2016/04/04, PEL

TCP/IP 완벽 가이드

- FTP/TFTP -

위 사랑 (sarang@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

목 차

- FTP(File Transfer Protocol)
- TFTP(Trivial File Transfer Protocol)

FTP

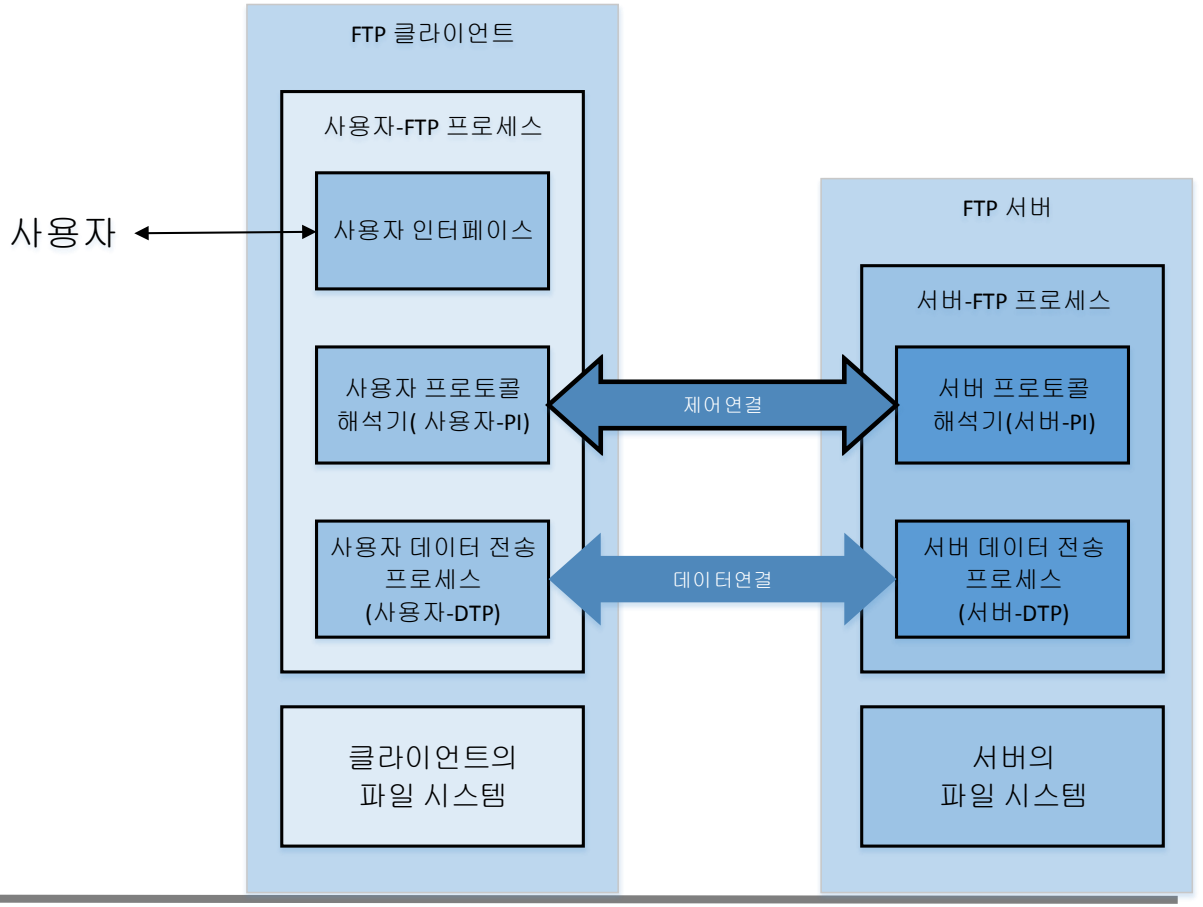
- FTP란?
  - File Transfer Protocol 의 약자
  - 네트워크를 통해 파일을 전송하는데 사용하는 프로토콜
  - 아키텍처 : 클라이언트/서버 구조
  - 프로토콜 : TCP 사용
  - Port : FTP서버는 20,21번 port 사용

FTP

- FTP프로세스 구성요소
  - 서버-FTP프로세스
    - **서버 프로토콜 해석기**(서버-PI, server protocol interpreter): 서버의 제어연결을 담당; FTP 주포트에서 대기하면서 사용자로부터 들어오는 연결 기다림; 서버 DTP관리
    - **서버 데이터 전송 프로세스**(서버-DTP, server data transfer process) : 사용자 DTP와 데이터 주고받음;
  - 사용자-FTP프로세스
    - **사용자 프로토콜 해석기**(사용자-PI, user protocol interpreter) : 클라이언트의 제어연결을 담당;서버 PI로 메시지보내면서 세션 초기화; 사용자 DTP 관리
    - **사용자데이터전송 프로세스**(사용자-DTP, user data transfer process) : 서버의 DTP와 데이터 주고받음
    - **사용자인터페이스**: 사용자중심 명령 제공; FTP 세션사용자에게 결과 정보 제공

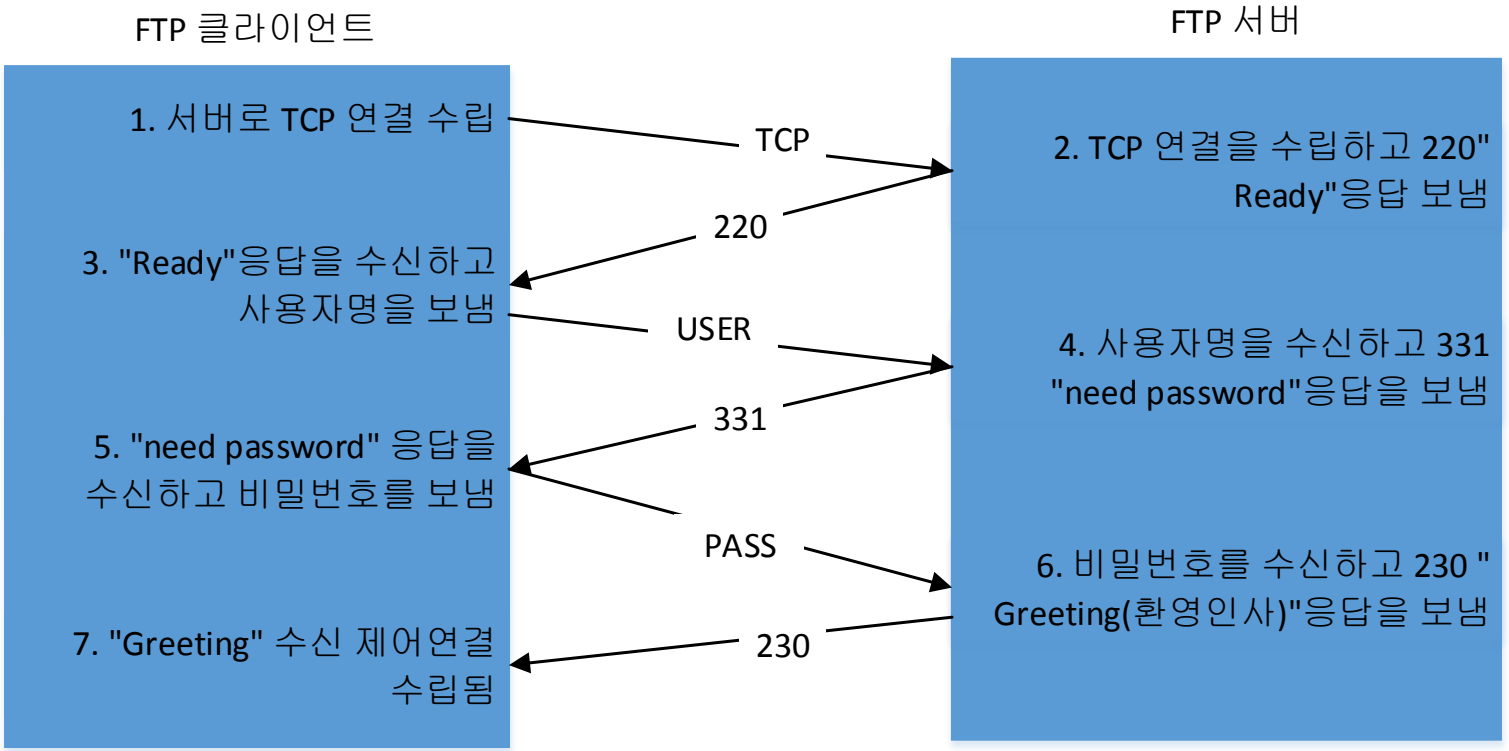
FTP

- FTP제어연결과 데이터연결
  - 제어연결
    - FTP 세션을 연결시킬 때 사용; 세션동안 연결된 상태로 유지하고 FTP명령과 응답 같은 제어정보만을 주고받을 때 사용
  - 데이터연결
    - 데이터가 전달될 때 사용



FTP사용자 인증

- 로그인
  - PASS명령을 이용해 사용자의 비밀번호 전송
  - 세션이 연결 된 후 환영인사 보냄



FTP

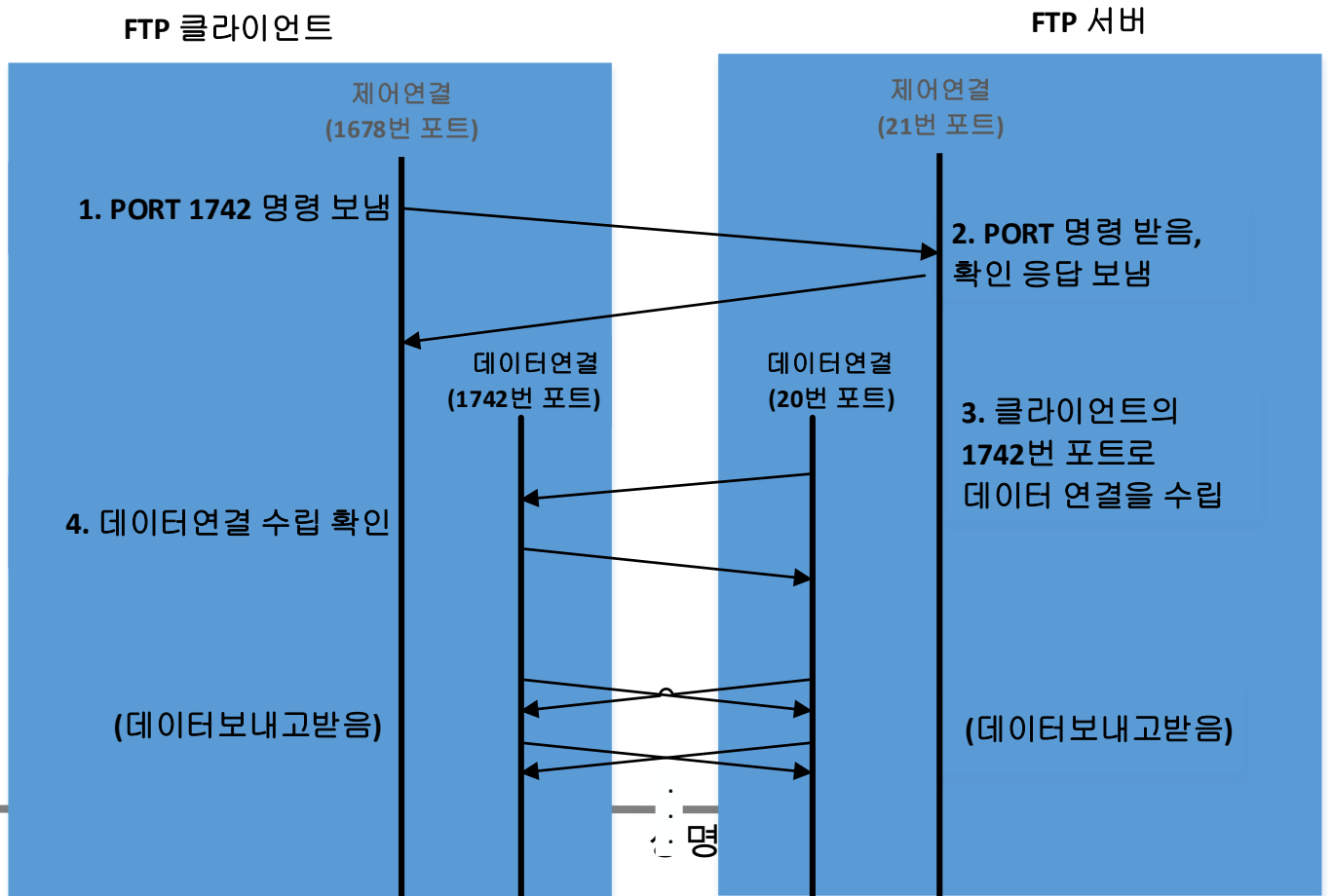
- FTP보안
  - 사용자인증방식에서 제어연결을 통해 사용자명과 비밀번호를 평문으로 전송(보안성 낮음)
  - 보안을 강화한 프로토콜 등장
    - FTPS(FTP over SSL/TLS secured channel)
      - ✓ 응용 계층 FTP와 전송계층 TCP 사이에 보안 소켓계층(SSL)을 추가하여 사용하는 형태
      - ✓ FTPS 포트 : 990(제어연결), 989(데이터연결)

FTP

- 익명 FTP
  - 일반대중에게 정보를 전달하고자 하는 기업이 사용
  - 익명사용자는 공개된 특정 디렉토리에서 파일을 읽는 권한만 가짐

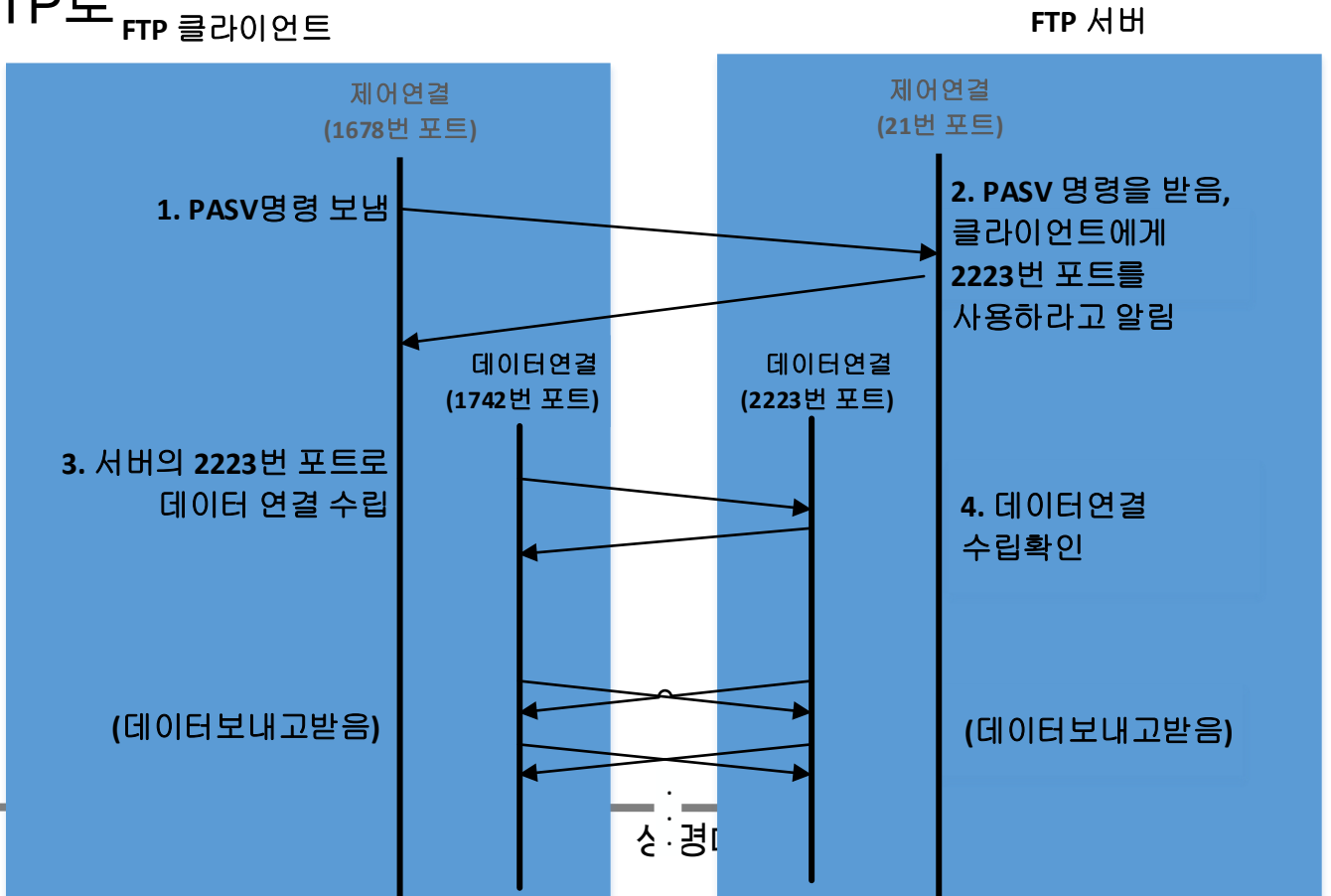
FTP

- 데이터연결 관리
  - 일반(능동)데이터 연결
    - 서버-DTP가 사용자-DTP로 TCP 연결을 수립하여 데이터채널을 초기화
    - 클라이언트가 능동적으로 포트 결정



FTP

- 데이터연결 관리
  - 수동데이터 연결
    - 클라이언트는 자신이 초기화한 데이터를 받아들이도록 수동 상태로 전환하라고 서버에게 명령(PASV 보냄)
    - 사용자-DTP가 서버-DTP로 TCP 연결을 수립하여 데이터채널을 초기화
    - 클라이언트에게 수동적 포트로 주어짐



FTP

- 전송모드
  - 스트림 모드(가장 많이 쓰임)
    - 단순한 바이트의 연속
    - TCP의 데이터스트림 기능과 신뢰성 있는 전송 서비스에 전적으로 의존
    - 헤더가 없기 때문에 파일의 끝을 나타내기 위해선 데이터 연결을 끊어야 함
  - 블록 모드
    - 데이터를 데이터블록으로 나눠서 개별적인 FTP 블록으로 캡슐화해서 전송
    - 3바이트짜리 헤더
  - 압축 모드
    - 런 랭스 부호화 사용(run length encoding)
      - ✓ 전송되는 데이터에서 연속된 패턴을 감지하여 총 메시지 길이가 줄어들도록 데이터를 표현하는 방식

FTP

- FTP 자료형
  - ASCII : 줄의 끝을 나타내는 문자를 사용하는 텍스트파일을 정의
    - 텍스트파일을 전송할 때 시스템마다 끝을 표현하는 문자가 다르기 때문에 에러 발생
      - ✓ 유닉스 : LF(라인 피드 문자)
      - ✓ 애플 : CR(캐리지 리턴 문자)
      - ✓ 윈도우: CR+LF
    - FTP프로세스가 변환하여 해결
  - 바이너리: 내부구조가 따로 없으며 FTP는 아무런 처리를 하지 않고 바이트를 하나씩 그대로 보냄
  - 로컬 : 한 바이트가 8비트가 아닌 파일(옥텟이 생겨난 이유..)을 다루는 데 쓰이는 자료형

FTP

- FTP 데이터구조
  - 파일 구조
    - 특별한 내부구조가 없는 연속된 바이트 흐름으로 구성
    - 대부분의 파일에서 쓰이는 기본 구조
  - 레코드 구조
    - 레코드 끝 문자로 구분된 일련의 연속된 레코드로 구성
  - 페이지 구조
    - 파일내부에 특별한 인덱스를 지닌 데이터 페이지
    - ARPAnet초기에 사용되던 컴퓨터를 위해 만든 구조

FTP

- FTP 명령
  - 제어 채널을 통해서 이루어짐
  - 기능 유형에 따라 나뉨
    - 접근제어 명령 : 사용자 로그인과 인증 과정과 관련된 명령, 접근 제어에 관련된 명령, 일반 세션 제어에 관련된 명령
    - 전송인자 명령 : 데이터 전송을 어떻게할 지와 관련된 명령(FTP 프로토콜 서비스 명령)
    - FTP 서비스 명령 : 실제 파일을 보내고 받는 등 파일 전송과 관련된 명령과, 파일을 삭제하고 파일 이름을 변경하는 보조기능과 관련된 명령

FTP

- FTP 명령(접근제어 명령)

명령코드	명령	설명
USER	User name(사용자명)	FTP세션을 수립하고자 하는 사용자를 식별
PASS	Password(비밀번호)	로그인 인증 과정에서 USER 명령으로 제공된 사용자명에 해당하는 비밀번호를 명시
ACCT	Account(계정)	FTP 세션 도중 인증된 사용자가 사용할 계정을 명시; 사용자명과 계정이 다른 시스템에서만 사용; 대부분의 시스템에서는 USER명령에서 사용자명을 자동으로 선택
CWD	Change working directory (작업 디렉토리 변경)	FTP 세션도중 사용자가 파일 전송을 위한 다른 디렉토리를 설정할 수 있도록 함
CDUP	Change to parent directory (상위 디렉토리 변경)	특수한 CWD명령으로 서비스의 디렉토리 구조상 한 단계 위로 올라가도록 함; 파일 시스템간의 디렉토리 구조를 가리기위해 별도로 구현; 사용자는 서버의 디렉토리 구조에 대한 정보 없이 CDUP만으로 상우 디렉토리로 갈 수 있음
SMNT	Structure mount (구조 마운트)	다른 자원에 접근하기 위해 특정 파일 시스템을 마운트 할 수 있도록 함
REIN	Reinitialize(재초기화)	FTP 세션을 재초기화하고 설정된 인자와 사용자 정보를 모두 초기화; 제어연결을 막 수립한 상태로 세션을 되돌려 놓음; USER명령의 반대되는 명령이라고 할 수 있음; 이 명령 직후에 USER명령을 통해 다른 사용자로 로그인
QUT	Logout(로그아웃)	FTP세션을 종료하고 제어 연결을 닫음; 세션전체를 종료

FTP

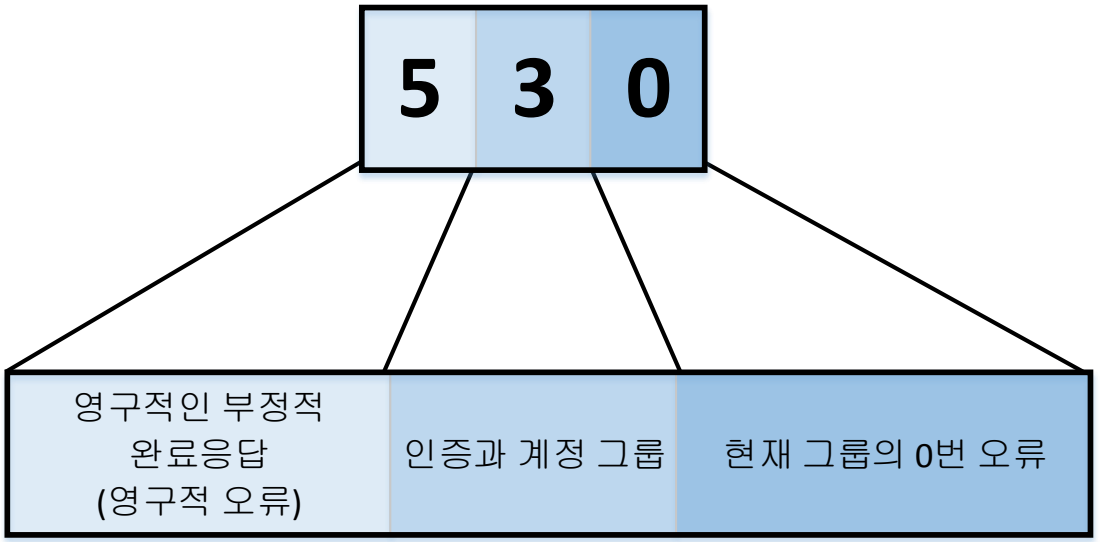
- FTP 명령(프로토콜 서비스 명령)

명령코드	명령	설명
PORT	Data Port(데이터 포트)	클라이언트가 지정된 포트번호를 사용하는 능동연결을 받아들이고자 한다는 사실을 FTP서버로 전송
PASV	Passive(수동)	사용자-DTP가 수동 데이터 연결을 초기화하는 것을 허용해 달라는 요청을 FTP 서버에게 보냄
TYPE	Representation type(표시형)	전송할 파일의 자료형을 명시할때 사용
STRU	File structure(파일 구조)	파일의 데이터구조(파일, 레코드, 페이지)명시
MODE	Transfer mode(전송 모드)	사용할 데이터모드(스트림, 블록, 압축모드) 명시

FTP

- FTP 응답
  - 사용자-PI가 제어 연결을 통해 서버-PI로 명령을 보낼때의 응답
  - 응답 코드와 응답 메시지텍스트로 구성되어 클라이언트에게 보내짐
  - 응답의 목적
    - 서버가 명령을 받았다는 것 확인
    - 명령을 받아들였는지, 에러가 발생했다면 어떤 에러가 발생했는지 클라이언트게 알려줌
    - 세션 사용자에게 전송의 상태 등 다양한 정보 전송

- FTP 응답코드
  - xyz로 구성
    - x: 명령에 성공, 실패 여부;성공한 명령이 완료되었는지,완료가 덜되었는지;실패한 명령을 다시 시도해야 하는지
    - y: 메시지 기능에 따른 그룹
    - z: y로 분류된 각 그룹에서 특정 메시지를 가리킴
    - 예시) 응답코드:530(로그인 실패)



▪FTP 응답코드

- 첫번째 자리수(x)의 해석

응답코드 형식	의미	설명
1yz	긍정적 사전 응답	서버가 명령을 받아들였고 아직 처리중이라는 것을 뜻하는 초기 응답 메시지
2yz	긍정적 완료 응답	명령을 성공적으로 처리하였고 처리 완료
3yz	긍정적 중간 응답	서버가 명령을 받아들이기는 했지만 추가정보를 기다리고 있기 때문에 처리가 늦춰진 상태; 일련의 명령 중간에 사용(ex)로그인 과정에서 USER명령 다음 PASS 명령 보내기 전)
4yz	일시적인 부정적 완료 응답	서버가 명령을 받아들이지 않았고아무런 행동도 취하지 않았지만 일시적인 에러이기 때문에 명령을 후에 다시 내려도 되는 상태(ex)일시적인 오류, 파일요청시 다른 자원이 그 파일을 사용중일때)
5yz	영구적인 부정적 완료 응답	서버가 명령을 받아들이지 않았고, 아무런 행동을 취하지 않음; 같은 명령을 내려도 같은 에러가 남(ex) 서버에 없는 파일 요청, 존재하지 않은 명령 보냄)

FTP 응답코드

- 두번째 자리수(y)의 해석

응답코드 형식	의미	설명
x0z	문법	문법 오류, 또는 기타 메시지
x1z	정보	상태 문의 등 정보 요청 메시지에 대한 응답 메시지
x2z	연결	제어 연결이나 데이터연결과 관련된 응답 메시지
x3z	인증과 계정	로그인 과정, 계정 과 관련된 응답 메시지
x4z	미지정	정의되지 않은 그룹
x5z	파일 시스템	서버의 파일 시스템과 관련된 응답 메시지

FTP

▪ FTP 사용자 명령어

사용자 명령어	설명
account <계정명>	서버에 있는 특정 계정으로 접근하기 위해 ACCT 명령 보냄
append <파일명>	APPE 명령을 이용해 파일 뒤에 데이터 추가
binary	이후 모든 전송을 이미지 자료형을 사용하도록 설정(=image명령어)
bye	FTP 세션 종료, FTP 클라이언트 종료(=exit,quit명령어)
cd<디렉토리-경로>	원격서버의 작업 디렉토리 변경
Chmod<파일명>	유닉스시스템에서 파일의 접근 권한 수정
close	현재 FTP 세션을 닫지만 FTP 명령행 유지
delete <파일명>	FTP 서버에 있는 파일 삭제
form <전송형식>	전송 형식을 설정
ftp<ftp-서버>	FTP 서버로의 세션을 염
ls [<파일규정>]	현재 작업디렉토리 목록 출력 및 파일 규정을 만족하는 파일들 출력
open <ftp-서버>	FTP서버로의 세션을 염
site	해당 사이트 전용 명령을 서버로 보냄
user<사용자명>	다른 사용자로 로그인할 때; 서버는 비밀번호 입력요구

TFTP

- TFTP란?
  - Trivial File Transfer Protocol의 약자
  - 가장 기본적인 파일 전송기능만 필요하고 단순하게 하는 것과 프로그램크기를 줄이는 것이 가장 중요한 과제일 경우 사용
  - 69번 port 사용

TFTP

- TFTP와 FTP 비교

	FTP	TFTP
전송	TCP	UDP(개별메시지로 포장)
명령	파일을 주고 받고 삭제하기 위한 명령	파일 보내고 받는 명령
데이터 표현 방식	ASCII, 바이너리, 로컬	ASCII,바이너리 방식
인증	로그인 기능 및 다른 인증기능 지원	없음

TFTP

- TFTP 동작 과정
  - T는 Trivial(간이)이기 때문에 동작이 FTP보다 간단함
  - 포트번호를 전송식별자(TID, Transfer identifier)라고 부름

  - 초기연결 : 클라이언트가 초기화 요청 보내고 서버가 응답
  - 데이터 전송 : 연결 수립 후 TFTP 메시지 교환
  - 연결종료 : 데이터를 담고 있는 마지막 TFTP 메시지를 보내고 응답 메시지를 받으면 연결 종료

TFTP

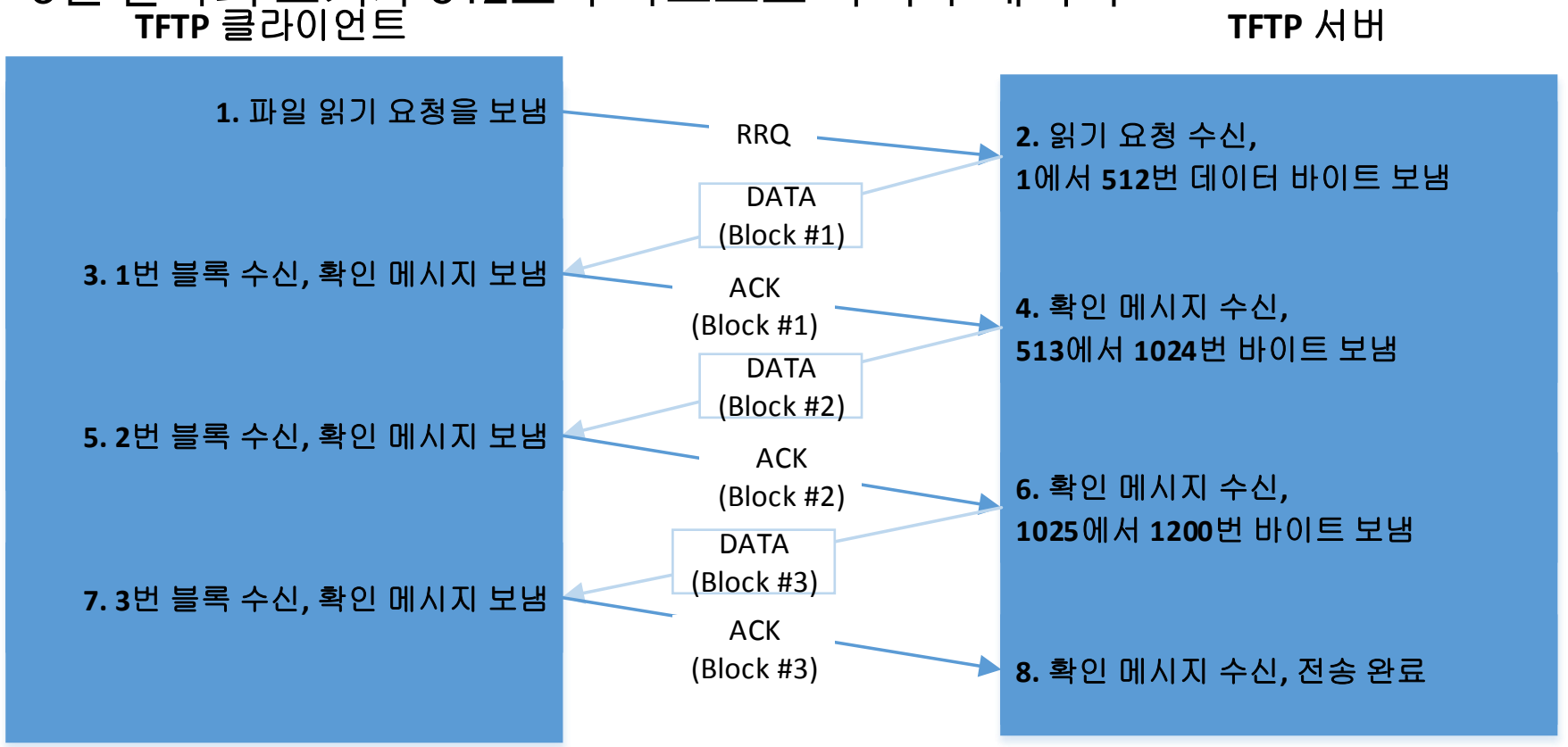
- 록스텝(lock step) 클라이언트/서버 메시징
  - 모든장비가 받는 메시지 하나당 응답메시지를 하나 보내는 방식
  - 재전송 측면에서 TFTP 구현을 간단하게 해줌

TFTP

- 초기 메시지 교환
  - TFTP를 초기화 하기위해 클라이언트가 메시지를 보냄
    - 읽기 요청 메시지(RRQ, read request): 서버에서 클라이언트로 파일 보내달라는 요청
    - 쓰기 요청 메시지(WRQ, write request): 클라이언트에서 서버로 파일 보내겠다는 요청
  - 전송모드 명시
    - ASCII텍스트 파일을 위한 netascii모드
    - 바이너리 파일을 위한 octer 모드
  - 데이터 블록 번호 매기기
    - 모든 데이터 메시지는 0~512바이트까지의 데이터블록을 포함
    - 블록의 번호는 블록을 포함하는 데이터 메시지 헤더에 들어있음
    - 512바이트보다 적게 채워진 메시지는 마지막 데이터 메시지

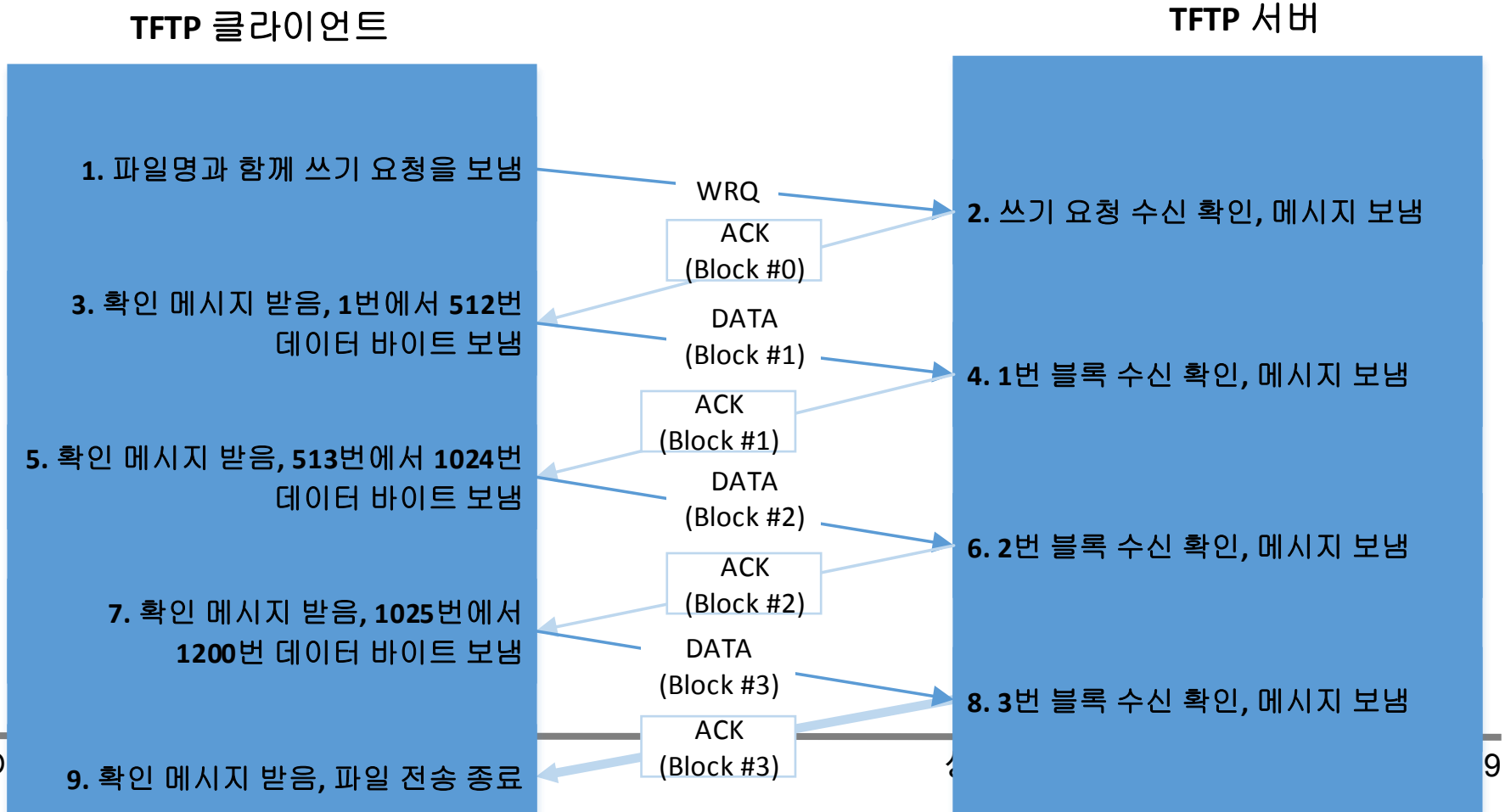
TFTP

- TFTP읽기과정(클라이언트가 1200바이트 파일 읽는다고 가정)
  - 클라이언트가 파일이름과 함께 읽기 요청 메시지 보냄
  - 서버는 1,2,3번 블록을 클라이언트에게 보냄
  - 3번 블록의 크기가 512보다 작으므로 마지막 메시지



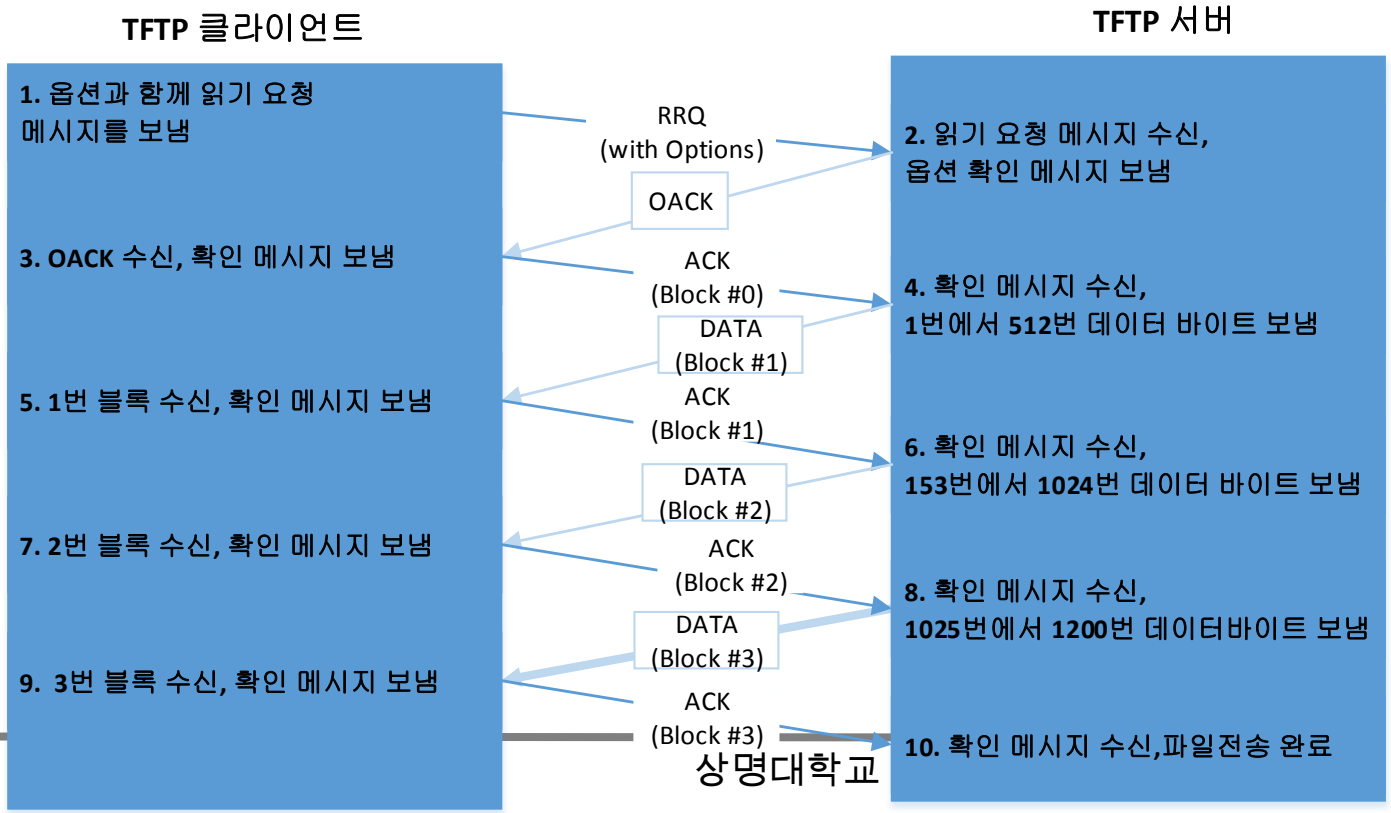
TFTP

- TFTP쓰기과정 (클라이언트가 1200바이트 파일 쓴다고 가정)
  - 클라이언트가 파일이름과 함께 쓰기 요청 메시지 보냄
  - 서버가 첫번째로 보낸 응답 메시지는 데이터를 받기 전에 보냈으므로 블록번호 0번
  - 클라이언트는 1,2,3번 블록을 서버에게 보냄



▪ TFTP옵션 협상(읽기 과정일때 옵션 협상 포함)

- 기본적으로 제공해야 하는 정보 외에 옵션 목록 포함
  - 옵션 코드와 옵션 값으로 표현
- 서버는 자신이 처리할 수 있는 옵션을 OACK에 넣어서 보냄



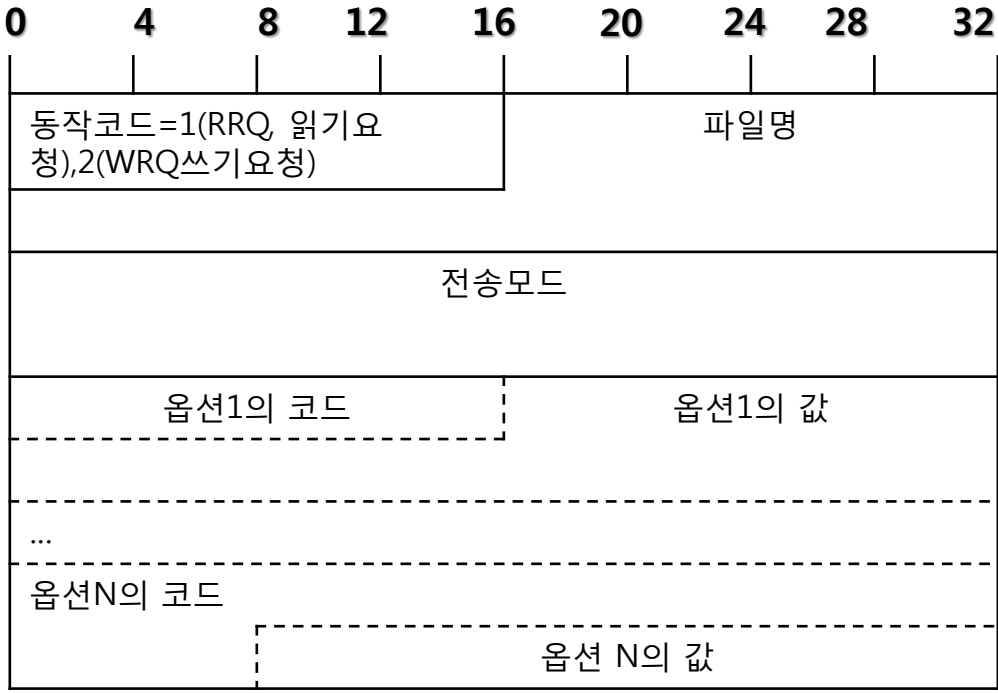
▪ TFTP 옵션

TFTP 옵션 명	TFTP 옵션 코드 (요청 메시지에서 사용)	RFC문서	설명
블록크기	Blksize	2348	효율성 증진이나 사용하는 네트워크의 한계 때문에 클라이언트와 서버가 512바이트 이외의 데이터블록 크기를 사용하도록 함
만료시간	interval	2349	클라이언트와 서버가 재전송 타이머에서 사용할 초 수 에 대해 합의하도록 함
전송크기	tsize	2349	파일을 보내기 전에 파일을 보내는 장비가 파일을 받는 장비에게 파일 크기를 미리 보낼 때 사용

TFTP

- TFTP메시지 형식
  - FTP와는 달리 전통적인 헤더/데이터 형식스킴을 사용하는 UDP에서 동작
  - 읽기요청과 쓰기 요청 메시지

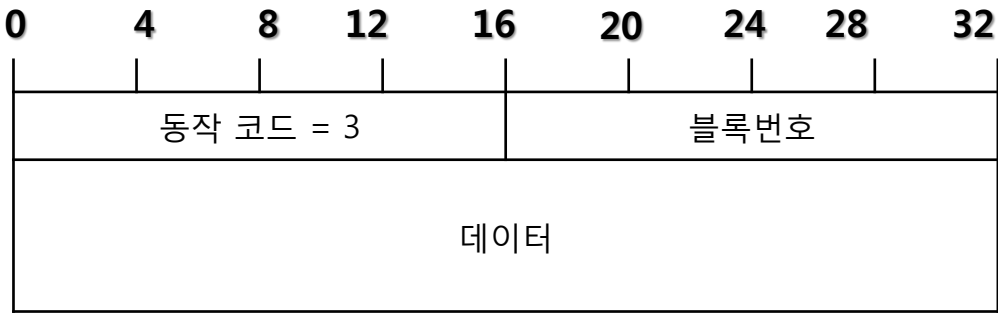
필드 명	크기 (바이트)	설명
동작코드	2	동작코드: TFTP메시지 형식을 지칭
파일명	가변	읽거나 쓸 파일의 이름
모드	가변	전송모드: 널로 끝을 표시한 "netascil" 이거나 "octer"
옵션	가변	클라이언트가 옵션을 지원할 때 사용 옵션 코드(blksize, interval, tsize) 옵션 값(클라이언트가 해당 옵션값으로 요청하고 있는 값)



▪ TFTP메시지 형식

• 데이터 메시지

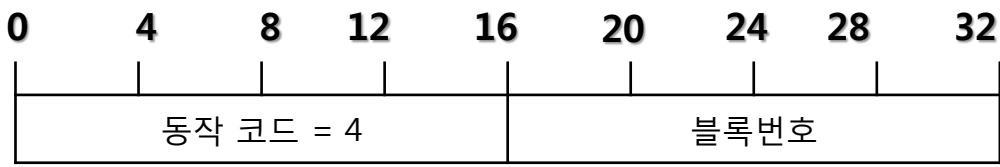
필드 명	크기 (바이트)	설명
동작코드	2	동작코드: TFTP메시지 형식을 지칭. 3은 데이터 메시지
블록번호	2	블록번호: 현재 포함하고 있는 데이터 블록의 번호
데이터	가변	데이터: 0에서 512바이트의 데이터



▪ TFTP메시지 형식

• 응답 메시지

필드 명	크기 (바이트)	설명
동작코드	2	동작코드: TFTP메시지 형식을 지칭. 4는 ACK 메시지
블록번호	2	블록번호: 현재 응답하고자 하는 데이터 블록의 번호, 옵션을 사용하지 않을 때의 쓰기 요청에 대한 응답 메시지이거나 OACK 메시지에 대한 응답 메시지를 보낼 때는 0이라는 값을 사용



▪ TFTP메시지 형식

• 오류 메시지

필드 명	크기 (바이트)	설명
동작코드	2	동작코드: TFTP메시지 형식을 지칭. 5은 오류메시지
오류코드	2	전달하고자 하는 에러의 종류. **0=정의 안됨. 자세한 내용은 오류 메시지 필드 참조.** **1=파일 없음** **2=접근위반** **3=디스크 꽉참, 할당량 초과** **4=불법 TFTP 동작** **5=전송 식별자(TID) 모름** **6=파일 이미 있음** **7=해당 사용자 없음** **8=불가능한 옵션 협상 때문에 클라이언트 전송 중단**
오류메시지	가변	"사람이 이해하기 " 위해 필요한 기술적인 문장

▪ TFTP메시지 형식

• 옵션응답 메시지

필드명	크기 (바이트)	설명
동작코드	2	동작코드: TFTP메시지 형식을 지칭. 6은 OACK 메시지
옵션	가변	서버가 사용하기로 한 옵션의 목록. 옵션 코드 : RRQ메시지나 WRQ 메시지에서 복사한 옵션의 이름 옵션 값 : 서버가 확인 한 값, 옵션에 따라 클라이언트가 제안한 옵션 값이거나 서버가 새롭게 제안한 값일 수 있음

감사합니다!