Sieci rozległe

(WAN)

Podstawowe informacje o WAN

- Sieć obejmująca obszary większe niż sieci LAN
- Najczęściej udostępniana przez firmy telekomunikacyjne, specjalizowanych ISP
- Wykorzystuje inne technologie przenoszenia ruchu niż sieci LAN
- Większość technologii WAN zdefiniowana jest w 1 i 2 warstwie modelu ISO/OSI

Podstawowe informacje o WAN

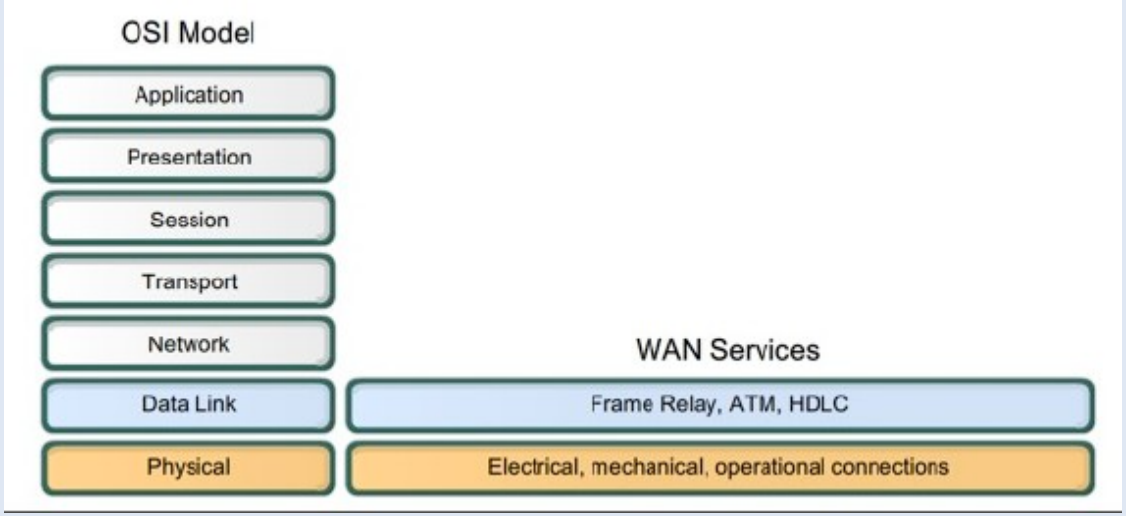
- Sieć obejmująca obszary większe niż sieci LAN
- Najczęściej udostępniana przez firmy telekomunikacyjne, specjalizowanych ISP
- Wykorzystuje inne technologie przenoszenia ruchu niż sieci LAN
- Większość technologii WAN zdefiniowana jest w 1 i 2 warstwie modelu ISO/OSI

Podstawowe informacje o WAN

- Sieć obejmująca obszary większe niż sieci LAN
- Najczęściej udostępniana przez firmy telekomunikacyjne, specjalizowanych ISP
- Wykorzystuje inne technologie przenoszenia ruchu niż sieci LAN
- Większość technologii WAN zdefiniowana jest w 1 i 2 warstwie modelu ISO/OSI

Podstawowe informacje o WAN

- *Sieć obejmująca obszary większe niż sieci LAN*
- *Najczęściej udostępniana przez firmy telekomunikacyjne, specjalizowanych ISP*
- *Wykorzystuje inne technologie przenoszenia ruchu niż sieci LAN*
- *Większość technologii WAN zdefiniowana jest w 1 i 2 warstwie modelu ISO/OSI*



Podstawowe pojęcia wykorzystywane w sieciach WAN

- *CPE (Customer Premises Equipment) wszystkie urządzenia po stronie klienta umożliwiające połączenie z siecią WAN (DCE i DTE)*
- *DCE (Data Communications Equipment) urządzenia przyłączone bezpośrednio do sieci dostawcy ISP (Local Loop)*
- *DTE (Data Terminal Equipment) urządzenia klienta umożliwiające połączenie końcowych urządzeń sieciowych (np. komputer, router) z siecią WAN poprzez urządzenia DCE*
- *Punkt styku (Demarcation Point) węzeł lokalny dostawcy sieciowego ISP w budynku u klienta do przyłączenia urządzeń klienta (CPE) do sieci dostawcy (Local Loop)*
- *Local Loop (Last-mile) połączenie od węzła sieciowego dostawcy ISP (CO) do klienta*
- *CO (Central Office) węzeł sieciowy dostawcy ISP*

Podstawowe pojęcia wykorzystywane w sieciach WAN

- *CPE (Customer Premises Equipment) wszystkie urządzenia po stronie klienta umożliwiające połączenie z siecią WAN (DCE i DTE)*
- *DCE (Data Communications Equipment) urządzenia przyłączone bezpośrednio do sieci dostawcy ISP (Local Loop)*
- *DTE (Data Terminal Equipment) urządzenia klienta umożliwiające połączenie końcowych urządzeń sieciowych (np. komputer, router) z siecią WAN poprzez urządzenia DCE*
- *Punkt styku (Demarcation Point) węzeł lokalny dostawcy sieciowego ISP w budynku u klienta do przyłączenia urządzeń klienta (CPE) do sieci dostawcy (Local Loop)*
- *Local Loop (Last-mile) połączenie od węzła sieciowego dostawcy ISP (CO) do klienta*
- *CO (Central Office) węzeł sieciowy dostawcy ISP*

Podstawowe pojęcia wykorzystywane w sieciach WAN

- *CPE (Customer Premises Equipment) wszystkie urządzenia po stronie klienta umożliwiające połączenie z siecią WAN (DCE i DTE)*
- *DCE (Data Communications Equipment) urządzenia przyłączone bezpośrednio do sieci dostawcy ISP (Local Loop)*
- *DTE (Data Terminal Equipment) urządzenia klienta umożliwiające połączenie końcowych urządzeń sieciowych (np. komputer, router) z siecią WAN poprzez urządzenia DCE*
- *Punkt styku (Demarcation Point) węzeł lokalny dostawcy sieciowego ISP w budynku u klienta do przyłączenia urządzeń klienta (CPE) do sieci dostawcy (Local Loop)*
- *Local Loop (Last-mile) połączenie od węzła sieciowego dostawcy ISP (CO) do klienta*
- *CO (Central Office) węzeł sieciowy dostawcy ISP*

Podstawowe pojęcia wykorzystywane w sieciach WAN

- *CPE (Customer Premises Equipment) wszystkie urządzenia po stronie klienta umożliwiające połączenie z siecią WAN (DCE i DTE)*
- *DCE (Data Communications Equipment) urządzenia przyłączone bezpośrednio do sieci dostawcy ISP (Local Loop)*
- *DTE (Data Terminal Equipment) urządzenia klienta umożliwiające połączenie końcowych urządzeń sieciowych (np. komputer, router) z siecią WAN poprzez urządzenia DCE*
- *Punkt styku (Demarcation Point) węzeł lokalny dostawcy sieciowego ISP w budynku u klienta do przyłączenia urządzeń klienta (CPE) do sieci dostawcy (Local Loop)*
- *Local Loop (Last-mile) połączenie od węzła sieciowego dostawcy ISP (CO) do klienta*
- *CO (Central Office) węzeł sieciowy dostawcy ISP*

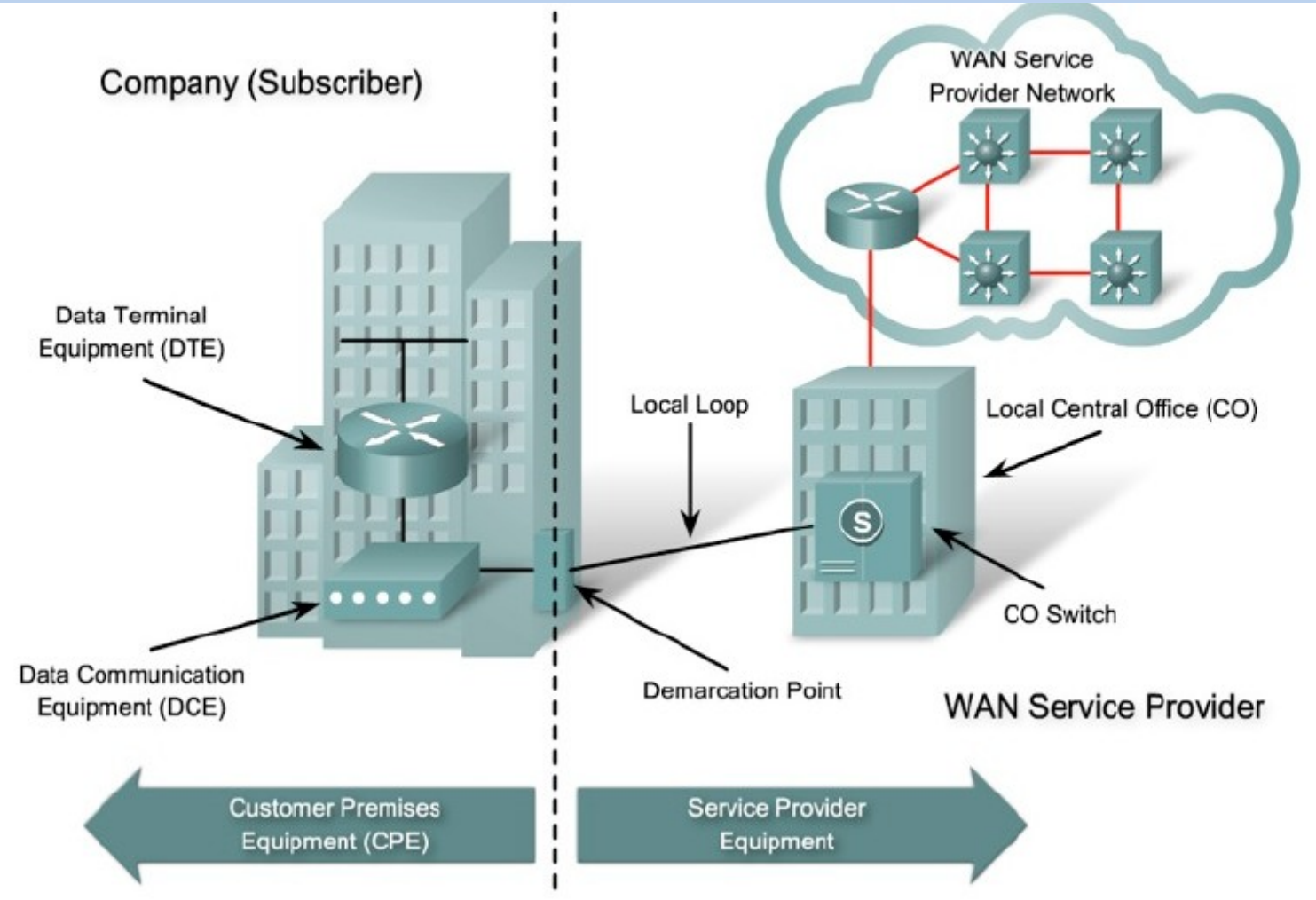
Podstawowe pojęcia wykorzystywane w sieciach WAN

- *CPE (Customer Premises Equipment) wszystkie urządzenia po stronie klienta umożliwiające połączenie z siecią WAN (DCE i DTE)*
- *DCE (Data Communications Equipment) urządzenia przyłączone bezpośrednio do sieci dostawcy ISP (Local Loop)*
- *DTE (Data Terminal Equipment) urządzenia klienta umożliwiające połączenie końcowych urządzeń sieciowych (np. komputer, router) z siecią WAN poprzez urządzenia DCE*
- *Punkt styku (Demarcation Point) węzeł lokalny dostawcy sieciowego ISP w budynku u klienta do przyłączenia urządzeń klienta (CPE) do sieci dostawcy (Local Loop)*
- *Local Loop (Last-mile) połączenie od węzła sieciowego dostawcy ISP (CO) do klienta*
- *CO (Central Office) węzeł sieciowy dostawcy ISP*

Podstawowe pojęcia wykorzystywane w sieciach WAN

- *CPE (Customer Premises Equipment) wszystkie urządzenia po stronie klienta umożliwiające połączenie z siecią WAN (DCE i DTE)*
- *DCE (Data Communications Equipment) urządzenia przyłączone bezpośrednio do sieci dostawcy ISP (Local Loop)*
- *DTE (Data Terminal Equipment) urządzenia klienta umożliwiające połączenie końcowych urządzeń sieciowych (np. komputer, router) z siecią WAN poprzez urządzenia DCE*
- *Punkt styku (Demarcation Point) węzeł lokalny dostawcy sieciowego ISP w budynku u klienta do przyłączenia urządzeń klienta (CPE) do sieci dostawcy (Local Loop)*
- *Local Loop (Last-mile) połączenie od węzła sieciowego dostawcy ISP (CO) do klienta*
- *CO (Central Office) węzeł sieciowy dostawcy ISP*

Podstawowe pojęcia wykorzystywane w sieciach WAN



Elementy WAN w warstwie fizycznej

- Określa sposób łączenia urządzeń (elektryczne i mechaniczne) i przesyłania sygnałów
- Najczęściej spotykane standardy:
  - EIA/TIA-232 (RS-232)
  - EIA/TIA-449/530
  - EIA/TIA-612/613 (HSSI)
  - V.35
  - X.21

Elementy WAN w warstwie fizycznej

- *Określa sposób łączenia urządzeń (elektryczne i mechaniczne) i przesyłania sygnałów*
- *Najczęściej spotykane standardy:*
  - *EIA/TIA-232 (RS-232)*
  - *EIA/TIA-449/530*
  - *EIA/TIA-612/613 (HSSI)*
  - *V.35*
  - *X.21*

Elementy WAN w warstwie łącza danych

- Określają sposób enkapsulacji i przesyłu danych dla protokołów WAN
- Najczęściej spotykane protokoły WAN L2:
  - MPLS (Multi Protocol Label Switching) - aktualny standard budowy nowoczesnych sieci WAN
  - HDLC (High-Level Data Link Control - standard budowy ramek ISO)
  - PPP (Point-to-Point Protocol)
  - ATM (Asynchronous Transfer Mode)
  - Frame Relay
  - ISDN

Elementy WAN w warstwie łącza danych

- *Określają sposób enkapsulacji i przesyłu danych dla protokołów WAN*
- *Najczęściej spotykane protokoły WAN L2:*
  - MPLS (Multi Protocol Label Switching) - aktualny standard budowy nowoczesnych sieci WAN
  - HDLC (High-Level Data Link Control - standard budowy ramek ISO)
  - PPP (Point-to-Point Protocol)
  - ATM (Asynchronous Transfer Mode)
  - Frame Relay
  - ISDN

Typy sieci WAN

- *Circuit Switching (przełączanie obwodów) np. ISDN*
- *Packet Switching (przełączanie pakietów) np. Frame Relay, ATM*
  - PVC (Permanent Virtual Circuit)
  - SVC (Switched Virtual Circuit)
- *Dedicated Point-to-Point (dedykowane łącza) np. PPP, HDLC*
- *Broadband VPN, np. xDSL*

Typy sieci WAN

- *Circuit Switching (przełączanie obwodów) np. ISDN*
- *Packet Switching (przełączanie pakietów) np. Frame Relay, ATM*
  - PVC (Permanent Virtual Circuit)
  - SVC (Switched Virtual Circuit)
- *Dedicated Point-to-Point (dedykowane łącza) np. PPP, HDLC*
- *Broadband VPN, np. xDSL*

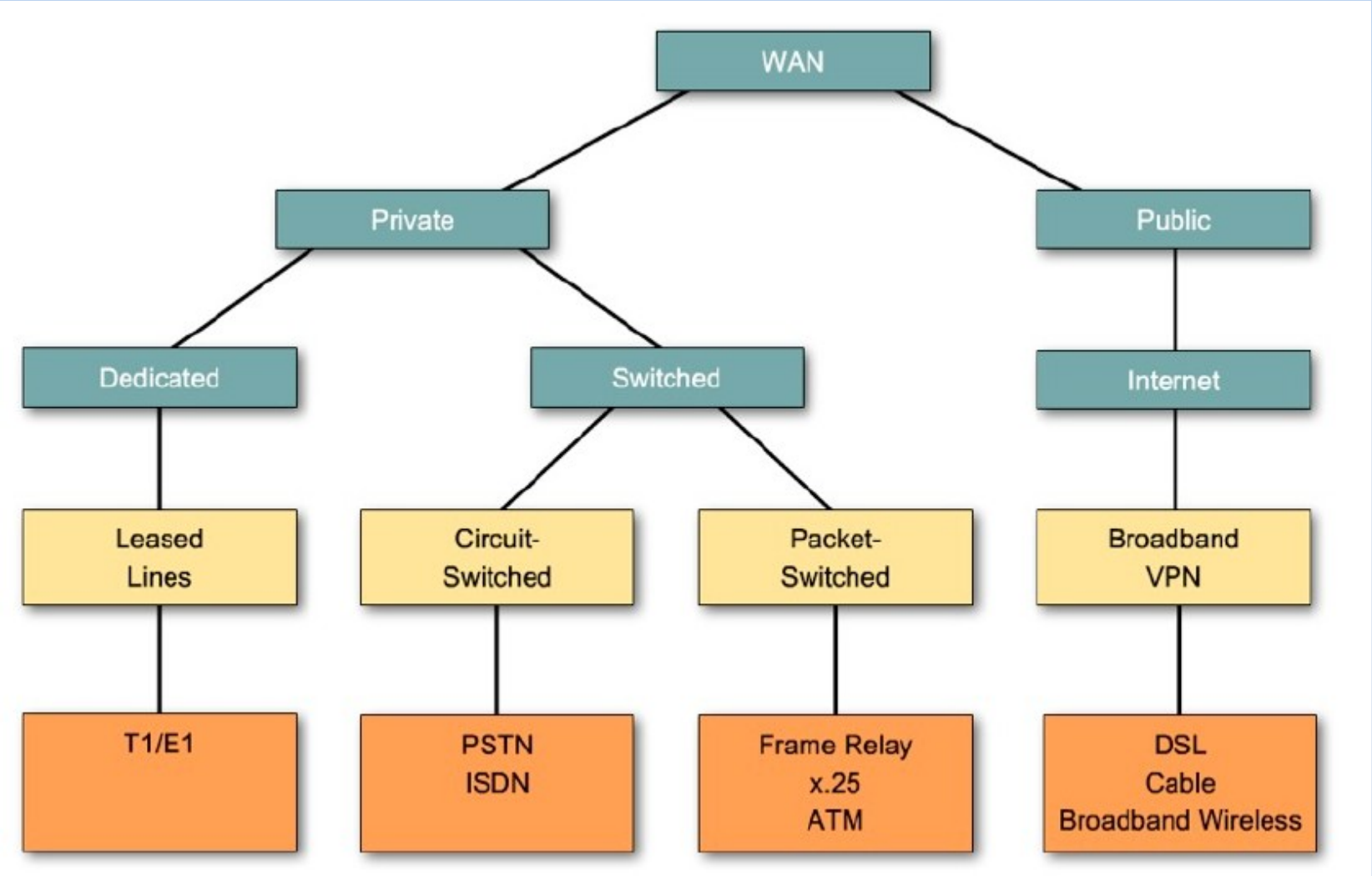
Typy sieci WAN

- *Circuit Switching (przełączanie obwodów) np. ISDN*
- *Packet Switching (przełączanie pakietów) np. Frame Relay, ATM*
  - PVC (Permanent Virtual Circuit)
  - SVC (Switched Virtual Circuit)
- *Dedicated Point-to-Point (dedykowane łącza) np. PPP, HDLC*
- *Broadband VPN, np. xDSL*

Typy sieci WAN

- *Circuit Switching (przełączanie obwodów) np. ISDN*
- *Packet Switching (przełączanie pakietów) np. Frame Relay, ATM*
  - PVC (Permanent Virtual Circuit)
  - SVC (Switched Virtual Circuit)
- *Dedicated Point-to-Point (dedykowane łącza) np. PPP, HDLC*
- *Broadband VPN, np. xDSL*

Typy sieci WAN



Ethernet w sieciach WAN

- Nazywany „Metro Ethernet”
- Ethernet jest sprawdzony, niedrogi, prosty w obsłudze
- W połączeniu z MPLS zapewnia bardzo nowoczesne rozwiązania klasy providerskiej dla obsługi zwykłego ruchu, głosu i wideo
- Przykład: ogólnopolska sieć PIONIER

Ethernet w sieciach WAN

- Nazywany „Metro Ethernet”
- Ethernet jest sprawdzony, niedrogi, prosty w obsłudze
- W połączeniu z MPLS zapewnia bardzo nowoczesne rozwiązania klasy providerskiej dla obsługi zwykłego ruchu, głosu i wideo
- Przykład: ogólnopolska sieć PIONIER

Ethernet w sieciach WAN

- *Nazywany „Metro Ethernet”*
- *Ethernet jest sprawdzony, niedrogi, prosty w obsłudze*
- *W połączeniu z MPLS zapewnia bardzo nowoczesne rozwiązania klasy providerskiej dla obsługi zwykłego ruchu, głosu i wideo*
- *Przykład: ogólnopolska sieć PIONIER*

Ethernet w sieciach WAN

- *Nazywany „Metro Ethernet”*
- *Ethernet jest sprawdzony, niedrogi, prosty w obsłudze*
- *W połączeniu z MPLS zapewnia bardzo nowoczesne rozwiązania klasy providerskiej dla obsługi zwykłego ruchu, głosu i wideo*
- *Przykład: ogólnopolska sieć PIONIER*

Protokół PPP

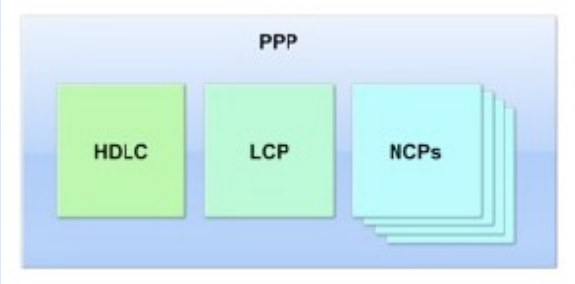
- PPP to rodzaj enkapsulacji ramek warstwy 2 na łączach szeregowych
- Umożliwia monitorowanie jakości połączenia oraz zapewnia autentykację urządzeń (PAP lub CHAP)
- Zawiera 3 główne komponenty:
  - Protokół HDLC dla enkapsulacji datagramów na łączach ppp
  - Link Control Protocol (LCP) dla zestawiania, konfiguracji i testowania połączenia
  - Zestaw protokołów Network Control Protocols (NCP) do zestawiania i konfiguracji różnych protokołów warstwy sieciowej (np. IPCP)

Protokół PPP

- PPP to rodzaj enkapsulacji ramek warstwy 2 na łączach szeregowych
- Umożliwia monitorowanie jakości połączenia oraz zapewnia autentykację urządzeń (PAP lub CHAP)
- Zawiera 3 główne komponenty:
  - Protokół HDLC dla enkapsulacji datagramów na łączach ppp
  - Link Control Protocol (LCP) dla zestawiania, konfiguracji i testowania połączenia
  - Zestaw protokołów Network Control Protocols (NCP) do zestawiania i konfiguracji różnych protokołów warstwy sieciowej (np. IPCP)

Protokół PPP

- *PPP to rodzaj enkapsulacji ramek warstwy 2 na łączach szeregowych*
- *Umożliwia monitorowanie jakości połączenia oraz zapewnia autentykację urządzeń (PAP lub CHAP)*
- *Zawiera 3 główne komponenty:*
  - Protokół HDLC dla enkapsulacji datagramów na łączach ppp
  - Link Control Protocol (LCP) dla zestawiania, konfiguracji i testowania połączenia
  - Zestaw protokołów Network Control Protocols (NCP) do zestawiania i konfiguracji różnych protokołów warstwy sieciowej (np. IPCP)

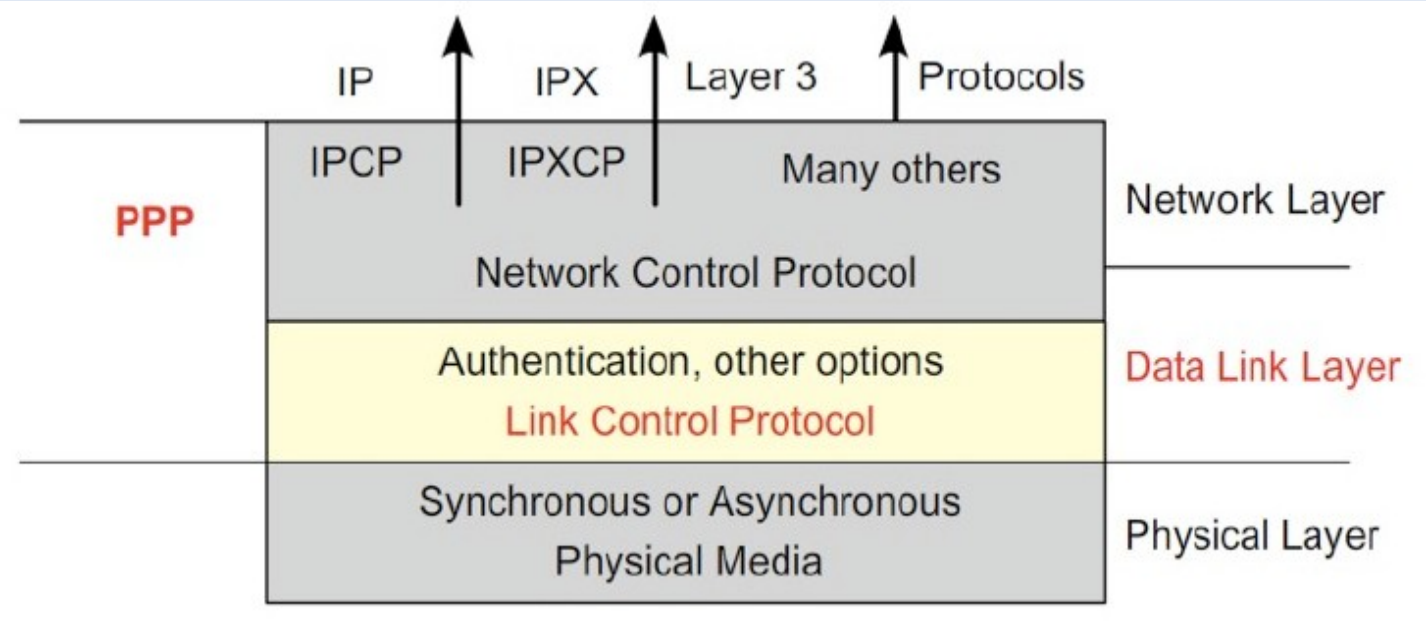


Architektura PPP

PPP składa się z dwóch sub-protokołów:
- Link Control Protocol (LCP) - negocjuje, zestawia, konfiguruje i testuje połączenie point-to-point
- Network Control Protocol (NCP) - konfiguruje komunikację z protokołami warstwy sieciowej

Architektura PPP

PPP składa się z dwóch sub-protokołów:
- Link Control Protocol (LCP) - negocjuje, zestawia, konfiguruje i testuje połączenie point-to-point
- Network Control Protocol (NCP) - konfiguruje komunikację z protokołami warstwy sieciowej



LCP – Link Control Protocol

LCP zapewnia automatyczną konfigurację interfejsów na każdym końcu łącza:

- *obsługuje zmienne limity wielkości pakietu*
- *wykrywa często występujące błędy w konfiguracji*
- *kończy połączenia*
- *określa status połączenia (działa poprawnie lub zostało zerwane)*
- *określa format enkapsulacji (autentykację, kompresję i wykrywanie błędów)*

LCP – Link Control Protocol

LCP zapewnia automatyczną konfigurację interfejsów na każdym końcu łącza:

- obsługuje zmienne limity wielkości pakietu
- wykrywa często występujące błędy w konfiguracji
- kończy połączenia
- określa status połączenia (działa poprawnie lub zostało zerwane)
- określa format enkapsulacji (autentykację, kompresję i wykrywanie błędów)

LCP – Link Control Protocol

LCP zapewnia automatyczną konfigurację interfejsów na każdym końcu łącza:

- *obsługuje zmienne limity wielkości pakietu*
- *wykrywa często występujące błędy w konfiguracji*
- *kończy połączenia*
- *określa status połączenia (działa poprawnie lub zostało zerwane)*
- *określa format enkapsulacji (autentykację, kompresję i wykrywanie błędów)*

LCP – Link Control Protocol

LCP zapewnia automatyczną konfigurację interfejsów na każdym końcu łącza:

- *obsługuje zmienne limity wielkości pakietu*
- *wykrywa często występujące błędy w konfiguracji*
- *kończy połączenia*
- *określa status połączenia (działa poprawnie lub zostało zerwane)*
- *określa format enkapsulacji (autentykację, kompresję i wykrywanie błędów)*

LCP – Link Control Protocol

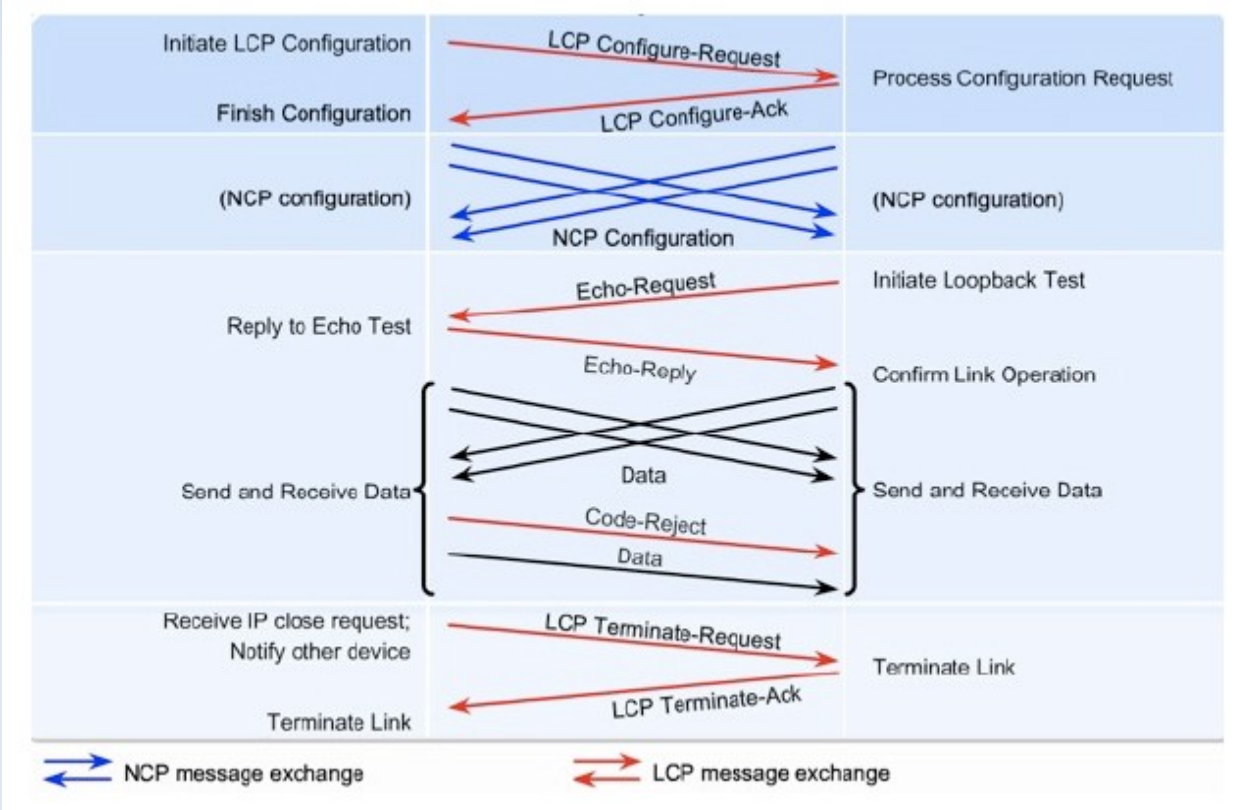
LCP zapewnia automatyczną konfigurację interfejsów na każdym końcu łącza:

- *obsługuje zmienne limity wielkości pakietu*
- *wykrywa często występujące błędy w konfiguracji*
- *kończy połączenia*
- *określa status połączenia (działa poprawnie lub zostało zerwane)*
- *określa format enkapsulacji (autentykację, kompresję i wykrywanie błędów)*

Funkcja	Opis działania	Protokół
Autentykacja	Wymaga haseł i przeprowadza ich wymianę	PAP, CHAP
Kompresja	Kompresuje dane u nadawcy i dekompresuje u odbiorcy	Stacker, Predictor, TCP header, MPCC
Wykrywanie błędów	Monitoruje utracone dane	Quality Magic Number
Multilink	Równoważnie obciążenia na kilku łączach	Multilink Protocol (MP)
PPP Callback	Nawiązuje połączenie zwrotne z klientem	

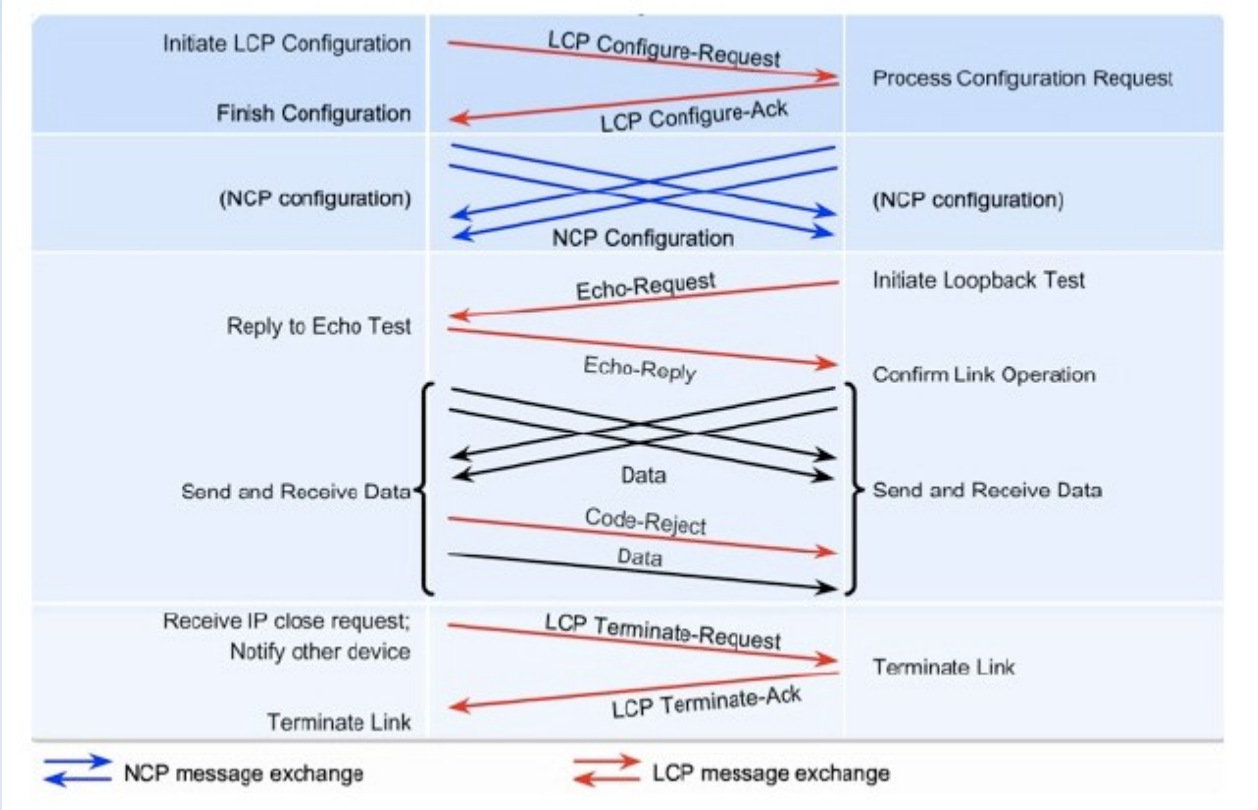
Schemat działania PPP

- Krok 1: nawiązanie połączenia (LCP)
- Krok 2 (opcjonalny): negocjacja konfiguracji przeprowadzenie autentykacji (LCP)
- Krok 3 (opcjonalny): określenie jakości połączenia (LCP)
- Krok 4: negocjacja konfiguracji protokołu warstwy sieciowej (NCP)
- Krok 5: zakończenie połączenia (LCP)



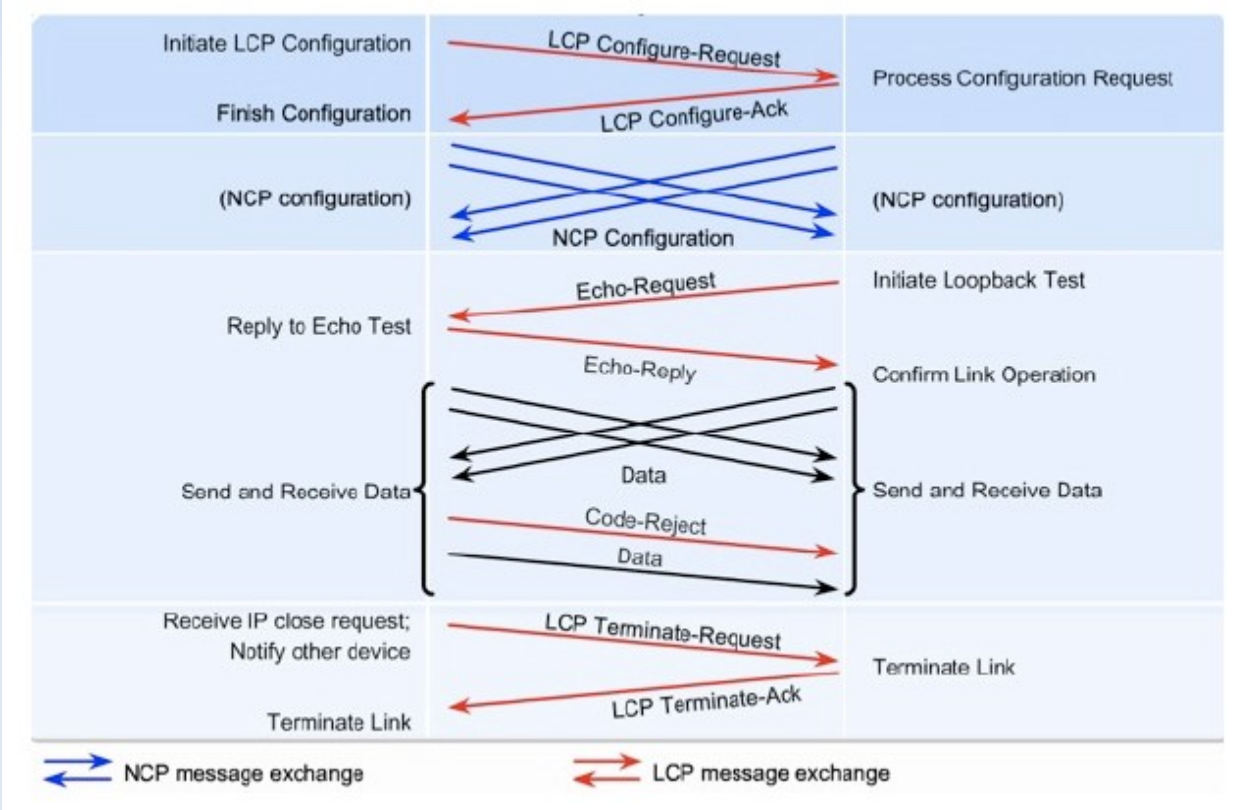
Schemat działania PPP

- Krok 1: nawiązanie połączenia (LCP)
- Krok 2 (opcjonalny): negocjacja konfiguracji przeprowadzenie autentykacji (LCP)
- Krok 3 (opcjonalny): określenie jakości połączenia (LCP)
- Krok 4: negocjacja konfiguracji protokołu warstwy sieciowej (NCP)
- Krok 5: zakończenie połączenia (LCP)



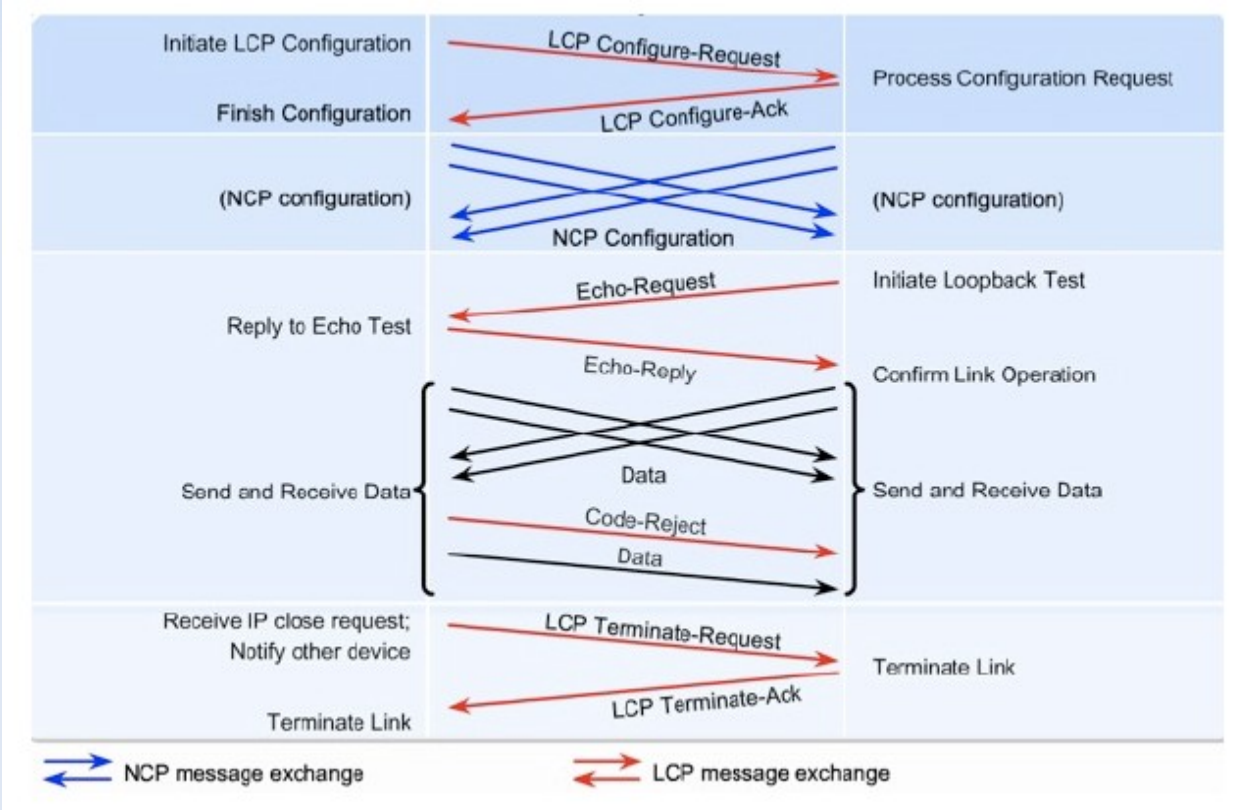
Schemat działania PPP

- *Krok 1: nawiązanie połączenia (LCP)*
- *Krok 2 (opcjonalny): negocjacja konfiguracji przeprowadzenie autentykacji (LCP)*
- *Krok 3 (opcjonalny): określenie jakości połączenia (LCP)*
- *Krok 4: negocjacja konfiguracji protokołu warstwy sieciowej (NCP)*
- *Krok 5: zakończenie połączenia (LCP)*



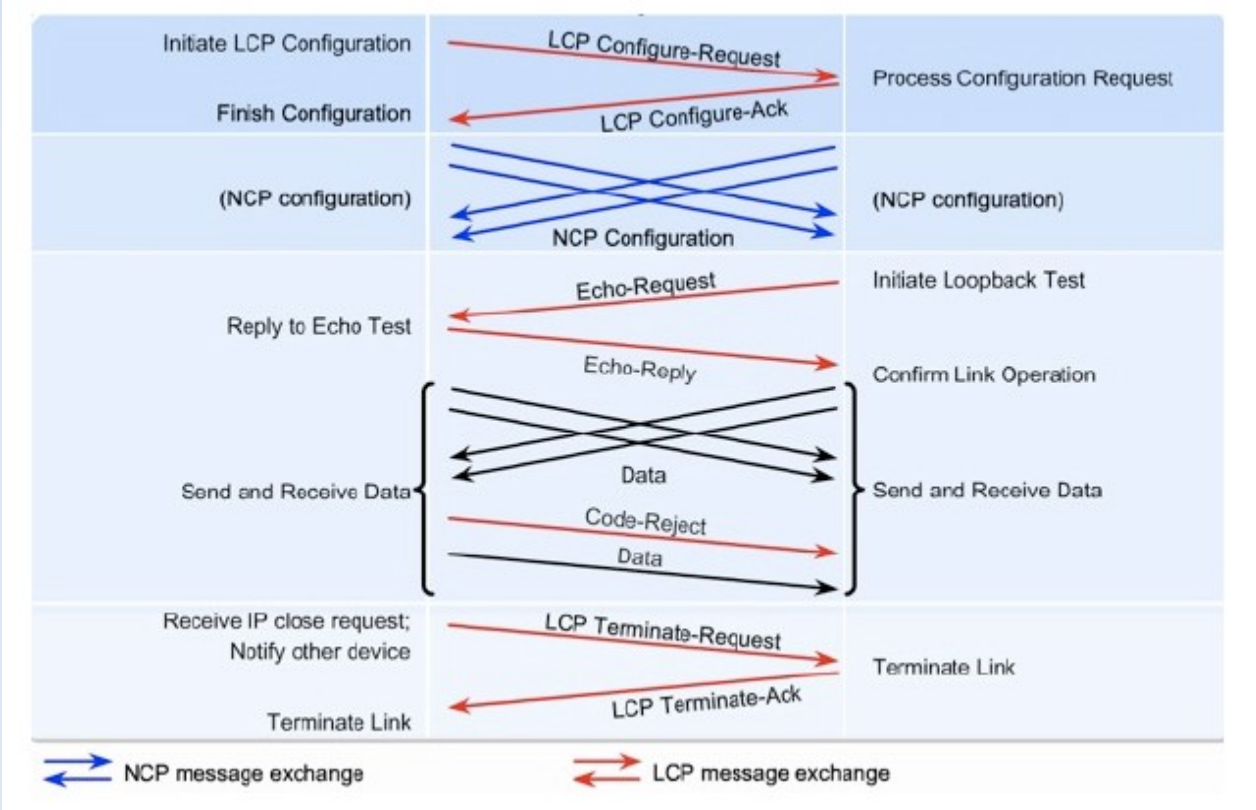
Schemat działania PPP

- *Krok 1: nawiązanie połączenia (LCP)*
- *Krok 2 (opcjonalny): negocjacja konfiguracji przeprowadzenie autentykacji (LCP)*
- *Krok 3 (opcjonalny): określenie jakości połączenia (LCP)*
- *Krok 4: negocjacja konfiguracji protokołu warstwy sieciowej (NCP)*
- *Krok 5: zakończenie połączenia (LCP)*



Schemat działania PPP

- *Krok 1: nawiązanie połączenia (LCP)*
- *Krok 2 (opcjonalny): negocjacja konfiguracji przeprowadzenie autentykacji (LCP)*
- *Krok 3 (opcjonalny): określenie jakości połączenia (LCP)*
- *Krok 4: negocjacja konfiguracji protokołu warstwy sieciowej (NCP)*
- *Krok 5: zakończenie połączenia (LCP)*



Nawiązywanie połączenia w PPP

- Każde urządzenie PPP wysyła pakiety LCP aby skonfigurować i sprawdzić łącze danych
- Pakiety LCP zawierają pole opcji konfiguracji, które umożliwia urządzeniom negocjację wykorzystania opcji (np. rozmiar MTU, kompresję pewnych pól PPP, autentykację)
- Jeśli pole opcji konfiguracji nie jest ustawione w pakiecie LCP przyjmowana jest wartość domyślna (np. brak autentykacji)
- Zanim jakiekolwiek pakiety warstwy sieciowej zostaną przesłane LCP musi zestawić połączenie i przeprowadzić negocjację opcji konfiguracyjnych
- Faza ta kończy się wysłaniem i odebraniem pakietu LCP „configuration acknowledgement”

Nawiązywanie połączenia w PPP

- Każde urządzenie PPP wysyła pakiety LCP aby skonfigurować i sprawdzić łącze danych
- Pakiety LCP zawierają pole opcji konfiguracji, które umożliwia urządzeniom negocjację wykorzystania opcji (np. rozmiar MTU, kompresję pewnych pól PPP, autentykację)
- Jeśli pole opcji konfiguracji nie jest ustawione w pakiecie LCP przyjmowana jest wartość domyślna (np. brak autentykacji)
- Zanim jakiekolwiek pakiety warstwy sieciowej zostaną przesłane LCP musi zestawić połączenie i przeprowadzić negocjację opcji konfiguracyjnych
- Faza ta kończy się wysłaniem i odebraniem pakietu LCP „configuration acknowledgement”

Nawiązywanie połączenia w PPP

- Każde urządzenie PPP wysyła pakiety LCP aby skonfigurować i sprawdzić łącze danych
- Pakiety LCP zawierają pole opcji konfiguracji, które umożliwia urządzeniom negocjację wykorzystania opcji (np. rozmiar MTU, kompresję pewnych pól PPP, autentykację)
- Jeśli pole opcji konfiguracji nie jest ustawione w pakiecie LCP przyjmowana jest wartość domyślna (np. brak autentykacji)
- Zanim jakiekolwiek pakiety warstwy sieciowej zostaną przesłane LCP musi zestawić połączenie i przeprowadzić negocjację opcji konfiguracyjnych
- Faza ta kończy się wysłaniem i odebraniem pakietu LCP „configuration acknowledgement”

Nawiązywanie połączenia w PPP

- *Każde urządzenie PPP wysyła pakiety LCP aby skonfigurować i sprawdzić łącze danych*
- *Pakiety LCP zawierają pole opcji konfiguracji, które umożliwia urządzeniom negocjację wykorzystania opcji (np. rozmiar MTU, kompresję pewnych pól PPP, autentykację)*
- *Jeśli pole opcji konfiguracji nie jest ustawione w pakiecie LCP przyjmowana jest wartość domyślna (np. brak autentykacji)*
- *Zanim jakiekolwiek pakiety warstwy sieciowej zostaną przesłane LCP musi zestawić połączenie i przeprowadzić negocjację opcji konfiguracyjnych*
- *Faza ta kończy się wysłaniem i odebraniem pakietu LCP „configuration acknowledgement”*

Nawiązywanie połączenia w PPP

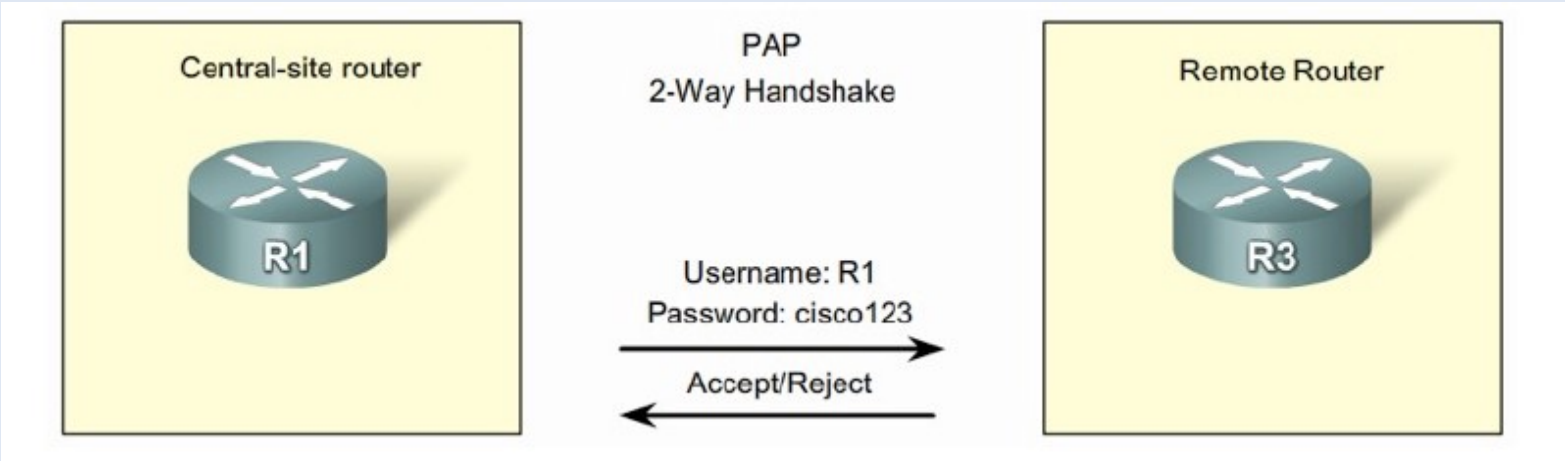
- *Każde urządzenie PPP wysyła pakiety LCP aby skonfigurować i sprawdzić łącze danych*
- *Pakiety LCP zawierają pole opcji konfiguracji, które umożliwia urządzeniom negocjację wykorzystania opcji (np. rozmiar MTU, kompresję pewnych pól PPP, autentykację)*
- *Jeśli pole opcji konfiguracji nie jest ustawione w pakiecie LCP przyjmowana jest wartość domyślna (np. brak autentykacji)*
- *Zanim jakiekolwiek pakiety warstwy sieciowej zostaną przesłane LCP musi zestawić połączenie i przeprowadzić negocjację opcji konfiguracyjnych*
- *Faza ta kończy się wysłaniem i odebraniem pakietu LCP „configuration acknowledgement”*

Protokoły autentykacji w PPP

- Po nawiązaniu połączenia i ustaleniu protokołu autentykacji może odbyć się faza autentykacji urządzeń
- PAP - autentykacja czystym tekstem

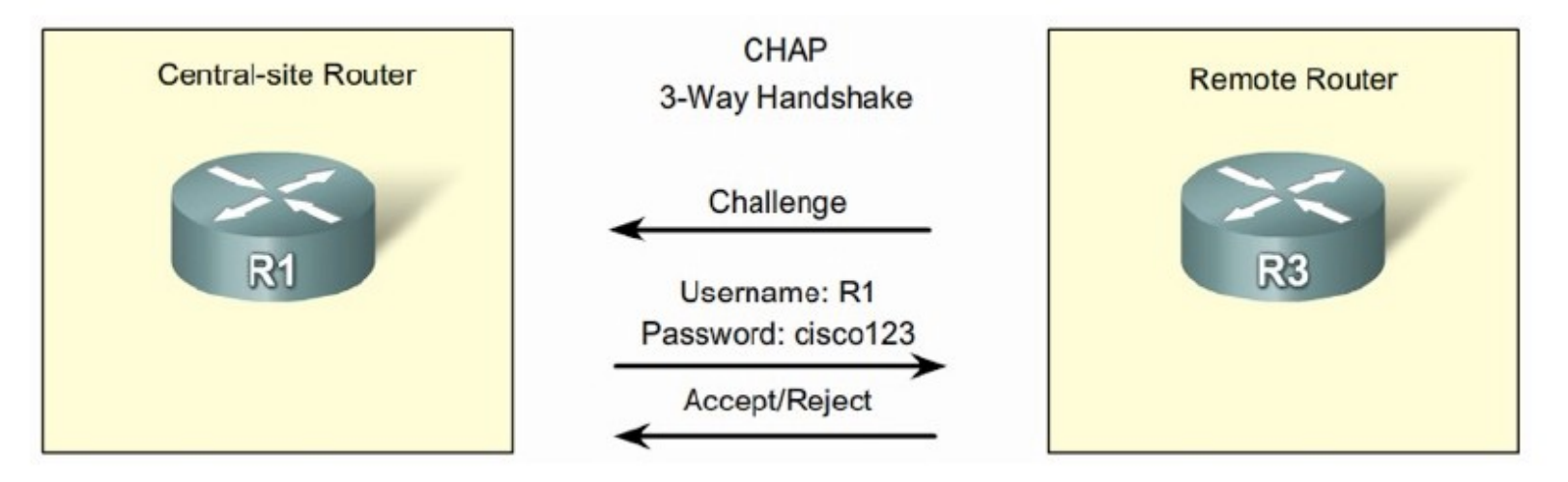
Protokoły autentykacji w PPP

- *Po nawiązaniu połączenia i ustaleniu protokołu autentykacji może odbyć się faza autentykacji urządzeń*
- *PAP - autentykacja czystym tekstem*



Protokoły autentykacji w PPP

- *CHAP - autentykacja szyfrowana*



Protokoły autentykacji w PPP

PAP - Password Authentication Protocol

- Umożliwia proste przekazanie danych identyfikacyjnych z wykorzystaniem mechanizmu „two-way handshake”
- Po zakończeniu fazy nawiązywania połączenia PPP wysyłane są nazwa użytkownika i hasło dopóki urządzenie nie zostanie zidentyfikowane lub nie zostanie zakończone połączenie
- Jest bardzo słabym protokołem autentykacji
- Hasła są przesyłane czystym tekstem bez możliwości ich szyfrowania

Protokoły autentykacji w PPP

PAP - Password Authentication Protocol

- Umożliwia proste przekazanie danych identyfikacyjnych z wykorzystaniem mechanizmu „two-way handshake”
- Po zakończeniu fazy nawiązywania połączenia PPP wysyłane są nazwa użytkownika i hasło dopóki urządzenie nie zostanie zidentyfikowane lub nie zostanie zakończone połączenie
- Jest bardzo słabym protokołem autentykacji
- Hasła są przesyłane czystym tekstem bez możliwości ich szyfrowania

Protokoły autentykacji w PPP

PAP - Password Authentication Protocol

- Umożliwia proste przekazanie danych identyfikacyjnych z wykorzystaniem mechanizmu „two-way handshake”
- Po zakończeniu fazy nawiązywania połączenia PPP wysyłane są nazwa użytkownika i hasło dopóki urządzenie nie zostanie zidentyfikowane lub nie zostanie zakończone połączenie
- Jest bardzo słabym protokołem autentykacji
- Hasła są przesyłane czystym tekstem bez możliwości ich szyfrowania

Protokoły autentykacji w PPP

PAP - Password Authentication Protocol

- *Umożliwia proste przekazanie danych identyfikacyjnych z wykorzystaniem mechanizmu „two-way handshake”*
- *Po zakończeniu fazy nawiązywania połączenia PPP wysyłane są nazwa użytkownika i hasło dopóki urządzenie nie zostanie zidentyfikowane lub nie zostanie zakończone połączenie*
- *Jest bardzo słabym protokołem autentykacji*
- *Hasła są przesyłane czystym tekstem bez możliwości ich szyfrowania*

Protokoły autentykacji w PPP

CHAP - Challenge Handshake Authentication Protocol

- Periodycznie weryfikuje tożsamość zdalnego hosta wykorzystując mechanizm „three-way handshake”
- Po zakończeniu fazy nawiązywania połączenia PPP router lokalny wysyła wiadomość „challenge” do zdalnego hosta
- Host zdalny odpowiada wysyłając wartość wyliczoną przez funkcję haszującą - zwykle jest to Message Digest 5 (MD5)
- Jest ona oparta na haśle i wiadomości „challenge”
- Router lokalny porównuje otrzymaną odpowiedź z własnymi obliczeniami
- Jeśli te wartości są zgodne proces autentykacji kończy się pomyślnie, w przeciwnym przypadku połączenie jest zrywane
- Dzięki wykorzystaniu zmiennej, unikalnej i nieprzewidywalnej wartości „challenge” wynikowy hash MD5 jest losowy i unikalny
- Powtarzanie mechanizmu autentykacji w czasie trwania połączenia ma na celu ograniczenie czasu na przeprowadzenie ataku na aktualnie wykorzystywany hash MD5

Protokoły autentykacji w PPP

CHAP - Challenge Handshake Authentication Protocol

- Periodycznie weryfikuje tożsamość zdalnego hosta wykorzystując mechanizm „three-way handshake”
- Po zakończeniu fazy nawiązywania połączenia PPP router lokalny wysyła wiadomość „challenge” do zdalnego hosta
- Host zdalny odpowiada wysyłając wartość wyliczoną przez funkcję haszującą - zwykle jest to Message Digest 5 (MD5)
- Jest ona oparta na haśle i wiadomości „challenge”
- Router lokalny porównuje otrzymaną odpowiedź z własnymi obliczeniami
- Jeśli te wartości są zgodne proces autentykacji kończy się pomyślnie, w przeciwnym przypadku połączenie jest zrywane
- Dzięki wykorzystaniu zmiennej, unikalnej i nieprzewidywalnej wartości „challenge” wynikowy hash MD5 jest losowy i unikalny
- Powtarzanie mechanizmu autentykacji w czasie trwania połączenia ma na celu ograniczenie czasu na przeprowadzenie ataku na aktualnie wykorzystywany hash MD5

Protokoły autentykacji w PPP

CHAP - Challenge Handshake Authentication Protocol

- Periodycznie weryfikuje tożsamość zdalnego hosta wykorzystując mechanizm „three-way handshake”
- Po zakończeniu fazy nawiązywania połączenia PPP router lokalny wysyła wiadomość „challenge” do zdalnego hosta
- Host zdalny odpowiada wysyłając wartość wyliczoną przez funkcję haszującą - zwykle jest to Message Digest 5 (MD5)
- Jest ona oparta na haśle i wiadomości „challenge”
- Router lokalny porównuje otrzymaną odpowiedź z własnymi obliczeniami
- Jeśli te wartości są zgodne proces autentykacji kończy się pomyślnie, w przeciwnym przypadku połączenie jest zrywane
- Dzięki wykorzystaniu zmiennej, unikalnej i nieprzewidywalnej wartości „challenge” wynikowy hash MD5 jest losowy i unikalny
- Powtarzanie mechanizmu autentykacji w czasie trwania połączenia ma na celu ograniczenie czasu na przeprowadzenie ataku na aktualnie wykorzystywany hash MD5

Protokoły autentykacji w PPP

CHAP - Challenge Handshake Authentication Protocol

- Periodycznie weryfikuje tożsamość zdalnego hosta wykorzystując mechanizm „three-way handshake”
- Po zakończeniu fazy nawiązywania połączenia PPP router lokalny wysyła wiadomość „challenge” do zdalnego hosta
- Host zdalny odpowiada wysyłając wartość wyliczoną przez funkcję haszującą - zwykle jest to Message Digest 5 (MD5)
- Jest ona oparta na haśle i wiadomości „challenge”
- Router lokalny porównuje otrzymaną odpowiedź z własnymi obliczeniami
- Jeśli te wartości są zgodne proces autentykacji kończy się pomyślnie, w przeciwnym przypadku połączenie jest zrywane
- Dzięki wykorzystaniu zmiennej, unikalnej i nieprzewidywalnej wartości „challenge” wynikowy hash MD5 jest losowy i unikalny
- Powtarzanie mechanizmu autentykacji w czasie trwania połączenia ma na celu ograniczenie czasu na przeprowadzenie ataku na aktualnie wykorzystywany hash MD5

Protokoły autentykacji w PPP

CHAP - Challenge Handshake Authentication Protocol

- Periodycznie weryfikuje tożsamość zdalnego hosta wykorzystując mechanizm „three-way handshake”
- Po zakończeniu fazy nawiązywania połączenia PPP router lokalny wysyła wiadomość „challenge” do zdalnego hosta
- Host zdalny odpowiada wysyłając wartość wyliczoną przez funkcję haszującą - zwykle jest to Message Digest 5 (MD5)
- Jest ona oparta na haśle i wiadomości „challenge”
- Router lokalny porównuje otrzymaną odpowiedź z własnymi obliczeniami
- Jeśli te wartości są zgodne proces autentykacji kończy się pomyślnie, w przeciwnym przypadku połączenie jest zrywane
- Dzięki wykorzystaniu zmiennej, unikalnej i nieprzewidywalnej wartości „challenge” wynikowy hash MD5 jest losowy i unikalny
- Powtarzanie mechanizmu autentykacji w czasie trwania połączenia ma na celu ograniczenie czasu na przeprowadzenie ataku na aktualnie wykorzystywany hash MD5

Protokoły autentykacji w PPP

CHAP - Challenge Handshake Authentication Protocol

- Periodycznie weryfikuje tożsamość zdalnego hosta wykorzystując mechanizm „three-way handshake”
- Po zakończeniu fazy nawiązywania połączenia PPP router lokalny wysyła wiadomość „challenge” do zdalnego hosta
- Host zdalny odpowiada wysyłając wartość wyliczoną przez funkcję haszującą - zwykle jest to Message Digest 5 (MD5)
- Jest ona oparta na haśle i wiadomości „challenge”
- Router lokalny porównuje otrzymaną odpowiedź z własnymi obliczeniami
- Jeśli te wartości są zgodne proces autentykacji kończy się pomyślnie, w przeciwnym przypadku połączenie jest zrywane
- Dzięki wykorzystaniu zmiennej, unikalnej i nieprzewidywalnej wartości „challenge” wynikowy hash MD5 jest losowy i unikalny
- Powtarzanie mechanizmu autentykacji w czasie trwania połączenia ma na celu ograniczenie czasu na przeprowadzenie ataku na aktualnie wykorzystywany hash MD5

Protokoły autentykacji w PPP

CHAP - Challenge Handshake Authentication Protocol

- Periodycznie weryfikuje tożsamość zdalnego hosta wykorzystując mechanizm „three-way handshake”
- Po zakończeniu fazy nawiązywania połączenia PPP router lokalny wysyła wiadomość „challenge” do zdalnego hosta
- Host zdalny odpowiada wysyłając wartość wyliczoną przez funkcję haszującą - zwykle jest to Message Digest 5 (MD5)
- Jest ona oparta na haśle i wiadomości „challenge”
- Router lokalny porównuje otrzymaną odpowiedź z własnymi obliczeniami
- Jeśli te wartości są zgodne proces autentykacji kończy się pomyślnie, w przeciwnym przypadku połączenie jest zrywane
- Dzięki wykorzystaniu zmiennej, unikalnej i nieprzewidywalnej wartości „challenge” wynikowy hash MD5 jest losowy i unikalny
- Powtarzanie mechanizmu autentykacji w czasie trwania połączenia ma na celu ograniczenie czasu na przeprowadzenie ataku na aktualnie wykorzystywany hash MD5

Protokoły autentykacji w PPP

CHAP - Challenge Handshake Authentication Protocol

- *Periodycznie weryfikuje tożsamość zdalnego hosta wykorzystując mechanizm „three-way handshake”*
- *Po zakończeniu fazy nawiązywania połączenia PPP router lokalny wysyła wiadomość „challenge” do zdalnego hosta*
- *Host zdalny odpowiada wysyłając wartość wyliczoną przez funkcję haszującą - zwykle jest to Message Digest 5 (MD5)*
- *Jest ona oparta na haśle i wiadomości „challenge”*
- *Router lokalny porównuje otrzymaną odpowiedź z własnymi obliczeniami*
- *Jeśli te wartości są zgodne proces autentykacji kończy się pomyślnie, w przeciwnym przypadku połączenie jest zrywane*
- *Dzięki wykorzystaniu zmiennej, unikalnej i nieprzewidywalnej wartości „challenge” wynikowy hash MD5 jest losowy i unikalny*
- *Powtarzanie mechanizmu autentykacji w czasie trwania połączenia ma na celu ograniczenie czasu na przeprowadzenie ataku na aktualnie wykorzystywany hash MD5*

W końcu koniec !!!