

TCP/IP 완벽 가이드

- 2부 TCP/IP 하위 계층 핵심 프로토콜 -

정재형(sj20jjh@sju.ac.kr)

세종대학교 프로토콜공학연구실

목 차

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

목 차

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

SLIP과 PPP 개요

- IP는 2계층에서 어떤 서비스를 제공해 준다고 가정
- 물리 계층에서의 기본적인 하위 계층 연결만을 맺는 경우 IP 운영 불가
 - 프레이밍을 지원하는 2계층 구현 필요
 - 네트워크 인터페이스 계층 프로토콜
 - SLIP
 - PPP

7	애플리케이션
6	
5	
4	전송
3	인터넷
2	네트워크 인터페이스
1	(하드웨어)

OSI모델 & TCP/IP 모델

SLIP과 PPP 개요

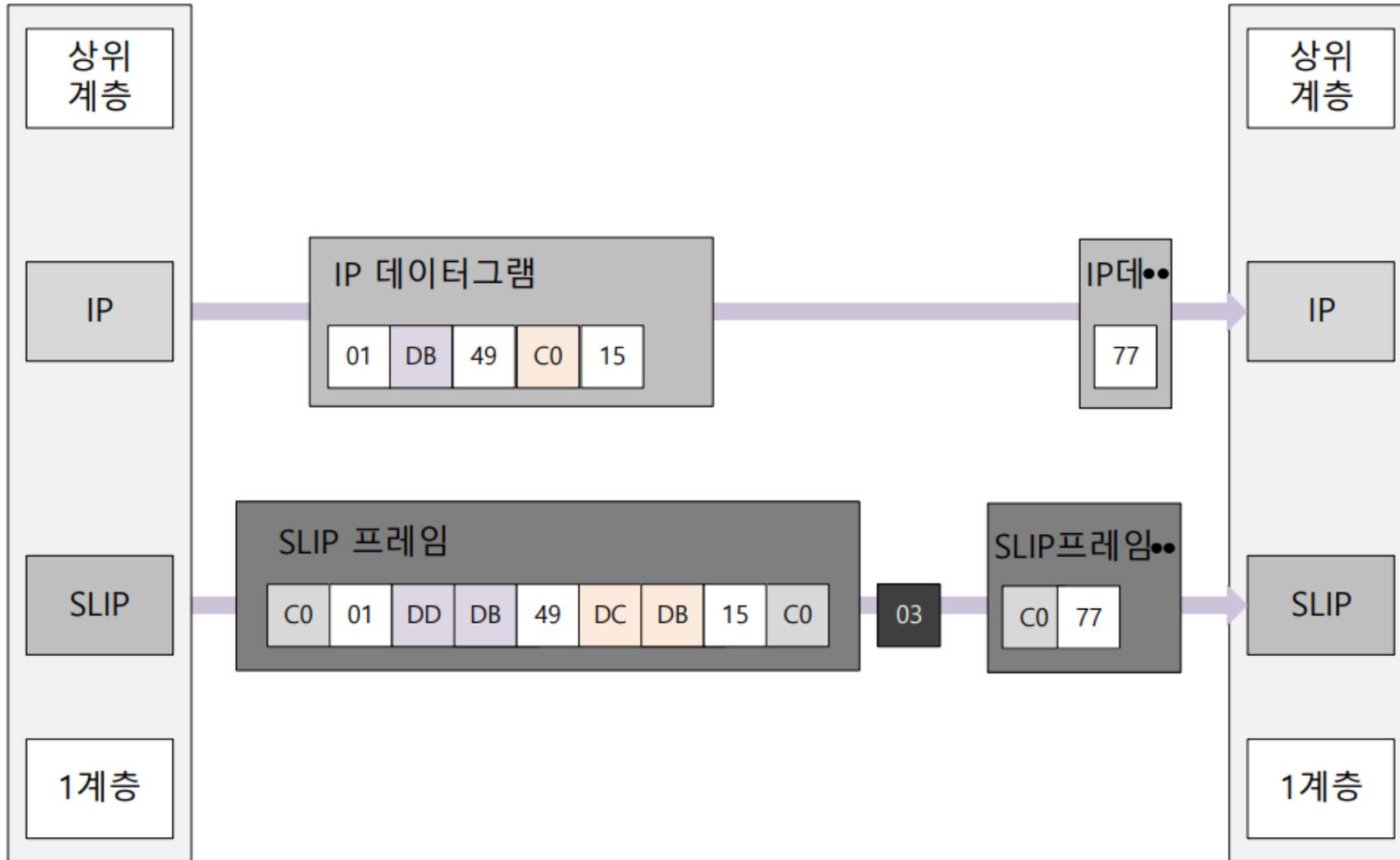
- 네트워크 인터페이스 계층 프로토콜
 - 직렬 회선 인터넷 프로토콜(SLIP, Serial Line Internet Protocol)
 - IP에 대한 기본 프레임만을 제공하는 매우 간단한 프로토콜
 - 점대점 프로토콜(PPP, Point-to-Point Protocol)
 - SLIP보다 복잡하고 기능이 다양(인증, 압축, 에러 탐지 등)
 - 프레임뿐만 아니라 보안과 성능을 강화하기 위한 여러 추가 기능 제공

SLIP

- 직렬 회선 인터넷 프로토콜(SLIP)
- 전송을 위한 데이터 프레임만을 수행
- SLIP 데이터 프레임 과정
 1. IP 데이터그램을 전달받음
 2. 데이터그램의 처음과 끝에 SLIP END 바이트 추가
 - SLIP END : 192, 16진수 C0
 - 데이터그램에 특수 바이트 값이 있으면 다른 값으로 치환
 - 192(C0) : SLIP END -> 219 220(DB DC)
 - 219(DB) : ESC -> 219 221(DB DD)
 3. SLIP 프레임을 바이트로 나누어 전송

SLIP

• SLIP 데이터 프레임밍 과정



SLIP

- 문제와 한계

- 데이터그램 크기 명세 표준이 없음
- 에러 탐지 및 정정 방법이 제공되지 않음
- 링크 관리를 위한 제어 메시지를 전송하지 않음
- 헤더 부재로 인한 유형 식별 불가능
- 주소 탐색을 지원하지 않음
- 속도 향상을 위한 압축을 지원하지 않음
- 기본적인 보안 기능을 지원하지 않음

PPP

- 점대점 프로토콜(PPP)

- 프레이밍뿐만 아니라 에러 탐지, 압축, 인증, 암호화와 같은 여러 기능과 특징을 포함
- 특징
 - SLIP보다 훨씬 포괄적인 프레이밍 방식
 - 단일 링크에서 여러 3계층 프로토콜을 다중화할 수 있는 캡슐화 프로토콜 명세 제공
 - 각 프레임 헤더에 순환 잉여 검사(CRC, cyclic redundancy check) 코드를 삽입하여 전송 프레임의 에러 탐지
 - 링크 인자 협상을 위한 안정적인 방식
 - 데이터그램 전송 전 링크 테스트, 링크 품질 모니터링 가능
 - 여러 인증 프로토콜을 통해 연결 인증 가능
 - 압축, 암호화, 링크 통합 같은 추가 선택 기능 지원

PPP

- 점대점 프로토콜(PPP)

- 구성 요소

- PPP 캡슐화 방법

- 특수 프레임 포맷 정의

- 링크 제어 프로토콜(LCP, Link Control Protocol)

- 장비간 링크의 수립, 유지, 종료를 책임짐
 - 두 장비가 링크 사용 방법을 협의하기 위해 여러 설정 인자를 교환하도록 함

- 네트워크 제어 프로토콜(NCP, Network Control Protocol)

- 여러 3계층 데이터그램 유형을 캡슐화하는 기능을 지원

- LCP 지원 프로토콜

- 링크 협상 과정에서 관리나 옵션을 설정하기 위해 사용

- LCP 선택적 기능 프로토콜

- 데이터그램이 장비간 전송될 때 동작을 향상시키기 위한 프로토콜

PPP

• 점대점 프로토콜(PPP)

• 일반 동작 과정

1. 링크 수립과 구성

- 두 장비가 정보를 교환하기 위해 링크 수립
- 링크의 운영을 관리하는 데 필요 인자에 동의해야 함
- LCP는 필요한 경우 지원 프로토콜의 도움을 받음
 - 링크가 수립되면 적절한 NCP가 호출됨

2. 링크 동작

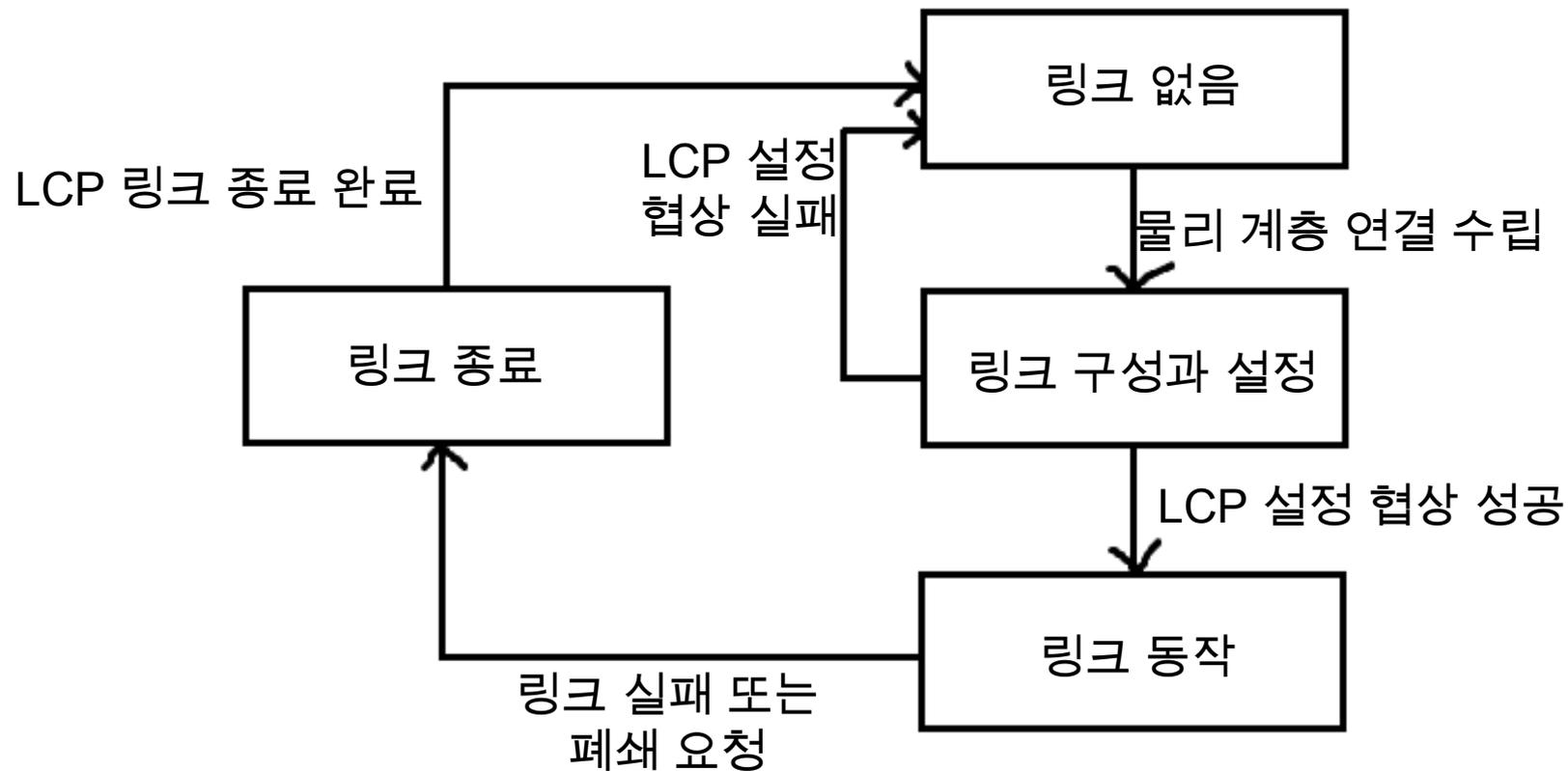
- 링크를 통해 데이터그램 전송
 - 3계층 데이터그램을 캡슐화하여 1계층으로 송신
 - 수신한 PPP 프레임의 헤더를 제거해 데이터그램을 3계층으로 올려보냄
 - 필요할 경우 선택적으로 특수 프로토콜을 이용할 수도 있음

3. 링크 종료

PPP

- 점대점 프로토콜(PPP)

- 그림 9-3



PPP

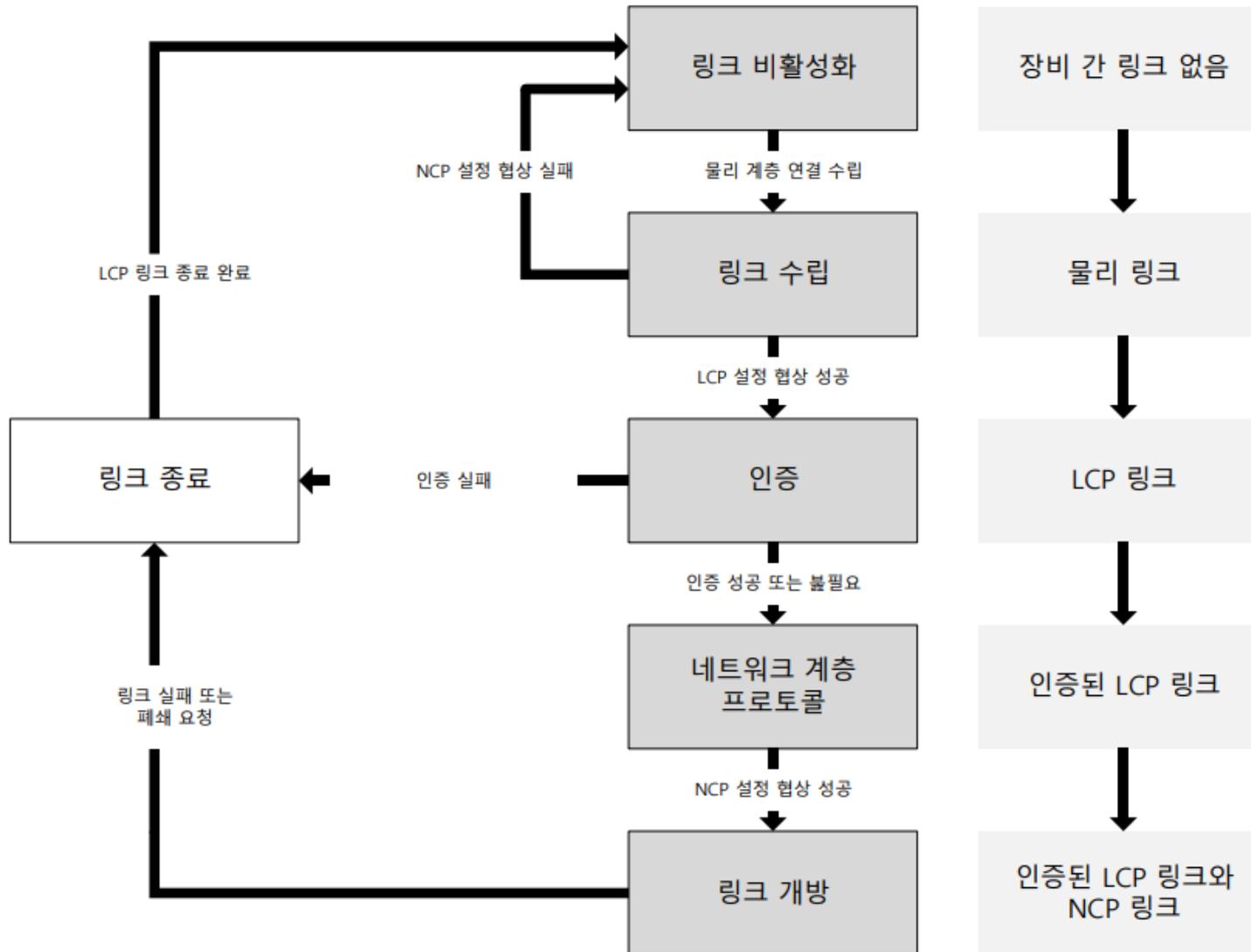
- 점대점 프로토콜(PPP)
 - PPP 링크 수립과 단계
 - 링크 비활성화 단계
 - 두 장비 간 아무런 물리 계층 연결이 존재하지 않는 상태
 - 링크 수립 단계
 - 물리 계층이 연결됨
 - LCP가 링크의 기본 설정 수행
 - LCP 설정요청 메시지 발송
 - 동의하면 승인 메시지 응답
 - 비동의시 비승인/거부 메시지 응답
 - 새 인자를 이용해 재요청 가능
 - 인증 단계
 - 반드시 해야 하는 것은 아님
 - 적절한 인증 프로토콜 사용
 - e.g., CHAP, PAP 등

PPP

- 점대점 프로토콜(PPP)
- PPP 링크 수립과 단계
 - 네트워크 계층 프로토콜 단계
 - 네트워크 계층 프로토콜에 맞는 설정을 위해 해당 NCP를 호출
 - 호출 후 확인 없이 링크 개방 단계로 넘어감
 - 링크 개방 단계
 - LCP 링크와 하나 이상의 NCP 링크가 열린 상태에서 동작
 - 성공적으로 구성된 각 NCP를 통해 데이터 전달 가능
 - 링크 종료 단계
 - 특수 LCP 종료 프레임 전송
 - 승인 시 링크 비활성화

PPP

• 점대점 프로토콜(PPP)



목 차

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

PPP 핵심 프로토콜

- 링크 제어 프로토콜(LCP)
 - 전반적인 운영을 책임지며 설정, 유지, 종료의 각 단계에서 핵심적인 역할을 담당
 - LCP 패킷
 - 물리 링크로 LCP 메시지를 전송하여 PPP 링크 제어
 - LCP 링크 설정
 - 설정요청 프레임 옵션
 - 최대 수신 유닛(MRU, Maximum Receive Unit)
 - 최대 데이터그램 크기
 - 인증 프로토콜(Authentication Protocol)
 - 사용하고자 하는 인증 프로토콜 유형
 - 품질 프로토콜(Quality Protocol)
 - 어떤 품질 모니터링 프로토콜을 이용할지 지정

PPP 핵심 프로토콜

- 링크 제어 프로토콜(LCP)
 - LCP 링크 설정
 - 설정요청 프레임 옵션
 - 매직 넘버(Magic Number)
 - 루프 백 링크 또는 기타 연결의 비정상 행위를 탐지
 - 프로토콜 필드 압축
 - 일반적인 16비트 프로토콜 필드 대신 압축된 8비트 프로토콜을 필드를 사용하고 싶다고 지정
 - 각 프레임마다 1바이트 대역폭 절약
 - 압축 제어 프로토콜(CCP, Compression Control Protocol)과는 별개
 - 주소와 제어 필드 압축(ACFC, Address and Control Field Compression)
 - Address와 Control 필드를 압축하여 대역폭 절약
 - 응답
 - 설정승인, 설정비승인, 설정거부

PPP 핵심 프로토콜

- 링크 제어 프로토콜(LCP)
 - LCP 링크 유지
 - 링크를 관리하거나 디버깅하기 위해 LCP 메시지 사용
 - 코드거부와 프로토콜거부
 - 에코요청, 에코응답, 버림요청
 - LCP 링크 종료
 - 종료요청 메시지 전송
 - 거부할 수 없음
 - 종료승인 메시지로 응답
- 기타 LCP 메시지
 - 식별 메시지
 - 남은 시간 메시지

PPP 핵심 프로토콜

- 네트워크 제어 프로토콜(NCP)
 - 특정 네트워크 계층 프로토콜에 유일한 인자를 협상
 - 각 LCP 링크별로 하나 이상의 NCP 운영 가능
 - PPP 인터넷 프로토콜 제어 프로토콜
(IPCP, Internet Protocol Control Protocol)
 - PPP 인터넷워킹 패킷 교환 제어 프로토콜
(IPXCP, Internetworking Packet Exchange Control Protocol)
 - PPP 넷바이오스 프레임 제어 프로토콜
(NBFCP, NetBIOS Frames Control Protocol)
 - PPP IP 버전 6 제어 프로토콜
(IPv6CP, IP Version 6 Control Protocol)

PPP 핵심 프로토콜

- 네트워크 제어 프로토콜(NCP)
 - NCP의 동작
 - 링크 설정
 - 설정요청, 설정승인, 설정비승인, 설정거부
 - 링크 유지
 - 코드거부 메시지
 - 링크 종료
 - 종료요청, 종료승인
 - LCP의 종료와는 별개
 - 필수적이지 않음

PPP 핵심 프로토콜

- 네트워크 제어 프로토콜(NCP)
- 인터넷 프로토콜 제어 프로토콜(IPCP)
 - 설정 옵션
 - IP 압축 프로토콜
 - 반 야콥슨(Van Jacobson) TCP/IP 헤더 압축 사용 여부
 - IP 주소
 - IP라 라우팅 용도로 사용할 IP 주소를 지정하거나 상대방에게 요청

PPP 핵심 프로토콜

- PPP 인증 프로토콜
 - 비밀번호 인증 프로토콜
(PAP, Password Authentication Protocol)
 - 챌린지 핸드셰이크 인증 프로토콜
(CHAP, Challenge Handshake Authentication Protocol)

PPP 핵심 프로토콜

- PPP 인증 프로토콜

- PAP

- 단계

- 인증 요청

- 이름과 비밀번호를 포함한 인증요청 메시지 송신

- 인증 응답

- 허용 시 인증승인 메시지 송신
 - 거절 시 인증비승인 메시지 송신

- 사용자 이름과 비밀번호를 평문 형태로 전송

- 보안 공격에 대한 방어책 부재

- 클라이언트가 인증절차를 제어

PPP 핵심 프로토콜

- PPP 인증 프로토콜

- CHAP

- 비밀번호를 전송하지 않음
- three-way handshake
 - 챌린지(Challenge)
 - 인증자가 초기화 장비에 챌린지 프레임 전송
 - 챌린지 텍스트를 포함
 - 특수한 의미가 없는 데이터
 - 응답
 - 초기화 장비가 비밀번호를 이용하여 챌린지 텍스트를 암호화하여 인증자에게 전송
 - 성공 또는 실패
 - 인증자는 같은 방식으로 챌린지 텍스트를 암호화 후 대조
 - 결과에 따라 성공 혹은 실패 메시지 송신
- 재생 공격에 대한 대비책 제공
- 서버가 인증 절차를 제어

목 차

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

PPP 기능 프로토콜

- PPP 링크 품질 모니터링 (LQM, Link Quality Monitoring)
 - 장비들이 링크의 품질을 분석할 수 있도록 하는 기능
- 링크 품질 리포팅(LQR, Link Quality Reporting)
 - 피어에게 현재 링크의 통계 정보를 주기적으로 전송 요청
- LQR 수립
 - 링크 수립 단계에서 기본 링크 인자 협상 과정의 일부로 수행
 - 설정요청 프레임에 품질 프로토콜 설정옵션 포함
 - 보고서 주기도 지정
 - 정보 보고서를 받는 시간 간격의 최댓값

PPP 기능 프로토콜

- LQR

- LQR 활성화

- 링크 통계를 추적하기 위한 카운터 생성
 - 각 카운터는 링크 사용과 관련된 서로 다른 통계 정보 포함
 - 링크가 수립될 때 0으로 설정 후 이벤트 발생 시 증가
- 품질 보고서를 보내는 시간 간격을 제어하기 위한 타이머 시작
 - 타이머 시간이 만료할 때마다 링크 품질 보고서 생성
 - 프로토콜 필드가 0xC025로 채워진 PPP 프레임으로 보고서 전송
- 통계 정보
 - 송수신한 프레임의 수
 - 송수신한 모든 프레임의 옥텟 수
 - 발생한 에러의 수
 - 버린 프레임의 수
 - 생성된 링크 품질 보고서 수

PPP 기능 프로토콜

- LQR

- 링크 품질 보고서 사용

- 링크 품질에 대한 구체적인 표준이 없음

- 링크 구현에 의존하기 때문

- 품질 보고서의 숫자에 근거하여 장비는 링크 품질에 대한 결론을 내리고 어떤 행동을 취할지 결정

- 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

- 버린 프레임의 비율이 증가

- 일부 장비는 단지 그 정보를 로그에 저장하고 아무런 조치를 취하지 않음

PPP 기능 프로토콜

- PPP 압축 제어 프로토콜과 압축 알고리즘
 - 직렬 연결의 문제점인 느린 속도를 개선하기 위해 라인으로 전송되는 데이터를 압축하여 성능 향상
 - 선택적인 압축 기능 제공
 - PPP 압축 제어 프로토콜(CCP, Compression Control Protocol)
 - PPP 링크에서의 압축을 협상하고 관리
 - PPP 압축 알고리즘
 - 실제 데이터 압축과 해제를 수행하는 알고리즘 모음
 - 공개 표준에서 정의되지 않은 사유 압축 방법 협상도 가능

PPP 기능 프로토콜

- CCP

- 두 장비가 어떻게 데이터를 압축할지를 결정
- LCP 링크 내에서 CCP 링크라는 압축 연결 수립
 - 압축 프레임 전송 가능
 - 관리, 종료를 위한 메시지 기능 제공

PPP 기능 프로토콜

- CCP

- CCP의 동작

- 링크 설정

- 설정요청, 설정승인, 설정비승인, 설정거부

- 링크 유지

- 코드거부 메시지
 - 리셋요청, 리셋승인
 - 압축 해제 과정에 오류 발생 시 압축 기능 초기화

- 링크 종료

- 종료요청, 종료승인
 - LCP의 종료와는 별개
 - 필수적이지 않음

PPP 기능 프로토콜

- CCP

- CCP 설정 옵션

- 두 장비가 사용할 압축 알고리즘을 협상
- CCP 옵션 유형(Type) 값으로 시작

CCP 옵션 유형(Type) 값	알고리즘 정의 RFC	압축 알고리즘(RFC 제목에 나오는 대로)
0	-	사유 프로토콜
1과 2	1978	PPP Predictor Compression Protocol
17	1974	PPP Stac LZS Compression Protocol
18	2118	Microsoft Point-to-Point Compression(MPPC) 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

- CCP

- 압축 알고리즘 운영

- 데이터 전송 전 압축 / 수신 후 압축 해제

- 압축되지 않은 PPP 프레임의 정보 필드에 들어갈 데이터를 받아 압축 알고리즘을 적용
 - 압축됐다는 것을 나타내기 위해 프로토콜 필드에 특수 값인 0x00FD를 넣음
 - 다중링크에서 압축을 사용했고 각 링크가 독립적으로 압축됐다면 0x00FB라는 값을 넣음
 - 원본 프로토콜 필드를 데이터 앞에 첨부하여 압축
 - 압축 해제 후 원본 프로토콜 필드 복구

- 하나 이상의 데이터 프레임을 압축 데이터 프레임에 넣을 수 있음

- LCP 프레임, 기타 프로토콜 제어 프레임은 압축되지 않음

- LCP 헤더 압축과 무관

PPP 기능 프로토콜

- PPP 암호화 제어 프로토콜과 암호화 알고리즘
 - PPP 암호화 제어 프로토콜 (ECP, Encryption Control Protocol)
 - PPP 링크에서 암호화를 협상하고 관리하는 데 쓰임
 - PPP 암호화 알고리즘
 - 실제 데이터를 암호화하고 복호화하는 알고리즘 모음

PPP 기능 프로토콜

- ECP

- ECP의 동작

- 링크 설정

- 설정요청, 설정승인, 설정비승인, 설정거부

- 링크 유지

- 코드거부 메시지
 - 리셋요청, 리셋승인
 - 암호화 과정에 오류 발생 시 암호 기능 초기화

- 링크 종료

- 종료요청, 종료승인
 - LCP의 종료와는 별개
 - 필수적이지 않음

PPP 기능 프로토콜

- ECP

- ECP 설정 옵션

- 두 장비가 사용할 암호화 알고리즘 협상
- ECP 옵션 유형값으로 시작
- 현재는 오직 두 알고리즘만이 정의되어 있음

ECP 옵션 유형값	알고리즘 정의 RFC	암호화 알고리즘(RFC 제목에 나오는 대로)
0	-	사유 프로토콜
2	2420	The PPP Triple-DES Encryption Protocol
3	2419	The PPP DES Encryption Protocol, Version 2

PPP 기능 프로토콜

- ECP

- 암호화 알고리즘 운영

- 데이터 전송 전 암호화 / 수신 후 복호화

- 암호화되지 않은 PPP 프레임의 정보 필드에 들어갈 데이터를 받아 암호화 알고리즘을 적용
 - 압축됐다는 것을 나타내기 위해 프로토콜 필드에 특수 값인 0x0053을 넣음
 - 다중링크에서 압축을 사용했고 각 링크가 독립적으로 압축됐다면 0x0055라는 값을 넣음
 - 원본 프로토콜 필드를 데이터 앞에 첨부하여 압축
 - 압축 해제 후 원본 프로토콜 필드 복구

- 하나의 암호화된 데이터 프레임은 하나의 데이터 프레임만 포함

- LCP 프레임, 기타 프로토콜 제어 프레임도 암호화될 수 있음
 - 압축 후 암호화 가능

PPP 기능 프로토콜

- PPP 다중링크 프로토콜

- 두 머신 사이에 하나 이상의 링크가 있는 경우

- 다중화로 인해 논리적 채널이 하나 이상

- e.g., ISDN 기본 속도 인터페이스

- (Integrated Service Digital Network Base Rate Interface)

- 두 개의 B 채널이 시분할 방식으로 다중화되어 하나의 구리선으로 전송

- 물리 계층 링크가 하나 이상

- 여러 링크를 결합하여 하나의 고성능 링크인 것처럼 사용하기 위해 PPP 다중링크 프로토콜(MP, Multilink Protocol) 이용

PPP 기능 프로토콜

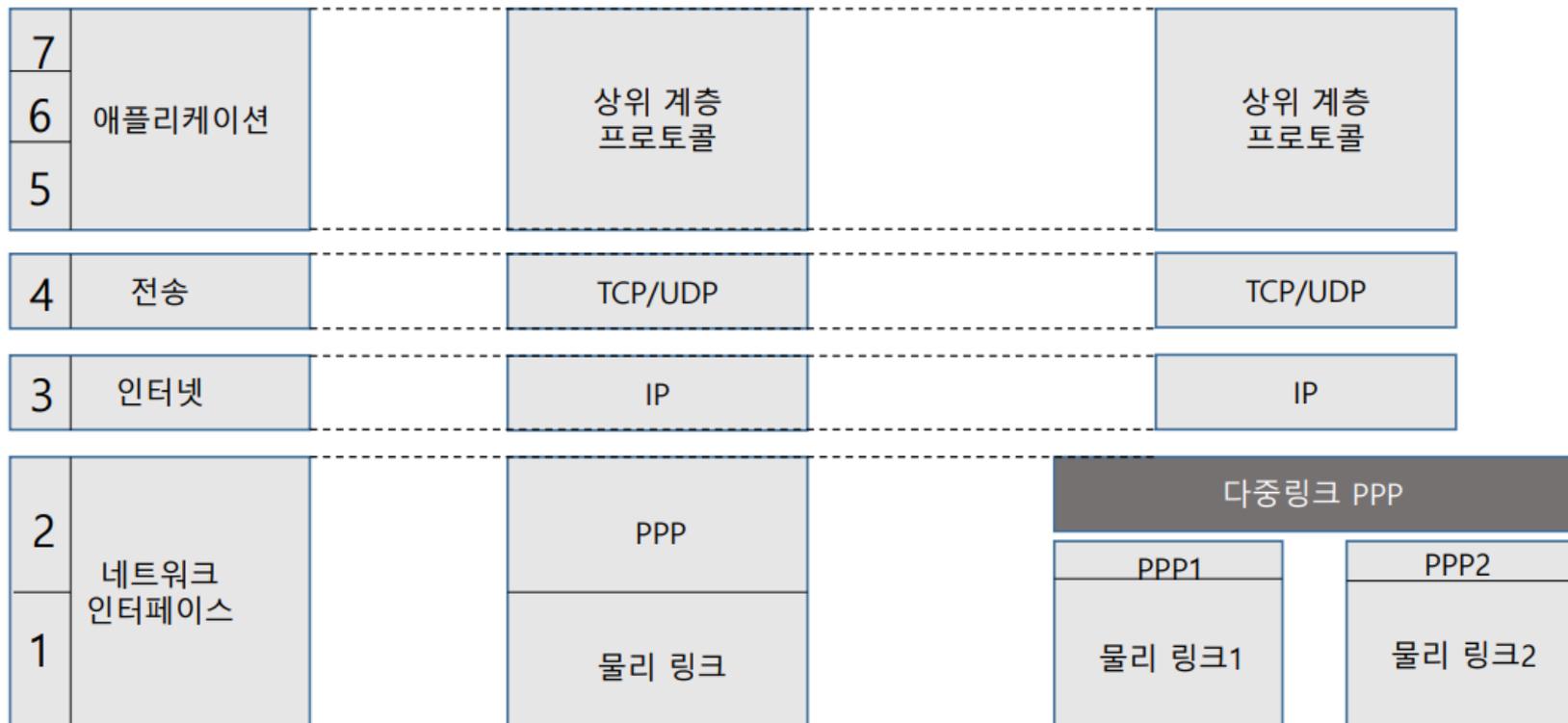
- MP

- 구조

- PPP의 선택적 기능

- PPP의 새로운 하위 계층으로 구현

- 일반 PPP 계층과 PPP를 이용하는 네트워크 계층 프로토콜 사이에 위치



PPP 기능 프로토콜

- MP

- 수립

- 양 장비의 PPP 소프트웨어에 기능이 구현
- MP를 사용하기로 협상

- 설정

- 다중링크 최대 수신 재구성 유닛
(Multilink Maximum Received Reconstructed Unit)
 - MP 사용의사를 표현
 - 지원하는 최대 PPP 프레임 크기 값 포함
- 다중링크 짧은 순서번호 헤더포맷
(Multilink Short Sequence Number Header Format)
 - 효율성을 높이기 위해 MP 프레임에서 짧은 순서 번호 필드 사용
- 종단 식별자(Endpoint Discriminator)
 - 어떤 링크가 어떤 장비로 연결되는지 파악

PPP 기능 프로토콜

- MP

- 운영

- 네트워크 계층과 일반 PPP 링크 사이에서 중간자 역할

- 송신

- 네트워크 계층 프로토콜로부터 데이터그램을 받아 PPP 프레임의 수정된 버전으로 캡슐화
- 캡슐화된 프레임을 단편화하여 여러 링크로 분배
- 분배된 프레임을 캡슐화하여 물리 링크로 전송
 - 크기가 작은 프레임, 링크 설정에 쓰이는 제어 프레임은 단편화되지 않음

- 수신

- 프레임 조각 재조합하여 원본 PPP 프레임 구성

PPP 기능 프로토콜

- PPP 대역폭 할당 프로토콜과 대역폭 할당 제어 프로토콜
 - 대역폭 할당 프로토콜(BAP, Bandwidth Allocation Protocol)
 - MP로 동작하는 장비들이 특정 링크를 묶음에 추가하거나 제거할 수 있도록 하는 방법 설명
 - 대역폭 할당 제어 프로토콜(BACP, Bandwidth Allocation Control Protocol)
 - 장비들이 BAP 사용 방법을 설정할 수 있게 함

PPP 기능 프로토콜

- BACP 운영

- 링크 설정 과정 중에 BAP를 수립하는 데 사용
- 설정요청, 설정승인, 설정비승인, 설정거부 메시지 이용
- 설정 옵션
 - Favored-Peer
 - 링크의 두 장비가 동시에 동일한 요청을 보낼 때 문제가 일어나지 않는 것을 보장하는 데 사용
 - 두 장비가 BAP를 지원하면 BACP 협상은 성공하고 BAP가 활성화

PPP 기능 프로토콜

- BAP 운영

- 장비들이 현재 PPP 링크 묶음에서 링크를 제거하거나 추가하기 위해 보낼 수 있는 메시지 모음을 정의

- BAP 메시지 유형

- 콜요청과 콜응답

- 링크 묶음에 링크를 추가하고, 새로운 물리 계층 링크를 초기화하고 싶은 장비는 상대방 장비에게 콜요청 프레임 송신, 콜 응답 수신

- 콜백요청과 콜백응답

- 상대 장비가 새 링크를 추가하라는 요청을 보내기 원할 때 사용

PPP 기능 프로토콜

- BAP 운영

- BAP 메시지 유형

- 콜상태표시와 콜상태응답

- 새로운 링크를 추가하려는 시도를 한 장비는 그 링크의 상태를 콜상태표시 프레임 송신, 콜상태응답 수신

- 링크제거요청(Link-Drop-Query-Request)과 링크제거응답(Link-Drop-Query-Response)

- 링크를 제거하기 위한 요청, 응답
 - 언제 링크를 추가하거나 제거할지 결정하는 것은 각 PPP 구현의 몫

TBA

- TBA
 - TBA
 - TBA
 - TBA
 - TBA

Thanks!

정재형 (sj20jjh@sju.ac.kr)