

TCP/IP 완벽 가이드

- 2-7부 TCP/IP 라우팅 프로토콜 -

이 하 늘(dlgksmf6789@sju.ac.kr)

세종대학교 프로토콜공학연구실

목 차

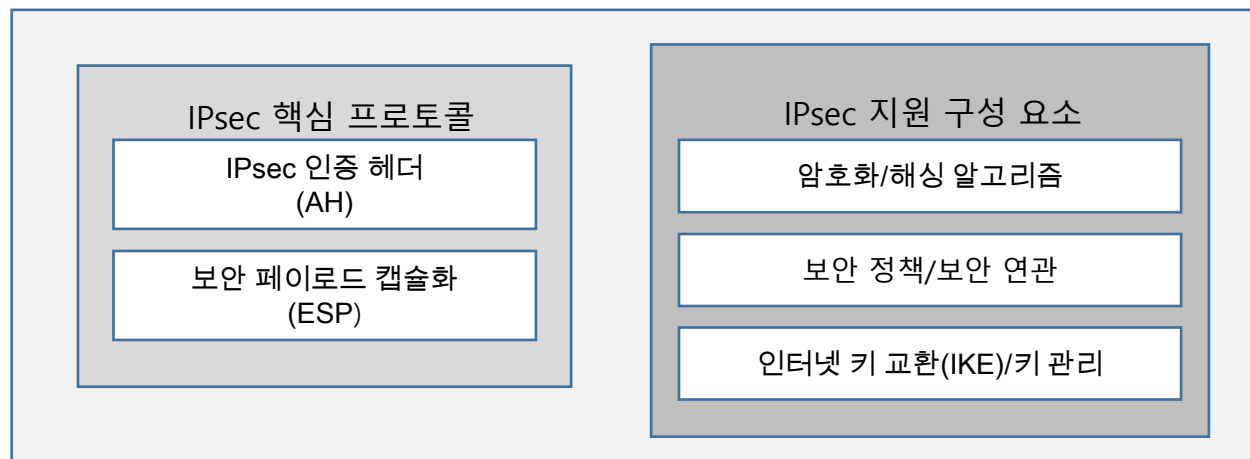
- 보충
 - IP Security(IPsec) 프로토콜
 - IP 이동성 지원(모바일 IP) 프로토콜
- 주요 라우팅 프로토콜 개념
- 라우팅 정보 프로토콜(RIP)
- 최단 경로 우선 프로토콜(OSPF)
- 경계 경로 프로토콜(BGP)
- 기타 라우팅 프로토콜

IP security(IPsec) 프로토콜

- IPsec(Internet Protocol Security)
 - IP의 안전한 통신을 보장하는 프로토콜 모음
 - 등장 배경
 - 네트워크가 확장 되면서 IP에서 보안을 보장하는 방법의 필요성이 증가
 - 기능
 - 데이터 암호화
 - 무결성 보장
 - 보안 공격으로부터 보호
 - 키 협상
 - 보안 모드
 - e.g., 터널모드, 전송모드

IP security(IPsec) 프로토콜

- IPsec의 핵심 프로토콜
 - IPsec 인증 헤더(AH, Authentication Header)
 - 무결성을 목적으로 하여 인증 기능을 제공하는 프로토콜
 - 보안 페이로드 캡슐화(ESP, Encapsulating Security Payload)
 - 데이터의 프라이버시 보호를 목적으로 암호화 기능을 제공하는 프로토콜



IP security(IPsec) 프로토콜

- IPsec 구현 방법
 - 종단 간 구현
 - 모든 호스트 장비에 IPsec을 구현하는 방법
 - 다수의 호스트의 존재로 인해 많은 작업을 필요로 함
 - 라우터 구현
 - 라우터에만 IPsec을 구현하는 방법
 - 종단 호스트 보다 작업량이 적음

IP security(IPsec) 프로토콜

- IPsec 구조

- TCP/IP 프로토콜 스택과 결합하는 방법

- 통합 구조

- IPsec을 IP 자체에 통합
 - IPsec의 보안 모드와 기능을 일반 IP처럼 쉽게 제공 가능
 - 추가 하드웨어나 계층이 필요하지 않음
 - 실용적이지 않음

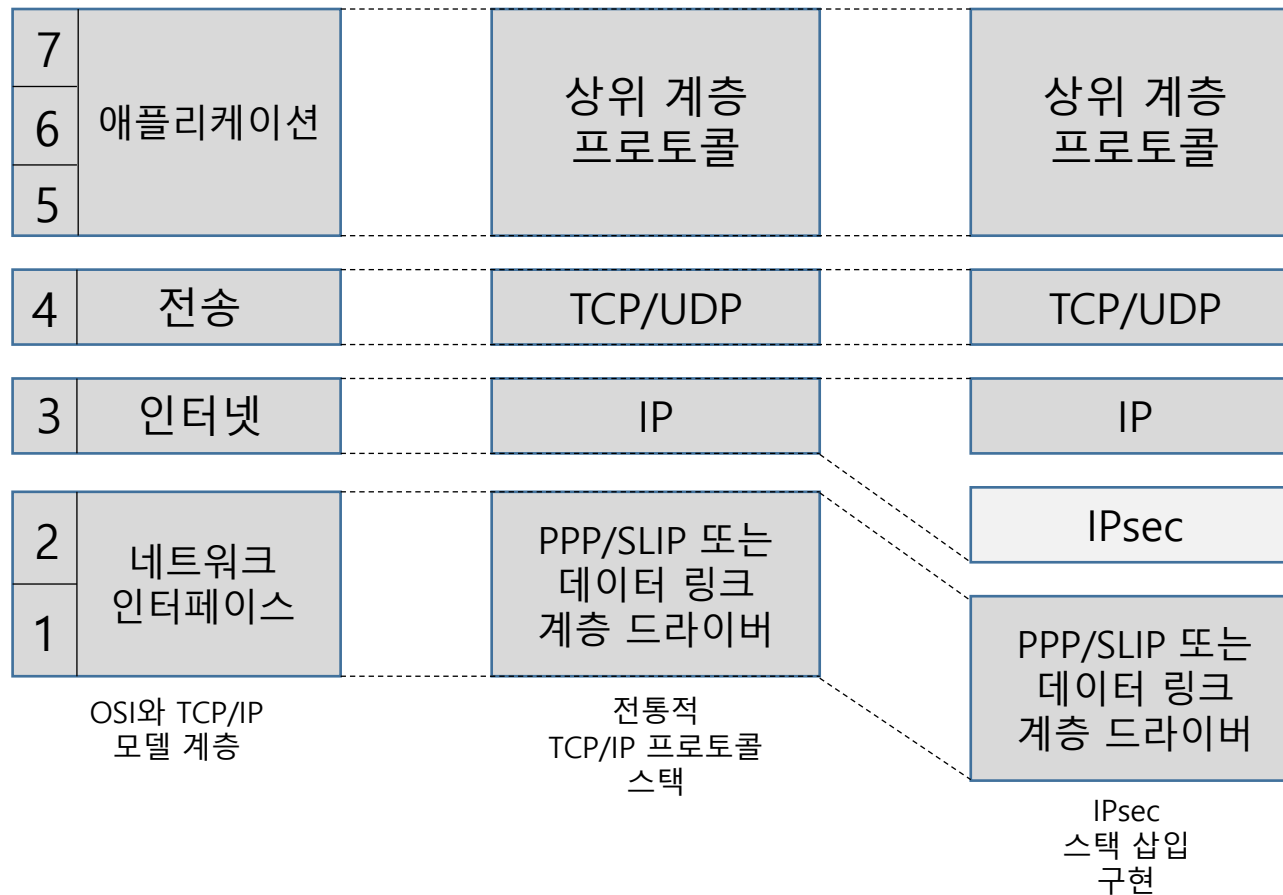
- 스택 삽입(BITS, Bump In The Stack) 구조

- IP와 IPsec이 별도의 계층으로 존재
 - IP 데이터그램이 아래 방향으로 이동하는 동안 IPsec은 그것을 가로채 보안 기능을 덧붙여 데이터 링크 계층으로 전달

IP security(IPsec) 프로토콜

- IPsec 구조

- TCP/IP 프로토콜 스택과 결합하는 방법
 - 스택 삽입(BITS) 구조



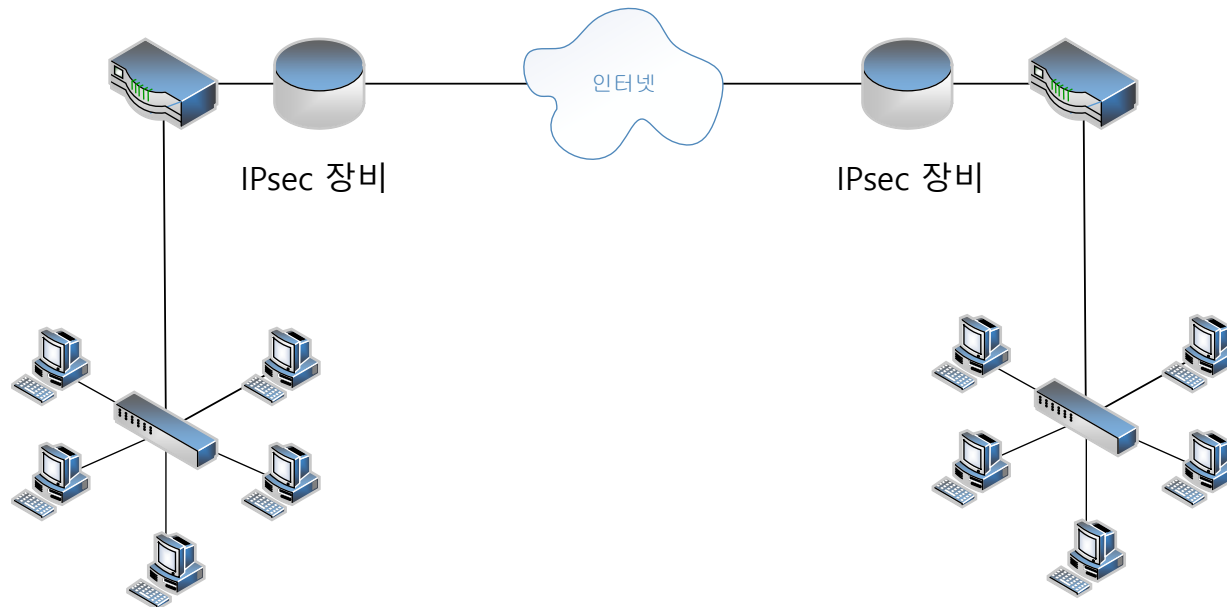
IP security(IPsec) 프로토콜

- IPsec 구조

- TCP/IP 프로토콜 스택과 결합하는 방법

- 라인 삽입(BITW, Bump In The Wire)

- IPsec 서비스를 제공하는 하드웨어 장비를 추가
 - 외부로 나가는 데이터그램을 가로채 IPsec 보호 기능을 추가해 송신
 - 내부로 들어오는 데이터그램의 IPsec 관련 헤더 제거
 - 네트워크가 복잡해지고 구현 비용이 비쌘

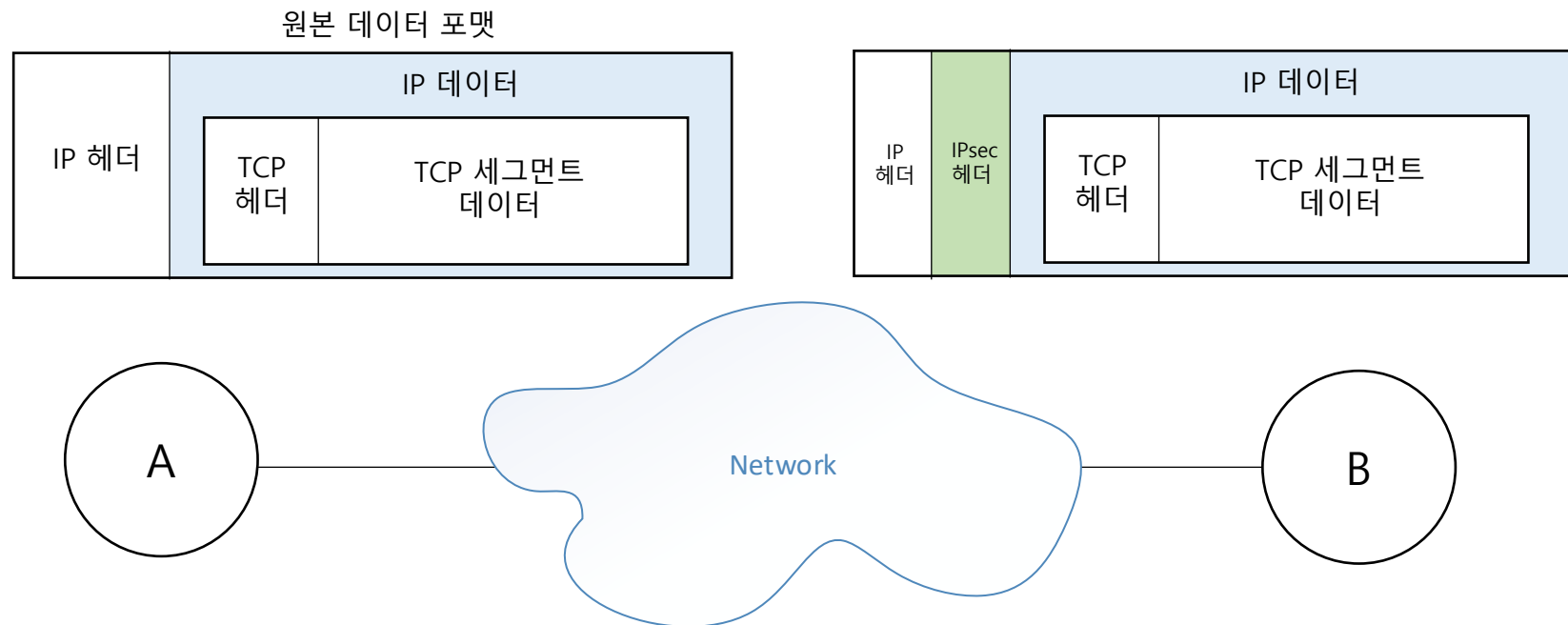


IP security(IPsec) 프로토콜

- IPsec 동작 모드

- 전송 모드

- 전송 계층에서 IP로 내려온 메시지를 보호
- AH, ESP, 혹은 AH와 ESP가 함께 있는 조합에 의해 처리
- IPsec 헤더는 원본 IP헤더와 IP 페이로드 사이에 위치

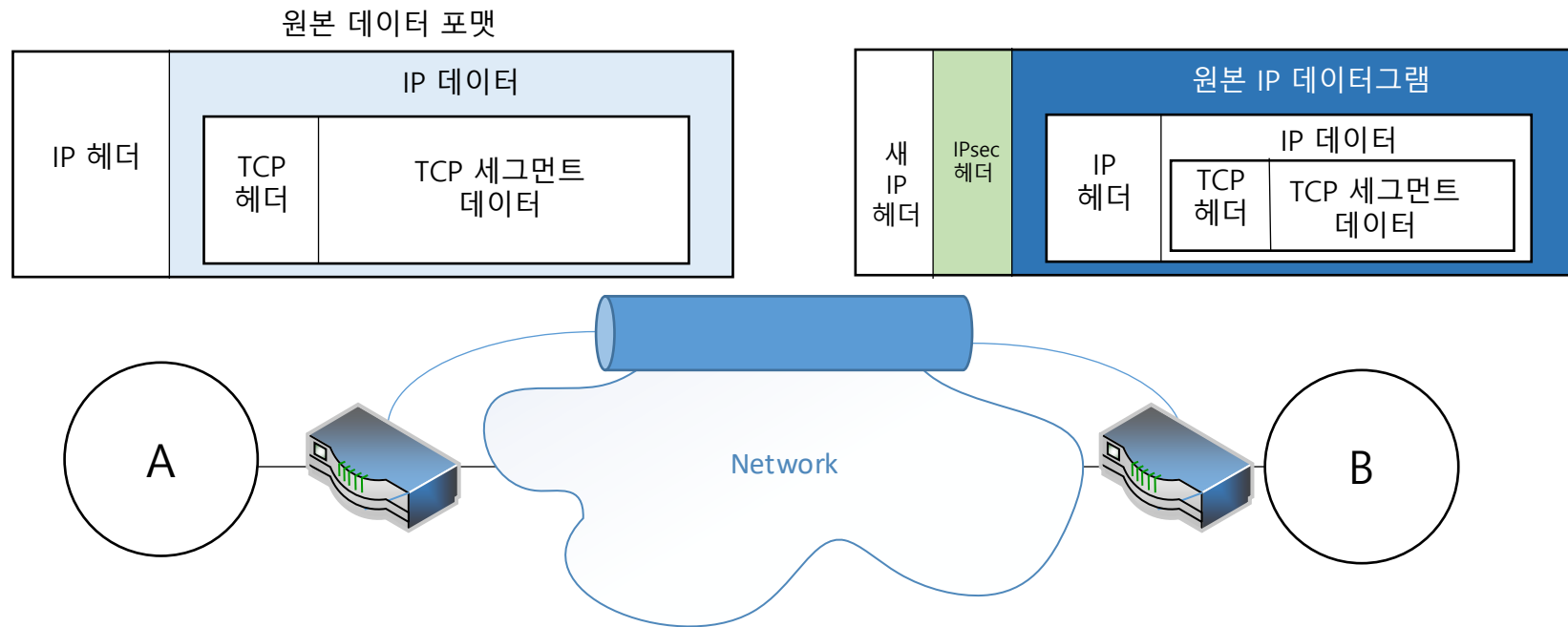


IP security(IPsec) 프로토콜

- IPsec 동작 모드

- 터널 모드

- 원본 데이터와 IP헤더를 캡슐화한 데이터그램 보호
- 라우터에 의해 새 IP 헤더 추가



IP security(IPsec) 프로토콜

- IPsec 보안 구성 요소

- 보안 연관(SA, Security Association)

- 한 장비와 다른 장비 사이에 인증과 암호 키를 주고 받는 방법을 명시

- 보안 연관 데이터베이스(SAD, Security Association Database)

- 장비의 보안 연관을 저장

- 보안 연관 트리플

- 보안 인자 색인(SPI, Security Parameters Index)

- 메시지 수신자가 데이터그램에 어떤 SA가 적용되었는지 파악하는데 사용

- IP 목적지 주소

- SA가 수립된 장비의 주소

- 보안 프로토콜 식별자

- 이 연관이 AH를 위한 것인지 ESP를 위한 것인지 지정

IP security(IPsec) 프로토콜

- IPsec 보안 구성 요소
 - 보안 정책(SP, Security Policy)
 - IPsec에 내장된 규칙
 - 장비가 수신하는 서로 다른 데이터그램을 어떻게 처리할 지 지시
 - 보안 정책 데이터베이스(SPD, Security Policy Database)에 저장

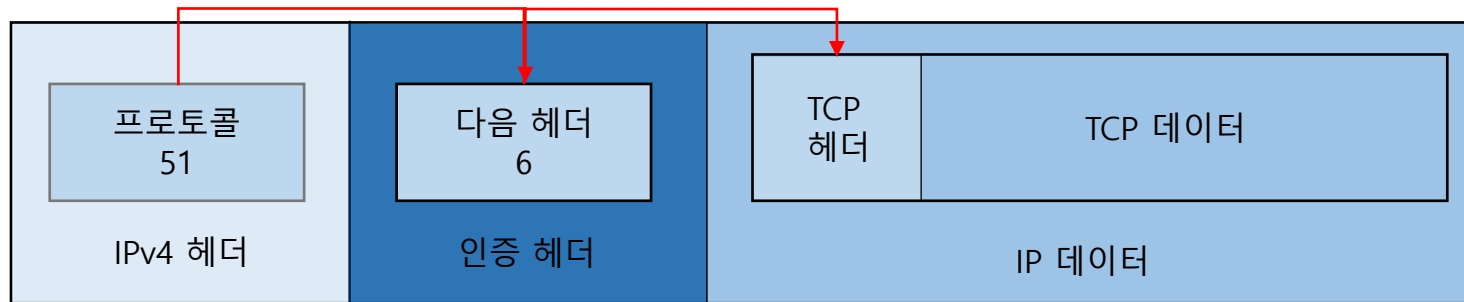
IP security(IPsec) 프로토콜

- IPsec 인증 헤더(AH)

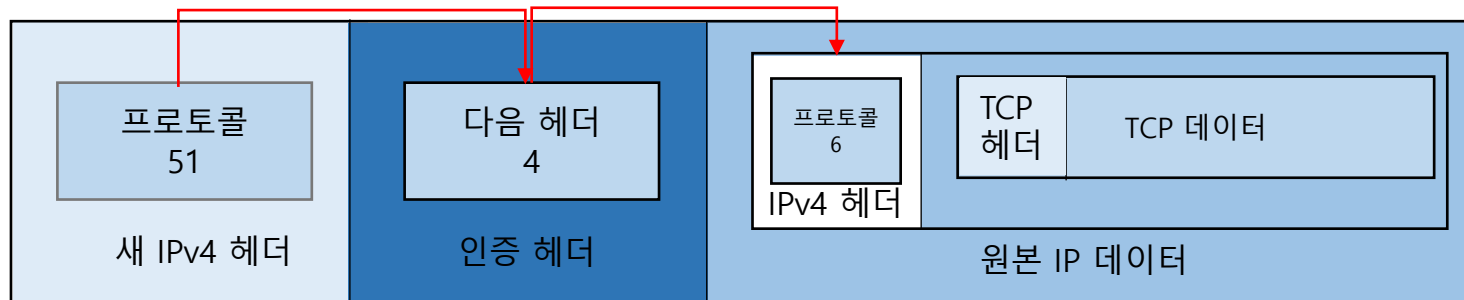
- 헤더를 추가하여 데이터그램 전체 또는 일부분에 대한 인증을 제공
- 무결성은 보장하지만 프라이버시는 보장하지 않음
- 과정
 - 특정 해싱 알고리즘과 키 사용하여 계산
e.g., MD5, SHA-1
 - 계산을 수행한 결과(ICV, Integrity Check Value)를 다른 필드와 함께 헤더에 넣어 전송
 - 헤더의 위치는 IPsec 모드 혹은 IP 버전에 따라 달라짐
 - 목적지 장비는 두 장비가 공유하는 키를 이용하여 계산 결과가 일치하는지 확인

IP security(IPsec) 프로토콜

- IPsec 인증 헤더(AH)
 - AH 데이터그램 위치와 연결
 - 전송 모드

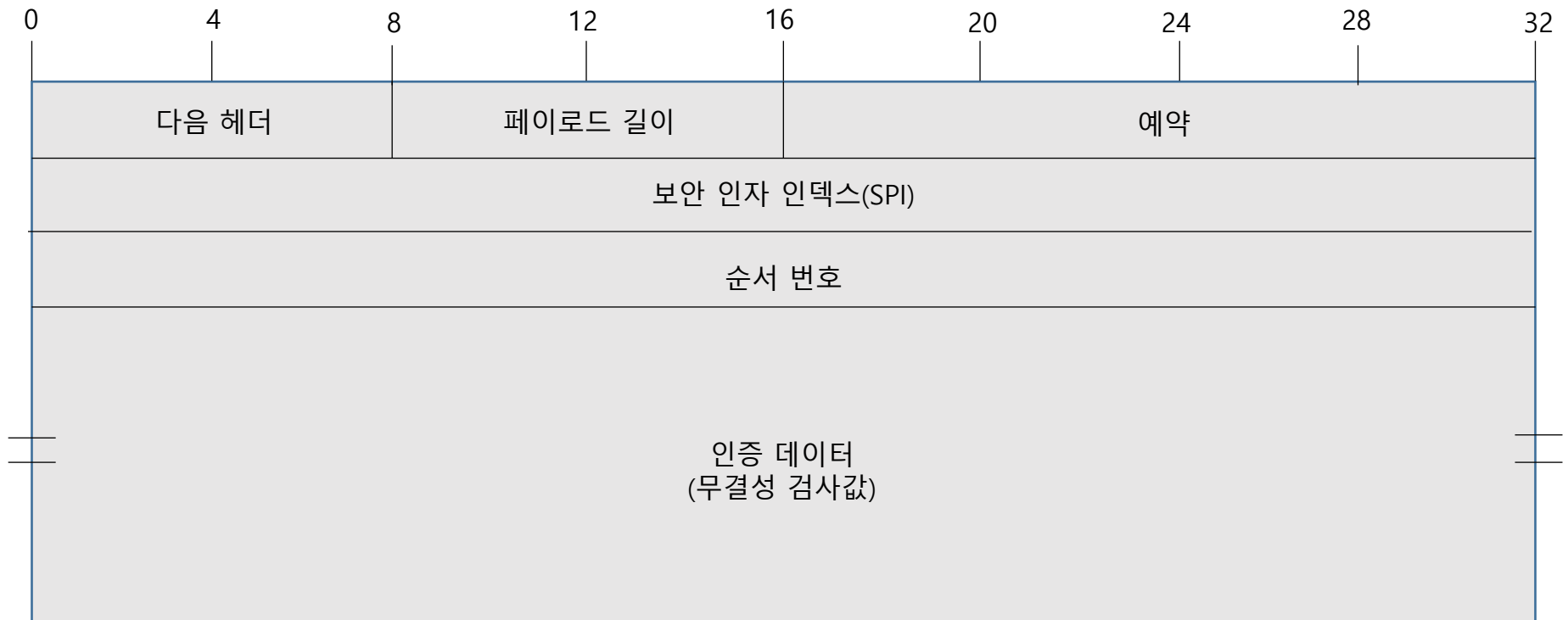


- 터널 모드



IP security(IPsec) 프로토콜

- IPsec 인증 헤더(AH)
- AH 포맷



IP security(IPsec) 프로토콜

- IPsec 인증 헤더(AH)
- AH 포맷

필드 이름	크기	설명
다음 헤더	1	AH 다음에 오는 헤더의 프로토콜 번호
페이로드 길이	1	인증 헤더 자체의 길이
예약	2	쓰이지 않음, 0으로 설정
SPI	4	목적지 주소와 보안 프로토콜 유형(AH)과 함께 패킷에 쓰이는 보안 연관(SA)을 식별
순서 번호	4	패킷이 송신될 때마다 값을 증가시켜 재전송 공격을 방지
인증 데이터	가변적	해시 알고리즘의 계산 결과인 무결성 검사 값(ICV)을 포함

IP security(IPsec) 프로토콜

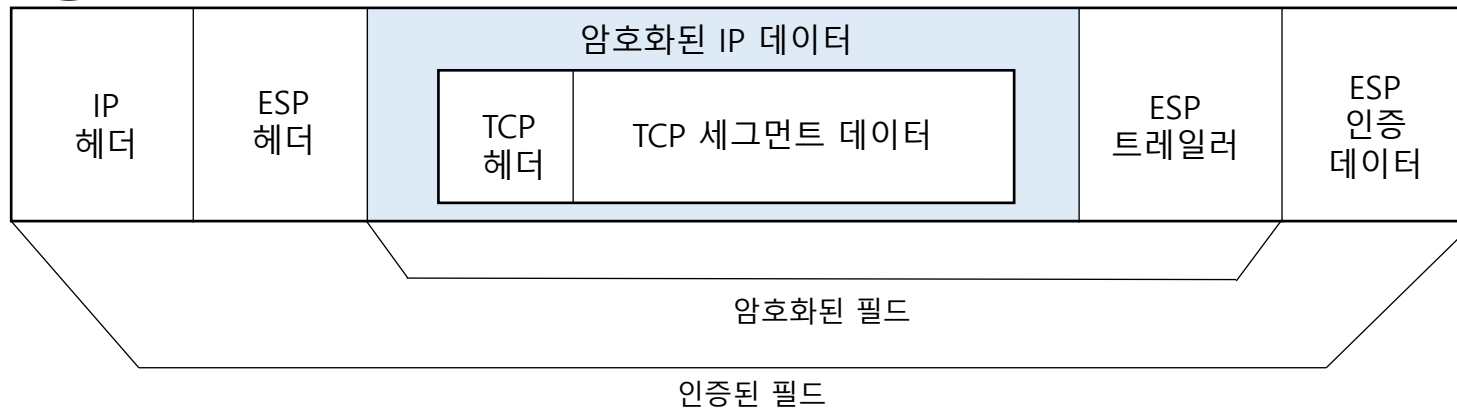
- IPsec 보안 페이로드 캡슐화(ESP)
 - IP 데이터그램을 암호화하여 프라이버시를 보장
 - ESP 필드
 - ESP 헤더
 - 보안 인자 색인(SPI)과 순서 번호 두 필드를 포함하며 암호화된 데이터 앞에 위치
 - ESP 트레일러
 - 암호화된 데이터 뒤에 위치하여 다음 헤더 필드 포함
 - ESP 인증 데이터
 - ICV 포함
 - ESP 선택적 인증 기능이 적용될 때 사용

IP security(IPsec) 프로토콜

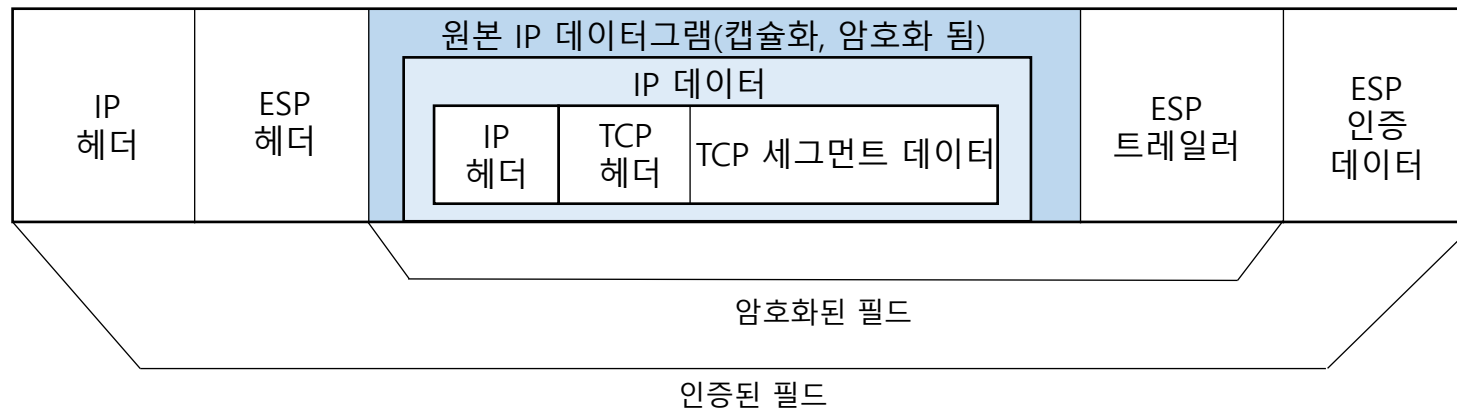
- IPsec 보안 페이로드 캡슐화(ESP)

- ESP 동작과 필드 사용

- 전송 모드

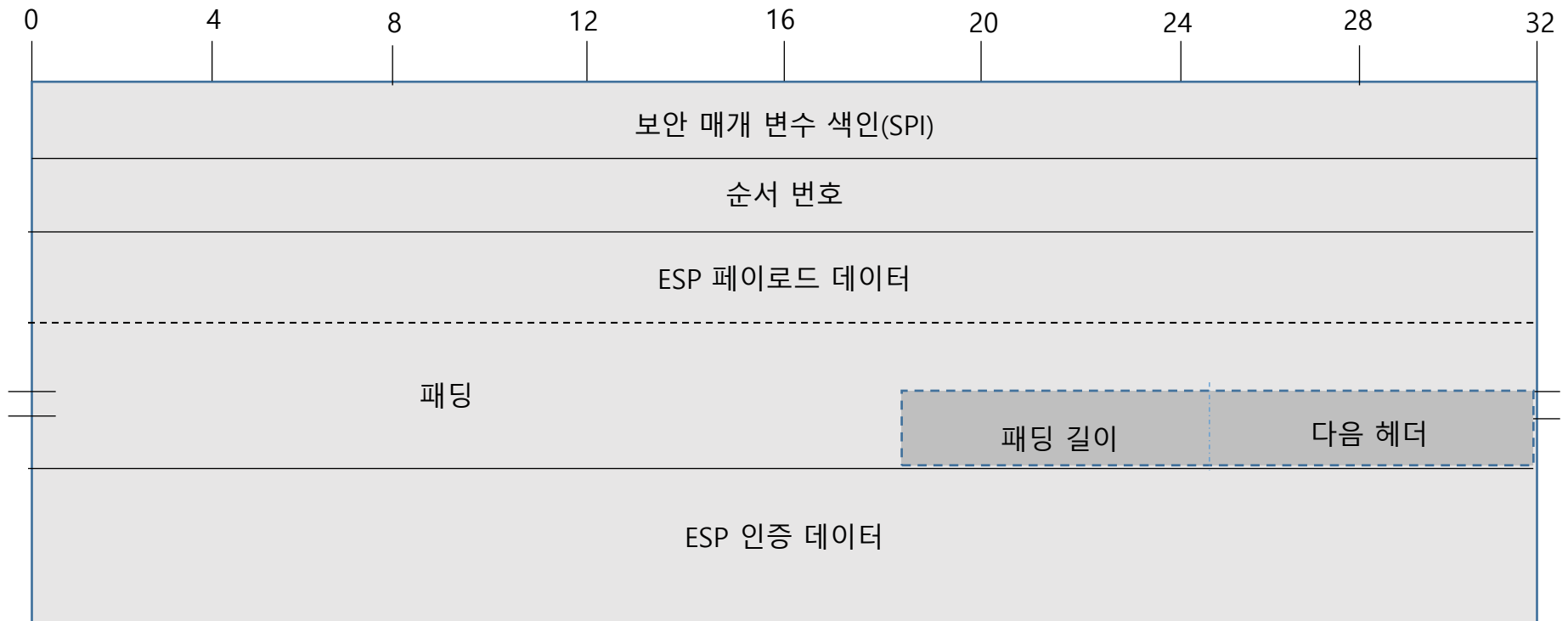


- 터널 모드



IP security(IPsec) 프로토콜

- IPsec 보안 페이로드 캡슐화(ESP)
- ESP 포맷



IP security(IPsec) 프로토콜

- IPsec 보안 페이로드 캡슐화(ESP)
- ESP 포맷

구간	필드 이름	크기	설명	암호화 범위	인증 범위
ESP 헤더	SPI	4	32비트 값으로, 패킷에 쓰이는 보안 연관(SA)을 식별		
	순서 번호	4	패킷이 송신될 때마다 값을 증가시켜 재전송 공격 방지		
페이로드	페이로드	가변적	암호화된 페이로드 데이터		
ESP 트레일러	패딩	가변적	암호화 또는 정렬을 위해 추가적인 패딩 바이트가 포함됨		
	패딩 길이	1	패딩 필드의 바이트 수		
	다음 헤더	1	패킷에서 다음 헤더의 프로토콜 번호를 포함		
ESP 인증 데이터		가변적	해시 알고리즘의 계산 결과인 무결성 검사 값(ICV)을 포함		

IP security(IPsec) 프로토콜

- IPsec 인터넷 키 교환(IKE, Internet Key Exchange)
 - 두 장비 사이에 안전하게 데이터를 암호화 하기 위해 비밀 정보를 교환하는 프로토콜
 - 개요
 - IPsec 장비가 SA를 자동으로 교환하도록 함
 - ISAKMP(Internet Security Association and Key Management Protocol)
 - 암호화 키와 보안 연관 정보를 교환하기 위한 구조 제공
 - 동작
 - 단계1
 - 두 장비가 어떻게 안전하게 정보를 교환할지에 대해 협상하는 과정
 - 협상을 통해 ISAKMP 자체를 위한 SA를 생성
 - 단계2
 - 1단계에서 수립한 SA를 이용하여 기타 보안 프로토콜을 위한 SA 생성
 - AH와 ESP를 위한 SA 인자를 협상

목 차

- 보충
 - IP Security(IPsec) 프로토콜
 - IP 이동성 지원(모바일 IP) 프로토콜
- 주요 라우팅 프로토콜 개념
- 라우팅 정보 프로토콜(RIP)
- 최단 경로 우선 프로토콜(OSPF)
- 경계 경로 프로토콜(BGP)
- 기타 라우팅 프로토콜

IP 이동성 지원(모바일 IP) 프로토콜

- 개요

- IP에서 이동 장비 문제

- 장비의 IP 주소는 네트워크에 연결되어 있다는 특성을 지님

- 방안

- IP 주소 변경

- 이동한 네트워크 쪽의 주소를 가지도록 변경

- IP 라우팅과 주소 간의 연결 끊기

- 전체 주소를 보고 다른 효율적인 라우터로 연결을 하도록 라우팅 방식을 바꿈

- 문제

- 시간이 매우 오래 걸림

- 다른 장비에게 바뀐 주소를 어떻게 알려야 하는가

IP 이동성 지원(모바일 IP) 프로토콜

- 개요

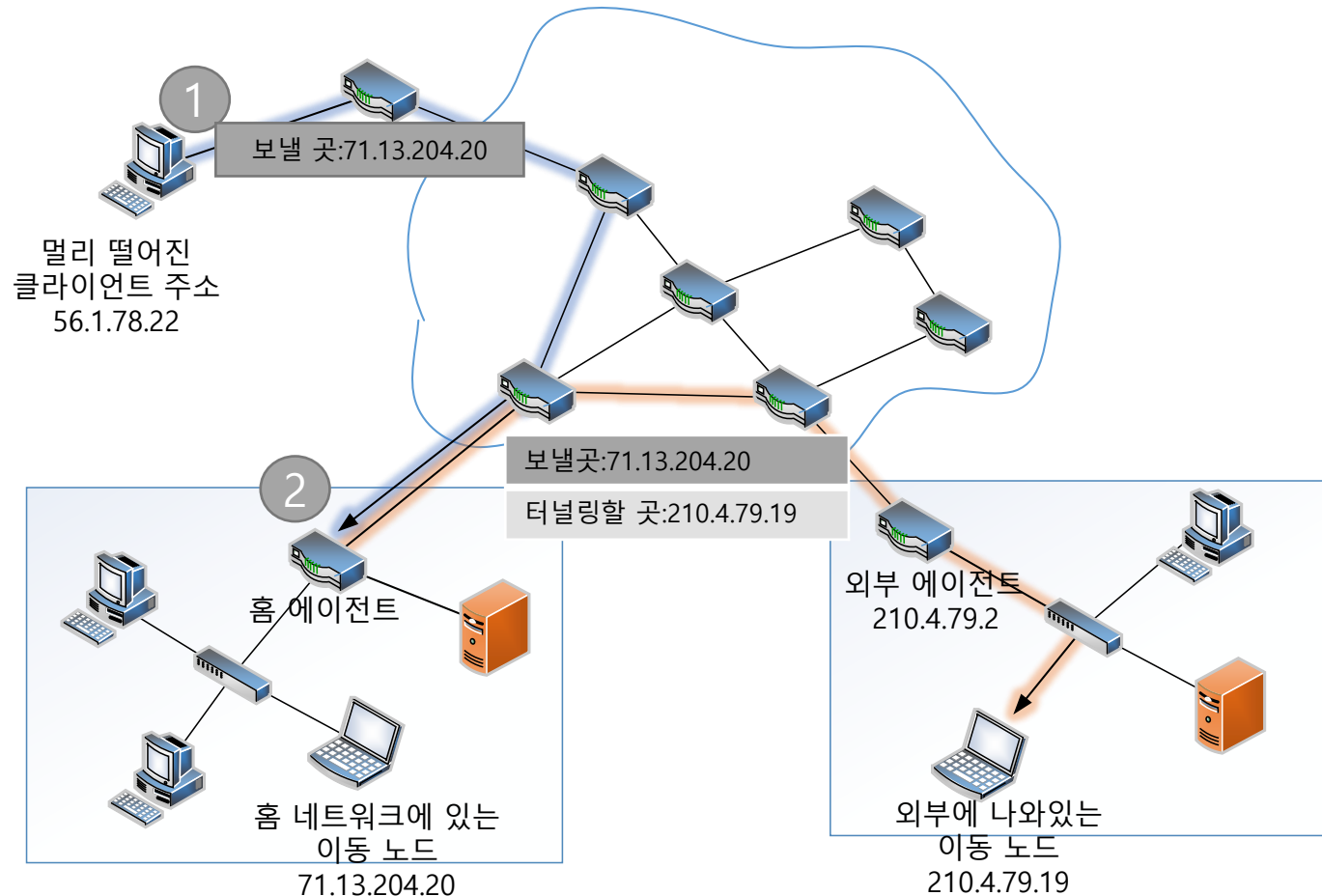
- 목표

- 기존 장비 주소를 사용하는 중단 없는 장비 이동성 지원
 - 새로운 주소 지정 방식이나 라우팅 수정 불필요
 - 모바일 IP가 어떻게 동작하는지 모르는 다른 장비와 통신 가능
- 하드웨어 변경 최소화
 - 홈 에이전트를 두는 것으로 인해 장비 변경을 최소화
- 보안
 - 인증 과정을 거침

IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP

- 홈 네트워크에 도착한 패킷을 이동 장비가 있는 외부 네트워크로 보내는 시스템



IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 장비 역할

- 이동 장비

- 네트워크 간을 이동하는 장비

- 홈 에이전트

- 홈 네트워크의 라우터

- 이동 장비가 받아야 할 데이터그램을 대신 받아서 전달

- 외부 에이전트

- 외부 네트워크의 라우터

- 홈 네트워크가 전달한 데이터그램을 받아서 이동 장비에게 전달

IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 주소

- 홈 주소

- 이동 장비에게 할당된 고정 IP 주소

- CoA(Care-of Address)

- 이동 장비가 홈 네트워크 외부로 움직였을 때의 임시 주소
 - 모바일 IP에서만 사용

IP 이동성 지원(모바일 IP) 프로토콜

- CoA의 종류

- 외부 에이전트 CoA

- 이동 장비가 자신만의 IP를 가지지 않고 외부 에이전트 CoA를 사용
- 장점
 - 같은 네트워크에 있는 모든 장비들이 같은 외부 CoA 사용
 - 여분의 주소나 주소를 얻기 위한 작업이 필요 없음
- 단점
 - 홈 에이전트가 보내는 모든 데이터그램은 외부 에이전트를 지나감

IP 이동성 지원(모바일 IP) 프로토콜

- CoA의 종류

- 공존 CoA

- 모바일 IP가 아닌 다른 기법을 사용해서 이동 장비에게 직접 할당된 주소
e.g., DHCP
- 외부 에이전트가 없거나 있더라도 오랫동안 연결을 유지하려 할 때 사용
- 장점
 - 홈 에이전트가 데이터그램을 직접 이동 장비에게 전달 가능
- 단점
 - 주소 고갈 문제가 생길 수 있음

IP 이동성 지원(모바일 IP) 프로토콜

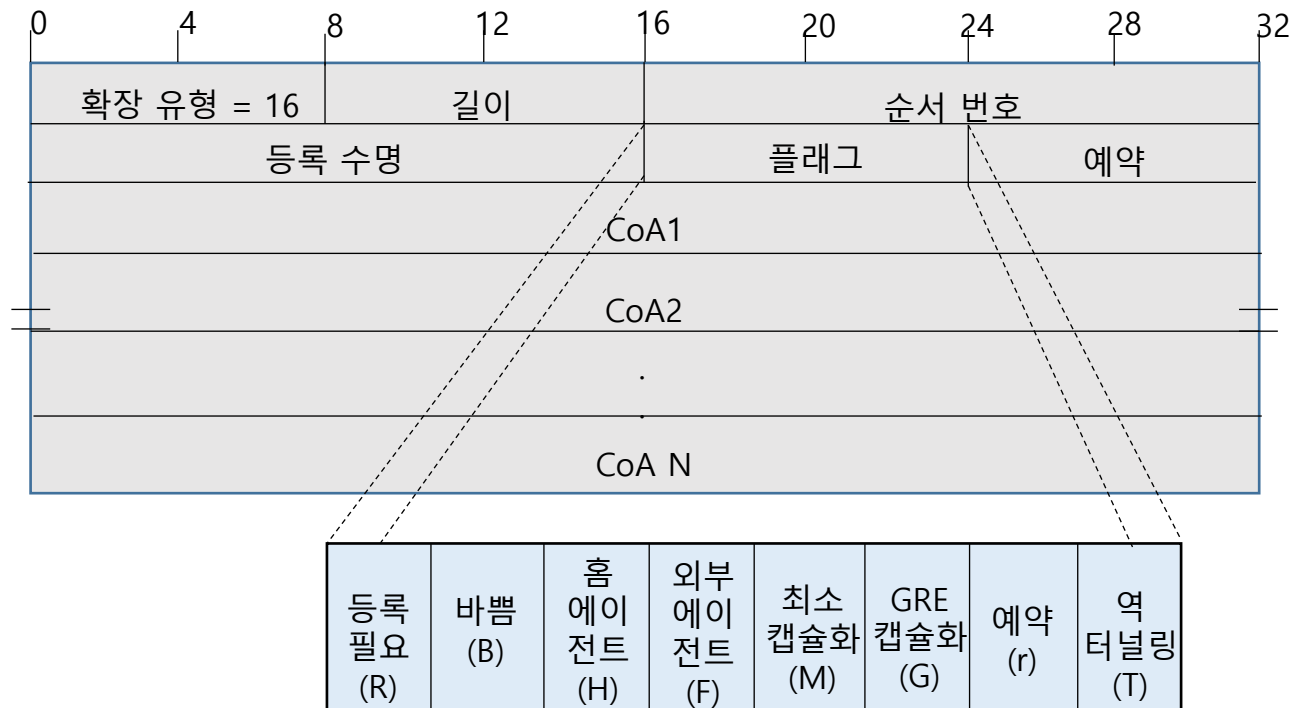
- 모바일 IP 에이전트 발견
 - 에이전트 발견의 목적
 - 에이전트/노드 통신
 - 에이전트는 자신에 대한 정보를 담은 메시지를 노드에게 전송
 - 노드는 에이전트에게 정보를 보내 달라고 요청
 - 현재 위치 발견
 - 노드가 홈 네트워크에 있는지 외부 네트워크에 있는지 확인
 - CoA 할당
 - 외부 에이전트 CoA를 사용하면 에이전트 발견 과정 중에 이동 장비가 사용할 CoA를 얻음

IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 에이전트 발견

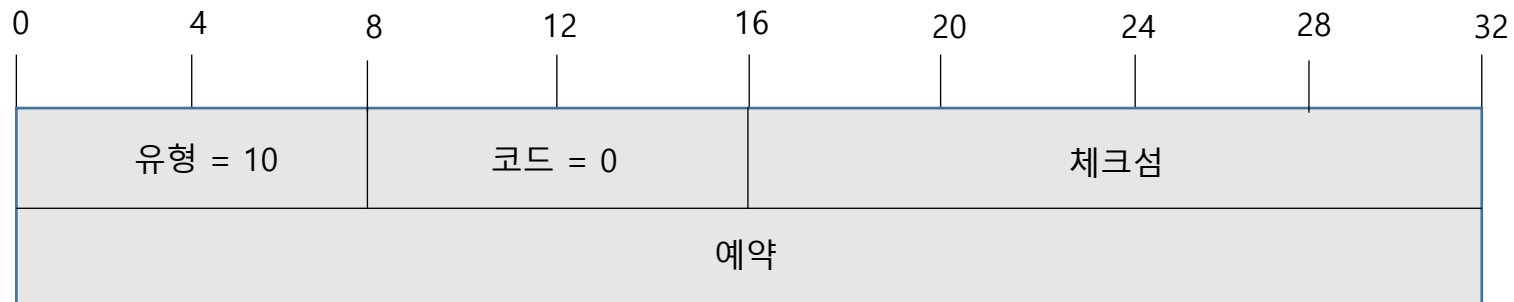
- 에이전트 광고

- 에이전트로 활동할 수 있는 라우터가 정기적으로 전송
- 자신의 존재와 기능을 노드에게 알림
- 메시지 포맷



IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 에이전트 발견
 - 에이전트 요청
 - 모바일 IP 장비가 로컬 에이전트에게 광고 메시지를 보내 달라고 요청
 - 메시지 포맷



IP 이동성 지원(모바일 IP) 프로토콜

- 에이전트 등록

- 홈 에이전트 등록

- 이동 장비가 홈 에이전트와 통신을 하면서 정보와 지시를 주고받는 것

- 홈 에이전트 등록 이벤트

- 등록 이동

- 장비가 외부 네트워크에 도착하면 등록 시작

- 등록 해제

- 홈 네트워크로 돌아오면 전달 취소

- 재등록

- 이동 시 CoA가 바뀌면 이동 장비는 홈 에이전트에게 알려 등록 수정

IP 이동성 지원(모바일 IP) 프로토콜

- 에이전트 등록

- 등록 요청과 등록 응답 메시지

- 사용자 데이터그램 프로토콜(UDP, User Datagram Protocol) 사용

- 등록은 다른 모바일 IP 통신과 달리 더 높은 계층에서 일어남

- 등록 과정

- 이동 장비가 사용하는 CoA의 종류에 따른 두 가지 방식

- 직접 등록(공존 CoA)

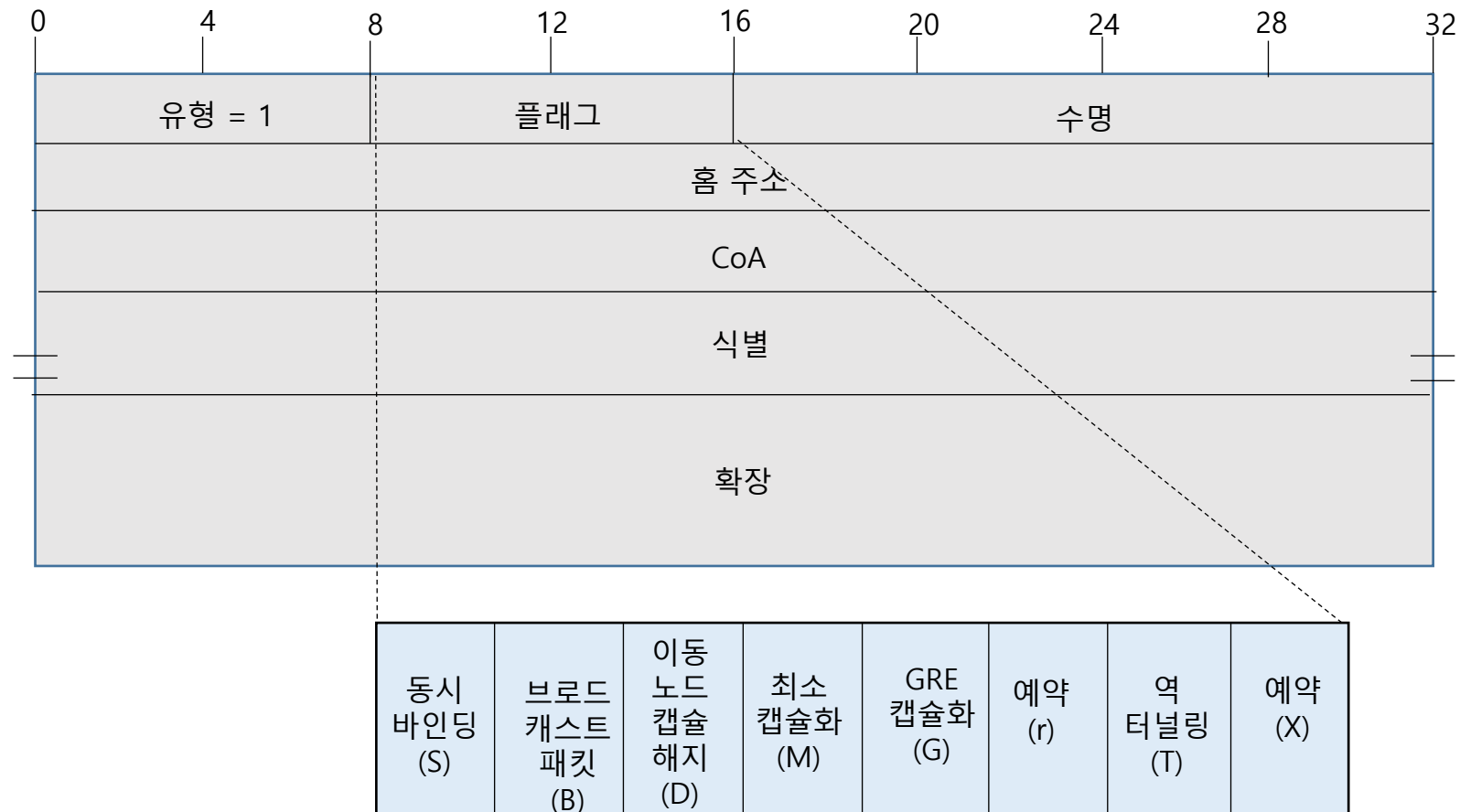
- 1. 이동 장비가 홈 에이전트에게 등록 요청 메시지 전송
 - 2. 홈 에이전트는 이동 장비에게 등록 응답 메시지 전송

- 간접 등록(외부 에이전트 CoA)

- 1. 이동 장비가 외부 에이전트에게 등록 요청 메시지 전송
 - 2. 외부 에이전트가 등록 요청을 처리하여 홈 에이전트에게 전송
 - 3. 홈 에이전트는 외부 에이전트에게 등록 응답 메시지 전송
 - 4. 외부 에이전트가 등록 응답을 받아 처리하고 이동장비에게 전송

IP 이동성 지원(모바일 IP) 프로토콜

- 에이전트 등록
- 등록 요청 메시지 포맷



IP 이동성 지원(모바일 IP) 프로토콜

- 에이전트 등록
- 등록 응답 메시지 포맷



IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 데이터 캡슐화와 터널링
 - 홈 에이전트는 패킷을 캡슐화하여 이동 장비의 CoA로 전달
- 모바일 IP 터널링
 - 캡슐화된 데이터그램의 자세한 정보를 임시로 숨김
 - 외부 에이전트 CoA
 - 외부 에이전트에서 터널이 끝남
 - 캡슐화된 데이터그램을 받아 헤더를 벗겨 원래 데이터그램을 이동 장비에게 전달
 - 외부 에이전트와 이동 장비는 같은 로컬 네트워크에 있기 때문에 데이터 링크 계층을 통해 전송
 - 공존 CoA 주소
 - 이동 장비에서 터널이 끝남
 - 장비가 캡슐화 헤더를 벗김

IP 이동성 지원(모바일 IP) 프로토콜

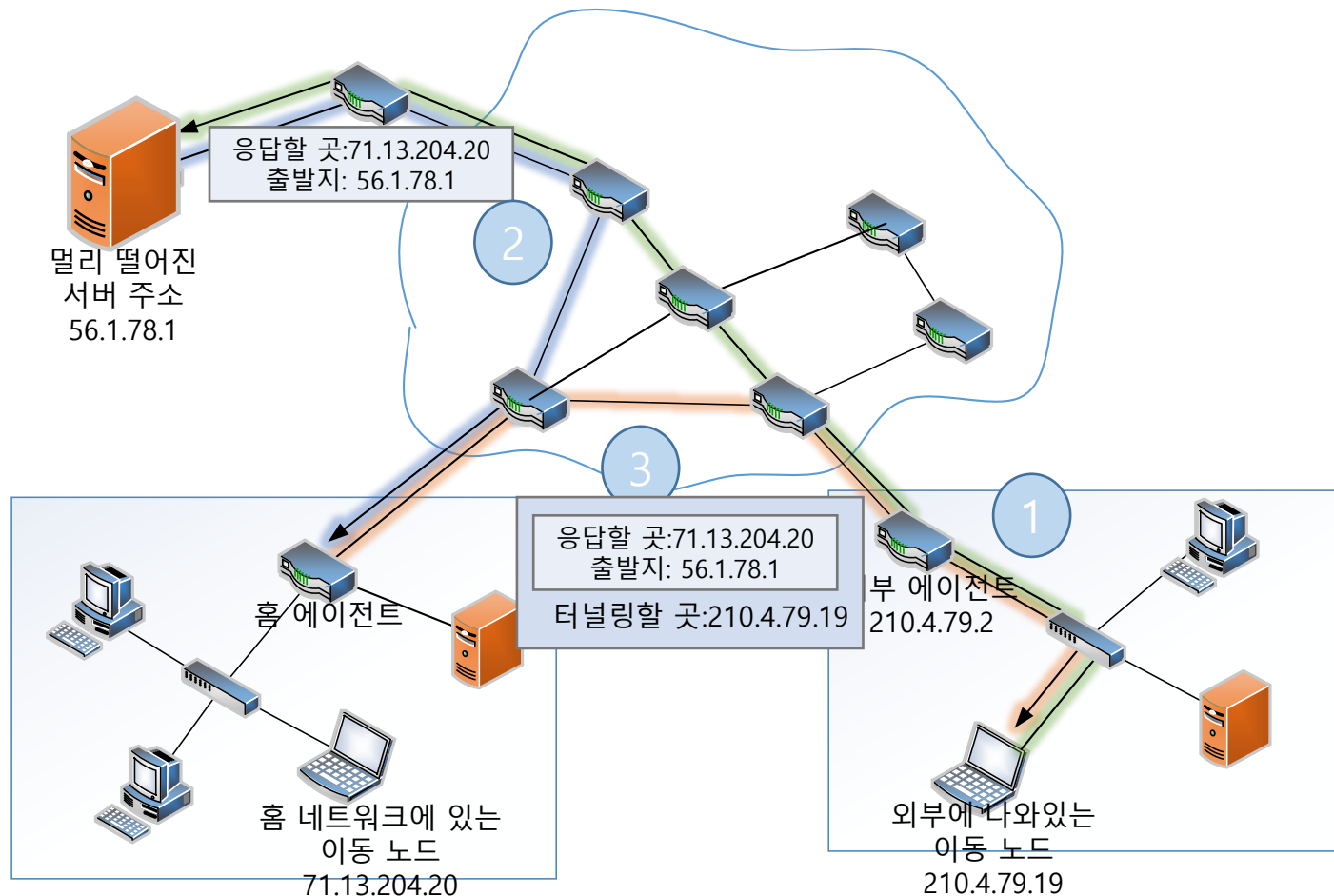
- 모바일 IP 데이터 캡슐화와 터널링

- 터널링 과정

1. 이동 장비는 외부 네트워크 어딘가에 있는 서버에게 모바일 IP 요청
2. 해당 서버는 이동 장비의 출발지 주소인 홈 네트워크로 응답 메시지 전송
3. 홈 에이전트는 도착한 응답을 이동 장비에게 터널링

IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 데이터 캡슐화와 터널링
- 터널링 동작 과정



IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 데이터 캡슐화와 터널링
 - 역터널링
 - 이동 장비가 데이터그램을 인터넷에 직접 전송할 수 없을 경우 사용
 - 홈 에이전트와 이동 장비 사이에 생기거나 외부 에이전트와 홈 에이전트 사이에 생김
 - 이동 장비는 데이터그램을 직접 전송하지 않고 홈 에이전트와의 터널을 통해 전송

IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP와 TCP/IP 주소 결정 프로토콜

- 이동 장비가 로컬 호스트에 없어 ARP를 사용할 수 없을 경우

- 해결 방법

1. ARP 프록싱

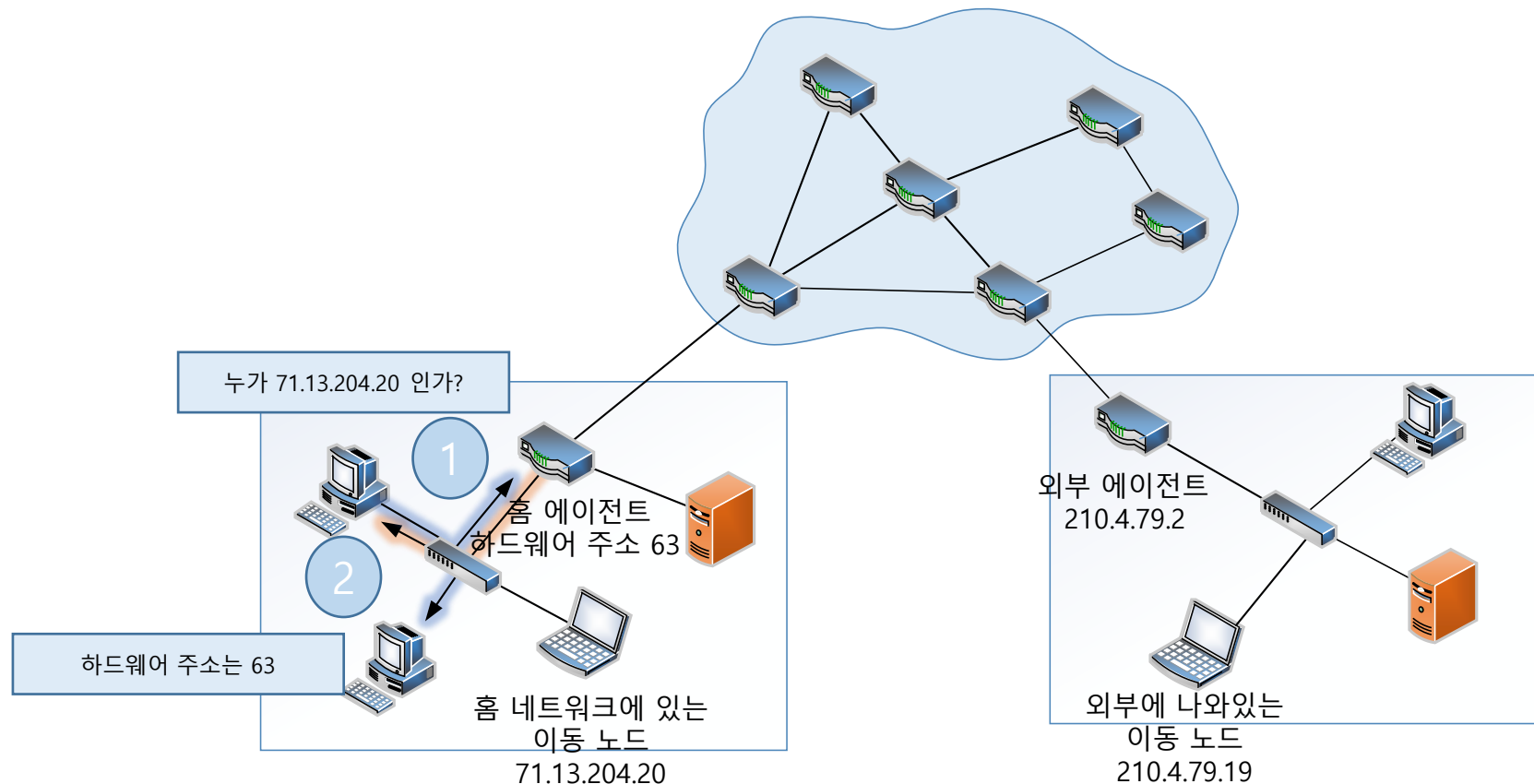
- 홈 에이전트는 이동 장비 대신 ARP 요청을 받음
- 대신 응답하면서 자신의 데이터 링크 계층 주소를 알림
- 홈 에이전트는 해당 데이터그램을 이동 장비에게 전송

2. 무상 ARP

- 이미 이동 장비에 대한 캐시를 갖고 있는 노드일 경우
- 홈 에이전트는 무상 ARP를 전송하여 이동 장비와 자신의 데이터 링크 계층 주소가 같다고 알림

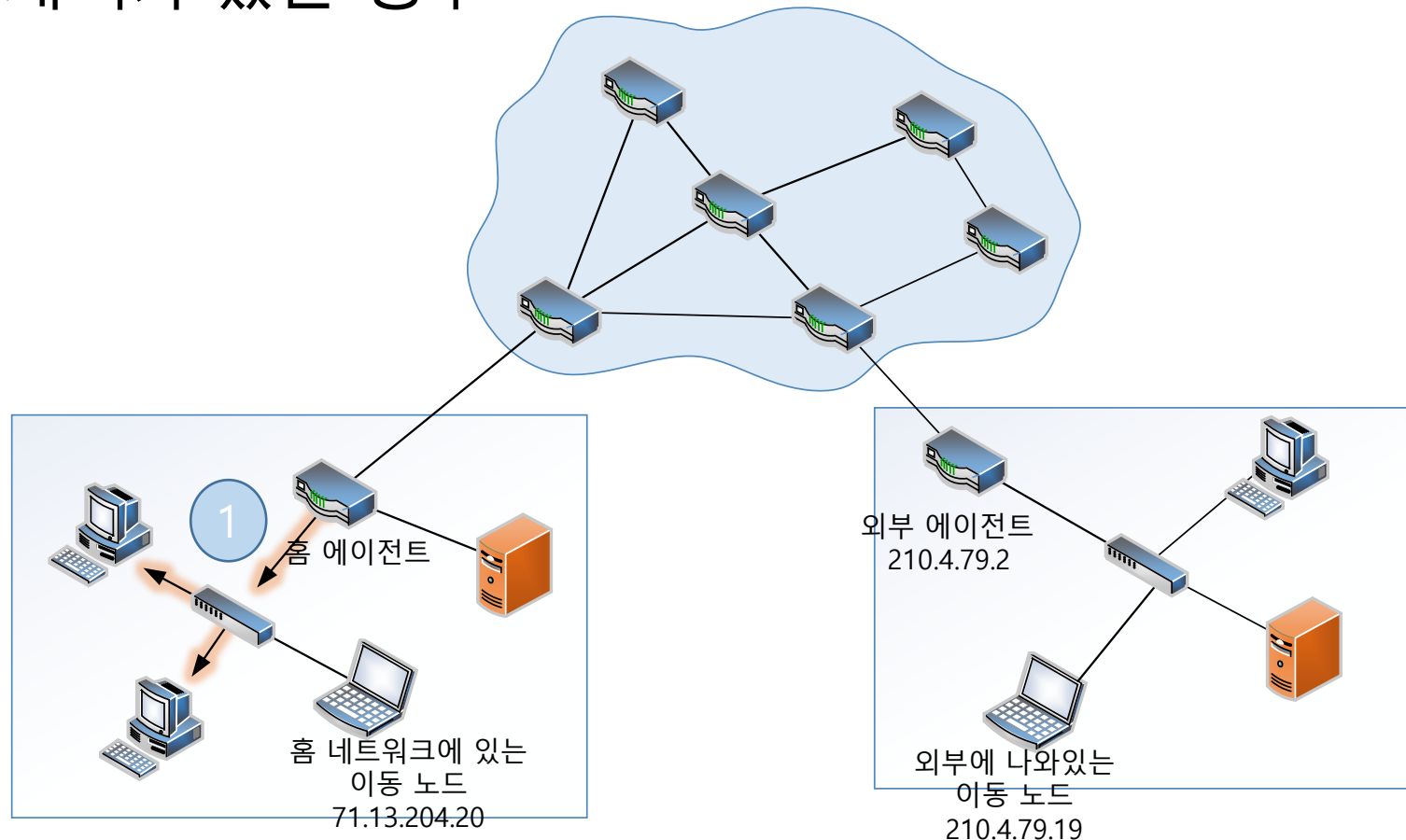
IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP와 TCP/IP 주소 결정 프로토콜
 - ARP 프록싱
 - 캐시가 없을 경우



IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP와 TCP/IP 주소 결정 프로토콜
 - 무상 ARP
 - 캐시가 있는 경우



IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 한계

- 비효율

- 노드와 이동 장비 간의 거리에 따라 비효율 정도가 달라짐
 - 전송자와 이동 장비가 같은 외부 네트워크에 있다면 가장 효율성이 떨어짐

- 보안 문제

- 전송 자체가 공개되어 있기 때문에 도청 가능
- 재생 공격 문제
- 등록 메시지 외의 메시지에 대한 인증의 부재
- 추가적인 인증과 기밀성을 위해 IPsec의 AH나 ESP를 사용

목 차

- 보충
 - IP Security(IPsec) 프로토콜
 - IP 이동성 지원(모바일 IP) 프로토콜
- 주요 라우팅 프로토콜 개념
- 라우팅 정보 프로토콜(RIP)
- 최단 경로 우선 프로토콜(OSPF)
- 경계 경로 프로토콜(BGP)
- 기타 라우팅 프로토콜

주요 라우팅 프로토콜 개념

- 라우팅 프로토콜 구조

- 자율 시스템 구조(AS, Autonomous System)

- 정의

- 인터넷을 각각 독립된 그룹 집합으로 나눈 구조
 - 특정 기관이나 관리 단체에서 통제하는 라우터와 네트워크 모음으로 구성
 - 아시아(APNIC), 북미(ARIN), 남미(LACNIC), 아프리카(AfriNIC) 등

- 프로토콜 유형

- 내부 라우팅 프로토콜

- AS 내부에서 라우팅 정보를 교환할 때 사용
e.g., RIP(Routing Information Protocol), OSPF(Open Shortest Path First)

- 외부 라우팅 프로토콜

- AS 간에 라우팅 정보를 교환할 때 사용
e.g., BGP(Border Gateway Protocol)

주요 라우팅 프로토콜 개념

- 라우팅 프로토콜 구조

- 자율 시스템 구조(AS)

- 라우터 종류

- 내부 라우터

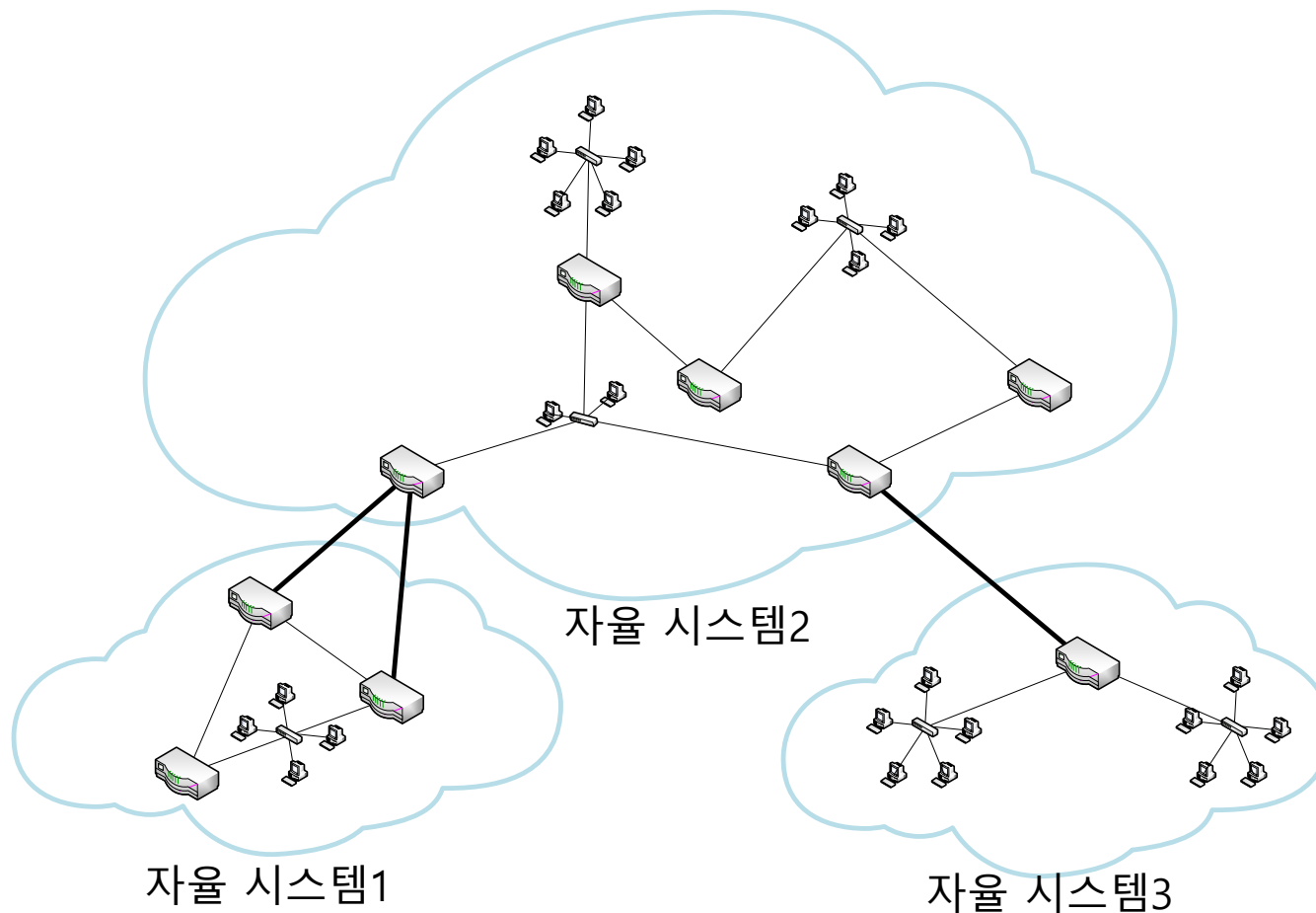
- 내부 라우터는 같은 AS에 있는 라우터에만 접속 가능

- 경계 라우터

- 경계 라우터는 같은 AS 내부에 있는 라우터 뿐 아니라 다른 AS에 있는 라우터와 통신 가능
 - 다른 AS와 트래픽을 공유하는 역할

주요 라우팅 프로토콜 개념

- 라우팅 프로토콜 구조
 - 자율 시스템 구조(AS)



주요 라우팅 프로토콜 개념

- 라우팅 프로토콜 알고리즘과 척도
 - 척도(metric)
 - 특정 경로의 효율을 측정할 때 나타내는 값(비용)
 - 알고리즘
 - 거리 벡터(벨만 포드) 라우팅 알고리즘
 - 두 네트워크 사이의 홉 수에 따른 경로 선택
e.g., RIP
 - 링크 상태(최단 경로 우선) 라우팅 알고리즘
 - 두 네트워크 간의 가장 짧은 경로를 동적으로 측정
e.g., OSPF
 - 혼합 라우팅 알고리즘
 - 위의 두 알고리즘을 혼합한 기능
e.g., BGP

목 차

- 보충
 - IP Security(IPsec) 프로토콜
 - IP 이동성 지원(모바일 IP) 프로토콜
- 주요 라우팅 프로토콜 개념
- 라우팅 정보 프로토콜(RIP)
- 최단 경로 우선 프로토콜(OSPF)
- 경계 경로 프로토콜(BGP)
- 기타 라우팅 프로토콜

라우팅 정보 프로토콜

- RIP

- 정의

- 네트워크 간의 거리 정보를 담은 항목을 라우팅 테이블에 저장하여 최적의 경로를 찾는 프로토콜
 - 거리는 출발지에서 목적지까지의 홉 수를 측정
 - 최대 15홉 까지 허용

- 특징

- 직관적이고 구현하기 쉬움
- 라우터 처리 시간이 짧음
- 작은 자율 시스템에서 사용하기 용이

라우팅 정보 프로토콜

- RIP

- 개요

- RIP-1

- 1988년, RFC 1058, “Routing Information Protocol”에 명시

- RIP-2

- 클래스 비사용 주소지정, 인증, 멀티캐스트 사용과 같은 기능 추가
 - 1998년, RFC 2453, “RIP version 2”에 명시

- RIPng

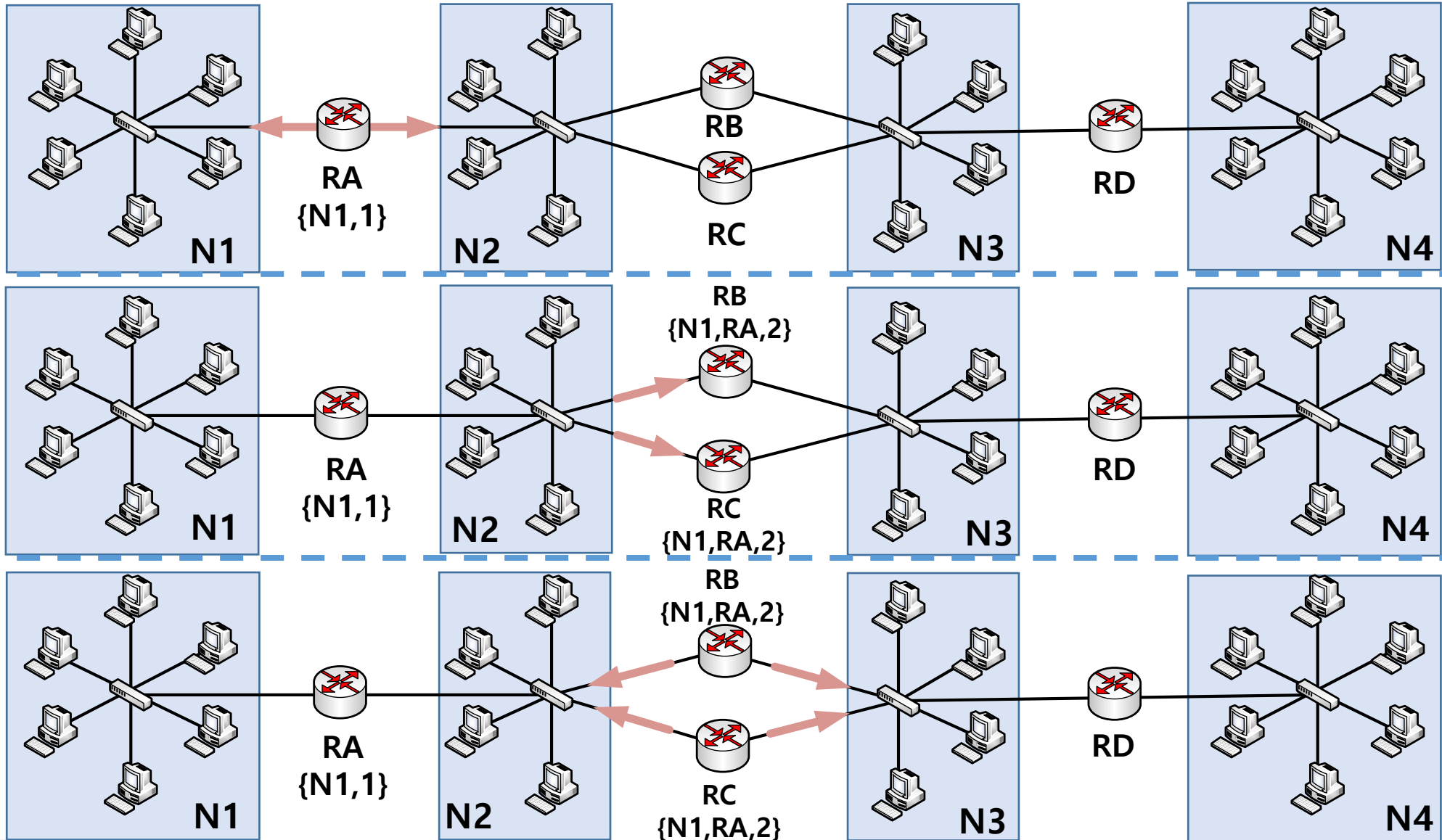
- RIP와 RIP-2에 기반을 둔 독립된 프로토콜
 - IPv6에서 동작하는 RIP

라우팅 정보 프로토콜

- RIP 경로 결정 알고리즘과 척도
 - 경로에 대한 정보를 서로 교환하여 라우팅 테이블을 최신으로 갱신
- 라우팅 테이블 저장 정보
 - 네트워크나 호스트의 주소
 - 라우터에서 네트워크나 호스트 까지의 거리
 - 데이터그램 전송 시 첫 번째로 지나는 라우터

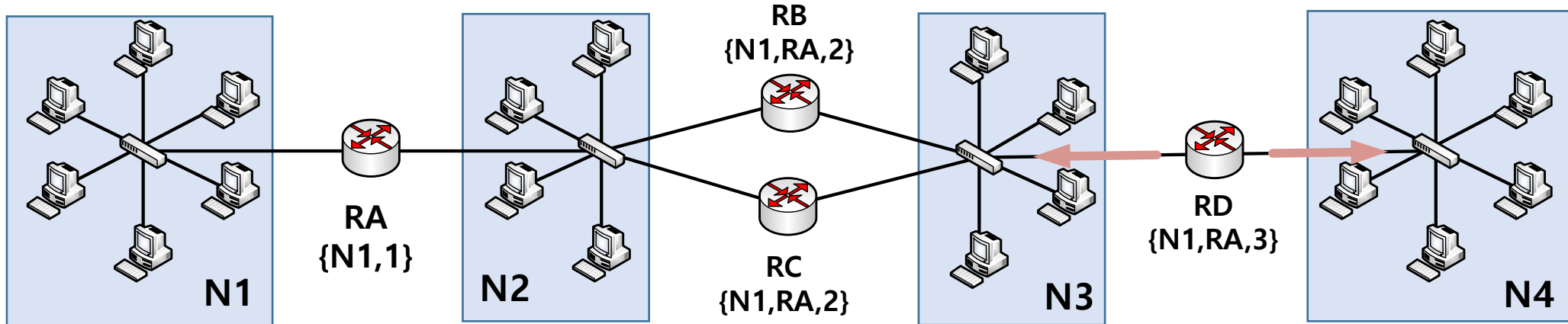
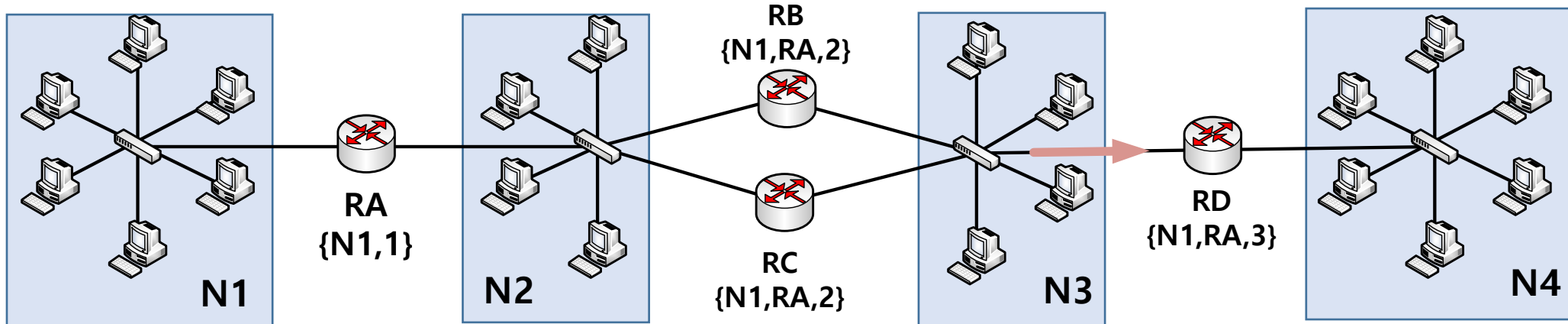
라우팅 정보 프로토콜

• RIP를 사용한 네트워크 정보 전파



라우팅 정보 프로토콜

- RIP를 사용한 네트워크 정보 전파



라우팅 정보 프로토콜

- RIP 일반 동작

- RIP 메시지와 기본 메시지 유형

- RIP-1, RIP-2는 UDP 520번 포트

- RIPng는 UDP 521번 포트

- RIP 메시지를 여러 장비에게 보낼 경우

- RIP-1은 브로드캐스트

- RIP-2, RIPng는 멀티캐스트

- 메시지 유형

- RIP 요청

- 한 라우터가 다른 라우터의 라우팅 테이블의 일부나 전체를 요청하는 메시지

- RIP 응답

- 라우팅 테이블의 일부나 전체를 전송하는 메시지

라우팅 정보 프로토콜

- RIP 일반 동작

- RIP 타이머

- 계층 타이머(30초)

- 최신 정보를 유지하기 위함

- 요청 받지 않아도 라우팅 테이블을 브로드캐스트/멀티 캐스트

- 만료 타이머(180초)

- 오래된 정보를 처리하기 위함

- RIP 응답 메시지를 받은 경우

- 경로가 존재한다고 생각하여 만료 타이머 초기화

- RIP 응답 메시지를 받지 않은 경우

- 타이머가 만료 되면 경로의 거리를 16으로 바꾸어 곧 지울 것이라고 표시

라우팅 정보 프로토콜

- RIP 일반 동작

- RIP 타이머

- 가비지 콜렉션 타이머(120초)

- 유효하지 않은 경로를 지울 때 까지 유예기간을 둠
 - 홉 수를 16으로 하여 경로에 문제가 있다는 것을 주변 라우터에게 알림
 - 만료되면 경로 삭제
 - 가비지 콜렉션 기간 동안 경로에 대한 새 응답이 오면 삭제 중단

라우팅 정보 프로토콜

- RIP 문제점과 해결책

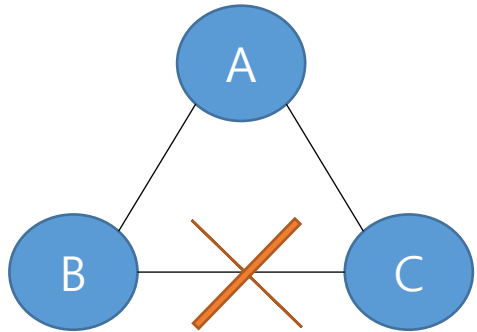
- 알고리즘과 관련된 문제

- 느린 수렴

- 모든 라우터가 같은 정보를 갖게 될 때 까지 걸리는 시간이 오래 걸림

- 라우팅 루프

- 데이터그램이 목적지를 찾지 못하고 끊임없이 순환하는 현상

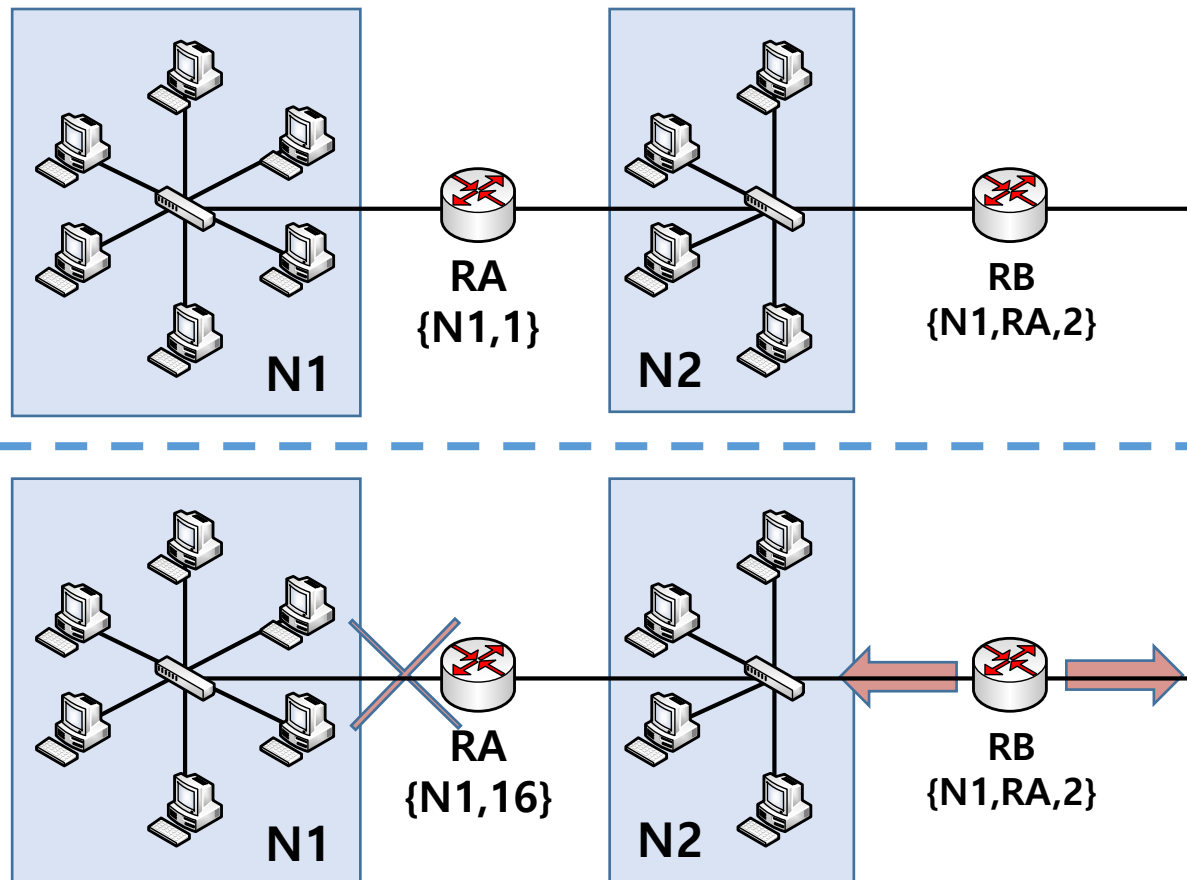


- 무한 세기

- 느린 수렴 시간으로 인해 라우터가 잘못된 경로를 라우터 사이에서 계속 주고 받는 현상

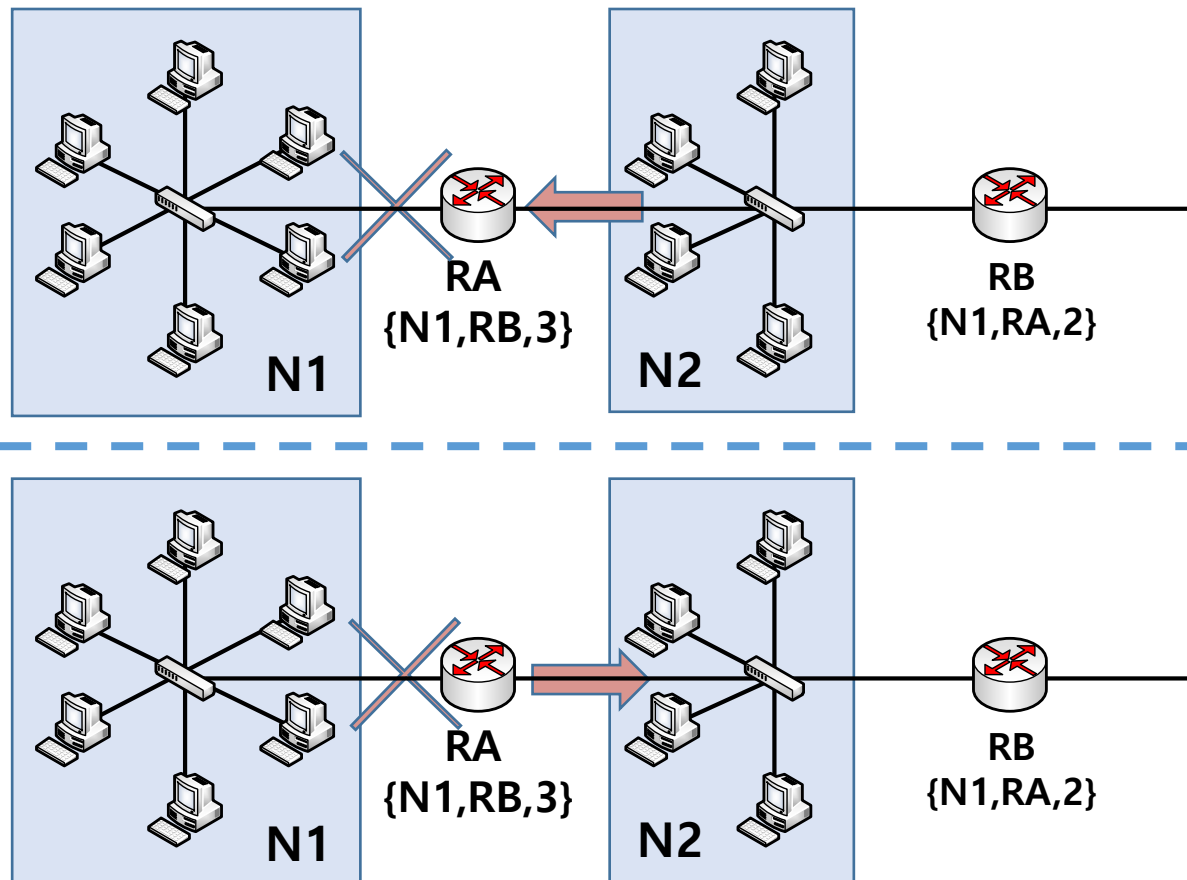
라우팅 정보 프로토콜

- RIP 문제점과 해결책
 - 알고리즘과 관련된 문제
 - 무한 세기



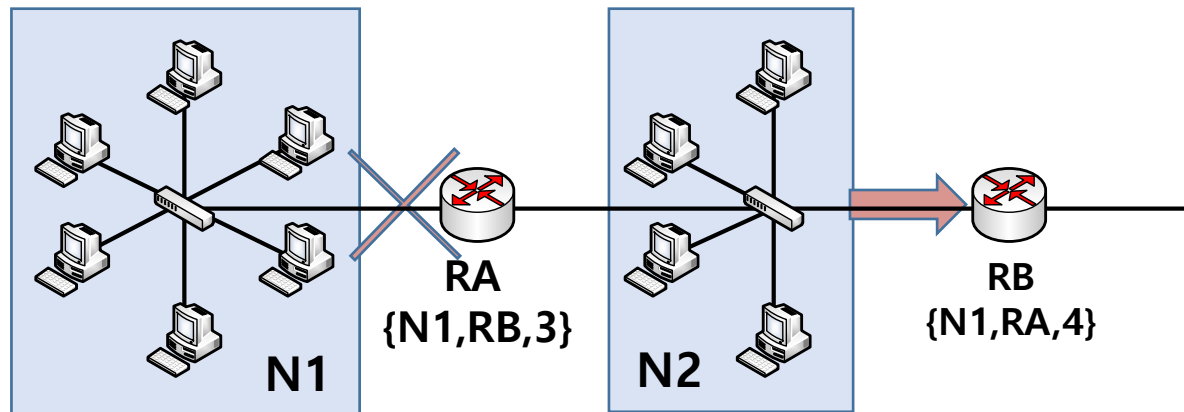
라우팅 정보 프로토콜

- RIP 문제점과 해결책
 - 알고리즘과 관련된 문제
 - 무한 세기



라우팅 정보 프로토콜

- RIP 문제점과 해결책
 - 알고리즘과 관련된 문제
 - 무한 세기



라우팅 정보 프로토콜

- RIP 문제점과 해결책
 - 알고리즘과 관련된 문제
 - 작은 무한값
 - 느린 수렴 문제를 줄이기 위해 무한값으로 작은 값을 사용
 - 크기를 원하는 대로 확장할 수 없음
- RIP의 척도 문제
 - 거리 척도로 홑 수 사용
 - 두 네트워크 간의 비용을 제대로 반영하지 못함
 - 동적인 척도 제공 불가
 - 실시간 데이터를 바탕으로 최적의 경로 계산 불가

라우팅 정보 프로토콜

- RIP 문제점과 해결책

- 해결책

- 수평 분할

- 응답 메시지를 보낼 때, 이전에 받았던 경로로는 보내지 않음
 - 무한 세기 문제 해결

- 포이즈ن 리버스 수평 분할

- 수평 분할처럼 전송하지 않는 것이 아니라 척도를 무한값이나 16으로 설정하는 것 의미
 - 무한 세기 문제 해결

라우팅 정보 프로토콜

- RIP 문제점과 해결책

- 해결책

- 트리거 갱신

- 라우터가 경로에 대한 척도를 바꾸게 되면 즉시 응답 메시지를 보내 인접 라우터에게 알림
 - 느린 수렴 문제 해결

- 홀드 다운

- 네트워크 접근이 불가능하다는 메시지를 받은 경우
 - 타이머(60초, 120초) 시작
 - 만료될 때 까지 메시지 받지 않음
 - 타이머가 만료되면 정보 갱신
 - 경로에 대한 정보를 받은 후 일정 시간 동안 경로의 상태를 지속해야 함
 - 상당한 지연 시간 필요

라우팅 정보 프로토콜

• RIP 버전별 메시지 포맷과 특성

• RIP-1

- 다양한 프로토콜로 이루어진 네트워크에서 사용될 수 있도록 예약된 필드가 많음

명령 유형	버전=1	0
주소 유형 식별자=2		예약
경로와 척도	IP 주소	
	예약	
	예약	
	척도	
	RIP 항목 2	
...		
RIP 항목 N		

하위 필드명	크기	설명
주소 유형 식별자	2	주소의 유형 식별
0	2	예약된 필드
IP 주소	4	라우터가 정보를 전달하는 경로의 주소
0	4	예약된 필드
0	4	예약된 필드
척도	4	IP 주소 필드가 지정하는 네트워크까지의 홑 수

라우팅 정보 프로토콜

- RIP 버전별 메시지 포맷과 특성

- 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
 - MD5를 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 버전별 메시지 포맷과 특성
- RIP-2

명령 유형	버전=2	0
↑ 주소 유형 식별자=2	예약	
RTE1 ↓	IP 주소	
	서브넷 마스크	
	다음 홉	
	척도	
라우팅 테이블 항목(RTE) 2		
...		
라우팅 테이블 항목(RTE) N		

목 차

- 보충
 - IP Security(IPsec) 프로토콜
 - IP 이동성 지원(모바일 IP) 프로토콜
- 주요 라우팅 프로토콜 개념
- 라우팅 정보 프로토콜(RIP)
- 최단 경로 우선 프로토콜(OSPF)
- 경계 경로 프로토콜(BGP)
- 기타 라우팅 프로토콜

최단 경로 우선 프로토콜

- 최단 경로 우선 프로토콜(OSPF)

- 정의

- 라우터들끼리 동적으로 최적의 경로를 결정하는 프로토콜

- 동작

- 링크 상태 데이터베이스(LSDB, Link-State Database)

- OSPF에서 가장 기본적인 데이터 구조
 - 최단 경로 트리 형성
 - 루트 라우터와 다른 네트워크 사이의 관계(비용)를 보여줌

- 링크 상태 광고(LSA, Link-State Advertisement)

- 각 라우터가 AS의 상태에 대해서 알고 있는 것을 다른 라우터에게 전해줄 때 사용하는 메시지

최단 경로 우선 프로토콜

- 최단 경로 우선 프로토콜(OSPF)

- 특징

- 큰 기관에 적합
- 보안을 위한 인증 지원
 - MD5를 이용한 인증
 - 클래스 단위 주소지정, 서브넷 클래스 단위 주소지정, 클래스 비사용 주소지정 지원
- AS가 클 경우 계층 토폴로지를 만들어 사용
 - LSA 트래픽 감소
 - 토폴로지
 - 컴퓨터 네트워크의 요소들을 물리적, 논리적인 연결 상태로 나타낸 것

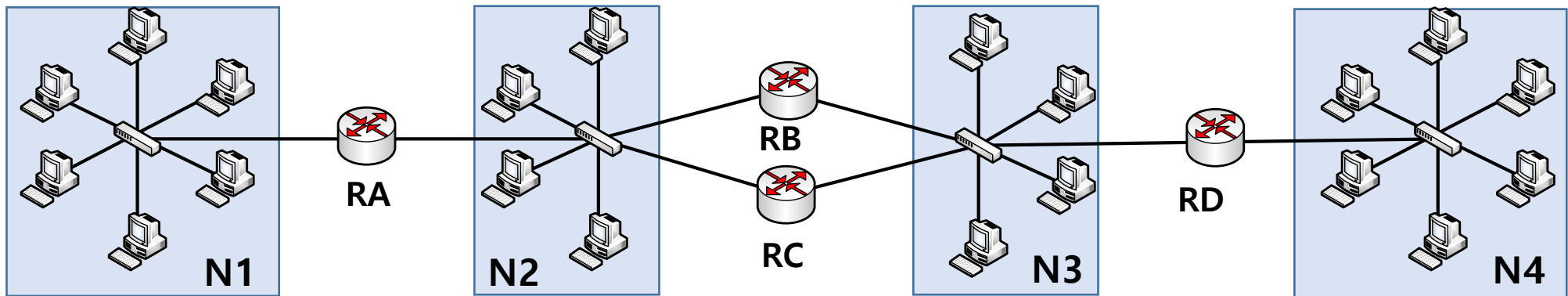
- 단점

- 높은 비용
- 복잡성

최단 경로 우선 프로토콜

- 기본 토폴로지

- AS 내에 있는 모든 라우터는 동등
 - 라우터는 서로 정보를 주고받고, LSDB를 관리
 - 모든 라우터가 동일한 LSDB를 소유



최단 경로 우선 프로토콜

• LSDB 예시

- ‘.’과 ‘0’은 라우터와 네트워크 또는 라우터가 연결됨을 의미
 - ‘.’은 패킷을 보내기 위한 비용
 - ‘0’은 패킷의 비용이 이중으로 계산되지 않도록 하기 위함

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

- 라우터 수가 증가하면 LSDB를 갱신하기 위한 메시지 양 증가에 따라 성능 저하 심각
 - AS 내 모든 라우터와 네트워크에 관한 LSDB를 모든 라우터가 관리해야 하기 때문
- 계층 토폴로지를 사용하는 AS에서 라우터는 동등하지 않음
 - 낮은 계층
 - 영역 내의 연결
 - 높은 계층(백본, 0)
 - 영역을 연결하는 계층

최단 경로 우선 프로토콜

- OSPF 계층 토폴로지

- 라우터 역할

- 내부 라우터

- 한 영역 내에 있는 라우터에만 연결
 - 한 영역에 대한 LSDB만을 가짐

- 영역 경계 라우터

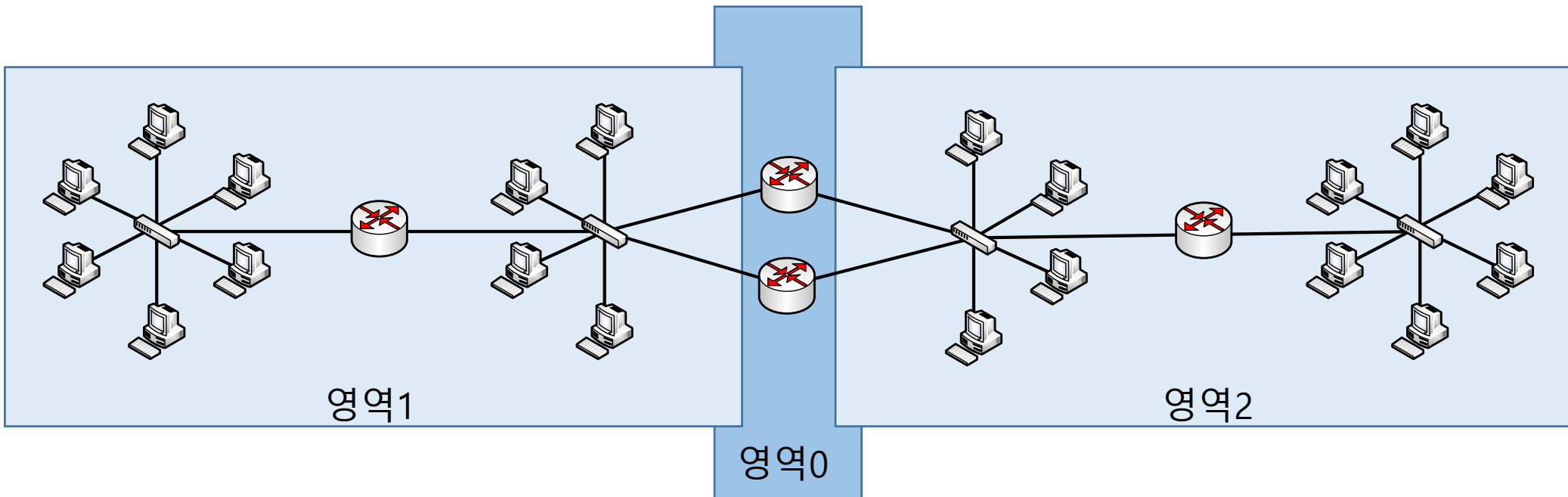
- 하나 이상의 영역에 연결된 라우터
 - 자신이 속한 각 영역에 대한 LSDB를 관리하며 백본에도 참여

- 백본 라우터

- 모든 영역의 경계 라우터를 포함
 - 영역 간에 라우팅 정보 전달

최단 경로 우선 프로토콜

- OSPF 계층 토폴로지



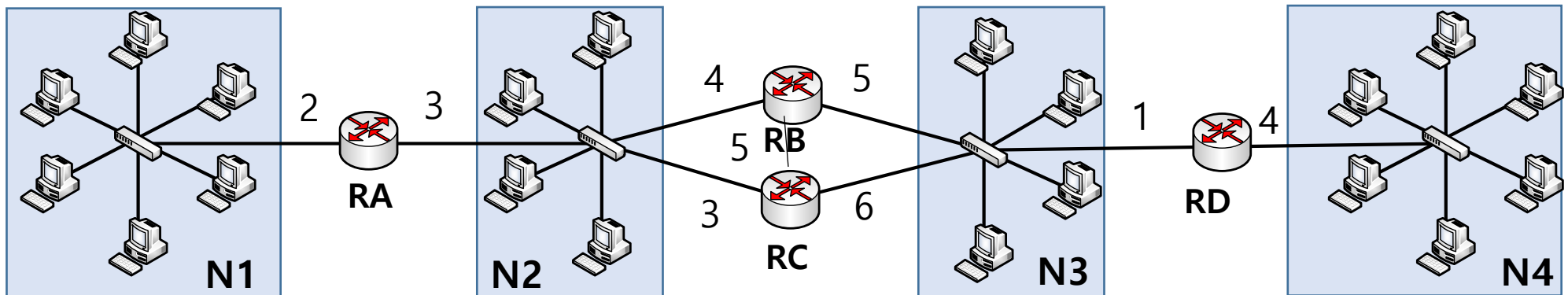
최단 경로 우선 프로토콜

- SPF 트리를 사용한 경로 설정
- SPF(Shortest Path First) 트리
 - AS 또는 영역 내의 라우터나 네트워크로 가기 위한 최단 경로를 결정하는 트리 생성
 - 경로가 여러 개라도 트리는 가장 짧은 경로만 보여줌
 - 네트워크로 가는 비용과 접근할 다음 홉 명시
- LSDB의 현재 상태에 따라 동적으로 계산

최단 경로 우선 프로토콜

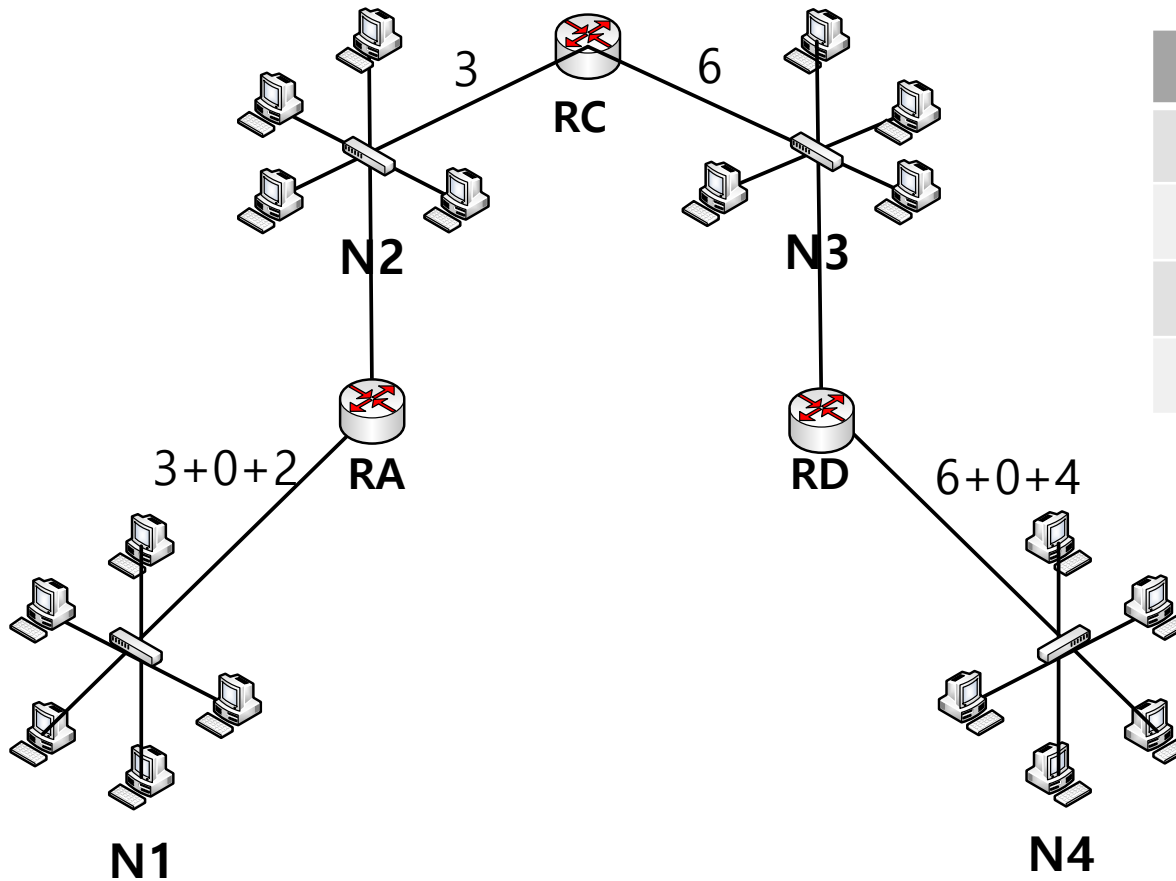
- SPF 트리를 사용한 경로 설정

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

- SPF 트리를 사용한 경로 설정



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

최단 경로 우선 프로토콜

- OSPF 일반 동작

- OSPF 메시지는 직접 IP 데이터그램을 만들어 전송
 - 프로토콜 ID: 89

- 메시지 유형

- Hello 메시지

- 이웃 라우터를 발견하고 주변 장비와 링크를 맺음
 - OSPF를 사용하는 방식과 관련된 인자를 주고받음

- 데이터베이스 설명 메시지

- AS나 영역의 토폴로지에 대한 설명을 실는 메시지
 - AS나 영역에 대한 LSDB를 다른 라우터에게 전달할 때 데이터베이스 설명 메시지 사용

최단 경로 우선 프로토콜

- OSPF 일반 동작

- 메시지 유형

- 링크 상태 요청

- 다른 라우터에게 LSDB 일부에 대한 갱신 정보를 요청할 때 사용

- 링크 상태 갱신

- LSDB에 있는 특정 링크에 대한 상태를 알릴 때 사용
 - 링크 상태 요청 메시지에 대한 응답으로 송신
 - 정기적으로 라우터에 의해 브로드캐스트/멀티캐스트

- 링크 상태 승인 메시지

- 링크 상태 갱신 메시지를 받았다고 승인 메시지를 보냄으로써 안정적으로 링크 상태 교환

최단 경로 우선 프로토콜

- OSPF 일반 동작

- 메시지 교환 과정

1. 라우터가 동작이 시작되면 Hello 메시지를 보내 주변에 OSPF를 실행하는 라우터가 있는지 확인
2. 새 라우터를 발견하면 데이터베이스 설명 메시지를 보내 새로 생긴 라우터의 LSDB 초기화
3. 주기적으로 로컬 네트워크에 링크 상태 갱신 메시지를 보냄
4. 링크 상태 갱신 메시지를 받으면 그에 해당하는 링크 상태 승인 메시지를 보냄

최단 경로 우선 프로토콜

• OSPF 메시지 공통 포맷

버전=2	유형	패킷 길이
라우터 ID		
영역 ID		
체크섬	인증 유형	
인증		
메시지 본문		

필드명	크기	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

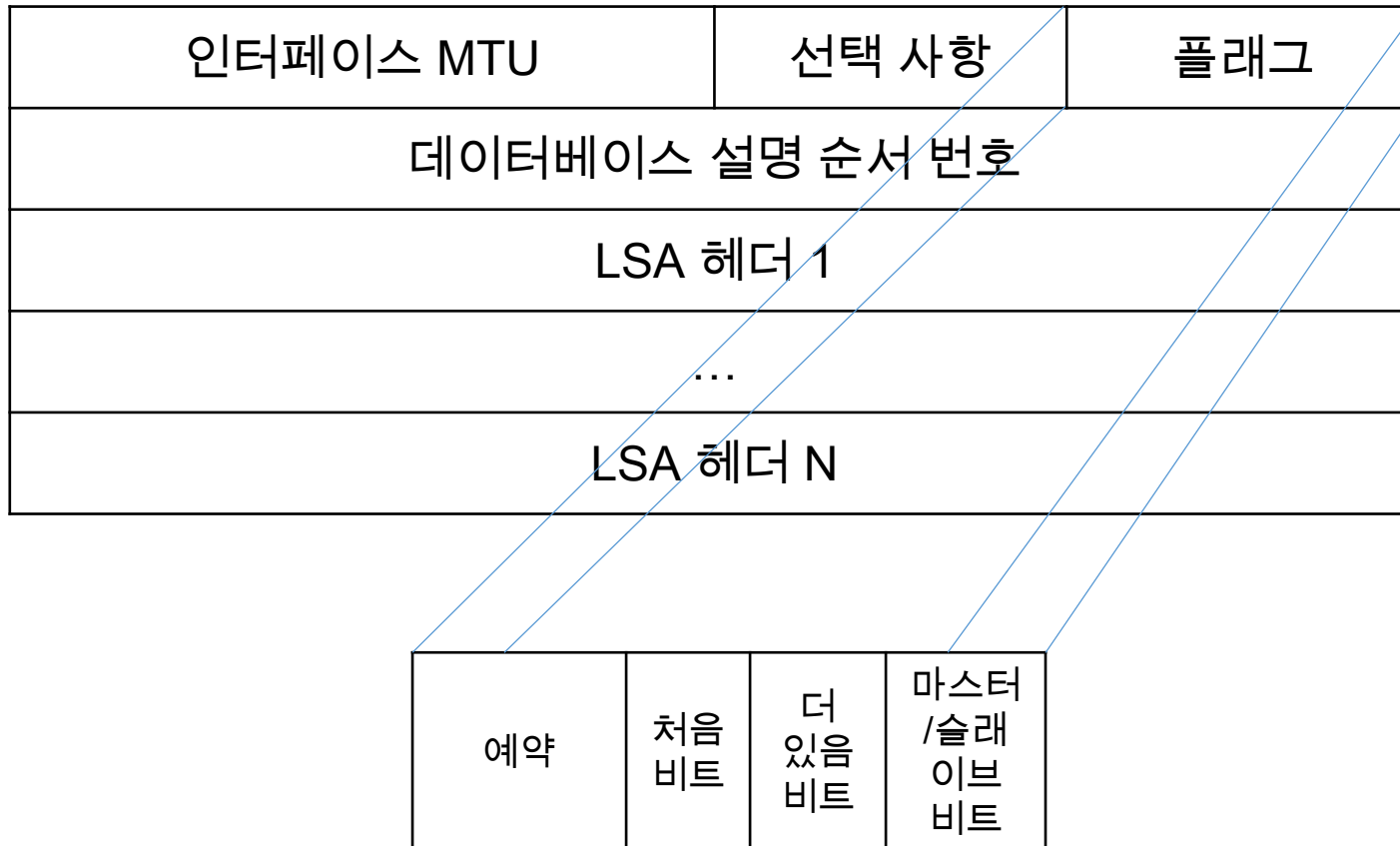
• Hello 메시지 포맷

네트워크 마스크		
전송간격	선택사항	라우터 우선순위
라우터 장애 간주 간격		
지정 라우터		
백업 지정 라우터		
주변 라우터1		
...		
주변 라우터 N		

필드명	크기	설명
네트워크 마스크	4	메시지를 보내고 있는 네트워크의 서브넷 마스크
전송 간격	2	Hello 메시지를 받기 원하는 간격
선택 사항	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
백업 지정 라우터	4	백업 지정 라우터의 주소
주변 라우터	4의 배수	라우터가 최근 받은 Hello 메시지를 보낸 주소

최단 경로 우선 프로토콜

- 데이터베이스 설명 메시지 포맷



최단 경로 우선 프로토콜

• 데이터베이스 설명 메시지 포맷

필드명	크기	설명
인터페이스 MTU	2	라우터의 인터페이스로 단편화하지 않고 보낼 수 있는 IP 메시지 크기
선택사항	1	라우터가 지원하는 OSPF 선택사항 기능을 알림
플래그	1	데이터베이스 설명 메시지 교환에 대한 정보를 알리는데 사용하는 플래그
데이터베이스 설명 순서 번호	4	데이터베이스 설명 메시지를 순서대로 정렬할 수 있도록 순서 번호 사용
LSA 헤더	가변	LSDB에 대한 정보를 전달하는 LSA 헤더 포함

• 데이터베이스 설명 메시지 플래그

필드명	크기	설명
예약	5/8	예약된 필드, 모든 값은 0
처음	1/8	데이터베이스 설명 메시지를 처음 보낸 경우 1
더 있음	1/8	데이터베이스 설명 메시지가 더 있다면 1
마스터/슬레이브	1/8	메시지를 보내는 라우터가 마스터면 1, 슬레이브면 0

최단 경로 우선 프로토콜

• 데이터베이스 설명 메시지 포맷

필드명	크기	설명
인터페이스 MTU	2	라우터의 인터페이스로 단편화하지 않고 보낼 수 있는 IP 메시지 크기
선택사항	1	라우터가 지원하는 OSPF 선택사항 기능을 알림
플래그	1	데이터베이스 설명 메시지 교환에 대한 정보를 알리는데 사용하는 플래그
데이터베이스 설명 순서 번호	4	데이터베이스 설명 메시지를 순서대로 정렬할 수 있도록 순서 번호 사용
LSA 헤더	가변	LSDB에 대한 정보를 전달하는 LSA 헤더 포함

• 데이터베이스 설명 메시지 플래그

필드명	크기	설명
예약	5/8	예약된 필드, 모든 값은 0
처음	1/8	데이터베이스 설명 메시지를 처음 보낸 경우 1
더 있음	1/8	데이터베이스 설명 메시지가 더 있다면 1
마스터/슬레이브	1/8	메시지를 보내는 라우터가 마스터면 1, 슬레이브면 0

최단 경로 우선 프로토콜

• 링크 상태 요청 메시지 포맷

↑ ↓ LSA 요청 번호 ↓ ↑	LS 유형
	링크 상태 ID
	광고 라우터
	LS 유형/링크 상태ID/광고 라우터 2
	...
	LS 유형/링크 상태ID/광고 라우터 N

필드명	크기	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

- 링크 상태 갱신 메시지 포맷

LSA 수
LAS 1
...
LSA N

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

최단 경로 우선 프로토콜

- 링크 상태 승인 메시지 포맷

LSA 헤더 1
...
LSA 헤더 N

필드명	크기	설명
LSA 헤더	가변	승인할 LSA를 식별하기 위한 LSA 헤더 필드

최단 경로 우선 프로토콜

• 링크 상태 승인 메시지 포맷

LS 나이	선택 사항	선택 사항
링크 상태 ID		
광고 라우터		
LS 순서 번호		
LS 체크섬	길이	

필드명	크기	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

목 차

- 보충
 - IP Security(IPsec) 프로토콜
 - IP 이동성 지원(모바일 IP) 프로토콜
- 주요 라우팅 프로토콜 개념
- 라우팅 정보 프로토콜(RIP)
- 최단 경로 우선 프로토콜(OSPF)
- 경계 경로 프로토콜(BGP)
- 기타 라우팅 프로토콜

경계 경로 프로토콜

- BGP

- 개요

- 커져가는 인터넷에 맞는 외부 라우팅 프로토콜의 필요성 부각
- 클래스 비사용 주소지정과 같은 변화에 맞는 수정
- 버전과 표준

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 Protocol3	BGP-3	메시지 식별 기능을 추가하여 경로 정보 교환을 최적화
1771	1995	A Border Gateway Protocol4	BGP-4	클래스 비사용 도메인 간 라우팅 지원 추가

경계 경로 프로토콜

- 기능과 특성

- AS간에 네트워크 접근 가능 정보를 교환하고 그 정보를 통해 네트워크로 가는 경로를 결정
- 각 AS는 BGP를 실행하는 라우터가 하나 이상 존재
- 경로 벡터 프로토콜
 - 네트워크에 관한 정보와 경로를 저장
 - BGP 라우터끼리 정보를 교환하여 인터넷워크에 전파
 - 라우팅 정보 기반(RIB, Routing Information Bases)
- TCP를 사용하여 메시지 제어

경계 경로 프로토콜

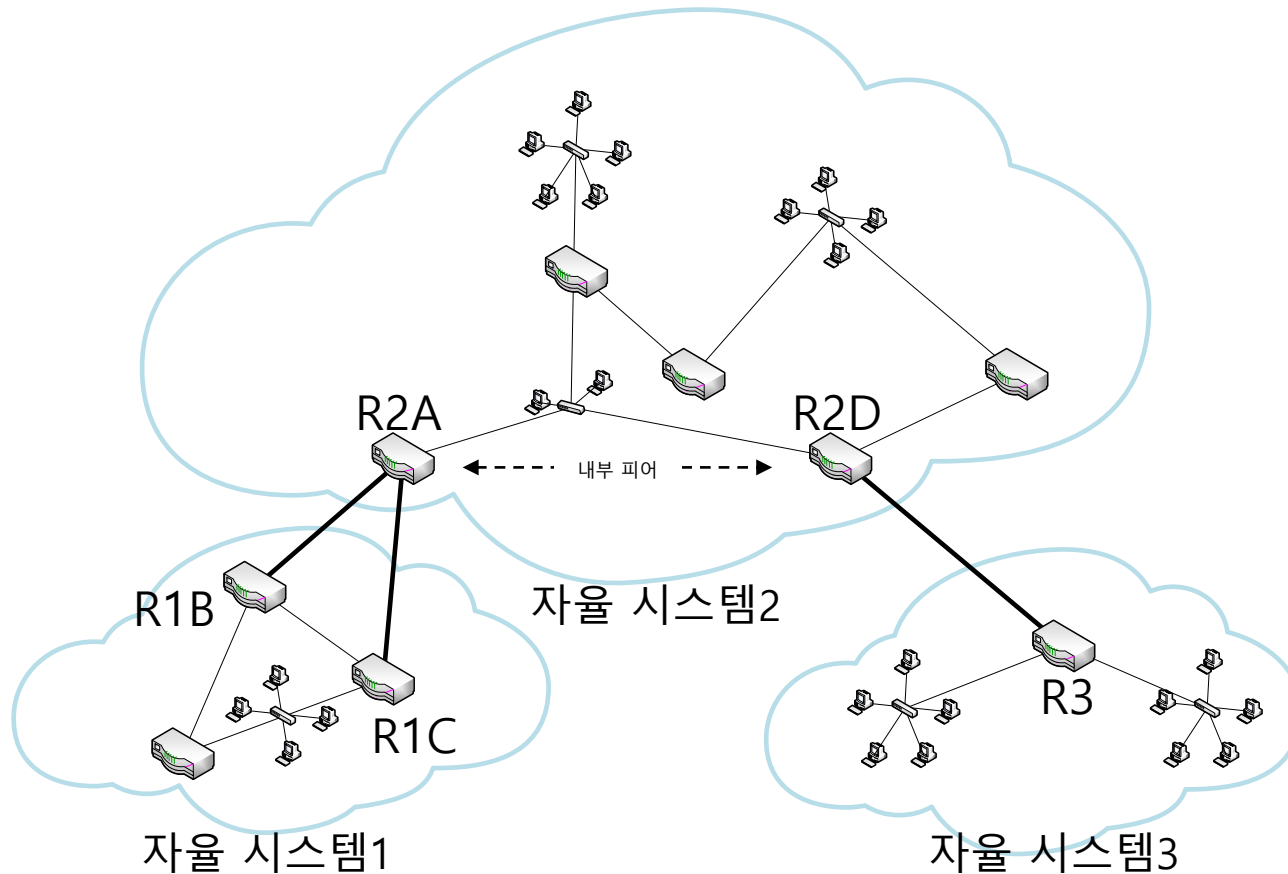
- 토폴로지
 - BGP의 유연성
 - AS의 인터넷워크가 어떤 토폴로지를 가지든 BGP 사용 가능
 - BGP는 AS 내부에서 일어나는 일에 대해서 모름
 - AS는 자신만의 내부 토폴로지를 가지고 자신만의 라우팅 프로토콜을 사용

경계 경로 프로토콜

- 토폴로지
- 구성 요소
 - 스피커
 - BGP용어로 통신하는 노드
 - 피어
 - 내부 피어(internal peer)
 - 같은 AS에 있는 주변 노드
 - 외부 피어(external peer)
 - 다른 AS에 있는 주변 노드

경계 경로 프로토콜

- 토폴로지
- 구성 요소

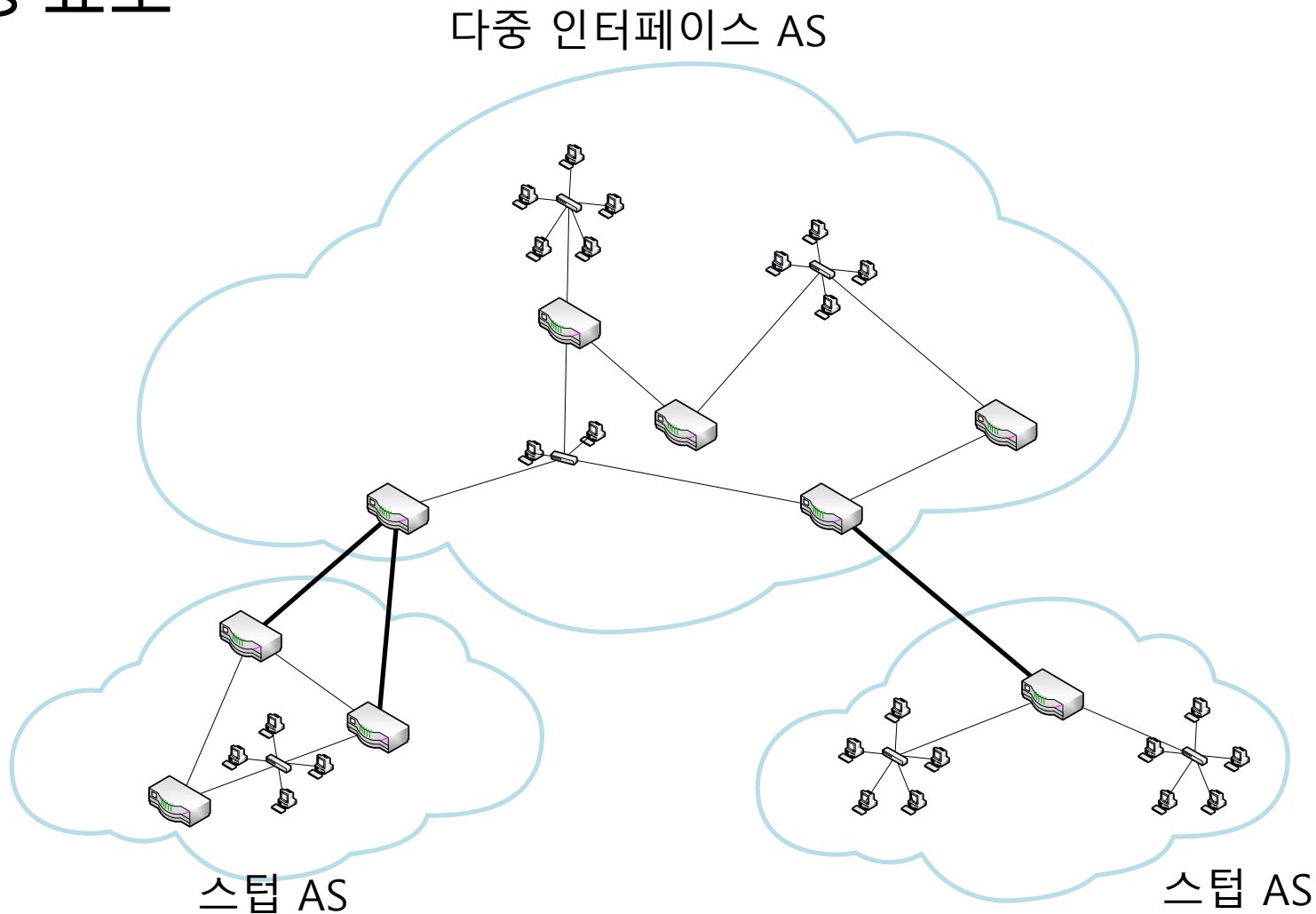


경계 경로 프로토콜

- 토폴로지
 - 트래픽 흐름 제어
 - 트래픽
 - 인터넷워크에 존재하는 메시지 흐름
 - 지역 트래픽
 - 같은 AS에서 발생하거나 AS로 전송되어야 하는 트래픽
 - 횡단 트래픽
 - 다른 AS로 전송되어야 하는 트래픽
 - AS 유형
 - 스텝 AS
 - 네트워크의 마지막에 있는 AS
 - 스텝 AS에서 출발하여 돌아오는 트래픽이 대부분
 - 다중 인터페이스 AS
 - 두 개 이상의 AS에 연결된 AS

경계 경로 프로토콜

- 토폴로지
- 구성 요소



경계 경로 프로토콜

- 토폴로지

- 라우팅 정책

- 횡단 트래픽을 처리하는 방식

- 횡단 금지 정책

- 횡단 트래픽을 전혀 처리하지 않음

- 제한된 AS 횡단 정책

- 특정 AS에서 오는 트래픽은 처리하지만 다른 AS에서 오는 트래픽은 받지 않음

- 기준 기반 횡단 정책

- 기준을 두고 횡단 트래픽을 허용할지 허용하지 않을지 결정

경계 경로 프로토콜

- 경로 저장과 광고
- 경로 정보 관리 기능
 - 경로 저장
 - 데이터베이스에 네트워크에 도달하는 방법 저장
 - 경로 갱신
 - 피어에서 갱신 메시지를 받은 후 갱신 메시지를 어떻게 사용할지 처리
 - 경로 선택
 - 경로 데이터베이스에 있는 정보를 사용하여 인터넷워크에 있는 네트워크로 가는 최적의 경로를 찾음
 - 경로 광고
 - BGP 스피커는 피어에게 경로 광고를 통해 네트워크에 대해서 알고 있는 정보와 도착 방법을 정기적으로 알림

경계 경로 프로토콜

- 경로 저장과 광고
- 라우팅 정보 기반(RIB) 데이터베이스
 - Adj-RIBs-In
 - 피어 BGP 스피커에서 받은 경로 정보를 보관하는 입력 데이터베이스 부분
 - Loc-RIB
 - BGP 장비가 유효하다고 판단하여 선택한 경로 정보를 저장하는 중요 데이터베이스
 - Adj-RIBs-Out
 - 정기적으로 Loc-RIB에 있는 정보를 알리기 위해 사용하는 데이터베이스

경계 경로 프로토콜

- 경로 판단과 결정 과정

- 입력 정보를 분석하여 경로 갱신, 선택, 광고 기능 수행
- 로컬 데이터베이스에 포함시킬 정보를 선별하고 DB 갱신 후 다른 피어 장비에게 전송할 경로 선택
- 1단계
 - 주변 AS에 있는 스피커가 보낸 경로를 분석하여 우선순위 할당
- 2단계
 - 우선순위에 따라 가장 좋은 경로를 선택하여 로컬 라우팅 정보 기반(Loc-RIB) 갱신
- 3단계
 - 스피커는 Loc-RIB에 있는 경로를 선택하여 다른 AS에 있는 주변 노드 스피커에게 전송

경계 경로 프로토콜

- 경로 판단과 결정 과정
 - 우선 순위를 할당하는 법칙
 - 라우터와 목적지 네트워크까지 가는 동안 거쳐야 하는 AS의 수
 - 경로를 사용할 수 없게 하는 특정 정책의 존재 여부
- 경로 선택 능력의 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

- 일반 동작

1. 스피커 지정과 연결 수립

- BGP 피어와 TCP 연결을 수립
- 각 라우터는 자신의 AS를 알리고 생성 메시지 전송

2. 경로 정보 교환

- BGP 피어 사이에 링크가 수립되면 전체 네트워크 정보와 라우팅 테이블 교환
- 갱신 메시지 교환
 - 변경된 경로에 대한 정보만 교환하기 때문에 대역폭을 최소한으로 줄일 수 있음

경계 경로 프로토콜

- 일반 동작

- 3. 연결 유지

- 스피커는 서로 연결되어 있다는 것을 확인하기 위해 주기적으로 킵 얼라이브 메시지 교환

- 4. 에러 보고

- BGP 통지 메시지
 - 피어에게 문제가 발생했다고 에러가 일어난 이유를 리포팅한다.
 - 통지 메시지를 보낸 장비는 둘 간의 연결 종료
 - 다시 협상하여 연결

경계 경로 프로토콜

- 일반 메시지 포맷

마커 (128비트)	
길이	유형
메시지 본문	

필드명	크기	설명
마커	16	메시지의 시작을 식별, 인증하기 위해 사용
길이	2	메시지의 총 길이
유형	1	BGP 메시지 유형
메시지 본문/ 데이터 부분	가변	생성, 갱신, 통지 메시지 유형을 구현하 기 위한 구체적인 필드

경계 경로 프로토콜

• 생성 메시지 포맷

마커 (128비트)		
길이	유형=1	버전
자율 시스템(AS)	홀드 시간	
BGP 식별자		
옵션 사항 파라미터 길이	파라미터 유형 1	파라미터 길이 1
파라미터 값 1		
...		
파라미터 유형 N	파라미터 길이 1	
파라미터 값 N		

필드값	크기	설명
마커	16	메시지의 시작을 식별, 인증하기 위해 사용
길이	2	메시지의 총 길이
유형	1	BGP 메시지 유형
버전	1	BGP 버전
자율 시스템	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

- 생성 메시지 포맷
 - 선택 사항 파라미터 구성

하위 필드 명	크기	설명
파라미터 유형	1	현재 인증 정보를 위한 단 하나의 선택 사항을 정의
파라미터 길이	1	파라미터 값 하위 필드의 길이를 명시
파라미터 값	가변	전달하려는 파라미터의 값

경계 경로 프로토콜

• 갱신 메시지 포맷

속성 플래그					속성 유형 코드
옵션 비트	형단 비트	부분 비트	연장 길이 비트	예약	

마커 (128비트)			
길이		유형=2	사용할 수 없는 경로 길이
사용할 수 없는 경로 길이	취소 경로 길 이 1	취소 경로 1점두사	
...			
취소 경로 길 이 N	취소 경로 N 점두사		
총 경로 속성값 길이		속성 유형1	
속성 길이1	속성 값 1		
...			
속성 유형 N		속성 길이 N	
속성 값 N			
NLRI 1 길이	네트워크 도착 기능 정보 1 점두사		
...			
NLRI N 길이	네트워크 도착 기능 정보 N 점두사		

경계 경로 프로토콜

• 갱신 메시지 포맷

하위 필드 명	크기	설명
속성 유형	4	속성의 유형을 정의
속성 길이	1 or 2	속성의 길이
속성 값	가변	경로 속성의 유형에 따라 달라짐

하위 하위 필드 명	크기	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
5	로컬 선호도
6	집선
7	집선 장비

경계 경로 프로토콜

- 킵 얼라이브 메시지 포맷

마커 (128비트)	
길이 = 19	유형 = 4

필드 명	크기	설명
마커	16	메시지의 시작을 식별, 인증하기 위해 사용
길이	2	메시지의 총 길이
유형	1	BGP 메시지의 유형

경계 경로 프로토콜

• 통지 메시지 포맷

마커 (128비트)		
길이	유형=3	오류 코드
오류 하위 코드	데이터	

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 메시지 를 받지 못함
5	유한 상태 머신 에러	한 동작 상태에서 다른 동작 상태 로 움직이는 방식
6	종료	다른 오류 코드로 설명하는 에러 상황과는 관계 없이 접속을 끝내고 싶을 때 사용

목 차

- 보충
 - IP Security(IPsec) 프로토콜
 - IP 이동성 지원(모바일 IP) 프로토콜
- 주요 라우팅 프로토콜 개념
- 라우팅 정보 프로토콜(RIP)
- 최단 경로 우선 프로토콜(OSPF)
- 경계 경로 프로토콜(BGP)
- 기타 라우팅 프로토콜

기타 라우팅 프로토콜

- 게이트웨이 게이트웨이 프로토콜(GGP, Gateway-Gateway Protocol)
 - 적은 수의 핵심 라우터만 있던 초기 인터넷에 사용된 프로토콜
 - 거리 기반 벡터 알고리즘
 - 가장 적은 홉 수로 최적의 경로 결정
 - RIP와 동일한 문제점
 - 클래스 단위 네트워크에서만 사용 가능
 - AS를 사용하는 방식으로 인터넷 구조가 바뀌어 가면서 사용되지 않음

기타 라우팅 프로토콜

- 외부 게이트웨이 프로토콜(EGP, Exterior Gateway Protocol)
- 초기 인터넷 시절 비핵심 라우터들이 네트워크 도착 가능 정보를 교환하기 위해 사용한 프로토콜
- BGP로 대체됨
 - 트리 구조를 기반으로 설계되어 다양한 토폴로지에는 사용될 수 없음
 - 라우팅 루프가 생길 수 있음

기타 라우팅 프로토콜

- 내부 경로 제어 프로토콜(IGRP, Interior Gateway Routing Protocol)
 - RIP와 유사하지만 단점을 개선하기 위해 개발
- 거리 벡터 라우팅 프로토콜
 - 홉 수, 인터넷워크 지연 시간, 대역폭, 안전성과 부하
- 다중 경로 라우팅 기능
 - 라우터 간의 여러 경로를 자동으로 사용하여 트래픽을 여러 경로에 분산

기타 라우팅 프로토콜

- 확장 내부 경로 제어 프로토콜(EIGRP, Enhanced Interior Gateway Routing Protocol)
- IGRP를 개선해서 나온 프로토콜
- 확산 갱신 알고리즘(DUAL, Diffusing Update Algorithm)
 - 링크의 대역폭과 지연 시간을 결합한 척도를 사용하여 최적의 경로 결정
- 라우터간 트래픽 양을 줄임
 - 정기적으로 경로 갱신을 보내지 않고 필요할 때 부분 갱신 정보만 보냄

Thanks!

이 하 늘(dlgksmf6789@sju.ac.kr)