KNOM Conference 2016

네트워크 기술 개발 현황 및 향후 방향

Institute for Information & Communication Technology Promotion(IITP)
will lead in realizing national welfare as the world's Best R&D institute
in ICT technologies through promotion of creative economy

유 재 형

미래부 IITP, 네트워크 CP

Contents

1 네트워크 기술의 고도화

02 네트워크 시장현황 및 전망

03 광통신기술

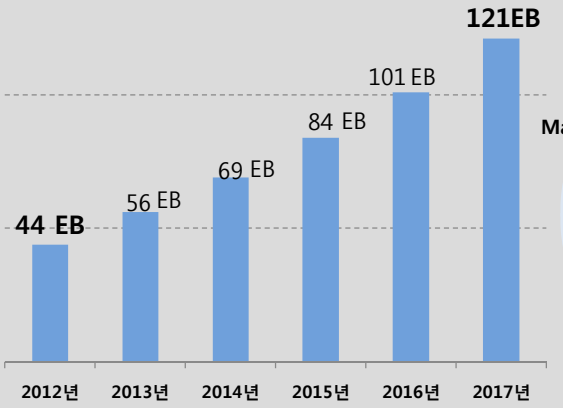
04 양자암호화 통신 기술

05 SDN/NFV 기술

06 결론

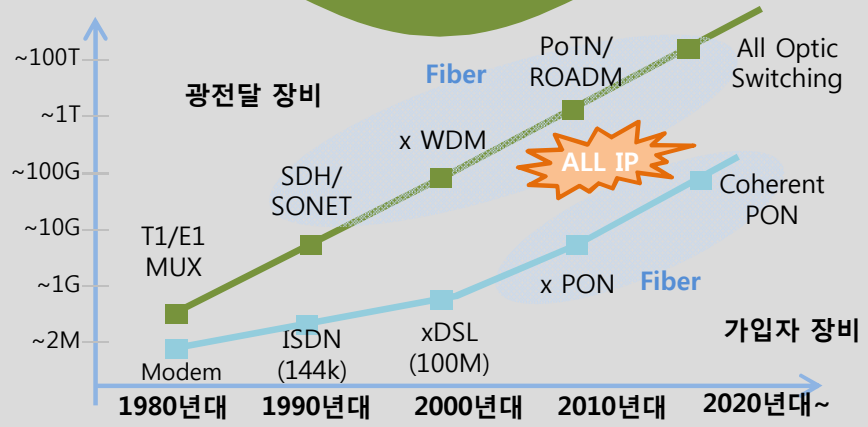
1. 네트워크 기술의 고도화

트래픽의 지속적 증가에 대응



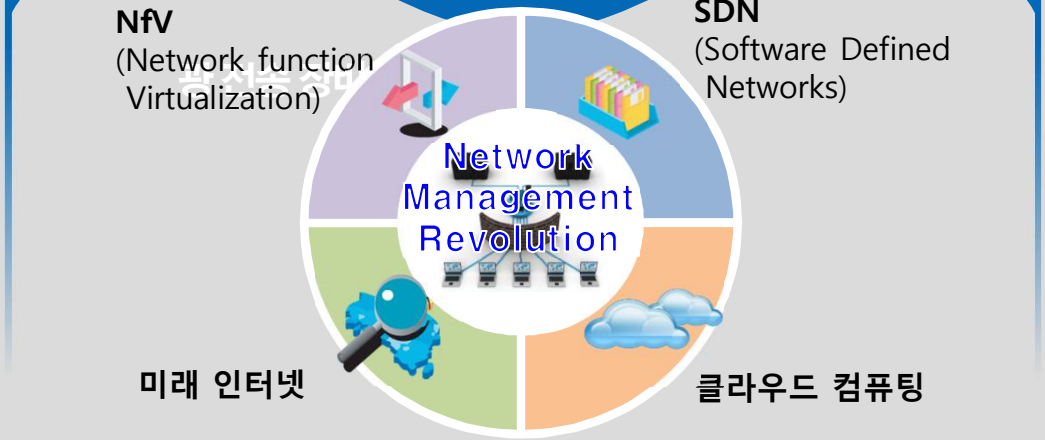
출처 : Cisco VNI (전세계 IP Traffic 전망, Exabytes per Month)

All Optic 기반의 대용량, 저전력, 저가격화

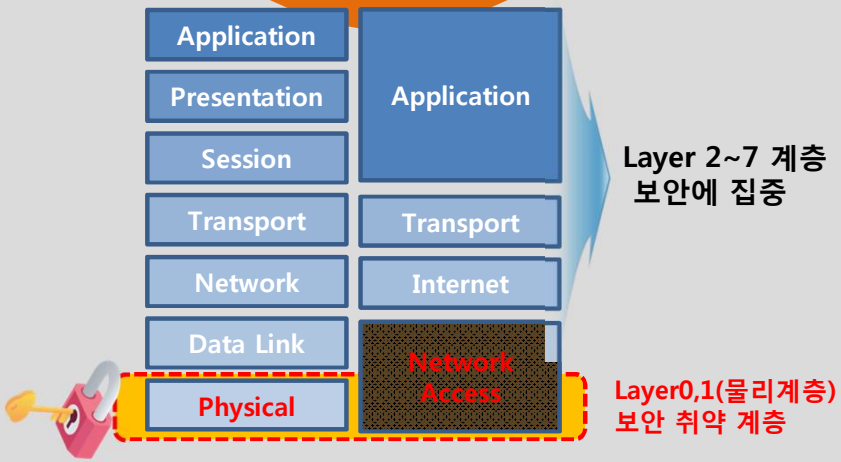


* 대용량(가입자당 1G), 저지연(msec)

네트워크 가상화 및 지능화



네트워크 인프라 보안 강화



2. 네트워크 시장현황 및 전망

전체 네트워크 장비시장

- 전세계 네트워크 장비 시장 성장률 : 3.4%
  1,226억 달러('14년) → 1,447억 달러('19년)

※ 출처 : GARTNER 2015

- 국내 네트워크 장비시장 : 15억 달러('14년) → 21억 달러('19년)
  국내 시장규모는 전세계시장의 1.3% 수준

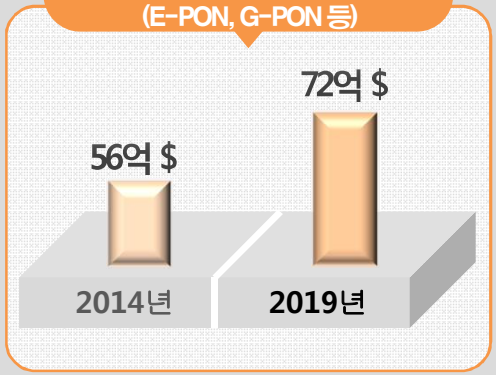
※ 출처 : GARTNER 2015

분야별 시장전망 (세계시장)

광 전송 장비 (WDM 등)

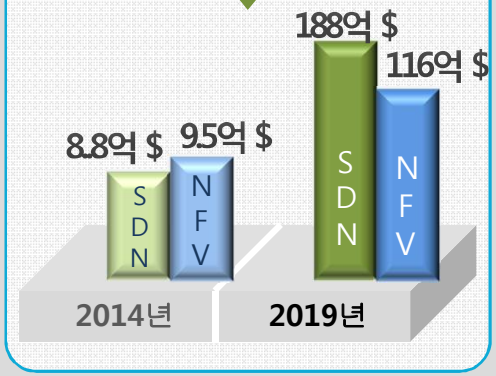
※ 출처 : GARTNER 2015

광가입자 장비 (E-PON, G-PON 등)



※ 출처 : GARTNER 2015

SDN / NFV



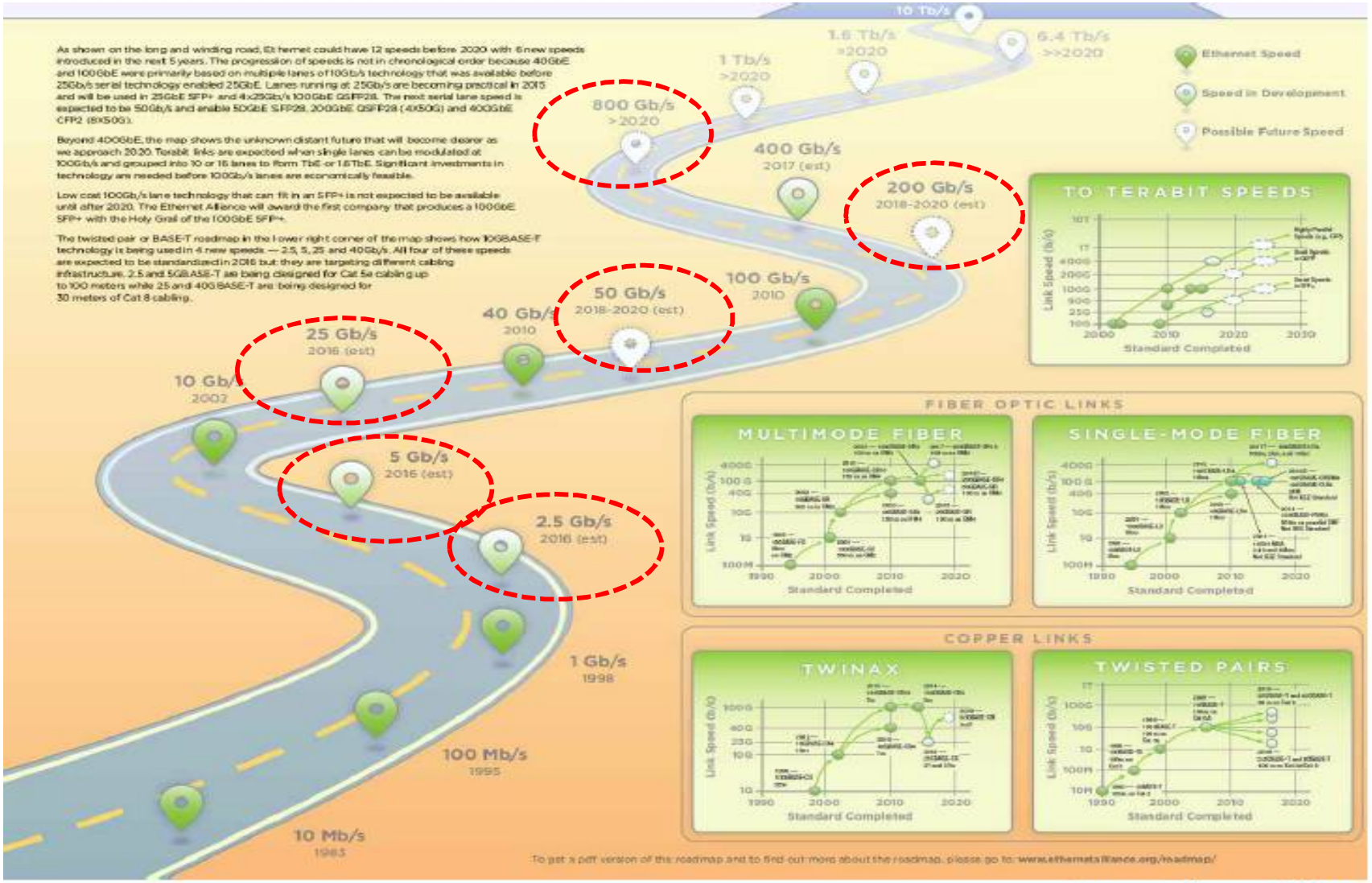
※ 출처 Infonetics 2015

네트워크 보안장비

※ 출처 : GARTNER 2014

3. 광통신 기술

◆Roadmap



Source: Ethernet Alliance

3. 광통신 기술

◆ 전송속도, 전송거리에 따라 적용기술이 다양

❖ 전송 거리 별 기술

- 장거리(100Km~, 400Gbps~): 소량, 광대역 고성능(고비용), DSP 사용
- Metro (10~100Km, 100~400G): 소형화, Pluggable, 가변 변조방식(QPSK ←→ QAM)
- 근거리(~10Km, ~400G): 소형화, PAM-4 등 멀티레벨 변조방식 사용

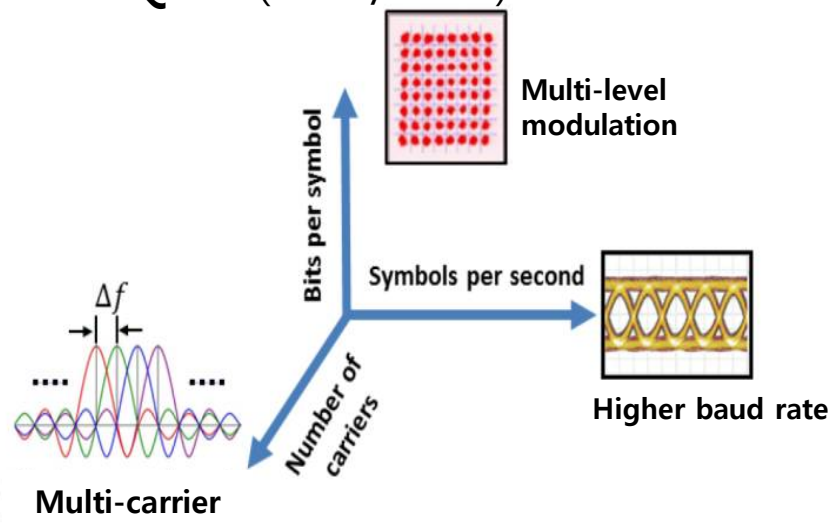
❖ 시스템/부품의 고속화, 스펙트럼 효율화 필요

- 멀티-레벨 변조: PAM-4, DP-QPSK (4bits/baud) , DP-16QAM (8bits/baud) …
- 멀티-캐리어 전송: x2, x4, x8, x10…

❖ 수작업 생산

- 초정밀 광학 기술 → 고도로 숙련된 기술자 필요
- 2주~8주/소자,모듈 → 고가격

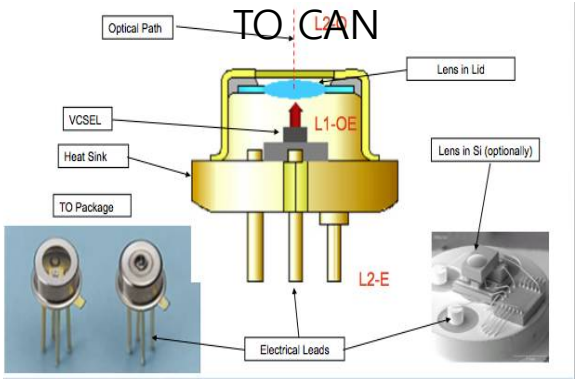
❖ 비용절감(저가격, 저전력, 소형화) 요구



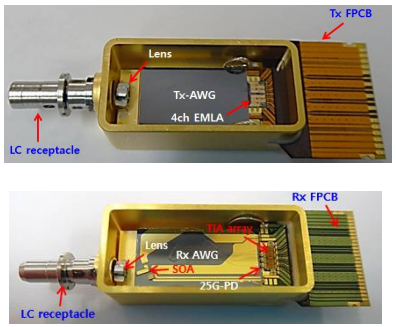
3-1. 광통신 기술—소자, 부품

- **광 기초 부품**
  - 렌즈, 거울, 프리즘 등
  - 화합물 반도체 Fab. 특수공정 필요
  - $0.5~$500
- **광소자/반제품**
  - LD, PD, Chip(ASIC), TOSA/ROSA 등
  - 패키징 기술 필요
  - $1~$3,000
- **광 모듈**
  - Transmitter, Receiver
  - Transceiver
  - 다양한 제품 라인 및 대량생산 기술 필요
  - $8~$20,000

TO CAN



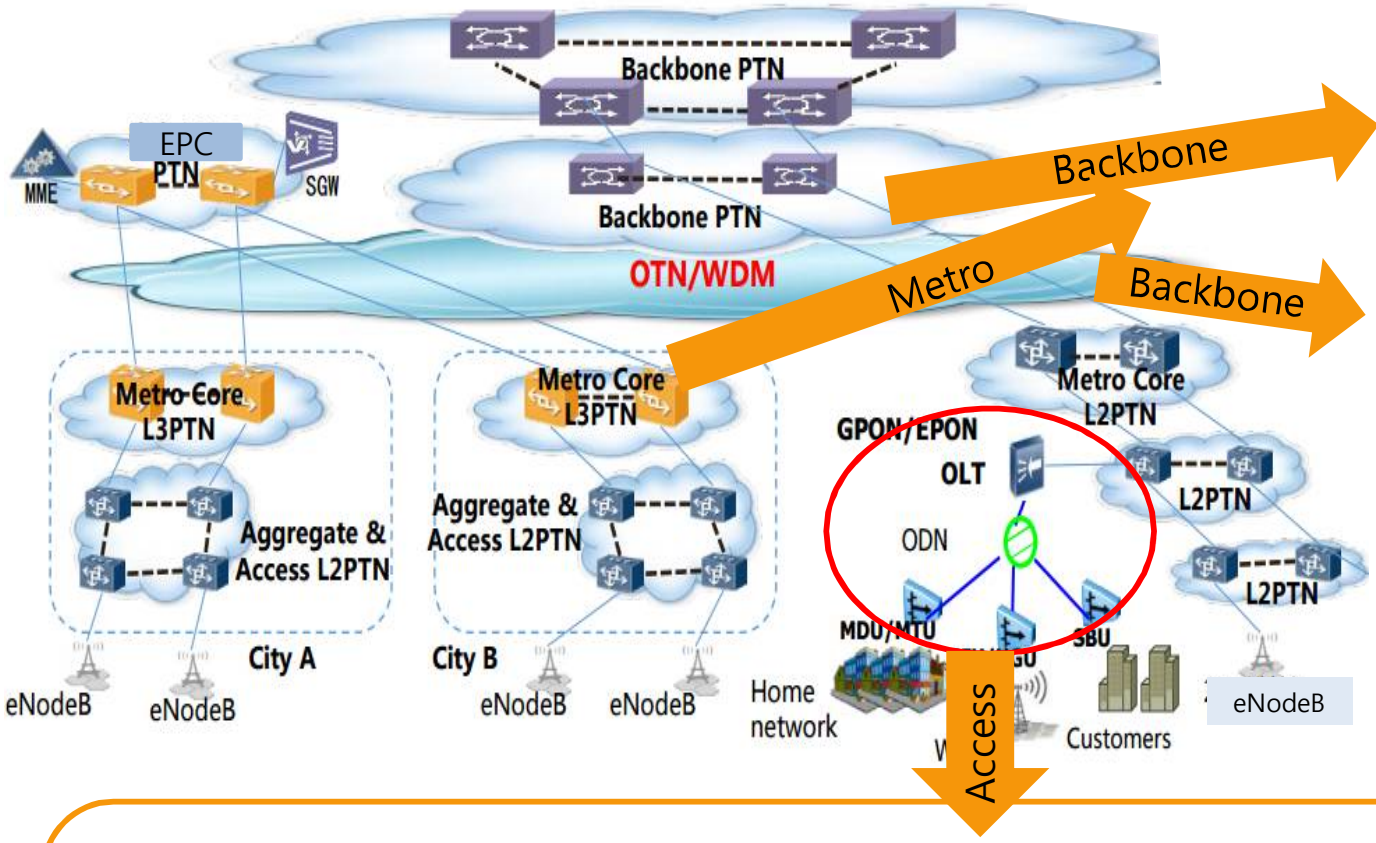
TOSA/ROSA



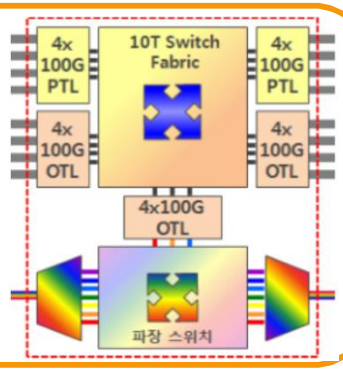
Transceiver

- **비고**
  - 현재 ~2.5G 급 광소자(LD, PD, TOSA, ROSA)는 국내 생산, 10G 급은 상용화 개발 완료 단계
  - 10G 급 이상의 광트랜시버는 외산 TOSA, ROSA를 수입하여 국내 조립 생산 중, 100G 이상의 광트랜시버는 개발 중

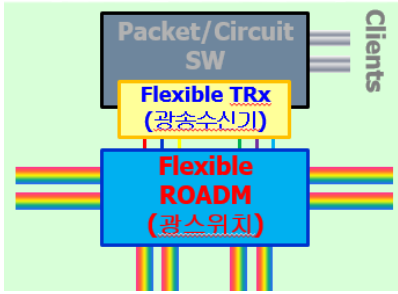
3-2. 광통신 기술—시스템



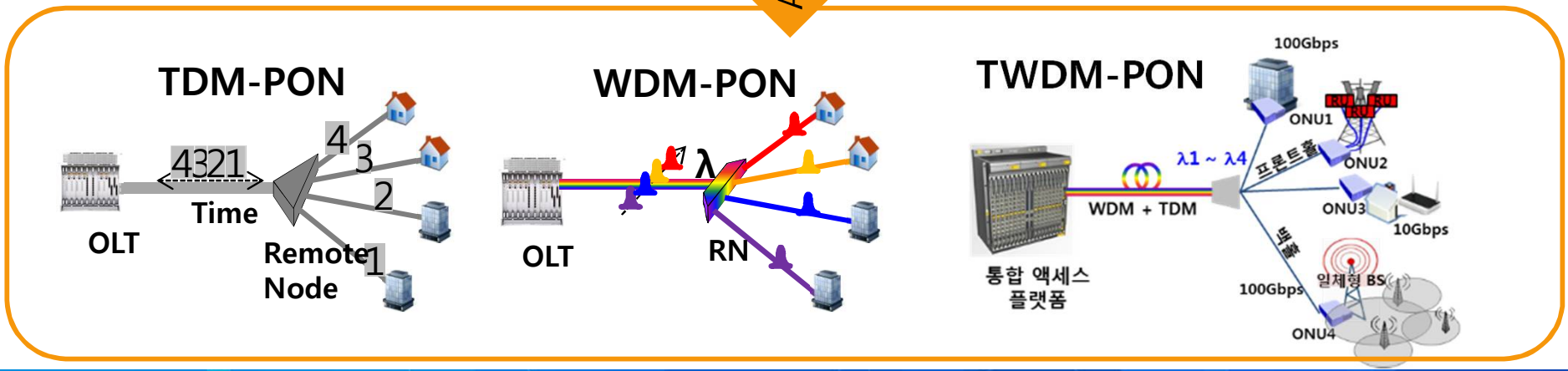
PTN+ OTN (MPLS-TP)



ROADM



8 degree



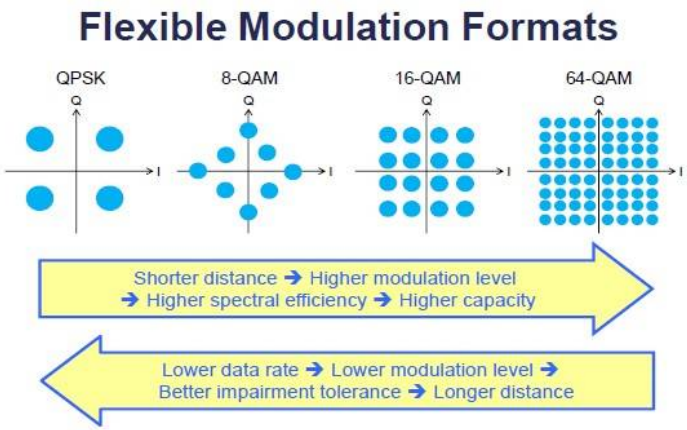
3-3. 광통신 기술- 주요 과제 수행실적/현황

	주요 기술(대표과제)	비고
1	100기가급 **초소형 광소자** 기술개발	1/4/16채널 실리콘 렌즈, CWDM AWG, 10G급 APD, 25G급 PD
2	**파장가변 LD 칩**, 광 위상변조 칩 개발	Metro 용
3	**멀티모드** 기반의 10 km급 광전송 기술 연구	6 Mode, 100Gbps/mode
4	100 Gbps급 Coherent OFDM **DSP** 기술 개발	DSP
5	25G x 4 ch **Silicon Photonics** 기술 개발	Drv+LD+MUX, DeMUX+PD+TIA
6	CDC Flexible **ROADM** 기술개발	Colorless, Directionless, Contentionless, 8 자유도
7	400G급 대역폭 가변 **광 트랜시버** 기술개발	
8	**NG-PON2** 상용시제품 개발	40G/10G, OLT 및 TWDM-PON
9	3.2/10Tera **PTN/OTN** 장비 개발	Carrier Ethernet

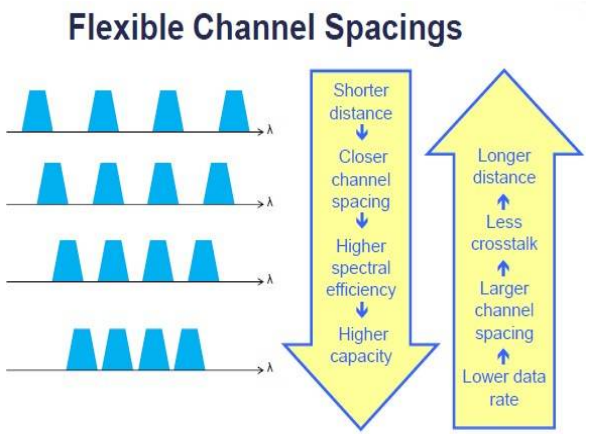
3-4. 광통신 기술- 발전방향

◆ Software Defined Optics (SDO): SDN for Flexible Photonic System

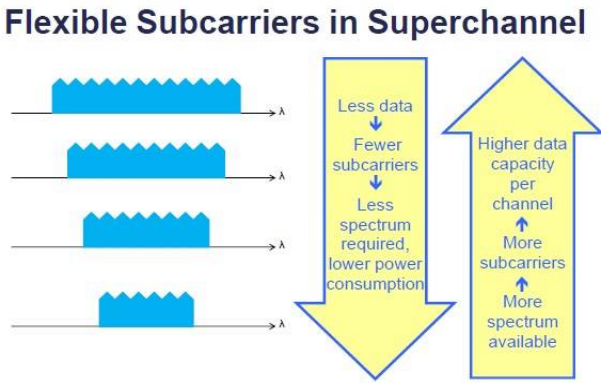
(Multi-level 변조)



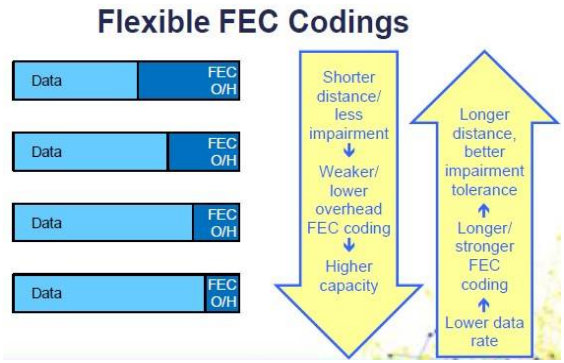
(Multi-carrier 사용)

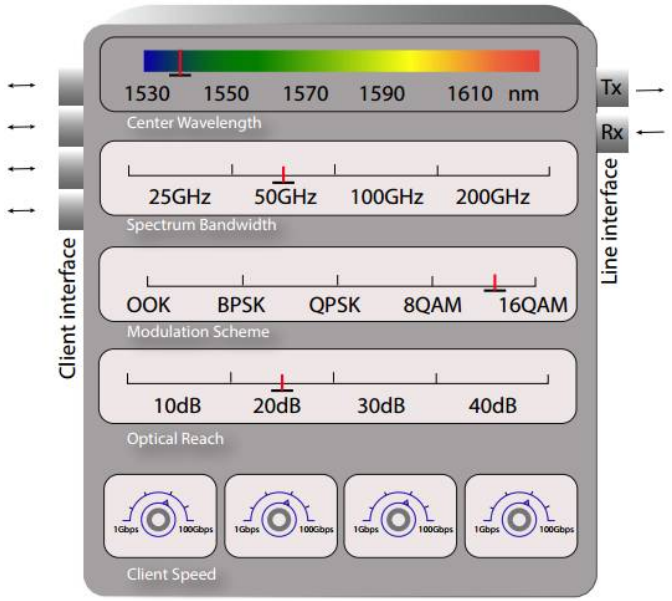


(대역폭 제어)



(에러 보정)





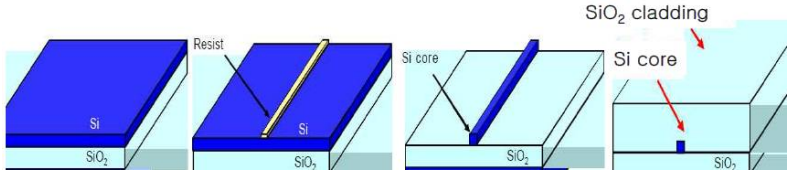
SDO 시스템 개념도
(Software로 선택 및 적응적으로변경)

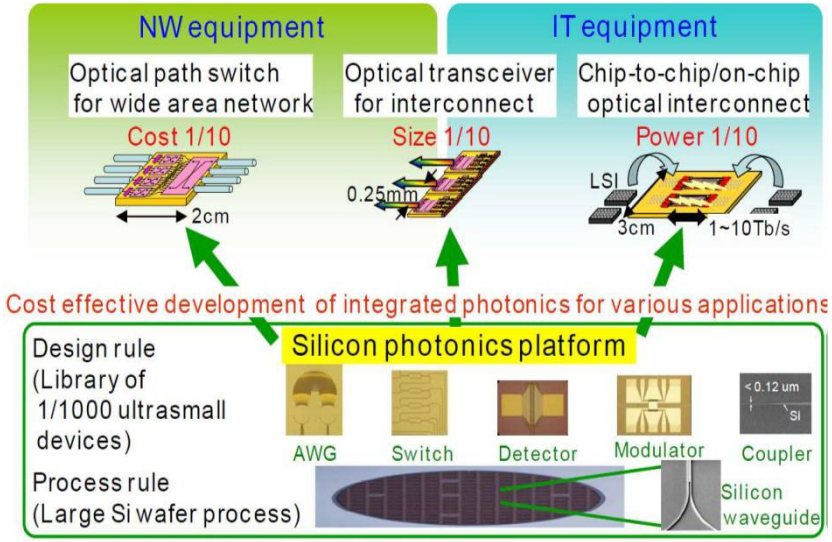
ONS 2016 자료

3-5. 광통신 기술- 발전방향

Silicon Photonics

❖ 반도체(CMOS) 제조 공정을 이용하여 광도파로(광섬유), AWG 등을 제작





❖ 특징 및 장점

- 가격, 크기, 전력소모가 1/10 이하
- 대량의 자동 생산으로 일정한 성능 유지
- 수동소자(MUX,파장 필터), 능동소자(PD, 광 스위치, 변조기 등) 및 CMOS 전자소자를 단일집적화 가능

❖ 단점

- 기술개발 초기 단계
- 소량생산에는 부적합

❖ 구현사례

- AWG + Ge PD (ETRI)

4. 양자암호화 통신 기술

4. 양자 암호화 통신

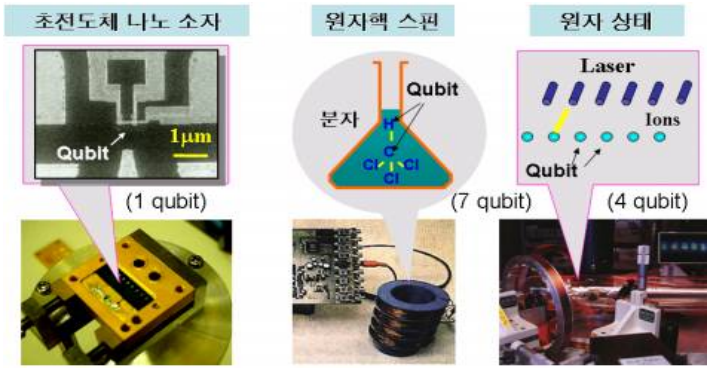
◆양자 컴퓨터

❖ 양자 컴퓨터는 이론적으로 슈퍼컴퓨터의 수억 배 이상의 성능
- 수만~ Qubit 필요(단위 양자의 정보량, 양자 얽힘)
- 10~20년 후?

❖ 캐나다 D-wave systems 社
- 2011년: 128 Qubit D-wave-1, 1,000만$
- 2013년: 512 Qubit D-wave 2X: 1,500만$+OPEX
- 2016년: 1024 Qubit 예정
- 록히드마틴: D-wave-I, 항공기 설계 최적화 문제 계산
- 구글: D-wave-II, 인공지능 기술 개발 진행
- 하버드 대학
  - 단백질 분자 모델링 및 분석
  - 슈퍼컴퓨터 30분 → 0.5초 (x 3,600배 속도)

❖ MIT, IBM 각각 5 qubit 양자컴퓨터 개발
- 2016.3월 발표
- 15자리 수의 소인수 분해 실험

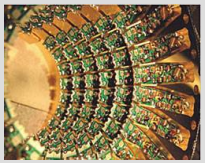
Qubit 생성 기술



4-1. 양자 암호화 통신 --- 기술 개발의 필요성

◆ 양자컴퓨터가 등장하면…

	DES	3DES	AES
개발 년도	1977년	1978년	2000년
Key 길이	56 bits	112, 168 bits	128, 192, 256 bits
500억 key/sec의 검사속도에서 최대 검사 시간	400일 (개발 당시는 해독에 2,000년 이상 걸릴 것으로 예상)	112의 경우 800일	128의 경우 $5x10^{21}$ 년
실제	1999년, DES Challenge Ⅲ에서 10,000대의 컴퓨터로 병렬처리하여 22시간 15분 만에 해독 (KISA 자료)		???
Reference	"New comparative study between DES, 3DES and AES", Journ Computing, Vol2., Issue3, Mar. 2010		

슈퍼 컴퓨터(Bit)	양자 컴퓨터 (Qubit)
	
암호 해독: 300자리 정수 소인수 분해에 걸리는 시간	
> 2천만년	30분

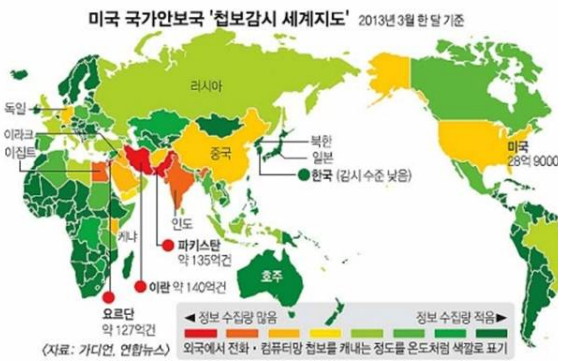
InfoWorld

Quantum computers pose a huge threat to security, and the NIST wants your help

An upcoming competition will invite the public to propose and test 'quantum-resistant' encryption schemes

◆ 국가보안 문제

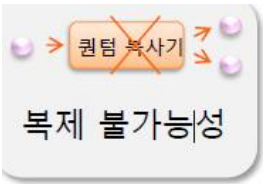
- ❖ 2013년, 스노든 사건
  - 미국 NSA의 무차별 도청, 서버해킹
- ❖ 금융, 군통신…



출처:영국가디언지, 번역 및 Edit : 연합뉴스

4-2. 양자 암호화 통신 개요

- **양자(Quantum, 量子)**
  - 물질의 최소단위: 전자, 원자, 소립자, 광자 등
- **양자의 특징**
  - 불확정성 원리(Uncertainty principle): 물리량(위치, 속도 등)을 동시에 측정 불가
  - 복제불가능(No-cloning): 특정 양자 상태를 다른 양자에 복사할 수 없음
  - 중첩 (Superposition): 두 가지 상태가 마치 동시에 존재하는 것처럼 측정
  - 이중성(Duality): 입자와 파동의 성질을 동시에 가짐
  - 양자 얽힘(Entanglement): 두 개 이상의 양자들의 상태가 동시에 변화하는 성질
- **양자암호통신**
  - 단일 광자(Single Photon)를 사용, 단일 광자는 단 1회의 관측만 가능, 복제 불가능, 양자중첩, 얽힘 등의 성질을 이용
  - 도청(정보탈취)이 근본적으로 불가능

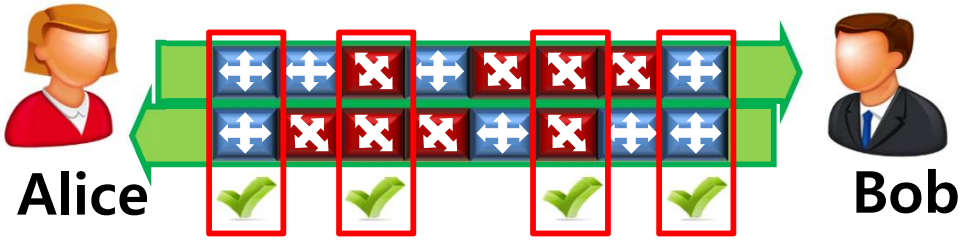


4-3. 양자 암호화 통신 -- 원리

◆ 원리

❖ BB84 프로토콜

- 1984년 Benett와 Brassard 개발



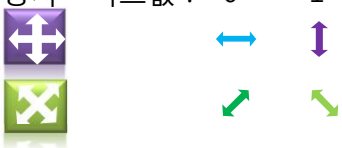
Alice's bit	0	1	1	0	1	0	0	1
Alice's basis(편광판)	+	+	×	+	×	×	×	+
Alice's polarization(편광)	→	↑	↖	→	↖	↗	↗	↑
Bob's basis(편광판)	+	×	×	×	+	×	+	+
Bob's measurement	→	↗	↖	↖	↑	↗	↑	↑
Shared key	0		1			0		1

중첩에 의해, 동일한 편광과 기저에 대해서 0 또는 1이 무작위로 결정되므로 배제

- Shared Key를 공유하면서 암호 통신을 수행함.
- Shared key가 일치하지 않으면 도청 가능성이 있으므로 버린다.

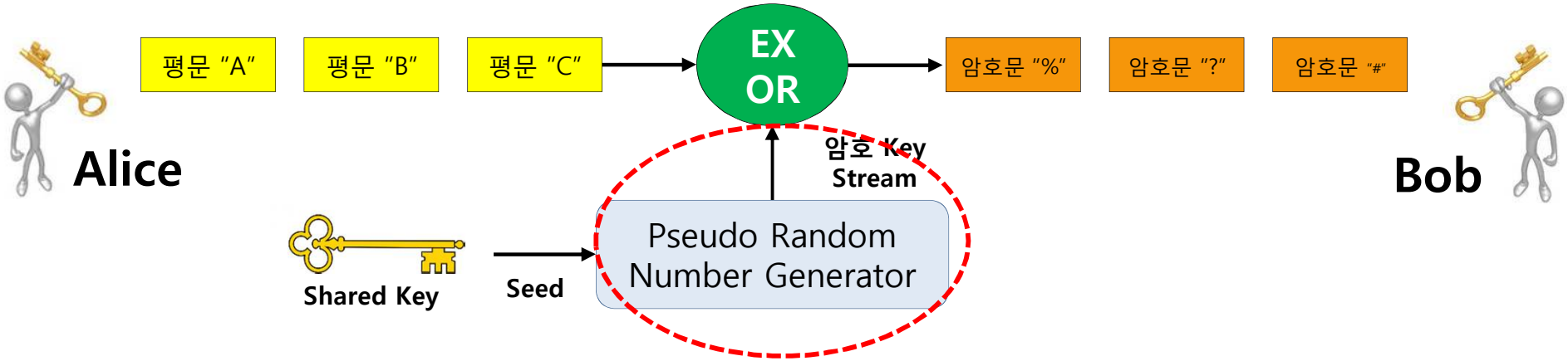
양자암호에서의 편광

편광자 비트값 : 0 1

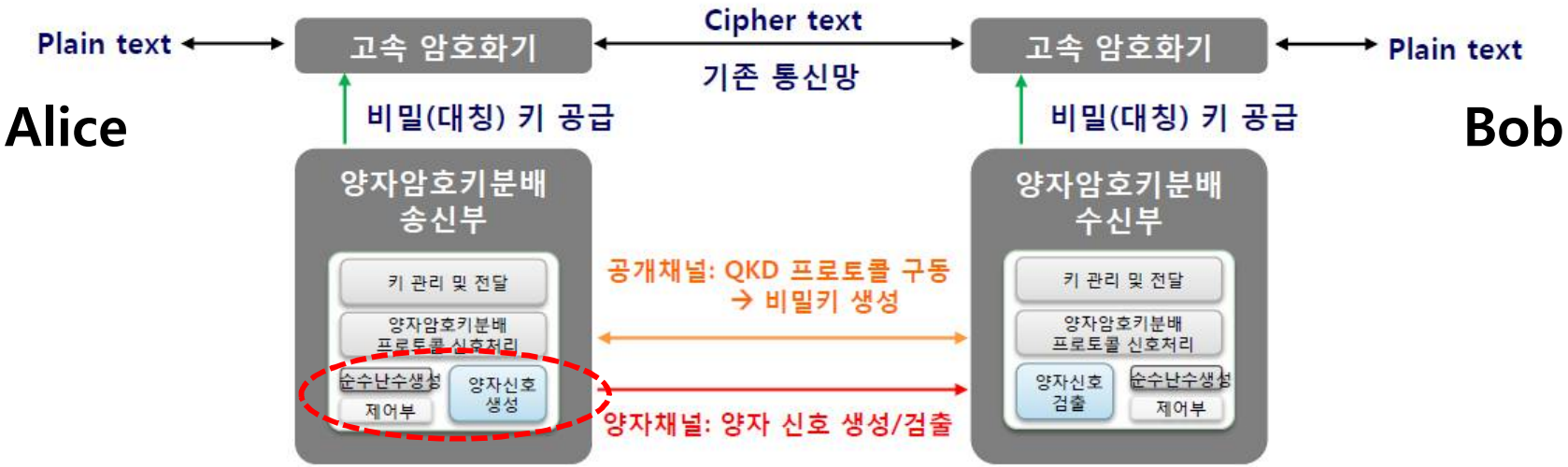


4-4. 양자 암호화 통신 개요

◆ 대칭키 암호화



◆ 양자 암호화



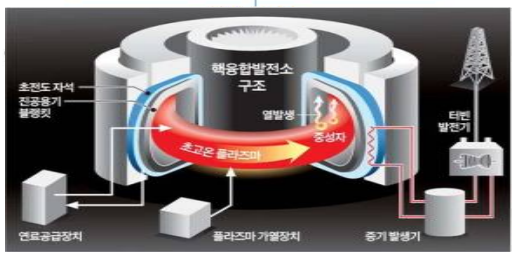
4-5. 양자 암호화 통신 – 해외 연구동향

◆ 양자 암호화 통신은 국가 안보에 필수적인 기술

- ❖ **북한**, 2016년 2월에 김일성 종합대학의 개발 발표
- ❖ **구글, IBM, 마이크로소프트, 도시바, 알리바바** 등이 개발참여 선언

미국 이전 거부 핵심기술

AESA 레이더	IRST	EO TGP	RF Jammer
여러 표적 동시 추적 기계식보다 탐지거리 2~3배	적외선신호로 표적 탐지	공대공, 공대지 표적영상 정보 획득	적의 레이더 등에 방해전파 발신



구분	주요 연구 동향
유럽	o Qurope(Quantum Europe) 프로그램을 통해 유럽의 연구개발 로드맵을 제시하고 일관된 연구 수행 o EU는 미래기술(FET, Future Emerging Technologies) 사업에 Quantum Simulation을 선정, 525억 투자 o 영국은 2013년 Autumn Statement를 통해 양자기술 산업화에 2015년부터 5년간 4,800억 투자 발표
미국	o 2008년 국가양자정보과학 비전 발표, NSF, IARPA, DARPA 등을 통해 **年 1조 투자**
러시아	o 2010년 Russian Quantum Center를 설립, 양자광학, 재료, 정보처리 기술 등에 집중 투자
캐나다	o 캘거리大, 워터루大, 토론토大 등에 양자정보통신학과를 설치, 미래 ICT 선도를 위한 인재 집중 양성 o 워터루大 Quantum-Nano Center를 설립, 年500억 투자
중국	o 中과학기술부는 2012년부터 5년간 양자기술 등에 2,900억 투자, 2016년 무선 양자암호 시험용 인공위성 발사 예정
일본	o FIRST 프로그램을 통해 양자정보처리(Quantum Information Processing)에 4년간 430억원 지원 o Riken, CREST 등을 통해 양자정보통신에 年 220억원 지원 o NICT는 2040년까지 기밀성이 보장된 사회를 위한 양자 로드맵에 따른 기술 개발을 진행 중
싱가포르	o 싱가포르국립대학을 통해 양자기술에 年1,300억 투자
브라질	o Pontificia 대학에서 스위스 Geneva 대학 그룹 등과의 협력 연구를 통해 기술 개발
말레이시아	o Kebangsaan, International Islamic 대학 등에서 유선 및 자유공간 양자암호 프로토콜 및 시스템 연구 수행 중

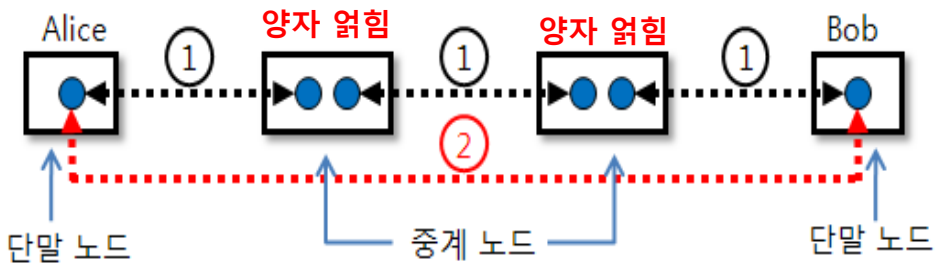
4-6. 양자 암호화 통신- 주요과제 수행실적/현황

◆ 2017년 말에 서울-대전 간에서 장거리 전송 시범 예정

	주요 기술(대표과제)	비고
1	양자 암호통신망 **QKD 시스템 및 소자** 기술 개발	**양자암호 송수신기 및 소자개발**, Testbed 구축
2	양자 암호 프로토콜 및 **1X64 양자 암호통신 가입자망(PON) 기술 개발**	QKD+RSA(공유키 암호) 개발, PON 용 송수신기 개발
3	양자 암호 **중계기** 기술 개발	서울-대전 간 장거리 중계 시험
4	**새로운 양자암호통신 프로토콜** 개발	Measurement- Device-Independent, 프로토콜 검증 및 개선

양자암호통신 Testbed 구축 현황

운영주체	구간	전송거리 (왕복)
SKT	분당~성남중심국	17.8Km
SKT	분당~수원중심국	53Km
SKT	분당~용인중심국	68Km
SKT	분당~양평중심국	107km
KISTI	SuperSiReN대전구간	11Km



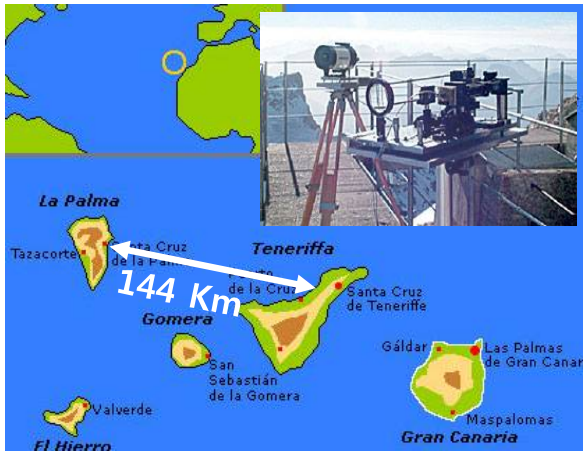
4-7. 양자암호화 통신 - 발전방향

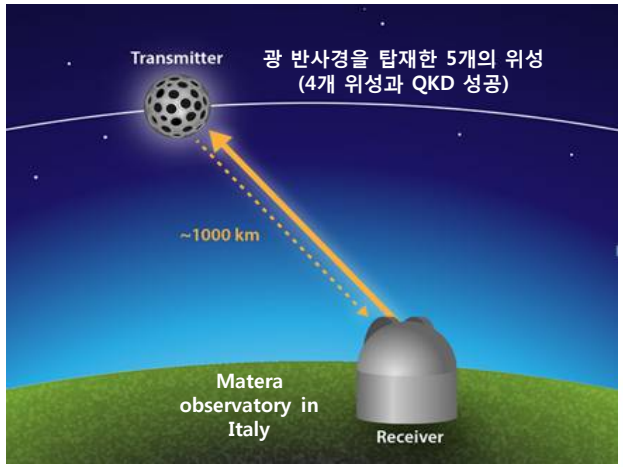
◆ 자유공간 레이저 기반 양자암호 통신 기술 개발

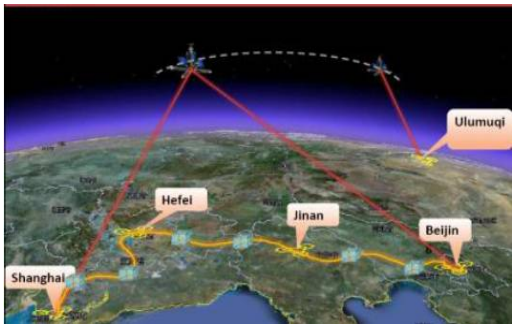
- ❖ **2007년 유럽** 연구팀, 북아프리카 Canary 제도의 2개 섬 간**(144km)에서 무선 QKD 전송 실험 성공**
- ❖ **2015년 이태리 연구팀, 1,000 Km 상공의 인공위성과 QKD 실험 성공**
- ❖ **중국 2016년 하반기에 무선 양자암호통신용 위성 발사 예정**

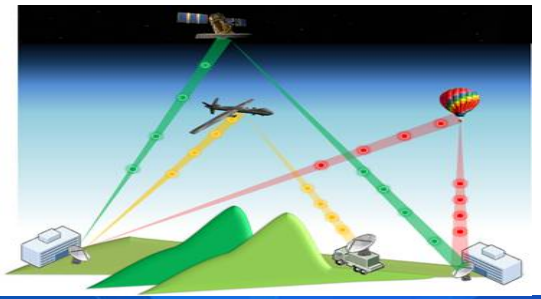
◆ 향후,

- ❖ **위성, 성층권 열기구, 고정 기지국 간 및 이동체(차량, 선박)에 적용 가능**







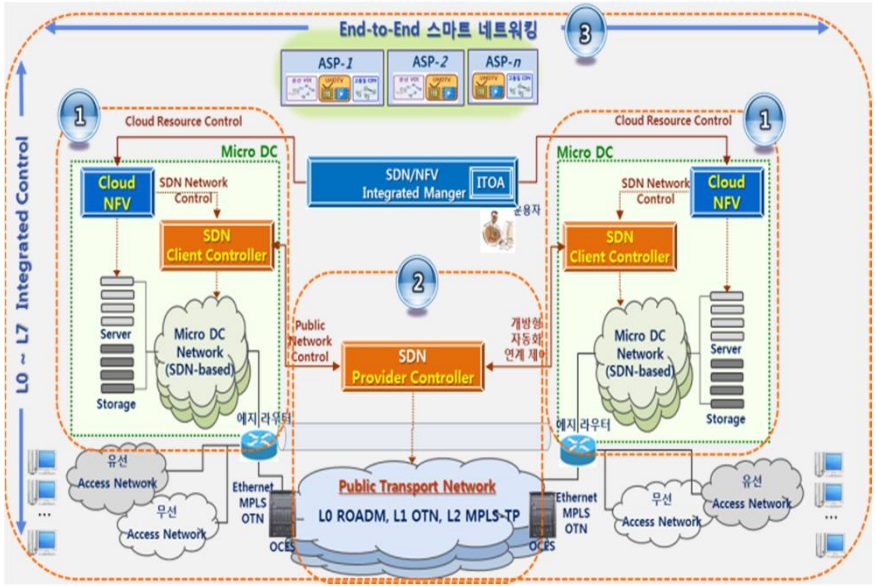


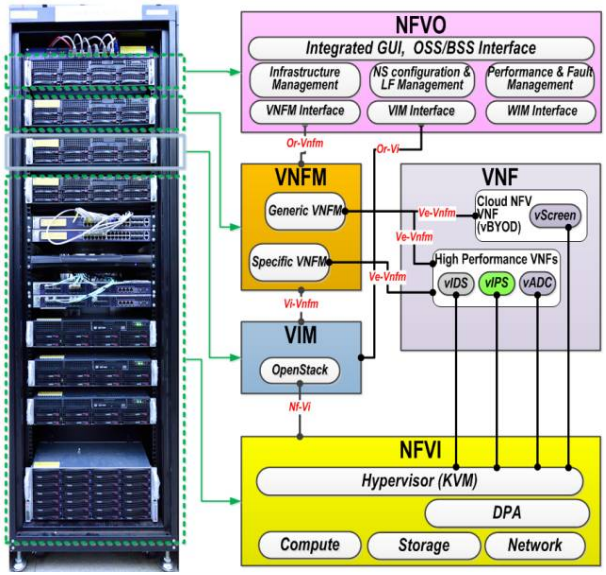
5. SDN/NFV 기술

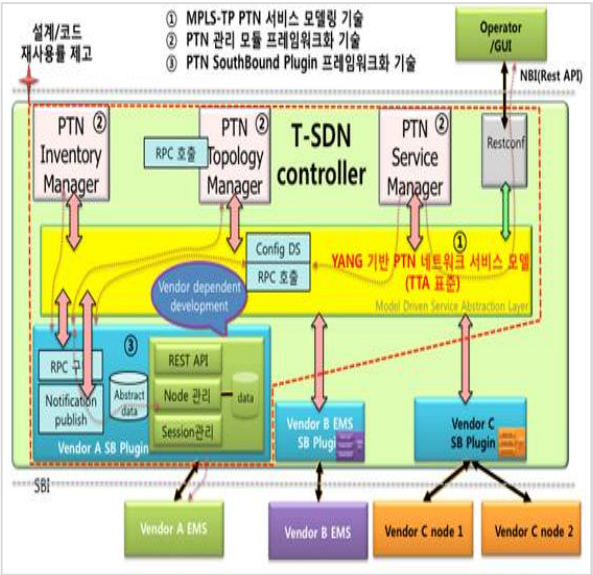
5. SDN/NFV 기술 개발 현황

	주요 기술(대표과제)	비고
(1)	Cloud SDN, Transport SDN 기술 개발	ONOS, ODL
(2)	SDN 기반 네트워크 은닉 기술 개발(RRM, RHM)	
(3)	SDN 기반 광 액세스망(vOLT+PON) 기술 개발	
(4)	가상 EPC 솔루션 개발	
(5)	네트워크 하이퍼바이저 개발, SBI(LISP, MPLS) 확장, Traffic Engineering 기술 개발	ONOS, OVX
(6)	Open Source 개발 과제(K-ONE, OpenWinCon) 등	OpenStack, ONOS, OPNFV

5-1. 기술개발 현황 (1) Cloud, Transport-SDN 기술 개발







- **Cloud SDN 및 NFV 개발**
  - OpenStack, ONOS 기반
  - PTN 및 MPLS-VPN을 경유한 Micro-DC 간 연결 및 VNF 이동 등
  - Orchestrator 및 VNF(IDS, IPS, 가상 라우터 등), VNFM, VIM 프레임워크 개발
- **Transport-SDN 개발**
  - OpenDayLight 기반
  - PTN(OCES) BoD, Traffic-offloading 제어

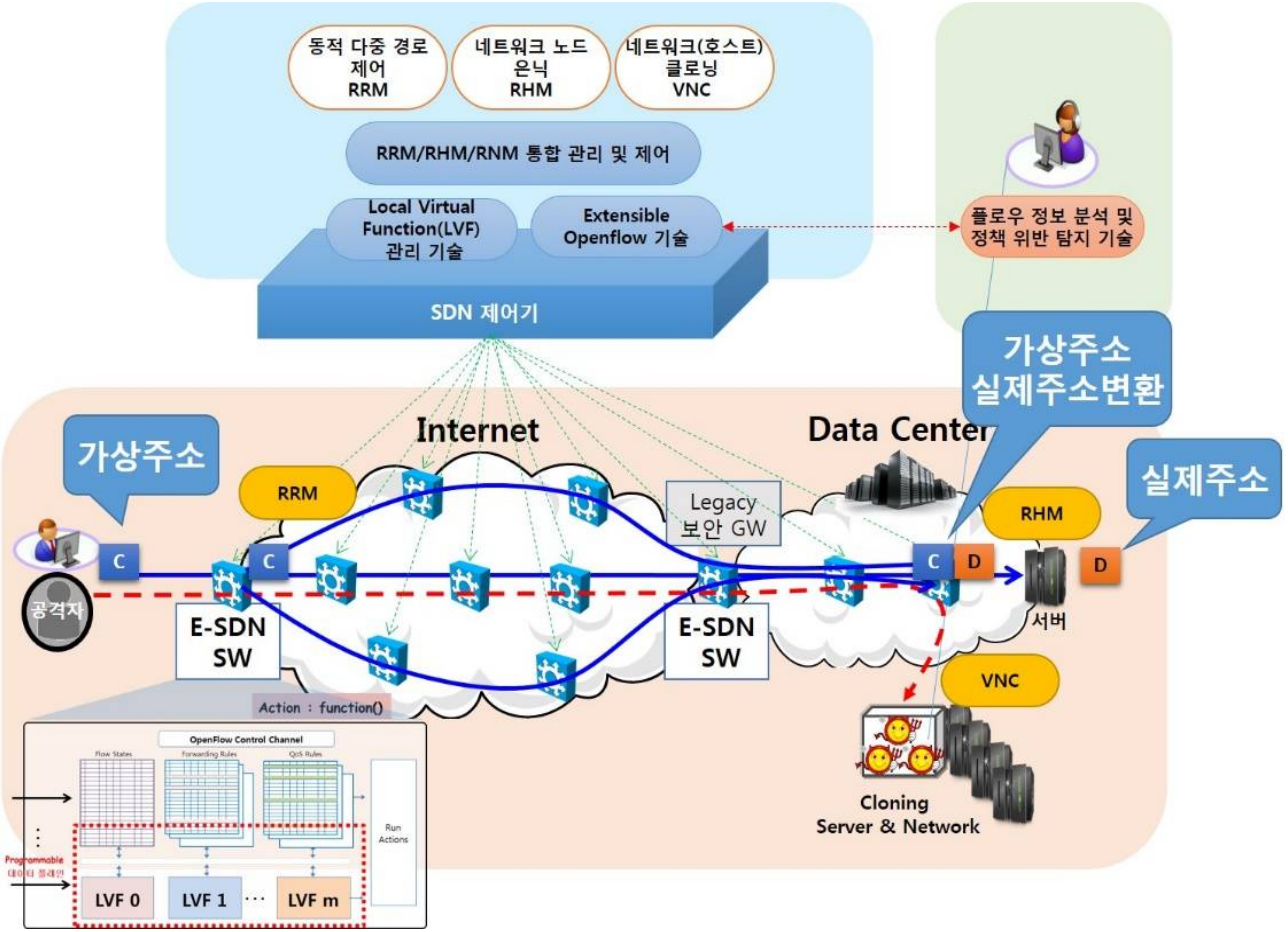
5-1. 기술개발 현황 (2) SDN 기반 네트워크 은닉 기술개발

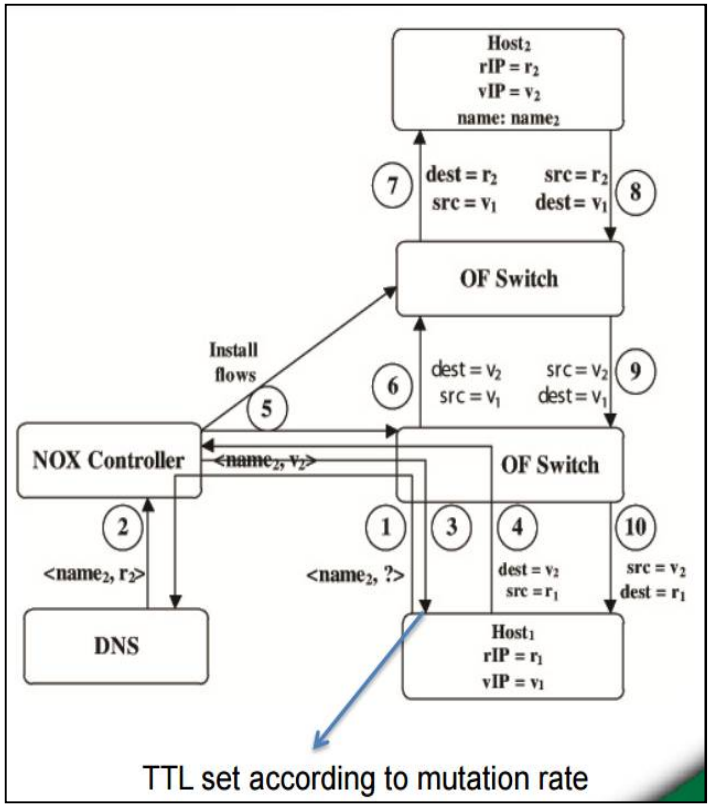
Moving Target Defense

Scan 및 Sniffing으로부터 보호

- **RRM** : 라우팅 경로를 주기적으로 변경
- **RHM** : Host의 IP 주소/Port 를 주기적으로 변경하여 Host를 보호
- **VNC** : 유해/의심 트래픽을 분석/차단하는 가상 네트워크 기술

RRM : Random Route Mutation
RHM : Random Host Mutation
VNC : Virtual Network Cloning
E-SDN : Extensible SDN

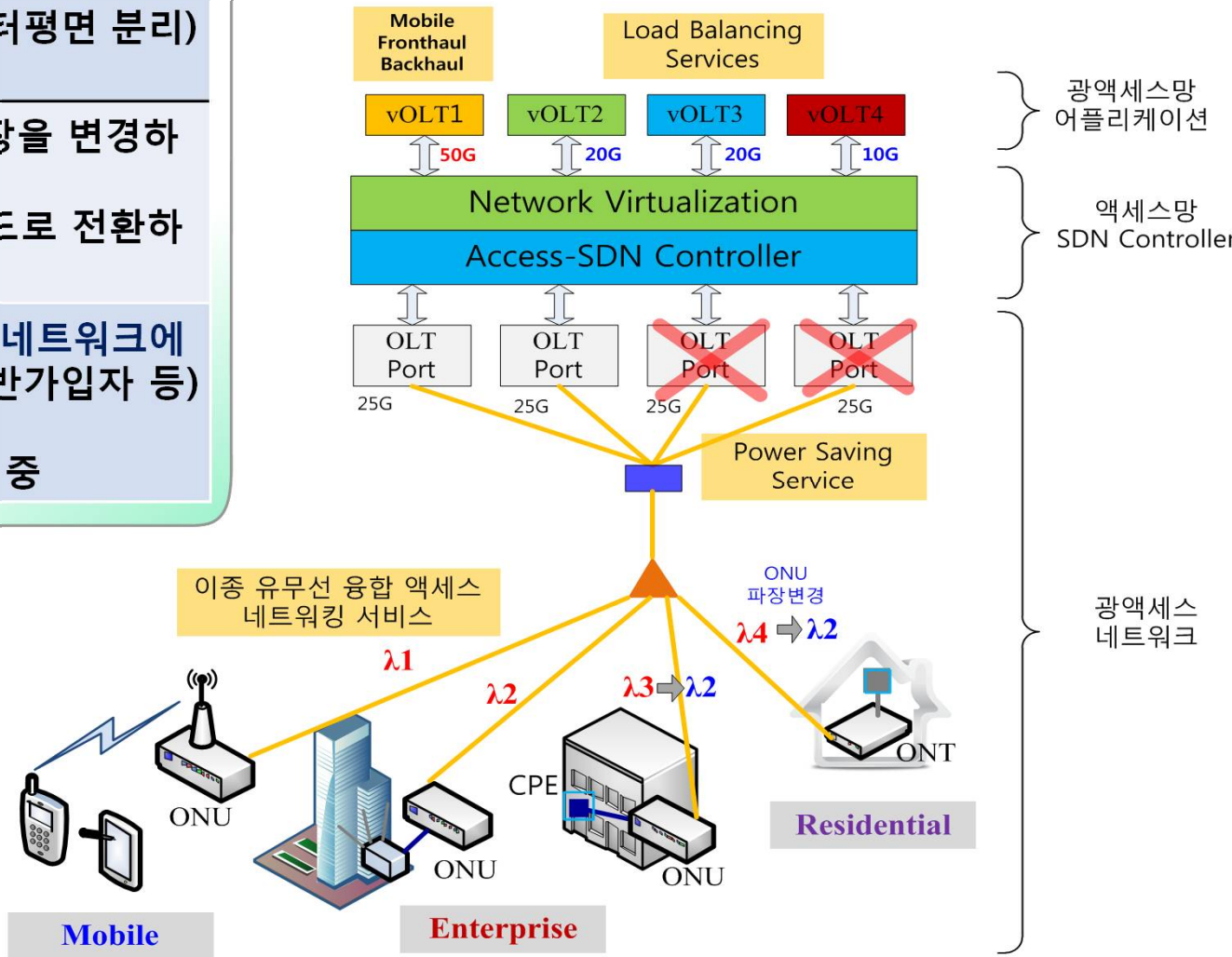




5-1. 기술개발 현황 (3) SDN 기반 광액세스망 제어기술 개발

기능	광액세스망 (OLT+PON) 가상화
OLT-PON 가상화	• OLT 가상화(제어평면과 데이터평면 분리) • PON 가상화
파장 가변 부하제어 (Load Balancing)	• 트래픽 양에 따라 ONU의 파장을 변경하여 OLT port를 절체하고, • 미사용 OLT port를 Sleep 모드로 전환하여 전력 절감
이종 유무선 서비스 통합 수용	• 이종 유무선 서비스를 PON 네트워크에 통합 수용(Mobile, 기업, 일반가입자 등) → CAPEX/OPEX를 절감 • 기존은 ptp WDM으로 운용 중

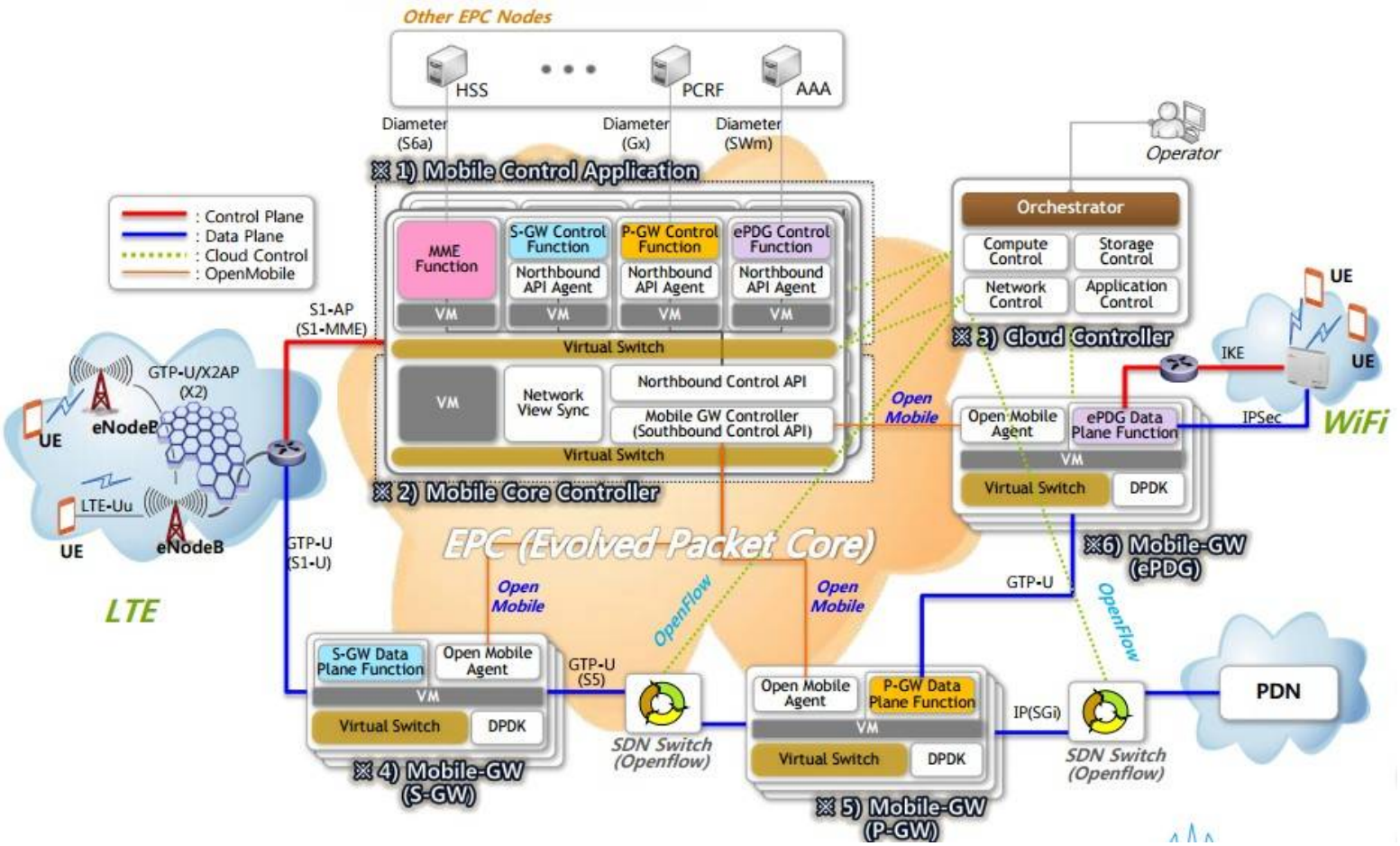
- 전체 네트워크 전력의 90% 및 비용의 50%를 액세스 네트워크에서 사용
- Mobile xHaul은 매우 낮은 latency와 jitter를 요구.
- Full-service access 기술 개발이 필요 (Mobile, Business, Residential)



[광액세스망 SDN 서비스 구조]

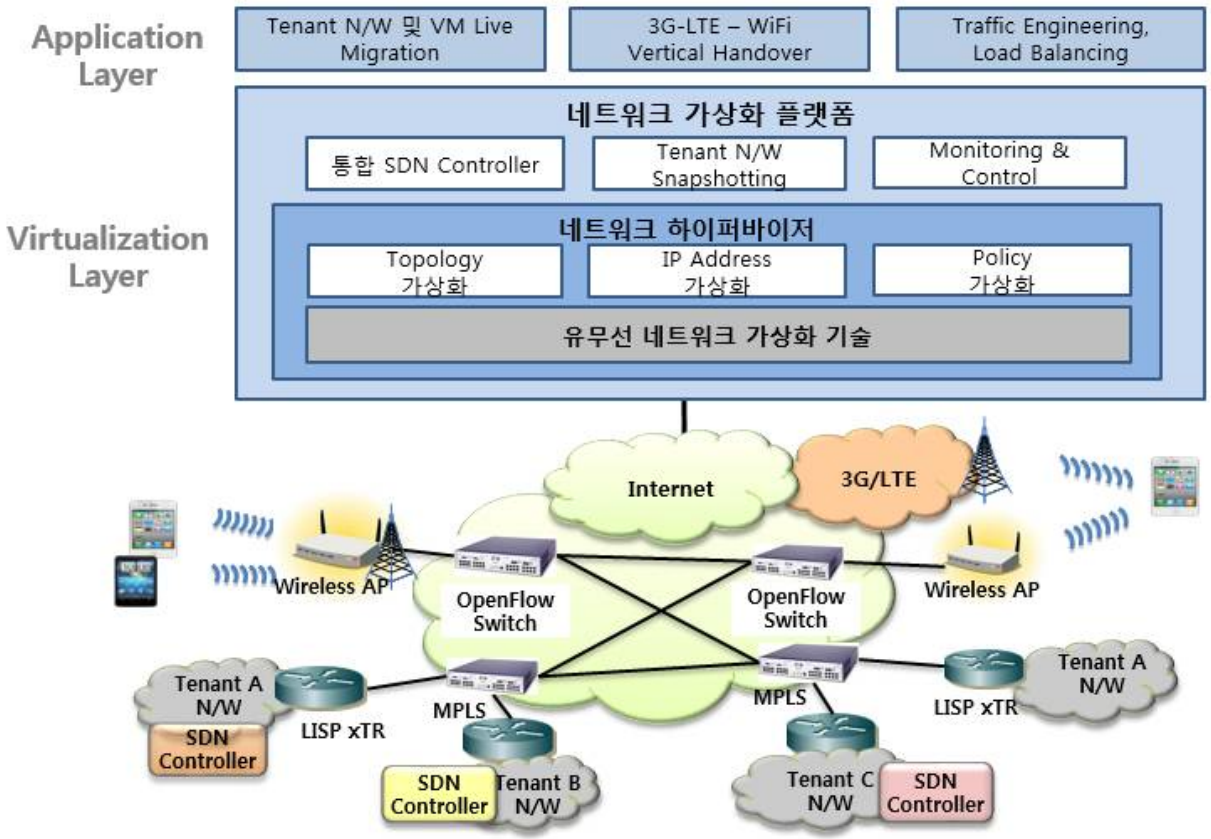
5-1. 기술개발 현황 (4) SDN/NFV 기반 vEPC 개발

- SGW, PGW, ePDG의 제어평면과 데이터 평면을 분리, MME 구현 등
- 가상 스위치에 GTP tunnel 구현
- 현재는 Private LTE 용도 (수만 가입자 동시 수용 규모) → 5G Core 용도로 발전



5-1. 기술개발 현황 (5) SDN 2.0 솔루션 개발

- SDN 기반의 확장성 있는(Scalable) 네트워크 가상화 솔루션 개발
- SBI 확장 (LISP)
- SDN 기반의 서비스(MPLS-TE, Traffic Engineering, Failover 등) 개발



네트워크 가상화 플랫폼

- 토폴로지 가상화
- 주소 가상화
- 정책 가상화
- 유무선 네트워크 가상화

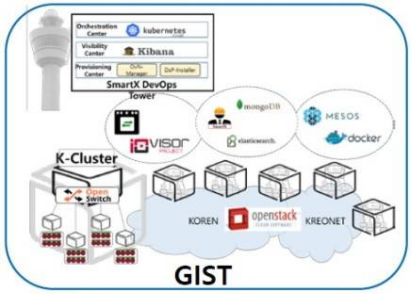
확장 SBI

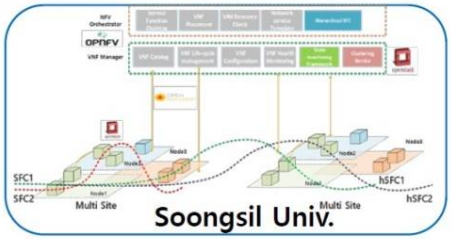
- Protocol Abstraction Layer
- 벤더 독립, LISP 프로토콜 개발

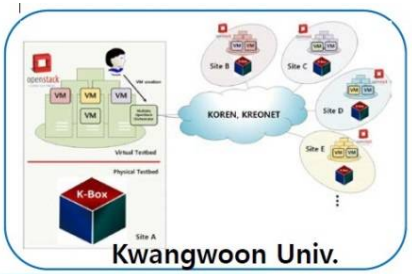
서비스 개발

- Traffic Engineering (Loadbalancing, Failover)
- MPLS VPN/TE
- LTE-WiFi Vertical Handover

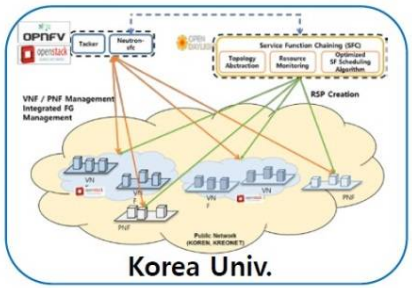
5-1. 기술개발 현황 (6) Open Source 개발

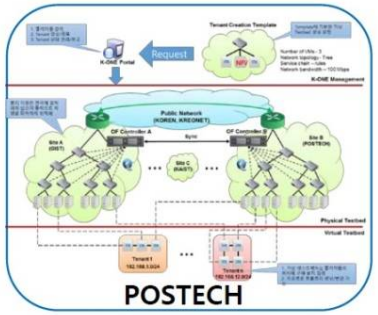


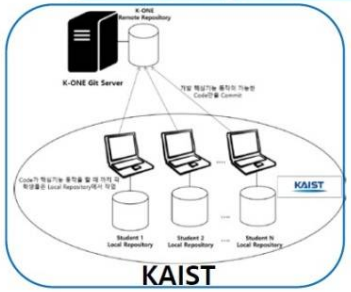




ONOS, OpNFV, OpenStack

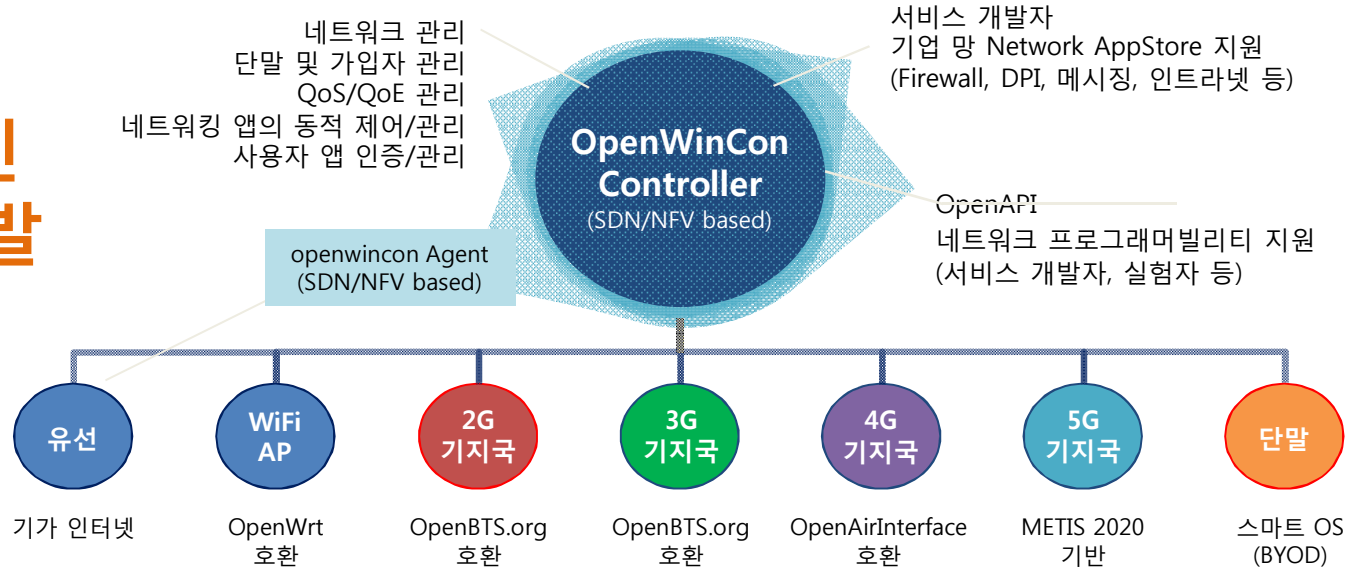






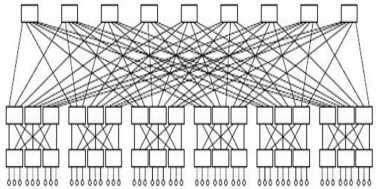
Various Environments

액세스 방식에 독립적인 통합 네트워킹 기술 개발

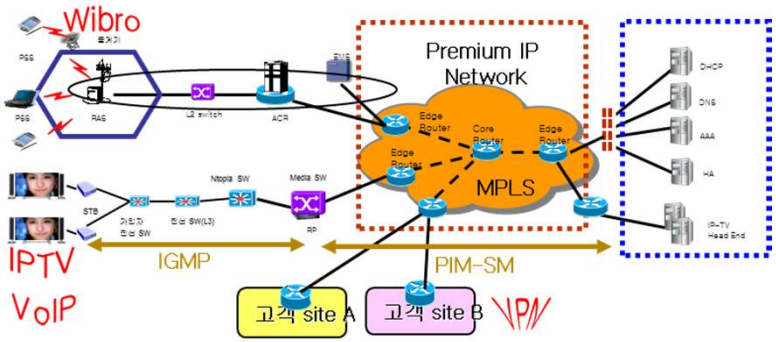


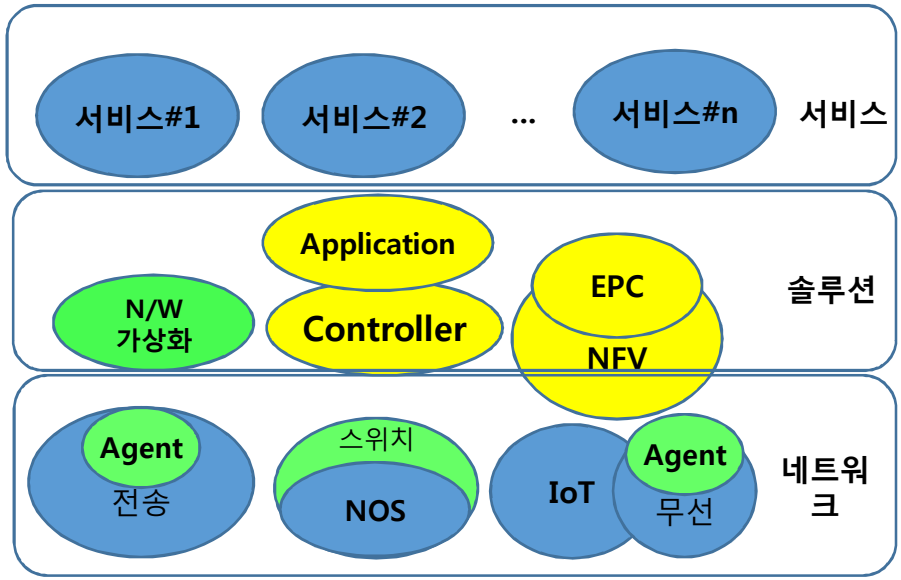
5-2. SDN/NFV 과제 수행 현황

- SDN 컨트롤러 기능 개발 및 애플리케이션 개발 과제가 대부분
- 시장이 큰 대형 (OpenFlow) 스위치 및 서비스 개발 과제는 부족
  - 예: 데이터센터 구축 비용(Cisco)
    - 27,000개 서버 : 1억 6천만 USD
    - (계위적) 네트워크 구성: 3,700만 USD
    - 컨트롤러 : 20만 USD +



  - 서비스= VoIP, IPTV, MPLS-TE, L3-VPN …
    - 캐리어 네트워크의 진입 장벽
    - 통신사업자의 Premium 망과 연동하여 구내망 내부까지 QoS 서비스를 확장 가능

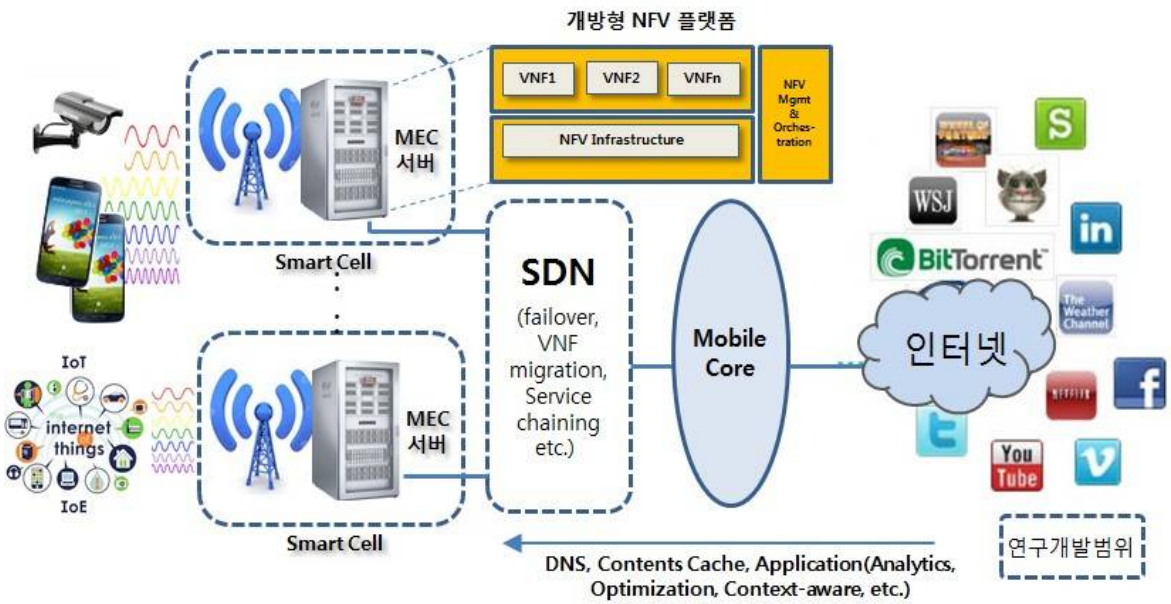


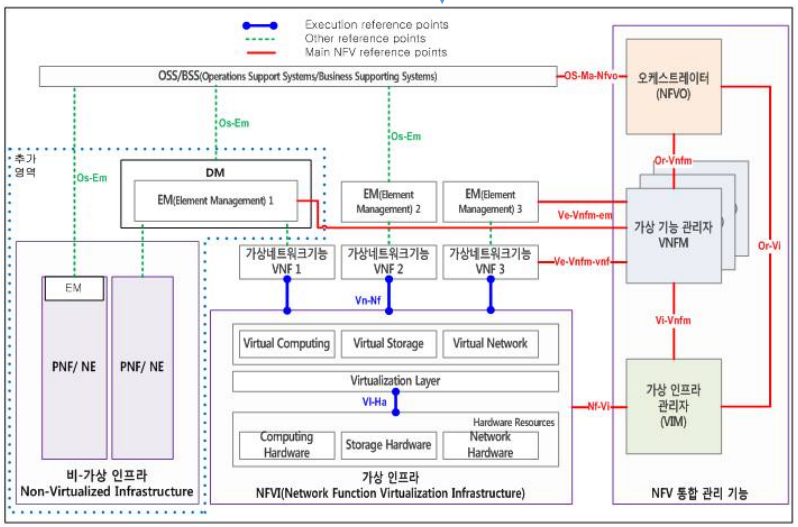


5-3. SDN/NFV 기술 개발 --발전 방향

- **mEC(mobile Edge Computing)+ VNF 기술**
- **요구기능**
  - 개방형 NFV 솔루션
  - 초고속, 저지연 서비스
  - 실시간 감시, 프로비저닝 및 scale-in/out
  - 서비스 체이닝, VNF Live migration
  - vEPC + Contents Cache + VR/AR servers … 개발 기술 or 소스코드 확보 문제

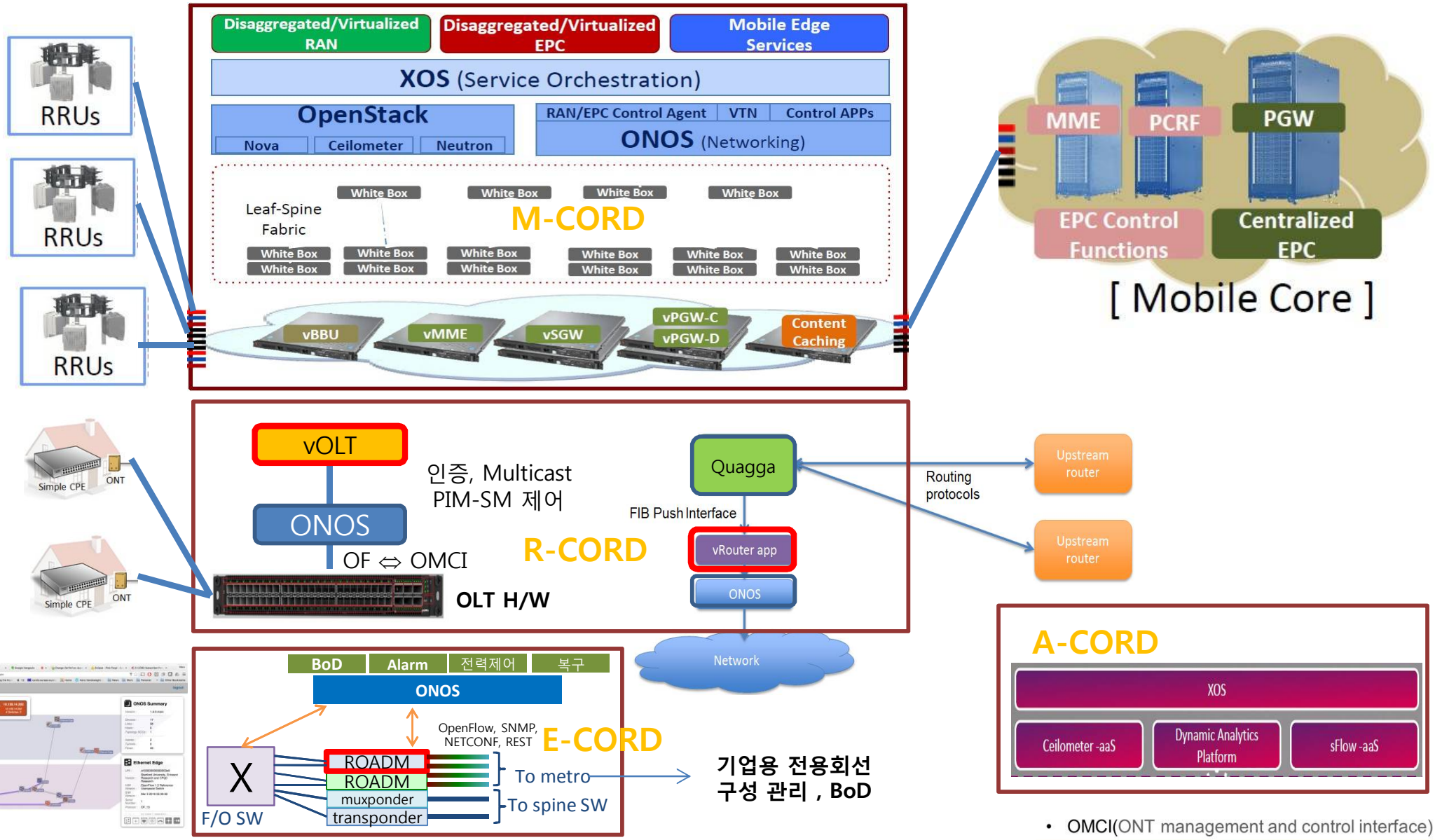
- **Framework 개발 과제 제안이 대부분**





5-3. SDN/NFV 기술 개발 --발전 방향

AT&T+ON.Lab … CORD(Central Office Re-architected as a Data Center)



- OMCI(ONT management and control interface)

5-3. SDN/NFV 기술 개발 --발전 방향

◆ Programmable Switch(H/W) 및 응용기능(S/W)

❖ 現 Fixed function ASICs → Programmable switch chips 등장

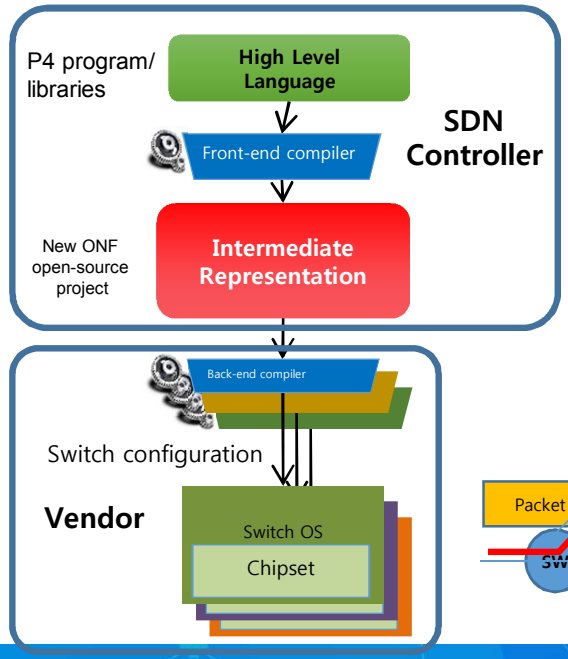
- 現 OpenFlow 규격은 TCAM model
  - 고정된 Match field 확장 문제 (현재 44 tuples = 약 170 bytes)
- Programmable Switch Chips
  - Flexible Match+Action ASICs: Intel Flexpipe, Cisco Doppler, Xpliant, Cavium …

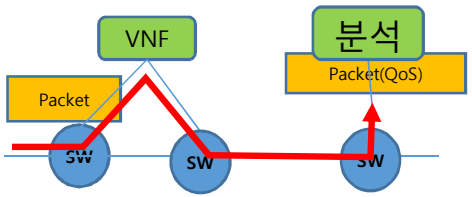
❖ 기술 동향

- P4: 데이터 평면 프로그래밍 언어 (≅ OpenFlow 2.0)
- POF: {Offset, Length}를 사용,Match →Action 수행

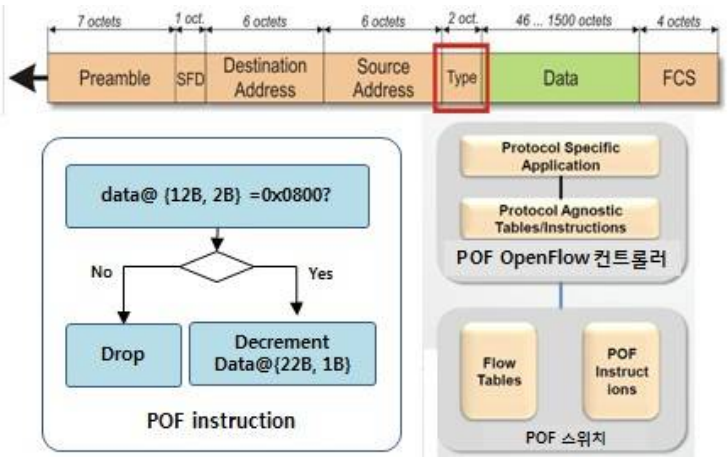
- 100G ~ 1 Tera bps 급의 속도
- 고도의 운용관리, 분석 기능
- 다양한 미들박스/서비스 구현 가능

P4 (Programmable, Protocol-independent Packet Processor)





VS



POF(Protocol Oblivious Forwarding)

6. 결론

◆ 광통신 기술

- ❖ 지속적인 트래픽 증가에 대비하여 고속, 저전력, 저가격화를 목표로 기술 개발 필요
- ❖ 광통신의 한계를 넘는 기술로서 Multimode 광통신기술 개발 필요
- ❖ 규격화된 제품의 양산이 가능한 Silicon Photonics 기술 개발
- ❖ Software-defined Optics 기술 개발

◆ 양자암호화 통신 기술

- ❖ 국가 안보에 필수적인 기술/해외 기술도입은 사실상 불가능 (예: 발사체/Lader Array)
- ❖ 유선 양자암호 기술의 상용화 추진
- ❖ 무선 양자암호화 기술 개발

◆ SDN/NFV 기술

- ❖ 시장규모의 성장이 가장 빠르며 현재의 네트워크 산업을 대체할 유망 기술
  - 수년 내에 데이터 센터 및 기업 통신망, 액세스 망의 핵심기술이 될 전망
- ❖ 저가의 고성능 Programmable 스위치 개발
- ❖ SDN 기반의 통신 서비스 개발
- ❖ CORD(or Edge Computing) 기술의 개발
- ❖ 단, 상용화 가능한 기술 개발 (확장성, 저비용)하고,
  - SDN 환경에 국한된 솔루션 개발은 바람직하지 않음
  - 現 인터넷과의 공존 기능을 개발(Overlay-SDN or SDN-WAN)

감사합니다