네트워크 관리 프로토콜 – SNMP

김우태 컴퓨터시스템응용 기술사
(matica5127@naver.com)

SNMP(Simple Network Management Protocol)

Concept	+ SNMP 주요 용어 + SNMP 개요 - SNMP 정의 - SNMP 구성요소 및 특징 + SNMP 의 동작 방식 + SNMP 접근 제한
KeyWord	MIB, SMI, ASN.1, Polling/Event Reporting, PDU(Get/Set/Trap)

+ SNMP 주요 용어

구 분	상세 설명	핵심 요소
MIB	- 관리 되어야 할 특정한 Information, Resource → Object - Object 의 집합체를 MIB	Object, Tree 구조
SMI	- Structure Management Information - MIB 를 정의하기 위한 일반적인 구조	**ASN.1 언어를 사용** (Abstract Syntax Notation)
정의된 모든 객체	- name, syntax, encoding 으로 구성 - name: 해당 객체 식별하기 위한 식별자(OID) - syntax: 객체의 데이터 유형 - encoding: 메시지 전송 시 비트 변환 규칙	OID, BER

- SNMP 는 ASN. 1 의 encoding rule 중 BER(Basic Encoding Rules)을 사용함.

1.N/W 관리 프로토콜, SNMP(Simple Network Management Protocol)의 개요

- **정의**: 시스템이나 N/W 관리자로 하여금 원격으로 네트워크 장비를 모니터링하고 환경설정 등의 운영이 가능하도록 하는 N/W 관리 프로토콜을 뜻함.
- SNMP 는 프로토콜일 뿐이고, N/W 관리를 하기 위해서는 관련 시스템이 갖추어져야 함.
- SNMP 는 N/W 관리를 가능하게 하는 프로토콜이지만, 여러 취약점들이 존재함 (DoS, Buffer Overflow, 비인가 접속 등)

1) SNMP 구성 요소

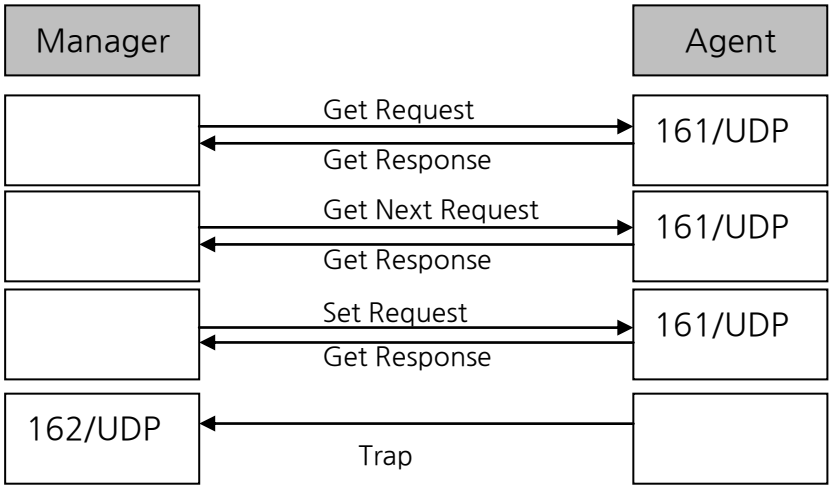
구 분	요소	상세 설명
관리 시스템	Manager	- Agent 에 필요한 정보를 요청하는 모듈

관리 대상	Agent	- 관리 대상 시스템에 설치되어 필요한 정보를 수집하고, Manager 에게 전달해주는 역할을 수행하는 요소

2) SNMP 의 특징

구 분	특 징
OSI 계층	- OSI 7 계층의 Application 계층 프로토콜
전송 계층	- 메시지는 단순히 요청과 응답 형식의 프로토콜에 의해 교환됨. - 따라서 전송 계층 프로토콜은 UDP 프로토콜을 사용함.
활용 방안	- N/W 관리를 위한 목적으로 주로 서버나 네트워크 장비에서 SNMP 를 설정한 후 관련 Agent 프로그램 이용ㅎ여 트래픽 관리 등을 위해 사용함.

2.SNMP 의 동작 방식

<table>
<tr><th>구분</th><th>주요 항목</th><th>설명</th></tr>
<tr><td>동작방식</td><td colspan="2"> 
</td></tr>
<tr><td rowspan="2">활용 포트</td><td>관리 시스템(Manager)</td><td>162/udp 포트 사용 (Polling 방식)</td></tr>
<tr><td>대행자(Agent)</td><td>161/udp 포트 사용 (Event Reporting 방식)</td></tr>
<tr><td rowspan="3">통신 전제 조건</td><td>SNMP Version</td><td>Manager 와 Agent 간 SNMP 버전 일치 필요</td></tr>
<tr><td>Community String</td><td>상호간에 설정한 Community String 이 일치해야 함.</td></tr>
<tr><td>PDU(Protocol Data Unit)</td><td>통신하기 위한 메시지 유형</td></tr>
<tr><td rowspan="3">PDU 유형</td><td>Get Request</td><td>- 관리 시스템이 Agent 로 원하는 객체의 특정 정보를 요청함.</td></tr>
<tr><td>Get Next Request</td><td>- 관리 시스템이 에이전트로 이미 요청한 정보의 다음 정보를 요청함.</td></tr>
<tr><td>Set Request</td><td>- 관리 시스템이 에이전트로 특정한 값을 설정하기 위해 사용함.</td></tr>
</table>

	Get Response	- Agent 가 관리 시스템에 해당 변수 값을 전송함.
	Trap	- Agent 가 관리 시스템에 어떤 정보를 비동기적(Asynchronous)으로 알리기 위해 사용함. - notify 라고 하며, callback 함수와 같은 역할
	Get Bulk Request	- 요청할 객체의 범위를 지정하여 한 번에 요청할 수 있음
	InformRequest	- 관리 시스템 간에 정보를 전달 하는 목적으로 사용함
수집 방식	Polling	- Manager 가 Agent 에게 정보를 요청하면 응답해주는 방식으로 Get, Set PDU 의 수집 방식임.
	Event Reporting	- Agent 가 이벤트 발생 시 이를 Manager 에게 알리는 방식으로 Trap 의 수집 방식임.

- Trap 를 제외한 나머지 PDU 는 모두 동기적(Synchronous)으로 동작함.
- Get Bulk Request, InformRequest 는 SNMPv2 에 추가된 PDU 임.

3.SNMP 접근 제한

- SNMP 는 트랙픽 정보뿐만 아니라 각종 H/W 정보까지 제공하는 등 관리자 입장에서는 매우 중요한 정보 제공되기 때문에 접근 제한에 주의하여야 함.
- SNMP 에 Write 권한이 있으면 H/W 장비의 설정 파일을 열람하는 것을 넘어서 직접 N/W 설정을 변경할 수 있음.

1) SNMP 버전별 특징

Version	상세 설명	보안성
SNMPv1	- SGMP(Simple Gateway Monitoring Protocol)을 발전시킨 SNMP 을 만듦	- 암호화 및 인증 기능이 없음 - community string 만 일치하면 모든 정보를 얻을 수 있음
SNMPv2	- v1 문제점을 보완하기 위해 암호화와 해시기능 추가 - SNMPv2c 를 가장 많이 사용하며, SNMPv2 에서 복잡한 보안기능을 제거한 Version 이며, 보안에 취약함	- 암호화(DES), 해시(MD5) - 송신처 인증 기능은 없음
SNMPv3	- 이전 SNMP 버전에서 제공되지 않았던 안전한 통신망 관리를 위한 기반기술을 제공함.	- 데이터 인증, 암호 기능 및 재사용 방지, 세분화된 접근 통제

- SNMPv1, SNMPv2c 는 Agent 와 Manager 간 request, response 과정이 모두 평문으로 전송되기 때문에 **Sniffing** 에 손쉽게 노출될 수 있음.
- SNMPv3 보안 서비스는 비인가된 사용자에 의한 데이터의 변경(무결성 침해), 도청(기밀성 침해), 재사용 공격에 대응하는 기능을 제공하는 “사용자 기반 보안모델(USM:User Securiry Model)”과 인가된 사용자의 MIB 접근 통제 기능을 제공하는 “뷰기반 접근통제 모델(VACM:View-based Access Control Model)”에 의해 제공됨.

2) community string

구분	상세 설명	비고
정의	- Manager 와 Agent 가 데이터를 교환하기 전에 상호간의	- 초기값: public 이거나 private

	인증을 위해서 사용되는 일종의 패스워드 - 초기값을 그대로 사용하기 않도록 주의하고 패스워드와 동일한 수준으로 변경해서 사용하고 관리되어야 함.	
사용 모드	- RO(Read Only), RW(Read Write) 모드를 제공함. - RW 모드를 사용한 경우에는 중요 설정 수정이 가능하기 때문에 심각한 보안 문제 유발할 수 있음.	- RW 모드는 가급적 사용을 자제하는 것을 권고함.

- SNMPv3 부터는 다양한 공격 위협(DoS, Buffer Overflow, 비인가 접속 등)에 대응하기 위해서 보안매개변수 필드(msgSecurityParameter)들을 사용함.

"끝"