2023/03/07, 2023 1학기 보안기초 세미나

TCP/IP 완벽 가이드

- 2-5부 IP 관련 기능 프로토콜 -

강 민 채(minchae@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

목 차

- 보충
- NAT 프로토콜
- IP Security(IPsec) 프로토콜
- 모바일 IP 프로토콜

목 차

- 보충
- NAT 프로토콜
- IP Security(IPsec) 프로토콜
- 모바일 IP 프로토콜

보충

- 암호 운영 모드의 암호 방식
  - 블록 암호
    - ECB(Electronic CodeBook) 모드
    - CBC(Cipher Block Chaining) 모드
  - 스트림 암호
    - CFB(Cipher FeedBack) 모드
    - OFB(Output FeedBack) 모드
    - CTR(CounTeR) 모드

보충

- PPP(Point to Point Protocol)의 에러 탐지 방법
  - LCP(Link Control Protocol) 프레임
    - 에코 요청/에코 응답 메시지
      - 링크가 정상적으로 동작하는지 확인하기 위해 주고받는 메시지
    - 버림 요청 메시지
      - 루프백 상태가 아닌지 확인하기 위해 보내는 메시지

보충

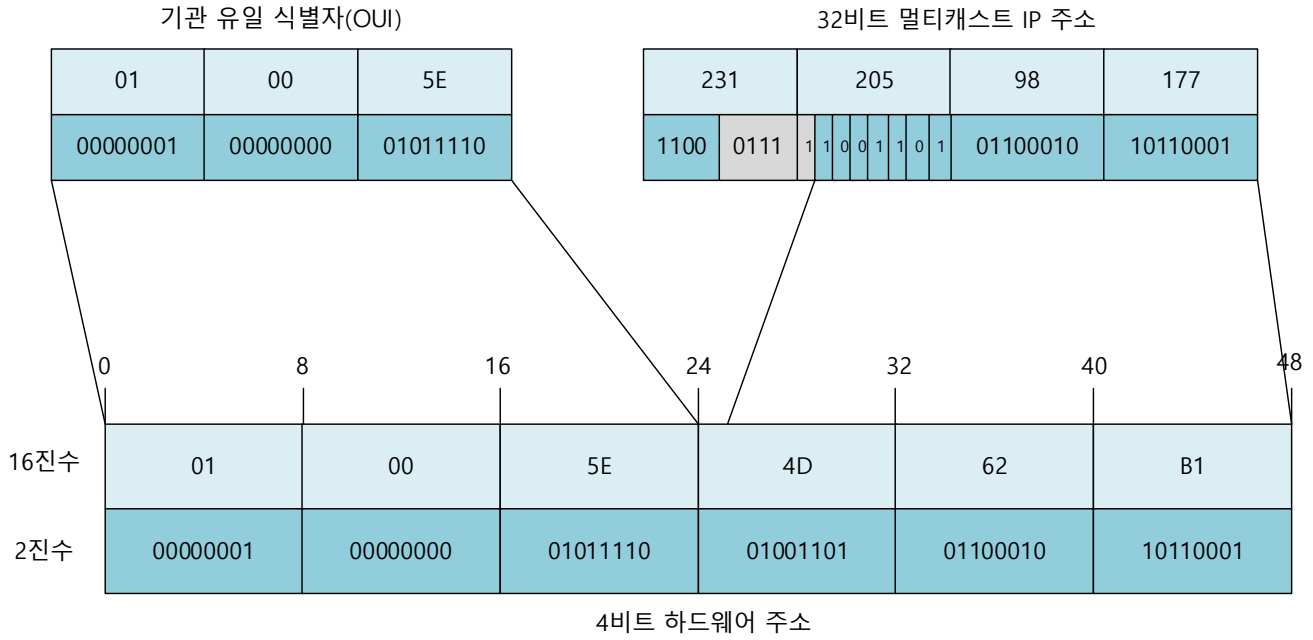
- PPP(Point to Point Protocol)의 링크 수립 단계
  - 송신 측은 LCP 설정요청 메시지를 수신 측에게 전송
  - 수신 측은 메시지에 동의 시 승인 메시지로 응답
  - 수신 측은 메시지에 비동의 시 거부 메시지로 응답
  - 수신 측이 메시지에 동의할 때까지 이 과정 반복
    - 수신 측이 메시지에 결국 동의하는 경우
      - 링크 상태는 LCP 개방으로 바뀌며 인증 단계로 넘어감
    - 수신 측이 메시지에 동의하지 못한 채 2초가 지날 경우
      - 송신 측은 LCP 시간초과 알림 메시지 출력
      - 물리 링크 종료

보충

- BAP(Bandwidth Allocation Protocol) 메시지 유형
  - 콜요청과 콜응답
    - 다중링크에 링크를 추가하고 싶은 장비는 콜요청 프레임을 보내고, 상대방 장비는 콜응답을 회신
  - 콜백요청과 콜백응답
    - 상대 장비가 다중링크에 링크를 추가하길 원하는 장비는 콜백요청 프레임을 보내고, 상대방 장비는 콜백응답을 회신
    - 해당 장비가 링크를 추가할 여건이 되지 않는 경우

보충

- IP 주소 직접 매핑 방식
  - 정의
    - 특정 방법을 이용해 상위 계층 주소를 하위 계층 주소로 매핑하는 방식
  - e.g.,
    - IEEE 802 주소지정 방법



보충

- Proxy ARP
  - 동작
    1. 출발지 장비가 ARP 요청 메시지를 브로드캐스팅
    2. 각 두 장비의 로컬 네트워크 사이에 위치한 라우터가 해당 요청에 자신의 하드웨어 주소로 응답
       - 라우터는 인접한 네트워크의 장비의 하드웨어 주소를 알고 있음
       - 브로드캐스트 메시지를 받은 라우터가 도착지 장비의 하드웨어 주소를 알고 있는 경우 응답
    3. 출발지 장비가 해당 라우터에게 메시지를 전달하면, 라우터는 그것을 목적지 장비에게 전달

보충

- RARP(Reverse ARP)
  - 한계점
    - 제한된 정보
      - RARP 서버는 오직 IP 주소만을 알려주며, 기타 중요 정보를 제공하지 않음
        - e.g.,
          - 서브넷 마스크
            - IP 주소 중 네트워크 ID 부분과 호스트 ID 부분을 나타내기 위한 정보
          - 게이트웨이
            - 서로 다른 네트워크 간의 통신을 가능하게 하는 장치

목 차

- 보충
- NAT 프로토콜
- IP Security(IPsec) 프로토콜
- 모바일 IP 프로토콜

NAT 프로토콜

- NAT(Network Address Translation) 프로토콜
  - 정의
    - 라우터를 통해 필요에 따라 사설 주소를 공인 주소로, 공인 주소를 사설 주소로 변환하는 프로토콜
  - 등장 배경
    - IP주소 비용 증가
      - IPv4를 사용함에 따라 IP주소가 희귀해져 비용이 증가함
    - 보안 우려의 증가
      - 많은 장비가 인터넷에 직접 연결되어 회사의 보안 위험 증가

NAT 프로토콜

- 장점
  - 공인 IP주소 공유
    - 다량의 클라이언트가 공인 IP 주소 공유 가능
  - 쉬운 확장
    - 로컬 네트워크에 새 장비를 추가하는 것이 쉬움
  - 로컬 통제력 강화
    - 사설 네트워크이므로 관리자의 통제력이 강화됨
  - 인터넷 서비스 제공자(ISP, Internet Service Provider) 선택의 유연성
    - 공인 주소만 바꾸면 되므로 ISP 변경이 용이함
  - 보안 강화
    - 각 클라이언트는 공인 IP 주소를 가지고 있지 않으므로 외부 공격자가 클라이언트에게 직접 접근하기 어려움

NAT 프로토콜

- 단점
  - 복잡성
    - NAT의 역할은 관리의 복잡성을 가증시킴
  - 호환성 문제
    - NAT는 애플리케이션 데이터 영역을 수정하지 않으므로 특정 애플리케이션과 호환성 문제 발생 가능
  - 보안 프로토콜 문제
    - 헤더의 변조를 탐지하는 IPsec(IP security)와 같은 프로토콜은 NAT에 의한 변경과 악성 해킹을 구분하기 어려움
  - 클라이언트 접근 지원 미비
    - 각 클라이언트에게 공인 IP주소가 없으므로 인터넷 접근에 제한이 있음
      - e.g., P2P 애플리케이션 설정 어려움

NAT 프로토콜

- 주소 구분
  - 특정 주소가 참조하는 장비의 위치에 따른 구분
    - 내부 주소
      - 로컬 네트워크의 장비를 참조하는 주소
    - 외부 주소
      - 외부 네트워크의 장비를 참조하는 주소
  - 특정 주소가 나타나는 네트워크 위치에 따른 구분
    - 로컬 주소
      - 로컬 네트워크의 데이터그램에 나타나는 주소
    - 전역 주소
      - 외부 네트워크의 데이터그램에 나타나는 주소

NAT 프로토콜

- 주소 종류
  - 내부 로컬 주소
    - 내부 네트워크에서 쓰이는 내부 장비의 주소
  - 내부 전역 주소
    - 내부 장비의 사설 주소가 변환된 공인 IP 주소
  - 외부 전역 주소
    - 공중 네트워크에서 외부 장비를 참조하는 주소
  - 외부 로컬 주소
    - 로컬 네트워크에서 외부 장비를 참조하는 주소

NAT 프로토콜

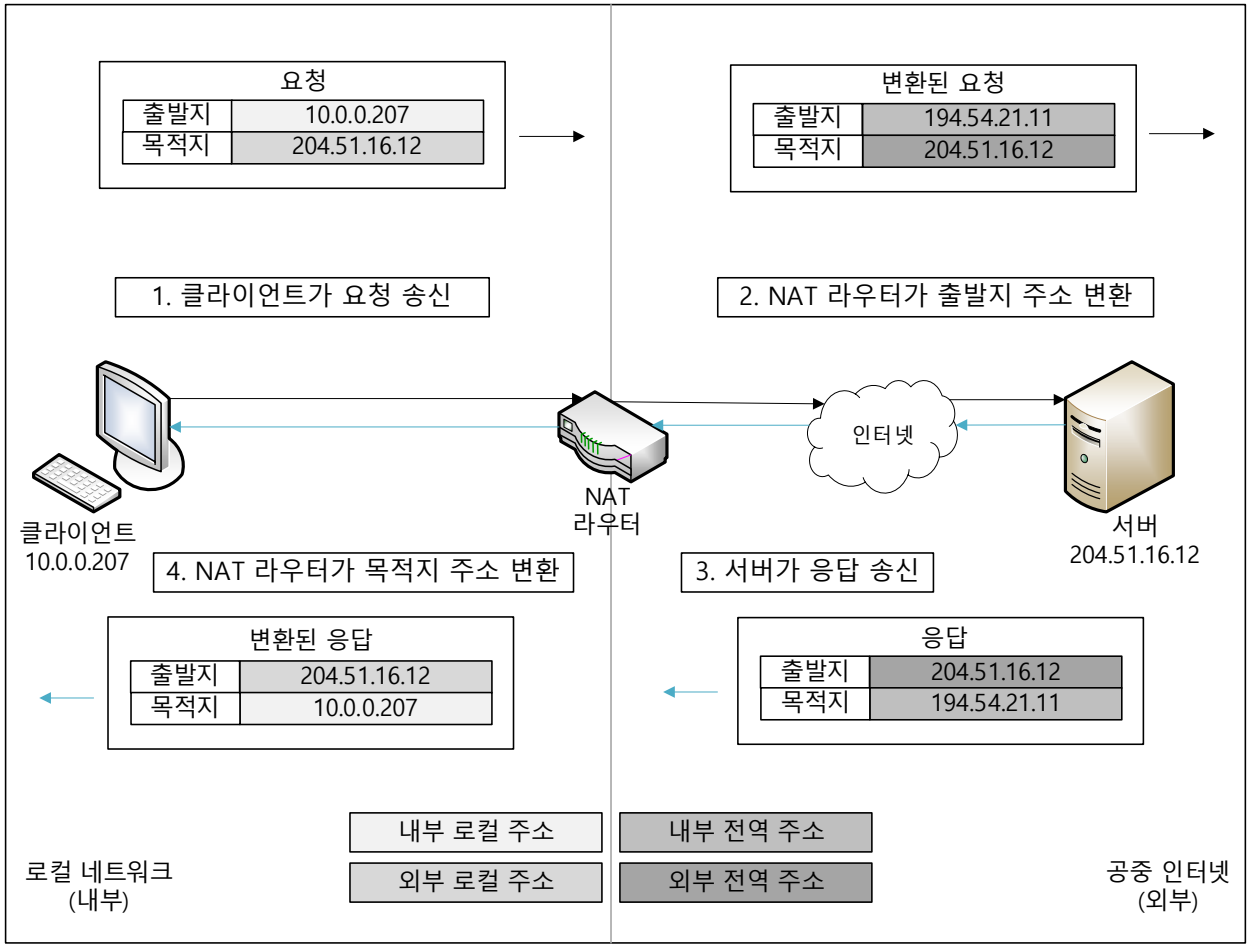
- 주소 변환
  - 변환 테이블
    - 정의
      - 내/외부 로컬 주소를 내/외부 전역 주소로 매핑하는 정보를 포함하는 테이블
    - 항목 추가 방법
      - 정적 매핑
        - 내/외부 장비의 전역 표현과 로컬 표현 사이에 정의된 영구적이고 고정된 관계의 정보를 매핑
        - 외부 네트워크에 항상 동일한 공인 주소로 표현되어야 할 장비에 적합
      - 동적 매핑
        - 필요 시 전역 주소 풀에서 전역 주소를 얻고, 세션 완료 후 전역 주소 풀에 사용한 전역 주소 반환
        - 클라이언트의 공인 IP주소 공유 촉진

NAT 프로토콜

- 동작 방식
  - IP NAT 단방향 (전통적/아웃바운드) 동작
    - 내부 네트워크에서 외부 네트워크로 요청/응답 통신이 시작된다는 가정 하에 설계된 전통적 NAT 동작 방식
    - 과정
      1. 내부 클라이언트가 요청을 생성하여 NAT 라우터에게 송신
      2. NAT 라우터는 출발지 주소를 변환한 뒤 외부 서버에게 송신
      3. 외부 서버가 응답을 생성하고 NAT 라우터에게 회신
      4. NAT 라우터는 목적지 주소를 변환하고 데이터그램을 내부 클라이언트에게 전달

NAT 프로토콜

- 동작 방식
  - IP NAT 단방향 (전통적/아웃바운드) 동작



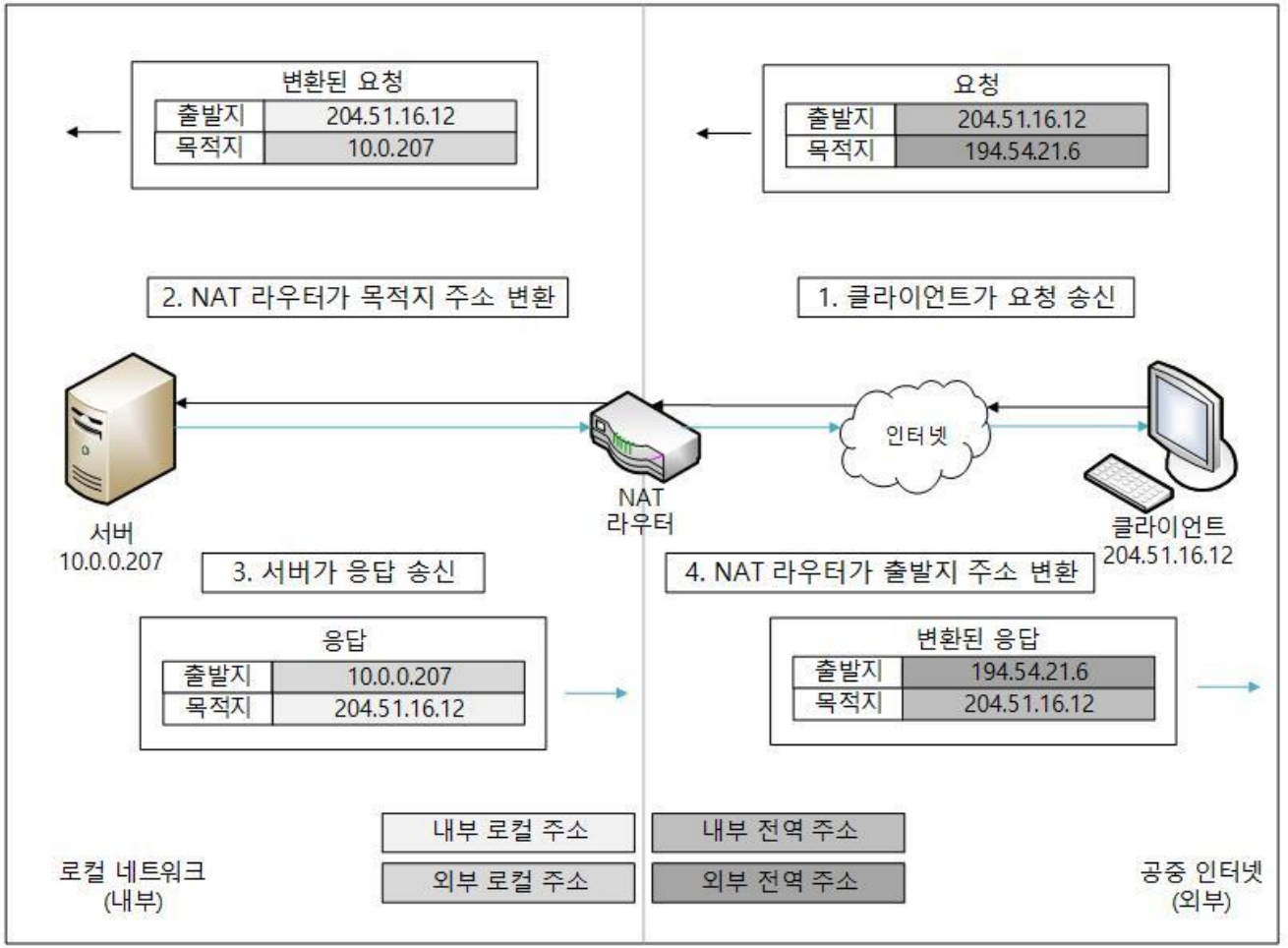
NAT 프로토콜

- 동작 방식
  - IP NAT 양방향 (Two-Way/인바운드) 동작
    - 외부 네트워크에서 내부 네트워크로 요청/응답 통신이 시작된다는 가정 하에 설계된 NAT 동작 방식

    - 과정
      1. 외부 네트워크 장비는 접근하고자 하는 내부 네트워크 장비의 이름을 이용해 DNS 요청을 DNS 서버에게 전송
      2. DNS 서버는 수신한 이름을 해당 장비의 내부 로컬 주소로 변환한 후, NAT를 통해 내부 전역 주소 매핑
      3. DNS 서버는 외부 장비에게 내부 장비의 전역 주소를 전송
      4. 외부 클라이언트가 요청을 생성하여 NAT 라우터에게 전송
      5. NAT 라우터가 목적지 주소 변환 후 내부 서버에 송신
      6. 내부 서버가 응답을 생성하고 NAT 라우터에게 송신
      7. NAT 라우터가 출발지 주소 변환 후 외부 클라이언트에 송신

NAT 프로토콜

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

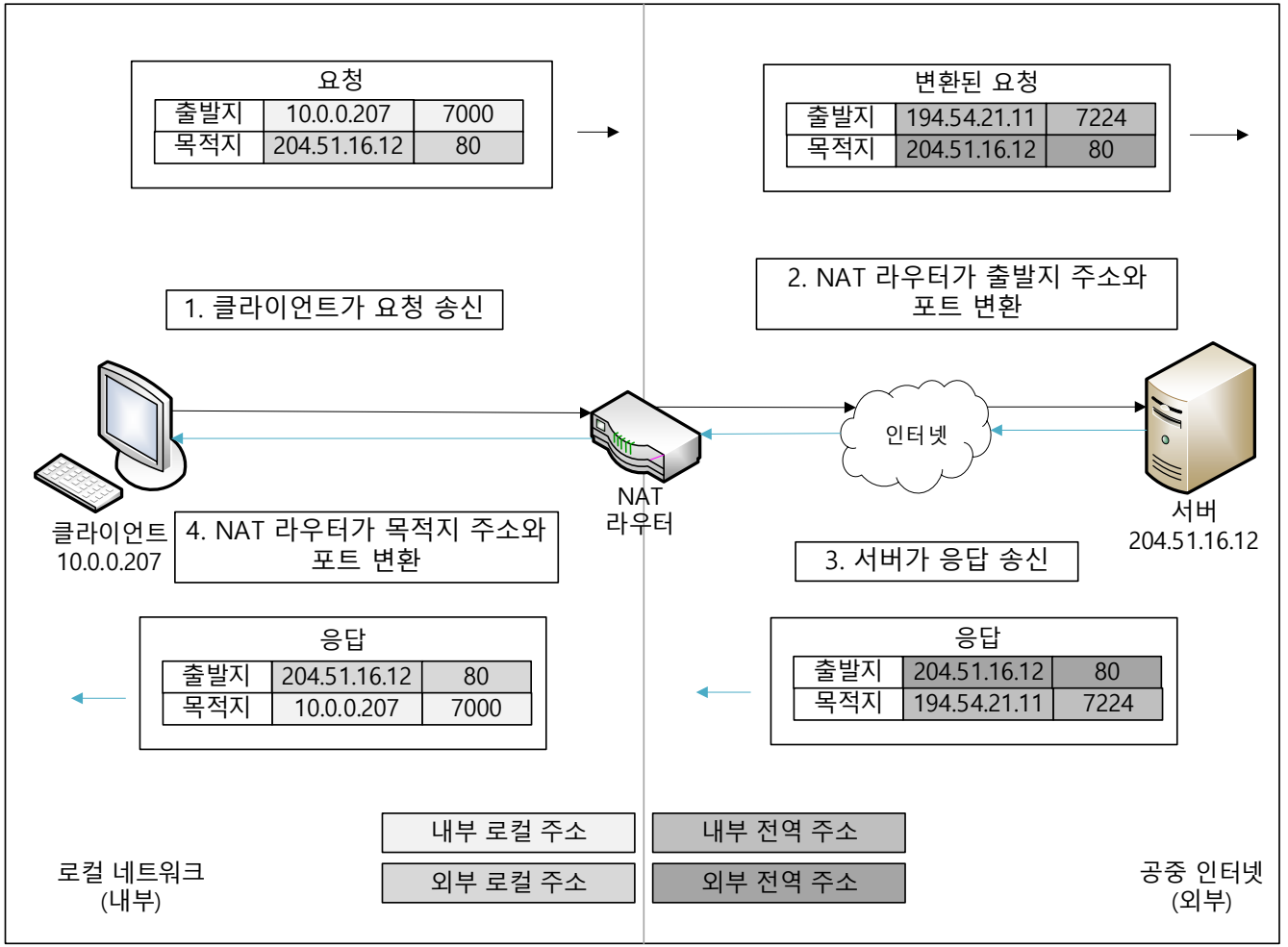


NAT 프로토콜

- 동작 방식
  - IP NAT 포트 기반 (과부하) 동작
    - 하나의 전역 주소로 다수의 로컬 주소를 매핑하고 포트 번호를 변환하여 개별 연결을 식별하는 NAT 동작 방식
    - 과정
      1. 내부 클라이언트가 요청을 생성하여 NAT 라우터에게 송신
      2. NAT 라우터는 출발지 주소와 포트를 변환하고 외부 서버로 송신
      3. 외부 서버가 응답을 생성하고 NAT 라우터에게 회신
      4. NAT 라우터는 목적지 주소를 변환하고 데이터그램을 내부 클라이언트에게 전달

NAT 프로토콜

- 동작 방식
  - IP NAT 포트 기반 (과부하) 동작

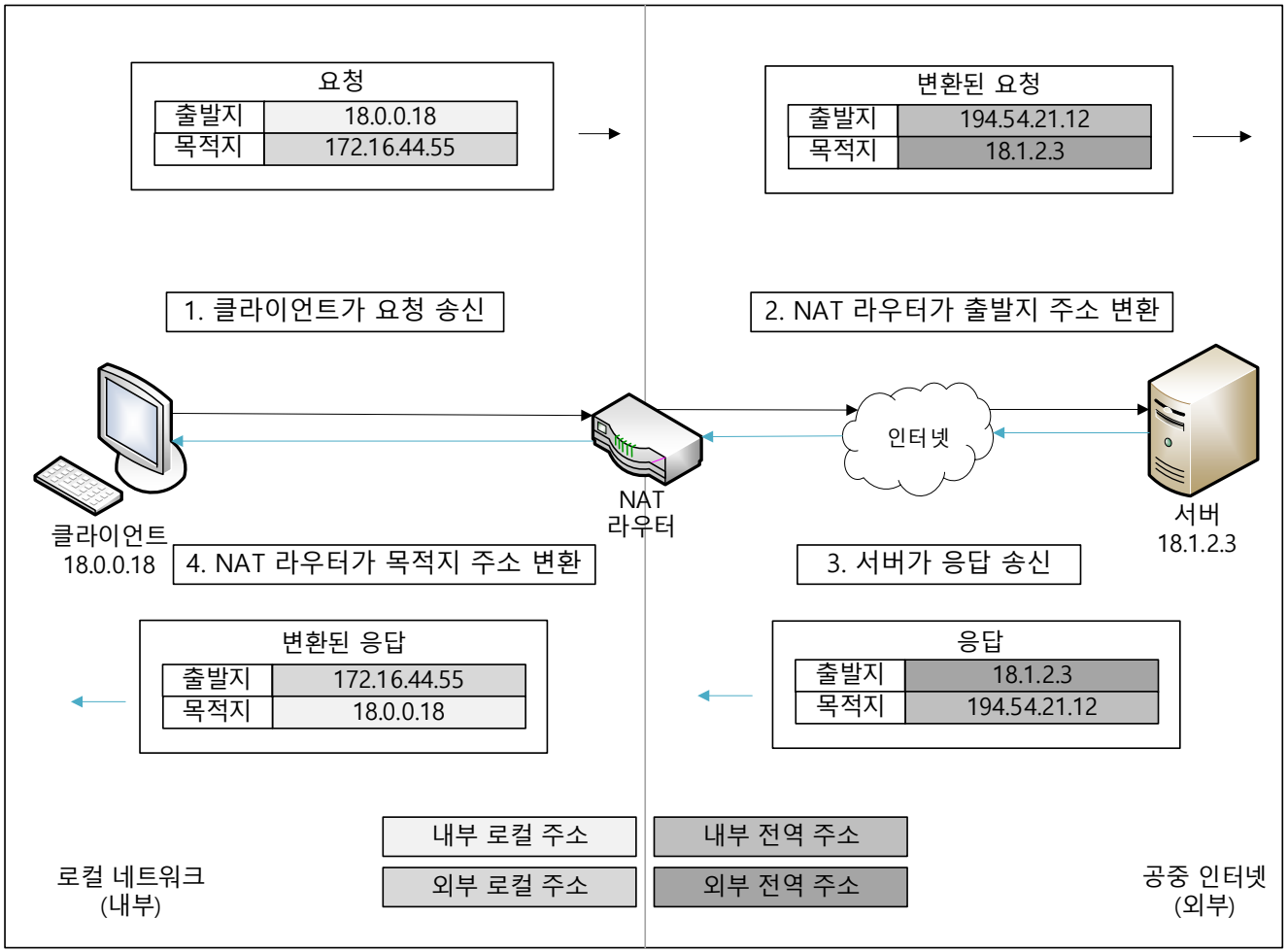


NAT 프로토콜

- 동작 방식
  - IP NAT 중복/2회 NAT 동작
    - 내부 네트워크의 주소와 외부 네트워크의 주소가 중복되는 경우를 대비한 NAT 동작 방식
    - 과정
      1. 내부 네트워크의 장비는 외부 네트워크의 장비의 이름을 통해 주소를 얻기 위해 DNS 요청 송신
      2. NAT 라우터가 해당 요청을 가로챈 후 외부 장비 주소의 특수 매핑을 위한 테이블을 참조하여 사설 주소로 매핑
      3. NAT 라우터는 해당 사설 주소를 클라이언트에게 전달
      4. 내부 클라이언트가 요청을 생성하여 NAT 라우터에게 송신
      5. NAT 라우터는 출발지 주소와 목적지 주소 변환 후 외부 서버에게 송신하고, 외부 서버는 응답 생성 후 NAT 라우터에게 회신
      6. NAT 라우터는 출발지 주소와 목적지 주소 변환 후 내부 클라이언트에게 전달

NAT 프로토콜

- 동작 방식
  - IP NAT 중복/2회 NAT 동작



목 차

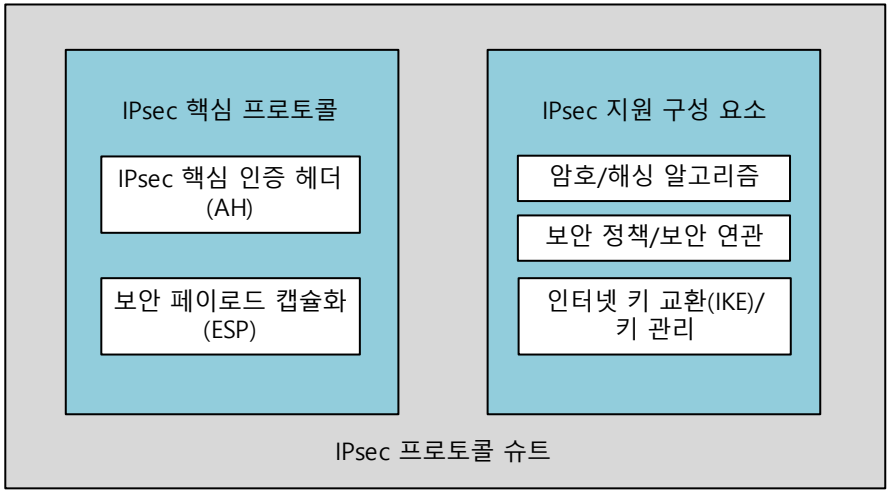
- 보충
- NAT 프로토콜
- IP Security(IPsec) 프로토콜
- 모바일 IP 프로토콜

IP Security(IPsec) 프로토콜

- 정의
  - 네트워크 계층에서 완전한 보안 솔루션을 제공하는 서비스와 프로토콜 모음
- 기능
  - 메시지의 기밀성 보장
  - 메시지의 무결성 인증
  - 재전송(Replay) 공격으로부터 보호
  - 보안 알고리즘과 키를 협상할 수 있게 함
  - 두 보안 모드 제공
    - 터널(Tunnel)
    - 전송(Transport)

IP Security(IPsec) 프로토콜

- 구성 요소



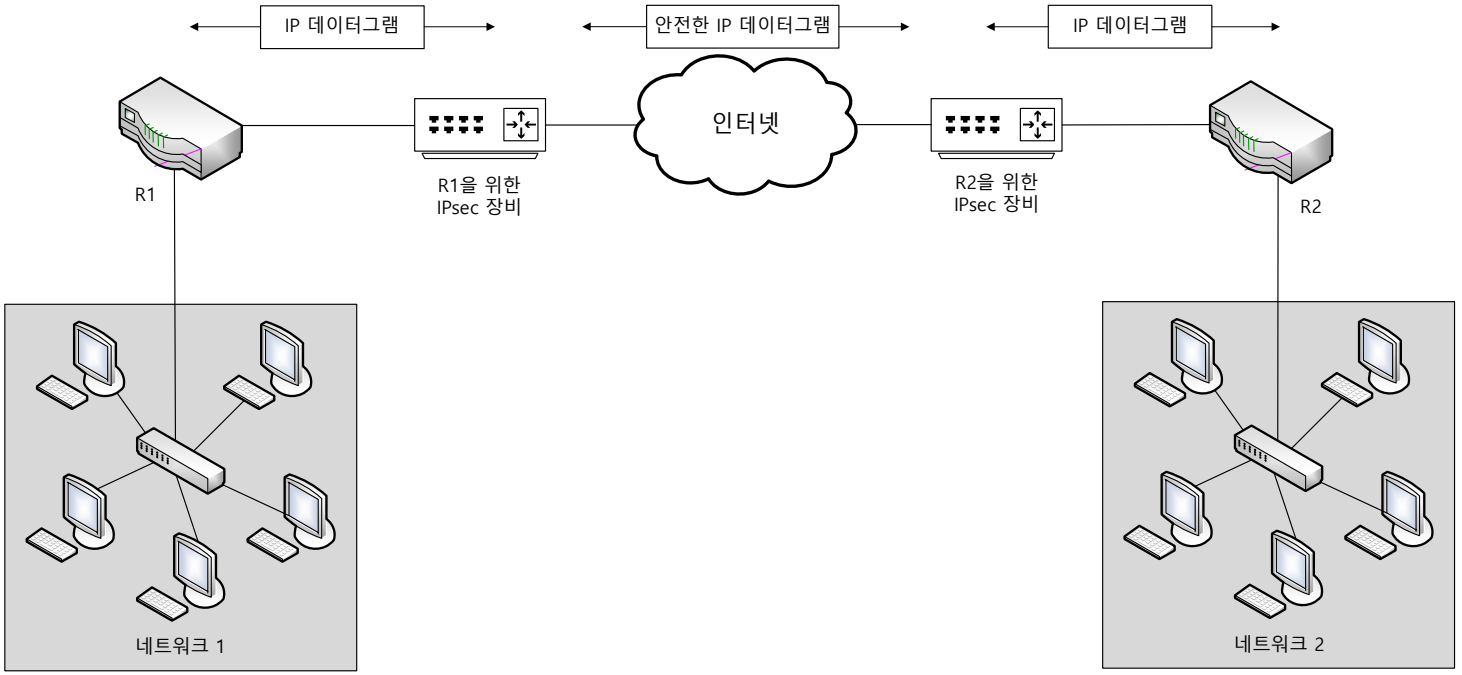
- 구현 방법
  - 종단 호스트 구현
    - IPsec을 모든 호스트 장비에 설치하는 방법
  - 라우터 구현
    - IPsec을 라우터에만 설치하는 방법
    - 구현한 라우터 쌍 사이만을 보호

IP Security(IPsec) 프로토콜

- TCP/IP 프로토콜 스택과의 결합 구조
  - 통합 구조
    - IPsec을 IP에 통합한 구조
    - 추가 하드웨어나 계층이 필요 없음
    - IPv4에서는 실용적이지 않음
  - 스택 삽입 구조(BITS, Bump In The Stack)
    - IPsec이 IP 계층과 데이터 링크 계층 사이에 별도 계층으로 위치한 구조

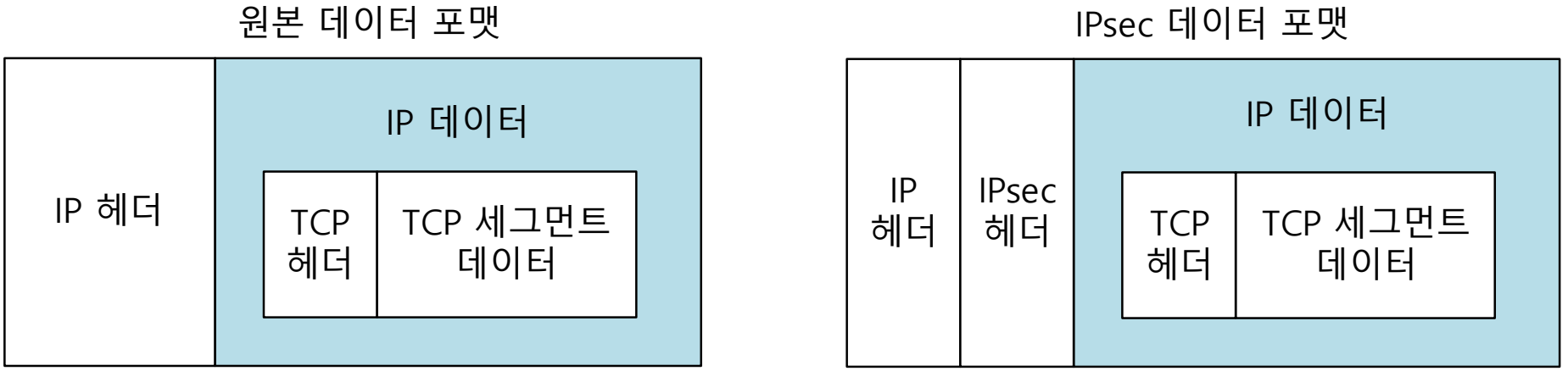
IP Security(IPsec) 프로토콜

- TCP/IP 프로토콜 스택과의 결합 구조
  - 라인 삽입 구조(BITW, Bump In The Wire)
    - 라우터와 인터넷 사이의 구간에 특수 IPsec 장비를 추가한 구조
    - IPsec 장비는 외부로 나가는 데이터그램에 IPsec 보호 기능 추가, 내부로 들어오는 데이터그램에 IPsec 관련 헤더 제거



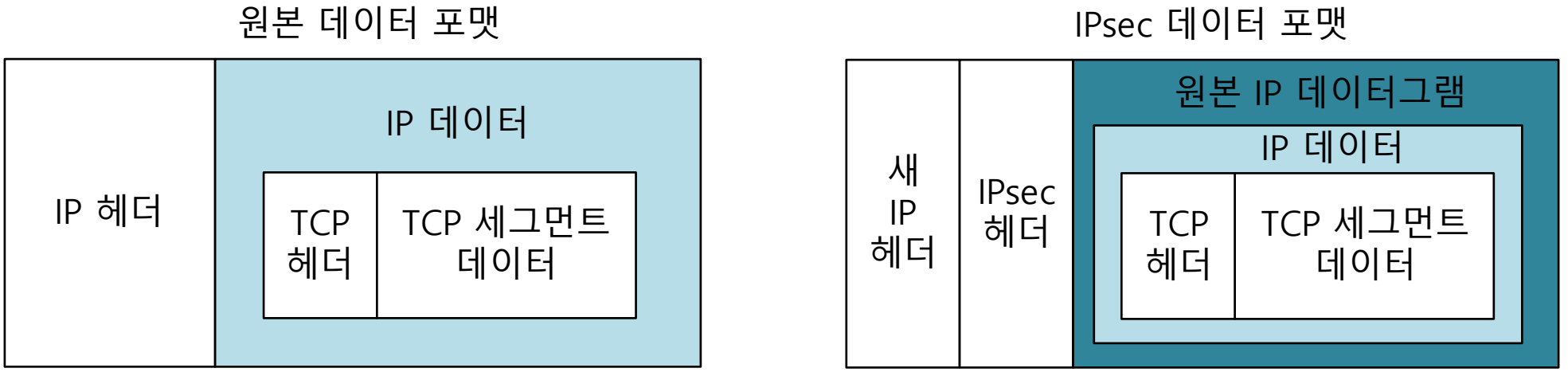
IP Security(IPsec) 프로토콜

- IPsec 동작 모드
  - 전송 모드(Transport Mode)
    - 전송 계층에서 IP로 전달되는 메시지를 IPsec 프로토콜로 포장하여 IP 계층으로 전달하는 모드
      - AH(Authentication Header) 또는 AH과 ESP(Encapsulating Security Payload)의 조합에 의해 처리됨
    - 주로 통합 구조에서 쓰임



IP Security(IPsec) 프로토콜

- IPsec 동작 모드
  - 터널 모드(Tunnel Mode)
    - IP헤더까지 추가된 메시지를 IPsec 프로토콜로 포장하여 데이터 링크 계층에 전달하는 모드
    - 주로 스택 삽입 구조와 라인 삽입 구조에서 쓰임



IP Security(IPsec) 프로토콜

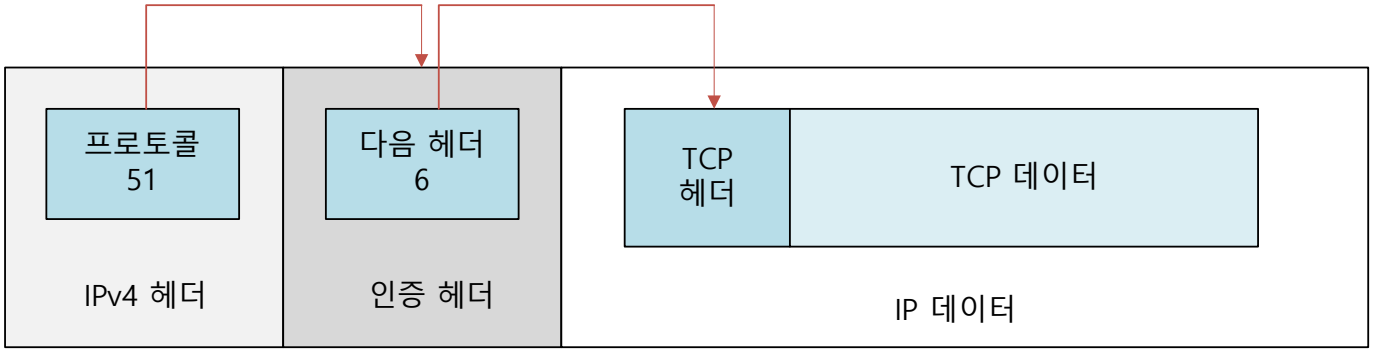
- IPsec 보안 구성 요소
  - 보안 정책(SP, Security Policy)
    - IPsec 구현에 내장된 규칙
    - 데이터그램 처리를 지시
      - IPsec에서 처리할 필요가 있는지의 여부를 결정
    - 장비의 보안 정책 데이터베이스(SPD, Security Policy Database)에 저장되어 있음
  - 보안 연관(SA, Security Association)
    - 장비 간 맺은 특정한 종류의 보안 연결을 포함하는 정보
    - 장비의 보안 연관 데이터베이스(SAD, Security Association Database)에 저장되어 있음

IP Security(IPsec) 프로토콜

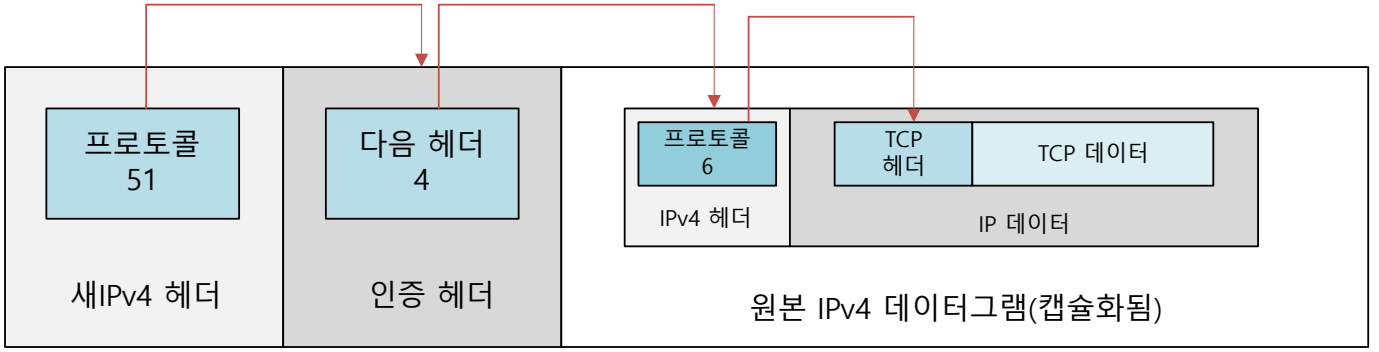
- IPsec 인증 헤더(AH, Authentication Header)
  - 정의
    - 데이터그램의 값에 의해 계산되는 헤더를 추가하여 데이터그램에 대한 인증을 제공하는 프로토콜
  - 과정
    1. 출발지 장비에서 AH는 공유하는 키를 이용해 계산을 수행
       - MD5, SHA-1 사용
    2. 출발지 장비는 결과(ICV, Integrity Check Value)를 다른 필드와 함께 헤더에 입력하여 전송
    3. 목적지 장비는 두 장비가 공유하는 키를 이용하여 동일한 계산 수행
    4. 목적지 장비는 데이터그램의 수정 여부 파악 가능

IP Security(IPsec) 프로토콜

- IPsec 인증 헤더(AH, Authentication Header)
  - 헤더의 위치와 연결
    - AH 이전 헤더는 다음 헤더(Next Header) 필드에 AH 헤더의 프로토콜 값인 51을 입력해 AH 헤더와 연결
    - 전송 모드

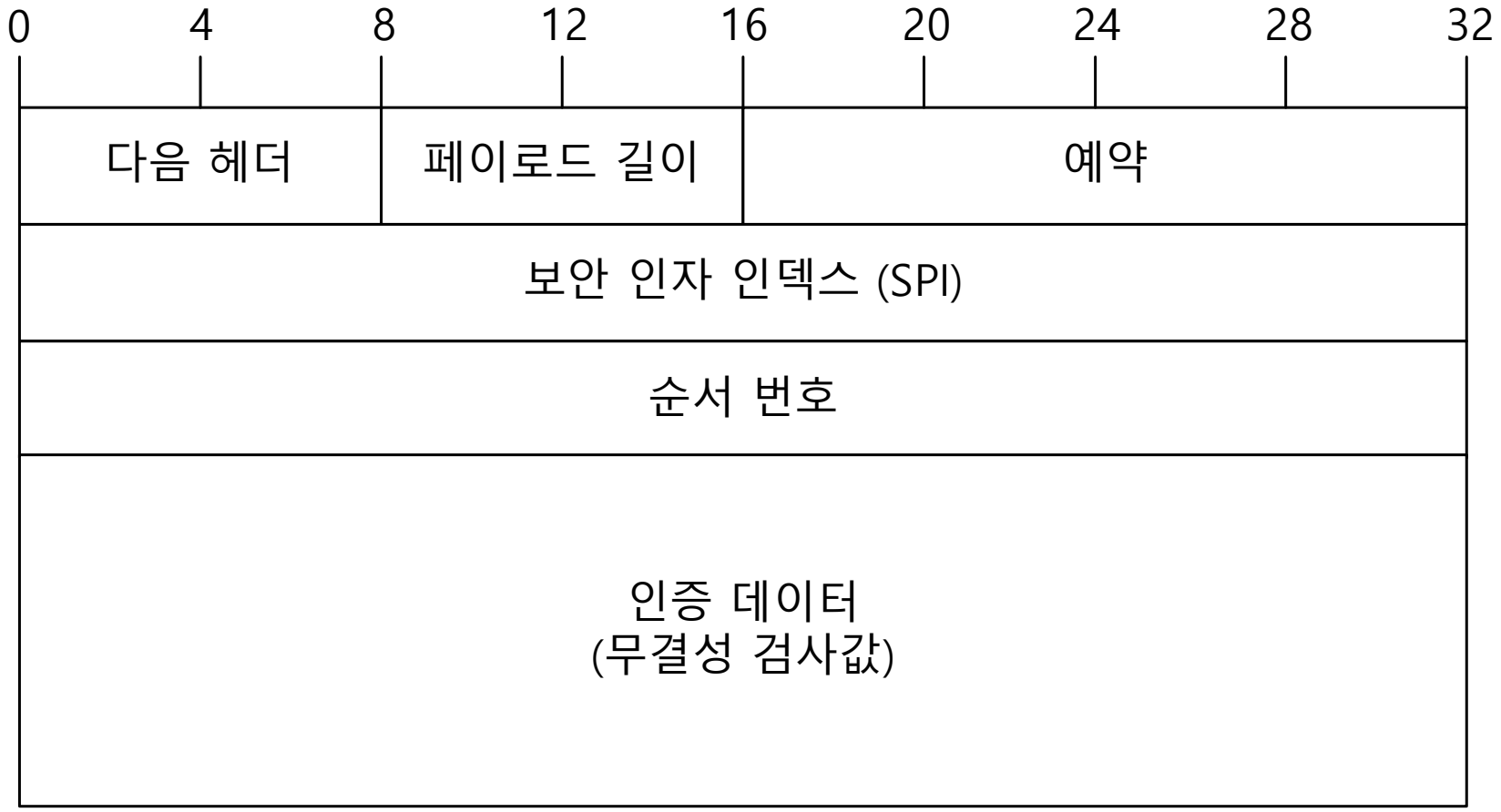


    - 터널 모드



IP Security(IPsec) 프로토콜

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



IP Security(IPsec) 프로토콜

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

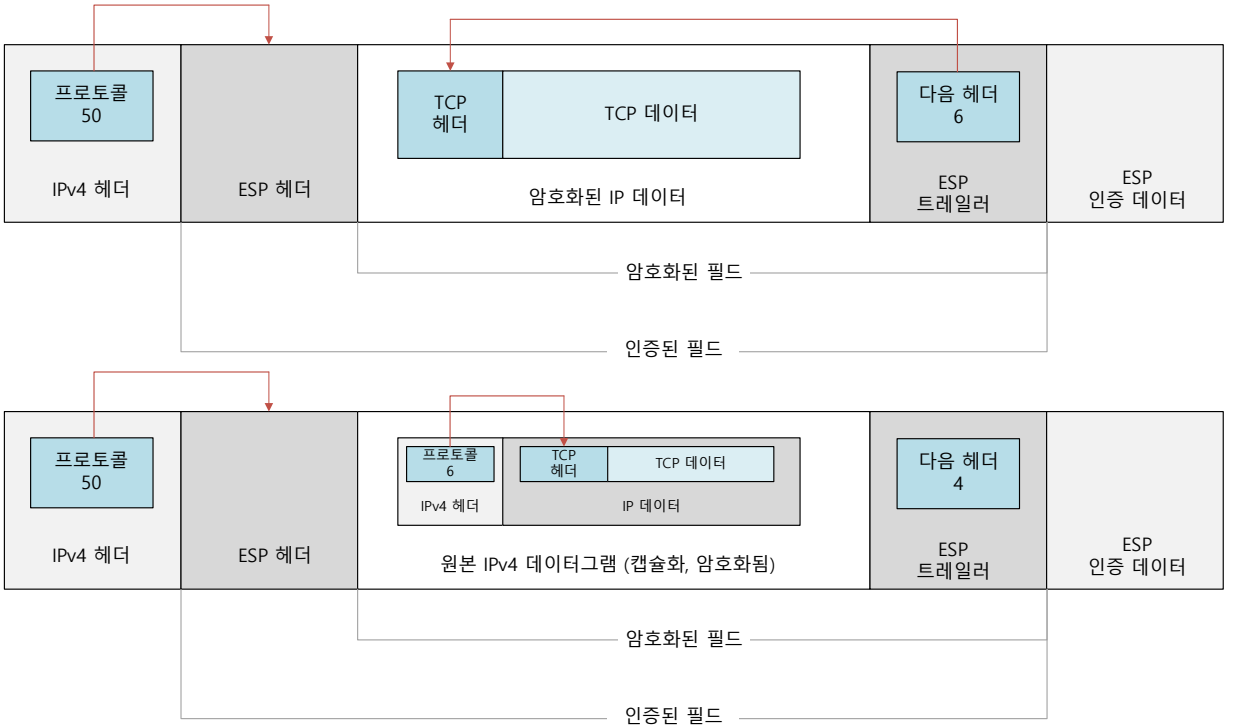
필드 이름	크기(바이트)	설명
다음 헤더	1	• AH 다음의 헤더 프로토콜 번호를 포함
페이로드 길이	1	• 인증 헤더의 길이에 2를 뺀 값
예약됨	2	• 쓰이지 않아 0으로 설정됨
SPI	4	• SA를 식별함
순서 번호	4	• SA가 구성될 때 0으로 설정, 통신할 때마다 1씩 증가 • 재전송 공격 방지
인증 데이터	가변적 (32비트 배수)	• 무결성 검사값(ICV) 포함

IP Security(IPsec) 프로토콜

- IPsec 보안 페이로드 캡슐화(ESP, Encapsulating Security Payload)
  - 정의
    - IP 데이터그램을 암호화하여 기밀성을 보장하는 프로토콜
  - 구성 요소
    - ESP 헤더
      - SPI 필드와 순서 번호 필드 포함
      - 암호화된 데이터 앞에 위치
    - ESP 트레일러
      - ESP의 다음 헤더 필드와 패딩, 패딩 길이 필드 포함
      - 암호화된 데이터 뒤에 위치
    - ESP 인증 데이터
      - ICV 포함
      - ESP의 선택적 인증 기능이 적용될 때 사용됨

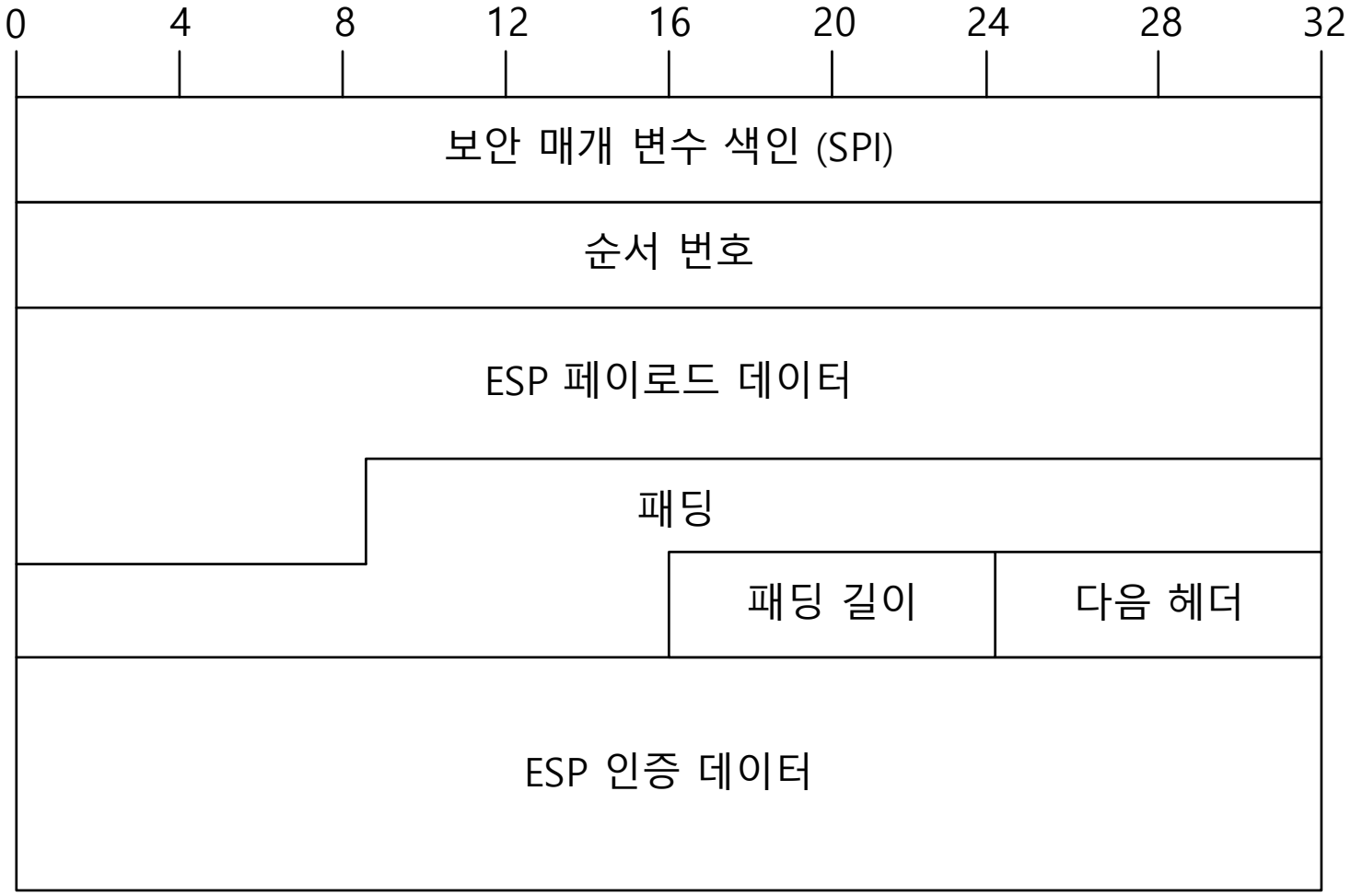
IP Security(IPsec) 프로토콜

- IPsec 보안 페이로드 캡슐화(ESP)
  - 헤더의 위치와 계산
    - 페이로드와 ESP 트레일러에 암호화 수행
      - DES, 3DES 사용
    - 필요 시 인증 데이터 필드를 제외한 전체 ESP 데이터그램에 대한 인증 수행
  - 전송 모드
  - 터널 모드



IP Security(IPsec) 프로토콜

- IPsec 보안 페이로드 캡슐화(ESP)
  - 포맷



IP Security(IPsec) 프로토콜

- IPsec 보안 페이로드 캡슐화(ESP)
  - 포맷

구간	필드 이름	크기(바이트)	설명	암호화 범위	인증 범위
ESP 헤더	SPI	4	• SA 식별		
	순서 번호	4	• SA가 구성될 때 0으로 설정 • 통신할 때마다 1씩 증가 • 재전송 공격 방지		
페이로드		가변적	• 암호화된 페이로드 데이터		
ESP 트레일러	패딩	가변적 (0~255)	• 암호화를 위한 추가적인 패딩 바이트 포함		
	패딩 길이	1	• 패딩 필드의 바이트 수		
	다음 헤더	1	• 다음 헤더의 프로토콜 번호 포함		
ESP 인증 데이터		가변적	• 선택적 ESP 인증 알고리즘 적용 • ICV 포함		

IP Security(IPsec) 프로토콜

- IPsec 인터넷 키 교환(IKE, Internet Key Exchange)
  - 정의
    - AH 또는 ESP에서 사용할 비밀 정보를 교환하기 위해 사용하는 프로토콜
  - 동작
    - IKE의 첫 프로토콜인 ISAKMP(Internet Security Association and Key Management Protocol) 구조 내에서 동작
      - 1단계: 두 장비는 협상을 통해 ISAKMP를 위한 SA인 ISAKMP SA를 생성
      - 2단계: 수립한 ISAKMP SA를 이용하여 기타 보안 프로토콜을 위한 SA 생성

목 차

- 보충
- NAT 프로토콜
- IP Security(IPsec) 프로토콜
- 모바일 IP 프로토콜

모바일 IP 프로토콜

- 정의
  - 장비가 통신 도중 다른 네트워크로 이동해도 정상적으로 데이터 송수신을 지원하는 프로토콜
- 목표
  - 이동 장비가 네트워크를 바꿔도 원래 IP를 유지
  - 모바일 IP와 기존 IP 장비 간의 통신
  - 이동 장비의 수의 제한이 없음
  - 모바일 IP의 강한 보안

모바일 IP 프로토콜

- 모바일 IP 장비 역할
  - 이동 장비
    - 네트워크 간을 이동하는 장비
  - 홈 에이전트
    - 이동 장비의 홈 네트워크 라우터
  - 외부 에이전트
    - 이동 장비가 현재 사용중인 네트워크의 라우터

- CoA(Care of Address)
  - 이동 장비가 외부 에이전트로부터 부여 받으며 지속적인 통신을 가능하게 하는 임시 주소

모바일 IP 프로토콜

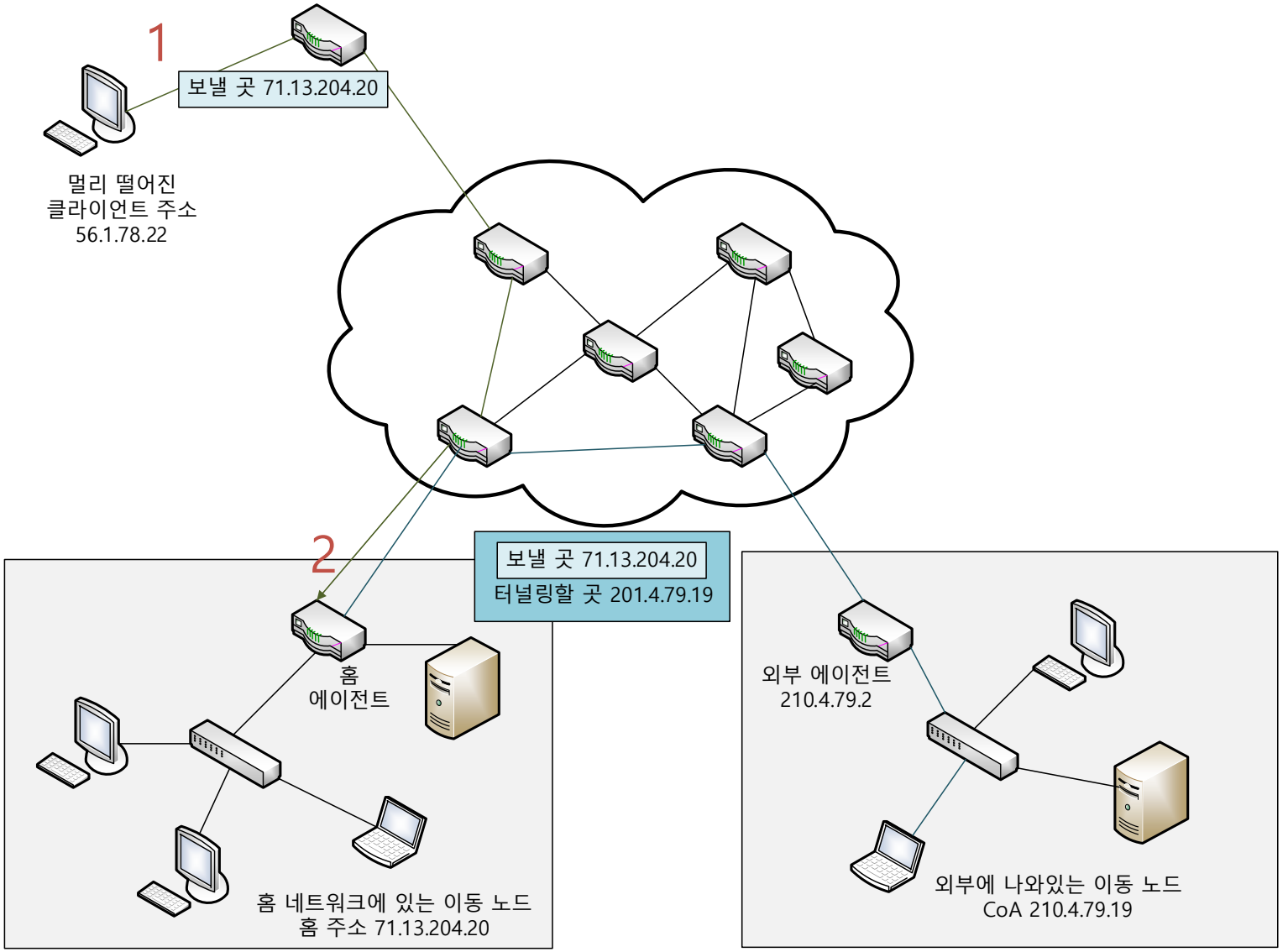
- CoA(Care of Address)
  - 할당 유형
    - 외부 에이전트 CoA
      - 외부 에이전트가 이동 장비에게 CoA를 광고 메시지에 실어 보내는 방식
        - 외부 네트워크에 있는 모든 이동 장비들이 같은 외부 CoA 사용
    - 공존 CoA(Co-Located CoA)
      - 이동 장비에게 직접 CoA가 할당되는 방식
        - 트래픽이 홈 에이전트에서 이동 장비로 바로 전달됨
        - 남은 IP 주소를 할당받아야 하므로, 주소 고갈 문제가 생길 위험이 있음

모바일 IP 프로토콜

- 동작
  1. 에이전트 통신
     - 이동 장비는 이동 후 로컬 네트워크의 에이전트 탐색
     - 이동 장비는 에이전트 광고 메시지 수신 혹은 에이전트 요청 메시지 송신을 통해 에이전트 식별
  2. 네트워크 위치 결정
     - 이동 장비는 에이전트를 식별하여 자신이 속한 네트워크가 외부 네트워크인지 판단
  3. CoA(Care of Address) 획득
     - 이동 장비는 외부 에이전트로부터 CoA 획득
  4. 에이전트 등록
     - 이동 장비는 홈 에이전트에 자신의 CoA 등록
  5. 데이터그램 전달
     - 홈 에이전트는 이동 장비에게 온 데이터그램을 장비로 전송

모바일 IP 프로토콜

- 동작

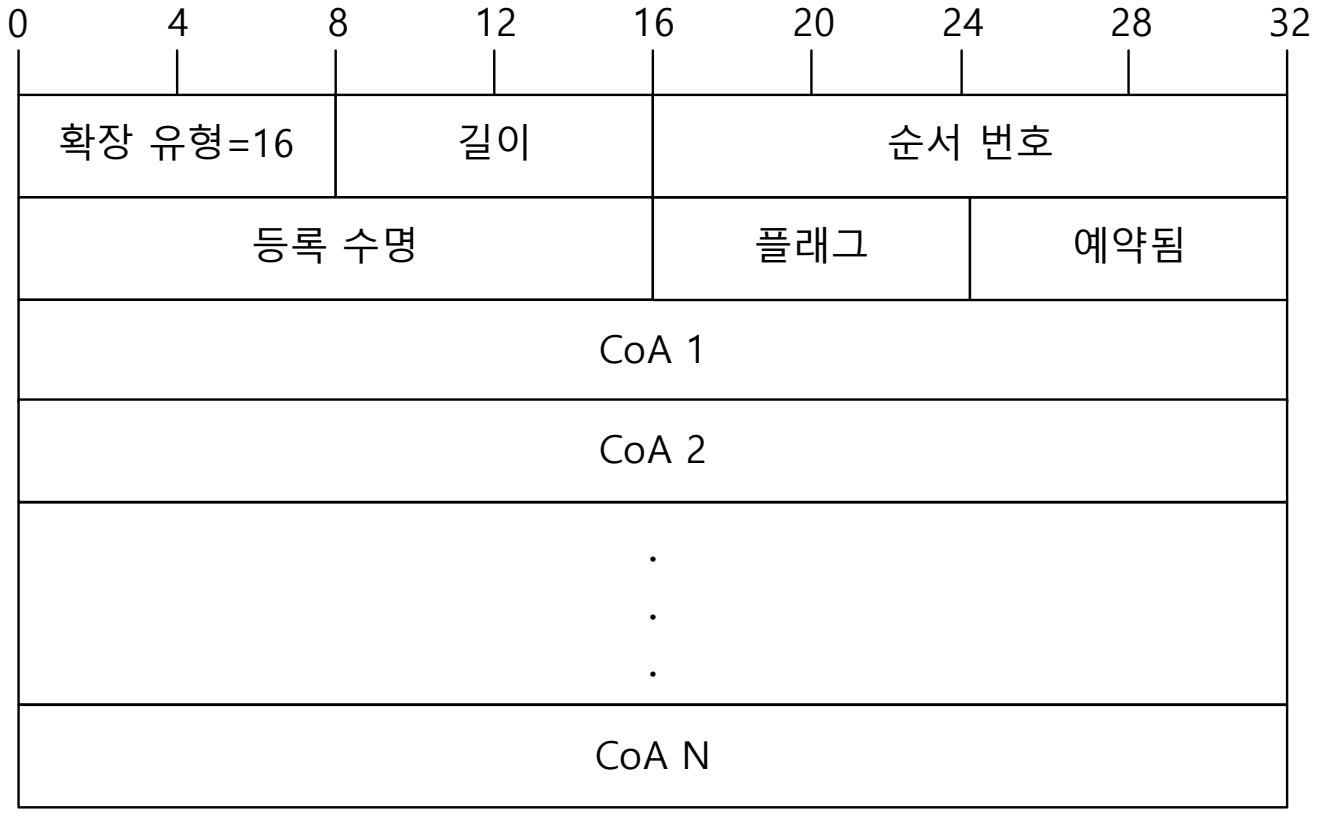


모바일 IP 프로토콜

- 모바일 IP 에이전트 발견
  - 과정
    1. 에이전트 통신
    2. 네트워크 위치 결정
    3. CoA(Care of Address) 획득
  - 사용하는 메시지
    - 에이전트 광고(Agent Advertisement)
      - 모바일 IP를 지원하는 라우터가 정기적으로 전송하는 메시지
    - 에이전트 요청(Agent Solicitation)
      - 모바일 IP 장비가 로컬 에이전트에게 에이전트 광고 메시지를 보낼 것을 요청하는 메시지

모바일 IP 프로토콜

- 모바일 IP 에이전트 발견
  - 사용하는 메시지 포맷
    - 에이전트 광고(Agent Advertisement)



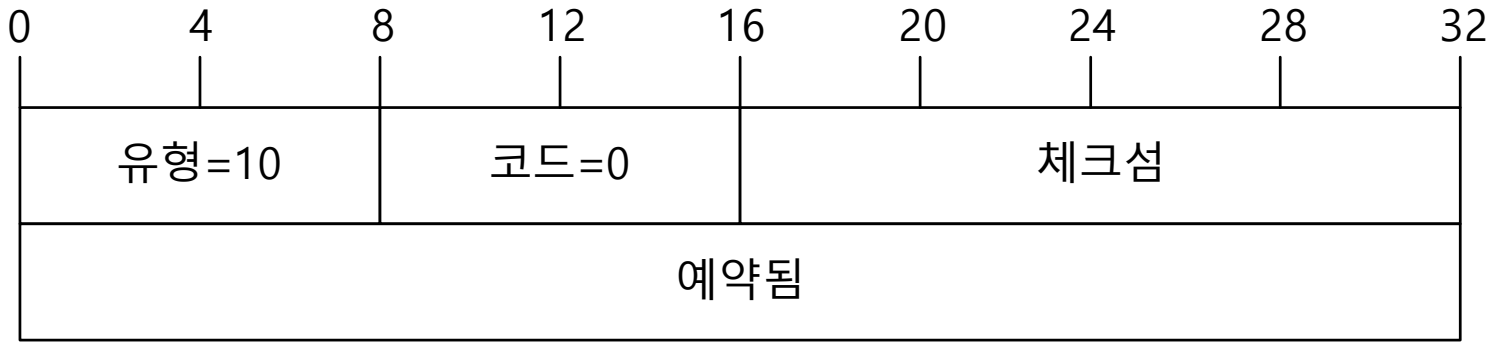
모바일 IP 프로토콜

- 모바일 IP 에이전트 발견
  - 사용하는 메시지 포맷
    - 에이전트 광고(Agent Advertisement)

필드 명	크기(바이트)	설명
유형	1	• 에이전트 광고 확장 유형 명시 • 이동 에이전트 광고 확장 유형값은 16
길이	1	• 유형과 길이 필드를 뺀 광고 메시지의 길이 명시
순서 번호	2	• 라우터 초기화 시 0으로 설정 • 광고 메시지를 송신할 때마다 1씩 증가
등록 수명	2	• 에이전트가 등록 요청을 받기 원하는 주기를 초 단위로 나타낸 것
플래그	1	• 에이전트 상태에 관한 정보
예약됨	1	• 0으로 설정됨, 의미 없음
CoA	가변 주소(주소당 4바이트)	• 이동 장비가 외부 에이전트 CoA로 사용할 수 있는 0개 이상의 주소 알림

모바일 IP 프로토콜

- 모바일 IP 에이전트 발견
  - 사용하는 메시지 포맷
    - 에이전트 요청(Agent Solicitation)



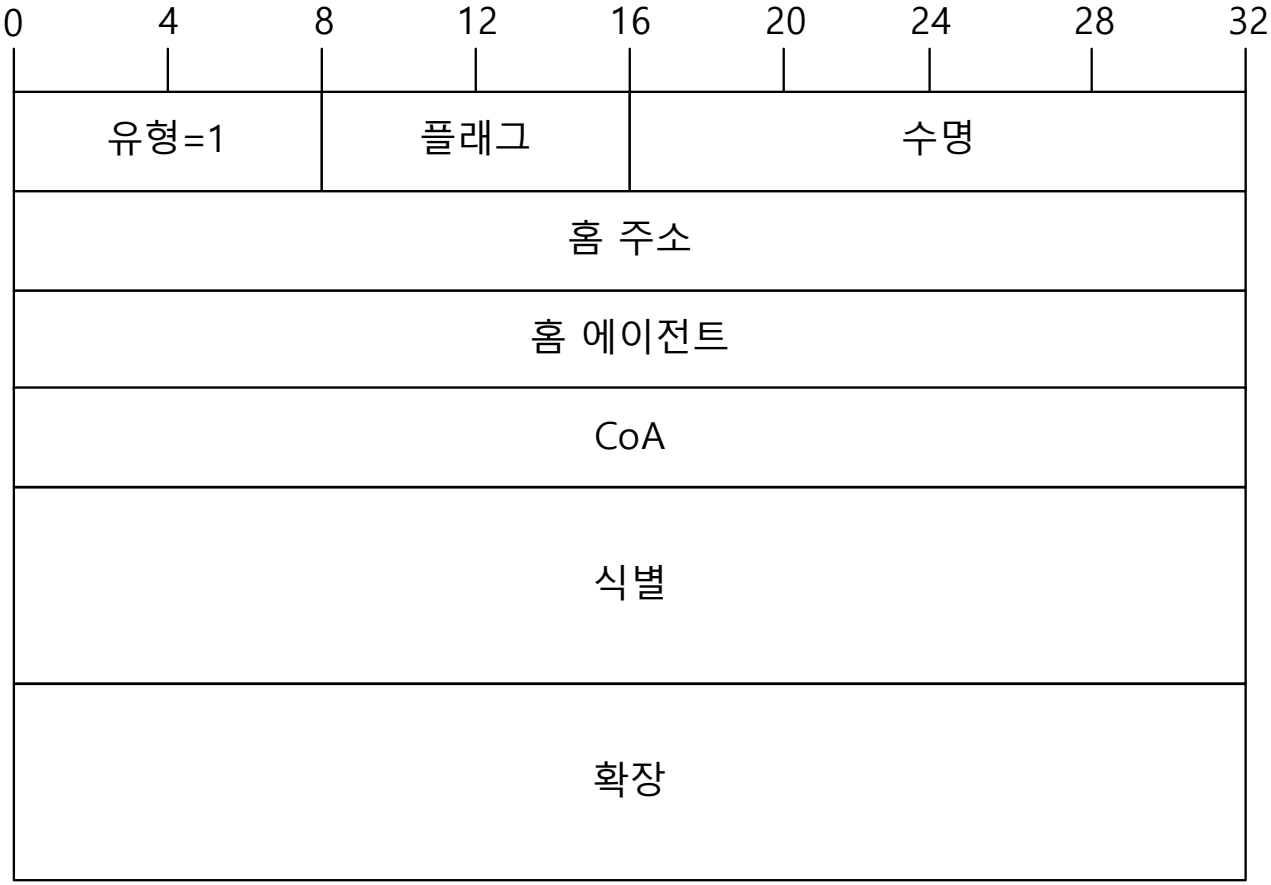
필드 명	크기(바이트)	설명
유형	1	메시지 유형 식별
코드	1	사용되지 않음, 0으로 설정
체크섬	2	요청 메시지에 대한 체크섬
예약됨	1	사용되지 않음, 0으로 설정

모바일 IP 프로토콜

- 모바일 IP 에이전트 등록
  - 이동 장비는 홈 에이전트에 자신의 CoA 등록
  - 등록 과정
    - 공존 CoA
      1. 이동 장비가 등록 요청을 홈 에이전트에게 전송
      2. 홈 에이전트는 이동 장비에게 등록 응답 전송
    - 외부 에이전트 CoA
      1. 이동 장비가 등록 요청을 외부 에이전트에게 전송
      2. 외부 에이전트가 등록 요청을 처리하여 홈 에이전트에게 전송
      3. 홈 에이전트는 외부 에이전트에게 등록 응답 전송
      4. 외부 에이전트는 등록 응답을 받아 처리하여 이동 장비에게 전송

모바일 IP 프로토콜

- 모바일 IP 에이전트 등록
  - 등록 요청 메시지 포맷



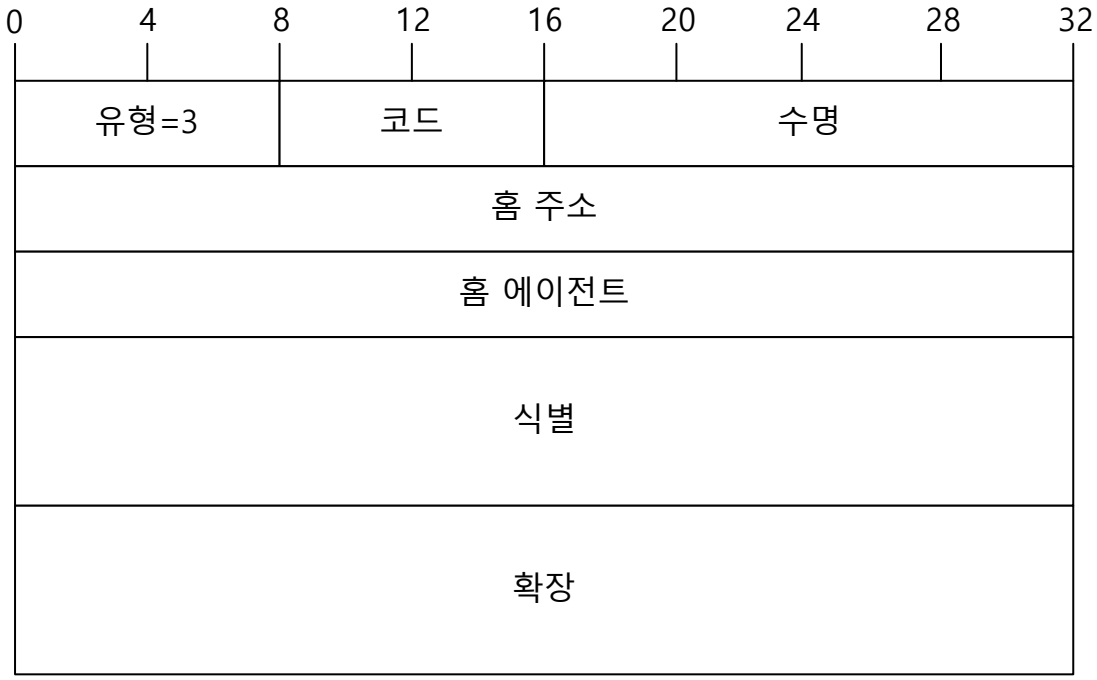
모바일 IP 프로토콜

- 모바일 IP 에이전트 등록
  - 등록 요청 메시지 포맷

필드 명	크기(바이트)	설명
유형	1	• 등록 메시지 유형 식별, 요청일 경우 1
플래그	1	• 이동 장비가 홈 에이전트에게 요청하는 것을 나타낸 정보 플래그
수명	2	• 이동 장비가 등록에 대해 요청하는 초 단위 등록 수명
홈 주소	4	• 이동 장비가 홈 네트워크에서 사용한 IP 주소
홈 에이전트	4	• 홈 에이전트의 IP 주소
CoA	4	• 이동 장비의 CoA
식별	8	• 등록 요청을 고유하게 식별하는 번호 • 응답과 요청을 한 쌍으로 묶기 위함
확장	가변	• 요청을 인증하기 위해 필요한 확장 필드

모바일 IP 프로토콜

- 모바일 IP 에이전트 등록
  - 등록 응답 메시지 포맷



필드 명	크기(바이트)	설명
코드	1	• 등록 요청에 대한 결과 • 0이면 등록이 허용됨 • 1이면 등록이 허용되지 않음

모바일 IP 프로토콜

- 모바일 IP 데이터 캡슐화
  - 홈 에이전트가 데이터그램을 이동 장비의 CoA로 재전송하기 위해 캡슐화하는 것
  - IP-in IP(IP Encapsulation within IP)
    - 하나의 IP 데이터그램을 다른 IP 데이터그램에 캡슐화하는 기법
    - 모바일 IP에서 새 헤더는 캡슐화한 데이터그램을 이동 장비의 CoA로 전송할 것을 명시

모바일 IP 프로토콜

- 모바일 IP 터널링
  - 모바일 IP 터널
    - 홈 에이전트가 이동 장비에게 보내는 캡슐화된 데이터그램이 거치는 경로
  - 과정
    - 외부 에이전트 CoA
      1. 터널은 데이터그램을 캡슐화하는 홈 에이전트에서 시작됨
      2. 캡슐화된 메시지를 외부 에이전트가 받아 외부 IP 헤더 제거
      3. 외부 에이전트가 이동 장비에게 데이터그램 전달
      4. 외부 에이전트에서 터널이 끝남
    - 공존 CoA
      1. 터널은 데이터그램을 캡슐화하는 홈 에이전트에서 시작됨
      2. 이동 장비에서 메시지를 받아 외부 IP 헤더 제거
      3. 이동 장비에서 터널이 끝남

모바일 IP 프로토콜

- 모바일 IP 역터널링
  - 필요 시 사용하는, 이동 장비와 홈 에이전트 사이 혹은 외부 에이전트와 홈 에이전트 사이의 터널을 통한 통신
  - 필요한 경우
    - 이동 장비가 특정 보안 규칙을 포함한 네트워크 진입으로 인해 자신의 원래 IP 주소로 메시지 전송이 어려울 경우
      - 스푸핑 방지를 위하여 네트워크가 자신의 네트워크 접두사와 불일치하는 출발지 주소를 사용한 메시지 전송을 불허할 때

모바일 IP 프로토콜

- 모바일 IP와 주소 결정 프로토콜(ARP, Address Resolution Protocol)
  - 홈 네트워크의 장비들이 홈 네트워크에서 이동 장비의 하드웨어 주소를 찾으려 메시지를 보내는 문제가 있음
  - 해결 방법
    - ARP 프록싱(ARP Proxing)
      - 홈 에이전트는 수신한 모든 ARP 요청에 대해 자신의 하드웨어 주소를 알리고, 대신 전달받은 데이터그램을 이동 장비에게 전송
    - 무상 ARP(Gratuitous ARP)
      - 이동 장비가 네트워크를 벗어난 순간 로컬 호스트의 기존 캐시 값이 무의미해짐
      - 홈 에이전트는 호스트들에게 무상 ARP 메시지를 전송하여 이동 장비의 하드웨어 주소가 홈 에이전트의 주소임을 알림
      - 로컬 호스트들은 캐시 값을 수정

모바일 IP 프로토콜

- 모바일 IP 비효율
  - 데이터그램을 항상 먼저 홈 네트워크로 보낸 후 다시 이동 장비에게 전달해야 함
    - 특히 이동 장비에게 메시지를 보내려는 장비가 이동 장비와 같은 네트워크에 있는 경우 비효율적임
  - 역터널링까지 사용하는 경우, 효율이 더 감소함

- 모바일 IP 보안 문제
  - 모바일 IP는 대체로 무선 네트워킹 사용
    - 전송이 공개되어 있음
      - 도청의 위험이 있음
      - 재전송 공격의 위험이 있음

Thanks!

강 민 채 (minchae@pel.sejong.ac.kr)