2021/08/14, 2021 네트워크 기초 세미나

TCP/IP 완벽 가이드

- Ⅱ-5부 IP 관련 기능 프로토콜 -

발표자 : 이 태 양(taeyang@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

목 차

- 네트워크 주소 변환(NAT) 프로토콜
- IP security (IPsec) 프로토콜
- 모바일 IP

네트워크 주소 변환(NAT) 프로토콜

- 네트워크 주소 변환(NAT, Network Address Translation) 프로토콜
  - 등장배경
    - IP 주소 고갈
      - IP 주소의 희소성이 증가함에 따라 주소 할당 비용이 증가함
    - 보안 위협 증가
      - 네트워크를 사용하는 악성 사용자가 증가함
  - 정의
    - NAT 라우터를 통해 사설 네트워크에서 인터넷과 통신할 수 있도록 하는 프로토콜
      - NAT 라우터는 사설 IP와 공인 IP를 상호 변환함

네트워크 주소 변환(NAT) 프로토콜

- 장점

장점	설명
공인 IP 주소 공유	여러 호스트가 공인 IP를 공유할 수 있도록 하여 주소 고갈 문제를 지연시킴
쉬운 확장	각 로컬 네트워크 장비에 공인 IP 주소를 할당할 필요 없음
통제력 강화	사설 네트워크에서의 구현으로 관리자의 통제력을 강화
ISP의 유연성	공인 IP 주소 변경으로 ISP 변경이 용이
보안 강화	공인 IP 사용으로 외부의 공격자가 클라이언트에 직접적으로 접근하는 것을 어렵게 함

네트워크 주소 변환(NAT) 프로토콜

- 단점

단점	설명
복잡성	NAT의 구현은 네트워크 구성과 관리의 복잡성 증가
호환성	애플리케이션 데이터 영역 수정 기능이 없어 애플리케이션 호환성 문제의 가능성이 있음
보안 프로토콜 문제	헤더의 변조를 탐지하는 IPsec에서 NAT로 인한 변경을 악성 데이터그램 해킹으로 인지할 수 있음
클라이언트 접근	공인 IP가 없는 클라이언트의 접근에는 한계가 있음

네트워크 주소 변환(NAT) 프로토콜

- 주소 구분
  - 주소가 참조하는 장비의 위치에 따른 구분

구분	설명
내부 주소 (Inside Address)	로컬 네트워크 장비를 가리키는 주소
외부 주소 (Outside Address)	공중 인터넷에 있는 장비를 가리키는 주소

  - 데이터그램의 네트워크 위치에 따른 구분

구분	설명
로컬 주소	내부 네트워크의 데이터그램에 나타나는 주소
전역 주소	외부 네트워크의 데이터그램에 나타나는 주소

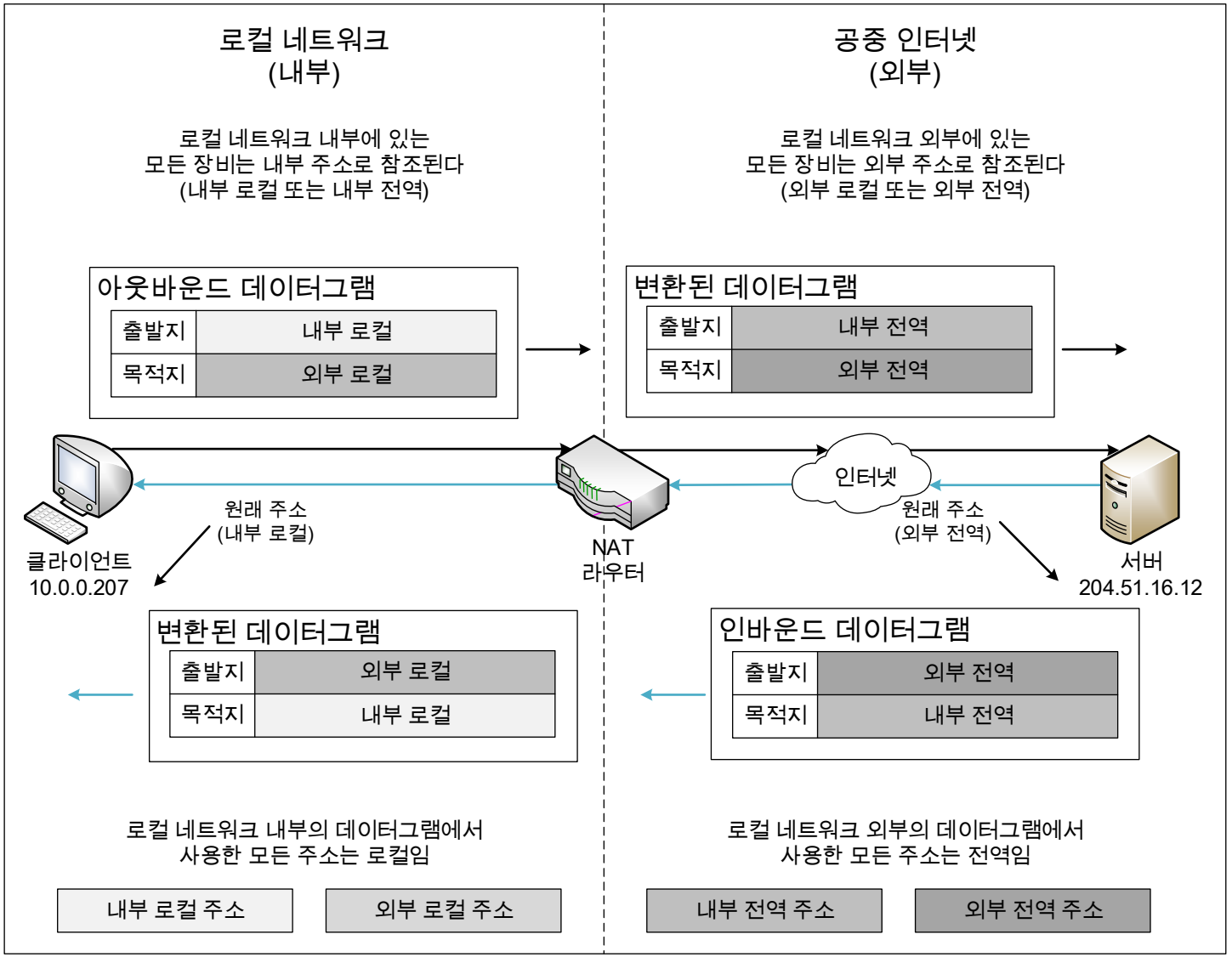
네트워크 주소 변환(NAT) 프로토콜

- 주소 구분
  - 주소 유형

유형	설명
내부 로컬 주소	로컬 네트워크 장비의 주소
내부 전역 주소	공중 네트워크에서 라우팅 가능한 IP 주소로 NAT 라우터에서 사용할 수 있는 공인 IP 주소
외부 전역 주소	공중 인터넷에서 참조하는 외부 장비의 주소
외부 로컬 주소	로컬 네트워크에서 참조하는 외부 장비의 주소

네트워크 주소 변환(NAT) 프로토콜

- 주소 구분



네트워크 주소 변환(NAT) 프로토콜

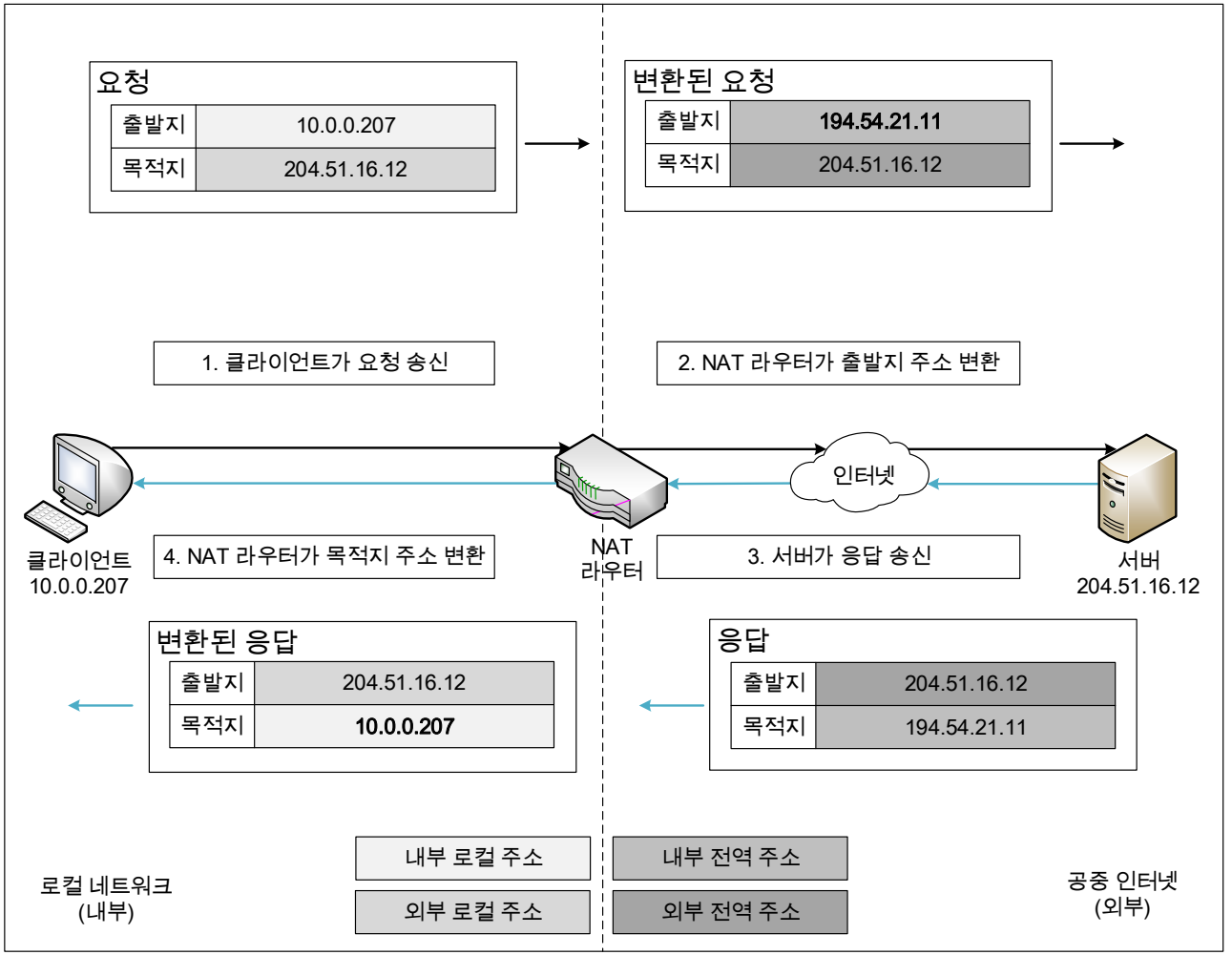
- 변환 테이블 관리
  - 변환 테이블
    - 내부 장비의 내부 로컬 주소를 내부 전역 주소로 매핑하는 정보가 저장되는 테이블
  - 변환 테이블에 항목을 추가하는 방법
    - 정적 매핑
      - 내부 또는 외부 장비의 전역 표현과 로컬 표현 사이에 정의된 영구적이고 고정된 관계
      - 외부 네트워크에서 항상 동일한 공인 IP로 표현되어야 할 장비에 적합
    - 동적 매핑
      - 사전에 정해지지 않고 NAT 라우터에서 정보가 필요할 때마다 즉시 생성되며 사용이 끝나면 버려지는 관계

네트워크 주소 변환(NAT) 프로토콜

- NAT 동작 방식
  - NAT 단방향 (Outbound) 동작
    - 내부 네트워크에서 외부 네트워크로 송신되는 데이터그램으로부터 통신이 시작되는 것
      - 로컬 네트워크의 클라이언트가 요청을 보내고, 인터넷 장비는 응답을 보내는 경우
    - 주소 변환
      - 외부로 나가는 요청 데이터그램은 출발지 주소가 변환됨
      - 내부로 들어오는 응답 데이터그램은 목적지 주소가 변환됨

네트워크 주소 변환(NAT) 프로토콜

- NAT 동작 방식
  - NAT 단방향 (Outbound) 동작

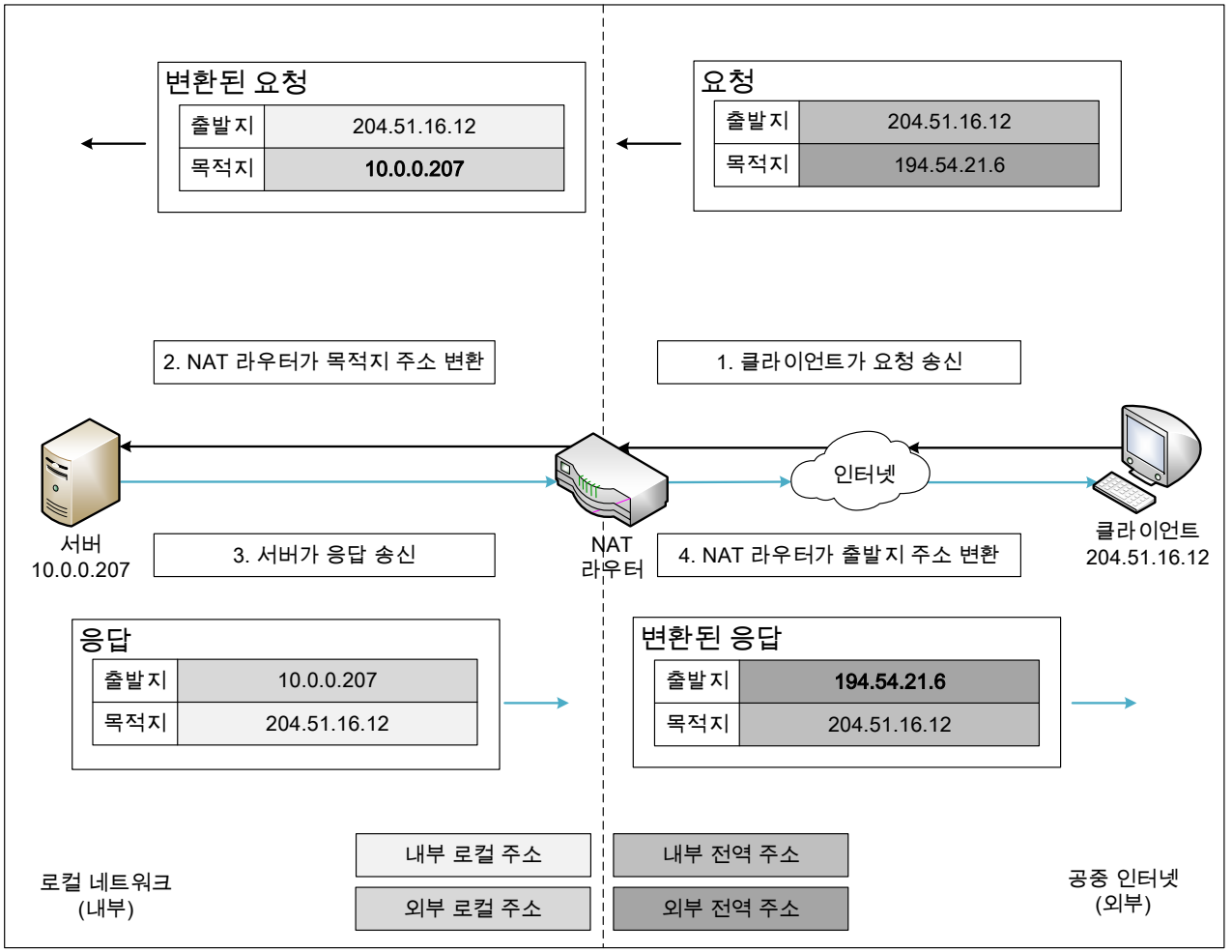


네트워크 주소 변환(NAT) 프로토콜

- NAT 동작 방식
  - NAT 양방향 (Two-Way/Inbound) 동작
    - 인터넷 장비가 요청을 보내고, 로컬 네트워크의 클라이언트가 응답을 보내는 상황을 허용하는 동작 방식
    - 인터넷 장비가 로컬 네트워크의 클라이언트로 데이터그램을 송신하기 위해 클라이언트의 내부 전역 주소를 알아야 함
      - 정적 매핑을 통해 내부 장비의 전역 주소를 외부로 알림
      - DNS (Domain Name System)을 사용한 동적 매핑으로 내부 전역 주소를 알림
    - 주소 변환
      - 내부로 들어오는 요청 데이터그램은 목적지 주소가 변환됨
      - 외부로 나가는 응답 데이터그램은 출발지 주소가 변환됨

네트워크 주소 변환(NAT) 프로토콜

- NAT 동작 방식
  - NAT 양방향 (Two-Way/Inbound) 동작

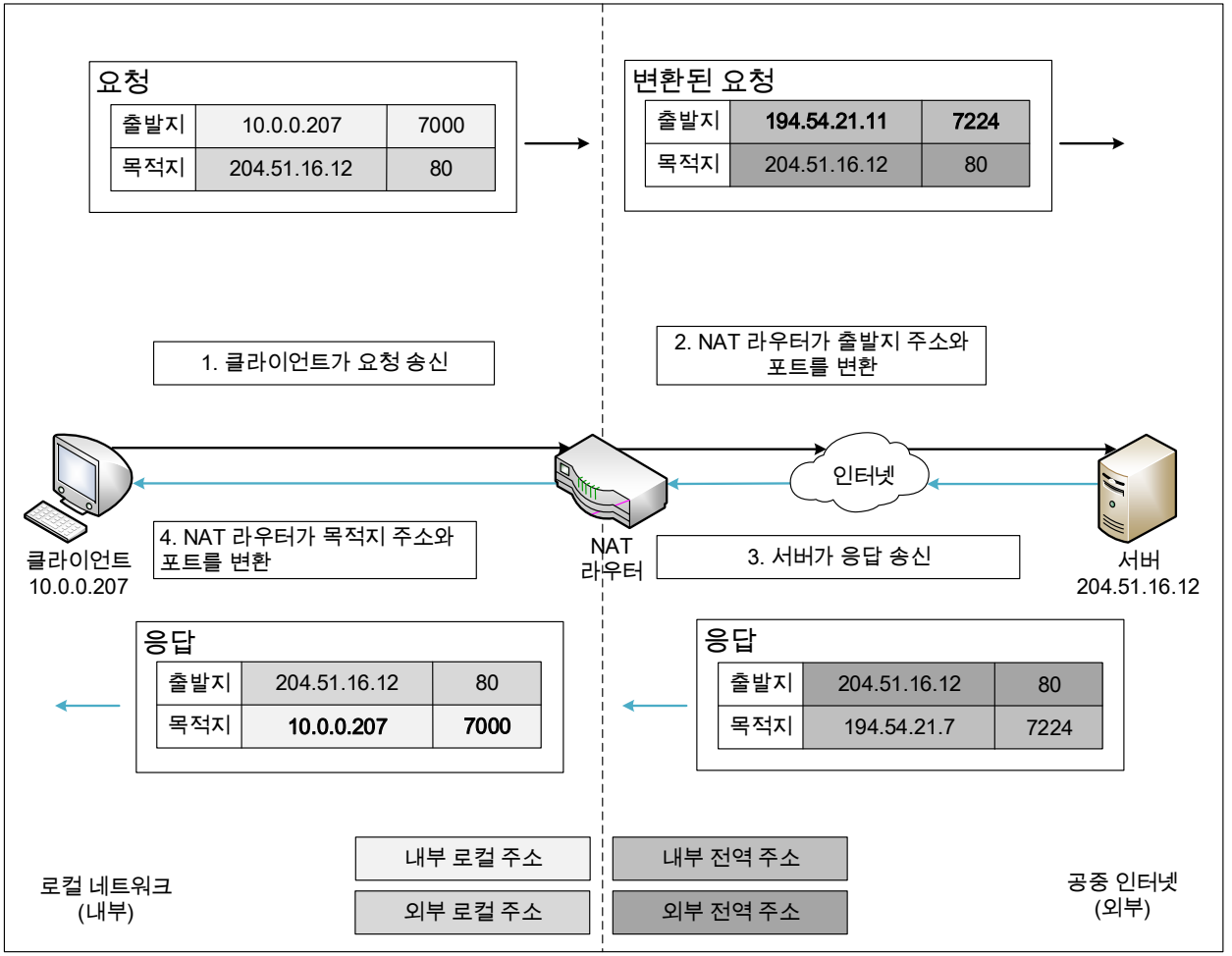


네트워크 주소 변환(NAT) 프로토콜

- NAT 동작 방식
  - NAT 포트 기반 (과부하) 동작
    - 사설 네트워크의 다수의 호스트가 동시에 하나의 내부 전역 주소를 공유하는 동작 방식
    - 주소 변환
      - 외부로 나가는 요청의 출발지 주소와 포트를 내부 로컬에서 내부 전역 형태로 변환
      - 내부로 들어오는 응답의 목적지 주소와 포트를 내부 전역에서 내부 로컬 형태로 변환

네트워크 주소 변환(NAT) 프로토콜

- NAT 동작 방식
  - NAT 포트 기반 (과부하) 동작

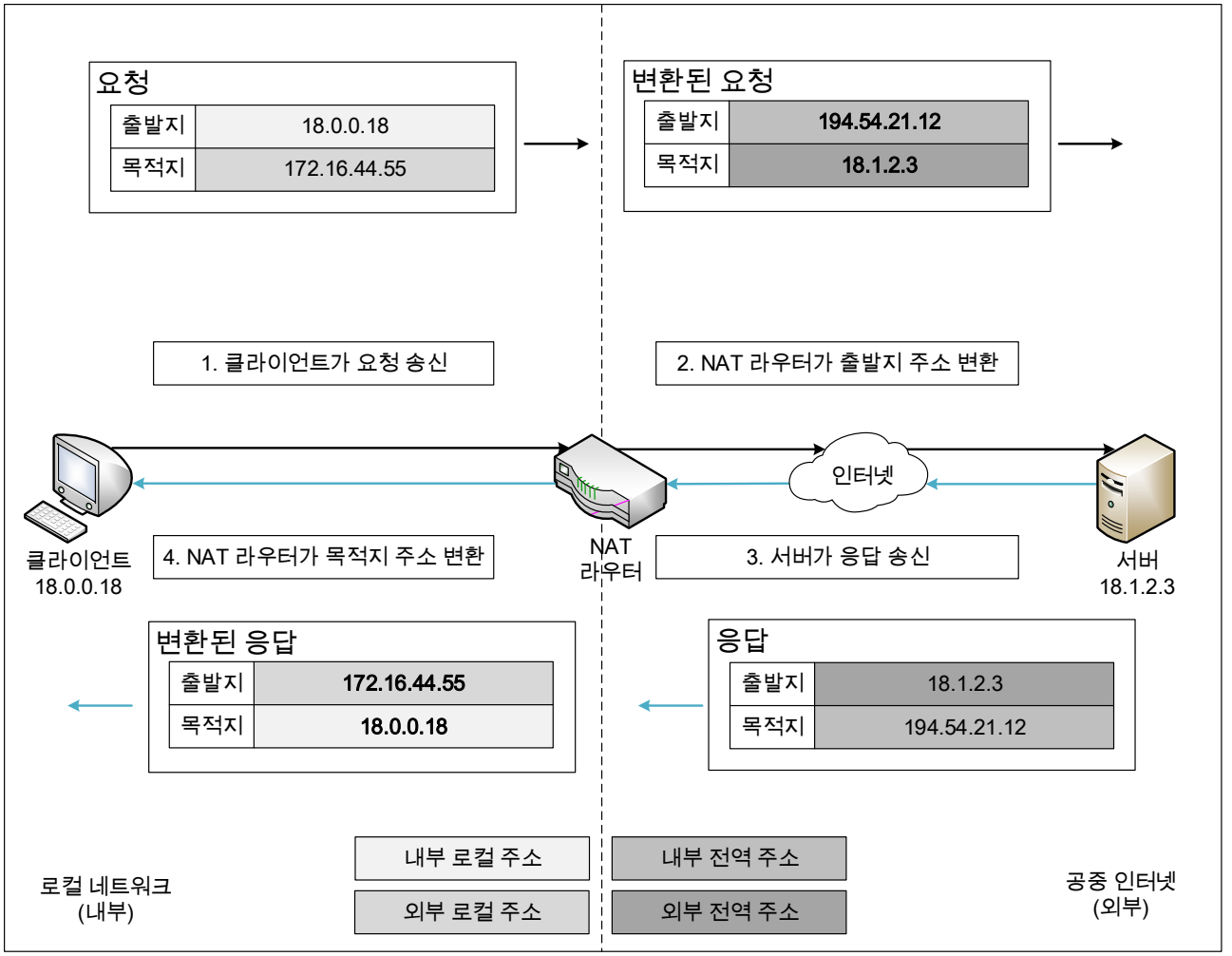


네트워크 주소 변환(NAT) 프로토콜

- NAT 동작 방식
  - NAT 중복/2회 NAT 동작
    - NAT 라우터가 관장하는 사설 네트워크와 내부 네트워크의 주소 공간과 충돌되는 중복 네트워크를 위한 매핑을 생성하는 방식
    - DNS(Domain Name System)에 의존하여 외부 장비의 주소를 획득
    - 주소 변환
      - 외부로 나가는 메시지는 내부 로컬 주소를 내부 전역 주소로, 외부 로컬 주소를 외부 전역 주소로 변환
      - 내부로 들어오는 메시지는 내부 전역 주소를 내부 로컬 주소로, 외부 전역 주소를 외부 로컬 주소로 변환

네트워크 주소 변환(NAT) 프로토콜

- NAT 동작 방식
  - NAT 중복/2회 NAT 동작



네트워크 주소 변환(NAT) 프로토콜

- 호환성 문제와 특수 처리 요구사항
  - IP주소 변경에 따른 문제
    - TCP와 UDP 체크섬 재계산
    - IPsec 무결성 검사에서는 NAT 사용 불가
      - IP 데이터그램의 TCP나 UDP 체크섬 갱신으로 무결성 검사를 할 수 없음
    - ICMP (Internet Control Message Protocol) 조작
      - IP 헤더 부분을 포함하는 ICMP 메시지를 검사하여 IP 헤더의 주소를 변환해야 함

IP security(IPsec) 프로토콜

- 정의
  - IP의 안전한 통신을 보장하는 서비스와 프로토콜의 모음
- 등장배경
  - 인터넷의 성장으로 IP의 보안 기능 부족 문제를 해결하기 위해 등장
- 기능

기능	설명
데이터 암호화	• 사용자 데이터 암호화
무결성 보장	• 메시지가 변조되지 않았음을 보장
보안 공격으로부터 보호	• 순서번호 값을 통해 재전송 공격을 방어
보안 알고리즘과 키 협상	• 보안 요구의 맞는 보안 알고리즘과 키 협상을 제공
보안 모드 제공	• 서로 다른 네트워크 요구 만족을 위해 보안 모드 제공 • e.g., 터널(Tunnel) 모드, 전송(Transport) 모드

IP security(IPsec) 프로토콜

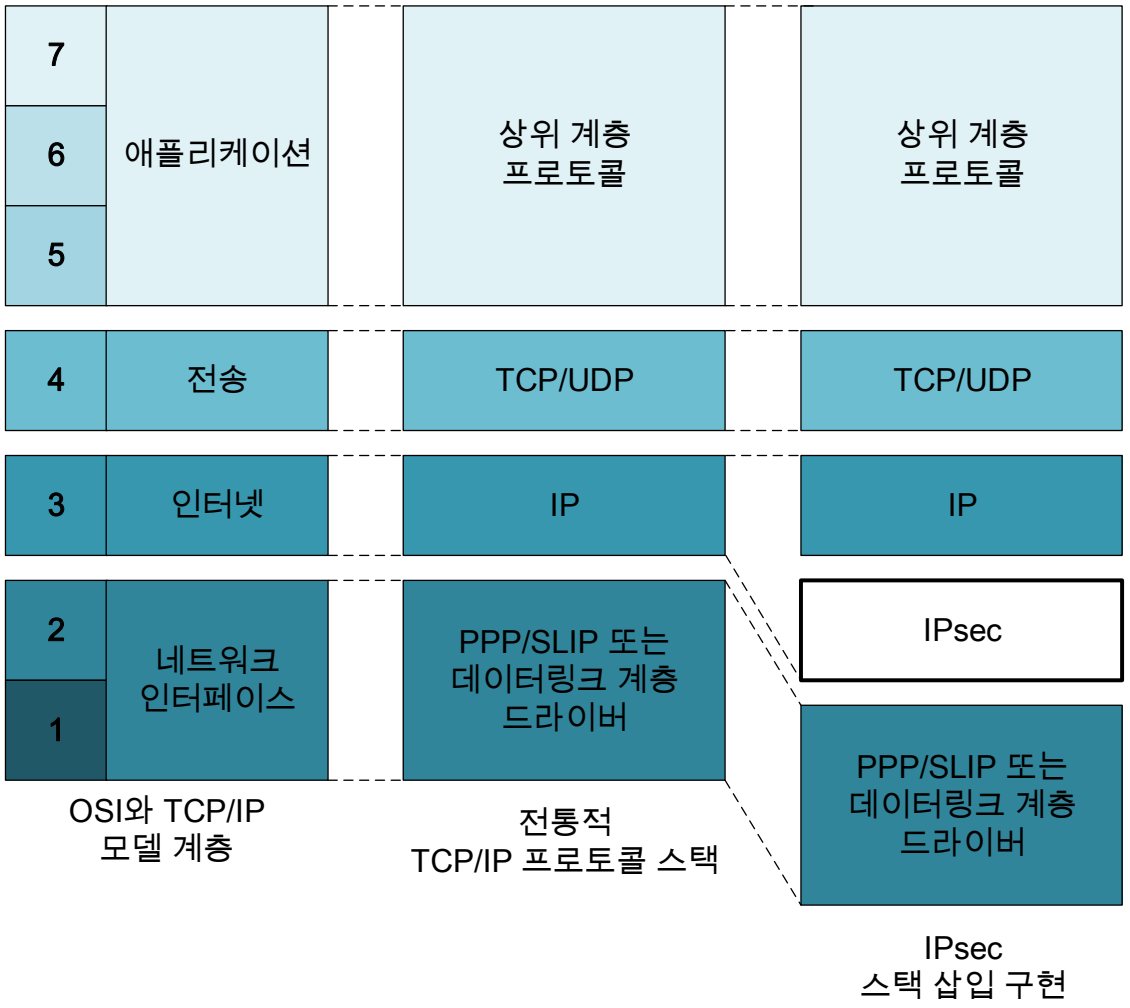
- 구현 방법
  - 종단 호스트 구현
    - IPsec을 모든 호스트 장비에 설치하는 것
    - 모든 장비 사이에 보안을 구현하여 유연성과 보안성을 높임
  - 라우터 구현
    - IPsec을 라우터에만 설치하는 것
    - 라우터와 로컬 호스트 사이의 연결은 보호되지 않음

IP security(IPsec) 프로토콜

- 구현 구조
  - 통합 구조
    - IPsec의 프로토콜과 기능을 IP 자체에 직접 통합하는 구조
    - IPv4는 각 장비의 IP 구현을 변경해야 하므로 실용적이지 않음
  - 스택 삽입 구조 (BITS, Bump In The Stack)
    - IP와 데이터 링크 계층 사이에 IPsec이 별도의 계층으로 존재하는 구조
    - 데이터그램을 데이터 링크 계층으로 전달하기 전에 데이터그램에 보안 기능을 덧붙인 뒤 전달

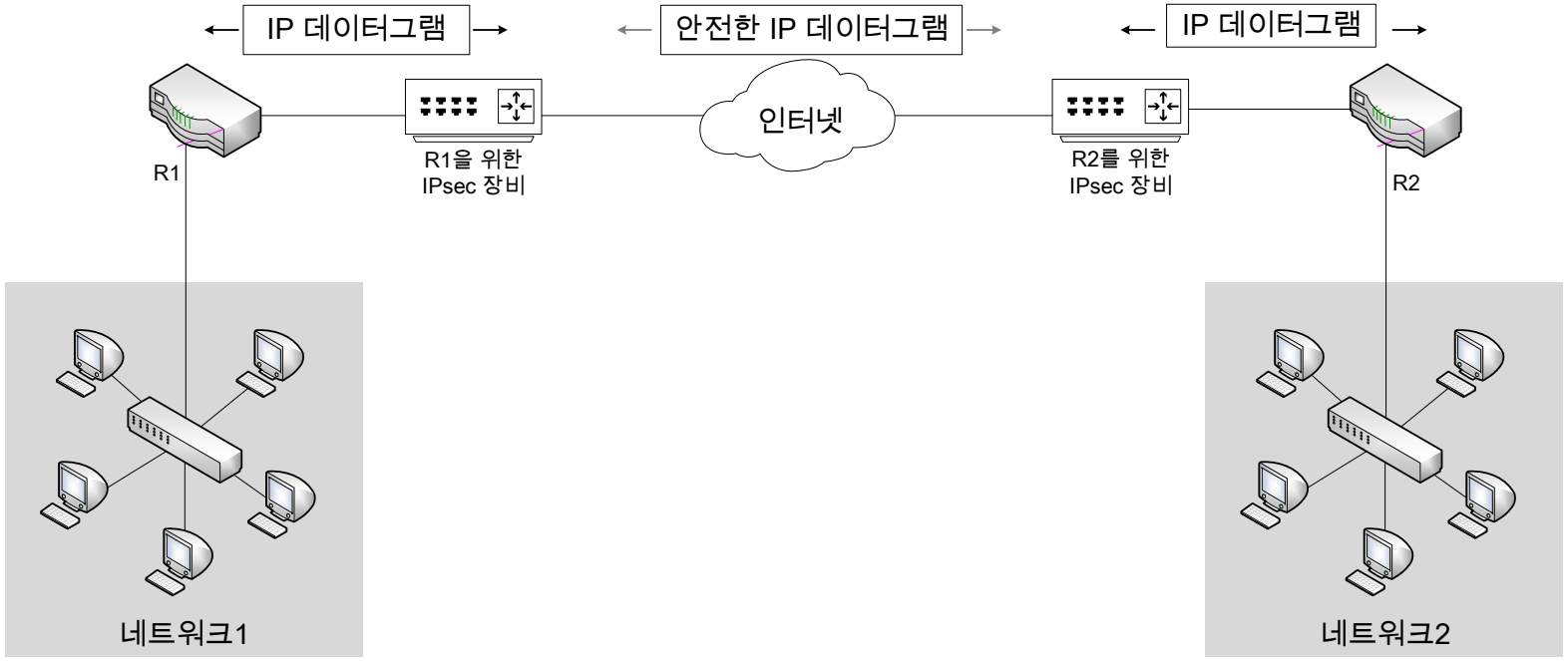
IP security(IPsec) 프로토콜

- 구현 구조
  - 스택 삽입 구조 (BITS, Bump In The Stack)



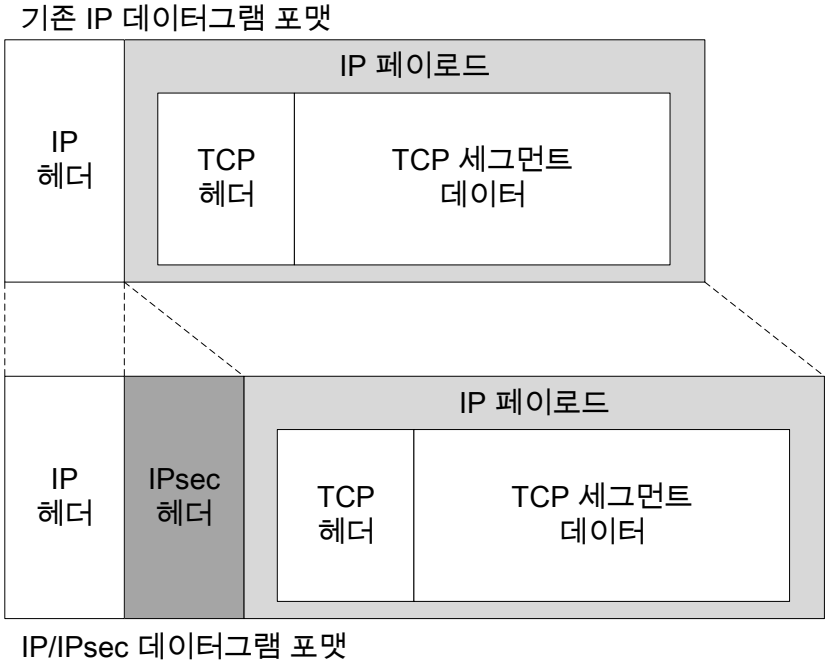
IP security(IPsec) 프로토콜

- 구현 구조
  - 라인 삽입 구조 (BITW, Bump In The Wire)
    - IPsec 서비스를 제공하는 하드웨어 장비를 추가한 구조



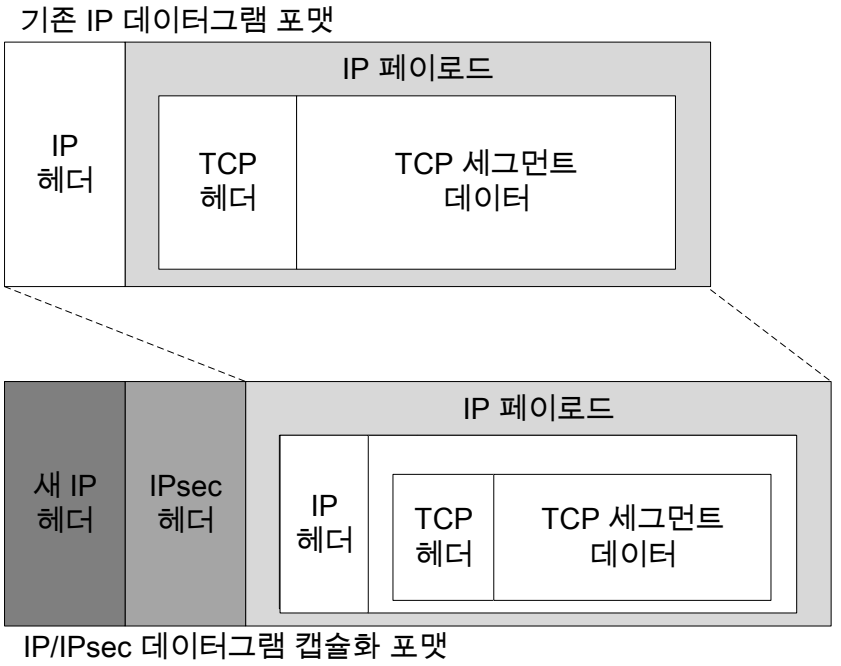
IP security(IPsec) 프로토콜

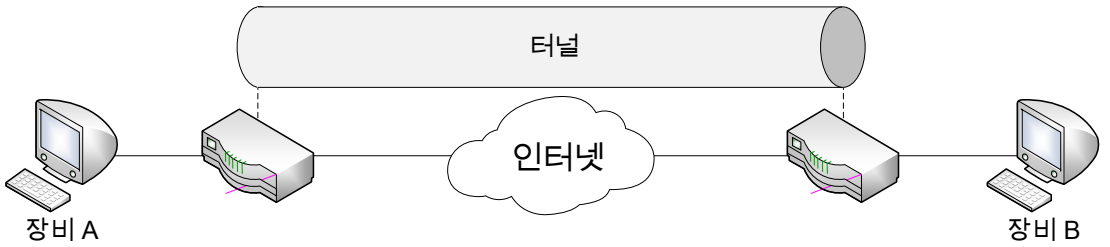
- 동작 모드
  - 전송 모드 (Transport Mode)
    - 전송 계층과 IP 계층 사이에 IPsec 계층에서 전달되는 메시지의 페이로드를 보호하는 모드
    - IPsec 구조와의 연관성
      - 통합 구조와 연관됨



IP security(IPsec) 프로토콜

- 동작 모드
  - 터널 모드 (Tunnel Mode)
    - 캡슐화된 IP 데이터그램이 또 다른 IP 데이터그램 안으로 캡슐화되는 모드
    - IPsec 구조와의 연관성
      - 스택 삽입 구조와 라인 삽입 구조와 연관됨





IP security(IPsec) 프로토콜

- 보안 구성 요소

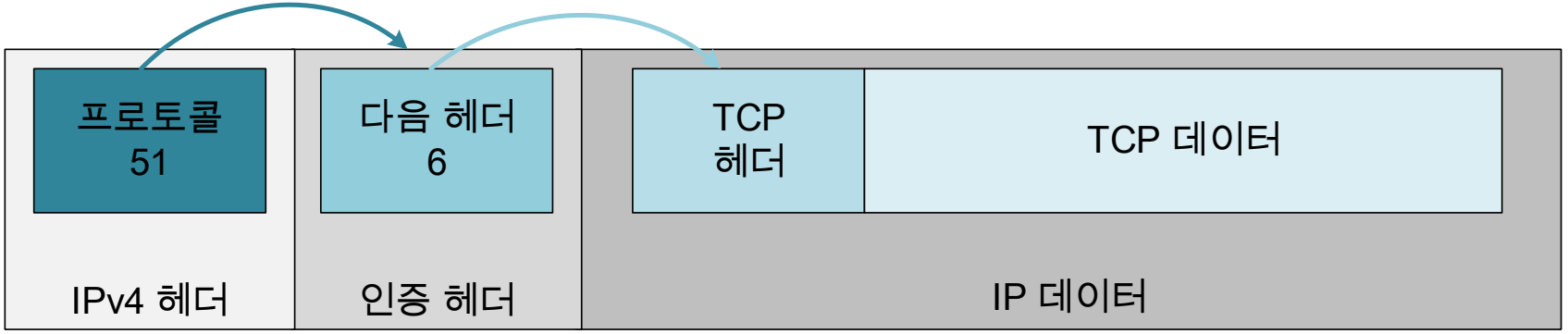
구성 요소	설명
보안 정책	• 데이터그램 유형에 따라 보안 제공 지침을 제시 • e.g., IPsec 구현에 내장된 규칙으로 패킷에 대한 IPsec 처리 여부를 결정 • 보안 정책 데이터베이스 (SPD, security Policy Database)에 저장됨
보안 연관 (SA, security Association)	• 두 장비 사이에 맺은 특정 보안 연결을 설명하는 보안 정보 • 보안 연관 데이터베이스 (SAD, security Association Database)에 저장됨
선택자 (Selector)	• IP 트래픽에 적용할 보안 정책이나 SA를 결정하는 규칙 모음

IP security(IPsec) 프로토콜

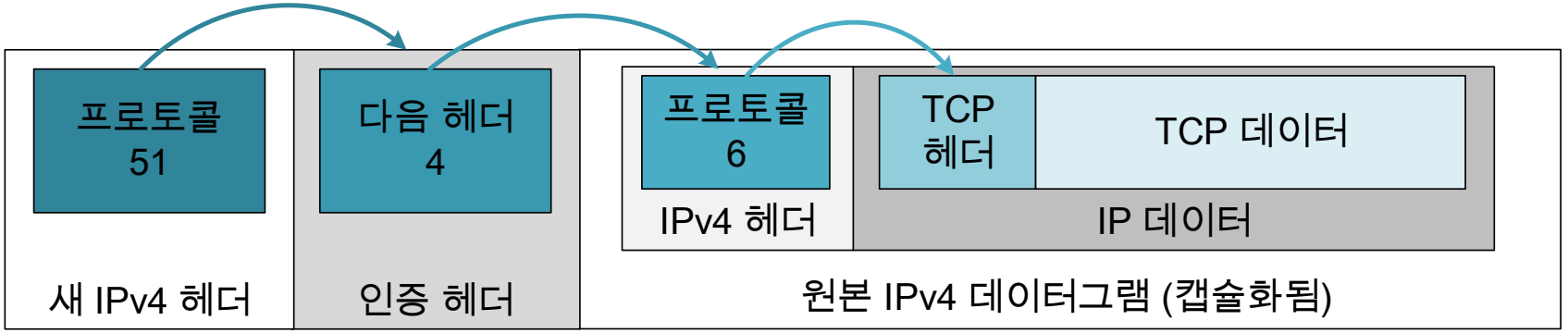
- 핵심 프로토콜
  - IPsec 인증 헤더 (AH, Authentication Header)
    - 데이터그램 값으로 계산되는 헤더를 추가하여 데이터그램의 무결성을 인증하는 서비스를 제공하는 프로토콜
    - 기능
      - 송신자로 표현된 장비가 실제로 그 메시지를 송신했다는 것을 수신 장비가 검증할 수 있는 서비스를 제공
      - 수신 장비는 중간 장비들이 데이터그램을 변경하지 않았음을 검증할 수 있음
      - 재전송 공격으로부터 보호
    - 동작 과정
      1. 특수 해싱 알고리즘과 특수 키로 AH 계산
      2. 계산 결과(ICV, Integrity Check Value)를 특수 헤더에 넣어 전송
      3. 목적지 장비는 공유하는 키로 동일한 계산 수행 후 결과값을 비교

IP security(IPsec) 프로토콜

- 핵심 프로토콜
  - IPsec 인증 헤더 (AH, Authentication Header)
    - AH 데이터그램 위치와 연결
      - 전송 모드



      - 터널 모드



IP security(IPsec) 프로토콜

- 핵심 프로토콜
  - IPsec 인증 헤더 (AH, Authentication Header)
    - 포맷

IP security(IPsec) 프로토콜

- 핵심 프로토콜
  - IPsec 인증 헤더 (AH, Authentication Header)
    - 포맷

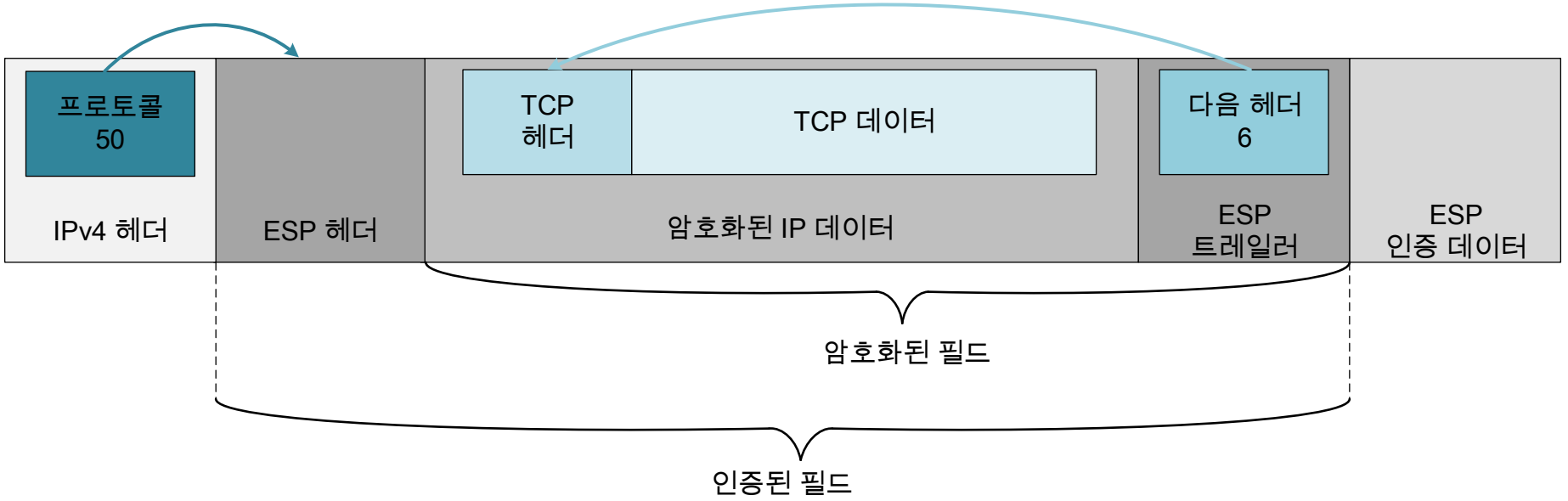
필드 이름	크기(바이트)	설명
다음 헤더	1	• AH 다음에 오는 헤더의 프로토콜 번호를 담고 있는 필드 • 헤더를 서로 연결하는 데 쓰임
페이로드 길이	1	• 인증 헤더 길이를 측정
예약됨	2	• 쓰이지 않는 필드로 0으로 설정
SPI	4	• 목적지 주소, 보안 프로토콜 유형, SA를 식별
순서 번호	4	• 각 데이터그램을 유일하게 식별하는 필드 • 두 장비간 SA가 구성될 때 0으로 초기화되는 카운터 필드 • 재전송 공격 방어에 사용됨
인증 데이터	가변적	• 무결성 검사값(ICV)을 포함하는 필드

IP security(IPsec) 프로토콜

- 핵심 프로토콜
  - 보안 페이로드 캡슐화 (ESP, Encapsulating security Payload)
    - IP 데이터그램을 암호화하여 지정된 수신자만 데이터를 볼 수 있도록 하는 프로토콜
    - 동작 단계
      1. 헤더 계산
         - 전송 모드에서는 원본 데이터그램의 IP 헤더 뒤에 위치
         - 터널 모드에서는 원본 데이터그램을 캡슐화하는 새 IP 데이터그램의 IP 헤더 뒤에 위치
      2. 트레일러 계산
         - ESP 트레일러 필드가 암호화될 데이터 뒤에 붙으면 ESP는 암호화를 수행
         - 페이로드와 ESP 트레일러는 암호화되지만, ESP 헤더는 암호화되지 않음
      3. ESP 인증 필드 계산
         - ESP 헤더, 페이로드, 트레일러로 계산을 수행

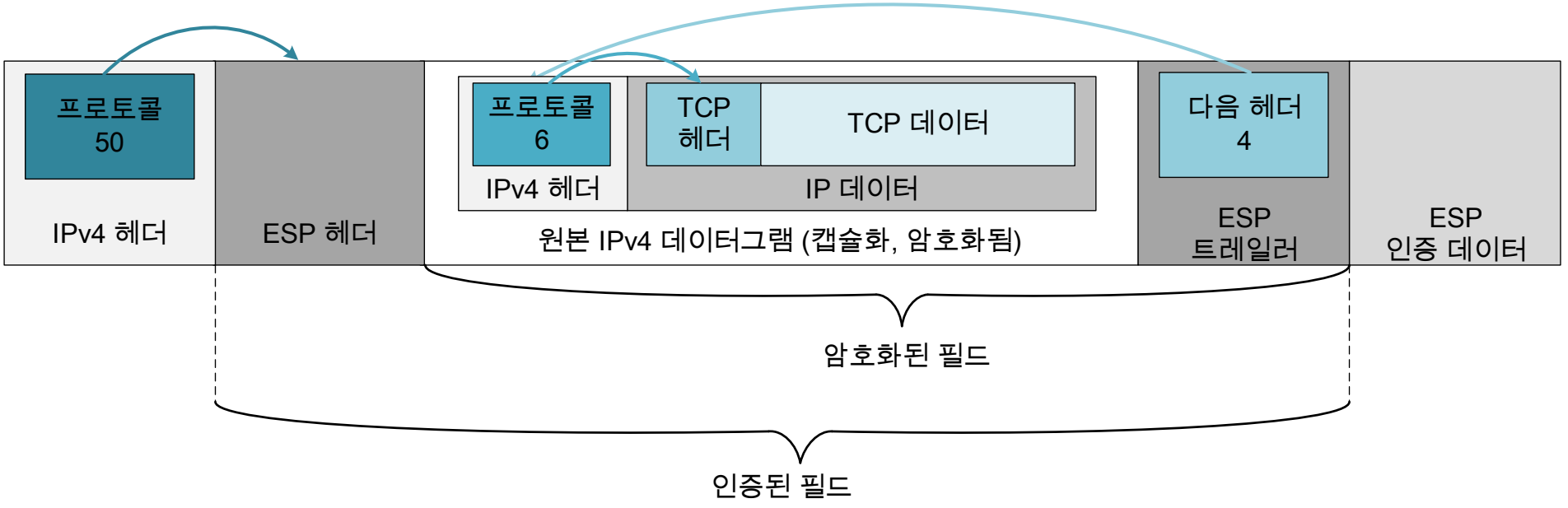
IP security(IPsec) 프로토콜

- 핵심 프로토콜
  - 보안 페이로드 캡슐화 (ESP, Encapsulating security Payload)
    - 동작과 필드 사용
      - 전송 모드



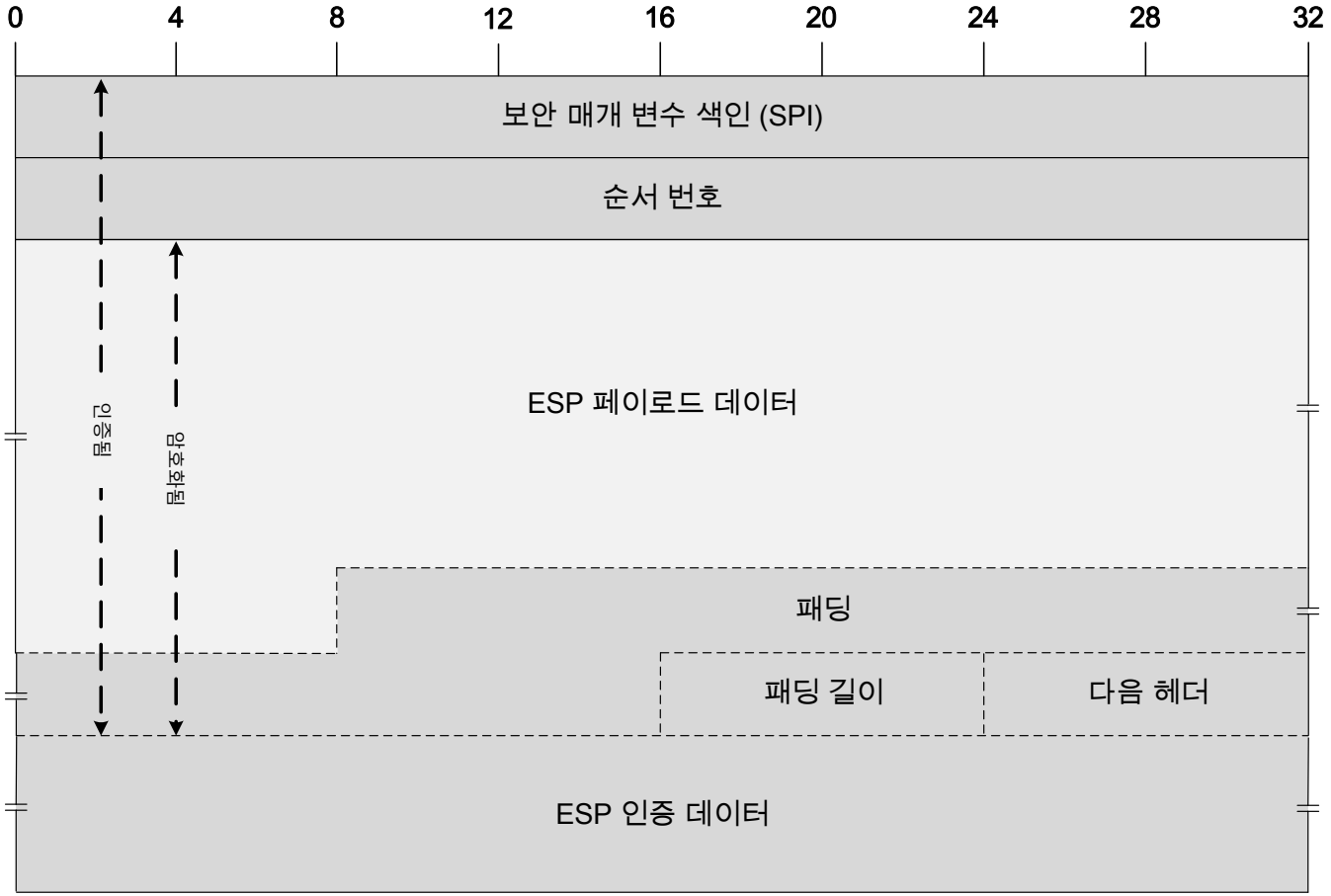
IP security(IPsec) 프로토콜

- 핵심 프로토콜
  - 보안 페이로드 캡슐화 (ESP, Encapsulating security Payload)
    - 동작과 필드 사용
      - 터널 모드



IP security(IPsec) 프로토콜

- 핵심 프로토콜
  - 보안 페이로드 캡슐화 (ESP, Encapsulating security Payload)
    - 포맷



IP security(IPsec) 프로토콜

- 핵심 프로토콜
  - 보안 페이로드 캡슐화 (ESP, Encapsulating security Payload)
    - 포맷

구간	필드 이름	크기(바이트)	설명	암호화 범위	인증 범위
ESP 헤더	SPI	4	데이터그램에 쓰이는 SA를 식별		↕
	순서 번호	4	SA가 구성될 때 0으로 초기화 되는 카운터 필드 재전송 공격으로부터 IPsec을 방어		
페이로드	페이로드	가변적	암호화된 페이로드 데이터	↕	
ESP 트레일러	패딩	가변적 (0에서 255)	암호화 또는 정렬을 위해 패딩 바이트가 추가되는 필드		
	패딩 길이	1	패딩 필드의 바이트 수		
	다음 헤더	1	다음 헤더의 프로토콜 번호를 담는 필드		
ESP 인증 데이터		가변적	ICV를 포함하는 필드		

IP security(IPsec) 프로토콜

- 핵심 프로토콜
  - 인터넷 키 교환 (IKE, Internet Key Exchange)
    - 두 장비가 보안 프로토콜에서 사용할 비밀 정보를 교환하는 것을 지원하는 프로토콜
    - 동작 단계
      1. IKE SA를 생성하여 암호화된 데이터를 송수신할 준비
      2. 교환할 데이터 보호 방식을 결정하여 IPsec SA를 생성
      3. 상호 합의한 방식대로 데이터를 교환함

모바일 IP

- 정의
  - 이동 환경에서 IP를 지원하기 위한 프로토콜
- 등장 배경
  - 기존 IP주소 기반으로 라우팅하는 IP 네트워크는 이동 장비를 지원하는 데에 한계를 가짐
  - 이동 장비에게도 IP 기능을 제공하는 것에 대한 필요 증가
- 목표
  - 이동 장비의 네트워크가 변경되더라도 기존 IP 주소 변경없이 계속 사용할 수 있도록 함
  - 작동 방식이 서로 다른 모바일 IP 장비와 기존 IP 장비의 통신을 원활하도록 함

모바일 IP

- 모바일 IP를 구현하는 장비

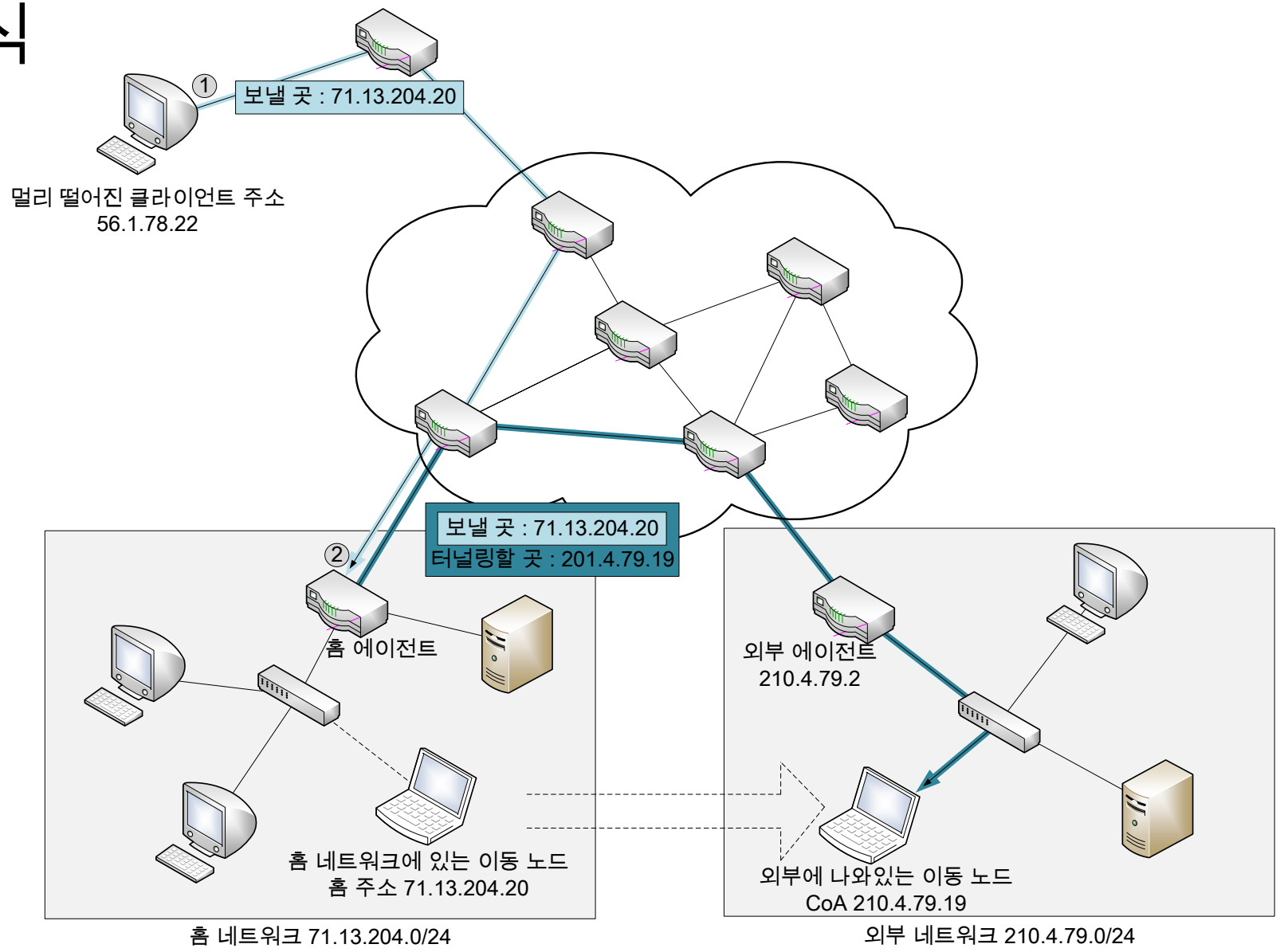
장비	설명
이동 장비	네트워크 간을 이동하는 장비
홈 에이전트 (Home Agent)	이동 장비의 홈 네트워크에 있는 라우터
외부 에이전트 (Foreign Agent)	이동 장비가 현재 사용하고 있는 네트워크의 라우터

모바일 IP

- 동작 방식
  - 이동 장비는 일반적으로 자신의 IP 주소의 네트워크 ID가 가리키는 홈 네트워크에 위치
  - IP 주소를 통해 전달되는 데이터는 장비의 홈 네트워크에 있는 라우터로 전달됨
  - 장비가 홈 네트워크에 있지 않은 경우, 홈 라우터는 장비의 현재 주소로 데이터를 전달
    - 장비가 새 임시 주소를 갖는 경우 바로 전달
    - 장비의 현재 네트워크 라우터로 전달

모바일 IP

- 동작 방식


①
보낼 곳 : 71.13.204.20
멀리 떨어진 클라이언트 주소
56.1.78.22
보낼 곳 : 71.13.204.20
터널링할 곳 : 201.4.79.19
②
홈 에이전트
외부 에이전트
210.4.79.2
홈 네트워크에 있는 이동 노드
홈 주소 71.13.204.20
외부에 나와있는 이동 노드
CoA 210.4.79.19
홈 네트워크 71.13.204.0/24
외부 네트워크 210.4.79.0/24

모바일 IP

- 동작 과정

1. 에이전트 통신
   - 에이전트의 광고 메시지를 통해 자신의 위치 확인
   - 에이전트의 광고 메시지를 수신하지 못한 경우 요청 메시지를 전송

2. 네트워크 위치 판단
   - 에이전트 발견 메시지 내용을 기반으로 자신이 홈 네트워크에 있는지 외부 네트워크에 있는지 판단

3. CoA (Care-of-Address) 획득
   - 이동 장비가 외부 네트워크에 있는 경우 CoA 임시 주소를 획득

모바일 IP

- 동작 과정

4. 에이전트 등록
   - 이동 장비는홈 에이전트에 자신의 위치를 알림
   - 홈 에이전트에 등록하여 자신에게 오는 데이터그램을 전달해줄 것을 요청

5. 데이터그램 전달
   - 이동 장비에게 온 데이터그램을 받아 실제 이동 장비의 위치로 전달
   - CoA 종류에 따라 전달 방식이 다름

모바일 IP

- 모바일 IP 주소
  - 홈 주소
    - 이동 장비에게 할당된 고정 IP 주소
    - 홈 네트워크에서 장비가 사용하는 주소
  - CoA (Care-Of Address)
    - 이동 장비가 홈 네트워크 외부로 움직였을 때 사용하는 임시 주소
    - 모바일 IP에서만 사용하며 IP 데이터그램을 전달하거나 관리 기능을 실행할 때만 사용됨

모바일 IP

- 모바일 IP 주소
  - CoA (Care-Of Address)
    - 유형
      - 외부 에이전트 CoA
        - 외부 에이전트의 IP 주소
        - 장점
          - 외부 네트워크에 있는 모든 이동 장비들이 같은 외부 CoA를 사용
      - 공존 CoA (Co-Located Care-of-Address)
        - 이동 장비에게 직접 할당된 주소
        - 홈 에이전트가 이동 장비에게 데이터그램을 직접 전달할 수 있도록 함
        - 장점
          - 모바일 IP 기능을 가지는 라우터가 없는 네트워크에서도 모바일 IP를 사용할 수 있음
        - 단점
          - 장비가 외부 네트워크에서도 유일한 IP 주소를 가져야 함

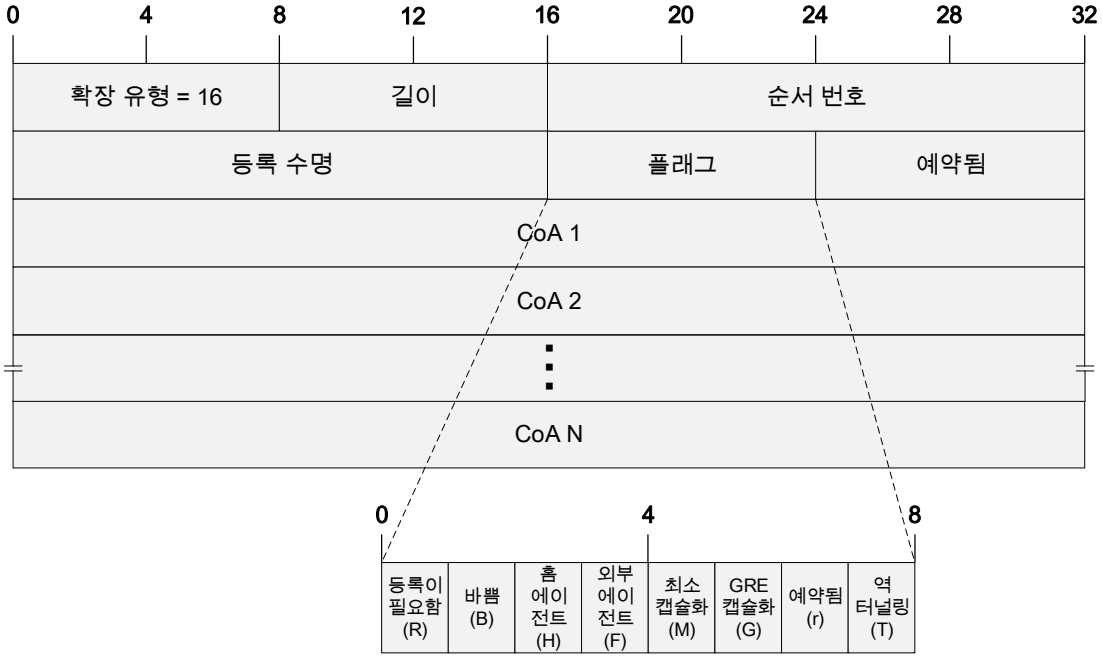
모바일 IP

- 모바일 IP 에이전트 발견
  - 이동 장비가 로컬 네트워크에 있는 에이전트와 접속을 시도하는 것
  - 목적

목적	설명
에이전트/노드 통신	• 에이전트에 대한 중요한 정보를 담은 메시지를 노드에게 전송 • 노드는 에이전트에게 정보를 요청
현재 위치 발견	• 노드가 홈 네트워크에 있는지 외부 네트워크에 있는지를 확인
CoA 할당	• 이동 장비가 사용할 CoA를 획득

모바일 IP

- 모바일 IP 에이전트 발견
  - 사용되는 메시지
    - 에이전트 광고 (Agent Advertisement)
      - 모바일 IP 에이전트의 역할 수행이 가능한 라우터가 정기적으로 전송하는 메시지
      - 에이전트는 이동 장비가 네트워크 대역을 소모하지 않도록 광고 메시지를 전송
      - 포맷



모바일 IP

- 모바일 IP 에이전트 발견
  - 사용되는 메시지
    - 에이전트 요청 (Agent Solicitation)
      - 모바일 IP 장비가 로컬 에이전트에게 에이전트 광고를 요청하는 메시지
      - 포맷

모바일 IP

- 모바일 IP 홈 에이전트 등록
  - 외부 네트워크에 있는 이동 장비가 모바일 IP 사용을 위해 필요한 정보와 지시를 홈 에이전트와 주고 받는 과정
  - 이동 장비 등록 이벤트

이벤트	설명
등록 이동	• 이동 장비가 외부 네트워크에서 등록을 시작
등록 해제	• 이동 장비가 다시 홈 네트워크로 돌아온 경우
재등록	• 외부 네트워크 간에서 이동하거나 CoA가 변경된 경우 • 등록 기간이 만료되었는데도 외부 네트워크에 있는 경우

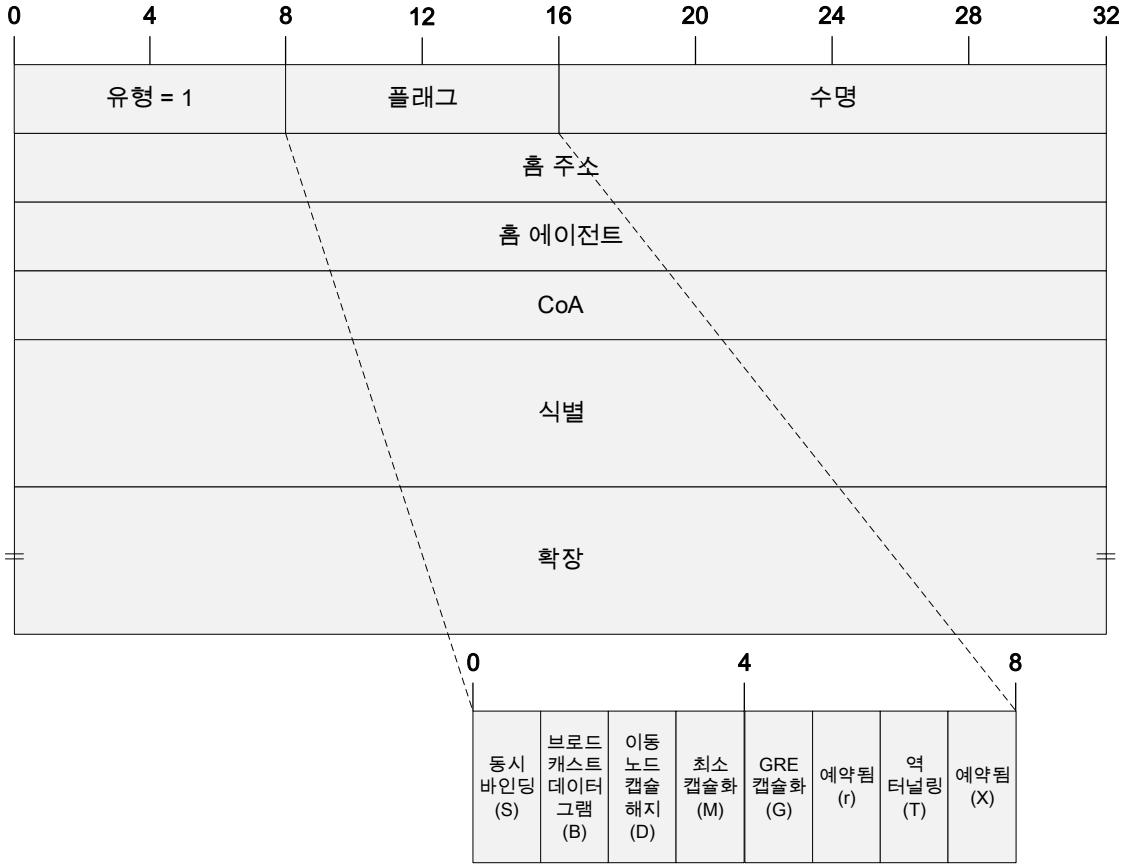
모바일 IP

- 모바일 IP 홈 에이전트 등록
  - 등록 과정
    - 공존 CoA를 사용하는 경우
      1. 이동 장비가 등록 요청을 홈 에이전트에게 전송
      2. 홈 에이전트는 이동 장비에게 등록 응답을 전송

    - 외부 CoA를 사용하는 경우
      1. 이동 장비가 등록 요청을 외부 에이전트에게 전송
      2. 외부 에이전트가 등록 요청을 처리하여 홈 에이전트에게 전송
      3. 홈 에이전트는 외부 에이전트에게 등록 응답을 전송
      4. 외부 에이전트가 등록 응답을 받아 처리하고 이동 장비에게 전송

모바일 IP

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



모바일 IP

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

모바일 IP

- 모바일 IP 데이터 캡슐화
  - 홈 에이전트는 이동 장비 주소로 온 데이터그램을 캡슐화하여 이동 장비의 CoA로 전송
  - IP-in-IP (IP Encapsulation within IP)
    - IP 데이터그램을 다른 IP 데이터그램의 페이로드로 만드는 캡슐화

모바일 IP

- 모바일 IP 터널링
  - 캡슐화된 데이터그램이 터널을 통해 안전하게 네트워크를 지나게 하는 것
  - 유형
    - 외부 에이전트 CoA를 사용하는 터널링
      - 외부 에이전트에서 터널이 끝남
      - 캡슐화된 메시지를 홈 에이전트에서 받아 외부 IP 헤더를 벗겨내고 원래 데이터그램을 이동 장비에게 전달
    - 공존 CoA를 사용하는 터널링
      - 이동 장비에서 터널이 끝남
      - 이동 장비가 캡슐화 헤더를 벗겨냄

모바일 IP

- 모바일 IP 터널링
  - 과정
    1. 이동 장비가 외부 네트워크에서 다른 네트워크에 있는 노드에게 요청 메시지를 전송
    2. 해당 노드는 이동 장비에게 응답을 전송하나 이동 장비의 홈 네트워크로 응답이 전송됨
    3. 홈 에이전트는 응답을 이동 장비에게 터널링함

모바일 IP

- 모바일 IP 역터널링
  - 이동 장비가 데이터그램을 인터넷으로 직접 전송할 수 없을 경우 활용되는 옵션 기능
  - 이동 장비의 모든 전송은 홈 에이전트와의 터널을 통해 이루어짐
  - 사용되는 경우
    - 이동 장비가 특별한 보안 규칙을 가진 네트워크에서 원래 IP 주소로 데이터그램을 전송하지 못하는 경우
    - 스푸핑(Spoofing)을 방지하기 위한 경우

모바일 IP

- TCP/IP 주소 결정 프로토콜(ARP, Address Resolution Protocol)관련 문제
  - 외부에 있는 이동 장비에게 데이터링크 계층 주소로 데이터그램을 직접 전송할 수 없음
  - 해결 방법
    - ARP 프록싱 (ARP Proxing)
      - 홈 에이전트는 이동 장비 대신 ARP 요청을 받음
      - 대신 응답하면서 자신의 데이터 링크 계층 주소를 알림
      - 홈 에이전트는 해당 데이터그램을 이동 장비에게 전송
    - 무상 ARP (Gratuitous ARP)
      - 이미 이동 장비에 대한 캐시를 갖고 있는 노드의 경우
      - 홈 에이전트는 무상 ARP 메시지를 전송하여 자신의 데이터 링크 계층 주소가 이동 장비의 주소와 같음을 알림

모바일 IP

- 모바일 IP 비효율
  - 전송자가 이동 장비의 홈 네트워크에서 얼마나 떨어져 있는가에 따라 비효율 정도가 결정됨
- 모바일 IP 보안 문제
  - 모바일 IP는 공개된 전송으로 도청의 가능성이 있음
  - 재전송 공격

Thanks!

이 태 양 (taeyang@pel.sejong.ac.kr)