

SIECI KOMPUTEROWE

wykład dla kierunku informatyka

semestr 4 i 5

dr inż. Michał Sajkowski

Instytut Informatyki PP

pok. 227G PON PAN, Wieniawskiego 17/19

Michal.Sajkowski@cs.put.poznan.pl

tel. +48 (61) 8 582 100

<http://www.man.poznan.pl/~michal/>

sieci komputerowe

wykład 8

protokół PPP

literatura uzupełniająca

wykład prawie w całości przygotowany na podstawie
tekstu i rysunków z książek:

R.W. McCarty, Jr. (red.), „Cisco WAN od podstaw”,
Mikom, Warszawa 2001

V. Amato, „Akademia sieci Cisco. Drugi rok nauki”,
Mikom, Warszawa 2001

„Vademecum teleinformatyka”, IDG Poland, Warszawa
1999

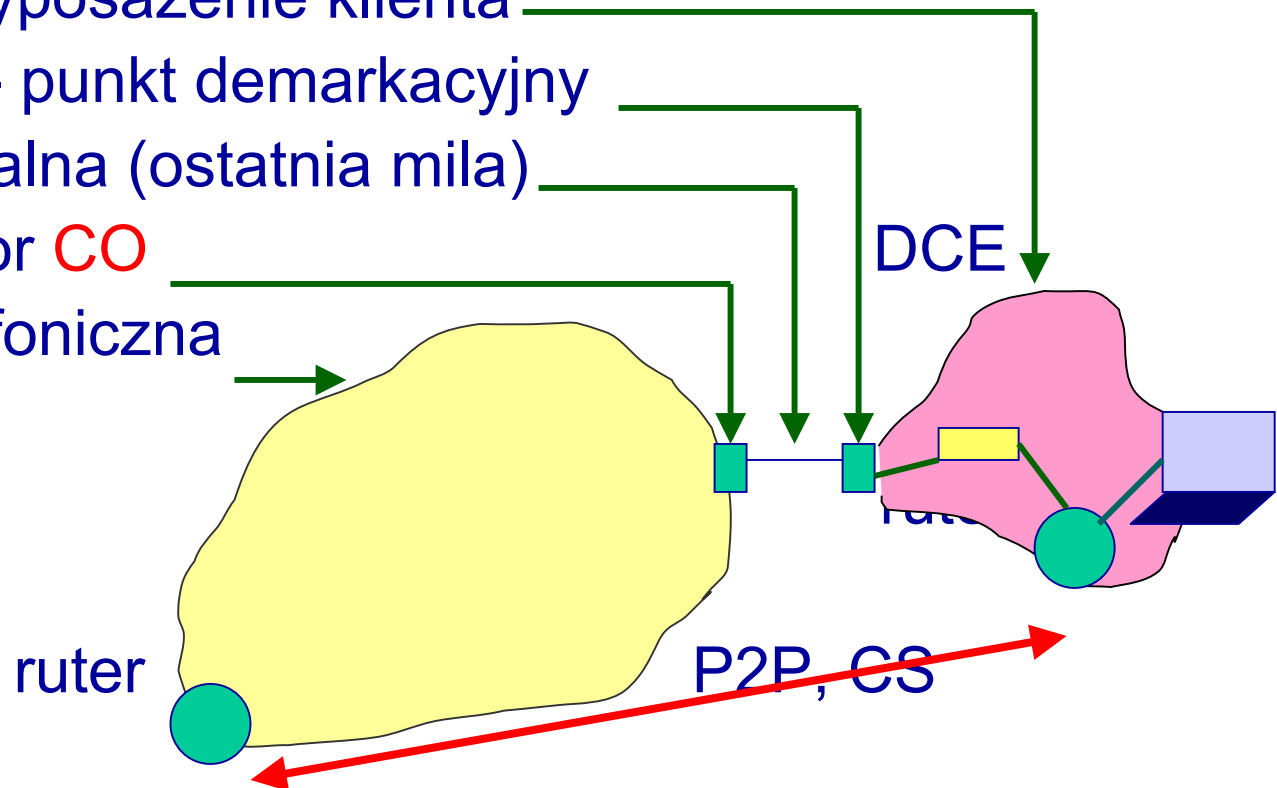
zakres wykładu

- miejsce protokołu PPP w sieciach rozległych
- krótka charakterystyka protokołu PPP

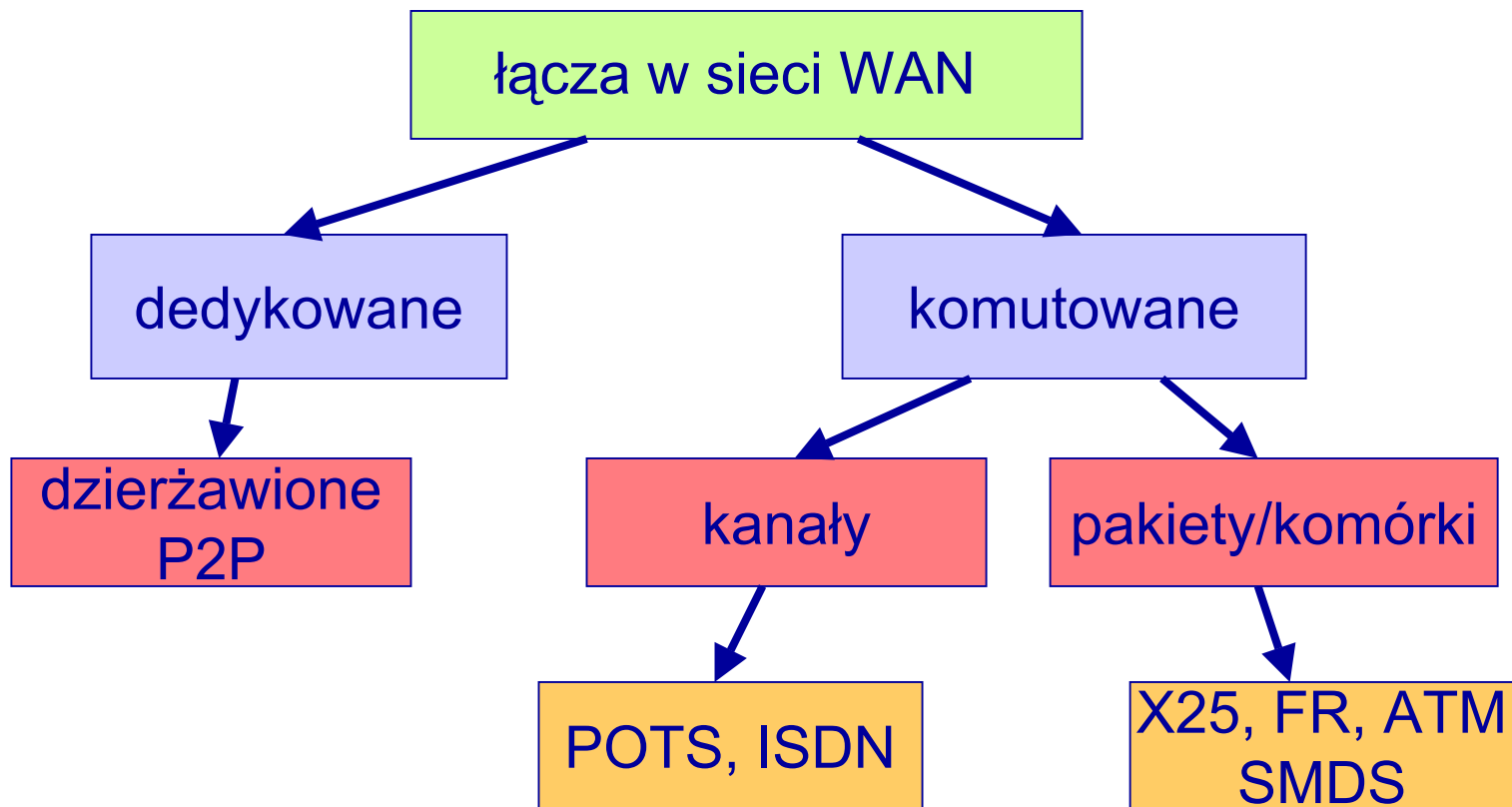
dostawa usług WAN

składniki usług sieci WAN:

- CPE - wyposażenie klienta
- demarc - punkt demarkacyjny
- pętla lokalna (ostatnia mila)
- komutator CO
- sieć telefoniczna

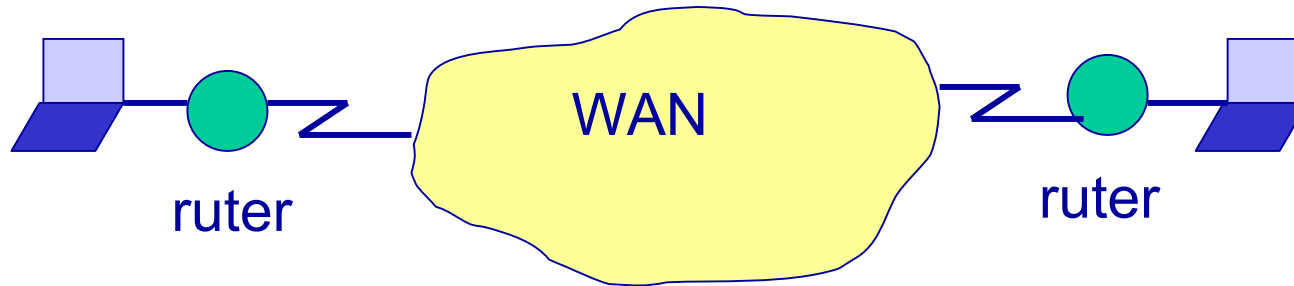


miejsce protokołu PPP w sieciach WAN



łącza dwupunktowe P2P

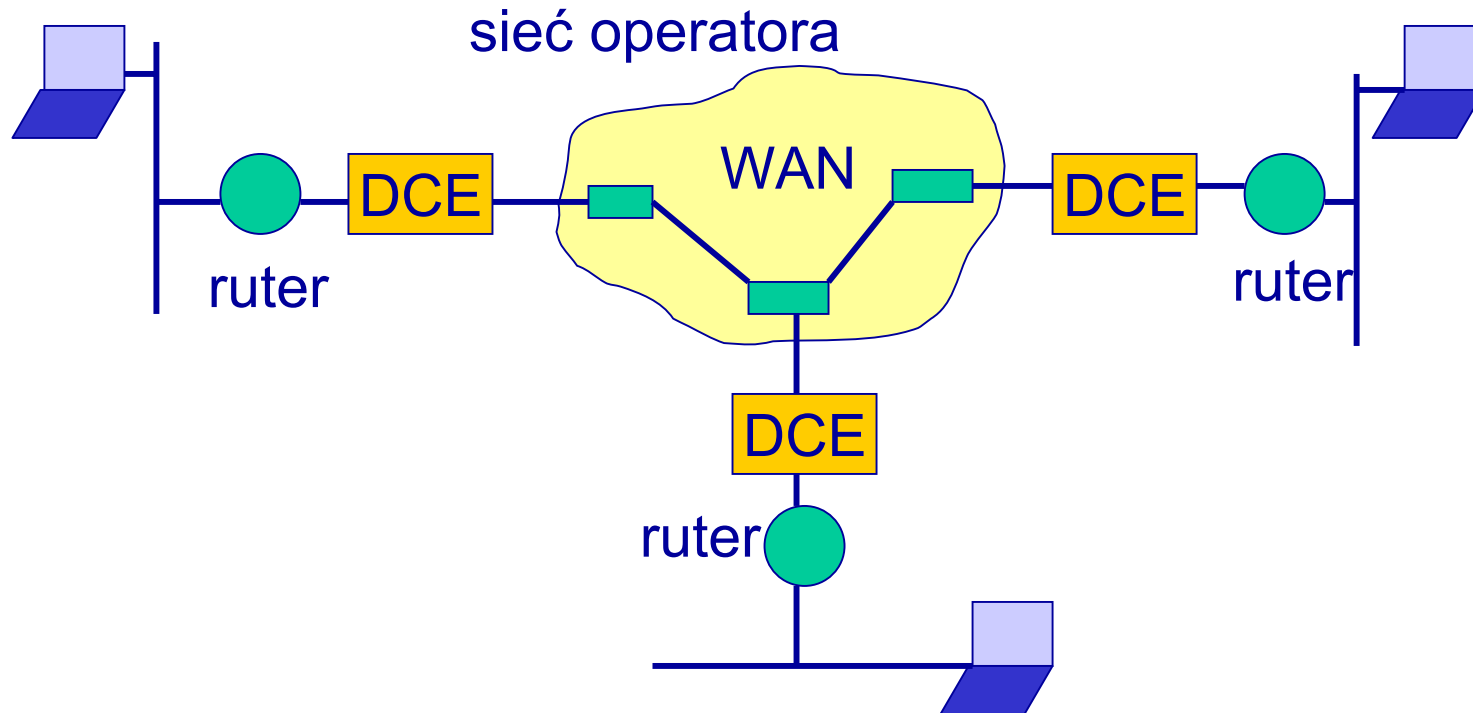
- ścieżka komunikacyjna od CPE przez sieć operatora do sieci zdalnej
- **łącza dzierżawione** od operatora



- opłata za szerokość pasma i odległość
- droższe od FR

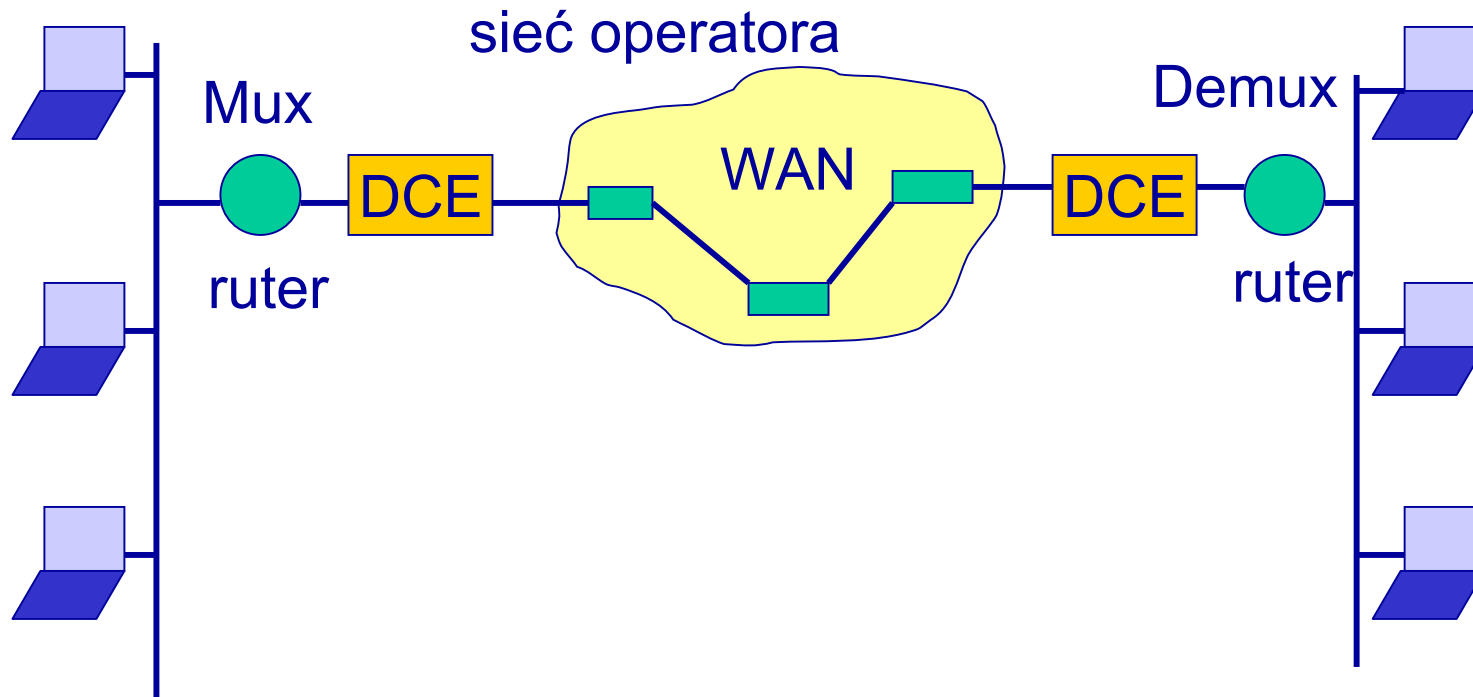
kanały komutowane

- połączenie ustanowione na czas „rozmowy”
- przykład **ISDN**



pakiety komutowane

- kanały wirtualne: komutowane SVC i stałe PVC
- przykład **X25, FR, ATM, SMDS**



kapsułkowanie w sieciach WAN

- warstwa łączy danych sieci WAN określa, w jaki sposób dane są kapsułkowane w celu przesłania ich do strony zdalnej
- najpopularniejsze typy kapsułkowania w łączach WAN:
- dwupunktowe: HDLC, PPP, LAPB
 - HDLC – domyślny dla łączy szeregowych (Cisco)
 - PPP – standard dla łączy szeregowych
- komutowane pakiety: FR IETF, X25 LAPB
- komutowane kanały: LAPD (ISDN)

krótka charakterystyka protokołu PPP

- **Point-to-Point Protocol** - protokół kapsułkowania, dla przesyłania ruchu IP na łączach dwupunktowych, szeregowych, dzierżawionych albo komutowanych
- jako metodę kapsułkowania datagramów na łączach szeregowych, PPP wykorzystuje protokół **HDLC**
- dla ustalania, konfigurowania i testowania łącza danych, stosuje protokół **LCP**
- dla wyboru i konfigurowania różnych protokołów sieciowych, wykorzystuje protokół **NCP (Network Control Protocol)**

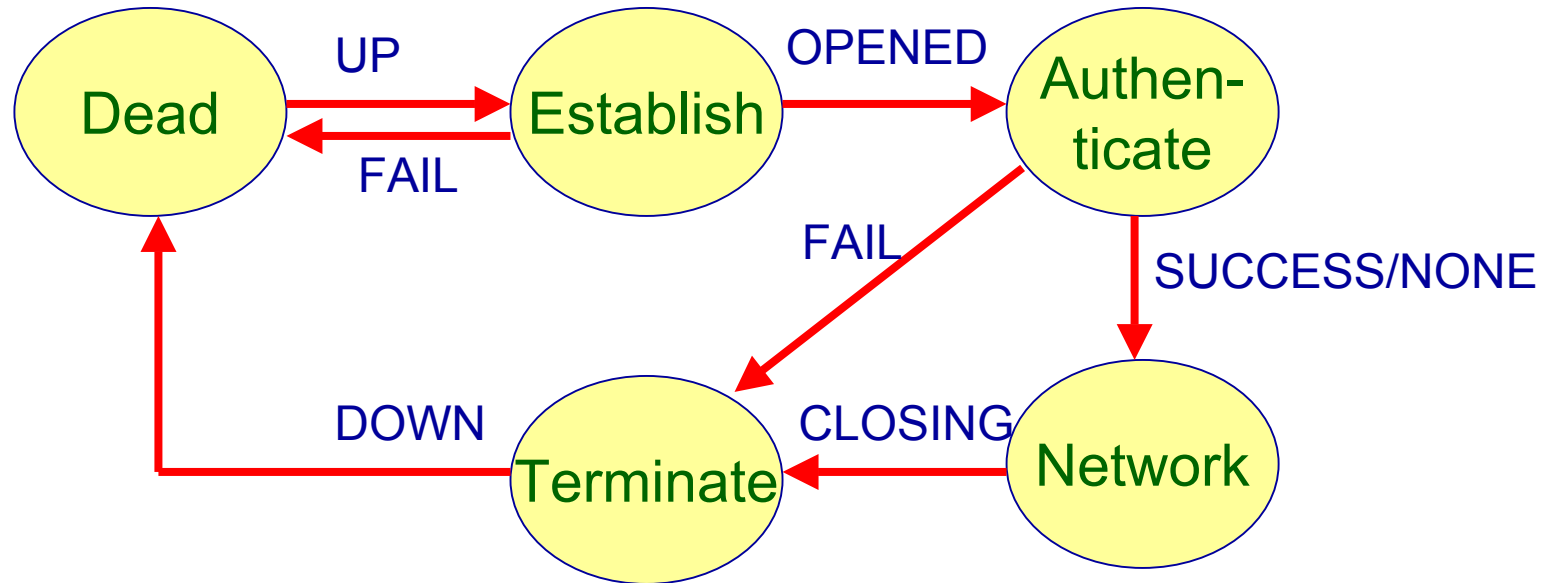
krótka charakterystyka protokołu PPP

- obsługa połączeń dwupunktowych przez linie szeregowo: protokół **SLIP** tylko datagramy **IP** (maks. 1006 bajtów) kapsułkowane w ramach przez łącza synchroniczne albo asynchroniczne, protokół **PPP**: **IP**, **Decnet**, **IPX**, **AppleTalk**, **OSI CNLP**
- **protokół PPP**:
- warstwa fizyczna: **RS232C**, **RS422**, **RS423**
- warstwa łącza danych: **HDLC + LCP**
- **LCP** (**Link Control Protocol**): konfigurowanie łącza, utrzymanie łącza, negocjacja współpracy z warstwą sieci, zakończenie połączenia

działanie protokołu PPP

- aby ustalić połączenie na łączy dwupunktowym:
- wywołująca stacja **PPP** nadaje ramki **LCP**, aby skonfigurować i przetestować łączy danych
- wywołująca stacja **PPP** nadaje ramki **NCP**, aby wybrać i skonfigurować jeden lub więcej protokołów sieciowych (**IP**, **IPX**, **Decnet**, **AppleTalk**, **OSI CNLP**)
- pakiety z każdego protokołu sieciowego są przesyłane przez łączy
- ramka **LCP**, albo ramka **NCP**, albo przekroczenie czasu nieaktywności, rozłącza łączy danych

diagram stanów (faz) łącza PPP



łącze PPP w stanie bezczynności

- warstwa fizyczna nie jest gotowa
- łącze zaczyna się i kończy w tym stanie
- kiedy zdarzenie zewnętrzne (wykrycie nośnej, konfiguracja przez administratora sieci) wskazuje, że warstwa fizyczna jest gotowa, to **PPP** przechodzi do fazy nawiązywania połączenia
- przejście do tej fazy sygnalizuje zdarzenie **UP** w diagramie przejść stanów

faza nawiązywania połączenia w PPP

- protokół **LCP** stosuje się do nawiązania połączenia, za pomocą wymiany pakietów Configure
- wymiana jest zakończona, a protokół **LCP** wchodzi w stan **Opened**, kiedy zostaje nadany i odebrany pakiet **Configure-Ack**
- zakłada się, że opcje konfiguracji przyjmują wartości domyślne do czasu ich zmiany przez wymianę pakietów konfiguracji
- opcje konfiguracji niezależne od danego protokołu w warstwie sieci są konfigurowane przez **LCP**, a opcje zależne są konfigurowane przez **NCP**
- odbiór **LCP Conf-Req** powoduje powrót do fazy nawiązania połączenia (z fazy **NCP** albo uwierzyteln.)

faza uwierzytelnienia w PPP

- oczekuje się, że strona zdalna (*peer*) się uwierzytelni, zanim pozwoli się na wymianę pakietów w warstwie sieci
- domyślnie, uwierzytelnienie nie jest obowiązkowe
- uwierzytelnienie powinno nastąpić jak najprędzej po nawiązaniu połączenia
- ocena jakości połączenia może występować współbieżnie z uwierzytelnieniem, ale nie powinna opóźniać uwierzytelnienia
- przejście z fazy uwierzytelnienia do fazy **NCP** może nastąpić dopiero po zakończeniu uwierzytelnienia
- gdy uwierzytelnienie zawiedzie, przejście do fazy rozłączenia połączenia

faza NCP w PPP

- każdy protokół sieciowy (IP, IPX, AppleTalk) musi być oddzielnie konfigurowany przez oddzielny protokół NCP
- każdy NCP może być otwarty i zamknięty w dowolnym czasie
- kiedy NCP wchodzi w stan Opened, PPP przesyła pakiety właściwego protokołu warstwy sieciowej
- kiedy NCP nie jest w stanie Opened, dowolne pakiety właściwego protokołu warstwy sieciowej są po cichu usuwane

faza rozłączenia połączenia w PPP

- **PPP** może rozłączyć połączenie w dowolnym czasie
- **przyczyny rozłączenia**: strata nośnej, błąd uwierzytelnienia, błąd jakości połączenia, upływ czasu bezczynności, administracyjne rozłączenie połączenia
- **LCP** zamyka połączenie wymieniając pakiety **Terminate**
- **PPP** przechodzi do fazy bezczynnego łącza

wymagania dla warstwy fizycznej

- **PPP** działa na dowolnym interfejsie DTE/DCE, n.p. EIA/TIA-232-C (RS232C, V.24), EIA/TIA-422, ITU-T V.35)
- warstwa fizyczna zapewnia łączy dwukierunkowe, dedykowane albo komutowane, pracujące w trybie asynchronicznym albo synchronicznym, przejrzyste dla ramek **PPP** warstwy łącza danych
- **PPP** nie nakłada wymagań na szybkość transmisji innych niż te, które nakłada aktualnie wykorzystywany interfejs DTE/DCE

warstwa łączy danych w PPP

- stosuje HDLC

flaga	adres	sterowanie	protokół	dane	...	FCS
-------	-------	------------	----------	------	-----	-----

- flaga - 01111110
- adres - 11111111 - standardowy adres rozgłaszania, PPP nie przydziela adresów poszczególnych stacji
- sterowanie - 00000001 - żąda przesłania danych użytkownika w ramce (nie w kolejności) - bezpołączeniowa usługa podobna do LLC typ 1

warstwa łączy danych w PPP

- **protokół** - dwa bajty identyfikujące protokół kapsułkowany w polu informacyjnym ramki
- **dane** - datagram protokołu (tego identyfikowanego wcześniej, np. IP), domyślnie długość **maks. 1500B**
- **FCS** - *frame check sequence* - domyślnie 2 bajty, maksymalnie 4 bajty uzgodnione przez implementacje **PPP**

protokół LCP w PPP

- **LCP** - link-control protocol - protokół sterowania łączem w **PPP**
- zadania **LCP**: nawiązanie, konfiguracja, utrzymanie i rozłączenie połączenia dwupunktowego
- **faza 1**: nawiązanie połączenia i negocjacja konfiguracji - faza jest zakończona po nadaniu i odebraniu ramki potwierdzenia konfiguracji
- **faza 2**:(opcjonalna) ocena jakości łącza, **LCP** opóźnia transmisję datagramów do chwili zakończenia tej fazy, uwierzytelnienie drugiej strony
- **faza 3**: przejście do konfiguracji protokołu NCP ►
- **faza 4**: rozłączenie połączenia

konfiguracja protokołu NCP

- rodzina protokołów NCP dla konfigurowania różnych protokołów sieciowych.
N.p. kiedy protokołem sieciowym jest IPv4, wtedy NCP przekształca się w IPCP, kiedy IPX, wtedy NCP jest IPXCP, kiedy AppleTalk, wtedy NCP jest ATCP, kiedy IPv6, wtedy NCP jest IPv6CP
- o zawartości pola dane (pakiety protokołów LCP, NCP i pozostałych) świadczy wartość pola protokół:
- 0021 (IP), 002B (IPX), 002D (skomp.nagł.TCP), 0201 (Hello 802.1d), 8021 (IPCP), 802B (IPXCP), 80FD (CCP), C001 (LCP)

protokoły uwierzytelnienia

- **PAP** – Password Authentication Protocol
- wymiana dwuetapowa, uwierzytelnienie tylko raz, po nawiązaniu połączenia, para nazwa użytkownika i hasło jest tak długo przesyłana, aż uwierzytelnienie jest potwierdzone (akceptacja/odmowa), albo połączenie jest rozłączone
- nie jest to protokół bezpieczny - hasła są przesyłane otwartym tekstem, możliwość podsłuchu haseł, brak ochrony przed atakami metodą prób i błędów
- strona zdalna bada ilość prób rejestracji

protokoły uwierzytelnienia

- **CHAP** – Challenge Handshake Authentication Protocol (preferowany)
- wymiana trójetapowa – uwierzytelnienie po nawiązaniu połączenia a następnie powtarzane okresowo w dowolnym późniejszym czasie, na wyraźne polecenie
- wezwanie, odpowiedź, akceptacja/odmowa:
- komputer wysyła do strony zdalnej prośbę o rozpoczęcie uwierzytelnienia, strona zdalna przesyła wartość porównywaną z wartością zapamiętaną po stronie lokalnej, gdy takie same – strona zdalna uwierzytelniona, gdy nie połączenie rozłączane

konfiguracja protokołu NCP

- zanim datagramy IP mogą być przesyłane, PPP musi wejść w fazę Network Layer Protocol, a protokół IPCP musi wejść w stan „opened”
- IPCP negocjuje parametry protokołu IP, n.p. użycie specyficznego protokołu kompresji
- dokładnie jeden datagram IP jest kapsułkowany w polu z danymi w ramce PPP, gdzie pole protokół = 0021_{hex}, większe datagramy są fragmentowane

protokół IPCP

- IPCP (RFC 1332) - <http://www.rfc-editor.org/>
- PPP Network Control Protocol (NCP) for IP
- IPCP odpowiedzialny za konfigurację, włączanie i wyłączanie modułów protokołu IP po obu stronach łącza P2P
- stosuje tę samą wymianę pakietów co LCP, ale pakiety nie mogą być wymieniane przed wejściem protokołu PPP w fazę NCP (gdy przyjdą wcześniej - odrzucane)
- jeden pakiet IPCP w ramce PPP, pole protokół=8021_{hex}
- stosowane kody - od 1 do 7 (od ConfReq do CodeReject)

podsumowanie

zastosowanie protokołu PPP w łączy dwupunktowym:

- łączy dzierżawione i komutowane (modemowe)
- na ISDN (RFC 1618)
- w X25 (RFC 1598)
- w sieci Frame relay (RFC 2427)
- na sieci Sonet (RFC 3225)
- na sieci ATM (AAL5) (RFC 2364)
- na sieci Ethernet (RFC 2516)

