TCP/IP 완벽 가이드

- II-5부 IP관련 기능 프로토콜 -

명 세인(sein@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

목 차

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

네트워크 주소변환 프로토콜

- IP NAT 개요
  - NAT: The IP Network Address Translator
    - 공인 IP를 공유하여 통신을 하는데 문제없이 변환
  - IPv4 클래스 비사용 주소지정은 32bits의 한정된 주소의 고갈 속도를 느리게 하는 정도, 근본적으로 해결하지 못함
  - IP주소가 희귀해 질수록 비싸짐
  - 네트워크가 커지면서 악성 사용자가 증가, 보안위협이 생김
  - 대부분의 호스트는 클라이언트, 동시에 접근하는 상황은 많이 없음

네트워크 주소변환 프로토콜

- IP NAT 개요
  - NAT라우터는 IP 데이터그램을 라우팅 하면서 사설 네트워크에서 온 데이터그램을 공인 IP주소로 변환
  - IP NAT의 장점
    - 대량의 호스트가 공인 IP주소를 공유
    - 공인 IP주소를 필요로 하지 않아 확장이 용이
    - 관리자의 통제력이 강화됨
    - 공인 IP 변경시 내부주소 수정이 불필요
    - NAT변환시 외부에서 클라이언트 공격이 어려움

네트워크 주소변환 프로토콜

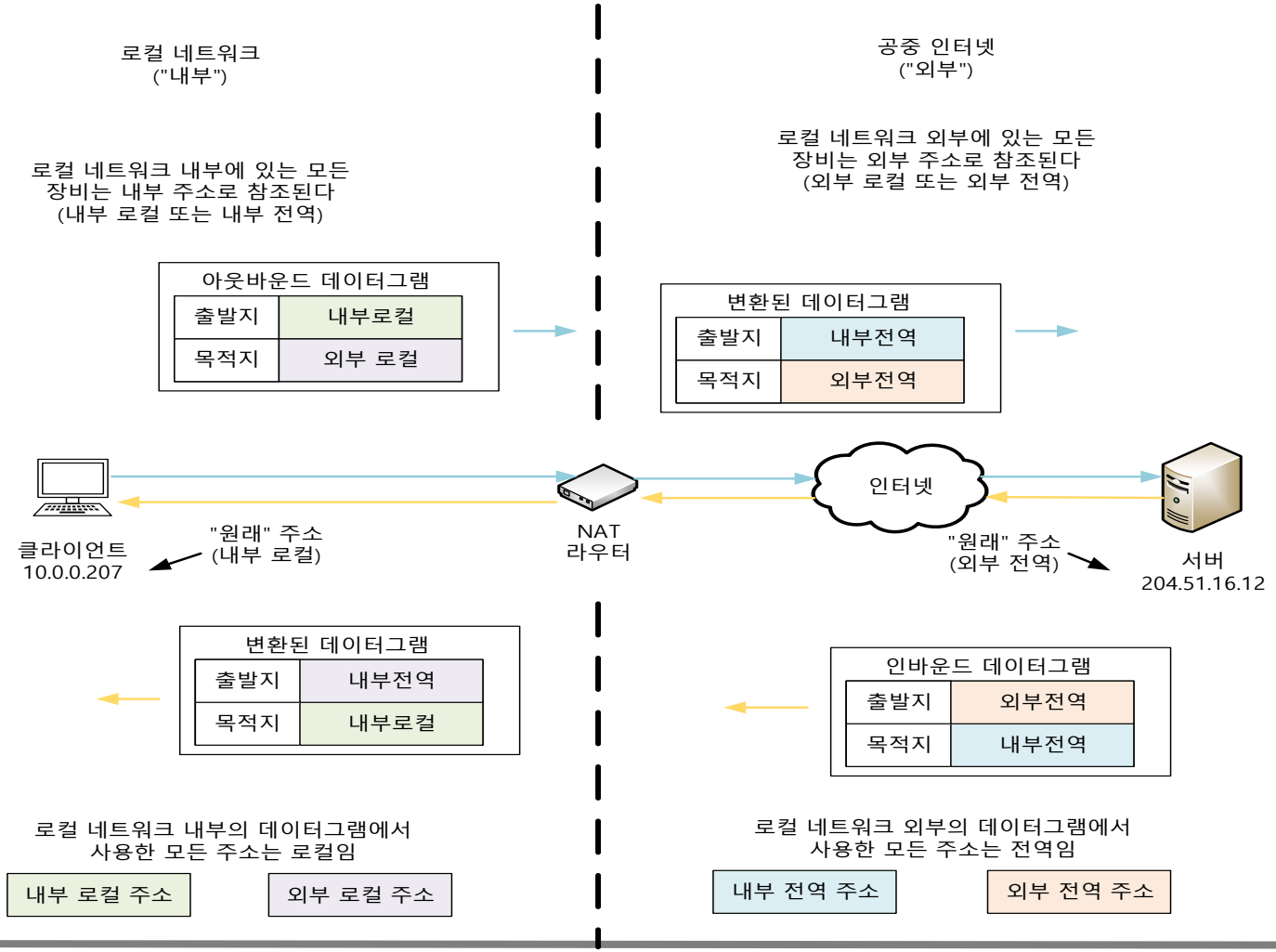
- IP NAT 개요
  - IP NAT의 단점
    - NAT이라는 추가적인 시스템이므로 복잡해짐
    - 호스트에 IP를 부여하지 않기 때문에 일부 애플리케이션 사용 불가
    - 보안 프로토콜(IPsec)과 호환문제가 있음
    - 클라이언트에 IP가 없으면 P2P설정 등이 어려움
    - 주소변환에 의한 성능이 저하됨

네트워크 주소변환 프로토콜

- IP NAT 주요용어
  - 내부주소 (Inside Address): NAT를 사용하는 장비는 모두 내부네트워크, 로컬 네트워크를 가리키는 모든 주소
  - 외부주소 (Outside Address): 로컬 네트워크가 아닌 주소
  - 로컬주소: 내부 네트워크의 데이터그램에 나타나는 주소
  - 전역주소: 외부 네트워크의 데이터그램에 나타나는 주소

네트워크 주소변환 프로토콜

- IP NAT 주요용어
  - IP NAT 내부/외부/로컬/전역 그림

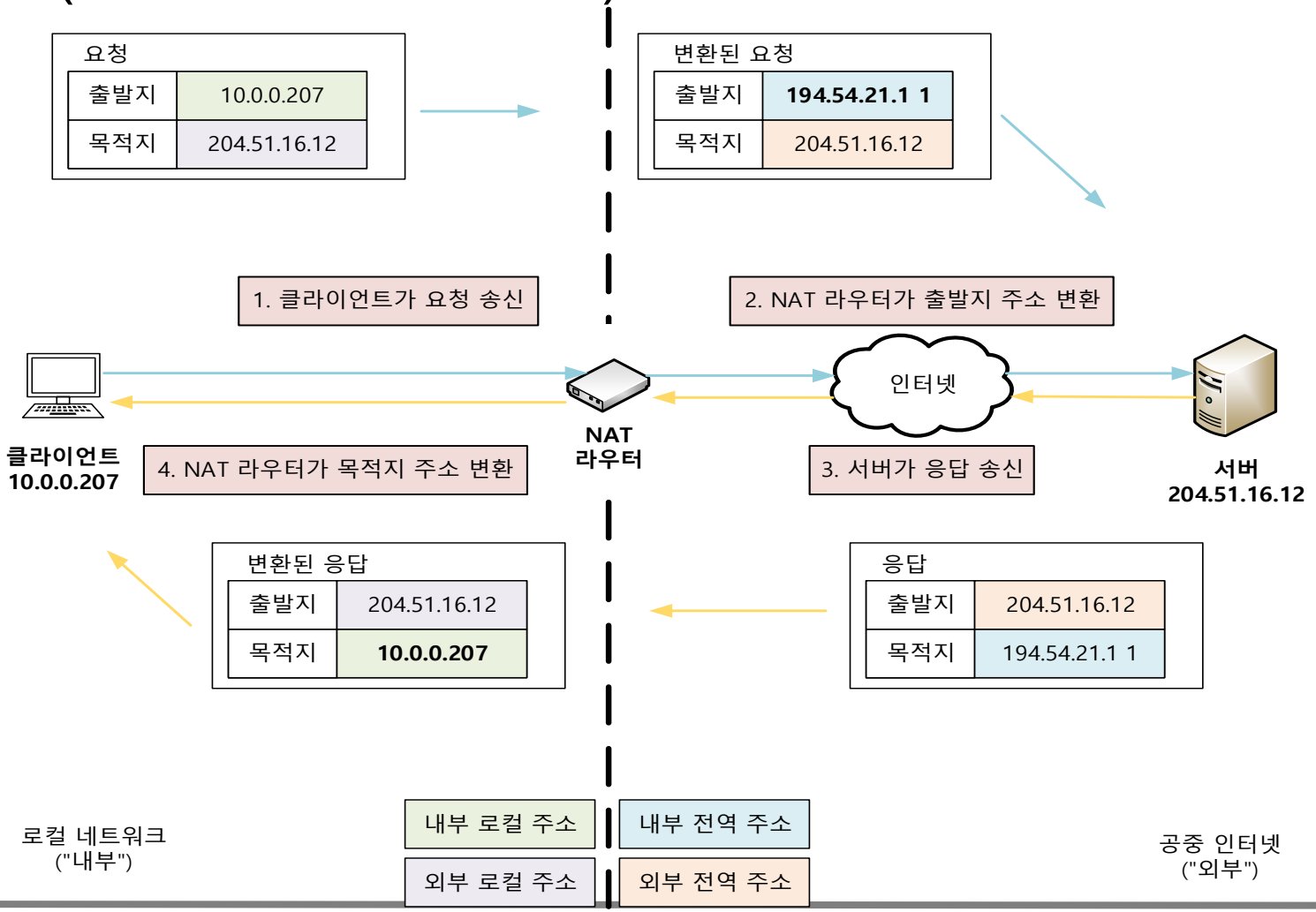


네트워크 주소변환 프로토콜

- IP NAT 주소 매핑
  - 정적 매핑: 전역과 로컬 사이의 주소 관계를 고정으로 매핑 되도록 설정, 수동으로 관리
  - 동적 매핑: 전역과 로컬 주소 표현을 필요할 때 마다 즉시 생성, 사용이 끝나면 버려짐, 자동으로 관리 가능
    - 다수의 내부 장비가 내부 전역 주소 Pool을 이용할 때 사용
  - 매핑을 복합적으로 사용할 수 있음 (중복 문제)

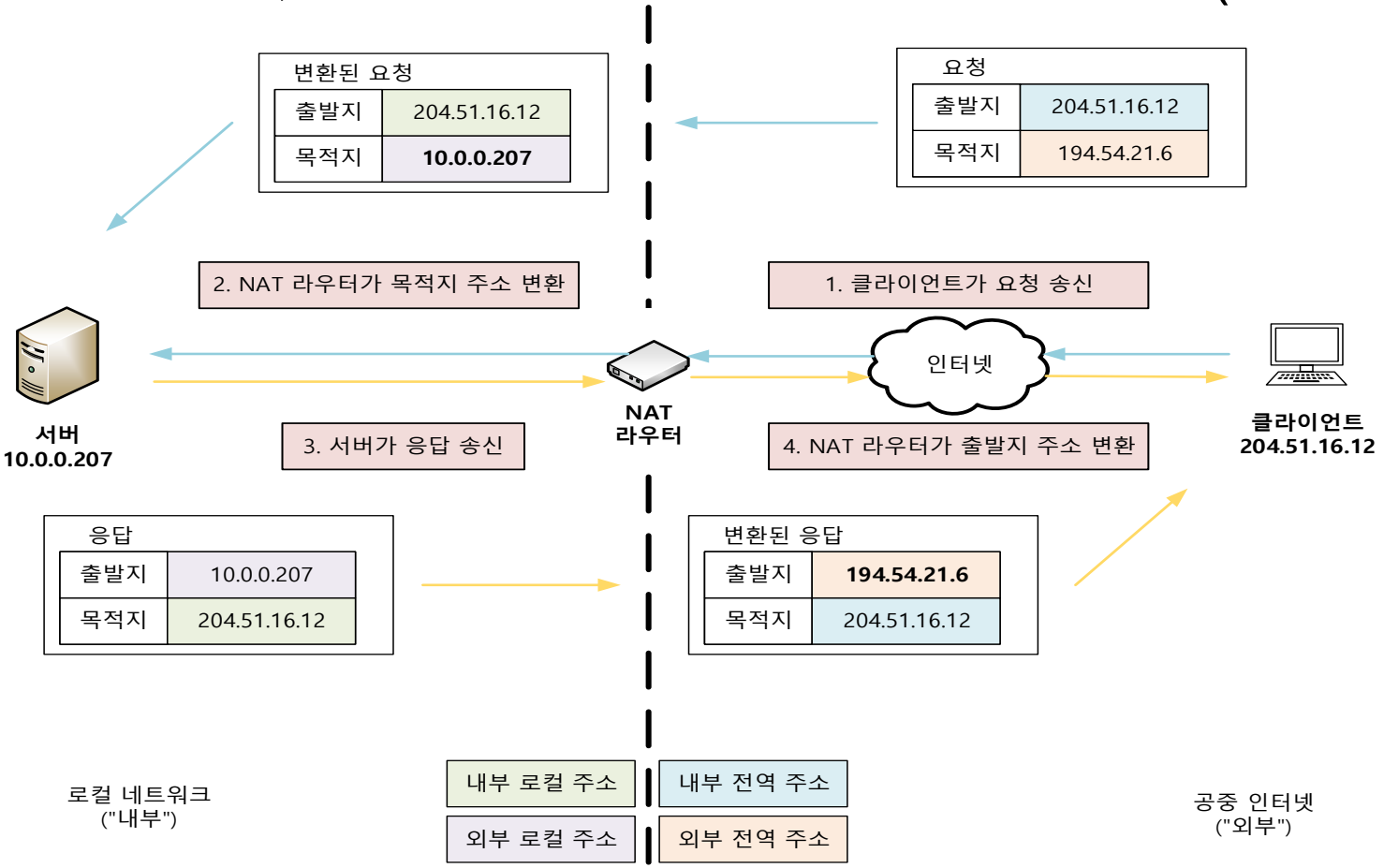
네트워크 주소변환 프로토콜

- IP NAT 단방향 동작
  - 단방향(전통적/아웃바운드) NAT의 동작 그림



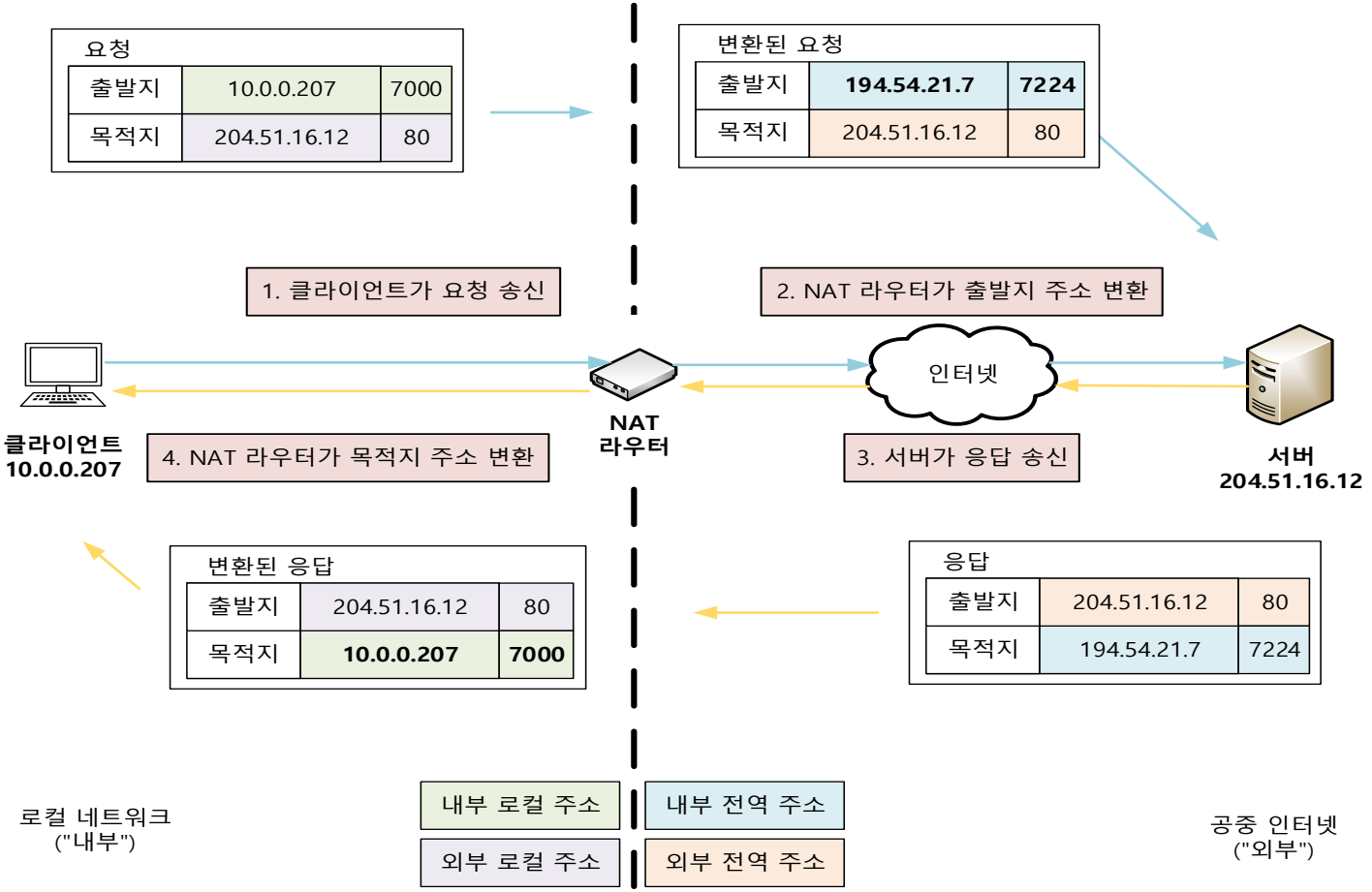
네트워크 주소변환 프로토콜

- IP NAT 양방향 동작
  - 양방향 (two-way/인바운드) NAT의 동작 그림
    - DNS를 사용, 외부 장비가 내부 장비에게 요청 (DNS 매핑)



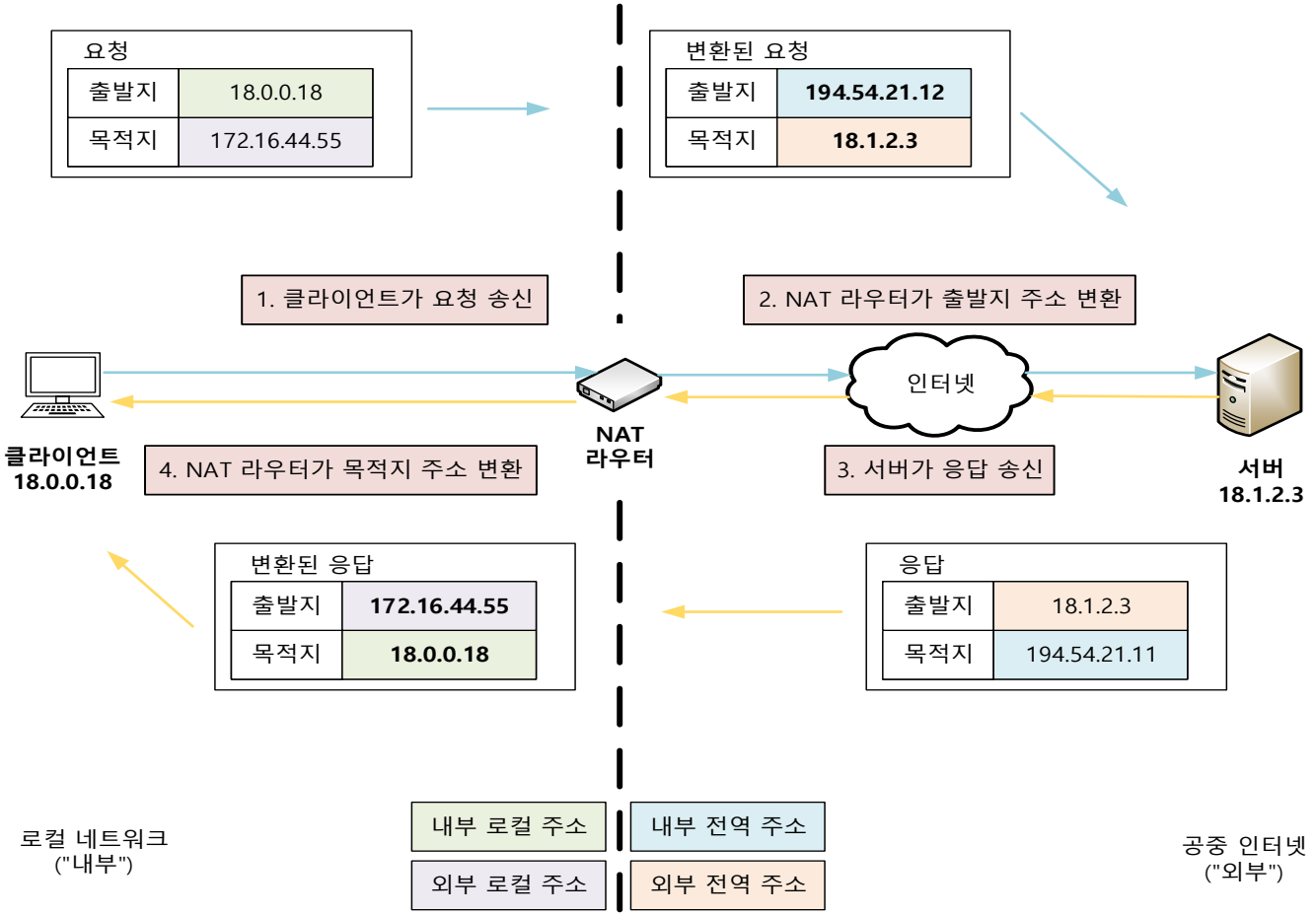
네트워크 주소변환 프로토콜

- IP NAT 포트기반 동작
  - 포트 기반 (과부하) NAT의 동작 그림
    - 사용할 수 있는 공인 IP주소가 전부 차있는 경우



네트워크 주소변환 프로토콜

- IP NAT 중복 동작
  - 중복 NAT/2회 NAT의 동작 그림
    - 내부 네트워크 주소와 외부 네트워크 주소가 겹칠 경우



네트워크 주소변환 프로토콜

- IP NAT 호환성과 특수처리
  - TCP/UDP 체크섬 계산
    - 헤더 IP주소 변경시 IP헤더 체크섬을 재계산 해야 함
  - ICMP 조작
    - ICMP는 원본 IP 헤더를 포함
    - NAT는 특정 ICMP 메시지를 조사하여 주소를 변경 해야 함
  - IP 주소를 내장하는 어플리케이션
  - 포트 변환에서의 추가적 문제
  - 주소나 포트 번호 변경에 의한 파급 효과
  - IPsec에서의 문제

목 차

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

IP Security

- IPsec 개요
  - IP 인터네트워크에서 보안을 보장하는 명확한 기능 부재
  - 과거 네트워크 크기가 작았을 때 프로토콜에 보안을 추가하기 보다는 네트워크가 있는 건물을 보안함
  - IPsec의 기능
    - 데이터 암호화
    - 메시지 무결성 인증
    - 재전송 방지
    - 보안 요구에 맞는 알고리즘, 키 협상 지원
    - 서로 다른 네트워크 요구에 맞춘 보안모드 (Tunnel, Transport)

IP Security

- IPsec 기능 (IPsec 프로토콜 슈트)
  - 핵심 프로토콜 표

IPsec 핵심 프로토콜	기능
IPsec 인증 헤더 (AH: Authentication Header)	무결성 인증 제공, 재전송 공격에 대한 인증 제공
보안 페이로드 캡슐화 (ESP: Encapsulating Security Payload)	암호화하여 기밀성 제공

  - 보조 구성요소 표

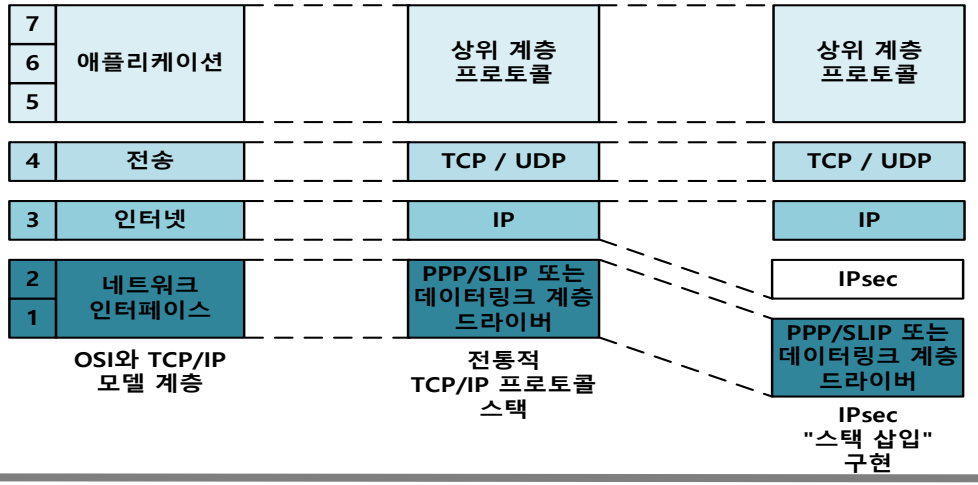
보조 구성 요소	기능
암호화/해싱 알고리즘	Message Digest 5 (MD5) Secure Hash Algorithm 1 (SHA-1)
보안 정책, 연관, 관리	장비간 보안 설정을 교환
키 교환 프레임워크와 방법	인터넷 키 교환 (IKE: Internet Key Exchange)

IP Security

- IPsec 구조와 구현방법
  - IPsec을 실제로 적용하는 구현 방법에 차이가 있음
    - IP의 버전
    - 애플리케이션 요구사항
    - 기타 요인
  - 종단 호스트 구현
    - 모든 호스트 장비에 구현하여 유연성과 보안성을 가장 높임
    - 모든 호스트에 구현하는 비용이 듦
  - 라우터 구현
    - 비교적 소수의 라우터에 구현
    - 로컬 네트워크 내부 보안은 보장하지 못함

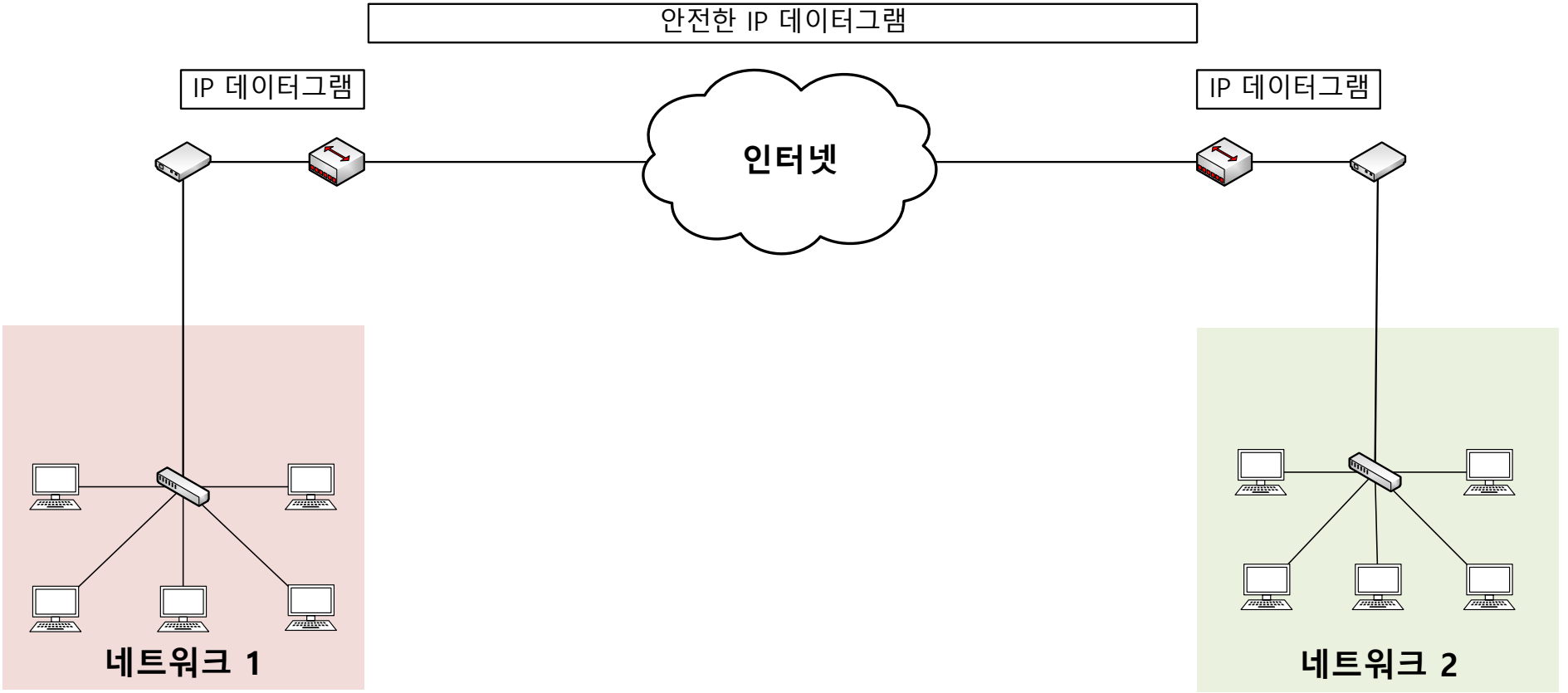
IP Security

- IPsec 구조와 구현방법
  - TCP/IP 프로토콜 스택과 결합하는 방법
    - 통합 구조
      - IP 자체에 통합하여 일반 IP처럼 지원
      - 추가적인 하드웨어계층이 필요치 않음
      - IPv4의 경우 IP구현을 변경 해야 함
    - 스택 삽입 구조 (BITS: Bump In The Stack)
      - IP와 별도의 구조 계층으로 존재, 추가적인 스택 기능을 함



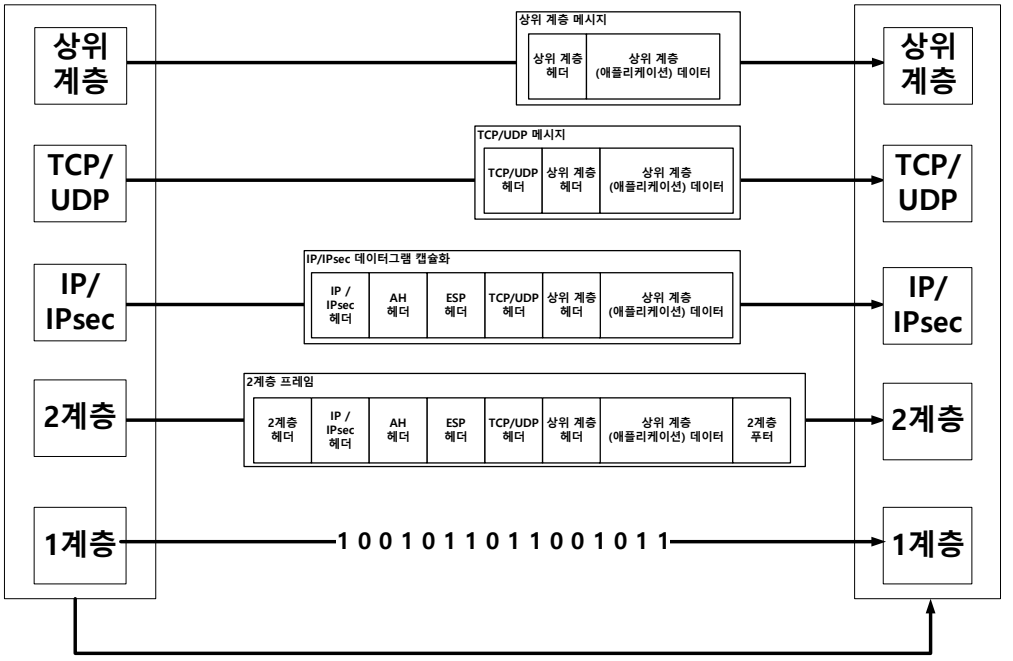
IP Security

- IPsec 구조와 구현방법
  - TCP/IP 프로토콜 스택과 결합하는 방법
    - 라인 삽입 구조 (BITW: Bump In The Wire)
      - IPsec 서비스를 제공하는 하드웨어 장비를 추가



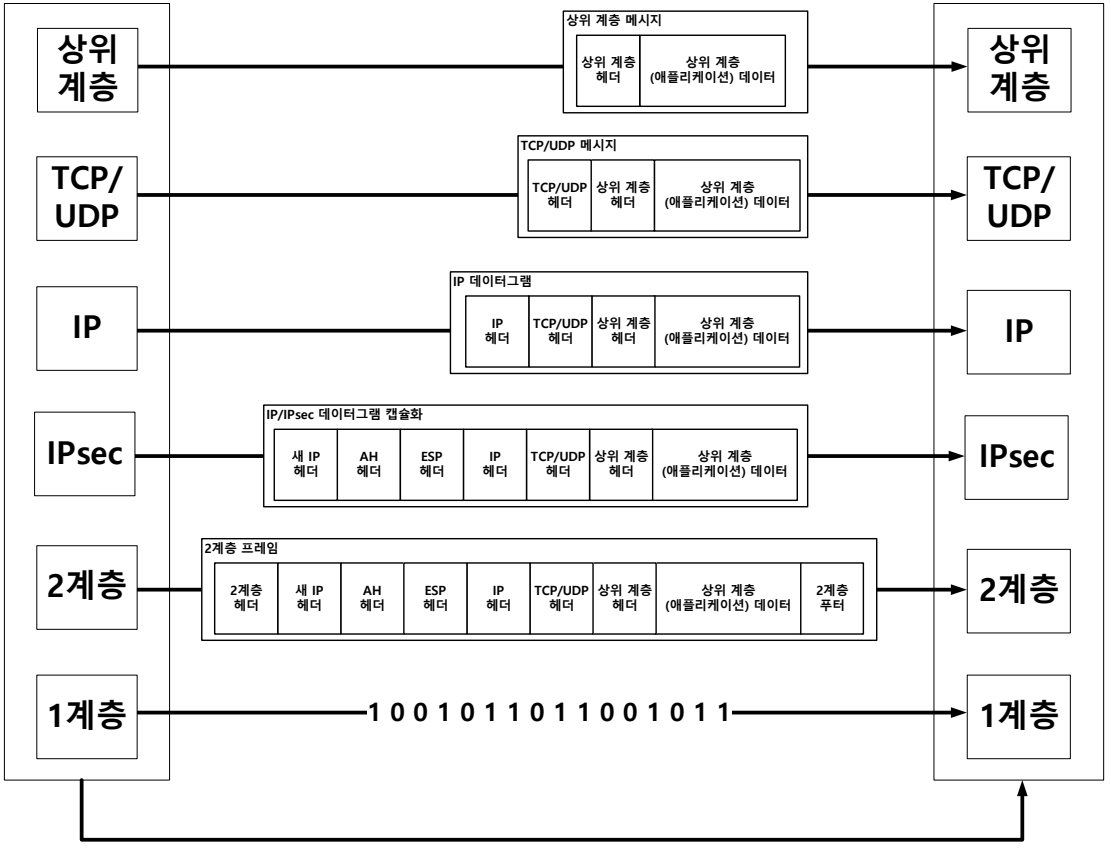
IP Security

- IPsec 모드: 전송과 터널
  - 세가지 기본 구현 구조에서 사용할지는 IPsec가 동작하는 구체적인 방법에 영향을 줌
  - 전송 모드 (Transport Mode)
    - 네트워크 계층과 같이 동작



IP Security

- IPsec 모드: 전송과 터널
  - 터널 모드 (Tunnel Mode)
    - 추가적인 캡슐화 진행
    - 계층이 추가된 것처럼 동작



IP Security

- IPsec 보안 구성 요소
  - 보안 연관, 보안 연관 데이터 베이스, 보안 정책, 보안 정책 데이터베이스, 선택자(Selector), 보안 인자 색인을 포함
  - 보안 정책
    - IPsec 구현에 내장된 규칙으로 적용되는 보안의 유형을 정의, 보안 정책 데이터베이스(SPD: Security Policy Database)에 저장됨
  - 보안 연관 SA (Security Association)
    - 특정 종류의 보안 연결을 설명하는 합의 되어야 할 보안 정보
    - 통신에 사용하는 보안 방법을 명시
    - 보안 연관 데이터베이스(SAD: Security Association Database)에 저장

IP Security

- IPsec 보안 구성 요소
  - 장비는 먼저 SPD를 검사
  - SPD의 보안 정책은 SAD의 특정 SA를 참조 할 수 있음
  - SA를 조회하고 내용에 따라 데이터그램 처리

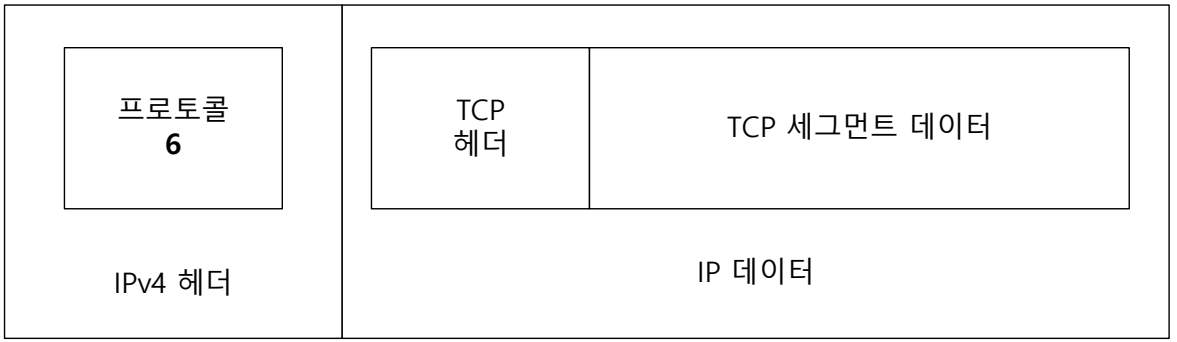
  - 선택자 (Selector)
    - IPsec는 각 SA가 자신이 적용될 데이터그램을 선택하기위한 규칙 모음을 정의
    - 이러한 규칙모음 각각을 선택자라 함

IP Security

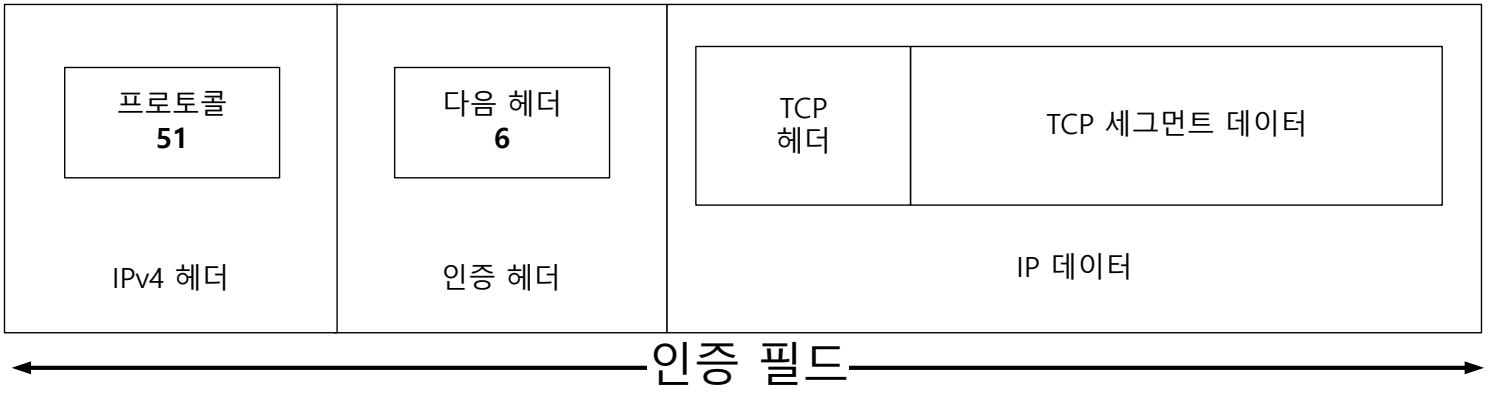
- IPsec 보안 구성 요소
  - 보안연관 트리플과 보안 인자 색인
    - 장비가 안전한 통신을 하기 위해서는 SA를 수립 해야함
    - SA는 단방향 이므로 각각이 인/아웃바운드 트래픽중 하나를 담당 (보안 수준이 방향에 따라 다를수 있음)
    - SA는 이름대신 트리플 이라 불리는 세 개의 인자 모음
      - 보안 인자 색인
        - 연결된 장비의 특정 SA를 유일하게 식별하기 위해 선택된 32비트 수
      - IP 목적지 주소
        - SA가 수립된 장비의 주소
      - 보안 프로토콜 식별자
        - 연관이 AH를 위한 것인지 ESP를 위한 것인지 지정
        - 둘 다 사용하는 경우 각각 별도의 SA를 지정

IP Security

- IPsec 인증 헤더 (AH)
  - 인증 헤더 구조 (전송모드)



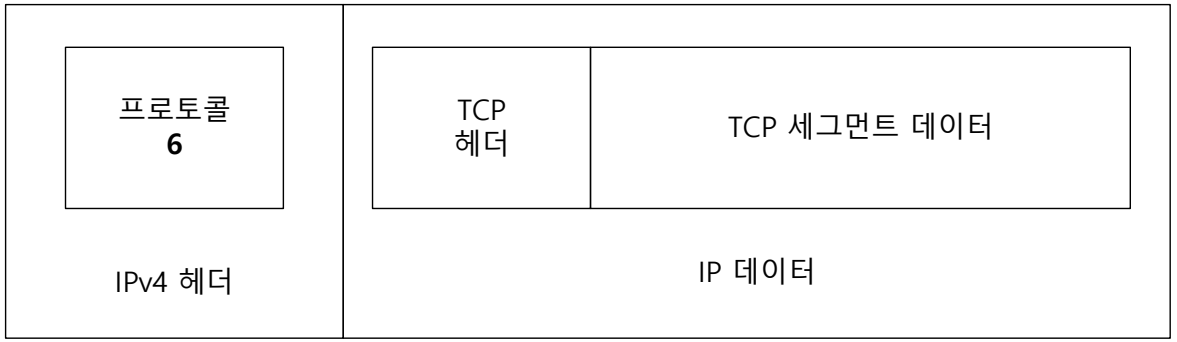
원본 IPv4 데이터그램 포맷



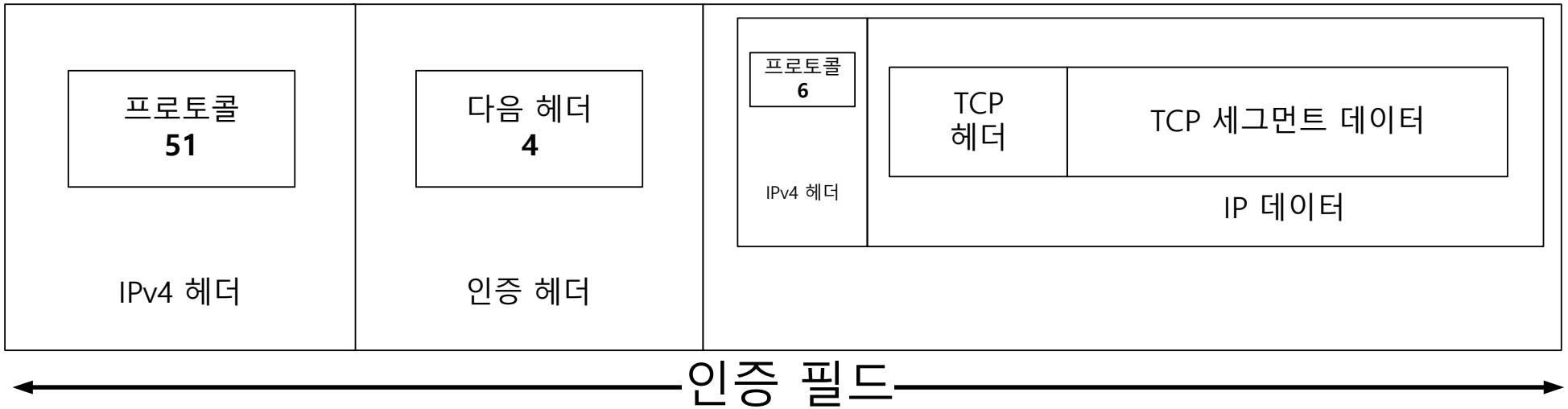
원본 IPv4 AH 데이터그램 포맷 – IPsec 전송모드

IP Security

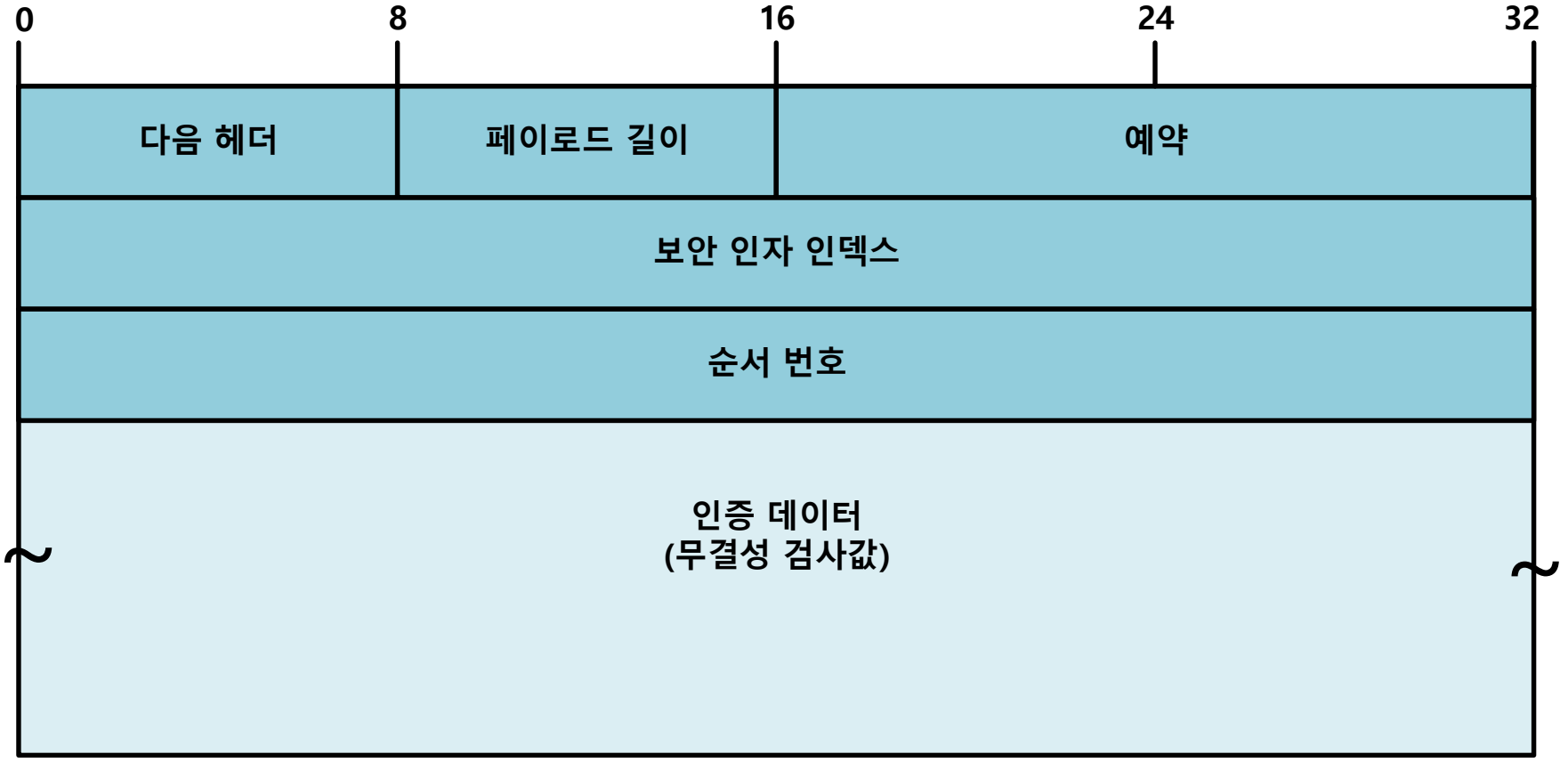
- IPsec 인증 헤더 (AH)
  - 인증 헤더 구조 (터널 모드)



원본 IPv4 데이터그램 포맷



- IPsec 인증 헤더 (AH)
  - 인증 헤더 포맷



IPsec AH를 포함하는 IPv4 데이터그램 포맷, 인증 헤더(AH) 포맷

IP Security

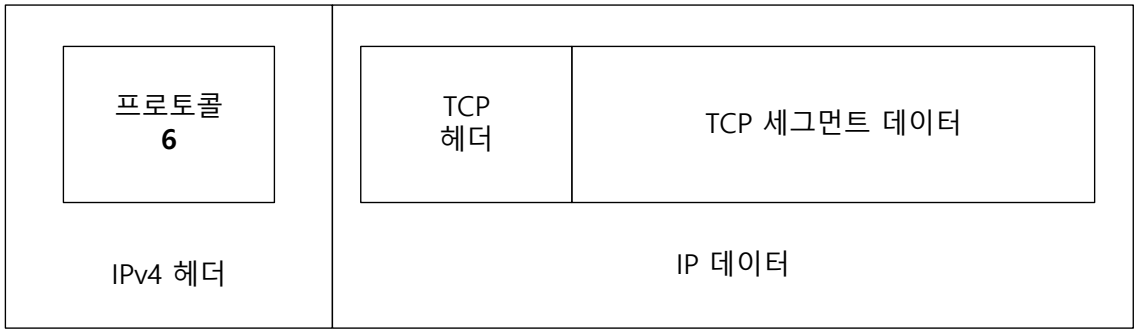
- IPsec ESP
  - 기밀성 제공
  - ESP 헤더
    - 보안 인자 인덱스와 순서번호(Sequence Number)
  - ESP 트레일러
    - 암호화된 데이터 뒤에 위치
    - 패딩, 패딩 길이 필드를 이용해 32비트 배수로 맞춤
  - ESP 인증 데이터
    - AH 프로토콜과 유사한 방식으로 계산되는 ICV를 포함

IP Security

- IPsec ESP
  - 3가지 기본 단계로 나뉨
    - 헤더계산
      - IPv4: AH와 같이 ESP 헤더 필드는 일반 IPv4 헤더 뒤에 위치
      - 전송모드는 IP 헤더 뒤
      - 터널 모드는 원본 데이터 그램을 캡슐화 하는 새 IP 데이터그램의 헤더 뒤
    - 트레일러 계산과 위치
      - ESP 헤더를 빼고 암호화
    - ESP 인증 필드 계산과 위치
      - 선택적인 ESP 인증 기능이 쓰일 경우에는 전체 ESP 데이터그램에 대한 계산이 이루어짐
      - 계산 대상은 ESP 헤더, 페이로드, 트레일러를 포함

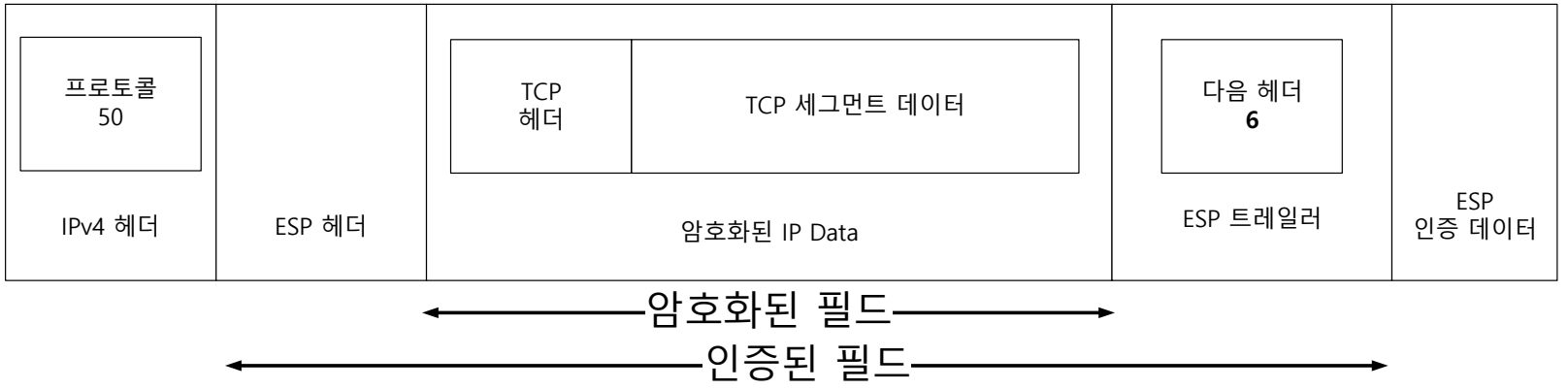
IP Security

- IPsec ESP
  - ESP 데이터 그램 포맷



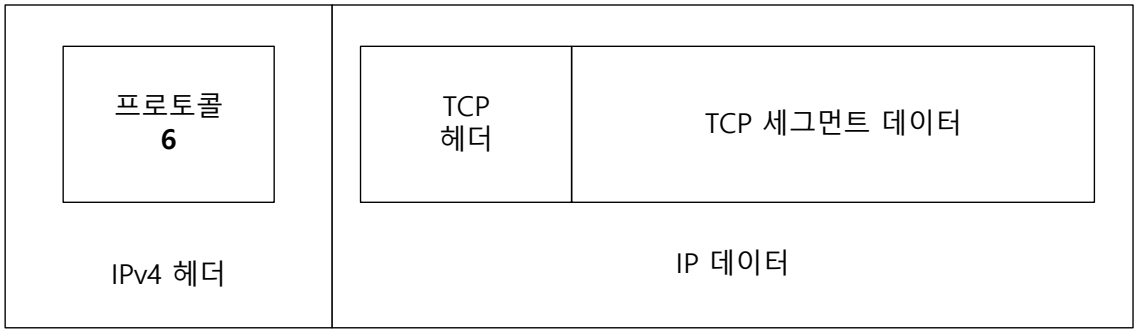
원본 IPv4 데이터그램 포맷

  - 전송모드 포맷

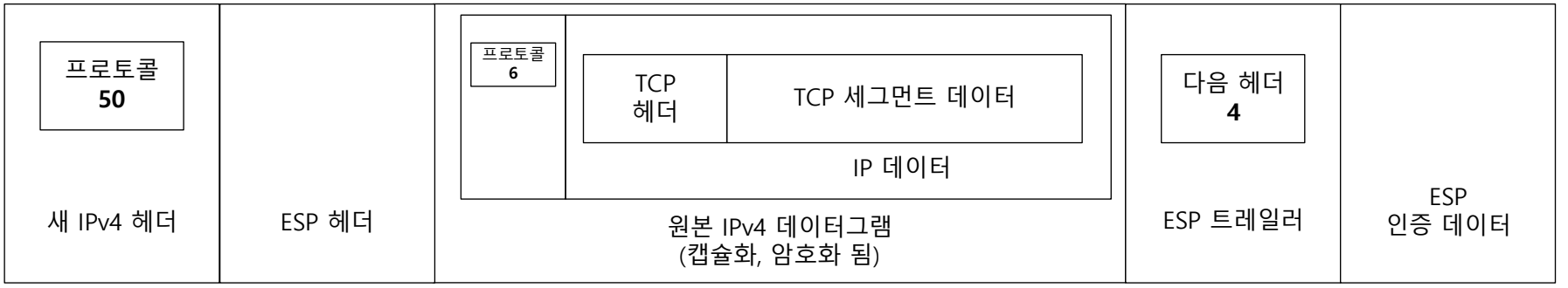


IP Security

- IPsec ESP
  - ESP 데이터 그램 포맷
    - 터널모드 포맷

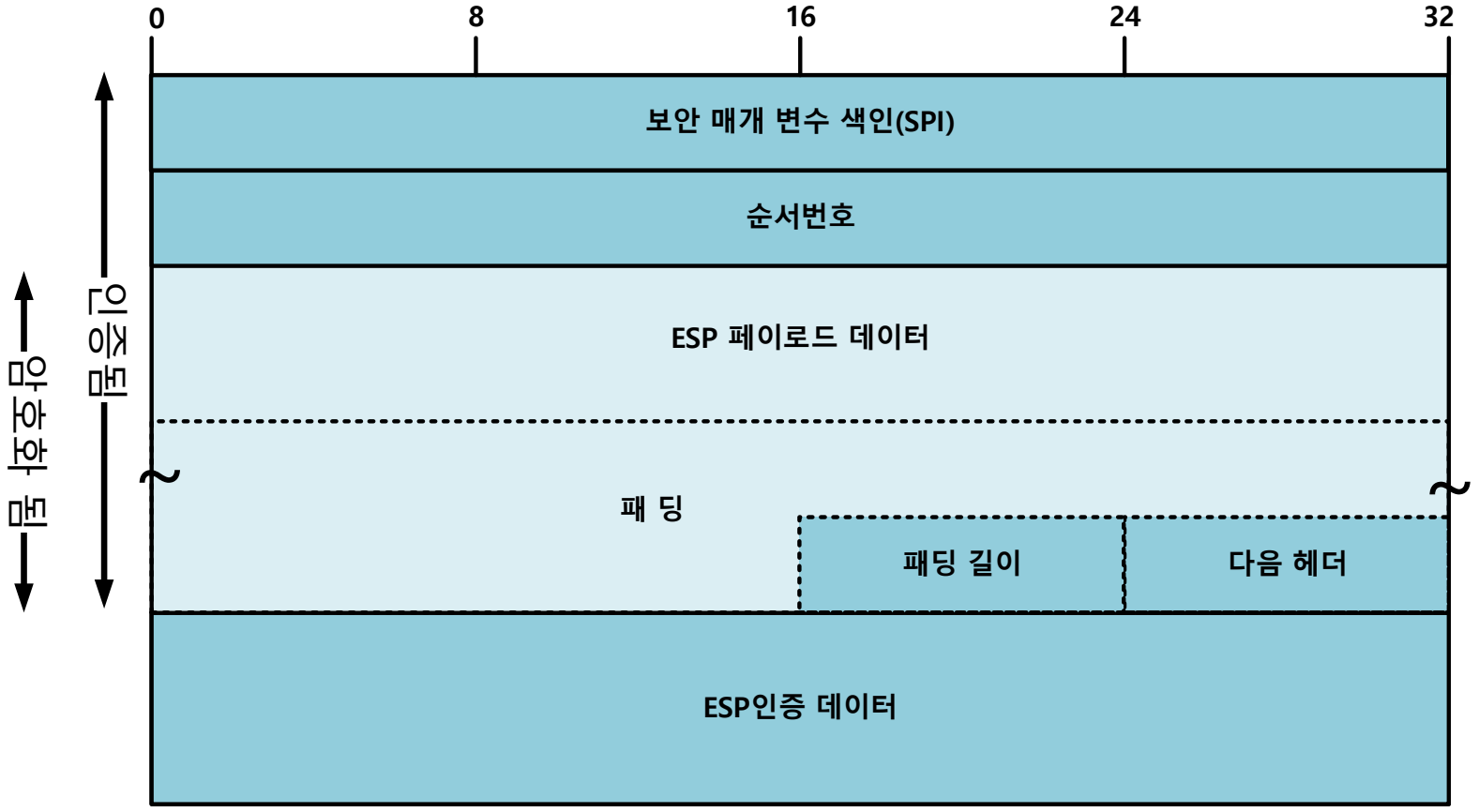


원본 IPv4 데이터그램 포맷



IP Security

- IPsec ESP
  - ESP 데이터 그램 포맷



IPsec ESP 포맷

IP Security

- IPsec IKE
  - 개요
    - 안전한 통신을 위해 필요로 하는 정보를 교환
      - IPsec 지원 장비가 SA를 교환하도록 하는 방식
      - 교환된 SA는 각 장비의 SAD에 추가
    - 인증 정보를 인코딩
    - 페이로드 암호화 수행의 암호 키

IP Security

- IPsec IKE
  - IKE 동작
    - OAKLEY와 SKEME의 일부분을 조합하여 ISAKMP로 교환

1. 정보를 어떻게 안전하게 교환할지에 동의하는 단계
   - 협상을 통해 ISAKMP 자체를 위한 SA인 ISAKMP SA를 생성
   - 이 보안연관으로 2단계에서 자세한 정보를 안전히 교환

2. 1단계 수립을 이용하여 기타 보안 프로토콜을 위한 SA를생성
   - 협상한 ISAKMP SA는 이후 협상에 쓰이는 다음 속성을 포함
     - DES(Data Encryption Standard) 같은 암호 알고리즘
     - 해시 알고리즘 (MD5, SHA1 등)
     - 인증 방법 (미리 공유한 키를 통한 인증 등)
     - Diffie-Hellman 그룹

목 차

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

모바일 IP

- 모바일 IP 개요
  - 모바일 컴퓨팅이 증가하면서 일반적인 IP 주소지정 방법이 이동환경을 잘 처리하지 못함
  - 네트워크ID와 호스트ID로 구별하는 주소체계에서 이동 장비가 선택할 수 있는 방안은 두 가지
    - IP 주소 변경
      - 주소를 바꿀 때마다 사람이 관여
      - 사용하던 모든 연결을 끊어야 함
      - 바뀐 주소를 다시 알리기가 힘듦
    - IP 라우팅과 주소 간의 연결 끊기
      - 네트워크 ID에 따라 라우팅하는 것이 아닌 전체 주소를 보고 라우팅
      - 이동컴퓨터에 대한 라우팅 정보가 과다 하게되어 테이블 관리 문제

모바일 IP

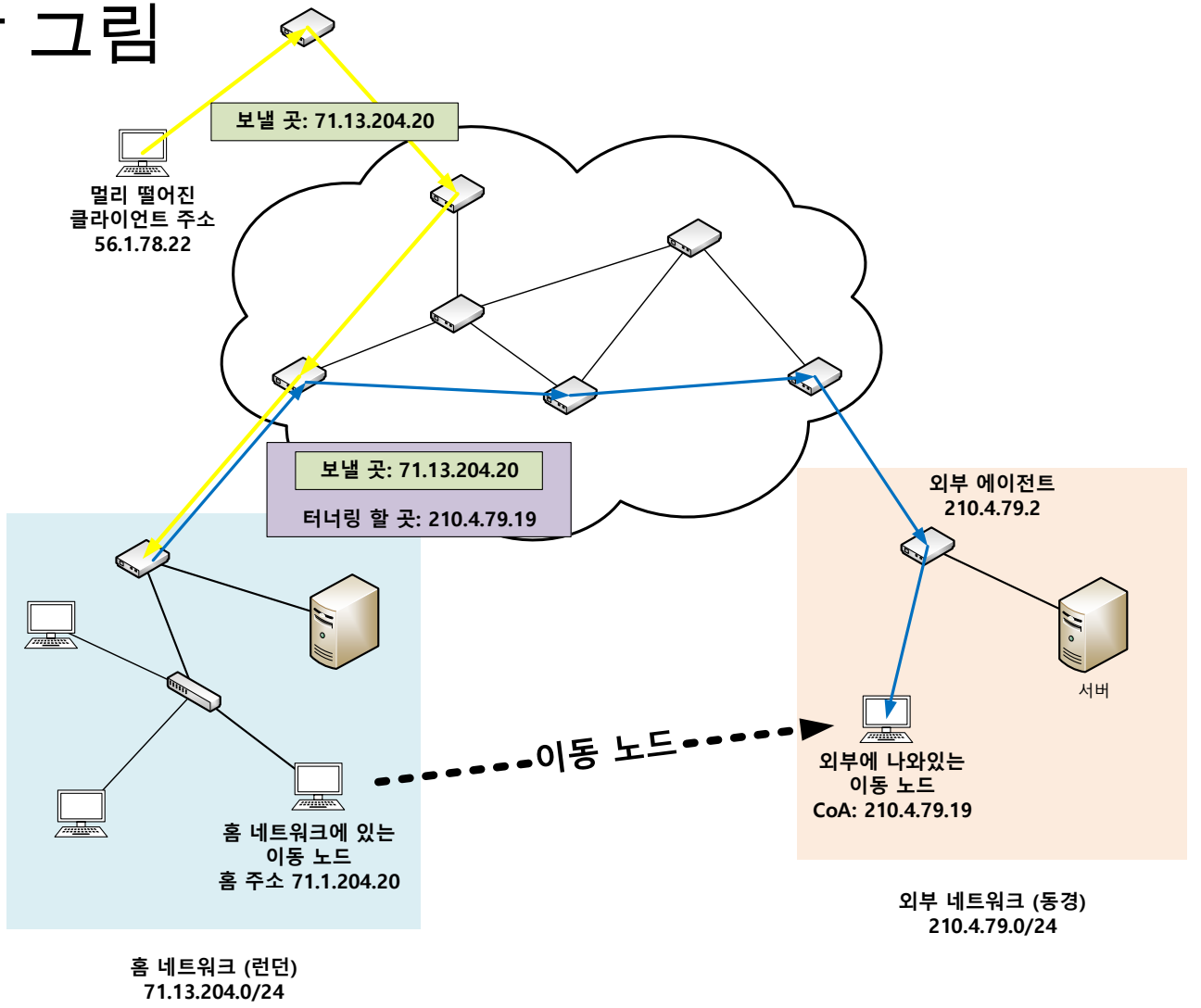
- 모바일 IP 개요
  - 모바일 IP
    - 기존 장비 주소를 사용, 이동시 중간이 없음
    - 새로운 주소지정, 라우팅 방법이 불필요
    - 상호 호환: 기존 장비는 모바일 IP의 동작을 몰라도 문제 없음
    - 계층 투명성: 모바일 IP 영향은 네트워크 계층에만 적용
    - 하드웨어 변경 최소화: 모바일 IP에 관련된 장비와 소프트웨어만 변경
    - 확장성: 어떤 네트워크로 이동해도 사용가능
    - 보안: 메시지를 리다이렉트(Redirect)하여 불법 노드가 문제를 일으키지 안도록 함

모바일 IP

- 모바일 IP 개요
  - 모바일 IP의 한계
    - 무선 환경에서는 한계를 가짐
      - 1초에 1번 이상 네트워크를 옮기지 않는 장비
      - 모바일 IP 작업에 따른 부하를 처리 할 수 있어야함
    - 고정 IP를 갖는 장비가 대상임
      - 장비는 자신의 홈 네트워크와 원래 IP 주소를 알아야함
        - DHCP(Dynamic Host Configuration Protocol)로 IP를 얻는 장비는 모바일 IP 사용이 힘듦

모바일 IP

- 모바일 IP 개념
  - 모바일 IP 기본동작 그림



모바일 IP

- 모바일 IP 개념
  - 모바일 IP 장비 역할
    - 이동 장비
      - 네트워크를 이동하는 장비
    - 홈 에이전트(Home Agent)
      - 홈 네트워크의 라우터
      - 이동장비가 받을 데이터그램을 받아서 이동장비에게 전달
      - 추가 기능도 구현해야함
    - 외부 에이전트 (Foreign Agent)
      - 이동장비가 현재 사용중인 라우터
      - 모바일 IP기능을 구현

모바일 IP

- 모바일 IP 개념
  - 모바일 IP 기능
    - 에이전트 통신
      - 이동장비는 에이전트 발견 해야 함
      - 에이전트가 보내는 광고 메시지를 받아 자신이 어디인지 알아냄
      - 광고를 못 받으면 에이전트에게 광고 요청
    - 네트워크 위치 결정
      - 에이전트 발견 메시지 내용을 기반으로 자신의 위치 판단

모바일 IP

- 모바일 IP 개념
  - 모바일 IP 기능
    - 장비가 외부로 이동한 경우
      1. CoA (Care-of-Address) 획득
         - 이동 장비는 CoA라는 임시 주소를 받음
         - 오직 목적지로 데이터 그램을 전달하는 용도
      2. 에이전트 등록
         - 이동장비가 외부인경우 홈 에이전트에게 데이터그램을 전달해 달라고 요청
         - 외부 에이전트가 중개자로개입 할 수 있음
      3. 데이터그램 전달
         - 홈 에이전트가 데이터 그램을 대신 받고 실제 이동 장비의 위치로 전달
         - CoA종류에 따라 직접 전달하거나 외부 에이전트에게 전송을 부탁 할 수 있음

모바일 IP

- 모바일 IP 주소
  - 홈 주소
    - 이동 장비에게 할당된 정상적인 고정(공인) IP주소
  - CoA (Care-of Address)
    - 이동 장비가 외부로 움직였을 때 사용하는 임시 주소
    - 일반적인 32bits IP 주소와 동일하지만 모바일 IP 에서만 사용

모바일 IP

- 모바일 IP 주소
  - CoA 유형
    - 외부 에이전트 CoA
      - 이동장비가 이동한 후 CoA가 외부 에이전트의 주소가 됨
      - 홈 에이전트가 CoA로 전송하면 외부 에이전트가 전달함

모바일 IP

- 모바일 IP 주소
  - CoA 유형
    - 공존 CoA (Co-Located Care-of-Address)
      - 모바일 IP 가 아닌 다른 기법을 사용해서 이동 장비에게 직접 할당된 주소를 의미 (수동, DHCP 등)
      - 공존 CoA를 사용하면 홈 에이전트가 직접 전송할 수 있음
    - 유형 의 차이
      - 외부: 주소 부족을 신경 안 씀, 해당 외부 네트워크의 모든 이동장비는 같은 CoA이다
      - 공존: 외부 에이전트가 없거나 연결을 오래 할 경우

모바일 IP

- 모바일 IP 에이전트 발견
  - 정상적인 IP장비는 전원을 키면 자신의 위치(네트워크)를 알지만 모바일 장비는 확신 할 수 없음
  - 에이전트 발견 과정
    - 에이전트/노드 통신
      - 이동 노드가 홈 에이전트와 접속을 시도
      - 에이전트에 대한 중요한 정보를 담은 메시지를 전송, 또는 노드가 에이전트에게 정보를 요청
    - 현재 위치 발견
      - 발견 과정을 종료하면 현재 네트워크 위치를 알 수 있음
    - CoA 할당
      - CoA를 사용하면 에이전트 발견 과정 중 이동 장비가 사용할 CoA 획득

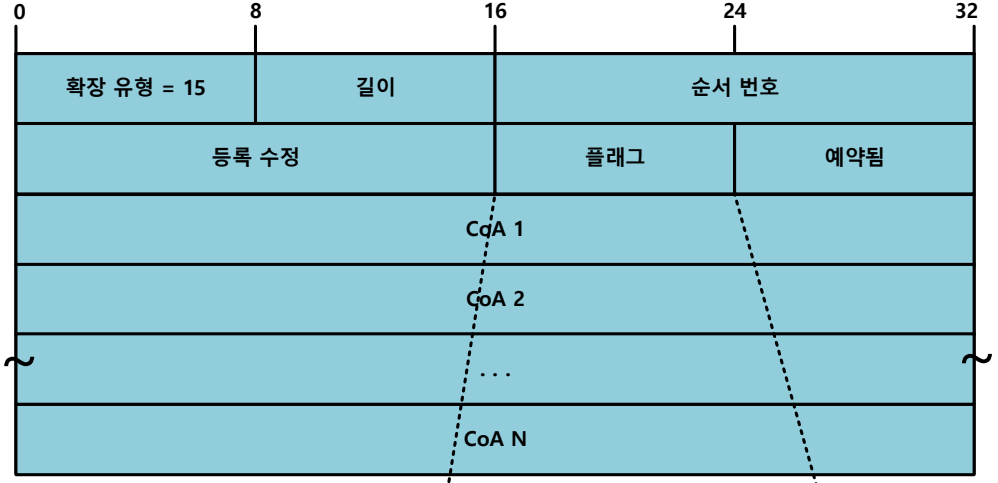
모바일 IP

- 모바일 IP 에이전트 발견
  - 에이전트 광고, 에이전트 요청 메시지
    - IP 라우터 발견 과정이 정의되어 있음
      - 라우터 광고 메시지
      - 라우터 요청 메시지
    - 에이전트 요청 (Agent Solicitation)
      - 모바일 IP장비가 로컬 에이전트에게 에이전트 광고 메시지를 요청
      - 요청 메시지 포맷
        - 라우터 요청메시지에서 바뀐것이 없음
        - 일반 라우터가 받으면 일반 광고, 모바일IP 라우터가 받으면 더긴 에이전트 광고 메시지를 보낼것

모바일 IP

- 모바일 IP 에이전트 발견
  - 에이전트 광고, 에이전트 요청 메시지
    - 에이전트 광고 (Agent Advertisement)
      - 모바일 IP로 활동 할 수 있는 라우터가 정기적으로 전송
      - 모바일 IP 관련 정보를 담은 하나 이상의 확장을 포함하는 라우터 광고 메시지임
      - 라우터 광고 메시지와 같은 포맷

모바일 IP 접두사 길이 확장 포맷



모바일 IP 이동 에이전트 광고 확장 포맷

모바일 IP

- 모바일 IP 홈 에이전트 등록과 등록 메시지
  - 이동 단말이 모바일 IP 동작을 위해 필요한 정보, 지시를 홈 에이전트와 주고 받음 (Home Agent Registration)
  - 이동 장비 등록 이벤트
    - 성공적으로 등록이 끝나면 이동성 바인딩(Mobility Binding)
    - 등록이 유지되는 기간에는 이동장비의 원래 홈 주소와 CoA가 결합
    - 등록 이동: 장비가 외부 네트워크에 도착하면 등록을 시작
    - 등록 해제: 다시 홈 네트워크로 돌아오면 전달 취소
    - 재등록: 외부에서 또다시 이동하거나, CoA가 바뀌면 이동 장비는 홈 에이전트에게 알려 등록을 수정

모바일 IP

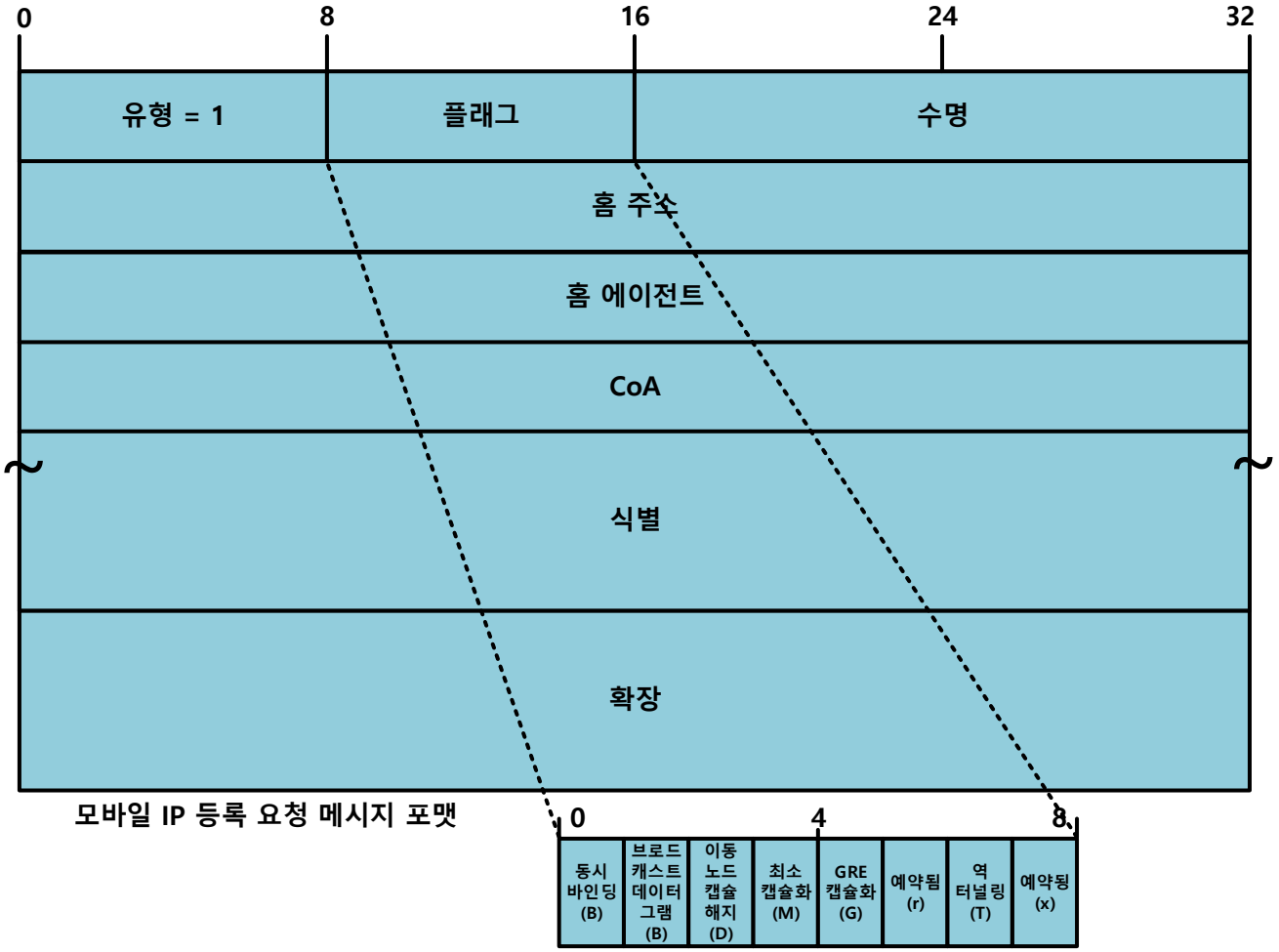
- 모바일 IP 홈 에이전트 등록과 등록 메시지
  - 등록 요청과 등록 응답 메시지
    - 이 두 메시지는 ICMP가 아니며 UDP 형식으로 동작
    - 에이전트는 434 포트에서 요청을 기다리고
    - 모바일 노드의 임시 포트로 응답을 돌려보냄
  - 등록 과정
    - 직접등록 (공존 CoA)
      1. 이동 장비가 등록 요청을 홈 에이전트에게 보냄
      2. 홈 에이전트는 이동 장비에게 등록 응답을 보냄

모바일 IP

- 모바일 IP 홈 에이전트 등록과 등록 메시지
  - 등록 과정
    - 간접 등록 (외부 CoA)
      1. 이동 장비가 등록 요청을 외부 에이전트에게 보냄
      2. 외부 에이전트가 등록 요청을 처리하여 홈 에이전트에게 보냄
      3. 홈 에이전트는 외부 에이전트에게 등록 응답을 보냄
      4. 외부 에이전트가 등록 응답을 받아 처리하고 이동 장비에게 전송

모바일 IP

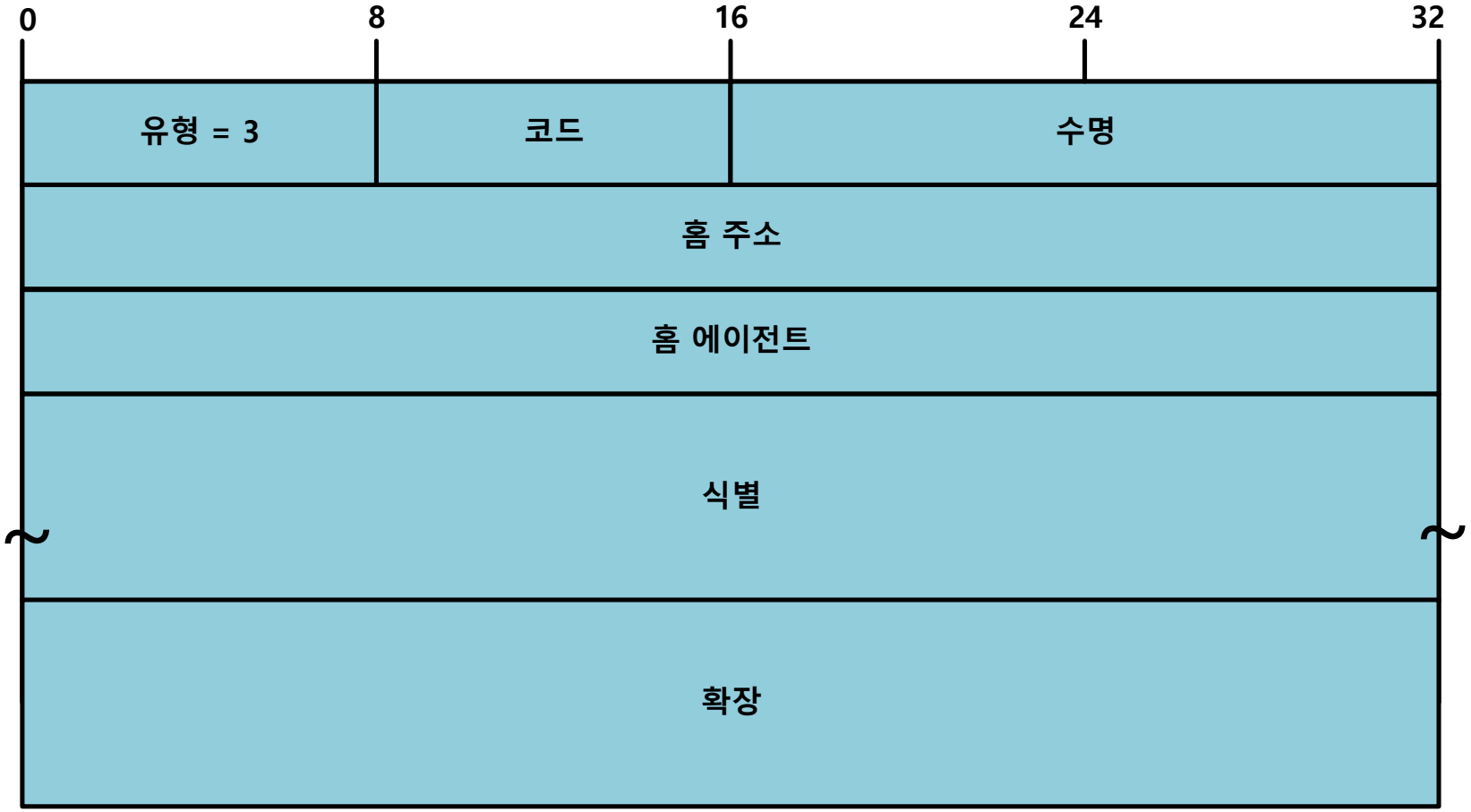
- 모바일 IP 홈 에이전트 등록과 등록 메시지
  - 등록 요청 메시지 포맷



모바일 IP 등록 요청 메시지 포맷

모바일 IP

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



모바일 IP 등록 응답 메시지 포맷

모바일 IP

- 모바일 IP 데이터 캡슐화, 터널링
  - 등록을 끝내면 통신 방법이 완전히 활성화 됨
  - 홈 에이전트가 데이터를 캡슐화 하여 전달
    - 데이터그램을 수정하지 않고 온전히 전송하기 위함
    - IP내 IP캡슐화 (IP Encapsulation within IP)
    - 캡슐화 장비와 디 캡슐화 장비 사이에 논리적인 터널을 만듬
  - 일반적인 모바일 IP 터널링
    - 외부 에이전트 CoA
      - 외부 에이전트에서 터널이 끝남, 캡슐화를 한번 벗겨내어 원본 데이터그램을 이동장비에게 (데이터링크 수준)전송
    - 공존 CoA주소
      - 이동 장비에서 터널이 끝나고 이동 장비가 캡슐화 헤더를 벗겨냄

모바일 IP

- 모바일 IP 데이터 캡슐화, 터널링
  - 터널링 요청
    - 이동장비는 요청 메시지를 전송 할 시(외부의 서버) 자신의 원래 IP 주소를 출발지 주소로 사용
    - 요청을 받은 노드는 응답을 출발지 IP주소로 응답
    - 홈 에이전트가 받아 이동 장비로 터널링
  - 삼각형 통신 구도

모바일 IP

- 모바일 IP 데이터 캡슐화, 터널링
  - 모바일 IP 역 터널링
    - 이동 장비가 데이터그램을 직접 인터넷에 전송 할 수 없을 수도 있음
    - 특정한 보안이 있는 네트워크로 이동한 경우 사용
    - 역 터널링 기법을 사용
      - 홈 네트워크와 이동 장비간 역 터널링이 구현 되어야 함
      - 총 4번의 전송 과정이 필요하므로 비효율적

모바일 IP

- 모바일 IP 와 TCP/IP 주소 결정 프로토콜
  - 모바일 IP가 제대로 구현되면 사용중인 홈 에이전트와 이동 장비간 통신은 원할
  - 하지만 홈에이전트 로컬네트워크의 다른 호스트가 이동장비에서 통신을 하면 문제가 생김 (이동 정보를 모를 수 도 있음)
  - 주소 결정 프로토콜 ARP 로 이동장비를 찾지만 이동 장비는 응답할 수 없음
  - 홈에이전트 로컬 호스트들이 이동 장비와 통신을 하려면 두 가지 작업이 필요

모바일 IP

- 모바일 IP 와 TCP/IP 주소 결정 프로토콜
  - ARP 프록싱 (ARP Proxing)
    - 홈 에이전트가 로컬 호스트 ARP에 응답
    - 호스트는 이동 장비에게 보내듯이 메시지를 전송
    - 홈 에이전트가 메시지를 받아 이동 장비에게 전달
  - 무상 ARP (Gratuitous ARP)
    - 홈 에이전트가 이동 장비의 IP주소에 대응하는 데이터 링크 주소가 홈 에이전트와 같다고 알림
    - 각각의 로컬 호스트들은 캐시를 수정

모바일 IP

- 모바일 IP 효율
  - 라우팅이 의미 없어질 경우 효율성이 떨어짐
    - 이동 장비에게 메시지를 보내는 장비가 같은 로컬인경우
  - 외부 네트워크에 오래 머무르거나 효율이 중요한 경우 모바일 IP 보다 다른 방법을 취할 수 있음

모바일 IP

- 모바일 IP 보안
  - 보통 무선이 많이 사용되는 모바일IP 의 경우 보안이 더 취약
  - 등록 요청과 등록 응답은 반드시 인증 되어야 함
    - 모든 모바일 IP 장비는 인증 기능을 지원해야 함
  - 재전송 공격 문제 등이 있음
  - 추가적으로 인증과 기밀성을 위해 IPsec를 사용 할 수 있음

보 충 목 차

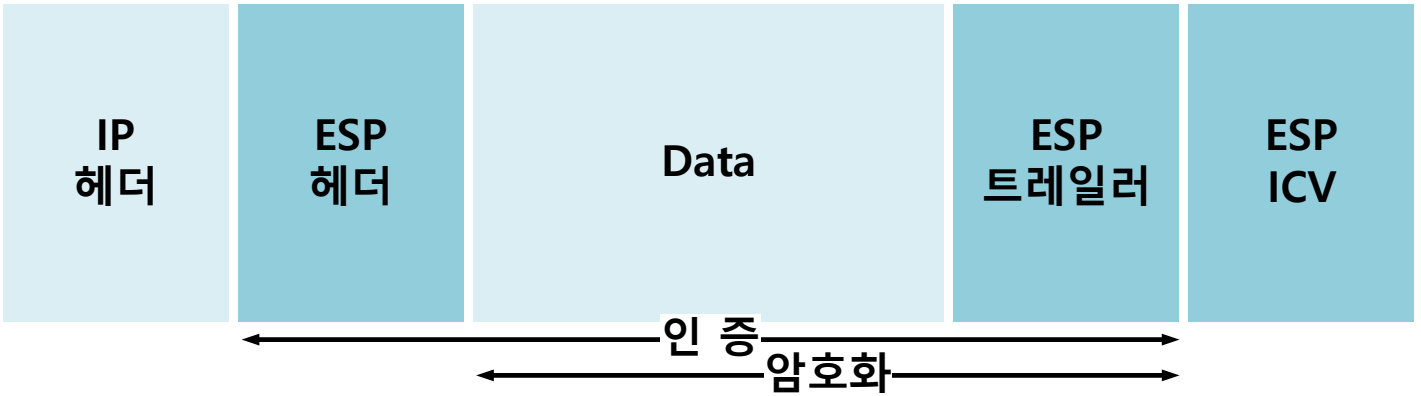
- IPsec 보충
  - 전송모드
  - 터널모드
  - 보안 연관, 보안 정책

IPsec 보충

- 전송 모드
  - 전송 모드의 AH 프로토콜

IPsec 적용 전

  - 전송 모드의 ESP 프로토콜

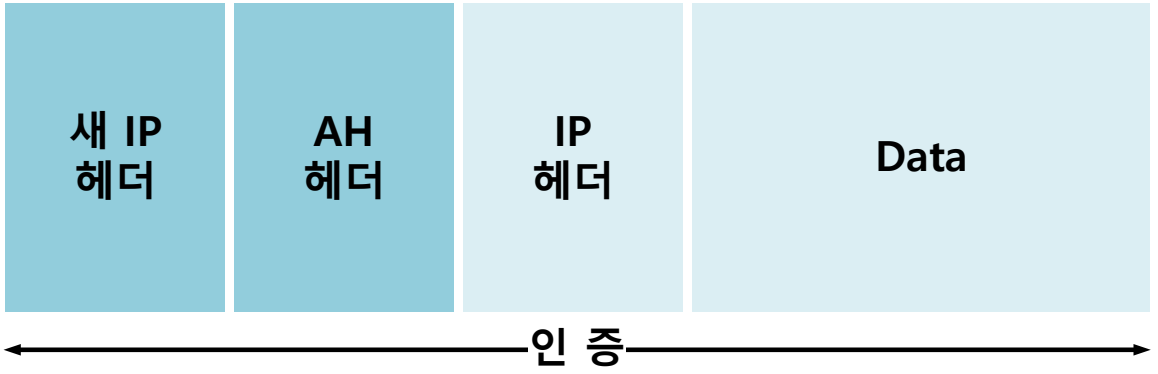


IPsec 보충

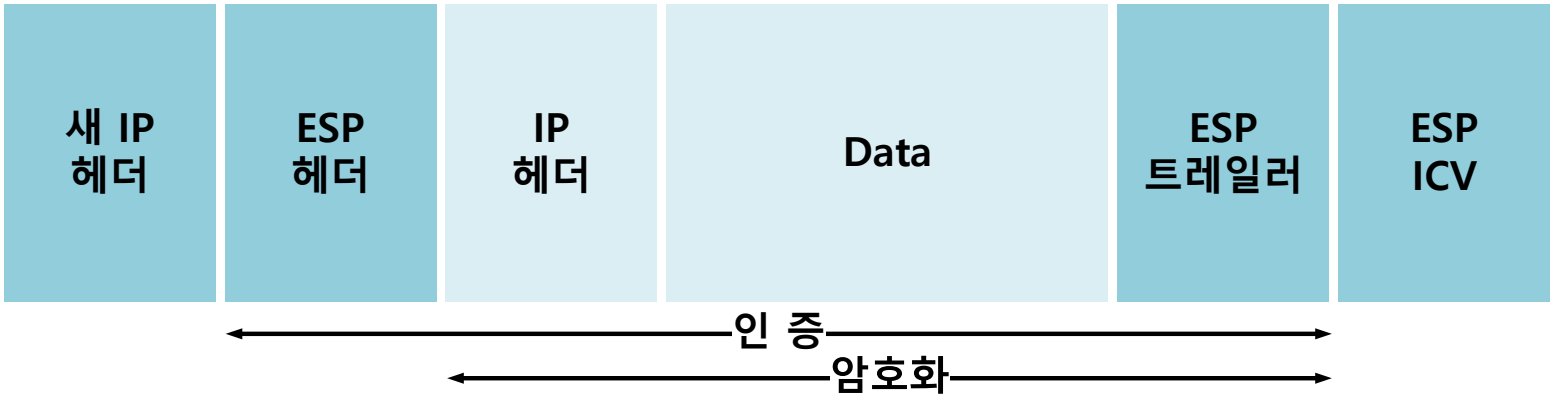
- 터널 모드

IPsec 적용 전

  - 터널 모드에서의 AH프로토콜



  - 터널 모드에서의 ESP프로토콜



IPsec 보충

- 보안 연관과 보안 정책
  - 보안 연관 (SA: Security Association)
    - 송/수신자 통신에 보안 서비스를 제공하기 위해 사전에 합의할 요소
    - 보안 연관 데이터 베이스에 저장됨
    - 보안 연관을 식별 할 매개변수
      - 보안 인자 색인 (SPI: Security Parameters index)
        - 데이터 그램에 적용된 SA를 식별
      - IP목적지 주소 (IP Destination Address)
        - SA가 수립된 장비의 주소 (최종 목적지 주소)
      - 보안 프로토콜 식별자 (Security Protocol Identifier)
        - AH/ESP를 사용중 인지 식별

IPsec 보충

- 보안 연관과 보안 정책
  - 보안 연관 데이터 베이스 (SAD: Security Association Database)

요소	의미
보안 매개변수 색인 (SPI: Security Parameter Index)	SA를 식별하도록 수신자가 선택한 32bits값
순서번호 카운터 (Sequence Number Counter)	순서 번호 필드를 위해 생성되는 32bits값
순서 계수기 오버플로우 (Sequence Counter Overflow)	순서 번호 카운터의 오버플로우에 대한 유/무를 가리키는 플래그
재전송 방지 윈도우 (Anti-Replay Window)	패킷 재전송 여부를 판별
AH 정보 (AH Information)	AH와 함께 사용되는 인증 알고리즘, 키, 키 사용주기와 관련 매개변수의 정보
ESP정보 (ESP Information)	ESP와 함께 사용되는 암호화/인증 알고리즘,, 키, 초기값, 키 사용 주기와 관련 매개변수의 정보
보안 연관 사용 주기 (Lifetime of this Security Association)	하나의 SA가 새로운 SA로 교체/종료되는 시간 간격 또는 바이트 카운트 값
IPsec 프로토콜 모드 (IPsec Protocol Mode)	전송/터널 모드 식별
경로 MTU (Path MTU)	

IPsec 보충

- 보안 연관과 보안 정책
  - 보안 정책 (Security Policy)
    - 패킷이 송/수신될 때 적용되는 보안의 유형을 정의
    - 보안 정책 데이터베이스에 저장됨 (SPD: security Policy Database)
      - 보안 정책 요소
        - 원격 IP 주소 (Remote IP Address)
        - 로컬 IP 주소 (Local IP Address)
        - 로컬과 원격 포트 (Local and Remote Ports)
        - 다음 계층 프로토콜 (Next Layer Protocol)
        - 동작 (Action)

감사합니다!