Sieci komputerowe **Wykład 1**

Systemy zamknięte - stare rozwiązanie protokół zależy od producenta urządzenia.

Systemy otwarte - pozwala na zmianę sprzętu bez reorganizacji sieci.
- zbudowane zgodnie z pewną normą,
- pozwalają na współpracę sprzętu i oprogramowania różnych producentów,
- są zdolne do wymiany informacji z innymi sys. otwartymi

Koniec lat 70 - Model ISO Reference Model for Open System Interconnection - OSI/ISO

Model odniesienia - stan specyficzny pewnego wzorca, nie jest to konkretna implementacja, istnieje wiele implementacji spełniających założenia systemu otwartego
Ważne organizacje:
- ISO -> International Organization for Standardization
- IEEE -> Institute of Electronic and Electronical Engineers Grupa 802 zajmuje się standaryzacją sieci lokalnych
- IETF -> Internet Engineering Task Force - standardy na poziomie TCP/IP
- ITU-T -> International Telecommunication Union- Telecommunications Sector
- TIA/EIA -> Telecommunications Industry Associations / Electronics Industry Associations - zajmuje się określaniem norm dotyczących okablowania

Rekomendacje: UWAGA TU BYŁ BŁĄD !
- Rekomendacje serii V - połączenie DTE poprzez modem do PSTN (public switching telephon network)
- Rekomendacje serii X - połączenie z sieciami PSDN (public switching digital network)
- Rekomendacje serii I - połączenie z ISDN (integrated system digital network)

Warstwy modelu OSI/ISO
- 7.Aplikacji
- 6. Prezentacji
- 5. Sesji
- 4. Transportu
- 3. Sieciowa
- 2. Łącza danych
- 1. Fizyczna

Warstwa fizyczna - odpowiedzialna za kodowanie strumienia danych przekazywanych przez wyższe warstwy do postaci sygnałów odpowiednich dla medium transmisyjnego, najczęściej impulsów elektrycznych. Przedmiotem zainteresowania tej warstwy są poziomy napięcia, kodowanie sygnału, media transmisyjne.

Warstwa łącza danych - zapewnia komunikacje pomiędzy hostami w ramach jednej sieci. Zajmuje się dostępem do medium, dostarcza fizycznej adresacji hostów. Pojęciem z warstwy łącza danych jest topologia sieci i ramka. Protokołami tej warstwy są np.: Ethernet, Token Ring, FDDI, Frame Relay.

*Warstwa łącza danych przekazuje **ramki** danych z warstwy sieciowej do fizycznej i odwrotnie - kiedy warstwa łącza otrzymuje bity danych z warstwy fizycznej, przekłada je na ramki.*

Warstwa łącza dzieli się na dwie podwarstwy:

- *sterowanie łączem logicznym (LLC) - kontroluje poprawność transmisji i współpracuje głównie z warstwą sieciową w obsłudze usług połączeniowych i bezpołączeniowych*
- *sterowanie dostępem do nośnika (MAC) - zapewnia dostęp do nośnika sieci lokalnej i współpracuje głównie z warstwą fizyczną*

Warstwa sieciowa - warstwa ta odpowiada za znalezienia najlepszej drogi łączącej dwa hosty, które mogą się znajdować w oddzielnych z punktu widzenia warstwy łącza danych sieciach. Jej zadaniem jest także dostarczenie logicznej adresacji. Jednym z protokołów w warstwie sieciowej jest IP
Zarządza adresowaniem przesyłek i tłumaczeniem adresów logicznych (jak adrs IP) na fizyczne (MAC). Warstwa sieciowa określa także trasę, którą pokonują dane między stacją źródłową a docelową. Jeżeli wysłane pakiety są zbyt duże w stosunku do topologii stacji docelowej, warstwa sieciowa zapewnia podział pakietów. Po dotarciu do celu pakiety te są łączone ponownie.

Warstwa transportowa - odpowiada za segmentacje danych z warstwy wyższej (*w tzw. strumień*) i ponowne ich złożenie w punkcie docelowym. Może zapewniać niezawodność przesyłania danych i parametry jakości transmisji (QOS - Quality of Service). Przykładowymi protokołami pracującymi w warstwie transportowej są TCP i UDP
Wprowadza pojęcie portu (jakby kolejny poziom adresacji).

Warstwa sesji - warstwa ta tworzy zarządza i kończy sesji pomiędzy komunikującymi się hostami. dokładniej: między dwoma procesami na różnych komputerach. Implementowana jest przez system operacyjny. Odpowiada m.in. za synchronizację danych między komputerami.
NFS -
Protokół NSF - Sieciowy system plików (ang. Network File System), opracowany przez firmę Sun Micorsystems, zapewnia odstęp do plików na bieżąco. Dostęp ten jest przezroczysty i zintegrowany. Wiele ośrodków używających TCP/IP stosuje NFS do łączenia systemów plików swoich komputerów. Z punktu widzenia użytkownika NFS jest niemal niezauważalny. użytkownik może używać dowolnych programów, które wykonują operacje wejścia-wyjścia na dowolnych plikach. Nazwy tych plików nie zależą od tego, czy chodzi o pliki odległe czy lokalne. Warstwa sesji realizuje również funkcję ochrony prowadzące do określenia czy stacje mają uprawnienia do komunikacji przez sieć. Koordynuje żądania usług (pojawiające się w czasie, gdy aplikacje komunikują się między stacjami) i odpowiedzi na nie.

Warstwa prezentacji - warstwa odpowiedzialna za reprezentacje danych. Implementowana przez system operacyjny. Do jej zadań należy na przykład konwersja pomiędzy różnymi standardami kodowania znaków, różnymi sposobami reprezentacji liczb.

XPR - zewnętrzna reprezentacja danych
(XDN -standardowa zewnętrzna reprezentacja danych, wykorzystywana do transmisji. To z niej (przy odbiorze) i na nią (przy wysyłaniu) są konwertowane informacje na specyficzne dla danego systemu lokalnego)

Warstwa aplikacji - warstwa najbliżej użytkownika. Aplikacje takie jak przeglądarka WWW, klient poczty elektronicznej, *aplikacje konferencyjne, FTP*.

Model Uproszczony

<table>
<tr><td rowspan="3">Aplikacji</td><td>Aplikacji</td></tr>
<tr><td>Prezentacji</td></tr>
<tr><td>Sesji</td></tr>
<tr><td>Transportu TCP/UDP *</td><td>Transportowa</td></tr>
</table>

IP	Sieciowa
Dostępu do sieci (driver sieciowy)	Łącza danych
	Fizyczna

Protokół komunikacyjny - zestaw reguł wymiany informacji zarówno danych użytkownika jak i informacji kontrolnej z odpowiednią warstwą w innym systemami.

Protokół = {składnia wiadomości, reguły wymiany, implementacja wyższej warstwy jest niemożliwa bez innej, każda warstwa ma dobrze zdefiniowany interfejs z warstwami położonymi bezpośrednio pod i nad nią}

Implementacja każdej warstwy jest niezależna od innej. Każda warstwa ma dobrze zdefiniowany interfejs z warstwami położonymi bezpośrednio pod nią i nad nią.
Komunikacja w modelu warstwowym

⇒ każda z implementowanych warstw modelu OSI/ISO w jednym systemie komunikuje się z implementacją tej samej warstwy w drugim systemie. Jest to komunikacja typu peer-to-peer.

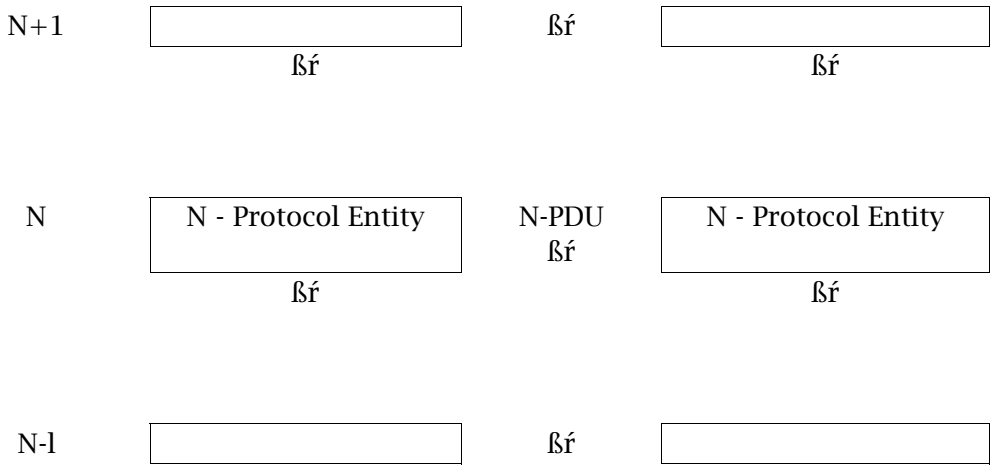
porcja danych na poziomie warstwy N nosi nazwę N-PDU (protocol data unit) i składa się z trzech podstawowych części:

1. nagłówka (header)
2. pole danych (payload)
3. zamknięcie (trailer)

PDU - Protocol Data Unit

Komunikacja w modelu warstwowym - rysunek

Wszystko działa na zasadzie enkapsulacji. Warstwa N modelu OSI/ISO dostając informacje z warstwy wyższej opakowuje ją sobie w niezbędne dla siebie informacje, oraz przekazuje niżej. Na samym dole dane są fizycznie przesyłane, a z drugiej strony kolejno rozpakowywane.



Jaki jest powód wprowadzenia modelu warstwowego ?

Ethernet	
IP	

TCP	

Sprzęt sieciowy

Nazwa urządzenia	Warstwa
Router	3
Mostek Przełącznica (switch)	2
HUB Regenerator sygnału (repeater)	1

Wyższe warstwy - czysty software

Zalety modelu warstwowego
- umożliwia niezależny rozwój warstw
- zmniejsza złożoność systemu
- standaryzuje interfejs
- zapewnia współpracę pomiędzy urządzeniami pochodzącymi od różnych producentów
- przyspiesza rozwój

Sieci komputerowe - podział
- Sieci rozległe WAN (Wide Area Network) ZSK (zdalne sieci komputerowe) - łączą sieci lokalne - przykładem jest globalna sieć Internet
- Sieci lokalne LAN (Local Area Network) LSK (lokalne sieci komputerowe) - biura, uczelnie, fabryki
- Sieci miejskie MAN (Metropolitan Area Network) MSK (miejskie sieci komputerowe) - do łączenia sieci lokalnych
- Sieci personalne PAN (Personal Area Network) PSK (personalne...) - np. z wykorzystaniem Bluetooth

Typy sieci wg Rodzaju komutacji
- Sieci z komutacja łączy (circuit switching)
  - POTS (Plan Old Telephone Service)
  - N-ISDN (Narrowband Integrated Services Digital Network)
- Sieci z komutacją pakietów (packet switching)
  - IP
  - X.25
  - Frame Relay
- Sieci z komutacją komórek (cell switching)
  - ATM (Asynchronious Transfer Mode)
    technologia przesyłania informacji w sieciach telekomunikacyjnych (szerokopasmowych) o bardzo wysokiej przepustowości, np. opartych na światłowodach, umożliwiająca optymalne wykorzystanie sieci. Cechuje ją praktycznie nieograniczone pasmo transmisji. Opiera się na asynchronicznej transmisji 53 bajtowych komórek. Została wynaleziona z myślą o przekazywaniu danych multimedialnych.
  - SMDS (Switched Multimegabit Data Service)
    technologia komutowanych usług przesyłania informacji z szybkością 45 Mb/s za pomocą pakietów o wielkości do 9188 B (które można dzielić na 53-bajtowe komórki. Usługa SMDS wypełnia lukę między szybkimi usługami sieci rozległych a usługami ATM. Każdy pakiet SMDS jest samodzielny, usługi SMDS nie tworzą obwodów wirtualnych.

Tryby transmisji:

- Simplex - transmisja jest możliwa tylko w jedną stronę (analogia: ulica jednokierunkowa)
- Half-duplex - transmisja w obie strony ale w danym czasie tylko w jedną (analogia: ruch na remontowanym moście)
- Duplex - równoczesna transmisja (ulica dwukierunkowa)

Bit - informacja jaka jest zawarta w wiadomości, że spośród dwóch jednakowo prawdopodobnych informacji zaszło jedno.

Przesyłanie informacji

- Bod (ang. Baud) - jeden sygnał elektryczny na sekundę
- M - ilość poziomów sygnału
- m - ilość bitów na sygnał $m=\log_2 M$
- R - bit rate [b/s] - ilość informacji na sekundę
- R_s - signaling rate [baud] - szybkość sygnałowa
- $R=R_s\log_2 M$

Np. Gdy sygnał ma 2 stany -> 1 baud=1 b/s;
300 baud i 4 bit/sigma -> 1200 b/s

DTE a DCE

DTE - Data Terminal Equipment czyli urządzenia końcowe, np. komputery, routery.

DCE - Data Communication Equipment czyli urządzenia pośredniczące w transmisji, np. switche, modemy, Huby

Bandwidth i Throughput

Szerokość pasma (bandwidth) - wyraża maksymalną teoretyczną przepustowość sieci. Podstawowa jednostka bit/s
Przepustowość (throughput) wyraża aktualne możliwości sieci w zakresie przesyłania danych w siecii jest mniejsza lub równa teoretycznej
Jednostka: bit/s
Zależy od:

- Wydajności sieci - zarówno komputerów końcowych, jak i elementów pośrednich
- Obciążenia sieci - a więc od aktywności innych urządzeń
- Typu danych - (przede wszystkim narzut na pola kontrolne)

Warstwa fizyczna
Zadania:

- Zapewnienie dostępu
- Kodowanie strumienia danych

Media komunikacyjne

- Przewodowe
  - Kable
  - Światłowody
- bezprzewodowe
  - radiowe (802.11, Bluetooth)

- podczerwień (IrDA)

<table>
<tr><td colspan="4">Kable</td></tr>
<tr><td colspan="3">Miedziany</td><td>Światłowód</td></tr>
<tr><td colspan="2">Skrętka</td><td>Koncentryk</td><td>Jednomodowy</td><td>Wielomodowy</td></tr>
<tr><td>Ekranowana</td><td>Nieekranowana</td></tr>
</table>

Skrętka

- Zawiera 4 pary kabli miedzianych, skręconych równomiernie
- Występują 2 rodzaje:
  - **Ekranowana** (STP - shielded twisted pair) - poprzez ekran (nie będący częścią obwodu) Zapewnia większą odporność na zakłócenia zewnętrzne. Dość droga - mało popularna
  - **Nieekranowana** (UTP - unshielded twisted pair) - łatwa w instalacji. Tańsza, bardziej popularna. Istnieje podział na kategorie.
- Segment do 100 m przy 100 Mbps. (L*p=const, L-długość, p-przepustowość reoretyczna)

Kabel koncentryczny

- 2 współśrodkowo ułożone kable oddzielone warstwą izolacji
- Występują 2 rodzaje:
  - **Cienki** - śr. 0,25", maks. dł. segmentu 185 m. Oporność falowa 50 ?, *maks. 30 komputerów, min. odl. 0,5m*
  - **Gruby** - śr. 0,50", maks. dł. segmentu 500 m. *Komputery dołączone co wielokrotność 2,5m*
- Umożliwia budowanie dłuższych segmentów niż skrętka
- Łatwa w instalacji i eksploatacji
- wychodzi z użycia
- *komputery przyłączanie są za pośrednictwem trójników, a końcach muszą być umieszczone terminatory*

Światłowód

- Informacja jest przenoszona przez wiązkę światła prowadzoną w szklanym przewodzie.
- Ze względu na sposób propagacji światła można podzielić światłowody na:
  - Jednomodowe
  - Wielomodowe
- Odporny na zakłócenia elektromagnetyczne. Nie emituje też nic na zewnątrz przewodu. Bardzo dużą szybkość transmisji (10 Gb/s)
- Niska tłumliwość.
- Drogi i trudny w instalacji.

WDM Wide Dense MultiCOŚTAM (na jednym włóknie wiele promieni świetlnych o różnych długościach fali - różnice rzędu kilku nanometrów) (wiele "lambd" o niewiele różniącej się długości fali)	DWDM BRAKI

	Światłowód jednomodowy	**Światłowód wielomodowy**

Szer. wiązki szklanej	8,2 ?m	62,5 ?m
Nadajnik	Laser	Diody luminescencyjne
Zasięg	70 km	2 km
Cena	drogie	Tanie

Problemy transmisji danych

- Osłabienia sygnału, tłumliwość $10\log(P_1/P_2)$ [db] P_1(moc wejściowa),P_2(moc wyjściowa) [W]
- Zniekształcenie sygnału (distroied)
- Zakłócenia od innych kabli. Zależą m.in. od: typu medium, odległości od innych kabli, odległości, na jaka przesyłamy dane....

Kodowanie -> Net - wykład 2

Kodowanie - dostosowanie reprezentacji informacji do postaci możliwej do przesłania w medium

- W przewodzie jest to odpowiednie napięcie, częstotliwość
- W światłowodzie jest to odpowiednia długość fali

CDMA (multipleksacja z podziałem kodu, czyli nadawanie wielu rozmów na wielu częstotliwościach, przy "dość" szybkiej zmianie częstotliwości przypisanej do danej rozmowy, pozwala na trzykrotnie szybszą transmisję bardzo trudną do podsłuchania).

NRI - stan wysoki: 1; stan niski: 0
NRZI - jeżeli następnym bitem jest 1 - to nie zmieniamy wartości sygnału, natomiast 0 powoduje zamianę
Manchester -zmiana stanu w środku sygnału. Zmiana ze stanu L -> H oznacza 1; zmiana z H -> L oznacza). Kod posiada własność samosynchronizacji
Manchester różnicowy - zawsze zmiana wartości w środku kodowanego bitu, przy czym za to, jaki bit kodujemy odpowiada zmiana (bądź jej brak) na początku kodowanego bitu. Jeżeli następuje zmiana sygnału, to oznacza, iż kodowanym bitem jest zero, natomiast brak zmiany oznacza jedynkę.

przesyłanie informacji
kodowanie 4B/5B - ciągi 4-bitowe są reprezentowane przez ciągi 5-bitowe

- Część symboli używana jest do funkcji kontrolnych, przykładowo aby uzyskać 100Mb/s musi osiągnąć częstotliwość 125MHz

Kodowanie 8B/6T

- używane są symbole trójwartościowe
- 8 bitów na 6 symbolach
- potrzebujemy 256 (2^8) mamy 727 (3^6)
- używa się tylko tych, które niosą odpowiednią zmienność (co najmniej dwie zmiany) i zrównoważone są ???????????? napięcie (np. 00:-+00-+, 14:0 -++0)
- można obniżyć częstotliwość wysyłania (np. zamiast 100MHz -> 75MHz (szybkość modulacji))

urządzenia warstwy pierwszej

- regenerator sygnału (repeater)
- pozwala zwiększyć rozmiar segmentu sieci
- zapewnia odtworzenie charakterystki sygnału
- hub (wieloportowy repeater)
- używany w topologii gwieździstej (może być centralnym punktem sieci)
- wzmacnia sygnał i przesyła na wszystkie pozostałe porty
  1. konwerter sygnału (transceiver)
     - układ transmisji i odbioru
     - generuje sygnał propagowany przez medium i odbiera sygnały
     - konwertuje sygnał
- część interfejsu sieciowego odpowiadająca za dostęp do medium

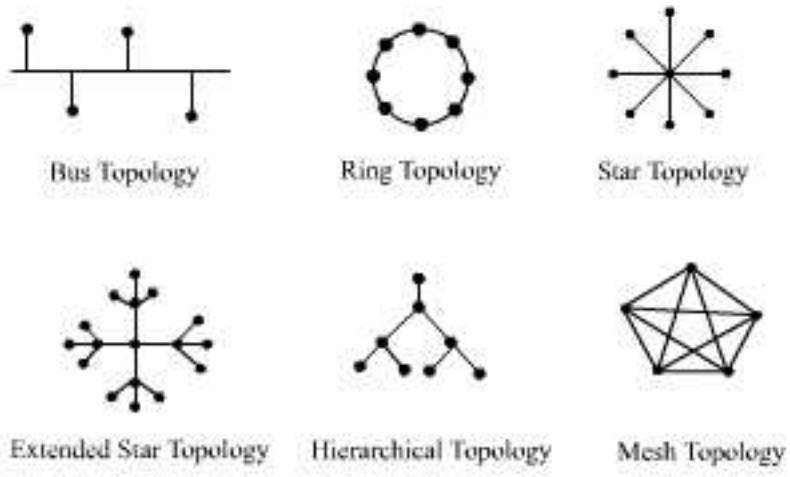
zadania warstwy łącza danych

- wykrywanie i ewentualne korygowanie błędów warstwy fizycznej
- serializacja i deserializacja informacji

- zapewnienie adresacji
- Dostęp do łącza
- Formatowanie i transmisji ramek

Topoligie sieci

⇒ Bus Topology (rolę szyny może pełnić hub)
⇒ Ring Topology
⇒ Star Topology
⇒ Extended Star Topology
⇒ Hierarchical Topology
⇒ Mesh Topology (topologia sieci zdalnych, np Internet, sieci miejskie)



Protokoły danych w sieciach WAN

⇒ High-Level Data Link Control (HDLC) - standard opracowany przez IEEE; obsługuje połączenia punkt-punkt jak i punkt-wiele_punktów; typowy w sieciach zdalnych
⇒ Frame Relay - uproszczona budowa ramki (uproszczona wersja X.25) nie posiada korekcji błędów
⇒ Point to Point Protocol (PPP) - standard opracowany przez IETF (enakpsulacja innych protokołów sieciowych)
⇒ Serial Line Integrate Protocol (SLIP) popularny standard do transmisji IP, obecnie wypierany przez PPP

Sieci lokalne

- Mała rozległość
- Duża przepustowość
- Topologie:
  - Szynowa
  - Gwieździsta
  - Drzewo
  - Pierścień
- media:
  - skrętka i światłowód

- koncentryk przechodzi do historii

Protokół powinien być prosty i łatwy w inicjacii, przystosowany do dużej zmienności sieci (bo czasami zdarza się przestawiać komputery), optymalnie wykorzystuje łącze, z wprowadzeniem wewntualnych priorytetów - przy czym bez monopolizowania jednej stacji. Powinien być również odporny na zakłócenia i uszkodzenia

standardy sieci IEEE 802
Dotyczą protokołów warstwy drugiej w sieciach lokalnych
- 802.3 Ethernet
- 802.4 Token Bus
- 802.5 Token Ring
- 8.2.11 Wireless Lan (łączność bezprzewodowa)
  - 802.11A - 54 Mb/s
  - 802.11B - 11Mb/s
- 802.15 PAN (Bluetooth)

Protokoły dostępu do sieci

Niedeterministyczny	Deterministyczny
stacja nadaje, gdy łącze jest wolne	stacja nadeje, gdy nadejdzie jej kolej
Każda strona jest równouprawniona (mogą pojawić się kolizje)	Może wprowadzać priorytety
Rywalizacyjny	Np. tokeny decydują o możliwosci nadawania
Problem z wielodostępem do medium	Problem z zarządzaniem tokenami
Dobry do zastsowań biurowych	Dobry do zastosowań przemysłowych
Ethernet	Token Ring, Token Bus, FDDI

Token krążący w pierścieniu -
- warunkiem nadawanie jest posiadanie tokenu, wówczas może transmitować przez pewien czas, po nim musi przekazać token następnemu
- skomplikowany w zarządzaniu
  - token może "paść" razem z komputerem - musi zostać odtworzony (generowanie tokenu - skomplikowany algorytm)

Ethernet - krótka historia
- opracowany w laboratorium Xerox w 1973
- oparty na sieci Aloha
- opublikowany w 1980 przez firmy DEC - Intel - Xerox (DIX)
- opracowany przez IEEE pod nazwą 802.3

CSMA/CD - **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection
Carrier Sense - *(wykrywanie fail nośnej)* gdy medium zajęte, nie nadajemy. gdy się zwolni odczekujemy czas IFG (dla Ethernetu 10Mb 0,9 us) i rozpoczynamy transmisję

Multiple Access *(dostęp wielokrotny)* - przy wolnym medium dwie stacje moga się zdecydować na rozpoczęcie nadawania w tym samym momencie. Wtedy następuje kolizja.

Collision Detection *(wykrywanie kolizji)*
- przy nałożeniu się dwu sygnałów zwiększa się czestotliwość, możliwe jest wiec wykrycie kolizji

- Jeśli stwierdzi wystąpienie kolizji nie wstrzymuje od razu transmisji, lecz wysyła tak zwaną sekwencję zagłuszającą (ang. jam sequence) o czasie trwania równym czasowi wysłania 32bitów Ułatwia to zauważenie kolizji przez wszystkie stacje. Następnie zaprzestaje nadawać.
- Gdy kolizja jest *zauważona* przed zakończeniem wysłania preambuły, cała *preambuła* jest wysyłana, a dopiero po niej transmituje się sekwencję zagłuszającą.
- Po odczekaniu losowego odstępu czasu (zgodnie z algorytmem exponential backoff) ponownie próbuje wysłać ramke. Podobnie postępowanie przeprowadzają wszystkie stacje, które chcą wysłać dane, a uczestniczyły w kolizji.
- W poprawnie działającej sieci kolizja nie może wystąpić po wysłaniu więcej niż 64B ramki (wiąze się to z wielkością szczeliny czasowej - przy 10Mb/s Ethernecie sygnał jest wstanie dotrzeć do wszystkich stacji i z powrotem)

Exponential backoff

⇒ Każde ze stron uczestniczących w kolizji rozpoczyna próbę wysłania ramki, Losują one niezależnie od siebie czas oczekiwania **r** wyrażony w szczelinach czasowych (51,2 us - przy czym nie wiem dla jakiej jest to sieci) zgodnie z algorytmem:

$0 \le r < 2^k$, gdzie k=min(n,10) n - numer próby, n<16

⇒ gdy nie powiedzie się 15 kolejnych prób, zaprzestaje się transmisji i generowny jest komunikat do warstwy wyższej (błąd medium transmisyjnego)

⇒ taka konstrukcja algorytmu preferuje stacje, które mają niewilką ilość nieudanych prób

Budowa ramki Etnernetowej i 802.3

Preambuła	Znacznik początku ramki	Adres docelowy	Adres źródłowy	Typ albo długość	Dane	Suma kontrolna
7B	1B	6B	6B	2B	46 - 1500B	4B

Zatem długość ramki wynosi 64 - 1518 B (nie wliczamy preambuły i znacznika początku ramki)

Standard IEEE 802.2

Warstwa łącza danych dzieli się na dwie podgrupy:

⇒ MAC (Medium Access Control) niższą zależną od stosowanej techniki np. 802.3, 802.5

⇒ LLC - zawiera własne PDU

Możliwe jest łączenie sieci o różnych standardach MAC urządzeń pracujących w warstwie 2 modelu OSI/ISO (następuje przepakowywanie informacji)

Standard 802.3

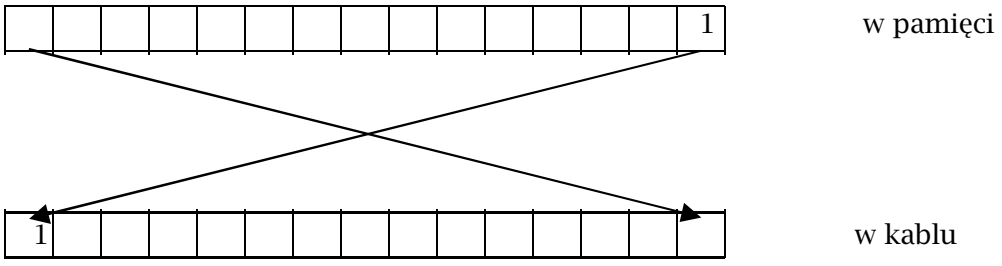
- Preambuła - służy do synchronizacji bitowej, pozwala interfejsowi dobrze przygotować się do odebrania danych
  Postać: naprzemienne 1 i 0
- Znacznik początku ramki - stan po synchronizacji bitowej
  Postać: 10101011
- Adres docelowy :
  - Adres pojednyczego hosta (unicast)
  - Adres grupowy (multicast)
  - Adres rozgłoszeniowy (broadcast)

- **Adresy warstwy łącza danych**
  - Adresy te są nazywane fizycznymi lub sprzętowymi
  - Adresy są na stałe związane z interfejsem sieciowym
  - Długość 48 bitów.

- Najczęściej zapisywane w postaci: 12:34:34:56:AA:DC
- Składają się z dwóch części:
  - Pierwsze 24 bity rozdawane przez IEEE oznaczają producenta (np. 00:00:0C oznacza CISCO). Ta część nazywa się OUI (Organization Unique Identification)
  - Pozostałe 24 bity przydzielają producenci
- zapewnia to unikatowość w skali globalnej

- Adres źródłowy

- unicast
- Adres rozgłoszeniowy (broadcast) - 6 bajtów jedynek (FF:FF:FF:FF:FF:FF) (taki pakiet jest odbierany przez wszystkie stacje)
- Adres grupowy (multicast) - najmłodszy bit najstarszego bajtu musi być równy 1.Jednak ponieważ w czasie transmisji bity w bajcie są odwrócone "w kablu" pierwszy bit musi być 1



przykładowo multicast: 1**1**:34:34:56:AA:DC

- Typ albo długość
  - W standardzie DIX (stosowany w Ethernecie) typ danej w polu dane (np. 0x8000 oznzcza IP)
  - W std. IEEE:
    - § Długość pola danych (gdy wartość mniejsza niż 1518)
    - § Typ gdy wartość większa niż 1536 - 0x6000
- Dane
  - Musi być co najmniej 46B - jeżeli danych jest mniej trzeba dopełnić (ang. pad - wypełniacz)
  - Standard IEEE zakłada dalszy podział tego pola:

????????DSAP	SSAP	Control	Dane

DSAP - Destination Service Adres Port, 1B, jest to kod protokołu warstwy wyższej
SSAP -
Control - 1-2B
Dane (lub pad) - ????????

1. Suma kontrolna
   a. An.g FCS (Frame cycle sequence) używa się metody CRC
   b. Obliczana przy nadawaniu ramki
   c. Ponownie obliczana przy odbiorze i porównywana z zawartością w ramce - jeśli się niezgadzają, ramka jest pomijana

Cycle Redundancy Check

X (m)	Y (m)

+ wielomian generacyjny G stopnia r
X - traktuje się jako współczynniki kolejnych wyrazów wielomianu W(x) stopnia m-1
Y - traktuje siejako współczynniki wielomianu będącego resztą z dzielenia modulo 2 wielomianu W(x) przez wielomian generacyjny G(x) stopnia r
Dla sieci wielomian G(x) jest stopnia 32
100000100110000010001110110110111 to oznacza ze jest postaci:

G^32(x) = x^32 + x^26 + x^23 + x^22 + x^16 + x^12 + x^12 + x^11 + x^10 + x^8 + x^7 + x^5 + x^4 + x^2 +x +1

ten wielomian gwarantuje:

2. wykrycie wszystkich błędów seryjnych o długości serii do 32
3. prawdopodobieństwo niewykrycie błędu seryjnego o długości serii większej niż 32 wynosi $2*10^{-10}$
4. CRC pozwala także na korekcję błędów, ale w sieciach lokalnych nie jest to stosowane

Network Interface Card (NIC)

5. urządzenie pracujące w warstwie pierwszej i drugiej modelu OSI/ISO
    a. zapewnia dostęp do medium
    b. zajmuje się formatowaniem ramek, obsługą protokołu warstwy łącza danych
    c. posiada (najczęściej niezmienny) adres MAC
6. połączona z urządzeniem sieciowym poprzez jego magistralę

NIC decyduje o odebraniu lub nieodebraniu danej ramki na podstawie jej adresu docelowego. Odbiera następujące ramki:

7. adres przeznaczenia jest równy własnemu adresowi MAC
8. adres przeznaczenia jest adresem rozgłoszeniowym
9. adres przeznaczenia należy do zbioru adresów grupowych, którym dana stacja odbiorcza jest zainteresowana.

najczęściej decyduje o postępowaniu z daną ramką jest podejmowana po przeczytaniu całej i sprawdzeniu sumy kontrolnej (choć np. bridge może podejmować decyzję już po przeczytaniu adresu docelowego)
pewne urządzenia sieciowe (np. bridge) działają w tak zwanym trybie promiscous odbierając wszystkie ramki

Token Ring .....ogólnie

10. do prowadzenia łączności niezbędne jest posiadanie uprawnień (token)
11. stacja otrzymująca ramkę:
    a. logiczn??? Jej zawartość ??????? DUZE BRAKI !?!?!?!???!!!

Token Bus

12. stacje połączone są w fizyczny pierścień
    a. każde stacja posiada połączenie z bezpośrednio poprzednią i następną
    b. można użyć koncentratora
13. fizycznym interfejsem jest TCU (trunk coupling unit)
    a. gdy stacja jest włączona przekazuje od niej ??????????/
    b. gdy stacja jest wyłączona przekazuje ramki dalej (bypass)

14. dane ???????standard ??? 4MB/s : 16Mb/s
15. medium : skrętka

Token Ring - Format ramek

SD	AC	ED

SD	AC	FC	DA	SA	INFO	FCS	ED	FS

SD (start delimiter) 1B
ED (end delimiter) 1B
- jeden bit wskazuje czy dana ramka jest ostatnia w serii
- jeden bit okresla, czy wystapił błąd, ustawiany przez pośrednie stacje

AC (access control) 1B
- trzy bity na piorytet
- jeden bit określa czy ramka(???) jest tokenem
- trzy bity rezerwacji pozwalające stacjom posiadającym ramki w wyższym piorytecie "zamówić" token
- jeden bit używany przez monitor sieci

FDDI

(Fiber Distributed Data Interface)

16. protokół oparty na przekazywaniu tokenu
17. postać ramki podobne do Token Ring
18. światłowód jako medium transmisji
19. kodowanie 4B/5B
20. szybkość 100 MB/s
21. ??????????????????
    a. ??????? DAS i SAS
    b. ??????????????
22. opracowana także wersja CDDI (copper)
23. typowa sieć miejska
24. często wykonywana jako sieć szkieletowa
25. duża niezawodność

max stacji 500

przesyłanie z szybkością 100Mb/s przy użyciu fali świetlnej 1300nm oraz przy ograniczeniu odległości do 200km, ze wzmacniakami w odległości co najwyżej 2 km

Tryby pracy FDDI

Dane synchroniczne

26. w trybie ciągłym, gwarantowana część pasma
27. stacje obsługujące ten tryb mają gwarantowaną część pasma SAT

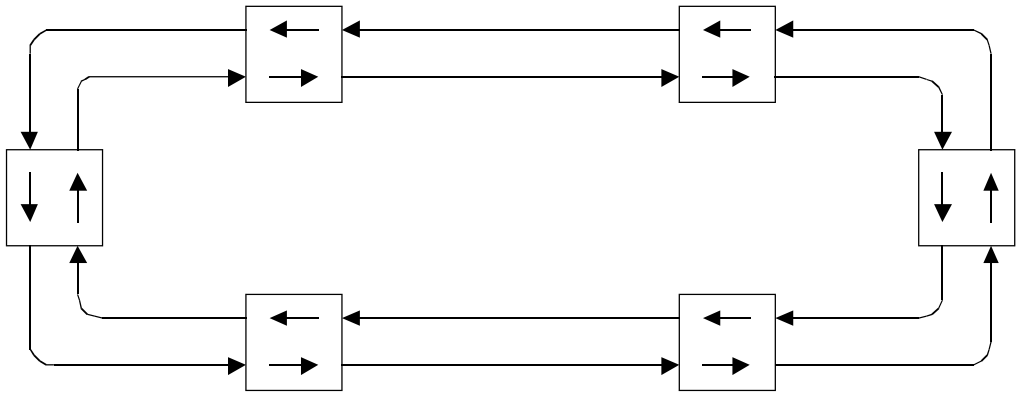
dane asynchroniczne

28. dane generowane z losowymi odstępami czasu i losową wielkością (max 4,5 kb)
29. ??????????????????????

Własności sieci FDDI

Sieć FDDI jest oparta na technice sieci-pierścienia z krążącym znacznikiem (ang. token ring) o szybkości 100Mb/s, mającej własność autokreacji (ang. self-healing). Sieć FDDI ma strukturę pętli, w której transmisja zaczyna się z jednego komputera, przebiega przez wszystkie pozostałe i kończy się tam, gdzie się zaczęła. FDDI jest siecą z krążącym znacznikiem , gdyż korzysta ze znacznika do kontroli transmisji. Gdy sieć jest nieobciążona, specjalna ramka zwana znacznikiem jest przesyłana między kolejnymi komputerami. Gdy komputer chce wysłać pakiet, musi poczekać aż otrzyma znacznik, wtedy może wysłać pakiet, a potem przekazać znacznik następnemu komputerowi. Krążący znacznik zapewnia sprawiedliwość (ang.
fairness): każdy komputer ma możliwość wysłania pakietu zanim inny komputer wyśle drugi pakiet.
Jednak najciekawszą własnością sieci FDDI jest jej zdolność do wykrywania i korygowania błędów. Sieć ta jest odporna na błędy, gdyż sprzęt jest w stanie automatycznie obsłużyć błędy.

Aby zapewnić automatyczną obsługę błędów, osprzęt FDDI używa dwóch niezależnych pierścieni połączonych ze wszystkimi komputerami. Na rysunku 2.10 widać topologię tej sieci

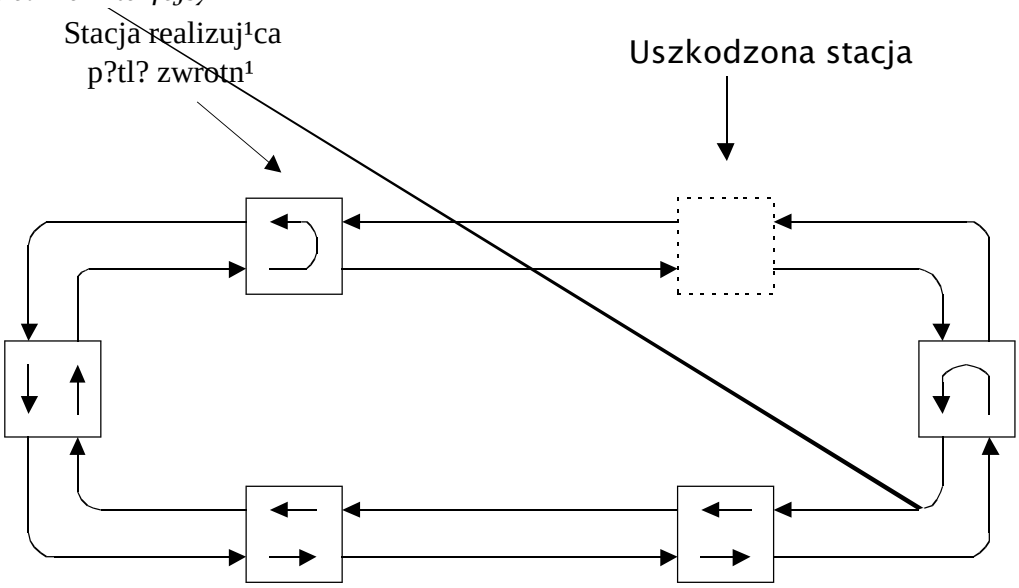


Rysunek 2.10 *Sieć FDDI z kablami optycznymi łącząca sześć komputerów. Strzałki pokazują kierunek ruchu w kablach i połączonych nimi komputerach*

Pierścień FDDI są nazywane przeciwbieżnymi, gdyż w każdym z nich pakiety wędrują w przeciwną stronę. Powody użycia przeciwbieżnych pierścieni staną się jasne, gdy opiszemy, w jaki sposób sieć FDDI reaguje na błędy.
Dopóki nie wystąpi błąd, dopóty sieć FDDI nie potrzebuje obydwu pierścieni. Do chwili wystąpenia błędu interfejsy sieci FDDI zachowują się tak samo, jak interfejsy w pierścieniu, porównując adres odbiorcy każdego pakietu z adresem swojego komputera. Interfejs zachowuje kopię pakietu przeznaczonego dla jego komputera, a oprócz tego przekazuje ten pakiet dalej wzdłuż pierścienia.
Gdy komputer chce wysłać pakiet, czeka na nadejście znacznika, chwilowo wstrzymuje przekazywanie krążących pakietów i wysyła swój pakiet. Po wysłaniu jednego pakietu interfejs wysyła znacznik i wznawia przekazywanie krążących pakietów. Nawet jeśli komputer w chwili otrzymania znacznika ma więcej niż jeden pakiet do przekazania, to wysyła tylko jeden pakiet przez przekazaniem znacznika. Ten sposób przekazywania znacznika zapewnia, że wszystkie komputery mają sprawiedliwy dostęp do sieci.

Sprzęt FDDI zachowuje się szczególnie ciekawie w przypadku wystąpienia błędu sprzętowego. Gdy interfejs wykryje, że nie może się porozumieć z sąsiednim komputerem, wykorzystuje drugi pierścień do ominięcia uszkodzenia. Na rysunku 2.11 pokazano przykładową się FDDI, w której wystąpiło uszkodzenia interfejsu - został on wyeliminowany z pierścienia przez dwa

sąsiednie interfejsy.



Rysunek 2.11 *Pierścień FDDI po awarii. Gdy sprzęt FDI wykrywa taką awarię, wykorzystuje ono drugi pierścień do obejścia miejsca uszkodzenia, aby pozostałe komputery mogły się nadal komunikować*

przeznaczenie drugiego pierścienia i przyczyna, dla której dane są w nim przesyłane przeciwbieżnie, powinny już być jasne. Uszkodzenie może oznaczać, że nastąpiło odłączenia kabla (na
przykład został on przypadkowo przecięty). Jeżeli kabel w obu pierścieniach został poprowadzony tą samą drogą, to jest bardzo prawdopodobne, że drugi kabel też został odłączony.
Sprzęt FDDI automatycznie wykorzystuje przeciwbieżny pierścień do utworzenia zamkniętej pętli do przesyłania danych w tym kierunku, w którym jest to możliwe. W ten sposób pozostałe komputery mogą się nadal komunikować mimo awarii.

Gdy sprzęt FDDI wykryje uszkodzenie sieci, tworzy automatycznie pętlę przy użyciu zapasowego pierścienia, co zapewnia ciągłość komunikacji między pozostałymi komputerami.

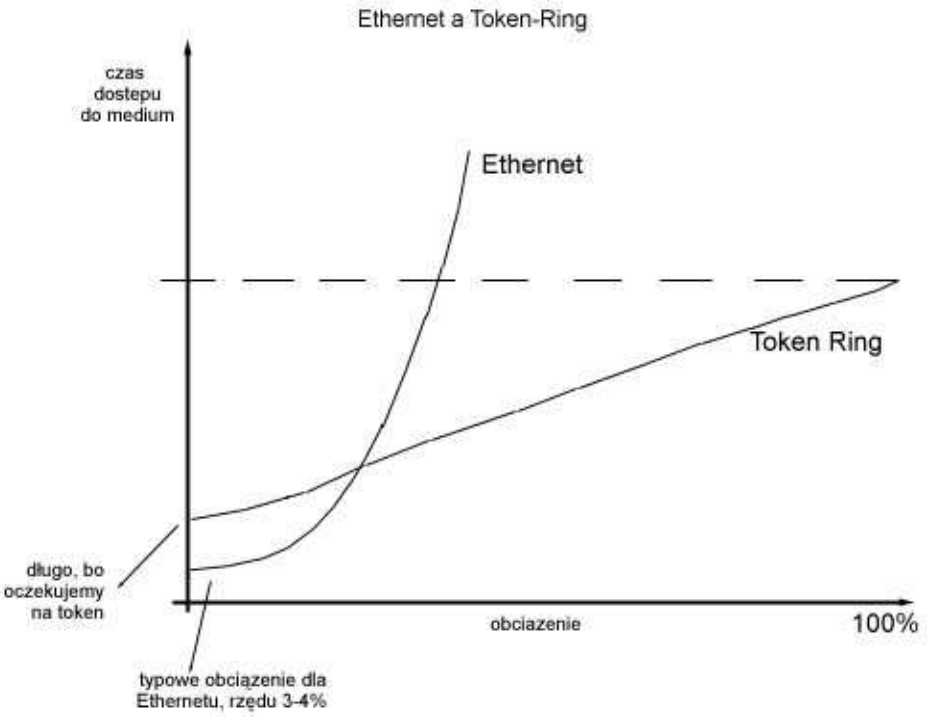
Format ramki FDDI

Pole	Długość w jednostkach 4-bitowych	Zawartość
PA	4 lub więcej	Preambuła
SD	2	Znacznik początku
FC	2	Kontrola ramki
DA	4 lub 12	Adres odbiorcy
SA	4 lub 12	Adres nadawcy
RI	0 do 60	Informacja o trasowaniu
DATA	0 lub więcej	Dane

FCS	8	Sekwencja kontrolna
ED	1	Znacznik końca
FS	3 lub więcej	Status ramki

Podobnie jak w przypadku innych technik, każdy komputer przyłączony do sieci FDDI ma przypisany adres, a każda ramka zawiera pole adresu odbiorcy. Jednak w celu zapewnienia większej elastyczności sieci FDDI, projektanci zezwolili na używanie wielu różnych formatów ramek. Pole adresu odbiorcy może mieć np. długość 4 lub 12 symboli (symbol oznacza 4 bity) Ramka zawiera także krótkie pole związane z wyznaczaniem trasy. Nadawca może użyć tego pola w celu wskazania, że ramkę należy najpierw przesyłając do punktu połączenia, a następnie do odbiorcy znajdującego się w innym, przyłączonym pierścieniu.

Jedną z zalet sieci FDDI jest duży rozmiar ramki. Ramka może zawierać 9000 4-bitowych symboli, jej łączna długość może zatem wynosić 4500 oktetów. Informacja w nagłówku zajmuje co najwyżej kilkaset oktetów a zatem pojedyncza ramka może zawierać 4 kilo-oktety danych użytkowania. W przypadku programów przesyłających znaczne ilości danych (np. przy przesyłaniu plików) duży rozmiar ramki oznacza zmniejszenie narzutu, a zatem większą przepływność

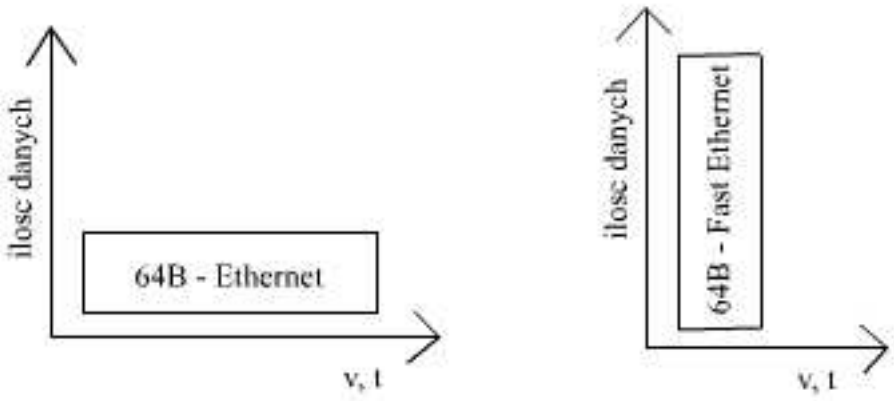


"Szybsze" wersje Ethernetu

- Dwa główne problemy
    a. zapewnienie, aby sprzęt sieciowy i urządzenia transmisyjne były w stanie obsłużyć szybszą transmisje
    b. zapewnienie spełniania wymagań istniejącego protokołu dostępu do medium

ad. 1 To zależy jedynie od postępu technicznego
ad. 2 Z założeń Ethernetu wynika związek pomiędzy minimalną długością ramki, a rozległością fizycznego segmentu sieci. Ponieważ dane są wysyłane szybciej a prędkość rozchodzenia się sygnału elektrycznego jest stała i wynosi 200 000 km/elektrycznego trzeba :

- albo zwiększyć minimalną długość ramki (odrzucone bo zmieniła by się wielkośc szczeliny międzyramkowej)
- albo zmniejszyć rozległość sieci



<rysunek> (Porównanie Ethernetu i FastEthernetu)

W obu przypadkach szybkość rozchodzenia się sygnału jest taka sama.
W Fast Ethernet ilość wysyłanych danych na sekundę jest 10 razy większa, a więc czas wysłania ramki jest 10 razy krótszy, 10 razy krótsza jest rozległość sieci
Fast Ethernet

- Formalnie zaakceptowany w 1995
- Dopuszczalne media: światłowód i skrętka
- Możliwa współpraca z urządzeniami 10 Mb/s (autonegocjacja)

Gigabit Ethernet

- Formalnie zaakceptowany w 1999
- Dopuszczalne media: światłowód i skrętka

- Szczelina czasowa (slot time) w sieci Ethernet odpowiada każdej z dwóch różnych wartości
  - Czas potrzebny na propagacje sygnału w systemie o maksymalnej dopuszczalnej wielkości w obie strony (tam i z powrotem)
  - Maksymalny czas niezbędny do wykrycia i usunięcia kolizji (przez sekwencję zagłuszającą)
- Wartości te wyrażają się najczęściej w ilości bitów transmitowanych w tym czasie w Ethernecie - jest to 512 bitów tj 51,2 ?s
- Istnieje oczywisty związek pomiędzy szczeliną czasową a rozległością sieci. Należy pamiętać także, że urządzenia warstwy pierwszej wzmacniające sygnał wnoszą niezerowe opóźnienie

64x8=512 -> 10 mB na sekunde -> 51,2 ?s

Ethernet - szczelina wynosi 512 bit dając maksymalną rozległość sieci 2800 m

Fast Ethernet - utrzymano wartość szczeliny czasowej ale te 512 bity przesyła się w około 10 razy krótszym czasie zatem należy zmniejszyć jej rozległość (do 205 m)

Gigabit Ethenet - rozległość sieci ok. 20 m była by nieakceptowana - trzeba coś zmienić

Gigabit Ethernet - gdzie można szukać oszczędności ?
- § szybszy sprzęt sieciowy (repeter/hub)
- § szybsza propagacja w kablu
- § zmniejszyć minimalne długości danych 64B

Wypełniacz (Carrier extension)
- ⇒ za ramką dopełnia do 512B
- ⇒ duży narzut dla pojedynczych małych ramek
- ⇒ gdy stacja ma do wypełnienia wiele ramek naraz wypełniacz nie jest między nimi potrzebny

Ramka	Wypełniacz

Ramka	IFG	Ramka	IFG	Ramka	IFG	Ramka

Nawiązywanie - krótkie ramki
Transmisja - długie ramki

Wielkość ta używana jest
- do ??? rozległych sieci
- jak podstawowa jednostka
- do określenia minimalnej długości ramki

Media transmisyjne w sieci Ethernet

10Base5 - gruby kabel koncentryczny 10 Mb/s maks. 500 m
10Base2 - cienki kabel koncentryczny 10 Mb/s maks. 185 m
10Base-T - skrętka kat. co najmniej 3 - 10 Mb/s maks. 100 m
10Base-FL - światłowód (fiber optic) 10 Gb/s
100Base-T - skrętka i światłowód
100Base-T4 - skrętka kat. 3, kodowanie 8B/6T

100Base-TX - dwie pary skrętki kat. 5, kodowanie 4B/5B maks. 200 m
100Base-FX - światłowód wielomodowy
1000Base-T - skrętka co najmniej kat.5

10Base5 - kodowanie Manchester
10Base2 - kodowanie Manchester
10BaseT - kodowanie Manchester
10BaseFL - kodowanie Manchester, fizycznie NZR

Gruby kabel koncentryczny - 10 Base5

- 10 Mb/s
- maks. 500m / stacje można podłączać co 2,5m (bo musi powstać fala stojąca)
- kodowanie Manchester
- komponenty sieci
  - interfejs sieciowy AUI (Adapter Unit Interface)
  - kabel tranceiverowy AUI (maks. 50m) (skrętka ekranowana, używane 8 kabli)
  - MAU (Medium Attachment Unit) - zewnętrzny tap/trancepiver
  - terminatory 50 ?

Cienki kabel koncentryczny -
Skrętka - } Zainteresowanym polecam skrypt do æwiczeñ ✳:

Gigabit Ethernet

1000BaseT - skrętka co najmniej kat.5, używane 4 pary do jednoczesnej, obustronnej transmisji

4D-Pams - pięciopoziomowe sygnały niosące 2bity/każdy

125 Mbaud na każdej z czterech par - maks. 100m

1000BaseX - różne podstandardy, kodowanie 8B/10B - używane 250 z 1024 sygnałów (balans poziomu) fizycznie NRZ

100BaseFX- światłowód wielomodowy, kod 4B/5B fizyczne NRZI

100BaseTX - dwie pary skrętki kat. >= 5. Kodowanie 4B/5B, fizycznie MLT-3 transmisja 125 Mbaud, maks. 100m

100BaseT4 - cztery pary skrętki kat.3 8B/6T

1000BaseT

- suplement 802.3ab do standardu IDEE
- miliard bitów na sekundę przez UTP
- skomplikowana metoda kodowania
  - te same pary używane do nadawania i odbioru
  - kodowanie 4D-Pams(a nie ma być 4D-PAM5 ???) / pięciopoziomowe sygnały niosące 2 bity każdy
- 125 Mbaud*4 part*2 bity/takt - 1000 Mb/s
- kat. >-5 dł. do 100m

CSMA/CD - obowiązuje tylko dla sieci pracujących w trybie półdupleksowym

Gigabitowy Ethernet występuje tylko w trybie fullduplekso wym. To co zostaje to postać ramki.

Konfiguracja maksymalna sieci Ethernet

- regenerator sygnału (repeater)
  - pozwala zwiększyć rozmiar segmentu sieci
  - zapewnia odtworzenie charakterystyki sygnału
  - ograniczenia - reguła 5-4-3 (reguła czterech repeaterów)
    - § można połączyć do pięciu segmentów sieci
    - § do tego używa się czterech repeaterów
    - § tylko do trzech segmentów można podłączyć komputery (pozostałe dwa to łącza między repeaterami)
- hub (wieloportowy repeater)
  - wzmacnia sygnał i przesyła na wszystkie pozostałe porty

Tryb pełnego dupleksu

- Ethernet - tryb półdupleksowy
- Pełny dupleks
  - równoczesna transmisja w obie strony
  - łącze musi być punkt-punkt. Oba interfejsy muszą obsługiwać ten tryb
  - przestawienie w tym tryb administracyjnie albo przez protokół autonegocjacji
  - wyższa przepustowość (np. 200 Mb/s na łączu 10 Mb/s)
  - osobne ścieżki dla odbioru i transmisji danych
    - § tak jak na skrętce jedynie fizycznie
    - § protokół CSMA/CD - pracuje tylko na półdupleksu

Trybie pełnego duplexu

- CSMA/CD - musi być wyłączony
- ignorowanie carrier sence (CS)
- brak , wielodostępu(MA)
  ignorowanie wystąpienia kolizji (CD)
- Huby nie mogą być używane
- Nie może być używane m.in. 10Base2/10Base5
- Brak ograniczeń protokołów na długość medium
- Odległość medium - odległość może być znacznie większa
- skrętki to nie dotyczy (100 m)
- światłowód np. 100 BaseFX do 2m na MMF i do 20km na jednomodowym
- opisany w suplemencie 802.3x (1997r.)

Protokół autonegocjacji

- Automatyczna konfiguracja sprzętowa Ethernetu
- Głównie skrętka
- Główne zadania
  - Dopasowanie szybkości interfejsu (np.. 10-100-1000 Mb/s)
  - Włączenie trybu pełnego dupleksu
- Procedura wykonywana jednokrotnie w czasie inicjalizacji połączenia
- Włączony system sygnalizacji
- Rozgłaszanie własnych możliwości
  - Tablica priorytetów (od najszybszych do 10BAseT)
  - Wybór HCD (highest common Denominator)

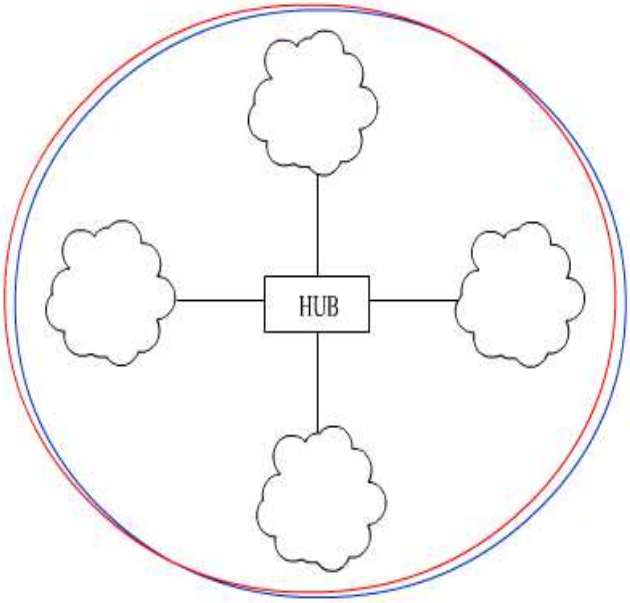
Domena kolizyjna a rozgłoszenia

Domena kolizyjna to fragment sieci, w której transmisja musi być realizowana przez urządzenie w sposób wykluczający prowadzenie w tym czasie transmisji przez inne urządzenia (granicę stanowią porty urządzeń : bridże, switch lub router)

Domena rozgłoszeniowa to fragment sieci, jaki pokonują ramki typu broadcast lub multicast (ograniczona przez urządzenia warstwy 3 tj. routery lub sieci wirtualne)

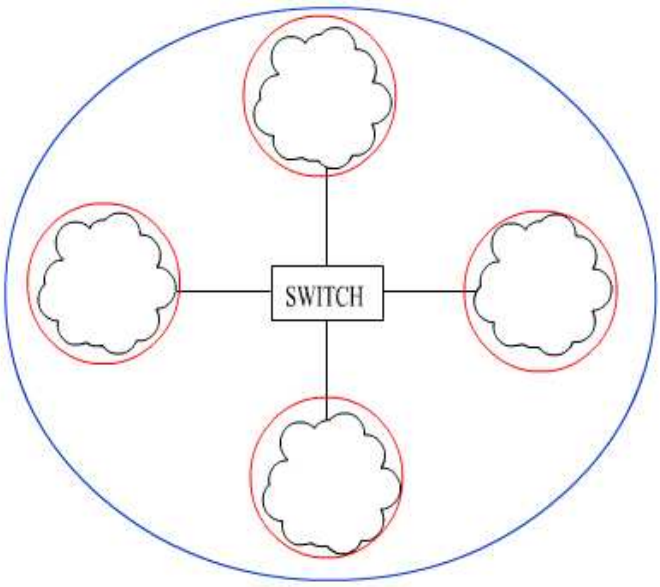
Żadne urządzenie warstwy drugiej nie ogranicza wielkości domeny rozgłoszeniowej !

Segmentacja urządzeń warstwy pierwszej



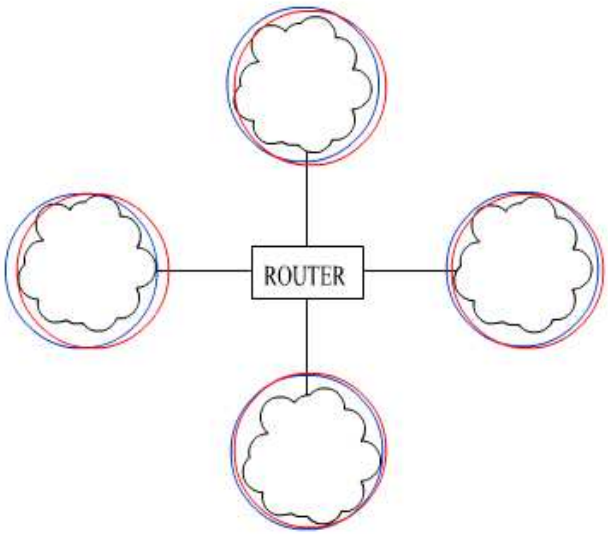
domena kolizyjna = domena rozgłoszeniowa

Segmentacja urządzeń warstwy drugiej



Ograniczenie domeny rozgłoszeniowej (separacja domeny kolizyjnej)

Segmentacja urządzeń warstwy trzeciej



Separacja domen kolizyjnych i rozgłoszeniowych. W pełni skalowalne rozwiązanie

---

Segmentacja sieci

2. Regenatory sygnałów pozwalając zwiększyć rozległość sieci ale w ten sposób zwiększa się też prawdopodobieństwo kolizji (wielkość domeny kolizyjnej)

3. BRAKI
4. Niewielkie opóźnienia wnoszone przez te urządzenia nie stanowią najczęściej problemu
5. Nie zmniejsza się wielkość domeny broadcastowej, gdyż ramki o odbiorcach grupowych i rozgłoszeniowych są przekazywane przez te urządzenia

Zasada działania urządzenia typu mostek (bridge)

⇒ Działa na poziome warstwy OSI/ISO - interpretuje więc zawartość ramek
⇒ Ze swojego punktu widzenia dzieli sieć na dwa segmenty, na podstawie numeru portu do którego podpięta jest podsieć
⇒ Posiada wiedzę pozwalającą na stwierdzenie w którym segmencie sieci znajduje się host o danym adresie MAC
⇒ W oparciu o tą wiedze podejmuje decyzję czy i jeżeli tak do którego portu przekazać ramkę, której adres docelowy pobiera i analizuje <pomieszały im się mostki ze switchami J>
⇒ (dalej będzie mowa o mostkach typu transparent)

Działanie mostka

<rysunek>

Mostki uczą się na adresie źródłowym

Zalety

- Mniejsza ilość ramek w każdym segmencie
- Ulega zmniejszeniu prawdopodobieństwo kolizji

Po kilku sekundach tablice są mazane

Skąd mostki wiedzą o położeniu komputerów ?

Uczą się same !

- Działają w trybie promiscuous pobierając adres źródłowy z każdej ramki i wpisując do specjalnej tablicy

Adres źródłowy	Nr. Portu przez który dany komputer jest osiągalny
•	•

-

Braki
Ze względu na zmienność sieci, nieodświeżane wpisy zachowują ważność tylko przez określony czas, a po jego upływie są usuwane

Jak mostki wykorzystują wiedzę ?

- Gdy mostek odbiera ramkę, porównuje jej adres docelowy z wartościami z tablicy FDB.
- Gdy port jest ten sam, jak port z którego przyszła ramka - nic nie robi
- Gdy port jest inny - przekazuje ją dalej (---------are U sure ?
- Gdy nie znajdzie wpisu - przykazuje na wszystkie (a ileż tych portów jest?) pozostałe porty
- Gdy adres jest adresem grupowym lub rozgłoszeniowym przekazuje na wszystkie pozostałe porty

- Ze względu na zmienność (?????????) sieci, nieodświeżane wpisy zachowują ważność tylko przez określony czas, po jago upływie są usuwane

Cykle (rysunek dwa kompy połączone przez dwa mostki)

- Ze względu na niezawodność istnieją połączenia redundantne
- Może nastąpić krążenie ramek w sieci
    - Komputer X wysyłą ramkę do komputera Y. Tablica obu mostków .....
- Rozwiązanie: dynamiczna adaptacja do warunków panujących w sieci, czasowa dezaktywacja nadmiarowych połączeń

Sieci komputerowe - wykład 4

Warstwa 3

Plan wykładu:
- miejsce w modelu OSI/ISO
- funkcje warstwy sieciowej
- adresacja w warstwie sieci
- protokół ARP
- protokoły RARP,BOOTP,DHCP

Warstwa sieci
Jej zadaniem jest dostarczenie logicznej adresacji. Warstwa ta odpowiada za znalezienie najlepszej drogi łączącej dwa hosty, której mogą się znajdować w oddalonych, z punktu widzenia warstwy łącza danych, sieciach.
Jedenym z protokołów pracujących w warstwie sieciowej jest Internet Protocol (IP). Inne: IPX, AppleTalk, NetBEUI)

Po co adresacja w warstwie sieci?

Mamy **adresy Ethernet** - unikalne w skali światowej ale:
- Instnieją różne standardy komunikacji, nie tylko Ethernet
- Adresy Ethernetowe mają PŁASKĄ przestrzeń adresową:
- Uniezależniamy się od warstwy lacza danych !
- Nieskalowalne
- Brak powiązań z geograficznym rozmieszczeniem

Adres IP
- Jest hierarchiczny
- Powiązany z położeniem geograficznym adresowych urządzeń, dzięki temu można znaleźć też drogę do odbiorcy
- Jest skalowalny
- Podobny w istocie do rozmów telefonicznych

Adres IP v 4
10110110110111010110101011001011- 32 bity

Sieć Host

mniejsza przestrzeń adresowa niż w Ethernecie (ok. 4,3mld). Są z tym związane kłopoty ponieważ zaczyna już brakować wolnych numerów IP

Skąd można uzyskać adres?
Ethernet - adres zaszyty na karcie sieciowej
W przypadku braku połączenia do sieci globalnej można podać dowolny adres
W przeciwnym wypadku:
Numer sieci należy uzyskać od NIC (Network Information Center) lub Internet Provider (tak było na wykladzie, choc mi wydaje się to glupie - przeciez inretnet proveder będzie miał te numery wlasnie od NIC)
Numery hostów przydzielane są wg własnego uznania (lokalny administrator)

Do czego przypisany adres?

- Adres nie jest związany ani z urządzeniem (komputery, drukarka, itp.) tylko z kartą sieciową. Host może mieć wiele kart sieciowych a więc wiele adresów IP.
- Każda karta sieciowa komputera w sieci IP ma przypisany co najmniej 1 adres IP
- Wszystkie hosty dołączone do tej samej z punktu widzenia warstwy łącza danych sieci mają identyczny adres sieci

adres sieci i hosta
<rys>

Routery
<rys>

- wyznacza drogę pakietom
- pozwala łączyć sieci o różnych standardach warstwy drugiej
- ograniczają domenę rozgłoszeniową

Notacja adresów
binarny ŕ 00000110 | 10000100 | 00000010 | 00000001
szesnastkowy ŕ 0x06840201
zapis dziesiętny ŕ 109314561
zapis dropkowo-dziesiętny ŕ 6.132.2.1

Klasy adresowe

Klasa	Ilość sieci	Ilość komputerów	
A	126	Ponad 16mln	ß sieć ŕ ß komputer ŕ 0xxxxxxx
B	ok. 65 tys.	Ok. 65tys.	ß sieć ŕ ß komputer ŕ 10xxxxxx
C	ponad. 16mln.	254	ß sieć ŕ ßkomp.ŕ 110xxxxx

D	multicast	1110xxxx
E	zarezerwowan e	1111xxxx

Wyznaczanie numeru sieci i hosta
197.50.33.254
\--/
11000101 - klasa C
nr sieci: 197.50.33.254
nr urządzenia: 254

1.0.0.0	-	127.255.255.255	Klasa A
128.0.0.0	-	191.255.255.255	Klasa B
192.0.0.0	-	223.255.255.255	Klasa C
224.0.0.0	-	239.255.255.255	Klasa D

Adresy specjalne

0.0.0.0 - ten komputer w tej sieci. Podawany jako adres źródłowy w trakcie uruchamiania komputera gdy nie zna on jeszcze swojego IP

0.x.y.z - komputer x.y.z w tej sieci. Podawany w uruchamiania jako adres źródłowy w komputerze posiadającym niekompletne informacje

x.0.0.0 - dowolny komputer w sieci x

127.x.y.z - adres loopback (pętla zwrotna). Pakiet wysłany na taki adres nie może zostać wysłany poza komputer. Pozwala aplikacjom pracującym na tym samym komputerze komunikować się poprzez stos TCP/IP

Adres typu broadcast

Mogą być podawany tylko jako adres docelowy

Ograniczony broadcast - 255.255.255.255 - adres wszystkich hostów w sieci lokalnej. Nigdy nie są przekazywane przez rutery.

Broadcast sieciowy - adres w którym części adresu komputera składa się z samych jedynek, zaś część sieci jest określona. Oznacza wszystkie komputery w danej sieci np. 130.1.255.255 - wszystkie komputery sieci 130.1

Adres IP specjalnego przeznaczenia

Nazwa	Sieć	Host	Źródło	
	0	0	OK	
	0	Host IP	OK	
Loopback	127	Cokolwiek	OK	OK
Ogr. Broadcast	-1	-1	Nigdy	OK
Broadcast skierowany do sieci	NetId	-1	Nigdy	OK.

Tworzenie podsieci - Cele

- Zbyt dużo komputerów w klasach A(2^{24}-2) B(2^{16}-2)
- Zmniejszenie domeny rozgłoszeniowej
- Pozwala ukryć szczegóły budowy sieci przed ruterami zewnętrznymi
- Mogą istnieć różne rodzaje sieci lokalnej, które trzeba jakoś połączyć
- Lepsze podsieci w klasie B niż wiele sieci klasy C, ponieważ redukuje to wzór tablic rutowania

Przykładowy adres IP klasy B: 129.156.10.18
Adres sieci: 149.156 | adres komputera 10.18
Adres sieci: 149.146| adres podsieci:10 | adres komputera 18

Maska podsieci

- Ma 4 bajty (32 bity) - identycznie jak adres IP
- Zawiera bity jedynek dla części logicznej adresacji sieci i bity zer dla części, która jest adresem komputera
- mogą być nieciągłe ale nie zaleca się takiej praktyki
- zapis: szesnastkowy, kropkowo-dziesiętny lub liczba bitów znaczących

<walnięty rysunek>
@#$!@#$%@#$%#$@%@#$%@#$%#$@@% 0xFFFFFF00 lub 255.255.255.0 lub /24
%#$@%@#$%@#$%@#$%@#$%#$%#$%$%0xFFFFFFC0 (tylko na hexy przeliczylem)
255.255.255.192 lub /26

Numer sieci, podsieci i hosta
<duzo cyferek, strzałek itd. Jak komuś się będzie chcialo to niech wrypie to tu>

Adresy IP specjalnego przeznaczenia
Broadcast skierowany do sieci
Oznacza wszystkie komputery w danej podsieci np.
10.20.30.255/24 wszystkie komputery w sieci 10 i podsieci 20.30
Broadcast skierowany do wszystkich komputerów we wszystkich podsieciach danej sieci
10.255.255.255/24 - wszystkie komputery w każdej podsieci sieci 10
adres nie powinien być przekazywany przez rutery

Protokół IP - właściwości

- § bezpołączeniowy - każdy pakiet przesyłany samodzielnie
- § brak potwierdzeń dostarczenia pakietu
- § brak timeout-u i retransmisji
- § brak kontroli poprawności danych - tylko kontrola nagłówka

- § brak kontroli przepływu
- § ograniczanie wiadomości
- § brak wykrywania powtórzeń tych samych pakietów
- § brak zachowania kolejności pakietów

Budowa datagramu IP

0 4	8	12	16	20	24	28	32
Wersja	Dł.nagł.	Typ usługi (TOS) DLK,RLB BDW,CST		Długość całkowita			
Identyfikacja				0	DF	MF	Suma kontrolna nagłówka
Adres źródłowy							
Adres docelowy							
Opcje (jeśli są)							
Dane							

- § *długość nagłówka*: wyrażana w jednostkach 32bitowych max rowna 15x4bajty = 60bajtów - narzuca ograniczenia w stosowaniu niektórych opcji. Typowo 20 (wiec wartość 5)
- § *typ usługi*
  - o opóźnienie (np. telenet)
  - o niezawodność (np. SNMP)
  - o przepustowość (np. ftp)
  - o koszt (np. news)
  - o priorytety
- *długość całkowita* : bajty - max 64 kB
- *czas życia (TTL)* liczba przeskoków; zapobiega krążeniu pakietów
- *protokół*: typ danych w polu dane
- *suma kontrolna nagłówka*: dotyczy tylko nagłówna; o poprawność danych muszą zabiegać protokoły wyższych warstw

Dzielenie datagramu IP

- Maksymalny rozmiar datagramu IP (65535 bajtów), może przekraczać maksymalny rozmiar pakietów warstwy niższej (np. Ethernet 1518 bajtów)
- Jeżeli warstwa IP ma do wysłania datagram to pyta interfejsu o jego MTU (maximum transmission unit), jeśli długość datagramu przekracza MTU to go fragmentuje
- Może dzielić komputer wysyłający i routery pośrednie
- Składanie następnie TYLKO u odbiorcy - routery pośrednie nie wykonują tej czynności. Podzielony datagram dociera w takim stanie do odbiorcy

Ramka IP - fragmetacja

Pola ważne przy fragmentacji:

- wszystkie fragmenty mają takie samo pole *identyfikacja*
- *DF - Don't Fragment*
- *MF - More Fragments*
- *Przesunięcie fragmentów* - numer pierwszego bajtu danych w stosunku do orginalnego datagramu (po 8 bajtów)
- <rys. pokazujący podział datagramu IP do ramki Ethernet , lub cos w tym stylu>

Składanie pakietów IP

Z każdym otwartym niezupełnym pakietem IP związany jest bufor, tablica znaczników i zegar

- na podstawie przesunięcia fragment wstawiany jest w odpowiednie miejsce w buforze
- wypełnienie trwa aż do otrzymania ostatniego fragmentu, tzn. najdalej przesunięty fragment posiada wyłączony bit *MF* i cały jest wypełniony
- Po każdym otwartym fragmencie ustawiany jest zegar. Inicjalizowany jest wartością max(wart_pocz,TTL). Jeżeli zegar zliczy do zera bufor jest zwalniany i pakiet odrzucany (np. Windows!!!)
- Fragmentowanie jest niewskazane bo jeżeli zginie jeden mały fragment niepodzielnej informacji to musimy ja wysłać od nowa (lepszym rozwiązaniem jest podzielić informację wcześniej) - o czemu to na czerwono??? mi pasuje jak najbardziej

Pozostałe pola datagramu IP

- *adres źródłowy* -ZAWSZE adres pojedynczego komputera
- *adres docelowy*
  - adres pojednyczego hosta
  - adres grupowy
  - adres rozgłoszeniowy
- *opcje*
  - zapis trasy - definiuje ścieżkę po której pakiet ma przejść

Dokumentacja

- Internet Protocol - RFC 972 (patrz: www.ietf.org/rfc)
- Tysiące książek dotyczących sieci komputerowych

Protokół ARP (Adres Resolution Protocol)

<rys. kompy połączone przez sieć, każdy ma nadany adres IP i Ethernetowy; przedstawienie danych w ramkach>

Odwzorowanie ramki adresu IP na adresach warstwy łącza danych

Ethernet	.*	Dane	CRC	

Ethernet destination address	Ethernet source address	Frame type, hard type, prot type, hard size,prot sieze,	Op	Typ	Adres nadawcy w protokole warstwy 2	Adres nadawcy w protokole warstwy 3	Adres odbiorcy w protokole warstwy 2	Adres odbiorcy w protokole warstwy 3
6B	6B	1B	1B	2B	6B (6B)	4B (4B)	6B (6B)	4B

Poprawnie jest w biblii:

Nagl. Ethernet	pytanie/odpowiedz ARP

Ethernet destination address	Ethernet source address	Frame type	Typ protokołu warstwy 2 (Eth=1)	Typ protokołu warstwy 3 (IP=0x8000)	rozmiar adresu w. 2	rozmiar adresu w. 3	Typ	Adres nadawcy w protokole warstwy 2	Adres nadawcy w protokole warstwy 3	Adres odbiorcy w protokole warstwy 2	Adres odbiorcy w protokole warstwy 3
6B	6B	2B	2B	2B	1B	1B	2B	nB	mB	n	mB

- Frame type: dla ARP- 0x0806
- Typ
  - zapytanie : wartość 1
  - odpowiedz: wartość 2

n, m - określana na podstawie rozmiaru adresu (podanego wczesniej)
dla pary Ethernet - IP n=6, a m=4

ARP - zasada działania

- zapewnia dynamiczne mapowanie adresów IP na adresy warstwy łącza danych
- <jakiś rysunek ramki>
- <rysunek prezentujący zasadę działania ARP
- zapytanie ARP zawiera adres IP hosta przeznaczenia oraz następujące żądanie "jeżeli jesteś właścicielem tego adresu IP to odpowiedz mi, odsyłając swój adres sprzętowy" Wysyłane jest do wszystkich hostów w sieci
- moja wersja: host który stwierdzi, iż docelowy adres wartswy trzeciej należy do niego, odpowiada analogicznym pakietem, tyle że z wypełnionym polem o adresie docelowym wartswy drugiej. Pakiet ten jest przesyłany unicastowo tylko do nadawcy

Własności ARP

- Każdy host zawiera tablicę ARP z zapisanymi odwzorowaniami pomiędzy adresami sprzętowymi
- proxy ARP
  - umożliwia ruterowi odpowiadanie na zapytanie ARP kierowane z jednej dołączonej do niego sieci przekazując informację o hoscie pracującym w drugiej sieci
  - umieszczony pomiędzy sieciami ukrywa przed nimi ich istnienie pozwalając na korzystanie w obydwu z tego samego adresu sieci (ja mam dokładnie tak)
  - pozwala na komunikację źle skonfigurowanym hostom
  - pozwala na komunikację z hostami źle(nie) obsługującymi podsieci
- Gratuitous (zbędny) ARP
  - Wyklucza istnienie dwóch hostów o takim samym adresie IP

- Pozwala na odświeżanie informacji po wymianie NIC

Domain Name System - system Nazw Domen

Cel: realizacja odwzorowania między nazwami logicznymi a adresami IP. Jest to tak zwany serwis prosty.

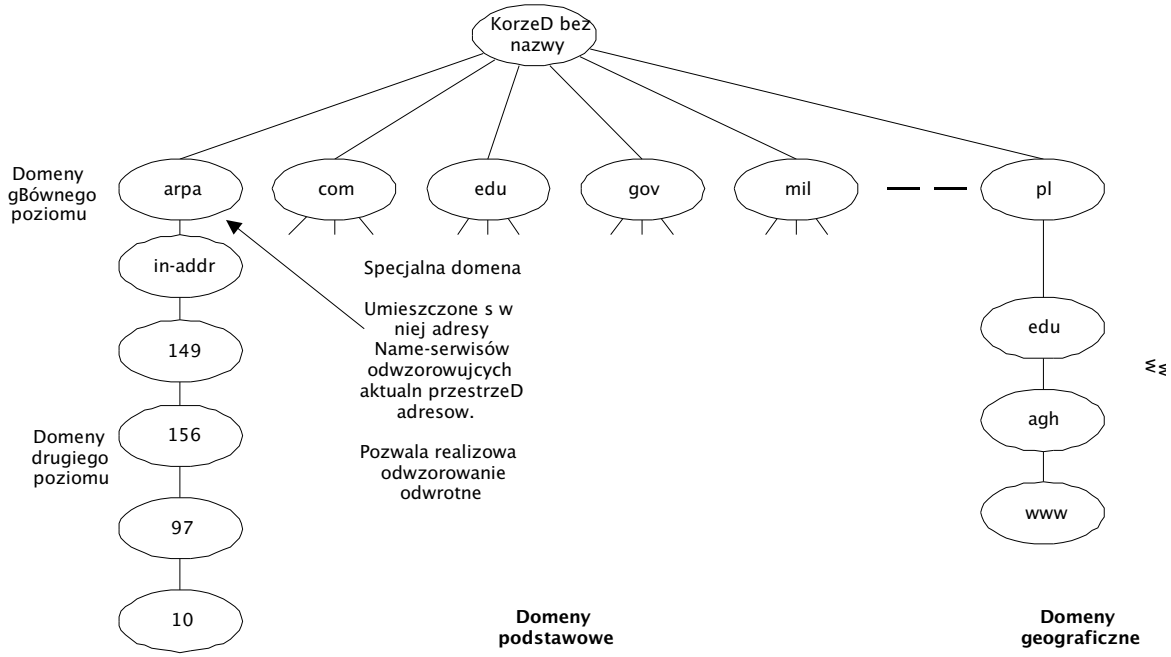
Pytanie czy istnieje odwrotny DNS - TAK !

Definicja

DNS to rozproszona baza danych używana przez aplikacje TCP/IP do odwzorowania nazw hostów na adresy IP i odwrotnie.

Rozproszenie polega na tym, że żaden system nie posiada pełnej informacji o tym odwzorowaniu, informacje te rozdzielane są pomiędzy niezależne serwery.

Hierarchiczna budowa nazw



Nazwy DNS

- Każdy węzeł drzewa może mieć etykietę do 63 znaków (A-Z,a-z,0-9,-). Wyjątkiem jest korzeń, który nie mam nazwy
- Nazwy nie rozróżniają wielkości liter
- Nazwa zakończona kropką jest nazwana absolutną, nazwą domeny lub w pełni określoną nazwą domeny (ang. FQDN)
- Zakłada się, że nazwa bez końcowej kropki musi być uzupełniona - jeżeli składa się z dwóch lub więcej członów
  - Może być znakowana jako w pełni określona
  - Może ona też być uzupełniona przez dodanie nazwy zależnej od lokalizacji węzła

Obszary i ich obsługa:

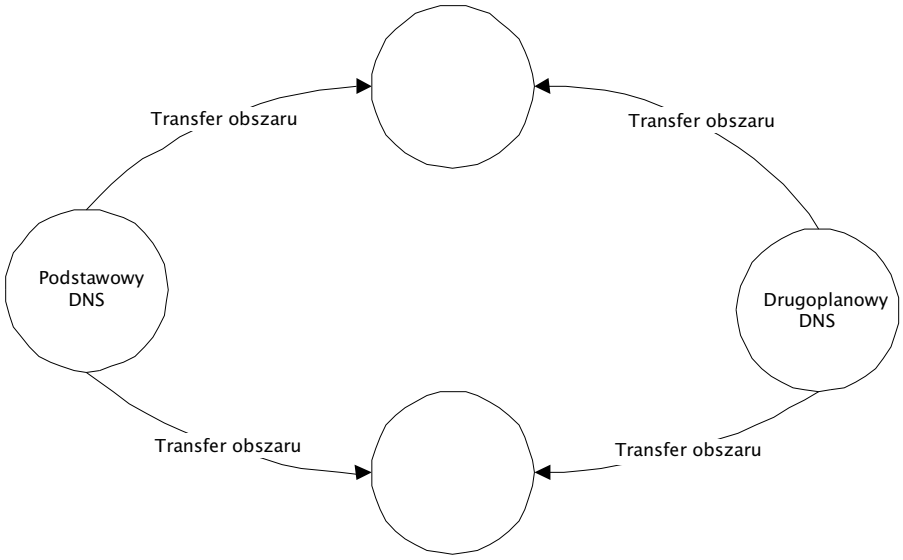
6. **Obszar** jest częścią drzewa DNS, która jest oddzielnie administrowana

- Może być podzielony na mniejsze obszary. Następuje wówczas delegacja odpowiedzialności

7. Delegowanie odpowiedzialności za zarządzanie etykietami sprawia, że rozwiązanie staje się skalowalne
   - Nigdy pojedyncza jednostka nie zarządza wszystkimi etykietami w drzewieOpdowiedzialność jest delegowana w dół
8. Na świecie znajduje się 6 serwerów , w których znajdują się kopie głównego węzła DNS*(o coś takiego chodziło)*

Podstawowe i drugoplanowe serwery nazw

- Każdy obszar musi zawierać podstawowy serwer nazw i jeden lub więcej drugoplanowych serwerów nazw
- Serwer drugoplanowy obejmuje informację poprzez transfer obszaru



Plik: *(to chyba jest malo istotne)*

1.2.2.3	IPAQ.domena
1.2.2.1	PC.domena
1.2.2.1	Sun.domena

Zapytania:

- Rozwiązywanie nazw polega na wysyłaniu zapytań i otrzymywaniu odpowiedzi
- Każdy serwer zna adresy hostów ze swojej domeny, adresy hostów do który delegował odpowiedz, adresy głównych serwerów nazw, adres serwera domeny macierzystej itd. (ftp.rs.internic.net/domain/named.root)
- Rekurencyjne i iteracyjne

Chętny do przerysowania rysunków ???

Pamięć podręczna

§ Wszystkie serwery DNS stosują pamięć podręczną aby zredukować wymianę komunikatów DNS i zwiększyć efektywną działalność
   - Odpowiedzi automatyczne - pochodzą od serwerów z odpowiedniej domeny
   - Odpowiedzi z pamięci podręcznej nie są automatyczne
   - Wraz z odpowiedzią automatyczną serwer otrzymuje TTL określający jak długo należy przechowywać daną informację w pamięci podręcznej

O co pytamy ? : Zapytania proste

- § Najczęściej występujące - jaki IP ma dana stacja
- § Zapytania wskazujące
  - o Po podaniu adresu IP dostajemy nazwę DNS 149.156.98.14 ->x.y.z
  - o Wykorzystana jest domena In-addr.arpa (dla w/w przykładu będzie to: 14.98.156.149.in-addr.arpa.)

Rysunek raczej oczywisty

O co pytamy ?: Inne typy

- o A - adres
- o MX - serwer poczty dla określonej nazwy maciek@poczta.pl -> mail.poczta.pl
- o NS - autorytatywny serwer DNS dla danej domeny
- o CNAME - nazwa kanoniczna (alias)
- o MINFO - informacje na temat komputera
- o Inne

Rekord w DNS

<Name, Value, Type, Lass, TTL)

Class - IN (Internet)
TTL - czas ważności

Np:
<edu.pl, dns.edu.pl, NS, IN>
<dns.edu.pl, 149.156.128.177,A,IN>

<'root',dns.edu.pl, NS, IN>
<dns.edu.pl, 149.156.128.177,A,IN>

Przykład konfiguracji serwera:

nie chce mi się przepisywać - dość oczywiste

UDP i TCP

DNS obsługuje zarówno UDP jak i TCP

- Dobrze znany port UDP i TCP nr. 53
- UDP stosowany jest najczęściej
- TCP wykorzystywany jest jeżeli odpowiedz od serwera nazw przekracza 512 bajtów - jest to wielkośc pakietu UDP jaki musi być w stanie odebrać końcowy host
- Jeżeli odpowiedz UDP zawiera informację o tym, że ilość informacji zastała obcięta do wymaganych 512 bajtów to resolver ponawia zapytanie do TCP
- TCP jest używane do transmitowania obszarów.
- Przy stosowaniu UDP programy muszą same obsługiwać czasy oczekiwania i retransmisji

NAT - Network Address Translation

Expanding Enterprise Connectivity with Network Address Translation (NAT)

- Market consolidation
  - Mergers
  - Acquisitins

- IP changes
- IP address management
- RFC 1918 usage
- IP address conservation
- Network privacy
- Cisco 10S Nat in RFC 1613

Inside Local (IL) - The IP address assigned to a host on the inside network. This address may be globally unique allocated out of the private address space defined in RFC 1918 or mey be officially allocated to some other organization

Inside Global (IG) - The IP address of an inside host as it appers to the outside world. These addresses can also be allocated out of the private address space defined in RFC 1918, or may be officially allocated to some other organization, or allocated from a globally-unique address space, typically provided by the ISPI (if the Enterprase is connected to the global Internet)

Outside Local (OL) - The IP address of an outside host as it appears to the inside network. These addressed can be allocated from the RFC 1918 space id desired.

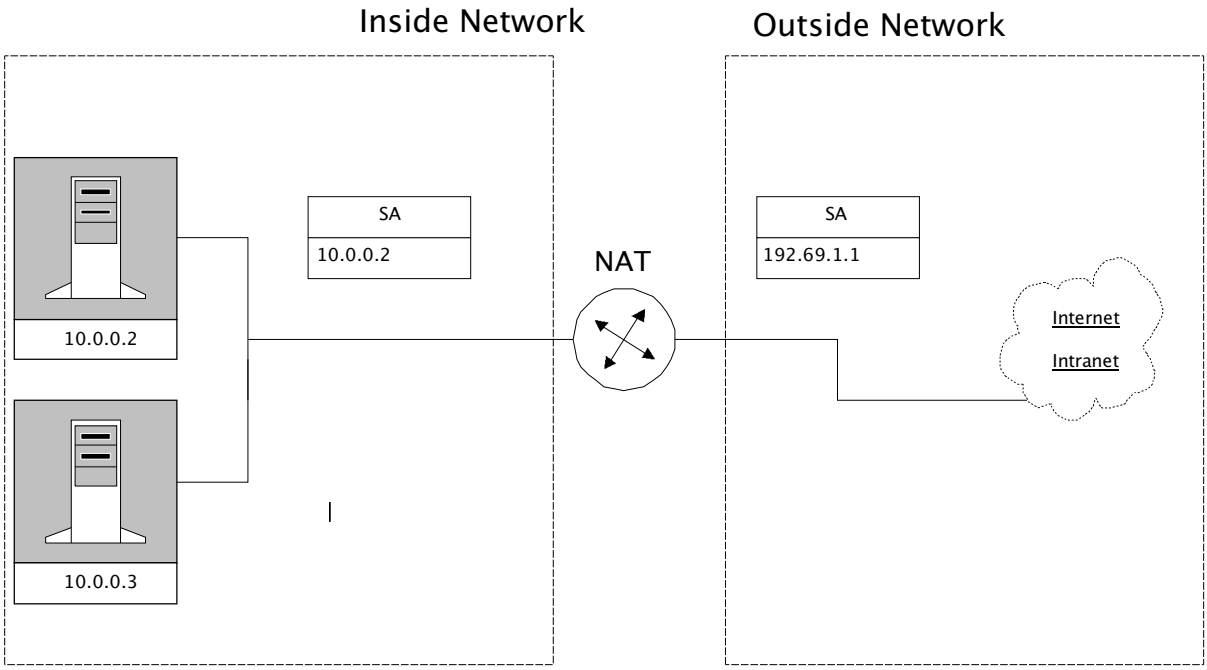
Outside Global (OG) - The IP address assigned to a host on the outside network
BRAKI

NAT modes:

- Static - statically configured one-to-one mapping between inside local and global addresses
- Dynamic mapping between the inside local and global addresses. Translations are created when needed

Port - to liczba (adres) dwubajtowa, która pozwala nam na adresowanie serwisu w obrębie komputera

- ??? Single Network Address Translation - maps one IP address to another. One-to-one translation work bi-directionally
- PORT Address Translation (PAT) - maps one IP address and port pair to another ???. Unique port numbers identify translations on single IP address. One-to_N translation. Consumers reqistered IP addresses. Works uni-directionally. Also called "Extended Network Address Translation)



The "internal" hosts use different required IP address as seen from the "outside" network

Nat Table	
Outside Local	???Outside Global???
171.68.1.1	10.0.0.20
171.68.1.2	10.0.0.21

Enables one to use internal addresses which "overlap" with external addresses.

Equivalent to "outside destination" translation

Rysunek

Nat Table	
Inside Local Ip Addres	**Inside Global** Ip Adres
10.0.0.2	**192.69.1.1:5001**
10.0.0.3	**192.69.1.1:5--2**

Port multiplexed "inside source" translation. All internal hosts are a single registered IP

Przykład konfiguracji NAT z DNS

Rysunek

Konfiguracja NAT'a:

	Source IP	Type	Destination IP	Type
1)	10.1.1.1	IL	10.1.1.10	IL

2)	10.1.1.10	IL	192.168.1.254	OL
3)	140.16.1.254	IG	10.1.1.10	OG
4)	10.1.1.10	OG	140.16.1.254	IG
5)	192.168.1.254	OL	10.1.1.10	IL
6)	10.1.1.10	IL	10.1.1.1	IL

Przykład 2 (bez pośrednioego DNS'a)
<Rysunek>

Konfiguracja NAT'a

	Source IP	Type	Destination IP	Type
1)	10.1.1.1	IL	192.160.1.75	OG
2)	140.16.1.55	IL	140.	OG
3)		OG		IL
4)		IL		IL

Plan wykładu:

- miejsce w modelu OSI/ISO
- tabela routingu
- routing statyczny kontra dynamiczny
- podział protokołów routingu
- protokoły wewnętrzne: RIP+RIP2,IGRP,OSFF
- protokoły zewnętrzne EGP,BGP

Miejsce w modelu OSI/ISO:

- warstwa sieciowa
- Funkcje warstwy sieciowej: Wprowadzenie jednolitej adresacji niezależnej od niższych warstw (IP)
- Dostarczenie pakietu do nadawcy od odbiorcy (RIP,IGRP,OSPF,EGP,BGP)

Podsieci

Przykład: adres IP klasy B 177.220.0.0

- postać binarna: 10110001.11001010.0.0
- dwa bajty na podsieć (max komputerów
- Maska: 255.255.240.0
- Pytanie:
  - jaka jest liczba podsieci? Odp.: 4bityč 2^4-2=14 podsieci
  - jaka jest możliwa liczba komputerów w podsieci? Odp.: 12 bitów č 2^12-2=4094komputery

Przykład: adres IP klasy C: 197.197.197.0 *(jak ktoś chce niech sobie przećwiczy i uzupełni)*

Classless Inter-Domain Routing (CIDR)

Problem 1:

- brak wolnych adresów sieci. Np. tylko 16384 sieci klasy B
- rozwiązanie: "dzielenie" adresów klasy B na mniejsze (odpowiadające klasy C)

Problem 2:

- wzrost wielkości tablic routingu
- rozwiązanie: agregacja tablic routingu w zależności od providera lub od lokalizacji geograficznej (kilka adresów należących do pewnego regionu geograficznego, bądź do jednego providera internetowego jest reprezentowane w tablicy routingu przez jeden prefiks - oczywiście pod warunkiem ze takie prefiks istnieje)

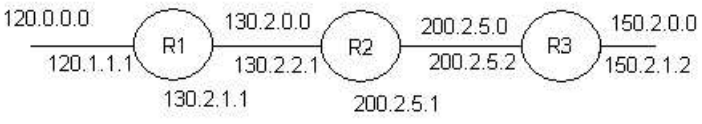
BGP-4 używa dwóch atrybutów do obsługi agreagacji (ang. aggregator)

Podsumowanie:

- Dzielenie adresów klasy B jest środkiem zapobiegającym ich wyczerpaniu
- Podobnie CIDR służy oszczędzaniu adresów przez ich gęstą alokację
- Techniki te są jednak środkami przejściowymi, jedynym rozwiązaniem omówionych problemów jest nowy schemat [adresowania] adresacji

Tablice routingu

Zawiera skojarzenia pomiędzy adresem IP przeznaczenia (może to być zarówno pełny adres komputera jak i adres sieci) a adresem IP routera następnego przejścia (**ang. next hop**)



R1	*R2*

Sieć docelowa	*IP następnego przejścia*	*Sieć docelowa*	*IP następnego przejścia*
200.2.5.0	*130.2.2.1*	*120.0.0.0*	*130.2.1.1*
150.0.0.0	*130.2.2.1*	*150.2.0.0*	*200.2.5.2*
120.0.0.0	*Bezp. dołączona*	*130.2.0.0*	*Bezp. dołączona*
130.2.0.0	*Bezp. dołączona*	*200.2.5.0*	*Bezp. dołączona*

Tablica routingu - wnioski

- routing IP jest dokonywany na podstawie kolejności przejść
- router nie zna pełnej trasy do żądanego z punktów przeznaczenia
- routing jest możliwy dzięki przekazywaniu datagramu do następnego routera. Zakłada się, że kolejny router jest "bliżej" punktu przeznaczenia niż komputer wysylający informację oraz że wysyłający komputer jest połączony z jakimś routerem, który odbiera od niego datagramy

Protokoły routingu

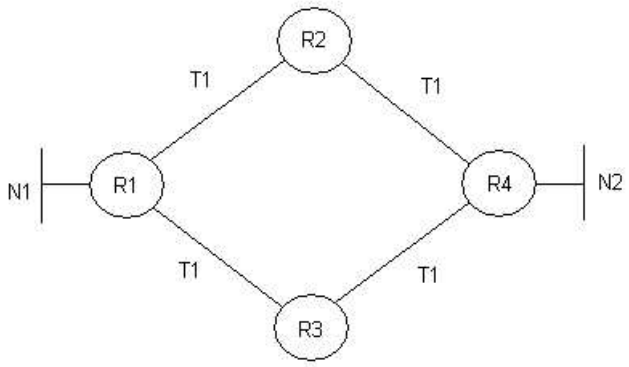
Zbieżność (cecha protokołów dynamicznego routingu) - po pewnym czasie tablice routningu dochodzą do pewnego, ustalonego stanu

- Router potrzebuje czasu na znalezienie alternatywnej ścieżki w wypadku zmiany topologii sieci (np. awaria)
- Czas, po którym routery będą miały jednakowy "obraz" sieci jest zależny od konfiguracji (np. odstęp między periodycznie rozsyłanymi pakietami)
- <rysuneczek>

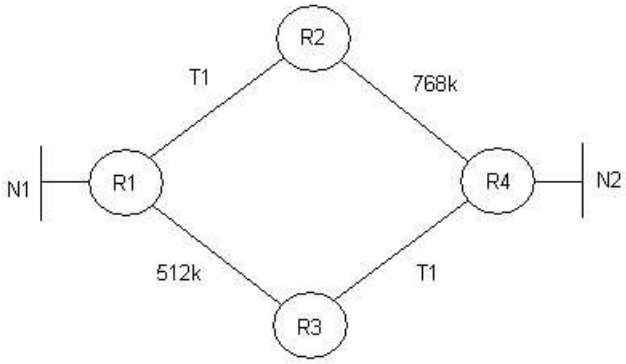
Czas wykrywania awarii

- łącza szeregowe: natychmiast (przerwa w obwodzie)
- Token Ring, FDDI: od razu
- Ethernet: dwa lub trzy cykle zegara "keepalive"
- Protokoły EIGAP Hello lub OSPF Hello

Równoważenie obciążenia



- T1 =1.5 Mb/s; E1 =2Mb/s>
- równe koszty ścieżek



- zbliżone koszty ścieżek

metryki:

- liczba hopów przez które musi przejść informacja do sieci docelowej
- uwzględnienie przepustowości łączy
- koszty łączy (wagi zależne od kosztów eksploatacji)
- stopa błędu bądź niezawodność
- opóźnienie na [każdym] danym łączu (opóźnienie propagacyjne łącza satelitarnego = 0.3s)
- aktualne obciążenie łącza

Routing statyczny vs. Dynamiczny

Routing statyczny	Routing dynamiczny
o Przewidywalny - trasa po której pakiet jest przysyłany jest dobrze znana i może być kontrolowana o Łącza nie są dodatkowo obciążone wiadomościami stużącymi do routowania o Łatwe do skonfigurowania w małych sieciach o Brak skalowalności o Brak obsługi redundantnych połączeń o Nieumiejętność dostosowania do dynamicznych zmian w konfiguracji sieci	o Skalowalność o Zdolność dostosowania się do zmian topologii sieci o Łatwość konfiguracji - nie popełniamy błędów o Większy stopień zawiłości działania sieci. Im lepiej protokół reaguje na zmiany w sieci tym bardziej skomplikowany musi być - trudność w implementacji - różnice pomiędzy sprzętem od różnych producentów o Konieczność okresowej wymiany danych - to z punktu widzenia użytkownika niepotrzebne obciążenie sieci

Klasyfikacja protokołów

- Podział ze względu na obszary zastosowań
  - Protokoły wewnętrzne
  - Protokoły zewnętrzne
  - *<rysunek wykonany na tablicy* AS - system autonomiczny>
- podział ze względu na charakter wymienianych informacji
  - protokoły dystans-wektor (czyli z wektorem odległości)
  - protokoły stanu łącza
- ????????????? - tak prawde mowiac żaden inny podzial mi się nie nasuwa

BO NIE BYŁO INNEGO;) podal tylko te dwa

Protokoły routingu wewnętrznego i zewnętrznego

Wewn.:

- stosowane wewnątrz jednej domeny administracyjnej
- proste, w małym stopniu obciążają routery
- mało skalowalne
- RIP (Routing Information Protocol), OSPF (Open Shortest Path First), EIGRP(Enhanced Interior Gateway Routing Protocol).

Zewn:

- odpowiadają za wymianę informacji pomiędzy obszarami niezależnie administrowanymi sieciami
- dają się skalować, łatwo obsługują duże sieci
- są skomplikowane, ilość dodatkowych informacji przesyłanych siecią może szybko zablokować pracę małej lub średniej sieci
- EGP (External Gate Protocol), BGP (Border Gate Protocol)

Można je używać zamiennie, ale nie jest to "mądre", bo zostały przeznaczone do innego trybu pracy!

Protokoły dystans-wektor

Router regularnie wysyła wszystkim swoim sąsiadom *(i tylko im!)* informacje na temat każdej dostępnej, znanej sobie sieci

- jak daleko do niej jest (**dystans**)
  - czas podróży
  - liczba przeskoków
  - koszt przesyłu
- jak się można do niej dostać (**wektor**)
  - zwykle "wyślij do mnie, bo ja wiem, jak to przesłać dalej".
  - inny router np. gdy router docelowy nie obsługuje danego protokołu routingu. Bardzo rzadko spotykane

<< bardzo ważny rysunek, który wszystko wyjaśnia (może znajdzie się ktoś kto go namaluje>> ŕwyjście: sieć znajduje się w stanie ustalonym

RIP (Routing Information Protocol)

- router wysyła informacje co 30s do wszystkich swoich sąsiadów - pakiety typu broadcast - o znanych sobie sieciach i odległości do nich
- Miarą odległości jest liczba routerów jaką należy przejść, żeby dostać się do danej sieci

Wady RIP - Zliczanie do nieskończoności

<rysuneczek: sieć 1- przerwane łącze - Ruter R1 -kabelek - Ruter R2 - kabelek -Router R3>

- Router R2 wysyła informację o dostępności sieci 1 co 30 sekund.
- Po 180 sekundach R1 wpisze do swojej tablicy nową drogę do sieci 1
- Jeśli zliczymy do 15 hopów - oznacza to sieć niedostępną

Zapobieganie zliczaniu do nieskończoności

- **dzielony horyzont (split horizon)** (uaktualnianie z podzelonym horyzontem)- router nie propaguje informacji o dostępności pewnej sieci na ten interfejs, przez który otrzymał informację o dostępności tej konkretnej sieci (*jakoś tak bo Zieliński w czasie wykładu coś się tłumaczył że asystenci źle sformułowali zdanie) - dobrze jest, w kazdym razie na tym to polega*

- **wstrzymanie (hold down)** - router wstrzymuje się z akceptacją komunikatów o dostępności sieci, o której awarii otrzymał informację (zazwyczaj na 60 sekund)

RIP - split horizont
Zmniejsza prawdopodobieństwo wystąpienia zjawisku zliczania do nieskończoności

RIP - wstrzymanie
- po otrzymaniu komunikatu od routera, że poprzednio dostępna sieć jest niedostępna włącz licznik (holt down timer)
- jeżeli otrzymasz komunikat od tego samego routera, że sieć jest dostępna, wyłącz licznik
- jeśli otrzymasz komunikat od innego routera ogłaszający lepszą trasę wyłącz licznik
- Jeżeli otrzyma gorsze trasy ignoruje je
- Po upływie licznika kasuj wpis

Wykład 7 **26.11.2001**

Routing dynamiczny cz.2

Wady RIP

- **Synchronizacja**. Co w 30 sek w sieci opartej na protokole RIP następuje znaczny spadek wydajności (synchronizacja komunikatów o tablicy routingu)
  - Mniejsza przepustowość lub większy procent zgubionych pakietów

- Rozwiązanie:
  - Inicjowanie routerów w różnych momentach
  - Dodanie małego dodatkowego czasu do interwału pomiędzy wysłaniem każdej informacji o zawartości tablic routingu (losowo)

- **Rozgłaszanie** - w przypadku Ethernet lub FDDI - naturalna metoda przesyłania informacji dotycząca routingu, w ISDN lub X.25 - "milczenie jest złotem"
- **Zbyt prosta metryka** - łącze X.25 i FDDI tyle samo warte
  - X.25 drogie i wolne
  - FDDI tanie i szybkie

Ja miałem to co wyzej MR z tą poprwaka
<a ja mam coś takiego tutaj>
W ISDN lub X.25 "milczenie jest złotem"

- ISDN "B"- 64kbps
- Kanał wirtualny X,25 - 9,6 kbps
  - Paczka z pakietem RIP zajmuje ok. 1 sek
  - Przy.....???????

Wady RIP

- Zbyt prosta metryka
- Łącze X.25 i FDDI "tyle samo warte"

<Rysunek nie wnoszący nic nowego>

RIP-2

- W ramce zawarta jest również maska podsieci
- Ramka może informować o trasach zewnętrznych (właściwość wykorzystywana przez EGP i BGP)
- Propagowany nie tylko adres następnego routera (next-hop), ale również numer domeny routingu

Tak ja mam;)

<Rysunek RIP-2>

- Router D może podać adres E jako "next-hop" w drodze do F.

- Wada RIP-1
  - W RIP-1 każdy komputer nadający z portu 520 jest uznawany za router
  - Konieczna ręczna konfiguracja routingu

- Mechanizm autentykacji RIP-2
    - W ramce RIP-2 można umieści pole zawierające "hasło"
    - Nie powoduje to utraty kompatybilności z RIP-1

- Wada RIP-1
    - Używa broadcastowego adresu MAC do rozsyłania informacji o dostępności sieci.
- RIP 2 używa do tego celu multicastowego adresu IP klasy D (224.0.0.0) a ja mam (224.0.0.9)
    - Nie są konieczne mechanizmy routowania pakietów klasy D, bo informacje dotyczą tylko lokalnej sieci

RIP-2 podsumowanie

§ Oferuje znaczące rozszerzenia względem RIP-1
    - Routing bazujący na przedrostkach podsieci
    - Automatyzacja pakietów ok
    - Kompatybilność z RIP-1
§ Nie eliminuje wad RIP
    - Taka sama metryka i istnienia zjawiska zliczania do nieskończoności

§ BRAKI !!
    - Np. konieczność liczenia do nieskończoności w razie zmian sieci

(tylko tyle bylo)

Interior Gateway Routing Protocol (IGRP)

§ Jeden z najczęściej używanych obecnie protokołów routingu
    - Przedstawiciel rodziny "dystans-wektor"
    - Definicja jest chroniona prawem autorskim Cisco System
§ Periodyczne komunikaty o zawartości tablic routingu (co 90 sekund)
§ Złożone metryki

Metryki elementarne

- Statyczne
    - Opóźnienie (ang. Delay *ozn. D*)
        § Mierzone w dziesiatkachmikrosekund
    - Przepustowość (ang. Bandwidth *ozn.B*)
        § Jednostka 10 000 000/przepustowość w kbos
        § 24 bity -> zakresy przepustowości od 1200 bps do 10 Gbps
        § Maksymalny rozmiar pakietu (ang. Maximum transmision unit, ozn. MTU)
- Dynamiczne
    - Niezawodność łącza (ang. Reliability *ozn. R*)
        § Stopień pewności, że pakiet dotrze do celu
        § 8 bitów:255 odpowiada 100%
    - Obciążenie łącza (ang. Load *ozn.L*)
        § Dotyczy najbardziej obciążonego łącza na ścieżce
    - Liczba routerów na ścieżce (ang. Hops *ozn. H*)

Metryka złożona

- T - opóźnienie transmisji
    - Dla pakietów o długości 10000 bitów T=B+D

    - Dla pakietów o innej długości $T = \frac{P * B}{10000 + D}$
    - Przy uwzględnieniu obciążenia łącza - dostępna tylko część przepustowości

$$T = P * \frac{B\left(\frac{256}{256 - L}\right)}{10000 + D}$$

    - Po uwzględnieniu współczynniku niezawodności $T = P * \frac{B\left(\frac{256}{256 - L}\right)}{10000 + D} * \frac{255}{R}$
- Wada tego podejścia
    - Krótkie okresy pomiaru obciążenia łącza powodują destabilizację ;)) jedno w glowie;))
- Rzeczywista (pełna) metryka

$$M = (K1 * B + K2 + \frac{B}{256 - L} + K3 * D) * \frac{K5}{R + K4}$$

- Współczynniki K1-K5 są ustalone przez administratora
    - Np. ustalenia K5=0 powoduje, że współczynniki niezawodności nie jest brany pod uwagę
    - Ustawienie domyślne (por. z opóźnieniem dla 10000b)
        - K1=K3=1
        - K2=K4=K5=0
- Sposoby zapobiegania pętlom
    - "podzielony horyzont"
    - "wstrzymywanie" (ang. path holdown)
- Routing wielościeżkowy
    - Dzielenie obciązenia między kilka możliwych ścieżek
    - pozytywny "efekt uboczny": zapasowa ścieżka w razie awarii na najlepszym łączu

Metryki IGRP

Stabilność:

- path holdown - przez pewien czas po stwierdzeniu zmiany w topologii (np. wyłączenie routera) nie jest przyjmowana żadna informacja dotycząca ścieżek , które w wyniku tej zmiany stały się nieosiągalne.
- split horyzont - informacja o ścieżce nie jest wysyłana w kierunku skąd nadeszła (dodatkowe zabezpieczenie)
- poisonis reverse - w stronę skąd nadeszła informacja o "dobrej" ścieżce wysyłana jest informacja o braku dostępności

Zegary:

- update timer - jak często rozsyłane są wiadomości (standardowo 90 sekund)
- invalid timer - jaki czas odczekać przed uznaniem ścieżki za nieczynną (nieważną) (3*updtae timer=270 sek)
- hold time - czas przetrzymywania ścieżki w stanie "hold down" (280 sek)
- flash timer - czas jaki ma upłynąć przed usunięciem ścieżki z tablicy routingu (630 sek)

Enhanced IGRP (EIGRP)

⇒ Wady IGRP

- Synchronizacja

- Nieefektywne algorytm zapobiegania pętlom

⇒ Algorytm DUAL (JJ.Garcia - Luma - Aceves) (diffusing update algorythm)
- Usuwanie pętli
- Zastosowanie zarówno w protokołach dystans-wektor, jak i w protokołach stałego łącza

Algorytm DUAL

⇒ Niech d(k,j) -odległość między k i j
l(k,j) - koszt łącza między k i j
- W przypadku protokołów dystans-wektor d(k,j) uzależnione od sąsiadów l(k,j) jest parametrem lokalnym
- Router wybiera następny router na ścieżce (*ozn.x*) tak aby zminimalizować czasy d(i,j)=l(i,x)+d(x,j)
- Przypuścmy, że router otrzymuje uaktualnienie jednej z rozważanych wielkości (np. l(i,k lub d(k,j)))
  - § Jezłi suma l'(i,k)+d'(k,j)<d(i,j) to przyjmuje k jako następny router na ścieżce do j
  - § W przeciwnym przypadku router powiadamia sąsiadów, których koszt dotarcia do j jest mniejszy o zmianie (przekazuje pakiet)
    - Jeśli jest choć jeden takie sąsiedni router przyjmuje d'(i,j)=l(i,k)+d(k,j) i ogłasza zmianę sąsiadom
- Aby móc przeprowadzać obliczenia router musi rozsyłać zapytania do sąsiadów

⇒ Rozszerzenia względem protokolu IGRP
- Komunikat "hello" - poznawanie sąsiadów
  - § Periodyczne wysyłane na adres multicastowy
  - § Odpowiedzią jest pakiet "hello" sąsiada
  - § Zapytania
  - § Odpowiedzi

<u>Protokoły stanu łącza</u>

⇒ Router przechowuje w pamięci "mapę sieci"
- Mapa jest regularnie uaktualniana
- Możliwe centralne wyznaczanie ścieżki do celu

⇒ Możliwość stosowania wielu metryk

⇒ Szybka reakcja na zmiany topologii
- Relatywne (w stosunku do protokołów dystans-wetor) małe pakiety informacyjne

⇒ Brak pętli
- Brak konieczności "liczenia do nieskończoności"

⇒ Wiele metryk

<rys>

D-C-A-B 1,5 Mbps 295 ms opóźnienia
D-E-B 64 kbps 20 ms opóźnienia

⇒ Ścieżka D-C-A-B ma większą przepustowość, ale nie można jednoznacznie stwierdzić, że jest lepsza od D-E-B
- Zagadnienie optymalizacji wielokryterialnej
- Ścieżka D-E-B ma mniejsze opóźnienie

⇒ Problem: router C może mieć inne preferencje niż D, potrzebny znacznik w pakiecie, którą strategię wybrać

<!!!! Rys !!!!!>

Skąd	Dokąd	Łącze	Metryka

A	B	1	1
A	D	3	1
B	A	1	1
B	C	2	1
B	E	4	1
C	B	2	1
C	E	5	1
D	A	3	1
D	E	6	1
E	B	4	1
E	C	5	1
E	D	6	1

OSPF (Open Shortest Path First)

⇒ Baza danych o sieci przechowywane w każdym z routerów

⇒ Każdy z routerów może wyliczyć optymalną ścieżkę do dowolnego miejsca

<rys>Awaria łącza 1 <- to na rys

- Routery A i B są odpowiedzialne za rozgłoszenie informacji i awarii łącza 1
- Pozostałe routery powtarzają wiadomość, o ile jej treść nie była dotychczas znana (czepiam się:))
- Wiadomość zawiera czas nadania
- Ten sposób przekazywania wiadomości o zmianie topologii sieci nazywa się **zalewaniem** (ang, flooding)
- Możliwość dzielenia obciążenia między różne ścieżki
    - Ścieżki o zbliżonych metrykach mogą równocześnie służyć do przesyłania pakietów
        - § Pakiety nie zawsze dojdą w kolejności wysłania
        - § Szybszy transfer informacji
    - Problem: wyznaczenie jakie części ruchu powinny być kierowane poszczególnymi ścieżkami
        - § Rozwiązanie zagadnienia wymaga analizy grafu (problem maksymalnego przepływu)

- Ścieżki zewnętrze
    - Jeżeli w danym systemie autonomicznym jest tylko jedno "wyjście na świat", to zagadnienie wyboru ścieżki jest trywialne zarówno dla protokołów dystans-wektor jak i stanu-łącza.
    - W przeciwnym wypadku najczęściej wybierane jest najbliższe (w sensie przyjętej metryki) łącze zewnętrzne
    - OSPF: w opisie topologii sieci jest umieszczony rekord stanu łącza zewnętrznego (ang. gateway with state record)

- Podstawowy problem: zapewnienie koherencji routingu
    - Warunek konieczny: identyczność wpisów topologii sieci w każdym routerze
    - Przykładu zagrożeń
        - § Zagubiony pakiet informacji o sieci
        - § Błędy pamięci
        - § Rozmyślne działanie człowieka

Open Shortest Path First

- Wybrane cechy OSPF
  - Zalewanie z potwierdzeniem
  - Zabezpieczenie pakietów z opisem sieci
  - Każdy rekord opisem łącza jest przechowywany tylko przez określony czas
    - § Jeśli do tego czasu nie zostanie odebrany komunikat odświeżający, to rekord jest usuwany
  - Wszystkie rekordy zabezpieczone sumą kontrolną
  - Komunikaty mogą być autoryzowane (np. przez podanie hasła)
- Założenia projektantów (IETF)
  - Separacja routerów od innych komputerów
  - Obsługa sieci rozgłoszeniowych (Ethernet, FDDI)
  - Obsługa sieci bez rozgłoszeń (X25,ATM)
  - Podział wielkich sieci na mniejsze
- Separacja routerów i innych komputerów
  - Łącze z sąsiednimi routerami identyfikowane przez adres tego routera, inne komputery adresowane przez numer sieci.
- Obsługa sieci rozgłoszeniowych
  - Wybór jednego routera do pełnienia roli reprezentanta zmniejsza liczbę rozgłoszonych ścieżek oraz liczbę wpisów w bazie topologii sieci

<rys - nie mam> <mam ale nic nie znaczacy>

  - Pakiet LSA (linka state advertisement) rozsyłane są na adres multicastowy 224.0.0.6 przeznaczony dla wybranych routerów (all-designated routers)
  - jeżeli pakiet zawiera nowe informacje. Wybrany router rozsyła je do innych do innych tego typu urządzeń dołączonych do tej samej sieci (wybierając adres 224.0.0.5)
- Obsługa sieci bez rozgłoszeń X.25, ATM
  - W przypadku łącz stosunkowo drogich za redukcje wykorzystywania łącz przemawiają nie tylko względy efektywności ale również możliwości firm, ?????, ale również względy finansowe
  - Różnica polega na niewykorzystywaniu adresów rozgłoszeniowych,w zamian wiele połączeń punkt-punkt
- Podział wielkich sieci na mniejsze
  - Liczba połączeń może rosnąc nawet z kwadratem liczby ???
  - Czas obliczeń ścieżki jest jednym z newralgicznych wskaźników dla dla efektywnej sieci
  - Wielkość pamięci routera jest ograniczona
- Kryteria wyboru ścieżki:
  - OSPF pozwala wybrać ścieżkę według określonego kryterium, bądź zbiór kryteriów spośród następujących:
    - § Minimalizacją kosztu
    - § Stopień pewności dotarcia pakietu do celu
    - § Max przepustowoś ścieżki (ß ??????????????????????) OK
    - § Min. opóźnienie

OSPF - algorytm Dijkstry

- Oznaczenia
  - E - zbiór węzłów, dla których najkrótsza ścieżka jest znana
  - R - zbiór pozostałych węzłów
  - O - uporządkowana lista ścieżek
- Algorytm

9. Niech E zawiera tylko węzeł początkowy, S zaś R wszystkie pozostałe

10. Niech O zawiera wszystkie jednosegmentowe ścieżki rozpoczynające się w S uporządkowane według metryki łącza
11. Jeżeli O jest zbiorem pustym lub metryką pierwszej ścieżki w O ma wartość nieskończoną to wszystkie węzły w R są nieosiągalne. STOP
12. Dla ścieżki P - najkrótszej w O
    - Usuń P z O
    - Niech V będzie końcem ścieżki P
        - Jeżeli U należy do E skocz do (3)
        - W przeciwnym wypadku P jest najkrótszą ścieżka do U

przenieś U z R do E

13. Zbuduj zbiór nowych ścieżek przez połączenie P ze ścieżkami wychodzącymi z V. Dodaj utworzone ścieżki do zbioru O. Kontynuuj od kroku (3). Koszt ścieżki: suma kosztów licząc od S.

OSPF

Protokoły zwwn. OSPF

- Hello Protocol
  - Sprawdzenie, czy łącze funkcjonuje
  - Wybór reprezentanta spośród routerów przyłączonych do jednej sieci (priorytet, identyfikator)
- Exchange Protocol
  - Synchronizajca zawartości bez danych opisujących topologię sieci
  - Asymetryczny (master-slave)
- Flooding protocol
  - Powiadamianie o zmianach w topologii sieci

EGP (Exterior Gateways' Protocol)

Internet podzielony jest nasystemy autonomiczne (AS)

- niemożliwe jest przechowywanie tablic routingu dotyczących wszystkich sieci na świecie
- systemy autonomiczne muszą się ze sobą komunikować
- każdy system autonomiczny jest identyfikowany przez 16-bitowy numer

Trzy podstawowe procedury EGP:

- pozyskanie sąsiadów
  - bycie sąsiadem oznacza przyjęcie ruchu z sąsiedniego AS
  - może to wymagać formalnej umowy
  - wymaga konfiguracji (rozszerzenie listy potencjalnych śasiadów)
- monitorowanie dostępności sąsiadów
  - wymiana pakietów "hello" i "I-hear-you" (najczęściej co 30s)
  - po kilku brakach odpowiedzi sąsiad uznawany jest za niedostępnego

EGP

- **pozyskiwanie informacji o dostępie (sieci | sasiadów) ß** **które jest poprawne?**
  - Każdy z ?????????????????????????????? odpytuje drugiego
  - ***<rysunek>***
  - wewnątrz sys. autonomicznego dowolny IGP: np. RIP,OSPF,IGRP
  - Metryka jest słabo zdefiniowana
    - § Wartość 255 odpowada nieskończoności, inne - nie wiadomo
  - Router brzegbowy nie zawsze anaosuje wszystkie sieci dostępne przez niego (w celu zapobieżenia pętlom)
  - EGP nie jest odporny na fałszywe informacje z zewnątrz
  - Przeznaczony jest dla sieci o topologii "drzewo"
  - Z ww. powodów EGP na znaczenie raczej historyczne

Border Gatway Protocol (BGP)

- ??
  - "środek przeciwko pętlom"
  - Każdy kompunikat o zmianie trasy do sieci niesie ze sobą ??????????????????????????????, przez które potencjalny ruch powinien przejść
  - Sprawdzanie, czy nie ma pętli jest proste, ruter brzegowy musi tylko sprawdzić, czy numer jego AS nie występuje na ścieżce
- BGP oferuje także zbiór atrybutów ścieżek
  - Odpowiadają one ?????????????????????? wyboru
- Informacje BGP nie mogą być przekazywane przez IGP

- *<rysunek>*
- BGP jest zbudowany nad protokołem TCP
- Funkcje kontroli błędów na poziomie TCP
- Typy pakeitów:
  - OPEN
  - UPDATE
  - NOTIFICATION
  - KEEPALIVE

CIDR (Classless Inter-Domain Routing)

- Ramka UPDATE protokołu BGP-4 (budowa ramki):
  - Unfeasible rutes length (2 oktety)
  - Unfeasible routes (zm.)
  - Total patch attribute length (2 oktety)
  - Path attributes (zm)
  - Network reachability information (zm)
- Adresy sieci przez CIDR mogą się "nakładać"
  - Np. 197.8.0.0/22 i 197.8.3.0/24

Literatura:

- ??

Reaview: IP Addresing

Claslec Versus Classful Routing Protocol

- Classless routing protocol advertise ??????????????????? and match the longest path
- Subnets must be contiguous with classful routing protocol
- <rysunek>
- Classless Notation
  - 131.108.0.0/16 versus 255.255.0.0
  - Summarizable blocks of subnets
  - <rysunek>: adresy od: 131.108.48.0/24 do 131.108.55.0/24 można zapisać krócej, jako: 131.108.48.0/21 (najdłuższy wspólny prefiks sieci)
  - Routing summarization:
  - <rysunek>
  - Routing protocols can summarize addresses of several networks into one address

Comparison of Routing Protocol

	Line State	Traditional Distance-Vector (czyt. RIP)	Advance Distance-Vector (czyt. IGRP)
Scalability	Good	Low	Excellent
Bandwidth	Low	High	Low
Memory	High	Low	Moderete
CPU	High	Low	Low
Convergence	Fast	Slow	Fast
Configuration	Moderate	Fast	ease

IRP

<tabelka *może ktoś ma źrodło tej tabelki???***>**

Name	
RIP	
RIP2	

IGRP	
EIGRP	
OSPF	
IS-IS	
BGP	

www.cisco.com/public/technotes/tech_protocol.shtml
www.cisco.com/univercd/cc/td/doc/ciscinterk/cdgs/idgip.htm (ß może ktoś sprawdzić linki?)

Warstwa transportowa (TCP i UDP)

Warstwa transportowa:
- zapewnienie niezawodnego przesyłu danych (wg. ISO)
- tworzenie połączenia
  - nawiązanie połączenia
  - uzgodnienie parametrów połączenia
  - wysyłanie danych wysokopriorytetowych
- Transmisja bezpołączeniowa
- Wniosek: warstwa transportowa ?????????????????????????????? QoS (Quality of servece)
- Enkapsulacja
  - <rysunek>

Transmission Control Protocol
- połączenie
  - nawiązanie połączenia
  - zamknięcie połączenia
  - dokładnie dwa końce połączenia
  - połączenie obustronne (full-duplex)
- niezawodny
  - porwierdzenie odbioru
  - kontrola przepływu danych - wyrównanie szybkości nadawania informacji z szybkościa odbioru informacji
  - suma kontrolna dla nagłówka i danych
  - porządkowanie kolejności segmentów
  - usuwanie segmentów zduplikowanych

Nagłówek TCP

<table>
<tr><td colspan="2">Numer portu źródła (16)</td><td colspan="2">Numer portu przeznaczenia (16)</td></tr>
<tr><td colspan="4">Numer sekwencyjny (32)</td></tr>
<tr><td colspan="4">Numer potwierdzenia (32)</td></tr>
<tr><td>Długośc (4)</td><td>Zarezerwowane (6)</td><td>Flagi (6)</td><td>Rozmiar okna (16)</td></tr>
<tr><td colspan="2">Suma kontrolna (16)</td><td colspan="2">Wskaźnik ważności (16)</td></tr>
<tr><td colspan="4">opcje</td></tr>
</table>

- TCP operuje pojęciem portu - połączenie proces-proces (end to end process)
- Numer sekwencyjny - numer pierwszego bajtu w wiadomości, który wysyłany w wiadomości do odbiorcy
- Numer potwierdzenia - numer ostatniego bajtu, który został potwierdzony
- Długość - długość nagłówka IP

- Rozmiar okna - okno= max długość bloku danych, które mogą być wysłane w ramach połączenia TCP bez potwierdzenia

Asocjacje

- Asocjacja jest to piątka:
  - (protokół, adres lokalny, proces lokalny, adres obcy, proces obcy)
- Półasocjacja, inaczejj gniazdo (socket) to trójka:
  - (protokół, adres lokalny, proces lokalny)
  - lub: (protokół, adres obcy, proces obcy)
- W przypadku protokołów TCP i UDP procesy identyfikowane są przez numery portów określone w nagłówku *(numery portów w TCP i UDP nie odpowiadają sobie)*

Porty

- Zestaw dobrze znanych portów określają porty, z którymi mogą łączyć się klienci, np.:
  - 21 - FTP
  - 23 - Telnet
  - 25 - Mail
  - 53 - DNS
  - do 1024 są to porty usług
- Porty efemeryczne - krótkotrwałe, określone przez moduł warstwy transportowej (tworzone??) na czas połączenia

Flagi TCP

Flaga	Opis
SYN	Synchronizacja numerów sekwencyjnych (ang. inital sequence Number (ISN)
ACK	Pole potwierdzenia zawiera aktualny numer potwierdzenia
FIN	Zakończenie przesyłania danych
RST	Zresetowanie połączenia
URG	Dane pilne począwszy od wskaźnika ważności
PSH	Przekierowanie danych do aplikacji najszybkicej jak to możliwe

Suma kontrolna

- Obliczanie sumy kontrolnej dla nagłówka danych oraz pseudonagłówka
- Pseudonagłówek:

Adres źródłowy (32)		
Adres przeznaczenia (32)		
0 (8)	Protokół = 6 (8)	Długość segmentu TCP (16)

Opcje

- maksymalny rozmiar segmentu (ang. Maximum Segment Size MSS)
  - im większe segmenty tym wydajniejsze przysyłanie danych
  - należy unikać fragmentacji pakietów IP
  - dane segmentu mogą niekorzystny wpływ np. na transmisję danych w czasie rzeczywistym
- Skalowanie okna
  - Znacznik czasowy - określone RTT (Round Trip Time)

Przykład połączenia

14. klient łączy się z serwerem otwierając połączenie poleceniem connect
    <rysunek>
15. serwer otrzymuje zgłoszenie od klienta

- moduł TCP tworzy unikatową asocjację:
  (tcp, 123.45.67.89, 23, 12.34.45.78, 1234)
  <rysunek>

Schemat stanów TCP
<duży rysunek>

Zegary TCP

Retransmision Timer - zegar odmierzający Timeout

Persistence Timer - zapobiega zakleszczeniu w sytuacji zgubienia pakietu zwiększającego okno

Keapalive Timer - pozwala na sprawdzenie aktywności drugiej strony połączenia

Retransmission Timer

RTT = a * RTT + (1 - a) * M

M -czas otrzymania potwierdzenia

a = 7/8

Sposób 1.

Timeout = b * RTT, gdzie b=2

Sposób 2. (alg. Jacobsona)

D = a * D + (1 - a) * (RTT - M)

Timeout = RTT + 4*D

<wykres: prawdopodobieństwo X RoundTripTime>

Dynamika estymacji RTT jest przeprowadzana wg. Alg. Karea ß ??????????????????????????

W sytuacji braku potwierdzenia nie jest zmieniane RTT, lecz zwiększa się Timeout 2 razy.

Ponowne wysłanie może spowodować niejednoznaczność, które ACK odpowiada ostatniemu wysłaniu.

Dlatego nie zmienia się RTT dla retransmitowanech zegarów *(ç zegarów czy cos innego?, bo to głupio brzmi)*

Persistence Timer

<rysunek pokazujący pakiety wędrujące pomiędzy nadawcą i odbiorcą, w czasie komunikacji coś idzie nie tak, ale nie wiem co>

Zastosowania:

- Przesyłanie danych wrażliwych na gubienie pakietów
  - Dane interaktywne: Telnet, SSH, mysz w X-Windows, ...
  - ??
  - dane masowe: FTP, Mail, News, itp.
- Nie pozwala na transmisję grupową (ang. Multicasting) - dokładnie dwa końce połączenia

User Datagram Protocol

Bardzo prosty protokół warstwy transportowej

- szybki
- zawodny
- bezpołączeniowy

Nagłówek UDP

- nagłówek ma rozmiar 8 bajtów
- suma kontrolna (nieobowiązkowa) wyliczana jest podobnie jak dla TCP wraz z pseudonagłówkiem

Numer portu źródła (16)	Numer portu przeznaczenia (16)
??????????????????????????????????(16)	Suma kontrolna (16)

Zastosowania

- Transmisja grupowa
- Transmisje w czasie rzeczywistym
- Przesyłanie danych nie wrażliwych na gubienie pakietów
- Przesyłanie w sieci LAN
  - NFS (Network File System), DNS

Literatura

- Stevens "Biblia TCP"
- Stevens "Programowanie zastosowań sieciowych w systemie UNIX"
- Comer "TCP/IP" t.2
- www.iana.org/assignmets/port_numbers *(ß jaj brzmi poprawnie ten adres?)*lub RFC 1700
- RFC 2001, 2018,2581,3042

Model uproszczony TCP

Warstwa aplikacji
ÝAPIÝAPIÝAPIÝAPIÝ
Warstwa transportowa
Warstwa sieci
Warstwa łącza

API - w ISO/OSI jest to transmision layer interface
Najpopularniejsze: (gniazda) socket interface (od BSD 4.0)

Interfejs programisty

- Interfejsy niskiego poziomu:
  - gniazda BSD (UNIX, Linux)
  - Transport Layer Interface -TLI (UNIX, Linux)
  - Winsock (Microsoft)
- Interfejsy wysokiego poziomu
  - Java.net (SUN)
  - Biblioteka MFC (Microsoft)

Gniazda BSD

Socket	tworzy gniazdo serw/kli
Bind	Wiąże adres i proces z docelowym zewn (/kli)
Listen	Tworzy kolejkę zgloszeń, serw
Accept	Oczekiwanie na zgłoszenie, serw
Connect	Ustanowienie połączenia , klie
Send[to]	Wysłanie danych serw/kli
Recv[from]	Pobranie danych, serw/kli

int socet(int family, int type, int protocol)

- zwraca: deskryptor gniazda sockfd
- argumenty:
  - family:
    - AF_UNIX - protokoły wewn. unixa
    - AF_INET - protokoły internetu
    - AF_NS - protokoły Xeroxa NS
    - AF_IMPLINK - warstwakanałowa IMP
  - Type: - rodzaje gniazda

        - § SOCK_STREAM - gniazdo strumieniowe
        - § SOCK_DGRAM - gniazdo datagramowe
        - § SOCK_RAW - gniazdo surowe
        - § SOCK_SEQPACKET - gniazdo surowe
    - o Protocol
        - § IPPROTO_UDP
        - § IPPROTO_TCP
        - § IPPROTO_ICMP
        - § IPPROTO_RAW

int bind (int socketfd, struct sockaddr * myaddr, int addrlen)
- o zwraca: zero albo kod błędu
- o argumenty:
    - o myaddr - ??????????????????
    - o addrlen - rozmiar struktury adresowej

int listen(int sockfd, int backlog)
- o argumenty:
    - o kacklog - rozmiar kolejki żądań połączenia - maks: 5

int accept (int sockfd, struct sockaddr * par(????????????) int * addrlen)
- o zwraca: deskryptor gniazda klienta
- o arg:
    - o par(????????) - adres klienta, którego żądanie zostało przyjęte

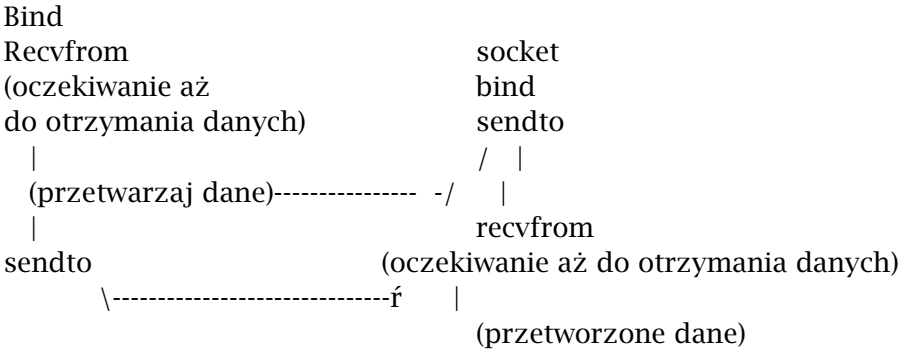
int connect (int sockfd, struct socketaddr * serwaddr,int addrlen)

int recvfrom(int sockfd, char * buf, int nbytes, int flags, struct sockaddr * from, int * addrlen)

Asynchroniczna obsługa gniazd
Select - oczekiwanie na liście gniazd (??????????????????????)
Signal - sygnał po przyjęciu wiadomości
Fork - utworzenie procesu potomnego

U?????????????? F??????? Interfejsu gniazd
Serwer połączeniowy klient
Socket
Bind
Listen
Accept
B??????????oczekiwanie na zgłoszenie
| socket
| ß---------- connect
| send
recv ß----------/ |
| \/
send----------ŕrecv
itd.

Teraz to samo, ale przesyłanie datagramowe
Serwer bezpołączeniowy (???) klient
Socket



dodatek z CISCO ACADEMY
Switching fabric
Quering - buffer mechanisms used to control congestion????

Distributed switching - implementation in which switching decisions are made at the local port or line module

Oversubscription - conecton *(albo congestion)* in which the total bendwidth of the ports is greater then the capacity of the switdhing fabric. Also refered to as a blocking architecture

Non-blocking - connecton *(albo congestion)* in which the fabric contrains more bandwidth than the sum total of all the ports

Had-of-line blocking - where congesion on are outboound put limits throughput to uncongested ports. Completely differt from over-aubsciption

Switching - process of transfering data from on input interface to an output interface (przełączanie w warstwie 3 jest znacznie szybsze niż w warstwie 2)

??????????????????????????????????????

Compunents of Multilayer switch Architecture

- congestion manegement
- switching decision
- switching fabric

Congestion management
Received clear (?????) multiple ports are cont???????? for the same port ??.?????
Imported if switch fabric is congested

Dynamic Buffer Quering
??
Fixed Buffer Quering
??/
Input Quering
??
Output Quering
??
Output Querring / Shared Buffer
??