ЛЕКЦІЯ 5

Послідовні канали зв'язку у WAN

та протоколи канального рівня: HDLC і PPP

Навчальна дисципліна

«Глобальні мережі»

Державний університет «Житомирська політехніка»
Кафедра кібербезпеки та захисту інформації

Що було й що буде сьогодні

Пригадуємо ключове з лекції 4 та плануємо лекцію 5

← Лекція 4: що знаємо

- 3-рівнева архітектура Metro Ethernet
- Транспорт: Native / EoS / EoMPLS
- Проблема 4094 VLAN → QinQ (16,8 млн)
- PBB 802.1ah — MAC-in-MAC, 16 млн I-SID
- ERPS (G.8032): кільцевий захист < 50 мс
- RPR (802.17): spatial reuse

Лекція 5: що вивчимо →

1. Виділені канали WAN — концепція
2. DTE / DCE — фізичне з'єднання
3. HDLC — базовий протокол ISO
4. Cisco HDLC vs ISO HDLC
5. PPP — RFC 1661; стек протоколів
6. Машина станів LCP (6 фаз)
7. Автентифікація: PAP vs CHAP
8. Налаштування у Cisco IOS

Виділені канали зв'язку у WAN

Leased lines — постійно виділена смуга від оператора між двома точками

Що таке виділений канал

Оператор надає клієнту у **постійне користування** канал з фіксованою пропускною здатністю між двома фізичними точками.

Ключові властивості:

- **смуга** гарантована 24/7 незалежно від часу доби і трафіку інших
- **затримка** стабільна, низький джитер
- **приватність** — трафік не змішується з чужим
- **фіксована плата** незалежно від обсягу переданого

Класика: T1 (1,544 Мбіт/с) · E1 (2,048 Мбіт/с) · T3, E3, OC-3 …

Де застосовуються



З'єднання головного офісу з філіями

точка-точка постійного трафіку



WAN-канали між маршрутизаторами

магістральні лінки провайдерів



Резервування дата-центрів

реплікація даних 24/7 з гарантованою смугою



Критичні системи

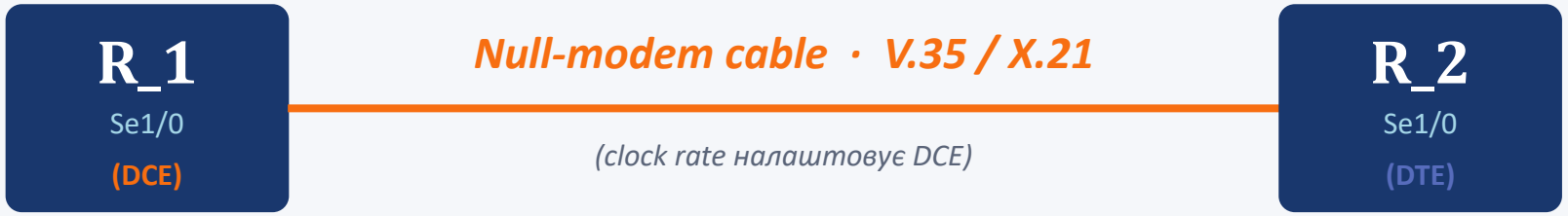
банки, платіжні системи, урядові мережі — де важлива приватність

Фізичне з'єднання: DTE, DCE, CSU/DSU

Термінологія Cisco та стандарти послідовних інтерфейсів



Реальна схема (з ISP-мережею)



Лабораторна схема (пряме з'єднання)

Стандарти інтерфейсів: V.35 · X.21 · EIA/TIA-232 · EIA/TIA-449 · EIA-530 (TIA-530-A) · EIA-612/613 (HSSI)

HDLC — High-Level Data Link Control

Базовий бітово-орієнтований протокол канального рівня; стандарт ISO/IEC 13239

Структура кадру HDLC

Flag	Address	Control	Data	FCS	Flag
01111110	адреса	тип+№	payload	CRC-16/32	01111110
1 байт	*1 байт*	*1–2 б*	*змінне*	*2–4 б*	*1 байт*

Flag 0x7E

01111110 — маркер початку й кінця кадру; bit stuffing запобігає збігам у payload

Три типи кадрів

I (Information — дані), S (Supervisory — контроль), U (Unnumbered — керування)

Бітово-орієнтований

оперує довільними послідовностями бітів (на відміну від байтових SLIP чи PPP)

Основа для інших

PPP, LAPB (X.25), LAPD (ISDN), LAPF (Frame Relay) — усі похідні від HDLC

Cisco HDLC vs стандартний HDLC

Cisco HDLC — пропрієтарна реалізація за замовчуванням на послідовних інтерфейсах

ISO HDLC

СТАНДАРТ

класичний стандарт (ISO/IEC 13239)

Розробник: ISO, ~1979 р.

Особливості:

- чітка структура кадру за стандартом
- підтримує тільки **один протокол** верхнього рівня
- без ідентифікатора протоколу в заголовку

Проблема:

не можна одночасно передавати IPv4, IPv6, IPX по одному каналу — HDLC не «знає», що всередині

Cisco HDLC

CISCO ONLY

розширення від Cisco Systems

Розробник: Cisco Systems

Особливості:

- додано 2-байтне поле **Type** (як у Ethernet)
- підтримка **кількох протоколів** верхнього рівня одночасно
- за замовчуванням на послідовних інтерфейсах Cisco

Обмеження:

працює тільки між пристроями Cisco. Для інших виробників — стандартний PPP

Практичний факт: у Cisco IOS **encapsulation hdlc** — це протокол **за замовчуванням** на будь-якому послідовному інтерфейсі

Чому HDLC вже мало: перехід до PPP

PPP — Point-to-Point Protocol, RFC 1661 (1994) — сучасний стандарт для двоточкових каналів

⚠ Обмеження HDLC

- **Немає автентифікації** — будь-хто, хто фізично підключиться до каналу, може передавати трафік
- **Стандартний HDLC** — тільки один протокол верхнього рівня на канал (проблема мультипротокольності)
- **Cisco HDLC** — пропрієтарний, не сумісний з іншими виробниками
- **Немає механізму** узгодження параметрів каналу (MTU, стиснення тощо) — все треба конфігурувати вручну
- **Немає перевірки якості каналу** — відсутні LQM/LQR

☑ Що вирішує PPP

✓ **Автентифікація** — вбудовані протоколи PAP та CHAP

✓ **Мультипротокольність** — NCP окремо для IPv4 (IPCP), IPv6 (IPv6CP), IPX (IPXCP) тощо

✓ **Відкритий стандарт** — RFC 1661 (IETF); всі виробники підтримують

✓ **Автоматичне узгодження** через LCP (MTU, стиснення, авторизація, magic number)

✓ **Моніторинг якості** — LQM (Link Quality Monitoring) через LQR-пакети

PPP — стек протоколів (RFC 1661)

Багатошарова архітектура: HDLC-подібне кадрування + LCP + NCP + автентифікація

Мережеві протоколи
IPv4, IPv6, IPX, AppleTalk …

NCP — Network Control Protocols
IPCP (RFC 1332), IPv6CP (RFC 5072), IPXCP …
по одному NCP на мережевий протокол

Автентифікація (опційно)
PAP (RFC 1334), CHAP (RFC 1994), EAP (RFC 2284)

LCP — Link Control Protocol
узгодження параметрів каналу; RFC 1661
серце PPP

HDLC-подібне кадрування
формат кадру запозичений з HDLC; RFC 1662

Фізичний рівень
Serial, ISDN, DSL, SONET …

LCP — «мозок» PPP

Встановлює, налаштовує й підтримує з'єднання. Узгоджує параметри: MTU, стиснення, автентифікацію, magic number для виявлення петель.

NCP — окремо для кожного протоколу

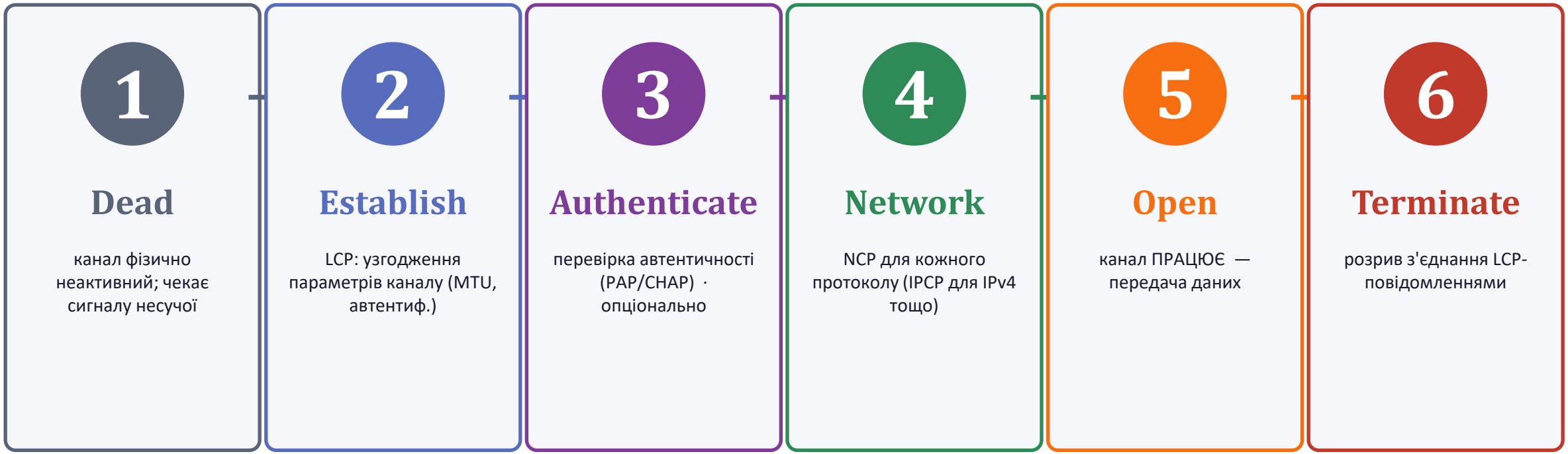
Для кожного мережевого протоколу — свій NCP: **IPCP** для IPv4 (адреси, стиснення VJ), **IPv6CP** для IPv6.

Автентифікація — опціональна

Виконується після LCP, **до** фази NCP. Два основні: **PAP** (простий, пароль у відкритому вигляді) та **CHAP** (challenge-response, безпечний).

Машина станів PPP — 6 фаз встановлення з'єднання

Послідовність LCP → Authentication → NCP; кожна фаза має чіткий результат



Ключові сигнали й перевірки

- **Establish** → надсилаються LCP Configure-Request; обидві сторони узгоджують параметри
- **Authenticate** → PAP надсилає ім'я+пароль; CHAP надсилає challenge → відповідь → результат
- **Network** → IPCP узгоджує IP-адреси; на екрані show interfaces з'являється «LCP Open, IPCP Open»

Автентифікація PPP: PAP та CHAP

Два стандартні протоколи автентифікації у PPP-каналах

PAP

НЕБЕЗПЕЧНО

Password Authentication Protocol · RFC 1334

Механізм: 2 повідомлення

1. **Клієнт → Сервер:** «Ось моє ім'я та пароль»
   (пароль у відкритому вигляді!)
2. **Сервер → Клієнт:** Authenticate-Ack або Authenticate-Nak

Мінуси:

- пароль передається у **відкритому вигляді** (clear text)
- тільки при встановленні каналу, не повторюється
- вразливий до перехоплення й replay-атак

Коли використовувати:

лише для сумісності зі старим обладнанням; CHAP не працює

CHAP

БЕЗПЕЧНО

Challenge Handshake Auth Protocol · RFC 1994

Механізм: 3 повідомлення (Challenge-Response)

1. **Сервер → Клієнт:** «Challenge» (випадкове число)
2. **Клієнт → Сервер:** MD5-хеш(Challenge + пароль)
3. **Сервер → Клієнт:** Success або Failure

→ ***пароль НІКОЛИ не передається каналом***

Плюси:

✓ пароль **не передається** по каналу
✓ повторна перевірка через випадкові інтервали
✓ захист від replay-атак (унікальний challenge)

Коли використовувати:

рекомендовано за замовчуванням для всіх PPP-з'єднань

Налаштування HDLC у Cisco IOS

Крок за кроком: активація інтерфейсу, DCE/DTE, IP-адреса

5 обов'язкових кроків

1. Обрати послідовний інтерфейс
   `interface Serial 1/0`
2. Для DCE — задати тактову частоту
   `clock rate 64000`
3. Обрати протокол інкапсуляції
   `encapsulation hdlc`
   `(HDLC — за замовчуванням)`
4. Присвоїти IP-адресу
   `ip address 196.1.1.1 255.255.255.252`
5. Активувати інтерфейс
   `no shutdown`

Приклад: R_1 (DCE) ↔ R_2 (DTE)

```
R_1> enable
R_1# configure terminal
R_1(config)# interface Serial 1/0
R_1(config-if)# description LINK_TO_R_2
R_1(config-if)# clock rate 64000
R_1(config-if)# ip address 196.1.1.1 255.255.255.252
R_1(config-if)# no shutdown
R_1(config-if)# exit

R_2(config)# interface Serial 1/0
R_2(config-if)# description LINK_TO_R_1
R_2(config-if)# ip address 196.1.1.2 255.255.255.252
R_2(config-if)# no shutdown
```

★ *На R_2 (DTE) команду clock rate НЕ виконуємо!*

Налаштування PPP + CHAP у Cisco IOS

Повний приклад: заміна інкапсуляції з HDLC на PPP + автентифікація CHAP

R_1 (DCE) — ім'я R_1, пароль mypass

```
R_1(config)# username R_2 password mypass
```
← ім'я СУСІДА!
```
R_1(config)# interface Serial 1/0

R_1(config-if)# clock rate 64000

R_1(config-if)# encapsulation ppp
```
← замість hdlc
```
R_1(config-if)# ppp authentication chap
```
← увімкнути CHAP
```
R_1(config-if)# ip address 196.1.1.1
255.255.255.252

R_1(config-if)# no shutdown
```

R_2 (DTE) — ім'я R_2, пароль mypass

```
R_2(config)# username R_1 password mypass
```
← ім'я СУСІДА!
```
R_2(config)# interface Serial 1/0

R_2(config-if)# encapsulation ppp
```
← замість hdlc
```
R_2(config-if)# ppp authentication chap
```
← увімкнути CHAP
```
R_2(config-if)# ip address 196.1.1.2
255.255.255.252

R_2(config-if)# no shutdown
```

Моніторинг і діагностика послідовних каналів

Команди show та debug для перевірки роботи HDLC/PPP

Команда	Призначення
`show controllers serial 1/0`	стан контролера, тип кабелю (DCE / DTE)
`show interfaces serial 1/0`	детальна інформація: encapsulation, LCP, IPCP, статистика
`show interfaces`	всі інтерфейси пристрою — короткий огляд
`show compress`	стан алгоритмів стиснення (Stac, MPPC, Predictor)
`show ppp multilink`	інформація про багатоканальні PPP-з'єднання
`debug serial interface`	трасування подій на послідовному інтерфейсі
`debug ppp negotiation`	покрокове відстеження узгодження LCP/NCP
`debug ppp authentication`	відстеження процесу PAP / CHAP автентифікації

Ключовий фрагмент виводу show interfaces при працюючому PPP:

```
Serial1/0 is up, line protocol is up   · Encapsulation PPP, LCP Open · Open: IPCP, CCP, CDPCP
```

Порівняння: HDLC vs PPP

Коли обирати HDLC, а коли PPP

Критерій	HDLC (Cisco)	PPP (RFC 1661)
Стандарт	пропрієтарний Cisco	відкритий, IETF
Сумісність	тільки Cisco ↔ Cisco	усі виробники
Автентифікація	немає	PAP, CHAP, EAP
Мультипротокольність	так (Cisco HDLC, поле Type)	так (окремі NCP)
Узгодження параметрів	немає	LCP (MTU, стиснення, …)
Стиснення	Stac	Stac, Predictor, LZS, MPPC
Моніторинг якості	немає	LQM / LQR
Складність налаштування	мінімальна (за замовч.)	потрібне явне налаштування
Використання	прості канали Cisco-Cisco	усі інші випадки

→ **Практичне правило:** усе, що не є Cisco↔Cisco → PPP. **У сумніві → PPP** *(відкритий, гнучкий, безпечніший).*

Підсумок лекції

01 **Виділені канали WAN**

leased lines: гарантована смуга 24/7; T1/E1; для критичних з'єднань

02 **DTE ↔ DCE ↔ мережа**

DCE (CSU/DSU) синхронізує; у лабораторії — DCE задає clock rate

03 **HDLC — база (ISO/IEC 13239)**

бітово-орієнтований; Flag 0x7E; кадри I/S/U; за замовчуванням у Cisco

04 **PPP — RFC 1661**

LCP (керування) + NCP (IPCP, IPv6CP) + автентифікація + HDLC-кадрування

05 **PAP vs CHAP**

PAP — clear text (небезпечно); CHAP — MD5 challenge-response (RFC 1994)

06 **6 фаз машини станів PPP**

Dead → Establish → Auth → Network → Open → Terminate

→ **Наступна лекція:** *моделі послуг та QoS*



Ваші запитання

Обговорення матеріалу лекції

Дякую за увагу!