

수업 내용 정리 보고서

작성일: 2026년 7월 28일

챕터 구성

- IGP/EGP 개념 및 EIGRP 동작 원리
- EIGRP 네트워크 안정화 및 SIA 방지 기술
- EIGRP 경로 제어 및 보안 설정
- 실무 운영 및 트러블슈팅 점검 가이드

IGP/EGP 개념 및 EIGRP 동작 원리

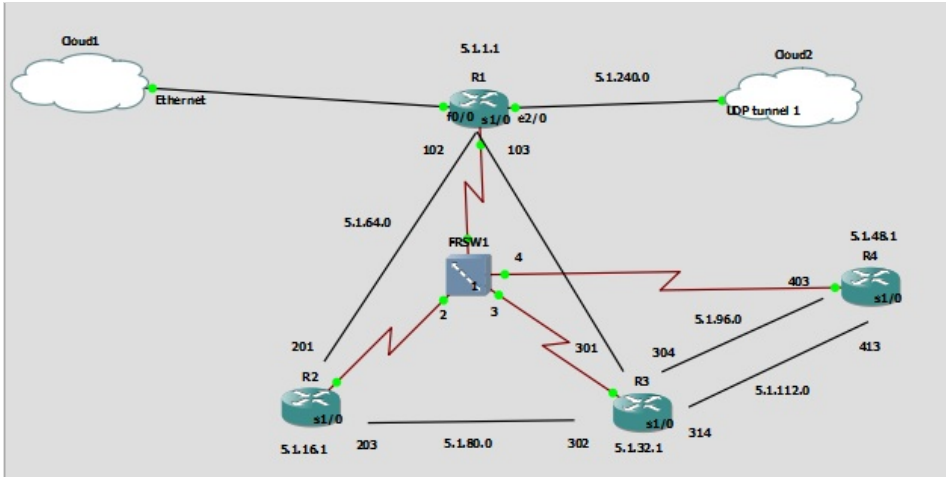
라우팅 프로토콜은 네트워크의 규모와 관리 주체에 따라 크게 IGP(Interior Gateway Protocol)와 EGP(Exterior Gateway Protocol)로 구분됩니다. IGP는 하나의 자율 시스템(AS, Autonomous System) 내부에서 라우팅 정보를 교환하기 위해 사용되며, EIGRP와 OSPF가 대표적인 예입니다. 반면, EGP는 서로 다른 AS 간에 라우팅 정보를 교환할 때 사용되는 프로토콜입니다.

1. 네트워크 구성 환경

본 실습에서는 IGP 프로토콜 중 하나인 EIGRP의 동작을 이해하기 위해 다음과 같은 네트워크 토폴로지를 구성하였습니다. R1 라우터는 Cloud1 및 Cloud2와 연결되어 외부망과의 접점 역할을 수행하며, FRSW1 스위치를 중심으로 R2, R3, R4 라우터가 유기적으로 연결되어 있습니다.

네트워크의 전체적인 연결 관계와 각 인터페이스의 IP 주소 할당 현황은 아래 구성도를 통해 확인할 수 있습니다.

R1(5.1.1.1)을 포함한 각 라우터의 IP 주소와 인터페이스 및 링크별 네트워크 대역 정보



R1, R2, R3, R4 라우터와 FRSW1 스위치 및 Cloud가 연결된 전체 네트워크 구성도

이 구성도에서 각 라우터 간의 링크는 특정 네트워크 대역(예: 5.1.16.0, 5.1.80.0 등)으로 연결되어 있으며, 이는 향후 EIGRP의 요약(Summarization) 및 쿼리(Query) 범위를 결정하는 기초 자료가 됩니다.

2. EIGRP의 핵심 동작 원리

EIGRP(Enhanced Interior Gateway Routing Protocol)는 DUAL(Diffusing Update Algorithm)이라는 알고리즘을 사용하여 루프가 없는 최적의 경로를 계산합니다. EIGRP는 단순히 경로를 찾는 것을 넘어, 장애 발생 시 즉각적인 복구를 위해 다음과 같은 개념을 활용합니다.

- **Successor (S)**: 토폴로지 테이블에서 계산된 가장 최적의 경로(Optimal Path)를 의미합니다.
- **Feasible Successor (FS)**: Successor가 사용할 수 없을 때를 대비해 미리 계산해 둔 백업 경로(Alternative Path)입니다.
- **Topology Table (P → A)**: 네트워크의 상태 변화에 따라 경로(Preferred)에서 대안(Alternative)으로 전환되는 과정을 관리합니다.

만약 현재 사용 중인 Successor 경로에 문제가 생겼을 때, 즉시 사용할 수 있는 Feasible Successor가 있다면 네트워크는 중단 없이 경로를 전환합니다. 하지만 적절한 FS가 없다면, 라우터는 인접한 라우터들에게 해당 경로를 알고 있는지 묻는 **Query(쿼리)** 과정을 거치게 됩니다. 이때 응답을 기다리는 **Reply(리플라이)** 과정이 수반됩니다.

주의사항: 플래핑(Flapping) 현상

네트워크 링크가 매우 짧은 간격으로 연결과 끊김을 반복할 경우, '파도타기 현상'이라고 불리는 플래핑이 발생할 수 있습니다. 이는 전체 네트워크에 지속적인 업데이트를 발생시켜 CPU 부하를 높이고 안정성을 저해하므로 주의가 필요합니다.

3. SIA(Stuck In Active)와 장애 대응 메커니즘

EIGRP 운영 중 가장 경계해야 할 상태 중 하나는 **SIA(Stuck In Active)**입니다. 이는 라우터가 Query를 보냈으나, 특정 인접 라우터로부터 제한 시간 내에 Reply를 받지 못해 '활성 상태(Active)'에 갇혀 버리는 현상을 말합니다.

이를 방지하고 네트워크 전체로 장애가 확산되는 것을 막기 위해 다음과 같은 메커니즘이 작동합니다.

- **RTO(Retransmission Timeout) 및 네이버 단절**: 일반적으로 RTO 설정에 따라 일정 시간(예: 3분) 동안 응답이 없으면, 해당 라우터는 인접 관계(Neighbor, AN)를 강제로 단절하여 네트워크 전체가 쿼리 응답을 기다리며 멈추는 것을 방지합니다.
- **Stub 설정**: 말단 라우터를 **Stub**으로 설정하면, 해당 라우터는 '말단인 척'을 하여 다른 라우터들로부터 Query를 받지 않도록 플래그를 설정할 수 있습니다. 이는 RTO 문제를 우회하고 쿼리 범위를 줄이는 매우 효과적인 방법입니다.
- **Redistribute(재분배)를 통한 제한**: 외부 경로를 재분배할 때, Query의 양이 무분별하게 확산되지 않도록 재분배 범위를 적절히 제한하여 설계해야 합니다.

4. 경로 최적화 및 관리 기법

네트워크의 효율성을 높이기 위해 다음과 같은 관리 명령 및 기법들이 사용됩니다.

기법	설명 및 목적
Offset-list	특정 인터페이스를 통과하는 경로의 Metric(비용)을 인위적으로 조정하여 경로 선택에 영향을 줍니다.
Key Chain	라우팅 업데이트 시 인증(Authentication)을 적용하여 보안을 강화합니다.
수동 축약 (Manual Summarization)	여러 개의 세부 네트워크를 하나의 메이저 네트워크로 묶어 광고합니다.

[실무 포인트] 수동 축약과 쿼리 발생 조건

수동 축약된 메이저 네트워크를 사용할 때, 쿼리가 발생하는 시점은 매우 중요합니다. 축약된 네트워크에 포함된 **모든 호스트(NI, Network Interface/Nodes)**가 **모두 다운되어야만** 해당 메이저 네트워크에 대한 쿼리가 발생합니다. 즉, 축약된 대역 내에 단 하나의 호스트라도 살아있다면 쿼리 확산을 차단할 수 없습니다.

5. 학습 내용 점검 체크리스트

- EIGRP에서 Successor와 Feasible Successor의 차이점을 설명할 수 있는가?
- SIA 현상이 발생하는 근본적인 원인과 이를 방지하기 위한 Stub의 역할을 이해했는가?
- RTO(3분 규칙)가 네트워크 안정성에 어떻게 기여하는지 알고 있는가?
- 수동 축약(Summarization)이 Query의 범위를 어떻게 제한하는지 파악했는가?
- 플래핑(Flapping) 현상이 발생했을 때 네트워크에 미치는 영향을 인지하고 있는가?

EIGRP 네트워크 안정화 및 SIA 방지 기술

네트워크 라우팅 프로토콜은 내부 네트워크(IGP, Interior Gateway Protocol)와 외부 네트워크(EGP, Exterior Gateway Protocol)로 구분됩니다. EIGRP(Enhanced Interior Gateway Routing Protocol)는 대표적인 IGP로서, 빠른 수렴(Convergence)과 효율적인 경로 계산을 위해 **DUAL(Diffusing Update Algorithm)** 알고리즘을 사용합니다. 하지만 네트워크 규모가 커지고 토폴로지가 복잡해질수록 경로의 변동이 전체 네트워크에 영향을 미치는 불안정성 문제가 발생할 수 있습니다.

1. 네트워크 불안정성: 플래핑(Flapping)과 파도타기 현상

네트워크 경로가 지속적으로 살아났다 죽었다를 반복하는 현상을 **플래핑(Flapping)**이라고 합니다. 특정 구간에서 발생한 플래핑은 라우팅 업데이트를 통해 인접 라우터로 전달되며, 마치 파도가 치듯 네트워크 전체로 확산되는 **파도타기 현상**을 유발합니다. 이는 불필요한 CPU 자원 소모와 대역폭 낭비를 초래하여 네트워크 전체의 성능을 저하시킵니다.

2. SIA(Stuck-In-Active) 발생 원인과 DUAL 알고리즘

EIGRP의 핵심인 DUAL 알고리즘은 최적 경로를 잃었을 때, 인접 라우터들에게 새로운 경로를 알고 있는지 묻는 **Query(Q?)** 과정을 거칩니다. 이때 라우터의 상태는 다음과 같은 흐름을 보입니다.

- **Passive(P) 상태:** 경로 정보가 안정적이며 별도의 확인 작업이 필요 없는 상태입니다.
- **Active(A) 상태:** 경로를 잃어버려 인접 라우터들에게 Query를 보내고 응답(Reply)을 기다리는 상태입니다.

만약 특정 라우터가 Query를 보냈음에도 불구하고, 네트워크 지연이나 장비 부하 등으로 인해 인접 라우터로부터 적절한 응답을 받지 못하면 해당 라우터는 **SIA(Stuck-In-Active)** 상태에 빠지게 됩니다. SIA가 지속되면 라우터는 더 이상 경로를 계산하지 못하고 멈춰 있게 되며, 이를 방지하기 위해 **RTO(Retransmission Timeout)** 메커니즘이 동작합니다.

RTO(Retransmission Timeout) 주의사항: EIGRP 환경에서 RTO가 약 3분을 초과하여 지속될 경우, 해당 라우터는 문제를 일으키는 이웃(AN, Adjacent Neighbor)과의 관계를 단절(Down)시켜 네트워크 전체의 마비를 막으려 시도합니다.

3. EIGRP 네트워크 안정화 및 SIA 방지 기술

SIA 현상을 방지하고 Query의 범위를 제한하여 네트워크를 안정화하기 위해서는 다음과 같은 설계 전략이 필요합니다.

① Stub 설정 (말단 노드 최적화)

라우터를 **Stub**로 설정하면, 해당 라우터는 인접 라우터에게 "나는 말단(Leaf) 노드이므로 나에게서 Query를 보내지 마라"는 플래그를 전달합니다. 이를 통해 Query가 불필요하게 말단 노드까지 전달되는 것을 차단하여 RTO 발생 가능성을 획기적으로 줄일 수 있습니다.

② 재분배(Redistribution)를 통한 범위 제한

서로 다른 라우팅 프로토콜 간의 경계에서 **재분배(Redistribute)**를 적절히 활용하면, Query가 전파되는 범위를 물리적/논리적으로 제한할 수 있습니다. 이는 특정 영역의 경로 변동이 전체 네트워크로 확산되는 것을 막는 방어선 역할을 합니다.

③ 수동 축약(Manual Summary) 활용

네트워크 규모를 줄이기 위해 **수동 축약(Manual Summary)**을 사용합니다. 축약된 메이저 네트워크(Major Network)를 사용하면 Query의 범위를 줄일 수 있습니다. 단, 주의할 점은 **축약된 메이저 네트워크에 속한 모든 호스트(NI)가 동시에 불능 상태가 되어야만** 해당 구간에 대한 Query가 발생한다는 점입니다. 따라서 적절한 축약은 Query의 양을 효과적으로 조절합니다.

④ 기타 관리 도구

- **Offset-list:** 메트릭(Metric) 값을 조정하여 특정 경로의 우선순위를 변경함으로써 경로의 안정성을 확보합니다.
- **Key Chain:** EIGRP 인증을 위해 사용하며, 보안을 강화하여 비인가된 라우터에 의한 경로 변동을 방지합니다.

이번 실습에서는 아래와 같은 토폴로지 환경에서 IGP 프로토콜인 EIGRP가 어떻게 동작하며, 이러한 안정화 기술들이 왜 필요한지를 학습합니다.

구성도를 살펴보면 R1이 상단에서 Cloud1, Cloud2와 연결되어 있으며, 하단의 R2, R3, R4 라우터가 FRSW1 스위치와 다양한 링크로 복잡하게 연결되어 있습니다. 이러한 다중 경로 환경에서는 하나의 링크 플래핑이 전체 네트워크의 Query 폭풍(Query Storm)으로 이어질 수 있으므로 SIA 방지 기술이 필수적입니다.

[학습 정리 및 점검 리스트]

점검 항목	확인 내용 및 기준
SIA 발생 여부	DUAL 상태가 Passive에서 Active로 전환된 후 응답(Reply)이 오지 않는지 확인
Stub 설정 확인	말단 라우터에 Stub 플래그가 설정되어 Query 전파를 차단하고 있는지 확인
축약 범위 검증	Manual Summary 적용 시, 하위 호스트의 장애가 전체 Query로 이어지지 않는지 확인
RTO 임계치	네이버 단절이 발생하기 전, Query 응답 시간이 3분 이내로 유지되는지 점검

실무 포인트: 대규모 네트워크 설계 시, 모든 라우터를 Query의 대상으로 두지 마십시오. Stub 설정과 적절한 Summary를 통해 Query의 전달 범위를 "계층화"하는 것이 네트워크 안정성의 핵심입니다.

EIGRP 경로 제어 및 보안 설정

오늘 학습한 내용은 내부 경로 결정 프로토콜(IGP, Interior Gateway Protocol) 중 하나인 **EIGRP(Enhanced Interior Gateway Routing Protocol)**의 안정성 확보와 경로 제어, 그리고 보안 설정에 관한 것입니다. 네트워크가 복잡해질수록 라우터 간의 경로 업데이트가 빈번해지며, 이 과정에서 발생하는 불안정성을 어떻게 제어하고 보안을 강화할 것인지가 핵심입니다.

1. 네트워크 구성 환경

실습에 사용된 네트워크 토폴로지는 R1, R2, R3, R4의 4개 라우터와 FRSW1 스위치, 그리고 외부와 연결된 Cloud 환경으로 구성되어 있습니다. 각 라우터는 고유한 IP 주소를 할당받아 연결되어 있으며, 이들 사이에서 EIGRP 프로토콜이 동작하며 최적의 경로를 계산하게 됩니다.

- **R1:** 5.1.1.1
- **R2:** 5.1.16.1
- **R3:** 5.1.32.1
- **R4:** 5.1.48.1

전체적인 연결 관계와 각 인터페이스의 IP 대역을 통해 라우팅이 이루어지는 흐름을 파악할 수 있습니다.

이 구성도는 이후 설명할 EIGRP의 쿼리(Query) 범위와 SIA(Stuck-In-Active) 현상이 발생할 수 있는 구조적 배경을 보여줍니다.

2. EIGRP 동작 원리와 불안정성 분석

EIGRP는 **DUAL(Diffusing Update Algorithm)** 알고리즘을 사용하여 루프 없는 최적 경로를 계산합니다. 하지만 네트워크의 특정 경로가 끊기거나 상태가 변할 때(Flapping), 다음과 같은 연쇄적인 반응이 일어날 수 있어 주의가 필요합니다.

DUAL 알고리즘과 상태 변화

라우터는 경로 정보의 상태를 관리합니다. 특정 네트워크에 대한 정보가 안정적일 때는 **Passive(P)** 상태를 유지하지만, 경로에 문제가 생겨 새로운 경로를 찾아야 할 때는 **Active(A)** 상태로 전환됩니다. 즉, **Topology: P → A** 과정이 발생합니다.

쿼리(Query)와 플래핑(Flapping) 현상

경로가 Active 상태가 되면, 라우터는 인접한 네이버(Neighbor)들에게 "이 경로를 알고 있느냐"라고 묻는 **Query(Q?)**를 보냅니다. 이에 대해 상대 라우터는 답변인 **Reply(Rep)**를 보내야 합니다. 만약 네트워크의 링크가 계속해서 붙었다 떨어졌다는 반복하는 **플래핑(Flapping)** 현상이 발생하면, 이러한 쿼리와 응답이 네트워크 전체로 퍼져나가는 **파도타기 현상**이 발생하여 네트워크 자원을 과도하게 소모하게 됩니다.

SIA (Stuck-In-Active)와 RTO

가장 심각한 문제는 쿼리를 보낸 라우터가 일정 시간 동안 응답(Reply)을 받지 못할 때 발생합니다. 이를 **SIA(Stuck-In-Active)**라고 합니다. EIGRP에는 이를 방지

하기 위한 RTO(Retransmission Timeout) 메커니즘이 있습니다. 일반적으로 RTO(15) 설정에 따라 3분이 지나도록 응답이 없으면, 해당 네이버(AN, Adjacency Neighbor)와의 관계를 단절하여 더 이상의 무한한 대기를 방지합니다.

3. 네트워크 안정화 및 SIA 방지 전략

네트워크 규모가 커질수록 쿼리의 범위가 넓어져 SIA 발생 확률이 높아집니다. 이를 방지하기 위한 세 가지 주요 전략을 학습했습니다.

- Stub 설정:** 특정 라우터를 **Stub**로 설정하면, 해당 라우터는 네트워크의 말단(End-node)인 것처럼 동작합니다. 이 플래그를 설정하면 주변 라우터들이 해당 라우터에게는 쿼리를 보내지 않게 되어, 쿼리 범위를 제한하고 RTO를 우회하는 효과를 얻을 수 있습니다.
- Redistribute (재분배) 활용:** 다른 프로토콜(EGP 등)과의 재분배를 통해 쿼리의 전파 범위를 물리적/논리적으로 제한함으로써 쿼리의 양을 관리할 수 있습니다.
- 수동 축약 (Manual Summarization):** 네트워크를 요약하여 광고하면 쿼리 발생 빈도를 획기적으로 낮출 수 있습니다. **수동 축약된 메이저 네트워크의 경우, 해당 네트워크에 속한 모든 호스트(NI, Network Interface)가 동시에 죽어야만 쿼리가 발생하기** 때문입니다. 이는 국소적인 장애가 네트워크 전체의 쿼리 폭풍으로 번지는 것을 막아줍니다.

4. 경로 제어 및 보안 설정

경로의 우선순위를 조절하거나 인가되지 않은 라우터의 접근을 막기 위한 설정 방법입니다.

- offset-list:** 특정 경로의 메트릭(Metric) 값을 인위적으로 조정하여, 트래픽이 선호하는 경로로 흐르도록 유도하는 경로 제어 기법입니다.
- key chain:** EIGRP 네이버 간의 인증을 위해 사용됩니다. 암호화된 키 체인을 설정함으로써 인가되지 않은 장비가 라우팅 정보를 주고받는 것을 차단하는 보안 기능을 수행합니다.

학습 요약 및 점검 리스트

실무 및 시험 관점에서 다음 사항을 반드시 확인하십시오.

점검 항목	핵심 내용	주의 사항
SIA 발생 여부	Query 후 Reply가 지연되는지 확인	3분(RTO) 경과 시 네이버 단절 주의
Stub 활용	말단 라우터에 Stub 설정 적용 여부	Stub 설정 시 해당 라우터로의 경로 학습 제한됨
축약 효과	Manual Summary를 통한 쿼리 범위 제한	모든 호스트 장애 시에만 쿼리 발생 확인
보안 설정	Key chain을 통한 인증 적용	키 불일치 시 Neighbor 형성 불가

[Self-Check Question]

- 네트워크 경로가 Active 상태로 전환될 때, 어떤 알고리즘이 작동하며 어떤 상태 변화가 일어나는가?
- SIA 현상을 방지하기 위해 Stub 설정을 사용하면 왜 쿼리 전파가 줄어드는가?
- 수동 축약을 적용했을 때, 쿼리가 발생하는 조건은 무엇인가?

실무 운영 및 트러블슈팅 점검 가이드

1. 네트워크 구성 및 학습 개요

오늘 실습에서는 IGP(Interior Gateway Protocol), 그중에서도 **EIGRP** 프로토콜의 동작 원리와 네트워크 안정성을 저해하는 요소들을 분석하였습니다. 먼저 전체적인 라우팅 환경을 파악하기 위해 구축된 토폴로지를 점검하였습니다.

네트워크는 R1을 중심으로 Cloud1, Cloud2와 연결되어 있으며, 내부적으로는 FRSW1 스위치를 통해 R2, R3와 연결됩니다. 또한 R3와 R4 사이의 링크를 포함하여 R1, R2, R3, R4 라우터가 유기적으로 연결된 구조를 가지고 있습니다. 각 인터페이스에는 5.1.1.1, 5.1.240.0, 5.1.64.0, 5.1.16.1 등 각기 다른 네트워크 대역이 할당되어 라우팅이 이루어집니다.

이 구성도는 향후 프로토콜의 Query 전파 범위와 SIA(Stuck-In-Active) 현상이 발생할 수 있는 지점을 파악하는 기초 자료로 활용됩니다.

2. IGP(EIGRP)의 안정성 저해 요소 분석

라우팅 프로토콜이 동작할 때, 특정 경로의 상태가 급격히 변하면 네트워크 전체에 영향을 줄 수 있습니다. 오늘 학습한 핵심 이슈는 크게 세 가지입니다.

- 플래핑(Flapping) 현상:** 링크나 인터페이스가 매우 짧은 간격으로 Up/Down을 반복하는 현상입니다. 이는 네트워크 전체에 **파도타기 현상(Wave Effect)**을 일으켜, 경로 계산을 반복하게 만듦으로써 CPU 부하를 가중시키고 네트워크 불안정을 초래합니다.
- DUAL 알고리즘과 Query 과정:** EIGRP는 DUAL(Diffusing Update Algorithm)을 사용하여 최적 경로를 계산합니다. 만약 최적 경로가 사라지면 라우터는 인접 라우터에게 **Query(Q?)**를 보내 새로운 경로를 확인하며, 이에 대한 응답(Reply)을 기다리는 과정을 거칩니다.
- SIA(Stuck-In-Active) 발생:** Query를 보낸 라우터가 인접 라우터로부터 일정 시간 내에 응답(Rep)을 받지 못할 경우, 해당 라우터는 SIA 상태에 빠지게 됩니다. 이는 경로 계산 프로세스가 멈춰버리는 심각한 상황을 의미합니다.

3. 트러블슈팅 및 안정화 전략

SIA 현상과 플래핑으로 인한 네트워크 마비를 방지하기 위해 실무에서 적용할 수 있는 대응 방안들을 정리하였습니다.

① SIA 방지 및 RTO 관리

SIA 상태가 지속되는 것을 막기 위해 **RTO(Retransmission Timeout)** 메커니즘이 작동합니다. 일반적으로 RTO 설정값에 따라 **약 3분이 경과하면** 응답이 없는 네이버(Neighbor, AN)를 단절(Down)시켜, 잘못된 경로 정보가 네트워크에 머물지 않도록 강제 조치합니다.

② Stub 설정을 통한 Query 범위 제한

Stub 설정을 활용하면 특정 라우터를 '말단 노드'인 것처럼 플래그(Flag)를 설정할 수 있습니다. Stub 라우터는 더 이상 경로 전달자가 아닌 말단으로 인식되므로, 상위 라우터가 Query를 보낼 때 이 라우터로는 Query를 보내지 않게 되어 RTO 발생 가능성을 획기적으로 줄일 수 있습니다.

③ 재분배(Redistribution) 및 수동 축약(Manual Summarization)

Query의 양을 물리적으로 제한하는 방법입니다.

- **Redistribute:** 다른 프로토콜과의 재분배를 통해 Query가 전파되는 경계를 설정함으로써, Query가 무분별하게 전체 네트워크로 퍼지는 것을 제한합니다.
- **수동 축약:** 네트워크 대역을 하나로 묶어 광고함으로써 라우팅 테이블을 단순화합니다. 중요한 점은 **수동 축약된 메이저 네트워크 내의 모든 호스트(NI)가 죽어야만** 해당 경로에 대한 Query가 발생한다는 것입니다. 즉, 개별 호스트의 장애가 전체 네트워크의 Query 폭풍으로 이어지는 것을 차단하는 효과가 있습니다.

④ 기타 관리 도구

- **Offset-list:** 특정 경로의 Metric(비용)을 조절하여 트래픽 경로를 제어합니다.
- **Key Chain:** 라우팅 프로토콜 간의 인증(Authentication)을 설정하여 보안성을 강화합니다.

4. 실무 운영 점검 체크리스트

네트워크 운영 중 라우팅 불안정이 감지될 경우, 다음 순서로 점검을 수행해야 합니다.

점검 단계	확인 항목	판단 기준 및 조치
1단계: 현상 파악	인터페이스 Flapping 여부	특정 링크의 Up/Down 반복 시 물리 계층(L1/L2) 점검
2단계: SIA 확인	Neighbor 상태 및 RTO 발생 여부	3분 이상 응답 없는 Neighbor가 있다면 Stub 설정 검토
3단계: Query 제어	Query 전파 범위 및 축약 상태	Query 범위가 너무 넓다면 수동 축약 또는 Redistribution 경계 설정
4단계: 보안 및 메트릭	Key Chain 및 Offset-list 적용	인증 설정 및 경로 최적화 상태 확인

주의사항: 수동 축약을 적용할 때는 축약된 범위 내의 네트워크가 모두 유효한지 확인해야 합니다. 만약 축약된 범위 전체가 불통이 되면 오히려 대규모 Query가 발생할 수 있으므로 주의가 필요합니다.