2021/01/15, 2021 보안 기초 세미나

TCP/IP 완벽 가이드

- 2-7부 TCP/IP 라우팅 프로토콜 -

박 재 형(jaehyoung@pel.sejong.ac.kr)

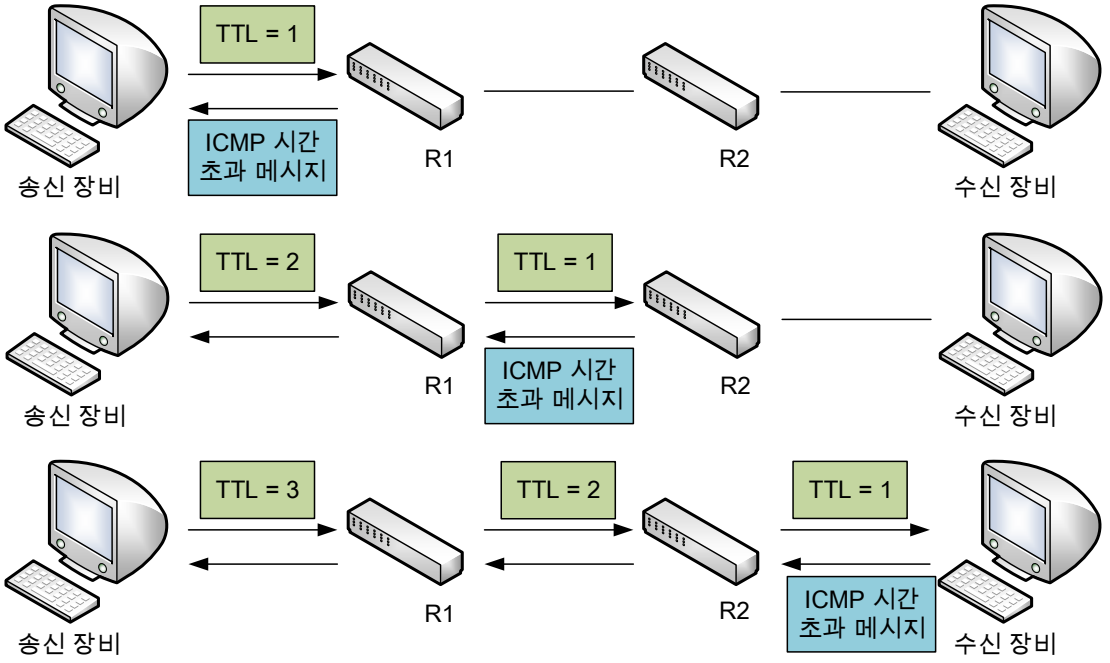
세종대학교 프로토콜공학연구실

목 차

- 보충
- 라우팅 프로토콜
- 라우팅 정보 프로토콜(RIP)
- 최단 경로 우선 프로토콜(OSPF)
- 경계 경로 프로토콜(BGP)
- 기타 라우팅 프로토콜

보충

- ICMPv4 경로 추적 메시지
  - Traceroute 유틸리티
    - 동작과정
      - 송신 장비는 수신장비에게 테스트 메시지 TTL값을 1, 2, 3 등과 같이 증가시켜 보냄
      - 수신장비는 테스트 메시지를 버리고 시간초과 메시지를 돌려 보냄



보충

- ICMPv4 경로 추적 메시지
  - 라우터의 순서를 파악하기 위해 사용되는 메시지
  - Traceroute 유틸리티를 이용하여 수행됨
  - 동작과정
    - 송신 장비가 수신 장비에게 Traceroute IP 옵션을 포함하여 하나의 데이터그램을 송신함
    - 송신 장비와 수신 장비 사이의 각 라우터는 옵션을 인지하고 송신장비에게 ICMP 경로 추적 메시지를 송신함

라우팅 프로토콜

- 정의
  - 라우터간 통신에서 패킷이 목적지까지 가능 방법을 결정해주는 프로토콜
- 알고리즘 분류

알고리즘	설명
거리 벡터(Distance Vector) 프로토콜 알고리즘	• 자신의 라우팅 테이블을 전송하여 라우터는 정해진 경로로 패킷을 전송함
링크 상태(Link State) 프로토콜 알고리즘	• 현재 네트워크에 있는 라우터들의 테이블을 모두 저장하여 접근 가능한지 검사하고 경로를 지정하여 패킷을 전송함 • 테이블은 지속적으로 갱신함 • 목적지 서브넷, 다음 홉 정보 등을 포함
혼합 라우팅 프로토콜 알고리즘	• 거리 벡터 알고리즘으로 동작하지만, 다음 홉 정보 등을 포함하여 패킷을 전송함 • 목적지 서브넷, 다음 홉 정보 등을 포함

라우팅 프로토콜

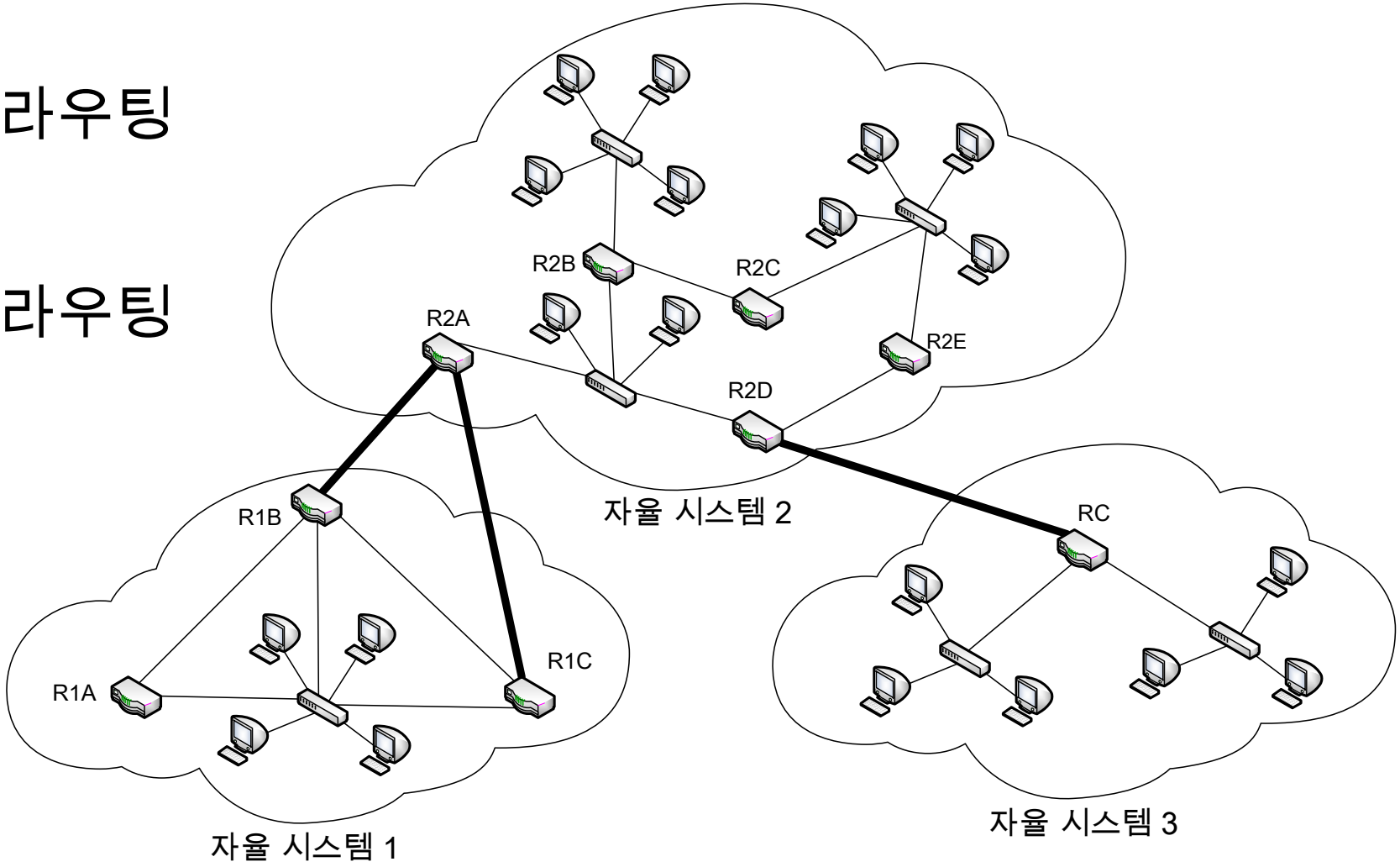
- 자율 시스템 구조(AS, Autonomous System)
  - 네트워크 환경에서 라우팅을 관리하기 위해 라우터를 그룹으로 묶은 구조
    - 라우터 그룹으로 이루어져 있으며 특정 기관이나 관리 기구에서 독립적으로 관리
  - 프로토콜 유형
    - 내부 라우팅 프로토콜(IGP, Interior Gateway Protocol)
      - AS 내부에서 라우팅 정보를 공유하기 위해 사용되는 프로토콜
      - e.g., RIP, OSPF 등
    - 외부 라우팅 프로토콜(EGP, Exterior Gateway Protocol)
      - AS 간 라우팅 정보를 공유하기 위해 사용되는 프로토콜
      - e.g., BGP 등

라우팅 프로토콜

- 자율 시스템 구조(AS, Autonomous System)
  - 라우터 종류
    - 내부 라우터(Internal router)
      - 같은 AS에 있는 라우터에만 접속 가능
      - 내부 라우팅 프로토콜 사용
    - 경계 라우터(Border router)
      - AS 내부에 있는 라우터 뿐만 아니라 다른 AS에 있는 라우터와 통신 가능
      - 내부/외부 라우팅 프로토콜 모두 사용

라우팅 프로토콜

- 자율 시스템 라우팅 구조
  - 얇은 선
    - 내부 라우팅
  - 굵은 선
    - 외부 라우팅



라우팅 정보 프로토콜(RIP)

- RIP(Routing Information Protocol)
  - 최소 홉 수를 파악하여 라우팅하는 프로토콜
  - 가장 오래되고 널리 사용되는 내부 라우팅 프로토콜

  - 특징
    - 홉 수를 기준으로 경로가 설정되는 거리 벡터 알고리즘 사용

    - 각 라우터는 30초를 주기로 라우팅 테이블의 경로 정보를 브로드캐스팅하여 업데이트

    - 최대 홉 수가 15홉으로 한정되어 크기가 작은 자율 시스템에 사용됨

라우팅 정보 프로토콜(RIP)

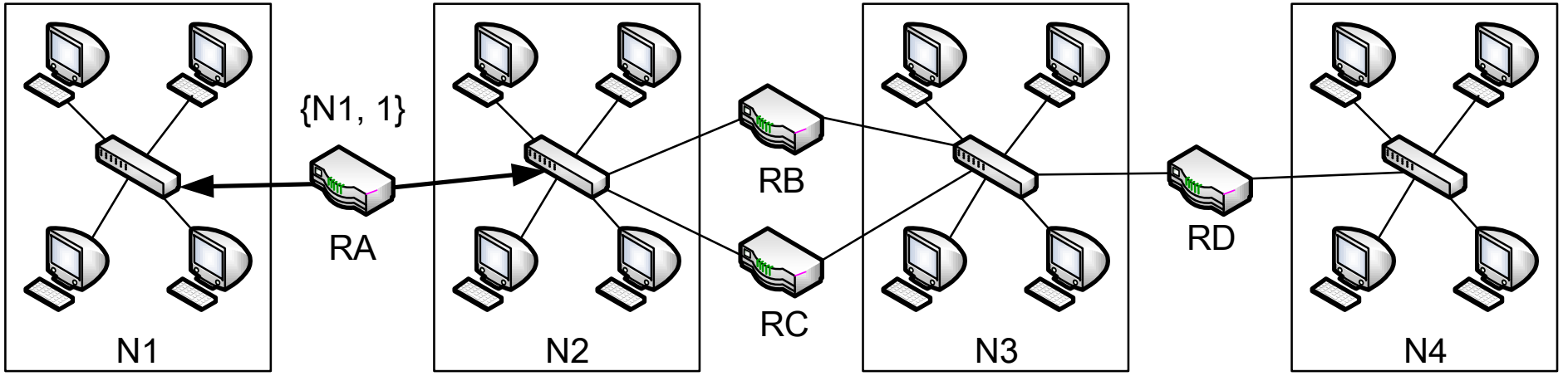
- RIP(Routing Information Protocol)
  - 버전
    - RIP-1
      - 1998년, “Routing Information Protocol”로 RFC 1058 문서에 정의
    - RIP-2
      - 1998년 “RIP Version 2”로 RFC 2453 문서에 정의
      - 기존 RIP-1에서 새로운 포맷을 정의하고 기능을 추가함
        - e.g., 클래스 비사용 주소지정, 인증, 멀티캐스트 등
    - RIPng
      - 1997년 “RIPng for IPv6”로 RFC 2080 문서에 정의
      - IPv6와의 호환성을 위해 새로 만들어진 버전

라우팅 정보 프로토콜(RIP

- 경로 결정 알고리즘
  - 경로 정보를 교환하여 라우팅 테이블을 갱신
    - 주요 저장 정보
      - 네트워크나 호스트의 주소
      - 라우터에서 네트워크나 호스트까지의 거리
      - 라우터에서의 첫 번째 홉
        - 네트워크나 호스트로 패킷을 보낼 때, 처음 보내는 곳

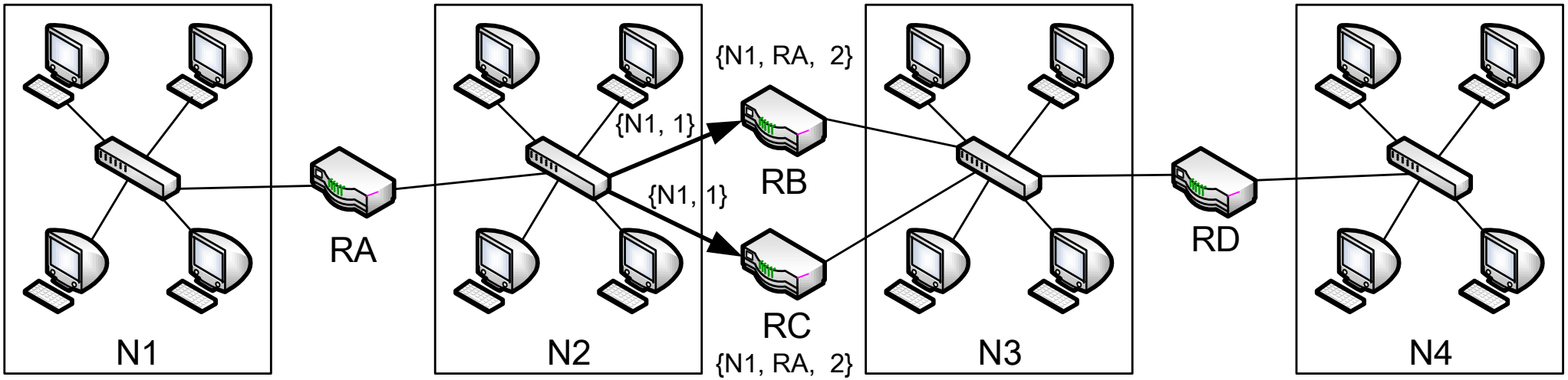
라우팅 정보 프로토콜(RIP)

- 경로 결정 알고리즘
  - 네트워크 라우팅 정보 전파(1/5)
    - 라우터 RA는 RIP 메시지에 {N1, 1}을 실어 연결된 네트워크에 전달
      - {N1, 1}: 네트워크 N1에 가기 위한 경로 비용 1
    - 네트워크 N2에 있는 RB, RC 라우터가 정보를 받음



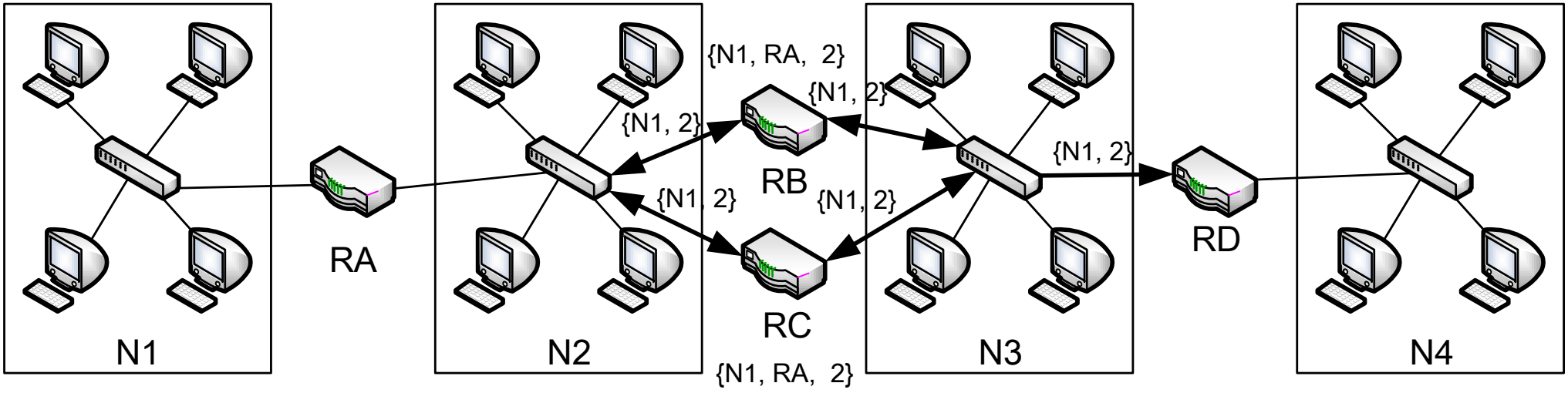
라우팅 정보 프로토콜(RIP)

- 경로 결정 알고리즘
  - 네트워크 라우팅 정보 전파(2/5)
    - 라우터 RB, RC는 라우팅 테이블에 N1에 관한 정보가 있는지 살펴봄 (N1에 관한 정보가 없다고 가정)
    - 라우터 RA 항목에 {N1, 2}를 저장



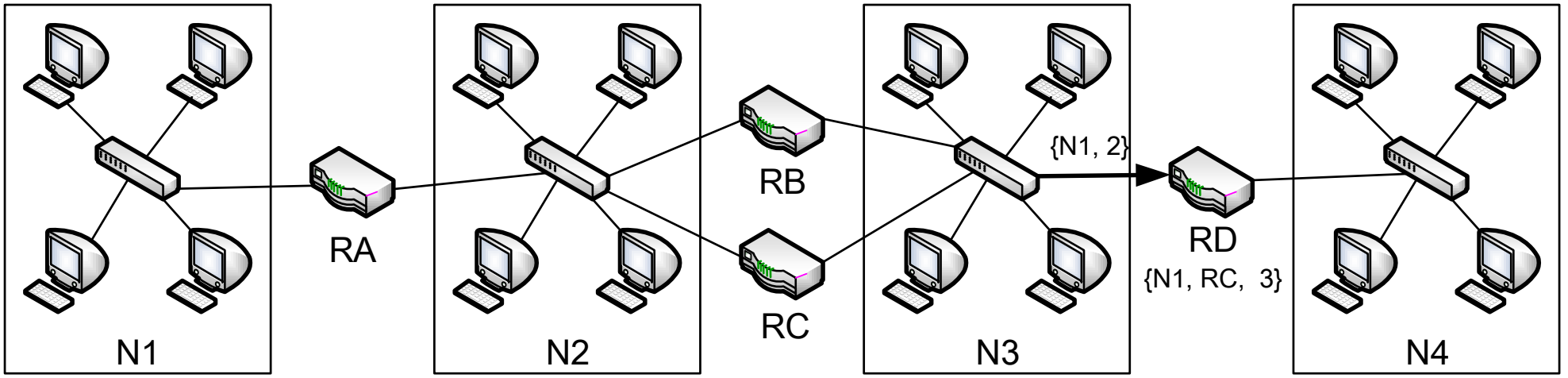
라우팅 정보 프로토콜(RIP)

- 경로 결정 알고리즘
  - 네트워크 라우팅 정보 전파(3/5)
    - 라우터 RB, RC는 자신이 연결된 네트워크인 N2와 N3에 라우팅 테이블 전송
    - N3에 있는 RD도 메시지를 받음



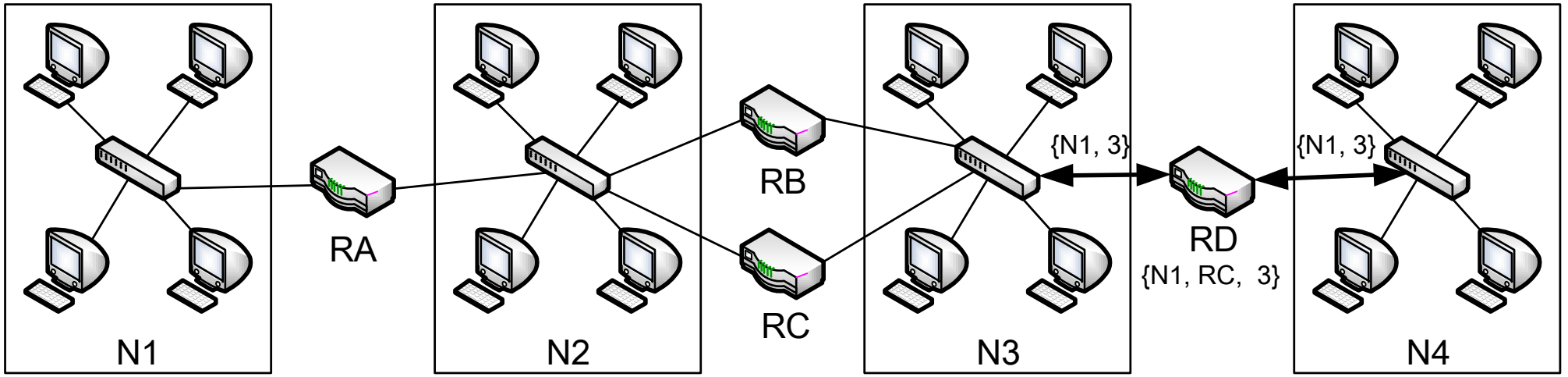
라우팅 정보 프로토콜(RIP)

- 경로 결정 알고리즘
  - 네트워크 라우팅 정보 전파(4/5)
    - 라우터 RD는 라우팅 테이블에 N1에 관한 항목이 없는지 조사함
    - RB, RC에 대한 {N1, 3}을 테이블에 추가
      - N1에 관해서는 RB, RC 둘 중 어느 것에 대해 생성해도 상관없음



라우팅 정보 프로토콜(RIP)

- 경로 결정 알고리즘
  - 네트워크 라우팅 정보 전파(5/5)
    - 라우터 RD가 네트워크 N4로 {N1, 3}을 송신하지만 수신할 라우터가 없음



라우팅 정보 프로토콜(RIP)

- 메시지와 유형
  - RIP 요청(RIP Request) 메시지
    - 다른 라우터의 라우팅 테이블 일부 또는 전부를 요청하는 메시지
    - 라우터가 네트워크에 처음 연결되는 등의 특정 상황에서 사용
  - RIP 응답(RIP Response) 메시지
    - 다른 라우터의 라우팅 테이블 일부 또는 전부를 전송하는 메시지
    - RIP 요청 메시지의 응답 이외에도, 주기적으로 라우팅 테이블을 갱신하기 위해 사용됨
  - RIP 메시지는 UDP를 이용하여 통신
    - RIP-1, RIP-2는 UDP 520번 포트 사용
    - RIPng는 UDP 521번 포트 사용

라우팅 정보 프로토콜(RIP)

- 타이머
  - 갱신(Update) 타이머
    - 최신 경로를 유지하지 위한 타이머(30초)
    - 주기적으로 라우팅 테이블을 브로드/멀티캐스트 전송
  - 만료(Timeout) 타이머
    - 오래된 정보를 방지하기 위한 타이머(180초)
      - 경로가 라우팅 테이블에 저장되는 시간을 한정 시킴
    - RIP 응답 메시지가 오면 초기화
    - RIP 응답 메시지가 오지 않으면 만료된 거리에 대해 곧 삭제된다는 것을 표시함(척도 필드 값: 16)

라우팅 정보 프로토콜(RIP)

- 타이머
  - 가비지 콜렉션 (Garbage Collection) 타이머
    - 유효하지 않은 경로를 찾아 제거하기 위한 타이머(120초)
      - 만료 타이머로 인한 삭제 표시 후, 시작되는 타이머
    - 타이머가 만료될 경우
      - 경로 삭제
    - 타이머가 만료되기전 RIP 응답 메시지를 받는 경우
      - 해당 경로의 타이머를 중단하고 삭제 후, 갱신 타이머 시작(30초)

라우팅 정보 프로토콜(RIP)

- 문제점
  - 느린 수렴(Slow Convergence)
    - 네트워크에서 일어난 변화가 모든 라우터로 전파되기까지 오랜 시간이 걸리는 현상
      - RIP 응답 메시지 사용으로 30초 간격의 시간 소요 때문
  - 라우팅 루프(Routing Loop)
    - 라우터 간 경로 정보가 반복되는 현상
    - e.g., 라우터 A가 네트워크 1로 갈 수 있는 항목을 가지고 라우터 B는 네트워크 1로 패킷을 보내기 위해서는 라우터 A로 보내는 테이블을 가질 때, 발생
  - 무한 세기(Counting to Infinite)
    - 느린 수렴 시간으로 인해 라우터가 잘못된 경로를 라우터 사이에서 계속 주고 받는 현상

라우팅 정보 프로토콜(RIP)

- 문제점
  - 작은 무한 값(척도 필드 값: 16)
    - 느린 수렴 문제를 줄이기 위해 크기가 작은 무한 값을 사용
    - 작은 무한 값 때문에 RIP를 사용하는 네트워크는 크기를 원하는 만큼 확장할 수 없는 문제
      - 최대 홉 수 15
  - 척도 문제
    - 경로를 측정하는 기준을 홉 수로만 판단
      - 속도나 거리 지연 등을 고려하지 않아 최적의 경로 선정에 비효율적

라우팅 정보 프로토콜(RIP)

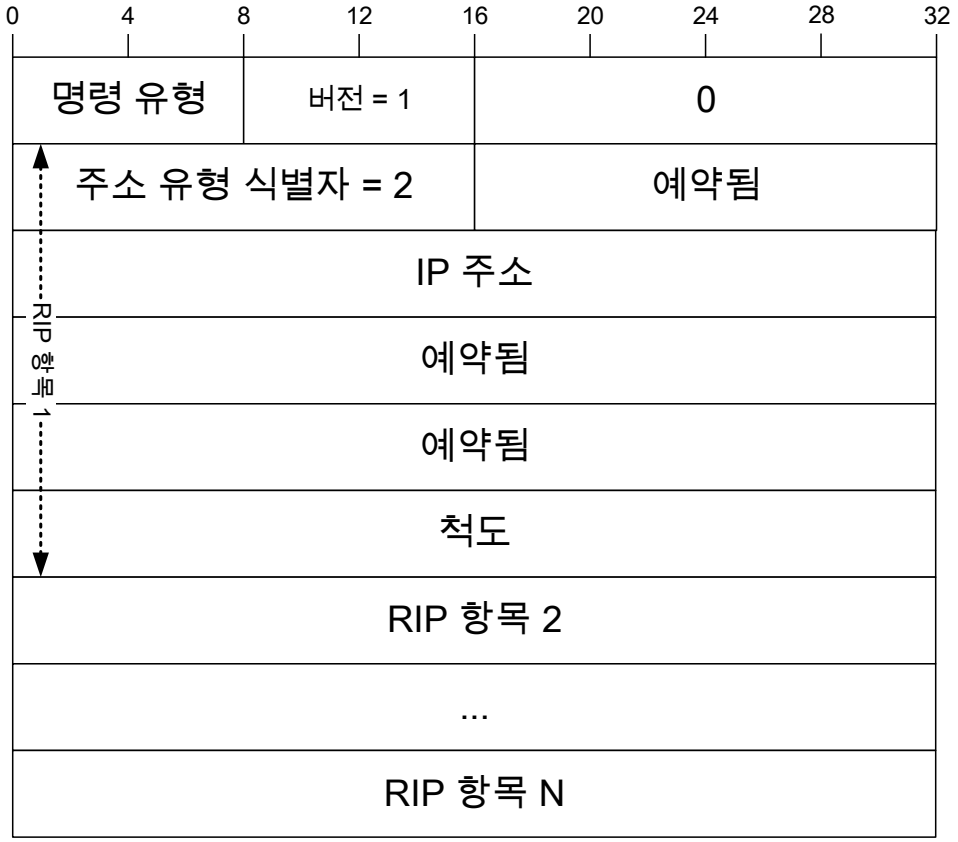
- 해결책
  - 수평 분할
    - 경로에 대한 RIP응답 정보를 받은 라우터는 자신이 접속하고 있는 네트워크로 그 정보를 다시 보내지 않음
      - 무한 세기 문제를 방지
  - 포이즌 리버스(Poisoned Reverse) 수평 분할
    - 다른 라우터가 특정 경로를 위해 자신의 경로를 사용하지 못하도록 무한 값(16) 응답 메시지를 전송
      - 라우팅 루프 문제를 해결
      - 특정 경로로 갈 수 없음을 알려주기 때문에 무한 세기 문제 방지

라우팅 정보 프로토콜(RIP)

- 해결책
  - 트리거 갱신(Triggered Update)
    - 네트워크 경로 정보가 변경된 경우 경로 갱신 정보를 즉시 인접 라우터에게 전달
      - RIP 응답 메시지로 전송
      - RIP의 느린 수렴 문제를 줄임
    - e.g., 가비지 콜렉션 타이머가 만료되어 이 경로가 유효하지 않다는 정보를 알리는 경우
  - 홀드 다운(Hold Down)
    - 네트워크 접근이 불가능 하다는 메시지를 받은 경우
      - 타이머(60초, 120초)를 설정
      - 타이머가 만료될 때까지는 메시지를 받지 않음
      - 타이머가 만료되면 경로 정보 갱신
    - 수정된 경로에 대한 반응이 느려 져 일시적으로 장애가 생겼던 네트워크를 사용하기 위해서는 지연 시간이 필요

라우팅 정보 프로토콜(RIP)

- 메시지 포맷
  - RIP-1
    - 다양한 프로토콜로 이루어진 네트워크에서 사용될 수 있도록 예약된 필드가 많음



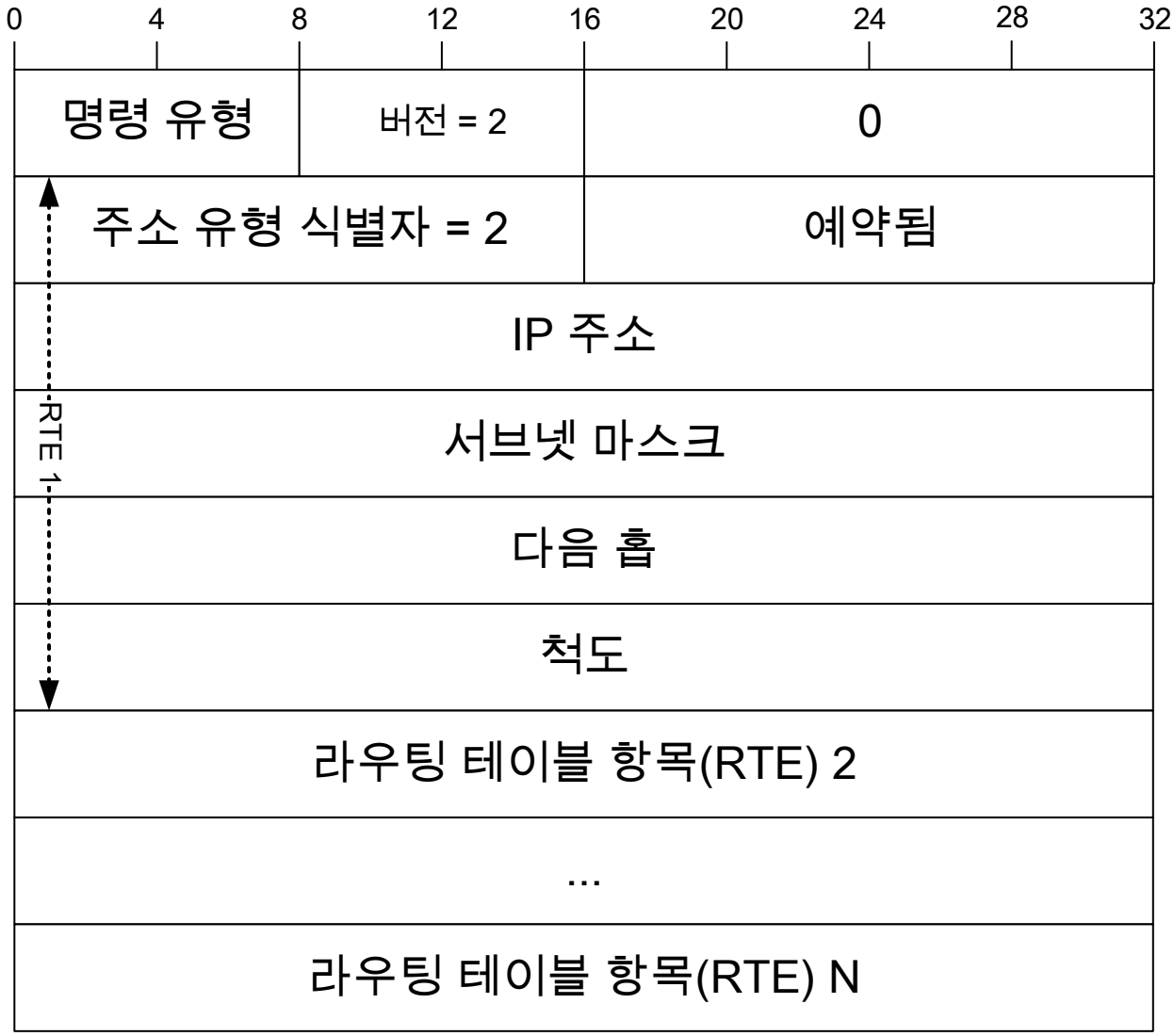
하위 필드명	크기 (바이트)	설명
주소 유형 식별자	2	주소의 유형 식별 (IP의 경우 필드 값 = 2)
0	2	예약된 필드(0)
IP 주소	4	라우터가 정보를 전달하는 경로의 주소
0	4	예약된 필드(0)
0	4	예약된 필드(0)
척도	4	IP 주소 필드가 지정하는 네트워크까지의 홉 수

라우팅 정보 프로토콜(RIP)

- 메시지 포맷
  - RIP-2
    - 클래스 비사용 주소 지정 지원과 서브넷 마스크 필드 추가
      - 서브넷 지원
    - 다음 홉 필드 추가
      - 다음 홉 라우터를 명시하여 라우팅 효율을 높임
    - 인증 기능
      - MD5(Message Digest 5)를 사용하여 라우터의 신원 확인
    - 경로 태그 필드 추가
      - 어떤 AS에서 정보를 얻었는지 식별
    - 멀티캐스팅 사용
      - 네트워크의 불필요한 트래픽을 줄이기 위해 브로드캐스트 대신 멀티캐스트 방식 사용

라우팅 정보 프로토콜(RIP)

- 메시지 포맷
  - RIP-2



최단 경로 우선 프로토콜(OSPF)

- OSPF(Open Shortest Path First)
  - 개요
    - 기존 RIP만으로는 인터넷 상의 모든 AS를 만족 시킬 수 없다는 것을 인지함
    - 이전 보다 좀더 복잡한 AS를 지원하기 위함
    - 1988년 IETF는 RIP보다 더 성능이 뛰어난 최단 경로 우선(SPF, Shortest Path First) 알고리즘을 사용하는 새로운 라우팅 프로토콜을 개발
    - 1989년, “The OSPF Specification” RFC 1131 문서로 정의
    - 1998년, “OSPF Version 2” RFC 2328 문서로 정의

최단 경로 우선 프로토콜(OSPF)

- OSPF(Open Shortest Path First)
  - 링크 상태 알고리즘을 사용하여 RIP을 보완하기 위한 라우팅 프로토콜
  - 특징
    - 라우터를 그룹으로 묶어 계층 토폴로지를 만듦
      - 트래픽 감소
      - 토폴로지(Topology)
        - 컴퓨터 네트워크의 요소들을 물리적, 논리적인 연결 상태로 나타낸 것
    - 보안을 위한 인증 지원
    - 표준 IP 주소 지정 지원
    - RIP에 비해 수렴시간이 빠름
      - 네트워크 변화 시, 즉시 라우팅 정보 전송

최단 경로 우선 프로토콜(OSPF)

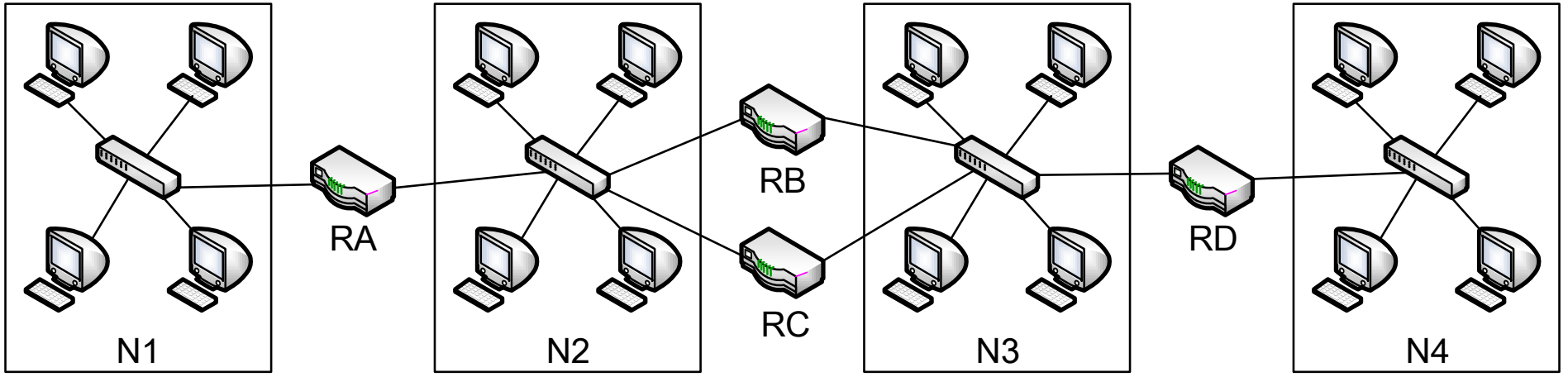
- 동작 원리
  - 라우터가 인터네트워크의 토폴로지와 상태에 대한 정보를 관리하는 데이터베이스를 가짐
  - 링크 상태 데이터베이스(LSDB, Link-State DataBase)
    - OSPF에서 가장 기본적인 데이터 구조
    - 네트워크나 다른 라우터로 향하는 링크와 이에 대한 비용(척도)이 저장된 데이터구조
      - 척도
        - 측정하거나 평가하는 기준

최단 경로 우선 프로토콜(OSPF)

- 동작 원리
  - 인터네트워크가 변경되면 상태 정보에 대한 갱신 메시지를 전송하여 각 라우터에게 경로를 다시 계산하도록 함
  - 링크 상태 광고(LSA, Link-State Advertisement)
    - AS에 대한 정보를 다른 라우터에게 전해줄 때, 사용하는 메시지
  - 경로 결정
    - LSDB를 사용하여 최단 경로 트리를 형성
    - 새로운 정보가 들어오면 트리를 새로 계산하여 네트워크 상태에 따라 동적으로 최적 경로 계산

최단 경로 우선 프로토콜(OSPF)

- 기본 토폴로지
  - AS 내의 모든 라우터는 동등
    - 각 라우터는 전체 AS 에 대한 정보를 관리하므로 동일한 LSDB를 가짐
  - LSDB 정보 저장과 전파
    - 각 라우터는 LSA를 포함하는 갱신 메시지를 주기적으로 교환하여 LSDB 생신



최단 경로 우선 프로토콜(OSPF)

- LSDB 예시
  - '•'과 '0'은 라우터와 네트워크 도는 라우터가 연결됨을 의미
    - '•'은 패킷을 보내기 위한 비용이 듦
    - '0' 은 패킷의 비용이 이중으로 계산되지 않도록 하기 위해 비용이 들지 않음

목적 라우터 / 네트워크	출발 라우터				출발 네트워크			
	RA	RB	RC	RD	N1	N2	N3	N4
RA					0	0		
RB			•			0	0	
RC		•				0	0	
RD							0	0
N1	•							
N2	•	•	•					
N3		•	•	•				
N4				•				

최단 경로 우선 프로토콜(OSPF)

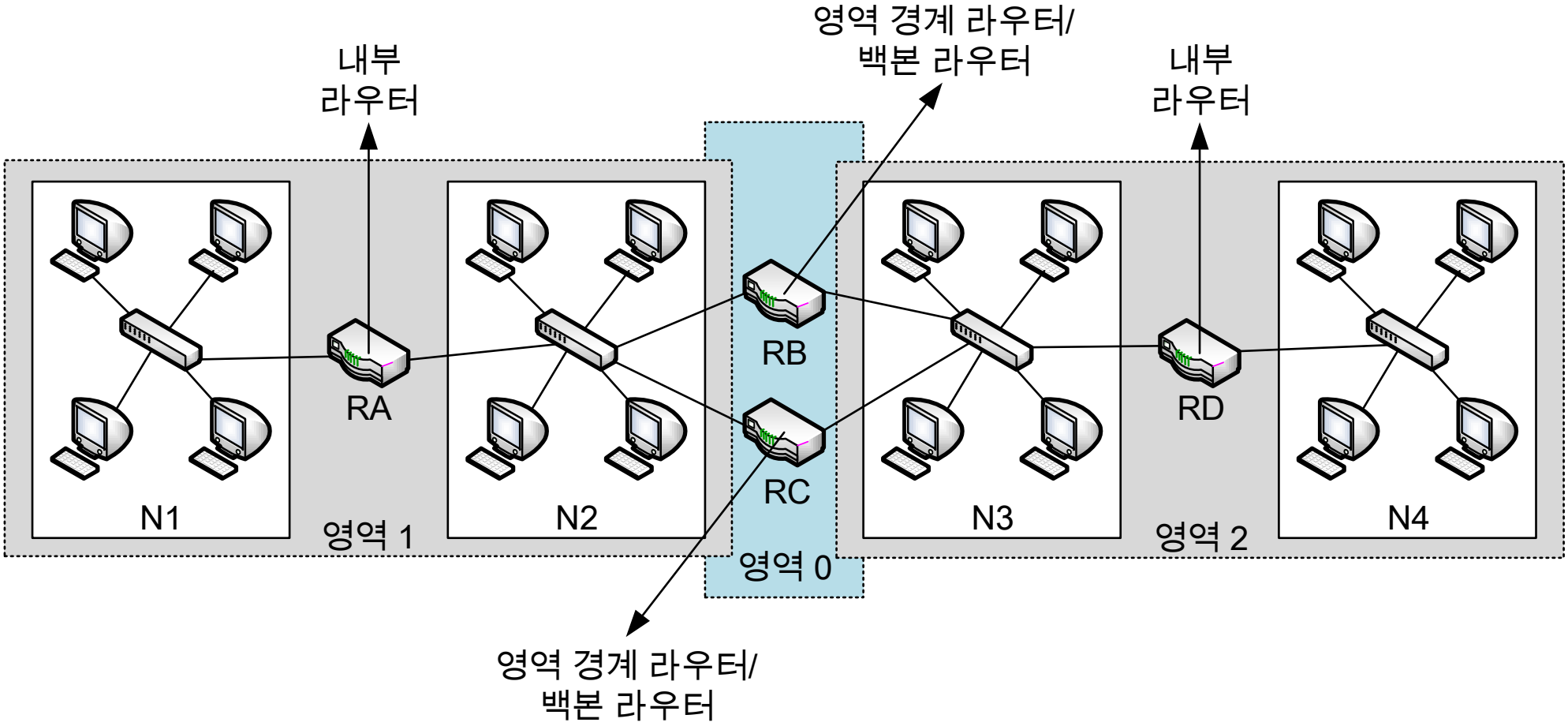
- 계층 토폴로지
  - 거대한 인터네트워크를 제어하고 관리할 수 있도록 AS는 계층 구조를 가짐
    - 거대한 LSDB를 관리해야 하기 때문
  - 영역
    - 번호가 부여되며, 독립적으로 관리되는 AS를 나누는 구조
  - 백본(backbone)
    - 높은 영역을 연결하는 계층을 의미

최단 경로 우선 프로토콜(OSPF)

- 계층 토폴로지
  - 라우터 역할
    - 내부 라우터
      - 한 영역 내에 연결된 라우터
      - 한 영역에 대한 LSDB만을 가짐
      - 외부 영역에 대해서는 알지 못함
    - 영역 경계 라우터
      - 하나 이상의 영역에 연결된 라우터
      - 자신이 속한 영역의 LSDB를 가짐
      - 백본에 참여
    - 백본 라우터
      - 모든 영역 경계 라우터를 포함하는 라우터
      - 영역 간의 라우팅 정보 전달

최단 경로 우선 프로토콜(OSPF)

- 계층 토폴로지



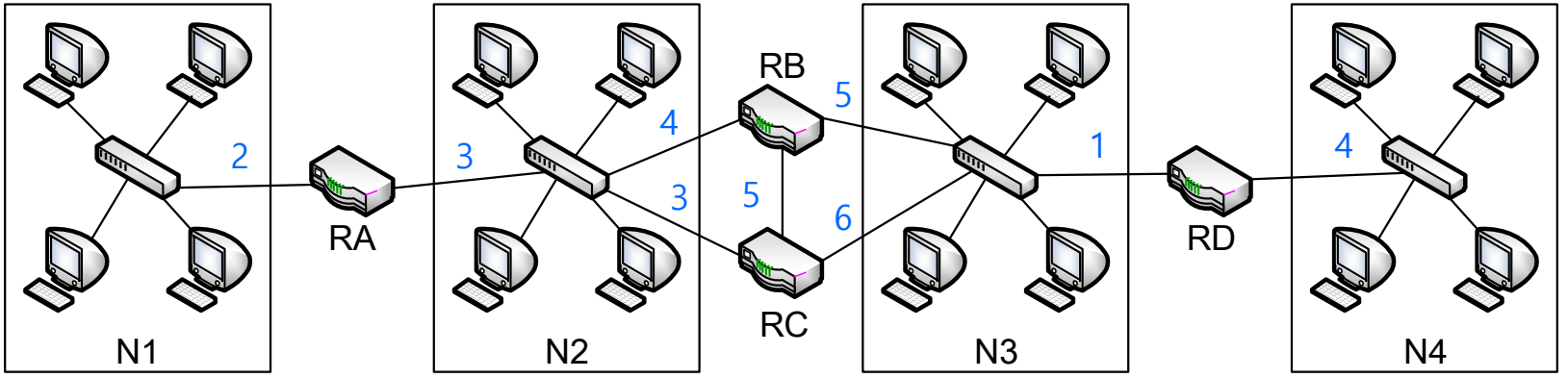
최단 경로 우선 프로토콜(OSPF)

- 경로 결정
  - 최단 경로 우선(SPF, Shortest Path First) 트리
    - AS 혹은 영역 내에 있는 네트워크나 라우터 간의 최단 경로를 결정하기위해 LSDB의 정보를 바탕으로 생성된 트리
    - 라우터는 SPF트리를 통해 최단 경로를 갖는 라우팅 테이블 생성
      - 다른 네트워크로 경로 비용과 다음 홉이 될 라우터 명시
      - 최단 경로 알고리즘
        - 다익스트라(Dijkstra) 알고리즘 사용
    - SPF 트리는 LSDB의 현재 상태를 기반으로 동적 계산

최단 경로 우선 프로토콜(OSPF)

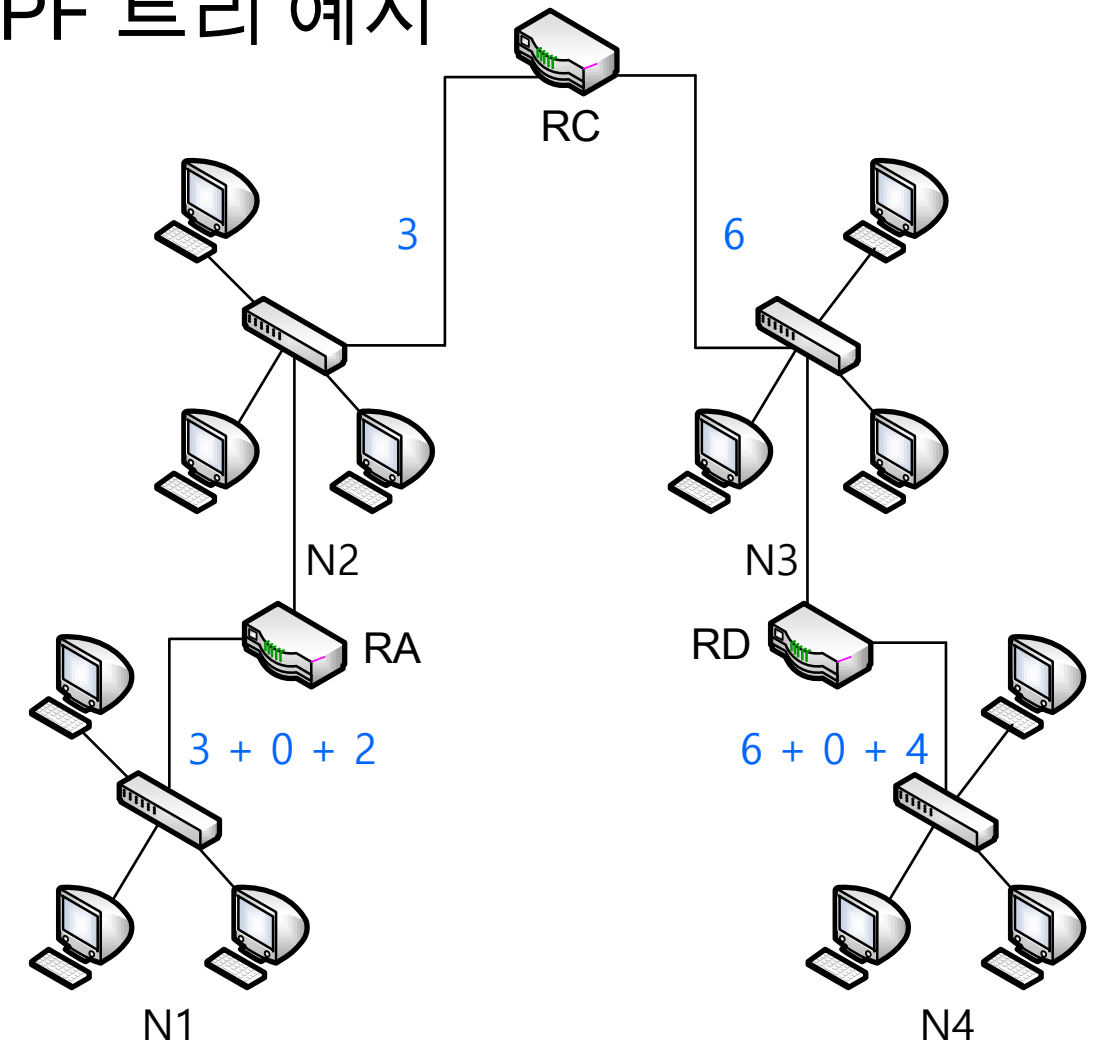
- 경로 결정
  - LSDB 예시

목적 라우터 / 네트워크	출발 라우터				출발 네트워크			
	RA	RB	RC	RD	N1	N2	N3	N4
RA					0	0		
RB			5			0	0	
RC		5				0	0	
RD							0	0
N1	2							
N2	3	4	3					
N3		5	6	1				
N4				4				



최단 경로 우선 프로토콜(OSPF)

- 경로 결정
  - SPF 트리 예시



목적 네트워크	비용	다음 홉
N1	5	RA
N2	3	로컬
N3	6	로컬
N4	10	RD

최단 경로 우선 프로토콜(OSPF)

- 동작 과정
  - OSPF 메시지는 패킷을 전송할 때, TCP/UDP를 사용하지 않고 IP 패킷에 의해 직접 전송
    - IP Protocol 필드 값: 89
  - OSPF 메시지 유형
    - Hello 메시지
      - 자신을 주변 장비들에게 알리거나, 주변 장비를 파악하는 메시지
      - AS나 영역 내에서 OSPF 관련 인자 주고 받음
    - 데이터베이스 설명 메시지
      - AS나 영역 토폴로지에 대한 LSDB 정보를 전달하는 메시지
      - Hello 메시지에 대한 응답 메시지
      - 큰 LSDB를 전송할 때는 나누어 전달
        - 송신 장비를 Master, 수신 장비는 Slave라고 부름

최단 경로 우선 프로토콜(OSPF)

- 동작 과정
  - OSPF 메시지 유형
    - 링크 상태 요청 메시지
      - LSDB에 대한 최신 정보를 요청하는 메시지
      - 현재 정보를 알고 싶은 링크를 명시
    - 링크 상태 갱신 메시지
      - LSDB에 있는 특정 링크에 대한 상태를 알리는 메시지
      - 링크 상태 요청 메시지에 대해 응답으로 송신
      - 주기적으로 링크 상태 정보를 브로드/멀티캐스트하여 갱신
    - 링크 상태 승인 메시지
      - 링크 상태 갱신 메시지에 대한 응답 메시지

최단 경로 우선 프로토콜(OSPF)

- 동작 과정
  - 메시지 교환
    1. 라우터는 주기적으로 Hello 메시지를 전송하여 주변에 OSPF를 실행하는 새로운 라우터 확인
       - 발견 시, 데이터베이스 설명 메시지를 전송하고 LSDB 초기화
    2. 초기화를 거친 라우터는 안정 상태로 들어가 주기적으로 링크 상태 갱신 메시지를 보내 링크 상태를 광고
    3. 링크 상태 갱신 메시지를 받은 라우터는 링크 상태 승인 메시지로 응답

최단 경로 우선 프로토콜(OSPF)

- 동작 과정
  - 메시지 인증
    - 표준에서 OSPF 메시지를 보안하기 위해 인증을 사용하도록 명시
    - 선택적으로 인증 방식 사용 가능
      - 간단한 비밀번호 인증
      - 해시 암호화(MD5)인증
      - 인증을 사용하지 않는 널(NULL)인증

최단 경로 우선 프로토콜(OSPF)

- 공통 헤더 포맷

필드명	크기 (바이트)	설명
버전	1	OSPF 버전 2 = 2
유형	1	OSPF 메시지의 유형 식별
패킷 길이	2	메시지의 길이를 바이트로 표시
라우터 ID	4	메시지를 생성한 라우터의 ID
영역 ID	4	메시지를 보낸 라우터가 속한 OSPF 영역을 나타냄
체크섬	2	에러 탐지
인증 유형	2	메시지에서 사용하는 인증 유형
인증	8	메시지의 인증을 위한 필드

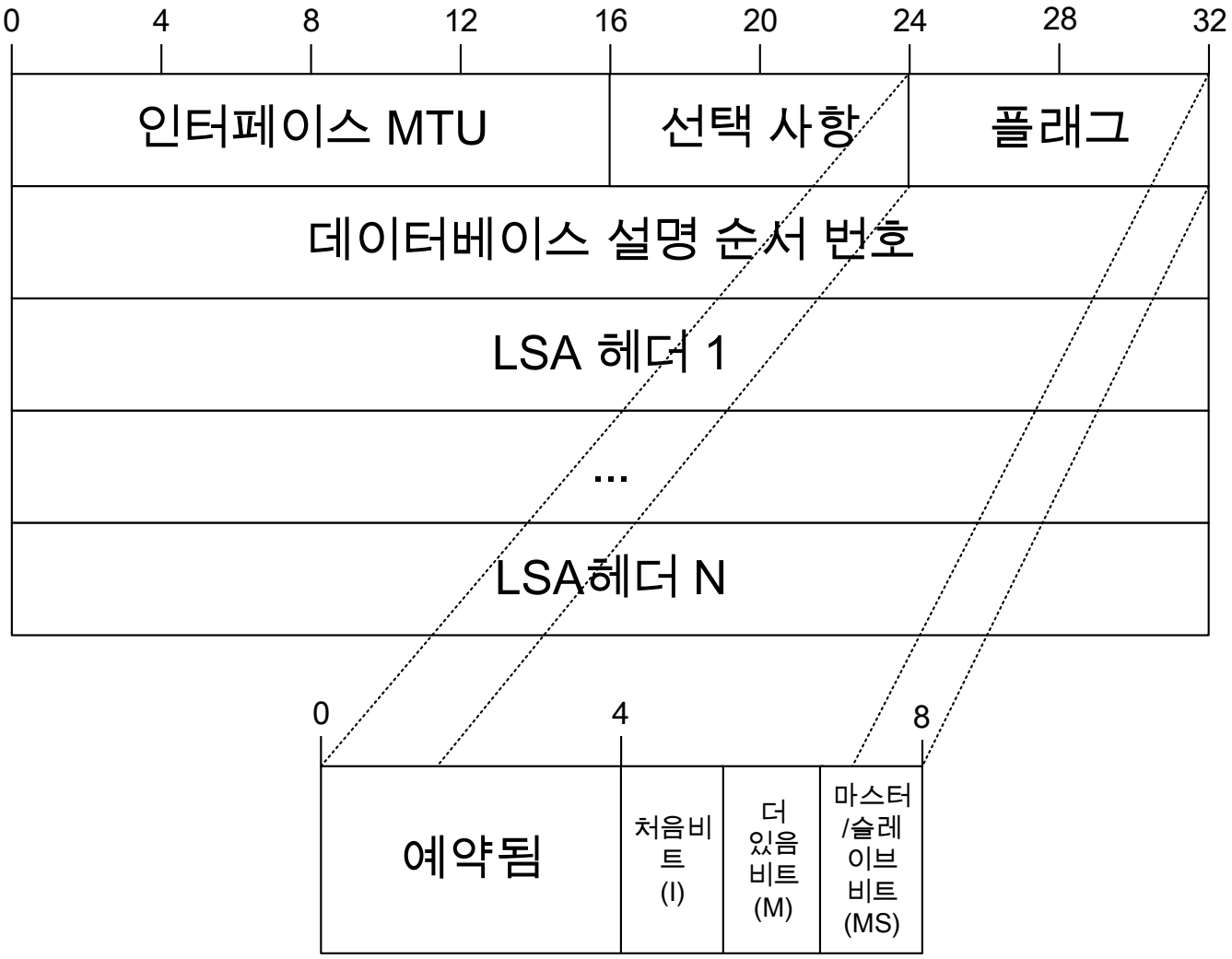
최단 경로 우선 프로토콜(OSPF)

- Hello 메시지 포맷

필드명	크기 (바이트)	설명
네트워크 마스크	4	메시지를 보내고있는 네트워크의 서브넷 마스크
전송간격	2	Hello 메시지를 받기 원하는 간격(단위: 초)
선태사항	1	라우터가 지원하는 OSPF 선택사항 기능
라우터 우선 순위	1	라우터의 우선순위를 알림
라우터 장애 간주간격	4	지정한 시간이 지나면 장애가 생겼다고 간주
지정 라우터	4	특별한 기능을 수행하도록 지명된 라우터의 주소 (없으면 0)
백업 지정 라우터	4	백업 지정 라우터의 주소 (없으면 0)
주변 라우터	4의 배수	라우터가 최근 받은 Hello 메시지를 보낸 주소

최단 경로 우선 프로토콜(OSPF)

- 데이터베이스 설명 메시지 포맷



최단 경로 우선 프로토콜(OSPF)

- 데이터베이스 설명 메시지 포맷 설명

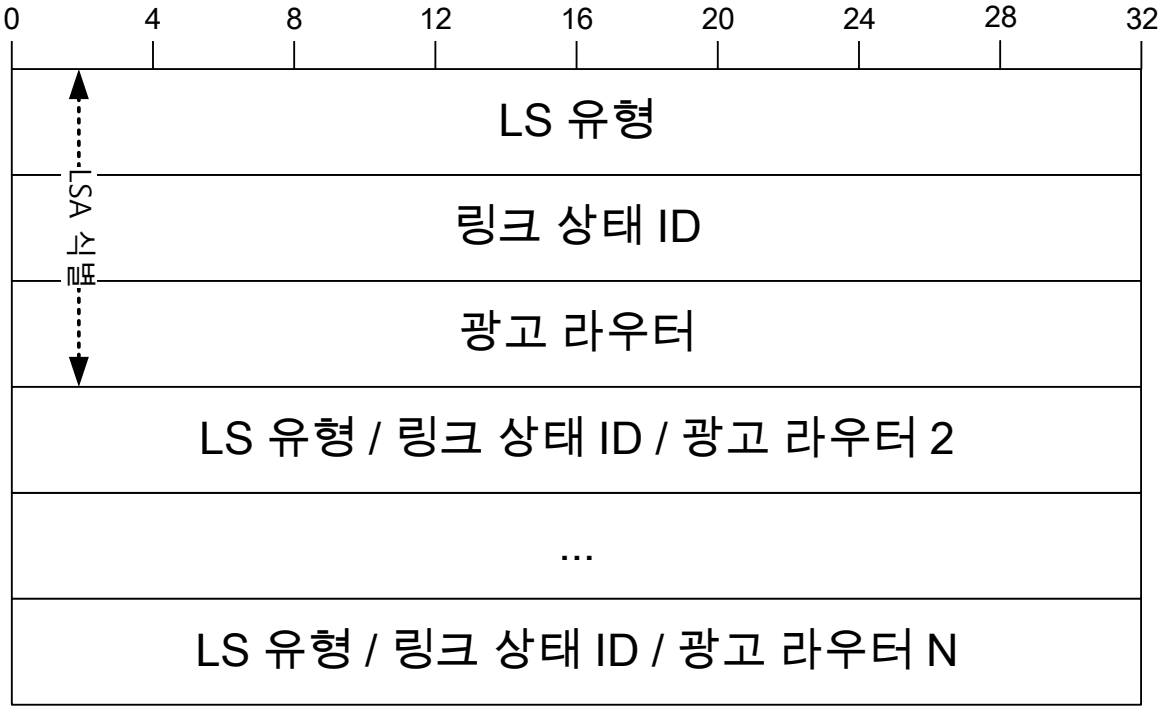
필드명	크기(바이트)	설명
인터페이스 MTU	2	라우터의 인터페이스로 단편화하지 않고 보낼 수 있는 최대 IP 메시지 크기
선택사항	1	라우터가 지원하는 OSPF 선택사항 기능을 알림
플래그	1	데이터베이스 설명 메시지를 순서대로 정렬할 수 있도록 순서 번호 사용
데이터베이스 설명 순서 번호	4	데이터베이스 설명 메시지를 순서대로 정렬할 수 있도록 순서 번호 사용
LSA헤더	가변	LSDB에 대한 정보를 전달하는 LSA 헤더를 포함

- 데이터베이스 설명 메시지 플래그 설명

필드명	크기(바이트)	설명
예약	5	예약된 필드(0으로 설정)
처음 (I, Initial)	1	데이터베이스 설명 메시지를 처음 보낼 경우 1로 설정
더 있음(M, More)	1	다음 데이터베이스 설명 메시지가 더 있으면 1로 설정
마스터 / 슬레이브	1	메시지를 보내는 라우터가 마스터이면 1, 슬레이브이면 0으로 설정

최단 경로 우선 프로토콜(OSPF)

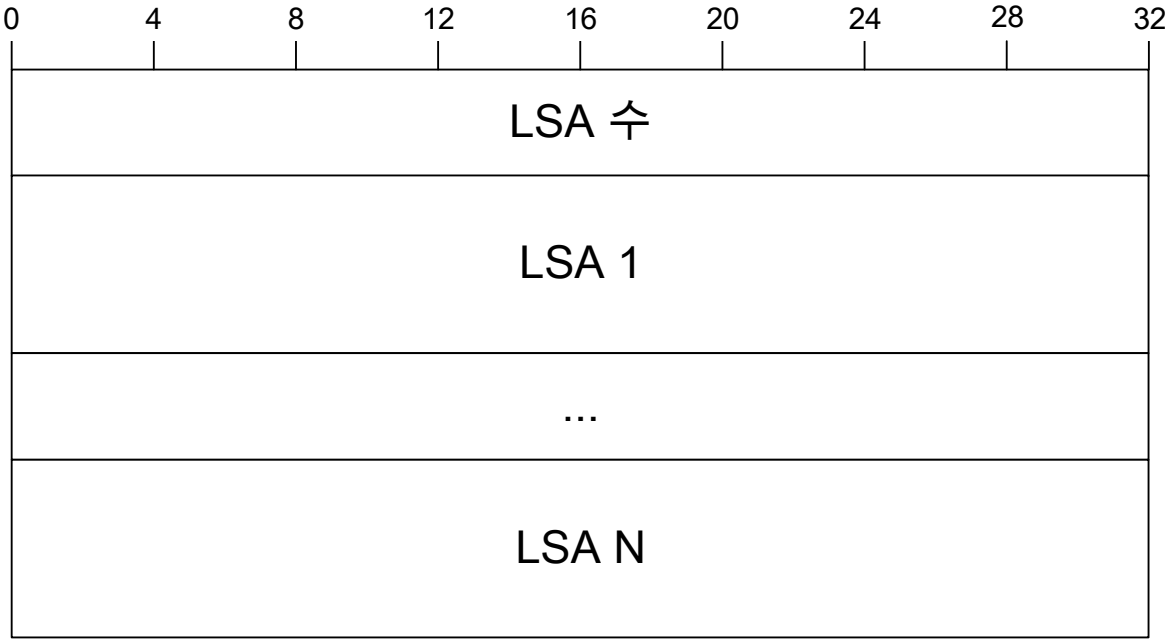
- 링크 상태 요청 메시지 포맷



필드명	크기(바이트)	설명
LSA 유형	4	원하는 LSA 유형
링크 상태 ID	4	LSA의 식별자로 연결된 라우터나 네트워크의 IP 주소를 주로 사용
광고 라우터	4	갱신이 요청된 LSA를 생성한 라우터의 ID

최단 경로 우선 프로토콜(OSPF)

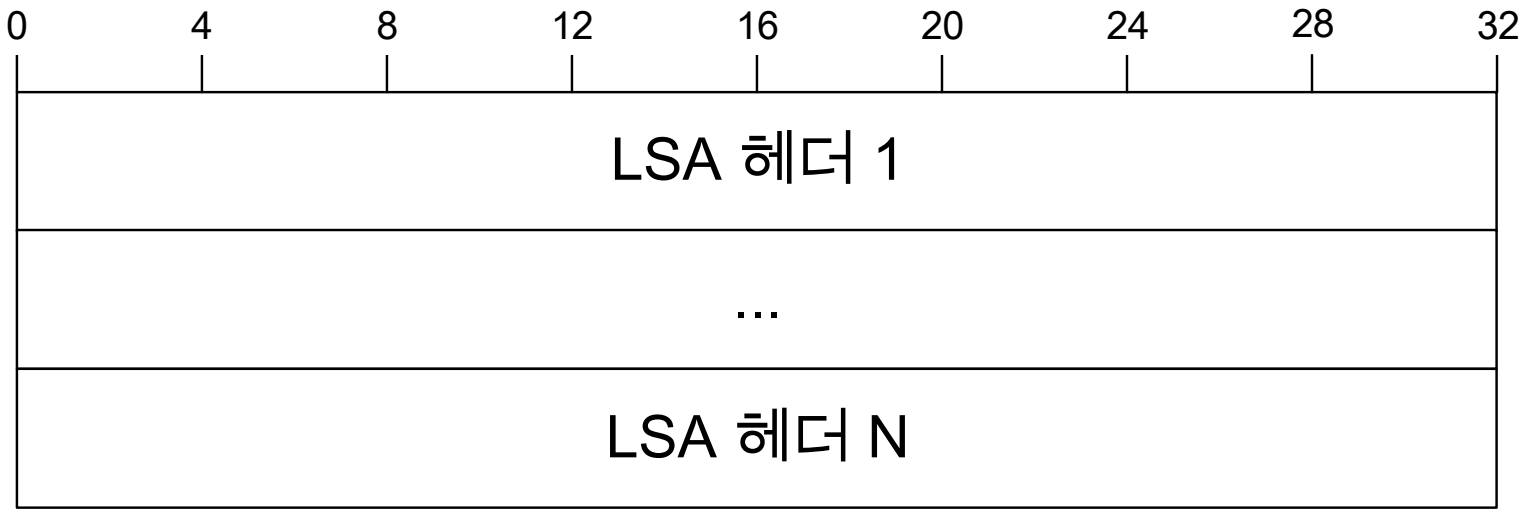
- 링크 상태 갱신 메시지 포맷



필드명	크기(바이트)	설명
LSA 수	4	메시지에 포함된 LSA의 수
LSA	가변	하나 이상의 LSA 포함

최단 경로 우선 프로토콜(OSPF)

- 링크 상태 승인 메시지 포맷



필드명	크기(바이트)	설명
LSA 헤더	가변	승인할 LSA를 식별하기 위한 LSA 헤더 필드

최단 경로 우선 프로토콜(OSPF)

- 링크 상태 광고 메시지 포맷

필드명	크기 (바이트)	설명
LS 나이	2	LSA가 생긴 후 지난 시간을 초단위로 표현
선택 사항	1	라우터가 지원하는 OSPF 선택사항 기능을 알림
LS 유형	1	LSA가 정보를 제공하는 링크의 유형을 알림
링크 상태 ID	4	링크를 식별
광고 라우터	4	LSA를 만든 라우터의 ID
LS 순서번호	4	오래되거나 중복된 LSA를 찾기 위해 사용하는 순서 번호
LS 체크섬	2	에러 탐지
길이	2	헤더 길이 20바이트를 포함하는 총 LSA 길이

경계 경로 프로토콜(BGP)

- BGP(Border Gateway Protocol)
  - 개요
    - 인터넷이 확장됨에 따라 AS의 수가 점차 늘어나 AS 간의 통신이 중요해짐
    - 인터넷에 더 나은 기능을 제공하는 새로운 외부 라우팅 프로토콜의 필요성 인지

RFC 번호	년도	이름	BGP 버전	설명
1105	1989	A Border Gateway Protocol	BGP-1	BGP의 초기 정의
1163	1990	A Border Gateway Protocol	BGP-2	버전 1에서의 방향성에 대한 개념 삭제
1267	1991	A Border Gateway Protocol 3	BGP-3	메시지 식별 기능을 추가하여 경로 정보 교환을 최적화
1771	1995	A Border Gateway Protocol 4	BGP-4	클래스 비사용 도메인 간 라우팅(CIDR) 지원 추가

경계 경로 프로토콜(BGP)

- 기능
  - AS 간에 네트워크 접근 가능 정보를 교환하고 그 정보를 기반으로 네트워크로 가는 경로 결정
- 특징
  - AS내에 BGP를 지원하는 하나 이상의 라우터 필요
  - BGP 라우터는 네트워크에 관한 정보와 경로를 라우팅 정보 기반(RIB, Routing Information Base) 데이터베이스에 저장
  - 경로 정보를 공유하기 위해 TCP 179번 포트를 사용하여 메시지 교환

경계 경로 프로토콜(BGP)

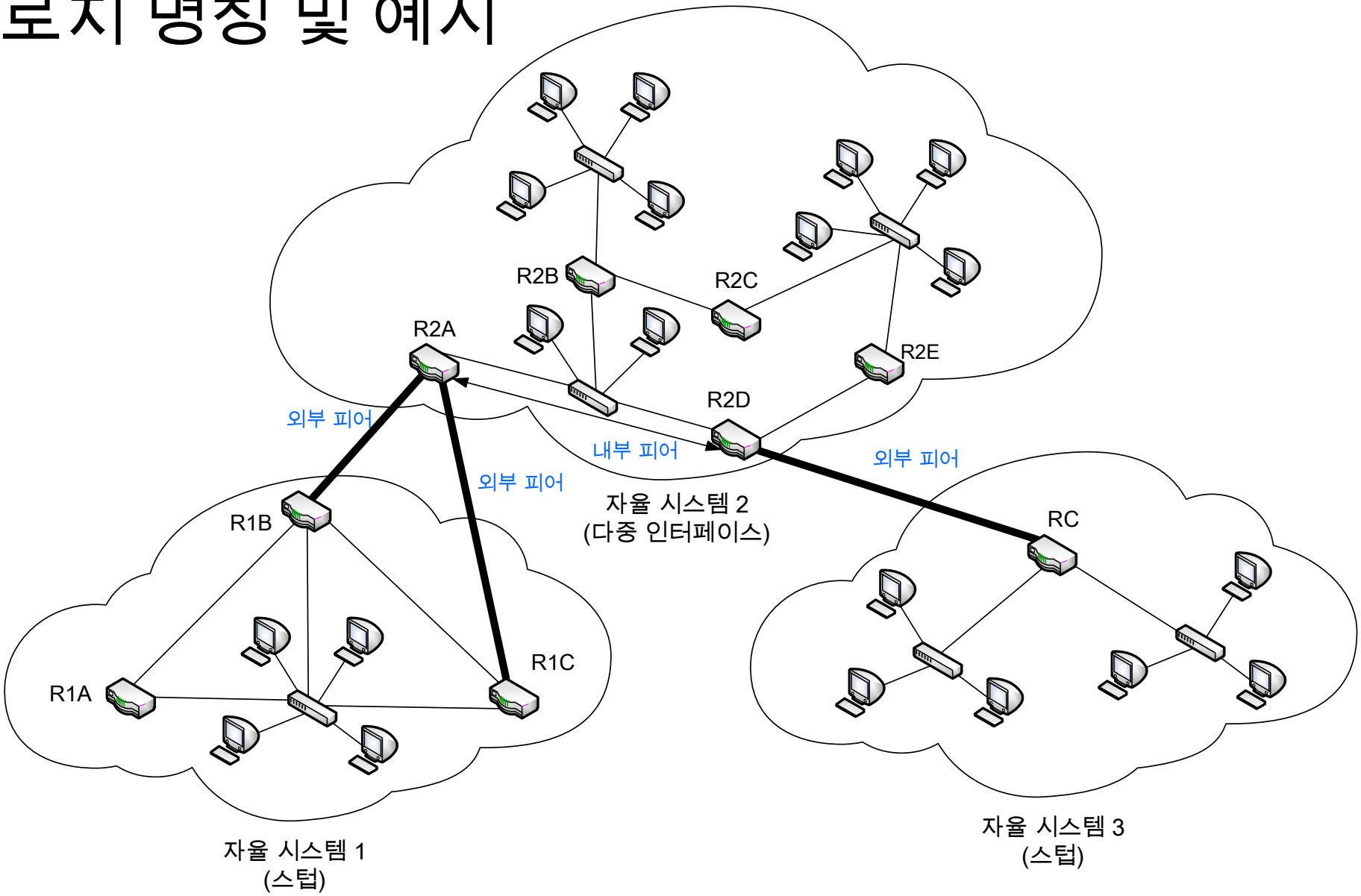
- 토폴로지
  - AS의 BGP 라우터가 다른 AS의 BGP 라우터에 연결되어 있는 경우
    - AS의 토폴로지와 상관없이 BGP 사용 가능
    - 갱신되는 토폴로지 처리 가능
  - BGP는 AS의 내부에 대한 처리는 하지 않음
    - AS를 연결하여 경로 정보를 다른 AS와 공유할 뿐

경계 경로 프로토콜(BGP)

- 토폴로지
  - 용어
    - 스피커(Speaker)
      - AS에서 BGP를 사용하기 위해 선택된 라우터
      - BGP의 메시지 교환 시스템을 통해 경로 정보 교환
    - 주변 노드(Neighbor Node)
      - 내부 피어(Internal Peer)
        - 같은 AS 내에서 통신하는 BGP 스피커
      - 외부 피어(External Peer)
        - AS 간에 통신하는 BGP 스피커

경계 경로 프로토콜(BGP)

- 토폴로지 명칭 및 예시



경계 경로 프로토콜(BGP)

- 토폴로지
  - 트래픽 흐름과 유형
    - 지역 트래픽(Local Traffic)
      - AS 내에서 발생하여 다른 AS로 전송되어야 하는 트래픽
    - 횡단 트래픽(Transit Traffic)
      - AS 밖에서 발생하여 다른 AS로 전송되어야 하는 트래픽
  - AS 유형
    - 스텁(Stub) AS
      - 하나의 AS와 연결된 AS
    - 다중 인터페이스(Multi Interface) AS
      - 두 개 이상의 AS에 연결된 AS

경계 경로 프로토콜(BGP)

- 토폴로지
  - AS 라우팅 정책
    - AS가 횡단 트래픽 전송을 제어하기 위한 정책
    - 횡단 금지 정책(No Transit Policy)
      - 횡단 트래픽을 전혀 처리하지 않음
    - 제한된 AS 횡단 정책(Restricted AS transit policy)
      - 특정 AS에서 오는 트래픽만 처리하고 다른 AS에서 오는 횡단 트래픽은 받지 않음
    - 기준 기반 횡단 정책(Criteria-based transit policy)
      - 다양한 기준을 기반으로 횡단 트래픽 처리에 대한 여부를 결정
      - e.g., 특정 시간, 트래픽 처리 잔여량 등

경계 경로 프로토콜(BGP)

- 경로 저장과 광고
  - BGP 장비 간의 경로 정보 교환을 통해 각 라우터가 IP 인터 네트워크에서 효율적으로 라우팅 할 수 있게 함
  - BGP 경로 정보 관리 함수
    - 경로 저장
      - 네트워크에 도달하는 방법과 다른 장비에서 받은 라우팅 정보를 경로 데이터베이스에 저장
    - 경로 갱신
      - Peer로 부터 갱신 메시지를 받은 후 자신의 경로 정보를 수정할 지에 대한 처리 방식 결정

경계 경로 프로토콜(BGP)

- 경로 저장과 광고
  - BGP 경로 정보 관리 함수
    - 경로 선택
      - 경로 데이터베이스에 있는 정보를 사용하여 인터네트워크에 있는 네트워크로 가는 경로를 선택
    - 경로 광고
      - Peer에게 네트워크에 대한 정보와 경로, 도착 방법 등을 주기적으로 알림

경계 경로 프로토콜(BGP)

- 경로 저장과 광고
  - BGP 라우팅 정보 기반(RIB) 데이터베이스
    - BGP 스피커가 경로 정보를 관리할 때 제대로 동작하기 위해 사용하는 중앙 데이터 구조
    - Adj-RIBs-In
      - Peer BGP 라우터로부터 받은 경로 정보를 보관하는 입력 데이터베이스
    - Loc-RIB
      - BGP 장비가 유효하다고 판단하여 선택한 라우터의 현재 경로 정보를 저장하는 데이터베이스
    - Adj-RIBs-Out
      - BGP 장비가 다른 라우터에게 알리기로 결정한 경로 정보를 보관하는 출력 데이터베이스

경계 경로 프로토콜(BGP)

- 경로 속성 값과 알고리즘
  - 경로 속성
    - 효율적이고 루프가 없는 경로를 계산하기 위해서는 목적지 네트워크로 가는 모든 경로의 상세한 정보가 필요
    - 경로 정보는 BGP 경로 속성 값의 형태로 BGP 스피커의 라우팅 정보 기반(RIB) 데이터베이스에 저장
      - 속성 값
        - 현재 라우터에서 목적지 네트워크까지 패킷이 거쳐가야 하는 경로에 대한 특성
      - 라우터는 경로 속성 값을 저장, 처리, 전송, 수신하여 어떤 경로를 선택할 지 결정
  - BGP 알고리즘
    - 경로 벡터 알고리즘 사용
      - BGP 라우터는 네트워크로 가는 방법에 대해 목적지 주소에 도착하기 위한 경로 설명을 덧붙여 광고

경계 경로 프로토콜(BGP)

- 경로 속성 값과 알고리즘
  - 경로 속성 클래스
    - 잘 알려진 의무 사항(Well-Known Mandatory) 속성 값
      - 모든 갱신 메시지의 경로에 필수적으로 포함되어야 하는 속성
      - BGP 라우터는 이 클래스의 속성 값을 모두 처리해야 함
    - 잘 알려진 임의 사항(Well-Known Discretionary)속성 값
      - 갱신 메시지에 선택적으로 포함되는 속성
      - BGP 라우터는 이 클래스의 속성 값을 처리할 수 있어야 함

경계 경로 프로토콜(BGP)

- 경로 속성 값과 알고리즘
  - 경로 속성 클래스
    - 선택 사항 횡단(Optional Transitive)
      - 속성 값을 식별할 수도 있고 갱신 메시지에 포함 시킬 수도 있음
      - 속성 값을 식별하지 못한 경우, 경로를 광고할 때 다른 BGP 장비에게 알림
    - 선택 사항 비 횡단(Optional non-Transitive)
      - 속성 값을 식별할 수도 있고 갱신 메시지에 포함 시킬 수도 있음
      - 속성 값을 식별하지 못한 경우, 다음 라우터에게 알리지 않음

경계 경로 프로토콜(BGP)

- 경로 속성 값과 알고리즘
  - 경로 속성 클래스 설명

BGP 경로 속성	속성 유형 값	분류	설명
근원	잘 알려진 의무 사항	1	경로 정보를 얻은 출처 명시
경로상의 AS	잘 알려진 의무 사항	2	설명하는 경로가 거쳐야 하는 AS를 나열
다음 홉	잘 알려진 의무 사항	3	목적지로 가기 위한 다음 홉 라우터를 명시
다중 출구/ 입구 설명 (MED)	비 횡단 선택사항	4	어떤 AS의 출구나 입구가 여러 개 있을 경우, 각각으로 가는 척도를 알림 (출구나 입구를 선택할 때 사용)
로컬 선호도	잘 알려진 임의 사항	5	같은 AS에 있는 BGP 스피커끼리 통신할 때 경로에 대한 선호도를 알리기 위해 사용
집선	잘 알려진 임의 사항	6	BGP 스피커는 더 구체적인 네트워크로 가능 중첩된 경로를 받을 수 있음
집선 장비	횡단 선택 사항	7	경로 집선을 수행한 라우터의 AS 번호와 BGP ID를 포함

경계 경로 프로토콜(BGP)

- 경로 판단과 결정 과정
  - 결정 과정 단계
    - 라우터는 입력 정보를 분석하여 경로 갱신, 선택, 광고 기능을 수행
    - 로컬 데이터베이스에 포함 시킬 정보를 선별
      - 데이터베이스를 갱신한 후 다른 장비에게 전송할 경로를 선택

1. BGP 스피커는 주변 AS에 있는 BGP 스피커가 보낸 경로를 분석하여 선호도 할당
   - 할당된 선호도와 광고로 전달된 각 네트워크에 대한 최적 경로를 기반으로 순위를 매김
2. BGP 스피커는 최적 경로를 선호도에 따라 선택하여 로컬 라우팅 정보 기반(Loc-RIB)을 갱신
3. BGP 스피커는 Loc-RIB에 존재하는 경로를 선택하여 다른 AS에 있는 주변 노드 BGP 스피커에게 전송

경계 경로 프로토콜(BGP)

- 경로 판단과 결정 과정
  - 선호도 할당 기준
    - 목적지 네트워크까지 거쳐야 하는 AS의 수
      - 적을 수록 좋음
      - 경로를 사용할 수 없게 하는 특정 정책의 존재 여부
      - 경로 정보의 생성지
  - 효율적인 경로 선택의 한계
    - BGP는 패킷이 AS를 지나는 데 필요한 비용을 알 수 없음
      - AS 내부 라우터 구조를 모름
    - AS의 상태에 따른 비효율 발생
      - 전체 경로의 효율을 보장할 수 없음

경계 경로 프로토콜(BGP)

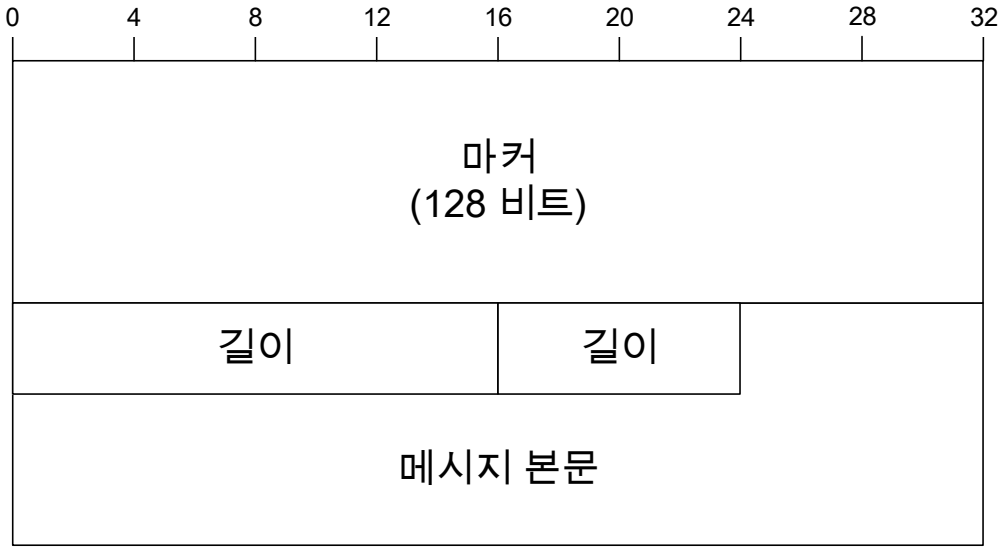
- 동작 원리
  - BGP 스피커 지정과 연결 수립
    - AS 간 통신을 위해서는 BGP 스피커가 지정되고 서로 연결되어야 함
      - BGP 스피커가 지정된 후 AS는 BGP 인터네트워크에 연결
      - BGP Peer와 TCP 연결을 수립하여 메시지 교환
  - 경로 정보 교환
    - BGP Peer 사이에 링크가 수립되면 전체 네트워크 정보와 라우팅 테이블 교환
  - 갱신 메시지 교환
    - 변경된 경로에 대한 갱신 정보만 교환하기 때문에 사용하는 대역폭을 최소한으로 줄일 수 있음

경계 경로 프로토콜(BGP)

- 동작 원리
  - 연결 유지
    - BGP 스피커는 서로 연결되어 있다는 것을 확인하기 위해 주기적으로 킵 얼라이브 메시지 교환
      - 보낼 정보가 없는 동안에도 장비 간 통신 유지
  - 에러보고
    - BGP 통지(Notification) 메시지
      - BGP Peer에게 에러가 발생했을 경우, 에러의 원인에 대한 정보를 제공하는 오류메시지
    - 통지 메시지를 보낸 장비는 둘 간의 BGP 연결 종료
      - 새 연결을 수립하려면 통지 메시지에서의 에러를 해결한 후에 처음부터 다시 협상해야 함

경계 경로 프로토콜(BGP)

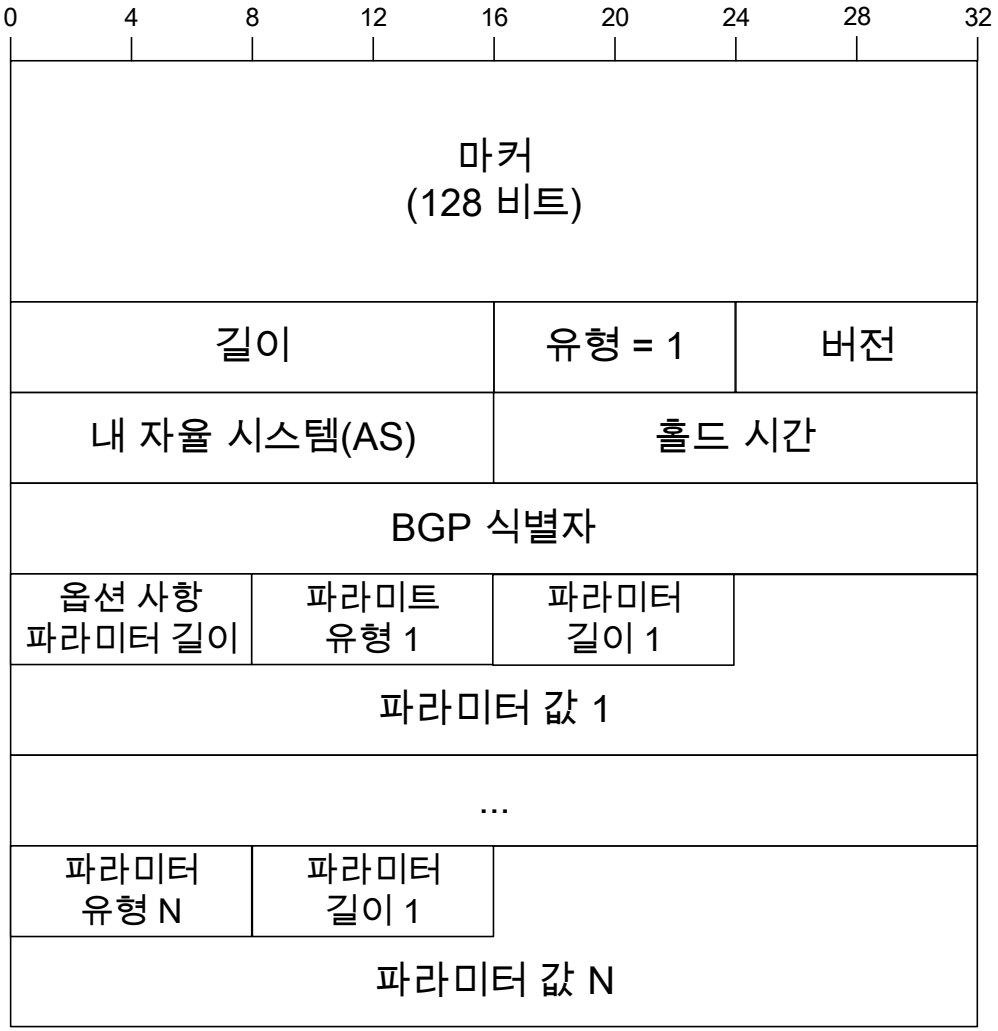
- 일반 메시지 포맷



필드명	크기 (바이트)	설명
마커	16	메시지의 시작을 식별, 인증하기 위해 사용
길이	2	메시지의 총 길이
유형	1	BGP 메시지 유형 (1 = 생성 2 = 갱신 3 = 통지 4 = 킵 얼라이브)
메시지 본문/ 데이터 부분	가변	생성, 갱신, 통지 메시지 유형을 구현하기 위한 구체적인 필드

경계 경로 프로토콜(BGP)

- 생성 메시지 포맷



필드명	크기 (바이트)	설명
마커	16	메시지의 시작을 식별, 인증하기 위해 사용
길이	2	메시지의 총 길이
유형	1	BGP 메시지 유형 (생성 메시지 = 1)
버전	1	BGP 버전
내 자율 시스템 (AS)	2	생성 메시지를 전송하는 라우터의 AS 번호
홀드 시간	2	BGP 메시지를 보낸 후, 몇 초간 메시지를 보내지 않아도 되는지에 대해 명시
BGP 식별자	4	BGP 스피커를 식별하는 값
선택사항 파라미터 길이	1	선택사항 파라미터에서 사용하는 바이트 수
선택사항 파라미터	가변	BGP 세션 수립 중 교환해야 하는 추가 파라미터를 전송 할 때 사용

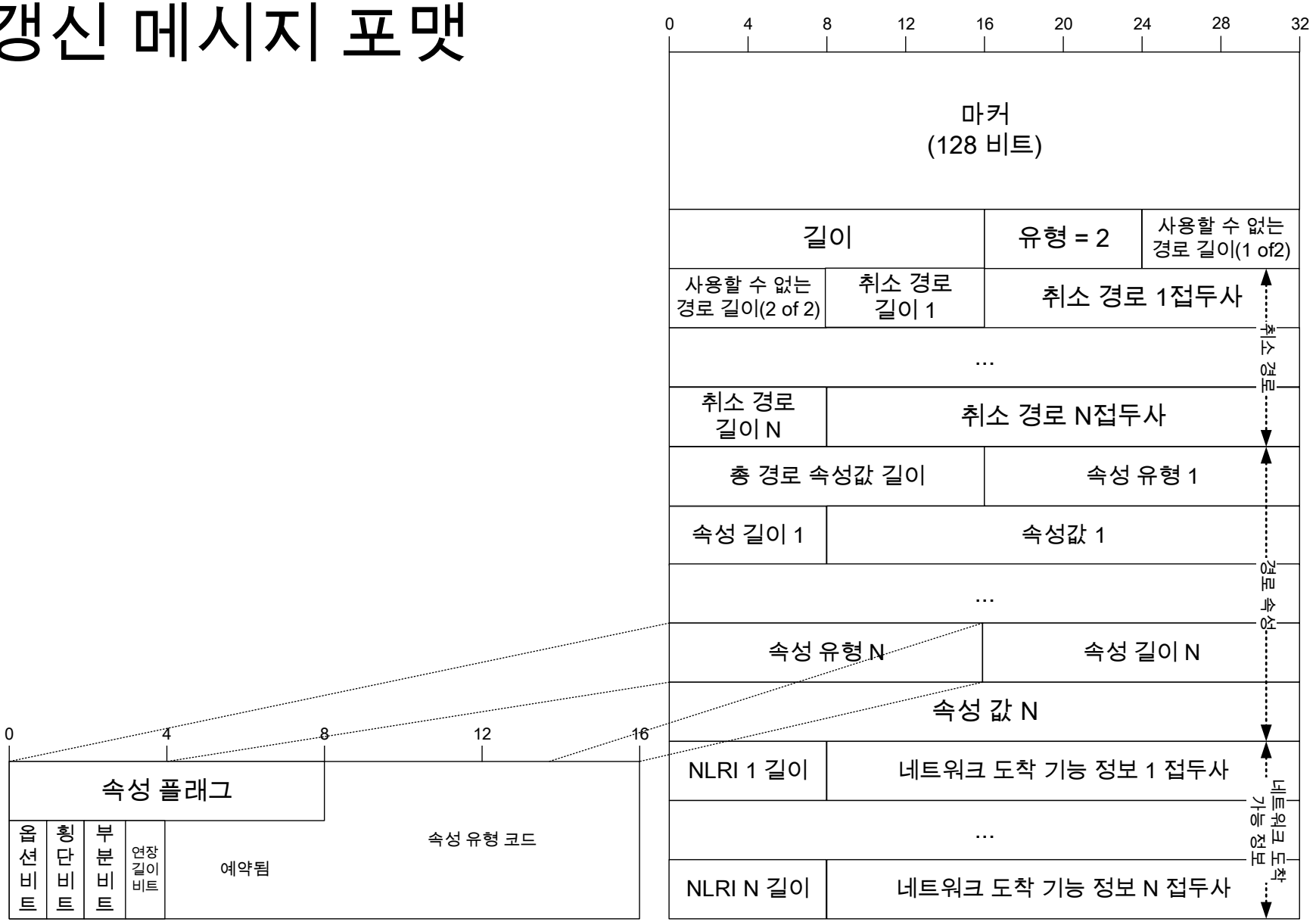
경계 경로 프로토콜(BGP)

- 생성 메시지 포맷
  - 선택 사항 파라미터 구성

하위 필드 명	크기(바이트)	설명
파라미터 유형	1	현재 인증 정보를 위한 단하나의 선택 사항을 정의 (인증 정보일 경우 1로 설정)
파라미터 길이	1	파라미터 값 하위 필드의 길이를 명시 (전체 파라미터 길이에서 2를 뺀 값)
파라미터 값	가변	전달하려는 파라미터의 값

경계 경로 프로토콜(BGP)

- 갱신 메시지 포맷



경계 경로 프로토콜(BGP)

- 갱신 메시지 포맷 설명

하위 필드명	크기(바이트)	설명
속성 유형	4	속성의 유형을 정의
속성 길이	1 or 2	속성의 길이 (속성의 길이가 긴 경우, 연장 길이 플래그를 설정하여 2바이트로 늘림)
속성 값	가변	경로 속성의 유형에 따라 달라짐

하위 하위 필드 명	크기 (바이트)	설명
선택 사항	1	선택 사항 속성이면 1, 잘 알려진 속성이면 0
횡단	1	선택 사항 횡단 속성이면 1, 비 횡단 속성이면 0
부분	1	1이면 횡단 속성에 대한 정보가 일부분, 0이라면 정보가 완전함을 의미
연장 길이	1	0이면 속성 길이 필드가 1바이트라는 것을 의미
예약	4	0으로 설정

값	속성 값 유형
1	근원
2	경로상의 AS
3	다음 홉
4	다중 출구/ 입구 설명(MED)
5	로컬 선호도
6	집선
7	집선 장비

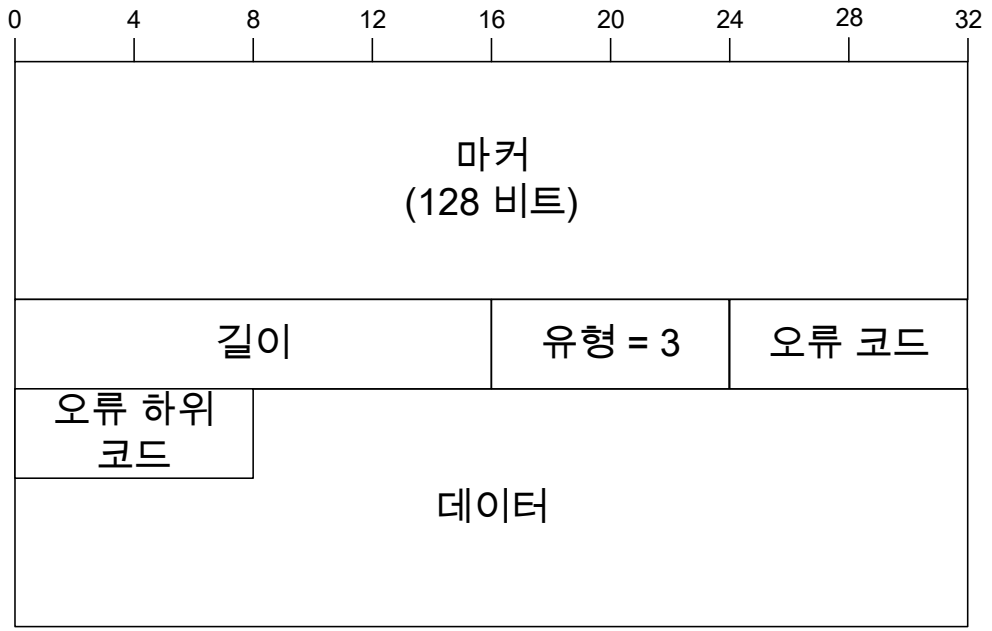
경계 경로 프로토콜(BGP)

- 킵 얼라이브 메시지 포맷

필드명	크기(바이트)	설명
마커	16	메시지의 시작을 식별, 인증하기 위해 사용
길이	2	메시지의 총 길이 (킵 얼라이브 메시지 길이는 19바이트로 고정)
유형	1	BGP 메시지의 유형 (킵 얼라이브 메시지 값은 4)

경계 경로 프로토콜(BGP)

- 통지 메시지 포맷



오류 코드값	코드 이름	설명
1	메시지 헤더 에러	BGP 헤더의 길이나 본문에서 발견된 문제
2	생성 메시지 에러	생성 메시지 본문에서 발견된 문제
3	갱신 메시지 에러	갱신 메시지 본문에서 발견된 문제
4	홀드 타이머 완료	홀드 시간이 만료되기 전에 메시지를 받지 못함
5	유한 상태 머신 에러	한 동작 상태에서 다른 동작 상태로 움직이는 방식
6	종료	다른 오류 코드로 설명하는 에러 상황과는 관계 없이 접속을 끝내고 싶을 때, 사용

기타 라우팅 프로토콜

- TCP/IP 게이트웨이 간 프로토콜(GGP, Gateway-Gateway Protocol)
  - 초기 네트워크의 핵심 라우터 간 경로 정보 통신을 위해 사용된 프로토콜
  - 1982년, “DARPA Internet Gateway” RFC 823 문서로 정의
  - 거리 벡터 알고리즘 사용
    - 홉 수로 장비 간 최적 경로를 결정
    - RIP의 문제점을 가짐
  - 클래스 단위 네트워크에서만 사용
  - AS를 사용하는 방식으로 인터넷 구조가 바뀌어 현재 사용되지 않음

기타 라우팅 프로토콜

- TCP/IP 외부 게이트웨이 프로토콜(EGP, Exterior Gateway Protocol)
  - 초기 네트워크의 비 핵심 라우터들이 네트워크 도착 가능 정보를 교환하기 위해 사용된 프로토콜
  - 1982년, “Exterior Gateway Protocol” RFC 827 문서로 정의
  - BGP로 대체되어 더 이상 사용하지 않음
    - 트리 구조 기반으로 설계되어 다양한 토폴로지에서 사용될 수 없음
    - 임의의 토폴로지에서 라우팅 루프가 생기는 문제가 있음

기타 라우팅 프로토콜

- 내부 경로 제어 프로토콜(IGRP, Interior Gateway Routing Protocol)
  - 1980년대 시스코에서 RIP의 단점을 개선하기 위해 여러 기능을 추가하여 개발한 프로토콜
  - 거리 벡터 알고리즘 사용
    - 홉 수, 대역폭, 지연시간, 안전성 등 여러 가지 척도로 최적 경로 결정
  - 다중 경로 라우팅(Multi path routing) 기능 추가
    - 라우터 간 경로를 자동으로 사용하여 트래픽을 여러 경로에 분산시킴

기타 라우팅 프로토콜

- 확장 내부 경로 제어 프로토콜(EIGRP, Enhanced Interior Gateway Routing Protocol)
  - 1990년대 시스코에서 IGRP를 개선시킨 프로토콜
  - 확산 갱신 알고리즘(DUAL, Diffusing Update Algorithm) 사용
    - 링크의 대역폭과 지연 시간을 결합한 척도를 사용하여 최적 경로를 결정
  - 라우터 간 트래픽 양을 줄임
    - 경로 갱신 정보를 주기적으로 전송하지 않고, 부분 갱신 정보만 전송하기 때문

Thanks!

박 재 형 (jaehyoung@pel.sejong.ac.kr)