

2020/07/24, 2020 보안 기초 세미나

TCP/IP 완벽 가이드

- 2부 TCP/IP 하위 계층 핵심 프로토콜 -

박재형 (jaehyoung@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

목 차

- 2 - 1부 TCP/IP 네트워크 인터페이스 계층 프로토콜
 - SLIP와 PPP 개요
 - PPP 핵심 프로토콜
 - PPP 인증 프로토콜
 - PPP 기능 프로토콜
 - PPP 프로토콜 프레임 포맷
- 2 - 2부 네트워크 인터넷 계층 연결 프로토콜
 - 주소 결정 프로토콜
 - 역순 주소 결정 프로토콜

목 차

- 2 – 1부 TCP/IP 네트워크 인터페이스 계층 프로토콜
 - SLIP와 PPP 개요
 - PPP 핵심 프로토콜
 - PPP 인증 프로토콜
 - PPP 기능 프로토콜
 - PPP 프로토콜 프레임 포맷
- 2 – 2부 네트워크 인터넷 계층 연결 프로토콜
 - 주소 결정 프로토콜
 - 역순 주소 결정 프로토콜

SLIP와 PPP 개요

- 네트워크 인터페이스 계층 프로토콜

- 두 장비가 논리적 링크만으로 통신 불가

- 1, 2계층: 물리적 링크
- 3계층: 논리적 링크

- 네트워크 인터페이스 계층을 이용하여 통신 가능

- 1, 2계층과 3계층을 연결할 수 있는 인터페이스 프로토콜 필요



OSI와 TCP/IP 4계층 모델

SLIP와 PPP 개요

- SLIP와 PPP

- 네트워크 인터페이스 계층 프로토콜

- SLIP (Serial Line Internet Protocol)

- IP에 대한 프레임링 (Framing)만을 제공하는 매우 간단한 프로토콜

- PPP (Point-to-Point Protocol)

- SLIP가 가진 한계점을 개선하기 위해 확장된 프로토콜

- 보완점: 보안, 압축, 인증 등

SLIP와 PPP 개요

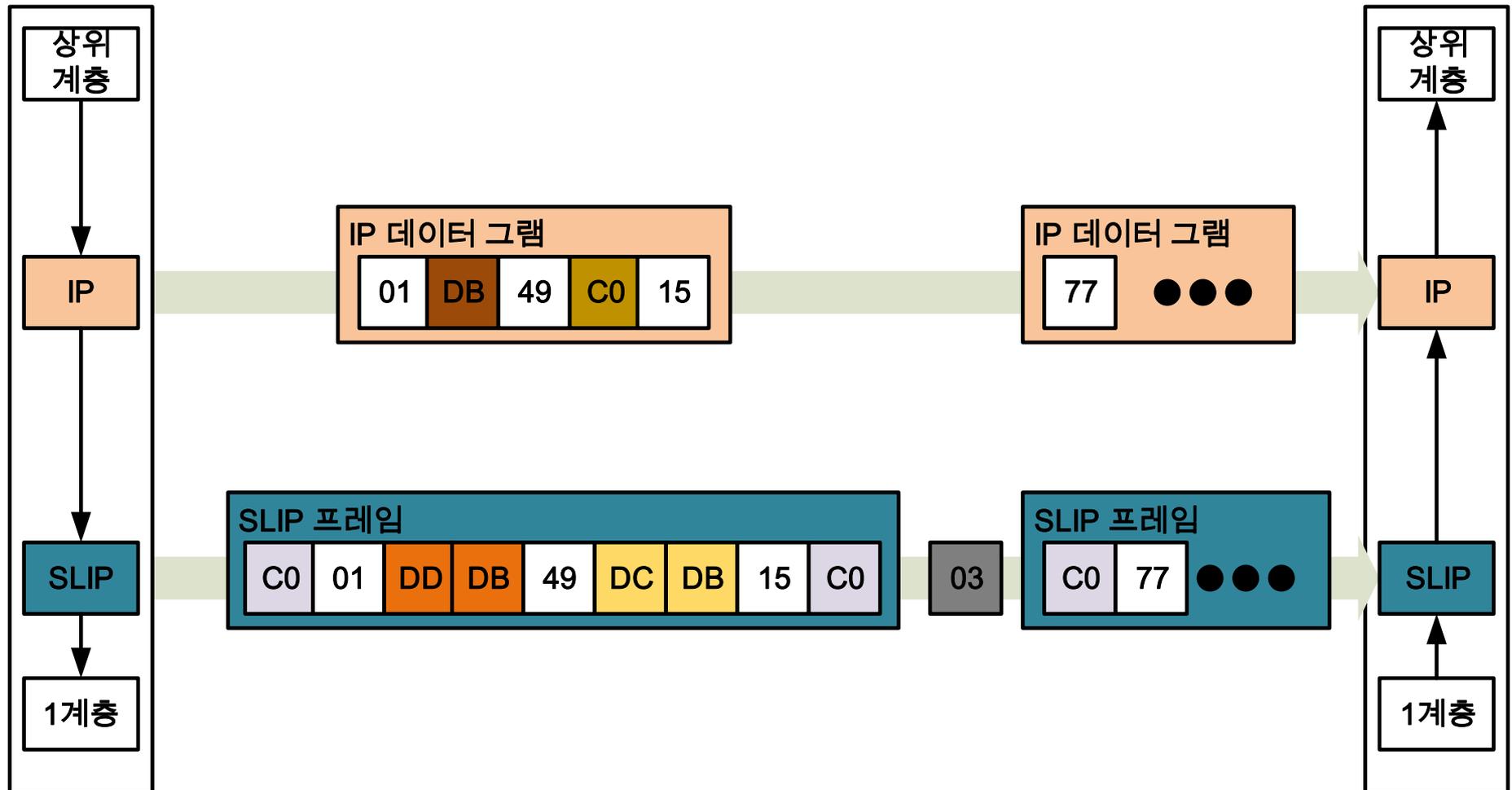
- SLIP (Serial Line Internet Protocol)

- IP 데이터 프레임링 과정

1. SLIP은 IP 데이터그램을 바이트로 나눈 뒤 물리 링크를 통해 전송
2. 바이트 시작 전과 마지막 바이트 끝에 SLIP END를 보냄
 - SLIP END: 16진수 C0
3. 전송 할 때, 전송할 데이터그램에 C0값이 있으면 DB, DC 2바이트로 치환
4. 전송 할 때, 전송할 데이터그램에 DB값이 있으면 DB, DD 2바이트로 치환
5. SLIP 프레임 전송

SLIP

- IP 데이터 프레임밍 과정



SLIP

- 한계점

- 에러 탐지 및 정정 기능을 제공하지 않음
- 헤더가 없기 때문에 프로토콜 유형 식별 불가능
- 속도 향상을 위한 압축기능 제공하지 않음
- 데이터 암호화와 같은 보안기능을 제공하지 않음

SLIP과 PPP 개요

- PPP (Point-to-Point Protocol)

- 프레이밍 기능 뿐만 아니라 에러탐지, 압축, 인증, 암호화 기능을 제공하는 네트워크 인터페이스 계층 프로토콜

- 특징

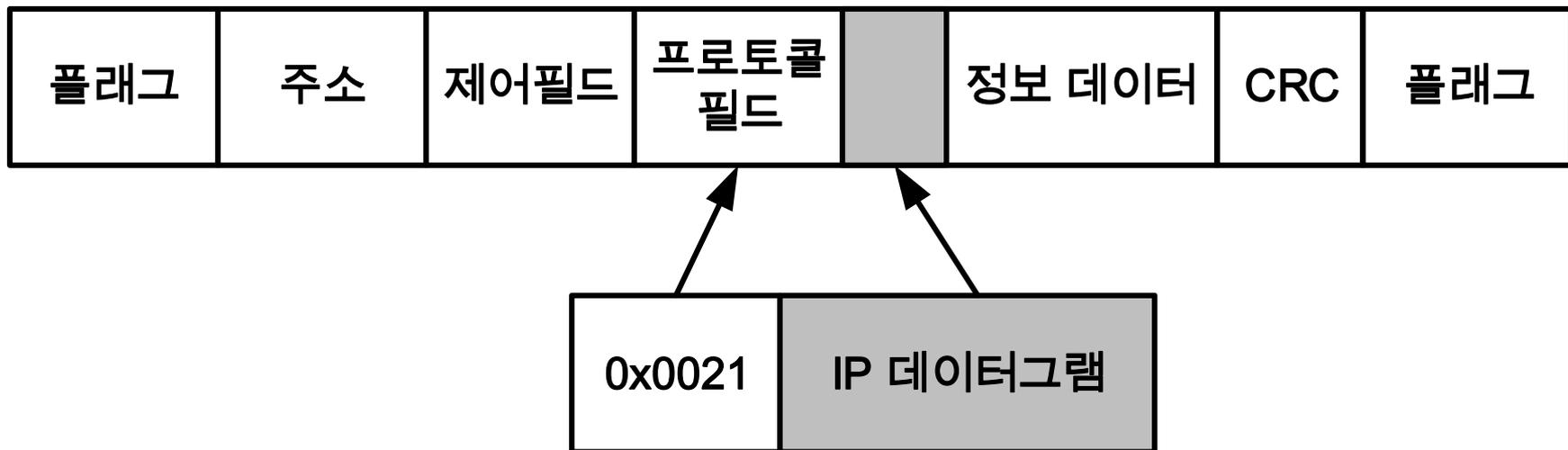
- 각 프레임 헤더에 CRC (Cyclic redundancy check) 코드를 삽입하여 전송 프레임의 에러 탐지
- PPP의 기능 프로토콜 사용으로 압축, 인증 암호화 기능 제공
 - 기능 프로토콜: PAP, CHAP, CCP, ECP 등
- 전송이 일어나기 전 링크 테스트, 링크 품질 모니터링 가능
 - 링크 테스트: 에코 요청/응답
 - 링크 품질 모니터링: LQM (Link Quality Monitoring) 설정 옵션

PPP

- PPP 주요 구성 요소

- PPP 캡슐화

- IP 데이터그램과 같은 3계층 메시지를 받아서 1, 2계층으로 전송하기 위해 PPP 포맷에 IP데이터그램을 추가하는 방법



- 0x0021 = IPv4 (internet Protocol, version 4)

PPP

- PPP 주요 구성 요소

- 링크 제어 프로토콜 (LCP, Link Control Protocol)
 - 장비간 링크의 수립, 유지, 종료를 책임지는 프로토콜
 - 링크 사용 방법을 협의 하기 위한 설정 인자 교환
 - 설정 인자: 최대 프레임 길이, 사용할 기능 프로토콜 결정
- 네트워크 제어 프로토콜 (NCP, Network Control Protocol)
 - 네트워크 계층 프로토콜의 사용을 협상하는 프로토콜

PPP

- PPP 인증 프로토콜

- 링크 수립과정에서 인증을 위해 선택적으로 사용 가능한 프로토콜
 - CHAP (Challenge Handshake Authentication Protocol)
 - PAP (Password Authentication Protocol)

- PPP 기능 프로토콜

- 링크가 수립되고 장비 간 패킷이 전송될 때 기능을 향상시키기 위한 프로토콜
 - CCP (Compression Control Protocol)
 - ECP (Encryption Control Protocol)
 - MP (Multilink Protocol)

PPP

- PPP 링크 수립과 단계
 - 링크 비활성화 (Link dead) 단계
 - 장비 간 아무런 물리계층 연결이 존재하지 않는 단계
 - 물리 계층 연결이 구성되면 링크 수립 단계로 넘어감
 - 링크 수립 (Link establishment) 단계
 - 링크의 기본 설정을 수행하는 단계
 - 물리 링크를 통해 LCP 설정요청 메시지 전송
 - 수신장비가 사용하고자 하는 인자와 송신장비가 사용하고자 하는 인자의 교환

PPP

- PPP 링크 수립과 단계
 - 링크 수립 (Link establishment) 단계
 - LCP설정 협상 성공 시
 - LCP 개방 (LCP open) 으로 바뀌며 인증 단계로 넘어감
 - LCP설정 협상 실패 시
 - 수신 장비는 받아들이지 않는 인자 정보 포함한 비 승인 메시지를 전송
 - 송신 장비는 수신장비가 받아들일 수 있는 새 인자로 다시 요청
 - 협상 하지 못한다면 링크 비활성화 단계로 되돌아감

PPP

- PPP 링크 수립과 단계
 - 인증 (Authentication) 단계
 - 수신 장비가 송신장비에게 접속하기 전에 인증을 요구하는 단계
 - 인증을 하기위해 인증 프로토콜 사용
 - e.g., CHAP, PAP
 - 네트워크 계층 프로토콜 (Network layer protocol) 단계
 - 네트워크 계층 프로토콜에 맞는 설정을 위해 NCP를 호출하는 단계

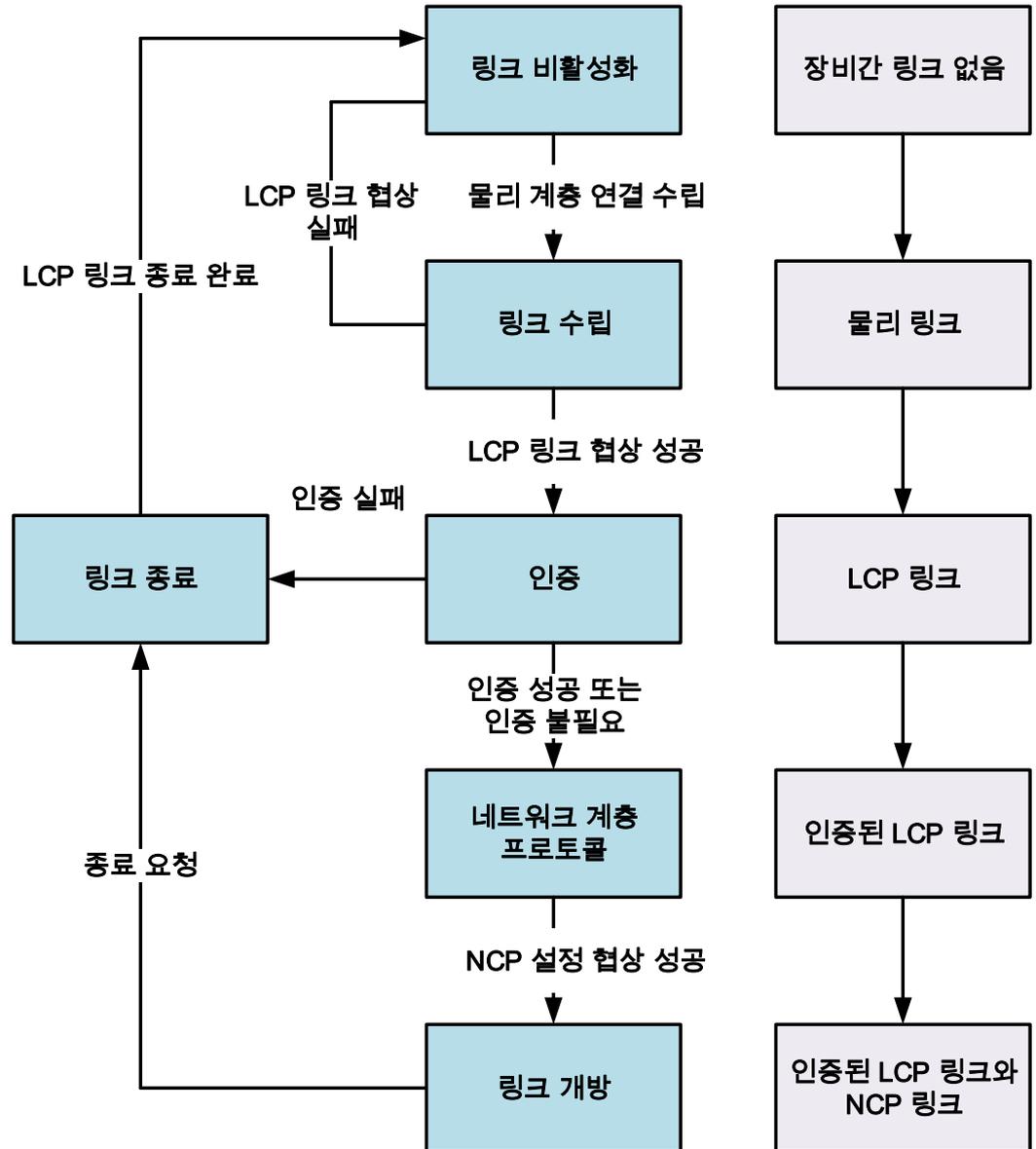
PPP

- PPP 링크 수립과 단계
 - 링크 개방 (Link open) 단계
 - 개방된 LCP 링크와 NCP 링크로 데이터가 송·수신 됨
 - 링크 종료 (Link termination) 단계
 - LCP 종료 프레임을 전송하고 수신장비는 승인함
 - 링크는 비활성화 단계로 돌아감

PPP

• PPP 링크 수립과 단계

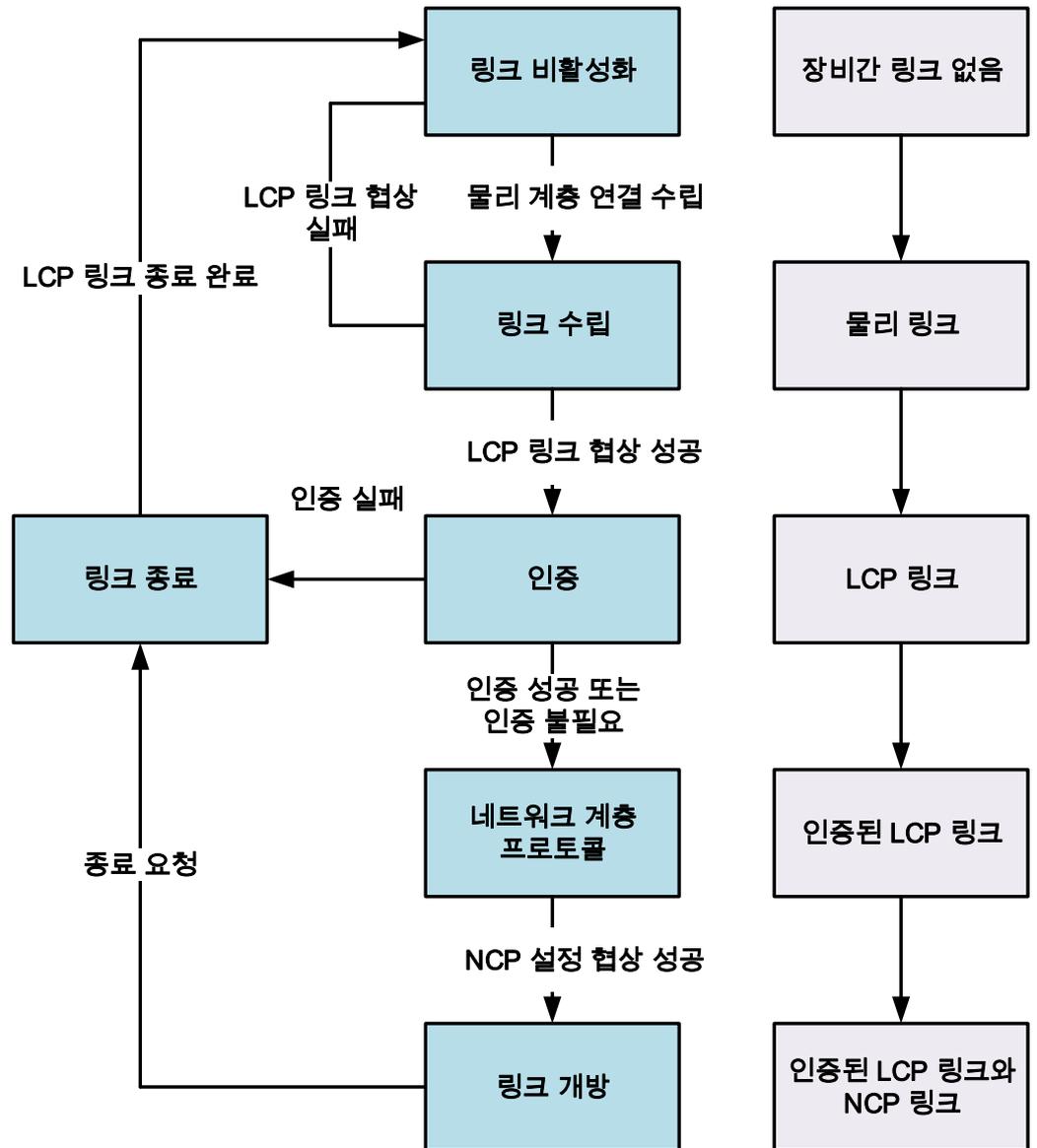
- 링크 비활성화 단계에서 물리 계층 연결 수립 시 링크 수립 단계로 넘어감
- 수립 실패 시 다시 링크 비활성화 단계로 돌아감
- 수립 성공 시 인증 단계로 넘어감
- 인증 실패 시 링크 종료 요청/응답으로 링크 종료



PPP

• PPP 링크 수립과 단계

- 인증 성공 시 네트워크 계층 프로토콜 단계로 넘어감 (NCP 호출)
- 협상 성공 시 링크 개방
- 링크 종료를 원할 때 종료요청/응답으로 링크 종료



목 차

- 2 – 1부 TCP/IP 네트워크 인터페이스 계층 프로토콜
 - SLIP과 PPP 개요
 - PPP 핵심 프로토콜
 - PPP 기능 프로토콜
 - PPP 프로토콜 프레임 포맷
- 2 – 2부 네트워크 인터넷 계층 연결 프로토콜
 - 주소 결정 프로토콜
 - 역순 주소 결정 프로토콜

PPP 핵심 프로토콜

- LCP (Link Control Protocol)
 - PPP에서 장비간 링크의 수립, 유지, 종료를 책임지는 프로토콜
 - 링크 설정
 - 최대 수신 유닛 (MRU, Maximum Receive Unit)
 - 링크에서 전달하고자 하는 최대 데이터그램 크기 지정
 - 인증 프로토콜 (Authentication protocol)
 - 사용하고자 하는 인증 프로토콜 유형 지정
 - e.g., PAP, CHAP
 - 품질 프로토콜 (Quality protocol)
 - 링크에 대한 품질 모니터링을 하기위한 프로토콜을 유형 지정
 - e.g., LQR

PPP 핵심 프로토콜

- LCP (Link Control Protocol)
 - 링크 설정
 - 매직 넘버 (Magic number)
 - 랜덤하게 생성된 값을 전송하고 동일한 숫자가 돌아오는지 판단
 - 루프 백 링크 또는 기타 연결의 비정상성을 탐지
 - 프로토콜 필드 압축 (PFC, Protocol Field Compression)
 - e.g., 송신 장비가 일반적인 16비트 Protocol 필드 대신 압축된 8비트 Protocol 필드 사용하고자 수신장비에게 요청
 - PPP 프레임마다 1바이트 대역폭 절약
 - 주소 제어 필드 압축 (ACFC, Address and Control Field Compression)
 - 대역폭 절약을 위한 주소와 제어 필드를 압축

PPP 핵심 프로토콜

• LCP

• LCP 링크 유지

- LCP 프레임 코드를 사용하여 링크를 관리하거나 유지함
 - 코드 거부와 프로토콜 거부
 - 인식되지 않은 LCP 프레임 코드를 받은 경우
 - 잘못된 프로토콜 인한 유효하지 않은 프레임을 받은 경우
 - 에코 요청/응답
 - 링크를 테스트하는 데 쓰임

• LCP 링크 종료

- 종료 요청/응답 메시지를 통해 링크 종료

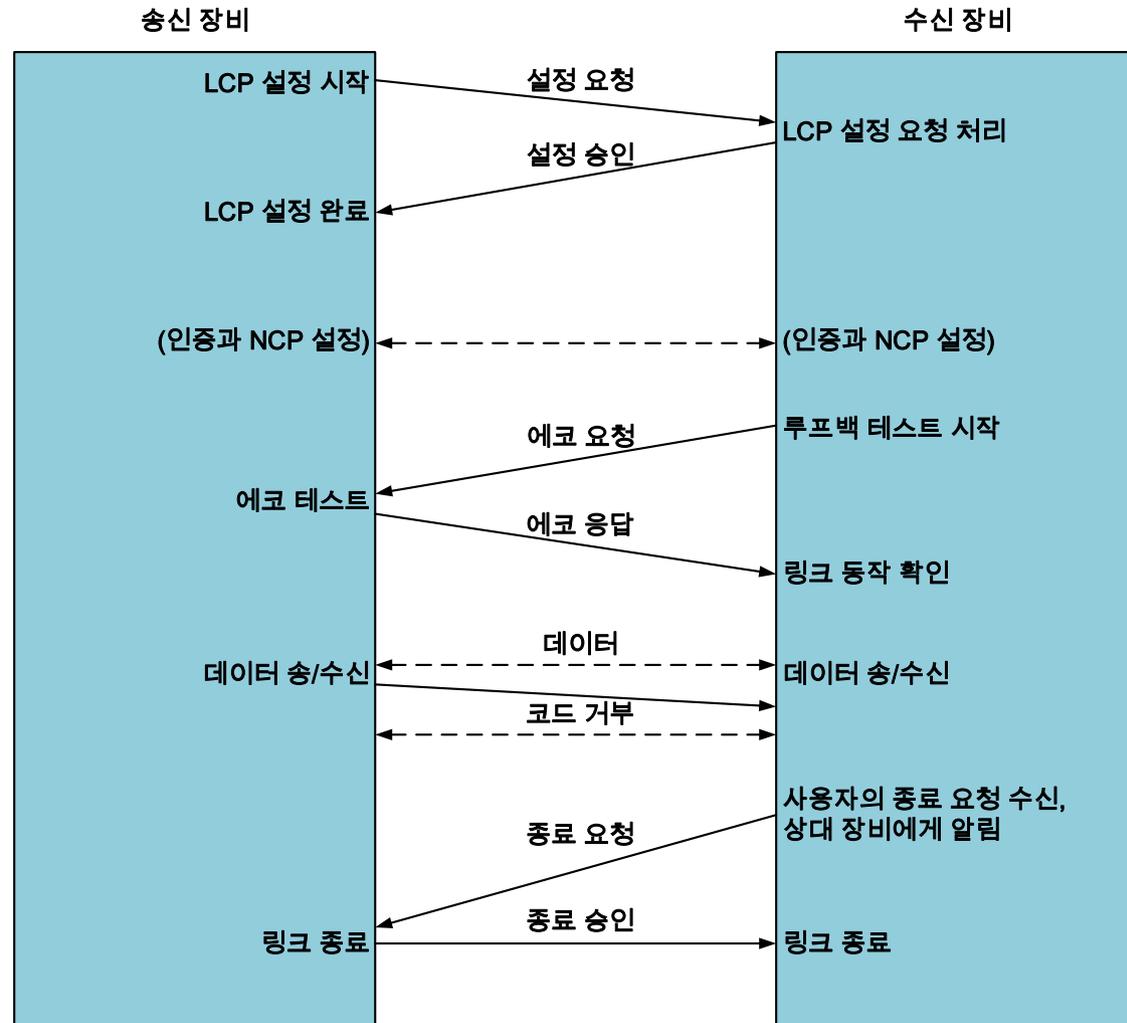
링크 상태	코드	프레임 유형
링크 설정	0x01	설정 요청
	0x02	설정 승인
	0x03	설정 비승인
	0x04	설정 거부
링크 종료	0x05	종료요청
	0x06	종료승인
링크 유지	0x07	코드 거부
	0x08	프로토콜 거부
	0x09	에코 요청
	0x0A	에코응답
	0x0B	버림 요청

LCP 프레임 코드

PPP 핵심 프로토콜

• LCP

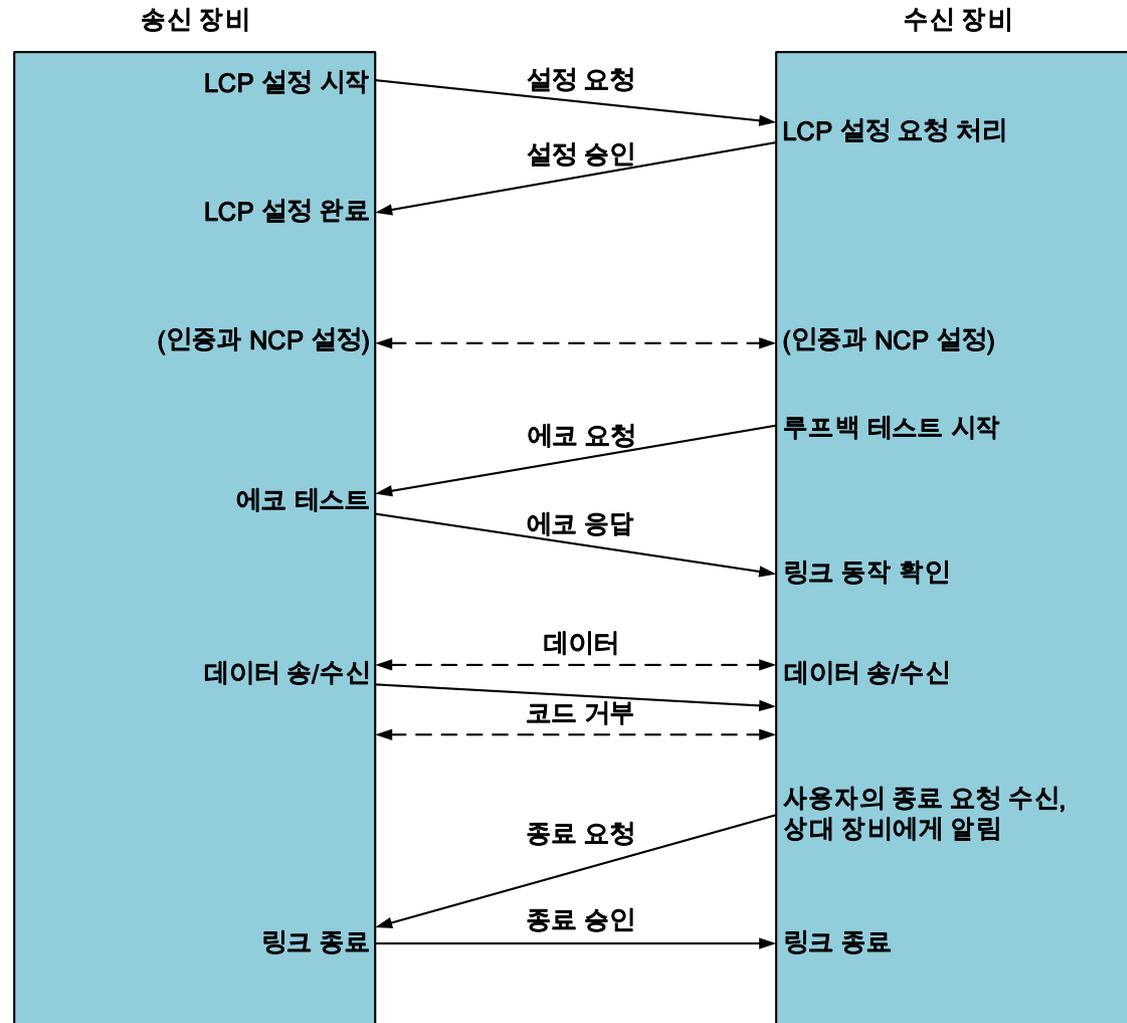
- LCP 메시지 교환 과정
 - LCP 링크 설정 요청/승인 과정으로 링크 생성
 - 인증과정을 통한 인증된 LCP 링크 생성
 - NCP 호출
 - 링크 동작 확인
 - 루프백 테스트
 - 에코 요청/응답



PPP 핵심 프로토콜

• LCP

- LCP 메시지 교환 과정
 - 데이터 송/수신
 - 종료를 원할때 종료 요청/응답으로 링크 종료



PPP 핵심 프로토콜

- NCP (Network Control Protocol)
 - PPP에서 장비간 사용할 인터넷 계층 프로토콜을 협상하는 프로토콜
 - LCP로 링크가 수립되면 각 인터넷 계층 프로토콜에 해당하는 NCP 전송
 - 각 LCP 링크 별로 NCP를 운영
 - IP에 해당하는 LCP 링크라면 IPCP (NCP)호출
 - RFC 명시
 - IP (LCP)링크 => IPCP (NCP)호출
 - IPX (LCP)링크 => IPXCP (NCP)호출
 - NBF (LCP)링크 => NBFCP (NCP)호출

PPP 핵심 프로토콜

- NCP
 - IPCP (Internet Protocol Control Protocol)
 - IP 데이터그램을 전송하기 위해 PPP가 수립될 경우 호출되어 IP사용을 협상 하기위한 NCP
 - IPCP 기능
 - TCP/IP 헤더 압축 여부 협상
 - IP 압축 프로토콜 사용
 - 대역폭 절약 가능
 - IP 라우팅 용도로 사용할 IP 주소를 지정
 - 상대방 IP주소 요청

PPP 핵심 프로토콜

• NCP

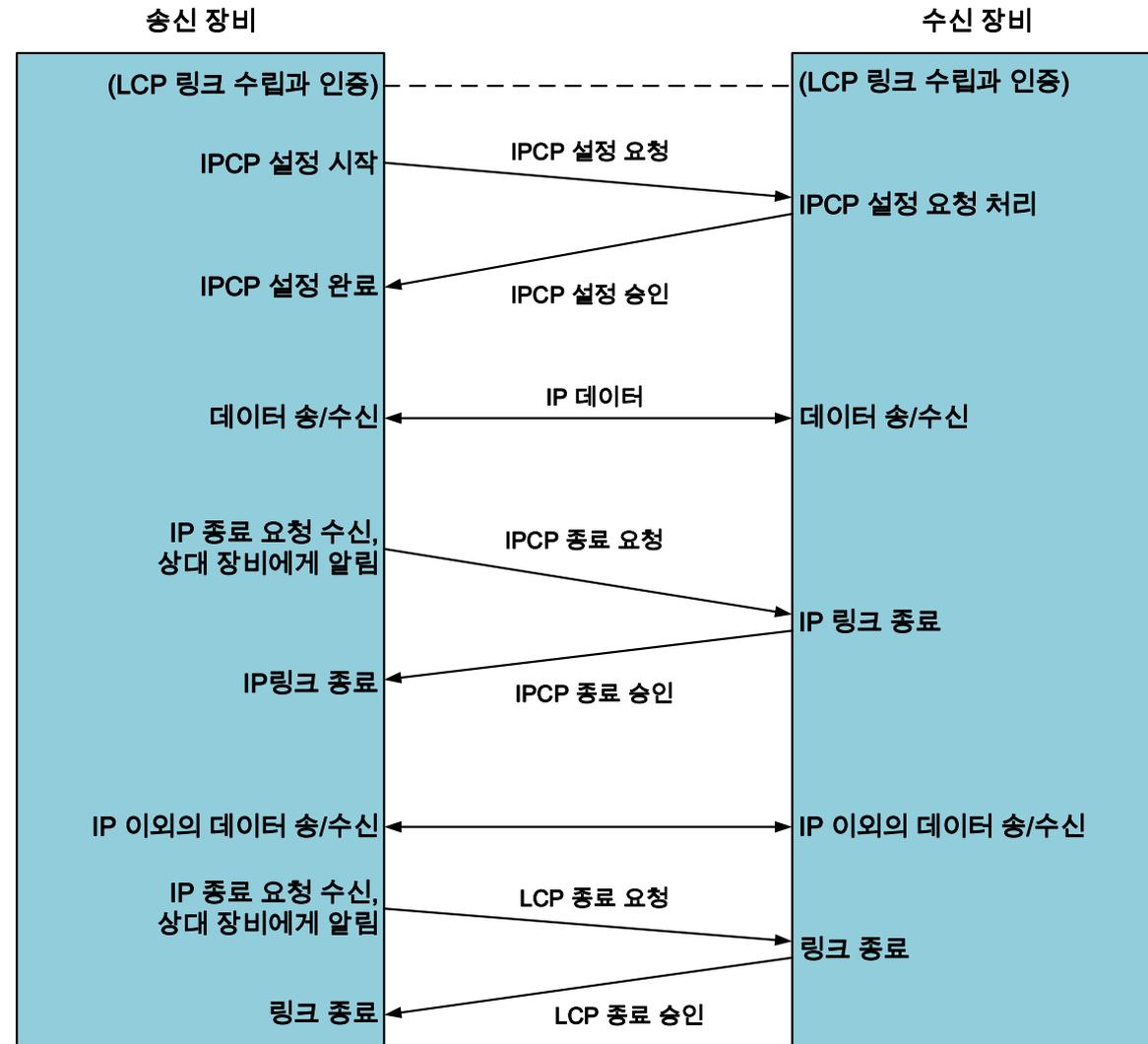
• IPCP(NCP)동작

- LCP 링크 수립

- IPCP 설정 요청/승인

- IP 데이터 송/수신

- IP 종료 요청이 수신
되면 IPCP 종료 요청/
승인



목 차

- 2 - 1부 TCP/IP 네트워크 인터페이스 계층 프로토콜
 - SLIP와 PPP 개요
 - PPP 핵심 프로토콜
 - PPP 인증 프로토콜
 - PPP 기능 프로토콜
 - PPP 프로토콜 프레임 포맷
- 2 - 2부 네트워크 인터넷 계층 연결 프로토콜
 - 주소 결정 프로토콜
 - 역순 주소 결정 프로토콜

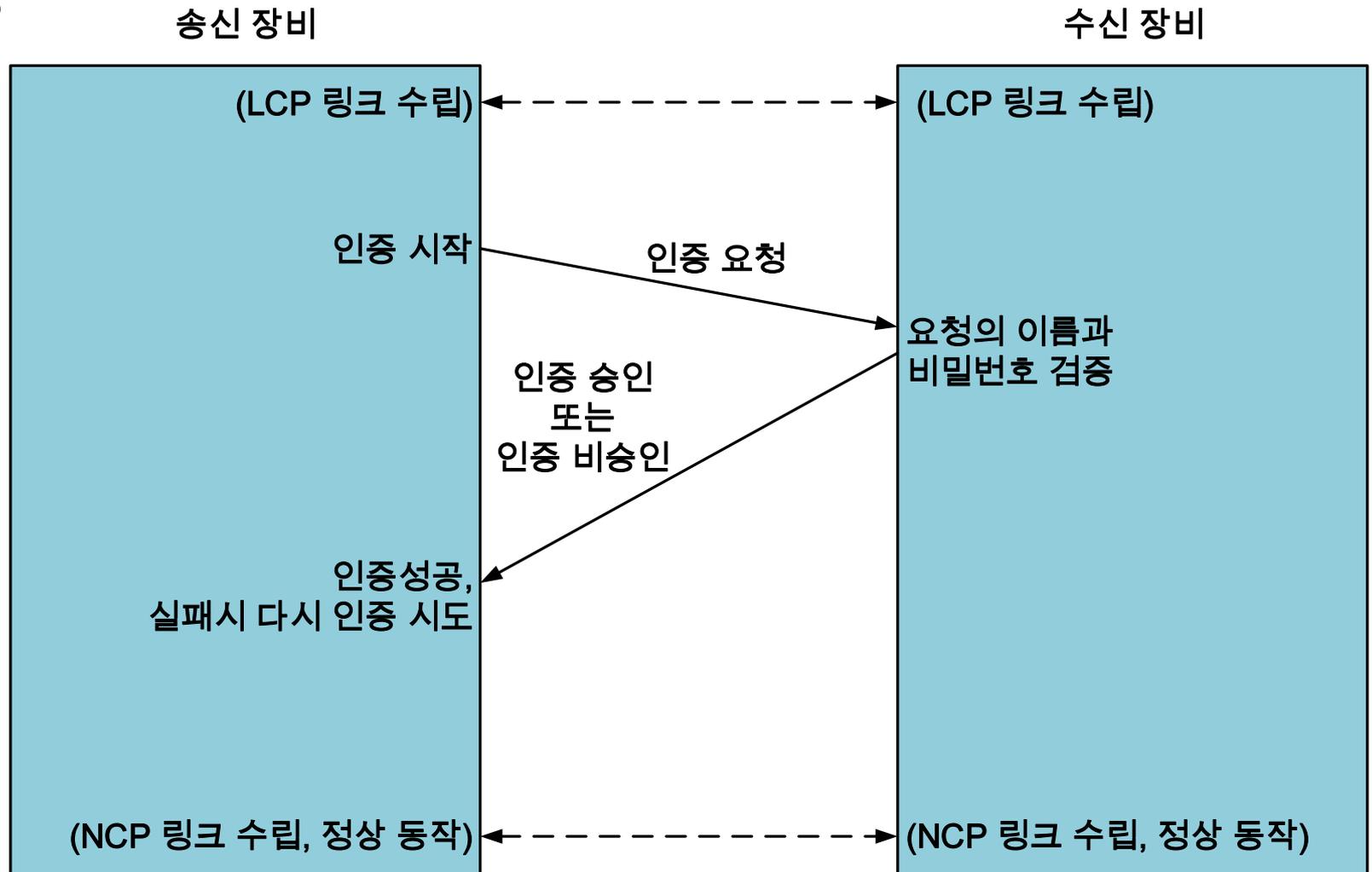
PPP 인증 프로토콜

- PPP에서 장비 간 인증 서비스를 제공하는 프로토콜
- PAP (Password Authentication Protocol)
 - 동작 방식
 - 인증 요청
 - 송신 장비는 인증 요청메시지와 이름과 비밀번호를 전송
 - 인증 응답
 - 수신 장비는 인증 요청 메시지를 검토하여 인증 승인 여부 메시지 전송
 - ID는 사용자 이름, 암호는 이전에 송신장비에게 알려준 비밀 번호
 - LCP 과정에서 알려줌
 - 결점
 - 사용자 이름과 비밀번호를 평문 형태로 전송

PPP 인증 프로토콜

- PAP

- 인증 과정



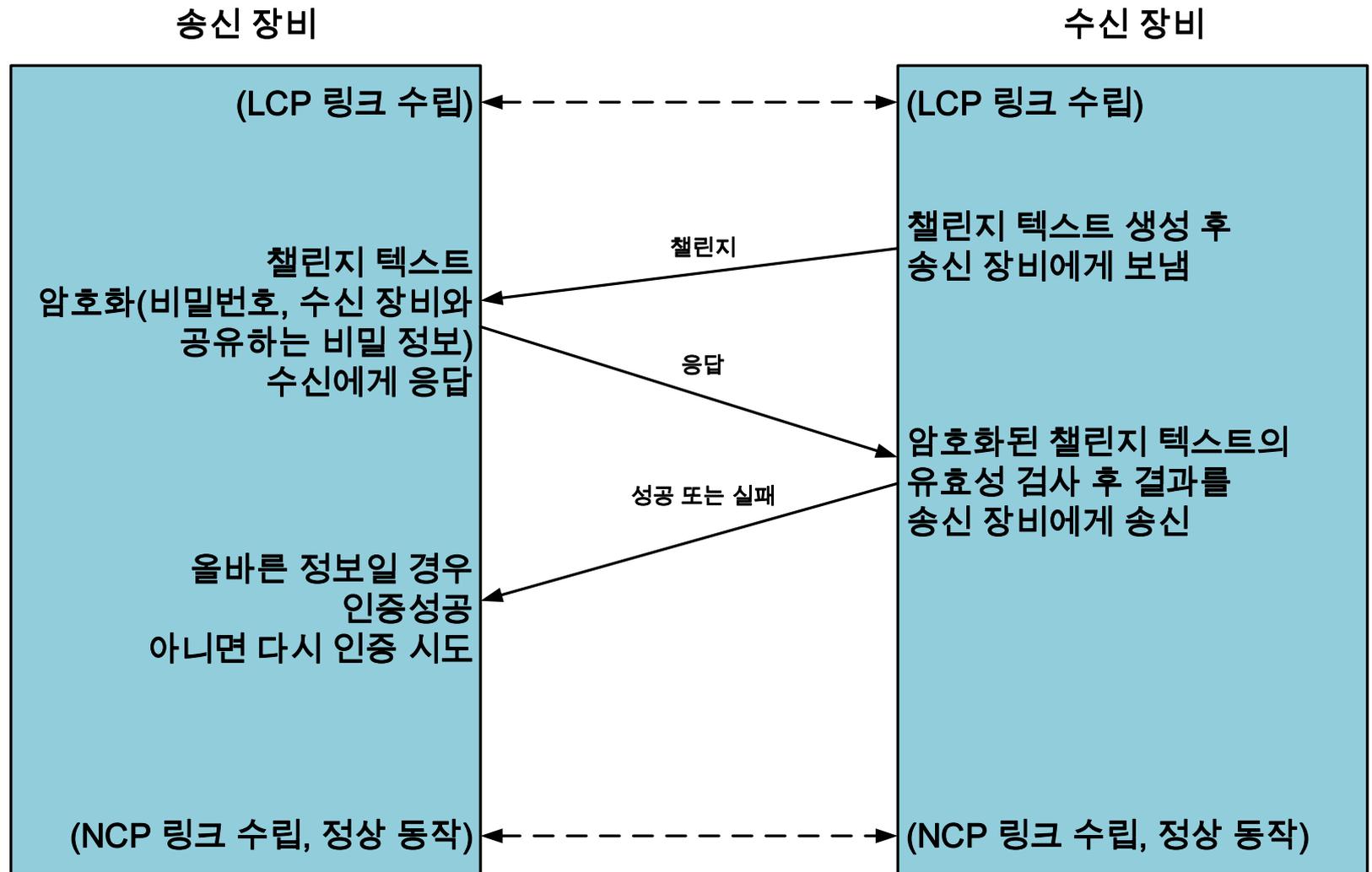
PPP 인증 프로토콜

- PPP에서 장비 간 인증 서비스를 제공하는 프로토콜
- CHAP (Challenge Handshake Authentication Protocol)
 - 동작 방식
 - 챌린지
 - 유효성 감사를 위한 메시지
 - 수신 장비는 챌린지 텍스트를 생성하여 송신 장비에게 전송
 - 양쪽 장비는 동일한 챌린지 텍스트를 가짐
 - 챌린지 메시지는 매번 바뀜(재전송 공격 방지)
 - 응답
 - 송신 장비는 비밀번호를 이용하여 챌린지 텍스트를 암호화
 - 암호화한 챌린지 텍스트를 수신 장비에게 전송
 - 인증 성공/실패
 - 수신 장비는 공유된 송신장비 비밀번호로 챌린지 텍스트를 암호화
 - 송신 장비가 전송한 암호화된 챌린지 텍스트와 비교 후 인증 성공 여부 메시지 전송

PPP 인증 프로토콜

- CHAP

- 인증과정



목 차

- 2 - 1부 TCP/IP 네트워크 인터페이스 계층 프로토콜
 - SLIP와 PPP 개요
 - PPP 핵심 프로토콜
 - PPP 인증 프로토콜
 - PPP 기능 프로토콜
 - PPP 프로토콜 프레임 포맷
- 2 - 2부 네트워크 인터넷 계층 연결 프로토콜
 - 주소 결정 프로토콜
 - 역순 주소 결정 프로토콜

PPP 기능 프로토콜

- LQM (Link Quality Monitoring)
 - PPP에서의 장비들이 링크의 상태를 분석 할 수 있도록 하는 기능
- LQR (Link Quality Reporting)
 - 상대방 장비에게 현재 링크 정보를 주기적으로 요청하는 것
 - 링크 정보: 송·수신한 프레임의 수, 발생한 에러의 수 등
- LQR 수립
 - 링크 수립 단계에서 인자 협상 과정의 일부로 수행됨
 - 설정 요청 프레임에 LQR 설정을 포함시켜 LQM 요청
 - 통계정보 주기 지정
 - 링크에 대한 정보를 받을 수 있는 시간

PPP 기능 프로토콜

- LQR

- LQR 활성화

- 링크 사용과 관련된 통계 정보를 담고 있는 카운터 생성 후 송/수신
 - 송·수신한 프레임의 수
 - 송·수신한 프레임의 바이트 수
 - 발생한 에러의 수
 - 버린 프레임의 수
 - 생성된 링크 품질 보고서 수

PPP 기능 프로토콜

- LQR

- LQR 사용

- 품질 보고서에 있는 통계 정보에 근거하여 장비는 링크 품질에 대한 결론을 내리고 어떤 행동을 취할지 결정
 - e.g.,
 - 에러의 절대값이 특정 임계치를 넘는 경우
 - 링크를 닫음
 - 버린 프레임의 비율이 증가한 경우
 - 프레임 설정 변경
 - 일부 장비는 정보를 로그에 저장하고 아무런 조치를 취하지 않음

PPP 기능 프로토콜

- CCP (Compression Control Protocol)
- PPP 데이터프레임을 압축하여 링크의 속도를 향상시키는 프로토콜
- CCP 운영
 - 링크 설정
 - 압축 설정은 인터넷 계층에서 수행
 - 인터넷 계층 프로토콜의 설정이 CCP일 때 사용
 - 링크 유지
 - 코드 거부
 - 유효하지 않은 코드 값이 있을 경우 코드 거부 메시지 전송
 - 리셋 요청/승인
 - 압축 해제 과정에서 오류가 발생할 경우 리셋 요청
 - 링크 종료
 - CCP 링크 종료 요청/승인 메시지를 통해 종료

PPP 기능 프로토콜

- CCP
 - CCP 설정
 - 두 장비가 사용할 압축 알고리즘을 협상
 - 압축 알고리즘 운영
 - 협상한 압축 알고리즘을 이용하여 데이터 전송 전 압축
 - 프레임이 압축됐다는 것을 나타내기 위해 PPP 프로토콜 필드에 특수 값 삽입 0x00FD
 - 압축된 경우 삽입
 - 다중링크에서 독립적으로 압축된 경우 0x00FB 삽입
 - LCP 프레임, 기타 프로토콜 제어에 쓰이는 프레임은 압축 불가능

PPP 기능 프로토콜

- ECP (Encryption Control Protocol)
 - PPP 데이터 프레임을 암호화와 복호화를 할 수 있도록 하는 프로토콜
 - ECP 운영
 - 링크 설정
 - 암호화 설정은 인터넷 계층에서 수행
 - 인터넷 계층 프로토콜의 설정이 ECP일 때 사용
 - 링크 유지
 - 코드 거부
 - 유효하지 않은 코드 값이 있을 경우 코드 거부 메시지 전송
 - 리셋 요청/승인
 - 암호화 과정에서 오류가 발생할 경우 리셋 요청
 - 링크 종료
 - ECP 링크 종료 요청/승인 메시지를 통해 종료

PPP 기능 프로토콜

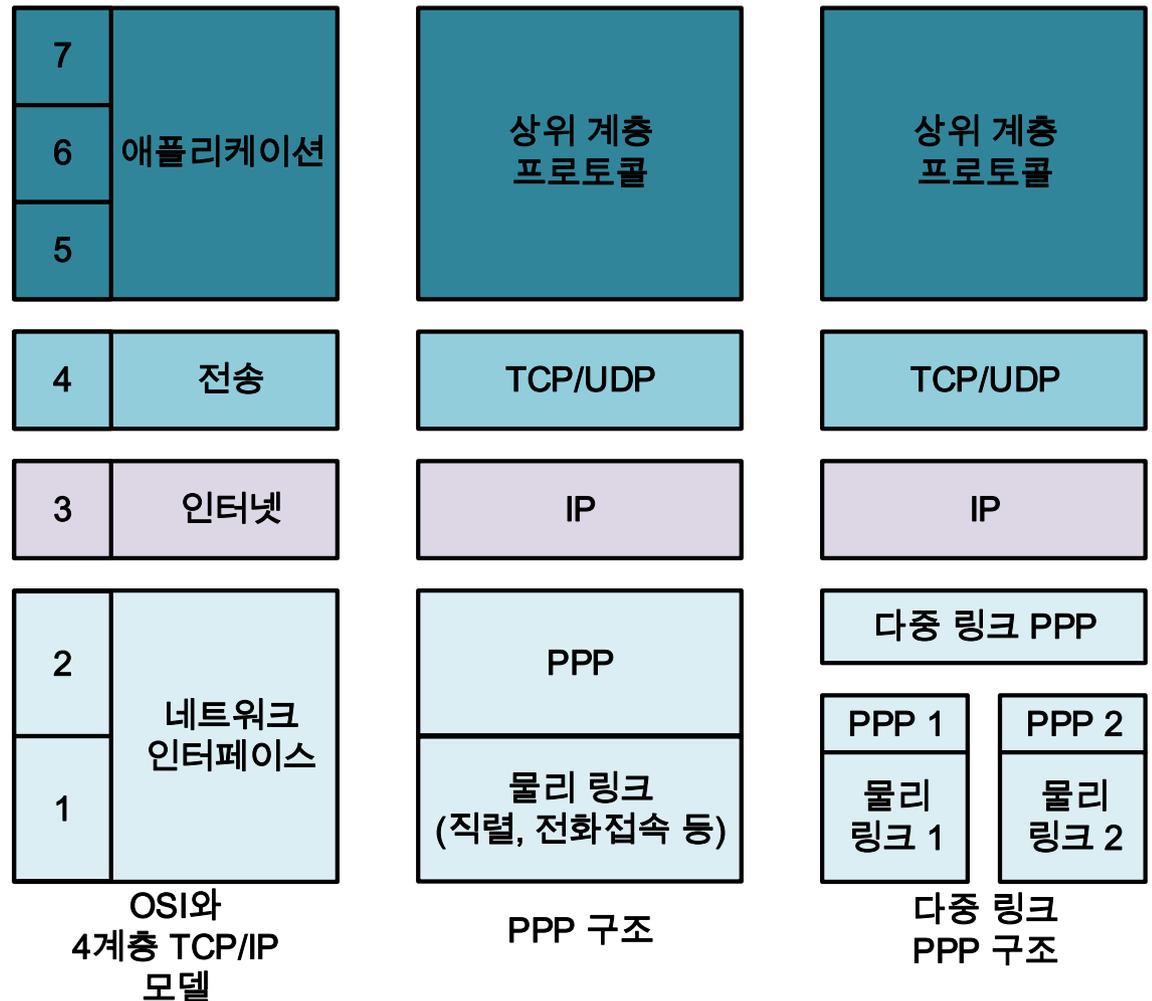
- ECP
 - ECP 설정
 - 두 장비가 사용할 암호화 알고리즘을 협상
 - 암호화 알고리즘 운영
 - 협상한 암호화 알고리즘을 이용하여 데이터 전송 전 암호화
 - 프레임이 암호화됐다는 것을 나타내기 위해 PPP 프로토콜 필드에 특수 값 삽입
 - 암호화된 경우 0x0053 삽입
 - 다중링크에서 독립적으로 암호화된 경우 0x0055 삽입
 - LCP 프레임, 기타 프로토콜의 제어에 쓰이는 프레임 암호화 가능

PPP 기능 프로토콜

- MP (Multilink Protocol)

- 전체 PPP 프레임을 단편화하여 서로 다른 물리 링크로 전송하는 프로토콜

- 분할된 PPP 링크를 하나의 링크로 사용



PPP 기능 프로토콜

- MP

- MP연결 수립과 설정

- LCP 링크 설정 과정 중 활성화됨

- 활성화를 위한 설정 옵션

- 다중링크 최대 수신 재구성 유닛 (Multilink Maximum Received Reconstructed Unit)
 - MP에서 지원하는 최대 PPP 프레임 크기 값 설정
- 다중링크 짧은 순서 번호 헤더 포맷 (Multilink Short Sequence Number Header Format)
 - MP 프레임에서 짧은 순서 번호 필드를 사용하는 것을 협상
 - 4비트 플래그와 12비트 순서번호 사용
- 종단 식별자 (Endpoint Discriminator)
 - 각 링크가 어떤 장비로 연결되는지를 파악하는 데 쓰임

PPP 기능 프로토콜

- MP

- MP운영

- 송신

- 인터넷 계층 프로토콜로부터 받은 데이터그램을 일반 PPP 프레임의 수정된 버전으로 캡슐화
 - 플래그, 단편화 시작, 단편화 끝, 순서 번호 프레임 추가
- 캡슐화된 프레임을 단편화하여 여러 링크로 분배
 - 크기가 작은 프레임, 링크 설정에 쓰이는 제어 프레임은 단편화되지 않음
- 각 링크로 분배된 프레임은 캡슐화되어 물리 계층으로 전송

- 수신

- 수신된 프레임 조각들을 재조합하여 원본 PPP 프레임으로 구성

PPP 기능 프로토콜

- MP 대역폭 할당 제어 프로토콜
 - 대역폭 할당 제어 프로토콜 (BACP, Bandwidth Allocation Control Protocol)
 - 장비들이 BACP를 사용할 수 있도록 설정 하는 프로토콜
 - 대역폭 할당 프로토콜 (BAP, Bandwidth Allocation Protocol)
 - MP로 동작하는 장비들의 특정 링크를 묶음에 추가하거나 제거하는 프로토콜
- BACP와 BAP는 MP의 동작을 동적으로 제어하는 데 사용

PPP 기능 프로토콜

- BAP

- BAP의 운영

- 콜 요청과 응답

- 새로운 물리 계층 링크를 추가하고 싶을 때 송신장비는 상대방 장비에게 콜 요청 (Call-Request) 프레임 전송
 - 상대방 장비는 콜 응답 (Call-Response)으로 응답

- 콜 백 요청과 응답

- 수신장비가 기존 링크와는 다른 링크를 추가하라고 요구할 때 콜 백 요청 (Callback-Request) 프레임 전송
 - 송신 장비는 콜 백 응답 (Callback-Response)으로 응답

PPP 기능 프로토콜

- BAP

- BAP의 운영

- 콜 상태 표시와 응답

- 송신장비는 링크의 상태를 콜 상태표시(CallStatus-Indication)프레임으로 상대방 장비에게 전송
 - 상대방 장비는 콜 상태 응답 (Call-Status-Response)으로 응답

- 링크 제거 요청과 응답

- 링크를 제거하기 위한 요청과 응답

목 차

- 2 – 1부 TCP/IP 네트워크 인터페이스 계층 프로토콜
 - SLIP와 PPP 개요
 - PPP 핵심 프로토콜
 - PPP 인증 프로토콜
 - PPP 기능 프로토콜
 - PPP 프로토콜 프레임 포맷
- 2 – 2부 네트워크 인터넷 계층 연결 프로토콜
 - 주소 결정 프로토콜
 - 역순 주소 결정 프로토콜

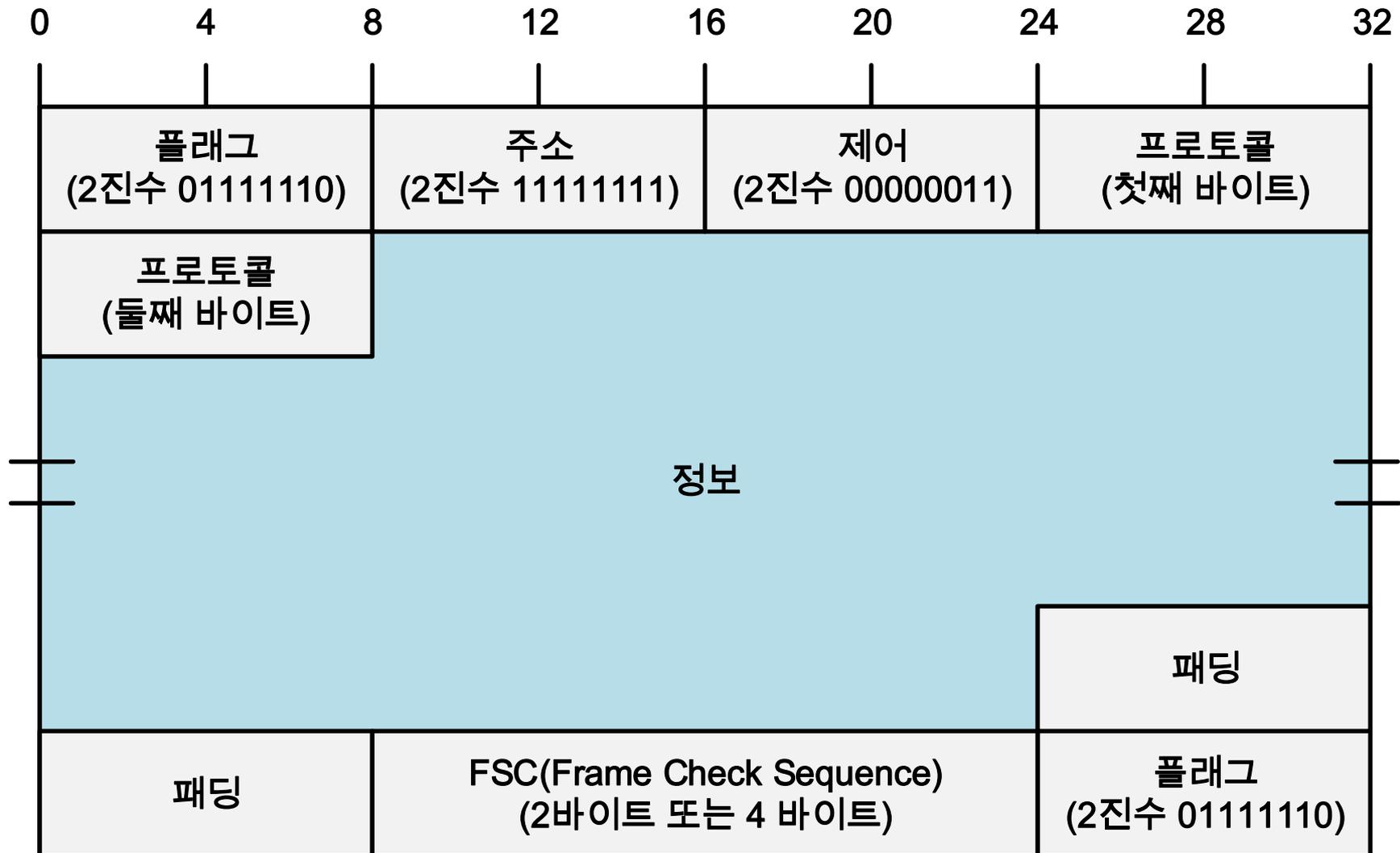
PPP 프로토콜 프레임 포맷

• PPP 일반 프레임 포맷

필드 이름	크기(바이트)	설명
플래그	1	PPP 프레임의 시작과 끝을 나타냄
주소	1	PPP는 두 장비 간 직접 연결을 다루기 때문에 이 필드는 항상 브로드캐스트 주소를 가리킴
제어	1	PPP에서는 2진수 00000011로 설정되어 있음
프로토콜	2	캡슐화된 패킷의 프로토콜을 식별 (LCP, NCP 등)
정보	가변적	프레임 종류에 따라, 데이터 또는 제어 정보를 포함한 0개 이상의 바이트로 된 페이로드
패딩	가변적	PPP 프레임의 크기를 맞추기 위한 필드
프레임 검사 순서번호 (FCS, Frame Check Sequence)	2(또는 4)	CRC 에러검출 기법에 의해 생성된 비트배열

PPP 프로토콜 프레임 포맷

• PPP 일반 프레임 포맷



PPP 프로토콜 프레임 포맷

- PPP 일반 프레임 포맷

- 프로토콜 필드 범위

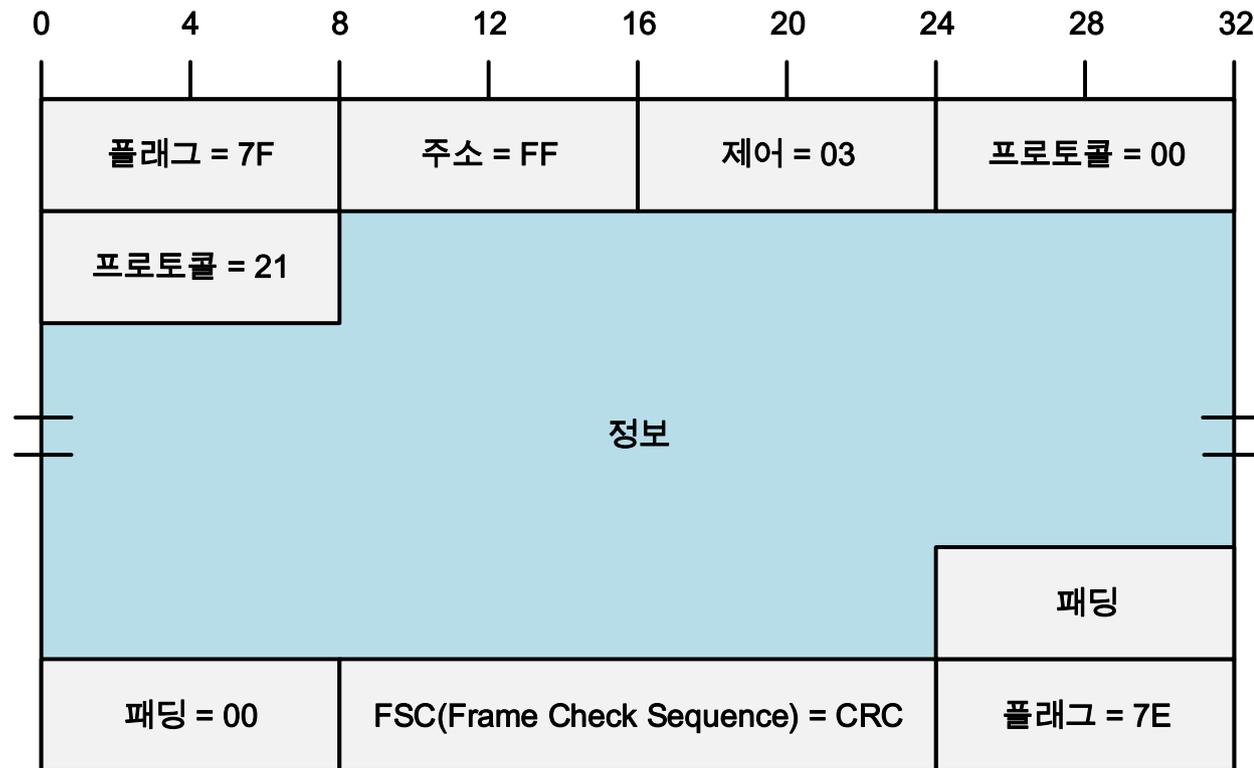
- 프레임 수신하는 장비를 위한 프레임 유형 식별자
- 필드 값의 첫 번째 바이트는 짝수, 두 번째 바이트는 홀수
- PPP 프로토콜 필드 범위 표

프로토콜 필드 범위(16진수)	설명
0000-3FFF	관련 NCP가 존재하는 캡슐화된 인터넷 계층 패킷, 압축이나 암호화된 패킷의 프레임을 나타내는 데 쓰이는 값 포함
4000-7FFF	잘 쓰이지 않는 프로토콜을 포함한 패킷, 관련 NCP가 존재하지 않는 프로토콜
8000-BFFF	0000-3FFF 범위에 있는 3계층 프로토콜 값에 대응하는 NCP 제어 프레임
C000-FFFF	LCP와 LCP 지원 프로토콜이 사용하는 제어 프레임

PPP 프로토콜 프레임 포맷

• PPP 일반 프레임 포맷 예제

- 플래그 (7E)
= PPP 시작
- 주소 (FF)
= 브로드캐스트 의미
- 제어 (03)
= PPP에서 사용
되는 고정된 설정
- 프로토콜 (00, 21)
= 인터넷 프로토콜
(IPv4)
- 플래그 (7E)
= PPP 끝



PPP 프로토콜 프레임 포맷

- PPP 일반 프레임 포맷

- PPP 필드 압축 방법

- 주소와 제어 필드 압축 (ACFC, Address and Control Field Compression)

- 활성화 시 PPP 프레임에 주소와 제어 필드를 사용하지 않음

- 프로토콜 필드 압축 (PFC, Protocol Field Compression)

- 압축할 경우 2바이트가 아닌 1바이트의 프로토콜 필드 값을 주고 받음

- 프로토콜 필드의 첫 바이트가 0일 경우 그 값을 보내지 않음

- 프로토콜 필드의 첫 바이트가 짝수/홀수인지 검사해 압축 여부를 판단

- 홀수라면 압축된 것을 의미

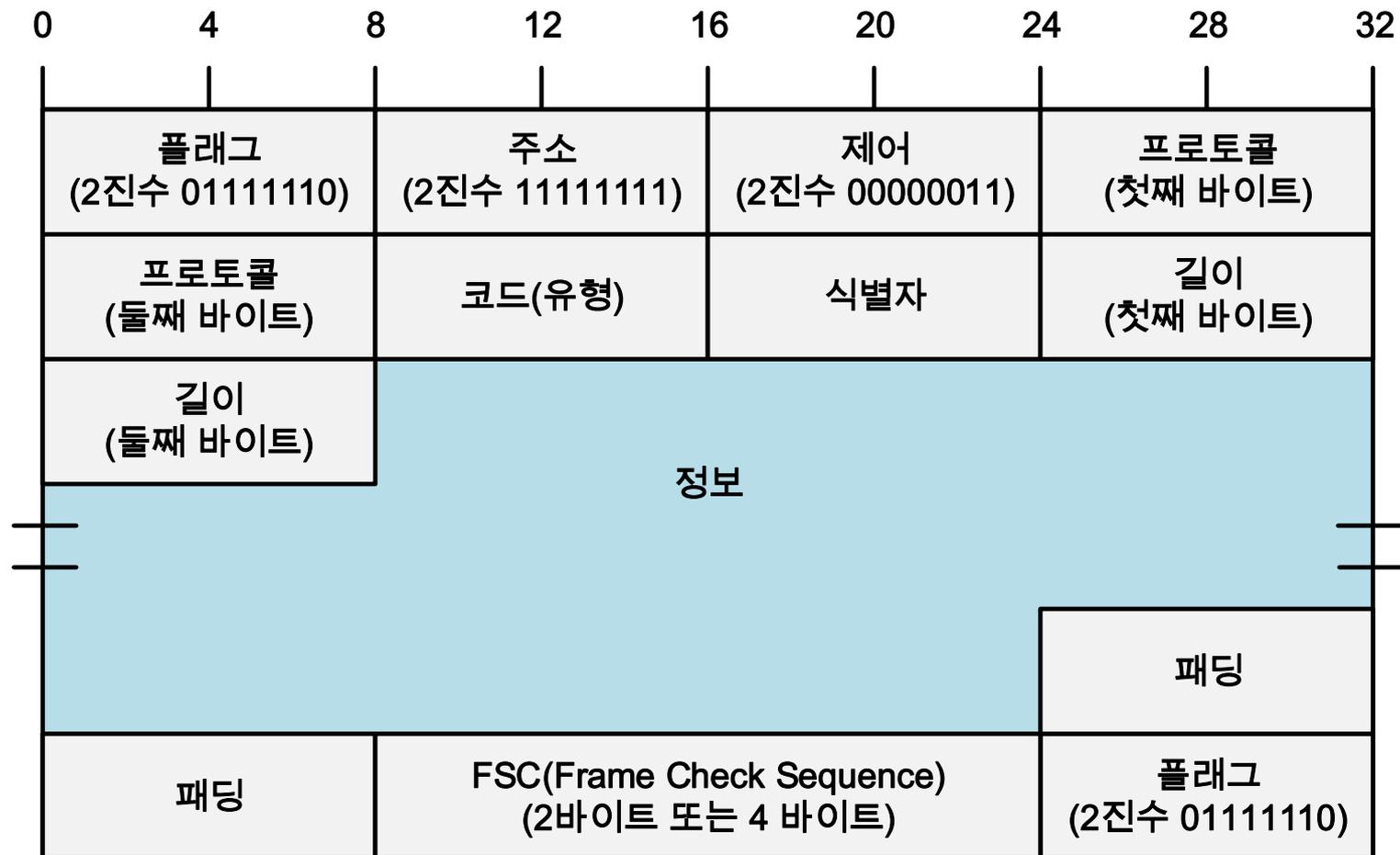
PPP 프로토콜 프레임 포맷

- PPP 일반 제어 프로토콜 프레임 포맷
 - PPP 제어 메시지 포맷의 필드는 PPP 일반 프레임 포맷의 정보 필드 안에 포함됨
- PPP 제어 메시지 포맷 표

필드 이름	크기(바이트)	설명
코드(유형)	1	어떤 유형의 제어 메시지가 있는지 나타냄 (링크 설정, 링크 유지, 링크 종료 등)
식별자	1	요청과 응답을 대응시키는 데 쓰임
길이	2	제어 프레임의 전체 필드 길이를 나타냄

PPP 프로토콜 프레임 포맷

- PPP 일반 제어 프로토콜 프레임 포맷
- PPP 제어 메시지 포맷



PPP 프로토콜 프레임 포맷

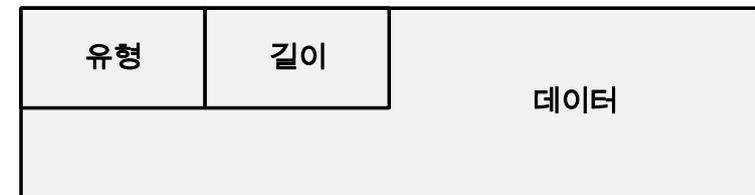
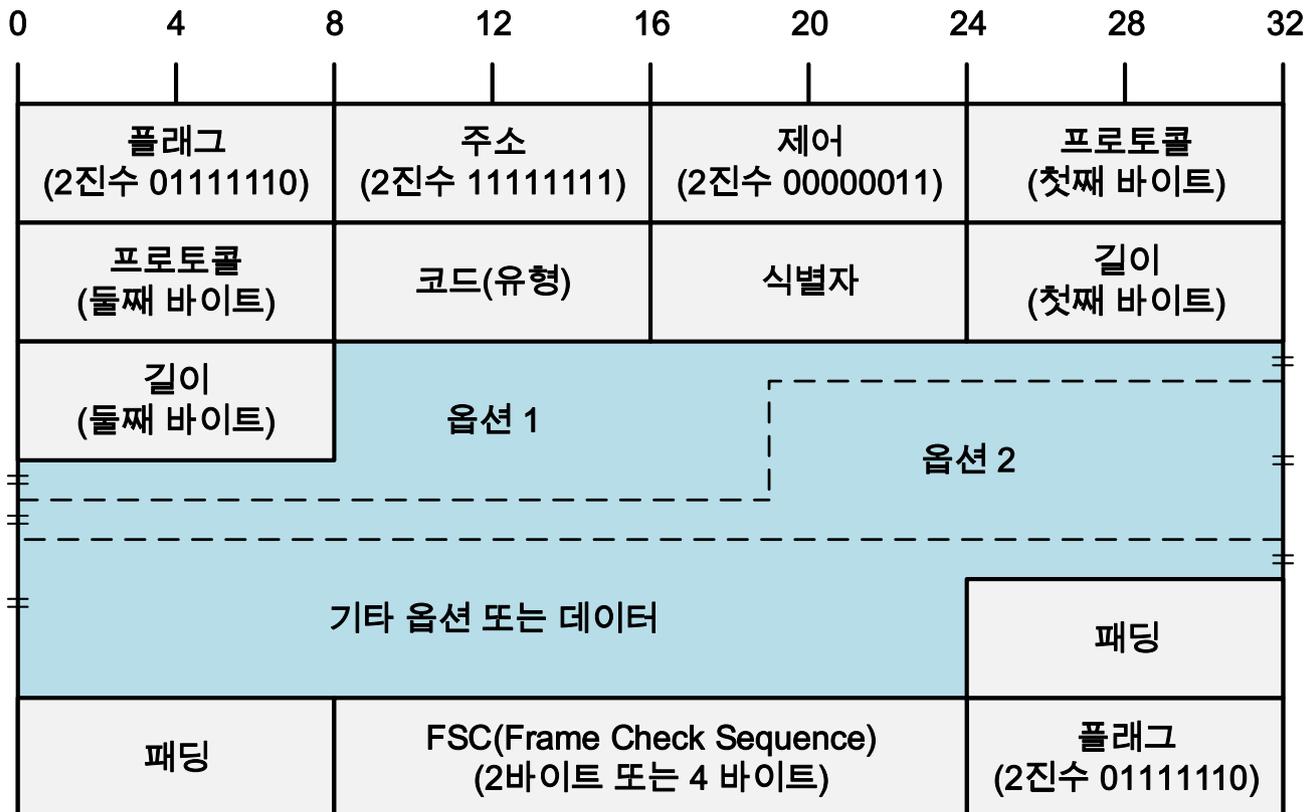
- PPP 일반 제어 프로토콜 프레임 포맷

- PPP 제어 메시지와 코드 값
 - 코드 필드는 특정 제어 프로토콜 내에서의 제어 프레임 유형을 나타냄

코드 값	제어 메시지	LCP	NCP	CCP와 ECP
1	설정 요청	V	V	V
2	설정 승인	V	V	V
3	설정 비승인	V	V	V
4	설정 거부	V	V	V
5	종료 요청	V	V	V
6	종료 승인	V	V	V
7	코드 거부	V	V	V
8	프로토콜 거부	V		
9	에코 요청	V		
10	에코 응답	V		
11	버림 요청	V		
12	식별	V		
13	남은 시간	V		
14	리셋 요청			V
15	리셋 승인			V

PPP 프로토콜 프레임 포맷

- PPP 일반 제어 프로토콜 프레임 포맷과 옵션 포맷
 - PPP 제어 메시지 옵션 포맷
 - 옵션은 유형, 길이, 데이터 3가지 요소로 구성



PPP 프로토콜 프레임 포맷

• PAP 프레임 포맷

• PAP 인증 요청 프레임 포맷

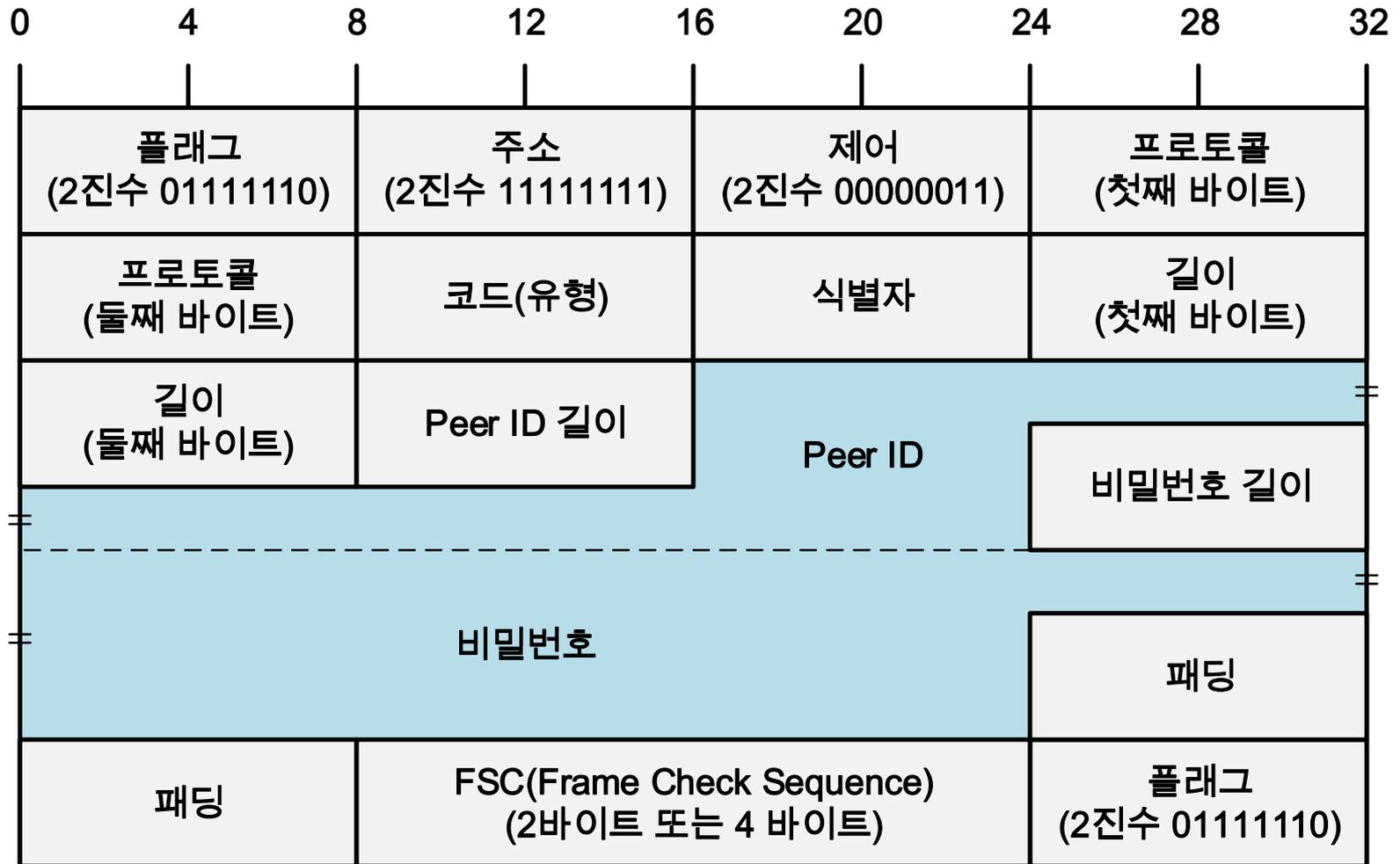
프레임 유형	코드 필드	식별자 필드	길이 필드	데이터 필드
인증 요청	1	각 프레임에 생성된 값	6 + Peer ID 길이 + 비밀번호	인증을 위한 사용자 이름과 비밀번호
인증 승인	2	인증 요청 복사 값	5 + 포함된 메시지 길이	메시지 하위 필드의 길이를 지정하는 Msg-Length 필드포함
인증 비승인	3			

• PAP 인증 요청 프레임 하위 필드

하위 필드 이름	크기(바이트)	설명
Peer ID 길이	1	Peer ID 필드의 길이
Peer ID	가변적	인증 대상이 되는 필드의 길이
비밀번호 길이	1	Password 필드의 길이
비밀 번호	가변적	인증할 이름에 대응되는 비밀번호

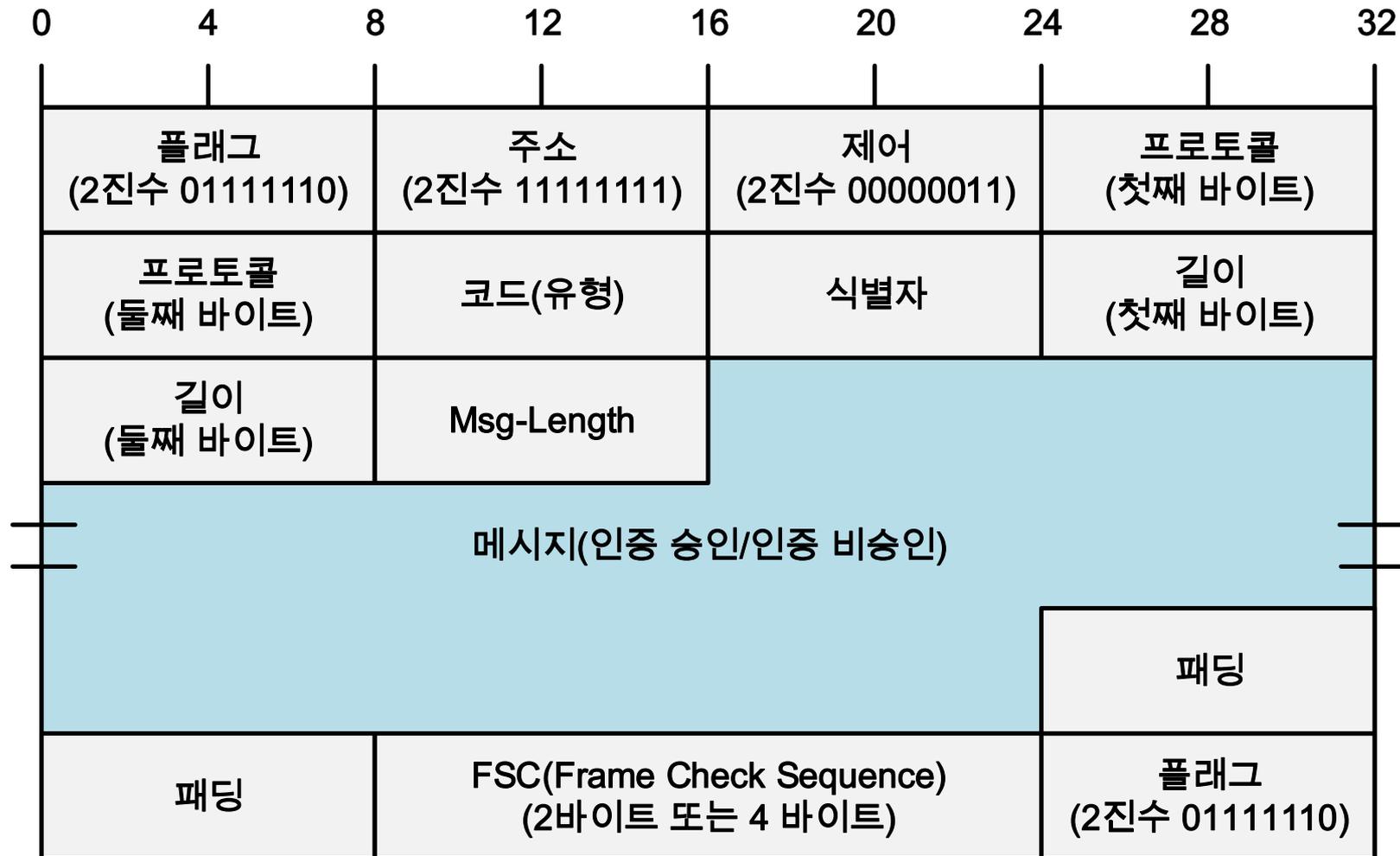
PPP 프로토콜 프레임 포맷

- PAP 제어 프레임 포맷
- PAP 인증 요청 프레임 포맷



PPP 프로토콜 프레임 포맷

- PAP 제어 프레임 포맷
- PAP 인증 승인 및 인증 비승인 프레임 포맷



PPP 프로토콜 프레임 포맷

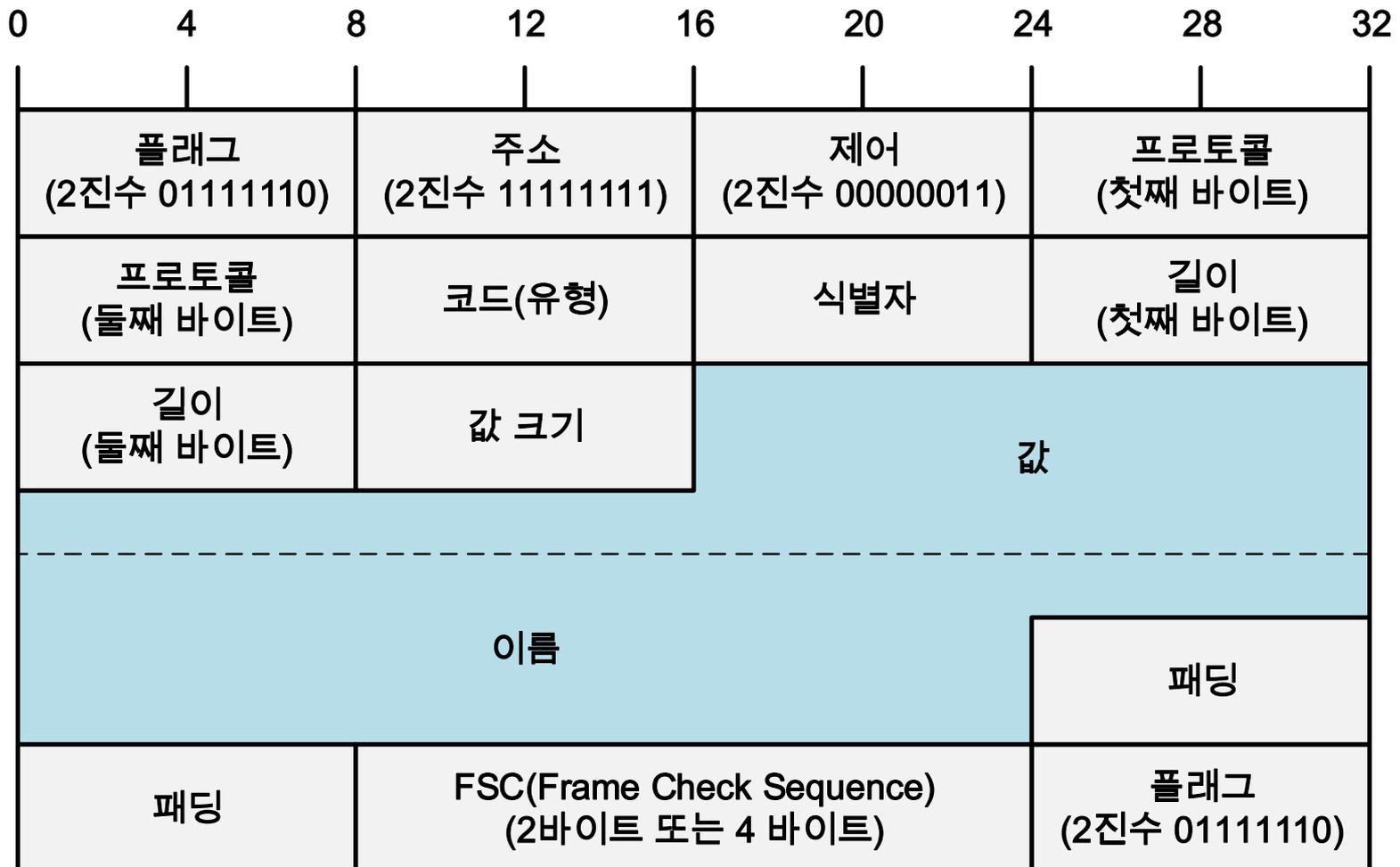
- CHAP 프레임 포맷
 - CHAP 챌리지와 응답 프레임 포맷

프레임 유형	코드 필드	식별자 필드	길이 필드	데이터 필드
챌리지	1	각 프레임별 새로 생성된 값	5 + 챌리지 문자열 길이 + Name 길이	챌리지 텍스트나 응답 텍스트, 그리고 시스템 식별자를 전달
응답	2	대응되는 챌리지 프레임의 식별자 필드에서 복사한 값	5 + Value 길이 + Name 길이	
성공	3	대응되는 응답 프레임의 식별자 필드에서 복사한 값	4(추가 데이터가 포함된 다면 그 이상)	인증이 성공 또는 실패 했는지 사용자에게 알리는 데 쓰임
실패	4			

PPP 프로토콜 프레임 포맷

- CHAP 프레임 포맷

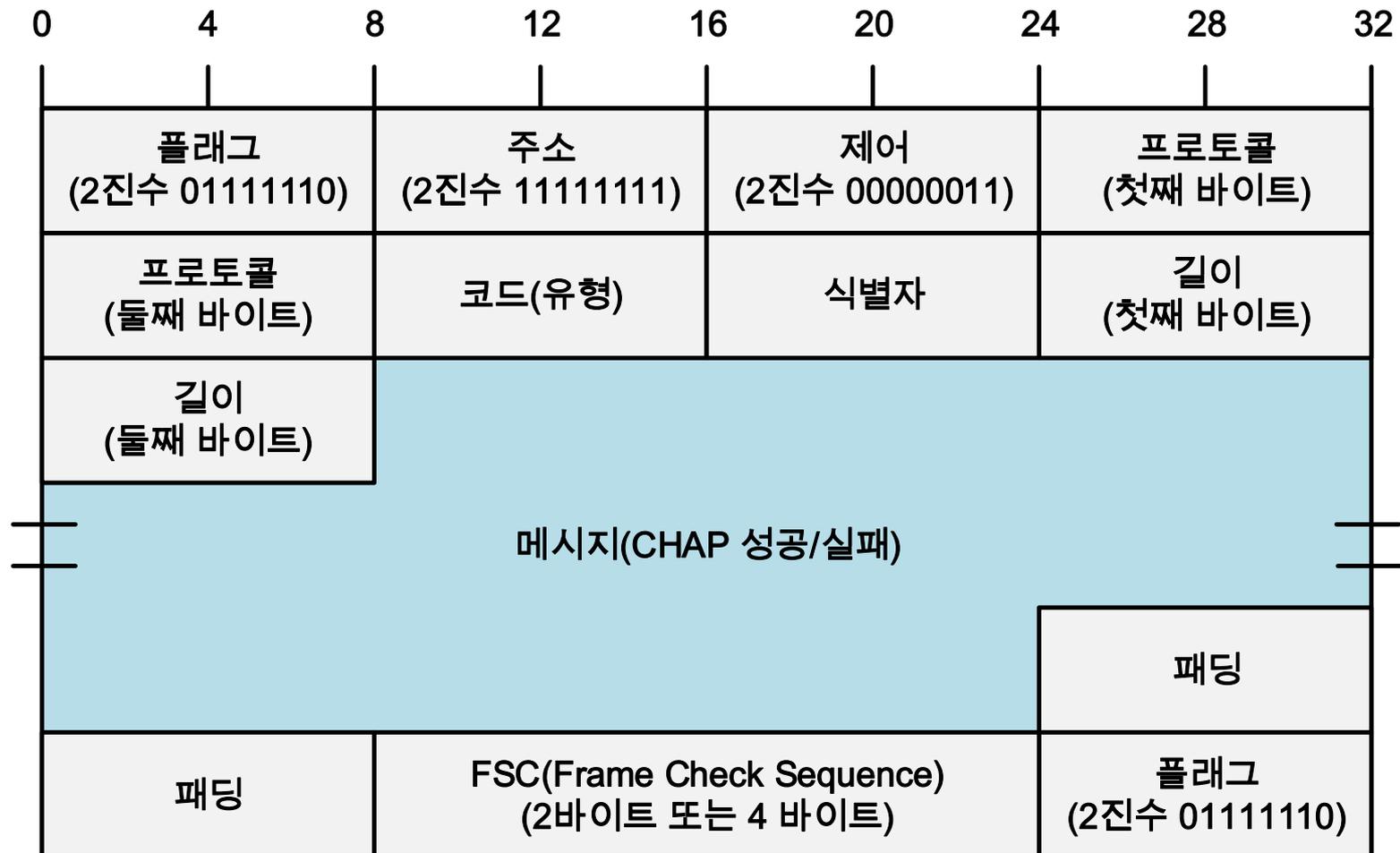
- CHAP 챌린지와 응답 프레임 포맷



PPP 프로토콜 프레임 포맷

- CHAP 프레임 포맷

- CHAP 성공과 실패 프레임 포맷



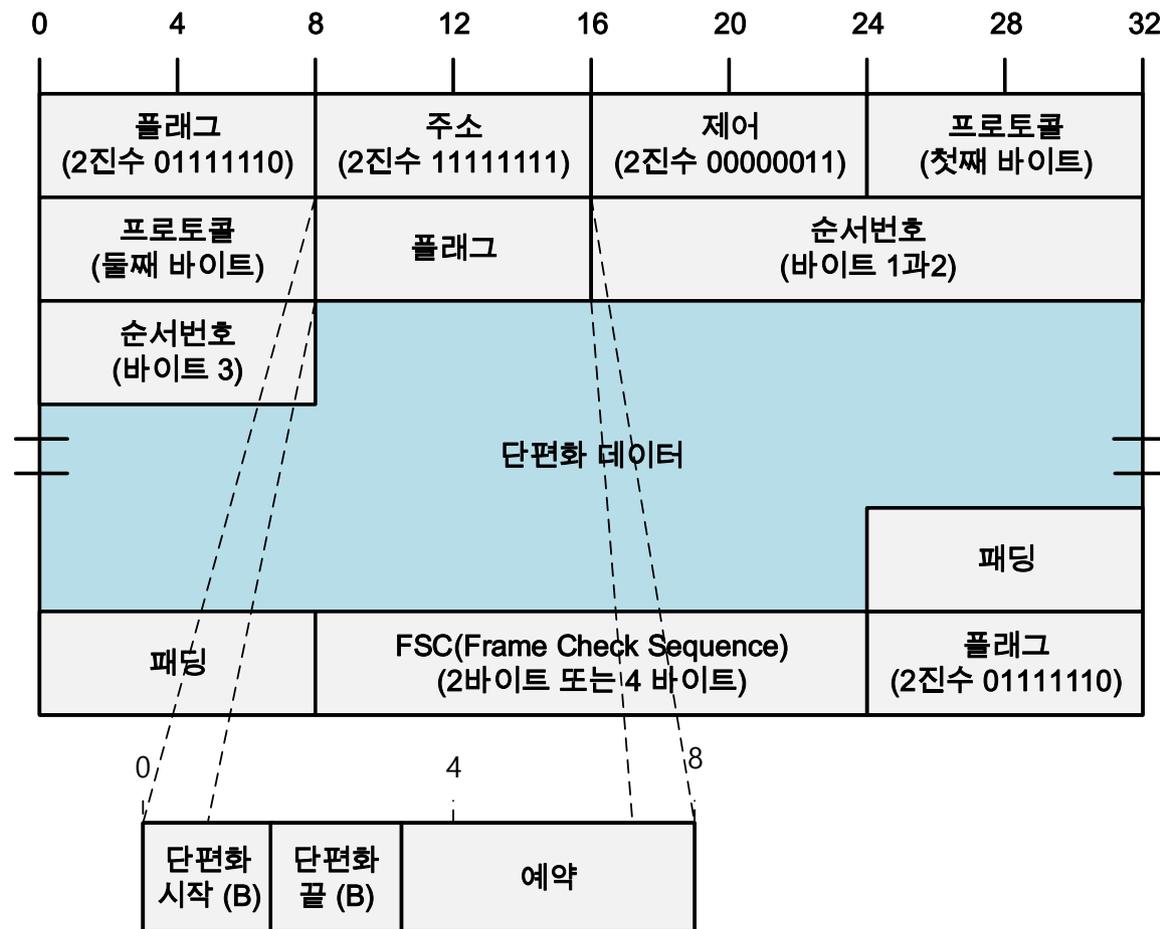
PPP 프로토콜 프레임 포맷

- MP 프레임 포맷
 - MP 단편화 프레임 포맷

필드 이름	크기(비트)	설명
B	1	단편화 조각의 시작을 나타내는 플래그
E	1	단편화 조각의 끝을 나타내는 플래그
예약	2 or 6	쓰이지 않음, 0으로 설정
순서 번호	12 or 6	재조합할 수 있도록 연속된 순서 번호를 부여 받음
단편화 데이터	가변적	원본 PPP 프레임에서 가져온 실제 단편화 데이터

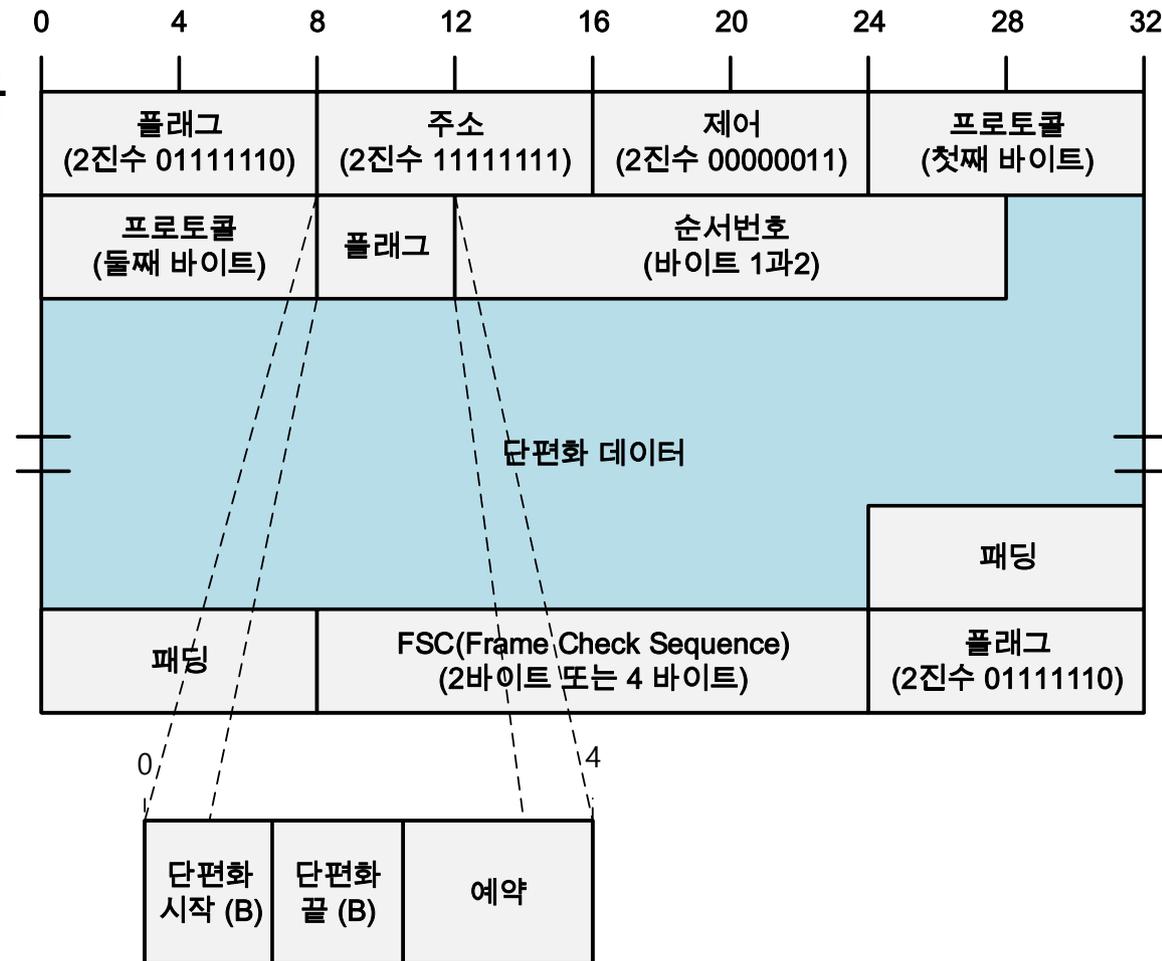
PPP 프로토콜 프레임 포맷

- MP 프레임 포맷
 - MP 단편화 프레임 포맷
 - 1바이트 플래그와 24비트 순서 번호 사용



PPP 프로토콜 프레임 포맷

- MP 프레임 포맷
 - MP 짧은 단편화 프레임 포맷
 - 4비트 플래그와 12비트 순서 번호 사용



목 차

- 2 – 1부 TCP/IP 네트워크 인터페이스 계층 프로토콜
 - SLIP과 PPP 개요
 - PPP 핵심 프로토콜
 - PPP 기능 프로토콜
 - PPP 프로토콜 프레임 포맷
- 2 – 2부 네트워크 인터넷 계층 연결 프로토콜
 - 주소 결정 프로토콜
 - 역순 주소 결정 프로토콜

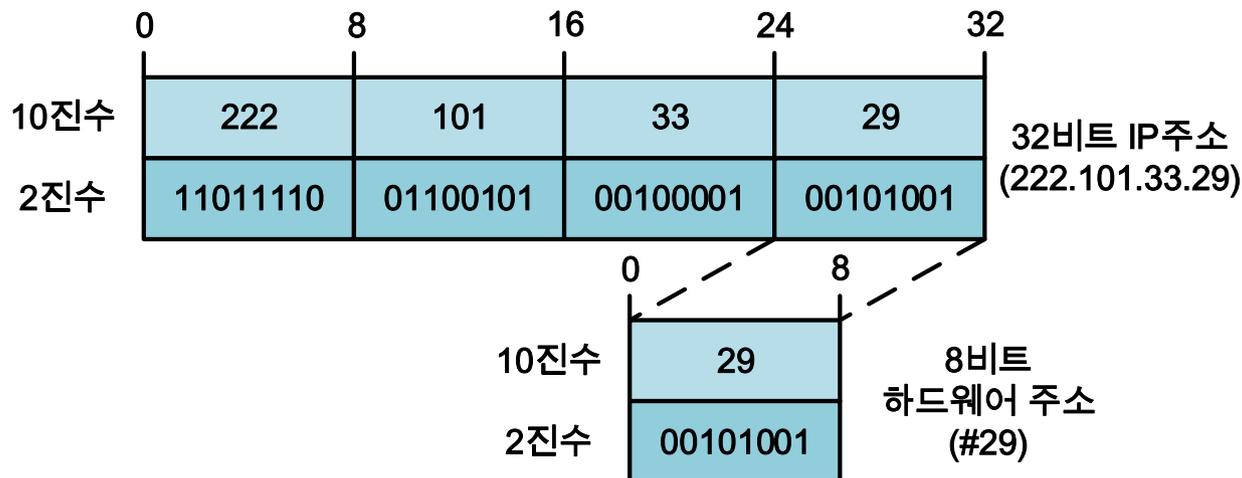
주소 결정 프로토콜

- 주소 결정

- 서버와 클라이언트가 통신 할 때 인터넷계층 주소를 물리 계층 주소로 변환하는 것
 - 논리적으로는 인터넷 계층 주소로 통신하지만 실제로 물리 계층 주소를 통해 물리적 통신이 필요

- 직접 매핑

- IP주소의 마지막 8비트에 MAC주소를 매핑하는 방법
 - 인터넷 계층 주소를 알면 물리 계층 주소를 알 수 있음



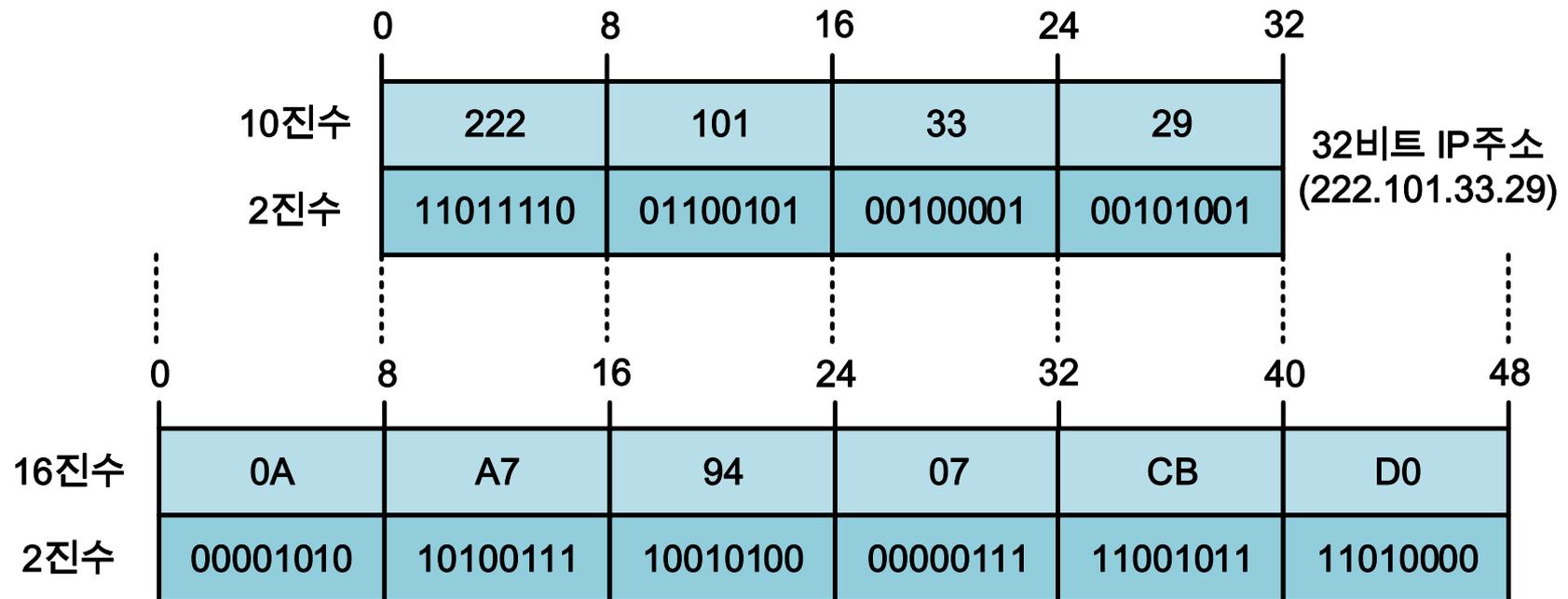
주소 결정 프로토콜

- 주소 결정

- 직접 매핑

- 문제점

- 물리 계층 주소가 인터넷 계층 주소보다 클 때는 직접 매핑 불가능



48비트 하드웨어 주소
(0A-A7-94-07-CB-D0)

주소 결정 프로토콜

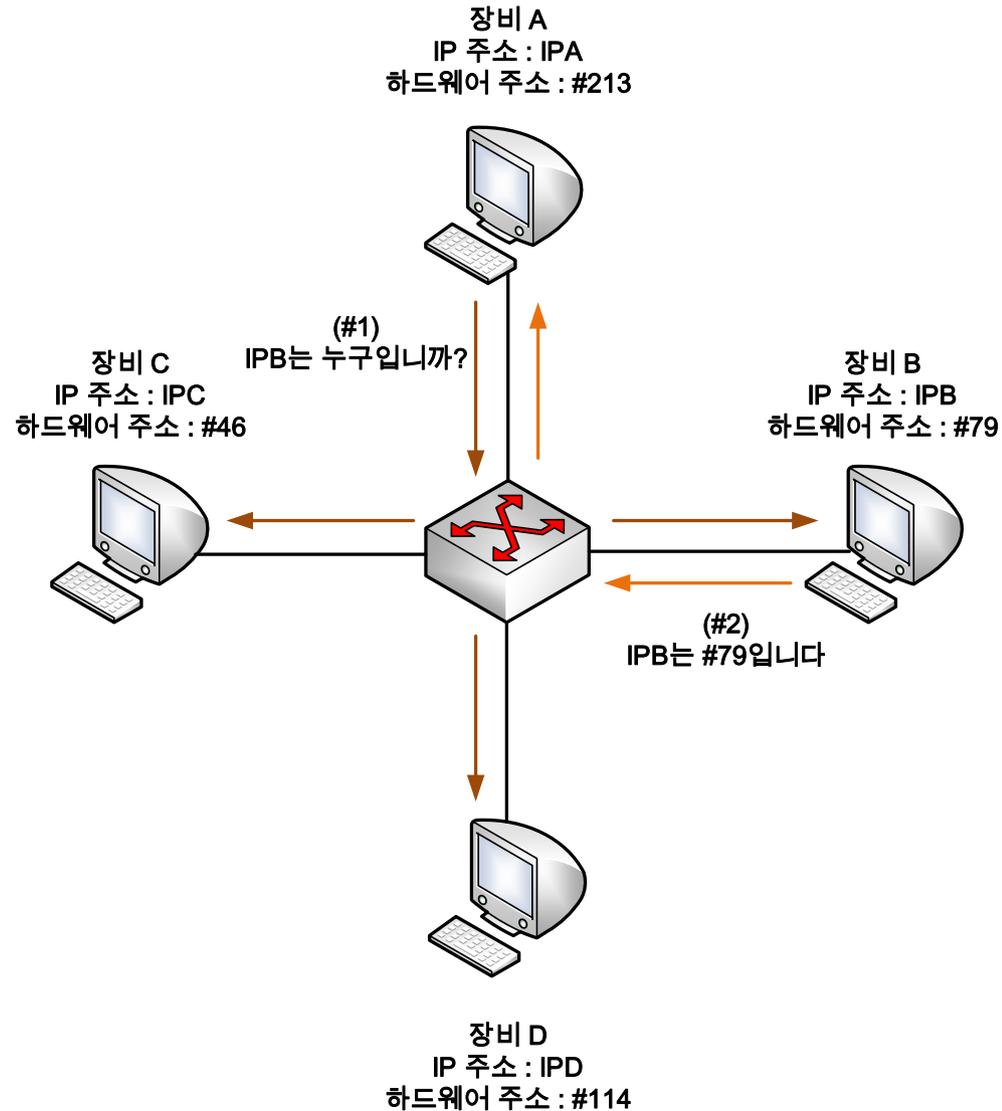
- 주소 결정

- 동적 주소 결정

- IP 주소를 알면 주소 유형이 다르더라도 브로드캐스트 요청으로 해당 물리 계층 주소를 찾아낼 수 있음

- 브로드캐스트 요청

- 요청 메시지와 하나의 유니캐스트 응답 메시지 교환으로 이루어짐



주소 결정 프로토콜

- 주소 결정

- 동적 주소 결정

- 문제점

- 모든 경로에서 데이터그램에 대해 확인하는 작업은 과부하를 발생 시킴
 - 프레임을 보낼때마다 주소 결정을 다시하면 프레임을 확인하는 작업에서 과부하 발생

- 문제점 개선 방법

- 캐싱

- 알아낸 하드웨어 주소를 다음에 또 사용할 수 있도록 캐시 테이블에 저장

- 교차 결정

- 장비 A가 장비 B의 주소를 파악할 때, 장비 B도 장비 A의 주소를 자신의 캐시에 저장

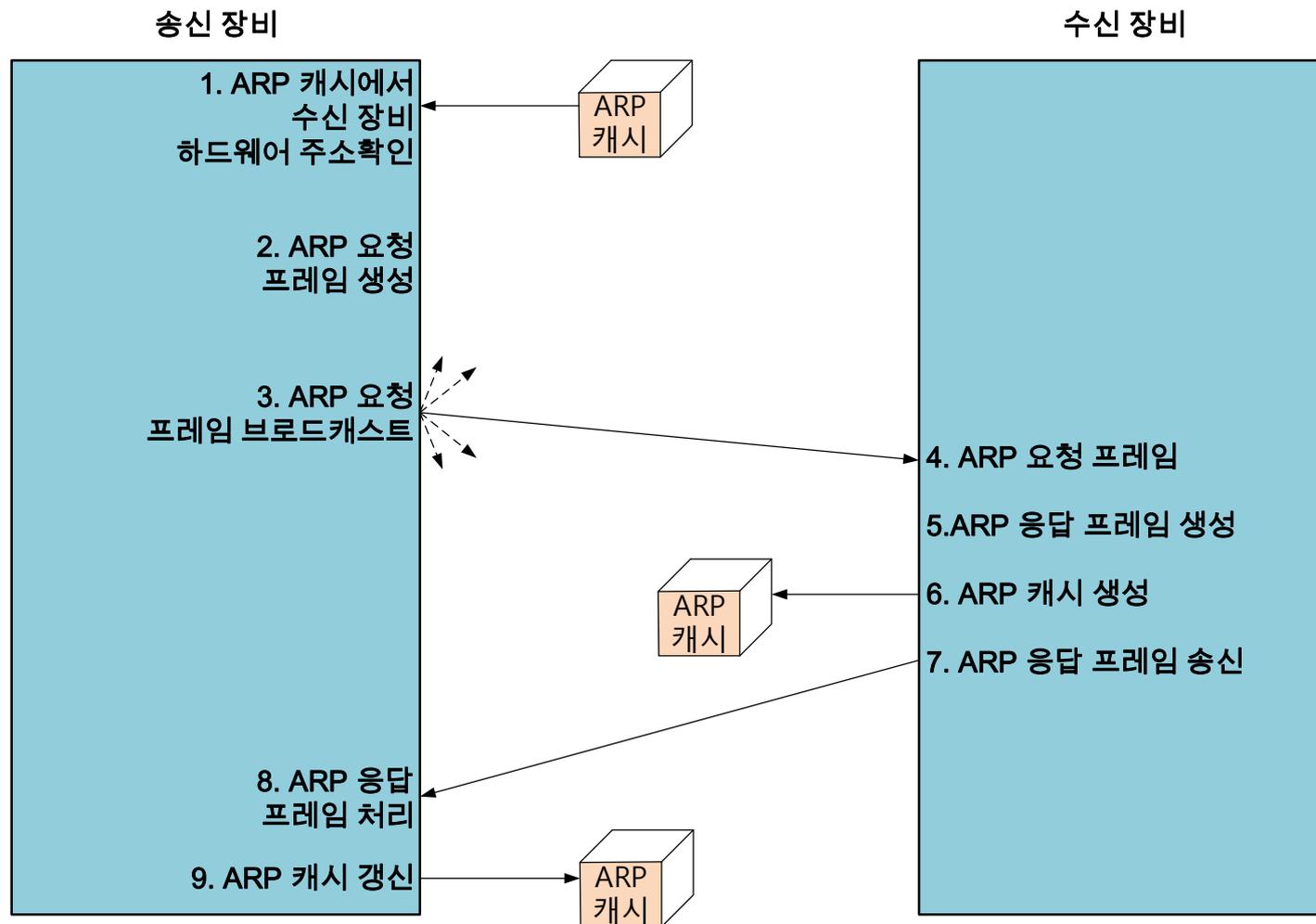
주소 결정 프로토콜

- ARP (Address Resolution Protocol)
 - IP 주소에 해당하는 물리 계층 주소를 파악하는 데 쓰이는 동적 결정 프로토콜
- ARP 기본 동작
 - 물리계층 주소를 얻고 싶은 장비의 IP 주소를 브로드캐스트 메시지로 전송
 - 해당 장비는 자신의 물리 계층 주소를 메시지 송신자에게 유니캐스트 방식으로 전송

주소 결정 프로토콜

• ARP

• ARP 트랜잭션 절차



주소 결정 프로토콜

• ARP

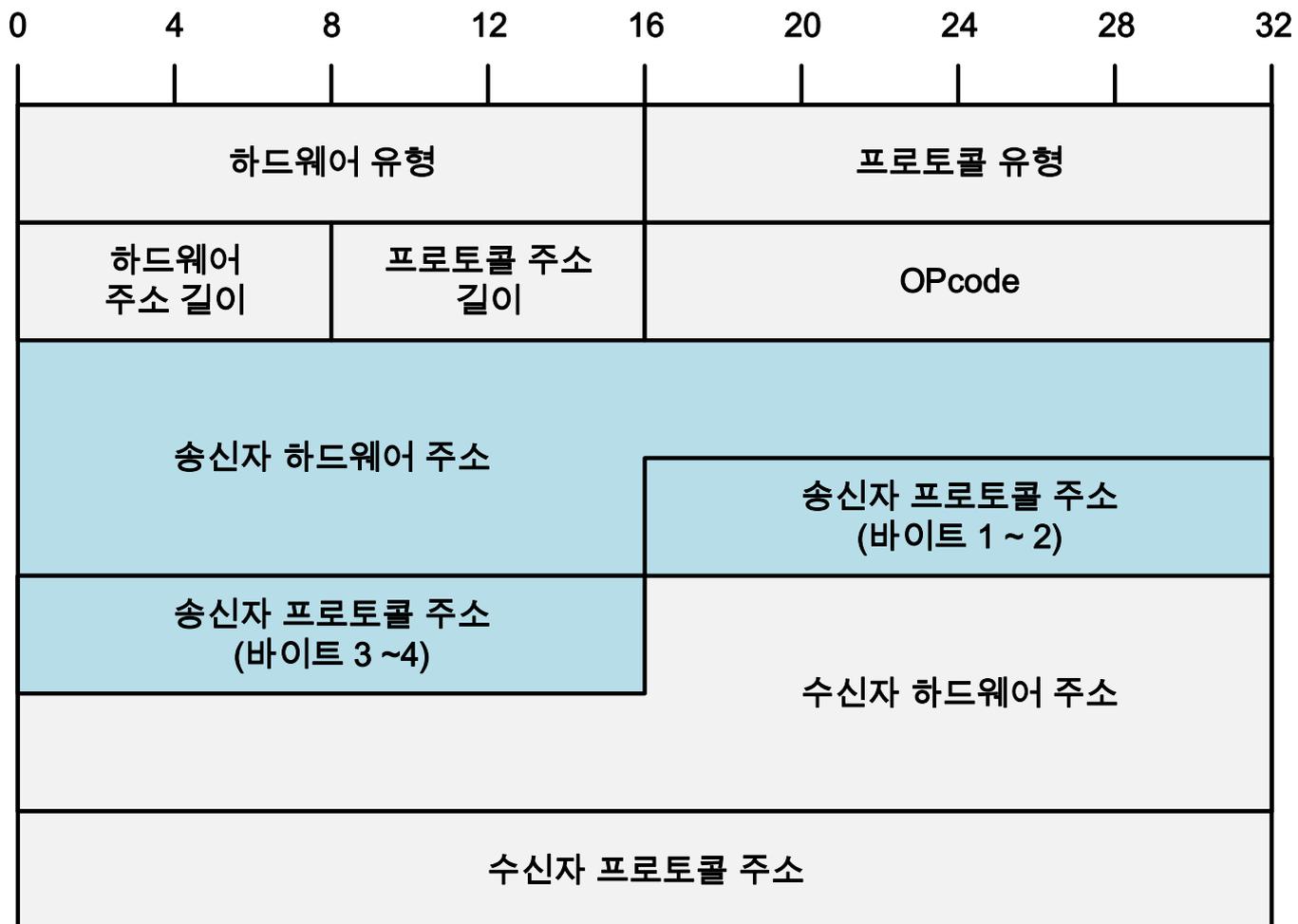
• ARP 메시지 포맷 표

필드 이름	크기(바이트)	설명
하드웨어 유형 (HRD, Hardware)	2	로컬 네트워크에서 사용하는 하드웨어의 유형 지정 (이더넷, 직렬회선 등)
프로토콜 유형 (PRO, Protocol)	2	메시지에서 사용하는 인터넷 계층 주소의 유형 지정
하드웨어 주소 길이 (HLN, Hardware Length)	1	메시지에 포함된 하드웨어 주소 길이를 바이트 단위로 지정
프로토콜 주소 길이 (PLN, Protocol Length)	1	메시지에 포함된 프로토콜 주소 길이를 바이트 단위로 지정
동작 코드 (OP, Opcode)	2	전송중인 ARP 메시지의 유형을 지정 (요청 = 1, 응답 = 2 등)
송신자 하드웨어 주소 (SHA, Sender Hardware Address)	가변적, HLN 값과 동일	메시지를 송신하는 장비의 하드웨어 주소
송신자 프로토콜 주소 (SPA, Sender Protocol Address)	가변적, PLN 값과 동일	메시지를 송신하는 장비의 IP 주소
수신자 하드웨어 주소 (THA, Target Hardware Address)	가변적, HLN 값과 동일	메시지를 수신하는 장비의 하드웨어 주소
수신자 프로토콜 주소 (TPA, Target Protocol Address)	가변적, PLN 값과 동일	메시지를 수신하는 장비의 IP 주소

주소 결정 프로토콜

- ARP

- ARP 메시지 포맷 그림



주소 결정 프로토콜

- ARP

- ARP 캐싱 (Caching)

- 자주 쓰는 주소에 대한 주소 결정 과정의 속도 향상을 위한 방법

- ARP 캐시

- 하드웨어 주소와 IP 주소를 포함하는 테이블 형태

- 캐시항목 추가 방법

- 정적 ARP 캐시 항목

- 캐시 테이블에 수동으로 추가
- 만료 기간없이 영구히 캐시에 남음

- 동적 ARP 캐시 항목

- ARP 주소 결정 결과인 하드웨어와 IP 주소 쌍을 캐시에 추가
- 일정 기간 동안 캐시가 남아 있다가 제거됨

주소 결정 프로토콜

- ARP

- ARP 캐싱 (Caching)

- 캐시 항목 만료

- 캐시에 유효하지 않은 하드웨어 및 IP 주소가 저장되는 문제를 피하기 위한 방법

- 유효하지 않은 캐시

- 수신 장비의 하드웨어의 상태가 변경되는 경우
 - 수신 장비 하드웨어 주소가 더 이상 네트워크에 남아있지 않게 됨
 - 수신 장비 IP 주소가 변경되는 경우
 - 수신 장비가 제거되었을 경우
 - 네트워크에서 장비가 제거되지만 송신 장비의 캐시에는 여전히 수신장비의 정보가 남아있음

주소 결정 프로토콜

- ARP

- ARP 프록시 (Proxy)

- 두 장비가 같은 로컬 네트워크에 있지 않을 경우에 라우터가 다른 네트워크에 있는 장비 대신 ARP 요청에 응답

- 동작 과정

- 송신 장비가 ARP 요청 메시지를 브로드캐스트
- 라우터가 수신 장비 대신 자신의 하드웨어 주소 전송
- 송신 장비의 요청 메시지를 수신 장비에게 전달

주소 결정 프로토콜

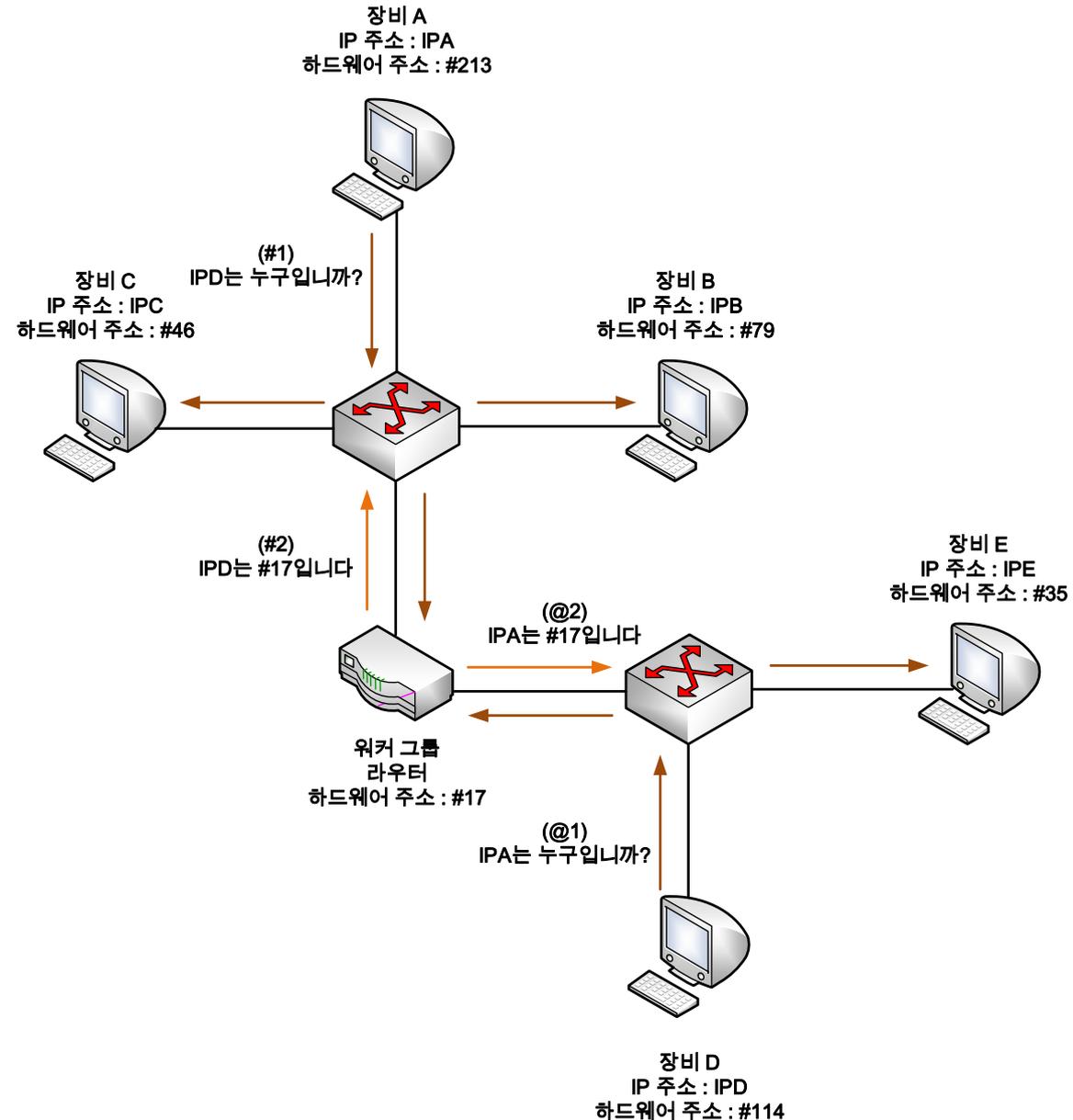
• ARP

• ARP 프록시 (Proxy)

• 동작 과정 그림

• 라우터

- 두 로컬 네트워크를 연결
- ARP 프록시로 동작하도록 설정



주소 결정 프로토콜

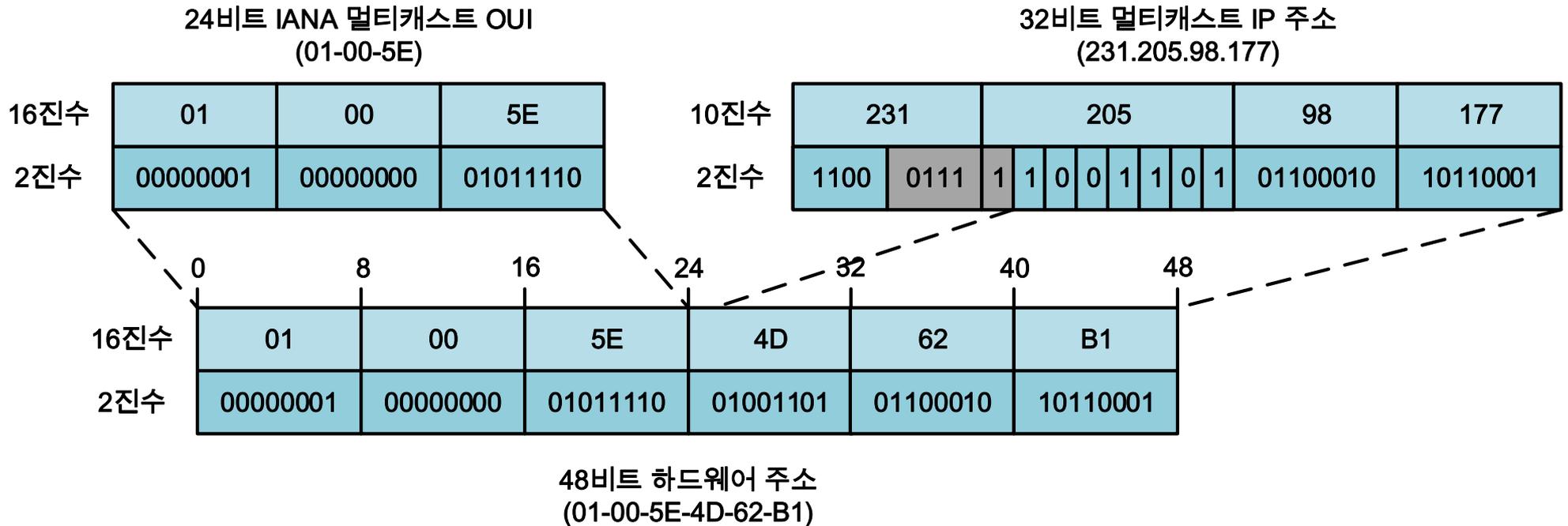
- IP 멀티캐스트 주소의 TCP/IP 주소 결정
 - IP 멀티캐스트 그룹 주소를 직접 매핑 기법을 통해 MAC 주소로 변환
- IEEE 802 주소 지정 방법 사용
 - 데이터 링크 계층 주소는 24비트 블록 2개로 구성
 - 상위 24비트는 기관 유일 식별자 (OUI, Organizationally Unique Identifier)
 - e.g., 인터넷 할당 번호 관리기관 (IANA, Internet Assigned Number Authority)
=01:00:5E
 - 하위 24비트는 개별 장비를 구분

주소 결정 프로토콜

- IP 멀티캐스트 주소의 TCP/IP 주소 결정
 - 멀티캐스트 IP 주소를 하드웨어 주소로 매핑
 1. 상위 24비트에 IANA 멀티캐스트 OUI (01:00:5E) 복사
 2. 25번째 비트는 0으로 설정
 3. 하위 23비트는 멀티캐스트 MAC주소의 나머지 23비트에 복사
 - 이후 5비트는 매핑에서 제외되며, 서로 다른 32개의 IP주소가 동일한 멀티캐스트 MAC 주소로 매핑 가능

주소 결정 프로토콜

- IP 멀티캐스트 주소의 TCP/IP 주소 결정
 - 멀티캐스트 IP 주소를 하드웨어 주소로 매핑



목 차

- 2 – 1부 TCP/IP 네트워크 인터페이스 계층 프로토콜
 - SLIP과 PPP 개요
 - PPP 핵심 프로토콜
 - PPP 기능 프로토콜
 - PPP 프로토콜 프레임 포맷
- 2 – 2부 네트워크 인터넷 계층 연결 프로토콜
 - 주소 결정 프로토콜
 - 역순 주소 결정 프로토콜

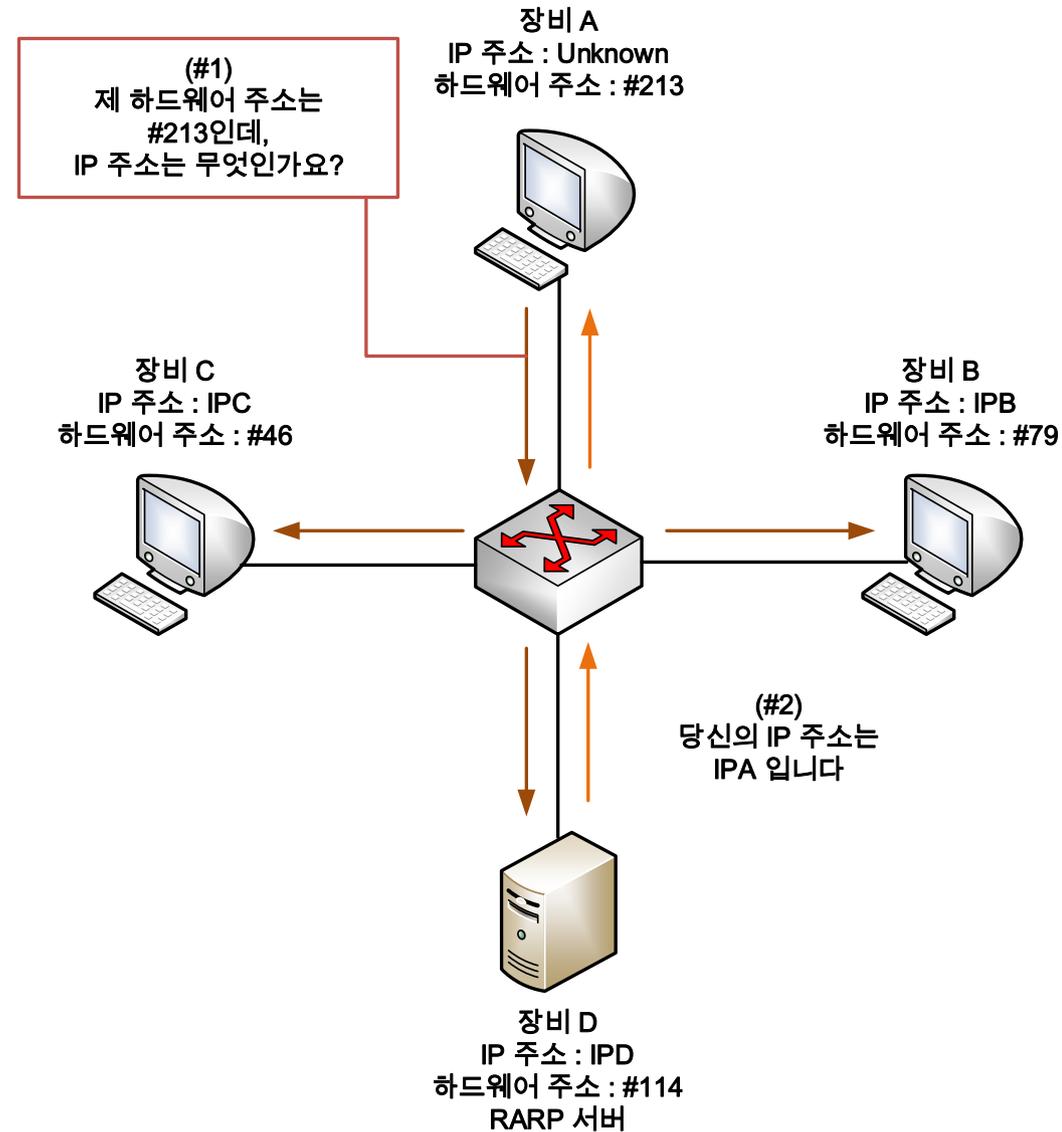
역순 주소 결정 프로토콜

- RARP (Reverse Address Resolution Protocol)
- 특수 RARP 서버에서 장비가 자신의 IP주소를 얻기 위한 방식
 - 장비의 하드웨어 주소를 브로드캐스트하고 RARP 서버가 그것에 IP 주소로 응답

역순 주소 결정 프로토콜

- RARP

- 동작 과정 그림



역순 주소 결정 프로토콜

- 역순 주소 결정 프로토콜 (RARP)
- RARP의 제약
 - 하드웨어 기반
 - RARP는 하드웨어 브로드캐스트를 통해 동작
 - 네트워크에서 1개이상의 RARP 서버를 운영해야 한다는 것을 의미
 - 수동 할당
 - RARP 서버의 하드웨어와 IP 주소 매핑 테이블은 수동으로 설정되어야 함
 - 제한된 정보
 - RARP는 호스트에게 오직 IP 주소만을 알려줌

Thanks!

박재형 (jaehyoung@pel.sejong.ac.kr)