2022/04/10 2022 네트워크 세미나

TCP/IP 완벽 가이드

- 2-5부 IP 관련 기능 프로토콜 -

김 지 혜(jihye@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

목 차

- IP 관련 기능 프로토콜
  - IP 네트워크 주소 변환(NAT) 프로토콜
  - IP 보안 (IPsec, IP Security) 프로토콜
  - IP 이동성 지원(모바일 IP) 프로토콜

목 차

- IP 관련 기능 프로토콜
  - IP 네트워크 주소 변환(NAT) 프로토콜
  - IP 보안 (IPsec, IP Security) 프로토콜
  - IP 이동성 지원(모바일 IP) 프로토콜

IP NAT 프로토콜

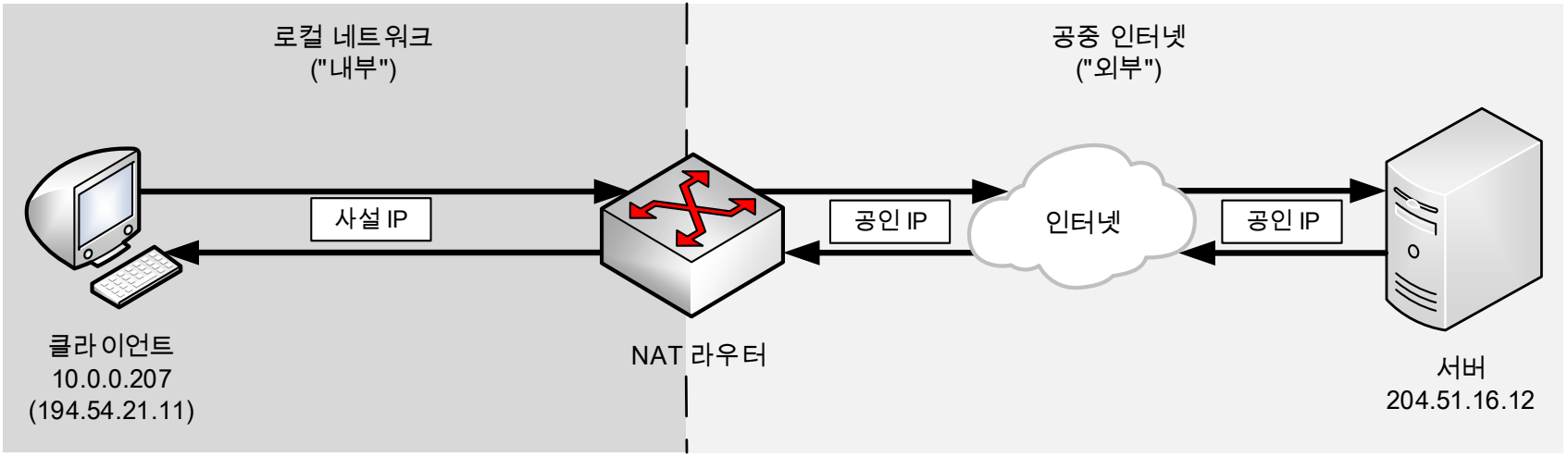
- IP 주소의 문제
  - 주소 공간 부족
    - 클래스 기반 주소 체계로 인한 주소 공간 부족
  - 주소 비용 증가
    - 할당하는 IP 주소가 증가할수록 그에 대한 비용도 증가
  - 보안 우려 증가
    - 악성 사용자의 네트워크 사용
    - 회사의 보안 위험 노출 증가

IP NAT 프로토콜

- IP 주소의 문제 해결 방법
  - 간접적인 네트워크 연결
    - 대부분의 호스트는 클라이언트 장비
      - 보통 클라이언트/서버 방식으로 동작
      - 클라이언트 입장에서 네트워크 외부에 존재하는 서버는 클라이언트와 직접적으로 연결될 필요가 없음
    - 인터넷 동시 접근 호스트가 많지 않음
      - 웹 서버에서 내용을 가져오는 동안만 접근한다고 표현
    - 라우팅 통신
      - 네트워크와 인터넷 간 통신은 라우터를 통해 이루어짐

IP NAT 프로토콜

- IP NAT(Network Address Translation) 개요
  - 정의
    - 공인 IP 주소와 사설 IP 주소를 상황에 맞게 변환하는 프로토콜
      - e.g., 공유기(라우터)
        - 내부 망과 외부 망 사이에서 중개자 역할을 하는 것



IP NAT 프로토콜

- IP NAT 개요
  - 공인 IP와 사설 IP
    - 공인 IP(Public IP)
      - 인터넷에서 사용자의 로컬 네트워크를 식별하기 위한 IP 주소
    - 사설 IP(Private IP)
      - 가정이나 회사 같은 로컬 네트워크에 할당된 IP 주소

	공인 IP	사설 IP
할당 주체	인터넷 서비스 공급자 (ISP, Internet Service Provider)	라우터(공유기)
할당 대상	개인 또는 회사의 서버(라우터)	개인 또는 회사의 기기
고유성	인터넷 상에서 유일한 주소	하나의 네트워크 안에서 유일
접근 여부	내/외부 접근 가능	외부 접근 불가능

IP NAT 프로토콜

- IP NAT 개요
  - 장점 (1/2)
    - 공인 IP 주소 공유
      - 하나의 공인 IP 주소에 여러 개의 사설 IP 주소 할당 가능
      - IP 주소 공간 부족 문제 해결
    - 쉬운 확장
      - 로컬 네트워크 장비는 공인 IP 주소를 이용하지 않기 때문에 로컬 네트워크에 장비를 추가하기 쉬움
    - 로컬 통제력 강화
      - 관리자가 로컬 네트워크만 관리하면 되기 때문에 관리하기 쉬움

IP NAT 프로토콜

- IP NAT 개요
  - 장점 (2/2)
    - 인터넷 서비스 제공자(ISP, Internet Service Provider) 변경 용이
      - 인터넷에 접속하기 위해 IP 주소를 할당하는 주체
      - 기관에서 ISP를 변경하는 경우에 공인 IP 주소만 변경하면 됨
        - 클라이언트 머신 주소를 다시 부여할 필요가 없음
    - 보안 강화
      - 내부 네트워크와 인터넷 사이에 생성된 방화벽
        - 간접 계층을 추가하는 것으로 볼 수 있음
      - 외부 공격자가 클라이언트에 직접 접근하기 어려움
        - 외부 공격자는 사설 네트워크의 내부 IP 주소를 알아야 접근 가능
        - 허용된 사용자는 할당된 공인 IP 주소를 통해 내부로 접근 가능

IP NAT 프로토콜

- IP NAT 개요
  - 단점 (1/2)
    - 복잡성
      - 네트워크 구성과 관리를 위한 추가 시스템이기에 관리의 복잡성
      - 주소 변환으로 인한 네트워크 문제 해결 복잡성
    - 공인 IP 주소 부족
      - 내부 클라이언트에 공인 IP 주소가 없기에, 일부 애플리케이션 기능을 수행하지 못할 수 있음
    - 특정 애플리케이션과의 호환성 문제
      - 애플리케이션 데이터 영역이 아닌 IP 헤더 필드만 수정
        - e.g., FTP(File Transfer Protocol)
          - NAT를 이용할 경우, 명령어는 전달되나 해석이 불가하여 실제 데이터가 전송되지 않는다는 문제 발생
          - FTP 프로그램을 수동 모드(Passive Mode)로 설정하여 문제 해결

IP NAT 프로토콜

- IP NAT 개요
  - 단점 (2/2)
    - 보안 프로토콜 문제
      - e.g., IPsec는 헤더 변조를 탐지하기에, NAT에 의한 변경과 악성 데이터그램 해킹을 구분하기 어려워함
    - 클라이언트 접근 지원 미비
      - 클라이언트에는 공인 IP 주소가 없기 때문에, 정당한 접근도 어려움
      - 피어투피어 설정이 어려움
    - 성능 감소
      - 데이터가 내부 네트워크와 인터넷을 오갈 때마다 주소 변환 필요

IP NAT 프로토콜

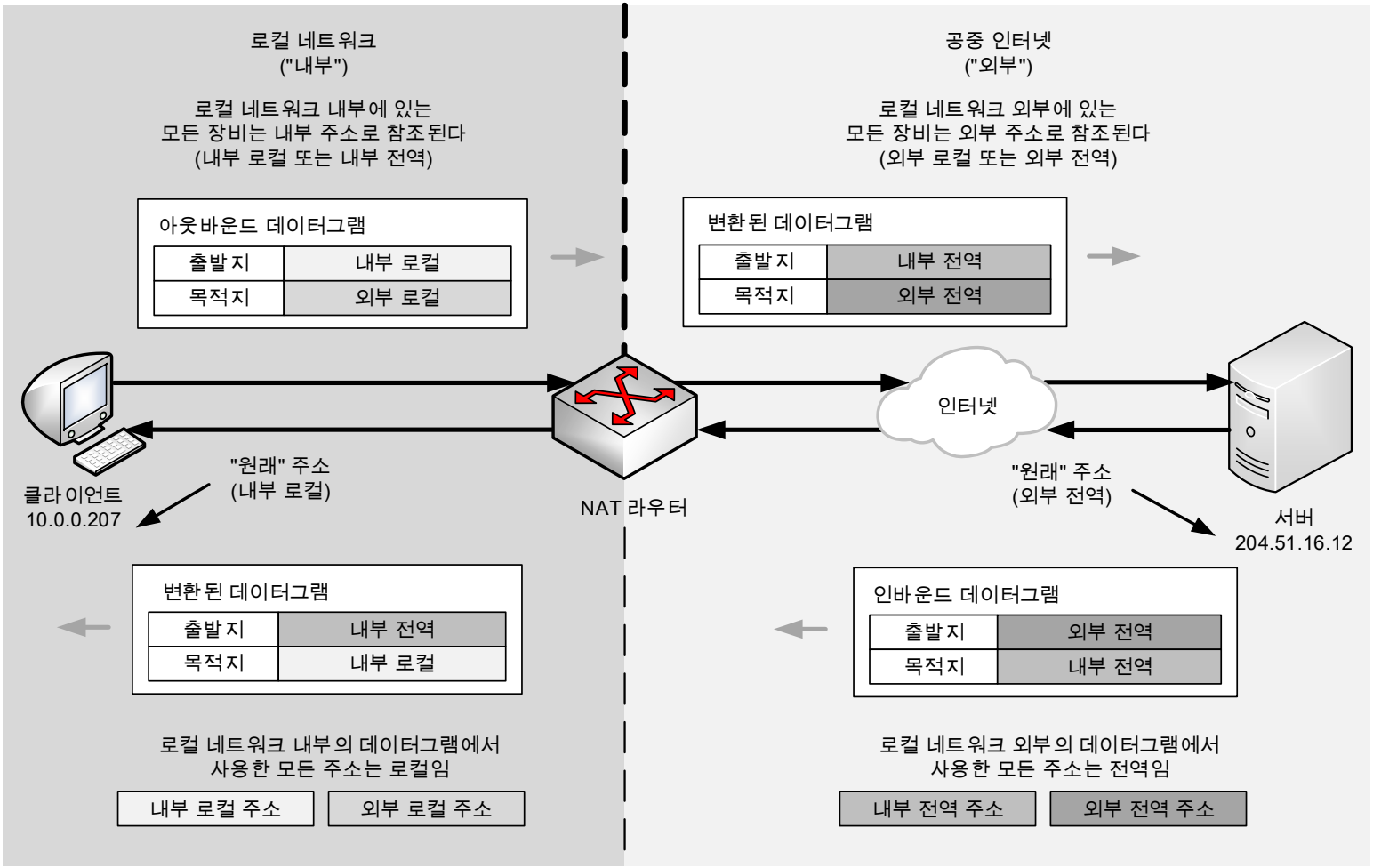
- IP NAT 주소
  - 주소가 참조하는 장비 위치에 따른 주소
    - 내부 주소(Inside Address)
      - 로컬 네트워크 내에 있는 모든 장비의 주소
    - 외부 주소(Outside Address)
      - 공중 인터넷에 있는 장비의 주소
  - 데이터그램이 나타나는 네트워크 위치에 따른 주소
    - 로컬 주소(Local Address)
      - 내부 네트워크의 데이터그램에 나타나는 주소
    - 전역 주소(Global Address)
      - 외부 네트워크의 데이터그램에 나타나는 주소

IP NAT 프로토콜

- IP NAT 주소
  - IP NAT에서의 네 가지 주소 유형
    - 내부 로컬 주소(Inside Local Address)
      - 내부 네트워크의 내부 장비 주소
    - 내부 전역 주소(Inside Global Address)
      - 내부 장비를 외부 네트워크에 표현하기 위해 변환된 주소
    - 외부 전역 주소(Outside Global Address)
      - 외부 네트워크의 외부 장비 주소
    - 외부 로컬 주소(Outside Local Address)
      - 외부 장비를 내부 네트워크에 표현하기 위해 변환된 주소

IP NAT 프로토콜

- IP NAT 주소
  - IP NAT에서의 네 가지 주소 유형



IP NAT 프로토콜

- IP NAT 주소
  - 정적 주소 매핑(Static NAT)
    - 개념
      - 하나의 사설 IP 주소와 하나의 공인 IP 주소를 경우에 따라 서로 변환하는 방식
    - 특징
      - 사설 IP 주소와 공인 IP 주소가 일대일로 매핑
      - 출발지와 목적지가 특정 IP 주소로 사전에 정의됨
      - 호환되지 않는 주소 체계를 가진 두 개의 네트워크가 서로 통신할 때 사용
      - 외부 네트워크에서 내부 네트워크로 접속할 경우 사용

IP NAT 프로토콜

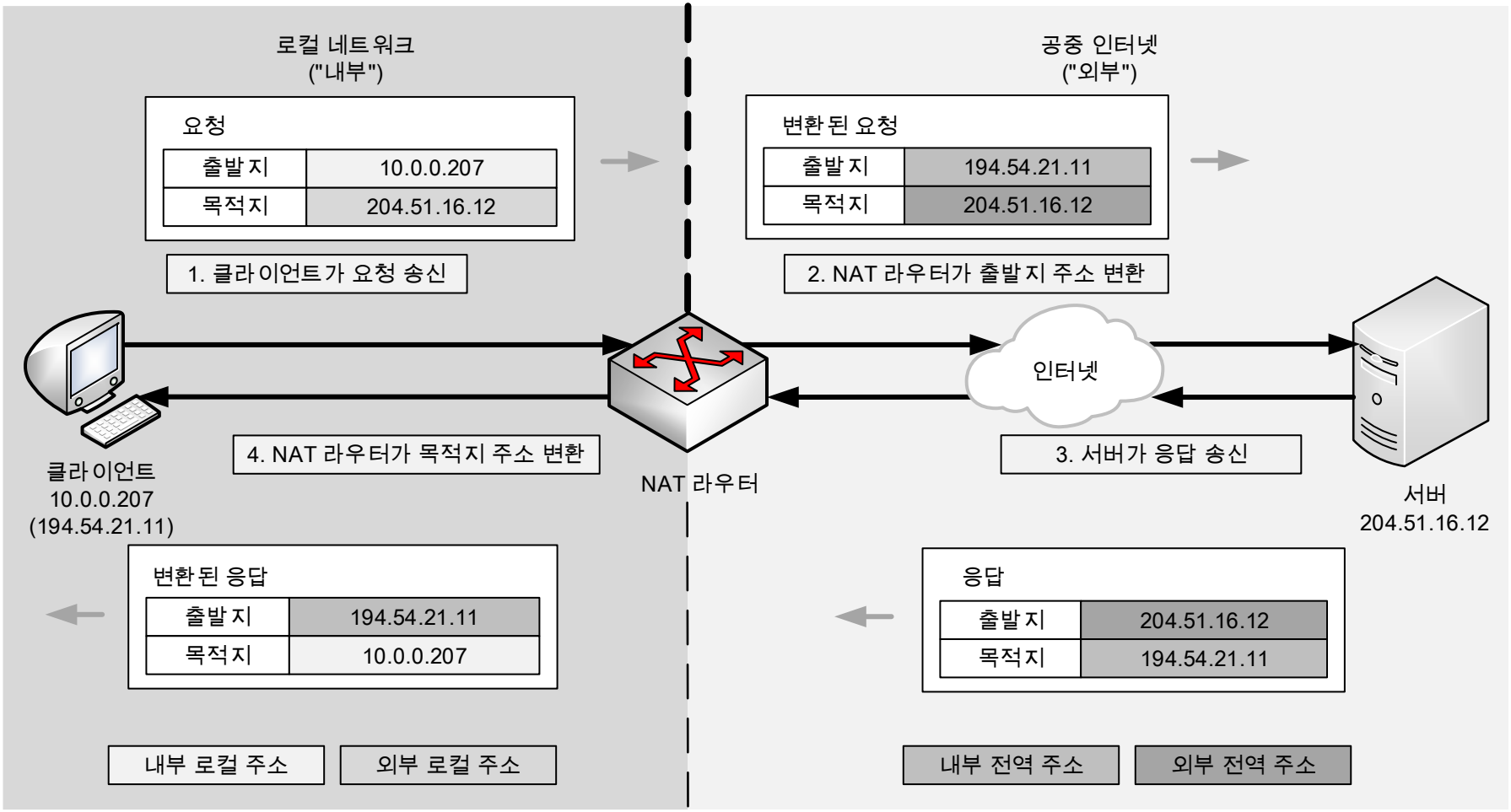
- IP NAT 주소
  - 동적 주소 매핑(Dynamic NAT)
    - 개념
      - 여러 개의 사설 IP 주소와 여러 개의 공인 IP 주소를 경우에 따라 서로 변환하는 방식
    - 특징
      - 사설 IP 주소와 공인 IP 주소가 그룹 대 그룹으로 매핑
      - 출발지나 목적지 중 최소 한 곳은 IP 주소 풀(Pool)로 설정되어야 함
      - 정해진 주소 풀(Pool)에 있는 주소들 중 사용되고 있지 않은 한 주소로 변환
        - 주소는 매번 새로 생성했다가 세션이 완료되면 다시 풀로 반환됨
      - 공인 IP 주소를 효율적으로 사용
        - 공인 IP 주소 개수가 사설 IP 주소 개수보다 적을 때 사용

IP NAT 프로토콜

- IP NAT 동작 방식
  - IP NAT 단방향(전통적/아웃바운드) 동작
    - 내부 네트워크에서 외부 네트워크로 사설 IP 주소를 공인 IP 주소로 변환하여 공유하는 방식
    - 내부 클라이언트의 요청과 외부 서버의 응답으로 이루어짐
    - 주소 변환
      - 외부로 송신 시 출발지 주소는 내부 로컬 주소에서 내부 전역 주소로 변환
      - 내부로 회신 시 목적지 주소는 내부 전역 주소에서 내부 로컬 주소로 변환

IP NAT 프로토콜

- IP NAT 동작 방식
  - IP NAT 단방향(전통적/아웃바운드) 동작

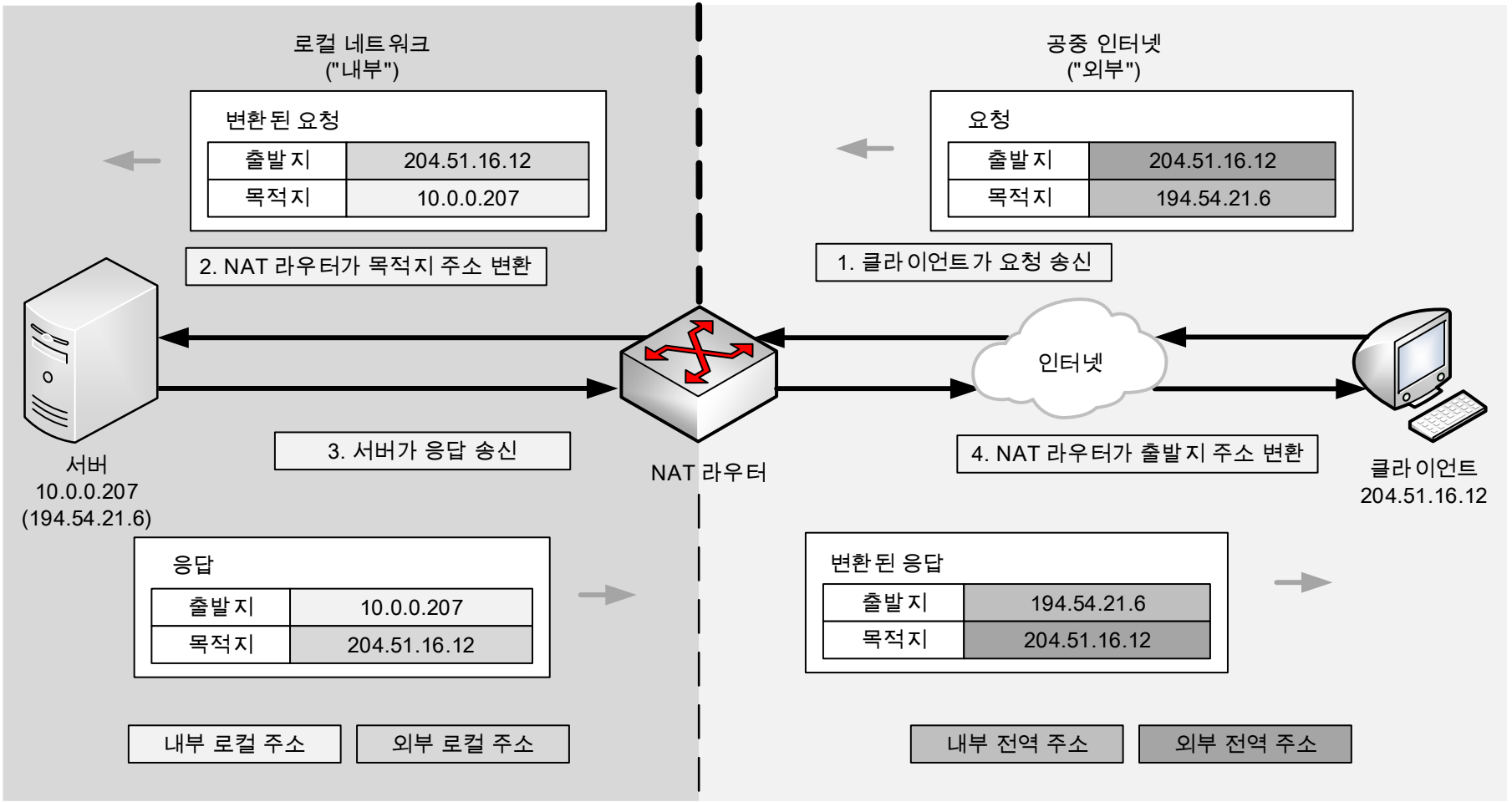


IP NAT 프로토콜

- IP NAT 동작 방식
  - IP NAT 양방향(Two-Way/인바운드) 동작
    - 외부 네트워크에서 내부 네트워크로 접근 가능한 방식
    - 외부 클라이언트의 요청과 내부 서버의 응답으로 이루어짐
    - 외부에서 내부로 접근하는 방법
      - 정적 주소 매핑 사용
      - DNS(Domain Name Service) 사용
    - 주소 변환
      - 내부로 송신 시 목적지 주소는 내부 전역 주소에서 내부 로컬 주소로 변환
      - 외부로 회신 시 출발지 주소는 내부 로컬 주소에서 내부 번역 주소로 변환

IP NAT 프로토콜

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

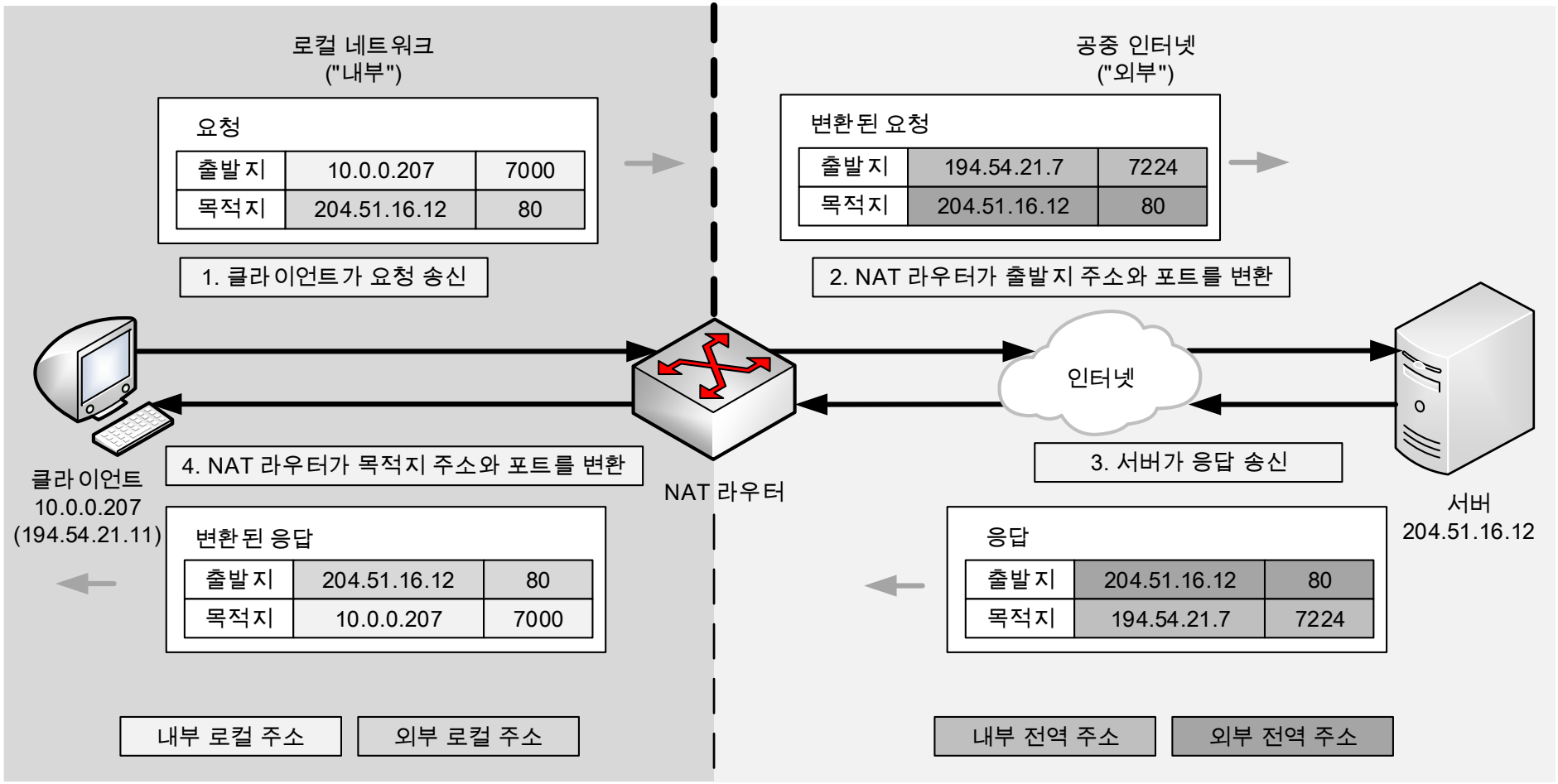


IP NAT 프로토콜

- IP NAT 동작 방식
  - IP NAT 포트 기반 동작(PAT, Port Address Translation)
    - 포트 번호를 변환하여 다수의 내부 로컬 주소가 동시에 하나의 내부 전역 주소를 공유하는 방식
      - TCP, UDP에서 사용하는 포트 번호
    - 주소 변환
      - 외부로 송신 시 출발지 주소와 포트를 내부 로컬 주소에서 내부 전역 주소로 변환
      - 내부로 회신 시 목적지 주소와 포트를 내부 전역 주소에서 내부 로컬 주소로 변환

IP NAT 프로토콜

- IP NAT 동작 방식
  - IP NAT 포트 기반 동작(PAT)

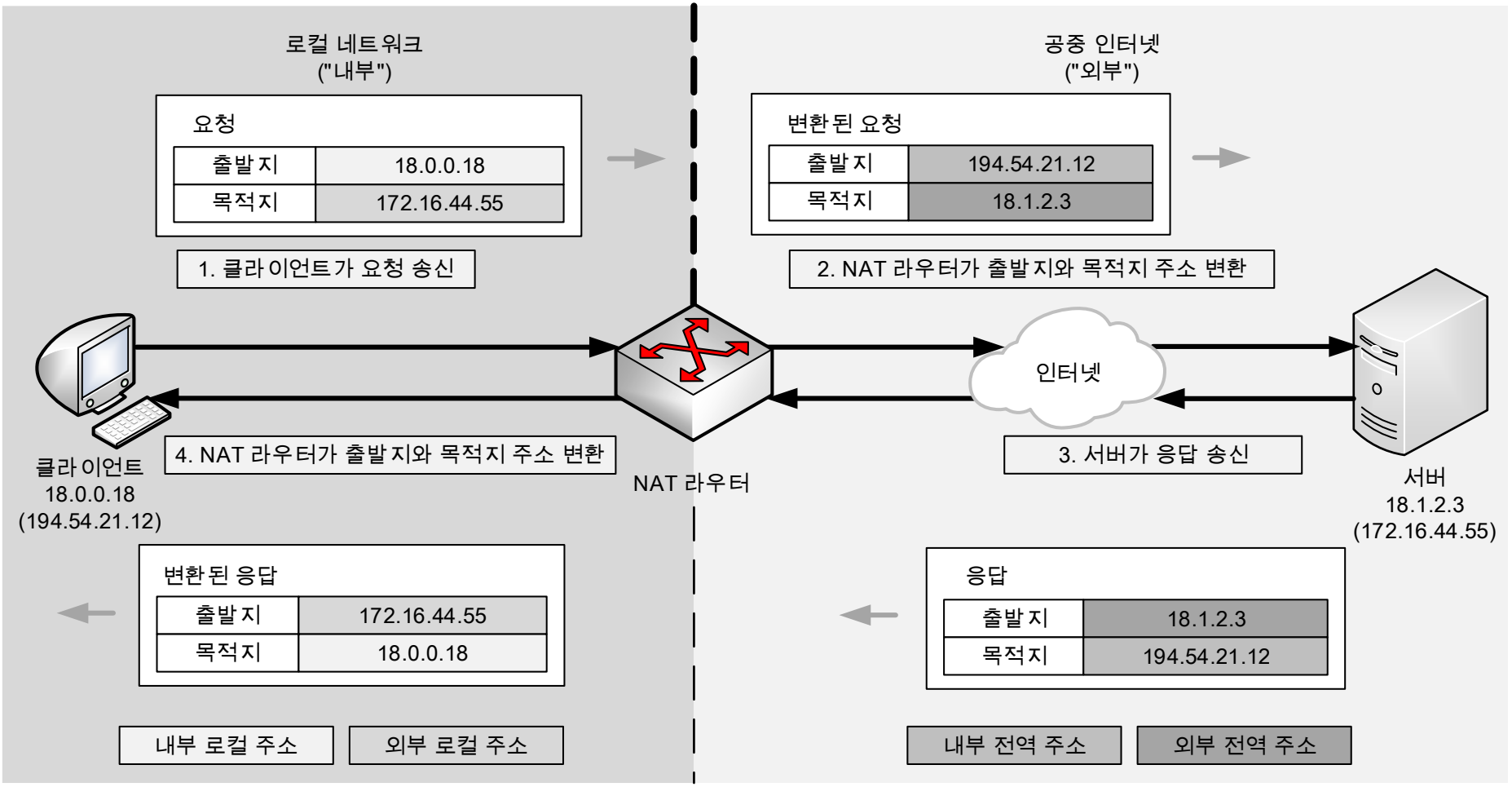


IP NAT 프로토콜

- IP NAT 동작 방식
  - IP NAT 중복 동작(2회 NAT 동작)
    - 내부 네트워크와 외부 네트워크가 중복 주소를 다루기 위한 방식
    - 주소가 중복되는 경우
      - 내부 네트워크와 내부 네트워크 간의 연결
        - 두 네트워크가 같은 주소 지정 방법을 사용하고 있는 경우
      - 내부 네트워크에 공인 IP 주소를 부적절하게 할당
      - 공인 IP 주소 할당의 유효 기간 만료
    - 주소 변환
      - 외부로 송신 시 출발지 주소를 내부/외부 로컬 주소에서 내부/외부 전역 주소로 변환
      - 내부로 회신 시 목적지 주소를 내부/외부 전역 주소에서 내부/외부 로컬 주소로 변환

IP NAT 프로토콜

- IP NAT 동작 방식
  - IP NAT 중복 동작(2회 NAT 동작)



IP NAT 프로토콜

- IP NAT 호환성
  - 호환성 문제
    - TCP와 UDP 체크섬 재계산
      - 헤더의 IP 주소를 변경한다는 의미
      - 체크섬은 출발지와 목적지 주소가 포함된 가상 헤더에 대해 계산되기 때문에 주소 변환 시 다시 계산되어야 함
    - ICMP 조작
      - NAT는 IP 헤더 부분을 변환하기 때문에, IP와 같이 사용되는 ICMP 메시지에 포함된 헤더 주소를 필요에 맞게 변환해야 함
    - 포트 변환에서의 추가적 문제
      - PAT 사용 시, 주소가 아닌 포트에서 문제 발생
    - 주소나 포트 번호 변경에 의한 파급 효과
      - 주소나 포트 번호를 치환하는 경우에 페이로드의 크기가 변경되는 경우, 추가적인 작업 처리 필요

목 차

- IP 관련 기능 프로토콜
  - IP 네트워크 주소 변환(NAT) 프로토콜
  - IP 보안 (IPsec, IP Security) 프로토콜
  - IP 이동성 지원(모바일 IP) 프로토콜

IPsec 프로토콜

- IPsec(Internet Protocol Security) 개요
  - 정의
    - 네트워크 계층에서 보안을 제공하는 프로토콜의 모음
    - IP의 안전한 통신을 보장하는 기술
      - e.g.,
        - IP 데이터그램의 송신지 위조
          - 진짜 은행에서 왔는지 공격자에게서 왔는지
        - 사생활 문제
          - 사적인 대화 내용 유출

IPsec 프로토콜

- IPsec 개요
  - 기능
    - 기밀성 보장
      - ESP(Encapsulating Security Payload) 프로토콜에서 제공하는 대칭 암호화를 이용하여 IP 데이터그램 암호화
    - 무결성 보장 및 데이터 송신지 인증
      - AH(Authentication Header) 프로토콜에서 제공하는 메시지 인증 코드(MAC) 이용
    - 보안 공격 방지
      - e.g., 송신 측에서 IP 데이터그램 별로 순서 번호를 전송하고, 수신 측에서 이를 유지하며 재전송(replay) 공격 방지
    - 보안 알고리즘과 키 관리
      - 키 교환을 위해 IKE(Internet Key Exchange) 프로토콜 이용
    - 보안 모드
      - e.g., 터널(tunnel) 모드와 전송(transport) 모드

IPsec 프로토콜

- IPsec 표준

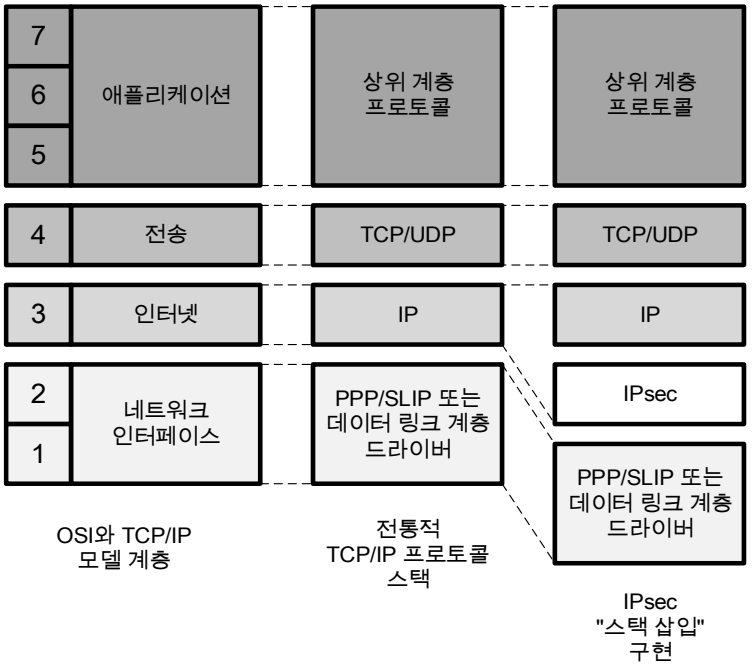
RFC 번호	이름	설명
2401	Security Architecture for the Internet Protocol	주요한 IPsec 표준 문서로, IPsec 기술 구조와 일반 동작, 여러 구성 요소가 어떻게 쓰이는지 설명
2402	IP Authentication Header	데이터 무결성과 원본 검증을 보장하는 AH 프로토콜 정의
2403	The Use of HMAC-MD5-96 within ESP and AH	AH와 ESP 프로토콜에서 사용하는 암호화 알고리즘인 MD5, HMAC의 변종 설명
2404	The Use of HMAC-SHA-1-96 within ESP and AH	AH와 ESP 프로토콜에서 사용하는 암호화 알고리즘인 SHA-1, HMAC의 변종 설명
2406	IP Encapsulating Security Payload(ESP)	기밀성을 위해 데이터를 암호화하는 ESP 프로토콜 설명
2408	Internet Security Association and Key Management Protocol(ISAKMP)	키 교환 및 보안 연관 협상 방법 정의
2409	The Internet Key Exchange(IKE)	두 장비 간 안전한 통신을 위한 보안 연관 협상 및 키 교환에 쓰이는 IKE 프로토콜 설명
2412	The OAKLEY Key Determination Protocol	키 교환을 위한 범용 프로토콜 설명

IPsec 프로토콜

- IPsec 구현 방법
  - 종단 호스트 구현
    - 모든 호스트 장비에 IPsec을 설치함으로써, 보안성을 높임
    - 다수의 호스트가 존재하기 때문에 라우터 구현보다 많은 작업 필요
  - 라우터 구현
    - 클라이언트와 연결된 라우터 간에 IPsec을 설치
    - 다수의 클라이언트 대신 소수의 라우터를 변경하기 때문에 호스트 구현보다 적은 작업 필요
    - 라우터와 로컬 호스트 사이의 연결은 보호되지 않음
      - 외부 이동만 보호하기 때문

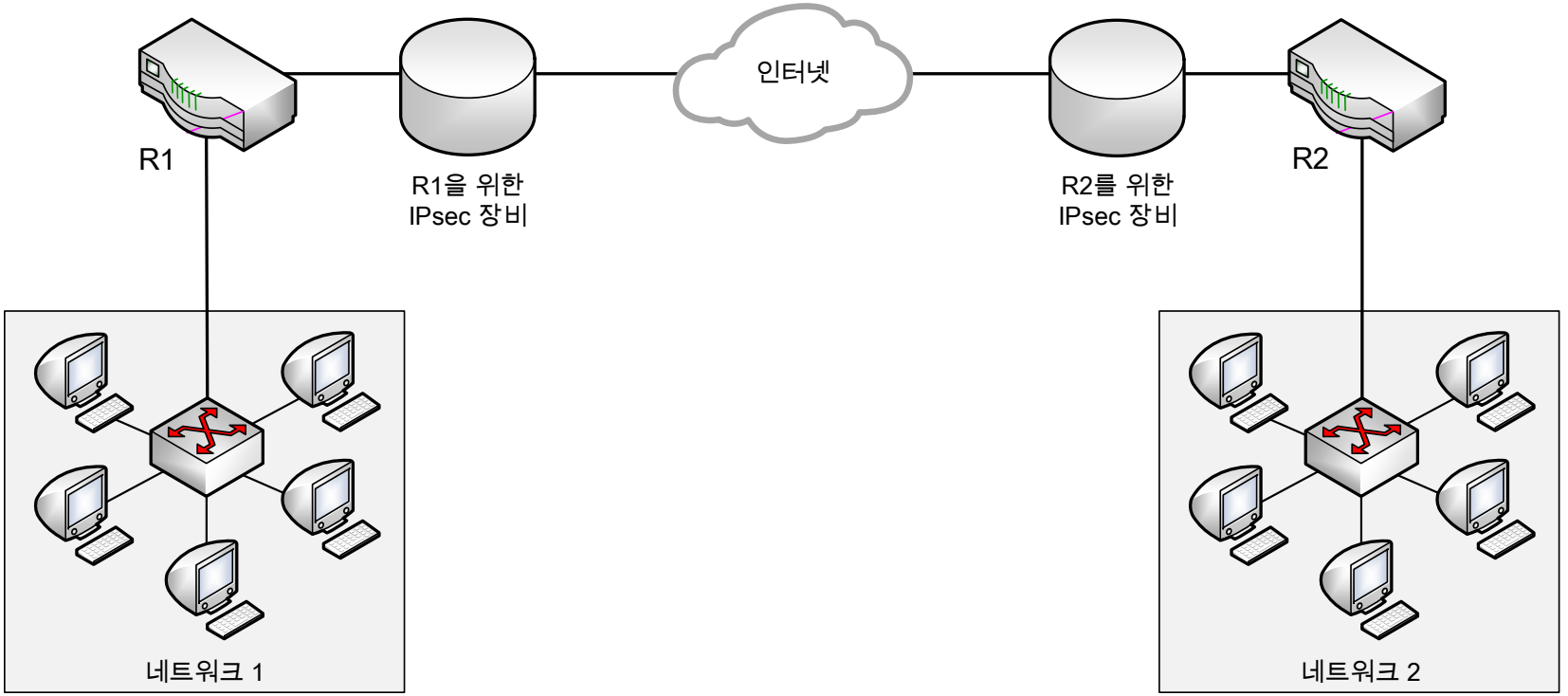
IPsec 프로토콜

- IPsec 구조
  - 통합 구조
    - IPsec 프로토콜과 기능을 IP 자체에 통합
    - 추가 하드웨어나 계층이 필요하지 않음
  - 스택 삽입(BITS, Bump In The Stack) 구조
    - 별도의 계층으로 존재
      - IP 장비에 IPsec 추가 가능
    - IP 데이터그램에 보안 기능을 덧붙인 후 전달
    - 통합 구조에 비해 TCP/IP 스택이 해야 할 일 증가
    - 보통 IPv4 호스트에 사용



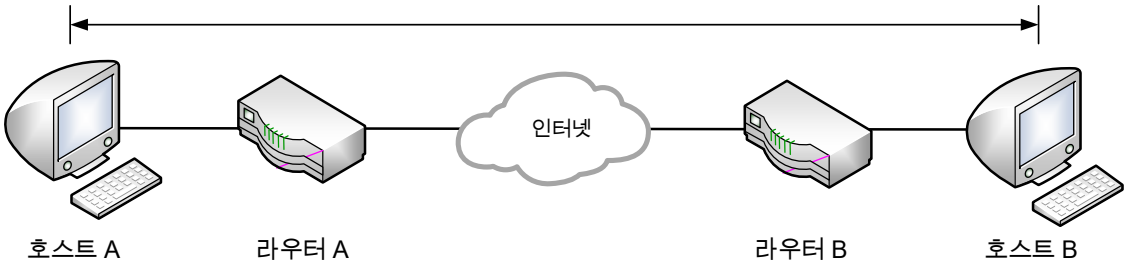
IPsec 프로토콜

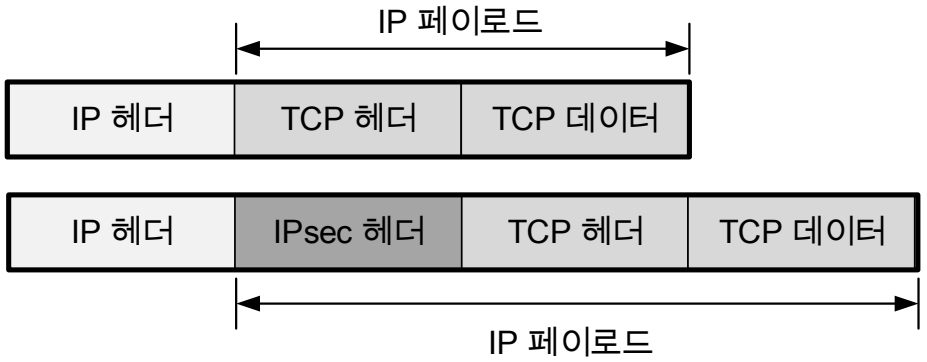
- IPsec 구조
  - 라인 삽입(BITW, Bump In The Wire) 구조
    - 라우터와 인터넷 사이에 특수 IPsec 장비 추가 가능
      - 외부로 송신 시 데이터그램에 IPsec 보호 기능 추가
      - 내부로 수신 시 데이터그램의 IPsec 관련 헤더 제거



IPsec 프로토콜

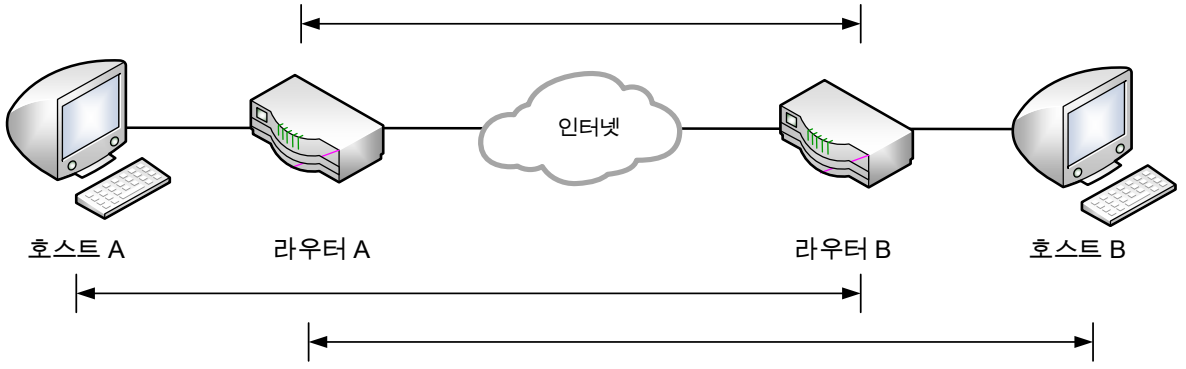
- IPsec 모드
  - 전송 모드(Transport Mode)
    - IP 헤더를 제외한 페이로드만 보호하는 모드
    - 특징
      - 원본 IP 데이터그램이 생성될 때, 데이터그램 속 IP 페이로드 앞에 IPsec 헤더 추가
      - 호스트가 IPsec 헤더를 추가해주기 때문에 IPsec을 적용한 데이터가 다른 호스트로 전송될 때, 두 호스트를 제외하고는 데이터를 볼 수 없음

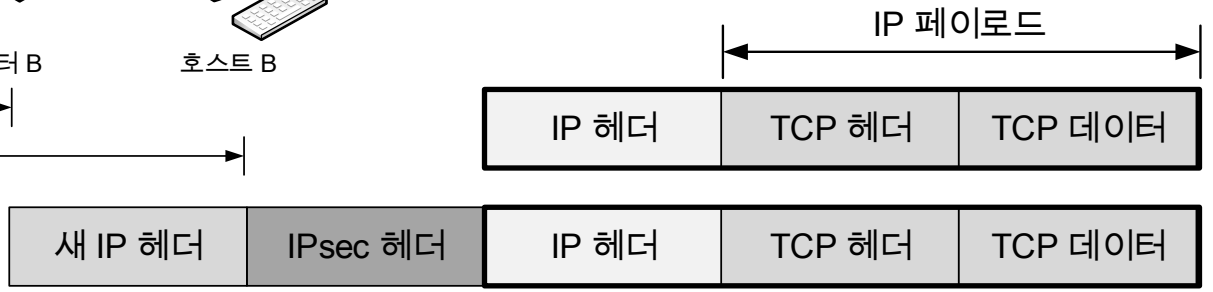




IPsec 프로토콜

- IPsec 모드
  - 터널 모드(Tunnel Mode)
    - IP 패킷 전체를 보호하는 모드
    - 특징
      - 원본 IP 데이터그램이 생성된 후, 해당 IP 데이터그램 전체 앞에 IPsec 헤더 추가
      - 두 개의 라우터 간, 호스트와 라우터 간 데이터 전송 시 사용
        - 라우터가 IPsec 헤더와 새 IP 헤더를 추가해주기 때문





IPsec 프로토콜

- IPsec 보안 구성 요소
  - 보안 연관(SA, Security Association)
    - 두 장비 사이에 맺은 보안 연결을 설명하는 보안 정보
    - 특징
      - 장비들은 각각 인바운드와 아웃바운드를 위한 2개의 SA 필요
      - 보안 연관 데이터베이스(SAD, Security Association Database)에 포함
    - SA를 정의하는 트리플(Triple)
      - 보안 인자 색인
        - 데이터그램 수신자가 데이터그램에 어떤 SA가 적용되는지 파악
      - IP 목적지 주소
        - SA가 수립된 장비 주소
      - 보안 프로토콜 식별자
        - SA가 AH(Authentication Header)와 ESP(Encapsulating Security Payload) 중 어느 것을 위한 것인지 지정

IPsec 프로토콜

- IPsec 보안 구성 요소
  - 보안 정책(SP, Security Policy)
    - 장비가 송·수신하는 서로 다른 데이터그램 처리 방법 지시
      - e.g., IPsec 내 특정 데이터그램 처리 필요 여부 결정
    - 보안을 어떻게 제공할 지에 대한 지침 제시
    - 보안 정책 데이터베이스(SPD, Security Policy Database)에 저장되어 있음
  - 선택자(Selector)
    - 장비가 특정 데이터그램에 어떤 보안 정책이나 보안 연관을 사용할 지 결정하는 규칙 모음

IPsec 프로토콜

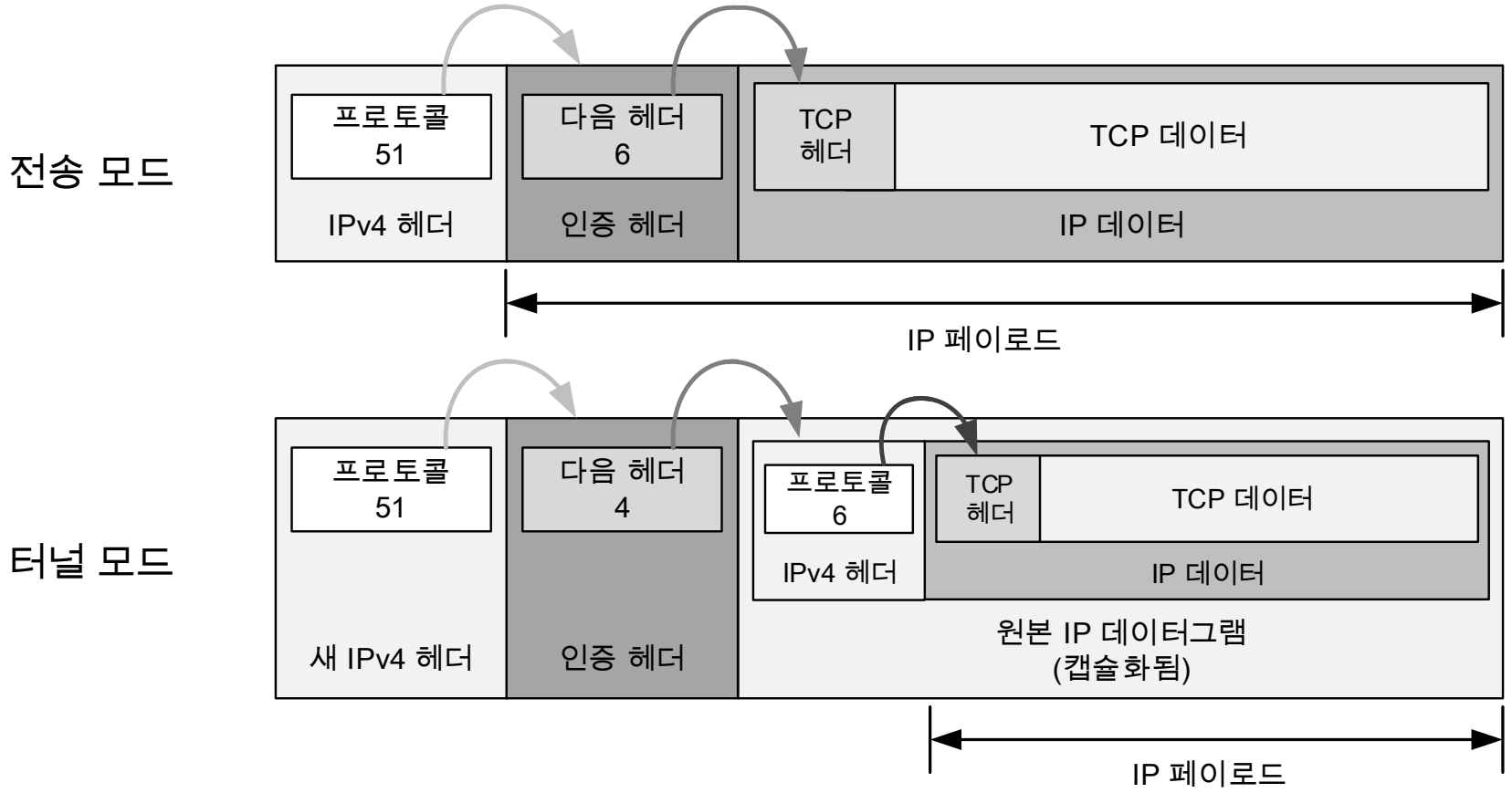
- IPsec 핵심 프로토콜
  - IPsec 인증 헤더(AH, Authentication Header)
    - 정의
      - 두 개의 시스템이 송·수신하는 IP 데이터그램에 대한 인증을 제공하는 프로토콜
    - 특징
      - 송신지 인증 및 데이터 무결성 보장
        - 메시지 인증 코드(MAC)는 데이터가 변조되었는지를 검증할 수 있도록 데이터에 덧붙이는 코드
      - 재전송 공격(Replay Attack)에 대해 보호 기능 제공
        - 송신 메시지에 순서 번호를 매회 1씩 증가시키며 넣음

IPsec 프로토콜

- IPsec 핵심 프로토콜
  - IPsec 인증 헤더(AH)
    - 동작 과정
      1. 특수 해싱 알고리즘과 특수 키를 사용하여 AH 계산
      2. 계산된 값(ICV, Integrity Check Value)을 다른 필드와 함께 특수 헤더에 넣어 전송
         - 헤더 위치는 IPsec 모드나 IP 버전에 따라 달라짐
      3. 공유되고 있는 키로 목적지 장비에서 동일한 방법으로 AH 계산 후 결과값 비교
         - 원본 데이터그램의 수정 여부 파악 가능

IPsec 프로토콜

- IPsec 핵심 프로토콜
  - IPsec 인증 헤더(AH)
    - AH 데이터그램 위치와 연결



IPsec 프로토콜

- IPsec 핵심 프로토콜
  - IPsec 인증 헤더(AH)
    - AH 포맷

필드 이름	크기 (바이트)	설명
다음 헤더	1	AH 다음 헤더의 프로토콜 번호 저장, 헤더 연결에 사용
페이로드 길이	1	인증 헤더 자체의 길이 측정
예약	2	사용되지 않고, 0으로 설정됨
SPI	4	목적지 주소와 AH와 함께 보안 연관(SA)을 식별
순서 번호	4	보안 연관을 사용하여 데이터그램 송신 시 증가, 재전송 공격으로부터 IPsec 방어 시 사용
인증 데이터	가변적	해싱 알고리즘의 계산 결과 (무결성 검사값) 포함

IPsec 프로토콜

- IPsec 핵심 프로토콜
  - IPsec 보안 페이로드 캡슐화(ESP, Encapsulating Security Payload)
    - 정의
      - 두 개의 시스템이 송·수신하는 IP 데이터그램에 대한 인증과 기밀성을 제공하는 프로토콜
    - 특징
      - 송신지 인증 및 데이터 무결성 보장
        - 메시지 인증 코드(MAC)는 데이터가 변조되었는지를 검증할 수 있도록 데이터에 덧붙이는 코드
      - IP 데이터그램을 암호화하여 기밀성 보장
        - 암호화 알고리즘은 데이터그램의 데이터를 키를 이용해 암호화 형태로 변환
        - 암호화된 데이터는 특수 포맷으로 포장되어 목적지로 전송
        - 목적지 장비는 동일 암호화 알고리즘을 이용해 데이터 복호화

IPsec 프로토콜

- IPsec 핵심 프로토콜
  - IPsec 보안 페이로드 캡슐화(ESP)
    - ESP 필드
      - ESP 헤더
        - 암호화된 데이터 앞에 위치
        - 보안 인자 인덱스(SPI) 필드와 순서 번호 필드를 포함
      - ESP 트레일러
        - 암호화된 데이터 뒤에 위치
        - 패딩과 패딩 길이 필드를 이용해 암호화된 데이터를 32비트에 맞춤
        - ESP의 다음 헤더 필드의 정보 포함
      - ESP 인증 데이터
        - 계산되는 무결성 검사값(ICV) 포함
        - 선택적인 인증 기능이 적용될 때 사용함

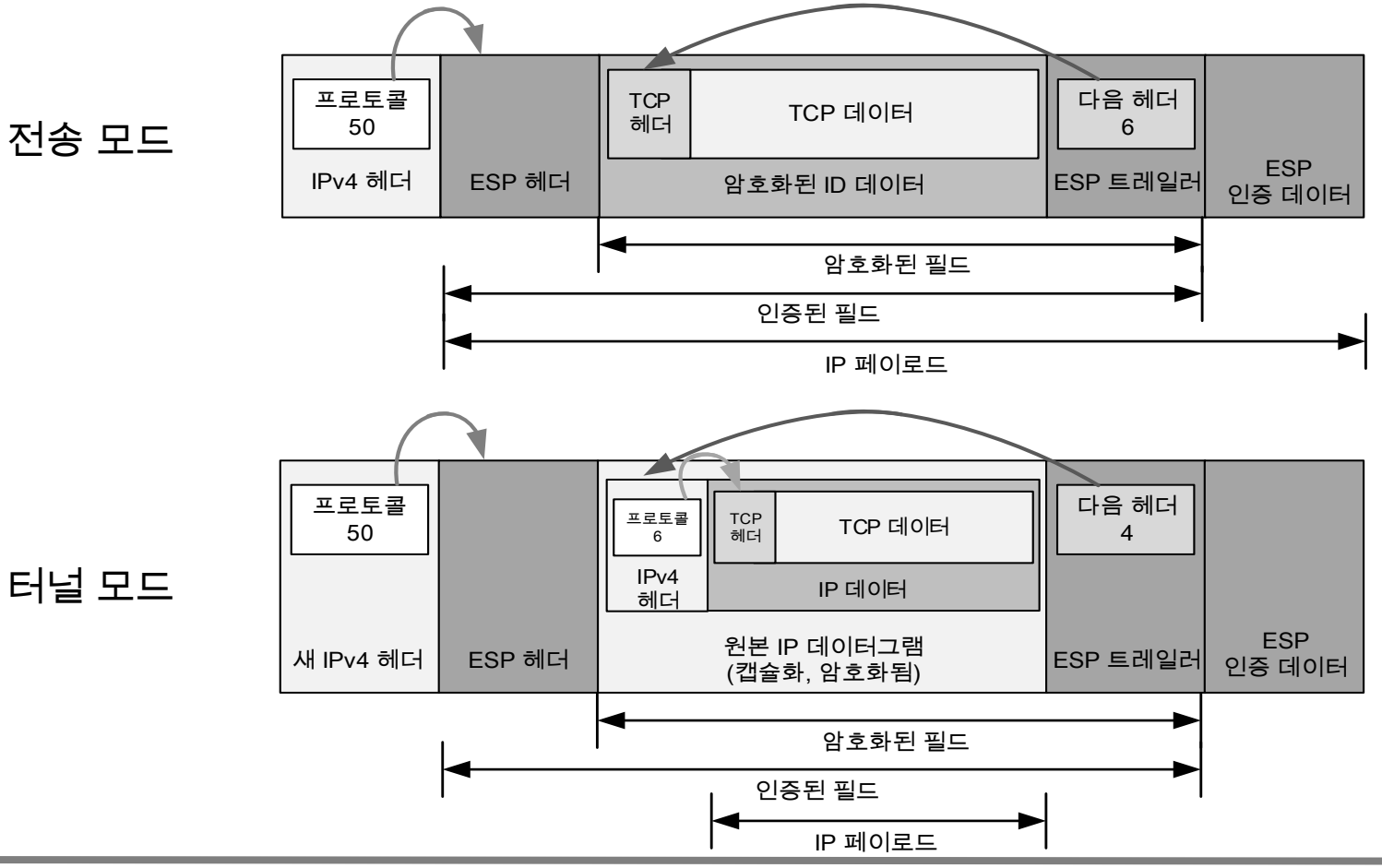
IPsec 프로토콜

- IPsec 핵심 프로토콜
  - IPsec 보안 페이로드 캡슐화(ESP)
    - ESP 동작 단계

1. 헤더 계산
   - 전송 모드에서, 원본 데이터그램의 IP 헤더 뒤에 위치
   - 터널 모드에서, 원본 데이터그램을 캡슐화하는 새 IP 데이터그램의 IP 헤더 뒤에 위치
2. 트레일러 계산
   - 트레일러 필드가 암호화될 데이터 뒤에 붙으면 ESP는 암호화 수행
   - 페이로드와 트레일러는 모두 암호화되지만, 헤더는 암호화되지 않음
3. 인증 필드 계산
   - 전체 ESP 데이터그램에 대한 인증 계산이 이루어짐
   - 계산 대상은 헤더, 페이로드, 트레일러

IPsec 프로토콜

- IPsec 핵심 프로토콜
  - IPsec 보안 페이로드 캡슐화(ESP)
    - ESP 데이터그램의 위치와 연결



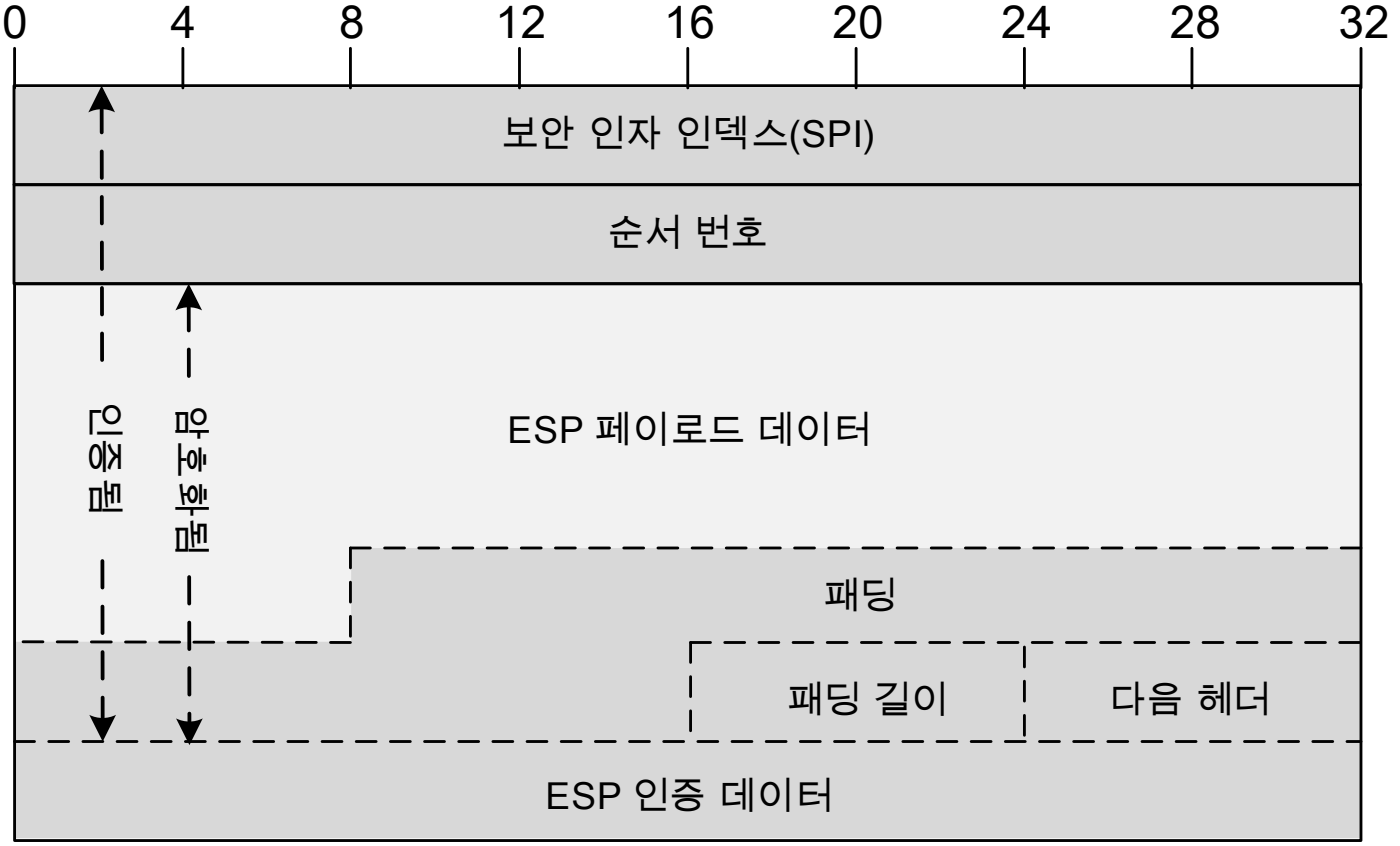
IPsec 프로토콜

- IPsec 핵심 프로토콜
  - IPsec 보안 페이로드 캡슐화(ESP)
    - ESP 포맷

구간	필드 이름	크기 (바이트)	설명	암호화 범위	인증 범위
ESP 헤더	SPI	4	목적지 주소와 ESP와 함께 보안 연관(SA) 식별		↕
	순서 번호	4	보안 연관을 사용하여 데이터그램 송신 시 증가, 재전송 공격으로부터 IPsec 방어 시 사용		
페이로드	페이로드	가변적	암호화된 페이로드 데이터	↕	
ESP 트레일러	패딩	가변적 (0~255)	암호화 또는 정렬을 위한 추가적인 패딩 바이트 포함		
	패딩 길이	1	패딩 필드의 바이트 수		
	다음 헤더	1	다음 헤더의 프로토콜 번호 저장 및 헤더 연결에 사용		
ESP 인증 데이터		가변적	계산된 무결성 결과값(ICV) 포함		

IPsec 프로토콜

- IPsec 핵심 프로토콜
  - IPsec 보안 페이로드 캡슐화(ESP)
    - ESP 포맷



IPsec 프로토콜

- IPsec 핵심 프로토콜
  - IPsec 인터넷 키 교환(IKE, Internet Key Exchange)
    - 정의
      - 두 장비가 보안 프로토콜에서 사용할 비밀 정보를 교환하기 위한 프로토콜
    - 동작 단계
      - ISAKMP(Internet Security Association and Key Management Protocol) 단계로 구성
        - 암호화 키와 보안 연관 정보 교환을 위한 구조 제공하는 프로토콜
      - 단계 1
        - 두 장비가 정보를 어떻게 안전하게 교환할지 협상
        - 협상을 통해 ISAKMP 자체를 위한 SA 생성
      - 단계 2
        - 생성된 SA를 이용하여 기타 보안 프로토콜을 위한 SA 생성
        - AH와 ESP 프로토콜을 위한 SA 인자 협상

목 차

- IP 관련 기능 프로토콜
  - IP 네트워크 주소 변환(NAT) 프로토콜
  - IP 보안 (IPsec, IP Security) 프로토콜
  - IP 이동성 지원(모바일 IP) 프로토콜

모바일 IP 프로토콜

- 모바일 IP(Mobile Internet Protocol) 개요
  - 이동 장비 문제
    - 네트워크 사이를 이동하기 때문에 IP 주소를 기반으로 라우팅할 수 없음
    - 해결 방안
      - IP 주소 변경
        - 이동한 네트워크의 네트워크 ID를 가지도록 호스트의 IP 주소 변경
      - IP 라우팅과 주소 간 연결 끊기
        - 전체 IP 주소를 보고 데이터그램을 전송하도록 라우팅 방식 바꿈
    - 해결 방안의 문제
      - 많은 시간이 걸림
        - IP 주소 바꿀 때마다 사람이 직접 관여해야 하기 때문
      - 다른 장비에게 변경된 주소를 알릴 방법이 없음
        - 이동 장비가 새 주소를 가져도, 다른 장비는 이동 장비의 원래 주소만 앎

모바일 IP 프로토콜

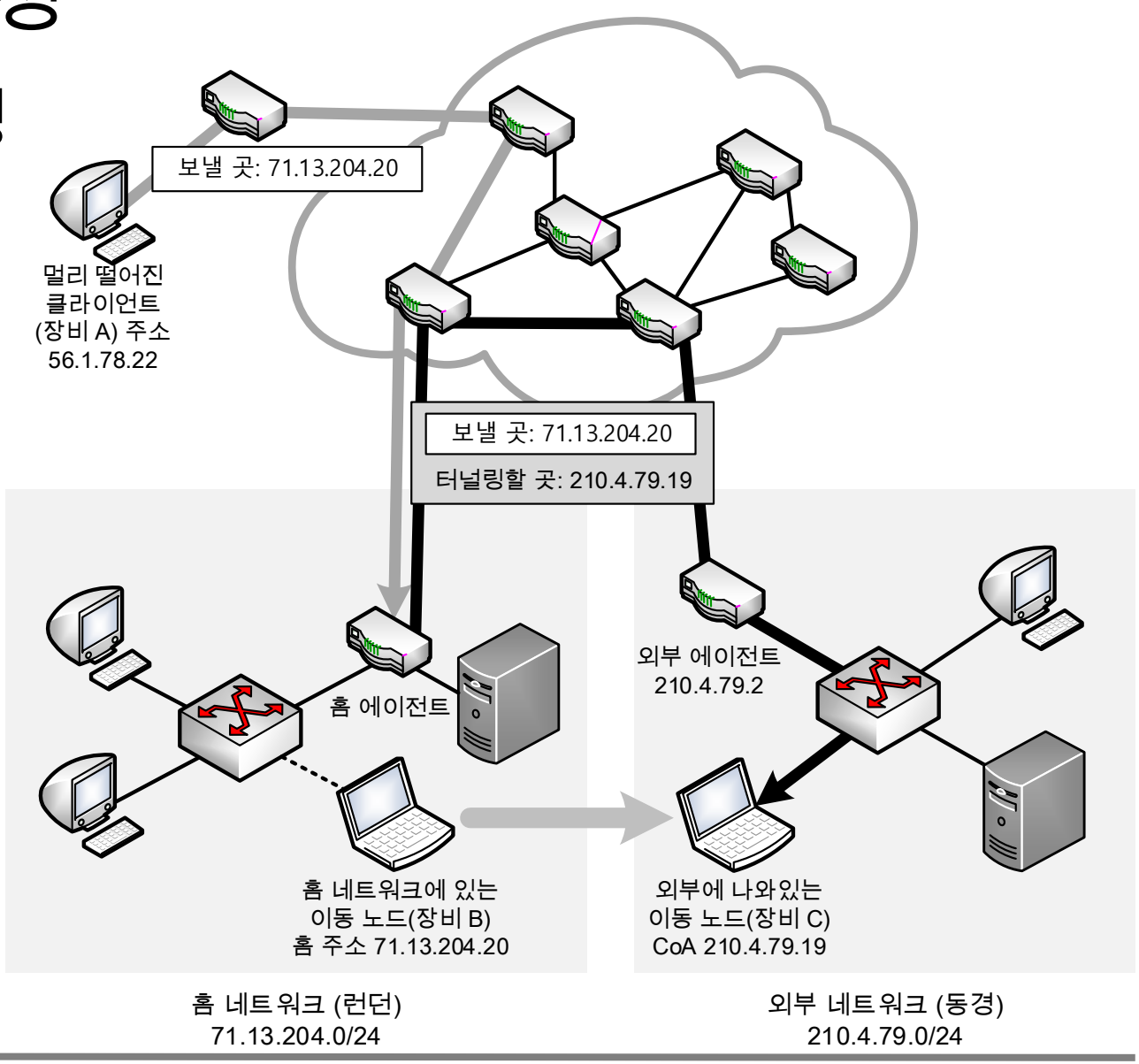
- 모바일 IP 개요
  - 목표
    - 기존 장비 주소 사용
      - IP 주소 지정 방식이나 라우팅 방식 유지
      - 기존 IP 장비와 통신 가능
    - 장비 변경 최소화
      - 이동 장비가 사용할 장비만 모바일 IP에 맞게 변경
      - 네트워크 사이에서 사용하지 않는 장비들은 변경할 필요 없음
    - 보안
      - 메시지를 리다이렉트(Redirect)함
      - 불법 노드 문제가 발생하지 않도록 인증 과정을 거칠 수 있게 도움

모바일 IP 프로토콜

- 모바일 IP
  - 정의
    - 이동 장비가 한 네트워크에서 다른 네트워크로 이동하며 원본 IP 주소를 유지하도록 하기 위한 프로토콜
  - 구현 장비
    - 이동 장비
      - 네트워크 간을 이동하는 장비
    - 홈 에이전트(Home Agent)
      - 홈 네트워크에 연결된 라우터
      - 이동 장비가 받아야 할 데이터그램을 대신 받아 이동 장비로 전달
    - 외부 에이전트(Foreign Agent)
      - 외부 네트워크에 연결된 라우터
      - 홈 에이전트가 전달한 데이터그램을 받아서 이동 장비로 전달

모바일 IP 프로토콜

- 모바일 IP 동작 과정
  - 일반적인 동작 과정



모바일 IP 프로토콜

- 모바일 IP 동작 과정
  - 홈 네트워크에서의 동작 과정
    1. 에이전트 통신
       - 이동 장비가 본인의 위치가 담긴 에이전트 광고 메시지를 받고 로컬 네트워크의 에이전트 발견
       - 받지 못한 경우에 에이전트 요청 메시지 전송
    2. 네트워크 위치 결정
       - 이동 장비는 에이전트 발견 메시지를 기반으로 홈 네트워크인지 외부 네트워크인지 판단

모바일 IP 프로토콜

- 모바일 IP 동작 과정
  - 외부 네트워크에서의 동작 과정
    1. CoA(Care-of Address) 획득
       - 에이전트 광고 메시지로 임시 주소(CoA) 부여
       - 목적지로 데이터그램을 전달하기 위해 사용
    2. 에이전트 등록
       - 이동 장비가 자신의 위치를 홈 에이전트에게 알림
       - 이동 장비가 자신에게 오는 데이터그램을 홈 에이전트가 전달해 달라고 요청
    3. 데이터그램 전달
       - 홈 에이전트는 이동 장비에게 송신된 데이터그램을 실제 이동 장비의 위치로 전달
       - CoA 종류에 따라 전달 방식 다름

모바일 IP 프로토콜

- 모바일 IP 주소
  - 홈 주소
    - 홈 네트워크에서 장비가 사용하는 주소
    - 이동 장비에게 할당된 고정 IP 주소
    - 데이터그램을 이동 장비에게 전달할 때 사용
  - CoA(Care-of Address)
    - 홈 네트워크의 외부에서 장비가 사용할 임시 주소
    - 이동 장비가 외부로 움직일 때 사용하는 주소
    - 외부 에이전트가 에이전트 광고 메시지에 추가하여 데이터그램을 전달할 때 사용

모바일 IP 프로토콜

- 모바일 IP 주소
  - CoA 유형
    - 외부 에이전트 CoA(Foreign Agent Care-of Address)
      - 외부 에이전트의 IP 주소와 동일
      - 외부 네트워크에 외부 에이전트가 있는 경우에 사용
      - 외부 네트워크의 이동 장비들이 동일한 IP 주소를 가져도 됨
    - 공존 CoA(Co-Located Care-of Address)
      - 모바일 IP가 아닌 방법으로 이동 장비에게 직접 할당된 주소
        - e.g., DHCP(Dynamic Host Configuration Protocol)
      - 데이터그램이 이동 장비로 직접 전송됨
      - 외부 네트워크에 외부 에이전트가 없는 경우에 사용
      - 외부 네트워크의 이동 장비들은 유일한 IP 주소를 가져야 함

모바일 IP 프로토콜

- 모바일 IP 에이전트 발견
  - 정의
    - 이동 장비가 로컬 네트워크에 있는 에이전트와 접속을 시도하는 방법
  - 목적
    - 에이전트/노드 통신
      - 에이전트에 대한 정보 메시지를 장비에게 전송
      - 노드(장비)가 에이전트에게 정보 요청
    - 현재 위치 발견
      - 노드(장비) 자신의 위치 파악 가능
        - e.g., 홈 네트워크인지 외부 네트워크인지
    - CoA 할당
      - 외부 에이전트 CoA 사용 시, 이동 장비가 사용할 CoA 획득

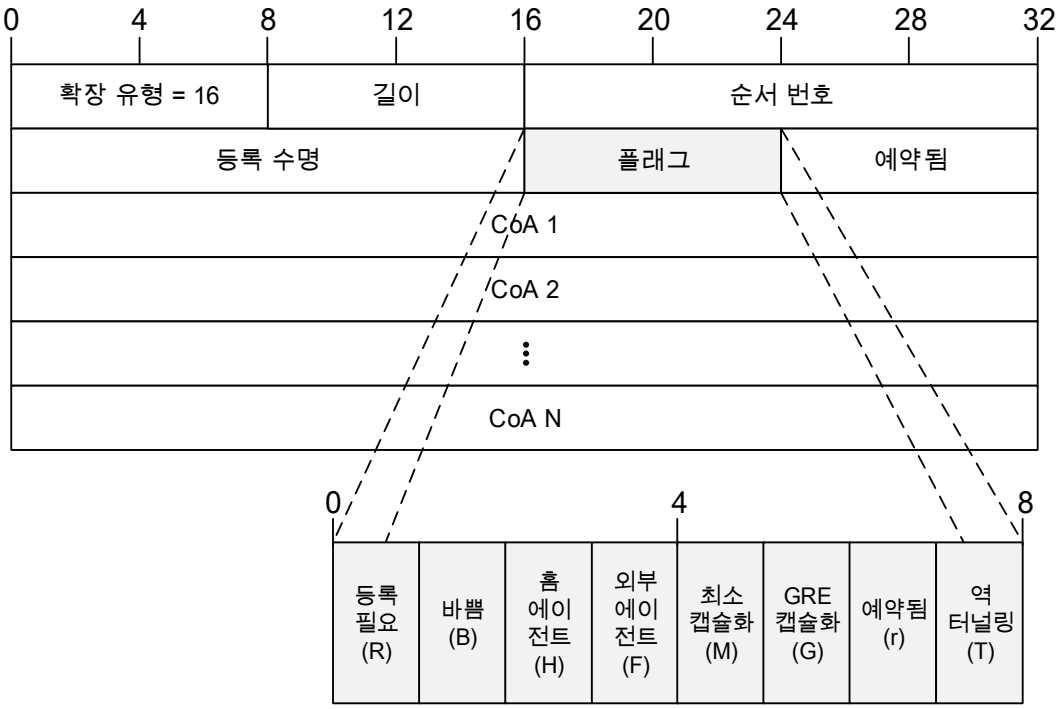
모바일 IP 프로토콜

- 모바일 IP 에이전트 발견
  - 사용하는 메시지
    - 에이전트 광고(Agent Advertisement) 메시지
      - 에이전트로 활동 가능한 라우터가 정기적으로 전송되는 메시지
      - 자신의 위치 파악에 사용
    - 에이전트 요청(Agent Solicitation) 메시지
      - 이동 장비가 에이전트 광고 메시지를 받지 못한 경우, 로컬 에이전트에게 전송을 요청하는 메시지

모바일 IP 프로토콜

- 모바일 IP 에이전트 발견
  - 사용하는 메시지 포맷
    - 에이전트 광고 메시지

필드명	설명
등록 필요(R)	외부 에이전트를 통해 등록해야 함
바쁨(B)	에이전트가 이동 장비에서 등록 받기에 현재 너무 바쁨
홈 에이전트(H)	링크에서 홈 에이전트로 전달 가능함을 알림
외부 에이전트(F)	링크에서 외부 에이전트로 전달 가능함을 알림
최소 캡슐화(M)	캡슐화 이용하여 터널링된 데이터그램 수신 가능
GRE 캡슐화(G)	
예약됨(r)	현재 사용하지 않으므로 0으로 설정
역 터널링(T)	역 터널링을 지원함



    - 에이전트 요청 메시지

모바일 IP 프로토콜

- 모바일 IP 에이전트 등록
  - 등록(Registration)
    - 이동 장비와 홈 에이전트가 통신하며 정보를 주고 받는 과정
  - 등록 이벤트
    - 등록 이동
      - 장비가 외부 네트워크에 도착하면 등록 시작
    - 등록 해제
      - 다시 홈 네트워크로 돌아오면 전달 취소
    - 재등록
      - 외부에서 다른 외부로 이동하거나 CoA가 바뀔 시 등록 수정
      - 등록 해제된 경우에도 같은 외부 네트워크에 머무르는 경우 재등록

모바일 IP 프로토콜

- 모바일 IP 에이전트 등록
  - 등록 요청과 응답 메시지
    - UDP(User Datagram Protocol) 사용
  - CoA 유형에 따른 두 가지 방식의 등록 과정
    - 직접 등록 방식(공존 CoA)
      1. 이동 장비가 홈 에이전트에게 등록 요청 메시지 전송
      2. 홈 에이전트가 이동 장비에게 등록 응답 메시지 전송
    - 간접 등록 방식(외부 에이전트 CoA)
      1. 이동 장비가 외부 에이전트에게 등록 요청 메시지 전송
      2. 외부 에이전트가 홈 에이전트에게 처리한 등록 요청 메시지 전송
      3. 홈 에이전트가 외부 에이전트에게 등록 응답 메시지 전송
      4. 외부 에이전트가 이동 장비에게 처리한 등록 응답 메시지 전송

모바일 IP 프로토콜

- 모바일 IP 데이터 캡슐화와 터널링
  - 데이터 캡슐화
    - 홈 에이전트는 데이터를 캡슐화하여 이동 장비 주소로 전송
      - 데이터그램을 이동 장비의 CoA로 재전송해야하기 때문
  - 터널링(Tunneling)
    - 캡슐화하는 장비와 역캡슐화하는 장비 간 논리적 터널 생성
    - 캡슐화된 데이터그램의 원본 IP 헤더를 임시로 숨기기 위해 사용
    - 터널의 시작은 데이터그램을 캡슐화하는 홈 에이전트
    - 터널의 끝은 CoA의 종류에 따라 달라짐
      - 외부 에이전트 CoA
        - 터널의 끝은 외부 에이전트
        - 홈 에이전트가 헤더를 벗겨낸 원래 데이터그램을 이동 장비에게 직접 전송
      - 공존 CoA
        - 터널의 끝은 이동 장비
        - 이동 장비에서 헤더를 벗겨냄

모바일 IP 프로토콜

- 모바일 IP 데이터 캡슐화와 터널링
  - 터널링 과정
    1. 이동 장비는 외부 네트워크의 한 서버에게 모바일 IP 요청
    2. 해당 서버는 이동 장비의 출발지 주소인 홈 네트워크에게 모바일 IP 요청에 대한 응답
    3. 홈 에이전트는 도착한 응답을 이동 장비에게 터널링
  - 역터널링
    - 이동 장비가 데이터그램을 인터넷에게 직접 전송할 수 없는 경우 사용
    - CoA 유형에 따라 이동 장비와 홈 에이전트 사이 혹은 외부 에이전트와 홈 에이전트 사이에 생김
    - 모든 전송은 홈 에이전트와의 터널을 통해 이루어짐

모바일 IP 프로토콜

- 모바일 IP와 TCP/IP 주소 결정 프로토콜
  - 이동 장비가 다른 네트워크에 있어 주소 결정 프로토콜 요청에 응답할 수 없다는 문제 존재
  - 해결 방법
    - ARP 프록싱(Address Resolution Protocol Proxing)
      - 홈 에이전트는 이동 장비의 홈 네트워크에서 전송되는 모든 ARP 요청을 받아야 함
      - 홈 에이전트는 이동 장비 대신 ARP 요청에 응답하며 자신의 데이터 링크 계층 주소 알림
      - 실제로 홈 에이전트가 해당 데이터그램을 이동 장비에게 전송
    - 무상 ARP(Gratuitous Address Resolution Protocol)
      - 이미 이동 장비에 대한 캐시를 가진 서버인 경우, 홈 에이전트는 무상 ARP를 전송하여 이동 장비 주소와 자신의 데이터 링크 계층 주소가 같다고 알림

모바일 IP 프로토콜

- 모바일 IP 보안 문제
  - 이동 장비가 무선 네트워킹을 사용
    - 전송 자체가 공개되어 있기에 누구나 도청 가능
  - 재전송 공격 문제
    - 누군가 데이터그램을 가로챘다가 이후에 전송하는 방식
  - 등록 메시지 이외의 메시지에 대한 인증이 없음

Thanks!

김 지 혜 (jihye@pel.sejong.ac.kr)