

ЗАНЯТТЯ № 1

ДОСЛІДЖЕННЯ ТА НАЛАГОДЖЕННЯ АГРЕГАЦІЇ КАНАЛІВ ETHERCHANNEL І MULTILINK PPP У МЕРЕЖАХ НА БАЗІ ОБЛАДНАННЯ CISCO

Мета заняття: ознайомитися з особливостями функціонування технологій та протоколів агрегації каналів у локальних (EtherChannel з протоколами LACP і PAgP) та глобальних (Multilink PPP) мережах; отримати практичні навички налагодження, моніторингу та діагностування роботи статичних і динамічних агрегованих каналів на комутаторах і маршрутизаторах Cisco; дослідити процеси передачі кадрів і пакетів через агреговані канали; ознайомитися з методами балансування навантаження між фізичними каналами агрегованого з'єднання та навчитися розраховувати, якими фізичними інтерфейсами проходитиме трафік при різних методах балансування.

Обладнання та програмне забезпечення

Для виконання заняття на робочому місці студента має бути наявним таке обладнання та програмне забезпечення:

1. Керовані комутатори Cisco серії Catalyst 2960 (моделі WS-C2960-24TT-L або WS-C2960-48TT-L або WS-C2960S-F24TS-L або WS-C3560-24TS) – 3 шт.
2. Маршрутизатори Cisco серії 1841/2801/2811/2821/2901/2911/2921 з інтерфейсними слотами для плат розширення – 2 шт.
 - Плати розширення Cisco WIC-2T (або аналогічні) для звичайних послідовних з'єднань – 2 шт.
 - Плата розширення Cisco VWIC2-1MFT-T1/E1 або VWIC1MFT-E1 (або аналогічна) для послідовного з'єднання через RJ-48 – 2 шт.
3. Робочі станції (ПК або ноутбуки) з операційною системою Windows/Linux – не менше 2 шт.
4. Консольний кабель Cisco (rollover) з конектором RJ-45 та перехідником на USB або COM-порт – 1 шт.
5. Ethernet-кабелі прямого типу (T568B) категорії Cat 5e/Cat 6 – не менше 10 шт. (для підключення фізичних каналів агрегованих з'єднань між комутаторами та робочими станціями).
6. Serial-кабелі:
 - нуль-модемні послідовні кабелі (V.35 DTE + V.35 DCE) – 2 шт.
 - кабелі RJ-48 для з'єднання через модуль VWIC – 2 шт.
7. Термінальна програма-емулятор (PuTTY, Tera Term, SecureCRT або аналогічна) – встановлена на робочій станції.

Схема підключення

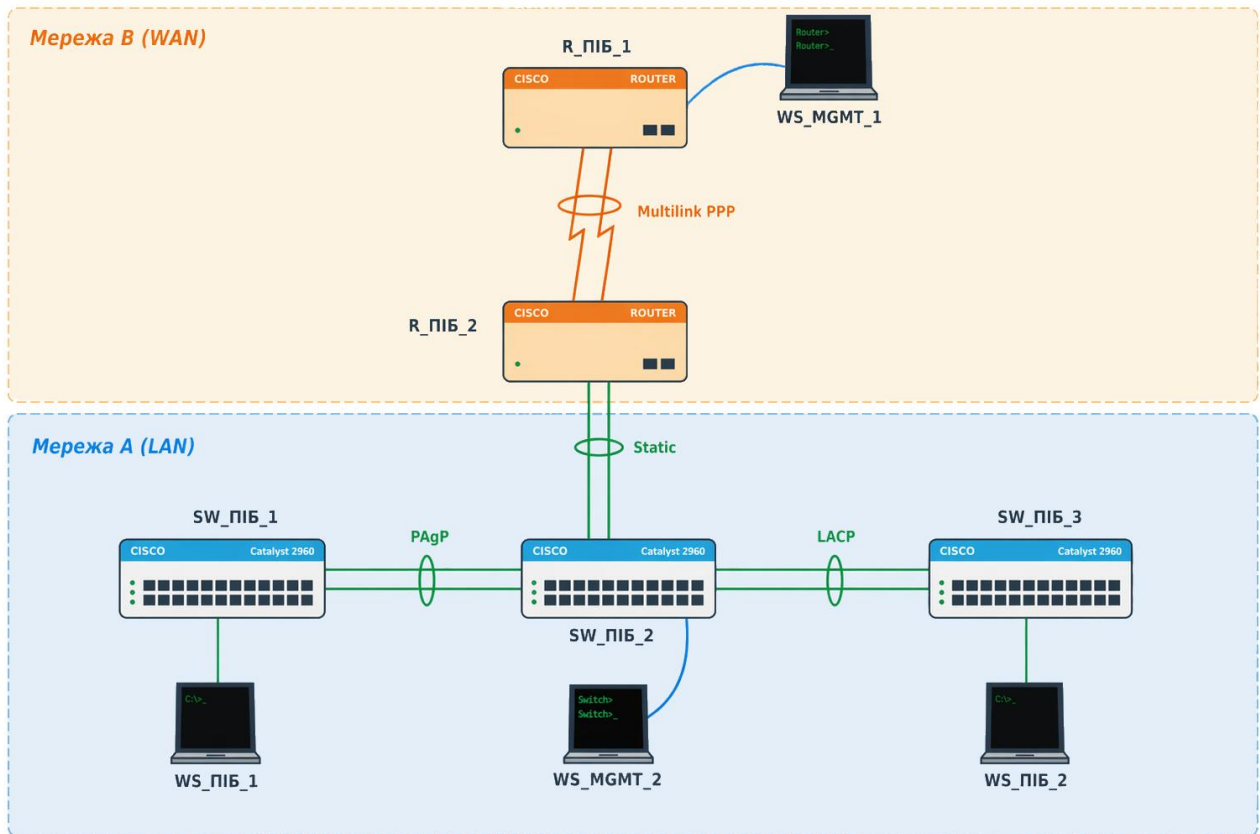


Рис. 1.1. Схема мережі, що будується у межах заняття

Примітка: ПІБ необхідно зазначати у скороченому форматі, який відповідає логіну для входу на платформу learn. Приклад: якщо логін для входу на learn – kb1_kmd, то назва комутатора має бути у форматі SW_kmd_1.

ЗАВДАННЯ

1. Ознайомитися з обладнанням та програмним забезпеченням робочого місця, перевірити наявність консольних, Ethernet- та Serial-кабелів.
2. Створити мережу відповідно до схеми на рис. 1.1. Під час побудови звернути увагу на вибір мережних з'єднань (тип кабелю, тип з'єднання).
3. Провести налагодження іменування всіх 5 пристроїв (R_ПІБ_1, R_ПІБ_2, SW_ПІБ_1, SW_ПІБ_2, SW_ПІБ_3).
4. Розробити схему IP-адресації пристроїв мережі. Для цього скористатися даними табл. 1.5 згідно з варіантом. Результати заповнити у табл. 1.1.

Параметри адресації мережі

Мережа/Пристрій	Інтерфейс	MAC-адреса	IP-адреса	Маска	Префікс
Мережа А	–	–			
Мережа В	–	–			
Маршрутизатор R1	Інтерфейс Multilink 1	–			
Маршрутизатор R2	Інтерфейс Multilink 1	–			
	Port-channel				
Комутатор SW1	Vlan 1				
Комутатор SW2	Vlan 1				
Комутатор SW3	Vlan 1				
WS1					
WS2					

5. Провести налагодження агрегованих каналів. Для цього згідно з варіантом (табл. 1.3) налаштувати:

- Агрегований канал EtherChannel (режим ON) між R_ПІБ_2 та SW_ПІБ_2 на двох фізичних Ethernet-інтерфейсах. На маршрутизаторі створити Port-channel-інтерфейс вручну командою **interface port-channel**, на комутаторі – автоматично командою **channel-group**. Призначити IP адресу.
- Агрегований канал на основі протоколу PAgP між SW_ПІБ_1 та SW_ПІБ_2 на двох фізичних Ethernet-інтерфейсах (режими згідно табл. 1.3).
- Агрегований канал на основі протоколу LACP між SW_ПІБ_2 та SW_ПІБ_3 на двох фізичних Ethernet-інтерфейсах (режими згідно табл. 1.3).
- налаштувати метод балансування навантаження для агрегованих каналів EtherChannel згідно з даними табл. 1.4.
- Виконати розрахунок, якими саме фізичними інтерфейсами Port-channel буде передаватися трафік у напрямку від робочої станції WS_ПІБ_1 (підключеної до SW_ПІБ_1) до WS_ПІБ_2 (підключеної до SW_ПІБ_3); Розрахунок здійснити на основі налагодженого методу балансування з урахуванням MAC- та IP-адрес пристроїв мережі. Результати розрахунку порівняти з реальним проходженням трафіку, що спостерігається за командами **show etherchannel port-channel** (колонка **Load**) або **debug**-командами. Оформити у вигляді таблиці 1.2.

Розподіл трафіку між фізичними каналами

№	Ділянка EtherChannel	Метод балансу- вання	Значення ключового поля	Молодші біти (дв.)	Біт вибору	Очікуваний інтерфейс	Факт. Load (hex)
1	SW1 → SW2 (PAgP)						
2	SW2 → SW3 (LACP)						
3	SW3 → SW2 (LACP)						
4	SW2 → SW1 (PAgP)						

Примітка: У кожному рядку стовпець «Значення ключового поля» заповнюється фактичним значенням src або dst (залежно від методу балансування) MAC- чи IP-адреси пристрою-джерела або отримувача на поточній ділянці. У стовпці «Молодші біти (дв.)» наводяться 4 молодші біти двійкового подання відповідного поля. У стовпці «Біт вибору» – значення молодшого біта (0 або 1); для методів src-dst-mac / src-dst-ip. Стовпець «Факт. Load» заповнюється на основі виведення команди **show etherchannel port-channel** (колонка «Load») на відповідному комутаторі; дві цифри у шістнадцятковій системі показують, які хеш-значення потрапили на цей фізичний інтерфейс. Якщо очікуваний та фактичний інтерфейси співпадають – розрахунок підтверджено.

6. Налаштувати агрегований канал Multilink PPP між R_ПІБ_1 та R_ПІБ_2, об'єднавши два фізичні канали (Serial DTE/DCE або RJ-48) у групу Multilink відповідно до даних табл. 1.3. Налаштувати автентифікацію PPP за протоколом CHAP/PAP, призначити IP-адресу інтерфейсу Multilink, увімкнути відповідну підтримку multilink на фізичних інтерфейсах.

7. Налаштувати параметри IP-адресації та шлюзів за замовчуванням на робочих станціях. Перевірити наявність зв'язку між усіма пристроями мережі командою **ping**. Використати команду **tracert (tracoute)** для спостереження шляху проходження пакетів.

8. Дослідити результати налагодження агрегованих каналів за допомогою команд **show etherchannel, show etherchannel summary, show etherchannel port-channel, show etherchannel load-balance, show lacp / show pagp neighbor, show interfaces port-channel, show ppp multilink, show interfaces multilink, show interfaces trunk**.

9. Дослідити відмовостійкість агрегованих каналів: по черзі відключати один з фізичних інтерфейсів кожного агрегованого каналу (команда **shutdown**) і спостерігати за станом каналу за допомогою команд **show etherchannel summary, show ppp multilink**. Переконатися, що зв'язність між пристроями зберігається. Поновити інтерфейс командою **no shutdown**.

10. Вивести та проаналізувати файли конфігурацій усіх комунікаційних пристроїв мережі (**show running-config**).

11. У випадку виявлення помилок у налагодженнях – визначити причину та усунути їх.

12. Продемонструвати виконану роботу керівнику практики та оформити звіт за заняттям.

ВАРІАНТИ ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

Варіант визначається за номером стійки, за якою працюють студенти, та номером класу, у якому виконуються завдання. Номери груп Port-channel (Po) обираються студентом самостійно з урахуванням обмежень платформи (на Catalyst 2960 – від 1 до 6).

Таблиця 1.3.

Параметри налагодження агрегованих каналів та мультилінку PPP

№ в-та	R2–SW2 (Static)	SW1–SW2 (PAGP)	SW2–SW3 (LACP)	R1–R2 (MLPPP)	Автентифікація MLPPP
1	ON / ON	desirable / desirable	active / active	V.35 DCE/DTE	PAP
2	ON / ON	desirable / auto	active / passive	RJ-48	CHAP
3	ON / ON	auto / desirable	passive / active	V.35 DCE/DTE	PAP
4	ON / ON	desirable / desirable	active / active	RJ-48	CHAP
5	ON / ON	desirable / auto	active / passive	V.35 DCE/DTE	PAP
6	ON / ON	auto / desirable	passive / active	RJ-48	CHAP
7	ON / ON	desirable / desirable	active / active	V.35 DCE/DTE	PAP
8	ON / ON	desirable / auto	active / passive	RJ-48	CHAP
9	ON / ON	auto / desirable	passive / active	V.35 DCE/DTE	PAP
10	ON / ON	desirable / desirable	active / active	RJ-48	CHAP
11	ON / ON	desirable / auto	active / passive	V.35 DCE/DTE	PAP
12	ON / ON	auto / desirable	passive / active	RJ-48	CHAP
13	ON / ON	desirable / desirable	active / active	V.35 DCE/DTE	PAP
14	ON / ON	desirable / auto	active / passive	RJ-48	CHAP
15	ON / ON	auto / desirable	passive / active	V.35 DCE/DTE	PAP
16	ON / ON	desirable / desirable	active / active	RJ-48	CHAP
17	ON / ON	desirable / auto	active / passive	V.35 DCE/DTE	PAP
18	ON / ON	auto / desirable	passive / active	RJ-48	CHAP
19	ON / ON	desirable / desirable	active / active	V.35 DCE/DTE	PAP
20	ON / ON	desirable / auto	active / passive	RJ-48	CHAP

Примітка: Позначення режимів протоколу PAgP: **desirable** – активний режим ініціації агрегації; **auto** – пасивний режим. Позначення режимів протоколу LACP: **active** – активний режим ініціації агрегації; **passive** – пасивний режим. Для автентифікації MLPPP використовуються протоколи **PAP** (Password Authentication Protocol) або **CHAP** (Challenge Handshake Authentication Protocol). Ім'я користувача та пароль автентифікації обираються студентом самостійно.

Таблиця 1.4.

Параметри налагодження методів балансування навантаження

№ варіанта	SW1 (PAGP-канал)	SW2 (усі канали)	SW3 (LACP-канал)
1	dst-mac	src-ip	dst-mac
2	src-mac	dst-mac	dst-ip
3	dst-ip	dst-ip	src-mac
4	src-mac	dst-mac	src-ip
5	dst-mac	src-ip	dst-mac
6	dst-ip	dst-ip	src-mac
7	src-ip	src-mac	dst-mac
8	dst-mac	dst-mac	dst-ip
9	src-ip	src-ip	src-ip
10	dst-mac	dst-ip	dst-ip
11	dst-ip	dst-mac	dst-mac
12	dst-mac	src-mac	src-ip
13	src-mac	dst-ip	src-mac
14	dst-ip	src-ip	dst-mac
15	src-mac	dst-mac	src-mac
16	src-ip	src-mac	dst-ip
17	dst-ip	dst-ip	dst-mac
18	src-mac	src-ip	dst-ip
19	src-ip	dst-mac	src-ip
20	src-mac	src-mac	dst-mac

Таблиця 1.5.

Параметри IP-адресації мережі

№ варіанта	IP-адреса мережі LAN-A	Префікс	IP-адреса шлюзу за замовчуванням/	IP-адреса мережі між В (MLPPP)
1	191.C.S.0	/24	Перша IP-адреса діапазону	172.C.S.0 /30
2	192.C.S.0	/25	Остання IP-адреса діапазону	172.C.S.4 /30
3	193.C.S.0	/26	Перша IP-адреса діапазону	172.C.S.8 /30
4	194.C.S.0	/27	Остання IP-адреса діапазону	172.C.S.12 /30
5	195.C.S.0	/28	Перша IP-адреса діапазону	172.C.S.16 /30
6	196.C.S.0	/24	Остання IP-адреса діапазону	172.C.S.20 /30
7	197.C.S.0	/25	Перша IP-адреса діапазону	172.C.S.24 /30
8	198.C.S.0	/26	Остання IP-адреса діапазону	172.C.S.28 /30
9	199.C.S.0	/27	Перша IP-адреса діапазону	172.C.S.32 /30
10	200.C.S.0	/28	Остання IP-адреса діапазону	172.C.S.36 /30
11	201.C.S.0	/24	Перша IP-адреса діапазону	172.C.S.40 /30
12	202.C.S.0	/25	Остання IP-адреса діапазону	172.C.S.44 /30
13	203.C.S.0	/26	Перша IP-адреса діапазону	172.C.S.48 /30
14	204.C.S.0	/27	Остання IP-адреса діапазону	172.C.S.52 /30
15	205.C.S.0	/28	Перша IP-адреса діапазону	172.C.S.56 /30
16	206.C.S.0	/24	Остання IP-адреса діапазону	172.C.S.60 /30
17	207.C.S.0	/25	Перша IP-адреса діапазону	172.C.S.64 /30
18	208.C.S.0	/26	Остання IP-адреса діапазону	172.C.S.68 /30
19	209.C.S.0	/27	Перша IP-адреса діапазону	172.C.S.72 /30
20	210.C.S.0	/28	Остання IP-адреса діапазону	172.C.S.76 /30

Примітка: С (class) – номер аудиторії: для ауд. 107 – 71, для ауд. 107а – 72, S (stand) – номер стійки (зазначено зверху стійки).

УВАГА! В залежності від години проведення практики значення може змінюватись за вимогою керівника.

ЗМІСТ ЗВІТУ З ЗАНЯТТЯ

Звіт з заняття повинен містити:

1. Номер, тему та мету заняття.
2. Короткі теоретичні відомості (за власним конспектом, обсягом 2–3 сторінки) з наступних питань: агрегація каналів у локальних мережах, EtherChannel, протоколи LACP та PAgP, режими налагодження агрегованих каналів, методи балансування навантаження, агрегація каналів у глобальних мережах, протокол Multilink PPP, протоколи автентифікації PPP (PAP, CHAP).
3. Перелік використаного обладнання та програмного забезпечення.
4. Схему (ФОТО) побудованої мережі з позначенням усіх пристроїв (R_ПІБ_1, R_ПІБ_2, SW_ПІБ_1, SW_ПІБ_2, SW_ПІБ_3) та інтерфейсів, через які виконано з'єднання.
5. Розроблену схему IP-адресації у вигляді табл. 1.1 (з конкретними значеннями IP-адрес, масок та префіксів) та представленими розрахунками.
6. Лістинги команд (або скріншоти термінального вікна) з результатами виконання для кожного з підзавдань 3–7, а саме:
 - налагодження статичного EtherChannel (R2–SW2);
 - налагодження динамічного PAgP-каналу (SW1–SW2);
 - налагодження динамічного LACP-каналу (SW2–SW3);
 - налагодження методу балансування навантаження;
 - Таблицю розподілу трафіку між фізичними каналами;
 - налагодження Multilink PPP (R1–R2);
 - налагодження IP-адресації пристроїв;
 - Результати перевірки працездатності мережі (вивід команд **ping**, **tracert**) між робочими станціями та до маршрутизаторів;
 - Вивід та аналіз результатів команд діагностики: **show etherchannel summary** (для SW1, SW2, SW3), **show etherchannel port-channel**, **show etherchannel load-balance**, **show lacp neighbor**, **show pagp neighbor**, **show ppp multilink**, **show interfaces multilink**, **show interfaces trunk**.
 - Результати дослідження відмовостійкості агрегованих каналів: вивід команд до та після відключення одного з фізичних інтерфейсів кожного каналу.
7. Опис проблем, що виникли під час виконання завдання, та шляхи їх усунення.
8. Висновки по заняттю.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Загальні відомості про агрегацію каналів

Агрегація каналів (англ. *link aggregation*) – технологія об'єднання декількох фізичних мережних інтерфейсів в один логічний канал з метою збільшення пропускної здатності та/або підвищення відмовостійкості з'єднання. Логічний агрегований інтерфейс функціонує як єдиний канал зв'язку, прозора для протоколів вищих рівнів моделі OSI.

Технологія агрегації каналів стандартизована у документах IEEE 802.1AX (раніше IEEE 802.3ad). На обладнанні Cisco агреговані канали між пристроями

прийнято називати **EtherChannel** (10BaseT/F), Fast EtherChannel (FEC, 100BaseTX/FX), Gigabit EtherChannel (GEC, 1000BaseT/FX). Незалежно від технології та методу агрегації, статичні та динамічні канали узагальнено називають **EtherChannel**.

Основними перевагами агрегації каналів порівняно із використанням одного фізичного з'єднання є:

- **збільшення пропускну́ї здатності** – пропускна здатність логічного інтерфейсу дорівнює сумі пропускну́х здатностей усіх фізичних інтерфейсів, що входять до його складу (до 8 або 16 активних каналів залежно від протоколу);
- **відмовостійкість** – у разі виходу з ладу одного або декількох фізичних каналів, решта продовжують передавати трафік без перерви зв'язку та без перенастроювання мережного обладнання;
- **балансування навантаження** – трафік розподіляється між фізичними каналами за одним із кількох алгоритмів, що дозволяє рівномірно завантажувати всі ланки агрегованого з'єднання;
- **прозорість для протоколів STP** – агрегований канал сприймається протоколом STP (Spanning Tree Protocol) як єдиний логічний зв'язок, що запобігає формуванню петель і дозволяє одночасно задіяти всі фізичні лінки.

Статичне агрегування (режим ON)

Статичне агрегування каналів виконується без застосування протоколів узгодження. Обидва кінці каналу налаштовуються у режимі **ON**, що означає безумовне об'єднання зазначених фізичних інтерфейсів у логічний канал EtherChannel незалежно від стану або налаштувань партнера.

Переваги статичного агрегування:

- відсутність додаткової затримки при активації каналу або зміні його налаштувань;
- простота реалізації – не потребує підтримки спеціальних протоколів обома сторонами;
- рекомендується компанією Cisco для з'єднань між комутатором та маршрутизатором (L3-пристроєм).

Недоліки статичного агрегування:

- відсутнє узгодження налаштувань із віддаленою стороною;
- помилки в налаштуванні можуть призвести до утворення петель у мережі;
- відсутня підтримка режиму "гарячого резерву" (standby) для інтерфейсів.

Протокол PAgP (Port Aggregation Protocol)

PAgP (Port Aggregation Protocol) – фірмовий протокол Cisco для динамічного узгодження агрегованих каналів. Протокол обмінюється пакетами PAgP між сусідніми пристроями для узгодження параметрів та автоматичного формування агрегованого каналу. PAgP підтримується лише на обладнанні Cisco і не може використовуватися для з'єднання з пристроями інших виробників.

Протокол PAgP підтримує два режими роботи:

- **desirable** (активний) – пристрій активно надсилає пакети PAgP до сусіда та ініціює формування агрегованого каналу;
- **auto** (пасивний) – пристрій не надсилає пакети PAgP першим, але відповідає на пакети PAgP від сусіда.

Агрегований канал на базі PAgP сформується лише при таких комбінаціях режимів: **desirable–desirable** або **desirable–auto**. Комбінація **auto–auto** не призводить до формування каналу, оскільки обидві сторони очікують ініціативи від партнера.

Протокол LACP (Link Aggregation Control Protocol)

LACP (Link Aggregation Control Protocol) – відкритий стандартний протокол агрегації каналів, визначений у стандарті IEEE 802.3ad (зараз IEEE 802.1AX). На відміну від PAgP, LACP є міжвендорним і підтримується обладнанням різних виробників, що робить його пріоритетним вибором у гетерогенних мережах.

Протокол LACP підтримує два режими роботи:

- **active** (активний) – пристрій ініціює надсилання LACPDU (LACP Data Unit) та активно формує агрегований канал;
- **passive** (пасивний) – пристрій відповідає на LACPDU від сусіда, але сам їх не ініціює.

Агрегований канал на базі LACP сформується при комбінаціях: **active–active** або **active–passive**. Комбінація **passive–passive** не призводить до формування каналу.

Суттєвою перевагою LACP є підтримка режиму **standby-інтерфейсів**: протокол дозволяє долучати до групи до 16 фізичних портів, з яких 8 будуть активними, а решта – перебувають у режимі гарячого резерву. У разі відмови активного порту один зі standby-портів автоматично переходить в активний режим.

Порівняння комбінацій режимів протоколів PAgP та LACP наведено в таблиці 1.6.

Таблиця 1.6.

Комбінації режимів PAgP і LACP, при яких формується EtherChannel

Протокол PAgP	auto	desirable	Протокол LACP	passive	active
auto	–	+	passive	–	+
desirable	+	+	active	+	+

Вимоги до фізичних інтерфейсів EtherChannel

Для успішного формування агрегованого каналу EtherChannel усі фізичні інтерфейси, що входять до його складу, повинні мати однакові налаштування:

- швидкість (speed) та режим дуплексу (duplex);
- режим доступу або транкінгу (access/trunk) та VLAN, що передаються;
- MTU;
- налаштування native VLAN для транкових портів.

Порушення будь-якої з цих вимог призводить до відмови у формуванні EtherChannel або нестабільної роботи каналу.

Методи балансування навантаження EtherChannel

Механізм балансування навантаження (load balancing) визначає, по якому з фізичних каналів EtherChannel передаватиметься конкретний кадр або пакет. Балансування виконується на рівні потоку (flow-based), тобто всі пакети одного потоку завжди передаються через один і той самий фізичний канал, що гарантує доставку без зміни порядку пакетів у межах потоку.

Вибір фізичного інтерфейсу здійснюється за хеш-функцією від значення обраного ключового поля. Результат хешування дозволяє обчислити індекс (0 або 1 при двох каналах, 0–3 при чотирьох тощо) за формулою: молодші N біт хешу (де $2^N \geq$ кількість фізичних каналів) визначають номер інтерфейсу.

На комутаторах Cisco Catalyst підтримуються методи балансування навантаження наведені в таблиці 1.7.

Таблиця 1.7.

Основні методи балансування навантаження EtherChannel на комутаторах Cisco

Метод	Опис
src-mac	На основі MAC-адреси відправника кадру
dst-mac	На основі MAC-адреси отримувача кадру
src-dst-mac	XOR MAC-адрес відправника та отримувача
src-ip	На основі IP-адреси відправника пакету
dst-ip	На основі IP-адреси отримувача пакету
src-dst-ip	XOR IP-адрес відправника та отримувача
src-port	На основі номера TCP/UDP-порту відправника
dst-port	На основі номера TCP/UDP-порту отримувача
src-dst-port	XOR номерів TCP/UDP-портів відправника та отримувача

Алгоритм розрахунку вибору фізичного інтерфейсу для методів на основі одного поля (src-mac, dst-ip тощо):

- взяти значення ключового поля (MAC або IP-адреса) у двійковому форматі;
- виділити молодші N біт ($N = \log_2(\text{кількість каналів})$);
- отримане двійкове число є індексом фізичного інтерфейсу.

Для методів з XOR (src-dst-mac, src-dst-ip, src-dst-port) спочатку виконується операція побітового XOR відповідних полів відправника та отримувача, після чого беруться молодші N біти результату.

Налагодження EtherChannel на обладнанні Cisco

Порядок налаштування агрегованих каналів EtherChannel на комутаторах Cisco складається з кількох кроків:

1. Вибрати групу фізичних інтерфейсів, що входять до логічного каналу.
2. Вимкнути вибрані інтерфейси командою **shutdown**.
3. Об'єднати інтерфейси у логічний канал та задати номер групи командою **channel-group [номер] mode [режим]**.

4. Налаштувати метод балансування навантаження командою **port-channel load-balance [метод]** (глобальна команда).
5. Повторити аналогічні кроки на протилежній стороні каналу.
6. Увімкнути інтерфейси командою **no shutdown** та перевірити стан каналу.

Для пристроїв третього рівня (маршрутизаторів або L3-комутаторів) логічний інтерфейс **port-channel** необхідно створювати вручну командою:

```
...
Router(config)# interface port-channel number
Router(config-if)# ip address IP_address network_mask
Router(config-if)# no shutdown
...
```

На комутаторах логічний інтерфейс **port-channel** створюється автоматично командою **channel-group**. Основний синтаксис команди:

```
channel-group [номер] mode { on | desirable [non-silent] | auto [non-silent] | active | passive }
```

де **group-number** – номер групи портів (номер логічного каналу), що створюється на пристрої, номери груп можуть не збігатися на різних сторонах логічного каналу;

mode – службова конструкція, за допомогою якої встановлюється варіант агрегації;

auto / desirable – увімкнути підтримку протоколу PAgP;

on – увімкнути статичну агрегацію EtherChannel;

active / passive – увімкнути підтримку протоколу LACP;

non-silent – службова конструкція, яка зазначає активацію у випадку, коли дані отримано з іншого кінця каналу.

Команда **port-channel load-balance** задається у режимі глобального конфігурування і застосовується до всіх агрегованих каналів пристрою:

```
...
Switch(config)# port-channel load-balance method
...
```

Команди моніторингу та діагностики EtherChannel

Для перегляду стану та параметрів агрегованих каналів EtherChannel використовуються команди діагностики представлені у таблиці 1.8.

Таблиця 1.8.

Команди діагностики EtherChannel, LACP та PAgP

Команда	Призначення
show etherchannel	Загальна інформація про всі агреговані канали пристрою
show etherchannel summary	Зведена таблиця стану агрегованих каналів і їх фізичних складових
show etherchannel port-channel	Детальна інформація про логічні port-channel інтерфейси
show etherchannel load-balance	Метод балансування навантаження, застосований на пристрої
show interfaces port-channel	Інформація про логічний інтерфейс port-channel

Команда	Призначення
show lacp neighbor	Параметри сусіднього пристрою за протоколом LACP
show lacp internal	Параметри LACP локального пристрою
show lacp counters	Лічильники LACP-повідомлень
show pagp neighbor	Параметри сусіднього пристрою за протоколом PAgP
show pagp internal	Параметри PAgP локального пристрою
show interfaces trunk	Параметри транкових з'єднань, у т.ч. агрегованих
show mac-address-table interface port-channel	Таблиця MAC-адрес для порту port-channel

Загальні відомості про протокол Point-to-Point (PPP)

PPP (Point-to-Point Protocol) – стандартний протокол канального рівня для встановлення прямих з'єднань між двома вузлами мережі. Визначений у документах RFC 1661, RFC 1662 та ряді доповнень. PPP широко застосовується на послідовних WAN-каналах (V.35, T1/E1) та замінив застарілий протокол HDLC як більш функціональний і гнучкий аналог.

Архітектура PPP включає такі підпротоколи:

- **LCP** (Link Control Protocol) – відповідає за встановлення, конфігурацію, тестування та завершення PPP-з'єднання. LCP узгоджує параметри з'єднання (MTU, стиснення, автентифікацію) перед передачею даних.
- **NCP** (Network Control Protocol) – сімейство протоколів для передачі через PPP-з'єднання пакетів різних мережних протоколів. Для передачі IP-пакетів використовується IPCP (Internet Protocol Control Protocol).
- **Протоколи автентифікації** – PAP та CHAP, що дозволяють перевірити справжність сторін з'єднання.

Процес встановлення PPP-з'єднання складається з трьох фаз:

- **Фаза LCP** – встановлення та узгодження параметрів каналу;
- **Фаза автентифікації** – перевірка справжності (за наявності конфігурації);
- **Фаза NCP** – узгодження параметрів мережного протоколу та початок передачі даних.

Протокол автентифікації PAP (Password Authentication Protocol)

PAP (Password Authentication Protocol) – простий протокол автентифікації у два кроки, визначений у RFC 1334. При використанні PAP клієнт надсилає своє ім'я та пароль у відкритому (незашифрованому) вигляді, а сервер порівнює ці дані зі своєю базою даних та надсилає у відповідь підтвердження або відмову.

Процес автентифікації за протоколом PAP:

- Клієнт надсилає пакет **Authenticate-Request** з іменем та паролем у відкритому вигляді;
- Сервер перевіряє отримані дані. При збігу надсилає **Authenticate-Ack**, при невідповідності – **Authenticate-Nak**.

Недолік PAP – передача пароля у відкритому вигляді, що робить його вразливим до перехоплення. Проте PAP може використовуватись у разі, коли система аутентифікації партнера не підтримує CHAP.

Протокол автентифікації CHAP (Challenge Handshake Authentication Protocol)

CHAP (Challenge Handshake Authentication Protocol) – більш захищений протокол автентифікації, визначений у RFC 1994. CHAP використовує трьохетапний механізм **challenge-response** та ніколи не передає пароль у явному вигляді. Замість цього пароль використовується лише для обчислення криптографічного хешу.

Процес автентифікації за протоколом CHAP:

- Аутентифікатор надсилає клієнту пакет Challenge з випадковим числом (challenge value) та своїм іменем;
- Клієнт обчислює значення response – MD5-хеш від конкатенації ID пакету, спільного секрету та challenge value;
- Клієнт надсилає пакет Response з обчисленим хешем та своїм іменем;
- Аутентифікатор самостійно обчислює очікуваний хеш та порівнює його з отриманим. При збігу надсилає **Success**, при розбіжності – **Failure**.

Ключові переваги CHAP над PAP:

- Пароль ніколи не передається відкритим текстом;
- Аутентифікація може повторюватися через довільні проміжки часу протягом сесії;
- Використання MD5-хешування забезпечує захист від атак відтворення (replay attack).

Налаштування автентифікації PAP та CHAP на маршрутизаторах Cisco:

Загальні команди для обох протоколів:

```
...  
Router(config)# username name-string password password  
Router(config)# interface interface-type interface-id  
Router(config-if)# encapsulation ppp  
...
```

Для PAP:

```
...  
Router(config-if)# ppp authentication pap  
Router(config-if)# ppp pap sent-username name-string password password  
...
```

Для CHAP:

```
...  
Router(config-if)# ppp authentication chap  
...
```

Концепція та призначення Multilink PPP

Multilink PPP (MLPPP, RFC 1990) – розширення протоколу PPP, що дозволяє об'єднувати декілька фізичних послідовних каналів в один логічний канал типу **Multilink** з метою збільшення сумарної пропускної здатності WAN-з'єднання та підвищення його відмовостійкості. MLPPP є аналогом EtherChannel для послідовних WAN-з'єднань між маршрутизаторами.

Принцип роботи Multilink PPP полягає у фрагментації вихідних пакетів та їхньому паралельному розподілі між фізичними каналами групи. На стороні отримувача фрагменти збираються у вихідний пакет у правильному порядку. Механізм нумерації фрагментів та порядковий номер у заголовку MLPPP забезпечують коректне складання навіть при різних затримках у фізичних каналах.

На відміну від EtherChannel, де трафік розподіляється на рівні кадрів або пакетів цілком, MLPPP розподіляє фрагменти одного пакета між різними каналами, що забезпечує краще балансування та нижчу затримку навіть при передачі великих пакетів.

Структура кадру Multilink PPP

Кадр Multilink PPP містить стандартний заголовок PPP з додатковим заголовком MLPPP. Заголовок MLPPP включає:

- **Sequence Number** (24 або 12 біт) – порядковий номер фрагмента, що забезпечує правильне складання пакета;
- **Bit B** (Begin) – встановлюється для першого фрагмента пакета;
- **Bit E** (End) – встановлюється для останнього фрагмента пакета;
- **Клас** – ідентифікатор черги для підтримки QoS (у розширених реалізаціях).

Налаштування Multilink PPP на маршрутизаторах Cisco

Для налаштування MLPPP на маршрутизаторі Cisco необхідно виконати такі кроки:

1. Створити логічний інтерфейс **Multilink** та призначити йому IP-адресу;
2. Налаштувати протокол PPP на фізичних послідовних інтерфейсах (encapsulation ppp);
3. Активувати підтримку multilink на фізичних інтерфейсах та включити їх у відповідну групу;
4. Налаштувати автентифікацію PAP або CHAP (за необхідності);
5. На DCE-стороні задати тактову частоту (clock rate).

Типовий сценарій налаштування MLPPP між Router1 (DCE) та Router2 (DTE):

```
Router1 (DCE-сторона)
```

```
...
```

```
Router1(config)# username Router_2 password Cisco123
```

```
Router1(config)# interface Multilink 1
```

```
Router1(config-if)# ip address 172.16.1.1 255.255.255.252
```

```
Router1(config-if)# ppp multilink
Router1(config-if)# ppp multilink group 1
Router1(config-if)# no shutdown
Router1(config-if)# exit
Router1(config)# interface Serial 0/0/0
Router1(config-if)# clock rate 64000
Router1(config-if)# encapsulation ppp
Router1(config-if)# ppp authentication chap
Router1(config-if)# ppp multilink
Router1(config-if)# ppp multilink group 1
Router1(config-if)# no shutdown
Router1(config-if)# exit
Router1(config)# interface Serial 0/0/1
Router1(config-if)# clock rate 64000
Router1(config-if)# encapsulation ppp
Router1(config-if)# ppp authentication chap
Router1(config-if)# ppp multilink
Router1(config-if)# ppp multilink group 1
Router1(config-if)# no shutdown
```

...

Router2 (DTE-сторона)

...

```
Router2(config)# username Router_1 password Cisco123
Router2(config)# interface Multilink 1
Router2(config-if)# ip address 172.16.1.2 255.255.255.252
Router2(config-if)# ppp multilink
Router2(config-if)# ppp multilink group 1
Router2(config-if)# no shutdown
Router2(config-if)# exit
Router2(config)# interface Serial 0/0/0
Router2(config-if)# encapsulation ppp
Router2(config-if)# ppp authentication chap
Router2(config-if)# ppp multilink
Router2(config-if)# ppp multilink group 1
Router2(config-if)# no shutdown
```

...

Команди моніторингу та діагностики Multilink PPP

Для моніторингу та діагностики MLPPP-з'єднань на маршрутизаторах Cisco застосовуються команди наведені у таблиця 1.9.

Таблиця 1.9.

Команди діагностики Multilink PPP

Команда	Призначення
show ppp multilink	Загальна інформація про MLPPP-групи та їх члени
show ppp multilink active	Активні MLPPP-з'єднання
show ppp multilink interface Multilink	Детальна інформація про конкретний Multilink-інтерфейс
show interfaces Multilink	Стан та статистика Multilink-інтерфейсу
show interfaces Serial	Стан та статистика фізичного послідовного інтерфейсу
show controllers Serial	Визначення ролі інтерфейсу (DCE/DTE) та тактова частота
debug ppp negotiation	Відстеження процесу узгодження PPP (LCP/NCP)
debug ppp authentication	Відстеження процесу автентифікації PAP/CHAP

Відмовостійкість Multilink PPP

Multilink PPP забезпечує автоматичну відмовостійкість: при виході з ладу одного або декількох фізичних каналів групи маршрутизатор автоматично продовжує передачу через інтерфейси, що залишились активними. Логічний Multilink-інтерфейс залишається у стані "up" доти, доки принаймні один фізичний канал групи є активним.

На відміну від EtherChannel, в MLPPP немає окремого механізму "standby"-портів, проте будь-який активний послідовний інтерфейс, що входить до групи, рівноправно бере участь у передачі трафіку. При відновленні відключеного інтерфейсу він автоматично повертається у групу та починає брати участь у передачі даних.

Ролі DCE та DTE у послідовних каналах

У послідовних двоточкових каналах кожен з пристроїв виконує одну з двох ролей:

- **DCE** (Data Communication Equipment) – відповідає за синхронізацію каналу. Саме DCE-пристрій задає тактову частоту передачі командою `clock rate`. У реальній мережі функцію DCE виконує обладнання провайдера або перетворювачі (CSU/DSU).

- **DTE** (Data Terminal Equipment) – кінцевий пристрій, що підключається до каналу. Маршрутизатор-DTE отримує тактові імпульси від DCE-пристрою.

В навчальних стендах роль DCE та DTE визначається типом кабелю (V.35 DCE або DTE). Команда **show controllers interface-type interface-id** дозволяє визначити роль інтерфейсу (виводить рядок "DCE" або "DTE").

Стандарти послідовних інтерфейсів

Для з'єднання послідовних каналів між маршрутизаторами Cisco використовуються кабелі наступних стандартів: V.35 (найпоширеніший у лабораторних стендах), X.21, EIA/TIA-232, EIA/TIA-449, EIA-530. У сучасних маршрутизаторах Cisco для WAN-з'єднань через плати розширення типу VWIC використовуються роз'єми RJ-48, що відповідають стандарту T1/E1 (ISDN BRI).

Протокол HDLC та перехід до PPP

За замовчуванням на послідовних інтерфейсах маршрутизаторів Cisco застосовується протокол **Cisco HDLC** – фірмова модифікація стандартного HDLC (High-Level Data Link Control). Cisco HDLC несумісний зі стандартним ISO HDLC та обладнанням інших виробників через додаткове поле типу протоколу в заголовку.

Для взаємодії маршрутизаторів різних виробників, а також для підтримки розширених можливостей (автентифікації, стиснення, multilink) необхідно перейти на протокол PPP командою:

```
...  
Router(config-if)# encapsulation ppp
```

```
...
```

Відмовостійкість агрегованих каналів та перевірка працездатності

Ключовою практичною перевагою агрегованих каналів є їхня відмовостійкість. Дослідження відмовостійкості виконується у такий спосіб:

- командою **shutdown** на одному з фізичних інтерфейсів агрегованого каналу імітується його відмова;
- за допомогою команд **show etherchannel summary** або **show ppp multilink** спостерігається новий стан каналу;
- командою **ping** перевіряється збереження зв'язності між кінцевими пристроями;
- командою **no shutdown** відновлюється відключений інтерфейс і підтверджується автоматичне повернення його до агрегованого каналу.

Команда **show etherchannel summary** у стовпці *Flags* відображає стан кожного фізичного інтерфейсу агрегованого каналу: **P** – інтерфейс активний (in bundle), **D** – інтерфейс не активний (down), **s** – у режимі standby (лише LACP).

Для перевірки наскрізного зв'язку між пристроями використовуються команди:

- **ping IP_address** – перевірка доступності вузла (ICMP Echo Request/Reply);
- **traceroute IP_address** – виведення повного маршруту проходження пакетів між вузлами, включно з усіма проміжними маршрутизаторами.

Рекомендована послідовність перевірки роботи EtherChannel і Multilink PPP

Рекомендована послідовність перевірки після завершення налаштування наведена нижче. Для кожної команди показано характерний вивід та пояснення ключових полів.

1. Перевірка стану EtherChannel.

```
Switch# show etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

Number of channel-groups in use: 1
Number of aggregators:          1
Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)          LACP        Fa0/1(P)  Fa0/2(P)
```

У стовпці Port-channel – стан агрегованого інтерфейсу: **(SU)** – Layer 2, in use (працює); **(SD)** – down. У дужках біля портів-членів: **(P)** – bundled (повноцінно входить у канал); **(I)** – stand-alone (виключений з каналу через несумісні режими); **(s)** – suspended (виключений через розбіжність параметрів). Стовпець Protocol – LACP або PAgP. Якщо колонка порожня – використовується статичний режим (**channel-group ... mode on**).

2. Деталізація переговорів LACP / PAgP.

```
Switch# show etherchannel detail
          Channel-group listing:
          -----
Group: 1
-----
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
Ports in the group:
-----
Port: Fa0/1
-----
Port state   = Up Mstr Assoc In-Bndl
Channel group = 1   Mode = Active
LACP Pdup sent: 23   LACP Pdup received: 22
```

Рядок «Port state = Up Mstr Assoc In-Bndl» свідчить про коректне включення інтерфейсу у канал. Якщо «Not-In-Bndl» – інтерфейс не зміг увійти. Лічильники LACP Pdup sent/received повинні зростати – якщо received залишається 0, на іншому боці LACP не налагоджено або порти у режимі passive з обох сторін.

3. Перевірка Multilink PPP.

```
Router# show ppp multilink

Multilink1, bundle name is R-2
Bundle up for 00:15:32, total bandwidth 3072, load 1/255
Receive buffer limit 24000 bytes, frag timeout 1000 ms
  0/0 fragments/bytes in reassembly list
  0 lost fragments, 0 reordered
  0/0 discarded fragments/bytes, 0 lost received
  0x12 received sequence, 0x15 sent sequence
Member links: 2 active, 0 inactive (max 255, min not set)
```

```
Se0/0/0, since 00:15:32
Se0/0/1, since 00:15:30
```

Поле «total bandwidth» дорівнює сумі швидкостей усіх активних членів (для двох T1-каналів: 1536+1536=3072 кбіт/с). Рядок «Member links: 2 active» підтверджує, що обидва канали увійшли в bundle. Якщо одного з них немає у списку – перевірити **ppp multilink** і **ppp multilink group** на цьому інтерфейсі.

4. Перевірка стану і параметрів Multilink-інтерфейсу.

```
Router# show interface Multilink 1
Multilink1 is up, line protocol is up
  Hardware is multilink group interface
  Internet address is 10.0.0.1/30
  MTU 1500 bytes, BW 3072 Kbit/sec, DLY 1000000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open, multilink Open
  Open: IPCP, CDPCP, loopback not set
```

Стан up/up – multilink-інтерфейс активний. Поля LCP Open та multilink Open означають, що PPP-сесія встановлена і агрегація працює. «IPCP» – IP-протокол узгоджений, отже IP-адреса передається через канал. Якщо стан up/down – фізичні канали є, але PPP-узгодження не завершилося (перевірити **encapsulation ppp** на обох сторонах та збіжність аутентифікації, якщо налагоджена).

5. Перевірка зв'язності.

```
Router# ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/8/12 ms
```

Успішний **ping** (100%) підтверджує наскрізну зв'язність агрегованого каналу. Часткові втрати (наприклад, 80%) при двох активних членах bundle можуть свідчити про проблему з одним з фізичних каналів – потрібна перевірка лічильників помилок командою **show interfaces serial** для кожного фізичного інтерфейсу.

Типові помилки при налагодженні EtherChannel і Multilink PPP

1. **Несумісні режими LACP/PAgP на сторонах каналу.** Для успішного формування агрегованого каналу режими інтерфейсів на обох сторонах повинні бути сумісними. Сумісні комбінації для LACP: **active – active**, **active – passive**. Несумісна – **passive – passive** (жодна сторона не ініціює переговори). Для PAgP: **desirable – desirable**, **desirable – auto**. Несумісна – **auto – auto**. Найпоширеніша причина непрацюючого EtherChannel – обидва кінці у пасивному режимі. Перевіряти командою **show etherchannel summary** (стан SU – агрегований канал працює).

2. **Розбіжність параметрів інтерфейсів-членів каналу.** Усі фізичні інтерфейси, що включені в один port-channel, повинні мати **ідентичні параметри**: швидкість, дуплекс, режим (access/trunk), дозволені VLAN на trunk, native VLAN. Розбіжність хоча б одного параметра призводить до того, що інтерфейс виключається з каналу зі статусом **err-suspended**. Виправляти – або привести параметри до однакових, або тимчасово вимкнути проблемний інтерфейс командою **shutdown**.

3. **Спроба змішати LACP і PAgP в одному port-channel.** LACP (стандарт IEEE 802.3ad) і PAgP (фІРмовий протокол Cisco) **несумісні між собою**. На обох сторонах повинен бути той самий протокол. Помилка часто виникає при підключенні Cisco-обладнання до іншого виробника – там доступний лише LACP, тому з боку Cisco також потрібно встановити LACP-режими (active або passive).

4. **Відсутність clock rate на DCE-стороні Serial-каналу при Multilink PPP.** На послідовних з'єднаннях за технологією V.35 одна сторона є DCE (надає синхронізацію), інша – DTE. Якщо на DCE-стороні не задано команду **clock rate**, фізичний канал залишається у стані **up/down** (line protocol is down). Перевіряти командою **show controllers serial interface-id** – відображається «clockrate is unset» для DCE або фактичне значення для DTE.

5. **НевІРне налагодження multilink-групи.** Команда **ppp multilink group number** повинна бути виконана на **кожному** Serial-інтерфейсі, що входить до **multilink-bundle**. Номер групи – однаковий на всіх інтерфейсах одного маршрутизатора, але на іншій стороні каналу він може відрізнитися. Якщо команда не виконана на одному з інтерфейсів, цей канал не агрегується і працює окремо.

6. **Помилкова інкапсуляція PPP.** Multilink PPP працює лише поверх інкапсуляції PPP. Якщо на інтерфейсі залишилася стандартна інкапсуляція HDLC (за замовчуванням для Cisco Serial), агрегація не функціонує. Обов'язково встановити **encapsulation ppp** на обох сторонах кожного фізичного Serial-каналу.

7. **ІР-адреса задана на фізичному інтерфейсі замість Multilink-інтерфейсу.** При використанні Multilink PPP ІР-адреса повинна бути присвоєна **логічному інтерфейсу Multilink number**, а не фізичним Serial-інтерфейсам. На фізичних інтерфейсах ІР-адреси НЕ призначаються – вони лише включаються до multilink-групи.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке агрегація каналів? Які переваги вона забезпечує?
2. Чим відрізняється EtherChannel від Multilink PPP?
3. Які три режими налагодження EtherChannel існують?
4. Чим протокол PAgP відрізняється від LACP? Який з них є стандартом IEEE?
5. Які режими має протокол PAgP? Які комбінації дозволяють створення каналу?
6. Які режими має протокол LACP? Які комбінації дозволяють створення каналу?
7. Які вимоги до фізичних портів для об'єднання в EtherChannel?
8. Які методи балансування навантаження підтримуються в EtherChannel? Як обрати оптимальний?
9. Як працює алгоритм хешування при балансуванні навантаження в EtherChannel?
10. Якою командою на комутаторі Cisco створюється EtherChannel? Якою – на маршрутизаторі?
11. Що таке Multilink PPP? Для чого він застосовується?
12. Чим відрізняються протоколи автентифікації PAP та CHAP?
13. Якими командами можна перевірити стан EtherChannel?
14. Якими командами можна перевірити стан Multilink PPP?
15. Як забезпечується відмовостійкість агрегованих каналів?
16. Що відбувається з трафіком при відключенні одного з фізичних інтерфейсів EtherChannel?
17. Чому режим ON (статичний) вважається менш надійним за динамічні режими PAgP/LACP?