

І н ф о р м а т и з а ц і я т а б е з п е к а

УДК 382

ЗУБОК В.Ю., доцент Інституту спеціального зв'язку і захисту інформації при НТУУ “Київський політехнічний інститут”, заступник директора ТОВ “Інформаційний центр “Електронні вісті”,
ГОЛОВІН А.Ю., курсант Інституту спеціального зв'язку і захисту інформації при НТУУ “Київський політехнічний інститут”

ОГЛЯД І ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДИК ТА ЗАСОБІВ ДОСЛІДЖЕННЯ ТОПОЛОГІЇ ІНТЕРНЕТУ

Анотація. Опис, приклади та порівняння трьох методів вивчення топології Інтернету.

Аннотация. Описание, примеры и сравнительный анализ трех методов изучения топологии Интернета.

Summary. Description, examples and comparison of three methods of study of topology of the Internet.

Ключові слова: топологія Інтернету, складна мережа, трасування, автономна система, реєстр маршрутизації.

У прикладних дослідженнях звичайно застосовують такі типи для мережного аналізу характеристики, як розмір мережі, мережна щільність, розподіл ступеню вузлів, ступінь центральності тощо. Аналіз складних мереж зараз широко використовується в економіці (аналіз ринків), менеджменті (відносини між підприємствами та всередині організацій), соціології, медицині (поширення вірусів інфекцій) та криміналістиці (взаємозв'язки терористичних організацій, шляхи розповсюдження наркотиків та зброї).

Інтернет, як характерний представник складних мереж, з огляду на свою структуру і динамічну поведінку, потребує спеціальних методик дослідження. Він, як глобальна телекомунікаційна мережа, складається із сотень тисяч вузлів, що здійснюють передачу методом пакетної комутації. Для передачі даних в якості стандарту використовуються єдині протоколи міжвузлової маршрутизації і правила побудови політик маршрутизації.

Для дослідження топології мережі Інтернет можна використати наступні методики:

1. Аналіз таблиць маршрутизації на рівні взаємодії автономних систем.
2. Метод traceroute – трасування маршрутів.
3. Аналіз баз даних реєстрів маршрутизації (наприклад – RIPE NCC Routing Registry).

За результатами різноманітних досліджень Інтернет-інфраструктури є можливість прослідкувати динаміку змін топології певних ділянок (чи “сегментів”) Інтернет. Особливий вплив на зв'язність мають мережі обміну трафіком (network access points чи traffic exchanges), які з'являються та розвиваються протягом багатьох років.

Метою роботи є розгляд зазначених методик та аналіз результатів їх застосування.

Еволюція Інтернету: частково керований розвиток. У 1969 році Агенція проектів з передових досліджень Міністерства оборони США розпочала науково-дослідний проект з побудови експериментальної мереж з пакетною комутацією. Мета – розробка технології передачі даних, яка була надійною, стійкою до ушкоджень мережі та не залежала від будь-якого виробника телекомунікаційного обладнання. Ця мережа отримала назву ARPANET.

Розробка була настільки вдалою, що організації, які мали відношення до проекту, стали використовувати її для повсякденного передавання даних. Тому у 1975 році відбулася конверсія ARPANET з науково-дослідної мережі в операційну мережу, за яку відповідала агенція з оборонних телекомунікацій (DCA).

У 1983 році протоколи TCP/IP було стандартизовано як військові стандарти. В університеті Берклі ці протоколи було інтегровано в операційну систем BSD UNIX. У 1985 році до існуючої мережі приєдналась наукова мережа Національної наукової фундації (NSF) – NSFnet. З того часу термін Інтернет став загальноживим.

Велика кількість вузлів Інтернету стала проблемою для керування мережею. Тому з 1986 році в NSFNet застосовувалась трирівнева мережна архітектура: місцеві (локальні мережі, мережі кампусів) підключались до регіональних мереж, які в свою чергу підключались до опорної мережі, що підтримувалась 6 загальнонаціональними суперкомп’ютерними центрами NSF, як наведено на Рис. 1 [1].



Рис. 1. Мережа NSFNet в 1986 – 1988 роках

До 1988 року основні канали передачі даних працювали на швидкості 56 Кбіт/с. В 1987 році консорціум за участі Merit (міжуніверситетської комп’ютерної дослідницької мережі), IBM, MCI виграв грант NSF на реінжиніринг та обслуговування NSFNet. В ході робіт канали були змінені на канали T1 (1,5 Мбіт/с). Канали T1 об’єднали 6 суперкомп’ютерних центрів та ще 13 вузлів мереж по всій території США (Рис. 2).

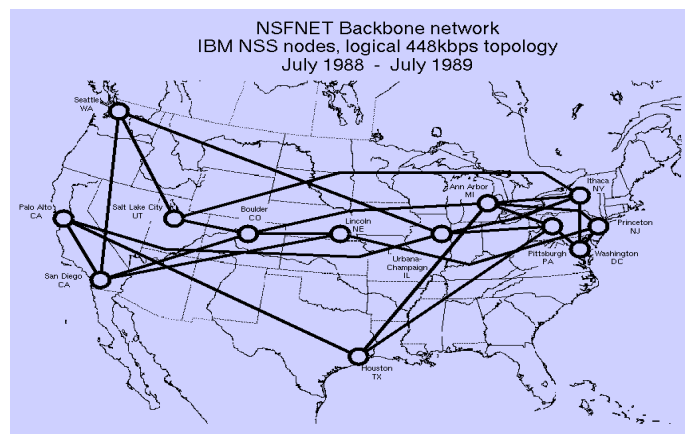


Рис. 2. T1-мережа NSFNet в 1988 – 1989 роках

За словами Елізи Геріх, віце-президента ICANN (нинішнього керівного органу Інтернету), яка особисто брала участь в цих роботах, така інфраструктура мала б

слугувати становим хребтом мережі протягом 5 років. Але вже за 18 місяців, у 1991 році, обсяги трафіку змусили переводити канали T1 на T3 – 45 Мбіт/с (з виступу на форумі RIPE NCC Regional Meeting, Москва, 29.09 – 01.10.10 р.). Схему нової мережі наведено на Рис.3. Точки доступу (network access point – NAP) спочатку були розділені на державні (федеральні – FIX) та комерційні (CIX). Приблизно з 1994 року такий розподіл зник. Разом з цим, зник розподіл користувачів на державні, академічні та комерційні організації. Поняття NAP та вимоги до них були формалізовані, і це відкрило шлях до побудови нових точок.

NAP, за термінологією NSFNET – це комплекс з одного чи більше швидкісних комутаторів, до яких під'єднується певна кількість маршрутизаторів для обміну трафіком. Всі мережі при підключенні до NAP автоматично отримують дозвіл обміну трафіком з іншими мережами. Пропускна спроможність мережі, що підключається, має бути співмірною з вже підключеними мережами.

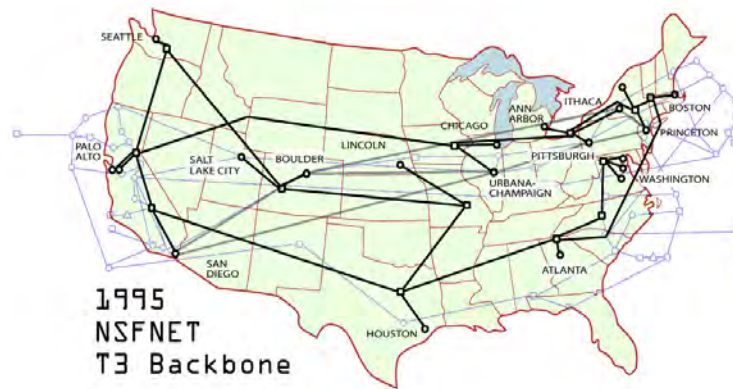


Рис. 3. T3-мережа NSFNet в 1992 – 1995 роках

Для кожної NAP призначалась посада – менеджер NAP. До його обов’язків входило розгортання, технічне, організаційне, комерційне обслуговування NAP та планування її розвитку.

Але існувала можливість взаємного підключення вузлів поза межами NAP, тому топологія Інтернету в результаті розвитку отримала так звану безмасштабну структуру.

В результаті розробки і публікації “NSFNet Acceptable Use Policy” та відкритості точок доступу Інтернет набув стрімкого розвитку. Тому у 1995 році близько 44 % префіксів у таблиці маршрутизації були з-поза меж США.

В топології сучасного Інтернету NAP, чи, як їх зараз називають, – мережі обміну трафіком або біржі трафіку (Internet Exchanges) відіграють дуже важливу роль. Лише деякі з них керуються політикою та процедурами того часу. Одною з “класичних” мереж обміну трафіком є Українська мережа обміну трафіком (UA-IX).

Ще на початку 1980-х років розробники Інтернет-технологій бачили тенденцію щодо швидкого зросту мережі, неструктурованого збільшення кількості шлюзів, які були під керуванням зовсім різного програмного забезпечення та не підлягали типовому обслуговуванню. Передбачуваними наслідками такого зросту стали:

- багаторазове збільшення потоків інформації, пов’язаної з передачею та обробкою таблиць маршрутизації;

- неможливість обслуговування Інтернету як єдиної системи через неможливість ізоляції помилок, збоїв маршрутизації;

- через різноманітність мережного обладнання, алгоритмів маршрутизації та програмного забезпечення в мережах, які взаємодіють через Інтернет, неможливо

забезпечити пропоновані зміни у всій мережі одночасно, бо це потребує адаптації до кожної окремої системи.

Тоді й виникла ідея увести поняття домену, або автономної системи, єдиної частки мережі, із будь-яким внутрішнім устроєм, але стандартними зовнішніми маршрутизаторами, які реалізують стандартні протоколи взаємодії з іншими автономними системами. Автономні системи повинні мати можливість не тільки взаємодіяти одна з одною, а й забезпечувати транзитні функції для автономних систем, які не мають безпосереднього зв'язку, аби забезпечити для кінцевого користувача “прозорість” Інтернету як єдиної мережі. Ця ідея знайшла відображення в документі RFC 827 “Зовнішній шлюзовий протокол” (Exterior Gateway Protocol – EGP), або протокол зовнішньої маршрутизації [2].

Аналіз таблиць маршрутизації на рівні автономних систем. Автономна система (AS) – це поєднана група з одного або більше IP-префіксів, які керуються одним чи більше операторами та мають єдину чітко визначену “зовнішню” політику маршрутизації. Кожна AS має 16-бітний номер для ідентифікації в процесі обміну інформацією с іншими AS [3].

Обмін маршрутною інформацією на рівні автономних систем здійснюється із використанням протоколу зовнішнього шлюзу (Exterior Gateway Protocol, EGP). В Інтернет діє протокол зовнішнього шлюзу BGP (Border Gateway Protocol) версії 4. BGP-4 призначений для обміну інформацією про маршрути, які реалізують політику маршрутизації між автономними системами. Для рішення по маршрутизації BGP-4 не використовує технічні метрики каналів, а здійснює вибір найкращого маршруту виходячи з правил, прийнятих у мережі, тобто політики маршрутизації. Протокол має засоби фільтрації маршрутною інформації, встановлення пріоритетів у відповідності із політикою, але не має засобів публікації цієї політики. Для публікації правил маршрутизації автономних систем використовуються централізовані бази даних – реєстри маршрутизації (Internet Routing Registry, IRR). Прикладом такого реєстру є БД RIPE NCC.

Найбільш точну і актуальну інформацію про зв'язки між вузлами мережі на рівні автономних систем можна отримати, дослідивши таблиці маршрутизації маршрутизаторів, які взаємодіють з найбільшою кількістю автономних систем. Для реалізації цієї методики дослідження необхідно мати чи безпосередній доступ до такого маршрутизатора, чи доступ через так звані сервери-“дзеркала” (looking glass servers). На Рис. 4 зображено приклад таблиці маршрутизації BGP:

```
> sh ip bgp neighbor 80.81.192.145 route
BGP table
                                Status codes: * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete
  Network      Next Hop      Metric LocPrf  Weight  Path
*> 193.107.109.0/24  80.81.192.145      100                21219 21354 50027 i
*> 213.5.192.0/21    80.81.192.145      100                21219 50130 50130 50130 50130 i
*> 193.34.72.0/22    80.81.192.145      100                21219 39189 39189 i
*> 193.107.108.0/24  80.81.192.145      100                21219 21354 50027 i
*> 213.111.104.0/21  80.81.192.145      100                21219 48683 i
*> 195.95.189.0/24  80.81.192.145      100                21219 41105 i ...
```

Рис.4. Фрагмент бази маршрутів протоколу BGP-4

Кожен мережний префікс містить атрибут AS_PATH, аналіз якого і дозволяє робити висновки стосовно взаємодії автономних систем.

Інформація, що знаходиться в цій таблиці, відображає актуальний стан взаємодій “прикордонних” маршрутизаторів автономних систем.

Трасування маршрутів. Трасування – спосіб визначення маршрутів слідування даних у мережах TCP/IP. Трасування реалізовано у вигляді службової утиліти багатьох операційних систем (tracert у системах Windows; traceroute – у Unix-подібних операційних системах). Функціонування утиліти tracert засновано на протоколі ICMP, traceroute – UDP. В обох випадках використовується інкрементація поля заголовка TTL (time-to-live) та аналіз адреси хоста, який повертає ICMP-повідомлення в разі вичерпання TTL. Приклад виконання трасування маршруту утилітою traceroute зображений на Рис. 5:

traceroute to www.google.com (66.102.13.106), 30 hops max, 40 byte packets (AS 3549)

1	gw.dev.nikrtr.ripe.net (193.0.4.2)	1.327 ms	2.286 ms	0.453 ms (AS 3303)
2	GigabitEthernet6-17.car2.ams1.level3.net (195.69.144.110)	1.040 ms	0.987 ms	1.145 ms (AS 3303)
3	ae-1-51.edge3.Amsterdam1.Level3.net (4.69.139.137)	0.954 ms	1.105 ms	0.975 ms (AS 3356)
4	212.72.42.14 (212.72.42.14)	1.465 ms	1.334 ms	1.408 ms (AS 3303)
5	209.85.254.92 (209.85.254.92)	1.549 ms	1.512 ms	2.031 ms (AS 3303)
6	216.239.49.30 (216.239.49.30)	5.425 ms	5.298 ms	5.406 ms (AS 3303)
7	64.233.174.137 (64.233.174.137)	5.364 ms	8.684 ms	6.648 ms (AS 3549)
8	ez-in-f106.1e100.net (66.102.13.106)	5.751 ms	5.581 ms	5.623 ms (AS 3549)

Рис. 5. Трасування маршруту утилітою traceroute

За рахунок особливостей роботи протоколів маршрутизації в мережі Інтернет зворотні маршрути часто не збігаються із прямими. Тому ICMP – відповідь від кожного проміжного маршрутизатора може йти своїм власним шляхом, який відрізняється від шляху, яким повертався б пакет від кінцевої точки призначення. Він може загубитися або прийти з великою затримкою, хоча в реальності із пакетами, адресованими кінцевому вузлу, такого б не сталося.

Для того щоб дізнатися структуру ділянки мережі за допомогою трасування маршруту, треба виконувати його з багатьох вихідних та для багатьох кінцевих вузлів. При цьому метод дає змогу дізнатись лише основні маршрути, оптимальні з точки зору протоколів маршрутизації в момент проведення експерименту. Тому в реальній практиці для вивчення мережі використовують накопичені дані traceroute з великої кількості вимірювань.

Дані traceroute містять також час проходження даних до кінцевої точки та в зворотному напрямку (round-trip time). На цей час ці дані використовуються проектом The Cooperative Association for Internet Data Analysis (CAIDA) для оцінки, зокрема, географічної відстані між вузлами та візуалізації Інтернету на географічній карті.

Аналіз накопичених даних маршрутизації. Існують наукові проекти, що безпосередньо займаються дослідженням Інтернет-інфраструктури протягом багатьох років. Прикладом такої організації є вже згаданий проект CAIDA, який націлений на аналіз та підтримку розвитку глобальної Інтернет-інфраструктури [4].

Дослідження ведуться у напрямках маршрутизації, топології, безпеки, аналізу трафіку та візуалізації.

Дослідження топології проводиться із 2004 року шляхом побудови знімків BGP таблиць, отриманих з декількох маршрутизаторів. У публічно доступних архівах CAIDA містяться файли із зв'язками між автономними системами. Проаналізувавши ці дані можна побудувати топологію зв'язків між автономними системи. Приклад такого файлу зображений на Рис. 6. Така інформація є дуже корисною, адже окрім топології можна також досліджувати розвиток мережі в ретроспективі.

```
# RouteViews BGP AS links annotated with inferred relationships.
# See http://as-rank.caida.org
#
# Dataset date: 20100120
# Alpha parameter of inference algorithm: 0.01000
#
# Format: <AS1> <AS2> <relationship>
# where
# <AS1> and <AS2> are AS numbers, and
# <relationship> is -1 if AS1 is a customer of AS2,
#                 0 if AS1 and AS2 are peers,
#                 1 if AS1 is a provider of AS2, and
#                 2 if AS1 and AS2 are siblings (the same organization).
8563 4323 -1
44919 39040 -1
44919 29691 -1
44919 6939 -1
28801 702 -1
28801 8422 -1
28801 8220 -1
5006 36784 1
5006 18723 1
5006 30055 1
5006 30220 1
5006 33362 1
5006 11619 1
```

Рис. 6. Файл даних про зв'язки між АС

Аналіз даних реєстрів маршрутизації. Політика маршрутизації – це набір правил, за якими автономна система приймає рішення стосовно маршрутизації. Обмін цими правилами з іншими автономними системами (за допомогою протоколів зовнішньої маршрутизації) також є частиною політики маршрутизації. Протокол маршрутизації BGP-4 не має засобів публікації політики маршрутизації. Для вирішення цієї проблеми у 1995 році був заснований Реєстр маршрутизації в Інтернеті (IRR). Мета IRR – забезпечити обмін між операторами мережі актуальною інформацією з маршрутизації та сприяти, таким чином, стабільності й цілісності маршрутизації Інтернету в цілому. IRR складається з декількох баз даних, в яких оператори публікують власні політики маршрутизації та анонси таким чином, що інші оператори можуть будувати свої вхідні та вихідні фільтри на основі даних IRR. Інформація з маршрутизації в IRR публікується на сервері маршрутів (routing information server, RIS) та зберігається в так званих об'єктах “Автономна система” за номером AS (aut-num). Інформація в об'єкті показує, як певна мережа маршрутизується в Інтернеті. Будується інформація на основі угод про взаємодію між AS з використанням понять import та export.

Web-інтерфейс RIS RIPE NCC (Рис. 7) не дає можливості зробити вибірку із БД необхідної інформації, а лише надає користувачеві інтерфейс для односкладних запитів.

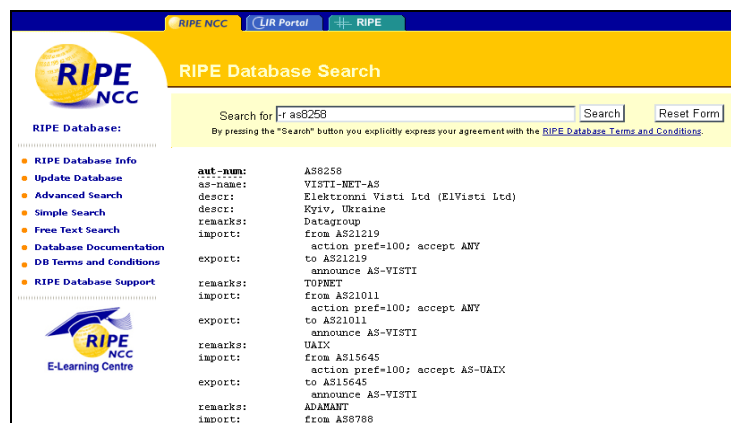


Рис.7. Інтерфейс бази даних RIPE NCC та відображення елементів маршрутизації

Для отримання інформації про структуру ділянки мережі за допомогою бази даних реєстру маршрутизації треба автоматизувати виконання запитів для багатьох автономних систем.

Інформація в реєстрі маршрутизації представлена у вигляді політики взаємодії між автономними системами через поля `import` та `export`, які відображають зв'язки.

Слід зазначити, що записи в полі `members` на сторінці в БД можуть бути двох типів:

- безпосередньо номери автономних систем;
- `as-set` – об'єднання автономних систем (зазвичай `as-set` – це провайдер, який обслуговує клієнтів).

Дані про взаємодію автономних систем, представлені в RIS, є найбільш загальними. Їхня особливість в тому, що вони відображають саме політику маршрутизації, але не містять даних про стан взаємодії між вузлами в певний момент часу. Можна сказати, що вони відображають можливість транзиту трафіку однієї автономної системи через іншу, але не відображають факту – чи є такий транзит у даний момент. Загалом, в даних IRR міститься інформація про кількість зв'язків, що на 20-50 % перевищує справжню, яку можна дослідити аналізом таблиць BGP-маршрутизаторів [5].

Висновки.

У результаті виконання аналізу розглянуто методики дослідження мережі Інтернет. Дослідження такого характеру є досить актуальні та мають за мету підтримку розвитку Інтернет-інфраструктури.

Використавши будь-який із представлених методів, можна отримати наглядну інформацію про топологію ділянки мережі і зробити висновки щодо її оптимальності, а також визначити “вузькі місця”. Але дані, отримані різними методами, будуть відмінними через особливості методик.

Дані, зібрані на основі аналізу BGP-таблиць, відображають актуальний стан взаємодій “прикордонних” маршрутизаторів автономних систем.

Використання утиліти `traceroute` дає змогу дізнатись лише основні маршрути, оптимальні з точки зору протоколів маршрутизації в момент проведення експерименту. В реальній практиці для вивчення мережі використовують накопичені дані `traceroute` з великої кількості вимірювань. Через це дані, отримані методом `traceroute`, є найбільш складно узагальнюваними.

Дані реєстрів маршрутизації загалом містять найбільшу кількість зв'язків, бо відображають правила (політику) взаємодії, а не реальний стан такої взаємодії. Натомість реальна картина зв'язків Інтернету змінюється кожної миті. Для вивчення та вдосконалення мережі на певній ділянці варто сконцентруватись на дослідженні BGP-таблиць маршрутизаторів цієї ділянки.

Використана література

1. NSF and the Birth of the Internet. – Режим доступу : [//www.nsf.gov/news/special_reports/nsf-net/60s_to_90s_map.pdf](http://www.nsf.gov/news/special_reports/nsf-net/60s_to_90s_map.pdf)
2. RFC 827. Exterior Gateway Protocol (EGP) Eric C. Rosen, Bolt Beranek and Newman Inc., October 1982. – Режим доступу : [//www.tools.ietf.org/html/rfc827](http://www.tools.ietf.org/html/rfc827)
3. RFC 1930. Guidelines for Creation, Selection, and Registration of an Autonomous System. J. Hawkinson, T. Bates, March 1996. – Режим доступу : [//www.tools.ietf.org/html/rfc1930](http://www.tools.ietf.org/html/rfc1930)
4. The Cooperative Association for Internet Data Analysis (CAIDA). – Режим доступу : [//www.caida.org/home/about](http://www.caida.org/home/about)
5. The Rich-club Phenomenon in the Internet Topology. Shi Zhou and Raul J. Mondragon, IEEE Communications, vol. 8, NO 3, March 2004.

~~~~~ \* \* \* ~~~~~