Лабораторна робота № 8
НАЛАГОДЖЕННЯ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ L2/L3 MPLS VPN У МЕРЕЖІ НА БАЗІ МАРШРУТИЗАТОРІВ CISCO

Мета заняття: налагодити функціонування технологій L2/L3 MPLS VPN у мережі на базі маршрутизаторів Cisco; отримати практичні навички налагодження VRF, протоколу розподілу міток LDP, протоколу MP-BGP та маршрутизації між граничними маршрутизаторами провайдера і клієнта; дослідити особливості побудови, маршрутизації та передачі даних у мережі MPLS з використанням механізмів VRF.

Теоретичні відомості

Загальні відомості про технологію MPLS

MPLS (Multiprotocol Label Switching) – технологія багатопротокольної комутації за мітками, у якій рішення про подальше пересилання пакета ухвалюється не за IP-адресою отримувача, а за значенням короткої мітки фіксованої довжини, доданої до пакета. Це дає змогу поєднати гнучкість мереж із комутацією пакетів із передбачуваністю віртуальних каналів, притаманною мережам із комутацією каналів.

Технологію називають багатопротокольною, оскільки вона не залежить ні від протоколу мережного рівня, пакети якого переносяться, ні від технології канального рівня, через яку передаються мічені пакети. Засобами MPLS можна передавати IP-пакети, кадри Ethernet, Frame Relay, комірки ATM тощо. Через своє розташування між заголовками канального та мережного рівнів заголовок MPLS часто називають заголовком «2,5 рівня».

Основними елементами технології MPLS є:

– **FEC** (Forwarding Equivalence Class) – клас еквівалентності пересилання, тобто група пакетів, які пересилаються однаково (одним шляхом і з однаковою обробкою), наприклад, усі пакети до певного IP-префікса;

– **LSR** (Label Switching Router) – маршрутизатор, що виконує комутацію пакетів за мітками;

– **LSP** (Label Switched Path) – шлях комутації за мітками, тобто послідовність LSR, через які проходить пакет певного FEC від входу до виходу MPLS-домену.

Серед маршрутизаторів MPLS-домену розрізняють:

– **граничні маршрутизатори провайдера** – E-LSR (LER, Label Edge Router), інша назва PE (Provider Edge). На вході в домен вони класифікують пакети за FEC і додають мітки, на виході – вилучають мітки. У L3 MPLS VPN саме на PE створюються VRF клієнтів;

– **транзитні маршрутизатори домену** – LSR, інша назва P (Provider). Вони комутують пакети лише за верхньою міткою і маршрутів клієнтів не мають.

Окрему групу становлять маршрутизатори клієнта – **CE** (Customer Edge). Вони обмінюються з PE звичайними IP-пакетами та маршрутною інформацією і MPLS не підтримують.

Заголовок MPLS складається з одного або кількох 32-бітних записів, які утворюють стек міток. Заголовок MPLS розміщується між заголовками канального та мережного рівнів (рис. 1). Кожен запис містить чотири поля:

– **Label** (20 біт) – значення мітки; діапазон 0–1 048 575, значення 0–15 зарезервовано для службових цілей;

– **TC** (Traffic Class, 3 біти; у ранніх документах – EXP) – клас трафіку для механізмів QoS (на рис. 1 – поле QoS);

– **S** (Bottom of Stack, 1 біт) – ознака останнього (нижнього) запису стеку;

– **TTL** (8 біт) – час життя пакета, аналог відповідного поля заголовка IP.

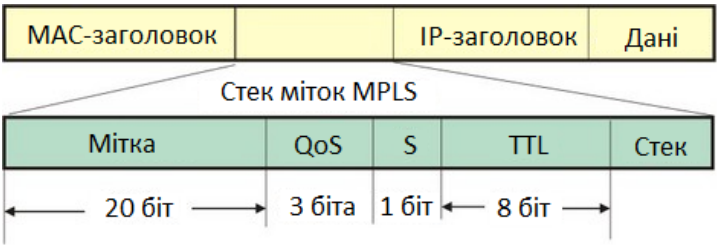


Рис. 1. Заголовок MPLS

Із мітками LSR виконує три базові операції: **push** – додавання мітки, **swap** – заміну верхньої мітки, **pop** – вилучення верхньої мітки. Ресурсомісткі дії (аналіз заголовка IP, класифікацію, фільтрацію) виконує лише вхідний E-LSR; транзитні LSR аналізують тільки верхню

мітку. За замовчуванням передостанній маршрутизатор LSP вилучає транспортну мітку (PHP, Penultimate Hop Popping), щоб вихідний E-LSR не виконував двох пошуків поспіль.

Для узгодження міток між сусідніми LSR використовують протокол **LDP** (Label Distribution Protocol). Кожен LSR призначає локальні мітки префіксам зі своєї таблиці маршрутизації та повідомляє їх LDP-сусідам. Прив'язки «FEC – мітка» зберігаються в таблиці LIB, а мітки, які фактично використовуються для пересилання, – у таблиці LFIB. LDP-сусіди виявляють один одного за допомогою UDP-повідомлень Hello на порт 646, після чого встановлюють сесію TCP (порт 646). Ідентифікатором LDP (LDP ID) зазвичай є IP-адреса інтерфейсу Loopback, тому вона має бути досяжною через протокол внутрішньої маршрутизації (IGP) провайдера.

Особливості технології L3 MPLS VPN

L3 MPLS VPN поєднує технологію MPLS із віртуальними таблицями маршрутизації VRF та розширенням протоколу BGP (MP-BGP). Ця технологія дає змогу провайдеру через одну спільну мережу з'єднувати територіально рознесені сайти багатьох клієнтів так, що маршрути й трафік різних клієнтів залишаються ізольованими.

VRF (Virtual Routing and Forwarding) – екземпляр таблиці маршрутизації та пересилання на маршрутизаторі PE, який належить конкретній VPN. Фактично VRF ділить один фізичний маршрутизатор на кілька незалежних віртуальних маршрутизаторів. До складу VRF входять: множина інтерфейсів, до яких підключено CE однієї VPN; окрема таблиця маршрутизації та таблиця CEF; правила імпорту й експорту маршрутів. Ім'я VRF має лише локальне значення в межах одного маршрутизатора, тому на різних PE одна й та сама VPN може мати різні імена VRF.

Кожен VRF характеризують два параметри:

– **RD** (Route Distinguisher) – 64-бітний розрізнювач маршрутів, який додається до IPv4-префікса і перетворює його на унікальний у мережі провайдера VPNv4-префікс (8 байт RD + 4 байти IPv4). Саме RD дозволяє клієнтам використовувати однакові адресні простори. На одному маршрутизаторі VRF може мати лише один RD;

– **RT** (Route Target) – розширений атрибут BGP (extended community), який додається до маршруту під час експорту з VRF і визначає, до яких VRF на інших PE цей маршрут буде імпортовано.

Різні комбінації RT дозволяють будувати як ізольовані VPN, так і топології з частковим обміном маршрутами (extranet, hub-and-spoke).

Маршрутами VPNv4 маршрутизатори PE обмінюються за допомогою **MP-BGP** (Multiprotocol BGP) – багатопротокольного розширення BGP із сімейством адрес VPNv4. Сесії MP-BGP встановлюються між інтерфейсами Loopback маршрутизаторів PE в межах однієї автономної системи провайдера (iBGP). На відміну від протоколів IGP, BGP надсилає оновлення лише явно заданим сусідам, які можуть розташовуватися за кілька переходів. Разом із VPNv4-префіксом MP-BGP передає VPN-мітку, призначену вихідним PE.

Отже, пакет VPN у мережі провайдера переноситься зі стеком із двох міток: верхня **транспортна мітка** (розподіляється LDP) доставляє пакет до вихідного PE, нижня **VPN-мітка** (розподіляється MP-BGP) вказує вихідному PE, до якого VRF і якого CE переслати пакет. Транзитні маршрутизатори P обробляють лише транспортну мітку, тому маршрути клієнтів на них не потрібні.

Між PE і CE може використовуватися статична маршрутизація або будь-який протокол маршрутизації (RIPv2, OSPF, EIGRP, eBGP). У цій роботі застосовано eBGP: кожен сайт клієнта має власний номер автономної системи, а PE встановлює з CE сесію eBGP у контексті відповідного VRF.

Основними перевагами L3 MPLS VPN є масштабованість, можливість перетину адресних просторів клієнтів, ізоляція маршрутної інформації та трафіку різних VPN, а також відсутність потреби в налагодженні тунелів між сайтами на боці клієнта.

Особливості технології L2 MPLS VPN

Для побудови VPN другого рівня за схемою «точка – точка» використовують технологію AToM (Any Transport over MPLS), яка забезпечує прозору передачу через MPLS-мережу кадрів протоколів другого рівня (Ethernet over MPLS, Frame Relay over MPLS, ATM over MPLS). Для клієнта канал EoMPLS виглядає як віртуальний «патч-корд» між двома сегментами мережі: L2 VPN не прив'язана до IP-адресації клієнта й працює на рівні кадрів Ethernet. На обладнанні Cisco такий канал (псевдопровід) налагоджують на інтерфейсах PE, до яких підключено клієнтів, командою **xconnect**, а його стан перевіряють командою **show mpls l2transport vc**.

Порядок налагодження L3 MPLS VPN на обладнанні Cisco

Налагодження L3 MPLS VPN складається з кількох етапів. Порядок їх виконання є таким:

1. Налагодити сайти клієнтів: VLAN і IP-адресацію комутаторів та робочих станцій, підінтерфейси та послідовні інтерфейси маршрутизаторів CE.

2. На маршрутизаторах P і PE створити інтерфейси Loopback з маскою /32 та налагодити IP-адресацію каналів ядра.

3. Налагодити протокол внутрішньої маршрутизації (IGP) у мережі провайдера, оголосивши в ньому канали ядра та адреси Loopback. Перевірити досяжність адрес Loopback.

4. Увімкнути MPLS на інтерфейсах ядра (на P – на всіх, на PE – лише на інтерфейсах до P). Перевірити встановлення сусідства LDP.

5. На кожному PE створити VRF для кожної VPN, задати RD і RT, прив'язати до VRF інтерфейси, до яких підключено CE, і повторно задати на них IP-адреси.

6. Налагодити сесію iBGP між PE через інтерфейси Loopback та активувати для неї сімейство адрес VPNv4.

7. Налагодити маршрутизацію між PE і CE: на PE – сесії eBGP у сімействах адрес ipv4 vrf, на CE – сесії eBGP з PE та оголошення мереж сайтів.

8. Перевірити таблиці маршрутизації VRF, таблицю VPNv4, таблиці міток і наскрізну досяжність сайтів кожної VPN.

Команди налагодження L3 MPLS VPN на маршрутизаторах Cisco

Для створення VRF використовують команду **ip vrf**, для задання його параметрів – команди **rd** і **route-target**, для прив'язки інтерфейсу до VRF – команду **ip vrf forwarding**. MPLS на інтерфейсах вмикають командою **mpls ip**. Обмін маршрутами VPN налагоджують у процесі BGP (команди **router bgp**, **neighbor**, **address-family**). Синтаксис команд та режими їх застосування наведено нижче.

Синтаксис команди ip vrf (режим глобального конфігурування):

ip vrf vrf-name,

де **vrf-name** – ім'я VRF, що створюється; має лише локальне значення і чутливе до регістру.

Синтаксис команди rd (режим конфігурування VRF):

rd route-distinguisher,

де **route-distinguisher** – розрізнювач маршрутів у форматі **ASN:nn** (номер автономної системи : число) або **A.B.C.D:nn** (IP-адреса : число), наприклад 65061:1 або 2:1.

Синтаксис команди route-target (режим конфігурування VRF):

route-target {import | export | both} route-target-ext-community,

де **import** – імпортувати у VRF маршрути з указаним RT; **export** – додавати вказаний RT до маршрутів, що експортуються з VRF; **both** – одночасно import та export; **route-target-ext-community** – значення RT у форматі, аналогічному RD. Команду route-target можна задати лише після команди rd.

Синтаксис команди ip vrf forwarding (режим конфігурування інтерфейсу):

ip vrf forwarding vrf-name,

де **vrf-name** – ім'я VRF, до якого прив'язується інтерфейс. Під час виконання команди IP-адреса з інтерфейсу видаляється, тому її потрібно задати повторно.

Синтаксис команд увімкнення та налагодження MPLS:

mpls ip

– вмикає комутацію за мітками та протокол розподілу міток на інтерфейсі (режим конфігурування інтерфейсу);

mpls label protocol ldp

– явно задає протокол розподілу міток LDP (глобально або на інтерфейсі; у сучасних версіях Cisco IOS LDP використовується за замовчуванням);

mpls ldp router-id interface [force]

– задає інтерфейс, адреса якого використовується як LDP ID (режим глобального конфігурування); параметр **force** змушує негайно змінити ідентифікатор;

mpls mtu bytes

– задає максимальний розмір міченого пакета на інтерфейсі; кожна мітка збільшує розмір пакета на 4 байти, тому для двох міток значення може бути збільшене до 1508 байт і більше (за потреби).

Синтаксис команд налагодження BGP для L3 MPLS VPN:

router bgp as-number

– запускає процес BGP автономної системи **as-number** (режим глобального конфігурування);

neighbor ip-address remote-as as-number
– задає сусіда BGP та номер його автономної системи; якщо номери AS збігаються, установлюється сесія iBGP, інакше – eBGP;

neighbor ip-address update-source interface
– задає інтерфейс (як правило, Loopback 0), адреса якого використовується як адреса джерела сесії iBGP;

address-family vpnv4 [unicast]
– перехід до налагодження сімейства адрес VPNv4 (режим конфігурування BGP);

neighbor ip-address activate
– дозволяє обмін маршрутами поточного сімейства адрес із сусідом;

neighbor ip-address send-community {standard | extended | both}
– дозволяє передавати сусіду атрибути community; для VPNv4 потрібні розширені атрибути (**extended**), у яких передаються значення RT;

address-family ipv4 vrf vrf-name
– перехід до налагодження сімейства адрес IPv4 в контексті VRF (сусіди CE задаються саме тут);

network network-number mask network-mask
– оголошення мережі в BGP; мережа має бути в таблиці маршрутизації з точно такою самою маскою, ключове слово **mask** обов'язкове, якщо маска відрізняється від класової;

redistribute {connected | static | ospf process-id | eigrp as-number | rip}
– перерозподіл у BGP маршрутів з інших джерел (альтернатива командам network).

Синтаксис команди створення псевдопроводу L2 MPLS VPN (режим конфігурування інтерфейсу):

xconnect peer-router-id vcid encapsulation mpls,
де **peer-router-id** – адреса Loopback віддаленого PE; **vcid** – ідентифікатор віртуального каналу, однаковий на обох кінцях.

Налагодження протоколів внутрішньої маршрутизації (RIPv2, OSPF, EIGRP) розглядалося в попередніх роботах. Для MPLS важливо, щоб адреси Loopback оголошувалися з маскою /32; для RIPv2 для цього слід задати команди **version 2** та **no auto-summary**.

Команди моніторингу та діагностики роботи MPLS та L3 MPLS VPN

Для перевірки налагоджень використовують як загальні команди (**show ip route**, **show running-config**, **ping**, **traceroute**), так і спеціалізовані команди, перелік яких наведено в табл. 1. Більшість команд, що стосуються VRF, мають параметр **vrf vrf-name**, без якого команда працює з глобальною таблицею маршрутизації.

Таблиця 1

Перелік команд діагностики роботи MPLS та L3 MPLS VPN на маршрутизаторах Cisco

Команда	Призначення
Команди діагностики роботи MPLS та LDP	
show mpls interfaces	Виведення інтерфейсів, на яких увімкнено MPLS, та їхнього стану
show mpls ldp neighbor	Виведення LDP-сусідів, стану сесій та адрес, що використовуються
show mpls ldp discovery	Виведення інформації про виявлення LDP-сусідів (повідомлення Hello)
show mpls ldp bindings	Виведення таблиці LIB: локальних і віддалених міток для кожного префікса
show mpls forwarding-table	Виведення таблиці LFIB: вхідна мітка, вихідна мітка або дія (Pop Label, No Label), вихідний інтерфейс, наступний перехід
debug mpls ldp …	Увімкнення режиму відлагодження LDP (наприклад, debug mpls ldp bindings – зміни прив'язок міток)
undebug all	Вимкнення всіх режимів відлагодження
Команди діагностики роботи VRF	
show ip vrf [brief | detail]	Виведення переліку VRF, їхніх RD, RT та інтерфейсів
show ip vrf interfaces	Виведення інтерфейсів, прив'язаних до VRF, та їхніх IP-адрес
show ip route vrf vrf-name	Виведення таблиці маршрутизації VRF
show ip cef vrf vrf-name prefix detail	Виведення запису CEF для префікса у VRF, зокрема стеку міток
ping vrf vrf-name ip-address	Перевірка зв'язку в контексті VRF
traceroute vrf vrf-name ip-address	Трасування маршруту в контексті VRF
Команди діагностики роботи BGP та MP-BGP	
show ip bgp summary	Виведення стану сесій BGP для IPv4 (зокрема на CE)
show ip bgp vpnv4 all summary	Виведення стану сесій VPNv4 між PE та сесій PE–CE у VRF
show ip bgp vpnv4 all	Виведення таблиці VPNv4-маршрутів, згрупованих за RD
show ip bgp vpnv4 vrf vrf-name	Виведення VPNv4-маршрутів окремого VRF

Команда	Призначення
show ip bgp vpnv4 all labels	Виведення VPN-міток (вхідних і вихідних), призначених префіксам
Команди діагностики роботи L2 MPLS VPN	
show mpls l2transport vc	Виведення стану псевдопроводів (віртуальних каналів) L2 MPLS VPN

Приклад налагодження функціонування мережі з використанням технології L3 MPLS VPN та маршрутизаторів Cisco

Розглянемо налагодження мережі провайдера, яка з'єднує два сайти одного клієнта (VPN A) через MPLS-домен (рис. 2). Приклад виконано у віртуальній мережевій лабораторії eve.ztu.edu.ua для G = 45 і N = 6. Мережа провайдера складається з двох граничних маршрутизаторів R-45-6-4-ELSR, R-45-6-6-ELSR (PE) та транзитного маршрутизатора R-45-6-5-LSR (P); як IGP використано EIGRP.

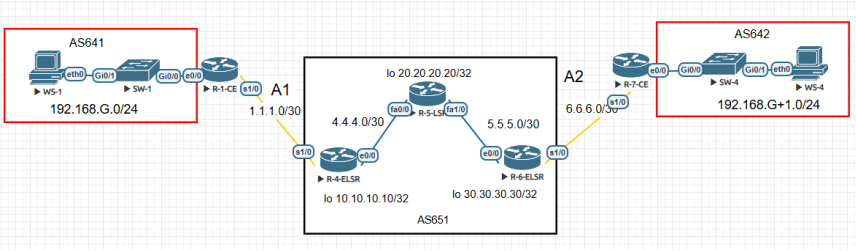


Рис. 2. Приклад мережі

Номери автономних систем сформовано за правилом, наведеним на рис. 7: значення G, G+1, G+2 та N беруться за останньою цифрою, а номер AS мережі провайдера не залежить від G (AS650N1). Для G = 45 і N = 6 сайт 1 має AS 64561, сайт 2 – AS 64562, мережа провайдера – AS 65061. На рис. 2 ці номери позначено скорочено. На обох PE для VPN A створено VRF (A1 на R-45-6-4-ELSR і A2 на R-45-6-6-ELSR) з однаковими RD і RT 2:1. Сесію iBGP (VPNv4) встановлено між адресами Loopback 0 маршрутизаторів PE – 10.10.10.10 і 30.30.30.30.

Під час побудови мережі для з'єднання пристроїв використано дані табл. 2. Для налагодження параметрів адресації пристроїв використано дані табл. 3.

Таблиця 2

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Інтерфейс сусіда	MPLS
Маршрутизатор R-45-6-1-CE	e0/0	Комутатор SW-45-6-1	Gi0/0	–
	s1/0	R-45-6-4-ELSR	s1/0	–
Маршрутизатор R-45-6-4-ELSR	s1/0 (VRF A1)	R-45-6-1-CE	s1/0	–
	e0/0	R-45-6-5-LSR	fa0/0	+

Пристрій	Інтерфейс	Підключення до пристрою	Інтерфейс сусіда	MPLS
Маршрутизатор R-45-6-5-LSR	fa0/0	R-45-6-4-ELSR	e0/0	+
	fa1/0	R-45-6-6-ELSR	e0/0	+
Маршрутизатор R-45-6-6-ELSR	e0/0	R-45-6-5-LSR	fa1/0	+
	s1/0 (VRF A2)	R-45-6-7-CE	s1/0	–
Маршрутизатор R-45-6-7-CE	s1/0	R-45-6-6-ELSR	s1/0	–
	e0/0	Комутатор SW-45-6-4	Gi0/0	–
Комутатор SW-45-6-1	Gi0/0 (trunk)	R-45-6-1-CE	e0/0	–
	Gi0/1 (access)	WS-1	eth0	–
Комутатор SW-45-6-4	Gi0/0 (trunk)	R-45-6-7-CE	e0/0	–
	Gi0/1 (access)	WS-4	eth0	–

Таблиця 3

Параметри адресації мережі для прикладу

Підмережа / пристрій	Інтерфейс / мережний адаптер / шлюз	IP-адреса	Маска підмережі	Префікс
Мережа сайту 1 VPN A	–	192.168.45.0	255.255.255.0	/24
Мережа сайту 2 VPN A	–	192.168.46.0	255.255.255.0	/24
Канал A1 (PE – CE)	–	1.1.1.0	255.255.255.252	/30
Канал A2 (PE – CE)	–	6.6.6.0	255.255.255.252	/30
Канали ядра	–	4.4.4.0, 5.5.5.0	255.255.255.252	/30
Маршрутизатор R-45-6-1-CE	Підінтерфейс e0/0.5 (VLAN 5)	192.168.45.254	255.255.255.0	/24
	Інтерфейс s1/0	1.1.1.2	255.255.255.252	/30
Маршрутизатор R-45-6-4-ELSR	Інтерфейс Loopback 0	10.10.10.10	255.255.255.255	/32
	Інтерфейс e0/0	4.4.4.2	255.255.255.252	/30
	Інтерфейс s1/0 (VRF A1)	1.1.1.1	255.255.255.252	/30
Маршрутизатор R-45-6-5-LSR	Інтерфейс Loopback 0	20.20.20.20	255.255.255.255	/32
	Інтерфейс fa0/0	4.4.4.1	255.255.255.252	/30
	Інтерфейс fa1/0	5.5.5.1	255.255.255.252	/30
Маршрутизатор R-45-6-6-ELSR	Інтерфейс Loopback 0	30.30.30.30	255.255.255.255	/32
	Інтерфейс e0/0	5.5.5.2	255.255.255.252	/30

Підмережа / пристрій	Інтерфейс / мережний адаптер / шлюз	IP-адреса	Маска підмережі	Префікс
	Інтерфейс s1/0 (VRF A2)	6.6.6.1	255.255.255.252	/30
Маршрутизатор R-45-6-7-CE	Інтерфейс s1/0	6.6.6.2	255.255.255.252	/30
	Підінтерфейс e0/0.7 (VLAN 7)	192.168.46.254	255.255.255.0	/24
Комутатор SW-45-6-1	Інтерфейс Vlan 5	192.168.45.253	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.45.254	–	–
Комутатор SW-45-6-4	Інтерфейс Vlan 7	192.168.46.253	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.46.254	–	–
Робоча станція WS-1	Мережний адаптер	192.168.45.1	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.45.254	–	–
Робоча станція WS-4	Мережний адаптер	192.168.46.1	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.46.254	–	–

Сценарії налагодження параметрів адресації інтерфейсів, протоколів маршрутизації, MPLS, VRF та BGP для пристроїв мережі наведено нижче.

Комутатор SW-45-6-1 і робоча станція WS-1 (комутатор SW-45-6-4 і робоча станція WS-4 налагоджуються аналогічно з VLAN 7 і адресами з табл. 3):

```
…
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-45-6-1
SW-45-6-1(config)#vlan 5
SW-45-6-1(config-vlan)#name VLAN5
SW-45-6-1(config-vlan)#exit
SW-45-6-1(config)#interface vlan 5
SW-45-6-1(config-if)#ip address 192.168.45.253 255.255.255.0
SW-45-6-1(config-if)#no shutdown
SW-45-6-1(config-if)#exit
SW-45-6-1(config)#ip default-gateway 192.168.45.254
SW-45-6-1(config)#interface GigabitEthernet 0/1
SW-45-6-1(config-if)#switchport mode access
SW-45-6-1(config-if)#switchport access vlan 5
```

SW-45-6-1(config-if)#exit
SW-45-6-1(config)#interface GigabitEthernet 0/0
SW-45-6-1(config-if)#switchport trunk encapsulation dot1q
SW-45-6-1(config-if)#switchport mode trunk
SW-45-6-1(config-if)#switchport nonegotiate
SW-45-6-1(config-if)#switchport trunk allowed vlan 5
SW-45-6-1(config-if)#end
SW-45-6-1#copy running-config startup-config
…

…
VPCS> set pcname WS-1
WS-1> ip 192.168.45.1/24 192.168.45.254
WS-1> save
…

Маршрутизатор R-45-6-1-CE (сайт 1 VPN A):

…
Router>enable
Router#configure terminal
Router(config)#hostname R-45-6-1-CE
R-45-6-1-CE(config)#interface Ethernet 0/0.5
R-45-6-1-CE(config-subif)#encapsulation dot1Q 5
R-45-6-1-CE(config-subif)#ip address 192.168.45.254 255.255.255.0
R-45-6-1-CE(config-subif)#exit
R-45-6-1-CE(config)#interface Ethernet 0/0
R-45-6-1-CE(config-if)#no shutdown
R-45-6-1-CE(config-if)#exit
R-45-6-1-CE(config)#interface Serial 1/0
R-45-6-1-CE(config-if)#ip address 1.1.1.2 255.255.255.252
R-45-6-1-CE(config-if)#no shutdown
R-45-6-1-CE(config-if)#exit
R-45-6-1-CE(config)#router bgp 64561
R-45-6-1-CE(config-router)#neighbor 1.1.1.1 remote-as 65061
R-45-6-1-CE(config-router)#network 192.168.45.0 mask 255.255.255.0
R-45-6-1-CE(config-router)#end
R-45-6-1-CE#copy running-config startup-config
…

Маршрутизатор R-45-6-5-LSR (P):

…
Router>enable
Router#configure terminal
Router(config)#hostname R-45-6-5-LSR
R-45-6-5-LSR(config)#interface Loopback 0
R-45-6-5-LSR(config-if)#ip address 20.20.20.20 255.255.255.255
R-45-6-5-LSR(config-if)#exit

R-45-6-5-LSR(config)#interface FastEthernet 0/0
R-45-6-5-LSR(config-if)#ip address 4.4.4.1 255.255.255.252
R-45-6-5-LSR(config-if)#mpls ip
R-45-6-5-LSR(config-if)#no shutdown
R-45-6-5-LSR(config-if)#exit
R-45-6-5-LSR(config)#interface FastEthernet 1/0
R-45-6-5-LSR(config-if)#ip address 5.5.5.1 255.255.255.252
R-45-6-5-LSR(config-if)#mpls ip
R-45-6-5-LSR(config-if)#no shutdown
R-45-6-5-LSR(config-if)#exit
R-45-6-5-LSR(config)#router eigrp 1
R-45-6-5-LSR(config-router)#network 20.20.20.20 0.0.0.0
R-45-6-5-LSR(config-router)#network 4.4.4.0 0.0.0.3
R-45-6-5-LSR(config-router)#network 5.5.5.0 0.0.0.3
R-45-6-5-LSR(config-router)#end
R-45-6-5-LSR#copy running-config startup-config
…

Маршрутизатор R-45-6-4-ELSR (PE): інтерфейс Loopback, канал до P з MPLS, EIGRP, VRF A1, MP-BGP та eBGP з CE.

…
Router>enable
Router#configure terminal
Router(config)#hostname R-45-6-4-ELSR
R-45-6-4-ELSR(config)#interface Loopback 0
R-45-6-4-ELSR(config-if)#ip address 10.10.10.10 255.255.255.255
R-45-6-4-ELSR(config-if)#exit
R-45-6-4-ELSR(config)#interface Ethernet 0/0
R-45-6-4-ELSR(config-if)#ip address 4.4.4.2 255.255.255.252
R-45-6-4-ELSR(config-if)#mpls ip
R-45-6-4-ELSR(config-if)#no shutdown
R-45-6-4-ELSR(config-if)#exit
R-45-6-4-ELSR(config)#router eigrp 1
R-45-6-4-ELSR(config-router)#network 10.10.10.10 0.0.0.0
R-45-6-4-ELSR(config-router)#network 4.4.4.0 0.0.0.3
R-45-6-4-ELSR(config-router)#exit
R-45-6-4-ELSR(config)#ip vrf A1
R-45-6-4-ELSR(config-vrf)#rd 2:1
R-45-6-4-ELSR(config-vrf)#route-target both 2:1
R-45-6-4-ELSR(config-vrf)#exit
R-45-6-4-ELSR(config)#interface Serial 1/0
R-45-6-4-ELSR(config-if)#ip vrf forwarding A1
R-45-6-4-ELSR(config-if)#ip address 1.1.1.1 255.255.255.252
R-45-6-4-ELSR(config-if)#no shutdown
R-45-6-4-ELSR(config-if)#exit
R-45-6-4-ELSR(config)#router bgp 65061

```
R-45-6-4-ELSR(config-router)#neighbor 30.30.30.30 remote-as 65061
R-45-6-4-ELSR(config-router)#neighbor 30.30.30.30 update-source
    Loopback0
R-45-6-4-ELSR(config-router)#address-family vpnv4
R-45-6-4-ELSR(config-router-af)#neighbor 30.30.30.30 activate
R-45-6-4-ELSR(config-router-af)#neighbor 30.30.30.30 send-community
    extended
R-45-6-4-ELSR(config-router-af)#exit-address-family
R-45-6-4-ELSR(config-router)#address-family ipv4 vrf A1
R-45-6-4-ELSR(config-router-af)#neighbor 1.1.1.2 remote-as 64561
R-45-6-4-ELSR(config-router-af)#exit-address-family
R-45-6-4-ELSR(config-router)#end
R-45-6-4-ELSR#copy running-config startup-config
…
```

Маршрутизатор R-45-6-6-ELSR (PE) налагоджується дзеркально:

```
…
Router>enable
Router#configure terminal
Router(config)#hostname R-45-6-6-ELSR
R-45-6-6-ELSR(config)#interface Loopback 0
R-45-6-6-ELSR(config-if)#ip address 30.30.30.30 255.255.255.255
R-45-6-6-ELSR(config-if)#exit
R-45-6-6-ELSR(config)#interface Ethernet 0/0
R-45-6-6-ELSR(config-if)#ip address 5.5.5.2 255.255.255.252
R-45-6-6-ELSR(config-if)#mpls ip
R-45-6-6-ELSR(config-if)#no shutdown
R-45-6-6-ELSR(config-if)#exit
R-45-6-6-ELSR(config)#router eigrp 1
R-45-6-6-ELSR(config-router)#network 30.30.30.30 0.0.0.0
R-45-6-6-ELSR(config-router)#network 5.5.5.0 0.0.0.3
R-45-6-6-ELSR(config-router)#exit
R-45-6-6-ELSR(config)#ip vrf A2
R-45-6-6-ELSR(config-vrf)#rd 2:1
R-45-6-6-ELSR(config-vrf)#route-target both 2:1
R-45-6-6-ELSR(config-vrf)#exit
R-45-6-6-ELSR(config)#interface Serial 1/0
R-45-6-6-ELSR(config-if)#ip vrf forwarding A2
R-45-6-6-ELSR(config-if)#ip address 6.6.6.1 255.255.255.252
R-45-6-6-ELSR(config-if)#no shutdown
R-45-6-6-ELSR(config-if)#exit
R-45-6-6-ELSR(config)#router bgp 65061
R-45-6-6-ELSR(config-router)#neighbor 10.10.10.10 remote-as 65061
R-45-6-6-ELSR(config-router)#neighbor 10.10.10.10 update-source
    Loopback0
R-45-6-6-ELSR(config-router)#address-family vpnv4
```

R-45-6-6-ELSR(config-router-af)#neighbor 10.10.10.10 activate
R-45-6-6-ELSR(config-router-af)#neighbor 10.10.10.10 send-community extended
R-45-6-6-ELSR(config-router-af)#exit-address-family
R-45-6-6-ELSR(config-router)#address-family ipv4 vrf A2
R-45-6-6-ELSR(config-router-af)#neighbor 6.6.6.2 remote-as 64562
R-45-6-6-ELSR(config-router-af)#exit-address-family
R-45-6-6-ELSR(config-router)#end
R-45-6-6-ELSR#copy running-config startup-config
…

Маршрутизатор R-45-6-7-CE (сайт 2 VPN A):

…
Router>enable
Router#configure terminal
Router(config)#hostname R-45-6-7-CE
R-45-6-7-CE(config)#interface Ethernet 0/0.7
R-45-6-7-CE(config-subif)#encapsulation dot1Q 7
R-45-6-7-CE(config-subif)#ip address 192.168.46.254 255.255.255.0
R-45-6-7-CE(config-subif)#exit
R-45-6-7-CE(config)#interface Ethernet 0/0
R-45-6-7-CE(config-if)#no shutdown
R-45-6-7-CE(config-if)#exit
R-45-6-7-CE(config)#interface Serial 1/0
R-45-6-7-CE(config-if)#ip address 6.6.6.2 255.255.255.252
R-45-6-7-CE(config-if)#no shutdown
R-45-6-7-CE(config-if)#exit
R-45-6-7-CE(config)#router bgp 64562
R-45-6-7-CE(config-router)#neighbor 6.6.6.1 remote-as 65061
R-45-6-7-CE(config-router)#network 192.168.46.0 mask 255.255.255.0
R-45-6-7-CE(config-router)#end
R-45-6-7-CE#copy running-config startup-config
…

Під час налагодження слід ураховувати такі особливості:

– команду **ip vrf forwarding** потрібно виконувати до задання IP-адреси: якщо адресу задано раніше, вона видаляється з інтерфейсу і її потрібно задати повторно;

– команду **route-target** неможливо виконати, доки для VRF не задано RD;

– MPLS вмикається лише на інтерфейсах ядра; мережі PE–CE не оголошуються в IGP провайдера;

– команда **neighbor … send-community extended** потрібна для передачі значень RT; у багатьох версіях Cisco IOS її додано

автоматично під час активації сусіда в сімействі адрес VPNv4, проте рекомендовано задавати її явно.

Хід налагодження зручно контролювати за системними повідомленнями маршрутизаторів: про встановлення сусідства EIGRP (%DUAL-5-NBRCHANGE … new adjacency), LDP (%LDP-5-NBRCHG: LDP Neighbor 30.30.30.30:0 (1) is UP), сесії iBGP (%BGP-5-ADJCHANGE: neighbor 10.10.10.10 Up) та сесії PE–CE у VRF (%BGP-5-ADJCHANGE: neighbor 1.1.1.2 vpn vrf A1 Up). Після активації сусіда в сімействі адрес VPNv4 сесія iBGP перевстановлюється (повідомлення Capability changed), оскільки сторони мають заново узгодити підтримувані сімейства адрес.

Результати виконання команд моніторингу та діагностики роботи MPLS та L3 MPLS VPN для розглянутого прикладу

З метою перегляду інформації про роботу MPLS та VRF для розглянутого прикладу використано команду **show mpls forwarding-table**. Перевірку зв'язку в контексті VRF і між сайтами VPN A здійснено за допомогою команд **ping vrf**, **ping** і **trace**. Результати роботи цих команд наведено на рис. 3–6.

```
R-45-6-4-ELSR#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  5.5.5.0/30       0             Et0/0      4.4.4.1
17         Pop Label  20.20.20.20/32   0             Et0/0      4.4.4.1
18         No Label   192.168.45.0/24[V]   \
                                       0             Se1/0      point2point
R-45-6-4-ELSR#
```

Рис. 3. Результат роботи команди show mpls forwarding-table на маршрутизаторі R-45-6-4-ELSR

У таблиці LFIB (рис. 3) для мереж 5.5.5.0/30 і 20.20.20.20/32 вихідною дією є **Pop Label**: кінцевим маршрутизатором для цих мереж є сам маршрутизатор R-45-6-5-LSR (4.4.4.1), тому R-45-6-4-ELSR як передостанній маршрутизатор LSP надсилає пакети без мітки (PHP). Запис 192.168.45.0/24[V] належить VRF (позначка [V]): це локальна VPN-мітка, яку R-45-6-4-ELSR призначив мережі сайту 1 і передав іншому PE через MP-BGP; пакети з цією міткою пересилаються до CE через Se1/0 без мітки (No Label).

```
R-45-6-4-ELSR#ping vrf A1 192.168.45.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.45.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/9 ms
R-45-6-4-ELSR#
```

Рис. 4. Результат виконання команди ping vrf на маршрутизаторі R-45-6-4-ELSR

Команда **ping vrf A1 192.168.45.254** (рис. 4) перевіряє досяжність підінтерфейсу CE сайту 1 саме з таблиці маршрутизації VRF A1. Без параметра **vrf** маршрутизатор шукав би адресу в глобальній таблиці, де мереж клієнта немає.

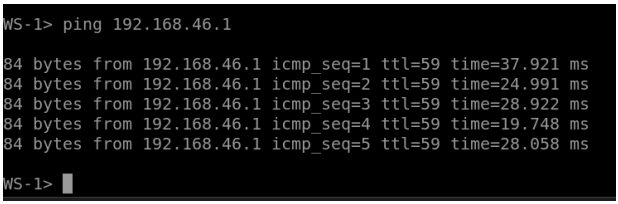


Рис. 5. Результат виконання команди ping на робочій станції WS-1

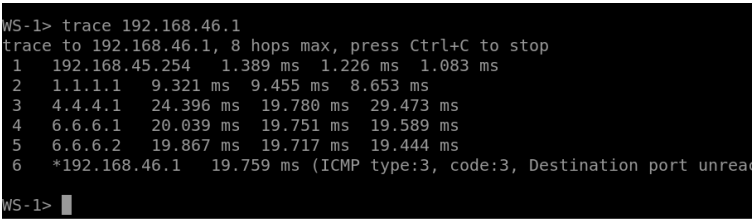


Рис. 6. Результат виконання команди trace на робочій станції WS-1

Робоча станція WS-1 отримує відповіді від WS-4 (рис. 5), отже, маршрути сайтів VPN A успішно передаються через MP-BGP. Трасування (рис. 6) показує шлях 192.168.45.254 (CE сайту 1) → 1.1.1.1 (PE, VRF A1) → 4.4.4.1 (P) → 6.6.6.1 (PE, VRF A2) → 6.6.6.2 (CE сайту 2) → 192.168.46.1. Відповідь від маршрутизатора P з адресою 4.4.4.1 з'являється тому, що за замовчуванням Cisco IOS копіює TTL з IP-заголовка в мітку і P формує повідомлення ICMP про вичерпання TTL.

Завдання на лабораторну роботу

1. У середовищі віртуальної мережевої лабораторії eve.ztu.edu.ua створити проєкт мережі (рис. 7). Для побудованої мережі заповнити описову таблицю, яка аналогічна табл. 2.

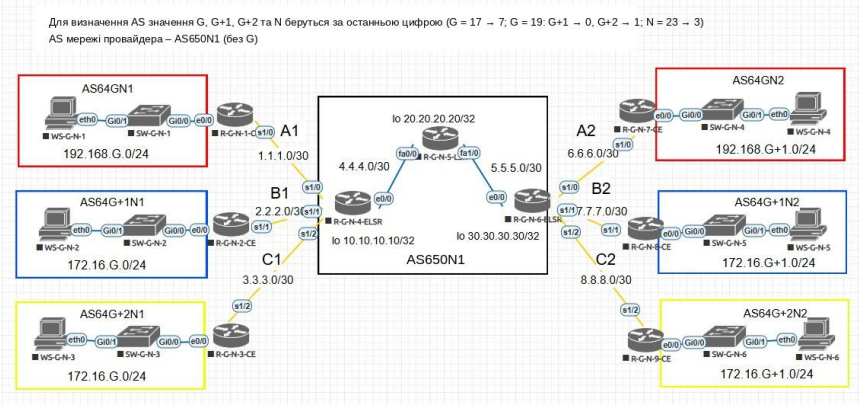


Рис. 7. Схема мережі

2. Розробити схему адресації пристроїв мережі. Для цього використати дані, наведені в проєкті (рис. 7). Результати навести у вигляді таблиці, яка аналогічна табл. 3. Номери VLAN для сайтів обрати самостійно (різні для кожного сайту).

3. На маршрутизаторах мережі провайдера налагодити інтерфейси Loopback, протокол внутрішньої маршрутизації (табл. 4) та функціонування технології MPLS. Перевірити встановлення сусідства LDP, вміст таблиць LIB і LFIB.

4. На маршрутизаторах PE налагодити VRF-екземпляри для VPN A, B, C з параметрами RD і RT за табл. 4 та прив'язати до них інтерфейси, до яких підключено CE.

5. Налагодити протокол BGP: сесію MP-BGP (VPNv4) між маршрутизаторами PE через інтерфейси Loopback, сесії eBGP між PE і CE з номерами автономних систем за рис. 7 (G, G+1, G+2 та N – за останньою цифрою; AS провайдера – 650N1). На CE оголосити мережі сайтів. Забезпечити обмін маршрутами між сайтами кожної VPN через MPLS-домен.

6. Дослідити особливості отримання службової та діагностичної інформації MPLS та VRF за допомогою відповідних команд моніторингу та відлагодження (табл. 1).

7. Дослідити процеси передачі даних між вузлами сайтів кожної VPN та перевірити відсутність зв'язку між сайтами різних VPN. Пояснити, чому VPN B і VPN C з однаковою адресацією не конфліктують. У разі відсутності зв'язку визначити причини порушення та усунути їх.

8*. За допомогою засобу перехоплення трафіку лабораторії (Wireshark) перехопити ICMP-пакети між сайтами VPN A на каналах R-G-N-4-ELSR – R-G-N-5-LSR та R-G-N-5-LSR – R-G-N-6-ELSR. Порівняти стек міток MPLS на обох каналах і пояснити відмінності.

Таблиця 4

Варіанти завдань для налагодження MPLS VPN з параметрами протоколів маршрутизації та RD для VRF

№ варіанта	Протокол маршрутизації (IGP)	RD = RT VRF A	RD = RT VRF B	RD = RT VRF C
Непарні	RIPv2	2:1	3:1	4:1
Парні	OSPF	4:1	5:1	6:1

** Завдання підвищеної складності (виконується за бажанням).*

Контрольні питання

1. Що таке MPLS? Чому технологію MPLS називають багатопротокольною?
2. Основні елементи технології MPLS: FEC, LSR, LSP.
3. Що таке LSR? Поділ маршрутизаторів MPLS за роллю (CE, PE/E-LSR, P/LSR).
4. Формат заголовка MPLS. Призначення полів.
5. Операції з мітками push, swap, pop. Що таке PHP?
6. Призначення та принцип роботи протоколу LDP.
7. Які таблиці формуються під час роботи MPLS (LIB, LFIB)?
8. Переваги використання MPLS VPN.
9. Особливості технології L2 MPLS VPN.
10. Що таке VRF? Його складові.
11. Параметри VRF: призначення RD і RT.
12. Призначення протоколу MP-BGP у L3 MPLS VPN.
13. Навіщо пакету VPN у мережі провайдера дві мітки? Хто розподіляє кожну з них?
14. Як забезпечується ізоляція VPN з однаковими адресними просторами?
15. Порядок налагодження L3 MPLS VPN на обладнанні Cisco.
16. Для чого призначена команда show mpls l2transport vc?
17. Для чого призначена команда show mpls forwarding-table? Що означають записи Pop Label і No Label?
18. Для чого призначена команда show ip route vrf? Її синтаксис.
19. Для чого призначені команди ping vrf та show ip bgp vpnv4 all?