

ОРГАНІЗАЦІЯ ЦЕНТРУ ОБЛІКУ ТА МОНІТОРИНГУ МЕРЕЖНОГО ТРАФІКУ ЗА ДОПОМОГОЮ БІЛІНГОВОЇ СИСТЕМИ «NG STAT»

У статті розглядається модель білінгової системи для обліку Інтернет-трафіку університетської мережі та досвід її комп'ютерної реалізації на базі операційної системи FreeBSD.

Постановка проблеми. Завдання підрахунку Інтернет-трафіку є актуальною проблемою, що постає перед системними адміністраторами, фахівцями, які відповідають за тарифікацію й облік послуг доступу по комутованих і виділених лініях. Тому на ринку програмного забезпечення є чимало різних систем обліку трафіку, або так званих білінгових систем [2].

Білінг (від англ. billing — складання рахунку) — у деяких видах бізнесу, зокрема, в телекомунікаціях — автоматизована система обліку наданих послуг, їх тарифікації і виставлення рахунків для оплати. На сучасних підприємствах використовують спеціалізовані білінгові системи — програмні продукти, що забезпечують автоматичне виконання всіх операцій і процедур, пов'язаних з білінгом [1].

Автоматизовані білінгові системи, що використовуються провайдерами, і сервери для контролю Інтернет-підключення в організаціях-клієнтах будуються навколо функції обліку трафіка, але інший функціонал їх сильно відрізняється.

Аналіз останніх досліджень і публікацій [2–4] свідчить, що для автоматизованих систем розрахунків характерна орієнтація у бік бухгалтерії й автоматизації бізнес-процесів оператора зв'язку. А сервери для контролю Інтернет-підключення, крім обліку трафіка, повинні гнучко управляти доступом користувачів до Інтернету, забезпечувати захист мережі, і, що особливо важливо, мати набір розвинених механізмів авторизації. Адже для провайдера з маршрутизованою мережею навіть авторизація на основі IP-адреси буде цілком достатньою, а от для організації, що використовує Інтернет, авторизація за IP-адресою ненадійна й незручна.

Саме тому шляхи розвитку програмних продуктів для провайдерів і для корпоративних користувачів розходяться усе далі. Кожен з цих програмних продуктів постійно оптимізується під завдання, характерні для своєї галузі використання. Так, якщо організація — Інтернет провайдер — слід вибирати автоматизовану систему розрахунків, якщо корпоративний користувач, то потрібний сервер контролю Інтернет-підключення. Для внутрікорпоративного використання сервер контролю Інтернет підключення не обов'язково повинен мати сертифікат, навпроти, наявність сертифіката здорожчує продукт і свідчить про його пристосованість під зовсім інші завдання.

Істотна частка програм реалізується на базі комп'ютера або сервера, який виконує функції маршрутизатора трафіку, або працює в режимі проксі-сервера. У найрозвинутіших операційних системах (Microsoft Windows Server, FreeBSD, Linux тощо) обидві моделі реалізовані одночасно. Програми розрізняються як наборами основних, так і додаткових функцій. Лідери галузі мають у своєму арсеналі максимальну кількість взаємопов'язаних сервісів, управляти якими можна за допомогою єдиного інтерфейсу.

Найзручніші для користувача такі програмні засоби, дистрибутив яких установлює на комп'ютер все, включаючи операційну систему й усі необхідні програми й утиліти. Це значно зручніше, ніж установлювати все окремо. Такі програми базуються на ОС Linux або FreeBSD.

Якщо говорити про подальший розвиток серверів контролю корпоративного Інтернет-підключення, то можна виділити такі напрями:

- програмні засоби матимуть додаткові сервіси для забезпечення всіх потреб клієнта для роботи з Інтернетом;
- доволі багато роботи буде виконано з інтеграції корпоративного поштового сервера й розв'язання завдань контролю спам-розсилок та інших загроз, пов'язаних з електронною поштою. Взагалі компонент інформаційної безпеки в серверах контролю корпоративного Інтернет-доступу буде істотно підсилюватися;
- розвиток користувацьких інтерфейсів відбуватиметься шляхом спрощення й автоматизації, щоб корпоративний Інтернет-доступ зрівнявся за простотою налаштування з мобільним телефоном.

Але такі програми, як правило, дорогі або мають доволі складний інтерфейс, деякі використовують проксі-сервер і дуже нестабільні в роботі при великих обсягах даних [3; 4]. Виходячи з того, що в Тернопільському національному педагогічному університеті імені Володимира Гнатюка вже створений корпоративний сервер з єдиною системою авторизації, ми вирішили написати власну білінгову систему, яка б максимально враховувала особливості архітектури та функціонування університетської мережі. **Метою** статті є розгляд практичних аспектів розробки центру обліку та моніторингу мережного трафіку на основі розробленої програми «NG-stat».

Починалося усе з розробки моделі розв'язання прикладної задачі (обліку Інтернет-трафіку), що передбачає дотримання таких вимог:

1. Система зберігає дані про весь трафік, що проходив через роутер, окрім трафіку тих підмереж, які виключені з обліку.

2. Система дає можливість отримувати дані про кожне з'єднання, що було встановлене через роутер, а також переглядати статистику в повному та спрощеному форматах.

3. Дані заносяться у базу даних безпосередньо, тобто збір статистики проводиться на рівні ядра операційної системи, і після перехоплення клієнтською програмою відразу відправляються у неї без використання будь-яких файлів. Це забезпечує значну швидкість опрацювання трафіку.

4. База даних містить дані про трафік за поточний і попередній місяці й має можливість надавати користувачеві звіт за кожен з них. Це необхідно для обмеження обсягу таблиць у БД.

5. Web-інтерфейс служить для відображення статистики у табличному та графічному виді, а також для керування білінговою системою незалежно від операційної системи.

Ця інформаційна модель стала основою для розробки комп'ютерної моделі системи обліку Інтернет-трафіку. Виходячи з неї, ми створили білінгову систему «NG stat». Програма збору статистики написана на Perl, протестована в операційних системах FreeBSD 5.5-STABLE і FreeBSD 6.2-STABLE.

Основні модулі розробленого білінгу

- 1 Модуль збору пакетів
- 2 Модуль внесення даних у БД
- 3 Серверна частина — опрацьовує Web-запити клієнта
- 4 Web-інтерфейс — дозволяє користувачам переглядати і модифікувати необхідні параметри, а також одержувати оперативні звіти;
- 5 База даних MySQL — єдине сховище і зв'язуюча ланка компонентів білінгової системи.

Перший етап розробки білінгової системи — встановлення програми `ng_ipacct`, що працює з пакетом `NETGRAPH`. Модуль `NETGRAPH`, доступний для операційної системи `FREEBSD`, починаючи з версії 4.xx, є механізмом об'єднання різних мережевих модулів її ядра у структури, що утворюють граф, і призначений для послідовної обробки пакетів даних. Тобто є можливість написати і використати достатньо зручну схему опрацювання даних в ядрі операційної системи. Більше того, легко здійснити зв'язок модуля ядра з `user-level` програмою.

Завантажувати в пам'ять `NETGRAPH` можна, використовуючи два методи: запускати потрібні модулі при старті або вкомпілювати їх відразу ж у ядро операційної системи. Ми вибрали останній варіант. Подальші дії полягали у компіляції ядра та установки програми `ng_ipacct`.

Подальша мета — одержати статистику й помістити її в базу даних. Для зняття статистики в `ng_ipacct` необхідно передати дані в контрольну точку, вивести їх й очистити контрольну точку для одержання наступної порції даних. Ось так це робиться для інтерфейсу `r10`:

```
root@ostwest : ipacctctl r10_ip_acct:r10 checkpoint
root@ostwest : ipacctctl r10_ip_acct:r10 show
root@ostwest : ipacctctl r10_ip_acct:r10 clear
```

У результаті можна побачити всі пакети, які проходили через інтерфейс. Статистика виводиться у досить зручному форматі:

```
<ip_джерела> <ip_призначення> <кількість пакетів> <кількість байт>
```

Наступний етап — потрібно, щоб усі дані зберігалися в базі даних MySQL для кожного хоста й інтерфейсу, розподілені по даті й часу. Для цього було визначено структуру бази даних,

її навантаження, вибрані оптимальні типи полів у таблицях, приділено увагу налаштуванню оптимальної продуктивності системи.

Програма `ng_ipasct` працює на рівні ядра, тому вимагає мало ресурсів системи, найбільш ресурсоємкою частиною в зборі статистики є перехоплення даних `user-level` програмою та запис цих даних у базу. Для економії системних ресурсів та збільшення продуктивності системи перехоплення даних розробленою програмою відбувається без запису на жорсткий диск, тобто джерелом даних є оперативна пам'ять, а не вінчестер.

Оскільки дані збираються дуже детально по кожному з'єднанню, на маршрутизаторах з великим потоком трафіку інформація накопичується дуже швидко. Тому було розв'язані також завдання оптимізації даних, що зберігаються в базі даних. Наприклад, якщо користувач здійснив кілька з'єднань з одним і тим же хостом в Інтернеті на один і той же порт у межах поточної порції даних, що вноситься в базу даних, немає необхідності зберігати ці дані як окремі рядки таблиці, а варто просумувати кількість переданої інформації протягом кожного з'єднання і ввести окреме поле таблиці — кількість з'єднань.

Оскільки в базі даних зберігаються дані лише за поточний та минулий місяці, після закінчення місяця дані з таблиці за минулий місяць експортуються у текстовий файл та архівуються. Для перегляду цих даних в системі розроблений механізм, що дозволяє перенести дані з архіву в резервну таблицю бази даних.

Також при записі даних, система розділяє вхідний та вихідний трафік, для цього у конфігураційному файлі системи були визначені локальні підмережі для яких здійснюється збір статистики.

Для підключення до бази даних зчитується конфігураційний файл і всі параметри, необхідні для того, щоб з'ясувати:

- з якого інтерфейсу збираються дані;
- ім'я сервера бази даних;
- ім'я бази даних;
- ім'я та пароль користувача для доступу до бази;
- підмережі, для яких проводиться збір статистики;
- підмережі, для яких не збирається статистика.

IP адреса	Порт	IP сервера	Кількість байт	Кількість з'єднань	Дата	Час	Тип трафіку
10.0.1.17	80	91.192.149.1	624	1	2008-04-21	11:03:21	Вихідний
10.1.1.19	53	192.175.48.1	290	1	2008-04-21	11:03:21	Вихідний
10.1.1.19	53	217.196.165.238	2796	14	2008-04-21	11:03:21	Вихідний
10.1.1.19	80	66.119.43.30	48	1	2008-04-21	11:03:21	Вихідний
10.1.1.181	138	10.255.255.255	239	1	2008-04-21	11:03:21	Вихідний
10.1.1.215	21	10.255.255.254	85	1	2008-04-21	11:03:21	Вихідний
10.1.1.215	22	10.255.255.254	2588	1	2008-04-21	11:03:21	Вихідний
10.1.2.5	80	58.211.78.72	48	1	2008-04-21	11:03:21	Вихідний
10.1.2.5	80	125.90.192.4	96	1	2008-04-21	11:03:21	Вихідний
10.1.2.38	138	10.255.255.255	229	1	2008-04-21	11:03:21	Вихідний
10.1.2.49	137	10.255.255.255	234	1	2008-04-21	11:03:21	Вихідний
10.1.2.77	137	10.255.255.255	78	1	2008-04-21	11:03:21	Вихідний
10.1.2.77	5900	1.3.3.7	96	2	2008-04-21	11:03:21	Вихідний
10.1.2.111	1728	66.252.13.209	144	1	2008-04-21	11:03:21	Вихідний
10.1.2.122	1728	66.252.13.209	96	1	2008-04-21	11:03:21	Вихідний
10.1.2.345	5900	66.252.13.228	144	1	2008-04-21	11:03:21	Вихідний
10.1.4.102	6646	10.255.255.255	792	1	2008-04-21	11:03:21	Вихідний

Рис. 1. Табличне представлення системи обліку Інтернет-трафіку

Після того як статистика отримана, настає найвідповідальніший етап. Необхідно привести до потрібного виду кожний перехоплений рядок, перевірити доступність сервера й необхідної бази даних і таблиці та внести дані.

Розроблений відповідний web-інтерфейс для роботи із системою. Він дає можливість адміністратору та користувачам системи переглядати дані про мережевий трафік за допомогою вибірки з бази даних за вказаними параметрами: IP-адреса джерела, порт, IP-адреса призначення, дата, час, напрям (вхідний, вихідний).

Також система дозволяє побачити адміністратору картину завантаження каналу в даний момент у графічному вигляді і надає дані про те, які IP-адреси і по яких портах вносять найбільшу частку в завантаження каналу. У системі передбачена можливість експортування зібраної інформації у файли pdf-формату, а також перегляд даних за минулі місяці з раніше створених архівних копій. Для адміністратора передбачені засоби управління користувачами системи.

Висновок. У процесі розробки системи «NG stat» були дотримані практично всі вимоги до білінгових систем, актуальні для роботи університетської мережі. Програма дозволяє надавати послуги з обліку трафіку при доступі в Інтернет. Для ідентифікації клієнта використовується його IP-адреса або інтерфейс маршрутизатора, через який він підключений до мережі. Система підтримує також віртуальні IP-адреси.

Ng_ipacct є зручним програмним пакетом для збирання повної й детальної статистики. Варто додати, що процес збирання статистики й запису отриманих даних засобами Perl є оптимальним, оскільки весь необхідний набір інструментів вбудований у нього.

У даний час білінгова система впроваджена і успішно експлуатується в Тернопільському національному педагогічному університеті імені Володимира Гнатюка.

ЛІТЕРАТУРА

1. Billing — Wikipedia, the free encyclopedia. — <http://en.wikipedia.org/wiki/Billing>.
2. Деньги любят счет — <http://www.vitmish.narod.ru/billing.htm>.
3. Дич Л. З. Развитие биллинговых систем // Компьютер-ИНФО. — 2001. — №15, 16, 20, 21.
4. Дич Л.З. Биллинговые системы: комплексное решение или специализация? // Технологии и средства связи. — 2001. — №4. — С. 43–48

Василь ФРАНЧУК

ВИКОРИСТАННЯ СИСТЕМИ УПРАВЛІННЯ ВМІСТОМ JOOMLA! У НАВЧАЛЬНОМУ ПРОЦЕСІ

В умовах розвитку відкритого інформаційного суспільства Інтернет-технології створюють унікальні можливості удосконалення засобів педагогічної діяльності та професійного розвитку. У зв'язку з цим виникає необхідність істотної зміни освітніх ресурсів як шкільного, так і вузівського рівня; створити й розробити нові засоби навчання, що відповідають таким вимогам, як:

1) актуальність відображуваних даних та їх відповідний зв'язок з конкретною предметною областю;

2) орієнтація на задоволення інформаційних потреб користувачів-учасників педагогічного процесу (учителів, студентів, учнів) та цілеспрямований розвиток їхнього інтересу.

Основними проблемами розвитку освітніх ресурсів є:

1) недостатня кількість викладачів і фахівців, що мають реальний досвід розробки освітніх Інтернет-ресурсів;

2) недостатньо розвинена комунікаційна інфраструктура в країні (незадовільна швидкість зв'язку у навчальних закладах при роботі в Інтернет);

3) невелика кількість інформаційних ресурсів освітнього характеру на українській і російській мовах.

Аналіз останніх досліджень потреб інформаційного суспільства свідчить, що існує певний дефіцит відповідних освітніх Інтернет-ресурсів. Безперечно, це залежить від рівня системних досліджень щодо проблеми розробки технології конструювання освітніх сайтів. Другий аспект розвитку освітніх Інтернет-ресурсів — розробка добре продуманого механізму керування даними на цих ресурсах. Зрозуміло, необхідність створення та наповнення сайту, що складається з багатьох сторінок або потребує постійного оновлення змісту, переобтяжено проблемами їх статичності. Використання тільки мови HTML сильно затягує в часі ці процеси, а періодичні