**SNMP – Giao thức quản lý mạng đơn giản**

1. **Giới thiệu**

* SNMP là “giao thức quản lý mạng đơn giản”, dịch từ cụm từ “Simple Network Management Protocol”. Là giao thức được sử dụng rất phổ biến để giám sát và điều khiển thiết bị mạng như switch, router, server ...
* Giao thức SNMP được thiết kế để cung cấp một phương thức đơn giản để quản lý tập trung mạng TCP/IP. Nếu bạn muốn quản lý các thiết bị từ 1 vị trí tập trung, giao thức SNMP sẽ vận chuyển dữ liệu từ client (thiết bị mà bạn đang giám sát) đến server nơi mà dữ liệu được lưu trong log file nhằm phân tích dễ dàng hơn
* SNMP dùng để quản lý tức là có thể theo dõi, có thể lấy thông tin, có thể được thông báo, và có thể tác động để hệ thống hoạt động như ý muốn.
* VD một số khả năng của phần mềm SNMP :
* Theo dõi tốc độ đường truyền của một router, biết được tổng số byte đã truyền/nhận.
* Lấy thông tin máy chủ đang có bao nhiêu ổ cứng, mỗi ổ cứng còn trống bao nhiêu.
* Tự động nhận cảnh báo khi switch có một port bị down.
* Điều khiển tắt (shutdown) các port trên switch.

1. **Hoạt động của SNMP:**

* Có 2 nhân tố chính trong SNMP: ***Manager*** và ***Agent***:
* Các SNMP agent sẽ giữ một sơ sở dữ liệu, được gọi là **Management Information Base (MIB)**, trong đó chứa các thông tin khác nhau về hoạt động của thiết bị mà agent đang giám sát. Phần mềm quản trị SNMP Manager sẽ thu thập thông tin này qua giao thức SNMP.
* Ưu điểm khi thiết kế hệ thống quản trị với SNMP sẽ giúp đơn giản hóa các quá trình quản lý các thành phần trong mạng, giảm chi phí triển khai.SNMP được thiết kế để có thể mở rộng các chức năng quản lý, giám sát. SNMP được thiết kế để có thể hoạt động độc lập với các kiến trúc và cơ chế của các thiết bị hỗ trợ SNMP.

1. **Các cơ chế bảo mật cho SNMP**

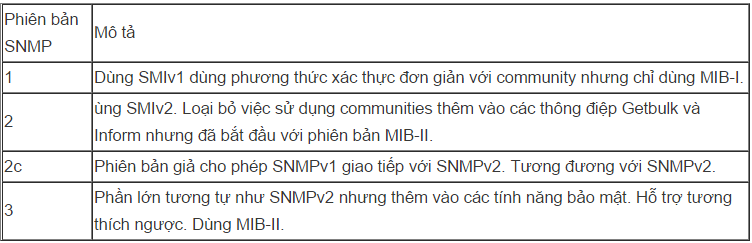
* Một SNMP management station có thể quản lý/giám sát nhiều SNMP element, thông qua hoạt động gửi request và nhận trap. Tuy nhiên một SNMP element có thể được cấu hình để chỉ cho phép các SNMP management station nào đó được phép quản lý/giám sát mình.
* Các cơ chế bảo mật đơn giản này gồm có : community string, view và SNMP access control list.
* ***Community String***: Community string là một chuỗi ký tự được cài đặt giống nhau trên cả SNMP manager và SNMP agent, đóng vai trò như “mật khẩu” giữa 2 bên khi trao đổi dữ liệu. Community string có 3 loại : Read-community, Write-Community và Trap-Community.
* ***View***: Một view phải gắn liền với một community string. Tùy vào community string nhận được là gì mà agent xử lý trên view tương ứng.
* ***SNMP access control list***: SNMP ACL là một danh sách các địa chỉ IP được phép quản lý/giám sát agent, nó chỉ áp dụng riêng cho giao thức SNMP và được cài trên agent. Nếu một manager có IP không được phép trong ACL gửi request thì agent sẽ không xử lý, dù request có community string là đúng.

Đa số các thiết bị tương thích SNMP đều cho phép thiết lập SNMP ACL.

1. **Các phiên bản SNMP**

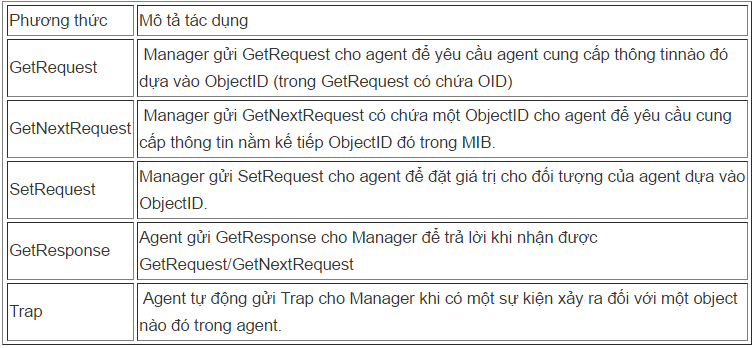
SNMP có 4 phiên bản : ***SNMPv1***, ***SNMPv2c***, ***SNMPv2u*** và ***SNMPv3***. Các phiên bản này khác nhau một chút ở định dạng bản tin và phương thức hoạt động.

Mô tả Phiên bản SNMP:



**5. Các phương thức SNMP**

Các giao thức SNMPv1 và SNMPv2 định nghĩa cách thức mà một phần mềm manager và một tác nhân agent có thể giao tiếp với nhau. Ví dụ, một manager có thể dùng ba thông điệp khác nhau để lấy các thông tin MIB từ các tác nhân agents với một thông điệp SNMP response được trả về từ tác nhân agent. SNMP dùng UDP để truyền thông tin, dùng thông tin SNMP response để cung cấp thông tin và công nhận (ack) việc nhận các thông điệp khác.



SNMPv2 hoạt động dựa trên 7 loại thông điệp

SNMPv2 PDU

* ***GetRequest***: Manager gửi GetRequest (chứa một hoặc nhiều OID) đến agent để lấy một hoặc nhiều giá trị của object trong MIB.
* ***GetNextRequest*** :Manager gửi GetNextRequest đến agent dùng để lấy giá trị của object nằm kế tiếp object được chỉ ra trong MIB.
* ***GetBulkRequest:*** Manager gửi GetBulkRequest đến agent để lấy nhiều giá trị của nhiều object.
* ***InformRequest***: Manager gửi InformRequest đến manager nhằm trao đổi thông tin với nhau.
* ***SetRequest***: Manager gửi SetRequest đến agent để thiết lập giá trị cho oject dựa vào OID. Chỉ những oject có quyền READ\_WRITE mới có thể thiết lập giá trị được.
* ***SetResponse***: Sau khi Agent nhận được các thông điệp GetRequest, GetNextRequest hay SetRequest thì nó sẽ gửi GetResponse để trả lời. Trong GetResponse có chứa OID của object được yêu cầu và giá trị của object đó.
* ***Trap:*** Trap được agent tự động gửi đến manager để thông báo trong agent có sự kiện hay biến cố xảy ra. Ví dụ: khi có một cổng bị tắt, người dùng đăng nhập thất bại. Việc gửi hay không gửi khi biến cố xảy ra do hãng sản xuất thiết bị agent quy định.

SNMP request/reponse dùng để quản lý còn SNMP trap dùng để cảnh báo. Nguồn gửi trap được gọi là Trap Sender và nơi nhận trap được gọi là Trap Receiver. Mỗi trap sender có thể gửi nhiều trap đến nhiều trap receiver cùng lúc.

Trap gồm 2 loại chính: generic trap (được qui định trong các chuẩn SNMP) và specific trap (do hãng sản xuất tự định nghĩa). Có thể phân biệt loại trap dựa vào mã số là một số nguyên chứa trong gói tin trap. Theo SNMPv1, generic trap có 7 loại sau: coldStart(0), warmStart(1), linkDown(2), linkUp(3), authenticationFailure(4), egpNeighborloss(5), enterpriseSpecific(6).

**CÔNG THỨC HÀNG ĐỢI M/M/C/K**

