Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет інформатики та обчислювальної техніки

Кафедра Обчислювальної Техніки

Лабораторна робота №1

з дисципліни "Безпека програмного забезпечення"

Тема: "Базова аутентифікація"

Виконав:

студент групи ІП-93

Домінський В.О.

Київ 2022

**Зміст**

[Вступ: 3](#_Toc120041156)

[1. Повний опис PPP 4](#_Toc120041157)

[1.1 Особливості PPP 4](#_Toc120041158)

[2. Взаємодія з іншими протоколами 4](#_Toc120041159)

[2.1 Компоненти PPP 4](#_Toc120041160)

[2.2 Робота PPP 5](#_Toc120041161)

[2.3 Переваги PPP 9](#_Toc120041162)

[Висновок: 10](#_Toc120041163)

[Посилання: 11](#_Toc120041164)

## Basic\_auth

PPP розшифровується як протокол "точка-точка". PPP - це протокол служби віддаленого доступу (RAS) Windows за замовчуванням і є протоколом рівня передачі даних (DLL), який використовується для інкапсуляції протоколів вищих мережевих рівнів для проходження через синхронні та асинхронні лінії зв'язку.

Спочатку був створений як протокол інкапсуляції для передачі численних рівнів мережевого трафіку через з'єднання "точка-точка". Крім того, PPP врегулював різні заходи, включаючи асинхронну і біт-орієнтовану синхронну інкапсуляцію, мультиплексування мережевих протоколів, узгодження сеансів і узгодження стиснення даних.

Перш за все, PPP лежить в основі верифікації, яка може бути використана на обох кінцях з'єднання "точка-точка" для підтвердження ідентичності обладнання або клієнтів. Протокол аутентифікації за допомогою пароля (PAP) і протокол аутентифікації за допомогою рукостискання (CHAP) можуть використовуватися на маршрутизаторах Cisco для перевірки.

### Особливості PPP

1. Кадрування пакетів - формулювання пакетів даних мережевого рівня в блоці каналу передачі даних.
2. Багатопротокольний - передача інформації з будь-якого мережевого рівня NCP вгору одночасно з демультиплексуванням.
3. Бітова прозорість - Повинна нести певну бітову структуру в полі даних.

## Взаємодія з іншими протоколами

### Компоненти PPP

Даний протокол використовує три компоненти, які дозволяють PPP передавати дані по послідовному каналу "точка-точка". Кожна частина має свою власну автономну роль і передбачає використання двох інших компонентів, не обмежуючи їхніх завдань. Цими трьома компонентами є :

1. Протокол High-Level Data-Link Control (HDLC) - HDLC є методом, який використовується для кадрування даних по каналах PPP. З огляду на ДПП, стандартна версія OSI використовується замість пропрієтарної версії Cisco. Ця стандартизація допомагає гарантувати, що різні постачальники можуть належним чином обмінюватися інформацією про виконання PPP.
2. Протокол управління каналами зв'язку (LCP) - відповідає за формулювання, конфігурацію, тестування, підтримку і припинення каналів передачі. Крім того, дві кінцеві точки з'єднання забезпечують переговори щодо встановлення альтернатив та використання функцій.
3. Протоколи управління мережею (NCP) - Кадри NCP використовуються для зв'язку та налаштування протоколів на мережевому рівні, які можуть бути використані протягом сеансу PPP. Існує один NCP для кожного протоколу вищого рівня, який підтримується PPP. NCP дозволяють PPP працювати через аналогічне з'єднання у відповідності з багатьма протоколами мережевого рівня. [1]

### Робота PPP

Підключення PPP, як правило, проходить через різні фази, які можна побачити на перехідній фазовій діаграмі, як показано нижче:

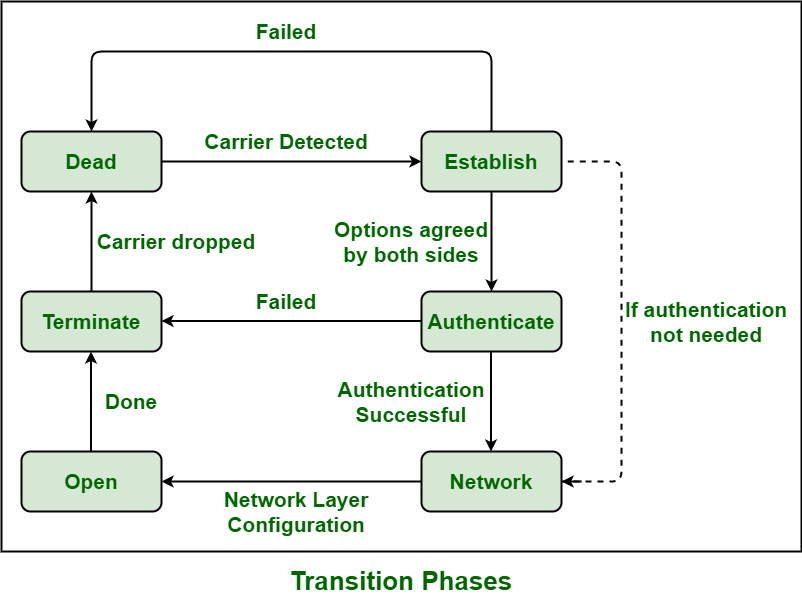


Рис. 1.1 Фазова діаграма PPP

* Мертвий
  + На цій фазі з'єднання в основному запускається і зупиняється. Виявлення несучої - це подія, яка використовується для того, щоб вказати, що фізичний рівень готовий, і тепер PPP перейде до фази встановлення. Відключення від модемної лінії повинно повернути лінію або з'єднання до цієї фази. Автоматизація LCP зазвичай знаходиться в початковій або стартовій фазі під час цієї фази.
* Встановлення
  + З'єднання переходить до цієї фази після виявлення присутності однорангового вузла. Коли один з вузлів починає зв'язок, то з'єднання переходить в цю фазу. Шляхом обміну кадрами або пакетами LCP узгоджуються всі параметри конфігурації. Якщо переговори досягають певної точки, з'єднання встановлюється, а потім система переходить або в протокол аутентифікації, або в протокол мережевого рівня. Закінчення цієї фази просто вказує на відкритий стан LCP.
* Аутентифікація
  + У PPP автентифікація не є обов'язковою. Однорангова автентифікація може бути запитана однією або обома кінцевими точками. PPP переходить до фази аутентифікації, якщо налаштовано протокол аутентифікації за допомогою пароля (PAP) або протокол аутентифікації за допомогою рукостискання (CHAP).
* Мережа
  + PPP в основному надсилає або передає пакети NCP для вибору і налаштування одного або декількох протоколів мережевого рівня, таких як IP, IPX і т.д., як тільки стан LCP відкрито і встановлено канал або з'єднання. Це особливо необхідно для налаштування відповідного мережевого рівня.
  + На цій фазі кожен з протоколів мережевого управління може бути відкритий і закритий в будь-який час, а також відбуваються переговори для цих протоколів. На мережевому рівні PPP також підтримує різні протоколи, завдяки яким PPP визначає, що два вузли встановлюють або розробляють угоду на мережевому рівні до того, як дані будуть обмінюватися на мережевому рівні.
* Відкритий
  + Зазвичай передача даних відбувається в цій фазі. Як тільки кінцеві точки хочуть завершити з'єднання, з'єднання переходить у фазу завершення, до цього моменту з'єднання залишається в цій фазі.
* Завершити
  + З'єднання може бути розірвано в будь-який момент часу за запитом будь-якої з кінцевих точок. LCP в основному необхідний для закриття або розриву з'єднання шляхом обміну пакетами завершення з'єднання. [3]

Кадр PPP, як правило, необхідний для інкапсуляції пакетів інформації або даних, які просто включають або інформацію про конфігурацію, або дані. PPP в основному використовує той самий базовий формат, що і HDLC. PPP зазвичай містить одне додаткове поле, тобто поле протоколу. Це поле протоколу присутнє відразу після контрольного поля і перед полем інформації або даних

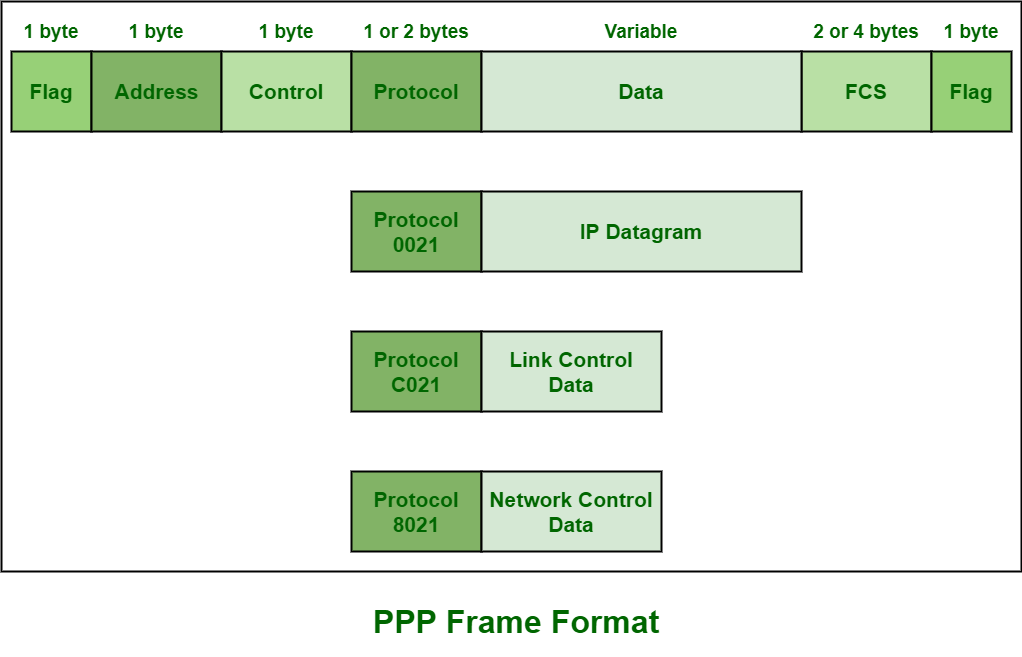


Рис. 1.2 Формат кадру PPP

Нижче наведені різні поля фрейму:

* **Поле прапора**
  + Кадр PPP, подібно до кадру HDLC, завжди починається і закінчується стандартним прапором HDLC. Він завжди має значення 1 байт, тобто двійкове значення 01111110.
* **Поле адреси**
  + Поле адреси - це, по суті, широкомовна адреса. У цьому полі всі одиниці просто вказують на те, що всі станції готові прийняти кадр. Воно має значення 1 байт, тобто 11111111 двійкове значення. З іншого боку, PPP не надає і не призначає індивідуальні адреси станцій.
* **Контрольне поле**
  + Це поле в основному використовує формат U-кадру, тобто ненумерованого кадру в HDLC. У HDLC контрольне поле необхідне для різних цілей, але в PPP це поле встановлено на 1 байт, тобто двійкове значення 00000011. Цей 1 байт використовується для каналу передачі даних без з'єднання.
* **Поле протоколу**
  + Це поле в основному ідентифікує мережевий протокол дейтаграми. Зазвичай воно ідентифікує тип пакету в полі даних, тобто, що саме передається в полі даних. Це поле має розмір 1 або 2 байти і допомагає ідентифікувати PDU (Protocol Data Unit), який інкапсулюється кадром PPP.
* **Поле даних**
  + Зазвичай містить дейтаграму верхнього рівня. Датаграма мережевого рівня особливо інкапсулюється в цьому полі для звичайних кадрів даних PPP. Довжина цього поля не є постійною, а скоріше змінюється.
* **Поле FCS**
  + Це поле зазвичай містить контрольну суму просто для ідентифікації помилок. Вона може мати розмір 16 біт або 32 біт. Вона також обчислюється над адресними, контрольними, протокольними і навіть інформаційними полями. Символи додаються до кадру для контролю та обробки помилок. [2]

### Переваги PPP

1. Ключовою перевагою PPP є те, що це розширюваний набір протоколів.
2. Він підтримує автентифікацію за допомогою PAP та CHAP.
3. Функція управління якістю з'єднань оцінює якість з'єднань. PPP розриває з'єднання у випадку занадто великої кількості помилок.
4. Механізм поступового кадрування, в порівнянні з одним символом END в SLIP.
5. Надійний процес узгодження змінних з'єднання, включаючи максимально можливий розмір кадру [1]

# Висновок:

Під час виконання роботи я обрати протокол моделі OSI та дав йому повний опис, а потім перейшов до опису взаємодії протоколу за варіантом (Я розглядав PPP (Point to Point)) з іншими протоколами рівня. Описав його переваги, недоліки

# Посилання:

* [Проект на GitHub](https://github.com/VsIG-official/Software-Security)