

수업 내용 정리 보고서

작성일: 2026년 7월 3일

챕터 구성

- [SNMP] 네트워크 관리 및 관제 프로토콜
- [Routing] 다이나믹 라우팅 프로토콜의 알고리즘과 비교
- [Practice] 인프라 운영 이슈 및 실무 설정 가이드

[SNMP] 네트워크 관리 및 관제 프로토콜

네트워크 규모가 커질수록 관리자가 모든 라우터, 스위치, 서버에 개별적으로 접속하여 상태를 확인하는 것은 불가능에 가깝습니다. 이를 해결하기 위해 네트워크 상의 장비들이 자신의 상태(CPU 온도, 네트워크 트래픽, 가동 시간 등)를 중앙에서 한눈에 파악할 수 있도록 표준화된 규격이 필요한데, 이것이 바로 **SNMP(Simple Network Management Protocol)**입니다. SNMP는 단순한 데이터 전송을 넘어, 네트워크 전체를 관제(Monitoring)하고 제어(Control)하는 데 초점이 맞춰진 프로토콜입니다.

1. SNMP의 핵심 구성 요소 및 통신 구조

SNMP 시스템은 정보를 요청하는 주체와 정보를 제공하는 주체, 그리고 실제 데이터를 가진 장치로 역할이 나뉩니다.

- **매니저(Manager):** 모니터링을 수행하는 서버입니다. 관리 대상 장비들에게 정보를 요청하고, 수집된 데이터를 해석하여 관리자에게 시각적으로 보여줍니다.
- **에이전트(Agent):** 모니터링을 받는 대상 장비(라우터, 스위치 등) 내에서 동작하는 소프트웨어입니다. 자신의 상태 정보를 MIB에서 찾아 매니저에게 전달합니다.
- **디바이스(Device):** MIB 정보를 실제로 수집하고 관리하는 물리적 장치 또는 소프트웨어입니다.

통신은 주로 **UDP(User Datagram Protocol)**를 사용하며, 각 역할에 따라 사용하는 포트가 다릅니다.

포트 번호	주체	용도 및 동작 방식
UDP 161	Agent	Manager의 MIB 정보 요청(Get/Set)에 응답하기 위해 항상 Listen 상태로 대기합니다.
UDP 162	Manager	Agent가 긴급 상황을 먼저 보고하는 Trap 또는 Inform 메시지를 받기 위해 대기합니다.

2. 데이터 구조: MIB와 OID

SNMP가 어떤 데이터를 주고받을지 결정하기 위해서는 일종의 '데이터 명세서'와 '주소 체계'가 필요합니다.

MIB (Management Information Base)

MIB는 장비가 관리하는 상태 정보들을 계층적(Tree) 구조로 정리해 놓은 데이터베이스 명세서입니다. 트리 구조를 채택함으로써 방대한 정보를 효율적으로 분류할 수 있습니다.

- **공통 항목:** 모든 네트워크 장비가 공통으로 가지는 정보(시스템 이름, Up-time 등)입니다.
- **Private MIB:** 제조사(Cisco, Juniper 등)마다 자신들의 장비 특성을 반영하여 별도로 만든 전용 항목입니다.

OID (Object Identifier)

MIB라는 트리 구조 내에서 특정 데이터가 어디에 위치하는지를 나타내는 '**숫자 주소**'입니다. 루트(.)에서 시작하여 하위 가지로 내려가며 점(.)으로 연결된 숫자들의 형태를 가집니다.

예시: 시스템 이름을 가져오고 싶다면 특정 OID 경로(예: 1.3.6.1.2.1.1.5.0)를 호출해야 합니다. 만약 상위 디렉토리 단계까지만 지정하여 요청할 경우, 해당 디렉토리에 속한 모든 관리 정보를 한꺼번에 가져오게 됩니다.

3. SNMP 동작 방식 및 알림(Notification)

SNMP는 기본적으로 Manager가 Agent에게 요청하는 방식과, Agent가 먼저 상황을 보고하는 방식 두 가지로 동작합니다.

기본 동작 (Get / Set)

- **SNMP Get:** Manager가 Agent의 MIB 정보를 읽어오는 동작입니다.
- **SNMP Set:** Manager가 Agent의 MIB 정보를 수정(세팅)하는 동작입니다.

알림 방식 (Notification: Trap vs Inform)

장비에 장애가 발생하는 등 긴급 상황(Emergencies, Alerts, Critical 등)이 발생했을 때, Agent가 Manager에게 먼저 보고하는 기능입니다. 이때 **신뢰성과 성능** 사이의 트레이드오프(Trade-off)가 발생합니다.

- **Trap:** Agent가 Manager에게 메시지를 던지기만 하고 끝납니다. UDP 기반이므로 메시지가 잘 전달되었는지 확인하는 절차(Ack)가 없습니다. 성능은 매우 좋지만, 메시지 유실 가능성이 있습니다.
- **Inform:** Trap과 유사하지만, Manager가 메시지를 잘 받았다는 확인 응답(Ack)을 보냅니다. UDP 위에서 Ack 과정을 흉내 내어 구현하며, Trap보다 신뢰성이 높지만 추가적인 통신이 발생하므로 성능은 다소 떨어집니다.

4. SNMP 버전별 차이점

보안성과 효율성에 따라 세 가지 버전으로 구분됩니다. 실무에서는 호환성과 편의성 때문에 v2가 가장 널리 쓰입니다.

버전	주요 특징	보안성	효율성
SNMPv1	최초의 버전. Community String을 인증에 사용.	낮음 (Plain Text)	낮음 (1회 요청 시 1개 데이터만 조회 가능)
SNMPv2	사실상의 표준(De-facto Standard).	낮음 (Plain Text)	높음 (GetBulkRequest 지원으로 대량 조회 가능)
SNMPv3	보안이 강화된 버전. 3단계 보안 등급 도입.	높음 (인증 및 암호화 지원)	높음 (Bulk Request 지원)

※ 주의사항: SNMPv1과 v2는 인증에 사용하는 'Community String'이 암호화되지 않은 평문(Plain Text)으로 전송됩니다. 따라서 패킷 스니핑에 매우 취약하므로, 보안이 중요한 환경에서는 반드시 SNMPv3 사용을 권장합니다.

5. 모니터링 생태계 및 관련 도구

SNMP로 수집된 데이터는 그대로는 사람이 읽기 어렵기 때문에, 이를 가공하고 시각화하는 도구들이 함께 사용됩니다.

- **snmpwalk**: Manager가 Agent의 MIB 정보를 트리 구조를 따라 훑으며(walk) 굼어올 때 사용하는 대표적인 툴입니다.
- **Cacti**: SNMP로 수집된 데이터를 자동으로 가공하여 웹 기반의 그래프로 보여주는 애플리케이션입니다.
 - **Cacti Spine**: PHP 스크립트 대신 C 언어로 작성된 멀티스레드 엔진을 사용하여 데이터 수집 속도를 높인 버전입니다.
- **RRD (Round Robin Database)**: Cacti 등이 데이터를 저장할 때 사용하는 방식입니다. 데이터가 오래될수록 해상도(상세도)를 낮추어 저장하거나 삭제함으로써, 정해진 용량 내에서 효율적으로 로그를 관리합니다.
- **fping**: 기존 ping의 확장 버전으로, 여러 호스트를 빠르게 점검할 수 있는 Fast-ping 도구입니다.

6. 실무 설정 (Cisco 환경 예시)

Cisco 장비에서 SNMP를 설정할 때는 접근 제어와 알림 설정을 함께 구성하는 것이 일반적입니다.

```
! 1. MIB 접근 범위 설정 (mib2 포함)
snmp-server view mib2 mib-2 included

! 2. 특정 ACL(Access-list)을 통한 접근 제어
access-list 10 permit any

! 3. Community String 설정 (Read-Only 권한, ACL 10 적용)
snmp-server community kong ro 10

! 4. Trap/Inform 전송 설정 (1.1.1.2 서버로 Inform 전송, 버전 2c 사용)
snmp-server host 1.1.1.2 informs version 2c kong
```

[학습 점검 체크리스트]

- **개념 확인**: SNMP에서 Manager와 Agent의 역할 차이를 설명할 수 있는가?
- **포트 식별**: Agent가 응답을 기다리는 포트(161)와 Manager가 Trap을 받기 위해 여는 포트(162)를 구분할 수 있는가?
- **비교 분석**: Trap과 Inform의 결정적인 차이점(Ack 유무)과 그에 따른 트레이드오프를 이해했는가?
- **버전 판별**: 왜 실무에서 v2를 많이 쓰며, 보안을 위해서는 왜 v3로 넘어가야 하는지 근거를 제시할 수 있는가?
- **실무 대응**: Community String이 평문으로 전송된다는 점이 모의해킹 관점에서 어떤 위험을 초래할 수 있는지 생각해보았는가?

[Routing] 다이나믹 라우팅 프로토콜의 알고리즘과 비교

네트워크 규모가 커짐에 따라 관리자가 모든 라우터의 경로 정보를 수동으로 입력하는 것은 불가능에 가깝습니다. **다이나믹 라우팅(Dynamic Routing)**은 라우터들이 서로 정보를 교환하며 최적의 경로를 스스로 결정하는 기술입니다. 이때 어떤 기준(Metric)으로 경로를 정하고, 어떤 방식으로 정보를 공유하느냐에 따라 프로토콜의 성격이 결정됩니다.

1. 라우팅 프로토콜의 분류 및 핵심 메커니즘

라우팅 프로토콜은 정보를 수집하고 전달하는 알고리즘에 따라 크게 세 가지 방식으로 나뉩니다. 각 방식은 '무엇을 기준으로 길을 찾느냐'의 차이가 있습니다.

프로토콜 종류	알고리즘 방식	핵심 기준 (Metric)	비유
RIP (Routing Information Protocol)	Distance Vector (거리 벡터)	Hop Count (최소 홉 수)	"지하철 역 개수가 가장 적은 노선을 선택한다."
OSPF (Open Shortest Path First)	Link State (링크 상태)	Cost (대역폭/속도 기반 가중치)	"역 개수가 많아도 급행열차(빠른 길)를 선택한다."
EIGRP (Enhanced Interior Gateway Routing Protocol)	Hybrid (RIP + OSPF)	Bandwidth, Delay 등 복합 요소	"속도와 응답 시간(지연)을 모두 고려한다."
BGP (Border Gateway Protocol)	Path Vector (경로 벡터)	Policy (정책 및 관리자 설정)	"속도보다 관리자의 정책(망 선택)을 따른다."

2. RIP (Routing Information Protocol) 심층 분석

RIP는 가장 단순한 형태의 프로토콜로, 이웃 라우터로부터 받은 라우팅 테이블 정보를 그대로 믿고 자신의 테이블을 업데이트하는 '소문 전파 방식'을 사용합니다.

RIPv1 vs RIPv2: 무엇이 달라졌는가?

실무에서는 보안과 효율성을 위해 반드시 RIPv2를 사용해야 합니다. 두 버전의 결정적인 차이는 다음과 같습니다.

- **전송 방식:** RIPv1은 모든 장비에 패킷을 뿌리는 **Broadcast**(255.255.255.255)를 사용하여 불필요한 트래픽을 유발하지만, RIPv2는 RIP 전용 **Multicast**(224.0.0.9) 주소를 사용하여 필요한 라우터만 수신하므로 효율적입니다.
- **서브넷 지원 (CIDR/VLSM):** RIPv1은 서브넷 마스크 정보를 포함하지 않는 **Classful** 방식입니다. 따라서 세밀하게 쪼개진 네트워크(VLSM)를 인식하지 못합니다. 반면 RIPv2는 마스크 정보를 포함하는 **Classless** 방식을 지원하여 현대적인 네트워크 설계가 가능합니다.

루프(Loop) 방지를 위한 방어 매커니즘

RIP는 지도 전체를 보지 못하고 이웃의 말만 믿기 때문에, 정보가 뱅글뱅글 도는 '라우팅 루프'에 빠질 위험이 큼니다. 이를 막기 위해 다음과 같은 기법을 사용합니다.

- **Split Horizon (수평 분할):** 특정 경로를 알려준 방향으로 다시 그 경로를 광고하지 않는 규칙입니다.
- **Poison Reverse (독약 역전파):** Split Horizon의 확장 개념으로, 경로가 끊겼을 때 해당 경로의 홉 수를 최대치(16)로 설정하여 되돌려줌으로써 즉각적인 불능 상태를 알립니다.
- **Route Poisoning (경로 포이즈닝):** 네트워크 장애 시 해당 경로의 홉 수를 16(도달 불가능)으로 설정하여 주변에 즉시 전파하는 방식입니다.
- **Triggered Update (트리거드 업데이트):** 주기적인(30초) 업데이트를 기다리지 않고, 장애 발생 즉시 정보를 쏘아 올려 변화를 빠르게 수습합니다.
- **Hold-down Timer:** 잘못된 정보가 떠도는 것을 막기 위해, 경로가 끊긴 후 일정 시간 동안 해당 경로에 대한 새로운 광고를 신뢰하지 않고 대기하는 시간입니다.

3. OSPF (Open Shortest Path First) 심층 분석

OSPF는 소문이 아닌 '지도 제작 방식'을 사용합니다. 모든 라우터가 네트워크 전체의 연결 상태를 파악하여 동일한 지도를 갖게 됩니다.

OSPF의 4단계 작동 절차

1. **이웃 탐색 (Hello):** Hello 패킷을 주기적으로 던져 인접한 라우터와 Neighbor 관계를 맺습니다.
2. **상태 광고 (LSA Flooding):** 자신의 연결 상태(선 속도, 연결 장비 등)를 담은 **LSA(Link State Advertisement)**를 작성하여 네트워크 전체에 뿌립니다.
3. **데이터베이스 구축 (LSDB):** 모든 라우터가 받은 LSA를 모아 **LSDB(Link State Database)**를 만듭니다. 이 결과, 모든 라우터는 동일한 네트워크 지도를 갖게 됩니다.
4. **최단 경로 계산 (SPF Algorithm):** 구축된 지도를 바탕으로 **Dijkstra(다익스트라) 알고리즘**을 실행하여 목적지까지 가장 비용(Cost)이 적게 드는 경로를 계산합니다.

[핵심 공식] OSPF Cost 계산

$$\text{Cost} = 10^8 / \text{Bandwidth(bps)}$$

대역폭(속도)이 커질수록 분모가 커지므로 Cost 값은 작아집니다. 즉, Cost가 낮은 경로가 최단 경로입니다.

4. 실무 주의사항: Auto-Summary와 불연속 네트워크 문제

라우팅 프로토콜을 설정할 때 가장 흔히 발생하는 실수 중 하나가 **Auto-Summary(자동 축약)** 기능입니다. 이 기능은 세부 네트워크 주소를 클래스 단위의 대표 주소로 묶어서 광고하여 라우팅 테이블의 용량을 줄여줍니다.

문제 상황 (Discontiguous Network): 만약 중간에 다른 대역의 네트워크가 끼어 있어 네트워크가 물리적으로 분리된 것처럼 보일 경우, Auto-Summary가 켜져 있으면 라우터들은 세부 주소를 구분하지 못하고 클래스 단위로만 인식합니다. 이로 인해 패킷이 엉뚱한 방향으로 전달되는 **블랙홀(Blackhole)** 현상이나 **루핑(Looping)**이 발생할 수 있습니다.

[실무 가이드] 현대의 VLSM/CIDR 환경에서는 반드시 **no auto-summary** 설정을 통해 자동 축약 기능을 꺼야 합니다.

5. 성능 지표: 컨버전스 타임 (Convergence Time)

네트워크 장애 발생 시 새로운 경로를 찾아 안정화되기까지 걸리는 시간을 **컨버전스 타임**이라고 합니다. 프로토콜별 성능 차이는 다음과 같습니다.

- **RIP (매우 느림):** Hold-down Timer 등으로 인해 경로 재설정에 수 분이 소요될 수 있습니다.
- **OSPF (빠름):** LSA Flooding과 즉각적인 SPF 계산을 통해 수초 내에 경로를 재구성합니다.
- **EIGRP (극도로 빠름):** 평소에 메인 경로(Successor) 외에 백업 경로(Feasible Successor)를 미리 계산해 두기 때문에, 장애 시 1초 미만의 즉각적인 전환이 가능합니다.

6. Cisco 실습 및 설정 가이드

Cisco 장비에서 RIP를 설정하고 검증하는 표준 절차입니다.

```
! 1. L3 라우팅 활성화 (스위치의 경우 필수)
Router(config)# ip routing

! 2. RIP 프로세스 진입 및 네트워크 광고
Router(config)# router rip
Router(config-router)# network 1.0.0.0           ! 서브넷화되지 않은 Major Network 등록
Router(config-router)# network 2.0.0.0
Router(config-router)# no auto-summary          ! [중요] 자동 축약 기능 해제

! 3. 설정 확인
Router# show ip protocols                       ! 실행 중인 프로토콜 및 설정값 확인
```

학습 점검 체크리스트

- RIPv1과 v2의 가장 큰 차이점 두 가지를 설명할 수 있는가? (힌트: 전송 방식과 서브넷 마스크 지원 여부)
- OSPF에서 대역폭이 넓은 선을 선택하는 이유는 무엇인가? (힌트: Cost 계산 공식)
- 왜 실무에서는 **no auto-summary** 설정을 반드시 확인해야 하는가? (힌트: 불연속 네트워크와 루핑 문제)
- 장애 발생 시 가장 빠르게 경로를 복구하는 프로토콜은 무엇인가? (힌트: EIGRP의 백업 경로 개념)

[Practice] 인프라 운영 이슈 및 실무 설정 가이드

현대 네트워크 인프라 운영의 핵심은 '**가시성 확보(Monitoring)**'와 '**효율적인 경로 제어(Routing)**'입니다. 본 장에서는 네트워크 장비의 상태를 관제하는 SNMP 프로토콜의 실무 적용 방법과, 복잡한 네트워크 환경에서 최적의 경로를 자동으로 찾아주는 다이나믹 라우팅 프로토콜의 운영 이슈 및 설정 가이드를 다룹니다.

1. SNMP를 이용한 네트워크 관제 및 모니터링

SNMP(Simple Network Management Protocol)는 네트워크상에 존재하는 다양한 호스트(라우터, 스위치, 서버 등)의 CPU 온도, 트래픽 상태, 인터페이스 활성화 여부 등 각종 상태 정보를 중앙에서 모니터링하고 제어하기 위한 표준 프로토콜입니다.

1.1 핵심 구성 요소와 동작 원리

- **Manager (관리 서버):** 모니터링을 수행하는 주체로, Agent에게 정보를 요청하거나 Agent가 보내는 알람을 수신합니다.
- **Agent (관리 대상 서버):** 자신의 상태 정보를 수집하여 Manager에게 제공하는 소프트웨어/칩셋입니다. 일반적으로 0번 LAN 포트가 Agent 포트로 사용되기도 합니다.
- **MIB (Management Information Base):** 장비가 수집하는 상태 정보의 '명세서'입니다. 계층형 트리(Tree) 구조로 되어 있어 효율적인 분류가 가능하며, 공통 항목 외에 제조사별 전용 항목(Private MIB)이 존재합니다.
- **OID (Object Identifier):** MIB 트리 내에서 특정 데이터가 위치한 '숫자 주소'입니다. 루트(.)부터 시작해 점으로 연결된 경로 형태를 띠며, 상위 디렉터리에서 조회를 멈추면 해당 하위의 모든 관리 정보를 가져옵니다.

1.2 SNMP 통신 방식 및 버전별 특징

SNMP는 UDP 기반으로 동작하며, 목적에 따라 161번(Agent 대기 포트)과 162번(Manager의 Trap/Inform 수신 포트)을 사용합니다.

구분	SNMPv1	SNMPv2 (사실상 표준)	SNMPv3
인증 방식	Community String (Plain Text)	Community String (Plain Text)	3단계 보안 등급 도입 (복잡한 설정)
요청 효율	단일 정보 조회 (트래픽 높음)	GetBulkRequest (다수 정보 일괄 조회)	Bulk Request 지원
특징	초기 버전	성능 향상, 하위 호환성 우수	보안성 강화, 설정 복잡

알림(Notification) 방식의 차이:

- **Trap:** Agent가 Manager에게 상황을 단순 전송합니다. UDP 기반이므로 수신 확인(Ack)을 하지 않아 성능은 좋으나 신뢰성이 낮습니다.

- **Inform:** UDP를 사용하지만 소프트웨어적으로 Ack 과정을 구현하여 수신 여부를 확인합니다. 신뢰성은 높으나 성능 부담이 있습니다.

1.3 실무 모니터링 툴 체인

- **snmpwalk:** Manager가 Agent의 MIB 트리 구조를 따라가며 모든 정보를 긁어올 때 사용하는 도구입니다.
- **Cacti:** SNMP로 수집된 데이터를 시각화하여 웹으로 보여주는 애플리케이션입니다. (RRDtool 기반)
 - **Cacti Spine:** PHP 기반의 기본 수집 방식보다 빠른 C언어 기반 멀티쓰레드 수집 엔진입니다.
- **RRD (Round Robin Database):** 로그 저장 시 고정된 용량을 유지하기 위해, 오래된 데이터일수록 해상도를 낮추어 저장하고 결국 삭제하는 순환 저장 방식입니다.
- **fping:** 일반 ping의 확장 버전으로, 다수의 호스트에 대해 빠르게 응답을 확인하는 Fastping 도구입니다.

2. 다이나믹 라우팅 프로토콜 분석

다이나믹 라우팅은 관리자가 직접 경로를 지정하는 정적 라우팅과 달리, 알고리즘에 따라 라우터 간에 지도 정보를 공유하고 최적의 경로(Metric)를 스스로 결정합니다.

2.1 프로토콜별 특성 및 경로 결정 기준(Metric)

프로토콜	알고리즘 유형	결정 기준 (Metric)	주요 특징
RIP	Distance Vector	홉 수 (Hop Count)	최소 홉수 경로 중심, 소규모 네트워크용
OSPF	Link State	비용 (Cost / 대역폭)	전체 지도 작성, 대규모 인프라 표준
EIGRP	Hybrid	복합 Metric (속도, 지연 등)	Cisco 전용, 매우 빠른 수렴 속도
BGP	Path Vector	정책 (Policy)	국가/통신사 간 외부 네트워크 연결 (Backbone)

2.2 RIP (Routing Information Protocol) 심층 분석

RIP는 이웃 라우터가 전해주는 라우팅 테이블을 주기적으로 복사하는 '소문 전파' 방식입니다.

RIPv1 vs RIPv2 차이점:

- **전송 방식:** v1은 브로드캐스트(255.255.255.255)를 사용하여 모든 장비에 부하를 주지만, v2는 멀티캐스트(224.0.0.9)를 사용하여 RIPv2 활성화 장비만 수신합니다.
- **서브넷 지원:** v1은 클래스 기반(Classful)으로 서브넷 마스크 정보를 보내지 않으나, v2는 CIDR/VLSM을 지원하여 마스크 정보를 함께 전송합니다.

루핑(Loop) 방지 메커니즘:

- **Split Horizon (수평 분할):** 정보를 배운 방향으로 다시 그 정보를 광고하지 않아 무한 뱅뱅이를 차단합니다.
- **Route Poisoning (경로 포이즈닝):** 네트워크 다운 시 홉 수를 16(도달 불가능)으로 설정하여 즉시 전파합니다.
- **Poison Reverse:** 포이즈닝된 경로를 받았을 때, 확인 차원에서 다시 16홉으로 되돌려 보내줍니다.
- **Triggered Update:** 30초 주기를 기다리지 않고 장애 발생 즉시 업데이트 패킷을 전송합니다.
- **Hold-down Timer:** 한 번 죽은 경로가 다시 살아났다고 보고될 때, 일정 시간 대기하여 잘못된 정보가 퍼지는 것을 방지합니다.

2.3 OSPF (Open Shortest Path First) 동작 프로세스

OSPF는 테이블을 복사하는 것이 아니라, 전체 네트워크의 '상태 명세서'를 공유하여 직접 지도를 그립니다.

1. **Neighbor 탐색:** Hello 패킷을 통해 동일 세그먼트(라우터 없이 직접 연결된 동일 서브넷 대역) 내의 이웃을 찾습니다.
2. **LSA 전파 (Flooding):** 자신의 링크 상태(속도, 연결 상태)가 담긴 LSA(Link State Advertisement) 명세서를 전체 영역에 뿌립니다.
3. **LSDB 구축:** 수집된 모든 LSA를 모아 모든 라우터가 동일한 전체 네트워크 지도(Topology Map)를 가집니다.
4. **SPF 계산:** 다익스트라(Dijkstra) 알고리즘을 사용하여 비용(Cost = 10^8 / 대역폭)이 가장 낮은 최단 경로를 계산해 라우팅 테이블에 등록합니다.

3. 실무 운영 이슈 및 주의사항

3.1 자동 요약(Auto-Summary)과 불연속 네트워크 문제

자동 요약은 세부 주소(예: 172.16.1.0/24)를 대표 주소(172.16.0.0/16)로 묶어 광고함으로써 라우팅 테이블 크기를 줄이는 기능입니다. 하지만 **불연속 네트워크(Discontiguous Network)** 환경에서는 치명적인 오류를 유발합니다.

사고 시나리오: A지사(172.16.1.0)와 B지사(172.16.2.0) 사이에 다른 대역의 망이 있을 때, 두 지사 라우터가 모두 "나 172.16.0.0/16 가지고 있음"이라고 광고하면 중간 라우터는 목적지가 양쪽에 있다고 판단하여 패킷을 번갈아 던지는 로드밸런싱을 수행하고, 결국 패킷이 유실되는 블랙홀 현상이 발생합니다.

따라서 현대의 VLSM/CIDR 환경에서는 **no auto-summary** 설정이 필수적입니다.

3.2 컨버전스 타임(Convergence Time) 비교

컨버전스 타임이란 네트워크 변화 발생 시 모든 라우터가 새로운 경로로 업데이트되는 데 걸리는 시간입니다.

- **RIP (매우 느림):** Hold-down Timer 등으로 인해 수 분이 소요될 수 있습니다.
- **OSPF (빠름):** LSA 플러딩과 즉각적인 SPF 계산으로 수 초 이내에 완료됩니다.
- **EIGRP (극도로 빠름):** DUAL 알고리즘을 통해 백업 경로(Feasible Successor)를 미리 계산해 두므로 1초 미만으로 전환됩니다.

4. Cisco 장비 실무 설정 가이드

4.1 SNMP 설정 예시

```
snmp-server view mib2 mib-2 included      ! MIB 뷰 설정
access-list 10 permit any                  ! 접근 제어 리스트
snmp-server community kong ro 10           ! 커뮤니티 이름 'kong', Read-Only 권한, ACL 10 적용
snmp-server host 1.1.1.2 informs version 2c kong ! Manager 서버로 Inform 전송 설정
```

4.2 RIP 설정 예시

```
conf t
ip routing      ! L3 라우팅 활성화 (스위치의 경우 필수)
router rip      ! RIP 설정 모드 진입
network 1.0.0.0 ! 광고할 메이저 네트워크(Class 단위) 등록
network 2.0.0.0
no auto-summary ! 자동 축약 비활성화 (실무 핵심 설정)
exit
show ip protocols ! 설정 확인
```

[종합 점검 체크리스트]

- **SNMP 보안:** Community String이 Plain Text로 전송되는 v2를 사용 중인가? 보안이 중요하다면 v3 도입을 고려했는가?
- **라우팅 루프:** RIP 운영 시 Split Horizon 및 Route Poisoning이 정상 작동하고 있는가?
- **경로 최적화:** 단순히 홉 수만 따지는 RIP보다 대역폭을 고려하는 OSPF/EIGRP가 필요한 환경인가?
- **설정 누락:** RIP 설정 시 no auto-summary 명령어를 입력하여 불연속 네트워크 문제를 방지했는가?
- **가시성 확인:** Cacti나 snmpwalk를 통해 Agent의 MIB 정보가 정확히 수집되고 있는가?