План лекції . Тема 3. Вступ до мережевого моніторингу.

- Значення мережевого моніторингу у сучасних мережевих інфраструктурах.
- Основні завдання та вимоги до мережевого моніторингу.
- Засоби та технології, що використовуються для збору мережевих даних.

Визначення мережевого моніторингу

Моніторинг мережі — це використання системи, яка постійно відстежує комп'ютерну мережу на наявність повільних або несправних компонентів і сповіщає адміністратора мережі (через електронну пошту , SMS або інші сигнали тривоги) у разі збоїв або інших проблем. Моніторинг мережі є частиною керування мережею .

Ще одне визначення

Моніторинг мережі — це практика моніторингу та аналізу продуктивності та працездатності комп'ютерної мережі, щоб переконатися, що вона працює ефективно та результативно. Він передбачає безперервне вимірювання та оцінку різних параметрів мережі для виявлення та вирішення проблем, оптимізації мережевих ресурсів і підтримки високого рівня якості обслуговування.

У сучасну цифрову епоху моніторинг мережі став ключовим аспектом управління IT-інфраструктурою. Здатність відстежувати продуктивність мережі та керувати нею має важливе значення для забезпечення ефективної та ефективної роботи мереж. Моніторинг продуктивності мережі може служити керівною силою для IT-фахівців, допомагаючи їм орієнтуватися в складнощах сучасної мережі. середовищ.

В рамках мережевого моніторингу використовуються спеціальні засоби та технології для збору, аналізу та візуалізації даних, що дозволяє адміністраторам мережі отримувати комплексну інформацію про стан мережі, виявляти аномалії, вирішувати технічні проблеми та підтримувати високий рівень її ефективності.
Ці систематичні дії направлені на виявлення повільних або несправних мережевих компонентів, таких як перевантажені сервери, збій чи зависання елементу мережі, несправні маршрутизатори, несправні комутатори, інші проблемні пристрої. У разі відмови мережі або подібного відключення система моніторингу мережі попереджає адміністратора мережі (**NA**). Моніторинг мережі - це підмножина управління мережею.

Моніторинг мережі відрізняється від традиційного системного моніторингу тим, що продуктивність контролюється з точки зору кінцевого користувача та вимірюється між двома точками в мережі. Наприклад:

- Продуктивність між користувачем, який працює в офісі, і додатком, який він використовує в дата-центрі компанії
- Продуктивність між двома офісами в мережі
- Продуктивність між головним офісом та Інтернетом
- Продуктивність між вашими користувачами та хмарою

Ключові аспекти мережевого моніторингу не відрізняються від інших видів моніторингу та включають:

- **Збір даних.** Мережевий моніторинг включає в себе збір різноманітних даних, таких як пакети, логи подій, використання ресурсів, стан обладнання та інші метрики, які характеризують стан мережі.
- **Аналіз та інтерпретація.** Отримані дані аналізуються для виявлення аномалій, прогнозування проблем та оцінки ефективності мережі. Це може включати в себе виявлення вузьких місць, проблем з безпекою, атак або інших аномалій.
- **Візуалізація.** Використовуються графіки, діаграми та інші засоби візуалізації для наглядного представлення стану мережі. Це допомагає швидше розуміти поточний стан та реагувати на проблеми.
- **Сповіщення та реагування.** Моніторингові системи можуть автоматично генерувати сповіщення або реагувати на виявлені проблеми. Це може включати в себе автоматичне відновлення роботи, відправлення повідомлень адміністраторам або запуск процедур безпеки.
- **Документація.** Ведення документації про мережевий моніторинг є важливим для аналізу та вдосконалення системи. Це включає в себе записи про виявлені проблеми, вжиті заходи та результати аналізу.

Пояснення основних понять та термінів

Хоча тут присутні лише фахівці, не зайвим буде згадаємо деякі основні терміни та поняття, що є важливими для розуміння теми мережевого моніторингу:

- **Мережа (Network).** Сукупність з'єднаних пристроїв чи систем, які можуть обмінюватися даними між собою. Мережі можуть бути локальними (**LAN**), глобальними (**GAN**), або іншими за масштабом, такими як мережі широкого доступу (**WAN**). Локальні мережі (**LAN**) охоплюють обмежену територію, таку як один будинок, підприємство чи установа. Мережі широкого доступу (**WAN**) включають в себе більші території, такі як регіон, країну чи навіть світ, і зазвичай використовують технології, такі як Інтернет, для з'єднання віддалених місць. Адміністратор мережі (**NA**) відповідає за конфігурацію, управління та підтримку мережевого обладнання та програмного забезпечення.
- **Моніторинг (Monitoring)**. У нас вже третя лекція курсу, тому лише нагадаю, що це систематичний контроль та відстеження подій, стану чи активності для отримання інформації та виявлення можливих проблем.
- **Мережевий моніторинг (Network Monitoring)**. Процес відстеження та аналізу стану мережі, її компонентів та трафіку для забезпечення ефективності, безпеки та доступності.

- **Системи моніторингу мережі (NMS).** Network Monitoring System - програмні засоби, призначені для моніторингу та аналізу мережевого трафіку. Вони забезпечують видимість у реальному часі продуктивності мережі та подій безпеки.

- **Трафік (Traffic)**. Об'єм даних, які пересилаються між пристроями у мережі. Трафік може бути виміряний в бітах, байтах або інших одиницях.

- **Пропускна спроможність (Bandwidth)**. Максимальний обсяг даних, який може бути переданий через мережу протягом певного часу.

- **Пакет (Packet)**. Невеликий блок даних, який пересилається через мережу. Пакети містять інформацію про джерело, призначення та самі дані.

- **Протокол (Protocol)**. Стандартні правила та формати для обміну даними між пристроями у мережі. Наприклад, TCP/IP - основний протокол Інтернету.

- **Адреса (Address)**. Унікальний ідентифікатор для пристрою чи служби в мережі. IP-адреси та MAC-адреси є прикладами.

- **Пінг (Ping)**. Команда для перевірки доступності пристрою у мережі шляхом відправлення короткого пакету та очікування відповіді.

- **SNMP (Simple Network Management Protocol)**. Протокол для управління та моніторингу мережевих пристроїв, або як звучить перше визначення цього протоколу - Simple Network Management Protocol — простий протокол керування мережею

- **Аномалія (Anomaly)**. Неочікувана чи відхилення від звичайного стану. У випадку мережевого моніторингу аномалія показників чи параметрів може вказувати на проблеми в мережі.

- **Firewall**. Програмно-апаратний засіб, що контролює та фільтрує мережевий трафік для забезпечення безпеки.

Ці терміни становлять основу для розуміння мережевого моніторингу та його ключових аспектів.

Роль мережевого моніторингу у сучасних технологічних системах

Якась дивна ситуація при вивченні моніторингу – як тільки починаєш розповідати про роль якоїсь складової, вона виявляється або дуже важливою, або головною ☺
Роль мережевого моніторингу у сучасних технологічних системах є необхідним елементом для управління сучасними технологічними системами, особливо з урахуванням зростання обсягів даних, складності мереж та загроз безпеки. Головні аспекти цієї ролі мережевого моніторингу:

- **Стабільність та продуктивність.**
  - ✓ **Виявлення проблем.** Мережевий моніторинг дозволяє виявляти аномалії та вказівники несправностей в роботі мережі.
  - ✓ **Прогнозування перевантажень**. Аналіз трафіку допомагає уникнути перевантажень, планувати ресурси та підтримувати стабільність.

- **Безпека та виявлення загроз.**
  - ✓ **Виявлення інцидентів**. Мережевий моніторинг допомагає виявляти атаки, несанкціонований доступ та інші потенційно небезпечні активності.
  - ✓ **Моніторинг заходів безпеки**. Спостереження за ефективністю заходів безпеки та швидке реагування на події безпеки.

- **Відділення проблем та швидке відновлення:**
  - ✓ **Ізоляція проблем.** Мережевий моніторинг дозволяє швидко ідентифікувати місце та природу проблем.
  - ✓ **Відновлення після відмов**. Автоматизовані системи моніторингу допомагають відновлювати роботу мережі після виникнення неполадок.

- **Оптимізація ресурсів:**
  - ✓ **Моніторинг використання ресурсів.** Слідкування за використанням обладнання та ресурсів допомагає оптимізувати роботу мережі.
  - ✓ **Планування розширень**. Аналіз трафіку допомагає у плануванні майбутніх розширень та апгрейдів.

- **Відповідність та аналітика:**
  - ✓ **Збір даних для відповідності**. Моніторинг забезпечує збір та архівацію даних для відповідності стандартам та регулятивам.
  - ✓ **Аналіз даних.** Використання аналітики для отримання важливих інсайтів щодо ефективності та стану мережі.

Оптимізація роботи мережі

Загальні поняття про стабільність та швидкість мережі необхідні для розуміння та ефективного управління мережевою інфраструктурою, що забезпечує стійку та швидку передачу даних.

- **Стабільність мережі** вказує на її здатність залишатися в робочому стані без непередбачених відмов чи значних коливань у роботі. Стабільність залежить від надійності обладнання, налаштувань конфігурації, ефективності маршрутизації та відсутності атак або неполадок.

- **Швидкість мережі** вказує на кількість даних, які можуть бути передані через мережу протягом певного часу. Швидкість вимірюється в бітах на секунду (bps), кілобітах на секунду (Kbps), мегабітах на секунду (Mbps), гігабітах на секунду (Gbps) і т.д. На швидкість мережі впливають:
  - ✓ пропускна здатність каналів
  - ✓ якість з'єднань
  - ✓ обсяг трафіку

- ✓ ефективність мережевого обладнання.

Зовсім нещодавно (16.11.2023 р.) співробітниками Датського технічного університету встановлено новий світовий рекорд швидкості передачі інформації через оптичне волокно з використанням одного передавача.
Раніше рекорд належав Інституту технологій з Німеччини, де була досягнута швидкість в 11 терабіт в секунду. Група співробітників по фотонним технологій з Технічного університету Данії значно перевершили своїх колег домігшись швидкості в 43 терабіта за секунду.
Ця швидкість дозволить виконати копіювання гігабайтного файлу за 0,2 мс, а копіювання терабайта займе до 0,18 секунди. У коментарях датських фахівців кажуть, що подібні дослідження дозволять прийти до значно більш високих швидкостей, які необхідні і актуальні в зв'язку з ростом обсягів переданого трафіку, розвитком Wi-Fi і стільникових мереж.

- **Взаємозв'язок між стабільністю та швидкістю** дуже тісний. Забезпечення стабільності часто пов'язано з оптимізацією швидкості та навпаки. Висока швидкість може призвести до нестабільності, якщо інфраструктура не готова впоратися з великим обсягом трафіку. Іншими словами взаємний вплив швидкості та стабільності мережі можна пояснити наступними трьома тезами:
  - ✓ **Швидкість і стабільність**. Висока швидкість мережі дозволяє швидко передавати дані між пристроями та користувачами, що покращує продуктивність та ефективність роботи. Проте, якщо інфраструктура мережі не готова впоратися з великим обсягом трафіку, це може призвести до перевантаження, втрати пакетів даних та зниження якості обслуговування.
  - ✓ **Стабільність забезпечується інфраструктурою**. Щоб забезпечити стабільність мережі, потрібно мати належно налаштовані маршрутизатори, комутатори, файрволи та інші пристрої, які розподіляють навантаження та контролюють трафік. Також потрібно використовувати механізми керування трафіком, які можуть регулювати швидкість передачі даних та захищати мережу від перевантаження.
  - ✓ **Оптимізація для підвищення продуктивності.** Про загальні підходи у оптимізації швидкості мережі (CDN, кешування контенту та використання високопродуктивних пристроїв маршрутизації та комутації) ми поговоримо трошки пізніше.
- **Фактори впливу**. На стабільність та швидкість впливає кілька факторів:
  - ✓ **Пропускна здатність**. Максимальний обсяг даних, який може бути переданий через мережу протягом певного часу. Одиниці вимірювання ті ж, що у у швидкості мережі (біт/с, Кбіт/с, Мбіт/с). Критерії встановлення пропускної здатності це
    - **Тип мережі.** Варіюється залежно від типу мережі, наприклад, Ethernet, Wi-Fi, або мобільного зв'язку.
    - **Протокол**. Варіюється залежно від протоколу, який використовується для передачі даних, наприклад, TCP, UDP, або HTTP.
    - **Апаратне забезпечення**. Залежить від апаратного забезпечення, яке використовується, наприклад, мережевих карт, маршрутизаторів, або комутаторів.

  Існує кілька способів вимірювання пропускної здатності мережі:
    - Тестування швидкості: Ви можете використовувати онлайн-сервіси або програмне забезпечення для тестування швидкості вашого інтернет-з'єднання.
    - Моніторинг мережі: Ви можете використовувати програмне забезпечення для моніторингу мережі, щоб відстежувати пропускну здатність мережі протягом певного часу.
    - Розрахунок: Ви можете розрахувати пропускну здатність мережі, знаючи ширину смуги пропускання та співвідношення сигнал/шум.
    - Важливо зазначити, що пропускна здатність мережі може бути динамічною і може змінюватися залежно від різних факторів, таких як завантаження мережі, наявність перешкод, або оновлення програмного забезпечення.
  - ✓ **Затримка та джиттер**. Затримка (Latency) це час, який займає передача даних від джерела до приймача через мережу. Затримка включає час, необхідний для проходження сигналу через маршрутизатори, комутатори, кабелі та інші мережеві пристрої. Зазвичай затримка вимірюється у мілісекундах (мс) або мікросекундах (мкс).
    Джиттер (Jitter) - це непередбачувані зміни в затримці передачі даних через мережу. Джиттер може виникати через зміну навантаження на мережу, коливання швидкості передачі даних або інші фактори, які впливають на стабільність мережевого з'єднання. Джиттер також вимірюється в мілісекундах (мс) або мікросекундах (мкс).
    Загальною метрикою, яка використовується для вимірювання і оцінки затримки та джиттеру, може бути середня затримка та середній джиттер. Ці метрики дають уявлення про типові часи затримки та коливання в мережі.
    Важливо зазначити, що низька затримка та джиттер допомагають забезпечити стабільний та швидкий зв'язок в мережі, особливо для додатків, які вимагають реального часу, таких як відеоконференції або онлайн-ігри.
  - ✓ **Втрати пакетів**. Кількість пакетів, які не досягли свого призначення через мережу.

- **Важливість балансу.**
  - ✓ **Оптимізація**. Забезпечення оптимального балансу між стабільністю та швидкістю для задоволення потреб користувачів та бізнес-процесів.
  - ✓ **Керування ресурсами**. Ефективне використання ресурсів, таких як пропускна здатність та енергія, для забезпечення стійкості та продуктивності.

Забезпечення стабільності та швидкодії

Вплив стабільності та швидкодії на користувачів та бізнес-процеси є невід'ємною частиною стратегії інфраструктурного управління та визначає успіх організації в сучасному конкурентному середовищі.

Таблиця 03.01

Користувачі	Бізнес-процеси
• **Задоволення користувачів**. ✓ **Стабільність**. Стабільна мережа забезпечує безперебійні з'єднання, що призводить до задоволення користувачів. Вони можуть впевнено використовувати сервіси без перебоїв. ✓ **Швидкість.** Швидка передача даних дозволяє користувачам отримувати доступ до ресурсів та послуг без	• **Неперервність операцій**. ✓ **Стабільність**. Для бізнесу критично важливо мати стабільну мережу, що дозволяє неперервно проводити операції та обслуговувати клієнтів. ✓ **Швидкість**. Швидка передача даних сприяє ефективності бізнес-процесів, зменшуючи час на виконання завдань та обробку інформації.

затримок, покращуючи їхню взаємодію з інтернетом та іншими сервісами. • **Продуктивність та ефективність.** ✓ **Стабільність**. Відсутність відмов та перебоїв забезпечує неперервну продуктивність користувачів, що є ключовим для бізнес-процесів. ✓ **Швидкість**. Швидка передача даних підвищує продуктивність та забезпечує ефективність в роботі з ресурсами та інструментами. • **Відгуки та лояльність**. ✓ **Стабільність.** Стабільна робота мережі призводить до позитивних відгуків і підтримує лояльність користувачів. ✓ **Швидкість.** Швидке обслуговування сприяє задоволенню користувачів, що впливає на їхню готовність залишатися в системі.	• **Конкурентоспроможність.** ✓ **Стабільність**. Організації з надійною мережею здатні уникати втрат часу та ресурсів, що робить їх конкурентоспроможними на ринку. ✓ **Швидкість**. Швидкі бізнес-процеси дозволяють реагувати на зміни ринку швидше, що може бути важливим для успіху підприємства. • **Безпека даних.** ✓ **Стабільність**. Стабільна мережа важлива для забезпечення безпеки даних та уникнення доступу до них несанкціонованими особами. ✓ **Швидкість**. Швидка передача даних може підвищити ефективність заходів забезпечення безпеки та захисту інформації.

Стратегії оптимізації для забезпечення стабільності та швидкодії мережі:

Таблиця 03.02

Категорія	Призначення	Стратегічні дії
Керування пропускною здатністю	Полягає в розподілі та контролі доступу до мережевої пропускної здатності з метою оптимізації трафіку та покращення швидкодії.	✓ **Пріоритетизація трафіку**. Встановлення пріоритетів для різних типів трафіку (наприклад, відео, голос, дані), щоб важливі дані мали вищий пріоритет та гарантований доступ до пропускної здатності. ✓ **Мережеві контролери пропускної здатності**. Використання спеціалізованих пристроїв та алгоритмів для управління пропускною здатністю та виявлення проблем.

Пріоритетизація трафіку може бути особливо важливою в ситуаціях, коли мережа перевантажена або коли важливі додатки чи послуги потребують стабільної пропускної здатності. Ось деякі методи пріоритетизації трафіку:

- **Quality of Service (QoS)** - це механізм, який дозволяє встановлювати пріоритети для різних видів трафіку на основі визначених параметрів, таких як тип даних (голос, відео, дані), протокол чи джерело/призначення. Наприклад, голосовий трафік може мати вищий пріоритет над трафіком відеоконференцій, а відео - над загальними даними.
- **Traffic Shaping (Формування трафіку)** використовується для керування пропускною здатністю шляхом обмеження швидкості передачі даних для певних типів трафіку. Наприклад, швидкість завантаження/відвантаження може бути обмежена для файлового трафіку, щоб забезпечити достатню пропускну здатність для інших важливих додатків, таких як голос або відео.
- **Packet Prioritization (Пріоритетизація пакетів)** полягає у встановленні пріоритету для індивідуальних пакетів даних у мережі. Це може бути досягнуто за допомогою маркування пакетів заздалегідь визначеними мітками (тегами), які вказують рівень пріоритету. Марковані пакети обробляються з вищим пріоритетом, що забезпечує їм перевагу при передачі через мережу.
- **Traffic Classification (Класифікація трафіку)** визначає типи трафіку на основі його характеристик, таких як порт призначення, протокол або структура даних. Після класифікації трафіку можна встановити правила для керування пропускною здатністю відповідно до потреб кожного типу трафіку.

Щодо мережевих контролерів пропускної здатності (Network Traffic Controllers) - це пристрої або програмне забезпечення, що використовуються для управління трафіком у мережі з метою оптимізації пропускної здатності та виявлення проблем.
Ось деякі аспекти використання спеціалізованих пристроїв та алгоритмів управління пропускною здатністю:

- **Quality of Service (QoS) Policies**. Мережеві контролери можуть застосовувати QoS політики для встановлення пріоритетів та керування трафіком на основі параметрів, таких як тип даних, джерело/призначення, протокол тощо. Наприклад, вони можуть надавати вищий пріоритет для голосового трафіку порівняно з відеоабо файловим трафіком.
- **Traffic Shaping and Policing**. Контролери можуть використовувати методи формування трафіку та контролю для керування швидкістю передачі даних. Це дозволяє регулювати трафік для забезпечення оптимального використання пропускної здатності мережі та уникнення перевантаження.
- **Deep Packet Inspection (DPI)**. Деякі контролери можуть використовувати DPI для аналізу вмісту пакетів даних і виявлення різних типів трафіку або патернів. Це дозволяє виявляти аномальний трафік, шкідливі програми або атаки на мережу.
- **Load Balancing**. Контролери також можуть використовуватися для розподілу трафіку між різними мережевими шляхами або серверами з метою збалансування навантаження і забезпечення оптимальної швидкості та доступності.
- **Traffic Monitoring and Analysis**. Контролери також можуть здійснювати моніторинг трафіку та аналізувати дані про його потік для виявлення аномалій, виявлення проблем у мережі або ідентифікації джерела проблем.

Network Traffic Controllers можуть бути реалізовані як спеціалізовані апаратні пристрої, так і програмне забезпечення, що запускається на загальнопризначених серверах або віртуальних машинах. Ці можливості додатково конфігуруються та налаштовуються залежно від потреб конкретної мережі або організації.
Щодо виробників, які займаються випуском та підтримкою Network Traffic Controllers, ось декілька провідних компаній:

- **Cisco Systems**
- **Juniper Networks**
- **Huawei**
- **F5 Networks**
- **Palo Alto Networks**

Використання технологій кешування	Використовуються для збереження копій часто використовуваних даних близько до користувачів, зменшуючи час доступу та навантаження на мережу.	✓ **Локальне кешування**. Зберігання копій даних на локальних пристроях чи серверах, що дозволяє зменшити час завантаження даних з віддалених джерел. ✓ **Використання CDN (Content Delivery Network)**. Розподілення копій контенту на серверах, розташованих у різних регіонах, для забезпечення швидкого доступу до контенту.

Локальне кешування впливає на стабільність та швидкодію мережі, надаючи такі переваги:

- **Зменшення трафіку**, яке забезпечується тим, що повторні запити до контенту можуть бути оброблені локально, без необхідності витрачати пропускну здатність мережі для запитів цього контенту з віддалених серверів. Це дозволяє зменшити загальний обсяг трафіку в мережі та робить її більш ефективною.
- **Покращена швидкість доступу**. Оскільки контент знаходиться ближче до кінцевого користувача, час доступу до цього контенту зменшується. Кешовані дані можуть бути доставлені швидше, оскільки вони вже знаходяться на локальному пристрої або на сервері, розташованому ближче до користувача.
- **Зменшення завантаження віддалених серверів**. Локальне кешування дозволяє розподіляти навантаження між локальними та віддаленими серверами. Це може зменшити навантаження на віддалені сервери, що дозволяє їм краще керувати запитами та забезпечити стабільнішу роботу.
- **Покращення доступності контенту при відсутності зв'язку з мережею**. Локальне кешування дозволяє користувачам отримувати доступ до контенту, навіть якщо вони втратили зв'язок з мережею. Це може бути особливо корисним для веб-сайтів або додатків, які надають важливу інформацію, доступ до якої може бути критичним навіть в умовах обмеженого зв'язку з Інтернетом.

Коротко щодо технології **Content Delivery Network.** CDN складається з мережі серверів, розташованих у різних частинах світу. Ці сервери можуть належати різним компаніям, які спеціалізуються на наданні послуг CDN. Ось кілька провідних компаній, які надають послуги CDN:
Akamai Technologies має одну з найбільших мереж CDN у світі. Вони надають послуги CDN для різних клієнтів, включаючи великі компанії, які потребують швидкої доставки контенту до своїх користувачів.
Cloudflare також пропонує широкий спектр послуг CDN, включаючи захист від DDoS-атак та інші додаткові функції безпеки.
Amazon Web Services (AWS) CloudFront. Amazon, має власну службу CDN під назвою CloudFront, яка інтегрується з іншими послугами AWS та надає швидку доставку контенту для веб-сайтів та додатків.
Google Cloud CDN. Google також пропонує свою службу CDN, яка інтегрується з іншими послугами Google Cloud і забезпечує швидку доставку контенту для користувачів.
Ці компанії розгортають свої сервери CDN у різних місцях світу, використовуючи глобальні мережі дата-центрів. Вони також відповідають за адміністрування та підтримку цих серверів, включаючи їхню конфігурацію, моніторинг, оновлення та захист від атак. Необхідно відмітити основні переваги використання CDN:

- **Розподілення навантаження.** розподіляє запити на контент між різними серверами, розташованими у різних географічних регіонах. Це дозволяє зменшити навантаження на один сервер та забезпечити більш стабільну роботу мережі, оскільки навантаження рівномірно розподіляється.
- **Кешування контенту.** Зберігає копії веб-сайтів та іншого контенту на своїх серверах. Коли користувач робить запит до веб-сайту, CDN може надати контент з сервера, який знаходиться найближче до користувача географічно. Це дозволяє зменшити час завантаження сторінок та покращити швидкість відгуку веб-сайту.
- **Зменшення відстані.** Оскільки CDN має сервери в різних частинах світу, вона допомагає скоротити фізичну відстань між сервером та кінцевим користувачем. Це зменшує затримку (латентність) при передачі даних і покращує швидкість завантаження контенту.
- **Захист від DDoS-атак.** CDN має захист від DDoS-атак, який допомагає уникнути перевантаження серверів та зберегти стабільність мережі у разі масштабних атак.

Оптимізація маршрутизації	Передбачає вибір та налаштування найкращих шляхів для передачі даних від відправника до отримувача. Забезпечує найкращий шлях для передачі даних, зменшуючи затримки та забезпечуючи стабільність шляху.	✓ **Ефективні протоколи маршрутизації**. Використання протоколів маршрутизації, таких як OSPF (Open Shortest Path First) - протокол динамічної маршрутизації , заснований на технології відстеження стану каналу (link-state technology) для знаходження найкоротшого шляху, або BGP (Border Gateway Protocol) - протокол динамічної маршрутизації, що належить до класу протоколів маршрутизації зовнішнього шлюзу, для забезпечення оптимальних маршрутів. ✓ **Динамічна адаптація**. Здатність системи адаптуватися до змін у мережевій топології, автоматично вибираючи оптимальні маршрути.

Стратегії оптимізації для забезпечення стабільності та швидкодії мережі спрямовані на покращення ефективності та продуктивності мережі, забезпечуючи стабільність та швидкодію в обслуговуванні користувачів та оптимізації бізнес-процесів.

Роль мережевого моніторингу в виявленні проблем.

Системи моніторингу та їхні можливості:
Ми чудово пам’ятаємо узагальнене визначення систем моніторингу - систем моніторингу представляють собою комплекс програмних та апаратних засобів, спрямованих на збір, аналіз та візуалізацію даних щодо стану мережі.

- Згадаємо **можливості систем моніторингу**:

  ✓ **Реальний час**. Здатність спостерігати за подіями в режимі реального часу, що дозволяє оперативно реагувати на неполадки.
  ✓ **Логування та архівація**. Збереження інформації про минулі події для подальшого аналізу та виявлення закономірностей.
  ✓ **Візуалізація**. Подання даних у зручній формі, що полегшує розуміння стану мережі.
  ✓ **Сповіщення та тривоги**. Автоматизоване сповіщення про аномалії чи небезпеку для оперативного реагування.

Переваги використання метрик для виявлення аномалій:

Метрики у мережевому моніторингу представляють числові показники, що вимірюють різні аспекти роботи мережі, такі як пропускна здатність, затримка, втрати пакетів тощо.

- Згадаємо **переваги використання метрик**:

  - ✓ **Раннє виявлення проблем**. Метрики надають можливість визначити зміни в стані мережі ще до того, як користувачі відчують наслідки.
  - ✓ **Об'єктивність**. Використання кількісних метрик дозволяє об'єктивно визначити рівень продуктивності та ідентифікувати аномалії.
  - ✓ **Тренди та аналіз**. Збір та аналіз метрик протягом тривалого періоду дозволяє виявляти тренди та передбачати можливі проблеми.

- А тепер - **приклади метрик для виявлення аномалій**:

  - ✓ **Кількість втрачених пакетів**. Зростання цієї метрики може свідчити про проблеми з надійністю мережі.
  - ✓ **Затримка (Latency)**. Великі затримки можуть вказувати на проблеми у мережевих шляхах чи обладнанні.
  - ✓ **Використання пропускної здатності**. Забігання до пікових значень може призвести до перевантаження та погіршення швидкодії.

Мережевий моніторинг, з використанням систем та метрик, дозволяє ефективно виявляти та аналізувати аномалії у мережі, покращуючи її стабільність та швидкодію.

Виявлення типових проблем через мережевий моніторинг

- **Відмови обладнання та перевантаження мережі** можуть призвести до втрати доступу до ресурсів, зниження продуктивності та незадовільного користування мережевими послугами.
  Виявлення відмов обладнання через мережевий моніторинг виконуються за допомогою:
  - ✓ **Метрики пропускної здатності** - загальне зменшення пропускної здатності може свідчити про перевантаження.
  - ✓ **Втрати пакетів**. Збільшення втрат пакетів може бути індикатором проблеми на рівні обладнання.

  Дії для виправлення:
  - ✓ **Масштабування ресурсів**. Збільшення обладнання чи оптимізація його роботи для уникнення відмов**.**
  - ✓ **Моніторинг завантаження**. Систематичне вивчення пропускної здатності та завантаження обладнання для передбачення можливих проблем.

- **Мережеві конфлікти та невірна конфігурація** можуть призводити до втрати з'єднання, помилок у передачі даних та порушень безпеки.
  Виявлення через мережевий моніторинг:
  - ✓ **Логи та журнали**. Зафіксовані помилки, невдалі спроби з'єднання чи зміни у конфігурації вказують на можливі конфлікти чи помилки.
  - ✓ **Метрика втрат пакетів**. Збільшення втрат пакетів може бути пов'язано з конфліктами мережевих адрес або проблемами конфігурації.

  Дії для виправлення:
  - ✓ **Аудит конфігурації**. Регулярне перевіряння конфігурації пристроїв для виявлення можливих конфліктів.
  - ✓ **Використання інструментів вирішення конфліктів**, які виявляють та вирішують конфлікти мережевих адрес та інші конфліктні ситуації.

Стратегії усунення проблем та відновлення роботи мережі

Таблиця 03.03

Автоматизовані засоби виявлення та реагування.	**Планування та впровадження патчів та оновлень.**
Використання систем автоматизованого моніторингу для постійного відстеження стану мережі та виявлення аномалій.	Регулярне планування та визначення необхідних оновлень та патчів для всієї мережевої інфраструктури.
Встановлення автоматичних заходів реагування на виявлені аномалії без необхідності втручання адміністратора.	Систематичне виконання процесу впровадження оновлень та патчів, забезпечуючи безпеку та ефективність мережі.
Переваги: ✓ **Швидке реагування**. Автоматизовані системи негайно виявляють проблеми та вживають заходів для їх усунення. ✓ **Мінімізація людського фактору**. Зменшення можливості помилок, пов'язаних з людським втручанням, завдяки автоматизації.	**Переваги**: ✓ **Закриття вразливостей**. Вчасне впровадження оновлень та патчів дозволяє закривати вразливості та запобігати атакам. ✓ **Покращення функціональності**. Оновлення можуть також включати нові функції та покращення, що поліпшують роботу мережі.
Приклади автоматизованих засобів: ✓ **SNMP-моніторинг**. Використання SNMP (Simple Network Management Protocol) для автоматичного моніторингу та керування мережевим обладнанням. ✓ **Системи автоматизованого виявлення інцидентів**. Використання SIEM (Security Information and Event Management) для виявлення та реагування на інциденти безпеки.	**Дії для виправлення**: ✓ **Розробка графіка оновлень**. Створення графіка для визначення регулярності та порядку впровадження оновлень. ✓ **Тестування перед впровадженням**. Перевірка оновлень на тестових системах перед їх впровадженням в продакшен-середовище.

Обидві стратегії спрямовані на забезпечення ефективного усунення проблем та відновлення роботи мережі, зменшуючи вплив негативних факторів на її стабільність та безпеку.

Забезпечення безпеки мережі

Виконується ефективним виявленням та реагуванням на атаки та вразливості в мережі.

Таблиця 03.04

• **Виявлення атак та вразливостей.**	• **Моніторинг потоків даних для виявлення ненормативної активності.**

Встановлення систем виявлення вторгнень (IDS) та систем виявлення аномальної поведінки (AD) для постійного моніторингу та виявлення незвичайних подій у мережі.	Встановлення систем, які аналізують об'єм та напрямок мережевого трафіку для виявлення ненормативної чи підозрілої активності.
Проведення регулярних сканувань вразливостей для виявлення слабких місць у мережевій інфраструктурі та програмних засобах.	Спостереження за змінами у поведінці мережі, що може вказувати на можливі загрози чи атаки.
Переваги: ✓ **Раннє виявлення загроз**. Системи виявлення дозволяють реагувати на потенційні загрози до їх реалізації. ✓ **Моніторинг в реальному часі.** Забезпечення моніторингу та виявлення подій в реальному часі для ефективного реагування на атаки.	**Переваги:** ✓ **Деталізована аналітика.** Можливість виявлення складних та хитрих атак через деталізовану аналітику потоків даних. ✓ **Зменшення помилкових тривог.** Використання аналітичних інструментів для відсіювання помилкових тривог та концентрації на реальних загрозах.
Дії для виправлення: ✓ **Постійне оновлення баз відомостей**. Забезпечення актуальності баз відомостей систем виявлення вторгнень та сканерів вразливостей. ✓ **Аналіз логів.** Регулярний аналіз логів для виявлення аномалій та відстеження потенційно шкідливих дій.	**Дії для виправлення:** ✓ **Впровадження систем аналізу поведінки.** Використання систем, які аналізують не лише сигнатури атак, але й зміни у звичайному поведінці. ✓ **Інтеграція з системами виявлення вторгнень.** Спільна робота систем аналізу потоків та систем виявлення вторгнень для комплексного захисту.

Основні завдання та вимоги до мережевого моніторингу

включають в себе:

Таблиця 03.05

Відстеження трафіку та ресурсів	✓ **Моніторинг використання мережевих ресурсів.** Вимірювання пропускної здатності, визначення використання широкосмугових каналів, ідентифікація основних джерел трафіку. ✓ **Аналіз трафіку для оптимізації пропускної спроможності**. Виявлення надмірної або неефективної використання мережевих ресурсів.
Виявлення та вирішення проблем	✓ **Автоматизоване виявлення несправностей**. Моніторинг для виявлення неполадок в роботі мережі, таких як відмови обладнання чи проблеми зі з'єднанням. ✓ **Швидке реагування на виникнення проблем**. Автоматичні повідомлення та сповіщення про невірну роботу чи зміни у стані мережі.
Моніторинг безпеки мережі	✓ **Виявлення атак та вразливостей**. Аналіз трафіку для ідентифікації можливих атак або вразливостей в системі. ✓ **Моніторинг потоків даних для виявлення ненормативної активності**. Визначення аномальної чи підозрілої активності у мережі.
Забезпечення високої доступності	✓ **Виявлення та усунення відмов**. Визначення можливих точок відмов та розробка стратегій для уникнення або усунення їхніх наслідків. ✓ **Моніторинг навантаження**. Визначення пікового навантаження та планування резервних ресурсів для запобігання перевантаженням.
Забезпечення відповідності до вимог і стандартів	✓ **Збір та аналіз даних для відповідності нормативам**. Використання мережевого моніторингу для перевірки відповідності безпековим стандартам та регулятивам. ✓ **Архівація та зберігання даних**. Забезпечення збереження даних моніторингу для подальшого аналізу та вирішення можливих питань безпеки чи відповідності.

Загальна мета мережевого моніторингу полягає в забезпеченні стабільності, безпеки та ефективності мережевої інфраструктури, а також в оперативному реагуванні на будь-які проблеми чи загрози.

Системи моніторингу трафіку

Існують як програмні так і апаратні рішення:

Таблиця 03.06

	Найбільш відомий приклад програмного рішення моніторингу трафіку - **Wireshark**: **Wireshark** є відкритим програмним інструментом для аналізу мережевого трафіку. Він дозволяє захоплювати та аналізувати пакети даних у реальному часі. Можливості: ✓ Детальний аналіз пакетів, включаючи дані кожного рівня мережевого стеку. ✓ Фільтрація та пошук пакетів за різними критеріями. ✓ Підтримка різних протоколів, включаючи TCP, UDP, IP, ICMP та інші.

	Приклад апаратного рішення моніторингу трафіку - **Cisco NetFlow**: **Cisco NetFlow** є апаратним засобом, розробленим для пристроїв Cisco. Можливості: ✓ Захоплення та аналіз метаданих про трафік для статистики та аналізу. ✓ Визначення трафіку за допомогою різних параметрів, таких як IP-адреси, порти, протоколи тощо. ✓ Моніторинг трафіку в режимі реального часу та створення звітів.
	Аналізатор пакетів **SolarWinds Network Performance Monitor (NPM)**: **SolarWinds NPM** є програмним рішенням для моніторингу та аналізу мережевого трафіку. Можливості: ✓ Аналіз пропускної здатності мережі та виявлення проблем у її роботі. ✓ Моніторинг трафіку на різних рівнях, включаючи рівні додатків та користувачів. ✓ Сповіщення про аномалії та відстеження статистики.
	Аналізатор пакетів **PRTG Network Monitor**: **PRTG** є програмним рішенням для моніторингу та аналізу мережевого трафіку. Можливості: ✓ Захоплення та аналіз пакетів даних для виявлення аномалій. ✓ Моніторинг пропускної здатності та визначення завантаження мережі. ✓ Створення звітів та графіків для аналізу та вивчення тенденцій.

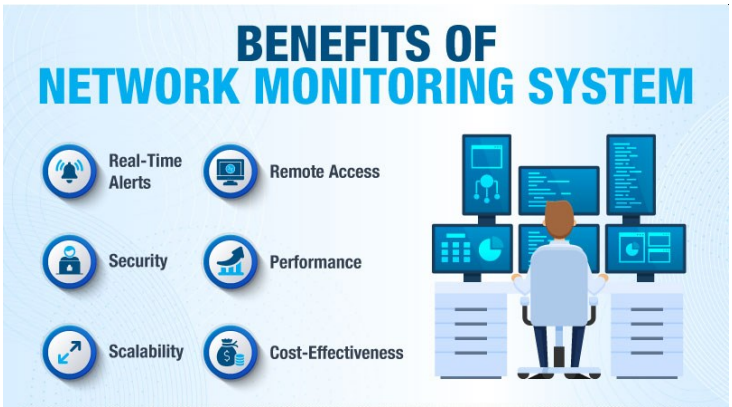
Обидва типи рішень (програмні та апаратні) та аналізатори пакетів надають адміністраторам мережі можливості ефективно моніторити трафік, виявляти аномалії та розуміти, як використовується мережева інфраструктура.

Системи моніторингу мережі (NMS)

Системи моніторингу мережі (Network Monitoring System) призначені для моніторингу та аналізу мережевого трафіку. Вони забезпечують видимість у реальному часі продуктивності мережі та подій безпеки. Рішення NMS дозволяють організаціям визначати потенційні загрози та вразливі місця, перш ніж впливати на їхні мережі.

Рішення для моніторингу мережі надає інформацію про стан мережі в будь-який момент часу. Це допомагає NA виявляти такі проблеми, як сповільнення або збої. Крім того, це дозволяє їм вжити заходів для вирішення проблем, перш ніж вони завдадуть шкоди.

Переваги системи моніторингу мережі (NMS):



- Сповіщення в режимі реального часу. Миттєве сповіщення, коли щось піде не так.
- Віддалений доступ. Перевірка стану мережі з будь-якої точки світу.
- Безпека. Відстеження, що роблять користувачі у вашій мережі.
- Продуктивність. Відстежувати, наскільки швидко працює мережа.
- Масштабованість. Додавання хостів до мережі, не вимагає зусиль про масштабованості.
- Економічна ефективність. Не доведеться купувати кілька одиниць обладнання, бо використовується завжди одне ядро системи.

Вище наведено лише деякі переваги системи керування мережею, а кожне конкретне програмне забезпечення керування мережею має багато інших переваг. У таблиці нижче наведено програмні NMS

Програмні рішення для мережевого моніторингу

Таблиця 03.07

	Назва	Тип	Функціональність
Nagios	Nagios Core	Відкрита платформа	✓ Моніторинг доступності та продуктивності пристроїв та сервісів. ✓ Сповіщення про аномалії та генерація звітів. ✓ Розширена система плагінів для різноманітності моніторингу.
ZABBIX	Zabbix	Відкрита платформа	✓ Моніторинг різноманітних пристроїв та служб за допомогою агентів. ✓ Збір та аналіз лог-файлів та статистики. ✓ Автоматичне виявлення пристроїв у мережі та їх параметрів.
PRTG NETWORK MONITOR	PRTG Network Monitor	Комерційна платформа	✓ Спостереження за станом пристроїв, здатності мережі та роботи служб. ✓ Моніторинг ресурсів, таких як CPU, пам'ять та диски. ✓ Аналіз мережевого трафіку та інформації про пропускну здатність.
NPM	SolarWinds Network Performance Monitor (NPM)	Комерційна платформа	✓ Моніторинг пропускної здатності та виявлення аномалій. ✓ Аналіз даних на різних рівнях, включаючи додаткові рівні та користувачів. ✓ Система оповіщень та генерація звітів для аналізу та прогнозування.
dynatrace	Dynatrace	Комерційна платформа	✓ Моніторинг реального часу та аналіз роботи додатків та сервісів. ✓ Виявлення та діагностика аномалій у роботі програмного забезпечення. ✓ Аналіз взаємодії між компонентами додатків та їх взаємозалежності.
zenoss	Zenoss	Відкрита платформа	✓ Моніторинг доступності та продуктивності мережевих пристроїв. ✓ Автоматизована інвентаризація мережевого обладнання. ✓ Аналіз та візуалізація даних зібраних з різних джерел.
CACTI	Cacti	Відкрита платформа	✓ Графічне відображення статистики мережевого трафіку. ✓ Моніторинг системних параметрів пристроїв. ✓ Створення власних шаблонів для моніторингу.
MUNIN	Munin	Відкрита платформа	✓ Автоматичне створення графіків для моніторингу різних параметрів. ✓ Простий інтерфейс для відслідковування змін в мережі. ✓ Повідомлення про аномалії та невідповідності.
	Prometheus	Відкрита платформа	✓ Моніторинг метрик з різних компонентів мережевої інфраструктури. ✓ Збір, візуалізація та аналіз даних. ✓ Підтримка реєстрів відкритих метрик (OpenMetrics).
sematext	Sematext Monitoring	Комерційна платформа	✓ Аналіз продуктивності та доступності пристроїв. ✓ Моніторинг додатків та інфраструктури в хмарних середовищах. ✓ Автоматизовані оповіщення та аналітика.
	The Dude from Mikrotik	Відкрита платформа	✓ Мапування мережі та відслідковування пристроїв. ✓ Моніторинг доступності та стану мережевих об'єктів. ✓ Візуалізація та аналіз трафіку.

Переваги використання сучасних технологій у мережевому моніторингу

Відношення до автоматизації мережевого моніторингу за допомогою штучного інтелекту.

- **Позитивні аспекти:**
  - **Ефективність.** Штучний інтелект може виявити аномалії в мережі навіть тоді, коли вони неочікувані або важко визначити за допомогою традиційних методів.
  - **Швидкість.** Автоматизовані системи штучного інтелекту можуть виявляти та реагувати на проблеми в реальному часі, що дозволяє швидше вирішувати проблеми.

- **Виклики та обмеження:**
  - **Навчання.** Штучний інтелект вимагає навчання на великих обсягах даних, а для деяких аспектів мережевого моніторингу може бути складно забезпечити достатньо великий та репрезентативний набір даних.
  - **Безпека.** Використання штучного інтелекту у мережевому моніторингу може викликати питання щодо безпеки та конфіденційності даних.

- **Роль ШІ у виявленні аномалій:**
  - **Аналіз великих обсягів даних**. Штучний інтелект може ефективно аналізувати великі обсяги мережевих даних та виявляти аномалії за короткий час.
  - **Моделювання поведінки.** Використання алгоритмів машинного навчання для створення моделей поведінки мережі та виявлення відхилень від звичайного.

Можливість автоматизації вирішення проблем за допомогою ШІ.

- **Автоматичні реакції.** На основі виявлених аномалій система штучного інтелекту може виробляти автоматичні реакції, такі як вимкнення атакуючого пристрою або переналаштування мережевих параметрів.
- **Оптимізація.** Штучний інтелект може автоматично оптимізувати роботу мережі, реагуючи на зміни у завантаженості чи інших умовах.

Існують численні успішні практичні реалізації використання штучного інтелекту в мережевому моніторингу та виявленні аномалій. Деякі приклади включають:

Таблиця 03.08

Приклад	Опис	Результати
Cisco Stealthwatch	Використовує аналіз мережевого трафіку, машинне навчання та штучний інтелект для виявлення аномалій у мережі та потенційних загроз безпеці.	Покращена виявлення загроз та зниження часу реакції на інциденти.
Darktrace	Використовує технологію машинного навчання для неперервного моніторингу мережі та виявлення аномальної активності.	Виявлення ранніх стадій атак та аномалій, що допомагає у запобіганні серйозним кіберзагрозам.
Splunk IT Service Intelligence (ITSI)	Використовує аналітику та машинне навчання для агрегації даних з різних джерел та виявлення аномалій в мережевому середовищі.	Покращена обізнаність про мережеві події та їх вплив на бізнес-процеси.
IBM QRadar	Використовує аналіз поведінки, машинне навчання та алгоритми виявлення аномалій для моніторингу мережі та виявлення потенційних загроз.	Ефективне виявлення та відправлення сповіщень про можливі загрози для швидкого реагування.

Ці платформи та рішення служать прикладами успішних використань штучного інтелекту в мережевому моніторингу, де вони допомагають виявляти аномалії, забезпечують захист від загроз та підвищують загальну безпеку мережевих інфраструктур. Зауважте, що дані практики можуть змінюватися з часом, і рекомендується перевіряти найновіші відомості.

Автоматизовані засоби вирішення проблем у мережевому моніторингу

Давайте розглянемо кілька **категорій автоматизованих засобів вирішення проблем у мережевому моніторингу** та їхні приклади.

Таблиця 03.09

Категорія АЗ	Призначення	Проблеми, що вирішують	Автоматизація	Розробники
Системи автоматичного виявлення та реагування (IDS/IPS)	IDS: система виявлення інтрузій (Intrusion Detection System) призначена для виявлення незвичайної або підозрілої активності в мережі або на окремих комп'ютерах. IPS: система запобігання інтрузіям (Intrusion Prevention System) вживає заходів для запобігання атакам або інтрузіям, включаючи блокування атакуючого трафіку чи інші заходи безпеки.	Виявлення та запобігання кіберзагрозам, таким як атаки на мережевий периметр або невірна конфігурація систем безпеки.	IDS виявляє аномалії та потенційні загрози в мережі. IPS реагує на виявлені загрози, блокуючи атакуючий трафік або іншим чином запобігаючи невірній активності.	Різні компанії надають IDS/IPS-рішення. Наприклад, Snort є відкритим рішенням, а Cisco, Palo Alto Networks, Check Point та Fortinet пропонують комерційні IDS/IPS-продукти у своїх сімействах мережевих засобів безпеки.
Системи автоматизованого виявлення та відновлення (AIDR)	Automated Incident Detection and Response, як зрозуміло з назви☺, використовується для автоматизованого виявлення випадків відмов у роботі та відновлення роботи мережевих компонентів.	Виявлення та відновлення випадків відмов у роботі апаратного забезпечення або мережевих служб.	AIDR автоматично виявляє аномалії у роботі мережевих елементів та відновлює роботу шляхом переключення на резервні мережеві шляхи або використання інших резервних ресурсів.	AIDR може представляти собою внутрішній розвиток конкретної організації або може бути продуктом від різних постачальників. Зазвичай, це спеціалізовані рішення в галузі кібербезпеки, але точний розробник може різнитися.
Системи автоматизованого моніторингу пропускної здатності (NPM)	Network Performance Monitoring використовується для моніторингу та аналізу пропускної здатності мережі, виявлення недоліків та оптимізації її роботи.	Виявлення недоліків у пропускній здатності мережі та планування її оптимізації.	Системи NPM автоматично моніторять пропускну здатність, виявляючи місця заторів або недоліки, і можуть надавати рекомендації з оптимізації.	Існує багато різних NPM-рішень, які можуть бути відкритими чи комерційними. Деякі популярні рішення включають SolarWinds Network Performance Monitor, PRTG Network Monitor, Cisco Prime Infrastructure та інші.
Системи автоматичного реагування на аномалії мережі	Концепція систем автоматичного виявлення та реагування на аномалії включає в себе використання різних технологій та підходів, таких як аналіз поведінки мережі, машинне навчання, алгоритми виявлення аномалій, та автоматизовані процеси реагування на виявлені проблеми.	Виявлення та реагування на аномалії в роботі мережі, такі як зміни у поведінці пристроїв чи несподівані великі навантаження.	Автоматизовані системи аналізують дані з пристроїв та мережі, виявляють аномалії та можуть автоматично виконувати відповідні заходи, такі як зміна конфігурації чи резервне планування мережі.	Конкретних розробників чи продуктів, які однозначно відповідають цій назві, може бути кілька. Також варто відзначити, що іноді під "системою автоматичного реагування на аномалії" може розумітися певна конфігурація різних продуктів для виявлення та вирішення аномалій, а не самостійний продукт.
Системи автоматичної зміни конфігурацій (NCCM)	Network Configuration and Change Management відповідає за зберігання, відслідковування та автоматизоване управління змінами конфігурацій мережевих	Виявлення та усунення проблем, пов'язаних з невірною конфігурацією	NCCM виявляє невірні або небезпечні конфігурації та може автоматично виконувати зміни для	Деякі компанії, що спеціалізуються в управлінні мережевою конфігурацією, включають SolarWinds NCM (Network Configuration

	пристроїв для забезпечення стабільності та безпеки мережі.	мережевих пристроїв.	відновлення стабільності та безпеки мережі.	Manager), Cisco Prime Infrastructure, Infoblox NetMRI та інші.

Хоча автоматизовані засоби вирішують багато проблем, в деяких випадках важливо залучити адміністраторів мережі (NA) або інших фахівців для вирішення складних проблем, які можуть вимагати аналізу глибокого рівня або врахування специфічних деталей конфігурацій.

Висновки.

Мережевий моніторинг є ключовим елементом сучасних мережевих інфраструктур, надаючи організаціям засоби для ефективного управління, забезпечення безпеки та оптимізації роботи мережі. У цій лекції ми розглянули основні аспекти та важливість мережевого моніторингу.

Мережевий моніторинг значно впливає на забезпечення стабільності, безпеки та ефективності мережевих інфраструктур та дозволяє операторам отримувати цінні дані про стан мережі для прийняття обґрунтованих рішень та вчасного виявлення аномалій.

Завдання мережевого моніторингу включають в себе виявлення аномалій, оптимізацію пропускної здатності, забезпечення безпеки та вчасну реакцію на проблеми. Вимоги полягають у високій точності, швидкодії та масштабованості систем моніторингу.

Ми згадали різноманітні засоби та технології, такі як SNMP, флейви (sFlow, NetFlow), аналізатори пакетів, системи виявлення і запобігання інтрузіям (IDS/IPS) та інші, які використовуються для збору різноманітних мережевих даних.

Загальною тенденцією є постійний розвиток та вдосконалення засобів моніторингу для відповіді на розширені потреби сучасних мережевих інфраструктур. Мережевий моніторинг є критичним елементом для забезпечення продуктивності та безпеки мережі в умовах стрімкого технологічного розвитку.