국가기술자격 기술사 시험문제

기술사 제 110 회 제 2 교시 (시험시간: 100분)

분야	정보통신	종목	컴퓨터시스템응용기술사	수험번호		성명	

※ 다음 문제 중 4문제를 선택하여 설명하시오. (각25점)

1. 데이터베이스 보안이 추구하는 3대 요소와 데이터의 무결성 저하 유형에 대하여 설명하시오.

2. 가상현실(VR : Virtual Reality)과 증강현실(AR : Augmented Reality)에 대하여 다음 내용을 설명하시오.

   1) VR과 AR 정의
   2) VR과 AR 차이점
   3) VR 및 AR 사례

3. 데이터 전송 오류가 발견된 경우 Data Link Layer에서 오류 복구를 수행하는 절차에 대하여 설명하시오.

4. 버스 상에 여러 노드가 연결된 경우 이용될 수 있는 HDLC(High-level Data Link Control)의 동작 모드를 설명하시오.

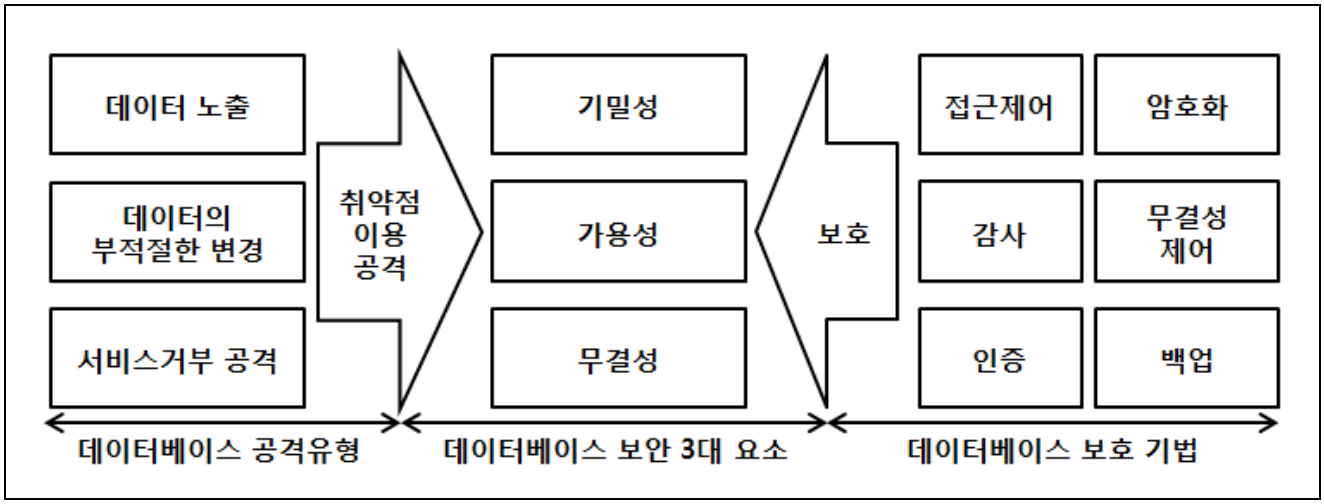
5. UV EPROM(UltraViolet Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM) 및 Flash 메모리를 쓰기(소거 및 프로그램) 관점에서 비교 설명하시오.

6. 방화벽, 침입탐지 시스템(IDS: Intrusion Detection System), 침입방지 시스템(IPS: Intrusion Prevention System) 및 웹 방화벽의 개념과 기능을 설명하시오.

종 목	문 제
컴퓨터시스템응용기술사	**2교시 1번**
데이터베이스 보안이 추구하는 3대 요소와 데이터의 무결성 저하 유형에 대하여 설명하시오..	

도메인/토픽	데이터베이스 > 데이터베이스 보안
키워드	기밀성, 무결성, 가용성 인식불가 데이터, 중복 데이터, 모순된 데이터, 데이터 이상, 데이터 읽기 비일관성, 데이터 비동시성
풀이 가이드	1. 위협과 위험으로부터의 데이터 보호, 데이터베이스 보안의 필요성 2. 데이터베이스 보안이 추구하는 3대요소 3. 무결성 저하 유형 4. 데이터베이스 보안이 추구하는 3대 요소 충족을 위한 방안
필수항목 /연관토픽	정보보안 3요소, 무결성 저하유형 접근제어, 암호화, 인증, 동시성 제어, 회복기법, 정규화
참고문헌	데이터베이스 보안 가이드라인, 한국 데이터베이스 진흥원, 2011 DB 보안 목적 및 필요성, DBGuide.net (http://www.dbguide.net/db.db?cmd=view&boardUid=152792&boardConfigUid=9&categoryUid=216&boardIdx=142&boardStep=1)
Advice	데이터베이스 보안의 목적에 대해 알고 있는지를 확인하는 문제로, 정보보안 3대 요소와 데이터 무결성에서 유추하여 작성도 가능합니다. 차별화를 위해 4단락에 데이터베이스 보안 3대 요소를 유지하기 위한 실무적인 방안을 제시한다면 고득점을 얻을 수 있을 것으로 보입니다.
작성자	108회 컴퓨터시스템응용기술사 / 심동욱 (itpe.gommaro@gmail.com)

1. 위협과 위험으로부터의 데이터 보호, 데이터베이스 보안의 개요



- IT 보안체계 취약점을 이용한 각종 공격(데이터 노출, 변조, 파괴 등)으로부터, 저장된 데이터 자산의 보호 및 신뢰성 제공, Compliance준수를 위한 데이터베이스 보안이 필요.
- 데이터베이스 보안 3대 요소 유지를 통하여 데이터베이스 보안 달성 가능.

2. 데이터베이스 보안이 추구하는 3대 요소

가. 데이터의 보호, 기밀성 (Confidentiality)

정의	- 선별적인 접근 체계를 만들어 인가되지 않은 개인이나 시스템에 의한 접근에 따른 정보 공개/노출을 차단.	
침해방식	Shoulder Sniffing	- 사용자의 어깨너머로 스크린에 보이는 데이터 관찰
	Traffic 분석	- 데이터베이스와 사용자 간 Traffic 분석으로 데이터 관찰.
	사회공학적 기법	- 해당 데이터에 권한접근이 있는 사람으로 가장하여 데이터접근
유지방안	접근 통제	- 데이터 분류 및 접근 권한 분류 및 권한 할당
	암호화	- 제 3자 획득 시 데이터 내용의 판별 불가

- 기밀성은 데이터베이스 내 중요 개인정보를 저장한 사람들의 프라이버시를 위한 최소 필수조건.

나. 데이터에 대한 원활한 접근, 가용성 (Availability)

정의	- 정당한 권한을 가진 사용자나 애플리케이션에 대해 원하는 데이터에 대한 원활한 접근을 제공하는 서비스를 지속할 수 있도록 보장.	
침해방식	DoS (Denial of Service)	- 데이터베이스 서버의 자원을 부족하게 하여 서비스를 제공하지 못하도록 하는 공격
	서비스 장애	- 정전, HW 고장, 시스템 업그레이드 시 장애, DB 오류발생
유지방안	DoS 대응	- CAR 감시, Router Filtering, Black / Sink hole 이용
	고가용 시스템	- 서비스 장애 발생 시 복구

- 허가된 사용자의 데이터베이스의 사용을 지속하기 위한 보안 요소.

다. 데이터의 위변조 및 파괴 방지, 무결성 (Integrity)

정의	- 정당한 방법에 의하지 않고선 데이터가 변경될 수 없으며, 데이터의 정확성 및 완전성과 고의/악의로 변경되거나 훼손 또는 파괴되지 않음을 보장.	
침해방식	데이터 변경 및 위조	- 원 데이터를 다르게 변경하여 삽입.
	시간차 공격	- 데이터 전달 순서 변경, 고의 지연
	Replay 공격	- 중복 데이터의 삽입.
유지방안	접근 통제	- 사용자의 데이터 변경 권한 검증
	의미적 무결성 제약	- 갱신 데이터의 의미적 정확성 검증
	복구시스템	- HW / SW 고장으로부터의 일관성 보장
	동시성 제어	- 동시 트랜잭션 수행 시 데이터 무결성 보장

- 데이터의 정확성, 완전성을 위해, 데이터 무결성 저하 유형을 파악하여 선 조치가 필요.

3. 데이터 무결성 저하유형

가. 잘못된 데이터 설계에 따른 데이터 무결성 저하유형

유형구분	설명
중복 데이터 (Redundant Data)	- 동일한 데이터가 여러 곳에 저장될 때 발생 - 데이터 비일관성과 데이터 이상 유발 가능성 존재
모순된 데이터 (Inconsistent Data)	- 분산되어 저장된 중복데이터가 서로 동일하지 않을 경우에 발생
데이터 이상 (Data Anomalies)	- 정규화되지 않은 데이터 설계로 인해 중복 데이터가 존재하는 상황에서 중복 데이터의 한쪽은 변경이 일어나고, 다른 한쪽은 변경이 일어나지 않을 경우에 발생

- 데이터 정규화 절차를 따르지 않은 잘못된 데이터 설계에 따른 무결성 저하.

나. 읽기 일관성 미지원 / 데이터 미검증에 따른 무결성 저하유형

유형구분	설명
인식불가 데이터 (Invalid Data)	- 유효하지 않은 데이터가 발생하지 않도록 검토와 검증절차(DB Constraints)를 거치지 않아, 입력/저장된 모든 데이터가 예외사항 없이 미유효
데이터 읽기 비일관성 (Data read inconsistency)	- 사용자가 항상 마지막으로 커밋된 데이터를 읽지 못하고, 또한 사용자가 변경한 내용이 커밋되기 전에 다른 사용자에게 노출
데이터 비동시성 (Data Noconcurrency)	- 복수의 사용자가 동시에 데이터에 접근하여 읽을 수 있지만 읽기 일관성을 상실

- 사용자의 실수 혹은 고의로 유효하지 않은 데이터를 삽입하거나, 애플리케이션의 입력 데이터 미검증, 혹은 DBMS가 지원하지 않거나 읽기 일관성 특징의 미약 적용이 원인.

4. 데이터베이스 보안이 추구하는 3대 요소 충족을 위한 방안

구분	방안	설명
보안정책	관리적 정책 수립	- 상위 수준에서 DB 보안 개념 및 중요성 정의
	기술적 정책 수립	- DBMS 특화된 보안 기술을 각 주제별로 상세 정의
	지원도구 및 가이드라인	- 기술적 정책의 부산물로 주제에 대한 상세 수행방법과 도구를 정의하고 정의된 가이드 및 도구를 제공
보안기법	접근제어	- 사용자가 DBMS에 로그인 및 SQL을 실행 시, 미리 정의된 보안 규칙에 따라 권한 여부를 판단하여 통제
	암호화	- 비정상적 데이터 유출이 발생할 경우, 비인가자에 의한 데이터 오용을 방지
	작업결재	- 관리자의 승인을 획득하도록 하는 관리적 보안 기술로, 매우 민감한 데이터에 대한 조작이 필요하거나 조회가 필요한 경우에 해당 데이터에 대한 권한을 갖고 있을지라도 승인을 거치도록 하여 엄격하게 관리해야 하는 경우에 적용
	취약점 분석	- 모의해킹(Penetration Test), 내부 보안감사(Security Auditing) 등의 과정을 통해 다양한 DB 취약점들을 도출하여 DB의 전체 보안 수준의 향상을 도모

- 데이터 자산 가치 증가로 인한 데이터의 중요성이 부각됨에 따라 정책적, 기술적 대책을 수립함으로써 데이터베이스 보안의 목표 달성 가능

종 목	문 제
컴퓨터시스템응용기술사	2교시 2번

가상현실(VR: Virtual Reality)과 증강현실(AR: Augmented Reality)에 대하여 다음 내용을 설명하시오
1) VR과 AR의 정의
2) VR과 AR의 차이점
3) VR 및 AR사례

도메인/토픽	디지털서비스 > 가상현실
키워드	인터렉션, 오감, 가상세계, 현실세계
풀이 가이드	VR과 AR의 차이점을 명확하게 설명하고 사례는 넓게 펼쳐서 설명 1. 정의, 필요에 따라 부각 배경 기재 가능 2. VR과 AR의 차이점, 가, 나로 분리하여 MECE하게 설명 3. VR과 AR의 사례, 가, 나로 분리하여 넓은 관점으로 설 4. VR과 AR의 한계점과 극복방안, 혹은 산업 활성화 방안
필수항목 /연관토픽	VR, AR, MR
참고문헌	주간기술동향 1754호(현실로 다가 온, VR/AR), 정보통신기술진흥센터, 2016. 7. 13 증강현실 그리고 증강휴먼, 한국인터넷진흥원, 2015. 8
Advice	VR과 AR의 정의를 어느 정도 분량으로 쓸지가 고민이었습니다. 실전에서 시험을 보았다면 이 부분에서 고민을 많이 했을 것 같습니다. VR과 AR에 대한 특징이나 관계도를 그려도 좋겠지만 문제에서 묻는 부분이 아니므로 과감히 정의만 작성 후에 차이점과 사례에 집중하는 것을 권장 드립니다. 그리고 4단락에 VR과 AR의 산업 성공을 위한 전략이나 현재 기술적 한계점/극복방안 등 수험자의 VR/AR에 대한 인사이트를 보여주는 쪽에 시간투자를 하면 어떨까 싶습니다. 또한 이 문제는 차별화가 쉽지 않으므로 수험자가 생각하는 VR/AR에 대해서 채점자 눈에 띄도록 전반적으로 답안에 녹여내는 것이 중요하며, 많은 시간을 들여 작성하기 보다는 25분 내에 문제에서 물어본 Fact만 짧게 작성하는 등 전략적 풀이가 필요한 문제라고 생각됩니다.
작성자	108회 컴퓨터시스템응용기술사 / 최정현 (cjhnim@gmail.com)

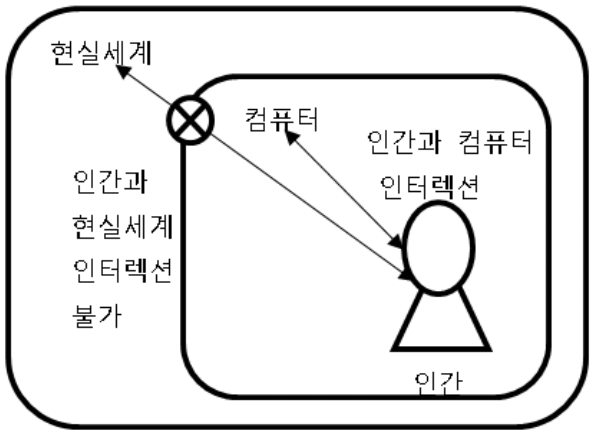
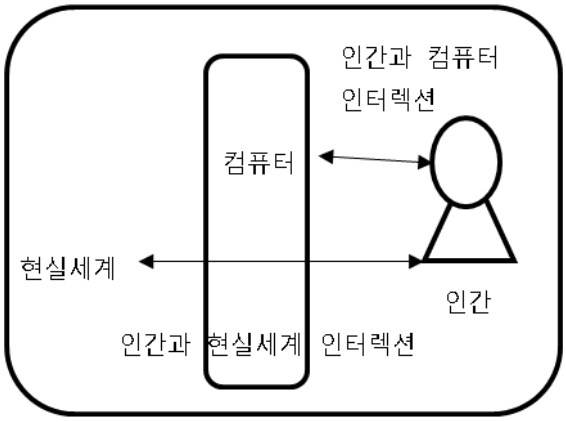
1. VR과 AR의 정의

VR의 정의	- 컴퓨터로 만든 가상세계를 기기를 통해 이용자가 실제 상황처럼 느끼게 해 주는 가상공간
AR의 정의	- 가상세계와 현실세계를 유기적으로 연동하고 3차원적으로 결합한 '확장된 현실'

- VR과 AR은 인간의 오감을 자극하여 가상의 정보를 제공한다는 점에서는 동일하지만 가상의 정보를 제공하는 방식에 있어 근본적 차이 존재

2. VR과 AR의 차이점

가. VR과 AR의 핵심 차이점

VR의 인터렉션	AR의 인터렉션
	

- VR과 AR 모두 컴퓨터와 인간이 인터렉션(Interection)이 가능한 점에서 공통점이 있으나 VR은 인간과 현실세계간 인터렉션(Interection)이 불가능하나 AR은 인간과 현실세계간의 인터렉션(Interection)이 가능한 차이점 존재

나. VR과 AR의 세부 차이점

구분	VR	AR
정보 전달 방식	- 효과가 큰 시각에 초점을 맞춰 산업 발전 중. - 진정한 VR을 위해서는 시각 뿐만이 아닌, 오감자극 효과 개발이 요구됨	- 시각 자극을 통하여 현실세계에 가상 오브젝트 삽입을 통한 서비스 제공
구현 기술 측면	- 멀미현상 해결을 위한 기술 요구 →각 감각기관별 가상현실을 현실과 똑같은 상황으로 재연하는 기술 개발이 필수적으로 요구됨	- 사용자의 이동과 주변 환경 변화에 대응하여 실시간 정보나 컨텐츠를 적응적 제공할 수 있는 기술 필요
적용 디바이스 측면	- 오감을 센싱하기 위한 HMD, Data Glove, 두부(Head) 위치 센서 필요	- 웨어러블 디바이스 혹은 모바일 디바이스를 통한 AR 제공 초점

제공 컨텐츠 측면	- 현실세계에서 직접 실행하기 어려운 사례를 가상세계에서 실시. → 사례: 범죄에 대처하고 예방할 수 있는 'VR범죄예방교육'	- 현실세계에 모의로 실행할 수 있는 사례를 AR로 구현. → 사례: 가구 상점 앱을 통해 직접 제품을 넣어보며 결제 가능

- VR과 AR은 서로 상호 보완적인 관계로 시장 형성될 것으로 예상되며, 이미 수많은 기기들이 보급되고 있으며 플랫폼 경쟁 심화 및 컨텐츠 확보 중요

3. VR과 AR의 사례

가. VR과 AR의 디바이스 사례

구분	사례	설명
VR	데스크탑형	- 페이스북 오큘러스, 소니 플레이스테이션VR, HTC Vive 등
	스마트폰 장착형	- 구글 카드보드, LG 360 VR, 삼성 기어 VR, uSense Impression Pi등
AR	독립기기형	- MS홀로렌즈, BMW AR 글래스
	스마트폰 연계	- 구글 글라스, 인텔 Recon Jet

- 기존 글로벌 IT 기업뿐만 아니라

① '포토닉스 라이트필드' 기술 기반 AR분야에서 관심 받는 업체인 Magic Leap,

② 360도 3D영상 컨텐츠 제작 및 촬영용 네오 카메라 개발사 Jaunt VR,

③ 가상현실HMD와 연동되는 러닝머신 형태의 VIrtuix Omni를 개발한 Virtuix

등 여러 신생기업 창업 및 투자 유치

나. VR과 AR의 플랫폼 사례

구분	사례	설명
소셜플랫폼	페이스북을 통한 가상현실 플랫폼 선언	- 지난 MWC에서 차세대 소셜 플랫폼으로 VR을 점찍으며 생태계 구축을 위한 투자 확대
VR플랫폼	구글의 '데이드림 (Daydream)'	- 구글 I/O 2016에서 가상현실(VR)기기용 게임과 각종 애플리케이션 개발 가능한 플랫폼을 3분기 중 출시

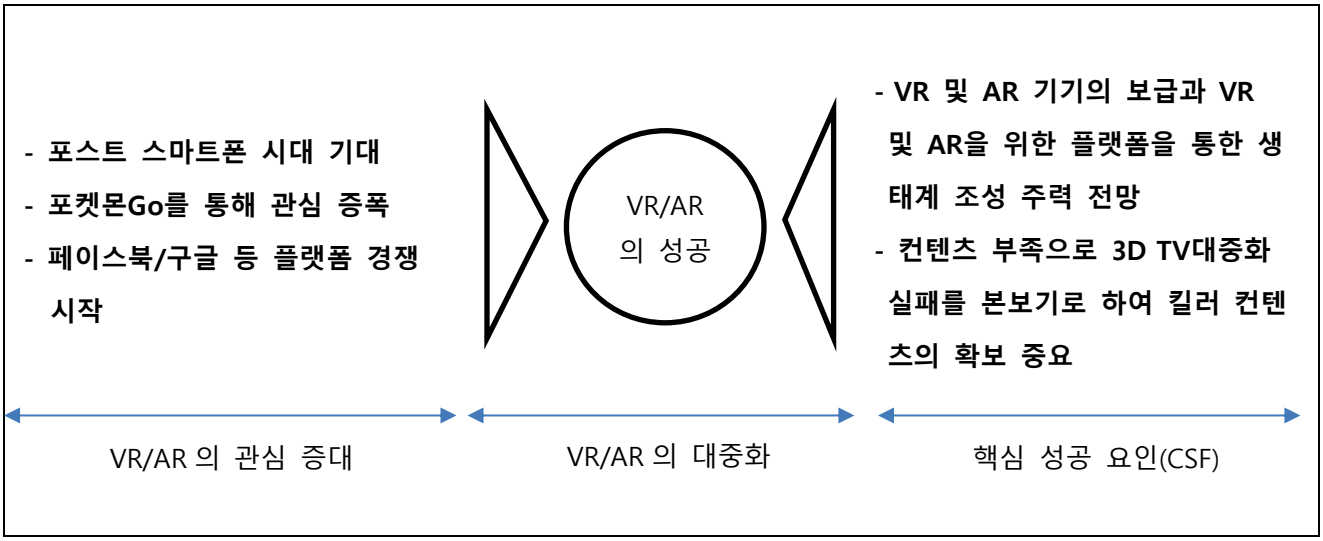
- 구글, 페이스북 등 글로벌 IT기업을 비롯해서 제조사, 통신사, 방송사 등 다양한 기업들이 VR및 AR 생태계 선점을 위해 본격적인 투자 시작

다. VR과 AR의 컨텐츠 사례

구분	사례	설명
동영상 플랫폼	유튜브, 페이스북, VRideo, Jaunt VR, 네이버, 곰TV, 통신3사	- 일반인들이 자신의 VR영상을 올려 공유할 수 있는 동영상 플랫폼 제공
건강	엘로이즈의 VR 테라피	- 지속적인 재활 운동과 건강관리를 할 수 있게 하는 헬스케어 기능성 게임 서비스 제공
공연	아크이터랙티브의 Fusion VR	- 모델하우스, 공연장, 박물관 등 활용 가능한 가상현실 솔루션 개발
공공	GOVR	- 공공데이터를 VR과 접목한 컨텐츠 제작 및 유통, 2016년 유니콘엔젤클럽으로부터 투자 유치

- 다양한 VR/AR 디바이스의 경쟁적 출시와 컨텐츠 제작 여건의 개선으로 VR 및 AR 기술을 활용한 새로운 컨텐츠 및 서비스 개발 시도가 컨텐츠 시장 전반으로 확산

4. VR과 AR 산업의 성공 방안



- VR/AR을 위한 생태계 조성 및 킬러 컨텐츠 확보를 통해 VR/AR산업의 대중화 선도

종 목	문 제
컴퓨터시스템응용기술사	2교시 3번
데이터 전송 오류가 발견된 경우 Data Link Layer에서 오류복구를 수행하는 절차에 대하여 설명하시오.	

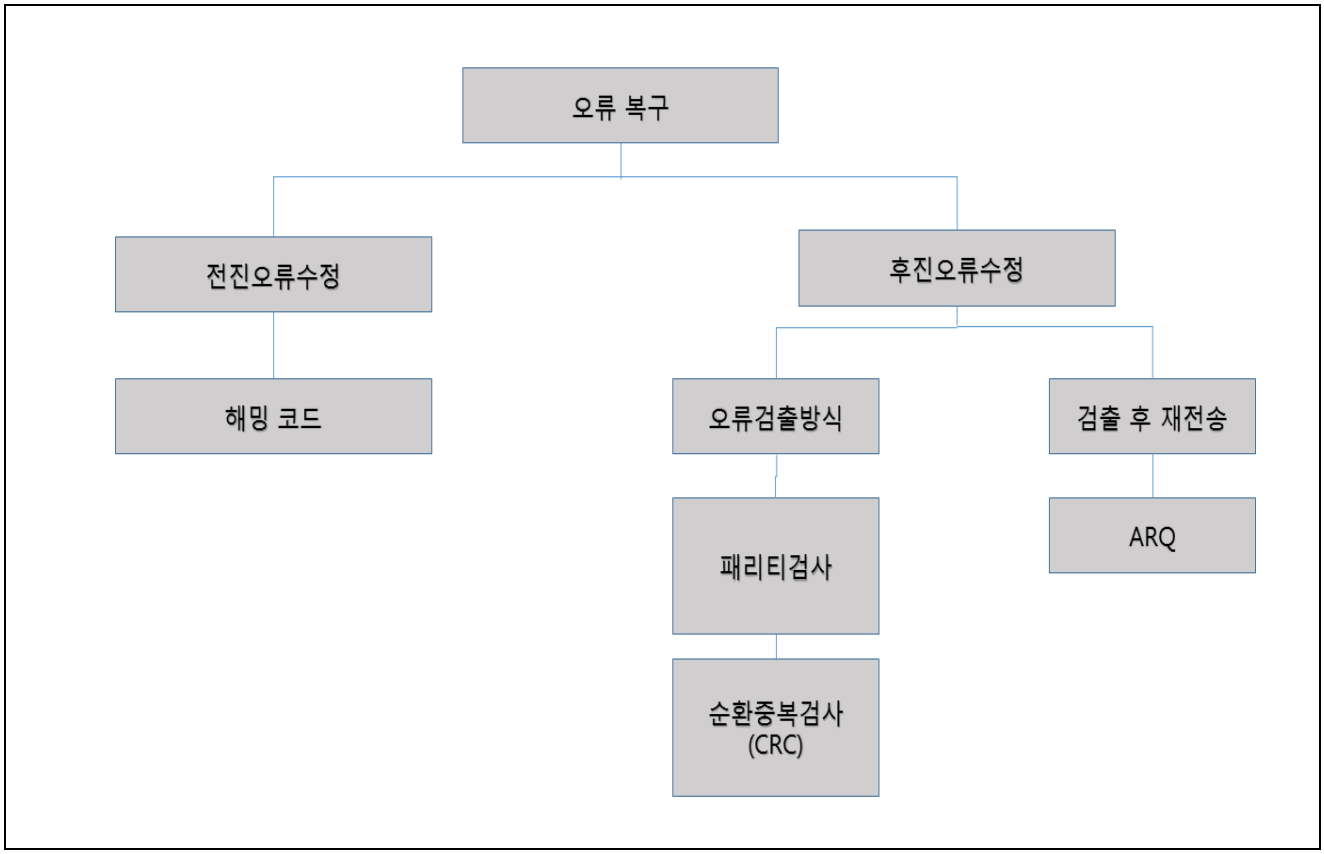
도메인/토픽	네트워크 > 네트워크 오류정정
키워드	FEC, BEC, 해밍코드, ARQ, CRC, CheckSum, Stop and wait, Go-Back-N, Selective Repetive
풀이 가이드	Data Link Layer에는 오류복구 방식을 크게 FEC/BEC로 나눌 수 있습니다. 1. Data Link Layer의 오류복구방법 설명 + FEC/BEC 간략히 설명 2~3. FEC, BEC 설명 - 대표방식/사례를 들어 설명
필수항목 /연관토픽	네트워크 오류정정기법 해밍코드, CRC, ARQ의 이해
참고문헌	FEC, 정보통신기술용어해설, 2014. 12 (http://www.ktword.co.kr/abbr_view.php?m_temp1=693) 해밍부호, 위키피디아, 2016. 4 (https://ko.wikipedia.org/wiki/%ED%95%B4%EB%B0%8D_%EB%B6%80%ED%98%B8)
Advice	본 문제는 전송오류 발견 시 복구를 위한 FEC/BEC에 대한 설명을 필수적으로 제시해야 하며, 무엇보다 오류복구를 수행하는 절차에 대해 상세하게 설명(묻는 내용을 상세히 설명) 해야 고득점이 가능합니다.
작성자	108회 컴퓨터시스템응용기술사 / 이형석 (ddrseok@naver.com)

1. Data Link Layer의 오류복구

가. 오류 복구의 개념

- OS 7 Layer의 하위의 두 계층 사이에서 데이터의 전송 오류를 검출하여 복구하는 기능

나. 오류 복구의 분류 및 방법



구분	FEC(전진오류수정)	BEC(후진오류수정)
방식 설명	- 송신 측에서 오류정정을 위한 제어 비트를 추가하여 전송하면, 수신 측에서 에러를 검출하고 수정하는 방식	- 수신 측에서 오류검출방식 및 재전송 방식을 이용하여 에러를 검출하고 수정하는 방식
수정방법	- 해밍코드 - 상승코드	- 패리티검사 - CRC - ARQ
활용	- 상대적으로 통신이 원활하지 않은 특수한 환경	- 송수신 단의 패킷 교환이 많은 통신망 환경

2. 전진오류 수정(FEC, Forward Error Correction)의 대표기법 해밍코드의 상세 설명

가. 해밍코드의 개념

- 선형 부호방법으로 수신측에서 오류가 발생한 비트를 찾아 직접 오류를 수정
- 1,2,4,8,16 비트위치에 패리티 비트를 삽입하여 오류 검출 및 정정

나. 해밍코드의 특징

- 1개의 오류비트 수정가능, 2비트까지 검출 가능
- 데이터 비트외에 추가되어야할 패리티 비트가 다수 필요

다. 해밍코드의 Parity Bit수와 Parity Bit 위치 결정

1) 4bit에 대한 Parity Bit 수와 Parity Bit 위치결정

공식	n+p <=2^p-1 식에서 P계산(n: data bit, p: parity bit)
ParityBit 수	4+p<=2^p-1 -> 최소 p값은 3
총비트수	총 bit 수 = n+p = 4+3=7
Parity bit 위치	총 비트 수에서 2^(0~(p-1))승 순으로 삽입되므로 1,2,4자리에 패리티 비트가 삽입됨

2) 해밍코드의 오류검색 방법

<오류발생의 경우>

- 10진수의 수 9가 BCD코드 1001에 해당한다. 해밍코드는 다음과 같다.

Bit	P0	P1	8	P2	4	2	1
행번호	1	2	3	4	5	6	7
9	0	0	1	1	0	1	1

패리티 비트 검사기에서 P0, P1, P2가 각각 짝수패리티인지 검사
P0는 짝수이지만 P1, P2는 홀수가 됨.
이때 짝수는 0, 홀수는 1로 하면
P0 : 1, 3, 5, 7 번째 비트들과 짝수패리티
P1 : 2, 3, 6, 7 번째 비트들과 짝수패리티
P2 : 4, 5, 6, 7 번째 비트들과 짝수패리티
P2, P1, P0를 표시하면 110이고 6번째 행을 가르킴. (000~111)
그러므로 수신측에서 6번째 1을 0으로 정정하면 됨.

- FEC의 대표적인 오류 복구는 해밍코드이며 Convolution Code도 포함된다.

3. 후진오류 수정(BEC, Backward Error Correction)의 대표기법 상세 설명

가. 패리티 검사

구분	설명	
개념	- 한 블록의 데이터 끝에 한 비트 추가, 구현이 간단하여 널리 사용	
종류	- 짝수 패리티 (Even Parity): 1의 전체 개수가 짝수 개가 되게 함 - 홀수 패리티 (Odd Parity): 1의 전체 개수가 홀수 개가 되게 함	
동작과정	송신측	① 짝수 또는 홀수 패리티의 협의에 따라 패리티 비트 생성 ② ASCII문자(7bit) + 패리티 비트(1bit) 전송
	수신측	1의 개수를 세어 오류 유무 판단(짝수 또는 홀수) → 맞지 않다면 재전송 요청
예시	홀수 패리티 사용 예 - 전송하고자 하는 데이터: 1101001 - 1의 개수를 홀수로 하기 위해 패리티 비트를 1로 지정 - 패리티 비트 추가한 최종 전송 데이터: 11101001 - 수신 측은 패리티 비트를 포함한 데이터 내의 1의 개수를 세어 홀수인지 판단하여 홀수가 아니면 재전송 요청	

- 짝수개의 오류는 검출이 불가능하다는 것이 단점

나. CRC (Cyclic Redundancy Check)

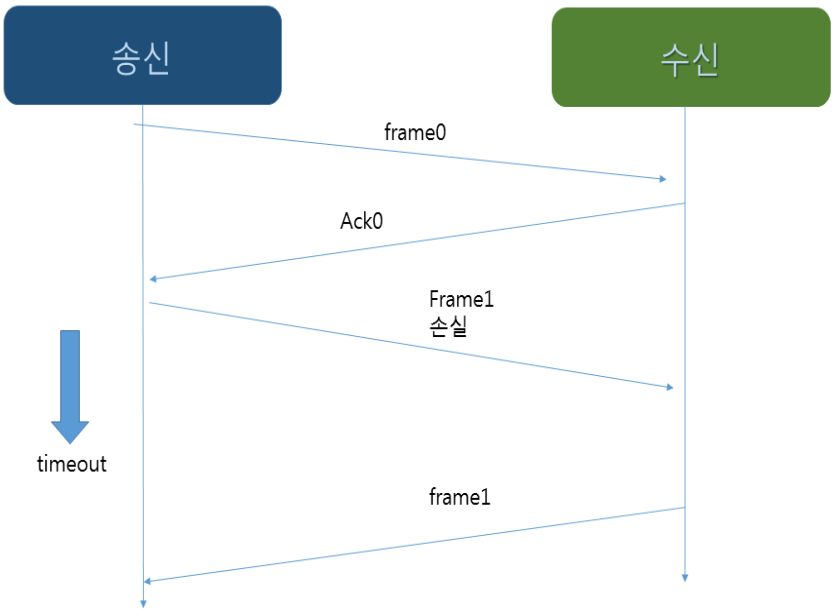
구분	설명
개념	- 오류 검출 방식 중에서 가장 성능이 우수하며 여러 비트에서 발생하는 집단 오류(burst error)도 검출이 가능**한 방식** - 임의의 비트 블록을 검사할 수 있음 - 이진 나눗셈 및 XOR (Exclusive OR) 연산을 기반
계산방법	- 메시지 (Message, D) 는 하나의 긴 2진수로 간주 - 특정한 이진수 (Generator or Pattern, P)에 의해 나누어짐 - P는 송/수신부에서 미리 약속하여 결정함 - 나머지를 BCC (Block Check Character, R)라고도 함 - R은 송신되는 프레임에 첨부 - 캐리(Carry)가 없는 Modulo-2 연산 = XOR
예시	- D = 10001101 (8 bits), - P = 1001 (4 bits) ① 전송하고자 하는 데이터 뒤쪽에 n개의 0을 삽입 n : R의 길이, D′ = 10001101000 ② D′를 P로 나눔: R을 산출해 냄 ③ D′의 뒤 n개의 0을 R로 대체함: D′ = 10001101110 ④ D′를 전송함 ⑤ 전송 받은 데이터(D′)를 P로 나눔 ⑥ 연산결과 나머지가 0이면 오류 없음

4. 오류복구기법 ARQ

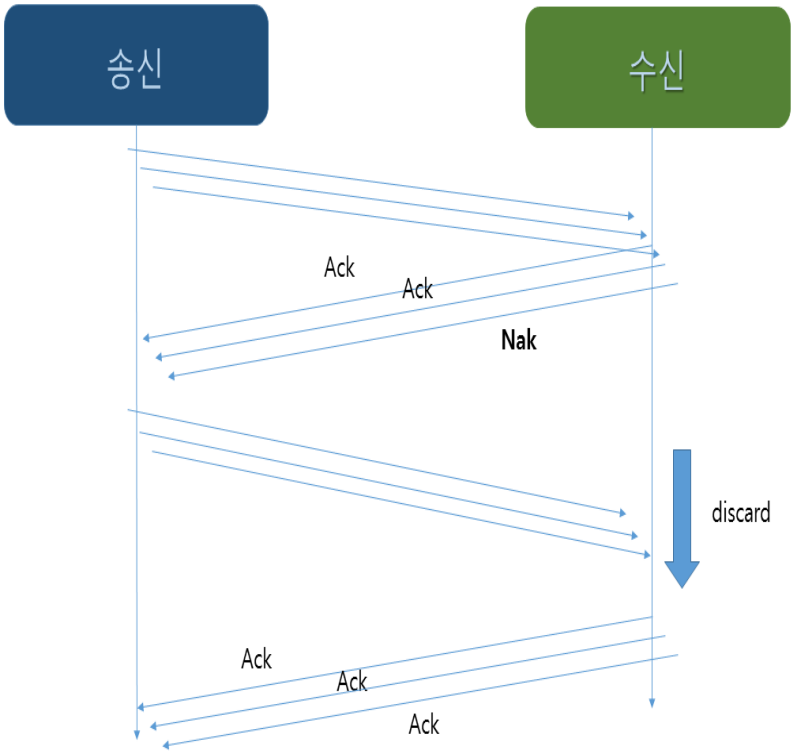
가. ARQ의 개념

- 수신측에서 오류 프레임에 대한 재전송 요구 또는 오류 정정을 하는 기법
- 흐름제어 기능과 연계

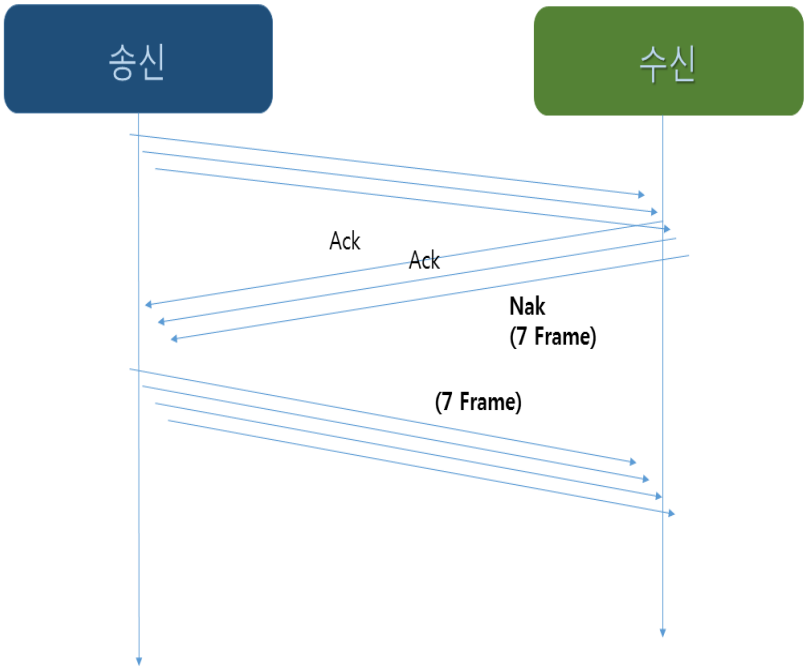
나. Stop and Wait ARQ

구분	설명
개념	- 송신 측이 하나의 프레임을 전송 - 수신 측에서는 해당 프레임의 오류유무를 판단 - 오류가 없을 경우 송신 측에게 ACK (Acknowledgement) 를 전송 - 오류가 있는 경우 NAK (Negative ACK) 를 전송하여 재전송 유도
특징	- 흐름제어 방식 중에 가장 간단한 형태 - 한번에 한 개의 프레임만 전송 - Destination can stop flow by not sending ACK
동작과정	- 송신 측은 데이터 전송 후 ACK, NAK를 받을 때 까지 대기 - 수신 측은 수신 프레임에 대하여 오류검사를 수행, 오류가 없으면 ACK를 송신, 오류가 있으면 NAK를 송신 - 송신 측에서 NAK를 수신할 경우 프레임을 재전송 

다. Go-Back-N ARQ

구분	설명
개념	- Sliding-window ARQ 의 일종 - Sender에서 오류 발생 확인은 Stop-and-wait 방식과 동일 - Sender에서 Receiver가 보낸 NAK 수신 - Sender에서 일정 Timer 동안 ACK or NAK을 수신 못함 - 오류 발생 프레임부터 Sliding-window 사이즈 내의 Frame들 재전송 - Receiver는 오류가 발생한 Frame 이후의 모든 Frame을 Discard
특징	- 일정 시간동안 송신자 대기 - 오류 프레임을 한꺼번에 전송
동작과정	- 수신 측이 4번 프레임이 잘못되었음을 인지하고 NAK를 전송 - 송신 측은 4번부터 Sliding-window 사이즈 내의 Frame들 재전송 

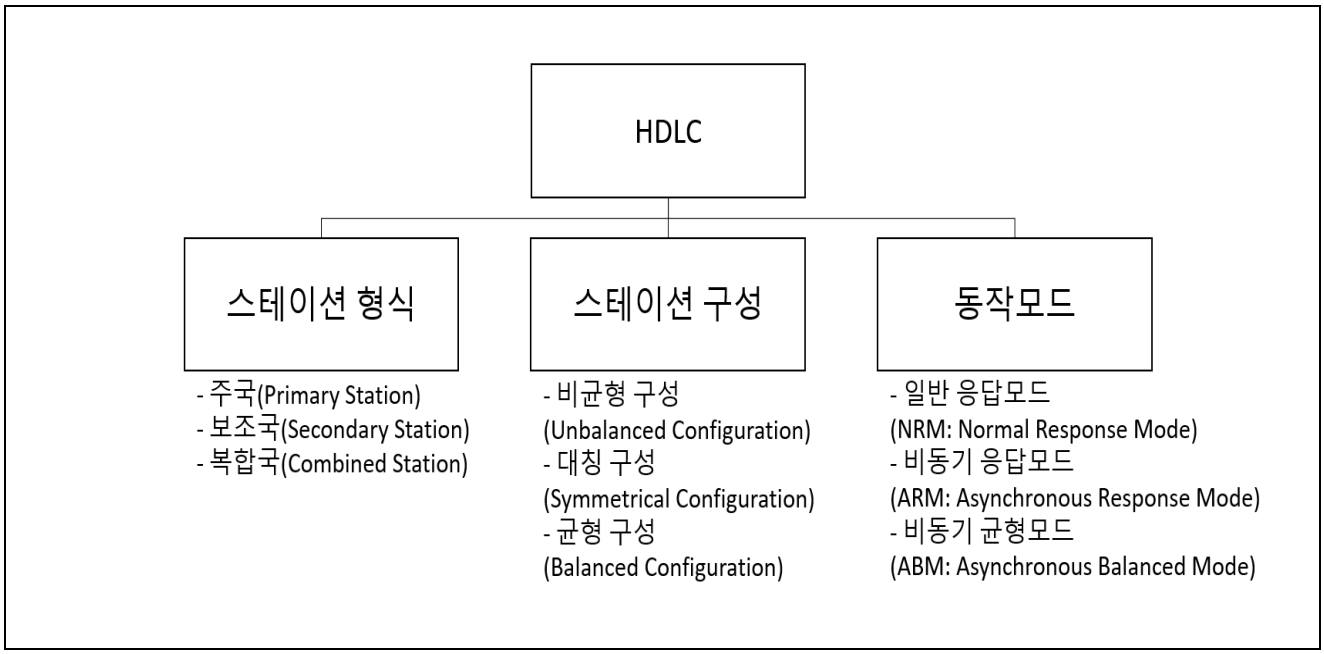
라. Selective Repeat ARQ

구분	설명
개념	- Sliding-window ARQ 의 일종 - 프레임 도착의 순서에 영향을 받지 않음 - 오류가 발생한 프레임만 재전송
특징	- 송신 측과 수신 측은 동일한 크기의 Sliding-window를 보유 - 수신 측은 프레임의 순서에 상관없이 수신 - 반드시 각각의 프레임에 대한 수신확인을 수행
동작과정	- 오류가 발생한 프레임만 재전송 

종 목	문 제
컴퓨터시스템응용기술사	2교시 4번
버스 상에 여러 노드가 연결된 경우 이용될 수 있는 HDLC(High-level Data Link Control)의 동작 모드를 설명하시오.	

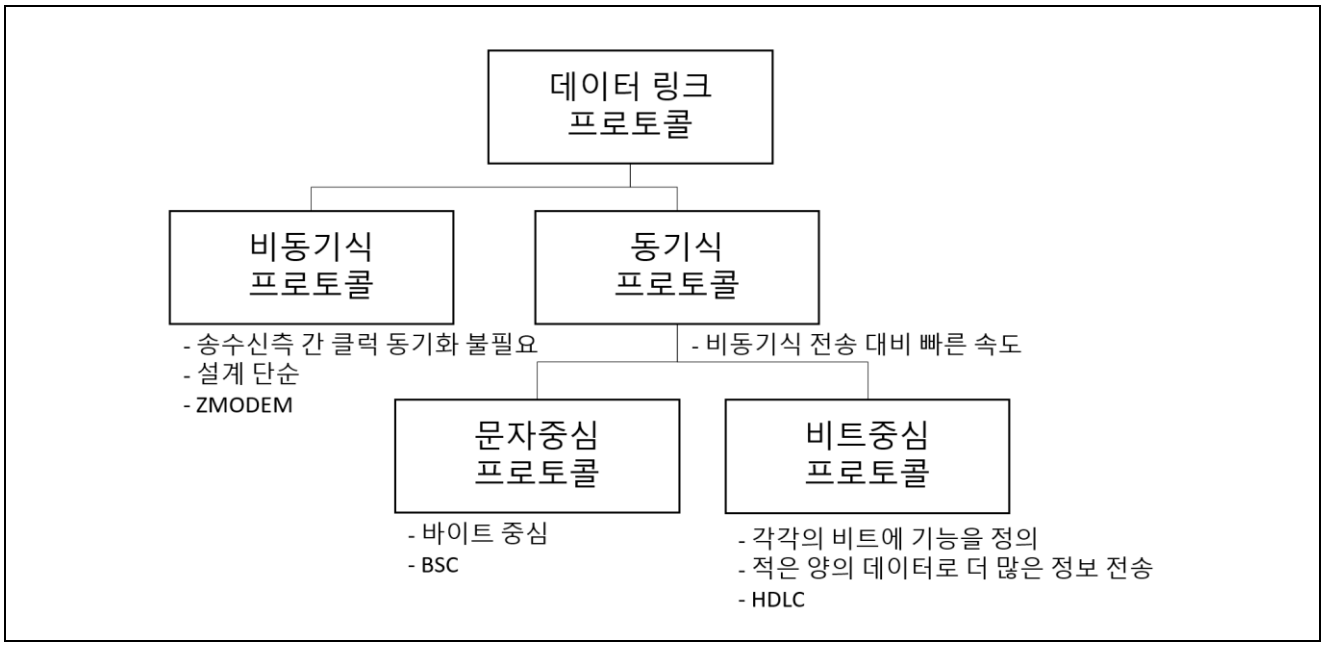
도메인/토픽	네트워크 > 데이터 통신 > 데이터 링크 계층
키워드	데이터 링크 계층, 동기식, 비트중심, 스테이션(주국, 보조국, 복합국), 스테이션간 명령/응답(Command/Response), 구성(비균형, 대칭, 균형), 동작 모드(NRM, ARM, ABM), 프레임(I-Frame, S-Frame, U-Frame)
풀이 가이드	1. HDLC 개요 2. HDLC 통신 구성 3. HDLC 동작 모드 4. 동작 모드 중 SABM 예시
필수항목 /연관토픽	OSI 7 Layer, TCP/IP 4 Layer 및 각 layer별 프로토콜 회선제어 방식: 회선경쟁 방식, 폴링/셀렉션 방식 링크 접근절차(Link Access Procedures: LAP) LAPB, LAPD, LAPM 기타 데이터 링크 프로토콜 SLIP, PPP
참고문헌	데이터통신의 이해, 생능출판사, 2008 정보통신 기술용어 해설, 차재복 (http://www.ktword.co.kr/) 데이터링크 프로토콜, 목원대학교 (elearning.kocw.net/contents4/document/lec/2013/Mokwon/LeeHyeuntae/9.pdf/) Data Link Protocols, Asst.Prof. Anan Phonphoem (slideplayer.com/slide/9442902/) Data & Computer Communications, Dr. Marwan Abu-Amara (http://slideplayer.com/slide/5365956/)
Advice	출제된 적이 없어 별도로 준비하지 않았을 경우 접근이 어려워 선택이 적었을 것으로 예상되지만, 선택하였을 경우 정확하게만 적으면 고득점이 가능한 문제입니다. 동작 모드 설명을 위해 HDLC를 사용하는 스테이션 및 구성에 대한 기본적인 내용과 함께 각 동작 모드별로 상세 설명을 전개하면 흐름이 이어지고, 가능한 경우 각 동작 모드 프레임 구성이나 예시를 보여주면 차별화된 답안이 될 것 같습니다. 관리/컴시응에서 HDLC가 기출 된 바는 없으나 정보통신기술사 93회 출제 문제입니다. 컴퓨터시스템응용기술사 시험의 경우 정보통신기술사 시험의 문제에서 종종 교차 출제가 되기 때문에 공통 도메인의 토픽들은 정보통신기술사 시험의 기출 문제들을 참고하시면 많은 도움이 됩니다.
작성자	108회 컴퓨터시스템응용기술사 / 차원호 (wonhocha@outlook.com)

1. 비트중심의 데이터 링크 프로토콜 HDLC의 개요



- HDLC(High-level Data Link Control)는 ISO에서 표준화한 동기식 비트중심의 데이터 링크 프로토콜로 점대점 방식이나 다중점 방식의 통신에 사용됨
- HDLC의 동작 모드에는 NRM, ARM, ABM 3가지 모드가 존재

[참고] 데이터 링크(Data Link) 프로토콜 분류



- 데이터 링크 프로토콜 > 동기식 프로토콜 > 비트중심 프로토콜 > HDLC

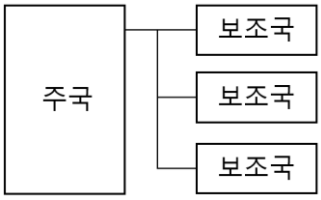
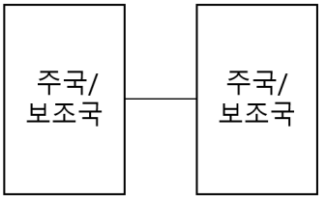
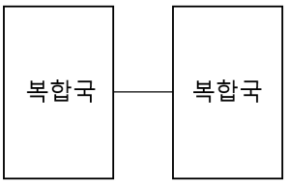
2. HDLC 동작을 위한 스테이션 형식 및 구성

가. HDLC를 사용하는 스테이션 형식

스테이션	내용	사용 프레임
주국 (Primary Station)	- 데이터 회선을 제어 - 채널상의 보조국에 명령 전송	- 명령(Command)
보조국 (Secondary Station)	- 주국으로부터 수신된 명령에 대한 응답 - 주국과 관계하는 세션은 하나만 가능	- 응답(Response)
복합국 (Combined Station)	- 명령과 응답을 모두 발생 - 전송의 성격과 방향에 따라 주국 또는 보조국으로 수행	- 명령(Command) 및 응답(Response)

- 스테이션간 관계에 따라 3가지 구성 형식이 존재

나. HDLC의 스테이션 구성

구성	토폴로지	핵심 사항
불균형 구성 (Unbalanced Configuration)		- 하나의 주국과 하나 이상의 보조국 지원 - '점대점 또는 다중점', '반이중 또는 전이중', '교환식 또는 비교환식'으로 동작 - 각 보조국을 제어하고 동작상태 및 설정에 대한 명령은 주국이 담당
대칭 구성 (Symmetrical Configuration)		- 독립된 두개의 점대점 불균형 스테이션 구성 제공 - 각 스테이션은 주국 상태와 보조국 상태를 갖기 때문에 논리적으로 두 개의 스테이션으로 간주 - 양단간 주국은 반대쪽의 보조국과 연결
균형 구성 (Balanced Configuration)		- 점대점으로만 접속되는 두 개의 복합형 스테이션으로 구성 - 반이중 또는 전이중으로 동작 - 두 지국은 단일회선으로 연결 각 스테이션은 링크제어에 대해 동일한 책임 보유

- 일반적으로 불균형 구성 및 균형 구성을 많이 사용

3. HDLC의 세가지 동작모드의 특성 및 상세 내용

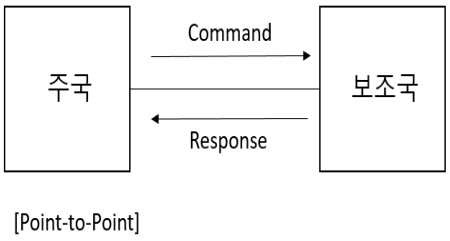
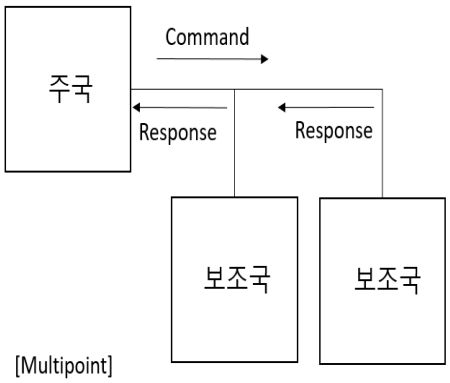
다. HDLC 동작 모드 특성

특성	NRM(일반 응답 모드)	ARM(비동기 응답 모드)	ABM(비동기 균형 모드)
스테이션 타입	- 주국 + 보조국	- 주국 + 보조국	- 복합국
구성	- 불균형	- 불균형	- 균형
연결 초기화 주체	- 주국	- 주국 또는 보조국	- 양쪽 복합국 모두 가능

- 3가지 동작 모드 지원을 위하여 정보(Information) 프레임, 감시(Supervisory) 프레임, 비번호(Unnumbered) 프레임을 사용

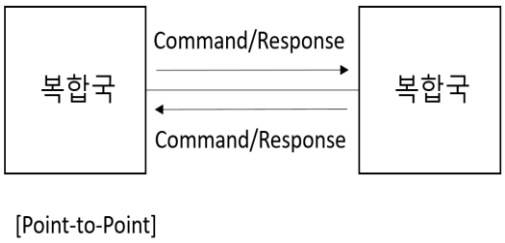
라. HDLC 동작 모드 상세 내용

① 불균형 구성에서 동작하는 NRM 및 ARM

동작 모드	링크 구성	동작 모드 상세 설명
NRM (Normal Response Mode)	 [Point-to-Point]	- 표준 주국-보조국 관계 - 일대일 또는 일대다 구성 - 보조국은 전송하기 전에 주국으로부터 명시적인 허가 필요 - 보조국은 허가를 받은 후 응답 프레임 전송 개시 - 응답 프레임은 데이터 포함 가능 - 프레임 전송 후 보조국은 다시 허가를 기다림
ARM (Asynchronous Response Mode)	 [Multipoint]	- 채널이 사용되지 않을 때 보조국은 주국의 허락없이 데이터 전송 가능 - 하나의 보조국만 ARM 동작 가능 - 주국와 보조국의 관계는 변하지 않음 - 보조국으로부터의 모든 전송은 주국으로 전송되어 최종 목적지로 중계 - 거의 사용되지 않음

- NRM과 ARM은 U-Frame의 SNRM(Set NRM) 및 SARM(Set ARM) 명령으로 연결 설정

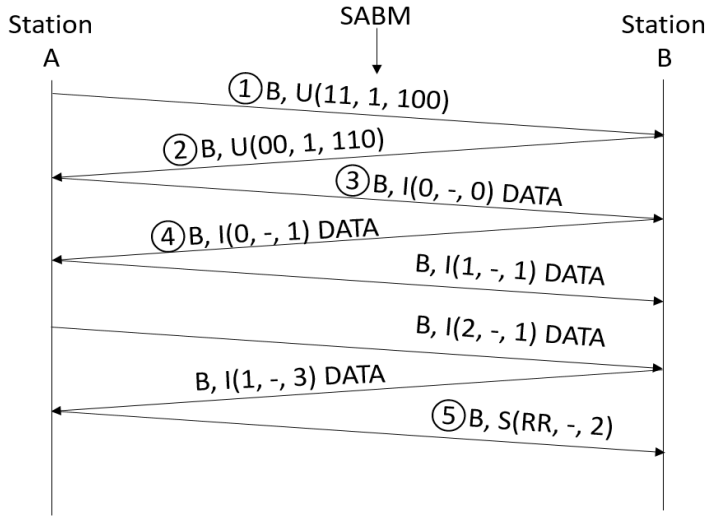
② 균형 구성에서 동작하는 ABM

동작 모드	링크 구성	동작 모드 상세 설명
ABM (Asynchronous Balanced Mode)	 [Point-to-Point]	- 점대점의 연결된 복합국만 사용 - 복합국은 상대와 동등한 권한을 갖는 스테이션 - 전송시작을 위한 허가 불필요 - P-to-P 환경에서 가장 많이 사용되는 모드 - Polling 오버헤드가 없어 효과적

- ABM은 U-Frame의 SABM(Set ABM) 명령으로 연결 설정.
- 주국과 보조국 사이는 Polling과 Selection, 복합국간은 SABM에 의한 데이터 전송

4. 스테이션 간의 대등관계(SABM)를 이용한 Peer-to-Peer 통신 예시

예시



U(CODE,P/F,CODE), I(N(S),P/F,N(R)), S(CODE,P/F,N(R))

설명

① A에서 B로 전송되는 프레임은 목적지가 B로 되어 있는 U-Frame. 11 100은 SABM통신임을 인지
② B는 A에게 U-Frame로 UA(Unnumbered Acknowledgement (00 110) 전송으로 수신 준비 알림
③ A는 B로 I-Frame에 데이터를 함께 전송. A와 B는 대등관계이므로 P/F 필드가 빠져 있음
④ B가 다음에 받을 순서번호 N(R)을 설정 후 A로 프레임 전송. 통신지속
⑤ A가 더 이상 보낼 데이터가 없음을 알리는 RR 설정을 한 S-Frame을 B로 전송. N(R)=2로 1번 프레임까지의 포괄적 수신 확인 및 자신은 RR 모드임을 알림

- [P/F 필드]: Poll/Final bit	- [N(S)]: 현재 전송하는 프레임의 순서번호
- [RR]: Receive Ready	- [N(R)]: 다음에 전송 받기를 원하는 프레임의 순서번호

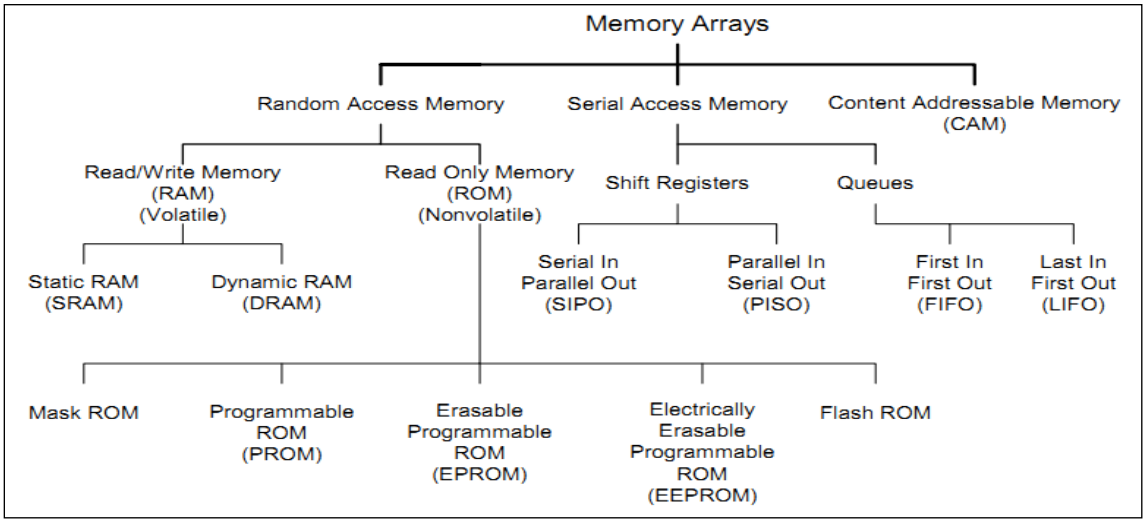
- SABM에서는 스테이션간 관계가 폴링/셀렉션 관계가 아니므로 I-Frame의 P/F 필드 생략.
- HDLC 프레임에서 주소필드는 명령은 목적지 주소, 응답은 송신측 주소를 가짐.

종 목	문 제
컴퓨터시스템응용기술사	2교시 5번

UV EPROM(UltraViolet Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM) 및 Flash 메모리를 쓰기(소거 및 프로그램) 관점에서 비교 설명하시오.

도메인/토픽	CA > 메모리 > 반도체메모리
키워드	ROM, PROM, EPROM, UVEPROM, EEPROM, Flash메모리 강한 자외선(234nm), 석영유리창
풀이 가이드	1. ROM의 특성의 서술(Read Only Memory) - 기존 정보를 삭제하고 쓸 수 있도록 기능을 추가함 - 자외선, 전기적 신호를 통해 기존 정보를 삭제 처리함 2. 삭제 메커니즘을 구체적으로 표현하여 구체성과 명확성으로 표현 필요 3. Flash메모리는 기존 WRITE와 DELETE메커니즘을 구조도로 표현 4. 기존 ROM의 발전과 FLASH메모리의 관계성을 고려하고 사용 현황을 제시
필수항목 /연관토픽	ROM메모리 구조 명시 FLASH memory
참고문헌	EEPROM, 위키피디아 (https://ko.wikipedia.org/wiki/EEPROM) EPROM, 위키피디아 (https://ko.wikipedia.org/wiki/EPROM) 플래시메모리, 위키피디아 (https://ko.wikipedia.org/wiki/플래시_메모리)
Advice	기본 토픽으로 컴시응에서는 Flash Memory의 읽기 쓰기 메커니즘을 정확히 이해하고 표현할 수 있어야 합니다. - UV EPROM과 EEPROM은 삭제 되는 메커니즘이 특징을 잘 표현하는 것이 중요!
작성자	108회 컴퓨터시스템응용기술사 / 정두현 (dhc97@naver.com)

1. 메모리 종류와 분류별 특성



종류	Read / Write	삭제가능여부	쓰기 기법	휘발성/비휘발성
RAM	- 읽기/쓰기	- 전기적 삭제	- 전기적	- 소멸 (휘발성)
ROM	- 읽기	- 불가	- 마스크	- 보존 (비휘발성)
PROM	- 읽기	- 불가	- 전기적	- 보존 (비휘발성)
EPROM	- 읽기/쓰기	- 자외선 삭제	- 전기적	- 보존 (비휘발성)
EEPROM	- 읽기/쓰기	- 전기적 삭제	- 전기적	- 보존 (비휘발성)

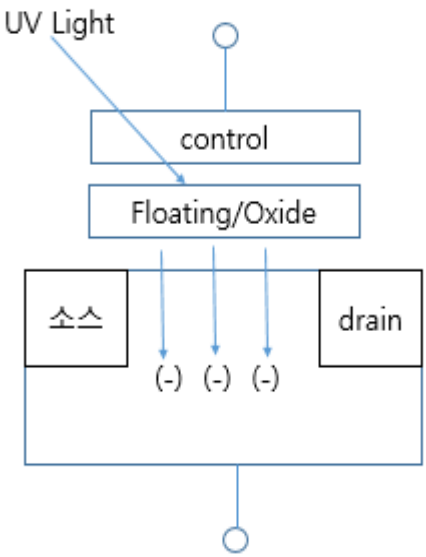
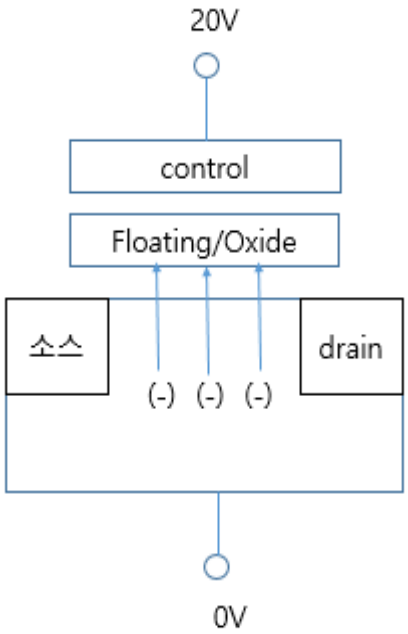
가. Non-Volatile Memory (비 휘발성 메모리)의 종류별 특성

- 전원이 차단되어도 이전 정보 기억하는 특성을 가지는 ROM(Read-Only Memory)을 의미

종류	특성
Masked ROM	- 특정 내용을 생산 공장에서부터 ROM에 기억시켜 출하하는 것으로 사용자의 의도에 의해 임의적으로 기억시킬 수 없음 - 메모리 중 Bit당 가격이 제일 저렴
PROM	(Programmable, Non-erasable, ROM) - 생산 공장 출하 시 기억된 것이 아무것도 없으며, PROM writer를 이용하여 사용자에 의해 한번 기억이 가능
(UV)EPROM	(Erasable, Programmable ROM) - 자외선을 사용하여 기억된 내용을 임의적으로 소거시킨 후, 전기적인 방법으로 재기억 시킬 수 있는 소자
EEPROM	(Electrically Erasable PROM) - 전기적 방법으로 정보를 소거, 저장 연속 진행
Flash Memory	- 기존 EPROM과 EEPROM의 변형으로 block 단위로 고속 수정 가능한 특징 - 메모리 반도체 내에서 D램의 비중은 저하되고 플래시 메모리 비중 상승

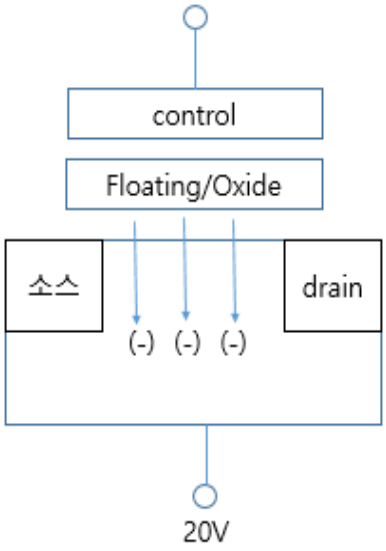
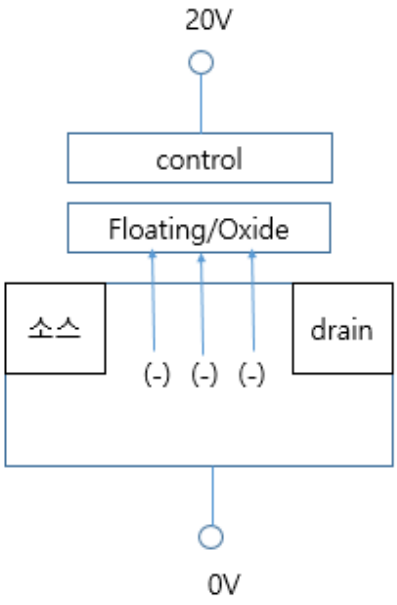
2. UV EPROM, EEPROM, FLASH Memory의 쓰기 메커니즘 관점의 비교

나. UV EPROM의 쓰기 메커니즘

동작	동작구조	설명
ERASE		- 자외선 조사 시(234nm) 절연이 파괴되어 전자가 이동 하여 소거됨 - 석영유리창, 자외선 조사 - 절연게이트 트랜지스터 이용 - 기록횟수: 고전압이 실리콘에 영향을 주어 20회 전 후 - 영구 보존 시, 차광 씰 부착
Program		- 소거된 대상으로 전자의 이동으로 정보가 기억됨 - 절연막으로 채워진 전자는 이동하지 않음 - 12V 전 후의 전압 부여

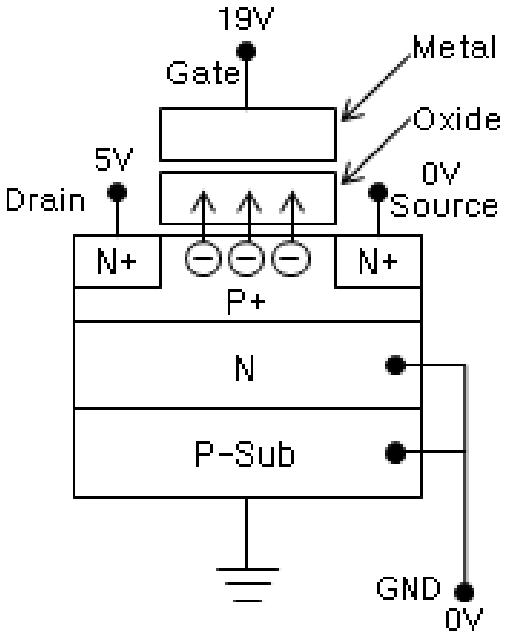
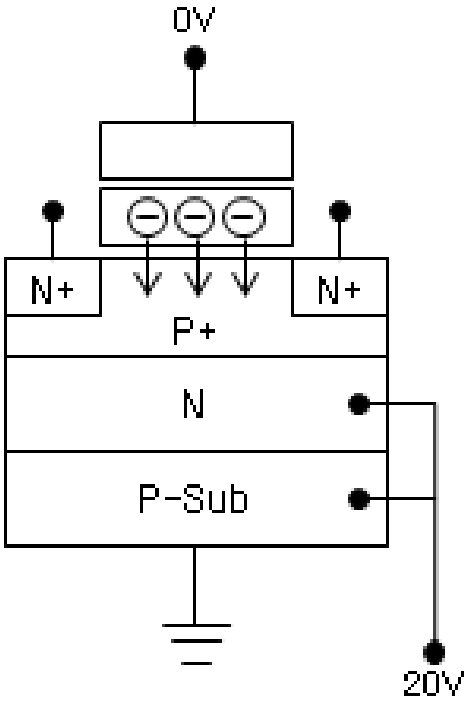
- UV EPROM은 UV Light Eraser를 이용하여 조사하여 초기화 됨

다. EEPROM의 쓰기 메커니즘

구분	동작구조	설명
Erase		- 자외선 조사 시(234nm) 전자가 이동하여 1로 채워짐 - 석영유리창, 자외선 조사 - 기록횟수: 고전압이 실리콘에 영향을 주어 20회 전 후 - 영구 보존 시, 차광 씰 부착
Program		- 소스 → 드레인으로 전력 이동 시, 전자가 이동하여 1로 채워짐 - 절연막으로 채워진 전자는 이동하지 않음 - 12V 전 후의 전압 부여

- EEPROM은 1바이트씩 롬라이터(Rom Writer)를 이용하여 초기화 처리됨

라. FLASH Memory의 쓰기 메커니즘

동작	동작구조	설명
Write Operation		**<터널 주입>** - 초기 모두 1로 채워짐 - 프로그램 할 때 Oxide는 전자를 채워 0으로 셋팅 - Gate쪽에 5V가 아닌 약 12~19V의 큰 전압을 주어 전기장의 세기를 증가 - 소스에서 드레인으로 전류를 흘러 전자가 oxide로 흘러 들어감
Erase Operation		**<터널 릴리즈>** - P+N층에 20V의 전압을 걸어주게 되어 Write와는 반대로 Oxide에 있던 전자들이 강한 전기장의 힘으로 전자가 사라지고 1의 상태가 됨

3. UV EPROM, EEPROM, FlashMemroy의 쓰기 관점의 특징적 비교

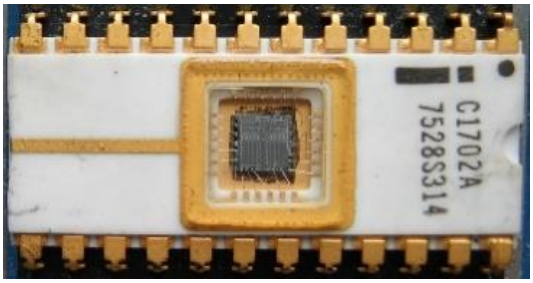
가. 특징적 비교

종류	Read / Write	삭제 방식	쓰기 방식	휘발/비휘발성
UV EPROM	- 읽기/쓰기	- 자외선 삭제	- 전기적	- 보존 (비휘발성)
EEPROM	- 읽기/쓰기	- 전기적 삭제	- 전기적	- 보존 (비휘발성)
Flash	- 읽기/쓰기	- 전기적 삭제	- 전기적	- 보존 (비휘발성)

나. 쓰기횟수 및 삭제 기기 비교

구분	UV EPROM	EEPROM	Flash Memory
쓰기 횟수	- 20회이하	- 10만번 (매우느림)	- 10만번(SLC)
삭제 처리	- UV Eraser	- 롬라이터	- 별도 필요 없음

[참고] UV EPROM

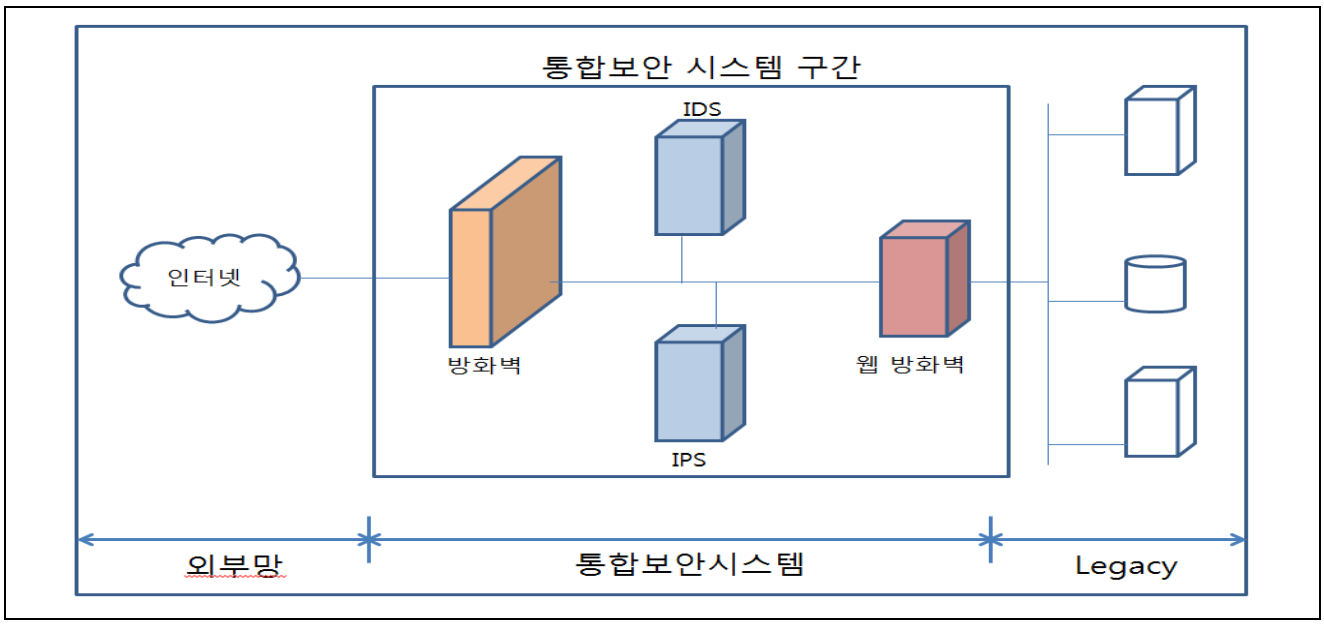
	
<UV EPROM>	<UV EPROM Eraser>

종 목	문 제
컴퓨터시스템응용기술사	**2교시 6번**
방화벽 침입탐지 시스템(IDS: Intrusion Detection System), 침입방지 시스템(IPS: Instrusion Prevention System) 및 웹방화벽의 개념과 기능을 설명하시오	

도메인/토픽	보안 > 통합보안관리 > 통합보안시스템
키워드	경보기능, 세션 차단기능, 실시간 탐지기능, HIDS, NIDS, 실시간 자동대응 기능, 실시간 분석 기능, 미확인 공격 탐지 기능, 사용자 요청 검사, 컨텐츠 보호, 위장, 다양한 웹 환경 지원 기능
풀이 가이드	1. 통합 보안 시스템 필요성 및 유형 2. IDS/IPS 개념 및 주요 기능 3. 기존 보안 시스템 문제점 및 웹 방화벽 개념, 주요기능 4. 기존 보안 시스템 연계를 통한 통합 보안 체계 구축 방안
필수항목 /연관토픽	통합보안시스템, ESM, Firewall, Web Firewall, IDS, IPS, UTMS
참고문헌	기술사 학습 자료
Advice	통합 보안 관리 시스템 유형을 이해하고, IDS/IPS 주요 기능과 한계점을 바탕으로 웹 방화벽의 핵심 기능을 작성한 후, 기존 보안 시스템과의 연계를 통한 통합 보안 관리 체계 구축 방안을 제시합니다.
작성자	108회 컴퓨터시스템응용기술사 / 조현철 (van_damme@naver.com)

1. 통합 보안 시스템 개요

가. 통합 보안 시스템 구성



- 외부로부터 불법적인 침입 및 공격에 대한 통합 대응을 위한 위한 통합 보안 시스템 구성

나. 통합 보안 시스템 유형

유형	설명
L4/L7 Switch	- 네트워크 대역폭 관리와 제어 및 로드 밸런싱 제공
IDS	- 보안 정책을 위반하는 행위, 즉 침입(intrusion)을 실시간으로 탐지하는 시스템
IPS	- 정보시스템 네트워크에서 침입탐지와 침입을 사전 예방하는 정보보호시스템
방화벽(Firewall)	- 외부로부터 허가되지 않은 불법적인 접근을 하지 못하도록 하는 시스템
웹 방화벽	- 웹 애플리케이션을 대상으로 시도되는 해킹을 차단해주는 솔루션

2. 실시간 침입 탐지 시스템, IDS 개념 및 주요 기능

가. IDS(Intrusion Detection System)의 개념

- 비인가된 사용자가 자원의 무결성(integrity), 기밀성(confidentiality), 가용성(availability)을 저해하는 일련의 행동들과 보안 정책을 위반하는 행위, 즉 침입(intrusion)을 실시간으로 탐지하는 시스템
- 외부 침입자뿐만 아니라 내부 사용자의 불법적인 오남용 행위를 대처하는 방법이 필요함
- 침입차단시스템(Firewall)이 해킹 당했을 때의 피해 최소화 필요 및 방화벽의 문제점 보완 필요성

나. IDS(Intrusion Detection System)의 주요 기능

주요 기능	내용
경보기능	- 경보, 이메일 발송, SNMP Trap 발송 등으로 통보
세션 차단기능	- 의심스러운 행위 감지 시에 해당 세션 차단
실시간 탐지	- 시스템이나 네트워크를 모니터링하여 실시간 침입 탐지 기능
Reporting	- 통계적 분석 및 reporting 기능

다. IDS(Intrusion Detection System)의 구성

구성요소	내용
정보수집기	- 호스트나 네트워크로부터 분석 자료 수집
정보분석기	- 시스템 설정과 패턴 DB의 설정에 따라 정보 분석
로그저장소	- 분석된 결과 저장
이벤트 보고기	- 로그 저장소의 분석결과를 해당 관리자에게 보고
패턴 생성기	- 침입 분석 자료를 통해 패턴 생성
패턴DB	- 패턴 생성기에 의해 생성된 패턴의 저장 관리

라. IDS(Intrusion Detection System)의 유형

분류	구분	내용
데이터 소스 기반	호스트 기반 (HIDS)	- 서버에 직접 설치됨에 따라 네트워크 환경과 무관 - 감사자료 다양, 정확한 침입탐지 가능
	네트워크 기반 (NIDS)	- 네트워크 세그먼트당 하나의 탐지기만 설치, 설치 용이 - 독립적으로 네트워크에서 실행되어 운영서버의 성능저하 없음
침입탐지 모델 기반	오용침입탐지 (Misuse)	- 특정 공격에 관한 기존의 축적된 지식을 바탕으로 패턴 설정 - 패턴과 축약 가공된 데이터를 비교, 일치 시 불법 침입 간주 - 새로운 공격탐지를 위해 지속적으로 새로운 공격패턴 갱신 필요
	이상침입탐지 (Anomaly)	- 사용자의 행동패턴을 분석, 정상 사용패턴과 비교해 이상 패턴 발견을 침입으로 간주 - 인공지능 알고리즘 사용

3. 침입 탐지와 실시간 방어를 위한 솔루션, IPS 개념 및 주요 기능

가. IPS(Instrusion Prevention System)의 개념

- 침입탐지시스템의 오판(False Positive)와 미탐(Miss Detection)의 문제 해결을 위해 등장한 정보시스템 네트워크에서 침입탐지와 침입을 사전 예방하는 능동형 정보보호시스템

필요성	설명
기존보안제품의 한계	- IDS는 공격을 감지하더라도 방어할 수 없고, 사람의 개입이 반드시 필요
효과적 공격탐지 필요	- IDS의 문제점인 높은 오탐율에 대한 해결 방안 필요
신속한 자동대응	- 대역 네트워크에 적합한 Wire Speed의 성능 보장 필요

나. IPS(Instrusion Prevention System)의 주요 기능

주요 기능	설명
실시간 자동 대응 기능	- 침입 및 바이러스 감염 등 상황에 맞는 실시간 자동 대응 기능 제공
실시간 분석 기능	- 광대역 통신망 패킷을 실시간 분석 기능 제공
미확인 공격 탐지 기능	- 알려지지 않는 공경에 대한 탐지 기능 제공
세션 기반 탐지 기능	- 패킷 기반 탐지 외에 세션 기반 탐지 기능 제공

다. IPS(Instrusion Prevention System)의 구성

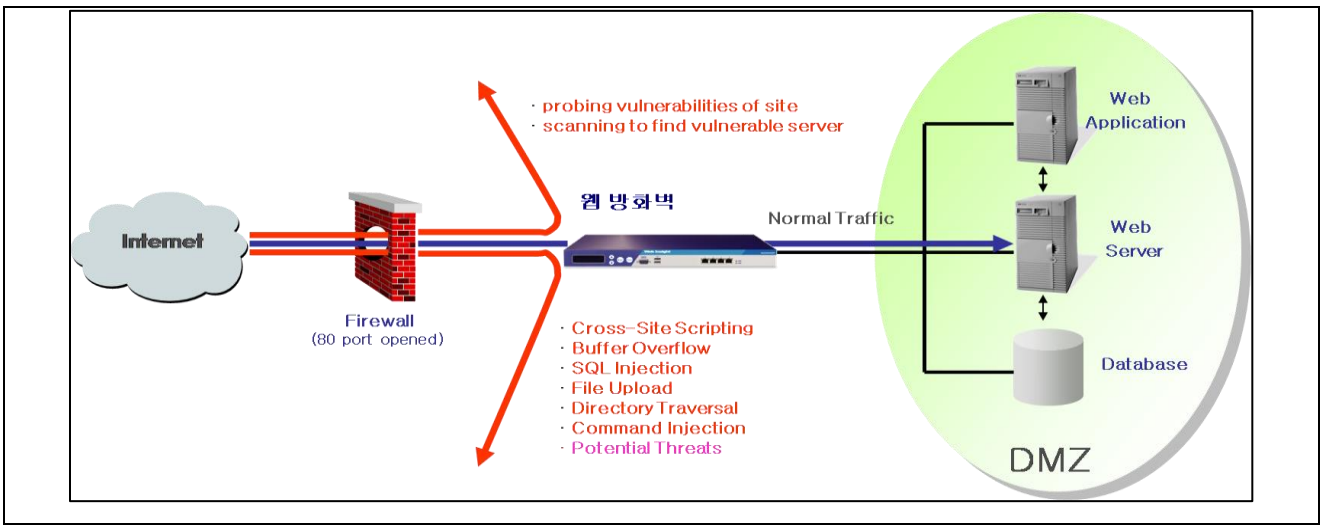
구분	항목	내용
시스템 구성	침입탐지에이전트 (침입탐지 센서)	- 네트워크에서 전송되는 패킷을 수집하고 공격 여부를 판단하는 핵심 모듈이며 탐지된 결과를 데이터 매니저에 전송
	관리자 콘솔	- 침입탐지 센서의 정책설정 및 로그 검색, 통계, 포트 등을 수행하는 관리자시스템으로 분산 환경하에 2개 이상의 관리콘솔을 두어, 다중 관리자 체계로 운영 가능
운영방안	Passive Monitoring	- IDS와 같이 동작 (인라인 모드가 아님 - 스니핑 모드) - 스위치의 미러링이나 Tap장비를 통해 트래픽을 관찰
	Inline Simulation	- 인라인 IPS 구성 (IPS초기 설치 시 유용) - 공격탐지 시 차단하지 않음
	Inline Protection	- 인라인 IPS 구성 - 공격 탐지 시 차단

라. IPS(Instrusion Prevention System) 유형

구분	HIPS (호스트 기반 IPS)	NIPS (네트워크 기반IPS)
설명	- 특정 서버 기반으로 어플리케이션 소프트웨어 형태로 설치, 시큐어 OS와 유사기능 수행	- 방화벽처럼 네트워크 인라인모드로 설치되어 공격을 차단해 주는 기능 수행 - 정책에 근거한 패턴 탐지
특징	- 서버기반의 커널 조작 등 불법적인 서버 침입 방지	- DDoS, 버퍼오버플로우 등 네트워크 기반 공격에 빠른 대응과 사전 차단 및 방비
목적	- 시스템 불법 침입 및 바이러스, 해킹 등 호스트 기반 보호	- 네트워크 기반의 공격 등 과도한 트래픽 공격방지
장점	- 커널 상에서 불법 응용 실행 방지 업데이트 및 패치 관리 용이	- 하드웨어 기반의 빠른 대응속도 - 대부분 자동 수행 기능
단점	- Agent 설치 비용 증가 - 정상적인 응용 프로그램 방해 가능성 발생	- 네트워크상의 단일 실패점 존재로 여분의 장비 필요 - 보안업데이트에 의존함

4. 웹 방화벽 개념 및 주요 기능

가. 웹 방화벽 개념



- 웹애플리케이션을 대상으로 시도되는 해킹을 차단해주는 솔루션
- 웹서버로 들어오는 웹 트래픽을 검사, 악의적인 코드나 공격유형이 포함된 웹 트래픽 차단
- 웹 어플리케이션의 보안 취약점을 방어하기 위한 웹 차단 도구

나. 웹 방화벽 주요 기능

주요 기능	설명
사용자 요청검사	- 어플리케이션 접근제어, 과다요청제어 (Web DoS) - 버퍼 오버플로우 차단, SQL/스크립트 차단 - 업로드 파일/요청형식 검사
컨텐츠 보호	- 신용카드 정보 유출 차단, 주민등록번호 유출 차단 - 웹변조 방지, 응답형식 검사, 코드노출 차단
위장	- URL 정보 위장, 서버 정보 위장 - 사용자에게 제공되는 정보 주 일부를 위장
SSL 복호화 지원 등 다양한 웹 환경 지원	- 암호화된 HTTPS 웹트래픽의 복호화를 통한 웹공격 검사

다. 웹 방화벽 유형

구분	항목	내용
설계방식	네트워크 기반 웹 방화벽	- 네트워크 구간에 인라인 트랜스 페런트 및 프락시 방식으로 구성되며 전송되는 웹 트래픽에 대한 분석 및 차단 기능 수행
	호스트 기반 웹 방화벽	- 각 웹 서버에 설치된 보안 에이전트와 마스터 서버, 관리용 콘솔 환경으로 구성
내부 아키텍처	Proxy 방식	- 웹서버 앞 단에서 웹 방화벽이 클라이언트 요청을 받아 필터링 처리 후, 다시 웹 서버와 재접속을 맺는 방식
	Filtering 방식	- 웹 방화벽이 웹 서버의 플러그인 모듈처럼 동작하는 방식

5. 기존 보안 솔루션 한계 및 통합 연계 방안

가. 웹 기반 환경에서의 기존 보안 솔루션의 한계

피해 유형	설명
L4/L7 Switch	- 네트워크 트래픽에 국한되며 https에 대한 전문적인 보안 불가
IDS	- 우회 공격과 SSL 패킷에 대해서는 방어 능력이 없으며 오탐 많음
IPS	- SSL 통신에 대해 검사가 불가하므로 웹 보안에 취약
방화벽(Firewall)	- 웹 프로토콜에 대한 제어 불가능(80 Port) - 임무의 초점은 네트워크 인프라를 보호하는데 있음

나. 기본 보안 솔루션 한계를 극복한 통합 연계 방안

방안	설명
전사적 보안 활동 수행	- 해킹 등 사이버위협에 대한 정보수집, 분석, 보안사고예방, 침해사고대응 등 전반적인 보안활동을 수행
통합 보안 관제 실시	- 침입방지시스템, 침입차단시스템, 서버보안시스템, 유해 트래픽 분석시스템, 취약성 점검 시스템, 보안해킹분석시스템, 위험관리시스템 등으로 구성하여 통합 보안관제를 실시
통합 보안 운영 체계 실시	- 시스템에서 발생하는 유해 트래픽 정보를 수집·분석해 종합적으로 대처할 수 있는 통합 보안관제 운영체계 수립
보안 관리 전문가에 의한 사고 예방	- 보안관리전문가에 의해 각종 보안시스템을 관리하며 해킹, 악성코드, 불법 자료유출 방지 등 보안 사고 예방 필요

6. 웹 방화벽 도입 고려사항 및 기대효과

가. 웹 방화벽 도입 고려사항

구분	고려사항	상세설명
성능	Throughput	- 웹 서비스의 총 트래픽을 고려하여 웹 방화벽이 처리 할 수 있는 성능 감안
	TPS	- 초당 처리 할 수 있는 처리량(Transaction Per Second) 고려
	Latency	- 방화벽 설치로 인한 지연 현상 최소화
기능	Health check	- 웹 서비스의 이상 유무를 확인
	bypass	- 장애 발생시 웹 서비스가 가능하게 하는 기능
보안	안정성	- 웹 해킹 탐지 및 SHA-1, HAS-160과 같은 160bit 해쉬 알고리즘과 AES, SEED, ARIA 알고리즘 사용

나. 웹 방화벽 도입 기대 효과

웹방화벽 도입 전	웹방화벽 도입 후
- 웹 소스 상 수많은 취약점 존재 - 웹 공격 가능 취약점에 무방비 - 웹 해킹에 따른 홈페이지 위변조, 정보 유출 등의 위험성 - 관리자의 끊임없는 서버관리 수고	- 비용 대비 효율적으로 웹 소스 상 취약점 최소화 - 웹 공격에 대한 최상의 방어 - 다양한 웹 해킹 공격에 대한 방어로 서비스 안전성 제고 - 다양한 리포트 제공을 통한 효율적 시스템 관리

- 웹 해킹 완벽 대비 및 안정적인 웹 서비스 환경 구축 기대

[참고] 웹 기반 해킹 피해 유형

피해 유형	설명
홈페이지 내용 위변조	- 웹 서버 해킹을 통해 위 변조된 내용 게시 - 신뢰성이 중요한 국가 정부기관 및 대기업은 큰 타격을 미침
거래 정보 변조	- 웹을 통해 상거래가 이루어지는 쇼핑몰 및 금융 기관 - 쇼핑몰의 경우 구매 수량, 가격 등의 변조를 통해 피해 발생
중요 정보 유출	- 해킹으로 운영자 권한을 획득하여 DB 서버의 주요 고객정보 및 금융정보 유출
악성 코드 유포	- 웹 서버 해킹을 통해 악성코드를 심어 놓고 사이트 접속자를 상대로 악성코드 유포

- 지속적인 홈페이지 침해 사례의 증가로 웹 방화벽은 최근 보안 시장의 최대 이슈로 등장