제39회 ITPE 실전 명품 모의고사 해설집

2025.12.21

제 39 회 ITPE 실전 명품 모의고사

일시 : 2025 년 12 월 21 일 제 3 교시(시험시간: 100 분)

분야	정보통신	자격종목	정보관리 컴퓨터 시스템 응용	수검 번호		성 명	

※ 다음 문제 중 4 문제를 선택하여 설명 하십시오. (각 25 점)

1. 전송계층의 제공 기능인 흐름제어에 대하여 다음을 설명하시오.

   가. TCP 의 흐름제어 개념 및 유형

   나. 슬라이딩 윈도우(Sliding Window)

   다. Silly Window Syndrome 및 해결방안

2. 대표적인 메시지 큐 시스템인 아파치 카프카(Apache-Kafka)에 대해서 다음을 설명하시오.

   가. 아파치 카프카 개념 및 특징

   나. 아파치 카프카와 Redis 비교 설명

3. IT 프로젝트의 성패는 기술 자체보다 조직의 가치 전달 체계(Value Delivery System)가 얼마나 정렬되고 작동하는가에 의해 결정된다. IT 프로젝트가 실패하는 주요 원인을 설명하고 IT 프로젝트를 성공적으로 수행하기 위한 전략을 기술하시오.

4. 최근 AI 모델 도입이 확산되면서 AI 모델이 외부 데이터 소스를 원활하게 이용하고 협업할 수 있도록 MCP(Model Context Protocol)를 도입하고 있다. 다음에 대해 설명하시오.

   가. MCP(Model Context Protocol) 개념 및 필요성

   나. MCP(Model Context Protocol) 구성요소

   다. MCP (Model Context Protocol) 도입 시 고려사항

5. 최근 국내 이동통신사에서 펨토셀(Femtocell) 장비가 변조되어 이동통신 핵심망(Core Network)에 비인가 접속하는 사고가 발생하면서 소형 기지국 장비에 대한 보안 우려가 커지고 있다. 다음에 대해 설명하시오.

가. 펨토셀 개념 및 주요기능

나. 펨토셀 보안 취약점 및 대응방안

[정보관리기술사 선택문제]

6. 국가정보자원관리원 화재 이후 재해복구의 중요성이 더욱 높아지고 있다. 다음 내용을 설명하시오

가. 재해복구시스템 구축절차

나. BIA(Business Impact Analysis)

다. DRaaS

[컴퓨터시스템응용기술사 선택문제]

6. 오픈 네트워크 프로젝트(OCP) 생태계 기반의 네트워크 기술중 SAI(Switch Abstraction Interface)가 핵심표준기술로 자리잡고 있다. 다음을 설명하시오

가. SAI 개념 및 특징

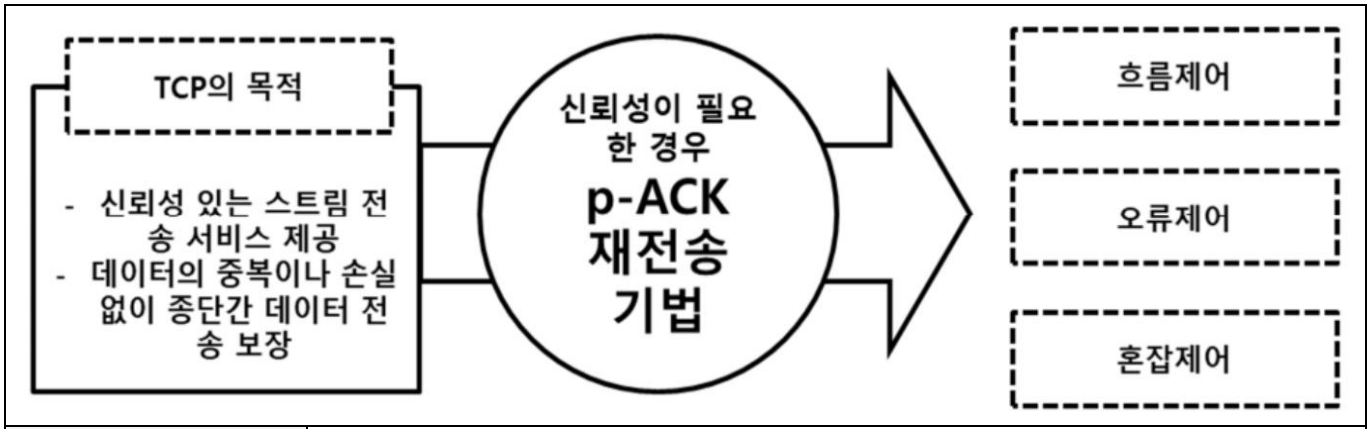
나. SAI 구조 와 기술요소

다. SAI 표준기술의 시사점

01	흐름제어		
문제	전송계층의 제공 기능인 흐름제어에 대하여 다음을 설명하시오. 가. TCP의 흐름제어 개념 및 유형 나. 슬라이딩 윈도우(Sliding Window) 다. Silly Window Syndrome 및 해결방안		
도메인	네트워크	난이도	중 (상/중/하)
키워드	Stop And Wait, Sliding Window, 윈도우, RWND, CWND, 열림, 닫힘, 윈도우 크기		
출제배경	TCP 4계층 흐름제어의 주요 유형 및 관련 토픽에 대한 숙지 여부 확인		
참고문헌	ITPE 기술사회 자료		
출제자	박서현 기술사(제 131회 정보관리기술사 / mondaysss@naver.com)		

I. 전송계층 송수신 제어, TCP의 흐름제어 개념 및 유형

가. TCP의 흐름제어 개념



개념	- 데이터를 효율적이고 송신자가 네트워크 환경, 수신자의 상황을 고려하여 데이터를 전송하도록 전송 속도를 제어하는 메커니즘

- TCP의 신뢰성 있는 데이터 전송을 위해 TCP는 흐름제어, 오류제어, 혼잡제어 기능을 수행하며 이중 흐름제어를 통해 수신자의 상황을 고려하며 전송 속도를 제어

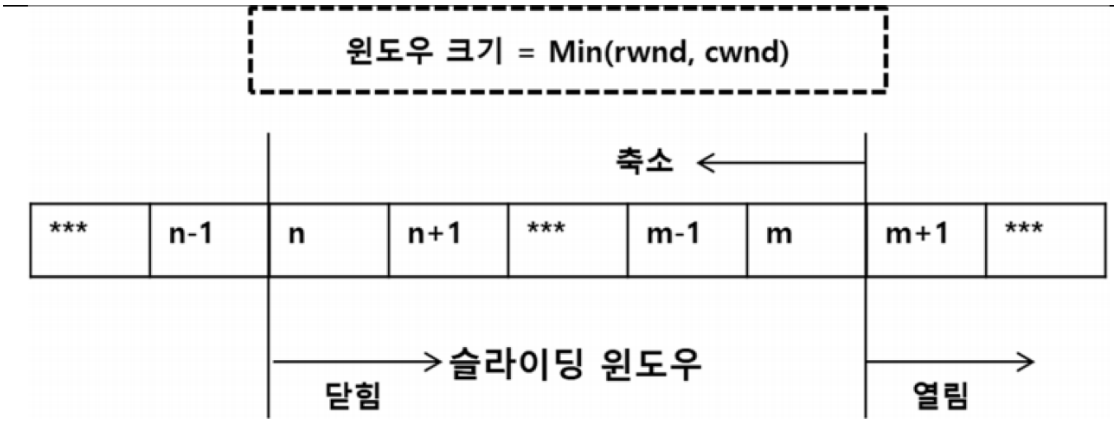
나. TCP의 흐름제어 유형

효율성	유형	설명
낮음	- Stop And Wait	- 한번에 1개 프레임 송신, ACK 받으면 다음 프레임 전송
높음	- Sliding Window	- 수신측에서 데이터 수신하면 ACK를 전송, 송신측에서 Window Size 이동하며 전송

- 현대에는 Stop And Wait 방식의 비효율성을 개선하여 데이터 전송 효율성을 높인 Sliding Window 방식으로 흐름제어를 수행

II. 슬라이딩 윈도우(Sliding Window) 설명

가. 슬라이딩 윈도우(Sliding Window) 개념도



개념	- 수신 측에서 설정한 윈도우 크기만큼 송신측에서 확인응답(ACK)없이 전송할 수 있게 하여 흐름을 동적으로 조절하는 제어 기법

나. 슬라이딩 윈도우(Sliding Window) 구성요소

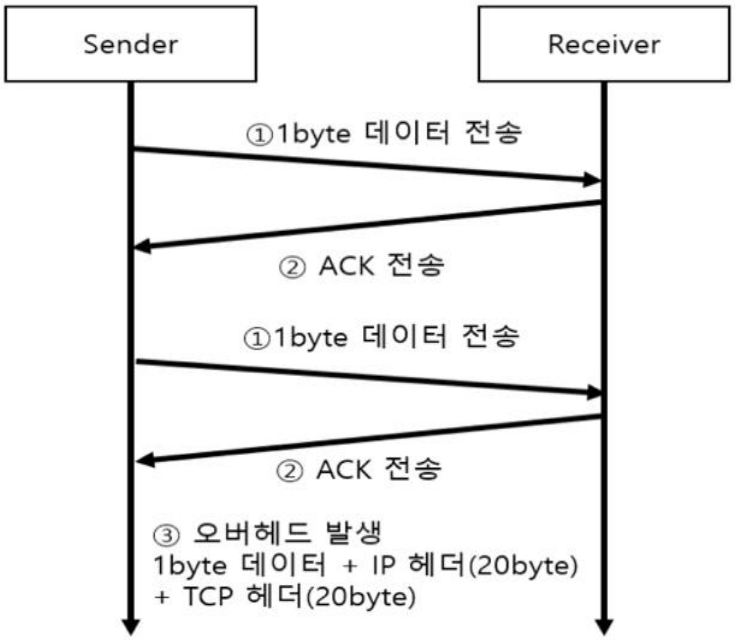
구분	구성요소	설명
기본 요소	- 윈도우(Window)	- 송수신 버퍼 - ACK 없이 즉시 전송 가능한 데이터
	- 윈도우 크기	- Min(rwnd, cwnd) : 수신측 윈도우(RWND)와 혼잡 윈도우(CWND) 중 작은 값으로 결정 - 혼잡상태가 발생하지 않도록 네트워크에서 결정하는 값
동작	- 윈도우 열림	- 수신측 ACK 도착 - 윈도우 우측 경계 오른쪽 이동하여 더 많은 데이터 전송가능
	- 윈도우 닫힘	- 데이터 전송하면 윈도우 좌측 경계 오른쪽 이동하여 더 이상 전송에 관여하지 않는 데이터

- 수신측으로부터 NAK(실패)를 수신하거나 타임아웃 발생 시 송신 측에서는 프레임을 재전송

III. Silly Window Syndrome 및 해결방안

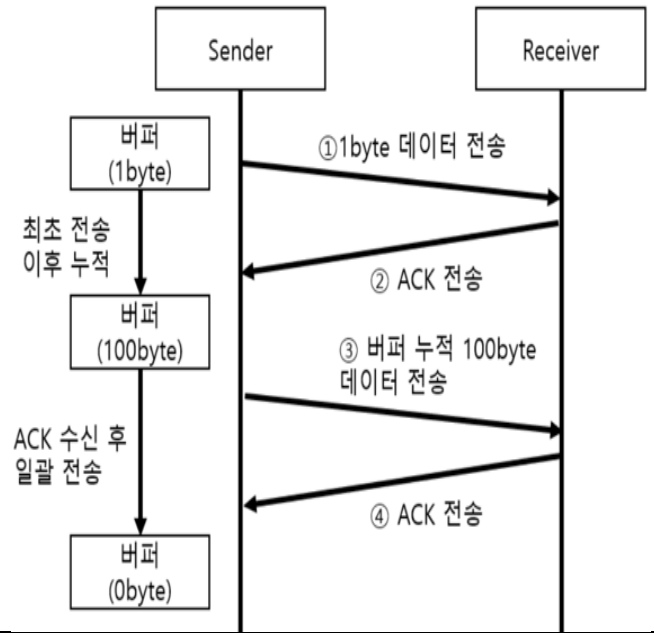
가. Silly Window Syndrome 설명

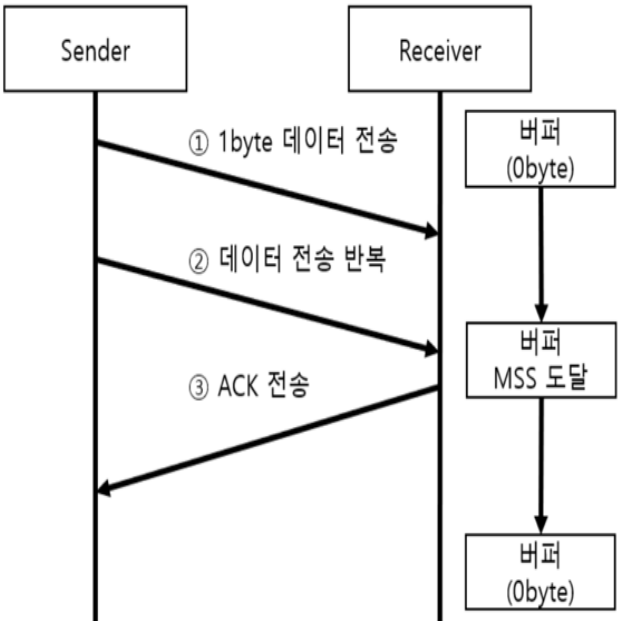
개념	- 데이터를 송수신하는 과정에서 송수신측 응용 프로그램의 낮은 데이터 생성, 소비 속도로 인해 전송 데이터보다 Header, Trailer 데이터의 크기가 더 커짐으로써 비효율성이 증가하는 현상



- 실제 전송되는 데이터보다 캡슐화 과정에서 추가되는 헤더 필드 데이터 사이즈 과다로 인한 오버헤드 발생하는 Silly Window Syndrome을 해결하기 위한 알고리즘 존재

나. Silly Window Syndrome 해결방안

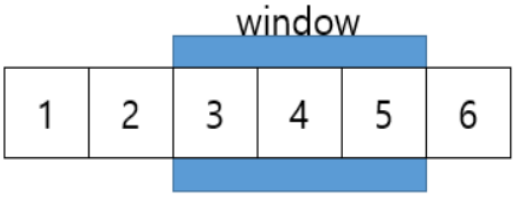
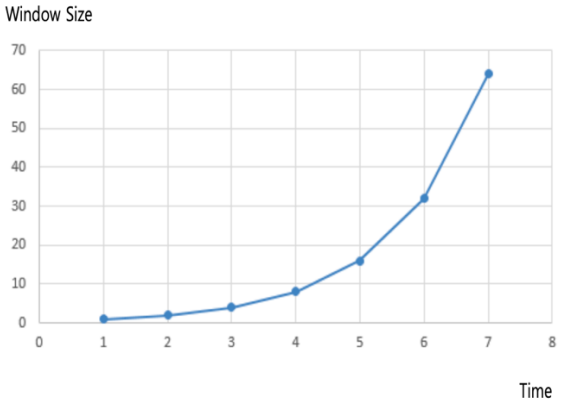
해결방안	개념도	설명
Nagle's Algorithm		- 송신측 해결방안 - 송신측에서 데이터 최초 전송시에는 1byte 그대로 전송하고 이후에는 버퍼에 데이터를 누적시키면서 수신 측에서 ACK를 회신받은 시점에 누적된 버퍼의 데이터를 한번에 전송하는 알고리즘 - MSS(Maximum Segment Size) 이상 모이면 전송하여 작은 세그먼트 감소

Clark's Solution		- 수신측 해결방안 - 수신측에서 버퍼 가용 공간을 확인하여 슬라이딩 윈도우 크기(Window Size)를 0으로 세팅하거나 수신측 버퍼가 MSS(Maximum Segment Size) 만큼 되었을 때 ACK를 회신하는 알고리즘 - 수신 버퍼 확보 시까지 전송 일시 중지 - 수신측은 수신 가능한 윈도우가 MSS 이상 비워질때까지 Window advertising(수신측이 송신측에게 수신가능한 윈도우 크기를 알려주는 것) 하지 않는 것이 핵심

- 송신 측에서는 Nagle 알고리즘, 수신 측에서는 Clark's Solution을 사용하여 작은 패킷 전송과 작은 윈도우 Advertising을 각각 억제함으로써 해결
- TCP의 신뢰성 확보를 위한 혼잡제어 기법으로 Slow Start 존재

IV. TCP의 Sliding Window와 Slow Start 비교

가. Sliding Window와 Slow Start 개념 비교

구분	Sliding Window	Slow Start
개념도		
개념	- TCP 신뢰성 확보를 위해 흐름제어 기능을 수행하는 알고리즘	- TCP 신뢰성 확보를 위해 혼잡제어 기능을 수행하는 알고리즘

나. Sliding Window와 Slow Start 상세 비교

구분	Sliding Window	Slow Start
목적	- 흐름제어 알고리즘	- 혼잡제어 알고리즘
윈도우 구조	- 송신기,수신기 모두에 유사한 윈도우 구조	- 윈도우 크기를 점진적으로 확대
윈도우 크기	- 한번에 전송할 수 있는 최대 프레임 크기	- 1~임계값으로 유동적
필요성	- 송신측의 데이터 전달과 네트워크의 처리 속도 차이를 조절하기 위해 필요	- 네트워크 내에 패킷의 수가 과도하게 증가하는 현상 방지
작동 방식	- 수신 측으로부터 ACK가 도착하여 윈도우의 오른쪽 경계가 오른쪽으로 이동 - 데이터(바이트)가 전송되면 윈도우의 왼쪽 경계가 오른쪽으로 이동	- 혼잡 회피를 위해 초기 윈도우 크기를 1로 시작하며 지수승으로 확대 - Packet Loss 발생시 Congestion Avoidance 단계로 넘어가며 1씩증가

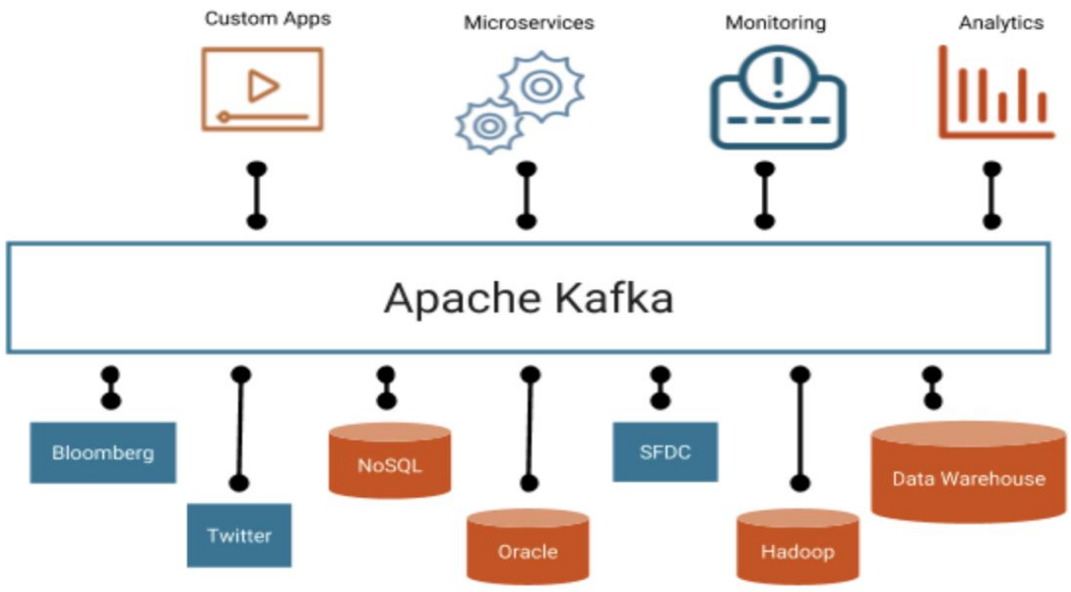
- 전송계층에서의 흐름제어는 전송지연이 매우 가변적이기 때문에 구현이 복잡

"끝"

02	아파치 카프카		
문제	대표적인 메시지 큐 시스템인 아파치 카프카(Apache-Kafka)에 대해서 다음을 설명하시오. 가. 아파치 카프카 개념 및 특징 나. 아파치 카프카와 Redis 비교 설명		
도메인	디지털서비스	난이도	하 (상/중/하)
키워드	Pub/Sub 구조, 멀티프로듀서, 멀티컨슈머, 분산스트리밍, 영속성, 고성능, 확장성, 이벤트브로커, 메시지브로커, 분산형 스트리밍 플랫폼, 인메모리 데이터저장소, 프로듀서·토픽·컨슈머, 채널		
출제배경	대표적 메시징 시스템인 아파치 카프카에 대한 숙지 확인		
참고문헌	ITPE 기술사회 자료		
출제자	박서현 기술사(제 131회 정보관리기술사 / mondaysss@naver.com)		

I. 고성능 분산 메시징 시스템, 아파치 카프카 개념 및 특징

가. 아파치 카프카의 개념



개념	대용량 실시간 로그 처리에 특화된 Pub-Sub 방식의 고성능 분산 메시징 플랫폼

나. 아파치 카프카의 특징

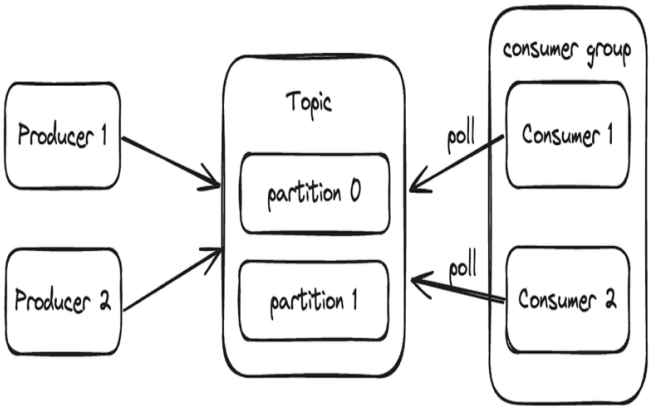
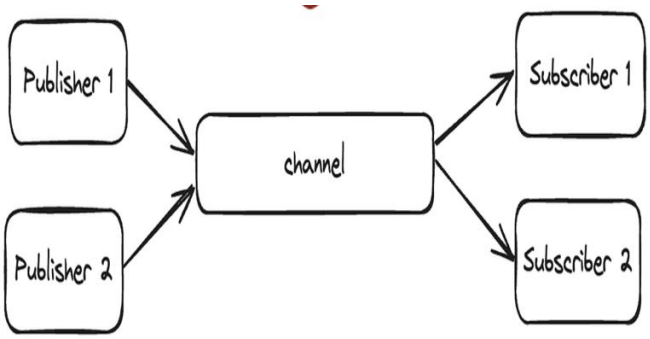
구분	특징	설명
구조	Pub/Sub 구조	- 데이터 생성주체(Pub)와 처리주체(Sub) 구분하여 비동기 처리
	멀티프로듀서, 멀티컨슈머	- 한 토픽에 여러 프로듀서 및 컨슈머 접근 가능
	분산 스트리밍	- 기본적으로 분산 시스템 기반 설계
기능	영속성	- 파일 시스템에 데이터를 일정기간 저장하여 오류 발생 시 데이터를 불러와 재실행 가능
	고성능	- 분산처리, 배치처리를 사용해 고성능 구현 - 대용량 데이터 처리 가능

	확장성	- 브로커 확장을 통해 높은 확장성 제공
	고가용성	- Replication 구현을 통해 고가용성 실현, 주키퍼에 의해 Fault Tolerance 구현

- 대표적인 메시징 시스템에는 아파치 카프카 외에도 Redis, RabbitMQ 등이 존재하며, Redis와는 상호보완적 관계로 시스템에 함께 적용되는 경우가 있음

II. 아파치 카프카와 Redis 비교 설명

가. 아파치 카프카와 Redis 개념 비교 설명

아파치 카프카	Redis
	
- 대규모 실시간 데이터 스트림을 저장·처리·전달하기 위한 분산형 스트리밍 플랫폼	- 캐시·세션 저장 등의 기능을 제공하는 실시간 처리에 최적화된 Key-Value 기반 인메모리 데이터저장 플랫폼

나. 아파치 카프카와 Redis 상세 비교 설명

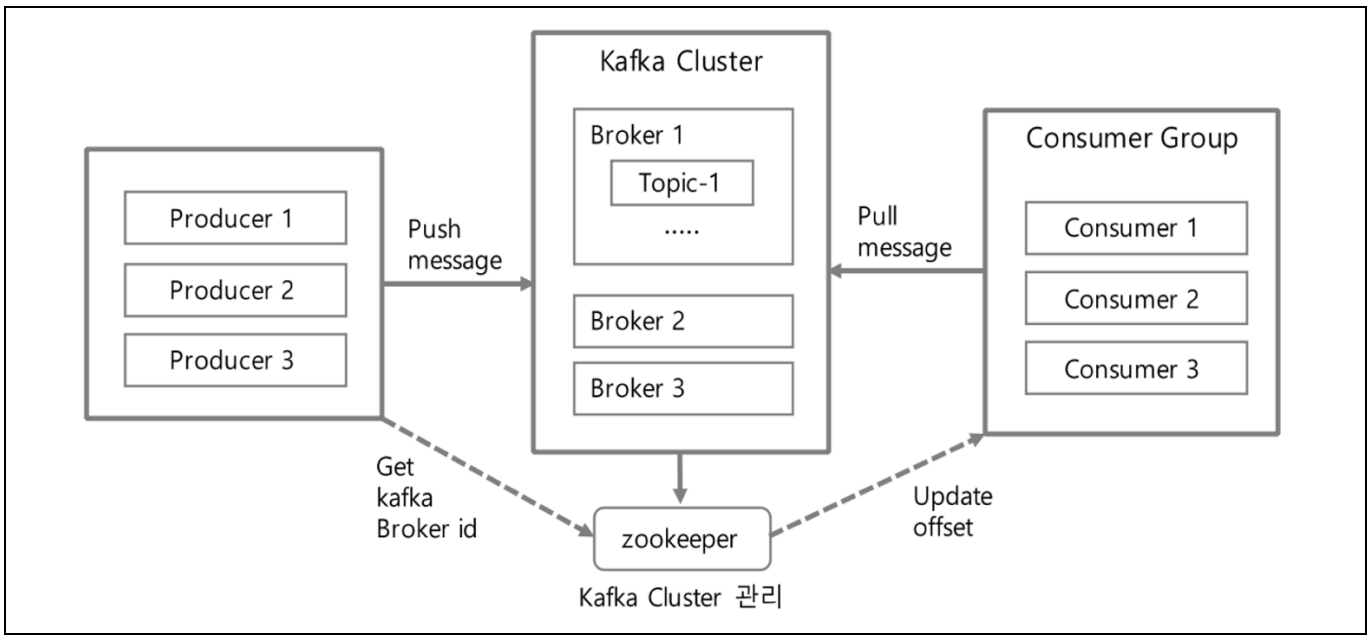
구분	아파치 카프카	Redis
주요 특징	- 대용량 분산처리 메시징 시스템 - 확장이 쉬움 - 이벤트 브로커	- 인메모리 기반 메시징 시스템 - 가볍고 빠름 - 메시지 브로커
목적	- 대규모 실시간 데이터 스트림 처리 - ex) 로그 저장	- 세션관리 등 데이터 캐싱 - ex) 실시간 알림
쓰레드 모델	- 멀티 쓰레드(대규모 스트리밍 병렬 처리 최적화)	- 싱글 쓰레드(빠른 단일처리 최적화)
병렬 처리	- 파티션 단위 병렬 특화	- 인스턴스 내 병렬 처리 없음(순차 실행)
확장 방식	- 파티션, 브로커 확장	- Redis Cluster 확장
구성요소	- Producer - Topic - Partition - Consumer	- Publisher - Channel - Subscriber

	- Broker	
장애 발생 시 메시지 손실	- 거의 없음	- 있음
지연시간	- 낮음	- 매우 낮음
대량 메시지 처리	- 최적화	- 가능하나 비교적 성능 낮음

- Redis와 아파치 카프카의 특성을 이해하여 시스템 내 상호보완적으로 사용 가능
- 이커머스 플랫폼에 적용한다면 Redis는 로그인 세션관리, 장바구니 데이터 저장·처리하는데 적용하고 아파치 카프카를 통해 주문 이벤트 처리(주문 이벤트 발생 시 결제시스템, 배송/물류 시스템에 전달), 이용자 행동분석 등에 적용 가능

III. 아파치 카프카의 동작방식

가. 아파치 카프카의 동작방식 개념도



나. 아파치 카프카의 동작절차

절차	관련 요소	설명
(1)메시지 생성 및 전송	Producer	- 데이터를 생성하는 역할을 담당(ex. 이벤트, 로그데이터 생성)
	Topic	- 생성한 메시지를 Topic이라는 카프카 내의 논리적 구분을 통해 전송
(2)메시지 저장	Broker	- 카프카 클러스터를 구성하는 서버로, Producer로부터 받은 메시지를 저장하는 역할 - Broker는 메시지를 Topic과 Partition 단위로 관리
(3)메시지 소비	Consumer	- Consumer는 메시지를 읽어 가는 역할 - 메시지를 처리하면서 필요에 따라 비즈니스 로직을 수행하고, 메시지를 외부 시스템에 저장하거나 실시간 분석을 수행
(4)메시지 보관 및 삭제	Kafka Cluster	- 메시지를 일정 기간 동안 보관하고, 그 기간이 지나면 메시지를 삭제 - Kafka는 분산 아키텍처를 통해 쉽게 확장이 가능

(5)모니터링	Zookeeper	- 카프카 클러스터의 메타데이터를 관리하고 조정하는 시스템

- 이 과정에서 아파치 카프카는 높은 처리량, 낮은 지연 시간, 높은 가용성을 제공하며, 다양한 실시간 데이터 처리 요구 사항을 충족

IV. 아파치 카프카의 성능향상을 위한 고려사항

가. 소프트웨어 측면의 아파치 카프카 성능향상을 위한 고려사항

구분	고려사항	설명
파티션	- 파티션 수	- 파티션은 병렬 처리의 핵심요소로, 병렬 처리량이 높아질수록 처리량은 증가하지만 파일 핸들 수 증가 및 메타데이터 관리로 인한 오버헤드 발생하여 오히려 성능 저하 발생
프로듀서	- 프로듀서 튜닝	- 프로듀서는 메시지를 배치(Batch) 로 묶어 전송함으로써 네트워크 오버헤드를 줄여 처리량을 극대화 - batch.size(배치로 묶을 최대 바이트 크기 설정), compression.type(메시지 압축 설정) 등의 설정 옵션 활용
컨슈머	- 컨슈머 최적화	- 브로커에서 한 번에 가져올 메시지 크기와 대기 시간을 조정하여 네트워크 왕복 횟수를 줄여 성능 최적화 - 관련 설정값 fetch.min.bytes, fetch.max.wait으로 조정

나. 하드웨어 측면의 아파치 카프카 성능향상을 위한 고려사항

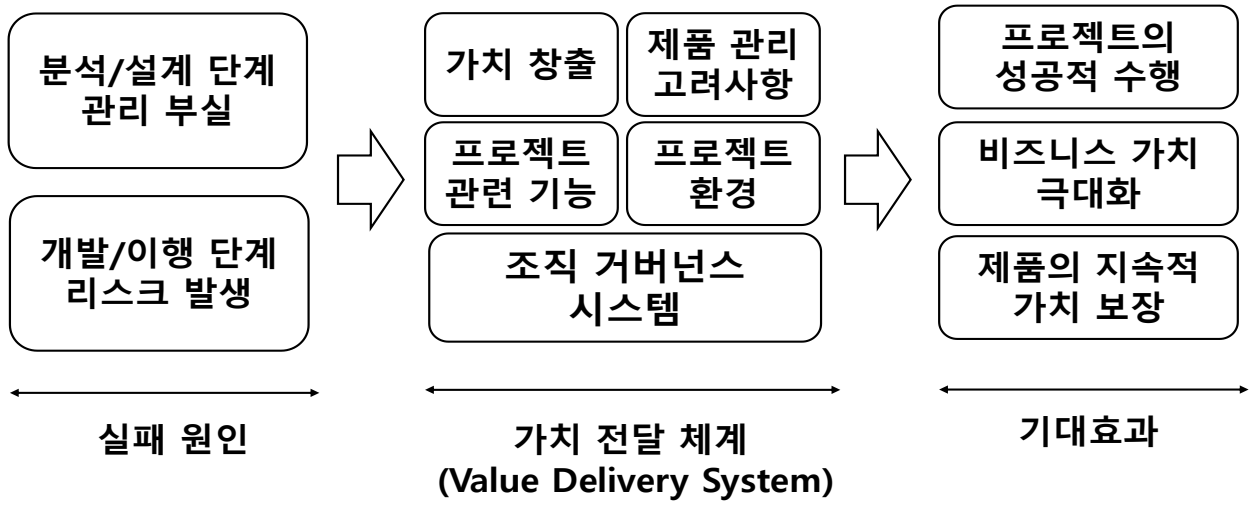
구분	고려사항	설명
코어	- CPU 최적화	- 브로커는 멀티코어 환경에서 병렬 처리 효율 증가
디스크	- SSD 사용	- 카프카의 성능은 디스크의 읽기/쓰기 처리량에 크게 의존하므로 HDD보다는 SSD를 사용하여 높은 처리량 확보 필요
분산화	- 클러스터링	- 메시지를 저장하고 프로듀서/컨슈머의 요청을 처리하는 브로커 노드를 최소 3개 이상 구성하여 고가용성과 안정성을 확보하고, 운영 환경에 따라 필요 시 늘리는 것도 고려

- 아파치 카프카의 높은 처리량, 고가용성 등의 이점을 활용하기 위해 성능 모니터링 및 지속적 개선 필요

"끝"

03	프로젝트 관리		
문제	IT 프로젝트의 성패는 기술 자체보다 조직의 가치 전달 체계(Value Delivery System)가 얼마나 정렬되고 작동하는가에 의해 결정된다. IT 프로젝트가 실패하는 주요 원인을 설명하고 IT 프로젝트를 성공적으로 수행하기 위한 전략을 기술하시오.		
도메인	프로젝트 관리	난이도	상 (상/중/하)
키워드	가치 전달 체계, 가치창출, 조직 거버넌스, 프로젝트 관련 기능, 프로젝트 환경, 제품관리 고려사항		
출제배경	IT 프로젝트의 주요 실패 요소와 가치 기반 성공 전략에 대한 이해 확인		
참고문헌	https://infoofit.tistory.com/353 https://blog.spotodumps.com/index.php/2021/08/12/the-structure-of-the-pmbok-7th-edition-download-free-pmbok-7th-pdf/ ITPE 기술사회 서브노트		
출제자	이다연 기술사(제 135회 정보관리기술사 / dlekdusz@naver.com)		

I. IT 프로젝트의 성공적 수행 위한, 프로젝트 관리 개요



개념	- 조직이 정보기술 프로젝트를 체계적으로 계획하고 실행하여 조직의 IT 목표를 성공적으로 달성하기 위한 관리 체계

II. IT 프로젝트가 실패하는 주요 원인

가. 분석/설계 단계에서의 실패 원인

구분	실패 원인	설명
요구사항 관리 측면	- 불분명한 요구사항 정의	- 프로젝트 초기부터 명확하지 않은 요구사항으로 계획 수립
	- 요구사항의 잦은 변경	- 사용자 기능요구사항의 변경 따른 수행 계획 혼란 초래
	- 비기능 요구사항 누락	- 성능, 품질, 보안 등 사용자 관점에서 중요도가 낮은 요구사항에 대한 미정의
범위 관리	- Scop Creep, Gold Plating	- 정의된 요구사항에 대한 미흡한 구현, 또는 과도한 구현 인한

측면		일정지연, 품질저하 발생
	- WBS 미작성	- 전체 범위 관리 미흡으로 중복 작업, 비용/일정 초과 가능성
설계 측면	- 기술 선정 오류	- 프로젝트 목표에 적합하지 않은 기술 적용 인한 리스크 발생
	- PoC 미수행	- 적용 기술 검토 미흡으로 인한 프로젝트 수행 과제 정의 혼란
계획 수립 측면	- 일정/예산 과소산정	- 현실적이지 않은 비용 및 계획으로 인한 산출물 품질저하
	- 리스크 식별 부족	- 리스크 발생 시 일정 및 비용 초과 가능성, 이해관계자 불만족

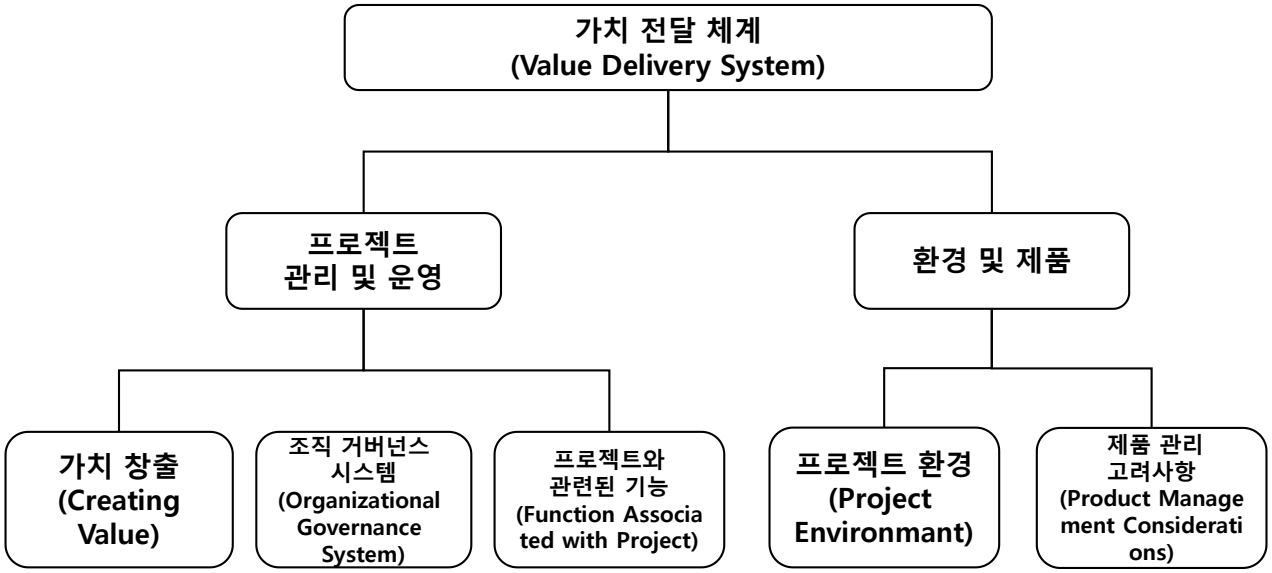
나. 개발/이행 단계에서의 실패 원인

구분	실패 원인	설명
구현 품질 측면	- 개발 표준 미준수	- 코드 품질 저하 인한 성능 문제 발생
	- 구현 오류 증가	- 코드 재작업 증가 인한 일정/비용 초과 가능성 존재
테스트 측면	- 기능 테스트 부족	- 요구사항에 정의된 기능이 올바르게 동작하지 않아 시스템 안정성 저하
	- 비기능 테스트 누락	- 보안, 성능, 품질 테스트 미수행 인한 사용자/이해관계자 불만족
운영 이행 측면	- 데이터 정합성 오류	- 데이터 불일치 인한 시스템 정확성, 안정성, 신뢰성 저하
	- 전환 절차 미흡	- 시스템 이행 시 혼란 초래, 이행 지연 인한 장애 가능성
협업/사용자 측면	- 커뮤니케이션 부족	- 개발과 운영, 관리조직 간 협업 불가로 시스템 구현 시 정확도 저하
	- 사용자 교육 미흡	- 실제 사용자 불만족으로 시스템 활용성 저하

- IT 프로젝트의 성공적 수행 위해 가치 전달 체계 기반으로 전략을 수립하여 프로젝트 수행 관리 필요

III. 가치 전달 체계(Value Delivery System) 설명(PMBOK 7th 기반)

가. 가치 전달 체계(Value Delivery System) 개념



개념	- 조직이 전략적 목표를 달성하기 위해 포트폴리오·프로그램·프로젝트·운영 활동이 상호 연계되어 고객과 이해관계자에게 지속적으로 가치를 제공하는 가치 창출 체계

나. 가치 전달 체계(Value Delivery System) 핵심요소

구분	핵심요소	설명
프로젝트 관리 및 운영	- 가치 창출 (Creating Value)	- 프로젝트에서의 가치 창출을 위해 시스템 내에서 프로젝트가 어떻게 작동하는지 설명
	- 조직 거버넌스 시스템 (Organizational Governance System)	- 거버넌스가 가치 전달 체계를 지원하는 방법
	- 프로젝트와 관련된 기능 (Function Associated with Project)	- 프로젝트 지원 기능 식별, 역할 정의
환경 및 제품	- 프로젝트 환경 (Project Environmant)	- 프로젝트에 영향을 주는 내/외부 요인 식별
	- 제품 관리 고려사항 (Product Management Considerations)	- 포트폴리오, 프로그램, 프로젝트 및 제품이 관련되는 방식 식별

- 가치 전달 체계의 각 핵심요소를 충족시키기 위한 IT 프로젝트 전략 수립하여 적용

IV. 가치 전달 체계(Value Delivery System) 기반 IT 프로젝트 수행 전략

가. 프로젝트 관리 및 운영 관점 IT 프로젝트 수행 전략

구분	수행 전략	설명
가치 창출 측면	- 가치 정렬	- 프로젝트 목표, 범위, 성과지표(KPI)를 비즈니스 전략과 정렬
	- 지속적 검증	- 프로젝트 단계별 산출물 검토 통해 가치 달성 여부 모니터링
	- 가치 기반 변화 수용	- 요구사항 변경을 Value Impact 관점에서 평가, 애자일(Agile) 방식으로 변경 적용
조직 거버넌스 시스템 측면	- 표준화 프로세스 및 템플릿 활용	- 표준 절차 명문화, 준수 노력 - PMBOK, ISO21500 등 표준 및 가이드 기반 관리
	- 규정/정책 감사	- 개인정보보호법, 보안정책, 개발·운영 표준 준수 - 체크리스트 통한 점검 항목 명확화
프로젝트와 관련된 기능 측면	- 통합 관리	- 개발, 운영, 업무 간 조정 역할 적극 수행, 이해관계자 요구 관리
	- 일정/비용 관리	- 규모산정 방법론 활용, EVM 통한 모니터링
	- 위험 관리	- 발생 가능 위험 사전 파악 및 대응방안 선제 마련 - 위험 인한 프로젝트 실패 가능성 최소화
	- 품질 관리	- 테스트 자동화, 정적/동적 분석 도구 통한 QA 프로세스 강화

나. 환경 및 제품 관점 IT 프로젝트 수행 전략

구분	수행 전략	설명
프로젝트 환경 측면	- 내부 환경 관리	- Value chain, BSC, 7S 모델 등을 통한 조직 문화, 개인 역량, 기술체계 파악 통한 수준 분석
	- 외부 환경 분석	- PEST, 5Force 등을 통한 시장, 산업 동향 분석
	- 역량 강화	- OKR 통한 팀과 개인 목표 정렬 - 교육, 지식공유 시스템 통한 역량 개선
제품 관리 고려사항 측면	- 고객 중심 사고방식 적용	- 제품/서비스가 제공하는 가치 중점 구현 - 사용자 경험(UX), 기능성 측면 지속 개선 수행
	- 요구사항 관리	- Product Backlog를 가치 기반 우선순위화 - Shift-Left 방식 요구사항 적용
	- 제품 라이프사이클 관리	- 프로젝트 이후 제품 지속성 고려한 프로젝트 수행 - MVP(Minimum Valuable Product), Lean Startup 기반 신속한 피드백 수행

- IT 프로젝트 성공의 핵심 요소는 비즈니스 가치를 실현하는 것이므로 가치 극대화하기 위한 전략을 세우고 이에 따른 계획을 구체적으로 수립하여 적용하는 것이 중요

"끝"

04	MCP (Model Context Protocol)		
문제	최근 AI 모델 도입이 확산되면서 AI 모델이 외부 데이터 소스를 원활하게 이용하고 협업할 수 있도록 MCP(Model Context Protocol)를 도입하고 있다. 다음에 대해 설명하시오. 가. MCP(Model Context Protocol) 개념 및 필요성 나. MCP(Model Context Protocol) 구성요소 다. MCP (Model Context Protocol) 도입 시 고려사항		
도메인	인공지능	난이도	상 (상/중/하)
키워드	개방형 프로토콜, AI 연동/확장, JSON-RPC, MCP Host, MCP Server, MCP Client		
출제배경	AI의 최신 트렌드 요소에 대한 전반적인 이해 확인		
참고문헌	https://blog.dfinite.ai/mcp-easy-explanation-guide		
출제자	이다연 기술사(제 135회 정보관리기술사 / dlekdusz@naver.com)		

I. LLM 환경의 상호운용성 확보 위한, MCP(Model Context Protocol)의 개념 및 필요성

가. MCP(Model Context Protocol)의 개념

- 대형 언어 모델(LLM) 어플리케이션과 외부 데이터 소스 및 도구 간의 원활한 통합을 가능하게 하는 Anthropic이 개발한 개방형 프로토콜

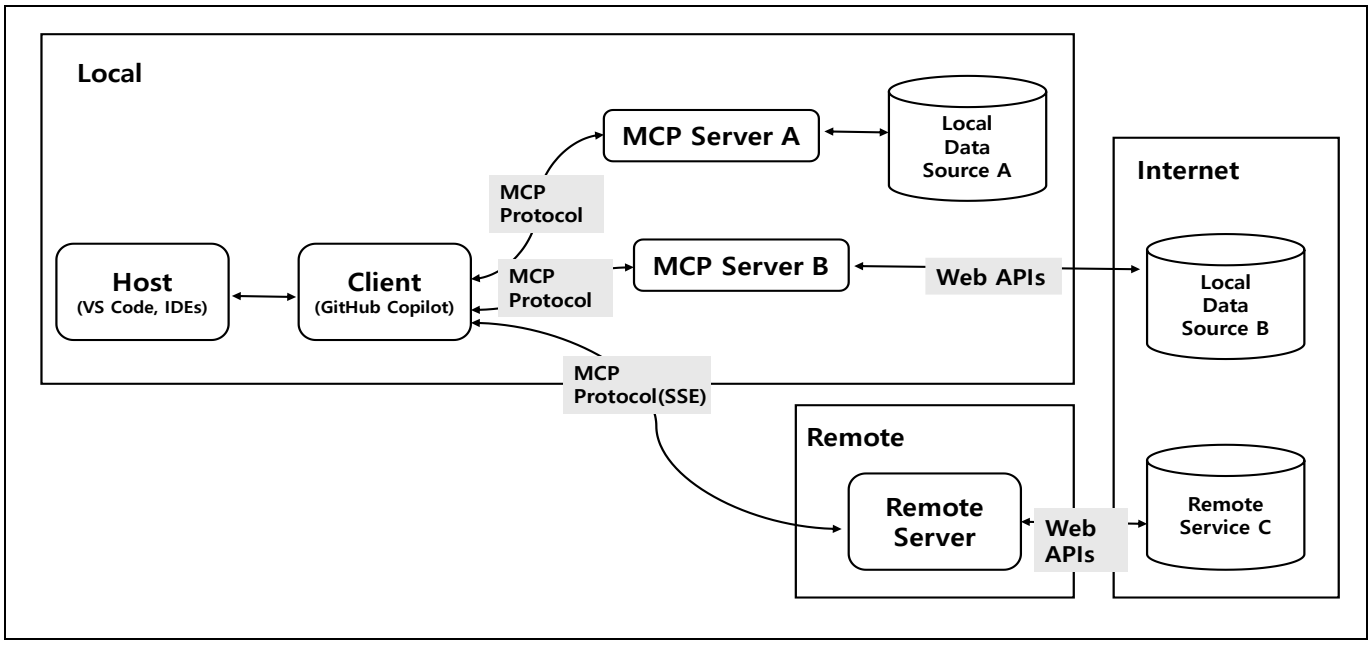
나. MCP(Model Context Protocol)의 필요성

구분	핵심 기술	설명
활용성 측면	- 컨텍스트 표준화 필요성 증가	- 다양한 도구 및 소스와 연동하는 과정에서의 중복 개발 및 비용 증가
	- 모델-도구간 상호운용성 확보	- 플랫폼마다 상이한 모델-도구간 연동방식 인한 호환성 저하
	- AI 에이전트 확장성 보장	- 소스에 연동/활용하기 위한 인터페이스 표준 미비
AI 관리 측면	- 보안/접근제어 요구사항 대두	- AI 연동 시 과도한 권한 부여로 인한 중요 정보 유출 가능성
	- AI 개발/운영 효율성 증대	- AI 모델 또는 소스 변경 시 연동 인터페이스 재개발로 인한 유지보수 부담 증가

- AI 모델과 소스와의 메시지 교환 역할 통해 AI 사용범위 확장 및 잠재력 극대화 역할 수행

II. MCP (Model Context Protocol) 구성도 및 구성요소

가. MCP (Model Context Protocol) 구성도



나. MCP (Model Context Protocol) 구성요소

구분	구성요소	설명
Actor group	- MCP Host	- 하나 이상의 MCP Server를 실행하고 관리하는 인프라 - 예) 개발자들이 만든 자체 MCP 환경
구분 2	- MCP Client	- 사용자의 요청을 생성, MCP Server에 전달하는 인터페이스 - 예) Chat GPT 앱, OpenAI Playground
	- MCP Server	- Client 요청을 수행, 결과를 반환하는 주체 - 예) Open AI의 Code Interpreter 서버
Context Structure	- Resource	- 텍스트, 로그, DB 스키마 등 LLM이 참고 및 활용 할 수 있는 외부 컨텍스트
	- Tool	- 외부 API 또는 기능을 실행하는 명령 단위. LLM이 호출 가능 - 예: 파일 목록 가져오기, 이메일 전송, 데이터베이스 조회 등
	- Prompts	- LLM이 작성해야 할 결과문의 지시문 또는 형식
Communication Protocol	- JSON-RPC 2.0	- Client/Server 간 요청과 응답을 주고 받는 형식 - 표준 입출력(stdin/stdout)이나 HTTP(SSE) 등을 활용

- AI 모델과 소스 간 통신을 표준화하여 상호운용성 및 활용성을 높이고 다양한 분야에서의 AI 활용도를 높여 AI 기능 확장 및 통합을 촉진

III. MCP (Model Context Protocol) 도입 시 고려사항

가. 기술적 관점 고려사항

구분	고려사항	설명
시스템 구조 측면	- 기존 환경과 호환성	- 기존 장비, 시스템과의 프로토콜 호환성 검토
	- 확장성	- 모델, 도구, 소스 추가 시 기능 확장 고려한 설계 필요
성능 측면	- 처리속도	- 모델 호출, 컨텍스트 로딩, 응답 속도 최적화
	- 안정성	- 모델 오류, 예외 처리, 장애 발생 시 복구 체계 확보
	- 에이전트 품질 관리	- 활용 도구 증가 시 적합한 도구 선정 판단 위한 정확도 관리
데이터 관리 측면	- 데이터 보안	- AI 접근 인한 기밀정보, 개인정보, 민감정보 유출 방지 대책 마련 필요
	- 데이터 품질	- 입력 및 소스 데이터의 품질 관리 체계 통한 최신성, 일관성, 정확성 확보

나. 관리적 관점 고려사항

구분	고려사항	설명
전략/목표 측면	- 비즈니스 목표 연계	- MCP 도입이 기업 전략/목표와 부합하는지 검토
	- 효율성 평가 도입	- 도입비용 대비 기대효과 평가 수행하여 효용성 확인
사용자 측면	- 사용자 교육 실시	- 사용자/관리자 대상 MCP 활용 교육
	- 운영/관리 역할 명확화	- MCP 관리, 유지보수 담당 조직 및 R&R 정의
프로세스 관리 측면	- 의사결정 프로세스 도입	- MCP 도입 및 변경 관련 의사결정 프로세스 마련
	- 보안/컴플라이언스 체계 수립	- MCP 관련 보안규제, 정보 유출 및 사고 대응 체계 구축
	- 표준화 프로세스 도입	- MCP 사용 관련 표준 및 프로세스, 운영 메뉴얼 정의

- MCP 도입 시 적용 범위 및 비용을 사전에 산정하여 기존 시스템에 대한 영향도와 연계 가능성 검토를 수행하고 기존 AI 관리 체계와 연계하여 거버넌스를 구축하는 것이 중요

IV. MCP 도입 시 기대효과

- MCP를 활용하여 모델 중심의 의사결정 체계를 고도화하고 데이터와 프로세스의 통합 관리를 통해 장기적인 경쟁력과 산업 보유 역량 강화 가능

"끝"

05	펨토셀(Femtocell)		
문제	최근 국내 이동통신사에서 펨토셀(Femtocell) 장비가 변조되어 이동통신 핵심망(Core Network)에 비인가 접속하는 사고가 발생하면서 소형 기지국 장비에 대한 보안 우려가 커지고 있다. 다음에 대해 설명하시오. 가. 펨토셀 개념 및 주요기능 나. 펨토셀 보안 취약점 및 대응방안		
도메인	정보보안	난이도	상 (상/중/하)
키워드	- (기능) 무선 접속 기능(RAN), 보안 기능, 네트워크 연동 기능, 운영·관리(OAM) 기능, 동기화 기능, 서비스 기능 - (취약점) 장비 물리적 탈취, 펌웨어 조작, 무선 인터페이스 공격, 인증 우회 공격, 허가되지 않은 펨토셀 등록, OTA 업데이트 위변조, 위치 정보 스푸핑, 핸드오버 공격, 트래픽 가로채기, IMSI, IMEI 탈취, SMS·ARS 기반소액 결제 악용 - (대응) 통신·전송 보안, 암호화·인증 강화, 접근 제어·위치 검증, 침해 탐지·대응, 시스템·SW 보안, 정책·운영 관리, 인증·등록 관리, 이용자·운영자 관리, 피해 구제 및 인센티브		
출제배경	최근 KT 불법 펨토셀이용 소액결제 사태에 따른 출제 예상		
참고문헌	ITPE 기술사회 자료 펨토셀 및 GRX 보안 취약점에 대한 연구(KISA, 2013.02.25) KT 불법 이동기지국(펨토셀) 해킹 사태와 대책에 관한 입장(경실련, 2025.09.22) 통신망의 숨겨진 위협, 펨토셀 (1): A사 소액결제 이슈와 긴급 업데이트 분석(2025.10.31)		
출제자	소민호 기술사(제 119회 정보관리기술사 / mhsope@naver.com)		

I. 소형 이동통신 기지국, 펨토셀 개념 및 주요기능

가. 펨토셀의 개념

구분	설명	
개념	- 인터넷 통신 시 전파 음영 지역에 설치해 통화 품질과 데이터 전송 속도를 향상시키는 소형 이동통신 기지국	
필요성	실내 통신 품질 개선	- 건물 내부·지하 등 기지국 신호가 약한 지역에서 음성·데이터 품질을 향상함
	네트워크 용량 확장	- 소형 기지국으로 트래픽을 분산해 매크로셀의 과부하를 완화함
	서비스 안정성 확보	- 혼잡 지역에서도 안정적인 통화·데이터 서비스를 지속적으로 제공함

- 펨토셀은 실내 음영지역의 통신 품질을 향상하고 네트워크 용량을 보완해 서비스 안정성을 높이는 소형 이동통신 기지국

나. 펨토셀의 주요기능

구분	주요기능	설명
무선 접속 기능 (RAN)	LTE/5G 무선 신호 제공	- 가정·사무실 내부에서 LTE·5G 무선 서비스 제공, 단말과 직접 통신 수행
	무선 자원 관리(RRM)	- 스케줄링, 전력 제어, 핸드오버 처리 등 무선 자원 최적화
	셀 커버리지 제공	- 소형 셀 기반으로 실내 음영지역 해소 및 품질 개선
보안 기능	IPSec 터널링	- 펨토셀 ↔ 이동통신사 코어망 간 암호화된 보안 터널 생성
	사용자 인증(EAP-AKA/USIM)	- HSS/UDM을 통해 단말 신원 인증 수행
	접속제어(CSG/ACL)	- 허용된 사용자만 접속하는 닫힌 가입자 그룹 운영
네트워크 연동 기능	백홀 연결	- 가정인터넷(FTTH/케이블)을 통해 이동통신사 코어망과 연결
	시그널링 처리	- 이동통신망(RNC/eNB/AMF)과 제어신호 교환(S1, N2/N3 인터페이스)
	Femto Gateway 연동	- Femto GW(HeNB-GW)를 통한 트래픽 집선·과금·제어 지원
운영·관리(OAM) 기능	원격 관리(TR-069/FMS)	- 구성 변경, 성능 모니터링, 알람 관리, 장애 분석
	원격 소프트웨어 업데이트(OTA)	- 기지국 펌웨어·소프트웨어를 자동 업데이트
	QoS 관리	- 음성/데이터 트래픽 품질을 보장하도록 우선순위·속도 제어
동기화 기능	시간·주파수 동기화	- GPS 또는 PTP 기반으로 기지국 간 간섭 방지를 위한 정밀 동기 제공
	위치 기반 서비스	- 펨토셀 위치 확인 및 기지국 ID·좌표 동기
서비스 기능	음성·데이터 서비스 제공	- LTE/5G 기반의 고품질 음성/데이터 서비스
	커버리지 확장	- 실내 품질 개선, 약전계 지역 해소
	트래픽 오프로드	- 매크로셀 기지국 트래픽 분산 및 네트워크 효율 향상

- 펨토셀은 실내에서 LTE·5G 무선 접속과 보안·네트워크 연동·운영관리·동기화·서비스 제공 기능을 수행해 고품질 통신과 트래픽 분산을 지원

II. 펨토셀 보안 취약점

가. 펨토셀의 기술 측면 보안 취약점

구분	취약점	설명
물리적 보안 취약점	장비 물리적 탈취	- 펨토셀은 가정·사무실에 설치되어 누구나 접근 가능하므로 분실, 도난, 변조 위험 존재
	펌웨어 조작	- 물리 접근을 통해 기기 내부 펌웨어를 변조하여 백도어 삽입, 권한 상승 가능
	디버그 포트 노출	- UART/JTAG 포트 노출 시 내부 OS 접근, 인증키·설정파일 탈취 가능
통신 구간 취약점	백홀 구간 공격	- 가정용 인터넷 기반으로 MITM, 스니핑 등 중간자 공격 가능
	IPSec 설정 오류	- 키 관리 미흡 또는 취약 알고리즘 사용 시 암호화 우회 가능
	무선 인터페이스 공격	- RF 스푸핑·재밍으로 기지국 신호 방해 또는 불법 접속 시도
기지국 기능 취약점	위치 정보 스푸핑	- GPS 스푸핑으로 위치/시간 동기 왜곡 가능
	핸드오버 공격	- 공격자가 단말을 가짜 펨토셀(페이크 셀)로 유도 가능
	트래픽 가로채기	- 내부 패킷 분석을 통해 음성·SMS·데이터 일부 노출 가능
개인정보 탈취 취약점	**IMSI/IMEI 탈취**	- 단말 접속 시 민감 가입자·단말 정보를 탈취 가능
	SMS·ARS 기반 결제 악용	- 본인 인증 SMS 가로채기 또는 위조 인증을 통해 소액 결제 피해 발생

- 펨토셀은 물리적 접근 용이성과 통신·기지국 기능 취약점으로 인해 장비 변조, 불법 접속 등 기술적 보안 위협에 노출됨

나. 펨토셀의 관리/운영 측면 보안 취약점

구분	취약점	설명
접속 관리 취약점	CSG(Closed Subscriber Group) 우회	- 접근제어 목록(ACL) 관리 미흡 시 비인가 단말 접속, 공격자의 승인 리스트 조작 가능
	인증 우회 공격	- EAP-AKA·USIM 절차 중 취약점 활용 시 단말 인증을 우회하여 불법 접속 가능
	허가되지 않은 펨토셀 등록	- 관리 시스템 계정 탈취, API 오남용을 통해 공격자가 악성 펨토셀을 코어망에 등록 가능
운영·관리 (OAM) 취약점	TR-069 프로토콜 취약점	- 기본 계정 방치, 암호 변경 미흡으로 원격 설정 서버 장악 및 대규모 펨토셀 통제 가능
	FMS(운영관리서버) 공격	- 통합 관리서버가 해킹되면 다수 장비에 악성 설정·펌웨어를 일괄 배포 가능
	OTA 업데이트 위변조	- 업데이트 파일 무결성 검증 부재 시 공격자가 악성 펌웨어를 배포 가능
정책 및 절차 취약점	보안정책 미비	- 패치 주기·암호 정책·접속 정책이 명확하지 않아 취약 구성 유지 가능
	운영 절차 부재	- 장비 등록, 철회, 장애 대응 절차 미흡으로 비인가 장비가 지속적으로 운영될 위험

	권한 관리 부족	- 관리자 권한 과다 부여·역할분리(RBAC) 미적용으로 내부자 위협 가능성 증가
공급망(Supply Chain) 취약점	검증되지 않은 펌웨어	- 제조사 업데이트 검증 체계 미흡 시 공급망 공격을 통해 악성 펌웨어 주입 가능
	서드파티 라이브러리 취약	- 펨토셀 소프트웨어 내부 오픈소스 혹은 외부 모듈 취약점이 공격 벡터로 활용 가능
	출고 전 보안 설정 미흡	- 출하 시 기본 패스워드·디버그 포트 활성 상태 등 초기 보안 설정 미비
모니터링·감사 취약점	이상 접속 탐지 부재	- 비정상 접속·트래픽 증가·인증 실패 반복 등을 탐지하는 모니터링 기능 부족
	로그 무결성 미보장	- 운영 로그가 조작되거나 삭제될 수 있어 침해 사고 분석 어려움
	감사·점검 체계 미흡	- 주기적인 보안 점검·구성 검증 부재로 취약점이 장기간 방치됨
기기 관리 부실	비인가 펨토셀 등록	- 장비 등록 승인 절차 미비로 공격자가 악성 기기를 코어망에 등록 가능
	철회/폐기 미처리	- 사용 중지된 펨토셀이 네트워크에 계속 연결되어 공격 통로로 악용 가능
	기기 라벨링·자산관리 미흡	- 설치 위치·관리번호 부재로 장애·침해 발생 시 추적 대응이 어려움
	무단 설치 및 이동	- 설치 위치 변경, 가정/사무실 이동 시 재인증·검증 절차 부재
	물리적 보호 없음	- 케이싱 잠금·탬퍼링 알람 미적용으로 기기 분해·키 탈취 가능
	설치환경 검증 부족	- 라우터/네트워크 보안 설정 부실(포트포워딩, DMZ 노출)로 공격 노출 확대

- 펨토셀은 물리적 접근 용이성, 통신 구간·접속 관리·운영관리 취약점, 기지국 기능 악용, 개인정보 탈취 등 다양한 보안 위협에 노출

III. 펨토셀 보안 취약점 대응방안

가. 펨토셀의 기술 측면 대응방안

구분	대응	설명
통신·전송 보안	IPSec 강력 암호화 적용	- 백홀 구간에 강력한 암호화(AES) 및 안전한 키 교환 방식 적용
	암호화된 백홀 (IPSec/mTLS)	- 펨토셀–코어망 간 통신은 인증서 기반 IPSec/mTLS로 암호화, 키 관리 체계 적용
	무결성 보호	- 데이터 변조 방지 위한 무결성 체크(ICV, integrity check) 적용
암호화·인증 강화	PKI 기반 양방향 인증 (X.509)	- 장비·서버 간 상호 인증으로 가짜 펨토셀 차단, 관리 명령·업데이트 출처 검증
	다단계 인증(OTP/생체)	- 관리자 계정 탈취를 어렵게 하여 원격 설정 변경·악성 펌웨어 업로드 방지
	USIM/EAP-AKA 인증 강화	- 단말–셀 간 상호 인증 강화로 비인가 단말 접속 차단
접근 제어·위치 검증	GPS/Cell-ID 교차검증	- 위치·Cell-ID 불일치 시 이동·위치 변조 의심, 불법 장비 탐지
	MAC/IMEI 기반 허용 목록	- 허가된 MAC/IMEI 장비만 백홀·관리 포트 접근 가능하도록 제한
	CSG/ACL 기반 접속 제어	- 허용 단말 리스트 기반 접속 제한으로 비인가 단말 차단
침해 탐지·대응	IDS/IPS 연동	- 비정상 트래픽·스푸핑 공격·접속 패턴을 실시간 탐지 후 차단
	SIEM 기반 상관 분석	- 여러 로그를 통합 분석해 공격 징후 조기에 탐지
	보안 로그 분석	- 비정상 무선 신호·접속 기록 분석 및 경보
시스템·SW 보안	OTA 업데이트 서명 검증	- 악성 펌웨어 배포 방지를 위해 업데이트 파일에 대한 서명·무결성 검증
	TR-069/OAM 인터페이스 보안 강화	- 인증·암호화 필수화, 기본 계정 삭제, 불필요 포트 차단
	JTAG/UART 포트 차단	- 디버그 포트 비활성화로 펌웨어 추출·변조·권한 상승 방지

- 펨토셀 보안은 통신 암호화·강력 인증·접근 제어·침해 탐지·시스템 보호 등을 강화해 물리·네트워크·운영 단계의 위협을 종합적으로 차단

나. 펨토셀의 관리/운영 측면 대응방안

구분	대응	설명
정책·운영 관리	보안 정책 및 운영 기준 수립	- 펨토셀 설치·운영·접속 관리 절차(SOP)를 정의해 운영 안정화
	정기 보안 점검	- 설정 변경, 접근 이력, 설치 위치 등을 정기 점검하여 이상 탐지
	펨토셀 회수 체계 강화	- 폐업·이사 등 사용 중단 장비의 전수조사·회수를 의무화해 불법 사용 방지
인증·등록 관리	인가된 기지국 인증	- 사업자 승인 장비만 운용되도록 인증 절차 운영하여 위조 장비 차단
	자산관리·장비등록 체계	- 펨토셀 고유 ID·설치 위치·소유자 정보를 DB에서 관리하여 장비 이력 추적
	기본 계정 제거 및 접근 관리 정책	- OAM/TR-069의 기본 계정 삭제, 강력 비밀번호 정책 적용
이용자·운영자 관리	보안 교육·인식 제고	- 이용자·관리자가 장비 분실·도난 및 비인가 접근 위험을 인지하도록 교육
	사고 신고·대응 절차 정립	- 사고 발생 시 신고·격리·조사 절차 마련 및 이용자에게 공지
	소액 결제 차단 서비스 제공	- 이용자가 소액 결제 한도 조정·차단을 할 수 있도록 안내해 스미싱 악용 예방
피해 구제 및 인센티브	피해 구제 절차 마련	- 유령 기지국·피싱 등 피해 발생 시 보상 및 신속 처리 절차 마련
	유령 기지국 신고 포상제	- 불법 기지국 신고 활성화를 위해 신고 포상제 운영

- 펨토셀의 관리적 대응은 정책·인증·교육·신고체계 등을 체계화하여 운영 과정에서의 인적·관리적 보안 위험을 예방하고 통제

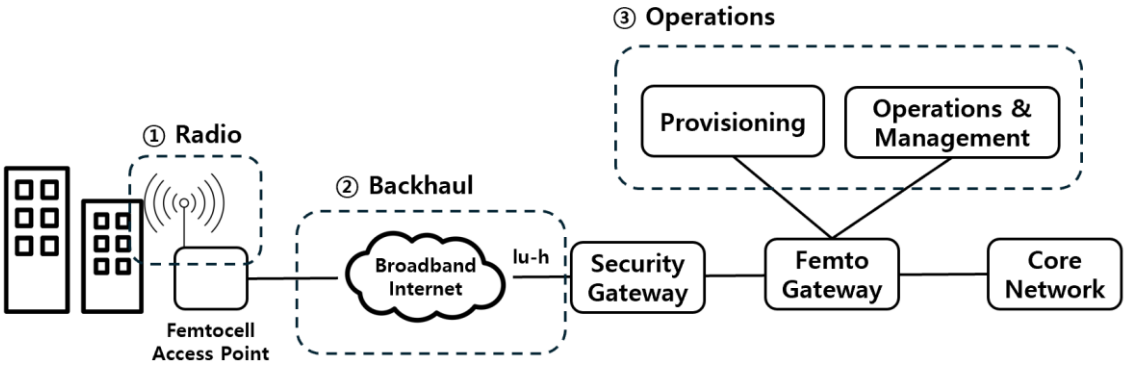
IV. 펨토셀의 고려사항

구분	고려사항	설명
설치·환경	최적 설치 위치 선정	- 실내 음영구역 개선 효과가 극대화되도록 전파 도달 범위, 장애물, 간섭 요소를 고려해 설치 필요
	백홀(Backhaul) 회선 품질 확보	- 펨토셀이 인터넷망을 통해 Core망에 연결되므로, 안정적인 유선 회선 속도·지연·패킷손실 관리 필요
전파·품질	매크로셀 간 간섭 관리	- 소형 기지국 특성상 주변 매크로 기지국과의 전파 간섭 방지 위해 출력 조절·주파수 계획 필요
	핸드오버 품질 관리	- 펨토셀 ↔ 매크로셀 이동 시 핸드오버 지연·끊김 방지 위해 파라미터 최적화 필요
운영·정책	가입자 접근 정책 설정	- 허용 단말만 접속시키는 폐쇄형(Closed) 또는 개방형(Open) 여부를 환경에 맞게 결정해야 함
	유지보수 및 원격관리	- 장애 대응을 위해 원격 로그 수집, 장비 상태 모니터링, 자동 업데이트 등 OAM 기능 고려 필요
보안·규제	장비 인증 및 적합성 확인	- 통신사·국가의 장비 인증, 전파법 적합성 평가(KC), 보안 인증 여부 확인 필요
	사용자 프라이버시 보호	- 펨토셀 이용 시 위치·통신기록 정보가 처리되므로, 개인정보 보호 규정·법적 요구사항 준수 필요
장비 생애주기 (Lifecycle)	노후 장비 회수·폐기 관리	- 사용 종료·보안 지원 중단된 펨토셀을 적시에 회수하고, 보안 취약 장비의 무단 사용을 방지해야 함
	반납·교체 절차 표준화	- 통신사는 교체·반납 절차를 명확히 정의하고, 사용자·대리점·택배 회수 등 일관된 프로세스를 운영해야 함

- 펨토셀은 설치·운영·보안·장비 관리 전 과정에서 체계적인 생애주기(Lifecycle) 관리가 필수적

"끝"

[참고] 펨토셀의 구성요소



구분	구성요소	설명
기지국 기능	FAP(Femto Access Point)	- 가정·사무실에 설치되는 초소형 기지국으로 LTE/5G 무선 신호 송수신 및 단말 연결 처리
	RF 모듈	- 무선 송·수신 및 주파수 변조·증폭을 수행하는 물리 계층 장치
	Baseband 프로세서	- 무선 프로토콜(L1/L2/L3) 처리, 스케줄링, 단말 관리 등 기지국 핵심 제어 기능 수행
네트워크 연동 기능	브로드밴드 백홀	- 가정용 인터넷(광·케이블)을 통해 이동통신 코어망으로 연결하는 유선 통신 경로
	Security Gateway (IPSec 게이트웨이)	- 펨토셀 ↔ 이동통신사 코어망 간 암호화·무결성 터널(IPSec) 생성
	Femto Gateway(HeNB-GW)	- 대규모 펨토셀 트래픽 집선, 시그널링 처리, 인증/과금 연동 수행
	RNC/eNB/AMF 연결 모듈	- 3G·LTE·5G 코어망으로 접속하기 위한 표준 인터페이스(S1, N2/N3) 제공
운영/관리 기능 (OAM)	FMS(Femto Management System)	- 펨토셀 원격 모니터링, 정책 배포, 소프트웨어 업데이트 수행
	ACS(TR-069 기반)	- 자동 구성 서버로, 초기 설정/보안정책/QoS 정책을 자동 배포
	CSG/ACL 관리	- 허용 가입자 리스트 기반의 닫힌 사용자 그룹 제어 기능
보안/인증 기능	IPSec 터널 모듈	- 외부 인터넷 환경에서 펨토셀 트래픽 보호용 암호화 및 무결성 제공
	USIM 인증 연동	- HSS/UDM과 연동하여 단말 인증 수행
부가 기능	GPS 모듈	- 시간·주파수 동기화, 위치 확인 수행
	QoS 모듈	- 음성·데이터 품질 보장, 우선순위 제어 기능
	전원 관리(PoE 가능)	- 원격 전원 제어 및 저전력 운영 기능

[참고] 펨토셀의 기술요소

기술	세부기술	설명
무선 접속 기술 (RAN)	LTE, 5G NR	- 펨토셀이 제공하는 무선 인터페이스로, 단말과의 무선 통신을 처리
	RF 신호처리	- 송수신·주파수 선택·필터링·증폭 등 물리 계층 무선 신호 처리
	Baseband 신호처리	- OFDM·MIMO·HARQ 등 무선 통신 프로토콜 처리
보안 기술	IPSec	- 펨토셀과 코어망 간 암호화된 터널링을 제공하여 보안성 확보
	EAP-AKA, USIM 인증	- 이동통신 단말의 가입자 인증 절차로 HSS/UDM과 연동
	CSG(Closed Subscriber Group)	- 허용된 단말만 접속하도록 제어하는 접근제어 기술
네트워크 연동 기술	S1(3GPP), N2/N3	- LTE/5G 무선 접속망과 코어망을 연결하는 표준 인터페이스
	브로드밴드 백홀	- 펨토셀이 인터넷망을 이용해 사업자 코어망과 연결되는 구조
	Femto Gateway(HeNB-GW)	- 다수 펨토셀의 집선·관리·시그널링 처리 기술
관리·운영(OAM) 기술	TR-069	- 기지국 원격 설정 및 자동 프로비저닝 기술
	FMS	- 대규모 펨토셀을 중앙에서 관리·모니터링하는 관리 기술
	소프트웨어 OTA 업데이트	- 원격으로 구성 변경 및 소프트웨어 업그레이드 수행
동기화 기술	GPS 기반 동기화	- 시간·주파수 동기 제공하여 기지국 간 간섭 최소화
	IEEE 1588 PTP	- 네트워크 기반 정밀 시간 동기화 기술
품질 보장(QoS) 기술	우선순위 기반 QoS	- 음성/데이터 트래픽을 구분하여 품질 보장
	트래픽 셰이핑	- 백홀 구간의 과부하를 방지하기 위해 트래픽을 제어

06	재해복구		
문제	국가정보자원관리원 화재이후 재해복구의 중요성이 더욱 높아지고 있다. 다음 내용을 설명하시오. 가. 재해복구시스템 구축 절차 나. BIA(Business Impact Analysis) 다. DRaaS		
도메인	IT경영	난이도	하 (상/중/하)
키워드	비즈니스 연속성 보장, 위험분석, 비즈니스 영향도 분석, 관리형DRaaS, 지원형DRaaS, DIY DRaaS ,' 비용효율, 복구시간단축		
출제배경	증가되는 보안사고, 재난, 재해로부터 비즈니스 연속성을 위한 체계적인 재해복구절차를 이해하고, 신기술을 적용한 재해복구서비스를 고려할 수 있음		
참고문헌	ITPE 서브노트 https://www.ibm.com/kr-ko/think/topics/draas		
출제자	배미경 기술사(제 135회 정보관리기술사 / hjmom0727@daum.net)		

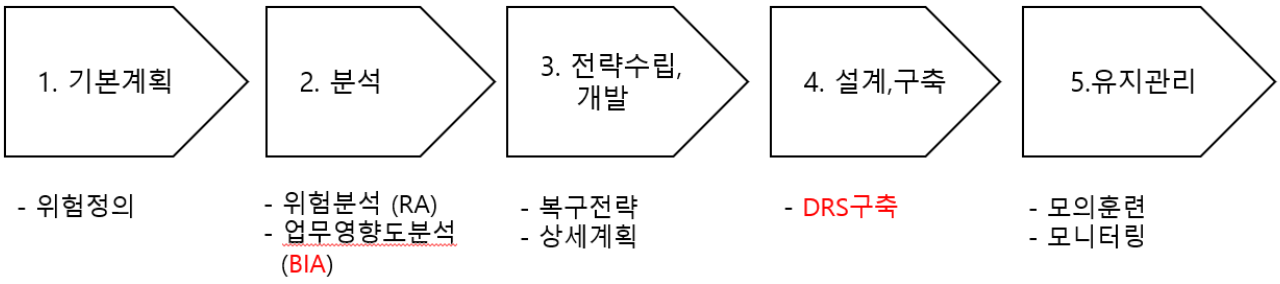
I. 비즈니스 연속성을 위한 전략, BCP(Business Continuity Planning)의 필요성

BCP 개념도	
BCP 개념	- 장애, 재난, 해킹 등 위기상황에서도 신속하고 체계적인 대응을 통해 비즈니스 연속성을 보장하기 위한 체계 및 관련 활동
필요성	- 신속한 핵심업무의 복구로 비즈니스 연속성 확보 - 재정적 손실 최소화 - 기업 이미지 및 신뢰도 유지 - 규제 및 법규 준수

- **비즈니스 연속성 보장**을 위해 체계적인 구축절차 검토와 영향도 분석(BIA), 신기술 이용 DR 서비스 적용 등으로 신뢰성과 비용효율성 증대가 가능

II. 재해복구시스템 구축 절차

가. 재해복구시스템 구축 절차의 개요



- 재해복구 시스템 구축은 계획, 분석, 전략수립, 개발, 설계, 유지관리 단계로 이루어지며, 일회성의 구축이 아니라 비즈니스 변화에 따른 정기적 분석 및 전략개선, 정기적 모의훈련을 통한 개선이 필요

나. 재해복구시스템 구축 절차의 상세

구분	구축 절차	설명
기본계획	- 환경분석 및 위험정의	- 경영환경분석, 업무분석, 전산환경분석 - 위험정의: 발생 가능한 위험에 관한 정의, 재난등급 정의
분석	- 위험분석 (RA : Risk Analysis)	- 업무 중단을 야기 시킬 수 있는 잠재적 위험요소 파악 - 현재 예방대책 수준진단으로 보안방향 도출 - 기술위험 및 업무영향을 정량적, 정성적으로 분석
	- 업무영향도 분석 (BIA : Business Impact Analysis)	- 업무를 대상으로 재해복구 최소단위 업무파악 - 업무중단에 의한 재무/비재무적 피해평가 (BIA) - 복구 우선순위 도출 : 복구목표시간(RTO), 복구목표지점(RPO)기준
전략수립, 개발	- 복구전략	- 예방체계 수립, 대응전략 수립 - 복구 우선순위에 의한 핵심업무 복구전략 수립 (복구정책, 복구조직, 복구전략, 중단 시나리오)
	- 계획개발	- 업무 및 전산시스템의 복구를 위한 상세계획 수립 (위험예방, 비상대응, 업무복구 및 복원, DRP, 대체사업장소등)
설계,구축	- DR시스템, 대체사업장 구축	- DR구축 : Mirrored, Hot, Warm, Cold - BCP관련조직, 대체사업장 마련
유지관리	- 모니터링/ 테스트	- BCP모니터링 및 경영진 보고 - 테스트를 통하여 미비점 파악 및 BCP계획 및 전략보완 - 반복적인 BCP 모의훈련(최소 1년한번) 과 피드백

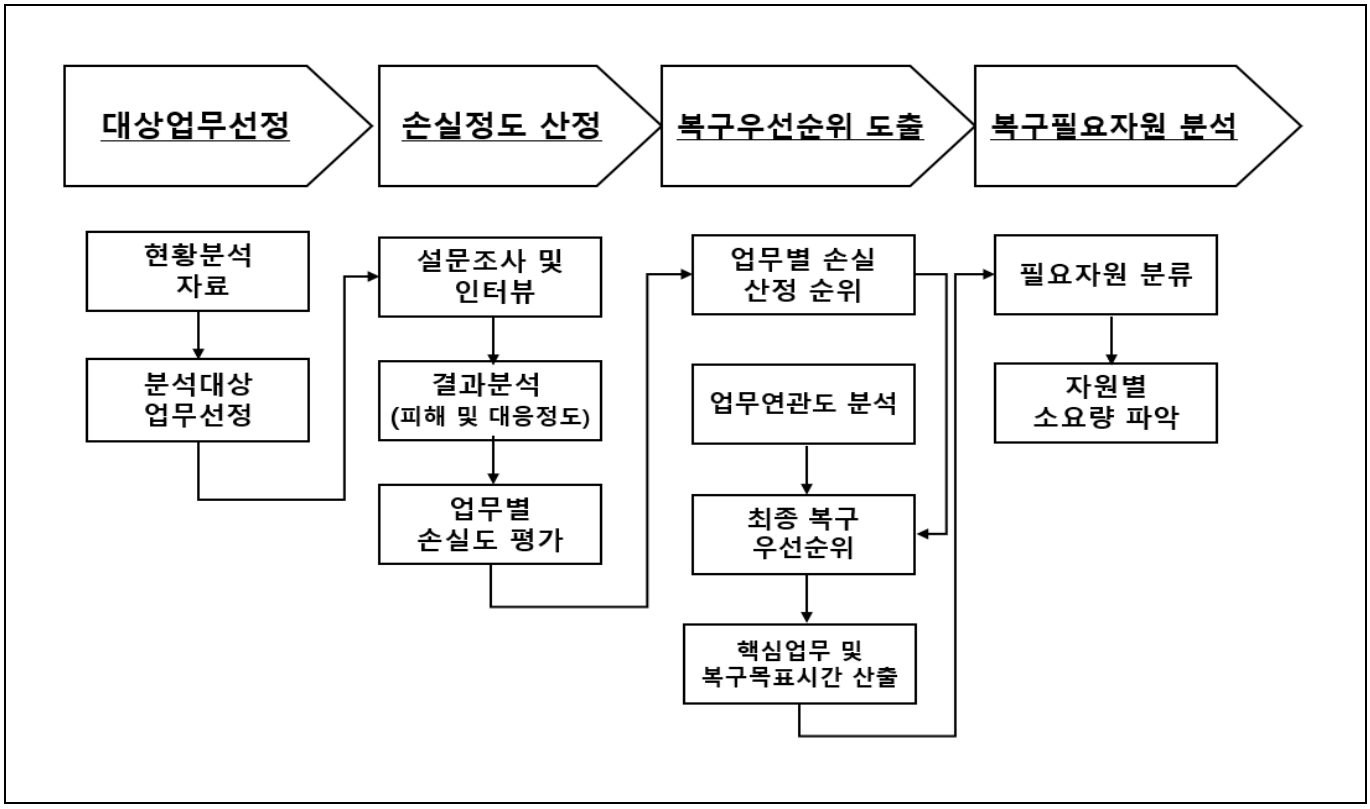
- 재해복구 시스템 구축은 시간과 비용이 많이 들어가므로 비즈니스 영향도(BIA)를 분석하여 차등화된 복구전략 수립이 필요

III. BIA(Business Impact Analysis)

가. BIA(Business Impact Analysis)의 개념

구분	설 명	
개념	- 재해 발생시 영향을 미칠 수 있는 단위업무를 정의하고, **업무중단 영향**에 대한 **정량적, 정성적 분석**을 통해 **복구 우선순위** 및 **복구목표**를 도출하는 **BCP의 핵심절차**	
목적	- 핵심 우선순위 결정	- 모든 핵심적 사업단위 프로세스를 부여하고 우선순위를 부여
	- 중단시간 산정	- 경쟁력 있는 기업으로 살아남기 위해 견딜 수 있는 최대 복구가능한 중단시간 산정
	- 자원 요구사항 분석	- 핵심 프로세스 또는 민감한 프로세서에 할당되어야 하는 자원 요구사항 분석

나. BIA(Business Impact Analysis)의 수행 절차



- BIA(Business Impact Analysis)을 통하여 재무적, 비재무적 지표에 따른 손실 산출 및 복구 순위 도출

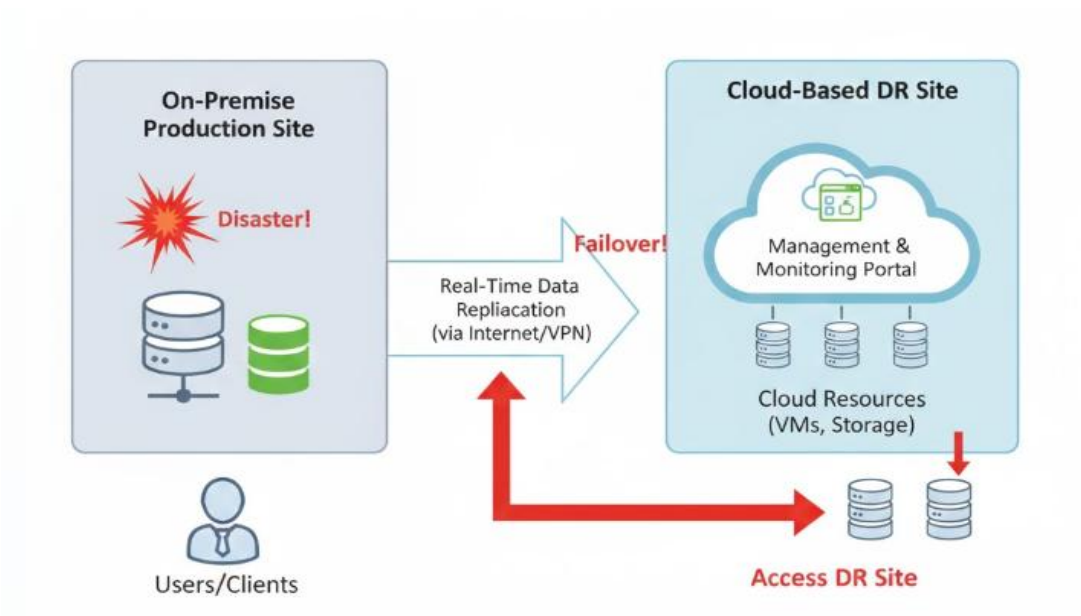
다. BIA(Business Impact Analysis)의 도출 사항 (주요 지표)

지표	설명	사례
RSO	- Recovery Scope Objective - 복구 대상이 되는 핵심업무 범위	- 인사계, 정보계, 대외계, 계정계 - 재난대비 단순 대이터 백업
RPO	- Recovery Point Objective - 핵심 업무의 복구를 위한 복구수준	- 특정 백업시점 데이터 복구 - 전일마감 데이터 백업시점 - 재해발생 시점 데이터 복구
RTO	- Recovery Time Objective - 업무 재개를 위해 필요한 시간	- 즉시, 2시간내, 4시간내, 8시간내, 24시간내
RCO	- Recovery Communication Objective - 네트워크 복구목표	- 지점, 주요 영업점, 전 영업점
BCO	- Backup Center Objective - 백업센터 구축목표	- 자체 재해복구시스템 구축

- BIA(Business Impact Analysis)를 통한 지표기반으로 복구목표를 산정하고 DRS 구축 방안을 마련함
- 클라우드 서비스를 이용한 DRS 시스템 구축으로 구축시간 및 비용효율을 증대 가능

IV. DRaaS(Disaster Recovery as a Service)

가.DRaaS(Disaster Recovery as a Service)의 개념

<table>
<tr><td>DRaaS 개념도</td><td colspan="2"> 
</td></tr>
<tr><td>DRaaS 개념</td><td colspan="2">- 클라우드 서비스를 통해 데이터를 보호하고, 재해나 장애 발생시 IT 환경을 신속하게 복구하여 비즈니스 운영을 지속할 수 있도록 지원하는 서비스</td></tr>
<tr><td rowspan="2">기대효과</td><td>- 비용 효율</td><td>- 초기투자 비용 절감, Pay per Use</td></tr>
<tr><td>- 신속한 복구</td><td>- 자동화된 복구 프로세스를 통해 최소한의 다운타임으로 복구 가능</td></tr>
</table>

	- **확장성**	- 클라우드 유연성 활용 데이터 증가와 서비스 확장이 용이
	- **보안 강화**	- 서비스 제공자는 데이터 암호화, 보안인증, 침입탐지 등 고급 보안기능 제공
	- **글로벌 접근**	- 여러 지리적 위치에 분산된 데이터 복제 지원

나. DRaaS 의 유형

모델	동작 방식	설명
관리형 DRaaS	- 전체 재해복구 과정을 DR 서비스 업체에 아웃소싱	- DR서비스 제공업체가 인프라, 클라우드, 온프레미스 서버, 하이브리드 시스템을 보호할 책임 - DR테스팅, 검증, 운영, 정비, 관리를 담당하고 재해 발생 시 서비스업체의 직원이 fail-over 과정을 관리 - DR서비스 제공업체에서 RPO 및 RTO 등을 포함하는 서비스수준계약 (SLA)를 제공
지원형 DRaaS	- 기업이 DR과정을 통제하면서 통합, 테스팅 담당	- 기업이 클라우드 서비스를 이용한 복제와 복구에 대한 테스팅 등을 담당하고, DR서비스 제공업체는 이에 대한 지원 - 고객 맞춤형으로 제작된 어플리케이션을 보유한 기업은 필요 한 경우에만 DR서비스 제공업체가 개입하는 지원형 서비스 도입
DIY형 DRaaS	- 기업이 DR 전체과정을 자체 관리	- IT조직 규모가 크고, 전문지식을 보유한 직원을 보유한 기업을 대상으로 클라우드에서 외부 복 제 및 호스팅의 이점을 제공 - 기업이 통합, 테스팅, 검증을 책임져야 하며, 재해발생 시 failover 과정을 직접 관리

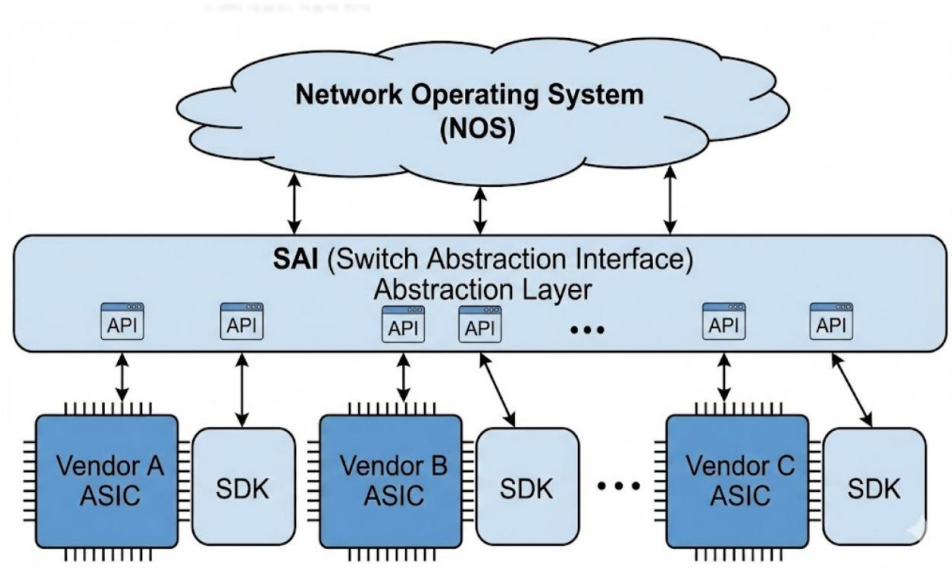
- 기업 정보기술팀의 조직규모와 전문기술 인력 보유 여부 등에 따라 DR서비스 유형을 결정

"끝"

06	SAI(Switch Abstraction Interface)		
문제	오픈 네트워크 프로젝트(OCP) 생태계 기반의 네트워크 기술 중 SAI(Switch Abstraction Interface)가 핵심표준기술로 자리잡고 있다. 다음을 설명하시오 가. SAI 개념 및 특징 나. SAI 구조 와 기술요소 다. SAI 표준기술의 시사점		
도메인	네트워크	난이도	상 (상/중/하)
키워드	벤더독립성, 하드웨어 추상화, OCP, NOS, Disaggregation, SAI API, SAI Adapter, Vendor SDK, ASIC, Syncd, 오픈 네트워킹 , TCO		
출제배경	개방형 혁신을 위한 네트워크 표준기술로 빠르게 발전, 진화하고 있는 SAI의 이해		
참고문헌	https://tilnote.io/pages/68c7c817beb70e99e0755eb3 https://www.opencompute.org/documents/switch-abstraction-interface-ocp-specification-v0-2-pdf		
출제자	배미경 기술사(제 135회 정보관리기술사 / hjmom0727@daum.net)		

I. 클라우드 네트워킹 혁신의 핵심, SAI(Switch Abstraction Interface)의 개념 및 특징

가. SAI(Switch Abstraction Interface)의 개념

SAI 개념도	
SAI 개념	- 네트워크 스위치 ASIC을 추상화하여, 상위 네트워크 OS가 **특정 벤더 칩에 종속되지 않고** 공통 API를 통해 스위치를 제어할 수 있도록 만들어주는 표준화된 API 인터페이스

- OCP(Open Compute Project) 네트워킹 분야에서 SAI는 데이터센터 스위치를 좀 더 유연하고 효율적으로 관리할 수 있도록 해 주는 기술로, 네트워크 장비의 새로운 표준으로 적용이 확대되고 있음
- MS가 주도하여 OCP에 제공한 표준기술

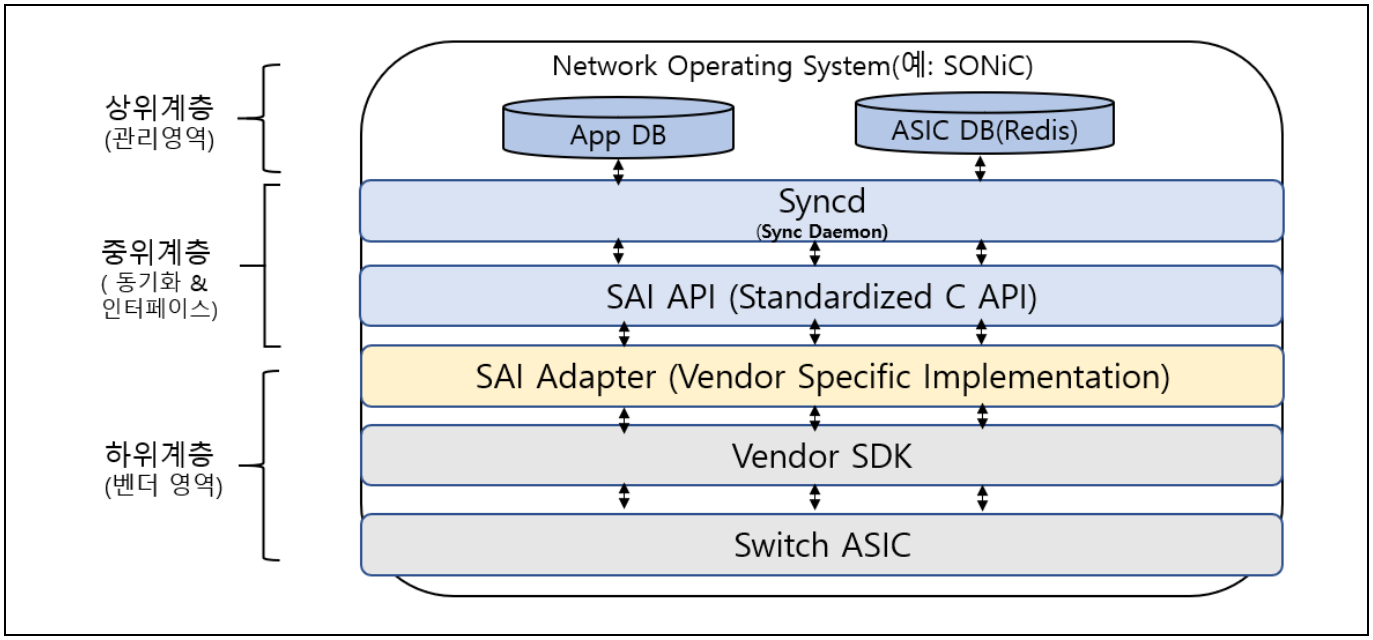
나. SAI(Switch Abstraction Interface)의 특징

구분	특징	설명
소프트웨어 관점 (NOS / Control Plane)	- **하드웨어 추상화**	- 스위치 칩셋의 복잡하고 벤더별로 상이한 내부 구현 세부 사항을 감추고, 일관된 API를 상위 네트워크 OS에 제공
	- 표준화된 API	- C 언어 기반의 함수 포인터 형태로 정의, L2/L3 스위칭, ACL, QoS 등 네트워킹 기능을 통일된 방식으로 설정
	- 상태 동기화 지원	- Syncd와 같은 제어 데몬을 통해 NOS가 설정한 의도된 상태(Desired State)와 실제 하드웨어 상태를 일치시킬 수 있는 구조를 제공
하드웨어 관점 (ASIC / Vendor)	- **벤더 독립성** 확보	- 네트워크 OS는 특정 하드웨어 제조사(칩셋)에 묶이지 않고, SAI를 구현한 모든 칩셋에서 동작가능. 이를 통해 벤더 록인(Vendor Lock-in)을 방지
	- 매핑 계층 제공	- 칩셋 제조사가 SAI 표준 함수를 자사의 Vendor SDK 명령어와 1:1로 변환(매핑)하는 어댑터(Adapter)를 제공
기타	- **Disaggregation** 가능	- 소프트웨어와 하드웨어의 분리(탈동조화)가 가능 - 사용자가 원하는 NOS와 하드웨어를 독립적으로 선택하고 조합하여 사용

- SAI는 클라우드 서비스 제공업체(CSP)와 대규모 데이터센터에서 네트워크 유연성과 효율성을 극대화하는 데 중요한 기술로 평가

II. SAI(Switch Abstraction Interface)의 구조와 기술요소

가. SAI(Switch Abstraction Interface)의 구조



- 실제 시스템 내부에서 데이터가 어떻게 흐르고 어떤 컴포넌트들이 상호작용하는지 상세하게 보여주는 구조

나. SAI(Switch Abstraction Interface)의 기술요소

구분	핵심 기술	설명
인터페이스 정의 (Standard Definition)	- **SAI API** (Headers)	- C언어로 정의된 표준 함수들의 집합 - 스위칭, 라우팅, QoS 등의 기능을 수행하기 위한 함수 프로토타입이 선언
	- Object Model	- 스위치의 논리적 자원(Port, VLAN, Virtual Router 등)을 객체(Object) ID와 속성(Attribute)의 쌍으로 정의하여 관리하는 모델
런타임 및 제어 (Control Plane)	- **ASIC DB** (Redis)	- 네트워크 OS(예: SONiC)의 어플리케이션들이 하드웨어에 내리고 싶은 설정 상태를 저장하는 인메모리 데이터베이스 (Key-Value Store)
	- **Syncd (**Sync Daemon)	- [핵심 컴포넌트] ASIC DB의 변경 사항을 감지하여, 이를 실제 SAI API 호출로 변환하고 하드웨어와 소프트웨어 간의 상태를 동기화하는 데몬 프로세스
	- SAI RPC	- 원격에서 SAI 객체를 제어하거나 테스트하기 위해 사용되는 원격 프로시저 호출 인터페이스 - 주로 PTF(테스트 프레임워크) 연동 시 사용
벤더 구현 (Vendor Implementation)	- **SAI Adapter** (Library)	- libsai.so와 같은 라이브러리 형태로 제공, 표준 SAI API 호출을 받아 특정 벤더의 SDK 명령어로 변환(Mapping)해주는 소프트웨어 모듈
	- Vendor **SDK**	- 칩셋 제조사(Broadcom, Nvidia, Intel 등)가 제공하는 고유의 하드웨어 제어 드라이버로, 실제 ASIC칩의 레지스터 조작
	- NPU / **ASIC**	- 실제 패킷 처리를 담당하는 네트워크 프로세서 유닛 (Network Processing Unit) 또는 주문형 반도체

- SAI는 설정입력, 동기화, API호출, 변화 및 실행의 순서로 작동하며, 이런 구조로 인해 상위계층(DB,Syncd)가 바뀌어도 코드를 수정할 필요가 없음

III. SAI(Switch Abstraction Interface)의 표준기술의 시사점

가. 기술적 관점의 시사점

구분	시사점	설명
기술 및 개발 관점	- **개발 단순화 및 가속화**	- 네트워크 OS 개발자는 다양한 하드웨어에 맞춘 복잡한 드라이버 코드를 작성할 필요 없이, 단일 SAI API에만 집중하여 개발 생산성 향상
	- 소프트웨어 품질 향상	- 공통의 인터페이스를 사용하여, 코드 재사용 가능 - 표준화된 테스트(PTF 등) 적용이 용이, 소프트웨어의 신뢰성과 품질이 향상
	- 신기술 도입 용이성	- 칩셋이 새로운 기능을 지원해도 SAI 인터페이스를 통해 상위 OS에 투명하게 전달, 새로운 하드웨어 기능을 빠르게 활용

기술 혁신 관점	- API 경제 원칙의 네트워킹 적용	- 표준화된 API를 통해 칩셋 기능에 쉽게 접근, 제어할 수 있어, 네트워크 기능개발 진입장벽이 낮아지고 소프트웨어 혁신 속도가 빨라짐
	- **지능형 네트워크** 관리 기반 마련	- 하드웨어 제어가 추상화되어, AI/ML 기반의 자동화된 네트워크 관리(Automation) 시스템 구축이 용이, 네트워크의 지능화(Intent-Based Networking)가 가속화

- 하드웨어 추상화를 완성하여 상위 네트워크 소프트웨어(NOS)의 개발 단순성과 혁신 속도를 극대화하며 지능형 네트워크 구현 기반을 마련

나. 관리적 관점의 시사점

구분	시사점	설명
비즈니스 및 시장 관점	- **벤더 록인(Lock-in) 방지**	- 특정 하드웨어 제조사에 종속되지 않고, 여러 벤더의 스위치를 자유롭게 선택,교체할 수 있어 구매 협상력이 강화
	- 경쟁 활성화 및 **비용 절감**	- 다양한 하드웨어/소프트웨어 공급자가 경쟁하여 제품 가격 하락하 및 고객은 비용 효율적인 솔루션을 구축이 가능
	- **개방형 생태계** 확장	- OCP(Open Compute Project) 기반의 개방형 네트워킹(Open Networking) 시장 성장을 촉진 - 중소기업 및 스타트업의 진입 장벽을 낮아짐
운영 및 관리 관점	- 기술 선택의 자유 극대화	- 사용자는 특정 벤더에 종속되지 않고, 최적의 가격 대비 성능을 제공하는 칩셋과 가장 기능이 풍부한 NOS를 독립적으로 조합하여 선택 가능
	- 장애 대응 및 관리 용이	- 표준화된 API로 문제 해결 프로세스가 통일 - 스위치 칩셋이 교체되어도 상위 관리 도구를 그대로 사용할 수 있어 관리 부담이 감소
	- **확장성 및 유연성** 향상	- 네트워크 요구사항 변화에 맞춰 하드웨어와 소프트웨어를 독립적으로 업그레이드할 수 있는 유연한 확장성을 확보

- 소프트웨어와 하드웨어의 분리(Disaggregation)를 가속하여 벤더 록인을 방지하고 최종 사용자의 TCO(총 소유 비용) 절감 및 선택의 자유를 극대화

IV. SAI(Switch Abstraction Interface)의 활용분야

활용분야	활용 목적	세부활용 및 효과
개방형 NOS (SONiC, FBOSS 등)	- 네트워크 OS가 특정 스위치 ASIC 벤더에 종속되지 않도록 추상화 계층 제공	- SONiC이 Broadcom, Intel, Marvell 등 다양한 ASIC을 단일 API(SAI)로 제어 - 벤더 종속성 제거 → 장비 교체 쉬움 - 대규모 데이터센터의 네트워크 유연성 확보
화이트박스 스위치	- 동일한 하드웨어 위에 다양한 NOS(Network OS) 탑재 가능하게 하는 표준 인터페이스 제공	- ODM(Delta, Edgecore 등) 스위치 + SAI 기반 NOS 조합 가능 - CAPEX 절감, 공급망 다양성 확보 - 트래픽 증가 대응을 위한 확장성 확보
대규모 클라우드/ 데이터센터 네트워킹	- 대규모 스케일 아웃 구조에서 표준화된 스위치 제어 인터페이스 제공 → 운영 자동화·최적화	- Microsoft Azure, Meta 등 Hyperscaler 가 SONiC/SAI 기반 네트워크 구축 - 장비 단종 리스크 감소 - 네트워크 자동화/버그 수정 속도 향상
SDN 및 네트워크 자동화	- 중앙 집중식 제어 및 네트워크 프로그래밍	- 표준 프로그래밍 인터페이스 - SDN 컨트롤러나 자동화 스크립트가 스위치의 포워딩 테이블, ACL, QoS 등의 기능을 표준화된 API 를 통해 직접적이고 일관되게 프로그래밍하도록 지원

- SAI는 클라우드 센터, NOS, SDN 등에 활용되어 벤더 종속성 제거, 유연성 확보, 운영 자동화의 효과 기대

"끝"

제 39 회 ITPE
실전 명품 모의고사 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2025년 12월 21일
집 필 강정배 PE, 전일 PE, 이상헌 PE, 소민호 PE, 현수 PE, 박서현 PE, 배미경 PE
출 판 **ITPE(Information Technology Professional Engineer)**
주 소 ITPE 대치점 서울시 강남구 선릉로 86길 17 선릉엠티빌딩 7층
ITPE 선릉점 서울시 강남구 선릉로 86길 15 3층 IT교육센터 아이티피이
ITPE 강남점 서울시 강남구 테헤란로 52길 21 파라다이스벤처타워 3층 303호
ITPE 영등포점 서울시 영등포구 당산동2가 하나비즈타워 7층 ITPE
ITPE 을지로점 서울시 중구 삼일대로 363, 2615호(장교동 장교빌딩)
ITPE 강북점 서울 종로구 수표로 96, 7층 (관수동,국일관드림팰리스)
연락처 070-4077-1267 / itpe@itpe.co.kr