnej karty rozszerzeń instalowanej wewnątrz komputera (PCI, ISA), zazwyczaj wykorzystującej w pewnym stopniu procesor komputera.

Modem kablowy
Motorola SB5101

Karta sieciowa

- **Interfejs sieciowy** (*ang. NIC – network interface connector*) - Karty sieciowe (*ang. NIC - Network Interface Card*) służy do przekształcania pakietów danych w sygnały, które są przesyłane w sieci komputerowej. Pracują w określonym standardzie, np. Ethernet, Token Ring, FDDI, WiFi. Każda karta NIC posiada własny, unikatowy w skali światowej adres fizyczny, znany jako adres MAC.

Karta sieciowa Ethernet - skrętka, złącze RJ45

Karta światłowodowa

Karta bezprzewodowa USB

Urządzenia warstwy łącza danych

Urządzenia warstwy 2 podejmują decyzje o przesyłaniu na podstawie adresów kontroli dostępu do medium MAC zawartych w nagłówkach przesyłanych ramek z danymi.

- **Most** (*ang. Bridge*)
- **Przełącznik** (*ang. Switch*)
- **Punkt dostępowy** (*ang. Acces Point*)

Most

Most (*ang. Bridge*) to urządzenie posiadające 2 lub więcej portów, służące do łączenia segmentów sieci. Na bieżąco identyfikuje swoje porty i kojarzy konkretne komputery.

- Pozwala na podniesienie wydajności i zwiększenie maksymalnych długości sieci.
- Zapewnia proste filtrowanie, odczytuje adres zapisany w ramce sieci Ethernet lub Token Ring i określa do jakiego segmentu należy przesłać dany pakiet.
- Mostek sieciowy jest niewidoczny w sieci, czyli jakbyśmy prześledzili trasę sygnału, to mostek sieciowy nie pokaże nam się jako komputer przekazujący sygnał – w przeciwieństwie do routera.

Przełącznik - switch

- **Przełącznik (*ang. switch*)** to urządzenie pracujące w warstwie drugiej modelu OSI (łącza danych), jego zadaniem jest przekazywanie ramek między segmentami.
- Przełącznik określa się też mianem wieloportowych mostów lub inteligentnych koncentratorów.
- Przełączniki w sieci LAN często zastępują koncentratory.
- Umiejętność przekazywania ramek tylko do jednego portu znacznie podniosła wydajność sieci i ograniczyła domenę kolizji. Jeśli docelowy adres MAC nie zostanie znaleziony w tablicy, przełącznik po prostu przekazuje go do wszystkich portów.
- Przełączniki uczą się adresów, odczytując źródłowe adresy MAC z każdej odebranej ramki, a następnie zapisując je w pamięci razem z informacją o porcie, na którym odebrano ramkę z danym adresem MAC. Dzięki temu przełącznik wie, które adresy należą do urządzeń podłączonych do poszczególnych portów.
- Podejmują decyzje przesyłania danych na podstawie adresów MAC

Punkt dostępowy

Punkt dostępu, punkt dostępowy (*ang. access point, AP*) – urządzenie zapewniające hostom dostęp do sieci komputerowej za pomocą bezprzewodowego nośnika transmisyjnego jakim są fale radiowe.

Punkt dostępowy jest zazwyczaj **mostem** łączącym bezprzewodową sieć lokalną (WLAN) z siecią lokalną (LAN). W związku z tym punkt dostępowy musi posiadać co najmniej dwa interfejsy sieciowe:

- bezprzewodowy działający w oparciu o standard IEEE 802.11 (Wi-Fi)
- przewodowy służący połączeniu PD z siecią standardu IEEE 802.3 (Ethernet) bądź modem standardu DSL

D-link DAP-2310

Punkt dostępowy zazwyczaj posiada jeden port LAN, którym dołączamy go do sieci przewodowej np. D-link DAP-2310. Może być też zrealizowany jako punkt dostępowy z wbudowanym ruterem np.: TP-Link TL-WR741ND

TP-Link TL-WR741ND

Ruter

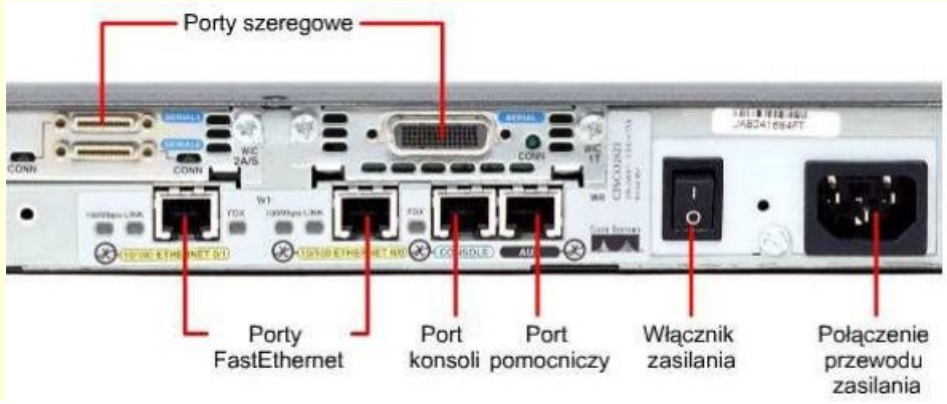
- **Router** – urządzenie sieciowe pracujące w trzeciej warstwie modelu OSI. Służy do łączenia różnych sieci komputerowych (różnych w sensie informatycznym, czyli np. o różnych klasach, maskach itd.), pełni więc rolę węzła komunikacyjnego. Na podstawie informacji zawartych w pakietach TCP/IP jest w stanie przekazać pakiety z dołączonej do siebie sieci źródłowej do docelowej, rozróżniając ją spośród wielu dołączonych do siebie sieci. Proces kierowania ruchem nosi nazwę trasowania, routingu lub routowania.
- Podejmują decyzje przesyłania danych na podstawie adresów IP
- Skuteczne działanie routera wymaga informacji na temat otaczających go urządzeń – innych routerów i hostów.
  - **Routing statyczny** – informację dostarcza administrator, wówczas nosi ona nazwę tablicy statycznej
  - **Routing dynamiczny** – informacja pozyskana przez sam ruter od sąsiadujących urządzeń pracujących w trzeciej warstwie; tablice tak konstruowane nazywane są dynamicznymi. Do najpopularniejszych algorytmów routigu dynamicznego zalicza się **RIP i OSPF**.

Rutery CISCO

Konfiguracja rutera może odbywać się poprzez interfejs użytkownika **CLI** (*ang Command Line Interface*) na dwa sposoby:

- Za pomocą terminala ASCII podłączonego do gniazda konsoli (RJ45). Terminalem może być zwykły komputer osobisty, na którym uruchomiono odpowiednie oprogramowanie emulacyjne, np. HyperTerminal lub Putty.
- Za pomocą sesji Telnet. Aby ustanowić sesję Telnet z routerem, należy skonfigurować adres IP dla co najmniej jednego interfejsu, a dla sesji terminala wirtualnego trzeba ustawić login i hasło.

Uwaga: Wprowadzanie jakichkolwiek zmian w konfiguracji routera Cisco za pomocą interfejsu CLI jest możliwe po przejściu do trybu konfiguracji globalnej (global config). Tryb konfiguracji globalnej jest podstawowym trybem konfiguracyjnym.



CLI

W interfejsie CLI jest używana struktura hierarchiczna. Struktura ta wymaga przejścia do odpowiedniego trybu w celu wykonania określonych zadań. System IOS udostępnia usługę interpretacji poleceń o nazwie EXEC. Po wprowadzeniu każdego polecenia usługa EXEC sprawdza jego poprawność i wykonuje je.

Cisco IOS występują dwa poziomy dostępu do sesji EXEC.

- **tryb użytkownika** (oznaczony symbolem >)
  - Tryb EXEC użytkownika udostępnia jedynie ograniczony zestaw podstawowych poleceń do monitorowania. Z tego powodu jest on również nazywany trybem „tylko do odczytu".
  - Tryb EXEC użytkownika nie udostępnia żadnych poleceń, które umożliwiają zmianę konfiguracji routera.
- **tryb uprzywilejowany** (tryb enable – oznaczony symbolem #).
  - umożliwia dostęp do wszystkich poleceń routera.
  - Do wejścia w ten tryb może być potrzebne hasło.
  - Polecenia związane z konfigurowaniem sieci i zarządzaniem nią wymagają od administratora sieci pracy w uprzywilejowanym trybie EXEC.
  - Tryb konfiguracji globalnej oraz wszystkie inne bardziej szczegółowe tryby konfiguracji są dostępne tylko z uprzywilejowanego trybu EXEC.

Uwaga: Aby z poziomu EXEC użytkownika uzyskać dostęp do uprzywilejowanego poziomu EXEC, należy po symbolu > wprowadzić polecenie enable. Jeśli skonfigurowane jest hasło, router zażąda jego podania. Ze względów bezpieczeństwa urządzenie sieciowe firmy Cisco nie wyświetla wprowadzanego hasła. Po wprowadzeniu poprawnego hasła symbol zachęty routera zmieni się na symbol #. Oznacza to, że użytkownik jest w uprzywilejowanym trybie EXEC. Po wprowadzeniu znaku zapytania w uprzywilejowanym trybie EXEC zostanie wyświetlonych o wiele więcej opcji poleceń niż w trybie EXEC użytkownika.

CLI

Wpisanie znaku zapytania (?) po znaku trybu EXEC użytkownika lub uprzywilejowanego trybu EXEC powoduje wyświetlenie listy dostępnych poleceń.

Polecenie show

- **show interfaces**: wyświetla dane statystyczne dotyczące wszystkich interfejsów routera. przykładzie:
- **show interfaces serial 0/1** – parametry portów szeregowych
- **show clock:** wyświetla godzinę ustawioną w routerze
- **show hosts:** wyświetla przechowywaną w pamięci podręcznej listę nazw i adresów hostów
- **show users:** wyświetla nazwy wszystkich użytkowników podłączonych do routera
- **show history:** wyświetla historię wprowadzonych poleceń
- **show arp:** wyświetla tablicę ARP routera Routery Cisco
- **show protocols:** wyświetla status wszystkich skonfigurowanych protokołów warstwy 3 w ujęciu globalnym i z uwzględnieniem konkretnych interfejsów

Przykład konfiguracji interfejsu

```
Router(config)#interface serial 0/0
Router(config-if)#ip address  <adress_ip> <maska_podsieci>
Router(config-if)#clock rate 56000
```

Router WiFi - WRTG54

Cechy punktu dostępowego:

- zgodny z 802.11g pracujący z częstotliwością 2.4GHz, - przepustowość do 54 Mbps,
- kompatybilność z klientami 802.11b (jednocześnie obsługuje karty Wireless-B z prędkością 11Mbps),
- moc nadajnika: 18 dBm (64mW),
- zapewnia: roaming, wybór najlepszego punktu dostępowego, równoważenie obiążenia (load balancing) oraz filtrowanie ruchu pakietów,
- WPA (Wi-Fi Protected Access):
- WPA PSK (Pre-shared key),

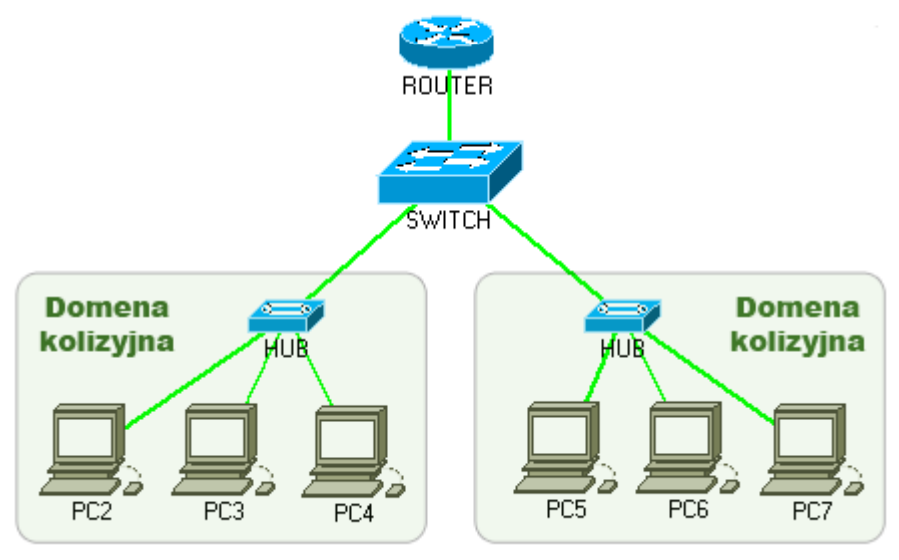
Cechy rutera

- **port WAN** w postaci gniazda RJ-45 (Ethernet 10/100) do podpięcia do modemu xDSL, modemu kablowego bądź szkieletu Ethernetowego,
- 4-portowy switch Fast Ethernet (**porty LAN**),
- NAT (Network Address Translation),
- Serwer / klient DHCP,
- filtrowanie IP, MAC oraz poszczególnych portów protokołu TCP/IP,
- Forwarding - przypisywanie usługom statycznych adresów IP w sieci LAN,
- Logging - tworzenie logów wywołań z i do sieci LAN,
- routing statyczny / dynamiczny (RIP-1 i RIP-2),
- konfiguracja przez przeglądarkę WWW - lokalna oraz zdalna,

Domeny kolizyjne

Domeny kolizyjne to obszar sieci, w którym może dojść do kolizji

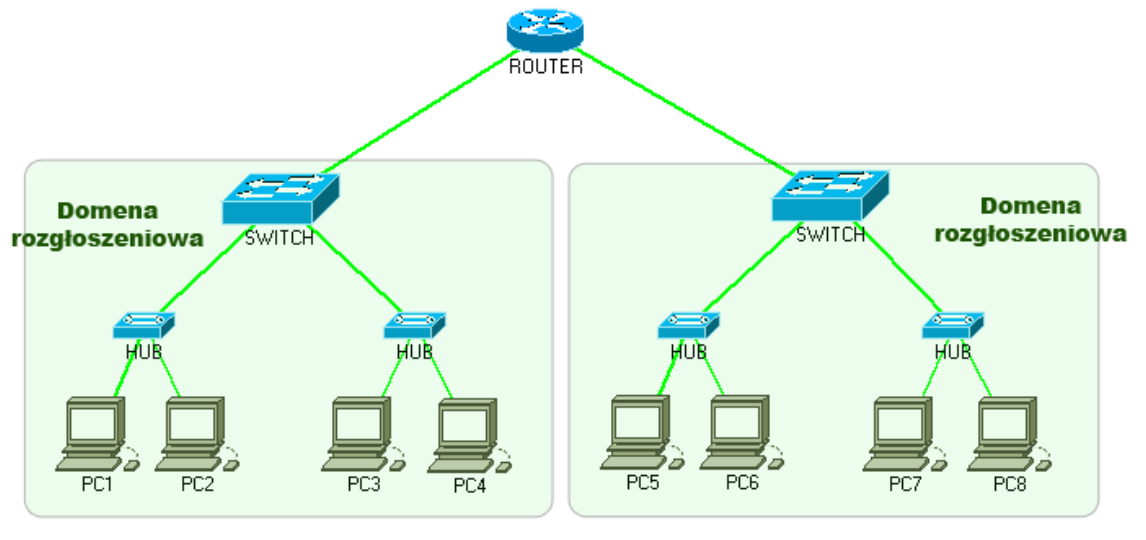
- Domenę kolizyjną ograniczają urządzenia pracujące w warstwach wyższych niż pierwsza modelu OSI.
- Koncentratory są wewnątrz domeny kolizyjnej (rozszerzają domenę kolizyjną)
- Switch (przełącznik) i router ograniczają domenę kolizyjną.



Domeny rozgłoszeniowe

Domena rozgłoszeniowa to taki obszar sieci, do którego dotrze informacja wysyłana przez jedno urządzenie do wszystkich innych – broadcast.

- Ruch rozgłoszeniowy jest przekazywany poprzez urządzenia pierwszej i drugiej warstwy modelu OSI, tj. koncentratory, huby, mosty czy switche. One zwiększają obszar domeny rozgłoszeniowej.
- Domenę rozgłoszeniową ograniczają urządzenia trzeciej warstwy – routery.
- Można również utworzyć sieć wirtualną VLAN (sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej), która również ograniczy obszar domeny rozgłoszeniowej.



IPv4 - wprowadzenie

- jest liczbą **32** bitową
- składa się z **4** oktetów oddzielonych kropką
- ile kombinacji liczb można zapisać na 8 bitach (oktecie)?

  2^8=256
- w zapisie dziesiętnym zakres oktetu wynosi:

  min = 0, **max = 255**
- w zapisie binarnym zakres oktetu wynosi:

  min = 00000000, **max = 11111111**

Przykład:

192 . 168 . 50 . 222

11000000 10101000 **00110010** 11011110

Oktet binarnie: 0 0 **1** **1** 0 0 **1** 0

wagi: 128 64 **32** **16** 8 4 **2** 1 => 32+16+2 = 50 w zapisie dziesiętnym

IPv4 - klasy

W każdym adresie IP, pewna część bitów (liczona od lewej strony), reprezentuje adres sieci, reszta natomiast stanowi adres konkretnego hosta. Jest to logiczne ponieważ pakiet najpierw musi trafić do właściwej sieci, dopiero potem trafia do konkretnego hosta. Jak w życiu, list najpierw trafia do miasta, dopiero potem pod wskazany numer domu na konkretnej ulicy. Jaka część bitów przeznaczona jest na adres sieci, a jaka na adres hosta określone jest przez tzw. **maskę podsieci**.

Maski sieciowe dla klas A, B, C

A: 255.0.0.0 => **sieć**.host.host.host (zakres: 1.0.0.1 - 126.255.255.254)
B: 255.255.0.0 => **sieć.sieć**.host.host (zakres: 128.0.0.1 - 191.255.255.254)
C: 255.255.255.0 => **sieć.sieć.sieć**.host (zakres: 192.0.0.1 - 223.255.255.254)

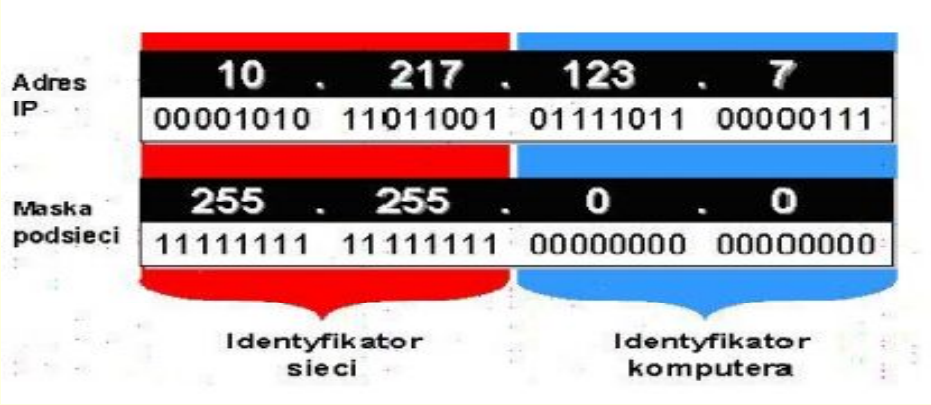
Liczba sieci = 2^(liczba bitów sieci)
Liczba hostów = 2^(liczba bitów hosta) – 2

Uwaga: -2 wynika z tego, że dwa adresy hosta są zarezerwowane (same zera w części hosta – adres sieci, same jedynki w części hosta – adres rozgłoszeniowy)

IPv4 – maska sieciowa

Adresowanie IP opiera się na hierarchii dwuwarstwowej, w której na 4 oktetach zapisany jest adres sieci i hosta.

- Maska (**NETMASK**) jest liczbą **32** bitową
- Ma charakterystyczną strukturę – tworzą ją dwa bloki: blok **„1”** i blok **„0”**: np. 255.255.255.0 = 11111111 11111111 11111111 00000000
- pozycje na których są ”**1**” wyznaczają wspólny adres sieci, pozycje na których są ”**0**” wyznaczają część hosta (identyfikatory urządzeń sieciowych)
- Maskę zapisuje się w postaci dziesiętnej (na przykład 255.255.255.224) lub w postaci skróconej jako liczbę po ukośniku: 10.0.0.5/27 co oznacza adres 10.0.0.5 i maskę 255.255.255.224 – 27 jedynek).



IPv4 - adres sieci, rozgłoszeniowy

- **Adres sieci (NETWORK)** - w części bitów adresu IP, odpowiadających za adres hosta występują same zera. Taki adres służy do identyfikacji sieci/podsieci i nie jest przypisany żadnemu konkretnemu urządzeniu.
- **Adres rozgłoszeniowy (BROADCAST)** – w części bitów adresu IP, odpowiadających za adres hosta występują same jedynki. Taki adres jest wykorzystywany do wysyłania pakietów IP do wszystkich urządzeń w danej sieci/podsieci, ale nie jest przypisany do żadnego urządzenia.

Przykład. Wyznacz adres sieci, adres rozgłoszeniowy

IP =	**192**	**168**	**1**	**133**
IP =	**11000000**	**10101000**	**00000001**	**10000101**
NETMASK =	**11111111**	**11111111**	**11111111**	**00000000**
	sieć	**sieć**	**sieć**	**host**
NETWORK =	**192**	**168**	**1**	**0**
BROADCADST =	**192**	**168**	**1**	**255**

NETWORK = IP **AND** NETMASK

IPv4 - adresy prywatne

W celu dowolnego wykorzystywania adresów IP stworzono specjalne prywatne pule adresowe w poszczególnych klasach adresów IP. Adresy można dowolnie powielać w sieciach prywatnych, natomiast aby sieć prywatną z tymi adresami IP podłączyć do sieci globalnej (publicznej) musimy zastosować **NAT (*ang. Network Adress Translation* – translacja adresów)** i posiadać przyznany adres publiczny.

Klasa	Adres sieci	Maska sieci	Dostępne adresy
A	10.0.0.0 /8	255.0.0.0	10.0.0.1 – 10.255.255.254
B	172.16.0.0 /12	255.240.0.0	172.16.0.1 – 172.31.255.254
C	192.168.0.0 /16	255.255.0.0	192.168.0.1 – 192.168.255.254

Adresy IP specjalnego przeznaczenia (oprócz adresów prywatnych):

0.0.0.0 - sieć nieznana, zwykle oznacza default
127.0.0.1 – localhost (pętla zwrotna)
255.255.255.255 - ograniczony broadcast (jedynie do sieci lokalnej)

IPv4 - podsieci

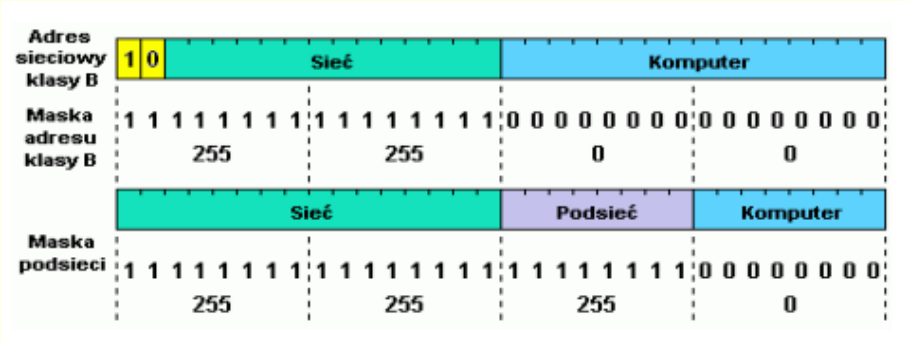
Hierarchia dwuwarstwowa wprowadza ograniczenia adresowania dzieląc nieefektywnie przestrzeń adresową. Dlatego wprowadzono adresowanie oparte na trzech warstwach, tj. na adres IP składa się adres sieci, podsieci i hosta.

- Podsieć jest wydzielona poprzez „zajęcie” części bitów adresu hosta.
- Do danej podsieci można podłączyć N-2 interfejsów (np. komputerów), gdzie N to liczba możliwych adresów w sieci. Dzieje się tak, ponieważ pierwszy adres (np.192.168.0.0/26) to adres sieci, a ostatni (192.168.255.255/26) to adres rozgłoszeniowy.

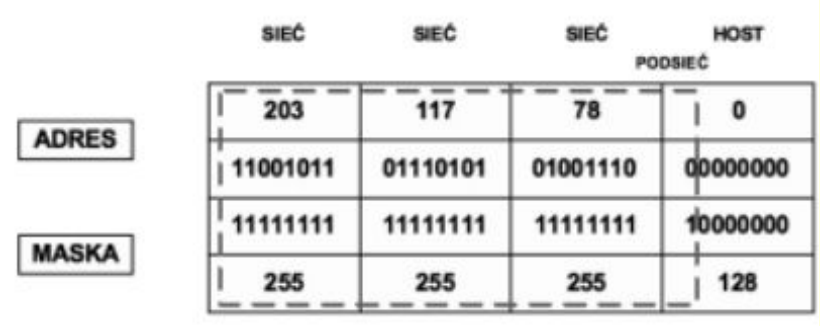
Przykład. W sieci 192.168.0.0/26, dodatkowe 2 bity adresu hosta w klasie A zostają zarezerwowana na cztery podsieci (2^2 = 4). W każdej podsieci zostaje 6 bitów na adresy hostów – mamy więc pulę 2^6 - 2 = 30 adresów dla hostów.

IPv4 - podsieci

Podział adresów na klasy A,B,C jest nieefektywny dlatego stosuje się model bezklasowy oparty na tzw. maskach podsieci.



Przykład 1:
pożyczamy 8 bitów z części hosta
➔
maska podsieci: 255.255.255.0
256 podsieci (2^8)
254 komputery (2^8-2)



Przykład 2:
Sieć klasy C
pożyczmy 1 bit z części hosta, pozostałe 7 definiują hosty
➔
maska podsieci 25-bitowa: 255.255.255.128
2 podsieci (2^1)
126 komputerów/podsieć (2^7-2=126)

IPv4 – przykłady zadań

Który adres IP jest adresem urządzenia pracującego w sieci 10.0.0.0/17?

A. 10.0.128.127
B. 10.0.127.128
C. 10.0.128.254
D. 10.0.254.128

Wskazówka: 10.0.0XXXXXXX.XXXXXXXX – adresy muszą mieć taki sam adres sieci (na 17 bitach)

Wskaż prawidłową postać maski podsieci

A. 255.255.255.255
B. 255.252.252.255
C. 255.255.0.128
D. 0.0.0.0

Wskazówka: Maska musi mieć lewostronny ciągły blok jedynek

Komputer ma adres IP 192.168.0.1, maska podsieci to 255.255.255.0. Który adres jest adresem rozgłoszeniowym podsieci, do której należy ten komputer?

A. 192.168.0.31
B. 192.168.0.63
C. 192.168.0.127
D. 192.168.0.255

Wskazówka: Adres rozgłoszeniowy w części hosta (ostatnie 8 bitów → maska = 0) ma same jedynki.
Adres sieci = 192.168.0.0
Adres rozgłoszeniowy = 192.168.0.255

IPv4 - zadania

1. Wykonaj polecenie wyświetlające adres IP i maskę twojego komputera (ipconfig w systemie Windows, ifconfig w systemie Linux). Oblicz liczbę jedynek w masce oraz adres IP sieci, w której znajduje się Twój komputer.
2. Podaj zakres i ilość adresów, które można przydzielić komputerom w tej sieci.
3. Podaj wzór na liczbę komputerów w podsieci dla maski 255.255.255.192
4. Oblicz zakres adresów komputerów i adres rozgłoszeniowy w sieci o adresie IP 150.150.64.0 i masce 255.255.192.0.
5. Dla adresu 172.17.1.14 i maski 255.255.240.0
   a) Przedstaw maskę w postaci skróconej.
   b) Podaj adres sieci oraz adres rozgłoszeniowy.
   c) Podaj zakres i ilość adresów, które można przydzielić komputerom w tej sieci.
6. Podziel sieć 192.168.111.0 /24 na 4 równe podsieci. Podaj tylko ich adresy i maski.

IPv6 - wprowadzenie

- Adres jest 128 bitowy.
- Adres zazwyczaj zapisuje się jako osiem 16-bitowych bloków zapisanych w systemie szesnastkowym oddzielonych dwukropkiem. Dozwolone jest pomijanie początkowych zer w bloku, a także pominięcie jednego ciągu bloków składających się wyłącznie z zer. Pominięte bloki zer oznacza się podwójnym separatorem bloków (dwukropek). Dopuszczalny jest tylko jeden podwójny dwukropek "::" w adresie.

Przykład: Poniższe adresy są równoznaczne:

2001:0db8:0000:0000:0000:0000:1428:57ab

2001:0db8:0:0:0:0:1428:57ab

2001:0db8:0:0::1428:57ab

2001:0db8::1428:57ab

2001:db8::1428:57ab

802.1Q - VLAN

VLAN (*ang. Virtual Local Area Network*) - sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej. Zastosowania VLAN to:

- Dzielenie sieci na grupy użytkowe: Inżynierowie, Zarządzanie
- Tworzenie typów użytkowników np. e-mail, WWW, itd.

Do tworzenia VLAN-ów wykorzystuje się konfigurowalne lub **zarządzalne przełączniki**, lub rutery zgodne z IEEE 802.1Q umożliwiające podział jednego fizycznego urządzenia na większą liczbę urządzeń logicznych, poprzez separację ruchu pomiędzy określonymi grupami portów. W przełącznikach zarządzanych zgodnych z IEEE 802.1Q możliwe jest znakowanie ramek (**tagowanie**) poprzez doklejenie do nich informacji o VLAN-ie, do którego należą. Dzięki temu możliwe jest transmitowanie ramek należących do wielu różnych VLAN-ów poprzez jedno fizyczne połączenie (**trunking**).

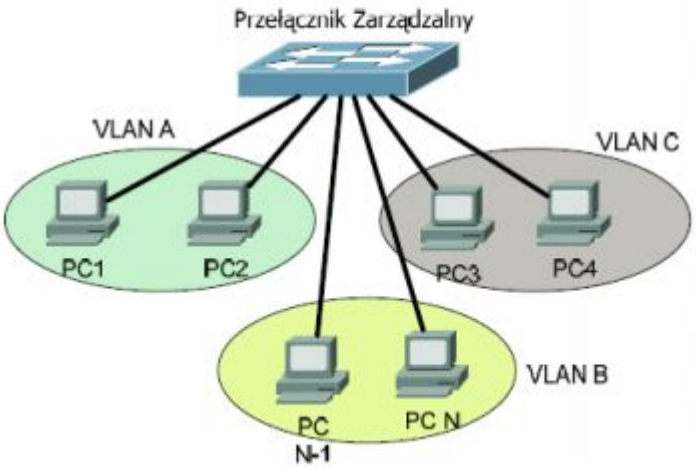
Zalety:

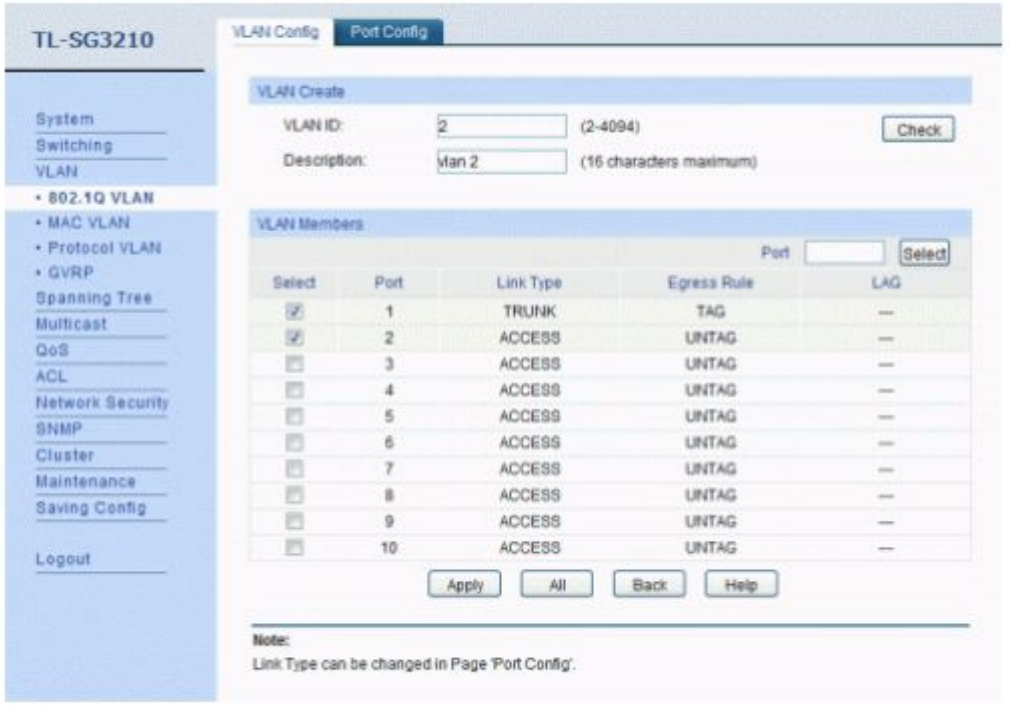
- Podniesienie bezpieczeństwa – komunikować się mogą tylko uprawnione podsieci np. operator jest logicznie odseparowany od pionu zarządzania
- Uporządkowanie ruchu sieciowego

Przełącznik TL-SG3210

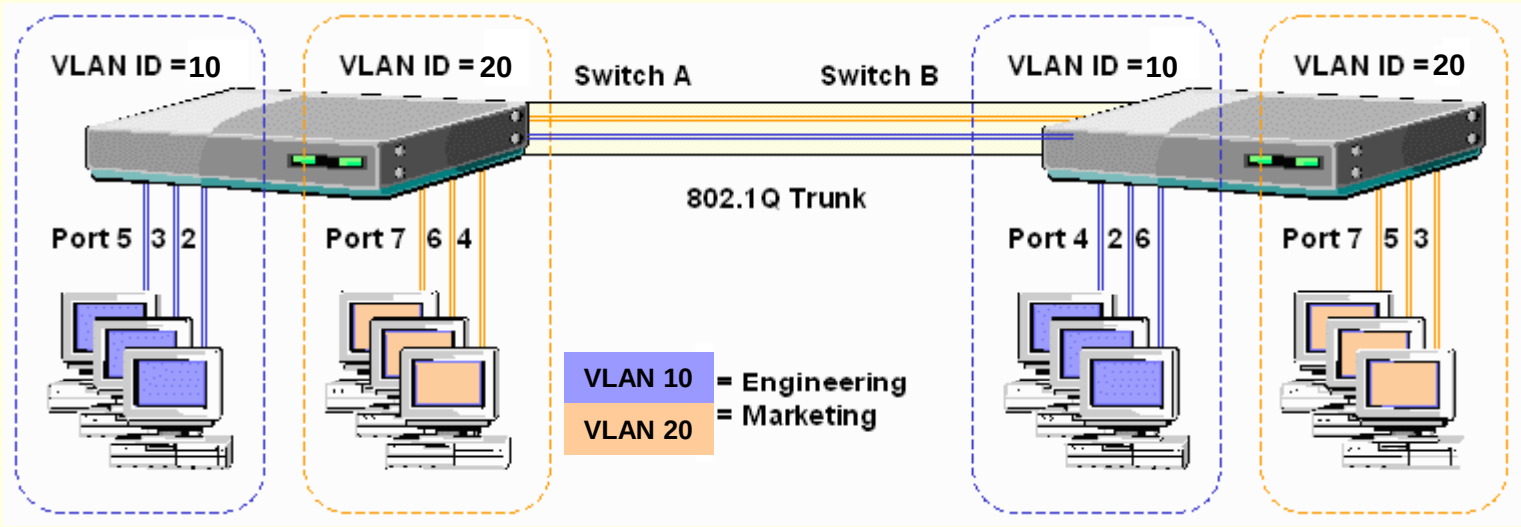
Przełącznik zarządzalny TL-SG3210

- 8 portów 10/100/1000Mb/s.
- przyjazny interfejs dostępny przez przeglądarkę internetową, konsola CLI lub wykorzystanie protokołów SNMP oraz RMON.
- tagowanie VLAN (zgodnie ze standardem 802.1Q), Port Isolation, Port Mirroring,





VLAN - przykład



Switch A:

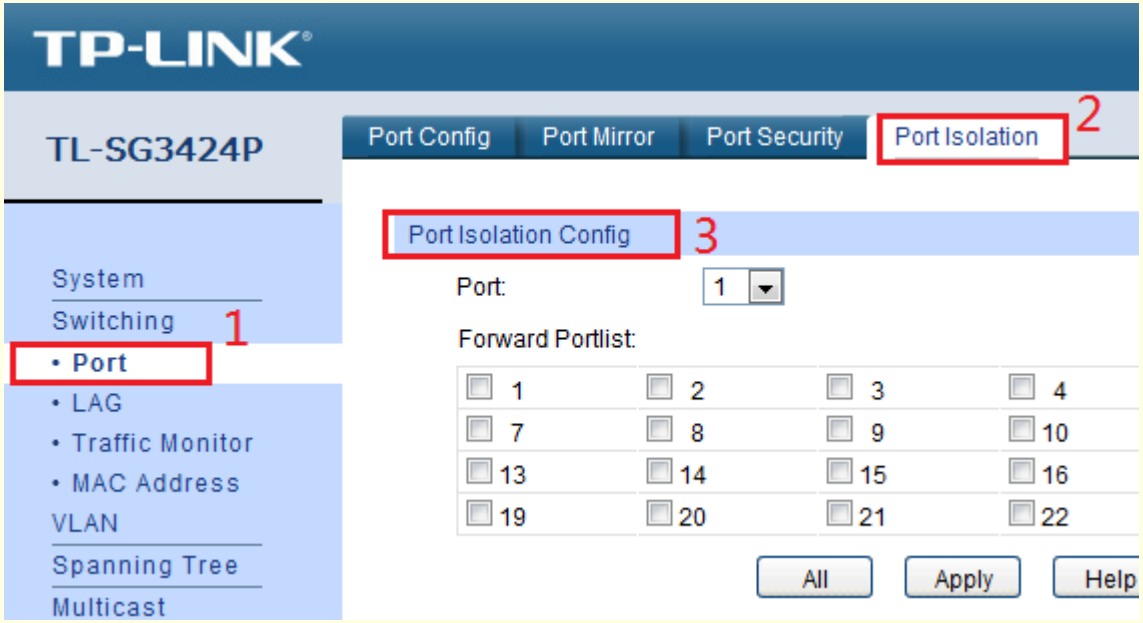
- port 1 (**TRUNK**: VLAN 10, 20)
- porty 2,3,5 (VLAN 10),
- porty 4,6,7 (VLAN 20),

Switch B:

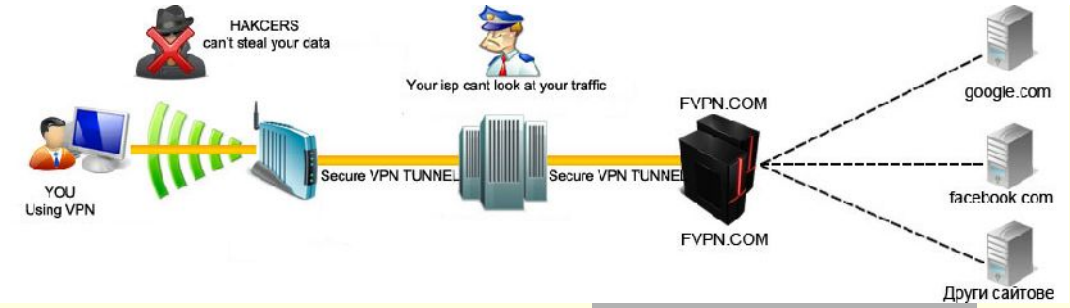
- port 1 (**TRUNK**: VLAN 10, 20)
- porty 2,4,6 (VLAN 10),
- porty 3,5,7 (VLAN 20),

Port mirroring

- **Port Mirroring** - funkcja pozwala na zdefiniowanie portu (mirroring port), na który będą kopiowane wszystkie pakiety "widziane" na zadanych, monitorowanych portach (mirrored ports). Funkcja często używana do podłączania systemów analizy ruch sieciowego do (mirroring port).
- **Port Isolation** – izolacja portów umożliwia zdefiniowanie odizolowanych grup połączeń pomiędzy portami bez tworzenia VLAN-ów



VPN



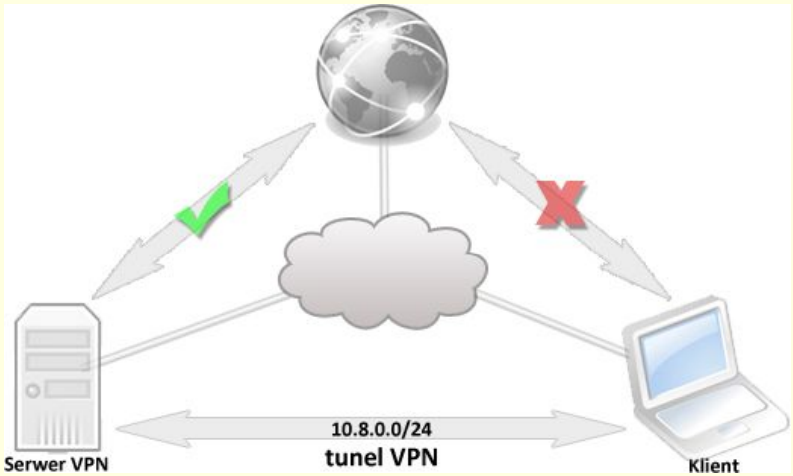
VPN (*ang. Virtual Private Network*) - wirtualna sieć prywatna (tunel), przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak Internet). Rozwiązania oparte na VPN stosowane są np. w sieciach korporacyjnych firm, których zdalni użytkownicy pracują ze swoich domów na niezabezpieczonych łączach. Wirtualne Sieci Prywatne charakteryzują się dość dużą efektywnością, nawet na słabych łączach (dzięki kompresji danych) oraz wysokim poziomem bezpieczeństwa (ze względu na szyfrowanie). Rozwiązanie to sprawdza się w firmach, których pracownicy często podróżują lub korzystają z możliwości telepracy.

Zastosowania:

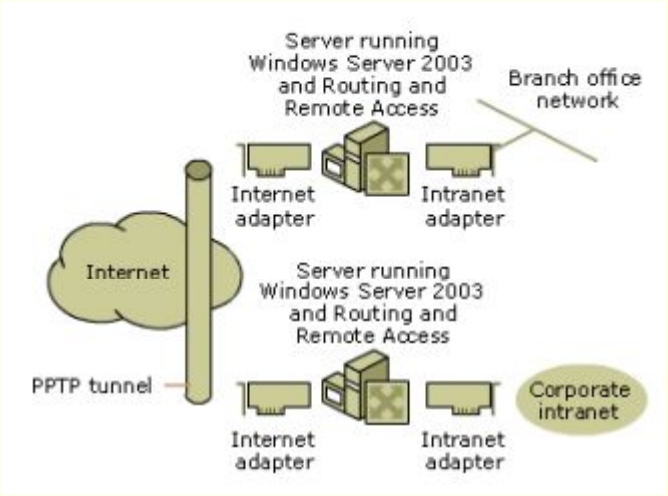
- **sieci dostępowe** - łączą zdalnych użytkowników: czyli pracowników mobilnych, konsultantów, sprzedawców, lokalne filie, z siedzibą firmy;
  - intranet - łączy odległe oddziały tej samej firmy;
  - ekstranet - zapewnia ograniczony dostęp do sieci firmowej zaufanym partnerom biznesowym.
- **ochrona użytkownika** podczas korzystania z publicznej sieci Wi-Fi
- **omijanie restrykcji** związanych z protokołem IP nakładane przez dostawcę internetu/państwo (ograniaczenia terytorialne – facebook, netflix itp.)
- **ochrona prywatności** w sieci Intenet

VPN - zastosowania

VPN – zastosowania



Omijanie restrykcji w dostępie do Internetu poprzez serwer VPN



Połączenia klienta VPN do sieci firmowej intranet z systemem operacyjnym Windows Server 2003

VPN - mechanizmy

Wirtualna sieć prywatna VPN korzysta z publicznej infrastruktury telekomunikacyjnej, która dzięki stosowaniu protokołów tunelowania, szyfrowania i procedur bezpieczeństwa zachowuje poufność danych.

Tunelowanie – tworzenie połączenia pomiędzy dwoma odległymi hostami dające wrażenie połączenia bezpośredniego:

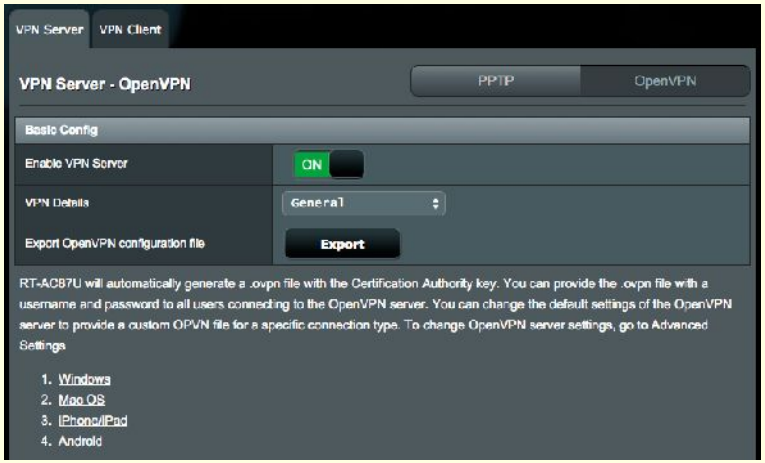
- tunel wykorzystuje technikę enkapsulacji jednego protokołu w innym, umożliwia zastosowanie mechanizmów szyfrowania lub translacji transmitowanych danych.
- umożliwia wykorzystanie metod kryptograficznych celem utworzenia bezpiecznego kanału tunelowania
- pozwala omijać blokowanie portów i usług (np. poprzez dozwolony port firewalla) http-tunnel

Najczęściej spotykane rodzaje VPN:

- **PPTP** (*ang. Point ot Point Tunneling Protocol*), L2TP (*ang. Layer Two Tunneling*) – używane w MS Windows
- **IPSec** - (*ang. Internet Protocol Security, IP Security*) – zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy szyfrowania pomiędzy komputerami. Protokoły tej grupy mogą być wykorzystywane do tworzenia Wirtualnej Sieci Prywatnej
- **SSTP** (*ang. Secure Socket Tunneling Protocol*)
- Tunelowanie **SSL/TLS** (SecureSocketLayer /Transport LayerSecurity).

OpenVPN

- OpenVPN – pakiet oprogramowania, który implementuje techniki tworzenia bezpiecznych połączeń punkt-punkt (VPN) lub strona-strona w sieciach routowanych lub mostkowanych. Umożliwia on tworzenie zaszyfrowanych połączeń między hostami przez sieć publiczną Internet (tunel) – używa do tego celu biblioteki OpenSSL oraz protokołów SSLv3/TLSv1. W przeciwieństwie do innych rozwiązań VPN nie bazuje na protokole IPsec jako medium.



OpenVPN – konfiguracja w ruterze ASUS RT-AC87U

VLAN, VPN - pytania

1. Co to jest sieć VLAN i jakie są korzyści ze stosowania tej technologii?
2. Jaka jest różnica pomiędzy VLAN i VPN?
3. Dzieli sieć fizyczną na wirtualne podsieci.

   a) VLAN, b) VPN c) IPSec d) SSL

4. Łączy zalety sieci prywatnych i publicznych, umożliwiając firmom o wielu ośrodkach korzystanie z systemu zachowującego się jak w pełni prywatna sieć, lecz przesyłającego dane między ośrodkami siecią publiczną

   a) VLAN, b) VPN c) IPSec d) SSL

5. Jakie urządzenie można wykorzystać do utworzenia VLAN:

   a) przełącznik, b) access point, c) ruter, d) modem

Routing IP

- Routing to wyznaczanie trasy dla pakietu danych, w taki sposób aby pakiet ten w możliwie optymalny sposób dotarł do celu. Odpowiedzialne są za to odpowiednie protokoły routowane, używane przez routery w tym celu.
- **Routing statyczny:** tablice rutingu
- **Routing dynamiczny:** RIP, OSPF, BPG, EIGRP

Jeśli TTL = 0 router odrzuca pakiet

Routery podejmują decyzje przesyłania danych na podstawie adresów IP

+	Bity 0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Wersja	Długość nagłówka	Typ usługi	Całkowita długość	
32	Numer identyfikacyjny			Flagi	Kontrola przesunięcia
64	Czas życia pakietu (TTL)		Protokół warstwy wyższej	Suma kontrolna nagłówka	
96	Adres źródłowy IP				
128	Adres docelowy IP				
160	Opcje IP				Uzupełnienie
192	Dane				

Metody routingu

Proces kierowania ruchem nosi nazwę trasowania, routingu lub rutowania.

Sposoby zdobywania przez routery informacji o ścieżkach są następujące:

- **trasa statyczna** - ręcznie definiuje ją administrator, jest jedyną trasą.
- **trasa domyślna** - ręcznie definiuje ją administrator. Używana jest wtedy, gdy następny krok nie jest bezpośrednio podany w tablicy routingu.
- **trasa dynamiczna** - administrator konfiguruje protokół routingu. Router wyznacza trasy otrzymując uaktualnienia od innych routerów.

IGP (*ang. Interior Gateway Protocols*), protokoły bramy wewnętrznej – rodzina protokołów trasowania pakietów danych wewnątrz systemu autonomicznego (*ang. Autonomous System, AS*).

- RIP, OSPF, EIGRP

IGMP (*ang. Internet Group Management Protocol*) – jeden z rodziny protokołów TCP/IP. IGMP służy do zarządzania grupami multicastowymi w sieciach opartych na protokole IP. Komputery wykorzystują komunikaty IGMP do powiadamiania routerów w swojej sieci o chęci przyłączenia się do lub odejścia z określonej grupy multicastowej.

BGP (*ang. Border Gateway Protocol*) zewnętrzny protokół trasowania (routingu). BGP w wersji czwartej jest podstawą działania współczesnego Internetu.

RIP

RIP (*ang. Routing Information Protocol*) - protokół Informowania o Trasach oparty na zestawie algorytmów wektorowych, służących do obliczania najlepszej trasy do celu. Do utworzenia metryki stosuje się jedynie liczbę przeskoków (liczba kolejnych routerów na danej trasie), natomiast jeżeli liczba przeskoków osiągnie 15, pakiety na następnym routerze zostaną odrzucone.

Własności:

- Routery wymieniają się swoimi tablicami routingu co określone odstępy czasu RIP standardowo co 30 sekund (z małymi różnicami) - wymienia się pełne tablice (stąd znaczne obciążenie sieci)
- Metryką trasy w protokole RIP jest ilość "hopów", jaką musi pokonać pakiet, by dotrzeć do sieci/hosta; 15 - trasa nieosiągalna
- Wybór mało optymalnych ścieżek (brak uwzględniania wagi innej niż "odległość”)
- Tylko RIPv2 przesyła maskę dla trasy

OSPF

OSPF (*ang. Open Shortest Path First*) - "pierwszeństwo ma najkrótsza ścieżka". W przeciwieństwie do protokołu RIP, OSPF charakteryzuje się dobrą skalowalnością, wyborem optymalnych ścieżek i brakiem ograniczenia skoków powyżej 15, przyspieszoną zbieżnością. Przeznaczony jest dla sieci posiadających do 500 routerów w wyznaczonym obszarze trasowania.

Właściwości:

- Trasowanie najmniejszym kosztem
- Mniejsze obciążenia łączy niż RIP
- Brak ograniczenia 15 skoków
- Szybsza zbieżność

EIGRP (cisco)

EIGRP (*ang. Enhanced Interior Gateway Routing Protocol*) – hybrydowy protokół trasowania opracowany przez Cisco Systems operujący na algorytmie wektora odległości. Jest przeznaczony do trasowania wewnątrz systemu autonomicznego (IGP). Od protokołów trasowania stanu łącza odróżnia go fragmentaryczna wiedza o strukturze sieci (zna on jedynie połączenia do swoich sąsiadów).

Cechy:

- Do przeliczania tras protokół EIGRP używa maszyny DUAL FSM (ang. Diffused Update Algorithm Finite State Machine).
- Stosowany jest on w sieciach o wielkości nieprzekraczającej 50 routerów,
- Do transportu pakietów wykorzystuje protokół Reliable Transport Protocol.
- EIGRP jest chętnie używany, ze względu na łatwą konfigurację, obsługę VLSM i krótki czas konwergencji.

Uwaga: VLSM (*ang. Variable Length Subnet Mask*) – cecha niektórych protokołów trasowania umożliwiająca podzielenie i rozróżnianie podsieci z już istniejących podsieci. VLSM umożliwia podział adresu np. klasy C (254 hosty, maska 255.255.255.0) na kilka mniejszych podsieci zawierających różne liczby hostów. Aby informacja o sieciach była dobrze rozprowadzana pomiędzy routerami, odpowiednie protokoły trasowania muszą wymieniać pomiędzy sobą pełną informację o sieciach łącznie z maskami.

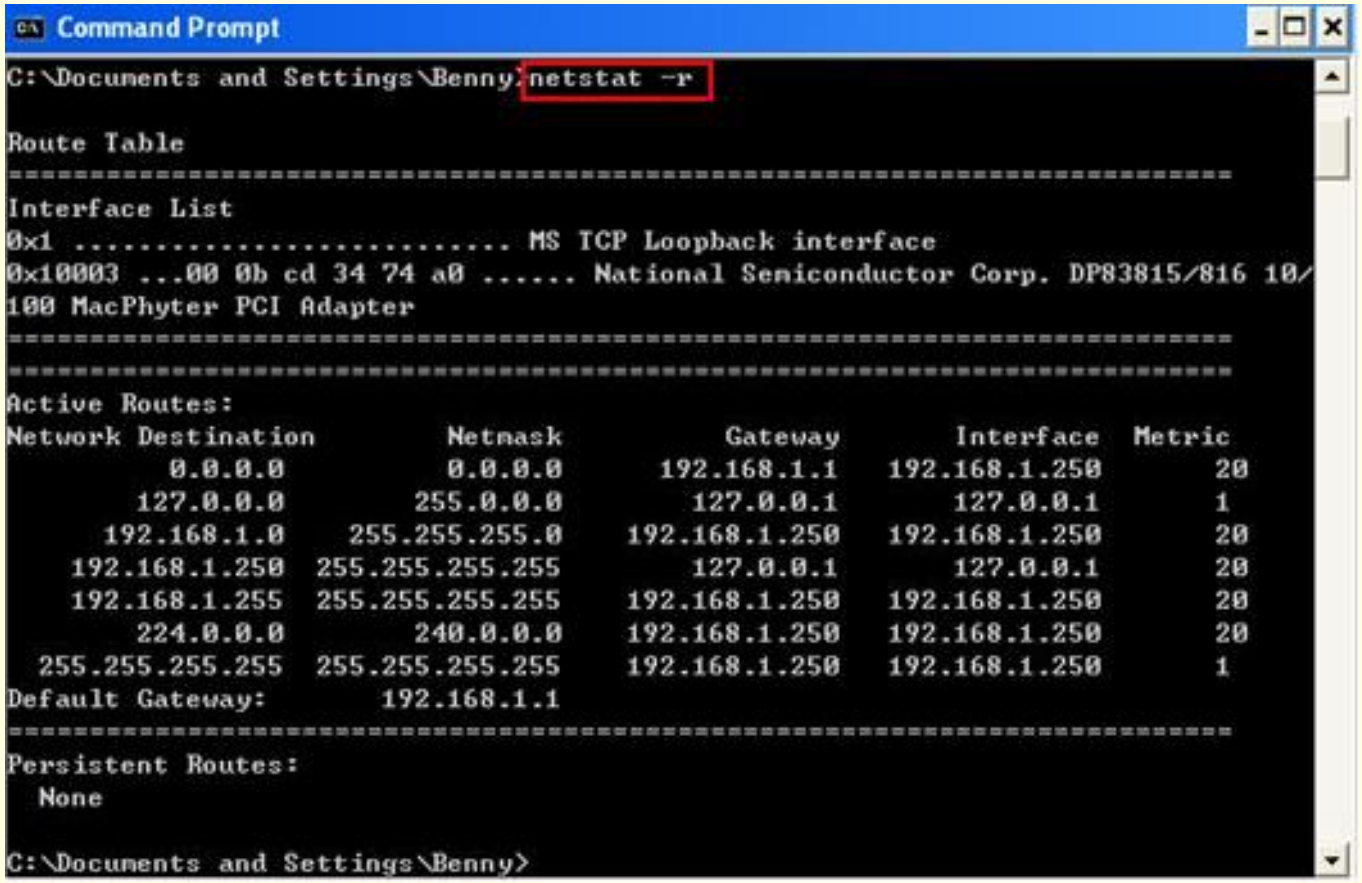
BGP

BGP (*ang. Border Gateway Protocol*) zewnętrzny protokół trasowania (routingu). BGP w wersji czwartej jest podstawą działania współczesnego internetu

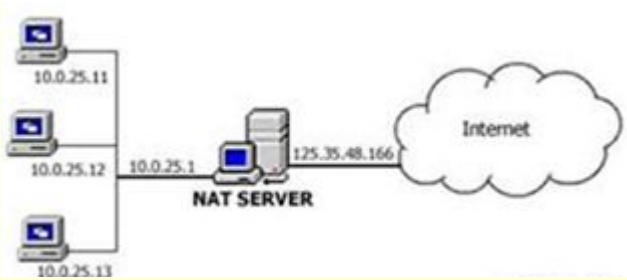
Cechy:

- Protokół wektora ścieżki;
- Używa TCP jako protokołu warstwy transportowej;
- Pełna tablica trasowania jest wymieniana tylko podczas początkowej sesji BGP;
- Aktualizacje przesyłane sa przez port TCP o numerze 179;
- Sesje BGP są utrzymywane przez wiadomości typu "keepalive";
- Każda zmiana w sieci powoduje wysłanie zawiadomienia o aktualizacji;
- BGP ma swoją własną tablicę BGP. Każda pozycja w sieci musi znaleźć się najpierw w tablicy BGP;
- BGP ma skomplikowaną tabelę atrybutów, np. sąsiedniego skoku i pochodzenia;
- Obsługuje VLSM i podsumowanie (zwane też bezklasowym trasowaniem międzydomenowym (ang. Classless Inter-Domain Routing (CIDR));

IPv4 – Tablica routingu



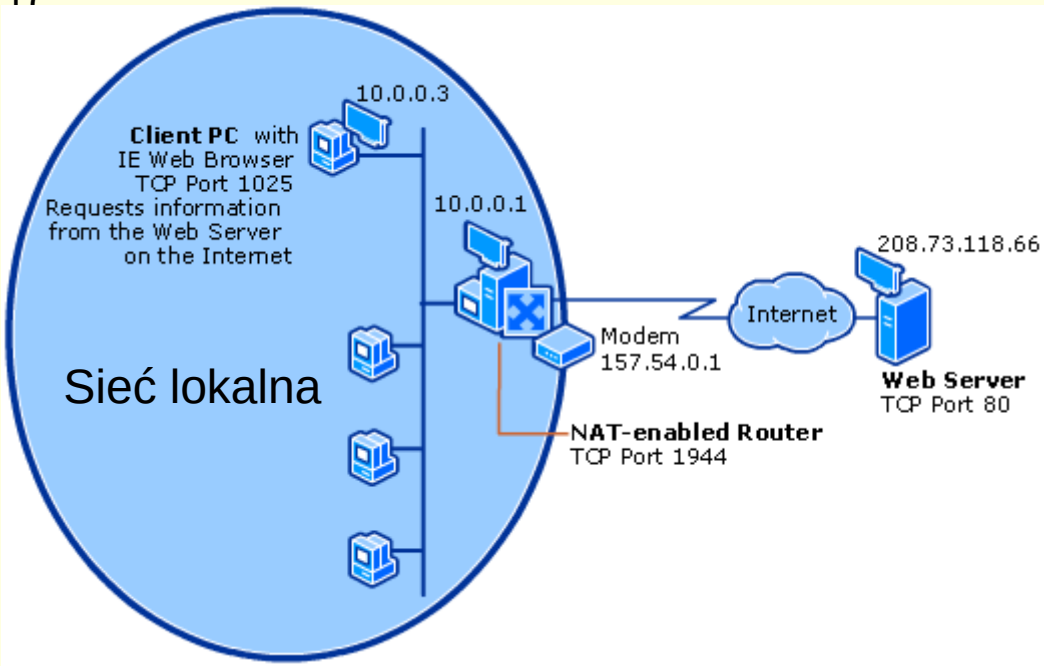
NAT



- **NAT** (*ang. Network Address Translation*) - translacja adresów sieciowych, znane również jako maskarada sieci lub maskarada IP (od ang. network/IP masquerading) – technika przesyłania ruchu sieciowego poprzez router, która wiąże się ze zmianą źródłowych lub docelowych adresów IP, zwykle również numerów portów TCP/UDP pakietów IP podczas ich przepływu.
- Daje możliwość zmapowania całej sieci (lub wielu sieci) do pojedynczego adresu IP. Większość systemów korzystających z NAT ma na celu umożliwienie dostępu wielu hostom w sieci prywatnej do Internetu przy wykorzystaniu pojedynczego publicznego adresu IP (zob. brama sieciowa).
- Jest niezbędny, gdy liczba adresów IP przydzielonych przez Dostawcę Usług Internetowych (ISP) jest mniejsza niż całkowita liczba maszyn, który mają mieć dostęp do Internetu.
- Sieci komputerowe, korzystające z adresów prywatnych, mogą zostać podłączone do Internetu przez jeden router, mający mniej adresów internetowych niż komputerów w tej sieci.
- Wykorzystuje się wolne porty, których jest 65535.

NAT

- Wszystkie komputery sieci lokalnej są widoczne w Internecie pod jednym adresem (w poniższym przykładzie 157.54.0.1). Serwer NAT wykorzystuje numery portów lokalnych do identyfikacji konkretnego komputera sieci lokalnej.
- Komputery 10.0.0.3 i 10.0.0.4 nawiązują połączenie z serwerem WWW o adresie IP: 208.73.118.66 (port docelowy dla WWW: 80) na portach źródłowych odpowiednio 1025 i 2026
- 10.0.0.3:1025 → 157.54.0.1:1944
- 10.0.0.4:2026 → 157.54.0.1:1947



Sieciowe systemy operacyjne

Sieciowy system operacyjny (*ang. network operating system*) – rodzaj systemu operacyjnego (wykorzystującego niektóre protokoły internetowe np. TCP/IP), pozwalającego na pracę w sieci komputerowej.

- **Architektura klient-serwer** – W architekturze klient-serwer pewne zadania wymagające intensywnego wykorzystania zasobów, takie jak usługi baz danych, udostępnianie stron WWW, plików, zadania wydruku, obsługa poczty itp. są realizowane przez serwer. Komputery klienckie korzystają z usług serwera poprzez sieć komputerową.
- Zarządzaniem serwerem i współpracą systemów klienckich zajmuje się administrator sieci informatycznej.

Przykładowe sieciowe systemy operacyjne:

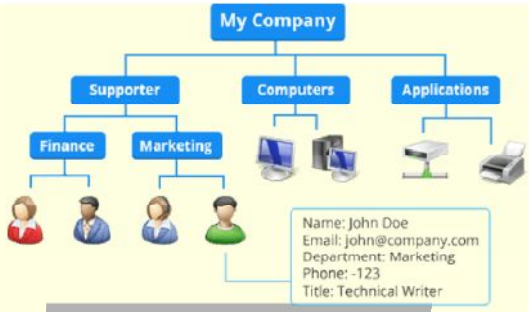
- Microsoft Windows Server (2008)
- GNU/Linux
- Novell NetWare
- Unix
- AppleTalk

Linux

Zalety: darmowy, bezpieczny, bardzo szybki, pozwala na wprowadzanie dowolnych modyfikacji

Wady: brak znanych komercyjnych pakietów narzędzi, słabe wsparcie dla niektórych podzespołów, stosunkowo trudny obsłudze w porównaniu do konkurentów

Usługa Active Directory

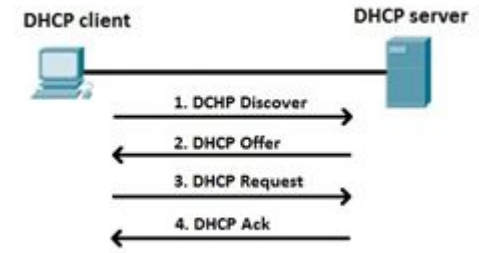


Active Directory, **AD** – usługa katalogowa (hierarchiczna baza danych) dla systemów Windows – Windows Server. Głównym powodem istnienia *Active Directory* jest uwierzytelnienie obiektów (np. użytkowników, komputerów), i autoryzacja (lub jej odmowa) dostępu do innych obiektów *Active Directory* (dowolnych, np. kontenera lub obiektu użytkownika) oraz do zasobów: w tym dyskowych, sieciowych oraz aplikacji.

Instalacja Active Directory w Windows Serwer 2008

1. **Serwer Manager → Roles → Add roles → Active Directory**
2. **Uruchom → dcpromo**. Uruchomiony zostanie kreator instalacji usług domenowych w usłudze Active Directory.
3. Utwórz nową domenę w nowym lesie – wprowadź nazwę w pełni kwalifikowaną FQDN domeny głównej.
4. Kreator usług domenowych sprawdza konfigurację serwera DNS. Jeśli nie został on zainstalowany wcześniej, zostanie teraz pobrany i skonfigurowany automatycznie.

Usługa DHCP

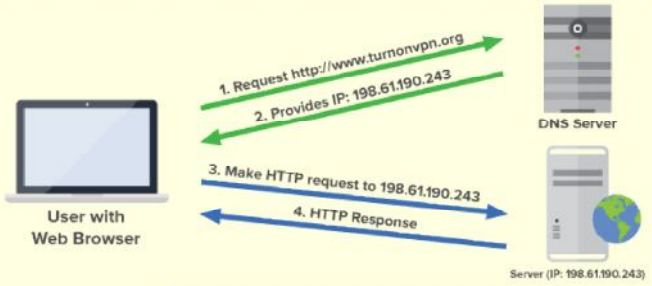


Usługa **DHCP** pozwala na automatyczne uzyskiwanie przez komputery klienckie adresów IP, co upraszcza zadanie administratorowi ponieważ nie musi on przypisywać kolejnym komputerom adresów ręcznie.

Instalacja DHCP w Windows Serwer 2008

1. **Serwer Manager → Roles → Add roles → DHCP Serwer**
2. Wybieramy interfejs, na którym usługa **DHCP** ma działać (**DHCP** ma przydzielać adres komputerom w naszej sieci wewnętrznej więc zaznaczamy tylko interfejs np. **LAN**) i klikamy **Next.** Następnie klikamy **Validate** obok adresu serwera DNS i jeśli pojawi się zielona ikona klikamy **Next.**
3. Dodajemy zakres adresów (add)
4. Wprowadzamy potrzebne dane, takie jak: **opis**, **zakres adresów**, **maskę podsieci** oraz **adres bramy** (są to dane, które również będą przydzielana dla klientów automatycznie przez serwer), zaznaczamy opcję **Activate this scope** i klikamy **OK**

Usługa DNS

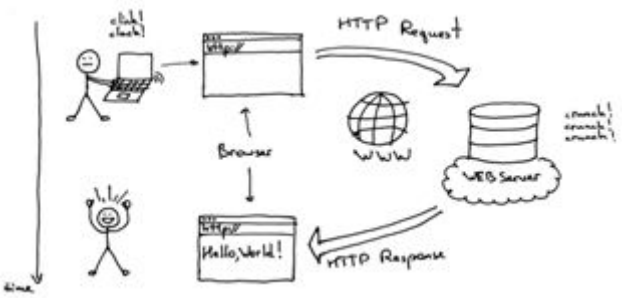


DNS – (*ang. Domain Name System)* (*pol. system nazw domenowych*) – system serwerów, protokół komunikacyjny oraz usługa obsługująca rozproszoną bazę danych adresów sieciowych. Pozwala na zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową. Dzięki DNS nazwa mnemoniczna, np. pl.wikipedia.org jest tłumaczona na odpowiadający jej adres IP, czyli 91.198.174.192.

Instalacja DNS w Windows Serwer 2008

1. **Serwer Manager → Roles → Add roles → DNS**
2. Konfiguracja DNS: **Start → Narzędzia administracyjne → DNS**
3. Tworzymy nową strefę wyszukiwania do przodu → strefa podstawowa i wprowadzamy nazwę strefy np. egzamin.pl
4. Wchodzimy teraz do nowo utworzonej strefy. Klikamy na niej PPM i wybieramy Nowy Host (A lub AAAA)
5. Wypełniamy pole domena nadrzędna np. www oraz adres IP naszego serwera

Serwer WWW



Serwer WWW obsługuje żądania protokołu komunikacyjnego HTTP lub HTTPS.

W środowisku Unix/Linux programem serwera WWW jest **apache**.

IIS (*ang. Internet Information Services*) – zbiór usług internetowych dla systemów rodziny Microsoft Windows. Obecnie pełni funkcje serwera FTP, FTPS, HTTP, HTTPS, NNTP oraz SMTP.

Instalacja IIS w Windows Serwer 2008

1. **Serwer Manager → Roles → Add roles → IIS**
2. FTP jest „usługą roli" IIS. Tak więc, w momencie, kiedy zostaniemy poproszeni o wybranie usług ról przewijamy ekran na sam dół i wybieramy opcję serwer FTP.
3. Konfigurujemy IIS: **Start → Narzędzia Administracyjne → Menedżer Internetowych Usług Informacyjnych**.
    1. Default Web Site → PPM → Ustawienia zaawansowane
    2. Witryny → PPM → Dodaj witrynę FTP.

Serwer FTP

FTP (*ang. File Transfer Protocol*) – protokół komunikacyjny typu klient-serwer umożliwiający dwukierunkowy transfer plików w układzie serwer FTP–klient FTP.

- Wykorzystuje dwa połączenia TCP – kontrolne, do przesyłania poleceń i do transmisji danych.
- **Tryb aktywny** – używa portu 21 dla poleceń (zestawiane przez klienta) i portu 20 do przesyłu danych (zestawiane przez serwer)
- **Tryb pasywny** – używa portu 21 dla poleceń i portu o numerze powyżej 1024 do transmisji danych (obydwa połączenia zestawiane są przez klienta).
- Serwer FTP, zależnie od konfiguracji, może pozwalać na anonimowy, czyli bez podawania hasła uwierzytelniającego, dostęp do jego zasobów. Najczęściej jednak serwer FTP autoryzuje każde połączenie za pomocą loginu i hasła.

Przykładowe serwery FTP:

- FileZilla (Microsoft Windows) lub element pakietu IIS (Internet Information Services)
- vsftpd (Linux)
- Pure-FTPd (Unix)

Przykładowe klienty FTP:

- Wiele nowoczesnych przeglądarek internetowych posiada wbudowane funkcje klienta FTP
- Dedykowane programy klientów: **Total Commander, FileZilla**, Konqueror

Uwaga: Większość prostych klientów FTP opiera się tylko na wpisaniu adresu serwera, nazwy użytkownika i hasła po czym możliwy jest dwustronny transfer plików przez sieć.

Polecenia powłoki

Testowanie połączenia sieciowego

- **ping**

Wyświetlenie trasy pakietu

- **traceroute** (Unix, Linux),
- **tracert** (Windows)

Konfiguracja interfejsów sieciowych

- **ifconfig** (Unix, linux),
- **ipconfig** (Windows)

Testowanie aktywnych połączeń sieciowych (stanu połączeń)

- **netstat**

Routing

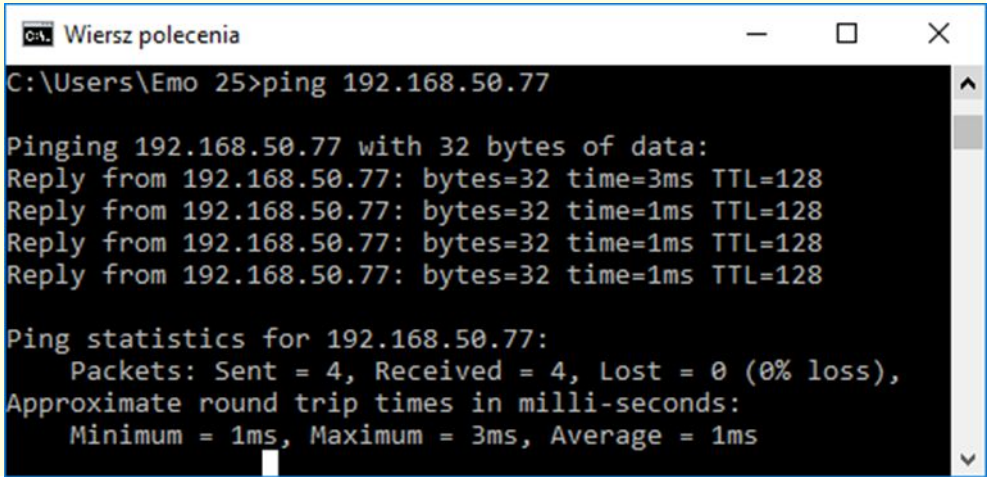
- **route**
- **ip** (Unix, Linux)

Wykonywanie operacji na grupach, użytkownikach, zasadach kont itp. (Windows).

- **net**

ping

- **ping** – polecenie używane w sieciach komputerowych TCP/IP (jak Internet) i służący do diagnozowania połączeń sieciowych. Pozwala na sprawdzenie, czy istnieje połączenie pomiędzy hostami testującym i testowanym. Umożliwia on zmierzenie liczby zgubionych pakietów oraz opóźnień w ich transmisji, zwanych lagami.
- Ping korzysta z protokołu ICMP, wysyła pakiety ICMP Echo Request i odbiera ICMP Echo Reply.
- Blokowanie wysyłania pakietów-odpowiedzi ICMP Echo Reply (stosuje się do tego celu zapory sieciowe lub filtry w routerach) jest jedną z powszechnych metod ochrony przed atakiem z sieci.
- **ping */?*** – dostępne opcje



traceroute, tracert

traceroute - program służący do badania trasy pakietów w sieci IP w systemach unixowych.

- Działanie traceroute opiera się na protokołach komunikacyjnych UDP oraz ICMP.
- Informacje o kolejnych routerach na trasie uzyskuje się w ten sposób, że ustawia się kolejne wartości pola TTL. Rutery zmniejszają TTL o jeden i gdy TTL osiągnie 0, router odrzuci pakiet wysyłając komunikat "Time Exceeded" do komputera źródłowego.

tracert - program służący do badania trasy pakietów w sieci IP w systemach Microsoft Windows.

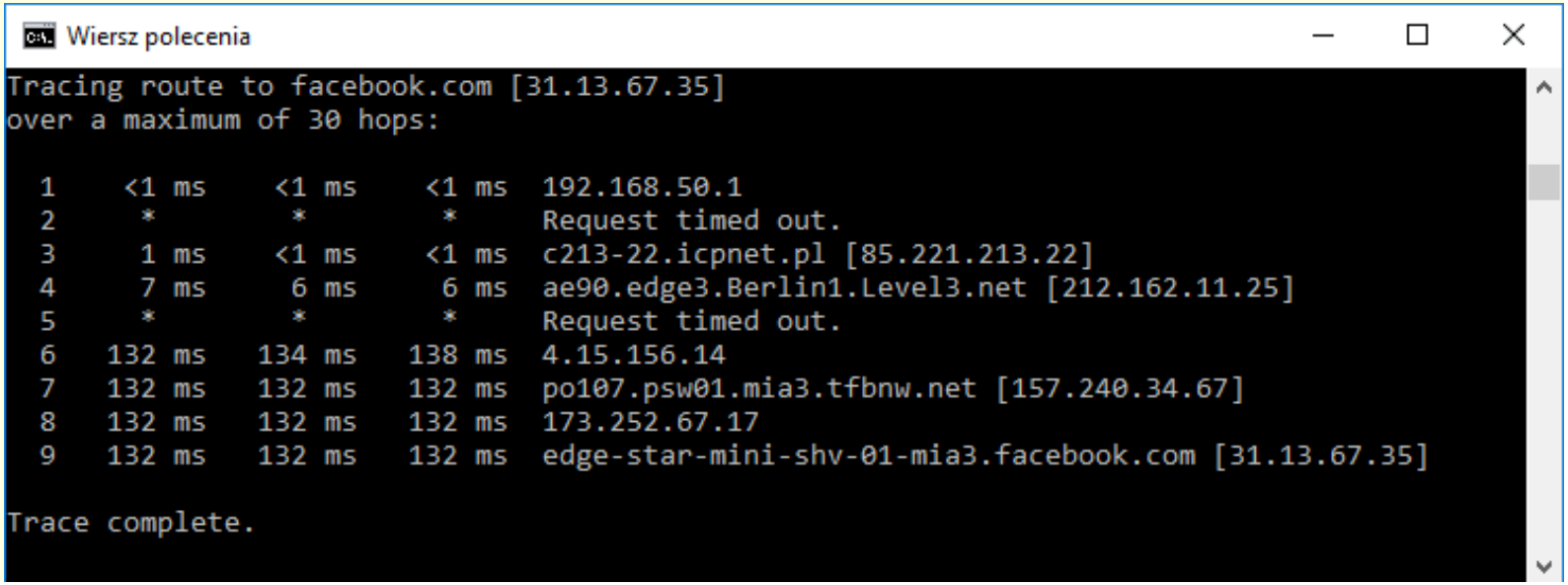
- pakiety to nie datagramy UDP, lecz komunikaty ICMP typu "Echo Request". Jeżeli taki komunikat osiągnie swoje przeznaczenie, to zawsze zostanie odesłana odpowiedź "Echo Reply".

Uwaga: Brak odpowiedzi na zadany pakiet sygnalizowany jest znakiem gwiazdki "*" i może wynikać z przeciążenia sieci, routera bądź z celowej konfiguracji urządzeń (ustawienia firewalla).

tracert facebook.com

Uwaga: Jeżeli router zostanie skonfigurowany w taki sposób, że nie zmniejsza wartości pola TTL przetwarzanych pakietów, nie będzie uwidoczniony przez traceroute, podobnie się także stanie, jeśli pakiet pokona część trasy kapsułkowany w tunelu lub sieci MPLS.

MPLS (*ang. Multiprotocol Label Switching*) – technika stosowana przez routery, w której trasowanie pakietów zostało zastąpione przez tzw. przełączanie etykiet. MPLS nazywany jest "protokołem warstwy 2,5", ponieważ korzysta z zalet warstwy 2 (modelu OSI) – wydajności i szybkości oraz warstwy 3 – skalowalności. Łącząc je, poprawia działanie usług dostarczanych w sieciach IP. Umożliwia rezerwacje pasma dla przepływu ruchu, gwarantuje rozróżnienie wymagań Quality of Service i implementowanie Virtual Private Network.



Polecenie ipconfig, ifconfig

ipconfig – polecenie w systemach operacyjnych Microsoft Windows służące do wyświetlania konfiguracji interfejsów sieciowych. Zwalnia i aktualizuje dzierżawy DHCP oraz wyświetla, rejestruje i usuwa nazwy DNS. Narzędzie pomocne przy wykrywaniu błędnego adresu IP, maski podsieci lub bramy domyślnej.

Przykłady użycia

- **ipconfig** – pokazuje skróconą informację o interfejsach
- **ipconfig /all** – pokazuje wszystkie dane interfejsów sieciowych
- **ipconfig /renew** – odnawia wszystkie dzierżawy adresu z DHCP
- **ipconfig /release** – zwalnia wszystkie dzierżawy adresu z DHCP
- **ipconfig /?** albo **ipconfig** / – wyświetla komunikat pomocy
- **ipconfig /flushdns** – czyści bufor programu rozpoznającego nazwy DNS
- **ipconfig /displaydns** – wyświetla zapamiętane tłumaczenia DNS→IP
- **ipconfig /registerdns** – aktualizuje ustawienia DNS poprzez komunikację z serwerem DNS

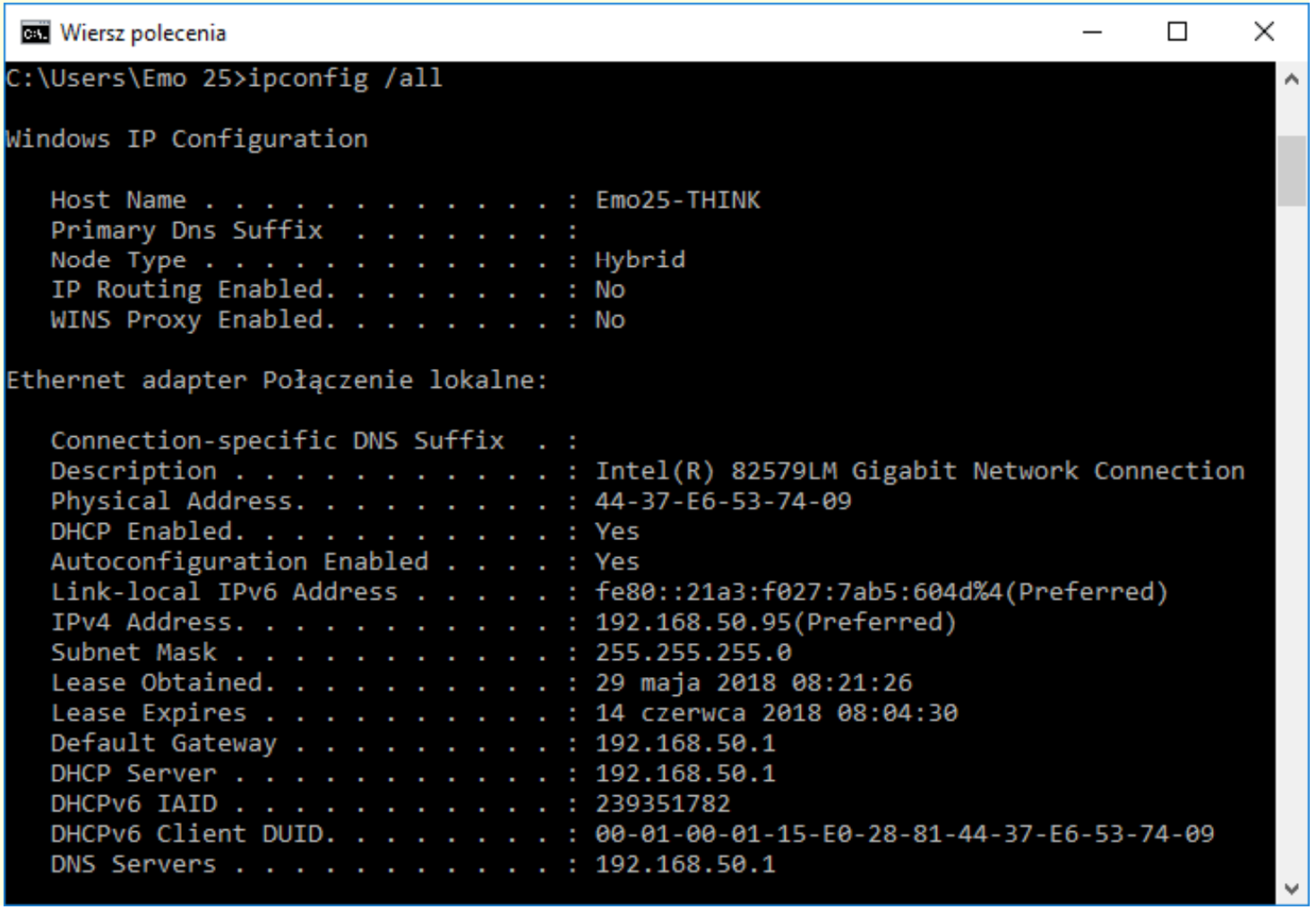
Odpowiednik w systemach UNIX to **ifconfig**.

Przykłady użycia

- **ifconfig** – wyświetla informacje o interfejsach sieciowych
- **ifconfig eth1 up** – włączenie karty sieciowej eth1
- **ifconfig eth1 down** – wyłączenie karty sieciowej eth1
- **ifconfig wlan0 69.72.169.1** – przyporządkowanie adresu 69.72.169.1 do karty wlan0
- **ifconfig eth0 192.168.2.5 netmask 255.255.255.0 broadcast 192.168.2.7**

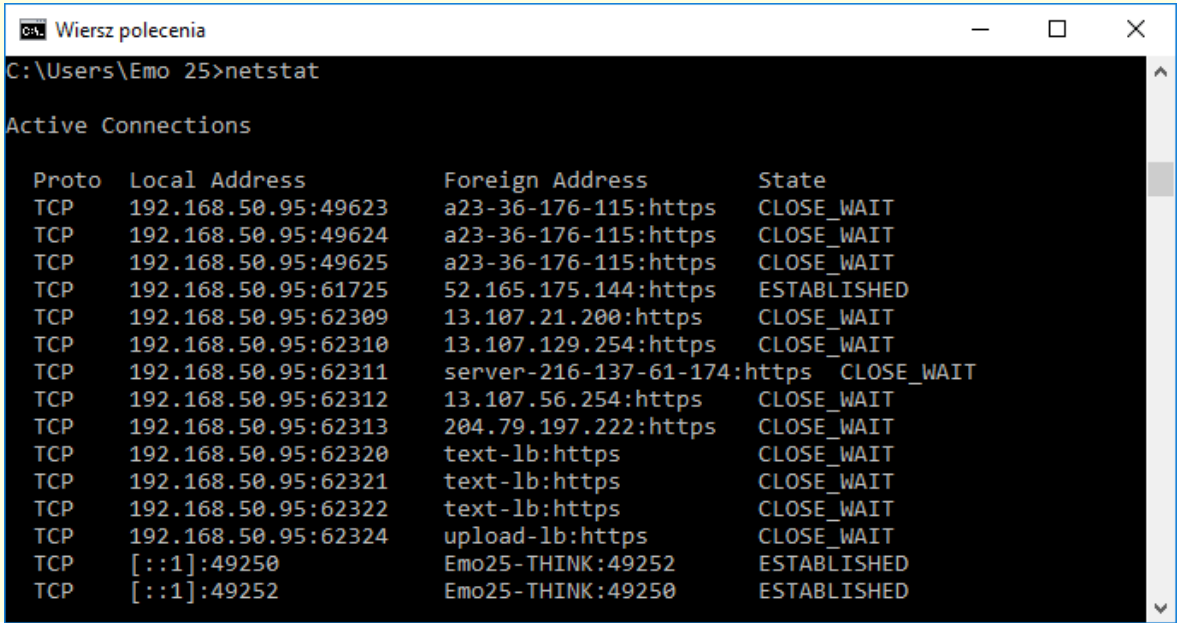
ipconfig /all

- Konfiguracja interfejsów sieciowych



Polecenie netstat

- **netstat** – jeden z najbardziej wszechstronnych i rozbudowanych programów narzędziowych odnoszących się do połączeń sieciowych. Polecenie netstat dostępne jest z linii poleceń w systemie Unix i zbliżonych oraz w systemach opartych na Windows **(Uruchom->CMD)**.
- Służy do wyświetlania aktywnych połączeń sieciowych TCP, tabeli trasowania protokołu IP, statystyki sieci Ethernet, statystyki protokołu IPv4, IPv6 oraz połączeń NAT i komunikatów netlinkowych.
- Polecenie netstat użyte bez parametrów powoduje wyświetlenie aktywnych połączeń protokołu TCP.



nestat

Składnia

- netstat [-a] [-b] [-e] [-n] [-o] [-p *protokół*] [-r] [-s] [*interwał*]

Parametry

-a – wyświetla wszystkie aktywne połączenia TCP, a także portów protokołu TCP i UDP, na których komputer nasłuchuje.

-b – (Windows XP z SP2) wyświetla wszystkie aktywne połączenia TCP, a także nazw programów używających portów protokołu TCP i UDP, na których komputer nasłuchuje.

-e – wyświetla statystykę sieci Ethernet. Można go łączyć z parametrem -s.

-n – wyświetla aktywne połączenia protokołu TCP. Adresy i numery portów są wyrażane numerycznie.

-o – wyświetla aktywne połączenia protokołu TCP, a także dołącza identyfikatory procesów (PID) poszczególnych połączeń, dzięki czemu można sprawdzić informacje o właścicielach portów dla każdego połączenia. Może być łączony z parametrami -a,-n i -p.

-p protokół – ukazuje połączenia protokołu. W tym przypadku parametr protokół może przyjmować wartości: udp, tcpv6, tcp lub udpv6. Gdy parametr -p zostanie użyty jednocześnie z parametrem -s, aby wyświetlić statystyki poszczególnych protokołów, parametr ten może przyjąć wartości: tcp, udp, icmp, udpv6, ip, tcpv6, icmpv6 lub ipv6.

-s – pokazuje oddzielne statystyki dla poszczególnych protokołów.

-r – wyświetla zawartość tabeli trasowania protokołu IP. Parametr jest odpowiednikiem polecenia route print.

interwał – umożliwia powtarzające się wyświetlenie wybranych informacji w odstępie określonej liczby sekund. Naciśnięcie klawisza CTRL+C spowoduje zatrzymanie wyświetlania informacji. Jeżeli parametr ten nie został użyty, polecenie netstat wyświetli wybrane informacje tylko raz.

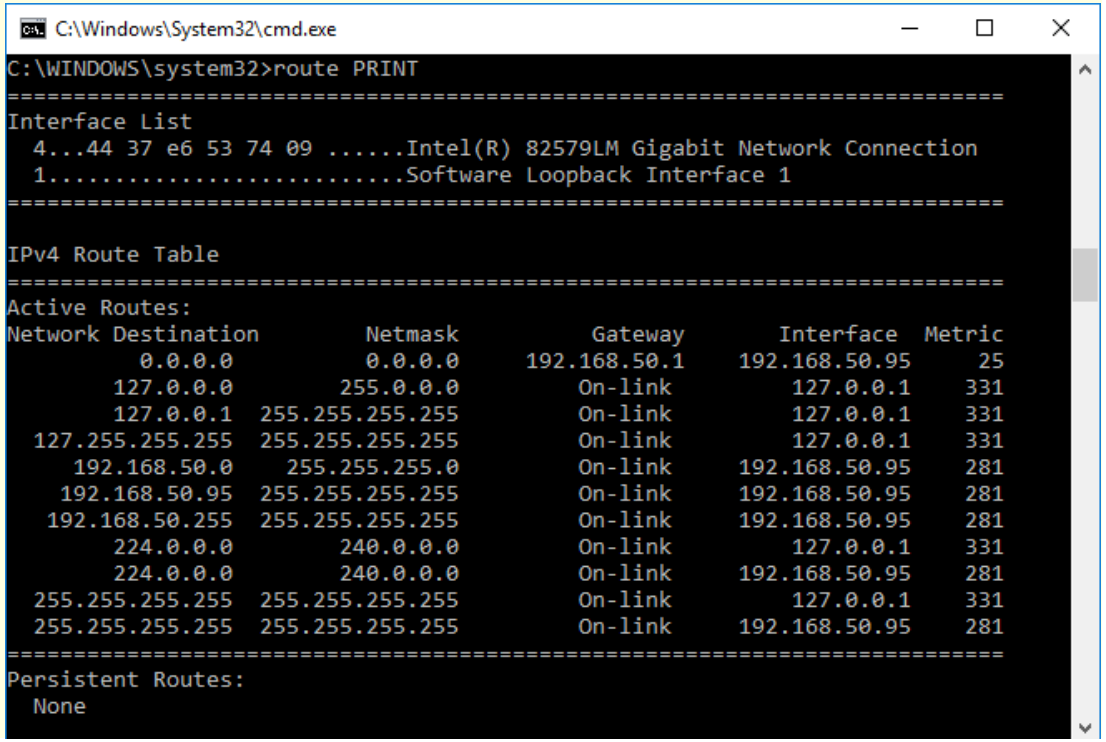
route

route – program narzędziowy w systemach uniksowych oraz Windows, który wyświetla i umożliwia zmiany tablicy trasowania pakietów sieciowych.

Parametry (Windows):

- ADD – dodaje wpis do statycznej tabeli routingu
- CHANGE – zmienia wpis w tabeli rutingu
- DELETE – usuwa wpis z tabeli rutingu
- PRINT – wyświetla tabelę rutingu

- **route /?** - pomoc



ip

ip - polecenie do konfiguracji interfejsów sieciowych, tablic tras czy tuneli w systemach operacyjnych Linux. W pełni wspiera protokoły IPv4 i IPv6, działa też z gniazdami BSD. Polecenie wchodzi w skład pakietu Iproute2 - narzędzi do zarządzania siecią i kontroli ruchu sieciowego (QoS) w systemach Linux. Iproute2 zastępuje starsze narzędzia ifconfig czy route jeszcze zachowane w dystrybucjach dla kompatybilności.

Przykłady

1. Informacje o adresach interfejsów sieciowych:

ip addr

2. Wyłączenie interfejsu eth0:

ip link set eth0 down

3. Wyświetlenie tras:

ip route

net

Polecenie **net** w systemach Windows służy do wykonywania operacji na grupach, użytkownikach, zasadach kont itp.

Przykłady użycia:

net user – ingerencja w konta użytkowników oraz wyświetlanie ich listy.

- **net user nazwa_użytkownika /add** – utworzenie nowego użytkownika.
- **net user nazwa_użytkownika hasło** – zmiana lub dodanie hasła.
- **net user nazwa_użytkownika /times:dni,godziny -** godziny oraz dni logowania
- **net user nazwa_użytkownika /del** – usuniecie konta

net use – podłacza lub odłacza komputer od udostępnianego zasobu

- **net use C: \\serwer\udzial /P:Yes** - mapowanie dysku sieciowego
- **net use X: /Delete** – usunięcie mapowanego dysku

net accounts – uaktualnia baze kont użytkowników oraz logowania dla wszystkich kont

- **net accounts /minpwlen:minimalna_ilość_znaków –** ustalenie minimalnej liczby znaków w haśle

net localgroup – modyfikuje grupy lokalne na komputerach.

- **net localgroup nazwa_grupy /add** - dodaje grupę lokalną,
- **net localgroup nazwa_grupy** - wyświetla informacje o grupie.
- **net localgroup nazwa_grupy nazwa_użytkownika /add** – dodanie użytkownika do danej grupy.
- **net localgroup nazwa_grupy /comment:"komentarz„** – dodanie komentarza
- **net localgorup nazwa_grupy /del** – usunięcie danej grupy

net share – wyświetla udziały sieciowe

Polecenia Linux

Polecenia związane z użytkownikami, grupami, loginami i zamykaniem systemu

- **shutdown** (zamykamy Linuxa)
- **adduser** (dodajemy nowego użytkownika)
- **newgrp** (dodajemy nową grupę)
- **passwd** (zmieniamy hasła)
- **logout** (wylogowanie się)
- **who** (sprawdzamy kto jest aktualnie zalogowany – też polecenia: users, w)
- **whoami** (sprawdzamy kim jesteśmy)
- **mesg** (zezwolenie na przyjmowania komunikatów)
- **write** (wysłanie wiadomości do danego użytkownika)
- **wall** (j/w tylko do wszystkich użytkowników)
- **rwall** (j/w tylko do wszystkich w sieci)
- **ruser** (wyświetla użytkowników pracujących w systemie)
- **talk** (możliwość interaktywnej rozmowy)
- **finger** (szczegółowe informacje o użytkownikach)
- **su** (zmieniamy się w innego użytkownika, lub na konto superużytkownika root)
- **chmod** (zmieniamy atrybuty/uprawnienia pliku)
- **chown** (zmieniamy właściciela pliku)
- **chgrp** (zmieniamy jaka grupa jest właścicielem pliku)

Polecenia Linux

Polecenia związane z katalogami

- ls (pokazuje nam zawartość katalogu)
- dir (okrojona wersja ls, pochodząca z msdos'a)
- pwd (pokazuje nam katalog w którym się znajdujemy)
- cd (zmieniamy katalog)
- rmdir (usuwamy katalog)
- mkdir (nowy katalog)

Polecenia związane z plikami

- cat (edytowanie tekstu)
- rm (usuwamy plik/i)

Polecenia związane z kopiowaniem i przenoszeniem, plików i katalogów

- mv (przenosimy plik lub zmieniamy jego nazwę)
- cp (kopiujemy plik)
- mvdir (przenosimy katalog lub zmieniamy jego nazwę)

Polecenia związane z procesami

- ps (pokazuje nam jakie procesy są aktualnie wykonywane)
- kill ("zabijamy" procesy)

Polecenia związane z pomocą

- help (wyświetla nam wszystkie polecenia w Linuxie)
- man (pokazuje nam pomoc do programu)

Polecenia związane z kompresją i archiwilizacją

- gzip (kompresuje nam archiwum *.gz)
- tar (archiwizuje nam archiwum *.tar)