

MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

**Universitatea Tehnică a Moldovei
Facultatea Electronică și Telecomunicații
Departamentul Telecomunicații și Sisteme Electronice**

**Admis la susținere
Șefă departament TSE:
Tîrșu Valentina, conf.univ.dr.**

„_____” _____ 2025

Soluții de monitorizare a rețelelor enterprise cu SNMP pe echipamente Cisco și Juniper

Teză de master

Student:

**Țurcan Mihai, SISRC-
231M**

Conducător:

**Țurcanu Tatiana,
conf.univ.dr.**

Chișinău, 2025

REZUMAT

La teza de master

Tema tezei “Soluții de monitorizare a rețelelor enterprise cu SNMP pe echipamente Cisco și Juniper”

Actualitatea și importanța temei. Teza de master își propune să analizeze și să implementeze soluții de monitorizare pentru rețelele enterprise utilizând protocolul SNMP pe echipamente Cisco și Juniper. Lucrarea abordează aspecte teoretice și practice, subliniind relevanța utilizării SNMP pentru administrarea eficientă a resurselor și optimizarea performanței rețelelor.

Într-un context tehnologic caracterizat de creșterea complexității infrastructurilor IT și de cerințe ridicate pentru performanță și securitate, monitorizarea rețelelor a devenit esențială. SNMP, un protocol standardizat, permite colectarea și analizarea datelor critice despre echipamentele de rețea.

Cuvinte-cheie: SNMP (Simple Network Management Protocol), Cisco, Juniper, monitorizare rețele, securitate rețele, optimizare performanță.

Scopul tezei. Lucrarea urmărește să prezinte soluții eficiente pentru monitorizarea rețelelor enterprise prin configurarea și utilizarea SNMP pe echipamente Cisco și Juniper. De asemenea, teza propune să compare soluțiile open-source și comerciale, să dezvolte scripturi personalizate pentru monitorizare și să identifice metode de optimizare a performanței rețelelor.

Obiectivele tezei sunt - studierea funcționalităților SNMP și a specificațiilor echipamentelor Cisco și Juniper, configurarea SNMP pentru monitorizarea parametrilor critici ai rețelelor, la fel și compararea avantajelor și dezavantajelor soluțiilor de monitorizare open-source și comerciale. Totodată ca obiective sunt crearea și testarea scripturilor pentru automatizarea proceselor de monitorizare cum și optimizarea performanței rețelelor pe baza datelor colectate.

Rezultate obținute în urma elaborării tezei sunt:

- Configurarea SNMPv2c și SNMPv3 pentru securitate și fiabilitate.
- Implementarea soluțiilor open-source precum Zabbix și Nagios și evaluarea soluțiilor comerciale precum SolarWinds și PRTG.
- Dezvoltarea și utilizarea de scripturi Python pentru extragerea și analiza datelor SNMP.
- Testarea performanței rețelelor și propunerea de îmbunătățiri ale configurațiilor.

Valoarea practică. Rezultatele obținute contribuie la înțelegerea și aplicarea unor metode moderne de monitorizare a rețelelor enterprise, oferind soluții eficiente și scalabile pentru administrarea resurselor critice. Lucrarea are aplicabilitate directă în infrastructurile IT complexe, sprijinind deciziile de optimizare și securizare a rețelelor.

SUMMARY

In the master's thesis

Topic “Enterprise network monitoring solutions with SNMP on Cisco and Juniper equipment”

Timeliness and importance of the topic. The master's thesis aims to analyze and implement monitoring solutions for enterprise networks using the SNMP protocol on Cisco and Juniper equipment. The paper addresses theoretical and practical aspects, emphasizing the relevance of using SNMP for efficient resource management and optimizing network performance.

In a technological context characterized by the increasing complexity of IT infrastructures and high requirements for performance and security, network monitoring has become essential. SNMP, a standardized protocol, allows the collection and analysis of critical data about network equipment.

Keywords: SNMP (Simple Network Management Protocol), Cisco, Juniper, network monitoring, network security, performance optimization.

Thesis purpose. The paper aims to present effective solutions for monitoring enterprise networks by configuring and using SNMP on Cisco and Juniper equipment. The thesis also proposes to compare open-source and commercial solutions, develop custom scripts for monitoring, and identify methods for optimizing network performance.

The objectives of the thesis are - studying the SNMP functionalities and specifications of Cisco and Juniper equipment, configuring SNMP for monitoring critical network parameters, as well as comparing the advantages and disadvantages of open-source and commercial monitoring solutions. At the same time, the objectives are to create and test scripts for automating monitoring processes as well as optimizing network performance based on the collected data.

Results obtained from the thesis are:

- Configuring SNMPv2c and SNMPv3 for security and reliability.
- Implementing open-source solutions such as Zabbix and Nagios and evaluating commercial solutions such as SolarWinds and PRTG.
- Developing and using Python scripts for extracting and analyzing SNMP data.
- Testing network performance and proposing configuration improvements.

Practical value. The results obtained contribute to the understanding and application of modern methods for monitoring enterprise networks, providing efficient and scalable solutions for managing critical resources. The work has direct applicability in complex IT infrastructures, supporting network optimization and security decisions.

CUPRINS

INTRODUCERE	7
1 Cadrul teoretic	9
1.1 Contextul monitorizării si conceptul de management al rețelelor enterprise	9
1.2 Protocolul SNMP, monitorizarea rețelelor enterprise cu SNMP	13
1.3 Echipamentele Cisco și Juniper și SNMP	18
1.4 Soluții de monitorizare, beneficii și provocări în monitorizarea cu SNMP a rețelelor Enterprise	24
2 Analiza Soluțiilor de Monitorizare	27
2.1 Cerințe de monitorizare pentru rețele enterprise	27
2.2 Instrumente software de monitorizare: Open Source vs. Comerciale	34
2.3 Implementarea SNMP pe echipamente Cisco și Juniper	47
2.4 Studii de caz și exemple practice	51
3 Cadrul aplicativ și implementarea practică	58
3.1 Configurarea SNMP pe echipamente Cisco	59
3.2 Configurarea SNMP pe echipamente Juniper	63
3.3 Crearea și utilizarea scripturilor de monitorizare	67
3.4 Analiza performanțelor rețelei și optimizarea configurațiilor	70
3.5 Configurarea soluției de monitorizarea pentru echipamentele Cisco și Juniper	74
3.6 Monitorizarea echipamentelor și vizualizarea datelor	86
CONCLUZII ȘI RECOMANDĂRI.....	87
BIBLIOGRAFIE	89

Introducere

Actualitatea și importanța temei. În contextul dezvoltării accelerate a tehnologiilor de comunicații și al complexității crescânde a rețelelor enterprise, monitorizarea eficientă a infrastructurilor IT a devenit un element esențial pentru asigurarea performanței și securității operaționale. În această eră a digitalizării, rețelele nu mai sunt doar canale de transmisie a datelor, ci fundații critice pentru succesul organizațiilor. O monitorizare adecvată asigură nu doar identificarea problemelor, ci și prevenirea lor printr-o gestionare proactivă.

Această lucrare se concentrează pe analiza și implementarea soluțiilor de monitorizare a rețelelor enterprise utilizând protocolul SNMP (Simple Network Management Protocol) pe echipamente Cisco și Juniper. Alegerea acestor echipamente se datorează poziției lor de lideri în industria de rețele, oferind funcționalități avansate și fiabilitate ridicată. Protocolul SNMP, utilizat pe scară largă în administrarea rețelelor, permite colectarea de date despre performanța și starea echipamentelor, oferind administratorilor posibilitatea de a gestiona eficient resursele și de a optimiza configurațiile rețelei.

Într-un mediu globalizat și extrem de competitiv, întreprinderile depind de rețelele lor pentru a susține procesele de afaceri critice. Creșterea volumului de trafic de date, migrarea către cloud și adoptarea Internetului lucrurilor (IoT) impun cerințe suplimentare asupra infrastructurilor IT. În aceste condiții, monitorizarea rețelelor a evoluat de la o activitate opțională la un proces indispensabil pentru a menține performanța optimă și securitatea datelor.

Protocolul SNMP, datorită simplității și eficienței sale, oferă o soluție standardizată pentru monitorizarea și gestionarea rețelelor. Prin utilizarea acestuia, organizațiile pot colecta date detaliate despre utilizarea resurselor, starea echipamentelor și performanța generală a rețelelor. În același timp, echipamentele Cisco și Juniper, cunoscute pentru capacitățile lor avansate și flexibilitatea în integrarea cu soluții software, reprezintă un exemplu ideal pentru aplicarea acestui protocol.

Scopul și obiectivele tezei - este de a evalua și implementa soluții eficiente pentru monitorizarea rețelelor enterprise utilizând SNMP, analizând în același timp performanțele echipamentelor Cisco și Juniper. În vederea atingerii acestui scop, lucrarea și-a propus următoarele obiective:

- Analiza teoretică a protocolului SNMP și a caracteristicilor echipamentelor Cisco și Juniper.
- Configurarea SNMPv2c și SNMPv3 pentru monitorizarea parametrilor critici ai rețelelor.
- Compararea soluțiilor de monitorizare open-source și comerciale pentru identificarea avantajelor și dezavantajelor acestora.

- Dezvoltarea de scripturi pentru automatizarea proceselor de monitorizare și analiza datelor colectate.
- Optimizarea configurațiilor rețelei pe baza datelor colectate și analizate.

Structura tezei

Sumarul compartimentelor tezei. Lucrarea este structurată în trei capitole, fiecare având rolul de a contribui la realizarea scopului propus:

- **Capitolul 1 “CADRUL TEORETIC”** abordează fundamentele teoretice ale protocolului SNMP, detaliind modul său de funcționare, beneficiile și aplicabilitatea acestuia în rețelele enterprise. De asemenea, sunt analizate caracteristicile echipamentelor Cisco și Juniper relevante pentru monitorizare.
- **Capitolul 2 “ANALIZA SOLUȚIILOR DE MONITORIZARE”** oferă o analiză comparativă a soluțiilor de monitorizare existente, incluzând atât soluții open-source (ex. Zabbix, Nagios), cât și soluții comerciale (ex. SolarWinds, PRTG). Sunt prezentate avantajele și limitările fiecărei categorii, precum și criteriile de selecție în funcție de cerințele rețelei.
- **Capitolul 3 “CADRUL APLICATIV ȘI IMPLEMENTAREA PRACTICĂ”** se concentrează pe partea practică a tezei, incluzând configurarea SNMP pe echipamentele Cisco și Juniper, utilizarea scripturilor personalizate pentru monitorizare, analiza datelor colectate și propunerea de soluții pentru optimizarea configurațiilor rețelei.

Valoarea practică a tezei. Această lucrare aduce o contribuție practică semnificativă prin detalierea proceselor de configurare și monitorizare a rețelelor enterprise, demonstrând eficiența utilizării SNMP. Soluțiile propuse pot fi aplicate în infrastructuri reale, sprijinind administratorii de rețea în asigurarea performanței și securității optime.

Teza reprezintă o resursă utilă atât pentru profesioniștii IT, cât și pentru organizațiile care doresc să-și îmbunătățească procesele de monitorizare și management al rețelelor, oferind o perspectivă integrată asupra utilizării SNMP pe echipamentele Cisco și Juniper.

BIBLIOGRAFIE

1. Stallings, W. (1999), *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*, Addison-Wesley.
2. Cisco Systems (2014), *SNMP Configuration Guide, Cisco IOS XE Release 3SE*.
3. Juniper Networks (2021), *SNMPv3 Configuration and Security Features*, Technical Documentation.
4. ȚURCANU, D., SPINU, N., POPOVICI, S., ȚURCANU, T. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. In: *Journal of Social Sciences*. 2021, IV (1), pp. 74–83. [https://doi.org/10.52326/jss.utm.2021.4\(1\).10](https://doi.org/10.52326/jss.utm.2021.4(1).10)
5. Paessler AG (2022), *SNMP Monitoring Basics*, PRTG Network Monitor Documentation.
6. SolarWinds (2021), *Network Performance Monitor: SNMP and Trap Configuration*, SolarWinds Documentation.
7. Juniper Networks (2020), *Juniper SNMP Configuration Overview*, Technical Documentation.
8. Tanenbaum, A. (2010), *Computer Networks*, Prentice Hall.
9. Stallings, W. (2013). *Data and Computer Communications*. Pearson Education.
10. PECA, L., ȚURCANU, D. Network security: Practical examples solved to be introduced in network security. Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Department Software Engineering and Automatics. – Chișinău: Tehnica-UTM, 2023. – 243 p. ISBN 978-9975-45-941-9. <http://repository.utm.md/handle/5014/22819>
11. PECA, L., ȚURCANU, D. Computer networks: Practical examples solved to be introduced in computer networks. Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Department Software Engineering and Automatics. – Chișinău: Tehnica-UTM, 2022. – 188 p. ISBN 978-9975-45-812-2. <http://repository.utm.md/handle/5014/20549>
12. Cisco Systems. (2020). *SNMP Configuration Guide, Cisco IOS Release 15.2*. Cisco Documentation.
13. Mauro, D., & Schmidt, K. (2005). *Essential SNMP*. O'Reilly Media.
14. Juniper Networks. (2020). *SNMP Monitoring on Juniper Devices*. Juniper Documentation.
15. Paessler AG. (2021). *PRTG Network Monitor Documentation*. Paessler Official Website.
16. SolarWinds. (2021). *Network Performance Monitor Documentation*. SolarWinds Official Website.

17. GRIGORESCU, O., BOTEZATU, L., MUTU, A., ȚURCANU, D. Contextual Remediations Prioritization System Designed to Implement Theoretical Principles of CVSS V4. In: University Politehnica of Bucharest scientific bulletin series C-Electrical Engineering and Computer Science. 2024, Volume 86, Issue 3, Page 121-138.
https://www.scientificbulletin.upb.ro/rev_docs_arhiva/rez833_656075.pdf
18. Gammel, B. (2016). *Monitoring and Performance Optimization for Enterprise Networks*. Wiley.
19. Smith, J. (2018). *Network Security Monitoring Using SNMP*. TechPress.
20. Johnson, P. (2020). *Enterprise Network Management and Monitoring Solutions*. TechWorld Publications.
21. BĂLUȚĂ, A., SOARE, R. M., RUGHINIȘ, R., ȚURCANU, D. GeckoNet - Self-Healing SDN Framework. In: 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet). 19-20 September, 2024, Bucharest, Romania.
<https://doi.org/10.1109/RoEduNet64292.2024.10722172>
22. Pinterest, © 2024 [Citat 24.10.2024]. Disponibil:
<https://dk.pinterest.com/pin/849843392153605912/visual-search/?x=16&y=16&w=532&h=457.62637362637366&cropSource=6&surfaceType=flashlight>
23. ScienceDirect, © 2024 Elsevier [Citat 24.10.2024]. Disponibil:
<https://www.sciencedirect.com/topics/computer-science/security-monitoring>
24. Mauro, D., & Schmidt, K. (2005). *Essential SNMP*. O'Reilly Media.
25. Zabbix, © 2001-2024 by Zabbix LLC [Citat 23.12.2024]. Disponibil:
https://www.zabbix.com/download?zabbix=6.0&os_distribution=ubuntu&os_version=24.04&components=server_frontend_agent&db=mysql&ws=apache
26. Tîrșu V., Sava L. Integrating elasticsearch and kibana in ict management *processes for economic efficiency in multimedia content administration*. In: The scientific heritage. Economic Sciences., Vol.1 № 142 (142), 2024, p.15-20 . Budapest, Hungary. ISSN 9215 — 0365, Cosmos Impact Factor - 3.336 SJIF Impact Factor - 5.78 DOI: , Categoria B+. Disponibil: <http://www.scientific-heritage.com/ru/arhiv/>
27. Tîrșu, V. Programare: Ghid metodic pentru lucrări de laborator. Chișinău: Ed. “Tehnica-UTM”, 2022, pag.130, ISBN 978-9975-45-861-0. Disponibil:
<https://library.utm.md/items/?biblionumber=2619626>

28. Sava, L., Vortolomei, D. Organizarea și analiza activității economice în domeniul telecomunicațiilor. Note de curs, Chișinău, Editura UTM, 2022, ISBN: 978-9975-45-805-4.