Лабораторна робота 4.
Адресація в TCP/IP-мережах. Багатоадресне розсилання

Мета роботи: ознайомлення та засвоєння типів адрес, які використовуються для ідентифікації хост-модулів комп'ютерних мереж, структури IP-адреси, особливостей багатоадресного розсилання.

План виконання лабораторної роботи

1. Ознайомитися з теоретичними відомостями, що викладені в методичному посібнику до лабораторної роботи та засвоїти їх.
2. Виконати завдання до лабораторної роботи.

1. ТЕОРЕТИЧНІ ВІДОМОСТІ

Стек протоколів TCP/IP призначений для об'єднання окремих підмереж, побудованих за різними технологіями канального та фізичного рівнів (Ethernet, Token Ring, FDDI, ATM, X.25 і т.д.) в одну об'єднану мережу. Кожна з технологій нижнього рівня має свою схему адресації. Тому на міжмережевому рівні потрібний один спосіб адресації, який дозволяє унікально ідентифікувати кожний вузол об'єднаної мережі. Таким способом у TCP/IP-мережах є IP- адресація.

Вузол об'єднаної мережі, який має IP-адресу, називається хостом (host).

В стеку TCP/IP протоколами різних рівнів використовуються наступні три типи адрес:

- символьні (доменні) імена;
- IP-адреси (логічні, мережеві);
- локальні (фізичні, апаратні).

Символьні доменні імена (domain name) застосовуються для зручності представлення IP-адрес. Людині незручно запам'ятовувати числові IP-адреси, тому була розроблена спеціальна служба DNS (Domain Name System), яка встановлює відповідність між IP-адресами і символьними доменними іменами.

IP-адреси (IP address) - це основний тип адрес, користуючись яким мережевий рівень передає повідомлення, які називаються IP-дейтаграмами (IP- пакетами). Ці адреси мають довжину 4 байти (для протоколу IPv4), які записуються в десятковому вигляді і значення байтів розділяються крапками, наприклад, 117.52.9.44. IP-адреса вузла в протоколі IP призначається незалежно від локальної адреси вузла. Маршрутизатор зазвичай входить відразу в кілька мереж. Тому кожен порт маршрутизатора має власну IP-адресу. Кінцевий вузол також може входити в декілька IP-мереж. У цьому випадку робоча станція повинна мати кілька IP-адрес, за кількістю мережевих адаптерів. Таким чином, IP-адреса характеризує не

окремий хост-вузол або маршрутизатор, а частину адреси одного мережевого з'єднання.

Локальна (фізична) адреса - це адреса, присвоєна вузлу відповідно до технології підмережі, яка входить в об'єднану мережу. Якщо мережею або сегментом є локальна мережа Ethernet, Token Ring або FDDI, то локальна адреса - це MAC-адреса (Media Access Control address).

MAC-адреси призначаються мережевим адаптерам і портам маршрутизаторів виробниками обладнання і є унікальними, оскільки розподіляються централізовано. MAC-адреса має, зазвичай, довжину 6 байтів і записується в шістнадцятковому вигляді, наприклад, OO-O8-AO-12-5F-72 або 00:08:A0:12:5F:72.

1.1. Структура IP-адреси

IP-адреса - це 32-розрядне двійкове число, розділене на групи по 8 біт, які називаються октетами, наприклад: 00010001 11101111 00101111 01011110

Зазвичай IP-адреси записуються у вигляді чотирьох десяткових октетів, які розділяються крапками. Таким чином, приведену вище IP-адресу можна записати у такій формі: 17.239.47.94.

Слід зауважити, що максимальне значення октету дорівнює (у двійковій системі) 11111111, що відповідає числу 255 в десятковій системі. Тому IP- адреси, в яких хоча б один октет перевищує це число, є недійсними.

Приклад: 172.16.123.1 - допустима адреса, 172.16.123.256 - недійсна адреса, оскільки 256 виходить за межі допустимого діапазону. IP-адреса складається із двох логічних частин - номеру (ідентифікатору) мережі і номеру (ідентифікатору) вузла в цій мережі. При передачі пакету із однієї мережі в іншу використовується тільки та частина IP-адреси, яка містить номер мережі. Коли пакет надходить у мережу призначення, адреса вузла вказує на конкретний вузол у цій мережі.

Щоб записати ID мережі, в поле номера вузла в IP-адресі записують нулі. Щоб записати ID хосту, в поле номера мережі записують нулі. Наприклад, якщо в IP-адресі 172.16.123.1 перші два байти відводяться під номер мережі, останні два байти - під номер вузла, то номери записуються наступним чином: ID підмережі: 172.16.0.0. ID хосту: 0.0.123.1.

По кількості розрядів, які відводяться для номера вузла (або номера мережі), можна визначити загальну кількість вузлів (або мереж): якщо число розрядів для номера вузла дорівнює N, то загальна кількість дорівнює 2^N - 2. Два вузли віднімаються внаслідок того, що адреси з усіма розрядами, що дорівнюють нулю або одиниці, є особливими і використовуються зі спеціальною метою.

Наприклад, якщо під номер вузла в деякій підмережі відводиться два

байти, то загальна кількість вузлів у такій підмережі дорівнює 2^{16} - 2 =65534 вузли.

Для визначення того, яка частина IP-адреси відповідає за ID мережі, а яка за ID хосту, використовуються два способи: за допомогою класів і за допомогою масок. Загальне правило: під ID мережі відводяться перші кілька бітів IP-адреси, біти, які залишилися, визначають ID хосту.

Існує п’ять класів IP-адрес: A, B, C, D і E (рис. 4.1). За приналежність до того чи іншого класу відповідають перші біти IP-адреси, які часто називають

ключем, який містить від 1 до 5 бітів. Результатом такого розподілу стало створення невеликої кількості великих мереж (класу А) з дуже великою кількістю хост-вузлів, помірної кількості середніх мереж (клас В) зі значною кількістю кінцевих вузлів, і великої кількості мереж (клас С) з невеликою кількістю хост-вузлів. Три з них (А, В, С) використовуються для адресації мереж, а два (D, E) мають спеціальне призначення.

Рисунок 4.1 - Класи IP-адрес

В таблиці 4.1 представлено основні показники мереж всіх класів. Повний діапазон адрес, які можуть мати хост-вузли, що підключаються до мереж відповідного класу, наступні:

клас А 1.0.0.1 - 126.255.255.254,

клас В 128.1.0.1 - 191.254.255.254,

клас С 192.0.1.1 - 223.255.254.254.

Таблиця 4.1 - Характеристика IP-адрес різних класів

Клас	Формат	Шаблон перших біт (ключ) першого октету	Десяткові значення першого байту адреси мережі	Максимальна кількість мереж	Максимальна кількість вузлів в одній мережі
A	Net.Node.Node.Node	0	1 - 126	126 (2^7-2)	16777214 (2^{24}-2)
B	Net.Net.Node.Node	10	128 - 191	16382 (2^{14}-2)	65532 (2^{16}-2)
C	Net.Net.Net.Node	110	192 - 223	2097150 (2^{21}-2)	254 (2^8-2)
D	-	1110	224 - 239	-	-
E	-	11110	240 - 247	-	-

Протокол IP підтримує три способи адресації:

- індивідуальну (unicast);

- групову (multicast);
- широкомовну (broadcast).

При **одиничній адресації** дейтаграми передаються конкретному одиничному пристрою.

При **широкомовній адресації** повідомлення надсилають одну дейтаграму, що доставляється всім пристроям мережі. Якщо широкомовний трафік призначений тільки для вузлів локальної мережі, то його реалізація не викликає особливих ускладнень. Якщо ж повідомлення необхідно передати в іншу мережу, то в цьому випадку глобальна мережа повинна мати значну пропускну спроможність.

При **груповій адресації** дейтаграмми доставляються певній групі пристроїв. При цьому не генерується надлишковий трафік, що особливо важливо при роботі в розподілених мережах. Дейтаграми із груповою та одиничною адресою розрізняються адресою. В заголовку IP-дейтаграми із груповою адресацією замість IP-адрес класів A, B, C записується адреса класу D, тобто групова адреса. **Групова адреса** призначається деяким пристроям-одержувачам (групі пристроїв). Відправник записує дану групову адресу в заголовок IP- дейтаграми. Дейтаграма буде доставлена всім членам групи. Перші чотири біти адреси класу D дорівнюють 1110, іншу частину адреси (28 біт) займає ідентифікатор групи.

Групові адреси лежать у діапазоні від 224.0.0.0 до 239.255.255.255. Наприклад, групові адреси, що використовуються в Інтернет, лежать у діапазоні 224.0.1.0 - 238.255.255.255, локальні групові адреси - в діапазоні 239.0.0.0 - 239.255.255.255, а зарезервовані групові адреси лежать у діапазоні 224.0.0.0 - 224.0.0.255. Зокрема, цей останній діапазон відведений протоколам маршрутизації та іншим низькорівневим протоколам. У таблиці 4.2 наведені деякі зарезервовані IP-адреси класу D.

В локальних мережах LAN (Local Area Network) використовуються **приватні IP-адреси** *(private IP address*), які називають також ***внутрішніми, внутрішньомережними, локальними або «сірими».*** Це IP-адреси, які належать до спеціального діапазону, що не використовується в Internet. Такі адреси використовуються в локальних мережах, і їх розподілення ніким не контролюється. До таких адрес відносяться:

10.0.0.1 - 10.255.255.254 (маска підмережі при безкласовій адресації 255.0.0.0 або префікс */8);

172.16.0.1 - 172.31.255.254 (маска підмережі при безкласовій адресації 255.240.0.0 або префікс */12);

192.168.0.1 - 192.168.255.254 (маска підмережі при безкласовій адресації 255.255.0.0 або префікс */16).

На сьогодні класова адресація «в чистому вигляді» не використовується, оскільки призводить до неефективного розподілу адресного простору, суттєвого збільшення розміру таблиць маршрутизації і, як наслідок, збільшення часу

доставки повідомлень. Для вирішення цих проблем використовують структуризацію мереж, тобто виділення підмереж. При цьому в деякій мережі будь-якого класу виділяються окремі області, підмережі, які повинні мати свої ідентифікатори (адреси).

Таблиця 4.2 - Зарезервовані адреси класу D

Адреса	Призначення
224.0. 0.0	Базова адреса мультикасту (зарезервована)
224.0. 0.1	Всі пристрої підмережі (даного сегменту мережі)
224.0. 0.2	Всі маршрутизатори підмережі
224.0. 0.4	Всі DVMRP-маршрутизатори
224.0. 0.5	Всі MOSPF-маршрутизатори сегменту мережі
224.0. 0.6	Всі DR-маршрутизатори сегменту мережі
224.0. 0.7	Аудіоновини
224.0. 0.9	RIP версії II
224.0. 0.10	Всі EIGRP-маршрутизатори сегменту мережі
224.0. 0.11	IEFT аудіо
224.0. 0.12	IEFT відео
224.0. 0.13	Всі PIM-маршрутизатори сегменту мережі
224.0. 0.22	Всі IGMP-маршрутизатори сегменту мережі
224.0. 0.251	Мультикастова адреса DNS (mDNS)

1.1. **Виділення підмереж. Поняття маски**

Якщо разом з IP-адресою використовувати маску, то це дозволить виконувати адресацію більш гнучко і відмовитися від класової адресації. При цьому частину мережі називають підмережею. Для виділення підмережі маршрутизатору необхідно «накласти» маску підмережі на IP-адресу, що дозволить виділити в адресі ідентифікатори мережі, підмережі та кінцевого хост- вузла.

Виділення (створення) підмереж - це властивість програмного забезпечення IP створювати декілька нових підмереж з однієї великої мережі. В результаті організація має одну адресу і створює необхідну їй структуру для кожної фізичної мережі (сегменту). Для ідентифікації підмережі використовується старша частина IP-адреси, що призначена для адресації хост- вузлів (рис. 4.2).

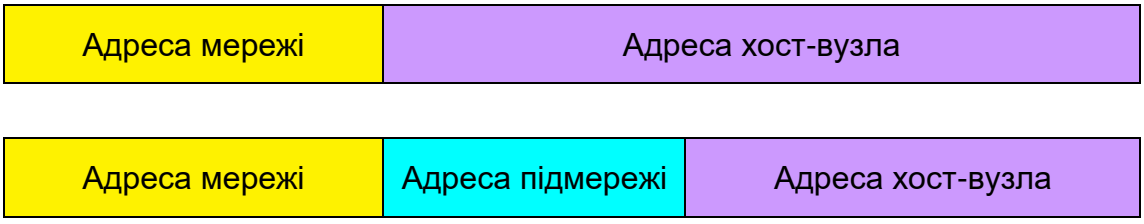


Рисунок 4.2 - Ідентифікація підмереж

Маска мережі та підмережі використовується для визначення того, які біти в IP-адреси визначають ідентифікатор мережі та підмережі, а які - ідентифікатор хост-вузла.

Маска являє собою 32-бітне слово, яке складається з послідовності «1», за якою йде послідовність «0»:

- «1» у масці визначають біти IP-адреси, в яких міститься ідентифікатор мережі та підмережі;
- «0» у масці визначають біти IP-адреси, в яких записаний ідентифікатор хост-вузла.

Наприклад, нехай для IP-адреси 172.16.155.5 задано маску 255.255.192.0. Двійковий вид відповідно такий:

- IP-адреса 10101100.00010000.10011011.00000101;
- маска 11111111.11111111.11000000.00000000.

Якщо ігнорувати маску й інтерпретувати адресу 172.16.155.5 на основі класів, то ідентифікатор мережі є 172.16.0.0, а вузла - 0.0.155.5 (оскільки адреса відноситься до класу B).

Якщо використовувати маску, то 18 послідовних одиниць у масці 255.255.192.0 після «накладання» на IP-адресу 172.16.155.5 ділять її на дві частини:

- ідентифікатор мережі 10101100.00010000.10;
- ідентифікатор вузла 011011.00000101.

У десятковій формі запис номера мережі і вузла після доповнення до 32 біт мають відповідно такий вигляд: 172.16.128.0 і 0.0.27.5.

Виділення з допомогою маски адреси мережі і хоста можна інтерпретувати як виконання логічної операції I (AND).

Для запису масок використовуються також такі формати запису з використанням префіксу, наприклад, 172.16.155.5/18 - 18 означає префікс, що вказує на кількість одиниць на початку маски.

1.2. **Загальні відомості про Multicast**

Існують такі типи мережевого трафіку (зауважимо, що не обов’язково використовуються всі чотири типи трафіку конкретною версією протоколу):

- **Unicast** - одноадресна розсилка - один відправник, один отримувач (наприклад, запит HTTP-сторінки у вебсервера);
- **Broadcast** - широкомовна розсилка - один відправник, отримувачі - всі пристрої в широкомовному сегменті (наприклад, ARP-запит);

- **Multicast** - багатоадресна розсилка - один відправник, багато отримувачів. (наприклад: IPTV);
- **Anycast** - одноадресна розсилка найближчому вузлу - один відправник, взагалі отримувачів багато, але фактично дані відправляються тільки одному (наприклад, Anycast DNS).

Основним принципом мультикастових розсилок є те, що відправник відправляє тільки одну копію трафіку, незалежно від кількості отримувачів, а трафік (потік даних) отримують тільки ті кінцеві системи, які дійсно зацікавлені в ньому.

Основне завдання групових запитів полягає в зменшенні навантаження на хости-вузли, які не приймають участі в роботі певного прикладного сервісу. При багатоадресному розсиланні відправник формує та відправляє один потік даних загальним маршрутом тим отримувачам, які підписані на цю розсилку. Перевага такого підходу полягає в тому, що додавання нових користувачів не вимагає збільшення пропускної здатності мережі загальним маршрутом до користувачів послуги, і відповідно, зменшується навантаження на проміжні модулі. При запуску на сервері застосування (додатку) з підтримкою групового розсилання, воно посилає в мережу повідомлення про те, що відповідна група доступна для приєднання. Клієнт, який бажає приєднатися до розсилки, посилає повідомлення про це. Всі проміжні маршрутизатори запам’ятовують, що за відповідним маршрутом знаходиться клієнт відповідної мультикастової групи.

Хост може належати одній або кільком групам. Якщо це можливо, мережева плата повідомляє, до якої групи належить хост, після чого мережева плата приймає тільки фрейми певної групи

Щоб технологія працювала, вона має підтримуватися сервером, клієнтом і усіма проміжними маршрутизаторами. Щоб комутатори направляли пакети тільки потрібним отримувачам, вони мають підтримувати IGMP snooping, в іншому випадку пакети розсилаються широкомовно. Також потрібно пам’ятати про те, що мультикаст може блокуватися міжмережевими екранами.

Недоліком групової розсилки є неможливість використання на транспортному рівні протоколу TCP. Використання протоколу UDP тягне за собою всі його недоліки: ненадійність доставки, відсутність засобів реагування на затори в мережі і т.д. Крім того, в окремих випадках при зміні маршрутів розсилки групові дейтаграми можуть втрачатися і дублюватися, і це має враховуватися застосуваннями.

Побудова об’єднаної мережі з підтримкою мультикастингу є набагато складнішим завданням, ніж організація групової розсилки в межах однієї мережі.

Якщо члени мультикастової групи знаходяться в різних мережах для

мультикастингу потрібна спеціальна власна маршрутизація. Тому для маршрутизації групових дейтаграм були розроблені спеціальні методи і протоколи маршрутизації.

Відзначимо, що не всі провайдери Internet підтримують багатоадресне з'єднання.

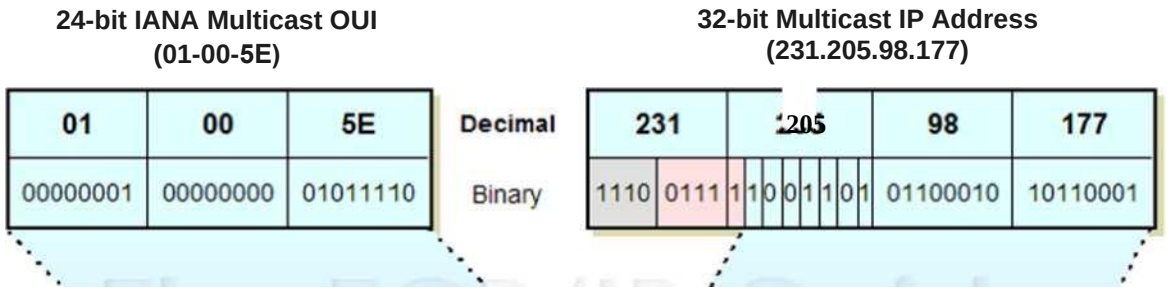
Для використання мультикастингу, він має підтримуватися в стеку TCP/IP сервера, клієнтів і проміжних маршрутизаторів. В локальних мережах за управління мультикаст-групами відповідає протокол IGMP (Internet Group Management Protocol), у глобальній мережі - протокол PIM (Protocol Independent Multicast).

Мультикастинг відбувається на канальному і мережевому рівнях. Для мультикастових груп зарезервовані адреси як на канальному, так і на мережевому рівнях.

В IPv4 для багатоадресної розсилки зарезервований діапазон адрес від 224.0.0.0 до 239.255.255.255(224.0.0.0/4), в IPv6 - ff00::/8. Адреси з цього діапазону можуть використовуватися тільки як адреси призначення, вони ніколи не можуть бути використані як адреси відправників.

Для визначення широкомовної MAC-адреси призначення в Ethemet-кадрах необхідно виконати додаткові кроки. При доставці unicast-повідомлень трафік направляється на унікальну MAC-адресу вузла призначення. Маршрутизатор дізнається про його MAC-адресу за допомогою протоколу визначення адрес ARP.

Для multicast-трафіка механізм визначення MAC-адрес модулів призначення інший. MAC-адреса багатоадресної розсилки - це особливе значення, яке в шістнадцятковому форматі починається з 01-00-5E (24 біти), а наступний 25-й біт повинен дорівнювати 0. Решта MAC-адреси багатоадресної розсилки створюється шляхом перетворення молодших 23 бітів IP-адреси групи багатоадресної розсилки в 6 шістнадцяткових (рис. 4.3, на якому показано відповідність IP-адреси 231.205.98.177 на мережевому рівні MAC-адресі 01:00:5E:4D:62:B1 на рівні Ethernet).



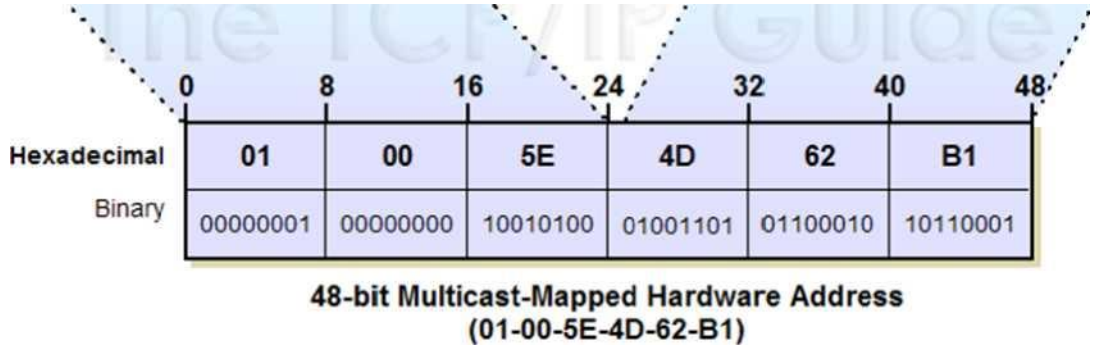


Рисунок 4.3 - Співвідношення мультикастних MAC- і IP-адрес

Оскільки при перетворенні IP-адреси в MAC-адресу втрачаються 5 бітів першого октету IP-адреси, отримана адреса не є унікальною. Кожній MAC-адресі

відповідають 32 IP-адреси групової розсилки. Це необхідно враховувати при призначенні IP-адрес багатоадресної розсилки.

В протоколі IPv6 при використанні багатоадресної передачі даних також необхідно, щоб кілька вузлів могли отримувати потік даних із загальною MAC- адресою. MAC-адреса групової передачі протоколу IPv6 починається з префіксу, який складається з 16 бітів - 0x33-33. Наступні 32 біти формуються із останніх 32 бітів ідентифікатора багатоадресної групи (*Group ID*). Наприклад: FF02::2 =33-33-00-00-00-02;
FF02:: 1:FF5C:B300= 33-33-FF-5C-B3-00

Групова адреса не ділиться на поля адреси мережі та вузла і опрацьовується маршрутизатором особливим чином.

В Windows переглянути членство в багатоадресних групах можна за допомогою команди: ***netsh interface ipv4 show joins.***

Загальні відомості про багатоадресну маршрутизацію

Багатоадресна розсилка забезпечує доставку потоку даних групі вузлів на IP-адресу групи багатоадресної розсилки. В цієї групи немає фізичних або географічних обмежень: вузли можуть знаходитися в будь-якому місці. Вузли, які зацікавлені в отриманні даних для певної групи, повинні приєднатися до цієї групи (підписатися на розсилку) за допомогою міжмережевого протоколу управління групами IGMP (Internet Group Management Protocol,). Після цього пакети багатоадресної розсилки, в полі призначення заголовку якого містяться групові адреси, будуть надходити на цей вузол і опрацьовуватися.

Кожна IP-адреса діапазону багатоадресного пересилання - це мультикастова група. Одна адреса - одна група, наприклад, IP-адресу 224.2.2.4 будуть отримувати тільки ті хости, які під'єднані до групи 224.2.2.4.

Протокол IGMP використовується клієнтським комп'ютером і сусідніми комутаторами для з'єднання клієнтського модуля і локального маршрутизатора, який здійснює групову передачу. Далі між локальним і віддаленими маршрутизаторами використовується протокол PIM (Protocol Independent Multicast), за допомогою якого груповий трафік направляється від сервера до численних клієнтів групової передачі.

Протокол IGMP реалізований у вигляді серверної і клієнтської частин, перша з яких виконується на маршрутизаторі, друга - на вузлі мережі, який отримує груповий трафік. Клієнт відправляє повідомлення про приналежність до якої-небудь групи локальному (найближчому) маршрутизатору, в цей час маршрутизатор перебуває в очікуванні повідомлень і періодично розсилає клієнтам запити (рис. 4.4).

Коли ініціюється багатоадресна передача, програмне забезпечення або сервіс створює багатоадресну групу. Ця адреса багатоадресної групи має IP- адресу з першим октетом у діапазоні 224-239 (клас D) і є адресою призначення для даного трафіку. Хост, який ініціює передачу, відправляє повідомлення (яке називається звітом про приналежність до IGMP) на адресу 224.0.0.2 (усім багатоадресним маршрутизаторам), вказуючи адресу багатоадресної групи. Комутатор отримує це повідомлення, додає багатоадресну групу у свою таблицю і додає порт прийому як учасника цієї групи. Він також пересилає цей звіт усім багатоадресним маршрутизаторам. Потім маршрутизатор додає ці хости в таблицю багатоадресної маршрутизації. Всі хости, які бажають стати учасниками групи, також відправляють повідомлення приєднання. Комутатор перехоплює ці повідомлення і додає порти прийому як учасників групи. Він також пересилає ці повідомлення багатоадресному маршрутизатору. Весь трафік, який відправляється на адресу призначення багатоадресного розсилання, направляється тільки на порти модулів, які є членами вказаної групи. Для того, щоб підтримувати інформацію про приналежність в актуальному стані, ініціатор IGMP-запиту продовжує відправляти запити приналежності. Всі хост-вузли, які бажають залишатися в групі, повинні відповідати на ці запити. Якщо хости, які входять у групу, не відповідають протягом встановленого часу, комутатор видаляє ці порти з таблиці групи. Після того як усі учасники будуть видалені з багатоадресної групи, комутатор видаляє адресу багатоадресної розсилки із своєї таблиці.

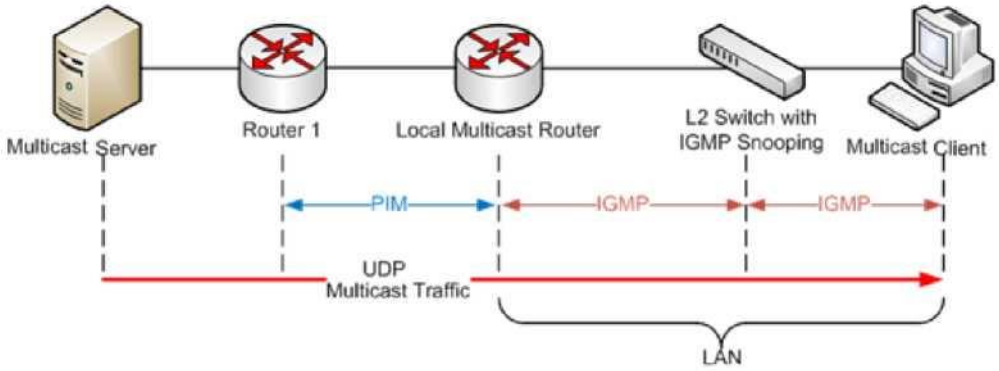


Рисунок 4.4 - Використання протоколів PIM і IGMP на ділянках мережі

Управління багатоадресною розсилкою на 2-му рівні моделі OSI (IGMP Snooping)

За замовчуванням, коли комутатор 2-го рівня отримує багатоадресний трафік, він починає передавати кадри на всі порти крім того, з якого надійшов цей кадр, оскільки в його таблиці комутації відсутній запис про багатоадресну MAC-адресу. Це не тільки недоцільно, але й може викликати проблеми на мережевих пристроях, змушуючи їх обробляти несподіваний для них потік даних.

Управління багатоадресною розсилкою на комутаторі 2-го рівня може бути виконане двома способами.

Перший спосіб полягає у створенні статичних таблиць комутації для портів, до яких під'єднані клієнти багатоадресних груп. Це дозволяє обмежити багатоадресний трафік і передавати його тільки через ті порти, до яких під'єднані вузли-підписники. Однак цей спосіб не дозволяє динамічно відслідковувати приєднання або вихід членів із багатоадресної групи. Іншим способом, який дозволяє вирішити проблему лавинної передачі багатоадресних пакетів і динамічно відслідковувати стан підписки вузлів, є функція IGMP- прослуховування (IGMP-Snooping).

IGMP Snooping - це функція другого рівня моделі OSI, яка дозволяє комутаторам вивчати членів багатоадресних груп, під'єднаних до його портів, прослуховуючи IGMP-повідомлення (запити і відповіді), які передаються між вузлами-підписниками і маршрутизаторами (або комутаторами рівня 3) мережі.

Коли вузол, який під'єднаний до комутатора, бажає ввійти в багатоадресну групу або відповідає на IGMP-запит, отриманий від маршрутизатора (або комутатора рівня 3) багатоадресної розсилки, він відправляє IGMP-відповідь, в якій вказана адреса багатоадресної групи. Комутатор аналізує інформацію в IGMP-відповіді і створює в своїй асоціативній таблиці комутації IGMP-Snooping (OIL) запис для цієї групи (якщо вона не існує). Цей запис зв'язує порт, до якого під'єднаний вузол-підписник, порт, до якого під'єднаний маршрутизатор (комутатор рівня 3)

багатоадресної розсилки, і MAC-адресу багатоадресної групи. Якщо комутатор отримує IGMP-відповідь для цієї ж групи від іншого вузла даного сегменту мережі, то він додає номер порту у вже існуючий запис асоціативної таблиці комутації IGMP Snooping (рис. 4.5).

Рисунок 4.5 - Використання IGMP Snooping на локальному комутаторі

Розглянемо приклад роботи функції IGMP Snooping у мережі, представленої на рисунку 4.6.

Комутатор L3 відправляє IGMP-запит про приналежність до групи комутатору L2, який розсилає його через усі порти, за виключенням порту-отримувача. ПК1 бажає приєднатися до багатоадресної групи 239.192.1.10 і відправляє IGMP-відповідь на адресу групи, вказуючи багатоадресну MAC- адресу призначення 0x01-00-5E-40-01-0A. Процесор комутатора L2 аналізує IGMP-відповідь і створює в асоціативній таблиці комутації IGMP Snooping (спочатку вона пуста) запис для MAC-адреси 0x01-00-5E-40-01-0A, що відповідає груповій адресі 239.192.1.10. Також у цей запис заноситься інформація про порти, до яких під’єднані ПК1 і комутатор L3.

ПК2 також бажає вступити в багатоадресну групу 239.192.1.10 і відправляє IGMP-відповідь на адресу групи, не очікуючи отримання чергового IGMP- запиту. Комутатор L2 аналізує IGMP-відповідь і додає *порт* 10, до якого під'єднаний ПК 2, у вже існуючий запис для MAC-адреси 0x01-00-5E-40-01-0A.

В результаті порти 1, 10 і 25 асоційовані з багатоадресною MAC-адресою 0x01-00-5E-40-01-0A. Для підвищення продуктивності при виконанні функції IGMP Snooping у комутаторах використовуються спеціалізовані мікросхеми
ASIC, які перевіряють IGMP-повідомлення на апаратному рівні.

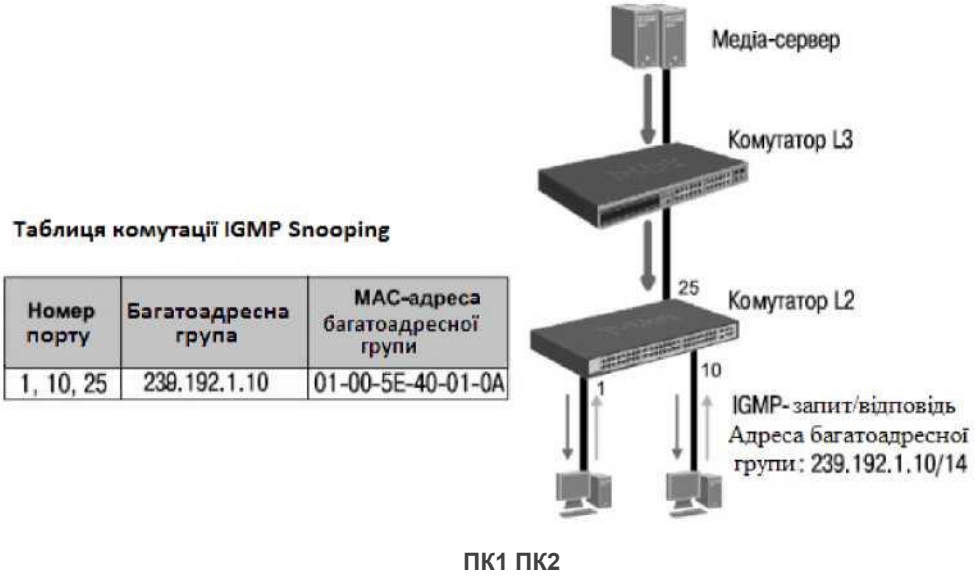


Рисунок 4.6 - Процес створення таблиці комутації IGMP Snooping

IGMP має три версії протоколу: v1, v2 і v3. Зазвичай IGMPv1 ідентифікує локальний маршрутизатор, використовуючи протокол багатоадресної маршрутизації. IGMPv2 додає можливість групових запитів, дозволяючи комутаторам відправляти повідомлення хостам у багатоадресній групі. IGMPv3 надає більше зручних можливостей для підтримки фільтрації певних джерел.

Маршрутизація мультикастових повідомлень на відрізку маршрутизатор - клієнт

При одноадресній маршрутизації кожний маршрутизатор перевіряє адресу призначення вхідного пакету і шукає його в таблиці комутації, щоб визначити, який інтерфейс використовувати для передачі пакету до місця призначення. Адреса джерела маршрутизатором не аналізується. Однак при багатоадресній маршрутизації адреса джерела (яка є простою адресою одноадресного розсилання) використовується для визначення напрямку потоку даних. Джерело багатоадресного трафіку вважається вхідним. Маршрутизатор визначає, які вихідні інтерфейси є адресатами для цієї

багатоадресної групи (адреси призначення), і відправляє пакет через відповідні інтерфейси. Термін «пересилка зворотного шляху» використовується для опису цієї концепції маршрутизації пакетів від джерела, а не до місця призначення.

Отже, IGMP працює на відрізку маршрутизатор - клієнт. Коли клієнт бажає приєднатися до групи, наприклад, 239.192.1.10, він відправляє IGMP-запит, тобто хост рапортує про те, що він бажає отримати трафік цієї групи. Процедура під'єднання клієнтського модуля до мультикастової групи представлена на рисунку 4.7.

Маршрутизатор R1, отримавши такий запит, формує вихідний список отримувачів. Якщо трафік вже існує, R1 відразу починає передавати його в інтерфейс, з якого отримав IGMP-запит. Повідомлення відправляються на ту ж мультикастову адресу 239.192.1.10, до якої бажав приєднатися хост. Так працює протокол IGMPv2.

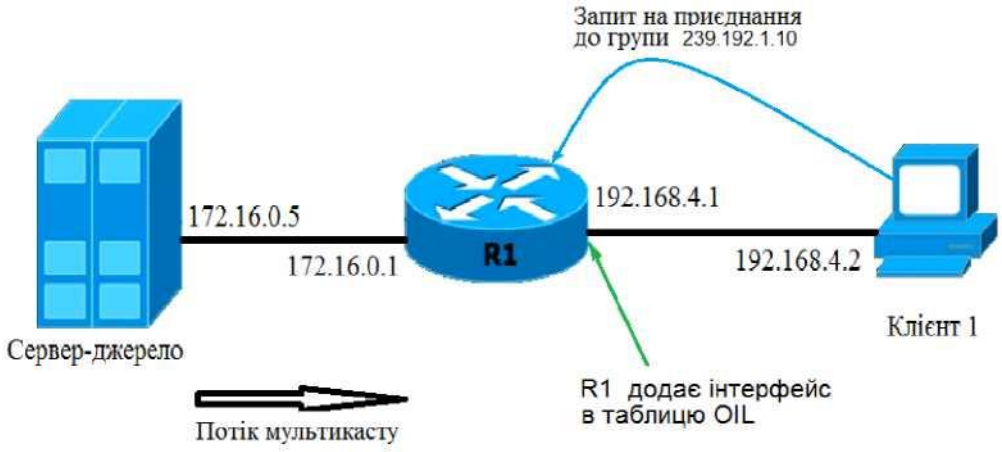


Рисунок 4.7 - Приєднання клієнта до мультикастової групи

Якщо клієнт вирішив від'єднатися, він відправляє пакет IGMP Leave (рис. 4.8). Отримавши цей пакет, маршрутизатор видаляє інтерфейс зі списку отримувачів і після деякої паузи (щоб впевнитися, що інших клієнтів немає) припиняє передавати трафік у цей інтерфейс. Періодично маршрутизатор розсилає спеціальні повідомлення IGMP Query з широкомовною адресою призначення (224.0.0.1). Такий пакет носить назву загального запиту General Query. У відповідь на General Query будь-який клієнт повинен відправити IGMP- повідомлення. Таким чином маршрутизатор перевіряє, в яких групах є отримувачі з конкретними інтерфейсами. Крім того, існують повідомлення Group Specific Query, які надсилаються на адресу конкретної групи.

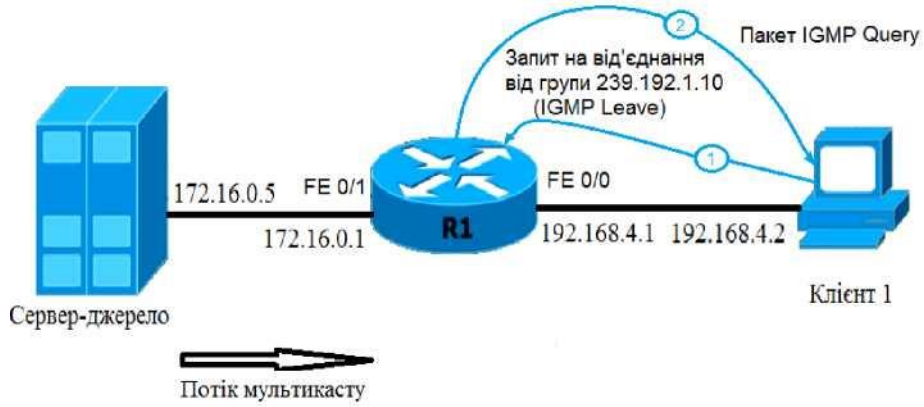


Рисунок 4.8 - Виконання запиту на вихід із мультикастової групи

Коли маршрутизатор отримує IGMP Leave, він не відразу видаляє інтерфейс. Спочатку він відправляє повідомлення Group Specific Query на випадок, якщо там є ще клієнти. Якщо вони є, то надходить IGMP-відповідь, якщо відповідь не надійшла - інтерфейс можна видалити.

Зазвичай протоколи IGMP і RIP включаються окремо, оскільки у них різні задачі, але на маршрутизаторах Cisco вони включаються одночасно.

Маршрутизація мультикастових повідомлень на відрізку сервер - маршрутизатор

Раніше було розглянуто випадок, коли на маршрутизатор мультикастовий трафік вже надходить. Розглянемо виникнення мультикастового трафіку. За допомогою протоколу IGMP маршрутизатор дізнається про клієнта. З іншого боку маршрутизатор отримує потік мультикасту. Тепер виникає задача з'єднати потік мультикасту з клієнтом. Таке з'єднання відбувається завдяки роботі протоколу PIM. Його задача полягає в побудові дерева (в розглянутому прикладі це дерево складається з одного маршрутизатора). Його таблиця маршрутизації містить записи про призначення портів, наприклад:

Incoming Interface: FastEthernet 0/1
Outcoming Interface list:
FastEthernet 0/0

Маршрутизатор приймає трафік на інтерфейс FastEthernet 0/1 і передає його на інтерфейс FastEthernet 0/0. Якщо протокол PIM не буде задіяний, то трафік не буде передаватися взагалі.

Розглянемо приклад складнішої мережі, структура якої представлена на рисунку 4.9.

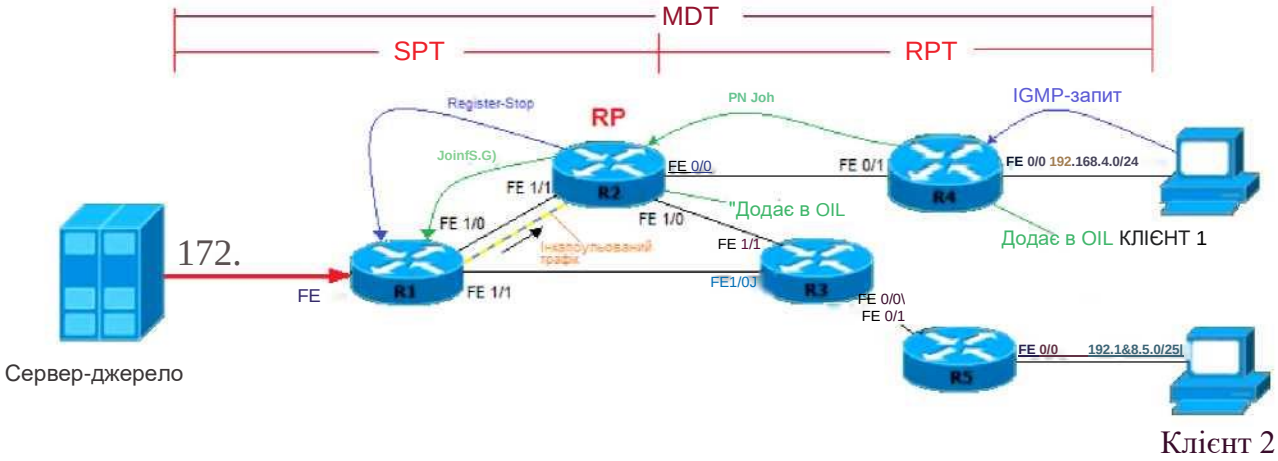


Рисунок 4.9 - Приклад мультикастової маршрутизації

Маршрутизатор R1 отримує потік UDP і знає про джерело мультикасту. Клієнт спілкується з маршрутизатором R4 через протокол IGMP, тому R4 знає про клієнта. Але R1 не знає куди передавати трафік, а R4 нічого не знає про джерело. Тому в мережі завжди є хоча б один маршрутизатор, який має інформацію як про джерело мультикасту, так і про клієнтів. Такий маршрутизатор називається точкою зустрічі RP (Rendezvous Point). До маршрутизатора RP надходить трафік від джерела і до нього ж прагнуть клієнти. Всі маршрутизатори в мережі повинні знати, який маршрутизатор є RP у мережі.

В першу чергу всі маршрутизатори повинні отримати інформацію про сусідні маршрутизатори в мережі. Роблять це вони за допомогою повідомлення **Hello.** Час життя TTL повідомлення **Hello** дорівнює 1.

Отже, клієнт 1 при підключенні відправляє IGMP-запит. Маршрутизатор R4 додає інтерфейс, з якого надійшов цей запит у список вихідних інтерфейсів, а потім відправляє пакет PIM Join у напрямку до RP. Таким чином він демонструє бажання приєднатися до мультикастового дерева. PIM Join надсилається на спеціальну (широкомовну) адресу 224.0.0.13 із TTL, що дорівнює 1. Практично всі пакети PIM використовують саме цю адресу призначення. Кожний маршрутизатор на шляху до RP буде використовувати її індивідуально, тобто маршрутизатор приймає такий PIM Join, опрацьовує його, видаляє старий, формує новий і відправляє його далі, і так до того моменту, поки PIM Join не надійде до RP. У розглянутому прикладі PIM Join надходить до RP відразу.

Маршрутизатор RP, отримавши PIM Join, додає інтерфейс у список

вихідних інтерфейсів OIL, формуючи таким чином одну гілку мультикастового дерева.

Нехай тепер клієнт 2 бажає під'єднатися до мультикастової групи. Він також відправляє IGMP-запит на R5. Маршрутизатор R5 формує пакет PIM Join і відправляє його в напрямку маршрутизатора RP. Така відправка відбувається через той інтерфейс, який веде до RP згідно з юнікастовою таблицею маршрутизації.

Маршрутизатор R3 отримує пакет PIM Join і не передає його далі, а опрацьовує і знищує. Якщо в нього ще немає клієнтів із цієї групи, він формує новий пакет PIM Join і відправляє його в напрямку RP. Маршрутизатор RP, отримавши PIM Join, додає відповідний запис у список вихідних інтерфейсів таблиці OIL.

Тепер сформоване повноцінне дерево, яке називається дерево від маршрутизатора RP до клієнта 1 та клієнта 2 (RPT), тобто маршрутизатор знає про наявність клієнтів.

Але поки-що на маршрутизаторі RP немає трафіку. Після запуску сервера- джерела маршрутизатор R1 починає отримувати трафік. Кожний вхідний мультикастовий пакет він упаковує в юнікастовий, додає юнікастову адресу отримувача пакету маршрутизатора RP і відправляє такий пакет як звичайний IP- пакет прямо на RP з TTL, який дорівнює 255. Таке повідомлення називається реєстрацією джерела на RP (PIM Register) і разом з повідомленням Register Stop передаються юнікастом на юнікастові адреси. Далі RP отримує цей юнікастовий пакет, вилучає з нього інкапсульований мультикаст і відразу відправляє його в побудоване дерево RPT, якщо воно є, тобто одна копія передається до інтерфейсу FastEthernet 0/0, а інша - на FastEthernet 1/0.

Кожний наступний маршрутизатор, отримавши мультикастовий трафік, теж розсилає його у всі свої інтерфейси згідно зі списками вихідних інтерфейсів.

Але така інкапсуляція (або тунелювання) не самий кращий варіант. По- перше, кожний пакет потрібно інкапсулювати, потім розпакувати. Крім того, збільшується довжина пакету, пов'язана з тунелюванням. По-друге, якщо на шляху від джерела до RP виявиться клієнт цієї групи (маршрутизатор RX на рис. 4.10), то трафік від сервера повинен спочатку передаватися до RP, а потім повернутися назад. В результаті, лінія зв'язку буде використовуватися двічі.

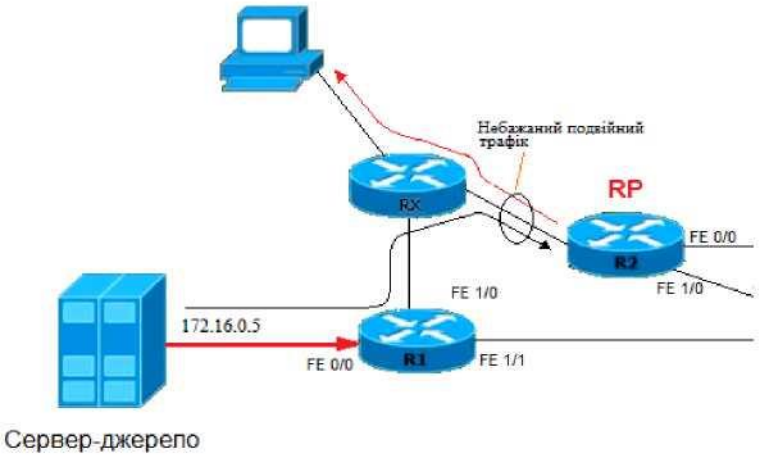


Рисунок 4.10 - Поява небажаного тунелювання

Тому, як тільки маршрутизатор RP отримує перший пакет PIM Register, він ініціює побудову дерева від сервера-джерела до себе. Для цього він відправляє пакет PIM Join (S,G) у напрямку сервера-джерела. Це не такий PIM Join, який направляли клієнтські маршрутизатори, це так званий Source Specific Join. У ньому вказується конкретна адреса сервера-джерела, від якого необхідно побудувати дерево. Тепер важливо, щоб дерево було побудоване саме від цього джерела, адже їх може бути кілька. Передається цей пакет до джерела так само, як і звичайний PIM Join: від вузла до вузла

Коли маршрутизатор R1 отримує такий PIM Join, паралельно з повідомленням PIM Register він починає відправляти чистий мультикаст по дереву, побудованим за допомогою PIM Join.

Коли на маршрутизатор RP починають надходити дві копії трафіку (інкапсульований і чистий), він відправляє пакет PIM Register Stop (теж юнікастовий, як і звичайний пакет PIM Register). Це не означає відмову від мультикасту, це повідомлення для маршрутизатора R1 про те, що потрібно припиняти відправляти інкапсульований трафік.

Побудоване дерево від джерела до RP називається найкоротшим шляхом від джерела до RP SPT (Shortest Path Tree).

Отже, розглянуто процес побудови шляху від джерела мультикасту до сервера RP (SPT) і шлях від клієнтів до сервера RP (RPT). Повний шлях від сервера да клієнтів має загальну назву MPT (Multicast Distribution Tree).

Завдання

1. При виконанні роботи використовується програмне забезпечення для аналізу протоколів комп’ютерних мереж **Wireshark**. Запустити програму Wireshark.
2. Відібрати для аналізу 3 кадри: 1 персональний (unicast), 1 груповий (multicast), 1 широкомовний (broadcast). Всі ці кадри скопіювати у звіт, позначивши в кожному з них MAC-адресу відправника, MAC-адресу отримувача, тип або довжину кадру. Для фільтрації широкомовних

кадрів необхідно в меню Analyze/Display Filter вибрати фільтр «Ethernet broadcast». Для фільтрації групових кадрів необхідного створити новий фільтр з назвою «Ethernet multicast». Для цього необхідно в меню Analyze/Display Filter вибрати New, у полі Filter Name набрати «Ethernet multycast», напроти Filter String натиснути кнопку Expression. У полі Field Name знайти рядок «Ethernet». Далі вибрати підрядок eth.multicast, у полі «Relation» вибрати «= =», в полі «Predefined Values» вибрати «This is a multicast frame». Аналогічно створюється фільтр для unicast.

Для спостереження за трафіком multicast почергово використайте:

а) фільтр захоплення,
б) фільтр відображення,
в) фільтр мережевого рівня,
г) фільтр канального рівня.

Контрольні запитання

1. Що таке хост?
2. Які види адрес використовуються в стеку TCP/IP? Наведіть приклади.
3. Із яких частин складається IP-адреса?
4. Що таке маска підмережі?
5. Як визначається номер підмережі в IP-адресі?
6. Визначте номер підмережі на основі маски: 116.98.04.39/27.
7. Які основні особливості протоколу IPv6?
8. Опишіть механізм визначення MAC-адрес призначення при виконанні пересилок багатоадресних повідомлень.
9. За яких двох етапів відбувається утворення каналу передачі даних при мультикастовому з'єднанні клієнта з відправником мультикасту?
10. У яких випадках мультикастинг користується юнікастовим способом адресації?
11. Що таке «точка зустрічі» Renderzvous Point у мультикастовій мережі?