

SIMPLE NETWORK MANAGMENT

PROTOCOL

(SNMP)

Rezumat:

Proiectul își propune realizarea unui instrument de monitorizare a unei rețele. Soluția propusă se bazează pe protocolul SNMP. Scopul acestui proiect este de a observa, în timp real, starea de funcționare a echipamentelor de comunicație sau a echipamentelor destinate anumitor servicii. Printre lucrurile observabile se enumeră traficul de download și upload, memoria RAM disponibilă, procentul de încărcare al CPU, spațiul liber pe hard disk, dar și alte valori care pot fi exprimate prin unități de măsură (ex: temperatură).

De ce avem nevoie de SNMP?

Nevoia de a monitoriza dispozitivele conectate la rețelele de calculatoare, care creșteau rapid la sfârșitul anilor 1980, a dus la dezvoltarea protocolului SNMP (Simple Network Management Protocol). Scopul principal al acestuia a fost să faciliteze managementul și monitorizarea echipamentelor de rețea, precum routere, switch-uri, servere și alte dispozitive, într-o manieră standardizată și eficientă. SNMP a fost creat pentru a rezolva problemele complexe de administrare a rețelelor, oferind un mod simplu și uniform de a gestiona și controla infrastructura rețelelor de date.

Informațiile obținute prin monitorizare pot fi folosite pentru a determina dacă resursele implicate sunt utilizate corespunzător, pentru a verifica cum lucrează echipamentele care sunt folosite în rețea, a urmări activitatea în cadrul unei rețele și pentru a identifica probleme care apar și de a lua măsurile necesare pentru rezolvarea lor.

Geeky description

SNMP este un protocol, care funcționează la nivelul aplicație al modelului TCP/IP. Acest protocol a apărut din nevoia companiilor de a evita situațiile neplăcute în

care componentele unei rețele să nu funcționeze la parametri optimi.

Majoritatea implementărilor folosesc UDP pentru transferul de mesaje, deoarece este considerat acceptabilă pierderea de pachete în comparație cu funcțiile pe care trebuie să le îndeplinească entitățile administrate.

UDP(User Datagram Protocol) este unul din principalele protocoale de comunicare folosit pentru a trimite mesaje (transmis ca o datagrama sub forma unui pachet de date) catre alte gazde prin intermediul IP network.

Arhitectura protocolului:

SNMP se bazează pe modelul manager / agent, care constă într-un administrator, un agent și o bază de date de management a informațiilor , gestionată de obiecte de protocol și de rețea.

Management Information Base (MIB) reprezintă o bază de date organizată ierarhic, care conține definițiile obiectelor de gestionat în rețea, cum ar fi parametrii de performanță și starea dispozitivelor. Fiecare obiect din MIB este identificat printr-un Object Identifier (OID), un șir unic de numere care permite managerului SNMP să acceseze și să modifice informațiile corespunzătoare agentului, facilitând astfel gestionarea eficientă a resurselor din rețea.

Evolutia SNMP:

❖ SNMPv1

- SNMP versiunea 1 este versiunea inițială a conceptului de SNMP, a fost introdusă pentru a răspunde nevoii de administrare a dispozitivelor ce folosesc protocolul IP.
- Prima versiunea a fost criticată pentru lipsa de securitate. Autentificarea se făcea printrun grup numit community string și era nu era codificată sub nicio formă.

❖ SNMPv2

- SNMPv2, revizuieste prima versiune și aduce îmbunătățiri la performanță, securitate, confidențialitate și comunicarea între manageri. Pe lângă

acestea, versiunea 2 include GetBulkRequest și detalierea mesajelor de eroare raportate către manager. GetBulkRequest suportă aducerea de tabele și cantități mari de date.

❖ **SNMPv3**

- Versiunea a treia nu aduce schimbări, în afară de partea de securitate. Cu toate acestea conține termeni diferiți față de versiunile anterioare.
- Această versiune are o structură modulară, permițând adăugări ușoare, dar și modificări.
- Modificările pe partea de securitate se referă la autentificare, criptare și controlul accesului. Autentificarea permite doar surselor autorizate să genereze cereri SNMP. Acest lucru se realizează prin crearea de cont de utilizator și respectiv a unei parole. Criptarea previne citirea sau modificarea mesajelor SNMP transmise prin rețea, iar controlul accesului la MIB-uri a fost implementat pentru a limita accesul la anumite informații.

