

TCP/IP 완벽 가이드

- 2-5부 IP 관련 기능 프로토콜 -

박 재 형 (jaehyoung@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

목 차

- 네트워크 주소변환 (NAT)프로토콜
- IP Security (IPsec)프로토콜
- IP 이동성 지원 (모바일 IP)프로토콜

네트워크 주소 변환 (NAT) 프로토콜

- 개요

- 등장배경

- IPv4 클래스 비사용 주소 지정은 IP 주소 고갈 속도를 늦추는 정도, 근본적인 해결은 하지 못함
- IP 주소 공간 고갈에 따른 할당 비용 증가, 보안 우려 증가 등의 문제를 보완할 기술이 필요

- IP NAT (Network Address Translation)

- NAT 라우터를 통해서 사설 네트워크와 공중 인터넷이 통신할 수 있도록 하는 것
 - NAT 라우터: 로컬 주소를 전역 주소로 또는 전역 주소를 로컬 주소로 변환

네트워크 주소 변환 (NAT) 프로토콜

- 개요

- IP NAT (Network Address Translation)

- 적은 수의 공용 IP를 사설 네트워크를 사용하는 호스트들이 공유 할 수 있음
- 외부장비가 실질적으로 NAT를 거치지 않고서는 공인IP를 가지고 있지 않기 때문에 사설 네트워크로 바로 접근하기 어려움

- IP NAT 구성이 가능했던 이유

- 대부분의 호스트는 클라이언트 장비
 - 노출이 필요 없는 클라이언트 장비가 통신을 알려진 서버에게 시작
- 동시에 인터넷에 접근하는 호스트는 많지 않음

네트워크 주소 변환 (NAT) 프로토콜

- 개요

- IP NAT의 장·단점

장점	단점
대량의 호스트가 소수의 공인 IP를 공유해 비용 절감과 공간 보존이 가능	NAT라는 추가적인 시스템이기 때문에 복잡해짐
사설 네트워크를 구성 함으로써 확장과 관리가 쉬움	특정 애플리케이션과 보안 프로토콜 (IPsec)과의 호환성 문제
인터넷 서비스 제공자 (ISP)변경 시 내부 주소를 다시 부여하지 않아도 됨	주소 변환으로 인한 성능 감소
외부에서는 내부주소를 알 수 없기 때문에 직접 접근이 어려움	공격자로부터 보호하지만 정당한 접근도 어려워질 수 있음

네트워크 주소 변환 (NAT) 프로토콜

- IP NAT 주소 구분

- 장비가 존재하는 위치에 따른 주소 표현
 - 내부 주소: 사설 네트워크에서 NAT를 사용하는 장비의 주소
 - 외부 주소: 사설 네트워크 외부에 있는 네트워크에서 존재하는 장비의 주소
- 내부/외부 관계없이 특정 네트워크에서 표현되는 주소
 - 로컬 주소: 내부 네트워크에서 표현되는 장비의 주소
 - 전역 주소: 외부 네트워크에서 표현되는 장비의 주소

네트워크 주소 변환 (NAT) 프로토콜

- IP NAT 주소 용어
 - NAT 내부/외부/로컬/전역 표

내부 로컬 주소 (Inside local address)	내부 전역 주소 (Inside global address)	외부 로컬 주소 (Outside local address)	외부 전역 주소 (Outside global address)
내부 네트워크에서 사용하는 장비의 주소 e.g., 사설 IP	내부 장비의 주소를 외부 네트워크에서 표현하기 위해 변환된 주소	외부 장비의 주소를 내부 네트워크에서 표현하기 위해 변환된 주소	공중 네트워크에서 사용하는 외부 장비의 주소 e.g., 공인 IP

네트워크 주소 변환 (NAT) 프로토콜

- IP NAT 주소 매핑

- NAT 라우터는 매핑 정보가 담긴 변환 테이블을 보고 전역 주소와 로컬주소를 변환시킴
 - e.g., 장비의 내부 로컬 주소를 내부 전역 주소로 매핑하는 정보
- 매핑 정보를 추가하는 방법
 - 정적 주소 매핑
 - 고정된 주소를 의미
 - 수동적으로 관리
 - 동적 주소 매핑
 - 필요할 때마다 주소를 즉시 생성, 사용이 완료되면 반환
 - 자동으로 관리
 - 정적 매핑 주소와 동적 할당에 쓰이는 주소가 중복되지 않도록 주의하면 함께 사용 가능

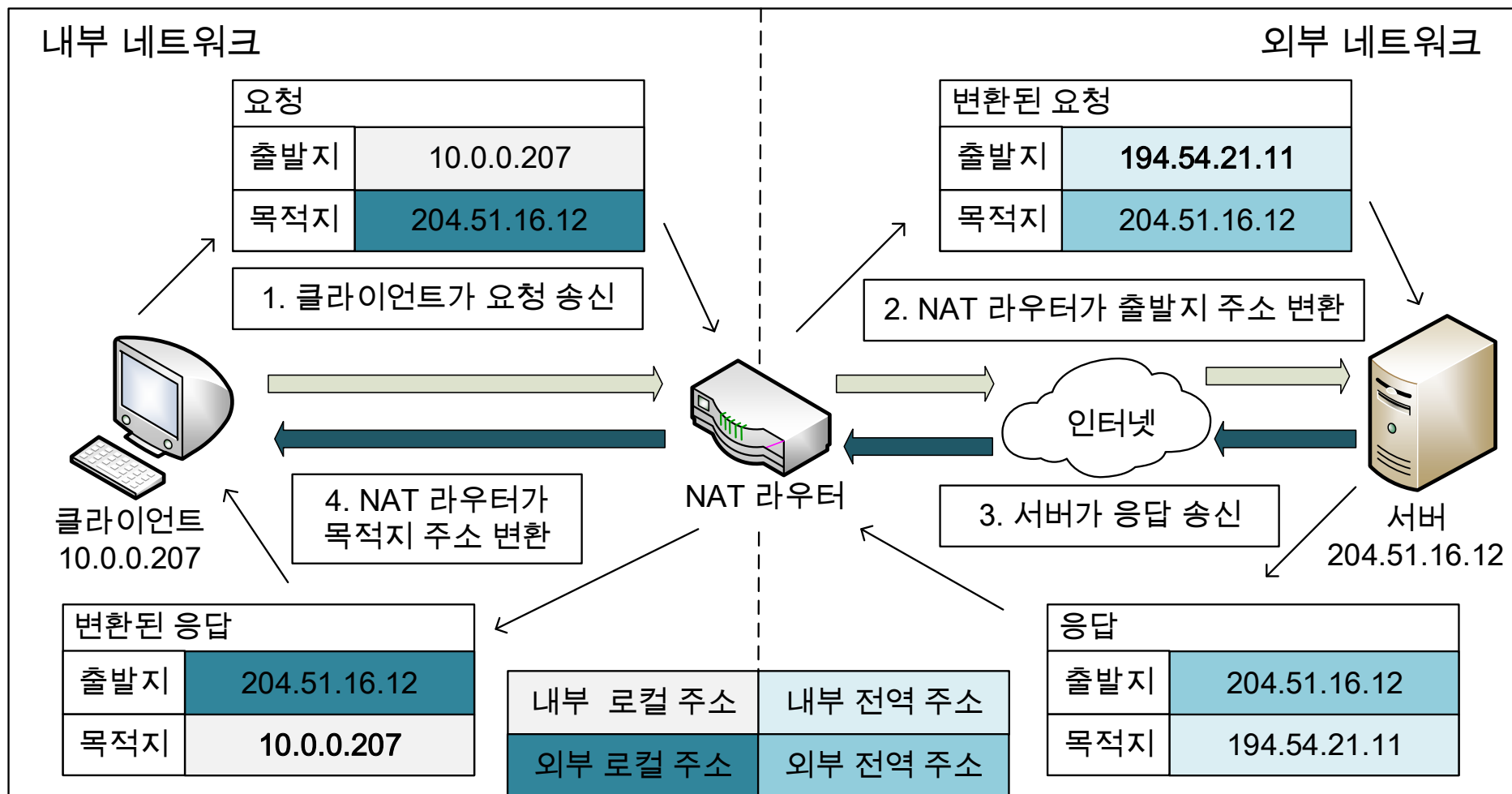
네트워크 주소 변환 (NAT)프로토콜

- NAT의 동작 방식
 - 단방향 (전통적/아웃바운드)동작
 - 내부 네트워크 장비가 외부 네트워크 장비로 요청할 경우
 - 양방향 (two-way/인바운드)동작
 - 외부 네트워크 장비가 내부 네트워크 장비로 요청할 경우
 - 포트기반 (과부하)동작
 - 사용할 수 있는 공인 IP가 전부 차 있는 경우
 - 중복/2회 NAT 동작
 - 내부 네트워크 주소와 외부 네트워크 주소가 중복될 경우

네트워크 주소 변환 (NAT) 프로토콜

- IP NAT 단방향 동작

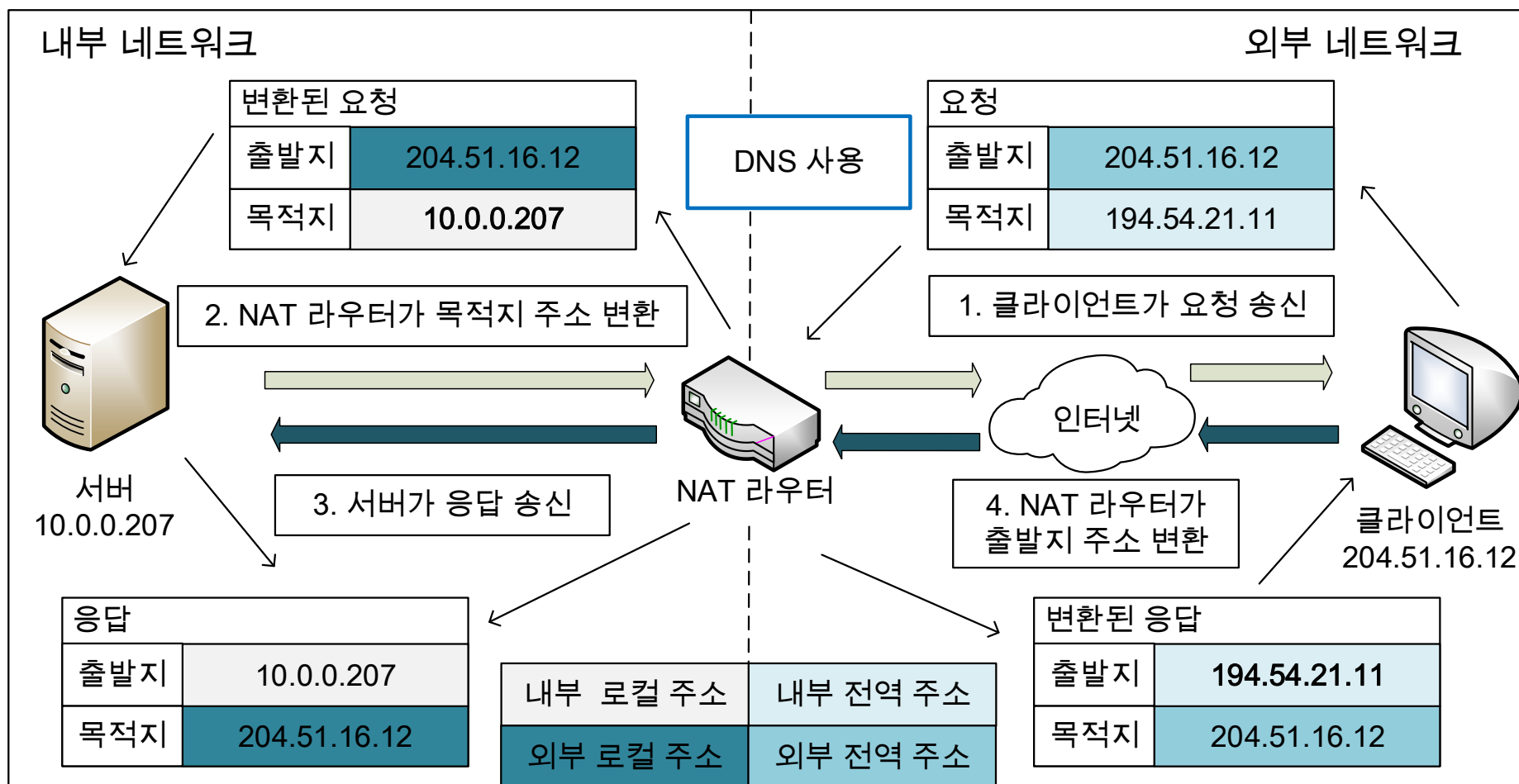
- 단방향 (전통적/아웃바운드) NAT 동작 그림



네트워크 주소 변환 (NAT) 프로토콜

- IP NAT 양방향 동작

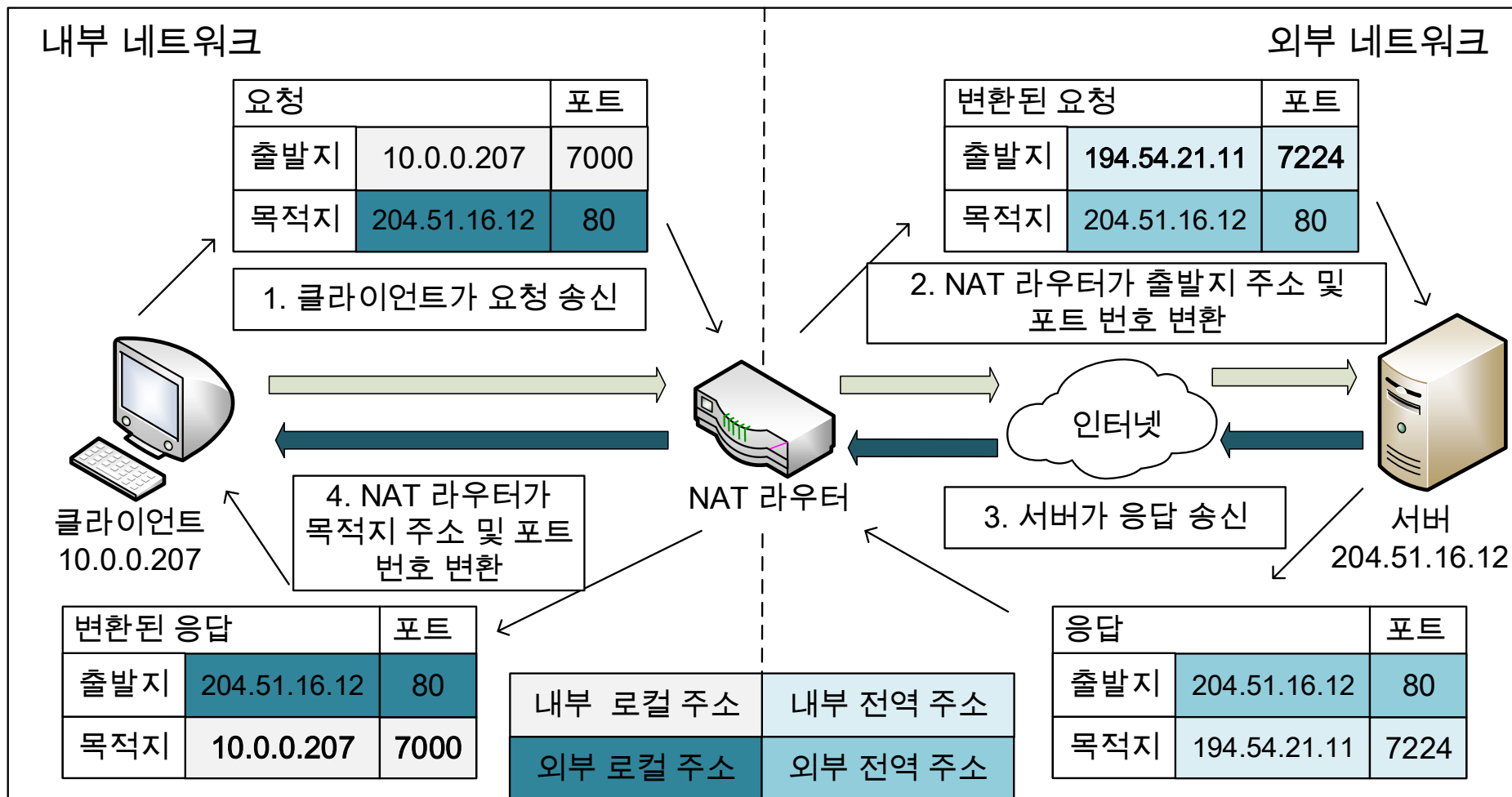
- 양방향 (two-way/인바운드) NAT 동작 그림



네트워크 주소 변환 (NAT) 프로토콜

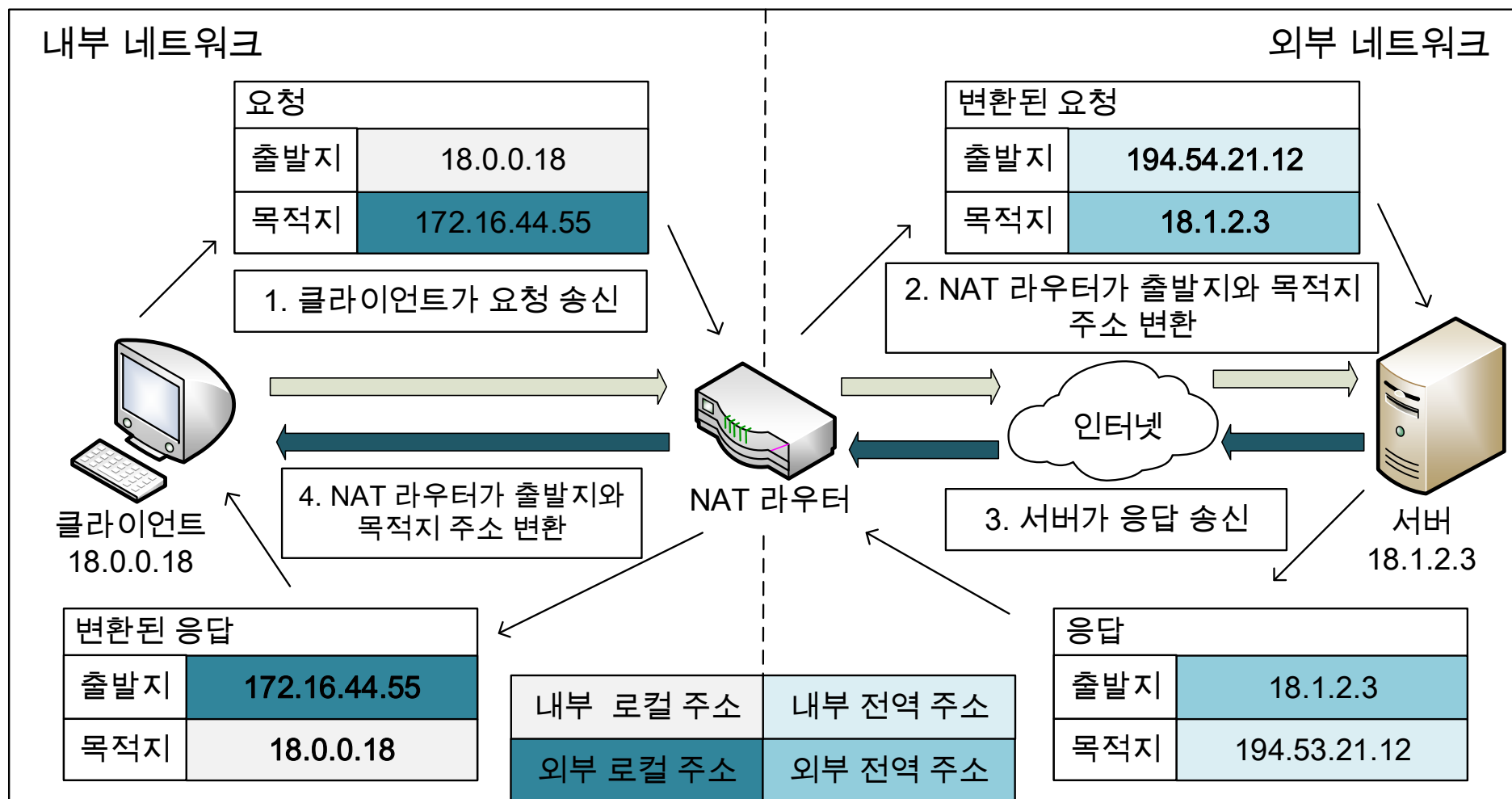
- IP NAT 포트기반 동작

- 포트기반 (과부하) NAT 동작 그림



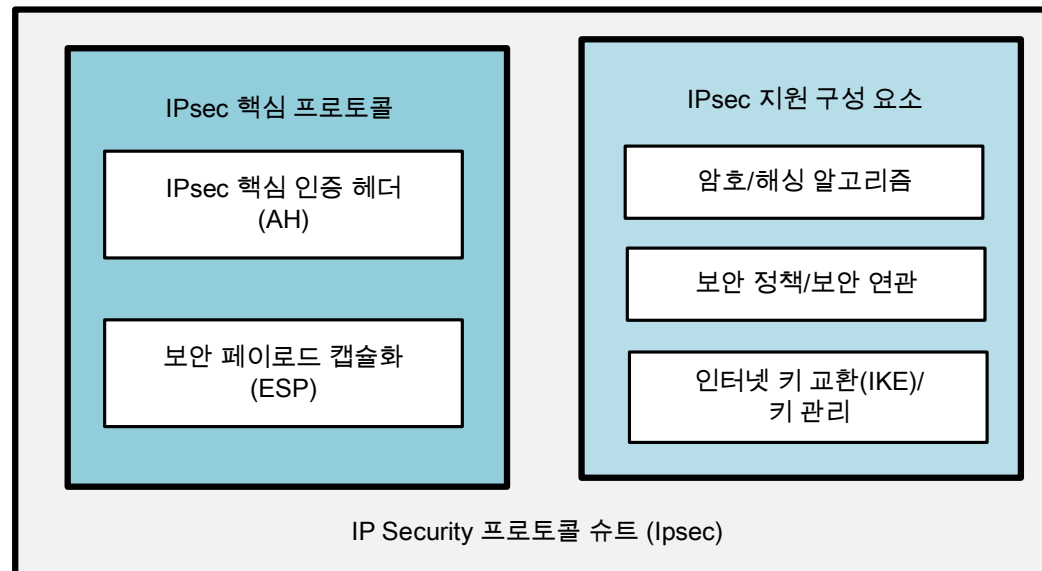
네트워크 주소 변환 (NAT) 프로토콜

- IP NAT 중복/2회 NAT 동작
- 중복 NAT/2회 NAT 동작 그림



IP Security (IPsec)프로토콜

- 개요
- 등장 배경
 - IP 보안 기능의 부재로 상위 계층 TCP/IP 애플리케이션이나 프로토콜이 보호 받지 못함
- 정의
 - 네트워크 계층에서의 보안을 위한 서비스와 프로토콜 모음
- 구성 요소



IP Security (IPsec)프로토콜

- 개요

- 기능

- 데이터 암호화
- 메시지의 무결성 인증
- 재전송 공격 (Replay attack)으로부터 보호
- 보안 요구에 맞는 보안 알고리즘과 키 협상
- 두 가지 보안 모드
 - 전송 (Transport)모드
 - 터널 (Tunnel)모드

IP Security (IPsec)프로토콜

- IPsec 구현

- 구현 방법

- 종단 호스트 구현

- 모든 호스트 장비에 설치하는 것
 - 모든 장비에 보안 구현이 가능하여 유연성과 보안성을 높임
 - IPsec 모드와 통합구조에 적용

- 라우터 구현

- 구현한 라우터 쌍 사이의 장비만 보호
 - 로컬 네트워크 내부 보안은 보장하지 않음
 - 터널모드와 스택 삽입 구조, 라인 삽입 구조에 적용

- 네트워크의 요구 사항에 따라 구현방법 고려

IP Security (IPsec) 프로토콜

- IPsec 구조

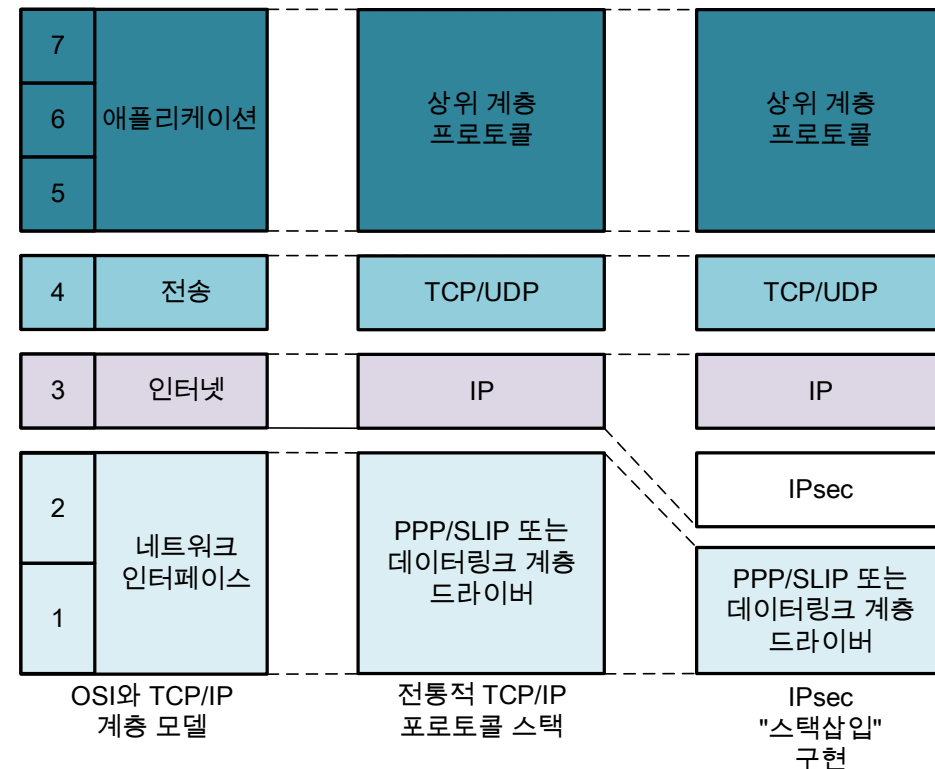
- TCP/IP 프로토콜 스택과 결합하는 방법

- 통합 구조

- IPsec의 프로토콜과 기능을 IP 계층에 직접 내장
 - 추가적인 하드웨어나 계층 불필요
 - IPv4 경우, 각 장비의 IP 구현을 변경해야 함

- 스택 삽입 구조 (BITS, Bump In The Stack)

- IP와 데이터 링크 계층 사이에 별도로 존재
 - 데이터 링크 계층에 가기 전에 보안 기능을 덧붙인 뒤 전달



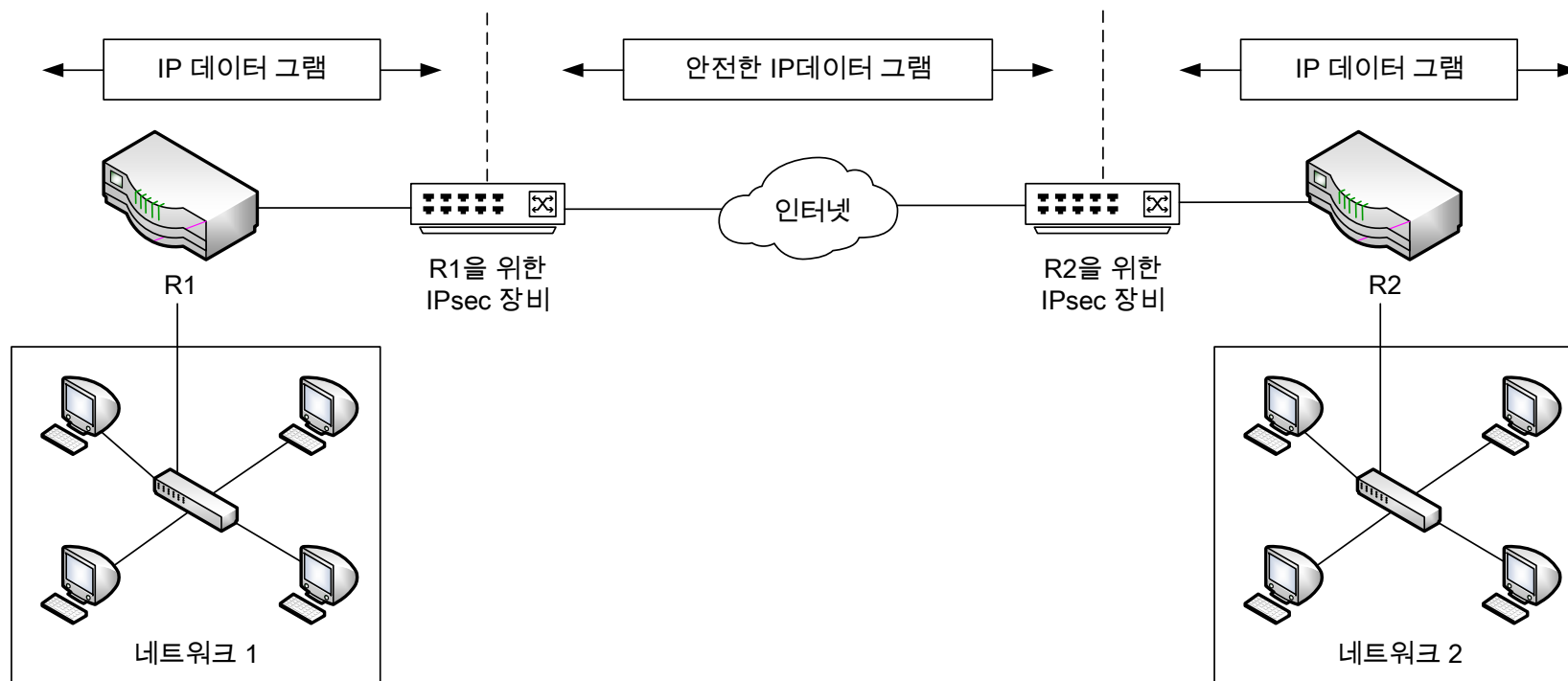
IP Security (IPsec) 프로토콜

- IPsec 구조

- TCP/IP 프로토콜 스택과 결합하는 방법

- 라인 삽입 구조 (BITW, Bump In The Wire)

- IPsec 서비스를 제공하는 하드웨어 장비를 기존 구성에 추가
 - 네트워크가 복잡해지고 구현 비용이 비쌈

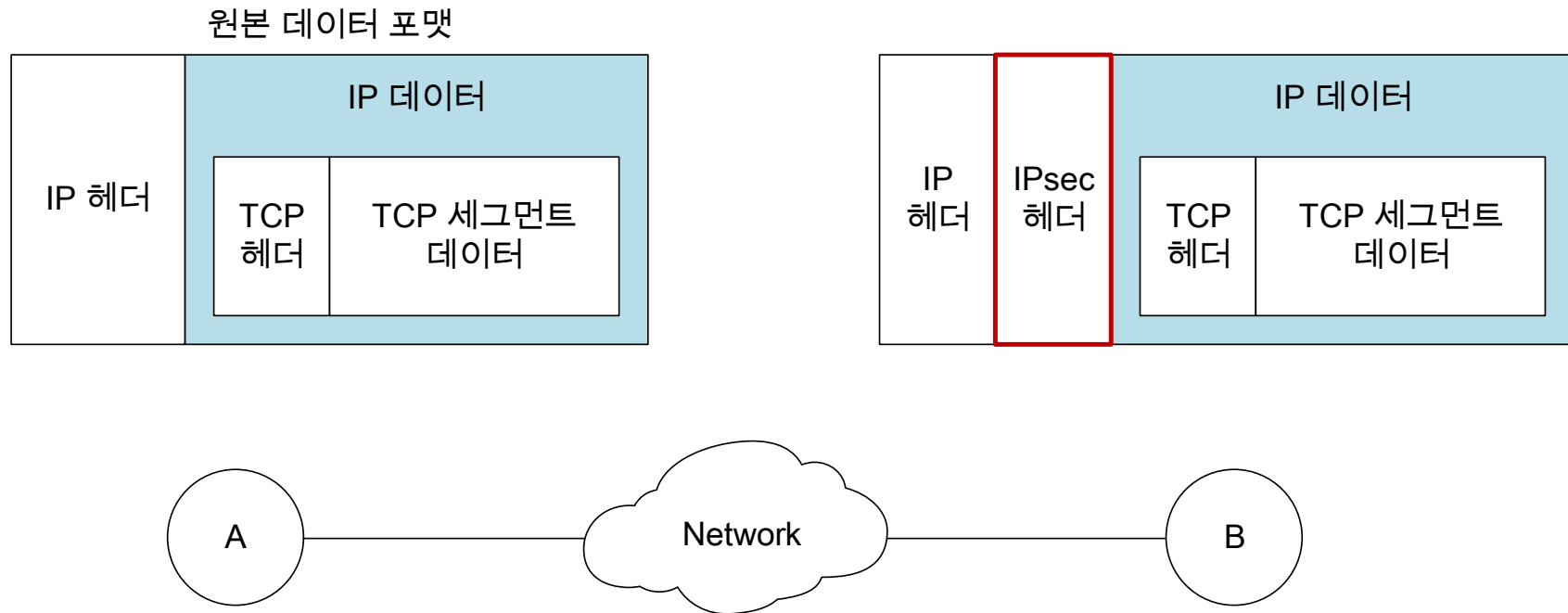


IP Security (IPsec) 프로토콜

- IPsec 동작 방식

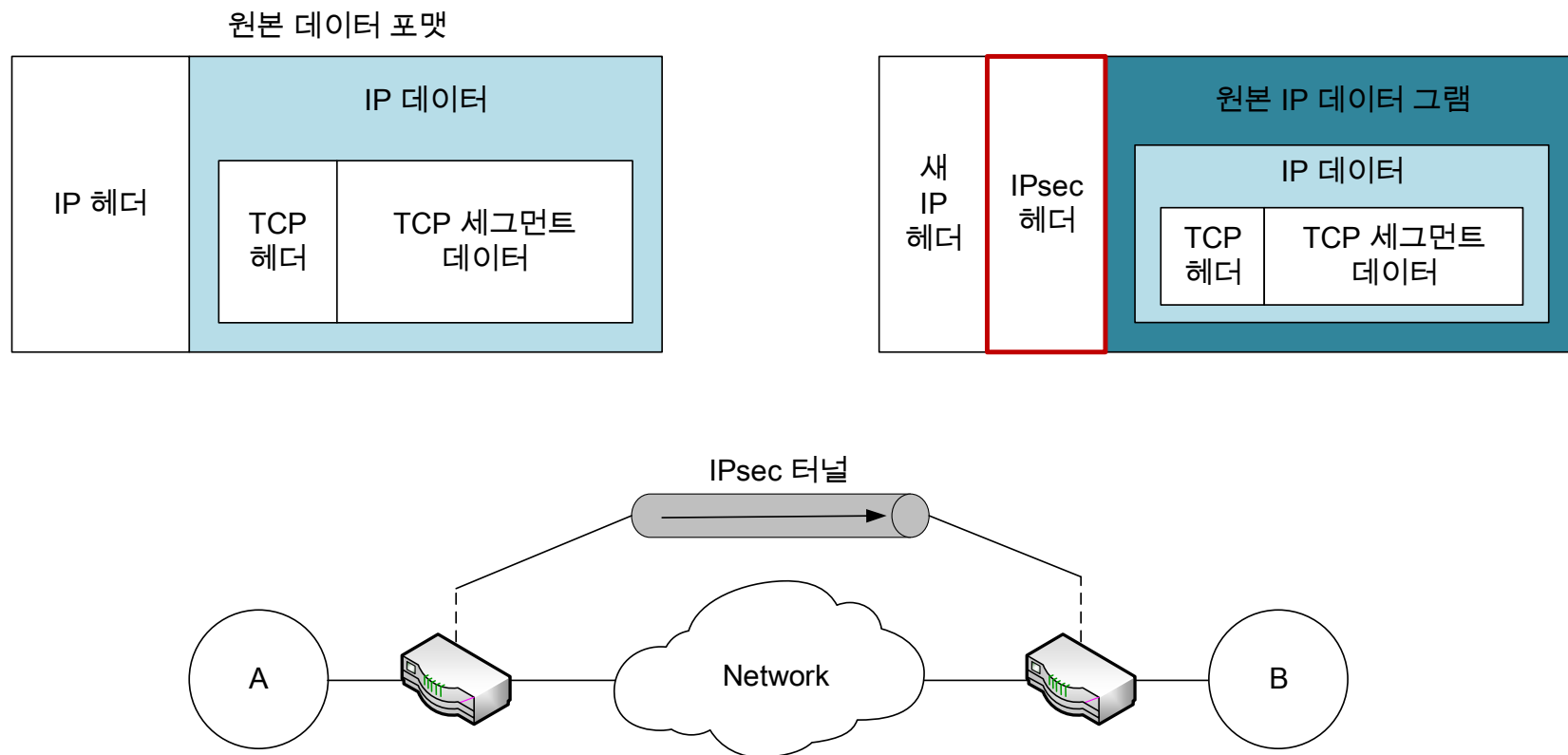
- 전송 모드 (Transport mode)

- 상위 계층 프로토콜을 보호하기 위해 사용
- IP 헤더는 보호되지 않고 IP 페이로드까지만 보호



IP Security (IPsec) 프로토콜

- IPsec 동작 방식
 - 터널 모드 (Tunnel mode)
 - 추가적인 캡슐화를 진행
 - IP 데이터그램 전체를 보호



IP Security (IPsec)프로토콜

- 보안 연관 (SA, Security Association)
 - 한 장비와 다른 장비 사이에 맺은 보안 방법을 명시
 - 보안 연관 데이터베이스 (SAD, Security Association Database) 에 저장
- SA는 트리플이라고 불리는 인자 모음으로 정의
 - 보안 인자 인덱스 (SPI, Security Parameters Index)
 - SA를 식별하도록 수신자가 선택한 32 bits 값
 - 메시지 수신자가 데이터그램에 어떤 SA가 적용되는지 파악하는 데 쓰임
 - IP 목적지 주소
 - SA가 수립된 장비의 주소
 - 보안 프로토콜 식별자
 - AH/ESP 보안 연결 식별
 - 둘 다 사용하는 경우 각각 별도의 SA를 지정

IP Security (IPsec)프로토콜

- 보안 정책 (SP, Security Policy)
 - 서로 다른 패킷들을 어떻게 처리 할 것인지 결정
 - 특정 데이터그램을 IPsec 에서 처리할 필요가 있는지 여부 결정
- 보안 정책 데이터 베이스 (SPD, Security Policy Database)에 저장
- SPD를 가지고 데이터에 어떤 작업을 할 건지 확인하고 SAD 내용에 따라 데이터그램을 처리

IP Security (IPsec)프로토콜

- IPsec 인증 헤더 (AH, Authentication Header)
 - 기능
 - 데이터의 무결성 (Integrity) 보장
 - 개체 인증 (Authentication)
 - 재전송 공격에 대한 보호기능 제공
 - 인증 데이터를 만들기 위해 해쉬 알고리즘 사용
 - e.g., MD5, SHA-1
 - AH 헤더 위치
 - 전송/터널 모드에 따라 적절한 위치에 삽입됨

IP Security (IPsec) 프로토콜

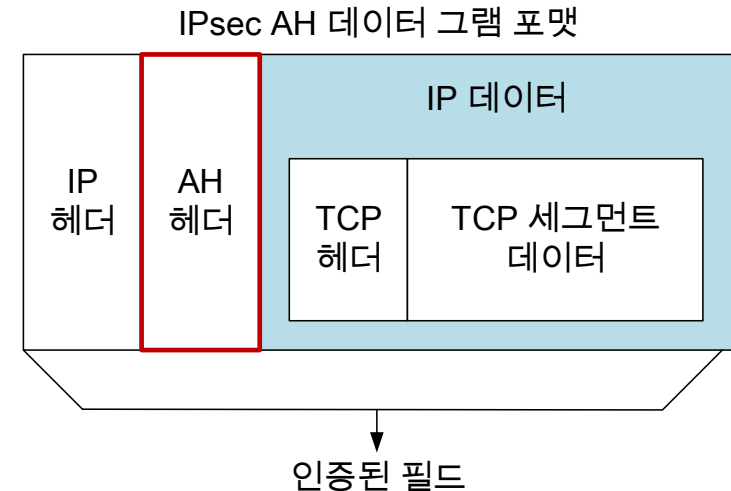
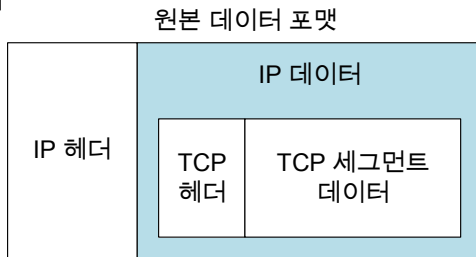
- IPsec 인증 헤더 (AH)
 - AH를 포함하는 패킷 포맷
 - 인증 데이터(가변 길이)
 - 전체 IP 패킷에 해쉬 함수를 적용한 결과 값



IP Security (IPsec) 프로토콜

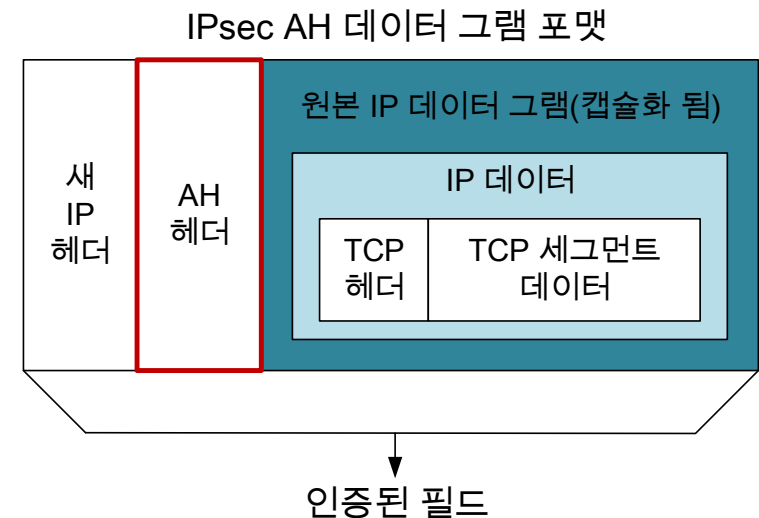
- 전송 모드의 AH 프로토콜

- 원본 IP 데이터그램의 헤더와 페이로드 사이에 AH 추가하여 캡슐화



- 터널 모드의 AH 프로토콜

- 캡슐화된 IP 데이터그램에 AH를 추가하여 새로운 IP 데이터그램으로 캡슐화



IP Security (IPsec)프로토콜

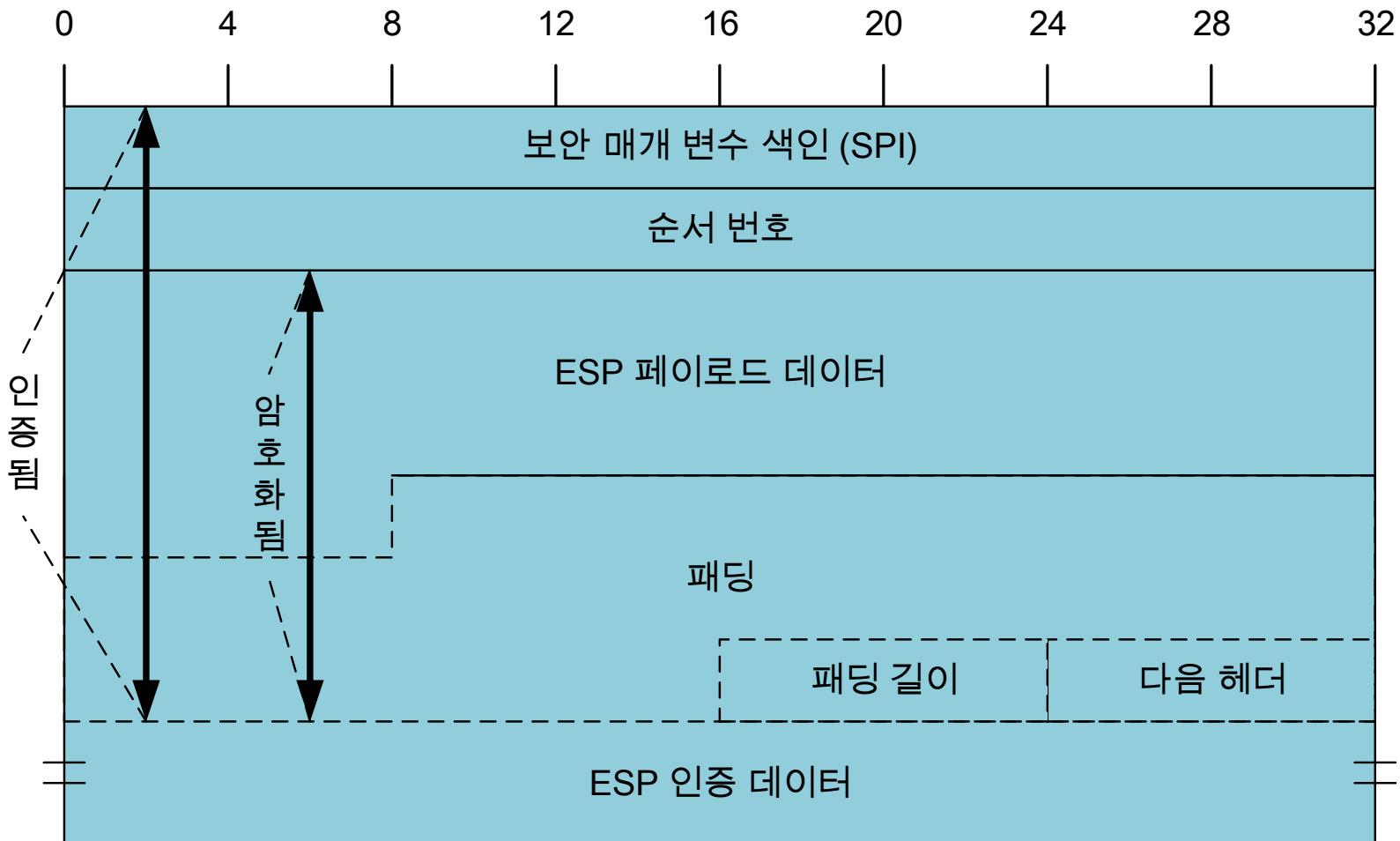
- IPsec 보안 페이로드 캡슐화 (ESP)
 - 기능
 - IP 데이터그램의 무결성, 인증, 암호화 제공
 - 데이터 기밀성 제공
 - 데이터를 암호화하여 지정된 수신자만 볼 수 있도록 함
 - 수신 측에는 인터넷 키 교환 (IKE, Internet Key Exchange)로 미리 교환한 Key 값을 이용하여 데이터를 복호화
 - DES, 3DES 등 사용

IP Security (IPsec)프로토콜

- IPsec 보안 페이로드 캡슐화 (ESP)
 - 요소 구분
 - ESP 헤더
 - 두 가지 모드마다 붙는 위치가 다름
 - 암호화 되지 않음
 - ESP 트레일러
 - 패딩이 필요한 경우, 패딩을 한 뒤 암호화 수행
 - ESP 인증 데이터 필드
 - 인증 서비스 제공
 - 해시 알고리즘을 사용한 값 사용

IP Security (IPsec) 프로토콜

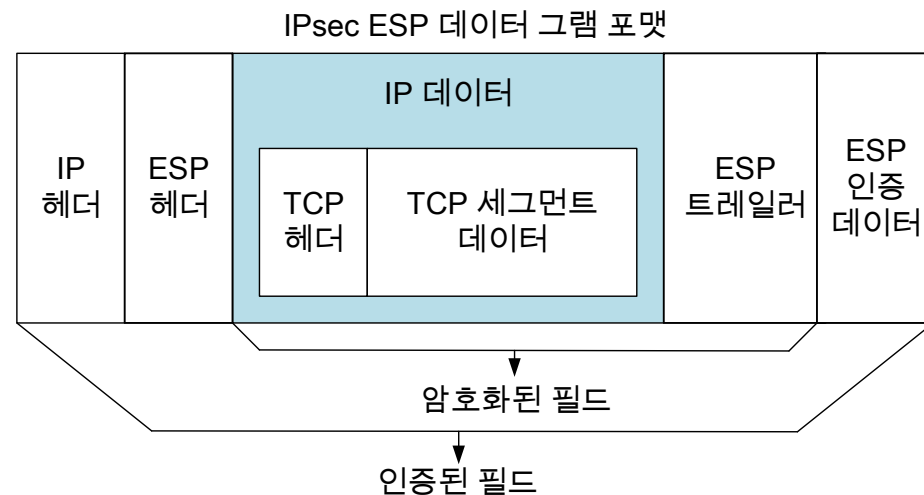
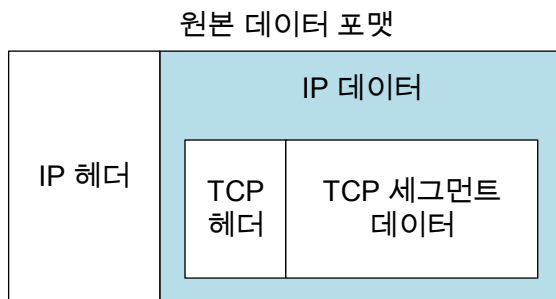
- IPsec 보안 페이로드 (ESP)
- ESP를 포함하는 패킷 포맷



IP Security (IPsec) 프로토콜

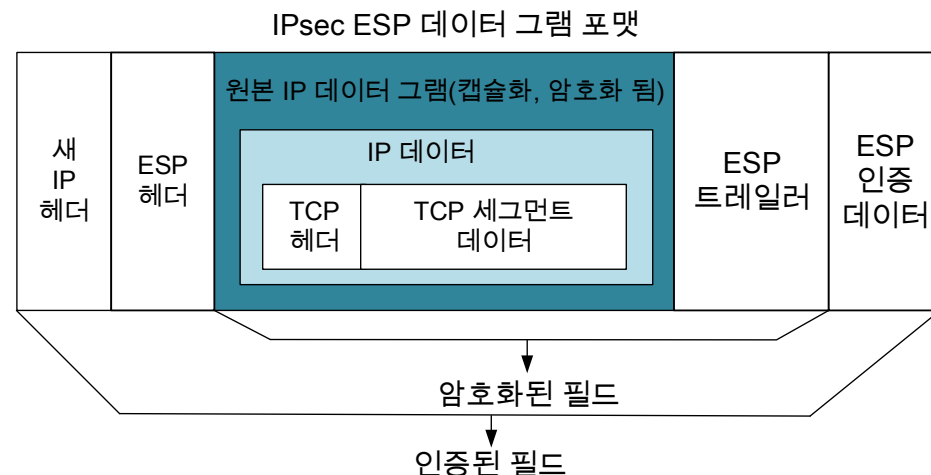
• 전송 모드의 ESP 프로토콜

- 암호화된 데이터 앞에 ESP 헤더 위치
- 암호화된 데이터 뒤에 ESP 트레일러 및 인증 데이터 위치



• 터널 모드의 ESP 프로토콜

- 원본 IP 데이터그램이 ESP 헤더와 트레일러, 인증 데이터로 둘러싸여 있음



IP Security (IPsec)프로토콜

- IPsec 인터넷 키 교환 (IKE, Internet Key Exchange)
 - 정의
 - 보안관련 설정들을 생성하고, 협상하며, 관리하는 프로토콜
 - 기능
 - 안전한 통신을 위해 필요로 하는 정보를 교환하기 위한 구조를 제공
- IKE 동작
 - ISAKMP (Internet Security Association and Key Management Protocol)구조 내에서 동작
 - 1단계: 안전한 교환을 동의하는 ISAKMP를 위한 SA를 생성
 - 2단계: 수립된 ISAKMP를 위한 SA를 이용해 AH/ESP 프로토콜을 위한 SA 생성

모바일 IP

- 개요

- 등장배경

- IP 네트워크에서 IP 주소 기반으로 라우팅을 하기 때문에 이동 장비를 지원 하지 못함
 - IP 주소는 네트워크 ID와 호스트의 ID로 나눠 서로 결합됨

- IP 주소 체계에서 이동 장비가 선택할 수 있는 방안

1. 이동한 네트워크로 IP 주소 변경

- 사용하고 있던 연결을 모두 끊고 다시 연결해야 함
- 다른 장비에게 바뀐 주소를 알리기 어려움

2. IP 라우팅 방식을 변경

- 전체 주소로 라우팅하게 되면 라우팅 테이블 항목 수가 많아져 관리가 어려움

모바일 IP

- 개요

- 해결책

- 이동성 지원 프로토콜(모바일 IP)을 정의하여 IP에 추가시켜 이동성 문제를 해결

- 모바일 IP

- 이동 장비의 홈 네트워크에 도착한 패킷을 이동 장비가 실제로 있는 네트워크로 전달하는 시스템

모바일 IP

- 모바일 IP 구성 장비

- 이동 장비

- 네트워크를 이동하는 장비

- 홈 에이전트 (Home agent)

- 이동 장비의 홈 네트워크의 라우터
- 이동 장비가 받아야 할 패킷을 대신 받아 이동 장비에게 전달

- 외부 에이전트 (Foreign agent)

- 이동 장비가 현재 위치하고 있는 네트워크의 라우터
- 새로운 홈 네트워크의 역할을 수행
- 모바일 IP 동작을 위해 이동 정보를 공유할 수 있음

모바일 IP

- 모바일 IP 주소

- 홈 주소

- 이동 장비에게 할당된 정상적인 고정 IP 주소

- CoA

- 임시 주소로 이동 장비가 네트워크 외부로 움직였을 때 사용하는 주소

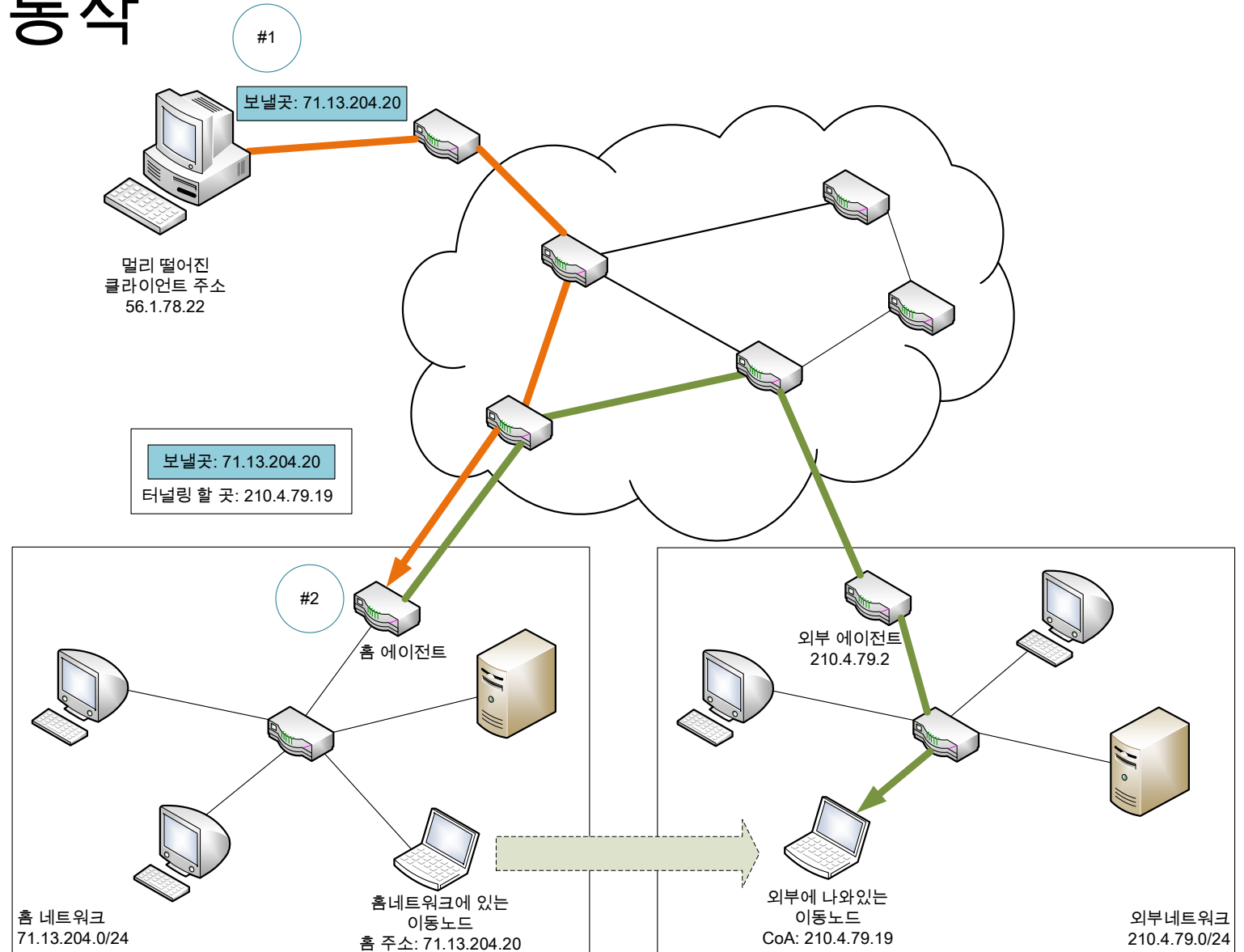
- 모바일 IP에서만 사용

- 데이터그램을 전달하거나 관리 기능을 실행 할 때만 사용

- 외부 에이전트가 광고 메시지와 같은 방법으로 얻을 수 있음

모바일 IP

• 모바일 IP 동작



모바일 IP

- 장점

- 기존 방식(장비, 주소지정, 라우팅) 변경 없이 중단 없는 이동성 지원
- 하드웨어 변경 최소화
 - 이동 장비가 사용할 라우터와 소프트웨어만 변경하면 됨
- 확장성
 - 어떤 네트워크로 이동하여도 지원 가능
- 보안
 - 메시지를 리다이렉트 (Redirect)하여 인증 과정을 거침
 - 데이터가 해당 네트워크의 자원인지 다른 네트워크의 자원인지 판단하여 경로를 바꾸는 것

모바일 IP

- 한계점
 - 무선 환경에서 한계를 가짐
 - 실시간(1초에 1번) 네트워크를 바꾸지 않을 것이라는 가정하에 설계됨
- 고정 IP를 갖는 장비에게만 지원
 - 원래 IP 주소와 네트워크를 알아야 하기 때문에 DHCP (Dynamic Host Configuration Protocol)을 통해 동적 IP를 가지는 장비는 사용 하기 힘들

모바일 IP

- CoA 종류

- 외부 에이전트 CoA

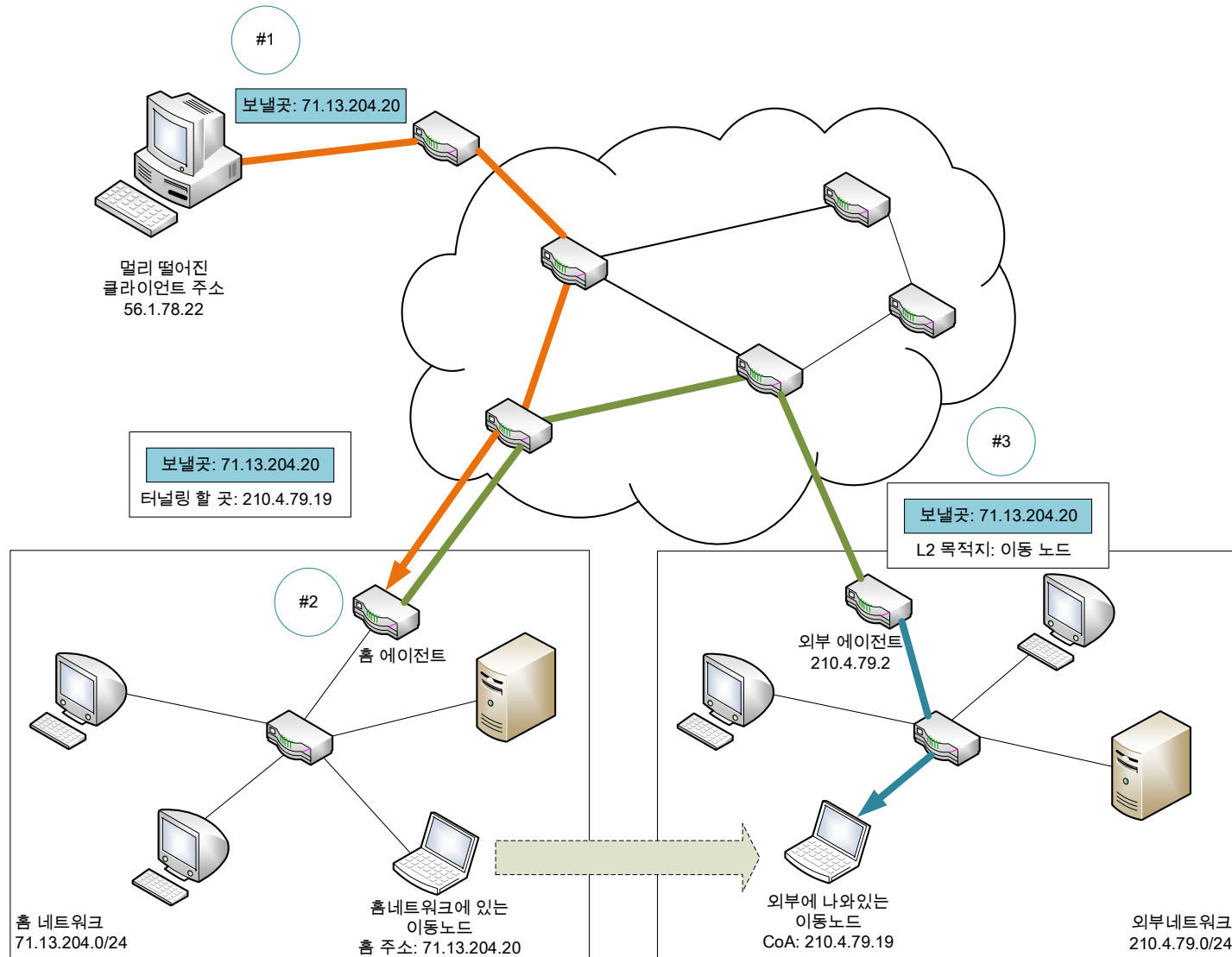
- 이동 장비는 외부 에이전트 IP 주소 사용
 - 데이터 링크 계층 기술로 외부 에이전트에게 데이터를 전달 받음
- 모든 패킷은 외부 에이전트를 거쳐서 감

- 공존 CoA

- 이동 장비는 직접 할당된 주소 사용
 - 직접 주소를 할당하거나 DHCP를 사용해서 자동으로 할당
- 데이터그램을 이동 장비가 직접 받음

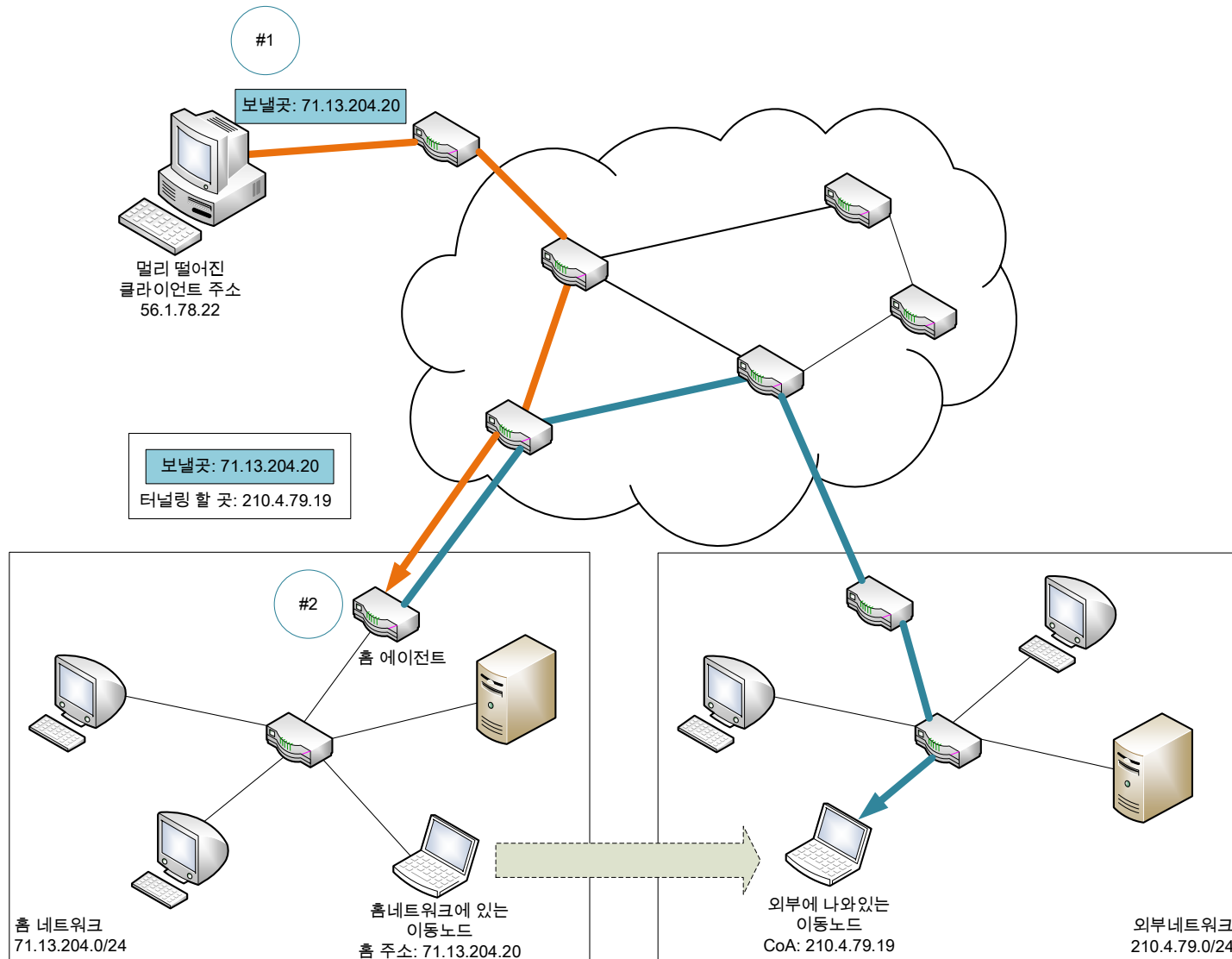
모바일 IP

• 외부 에이전트 CoA를 사용하는 모바일 IP 동작



모바일 IP

- 공존 CoA를 사용하는 모바일 IP 동작



모바일 IP

- 두 가지 CoA의 차이점
 - 외부 에이전트 CoA
 - 외부 에이전트가 있는 경우
 - 외부 네트워크에 있는 모든 이동 장비들이 같은 외부 CoA를 사용
 - 각자 다른 IP주소를 가질 필요가 없기 때문에 주소 고갈 문제가 없음
 - 공존 CoA
 - 외부 에이전트가 없는 경우
 - 각 장비가 외부 네트워크에서도 유일한 IP 주소를 가져야함
 - 모바일 IP 기능이 없는 네트워크를 지날 때에도 CoA 사용 가능
 - 연결을 오랫동안 유지하는 경우

모바일 IP

- 모바일 IP 기능

- 에이전트 발견

- 광고 또는 요청 단계 이후에 이동 노드는 자신의 위치와 에이전트의 존재를 알게 됨

- 에이전트 등록

- 에이전트에 등록 후, 패킷을 직접 또는 간접으로 전달

모바일 IP

- 에이전트 발견

- 이동 장비가 자신의 위치를 판단하고 홈 에이전트나 외부 에이전트와의 관계를 유지하는 것

- 에이전트 발견 과정

1. 에이전트/노드 통신

- 에이전트 광고 메시지를 사용하여 주기적으로 자신의 존재를 알림 (브로드캐스트)
- 에이전트 광고 메시지를 받지 못했을 때 직접 에이전트 요청 메시지를 보냄

2. 현재 위치 판단

- 이동 장비의 위치를 파악(홈 or 외부)

3. CoA (Care-of-Address) 할당

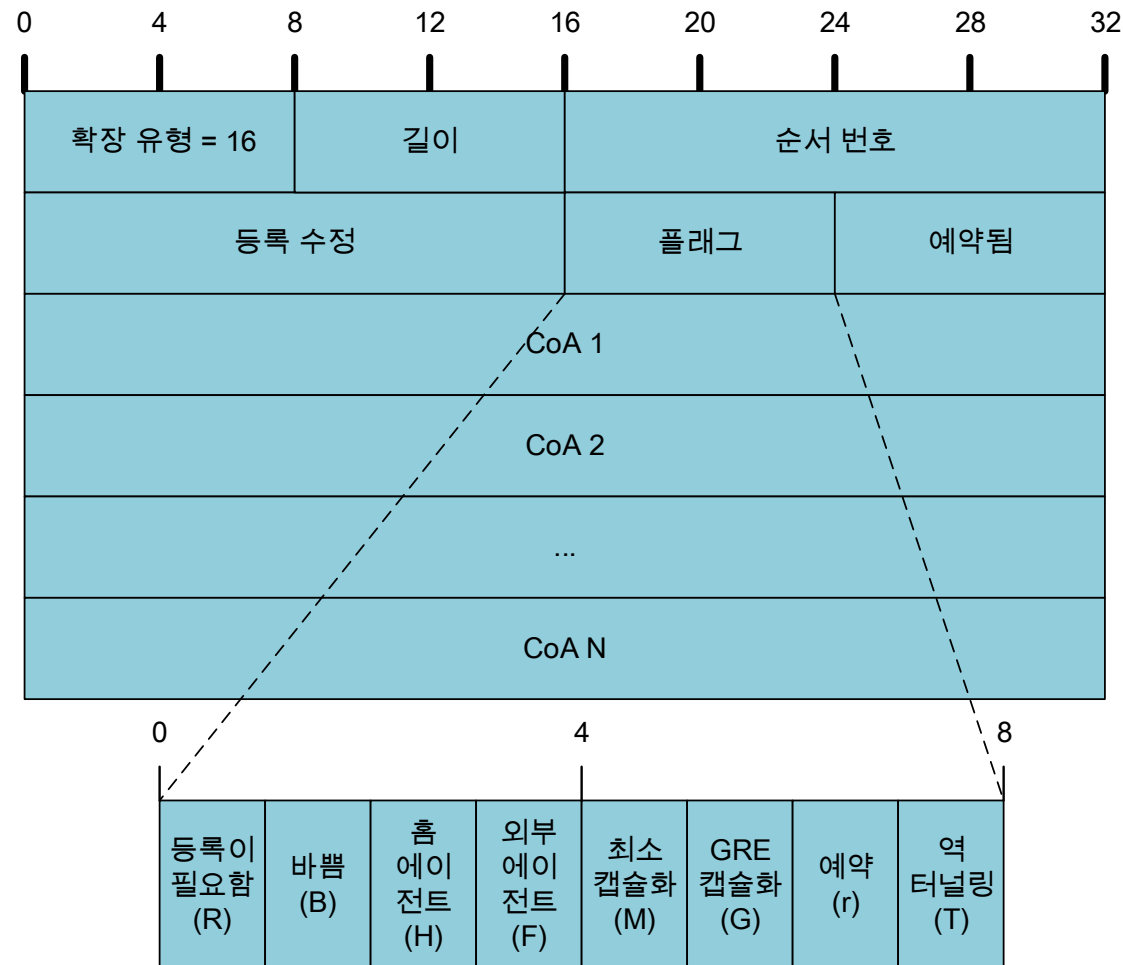
- 이동 장비가 사용할 CoA를 얻음
 - 목적지로 데이터그램을 전달할 때 사용

모바일 IP

- 에이전트 광고 (Agent advertisement)
 - 에이전트 광고 메시지
 - 모바일 IP 에이전트로 활동할 수 있는 라우터가 정기적으로 전송
 - 모바일 IP 관련 정보와 하나 이상의 확장을 포함하는 라우터 광고 메시지로 구성
 - 이동 에이전트 광고 (Mobility Agent Advertisement) 확장
 - 에이전트가 모바일 IP 기능을 갖추었다는 것을 알리는 기본 확장
 - 접두사 길이 (Prefix-Length) 확장
 - CoA 주소의 네트워크 ID의 비트 수를 알려줌
 - 1바이트 패딩 (One-Byte Padding) 확장
 - 메시지 길이 짝수로 패딩

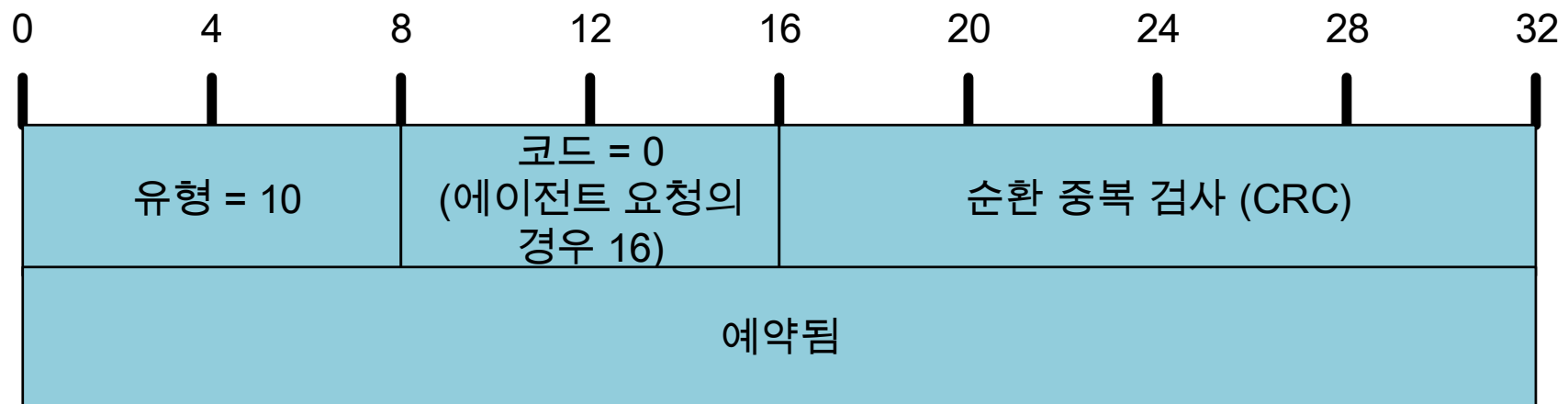
모바일 IP

- 에이전트 광고
- 메시지 포맷



모바일 IP

- 에이전트 요청 (Agent solicitation)
 - 에이전트 요청 메시지
 - 모바일 IP 장비가 홈 에이전트에게 광고 전송을 요청
 - 메시지 포맷



모바일 IP

- 에이전트 등록

- 홈 에이전트 등록 (Home agent registration)

- 이동 장비가 홈 에이전트와 통신을 하면서 필요한 정보와 지시를 주고 받는 것

- 이동 장비 등록 이벤트

- 등록 이동

- 장비가 외부 네트워크에 도착하면 등록을 시작

- 등록 해제

- 다시 홈 네트워크로 돌아오면 전달을 취소하는 과정

- 재등록

- 다른 외부 네트워크로 이동하거나 CoA가 바뀌면 이동 장비는 홈 에이전트에게 알려 재등록

모바일 IP

- 에이전트 등록

- 등록 요청과 응답 메시지

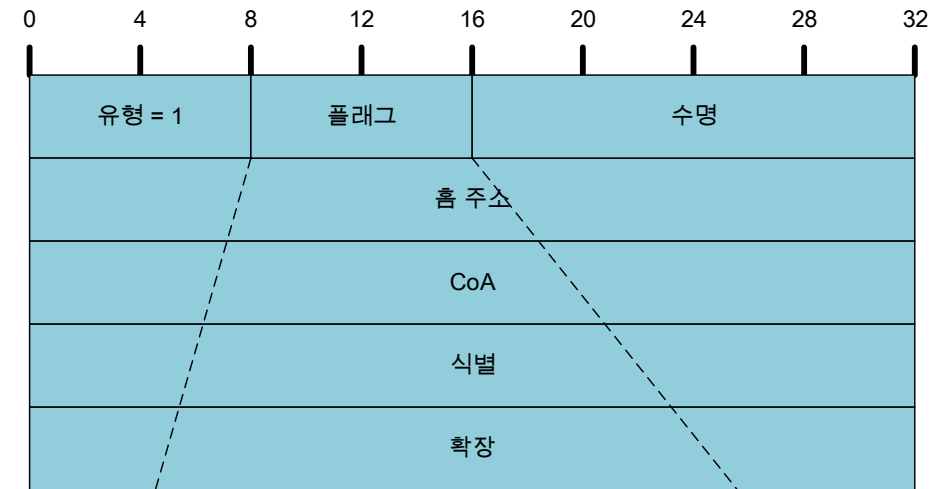
- 전송 계층의 UDP (User Datagram Protocol)에 의해 전달
 - 에이전트는 UDP 434 포트에서 등록 요청
 - 모바일 노드가 사용한 임시 포트로 응답

- 등록 과정

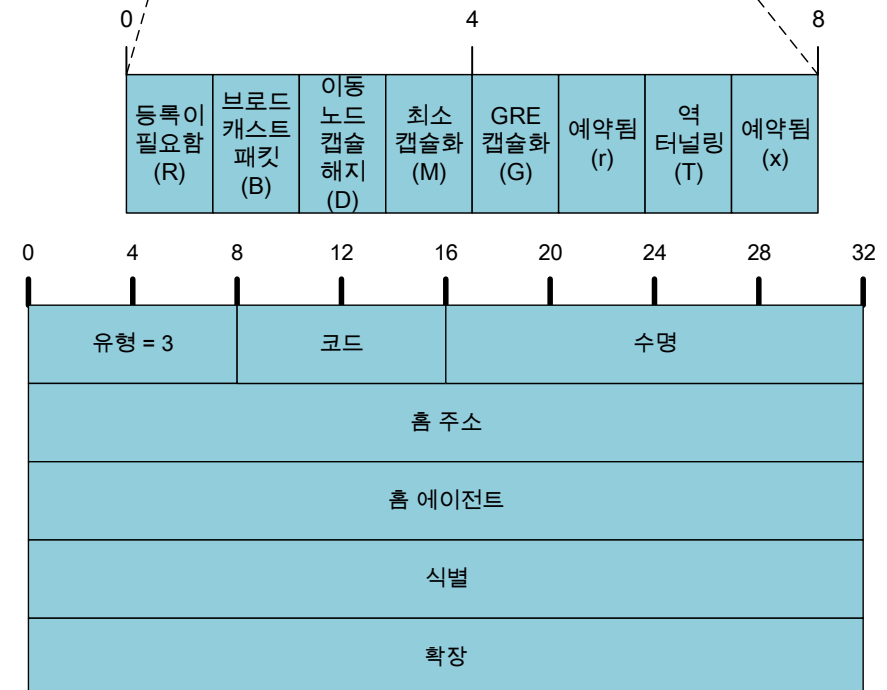
- 이동 장비가 사용하는 CoA의 종류에 따른 두 가지 방식
 - 직접 등록(공존 CoA)
 1. 이동 장비가 홈 에이전트에게 등록 요청 메시지 전송
 2. 홈 에이전트는 이동 장비에게 등록 응답 메시지 전송
 - 간접 등록(외부 에이전트 CoA)
 1. 이동 장비가 외부 에이전트에게 등록 요청 메시지 전송
 2. 외부 에이전트가 등록 요청을 처리하여 홈 에이전트에게 전송
 3. 홈 에이전트는 외부 에이전트에게 등록 응답 메시지 전송
 4. 외부 에이전트가 등록 응답을 받아 처리하고 이동 장비에게 전송

모바일 IP

- 등록 요청 메시지 포맷

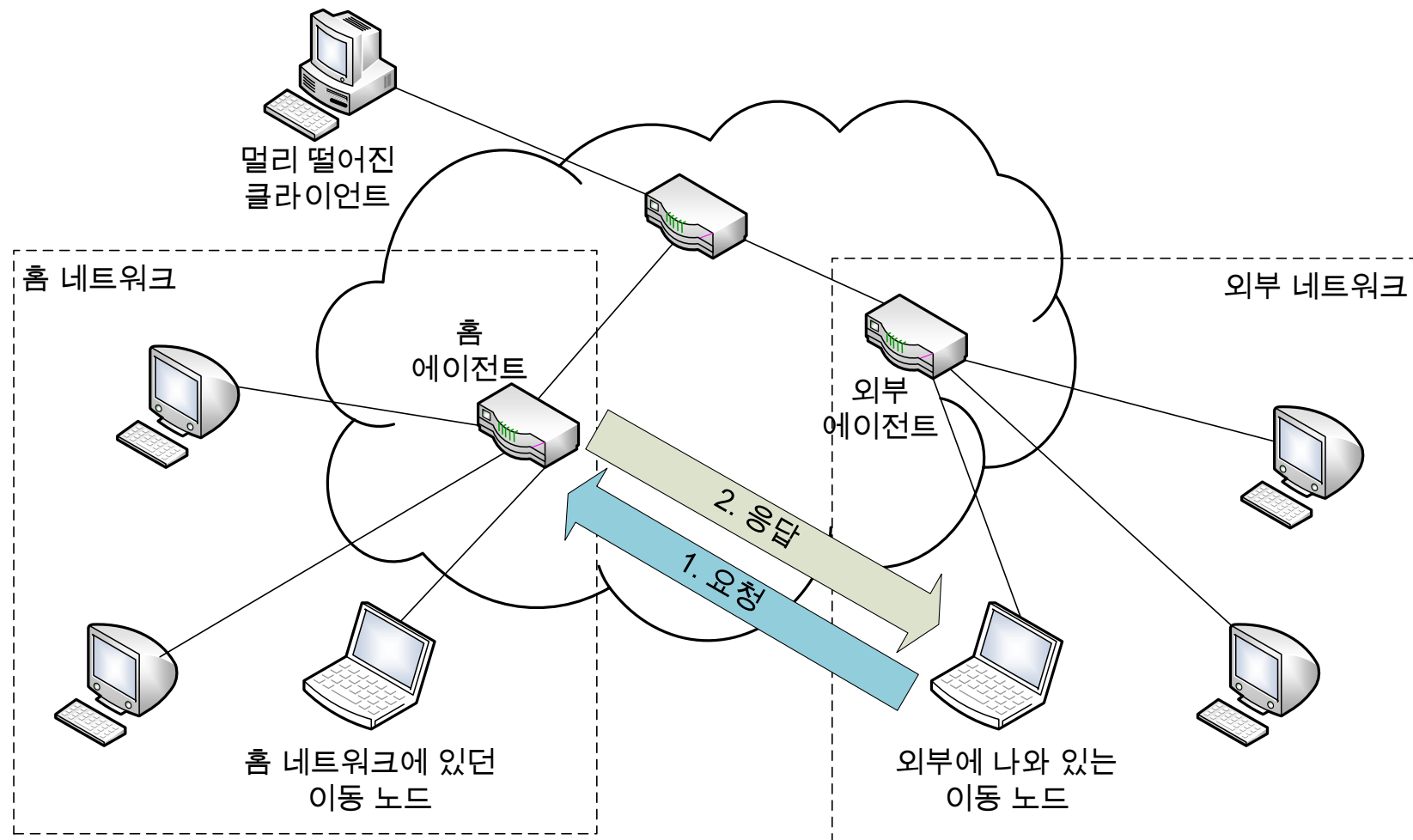


- 등록 응답 메시지 포맷



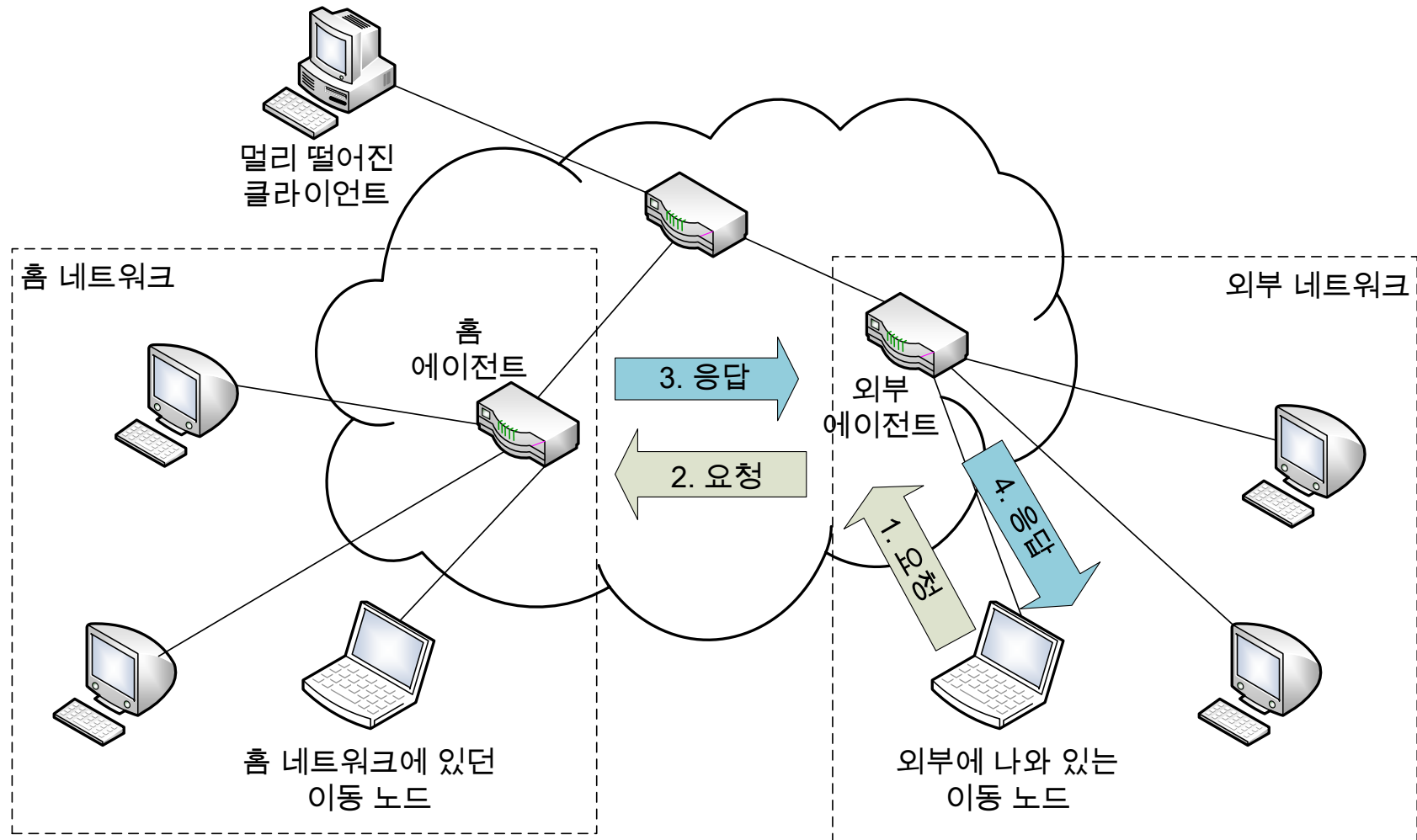
모바일 IP

- 에이전트 등록 과정
- 직접 등록 그림



모바일 IP

- 에이전트 등록 과정
- 간접 등록 그림



모바일 IP

- 데이터 캡슐화와 터널링
 - 모바일 IP 터널링
 - 외부 에이전트 CoA
 - 외부 에이전트에서 터널이 끝남
 - 홈 에이전트에게 받은 캡슐화된 데이터그램의 IP 헤더를 벗겨내고 원본 데이터그램을 이동 장비에게 전달
 - 외부 에이전트와 이동 장비는 같은 네트워크 안에 있기 때문에 데이터 링크 계층을 통해 전송
 - 공존 CoA
 - 이동 장비에서 터널이 끝남
 - 이동 장비가 캡슐화 헤더를 벗겨 냄

모바일 IP

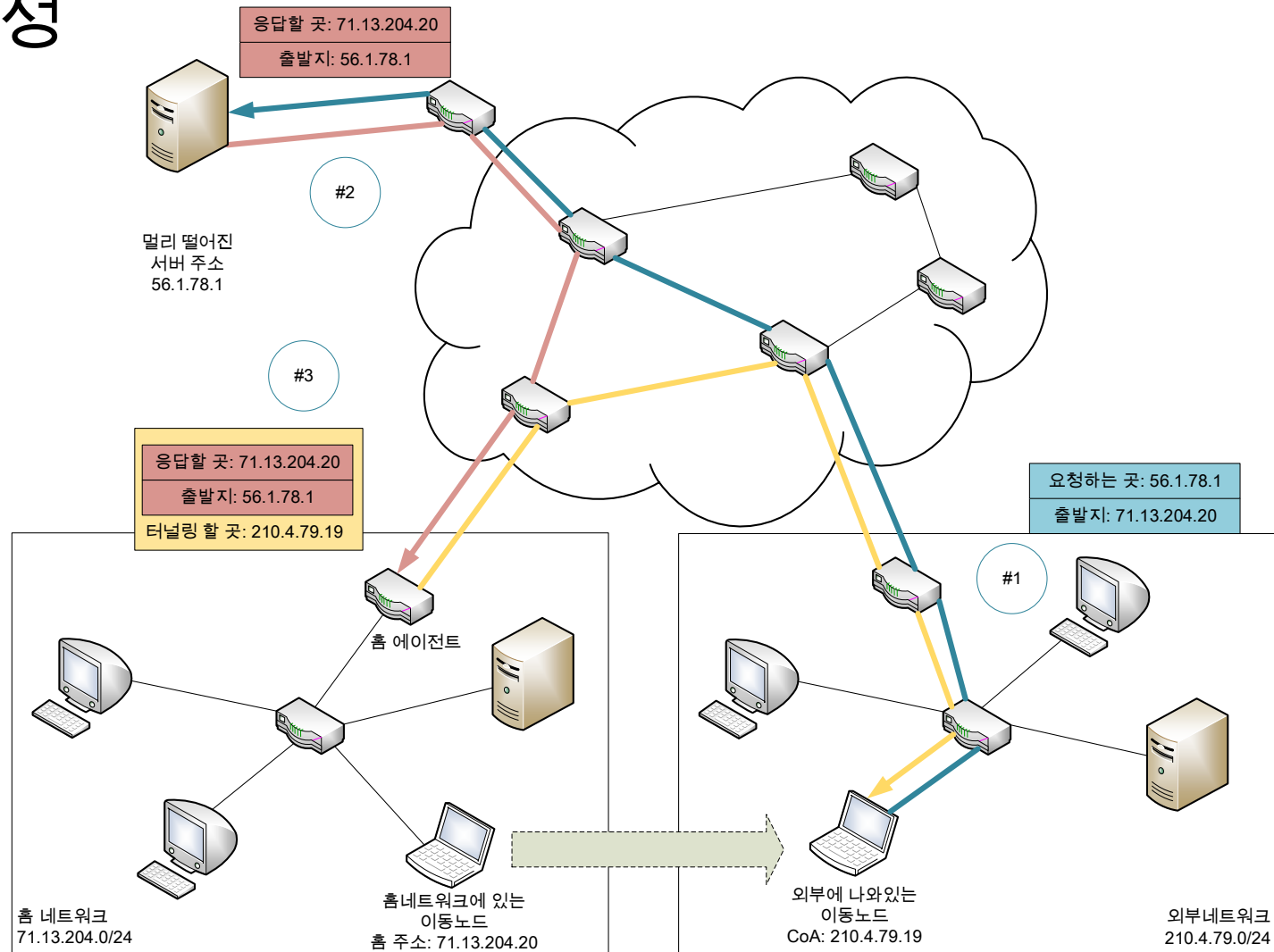
- 데이터 캡슐화와 터널링

- 터널링 과정

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

모바일 IP

- 데이터 캡슐화와 터널링
- 터널링 동작 과정



모바일 IP

- 데이터 캡슐화와 터널링

- 역 터널링

- 특정한 보안이 있는 네트워크로 이동해 자신의 원래 IP주소로 전송 하지 못하는 경우 사용
- 총 4번의 과정이 필요하기 때문에 비효율적
- 이동 장비, 홈 에이전트와 외부 에이전트에 역터널링이 구현되어 있어야 함
- 모든 전송은 홈 에이전트를 통해 전송, 이동 장비는 데이터를 직접 전송 하지 않음

모바일 IP

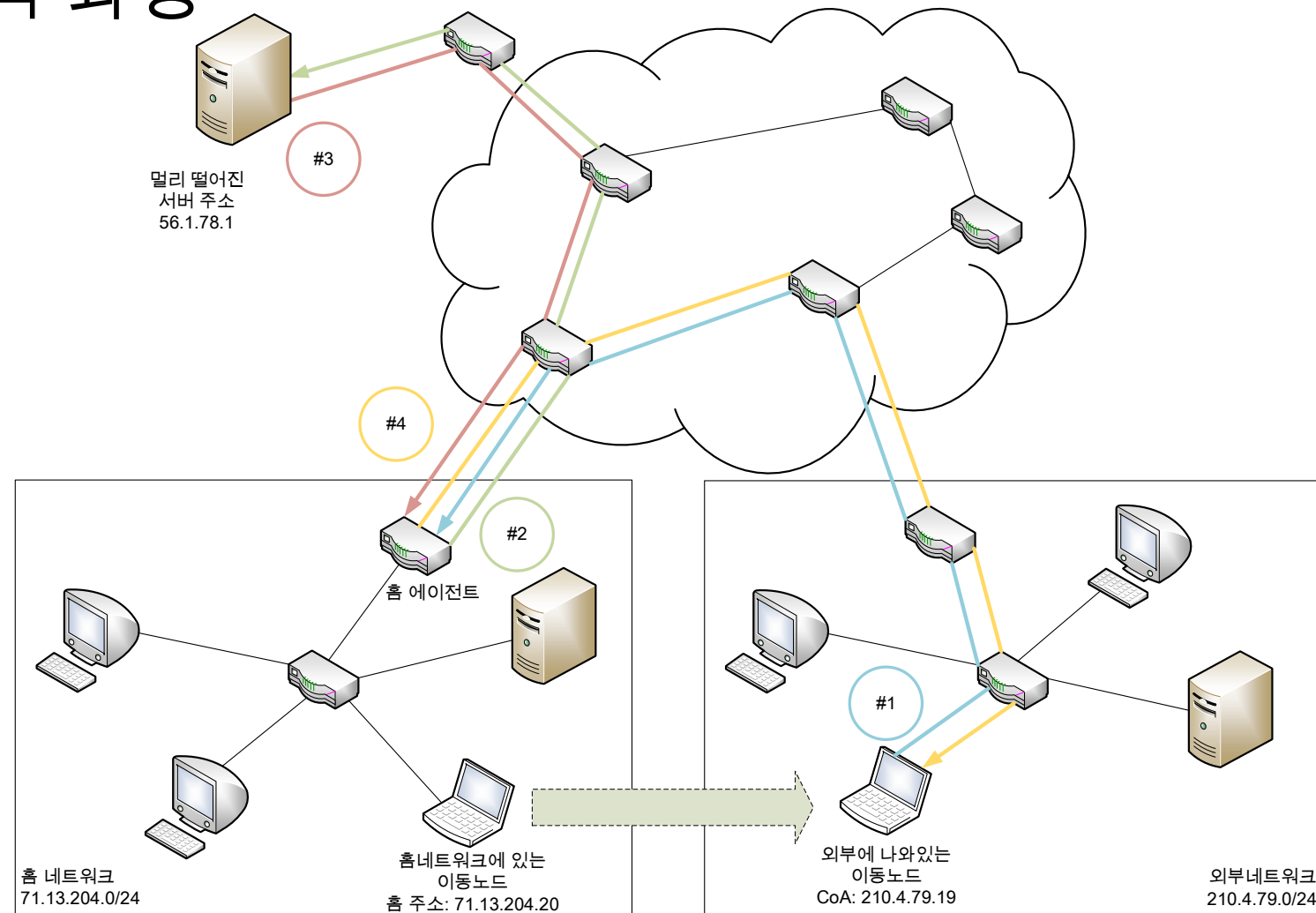
- 데이터 캡슐화와 터널링

- 역 터널링 과정

1. 이동 장비가 전송할 데이터그램을 홈 에이전트에게 전송
2. 홈 에이전트가 대신 멀리 떨어져 있는 서버로 데이터그램 전송
3. 떨어져 있는 서버는 홈 에이전트로 응답 메시지 전송
4. 홈 에이전트는 이동 장비에게 데이터그램 전달

모바일 IP

- 데이터 캡슐화와 터널링
- 역 터널링 동작 과정



모바일 IP

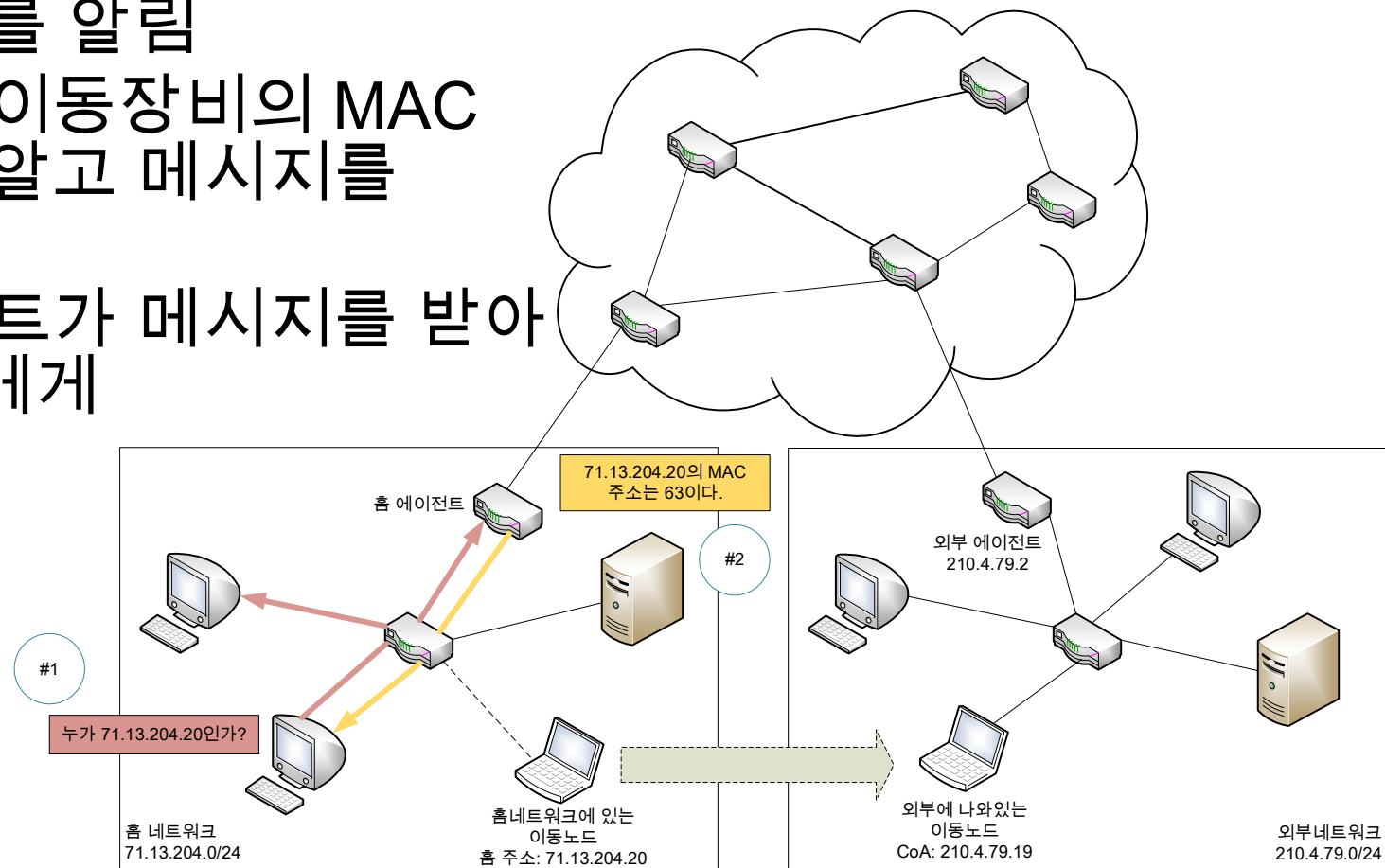
- 모바일 IP와 TCP/IP 주소 결정 프로토콜
 - IP 동작을 수정 했기 때문에 문제가 생할 수 있음
 - ARP(주소 결정 프로토콜)을 이용해 로컬 네트워크 안에 다른 호스트가 이동한 노드에게 데이터 링크 계층 주소로 데이터를 보내고자 할 경우
- ARP 문제를 해결하기 위해 두 가지 추가적인 작업이 필요
 - ARP 포록싱 (ARP 캐시가 없는 경우)
 - 무상 ARP (ARP 캐시가 있는 경우)

모바일 IP

- 모바일 IP와 TCP/IP 주소 결정 프로토콜

- ARP 프록싱 (ARP 캐시가 없는 경우)

1. 홈 에이전트가 ARP요청시 자신의 MAC주소를 알림
2. 호스트는 이동장비의 MAC 주소인줄 알고 메시지를 전송
3. 홈 에이전트가 메시지를 받아 이동장비에게 전달

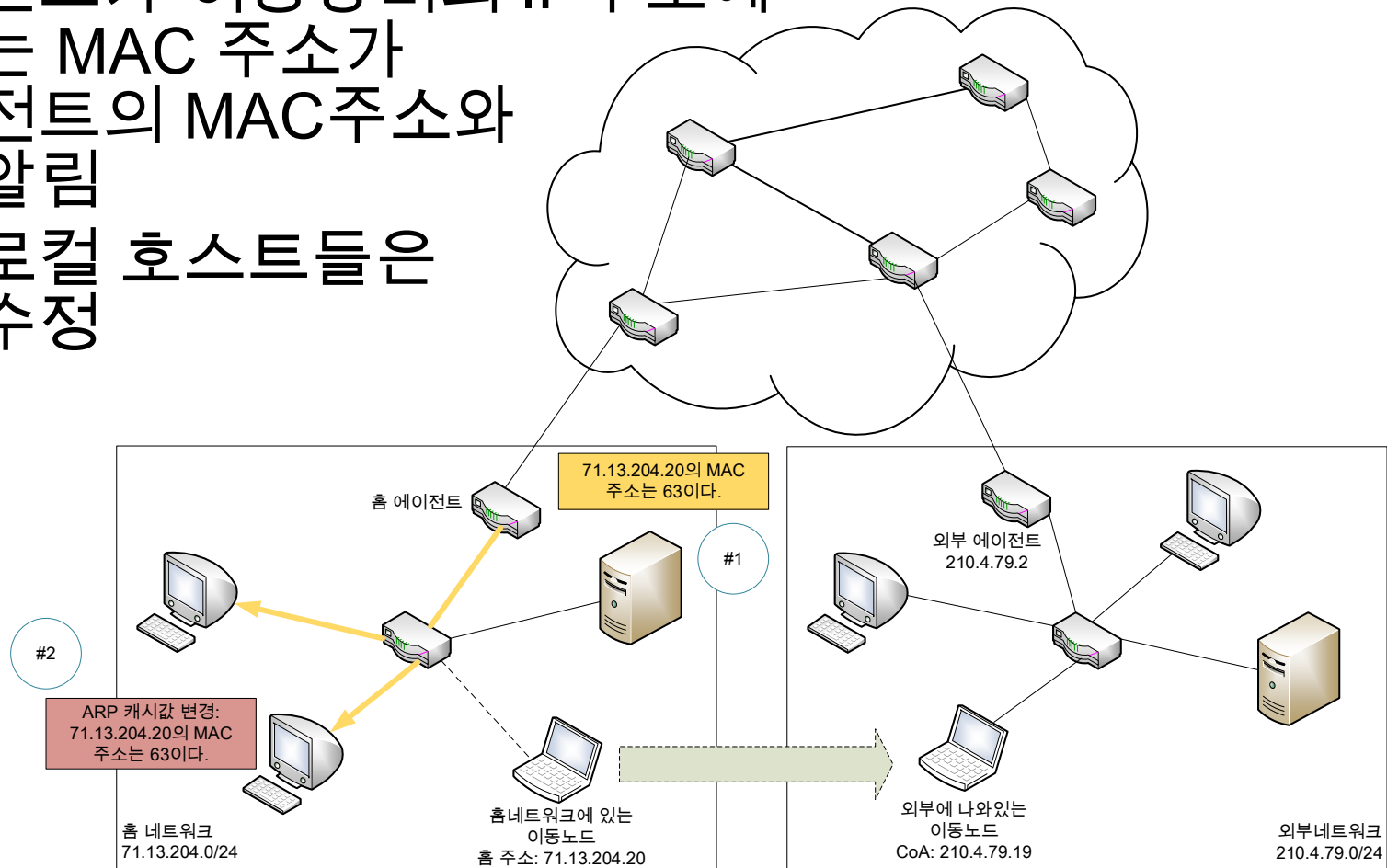


모바일 IP

- 모바일 IP와 TCP/IP 주소 결정 프로토콜

- 무상 ARP (ARP 캐시를 가진 경우)

1. 홈 에이전트가 이동장비의 IP주소에 대응 하는 MAC 주소가 홈 에이전트의 MAC주소와 같다고 알림
2. 각각의 로컬 호스트들은 캐시를 수정



모바일 IP

- 모바일 IP 효율

- 전송자가 이동 장비의 네트워크에서 얼마나 떨어져 있는가에 따라 비효율 정도가 결정됨
 - 이동한 장비와 메시지를 보내는 장비가 같은 로컬 네트워크인 경우 효율성이 떨어짐
- 외부 네트워크에 오래 머무르거나 효율이 중요한 애플리케이션의 경우 모바일 IP를 사용하지 않음

모바일 IP

- 모바일 IP 보안 문제

- 주로 무선 통신으로 이용되기 때문에 보안에 취약
 - 전송 자체가 공개 되어 있음
- 등록 요청과 등록 과정에서 공격 가능
 - 모든 모바일 IP 장비에 인증을 지원 해야 함
- 재전송 공격을 막기 위한 식별 필드가 존재하나 메시지에 대한 인증을 하기 위해서는 IPsec과 함께 사용

Thanks!

박 재 형 (jaehyoung@pel.sejong.ac.kr)