



# 인터넷에서 사용되는 여러 기술

## SNMP(Simple Network Management Protocol)

글. 조인준 KBS 미디어기술연구소 차장

인터넷과 네트워크 사용이 확산하면서 다양한 네트워크 장비(라우터, 스위치, 서버 등)를 효과적으로 관리하고 장애를 신속히 탐지할 수 있는 표준 프로토콜의 필요성이 커지기 시작했습니다. 이에 인터넷 표준과 기술을 개발하고 관리하는 국제표준기구인 IETF(Internet Engineering Task Force)는 1988년 다음 세 개의 RFC(Request for Comments)를 통해 SNMP의 첫 번째 버전인 SNMPv1의 프로토콜 구조에 대한 표준을 정의했습니다.

- **RFC 1065 : Structure and Identification of Management Information for TCP/IP-based Internets**

네트워크 관리 정보의 구조와 식별 방법(SMI, Structure of Management Information)에 대해 정의한 문서이며 SNMP를 통해 관리할 수 있는 네트워크 정보가 어떻게 구성되고 식별되는지에 대해 규정하고 있음. MIB(Management Information Base)에서 객체를 정의할 때 데이터 형식, 식별자, 범위 등을 표준화해 SNMP 프로토콜을 통한 데이터 교환을 효율적으로 수행할 수 있도록 함.

- **RFC 1066 : Management Information Base for network management of TCP/IP-based Internets**

SNMP를 통해 관리되는 정보의 초기 표준을 정의한 문서이며 네트워크 장비의 다양한 상태 정보(네트워크 인터페이스 상태, 오류 등)를 계층 구조로 표현하고 고유 식별자(OID : Object Identifier)를 할당하여 접근할 수 있게 함. 초기 MIB는 이후 여러 확장을 통해 현재의 다양한 MIB 표준으로 발전.

- **RFC 1067 : Simple Network Management Protocol**

SNMP 프로토콜의 초기 표준을 정의하고 있으며 네트워크 관리자가 SNMP 에이전트에 데이터를 요청하거나 설정을 변경하기 위한 기본 동작(Get, Set, Trap 등)과 메시지 포맷, 통신 방식 등이 규정되어 있음. 이후 개선과 보안 강화가 이루어져 오늘날의 SNMP 표준(SNMPv2, SNMPv3)으로 발전.

현재까지 SNMP는 보안을 거쳐 3개의 버전이 만들어졌으며, 버전별 간략한 특징은 다음과 같습니다.

- **SNMPv1** : 최초 버전으로 기본적인 관리 기능만 제공하며 보안 기능이 미흡
- **SNMPv2** : 성능이 개선되었으나 보안이 취약한 편
- **SNMPv3** : 인증과 암호화 기능을 추가해 보안을 강화한 버전

SNMP는 앞서 말씀드린 대로 여러 네트워크 장비의 상태를 중앙에서 실시간으로 모니터링하고 관리할 수 있게 해줍니다. 이와 같은 기능을 수행하기 위해 SNMP에서는 네트워크상의 장치들을 다음과 같이 Managed Device와 Network Management System 두 가지로 분류합니다.

- **NMS(Network Management System)**
  - SNMP를 이용해 네트워크상의 장치를 관리하는 시스템
  - SNMP 서버에 해당
- **Managed Device**
  - SNMP를 이용한 관리 대상이 되는 네트워크상의 장치
  - 네트워크상의 라우터나 스위치 등이 해당

NMS(Network Management System)와 Managed Device 사이에 수행되는 다음 세 가지 주요 기능을 통해 SNMP를 통한 네트워크 관리가 이루어집니다.

#### 🔗 네트워크 관리 이슈 발생 시 Managed Device가 이를 NMS에 리포트

단말 A와 연결된 네트워크 스위치 인터페이스가 하드웨어 고장인 경우 Managed Device인 스위치는 포트 고장을 SNMP를 통해 NMS에 알릴 수 있습니다. 고장 메시지를 받은 NMS는 설정에 따라 네트워크 관리자에게 알람이나 이메일 등을 보내는 방식으로 문제가 발생했음을 알릴 수도 있습니다.

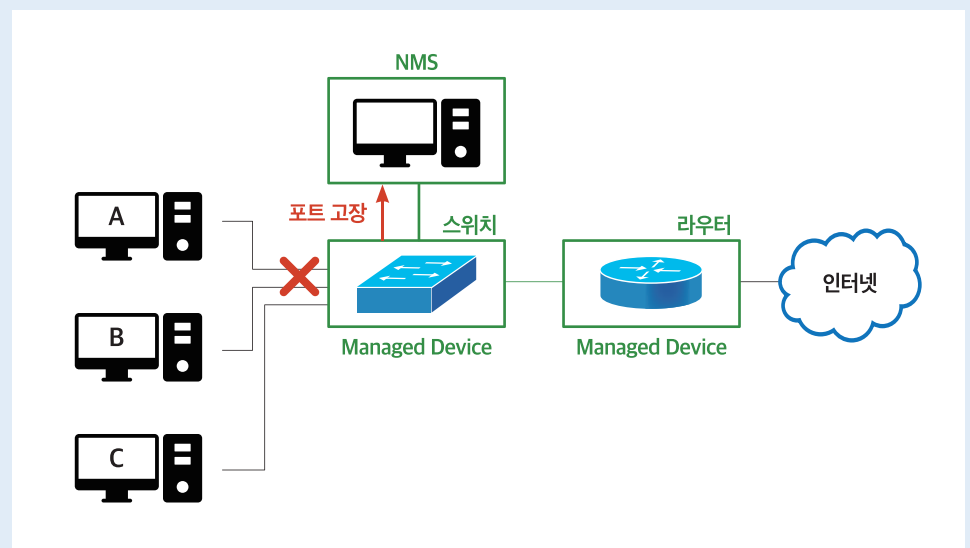


그림 1. Managed Device의 고장 리포트

NMS가 Managed Device에 현재 상태에 대한 정보 요청

예를 들어 NMS는 라우터에 개별 인터페이스를 통해 오가는 데이터 트래픽에 관한 정보를 요청할 수 있고, 이 요청을 받은 라우터는 개별 인터페이스를 통해 들어오고 나가는 데이터의 바이트 수, 수신 및 송신된 패킷 수, 수신 및 송신 중 발생한 에러 패킷 수, 수신 및 송신이 중단된 패킷 수 등의 트래픽 관련 정보를 응답으로 줄 수 있습니다.

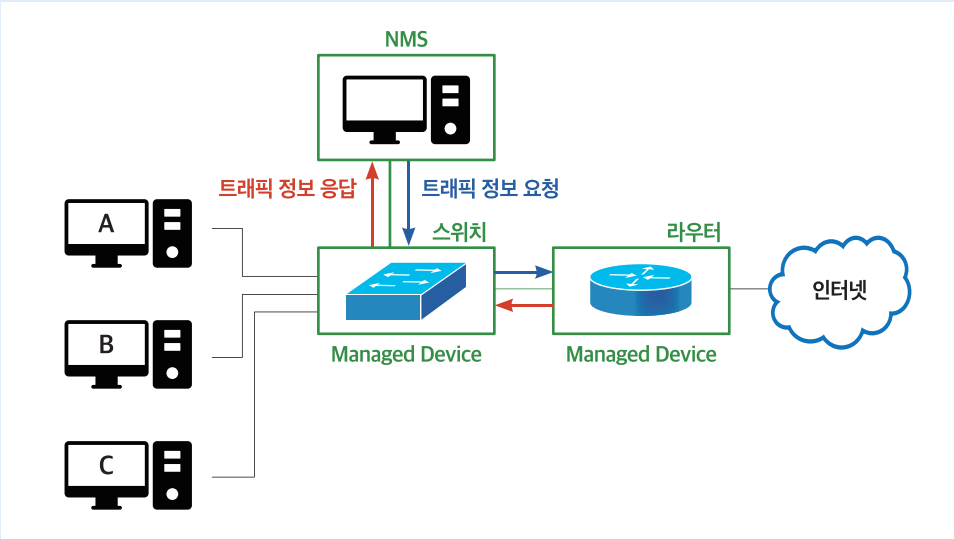


그림 2. Managed Device 모니터링

NMS에 의한 Managed Device의 설정 변경

NMS에 의한 Managed Device 설정 변경의 예로 NMS는 라우터 인터페이스의 IP 주소 변경을 요청할 수 있습니다. [그림 3]과 같이 168.126.63.1인 라우터 인터페이스의 IP 주소를 168.126.63.3으로 변경해달라고 요청할 수 있고, 이를 수행한 라우터는 변경이 완료되었음을 응답할 수 있습니다.

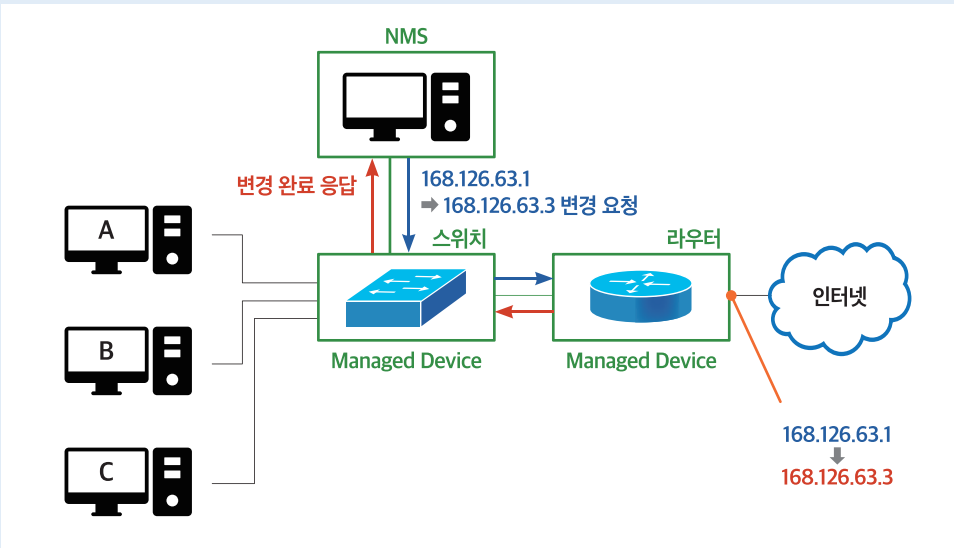


그림 3. Managed Device 설정 변경

NMS와 Managed Device 사이의 주요 기능 수행 및 처리 과정들을 [그림 4]를 통해 조금 더 깊게 들여다보도록 하겠습니다.

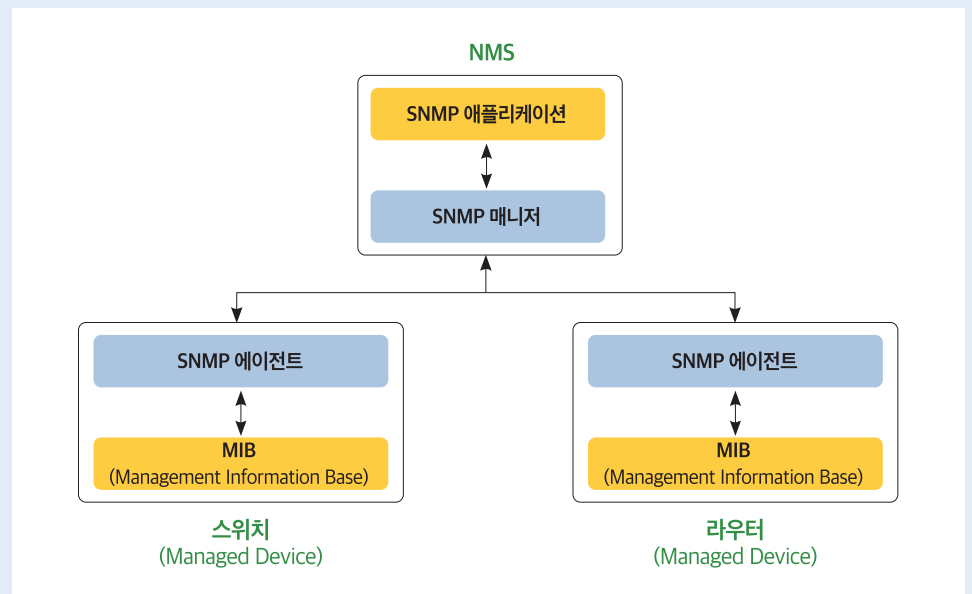


그림 4. SNMP 구성요소

NMS의 내부에서 동작하는 SW의 모듈은 크게 SNMP 애플리케이션과 SNMP 매니저로 나눌 수 있으며 이 둘의 상호작용을 통해 네트워크 장치의 상태를 모니터링하고 제어합니다. SNMP 매니저는 네트워크의 중앙 관리를 담당하며, Managed Device(라우터, 스위치, 서버 등)와 통신해 장치의 상태 정보를 요청하고, 응답을 받아 처리합니다. SNMP 애플리케이션은 SNMP 매니저의 기능을 실행하고 사용자에게 정보를 제공하는 역할을 합니다. SNMP 애플리케이션의 도움으로 관리자는 네트워크 상태를 시각적으로 모니터링하고 관리할 수 있습니다. 또한 SNMP 애플리케이션은 주기적으로 SNMP 매니저를 통해 네트워크 장치의 상태 정보를 수집하여 데이터베이스에 저장할 수도 있으며 수집된 데이터는 그래프나 도표 등의 형식으로 시각화되어 관리자에게 정보를 제공하고 특정 조건에 따라 관리자에게 경고 및 알림을 보낼 수도 있습니다.

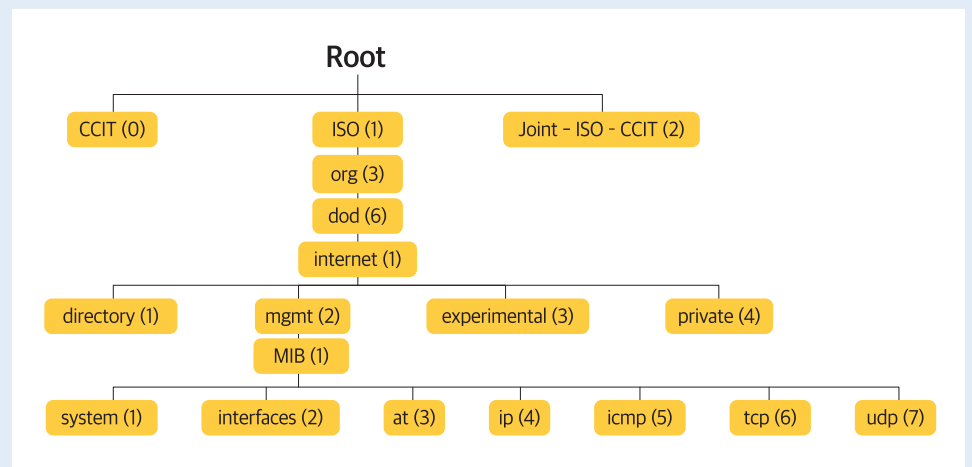


그림 5. OID(Object Identifier) 계층 구조

라우터, 스위치 등의 Managed Device에는 SNMP 에이전트와 MIB(Management Information Base)가 있습니다. SNMP 에이전트는 장치의 상태나 성능 데이터를 수집하며, SNMP 매니저가 요청하는 데이터에 응답하고, 필요한 경우 또는 특정 이벤트 발생 시 SNMP 매니저에 알림을 보냅니다. MIB(Management Information Base)는 네트워크 장치에서 관리하는 데이터 항목들을 계층적으로 정의한 데이터베이스와 같은 것입니다. MIB는 각 관리 항목을 고유하게 식별하기 위해 OID(Object Identifier)라는 것을 사용합니다. [그림 5]는 OID의 계층 구조를 나타낸 것이고, 현재 설명에 필요한 부분 이외에 생략된 부분도 많이 있습니다. [그림 5]의 루트부터 시작해서 좌에서 우로 계층별 요소를 나타내는 숫자를 콤마로 구분해서 나열한 1.3.6.1.2.1.1은 system 관련 데이터들에 관한 OID가 됩니다. 1.3.6.1.2.1.1의 하위 OID인 1.3.6.1.2.1.1.5는 시스템 이름을 나타내는 데이터의 OID로써 [그림 6]과같이 NMS가 시스템 이름을 나타내는 OID인 1.3.6.1.2.1.1.5로 해당 데이터를 요청하면 Managed Device인 스위치는 자신의 시스템 네임인 'SW-1'을 NMS에 응답합니다. OID는 공통으로 사용하는 것들도 있지만 제품이 특성에 따라 제조사별로 따로 정의된 것들도 존재해서 이에 대한 정보를 제공하는 인터넷 사이트가 있을 정도입니다.

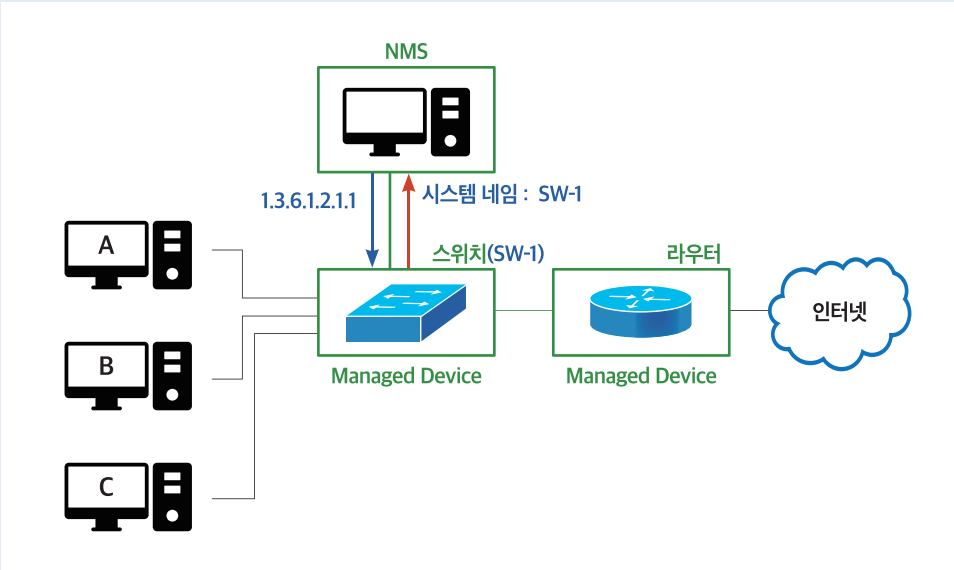


그림 6. OID를 통한 정보요청

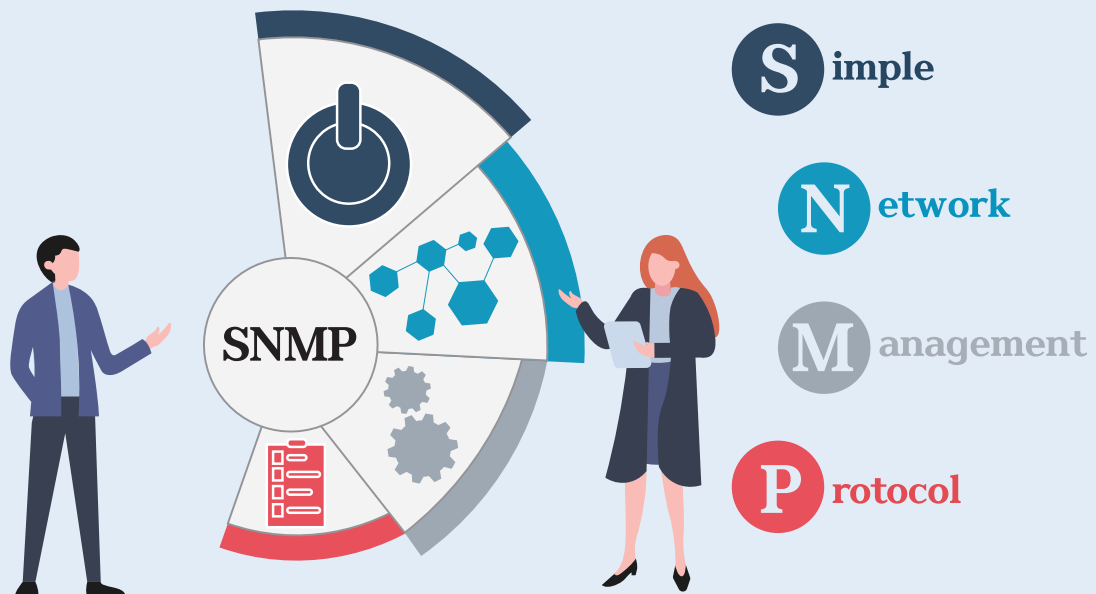
OID를 통해 주고받는 SNMP 메시지들의 종류와 기능은 [표 1]과 같습니다.

표 1. SNMP 메시지

| SNMP 메시지 | 기능 및 용도                                                                                                             |
|----------|---------------------------------------------------------------------------------------------------------------------|
| Get      | - 네트워크 장치의 현재 상태 정보(CPU 사용률이나 메모리 상태 등)를 가져오기 위해 주로 사용<br>- NMS가 장치에 특정 OID를 요청하면, 장치는 해당하는 값을 포함한 Response 메시지를 반환 |
| GetNext  | - 요청한 OID의 바로 다음 OID에 있는 값을 요청하여 MIB 전체 데이터를 순차적으로 조회                                                               |
| GetBulk  | - 다수의 값을 한꺼번에 요청하여 대규모 데이터 수집                                                                                       |

| SNMP 메시지 | 기능 및 용도                                                                                                                                                                                                        |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Set      | <ul style="list-style-type: none"> <li>- 네트워크 장치의 특정 값을 설정하거나 변경하기 위해 사용</li> <li>- NMS가 장치에 특정 OID 값을 변경하도록 요청하면, 장치는 변경 내용을 적용하고 Response 메시지로 결과를 반환</li> </ul>                                             |
| Response | <ul style="list-style-type: none"> <li>- Get, GetNext, GetBulk, 또는 Set 요청에 대한 응답을 반환하는 메시지</li> <li>- 요청한 정보의 성공적인 응답 값을 포함하거나, 에러가 발생했을 경우 에러 코드를 반환</li> </ul>                                               |
| Trap     | <ul style="list-style-type: none"> <li>- 네트워크 장치가 관리 시스템에 비동기적으로 알림을 보낼 때 사용</li> <li>- 요청에 의한 것이 아니라 장치에서 정의된 특정 이벤트가 발생하면 Trap 메시지를 NMS로 전송</li> <li>- 주기적인 요청 없이도 즉각적인 알림을 보장할 수 있어 실시간 모니터링에 유용</li> </ul> |
| Inform   | <ul style="list-style-type: none"> <li>- Trap과 유사하게 비동기적인 알림을 위한 메시지지만, Trap과 달리 Inform은 전송 후 응답을 요구</li> <li>- 장치가 Inform 메시지를 NMS로 보내면, NMS는 이를 확인하는 응답 메시지를 보냄</li> </ul>                                   |

지금까지 라우터, 스위치 등 다양한 네트워크 장치의 상태 데이터를 수집이나 설정 변경을 통해 네트워크 관리를 가능하게 하는 SNMP에 대해 간략히 알아보았습니다. 다음 편에도 여러분께 유용할 수 있는 주제로 다시 찾아뵙겠습니다. 



#### P.S.

C군이 여러분께 전하는 내용 중 전문적 성격이 짙은 것은 엄밀한 언어를 사용하여 설명하기에는 한계가 있습니다.  
본 내용은 설명하는 대상에 대한 전체적 맥락의 이해에만 이용하시고, 그 이상은 권위 있는 전문자료를 참고하시기 바랍니다.