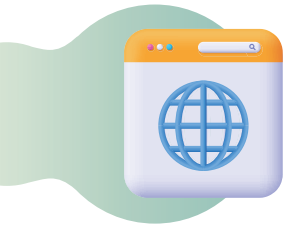

인터넷에서 사용되는 여러 기술

SNMP 이야기 1

Simple
Network
Management
Protocol

글.
조인준
KBS 미디어기술연구부 수석연구원

초기 인터넷 환경이 형성되던 시기에는 네트워크 규모가 비교적 작아서 네트워크 장비의 상태를 직접 확인하거나 단순한 관리 도구를 사용하여 운영하는 것이 가능했습니다. 그러나 인터넷이 급격히 확장되면서 네트워크는 점차 대형화되고 복잡해졌으며, 다양한 제조사의 장비와 서로 다른 통신 기술이 혼재하는 환경으로 발전하게 되었습니다. 이렇게 빠르게 규모가 커지는 네트워크 환경에서는 네트워크 전체 상태를 일관된 방식으로 관리하고 장애를 신속하게 파악하기 위한 체계적인 관리 기술이 필요해졌습니다. 특히 TCP/IP가 인터넷의 핵심 프로토콜로 자리 잡으면서, TCP/IP 기반 네트워크 환경을 효율적으로 관리할 수 있는 표준 기술의 필요성이 크게 대두되었습니다.

하지만 1980년대 초반까지는 TCP/IP 네트워크 관리를 위한 단일 표준이 존재하지 않았습니다. 당시 여러 연구 그룹과 표준화 단체에서는 각기 다른 접근 방식의 관리 기술을 개발하고 있었습니다. 대표적으로 국제 인터넷 표준화 기구인 IETF(Internet Engineering Task Force)의 공식 표준문서인 RFC(Request For Comments) 1021~1024에 정의된 HEMS(High-Level Entity Management System)/HEMP(High-Level Entity Management Protocol)는 고수준 관리 개념을 기반으로 설계된 기술이었으며, RFC 1028에 정의된 SGMP(Simple Gateway Monitoring Protocol)는 게이트웨이 장비 상태를 단순하게 모니터링하기 위한 프로토콜이었습니다. 또한 OSI 프로토콜 체계에서 개발된 CMIP(Common Management Information Protocol)는 기능적으로 강력했으나 구조와 구현 복잡도가 높아 TCP/IP 중심 인터넷 환경에서는 널리 채택되지 못했습니다.

이처럼 여러 기술이 경쟁하던 상황에서 IETF는 TCP/IP 환경에서 통합적으로 사용할 수 있는 네트워크 관리 표준이 필요하다는 점을 인식하게 되었습니다. 이에 따라 1988년 RFC 1052가 발표되었으며, 해당 문서는 SGMP를 기반으로 보다 확장 가능하고 범용적인 관리 프로토콜을 개발할 것을 권고했습니다. 이 권고를 바탕으로 SNMP(Simple Network Management Protocol)가 개발되었으며, SNMP 워킹 그룹(특정 기술 과제 해결과 표준 수립을 목적으로 하는 실무 기반의 전문가 조직)에 의해 현대 네트워크 관리에서 가장 널리 사용되는 표준 기술로 자리 잡았습니다.

SNMP는 기존 기술에 비해 구현의 복잡도를 획기적으로 낮추고 자원 소모를 최소화한 구조를 가지면서도, 다양한 장비에서 공통적으로 사용할 수 있는 범용성을 확보했습니다. 특히 관리 기능을 수행하는 네트워크 관리 시스템과 관리 대상이 되는 장비를 분리하고, 관리 정보를 표준화된 데이터 구조로 정의함으로써 제조사나 장비 유형에 관계없이 네트워크 상태를 통합적으로 관리할 수 있도록 하였습니다. 이러한 설계는 SNMP가 빠르게 확산하는 중요한 계기가 되었습니다.

초기 SNMP는 주로 라우터, 브리지(오늘날 스위치와 유사한 역할의 장비), 허브와 같은 네트워크 인프라 장비를 관리하기 위해 사용되었습니다. 그러나 인터넷과 네트워크 기술이 발전하면서 네트워크에 연결되는 장비의 종류가 급격히 다양해졌습니다. 이에 따라 SNMP 역시 단순한 네트워크 장비 관리 프로토콜을 넘어 네트워크에 연결된 다양한 장비를 관리할 수 있는 범용 관리 기술로 발전하게 되었고, 오늘날에는 네트워크 스위치나 라우터와 같은 전통적인 네트워크 장비뿐만 아니라 네트워크 프린터, 저장 장치, 각종 서버, 그리고 사물인터넷(IoT) 장치에 이르기까지 매우 다양한 장치에서 사용되고 있습니다. 이러한 확장은

SNMP가 장비의 내부 상태와 운영 정보를 표준화된 체계로 제공하는 유연성을 갖추었기에 가능했습니다. 종합하면, SNMP는 TCP/IP 기반 네트워크 확산과 함께 증가한 네트워크 관리 요구를 해결하기 위해 개발되었으며, 이후 지속적인 개선과 확장을 통해 오늘날 다양한 네트워크 기반 장비를 통합적으로 관리할 수 있는 대표적인 네트워크 관리 표준 기술로 자리 잡았습니다.

SNMP 개념과 의미

SNMP(Simple Network Management Protocol)는 이름에서 알 수 있듯이 네트워크 관리(Network Management)를 위한 프로토콜(Protocol)을 의미합니다. 여기에서 'Simple'이라는 표현은 절대적인 단순성을 의미하는 것이 아니라, 당시 존재하던 복잡한 네트워크 관리 프로토콜과 비교했을 때 상대적으로 단순한 구조를 지향한다는 의미를 가지고 있습니다. 실제로 초기 SNMP 역시 단순한 구조라고 보기는 어려웠고, 이후 버전이 높아지며 다양한 기능과 표준이 추가된 결과 현재의 SNMP는 상당히 복잡한 체계를 갖추게 되었습니다. 체계가 복잡해지다 보니 SNMP는 프로토콜이라는 이름을 가지고 있음에도 다른 네트워크 프로토콜들과 동일한 개념으로 이해하기에는 맞지 않는 측면을 가지고 있습니다. 낮은 수준에서 SNMP는 네트워크 장치 간에 관리 정보를 교환하기 위한 실제 통신 프로토콜을 의미합니다. 반면 보다 넓은 의미에서 SNMP는 단순 프로토콜의 범위를 넘어, 네트워크 관리 기능 및 이를 운영하는 체계 전반을 아우르는 개념으로 사용되기도 합니다.

인터넷 표준 관리 프레임워크 구조

SNMP 워킹 그룹이 설계한 TCP/IP 네트워크 관리 체계는 단일 프로토콜에 국한되지 않고, 여러 요소가 유기적으로 결합된 [그림 1]의 인터넷 표준 관리 프레임워크(Internet Standard Management Framework)라는 종합 아키텍처를 기반으로 합니다. 이 프레임워크는 전통적으로 세 가지 핵심 요소로 구성됩니다. 우선 관리 정보의 문법과 표현 규칙을 규정하는 SMI(Structure of Management Information)와 이 규칙에 따라 관리 대상 객체들을 체계적으로 집합시켜 놓은 데이터베이스인 MIB(Management Information Base)가 관리 정보의 토대를 이룹니다. 여기에 실제 정보를 주고받는 통신 규약인 SNMP 프로토콜이 더해져 네트워크 관리 기능이 구현됩니다. 또한 SNMPv3에서는 보안성과 접근 제어 강화를 위해 사용자 보안 모델과 접근 제어 모델 등 보안 및 운영 모델이 추가되어 전체 관리 체계의 중요한 구성 요소로 확장되었습니다. 표준화 초기에는 공식 명칭인 '인터넷 표준 관리 프레임워크'로 정의되었으나, 실제 운영 환경에서 SNMP가 핵심적인 역할을 수행함에 따라 오늘날에는 이를 관례적으로 SNMP 프레임워크(SNMP Framework) 또는 단순히 SNMP라 지칭하게 되었습니다. 이로 인해 통상 이 아키텍처 전체를 SNMP라는 용어로 부르는 경우가 많으므로, 맥락에 따라 SNMP가 데이터를 실어 나르는 통신 규약만을 의미하는지, 혹은 정보를 정의하고 관리하는 프레임워크 전반을 지칭하는지 명확히 구분하여 이해할 필요가 있습니다.

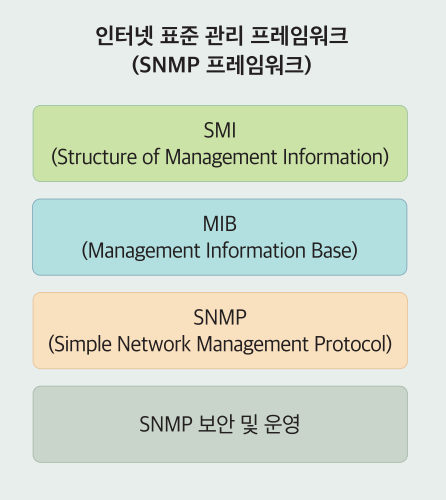

그림 1. 인터넷 표준 관리 프레임워크
(Internet Standard Management Framework)

SNMP 설계 원칙

SNMP와 인터넷 표준 관리 프레임워크는 다음과 같은 설계 원칙을 기반으로 구성되어 있습니다.

☑ SNMP는 다양한 네트워크 장비와 객체에 대한 관리 정보를 간단하게 정의하고, 관리 장치와 대상 장비 간에 해당 정보

를 교환할 수 있는 보편적인 방법을 제공하도록 설계

- ☑ 관리 정보의 정의와 통신 기능을 네트워크 관리 애플리케이션과 분리함으로써 관리 시스템의 확장성과 유연성 확보
- ☑ SNMP 프로토콜 자체는 비교적 소수의 이해하기 쉬운 연산으로 구성되어 구현 부담을 줄이도록 설계
- ☑ 장비 제조업체가 SNMP 기능을 비교적 쉽게 제품에 적용할 수 있도록 구현의 단순성과 표준화를 고려

SNMP 동작 계층과 전송 방식

SNMP는 TCP/IP 모델의 응용 계층에서 동작하는 네트워크 관리 프로토콜로 설계되었으며, 일반적으로 IP 네트워크 환경에서 사용됩니다. SNMP 메시지는 전송 계층 프로토콜 위에서 전달되며, 대부분의 구현에서는 경량성과 효율성을 위해 UDP(User Datagram Protocol)를 사용합니다. 하지만 SNMP는 필요에 따라 다른 전송 메커니즘 위에서도 동작할 수 있도록 설계되었으며, 최신 SNMP 표준에서는 TCP, TLS/DTLS 기반 보안 전송 등 다양한 전송 프로토콜 환경에서도 SNMP 정보를 전달할 수 있도록 전송 매핑 구조가 정의되어 있습니다.

SNMP 표준 발전 과정

SNMP 또한 시간이 흐름에 따라 네트워크 기술과 함께 발전해 왔으며, 여러 버전의 표준이 순차적으로 등장했습니다. 최초의 SNMP는 1988년에 발표되었으며 SNMPv1이라고 불립니다. SNMPv1은 구현이 비교적 용이하여 초기 네트워크 환경에서 널리 사용되었고, 다양한 장비에서 지원되면서 빠르게 확산되었습니다. 그러나 SNMPv1은 인증 및 접근 제어 기능이 제한적이어서 보안 측면에서 여러 취약점이 존재했습니다. 이러한 문제를 해결하기 위해 SNMPv2가 개발되었지만, 개발 과정에서 여러 표준안이 등장하면서 표준이 분산되는 문제가 발생하였습니다. 결과적으로 SNMPv2의 여러 표준안은 제한적인 사용에 그쳤으며 완전한 통합 표준으로 자리 잡지 못했습니다. 이후 이러한 문제를 해결하기 위해 SNMP 프레임워크와 프로토콜을 재정비한 SNMPv3가 발표되었으며, SNMPv3에서는 강력한 인증 및 암호화 기능이 추가되고 관리 프레임워크 구조가 정비되었습니다. 이를 통해 SNMP는 다시 단일 표준 관리 프로토콜로 통합되었으며, 현재까지도 네트워크 관리 분야에서 중요한 표준 기술로 활용되고 있습니다.

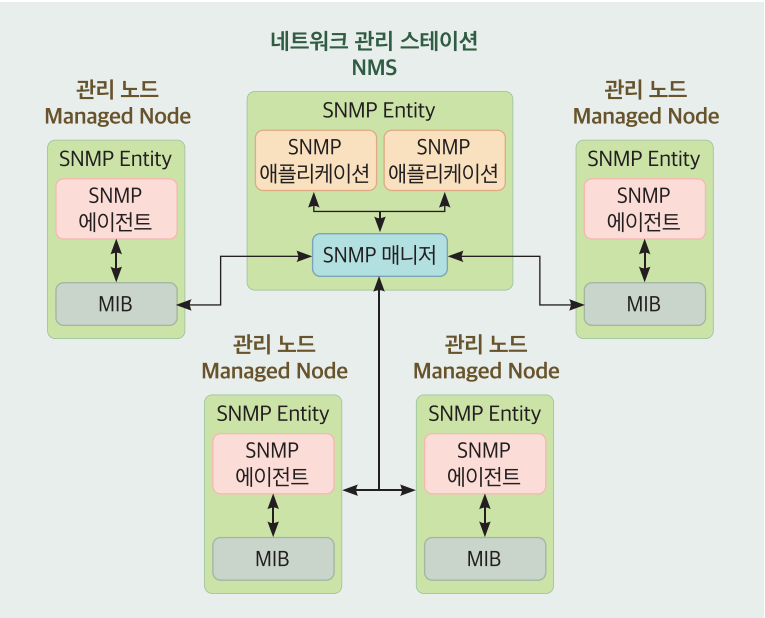

그림 2. SNMP 관리 시스템 구성 장치

SNMP 관리 모델과 동작 개념

SNMP(Simple Network Management Protocol)는 Simple 하다는 이름과 달리 다양한 버전과 표준, 그리고 활용 방식이 존재하는 비교적 복잡한 네트워크 관리 기술입니다. 따라서 SNMP를 올바르게 이해하기 위해서는 먼저 SNMP의 동작 모델과 TCP/IP 기반 네트워크 관리 시스템을 구성하는 요소, 그리고 관련 용어들을 살펴볼 필요가 있습니다. SNMP의 기본 목적은 TCP/IP 환경에서 네트워크 관리에 필요한 정보를 효율적으로 교환하는 것입니다. 이를 위해 SNMP는 네트워크 관리자가 특정 관리 장치를 활용하여 네트워크에 연결된 여러 장치들로부터 정보를 수집하고, 필요할 경우 해당 장치의 동작을 제어할 수 있도록 설계되었습니다. 이러한 구조에서 SNMP는 [그림 2]와 같이 크게 두 가지 유형의 장치를 정의하고 있습니다.

SNMP 관리 시스템 구성 장치

첫 번째는 네트워크 관리 스테이션(NMS, Network Management Station)입니다. NMS는 네트워크 관리 기능을 수행하기 위한 특수 소프트웨어를 실행하는 장치로, 관리 노드로부터 정보를 수집하고 제어 명령을 전달하는 역할을 수행합니다. 대규모 네트워크에서는 전용 고성능 장치가 NMS로 사용되기도 하지만, 실제로 NMS의 역할을 결정하는 것은 하드웨어가 아니라 소프트웨어이므로 하나의 장치가 다른 기능과 함께 NMS 역할을 동시에 수행할 수도 있습니다.

두 번째는 관리 노드(Managed Node)입니다. 관리 노드는 SNMP를 통해 관리될 수 있도록 관련 소프트웨어가 설치된 일반적인 네트워크 장치를 의미합니다. 대부분의 관리 노드는 TCP/IP 통신이 가능한 장치로 구성되며, 일반적인 호스트뿐 아니라 라우터, 허브, 스위치와 같은 네트워크 장비도 포함됩니다. 또한 프린터, 스캐너, 가전제품, 의료 장비 등 TCP/IP 네트워크에 연결될 수 있는 다양한 장치 역시 관리 노드가 될 수 있습니다.

SNMP Entity 구성 요소

SNMP 기반 네트워크 관리에 참여하는 모든 장치는 SNMP Entity라고 불리는 소프트웨어를 실행합니다. SNMP Entity는 SNMP 프로토콜의 기능을 구현하는 핵심 요소이며, 장치 유형에 따라 서로 다른 구성 요소로 이루어집니다.

네트워크 관리 스테이션의 SNMP Entity는 두 가지 요소로 구성됩니다. SNMP 매니저(SNMP Manager)는 SNMP 프로토콜을 구현하여 관리 노드의 SNMP 에이전트와 통신하며, 관리 정보를 수집하고 제어 명령을 전달하는 역할을 수행합니다. 또한 SNMP 애플리케이션(SNMP Application)은 네트워크 관리자가 SNMP 기능을 활용할 수 있도록 사용자 인터페이스와 관리 기능을 제공합니다.
관리 노드의 SNMP Entity 역시 두 가지 주요 요소로 구성됩니다. 첫 번째는 SNMP 에이전트(SNMP Agent)로 SNMP 프로토콜을 구현하여 관리 노드의 정보를 NMS에 제공하고, NMS로부터 전달되는 명령을 수신하여 장치 동작에 반영하는 소프트웨어입니다. 두 번째는 관리 정보 베이스(MIB, Management Information Base)로 관리 노드에 저장되는 관리 정보의 구조와 유형을 정의합니다. SNMP를 통해 교환되는 모든 정보는 MIB에 정의된 객체 형태로 표현됩니다.

SNMP 동작 구조 및 상호작용 방식

지금까지의 내용을 종합하면, SNMP는 소수의 네트워크 관리 스테이션이 다수의 관리 노드와 상호작용하는 구조로 동작합니다. NMS에서 실행되는 SNMP 매니저와 관리 노드에서 실행되는 SNMP 에이전트는 SNMP 프로토콜을 통해 관리 정보를 교환합니다. 또한 SNMP 애플리케이션은 관리자가 네트워크 상태를 모니터링하고 제어할 수 있도록 인터페이스를 제공하며, 각 관리 노드의 MIB에 저장된 정보를 활용하여 네트워크 관리 기능을 수행합니다. 이처럼 SNMP는 구조적으로 단순해 보일 수 있지만, 실제로는 다양한 장치와 관리 요소들이 유기적으로 연동되어 동작하는 정교한 네트워크 관리 체계를 형성하고 있습니다.

지금까지 보신 것과 같이 SNMP는 관리 주체와 대상이 유기적으로 맞물려 동작하는 체계입니다. 이어지는 글에서는 이러한 상호작용의 밑바탕이 되며 SNMP가 데이터를 정의하고 관리하는 구체적인 체계인 SMI와 MIB의 구조에 대해 다루어 보겠습니다.

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.