УДК 004.738

Ференз А.Р., магістрант,
Фальковський І.Г., ст. викладач
Державний університет «Житомирська політехніка»

ОГЛЯД МЕРЕЖЕВИХ ПРОТОКОЛІВ, ЩО ВИКОРИСТОВУЮТЬСЯ ДЛЯ МОНІТОРИНГУ

Ефективний моніторинг мережевої інфраструктури забезпечується спеціалізованими протоколами, які дозволяють збирати дані про стан пристроїв, продуктивність і безпеку мережі. Їхнє комбіноване використання забезпечує комплексний підхід до управління мережею, дозволяючи виявляти несправності, оптимізувати трафік і підвищувати безпеку.

1) Ping – базовий метод активного моніторингу, що використовує протокол ICMP. Система надсилає Echo Request і очікує Echo Reply, перевіряючи доступність пристрою та вимірюючи затримку з'єднання. Простота та вбудованість у більшість операційних систем роблять Ping основним інструментом для генерації аварійних сповіщень.

2) SNMP (Simple Network Management Protocol) – широко використовуваний протокол для активного (GET-запити) та пасивного (traps, informs) моніторингу. Існують три версії SNMP:

- SNMP v1 (1988): базова версія з обмеженою функціональністю та слабкою безпекою (автентифікація через community string).
- SNMP v2c (1993): покращена продуктивність, підтримка 64-бітних лічильників, але без змін у безпеці.
- SNMP v3 (2002): додано шифрування, автентифікацію користувачів і контроль доступу, що значно підвищило безпеку.

3) Syslog, стандартизований у RFC 5424, передає текстові лог-повідомлення через UDP до центрального сервера. Повідомлення містять Facility, Severity та опис події (наприклад, помилки чи зміни конфігурації). Централізоване зберігання логів полегшує аналіз подій і діагностику проблем, хоча доставка не гарантується.

4) Протоколи мережевих потоків (NetFlow, sFlow, IPFIX) призначені для збору даних про IP-потоки для подальшого аналізу трафіку та безпеки.

- NetFlow: розроблений Cisco, забезпечує детальний збір даних про мережеві потоки, фіксуючи такі параметри, як IP-адреси джерела та призначення, порти, протоколи, обсяг трафіку та часові мітки. NetFlow v9 розширює можливості завдяки підтримці IPv6, MPLS і гнучких шаблонів. Є пропрієтарним протоколом.

- sFlow: застосовує вибірковий підхід (sampling), відбираючи зразки пакетів і даних інтерфейсів, що значно знижує навантаження на мережеве обладнання порівняно з NetFlow. Це робить sFlow ідеальним для моніторингу великих і високонавантажених мереж. Однак через вибірковий характер збору даних деталізація інформації нижча, що може обмежувати точність аналізу. Є відкритим стандартом.
- IPFIX: стандартизована IETF еволюція NetFlow (на основі NetFlow v9), вирізняється гнучкістю та адаптивністю завдяки підтримці кастомних шаблонів для збору даних. Це дозволяє налаштовувати протокол для специфічних потреб, що робить його універсальним для сучасних мереж, включаючи хмарні та SDN-середовища.

5) Cisco Discovery Protocol (CDP) та Link Layer Discovery Protocol (LLDP). CDP – пропрієтарний протокол Cisco, який виявляє сусідні пристрої, надаючи дані про ідентифікатор, IP-адресу, тип і модель обладнання, версію ПЗ, активні інтерфейси, VLAN та споживання енергії в PoE-середовищах. LLDP – відкритий стандарт, що працює на канальному рівні, сумісний із пристроями різних виробників. Він передає дані про тип пристрою, порт, VLAN ID і адреси управління. Використання LLDP ідеально підходить для гетерогенних мереж.

6) WMI (Windows Management Instrumentation (WMI) – це інструмент Microsoft для моніторингу та управління Windows-системами. Він дозволяє отримувати дані про стан операційної системи, апаратного забезпечення та програм через простий інтерфейс. WMI підтримує автоматизацію завдань (наприклад, моніторинг диска чи налаштування мережі), централізоване управління через єдину консоль, інтеграцію з PowerShell і System Center, а також забезпечує захист даних завдяки вбудованим механізмам безпеки.

В доповіді буде представлено огляд вищезгаданих мережевих протоколів для моніторингу з акцентом на їхні особливості, переваги та сфери застосування.

Список використаних джерел:

1. Ultimate Guide to Network Monitoring? URL: https://www.dnsstuff.com/network-monitoring
2. Types of Network Management Protocols. URL: https://www.liveaction.com/resources/blog-post/types-of-network-management-protocols/
3. Network Monitoring Protocols. URL: https://www.kentik.com/kentipedia/network-monitoring-protocols/