

5G 엣지 환경에서의 보안 위협

2021.11.17

한국전자통신연구원(ETRI) 정보보호연구본부

김 영 수

(blitzkrieg@etri.re.kr)

Contents

- 5G 통합 서비스
- 5G 네트워크 환경 변화
- 5G MEC
 - Edge 개념
 - Edge 차원의 보안 위협
 - 사업자별 Edge 뷰포인트

5G 융합 서비스 - 5G 포럼

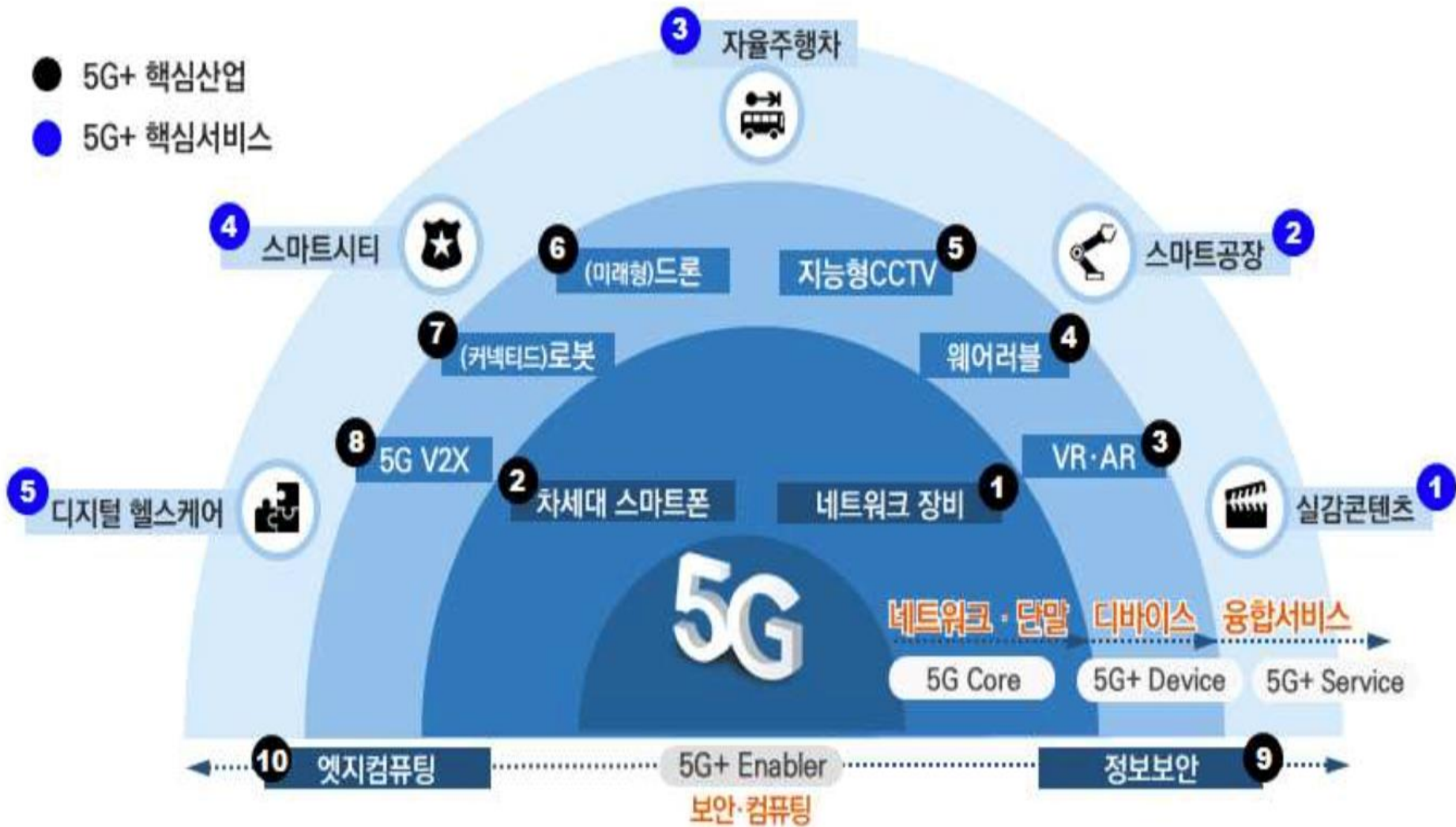
기계학습 기반 빅데이터 분석을 통한
사용자 컨텍스트 및 상황인지 AI 비서 서비스



5 Mega Trends of Mobile Service

- Data Traffic 양의 폭발적 증가
- Device 수의 폭발적 증가
- Cloud Computing 의존성 증가
- Big Data 기반 지식 서비스 증가
- Mobile 기반 융합미디어 서비스 확산

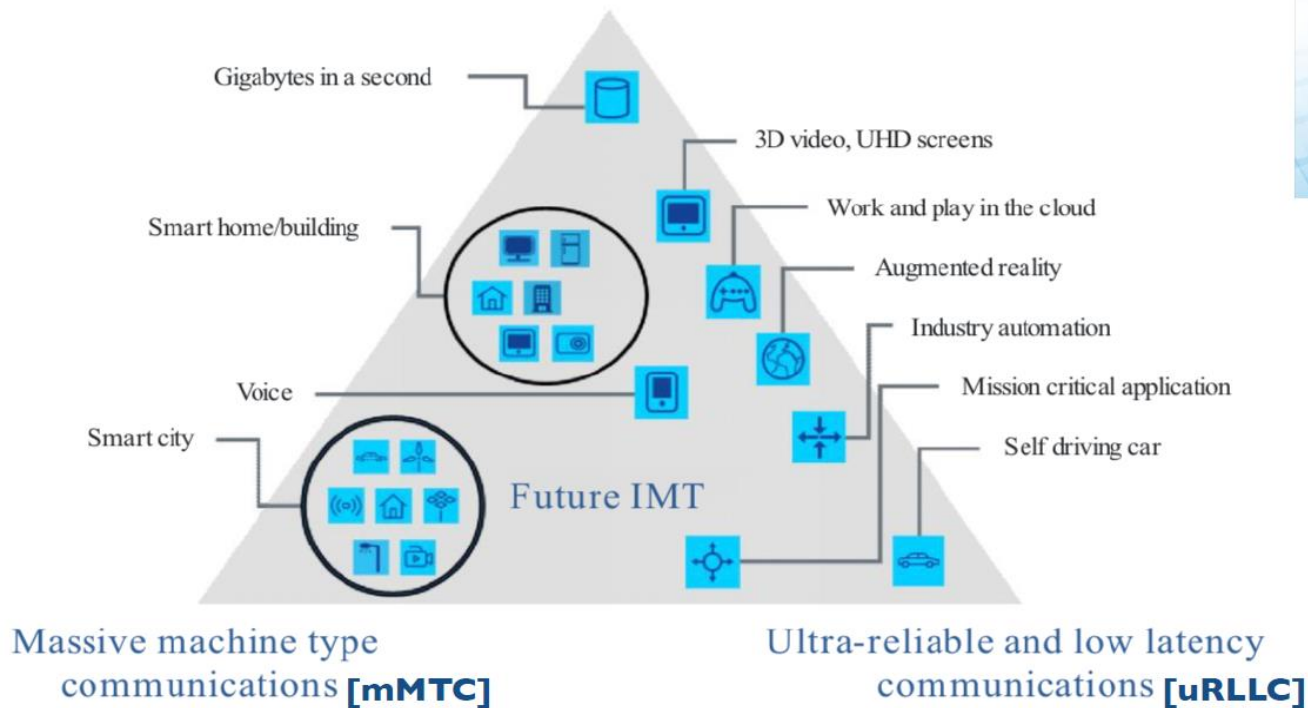
5G 융합 서비스 - 5G+ 전략



5G 융합 서비스 - IMT2020 사용 시나리오 (ITU-R)

Human-centric use cases for access to multi-media content, service and data for improved performance and an increasingly seamless user experience

Enhanced mobile broadband [eMBB]



Recommendation ITU-R
M.2083-0 (09/2015)

- * eMBB: 초고속
- * mMTC: 초연결
- * uRLLC: 초저지연

Typically transmitting a relatively low volume of non-delay-sensitive data

Stringent requirements for capabilities such as throughput, latency and availability

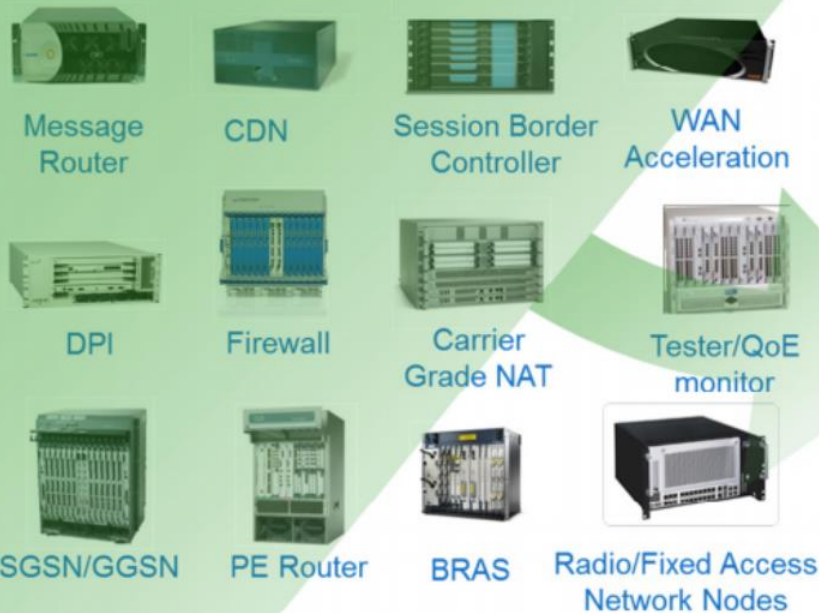
5G 네트워크 환경 변화

- 접속 환경 다변화
 - Massive/Heterogeneous Devices
 - Multiple Access Technologies
- 네트워크 소프트웨어화
 - NFV(Network Functions Virtualization)
 - SDN(Software-Defined Networking)
 - Network Slicing
- 분산 네트워크 구조화
 - MEC(Multi-access Edge Computing)
 - SBA(Service-Based Architecture)

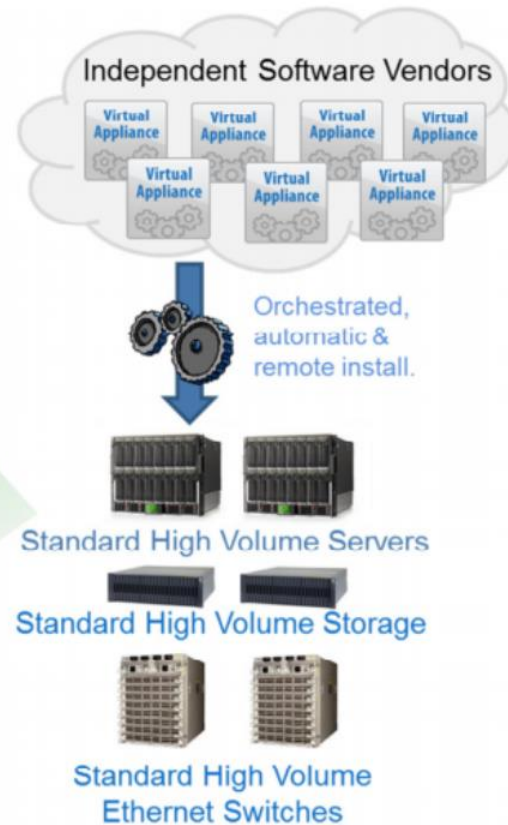
5G 네트워크 환경 변화 - NFV

Implementing network functions in software (programs)
running on top of industry-standard hardware (instead of dedicated hardware)

Classical Network Appliance Approach



- Fragmented non-commodity hardware.
- Physical install per appliance per site.
- Hardware development large barrier to entry for new vendors, constraining innovation & competition.

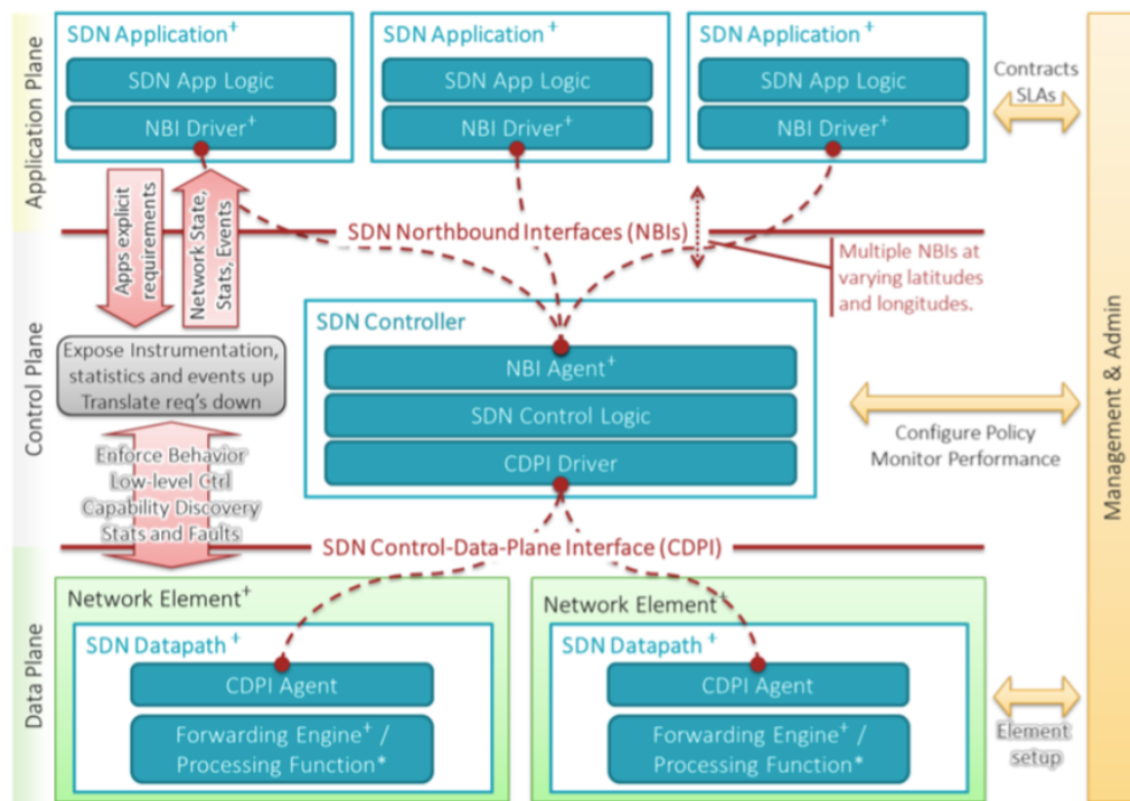


Network Functions Virtualisation Approach

- ☆ Decoupling SW from HW
- ☆ Flexible NF deployment
- ☆ Dynamic Operation
- ☆ Avoid vendor lock-in

5G 네트워크 환경 변화 - SDN

An approach to designing, building, and managing networks that separates the network's control or SDN network policy and forwarding planes thus enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services



- ☆ *Applications can be network aware*
- ☆ *Logically centralized control plane*
- ☆ *Decoupled control plane from the data plane*

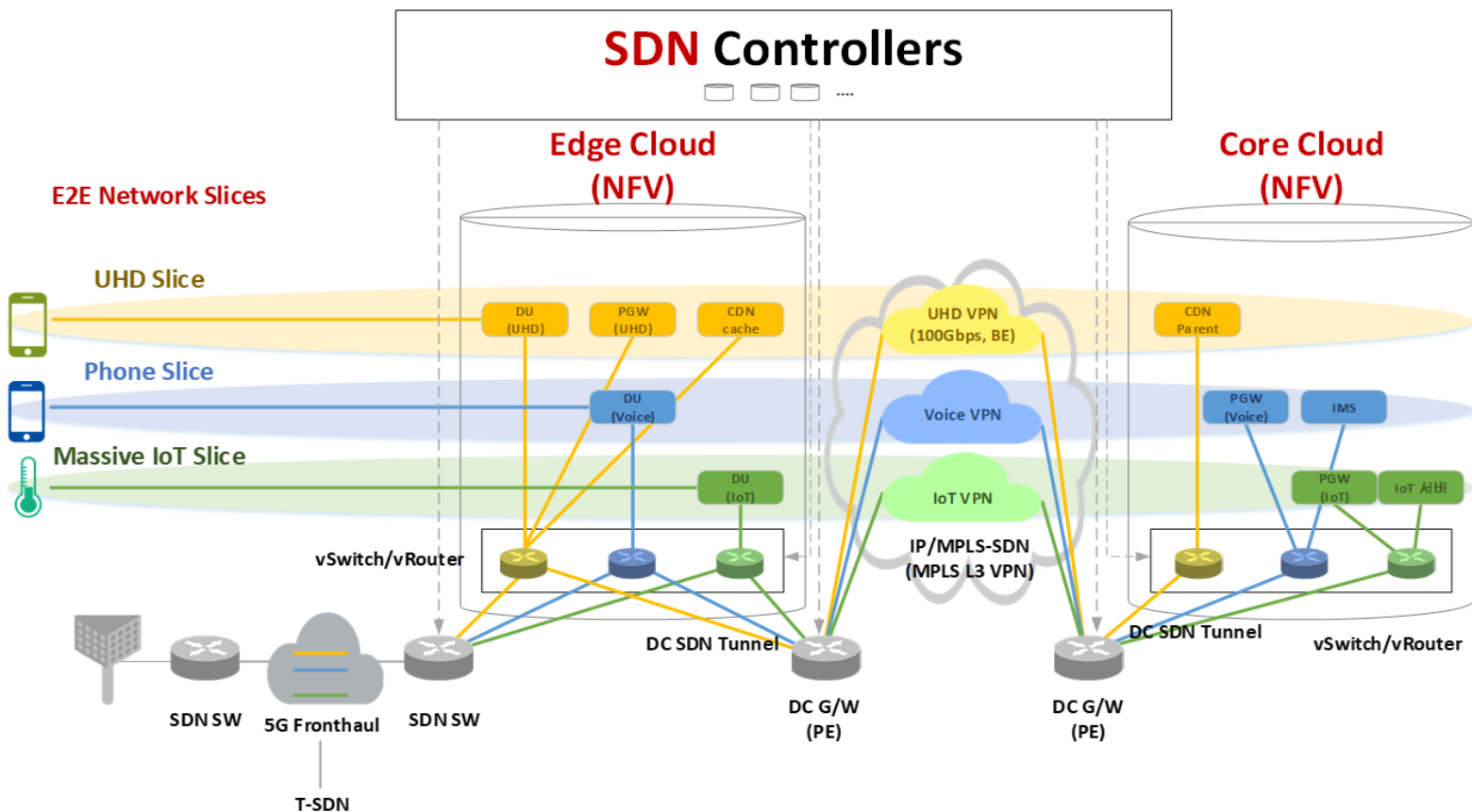
- 개방형 API(오픈플로우)를 통해 네트워크의 트래픽 전달 동작을 SW 기반 컨트롤러에서 제어/관리하는 접근방식
- 트래픽 경로를 지정하는 컨트롤 플레인과 트래픽 전송을 수행하는 데이터 플레인이 분리
- 네트워크의 세부 구성정보에 얽매이지 않고 요구사항에 따라 네트워크를 관리할 수 있음

⁺ indicates one or more instances | * indicates zero or more instances

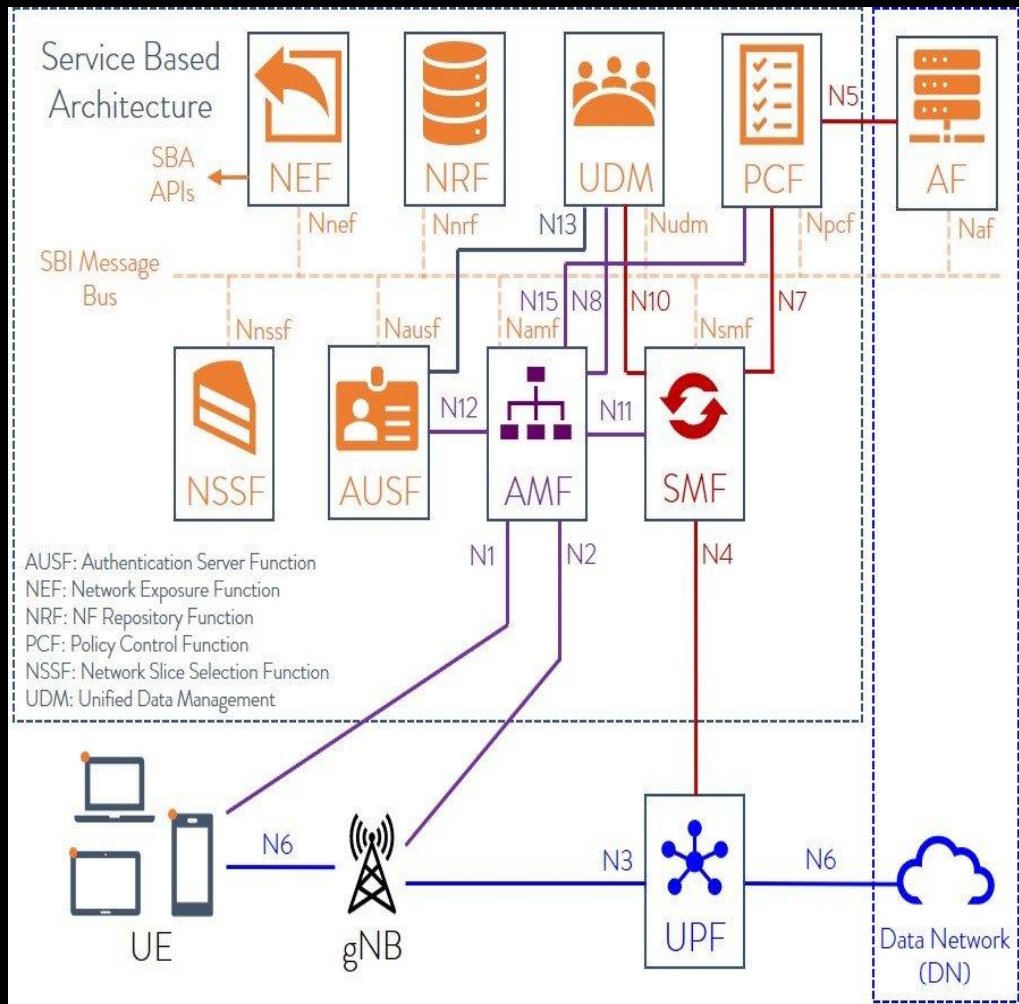
5G 네트워크 환경 변화 – Network Slicing

Network Slicing: NFV와 SDN 기술을 적용하여 서비스 별 요구 품질을 만족시키는 기술

- 품질 요구사항이 다른 서비스들을 단일망에서 융통성 있게 수용
- 서비스 별로 대역폭 할당, 경유 네트워크 기능을 할당할 수 있음



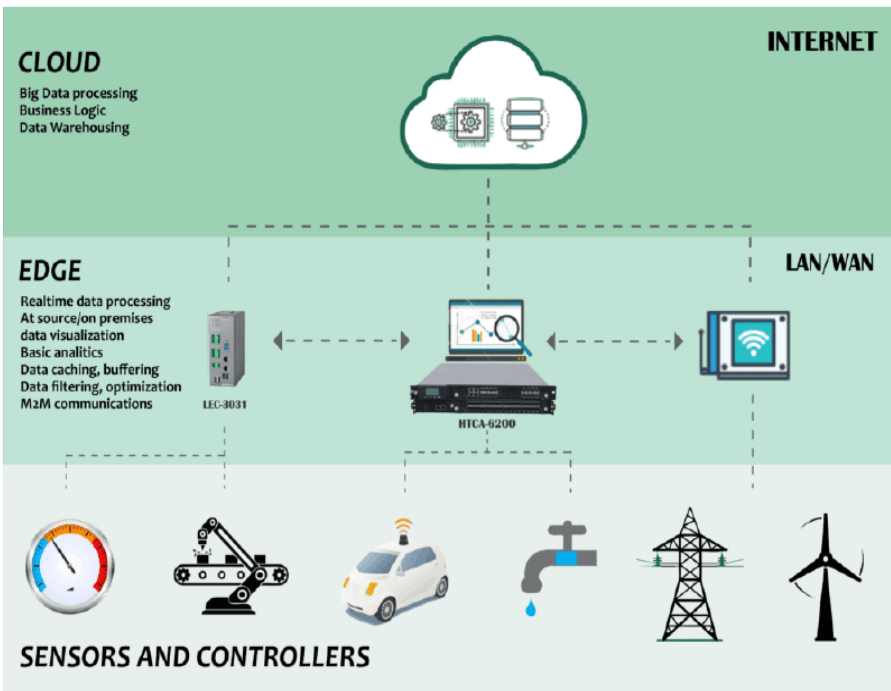
5G 네트워크 환경 변화 - SBA



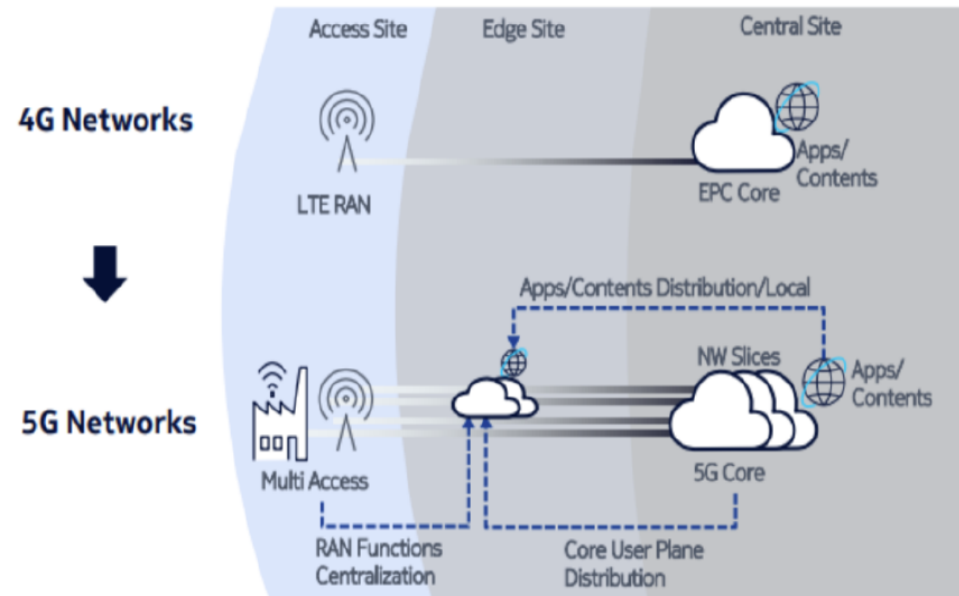
- Flexibility and scalability
- Modulization
 - 5G CN(Core Network) functions → Each NF(Network Function)s
- Define Interaction between each NFs
- Provider-Consumer Relationship
- Easy to add, alter or reuse NFs
- Service Chaining Scenarios
 - Linking related NFs Set
- Only available on NFs of CP(Control Plane)
 - not UP(User Plane)

5G 네트워크 환경 변화 - MEC

A network architecture that enables the placement of computational and storage resources within the RAN to improve network efficiency and the delivery of content to end users



- ☆ Low latency
- ☆ Reduction of backhaul and core network traffic
- ☆ In-network data processing

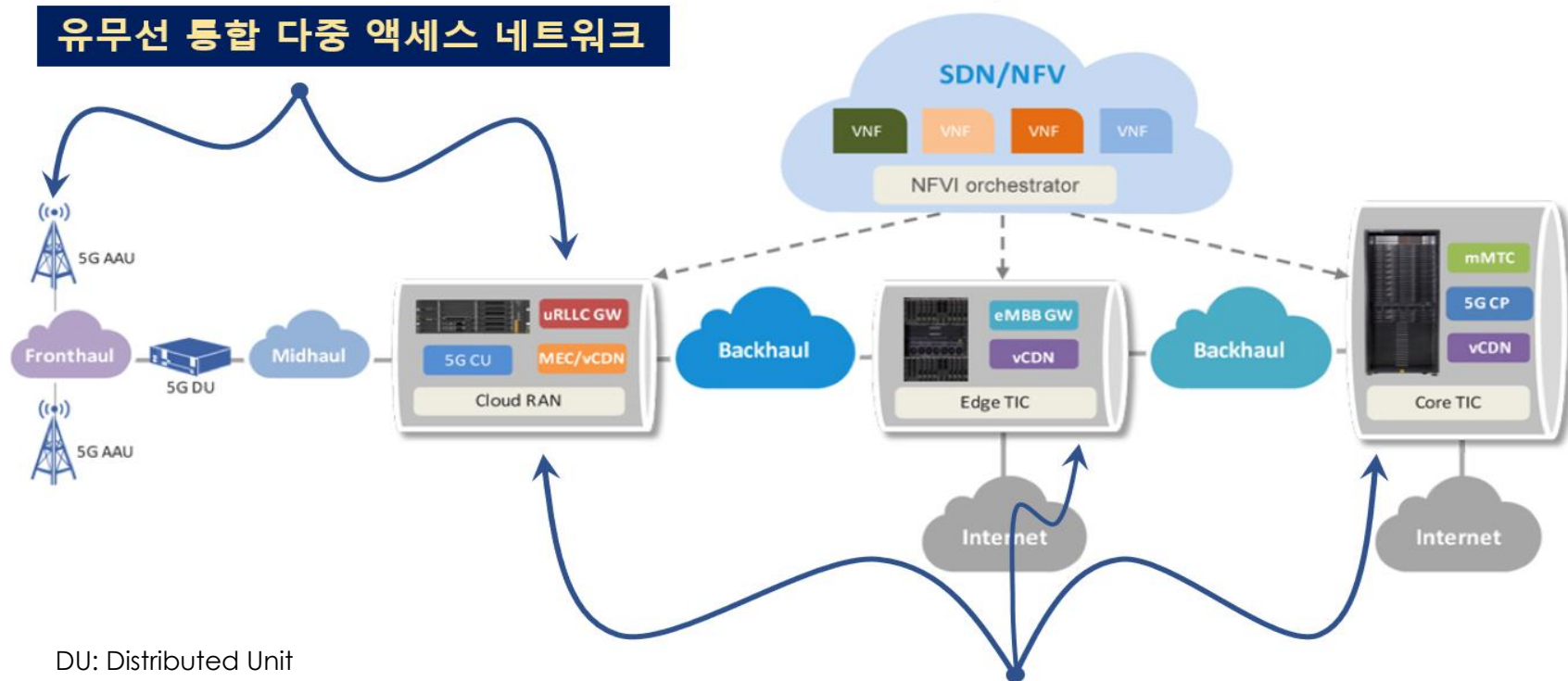


5G 네트워크 환경 변화

수많은 다양한 종류의 센서 · 기기 연결

유무선 통합 다중 액세스 네트워크

본격적인 네트워크 인프라 가상화

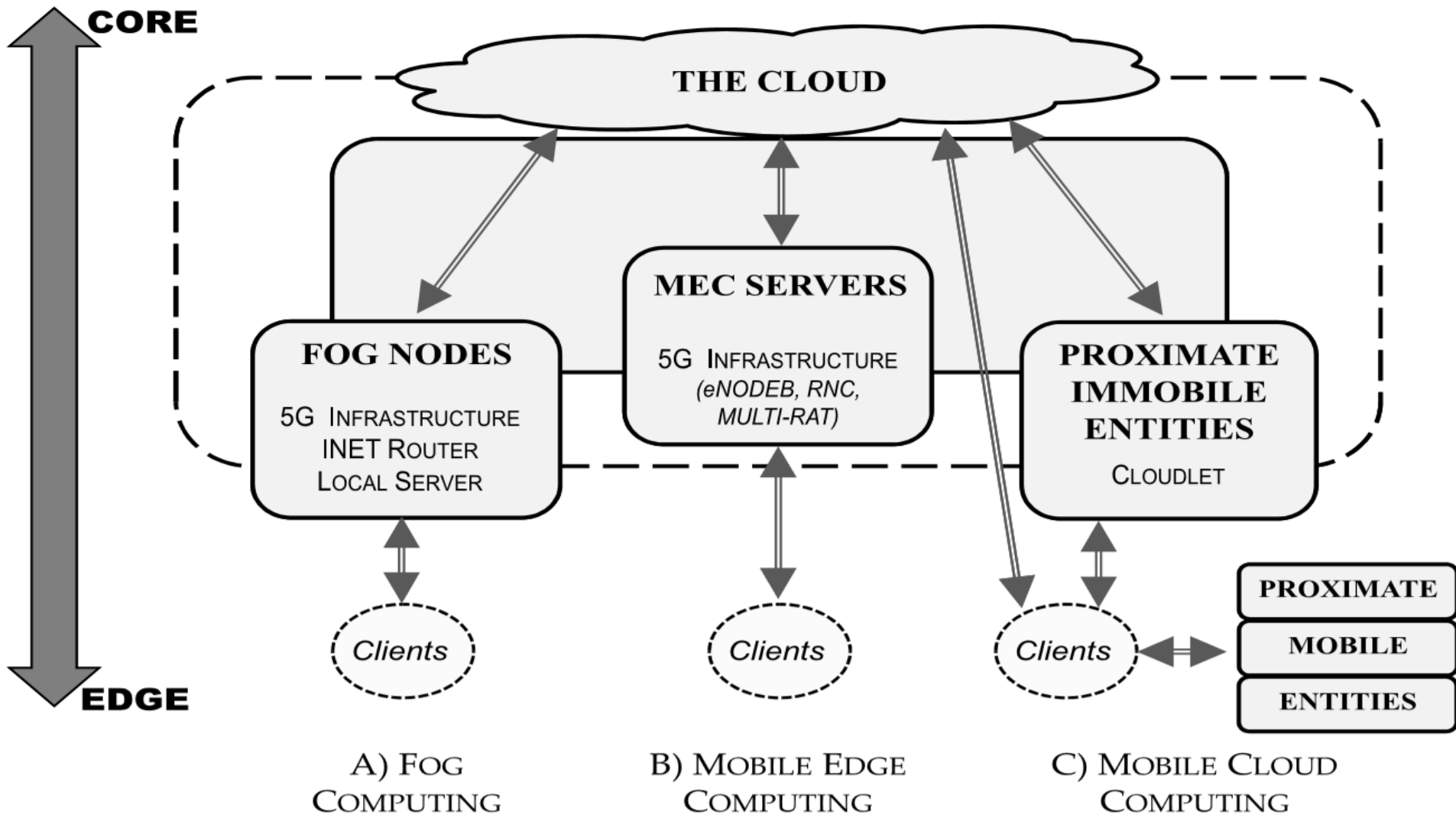


DU: Distributed Unit
CU: Centralized Unit
AAU: Active Antenna Unit
vCDN: virtual Content Delivery Network
TIC: Trusted Internet Connection

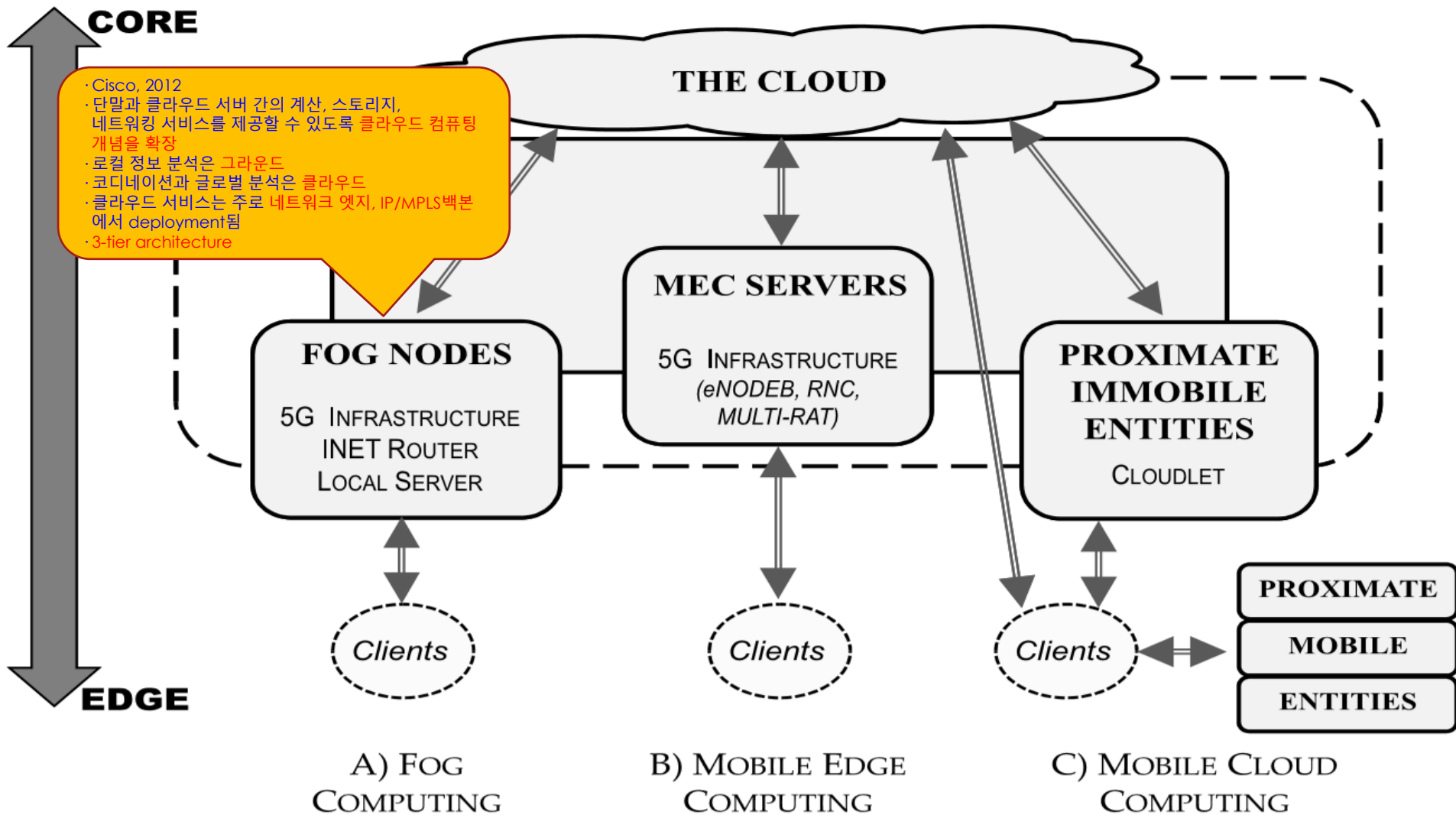
서로 다른 품질 특성을 갖는 다양한 서비스 융합

네트워크 코어 기능의 분산 배치

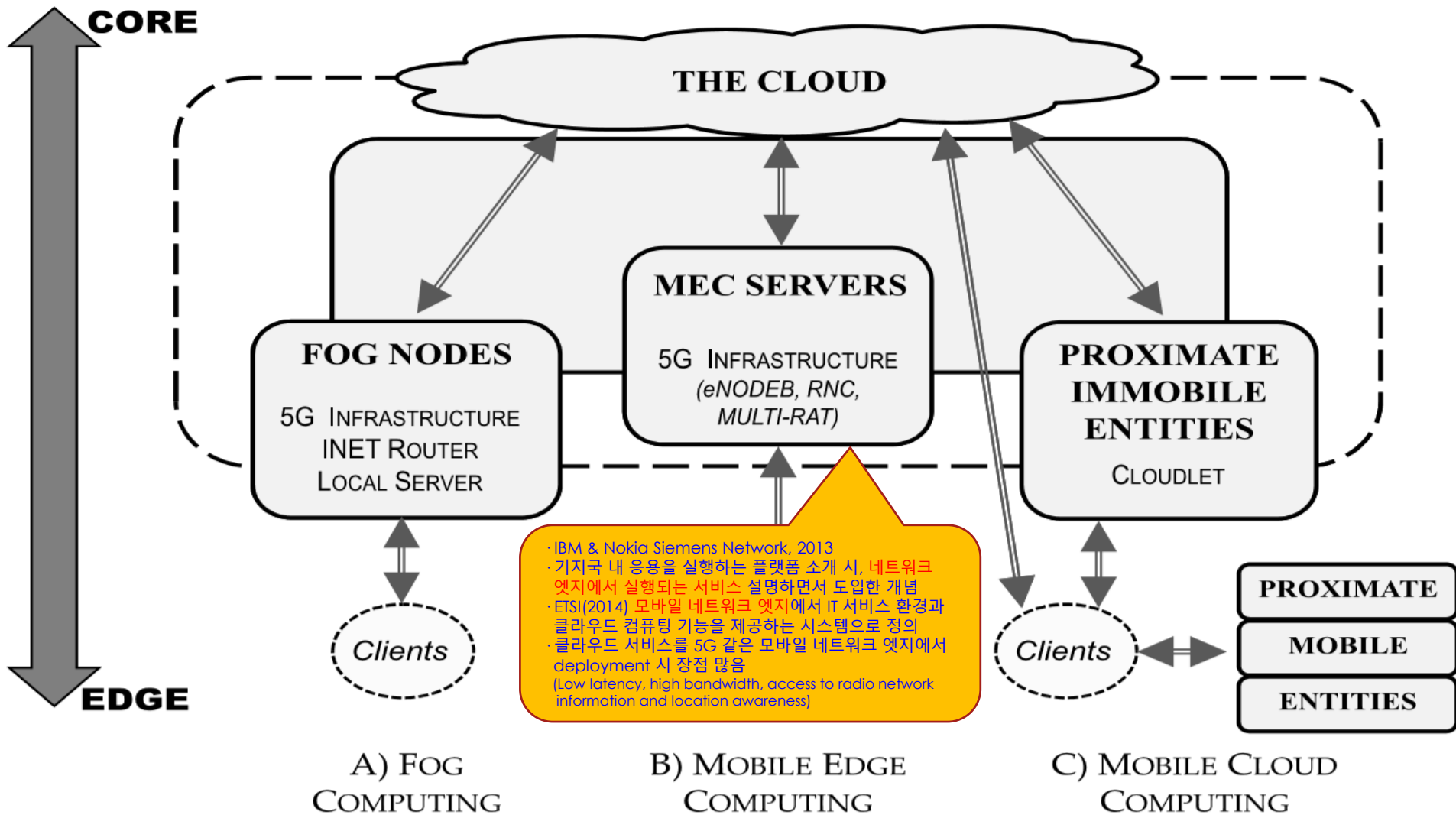
5G MEC - Edge 개념



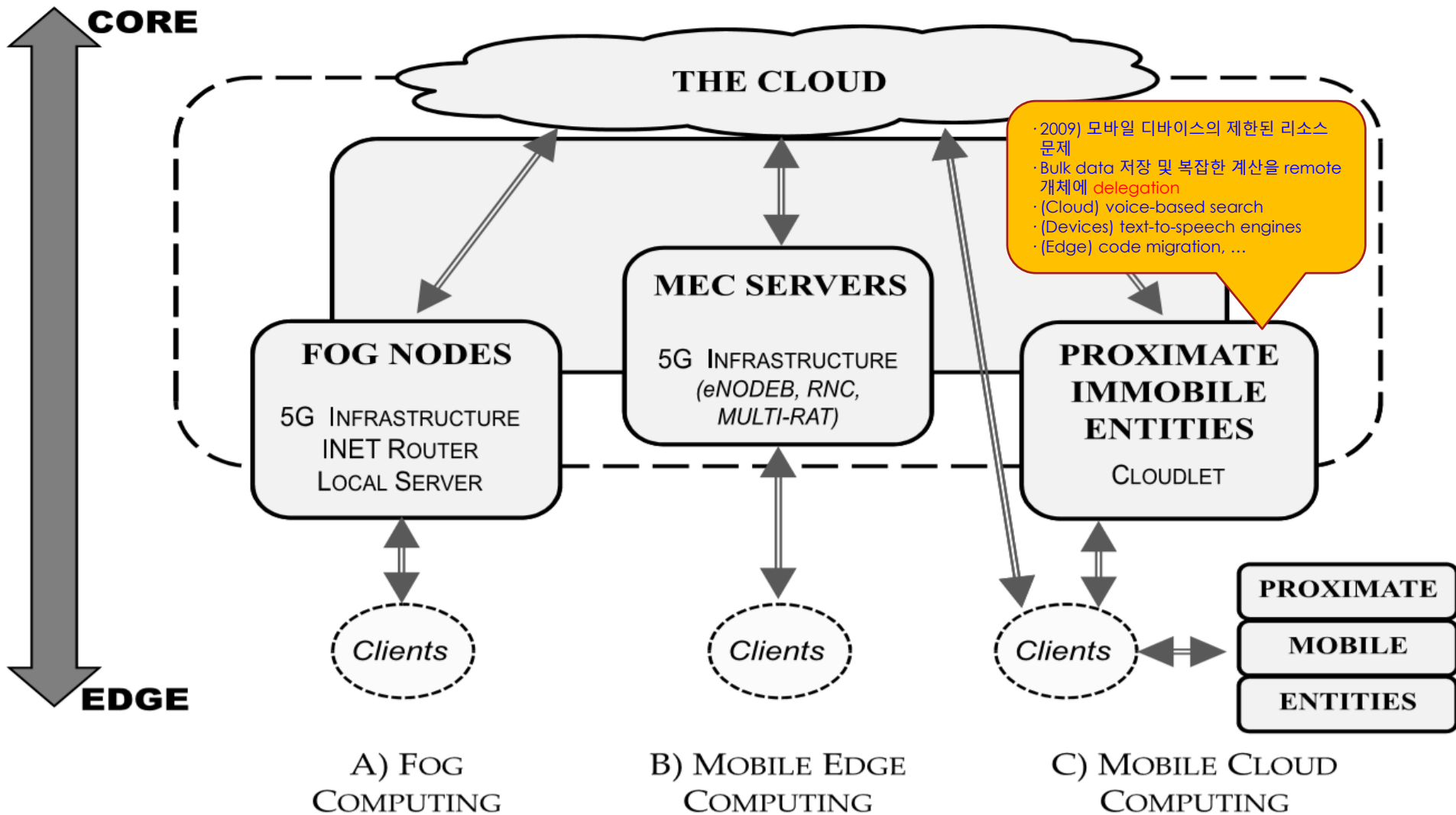
5G MEC – Edge 개념



5G MEC – Edge 개념



5G MEC – Edge 개념



5G MEC – Edge 개념

	MEC	Fog Computing	MCC	Cloud
Ownership	Telco companies	Private entities, individuals		Private Entities
Deployment	Network Edge	Near-edge, edge	Network edge, devices	Network Core
HW	Heterogeneous servers		Servers, user devices	Servers
NW Architecture	N-tier, decentralized, distributed			Centralized
Mobility	Yes			N/A
Latency	Low			Average
Local Awareness	Yes			N/A
Scalability	High			Average

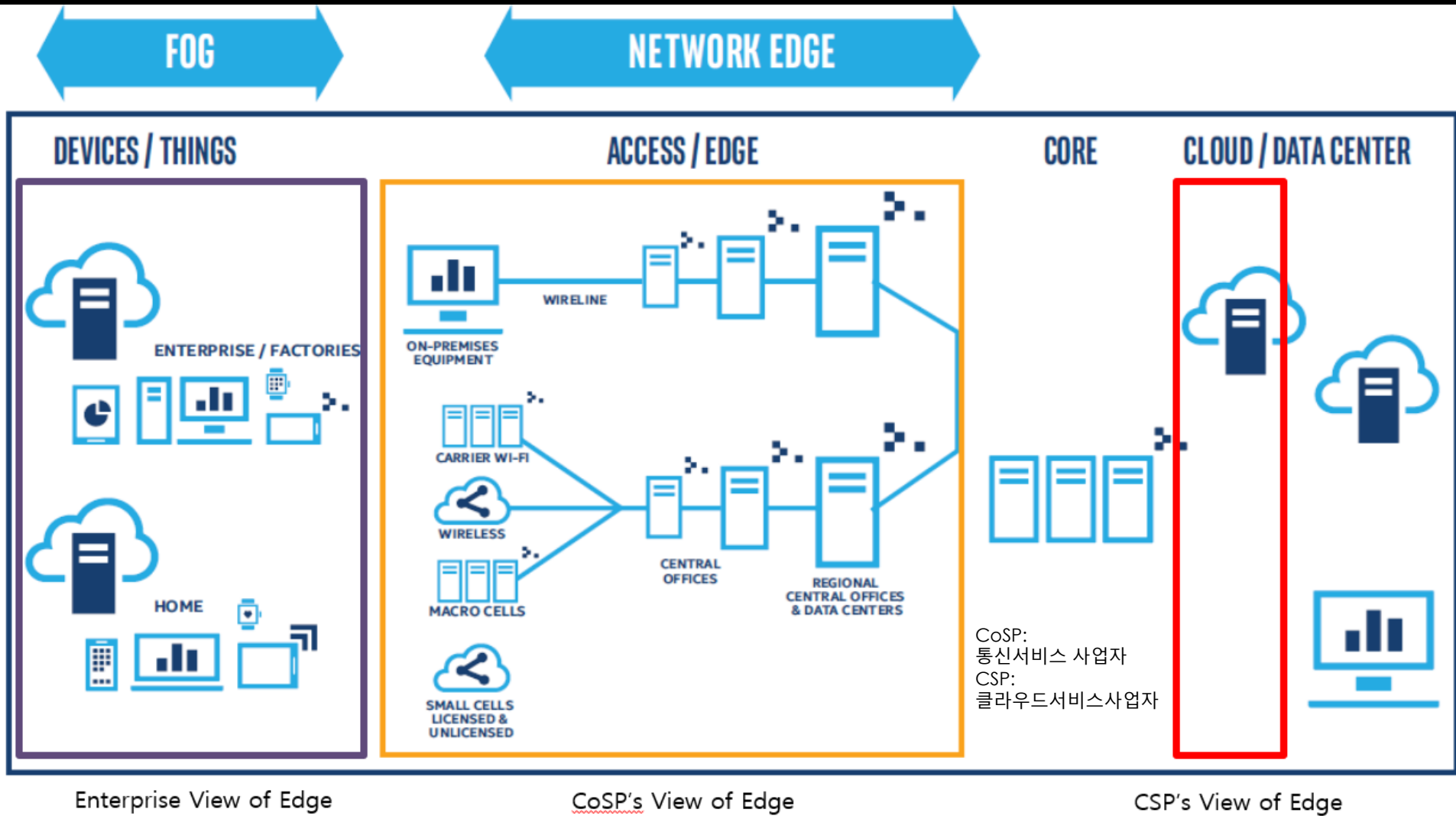
5G MEC – Edge 관점에서의 보안 위협

- Identity & Authentication
 - 다양한 **신뢰 도메인**이 **혼재** (사용자/서비스제공자, VM/컨테이너 서비스, UE/코어 인프라)
 - 중앙서버 없이 사용자에게 의해 관리되는 P2P 형태의 **distributed authentication 메커니즘** 필요
- Access Control
 - 작업 요청 승인 (VM 구동 서비스제공자, edge data center API에 접근하는 VM 등)
 - 각 도메인 대상 **보안정책 배포/저장/효력발생 승인 인프라** 구축 및 도메인별로 특화된 **인증정책** 관리
- Protocol & Network Security
 - 서로 다른 admin이 관리하는 이 기종 환경 내 컴포넌트 간의 **정확한 configuration** 필요
 - **각기 다른 통신 기술**을 사용하는 개체들 간의 **안전한 커넥션** 구축
- Trust Management
 - 각 개체 간의 **decision-making** 프로세스에서 **평판**이 중요. 평판 정보 저장, 배포, 저지연성 보장 관건

5G MEC – Edge 관점에서의 보안 위협

- Intrusion Detection Systems
 - 로컬 인프라 모니터링 결과를 상호 공유함으로써 서비스 인프라에 대한 전역적 공격에 대한 방어 가능
 - 디펜스 메커니즘) **Autonomous**. Interoperable exchange format. 로컬/글로벌 균형
- Privacy
 - 내부자에 의한 usage profiling, location tracking, 민감 정보 유출 등
 - Anonymity와 responsibility 간의 균형 필요
- Virtualization
 - 공격자에 의해 제어되는 **malicious VM**은 다양한 edge 서비스에 영향을 줄 수 있음
 - **VM isolation** 정책, **Hypervisor** 강화, **VM의 역할 세분화 및 분리**
- Fault Tolerance and Resilience
 - 100% 안전하고 면역력을 지닌 패러다임은 없음 (**설정 오류, 취약성, SW 업데이트 지연 등**)
 - 전략 필요 (Redundant operation, failover capabilities, disaster recovery mechanisms)
- Forensics
 - Edge 패러다임에서의 **증거 관리**는 복잡한 이슈임 (다양한 actors, 인프라, 기술, 시나리오)
 - Cloud forensics, mobile forensics, virtualization forensics, storage forensics 등

5G MEC – 사업자별 Edge 뷰포인트



감사합니다

National AI Research Institute - Making a Better Tomorrow

ETRI

한국 전자통신연구원