ĐẠI HỌC BÁCH KHOA HÀ NỘI
Trường Công nghệ thông tin và truyền thông

Báo cáo tuần 1

Xây dựng phần mềm đọc thông tin SNMP từ thiết bị

Nhóm 7
Trịnh Hoàng Chi
Nguyễn Quang Huy

Trợ giảng hướng dẫn: TG. Nguyễn Quốc Khánh _____

Chữ kí TGHD

Khoa: Kỹ thuật máy tính

Trường: Công nghệ Thông tin và Truyền thông

HÀ NỘI, 11/2024

MỤC LỤC

DANH MỤC HÌNH VẼ

CHƯƠNG 1. Giới thiệu về SNMP

1.1 Tổng quan về giao thức

Giao thức Simple Network Management Protocol (SNMP) là một giao thức mạng tiêu chuẩn được sử dụng để giám sát và quản lý các thiết bị mạng. Nó cho phép các thiết bị mạng như máy chủ, router, switch, tường lửa và các thiết bị khác giao tiếp với một trạm quản lý (thường là một phần mềm hoặc thiết bị) để cung cấp thông tin về trạng thái, hiệu suất, và các sự kiện khác trong mạng. SNMP hoạt động dựa trên mô hình quản lý thông tin có thể được truy cập, thực hiện các thay đổi và thu thập thông tin từ các thiết bị mạng.

Giao thức SNMP là một trong những giao thức mạng được chấp nhận rộng rãi để quản lý và giám sát các phần tử mạng. Hầu hết các thiết bị mạng được cung cấp đi kèm với SNMP agent. Các agent này phải được kích hoạt và cấu hình để giao tiếp với các công cụ giám sát mạng hoặc hệ thống quản lý mạng (NMS).

1.2 Các thành phần của SNMP:

SNMP hoạt động theo mô hình client-server với các thành phần chính bao gồm 5 thành phần chính là SNMP Manager, Managed Devices, SNMP Agent, MIB và OID.

1.2.1 SNMP Manager (NMS)

Trình quản lý SNMP, hay SNMP Manager (còn được gọi là NMS- Network Management Server), là hệ thống trung tâm được áp dụng để theo dõi mạng SNMP.Đây thường là một máy tính được sử dụng để chạy một hoặc nhiều hệ thống quản lý mạng. SNMP Manager có khả năng truy cập và điều khiển các thông tin của SNMP Agent trên các thiết bị mạng.

Các chức năng chính của SNMP manager: Truy vấn các SNMP Agent. Nhận response từ các Agent. Đặt các biến trong Agent. Xác nhận các sự kiện không đồng bộ từ các Agent.

SNMP Manager thường sử dụng phần mềm như SolarWinds, PRTG Network Monitor, hoặc các công cụ mã nguồn mở như Nagios.

1.2.2 Managed Devices

Managed Devices là những thành phần trong mạng hỗ trợ SNMP và được điều khiển bởi SNMP Manager. Ví dụ: Máy in, rounter, switch,. . .

1.2.3 SNMP Agent (Server)

Agent là phần mềm chạy trên các Devices, cho phép chúng kết nối với NMS. Agent thu thập và lưu trữ các dữ liệu từ thiết bị rồi chuyển chúng đến với NMS khi

có yêu cầu. NMS và Agent liên lạc với nhau thông qua Internet.

1.2.4 MID - Management Information Base

Management information base(Cơ sở thông tin quản lý) là một file văn bản (có đuôi .mib) dùng để phân loại và mô tả thông tin của tất cả các đối tượng được sử dụng bởi một thiết bị cụ thể hỗ trợ và cho phép SNMP kiểm soát. Cơ sở dữ liệu này phải được tải vào SNMP Manager (NMS) để có thể xác định và theo dõi trạng thái của các thuộc tính này. Mỗi mục MIB được đính kèm với một định danh đối tượng (OID).

1.2.5 OID

Là định danh cho một thiết bị được quản lý nên OID có tính duy nhất. OID là một chuỗi số được phân tách bởi các dấu chấm.
OID trong SNMP của một thiết bị thường là cố định và được xác định bởi MIB Ví dụ về OID: 1.3.6.1.2.1.1.1.0

- 1: Root
- 3: ISO
- 6: Internet
- 1.2.1: MIB-2
- 1.1.0: System Description

1.3 Thông tin cung cấp:

SNMP cung cấp môi trường để người sử dụng giám sát và điều khiển các thiết bị, cũng như thông tin các thiết bị thu nhận được bao gồm:

- Thông tin về Hiệu suất
- Trạng thái của Thiết bị và Giao diện
- Thông tin về Cấu hình
- Thông tin về Bảo mật
- Thông tin về Môi trường
- Thông tin về Trạng thái và Sự kiện

1.4 Cấu trúc dữ liệu trong SNMP

SNMP có cấu trúc dữ liệu dựa trên quan hệ giữa MIB và các OID theo mô hình cây phân cấp, qua đó tổ chức và quản lí các thiết bi mạng. MIB là một cấu trúc dữ liệu định nghĩa các đối tượng được quản lý, được thiết kế để quản lý các thiết bị không chỉ riêng TCP/IP. RFC1155 mô tả cấu trúc của file MIB, cấu trúc này gọi

là SMI (Structure of Management Information).
Cơ sở thông tin quản lý MIB được cấu trúc theo mô hình cây phân cấp và mỗi đối tượng có một giá trị nhận dạng (Object Identifier) thể hiện qua tên đối tượng. Nút gốc của cây phân trong MIB không có tên. Dưới gốc là 3 cây con gồm Ccitt(0), Iso(1) và Joint-Iso-ccitt(2).Tất cả mọi thứ thuộc về cộng đồng Internet đều nằm dưới .iso.org.dod.internet, mọi object của các thiết bị TCP/IP đều bắt đầu với prefix " .1.3.6.1".

1.5 Cấu trúc gói tin SNMP

1.5.1 Các thành phần trong gói tin SNMP

Một gói tin SNMP được thiết kế để truyền dữ liệu quản lý mạng giữa SNMP Manager và SNMP Agent. Cấu trúc gói tin tuân theo mô hình ASN.1 (Abstract Syntax Notation One) và được mã hóa bằng BER (Basic Encoding Rules).
Một gói tin SNMP bao gồm 3 thành phần chính:

- Version: Phiên bản SNMP (SNMPv1, SNMPv2c, SNMPv3).
- Community String: Chuỗi ký tự dùng để xác thực giữa SNMP Manager và SNMP Agent.
- PDU (Protocol Data Unit): Chứa thông tin chính của gói tin, như yêu cầu (Request) hoặc phản hồi (Response).

1.5.2 Thành phần chi tiết trong PDU

PDU là phần quan trọng nhất trong gói tin SNMP, bao gồm các thành phần:

- PDU Type: Loại PDU, cụ thể:

Loại PDU	Giá trị PDU Type	Mô tả
GetRequest	0	Yêu cầu giá trị của một hoặc nhiều đối tượng từ SNMP Agent.
GetNextRequest	1	Lấy đối tượng kế tiếp trong cây MIB.
SetRequest	2	Thay đổi giá trị của một đối tượng.
Response	3	Phản hồi từ SNMP Agent đến SNMP Manager.
Trap	4	Thông báo sự kiện hoặc lỗi từ SNMP Agent đến SNMP Manager.
GetBulkRequest	5 (SNMPv2/v3)	Lấy nhiều dữ liệu trong một yêu cầu, cải thiện hiệu suất so với GetRequest.
InformRequest	6 (SNMPv2/v3)	Tương tự Trap nhưng yêu cầu SNMP Manager xác nhận đã nhận thông báo.

Hình 1.1: PDU Type

- Request ID: ID duy nhất để nhận diện yêu cầu và kết hợp nó với phản hồi tương ứng.
- Error Status: Trạng thái lỗi (chỉ có trong phản hồi), ví dụ: noError, tooBig,

noSuchName, . . .

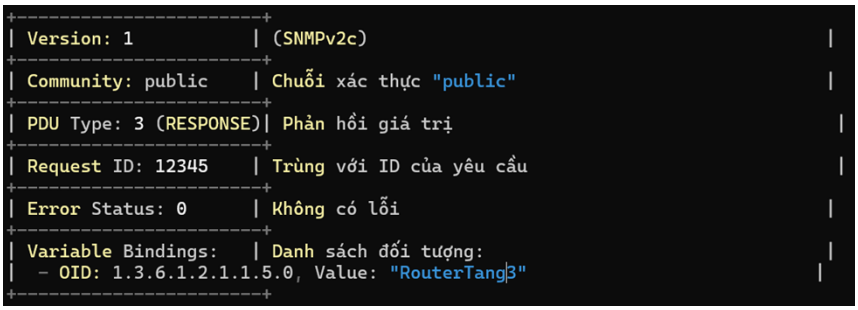
- Error Index: Chỉ định đối tượng trong danh sách xảy ra lỗi (nếu có lỗi).
- Variable Bindings: Danh sách OID và giá trị tương ứng.

1.5.3 Ví dụ gói tin SNMP:

- Yêu cầu SNMP Get lấy giá trị của đối tượng có OID 1.3.6.1.2.1.1.5.0 (tên thiết bị).
- Cấu trúc gói tin request:

Hình 1.2: Cấu trúc gói tin request

- Giá trị trả về: "RouterTang3" – Router Tầng 3
- Cấu trúc gói tin response:



Hình 1.3: Cấu trúc gói tin response

(*) Ghi chú: Với SNMPv1/v2c, Community String được gửi dưới dạng văn bản thuần (plaintext), dễ bị tấn công đánh cắp. SNMPv3 có thêm các trường bảo mật Authentication Parameters (Xác thực người dùng) và Privacy Parameters (Mã hóa dữ liệu để đảm bảo tính bảo mật)

1.6 Các phương thức trao đổi thông tin trong SNMP

1.6.1 Cách lấy thông tin:

- Polling: NMS gửi yêu cầu lấy thông tin đến Agent và Agent phản hồi lại thông tin được yêu cầu.
- Notifing: Agent gửi thông báo mà không cần yêu cầu từ NMS để cảnh báo

nhanh chóng về các sự kiện.

1.6.2 Lệnh lấy thông tin:

- Get Request: SNMP Manager gửi yêu cầu Get Request tới SNMP Agent để lấy thông tin về một mục đích cụ thể. Agent phản hồi bằng cách cung cấp giá trị được yêu cầu thông qua tin nhắn phản hồi (Response).
- GetNextRequest: SNMP Manager yêu cầu đối tượng tiếp theo trong cơ sở dữ liệu MIB. SNMP Manager có thể liên tục yêu cầu dữ liệu cho đến khi hết dữ liệu để nắm bắt được được tất cả dữ liệu có sẵn trên SNMP Agent.
- GetBulkRequest: SNMP Manager yêu cầu truy xuất lượng dữ liệu lớn đồng thời từ các SNMP Agent bằng việc thực hiện nhiều lệnh GetNextRequest.
- Get Response: SNMP Agent trả về phản hồi Get Response chứa thông tin yêu cầu từ SNMP Manager.
- Set Request: SNMP Manager gửi yêu cầu Set Request tới SNMP Agent để thay đổi giá trị của một mục đích cụ thể.
- Set Response: SNMP Agent trả về phản hồi Set Response để xác nhận yêu cầu Set Request đã được thực hiện thành công.
- - Trap: Trap là một thông báo "bẫy" không được yêu cầu bởi Manager, cung cấp thông tin về các sự kiện trên thiết bị. Các SNMP Trap đã được đổi tên thành “Notifications” trong các phiên bản SNMP sau này. Agent không tự gửi Trap theo yêu cầu từ Manager mà hoạt động tự động khi phát hiện có lỗi xảy ra.
- Inform: SNMP Agent gửi SNMP Inform để thông báo cho SNMP Manager về các sự kiện quan trọng như khắc phục lỗi mạng hoặc báo cáo tình trạng mạng.