



기말고사

바이트 스테핑 사용 이유 및 방법

문자 중심 프로토콜의 프레임 짜기 중 플레그와 같은 형태의 데이터가 플레그로 오인 받지 않게하기 위해 사용

텍스트에 플레그나 탈출문자가 있을 때마다 여분의 탈출문자를 추가하는 처리

비트 스테핑 사용 이유 및 방법

비트 중심 프로토콜의 프레임 짜기 중 플레그와 같은 비트 형태의 데이터를 플레그로 오인 받지 않기 위해 사용

0 뒤에 연속하는 다섯 개의 1인 경우 그 뒤에 0을 추가하는 방법으로 처리

데이터 링크 계층에서 MAC 프로토콜을 사용하는 이유

네트워크 상의 여러 장치가 공유하는 매체에 대한 접근을 제어할 때 사용되며,
여러 장치가 동시에 데이터를 전송하려고 할 때 충돌이 발생하지 않도록 조정하고
매체 접근을 조정하여 효율적인 데이터 전송을 가능하게 하기위해 사용됨.

MAC 프로토콜 중 제어 접근 방식 3개

1. 예약 (Reservation)
2. 폴링 (Polling)
3. 토큰 패싱 (Token passing)

MAC 프로토콜 중 임의 접근 방식 방식 3개

1. 알로하
2. CSMA/CD → Carrier Sense Multiple Access with Collision Detection
충돌 검출 반송파 감지 다중 접속
3. CSMA/CA → Carrier Sense Multiple Access with Collision Avoidance
충돌 회피 반송파 감지 다중 접속

MAC 프로토콜 중 채널화 방식 3개

1. FDMA (주파수) Frequency Division Multiple Access
2. TDMA (시간) Time-Division Multiple Access
3. CDMA (코드) Code-Division Multiple Access

CSMA/CD와 ALOHA 차이

1. 지속 과정 추가

CSMA/CD에 1-persistent method 추가

2. 충돌 신호 전송

CSMA/CD → jam-signal(충돌 시그널) 사용, ALOHA → 시간 내 ACK 못받으면 충돌로 간주 후 재전송

3. 프레임 전송 방식

ALOHA에는 전송 절차가 따로 없음, CSMA/CD → 충돌 감지 체크 후 전송

CSMA/CD 예제

■ 예제 12.5: CSMA/CD를 사용하는 네트워크의 대역폭이 10 Mbps 이다. 최대 전파 시간(장치에서의 지연 시간을 포함하되 충돌을 알리는 데 걸리는 시간을 무시)은 $25.6\mu\text{s}$ 이다. 최소 프레임의 크기는?

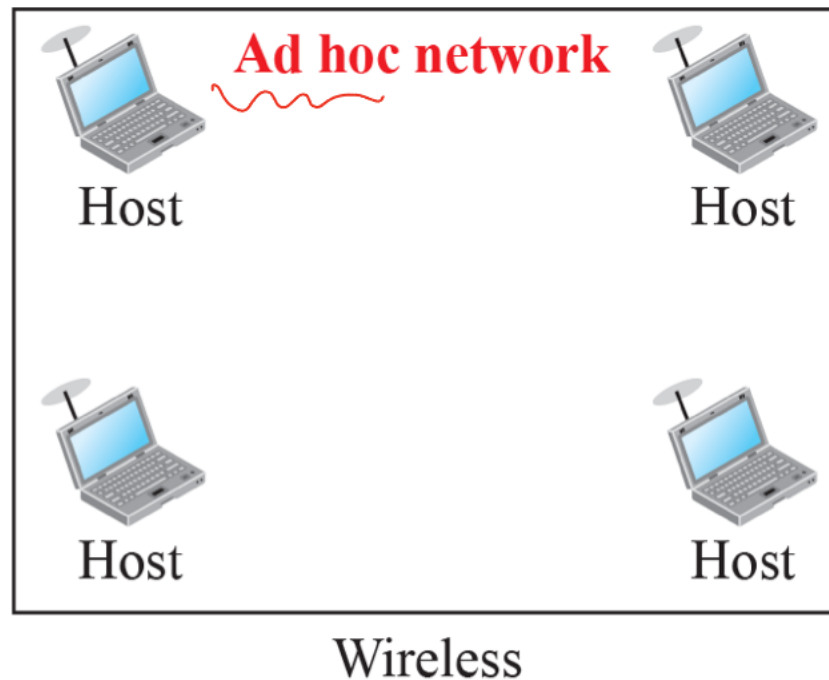
■ 해답: 최소 프레임 전송 시간은 $T_f = 2 \times T_p = 51.2 \mu\text{s}$. 이는 최악의 경우에는 지국이 전송하면서 충돌 여부를 확인하기 위해서는 최소 $51.2 \mu\text{s}$ 동안 기다려야 한다는 것을 의미한다. 프레임의 최소 크기는 $10 \text{ Mbps} \times 51.2 \mu\text{s} = 512\text{비트}$, 즉 64바이트이다. 이는 뒤의 상에서 보겠지만 실제로 표준 이더넷 프레임의 최소 크기이다.

CSMA/CA 충돌 회피 전략

1. 프레임 간 공간 (IFS / Interframe Space)
2. 경쟁 구간 (Contention window)
3. 응답 (Acknowledgement)

애드혹이란 ?

서로 자유롭게 통신하는 호스트의 집합



WLAN에서 CSMA/CD 사용 불가능한 이유

1. 프레임 송신과 충돌 신호 수신을 동시에 수행하기 위한 충분한 전력을 갖지 못함
2. 숨겨진 지국 문제로 충돌이 발생하여도 감지되지 않을 수 있음
3. 거리가 멀어 신호감쇠가 발생할 수 있으며, 이로 인해 충돌을 감지하지 못할 수 있음

NAV란?

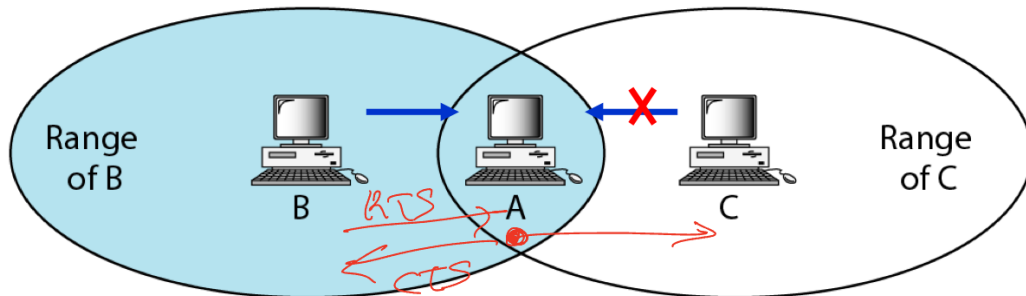
Network Allocation Vector의 약어로 특정 무선 장치가 매체를 점유하고 있을 때

다른 장치들이 전송을 시도하지 않도록 막는 역할

전송을 시작하기전에 NAV 값을 확인하여 매체가 현재 사용 중인지 여부를 판단

숨겨진 지국 문제란?

다른 영역의 지국과 전송중인 지국에 데이터를 전송하여 충돌이 발생할 수 있는 문제

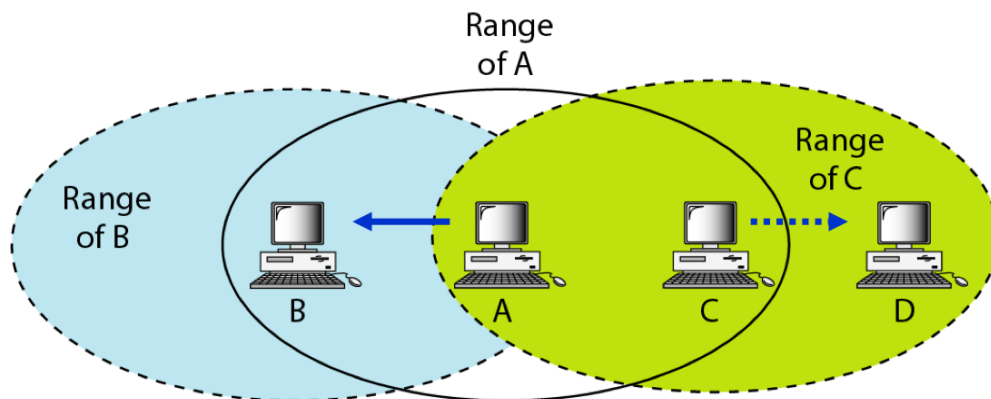


B and C are hidden from each other with respect to A.

RTS와 CTS를 사용하여 해결이 가능하다.

노출된 지국 문제란?

지국이 실제 사용할 수 있는 채널의 사용을 자제하는 문제



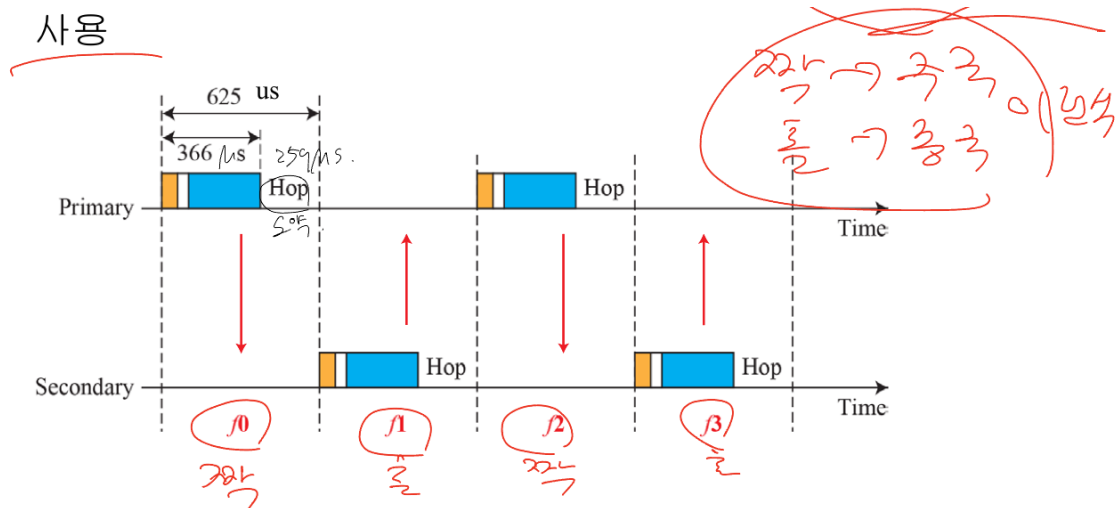
C is exposed to transmission from A to B.

C는 A가 전송하는 것을 감지하고 전송을 자제

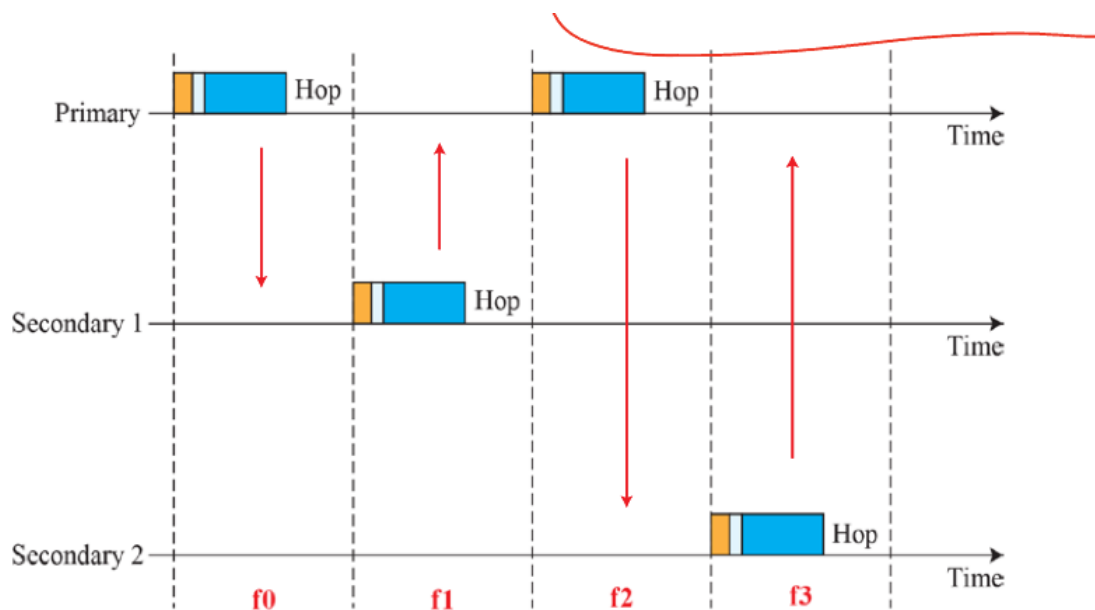
단일 종국 통신, 다중 종국 통신이란?

블루투스에는 TDD-TDMA(Time division duplex TDMA)을 사용한다.

단일 종국 통신은 시간을 슬롯으로 나눈 뒤 주/종국은 각각 짝/홀수 슬롯을 사용하는 것이고



다중 종국 통신은 poll/select와 유사한 방법으로 종국이 지정된 순서에 따라 번갈아가며 데이터를 전송하는 것



주국과 중국 간 링크 존재

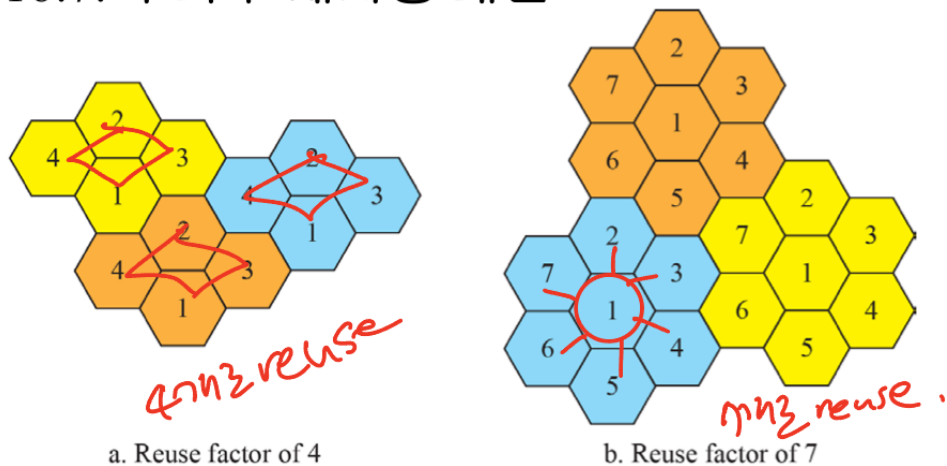
- SCO (Synchronous Connection-oriented) : 동기 연결 지향
: 대기시간을 피하는 것이 오류없는 전송(무결성)보다 중요할 경우
- ACL (Asynchronous Connectionless) : 비동기 비연결
: 데이터의 무결성이 지연보다 중요 → 재전송 사용(stop & wait 사용)

셀 방식에서 주파수 재사용 원칙

셀에서 전부 다른 주파수를 사용하면 주파수가 모자람.

한 패턴에서 같은 번호를 가진 셀들은 같은 주파수 집합을 사용하는 것을 말함

□ 그림 16.7: 주파수 재사용 패턴 ✓



핸드오프 (Hand off)란?

통화 중에 이동국이 한 셀에서 다른 셀로 이동하는 것

하드 핸드오프

- 핸드오프 시 새로운 기지국과 통신이 설정되기 전 이전 기지국과 통신이 먼저 끊어지는 것

소프트 핸드오프

- 핸드오프 시 이동국이 동시에 두 기지국과 통신

Loop 문제 & 해결방안?

시스템의 신뢰성을 위해 한 쌍의 LAN에 하나 이상의 스위치가 설치되었을 경우, Loop를 형성할 수 있음

각 스위치에서 flooding 한 프레임이 다른 스위치로 유입되면서 loop를 돌며 프레임 복사가 반복됨

Spanning Tree Algorithm으로 해결

VLAN 이란?

가상 근거리 네트워크로 서로 다른 물리적엔 LAN에 속해 있을 때 두 지국 사이의 가상 연결을 만드는 것

피지배킹 (Piggybacking)

데이터를 보낼 때 ACK의 순서 번호를 같이 보내는 방식으로, ACK message의 추가적인 생성이 없어도 된다.

PPP (Point to Point Protocol)

→ 세 가지 내부 프로토콜이 다중화가 됨

1. 링크 제어 프로토콜 (LCP, Link Control Protocol) → 데이터 링크층 연결 설정 및 해제
2. 인증 프로토콜 (AP, Authentication Protocol) → 인증 관련 프로토콜
3. 네트워크 제어 프로토콜 (NCP, Network Control Protocol) → 네트워크 계층 연결 설정 및 해제

OSI 계층에서 데이터 링크 계층에 해당하는 프로토콜이 아닌 것?

→ 데이터 링크층의 프로토콜에는 정지/대기 프로토콜(HDLC)만 존재

HDLC

- 비트 중심 프로토콜
- 정지 / 대기 프로토콜로 구현
- PPP나 이더넷 프로토콜 및 무선 LAN 프로토콜의 기본
- 흐름제어 및 에러 제어 가능
- 두 가지 전송 모드를 제공
 - 정규 응답 모드 (NRM) / 은행 ATM 기
: 주국과 종국으로 구성, Point to Point, MultiPoint로 구성 (점 대 점, 다중점)
 - 비동기 균형 모드
: 각 지국은 주국이자 종국 (점 대 점)

HDLC 프레임 종류

1. 정보 프레임 (I-프레임, Information frames) → 데이터를 실어 나르는 용도
2. 감시 프레임 (S-프레임, Supervisory frames) → 흐름 제어, 오류 제어
3. 무번호 프레임 (U-프레임, Unnumbered frames) → 연결 장치 간 세션 관리, 제어 정보 교환