План лекції . Тема 4. Протоколи збору трафіку.

- Протоколи збору трафіку: SNMP, Netflow, IPFIX, sFlow, JFlow
- Визначення та основні характеристики та інструменти SNMP
- Огляд протоколів IPFIX та JFlow
- Визначення та основні характеристики протоколів NetFlow та sFlow.
- Використання протоколів NetFlow та sFlow для збору мережевих статистичних даних.
- Аналіз та використання даних, зібраних за допомогою протоколів NetFlow та sFlow.

Вступ

Мережеві протоколи відіграють ключову роль у вдосконаленні ефективності мережі, забезпечуючи збір та аналіз важливих статистичних даних. Вони дозволяють мережевим адміністраторам відстежувати трафік, ідентифікувати проблеми та аномалії, оптимізувати ресурси та приймати обгрунтовані рішення для поліпшення загальної ефективності мережевого середовища.

Протоколи мережевого моніторингу є необхідною складовою загальної стратегії управління мережею. Їх використання дозволяє забезпечити стабільність, безпеку та ефективність мережі. Ці протоколи забезпечують засоби для отримання об'єктивної інформації про мережевий трафік та його характеристики, що дозволяє розробляти та впроваджувати ефективні стратегії управління ресурсами, планування мережі та виявлення проблем. У результаті, ці протоколи сприяють підвищенню надійності та продуктивності мережі, що відповідає загальним цілям управління мережею.

Протоколи FLOW – це сімейство протоколів, які використовуються для експорту інформації про маршрутизацію та комутацію з мережевих пристроїв. Ця інформація може використовуватися для моніторингу мережі, аналізу трафіку та планування мережі.

Функціональні можливості:

- **Моніторинг мережі**. Дозволяють виконувати моніторинг мережевого трафіку та виявлення проблем з мережею.
- **Аналіз трафіку**. Можуть використовуватися для аналізу мережевого трафіку та визначення його характеристик.
- **Планування мережі**. Дозволяють виконувати планування мережі та прогнозування потреб у пропускній здатності.

Типи протоколів FLOW:

- **NetFlow**. Розроблений Cisco Systems і є найпоширенішим протоколом FLOW.
- **IPFIX**. Протокол є стандартом IETF і може використовуватися для експорту даних FLOW з різних типів мережевих пристроїв. IETF - це скорочення від "Internet Engineering Task Force" (Інженерна робоча група Інтернету) - організація, що займається розробкою та стандартизацією протоколів Інтернету.
- **sFlow**. Розроблений компанією InMon Corporation - американською компанією, що спеціалізується на моніторингу мережевого трафіку і аналітиці мережевої продуктивності. Може використовуватися для експорту даних FLOW з різних типів мережевих пристроїв.

Використання NetFlow та sFlow є невід'ємною частиною сучасних мережевих технологій, оскільки ці протоколи надають важливі статистичні дані для ефективного управління мережевим середовищем, але розповідь про мережеві протоколи була б неповною без загального огляду протоколів збору трафіку.

Протоколи збору трафіку: SNMP, IPFIX, JFlow

SNMP

Протокол простого мережевого моніторингу SNMP – протокол прикладного рівня, який є частиною протоколу TCP/IP. Він дозволяє керувати продуктивністю мережі, знаходити й усувати проблеми, планувати зростання мережі. Він збирає статистику по трафіку до кінцевого хоста через пасивні датчики, які реалізуються разом з маршрутизатором.

Головні розробники та організації, що брали участь у створенні SNMP:

- IETF (Internet Engineering Task Force) – міжнародна організація, що займається розробкою та стандартизацією мережевих протоколів, у тому числі SNMP.
- Marshall T. Rose – один із ключових авторів SNMP, а також основних RFC, які визначають цей протокол.
- Jeffrey D. Case, Keith McCloghrie, Martin Schoffstall, James R. Davin – група експертів, що працювала над створенням SNMPv1.
- OSI Management Framework – на початку SNMP розглядався як тимчасове рішення, поки не буде завершена більш складна система управління мережею в моделі OSI (CMIP – Common Management Information Protocol), але врешті-решт SNMP став стандартом де-факто.

Існують дві версії (SNMP v1 і SNMP v2), SNMP v2 побудований на SNMP v1 і пропонує ряд удосконалень, таких як додавання операцій з протоколами. Стандартизований ще один, додатковий варіант версії SNMP. Версія 3 (SNMP v3) який відрізняється від перших двох підвищеною безпекою використання.

Загалом, для протоколу SNMP притаманні три ключові компоненти: керовані пристрої (Managed Devices), агенти (Agents) та системи управління мережею (NMSs – Network Management Systems) (рис. 04.01).

Керовані пристрої включають в себе SNMP-агента і можуть складатися з маршрутизаторів, перемикачів, комутаторів, концентраторів, персональних комп'ютерів, принтерів і інших елементів, подібних до цих. Вони несуть відповідальність за збір інформації та роблять її доступною для системи управління мережею (NMS).

Агенти включають в себе програмне забезпечення, яке володіє інформацією з управління, і переводять цю інформацію в форму, сумісну з SNMP. Вони закриті для пристрою управління.

Системи управління мережею (NMS) виконують додатки, які займаються моніторингом і контролем пристроїв управління. Ресурси процесора і пам'яті, які необхідні для управління мережею, надаються NMS. Для будь-якої керованої мережі повинна бути створена хоча б одна система управління. SNMP може діяти виключно як NMS, або агент, або може виконувати свої обов'язки або ін.

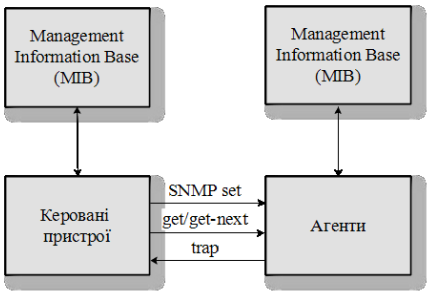


Рис. 04.01. Архітектура SNMP

Існує 4 основних команди, що використовуються SNMP NMS для моніторингу і контролю керованих пристроїв: **читання, запис, переривання і операції перетину.**

Операція читання розглядає змінні, які зберігаються керованими пристроями. **Команда запису** змінює значення змінних, які зберігаються керованими пристроями. **Операція перетину** отримує інформацію, які змінні керованих пристроїв підтримуються, і збирає інформацію з підтримуваних таблиць змінних. **Операція переривання** використовується керованими пристроями для того, щоб повідомити NMS про настання певних подій.

Іншими словами, SNMP використовує 4 протокольні операції в порядку дії: **Get, GetNext, Set і Trap**.

- ✓ **Get** використовується, коли NMS видає запит на інформацію для керованих пристроїв. SNMPv1-запит складається з заголовка повідомлення і одиниці даних протоколу (PDU). PDU – повідомлення містить інформацію, яка необхідна для успішного виконання запиту, який буде або отримувати інформацію від агента, або ставити значення в агента. Керований пристрій використовує SNMP агентів, розташованих в ньому, для отримання необхідної інформації і потім посилає повідомлення NMS, з відповіддю на запит. Якщо агент не володіє будь якою інформацією стосовно запиту, він нічого не повертає.
- ✓ **GetNext** буде отримувати значення наступного примірника об'єкта.
- ✓ **Set.** Для NMS також можливо надсилати запит (операція Set), коли встановлюється значення елементів без агентів.
- ✓ **Trap.** Коли агент повинен повідомити NMS – події, він буде використовувати операцію Trap.

SNMP – протокол рівня додатків, який використовує пасивні сенсори, щоб допомогти адміністратору простежити за мережним трафіком і продуктивністю мережі, SNMP може бути корисним інструментом для мережного адміністратора, він створює можливість для загрози безпеки, тому що він позбавлений можливості автентифікації.

Моніторинг та управління по SNMP передбачає три режими роботи з пристроями:

- ➢ **Збір лише важливих значень**. В цьому випадку розглядаються тільки ті змінні, дані яких використовуються під час моніторингу. Такий підхід дозволяє заощадити обчислювальні і мережеві ресурси.
- ➢ **Збір всіх значень з MIB-директорії.** Система збирає значення всіх змінних, для яких існують MIB-опису. Режим забезпечує збір повної інформації про роботу пристрою. Проаналізувавши ці дані, зможемо вирішити, які аспекти потребують моніторингу.
- ➢ **Збір всіх значень, доступних при скануванні.** Система збирає всі доступні SNMP-змінні, незалежно від того, є їх опису чи ні. Нерозпізнані величини представляються в табличній формі і просто не мають зрозумілих описів і імен. Такий підхід дозволяє отримати всі дані, що надаються пристроєм, а потім підібрати для невизначених значень MIB з метаінформацією.

Протягом багатьох років регулярний моніторинг мережі виконувався протоколом SNMP, який надає огляд IT-інфраструктури, надаючи мережним адміністраторам інформацію про наявність його компонентів і, як зрозуміло з наявності різних версій, SNMP пройшов декілька еволюційних етапів, кожен з яких приносив покращення в безпеці, ефективності та функціональності.

Розглянемо детальніше версії SNMP

- ➢ **SNMPv1 (1988).** Це перша версія протоколу, яка отримала широке поширення завдяки простоті впровадження.

Основні особливості:

Використовує "community strings" для аутентифікації (public – для читання, private – для запису).

Підтримує базові операції:

Get – отримання значення певного параметра.
Set – зміна значення параметра.
GetNext – отримання наступного значення в таблиці OID (об'єктний ідентифікатор).
Trap – надсилання повідомлення про події агентом до сервера SNMP Manager.

Недоліки SNMPv1:

Відсутність механізму шифрування → всі дані передаються у відкритому вигляді. Community strings (рядки аутентифікації) передаються незахищеними.
Немає підтримки групових запитів → обмежена ефективність при зборі великих обсягів даних.
Через ці обмеження SNMPv1 більше не рекомендується для використання в сучасних мережах.

- ➢ **SNMPv2 (1993–1996) –** Покращена продуктивність Щоб усунути обмеження SNMPv1, було розроблено SNMPv2, який приніс значні покращення у швидкості збору даних і функціональності.

Основні покращення у SNMPv2:

Операція GetBulk – дозволяє отримувати великі обсяги даних за один запит (замість послідовного GetNext в SNMPv1).
Розширені SNMP Traps – агент може надсилати більше деталей про подію.
Покращена обробка помилок – введено більш детальні коди помилок для кращої діагностики.

Різновиди SNMPv2:

- ✓ **SNMPv2p (Party-based SNMPv2)** – перша версія з покращеною безпекою, але була складною у впровадженні, тому не стала популярною.
- ✓ **SNMPv2u (User-based SNMPv2)** – ще одна спроба покращити безпеку, яка теж не отримала широкого використання.
- ✓ **SNMPv2c (1996)** – спрощена версія, яка повернулася до community strings як в SNMPv1, але з усіма покращеннями продуктивності SNMPv2.

Недоліки SNMPv2c:

Все ще відсутнє шифрування, аутентифікація здійснюється через відкриті рядки (community strings).
Community strings можна перехопити, що робить SNMPv2c небезпечним для використання в незахищених мережах.

- ➢ **SNMPv3 (2002)** – Безпечний SNMP. Щоб виправити проблеми безпеки попередніх версій, було створено SNMPv3, який вперше додав шифрування, аутентифікацію та контроль доступу.

Основні покращення SNMPv3:

- ✓ Аутентифікація користувачів – введена система ідентифікації через облікові записи.
- ✓ Шифрування трафіку – використання AES або DES для захисту SNMP-запитів і відповідей.
- ✓ Контроль доступу – можливість обмежити права користувачів (read-only, read-write, no-access).
- ✓ Захист від атак "людина посередині" (MITM) – захист від підміни SNMP-повідомлень.

Три рівні безпеки в SNMPv3:

- ✓ **noAuthNoPriv** – без аутентифікації та шифрування (аналог SNMPv2c).
- ✓ **authNoPriv** – з аутентифікацією (MD5 або SHA), але без шифрування.
- ✓ **authPriv** – з аутентифікацією та шифруванням (AES або DES).

Переваги SNMPv3:

- ✓ Надійний рівень безпеки (шифрування + автентифікація).
- ✓ Гнучка система керування доступом.
- ✓ Підходить для корпоративних і критичних інфраструктур.

Недоліки SNMPv3:
Ускладнена конфігурація порівняно з SNMPv1/v2c та значно вищі вимоги до ресурсів через шифрування.

Хронологія розвитку SNMP:

1988 – SNMPv1	(RFC 1157)	розроблений як тимчасове рішення для моніторингу мереж TCP/IP.
1993-1996 – SNMPv2	(RFC 1441-1452)	покращує продуктивність, але версія SNMPv2p не стає популярною.
1996 – SNMPv2c	(RFC 1901-1908)	стає основною версією SNMPv2, але без покращеної безпеки.
1996 – SNMPv2p	(RFC 1441-1452)	Party-based SNMPv2, нова модель безпеки на основі "party-based" доступу. Залишився складним у реалізації, тому не став популярним.
1996 – SNMPv2u	(RFC 1909-1910)	User-based SNMPv2, альтернативна версія, що спрощує механізм безпеки, орієнтуючись на користувачів. Не отримала широкого розповсюдження через відсутність зворотної сумісності зі SNMPv1.
2002 – SNMPv3	(RFC 3411-3418)	додає автентифікацію, шифрування та контроль доступу.

SNMPv2p та SNMPv2u залишилися проміжними версіями, не отримали широкого розповсюдження, а SNMPv2c став основною версією SNMPv2.

Для повноцінного вивчення основ моніторингу за допомогою SNMP (Simple Network Management Protocol) існує велика кількість програмних інструментів, які можуть бути корисними на різних етапах освоєння цієї технології. Вибір конкретного інструменту залежить від рівня складності досліджуваних мережевих сценаріїв, а також від специфіки роботи з різними версіями SNMP.

1. Інструменти для базового моніторингу SNMP, іншими словами, інструменти що підходять для побудови простих навчальних стендів і початкового знайомства з SNMP доцільно використовувати такі рішення:

- **snmpd (Net-SNMP)** – один із найпоширеніших SNMP-агентів, який дозволяє організувати базове опитування мережевих вузлів та отримувати інформацію про їхній стан. Підтримує SNMPv1, SNMPv2c та SNMPv3.Основні файли:
  - ✓ snmpd.conf – файл конфігурації агента;
  - ✓ snmpd – основний виконуваний файл (демон);
  - ✓ snmpwalk, snmpget, snmpset – утиліти для взаємодії з агентом.
- **MiniSNMPd** – легковаговий SNMP-демон, який займає мінімальний обсяг пам'яті та є зручним для запуску у віртуалізованих середовищах або на пристроях з обмеженими ресурсами. Основні файли:
  - ✓ minisnmpd.conf – конфігураційний файл;
  - ✓ minisnmpd – виконуваний файл демона.

2. Інструменти для моделювання складних SNMP-мереж. У випадках, коли потрібно працювати зі складними мережевими середовищами, необхідно використовувати спеціалізовані симулятори SNMP, які дають змогу створювати віртуальні пристрої для тестування моніторингових систем. До таких відносяться:

- **SolarWinds SNMP Simulator** – потужний комерційний інструмент для емуляції SNMP-пристроїв. Дозволяє налаштовувати відповіді на SNMP-запити, що спрощує тестування SNMP-моніторингу без фізичних пристроїв. Основні файли:
  - ✓ snmp-simulator.exe – виконуваний файл для запуску симулятора;
  - ✓ snmp-devices.cfg – файл конфігурації емуйованих пристроїв.

- **OpenNMS SNMP Mock** – безкоштовний SNMP-емулятор, що дозволяє створювати віртуальні SNMP-пристрої для тестування систем моніторингу. Основні файли:

snmp-mock.jar – виконуваний файл у форматі Java Archive;
mock-config.xml – файл налаштувань параметрів емуляції.

3. Інструменти для роботи з SNMPv3. Якщо необхідно працювати з безпечними версіями SNMP, зокрема з SNMPv3, який підтримує автентифікацію та шифрування, варто використовувати спеціалізовані інструменти:

- **iReasoning SNMP Manager** – графічний клієнт для роботи з усіма версіями SNMP, включаючи SNMPv3. Забезпечує зручний інтерфейс для виконання SNMP-запитів та аналізу відповідей. Основні файли:
  - ✓ iReasoning_SNMP_Manager.exe – виконуваний файл програми;
  - ✓ snmpv3-config.xml – файл конфігурації для SNMPv3.
- **Net-SNMP** – універсальний набір утиліт для роботи зі SNMP, що підтримує SNMPv3 з автентифікацією та шифруванням. Основні файли аналогічні snmpd.

4. Інструменти для тестування SNMP-трапів. SNMP-трапи – це механізм повідомлення про події в мережі, коли SNMP-агент надсилає повідомлення SNMP-менеджеру про зміну стану або виникнення помилки. Для тестування SNMP-трапів використовуються такі утиліти:

- **SNMPTT (SNMP Trap Translator)** – спеціалізована програма для отримання, фільтрації та обробки SNMP-трапів, що перетворює їх на більш зрозумілий формат. Основні файли:
  - ✓ snmptt.ini – головний конфігураційний файл;
  - ✓ snmptt – виконуваний файл.

Вибір інструмента для моніторингу SNMP залежить від конкретних завдань:
Для початкового вивчення підходять snmpd (Net-SNMP) або MiniSNMPd.
Для моделювання складних мереж можна використовувати SolarWinds SNMP Simulator або OpenNMS SNMP Mock.
Якщо потрібна підтримка SNMPv3, доцільно застосовувати iReasoning SNMP Manager або Net-SNMP.
Для роботи з SNMP-трапами рекомендовано SNMPTT.

У лабораторних роботах ми будемо використовувати у якості SNMP-сервера на Ubuntu snmpd та snmp(snmpwalk). Інструменти snmpd (демон SNMP) та snmp (клієнтські утиліти, включаючи snmpwalk, snmpget, snmpset) є частиною Net-SNMP – це кросплатформовий набір утиліт для роботи з протоколом SNMP. Вони доступні для різних Linux/Unix операційних систем (в т.ч. MacOS, Android, OpenWRT), хоча можуть мати деякі відмінності в назвах пакетів та способах встановлення.

На Windows немає snmpd, оскільки відсутній нативний Net-SNMP-агент, але є альтернативні варіанти:

- ✓ **Windows SNMP Service** (вбудований у Windows) виконує роль SNMP-агента (snmpd на Linux). SNMP Service вмикається через "Увімкнення або вимкнення компонентів Windows". Налаштовується через services.msc.
- ✓ **Net-SNMP для Windows** - SNMP-агент (snmpd) та клієнтські утиліти (snmpwalk, snmpget), що можуть бути завантажується з офіційного сайту Net-SNMP: https://net-snmp.sourceforge.io та встановлені на сервері або робочій станції Windows.

Мережева модель

Перш ніж заглиблюватися у вивчення протоколів збору та аналізу мережевого трафіку, таких як NetFlow, sFlow чи IPFIX, доцільно спершу розглянути загальну мережеву модель. Це дозволить краще зрозуміти, як дані передаються в мережі, які рівні взаємодіють між собою та де саме розташовуються засоби моніторингу. Крім того, варто звернути увагу на розширену ієрархічну модель, що включає рівні додатків та механізми збору телеметрії, оскільки саме ці аспекти відіграють ключову роль у впровадженні систем мережевого моніторингу.

Однак велика кількість компонентів інфраструктури призводить до того, що спроба вручну проаналізувати та усунути неполадки трафіку, що проходить через безліч точок доступу, комутаторів та маршрутизаторів, є майже нездійсненним завданням навіть для найорганізованішої команди фахівців.

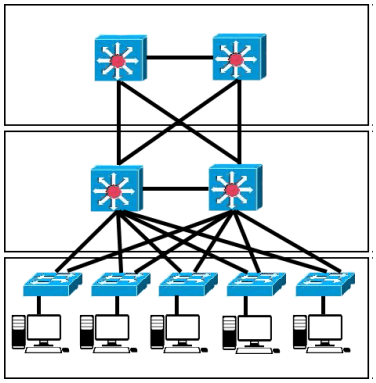


Рис. 04.02. 3-рівнева ієрархічна модель Cisco

Сучасні інструменти мережевої аналітики забезпечують вихід із цього трудомісткого та складного процесу. Програмне забезпечення для мережевої аналітики спираючись на традиційні протоколи та методи моніторингу, використовує складніші методи збору даних. Надалі всі зібрані дані аналізуються як реального часу з використанням штучного інтелекту і машинного навчання. Головною перевагою аналітичної платформи, що об'єднує всі джерела даних, є можливість в автоматичному режимі опрацьовувати набагато більшу кількість інформації, ніж могли безліч фахівців у ручному режимі раніше. Отримані в такий спосіб знання дозволять як оцінювати поточний стан мережі а й прогнозувати можливий розвиток подій у майбутньому (використовуючи при цьому системи предиктивної аналітики).

Щоб скористатися перевагами мережевої аналітики, підприємству потрібна інфраструктура, здатна генерувати дані про продуктивність та використання мережі. Засоби моніторингу мережі, які здійснюють аналіз даних, що передаються по ній, можуть бути програмними або апаратними.

Потоковий мережевий моніторинг відбувається на умовних, кількох взаємопов'язаних рівнях:

1. Рівень програм.
2. Рівень засобів моніторингу.
3. Рівень доступу.
4. Рівень мережі.

Програмні інструменти аналізу трафіку можуть бути безкоштовними (наприклад, nTop або Wireshark) або платними. Останні характеризуються ширшими функціональними можливостями, і користувачі комерційних продуктів можуть скористатися підтримкою постачальника. Очевидно, що підприємствам і розвиненим користувачам краще використовувати платні версії. Для початку проектування системи моніторингу мережі рекомендується провести аналіз середовища та додатків у якому вони будуть запускатися та скласти список поточних та майбутніх вимог до моніторингу інфраструктури. Чи будуть це інструменти для класичної мережевої архітектури розгортання мережі або це буде “хмара” - залежить від оцінки бюджету та можливостей інвестувати в моніторинг. Вибір інструменту для моніторингу системи є складним завданням, через велику кількість продуктів на ринку.

На рис.4.03 наведено розширену модель мережі, яка включає на противагу класичній схемі з попередньої ілюстрації ще і кілька рівнів забезпечення моніторингу.

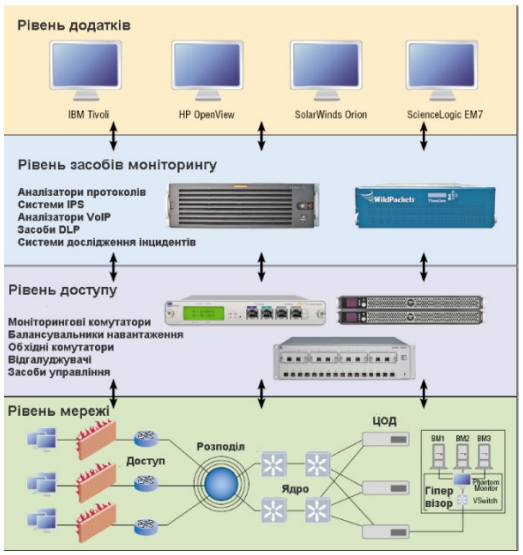


Рис. 04.03. Розширена ієрархічна модель мережі

Вибір інструменту для моніторингу системи є складним завданням, через велику кількість продуктів на ринку. На розширеній ієрархічній моделі на рівні додатків наведено у якості прикладу 4 програмних комплекси різних виробників.

Апаратні засоби можна розділити на дві умовні категорії.

Перша - рішення на базі серверних або комп'ютерних платформ зі спеціальними платами захоплення пакетів DAG (Data Acquisition and Generation), з встановленим програмним забезпеченням аналізу захопленого трафіку, а друга - це інтегровані пристрої мережевого моніторингу типу plug-and-play.

На відміну від звичайних мережевих адаптерів, плати DAG здатні захоплювати (в оперативну пам'ять хост-машини) абсолютно весь трафік, що подається на них (втрати пакетів практично виключені) на повній швидкості мережевих каналів, створюючи при цьому мінімальне навантаження на центральні процесори хост-машини, що дозволяє задіяти майже всю їхню потужність для аналізу захоплених даних і тим самим значно прискорити його.

Такі інструменти, як мережні відгалужувачі, що відносяться до **другої категорії**, завжди забезпечують повний контроль переданого трафіку. Цим дані пристрої вигідно відрізняються від SPAN-порту в комутаторі. Справа в тому, що комутатор відфільтровує дуже короткі пакети та пакети з помилками CRC, внаслідок чого вони не можуть контролюватись засобом моніторингу, підключеним до SPAN-порту. Крім того, при перевантаженні комутатор може відкидати пакети, що передаються в рамках SPAN-сесії, оскільки ці пакети обробляються як мають нижчий пріоритет, ніж у звичайних пакетів, що пересилаються між портами комутатора. До того ж, копіюючи трафік у SPAN-порт, комутатор змінює часові співвідношення на рівні пакетів (інтервали, затримки) та збільшує джиттер, що погіршує точність аналізу аудіо- та відеотрафіку.

Мережевий відгалужувач, «мідний» або волоконно-оптичний, не знижує надійності лінії, в розрив якої він включений. Справа в тому, що у разі збою в подачі електроживлення «мідний» відгалужувач продовжить пропускати трафік лінії з одного свого мережевого порту на інший, а типовий волоконно-оптичний відгалужувач повністю пасивний і взагалі не потребує електроживлення. Фактично типовий волоконно-оптичний

відгалужувач є найпростішим оптичним спліттером , який сумісний з різними мережевими технологіями канального рівня, наприклад Ethernet і ATM. Оснастивши (на етапі будівництва кабельної інфраструктури) критично важливі магістральні лінії зв'язку волоконно-оптичними мережевими відгалужувачами, потім до них можна буде підключати будь-які пристрої моніторингу або забезпечення інформаційної безпеки, не перериваючи передачі трафіку цими лініями.

Рис. 04.04. Мережевий відгалужувач.

Мережеві відгалужувачі та пристрої моніторингу, що підключаються до них, для забезпечення інформаційної безпеки зазвичай не мають IP-адрес, тому вони логічно ізольовані від іншого мережевого обладнання і не можуть бути атаковані хакерами.

До яскравого прикладу "мідного" відгалужувача відносяться такі продукти Ixia, як Gig Zero Delay Ta, 10/100/1000BaseT Tap. Оптичні відгалужувачі представлені пристроями сімейства Flex Tap. Перші підтримують максимальну швидкість передачі від 10 до 1000 Мбіт/с, а другі оптимізовані для різних швидкостей передачі: 1, 10, 40 або 100 Гбіт/с. Випускаються моделі волоконно-оптичних відгалужувачів для одномодового або багатомодового волокна, з різними типами роз'ємів та коефіцієнтами розподілу потужності.

На вирішальному етапі впровадження засобів мережевої аналітики існує одна з важливих проблем, що стоять перед багатьма організаціями і полягає в тому, як інтегрувати існуючі системи моніторингу та аналітики від різних постачальників. У ряді випадків це буває неможливо, оскільки багато аналітичних продуктів не можуть імпортувати пропрієтарні дані телеметрії, що мають несумісні стандарти. На даний момент обмежує специфічність інформації, яку може оцінити аналітичне програмне забезпечення. В результаті може виникнути ситуація, коли ці дані доведеться вводити вручну, що може бути занадто обтяжливим для IT-фахівців. Однак інструменти мережного аналізу таких компаній, як CA Technologies (CA Performance Management), ExtraHop (ExtraHop Performance) LiveAction (LiveNX) та Nyansa (Voyance) вирішують проблему серед різних постачальників. З іншого боку, якщо компанія управляє мережею, оснащеною в основному одним постачальником рішень, аналітична платформа цього постачальника, швидше за все, може запропонувати додаткові функції та переваги в рамках своєї власної екосистеми. Крім того, великі постачальники рішень мають великі можливості та ресурси для надання можливостей постійної підтримки в глобальному масштабі та цілодобово. Використовуючи обширні дослідження ринку мережевої аналітики, а також дані опитувань стосуються моніторингу всієї або частини корпоративної мережі або гібридного/мульти-хмарного середовища з використанням розширеного збору даних, об'єднання даних та аналітики, фахівці компанії TechTarget рекомендують ознайомити з прикладами 5 видів продуктів для мережевого моніторингу та аналітики.

IPFIX

IPFIX (IP Flow Information Export) – це стандартний протокол збору, експорту та аналізу мережевого трафіку, розроблений IETF (Internet Engineering Task Force). Він базується на NetFlow v9, але з розширеними можливостями, що забезпечують універсальний формат передачі даних про мережеві потоки. IPFIX дозволяє маршрутизаторам, комутаторам, мережевим зондами та іншим пристроям передавати детальну статистику про трафік у вигляді потоків на сервери збору даних для подальшого аналізу.

Хронологія розвитку IPFIX

- 📌 2001 рік – Cisco розробила NetFlow v9 – протокол для експорту мережевого трафіку, який став основою для IPFIX.
- 📌 2004 рік – робоча група IETF почала розробку універсального стандарту, заснованого на NetFlow v9.
- 📌 2008 рік – офіційна специфікація IPFIX була затверджена у RFC 5101 та RFC 5102.
- 📌 2013 рік – вийшло доповнення RFC 7011, яке удосконалило гнучкість та ефективність IPFIX.
- 📌 2020-ті роки – IPFIX активно використовується в SIEM-системах, мережевому моніторингу та аналізі загроз.

Стандартна реалізація протоколу складається з трьох типових функціональних компонент, що використовуються для аналізу IPFIX:

- **IPFIX Exporter** - маршрутизатор, комутатор, що зондує, або хост-програмний агент з підтримкою IPFIX, який відстежує статистику ключів і іншу інформацію про потік IP – пакетів і генерує записи потоку, які вміщені в UDP і відправляються в збирач потоків.
- **Collector IPFIX** - додаток, відповідальний за прийом пакетів записів потоку, опрацювання даних із записів потоку, попередню обробку і збереження запису потоку від одного або декількох експортерів потоку.
- **IPFIX Analyzer** - програмний додаток, який надає табличні, графічні та інші інструменти і візуалізації, щоб мережні оператори та інженери могли аналізувати дані потоку для різних випадків використання, включаючи моніторинг продуктивності мережі, усунення неполадок і планування пропускної здатності.

На рис. 04.05 наведена «страшна схема» розширеної архітектури IPFIX. Ми не будемо детально на ній зупинятися, бо вона базується на NetFlow v9, а опис цих протоколів нас чекає попереду.

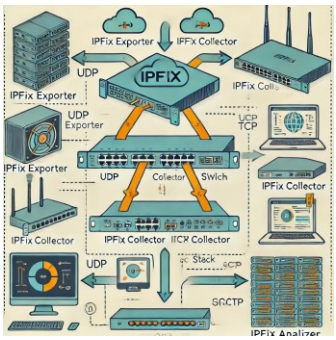


Рис. 04.05. Розширена архітектура IPFIX

Основні інструменти для роботи з IPFIX

✅ Колектори (IPFIX Collectors):

- ✓ nfdump/nfsen – потужний інструмент для збору та аналізу NetFlow/IPFIX.
- ✓ IPFIXcol – один із популярних колекторів з підтримкою SQL-баз даних.
- ✓ Elasticsearch + Logstash + Kibana (ELK) – застосовується для аналізу трафіку у великих інфраструктурах.

✅ Аналізатори (IPFIX Analyzers):

- ✓ ntopng – інтерактивний веб-аналізатор мережевого трафіку.
- ✓ Wireshark – підтримує IPFIX для розширеного аналізу мережевих потоків.
- ✓ Plixer Scrutinizer – комерційне рішення для детального аналізу трафіку.

Переваги та недоліки IPFIX

✅ **Переваги:**

- ✓ Гнучкість – підтримує різні типи даних та адаптується до потреб адміністраторів.
- ✓ Стандартність – є відкритим та офіційно затвердженим IETF.
- ✓ Розширені можливості порівняно з NetFlow (наприклад, підтримка нестандартних полів).
- ✓ Висока деталізація трафіку – дозволяє відстежувати не лише IP-адреси, а й метрики часу, QoS, VPN-трафік тощо.

❌ **Недоліки:**

⚠ Вимагає більше ресурсів для обробки даних, ніж NetFlow v9, на якому базується.

⚠ Ускладнена конфігурація – потребує ретельного налаштування експортерів та колекторів.

⚠ Не всі комерційні пристрої повністю підтримують IPFIX (деякі виробники залишаються на NetFlow).

🏁 **Висновок**

IPFIX є потужним інструментом для детального аналізу мережевого трафіку та моніторингу загроз, що успадкував багато переваг NetFlow, але водночас став більш універсальним та гнучким стандартом. Завдяки підтримці відкритих форматів та розширених можливостей, IPFIX активно використовується в мережевій безпеці, кібермоніторингу та аналізі продуктивності мереж, проте має і ряд суттєвих недоліків.

JFlow

JFlow —мережевий протокол збору та аналізу потоків даних, розроблений компанією Juniper Networks. Він використовується для моніторингу IP-трафіку в маршрутизаторах, комутаторах і брандмауерах, дозволяючи адміністраторам отримувати детальну статистику про використання смуги пропускання, аналізувати продуктивність мережі та виявляти потенційні загрози безпеці.

📜 **Історія розвитку та концепція**

Протокол ***JFlow*** є фактично еквівалентом ***Cisco NetFlow*** і працює за аналогічним принципом. Концепція збору потоків даних була розроблена у 1990-х роках для моніторингу продуктивності мереж і аналізу використання ресурсів. Основна ідея полягає у відстеженні послідовності IP-пакетів, які мають однакові параметри (IP-адреси джерела/одержувача, порти, протокол та QoS), що дозволяє ефективно агрегувати інформацію та зменшувати навантаження на мережу.

Juniper Networks впровадила JFlow як власний варіант NetFlow, який інтегрується в їхні пристрої та операційну систему Junos OS. Протокол працює на принципі експорту потокових даних з пристроїв до сервера збору, де виконується їх аналіз і візуалізація.

⚙ **Принцип роботи JFlow**

JFlow базується на вибірці (sampling) потоків даних і працює за таким алгоритмом:

- ✓ Маршрутизатор/комутатор збирає інформацію про IP-пакети, що проходять через нього.
- ✓ На основі певних параметрів (IP-адреси, порти, протокол, QoS) визначаються потоки.
- ✓ Потік вважається активним, доки триває передача даних. Якщо потік завершується або досягає таймауту, інформація про нього експортується до сервера збору даних.
- ✓ Сервер аналізує отримані дані, агрегує їх і формує звіти про використання мережі.

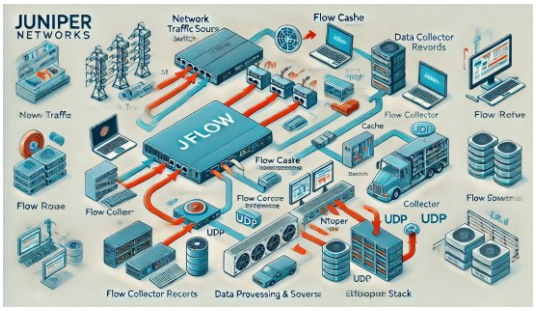


Рис. 04.06. Розширена архітектура JFlow

Протокол експортує зібрані дані через UDP до серверів моніторингу, таких як:

- ✓ PRTG Network Monitor
- ✓ Elasticsearch (через Logstash)
- ✓ ntopng
- ✓ Flow-tools
- ✓ SolarWinds NetFlow Traffic Analyzer

🔄 **Відмінності JFlow від інших flow-протоколів**

Протокол	Виробник	Відмінності
NetFlow	Cisco	Оригінальний протокол, має версії 5, 7, 9, IPFIX (стандарт IETF)
JFlow	Juniper	Аналог NetFlow, сумісний із версією 5/9, використовується у Junos OS
sFlow	HP, Extreme Networks	Використовує вибіркову вибірку (sampling) замість збору всіх потоків
IPFIX	Стандарт IETF	Розширений NetFlow v9 з можливістю додаткових полів
NetStream	Huawei	Власний аналог NetFlow від Huawei
RFlow	Mikrotik	Спрощена версія NetFlow для RouterOS

Основна відмінність JFlow від sFlow полягає в методі збору даних:

- ✓ **JFlow (NetFlow)** записує весь потік та зберігає інформацію у кеші перед передачею.
- ✓ **sFlow** працює на базі вибірки (sampling), що зменшує навантаження, але може призводити до втрати точності.

✅ **Переваги JFlow**

✓ Висока деталізація — збір повної інформації про сесії дозволяє отримувати точні аналітичні дані.

✓ Сумісність — підтримує NetFlow v5/v9, тому легко інтегрується з існуючими рішеннями для аналізу трафіку.

✓ Оптимізація продуктивності — працює на рівні ядра Junos OS, що забезпечує швидкість обробки.

✓ Мінімальне навантаження на мережу — UDP-експорт потоків не впливає на продуктивність трафіку.

❌ **Недоліки JFlow**

❌ Прив'язка до Juniper — технологія використовується лише на пристроях Juniper Networks.

❌ Необхідність зовнішнього сервера — для зберігання та обробки даних потрібне додаткове програмне забезпечення.

❌ Не всі версії Junos підтримують NetFlow v9 — у старих пристроях може бути доступна лише v5.

🏁 **Висновок**

JFlow є потужним інструментом для збору мережевого трафіку, що надає детальну статистику про використання пропускної здатності. Він особливо корисний для аналізу продуктивності, виявлення аномалій у мережі, оптимізації QoS та забезпечення безпеки. Завдяки сумісності з NetFlow, його можна легко інтегрувати з популярними системами моніторингу. Однак, через обмеження на використання тільки в екосистемі Juniper, організації з різнорідним мережевим обладнанням можуть віддати перевагу універсальним рішенням, таким як IPFIX або sFlow.

На початку лекції, були згадані ще два FLOW протоколи, які ми розглянемо детальніше.

Визначення та основні характеристики протоколів NetFlow та sFlow.

Історія та походження протоколу NetFlow

Протокол NetFlow є важливою складовою інфраструктури мережевого моніторингу та обліку трафіку. Розроблений компанією Cisco Systems, він визначається як мережевий протокол, спрямований на облік мережевого трафіку, і став фактичною стандартною практикою в цьому напрямку.

- **Походження та початок розвитку.** Історія NetFlow налічує кілька десятиліть, з початку робіт над ним у середині 1990-х років. Cisco, лідер в галузі мережевих технологій, почала впроваджувати цей протокол як рішення для відслідковування трафіку в мережах. В основі створення NetFlow лежала необхідність забезпечити адміністраторам мережі засобами для збору та аналізу інформації про мережевий трафік, що стало все більш важливим у зростаючому світі комп'ютерних мереж.
- **Стандартизація та поширення.** З часом NetFlow став не лише виробничим рішенням Cisco, але й стандартом для багатьох інших виробників мережевого обладнання, таких як Juniper і Enterasys. Це внесло великий вклад у його поширення та застосування в інших мережевих середовищах, роблячи його ефективним інструментом для різних типів компаній та організацій.
- **Функції та можливості.** Аналізуючи дані, які надає NetFlow, адміністратори мереж можуть отримувати детальну інформацію про джерело та призначення трафіку, клас обслуговування та причини перевантаження. Це відкриває можливості для вчасного виявлення проблем, вдосконалення ефективності мережі та забезпечення безпеки.
- **Версії та розвиток.** Існують кілька версій протоколу NetFlow, але на 2011 рік найбільш поширеними є версії 5 і 9. Версія 5 визначає формат обміну даними та стала дуже поширеною у мережевих пристроях Cisco. Версія 9, яка є більш розширеною і забезпечує більше можливостей, також послужила основою для створення відкритого стандарту під назвою IPFIX (Internet Protocol Flow Information eXport - експорт інформації про потоки IP). IPFIX визначається як стандарт, що регулює механізми експорту інформації про потоки IP, що дозволяє використовувати аналогічні можливості не лише на обладнанні Cisco, але й на різних платформах та пристроях, роблячи протокол більш універсальним та гнучким.

Таким чином, NetFlow, розпочавши свій шлях у світі мережевих технологій, став важливим стандартом для обліку та аналізу мережевого трафіку, що визначає його великий вплив на розвиток інфраструктури моніторингу та управління мережею.

Принцип дії протоколу NetFlow полягає в наступному.

При відкритті чергового сеансу передачі даних на мережевому обладнанні формується інформація про даний сеанс, так званий потік (flow). Відомості про потік включають кількість переданих байтів, вхідний і вихідний інтерфейси для сеансу, IP-адреси відправника / одержувача, порти відправника / одержувача, номер протоколу IP, параметри QoS і т.д. Потоки акумулюються на мережевому пристрої і відправляються колектору NetFlow в датаграму UDP. Колектор NetFlow агрегує отриману інформацію, проводить аналіз і формує зручні для сприйняття звіти і графіки. Один з популярних колекторів NetFlow – NetFlow Analyzer, але існують колектори.. Протокол NetFlow дозволяє отримати повну картину трафіку в каналах. Можна переглянути якісний склад трафіку (IP-адреси, порти, додатки) в будь – якому сегменті мережі, а також оцінити, яку частку пропускної здатності каналу (у відсотковому відношенні) займає той чи інший потік.

Основні характеристики протоколу NetFlow

Протокол NetFlow, як ключовий інструмент для обліку та аналізу мережевого трафіку, відрізняється рядом важливих характеристик, що визначають його ефективність та застосування в різних мережевих середовищах.

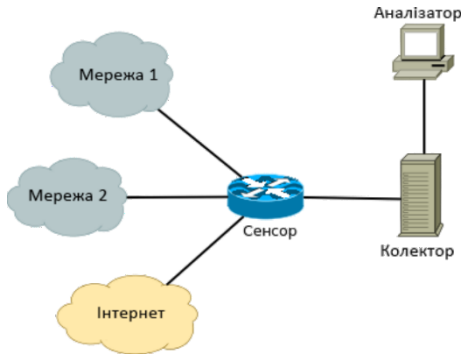
- ✓ **Передача даних.** Передача даних в рамках протоколу NetFlow відбувається за допомогою створення та експорту "потоків" з різних мережевих пристроїв. Потік - це набір даних, що визначає комунікаційну сесію між двома пристроями в мережі. Кожен потік містить ключову інформацію, таку як джерело і призначення трафіку, порти, протокол та інші атрибути. Ці дані надсилаються до NetFlow-коллектора в реальному часі, що дозволяє адміністраторам отримувати негайну звітність про мережевий стан та трафік.

  Однією з ключових переваг передачі даних за допомогою потоків є зменшення обсягу інформації, що передається, забезпечуючи ефективну використання пропускної здатності мережі. Крім того, це робить NetFlow ефективним інструментом для моніторингу великих та високовитратних мереж.

- ✓ **Підтримувані пристрої.** Початково розроблений компанією Cisco, NetFlow вперше з'явився на мережевих пристроях цього виробника. Проте з розвитком та зростанням популярності, інші виробники мережевого обладнання, такі як Juniper, Enterasys, та інші, також почали імплементувати підтримку NetFlow в свої пристрої.

  Сучасний екосистема NetFlow охоплює широкий спектр обладнання, включаючи рутери, комутатори, файрволи та інші мережеві пристрої. Це забезпечує адміністраторам мереж можливість використання NetFlow в різних топологіях мережі та конфігураціях, що робить його важливим інструментом у багатьох сценаріях.

- ✓ **Архітектура.** Для збору інформації про трафік за протоколом NetFlow потрібні такі компоненти:
  - **Сенсор.** Збирає статистику з трафіку, що проходить через нього. Зазвичай це L3-комутатор або маршрутизатор, хоча можна використовувати і сенсори, що окремо стоять, одержують дані шляхом дзеркалювання порту комутатора.
  - **Колектор.** Збирає отримані від сенсора дані та поміщає їх у сховище.
  - **Аналізатор.** Аналізує зібрані колектором дані та формує придатні для читання людиною звіти (часто у вигляді графіків).



- ✓ **Формат даних** NetFlow визначається версією протоколу. Дві найбільш використовувані версії - 5 і 9 - відрізняються у своїх підходах до структури даних.
  - ➢ **Версія 1.** Протоколу NetFlow на сьогоднішній день вже застаріла і не використовується.
  - ➢ **Версії 2-4.** Ніколи не включалися в Cisco IOS, і, відповідно, не підтримуються.
  - ➢ **Версія 5**. Використовує фіксований формат запису, що містить основну інформацію про потік, таку як IP-адреси джерела та призначення, порти, протокол та об'єм переданого трафіку. Версія 5 була доповнена вимогами про номери автономних систем, використовуваних в протоколі граничного шлюзу (BGP), і номер потоку. Ця версія досі використовується, якщо немає потреби у додатковій інформації, яка надається більш пізніми версіями протоколу та дозволяє ефективно передавати базові дані для аналізу та моніторингу.
  - ➢ **Версія 6.** Ніколи не включалися в Cisco IOS. Не підтримується.
  - ➢ **Версія 7.** Стала розвитком версії 5 і вона стала підтримуватися в серії комутаторів Cisco Catalyst.
  - ➢ **Версія 8.** У цій версії була введена можливість агрегації даних, що актуально при великих обсягах даних протоколу NetFlow.
  - ➢ **Версія 9.** Забезпечує більшу гнучкість, дозволяючи включати додаткові атрибути в запис про потікза рахунок істотного збільшення кількісті полів в порівнянні з версією 5. Ці додаткові поля дозволяють розширити і уточнити інформацію, що проходить в мережевому потоці. Наприклад, версія 9 включає інформацію 2-го рівня мережної моделі: підтримка IPv6, групових (Multicast) розсилок, параметри протоколів MPLS, BGP і інше. Але основне нововведення версії 9 – це використання шаблонів, що забезпечує легке розширення протоколу за рахунок використання нових типів шаблонів даних.
  - ➢ **IPFIX.** Важливою особливістю є те, що на основі версії 9 був розроблений стандарт IPFIX (Internet Protocol Flow Information eXport), який став відкритим стандартом для обміну інформацією про потоки IP. IPFIX створений як стандарт, що може бути використаний на різних платформах та обладнанні, незалежно від виробника. Це дозволяє різним вендорам реалізовувати цей стандарт у своїх пристроях та програмних рішеннях, забезпечуючи уніфікований підхід до обміну інформацією про потоки IP.

- ✓ **Опис протоколу.** NetFlow використовує UDP ("User Datagram Protocol" - протокол користувацького дейтаграмного протоколу) або SCTP ("Stream Control Transmission Protocol" - протокол керування потоком передачі) для передачі даних про трафік колектору. Як правило, колектор слухає порт **2055, 9555** чи **9995**. Сенсор виділяє з проходить трафіку потоки , що характеризуються наступними параметрами:
  - Адреса джерела;
  - Адреса призначення;
  - Порт джерела для UDP та TCP;
  - Порт призначення для UDP та TCP;
  - Тип та код повідомлення для ICMP ;
  - Номер протоколу IP ;
  - Мережевий інтерфейс (параметр ifindex SNMP);
  - IP Type of Service .

  Потоком вважається набір пакетів, які у одному напрямі. Коли сенсор визначає, що потік закінчився (за зміною параметрів пакетів, або скидання TCP-сесії), він відправляє інформацію в колектор. Залежно від налаштувань він також може періодично відправляти в колектор інформацію про потоки, що все ще йдуть.
  Зібрана інформація надсилається у вигляді записів, що містять такі параметри (для версії 5):
  - номер версії протоколу;
  - Номер запису;
  - Вхідний та вихідний мережевий інтерфейс;
  - Час початку та кінця потоку;
  - Кількість байт та пакетів у потоці;
  - Адреса джерела та призначення;
  - Порт джерела та призначення;
  - номер протоколу IP;
  - значення Type of Service;
  - Для TCP-з'єднань - всі прапорці, що спостерігаються протягом з'єднання;
  - Адреса шлюзу;
  - Маски підмережі джерела та призначення.

Версія 9 також підтримує додаткові поля, такі як заголовки IPv6 , мітки потоків MPLS та адресу шлюзу BGP . Деякі сенсори можуть також підтримувати номер автономної системи .

Якщо використовується UDP, то втрачений через проблеми з мережею запис не буде отриманий колектором. Колектор може визначити втрати пакетів за значеннями номера запису, які за стандартом мають бути зростаючими.
Якщо сенсором виступає мережний пристрій (маршрутизатор чи комутатор), то економії ресурсів NetFlow включають лише тих інтерфейсів, у яких хочуть збирати статистику.
Для економії ресурсів процесора також застосовується "sampled NetFlow". У цьому випадку сенсор аналізує не всі, а кожен n-ий пакет, де n може бути заданим адміністративно або випадковим чином, що вибирається. При використанні sampled NetFlow одержувані значення не точними, а оціночними.

🏁 Висновок

Характеристики **NetFlow** визначають його як потужний інструмент для моніторингу та управління мережею. Здатність передачі даних в реальному часі, підтримка на різних мережевих пристроях та гнучкість формату даних роблять його ефективним засобом для отримання детальної інформації про мережевий трафік та забезпечення адекватного управління мережею.

Походження та розвиток sFlow

sFlow – це відкритий стандарт для моніторингу трафіку в мережах, призначений для надання детальної статистики та аналізу в реальному часі. Розглянемо походження та розвиток цього протоколу, який визначає його сутність та значення в сучасних мережевих технологіях.

- **Історія та Походження sFlow.** sFlow був вперше представлений компанією InMon Corporation на початку 2000-х років. Головною метою створення було розробити універсальний стандарт, який дозволяв багатьом виробникам мережевого обладнання реалізувати моніторинг трафіку на своїх пристроях.

Важливою перевагою sFlow є його відкритість та здатність працювати на різних мережевих пристроях, незалежно від їхнього виробника чи моделі. Це відмінно від інших протоколів, які можуть бути властивими лише певному обладнанню.

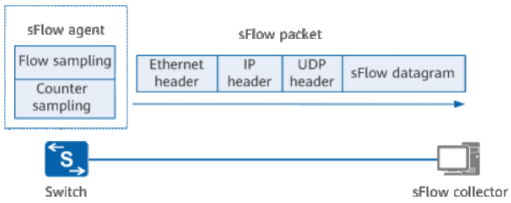


Рис. 04.02. Архітектура sFlow

- **Універсальність та розвиток sFlow.** sFlow визначається своєю універсальністю та розширюваністю. Завдяки принципу вибіркового вибору та зразків, sFlow може збирати статистику лише з частини трафіку, зменшуючи навантаження на мережу та забезпечуючи широкий обхват аналізу.
  Розвиток sFlow включав у себе не лише поширення його підтримки серед різних виробників, а й постійне вдосконалення стандарту. Додаткові функції та можливості були додані в нових версіях протоколу, що розширює його функціональність та адаптує для змін у мережевих технологіях.
- **Активне та пасивне відстеження.** Однією з ключових особливостей sFlow є можливість як активного, так і пасивного відстеження. У режимі активного відстеження sFlow взаємодіє з мережевим обладнанням, надсилаючи зразки трафіку на аналіз. У пасивному режимі sFlow збирає дані з вже існуючого трафіку без втручання у роботу мережі.
- **Відкриті реалізації та стандартизація.** Однією з ключових переваг sFlow є наявність відкритих реалізацій для різних операційних систем та платформ. Це дозволяє використовувати sFlow на серверах, комутаторах, маршрутизаторах та іншому обладнанні.
  Стандарт сфокусований на відкритості і стандартизації, і це робить його придатним для широкого спектру застосувань. Багато вендорів використовують sFlow як основний інструмент для мережевого моніторингу, забезпечуючи адміністраторам мереж високий рівень контролю та аналізу мережевого трафіку.

Унікальні характеристики sFlow.

sFlow, як протокол для моніторингу трафіку в мережах, вирізняється своїми унікальними характеристиками, які роблять його ефективним та гнучким інструментом для адміністраторів мереж.

- **Активне та пасивне відстеження.**
  - ✓ **Активне відстеження** визначається можливістю sFlow взаємодіяти з мережевим обладнанням для збору та надсилання статистики трафіку. Цей режим дозволяє вибірково збирати дані з різних точок мережі, адаптуючися до конкретних вимог адміністратора. Наприклад, можливість визначити певні порти чи пристрої для моніторингу, дозволяє вимірювати трафік на обраній частині мережі, що є важливим для точного аналізу та управління.
  - ✓ **Пасивне відстеження** означає можливість sFlow збирати дані з існуючого трафіку без втручання у роботу мережі. Цей режим особливо корисний для аналізу та моніторингу трафіку без його переривання чи впливу на нього. Наприклад, адміністратор може використовувати пасивне відстеження для виявлення аномалій або моніторингу пропускної здатності без значного впливу на нормальну роботу мережі.

Розглянемо конкретні сценарії застосування активного та пасивного відстеження sFlow:

Таблиця 04.01

Активне відстеження	Пасивне відстеження
Припустимо, що адміністратор мережі хоче детально моніторити трафік на конкретному комутаторі в центральному офісі. Використовуючи активне відстеження sFlow, він може налаштувати цей комутатор для вибіркового збору даних і періодично надсилання їх до централізованого моніторингового сервера. Такий підхід дозволяє зосередитися на конкретних аспектах мережі та забезпечити більш ефективний моніторинг.	Припустимо, що мережевий адміністратор хоче вивчати поведінку користувачів на сервері без втручання у конфігурацію самого сервера. Використовуючи пасивне відстеження sFlow на суміжньому комутаторі, він може збирати статистику трафіку, визначаючи найактивніші порти та типи послуг, які використовуються. Це дозволяє адміністраторові отримати інформацію про використання ресурсів сервера без прямого взаємодії з самим сервером.

Лекція присвячена також NetFlow, у якого немає явної підтримки активного відстеження. Однак деякі виробники мережевого обладнання можуть використовувати власні реалізації, які можуть включати елементи активного моніторингу, але це вже залежить від конкретного обладнання та виробника.
sFlow, навпаки, більше орієнтований на активний моніторинг. sFlow дозволяє відстежувати трафік на активних пристроях, які підтримують цей протокол. sFlow відправляє відібрані зразки пакетів з активних мережевих пристроїв до аналізатора, де їх можна використовувати для моніторингу та аналізу. Отже, в цьому випадку sFlow має більшу спрямованість на активний моніторинг, тоді як NetFlow, який зазвичай працює у пасивному режимі, може включати елементи активного моніторингу в окремих виробників обладнання.

Формат даних.

Формат даних sFlow визначає, як саме інформація про трафік буде структурована та передаватися. sFlow використовує JSON-подібний формат для опису даних, що робить його легким для розуміння та обробки. Кожний зразок (sFlow sample) містить інформацію про конкретний аспект мережевого трафіку, такий як IP-адреса, порти, протоколи, типи послуг та інші важливі атрибути.

Розглянемо приклад структури даних sFlow в форматі JSON-подібного запису:

```
{
  "agent_address": "192.168.1.1",
  "input_port": 1,
  "output_port": 2,
  "packet_count": 1000,
```

"byte_count": 120000,
"protocol": "TCP",
"source_ip": "10.0.0.1",
"destination_ip": "10.0.0.2",
"source_port": 5000,
"destination_port": 80
}

У цьому прикладі зразок sFlow містить інформацію про передачу трафіку з IP-адреси 10.0.0.1 на IP-адресу 10.0.0.2 через TCP-з'єднання на порті 80. Дані про кількість пакетів та обсяг байтів також включені для повного опису трафіку.
Описаний формат даних дозволяє адміністраторам ефективно аналізувати та обробляти інформацію, зібрану за допомогою sFlow, спрощуючи взаємодію з моніторинговими системами та іншими інструментами аналізу мережевого трафіку.

🏁 Висновок

sFlow виникає як універсальний стандарт для моніторингу та аналізу трафіку в мережах. З його походженням від компанії InMon і активним розвитком у вигляді відкритих реалізацій та стандартів, sFlow став важливим інструментом для адміністраторів мереж, які прагнуть забезпечити ефективний моніторинг та управління своєю інфраструктурою.

Використання протоколів NetFlow та sFlow для збору мережевих статистичних даних.

Збір даних NetFlow

✓ **Як працює збір даних NetFlow.** Протокол NetFlow є ефективним інструментом для збору та аналізу статистики трафіку в мережах. Розглянемо, як саме відбувається збір даних NetFlow та які процеси відбуваються під час цього процесу.

1. **Експорт даних.** Процес збору даних NetFlow розпочинається на мережевих пристроях, таких як маршрутизатори чи комутатори. Кожен такий пристрій, який підтримує NetFlow, володіє таблицями потоків, в яких зберігається інформація про протоколи, IP-адреси, порти та інші атрибути трафіку.

   Коли пристрій розпізнає новий потік (у вигляді пакету або групи пакетів, що належать одному потоку), він приймає рішення про експорт цих даних до зовнішнього агенту, який може бути NetFlow-колектором або іншим пристроєм, призначеним для збору і обробки даних.

2. **Формування пакетів NetFlow.** Щоб передати інформацію про потоки до колектору, дані повинні бути упаковані в спеціальні пакети NetFlow. Ці пакети містять ключову інформацію про кожен потік, яка дозволяє аналізувати трафік на більш високому рівні.
   Наприклад, пакет NetFlow може містити наступну інформацію для кожного потоку:
   - Номер версії протоколу.
   - Номер запису.
   - Вхідний та вихідний мережевий інтерфейс.
   - Час початку та кінця потоку.
   - Кількість байт та пакетів у потоці.
   - Адреса джерела та призначення.
   - Порт джерела та призначення.
   - номер протоколу IP.
   - значення Type of Service.
   - Для TCP-з'єднань - всі прапорці, що спостерігаються протягом з'єднання.
   - Адреса шлюзу.
   - Маски підмережі джерела та призначення.

3. **Відправлення до NetFlow-колектора.** Сформовані пакети NetFlow відправляються до NetFlow-колектора за допомогою мережі. NetFlow-колектор може бути спеціальним пристроєм або програмним забезпеченням, призначеним для збору та обробки даних NetFlow.

   Цей колектор приймає пакети, дешифрує їх та зберігає інформацію у вигляді записів або бази даних для подальшого аналізу. Одним з основних завдань колектора є збереження історії потоків для подальшого вивчення та виявлення аномалій чи проблем у мережі.

4. **Аналіз та використання даних NetFlow.** Отримані дані NetFlow надають адміністраторам мережі детальний огляд того, як використовуються ресурси мережі. Інструменти аналізу можуть включати графіки трафіку, звіти про користувачів, виявлення аномалій та оптимізацію роботи мережі.
   Приклад:
   Розглянемо сценарій, де NetFlow використовується для аналізу трафіку в офісній мережі. Мережевий адміністратор виявляє, що певний комп'ютер витрачає надмірно багато ресурсів мережі. Збираючи дані NetFlow, він може ідентифікувати IP-адресу цього комп'ютера, перевірити, які додатки використовуються, і при потребі вжити заходів для обмеження або оптимізації трафіку, що генерується цим пристроєм.

Аналіз архітектури протоколу NetFlow

NetFlow дозволяє пристроям Cisco передавати дані про трафік, що проходить через даний пристрій, на будь – який хост в мережі, де ці дані можуть накопичуватися, зберігатися в певному виді і відповідно відображатися. Таким чином маємо три типи обєктів, які працюють з NetFlow: сенсор, колектор, аналізатор (рис. 04.01).

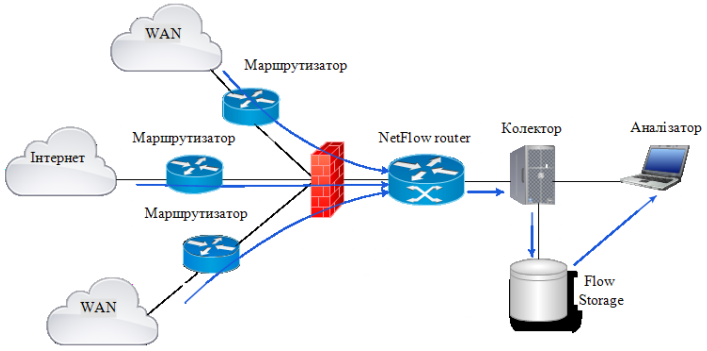


Рис. 04.03. Архітектура NetFlow

Для захоплення, передачі та аналізу даних NetFlow слід використовувати вже знайомі нам компоненти компоненти з підтримкою NetFlow, які ми згадували кілька разів:

- **Сенсор (Exporter)** – збирає статистику трафіка по проходить через нього. Зазвичай це L3 – комутатор або маршрутизатор, хоча можна використовувати і окремі сенсори, які отримують дані шляхом відображення трафіка. Сенсор прослуховує мережу і фіксує дані сеансу. Також як Snort або будь-яка інша система виявлення вторгнень, сенсор повинен мати можливість підключитися до хабу, переглядати порт комутатора або будь – якого іншого пристрою, для перегляду мережного трафіку. Якщо використовувати систему пакетної фільтрації на базі BSD або Linux, то це чудове місце для сенсора NetFlow, так як весь трафік буде проходити через цю точку. Сенсор буде збирати інформацію про сеанси і скидати її в колектор.

Сенсор виділяє з трафіку потоки, які характеризуються наступними параметрами (рис. 04.04):

- ✓ IP адреса джерела даних;
- ✓ IP адреса приймача даних;
- ✓ Порт джерела для UDP і TCP;
- ✓ Порт призначення для UDP і TCP;
- ✓ Тип і код повідомлення для ICMP;
- ✓ Номер протоколу IP;
- ✓ Мережний інтерфейс (параметр ifindex SNMP);
- ✓ IP Type of Service.

Фактично це інформація, що береться безпосередньо з потоків, про яку ми вже згадували. Потоком вважається набір пакетів, що проходять в одній області. Коли сенсор визначає, що потік закінчився (за зміною параметрів пакетів), він відправляє інформацію в колектор. В залежності від налаштувань він також може періодично відправляти в колектор інформацію про все ще поточні потоки.

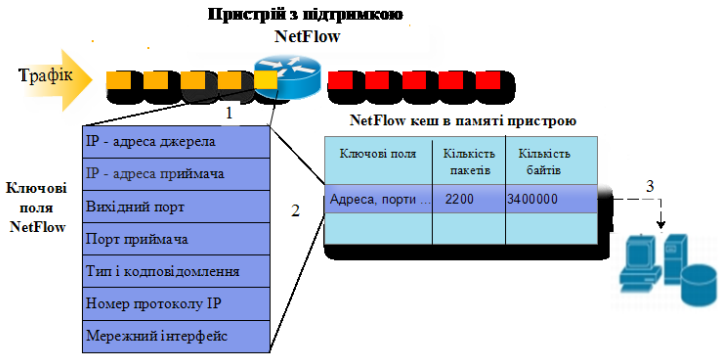


Рис. 04.04. Параметри трафіка

Таким чином, процес збору даних NetFlow дозволяє NA ефективно контролювати та оптимізувати роботу мережі, забезпечуючи високу продуктивність та ефективне використання ресурсів.

Роль NetFlow-коллектора.

NetFlow-коллектор відповідає за приймання, зберігання та аналіз даних, що надходять від різних мережевих пристроїв, які підтримують протокол NetFlow. Розглянемо роль NetFlow-коллектора більш детально, включаючи його визначення, функції та приклади використання.

- **Визначення NetFlow-коллектора.** NetFlow-коллектор - це програмне чи апаратне забезпечення, яке призначене для збору, аналізу та зберігання даних NetFlow, надісланих мережевими пристроями, такими як маршрутизатори чи комутатори. Його основною метою є створення централізованої точки збору інформації про мережевий трафік для подальшого аналізу та моніторингу. Тобто **NetFlow-коллектор - це інший сервер або комп'ютер, на якому запускається програмне забезпечення приймача NetFlow, призначене для збору, запису, фільтрування та аналізу отриманих потоків**, таких як PRTG NetFlow Analyzer Paessler.

- **Функції NetFlow-коллектора.**

  - ✓ **Приймання даних**. Основна функція колектора - це приймання даних NetFlow від мережевих пристроїв. Колектор повинен бути налаштований для слухання відповідних портів, на яких надходять дані від пристроїв. Програмне забезпечення колектора повинно підтримувати ту саму версію NetFlow, що і сервер-експортер. Наприклад, для моніторингу маршрутизатора Cisco з використанням NetFlow v5 потрібно буде використовувати датчик NetFlow v5. Для маршрутизатора, що використовує NetFlow v9, потрібен датчик NetFlow v9. Обидва датчики можуть бути включені на одному комп'ютері одночасно, так що єдиний колектор може отримувати дані з обох версій NetFlow і повідомляти про них. IP-адреса колектора та порт призначення повинні бути налаштовані на маршрутизаторі або самостійно. У деяких випадках SNMP може бути використаний для ввімкнення NetFlow та налаштування IP-адреси колектора для надсилання даних. У Cisco IOS команда ip flow-export може використовуватися для налаштування IP-адреси призначення з командного рядка. Один з найпопулярніших портів, який використовується для експорту NetFlow, становить 2055, але в основному можна використовувати будь – який порт, якщо правильно вказати його в приймачі NetFlow.

- ✓ **Зберігання інформації**. Колектор зберігає отримані дані для подальшого використання та аналізу. Час зберігання може варіюватися від декількох годин до кількох місяців в залежності від конфігурації та потреб користувача.

- ✓ **Аналіз та візуалізація**. Колектор може використовувати вбудовані чи сторонні інструменти для аналізу та візуалізації зібраних даних. Це дозволяє адміністраторам отримати інсайти щодо трафіку, виділяти аномалії та приймати рішення щодо оптимізації мережі. Діаграми NetFlow експортуються за допомогою протоколу обробки користувацьких даних UDP та SCTP.

- ✓ **Повідомлення про аномалії**. Колектор може автоматично сповіщати адміністратора про виявлені аномалії або подозрілу активність в мережі. Це дозволяє оперативно реагувати на потенційні проблеми та забезпечити безпеку мережі.

- **Приклади використання NetFlow-коллектора.**
  - ✓ **Моніторинг трафіку**. Колектор може використовуватися для детального моніторингу трафіку в мережі. Наприклад, адміністратор може аналізувати, які додатки використовуються користувачами, визначати трафік, який займає найбільше пропускної здатності, та визначати споживання ресурсів.

  - ✓ **Аналіз безпеки**. Колектор NetFlow може служити інструментом для виявлення потенційно шкідливих або небезпечних активностей в мережі. Відстеження незвичайних патернів або аномалій може допомогти вчасно виявляти атаки чи недоліки в безпеці мережі.

  - ✓ **Планування мережевого ресурсу**. Аналіз даних NetFlow дозволяє адміністраторам краще розуміти використання ресурсів мережі. Це полегшує процес прийняття рішень щодо розширення або оптимізації мережі для задоволення поточних та майбутніх потреб.

Функції та призначення NetFlow-аналізатора.

Аналізатор аналізує зібрані колектором дані і формує придатні для читання людиною звіти (часто у вигляді графіків). NetFlow Analyzer – це просте рішення для адміністраторів, щоб краще розуміти споживання смуги пропускання, тенденції трафіку, додатки, хости і аномалії трафіку, візуалізувати трафік за допомогою мережевих пристроїв, інтерфейсів і підмереж, сегментів трафіку і кінцевих користувачів. NetFlow Analyzer використовує Cisco NetFlow, IPFIX, sFlow і сумісні NetFlow подібних протоколи, щоб допомогти адміністратором з контролем смуги пропускання, дослідженням мережевого трафіку, аналіз і звітністю. Це дозволяє оптимізувати свої мережі і додатки, планувати розширення мережі, економити час, необхідний для усунення неполадок і діагностики, а також підвищити безпеку – в свою чергу, значно знижуючи операційні витрати і підвищуючи продуктивність мережної команди.

Загалом, програмне забезпечення NetFlow Analyzer є невід'ємною частиною будь – якої інфраструктури безпеки для виявлення аномалій в мережі і усунення неполадок з погрозами. Він доповнює брандмауери, орієнтовані на кінцеві точки мережі, забезпечуючи внутрішній вигляд мережі. На відміну від сигнатурних антивірусів, які стикаються з відомими погрозами, ця концепція не попереджувальної, але швидкої реакції необхідна для підвищення атак з нульовим днем. І у вас також є історичний архів даних для подальшого розслідування, коли це буде визнано за необхідне. Таким чином, він фактично охоплює найважливіші загрози, з якими стикаються мережі в даний час, такі як передові постійні погрози, внутрішні загрози і навіть зловживання співробітниками, несанкціонований доступ і випадки витоку даних.

Висновок

NetFlow Analyzer, повний інструмент аналізу трафіку, використовує технології потоку, щоб забезпечити видимість в мережі в режимі реального часу. Аналізатор NetFlow, в першу чергу інструмент моніторингу пропускної здатності, оптимізує тисячі мереж по всьому світу, надаючи цілісне уявлення про пропускну здатність мережі та структурі трафіку. NetFlow Analyzer – це уніфіковане рішення, яке збирає, аналізує і повідомляє про те, для чого використовується ваша пропускна здатність мережі і ким.

Застосування NetFlow в реальних сценаріях

- **Виявлення та вирішення проблем зі швидкістю мережі.** У великій компанії, де працює багато співробітників, адміністраторам важливо знати, чи виникають проблеми зі швидкістю мережі. Вони використовують NetFlow для визначення, які пристрої та додатки споживають найбільше пропускної здатності, і вживають заходів для оптимізації трафіку та вирішення проблем.

- **Моніторинг користувацької активності.** У навчальному закладі адміністратори використовують NetFlow для моніторингу активності користувачів у мережі. За допомогою NetFlow вони можуть визначити, які веб-сайти використовуються, які додатки завантажуються та як користувачі використовують мережеві ресурси.

- **Оптимізація використання хмарних служб.** Компанія, яка використовує хмарні служби для зберігання та обробки даних, використовує NetFlow для моніторингу трафіку до та з хмарних сервісів. Це допомагає адміністраторам вирішувати питання ефективності та безпеки використання хмарних ресурсів.

- **Виявлення та обмеження несанкціонованого доступу.** У фінансовій установі NetFlow використовується для виявлення несанкціонованого доступу до чутливої інформації. Якщо система виявляє надмірний обсяг трафіку або надто активних підключень до конкретного ресурсу, може бути викликано сповіщення та застосовані обмеження доступу.

- **Моніторинг віртуальних мереж.** В організації, яка використовує віртуалізацію, NetFlow дозволяє адміністраторам відстежувати трафік між віртуальними машинами та ефективно управляти ресурсами віртуальної мережі.

Типові проблем у мережі, які можна знайти за допомогою аналізу NetFlow

- **Хтось сканує мережу.** Напевно немає такої локальної мережі, де не виявиться хостів, які її сканують. Хости, які не повинні це робити. Це може бути "специфічне" ПЗ і проблема вирішується звичайними правилами на міжмережевому екрані. Може бути "гуру", який грається з Kali Linux, проходячи PenTest курси (що дуже похвально!). Може бути справді заражений ПК, який в автоматичному режимі веде сканування мережі.

- **Великі втрати по мережі (скачалось 60мб, до користувача дійшло 10).** Досить часто можна виявити проблеми із втратами на певних ділянках мережі. В інциденті Flowmon може значитися, що з цільової системи було завантажено 60мб, в той час, як користувач отримав всього 10мб. Так, іноді користувачі дійсно говорять правду, що якась програма дуже повільно працює.

- **Безліч підключень з периферійних пристроїв (принтерів, камер) до серверів.** Дуже поширений інцидент. Зробивши найпростіший фільтр, можна побачити, що до контролера домену йдуть періодичні запити від периферійних пристроїв. Як правило цих коннектів/запитів бути не повинно, хоча бувають і "легальні" речі. У будь-якому випадку, після розслідування безпека виявляє, що у них є цілий клас пристроїв, за якими теж потрібно стежити і хоча б винести в окремий сегмент.

- **Підключення до серверів по нестандартних портах.** Частий кейс. Наприклад, виявляється DNS сервер, до якого йдуть запити не тільки по 53 порту, а й по купі інших. Тут одразу вимальовуються дві проблеми: або хтось дозволив інші порти до сервера DNS, або на DNS сервері піднято інші служби/сервіси. Обидві проблеми вимагають розгляду.

- **Підключення до інших країн.** Особливо це цікаво для якогось сегмента з камерами чи СКУД (Система контролю доступу та управління пропусками). Виявляється, деякі китайські пристрої наполегливо "стукають" до себе на батьківщину або кудись у Бангладеш.

- **Перед звільненням співробітника різко зростає його трафік.** Швидше за все, користувач робить бекапи якоїсь робочої інформації. Чи це дозволено політикою компаній невідомо, але інформація легко отримується і може бути досліджена.

- **Множинні DNS запити від хоста користувача.** Ця проблема часто є ознакою зараженого ПК, чи "особливостями" якогось специфічного ПЗ. У будь-якому випадку це корисна інформація для роздумів, особливо коли комп'ютер користувача генерує під 1000 запитів DNS на годину.

- **"Ліві" DHCP сервери в мережі.** Ще одна хвороба багатьох великих мереж. Користувач запустив VirtualBox або VMWare Workstation, при цьому забув вимкнути вбудований DHCP сервер, від чого періодично лягає якийсь сегмент мережі. Аналіз NetFlow дуже швидко допомагає виявити нашого порушника.

- **"Петлі" в локальній мережі.** Дуже поширена проблема, викликана кадровим плином фахівців. У деяких компаніях комутатори успішно справляються з цими петлями (через грамотне налаштування обладнання) і їх особливо ніхто не помічає. А в деяких — усю мережу періодично штормить, і ніхто не може зрозуміти, що відбувається.

Як не дивно, реальні приклади застосування NetFlow дещо відрізняються та є більш широкими від теоретичних функцій та призначення, що демонструє гнучкість та важливість NetFlow у різних сценаріях, де він використовується для розв'язання конкретних завдань з моніторингу, оптимізації та безпеки мережі.

Методи збору даних sFlow.

sFlow є ефективним протоколом для моніторингу трафіку у реальному часі та забезпечення детальної інформації про використання мережі. Цей протокол використовує інноваційний підхід до збору даних, що дозволяє отримувати зразки трафіку, забезпечуючи збалансований погляд на мережеву активність. Давайте розглянемо методи збору даних sFlow та їх приклади в різних сценаріях.

1. **Активне відстеження.** sFlow використовує метод активного відстеження для збору даних. Мережеве обладнання, таке як маршрутизатори чи комутатори, взаємодіє з пристроями, щоб активно визначати зразки трафіку для подальшого аналізу.
   Приклад. Велика корпоративна мережа використовує sFlow на своїх комутаторах для збору інформації про трафік. Комутатори, за допомогою активного відстеження, регулярно вибирають зразки пакетів та метадані і передають їх аналітичному серверу для подальшого аналізу.
2. **Пасивне відстеження.** sFlow може використовувати пасивний метод відстеження, де аналізатор трафіку спостерігає за пакетами, які прокладають шлях через мережевий пристрій. Це дозволяє збирати дані без прямого взаємодії з мережевим обладнанням.
   Приклад. Провайдер інтернет-послуг використовує sFlow для пасивного відстеження трафіку, який проходить через їх маршрутизатори. Аналізатор трафіку моніторить весь вхідний та вихідний трафік для виявлення аномалій, атак чи нестандартного використання ресурсів.
3. **Збір метаданих та виборок.** sFlow дозволяє збирати метадані та вибірки трафіку. Метадані надають додаткову інформацію про пакети, таку як IP-адреси, порти, протоколи тощо. Вибірки трафіку представляють собою зразки конкретних пакетів, що дозволяє визначити типи трафіку та аналізувати їх.
   Приклад. Підприємство використовує sFlow для збору виборок трафіку на своїх серверах. Це дозволяє адміністраторам визначати, які додатки та служби генерують трафік, і вживати заходів для оптимізації мережі.
4. **Аналіз та візуалізація даних.** sFlow забезпечує дані для аналізу та візуалізації трафіку. Аналітичні інструменти можуть використовувати ці дані для створення графіків, діаграм та звітів для зручного сприйняття мережевої активності.
   Приклад. Телекомунікаційна компанія використовує sFlow для збору даних про трафік на своїх ключових маршрутизаторах. Аналітична платформа використовує ці дані для візуалізації обсягів трафіку та виявлення підвищених навантажень.

Пакет sFlow

Пакети sFlow інкапсулюються за допомогою UDP. За замовчуванням номером порту призначення для пакетів sFlow є добре відомий порт 6343. Пакети sFlow використовують такі формати заголовків: зразок потоку, зразок розширеного потоку, зразок лічильника та зразок розширеного лічильника. Зразок Expanded Flow і Expanded Counter sample є доповненнями до sFlow версії 5 і є розширеннями зразка Flow і Counter sample відповідно, але вони несумісні з попередніми версіями. Увесь вміст розширеної вибірки має бути інкапсульований із заголовком у форматі зразка Expanded Flow або Expanded Counter.

Агент sFlow забезпечує відбір проб потоку та лічильник проб. За допомогою вибірки потоку агент sFlow відбирає пакети в заданому напрямку на певному інтерфейсі на основі частоти дискретизації та аналізує пакети, щоб отримати інформацію про вміст пакетних даних. Вибірка потоку зосереджується на деталях трафіку, полегшуючи моніторинг і аналіз поведінки трафіку в мережі.

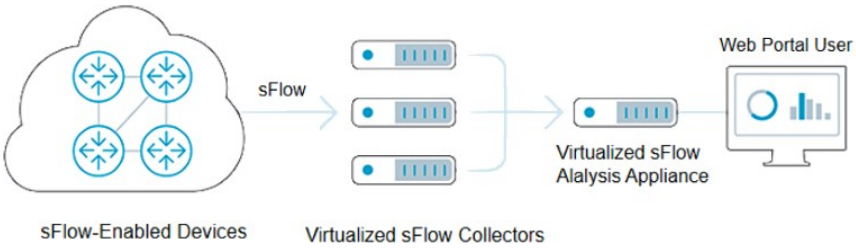


Рис. 04.05. Параметри трафіку

Реалізація аналізу даних за допомогою sFlow.

Розглянемо, як реалізується аналіз даних за допомогою sFlow та як цей процес допомагає вдосконалювати ефективність мережі та забезпечувати безпеку.

1. **Збір та агрегація даних.** sFlow забезпечує постійний збір трафікових даних з мережевих пристроїв, таких як комутатори чи маршрутизатори. Отримані дані включають зразки трафіку, метадані та виборки. Ці дані у подальшому агрегуються, щоб створити повну картину мережевої активності.
   Приклад. Агреговані дані дозволяють визначити топ-протоколи, обсяги трафіку та взаємодії між різними мережевими областями.

2. **Виявлення топології та залежностей.** Аналіз sFlow може виявляти топологію мережі та взаємозв'язки між пристроями. З цими даними можна визначити, як пристрої взаємодіють та які елементи мережі є ключовими.
   Приклад. Виявлення точок перевантаження та знаходження шляхів зайвого трафіку для подальшої оптимізації мережі.
3. **Аналіз аномалій та загроз.** sFlow дозволяє виявляти аномалії та потенційні загрози безпеки. Аналітика враховує асиметрії трафіку, незвичайні патерни та інші аномалії, які можуть свідчити про атаки або несправності в мережі.
   Приклад. Виявлення надмірного використання банд-ширини або спроби несанкціонованого доступу.
4. **Класифікація та оптимізація трафіку.** Аналіз sFlow дозволяє класифікувати трафік за додатками, пристроями та користувачами. Це дозволяє оптимізувати мережеві ресурси, визначаючи пріоритети та вирішуючи проблеми зі швидкістю.
   Приклад. Виділення пріоритетного трафіку для критичних застосунків та підтримка якісної роботи.
5. **Визначення трендів та прогнозування.** Дозволяє визначати тренди та прогнозувати майбутні вимоги мережі. Це корисно для планування росту та оптимізації інфраструктури.
   Приклад. Прогнозування збільшення обсягів трафіку та підготовка мережі до масштабування.
6. **Візуалізація та звітність.** sFlow дозволяє створювати візуалізації та звіти, які полегшують сприйняття складних даних мережі. Інтерактивні панелі та графіки роблять аналіз доступним для широкого кола користувачів.
   Приклад. Створення графіків для представлення керівництву стану мережі та використання ресурсів.

Переваги sFlow порівняно з іншими методами збору мережевих статистичних даних.

sFlow порівняно з іншими методами, він має кілька важливих переваг. Давайте розглянемо, як sFlow виправдовує свою важливість порівняно з іншими традиційними методами збору статистики мережі.

1. **Ефективність та економія ресурсів.** sFlow використовує метод збору зразків трафіку, що дозволяє значно зменшити обсяг даних, що передаються, у порівнянні з повним збором пакетів. Це призводить до економії пропускної здатності мережі та ресурсів сховища даних.
   Порівняння: SNMP (Simple Network Management Protocol) та RMON (Remote Monitoring) можуть вимагати передачі повного обсягу даних, що може призвести до перевантаження ресурсів.
2. **Гнучкість та спрощена конфігурація.** sFlow дозволяє гнучко налаштовувати параметри збору даних, визначати частоту та обсяг зразків трафіку. Це робить його більш адаптивним до змінних умов мережі та потреб користувача.
   Порівняння: Класичні методи мережевого моніторингу, такі як протоколи SNMP або RMON, можуть бути менш гнучкими у відношенні конфігурації та адаптації.
3. **Точність та повнота даних.** sFlow надає точні та повні дані за допомогою вибіркового методу збору зразків трафіку. Це дозволяє визначити ключові параметри трафіку без перевантаження мережі.
   Порівняння: Деякі інші протоколи можуть втрачати дані або надавати менш детальну інформацію, особливо при великому обсязі трафіку.
4. **Підтримка комплексних середовищ.** sFlow може використовуватися на різноманітних мережевих пристроях, включаючи комутатори, маршрутизатори та віртуальні області, що робить його відмінним вибором для комплексних мережевих середовищ.
   Порівняння: Деякі інші протоколи можуть бути обмежені підтримкою або сумісністю з окремими типами обладнання.
5. **Масштабованість.** sFlow легко масштабується для великих мереж та потоків трафіку. Збір зразків дозволяє виявляти аномалії та аналізувати трафік, незалежно від обсягу.
   Порівняння: У деяких випадках інші протоколи можуть стикається з обмеженнями масштабування або потребою в додаткових ресурсах.

Порівняння методу збору даних NetFlow та sFlow

У чому ключові відмінності між Netflow, як стандарту став таким де-факто, і тим же sFlow? Ключових є кілька. По-перше, Netflow має поля, що настроюються користувачем на відміну від фіксованих полів в sFlow. А по-друге, і це - найголовніше, sFlow збирає так звану семпльовану телеметрію; на відміну від несемпльованої у Netflow та IPFIX. У чому між ними різниця?

Таблиця 04.02

Функція	**NetFlow**	**sFlow**
Захоплення пакетів	Не захоплює пакетів зовсім.	Копіює всі пакети та семплює 1 з N для відправки на колектор.
Підтримка протоколів	Рівень 2 IPv4 та IPv6	Незалежний від мережевого рівня
Конфігуровані поля	Flexible NeFlow – поля, що налаштовуються користувачем (шаблон)	Фіксовані поля протоколу
Записи потоків	Підтримка запису потоків IPv4 та IPv6 для всього трафіку	Запис потоку не виконується, копіюються перші N байт пакету.

Апаратне прискорення	Так, запис потоків виконується Hard ware («в залізі») без впливу на Data Plane	Апаратне прискорення можливе. Зазвичай, пакети захоплюються ПЗ.
Індустріальний стандарт	IpFix	sFlow v5
Часові мітки потоків (час початку та завершення потоку)	Так	Ні
Packet rates (кількість пакетів у потоку)	Так	Ні
Підрахунок байт (число байт у потоку)	Так	Частково

Важко сприйняти одразу, що наведено у цій порівняльній таблиці, але є дуже класне пояснення.
Уявіть, що ви вирішили ознайомитися з друкованою книгою великого об'єму. У вас є три варіанти досягти поставленої мети

- прочитати книгу повністю,
- пробігти її очима, зупиняючись на кожній 10-й або 20-й сторінці,
- спробувати знайти переказ ключових концепцій у будь-якому блозі або сервісі.

Так ось несемпльована телеметрія - це читання кожної "сторінки" мережного трафіку, тобто аналіз метаданих по кожному пакету. Семпльована телеметрія — це вибіркове вивчення трафіку, сподіваючись, що в обраних семплах виявиться те, що вам потрібно. Залежно від швидкості каналу, семпльована телеметрія віддаватиме для аналізу кожен 64-й, 200-й, 500-й, 1000-й, 2000-й або навіть 10000-й пакет.
У контексті моніторингу це означає, що семпльована телеметрія добре підходить для виявлення DDoS-атак, сканування, розповсюдження шкідливого коду, але може пропустити атомарні або багатопакетні атаки, які не потрапили в семпл, надісланий для аналізу. За допомогою спектр виявлених атак набагато ширше. Ось невеликий перелік подій, які можна виявляти за допомогою засобів аналізу мережевої телеметрії.

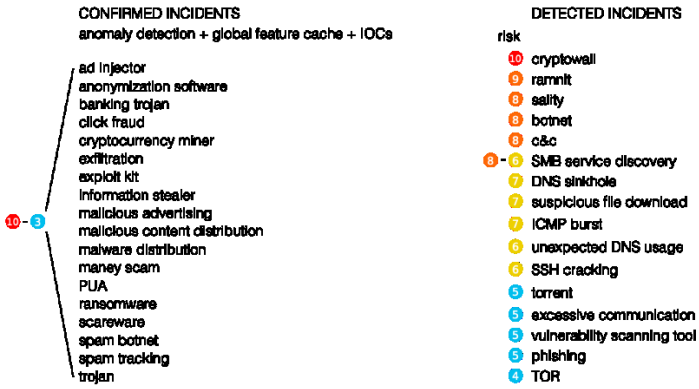


Рис. 04.06. Події, що виявляються за допомогою аналізу мережевої телеметрії.

Зрозуміло, що аналізатор Netflow з відкритим кодом не допоможе у цьому, оскільки його основне завдання — збирати телеметрію та виконувати її базовий аналіз з точки зору IT. Щоб виявити загрози безпеці на основі потоку, аналізатору необхідно додати різні engines та алгоритми, які виявлятимуть проблеми кібербезпеки на основі стандартних або використаних полів Netflow, збагачувати стандартні дані зовнішніми даними з різних джерел аналізу загроз.
Іншими словами, оскільки sFlow містить повний заголовок пакета, він дає ширшу картину мережевого трафіку, забезпечуючи повний рівень (L2, L3, L4 і до L7) видимості всіх типів трафіку у мережі, включаючи IP-адреси та VLAN, з яких можливо «витягти» будь-яке поле. NetFlow по суті містить лише частину цих полів.
NetFlow «перетравлює» набагато більше інформації, ніж sFlow, а тому використовує набагато більше ресурсів, ніж sFlow, створюючи більше навантаження на мережеві пристрої, що робить sFlow кращим вибором для пристроїв нижчого рівня. Проте, який із цих протоколів краще підходить для конкретної мережі, залежатиме від того, що підтримують конкретні мережеві пристрої та провайдери мережі.

Аналіз та використання даних, зібраних за допомогою протоколів NetFlow та sFlow.

Інструменти для обробки та аналізу даних.

Збір та аналіз даних, що надходять від протоколів NetFlow та sFlow, вимагає відповідних інструментів для ефективного використання цієї інформації. Розглянемо основні інструменти для обробки та аналізу зібраних даних, які допомагають мережевим адміністраторам зрозуміти стан мережі, виявляти проблеми та оптимізувати ресурси.

- **NetFlow та sFlow колектори.** Спеціальні програмні чи апаратні компоненти, що відповідають за збір і агрегацію даних від пристроїв, які підтримують протоколи NetFlow та sFlow. Ці компоненти відомі як коллектори. Деякі з популярних NetFlow колекторів включають PRTG Network Monitor, SolarWinds NetFlow Traffic Analyzer та Scrutinizer. Для sFlow існують також спеціальні колектори, такі як InMon sFlowTrend та sFlow-rt.
- **Аналітичні інструменти.** Одним з популярних виборів є Wireshark, який підтримує аналіз NetFlow та sFlow пакетів. Він дозволяє переглядати і розбирати трафік для деталізованого розуміння мережевих подій. Інші інструменти, такі як Cisco Stealthwatch, SolarWinds NTA та ManageEngine NetFlow Analyzer, надають розширені можливості аналізу та візуалізації даних.
- **Визначення ключових показників продуктивності.** Для визначення KPI необхідні спеціальні інструменти для моніторингу та оцінки різних аспектів мережі. Такі інструменти включають Grafana, Kibana, а також вбудовані функції в NetFlow та sFlow колекторів.
- **Інструменти для виявлення аномалій** використовують для виявлення незвичайної або підозрілої активності у мережі. SolarWinds Security Event Manager, Splunk та ELK Stack є популярними інструментами для цього завдання.
- **Візуалізація та звітність.** Інструменти для візуалізації та звітності грають важливу роль у сприйнятті складних даних. Grafana, Kibana, Power BI та Tableau - це інструменти, що дозволяють створювати динамічні графіки та звіти.
- **Інтеграція з іншими системами.** Деякі інструменти можуть бути інтегровані з іншими системами управління, такими як системи моніторингу здоров'я мережі чи системи безпеки. Це важливо для комплексного підходу до управління мережею.

- **Використання штучного інтелекту та машинного навчання** може надати автоматизовані функції для аналізу та прогнозування, наприклад, оптимізація роботи мережі або виявлення аномальної поведінки.

Визначення ключових показників продуктивності

Визначення ключових показників продуктивності (KPI) є важливою частиною мережевого моніторингу, і протоколи NetFlow та sFlow стають невід'ємною складовою цього процесу. Розглянемо, як ці протоколи можуть визначати KPI.

- **Передача даних та обсяг трафіку.** Один з основних KPI, що визначається протоколами NetFlow та sFlow, - це обсяг переданих даних. За допомогою цього параметра можливо визначити, яка частина мережі використовується найбільше, і виявити можливі перевантаження. NetFlow, наприклад, надає інформацію про використання пропускної здатності на різних рівнях мережі, визначаючи, які додатки або сервіси забирають більше ресурсів. За допомогою sFlow можна визначити обсяг трафіку на різних портах та пристроях. Це дозволяє виконувати оптимізацію мережевого трафіку. Розглянемо стратегії оптимізації мережевого трафіку.
  - ✓ **Аналіз трафіку та визначення потреб.** Оптимізації мережевого трафіку починається з аналізу трафіку для визначення його характеристик і потреб. NetFlow та sFlow дозволяють збирати детальні дані про види трафіку, його джерела та призначення.
  - ✓ **Ідентифікація та усунення зайвого трафіку.** Виявлення зайвого чи непотрібного трафіку, такий як пакети від небажаних джерел чи несанкціоновані підключення. Видаляючи або фільтруючи цей трафік, можна значно покращити ефективність мережі.
  - ✓ **Балансування навантаження та маршрутизація.** NetFlow надає аналітику з розподілу навантаження, дозволяючи адміністраторам балансувати навантаження між різними мережевими шляхами. Це допомагає уникнути перевантаження окремих лінків та підвищує доступність.
  - ✓ **Впровадження кешування та оптимізація пропускної здатності.** За допомогою sFlow можна виявити часто використовувані запити чи дані, що дозволяє оптимізувати пропускну здатність за допомогою кешування та розподілення навантаження.
  - ✓ **Адаптація до змін умов та завантаження.** NetFlow та sFlow надають засоби для моніторингу та аналізу змін у мережевому трафіку під час пікового навантаження чи інших витоків. Це дозволяє мережі адаптуватися до нових умов та максимально використовувати ресурси.
- **Профілювання трафіку.** За допомогою NetFlow та sFlow можна визначити типи трафіку, які присутні в мережі. Наприклад, розпізнання VoIP-трафіку чи визначення, які додатки споживають більше ресурсів. Профілювання трафіку дозволяє адміністраторам ефективно керувати ресурсами, визначаючи, які додатки чи сервіси є найбільш критичними для продуктивності бізнес-процесів.
- **Затримки та втрати пакетів.** Протоколи NetFlow та sFlow можуть фіксувати затримки та втрати пакетів у мережі. Це дозволяє визначити, наскільки ефективно працює мережа, і швидко виявити проблеми, такі як перевантаження або неправильна конфігурація обладнання. За допомогою цих даних можна визначити, чи необхідно вжити заходів для оптимізації роботи мережі та забезпечення високої якості обслуговування.
- **Підтримка QoS (Quality of Service).** NetFlow та sFlow дозволяють визначати параметри QoS для різних видів трафіку. Це дозволяє ефективно управляти пропускною здатністю та гарантувати високу якість обслуговування для критичного трафіку. За допомогою цих протоколів можна встановлювати пріоритети та контролювати резервування пропускної здатності для покращення продуктивності.
- **Виявлення аномалій та безпека.** NetFlow та sFlow можуть служити ефективними інструментами для виявлення аномальної поведінки. За допомогою вивчення зразків трафіку можна виявляти незвичайні події, що можуть свідчити про атаки або інші проблеми в мережі.
  - ✓ **Моніторинг зв'язків та поведінки.** За допомогою аналізу потоків трафіку можна виявляти незвичайні або підозрілі патерни. Наприклад, велика кількість спроб з'єднань до певного сервера чи зміна типу трафіку може свідчити про проблеми або атаки.
  - ✓ **Аналіз великих обсягів даних** за короткий період часу. Це дозволяє виявляти аномалії, такі як великі скачки трафіку, що можуть свідчити про деякі проблеми, наприклад, велике завантаження мережі чи атаку. За допомогою цього аналізу можна визначити часові і просторові залежності аномальних явищ, що допомагає в усуненні проблем у найкоротший термін.
  - ✓ **Виявлення Denial-of-Service (DoS) та Distributed Denial-of-Service (DDoS) Attack**. Дозволяє виявляти атаки типу DoS та DDoS, де атакуючий намагається призупинити нормальну роботу мережі чи обслуговування сервера, завантажуючи його. Виявлення зростання трафіку або спроб з'єднань, яке виходить за межі звичайних показників.
  - ✓ **Вимірювання пропускної здатності та швидкості відгуку.** Виявлення зниження швидкості передачі даних або підвищення часу відгуку може свідчити про проблеми, такі як перевантаження лінків або несправності у пристроях. Це дозволяє вчасно реагувати на зміни у продуктивності мережі та уникати витрат часу на вирішення проблем у разі їхнього виникнення.
  - ✓ **Моніторинг безпеки та виявлення вразливостей.** Аналіз трафіку дозволяє виявити підозрілі підключення чи аномалії, що можуть бути наслідками вразливостей. Це важливо для підтримки безпеки мережі та запобігання можливим атакам.
- **Моніторинг пропускної здатності лінків.** Протоколи NetFlow та sFlow надають інформацію про використання пропускної здатності лінків між пристроями. Це дозволяє вчасно виявляти перевантаження та планувати розширення лінків.

Висновки.

Резюмуючи основні аспекти NetFlow, слід вказати на його ключові характеристики, такі як здатність збору детальних даних про мережевий трафік, виявлення проблем та використання в різноманітних сценаріях. Щодо sFlow, важливо визначити його унікальні можливості, такі як активне та пасивне відстеження, які роблять його ефективним інструментом для аналізу мережі.

Використання NetFlow та sFlow у щоденній роботі NA відіграє важливу роль у підтримці ефективності та безпеки мережі. NA можуть ефективно моніторити та управляти мережевим трафіком, виявляти аномалії та вирішувати проблеми в реальному часі. Збір та аналіз даних, наданих цими протоколами, робить можливим покращення продуктивності та оптимізацію інфраструктури.

Розглядаючи шляхи подальшого розвитку NetFlow та sFlow, можна звернутися до новітніх технологій, таких як підтримка швидших швидкостей передачі даних, розширення функціональності для аналізу мережевих пакетів, а також адаптацію до змін у вимогах до безпеки.

Загальною тенденцією може бути інтеграція протоколів NetFlow та sFlow з іншими інструментами моніторингу та аналізу мережі, що розширює їхню функціональність та забезпечує більшу зручність в управлінні мережею.

Збір та аналіз мережевих даних за допомогою NetFlow та sFlow є ключовими аспектами для успішного функціонування та ефективного управління сучасними мережами.