МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«НАЦІОНАЛЬНИЙ ГІРНИЧИЙ УНІВЕРСИТЕТ»

ІНСТИТУТ ЕЛЕКТРОЕНЕРГЕТИКИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра автоматизації та комп'ютерних систем

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні вказівки до виконання лабораторних робіт
студентами напряму підготовки
6.050102 Комп'ютерна інженерія

Дніпропетровськ
НГУ
2012

Комп’ютерні мережі. Методичні вказівки до виконання лабораторних робіт студентами напряму підготовки 6.050102 Комп’ютерна інженерія / Я.В. Панферова, І.В. Кмітіна, Л.І. Цвіркун. – Д.: Національний гірничий університет, 2012. – 31 с.

Автори:
Я.В. Панферова, асист.;
І.В. Кмітіна, асист.;
Л.І. Цвіркун, проф.

Затверджено методичною комісією з напряму підготовки 6.050102 Комп’ютерна інженерія (протокол № 1 від 12.01.12) за поданням кафедри автоматизації та комп’ютерних систем (протокол № 7 від 11.01.12).

Подано методичні вказівки до виконання лабораторних робіт з дисципліни “Комп’ютерні мережі” студентами напряму підготовки 6.050102 Комп’ютерна інженерія.

Відповідальний за випуск завідувач кафедри автоматизації та комп’ютерних систем, д-р техн. наук, проф. В.В. Ткачов.

ЗМІСТ

ВСТУП

Комп'ютерні мережі з'явилися порівняно недавно, наприкінці 60-х років минулого сторіччя. Однак вони привнесли в телекомунікаційний світ щось зовсім нове – створені цивілізацією невичерпні запаси інформації, які поповнюються із зростаючою швидкістю.

Доступність комп'ютерних мереж у сполученні з потужними і компактними обчислювальними й комунікаційними засобами дозволяє зробити новий крок на шляху розвитку мобільних обчислень і комунікацій, «хмарних» технологій.

Нормативна навчальна дисципліна «Комп'ютерні мережі» належить до професійно-практичного циклу і займає важливе місце у підготовці бакалаврів.

Методичні вказівки призначені для студентів напряму підготовки 6.050102 Комп'ютерна інженерія, які вивчають дисципліну «Комп'ютерні мережі».

Методичні вказівки включають низку частково взаємопов'язаних робіт, під час виконання яких студенти мають можливість отримати досвід роботи з мережевим аналізатором Wireshark, утилітами операційної системи Windows XP, навчитися організовувати підмережі, визначати правильні ідентифікатори мереж для даної маски підмережі та відповідні ідентифікатори вузлів для кожної мережі або підмережі, а також розбивати мережу на підмережі за допомогою маски змінної довжини VLSM та розраховувати сумарний маршрут для кожного маршрутизатора.

Перед виконанням лабораторної роботи студенти повинні:

- ознайомитися з методичними вказівками;
- повторити лекційний матеріал, пов'язаний з лабораторною роботою;
- підготовити відповіді на питання, які наведені у методичних вказівках наприкінці кожної лабораторної роботи.

Виконавши ці завдання, студент повинен продемонструвати викладачеві роботу на комп'ютері або в зошиті, оформити звіт за результатами даної лабораторної роботи, захистити його та здати викладачеві.

Загальні вимоги до виконання лабораторної роботи, що мають забезпечити максимальну оцінку:

- повна відповідність звіту про виконання лабораторної роботи методичним рекомендаціям;
- володіння теоретичним матеріалом стосовно предмета досліджень;
- загальна та професійна грамотність, лаконізм та логічна послідовність викладу матеріалу;
- відповідність оформлення звіту чинним стандартам.

1 ЛАБОРАТОРНА РОБОТА № 1
ВИВЧЕННЯ ІНТЕРФЕЙСУ ПРОГРАМИ WIRESHARK

1.1 Мета лабораторної роботи

Ознайомитися з програмою Wireshark для аналізу мережевих протоколів. Вивчити інтерфейс програми, її основні функціональні можливості, отримати практичні навички написання фільтрів.

1.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки, такі питання:

- робота з командним рядком операційної системи Windows XP;
- модель OSI та взаємодія протоколів;
- правила написання фільтрів для аналізаторів мережевих протоколів,

а також визначити статичні характеристики мережевого трафіку, використовуючи захоплення пакетів.

Запустити програму Wireshark і вивчити її основні функціональні можливості, виконавши такі дії:

– здійснити захоплення M пакетів (де $M = 100n$, а n – номер у списку групи) мережевого трафіку програмою Wireshark без фільтра та уважно переглянути результат;

– визначити, які протоколи використовуються в мережі;

– визначити статичні характеристики мережевого трафіку:

1) відсоткове співвідношення трафіку різних протоколів у мережі;
2) середню швидкість трафіку (кадрів/с, байт/с);
3) мінімальний, максимальний і середній розміри кадрів;

– настроїти фільтр на захоплення пакетів ARP, які були генеровані тільки робочою станцією. Перевірити результат, включивши захоплення пакетів і запустивши зі свого вузла в командному рядку команду *ping* на сусідній вузол. Переглянути список доступних вузлів можна введенням у командному рядку *net view*;

– написати фільтр для перегляду тільки поштового трафіку на порти 110 (POP3) і 25 (SMTP), що відправляється до вузла з адресою 201.15.14.100.

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- опис завдання з початковими умовами та даними;
- статичні характеристики захопленого мережевого трафіку;
- скріншоти програми Wireshark в ході виконання роботи й відповідні коментарі.

1.3 Теоретичні відомості

1.3.1 Інтерфейс графічного аналізатора протоколів

Wireshark – графічний аналізатор мережевих протоколів. Сайт програми – www.wireshark.org. Дане програмне забезпечення дозволяє у режимі реального часу захоплювати пакети з мережі й аналізувати їхню структуру. Також можна аналізувати структуру пакетів, зроблених за допомогою утиліти *tcpdump* та інших аналізаторів.

У програмі Wireshark є кілька імен: Wireshark – нове ім'я програми, Ethereal – старе ім'я програми. Назва програми змінилася в 2006 році з ліцензійних причин.

Основне вікно (рисунок 1.1) ділиться на зону меню, панелі інструментів і три вікна. Розмір кожного вікна можна змінювати за своїм бажанням.

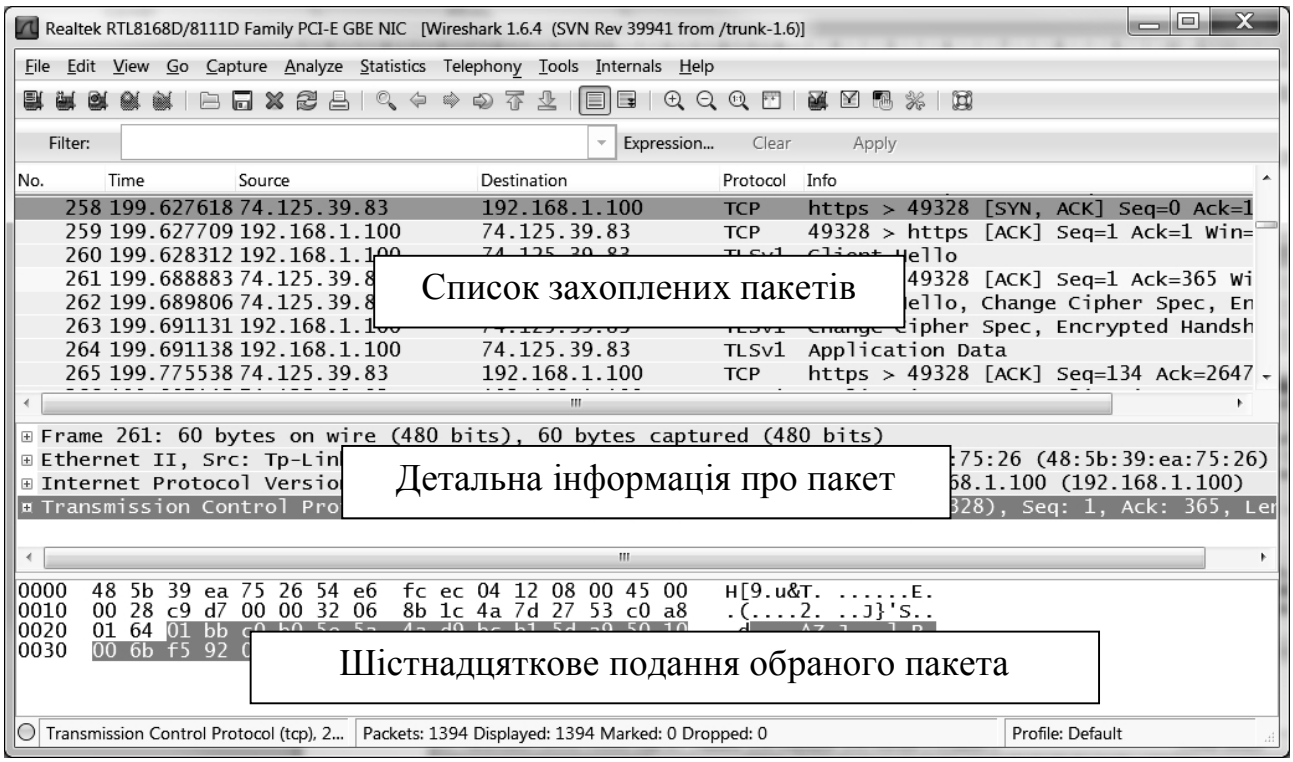


Рисунок 1.1 – Основне вікно Wireshark із захопленими пакетами

Верхнє вікно містить список пакетів, захоплених з мережі. При натисканні правої кнопки миші на тому чи іншому пакеті з'явиться контекстне меню.

Список можна відсортувати за будь-яким полем (у прямому або зворотному порядку). Для цього потрібно натиснути на заголовок відповідного поля.

Кожний рядок містить такі поля (за умовчанням): порядковий номер пакета, час надходження пакета, джерело пакета, пункт призначення (адресат), протокол, інформаційне поле.

Список відображуваних полів настроюється в меню Edit/Preferences/Columns. Для того, щоб цей список запам’ятати, необхідно натиснути кнопку “Apply”.

Середнє вікно містить так зване “Дерево протоколів” для обраного пакета у верхньому вікні.

У цьому вікні в ієрархічному вигляді відображається вкладення пакетів відповідно до моделі взаємодії відкритих систем OSI. Після натискання правою кнопкою миші на тому чи іншому пакеті з'явиться контекстне меню.

Нижнє вікно містить шістнадцяткове подання обраного пакета. При виборі того або іншого поля в середньому вікні автоматично буде підсвічуватися відповідна ділянка шістнадцяткового подання.

1.3.2 Фільтрація під час захоплення

Для захоплення або відображення тільки тих пакетів, які цікавлять, використовуються два види фільтрації: під час захоплення і під час відображення.

Фільтрація під час захоплення робиться з використанням правил Capture Filter (рисунок 1.2).

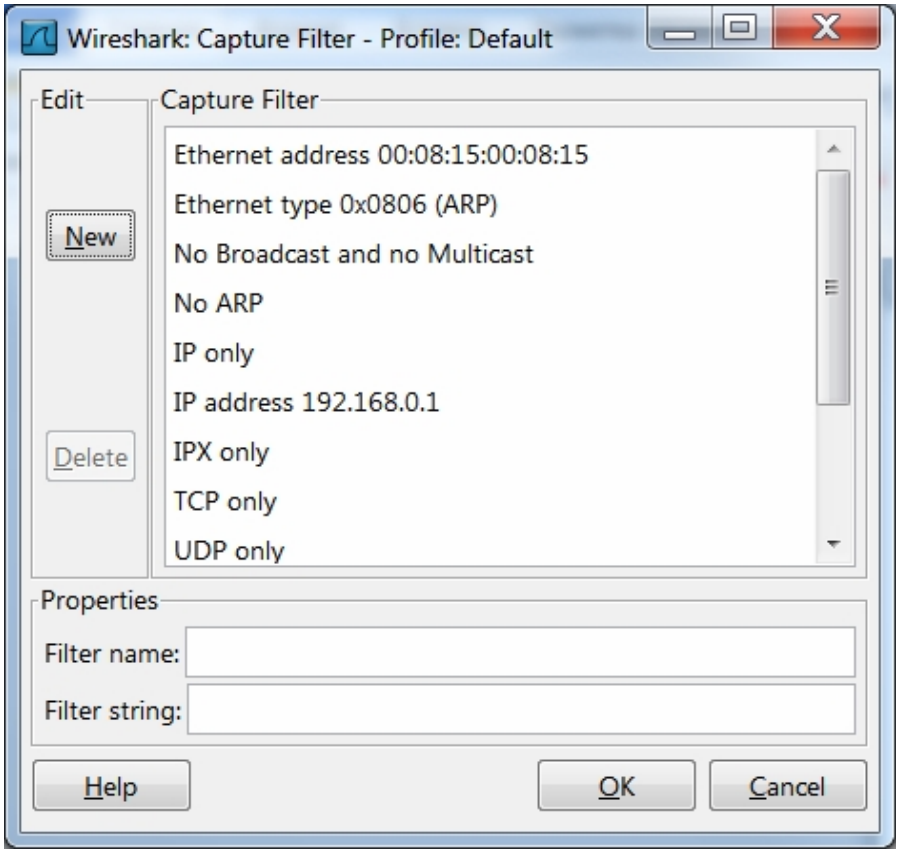


Рисунок 1.2 – Діалогове вікно Capture Filter

Вікно Capture Filter можна викликати через меню Capture/Capture Filter або через меню Capture/Options (рисунок 1.3).

В цьому випадку захоплюватимуться (запам'ятовуватимуться) тільки пакети, що задовольняють задані правила. Слід зауважити, що інформація про пакети, які не задовольняють фільтр, втрачається.

Фільтр складається (чи вибирається) до початку захоплення. При створенні фільтрів можна використати логічні операції *and*, *or* або *not*:

[not] **primitive**[and|or [not] **primitive**...]

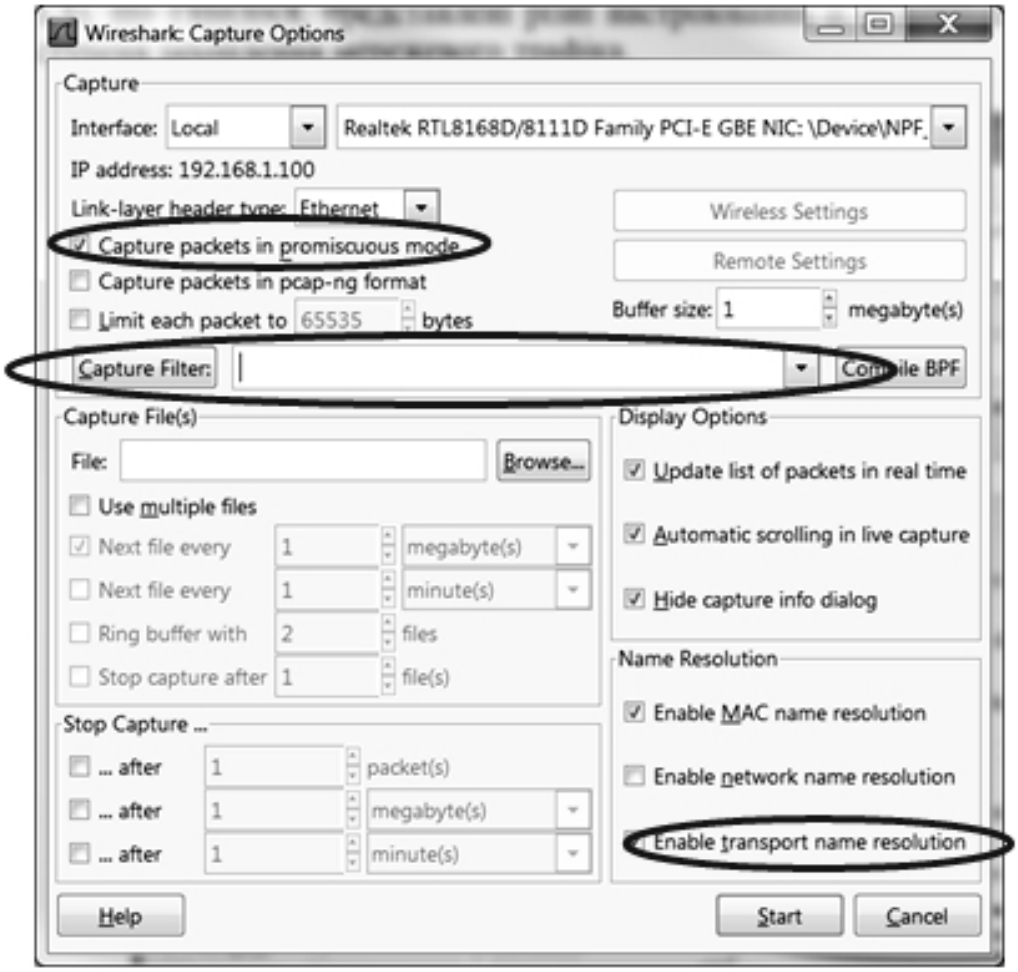


Рисунок 1.3 – Вікно опцій захоплення

Примітиви, які можуть бути використані для захоплення, вказані в таблиці 1.1.

Наприклад, фільтр для захоплення всього telnet трафіку, що передається і приймається всіма вузлами, окрім 10.0.0.5, має вигляд:

tcp port 23 and not host 10.0.0.5

Таблиця 1.1

Примітиви для захоплення пакетів

Примітив	Призначення
[src|dst] host <host>	Дозволяє фільтрувати пакети по імені вузла або за IP-адресою. Опціонально може бути доданий параметр [src|dst] – джерело і приймач захоплення
ether [src|dst] host <ehost>	Дозволяє фільтрувати пакети за адресою вузла. Можливе використання параметра [src, dst]
gateway <шлюз>	Дозволяє фільтрувати пакети, що використовують вказаний ім'ям хост як шлюз

Продовження таблиці 1.1

Примітив	Призначення
[src|dst] net <net> [{mask <mask>}|{len <len>}]	Дозволяє фільтрувати пакети за номером мережі. Можуть бути використані маски для мереж
[tcp|udp] [src|dst] port <port>	Дозволяє фільтрувати пакети за вказаними номерами портів для протоколів tcp чи udp
less|greater <length>	Дозволяє фільтрувати пакети, розмір яких менше (більше) або дорівнює вказаному значенню
ip|ether proto <protocol>	Дозволяє фільтрувати пакети за вказаним протоколом
ether|ip broadcast|multicast	Дозволяє фільтрувати широкомовні і групові пакети
<expr> relop <expr>	Дозволяє створювати складні фільтри, які дають можливість вибирати (шукати) байти (діапазони байт) у фільтрованих пакетах

1.3.3 Фільтрація під час перегляду

Фільтрація під час перегляду застосовується при показі вже захоплених пакетів з використанням правил Display Filter (рисунок 1.4).

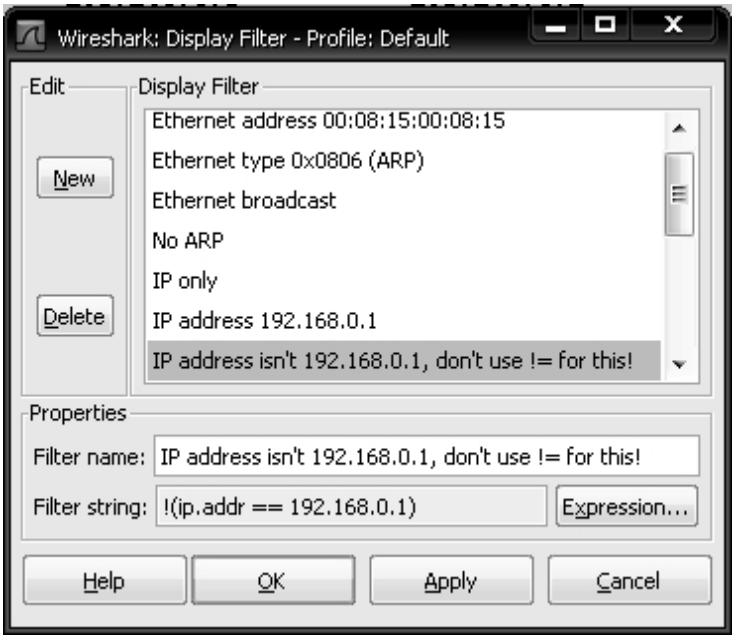


Рисунок 1.4 – Діалогове вікно Display Filter

Один і той же набір пакетів можна аналізувати за допомогою різних фільтрів. Ці фільтри можуть застосовуватися і при аналізі раніше сформованих і збережених наборів пакетів.

При використанні даного виду фільтрації надаються більш широкі можливості для формування фільтрів, ніж у попередньому випадку. Фільтри можна комбінувати один з одним з використанням операцій порівняння (таблиця 1.2) та логічних операцій (таблиця 1.3).

Таблиця 1.2

Операції порівняння

Позначення	Операція	Значення	Приклад
eq	= =	Дорівнює	ip.addr == 10.0.0.5
ne	!=	Не дорівнює	ip.addr != 10.0.0.5
gt	>	Більше	frame.pkt_len> 10
lt	<	Менше	frame.pkt_len< 10
ge	>=	Більше або дорівнює	frame.pkt_lenge>= 0x100
le	<=	Менше або дорівнює	frame.pkt_len<= 0x20

Таблиця 1.3

Логічні операції

Позначення	Операція	Значення	Приклад
and	&&	Логічне І	ip.addr==10.0.0.5 and tcp.flags.fin
or	||	Логічне АБО	ip.addr==10.0.0.5 or ip.addr==192.1.1.1
xor	^^	Виключне АБО	tr.dst[0:3] = = 0.6.29 xor tr.src[0:3] = = 0.6.29
not	!	Логічне НІ	not llc
[…]		Одержування значення полів з пакетів	eth.src[0:3] == 00:00:83 0 – початкове значення, 3 – довжина
			Можна також використати «-»: eth.src[1-2] == 00:83 1 – ліва межа інтервалу, 2 – права межа
			eth.src[:4] == 00:00:83:00 Від самого початку, вказана кількість. Еквівалентно 0:4
			eth.src[4:] == 20:20 Починаючи від 4 і до кінця
			eth.src[2] == 83 Вибіркове значення. Еквівалентно 2:1
			Можна також використовувати кілька способів вказівки параметрів, розділяючи їх комою eth.src[0:3,1-2,:4,4:,2]==00:00:83:00:83:00:00:83:00:20:20:83

Наприклад, фільтр для відображення тільки трафіку HTTP і DNS має вигляд: tcp.port = = 80 || tcp.port = = 53.

Фільтри відображення задаються в рядку під панеллю інструментів. Для цього в рядку потрібно ввести вираз фільтру і натиснути кнопку “Apply”. Після цього у верхньому вікні залишаться пакети, що належать цьому фільтру.

Кнопкою “Reset” дія фільтра скасовується.

Натиснувши кнопку “Filter” під панеллю інструментів, можна викликати вікно Display Filter та зберігати створені вирази під певними іменами для наступного використання і т.п.

Основні типи примітивів, які використовуються для написання фільтрів відображення, можна подивитися і вибрати, натиснувши кнопку Expression (рисунок 1.5).

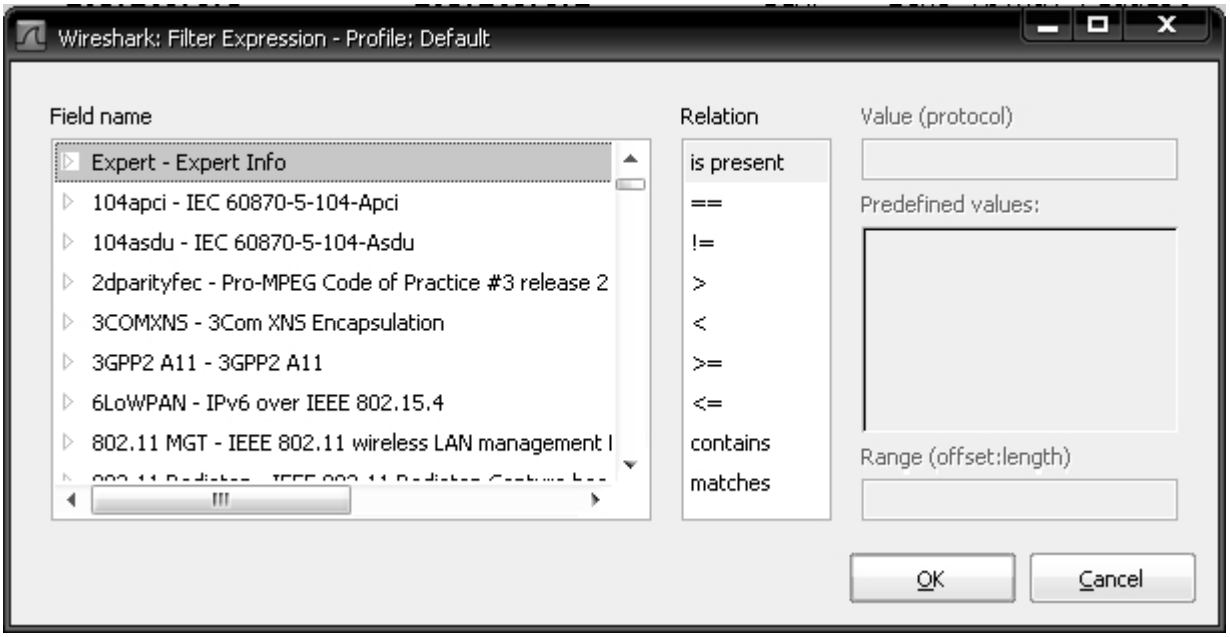


Рисунок 1.5 – Діалогове вікно Filter Expression

Більш простіший шлях складання фільтрів описаний далі. Зробивши захоплення (запис) необхідного трафіку, треба вибрати рядок з пакетом, що цікавить, а потім – відповідне поле і натиснути праву кнопку миші. У контекстному меню, що з'явилося, вибрати один з рядків (Apply Filter, Prepare Filter) та сформувати необхідний найпростіший фільтр.

Даний фільтр можна доповнити, вибираючи інші пакети та повторюючи дії. При необхідності отриманий фільтр можна зберегти, а також змінити і доповнити, використовуючи меню Analyze/Display filters.

Після того як задано відповідний фільтр, розпочинається процес захоплення пакетів.

Для цього потрібно перейти в меню Capture/Options або скористатися комбінацією клавіш CTRL+K. У вікні конфігурації захоплення Capture Options (рисунок 1.3), що з'явиться, подані різні настроювання й фільтри для визначення ступеня захоплення мережевого трафіку.

Якщо прапорець “Capture packets in promiscuous mode” (режим “нерозбірливого” захоплення) не встановлений, буде виконуватися захоплення пакетів, призначених тільки для цього комп'ютера. А якщо встановлений, буде виконуватися захоплення всіх пакетів, призначених для цього комп'ютера, а також усіх пакетів, виявлених мережевою платою комп'ютера в тому ж сегменті мережі (тобто тих, які “проходять” через мережеву плату, але не адресовані на цей комп'ютер).

Параметр “Enable transport name resolution” (активація трансляції мережевих імен) дозволяє встановити/скасувати режим трансляції мережевих адрес, виявлених у пакетах, в імена.

Інші основні параметри наведені нижче.

Interface – вибирається мережевий інтерфейс (реальний або віртуальний), через який буде здійснюватися захоплення.

Capture Filter – натисканням на кнопку “Capture Filter” можна застосувати той або інший фільтр (з раніше збережених). Якщо таких нема, його можна вказати явно в рядку редагування.

Update list of packets in real time – оновлення списку захоплених пакетів у режимі реального часу.

Набір параметрів *Capture File(s)* – дозволяє записувати зібрані програмою пакети у файл. Якщо файл не зазначений, програма буде записувати пакети в тимчасовий файл.

Набір параметрів *Stop Capture* – дозволяють задати те або інше значення, при досягненні якого процес захоплення пакетів припиниться.

Набір параметрів дозволу імен *Name Resolution* – допомогають визначити, які зі способів розв'язання імен повинні використовуватися.

Натискання кнопки “Start” запускає процес захоплення даних. У процесі захоплення пакетів в окремому вікні відображаються їхні типи й кількість.

Слід не забувати вибирати фільтр захоплення, який був підготовлений заздалегідь. А якщо ні, то буде спостерігатися весь трафік у загальному середовищі передачі й розібратися в захоплених пакетах буде важко.

Після того як зроблено захоплення необхідних пакетів, можна зупинити цей процес, натиснувши кнопку “Stop”. У результаті з'явиться вікно із захопленими пакетами відповідно до зазначеного фільтра, як показано на рисунку 1.1.

1.4 Питання для підготовки до захисту лабораторної роботи

1. У якому випадку вузол може бачити всі пакети в даному сегменті Ethernet?

2. Який протокол канального рівня підтримує мережа комп'ютерного класу?

3. Знайдіть два різні типи адрес відправника й одержувача.

4. Дайте визначення терміну “інкапсуляція”, використовуючи як приклад будь-який захоплений пакет.

5. До якого рівня моделі OSI належить протокол IP?

2 ЛАБОРАТОРНА РОБОТА № 2
ПОБУДОВА ПІДМЕРЕЖ ЗА ДОПОМОГОЮ МАСКИ ПОСТІЙНОЇ ДОВЖИНИ

2.1 Мета лабораторної роботи

Навчитися розбивати мережу на підмережі за допомогою маски постійної довжини, визначати адреси підмереж, а також діапазон IP-адресації вузлів для підмереж.

2.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки до даної роботи, такі питання:

– правила переходу з двійкової системи числення в десяткову та навпаки;

– IP-адресація в мережах;

– використання масок в IP-адресації.

Скласти схему IP-адресації мережі з використанням маски для відповідності вимогам топології мережі, поданої на рисунку 2.1.

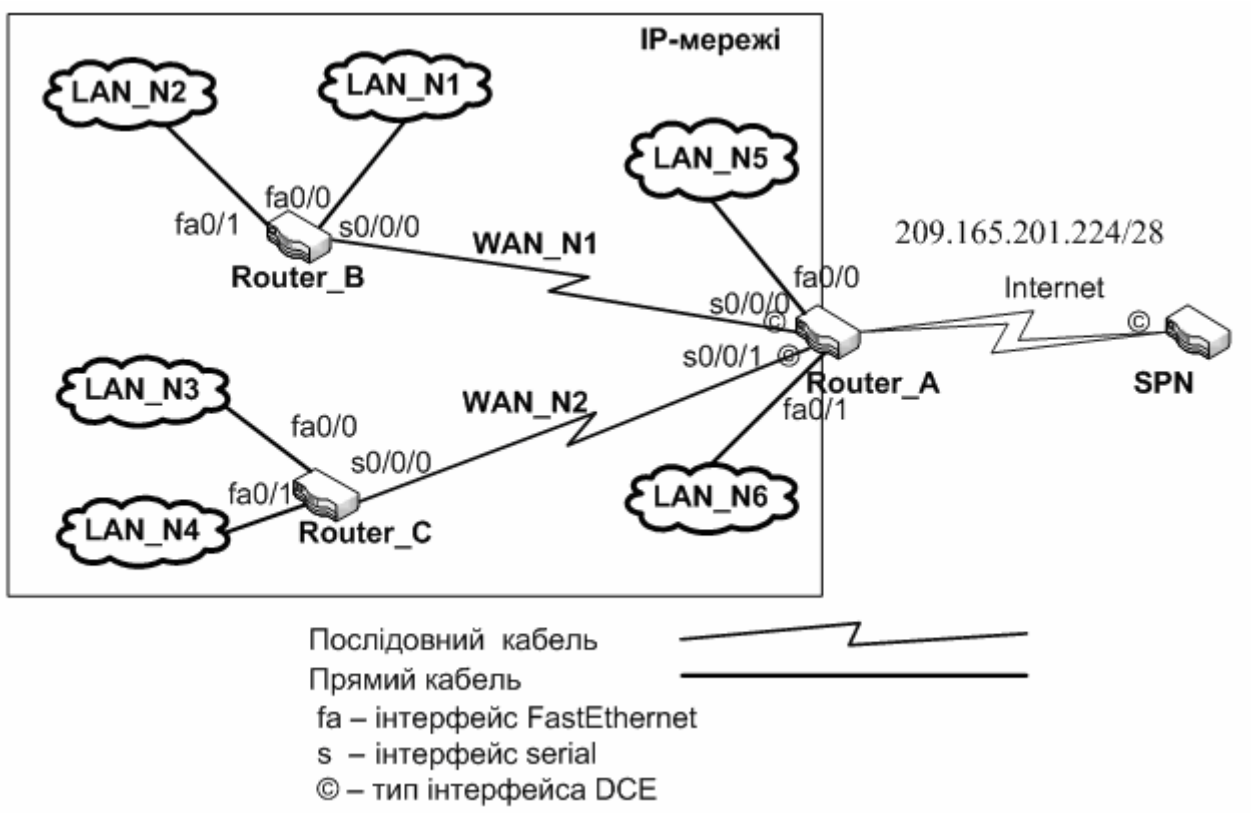


Рисунок 2.1 – Топологія мережі

Для адресації виділений мережний блок *IP-мережі* (таблиця 2.1) і висунуті такі вимоги:

– для LAN_N1 буде потрібно N_1 IP-адрес вузлів;

– для LAN_N2 буде потрібно N_2 IP-адрес вузлів;
– для LAN_N3 буде потрібно N_3 IP-адрес вузлів;
– для LAN_N4 буде потрібно N_4 IP-адрес вузлів;
– для LAN_N5 буде потрібно N_5 IP-адрес вузлів;
– для LAN_N6 буде потрібно N_6 IP-адрес вузлів;
– для WAN_N1 каналу між маршрутизаторами Router_A і Router_B будуть потрібні IP-адреси для кожного кінця каналу;
– для WAN_N2 каналу між маршрутизаторами Router_A і Router_C будуть потрібні IP-адреси для кожного кінця каналу.

Таблиця 2.1

Варіанти завдань

№ вар.	Адреса мережі	LAN_N1	LAN_N2	LAN_N3	LAN_N4	LAN_N5	LAN_N6
1.	180.16.0.0/16	500	1000	450	50	40	900
2.	190.17.0.0/18	1200	10	15	200	120	90
3.	45.0.0.0/8	56	10	600	660	10	60
4.	175.30.0.0/16	360	42	500	1000	30	800
5.	185.138.0.0/16	150	200	30	25	800	450
6.	178.13.0.0/16	250	350	1000	1500	2000	50
7.	182.210.0.0/18	100	25	30	120	10	50
8.	190.10.0.0/20	60	25	30	50	10	30
9.	181.140.0.0/19	250	950	150	110	60	1000
10.	175.28.0.0/18	2000	500	450	45	1800	95
11.	184.48.0.0/20	130	78	135	895	14	85
12.	188.98.0.0/16	460	510	12	14	890	980
13.	18.48.0.0/16	460	4500	3500	7000	500	4080
14.	187.68.0.0/16	490	980	450	120	870	100
15.	190.16.0.0/16	3000	490	160	2500	450	200
16.	90.0.0.0/8	50000	4000	1600	2000	3900	30000
17.	189.87.0.0/18	630	480	190	210	380	690
18.	179.91.0.0/19	20	480	500	30	110	90
19.	177.131.0.0/20	30	150	200	20	500	430
20.	177.13.0.0/21	8	10	170	60	200	230
21.	19.16.0.0/16	8000	630	7800	500	1000	450
22.	183.190.0.0/16	1900	1020	87	118	2000	970
23.	13.190.0.0/16	8100	8000	500	200	500	250
24.	183.250.0.0/20	70	90	250	10	12	240
25.	188.215.0.0/19	95	100	25	30	510	5

Необхідно задати схему поділу мережі на підмережі в заданому сценарії. Вихідні дані наведені в таблиці 2.1 згідно з варіантом.

При цьому IP-адреси будуть потрібні для кожного інтерфейсу локальної мережі кожного маршрутизатора.

Необхідно визначити:

– широкомовну адресу для кожної підмережі;

– кількість необхідних підмереж;

– кількість необхідних IP-адрес;

– кількість IP-адрес, які необхідні для найбільшої мережі LAN;

– маску підмережі;

– діапазон коректних ідентифікаторів підмереж;

– діапазон коректних ідентифікаторів вузлів у підмережах;

– кількість IP-адрес, які необхідні для кожного каналу WAN між маршрутизаторами;

– кількість IP-адрес, які доступні у початковій і поділеній мережах;

– відсоток адресного простору в початковій і поділеній мережах.

Підготувати звіт про виконання лабораторної роботи, який повинен включати:

– тему і мету лабораторної роботи;

– опис завдання з початковими умовами і даними;

– відповіді на зазначені питання;

– розрахунок адресації мережі згідно із завданням, поданий у вигляді таблиць 2.2 та 2.3;

– схему вирішення адресації заданої мережі у вигляді логічної топології згідно з рисунком 2.2.

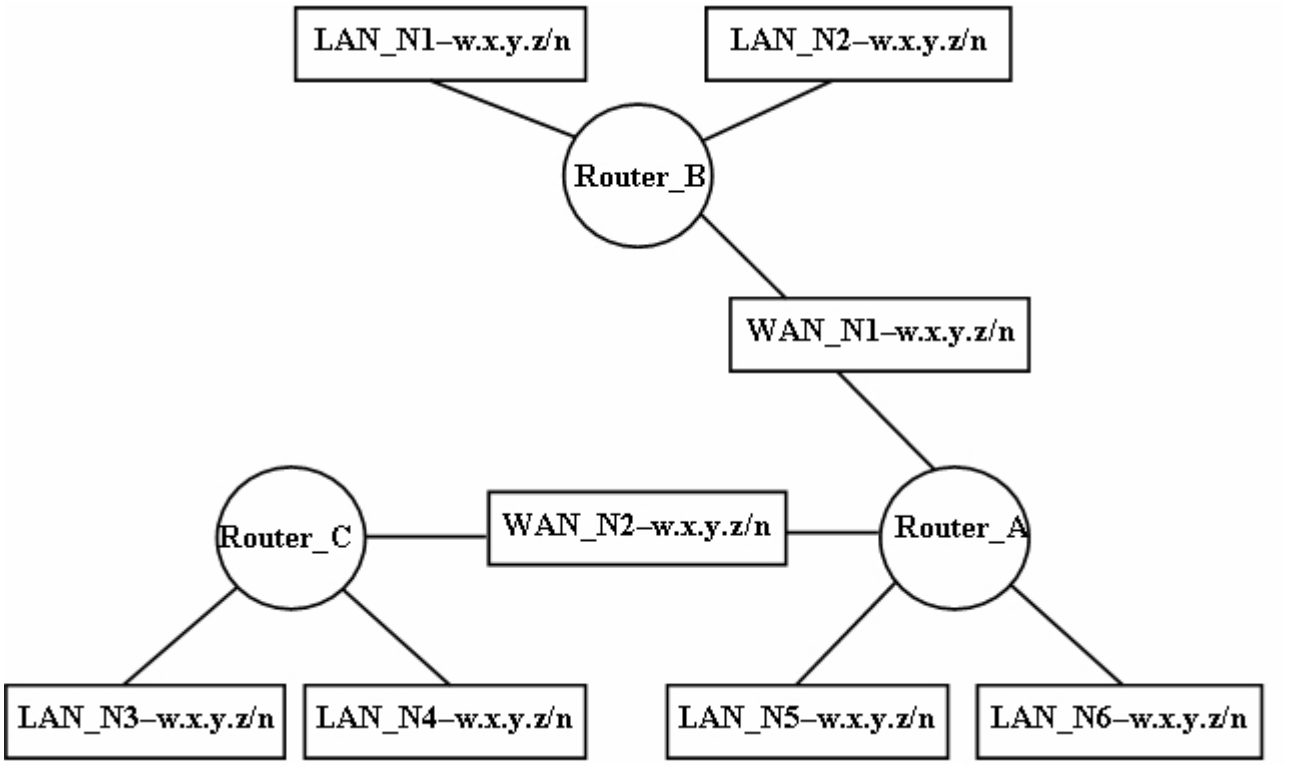


Рисунок 2.2 – Схема вирішення адресації заданої мережі

Таблиця 2.2

Визначення маски підмережі в організації

Початкова адреса мережі	Розрахована маска підмережі в десятковому вигляді	Розрахована маска підмережі в двійковому вигляді	Кількість зарезервованих біт для адрес підмереж	Кількість комбінацій підмереж для визначеної маски
…	…	…	…	…

Таблиця 2.3

Можливі варіанти адрес підмереж та вузлів

Двійковий формат адрес підмереж для визначеної маски	Десятковий формат адрес підмереж для визна-ченої маски	Початкове значення діапазону допустимих адрес вузлів у підмережі	Кінцеве значення діапазону допустимих адрес вузлів у підмережі	Кількість вузлів у підмережі	Широкомовна адреса в підмережі
…	…	…	…	…	…

2.3 Теоретичні відомості

2.3.1 Загальні відомості з побудови підмереж

Підмережа (subnet) – це фізичний сегмент TCP/IP мережі, в якому використовуються IP-адреси із загальною адресою мережі. При використанні підмереж рекомендується дотримуватися стандарту RFC 950 “Стандартні процедури організації підмереж IP”.

Формування підмереж вирішує проблему зростання таблиць маршрутизації, оскільки конфігурацію підмереж корпоративної мережі ніколи не видно за межами організації.

Формування підмереж також забезпечує вирішення другої проблеми, пов’язаної з виділенням організації нового мережевого номера або номерів при її зростанні. Організації можна виділити один номер мережі, після чого адміністратор отримує право довільно давати номери підмереж кожній зі своїх внутрішніх мереж. Це дозволяє впроваджувати додаткові підмережі без необхідності отримання нового мережевого номера.

На рисунку 2.3 показаний приклад розподіленої мережі, що складається з декількох логічних мереж, які використовують концепцію підмереж всередині однієї адреси класу B. Граничний маршрутизатор отримує весь трафік, адресований мережі 130.5.0.0 з Internet, і передає його внутрішнім підмережам, ґрунтуючись на інформації, що міститься в третьому октеті.

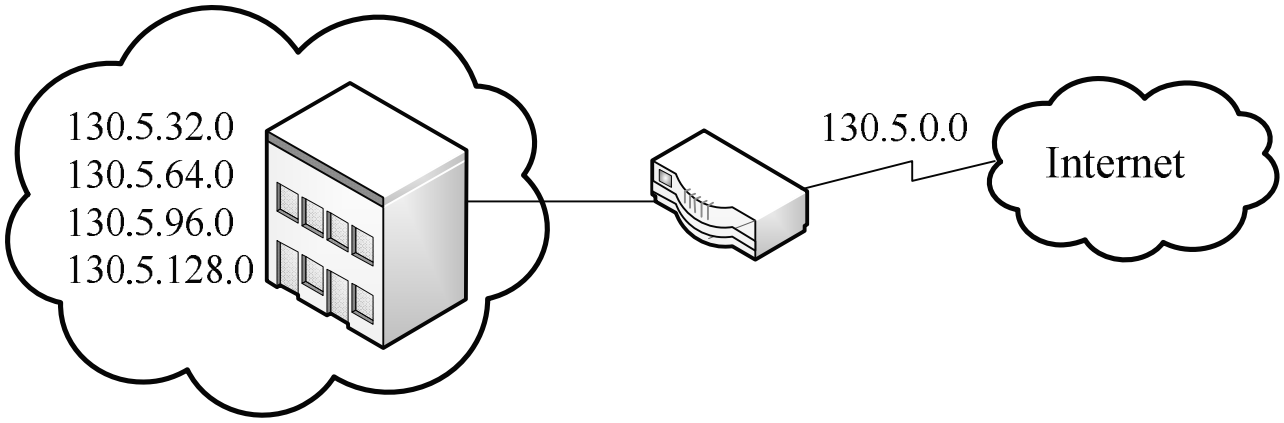


Рисунок 2.3 – Введення підмереж в організації

Перед початком роботи з підмережею необхідно визначити, яким вимогам повинна відповідати мережа зараз і яким у майбутньому.

Використовують таку схему:

1. Визначають кількість фізичних сегментів мережі.
2. Визначають кількість IP-адрес, які необхідні для кожного сегмента. Кожному вузлу TCP/IP потрібна принаймні одна IP-адреса.
3. Відповідно до вимог визначають:

– одну маску підмережі для всієї мережі;

– унікальні адреси підмереж для кожного фізичного сегмента;

– діапазон адрес вузлів для кожної підмережі.

Перед тим як сформувати маску підмережі, приблизно визначають, скільки сегментів і вузлів у сегменті буде потрібно в майбутньому.

Задавши більше біт для маски підмережі, можна збільшити кількість підмереж, але максимальна кількість вузлів у кожній з них тоді скоротиться.

Наприклад, для мережі класу B:

3 біти = 8 (2^3) підмереж = 8 190 (2^{13}-2) вузлів у підмережі;

8 біт = 256 (2^8) підмереж = 254 (2^8-2) вузла в підмережі.

Якщо використовувати більше біт, ніж необхідно, це дозволить у майбутньому збільшити кількість підмереж, але обмежить кількість вузлів у кожній з них. І навпаки, використовуючи менше біт, можна збільшити кількість вузлів у підмережі, проте лімітується кількість підмереж.

2.3.2 Визначення маски підмережі

Завдання маски підмережі необхідно, якщо мережа розбивається на підмережі. Для цього виконуються такі операції:

1. Визначається кількість фізичних сегментів у мережі та перекладається це значення в двійковий формат.

2. Підраховується, скільки біт необхідно для запису отриманого значення в двійковому форматі. Наприклад, якщо в мережі шість сегментів, двійкове значення дорівнює 110 і для його запису потрібно 3 біти.

3. Ці біти записуються одиницями (кількість необхідних біт дорівнює кількості записуваних одиниць).

Доповняють їх праворуч нулями до одного байта. Перекладається отримане двійкове значення в десятковий формат.

У розглянутому прикладі для адреси підмережі знадобилося 3 біти. Перевівши 11100000 в десяткове число, отримаємо 224. Тоді маска підмережі буде мати вигляд 255.255.224.0 (для адреси мережі класу B).

2.3.3 Визначення адрес підмереж

Слід зауважити, що коли схема введення підмереж була опублікована в документі RFC 950, заборонялося використання номерів підмереж, у яких усі біти встановлені в одиниці або нулі. Причиною такого обмеження є необхідність усунення можливих проблем при роботі тих протоколів маршрутизації, які не переносять у своїх службових повідомленнях маску підмережі. З розробкою протоколів маршрутизації, що переносять маску підмережі (OSPF, RIPv2) з кожним рекламованим маршрутом, стало можливо всупереч документу RFC 950 використати підмережі, усі біти яких встановлені в одиницю і нуль. З цієї причини виробники дозволяють настроювати підмережі з такими номерами на портах своїх маршрутизаторів.

Для завдання адрес підмереж використовується та сама кількість біт, що і для відповідної маски підмережі.

Визначити діапазон адрес підмереж, що входять в об’єднану мережу, можна двома способами.

Спосіб 1

1. Виписуються всі можливі комбінації біт, що використовуються для формування маски підмережі.

2. Переводяться в десятковий формат значення комбінації біт для кожної підмережі. Кожне таке значення являє собою одну мережу і використовується для визначення діапазону адрес вузлів у ній.

225.	255.	224.	0
11111111.	11111111.	**111**00000.	00000000

00000000 = 0
00100000 = 32
01000000 = 64
01100000 = 96
10000000 = 128
10100000 = 160
11000000 = 192
11100000 = 224

Спосіб 2

Описаний вище спосіб визначення адрес підмереж неефективний, якщо під маску підмережі відводиться більше 4 бітів. У такому випадку доведеться виписувати і перетворювати велику кількість бітових комбінацій. Для швидкого визначення діапазону адрес підмереж використовується другий спосіб.

1. Записують одиницями кількість бітів, які необхідні для адрес підмереж, і доповняють їх справа нулями до одного байта.

Наприклад, якщо використовуються 3 біти для адрес підмереж, то це значення можна записати як 11100000.

2. Перетворюють найменш значущий біт на десяткове число. Виходить прирощення для кожної чергової підмережі.

У попередньому прикладі воно дорівнює 32.

3. Починаючи з нуля і до 256, виписують послідовно одержувані за допомогою збільшення значення.

2.3.4 Визначення адрес вузлів у підмережі

При адресації вузлів необхідно враховувати ті обмеження, які вносяться особливим призначенням деяких IP-адрес. Так, номер вузла не може складатися тільки з одних двійкових одиниць або тільки з одних двійкових нулів.

Звідси випливає, що максимальна кількість вузлів для кожної підмережі на практиці має бути зменшена на 2. Якщо відомо необхідне для адреси вузлів число біт, то можна піднести число 2 до степеня, що дорівнює числу біт, а потім відняти від отриманого значення 2, тобто 2^{13}-2 = 8190.

Діапазон адрес вузлів у підмережі можна визначити за допомогою короткої процедури. Кожне чергове значення адреси підмережі, збільшене на одиницю, не що інше, як початок діапазону адрес вузлів у підмережі. Наступне можливе значення адреси підмережі, зменшене на 2 одиниці, дає кінцеве значення діапазону допустимих адрес вузлів.

У таблиці 2.4 наведені допустимі діапазони адрес вузлів для мережі класу В у разі, коли для маски підмережі використовуються 3 біти.

Таблиця 2.4

Діапазони адрес вузлів для мережі класу В з маскою 255.255.224.0

№ п/п	Адреса підмережі	Діапазон допустимих адрес вузлів у підмережі
1.	x.y.00000000.0 = x.y.0.0	x.y.0.1 – x.y.31.254
2.	x.y.00100000.0 =x.y.32.0	x.y.32.1 – x.y.63.254
3.	x.y.01000000.0 = x.y.64.0	x.y.64.1 – x.y.95.254
4.	x.y.01100000.0 = x.y.96.0	x.y.96.1 – x.y.127.254
5.	x.y.10000000.0 = x.y.128.0	x.y.128.1 – x.y.159.254
6.	x.y.10100000.0 = x.y.160.0	x.y.160.1 – x.y.191.254
7.	x.y.11000000.0 = x.y.192.0	x.y.192.1 – x.y.223.254
8.	x.y.11100000.0 = x.y.224.0	x.y.224.1 – x.y.255.254

Широкомовною буде адреса, у якій усі біти поля номера пристрою встановлені в одиницю, тобто він на одиницю менше наступного по порядку можливого значення адреси підмережі.

Наприклад, для підмережі №3 широкомовна адреса x.y.95.255.

2.4 Питання для підготовки до захисту лабораторної роботи

1. Скільки біт необхідно використати для маски підмережі?
2. Який запас на випадок появи додаткових мереж необхідно залишити?
3. Який запас на випадок збільшення числа вузлів необхідно залишити?
4. Якщо треба 12 підмереж класу С, то яку маску підмережі слід використати?
5. Яка частина IP-адреси 200.12.135.14 являє собою вузол за наявності маски підмережі за умовчанням?

3 ЛАБОРАТОРНА РОБОТА № 3
ОРГАНІЗАЦІЯ ПІДМЕРЕЖ ЗА ДОПОМОГОЮ МАСКИ ЗМІННОЇ ДОВЖИНИ (VLSM)

3.1 Мета лабораторної роботи

Навчитися розбивати мережу на підмережі за допомогою маски змінної довжини VLSM, а також визначати адреси підмереж і діапазон IP-адрес вузлів для підмереж. Присвоювати інтерфейсам обладнань та вузлів адреси згідно з розрахованою топологією.

3.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки до даної роботи, такі питання:

- правила переходу з двійкової системи числення в десяткову та навпаки;
- IP-адресація в мережах;
- використання масок змінної довжини VLSM в IP-адресації.

Згідно з варіантом скласти схему IP-адресації поділу мережі організації як у лабораторній роботі № 2, використовуючи метод VLSM.

Для цього спочатку визначається підмережа, що належить до найбільшого сегмента або сегментів мережі. Їй присвоюється перша доступна підмережа цієї мережі. У таблицю 3.1 необхідно занести відповідні дані.

Тепер визначається підмережа, що належить до наступного за розміром сегмента або сегментів мережі і також присвоюється доступна підмережа цієї мережі.

Так треба продовжувати поділ підмереж відповідного розміру на підмережі до тих пір, поки не буде досягнута потрібна кількість вузлів у кожній підмережі. Відповідні результати необхідно подати у вигляді таблиці (таблиця 3.1).

Призначте підмережу для кожного з каналів між маршрутизаторами. Починати треба з наступної підмережі.

Заповніть таблицю 3.2 відповідними адресами.

Таблиця 3.1

Підмережі організації

Назва підмережі	Необхідна кількість вузлів	Виділена кількість вузлів	Адреса підмережі	Маска підмережі у десятковому форматі	Префікс	Діапазон допустимих IP-адрес вузлів	Широкомовна адреса
…	…	…	…	…	…	…	…

Таблиця 3.2

Підмережі каналів WAN між маршрутизаторами

Адреса підмережі	Маска підмережі у десятковому форматі	Префікс	Діапазон допустимих IP-адрес вузлів	Широкомовна адреса
Канал WAN_N1 між маршрутизаторами Router_A та Router_B				
…	…	…	…	…
Канал WAN_N2 між маршрутизаторами Router_A та Router_C				
…	…	…	…	…

Заповніть таблицю 3.3 відповідними IP-адресами для інтерфейсів маршрутизаторів. Використовуйте першу доступну IP-адресу вузла для LAN інтерфейсу маршрутизатора.

Таблиця 3.3

IP-адреси інтерфейсів маршрутизаторів

Пристрій	Інтерфейс	IP-адреса	Маска підмережі у десятковому форматі
Router_A	fa0/0		
	fa0/1		
	s0/0/0		
	s0/0/1		
Router_B	fa0/0		
	fa0/1		
	s0/0/0		
Router_C	fa0/0		
	fa0/1		
	s0/0/0		

Для зображення кожної локальної мережі (LAN_N1 – LAN_N6) використовуйте по одній робочій станції. Заповніть таблицю 3.4 відповідними IP-адресами для кожної робочої станції.

Таблиця 3.4

IP-адреси робочих станцій у підмережах

Підмережа	IP-адреса вузла	Маска підмережі	Адреса шлюзу
LAN_N1			
LAN_N2			
LAN_N3			
LAN_N4			
LAN_N5			
LAN_N6			

Дайте відповіді на такі питання та порівняйте з відповідями лабораторної роботи № 2:

– кількість необхідних підмереж;
– кількість необхідних IP-адрес;
– кількість IP-адрес, які необхідні для найбільшої мережі LAN;
– кількість IP-адрес, які необхідні для другої найбільшої мережі LAN;
– кількість IP-адрес, які необхідні для найменшої мережі LAN;
– кількість IP-адрес, які необхідні для кожного каналу WAN між маршрутизаторами;
– кількість IP-адрес, які доступні у початковій і поділеній мережах;
– відсоток адресного простору, що використовується в початковій і поділеній мережах.

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– тему і мету лабораторної роботи;
– опис завдання, що включає початкові умови та дані;
– відповіді на питання;
– таблиці розподілу адрес підмереж LAN_N1 – LAN_N6 (таблиця 3.1);
– таблицю призначення IP-адрес підмережам каналів WAN між маршрутизаторами (таблиця 3.2);
– таблицю призначення IP-адрес інтерфейсам маршрутизаторів (таблиця 3.3);
– таблицю призначення IP-адрес робочім станціям в підмережах LAN_N1 – LAN_N6 (таблиця 3.4);
– схему топології мережі із застосуванням методу VLSM.

3.3 Теоретичні відомості

3.3.1 Підмережі змінної довжини

У 1987 році документом RFC 1009 був визначений порядок використання декількох масок у мережі, яка розділена на підмережі.

В цьому випадку маски підмереж мають різну довжину і називаються масками підмереж змінної довжини (VLSM – Variable Length Subnet Mask).

По суті метод VLSM передбачає поділ на підмережі адресного простору, який заснован на використанні класів. Але потім підмережі поділяються на підмережі до тих пір, поки не буде досягнута необхідна кількість вузлів у кожній підмережі.

Реалізацію VLSM часто називають «підмережі на підмережі».

При використанні методу VLSM вводиться ряд нових правил.

По-перше, застосовується новий стиль запису масок підмережі через пряму косу риску (/). Він передбачає вказівку після IP-адреси розширеного мережевого префікса, тобто після прямої косої риски зазначається кількість бітів (одиниць, що підряд йдуть) у масці замість запису маски в точково-десятковому вигляді.

Наприклад, мережу 172.24.100.45 з маскою 255.255.0.0 можна записати як 172.24.100.45/16.

Цей запис набагато компактніший і зручніший.

По-друге, дозволено застосовувати до різних частин мережі різні маски. Це дає можливість у разі потреби розділяти мережу на менші частини. Єдина вимога при цьому полягає в тому, щоб діапазони адрес у підмережах не перекривали одна одну.

3.3.2 Приклад розрахунку підмереж за допомогою маски VLSM

Організації виділили діапазон адрес 172.16.0.0/16. Необхідно мати декілька окремих IP-підмереж для різних підрозділів організації, а саме:

- мережу розміром до 1000 вузлів для операційного відділу;
- мережу розміром у 250 вузлів для користувачів, які підключаються до офісної мережі за допомогою модемного з’єднання;
- мережу розміром у 100 вузлів у презентаційній залі для користувачів ноутбуків з Wi-Fi;
- три мережі розміром від 40 до 60 вузлів для різних відділів компанії та віддалених офісів;
- п’ять мереж по 2 вузла в кожній для з’єднання типу «точка-точка» між філіалами;
- мережу у 60 вузлів для мобільних користувачів, що застосовують VPN для доступу у корпоративну мережу під час відряджень.

Зробимо підсумок мереж, які містять у собі певну кількість вузлів:

- 1 мережа – 1000 вузлів;
- 1 мережа – 250 вузлів;
- 1 мережа – 100 вузлів;
- 4 мережі – по 60 вузлів кожна;
- 5 мереж – по 2 вузла кожна.

Таким чином, необхідно організувати 12 підмереж для 1600 користувачів.

Після організації підмереж на основі класу B з використанням, наприклад, розширеного мережевого префікса /22 буде отримано 64 підмережі й 1022 вузла в кожній підмережі.

Оскільки тільки в одній підмережі є 1000 вузлів, то в інших мережах потреба в розміщенні вузлів значно менша, і тому адреси використовуються неефективно. Це означає, що ця організація не використовує понад 63000 IP-адрес.

Основне вирішення цієї проблеми полягає у використанні маски підмережі змінної довжини VLSM, яка дасть можливість адміністратору створювати у рамках своєї організації підмережі необхідного розміру.

Загальна схема поділу мережі на підмережі з масками змінної довжини описана далі.

Спочатку мережа розділяється на підмережі максимально необхідного розміру. Потім деякі підмережі діляться на більш дрібні і рекурсивно далі до тих пір, поки це необхідно.

Відбувається свого роду рекурсія підмереж.

Таким чином, рекурсивний поділ адресного простору організації може бути виконаний з урахуванням побажань адміністратора мережі. Окрім рекурсії адрес підмереж, введення маски VLSM дозволяє значно зменшити об'єм таблиць маршрутизації на маршрутизаторах в організації.

Оскільки метод VLSM дозволяє виділяти підмережі розміром, піднесеним до двійки, в нашому прикладі доведеться ділити діапазон таким чином (з урахуванням того, що корисних адрес на два менше, ніж усього адрес у підмережі): 1x1024, 1x256, 1x128, 4x64, 5x4.

Щоб максимально ефективно використати адресний простір, рекомендується виділяти спочатку великі діапазони, потім – менші.

Для виділення переведемо адресу мережі організації у двійкове подання і відокремимо вже зафіксовану маскою частину (маємо намір не переводити незадіяну в операції частину, щоб не робити зайвих обчислень).

Вибираємо спочатку блок у 1024 адреси, розмір якого 2^{10}, і відрізаємо десять бітів справа:

172.16.000000|00.00000000

Заповнюємо "відрізану" частину одиницями й отримуємо кінець діапазону, тобто широкомовну адресу підмережі на 1024 адреси:

172.16.000000|11.11111111

Це підмережа – 172.16.0.0/22, широкомовна адреса – 172.16.3.255.

Продовжуємо. Збільшуємо останню адресу отриманої мережі на одиницю і виділяємо блок у 256 адрес:

172.16.00000100.|00000000

172.16.00000100.|11111111

Отримуємо підмережу 172.16.4.0/24 з діапазоном IP-адрес хостів 172.16.4.1–172.16.4.254 розміром у 254 адреси. Широкомовна адреса – 172.16.4.255.

Знову збільшуємо останню адресу отриманої мережі на одиницю і відрізаємо:

172.16.00000101.0|0000000
172.16.00000101.0|1111111

Отримуємо підмережу 172.16.5.0/25, діапазон 172.16.5.1–172.16.5.126 з числом адрес вузлів 126. Широкомовна адреса – 172.16.5.127.

Тепер нам треба аж 4 підмережі по 64 адреси:
172.16.00000101.10|000000
172.16.00000101.10|111111 – підмережа 172.16.5.128/26;

172.16.00000101.11|000000
172.16.00000101.11|111111 – підмережа 172.16.5.192/26;

172.16.00000110.00|000000
172.16.00000110.00|111111 – підмережа 172.16.6.0/26;

172.16.00000110.01|000000
172.16.00000110.01|111111 – підмережа 172.16.6.64/26, діапазон адрес вузлів 172.16.6.65–172.16.6.126, широкомовна адреса – 172.16.6.127.

І ще 5 мереж по 4 адреси:
172.16.00000110.100000|00
172.16.00000110.100000|11 – підмережа 172.16.6.128/30;

172.16.00000110.100001|00
172.16.00000110.100001|11 – підмережа 172.16.6.132/30;

172.16.00000110.100010|00
172.16.00000110.100010|11 – підмережа 172.16.6.136/30;

172.16.00000110.100011|00
172.16.00000110.100011|11 – підмережа 172.16.6.140/30;

172.16.00000110.100100|00
172.16.00000110.100100|11 – підмережа 172.16.6.144/30, діапазон адрес вузлів 172.16.6.145–172.16.6.146, широкомовна адреса – 172.16.4.147.

У результаті використано 1684 $(1024+256+128+4\times64+5\times4)$ адреси в поділеній мережі методом VLSM замість 65536 адрес початкової мережі.

Таким чином, використано в 39 разів менше або 2% доступного адресного простору початкової мережі.

3.4 Питання для підготовки до захисту лабораторної роботи

1. Яким чином за допомогою методу VLSM можна збільшувати кількість адрес?
2. Які переваги дає метод VLSM?
3. Що таке розширений мережевий префікс?
4. Визначте маску підмережі, що відповідає діапазону IP-адрес від 128.71.64.1 до 128.71.79.254.
5. Яка частина IP-адреси 200.12.135.14 являє собою вузол за наявності маски підмережі за умовчанням?

4 ЛАБОРАТОРНА РОБОТА № 4
РОЗРАХУНОК СУМАРНОГО МАРШРУТУ (CIDR)

4.1 Мета лабораторної роботи

Навчитися розраховувати сумарний маршрут для кожного маршрутизатора. Виконати загальне підсумовування маршрутів, щоб Router_A міг передавати більш лаконічну таблицю маршрутизації постачальнику послуг Інтернету.

4.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки до даної роботи, такі питання:

– створення супермережі;
– підсумовування маршрутів;
– використання технології CIDR у маршрутизації;
– правила розрахунку сумарних маршрутів.

Розрахувати сумарний маршрут для кожного маршрутизатора згідно з даними топології, яка получена в лабораторній роботі № 3.

Необхідно почати з маршрутизатора Router_B. Обчислити сумарний маршрут і дані занести у таблицю 4.1.

Далі заповнити таблицю 4.2 для Router_C . Потім розрахувати сумарний маршрут для Router_A – таблиця 4.3.

Маршрутизатор Router_A виконає підсумовування своєї власної мережі на інтерфейсах FastEthernet та Serial, а також зможе підрахувати сумарні маршрути від Router_B та Router_C.

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– тему і мету лабораторної роботи;
– опис завдання, з початковими умовами та даними;

– розраховані сумарні маршрути для маршрутизаторів мережі організації, які подані у вигляді відповідних таблиць (таблиці 4.1–4.3);

– IP-адресу мережі організації на маршрутизаторі SPN.

Таблиця 4.1

Таблиця підсумовування для Router_B

Router_B	Адреси підмереж у десятковому форматі	Адреси підмереж у двійковому форматі	Префікс
fa0/0			
fa0/1			
Сумарний маршрут			

Таблиця 4.2

Таблиця підсумовування для Router_C

Router_C	Адреси підмереж у десятковому форматі	Адреси підмереж у двійковому форматі	Префікс
fa0/0			
fa0/1			
Сумарний маршрут			

Таблиця 4.3

Таблиця підсумовування для Router_A

Router_A	Адреси підмереж у десятковому форматі	Адреси підмереж у двійковому форматі	Префікс
fa0/0			
fa0/1			
serial 0/0/0			
serial 0/0/1			
Сумарний маршрут від Router_B			
Сумарний маршрут від Router_C			
Сумарний маршрут			

4.3 Теоретичні відомості

У сучасних маршрутизаторах застосовується особливий тип IP-адрес, що називаються адресами безкласової міждоменної маршрутизації (Classless Inter-Domain Routing, CIDR).

У цих адресах не використовується поняття класу мережі. Концепція безкласової міждоменної маршрутизації була офіційно документована у вересні 1993 року в RFC 1517-1520. Її поява викликана кризами, що почастішали, в мережі Internet.

Ця технологія дозволяє:

– економніше й ефективніше використовувати адресний простір за рахунок того, що постачальники послуг можуть більш точно видавати блоки адрес відповідно до вимог клієнта;

– зменшити кількість записів у таблицях маршрутизації за рахунок підсумовування маршрутів, що називається створенням супермереж (supernetting).

При цьому один запис у таблиці маршрутизації може становити сотні адрес, що зменшує використання смуги пропускання для оновлень маршрутизації і приводить до прискорення пошуку в таблицях.

Основний принцип методу CIDR полягає в тому, що поняття класу вже не застосовується. Метод CIDR замість традиційних класів адрес протоколу IP використовує розширений мережевий префікс.

У CIDR кожен елемент маршрутної інформації рекламується маршрутизаторами спільно з мережевим префіксом. Маршрутизатори, що підтримують метод CIDR, не перевіряють клас адреси звичайними методами, замість цього вони покладаються на інформацію про мережевий префікс, що прийшла з рекламованим маршрутом.

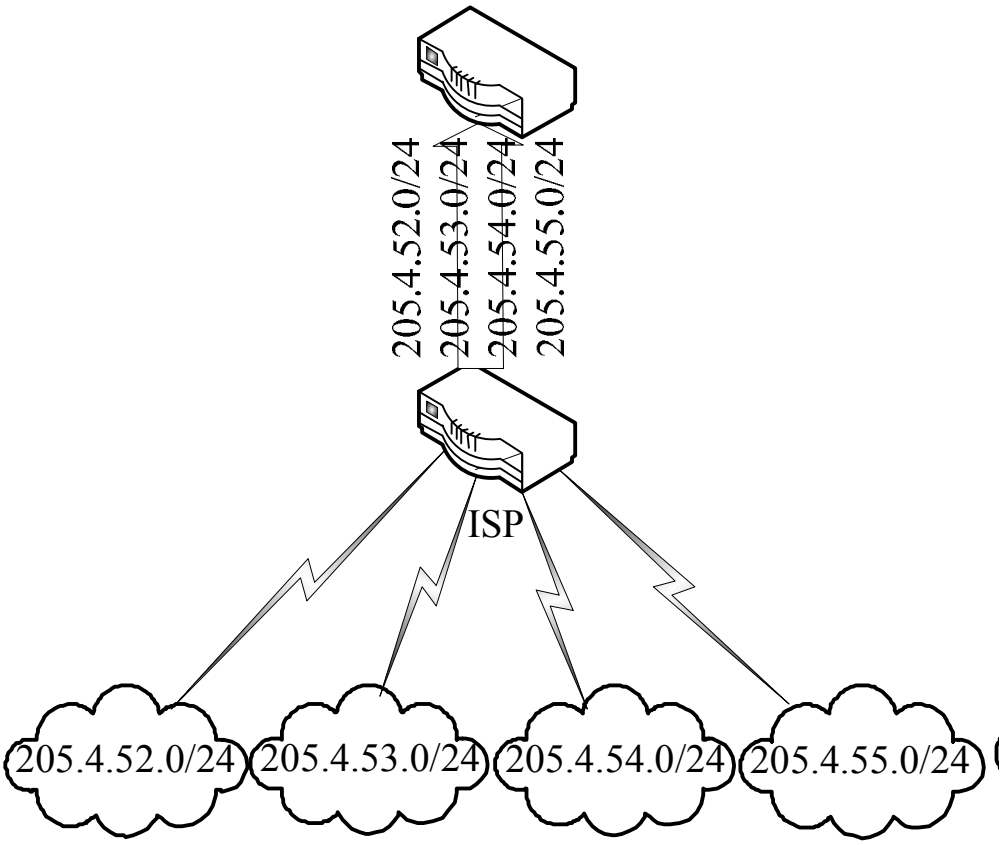
Неодмінною умовою застосовності CIDR є наявність в організації, що розпоряджається адресами, безперервних діапазонів адрес. Нині класова модель вважається застарілою. Маршрутизація, а також видача блоків IP-адрес (переважно) здійснюються за моделлю CIDR, хоча класи мереж ще міцно утримуються в термінології.

Схема адресації VLSM і CIDR дозволяє використовувати підсумовування маршрутів, що скорочує кількість записів в оновленнях маршрутизації і записів у локальних таблицях.

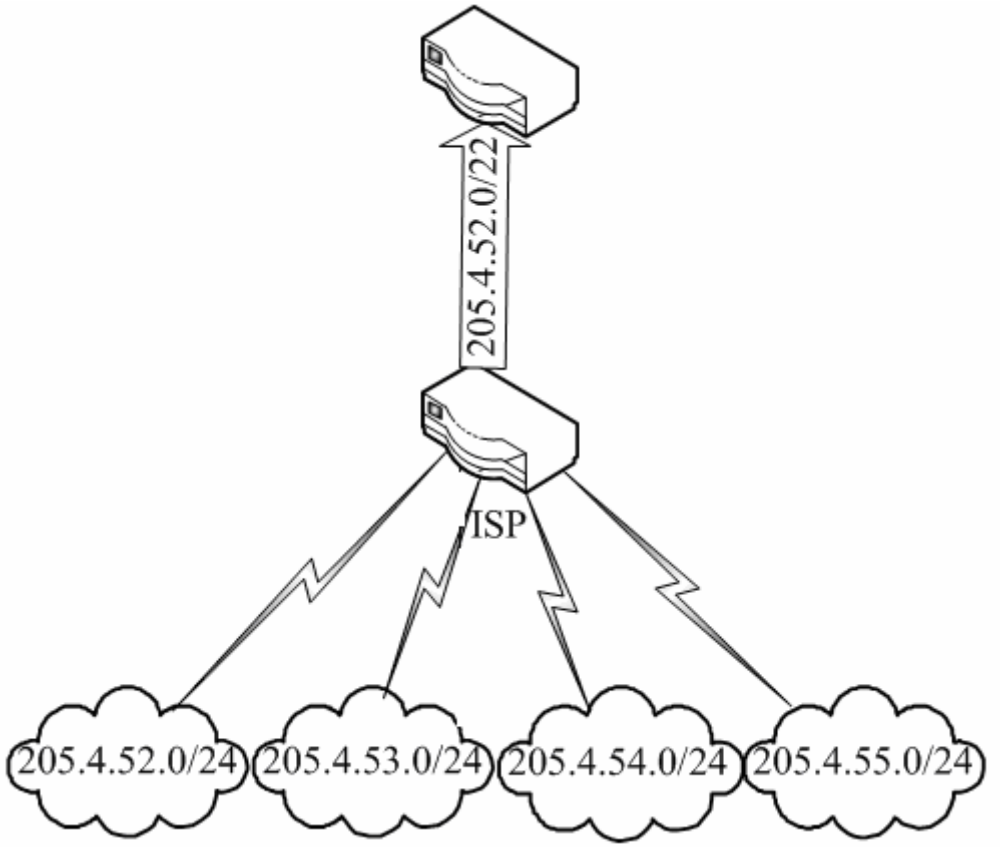
Процес організації супермереж протилежний процесу розділення мережі на підмережі. Замість того, щоб збільшуватися, кількість бітів у масці постійно зменшується. Це дозволяє об'єднати дрібніші суміжні мережі разом. Підсумовування маршрутів, що також називається об'єднанням або агрегацією маршрутів, відбувається на межі мережі граничного маршрутизатора.

Без CIDR і підсумовування маршрутів маршрутизатор повинен містити індивідуальну інформацію для всіх підмереж.

Наприклад, на рисунку 4.1, а показано, що компанія отримала у провайдера ISP чотири мережі класу C, адреси в яких безперервні: 205.4.48.0/24, 205.4.52.0/24, 205.4.56.0/24 і 205.4.60.0/24.



а)



б)

Рисунок 4.1 – Надання компанії адрес мережі без використання CIDR на маршрутизаторі (а), з використанням CIDR (б)

Перші 24 біти являють собою адресу підмережі.

Оскільки перші 24 біти адреси кожної з цих чотирьох підмереж унікальні, то класовий маршрутизатор бачить чотири унікальних мережі й повинен створити в таблиці рядок маршрутів для кожної з цих підмереж (таблиця 4.4).

Таблиця 4.4

Таблиця маршрутів

Адреса підмереж у десятковому форматі	Адреса підмереж у двійковому форматі			
205.4.52.0/22	11001101	00000100	00110100	00000000
205.4.53.0/22	11001101	00000100	00110101	00000000
205.4.54.0/22	11001101	00000100	00110110	00000000
205.4.55.0/22	11001101	00000100	00110111	00000000

Проте ці чотири адреси підмереж мають загальну частину (однакові перші 22 біти).

CIDR – сумісний маршрутизатор, може підсумовувати маршрути до цих чотирьох підмереж, використовуючи загальний 22-бітовий префікс в адресах (11001101 0000100 001101).

Для подання цього префікса в десятковій формі доповнимо його справа нулями:

11001101 00000100 00110100 00000000 = 205.4.52.0.

22-бітова маска підмережі буде мати вигляд:

11111111 11111111 11111100 00000000 = 255.255.252.0.

Отже, одна адреса й одна маска визначають безкласовий префікс, який підсумовує маршрути чотирьох підмереж: 205.4.52.0/22.

Провайдер ISP надає мережу компанії зовнішньому світу як мережу 205.4.52.0/22 (рисунок 4.1, б).

CIDR дозволяє провайдерам ефективно розподіляти і підсумовувати безперервні простори IP-адрес.

Слід звернути увагу, що таке підсумовування маршрутів можливе тільки у тому випадку, якщо всі маршрутизатори в мережі використовують безкласовий протокол маршрутизації, наприклад OSPF, RIPv2 або EIGRP.

4.4 Питання для підготовки до захисту лабораторної роботи

1. Як CIDR і VLSM сприяють економному використанню адресного простору?

2. Які завдання виконує маршрутизація CIDR?

3. Що є неодмінною умовою застосовування CIDR?

4. Чи можливо для мережі класу С використати префікс /20?

5. Що таке підсумовування маршрутів і як воно сприяє зменшенню таблиць маршрутів на маршрутизаторах?

ПЕРЕЛІК ПОСИЛАНЬ

1. Буров, Є. Комп‘ютерні мережі [Текст] / Є. Буров. – Л.: БаК, 2003. – 584 с.

2. Закер, К. Компьютерные сети. Модернизация и поиск неисправностей [Текст]: пер. с англ. / К. Закер. – С.Пб.: БХВ-Петербург, 2001. – 1008 с.

3. Ногл, М. TCP/IP. Иллюстрированный учебник [Текст] / М. Ногл. – М.: ДМК Пресс, 2001. – 480 с.

4. Лайден, К. TCP/IP [Текст]: учеб. пособие [пер. с англ.] / К. Лайден, М. Виленски. – 3-е изд. – М.: Вильямс, 2001. – 432 с.

5. Крейг, Х. Персональные компьютеры в сетях TCP/IP [Текст] / Х. Крейг. – К.:BHV, 1997. – 384 с.

6. Олифер, Е.Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. для вузов / Е.Г. Олифер, Н.А. Олифер. – 3-е изд. – С.Пб.: Питер, 2006. – 958 с.

7. Гук, М. Аппаратные средства локальных сетей [Текст]: энциклопедия / М. Гук. – С.Пб.: Питер, 2005. – 573 с.

Панферова Яна Володимирівна
Кмітіна Ірина Вячеславівна
Цвіркун Леонід Іванович

КОМП'ЮТЕРНІ МЕРЕЖІ. МЕТОДИЧНІ ВКАЗІВКИ ДО ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ СТУДЕНТАМИ НАПРЯМУ ПІДГОТОВКИ 6.050102 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Редактор Ю.В. Рачковська

Підписано до друку 24.01.12. Формат 30х42/4.
Папір офсет. Ризографія. Ум. друк. арк. 1,8.
Обл.-вид. арк. 1,72. Тираж 60 пр. Зам. №

Державний ВНЗ "Національний гірничий університет".
49005, м. Дніпропетровськ, просп. К. Маркса, 19.