

TCP/IP 완벽 가이드

- 2-5부 IP 관련 기능 프로토콜 -

이 하 늘 (dlgksmf6789@sju.ac.kr)

세종대학교 프로토콜공학연구실

목 차

- 보충
 - PPP 기능 프로토콜
 - IP 멀티캐스트의 주소의 TCP/IP 주소 결정
 - 역순 주소 결정과 TCP/IP 역순 주소 결정 프로토콜
- 네트워크 주소 변환(NAT) 프로토콜
- IP Security(IPsec) 프로토콜
- IP 이동성 지원(모바일 IP) 프로토콜

PPP 기능 프로토콜

- PPP 링크 품질 모니터링과 리포팅
 - PPP 링크 품질 모니터링(LQM, Link Quality Monitoring)
 - 링크가 얼마나 잘 동작하고 있는지 품질을 분석할 수 있도록 하는 기능
 - 링크 품질 리포팅(LQR, Link Quality Reporting)
 - 모니터링 기능 중 유일하게 존재하는 기능
 - 반대쪽에 있는 장비에게 현재 링크의 통계 정보를 수집하여 주기적으로 전송 요청

PPP 기능 프로토콜

- 링크 품질 리포팅(LQR)
- LQR 수립
 - 링크 수립 단계의 링크 인자 협상 과정의 일부로 수행
 - 장비는 설정요청 프레임에 품질 프로토콜 설정 옵션을 포함시켜 링크 모니터링 요청

옵션	설명
보고서 주기	정보 보고서를 받는 시간 간격의 최댓값

PPP 기능 프로토콜

- 링크 품질 리포팅(LQR)
- LQR 활성화
 - 링크 통계를 추적하기 위한 카운터 생성
 - 통계 정보를 담고 있는 품질 보고서를 보내는 시간 간격을 제어하기 위한 타이머 시작
 - 보고서는 PPP 프로토콜 필드가 0xC025로 채워진 PPP프레임으로 전송

PPP 기능 프로토콜

- 링크 품질 리포팅(LQR)
 - 제공하는 정보
 - 송수신한 프레임의 수
 - 송수신한 모든 프레임의 옥텟(바이트)수
 - 발생한 에러의 수
 - 버린 프레임의 수
 - 생성된 링크 품질 보고서 수

PPP 기능 프로토콜

- 링크 품질 리포팅(LQR)
- 링크 품질 보고서 사용
 - 일부 장비는 에러의 절대값이 특정 임계치를 넘으면 링크를 닫음
 - 일부 장비는 연속적인 보고서 추이를 분석하여 특정한 변화를 감지한 경우 링크에 대한 조치를 취할 수 있음
 - 일부 장비는 단지 그 정보를 로그에 저장하고 아무런 조치를 취하지 않음

PPP 기능 프로토콜

- PPP 압축 제어 프로토콜(CCP, Compression Control Protocol)
- 정의
 - 압축을 어떻게 할 지 설정하고 협상하는 프로토콜
- 특징
 - 두 장비 간의 LCP 링크 내에서 CCP 링크라는 압축 연결을 수립하는 데 사용
 - CCP 링크를 관리하고 종료하기 위한 메시지 기능도 제공
 - LCP의 동작 방식과 유사
 - 링크 유지 단계에서 리셋 요청과 리셋 승인 메시지 유형이 추가

PPP 기능 프로토콜

- PPP 압축 제어 프로토콜(CCP)
 - 압축 알고리즘 운영
 - CCP 옵션 값 마다 지정된 압축 알고리즘이 존재
 - 송신자는 데이터를 전송하기 전에 압축, 수신자는 데이터를 수신한 다음 해제
 - 압축되지 않은 PPP 프레임의 정보 필드에 들어갈 데이터를 받아 압축 알고리즘을 적용
 - 압축됐으면 PPP 프로토콜 필드에 0x00FD
 - 다중링크를 독립적으로 압축한 경우 0x00FB

PPP 기능 프로토콜

- PPP 압축 제어 프로토콜(CCP)
- CCP 설정 옵션

유형값	RFC	압축 알고리즘
0	-	OUI
1,2	1978	PPP Predictor Compression Protocol
17	1974	PPP Stac LZS Compression Protocol
18	2118	Microsoft Point-to-Point Compression Protocol
19	1993	PPP Gandalf FZA Compression Protocol
21	1977	PPP BSD Compression Protocol
23	1967	PPP LZS-DCP Compression Protocol
26	1979	PPP Deflate Protocol

PPP 기능 프로토콜

- PPP 암호화 제어 프로토콜(ECP, Encryption Control Protocol)
- 정의
 - 장비가 어떻게 데이터를 암호화할지 협상하는 프로토콜
- 특징
 - ECP 연결을 협상하면 장비들은 링크를 통해 암호화된 프레임 전송 가능
 - LCP의 동작 방식과 유사
 - 링크 유지 단계에서 리셋 요청과 리셋 승인 메시지 유형이 추가로 사용

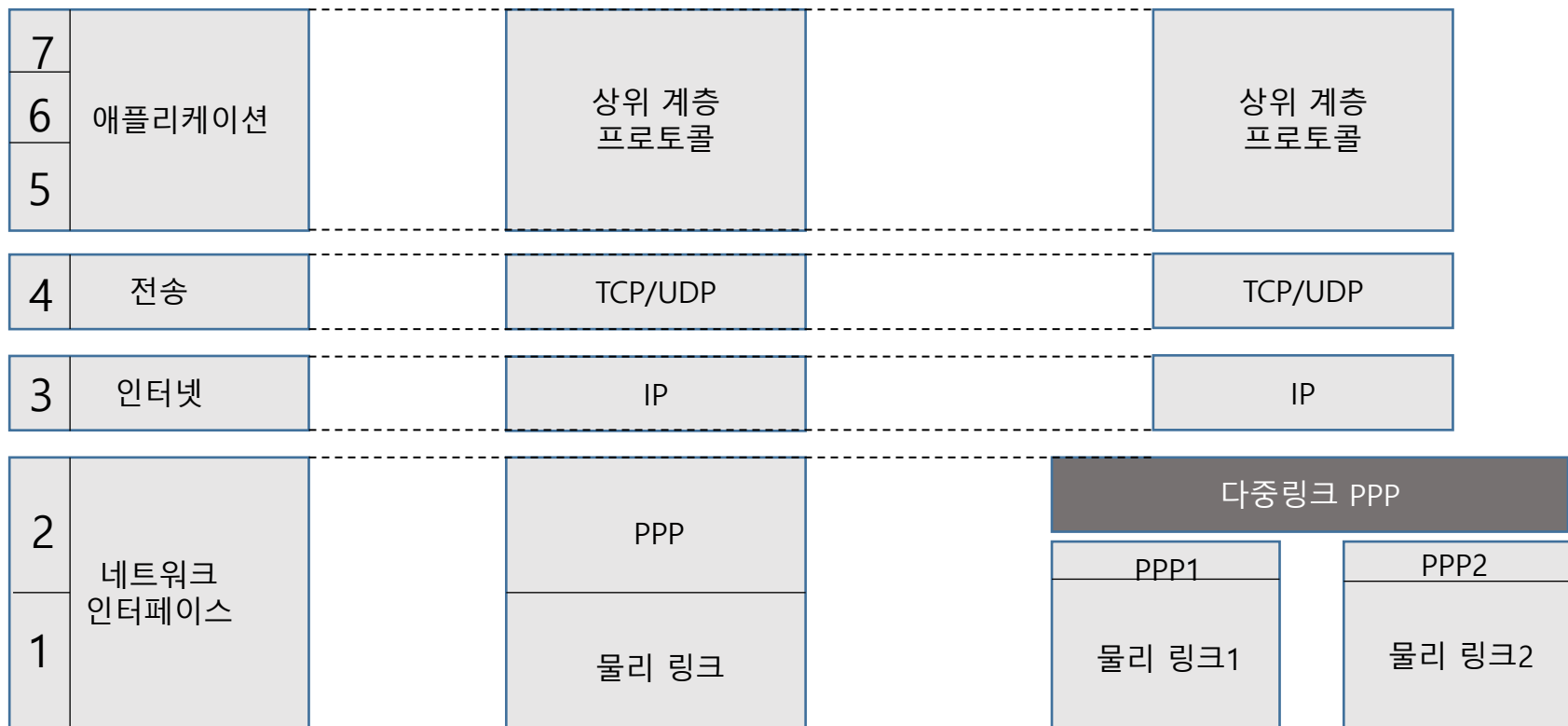
PPP 기능 프로토콜

- PPP 암호화 제어 프로토콜(ECP)
 - 암호화 알고리즘 운영
 - ECP 옵션 값 마다 지정된 암호화 알고리즘 존재
 - 송신자가 데이터 전송 전 암호화, 수신자가 데이터 수신 후 복호화
 - PPP 프로토콜 필드에 특수 값 추가
 - 암호화 0x0053
 - 다중링크 독립적으로 암호화 0x0055
 - ECP 설정 옵션 유형 값

유형 값	알고리즘 정의 RFC	암호화 알고리즘
0	-	사유 프로토콜
2	2420	The PPP Triple-DES Encryption Protocol
3	2419	The PPP DES Encryption Protocol. v2

PPP 기능 프로토콜

- PPP 다중 링크 프로토콜(MP, Multilink Protocol)
- 여러 링크를 결합하여 하나의 고성능 링크인 것처럼 사용하는 기능을 제공하는 프로토콜



PPP 기능 프로토콜

- PPP 다중 링크 프로토콜(MP)
 - 수립과 설정 옵션
 - 다중링크 최대 수신 재구성 유닛
 - 협상을 시작하는 장비가 MP를 지원하며 사용하고 싶다는 것을 알림
 - 다중링크 짧은 순서번호 헤더 포맷
 - 장비들의 효율성을 높이기 위해 MP 프레임에서 짧은 순서 번호 필드를 사용하는 것을 협상하도록 함
 - 종단 식별자
 - 시스템 식별
 - 장비들이 어떤 링크가 어떤 장비로 연결되는지 파악

PPP 기능 프로토콜

- PPP 다중 링크 프로토콜(MP)

- 운영 역할

- 송신

- 적절한 NCP로 설정된 네트워크 계층 프로토콜로부터 데이터그램 받음
 - 데이터그램을 MP 프레임으로 프레임링
 - 각 링크로 분배된 프레임은 캡슐화 되어 물리 링크로 전송

- 수신

- 물리 링크에서 받은 프레임 조각을 재조합 하여 원본 프레임 구성

PPP 기능 프로토콜

- PPP 대역폭 할당 프로토콜과 제어 프로토콜
 - 필요할 때마다 링크를 전체 링크 묶음에 추가하고 필요하지 않을 경우에 제거하도록 MP 설정을 돕는 프로토콜
 - 대역폭 할당 프로토콜
(BAP, Bandwidth Allocation Protocol)
 - 1계층 링크 묶음 위에서 MP로 동작하는 장비들이 특정 링크를 묶음에 추가하거나 제거할 수 있도록 하는 메시지 모음을 정의
 - 대역폭 할당 제어 프로토콜
(BACP, Bandwidth Allocation Control Protocol)
 - BAP를 수립하는 데 쓰임

PPP 기능 프로토콜

- PPP 대역폭 할당 프로토콜과 제어 프로토콜
- BACP 운영: BAP 사용 설정
 - 협상 설정 옵션: Favored-Peer
 - 링크의 두 장비가 동시에 동일한 요청을 보낼 때 문제가 일어나지 않는 것을 보장하는 데 사용

PPP 기능 프로토콜

- PPP 대역폭 할당 프로토콜과 제어 프로토콜
- BAP 운영: 링크 추가와 제거
 - 링크를 제거하거나 추가하기 위해 보낼 수 있는 메시지 모음을 정의
 - 콜요청과 콜 응답
 - 링크 묶음에 링크를 추가하고 링크를 초기화하고 싶은 장비는 상대방에게 콜 요청 프레임 송신, 콜 응답 수신
 - 콜백요청과 콜백응답
 - 상대 장비가 새 링크를 추가하라는 요청을 보내기를 원할 때 사용

PPP 기능 프로토콜

- PPP 대역폭 할당 프로토콜과 제어 프로토콜
- BAP 운영: 링크 추가와 제거
 - 링크를 제거하거나 추가하기 위해 보낼 수 있는 메시지 모음을 정의
 - 콜상태표시와 콜상태응답
 - 새로운 링크를 추가하려고 시도한 장비가 콜상태표시를 송신, 콜상태응답 수신
 - 링크제거요청과 링크제거응답
 - 링크를 제거하기 위한 요청과 응답

목 차

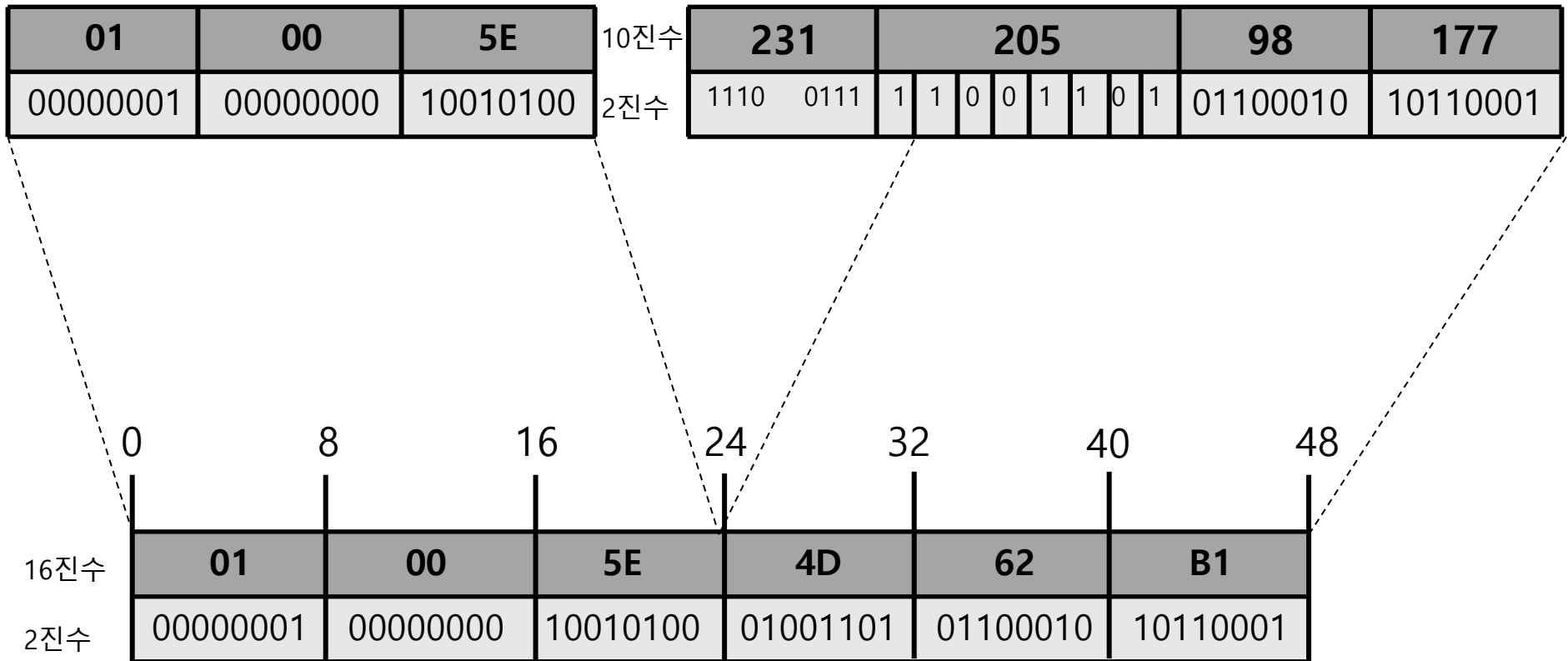
- 보충
 - PPP 기능 프로토콜
 - IP 멀티캐스트의 주소의 TCP/IP 주소 결정
 - 역순 주소 결정과 TCP/IP 역순 주소 결정 프로토콜
- 네트워크 주소 변환(NAT) 프로토콜
- IP Security(IPsec) 프로토콜
- IP 이동성 지원(모바일 IP) 프로토콜

주소 결정과 프로토콜

- IP 멀티캐스트 주소의 TCP/IP 주소 결정
 - IP 멀티캐스트 주소를 직접 매핑을 사용하여 MAC 주소로 변환
- IEEE 802 주소 지정 방법
 - 24비트 블록 2개로 구성된 데이터링크 계층 주소
 - 상위 24비트는 기관 유일 식별자 (OUI, Organizationally unique identifier)
 - 하위 24비트는 개별 장비를 구분하는 데 쓰임

주소 결정과 프로토콜

- IP 멀티캐스트 주소의 TCP/IP 주소 결정

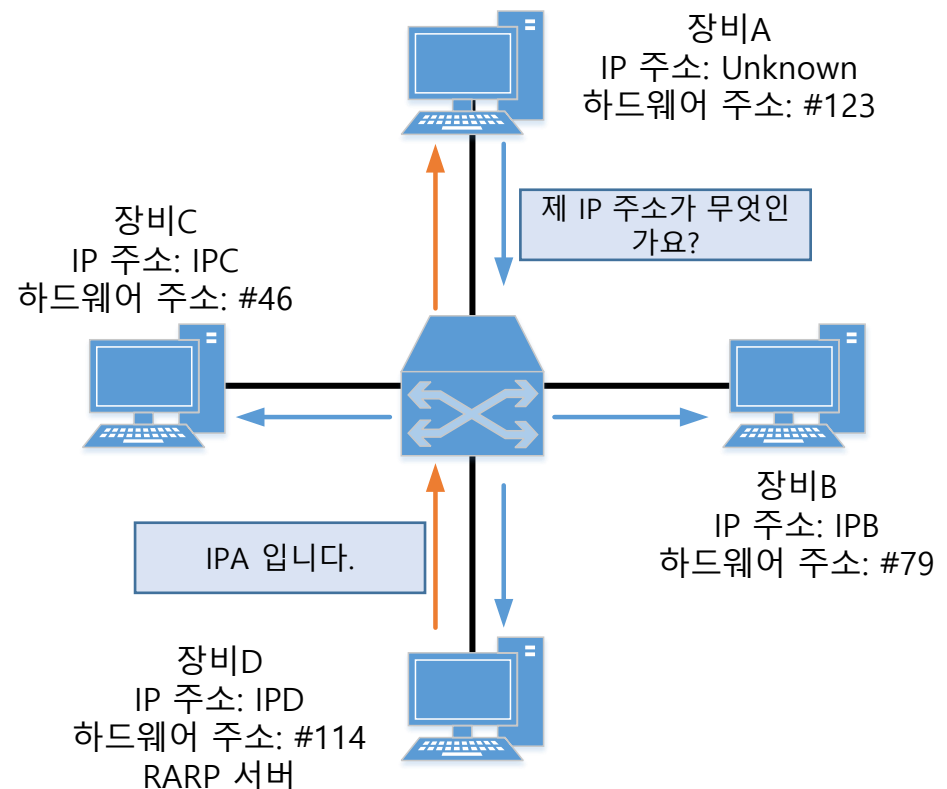


목 차

- 보충
 - PPP 기능 프로토콜
 - IP 멀티캐스트의 주소의 TCP/IP 주소 결정
 - 역순 주소 결정과 TCP/IP 역순 주소 결정 프로토콜
- 네트워크 주소 변환(NAT) 프로토콜
- IP Security(IPsec) 프로토콜
- IP 이동성 지원(모바일 IP) 프로토콜

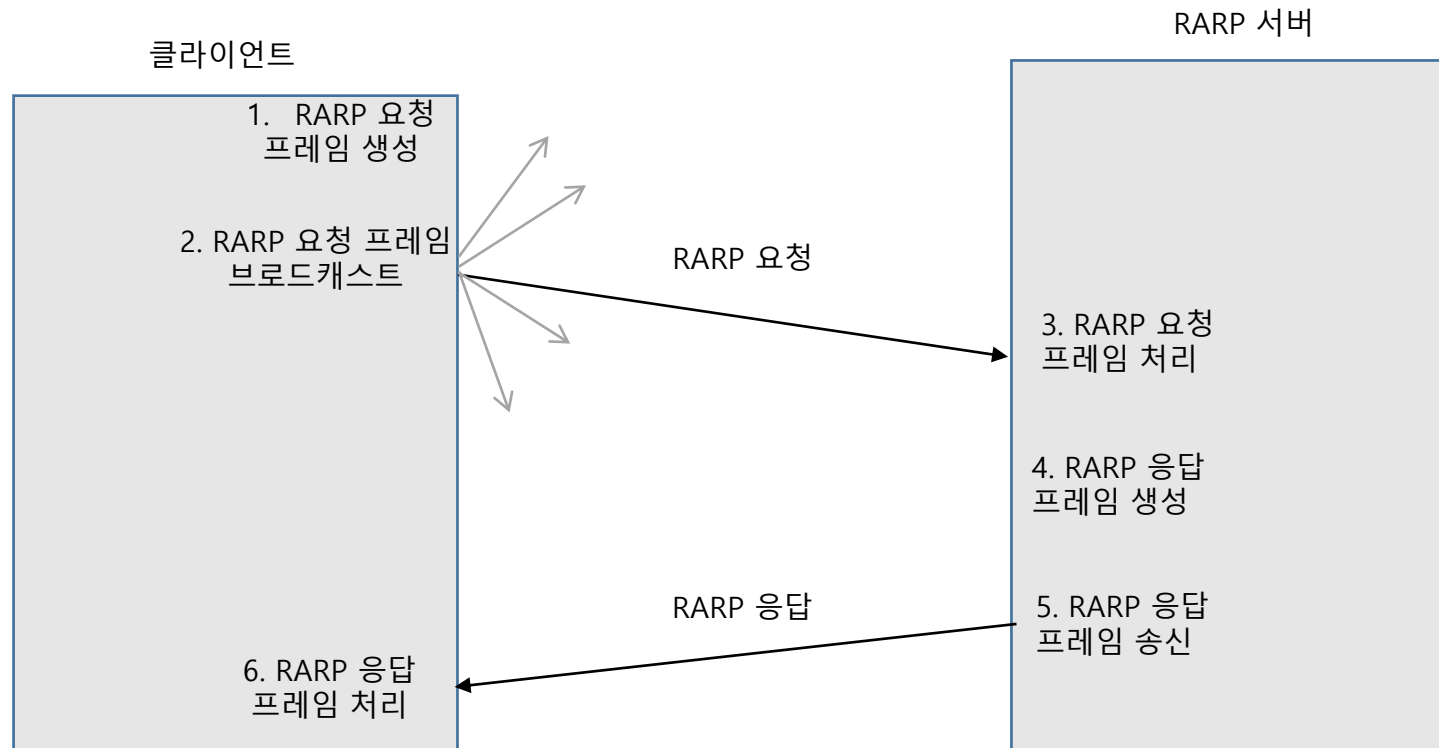
역순 주소 결정과 프로토콜

- 역순 주소 결정 프로토콜 (RARP, Reverse Address Resolution Protocol)
- ARP를 역순으로 적용한 프로토콜
- 장비가 자신의 하드웨어 주소를 브로드 캐스트하고 RARP 서버가 IP 주소로 응답
- 동작 구성



역순 주소 결정과 프로토콜

- 역순 주소 결정 프로토콜
- 동작 과정



역순 주소 결정과 프로토콜

- 역순 주소 결정 프로토콜

- 제약

- 모든 네트워크 세그먼트에서 RARP 서버를 운영해야 함
- IP 주소에 대한 중앙 관리를 어렵게 함
- 수동 할당
 - 각 RARP 서버별로 IP 주소 매핑 테이블을 수동 설정 해야함

- 제한된 정보

- 오직 IP 주소만 알려줌
- 서브넷 마스크나 기본 게이트웨이 같은 다른 기타 중요 정보를 제공 할 수 없음

목 차

- 보충
 - PPP 기능 프로토콜
 - IP 멀티캐스트의 주소의 TCP/IP 주소 결정
 - 역순 주소 결정과 TCP/IP 역순 주소 결정 프로토콜
- 네트워크 주소 변환(NAT) 프로토콜
- IP Security(IPsec) 프로토콜
- IP 이동성 지원(모바일 IP) 프로토콜

네트워크 주소 변환 프로토콜

- 네트워크 주소 변환(NAT, Network Address Translation)
- 정의
 - IP 패킷을 라우팅하여 사설 IP 주소와 공인 IP 주소를 서로 변환하는 기술
- 등장 배경
 - IP 주소 고갈
 - 늘어난 인터넷 이용자에 의한 IP 주소 비용의 증가
 - 보안 우려 증가
 - 악성 사용자들의 증가와 인터넷에 연결된 장비의 증가

네트워크 주소 변환 프로토콜

- 네트워크 주소 변환(NAT)
 - NAT 구성의 전제 조건
 - 클라이언트/서버 방식
 - 대부분의 호스트는 클라이언트 장비
 - 클라이언트 장비는 외부에 노출될 필요가 없음
 - 인터넷 동시 접근 장비의 적음
 - 인터넷 통신의 라우팅
 - 네트워크와 인터넷 간의 통신은 트래픽 흐름을 제어하는 역할을 하는 라우터를 통해 이루어짐

네트워크 주소 변환 프로토콜

- 네트워크 주소 변환(NAT)

- 장점

- 공인 IP 공유

- 대량의 호스트가 소수의 공인 IP 주소 공유 가능

- 쉬운 확장

- 로컬 네트워크는 사설 주소를 이용하기 때문에 새 장비를 추가 하는 것이 용이

- 통제력 강화

- 관리자는 통제력을 강화할 수 있고, 인터넷 연결도 가능

- 인터넷 서비스 제공자 선택의 유연성

- 공인 주소만 바꾸면 되기 때문에 ISP 변경이 용이

- 보안 강화

- NAT는 하나의 간접 계층을 추가하는 것과 마찬가지로 방화벽을 자동으로 생성

네트워크 주소 변환 프로토콜

- 네트워크 주소 변환(NAT)

- 단점

- 복잡성

- 공인 주소 부족으로 인한 문제

- 클라이언트에 공인 IP 주소가 없기 때문에 일부 애플리케이션에서 문제가 발생할 수 있음

- 호환성 문제

- NAT는 데이터그램의 IP 헤더만 수정하고 데이터는 수정하지 않기 때문에 특정 애플리케이션에서 동작하지 않을 수 있음

- 보안 프로토콜 문제

- IPsec의 경우 헤더의 변조를 탐지하기 때문에 NAT에 의한 변경과 악성 데이터그램 해킹을 잘 구분하지 못함

네트워크 주소 변환 프로토콜

- 네트워크 주소 변환(NAT)
 - 단점
 - 클라이언트 접근 지원 미비
 - 외부에서 로컬 네트워크의 클라이언트로 접근 하는 것이 어려워짐
 - 성능 감소

네트워크 주소 변환 프로토콜

- 네트워크 주소 변환(NAT) 주소 용어
 - 주소가 참조하는 장비의 위치에 따른 구분
 - 내부 주소
 - 로컬 네트워크의 장비를 가리키는 모든 주소
 - 외부 주소
 - 공중 인터넷에 있는 장비를 가리키는 주소
 - 데이터그램이 나타나는 네트워크의 위치에 따른 구분
 - 로컬 주소
 - 내부 네트워크의 데이터그램에 나타나는 주소
 - 전역 주소
 - 외부 네트워크의 데이터그램에 나타나는 주소

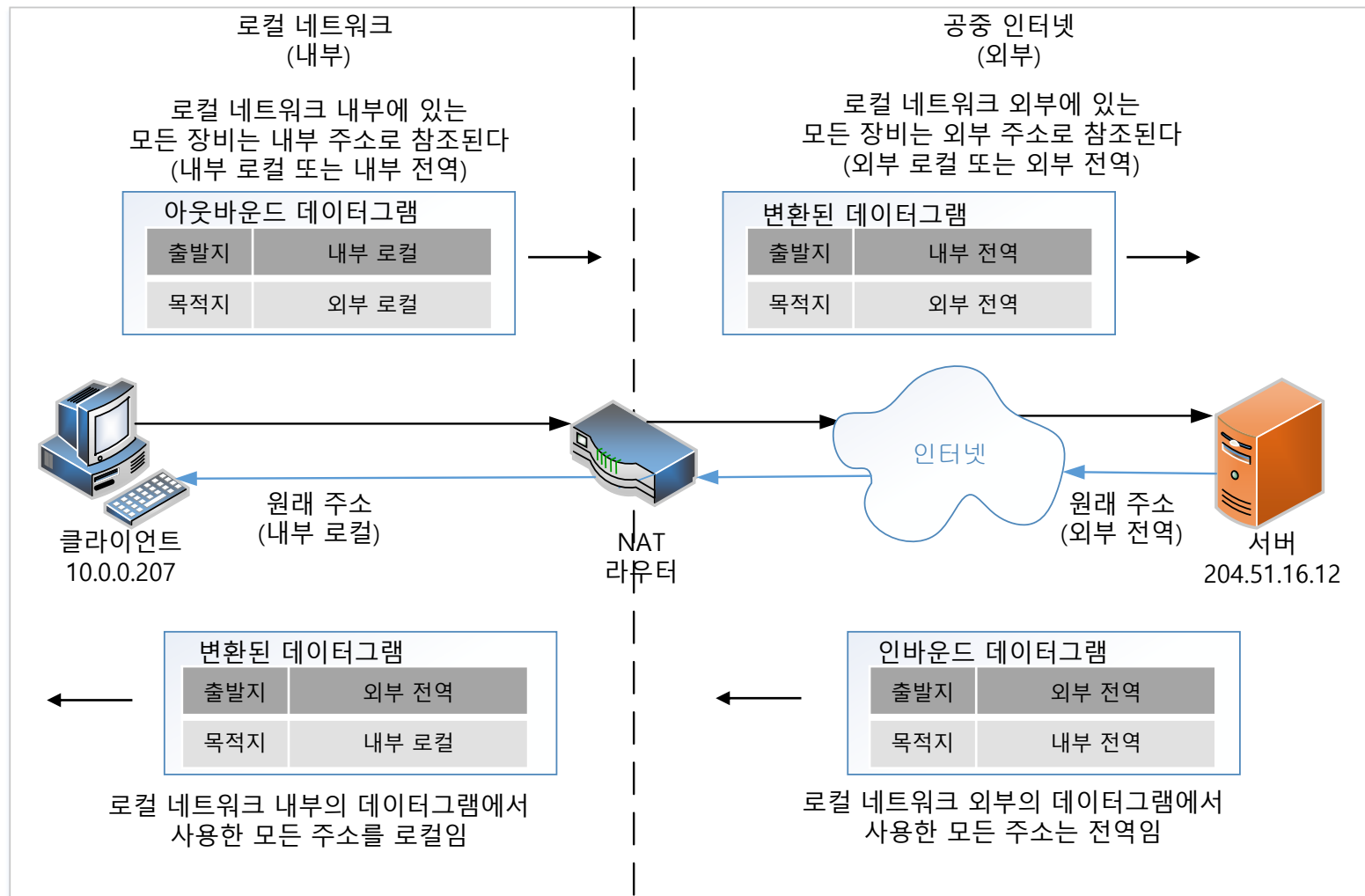
네트워크 주소 변환 프로토콜

- 네트워크 주소 변환(NAT) 주소 용어
 - 주소 유형

내부 로컬 주소	내부 전역 주소	외부 전역 주소	외부 로컬 주소
일반적인 로컬 주소 지정 방법	공중 네트워크에서 라우팅 가능한 공인 IP 주소	외부에 있는 장비의 라우팅 가능한 공인 IP 주소	로컬 네트워크에서 참조하는 외부 장비의 주소

네트워크 주소 변환 프로토콜

• 네트워크 주소 변환(NAT) 주소 용어



네트워크 주소 변환 프로토콜

- 정적 주소 매핑과 동적 주소 매핑
 - 변환 테이블
 - 내부 로컬 주소를 내부 전역 주소로 매핑하는 정보를 포함
 - 정적 매핑
 - 내부 혹은 외부 장비의 로컬과 전역 주소 사이의 고정된 값
 - 외부 네트워크에 항상 동일한 주소로 표현되어야 할 장비에 적합
 - 수동으로 관리
 - 동적 매핑
 - 전역과 로컬 장비의 표현이 생성되고 사용되면 사라지는 값
 - 자동으로 동작

네트워크 주소 변환 프로토콜

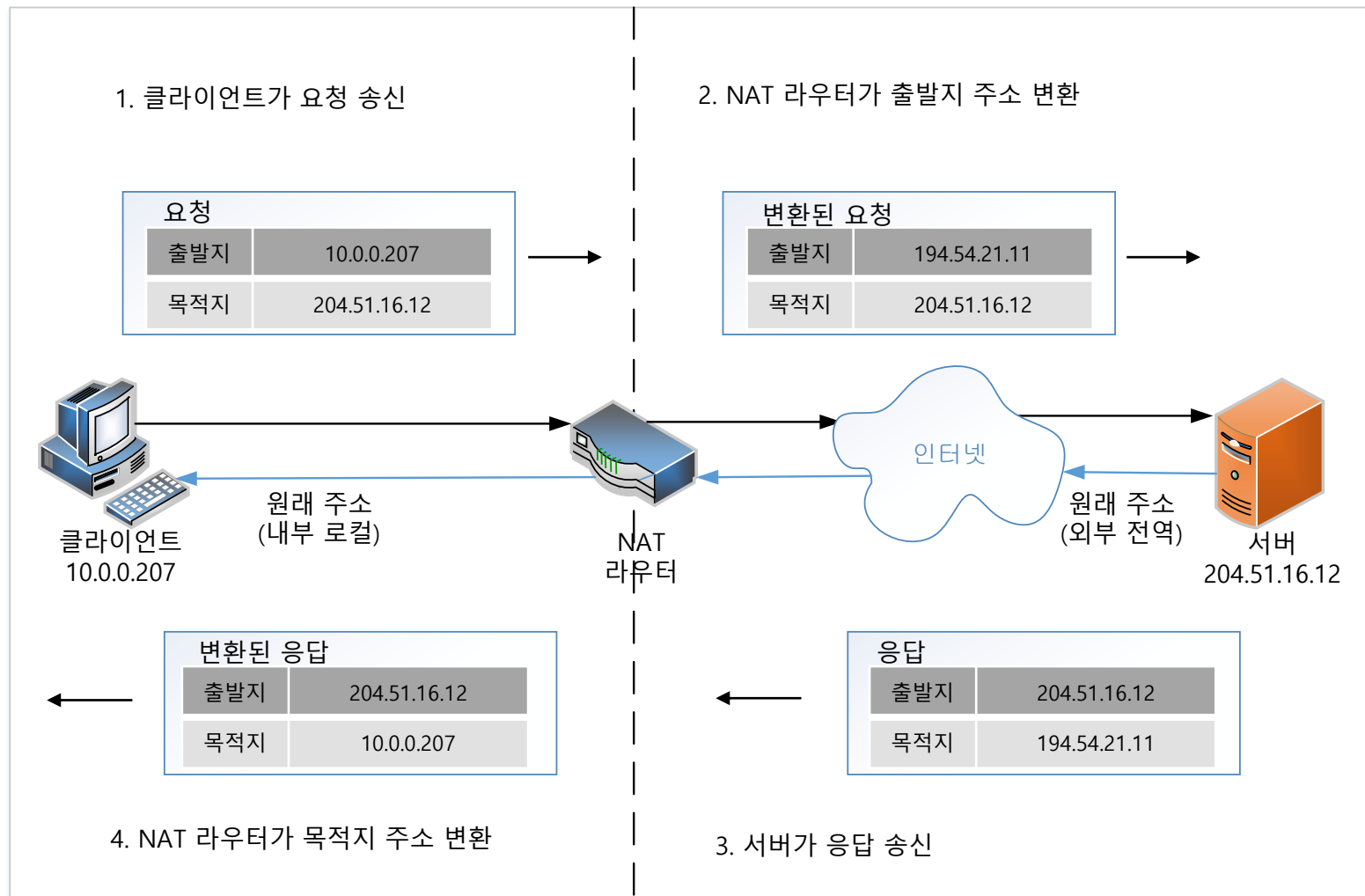
- 동작 방식

- IP NAT 단방향 (전통적/아웃바운드) 동작

- 사설 네트워크의 호스트가 공중 인터넷에 연결할 때 공인 IP 주소를 공유하도록 하기위해 고안
- 변환
 - 외부로 나가는 데이터그램은 출발지 주소가 변환
 - 내부로 들어오는 데이터그램은 목적지 주소가 변환

네트워크 주소 변환 프로토콜

- IP NAT 단방향 (전통적/아웃바운드) 동작



네트워크 주소 변환 프로토콜

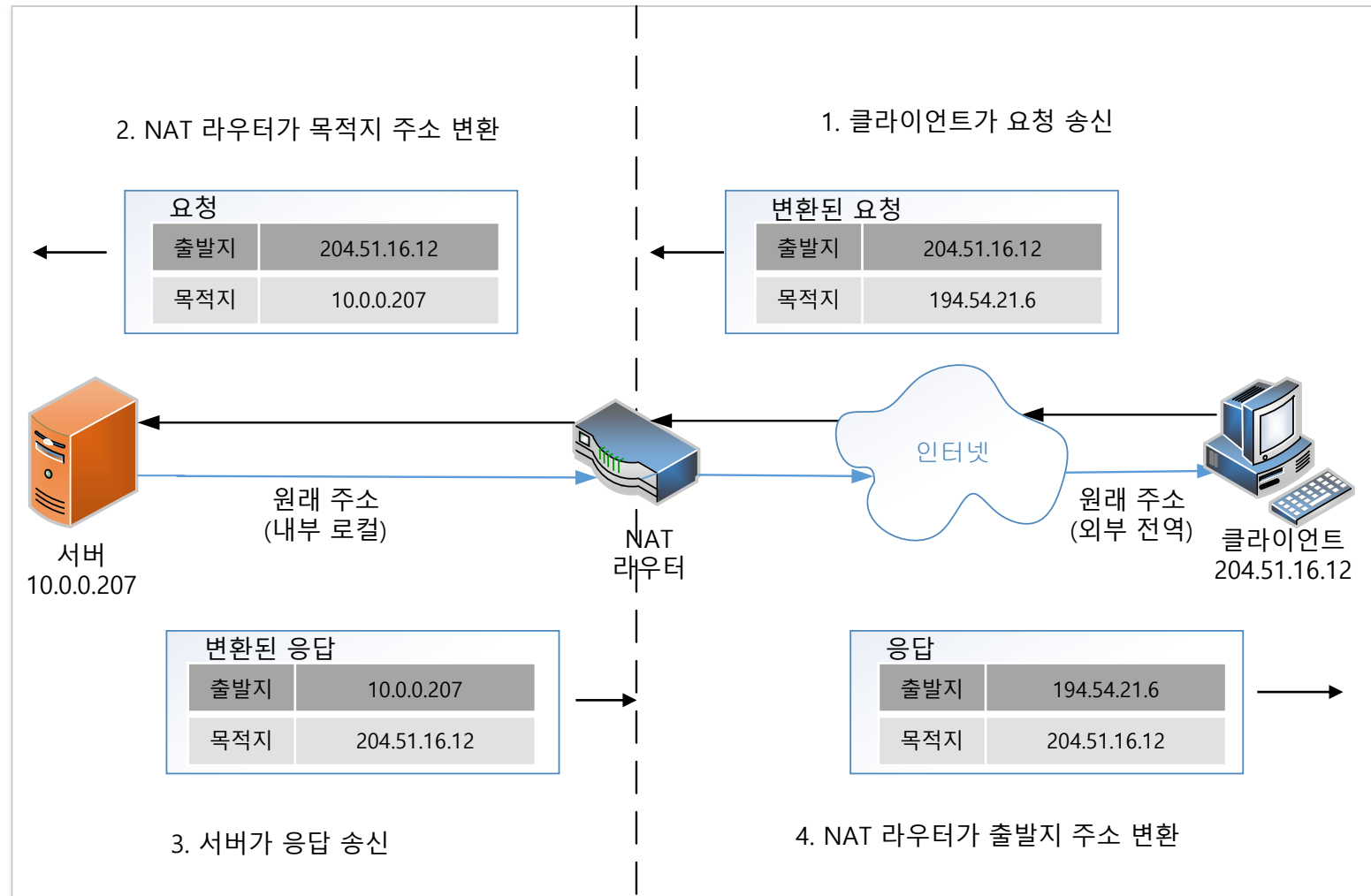
- 동작 방식

- IP NAT 양방향(Two-Way/인바운드) 동작

- 외부 네트워크 장비가 내부 네트워크 장비로 요청할 경우
- 외부 장비는 내부 장비의 주소를 알아도 패킷을 전송할 수 없음
 - 내부 장비의 NAT 라우터가 무엇인지 모름
 - 내부 전역 주소를 알아야 함
- 해결 방안
 - 정적 매핑 사용
 - DNS 사용

네트워크 주소 변환 프로토콜

• IP NAT 양방향(Two-Way/인바운드) 동작



네트워크 주소 변환 프로토콜

- 동작 방식

- IP NAT 포트 기반 (과부하) 동작

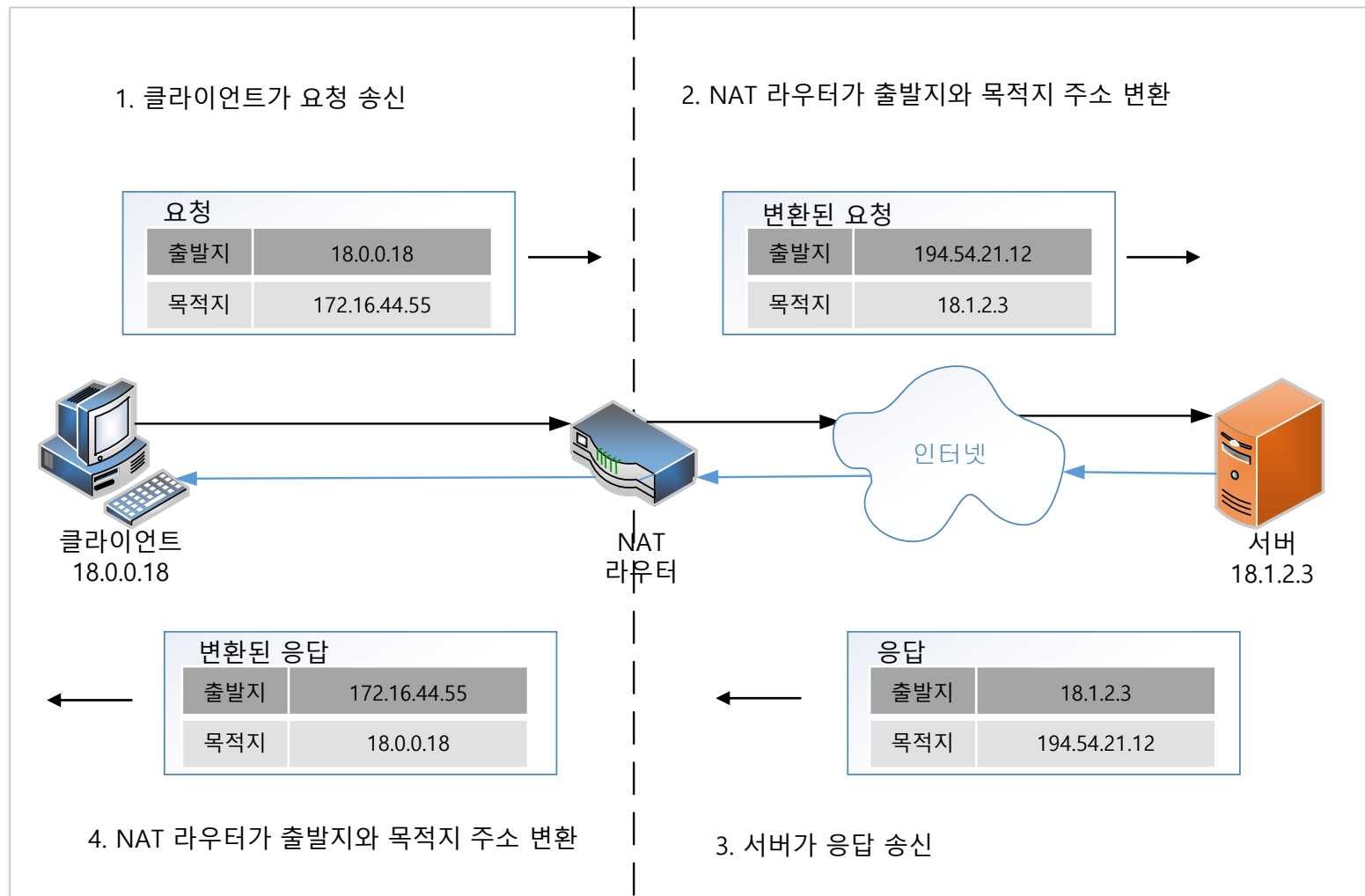
- 다수의 내부 로컬 주소가 하나의 내부 전역 주소를 공유
- 사용 가능한 내부 전역 주소가 없을 경우의 해결책
- 클라이언트와 서버의 서로 다른 애플리케이션이 충돌 없이 동작하도록 해줌
- 포트 번호도 변경 가능
- 구현이 복잡하고, 호환성 문제가 발생할 가능성이 큼

네트워크 주소 변환 프로토콜

- 동작 방식
 - IP NAT 중복/2회 NAT 동작
 - 내부 네트워크의 주소와 공중 네트워크의 주소가 중복될 경우 사용
 - 중복 주소의 경우 내부에서 외부로, 외부에서 내부로의 주소를 모두 변경

네트워크 주소 변환 프로토콜

- IP NAT 중복/2회 NAT 동작



네트워크 주소 변환 프로토콜

- 호환성 문제와 특수 처리 요구사항
 - IP 변경으로 인한 호환성 문제
 - TCP와 UDP 체크섬 재계산
 - 체크섬은 헤더에 대해 계산되기 때문에 IP 주소가 변경되면 다시 계산되어야 함
 - ICMP 조작
 - ICMP 메시지를 검사하여 주소를 바꿔야 함
 - IP 주소를 내장하는 애플리케이션
 - 데이터 페이로드 안에 IP 주소를 포함하는 경우
e.g., FTP(File Transfer Protocol)

목 차

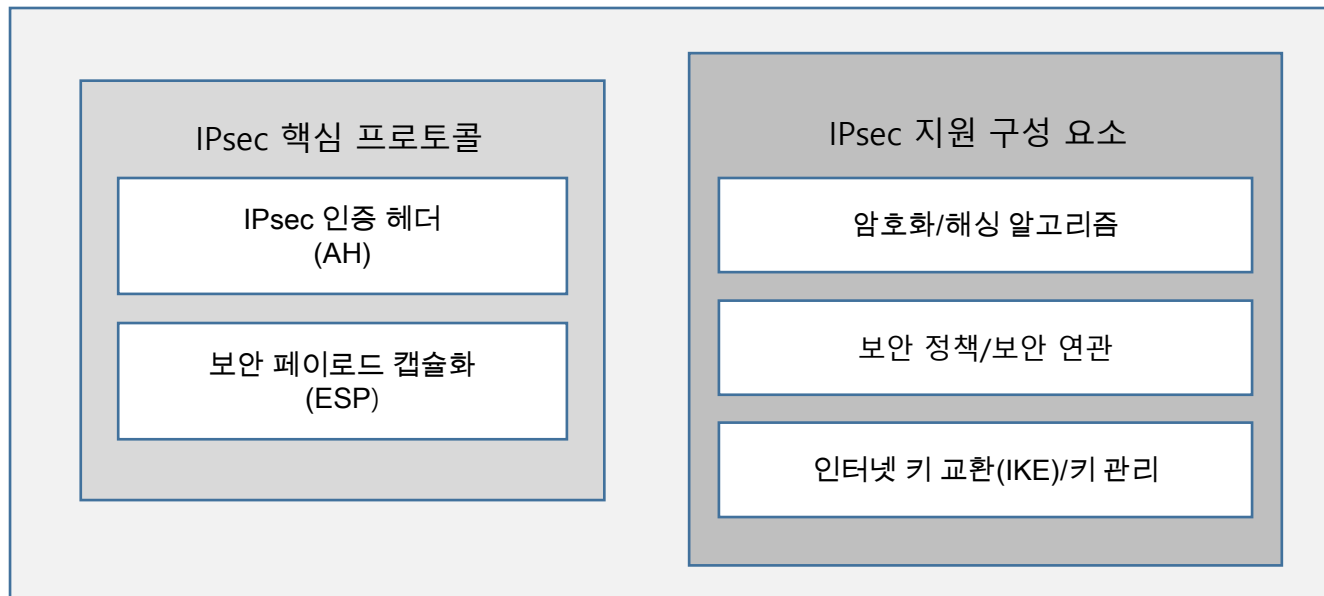
- 보충
 - PPP 기능 프로토콜
 - IP 멀티캐스트의 주소의 TCP/IP 주소 결정
 - 역순 주소 결정과 TCP/IP 역순 주소 결정 프로토콜
- 네트워크 주소 변환(NAT) 프로토콜
- IP Security(IPsec) 프로토콜
- IP 이동성 지원(모바일 IP) 프로토콜

IP Security(IPsec) 프로토콜

- IPsec(Internet Protocol Security)
 - IP의 안전한 통신을 보장하는 프로토콜 모음
 - 등장 배경
 - 매우 작은 사적 네트워크에서 거대 공중 네트워크로 변하면서 IP에서 보안을 보장하는 방법의 부재
 - 기능
 - 데이터 암호화
 - 무결성 인증
 - 보안 공격으로부터 보호
 - 보안 알고리즘과 키 협상
 - 보안 모드
 - e.g., 터널모드, 전송모드

IP Security(IPsec) 프로토콜

- IPsec의 핵심 프로토콜
 - IPsec 인증 헤더(AH)
 - 인증 서비스 제공
 - 보안 페이로드 캡슐화(ESP)
 - 암호화하여 프라이버시 보장



IP Security(IPsec) 프로토콜

- IPsec 구현 방법

- 종단 호스트 구현

- 모든 호스트 장비에 설치하여 유연성과 보안성을 높임
- 다수의 호스트의 존재로 인해 많은 작업을 필요로 함

- 라우터 구현

- 종단 호스트 보다 작업량이 적음
- 라우터와 로컬 호스트 사이의 연결을 보호되지 않음

IP Security(IPsec) 프로토콜

- IPsec 구조

- TCP/IP 프로토콜 스택과 결합하는 방법

- 통합 구조

- IPsec을 IP 자체에 통합
 - IPsec의 보안 모드와 기능을 일반 IP처럼 쉽게 제공 가능
 - 추가 하드웨어나 계층이 필요하지 않음
 - 실용적이지 않음

- 스택 삽입(BITS, Bump In the Stack) 구조

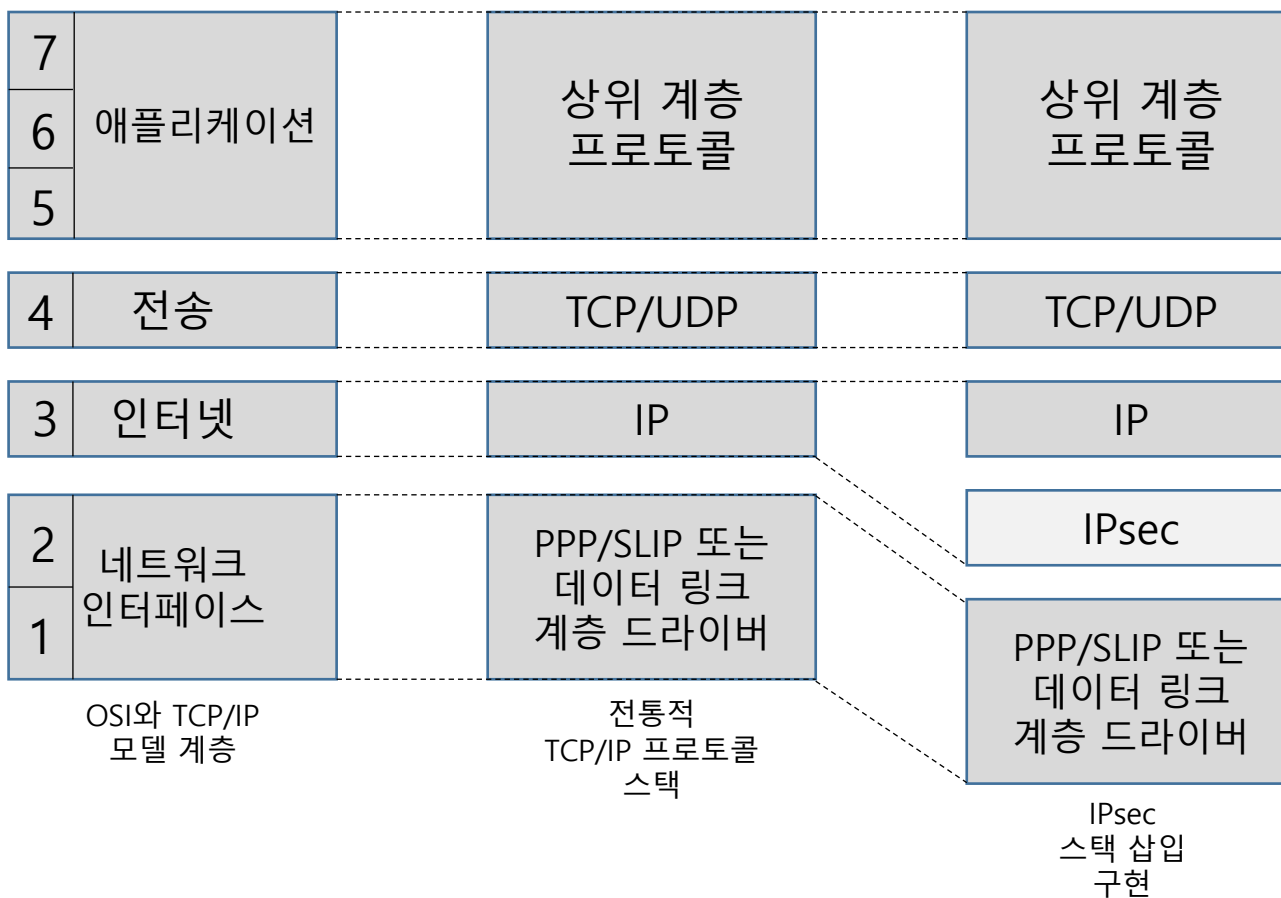
- IP와 IPsec이 별도의 계층으로 존재
 - IP 데이터그램이 아래 방향으로 이동하는 동안 IPsec은 그것을 가로채 보안 기능을 덧붙여 데이터 링크 계층으로 전달

IP Security(IPsec) 프로토콜

- IPsec 구조

- TCP/IP 프로토콜 스택과 결합하는 방법

- 스택 삽입(BITS) 구조



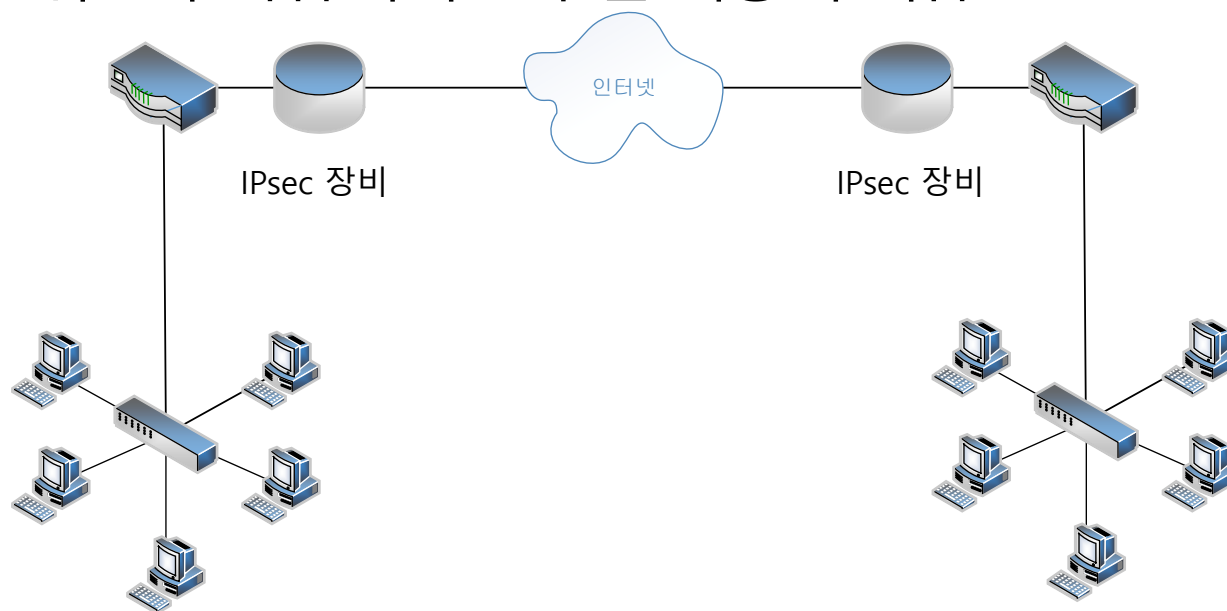
IP Security(IPsec) 프로토콜

- IPsec 구조

- TCP/IP 프로토콜 스택과 결합하는 방법

- 라인 삽입(BITW, Bump In The Wire)

- IPsec 서비스를 제공하는 하드웨어 장비를 추가
 - 외부로 나가는 데이터그램을 가로채 IPsec 보호 기능을 추가해 송신
 - 내부로 들어오는 데이터그램의 IPsec 관련 헤더 제거
 - 네트워크가 복잡해지고 구현 비용이 비쌈

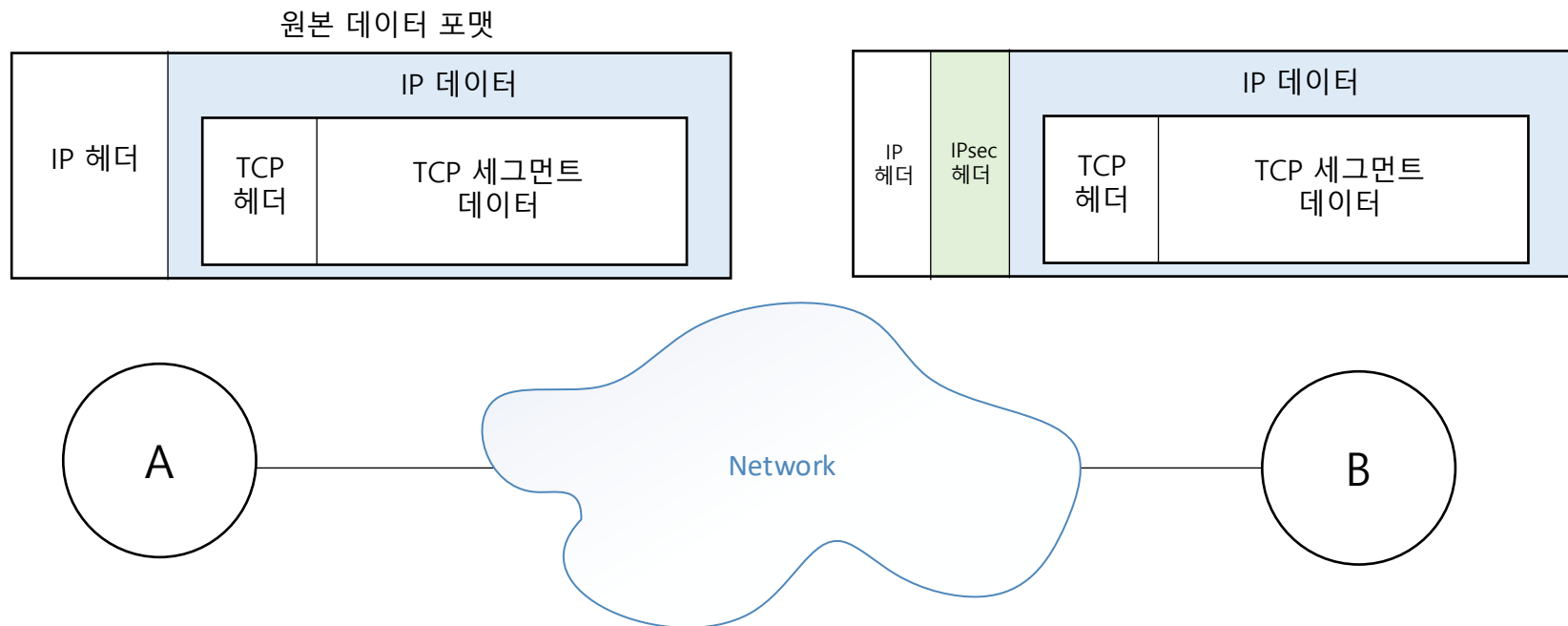


IP Security(IPsec) 프로토콜

- IPsec 동작 모드

- 전송 모드

- 전송 계층에서 IP로 내려온 메시지를 보호
- AH, 혹은 AH와 ESP 조합에 의해 처리
- 위의 헤더는 원본 IP헤더와 IP 페이로드 사이에 위치

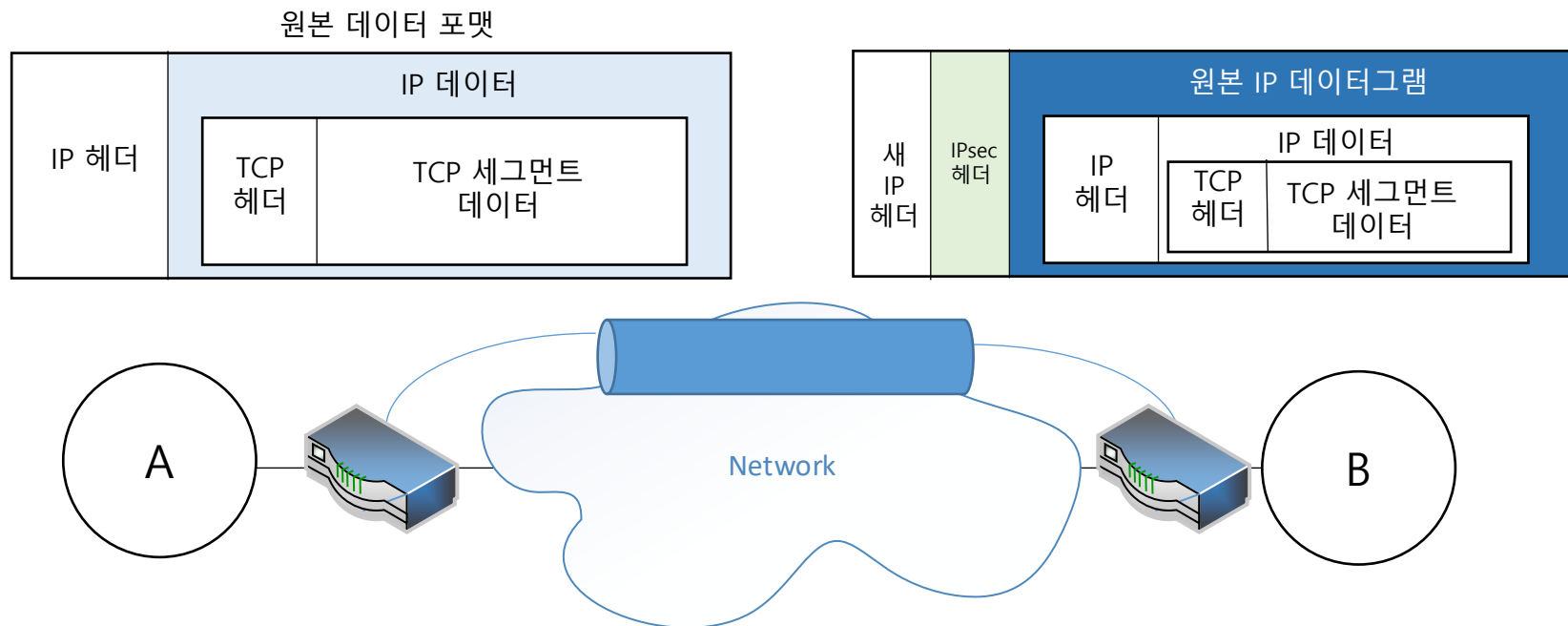


IP Security(IPsec) 프로토콜

- IPsec 동작 모드

- 터널 모드

- IP 헤더가 이미 추가되어 있는 캡슐화된 IP 데이터그램 보호
- 전체 원본 데이터그램이 또 다른 데이터그램 안으로 캡슐화



IP Security(IPsec) 프로토콜

- IPsec 동작 모드

- 전송 모드와 터널 모드 비교

- 터널모드는 원본 IP 데이터그램 전체를 보호

- 헤더 순서

- 전송 모드: IP 헤더, IPsec 헤더, IP 페이로드

- 터널 모드: 새 IP 헤더, IPsec 헤더, 기존 IP 헤더, IP 페이로드

- 전송모드는 IPsec이 IP에 통합

- 터널 모드는 헤더를 붙이고 난 뒤 IPsec을 적용하는 BITS, BITW 구현과 대응

IP Security(IPsec) 프로토콜

- IPsec 보안 구성 요소

- 보안 연관(SA, Security Association)

- 한 장비와 다른 장비 사이에 맺은 보안 방법을 명시
- 보안 연관 데이터베이스(SAD, Security Association Database)
 - 장비의 보안 연관을 저장

- 보안 연관 트리플

- 보안 인자 색인(SPI, Security Parameters Index)
 - 메시지 수신자가 데이터그램에 어떤 SA가 적용되었는지 파악하는데 사용
- IP 목적지 주소
 - SA가 수립된 장비의 주소
- 보안 프로토콜 식별자
 - 이 연관이 AH를 위한 것인지 ESP를 위한 것인지 지정

IP Security(IPsec) 프로토콜

- IPsec 보안 구성 요소
 - 보안 정책(SP, Security Policy)
 - IPsec에 내장된 규칙
 - 장비가 수신하는 서로 다른 데이터그램을 어떻게 처리할 지 지시
 - 보안 정책 데이터베이스(SPD, Security Policy Database)에 저장

IP Security(IPsec) 프로토콜

- IPsec 보안 구성 요소

- 선택자(selector)

- 장비가 특정 데이터그램에 어떤 SA나 보안 정책을 사용할지 결정
- 각 SA가 자신이 적용될 데이터그램을 선택하기 위한 규칙 모음을 정의할 수 있도록 함

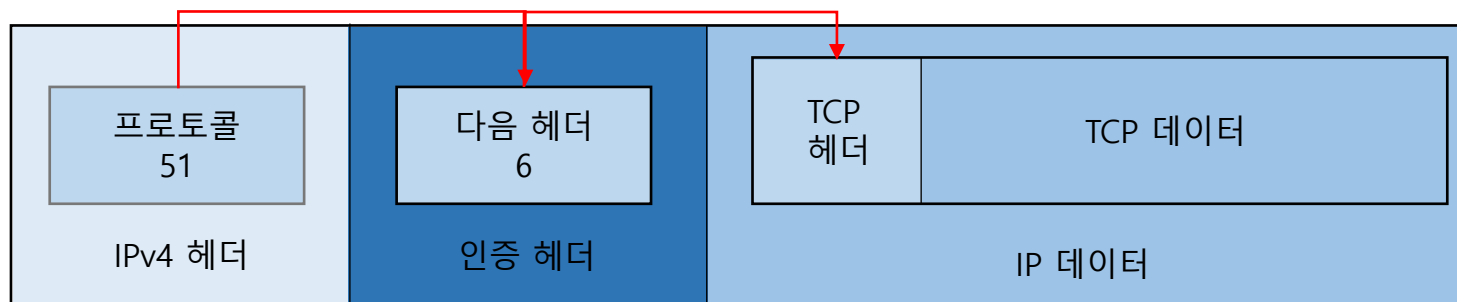
IP Security(IPsec) 프로토콜

- IPsec 인증 헤더(AH)

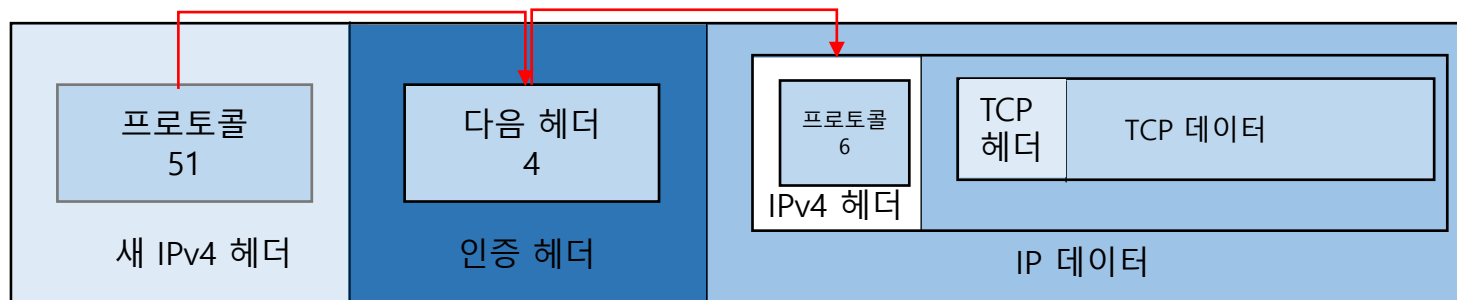
- 헤더를 추가하여 데이터그램 전체 또는 일부분에 대한 인증을 제공
- 무결성은 보장하지만 프라이버스는 제공하지 않음
- 과정
 - 특수 해싱 알고리즘과 특수 키 사용하여 계산
 - 계산을 수행한 결과(ICV, Integrity Check Value)를 다른 필드와 함께 특수 헤더에 넣어 전송
 - 헤더의 위치는 IPsec모드 혹은 IP 버전에 따라 달라짐
 - 목적지 장비는 두 장비가 공유하는 키를 이용하여 계산

IP Security(IPsec) 프로토콜

- IPsec 인증 헤더(AH)
 - AH 데이터그램 위치와 연결
 - 전송 모드



- 터널 모드



IP Security(IPsec) 프로토콜

- IPsec 인증 헤더(AH)
- AH 포맷



IP Security(IPsec) 프로토콜

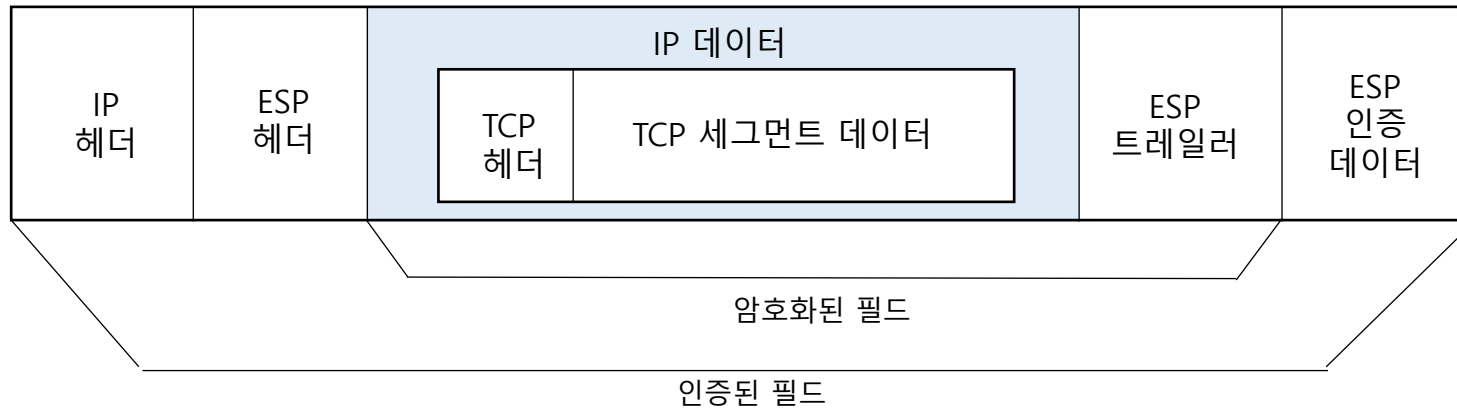
- IPsec 보안 페이로드 캡슐화(ESP)
 - IP 데이터그램을 암호화하여 프라이버시를 보장
 - ESP 필드
 - ESP 헤더
 - SPI와 순서 번호 두 필드를 포함하며 암호화된 데이터 앞에 위치
 - ESP 트레일러
 - 암호화된 데이터 뒤에 위치하여 다음 헤더 필드 포함
 - ESP 인증 데이터
 - ICV 포함
 - ESP 선택적 인증 기능이 적용될 때 사용

IP Security(IPsec) 프로토콜

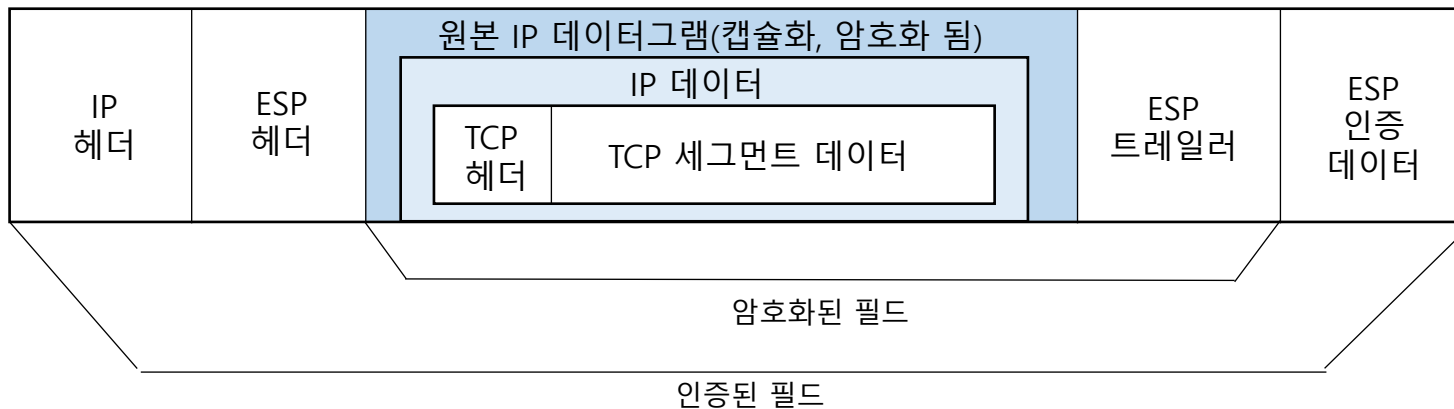
- IPsec 보안 페이로드 캡슐화(ESP)

- ESP 동작과 필드 사용

- 전송 모드

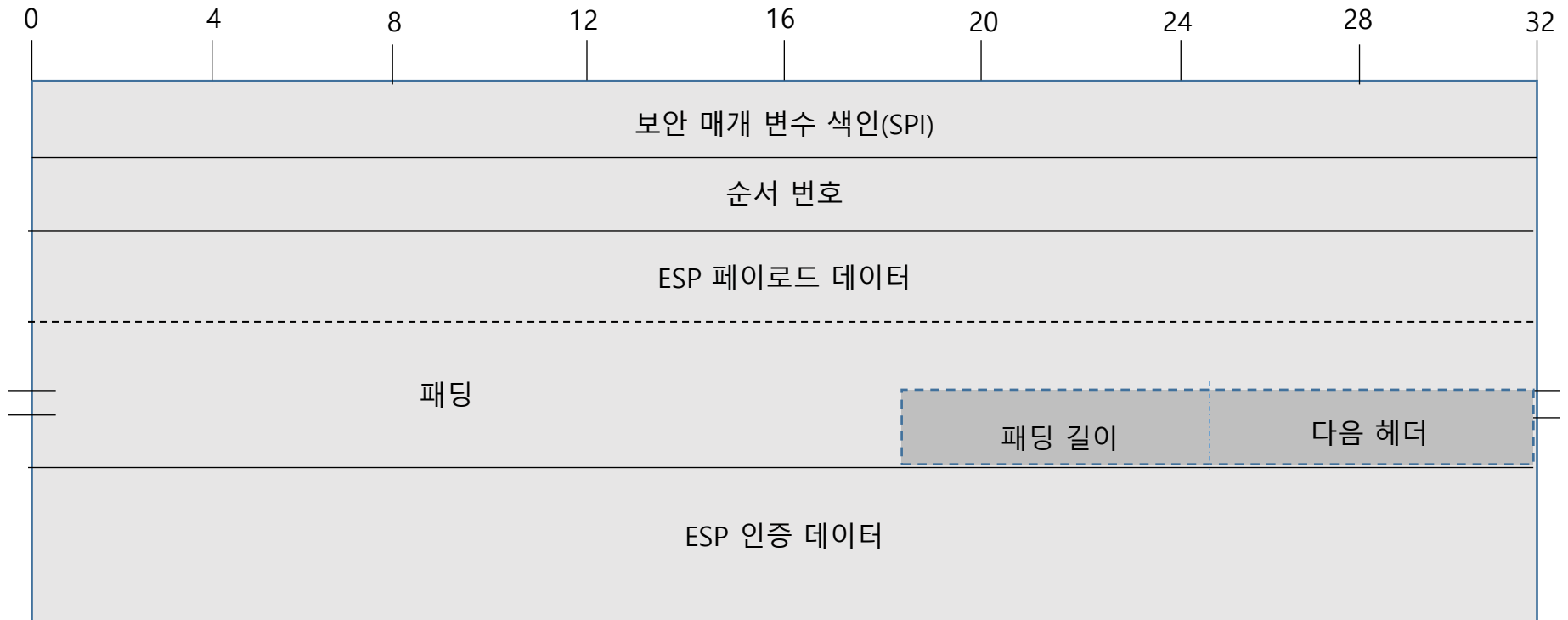


- 터널 모드



IP Security(IPsec) 프로토콜

- IPsec 보안 페이로드 캡슐화(ESP)
- ESP 포맷



IP Security(IPsec) 프로토콜

- IPsec 인터넷 키 교환(IKE, Internet Key Exchange)
 - 두 장비 사이에 안전하게 데이터를 암호화 하기 위해 공유하는 비밀 정보
 - 개요
 - IPsec 지원 장비가 SA를 교환하도록 동작
 - ISAKMP(Internet Security Association and Key Management Protocol)
 - 암호화 키와 보안 연관 정보를 교환하기 위한 구조 제공동작
 - 단계1
 - 협상을 통해 ISAKMP 자체를 위한 SA를 생성
 - 단계2
 - 1단계에서 수립한 SA를 이용하여 기타 보안 프로토콜을 위한 SA 생성

목 차

- 보충
 - PPP 기능 프로토콜
 - IP 멀티캐스트의 주소의 TCP/IP 주소 결정
 - 역순 주소 결정과 TCP/IP 역순 주소 결정 프로토콜
- 네트워크 주소 변환(NAT) 프로토콜
- IP Security(IPsec) 프로토콜
- IP 이동성 지원(모바일 IP) 프로토콜

IP 이동성 지원(모바일 IP) 프로토콜

- 개요

- TCP/IP에서 이동 장비 문제

- IP 주소가 호스트의 네트워크에 결합되어 있음

- 방안

- IP 주소 변경

- 이동한 네트워크의 네트워크 ID 가지도록 호스트의 IP 주소를 변경

- IP 라우팅과 주소 간의 연결 끊기

- 전체 주소를 보고 데이터그램을 전송하도록 장비에 대한 라우팅 방식을 바꿈

- 문제

- 시간이 매우 오래 걸림

- 다른 장비에게 바뀐 주소를 어떻게 알려야 하는가

IP 이동성 지원(모바일 IP) 프로토콜

- 개요

- 해결책

- 기존 장비 주소를 사용하는 중단 없는 장비 이동성 지원
- 새로운 주소 지정 방식이나 라우팅 수정 불필요
- 상호 작용
- 계층 투명성
- 하드웨어 변경 최소화
- 확장성
- 보안

IP 이동성 지원(모바일 IP) 프로토콜

- 개요

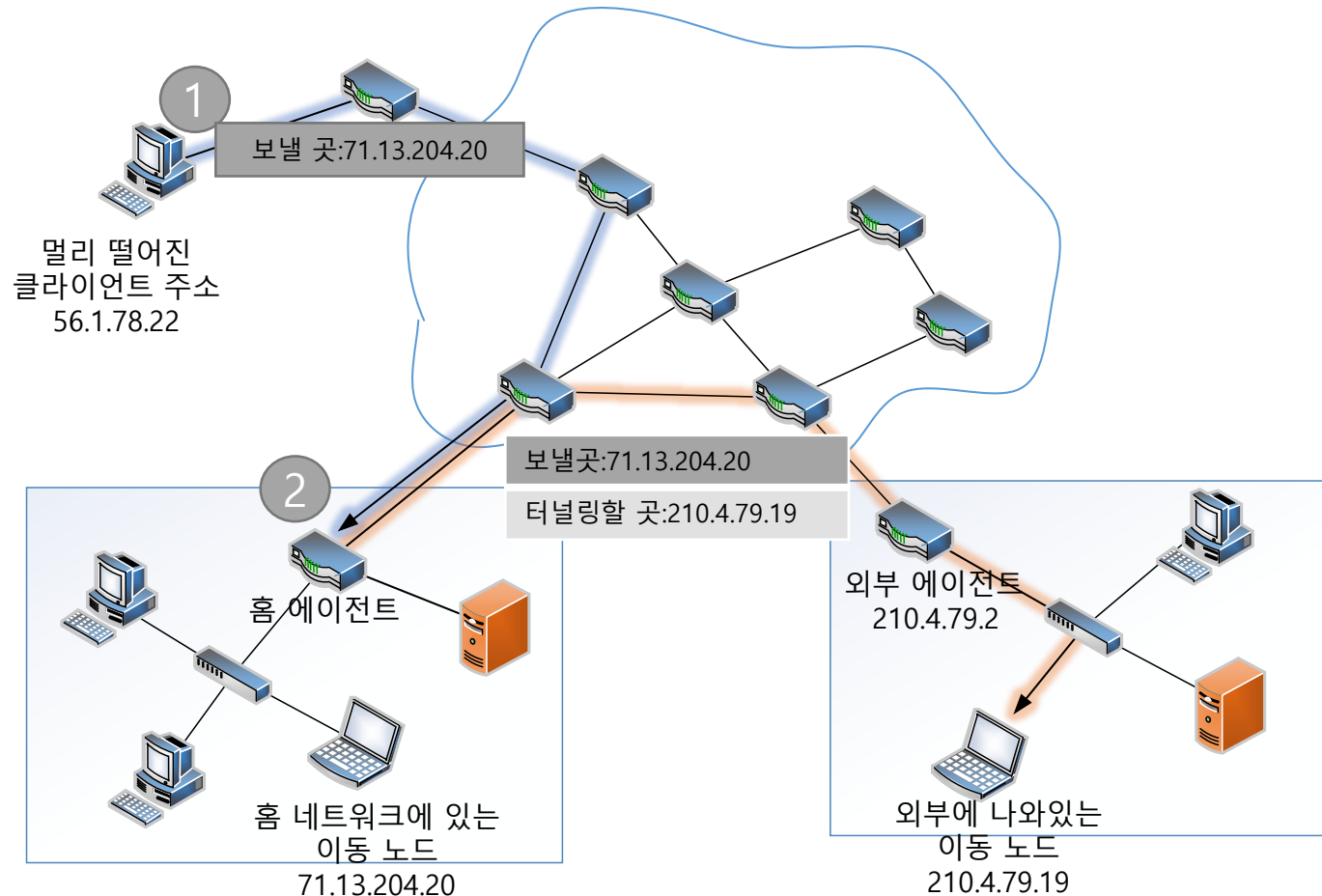
- 모바일 IP 한계

- 모바일 IP는 1초에 1번 이상 네트워크를 바꾸지 않을 것이라는 가정 하에 설계됨
- DHCP(Dynamic Host Configuration Protocol)과 같은 IP를 동적으로 얻는 장비는 모바일 IP를 사용하기 어려움

IP 이동성 지원(모바일 IP) 프로토콜

• 모바일 IP

- 홈 네트워크에 도착한 패킷을 이동 장비가 있는 외부 네트워크로 보내는 시스템



IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 장비 역할

- 이동 장비

- 네트워크 간을 이동하는 장비

- 홈 에이전트

- 홈 네트워크의 라우터

- 이동 장비가 받아야 할 데이터그램을 대신 받아서 전달

- 외부 에이전트

- 외부 네트워크의 라우터

- 홈 네트워크가 전달한 데이터그램을 받아서 이동 장비에게 전달

IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 주소

- 홈 주소

- 이동 장비에게 할당된 고정 IP 주소

- CoA(Care-Of Address)

- 이동 장비가 홈 네트워크 내부로 움직였을 때의 임시 주소
 - 모바일 IP에서만 사용

IP 이동성 지원(모바일 IP) 프로토콜

- CoA
 - 외부 에이전트 CoA
 - 노드의 CoA는 외부 에이전트의 주소
 - 홈 에이전트가 보내는 모든 데이터그램은 외부 에이전트를 지나감
 - 여분의 주소나 주소를 얻기 위한 작업이 필요 없음

IP 이동성 지원(모바일 IP) 프로토콜

- CoA
 - 공존 CoA
 - 이동 장비에게 직접 할당된 주소
e.g., DHCP
 - 홈 에이전트가 데이터그램을 직접 이동 장비에게 전달 가능
 - 주소 고갈 문제가 생길 수 있음
 - 외부 에이전트가 없거나 있더라도 오랫동안 연결을 유지하려 할 때 사용

IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 에이전트 발견
 - 에이전트 발견의 목적
 - 에이전트/노드 통신
 - 에이전트에 대한 정보를 담은 메시지를 노드에게 전송
 - 노드가 에이전트에게 정보를 보내 달라고 요청
 - 현재 위치 발견
 - 노드가 홈 네트워크에 있는지 외부 네트워크에 있는지 확인
 - CoA 할당
 - 외부 에이전트 CoA를 사용하면 이동 장비가 사용할 CoA를 얻음

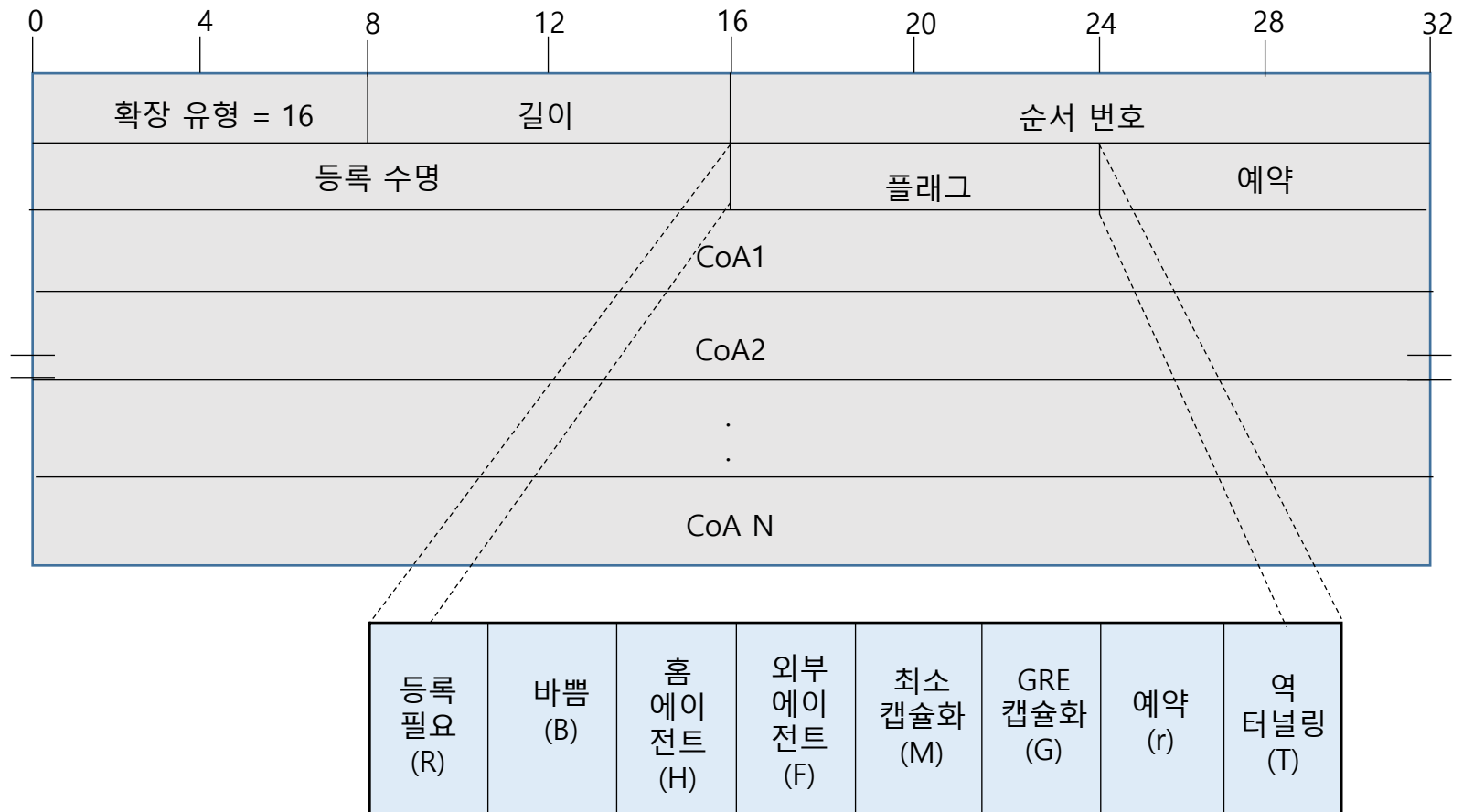
IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 에이전트 발견
 - 에이전트 광고
 - 에이전트로 활동할 수 있는 라우터가 정기적으로 전송
 - 이동 에이전트 광고 확장
 - 에이전트가 모바일 IP 기능을 갖추었다는 것을 알림
 - 접두사 길이 확장
 - CoA 주소 내 네트워크 ID를 알림
 - 1바이트 패딩 확장
 - 메시지 길이를 짝수로 패딩

IP 이동성 지원(모바일 IP) 프로토콜

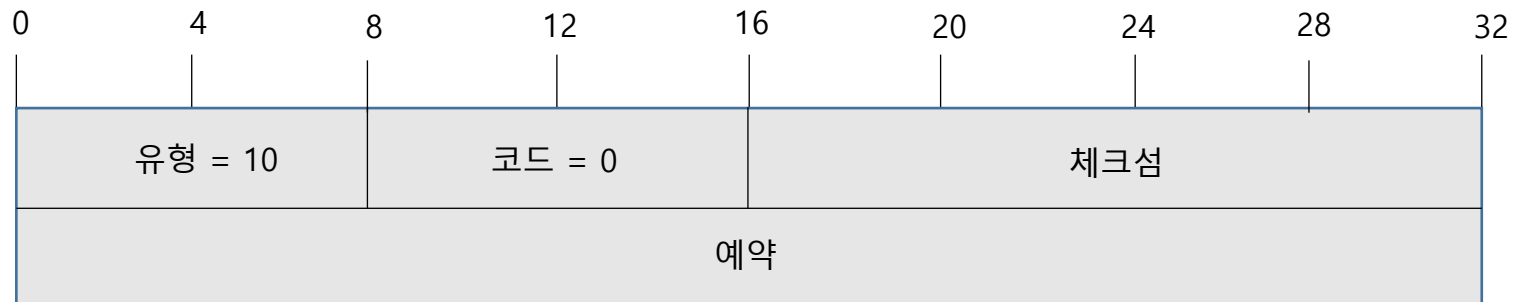
- 모바일 IP 에이전트 발견

- 에이전트 광고
 - 메시지 포맷



IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 에이전트 발견
 - 에이전트 요청
 - 모바일 IP 장비가 로컬 에이전트에게 광고 메시지를 보내 달라고 요청
 - 메시지 포맷



IP 이동성 지원(모바일 IP) 프로토콜

- 에이전트 등록

- 홈 에이전트 등록

- 이동 장비가 홈 에이전트와 통신을 하면서 정보와 지시를 주고받는 것

- 이동 장비 등록 이벤트

- 등록 이동

- 장비가 외부 네트워크에 도착하면 등록 시작

- 등록 해제

- 홈 네트워크로 돌아오면 전달 취소

- 재등록

- 이동 시 CoA가 바뀌면 이동 장비는 홈 에이전트에게 알려 등록 수정

IP 이동성 지원(모바일 IP) 프로토콜

- 에이전트 등록

- 등록 요청과 등록 응답 메시지

- 사용자 데이터그램 프로토콜(UDP, User Datagram Protocol) 사용

- 등록은 다른 모바일 IP 통신과 달리 더 높은 계층에서 일어남

- 등록 과정

- 이동 장비가 사용하는 CoA의 종류에 따른 두 가지 방식

- 직접 등록(공존 CoA)

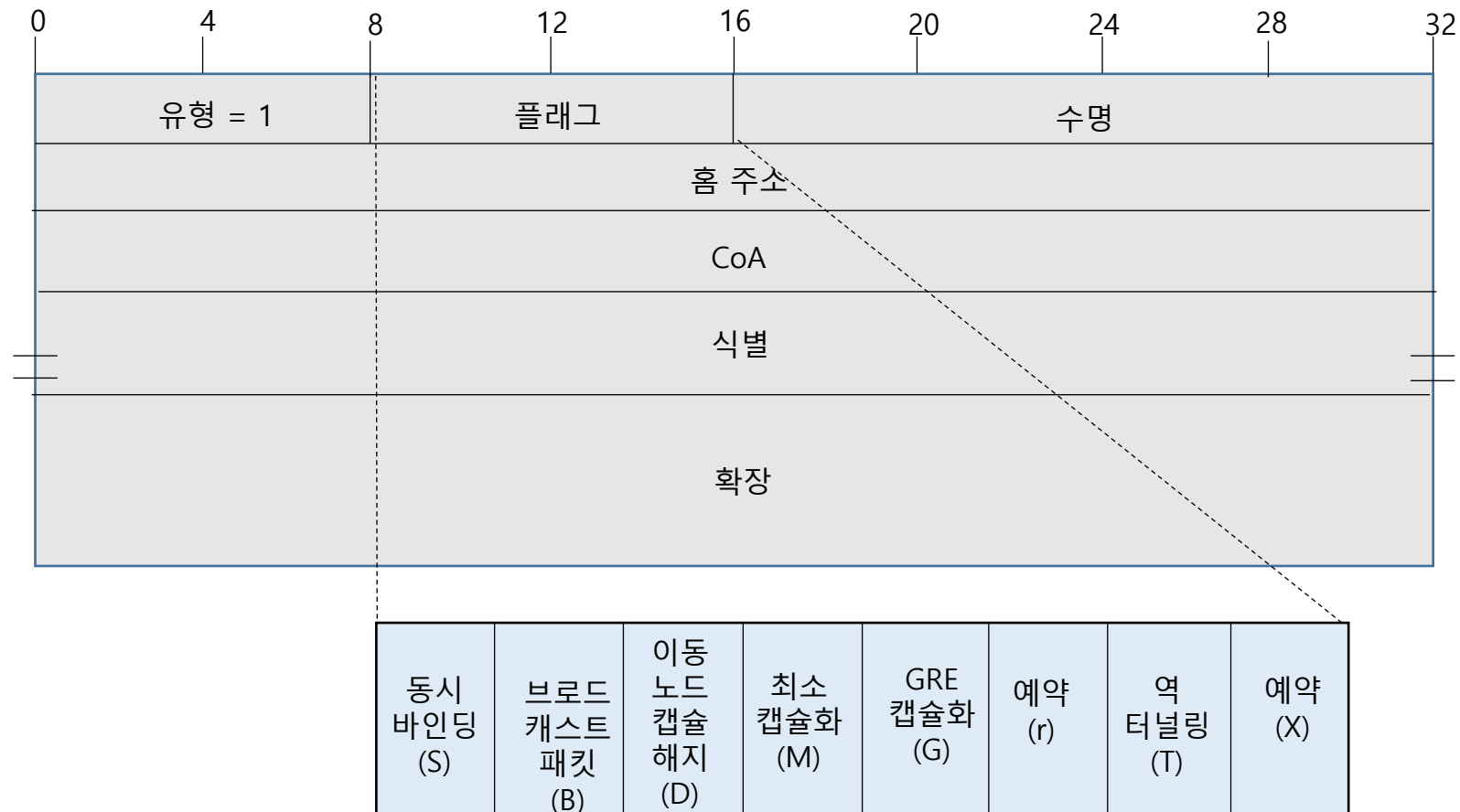
1. 이동 장비가 홈 에이전트에게 등록 요청 메시지 전송
2. 홈 에이전트는 이동 장비에게 등록 응답 메시지 전송

- 간접 등록(외부 에이전트 CoA)

1. 이동 장비가 외부 에이전트에게 등록 요청 메시지 전송
2. 외부 에이전트가 등록 요청을 처리하여 홈 에이전트에게 전송
3. 홈 에이전트는 외부 에이전트에게 등록 응답 메시지 전송
4. 외부 에이전트가 등록 응답을 받아 처리하고 이동장비에게 전송

IP 이동성 지원(모바일 IP) 프로토콜

- 에이전트 등록
- 등록 요청 메시지 포맷



IP 이동성 지원(모바일 IP) 프로토콜

- 에이전트 등록
- 등록 응답 메시지 포맷



IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 데이터 캡슐화와 터널링
 - 홈 에이전트는 패킷을 캡슐화하여 이동 장비의 CoA로 전달
- 모바일 IP 터널링
 - 외부 에이전트 CoA
 - 외부 에이전트에서 터널이 끝남
 - 캡슐화된 데이터그램을 받아 헤더를 벗겨 원래 데이터그램을 이동 장비에게 전달
 - 외부 에이전트와 이동 장비는 같은 로컬 네트워크에 있기 때문에 데이터 링크 계층을 통해 전송
 - 공존 CoA 주소
 - 이동 장비에서 터널이 끝남
 - 장비가 캡슐화 헤더를 벗김

IP 이동성 지원(모바일 IP) 프로토콜

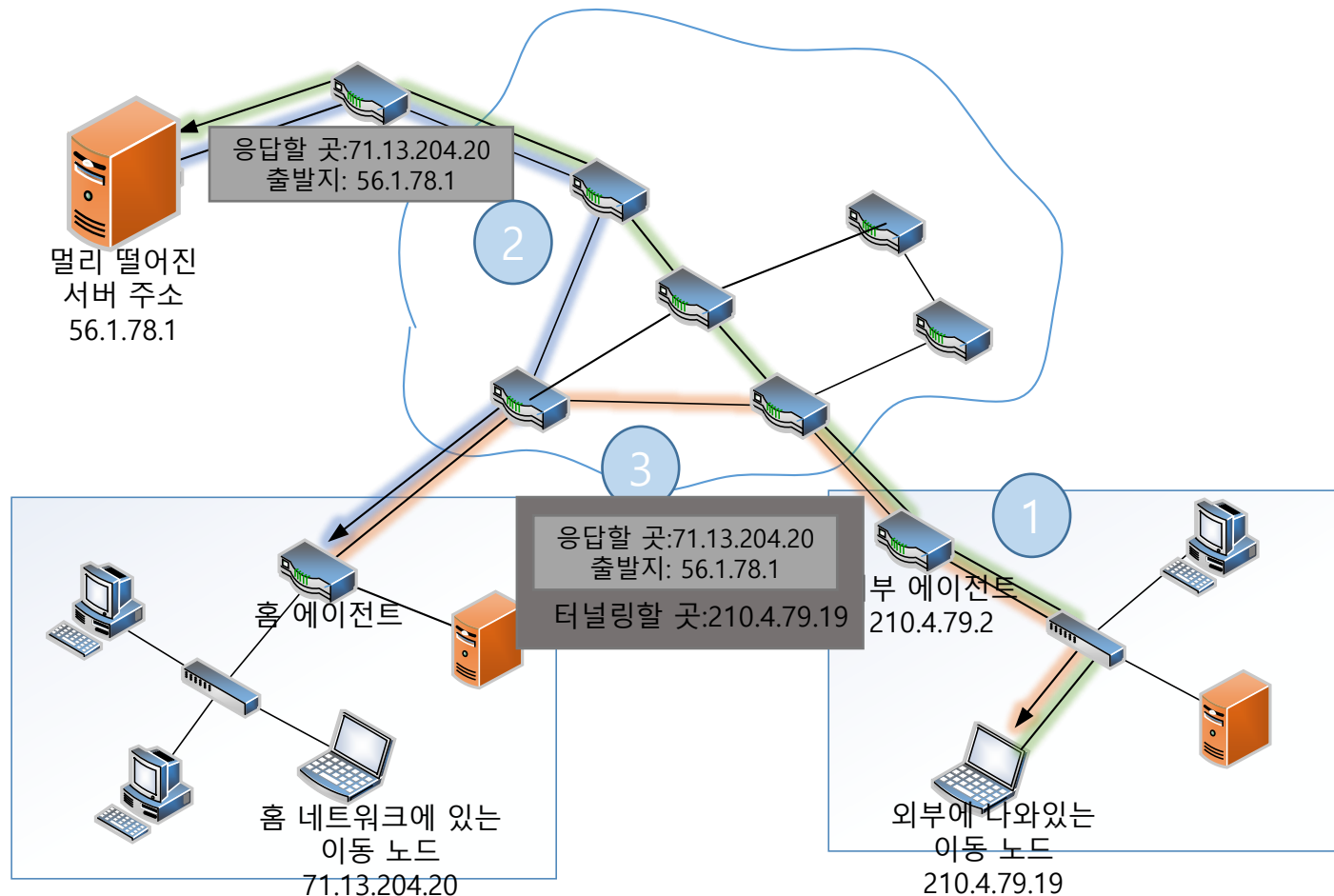
- 모바일 IP 데이터 캡슐화와 터널링

- 터널링 과정

1. 이동 장비는 외부 네트워크 어딘가에 있는 서버에게 모바일 IP 요청
2. 해당 서버는 이동 장비의 출발지 주소인 홈 네트워크로 응답 메시지 전송
3. 홈 에이전트는 도착한 응답을 이동 장비에게 터널링

IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 데이터 캡슐화와 터널링
- 터널링 동작 과정



IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 데이터 캡슐화와 터널링
 - 역터널링
 - 이동 장비가 데이터그램을 인터넷에 직접 전송할 수 없을 경우 사용
 - 총 4번의 전송 과정이 필요하기 때문에 비효율적
 - 이동 장비는 데이터그램을 직접 전송하지 않고 홈 에이전트와의 터널을 통해 전송

IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP와 TCP/IP 주소 결정 프로토콜

- 이동 장비가 로컬 호스트에 없어 ARP를 사용할 수 없을 경우

- 해결 방법

1. ARP 프록싱

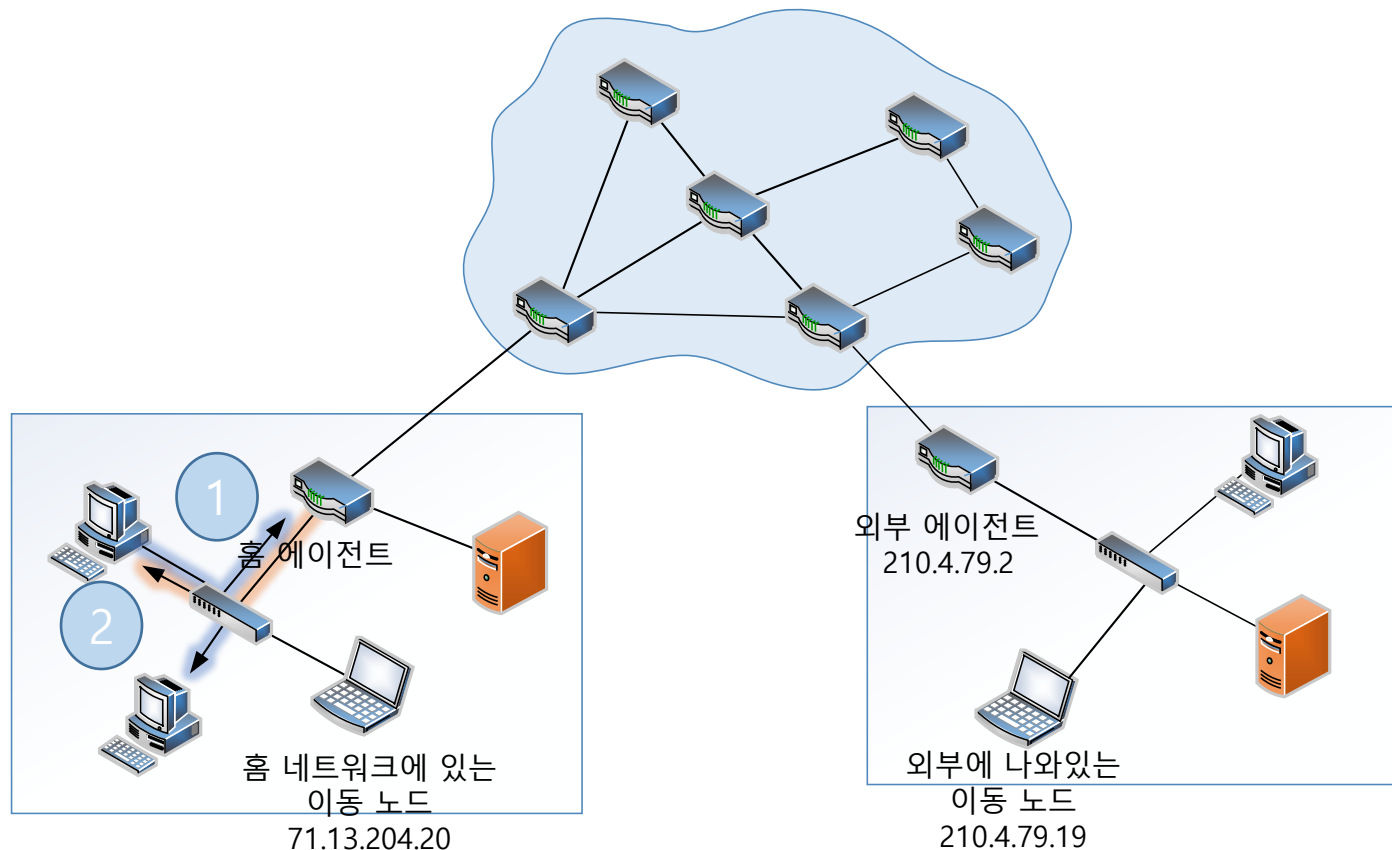
- 홈 에이전트는 이동 장비 대신 ARP 요청을 받음
- 대신 응답하면서 자신의 데이터 링크 계층 주소를 알림
- 홈 에이전트는 해당 데이터그램을 이동 장비에게 전송

2. 무상 ARP

- 이미 이동 장비에 대한 캐시를 갖고 있는 노드일 경우
- 이동 장비가 홈 에이전트의 데이터 링크 주소가 자신과 같다고 로컬 장비들에게 알림

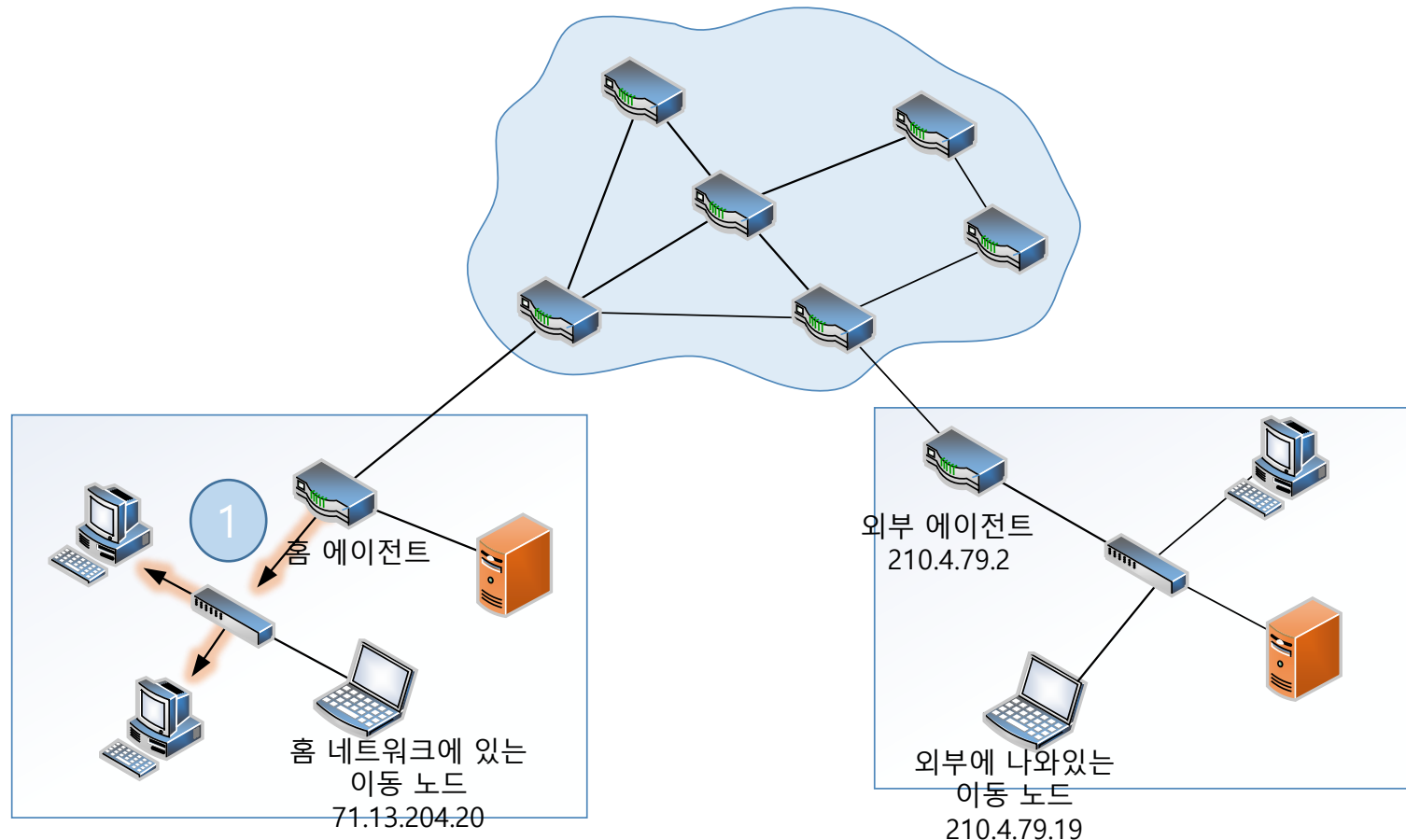
IP 이동성 지원(모바일 IP) 프로토콜

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



IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP와 TCP/IP 주소 결정 프로토콜
- 무상 ARP



IP 이동성 지원(모바일 IP) 프로토콜

- 모바일 IP 효율과 보안 문제

- 효율

- 노드와 이동 장비 간의 거리에 따라 비효율 정도가 달라짐
 - 전송자와 이동 장비가 같은 외부 네트워크에 있다면 가장 효율성이 떨어짐

- 보안 문제

- 전송 자체가 공개되어 있기 때문에 도청 가능
- 재생 공격 문제
- 등록 메시지 외의 메시지에 대한 인증의 부재
- 추가적인 인증과 기밀성을 위해 IPsec의 AH나 ESP를 사용

Thanks!

이 하 늘(dlgksmf6789@sju.ac.kr)