
CHAPTER 08 **근거리 통신망: 유선 이더넷**

1. IEEE 표준 이더넷	291
2. Ethernet II 프레임 형식	292
3. Ethernet II 덤프 분석	295
요약	301
연습문제	302

CHAPTER 09 **주소 변환 프로토콜(ARP)**

1. 주소 변환	306
2. 주소 변환 프로토콜(ARP)	308
2.1 ARP 패킷 형식	310
2.2 캡슐화	311
2.3 동작	311
2.4 프락시 ARP	314
3. ARP 덤프 분석	315
요약	321
연습문제	322

CHAPTER 10 **인터넷 프로토콜(IP)**

1. 개요	330
2. 데이터그램	331
2.1 IPv6 데이터그램 기본 헤더	338
2.2 흐름 레이블	339
2.3 IPv4와 IPv6 헤더 비교	340
3. 단편화	341
3.1 최대 전달 단위(MTU)	341
3.2 단편화와 관련된 필드	343
4. 옵션	346
4.1 형식	347
4.2 옵션 유형	348
5. 검사합	357

5.1 송신자의 검사합 계산	357
5.2 수신자의 검사합 계산	357
5.3 IP 패킷의 검사합	358
6. IP 패키지	360
6.1 헤더 추가 모듈	361
6.2 처리 모듈	362
6.3 큐	363
6.4 라우팅 테이블	363
6.5 포워딩 모듈	363
6.6 MTU 테이블	363
6.7 단편화 모듈	363
6.8 재조립 테이블	364
6.9 재조립 모듈	365
7. 인터넷 프로토콜(IP) 덤프 분석	366
요약	375
연습문제	376

CHAPTER 11 인터넷 제어 메시지 프로토콜(ICMP)

1. 개요	384
2. 메시지 유형	385
3. 디버깅 도구	400
4. ICMP 패키지	406
5. ping 명령어를 이용한 ICMP 덤프 분석	408
5.1 패킷 캡처 개시와 ping 명령어 실행	408
5.2 패킷 캡처 정지와 내용 확인	412
5.3 ICMP 덤프 분석	413
요약	417
연습문제	418

CHAPTER 12 전송층 개요

1. 개요	428
2. 전송층 서비스	430

2.1 프로세스-대-프로세스 통신	430
2.2 주소 체계: 포트 번호	430
2.3 캡슐화와 역캡슐화	434
2.4 다중화와 역다중화	435
2.5 흐름 제어	436
2.6 오류 제어	439
2.7 흐름 제어와 오류 제어의 결합	440
2.8 혼잡 제어	442
2.9 비연결형과 연결형 서비스	444
3. 전송층 프로토콜	446
3.1 단순 프로토콜	447
3.2 정지-후-대기 프로토콜	448
3.3 <i>N</i> -프레임-후퇴 프로토콜	453
3.4 선택적 반복 프로토콜	461
3.5 양방향 프로토콜: 피기백킹	466
요약	468
연습문제	469

CHAPTER 13 사용자 데이터그램 프로토콜(UDP)

1. 개요	474
2. 사용자 데이터그램	475
3. UDP 서비스	478
3.1 프로세스-대-프로세스 통신	478
3.2 비연결형 서비스	479
3.3 흐름 제어	480
3.4 오류 제어	480
3.5 혼잡 제어	482
3.6 캡슐화와 역캡슐화	482
3.7 큐잉	484
3.8 다중화와 역다중화	485
3.9 UDP와 일반 단순 프로토콜과 비교	486
4. UDP 응용	486
4.1 UDP 특징	487
4.2 대표적인 응용	488
5. UDP 패키지	489

5.1 제어 블록 테이블	490
5.2 입력 큐	490
5.3 제어-블록 모듈	490
5.4 입력 모듈	491
5.5 출력 모듈	491
5.6 예제	492
6. UDP 덤프 분석	494
요약	497
연습문제	498

CHAPTER 14 전송 제어 프로토콜(TCP)

1. TCP 서비스	508
1.1 프로세스-대-프로세스 통신	509
1.2 스트림 전달 서비스	510
1.3 전이중 통신	512
1.4 다중화와 역다중화	512
1.5 연결형 서비스	513
1.6 신뢰성 서비스	513
2. TCP 특징	513
2.1 번호화 시스템	513
2.2 흐름 제어	515
2.3 오류 제어	516
2.4 혼잡 제어	516
3. 세그먼트	516
3.1 형식	516
3.2 캡슐화	519
4. TCP 연결	520
4.1 연결 설정	520
4.2 데이터 전송	523
4.3 연결 종료	526
4.4 연결 재설정	529
5. 상태 천이 다이어그램	529
5.1 시나리오	531
6. TCP 창	533
6.1 송신 창	534

6.2 수신 창	535
7. 흐름 제어	536
7.1 창 열기와 닫기	537
7.2 창 축소	537
7.3 어리석은 창 신드롬	538
8. 오류 제어	541
8.1 검사합	541
8.2 확인응답	541
8.3 재전송	543
8.4 순서가 어긋난 세그먼트	544
9. 혼잡 제어	545
9.1 혼잡 창	545
9.2 혼잡 제어 원칙	545
10. TCP 타이머	550
10.1 재전송 타이머	550
10.2 영속 타이머	551
10.3 킵얼라이브 타이머	551
10.4 시간 대기 타이머	552
11. 옵션	552
12. TCP 패키지	555
12.1 전송 제어 블록	556
12.2 타이머	557
12.3 메인 모듈	557
12.4 입력 처리 모듈	560
12.5 출력 처리 모듈	561
13. TCP 덤프 분석	561
요약	572
연습문제	574

PDF 파일 제공

CHAPTER 15 응용층 개요

1. 클라이언트-서버 개념	586
1.1 서버	588
1.2 클라이언트	588
1.3 동시성	588

1.4 서버의 동시성	589
1.5 소켓 인터페이스	591
1.6 UDP를 이용한 통신	602
1.7 TCP를 이용한 통신	606
1.8 미리 정의된 클라이언트 서버 응용들	612
2. Peer-to-peer 개념	613
요약	614
연습문제	615

CHAPTER 16 동적 호스트 설정 프로토콜(DHCP)

1. 개요	620
1.1 이전 프로토콜	621
2. DHCP 동작 절차	622
3. 설정	630
3.1 정적 주소 할당	630
3.2 동적 주소 할당	630
3.3 상태 천이	631
3.4 초기(INIT) 상태	632
3.5 선택(SELECTING) 상태	632
3.6 요청(REQUESTING) 상태	633
3.7 바운드(Bound) 상태	633
3.8 재설정(Renewing) 상태	633
3.9 재연결(Rebinding) 상태	633
3.10 다른 이슈들	633
3.11 메시지 교환	634
4. DHCP 패킷 분석	635
4.1 Discover 패킷	636
4.2 Offer 패킷	638
4.3 Request 패킷	639
4.4 Acknowledgement 패킷	640
4.5 DHCP 임대 갱신	641
요약	642
연습문제	643

CHAPTER 17 도메인 이름 시스템(DNS)

1. DNS의 필요성	648
2. 이름 공간	650
2.1 계층적 이름 공간	650
2.2 도메인 이름 공간	651
2.3 도메인	653
2.4 이름 공간의 분산	654
3. 인터넷에서 사용되는 DNS	657
3.1 일반 도메인	657
3.2 국가 도메인	658
3.3 인버스 도메인	659
3.4 도메인 관리 체계	660
3.5 한국의 DNS 관리 체계	662
4. 변환	663
4.1 변환기	664
4.2 재귀적 변환	665
4.3 반복적 변환	666
4.4 캐싱	667
5. DNS 메시지	668
5.1 헤더	668
6. 레코드 유형	671
6.1 조회 레코드	671
6.2 자원 레코드	673
7. 캡슐화	675
8. DDNS	675
9. DNS 보안	676
10. DNS 덤프 분석	676
요약	683
연습문제	684

CHAPTER 18 WWW와 HTTP

1. WWW의 구조	699
1.1 하이퍼텍스트와 하이퍼미디어	701
1.2 웹 클라이언트	701

1.3 웹 서버	702
1.4 단일 자원 위치기(URL)	702
2. 웹 문서	703
2.1 정적 문서	703
2.2 동적 문서	703
2.3 액티브 문서	706
3. 하이퍼텍스트 전송 프로토콜(HTTP)	708
3.1 HTTP 트랜잭션	709
3.2 조건부 요청	715
3.3 영속성	716
3.4 쿠키	718
3.5 웹 캐시: 프락시 서버	721
3.6 HTTP 보안	722
4. HTTP 덤프 분석	723
4.1 HTTP 요청 메시지	723
요약	730
연습문제	731

PDF 파일 제공

부록

부록 1 ASCII 문자 코드표	740
부록 2 Microsoft Edge와 Chrome에서 캐시 삭제 방법	741

참고문헌	745
찾아보기	746

PDF 다운로드 안내

15장, 16장, 부록은 PDF 파일로 제공합니다. 생능출판사 홈페이지(www.booksr.co.kr)에서 'wireshark로 배우는 컴퓨터 네트워크' 또는 저자명으로 검색 후 보조자료에서 다운로드 받을 수 있습니다.

01

CHAPTER

개요

contents

1. 인터넷의 역사
2. 프로토콜과 표준
3. 표준화 기구
4. 인터넷 표준
5. 인터넷 관리

01

CHAPTER

개요

학습 목표

- 인터넷에 대한 국제 및 국내의 간단한 역사를 배운다.
- 인터넷을 설명할 때 자주 사용되는 프로토콜과 표준에 대한 정의를 알게 된다.
- 표준을 제정하는 국제 표준화 기구와 국내 표준 제정 기관을 설명할 수 있다.
- 인터넷 표준을 규정하고 이들 표준이 개발된 메커니즘을 설명할 수 있다.
- 인터넷 관리기관과 이와 관련된 기관에 대해 알게 된다.

오늘날 인터넷(Internet)은 우리의 일상생활에 엄청난 변화를 가져왔다. 휴가를 위한 여행 정보를 얻는 방법에서부터 사업에 이르기까지 거의 모든 분야에 영향을 주었다. 최근에 인터넷을 사용하는 방법을 살펴보면 개인적으로나 사업적으로 전자우편을 보내고, 각종 증명서를 발급받고, 공공요금을 지불하고, 전 세계의 신문을 읽을 수 있고, 사고 싶은 물건을 구매하고, 영화나 연극 또는 호텔, 기차, 비행기 표를 예약할 수 있는 것은 모두 인터넷을 사용할 수 있으므로 가능하게 된 것이다.

인터넷은 구조적이고 조직화되어 있는 시스템이다. 인터넷의 동작 과정과 TCP/IP에 계층구조를 이해하기 위해 먼저 간단하게 인터넷에 대한 역사를 설명한다. 물론 우리나라에서 진행되었던 인터넷과 관련된 초고속통신망의 발전과정도 살펴본다. 그런 다음 각 프로토콜의 개념과 표준, 그리고 서로에 대한 관계를 설명한다. 아울러 인터넷 표준 개발과 관련된 여러 기관을 설명한다. 이 표준은 어떤 특정 기관에 의해서가 아니라, 많은 사용자가 의견 교환을 통하여 개발되고 있다. 표준이 만들어지고 발전해 가는 메커니즘에 대해서도 살펴보도록 한다. 또한, 이 장에서는 인터넷을 관리하는 그룹과 간단한 역사에 대해서도 살펴보도록 한다.

1. 인터넷의 역사

네트워크(network, 또는 망)는 컴퓨터나 교환기, 라우터와 같은 통신 장치들을 서로 연결한 그룹이다. 인터넷(internet-소문자 i)은 서로 통신할 수 있는 둘 또는 그 이상의 네트워크이다. 인터넷(Internet-대문자 I)이라 부르는 가장 대표적인 인터넷(소문자 i)은 100만 개 이상의 네트워크가 상호 연결된 네트워크이다. 전 세계적으로 거의 모든 국가에서 정부 기관, 학교, 연구기관, 회사와 도서관 등과 같은 기관뿐만 아니라 일반 개인들도 인터넷을 사용하고 있다. 이 중의 대부분은 일반 사용자이다. 이렇게 엄청난 규모의 통신 시스템은 1969년부터 시작되었다.

1.1 ARPANET

1960년대 중반에 연구기관의 대형 컴퓨터들은 독립 실행형(stand-alone) 장비였으며 제조업자가 다른 컴퓨터끼리 서로 통신을 할 수 없었다. 미국 국방성(DOD: Department of Defense)의 ARPA(Advanced Research Project Agency)에서 연구원들이 비용도 줄이고, 중복 연구가 이루어지지 않도록 연구 내용을 공유하기 위하여 컴퓨터를 서로 연결하는 방법을 연구하게 되었다.

1967년 ACM(Association for Computing Machinery) 모임에서 ARPA는 컴퓨터를 연결한 소규모 네트워크인 ARPANET에 대한 아이디어를 제안하였다. 이 아이디어는 각 컴퓨터(제조업자가 서로 다른)를 IMP(Interface Message Processor)라는 특정 컴퓨터에 연결하는 것이었다. 그런 다음 IMP들을 서로 연결하였다. 각 IMP는 연결된 호스트뿐만 아니라 다른 IMP와 통신할 수 있는 기능이 있었다.

1969년에 ARPANET는 IMP를 통하여 4개의 노드인 로스엔젤레스(LA)에 있는 캘리포니아주립대학(UC)과 산타바바라(SB)에 있는 캘리포니아주립대학(UC), 스탠포드연구소(SRI), 그리고 유타대학(University of Utah)에 있는 호스트를 연결하여 네트워크를 구성하였다. 이때 NCP(Network Control Protocol)라는 소프트웨어가 호스트 간의 통신을 제공하였다.

1.2 인터넷의 탄생

1972년에 ARPANET 그룹의 핵심 멤버인 빈트 서프(Vint Cerf)와 밥 칸(Bob Kahn)은