НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут комп’ютерних інформаційних технологій

Кафедра комп'ютерних систем та мереж

# Лабораторна робота № 4

з дисципліни «Комп’ютерні мережі»

Виконав: Клокун В. Д. Роботу захищено:

Група: СП-425

Перевірив: Зіньков Ю.Г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Київ 2019

**Маршрутизатори і їх функції. Групове розсилання**

**Маршрутизатори, їх функції і класифікація**

Маршрутизатори призначені для забезпечення зв'язку між великою кількістю мереж. Такий зв'язок дає можливість комп'ютерам з різних мереж обмінюватися між собою інформацією. Зв'язані мережі можуть належати одній компанії або ж бути географічно розосереджені і належати кому завгодно. Зазвичай мережі, розділені великими відстанями, зв'язуються за допомогою розподільних мереж. Розподільні мережі засновані на великій кількості різних технологій, включаючи маршрутизатори, засоби передавання і різних типів ліній. Маршрутизатори створювалися лише для об’єднання розподільних мереж в єдину глобальну мережу .

Маршрутизатор є інтелектуальним пристроєм, який працює переважно на перших трьох рівнях еталонної моделі OSI. Проте подібно до будь-якого іншого вузла мережі, маршрутизатор здатний до взаємодії на будь-якому з семи рівнів моделі OSI. Необхідність використання перших трьох рівнів існує практично завжди. Для зв'язку з локальною мережею маршрутизатор використовує перші два рівні еталонної моделі (конструкції канального рівня). Найбільш важливою функцією є здатність маршрутизаторів ідентифікувати мережеві маршрути на основі адрес третього рівня. Цей механізм дозволяє маршрутизаторам взаємодіяти з численними мережами, використовуючи адресацію мережевого рівня незалежно від місця розта-шування і технології роботи мереж.

Для того, щоб зрозуміти принципи маршрутизації і розібратися в роботі маршрутизаторів, необхідно розуміти два аспекти їх роботи: фізичний і логічний. З фізичної точки зору маршрутизатор складається з величезної кількості компонентів, кожен з яких виконує строго задану функцію. З логічної точки зору маршрутизатор виконує певні дії, включаючи виявлення інших маршрутизаторів, здобуття інформації про потенційно досяжні мережі і вузли, визначення і відстежування потенційних маршрутів і передавання дейтаграм одержувачам. Це дозволяє формувати і використовувати міжнародні мережі, включаючи розподільні.

Логічні функції маршрутизатора так само важливі, як і забезпечення фізичного взаємозв'язку множини мереж. Наприклад, для об'єднаної мережі потрібно, щоб між відправником і одержувачем був хоча б один фізичний канал передавання даних. Проте існування і використання фізичного каналу – це дві різні речі. Природно, що для нормальної роботи відправник і одержувач повинні "розмовляти" однією мовою (використовувати єдиний протокол маршрутизації). Крім того, така мова (протокол маршрутизації) дає можливість шляхом спілкування з проміжними маршрутизаторами знаходити найкоротший маршрут для передавання даних.

Таким чином, маршрутизатор повинен забезпечувати такі функції :

• фізична взаємодія;

• логічна взаємодія;

• безпека;

• визначення маршруту передавання даних.

Маршрутизатор має як мінімум два (зазвичай набагато більше) фізичні порти введення-виведення. Порти введення-виведення або, як їх часто називають інтерфейси, використовуються для фізичного приєднання середовища в якому відбувається передавання до маршрутизатора. Кожен порт приєднаний до плати розширення, яка у свою чергу під’єднується до системної плати маршрутизатора. Таким чином, системна плата маршрутизатора забезпечує взаємодію декількох мереж.

Системний адміністратор повинен налаштовувати кожен інтерфейс маршрутизатора за допомогою відповідного інтерфейсу (консолі). Конфігурація включає визначення номерів портів в маршрутизаторі вказанням технології передавання даних і доступної смуги пропускання для мереж, під’єднаних до інтерфейсу, вказанням типів протоколів, які використовуватимуться з цим інтерфейсом. Параметри конкретного порту повинні залежати від типу мережевого інтерфейсу.

Слід зазначити, що в платформах верхнього рівня інтерфейси (VIP2 або лінійна плата) здатні передавати пакети без переривання робо-ти основного процесора.

За сферами застосування маршрутизатори поділяються на декілька класів.

**Магістральні маршрутизатори** (backbone routers) призначені для побудови центральної мережі корпорації. Центральна мережа може складатися з великої кількості локальних мереж, розкиданих по різних будівлях і використовуючих найрізноманітніші мережеві технології типів комп'ютерів і операційних систем. Магістральні маршрутизатори це найбільш потужні пристрої, що здатні обробляти декілька сотень тисяч або навіть декілька мільйонів пакетів в секунду, мають велику кількість інтерфейсів локальних і глобальних мереж. Підтримуються не лише середньошвидкісні інтерфейси глобальних мереж, такі як Т1/Е1, але і високошвидкісні, наприклад, АТМ або SDH з швидкостями 155 Мбіт/с або 622 Мбіт/с і більше. Найчастіше магістральний маршрутизатор конструктивно виконаний за модульною схемою на основі шасі з великою кількістю слотів - до 12 - 14. Велика увага приділяється в магістральних моделях надійності і відмовостійкої маршрутизатора, яка досягається за рахунок системи терморегуляції, надлишкових джерел живлення, замінюваних „на ходу” (hot swap) модулів, а також симетричного мультипроцесорування.

**Маршрутизатори регіональних відділень** з’єднують регіональні відділення між собою і з центральною мережею. Мережа регіонального відділення, так само як і центральна мережа, може складатися з декількох локальних мереж. Такий маршрутизатор зазвичай є деякою спрощеною версією магістрального маршрутизатора. Якщо він виконаний на основі шасі, то кількість слотів його шасі менша: 4 - 5. Можливий також конструктив з фіксованою кількістю портів. Підтримувані інтерфейси локальних і глобальних мереж менш швид-кісні.

**Маршрутизатори віддалених офісів** з’єднують, як правило, єдину локальну мережу видаленого офісу з центральною мережею або мережею регіонального відділення з глобального зв’язку. У максимальному варіанті такі маршрутизатори можуть підтримувати і два інтерфейси локальних мереж. Маршрутизатор видаленого офісу може підтримувати роботу по комутованій телефонній лінії як резервний зв'язок для виділеного каналу. Існує дуже велика кількість типів маршрутизаторів видалених офісів. Це пояснюється як масовістю потенційних споживачів, так і спеціалізацією такого типу пристроїв, що виявляється в підтримці одного конкретного типу глобального зв’язку.

**Маршрутизатори локальних мереж** (комутатори 3-го рівня) призначені для розділення великих локальних мереж на підмережі. Основна вимога, що висувається до них - висока швидкість маршрутизації, оскільки в такій конфігурації відсутні низькошвидкісні порти. Всі порти мають швидкість принаймні 10 Мбіт/с, а багато хто працює на швидкості 100 Мбіт/с та більше.

**Відображення IP-адрес на локальні адреси, технологія NAT**

NAT (від англ. Network Address Translation – ʼʼперетворення мережевих адресʼʼ) - це механізм в мережах TCP/IP, що дозволяє перетворювати IP-адреси транзитних пакетів (рисунок). Також має назви IP Masquerading, Network Masquerading і Native Address Translation.

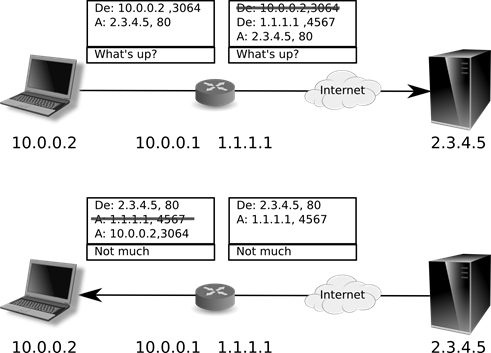


Рисунок – Принцип роботи NAT

Перетворення адрес методом NAT може проводитися майже будь-яким маршрутизуючого пристроєм – маршрутизатором, сервером доступу, міжмережевим екраном. Найбільш популярним є SNAT, суть механізму якого полягає в заміні адреси джерела (англ. source) при проходженні пакета в один бік і зворотного заміні адреси призначення (англ. destination) у відповідному пакеті. Поряд з адресами джерело/призначення можуть також замінюватися номери портів джерела і призначення.

Приймаючи пакет від локального комп'ютера, роутер дивиться на IP-адресу призначення. Якщо це локальний адресу, то пакет пересилається іншому локальному комп'ютеру. Якщо ні, то пакет треба переслати назовні в Інтернет. Але ж зворотною адресою у пакеті вказано локальний адресу комп'ютера, який з Інтернету буде недоступний. Тому роутер ʼʼна льотуʼʼ виробляє трансляцію IP-адреси і порту і запам'ятовує цю трансляцію у себе в тимчасовій таблиці. Через деякий час після того, як клієнт і сервер закінчать обмінюватися пакетами, роутер зітре у себе в таблиці запис про n-ий порт за строком давності.

Крім source NAT (надання користувачам локальної мережі з внутрішніми адресами доступу до мережі Інтернет) часто застосовується також destination NAT, коли звернення ззовні транслюються міжмережевим екраном на комп'ютер користувача в локальній мережі, що має внутрішній адресу і тому недоступний ззовні мережі безпосередньо (без NAT).

Існує 3 базових концепції трансляції адрес: статична (Static Network Address Translation), динамічна (Dynamic Address Translation), маскарадний (NAPT, NAT Overload, PAT).

Статичний NAT – Відображення незареєстрованого IP-адреси на зареєстрований IP-адресу на підставі один до одного. Особливо корисно, коли пристрій повинен бути доступним зовні мережі.

Динамічний NAT – Відображає незареєстрований IP-адресу на зареєстровану адресу від групи зареєстрованих IP-адрес. Динамічний NAT також встановлює безпосереднє відображення між незареєстрованим та зареєстрованим адресою, але відображення може мінятися залежно від зареєстрованої адреси, доступного в пулі адрес, під час комунікації.

Перевантажений NAT (NAPT, NAT Overload, PAT, маськарадінг) – форма динамічного NAT, який відображає кілька незареєстрованих адрес в єдиний зареєстрований IP-адреса, використовуючи різні порти. Відомий також як PAT (Port Address Translation). При перевантаженні кожен комп'ютер у приватній мережі транслюється в той же самий адресу, але з різним номером порту.

Механізм NAT визначений в RFC 1631, RFC 3022.

NAT виконує три важливі функції:

- Дозволяє заощадити IP-адреси (тільки у випадку використання NAT в режимі PAT), транслюючи декілька внутрішніх IP-адрес в один зовнішній публічний IP-адресу (або в декілька, але меншою кількістю, ніж внутрішніх). За таким принципом побудована більшість мереж в світі: на невеликий район домашньої мережі місцевого провайдера або на офіс виділяється 1 публічний (зовнішній) IP-адресу, за яким працюють і отримують доступ інтерфейси з приватними (внутрішніми) IP-адресами.

- Дозволяє запобігти або обмежити обіг зовні до внутрішніх хостам, залишаючи можливість звернення зсередини назовні. При ініціації з'єднання зсередини мережі створюється трансляція. Відповідь пакети, вступники зовні, відповідають створеної трансляції і тому пропускаються. Якщо для пакетів, що надходять зовні, відповідної трансляції не існує (а вона може бути створеною при ініціації з'єднання або статичної), вони не пропускаються.

- Дозволяє приховати певні внутрішні сервіси внутрішніх хостів/серверів. По суті, виконується та ж зазначена вище трансляція на певний порт, але можливо підмінити внутрішній порт офіційно зареєстрованої служби (наприклад, 80-й порт TCP (HTTP-сервер) на зовнішній 54055-й). Тим самим, зовні, на зовнішньому IP-адресі після трансляції адрес на сайт (або форум) для обізнаних відвідувачів можна буде потрапити за адресою http://example.org:54055, але на внутрішньому сервері, що знаходиться за NAT, він працюватиме на звичайному 80-му порту. Підвищення безпеки і приховування ʼʼнепублічнихʼʼ ресурсів.

Як недоліки можна визначити таке:

- Старі протоколи. Протоколи, розроблені до масового впровадження NAT, не в змозі працювати, якщо на шляху між взаємодіючими хостами є трансляція адрес. Деякі міжмережеві екрани, які здійснюють трансляцію IP-адрес, можуть виправити цей недолік, відповідним чином замінюючи IP-адреси не тільки в заголовках IP, але і на більш високих рівнях (наприклад, в командах протоколу FTP). Див Application-level gateway.

- Ідентифікація користувачів. Через трансляції адрес ʼʼбагато в одинʼʼ з'являються додаткові складнощі з ідентифікацією користувачів і необхідність зберігати повні логи трансляцій.

- Ілюзія DoS-атаки. Якщо NAT використовується для підключення багатьох користувачів до одного і того ж сервісу, це може викликати ілюзію DoS-атаки на сервіс (безліч успішних і неуспішних спроб). Наприклад, надмірна кількість користувачів ICQ за NAT призводить до проблеми з підключенням до сервера деяких користувачів через перевищення допустимої швидкості підключень. Частковим вирішенням проблеми є використання пулу адрес (групи адрес), для яких здійснюється трансляція.

- Пірінгові мережі. У NAT-пристроях, що не підтримують технологію Universal Plug & Play, в деяких випадках, необхідна додаткова настройка (див. Трансляція порт-адреса) при роботі з пірінговимі мережами і деякими іншими програмами, в яких необхідно не тільки ініціювати вихідні з'єднання, але також брати вхідні.

NAT Traversal (проходження або автонастройка NAT) – це набір можливостей, що дозволяють мережевим додаткам визначати, що вони знаходяться за пристроєм, що забезпечує NAT, дізнаватися зовнішній IP-адресу цього пристрою і виконувати зіставлення портів для пересилання пакетів з зовнішнього порту NAT на внутрішній порт, використовуваний додатком; все це виконується автоматично, користувачеві немає необхідності вручну налаштовувати зіставлення портів або вносити зміни в якісь інші параметри. Однак існують запобіжні заходи у довірі до таких додатків – вони отримують обширний контроль над пристроєм, з'являються потенційні уразливості.

Протокол DHCP

DHCP ([англ.](https://uk.wikipedia.org/wiki/Англійська_мова) *Dynamic Host Configuration Protocol* — протокол динамічної конфігурації вузла) — це стандартний [протокол](https://uk.wikipedia.org/wiki/Мережний_протокол) [прикладного рівня](https://uk.wikipedia.org/wiki/Протокол_прикладного_рівня), який дозволяє [комп'ютерам](https://uk.wikipedia.org/wiki/Комп'ютер) автоматично отримувати [IP-адресу](https://uk.wikipedia.org/wiki/IP-адреса) та інші параметри, необхідні для роботи в [мережі](https://uk.wikipedia.org/wiki/Комп'ютерна_мережа). Для цього комп'ютер звертається відповідно — до DHCP-[сервера](https://uk.wikipedia.org/wiki/Сервер). Мережевий адміністратор може задати діапазон адрес, які будуть розподілені між комп'ютерами. Це дозволяє уникнути ручного налаштування комп'ютерів мережі й зменшує кількість помилок. Протокол DHCP використовується в більшості великих мереж [TCP/IP](https://uk.wikipedia.org/wiki/TCP/IP).

DHCP є розширенням протоколу [BOOTP](https://uk.wikipedia.org/wiki/BOOTP), що використовувався раніше для забезпечення [бездискових робочих станцій](https://uk.wikipedia.org/w/index.php?title=Бездискова_робоча_станція&action=edit&redlink=1) IP-адресами при їхньому завантаженні. DHCP зберігає [зворотну сумісність](https://uk.wikipedia.org/wiki/Зворотна_сумісність) з BOOTP.

Стандарт протоколу DHCP був прийнятий у жовтні [1993](https://uk.wikipedia.org/wiki/1993) року. Остання версія протоколу (березень [1997](https://uk.wikipedia.org/wiki/1997) року) описана в [RFC 2131](https://tools.ietf.org/html/rfc2131). Нова версія DHCP, призначена для використання в середовищі [IPv6](https://uk.wikipedia.org/wiki/IPv6), зветься [DHCPv6](https://uk.wikipedia.org/w/index.php?title=DHCPv6&action=edit&redlink=1) і визначена в [RFC 3315](https://tools.ietf.org/html/rfc3315) (липень [2003](https://uk.wikipedia.org/wiki/2003) року).

Крім IP-адреси, DHCP також може повідомляти клієнтові додаткові параметри, необхідні для нормальної роботи в мережі. Ці параметри називаються опціями DHCP. Список стандартних опцій можна знайти в [RFC2132](https://tools.ietf.org/html/rfc2132). Деякими з найбільш часто використовуваних опцій є:

* IP-адреса маршрутизатора за замовчуванням;
* маска підмережі;
* адреси серверів DNS;
* ім'я домену DNS.

Деякі постачальники програмного забезпечення можуть визначати власні, додаткові опції DHCP.

**Алгоритм роботи протоколу :**

Протокол DHCP побудований так, що клієнт може звертатися із запитом відразу до декількох серверів.

Клієнт DHCP, що потребує адресу, посилає широкомовний пакет DHCPDISCOVER в пошуках сервера. Пакет містить апаратну адресу запитувача клієнта. Потім один або кілька серверів DHCP розглядають запит і посилають у відповідь пакет DHCPOFFER, що містить пропоновану IP-адресу і "час оренди".

Клієнт вибирає адресу з отриманих пакетів DHCPOFFER. Вибір клієнта залежить від його призначення - наприклад, він може вибрати адресу з найбільшим часом оренди. Слідом за тим клієнт посилає пакет DHCPREQUEST з адресою вибраного сервера.

Обраний сервер посилає підтвердження (DHCPACK) і процес узгодження завершується. Пакет DHCPACK містить обумовлені адресу та час оренди. Сервер позначає виділену адресу як зайняту - до закінчення терміну оренди цю адресу не можна буде присвоїти іншому клієнту. Клієнту залишилося тільки сконфігурувати себе відповідно до надісланих даних і можна приступати до роботи в мережі.

Отже, на запит DHCPDISCOVER може відповісти кілька серверів. Клієнт повинен вибрати одну з пропозицій і послати у відповідь пакет DHCPREQUEST з ідентифікатором вибраного сервера. Інші сервери переглядають пакет DHCPREQUEST і укладають на основі ідентифікатора сервера, що їх пропозиція була відкинута. Таким чином, вони знають, що запропоновані ними IP-адреси вільні для призначення іншим клієнтам.

У разі якщо сервер не може прийняти конфігурацію, він посилає пакет DHCPNAK (відмова в підтвердженні), що змушує клієнта почати процес узгодження заново.

Виходячи з цього, якщо в мережі два DHCP-сервера з різними конфігураціями, немає ніякої гарантії, що клієнт вибере саме ваш сервер.

**Групове розсилання пакетів. Адреса групового розсилання**

Мультікастінгом (multicasting) називається розсилка дейтаграм групі одержувачів. Для ідентифікації груп використовуються спеціальні адреси одержувача; ці адреси призначаються з класу D в діапазоні 224.0.0.0 - 239.255.255.255. Дейтаграмма, спрямована на групову адресу, повинна бути доставлена ​​всім учасникам групи.

Всі адреси в діапазоні 224.0.0.0 - 238.255.255.255 призначені для використання в масштабі Інтернет. Адреси виду 239.Х.Х.Х зарезервовані для внутрішнього використання в приватних мережах.

Додатки групової розсилки дейтаграм досить очевидні і перспективні: це розсилка новин, трансляція радіо- або відеопрограм, дистанційне навчання, і т.п. Мультікастінга активно використовується також і для передачі службового трафіку (маршрутної інформації, повідомлень служби точного часу і ін.).

Групова розсилка зменшує навантаження на мережу.

Одержувачів дейтаграм з певним груповим адресою називають членами даної групи. Відправник груповий дейтаграми не зобов'язаний знати індивідуальні IP-адреси одержувачів і не зобов'язаний бути членом групи.

Недоліком груповий розсилки є неможливість використання протоколу TCP. Використання ж протоколу UDP тягне за собою: ненадійність доставки, відсутність коштів реагування на затори в мережі і т.д. Крім того, в окремих випадках при зміні маршрутів розсилки групові дейтаграми можуть не тільки губитися, а й дублюватися.

Для організації IP-мережі з підтримкою мультікастінга необхідно наступне:

-підтримка мультікастінга в стеці TCP / IP розташованих в мережі хостів;

-підтримка групової або широкомовної розсилки на рівні доступу до мережі.

У Ethernet існує спеціальний діапазон адрес для групової розсилки IP-дейтаграм: 01: 00: 5e: X: Y: Z, де ХYZ - молодші 23 біта IP-адреси. Тобто, групового IP-адресою 224.255.0.1 на рівні Ethernet буде відповідати MAC-адресу 01: 00: 5e: 7f: 00: 01.

Маршрутизатор знає, члени яких груп знаходяться в безпосередньо приєднаних до нього мережах. IP-мультікастінга-пакети инкапсулируются при передачі через тунелі так, що вони виглядають як звичайні IP-унікаст-пакети.

Мультікастинга-маршрутизатор при посилці пакету через тунель готує IP-пакет з заголовком, який містить адресу маршрутизатора-партнера на іншому кінці тунелю. Маршрутизатор-приймач витягує вкладений мультікастінга-пакет і направляє далі, якщо це потрібно.

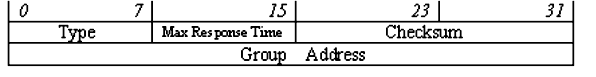
**Основні протоколи групового розсилання.**

Протокол IGMP (Internet Group Management Protocol) призначений для реєстрації на маршрутизаторі членів груп, що знаходяться в безпосередньо приєднаних до нього мережах (в LAN). Маючи цю інформацію, маршрутизатор може повідомляти іншим маршрутизаторів (за допомогою протоколів групової маршрутизації DVMRP, MOSPF, PIM, CBT) про необхідність пересилання йому дейтаграм для груп.

IGMPv1 - RFC-1112, IGMPv2 - RFC-2236, IGMPv3 - RFC-3376.

IGMP працює безпосередньо поверх IP, і ідентифікується значенням поля "Protocol" = 2 в заголовку IP-дейтаграми. За замовчуванням мультикаст-дейтаграми мають значення поля TTL = 1, що обмежує їх поширення однієї субсетей. Додатки можуть збільшувати значення TTL. Перша дейтаграмма, тим не менш, завжди має TTL = 1. Якщо отримання цієї дейтаграми не підтверджується сервером, надсилається друга - з TTL = 2 і т.д. Попутно вимірюється і число кроків між клієнтом і сервером. Для випадку, коли число кроків не більше 1 (для LAN), зарезервований блок IP адрес 224.0.0.0 - 224.0.0.255. Маршрутизатор не обробляє пакети з такими адресами.

За IP-заголовком в дейтаграмі слідує повідомлення IGMP:



• Type (8 біт) - тип повідомлення, якщо починається з 1, то це запит, відправлений

мультікастінга-маршрутизатором, з 2 вказує, що це відгук посланий вузлом.

• Max Response Time (8 біт) - максимальний час відгуку, задіяно тільки в

повідомленнях типу Membership Query (в IGMPv1 не використовувалося і ставилося в 0).

• Checksum (16 біт) - контрольна сума.

• Group Address (32 біта) - груповий IP-адреса.

Існують наступні типи повідомлень:

• Membership Query (Type = 17) - запит про наявність в мережі членів груп (відправляється маршрутизатором). Запити про всі наявні групах - загальні запити

 - відправляються за адресою 224.0.0.1 ( "всіх вузлів"); запити про наявність членів певної групи - приватні запити - відправляються за адресою цієї групи.

• Membership Report (Type = 22) - повідомлення про наявність в мережі члена групи

(Відправляється хостом - членом групи за адресою групи).

• Leave Group (Type = 23) - повідомлення про від'єднання хоста від групи (відправляється від'єднати хостом за адресою 224.0.0.2 - "всім маршрутизаторів").

Функціонування IGMP протоколу:

1. Маршрутизатор періодично розсилає за адресою 224.0.0.1 загальний запит Membership Query, при цьому поле "Group Address" обнулити. Період цих розсилок може змінюватися адміністратором; значення за замовчуванням - 125 с.

2. Прийнявши такий запит, кожен одержувач групових дейтаграм вичікує випадкове час "Max Response Time" з Membership Query. Якщо за цей час хтось інший вже відповів маршрутизатора, то даний хост не відповідає, інакше він сам посилає Membership Report. Max час затримки (зазвичай 10 с) дозволяє уникнути посилки безлічі відповідей з адресою однієї і тієї ж групи: маршрутизатора не потрібно знати, скільки саме членів даної групи є у нього в мережі, йому потрібно лише сам факт наявності членів.

3. Повідомлення Membership Report надсилається на адресу групи, і цю ж адресу поміщається в поле "Group Address". Слід зазначити, що маршрутизатор є членом всіх груп, тобто отримує повідомлення, спрямовані на будь-який груповий адресу.

4. Якщо хост є членом кількох груп, то вищеописана процедура з очікуванням і відправкою відповіді виконується незалежно для кожної групи.

5. При підключенні хоста до нової групи він самостійно відправляє повідомлення типу. Membership Report, не чекаючи чергового запиту від маршрутизатора.

6. Для кожної групи, члени якої виявилися в мережі, маршрутизатор веде відлік часу неактивності. Якщо жодного Membership Report для цієї групи не було отримано за певний період (за замовчуванням - 260 с), то маршрутизатор вважає, що членів цієї групи в мережі більше немає.

7. Коли хост від'єднується від групи, він може послати повідомлення Leave Group по груповій адресі 224.0.0.2 ( "всім маршрутизаторів"); адреса групи міститься в поле "Group Address". Хосту слід зробити це, якщо на останній запит Membership Query від імені цієї групи відповідав саме цей хост.

8. Отримавши повідомлення Leave Group, маршрутизатор генерує приватний запит Membership Query для членів тільки цієї групи. Якщо за час, вказаний в полі "Max Response Time" запиту (за замовчуванням - 1 с), маршрутизатор не отримав жодного Membership Report, він вважає, що членів даної групи в мережі більше немає. Для надійності запит шлётся 2 рази.

9. Якщо до однієї мережі підключені декілька маршрутизаторів, що підтримують протокол IGMP, то запити розсилає тільки маршрутизатор з найменшим IP-адресою (тобто, якщо маршрутизатор отримав з мережі Membership Query з IP-адресою відправника меншим, ніж його власний адресу, він повинен перестати посилати запити та перейти в режим прослуховування обміну IGMP-повідомленнями).

10. Для забезпечення сумісності з першою версією протоколу IGMP передбачено повідомлення Membership Report version 1 (Type = 18), а також деякі спеціальні дії протоколу.

11. Членство в групі може динамічно змінюватися. Будь-хост може увійти в групу і вийти з групи в будь-який час за власною ініціативою, хост може бути членом великої кількості груп.

**DVMRP**

Протокол DVMRP (Distance Vector Multicast Routing Protocol, RFC-1075) - найстаріший протокол групової маршрутизації, він використовується в ядрі експериментальної мережі MBONE. Протокол працює за технологією RPF з урізанням, але для побудови дерев використовується власний дистанційно-векторний протокол, аналогічний протоколу RIP.

Протокол DVRMP простий в реалізації і досить ефективний, але він підходить тільки для невеликих мереж з високою щільністю одержувачів. До недоліків методу RPF, описаним в следудующем пункті (щодо великий розмір збереженої таблиці і необхідність розсилки "пробних" дейтаграм по всій системі мереж), додається обмеження на розмір системи мереж, успадковане від протоколу RIP (в DVMRP значення нескінченності дорівнює 32).

**MOSPF**

Протокол MOSPF (Multicast OSPF, RFC-1584) є розширенням протоколу OSPF. Маршрутизатор, що підтримує це розширення, встановлює біт "М" в поле "Options" повідомлення "Hello". У базі даних стану зв'язків вводиться додатковий тип запису: для зазначеної мережі перераховуються всі групи, члени яких є в цій мережі. Ці записи, як і всі інші записи бази даних стану зв'язків, поширюються по системі мереж за допомогою протоколу віяловій розсилки. Для транзитної мережі запис вноситься в базу даних виділеним маршрутизатором. Дерева розсилки групових дейтаграм будуються за методом RPF на основі бази даних стану зв'язків. Відзначимо, що розсилка "пробних" групових дейтаграм і подальше усічення непотрібних гілок дерева в даному випадку не проводиться, тому що інформація про наявність в мережах членів груп вже міститься в базі даних.

Протокол MOSPF має серйозну проблему, пов'язану з масштабуванням: для кожної пари "джерело-група" проводиться окремий запуск алгоритму SPF для розрахунку дерева розсилки. При великому числі джерел, а також при нестабільній топології системи мереж, на ці обчислення витрачаються істотні обчислювальні ресурси маршрутизаторів. Крім того, слід врахувати необхідність віяловій розсилки інформації про членство в групах при її зміні. І, нарешті, очевидно, що MOSPF вимагає використання OSPF як протокол маршрутизації, тобто, не є незалежним і може застосовуватися тільки в OSPF-системах.

**PIM DM**

PIM (Protocol Independent Multicast) - два протоколи групової маршрутизації (для щільного і розрідженого розташування членів груп, відповідно dense mode і sparse mode), які не залежать від використовуваного протоколу "звичайної" маршрутизації. PIM DM (PIM Dense Mode) використовується в системах мереж з великою щільністю одержувачів. Цей протокол реалізує метод RPF з урізанням (модифікований, тобто без доступу до внутрішніх таблиць протоколу маршрутизації, внаслідок чого досягається незалежність від протоколу маршрутизації). Необхідність періодичної посилки "пробних" дейтаграм не є істотним недоліком при щільному розташуванні одержувачів.

**Протокол PIM SM**

**Протокол PIM SM** (Protocol Independent Multicast, Sparse mode, RFC-2362) застосовується для маршрутизації дейтаграм для нечисленних груп, члени яких перебувають далеко один від одного (в цьому випадку недоліки методу RPF з урізанням стають істотними). Функціонування протоколу можна коротко описати як метод CBT, що переходить в RPF. Замість флудинг, як в PIM DM, в PIM-SM вибирається один маршрутизатор, який буде зберігати інформацію про групах і джерелах. Це звичайний маршрутизатор PIMSM, який виконує роль rendezvous point (RP). Всі маршрутизатори в домені PIM SM повинні знати, хто виконує роль RP. Маршрутизатор, в мережі якого зареєструвалися члени групи, посилає в RP повідомлення Join, яке обробляється проміжними маршрутизаторами як в технології CBT - таким чином формується початкове дерево розсилки.

Відправник дейтаграм (точніше, маршрутизатор), посилає в RP повідомлення Register, в яких инкапсулируются групові дейтаграми. RP витягує дейтаграми з цих повідомлень і розсилає їх по сформованому дереву розсилки. Якщо відправник працює досить інтенсивно, то RP посилає в його сторону повідомлення Join - тобто, відправник стає членом групи і може розсилати групові дейтаграми по дереву безпосередньо, минаючи стадію тунелювання в точку рандеву. Поширення групових дейтаграм по дереву розсилки здійснюється аналогічно методу CBT: дейтаграмма розсилається через всі інтерфейси, що належать дереву.

**Протокол CBT**

**Протокол CBT** (RFC-2189) реалізує метод CBT .

У протоколі CBT передбачена можливість взаємодії з DVMRP.

**Висновок:** Застосування того чи іншого протоколу групової маршрутизації суттєво залежить від того, як щільно або розріджено розташовані одержувачі групового трафіку. Для щільного розташування придатні протоколи DVMRP, MOSPF і PIM DM; для розрідженого підходять PIM SM і CBT. Всі перераховані протоколи знаходяться в експериментальній стадії. Протокол DVMRP, як зазначалося вище, використовується в ядрі MBONE. Однак найбільш перспективними виглядають протоколи PIM DM і PIM SM; вони також підтримуються маршрутизаторами Cisco.

**Маршрутизація трафіка групового розсилання**

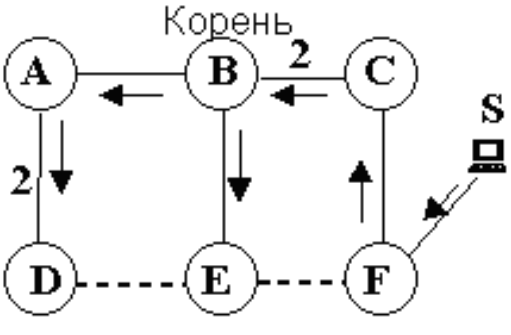
Існують різні алгоритми і протоколи для побудови мультикастингового дерева. Основним припущенням, яке при цьому робиться, є те, що маршрутизатор знає, члени яких груп знаходяться в безпосередньо приєднаних до нього мережах. Завданням цього розділу є опис методів (алгоритмів) маршрутизації групових дейтаграм, тобто просування їх через систему мереж від відправника до членів групи.

**Віялова розсилка** - найбільш простий метод маршрутизації групових дейтаграм, при якому дейтаграмма розсилається в усі мережі системи незалежно від наявності в тій чи іншій мережі членів групи. Але, через виникнення лавинного ефект від дублювання потрібна перевірка на повтор. При надходженні груповий дейтаграми маршрутизатор перевіряє, вперше він отримує цю дейтаграмму. Якщо так, то маршрутизатор розсилає дейтаграмму через всі свої інтерфейси, крім того, з якого вона була отримана. Інакше дейтаграмма ігнорується.

**Spanning Trees**

В системі мереж ABCDEF вибирається кореневої маршрутизатор B, після цього з графа системи виділяється підграф-дерево, що з'єднує кореневої маршрутизатор з усіма іншими маршрутизаторами системи ("Остов дерево"). Процедура проводиться лише при ініціалізації системи, а в процесі роботи мережі ST не змінюється.

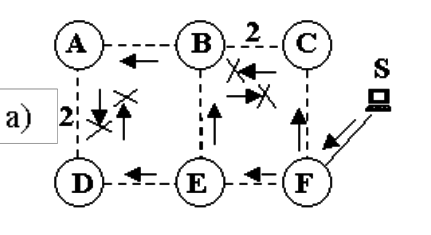
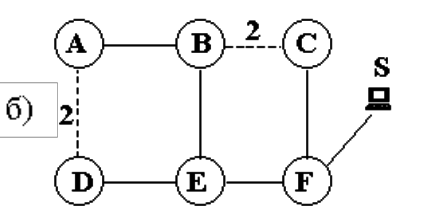
На рис. показана розсилка групової дейтаграми по остовому дереву: S-джерело, A-F -маршрутизатори; гілки дерева позначені суцільними лініями; метрики всіх мереж, крім явно зазначених, рівні одиниці.



Після побудови ST кожен маршрутизатор зберігає для кожного з інтерфейсів тільки прапор "цей інтерфейс належить ST". Групова дейтаграмма від будь-якого вузла S поширюється в такий спосіб: отримана маршрутизатором дейтаграмма ретранслюється через всі інтерфейси, що належать остов дереву, крім того інтерфейсу, з якого вона була отримана.

**RPF (Reverse Path Forwarding).**

На рис. показаний метод RPF: а) розсилка дейтаграм; б) дерево розсилки, S - джерело, A-F - маршрутизатори; метрики всіх мереж, крім явно зазначених, рівні 1.

Маршрутизатор отримав через якийсь інтерфейс групову дейтаграмму від джерела S. Якщо через цей інтерфейс лежить найкоротший маршрут від даного маршрутизатора до вузла S, то ретранслювати дейтаграмму через все інтерфейси крім того, з якого вона отримана, інакше дейтаграмму ігнорувати. Наприклад, маршрутизатор В проігнорує дейтаграмму від вузла С, але прийме дейтаграмму від вузла Е і ретранслює її через інші інтерфейси (рис. А).

**Метод CBT** (Дерева з фіксованим ядром) заснований на тому, що для кожної групи призначається головний маршрутизатор, званий ядром, - він буде коренем дерева розсилки (вузол В на рис.). Всі маршрутизатори, до яких можуть бути підключені потенційні члени групи, знають адресу ядра. Після того, як член групи зареєструвався на маршрутизаторі за допомогою протоколу IGMP, маршрутизатор посилає в сторону ядра повідомлення Join для приєднання до дерева розсилки. Проміжні маршрутизатори, пересилаючи це повідомлення у бік ядра, одночасно позначають інтерфейси, через які отримані повідомлення Join, як належать дереву розсилки для даної групи. Повідомлення слідує до ядра або до першого маршрутизатора, вже приєднаного до дерева розсилки.

Стан приналежності до дерева має певний термін придатності, тому періодично потрібно посилка підтверджень. Кожен маршрутизатор посилає підтвердження вищестоящому (по шляху до ядра) маршрутизатора. Непідтверджені протягом деякого часу гілки дерева усікаються. Розсилка же самих групових дейтаграм маршрутизаторами відбувається аналогічно методу ST: дейтаграмма розсилається через всі інтерфейси, що належать дереву розсилки, крім того, з якого дейтаграмма була отримана. Якщо джерело дейтаграми не є членом групи, то його маршрутизатор спочатку инкапсулює групову дейтаграмму в звичайну, адресовану ядру, а ядро ​​вже ініціює групову розсилку по дереву.

На рис. показаний метод CBT. а) посилка повідомлень Join; б) сформоване дерево розсилки S - джерело, A-F маршрутизатори; до маршрутизатора А не підключені члени групи; метрики мереж, крім явно зазначених, рівні 1.

