가상ID 기반의 기업망-모바일-클라우드의 스마트한 연결을 제공하는 VPC 네트워킹 기술

정부금, 안병준, 박혜숙, 김기철*, 이동철**
한국전자통신연구원, ㈜아큐픽스*, ㈜LG유플러스**

요 약

클라우드 컴퓨팅이란 공유된 IT 자원을 네트워크 상에서 가상화를 통하여 독립적으로 사용할 수 있는 개념으로 저탄소 녹색 시대를 위한 에너지 절감 솔루션이다. 특히 비용 절감이 필수적인 기업과 공공기관 등에서 IT 자원의 개별적 소유에 시간과 비용을 투입하지 않고 사용한만큼의 비용을 지불할 수 있다. 이에 정부에서는 2015년 9월부터 시행되는 클라우드법 제정을 통하여 클라우드 컴퓨팅의 활성화를 적극 장려하고 있다. 그러나 신뢰성있는 서비스 제공을 위해서는 보안성, 성능, 안정성 제공을 위한 네트워크 기능의 한계 극복이 필수적이다. 이에 본 논문에서는 언제 어디서나 다양한 기기로 업무를 수행할 수 있는 모바일 스마트워크가 가능하도록 하는 단말과 기업망, 클라우드를 안전하게 연결하는 가상 사설 클라우드(Virtual Private Cloud) 네트워킹 구조를 제안한다. 본 구조에서는 클라우드 내에서 사설 주소의 중복 문제 해결을 위하여 위치 주소와 아이디 분리 프로토콜 기반 위에 기업망 등의 엔터프라이즈 ID 개념을 적용하여 주소 확장성을 제공하였다. 또한 이러한 기술을 적용한 VPC 매니저, 서비스 게이트웨이 및 에이전트로 구성된 VPC 네트워킹 솔루션으로 테스트베드를 구축하고 그 운용 경험을 통해서 실 사업자망에 적용 가능한 비즈니스 모델 도출이 가능할 것으로 기대한다.

Ⅰ. 서 론

인터넷을 그림으로 표현할 때 구름(클라우드)으로 나타낸다. 또한 구름처럼 함께 그룹 지어져 있는 객체의 모음을 클라우드라고 한다[1]. 즉, 클라우드 컴퓨팅이란 네트워크를 통해서 컴퓨팅 자원들을 제공받을 수 있는 것을 의미하는 것으로, 예전 일부 소수층에서 개인 별장을 소유하는 것에서 현재는 공동 관리의 콘도 등을 필요 기간 동안 개인이 빌려 쓰는 것처럼, 각 기업에서 IT 시스템을 필요로 할 때 고가의 비용과 장시간을 투입하여 개별적으로 구축하지 않고, 이미 안정적으로 구축된 클라우드 센터에서 즉각적으로 자원을 제공받고 사용한 만큼의 비용을 지불할 수 있는 것이다.

기업이나 정부기관 등 특정 단체를 위한 특화된 클라우드 서비스를 VPC (Virtual Private Cloud, 가상 사설 클라우드)라고 하며, 공공(Public) 클라우드에 비해 더 높은 보안성, 성능, 안정성이 요구된다. 특히, 언제 어디서나 모바일로 업무를 수행할 수 있는 스마트워크 시대로 진화해 감에 따라 기업망을 위한 VPC 서비스 도입은 급격히 증가할 전망이다[2][3][4].

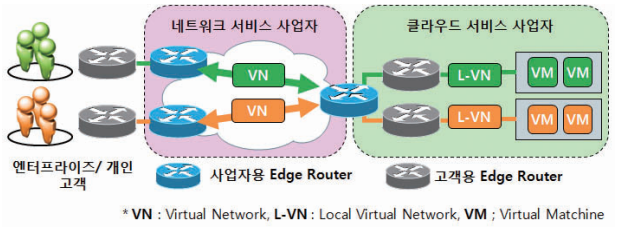

그림 1. VPC 기술의 개념

VPC 서비스란 사용자의 서비스나 애플리케이션을 사용자 데스크톱이 아닌 공동 서버에 저장해 두고 필요할 때마다 열어볼 수 있는 기술로 공용 또는 공공 클라우드 내에 엔터프라이즈 또는 개인 클라우드가 존재하지만 사용자는 엔터프라이즈에서 서비스를 제공 받는 것과 동일한 작업 환경을 제공받는 서비스이다. 이러한 클라우드 서비스를 위한 가상사설망 기술을 VPC 네트워킹 기술이라고 한다[5].

이러한 클라우드의 활성화와 안전한 사용을 위하여 정부에서는 2015년 3월 제정하여 9월부터 시행되는 클라우드법을 통하여 클라우드 컴퓨팅의 발전과 이용자 보호를 위한 환경을 조성하고자 노력하며, 서비스 제공자에게는 신뢰성있는 서비스를 제공하도록 책무를 부여하고 있다[6].

VPC 서비스를 위해서는 IP 네트워크 주소의 충돌없이 가용성 및 확장성 확보가 필요한데, 사설 주소를 기업별로 중복으로 할당할 수 있기 때문에 독립적인 폐쇄망으로 이용될 때는 문제가 없지만, 클라우드 환경에서는 동일한 주소가 클라우드 내에 존

재하게 되는 문제점이 있기 때문이다. 이의 해결책으로 거의 무한대로 할당 가능한 IPv6 주소를 사용하면 되나 모든 엔터프라이즈 망을 IPv6로 전환하는 것은 단기간에 가능하지 않다. 따라서, 기존 사설 IPv4 주소를 사용하는 환경에서 클라우드 컴퓨팅이 가능하도록 하여야 한다.

따라서, 모바일 스마트워크 환경에서 공공망을 경유하여 사설망에 접근하는 경우, 통신사업자들은 액세스 망과 단말에 사설 IPv4 주소를 할당하고, ACR이나 GGSN, PDN 게이트웨이에서 NAT를 통하여 공인주소로 변환하는데[7], 사설주소를 사용하는 엔터프라이즈용 단말이 주소의 변경 없이 클라우드 컴퓨팅 서비스를 이용하고자 할 때, 공공망에서 관리하는 사설 주소와 엔터프라이즈 단말의 사설 주소간의 충돌 문제가 발생하여 서비스가 불가능한 상태가 되는 문제점 및 사용자 단말의 수 증가로 인해 사설 IP 주소의 확장성 문제를 해결해야 한다[8,9,10].

본 논문에서는 이러한 문제점을 해결하기 위하여 클라우드 내의 가상머신에서는 공공 IP 사용, 엔터프라이즈 서버와 가상머신간에 동일한 사설 주소를 사용할 수 있는 새로운 구조의 VPC 네트워킹 구조를 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 현황 분석으로 국내외 VPC 기술 현황, 관련 표준화 동향, VPC 네트워킹을 위한 핵심 기술인 주소 음영화 프로토콜로서 아이디/주소 분리 프로토콜에 대해서 분석하며 3장에서는 안전한 클라우드 서비스 제공을 위한 새로운 모바일 VPC 구조를 제시하고, 이를 이용한 테스트베드의 구축에 대하여 기술하며, 동일 VPC 내에서도 접근 그룹을 분리하여 클라우드 서비스를 제공할 수 있는 그룹통신 제어 확장 기술 개발과 상용망에의 적용 가능성을 보여주는 홈 클라우드에의 응용 방안을 제안하며, 4장 결론에서는 본 기술의 의의와 활용성 및 앞으로의 발전 방향을 제시한다.

Ⅱ. VPC 기술 현황

클라우드 컴퓨팅 기반의 스마트워크 시대로 진화해 감에 따라 기존 네트워크는 많은 문제점을 노출하고 있으며 이를 해결하기 위한 기술의 발전이 가속화되고 있다. 'IDC Enterprise Panel'에서의 조사 결과에 의하면 클라우드 모델에서 가장 중요한 이슈와 도전은 보안(Security) 문제라고 응답하였으며 이를 위한 연구개발이 활발하게 진행되고 있다. 그러나 현재 세계 및 국내 장비 시장은 외국의 몇몇 시장 지배 장비 업체들이 독점을 하고 있으며, 중국 업체들의 저가 장비 시장 잠식으로 국내 산업체의 어려움이 계속되고 있다. 하지만 클라우드 분야에서의 시장 선점을 위하여 국내에서도 클라우드 관련 기술 개발이 많이 진행되고 있는 상황이다.

클라우드 분야 연구에서는 사용자와 데이터 센터 간의 안전하고, 신뢰할 수 있으며, 확장 가능한 네트워크 구조 설계 등이 해결해야 될 이슈이다. 클라우드 컴퓨팅 활성화에 가장 큰 장벽으로 대두되는 보안이슈를 뛰어넘을 만큼의 비즈니스적인 가치를 줄 수 있어야 고객을 움직일 수 있을 것이며, 금융권, 공공부문을 중심으로 성공적인 레퍼런스를 확보하는 것이 중요하다.

1. 국내외 산업체 기술 동향

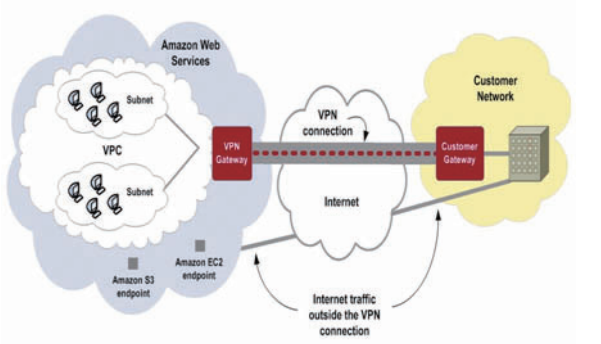

그림 2. AWS (Amazon Web Service) 기술

아마존과 Verizon은 사설 클라우드 자원을 은닉하는 VPC/VCN (Virtual Cloud Networking) 기술을 개발하고 있으나, 모바일 클라우드 환경을 지원하고 있지 않다. 아마존의 클라우드 서비스는 퍼블릭이지만 기업 고객들이 가상의 데이터센터를 구현할 수 있도록 프라이빗을 지원하는 서비스이다. 아마존 VPC(Virtual Private Cloud) 서비스는 고객기업의 인프라에 아마존의 AWS(Amazon Web Services)를 연동시켜주어 기업의 방화벽이나 보안이 유지된 상태에서 아마존의 솔루션이 제공되며, 2009년 아마존 웹 서비스를 통해 첫 선을 보인 아마존 VPC 서비스는 공동 데이터센터 또는 서버와 서비스 사용자를 암호화된 가상사설망(VPN)을 통해 연결해 기업 보안 네트워크를 제공한다[11].

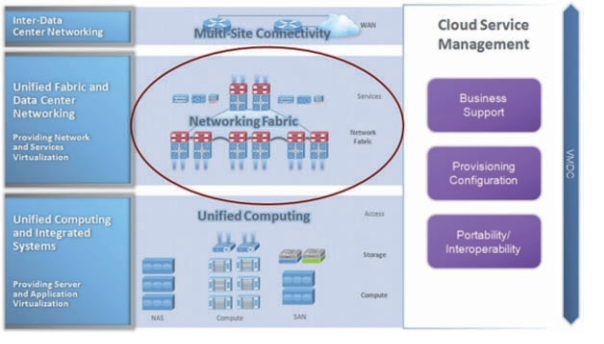

그림 3. Cisco의 VMDC 솔루션 상위 개념도

Cisco는 다양한 종류의 클라우드 내, 클라우드 간, 그리고 클라우드를 넘어 최종 사용자와 연결해주며, 여러 데이터 센터를 통합하여 하나의 데이터 센터로 작동할 수 있도록 하는 클라우드 인프라 구축 및 상황인식 보안 및 가속화된 구축을 지원하는 솔루션을 제공한다. 시스코 VMDC(Virtualized Multi-Tenant Data Center) 구조는 end-to-end 아키텍처와 사설 클라우드 네트워크 설계를 제공하여, 서비스 제공자가 엔터프라이즈 사용자에게 Public, Hybrid, 가상 Private클라우드를 위한 인프라를 제공할 수 있다. 시스코 사설 클라우드 포트폴리오는 모듈러 구조로 구성되어 있으며, 시스코의 통합 데이터센터 네트워킹 솔루션을 통해 엔터프라이즈가 사설 클라우드 서비스로 진화할 수 있는 기술을 제공한다[12].

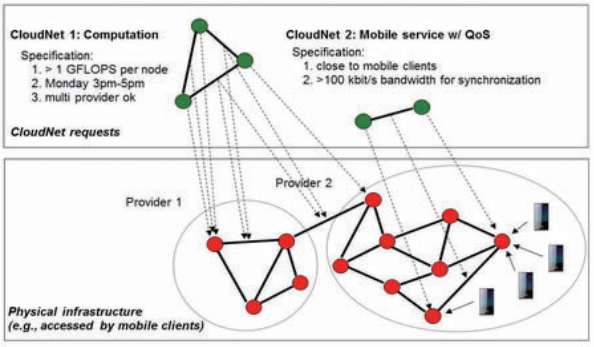

그림 4. CloudNet 구조 개념도

CloudNet 프로젝트는 클라우드와 가상 네트워킹을 연결하는 것으로, 클라우드 자원을 연결하는 가상 네트워크를 제공한다. 가상 네트워크는 하나의 공공 물리 인프라 네트워크를 다수의 CloudNet으로 구성하여 독립적으로 운용하며, VPC 망과 엔터프라이즈 망간에 VLAN/VPN 기반으로 네트워크 연결성을 제공한다[13].

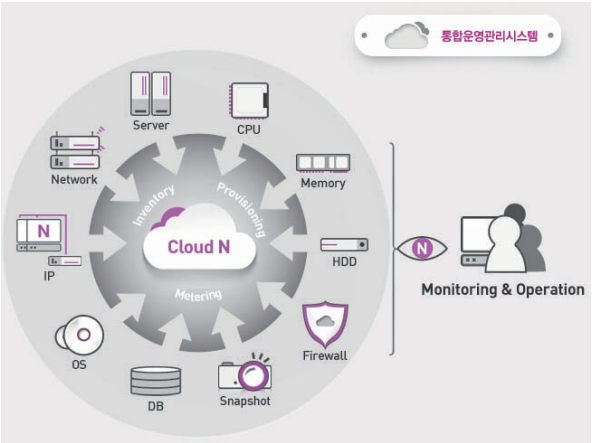

그림 5. LG U+ Cloud의 N 서비스

LG U+의 기업 클라우드 서비스인 "Cloud N"은 최적화된 IT 인프라 환경의 구축과 운영을 지원하는 클라우드 기반의 통합 메니지드 서비스이다. 2010년 Security, Scalability, Speed를 확보한 가상 인프라 서비스로 기반 서비스를 마련하고, 2011년 가상 인프라 솔루션을 결합하여 클라우드 기반의 플랫폼 서비스를 제공하였으며, 2012년 고객이 직접 설계하는 가상 데이터센터 서비스를 제공하였다. Cloud N은 다중의 물리적 계층, Region, Zone, Virtual Zone 의 분산구조로 되어있으며, 기존 레거시 시스템의 마이그레이션이 가능하다. 부하분산과 분산된 Zone 간 부하 균등 네트워크 보안을 위한 VPN을 통해 IT 인프라가 인터넷 접속이 가능하도록 구현한 네트워크 서비스를 제공한다[14].

2. VPC 관련 기술 국내외 표준화 동향

국내에서는 정보통신 기술협회 (TTA) SPG (Special Project Group) 21에서 퍼스널 클라우드, 모바일 클라우드, 보안, 인프라 서비스 등을 비롯하여 클라우드 기반 서비스들에 관련된 기술 표준화 작업을 진행하고 있으며, 민간 중심의 시장 요구를 표준에 반영하기 위한 목적으로 클라우드 컴퓨팅 포럼 (CCF)이 2009년 7월에 출범하여 표준개발분과와 표준보급확산 분과를 운영하고 있다.

VPC와 같은 클라우드 네트워킹 기술 분야에서는 컴퓨팅 기술과 네트워킹 기술이 개별적으로 사용될 때와는 다른 많은 문제들이 나타나는데, 대표적으로 기존 VPN 기술로 multi-tenancy 수용 시 발생하는 사설 IP 중첩문제, VLAN-aware customer bridging 문제, L3 서브넷 경계를 넘어가는 VM mobility와 같이 VM 확장성 확보 시 발생하는 제반 문제 등이 있다. 이러한 문제들을 해결하기 위해 IETF NVO3 (Network Virtualization Overlays) WG은 데이터센터 환경에서 L3 인터넷에 오버레이 되는 멀티-테넌트 사설 가상 클라우드 네트워크를 구축하기 위한 프로토콜들을 개발하고 있다. 가상랜 기술을 클라우드 네트워킹에 적용할 때 발생하는 문제들(VLAN-aware customer-bridging problem)을 해결하기 위해 브릿지와 라우터의 장점을 결합한 RBridges (Routing Bridges) 또는 TRILL (Transparent Interconnection of Lots of Links) 스위치라고 불리는 장치에 구현되는 RFC들을 제정한 데 이어서 2014년에는 RFC 7348 (Virtual eXtensible Local Area Network, VXLAN)과 RFC 7365 (Framework for Data Center Network Virtualization)를 제정하고 현재 이들의 확장을 위한 표준화 작업을 진행하고 있다.

IEEE는 클라우드에서 실행되는 가상머신 (VM)들 간의 가상 네트워킹 관련 2개의 주요 표준으로서 가상 네트워크 스

위치(또는 브릿지)의 데이터 평면 기능들에 대한 규격에 초점을 맞춘 IEEE 802.1Qbg (Edge Virtual Bridging)과 IEEE 802.1BR (Bridge Port Extension)을 2012년에 제정하였다.

한편 클라우드 컴퓨팅을 활용한 네트워킹 서비스와 관련된 표준화 작업으로 ITU-T SG13에서 Y.3512 (Cloud computing – Functional requirements of Network as a Service)를 2014년에 제정하고 현재는 NaaS 기능구조 권고안을 개발하고 있다. 또한 2014년 12월에 만들어진 ETSI MEC (Mobile Edge Computing) ISG (Industry Specification Group)은 모바일 네트워크 에지에서 클라우드 컴퓨팅 능력 및 IT 서비스 환경을 제공하기 위한 표준 개발에 착수 했다.

이밖에 국제 사실(De-facto) 표준화 기구도 각자의 목적에 따라서 클라우드 관련 표준 개발을 추진하고 있는데, 이와 관련된 대표적인 기구들로는 DMTF (Distributed Management Task Force), OGF (Open Grid Forum), OCC (Open Cloud Consortium), CCIF (Cloud Computing Interoperability Forum) 등이 있다.

3. ID/Locator 분리 기술

기본적으로 IP 주소는 위치정보(Locator)와 식별자(Identifier)의 조합으로 구성되어 있다. 주소의 확장성 및 이동성 등의 문제를 해결하기 위해서 위치정보와 식별자 분리 기술이 핵심 이슈가 되고 있다. 기업망 내에 있던 단말이 외부로 이동할 경우, 이동성 제공을 위해서는 이동하는 단말의 위치와 상관없이 단말을 식별할 수 있어야 하며, 이동 중에도 통신 세션은 항상 유지되어야 한다. 따라서, 이러한 이동성 및 멀티호밍을 지원하기 위해서는 단말의 식별자는 동적으로 두 개 이상의 위치정보와 매핑되어야 한다. 즉, 통신중인 이동단말이 이동했을 경우 단말의 위치는 변경되었기 때문에 위치정보는 바뀌게 되지만 통신중인 단말의 식별자는 변경되어서는 안 되는 것이다.

HIP(Host Identity Protocol)은 IRTF (Internet Research Task Force)에서 표준화된 기술로, 인터넷 망이 IP를 통해 호스트에 대한 식별과 호스트의 위치를 식별함으로 인해 이동성과 멀티호밍 서비스를 제공하지 못하는 문제점을 해결하기 위한 것이다. 전송계층과 응용계층에서 세션을 유지하기 위해 호스트 ID를 사용하여 공개 키 암호 방식을 기반으로 위치에 독립적인 호스트 ID를 이용하는 것으로, 호스트에 HIP 스택을 도입하여 데이터를 송수신하고, 기존의 보안/암호화 프로토콜을 제어 신호로 이용한다[15].

LISP(Locator/ID Separation Protocol)은 IP 주소를 장치 식별(EID)과 네트워크에 접속한 장치의 위치(RLOC)로 분리하는 새로운 라우팅 구조이다. CISCO IOS와 Nexus에 탑재 되어

표 1. ID/Locator 분리 기술 비교

항목	HIP	LISP	MOFI
분리 기반	Host 기반	Network 기반	Network 기반
표준화 현황	IRTF RFC4423 등 18개 RFC	IETF draft-ietf-lisp-22	IETF mext WG
ID	Host Identifier	EID (IPv4주소)	HID(IPv6 주소)
Locator	IPv4/IPv6주소	RLOC	IPv4/IPv6 주소
Network Element	End host solution	ETR, ITR, MR, MS, ALT *	AR, LMC, DMS **
Data Plane 스택	HIP Shim 헤더	LISP Data	ADP/BDP
Control Plane 프로토콜	HIP base exchange	LISP Control ALT	SDMC
Tunnel	end-to-end security tunnel	GRE	No
구현사례/상용화	OpenHIP, HIPL (Linux,Windows, FreeBSD, MacOS)	CISCO IOS/ Nexus	경북대학교 Testbed
관련 업체	Boeing, Ericsson, 다수 Testbed	CISCO	–

* ETR(Egress Tunnel Router), ITR(Ingress Tunnel Router), MR(Map Resolver), MS(Map Server), ALT(Alternative Topology device)
** AR(Access Router), LM(Local Mobility Controller), DMS(Distributed Map Server)

상용화가 된 기술로 호스트의 수정 없이 터널링과 맵핑 기술을 통해 네트워크 기반으로 제공되어 기술 도입이 빠른 반면, 이동이나 멀티호밍에 관련 없는 데이터 패킷에 대한 추가적인 처리가 요구된다. 멀티호밍과 이동성 지원, 데이터 센터 가상화, 새로운 서비스 및 기술 도입의 용이성 면에서는, 단시간에 가장 빠른 성과를 낼 수 있는 기술이다[16].

MOFI(Mobile Oriented Future Internet)은 이동환경을 지원하기 위한 미래 인터넷의 새로운 구조이다. 이 기술은 HID와 로컬 위치자를 구분하였다. 이동성 지원을 위해 로컬 라우팅은 GIC-LLR (Global ID-based Communication with Local LOC based Routing)을 이용하고, 글로벌 라우팅을 위해 SDMC(Scalable Distributed Mobility Control)제어 프로토콜을 정의한다. 국내 연구 사업의 일환으로 만들어진 이 프로토콜은 현재 경북대학교에서 테스트베드를 구축하여 시험 운용하고 있다[17].

Ⅲ. 모바일 VPC 네트워킹 기술

1. 시스템 구조

본 절에서는 인터넷 망을 통하여 모바일 단말에서 프라이빗

클라우드 서비스를 안전하게 제공받을 수 있는 모바일 VPC 네트워킹의 구조와 구현에 대하여 기술한다.

기업망-이동단말-클라우드망을 신뢰성 있게 연동하기 위해서는 우선 안전한 연결성이 보장되어야 하는데, 이를 위해서 사설 IP 주소를 지원하는 가상 IP-in-IP 터널링과 사설 주소 기반의 IPSec 기술이 필요하다. 또한 사설 주소의 확장성이 제공되어야 하는데 사설 주소가 외부에 유출되지 않도록 은닉(hiding)하고, VPC 단위로 확장 가능해야 한다. 또한 VPN의 동적 재구성 및 모바일 VPC 시그널링을 통하여 단말의 이동성을 제공해야 한다. 이를 위해서는 VPN 기반의 주소 음영화 프로토콜 기술이 필요하다. 이러한 기술을 제공하는 모바일 VPC 네트워킹 구조는 다음 〈그림 6〉과 같이 VPC 게이트웨이, VPC 매니저, VPC 에이전트로 구성된다. VPC 게이트웨이는 관리하는 주체와 적용되는 네트워크 위치에 따라서 클라우드 사업자용, 인터넷 사업자용 또는 엔터프라이즈용 서비스 게이트웨이로 구분 가능하다.

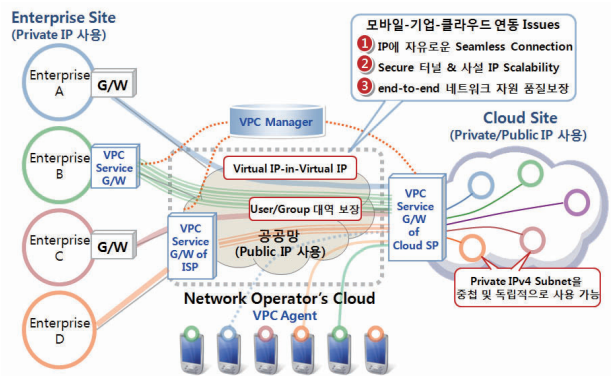

그림 6. 모바일 VPC 네트워킹 구조-구성 요소

이러한 모바일 VPC 네트워킹 구조상에서 각 구성요소들은 단독 혹은 서로 결합/연동하여 동작하며 다음과 같은 기술들을 기반으로 한다.

- VPC 시그널링 기술
  VPC 서비스의 가입자(스마트 디바이스) 및 그룹(스마트 오피스)의 인증, IP 계층 암호화와 온-디맨드 site-to-site 및 client-to-site 간의 안전한 터널 연결성을 제공하기 위해 단말의 이동성 제공 및 기업/기관에서 사전 할당된 사설 IP 주소를 사업자 망에서 사용할 수 있도록 하는 기술
- 네트워크 기반의 VPC 게이트웨이 기술
  기업망과 클라우드간의 안전한 네트워크 사용을 위한 대역폭 보장으로 end-to-end 네트워크 자원 가상화를 제공하고, 클라우드와 기업망 사이의 공인/사설 IP 주소에 따른 끊김 없는 접속을 제공하는 기술
- VPN 기반의 주소 음영화 프로토콜
  사설 IP 주소를 여러 기업 망이 독립적으로 사용할 수 있도록 IP 주소 확장성을 제공하고, 공공망에서는 엔터프라이즈 내에서 사용하는 사설 IP 주소가 은닉되어 보호되어야 하는데, 이를 위해서 주소 음영화 프로토콜을 사용하여 사설 IP 주소를 여러 기업망에서 독립적으로 사용할 수 있도록 하는 기술

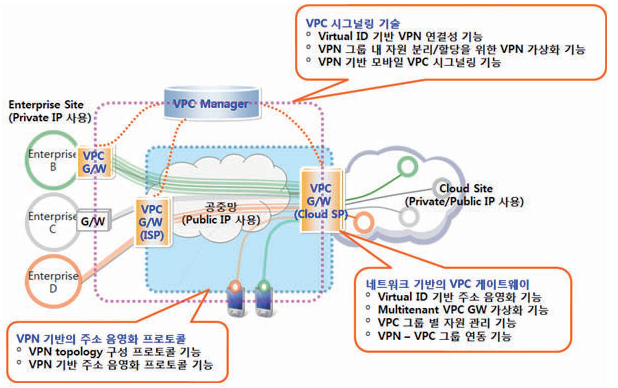

그림 7. 모바일 VPC 네트워킹 세부 기술

2. VPC 서비스 시나리오

확장성 있는 가상 ID 기반의 기업망-클라우드-모바일기기 연결을 제공하는 가상 사설망 기술은 인터넷 이용을 통해 프라이빗 클라우드 서비스를 안전하게 보장하기 위하여 시그널링 기술, 네트워크 기술 및 클라우드 기술 기반의 안전한 가상 인프라를 제공하여 프리미엄 IT서비스를 창출하게 하는 신개념의 가상 사설 클라우드 (VPC) 기술이다. 이러한 VPC 기술을 이용하는 서비스 시나리오는 다음과 같다.

가. Secure tunnel을 사용하는 VPC 서비스 시나리오

클라우드 사이트와 엔터프라이즈 사이트를 연결하는 VPC 게이트웨이 간에 secure tunnel을 생성하여 각 VPC 별로 독립적으로 안전한 연결을 제공한다. 또한, 하나의 터널 내 여러 개의

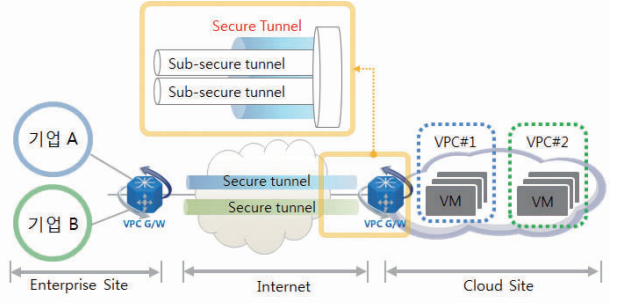

그림 8. 안전한 터널을 사용하는 VPC 서비스 시나리오

sub-secure tunnel을 구성하여 서비스 또는 사용자 별로 구분되는 통신채널을 제공할 수 있다.

나. 주소 확장성 및 모바일 이동성 제공 VPC 서비스 시나리오

클라우드 사이트 내 서로 다른 VPC 그룹에서 동일한 주소를 사용하면 주소 중복이 발생하게 되는데, 이러한 주소 중복 허용이 가능하도록 주소 확장성을 제공하는 VPC 서비스가 가능하다. 즉, VPC GW 간에는 VPC별 별도의 secure tunnel을 구성하고, 클라우드 사이트에서는VPC GW에서 VPC 그룹별로 다른 고유한 그룹ID(예, <그림9>에서의 IPA, IPB)를 추가하여 전달함으로써, VPC 그룹 간에 중복된 주소를 사용할 수 있도록 하는 것이다.

또한, 사용자가 기업 망을 벗어나서도 VPC와 직접 연결이 가능하도록 안전한 터널을 제공하며, 이 경우에도 주소 중복을 허용함으로써 주소 고갈문제에 대응할 수 있다.

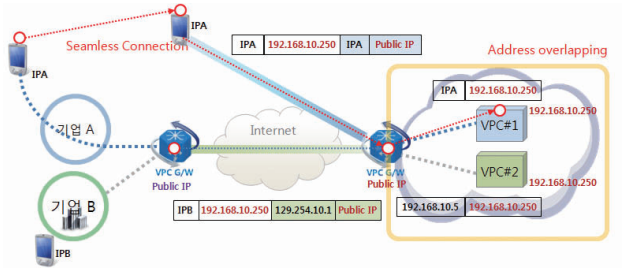

그림 9. 주소 확장성 및 모바일 이동성을 제공하는 VPC 서비스 시나리오

다. 주소 은닉을 제공하는 VPC 서비스 시나리오

<그림 10>에서와 같이VPC GW는 주소 음영화 프로토콜을 사용하여, 매핑 시스템과 통신하여 목적지 주소에 대한 위치 주소 값을 받아 터널링을 제공하는 서비스가 가능하다. 즉, 서버의 공인 주소를 외부에 공개하지 않고 해당 서버에 안전하게 접속할 수 있어, 인터넷상의 악성 공격으로부터 서버를 보호할 수 있다.

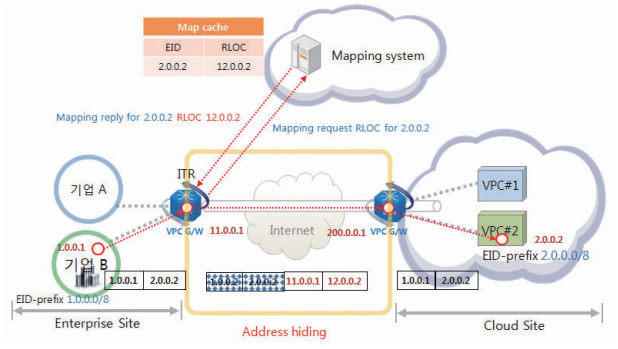

그림 10. 주소 은닉을 제공하는 VPC 서비스 시나리오

3. 테스트베드 구축 및 시험

개발된 모바일 클라우드 기술을 적용하기 위하여 실제 서비스 가능한 형태의 테스트베드를 구축하였다. VPC 매니저와 맵-서버, VPC 게이트웨이 기능이 소프트웨어로 구현된 서버들과 가상 사설 클라우드 구축 및, LG U+ 망카와 내부 게이트웨이 역할을 하는 AP를 랙 상에 실장하였다.

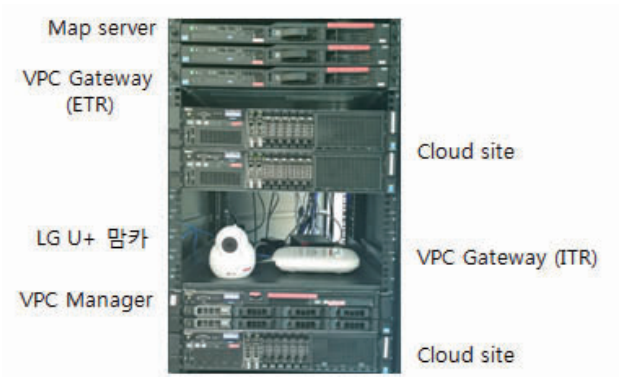

그림 11. 테스트베드 snapshot

VPC 에이전트가 탑재된 이동단말과 외부 게이트웨이, Map Server가 연동되어 주소음영화 프로토콜이 동작하여 가상 ID와 공인/사설 IP의 연결이 설정되고 클라우드 사이트의 가상 사설 클라우드 내에 있는 인스턴스와 정상적으로 통신이 수행되어 인스턴스에서 전송하는 영상이 이동 단말에서 정상적으로 플레이되는 서비스 시나리오가 가능하다. 또한 LG U+의 망카 영상을 해당 가상 사설 클라우드 내의 인스턴스에서 수신할 수 있으며, 각 사별로 독립적인 사설 클라우드 구성 및 단말이 사내 혹은 사외에 위치하더라도 자신의 클라우드에의 접속이 가능하며, WiFi, LTE 망에서 접속 및 이동 시에도 서비스가 끊김 없이 연속됨을 볼 수 있다.

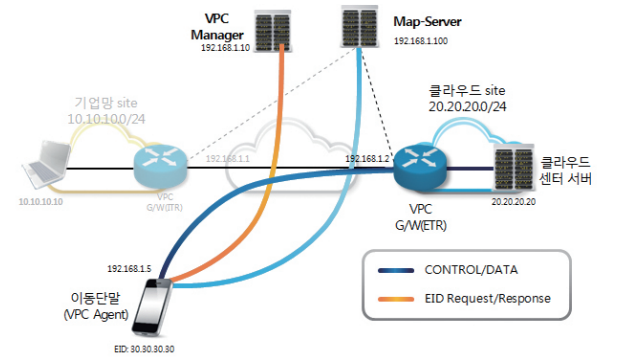

그림 12. 테스트베드 상의 VPC 서비스 구성도

단말에 가상 ID를 부여하여 단말의 위치에 기반한 IP 주소와 독립되어 위치에 무관하게 가상 ID로 통신이 가능하도록 하기 위하여 Map Server와 VPC 게이트웨이 간에 제어 메세지를 주고 받는다. 또한, 클라우드 사이트의 VPC 게이트웨이에 연결된 노드와 엔터프라이즈 사이트의VPC 게이트웨이에 연결된 노드와의 통신이 정상적으로 이루어져야 하는데 이를 위해서 각 VPC 게이트웨이를 거쳐서 데이터 메세지가 전송된다.

구축된 클라우드 사이트에는 GUI를 통하여 인가된 사용자로 접속하게 되면 클라우드 내 자원의 현황 – 생성된 인스턴스 개수, 사용 중인 가상 CPU 수, 메모리 사용량, 스토리지 현황 등에 대한 통계를 볼 수 있으며, 현재 동작 중인 인스턴스 리스트 등 세부 정보를 조회할 수 있고, 새로운 VM 생성, 스토리지 할당 등 가상 클라우드 서비스를 제공 받을 수 있다.

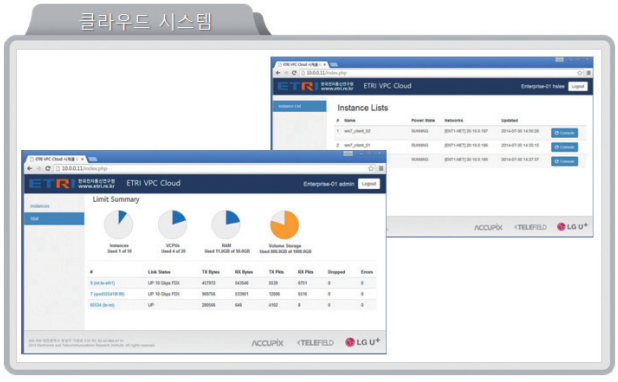

그림 13. 구축된 VPC 사이트 정보

4. VPC 기반의 그룹통신 확장기술 개발

본 논문에서 제안한 가상 ID 기반의 VPC 네트워킹 기술을 확장하여 사용자 그룹별 분리 및 제어 서비스가 가능하다. 즉, 같은 VPC 내에서도 사용자 그룹을 분리하여 접근 가능한 클라우드 자원을 분리할 수 있게 된다. 예를 들어, 〈그림 14〉에서와 같이, 단말 1-1과 2-1, m1, 서버 S-1을 GROUP A로 설정하고, 단말 1-2, 2-2와 server S-2를 GROUP B로 설정한 경우, GROUP A의 멤버 m1이 VPC 클라이언트 단말에서 로그인한 경우, 단말 1-1, 2-1과 서로 통신 가능하고 서버 S-1에만 접속 가능하여, 동일 VPC 내에서도 그 외 다른 단말과의 통신이나 다른 서버에의 접속은 가능하지 않다. GROUP B 에서도 동일하게 동작된다. 이러한 그룹 통신 기능은 사내에서 조직, 직급 등을 분류하여 운용할 때 정부 기관 등에서 사용자의 등급에 따른 차등화 서비스 제공에 활용 가능하다.

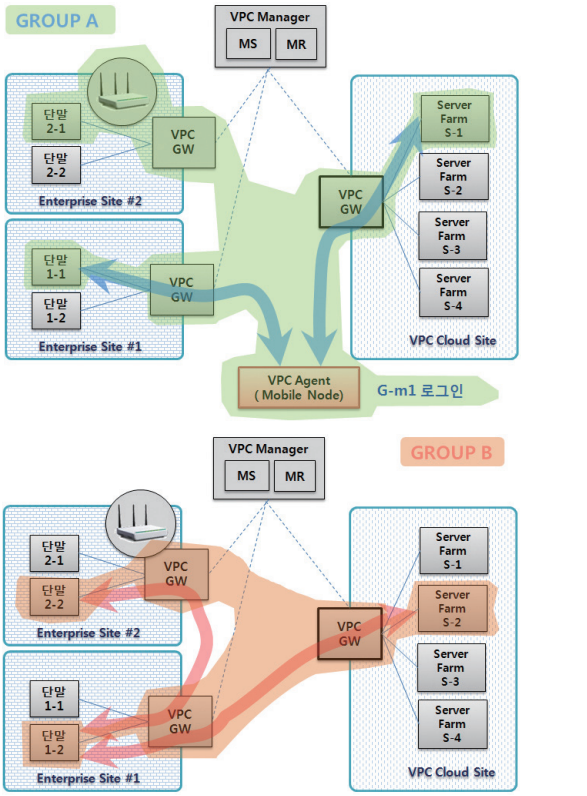

그림 14. VPC 기반의 그룹통신 확장 기술

5. VPC 기술 기반의 홈-클라우드 응용 방안

가상 ID 기반의 VPC 네트워킹 서비스에 3.4절의 그룹통신 기능을 확장하면, ISP 망을 사용하는 홈들 사이의 사설 주소의 중복을 수용하는 홈 네트워킹 서비스에 적용이 가능하다. 홈에서는 홈게이트웨이 내에서 사설망 주소를 사용하게 되는데, 홈 외부에서 VPC를 통해서 외부와 내부를 같은 사설망으로 이용할 수 있게 되어, 한번 홈 클라우드를 구성하면 기존의 서비스 별로 홈 내외 연동을 위한 서버의 중복 구축이 필요한 문제점을 해결할 수 있다. 이는, 가상 ID 기반 주소 음영화 기능을 활용하여 동일한 사설 IP가 할당되어도 VPC GW를 통한 주소 음영화 기능으로 주소 중복 문제가 해결되기 때문이다.

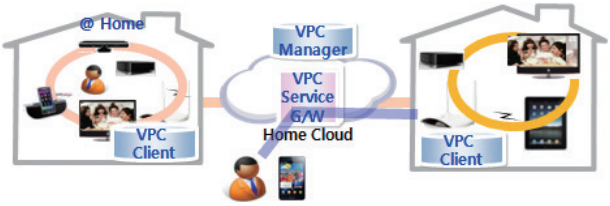

그림 15. VPC 기반의 홈-클라우드 응용 방안

IV. 결 론

본 논문에서는 기업망-모바일-클라우드의 스마트한 연결을 위한 가상 ID 기반의 VPC 네트워킹 기술을 제시하였다. IT 자원을 독자적으로 구축하지 않고 클라우드에서 할당 받아 사용할 수 있는 VPC 서비스는 기업이나 기관의 비용 절감 및 업무의 효율성을 높일 수 있는 장점이 있으며 에너지 절감효과가 있어 그린 IT 실현을 위한 필수 기술이다. 그러나 기존의 기술은 동일 클라우드 내 여러 사설 클라우드 수용 시 사설IP의 중복으로 인하여 서비스가 불가능한 문제가 있다. 또한 이동성을 고려하지 않고 있어 모바일 스마트 기기 수용에 한계가 있다. 이러한 문제점을 해결하기 위하여 본 논문에서는 사설 주소를 사용하는 엔터프라이즈용 단말이 주소의 변경 없이 클라우드 서비스를 이용 가능하도록 주소 음영화 프로토콜을 적용하고, 단말의 이동성 제공이 가능한 VPC 네트워킹의 구조 및 구현에 대하여 기술하였다. 또한 이를 확장하여 동일 VPC내에서 세부 그룹별 관리가 가능한 그룹 통신 기능을 개발하였으며, 이러한 기술을 적용하여 ISP망에서 주소 중복을 허용하는 홈 네트워킹 서비스가 가능한 응용 모델을 제시하였다.

본 기술은 통신사업자 망에서 모바일 스마트기기를 통한 기업 가상 클라우드 접속 서비스 제공을 위한 솔루션 및 보안성이 중요한 국가 공공기관의 스마트워크 플랫폼으로 활용 가능하다.

또한, 클라우드 서비스의 시장 확산을 저해하는 주요 우려 · 장애 요인인 이동성, 정보유출 가능성(보안성), 확장성, 성능예측의 불확실성(품질보장) 등의 문제를 오버레이 기반의 VPC 네트워크 기술로 해결함으로써, IT 기반 네트워크형 사회로의 전환과 IT 인프라의 고도화 및 확충을 가능하게 할 것이다.

Acknowledgement

본 연구는 미래창조과학부 및 정보통신기술진흥 센터의 정보통신 · 방송 연구개발사업의 일환으로 수행하였음. [10043437, 안전하고 확장성있는 가상 ID 기반의 기업망-클라우드-모바일기기 연결을 제공하는 가상 사설망 기술 개발]

참 고 문 헌

[1] Barrie Sonsinsky, “Cloud Computing Bible”, Wiley Publishing, 2011, p108

[2] IDC, “Worldwide Cloud Systems Management Software 2015 – 2019 Forecast”, April 2015.

[3] Gartner, “Hyper Cycle for Small and Midsize Businesses”, 2014

[4] Gartner, “Magic Quadrant for Cloud Infrastructure as a Service, Worldwide”, May 2015

[5] 현종웅, “엔터프라이즈 망과 클라우드 연결형 가상사설클라우드(VPC) 기술 현황 및 전망, 2012.7

[5] 미래창조과학부, “클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률”, 2015.3

[6] 3GPP, “The Evolved Packet Core”

[7] Tharam Dillion, “Cloud Computing: Issues and Challenges”, 2010 24th IEEE ICAINA

[8] Yashpalsinh Jadeja, “Cloud Computing - Concepts, Architectures and Challenges”, 2012 ICCEET

[9] F. John Karautheim, “Private Virtual Infrastructure for Cloud Computing”, June 2009, Proceedings of the cloud computing

[10] Amazon, “Introducing Amazon Virtual Private Cloud (VPC), 2009

[11] Cisco, “Virtualized Multi-Tenant Data Center, 2010

[12] Cloudnets, “Connecting Wide-Area Cloud Resourtces with Virtual Networking”, 2012

[13] LG U+ “Cloud N - Total Managed Cloud Service”, 2012

[14] IRTF, “HIP Experiment Report”, 2011

[15] Cisco, “Locator ID Separation Protocol (LISP) VM Mobility Solution”, 2011

[16] Ji-In Kim, “Mobile Oriented Future Internet (MOFI): Architectural design and Implementations”, ETRI Journal, 2013

약 력

정 부 금

1986년 부산대학교 이학학사
1991년 숙명여자대학교 이학석사
1986년~현재 한국전자통신연구원 책임연구원
관심분야: 클라우드네트워킹

안 병 준

1984년 한양대학교 공학사
1986년 한양대학교 공학석사
1999년 Iowa State Univ. 공학박사
1986년~현재 한국전자통신연구원 책임연구원
관심분야: 클라우드네트워킹

박 혜 숙

1992년 경성대학교 이학학사
1994년 부산대학교 이학석사
2005년 충남대학교 이학박사
1994년~현재 한국전자통신연구원
클라우드네트워킹연구실장
관심분야: 클라우드네트워킹, 고신뢰네트워킹

김 기 철

1990년 전북대학교 공학사
1998년~1999년 대우전자 연구소 선임연구원
1999년~2009년 ㈜휴텔, VK, 아로마(홍콩),
신지소프트 개발담당
2009년~현재 ㈜아큐픽스(구, 텔로드) 플랫폼사업팀
이사
관심분야: IoT, 네트워크 보안

이 동 철

1992년 경상대학교 공학사
1994년 경상대학교 공학석사
2006년 경상대학교 공학박사
1994년~1996년 금호정보통신연구소 주임연구원
1997년~현재 LG유플러스 부장
관심분야: 근거리무선통신, VoIP디바이스,
IoT디바이스