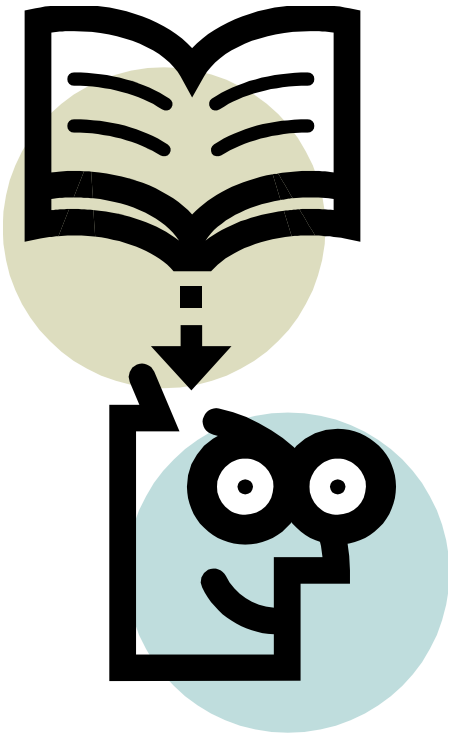
Projektowanie i Realizacja Sieci Komputerowych

Wykład 8 i 9

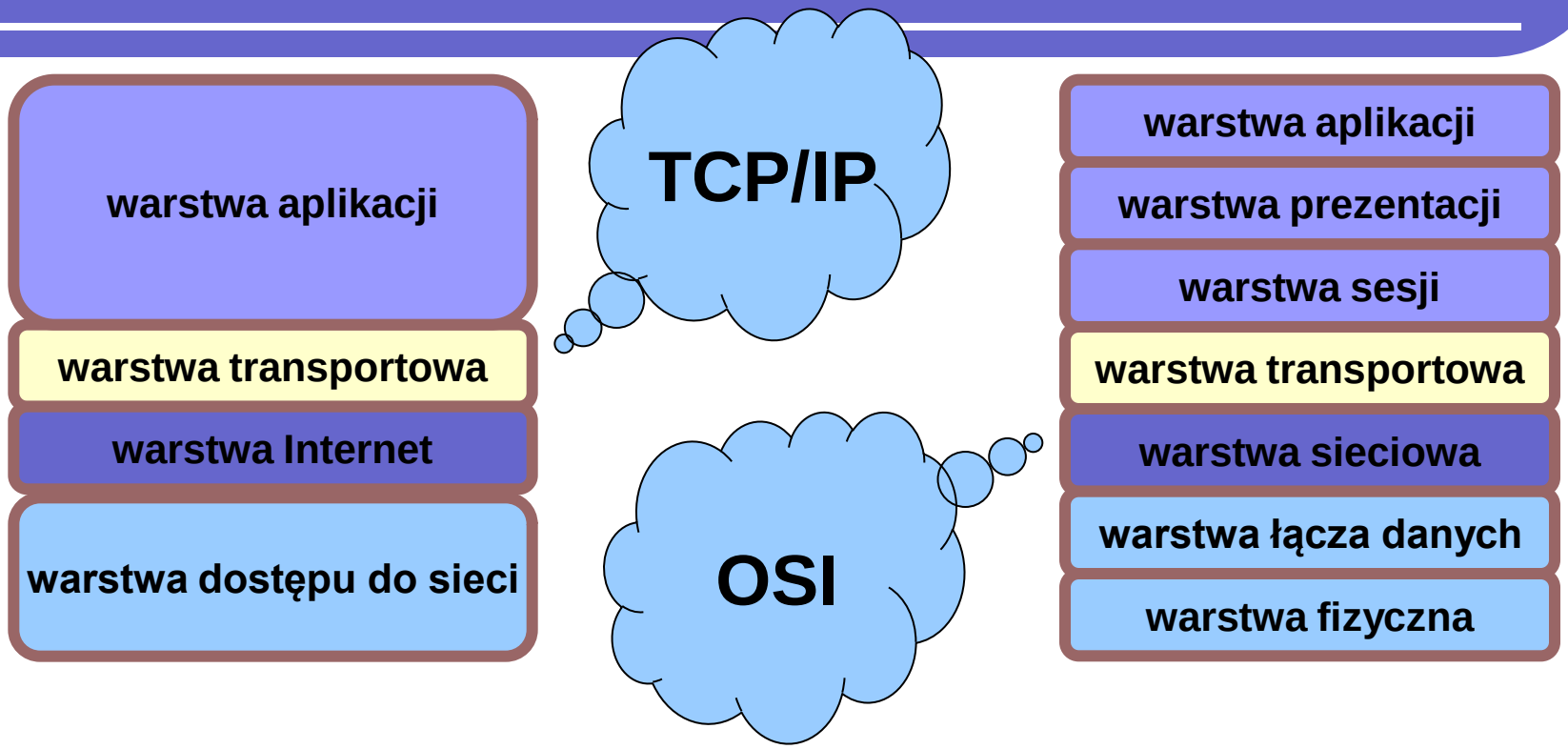
- **Zestaw protokołów TCP/IP**
- **Adresacja IP**
- **RARP, BOOTP, DHCP, ARP**
- **Protokół IP, ICMP**
- **Routing – protokoły i urządzenia**
- **Protokoły TCP i UDP**



dr inż. Artur Sierszeń asiersz@kis.p.lodz.pl

dr inż. Łukasz Sturgulewski luk@kis.p.lodz.pl

Zestaw protokołów TCP/IP



- **Warstwa dostępu do sieci**: technologie sieci LAN i WAN (np. Ethernet)
- **Warstwa Internet**: IP (*Internet Protocol*), ICMP (*Internet Control Message Protocol*)
- **Warstwa transportowa**: TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*)
- **Warstwa aplikacji**: TELNET, FTP, SMTP, DNS, SNMP, DHCP

Warstwa sieciowa – warstwa 3

- Odpowiada za transmisję bloków informacji poprzez sieć.
- Określa, jaką drogą przesyłane będą poszczególne jednostki danych (routing).
- Podstawową jednostką informacji w warstwie sieciowej jest **pakiet**.
- Umożliwia uniezależnienie warstw wyższych od transmisji danych, rodzaju technologii komutacji itp.

Definicje

- **Warstwa 3 modelu OSI:**
  Zapewnia najlepsze (jak to jest możliwe) dostarczenie pakietów od punktu początkowego (sieci źródłowej) do punktu końcowego (sieci docelowej).
- **Routing** (wyznaczanie ścieżki):

  Czynność polegająca na kierowaniu drogą przepływu pakietów informacji w sieci komputerowej.
- **Router:**

  Urządzanie (może być także program) realizujące routing. Jest to najbardziej inteligentne i zaawansowane urządzenia sieciowe instalowane w węzłach sieci.

Routing

- Routing = Wyznaczanie ścieżki pakietu.
- Wyznaczanie ścieżki to proces, który umożliwia routerowi wybranie następnego skoku w drodze pakietu do adresata.
- W tym procesie mogą być brane pod uwagę różne czynniki np.:
  - Odległość do celu;
  - Przepustowość łącza;
  - Obciążenie łącza;
  - Koszt łącza.

Routing

- **Protokół routowalny:** Protokół warstwy sieciowej dopuszczający kierowanie przepływem pakietów np. IP (*Internet Protocol*).
- **Protokół routingu:** Protokół określający sposób kierowania pakietami routowalnego protokołu sieciowego. Protokół routingu ułatwia obsługą protokołów routowalnych poprzez dostarczenie mechanizmów umożliwiających wymianę informacji o trasach (ścieżkach) np. RIP (*Routing Information Protocol*), IGRP (*Interior Gateway Routing Protocol*), EIGRP (*Enhanced Interior Gateway Routing Protocol*), OSPF (*Open Shortest Path First*).
- **Routing wieloprotokołowy:** Routery mogą obsługiwać wiele protokołów routingu oraz wiele protokołów routowalnych.

Router

- **Router pracuje w trzeciej warstwie modelu OSI.**
- Łączy ze sobą segmenty sieci lub całe sieci.
- Może łączyć sieci pracujące w różnych technologiach warstwy drugiej np.: Ethernet i Token Ring.
- Podejmuje decyzje o porcie na który zostanie przesłany pakietu na podstawie adresu grupy jednostek (adres sieci – część adresu IP) tak aby ścieżka jaką będzie poruszał się pakiet była optymalna.
- Najważniejsze (najbardziej zaawansowane) z urządzeń regulujących ruch w sieciach.
- Graficzny symbol routera:

Adresowanie płaskie i hierarchiczne

- Adresowanie płaskie:
  - Przy nadawaniu adresu jednostka otrzymuje następny wolny adres.
  - Brak struktury schematu adresowania.
  - Na przykład adres MAC.
- Adresowanie hierarchiczne:
  - Nie można przydzielać adresów losowo, na zasadzie następny wolny.
  - Przy nadawaniu adresu ważne jest położenie jednostki w strukturze.
  - Na przykład adres IP.

Adresy IP

- Główne zadania stawiane systemowi adresowania w sieciach rozległych:
  - Potrzeba globalnego systemu identyfikacji każdej jednostki przyłączonej do sieci.
  - Identyfikator ma za zadanie określić: nazwę, adres i trasę do jednostki docelowej.
- W najpopularniejszej obecnie wersji IPv4 używa się 32-bitowych adresów.
  Adres IP składa się z pary (*ids*, *idm*), gdzie:
  - *ids* – określa sieć w której znajduje się dana jednostka;
  - *idm* – określa jednoznacznie jednostkę w tej sieci.
- Adresy IP zostały podzielone na klasy (zwiększa to znacznie elastyczność tego rozwiązania). Klasa, do której należy dany adres, jest identyfikowana przez pierwsze bity adresu (analizowane do napotkania zera).

Adresy IP

Klasa	*Charakterystyka*
A	**7** bitów adres sieci **24** bity adres jednostki w tej sieci Klasa wykorzystywana w duzych sieciach
B	**14** bitów adres sieci **16** bitów adres jednostki w tej sieci Klasa wykorzystywana w srednich sieciach
C	**21** bitów adres sieci **8** bitów adres jednostki w tej sieci Klasa wykorzystywana w malych sieciach

Adresy IP

- Adres IP określa sieć oraz konkretny węzeł w tej sieci – nie jest więc związany z jednostką, ale z przyłączeniem do sieci.
- W celu ułatwienia analizy adresu IP, a także jego zapamiętania, stosuje się konwencję zapisu:

  a.b.c.d

  gdzie *a*, *b*, *c*, *d* są liczbami całkowitymi z zakresu 0-255, oznaczającymi kolejne 8 bitów z całego 32 bitowego adresu.

Przydzielanie adresów IP

- Początkowo jedyną organizacją dokonującą przydziałów numerów IP była IANA (*Internet Assigned Numbers Authority*).
- Później części przestrzeni adresowej były przekazywane w zarząd różnych lokalnych organizacji, przez które został przejęty proces przydzielania adresów IP.
- Pod adresem:

  http://www.iana.org/assignments/ipv4-address-space

  znajduje się aktualny przydział adresów IP dla organizacji i firm.

Adresy specjalne

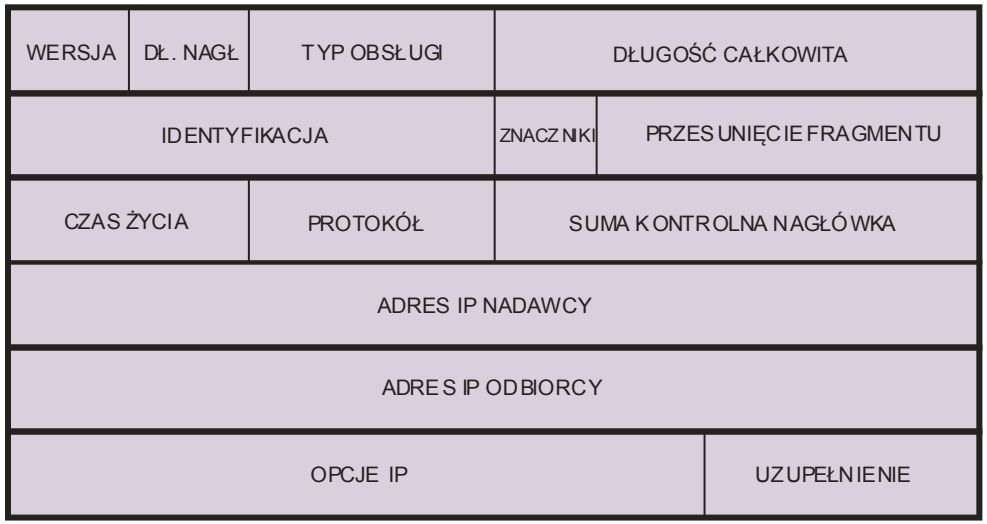
Istniej kilka kombinacji zer (bieżący) i jedynek (każdy):

- **ids = zera, idm = zera**: Dany komputer (do wykorzystania tylko w czasie rozruchu systemu).
- **ids = zera, idm = komputer**: Komputer w danej sieci (do wykorzystania tylko w czasie rozruchu systemu).
- **ids = jedynki, idm = jedynki** : Ograniczone rozgłaszanie (w sieci lokalnej). W ograniczonym rozgłaszaniu mamy możliwość wysłania pakietów do wszystkich jednostek znajdujących się w tej samej sieci lokalnej, co nadawca. Nie jest wymagana znajomość adresu sieci.
- **ids = sieć, idm = jedynki**: Ukierunkowane rozgłaszanie. Wysyłanie pakietów do wszystkich jednostek znajdujących się w sieci wyspecyfikowanej w adresie. To czy usługa zostanie zrealizowana zależy od sieci, do której wysyłamy pakiety.
- **127.0.0.1**: Pętla zwrotna. Adres pętli zwrotnej służy do testowania TCP/IP oraz komunikacji międzyprocesowej lokalnej dla danej jednostki. Oprogramowanie protokołu komunikacyjnego przekazuje pakiety z adresem pętli zwrotnej bezpośrednio jednostce bez wysyłania ich w sieć. Adresy pętli zwrotnej mają numer sieci równy 127.

Protokół IP

- W warstwie sieciowej dane są enkapsulowane w pakiety:

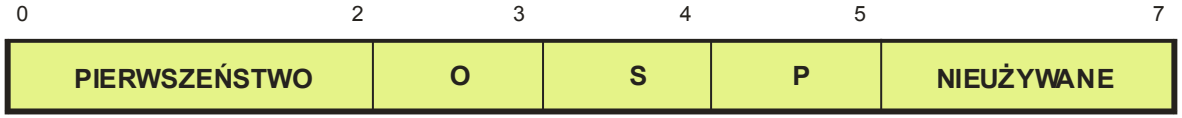
- Protokół przyjmuje dane z warstwy wyższej (transportowej), nie troszcząc się zupełnie o ich zawartość.
- Nagłówek pakietu IP:



Nagłówek pakietu IP

- **WERSJA** (4 bity): Wersja protokołu IP, z którego użyciem utworzono ten pakiet (obecnie jest to wersja czwarta).
- **DŁUGOŚĆ NAGŁÓWKA** (4 bity):

  Większość pól nagłówka ma stałą wielkość, oprócz pól OPCJE IP i UZUPEŁNIENIE. Wielkość ta określa długość nagłówka mierzoną w 32 bitowych słowach.
- **TYP OBSŁUGI** (8 bitów):



  - **Pierwszeństwo**: Pole to, pomimo iż daje duże możliwości kontroli przepływu danych, nie jest praktycznie wykorzystywane. Wartość tego pola jest liczbą całkowitą z przedziału od 0 do 7, gdzie 0 – normalny stopień ważności, a 7 – najwyższy stopień ważności (sterowanie siecią).
  - **O**: Bit oznaczający prośbę o krótkie czasy oczekiwania.
  - **S**: Bit oznaczający prośbę o przesyłanie pakietu szybkimi łączami.
  - **P**: Bit oznaczający prośbę o dużą pewność poprawnego przesłania danych.

  Uwaga: Powyższe prośby są traktowane w formie sugestii - nie mają i nie mogą mieć charakteru żądania!

Nagłówek pakietu IP

- **DŁUGOŚĆ CAŁKOWITA** (16 bitów): Całkowita długość pakietu IP mierzona w oktetach.
- Kontrola fragmentacji i składania pakietu (Fragmentacja następuje w wyniku przesyłania pakietów przez sieci o różnym MTU (*Maximum Transfer Unit*)):
  - **IDENTYFIKACJA** (16 bitów): Umożliwia identyfikacje fragmentów należących do tego samego pakietu.
  - **ZNACZNIK** (3 bity): Umożliwia kontrolę fragmentacji (pierwszy bit = 1 oznacza nie fragmentuj, młodszy bit = 1 oznacza „dalsze fragmenty").
  - **PRZESUNIĘCIE FRAGMENTU** (13 bitów): Mierzone w jednostkach 8-oktetowych. Fragmenty pakietu mogą docierać do celu w różnej kolejności, a dzięki temu polu możliwe jest prawidłowe połączenie wszystkich części.
- **CZAS ŻYCIA** (8 bitów): Określa jak długo pakiet może być transportowany w sieci. Nadawca decyduje o czasie życia a urządzenia obsługujące transmisję (*routery*) zmniejszają wartość tego parametru. W przypadku osiągnięcia zera, usuwają pakiet z sieci.
- **PROTOKÓŁ** (8 bitów): Określa protokół wyższego poziomu, który został użyty do stworzenia treści pola danych pakietu.
- **SUMA KONTROLNA NAGŁÓWKA** (16 bitów): Zapewnia kontrolę poprawności nagłówka (przy obliczaniu tego pola przyjmuje się, że suma kontrolna nagłówka równa się zero).
- **ADRES IP NADAWCY i ADRES IP ODBIORCY** (po 32 bity): Omówione wcześniej adresy IP jednostki wysyłającej i odbierającej pakiet.

Podsieci (*Subnets*)

- Czasem wymagany jest podział sieci opartej o adresy klasy A, B lub C na kilka mniejszych (lepsze gospodarowanie dostępną pulą adresów).
- Podsieć wydzielana jest poprzez zapożyczenie bitów z części hosta adresu IP.
- Minimalna ilość pożyczanych bitów: 2
- Maksymalna ilość pożyczonych bitów: 2 bity muszą zostać na część hosta.

Maska podsieci

- Określa jaka część adresu IP jest częścią sieci a jaka częścią hosta.
- Jest 32-bitową liczą, w której bity 1 oznaczają część sieci a bity 0 część hosta.
  - Zapisywana przeważnie zgodnie z notacją *a.b.c.d* gdzie a, b, c, d liczby całkowite z przedziału <0; 255>.

Maska podsieci

	Network	Subnet	Host
IP Host Address 172.16.2.120	10101100 00010000	00000010	01111000
Subnet Mask 255.255.254.0 or /23	11111111 11111111	11111110	00000000
Subnet	10101100 00010000 172 16	00000010 2	00000000 0

Maska podsieci

- 128
- 192
- 224
- 240
- 248
- 252
- 254

Metody przyznawania adresów IP

- Statyczne.
- Dynamiczne:
  - RARP
    (*Reverse address resolution protocol*)
  - BOOTP
    (*BOOTstrap protocol*)
  - DHCP
    (*Dynamic host configuration protocol*)

RARP (*Reverse address resolution protocol*)

- Ustalanie własnego adresu IP (maszyny bezdyskowe).
- Etapy uzyskiwania adresu IP:
  - Wysłanie zapytania RARP do serwera.

    Pakiet IP z zapytaniem wysyłany jest na adres 255.255.255.255.
  - Wyszukanie w bazie serwera adresu IP dla danego adresu MAC.

    Jeśli w sieci jest więcej niż jeden serwer RARP może przyjść kilka odpowiedzi.
  - Wysłanie odpowiedzi na adres MAC nadawcy.

    Jeśli nadawca nie otrzyma odpowiedzi po upływie określonego czasu wysyła ponowne zapytania.

RARP (*Reverse address resolution protocol*)

- Komunikat RARP jest umieszczany w części pakietu przeznaczonej na dane.

- Gdy w sieci jest kilka serwerów RARP:
  - Podział na serwer podstawowy i zapasowe.
  - Brak odpowiedzi z serwerów zapasowych przy pierwszym zapytaniu.
  - Opóźnianie odpowiedzi z serwerów zapasowych.

BOOTP (*BOOTstrap Protocol*)

- Protokół BOOTP jest protokołem warstwy aplikacji (używa UDP oraz IP).
- Przy wysyłania pakietów wykorzystywany jest adres rozgłaszania 255.255.255.255
- Ponieważ BOOTP używa protokołu UDP należało:
  - Wprowadzić wymóg używania w UDP sumy kontrolnej.
  - Nie fragmentować pakietów IP (ponieważ nie wszystkie jednostki mają odpowiednią ilość pamięci aby przechowywać części pakietów).
  - Umożliwić odbieranie wielu odpowiedzi z wielu serwerów (przetwarzana jest oczywiście tylko pierwsza!).
  - Zaimplementować obsługę retransmisji zapytania po upływie określonego czasu:
    - Aby unikną równoczesnych transmisji losuje się czas oczekiwania (0 – 4s).
    - Aby dodatkowo nie obciążać sieci podwaja się czas oczekiwania po każdej nie udanej retransmisji (po osiągnięciu 60s wracamy do przedziału 0 – 4s).
- Brak dynamicznej konfiguracji węzła (plik konfiguracyjny serwera BOOTP zawiera wszystkie potrzebne informacje dla każdego węzła w sieci).
- W przypadku, gdy następują częste zmiany sieci oraz gdy liczba jednostek przekracza dostępną pulę adresów IP statyczny system stosowany w BOOTP po prostu się nie sprawdza.

DHCP (*Dynamic host configuration protocol*)

- Jest kompatybilny z BOOTP (serwer DHCP może odpowiadać na komunikaty BOOTP).
- DHCP obsługuje trzy metody przyznawania adresów:
  - Statyczne (ręczne tworzenie pliku konfiguracyjnego).
  - Automatyczne przyznawanie stałego adresu dla jednostki włączającej się po raz pierwszy do sieci (dynamiczne bez ograniczeń).
  - Automatyczne przyznawanie adresu na określony czas (dynamiczne na czas).
- Jednostki są identyfikowane przez serwer po identyfikatorze, którym przeważnie jest ich adres sprzętowy.
- Sposób obsługi jednostki zależy od konfiguracji serwera.

DHCP (*Dynamic host configuration protocol*)

- Dynamiczne przyznawanie adresów, a więc możliwość obsługi dowolnego węzła, daje możliwość budowania samokonfigurujących się sieci.
- Rola administratora przy konfiguracji serwera DHCP:
  - Wyznaczanie puli adresów, z której może korzystać serwer;
  - Określenie reguł, którymi posługuje się serwer przy przyznawaniu adresów;
  - Czas, na który serwer przyznaje adres (dla szybko zmieniających się stanów sieci – krótki).

DHCP – Procedura uzyskania adresu

1. Klient startuje (stan INICJALIZUJ);
2. Klient wysyła komunikat DHCPDISCOVER (port 67, UDP);
3. Klient przechodzi w stan WYBIERZ;
4. Serwer wysyła DHCPOFFER;
5. Klient zbiera komunikaty DHCPOFFER;
6. Klient wybiera jedną z odebranych ofert (przeważnie pierwszą, jaką otrzymał);
7. Klient negocjuje w sprawie wynajęcia – komunikat DHCPREQUEST;
8. Klient przechodzi w tan PROŚBA;
9. Serwer potwierdza rozpoczęcie wynajmu adresu – wysyła DHCPACK;
10. Klient po odebraniu tego potwierdzenia przechodzi w stan POWIĄZANIE.

DHCP – Zakończenie wynajmu adresu

1. Klient wysyła komunikat DHCPRELEASE;
2. Przejście w stan INICJALIZUJ.

DHCP – Odnowienie wynajmu adresu

Będąc w stanie POWIĄZANIE klient ustawia trzy zegary:

- **Czas odnowienia:**
  1. Klient wysyła do serwera komunikat DHCPREQUEST;
  2. Klient przechodzi w stan ODNÓW;
  3. Jeśli serwer zaakceptuje prośbę klienta wysyła komunikat DHCPACK, a klient po jego odebraniu przechodzi w stan POWIĄZANIE;
  4. Jeśli serwer odrzuci prośbę klienta wysyła komunikat DHCPNACK, a klient po jego odebraniu przechodzi w stan INICJALIZUJ;
- **Czas przewiązania:**
  1. Klient przechodzi ze stanu ODNÓW do stanu PRZEWIĄŻ;
  2. Klient wysyła komunikat DHCPREQUEST do serwerów DHCP;
  3. Jeśli serwer zaakceptuje prośbę klienta wysyła komunikat DHCPACK, a klient po jego odebraniu przechodzi w stan POWIĄZANIE;
  4. Jeśli serwer odrzuci prośbę klienta wysyła komunikat DHCPNACK, a klient po jego odebraniu przechodzi w stan INICJALIZUJ;
- **Czas zakończenia:**
  1. Klient wysyła komunikat DHCPRELEASE;
  2. Przejście w stan INICJALIZUJ.

Metody ustalania adresu MAC

- Protokół ARP (*Address Resolution Protocol*) umożliwia ustalenie, na podstawie adresu logicznego IP, adresu fizycznego MAC odbiorcy, do którego mają zostać przesłane informacje.

ARP (*Address Resolution Protocol*)

- Protokół ARP umożliwia jednostce nadawcy określenie adresu MAC odbiorcy znając jedynie jego adres IP.

MAC celu MAC źródła	IP celu IP źródła	Komunikat ARP

- Etapy uzyskiwania adresu MAC:
  - Wysłanie zapytania ARP.

    Ramka z zapytaniem wysyłana jest na adres rozgłoszeniowy FF.FF.FF.FF.FF.FF.
  - Wysłanie odpowiedzi do nadawcy przez poszukiwaną jednostkę.

    Ramki odbierają wszystkie jednostki w sieci (rozgłoszenie) zaś na komunikat ARP odpowiada tylko jednostka o pasującym adresie IP.
  - Aktualizacja tablicy ARP przez jednostkę która wysłała zapytanie ARP.

    Dzięki tablicy ARP jednostka nie musi przed wysłaniem każdej ramki wyznaczać ponownie adresu MAC.

ICMP (*Internet Control Message Protocol*)

- Protokół ICMP jest częścią protokołu IP i służy do przekazywania informacji o sytuacjach wyjątkowych.
- Powstał z myślą o udostępnieniu routerom mechanizmu powiadamiania węzłów o przyczynach problemów w dostarczeniu pakietów do celu. Jednak może być wykorzystany do komunikacji pomiędzy dwoma dowolnymi węzłami w sieci.
- Komunikaty ICMP są wysyłane do pierwotnego nadawcy, który musi otrzymaną wiadomość, zinterpretować i podjąć odpowiednie kroki w celu wyeliminowania błędów.
- Komunikat ICMP jest przesyłany przez sieć w części danych pakietu IP (mimo to nie jest on protokołem wyższego poziomu, lecz stanowi rozszerzenie protokołu IP).
- Komunikat o błędzie nie jest tworzony, jeśli błąd powstał przy przesyłaniu komunikatu ICMP.

Typy komunikatów

- Prośba o echo,
- Odbiorca nieosiągalny,
- Tłumienie nadawcy,
- Zmień trasowanie,
- Przekroczenie czasu,
- Inne kłopoty,
- Prośba o czas,
- Prośba o maskę adresową.

Budowa komunikatu ICMP

Każdy komunikat ICMP ma swój własny format.

Jednak istnieje kilka cech wspólnych.

Pierwsze pola komunikatu są takie same:

- TYP (8 bitów) – Identyfikator typu komunikatu;
- KOD (8 bitów) – Dalsze informacje na temat rodzaju komunikatu;
- SUMA KONTROLNA – odnosi się wyłącznie do komunikatu ICMP i jest obliczana wg tych samych reguł, co w przypadku IP.

Prośba o echo

Pomyślna odpowiedź tzw. „odpowiedź z echem” oznacza, że komunikacja między węzłami funkcjonuje prawidłowo.

TYP (8 lub 0)	KOD	SUMA KONTROLNA
IDENTYFIKATOR		NUMER KOLEJNY
DANE		
...		

- TYP: 8 – prośba o echo, 0 – odpowiedź z echem;
- IDENTYFIKATOR – umożliwia powiązanie próśb i odpowiedzi przez nadawcę;
- NUMER KOLEJNY – umożliwia powiązanie próśb i odpowiedzi przez nadawcę;
- DANE – te same dane są w prośbie i odpowiedzi z echem.

Odbiorca nieosiągalny

Wysyłane przez router, jeśli nie jest on w stanie nic dalej zrobić z pakietem (router wysyła komunikat ICMP i traci pakiet).

TYP (3)	KOD (0 – 12)	SUMA KONTROLNA
ZERO (nieużywane)		
Nagłówek oraz pierwsze 64 bity pakietu, który spowodował błąd.		
...		

Tłumienie nadawcy

Komunikat wysyłany przez router w celu powiadomienia nadawcy o zbyt dużym obciążeniu napływającymi pakietami.

TYP (4)	KOD (0)	SUMA KONTROLNA
ZERO (nieużywane)		
Nagłówek oraz pierwsze 64 bity pakietu, który spowodował błąd.		
...		

Zmień trasowanie

Komunikat przesyłany z routera do węzła znajdującego się w tej samej sieci i próbującego wysyłać pakiety przez powyższy router podczas gdy istnieje bardziej optymalna droga.

TYP (5)	KOD (0 – 3)	SUMA KONTROLNA
ADRES ROUTERA (zapewniającego bardziej optymalną obsługę)		
Nagłówek oraz pierwsze 64 bity pakietu, który spowodował błąd.		
...		

Przekroczenie czasu

Router porzuca pakiet, gdy licznik czasu jego życia został wyczerpany, oraz wysyła komunikat ICMP „przekroczenie czasu” (KOD 0).

Ten sam komunikat jest wysyłany, gdy zostanie przekroczony czas na składanie fragmentów pakietu w węźle (KOD 1).

TYP (11)	KOD (0 – 1)	SUMA KONTROLNA
ZERO (nieużywane)		
Nagłówek oraz pierwsze 64 bity pakietu, który spowodował błąd.		
...		

Inne kłopoty

Komunikat „inne kłopoty” jest wysyłany przez router gdy stwierdzi np. błędy w nagłówku pakietu.

TYP (12)	KOD (0 – 1)	SUMA KONTROLNA
WSKAŹNIK	ZERO (nieużywane)	
Nagłówek oraz pierwsze 64 bity pakietu, który spowodował błąd.		
...		

- WSKAŹNIK – wskaźnik do oktetu, który spowodował błąd (KOD 0). Jeśli brakuje jakiejś opcji pole WSKAŹNIK nie jest wypełniane tylko zwracany jest KOD 1.

Prośba o czas

Komunikat „prośba o czas” umożliwia synchronizację zegarów i szacowanie czasu przesyłania pakietów.

TYP (13 – 14)	KOD (0)	SUMA KONTROLNA
IDENTYFIKATOR		NUMER KOLEJNY
CZAS POCZĄTKOWY (wypełnia pierwotny nadawca przed wysłaniem)		
CZAS OTRZYMANIA (wypełnia odbiorca tuż po otrzymaniu)		
CZAS ODESŁANIA (wypełnia odbiorca tuż przed wysłaniem odpowiedzi)		

Prośba o maskę adresową

Jednostka wysyła do routera to zapytanie, aby ustalić maskę podsieci.

TYP (17 – 18)	KOD (0)	SUMA KONTROLNA
IDENTYFIKATOR		NUMER KOLEJNY
MASKA ADRESOWA		

Domyślna brama (*default gateway*)

- Jeśli komunikacja ma przebiegać pomiędzy jednostkami znajdującymi się w różnych sieciach należy podać adres IP bramy domyślnej (interfejsu routera).
- Protokół ARP umożliwia pozyskanie informacji o adresie MAC bramy.
- Wysyłany pakiet zawiera adres IP nadawcy, adres IP końcowego odbiorcy, ramka zaś adres MAC nadawcy oraz adres MAC bramy.

Routing

- **Protokół routowalny:** Protokół warstwy sieciowej dopuszczający kierowanie przepływem pakietów np. IP (*Internet Protocol*), IPX, AppleTalk .
- **Protokół routingu:** Protokół określający ścieżki, po których będą się poruszać pakiety protokołu routowalnego w drodze do jednostki docelowej np. RIP (*Routing Information Protocol*), IGRP (*Interior Gateway Routing Protocol*), EIGRP (*Enhanced Interior Gateway Routing Protocol*), OSPF (*Open Shortest Path First*).
- **Routing wieloprotokołowy:** Routery mogą obsługiwać wiele protokołów routingu oraz wiele protokołów routowalnych.

Adres sieciowy

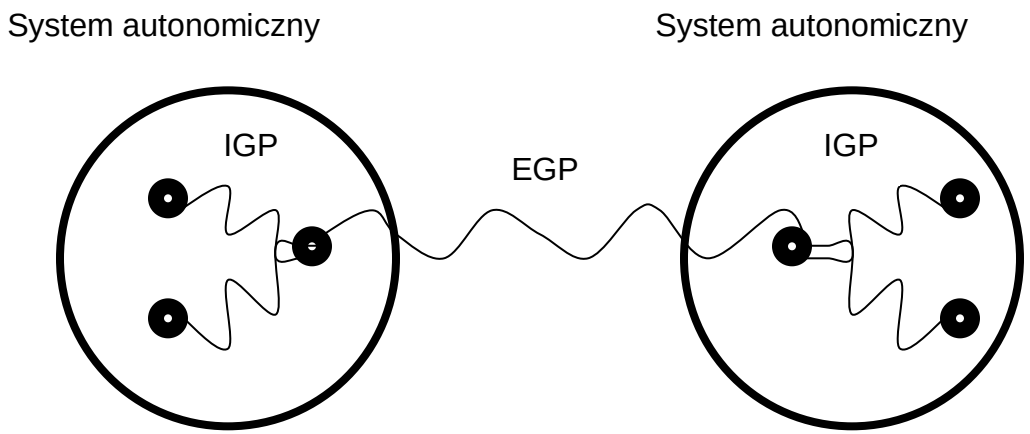
Adres sieciowy składa się z dwóch części:

- **sieci**: służy do identyfikacji sieci;
- **hosta**: służy do identyfikacji jednostki w danej sieci.

- Część sieciowa adresu wykorzystywana jest przez router do podjęcia decyzji o wyborze właściwej ścieżki.
- Spójny schemat adresowania (adresy IP obowiązujące w warstwie trzeciej modelu OSI) ułatwia znalezienie właściwej ścieżki do odbiorcy (bez korzystania z transmisji rozgłoszeniowej).

System autonomiczny

- Każdy zbiór sieci i routerów zarządzany przez jedno ciało jest uważany za pojedynczy system autonomiczny.
- W ramach systemu autonomicznego istnieje swobodny wybór wewnętrznej architektury wyznaczania tras.
- Do przekazywania informacji o osiągalności innym systemom wydelegowany jest jeden bądź kilka routerów.



Routing statyczny

- Ręczne ustalanie tras przez administratora.
- Dobry w sieciach wolno zmieniających się.
- Przydatny ze względu na bezpieczeństwo – możliwość ukrycia części sieci czyli decyzji, które informacje mają być rozgłaszane.
- Przydatny gdy przy dostępie do sieci wykorzystywana jest tylko jedna ścieżka.
- Brak odporności na błędy (utrudnione korzystanie ze ścieżek alternatywnych).
- Zupełnie nie zdaje egzaminu w rozbudowanych szybko zmieniających się sieciach.

Routing dynamiczny

- Administrator ustala konfigurację inicjującą routing dynamiczny.
- Informacje o trasach są wymieniane pomiędzy urządzeniami, które automatycznie dokonują zmian w swoich tablicach routingu.
- Następuje automatyczne dostosowywanie się do zmian w topologii sieci.

Tablica routingu

Przykładowa tablica routingu:

Cel	Następny router	Odległość	Liczniki czasowe	Flagi
Sieć A	Router 1	3	t1, t2, t3	x, y
Sieć B	Router 2	5	t1, t2, t3	x, y
...	...	...	...	...

Trasa domyślna

- Trasą domyślną są wysyłane pakiety dla których kolejny skok nie jest znany (brak wpisu w tablicy routingu).
- Trasa domyślna jest definiowana na sztywno (statycznie) przez administratora.

Metryki

Metryki – umożliwiają określanie najlepszej ścieżki do sieci – tylko routing dynamiczny.

- Tablica routingu powinna zawierać „najlepsze” informacje, stąd każda ścieżka ma swoją metrykę określającą jej „dobroć”. Generalnie im metryka mniejsza tym ścieżka lepsza.
- Do wyznaczenia metryki można używać kilku cech charakterystycznych dla ścieżek:
  - Długość ścieżki (liczba skoków) – liczba routerów które musi przebyć pakiet w drodze do sieci docelowej;
  - Niezawodność – stopa błędu łącza w sieci;
  - Opóźnienie – czas potrzebny do przesłania pakietu od nadawcy do odbiorcy;
  - Pasmo (przepustowość) – szerokość łącza;
  - Obciążenie – obciążenie danej ścieżki (łącza, routerów);
  - Koszt transportu – wartość przypisywana przez administratora określająca koszt przesłania danych.

Cele protokołów routingu

- Prostota.
- Małe obciążenie sieci (dodatkowym ruchem).
- Odporność na zakłócenia, stabilność.
- Szybka zbieżność (stan, w którym wszystkie routery wykorzystują te same informacje o stanie sieci).
- Elastyczność, adaptacyjność do zmiennych warunków sieci.

Algorytmy routingu

- **Wektor odległości** (*distnace vector*) (algorytm Bellmana-Forda): Określa kierunek i odległość do danej sieci.
- **Stan łącza** (*link state*): Metoda najkrótszej ścieżki – router tworzy i przechowuje bazy danych dotyczących topologii partycji sieci, w której się znajduje (zna wszystkie routery pośrednie w drodze do celu).
- **Hybrydowy**: Stanowi połączenia algorytmu wektor odległości oraz stan łącza.

Wektor odległości (*distance vector*)

- Routery wysyłają własne tablice routingu do sąsiadów, a ci na podstawie otrzymanych informacji dokonują aktualizacji swoich tablic routingu.
- Każda sieć w tablicy routingu ma wektor zakumulowanej odległości, który mówi jak daleko jest w danym kierunku do wybranej sieci. Jeśli sieć jest bezpośrednio przyłączona do routera to odległość wynosi 0.
- Zmiana konfiguracji sieci pociąga za sobą konieczność uaktualnienia tablic routingu, postępując krok po kroku od routera do routera.

Wektor odległości (*distance vector*)

- **Problemy**:
  - Pętle routingu: Pojawiają się, gdy zbieżność protokołu routingu jest zbyt wolna.
  - Liczenie do nieskończoności: występuje na skutek pojawienia się pętli routingu. Każde przejście pakietu przez kolejny router powoduje zwiększenie wektora odległości. Jeśli sieć docelowa jest niedostępna i pojawiła się pętla routingu, pakiet może krążyć w sieci w nieskończoność a wartość wektora odległości będzie rosła do nieskończoności.
- **Rozwiązania**:
  - Maksymalna liczba skoków (metryka): Po osiągnięciu tej wartości sieć docelowa uważana jest za niedostępną.
  - Podzielony horyzont (*split horizon*): Informacje o trasie nie są wysyłane z powrotem do miejsca, z którego one pochodzą.
  - Liczniki wstrzymania: Gdy przybędzie informacja o niedostępności sieci uruchamiany jest licznik wstrzymania. Po upływie czasu wstrzymania sieć oznaczana jest jako niedostępna. Jeśli przed upływem czasu router otrzyma lepszą ofertę licznik wstrzymania jest usuwany i nowa ścieżka jest zapamiętywana. Jeśli otrzymana oferta będzie gorsza od istniejącej nic się nie dzieje.

Stan łącza (*link state*)

- Metoda najkrótszej ścieżki – router tworzy i przechowuje bazy danych dotyczących topologii partycji sieci, w której się znajduje (zna wszystkie routery pośrednie w drodze do celu).
- Routing stanu łącza korzysta z:
  - Ogłoszeń stanu łącza LSA (*Link State Advertisement*);
  - Topologicznej bazy danych;
  - Algorytmu najkrótszej ścieżki - SPF (*Shortest Path First*);
  - Drzewa SPF;
  - Tablicy routingu ścieżek i portów prowadzących do sieci docelowych.

Stan łącza (*link state*)

- **Problemy**:
  - Przetwarzanie: Modyfikowanie tablicy routingu, wykorzystując protokół stanu łącza, wymaga dość skomplikowanych obliczeń.
  - Zapotrzebowanie na pamięć: Przechowywanie wszystkich informacji potrzebnych do tworzenia tablicy routingu wymaga dużej ilości pamięci.
  - Zapotrzebowanie na pasmo: Pierwotna operacja odkrywania struktury sieci wymaga wysłania dużej ilości pakietów LSA, co może obciążyć łącza sieci. W stanie zbieżności pakietów jest znacznie mniej.
  - Uaktualnianie stanu łącza: Aby routing działał prawidłowo (generacja prawidłowych tras) wszystkie routery muszą otrzymywać niezbędne (w prawidłowej kolejności) pakiety LSA.
- **Rozwiązanie**:

  Mechanizm stanu łącza:
  - Zmniejszenie liczby wysyłanych pakietów w stanie zbieżności.
  - Uaktualnienia mogą być wysyłane do grup. W grupie znajduje się jeden przedstawiciel, który przechowuje spójne dane o topologii sieci.
  - Wprowadzenie struktury hierarchicznej routerów (w dużych sieciach).
  - Wprowadzenie mechanizmów koordynacji uaktualnień: znaczniki czasu, mechanizmy starzenia i inne.

Hybrydowy

- Stanowi połączenia algorytmu wektor odległości oraz stan łącza.
- Do wyznaczenia najlepszej trasy wykorzystywany jest algorytm wektor-odległość, jednak uaktualnienia tabeli routingu następuje dopiero w wyniku zmiany konfiguracji sieci.

Protokół RIP (*Routing Information Protocol*)

RIP został opracowany przez firmę *Xerox Network Systems*. Swoją dużą popularność zawdzięcza programowi (demonowi Unix'owemu) *routed* opracowanemu w *University of California* w *Berkeley*. Ponieważ *routed* wchodzi w skład wielu systemów Unix'owych, stał się w sposób naturalny najczęściej stosowanym programem tego typu.

Główne zadania realizowane przez *routed*:

- Zapewnienie niesprzeczności informacji o trasach oraz informacji o osiągalności między jednostkami;
- Zapewnienie szybkiego rozgłaszania informacji o stanie i konfiguracji sieci.

Protokół RIP (*Routing Information Protocol*)

Protokół RIP jest implementacją algorytmu wyznaczania tras wektor-odległość. Jednostki uczestniczące w procesie podzielone są na dwie grupy:

- Czynne: Jednostki oferujące informacje o trasach innym jednostkom (są to wyłącznie routery). Rozgłaszanie odbywa się co 30 sekund;
- Bierne: Jednostki nasłuchujące informacji od jednostek czynnych, same niczego nie oferują.

Zarówno jednostki czynne jak i bierne odbierają rozgłaszane komunikaty i modyfikują własne tabele tras (algorytm wektor-odległość).

Protokół RIP (*Routing Information Protocol*)

- Rozgłaszane komunikaty zawierają pary: adres sieci i odległość do tej sieci.
- Odległość w protokole RIP określa się używając liczby etapów, która oznacza liczbę routerów, przez które musi przejść pakiet, aby dotarł do omawianej podsieci (łatwo się domyśleć, że minimalna liczba routerów nie oznacza optymalnej, najszybszej drogi do celu).
- W przypadku dużej ilości wymienianych informacji mogłaby zaistnieć sytuacja częstych zmian tras, dlatego trasy modyfikowane są tylko wtedy, gdy jednostka uzyska lepszą ofertę.

Protokół RIP (*Routing Information Protocol*)

- Stosowane liczniki czasowe:
  - *routing update timer* (30 sekund): Częstotliwość rozsyłania informacji o routingu;
  - *route invalid timer* (90 sekund): Czas po upływie, którego możemy przypuszczać, że trasa jest nieaktualna jeśli jednostka nie otrzyma ponowienia jej oferty;
  - *route flush timer* (270 sekund): Czas po upływie, którego nastąpi wykasowanie informacji o trasie jeśli jednostka nie otrzyma ponowienia jej oferty.

Protokół RIP (*Routing Information Protocol*)

Trzy główne problemy, z jakimi można się spotkać korzystając z protokołu RIP:

- Brak automatycznego wykrywania zapętleń w trasowaniu;
- Ograniczenie maksymalnej liczby etapów, jakie przebywa komunikat do 16 w celu uniknięcia niestabilności;
- Powolna zbieżność lub naliczanie do nieskończoności (dzięki ograniczeniu ilości etapów do 16 częściowo rozwiązano ten problem).

Protokół RIP (*Routing Information Protocol*)

Format komunikatów.

Wyróżniamy dwa główne typy komunikatów (ich struktura jest dokładnie taka sama):

- Komunikaty z informacjami o trasach;
- Komunikaty z prośbami o informacje.

Typ pola	*Długość pola*	*Funkcja*
A	1 bajt	**KOMENDA** – zapytanie lub odpowiedź o część lub całą tablicę routingu.
B	1 bajt	**NUMER WERSJI RIP**
C	2 bajty	**POLE ZEROWE**
D	2 bajty	**IDENTYFIKATOR SIECI** – dla IP przyjmuje wartość 2.
C	2 bajty	**POLE ZEROWE**
E	4 bajty	**ADRES IP SIECI DOCELOWEJ**
C	4 bajty	**POLE ZEROWE**
C	4 bajty	**POLE ZEROWE**
F	4 bajty	**METRYKA** – liczba routerów na drodze do celu.
Uwaga: Pozycje od D do F mogą się powtórzyć do 25 razy.		

Protokół OSPF (*Open Shortest Path First*)

- Protokół OSPF jest oparty na algorytmie stanu łącza, został opracowany w grupie roboczej *Internet Engineering Task Force*.
- Jak sama nazwa wskazuje protokół ten ma charakter otwarty tzn. każdy użytkownik ma dostęp do pełnej dokumentacji oraz może go implementować we własnych rozwiązaniach bez wnoszenia jakichkolwiek opłat licencyjnych.
- Jest to jeden z nielicznych protokołów, które wykorzystują **trasowanie zależne od typu obsługi**. Można zdefiniować wiele tras prowadzących do tego samego celu. Wybór pomiędzy nimi będzie zależał od pola **typ obsługi** w nagłówku pakietu IP.
- Jest to jeden z nielicznych protokołów, które wykorzystują **mechanizm równomiernego obciążenia**. Jeśli istnieje kilka tras o tym samym koszcie to ruch zostanie rozłożony równomiernie pomiędzy nimi.

Protokół OSPF (*Open Shortest Path First*)

- Umożliwia podział zasobów sieci na niezależne **obszary**. Dzięki temu wiele grup może brać razem udział przy wyznaczaniu tras. Grupy mogą wewnętrznie dokonywać zmian topologii bez informowania innych.
- Umożliwia wybranie jednego routera zwanego **wyróżnionym routerem**, który odpowiedzialny jest wysyłanie komunikatów o wszystkich łączach i routerach w sieci za którą jest odpowiedzialny.
- Umożliwia wymianę informacji, które przybyły z innych ośrodków (zewnętrznych). Format komunikatów pozwala odróżnić informacje otrzymane z zewnętrznych obszarów od tych wewnętrznych.
- Przy wymianie informacji o routingu między urządzeniami wymagane jest **uwierzytelnianie**.

Warstwa transportowa – warstwa 4

- Najważniejsza zadania warstwy transportowej:
  - Transport i regulacja przepływu informacji pomiędzy nadawcą i odbiorcą.
  - Niezawodny i przezroczysty transfer danych między punktami końcowymi (hostami).
  - Kontrola transmisji oraz wykrywanie błędów transmisji.
- Jednostką informacji na poziomie warstwy transportowej jest **segment**.
- Niezawodność połączenia w warstwie transportowej realizuje się wyłącznie środkami programowymi.

Warstwa transportowa

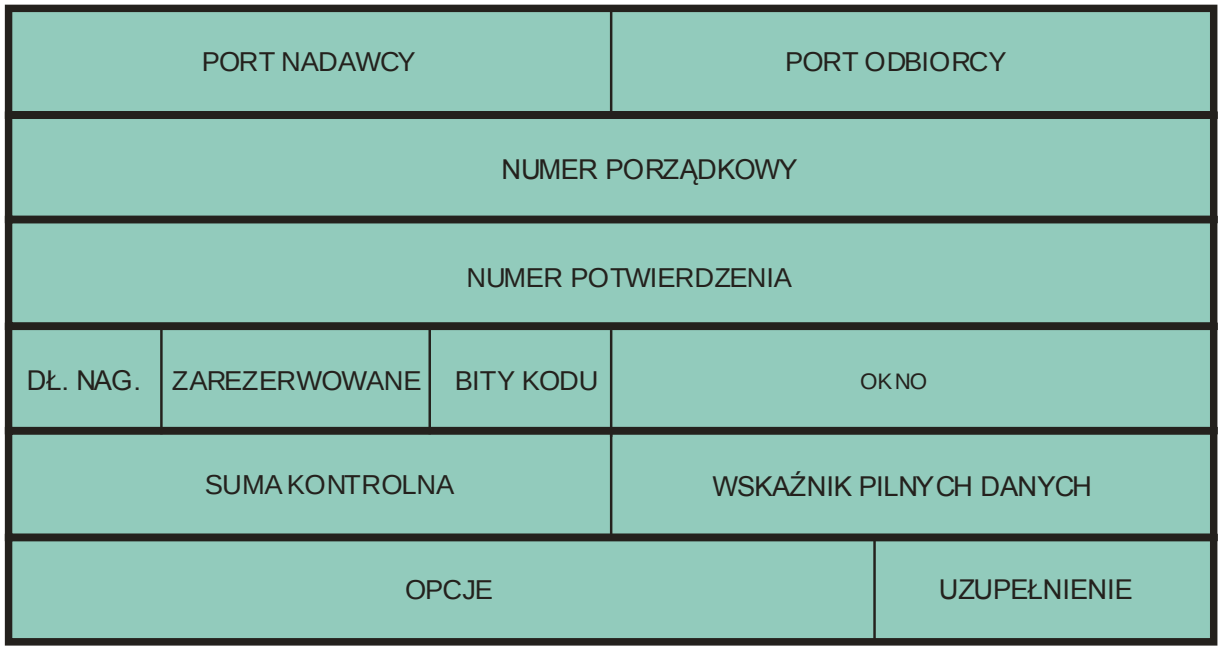
- Rodzina protokołów TCP/IP zawiera dwa protokoły warstwy transportowej:
  - TCP (*Transmission Control Protocol*)
  - UDP (*User Datagram Protocol*)
- Warstwa sieciowa:
  dostarczenie danych
- Warstwa transportowa:
  kontrola poprawności danych

TCP - własności usługi niezawodnego dostarczania danych

- Przesyłanie strumieni (przekazanie odbiorcy tego samego ciągu oktetów, który wysłał nadawca).
- Łączenie w obwód wirtualny (tworzenie wirtualnego połączenia między nadawcą i odbiorcą w celu ustalenia gotowości obu jednostek a później w celu wykrywania błędów transmisji).
- Przesyłanie z użyciem buforów (oczekiwanie i wysyłanie większej ilości danych tak, aby ograniczyć zbędny ruch w sieci – mechanizm wypchnięcia, gdy dane należy wysłać natychmiast).
- Brak strukturyzacji strumienia (brak rozróżniania rodzaju przesyłanych danych użytkownika).
- Połączenie w pełni dwukierunkowe.

Segment TCP

a.) postać ogólna



b.) postać szczegółowa nagłówka

Segment TCP

W TCP informacje między jednostkami są wymieniane w postaci segmentów TCP.
Dotyczy to zarówno danych jak i procesów otwierania czy zamykania połączenia.

- PORT NADAWCY i PORT ODBIORCY (16 bitów): Porty TCP określające programy wymieniające między sobą dane.
- NUMER PORZĄDKOWY (32 bity): Liczba porządkowa pozwalająca odtworzyć właściwą kolejność segmentów.
- NUMER POTWIERDZENIA (32 bity): Określa numer oktetu, który nadawca spodziewa się otrzymać w następnej kolejności.
- DŁUGOŚĆ NAGŁÓWKA (4 bity): Określa rozmiar nagłówka segmentu jako wielokrotność 32 bitów.
- ZAREZERWOWANE (6 bitów): Przeznaczone do ewentualnego wykorzystania w przyszłości.

Segment TCP

- BITY KODU (6 bitów): Określają przeznaczenie zawartości segmentu:
  Bity pola BITY KODU opisane od lewej do prawej:
  - URG – Wskaźnik pilności jest istotny;
  - ACK – Pole potwierdzenia jest istotne;
  - PSH – Ten segment zawiera prośbę o natychmiastowe wysłanie;
  - RST – Skasuj połączenie;
  - SYN – Zsynchronizuj numery porządkowe;
  - FIN – Koniec strumienia bajtów u nadawcy.
- OKNO (16 bit): Liczba oktetów którą może nadać nadawca bez potwierdzenia (16-bitowa liczba całkowita);
- SUMA KONTROLNA (16 bit): Służy do kontroli poprawności transmisji danych i nagłówka (16 bitów). Do jej obliczenia także stosuje się pseudonagłówek.
- WSKAŹNIK PILNYCH DANYCH (16 bit): Oznacza miejsce w segmencie gdzie kończą się pilne dane. Pilne dane powinny zostać dostarczone do programu po stronie odbiorcy poza strumieniem tak szybko jak to jest tylko możliwe.
- OPCJE: Jedna z opcji służy do ustalenia maksymalnego rozmiaru segmentu. Rozmiar segmentu zależy od:
  - buforów jednostki nadawcy i odbiorcy;
  - rodzaju sieci przez, którą będzie podróżował segment.

TCP - Nawiązywanie połączenie między punktami końcowymi

- Oba punkty końcowe muszą zgodzić się na współpracę.
- Jeden z punktów wykonuje funkcję pasywnego otwarcia (sygnalizując gotowość do nawiązania połączenia).
  Drugi używa funkcji aktywnego otwarcia aby ustalić połączenie.
- Nawiązanie połączenia TCP:
  - Węzeł 1: Wysyła segment, w którym pole kodu ma ustawiony bit SYN;
  - Węzeł 2: Wysyła segment, w którym pole kodu ma ustawione bity SYN i ACK;
  - Węzeł 1: Wysyła segment, w którym pole kodu ma ustawiony bit ACK.
- Zamykanie połączenia:
  - Węzeł 1: Wysyła segment, w którym pole kodu ma ustawiony bit FIN;
  - Węzeł 2: Wysyła segment, w którym pole kodu ma ustawiony bit ACK;
  - Węzeł 2: Wysyła segment, w którym pole kodu ma ustawione bity FIN i ACK;
  - Węzeł 1: Wysyła segment, w którym pole kodu ma ustawiony bit ACK.

TCP - Realizacja niezawodnego połączenie

- Metoda „**Pozytywne potwierdzanie z retransmisją**”:
  Nadawca zapisuje informacje o każdym wysłanym pakiecie (uruchamia także licznik czasowy) i przed wysłaniem następnego pakietu czeka na potwierdzenie (komunikat ACK).
- **Wykrywanie duplikatów**:
  Każdy pakiet ma przydzielany numer identyfikacyjny, który musi być odesłany przez odbiorcę (potwierdzenie otrzymania pakietu).
- Technika „**Przesuwających się okien**”:
  Umożliwia przesyłanie wielu pakietów zanim nadawca otrzyma potwierdzenie.
- Technika „**Zmiennych rozmiarów okien**”:
  Nadawca i odbiorca ustalają w czasie transmisji rozmiar okna, dzięki temu można płynnie regulować generowany ruch.
- **Uwaga**:
  W TCP mechanizm okien działa na poziomie oktetów a nie segmentów.

TCP – Identyfikacja jednostek

- Protokół TCP jest zorientowany na połączenie, które musi nastąpić pomiędzy dwoma jednostkami końcowymi przed rozpoczęciem transmisji.
  Każdy punkt końcowy jest identyfikowany przez adres IP i port węzła np.:

  192.51.212.4:80

  Ten zapis oznacza port 80 węzła o adresie IP 192.51.212.4

- Uwaga:

  Połączenie identyfikowane jest przez parę punktów końcowych stąd np. punkt 192.51.212.4:80 może występować w dwóch różnych połączeniach.

UDP - Właściwości

- Minimalna, dodatkowa ilość przesyłanych danych przez sieć (małe obciążenie).
- Programy użytkowe biorą na siebie całą odpowiedzialność za rozwiązywanie problemów niezawodności, czyli:
  - gubienie komunikatów;
  - duplikowanie;
  - opóźnienia;
  - dostarczanie w niewłaściwej kolejności;
  - utratę łączności z adresatem.

Segment UDP

Port UDP nadawcy	Port UDP odbiorcy
Długość komunikatu UDP	Suma kontrolna UDP
DANE	
...	

- PORTY (16 bitów): Używane do odnajdywania procesu oczekującego na dany segment.
- DŁUGOŚĆ (16 bitów): Liczba oktetów segmentu UDP (min. 8).
- SUMA KONTROLNA (16 bitów): (może być zero, gdy nie używana). W celu obliczenia sumy kontrolnej stosuje się pseudonagłówek.

UDP - Problemy

- Uwaga:
  - Aplikacje wykorzystujące UDP, napisane bez obsługi błędów transmisji, ale testowane w środowisku sieci lokalnej, mogą działać bardzo dobrze, podczas gdy w sieci rozległej praktycznie przestaną funkcjonować.

Numery portów

- TCP i UDP korzystają z numerów portów by dostarczyć dane do wyższych warstw modelu.
- Programiści używają numerów portów zgodnie z dokumentem RFC 1700.
- Podział:
  - Porty poniżej 255 – dla publicznych aplikacji
  - Porty od 255 do 1023 – dla firm i ich komercyjnych aplikacji
  - Porty powyżej 1023 – niezarezerwowane

Najpopularniejsze numery portów

Numer portu	*Usługa*
7	ECHO
13	DAYTIME
20	FTP-DATA
21	FTP
23	TELNET
25	SMTP
37	TIME
42	NAMESERVER
53	DOMAIN
69	TFTP
113	AUTH
161	SNMP
162	SNMP-TRAP

Wykład 8 i 9

KONIEC