Simple Network Managment Protocol (SNMP)

1.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).

2.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.

3.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 comunicatie folosit pentru a trimite mesaje (transmis ca o datagrama sub forma unui pachet de date) către alte gazde prin intermediul IP network.

4.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.

Managerul oferă interfața dintr om și sistemul de management.

Agentul oferă interfața între manager și dispozitivele fizice ce urmează a fi gestionate, cum ar fi bridge-uri, hub-uri, routere, servere de rețea sau computer-ul unui utilizator. Aceste obiecte gestionate ar putea fi hardware, parametrii de configurare, statisticile de performanță și altele.

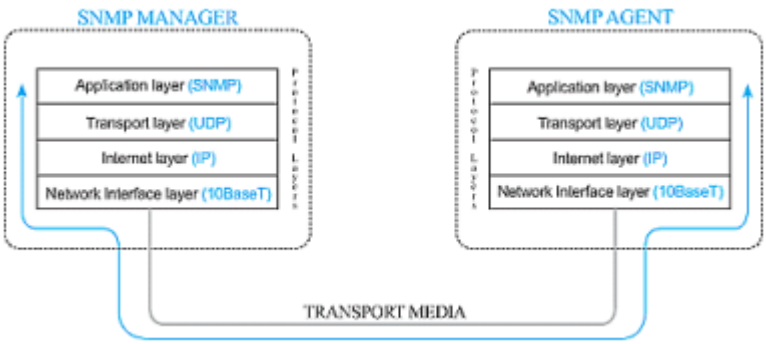

Figura 4.1: Comunicarea între managerul și agentul SNMP

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.

Aceste obiecte sunt aranjate în ceea ce este cunoscut ca bază de date a informațiilor virtuale, denumită Baza de gestionare a informațiilor, de asemenea, numită și MIB (Management Information Base). SNMP permite managerilor și agenților de a comunica cu scopul de a accesa aceste obiecte.

Managerul și agentul utilizează baza de gestionare a informațiilor și un set de comenzi relativ mic, pentru a schimba informații. MIB este organizat într-o structură de arbore cu variabile individuale, cum ar fi punctul de stare sau descriere, fiind reprezentat ca frunzele de pe ramuri (vezi Figura 4.2). Un tag numeric lung sau un obiect de identificare (OID) este folosit pentru a distinge fiecare variabilă unică în MIB și în mesajele SNMP.

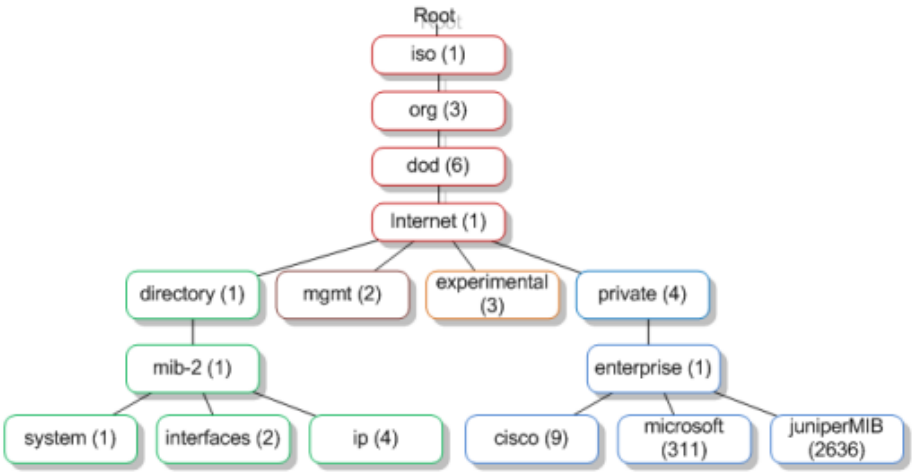

Figura 4.2: Exemplu de arbore OID

Managerul SNMP nu poate monitoriza dispozitive cu excepția cazului în care le-a compilat fișierele MIB. MIB-ul este, de asemenea, un ghid de capabilități a dispozitivelor SNMP.

Fiecare elemente SNMP gestionează obiecte specifice cu fiecare obiect având caracteristici specifice. Fiecare obiect/caracteristică are un obiect unic de identificare constând din numere separate prin puncte zecimale (de exemplu: 1.3.6.1.4.1.2636.1).

Unele protocoale sunt orientate pe octet, pe când altele sunt orientate pe pachete. Pachetele conțin antet, date și octeți de control. Protocolul SNMP este orientat pe pachete (vezi Figura 4.3), PDU (protocol Data Unit). Un PDU are următoarele câmpuri:

- Version – versiunea de SNMP;
- Community – denumirea grupului din care face parte;
- Request ID – este trimis înapoi la manager împreună cu răspunsul pentru a ști la ce cerere
  se referă un răspuns;
- Error code – agentul plasează un cod de eroare în acest câmp, dacă are loc o eroare la
  procesarea cererii;
- OID – obiectul din MIB;
- Value – valoarea care se dorește setată, dacă mesajul este un SetRequest, o valoare nulă
  dacă mesajul este un GetRequest și valoarea returnată pentru OID, dacă mesajul este un GetResponse.

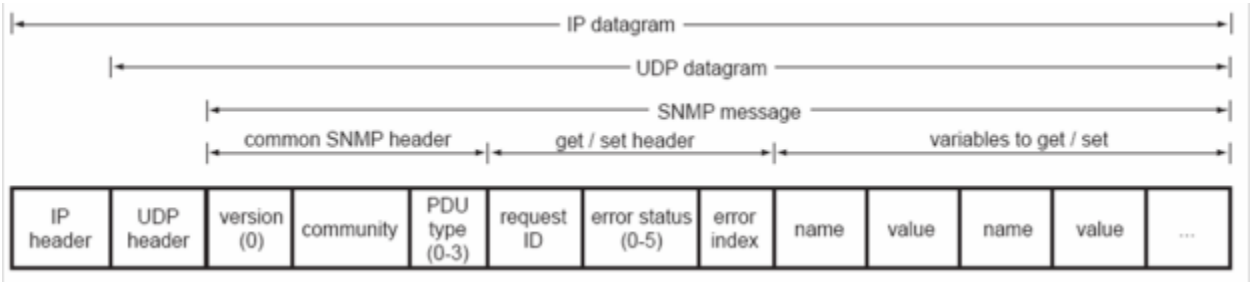

Figura 4.3: Formatul unui PDU

Există 7 tipuri de PDU:

- GetRequest – o cerere manager-agent pentru a primi o valoare sau o listă de valori a unui obiect din MIB;
- SetRequest – o cerere de la manager la agent pentru a seta sau modifica o valoare;
- GetNextRequest – managerul solicită valoarea obiectului care urmează după obiectul precizat în cerere;
- GetBulkRequest – o versiune optimizată a GetNextRequest, managerul poate cere mai multe iterații de GetNextRequest;
- GetResponse – mesajul trimis de agent, ca urmare a cererii de tip GetRequest, GetNextRequest sau SetRequest;
- Trap – o atenționare trimisă de agent către manager, atunci când apare un eveniment neașteptat legat de dispozitivul monitorizat;
- InformRequest – asigură livrarea mesajelor Trap. De-a lungul timpului au fost dezvoltate mai multe versiuni al SNMP.

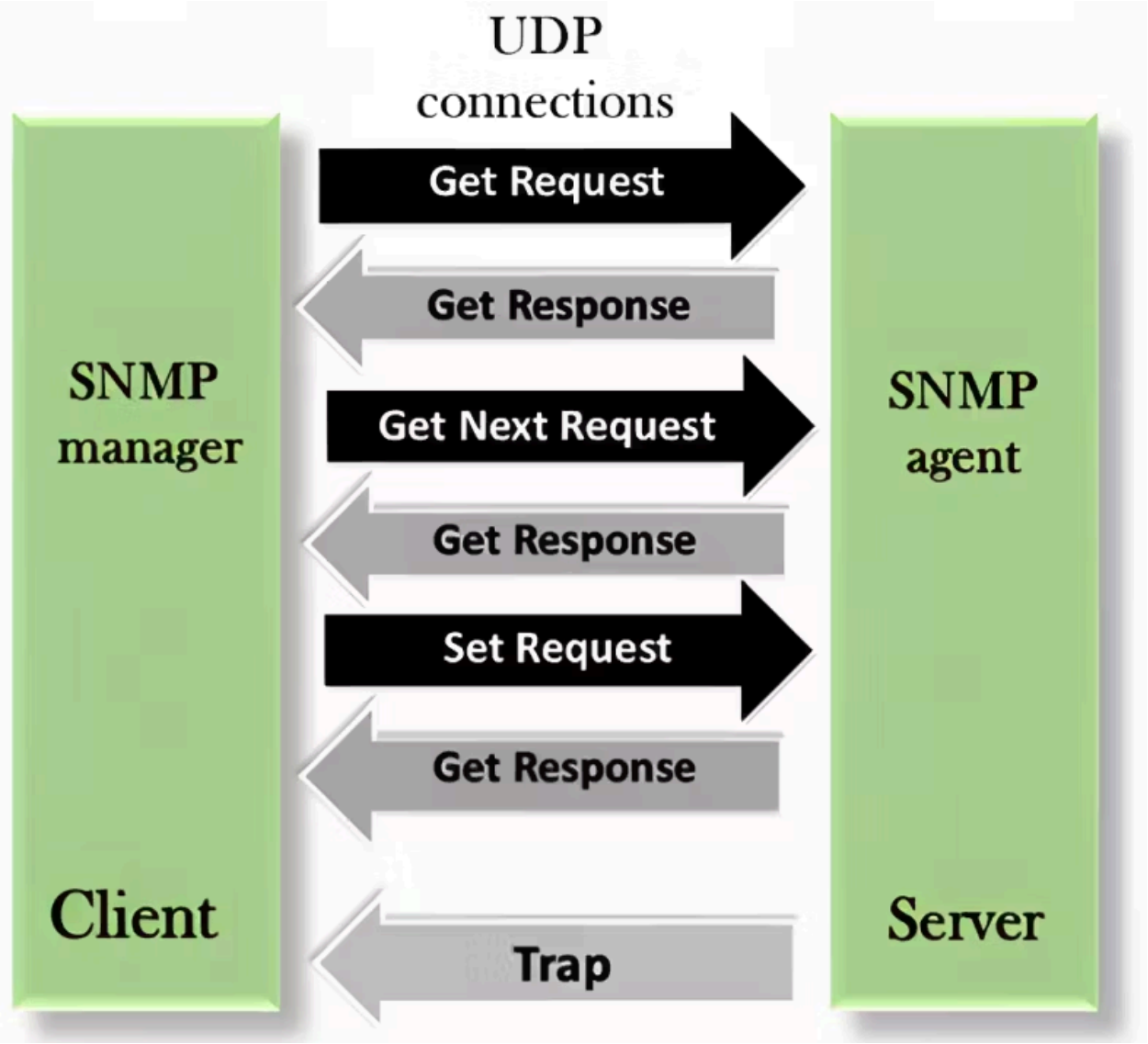

Figure 4.4: SNMP overview

5.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. Este definit în RFC 1157.
- ➢ SNMP oferă utilizatorilor un set simplu de operații, care permite acestor dispozitive să fie administrate de la distanță. Baza protocolului este un set

de operații, care oferă administratorilor posibilitatea de a urmări sau modifica parametrii unor dispozitive ce suportă SNMP.

- ➢ Prima versiunea a fost criticată pentru lipsa de securitate. Autentificarea se făcea printr- un grup numit *community string* și era nu era codificată sub nicio formă.

❖ SNMPv2

- ➢ SNMPv2, revizuiește 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. SNMPv2c (Community-Based Simple Network Management Protocol version 2) este definită în RFC 1901 – RFC 1908. Această versiune a fost considerată, până să apară versiunea a treia, un standard pentru SNMP.

❖ 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.
- ➢ Din punct de vedere al termenilor, versiunea a treia nu folosește termeni de agent și manager, ci de entități. Fiecare entitate având un Engine și un modul software de funcții ce inițiază sau răspund la cereri SNMP. Engine-ul furnizează securitatea, controlul de acces și procesarea mesajelor.
- ➢ Versiunea a treia este compatibilă cu versiunile anterioare, lucru pe care nu-l putem spune și față de versiunea a doua.

6.Componenta hardware:

Sistemul de monitorizare a rețelei folosește protocolul SNMP (Simple Network Management Protocol) pentru a colecta și centraliza informațiile despre starea echipamentelor de rețea și a serverelor. Stația de management („Management Station”) joacă un rol central, conectându-se la echipamentele de rețea (cum ar fi switch-urile, routerele și firewall-urile) și la servere pentru a monitoriza parametrii esențiali de funcționare.

Stația de management primește date prin protocolul SNMP și este configurată să trimită alerte în cazul detectării unor erori, anomalii sau scăderi de performanță. Utilizatorul poate astfel interveni rapid pentru remedierea problemelor, asigurând continuitatea operațiunilor și o funcționare optimă a infrastructurii IT.

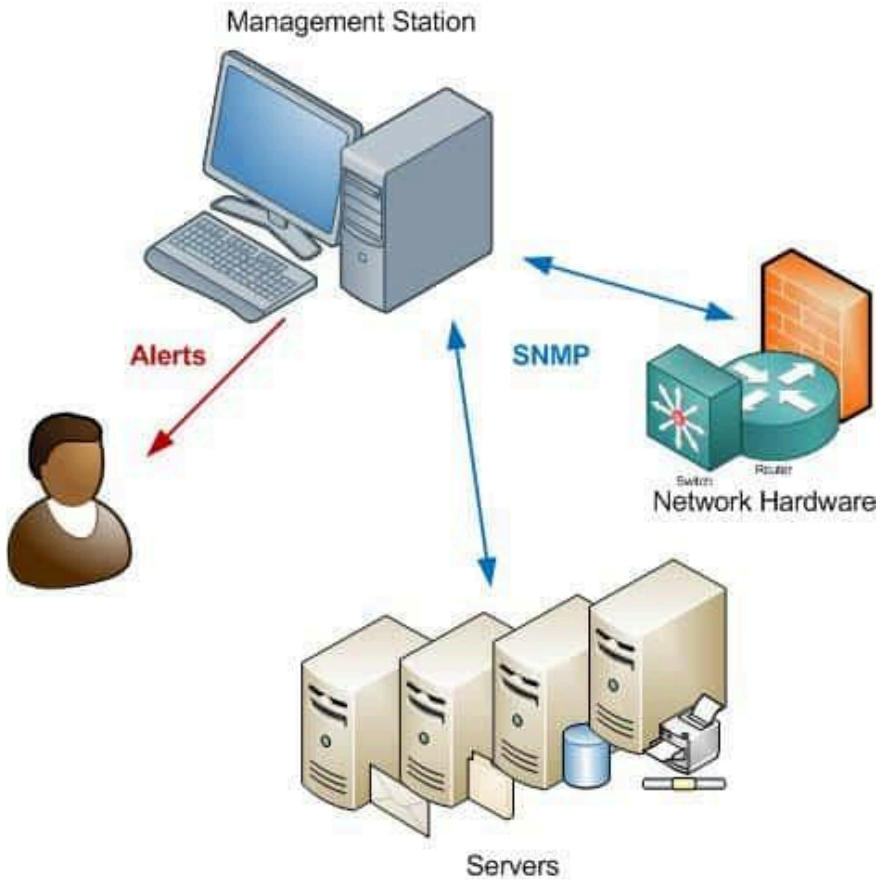

Figura 6: Arhitectura de Monitorizare Hardware prin SNMP

7.Componenta software:

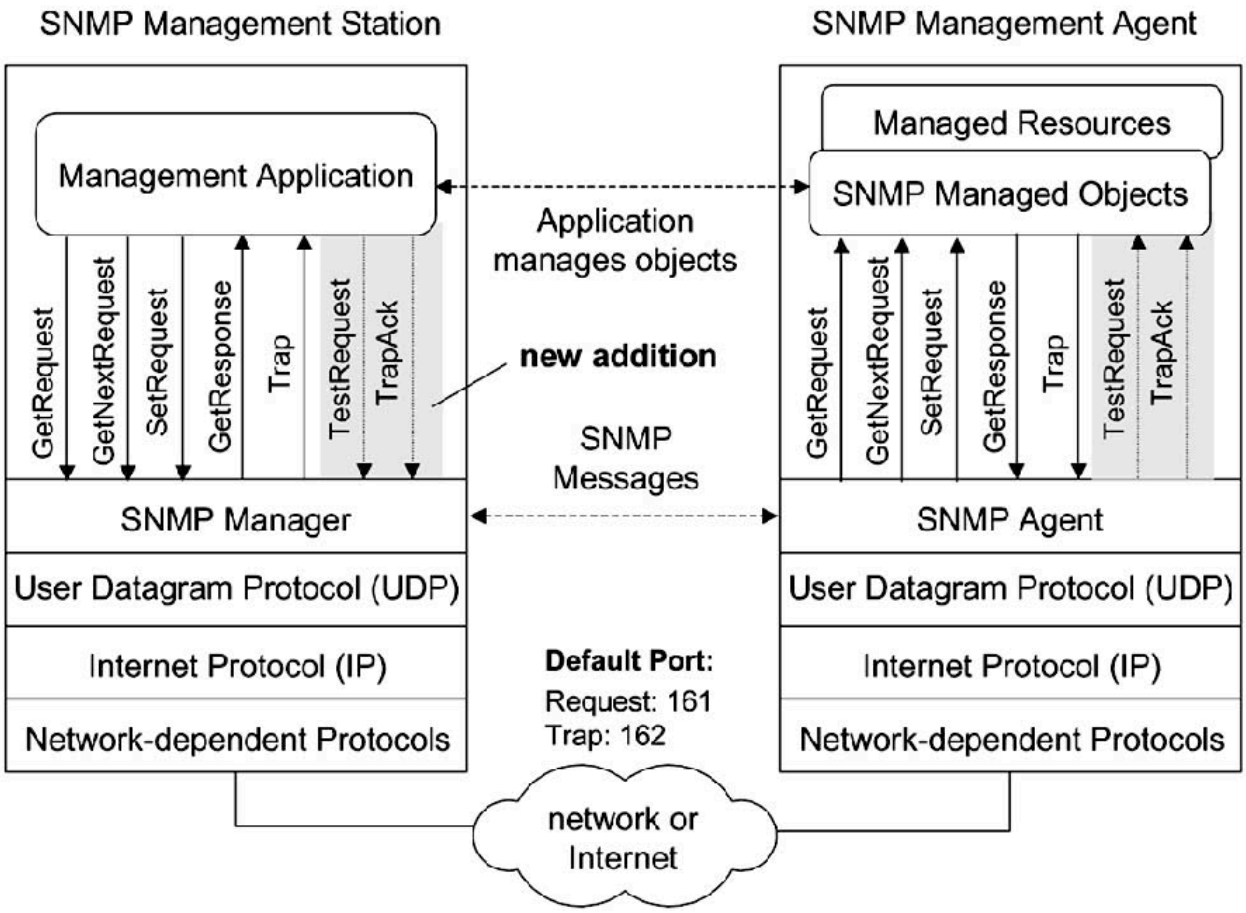

Figura 7:Imaginea arhitecturii comunicării SNMP

Diagrama ilustrează arhitectura software a unui sistem SNMP (Simple Network Management Protocol), în care Stația de Management SNMP comunică cu Agentul de Management SNMP pentru a monitoriza și administra resursele de rețea.

Stația de Management SNMP conține aplicația de management, care coordonează și monitorizează resursele rețelei, și componenta SNMP Manager, care trimite cereri și primește răspunsuri de la SNMP Agent. Comunicarea se face prin protocolul UDP (User Datagram Protocol).

În partea dreaptă a diagramei, Agentul SNMP interacționează cu resursele gestionate (Managed Resources) și cu obiectele administrate (SNMP Managed Objects) pentru a obține sau modifica date, pe care le transmite ulterior către stația de management.

8.Bibliografie:

Carti:

Douglas Mauro, Kevin Schmidt, „Essential SNMP”, O'Reilly, 2008.

Kevin R. Fall, W. Richard Stevens, „The Protocols”, Addison-Wesley Professional Computing Series, 2012.

Sidnie M.Feit, SNMP: A Guide to Network Management

Aaron Leskiw, SNMP Tutorial Part 2: Rounding Out the Basics

Site-uri:

Simple Network Management Protocol - Wikipedia

What is Simple Network Management Protocol (SNMP)? Definition from SearchNetworking

Simple Network Management Protocol (SNMP) - GeeksforGeeks

Video:

How SNMP Works - a quick guide

SNMP Operation (CCNA Complete Video Course Sample)

SNMP Explained | Simple Network Management Protocol | Cisco CCNA 200-301

SNMP Theory + Practical | Simple Network Management Protocol Details | How S…