TCP/IP 완벽 가이드

- IP 관련 기능 프로토콜 -

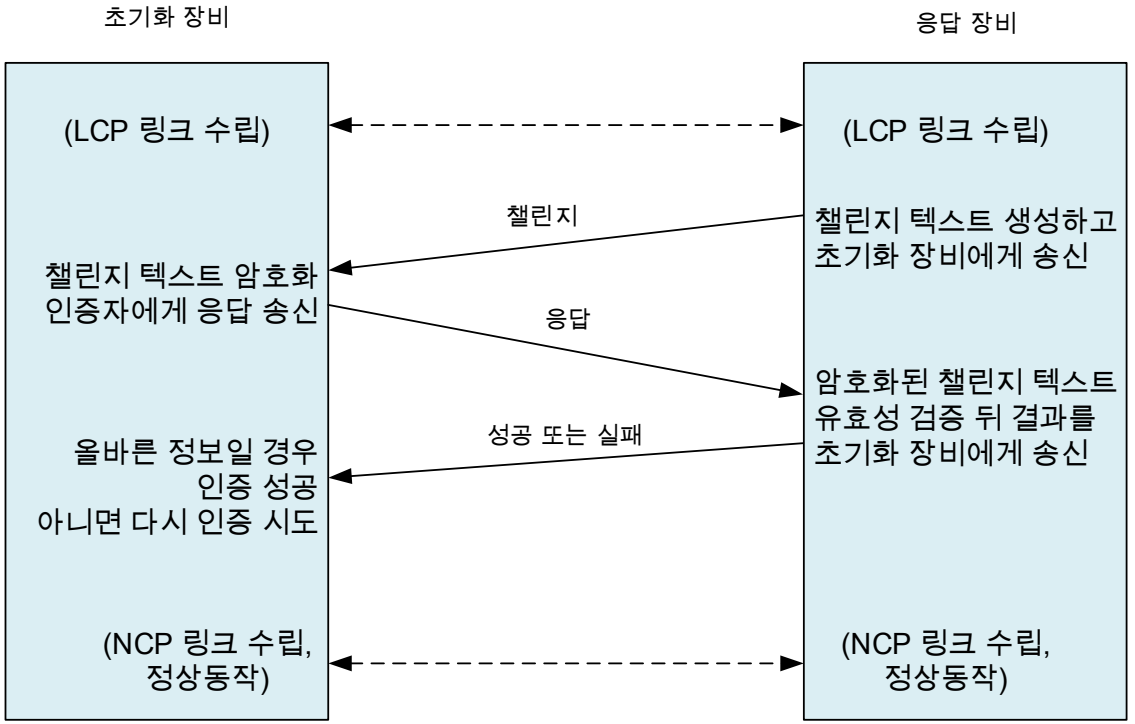
전 상 기(sanggi@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

목 차

보충

- PPP 인증 프로토콜
  - 챌린지 핸드셰이크 인증 프로토콜
    - 쓰리웨이 핸드셰이크 기법
      - 과정



      - 암호화 방법
        - MD5 해쉬를 이용함

IP 네트워크 주소 변환 프로토콜

- IP 네트워크 주소 변환(NAT, Network Address Translation) 개요
  - 등장 배경
    - 주소 공간 고갈
      - 인터넷 이용자가 급격히 증가에 32비트만 주소만으로 부족
    - IP 주소 비용 증가
      - 주소가 희귀해지면서 비용이 증가
    - 보안 우려의 증가
      - 인터넷 사용 증가에 따른 악성 사용자들이 늘어남
  - 등장 가능 이유
    - 대부분의 호스트는 클라이언트 장비
    - 동시에 인터넷에 접근하는 호스트는 많지 않음
    - 인터넷 통신은 라우팅이 됨

IP 네트워크 주소 변환 프로토콜

- IP 네트워크 주소 변환 개요
  - IP NAT의 장점
    - 공인 IP 주소 공유
    - 쉬운 확장
    - 로컬 통제력 강화
    - 인터넷 서비스 제공자(ISP, Internet Service Provider) 선택의 유연성
      - 공인 주소만 바꾸면 되기 때문에 네트워크의 모든 클라이언트 주소를 다시 부여할 필요가 없음
    - 보안 강화
      - 공인 IP 주소를 사용해서 외부 공격자가 클라이언트 장비에 직접 접근이 어려움
    - 투명함
      - 주소 변환이 라우터에서만 일어남

IP 네트워크 주소 변환 프로토콜

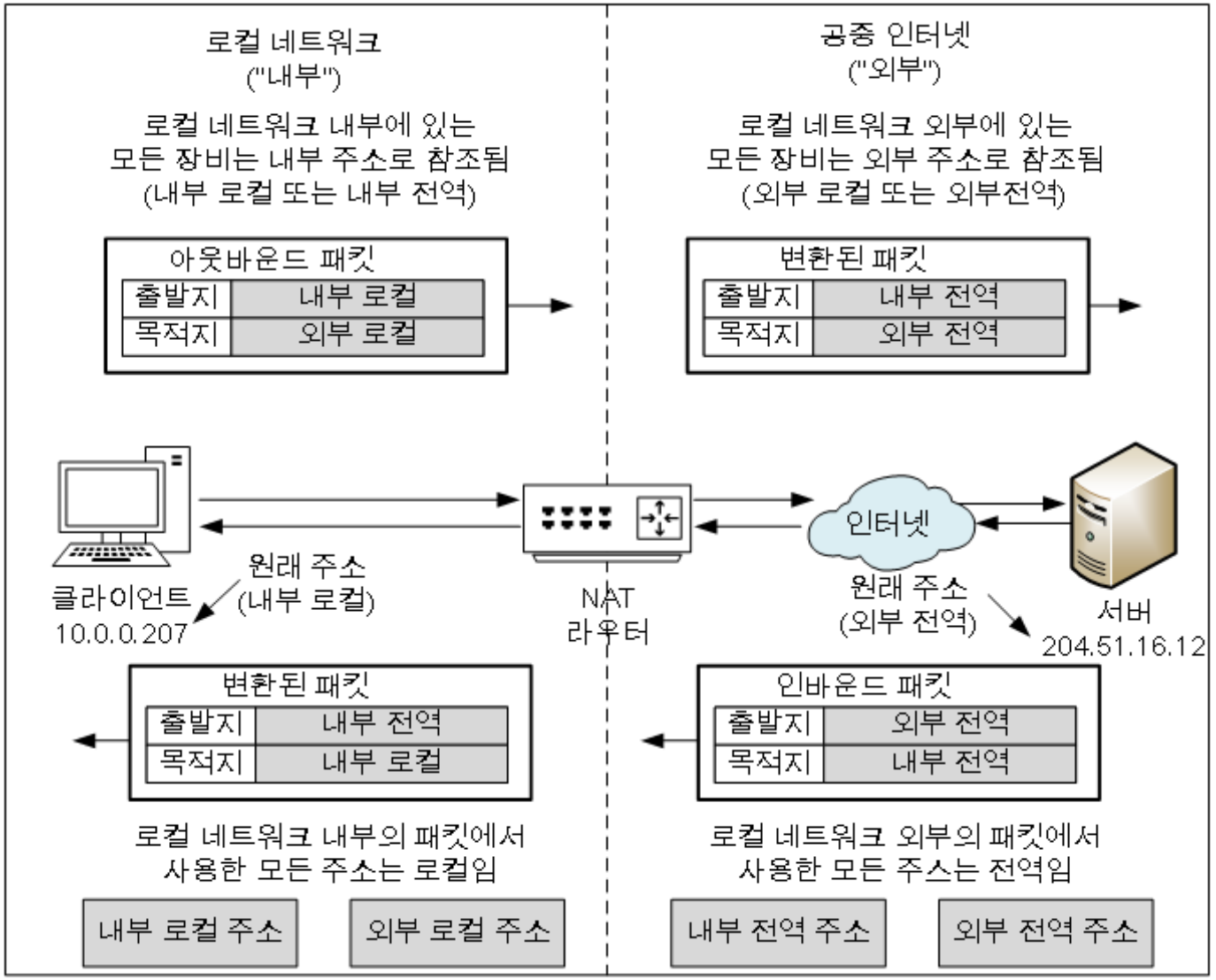
- IP 네트워크 주소 변환 개요
  - IP NAT의 단점
    - 복잡성
    - 공인 주소 부족으로 인한 문제
    - 특정 애플리케이션과의 호환성 문제
      - NAT는 패킷 IP 헤더 필드만을 수정하기 때문
    - 클라이언트 접근 지원 미비
      - 피어투피어 애플리케이션을 설정하는 것이 어려움
    - 성능 감소

IP 네트워크 주소 변환 프로토콜

- IP NAT 주소 용어
  - 내부 로컬 주소(Inside local address)
    - 로컬 네트워크의 장비 주소
  - 내부 전역 주소(Inside global address)
    - 공중 네트워크에서 라우팅 가능한 IP 주소로 내부 장비를 외부 세계에 표현하는 데 쓰임
  - 외부 로컬 주소(Outside local address)
    - 로컬 네트워크에서 참조하는 외부 장비의 주소
  - 외부 전역 주소(Outside global address)
    - 공중 인터넷에서 참조하는 외부 장비의 주소

IP 네트워크 주소 변환 프로토콜

- IP NAT 주소 용어



IP 네트워크 주소 변환 프로토콜

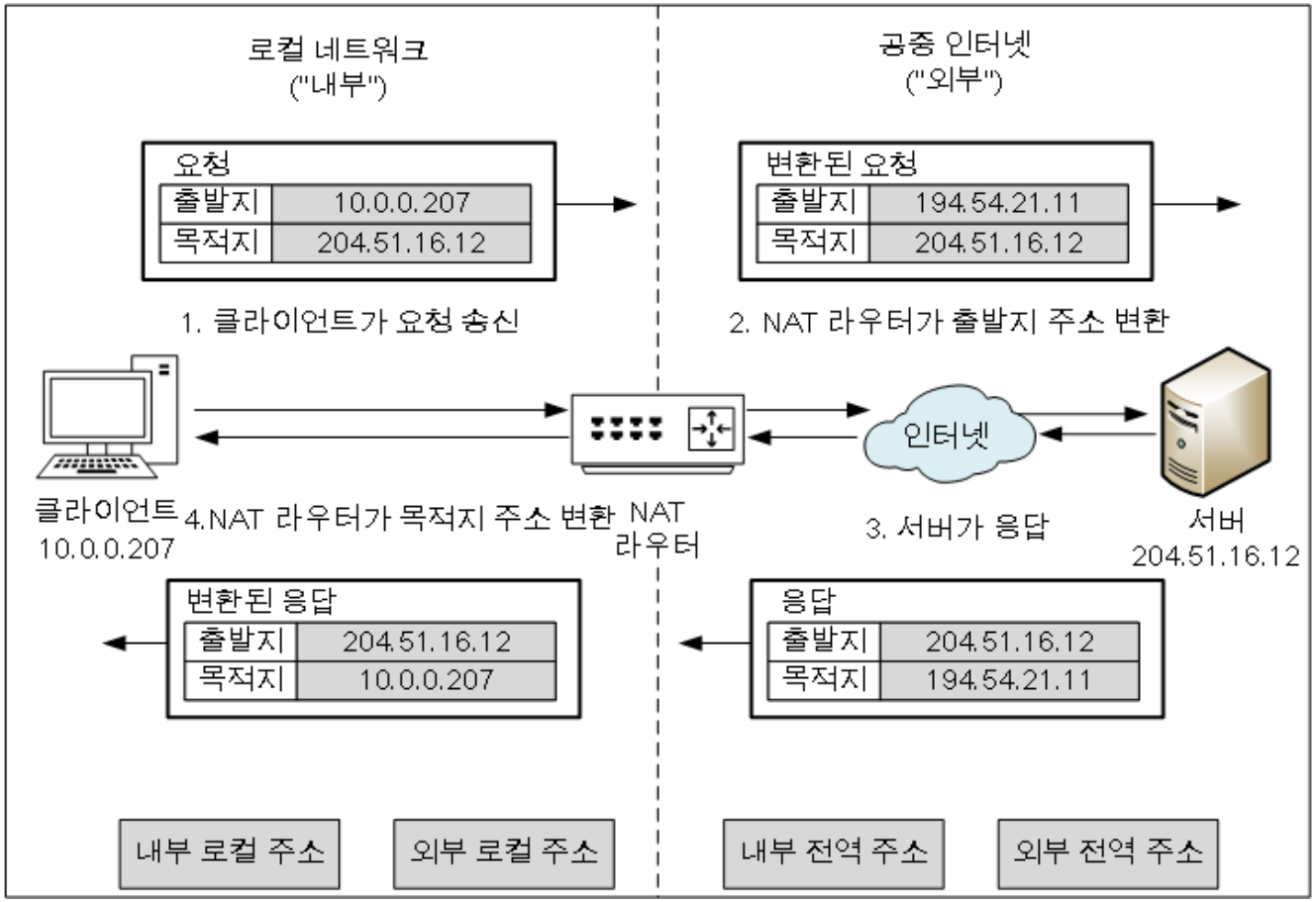
- IP NAT 정적 주소 매핑과 동적 주소 매핑
  - 라우터의 NAT 소프트웨어는 변환 방법을 지시하는 변환 테이블을 관리
    - 변환 테이블은 내부 장비의 내부 로컬 주소를 내부 전역 주소로 매핑하는 정보를 포함
      - 필요한 경우 외부 전역 주소와 외부 로컬 주소간의 매핑 정보로 포함할 수 있음
  - 방법
    - 정적 매핑
      - 내부 또는 외부 장비의 전역 표현과 로컬 표현 사이에 정의된 영구적이고 고정된 관계
      - 외부 네트워크에 항상 동일한 공인 주소로 표현되어야 할 장비에 적합

IP 네트워크 주소 변환 프로토콜

- IP NAT 정적 주소 매핑과 동적 주소 매핑
  - 방법
    - 동적 매핑
      - 전역과 로컬 주소 표현은 NAT 라우터에서 필요할 때마다 생성하며 끝나면 버림
      - 다수의 내부 장비가 내부 전역 주소 풀(Pool)을 이용할 때 쓰임
      - 일반 클라이언트의 공인 IP 주소 공유를 촉진하기 위해 쓰이는 경우가 많음

IP 네트워크 주소 변환 프로토콜

- IP NAT 단반향(전통적/아웃바운드) 동작
- 내부 네트워크 장비가 외부 네트워크 장비로 요청할 경우
  - 동작 과정

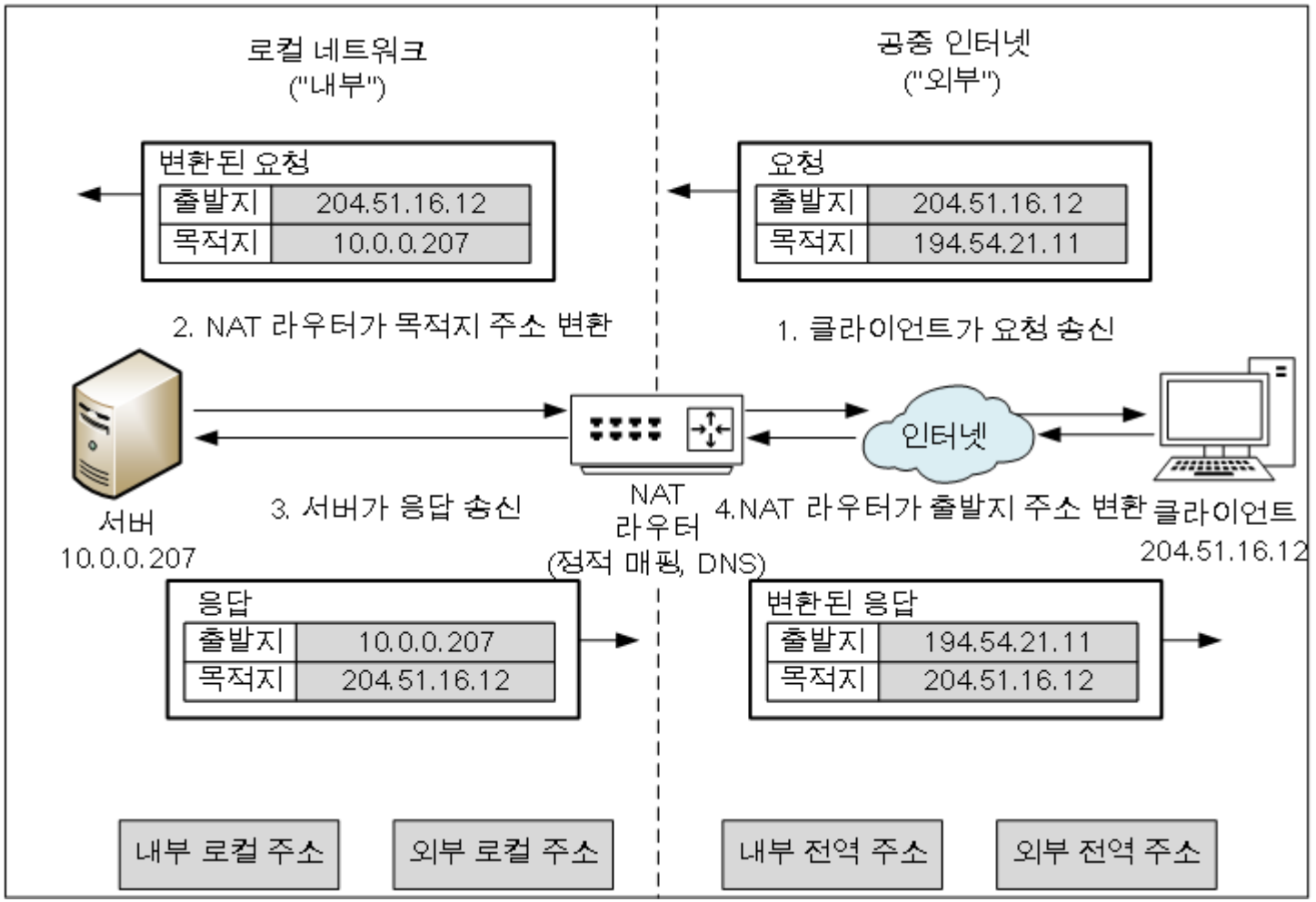


IP 네트워크 주소 변환 프로토콜

- IP NAT 양방향(Two-Way/인바운드) 동작
  - 외부 네트워크 장비가 내부 네트워크 장비로 트랜잭션을 시작하기 원할 수 있음
  - NAT를 사용하는 네트워크가 비대칭 구조이기 때문에 어려움
  - 출발지 장비가 목적지 장비의 NAT 라우터가 무엇인지 모를 경우
    - 정적 매핑과 도메인 네임 시스템(DNS, Domain Name System)을 사용하여 해결 가능

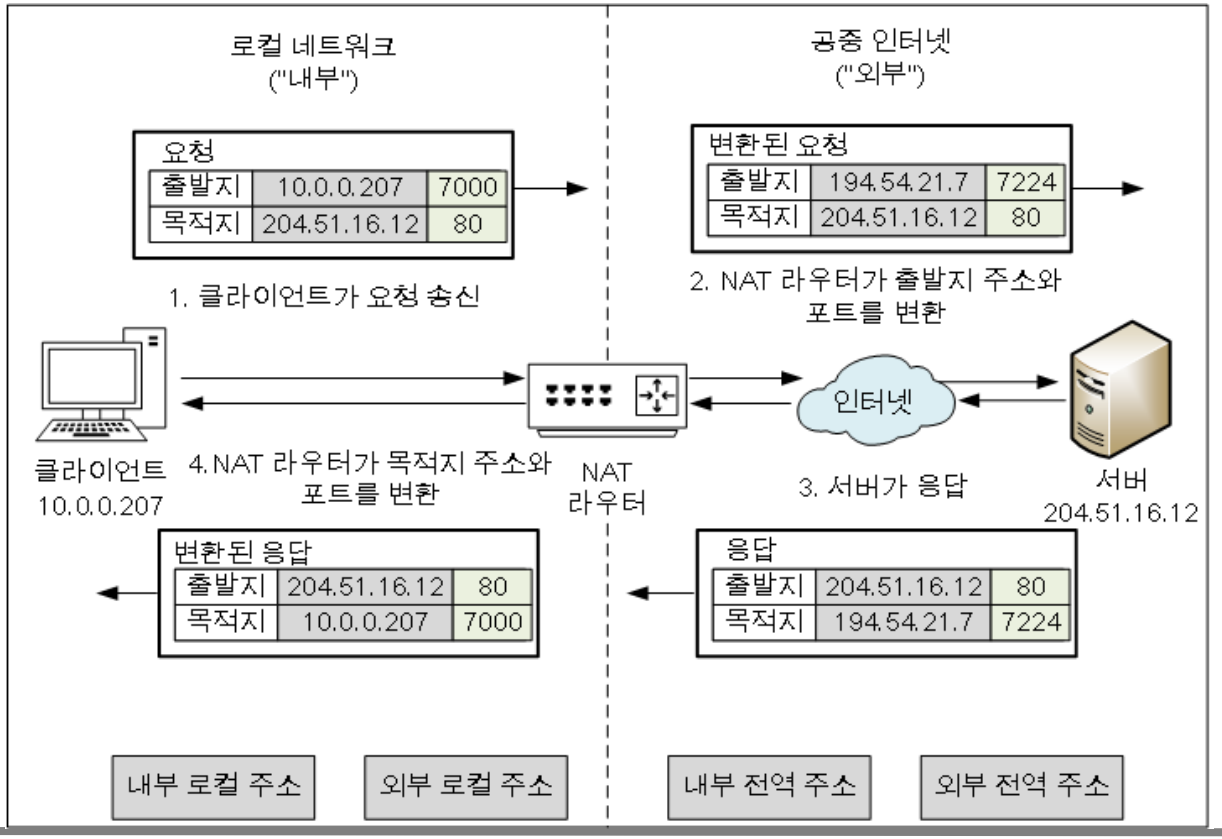
IP 네트워크 주소 변환 프로토콜

- IP NAT 양방향(Two-Way/인바운드) 동작
  - 동작 과정



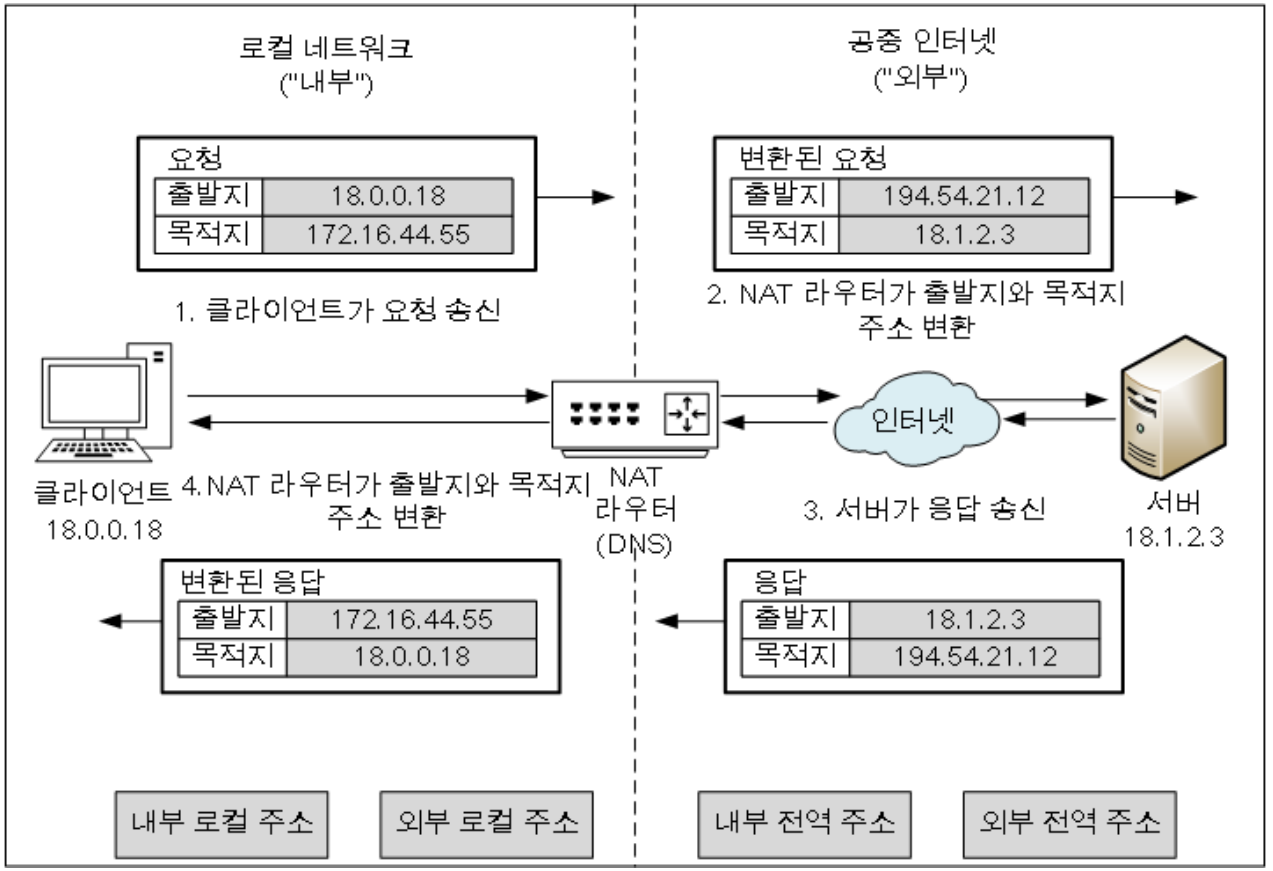
IP 네트워크 주소 변환 프로토콜

- IP NAT 포트 기반(과부하) 동작
  - 포트 번호는 TCP/IP 클라이언트와 서버의 서로 다른 애플리케이션이 간섭 없이 동시에 통신할 수 있도록 함
  - 사용할 수 있는 공인 IP가 가득 차 있는 경우 사용 가능
  - 동작 과정



IP 네트워크 주소 변환 프로토콜

- IP NAT 중복/2회 NAT 동작
  - 내부 네트워크에서 사용하는 주소와 외부 네트워크에서 사용하는 주소가 겹칠 경우
  - DNS에 의존
  - 동작 과정



IP 네트워크 주소 변환 프로토콜

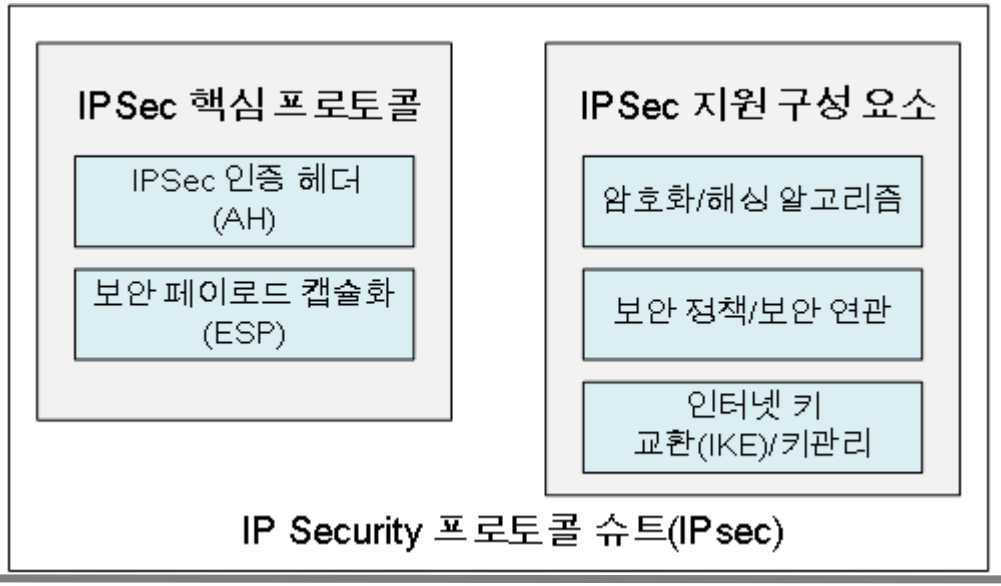
- IP NAT 호환성 문제와 특수 처리
  - 주요 문제와 요구 사항
    - TCP와 UDP 체크섬 재계산
      - 헤더의 IP 주소를 변경하면 IP 헤더의 체크섬을 다시 계산해야 함
    - 인터넷 제어 메시지 프로토콜(ICMP, Internet Control Message Protocol) 조작
      - NAT는 IP 헤더의 주소를 변환하기 때문에 ICMP 메시지를 보고 포함된 헤더의 주소를 변환해야 함
    - IP 주소를 내장하는 애플리케이션
    - 포트 변환에서의 추가적 문제
    - 주소나 포트 번호 변경에 의한 파급 효과
    - IPsec에서의 문제
      - IPsec 전송 모드에서 사용할 수 없음

IPsec 프로토콜

- 개요
  - 등장 배경
    - IP 계층에서 TCP/IP 프로토콜과 애플리케이션의 안전을 보장하는 기능이 없음
  - 장점
    - 프라이버시 보호를 위한 사용자 데이터 암호화
    - 메시지의 무결성을 인증하여 중간에서 변조되지 않았음을 보장
    - 재전송 공격 (Replay attack)으로 부터 보호
    - 장비가 자신의 보안 요구에 맞는 보안 알고리즘과 키를 협상할 수 있도록 함
    - 서로 다른 네트워크 요구를 만족시키기 위한 두 보안 모드
      - 터널(Tunnel) : IP 헤더가 이미 추가된 IP 패킷을 보호하는데 쓰임
      - 전송(Transport) : IPsec 헤더는 IP 페이로드에만 적용 됨

IPsec 프로토콜

- IPsec 일반 동작, 구성 요소, 프로토콜
  - IPsec 핵심 프로토콜
    - IPsec 인증 헤더(AH)
      - IPsec을 위한 인증 서비스를 제공
      - 패킷의 데이터 무결성을 보장
      - 재전송 공격(Replay attack)에 대해 보호
    - 보안 페이로드 캡슐화(ESP)
      - 프라이버시를 보장
  - IPsec 구성 요소



IPsec 프로토콜

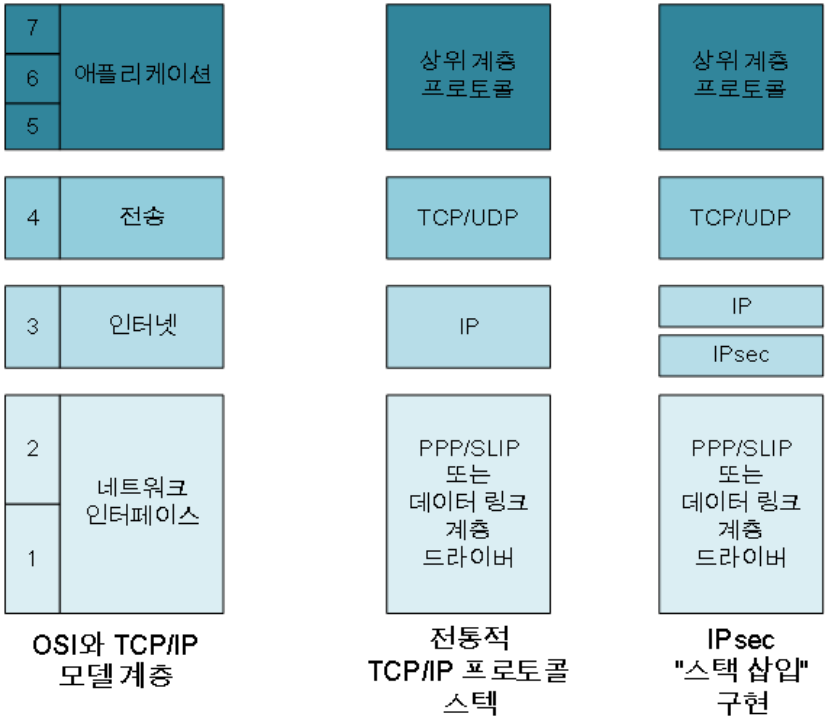
- IPsec 일반 동작, 구성 요소, 프로토콜
  - IPsec 보조 구성 요소
    - 암호화/해싱 알고리즘
      - 3DES(Triple Data Encrytion Standard)
      - AES(Advanced Encryption Standard)
      - MD5(Message Digest 5)
      - SHA-1(Secure Hash Algorithm 1)
    - 보안 정책, 보안 연관, 관리 방법
    - 키 교환 프레임워크와 방법
      - 키 공유, 보안 연관 정보를 교환하기 위한 방법
        - 인터넷 키 교환(IKE, Internet Key Exchange)를 제공

IPsec 프로토콜

- IPsec 구조와 구현 방법
  - 구현 방법
    - 종단 호스트 구현
      - 모든 호스트 장비에 설치하면 유연성과 보안성을 가장 높일 수 있음
      - 네트워크의 모든 두 장비 사이에 보안을 구현 가능
      - 전송모드와 통합구조에 적용
    - 라우터 구현
      - 구현한 라우터 쌍 사이만 보호
      - 로컬 호스트 사이의 연결은 보호되지 않음
      - 터널모드와 스택 삽입 구조, 라인 삽입 구조에 적용

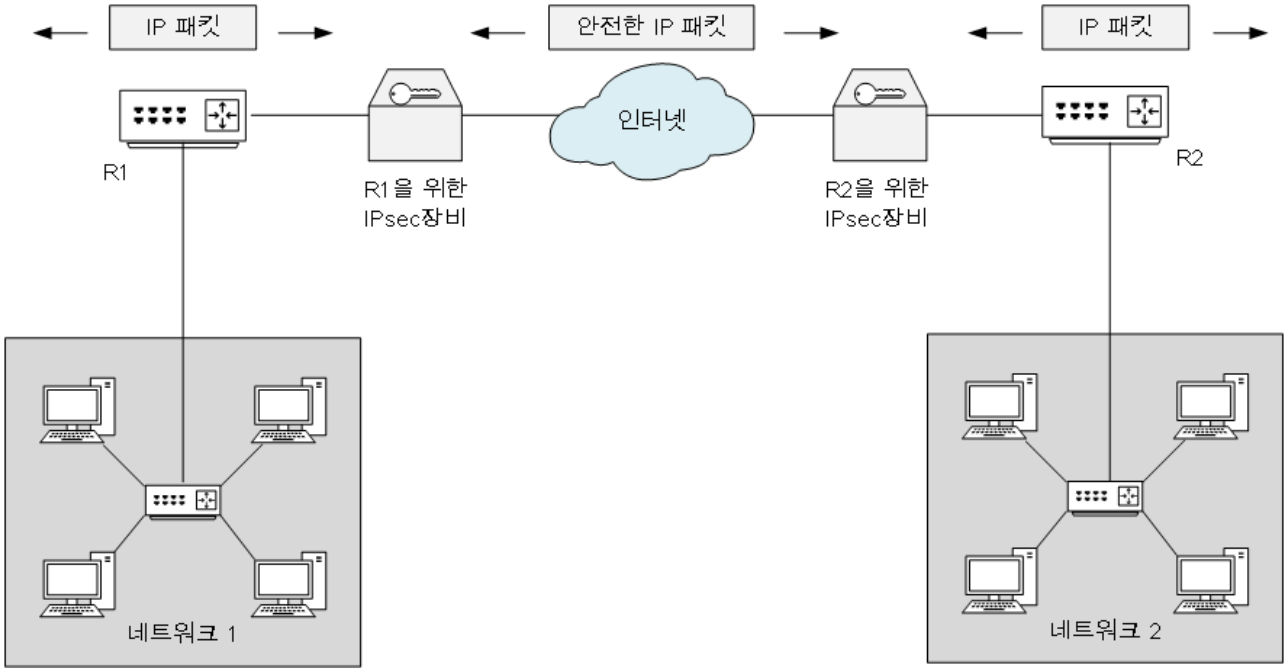
IPsec 프로토콜

- IPsec 구조와 구현 방법
  - 구조
    - 통합 구조
      - IPsec 보안 모드와 기능이 일반 IP처럼 제공
      - 추가 하드웨어나 계층이 필요하지 않음
      - IPv4 경우 IPsec을 통합하려면 각 장비의 IP 구현을 변경해야 함
    - 스택 삽입(BITS, Bump in the stack) 구조
      - IP 패킷이 프로토콜 스택의 아래 방향으로 이동하는 동안 IPsec은 그것을 가로채서 보안 기능을 덧붙임



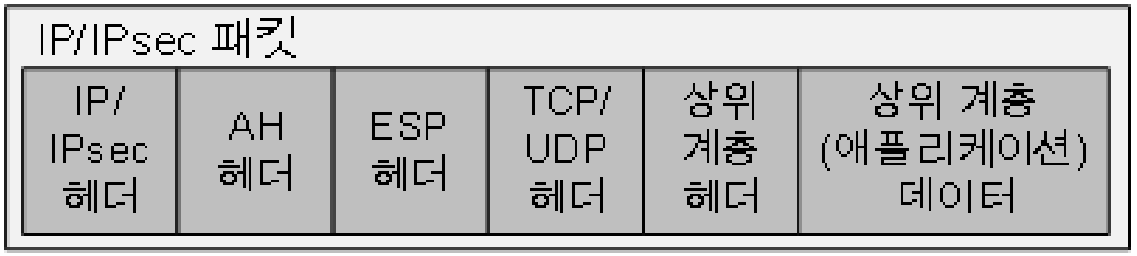
IPsec 프로토콜

- IPsec 구조와 구현 방법
  - 구조
    - 라인 삽입(BITW, Bump in the wire) 구조
      - IPsec 서비스를 제공하는 하드웨어 장비를 추가
        - 이 장비는 외부로 나가는 패킷을 가로채 IPsec 보호 기능을 추가해 송신하고 내부로 들어오는 패킷 IPsec 관련 헤더를 제거



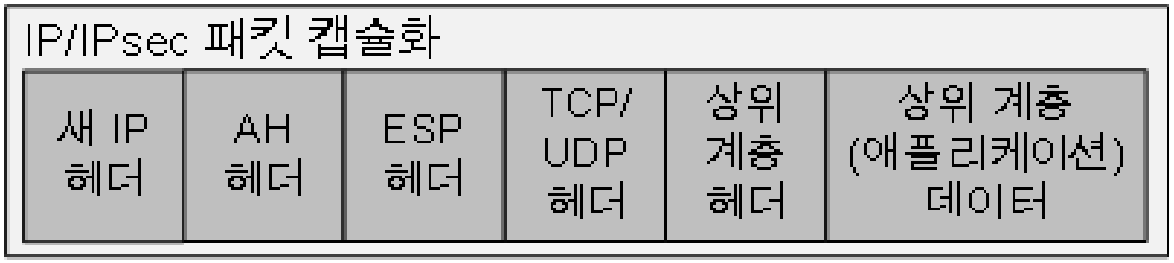
IPsec 프로토콜

- IPsec 모드
  - 개요
    - IP 패킷의 보호 되는 부분과 배열에 영향을 줌
    - 보안 연관(SA, Security Associations)을 정의하는 기초로도 쓰임
  - 전송 모드(Transport mode)
    - 전송 계층에서 내려온 메시지를 보호
    - IP 헤더에는 적용되지 않고 IP 페이로드에만 적용



IPsec 프로토콜

- IPsec 모드
  - 터널 모드(Tunnel mode)
    - IP 헤더가 이미 추가되어 캡슐화된 IP 패킷을 보호하는데 쓰임
    - 원본 IP 패킷이 또 다른 IP 패킷 안으로 캡슐화 됨



IPsec 프로토콜

- IPsec 보안 구성 요소
  - 보안 정책 (SP, Security Policy)
    - 장비가 수신하는 서로 다른 패킷을 어떻게 처리할지 지시함
    - 보안 정책은 보안 정책 데이터베이스(SPD, Security Policy Database)에 저장
  - 보안 연관(SA, Security Association)
    - 장비 사이에 맺은 보안 연결을 설명하는 보안 정보
    - 보안 연관은 보안 연관 데이터베이스(SAD, Security Association Database)에 포함
  - 선택자(Selector)
    - SA가 적용될 패킷을 선택하기 위한 규칙 모음

IPsec 프로토콜

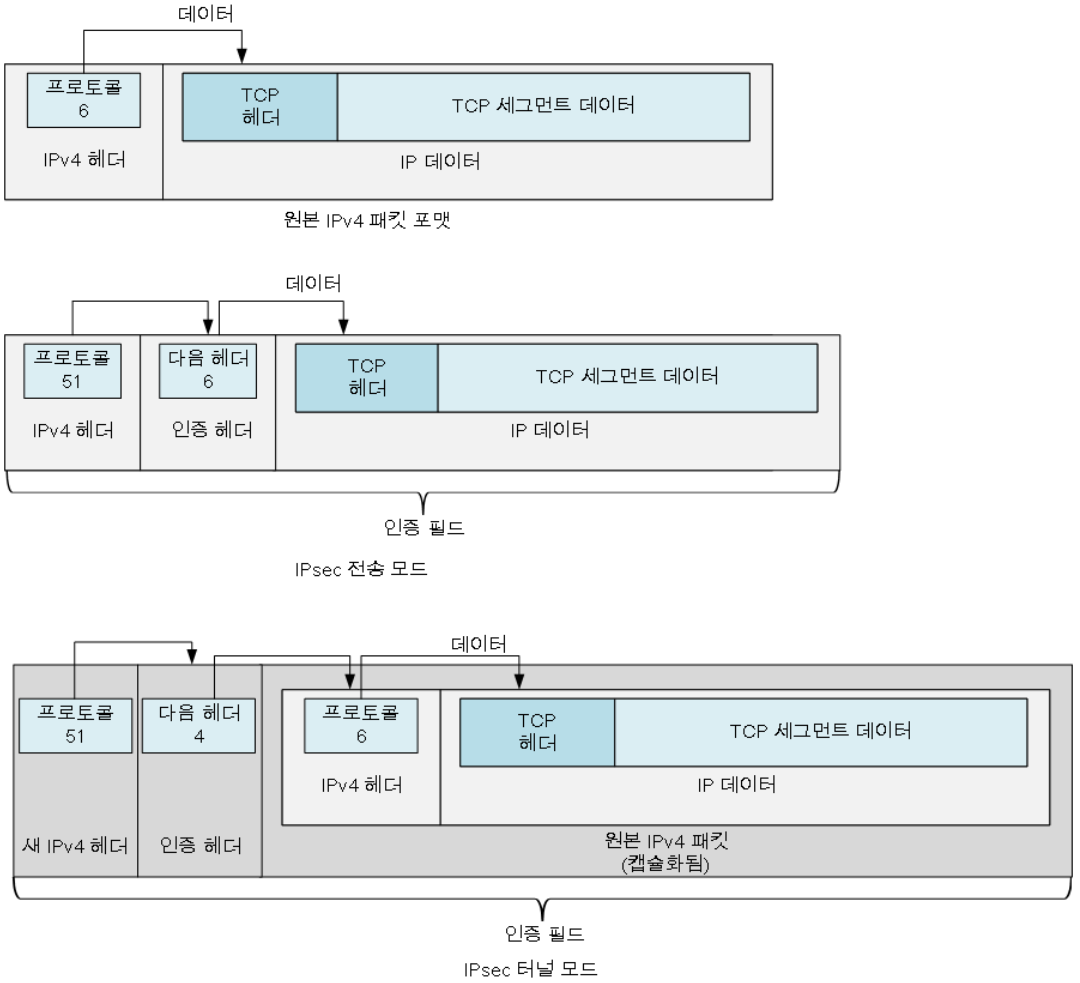
- IPsec 보안 구성 요소
  - 보안 연관 트리플과 보안 인자 색인
    - 보안 인자 색인(SPI, Security Parameters Index)
      - SA를 식별하도록 수신자가 선택한 32비트 값
      - 메시지 수신자가 패킷에 어떤 SA가 적용되는지 파악하는데 쓰임
    - IP 목적지 주소
      - SA가 수립된 장비의 주소
    - 보안 프로토콜 식별자
      - AH,ESP 보안 연관 식별
      - 둘 다 사용시 각각 별도의 SA를 이용

IPsec 프로토콜

- IPsec 인증 헤더(AH, Authentication Header)
  - 개요
    - 패킷 값에 근거하여 계산되는 헤더를 추가하여 패킷 전체 또는 일부분에 대해 인증을 제공
      - 패킷의 부분과 헤더의 위치는 IPsec 모드와 버전에 따라 달라짐
    - 특수 해싱 알고리즘 사용
      - MD5, SHA-1
    - 계산을 수행한 뒤 무결성 검사 값(ICV, Integrity Check Value)을 다른 필드와 합계 특수 헤더에 넣음
    - 재전송 공격에 대한 보호기능 제공

IPsec 프로토콜

- IPsec 인증 헤더
  - AH를 포함하는 패킷 포맷



IPsec 프로토콜

- IPsec 인증 헤더
  - AH 포맷

필드 이름	크기(바이트)	설명
다음 헤더	1	AH 다음에 오는 헤더 프로토콜 번호를 담음
페이로드 길이	1	인증 헤더 자체의 길이(2를 뺀 값)
예약됨	2	쓰이지 않음, 0으로 설정
SPI	4	목적지 주소와 보안 프로토콜 유형과 함께 패킷에 쓰이는 SA를 식별
순서 번호	4	SA 내에서의 패킷을 식별하며 재전송하는 것을 방지
인증 데이터	가변적	무결성 검사 값(ICV)을 포함

IPsec 프로토콜

- IPsec 인증 헤더
  - AH 포맷

IPsec 프로토콜

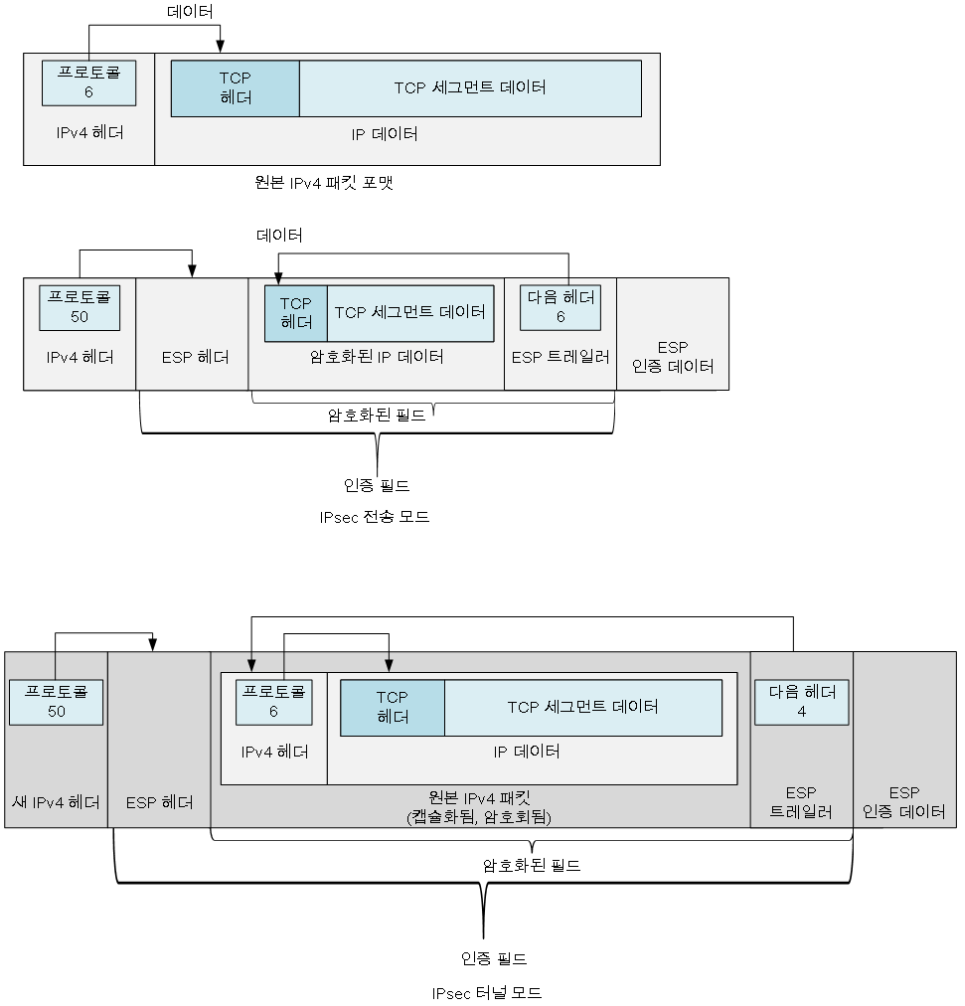
- IPsec 보안 페이로드 캡슐화(ESP, Encapsulating Security Payload)
  - 개요
    - IP 패킷을 암호화하여 프라이버시를 보장
    - 암호화 알고리즘과 키를 사용
    - 인터넷 키 교환(IKE, Internet Key Exchange)로 키를 교환
  - ESP 필드
    - ESP 헤더
      - 모드에 따라 위치가 달라짐
    - ESP 트레일러
      - 패딩과 패딩 길이 필드를 이용해 암호화된 데이터를 32비트 경계에 맞춤
      - ESP의 다음 헤더 필드도 포함

IPsec 프로토콜

- IPsec 보안 페이로드 캡슐화
  - ESP 필드
    - ESP 인증 데이터
      - ICV를 포함
      - ESP의 선택적인 인증 기능이 적용될 때 쓰임

IPsec 프로토콜

- IPsec 보안 페이로드 캡슐화
  - ESP를 사용하는 패킷 포맷



IPsec 프로토콜

- IPsec 인터넷 키 교환(IKE, Internet Key Exchange)
  - 개요
    - IPsec 프로토콜 중 하나
    - IPsec 지원 장비가 SA를 교환하도록 하는 방식으로 동작
  - IKE 동작
    - ISAKMP(Internet Security Association and Key Management Protocol)
      - 두 가지 키 교환 프로토콜의 기능을 결합한 방법
        - Oakley
        - SKEME
      - ISAKMP 단계 1
        - 정보를 어떻게 교환할지에 동의하는 준비 단계
        - ISAKMP 자체를 위한 ISAKMP SA를 생성
      - ISAKMP 단계 2
        - AH와 ESP 프로토콜을 위한 SA 의 인자를 협상

IPsec 프로토콜

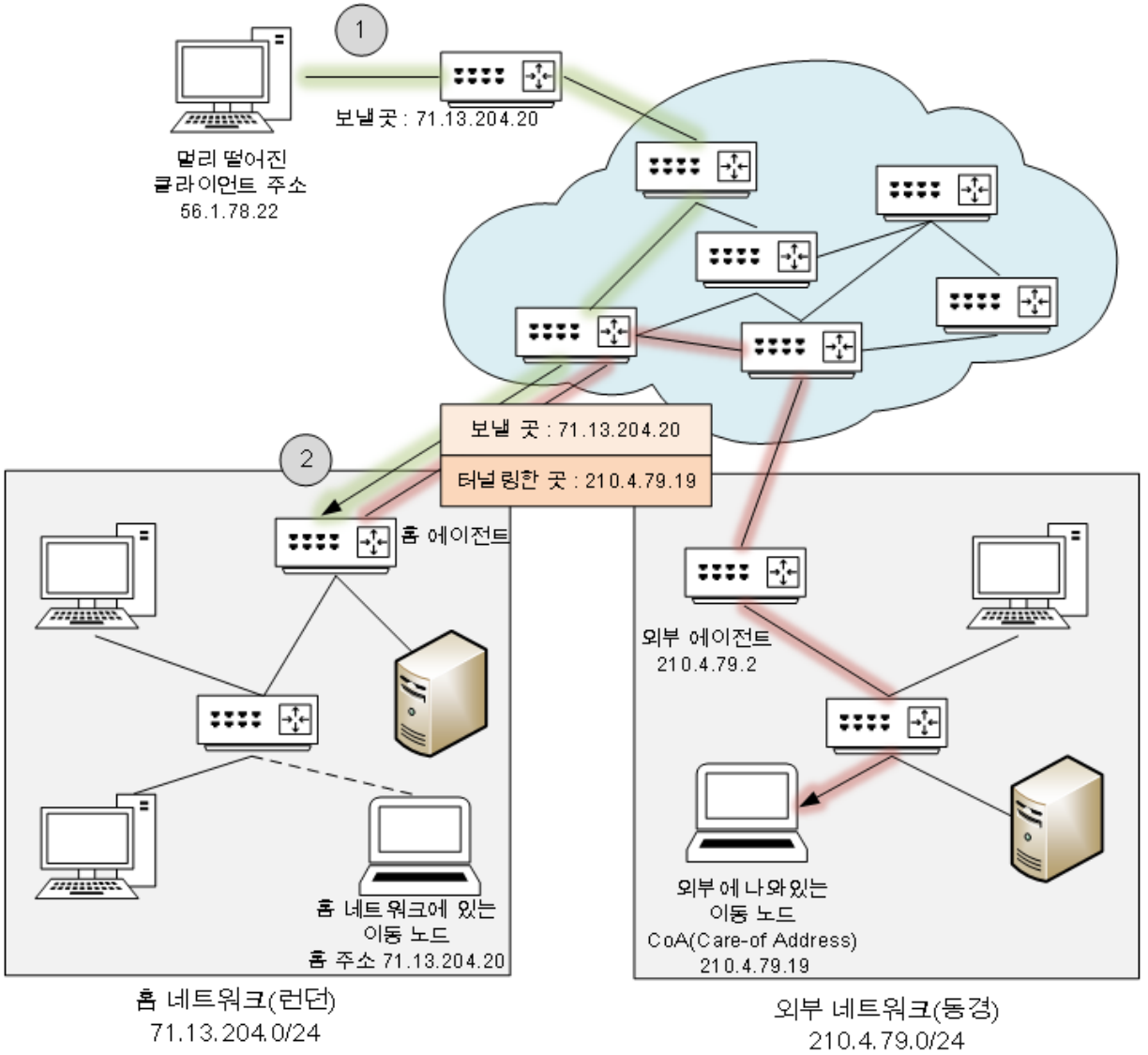
- IPsec 인터넷 키 교환
  - IKE 동작
    - ISAKMP(Internet Security Association and Key Management Protocol)
      - 1단계 ISAKMP SA에 포함되는 속성
        - 암호화 알고리즘
        - 해시 알고리즘
        - 인증 방법
        - 디피-헬만(Diffie-Hellman) 그룹

모바일 IP

- 개요
  - 등장 배경
    - 무선 LAN 기술이 도입되면서 장비들이 움직이면서 통신할 수 있게 됨
    - IP 네트워크는 IP 주소 기반으로 라우팅하기 때문에 이동 장비를 지원할 때 문제가 생김
- 모바일 IP의 한계
  - 무선 환경에서는 한계를 가짐
    - 빠르지 않은 움직임을 목표로 함
  - 고정 IP를 갖는 장비를 대상
    - 장비는 자신의 홈 네트워크와 원래 IP 주소를 알아야 함
      - DHCP(Dynamic Host Configuration Protocol)를 통해 IP를 동적으로 얻는 장비는 사용하기 힘듦

모바일 IP

- 모바일 IP 일반적인 동작 방식



모바일 IP

- 모바일 IP 장비 역할
  - 이동 장비
    - 네트워크 간을 이동하는 장비
  - 홈 에이전트(Home Agent)
    - 홈 네트워크 라우터로 패킷을 대신 받아 이동 장비에게 전달
  - 외부 에이전트(Foreign Agent)
    - 이동 장비가 현재 사용하고 있는 네트워크의 라우터
    - 모바일 IP 동작을 위해 이동 정보를 공유할 수 있음

모바일 IP

- 모바일 IP 기능
  - 에이전트 통신
    - 에이전트가 보내는 광고 메시지를 통해 자신이 어디인지 알아냄
    - 에이전트 광고를 못 들으면 에이전트 요청 메시지를 전송
  - 네트워크 위치 결정
    - 이동 장비는 에이전트 발견 메시지 내용을 기반으로 자신의 위치 판단

모바일 IP

- 모바일 IP 기능
  - 장비가 외부 네트워크에 있을 경우
    - CoA(Care-of-Address) 획득
      - 이동 장비는 CoA라는 임시 주소를 받음
      - 목적지로 패킷을 전달할 때 이외는 사용하지 않음
    - 에이전트 등록
      - 이동 장비는 홈 에이전트에게 자신의 위치를 알리고 패킷을 홈 에이전트가 전달해 달라고 요청
      - 외부 에이전트가 중개자로 개입할 수도 있음
    - 패킷 전달
      - 홈 에이전트가 패킷을 대신 받고 실제 이동 장비의 위치로 전달
      - CoA종류에 따라 직접 전달하거나 외부 에이전트에게 전송을 부탁할 수 있음

모바일 IP

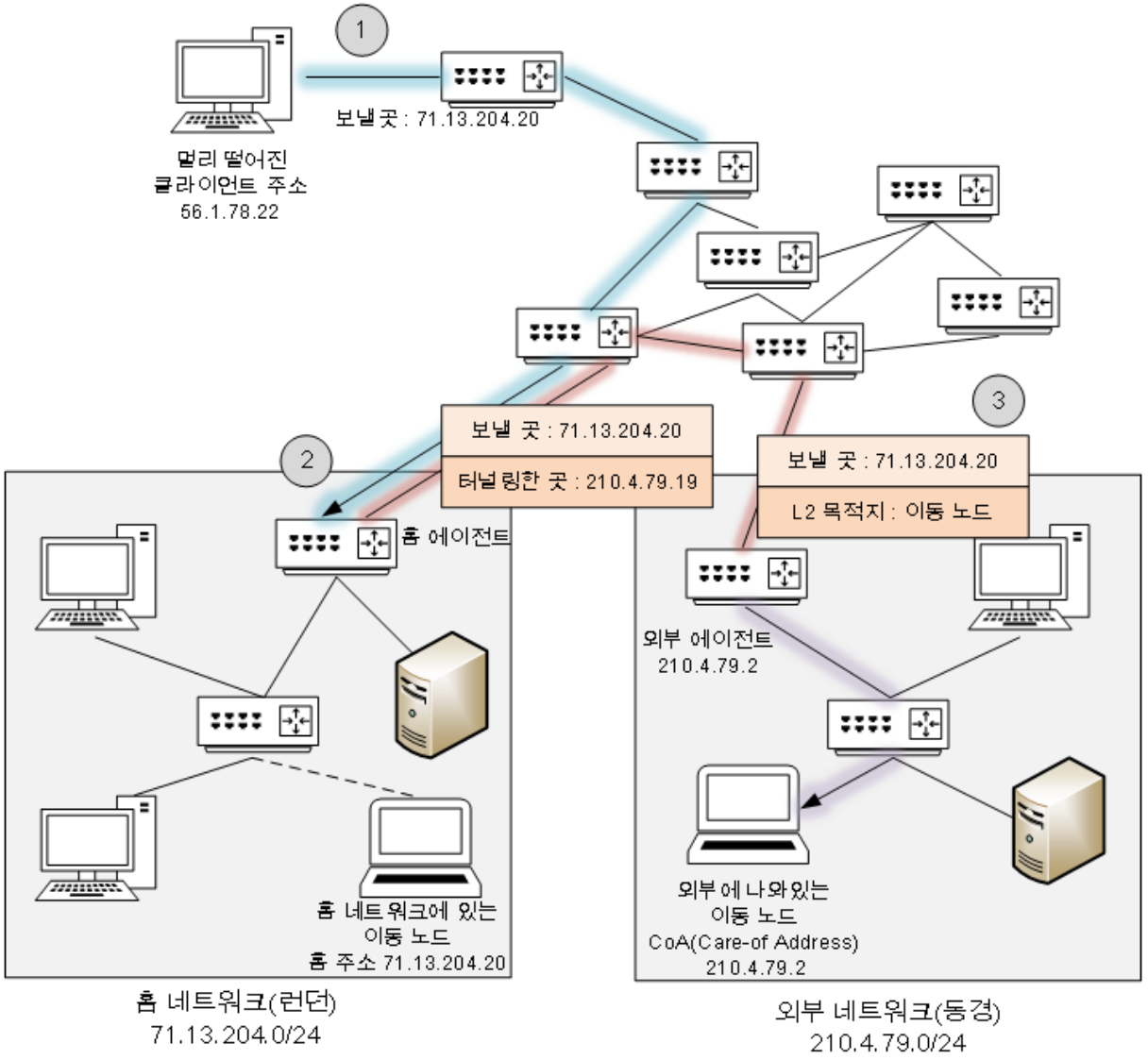
- 홈 주소와 CoA
  - 홈 주소
    - 이동 장비에게 할당된 고정 IP 주소
    - 홈 네트워크에서 장비가 사용하는 주소이고 패킷을 이동 장비에게 보낼 때 사용
  - CoA
    - 이동 장비가 홈 네트워크 외부로 움직였을 때 사용하는 임시 주소
    - 일반적인 32비트 IP 주소와 동일 하지만 모바일 IP에서만 사용

모바일 IP

- 홈 주소와 CoA
  - CoA 유형
    - 외부 에이전트 CoA
      - 이동 장비가 이동한 후 CoA가 외부 에이전트의 주소가 됨
        - CoA는 외부 에이전트가 에이전트 광고 메시지에 실어 보냄
      - 홈 에이전트가 CoA로 전송하면 외부 에이전트가 전달

모바일 IP

- 홈 주소와 CoA
  - CoA 유형
    - 외부 에이전트 CoA
      - 동작 과정

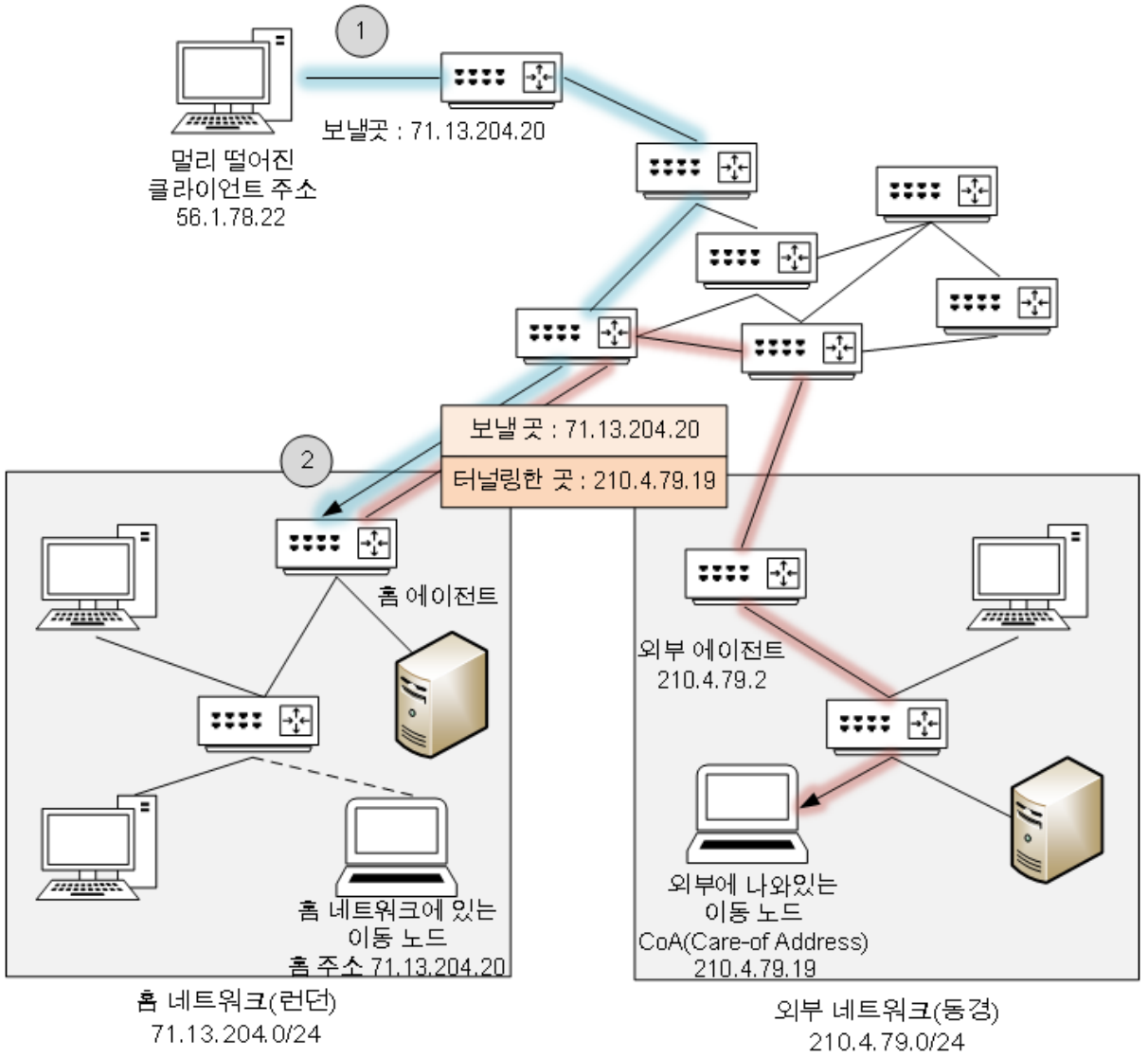


모바일 IP

- 홈 주소와 CoA
  - CoA 유형
    - 공존 CoA
      - 모바일 IP가 아닌 다른 기법을 사용해서 이동 장비에게 직접 할당된 주소
        - 직접 주소를 할당하거나 DHCP를 사용해서 자동으로 할당
      - 공존 CoA를 사용하면 홈 에이전트가 직접 전송할 수 있음

모바일 IP

- 홈 주소와 CoA
  - CoA 유형
    - 공존 CoA
      - 동작 과정



모바일 IP

- 홈 주소와 CoA
  - CoA 유형
    - 유형에 따른 차이
      - 외부 에이전트 CoA
        - 자동화된 주소, 주소 고갈 문제가 없음
      - 공존 CoA
        - 모바일 IP 기능을 가지는 라우터가 없는 네트워크를 지날 때에도 모바일 IP를 사용할 수 있음

모바일 IP

- 모바일 IP 에이전트 발견
  - 에이전트 발견 과정
    - 에이전트/노드 통신
      - 이동 노드가 로컬 네트워크에 있는 에이전트와 접속을 시도하는 방법
      - 에이전트에 대한 정보를 담은 메시지를 노드에 전송, 또는 에이전트에게 정보를 요청
    - 현재 위치 발견
      - 에이전트 발견 과정을 통해 노드는 자신이 어디에 있는지 알 수 있음
    - CoA 할당
      - 외부 에이전트 CoA를 사용하면 에이전트 발견 과정 중 사용할 CoA를 얻음

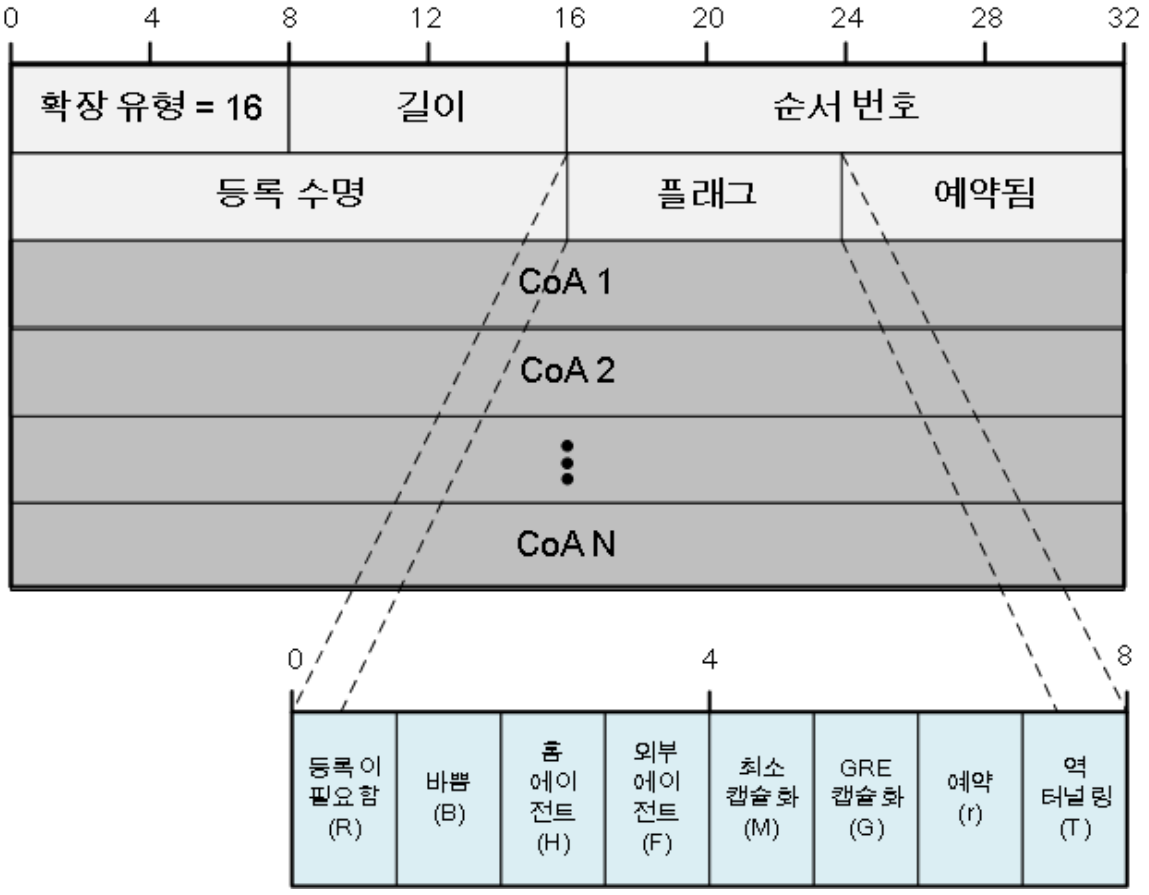
모바일 IP

- 모바일 IP 에이전트 발견
  - 에이전트 광고와 에이전트 요청 메시지
    - 에이전트 광고(Agent advertisement)
      - 이동 에이전트 광고(Mobility Agent Advertisement) 확장
        - 에이전트가 모바일 IP 기능을 갖추었다는 것을 알리는 기본 확장
      - 접두사 길이(Prefix-Length) 확장
        - 라우터 주소의 접두사 길이를 알리는 옵션 확장

      - 1바이트 패딩(One-byte padding)
        - ICMP 메시지 구현을 위해 메시지의 길이를 짝수로 만듦

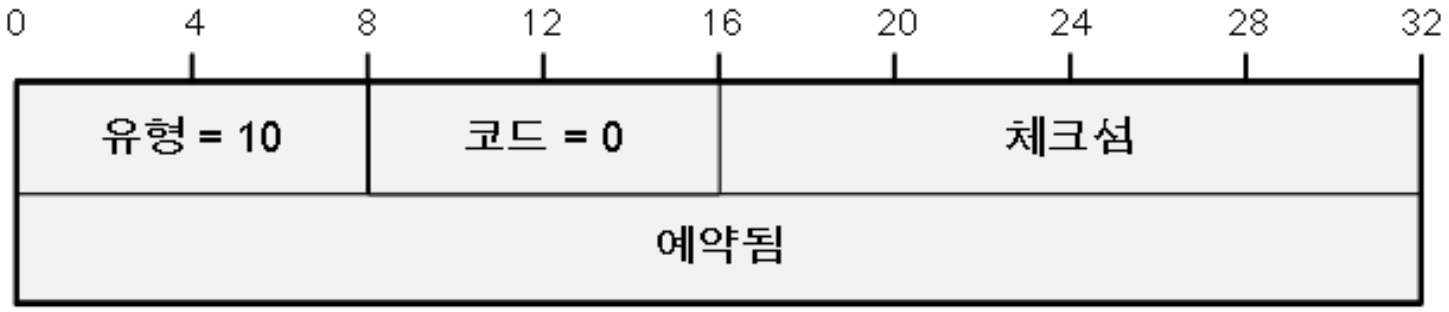
모바일 IP

- 모바일 IP 에이전트 발견
  - 에이전트 광고와 에이전트 요청 메시지
    - 에이전트 광고(Agent advertisement)
      - 메시지 포맷



모바일 IP

- 모바일 IP 에이전트 발견
  - 에이전트 광고와 에이전트 요청 메시지
    - 에이전트 요청(Agent solicitation)
      - 메시지 포맷



모바일 IP

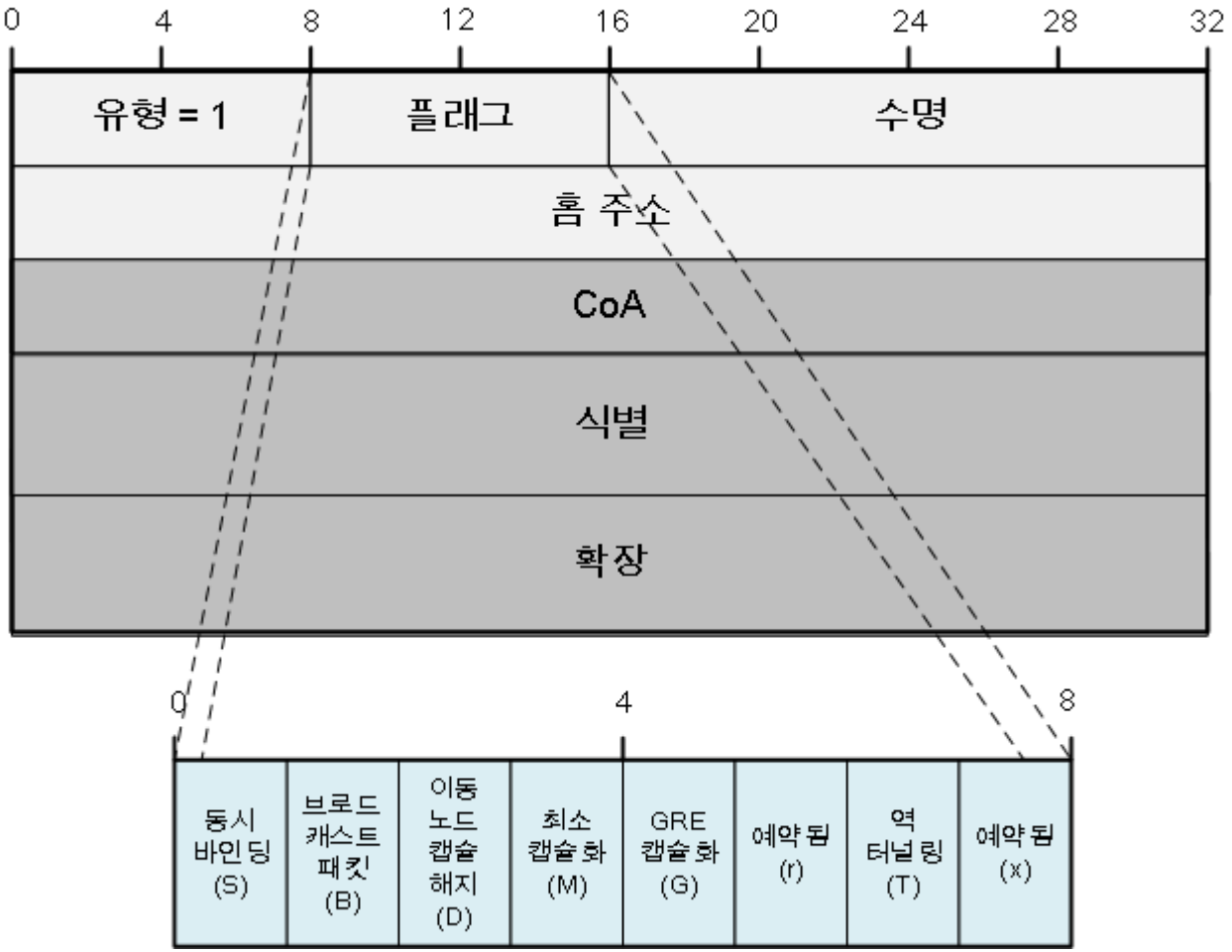
- 모바일 IP 홈 에이전트 등록과 등록 메시지
  - 홈 에이전트 등록(Home agent registration)
    - 홈 에이전트와 통신을 하면서 필요한 정보와 지시를 주고 받는 과정
  - 이동 장비 등록 이벤트
    - 등록 이동
      - 장비가 외부 네트워크에 도착하면 등록을 시작
    - 등록 해제
      - 다시 홈 네트워크로 돌아오면 전달을 취소하는 과정
    - 재등록
      - 다른 외부 네트워크로 이동하거나 CoA가 바뀌면 이동 장비는 홈 에이전트에게 알려 등록을 수정
      - 등록의 기한이 만료되었는데도 여전히 외부 네트워크에 머무르면 재등록

모바일 IP

- 모바일 IP 홈 에이전트 등록과 등록 메시지
  - 등록 요청과 등록 응답 메시지
    - UDP(User Datagram Protocol)를 사용
    - 에이전트는 UDP 434 포트에서 등록 요청을 기다리고 모바일 노드가 사용한 임시 포트로 응답을 돌려 보냄
  - 등록 과정
    - 직접 등록 방식(공존 CoA)
      1. 이동 장비가 등록 요청을 홈 에이전트에게 보냄
      2. 홈 에이전트는 이동 장비에게 등록 응답을 보냄
    - 간접 등록 방식(외부 에이전트 CoA)
      1. 이동 장비가 등록 요청을 외부 에이전트에게 보냄
      2. 외부 에이전트가 등록 요청을 처리하여 홈 에이전트에 보냄
      3. 홈 에이전트는 외부 에이전트에게 등록 응답을 보냄
      4. 외부 에이전트가 등록 응답을 받아 처리하고 이동 장비에게 전송

모바일 IP

- 모바일 IP 홈 에이전트 등록과 등록 메시지
  - 등록 요청 메시지 포맷



모바일 IP

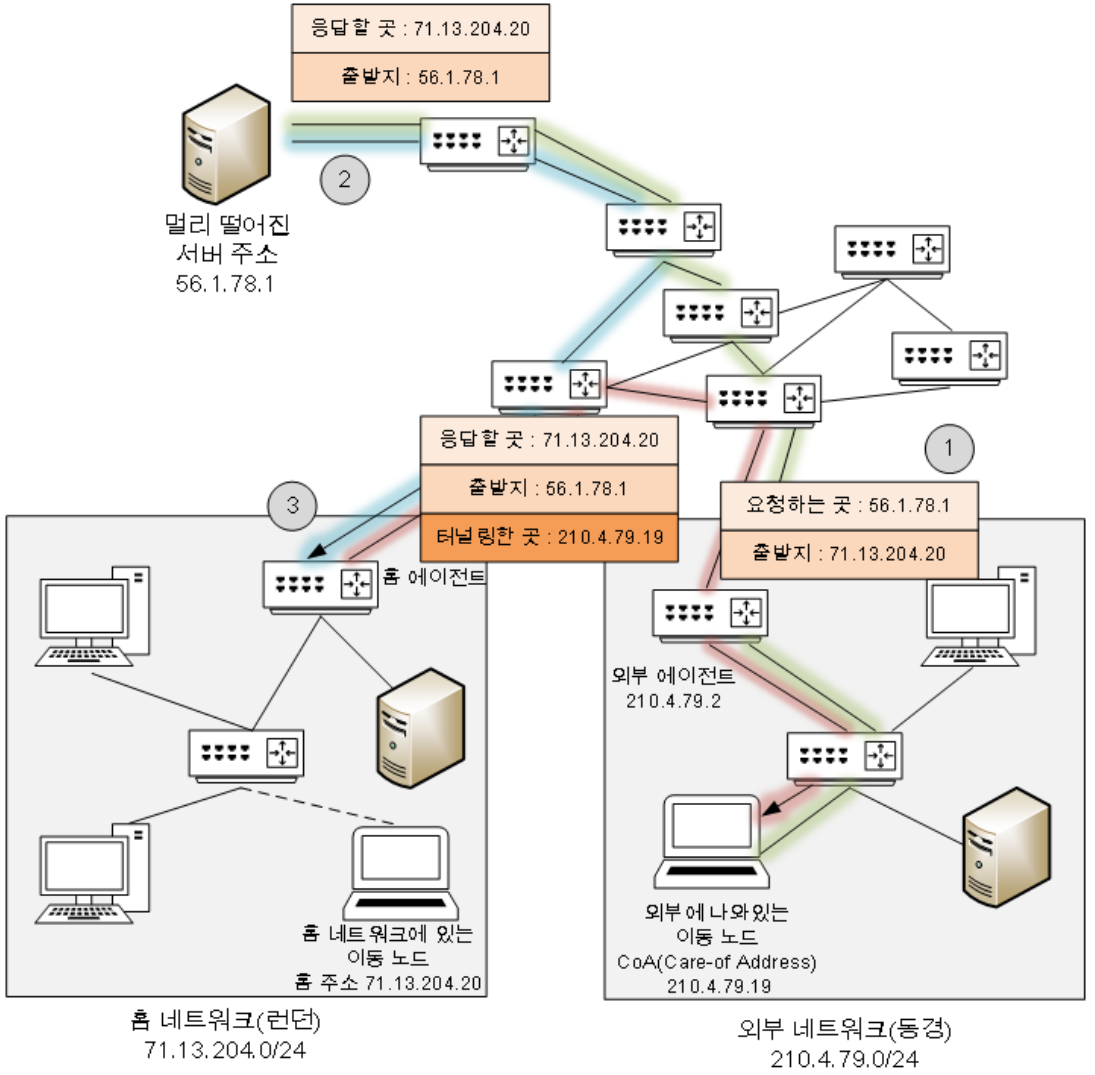
- 모바일 IP 홈 에이전트 등록과 등록 메시지
  - 등록 응답 메시지 포맷

모바일 IP

- 모바일 IP 데이터 캡슐화와 터널링
  - 이동 장비에게 패킷을 전달할 때 캡슐화하여 노드의 CoA로 전송
  - 일반적인 모바일 IP 터널링
    - 외부 에이전트 CoA
      - 외부 에이전트에서 터널이 끝남
      - 캡슐화된 메시지를 홈 에이전트에서 받아 외부 IP 헤더를 벗겨내고 원래 패킷을 이동 장비에게 전달
      - 외부 에이전트는 데이터 링크 계층을 통해 데이터를 이동 장비로 직접 전송
    - 공존 CoA 주소
      - 이동 장비에서 터널이 끝나고 이동 장비가 캡슐화 헤더를 벗김

모바일 IP

- 모바일 IP 데이터 캡슐화와 터널링
  - 동작 과정

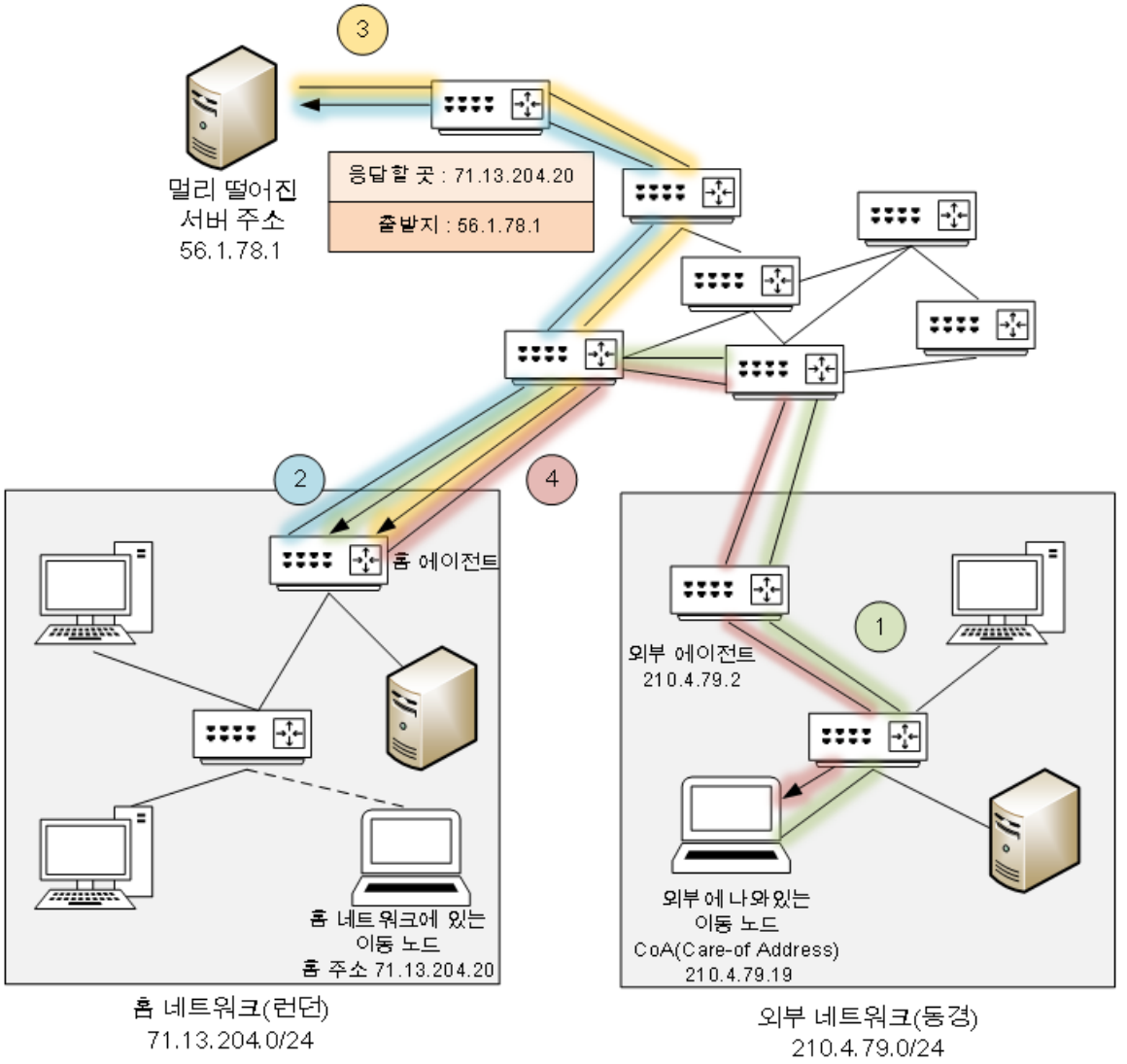


모바일 IP

- 모바일 IP 데이터 캡슐화와 터널링
  - 모바일 IP 역 터널링
    - 이동 장비가 패킷을 직접 인터넷에 전송 할 수 없을 경우 사용
      - 특정한 보안 규칙을 가지고 있는 네트워크에 들어간 경우
    - 총 4번의 과정이 필요하여 비효율적임

모바일 IP

- 모바일 IP 데이터 캡슐화와 터널링
  - 모바일 IP 역 터널링
    - 동작 과정

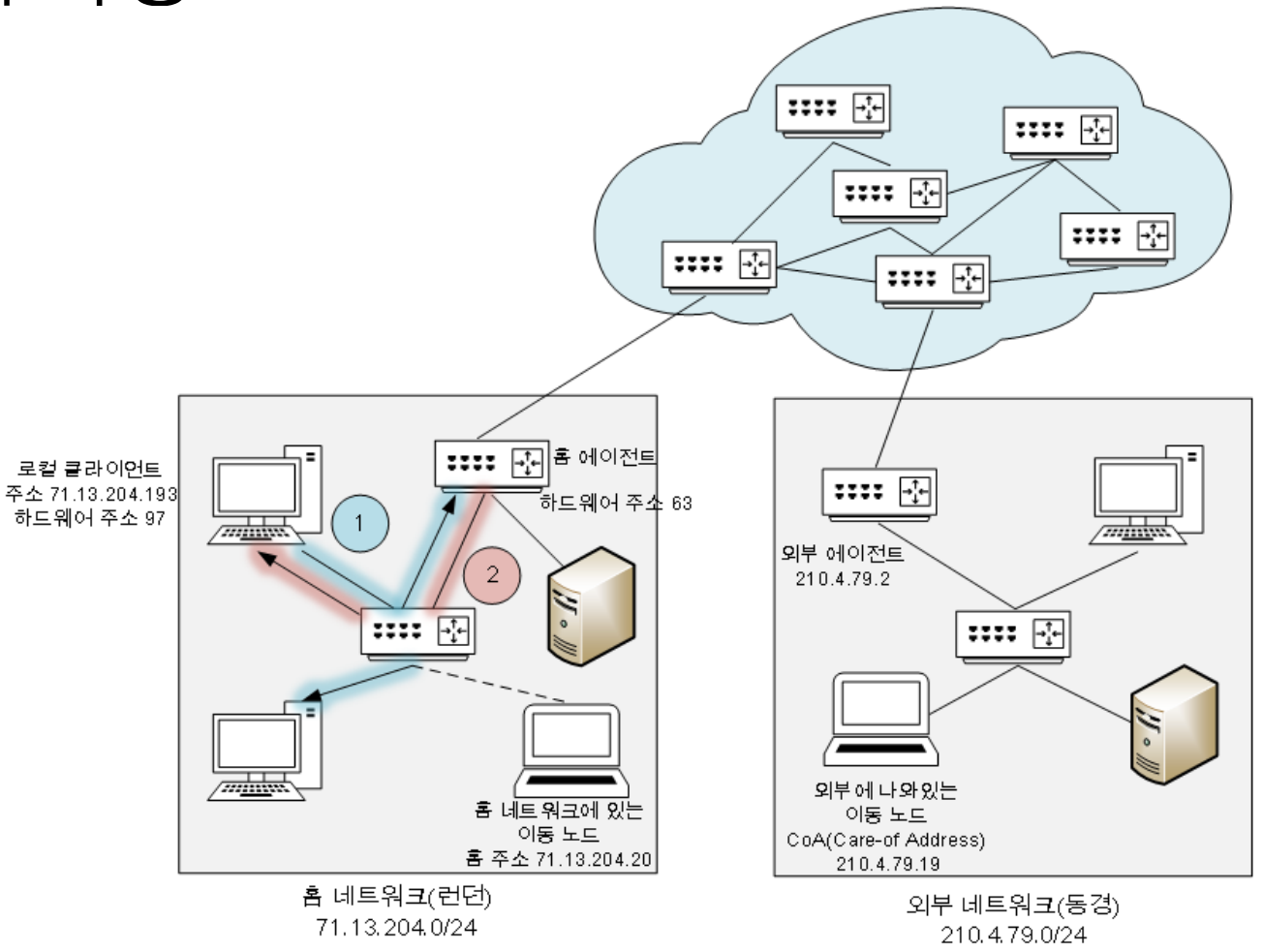


모바일 IP

- 모바일 IP와 TCP/IP 주소 결정 프로토콜
  - ARP를 사용해서 이동 장비의 데이터 링크 계층 주소를 찾아 패킷을 직접 보내려고 할 때 문제
  - ARP 문제 해결을 위한 두 가지 작업
    - ARP 프록싱(ARP proxing)
      - 홈 에이전트가 로컬 호스트 ARP에 응답
      - 홈 에이전트가 메시지를 받아 이동 장비에게 전달
    - 무상 ARP(Gratuitous ARP)
      - 홈 에이전트가 이동 장비의 IP 주소에 대응하는 데이터 링크 주소가 홈 에이전트와 같다고 알림
      - 각각 로컬 호스트들은 캐시를 수정

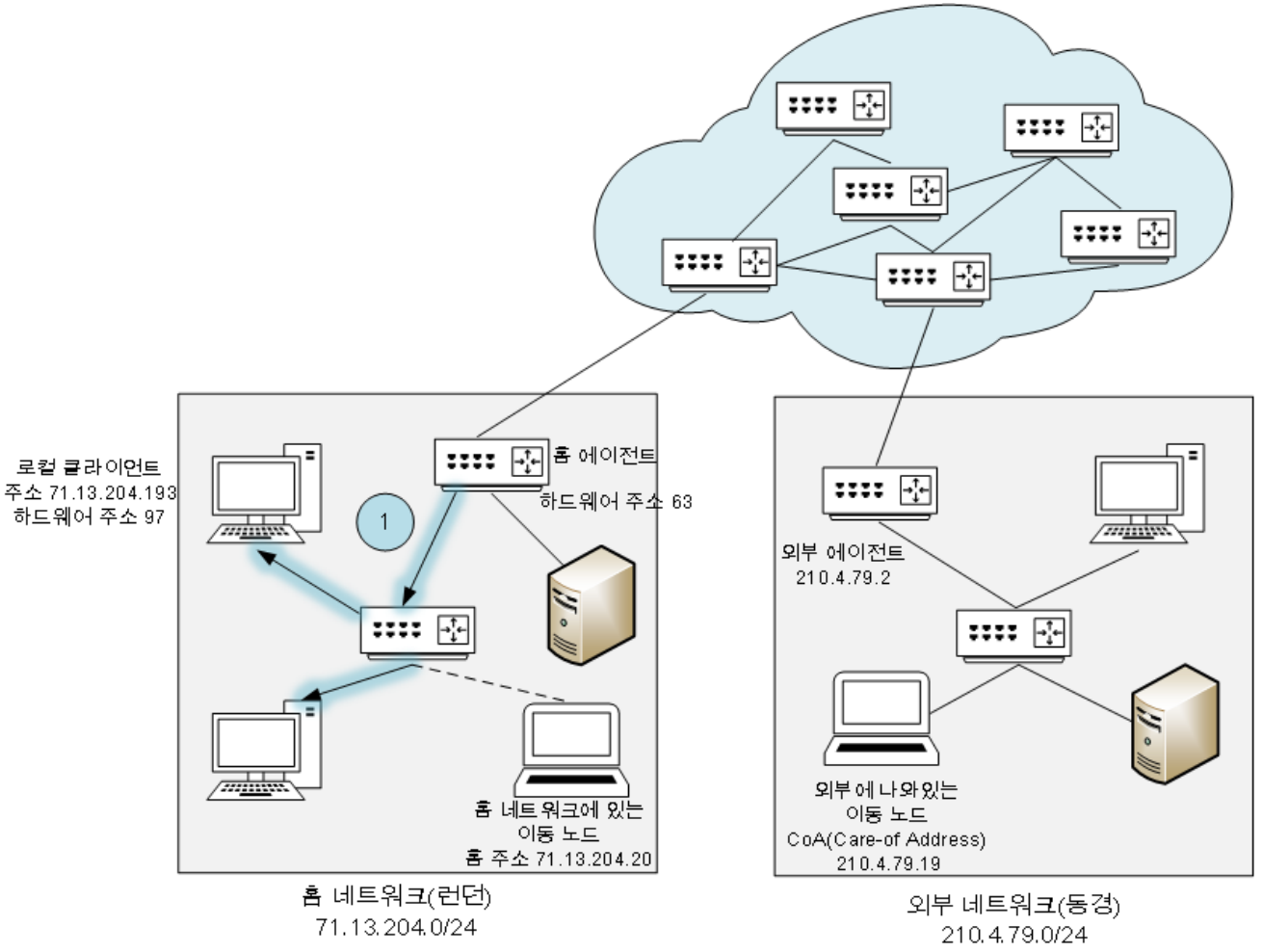
모바일 IP

- 모바일 IP와 TCP/IP 주소 결정 프로토콜
  - ARP 프록싱 동작 과정



모바일 IP

- 모바일 IP와 TCP/IP 주소 결정 프로토콜
  - 무상 ARP 동작 과정



모바일 IP

- 모바일 IP 효율
  - 전송자와 이동 장비의 홈 네트워크의 거리에 따라 비효율 정도가 결정
  - 외부 네트워크에 오래 머무르거나 효율이 중요한 애플리케이션의 경우 모바일 IP보다 다른 방법을 이용
- 모바일 IP 보안 문제
  - 주로 무선 통신으로 이용되기 때문에 보안에 취약
  - 등록 요청과 등록 응답은 인증 되어야 함
  - 재전송 공격 문제 등이 있음
  - 인증과 기밀성을 위해 추가적으로 IPsec을 사용 할 수 있음

감사합니다!