Trusted IP Network Innovator
MC MOBILE CONVERGENCE

高信賴 국방정보통신망 실현을 위한

네트워크 기반 정보보호 기술

2016. 2. 26.

CST 대표컨설턴트 이인화
inhlee@cst.co.kr
M. 010-2727-1838

CST ICT CONSULTING

Contents

I. IP Network 리뷰

II. 동향과 요건

III. TIPN 시스템

IV. 차별성 및 기대효과

2016 CST Proprietary

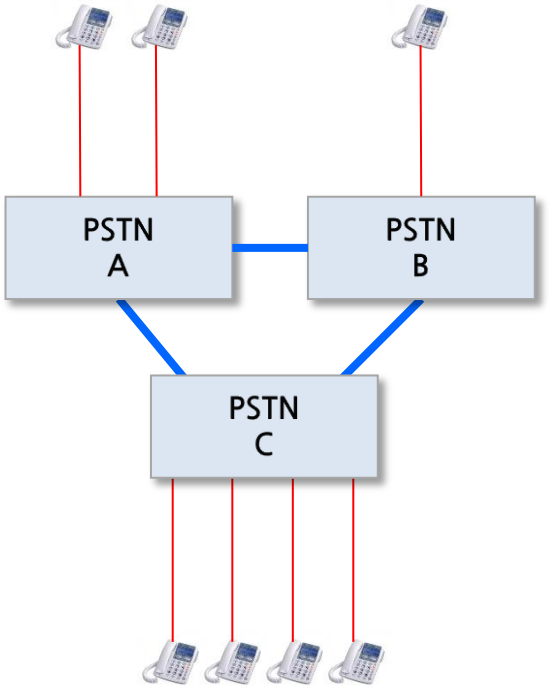
I. IP Network 리뷰

전화망으로 IP망 (인터넷) 해석

- 전화망 : PSTN 의 교환 단위는 단말 대수 → 7개 단말 간에 21개 경로
- 인터넷 : Router의 교환 단위는 LAN 대수 → 4개 LAN 간에 6개 경로

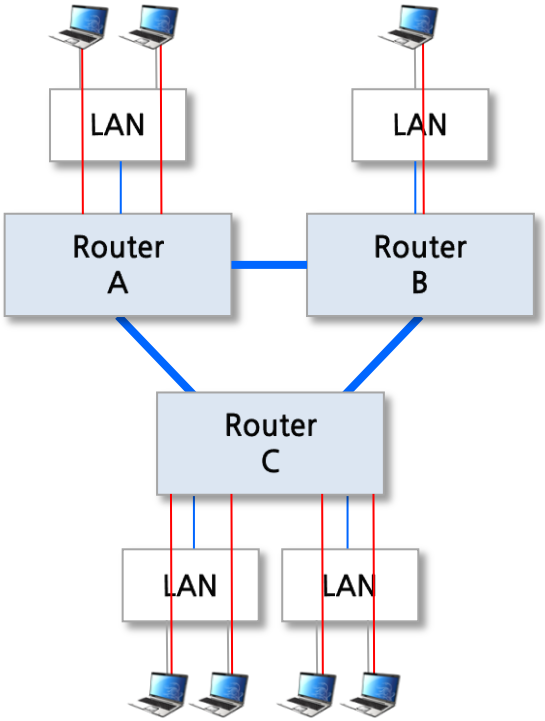
* n =1,000 대 이면 PSTN은 500*999 = 499,500 개의 경로가 되지만, IP Network은 여전히 n=4가 되어 경로는 6개 뿐임

전화망 (Circuit)



$$\frac{n(n-1)}{2} = \frac{7(7-1)}{2} = \mathbf{21}\text{개 경로}$$

IP망 (Packet)



$$\frac{n(n-1)}{2} = \frac{4(4-1)}{2} = \mathbf{6}\text{개 경로}$$

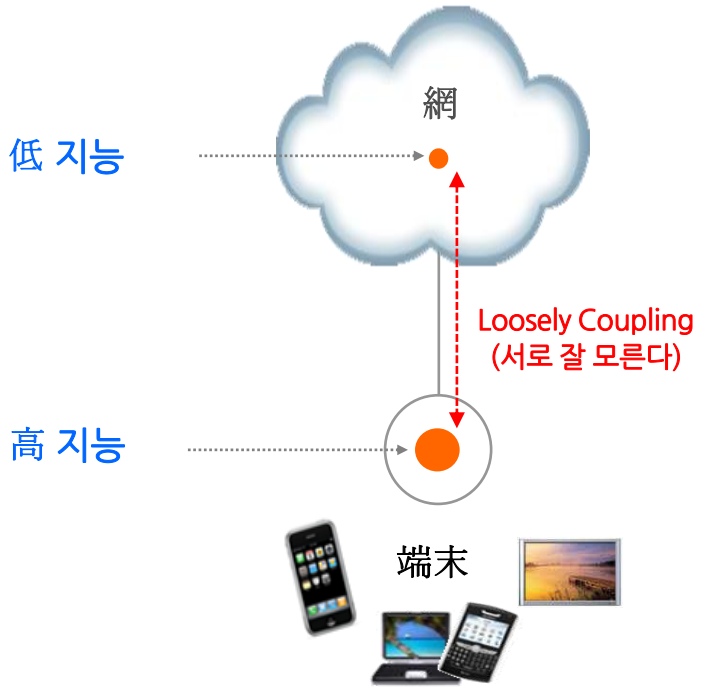
2016 CST Proprietary

網과 端末의 지능

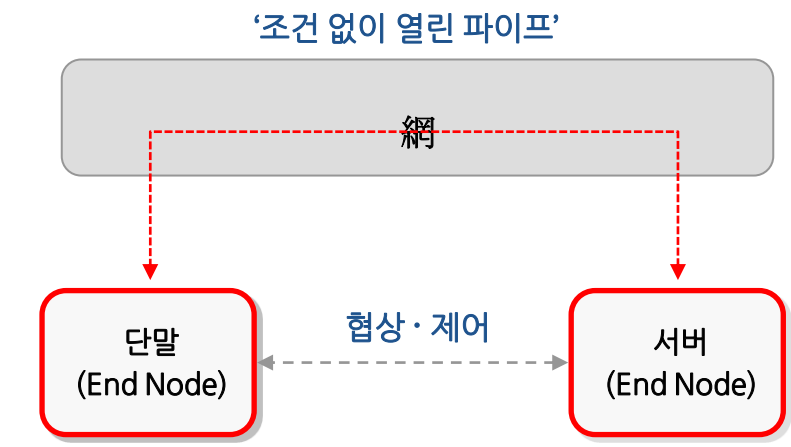
서비스 인지(Awareness) 지능이 端末에 편중

- 端末은 網에 항상 연결된 상태(Always On)에 있으나, 서로는 잘 모르는 관계
- '網은 지능이 낮아 端末이 쓰는 서비스 내용을 모른다'

낮은 網 지능, 높은 端末 지능



단말간에 직접 협상-제어 수행



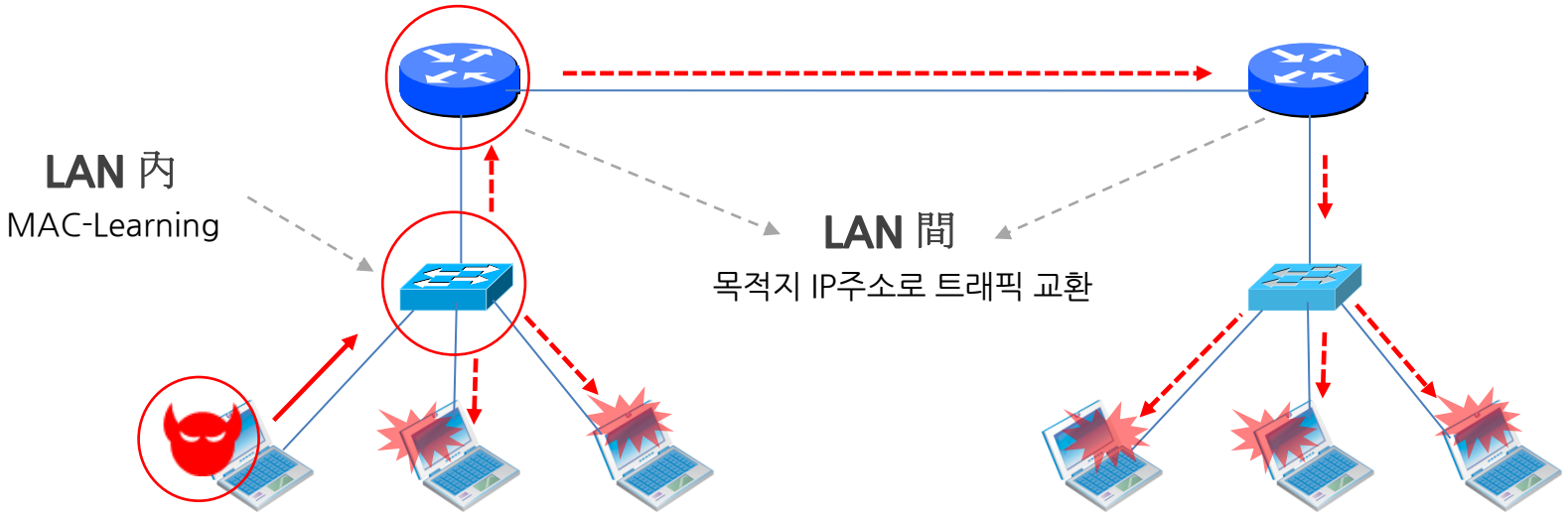
End-to-End Principal

- End Node 상호간 직접 서비스 협상 · 제어를 수행

주소 정보가 쉽게 노출(Open)

LAN 취약점 * Router 취약점 => 취약점 증폭 : LAN (공유 매체) * Router (공유 경로)

- LAN에는 이웃 단말의 주소가 방송으로 들리고, Router는 악성코드 트래픽 여부를 판단하지 못한다.



• LAN 內 : 단말 상호간의 MAC 주소를 방송으로 알린다 → 누구에게나 들린다!

• LAN 間 : 목적지 IP 주소로만 교환 여부를 결정된다 → 너무 간단하게 악성코드가 퍼진다!

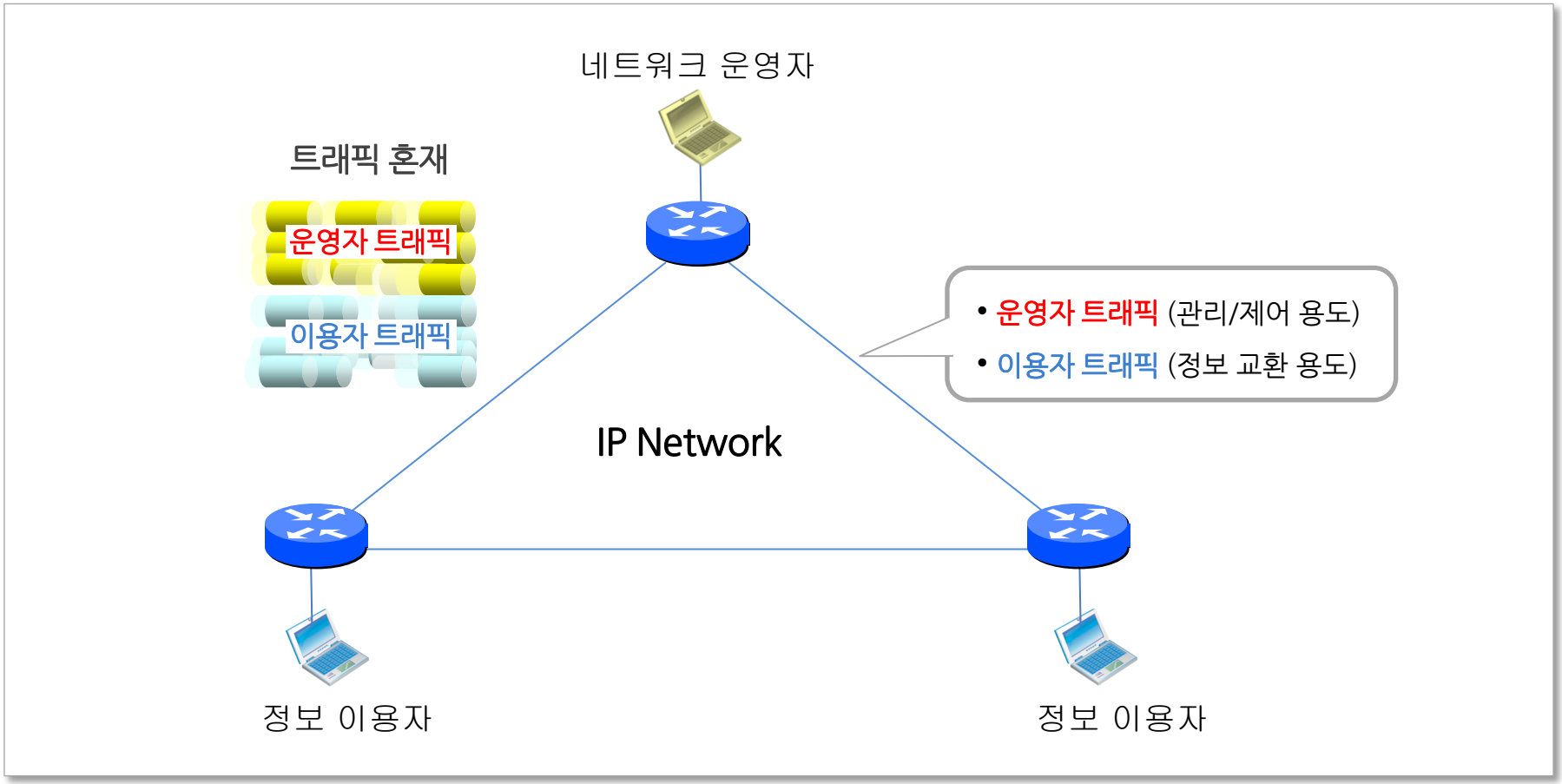
취약점 증폭 현상 => 누구나 이웃의 주소를 엿들을 수 있고 악성코드가 쉽게 퍼진다!

2016 CST Proprietary

속성이 다른 트래픽이 혼재

관리/제어 용도의 트래픽이 쉽게 노출

- Management/Control Plane Traffic : 네트워크 관리/제어 용도의 트래픽
- User Data Plane Traffic : 이용자 단말 간에 정보 교환 용도의 트래픽
  - **네트워크 관리/제어를 위한 운영자 용도의 트래픽을 이용자가 쉽게 볼 수 있다.**

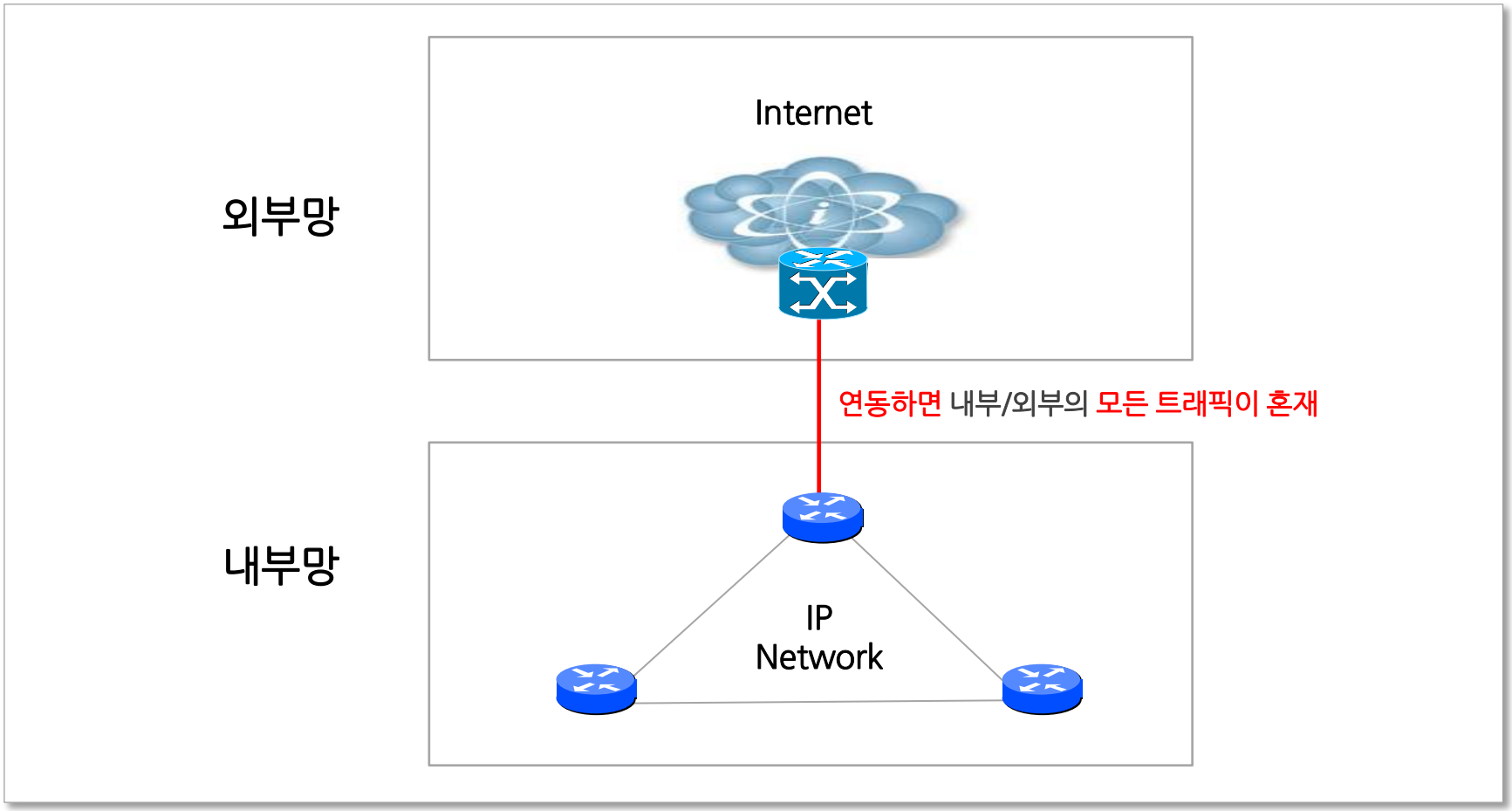


2016 CST Proprietary

내부와 외부의 불완전한 분리

내부와 외부 라우팅 영역(Routing Domain)의 손쉬운 결합

- 내부망과 외부망을 물리적으로 분리하여 구성한 경우도, 서로 연동하면 라우팅 영역이 결합됨
  - 결합된 라우팅 영역에는 내부/외부의 모든 트래픽이 혼재할 수 있고, 트래픽 속성을 식별하는 기능은 없다.

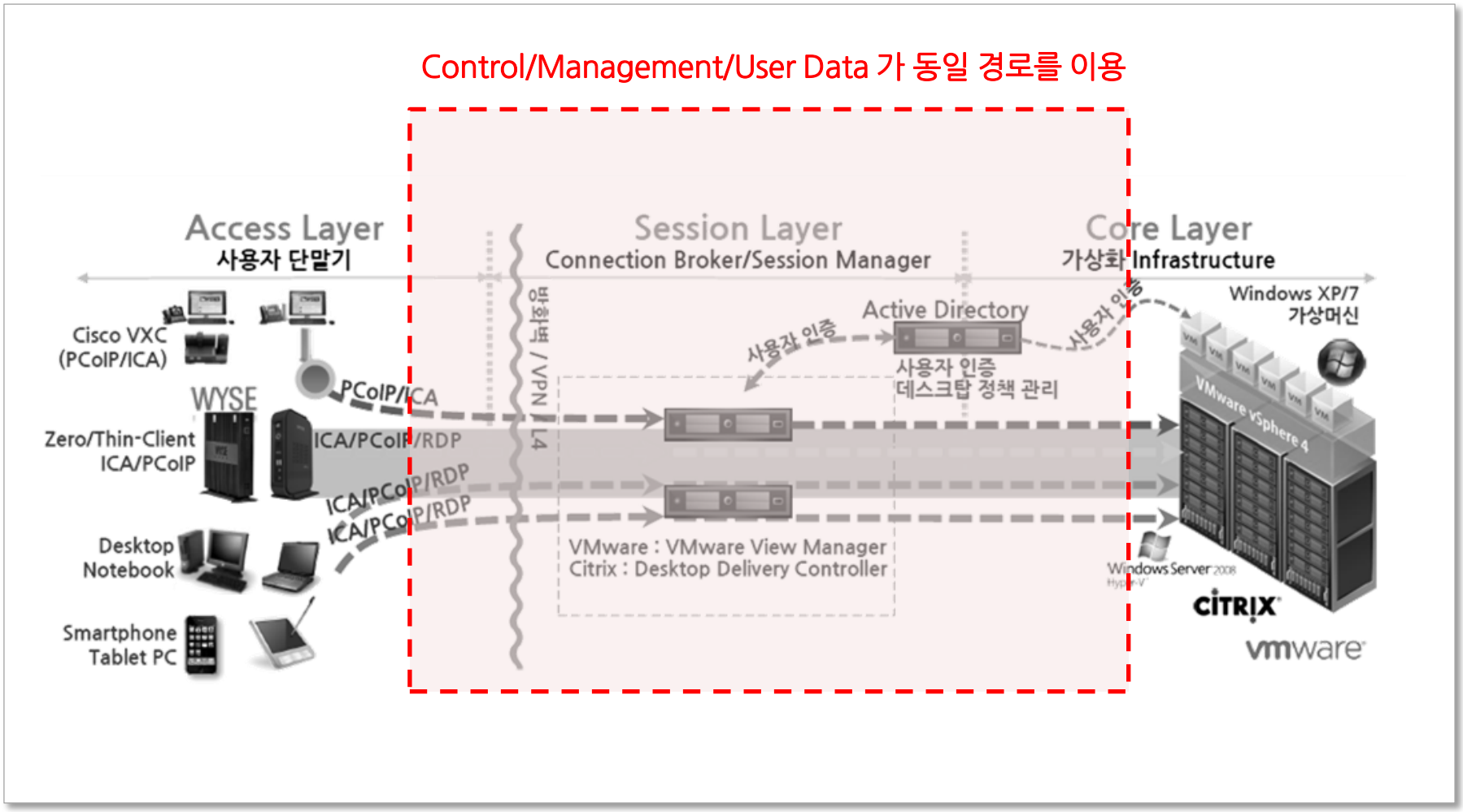


2016 CST Proprietary

불안전한 내부망 분리(1/2)

Server-based 망분리 경우도 여러 트래픽이 혼재

◆ 서버 기반(SBC)의 논리적 망분리를 실시한 경우에도 관리/제어 트래픽이 이용자 트래픽과 여전히 혼재된다.

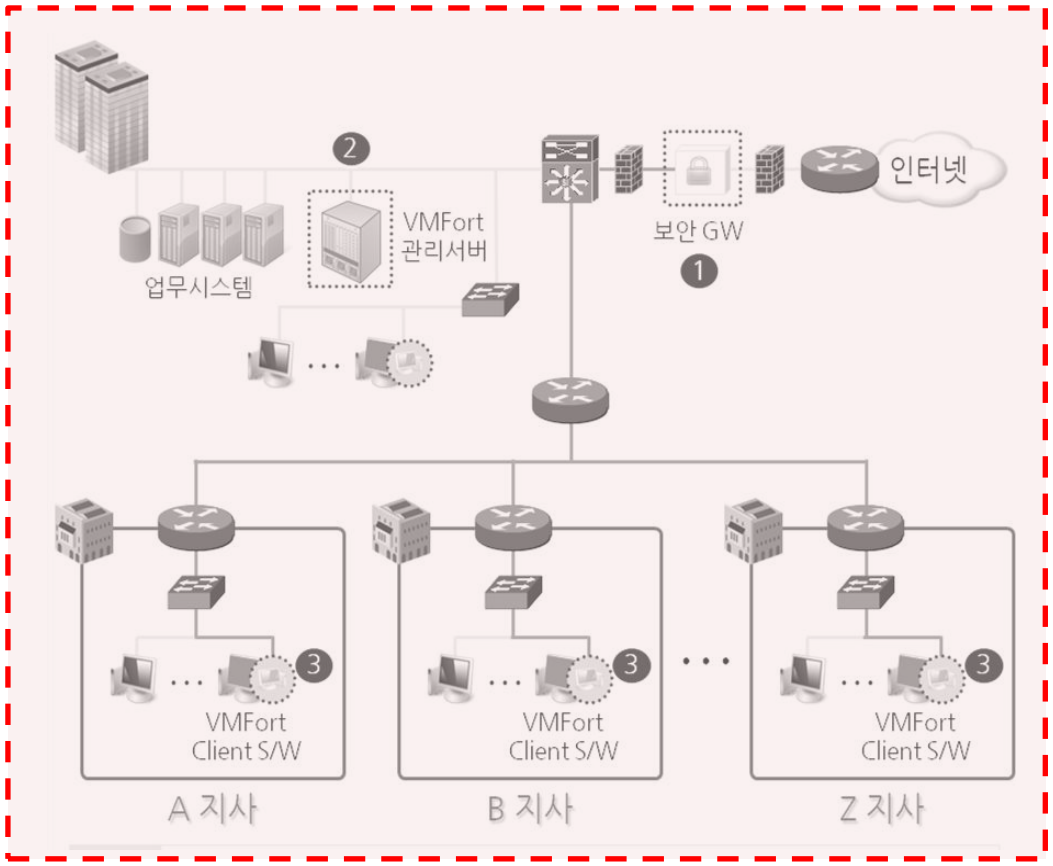


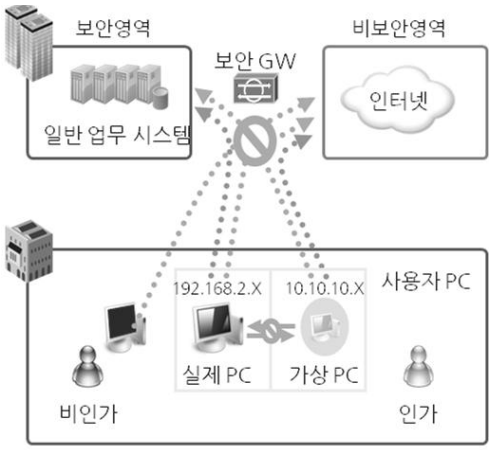
불안전한 내부망 분리(2/2)

Client-based 망분리 경우도 여러 트래픽이 혼재

- 단말 기반(CBC)의 논리적 망분리를 실시한 경우에도 관리/제어 트래픽이 이용자 트래픽과 여전히 혼재된다.

Control/Management/User Data 가 동일 경로를 이용

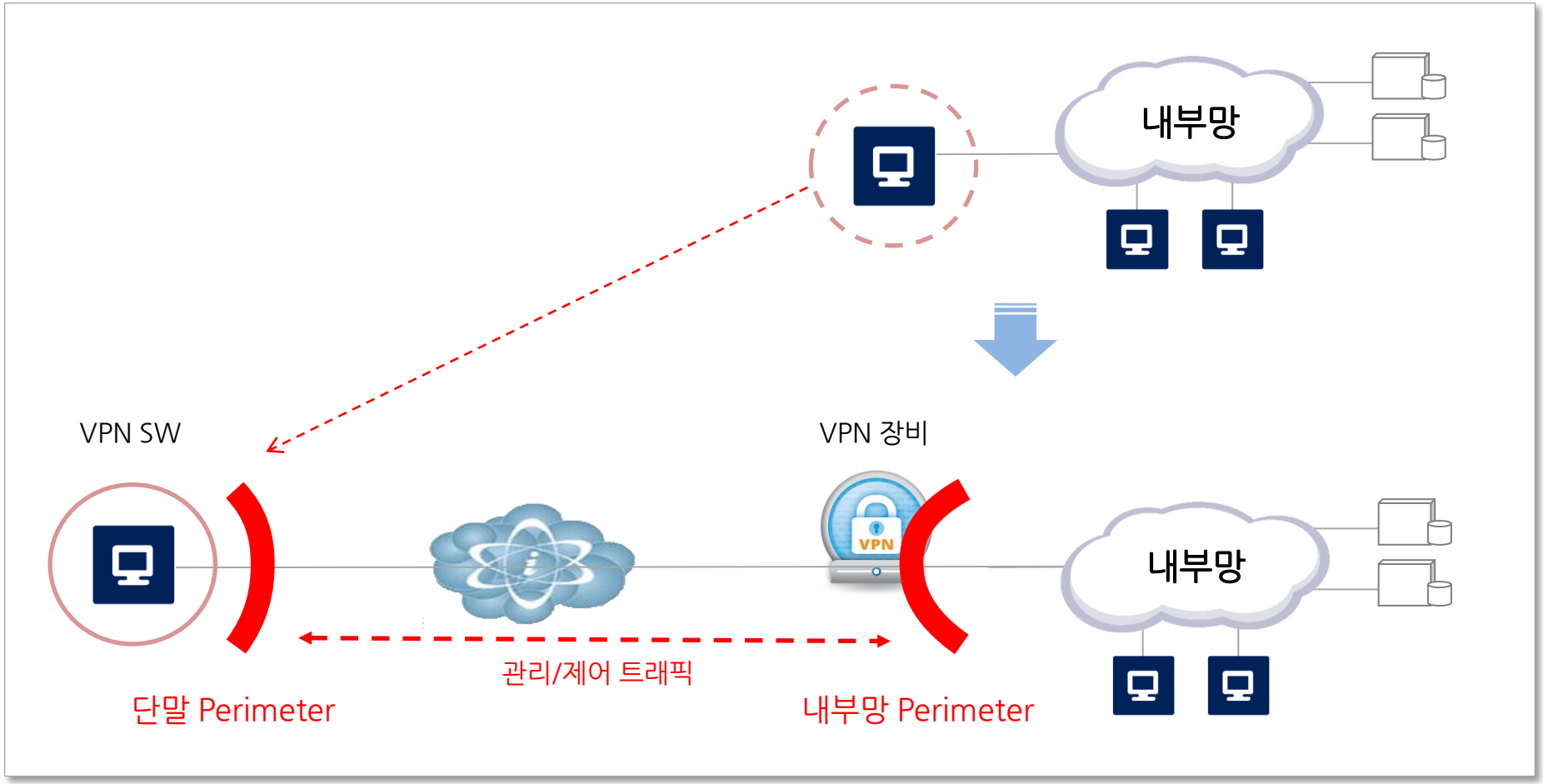




기존 VPN의 불완전한 경계

인터넷에 관리/제어 정보가 노출

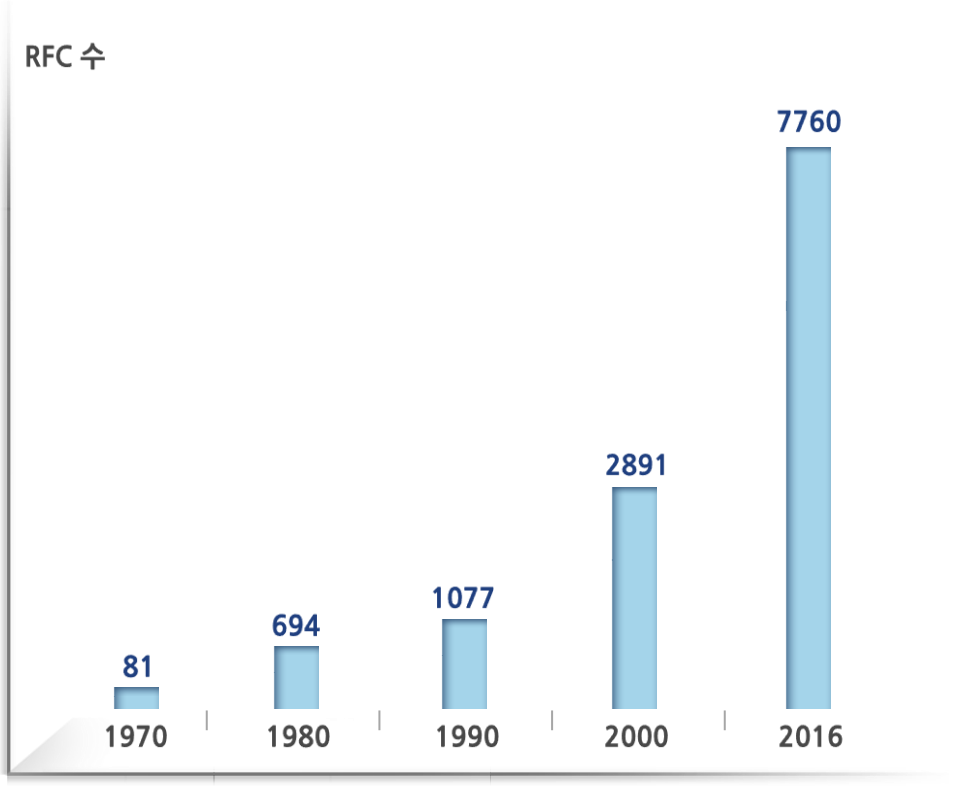
- 인터넷에서 사내망 접속을 제공하는 경우에 인증, VPN Tunnel, 암호화, 방화벽 구성 등이 필요
  - VPN장비는, 단말이 인터넷과 경계를 갖고 내부망이 인터넷과 경계를 갖도록 구성하는 기능을 수행하지만, 이 경우에도 VPN 관리/제어 트래픽이 인터넷에서 노출된다.



복잡하게 변한 IP망

- 새로운 유형의 접속 요구가 발생하면 **전반적인 장비의 조작 및 메커니즘 업데이트가 필요**
  - 탄생 초기에 대비하여 규격의 개수가 약 100배에 육박
  - 장비 발주 요구명세서 5천 500개
  - 소스코드 1천만 라인

IP Protocol 제정 추이 (IETF)



- "시스코나 주니퍼같은 회사는 SDN 시장에 대응하기 위해 기존 제품의 SW를 업그레이드하는데요. 이들 장비의 기능은 **발주 요구명세서 기준 5천500개** 정도예요. **소스코드만 1천만 줄을** 넘어요. 여기에 SDN 기능을 더하려면 그 소스코드를 여기저기 고치느라 많은 인력, 비용, 시간이 들죠. 반면 신생 벤처들은 처음부터 그런 기능에 초점을 맞춘 기술을 개발합니다. 더 적은 리소스로 더 빨리 대응할 수 있는 거죠."

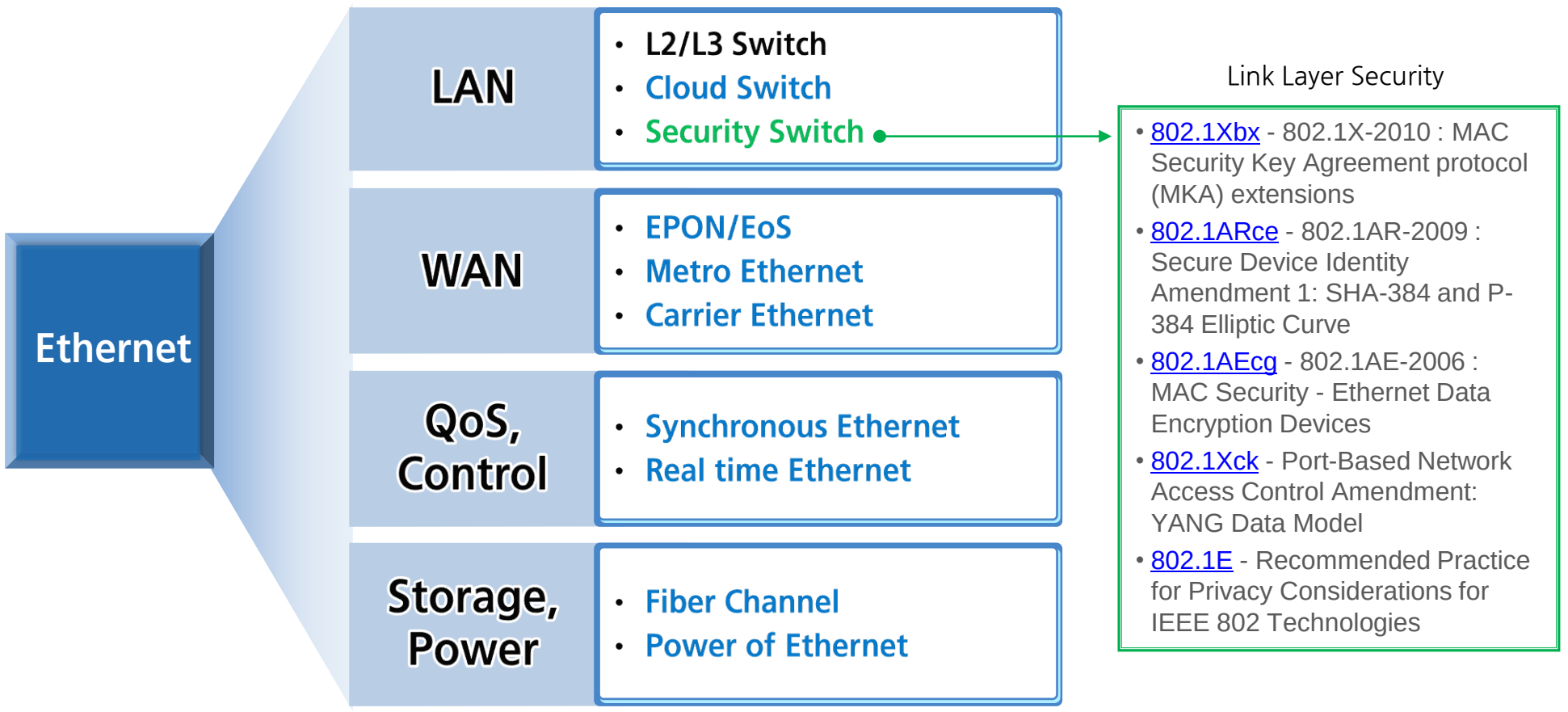
-SDN 개발회사 -

* RFC(Request For Comments) : 인터넷에서 기술을 구현하는 데에 필요한 절차 등을 제공하는 공문서로 IETF(Internet Engineering Task Force)에서 간행함

2016 CST Proprietary

LAN의 보안

- Ethernet은 경제성, 호환성, 투자보호 (Price, Backward Compatibility, Future Safe) 측면에서 강점을 갖는 기술로 새로운 용도에 확대 적용되고 있으며 보안 기능을 갖춘 스위치로 발전



2016 CST Proprietary

OS - LAN - IP의 취약성

사후 방어체계 (침해의 90%가 선제적 대응에 한계)

◆ 개별 장비로 사후 방어하는 현재의 대응체계로는 조직화/지능화된 사이버 테러 대응에 한계가 발생한다.

개방형 OS ·미디어 ·네트워크를 이용하는 환경

개방형 OS의 취약성

개방형
디바이스 OS

LAN의 취약성 (공유)

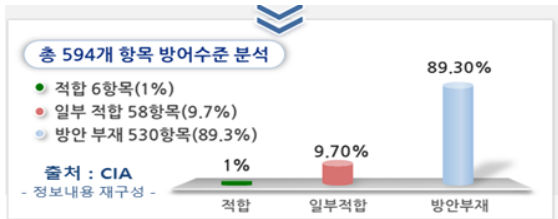
공유형
접속 미디어

IP의 취약성 (비연결)

비연결형
네트워크

침해 유형

		현행 솔루션																					
		AV	방화벽	IPS	취약점 모니터링	Remote Access VPN	파일 무결성 모니터링	Application Whitelist	802.1x	Encrypt at rest	Encrypt in motion	MFA	DB 접속 모니터링	웹방화벽	Privileged Access Mgmt	SIEM	DLP	WiFi IPS	Honey token	DNS Sinkhole	Web Incerse Proxy	Telco Ddos service	Not Running at Admin
인터넷 서비스	DoS																					Maybe	
	인증서 피싱																						
	비밀번호 추측											YES			Maybe	Maybe							
	OS&앱 취약점 공격		Maybe	Maybe	Maybe		Maybe	Maybe															Maybe
	SQLi/코드 주입 공격												Maybe	Maybe									
	교차 사이트 스크립팅(XSS)												Maybe	Maybe									
	사이트간 위조요청																						
보안 취약 특성	페이로드를 통한 피싱	Maybe		Maybe	Maybe		Maybe	Maybe															Maybe
	드로퍼/익스플로이트 피싱	Maybe		Maybe	Maybe		Maybe	Maybe												Maybe			Maybe
	자바스크립트 취약점			Maybe												Maybe				Maybe			
	브라우저 조작							Maybe															
	WiFi의 중간자 공격					YES					YES												
	이더넷의 부정사용자 공격		Maybe						YES									Maybe					
	DNS 스프핑																						
	전자인증서 취약점 공격																						
내부 운영의 취약	네트워크 스캐닝		Maybe	Maybe																			
	패스 더 해쉬															Maybe							
	패스 더 티켓																						
	패스워드 크래킹														Maybe								
	OS&앱 취약점 공격		Maybe	Maybe	Maybe		Maybe	Maybe															Maybe
	SQLi/코드 주입 공격												Maybe	Maybe									
	교차 사이트 스크립팅(XSS)												Maybe	Maybe									
	디렉토리 접근공격													Maybe									
	백업서버 공격		Maybe							YES													
	ARP 스푸핑			Maybe							YES												
	키보드 입력정보, 화면 탈취							Maybe															
	악의적 내부 사용자			Maybe						Maybe			Maybe		Maybe	Maybe	Maybe		Maybe				

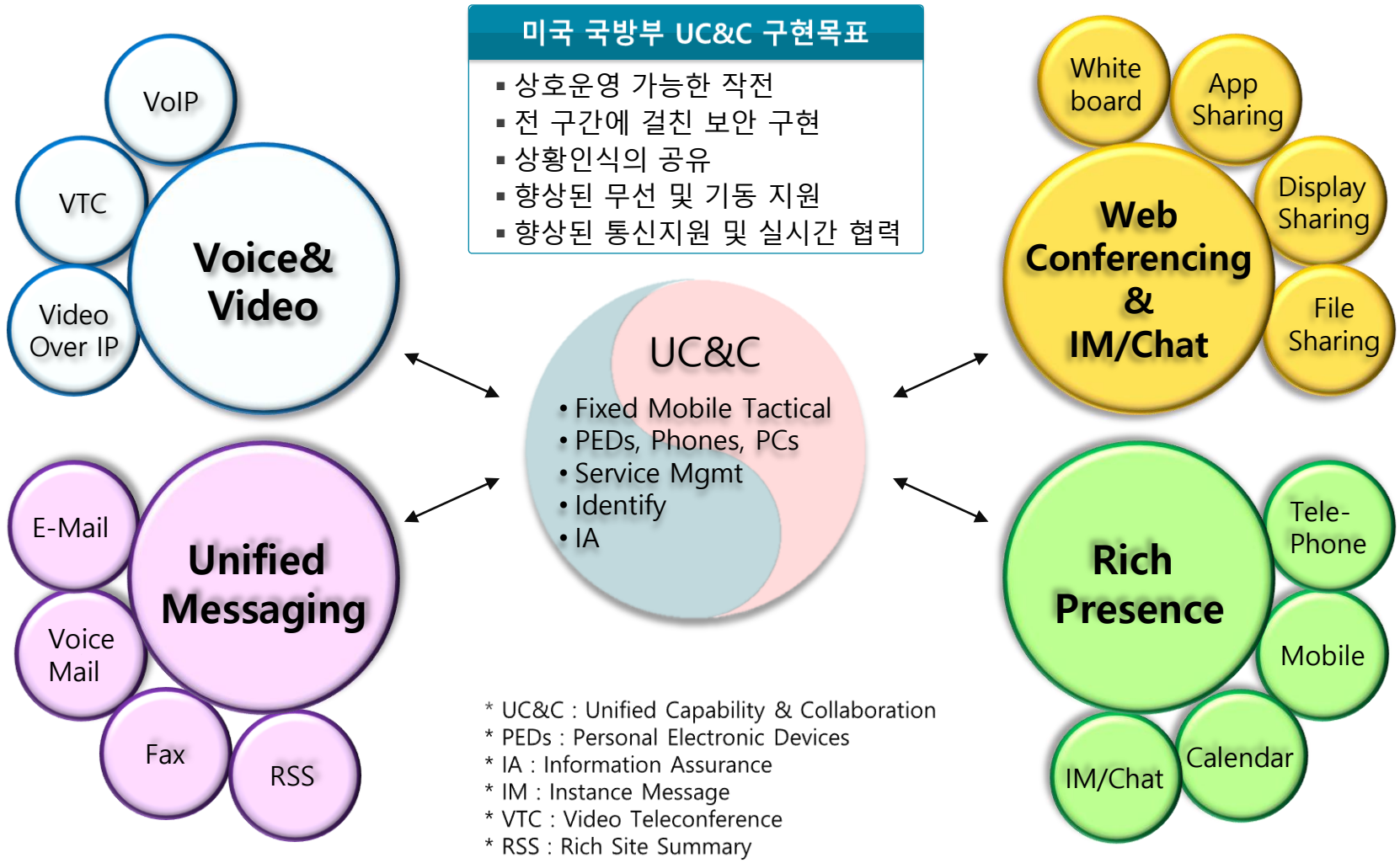


II. 동향과 요건

- 새로운 환경
- 진화의 방향
- 구현 요건

통합 능력과 협업(UC&C) 환경

- 기술에 구애 없이 상호 운영되고 가용성과 보안성을 보장하는 IP 네트워크 인프라로 음성, 영상, 데이터가 통합된 서비스를 언제 어디서나 이용하는 환경을 제공



2016 CST Proprietary

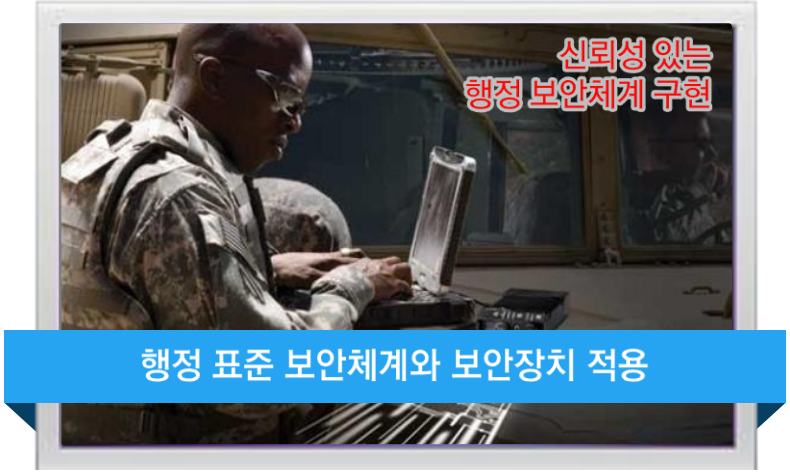
네트워크 환경의 변화

- 모바일 정보 이용 요구의 폭발적 증가, 보안의 중요성 증대로 선제적으로 침해공격을 방어하고 어디서든 실시간 고속의 고신뢰 접속을 보장하는 네트워크 환경 요구

이상 징후 탐지, 침입자 격리, Network운영 지속

도메인 체계에 관계없이 네트워크 보호작업 수행

상용 스마트단말을 활용한 행정의 보안 통신



행정 표준 보안체계와 보안장치 적용

2016 CST Proprietary

서비스 환경의 변화

- 기술에 구애 없이 상호 운영되고 가용성과 보안성을 보장하는 IP 네트워크 인프라로 데이터, 음성, 영상이 통합된 서비스를 5-Any (시간, 장소, 매체, 정보, 사람) 방식으로 자동 인식하여 이용하는 환경을 제공

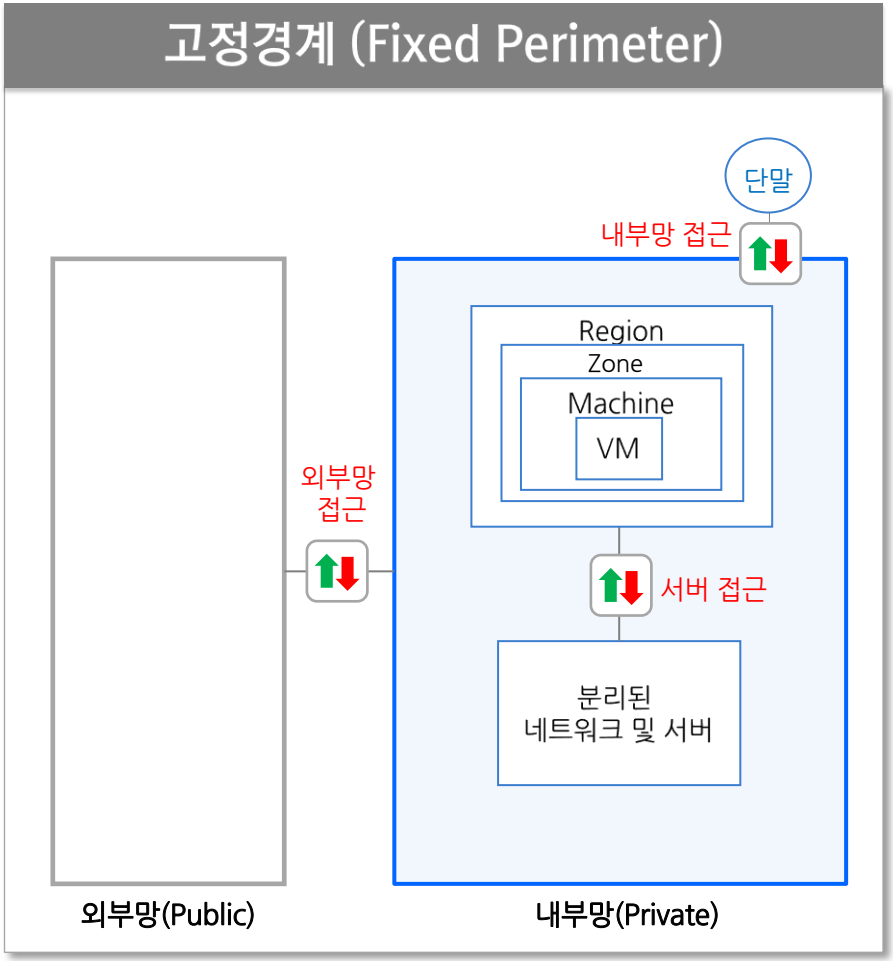
* UC&C : Unified Capability & Collaboration (통합능력과 협업)

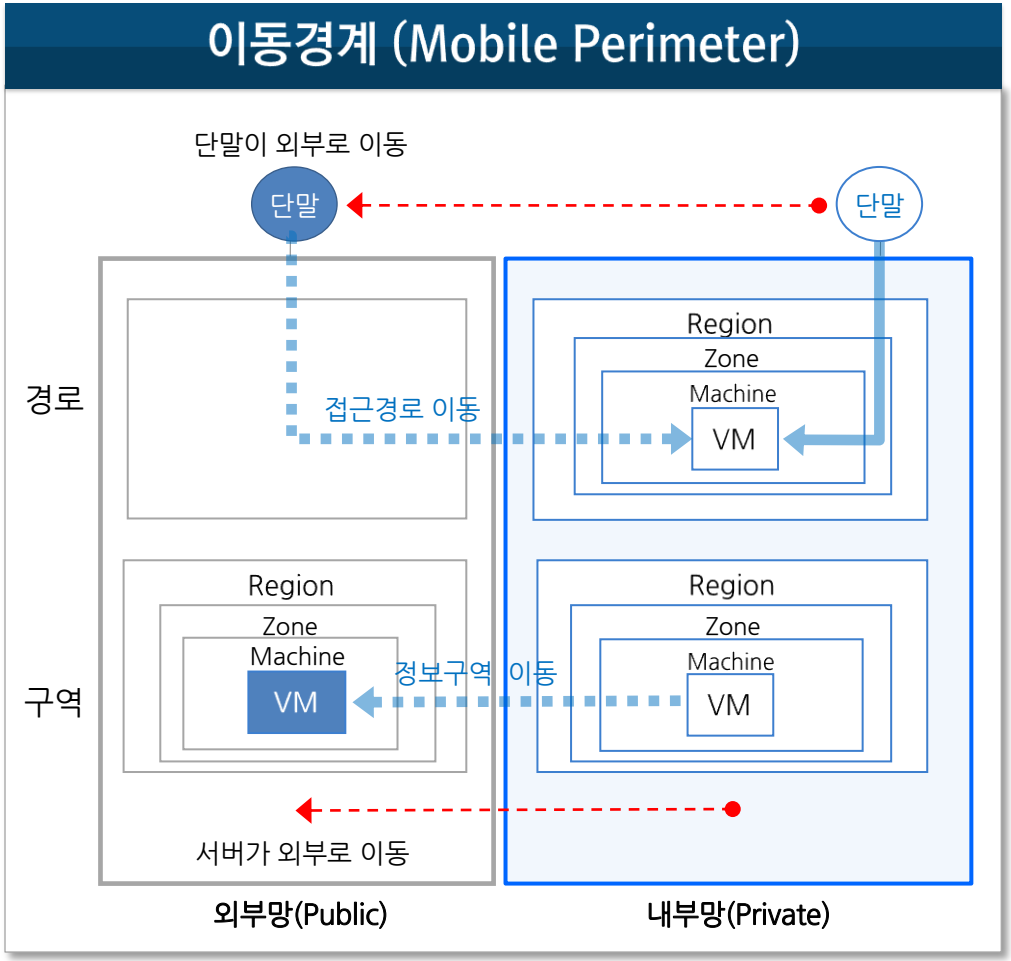
2016 CST Proprietary

정보보호 환경의 변화

- 기존 보안은 물리적으로 고정된 경계(Fixed Perimeter) 영역으로 출입하는 지점에서만 통제

- "단말/서버 등이 이동하는 환경에서는 이동경계(Mobile Perimeter) 영역으로 출입을 통제할 수 있는 새로운 보호개념이 필요하다. "CSA Software Defined Perimeter WG, Vidder 등)

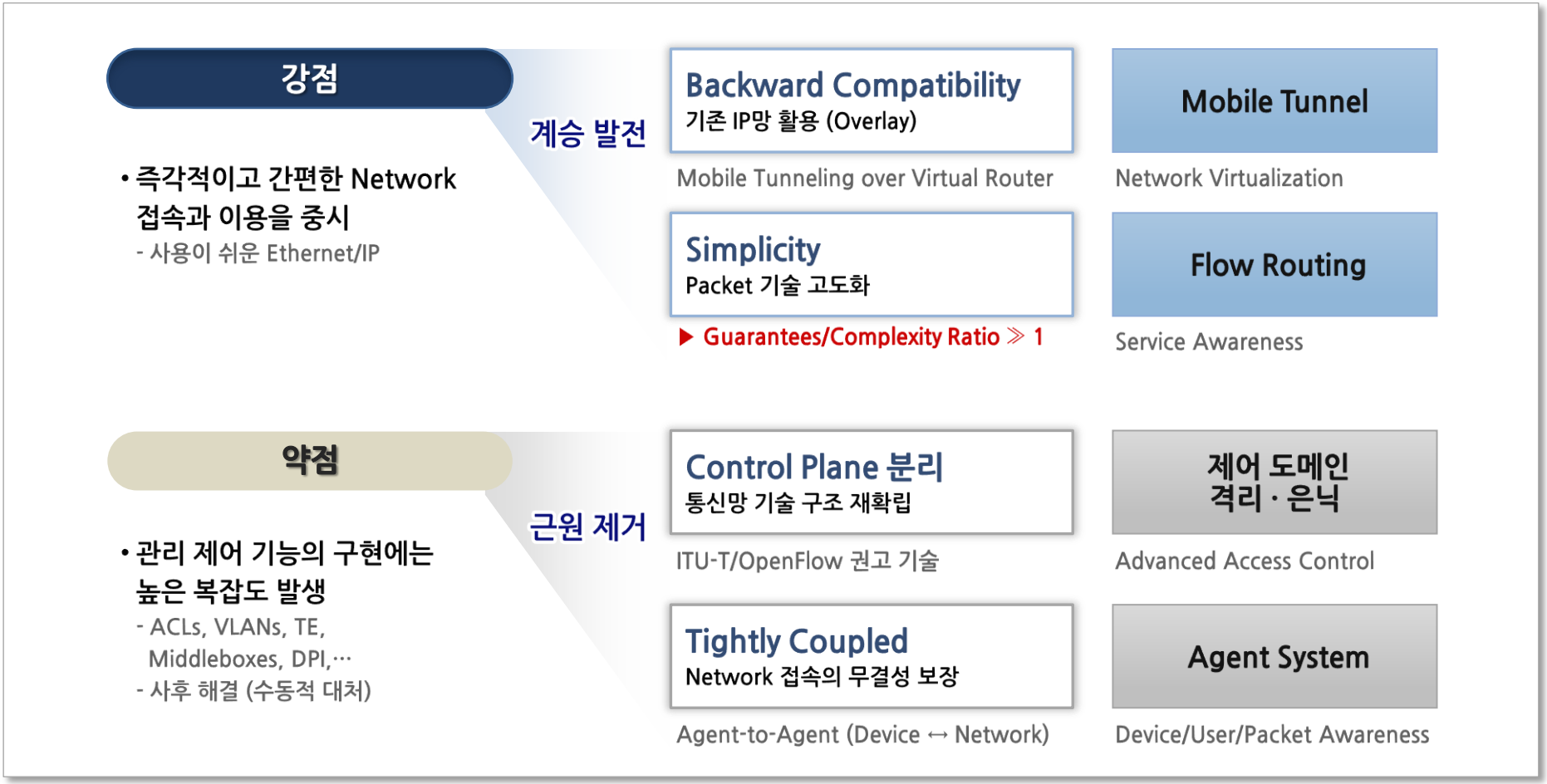




2016 CST Proprietary

IP망 기술 전략

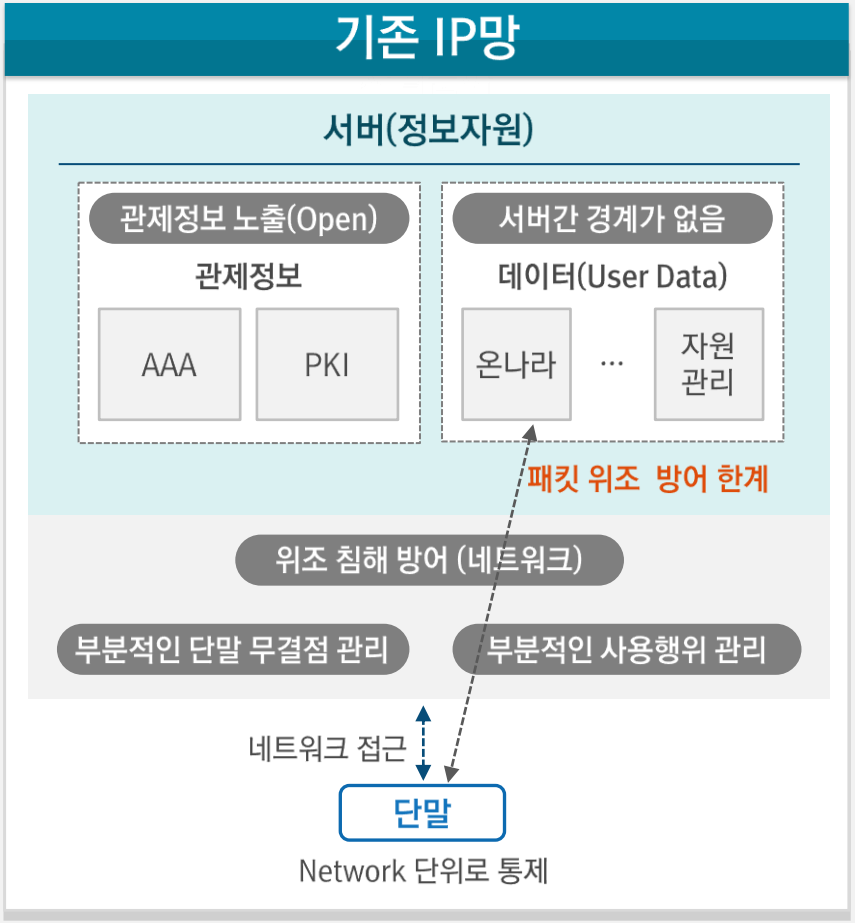
- 기존 IP망의 강점을 계승하고 약점은 근원적으로 제거
  - 강점 : 누구나 항상 연결할 수 있고 간편하게 이용된다.
  - 약점 : CPND 전반에 걸쳐 관리/제어 기능을 빠르고 지속적으로 보강하여야 한다.



2016 CST Proprietary

단말마다 경호원과 전용선(터널) 할당

- 정보자원의 보호구역과 경계선을 지정하고(인가 前), 접근하는 사용자-단말의 무결성을 검증하여 지정된 보호구역으로만 접근을 인가하며(인가 中), 접근인가 이후에는 비정상적인 행위를 탐지하고 관리(인가 後) 하는 全주기에 걸친 선제적인 침해대응이 필요

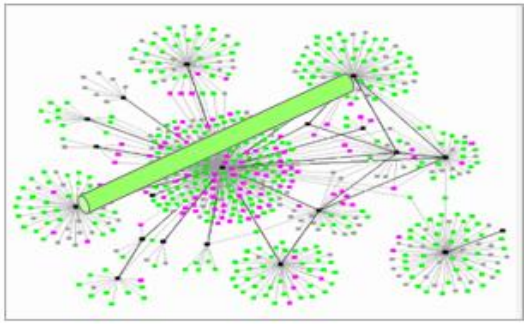


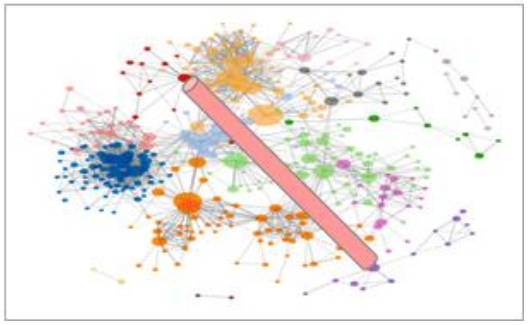
터널과 IP터널

- IP 터널(인터넷 터널)은 기존 네트워크 도메인의 라우팅 정책에 간섭을 받지 않고 우회하여 보안(Security), 연동(Interworking), 가상(Virtualization), 중첩(Overlay), 분할(Segmentation), 이동(Mobility) 등의 목적에 부합하는 경로를 새롭게 구성하는 기술
  - 터널링(Tunneling)은 새로운 네트워크 도메인 라우팅 정책에 부합되도록 패킷의 라우팅 헤더를 캡슐화(Encapsulation)하여 추가하거나 새로운 정책에 부합하도록 헤더를 변환(Translation)
  - IP 터널의 입구지점과 출구지점을 임의로 지정하면 트래픽이 IP 터널 입구로 들어갈 때 새로운 IP헤더가 구성되고 IP헤더는 터널 통과 후 출구에서는 원래의 IP헤더로 복원

교통 터널

인터넷 터널



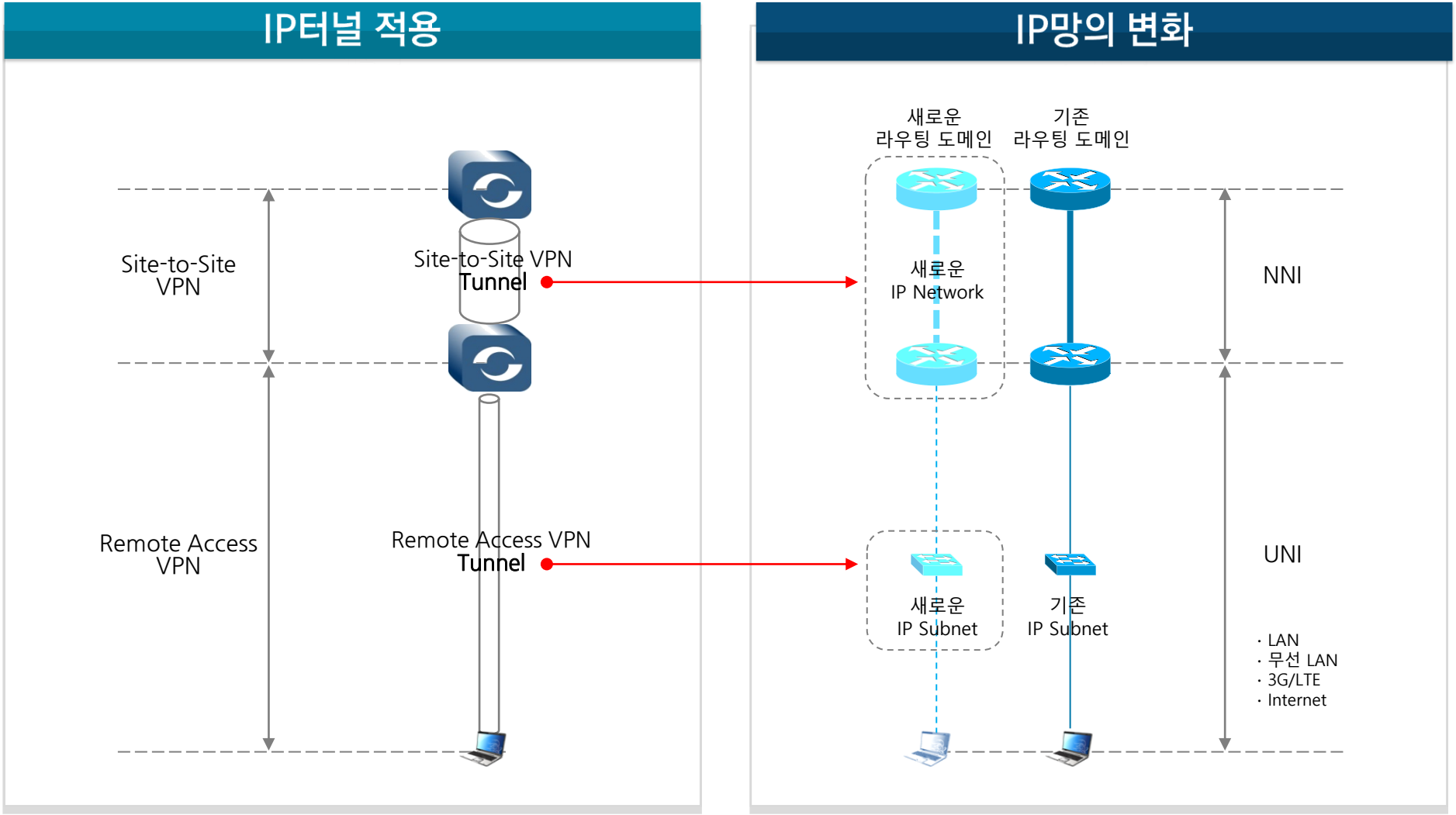


- 터널로 트래픽을 전달하면 측정(Measure), 보고(Report), 검증(Verify) 등에 효율적
- 라우팅 정책에 따라 원하는 트래픽을 발신지 주소, 발신지 서비스 번호, 수신지 주소, 수신지 서비스 번호, 서비스 속성 등의 값으로 지정하면 터널로 유입되어 터널 출구로 자동 전달
- VPN은 2가지 기본적인 요소로 구성
  - 터널링으로 VPN의 “Virtual”을 담당
  - 개인 또는 기관의 VPN데이터 보호
- “Virtual”은 조직의 요구에 따라 동적으로 VPN을 개설하는 것으로 전용선을 개설하는 것과는 달리 항상 연결되어 있지 않고 필요한 경우에만 연결하여 사용하여 효율적

2016 CST Proprietary

IP터널의 기능

- Remote Access VPN Tunnel은 새로운 IP Subnet을 생성
- Site-to-Site VPN Tunnel은 새로운 IP Network(라우터 및 라우팅 도메인)을 생성

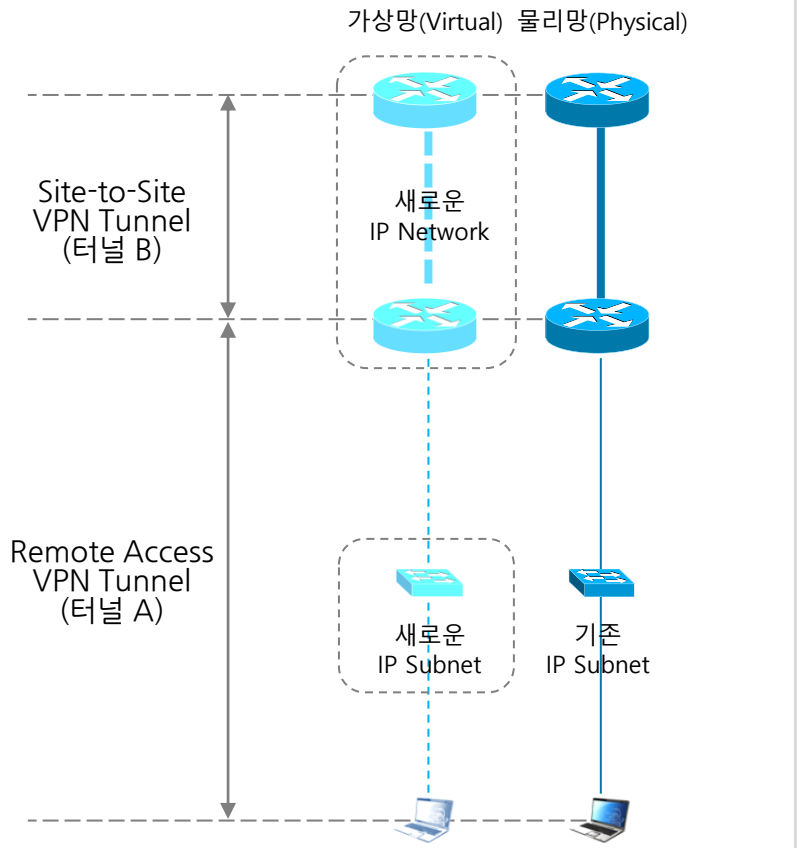


NNI : Network to Network Interface
UNI : User Network Interface

IP터널의 고려사항

- IP터널은 가상 서킷(Virtual Circuit*)의 속성을 갖추어야하고 안전하고 효율성 있는 네트워크 구성을 제공할 수 있어야 함

IP VPN



* a VPN is a network of virtual circuits for carrying private traffic
* Tunnels : The "Virtual" in VPN(reference : Building and Managing Virtual Private Networks by Dave Kosiur)

IP터널의 요건

▶ 터널은 새로운 IP주소가 필요
- 단말별로 물리망 IP주소와 더불어 가상망 IP주소 필요

▶ 터널의 IP주소의 선정 옵션
- 물리망에 있는 물리라우터의 기존 IP Subnet 주소 대역 사용
- 물라망에 있는 물리라우터의 새로운 IP Subnet 주소 대역 사용
- **가상망에 있는 가상라우터의 IP Subnet 주소 대역 사용**

▶ 터널 A와 터널 B의 연동 옵션
- 터널 A와 터널 B가 연동 없이 사용
- 터널 A가 터널 B에서 종단되어 터널 B를 사용
- **터널 A가 터널 B와 연동되어 터널 B를 경유(Tunnel-in-Tunnel)**

▶ 터널은 가상 서킷이다(Tunnel is Virtual Circuit). 따라서
- 가상 경로(Virtualization) 제공,
- **안전한 경로(Security) 보장,**
- **대역 할당(Bandwidth) 지원,**
- **이동성 (Mobility) 지원 등이 필요**

2016 CST Proprietary

IP터널의 요건(1/2)

- 인가된 단말에만 터널을 동적으로 제공하고 정보 이용의 품질과 모바일 서비스를 보장
- 가상 라우팅 도메인 별로 라우팅 정책을 부여하여 신뢰성, 확장성, 효율성 있는 망 구성을 지원

기존 IP터널의 속성

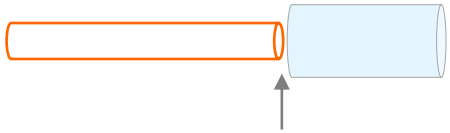
▶ 정적 구성(Permanent)

• Always-On
• Shared Path

▶ 이기종 터널 간의 연동

• Remote Access VPN Tunnel

• Site-to-Site VPN Tunnel

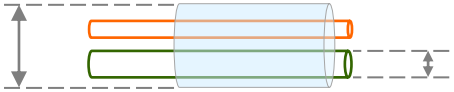


가상 서킷의 속성

▶ 동적 구성(Dynamic)

• On-Demand

▶ 대역 보장(Bandwidth)

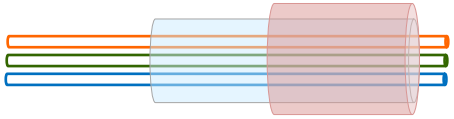


• Channel

▶ 이동(Mobility)

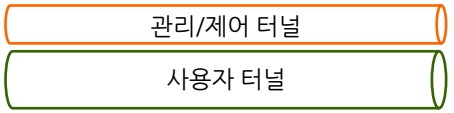
• Hand-Over

▶ 중첩(Overlay)



• Add Drop Multiplexing
• Aggregation

▶ 보안(Security)



• Out-of-Band Management & Control

IP터널의 요건(2/2)

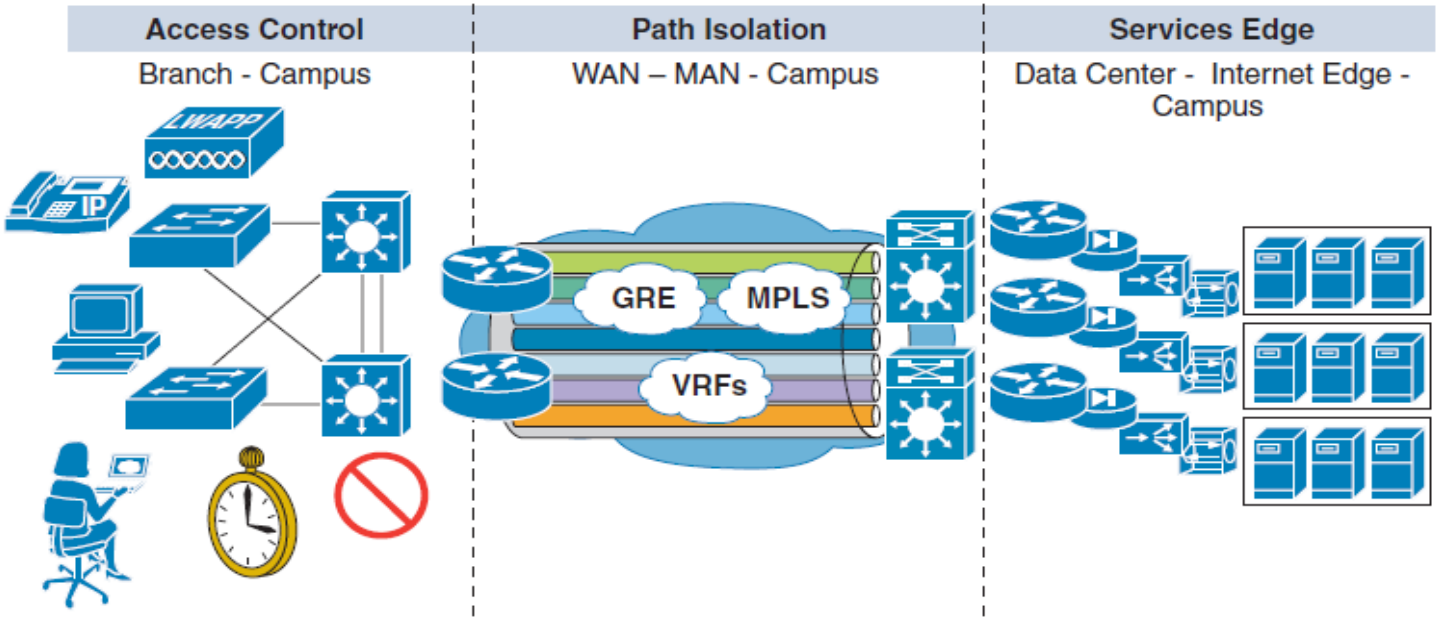
- (병행 운용) 기존 IP망의 주소, 보안 장비 등의 구성의 변경 없이 병행하여 운용 할 수 있어야 한다.
- (PBR기반 터널 설정) 단말로 부터 개설된 터널은 동일 라우팅 도메인에서 종단되거나 다른 라우팅 도메인에서도 종단될 수 있어야 한다.
- (동적 터널 연동) 터널은 새로운 라우팅 정책을 적용한 가상 라우팅 도메인과 동적으로 연동될 수 있어야 한다.
- (이종 터널 연동) 철도와 도로의 운송이 바로 연결되듯이 이종터널간의 연동을 지원하여야 하고, 철도 또는 도로의 운송 속성을 보장하여야 한다. 또한 원하는 지능형(품질, 이동성, 보안성 등) 속성을 추가적으로 정의할 수 있어야 한다.
- (단말 무결성 검증) 터널은 단말의 무결성 검증이 성공적으로 종료된 경우에만 개설되고 주기적으로 검증하여 사용 중에도 보안 요건을 충족하지 못할 경우에는 절단할 수 있어야 한다.
- (망 무결성 검증) 터널과 기존 경로를 혼용하여 라우팅 도메인을 구성할 수 없고 터널로만 구성된 라우팅 도메인을 만들어야 한다(All-Tunnel).
- (동적 상황 추적) 터널의 개설에서 부터 종료시점까지 전체 생애 주기를 추적 관리하고 제어할 수 있어야 한다.
- (정보 접근 제어) 인가 없이는 보이지도 알 수도 없는 기밀성(Confidentiality), 여러 요소가 체계적으로 빈틈이 없는 무결성(Integrity), 만족스럽게 안정적으로 동작하는 가용성(Availability)을 동시 제공하여 全주기(접근 인가 前단계, 인가 신청中, 인가 後단계)에 걸친 선제적으로 침해를 방어한다.

IP망에서 IP터널은 선택이 아닌 필수 기능!

2016 CST Proprietary

CISCO Framework

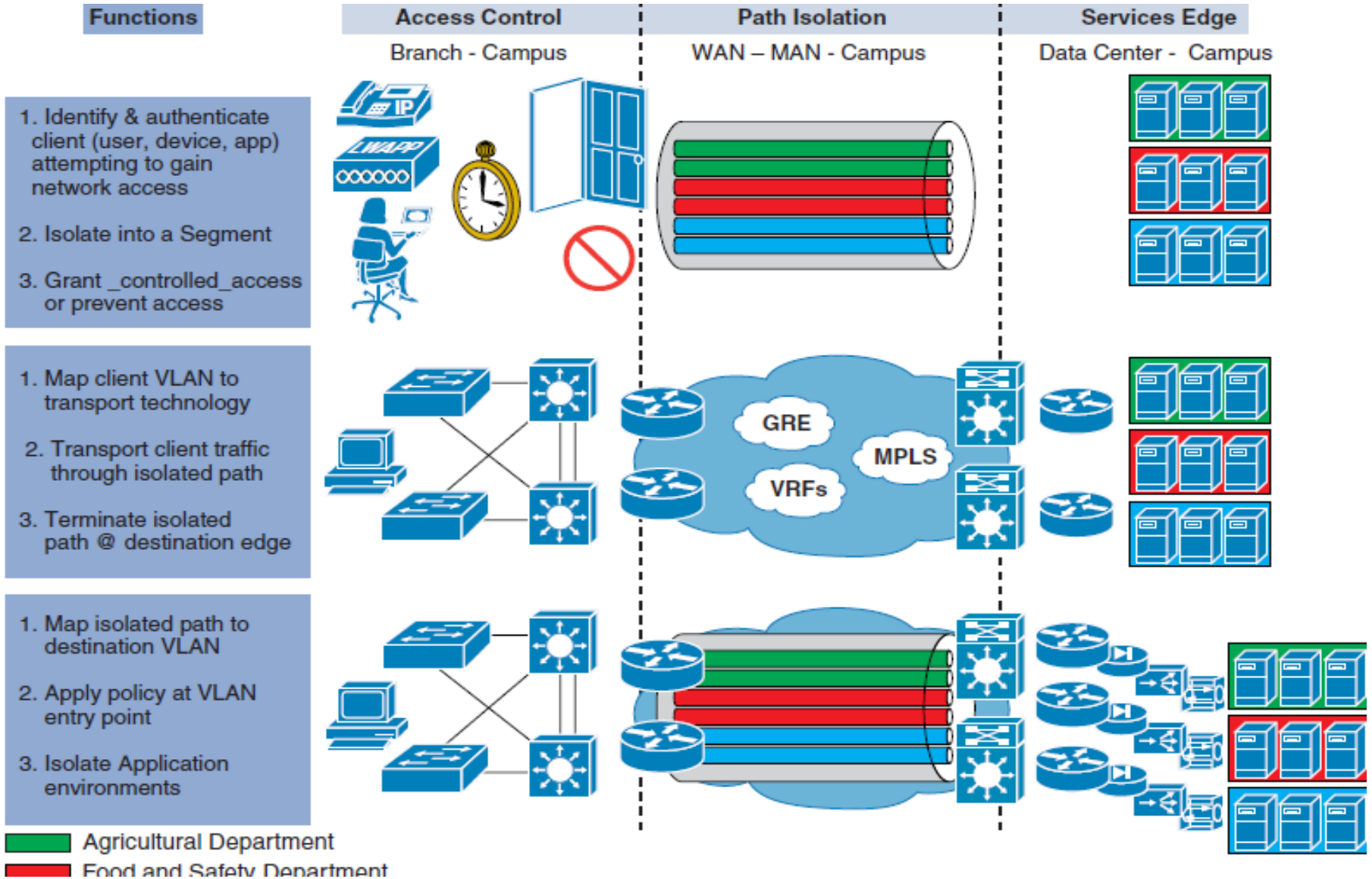
- Network Virtualization = Access Control + Path Isolation + Service Edge
  - 접근 제어: 인증 클라이언트(사용자, 단말, 앱)는 네트워크 접근, VLAN/ACL로 분리
  - 경로분리: L3 계위에서 분할하여 격리된 트래픽 전달
  - 서비스 제어: 이용유형(전용/공유 방식), 분할된 단위로 정책 적용



Functions	Authenticate client (user, device, app) attempting to gain network access Authorize client into a Partition (VLAN, ACL) Deny access to unauthorized clients	Maintain traffic partitioned over Layer 3 infrastructure Transport traffic over isolated Layer 3 partitions Map Layer 3 Isolated Path to VLANs in Access and Services Edge	Provide access to services: Shared Dedicated Apply policy per partition Isolated application environments if necessary

2016 CST Proprietary

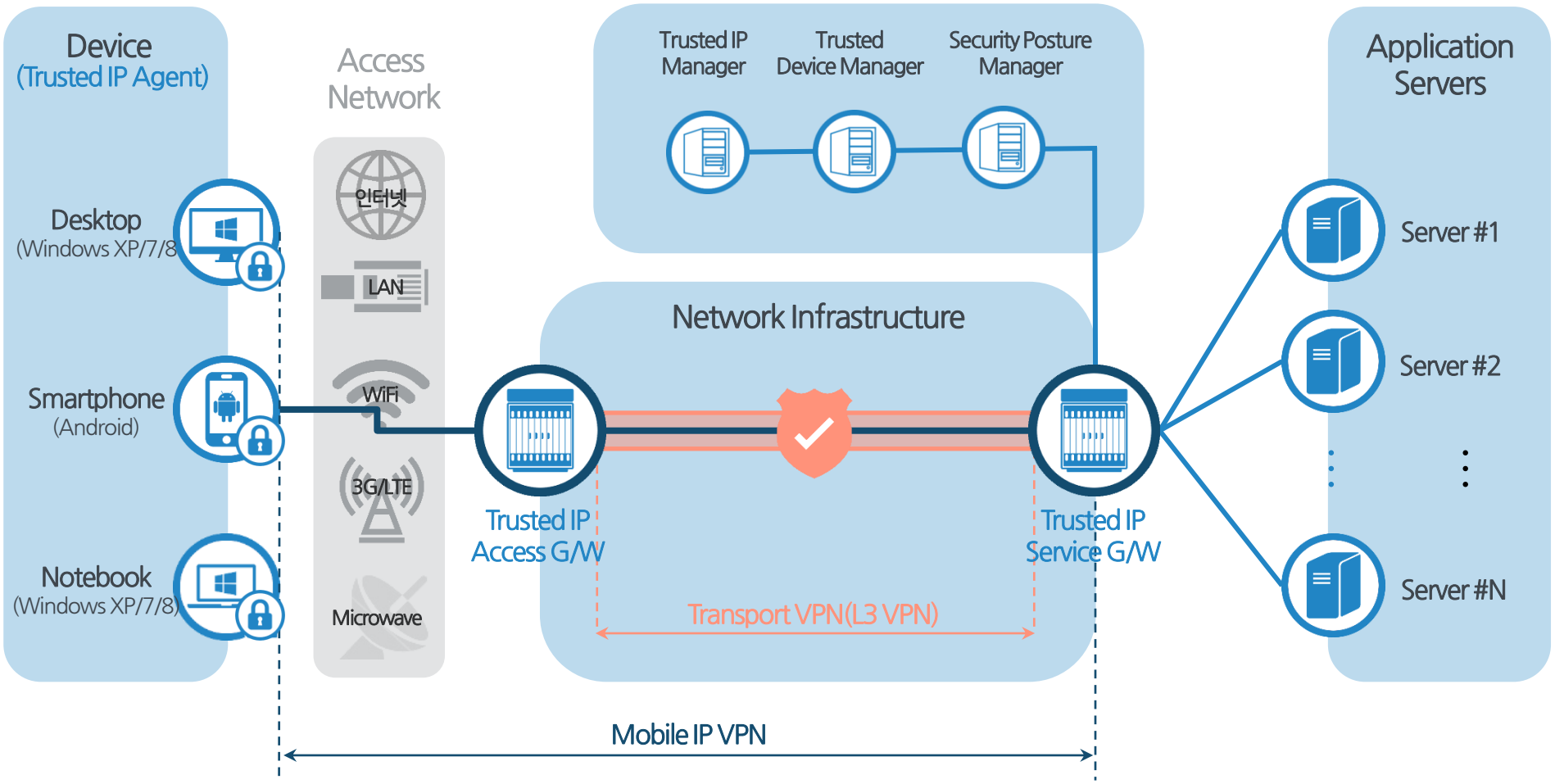
CISCO Framework



III. TIPN 시스템

- 시스템 구성
- 시스템 동작
- 시스템 기능
- Trusted WiFi
- 솔루션 적용 분야

시스템 구성


Device
(Trusted IP Agent)
Desktop
(Windows XP/7/8)
Smartphone
(Android)
Notebook
(Windows XP/7/8)
Access
Network
인터넷
LAN
WiFi
3G/LTE
Microwave
Trusted IP
Manager
Trusted
Device Manager
Security Posture
Manager
Network Infrastructure
Trusted IP
Access G/W
Trusted IP
Service G/W
Transport VPN(L3 VPN)
Application
Servers
Server #1
Server #2
Server #N
Mobile IP VPN

구성 요소

TIPN Gateway

Trusted IP Access Gateway

단말 집선 장소에 위치하여 인증 패킷을 통합 관제 네트워크에 올려주는 역할을 하며 가상 네트워크별 White List 기반 접근 통제

Trusted IP Service Gateway

서버 집합 장소에 위치하여 Trusted IP Access Gateway 와 연계하여 가상화된 네트워크를 네트워크 및 서버별로 접근 통제 및 관리 (터널 생성 및 종료)

Optional

IPSec VPN Device

- IKE Phase I / IKE Phase II
- 터널 모드 암호화/복호화 제공
  - ESP 프로토콜

IPSec Agent

Secure Container Agent

Secure Container Manager

- 단말 다운로드 파일 수정 및 관리
- 단말 파일 변경 실시간 감시

TIPN Manager / Agent

Trusted IP Manager

- 터널, 가상네트워크 구성 및 연동 관리
- 터널 및 가상경로 별 품질보장관리
- 인증 서버(AAA) 연계

Security Posture Manager

- 단말의 소프트웨어 이미지 관리
- Agent 이미지와 정상 상태의 이미지 비교
- 접속 인가 전단계 및 접속 중에도 수행

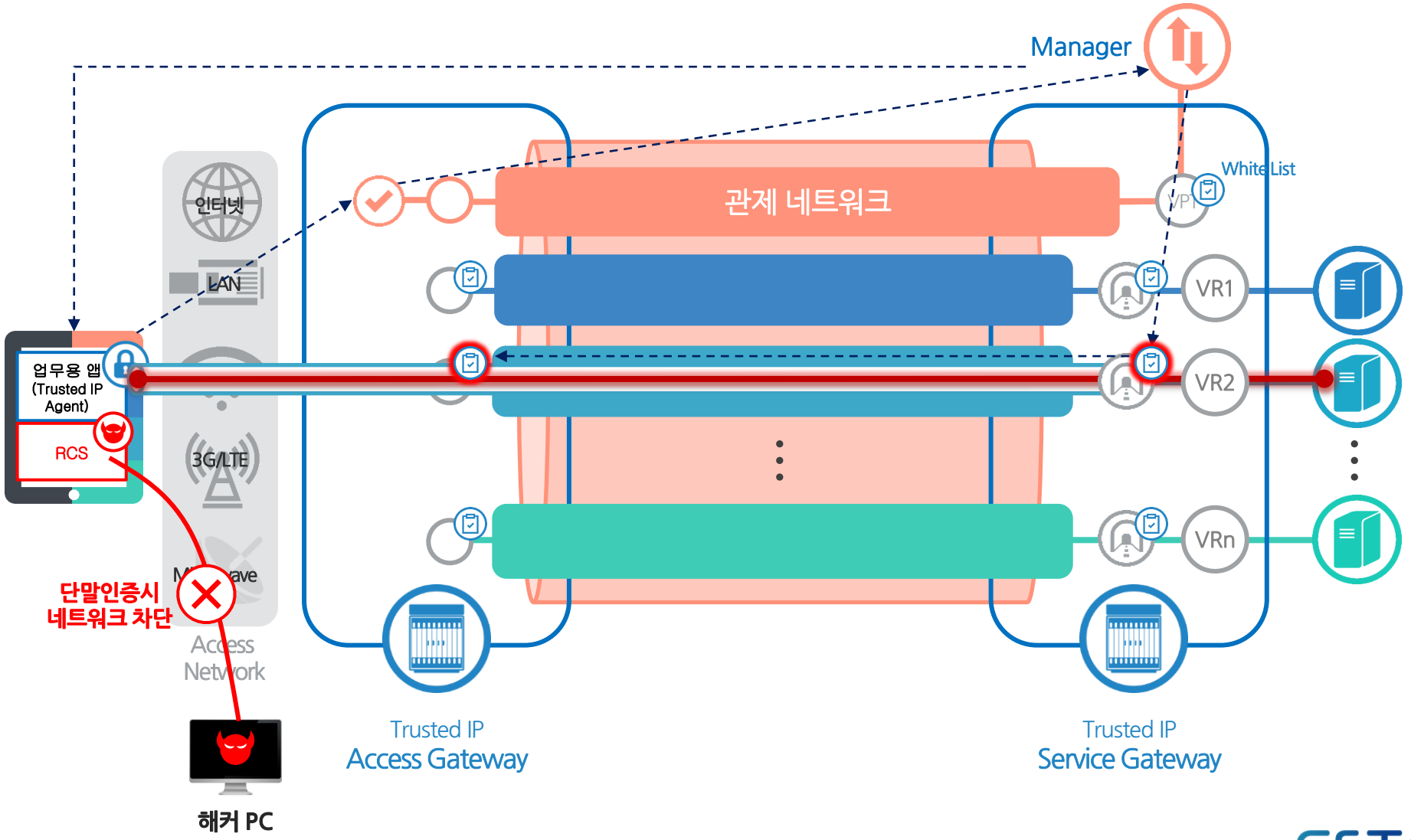
Trusted Device Manager

- 디바이스 관리 및 보안 정책 수행
- 디바이스의 인증/상태 관리
- 설치 소프트웨어 관리

2016 CST Proprietary

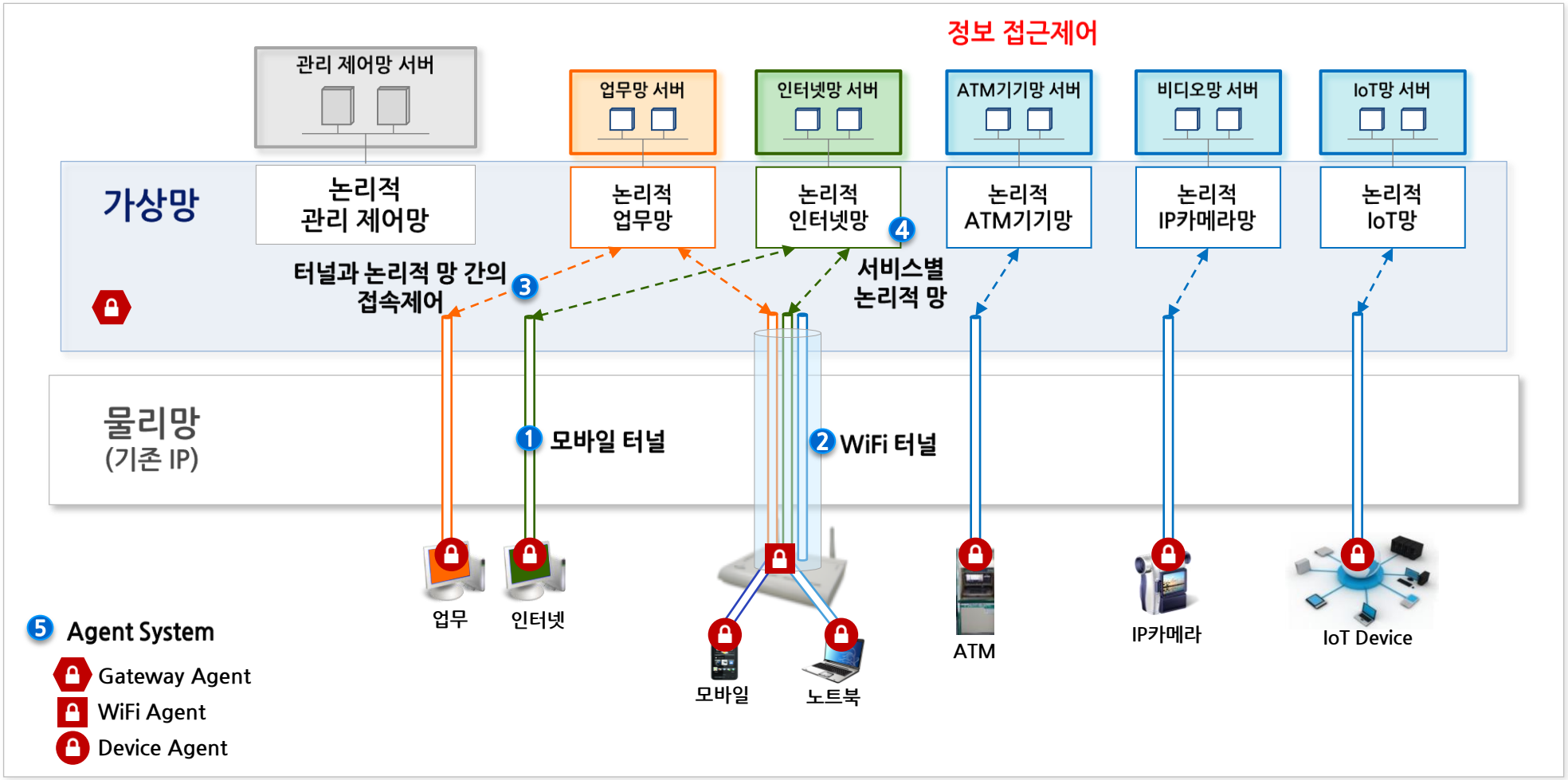
시스템 동작

- 관제 도메인을 별도의 가상 네트워크로 구현하고 필요한 만큼의 분리된 망을 가상화 기술로 생성



시스템 기능

- 기존 물리망 환경에 구애됨이 없이 모바일/WiFi 터널로 분리(Perimeter)된 가상망에서 지정된 구역의 정보 서버에만 접근 허가



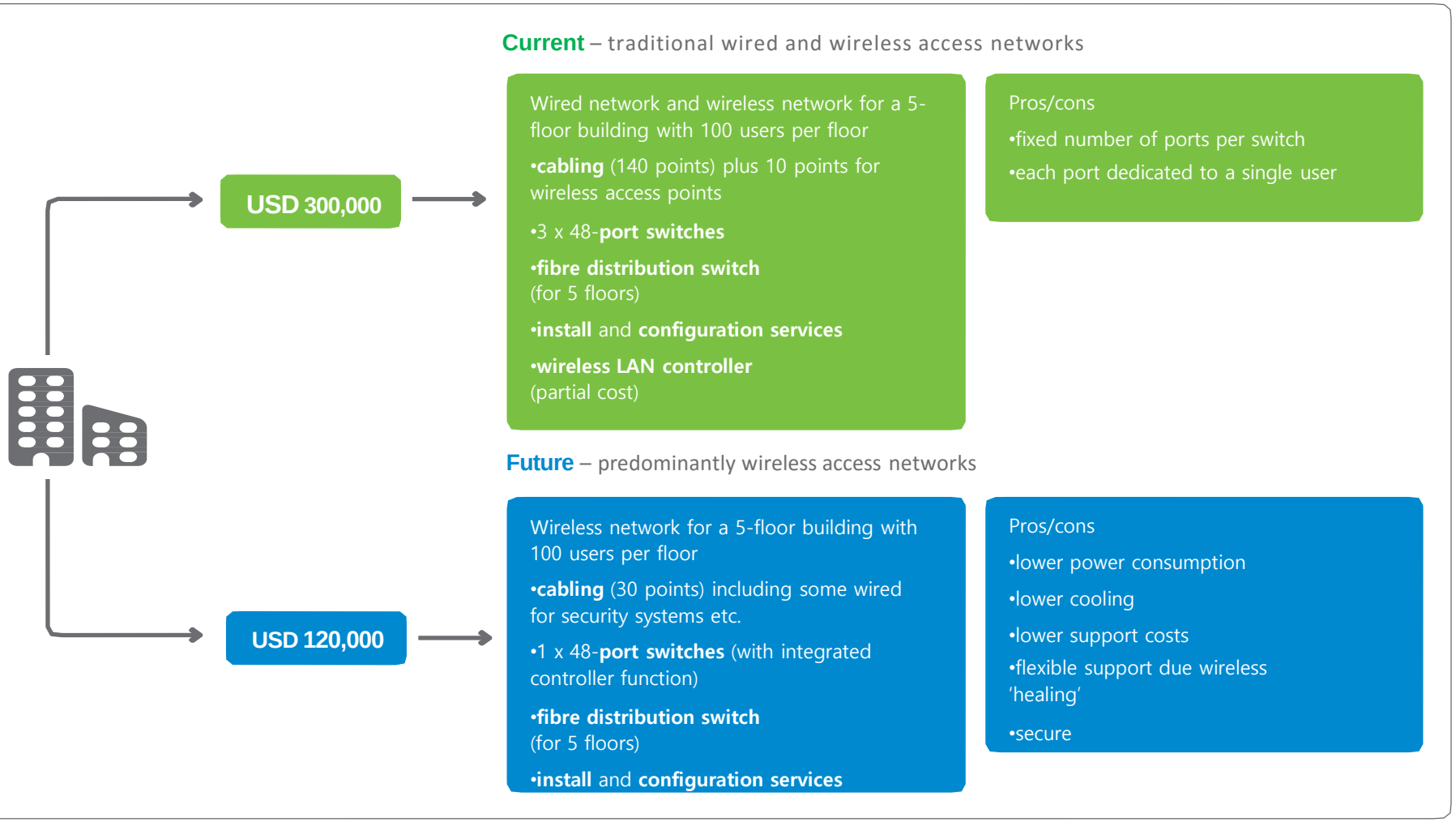
Trusted M-WiFi 검토

- 검토 배경
  - (모바일 데이터 수용 한계) 상용환경에서는 WiFi 이용이 급증하고 있으나, 국방에서는 보안 취약성 문제로 기술 도입 미흡
  - (Trusted WiFi 기술의 성숙) Trusted WiFi(Trusted WiFi) 기술의 상용화가 완료되고 국가정보원 보안성 검증이 통과되어 국방 분야의 기술 도입 환경이 조성됨
  - (무선LAN의 부각) 유선 80% : 무선 20% → 유선 20% : 무선 80% 시대
    ('2013 Network Barometer)

- 검토 절차
  - 기술개발, 구축운용 등의 사례 분석
  - 구축 요건 및 목표 정립
  - 구축 설계, 구축 타당성 분석 및 예산 계획
  - 시범 사업 및 상세 설계
  - 본 사업 추진

WiFi로 비용 절감과 편익 증대

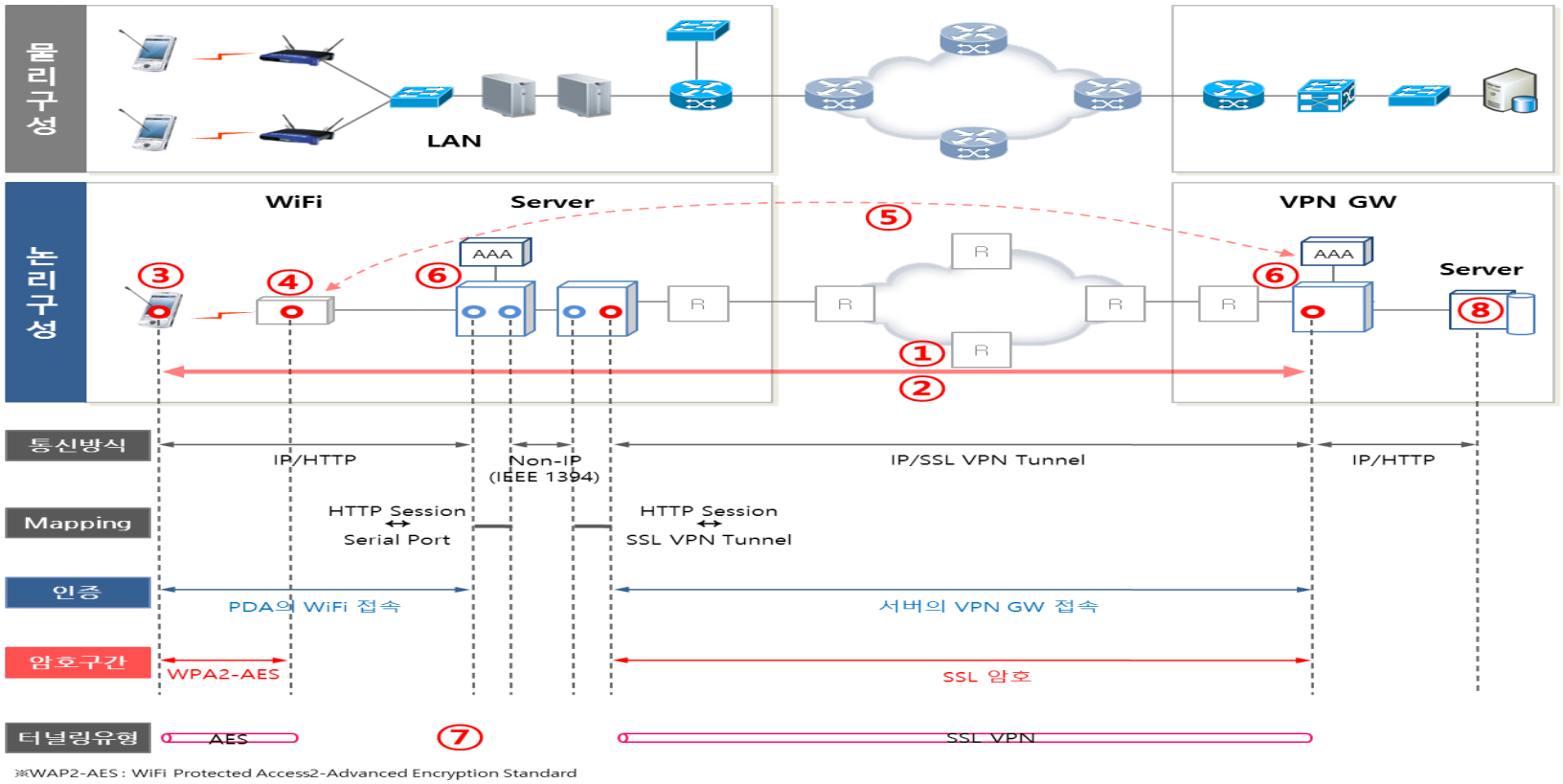
- WiFi로 경제적인 무선LAN 환경 구축



출처 : Network Barometer Report 2013

2016 CST Proprietary

WiFi 구축 유형 (서버 기반)

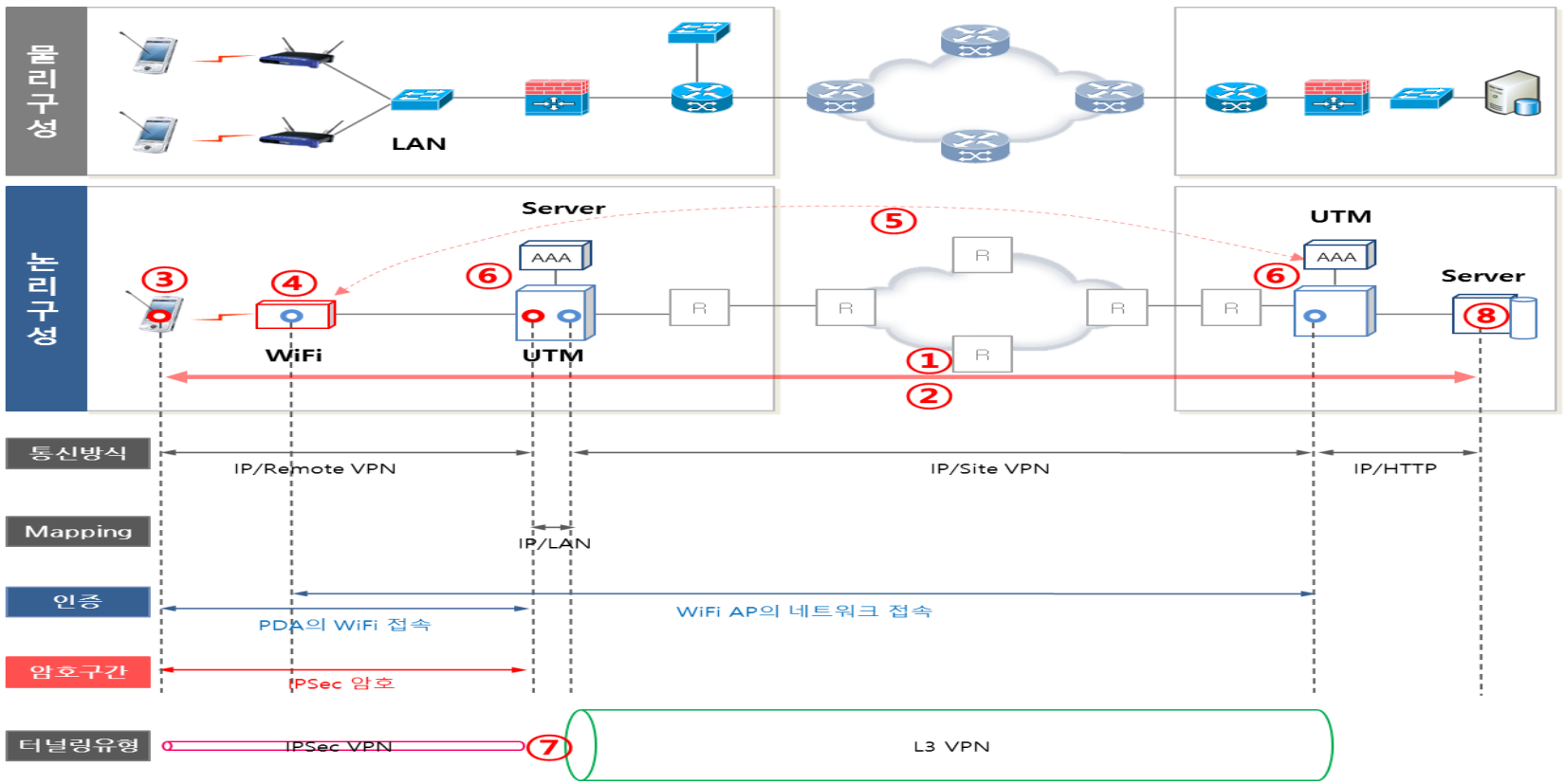


1. **IP망의 개방성** : User Data와 관제 Data가 동일한 도메인을 사용
2. **위조된 접근 공격** : 단말, 사용자, 패킷 등의 위조된 네트워크/서버 접근 공격
3. **단말의 무결점 관제** : 단말의 형상/형질 정보 변형 여부를 검증
4. **Rogue AP 접속** : 가짜 AP의 접속, 관제정보(암호키) 유출
5. **AP 환경설정정보의 노출** : 비인가 관리자의 불법적인 AP 접근
6. **관제서버의 노출** : 관제정보가 사용자 단말에서 접근되는 현상
7. **VPN의 단절** : WiFi 구간의 VPN과 IP백본망 구간의 VPN이 단절
8. **서버경계 통제** : 타 서버의 접근을 근원적으로 차단하는 기능 부재

*UTM : Unified Threat Management

2016 CST Proprietary

WiFi 구축 유형 (UTM*기반)



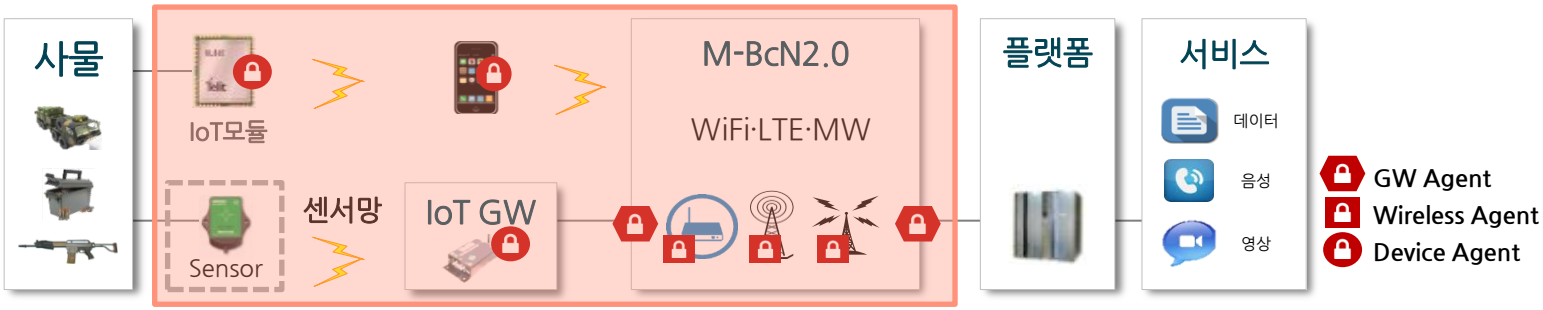
1. **IP망의 개방성** : User Data와 관제 Data가 동일한 도메인을 사용
2. **위조된 접근 공격** : 단말, 사용자, 패킷 등의 위조된 네트워크/서버 접근 공격
3. **단말의 무결점 관제** : 단말의 형상/형질 정보 변형 여부를 검증
4. **Rogue AP 접속** : 가짜 AP의 접속, 관제정보(암호키) 유출
5. **AP 환경설정정보의 노출** : 비인가 관리자의 불법적인 AP 접근
6. **관제서버의 노출** : 관제정보가 사용자 단말에서 접근되는 현상
7. **VPN의 단절** : WiFi 구간의 VPN과 IP백본망 구간의 VPN이 단절
8. **서버경계 통제** : 타 서버의 접근을 근원적으로 차단하는 기능 부재

*UTM : Unified Threat Management

2016 CST Proprietary

Trusted WiFi 요건

인가 없이는 보이지도 알 수도 없는 기밀성, 여러 요소가 체계적으로 빈틈이 없는 무결성, 만족스럽게 안정적으로 동작하는 가용성을 동시 제공하여 솟주기에 걸친 선제적인 침해대응 실현



Rouge AP의 접속 침해 방어	가짜 AP의 접속, AP 관제정보 (암호키) 유출 방지
AP의 원격관제 차단	비인가 관리자의 불법적인 AP 접근 (AP관제의 분리, 원격관제 차단)
단말의 AP 접속 제어	AP에 접속하면 3G 등 타 망 접속 차단, AP별 모바일 단말 관리(MDM), Red Zone 기능제어
AP Security Posture	AP 구성 내용의 무결점을 검증하는 기능
Trusted AP OS	Root 권한탈취 방지, 보안 Kernel, 관리 분리, 자원통제, 원격실행 방지, 접속 단말기의 상호인증 등
AP Router기능 삭제	일반 AP의 Bridging/Routing 기능 삭제
모바일 VPN 터널링	인가된 사용자의 VPN 터널 만을 전송 (White List기반)
모바일 VPN 집선	모바일 VPN 터널을 집선하여 가상망과 연동 (Multi-Tenant VPN)
위조 침해 방어	단말/사용자/패킷 등의 위조된 네트워크 및 서버 접근 공격 차단

용도의 분리	다수의 기관/사용자그룹에 독립적인 VPN 구성 (Multi-Tenant VPN)
관제의 분리	관리제어 정보의 격리 운영 (Closed Management & Control)
경로의 분리	다수의 가상 라우팅 도메인 구성 (Virtual Networking)
주소의 분리	물리 주소(가변)와 논리 주소(고유) 사용 지원 (Tunnel-in-Tunnel)
서버의 분리	Virtual Private Cloud 접속 서비스 (Hybrid Cloud)
단말의 분리	다수의 VPN 동시 접속 지원 (Multiple Virtual Machine/Storage)
대역의 분리	End-to-End기반 품질보장 서비스 (Per Flow QoS)
실시간 단말 무결점 관제	모바일 단말의 형상/형질정보를 분석/검증/통제하여 무결점 보장
인가 단말의 비정상 행위 제어	정상적인 접근인가 이후에서 발생되는 비정상적인 정보이용 행위를 탐지하고 관리

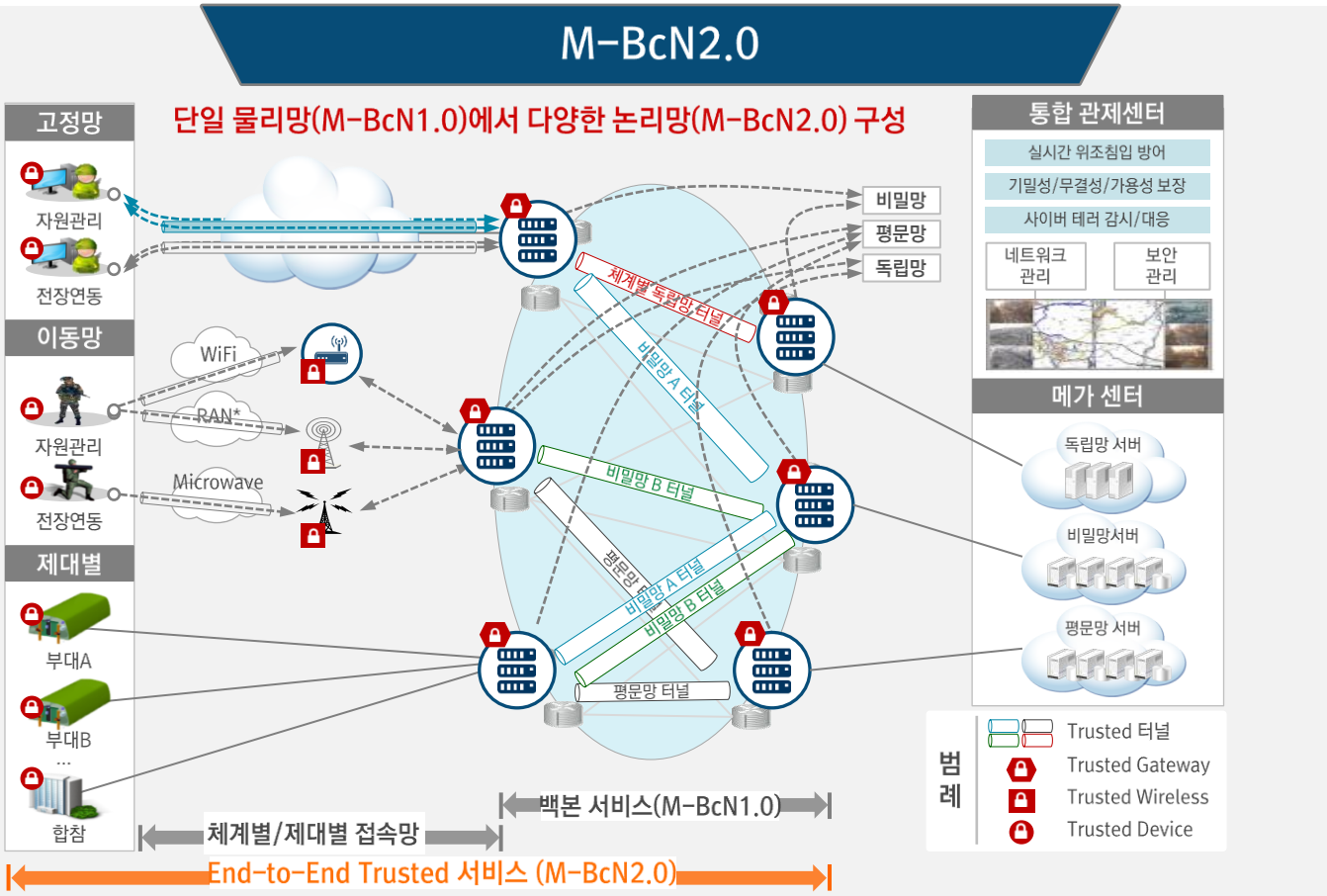
2016 CST Proprietary

Trusted M-BcN (예시)

- 어디서든 실시간 고속의 고신뢰 접속을 보장하는 네트워크에서 독립망(연합, 정보, 기무 등) · 비밀망 · 평문망 등의 통신수요를 통합 논리망 체계로 제공

고도화 목표

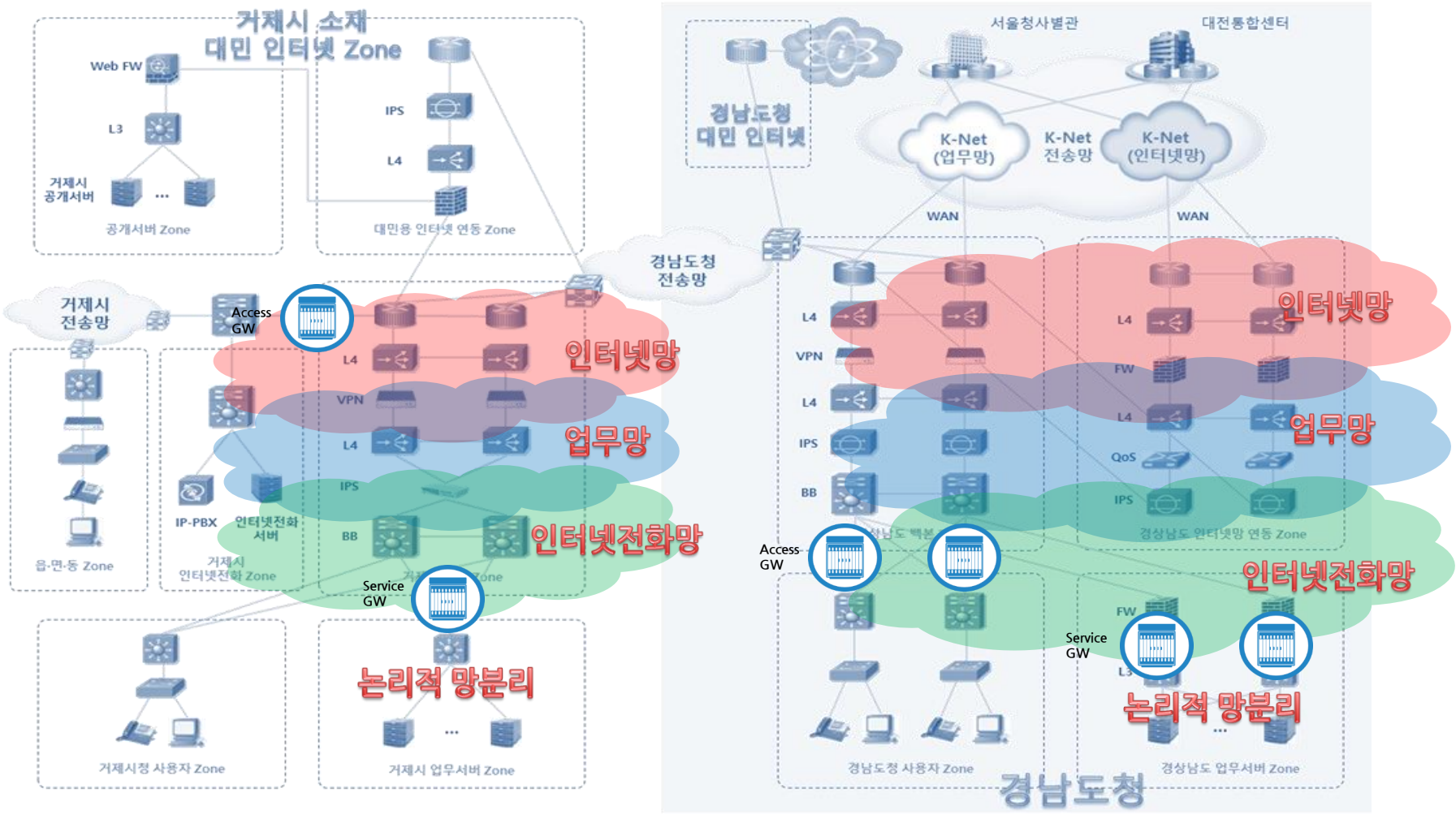
단일 물리망 Single Domain	통합 논리망 Multiple Domain
개방망 Open	폐쇄망 Closed
네트워크 간 Network-only	단말 간 End-to-End
유선 Wired	무선 Wireless
텍스트 · 음성 Text · Voice	실감 미디어 Rich-media
비실시간 Non-real time	실시간 Real time
계획되어진 Scheduled	즉각적인 Ad hoc



*RAN : Radio Access Network

솔루션 적용 분야 : 논리적 망 분리(예시)

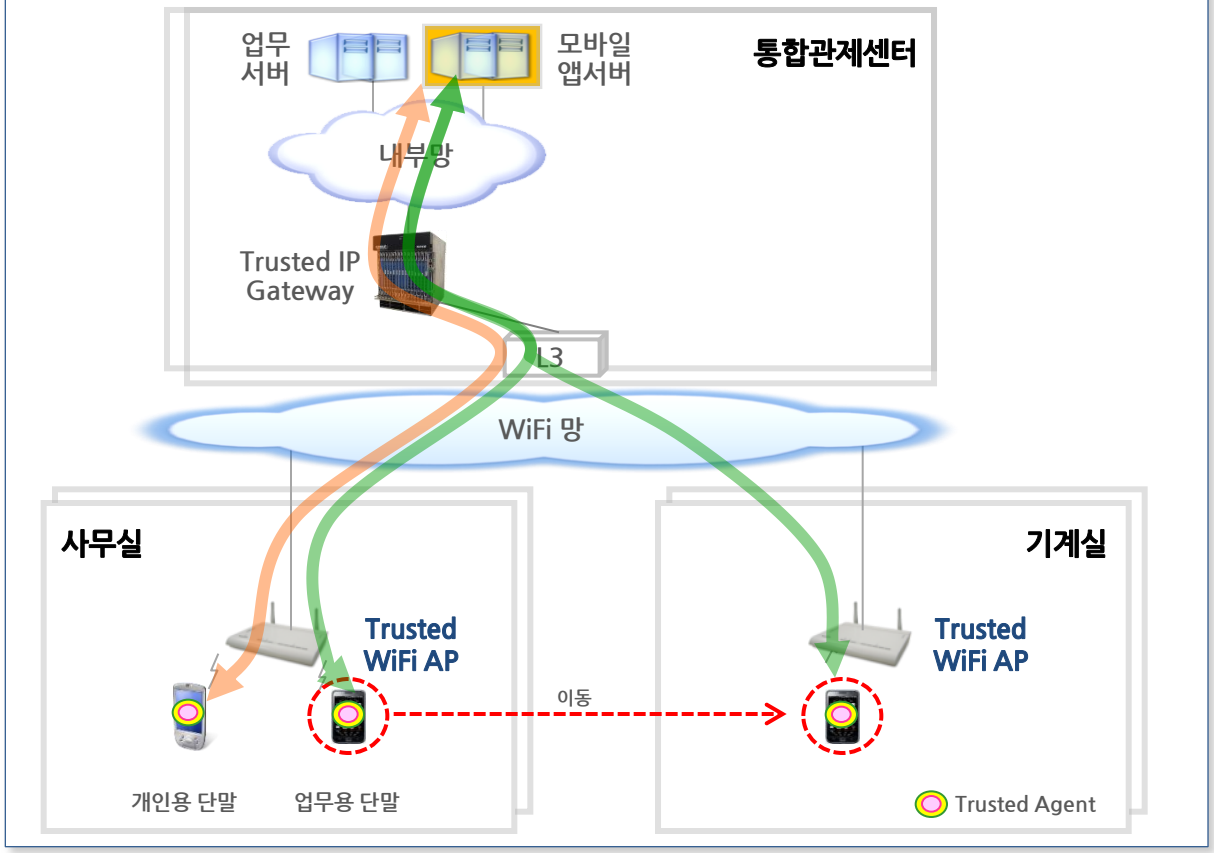
- 1개 물리적인 IP망에서 필요한 수 만큼의 다양한 논리망 구성 제공
  - 행정업무망, 인터넷망, 인터넷전화망, 스마트워크망 등 업무/서비스 유형별로 분리



솔루션 적용 분야 : Smart Work

- 권한 있는 단말/사용자에 대해 언제 어디서든 '안전한' 접근을 보장하여 실시간 업무 처리
- 단말 유형(개인, 업무)에 따라 서비스 접근을 차별화
- 기존 통신망 환경의 변화 없이 구축/관리되는 체계(Overlay 모델)

적용 형태



제공 기능

▶ 서비스 접근 차별화

- 업무용 모바일 단말(ex. 노트북, 스마트폰, 테블릿)의 유형에 따른 서비스 차별화가 가능하도록 구축
- 업무 현장에서 WiFi 망에 접속하여도 안정적으로 업무 서비스의 연속성 보장
- 개인 및 업무 전용 단말의 차별화된 관리제어 기준 마련

▶ 호환성 확보

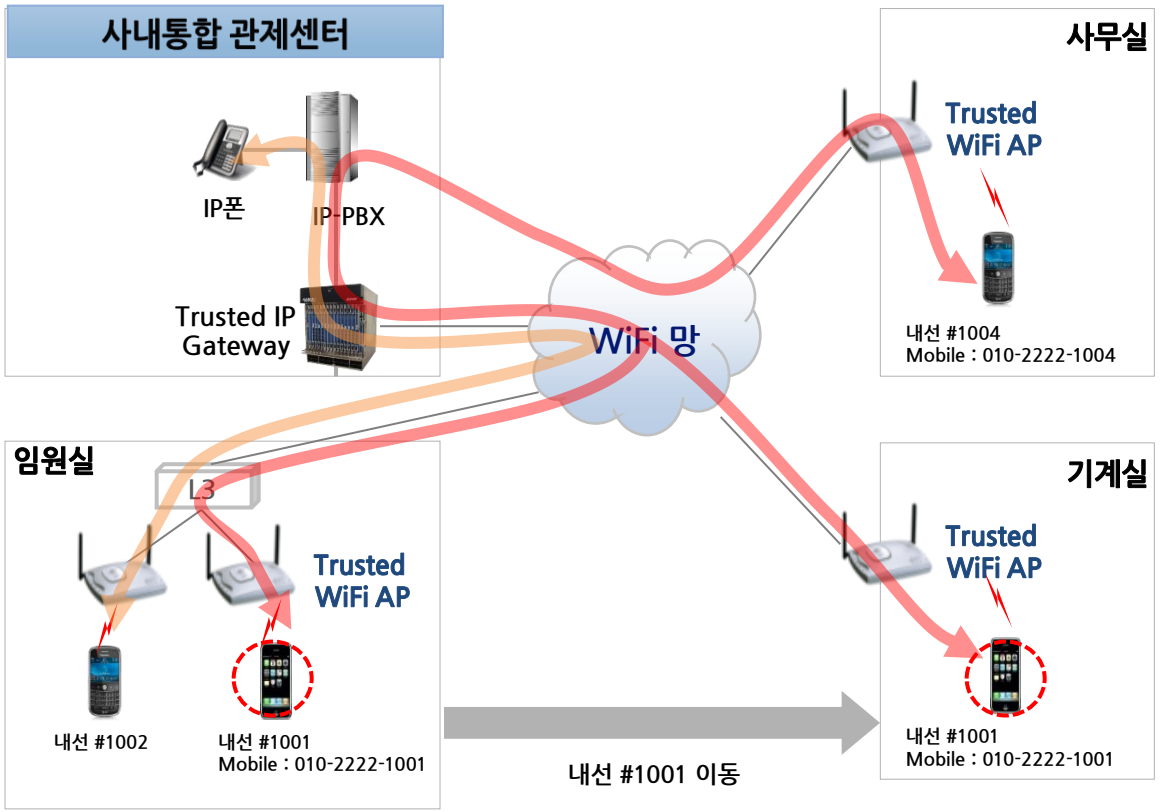
- 기존 업무 통신망 환경에서 구축 및 관리가 용이한 구조로 구축

2016 CST Proprietary

솔루션 적용 분야 : Mobile VoIP

- 고정된 사설 IP주소를 할당하여 이동성, 품질 보장성, 보안성이 확보된 음성통화 서비스를 제공
- 모바일 기반의 End-to-End Managed Connectivity 제공
- 보안성이 내재된 프리미엄 모바일 서비스 제공

적용 형태



제공 기능

▶ 이동성

- 사무실내 음성통화서비스(WiFi)의 연속성 제공
- 장소에 관계없이 단일번호를 이용하여 Mobile VoIP 서비스 제공

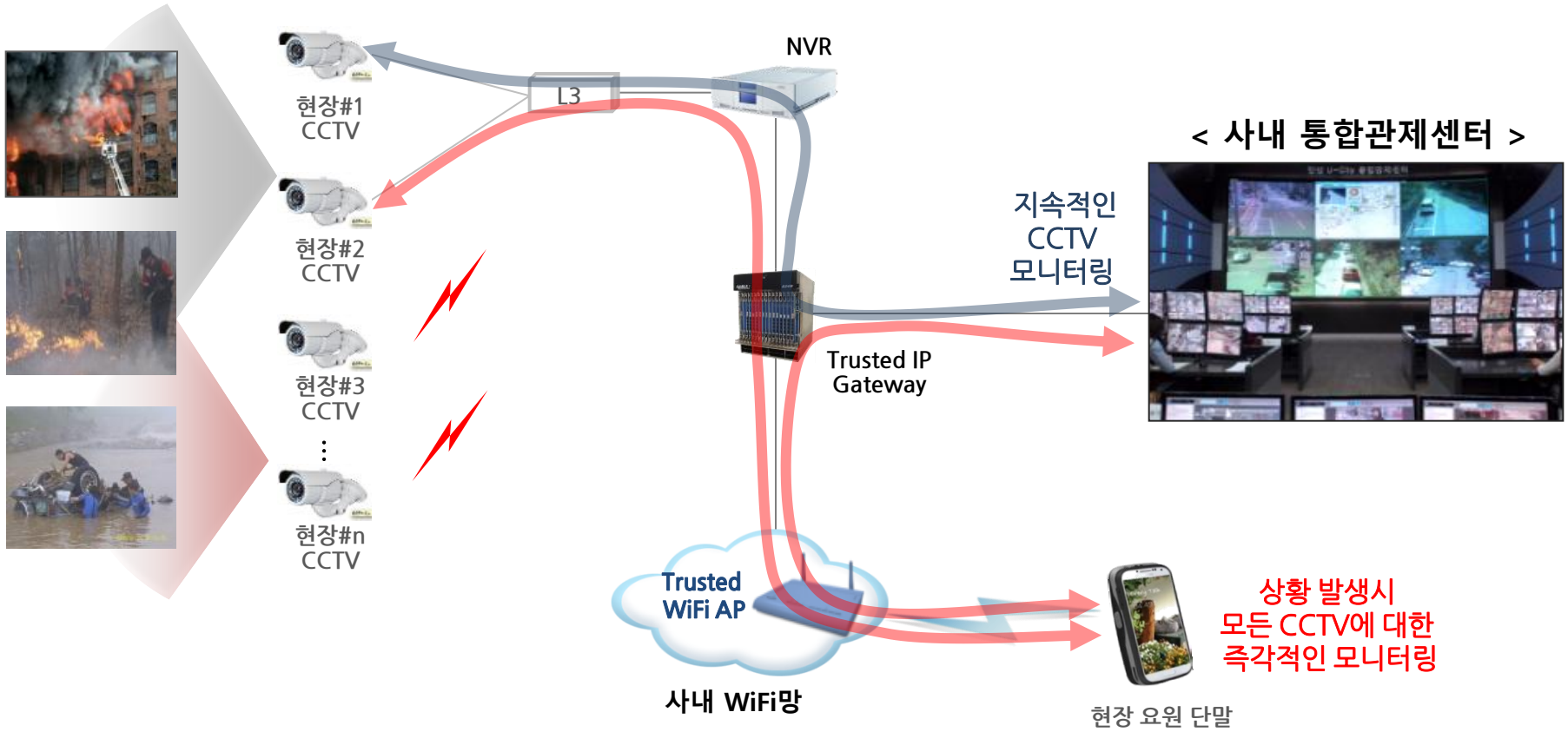
▶ 품질 보장 및 보안성

- 저비용, 고효율, 이용자 편의성 제공이 가능한 모바일 기반 음성통화 서비스 환경 구축
- 보안성이 강화된 내부 무선망(WiFi) 환경 구축

2016 CST Proprietary

솔루션 적용 분야 : IP Camera/m-CCTV

- 위급 상황발생시 현장 요원의 단말을 통해 모든 CCTV에 대한 즉각적인 모니터링 기능 제공
- 통합관제센터에서 모든 CCTV를 지속적으로 모니터링 하여 현장요원과 유기적인 공조체제 유지



2016 CST Proprietary

솔루션 적용 분야 : IP-PTT(Push to Talk)

- WiFi망으로 통합관제센터/현장/기타 원격지에서 발언권 통제/그룹통화 등 직접 지휘 통제
- 이용자 상호간의 공용 통신(IP-PTT)을 제공하여 기존 무전기의 기능을 보완 및 대체 가능

적용 형태

제공 기능

• Trusted WiFi 기반 IP-PTT 서비스

- PTT Group 추가/수정/삭제
- 단말 정보 View
- 다자간 통화를 위한 멀티 세션 지원
- 양방향 영상/음성 VoIP Call
- 1:1, 1:N 영상/음성 PTT Call
- 1:1, 1:N, 1:Group SMS 전송 지원
- 복수의 PTT 그룹 호출 기능 지원
- 그룹 참여 기능 지원
- PTT Master(호출자) 권한 이양 지원
- 비상통화 기능 지원
-단말기 유/무효화 기능 지원
- PTT 발언권 가로채기 기능 지원

• 모바일 정보시스템과 연동 지원

• IoT 서비스와 연동 지원

2016 CST Proprietary

Ⅳ. 차별성 및 기대효과

- 차별성
- 기대 효과
- [참고]

기대효과

내부적 요구와 환경적 요구를 동시에 충족

- TIPN은 안전한 사이버 사회 구현의 내부적 환경적 요건을 받들어 안전한 삶을 실현한 기술

내부적 요구

개방 · 노출 상태의 통제

- 개방(Open) → 폐쇄(Closed)
- 네트워크 경계 + 정보자원 경계
- 네트워크 접근 위조방어 + 정보자원 접근 위조방어
- 접속 단말의 무결점 검증 결여
- 비정상 사용 행위 제어 결여

관제정보가 개방 / 정보자원이 노출

환경적 요구

사이버 안전 구현 대안

- **일하는 방식 혁신**
  - 단편적 역량 → 통합적 역량
- **사이버 안전사회 위협**
  - 일시적·부분적 → 지속적·전방위적
- **침해공격 방어 기술**
  - 사후적 방어 → 선제적 방어

지속 · 선제적 안전 통합역량 필요

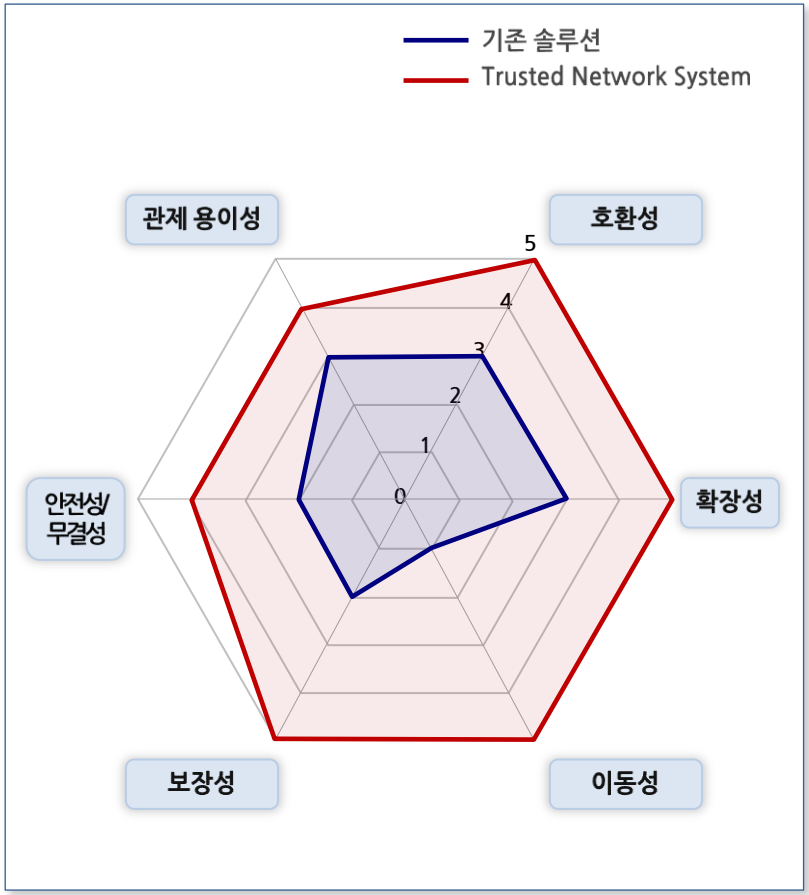
2016 CST Proprietary

기대효과

기술적 기대 효과

- World Best, World First한 Overlay 기술
- 통합 능력과 협업(UC & C) 서비스 솔루션

항 목		기존 솔루션	Trusted Network System
호환성	• 기존 토폴로지 및 장비들과의 호환성	△	○
보장성	• 서비스별/이용자별 품질보장 • 공평성 (Fair Use)	△ X	○ ○
이동성	• 유무선망간/이기종 무선망간 • 보안통신용 터널	X X	○ ○
안전성 무결성	• VR 기반 독립된 네트워크 분리 • 종단간 암호화 터널 • 단말의 위변조 방지	X X △	○ ○ ○
관제 용이성	• 실시간 자동 관제 • 관리와 제어의 통합 • 단말/서비스 통합제어	△ △ X	△ ○ ○
확장성	• IPv6 및 센서망(IoT) 수용 • 추가 기능 적용 용이	△ ○	○ ○



※기존 솔루션은 보안장비, 네트워크 장비, 관리 Tool 등 다양한 유형의 장비들로 구성됨

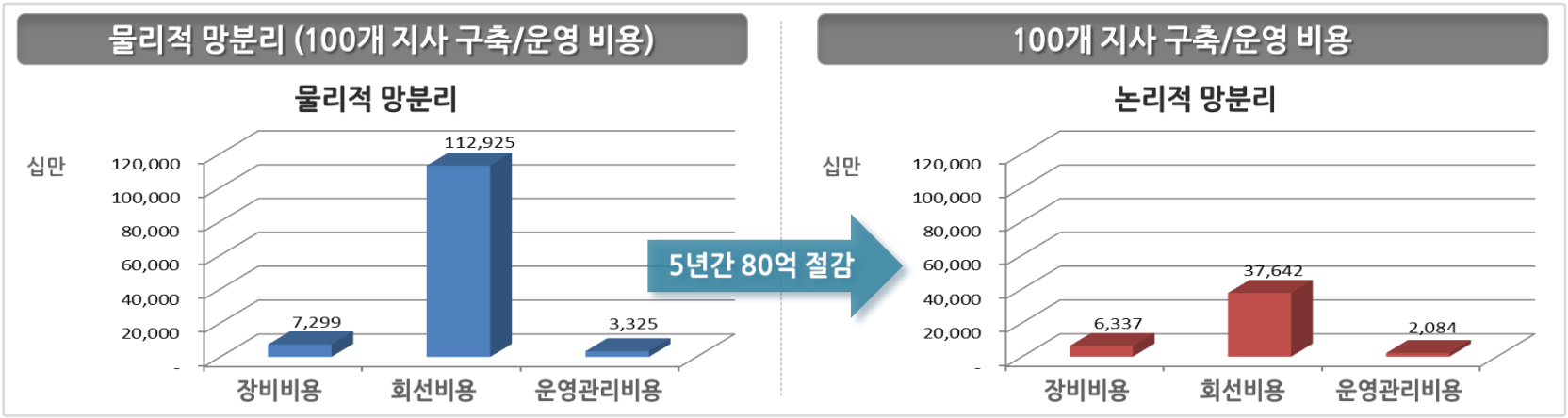
2016 CST Proprietary

기대효과

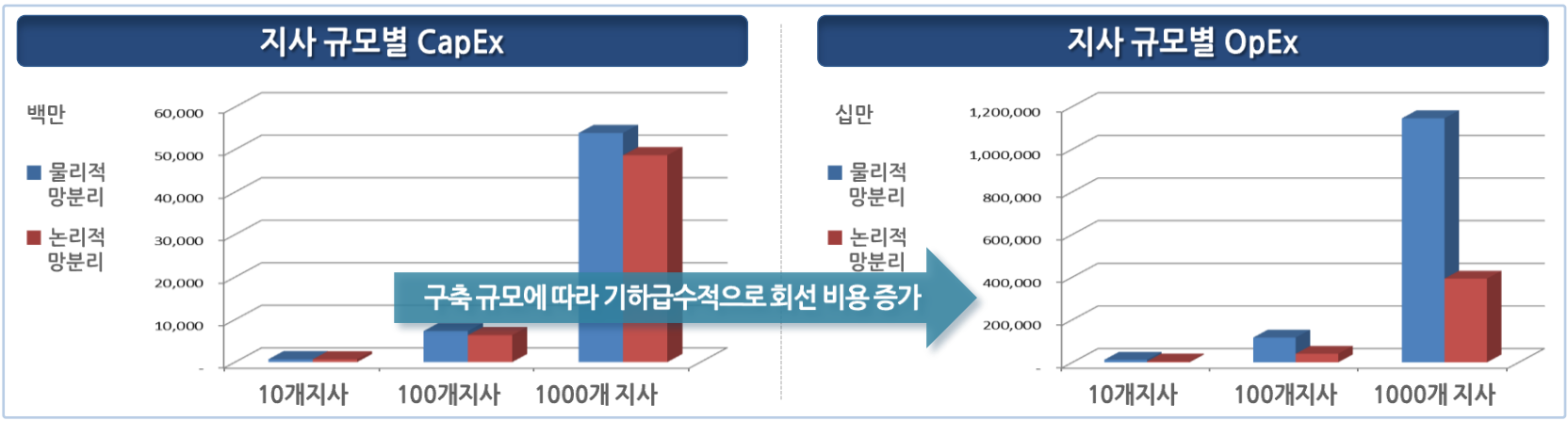
논리적 망 분리 효과

- 회선비용을 경감시켜 저렴한 비용으로 인터넷 망과 완전 격리된 업무 망 구축이 가능
  - 전국에 있는 100개 지사 보유 기관의 경우 회선비용에서 5년간 80억 원의 절감 효과를 기대

구축/운영 비용 비교

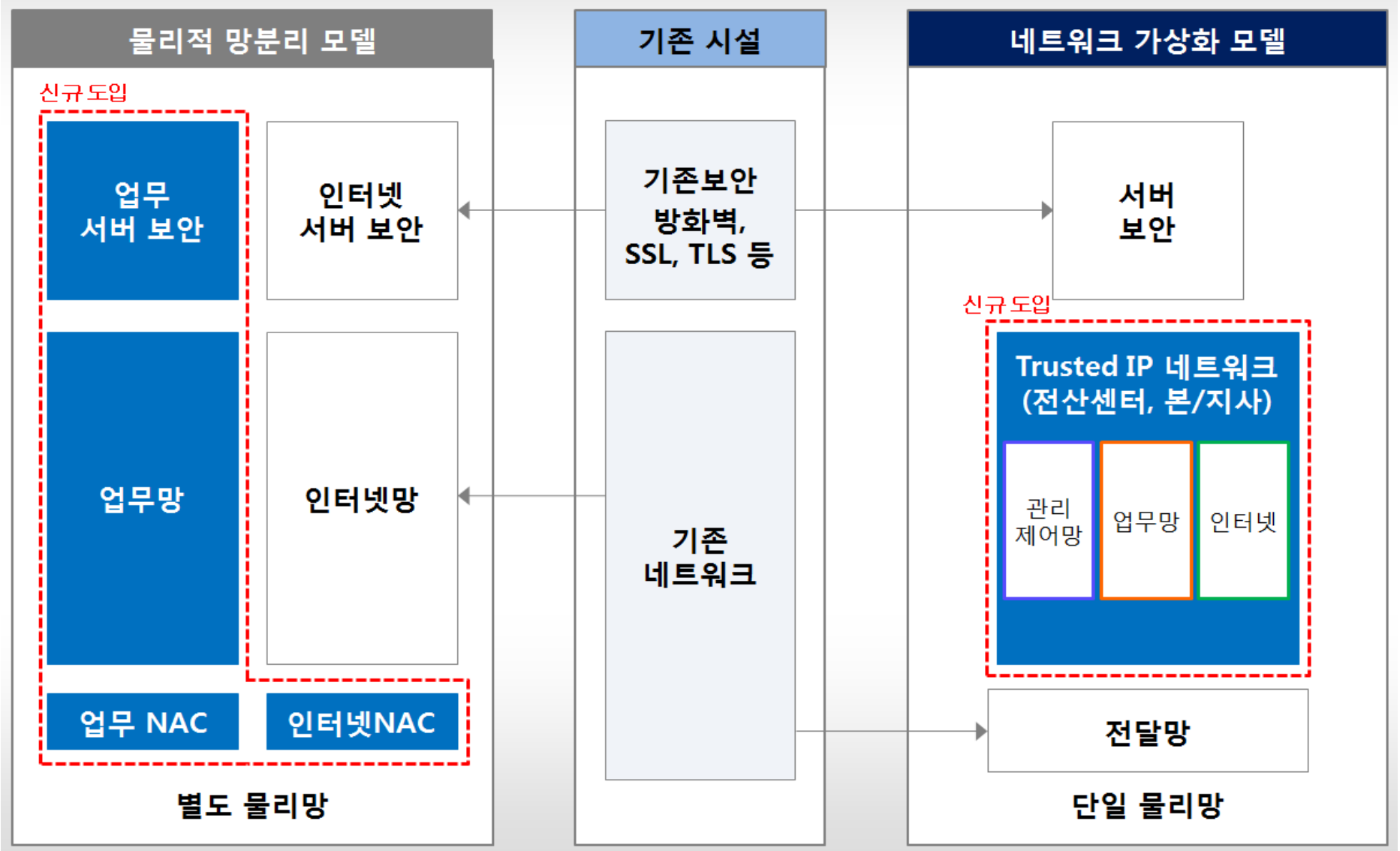


지사 규모별 비용 비교



2016 CST Proprietary

기대효과 (분석 기준)

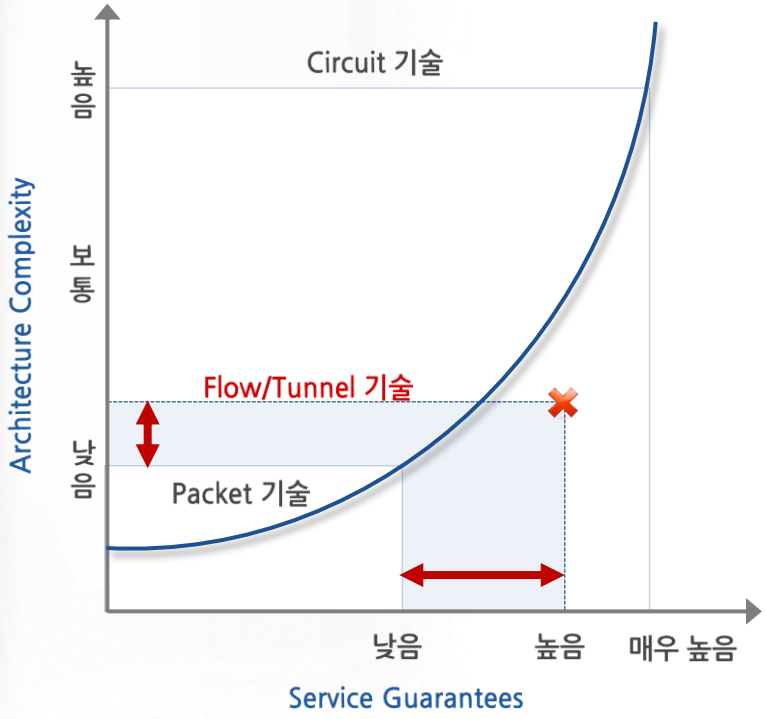

물리적 망분리 모델
기존 시설
네트워크 가상화 모델
신규 도입
업무
서버 보안
인터넷
서버 보안
기존보안
방화벽,
SSL, TLS 등
서버
보안
업무망
인터넷망
기존
네트워크
신규 도입
Trusted IP 네트워크
(전산센터, 본/지사)
관리
제어망
업무망
인터넷
업무 NAC
인터넷NAC
전달망
별도 물리망
단일 물리망

[참고] 간단성 대비 높은 보장성

- Flow/Tunnel 기술을 활용하여 높은 수준의 보장기능을 간결한 구조로 제공
- 미국 국방성의 전술 무기인 'Black Core Network' 기술 반영

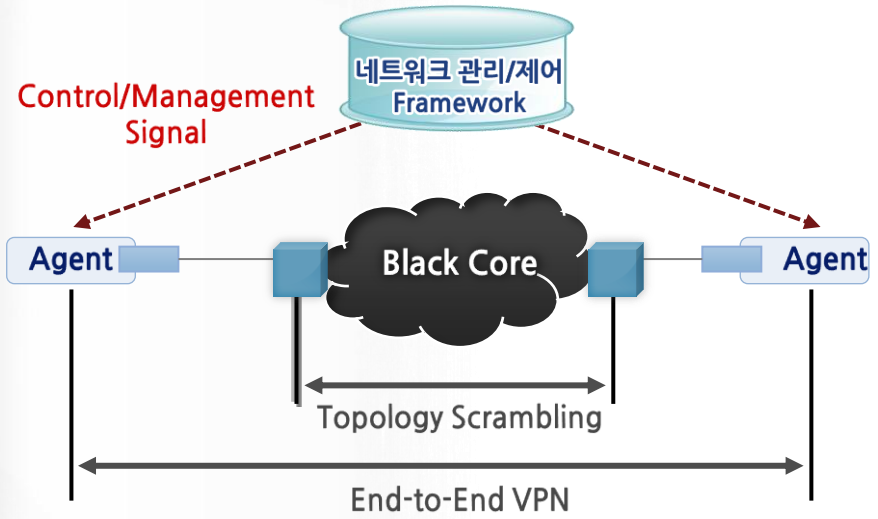
Flow/Tunnel 기술

(Packet 기술보다는 약간 복잡하지만, Circuit 수준의 높은 보장성을 제공) ▶ Guarantees/Complexity Ratio ≫ 1



미국 GIG(Global Information Grid) 프로젝트

(미국방성(US DoD) GIG 3.0 Design Factors, 2011.01)



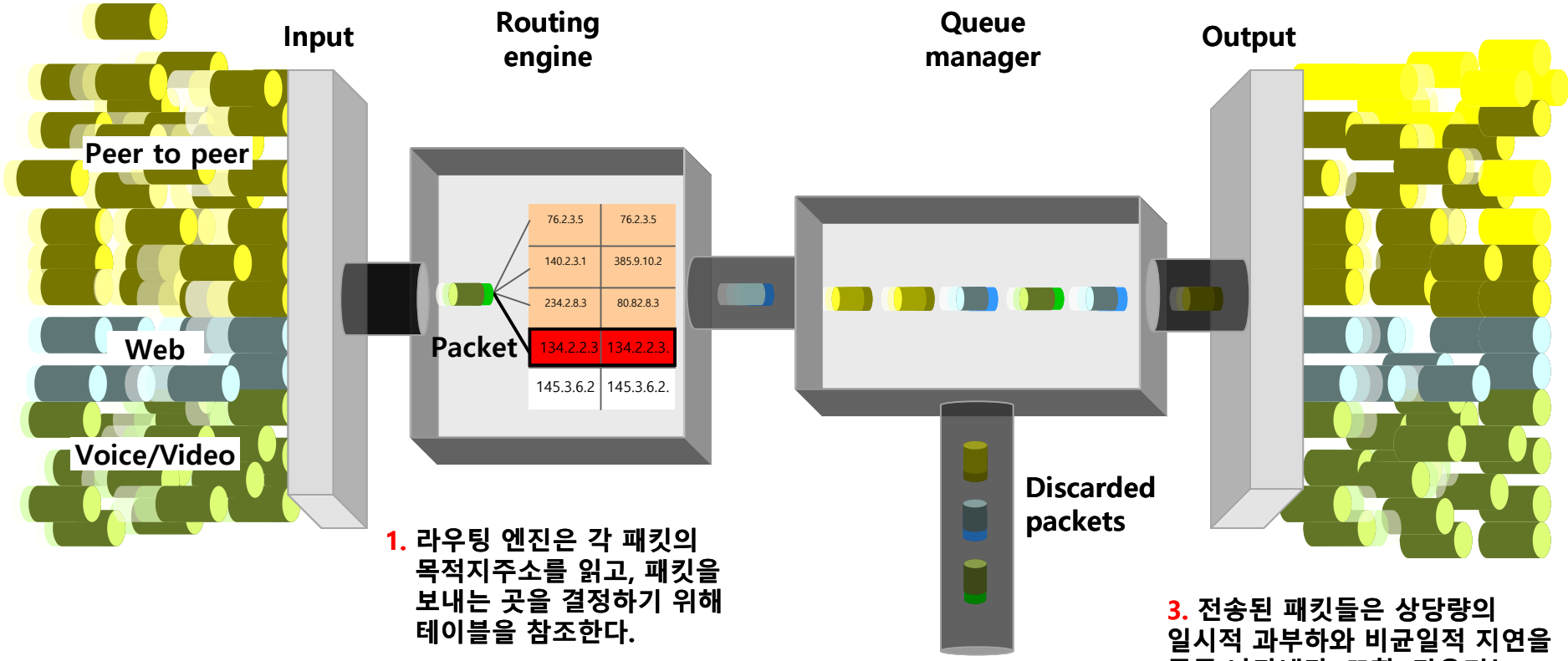
주요기술

네트워크 관리/제어 망 분리, 종단간 VPN 구성, 비밀등급별 트래픽 암호화, 네트워크 동적 구조 변화 구성 등

2016 CST Proprietary

[참고] Conventional Router

- Routing Table



1. 라우팅 엔진은 각 패킷의 목적지주소를 읽고, 패킷을 보내는 곳을 결정하기 위해 테이블을 참조한다.

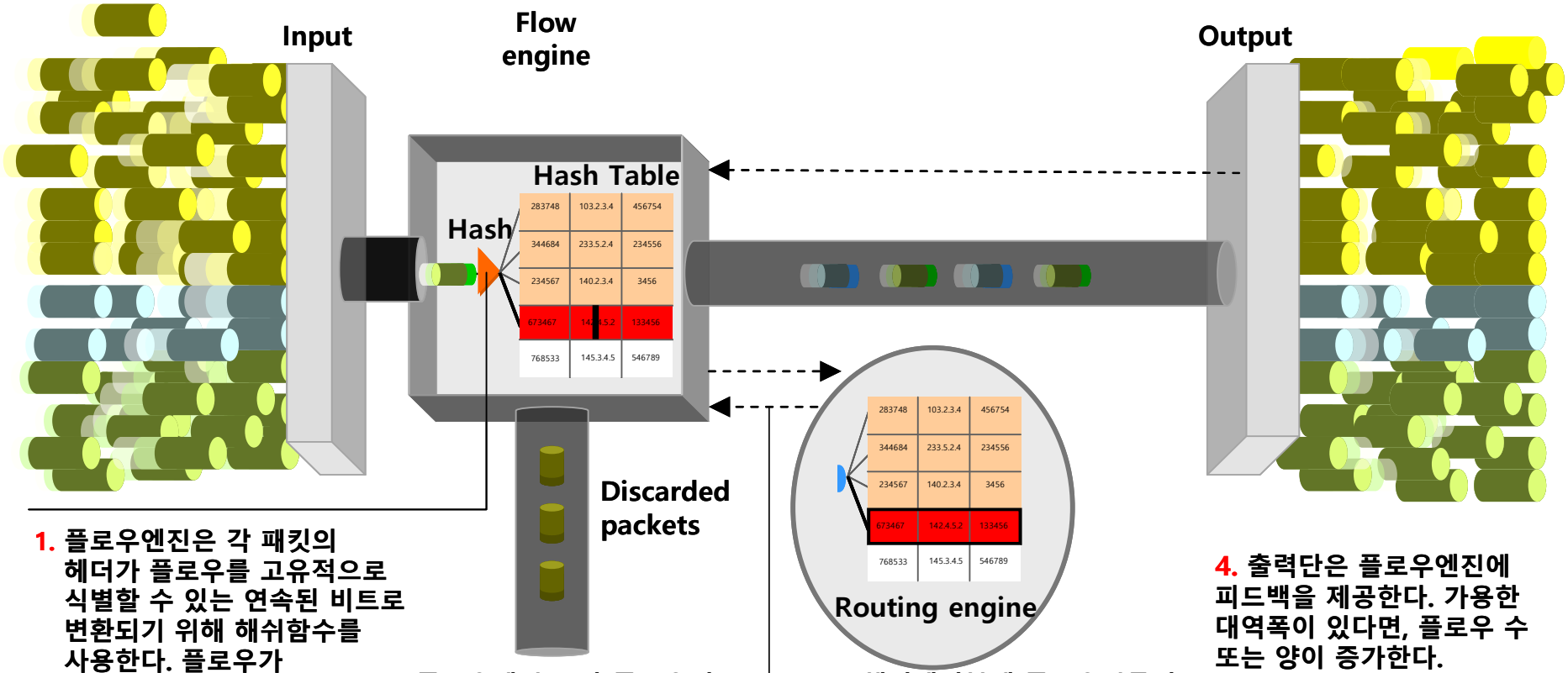
2. 큐 매니저는 전송될 때까지 패킷을 버퍼링한다. 혼잡상황이 발생하면, 처리량을 줄이기 위해 무작위로 패킷을 폐기한다.

3. 전송된 패킷들은 상당량의 일시적 과부하와 비균일적 지연을 종종 나타낸다. 또한, 라우터는 트래픽의 특정 종류를 제어할 수 없게 될 때가 있다.

2016 CST Proprietary

[참고] Flow Router

- Flow Control Block



1. 플로우엔진은 각 패킷의 헤더가 플로우를 고유적으로 식별할 수 있는 연속된 비트로 변환되기 위해 해쉬함수를 사용한다. 플로우가 해쉬테이블에 저장되어 있다면, 패킷은 출력장치로 바로 이동한다.

2. 플로우엔진은 각 플로우의 지속기간과 식별처리량을 계속적으로 추적한다. P2P Flow를 제한 할 수 있는 반면, 웹,음성,비디오를 보호하기 위해 선택적으로 패킷을 폐기한다.

3. 해시테이블에 플로우기록이 없을시에는, 라우팅엔진이 패킷의 이동장소를 결정한다. 해시테이블은 새로운 플로우를 갱신되며, 그리하여 후속패킷은 라우팅엔진 단계를 생략하게 된다.

4. 출력단은 플로우엔진에 피드백을 제공한다. 가용한 대역폭이 있다면, 플로우 수 또는 양이 증가한다. 제약적인 대역폭인 경우에는, 플로우를 줄인다.

감사합니다!
(Q&A)
Trusted IP Network Innovator
MC MOBILE CONVERGENCE
CST
ICT CONSULTING

고품질 융합서비스를 위한
국방 기반체계 연동기술 개발

2016. 2. 26.

박 혜 숙
한국전자통신연구원

Smart & Green Technology Innovator
ETRI

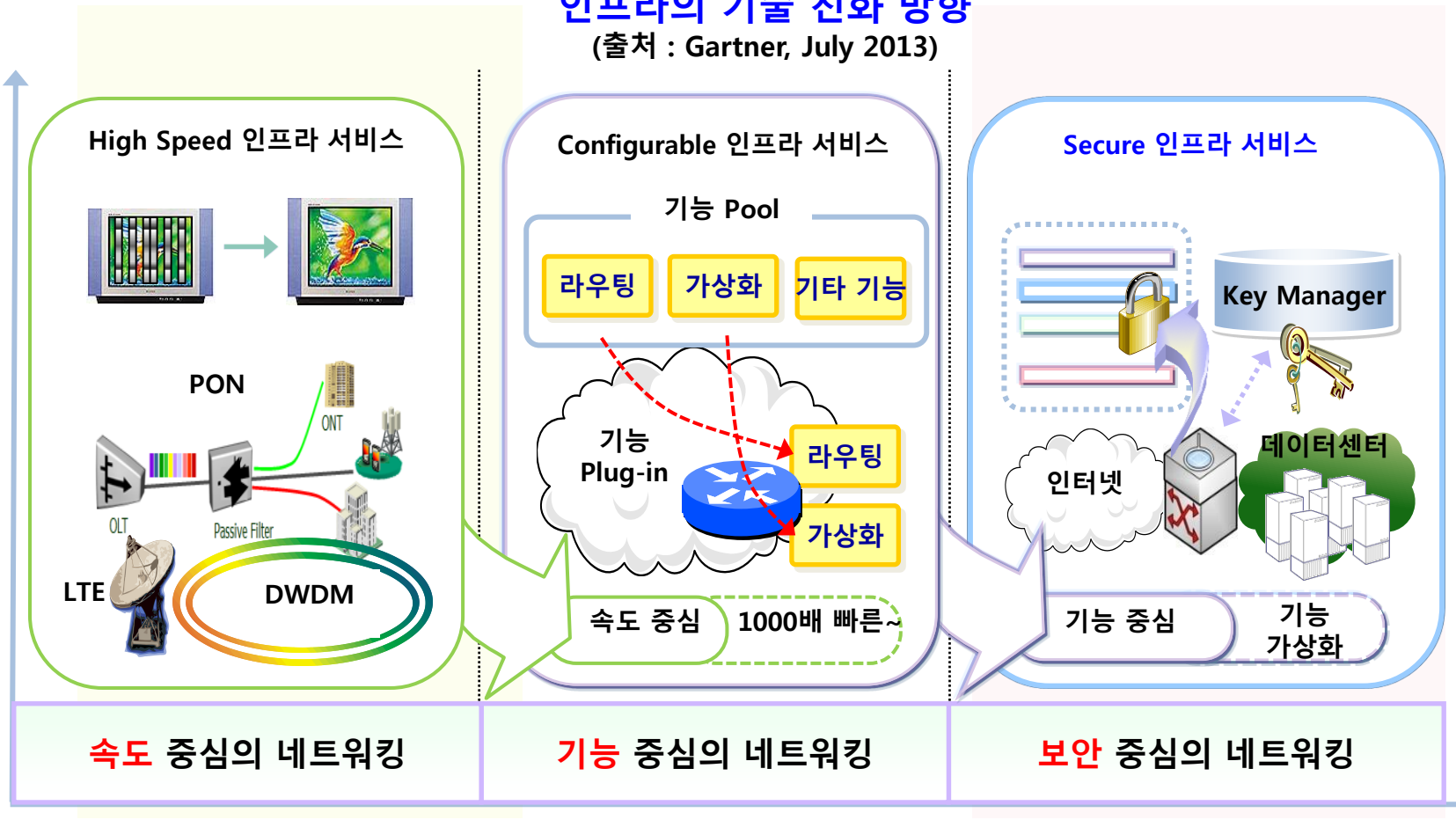
목 차

1. 기술 동향
2. 과제 개요
3. 추진전략
4. 주요성과

- 안전한 정보인프라 구축은 전세계적인 공통 현안사항
- 속도(빠른)→ 기능(똑똑한)→ 보안(안전한) 중심의 인프라로 진화 · 발전 中

인프라의 기술 진화 방향

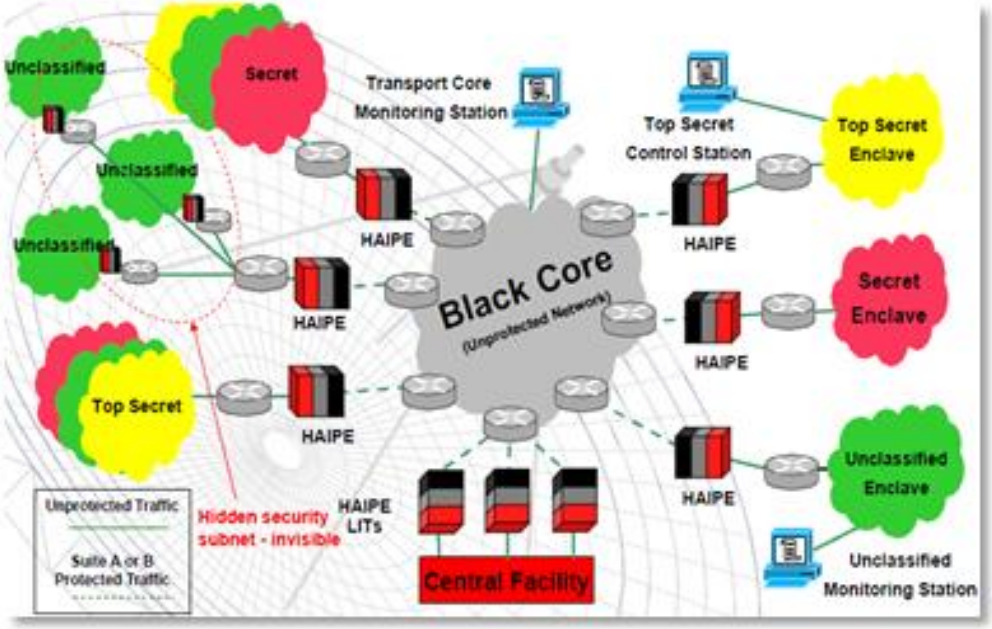
(출처 : Gartner, July 2013)

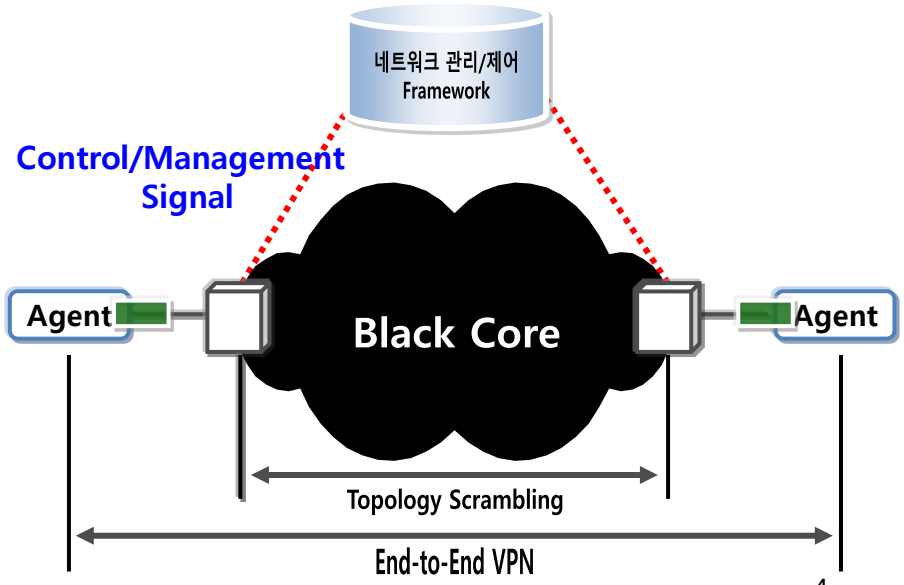


1. 기술동향

GIG(Global Information Grid) 프로젝트 (2001.9.11 테러 이후 미국 정보공유 가속화 !!)

- **(목적)** 네트워크 중심전 환경에 대비하여 **전 세계 네트워크를 미국방성의 안전한 가용네트워크로 만들기 위한 총체적 통신프로젝트**
  - GIG 개념 정의('02년), GIG 1.0('07년)→GIG 2.0('09년)→GIG 3.0('11년) 발표
- **인터넷 등 보호되지 않는 네트워크를 경유하는데 있어서 안전하게 유통하는 'Black Core Network' 기술**을 개발하여 '20년 국방 네트워크 고도화 추진
- **(주요기술) 네트워크 관리/제어 망 분리, 종단간 VPN 구성, 비밀등급별 트래픽 암호화, 네트워크 동적 구조 변화 구성 등** ※ 출처 : 미국방성(US DoD) - GIG 3.0 Design Factors (11 Jan. 2011)





1. 기술동향

국방 요구사항

NCW는 여러 전투 요소들을 네트워크로 연결하여 전장 상황을 공유하고 통합적이고 효율적인 전투력을 창출하고자 하는 것 → NCW 환경에서는 **정보의 유통을 위한 통신이 가장 중요**

미래 전쟁 수행 패러다임

EBO와 RDO의 성공의 필요조건은 NCW의 성공이며 NCW의 핵심 요소인
네트워크의 역할 및 활용도는 다음 4가지로 구분

상황인식 공유	신속한 지휘 및 의사결정	정보 우세	자체 통합
• 지리적으로 분산된 아군 전력간의 전장공간에 대한 상황인식 공유	• 네트워크 연결을 통한 상황 인식 및 정밀성 제공으로 적시에 표적에 대한 반응 가능	• 적시적이고 정확하며 타당성 있는 정보 획득으로 정보 우위 확보	• 하급제대는 공유된 상황 인식과 지휘관 의도를 바탕으로 독립적인 작전수행

NCW의 성공을 위해 군의 네트워크는 상기 4가지 역할을 충족해야 하며
이를 위해 공중, 위성까지 연결되는 다양한 네트워크를 통합하여 생존성을 보장하고,
지휘통신전력부터 공중전력까지 네트워크를 중심으로 통합되어야 함

※ All IP 기반의 통합망 구축을 위한 정보화 계획 수립(국방부)

2. 과제 개요

과 제 명	고품질 융합서비스를 위한 국방 기반체계 연동 기술 개발
연구기간	2013. 5. ~ 2016. 2. (3년)
총 연구비	8,001 백만원 (정부 6,000 백만원 / 민간 2,001 백만원)
당해년도 연구비	2,667 백만원 (정부 2,000 백만원 / 민간 667 백만원)
총 참여인력(M/Y)	159 명 (68.07 M/Y)
당해연도 참여인력(M/Y)	54 명 (22.69 M/Y)
주관연구기관	한국전자통신연구원
연구책임자	박혜숙 실장
공동연구기관 (연구책임자)	㈜텔레필드 (이희원 팀장) ㈜아큐픽스 (김기철 이사) ㈜SNI (남성엽 연구위원) 넷진테크㈜ (이상문 이사) 숭실대학교 (신용태 교수) 국방기술품질원(권경용 책임)

2. 과제 개요

개발 필요성

미 "중국 IT장비 구입 전면 금지"

오바마 대통령 법안 서명… 해킹의혹 중국정부에 실질적 강타

양국 사이버전쟁 확대 가능성

'해킹 의혹' 사건으로 미·중간 외교 갈등이 가열되고 있는 가운데, 미국이 주요 정부기관에 중국산 정보기술(IT) 시스템 구입을 금지토록 했다. 주요 2개국(G2) 간에 사이버 전쟁으로 확대될 수도 있다는 분석이 나오고 있다.

27일 오바마 대통령은 미 의회가 입안한 정부 지출 관련 법안에 서명했다. 법안의 '섹션 516' 조항에 따르면 상무부와 법무부, 나사(미 항공우주국), 국립과학재단(NSF) 등은 중국 정부와 연계된 업체에서 IT 시스템을 구입하는 것이 전면 금지된다.

이 조항은 27일부터 당장 발효되며 시한은 2013년 회계연도가 끝나는 오는 9월30일까지다. 다음 회계연도에도 별다른 변수가 없다면 효력이 연장될 가능성이 크다.

AP는 "미국 정부가 광범위하고 조직적인 해킹 의혹을 사고 있는 중국 정부에 처음으로 실질적 강타를 날렸다"고 전했다.

섹션 516 조항은 지난해 연말부터 발생한 해킹사건의 배후에 중국인민해방군(PLA) 해커부대가 있다는 의혹이 제기되면서 대책이 필요하다는 목소리가 높았던 만큼 의회가 특별하게 신경을 써서 입안했던 것으로 전해졌다. 미국에서는 뉴욕타임스와 블룸버그, 월스트리트저널, 페이스북, 애플 등의 업체는 물론 법무부와 에너지부 등 정부부처까지 해킹을 당했다.

IT 시스템 구입 금지는 중국 정부가 소유·운영하는 국영기업과 함께 정부 보조금을 받는 모든 업체가 대상이다. 금지 물품도 이들 업체가 생산하고 제조하거나 조립하는 IT 시스템으로 구체적으로 명시됐다. 단, 국가 이익을 위해 필요할 경우에는 연방수사국(FBI)과 협의해 사이버 스파이 행위나 시스템 마비 우려가 없다고 판단되면 구입을 허용하도록 했다.

사이버 보안 정책 전문가인 스튜어트 베이커 전 국토안보부 차관보는 "미국 정부의 중국산 IT 시스템 구입 금지는 방향의 전환"이라며 "당분간 이같은 움직임이 계속될 것으로 보인다"고 말했다.

신동규기자 dkshin@dt.co.kr

종합

초고속 통신망 자랑하지만…장비는 글로벌 기업이 70% 장악

기사본문 | SNS댓글 쓰기 | CAR VS CAR 자동차 설문조사 이벤트

입력: 2013-01-23 15:30 / 수정: 2013-01-23 15:30

네트워크 장비 산업 전단

제품 수입 의존도 심화…현장 맞춤형 인재 양성 절실
기획서 수출까지 안증기반 구축

국내 네트워크 산업을 지탱하는 통신장비 업체들의 생존권이 위협받고 있다.

국내 네트워크 장비시장에서 국내 기업들이 차지하는 비율은 전체의 30% 수준. 나머지 70%는 글로벌 업체들이 잠식하고 있다. 세계 최고 수준의 초고속 통신망을 자랑하지만 외산 장비에 대한 높은 의존도로 정작 국내 네트워크 장비산업은 통반성장하지 못하고 있다. 이에 대해 국산 네트워크 장비 업체들이 다시 도약하기 위해선 우선 내수시장에서 신뢰를 확보하고 이를 바탕으로 글로벌 업체와 경쟁하며 해외로 진출해야 한다는 목소리가 높아지고 있다.

"국방개혁위해 정보화 기반 강화"

국방정보화 세미나… 지휘구조 변화 맞춰 C4I 우선 계획

강경규 기자 kjk@dt.co.kr | 입력: 2011-07-10 20:20

[2011년 07월 11일자 6면 기사]

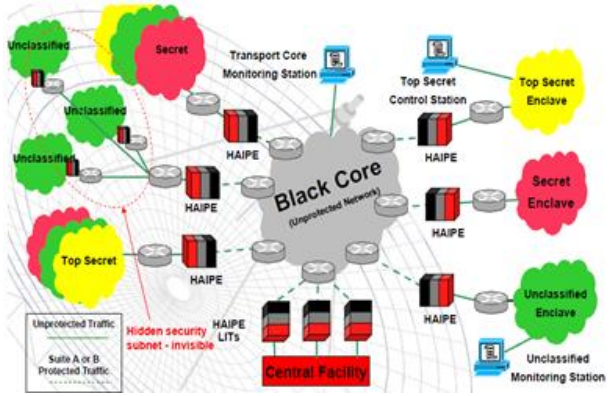
국방부가 2011년부터 2030년까지 추진하는 '국방개혁 307' 추진에 국방정보화가 중추적인 역할을 하게 될 것이라며 지휘구조 변화 등에 맞춰 정보화 기반도 강화해갈 것이라고 밝혔다.

홍규덕 국방부 개혁실장은 8일 서울 청량리 국방연구원에서 열린 9회 국방정보화 정책 세미나에서 "국방부가 추진하는 국방개혁 과제 73개 중 3개가 직접적인 정보화 과제이며 13개가 의존도가 높고 나머지 과제들도 정보화 없이는 성공할 수 없다"며 "국방부 전 부문에서 정보화 마인드를 가져야 하며 IT거버넌스 차원에서 정보화가 돼야 한다"고 말했다.

유철희 국방부 정보화기획관도 "73개 과제중 정보화 과제 3개라고 하지만 70여개 나머지 과제 모두 정보화와 연관이 있으며 때문에 국방정보화가 국방개혁의 성공과 효율적인 추진을 보장할 수 있다"고 말했다.

GIG(Global Information Grid) : Black Core Network 기술

- 미국의 경우, 국방성을 중심으로 'Black Core Network' 기술을 개발하여 2020년까지 국방네트워크의 고도화를 추진 중임
- 전세계 네트워크를 미국방성의 가용네트워크로 만들 수 있도록 논리적 망으로 구성하여 모든 전장자원 정보의 상호연결, NCW, 실시간 정보유통 가능
- 비밀등급별로 구분된 망을 Black Core라는 네트워크를 통해 안전하게 통합
- 전/평시에 전체 DoD 및 관련된 유관 조직의 전략적, 운영적, 전술적 작전 지원
- 공통적인 IP 인프라에서 다른 정보접근 요구를 갖는 단말들의 원활한 통신수행



※ 미국방성(US DoD) - GIG 3.0 Design Factors (11 Jan. 2011) 참조

→ All-IP기반의 군 정보통신망 구축을 위한 국산 핵심 네트워크 기술 개발 필요 !!

2. 과제 개요

연구 목표

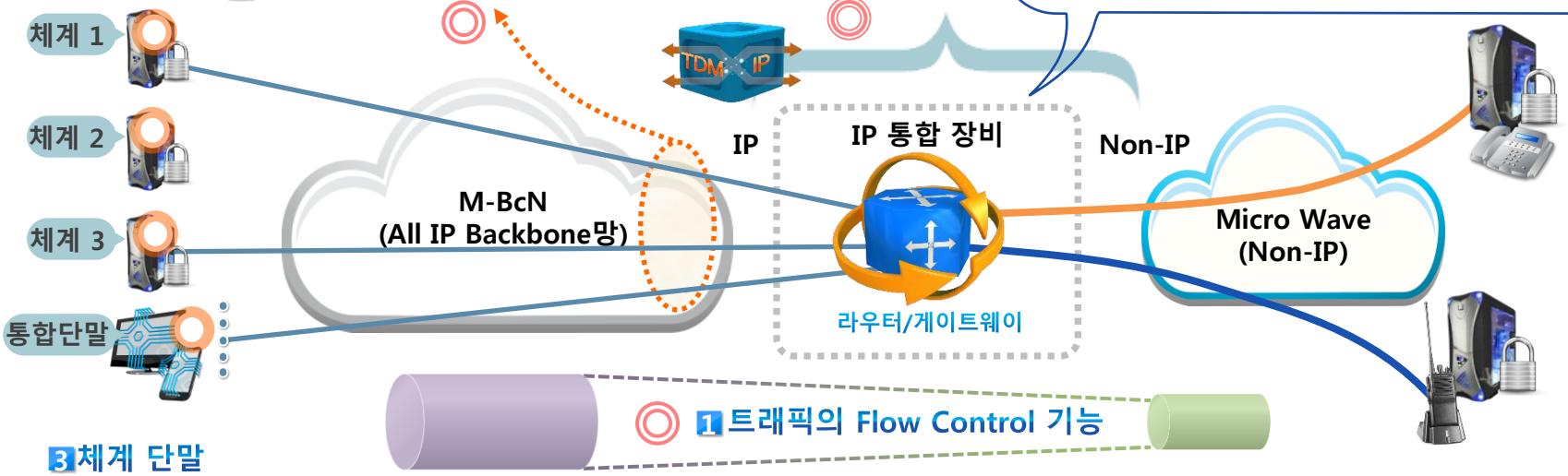
기술의 정의

트래픽 용량이 상이한 유선-무선 망의 이용 효율을 향상시키고, 목적별 개별망을 통합하기 위한 군(軍) 통신망 기술과 다기능 접속 장비 개발

- ✓ (미래부 재원) 국방IT융합과제
- ✓ (국방부 소요) 국군지휘통신사령부

<< 유.무선 및 다 체계 통합 Issues >>

1. 유 . 무선간의 용량 차이에 의한 트래픽 제어
2. 다중 체계(망)의 개별적 속성을 유지한 망 통합
3. 다 체계 접속 단말 소프트웨어
4. IP와 TDM 인터페이스의 연동



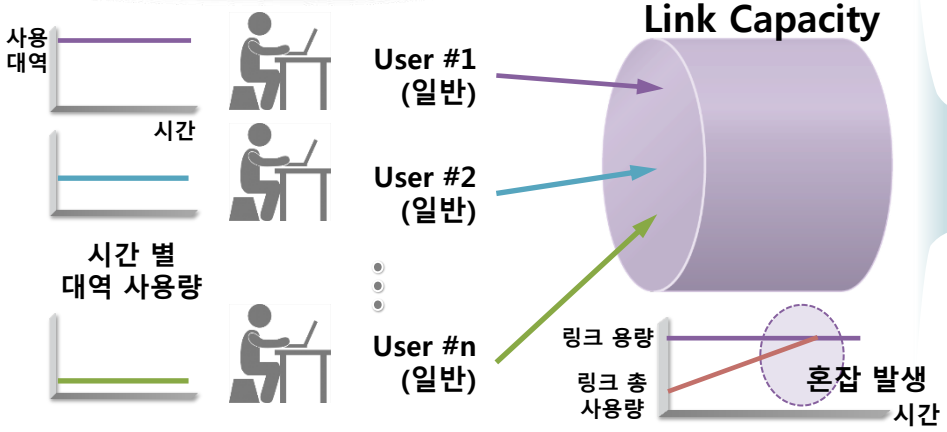
<< 개발 할 기술 >>

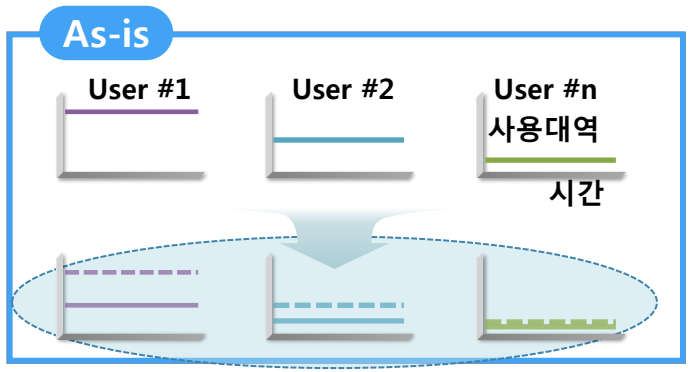
1. 동적, 지능적 대역 제어 기술
2. 다중 가상 네트워크 기술
3. 다 체계 접속 단말 소프트웨어
4. 다기능 접속 장비 기술

★최종산출물 (IP 통합 장비)

- : 라우터/게이트웨이에 탑재되는 대역 제어, 가상 네트워크 제어 소프트웨어
- : 단말에 탑재되는 Agent 소프트웨어
- : 다기능 접속 장비

지능적 대역 제어 기술



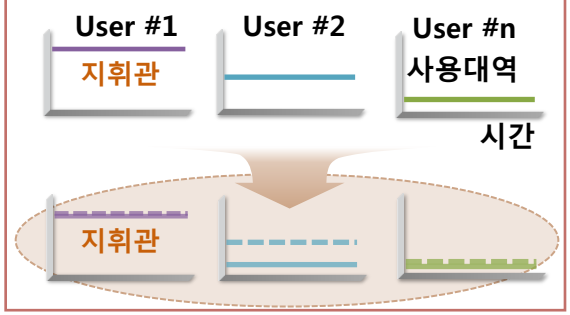


혼잡발생시 모든유저의 트래픽을 확률적으로 드랍
(대역을 거의 사용하지 않는 User #n의 패킷도 드랍)

고가의 무선 자원과 유선 자원을 융합시 또는 다체계 망을 통합시에 네트워크의 효율성 제고를 위한 동적/지능적 대역 제어 기술 개발

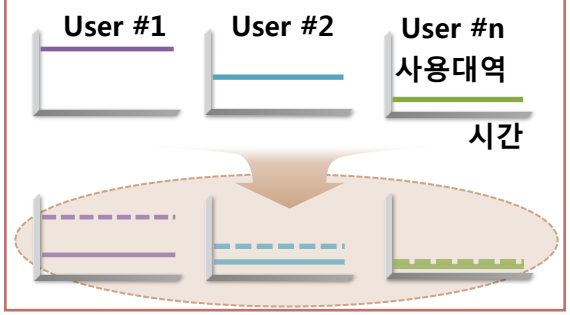
To-be

1 차등적 품질 보장기술



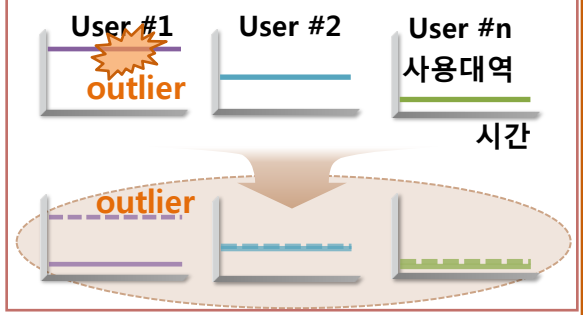
혼잡 발생시 차등적 품질 제공
(지휘관의 트래픽 보호)

2 균등 대역 분배기술



혼잡 발생시 대역 균등 분배
(적은 대역 사용자 보호 가능)

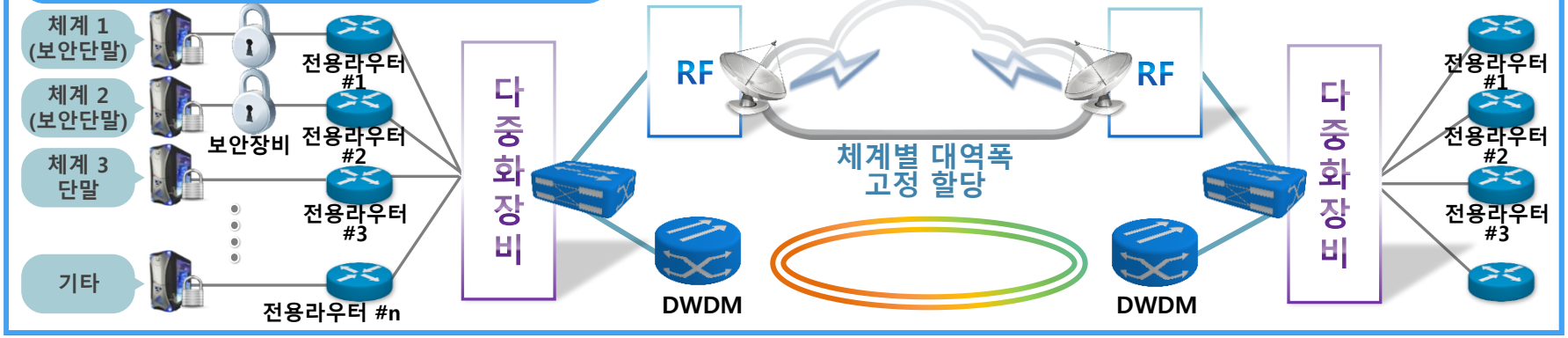
3 공평 대역 분배기술



혼잡 발생시 과도대역 사용유저(outlier로 명명)식별 후, outlier만 대역 규제

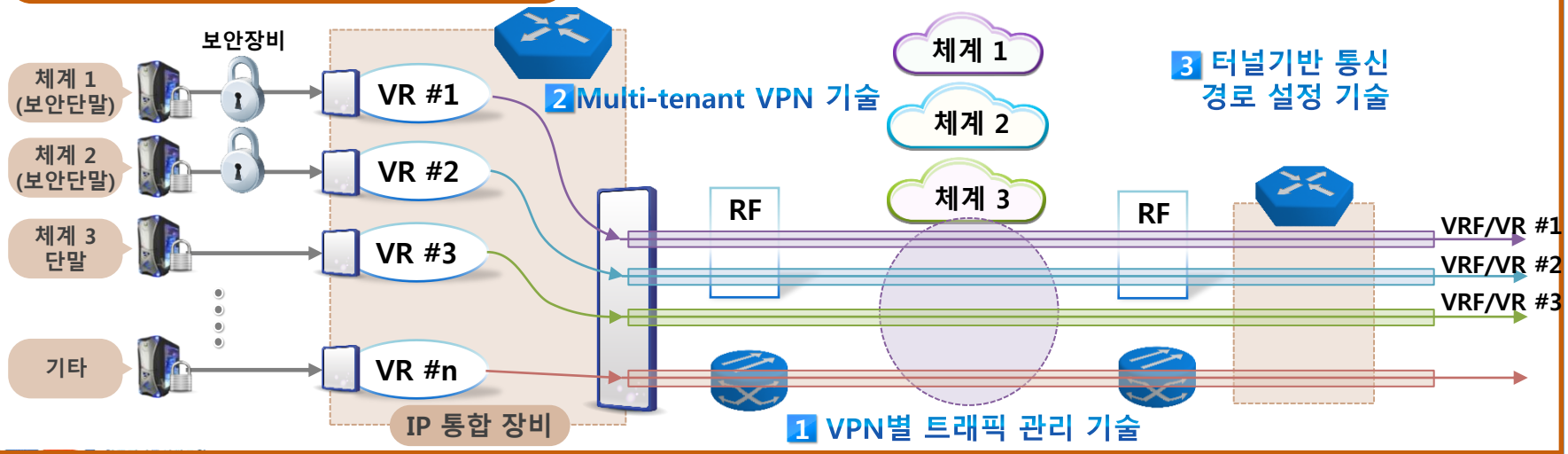
다중 가상 네트워크 기술

목적 별 물리적 개별 망 운용 (As-is)



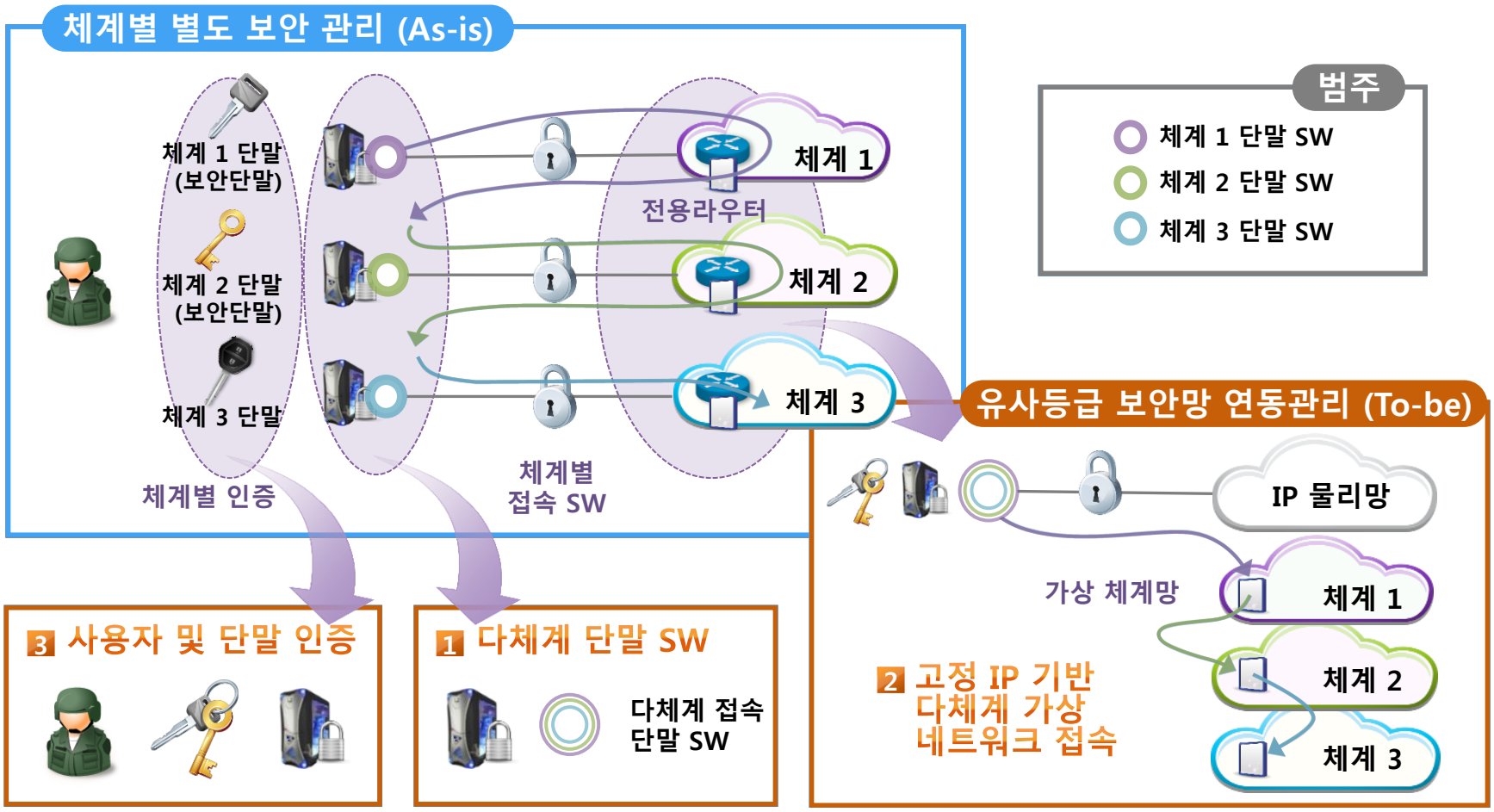
목적별 개별 물리망을 하나의 망으로 통합하는 한편, 터널 기반의 논리적 망 분리를 통해 각 체계별 요구 사항을 보장하는 다중 가상 네트워크 기술 개발

다중 가상 네트워크 기술 (To-be)



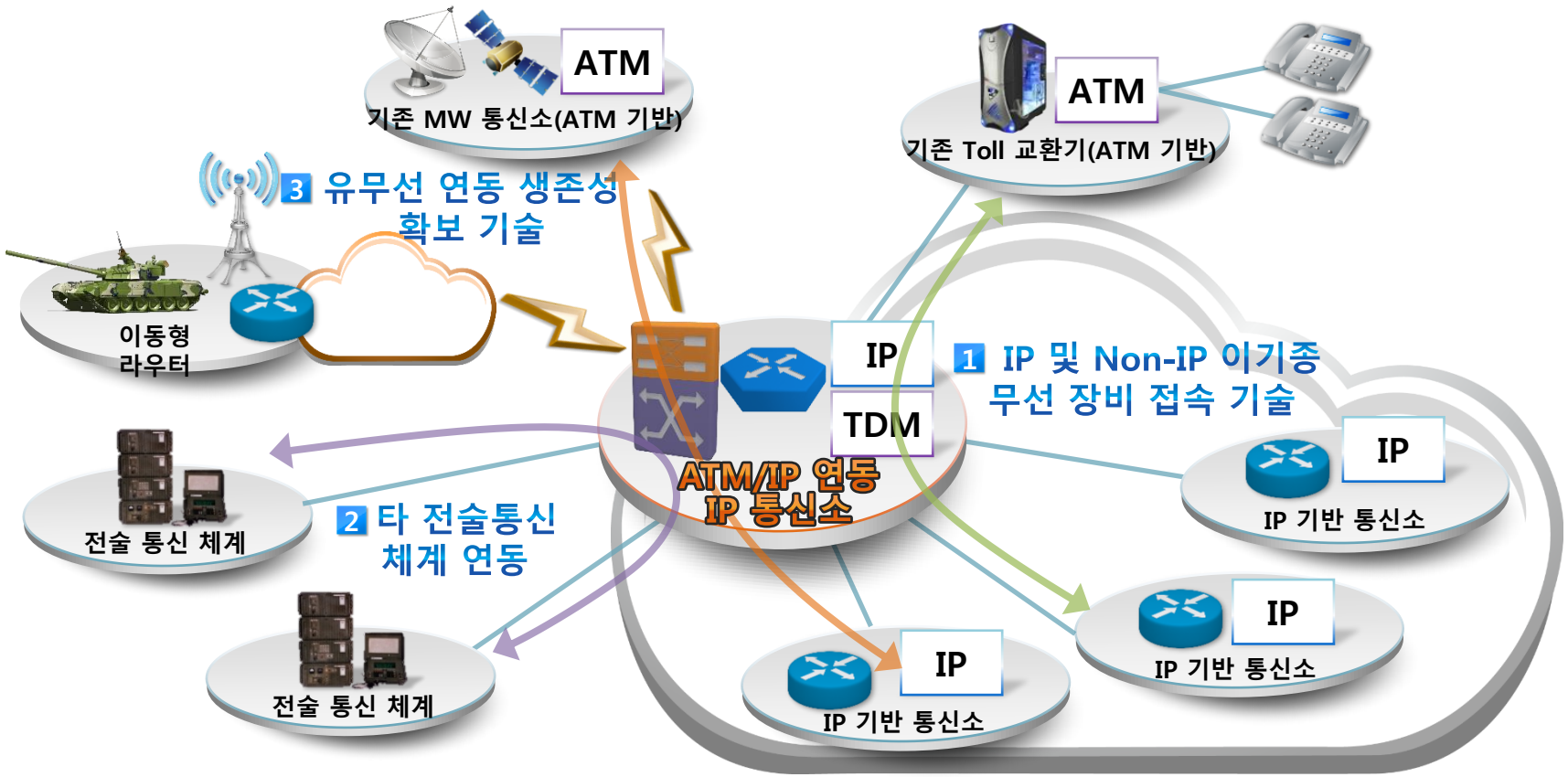
단말 소프트웨어 기술

다중 체계 및 망의 안전한 접속을 제공하기 위한 단말 소프트웨어 기술 개발



다기능 접속 장비 기술

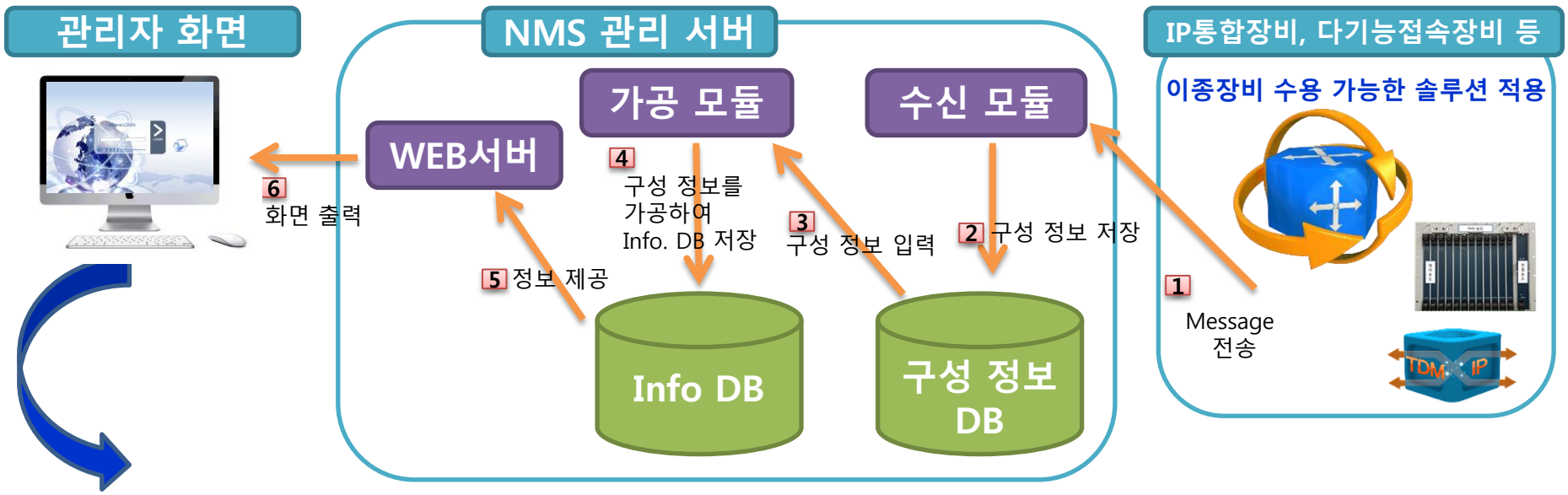
기존의 IP 및 Non-IP, 유무선 기반의 저속 및 TDM 서비스 연동을 위한 IP와 TDM의 다기능 접속 장비 기술 개발



2. 과제 개요

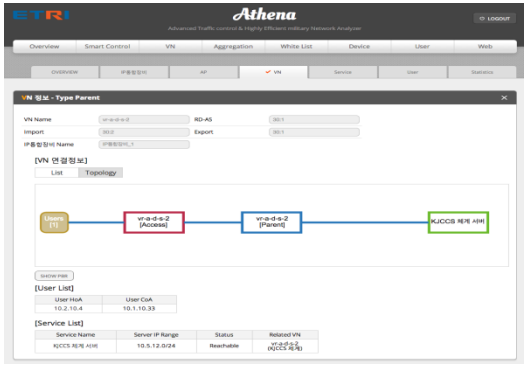
GUI 운용-뷰(1/3)

한 통신소의 이기종 장비에 대한 EMS/NMS GUI 시스템 개발

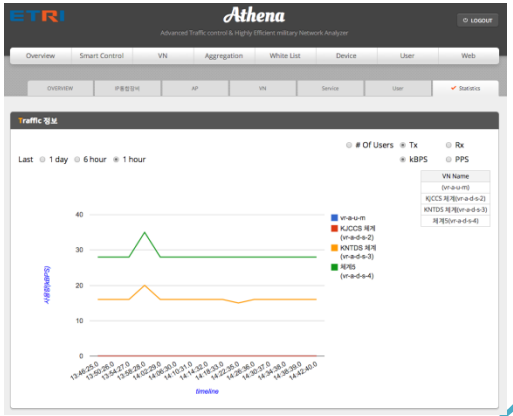


가상네트워크 운용 화면

가상네트워크 관리



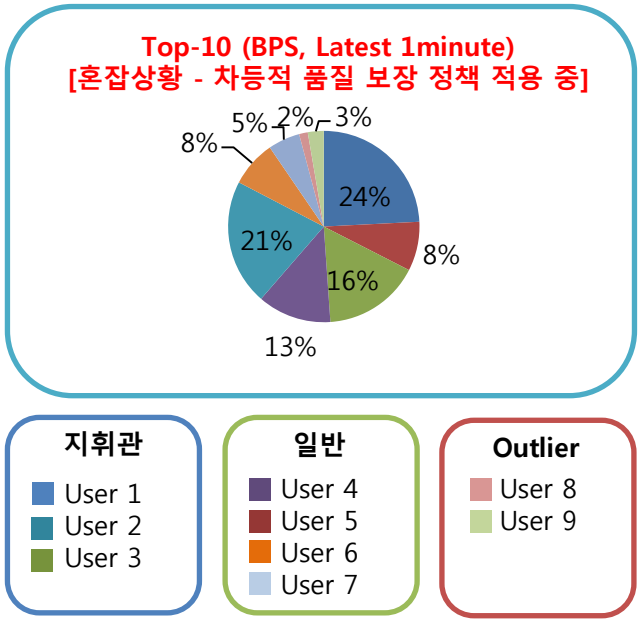
네트워크별 통계 정보 수집

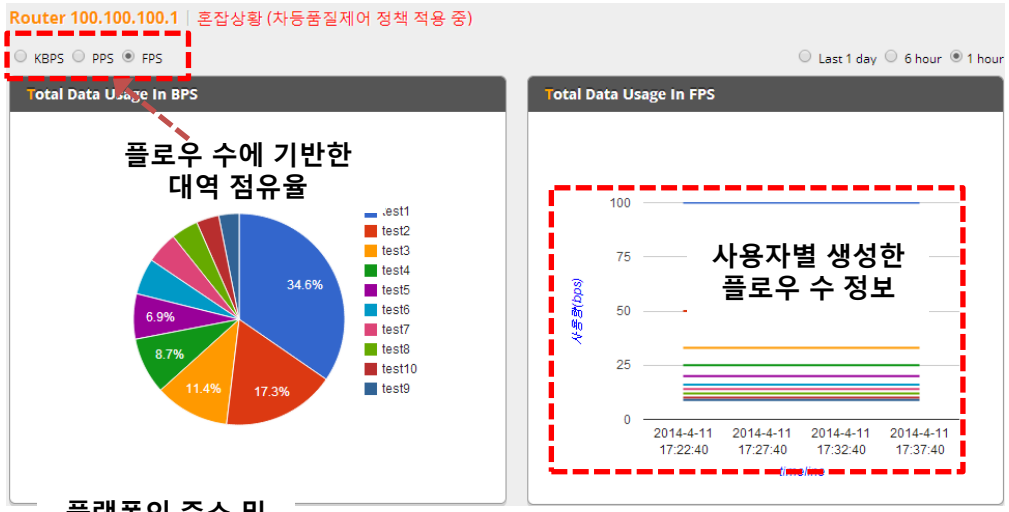


2. 과제 개요

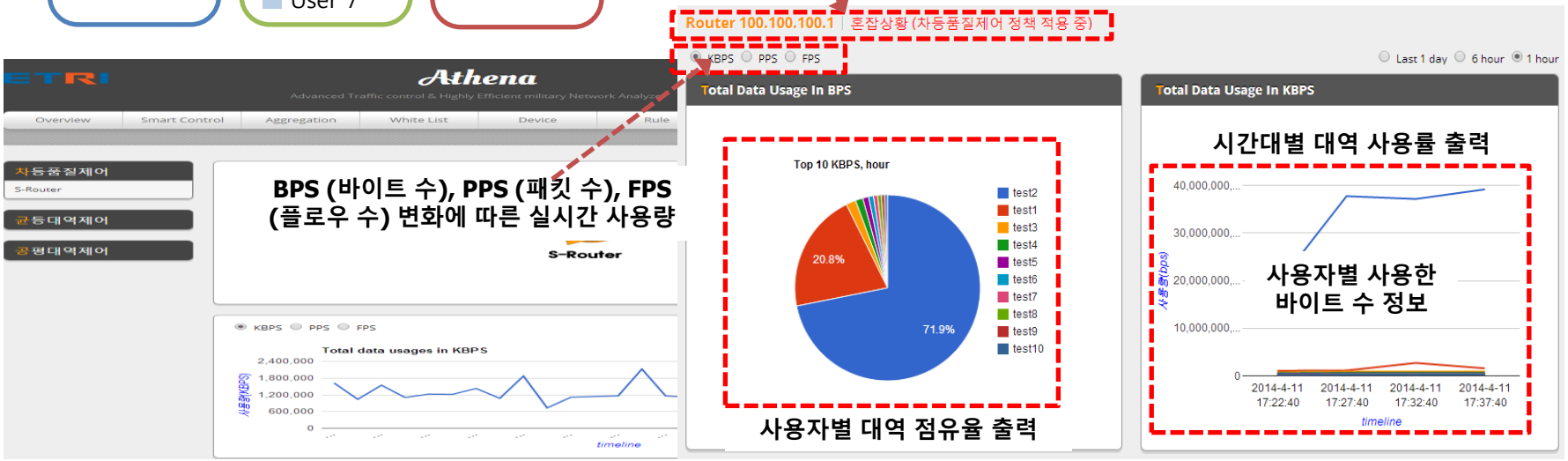
GUI 운용-뷰(2/3)

지능적 대역 제어 운용뷰 GUI 시스템





플랫폼의 주소 및
현재 상황 출력



2. 과제 개요

GUI 운용-뷰(3/3)

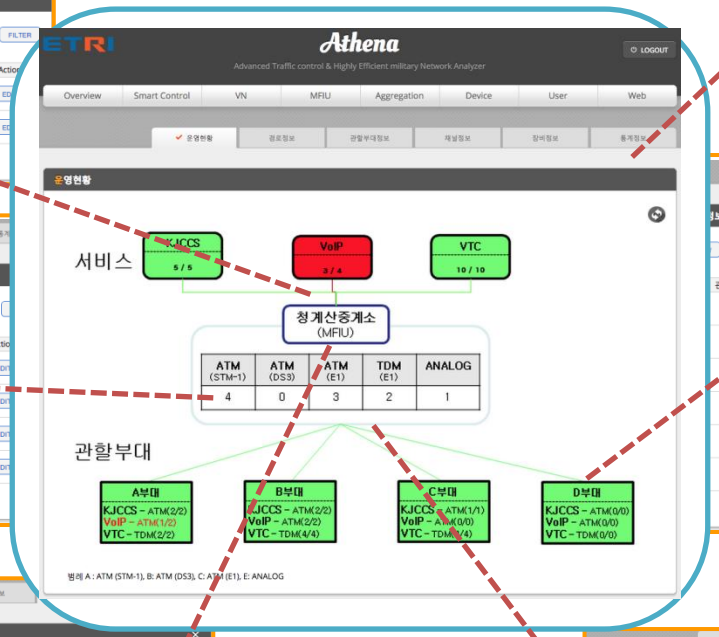
Non-IP/IP 자원 관리 및 운용뷰를 위한 EMS/NMS GUI 화면 정의

중계소 운영현황 화면

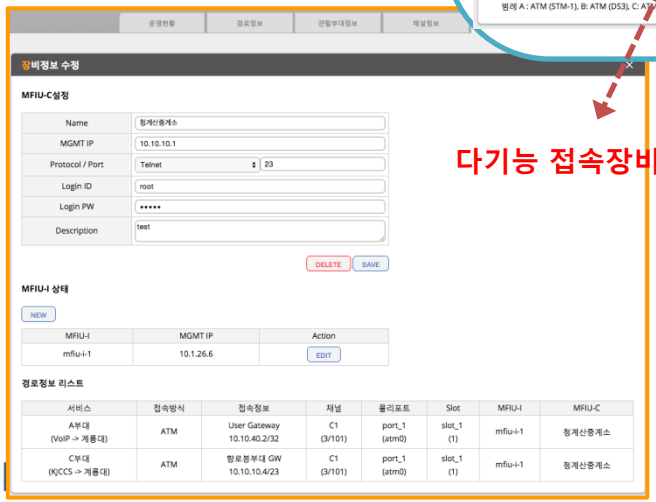
중계소에 연결된 관할부대 정보와 사용중인 서비스를 표시

사용중인 서비스의 경로 표시

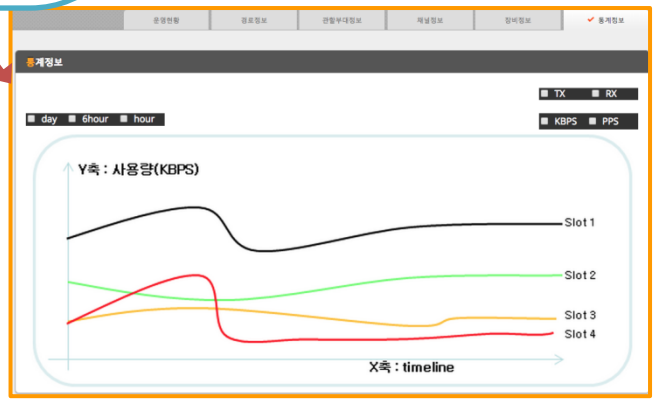
다기능접속장비 채널 정보 표시



중계소에 접속중인 부대정보 관리



다기능 접속장비 등록 및 관리



인터페이스별 통계 정보

2. 과제 개요

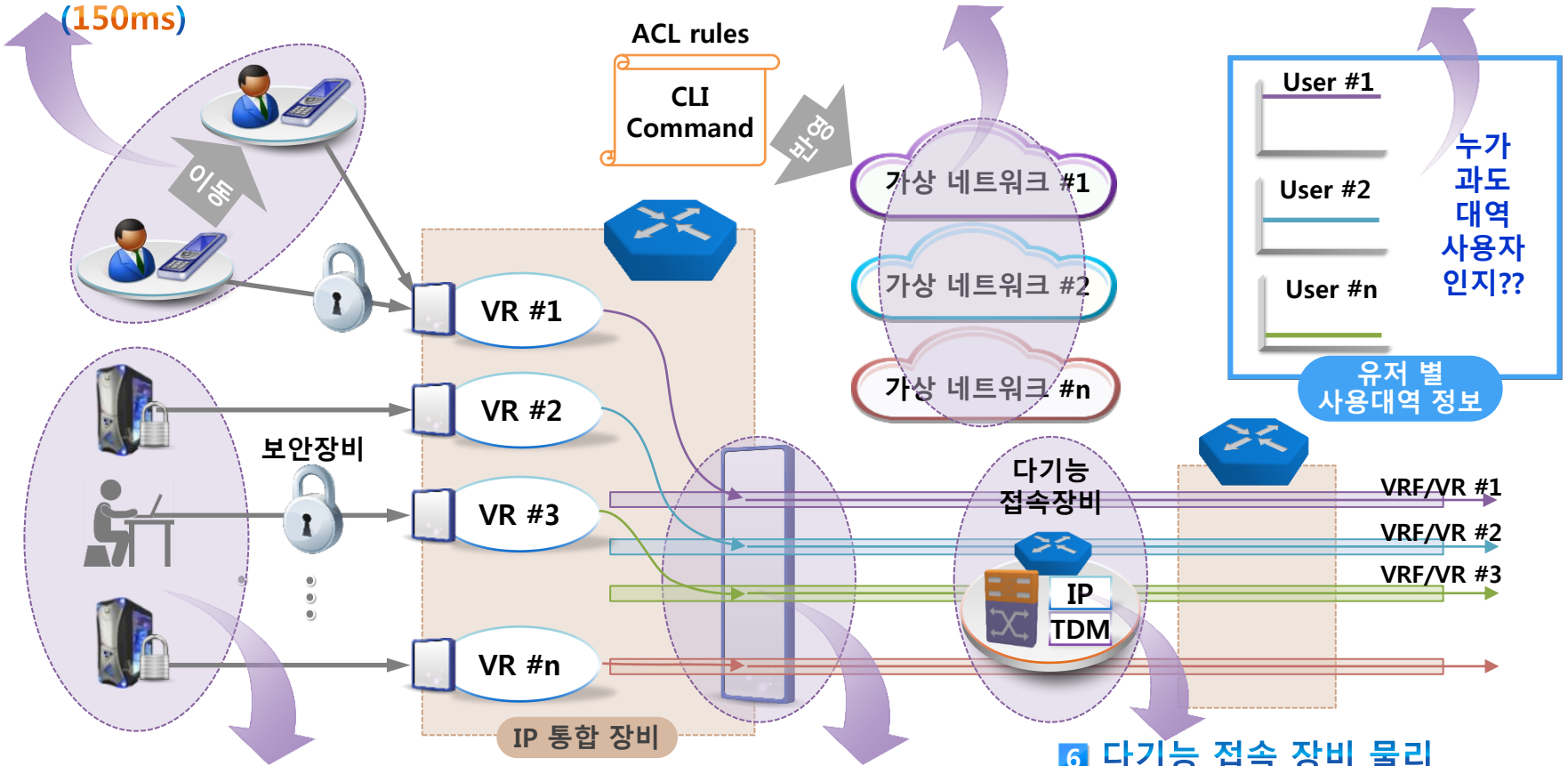
정량적 목표 개념

목적 : 고품질 융합서비스를 위한 국방 기반체계 연동 기술 확보

5 단말 기반의 이종망 핸드오버 지연 (150ms)

1 확정적 품질 보장을 위한 제어 정책 설정 룰 수 (4K개 이상)

2 과도 대역 사용자/서비스 식별 알고리즘의 정확성 (95%)



4 가상 네트워크에 수용 가능한 총 가입자 수 (20K 가입자)

3 체계통합을 위한 다중 가상 네트워크 터널 수 (64개 이상)

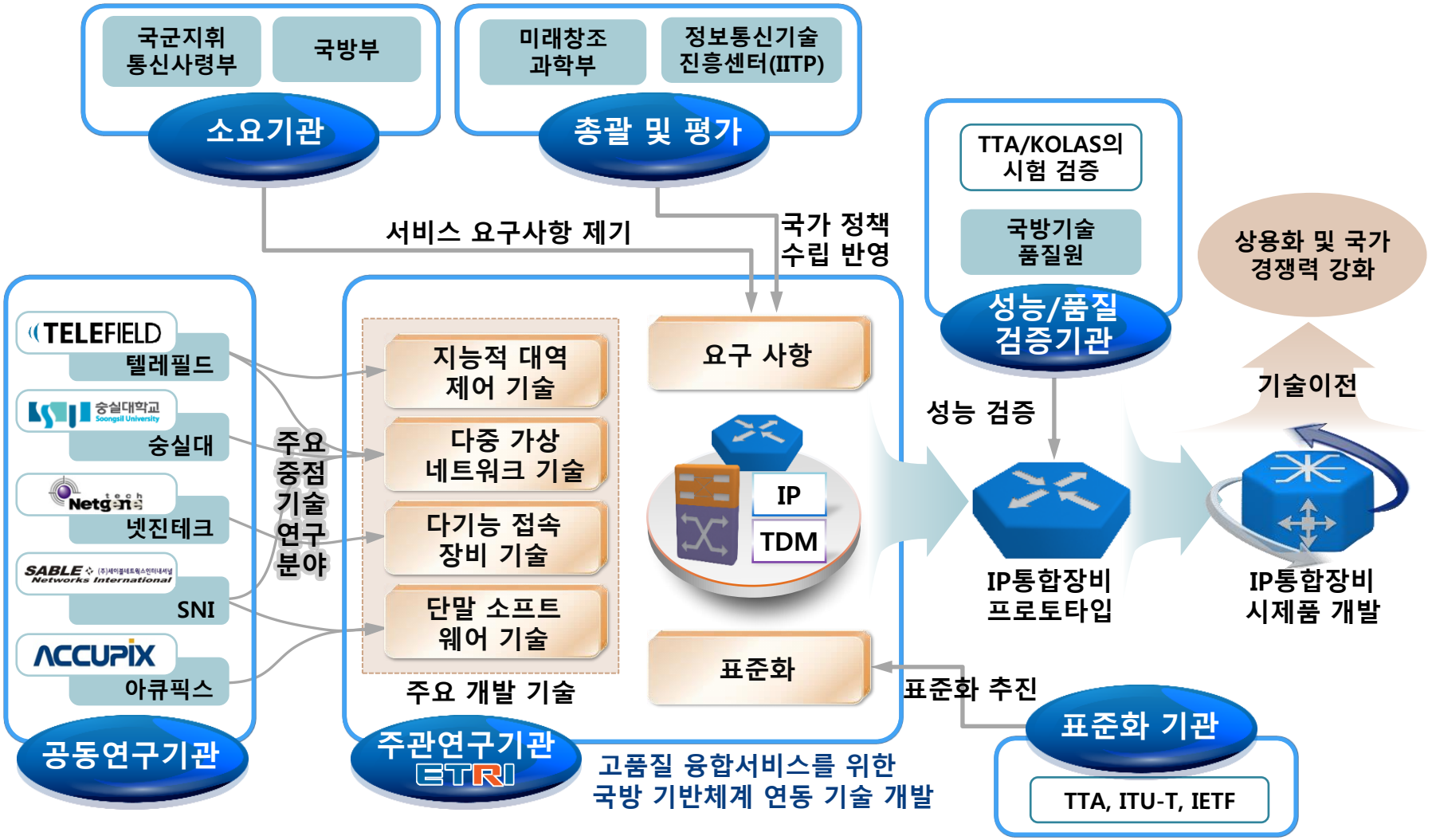
6 다기능 접속 장비 물리 인터페이스 성능 (Line Rate 100%)

7 다기능 접속 장비 장시간 신뢰성 시험 (24시간 장비 가동중 패킷손실 0%)

3. 추진전략

개발 추진 체계

- 국방부 및 합동참모본부(국군지휘통신사령부)와 긴밀한 협의를 통해서 군의 요구사항 수렴
- 네트워크 장비상에서의 원천기술 개발이 필요하므로 네트워크 장비 개발 업체와의 공동개발 수행



※ 국방 품질 담당기관을 두고 각 단계별 결과물에 대한 품질관리

4. 주요성과 – 개발 환경 구축

선도적 개발 환경 구축

PE Web 개발환경 구축

- **PE (Process Engineering) Web 환경 구축 및 운영 → http://pe.etri.re.kr**
  - 공개 SW를 활용한 개발 환경구축
    - CVS → 소스 관리
    - Apache : Web → 사용자 접속 관리
    - MySQL : DataBase → DB 관리
  - 각 개발 단계 별 관리를 통한 **연구개발 생명주기관리**
  - 시스템 명, 사업명 단위의 **형상 관리**
  - **문서관리** : **DMS** (Document Management System)
  - 소스 및 패키지 **버전 관리** : **CVS** (Concurrent Version System)
  - **문제점 및 이슈 관리** : **ECR** (Engineering Change Request) 등록
  - Build 및 package 관리 (Daily **Build**)
  - 사용자 관리 (Management Function)
  - 패키지 관리와 연동된 진도 관리

→ 기술 문서, 소스 레벨의 Cross Checking 가능, 개발 이력(History) 자동 관리 가능

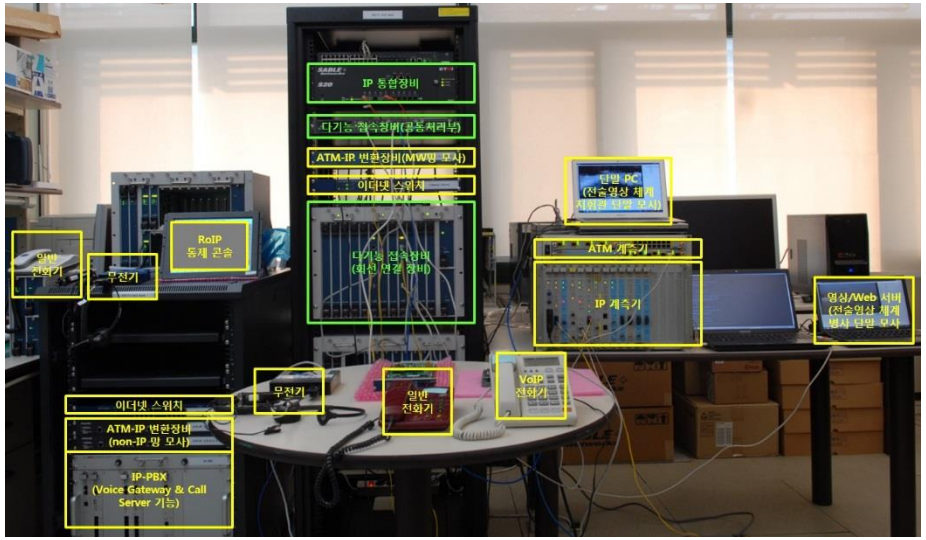
※ 상용 제품을 위한 개발환경의 선도적 구축으로 목표 달성 가능성 제고 !!

4. 주요성과 – 연동시험 환경 구축

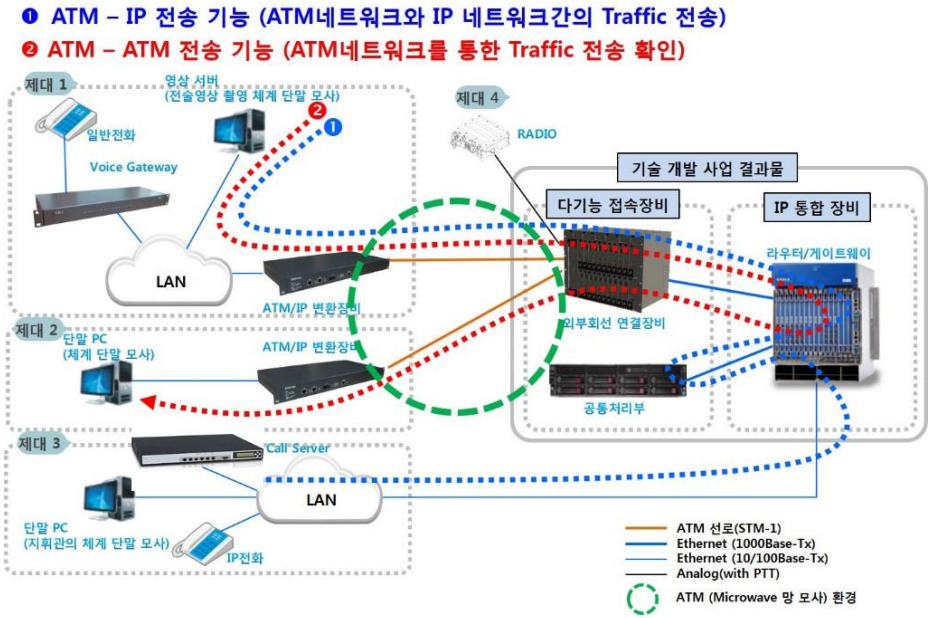
실험실내 시험환경 구축

IP 기반의 기반체계 통합망 연동시험 및 기능검증 시험환경 구축

- 유-무선(IP-TDM) 및 다체계 전술망 모사 → 실제 환경을 유사하게 모사할 수 있는 시험환경 구축
  - ATM→IP, ATM→ATM 전송기능 시험, ATM/IP 변환장비는 microwave망을 모사
- VoIP(유선망)와 RoIP(무선망) 통화 연동시험 환경
- 영상 서비스를 통한 체계별 서비스 연속성/생존성 기능시험 환경
- 계측기를 이용한 트래픽 폭주(전시상황) 모사 환경



시험 환경 구축



IP-ATM(Microwave) 망 연동 및 기능 시험 모사 환경

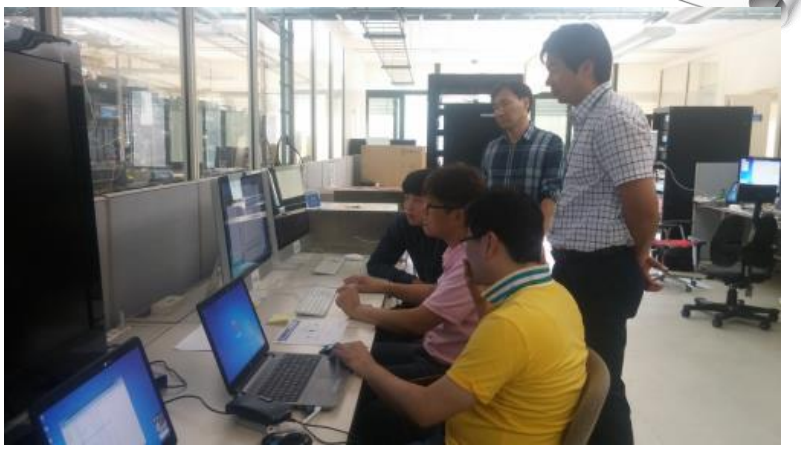
※ 연동시험 환경 구축 → 국방망 연동시험을 모사한 시연환경 구축으로 목표 달성 가능성 제고 !!

4. 주요성과 - 시험검증

결과물의 제3자 검증

정량적 항목에 대한 KOLAS 인증기관의 제3자 검증

- 과제 정량적 항목 6개 항목에 대한 제3자 검증 완료
- KOLAS 인증 기관 : 한국아이티평가원
- 시험 일시 및 장소 : 10/5 ~ 10/8, ETRI



항목	3자 검증 결과
확정적 품질 보장을 위한 제어 정책 설정 룰 수	4K개 이상 정책 설정 가능 (합격)
체계통합을 위한 다중 가상 네트워크 터널 수	70개 가상 네트워크 터널 생성 및 동작 확인 (합격)
가상 네트워크에 수용 가능한 가입자 수	20000가입자 서비스 수용 가능 여부 확인 (합격)
단말 기반의 이종망 핸드오버 지연 시간	유선→무선, 무선→유선 핸드오버 지연 50ms 이내 (합격)
다기능 접속 장비 물리 인터페이스 성능	256Byte 패킷 기준 Interface Line Rate의 100% (합격)
다기능 접속 장비 장시간 신뢰성 시험	24시간 이상 시험 결과, 99.999998%신뢰성 (합격)

시험 결과

시험성적서

KSEL 한국아이티평가원	성적서 번호	시험 유형
주소: 서울시 송파구 가락동 124-20 5층 Tel: 02-400-8221, FAX: 02-400-8212	KSEL-PT-R-2015-32 (페이지 1/6)	KSEL Tested

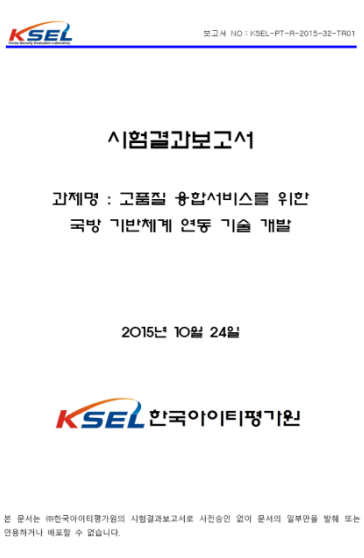
1. 신청기관
   - 기 관 명 : 한국전자통신연구원
   - 주 소 : 대전광역시 유성구 가정로 218
   - 신청일자 : 2015년 09월 03일
2. 시험성적서의 용도 : 수요처 제출용
3. 시험대상 : 고품질 융합서비스를 위한 국방 기반체계 연동 기술
4. 시험환경 : 상온
5. 시험기간 : 2015년 10월 05일 ~ 2015년 10월 08일
6. 시험방법 : ㈜한국아이티평가원과 한국전자통신연구원(클라우드네트워킹 연구실)이 평등으로 제정한 시험기준 및 절차에 따라 시험
7. 시험결과 : 시험결과 및 시험결과보고서(KSEL-PT-R-2015-32-TR01) 참조

확 인	시험자 성명 : 전 수 혁	기술책임자 성명 : 여 용 기

2015 년 10 월 26 일

주식회사 한국아이티평가원 대표이사

제3자(KOLAS 인증기관) 시험성적서



KSEL 한국아이티평가원 보고서 NO : KSEL-PT-R-2015-32-TR01

시험결과보고서

과제명 : 고품질 융합서비스를 위한 국방 기반체계 연동 기술 개발

2015년 10월 24일

KSEL 한국아이티평가원

본 문서는 ㈜한국아이티평가원의 시험결과보고서로 사전승인 없이 문서의 일부만을 발췌 또는 인용하거나 배포할 수 없습니다.

결과보고서

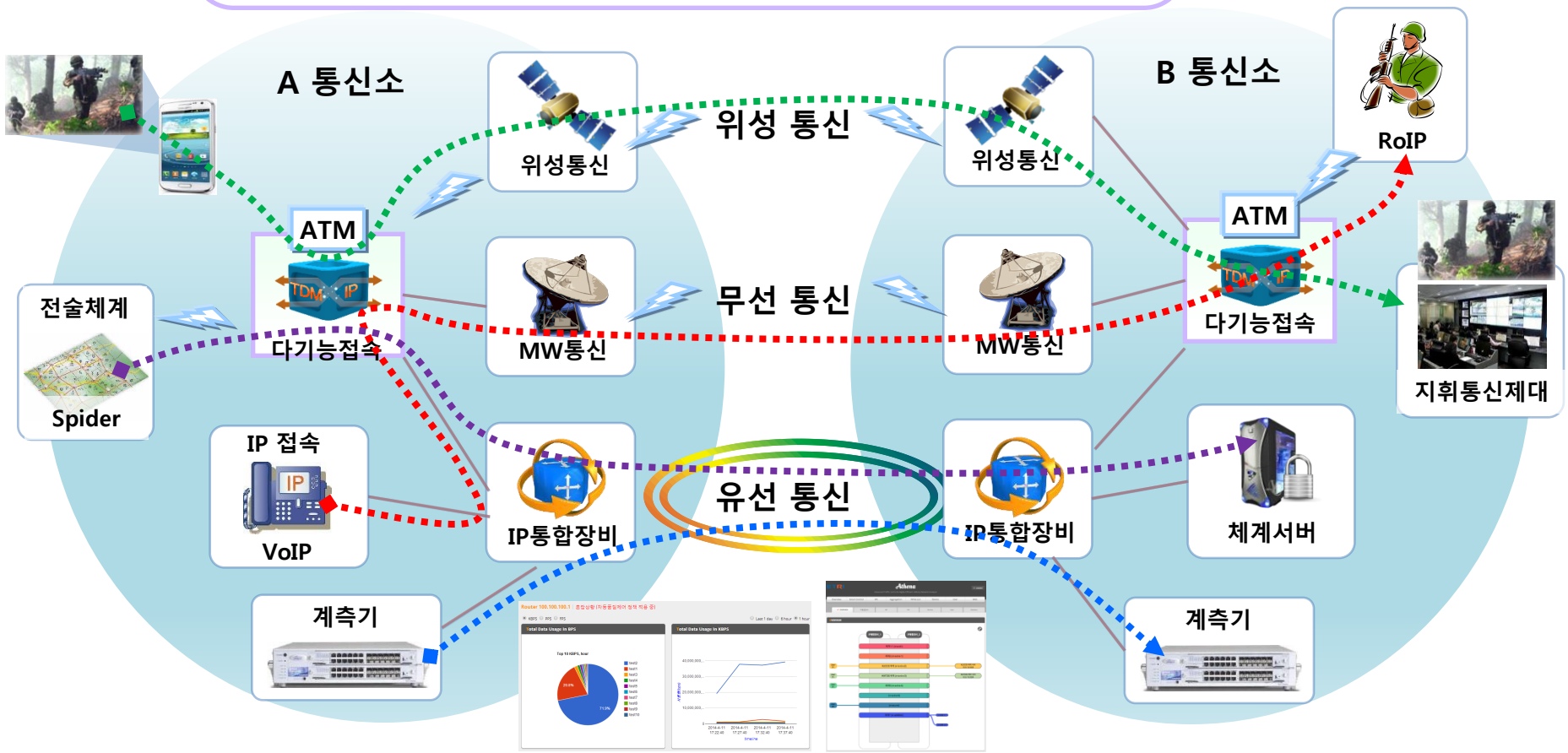
4. 주요성과 – 국방망 연동시험

연동시험 개념

All-IP 기반의 체계 통합망 연동시험 및 기능 검증

- 유-무선(IP-TDM) 및 다체계 전술망 모사
- VoIP(유선망)와 RoIP(무선망) 통화 연동시험 환경
- 영상 서비스를 통한 체계별 서비스 연속성/생존성 기능시험 환경
- 계측기를 이용한 트래픽 폭주(전시상황) 모사 환경

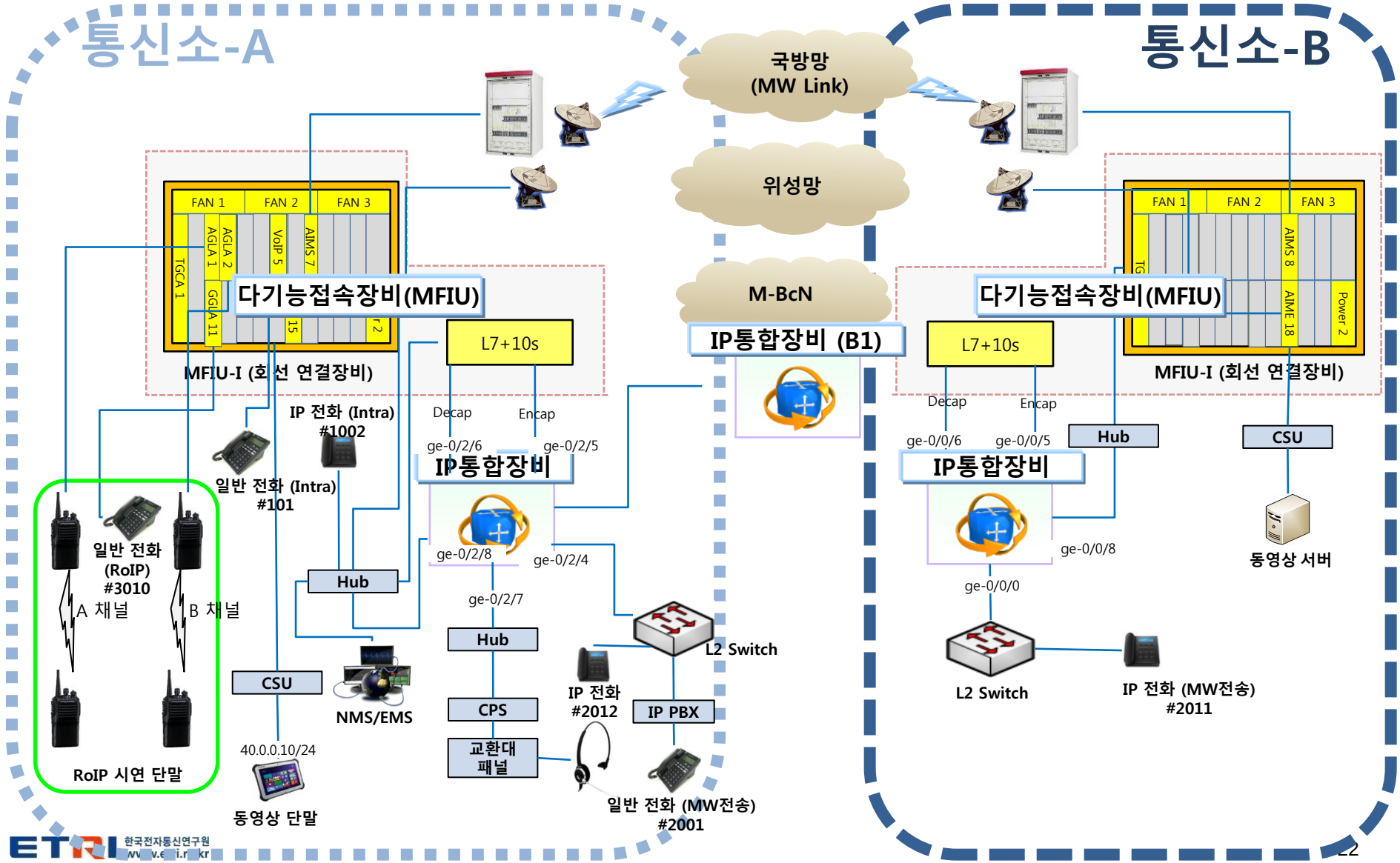
■ 연동시험 일정
✓ (일정) 11.9~11.13
✓ (장소) 국군지휘통신사 사령부내 2개 통신대대



※ 과제 개발 결과물에 대한 국방망 연동시험

국방망 연동시험 구성도

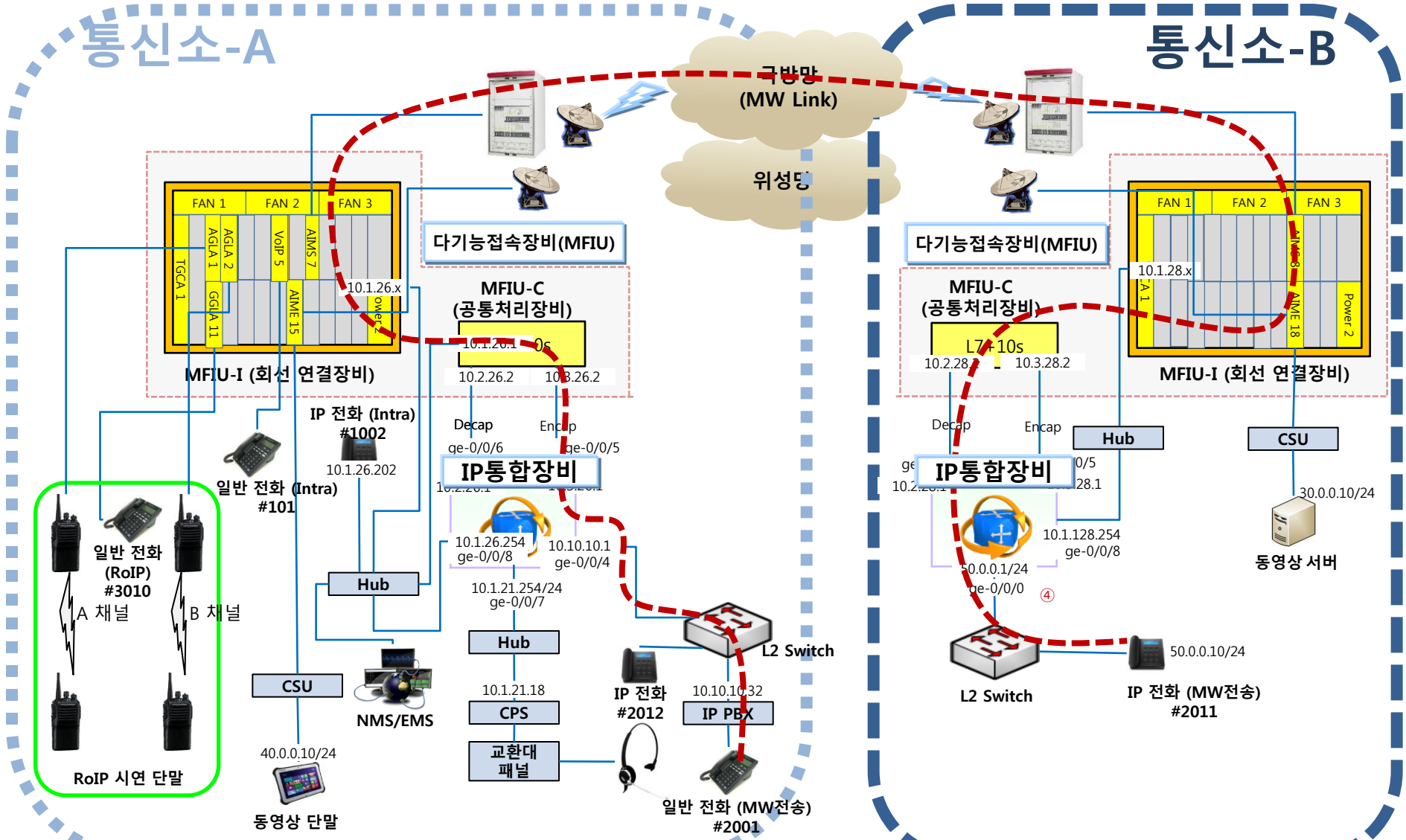
국방망 연동시험 : MW/위성 망 접속 및 군-무전기 연동 시험



IP↔Non-IP (MW/위성) 접속

주요 기능 (1)

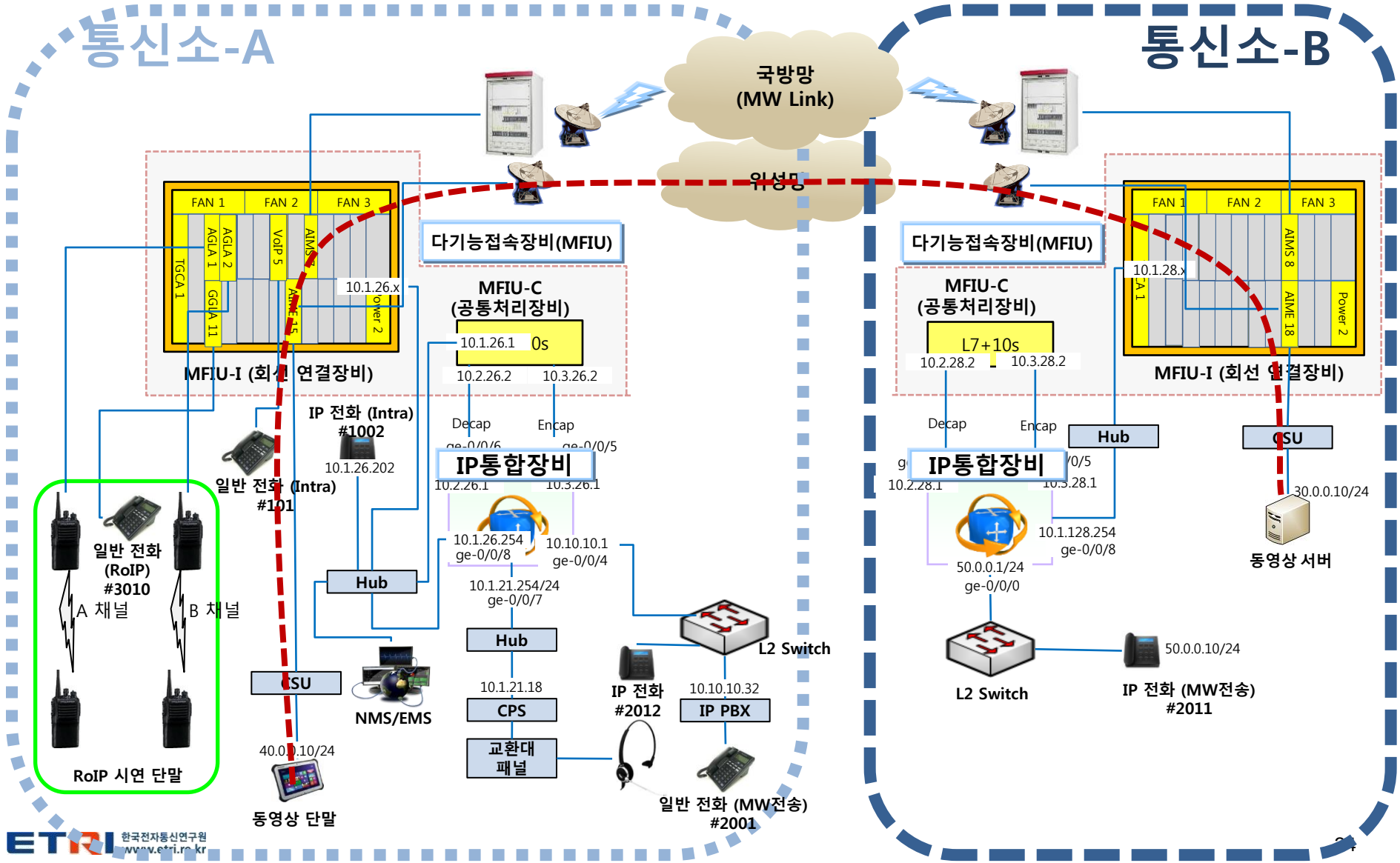
① 음성 통화 시연 –MW망 경유 일반전화↔IP 전화



IP↔Non-IP (MW/위성) 접속

주요 기능 (2)

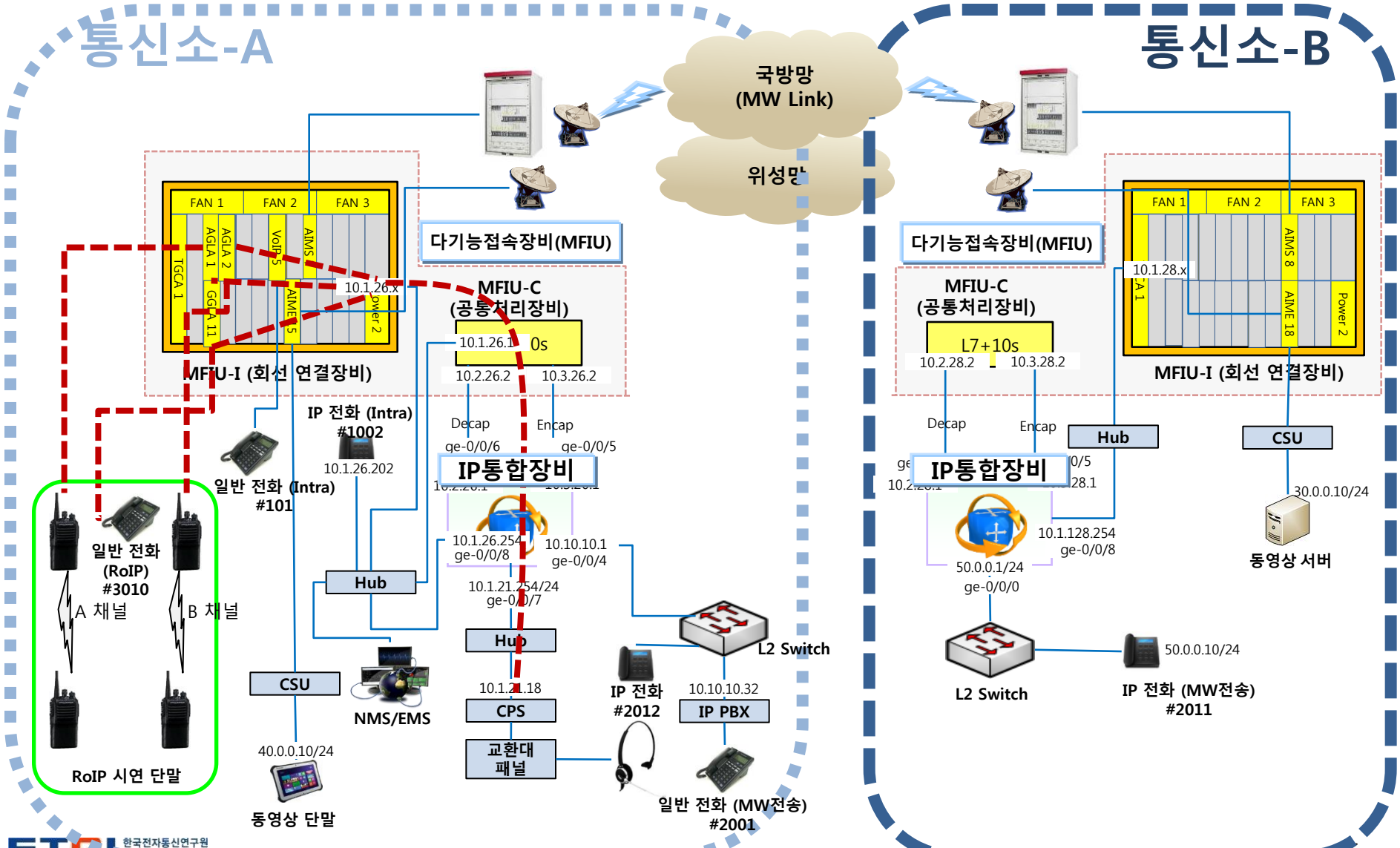
② 영상 전송 시연 – 위성망 경유 E1회선



IP↔Non-IP (MW/위성) 접속

주요 기능 (3)

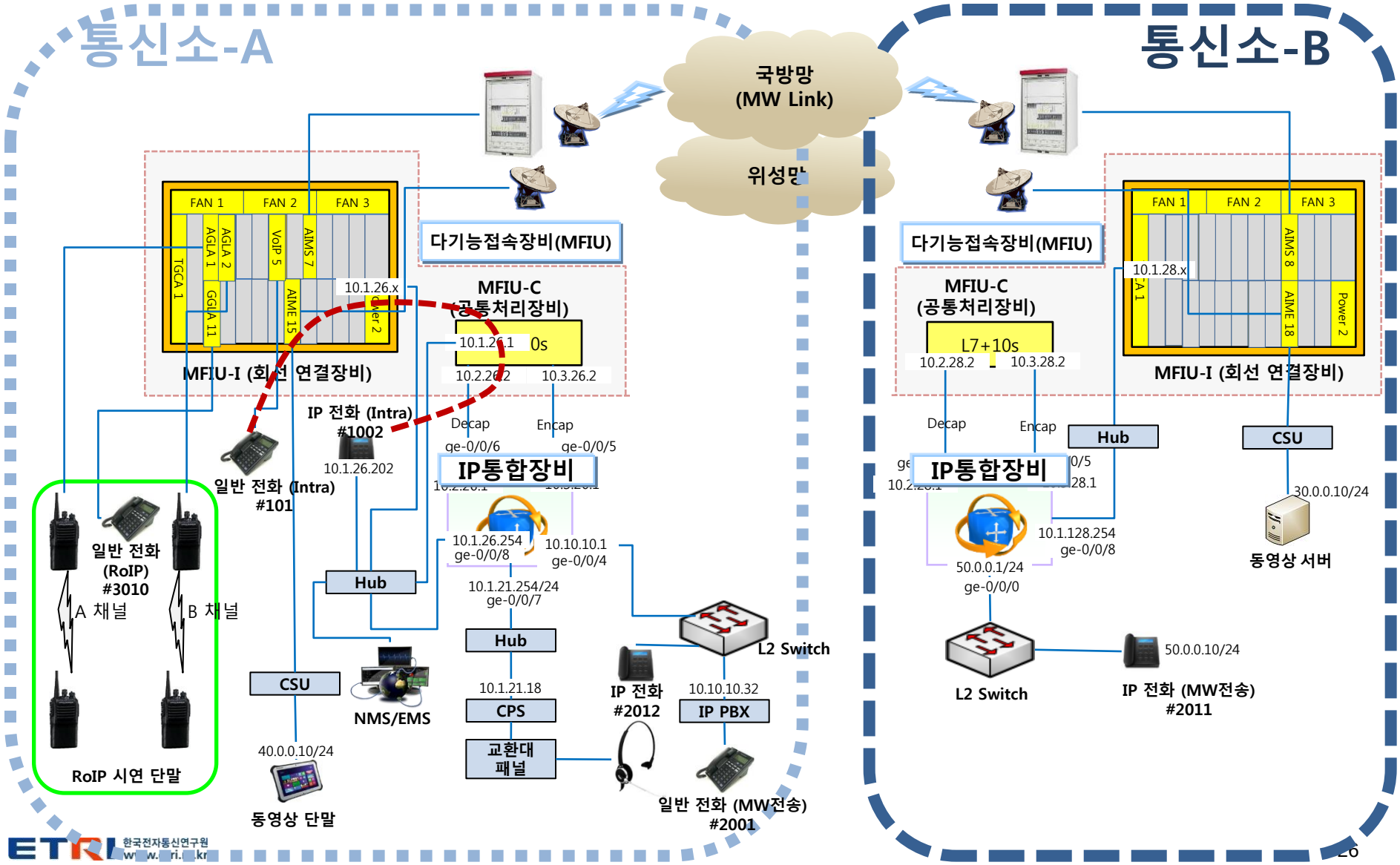
③ RoIP 시연 – 이종 주파수 무전기 그룹간 통화, 유선전화↔무전기 통화



IP↔Non-IP (MW/위성) 접속

주요 기능 (4)

④ Intra-site IP-PBX: 부대 내부 일반전화 ↔IP전화 교환 (간이 IP-PBX)



시연 및 언론 홍보

과제 결과물에 대한 국망방 연동 시연회 및 홍보

- 일시 및 장소 : 2015. 11. 13. (금), 국군지휘통신사령부내 통신대대
- 합동참모본부, 육군본부 및 국군지휘통신사령부 관련 장교들에게 시연
- 국방망 연동 서비스 시연
  - 지능적 고품질 서비스 연동
  - 다체계 가상 네트워크 서비스 연동
  - IP↔Microwave (non-IP) 접속 서비스
  - 단말 서비스 연동

국방망 연동 시연회

연동시험 결과 시연회

디지털타임스 2015년 11월 19일 목요일 002면 종합

군 통신망 'IP기반망'으로 통합 운용

ETRI, IP통합장비·다기능 접속장비 개발 … 내년 상반기 상용화

용도별로 서로 달라 통합 운용이 어려웠던 군 통신망을 IP 기반으로 통합해 사용할 수 있는 기술이 개발됐다. 군 통신망의 효율성과 경제성을 높이고 외산 위주의 군 통신망을 국산 기술로 대체하는 계기가 될 전망이다.

한국전자통신연구원(ETRI)은 넷진테크, SNI, 아큐픽스, 텔레필드, 숭실대 등과 공동으로 국방망에 활용할 수 있는 'IP 통합장비'와 '다기능 접속장비'를 개발하는 데 성공했다고 18일 밝혔다.

IP 통합장비를 이용하면 용도에 따라 100개 이상의 다양한 군 통신망 중 유사하게 사용되는 망(최대 64개)을 하나의 장비로 통합할 수 있다. 네트워크 가상화 기술을 적용해 서로 다른 망을 하나로 묶어 사용할 수 있다. 다기능 접속장비는 그동안 IP나 ATM(비동기전송모드) 등 인터페이스가 서로 달라 연동하기 어려웠던 군 통신망이나 전술망, 국방 무선망 등 서로 다른 망을 IP 기반으로 통합·연동하는 데 쓰일 수 있다.

유사시 군 통신이 끊기지 않도록 '올-IP 융합망'으로 활용할 수 있다.

이 기술은 최근 국방기술품질원의 품질관리 연동시험을 성공적으로 마쳤으며, 지난 13일에는 ETRI와 국군지휘통신사령부 전문가들이 참석한 가운데 시연회가 이뤄졌다. ETRI는 신속한 지휘와 의사결정이 가능한 미래 네트워크 중심전(NCW)에서 효과를 발휘할 수 있을 것으로 기대하고 있다.

네트워크 장비 업체 등에 관련 기술을 이전해 내년 상반기 상용화할 계획이다.

박혜숙 ETRI 클라우드네트워킹연구실장은 "이 기술은 IT에 기반한 군 네트워크 구축 가능성을 한층 높여주고, 국방·IT 융합기술의 실질적 사례가 될 것"이라고 말했다.

대전=이준기기자 bongchu@dt.co.kr

전자신문 2015년 11월 19일 목요일 024면 전국

유사시에도 전송 중단 없는 '군통망'

ETRI, 넷진테크·숭실대 등 공동연구 'IP통합장비' '다기능 접속장비' 개발

물리적 유·무선망 64개 하나로 통합 내년 상용화 목표…기술이전 추진도

군 통신망을 64개까지 하나로 통합할 수 있는 첨단 네트워크 기술이 개발됐다.

한국전자통신연구원(ETRI·원장 김흥남)은 넷진테크, SNI, 아큐픽스, 텔레필드, 숭실대 등과 공동으로 국방망에 활용 가능한 'IP통합장비' 및 '다기능 접속장비' 개발에 성공했다고 18일 밝혔다.

이 기술은 국방통신망 핵심 네트워크 기술이다. 물리적 유무선망 64개를 하나로 통합할 수 있다.

기존 망은 망마다 인터넷프로토콜(IP)이나 비동기전송모드(ATM) 등 인터페이스가 서로 달라 연동이 어려웠다.

연구진은 군통신망 통합 연동을 위해 '다기능 접속장비'를 개발했다. 유사시에도 망 전송이 중단되지 않는 '올-IP'융합망 개념을 제공한다.

ETRI와 관련업체는 지난 9일부터 닷새간 경기도 과천 국군지휘통신사령부에서 연동시험을 실시했다. 연동시험에서는 △네트워크 효율성 제고를 위한 동적·지능적 대역제어기술 △목적별 개별망을 통합할 수 있는 다체계 가상네트워크 서비스 연동 △IP와 Non-IP(마이크로웨이브 및 위성)망 다기능 접속 서비스 연동 △다체계 접속을 제공하는 단말 소프트웨어 서비스 연동을 중점 체크했다.

연구진은 이 기술개발로 군 통신 네트워크 효율성과 경제성이 좋아질 것으로 기대했다. 군 통신망 보안도 한층 강화될 것으로 내다봤다.

내년 상반기 상용화를 목표로 하는 ETRI는 업체만 원하면 향후 네트워크 장비업체 등에 추가 기술이전도 추진할 예정이다.

박혜숙 ETRI 클라우드네트워킹연구실장은 "외산 기술 의존도가 높은 우리나라 자주 국방 실현을 앞당기는 계기가 될 것"이라고 전망했다.

조인희 국군지휘통신사령관도 "네트워크 작전을 주도하는 사령부로 발전하는 초석을 마련한 셈"이라고 덧붙였다.

이 기술은 미래창조과학부 IT·SW융합산업원천기술개발사업과 국방부 국군지휘통신사령부 지원을 받아 개발됐다.

대전=박희범기자 hbpark@etnews.com

2015년 11월 19일 목요일 020면 정보통신

국방망 보안 강화 기술개발

…다기능 접속장비

…이 군대 안에서 사용하는 …망을 인터넷(IP) 기반으로 …는 기술을 개발했다. 앞 …식 공유와 신속한 지휘 및 …가능한 네트워크 중심전에서 효과를 발휘할 수 있을 전망이다.

18일 한국전자통신연구원(ETRI)은 ㈜넷진테크, ㈜SNI, ㈜아큐픽스, ㈜텔레필드, 숭실대 등과 공동으로 국방망에 활용 가능한 'IP통합장비'와'다기능 접속장비' 개발에 성공했다고 밝혔다.

이 기술은 국방통신망의 핵심 네트워크 기술로 여러 개의 물리적 유·무선망을 하나의 망으로 통합할 수 있다. 이를 국방망에 적용하면 네트워크의 효율성과 경제성 증대는 물론, 외국산 국방통신망을 대체도 가능하다.

ETRI가 개발에 성공한 'IP통합장비' 기술은 용도별로 100여개의 다양한 군 통신망 중 유사 등급의 망 64개 이상을 하나의 장비로 통합할 수 있도록 하는 기술이다. 여기에는 네트워크 가상화 기술이 적용, 논리적 통합이 가능하도록 망을 하나로 묶었다. 해당 기술개발로 군 통신의 네트워크 효율성 증대는 물론 유선과 무선 통신망의 연동이 가능해졌다. 또한 군 통신망의 보안도 한층 강화될 것으로 기대하고 있다.

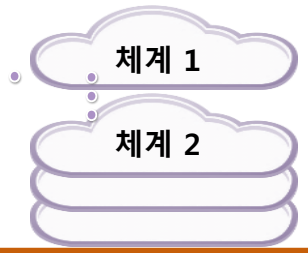
향후 ETRI는 연구진의 기술개발 덕택으로 국산 장비로의 대체를 통해 미래 네트워크 중심전(NCW)에도 보다 안전한 대비가 가능해질 것으로 보고 있다. 박지영 기자

5. 기대효과

산출물: As-Is → To-Be

각 군별 개별 물리망(현재)

개발 후



각 군별 논리적 분리망(개발 후)

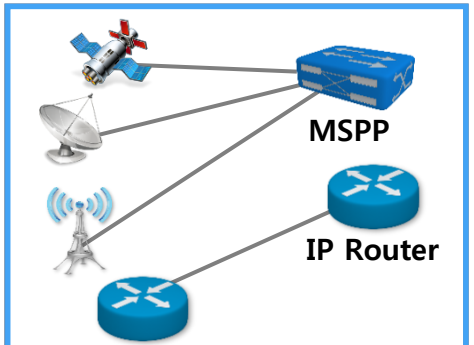
다체계 단말 SW(개발 후)

다체계 접속 단말 SW

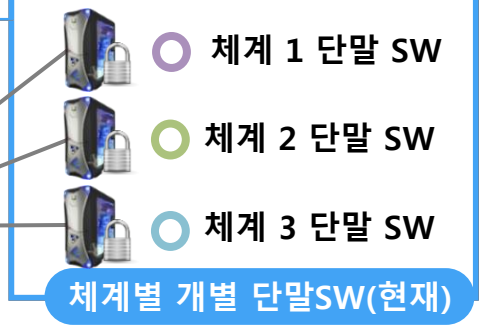
4 다중체계 및 망 접속을 위한 단말 소프트웨어

개발 후

2 다중 가상 네트워크 기술 개발



각 망별 개별 접속(현재)

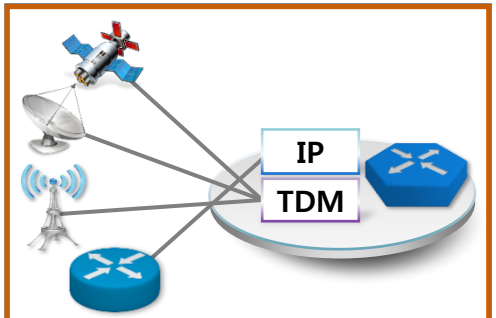


체계별 개별 단말SW(현재)

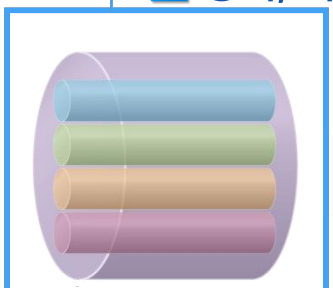
3 다기능 접속 장비 개발

1 동적, 지능적 대역 제어 기술 개발

개발 후

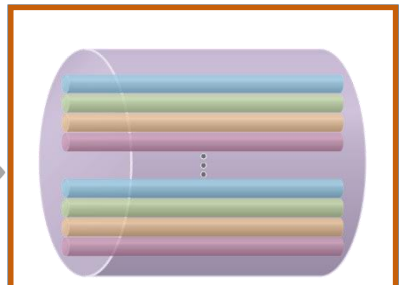


다기능 통합 접속(개발 후)



정적 관리(현재)

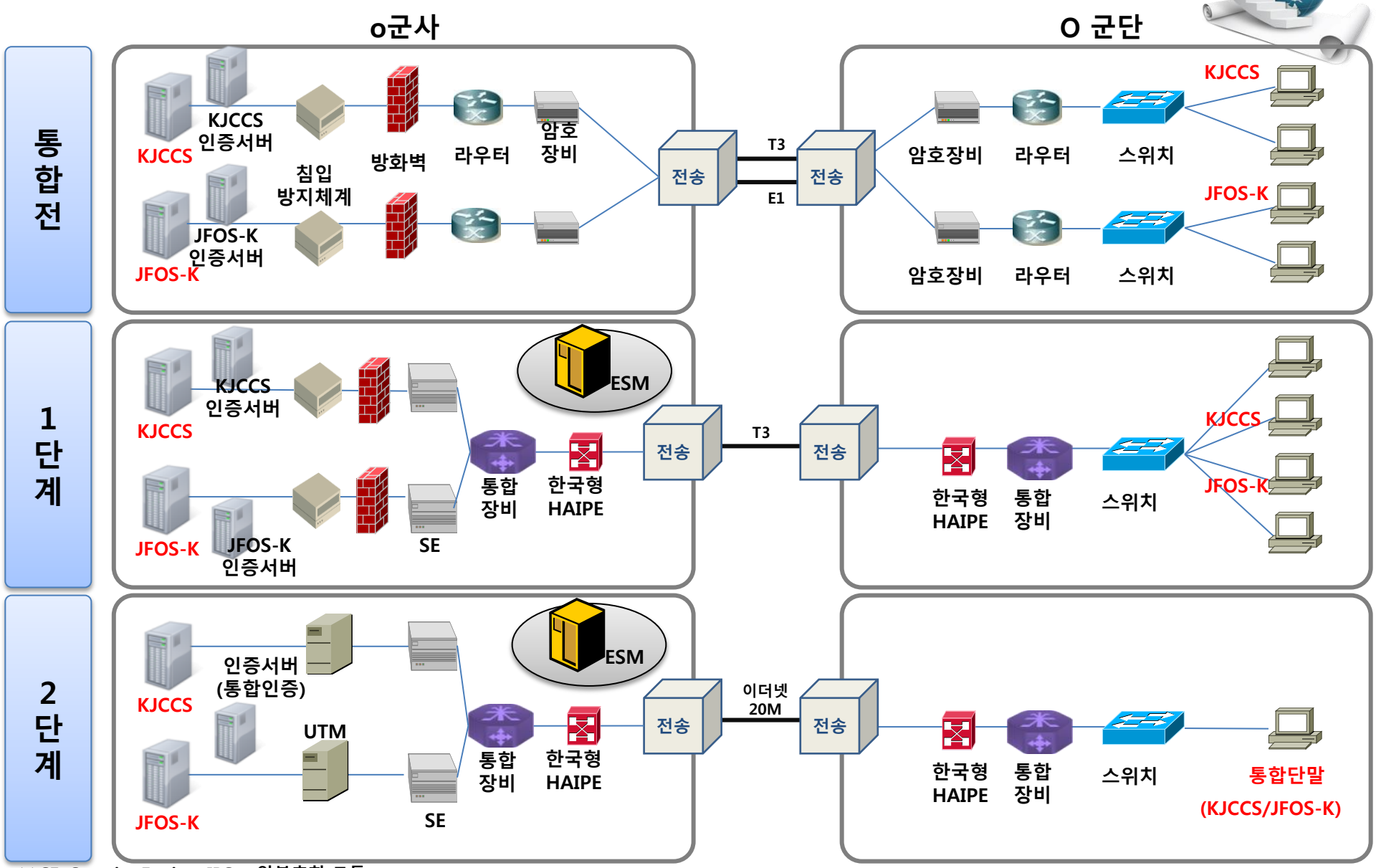
개발 후



개별 동적-세부 관리(개발 후)

5. 기대효과

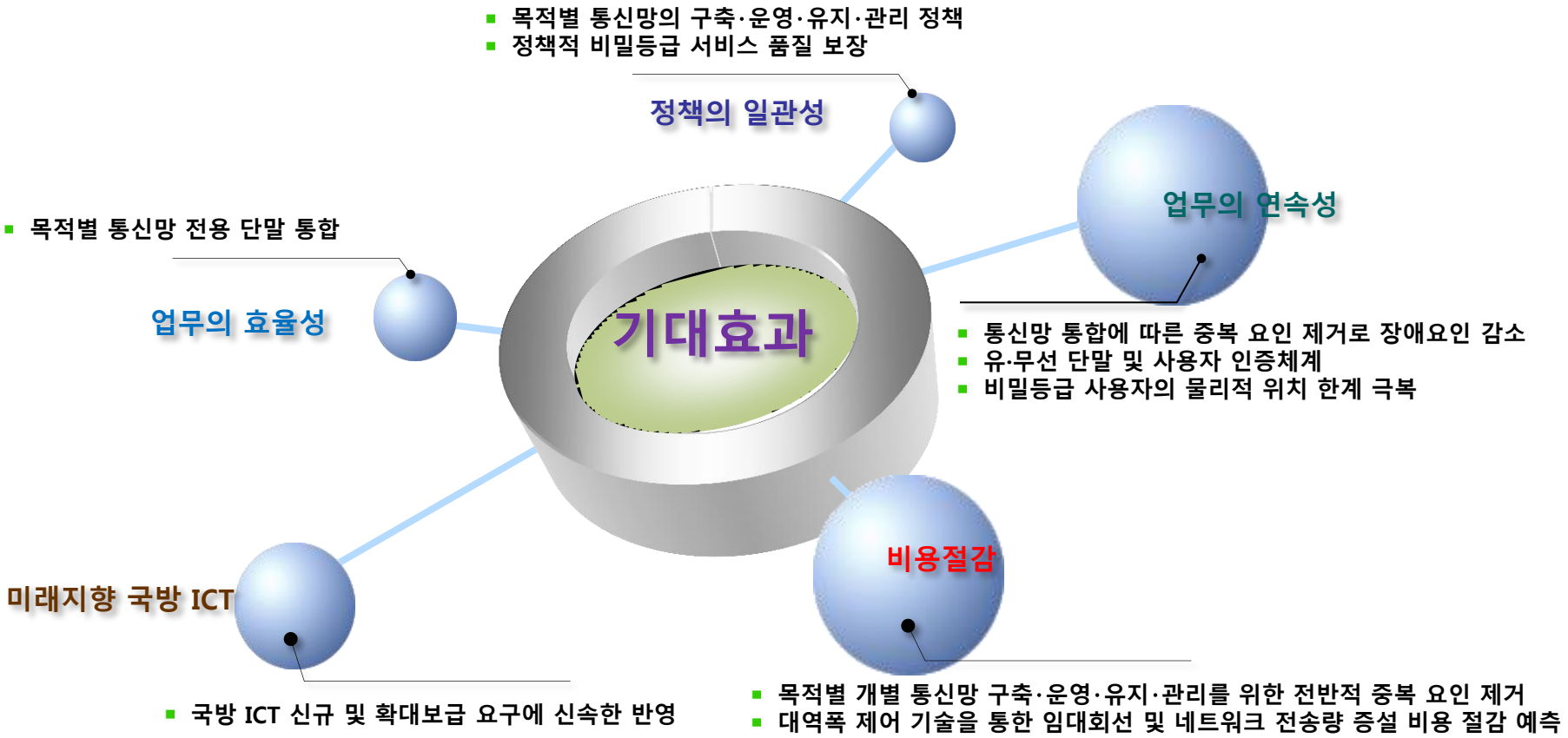
유사통신망 통합 예시



※ SE: Security Engine, IPSec 암복호화 모듈

5. 기대효과

기대효과는 정책의 일관성을 유지함과 동시에 업무의 효율성과 연속성을 기대할 수 있으며, 무엇보다도 중요한 예산절감과 미래지향의 국방 ICT 체계 구축을 위한 핵심 기술 개발



"경청해 주셔서 감사합니다"

parkhs@etri.re.kr

감사합니다

고속 보안 게이트웨이용 임베디드 플랫폼 개발

건국대학교 항공우주정보시스템공학과

박 정 근 교수

고속 보안 게이트웨이 개념

휴대용 통신장비

지원 무기 체계

상황 전파용 유선 전화기

이동형 통신 장비

영상 기록 장비

고속 보안 게이트웨이

임베디드 플랫폼 요구

다양한 HW 형태	특징
이동식 휴대기기	경량화, 항온/항습/방진
스마트폰 결합형	부착 또는 앱(App)
드론 탑재형	이동식 휴대기기 변형
센서 결합형	최소 기능, SoC 개발 필요

고속 보안 게이트웨이 임베디드 플랫폼

단말 또는 센서 정보의
수집 / 분석 / 저장 / 전송

정보처리 플랫폼

무선 통신, 라우팅

보안: 암호화, 인증, 데이터 정규표현식 전수조사

고속 패킷 처리

하드웨어 지원

임베디드 플랫폼

통신 기능

구분	내용	비고
통신 방식	Wi-Fi AP(Access Point), LTE	센서 정보 Wi-Fi로 수신, 망 연결은 Wi-Fi 또는 LTE
데이터 전송	센터(통제실) 서버 간 통신	정보시스템, 인증시스템, SIEM과 통신
	지역(전장) 게이트웨이 간 통신	센터 연결 불가 등의 경우
라우팅	ad hoc routing	망 변경 시 우회 경로 탐색
핸드오버	센서 접속 보안게이트웨이 변경 시	데이터/접속의 중복 및 유실 관리

- ad hoc routing은 여러 방식(table-driven, on-demand 등)의 응용 연구 필요
- 센서 정보 수집 및 데이터 전송:
  - ✓ 보안게이트웨이는 네트워크 간 전송을 담당, 또는
  - ✓ 보안게이트웨이에서 일차 데이터 처리 (정보처리 플랫폼)

보안 기능

구분	내용	비고
인증	접속 기기 (센서 등) 인증	
	보안게이트웨이 간 인증	
	인증 정보 분산 관리	센터의 인증 서버 연결 불가의 경우, 인증 정보의 보안게이트웨이 분산 관리
암호화	센터(통제실) 간 암복호화	
	보안게이트웨이 간 암복호화	
데이터 검사/차단	정규표현식 기반 Deep Packet Inspection	정규표현식 전수조사
	시그너처(정규표현식 탐지규칙) 분산 관리	센터 서버 접속 불가의 경우, 시그너처 업데이트 유실 방지

고속 패킷 처리 기능

구분	내용	비고
고속 패킷 입출력	사용자 레벨 패킷 매핑 드라이버	공유 메모리 기반 패킷버퍼 매핑 Zero-copy, lock-free 구조
고속 패킷 프로세싱	Scalable 멀티코어 패킷 프로세싱 플랫폼	세션 기반 동적 로드 밸런싱 멀티코어 스케줄링
인터페이스	보안 모듈 연동 API	Fast-path API 동적 보안 모듈 관리

고속 패킷 처리?

NIC
(Network Interface Card)

고속 네트워크 카드
10 Gbps 이상

기존 OS

20년간 정체!

애플리케이션

고성능 CPU
3GHz 이상, 멀티 코어, 큰 캐쉬

애플리케이션으로 패킷 전달 속도가 감소, CPU 유휴!

(기준: 10Gbps NIC, 64 byte Packet, 2.4 GHz Intel Xeon E5645 on native Linux stack)

NIC

개선된 플랫폼

애플리케이션

고속 패킷 처리의 목표

Wire-Speed로 애플리케이션에 패킷 전달

네트워크 환경 변화: SDN/NFV

PC/스마트폰

과거 컴퓨터 산업

애플리케이션

합쳐서 제공

OS

하드웨어

현재 PC/스마트폰 산업

애플리케이션

따로 따로

OS

따로 따로

하드웨어

네트워크

현재 네트워크 산업

애플리케이션

합쳐서 제공

OS

하드웨어

향후 네트워크 산업 (SDN 기반)

애플리케이션

따로 따로

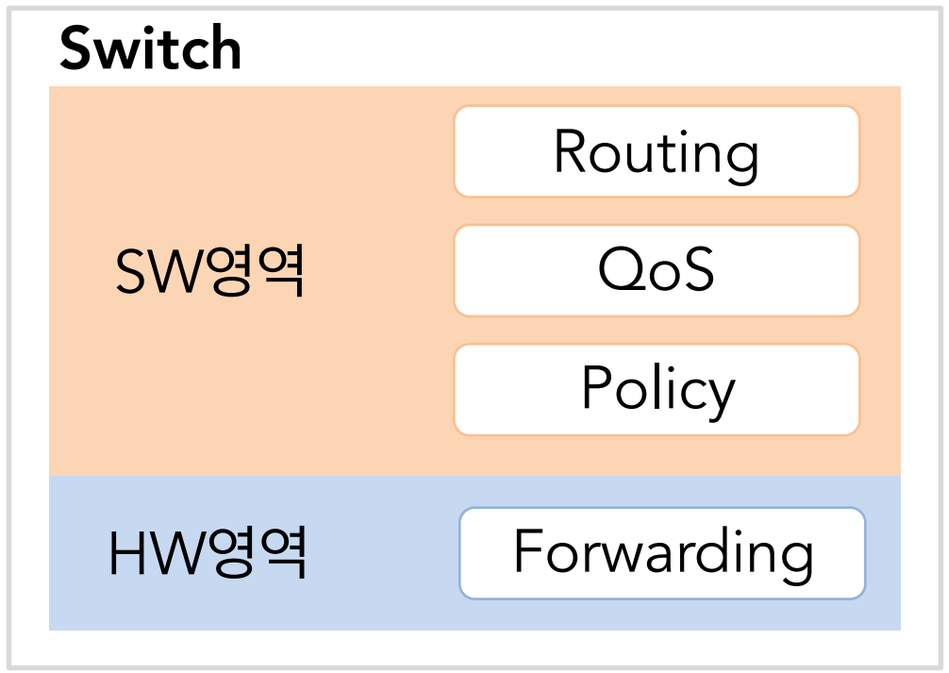
OS

따로 따로

하드웨어

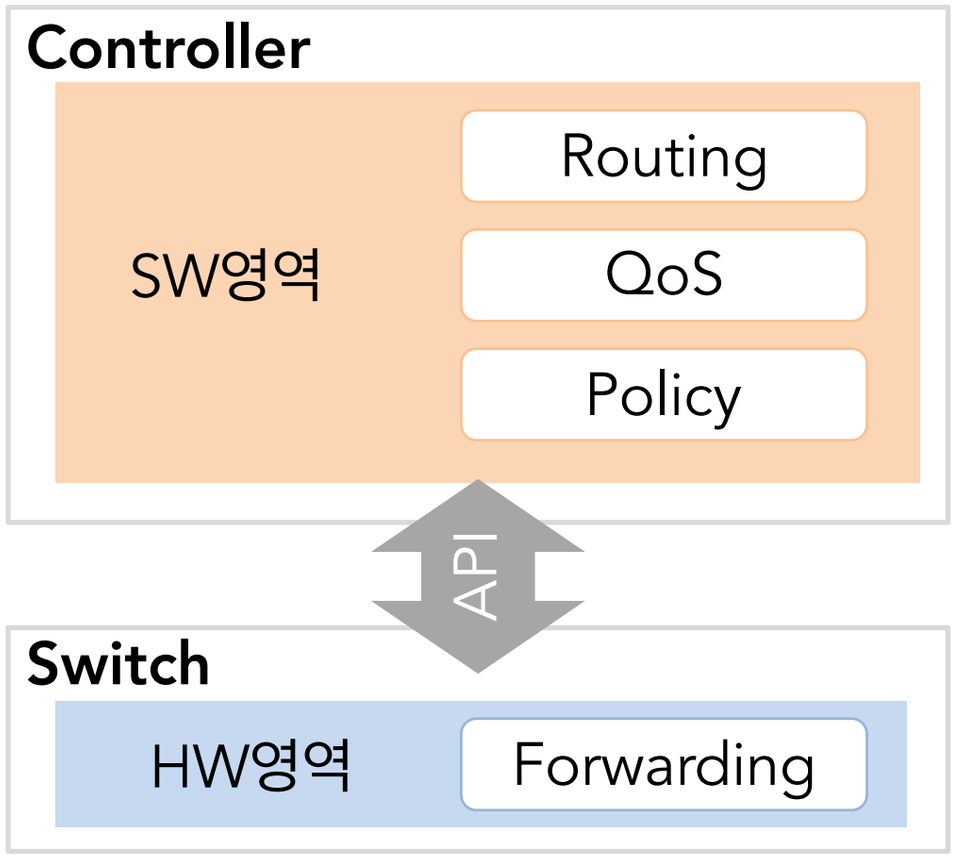
네트워크 환경 변화: SDN/NFV과 고속 패킷 처리

기존 네트워크 장비



분리

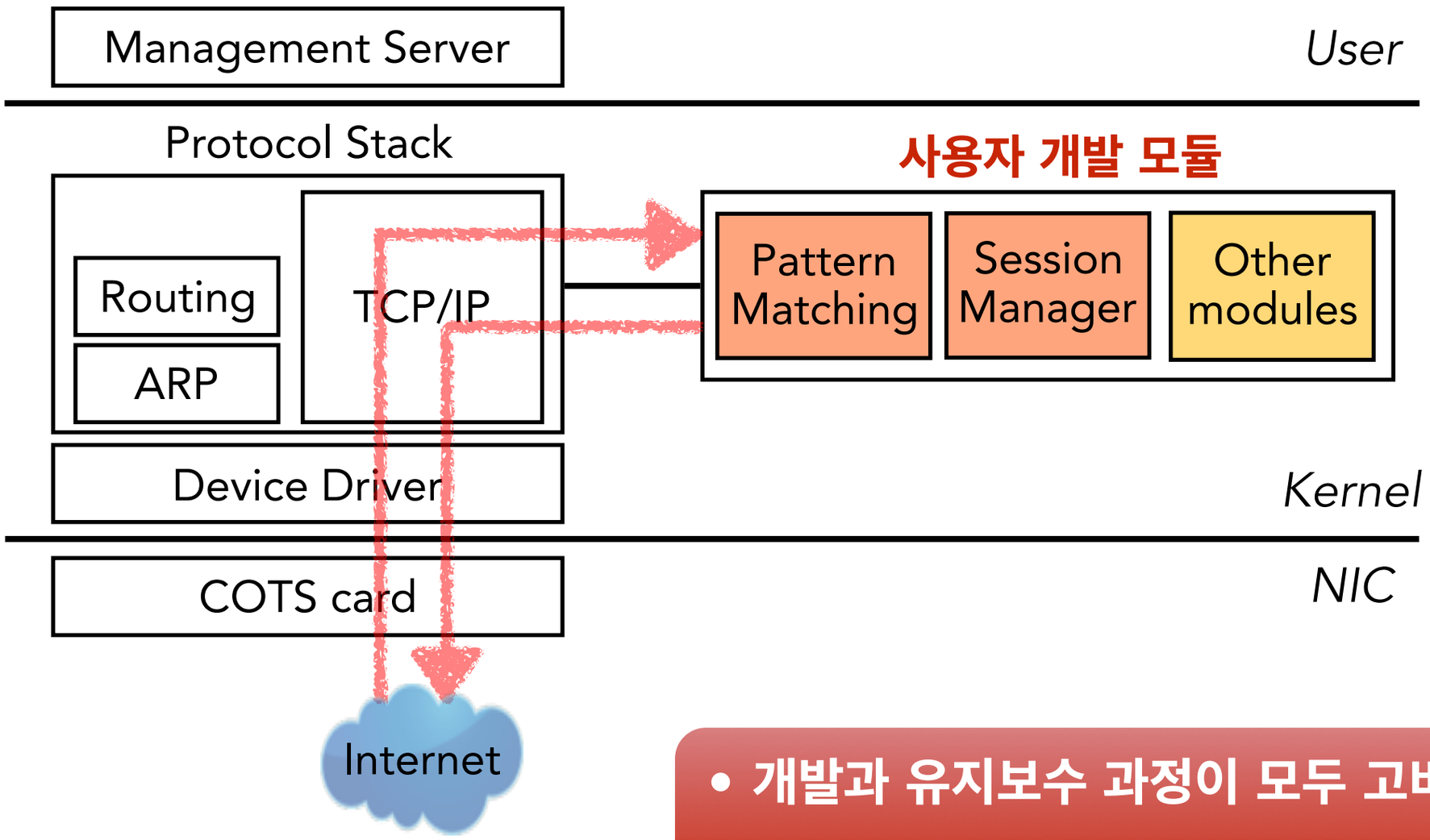
SDN 네트워크 장비



- ✓ SDN의 HW는 **범용 서버를 기반**
- ✓ **SW 기반 고속 패킷 처리 기술 필요**

고속 패킷 처리 구현 기술 (1/2)

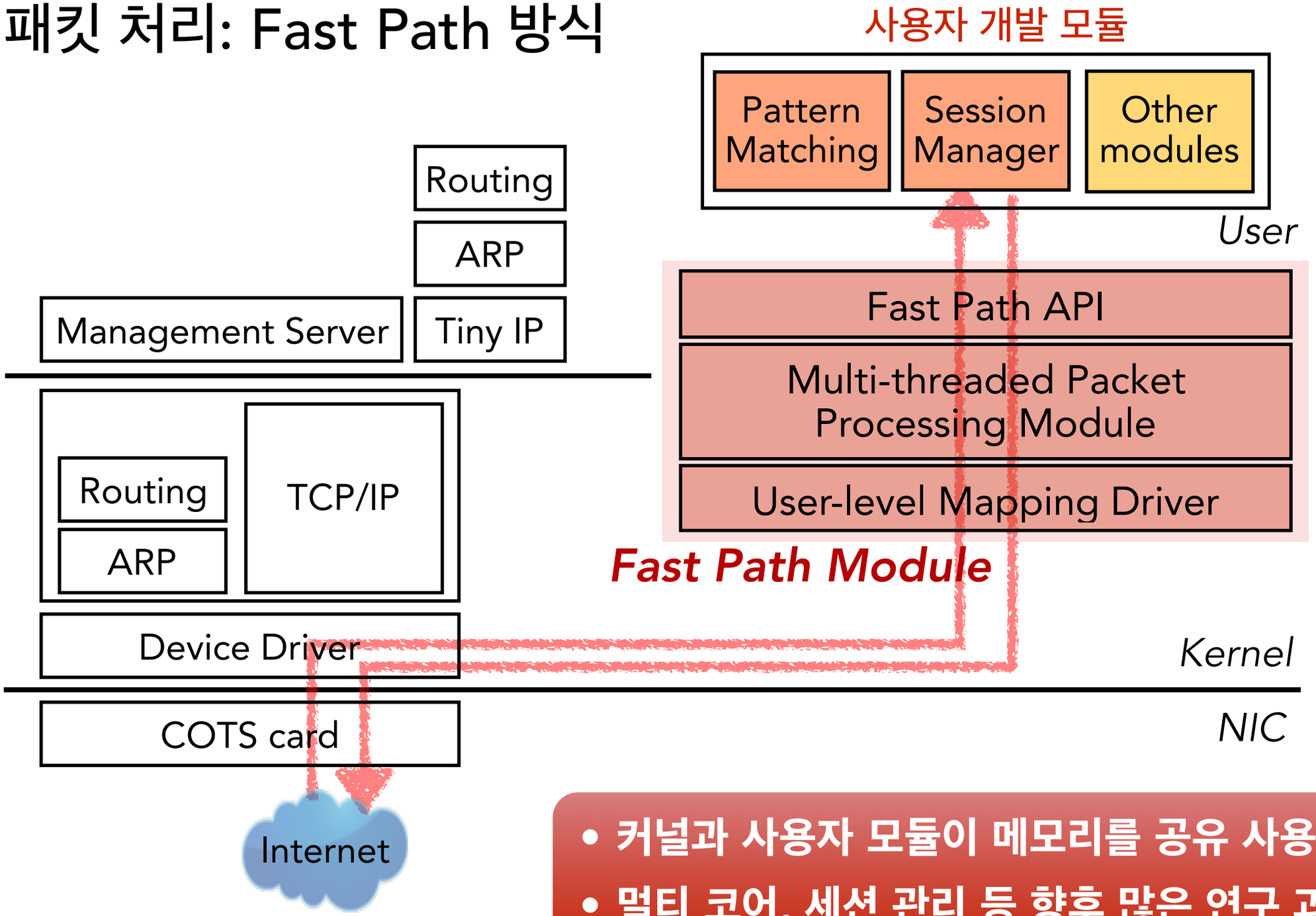
전통적인 패킷 처리: 커널 모드(Kernel Mode) 방식



- 개발과 유지보수 과정이 모두 고비용 저효율
- 최근 급격히 빨라진 네트워크 속도를 감당하지 못함

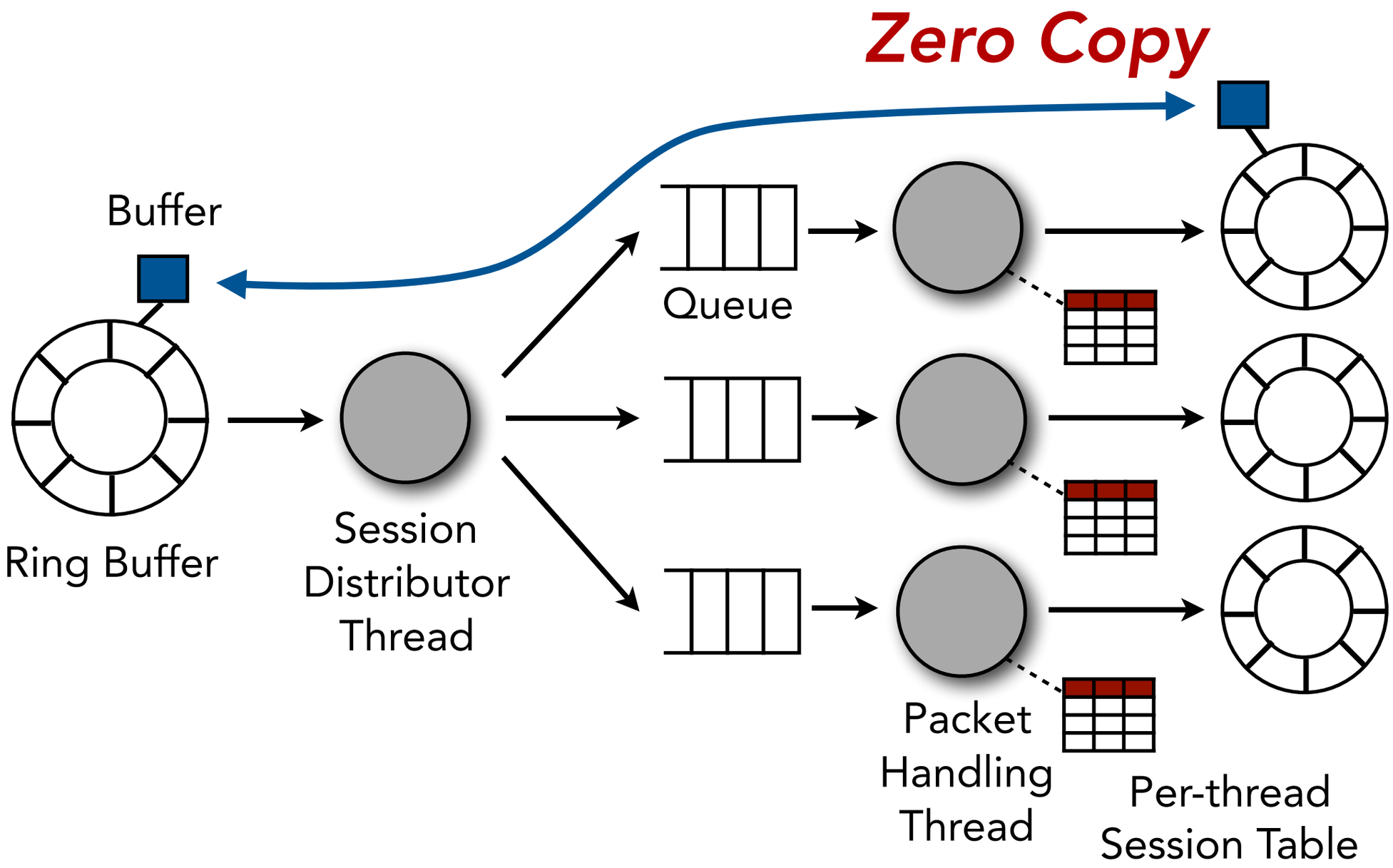
고속 패킷 처리 구현 기술 (1/2)

최근 패킷 처리: Fast Path 방식



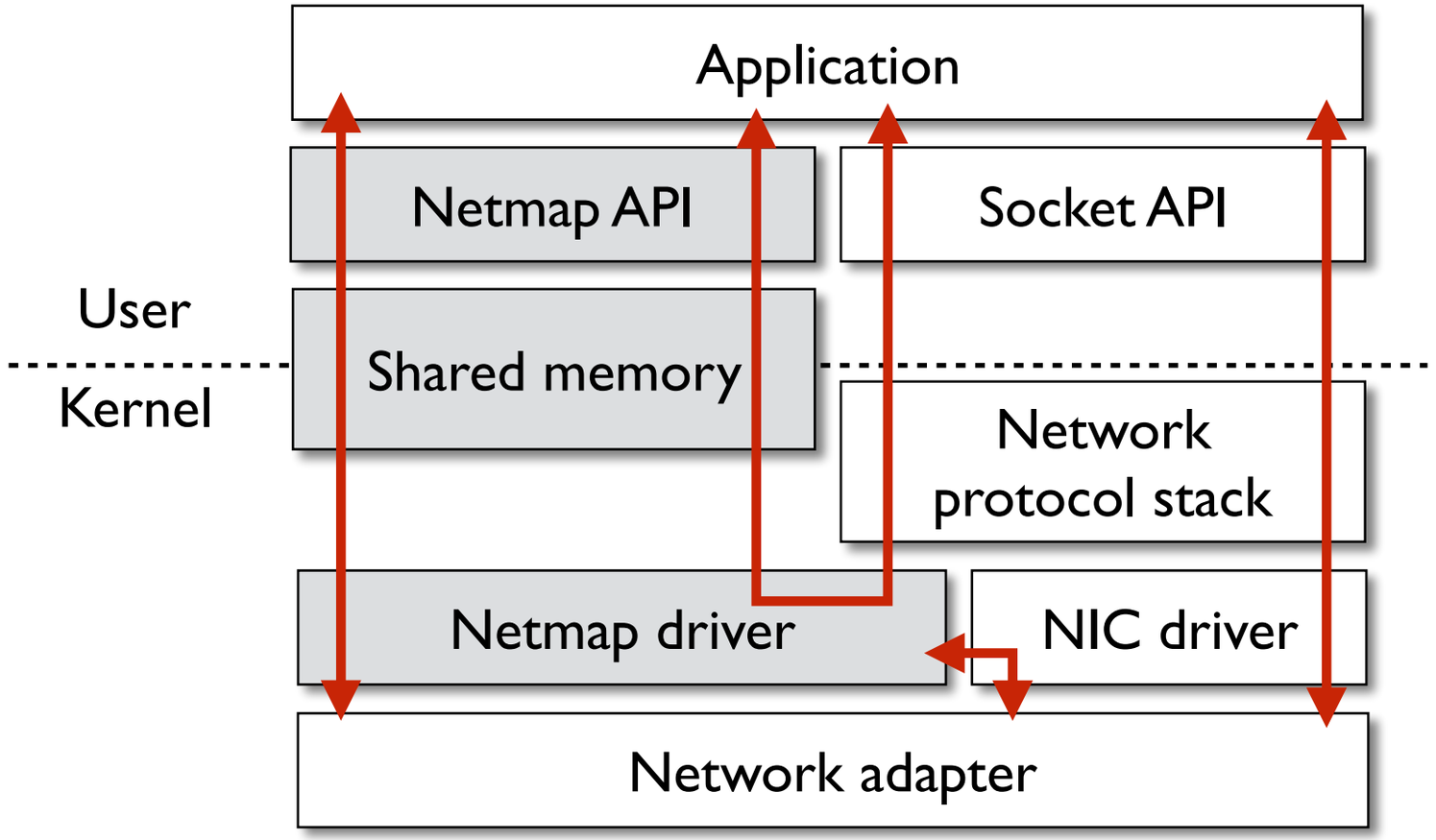
- 커널과 사용자 모듈이 메모리를 공유 사용
- 멀티 코어, 세션 관리 등 향후 많은 연구 과제

Fast Path 방식의 패킷 흐름



Netmap 구조 개요

- Netmap driver
  - 네트워크 인터페이스(NIC)가 Netmap을 사용할 수 있도록 하는 인터페이스
- Shared memory
  - 유저 모드와 커널 모드에서 공유하는 Netmap 패킷 저장 자료구조
- Netmap API
  - Netmap 자료구조 제어용 API



고속 패킷 처리의 글로벌 현황

인텔(Intel) DPDK

인텔 HW에 최적화된 플랫폼 &

- 세션 기반의 보안 처리에 최적화 되지 않음
- 하드웨어 기반 Flow Classification에 제한

CPU 유연성, S/W 기반 Classification 등의 확장성(Scalability)에 한계

상용 제품군

- 6WIND, CalSoft, Tieto, Wind River 등
- DPDK 기반 플랫폼

- **인텔 CPU 환경에만 적용,**
- **확장성 제한,**
- **경량 환경 적용 미비**

Packet Shader

- GPU에 의한 패킷 처리 고속화

- **전용 하드웨어 사용의 한계**
- **범용 적용시 성능 보장 한계**