ГУЗІЙ М. М., канд. техн. наук, доц.
СТАНІСЛАВОВА О. В.
КАДЕТ М. В

АНАЛІЗ ТЕХНОЛОГІЙ МОНІТОРИНГУ КОМП'ЮТЕРНИХ МЕРЕЖ

Розглянуто проблему моніторингу комп'ютерних мереж. Визначено загальносистемні вимоги, структуру, а також вимоги програмного забезпечення, систем моніторингу комп'ютерних мереж.

The problem of computer's monitoring is considered. General system's requirements are determined. Structure, software requirements and also systems of computer's network are described in the article.

Постановка проблеми

Сучасні комп'ютерні системи побудовані на мережі Internet, або об'єднані в локальну мережу з подальшим виходом до Internet. Ураховуючи сучасний стан інформаційних і комунікаційних технологій для концентрації інформації щодо комп'ютерних мереж постає проблема моніторингу. Доцільним є створення програм мережевого моніторингу для забезпечення доступу до інформації, стосовно мережевого контенту, топології, обладнання як спеціалістів так і користувачів.

У широкому сенсі *моніторинг* — спеціально організоване, систематичне спостереження за станом об'єктів, явищ, процесів з метою їх оцінки, контролю або прогнозу.

Моніторинг — систематичний збір і обробка інформації, яка може бути використана для поліпшення процесу ухвалення рішення, а також побічно для інформування громадськості або прямо як інструмент зворотного зв'язку в цілях здійснення проектів, оцінки програм або вироблення політики. Він несе одну або більш з *трьох організаційних функцій:*

1. Виявляє стан критичних або таких, що знаходяться в стані зміни явищ середовища, відносно яких буде вироблений курс дій на майбутнє;
2. Може допомогти встановити відносини з своїм оточенням, забезпечуючи зворотний зв'язок, відносно попередніх успіхів і невдач певної політики або програм;
3. Може бути корисний для встановлення відповідності правилам і контрактним зобов'язанням.

Терміном *моніторинг мережі* визначають роботу системи, яка виконує постійне спостереження за комп'ютерною мережею у пошуках повільних або несправних систем і яка при виявленні збоїв повідомляє про них мережевого адміністратора. Ці завдання є підмножиною завдань управління мережею.

Існує ряд програм мережевого моніторингу:

Програма *ping*, програма *ipconfig*, сервери *SNMP*, *Zabbix (Open Source)*, *NetXMS (Open Source)*, *Big Brother*, *Optivity*, *Caligare Flow Inspector*, *MRTG*, *RRDtool*, *Intellipool Network Monitor*, *Ipswitch WhatsUp*, *ManageEngine OpManager*, *Netmon — Appliance based network monitoring suite with email and pager alert system*, *Cricket*, *PRTG*, *Packet Analyzer: Network Traffic Monitoring, Analysis and Troubleshooting*, *NetVizor*, *NetDecision*, *HP OpenView Network Node Manager (NNM)*, *Cisco Works NMS*.

Мережі *Ethernet*, хаби і комутатори

У мережах *Ethernet* хаби (концентратор, *hub*) і комутатори (*switch*) є центральними точками підключення до мережі комп'ютерів або інших мережевих пристроїв. У сукупності ці комп'ютери складають сегмент мережі. В рамках цього сегменту всі комп'ютери можуть «спілкуватися» безпосередньо один з одним. Хаби — менш «інтелектуальні» пристрої, ніж комутатори: вони просто приймають вхідні пакети через один порт і передають їх на інші порти. Ця властивість відмінно підходить для моніторингу в режимі *promiscuous* (від англ. нерозбірливий).

На відміну від хабів, комутатори аналізують всі пакети по мірі їх надходження і перевіряють *MAC*-адреси джерела і призначення. Після цього пакет передається в потрібний порт. У комутованих мережах мережевий аналізатор обмежений в своїх функціях прийомом *broadcast*- і *multicas*t-пакетів, а також прийомом трафіку, що передається і отримується тим комп'ютером, на якому встановлений аналізатор. Нижче показана типова картина мережевої активності в комутованій мережі.

На рис. 1 можна побачити велику кількість *broadcast*-пакетів, що посилаються хостами локальної мережі на *IP-broadcast*-адреси, при цьому ви не можете побачити нормальний *unicast*-трафік між цими хостами і Інтернетом. Не дивлячись на те, що більшість комутаторів не дозволяють здійснювати моніторинг в режимі *promiscuous*, багато комутаторів можуть бути конфігуровані так, щоб переправляти пакети на спеціальний порт для моніторингу. Нижче буде описане застосування хабів і комутаторів в моніторингу мереж.

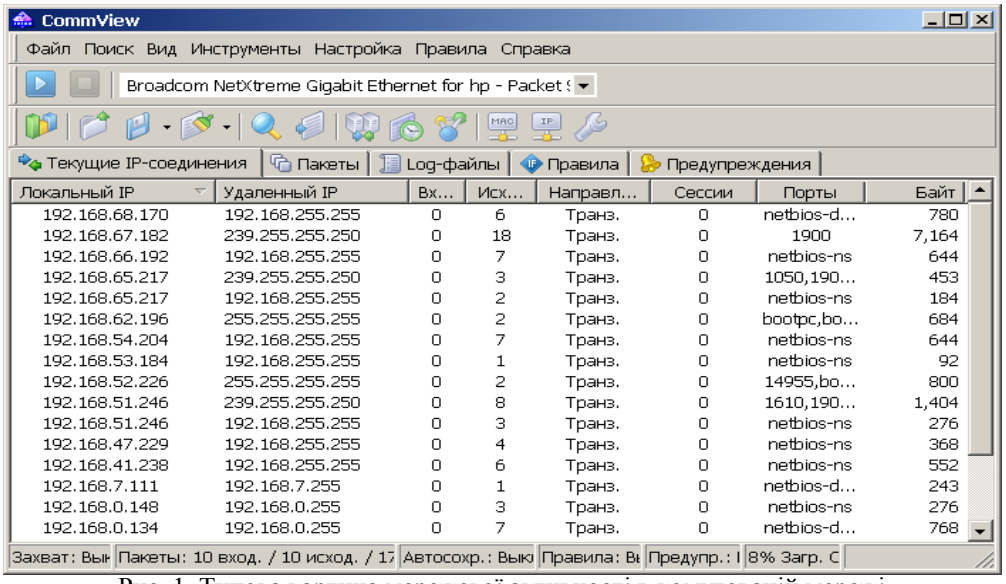


Рис. 1. Типова картина мережевої активності в комутованій мережі

Моніторинг за допомогою хабів

У невеликих мережах хаби достатньо поширені з-за їх невеликої вартості, але все таки слід звернути увагу на можливі проблеми в їх застосуванні. По-перше, хаби відкриті для несанкціонованого моніторингу зсередини вашого сегменту мережі, оскільки кожен порт може бути використаний для *promiscuous*-моніторингу. По-друге, різні види «інтелектуальних» хабів *(«auto-sensing», «dual-speed», «switching», «intelligent»)* можуть не дозволити вам вести моніторинг всього сегменту мережі. Цю проблему розглянемо навівши декілька варіантів мереж з використанням хабів (рис. 2—4).

Це найбільш простій і очевидний варіант. Тут будь-який комп'ютер, підключений до хабу, може бути комп'ютером для моніторингу, оскільки хаб передає прийняті/передані дані від маршрутизатора *(router)* на всі порти. Також відзначимо, що можливий моніторинг обміну між локальними ПК.

У цьому варіанті (рис. 3) хаб знаходиться між маршрутизатором і комутатором. Ви можете спостерігати дані, прийняті/передані з Інтернету, але дані, якими обмінюються локальні ПК, вам недоступні.

Варіант 1

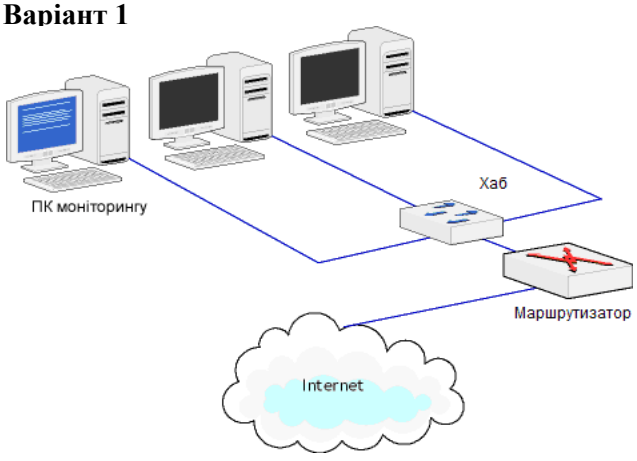


Рис. 2. Моніторинг за допомогою хабів

Варіант 2

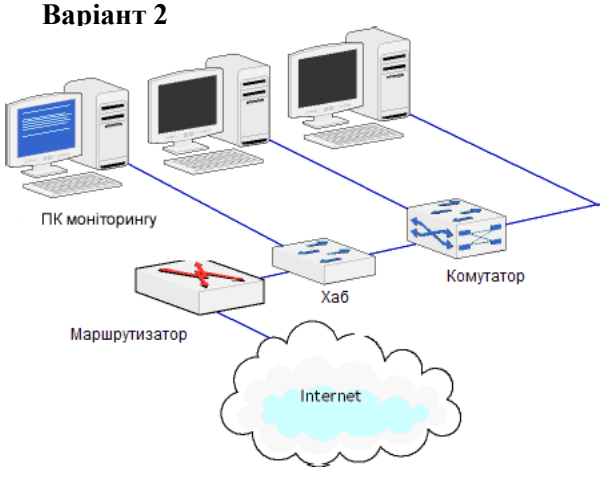
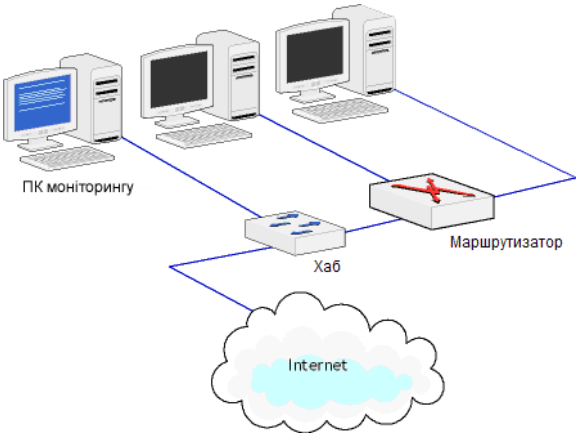


Рис. 3. Моніторинг за допомогою хабів



Варіант 3

У даному варіанті показано, як можна здійснювати моніторинг невеликої локальної мережі, в якій немає комутатора. Це типова топологія домашньої або невеликої офісної мережі, де маршрутизатор суміщений з комутатором, до якого у свою чергу підключені інші комп'ютери. Для моніторингу даних, що передаються або

приймаються з Інтернету, ви можете встановити хаб між Інтернетом і вашим маршрутизатором. Важливо відзначити, що програма мережевого моніторингу не зможе розрізняти трафік від різних робочих станцій, якщо у цих робочих станцій, що знаходяться за маршрутизатором, не буде зовнішніх *(routable) IP*-ад-рес. Якщо у них немає зовнішніх *IP*-адрес, то всі пакети матимуть одну *IP*-адресу, тобто публічна *IP*-ад-реса вашої мережі.

Рис. 4. Моніторинг за допомогою хабів

Хаби: можливі проблеми

Крім того, щоб хаби мають меншу продуктивність, ніж комутатори, ви можете зіткнутися ще з двома проблемами при promiscuous-моніторингу з використанням хабів.

Перша проблема пов'язана з двохшвидкісними *(«auto-sensing»)* хабами, які підтримують апаратуру, що працює як із швидкістю 10 Мбіт/с, так і 100 Мбіт/с. Такі хаби не передають даних з портів, що працюють із швидкістю 10 Мбіт/с, портам, що працюють із швидкістю 1000 Мбіт/с і навпаки. Цю проблему можна вирішити, налашлувавши все ваше устаткування на якусь одну швидкість. Більшість багатошвидкісних карт дають вам можливість задати бажану швидкість.

Друга проблема пов'язана з хабами, які тільки формально називаються хабами, але всередині є комутаторами (так роблять деякі виробники, наприклад, *Linksys*). Виробники часто називають їх «інтелектуальними» або «комутованими», але можуть і не робити це. Навіть якщо в документації цього явно не вказано, хаб цілком може виявитися комутатором. Єдиний спосіб з'ясувати це — спробувати попрацювати з такою апаратурою. Старі і недорогі хаби найчастіше виявляються «справжніми» хабами. Іншим хорошим індикатором того, що перед вами «справжній» хаб — це індикатор *(LED)* колізій. У комутованих мережах колізій не буває, тому у комутатора ви такого індикатора не побачите.

Моніторинг за допомогою комутаторів

Керований *(managed)* комутатор з підтримкою дзеркалювання *(mirroring)* портів (функція, що дає змогу перенаправляти трафік з одних портів на певний порт комутатора) — ідеальний пристрій для мережевого моніторингу. Настройки дзеркалювання портів залежать від моделі і виробника (існують десятки подібних моделей, з цінами від $100 до кількох тисяч).

Нижче показано два типові варіанти з використанням з дзеркалювання портів (рис. 5, 6).

Варіант 1

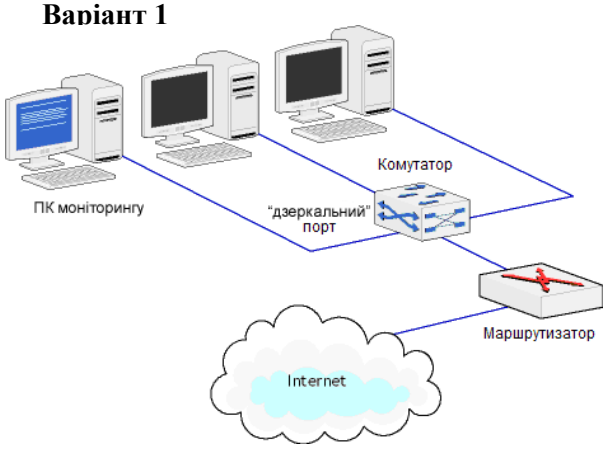


Рис. 5. Моніторинг за допомогою комутаторів

Варіант 2

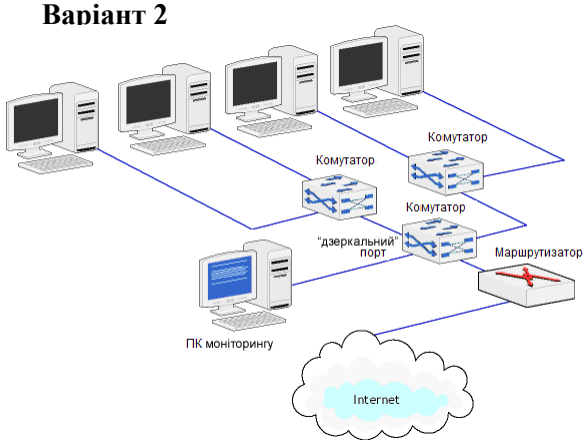


Рис. 6. Моніторинг за допомогою комутаторів

У цьому варіанті головний комутатор має функцію дзеркалювання портів. ПК моніторингу підключений до «дзеркального» порту, на який переправляється весь трафік з локальних робочих станцій і маршрутизатора. Комутатор можна налаштувати на перенаправлення даних з одного або з кількох портів.

Якщо в сегменті локальної мережі використовуються некеровані *(unmanaged)* комутатори, що не підтримують дзеркалювання портів, то ви можете додати керований комутатор. Направляючи Інтернет-трафік через комутатор, що підтримує дзеркалювання портів, ви підключаєте ПК моніторингу до дзеркального порту і тим самим отримуєте можливість перехоплювати трафік між локальними робочими станціями і маршрутизатором. Майте на увазі, що при даному мережевому підключенні у вас не буде можливості спостерігати трафік між локальними робочими станціями, оскільки він проходить через некеровані комутатори, і, отже, не доходить до керованого комутатора

Мережі *Wi-Fi* (802.11)

Навколо promiscuous-моніторингу *Wi-Fi*-мереж часто виникає багато плутанини, особливо серед користувачів, які професійно не займаються розробкою ПЗ для безпровідних мереж. Може показатися логічним, що якщо будь-який *Ethernet*-адаптер підходить для моніторингу локальних мереж, то і будь-який безпровідний адаптер підходить для тих же цілей в мережах 802.11 *a, b* або *g*. Теоретично це вірно, але насправді це далеко від реального положення справ.

Деякі виробники програм мережевого моніторингу пропонують вирішення даної проблеми за допомогою спеціальних драйверів з можливістю *RF*-моніторингу для обмеженої кількості бездротових карт. Таким чином, досить мати підтримувану бездротову карту, замінити початковий драйвер спеціальним — і ви можете здійснювати моніторинг бездротової мережі. Часто виникає питання — чи «Підтримує моя карта режим *promiscuous*»? На жаль, дане питання позбавлене сенсу. Це залежить від наявності драйвера. Правильне питання повинне звучати так: «Чи існує драйвер *RF*-моніторингу для моєї *Wi-Fi*-карти і операційної системи?».

Коли ваш мережевий аналізатор запущений і працює, вам необхідно залишатися в межах дії сигналу. Мабуть, це єдина умова моніторингу. Програма перехопить і відобразить пакети бездротової мережі, покаже вузли і точки доступу, рівень сигналу і інші важливі показники і статистику (рис. 7, 8).

Рис. 7. Моніторинг в мережі *Wi-Fi*

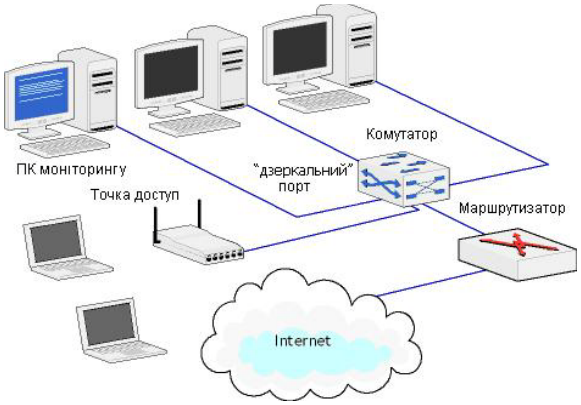


Рис. 8. Конфігурація мережі для бездротової мережі

Схема бездротового моніторингу достатньо проста: кілька комп'ютерів і точок доступу, а також комп'ютер з мережевим аналізатором поблизу. Ваш мережевий аналізатор покаже вузли бездротової мережі (рис. 9) приблизно так:

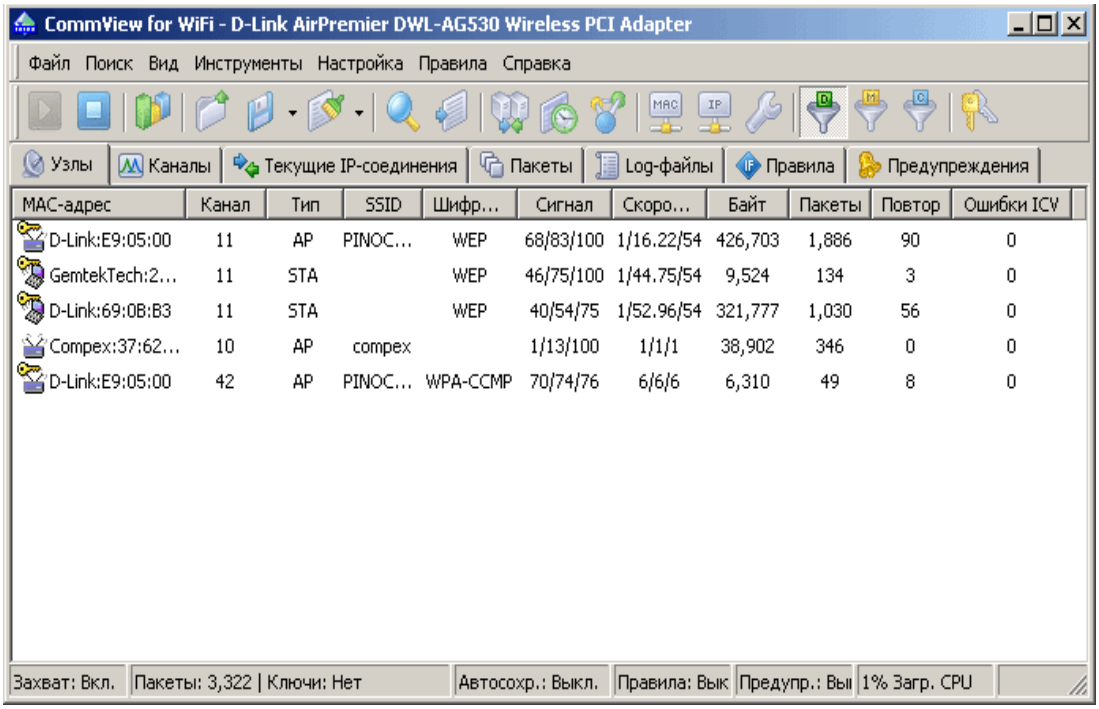


Рис. 9. Типова картина вузлів бездротової мережі за допомогою мережевого аналізатора

Варто відзначити, що в рамках даної конфігурації ви не зможете спостерігати трафік між бездротовими станціями і отримувати доступ до таких характеристик бездротової мережі, як рівень сигналу, швидкість передачі даних або дізнаватися про спроби вторгнення.

Висновок

Моніторинг і аналіз мережі представляє собою важливі етапи контролю роботи мережі. Для виконання цих етапів розроблено ряд програм і засобів, що працюють автономно і тоді, коли їх втручанні необхідне. До складу автономних програмних засобів моніторингу і аналізу входять засоби діагностики, аналізатори протоколів, експертні системи, сканери і тестери, багатофункціональні системи.

Існує необмежена кількість конфігурацій мережі. Проте, розуміння основних принципів мережевого моніторингу дозволить користувачеві забезпечити прозорість мережі практично в будь-якій ситуації. Природно, прозорість мережі не є кінцевою метою. Це всього лише основа, потрібна для правильної і грамотної роботи з програмами мережевого аналізу і моніторингу.

ЛІТЕРАТУРА

1. *Закер К.* Компьютерные сети. Модернизация и поиск неисправностей // СПб. : БХВ — Петербург, 2001. — 1008 с.

2. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы // Учебник для вузов. — 3-е изд. СПб. : Питер, 2006. — 958 с

3. *Рошан П., Лиэри Дж.* Основы построения беспроводных локальных сетей стандарта 802.11 // — М.: Издательский дом «Вильямс», 2004. — 304 с