DRAGON 설치 및 테스트 가이드

작성자: 김민아, 홍원택, 공정욱

연구망개발팀, CNI 사업단, 한국과학기술정보연구원
{petimina, wthong, kju}@kisti.re.kr

최종수정일: 2008년 5월 13일

Abstract

DRAGON은 GMPLS에 기반하여 고대역폭을 요구하는 e-Science 와 같은 응용들에 동적이며 결정적인 전용의 LSP를 만들어 주기 위한 소프트웨어이다. 본 문서에서는 DRAGON의 최신 버전인 dcn-software-suit-0.2 기반으로 KISTI에서 개발한 DRAGON VLSR을 설치하고 그 VLSR과 NARB를 테스트할 수 있도록 하나의 가이드를 제공하고자 한다.

Topics

1. 개요

National Science Foundation(NSF)에서 지원하는 DRAGON 프로젝트는 고 대역폭을 요구하는 e-Science 어플리케이션들을 위한 동적이고 결정적인, 관리 가능한 종단간의 네트워크 전송 서비스의 연구와 개발에 대한 것이다.

이러한 구현을 위해 DRAGON은 IP 네트워크 구조를 사용하며 종단 사용자의 요청에 즉각 직접적으로 대응하는 동적이고 결정적(deterministic) 네트워크 경로를 만들기 위해

Generalized Multi-Protocol Label Switching (GMPLS) 기반의 광코어 네트워크를 만든다. GMPLS에서 Label Switching Routers(LSRs)로 작동하는 광 수신 장비와 스위칭 장비는 패킷, 파장, 광전송 등 여러 가지 네트워크 기술을 포괄하는 결정적 네트워크 자원을 제공한다. 이것은 GMPLS에서 정의된 연결, 자원 관리 메커니즘에 그 기초를 두며 연구, 교육(R&E) 네트워크에 기반한 지역 간, 국가 간, 글로벌 광파장의 여러 기능들을 모델링한다[1].

본 문서의 기본적인 목적은 고해상도의 비디오나 짧은 지연을 요구하는 고 대역폭 응용을 위한 네트워크를 동적으로 할당하기를 원하는 사용자를 위해 DRAGON 소프트웨어를 설치하고 사용하는 데 필요한 사항들을 설명하는 것이다. DRAGON 소프트웨어의 기본 동작 및 소프트웨어 아키텍쳐에 관한 보다 자세한 사항은 다음 URL에 “DRAGON 시스템 분석 및 Cisco 7609, Force10 C300 모듈 개발 보고서"를 참조한다.

http://good.kreonet.net/lambda/doku.php?id=documents

Figure 1은 트래픽 엔지니어링을 제공하는 이더넷 스위치와 DRAGON 소프트웨어를 사용하여 만들어진 일반적인 네트워크 토폴로지를 묘사하고 있는데 많은 수의 VLSR들로 이루어진다.

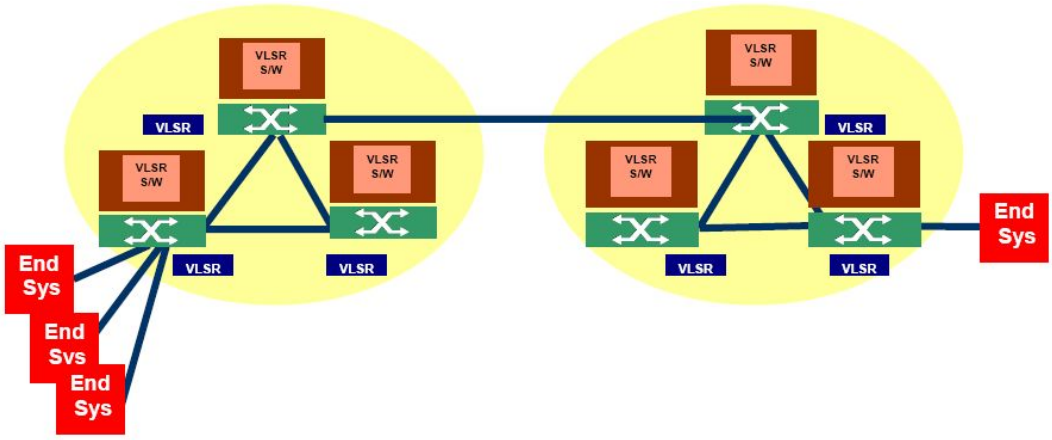

Figure 1. General DRAGON S/W Network Topology

현재 DRAGON의 가장 최근 버전은 Internet2를 위한 Dynamic Circuit Network(DCN)의 일부분인 Domain Controller (DC) 로 활용되고 있는 dcn-software-suit-0.2이다. 본 문서는 dcn-software-suit-0.2에 포함된 VLSR 과 NARB의 설치 및 시험을 위한 가이드이며, dcn-software-suit-0.2를 기반으로 KISTI에 의해 개발된 추가 확장 모듈의 설치 및 시험을 위한 가이드이다.

1.1 DRAGON Components

DRAGON 소프트웨어는 다음의 주요 요소들로 구성되어 있다.

- VLSR(Virtual Label Switch Router)
  제어평면 구성요소로 OSPF-TE, RSVP-TE와 프로비저닝을 시작할 수 있는 사용자 인터페이스를 제공한다. Internet 2의 Ciena Core Director가 있는 하나 혹은 그 이상의 네트워크 장비들에 설정할 수 있다. 이것은 이더넷 SONET circuit의 다양한 이더넷 포드들에 활용될 수 있다. 또한 VLSR은 GMPLS를 지원하지 않는 이더넷 스위치들을에서 자동 VLAN 설정을 통해 동적인 circuit을 설정할 수 있다.
- NARB (Network Aware Resource Broker)/RCE (Resource Computation engine)
  제어 평면 구성요소로 멀티 도메인 멀티 레벨 Path Computation Element(PCE) 와 도메인 간 라우팅 기능을 제공한다.
- DRAGONMon(DRAGON Monitor)
  존재하는 LSP의 상태를 감시하고, 다른 시스템이 접근할 수 있도록 MySQL 데이터베이스에 저장한다.

1.2 DRAGON 소프트웨어 다운로드

DRAGON 소프트웨어는 DCN 소프트웨어의 일부로 배포되며, 다음 URL 로 다운로드 받을 수 있다.

https://wiki.internet2.edu/confluence/display/DCNSS

다운로드 후에 다음의 명령어로 압축을 푼다.

```
[root@kisti-1 ~]# gunzip dcn-software-suite-0.2.tar.gz
[root@kisti-1 ~]# tar -xvf dcn-software-suite-0.2.tar
```

압축을 풀면 dcn-software-suite-0.2 아래에 다음의 파일과 디렉토리가 생성된다.

```
[root@kisti-1 dcn-software-suite-0.2]# ls
CHANGES  dragon  idc  README
```

이중 DRAGON 소프트웨어는 dragon 디렉토리에 존재한다. dragon 디렉토리에는 두 개의 tar 파일 dragon-sw-snapshot.2007Dec21.tar 와 narb-sw-snapshot.2007Dec21.tar 가 생성되어 있다. VLSR을 위해서는 dragon-sw-snapshot.2007Dec21.tar을 NARB를 위해서는 narb-sw-snapshot.2007Dec21.tar 을 풀면 된다.

```
[root@kisti-1 dragon]# tar -xvf dragon-sw-snapshot.2007Dec21.tar
[root@kisti-1 dragon]# tar -xvf narb-sw-snapshot.2007Dec21.tar
```

압축을 푼 시스템을 VLSR로 사용한다 할지라도 NARB와의 연결에 대한 테스트를 위해서는 NARB도 압축을 풀어서 설치 하는 것이 좋다.

dcn-software-suite-0.2/dragon 디렉토리에 압축을 풀고나면, dragon-sw 와 narb-sw 디렉토리가 생성된다. 설치는 다시 각 하위 디렉토리로 이동하여 진행된다.

```
[root@kisti-1 dragon]# ls
docs          dragon-sw-snapshot.2007Dec21.tar   narb-sw-snapshot.2007Dec21.tar
dragon-sw     narb-sw
```

2. DRAGON 및 NARB 설치

2.1 설치에 앞서

DRAGON 소프트웨어를 설치하기 전에 몇 가지 먼저 준비해야 할 것이 있다. 본 절에서는 VLSR과 NARB/RCE를 위한 시스템, 하드웨어 및 소프트웨어 요구사항을 정리한다. NARB/RCE와 VLSR의 시스템, 하드웨어 및 소프트웨어 요구사항은 거의 동일하다.

2.1.1 시스템 요구사항

1) Hardware

다음은 DRAGON 을 설치하고 실행하는 필요한 시스템 최소사양이다.

- 500MH의 프로세서 속도 (Pentium III level)
- 256 RAM
- OS 설치 후 1GB 이상의 하드 디스크 여유 공간
- 두 개 이상의 네트워크 인터페이스 (Fast or Gigabit)

KISTI의 확장 추가 모듈의 개발과 테스트는 Intel Hyerpertown QuadCore 5410 System (2.33GHz), 4GB ECC Fully Buffered DDR2 (8 DIMMs) Max 32GB 메모리, 320GB 하드디스크, PCI-E Type 1G 광타입, UTP 타입 NIC이 있는 시스템에서 이루어 졌다.

2) Operating System

호스트와 VLSR 제어 시스템은 리눅스(kernel version 2.4.20 이거나 그 이상)나 FreeBSD(kernel version 4.11 이거나 그 이상), 혹은 리눅스, FreeBSD의 hybrid 에서만 실행 가능하다. DRAGON 소프트웨어의 개발 그룹에서는 이 소프트웨어를 RedHat v9, RedHat Fedora Core3 와 4, RedHat Enterprise Linux AS release 4, Debian 4.0, FreeBSD4.11-RELEASE 와 6.1-RELEASE에서 테스트 하였다. KISTI의 확장 추가 모듈의 개발과 테스트는 RedHat Fedora Core 7에서 이루어 졌다.

2.1.2 소프트웨어 요구사항

• ssh

ssh는 원격 장치에 안전하게 로그인 할 수 있는 방법을 제공한다. ssh를 사용하여 안전하지 않은 채널 상에서도 안전하게 파일을 다른 곳으로 옮길 수 있다. 네트워크에 있는 장치에 대해 루트 권한을 가지고 있는 사람이나 물리적으로 접근할 수 있는 사람은 다양한 방법을 통해서 인가되지 않은 접속을 할 수 있다. ssh는 보통 리눅스와 FreeBSD 설치 패키

지에 포함 되지만 그렇지 않은 경우에는 설치하면 되며 주소는 다음과 같다.

ftp://ftp.net.ohio-state.edu/pub/security/ssh

• GNU Compilers

gcc/g++: 소프트웨어는 GNU GCC/G++ 2.95.x, 3.2.x, 3.4.x 와 4.0.x 버전에서 컴파일 되었다. KISTI 확장 모듈 개발은 GCC 4.1.2 i386-redhat-linux로 컴파일 되었다. 시스템은 64bit를 지원하지만, 소프트웨어의 소스 내에 unit32 타입이 있기 때문에 이를 성공적으로 컴파일 하기 위해서는 GCC는 32bit 컴파일러여야 한다.

bision: bison은 .y 파일들을 파싱하기 위한 GNU 파서 제네레이터이다.
flex: flex 는 .l 파일을 파싱하기 위한 빠른 어휘 분석 제네레이터이다.

• Net-SNMP

DRAGON 소프트웨어는 Net-SNMP의 설치가 요구된다. 문서에서 제시하는 예제는 Net-SNMP version 5.1.1을 사용하였다. 이것의 다운로드는 다음 링크에서 가능하다.

http://prdownloads.sourceforge.net/netsnmp/

Net-SNMP는 IPv4와 IPv6 둘 다 가능한 SNMP v1, SNMP v2c, SNMP v3을 구현하기에 적합한 어플리케이션이다. 이 어플리케이션은 Command Line 어플리케이션, 그래픽 MIB Browser, SNMP 알림을 수신하기 위한 데몬 어플리케이션, C와 Perl API들이 제공하며, 새로운 SNMP 어플리케이션 개발을 지원할 수 있도록 관리 정보에 대한 SNMP 쿼리/응답 에이전트와 확장 에이전트를 포함한다. Net-SNMP의 모든 버전은 다음 링크에서 이용가능하다.

http://www.net-snmp.org/download

Net-SNMP를 다운 받은 후 다음의 과정으로 설치한다.

1. > ./configure
2. > make
3. > make install
4. > cp EXAMPLE.conf /usr/local/share/snmp/snmpd.conf
5. > ln -s /usr/local/lib/libnetsnmp.so.8 /usr/lib/libnetsnmp.so.8

마지막 4와 5의 과정을 수행하지 않으면 DRAGON 소프트웨어를 제대로 실행할 수 없다. RSVPD 실행 시 libnetsnmp.so.8 에 대한 링크 오류가 발생했다면, 5의 명령어를 수행하면 된다. 이것은 RSVPD는 실행 시 동적 라이브러리 참조 디렉토리로 /usr/lib 를 사용하지 않기 때문이다. 따라서, RSVPD를 위해 실제 라이브러리가 있는 곳에 링크를 걸어준다. KISTI 확장 개발 모듈은 net-snmp-5.1.4 버전으로 개발되었다.

• SVN

svn은 오픈소스버전 제어 시스템의 하위 버전 제어에 사용하는 명령이다. 하위 버전에서, 파일의 트리는 중앙 저장 장소에 유지된다. 저장 장소에서는 파일의 구성과 디렉토리의 변경 사항에 대한 모든 사항을 저장한다. 이것은 만약 잘못된 변경 사항으로 데이터가 구성될 경우, 모든 작업이 변경되기 때문에 이전 데이터는 손실됨을 의미한다. 즉, 파일에 대한 변경이 일어났다 하더라도, 파일의 다른 버전만큼 오리지널 파일은 항상 어디에서든 참조될 수 있다. SVN의 설치 유무를 알기 위해서는 다음의 명령어를 실행하면 된다. 만일 설치되어 있다면 아래와 같이 설치 된 곳을 위치를 알려 줄 것이다.

```
[root@kisti-1 lib]# whereis svn
svn: /usr/bin/svn /usr/share/man/man1/svn.1.gz
```

설치되어 있지 않다면, 하위 버전은 다음 링크로부터 설치할 수 있다.

http://subversion.tigris.org

• libxml2

libxml2는 XML 파일들을 파싱하기 위해서 사용된다. DRAGON CSA 소프트웨어는 XML로 설명된 특정 응용 토폴로지 제공을 지원하기 위해 이 라이브러리를 필요로 하며 그것은 특성들이 VLSR과 무관할지라도 libxml2 라이브러리로 컴파일 되어야 한다. 일반적으로 이 라이브러리는 /usr/lib 에 설치되어 있다.

2.2 VLSR 설치

다운로드 받은 소프트웨어 패키지의 압축을 풀고 나면, VLSR은 /DCN 설치디렉토리 /dcn-software-suite-0.2/dragon/dragon-sw 에 압축이 풀려있는 상태이다. VLSR의 설치는 먼저 이 디렉토리로 이동하여 시작한다.

```
[root@kisti-1 dragon-sw]# pwd
/root/dcn-software-suite-0.2/dragon/dragon-sw
[root@kisti-1 dragon-sw]#
```

2.2.1 Basic Installation

DRAGON package가 설치되거나 검사된 디렉토리로 이동한다. 마지막으로 DRAGON 소프트웨어를 설치하기 위한 명령을 수행한다.

```
[root@kisti-1 dragon-sw]# ./do_build.sh
[root@kisti-1 dragon-sw]# ./do_install.sh
```

디폴트로 소프트웨어는 /usr/local/dragon에 설치된다. 단계적인 설치 방법을 사용하고자 한다면, KOM-RSVP (DRAGON RSVPTE)를 포함한 DRAGON 소프트웨어와 GNU

ZEBRA (DRAGON OSPF-TE와 CSA 포함)를 각각의 디렉토리에 들어가 직접 설치 할 수도 있다.

a) KOM-RSVP:
kom-rsvp 디렉토리에 들어가서,

```
#cd kom-rsvp
```

kom-rsvp 코드가 구성되었다면, return을 입력하여 되돌아갈 수 있다.

```
#. /configure ---with-snmp=/usr/local
```

이 명령은 /usr/local에(또는 지정된 경로) 설치된 net-snmp 헤더파일을 가지고 kom-rsvp와 snmp를 구성한다. 구성 한 후, 디렉토리는 비워지며 파일 의존성은 재구성된다. :

```
# gmake clean
# gmake depend
```

마지막으로 코드가 재컴파일 되며, 새로운 바이너리와 라이브러리가 시스템이 설치된다.

```
# gmake
# sudo gmake install
```

b) GNU ZEBRA:
OSPF는 다음과 같이 설치될 수 있다. :
dragon-sw 디렉토리 내부의 zebra 디렉토리로 이동한다.

```
# cd zebra
```

다음 명령을 수행하여 프로토콜을 구성한다. prefix 명령은 ZEBRA-OSPF가 설치될 장소를 지시한다.

```
#. /configure --prefix=/usr/local/dragon ---enable-dragon
```

마지막으로, 코드를 컴파일하고 파일을 설치한다.

```
# make
# sudo make install
```

2.2.2 Advanced Installation

사용자는 소프트웨어 구성을 자신에게 맞추어 타겟 옵션을 사용할 수 있다. 목적에 맞게 사용하기 위해서 본 설치 방법을 권장한다.

```
# ./do_build.sh [target]
```

build option[target]은 구성하려는 컨트롤 개체의 종류를 말한다. 컨트롤 개체는 다음 중 하나이다. [target] option이 없을시, 디폴트로 vlsr이 사용된다.

vlsr	-- 스위치 종류에 따른 자동 설정을 사용하는 일반적인 VLSR 구성
vlsr-verbose	-- Building a VLSR 사용자의 대화식 입력을 통한 VLSR 구성
vlsr-force10	-- Force10 E300/E600 스위치에서 동작하는 VLSR 구성
vlsr-force10-v6	-- 소프트웨어 버전 6.x.x.x Force10 스위치에서 동작하는 VLSR 구성
vlsr-force10-v6-c300	-- 소프트웨어 버전 6.x.x.x Force10 c300 스위치에서 동작하는 VLSR 구성 (KISTI에 의해 추가됨)
vlsr-cat3750	-- Cisco Catalyst 3750 스위치를 위한 VLSR 구성
vlsr-cat6500	-- Cisco Catalyst 6500 스위치를 위한 VLSR 구성
vlsr-raptor	-- Raptor E1010 스위치에서 동작하는 VLSR 구성
csa	-- Client System Agent 구성
narb	-- NARB 서버를 위한 소프트웨어 컴포넌트 구성

디폴트로, 이 소프트웨어는 /usr/local/dragon에 설치된다. do_build.sh and do_install.sh 스크립트를 실행하기 전에 환경 변수 $DRAGON_PREFIX의 설정을 통해 설치 디렉토리를 변경할 수 있다.

다음은 보다 단계적인 설치과정을 제공한다. DRAGON RSVP-TE (KOM-RSVP)을 위해 --with-snmp 옵션을 가진 ./configure 스크립트를 실행했을 때, 두 가지 파라미터가 요구된다.

```
Switch Vendor/Model number (Default: AutoDetect):
```

하나는 Section 4.0에서 정의된 Vendor/Model ID(Force10E600, RaptorER1010)이다. 이것을 사용하지 않는다면 AutoDetect를 사용하게 되며, VLSR은 쿼리 시스템에 의해 자동적으로 SNMP을 통해 스위치의 벤더/모델을 결정한다.

```
Switch control port (Default: 255):
```

스위치 제어 포트(switch control port)는 제어 네트워크로 스위치를 연결하기 위한 스위치 포트이다. 만약 스위치 제어 포트가 데이터-플레인 포트로써 이동된다면, 스위치는 컨트롤-플레인으로부터 끊어질 것이다. 데이터-플레인 포트로 변경되는 것을 피하기 위해 스위치 제어 포트(switch control port)를 설정할 수 있다.

DRAGON RSVP-TE (KOM-RSVP) 소프트웨어는 --with-snmp을 추가하는 사전-컴퍼일 구성 옵션을 가진다.

--enable-switch-cli-access는 CLI 제어 메소드를 사용하기 위해 VLSR을 설정한다. vlsr-force10과 vlsr-force10-v6로 target 을 설정할 경우 자동으로 요구한다. 이때 해당 스위치를 접근하여 사용할 수 있는 Username과 Password를 입력하면 된다.

사용자이름, 패스워드 CLI 타입(telnet,ssh)의 입력이 요구된다.

```
Username (Default: unknown):
Password (Default: unknown):
CLI Session Type (Default: none):
```

--enable-switch-port-shutdown은 VLAN으로부터 벗어난 경우나 다른 VLAN으로부터 종료하였을 경우, 스위치 데이터 포트를 종료하기 위해 수행한다.

2.2 NARB 설치

다운로드 받은 소프트웨어 패키지의 압축을 풀고나면, NARB는 /DCN 설치디렉토리 /dcn-software-suite-0.2/dragon/narb-sw 에 압축이 풀려있는 상태이다. NARB의 설치는 먼저 이 디렉토리로 이동하여 시작한다.

```
[root@kisti-1 narb-sw]# pwd
/root/dcn-software-suite-0.2/dragon/narb-sw
[root@kisti-1 narb-sw]#
```

컴파일과 인스톨은 매우 간단한다. VLSR과 마찬가지로 두 가지의 명령어를 수행하면 된다. 그러나, 추가적인 선택사항은 없다.

```
[root@kisti-1 dragon-sw]# ./do_build.sh
[root@kisti-1 dragon-sw]# ./do_install.sh
```

3. Basic DRAGON VLSR 설정 및 시험

본 장에서는 하나의 VLSR과 하나의 스위치가 설치된 가장 기본이 되는 네트워크 토폴로지에서 동일 스위치내의 두 개의 포트를 연결하는 간단한 시험을 통해 VLSR의 동작원리를 살펴본다. 보다 복잡한 설정들은 이러한 설정을 기본으로 한다.

Figure 2는 시험 네트워크의 토폴로지를 보여준다. 네트워크는 하나의 switching hub 인 cisco 3750 스위치로 제어 채널을 위한 모든 시스템이 연결되어 있다. VLSR1 시스템은 Cisco 7609 스위치를 제어하기 위한 VLSR이 설치된 장비이며, 여기에 데이터 평면의 종단 소프트웨어인 CSA (Client System Agent)를 CSA1 시스템과 CSA2 시스템에 설치한다. CSA1 시스템은 Cisco7609 Switch의 Gi8/0/2 포트에 연결되어 있으며, CSA2 시스템은 Gi8/0/1 포트에 연결되어 있다. 이 시험에서 우리는 Gi8/0/2 포트와 Gi8/0/1 포트를 DRAGON 소프트웨어를 통해 자동으로 하나의 VLAN으로 묶어 CSA1과 CSA2가 통신이 가능하게끔 연결되는 것을 본다.

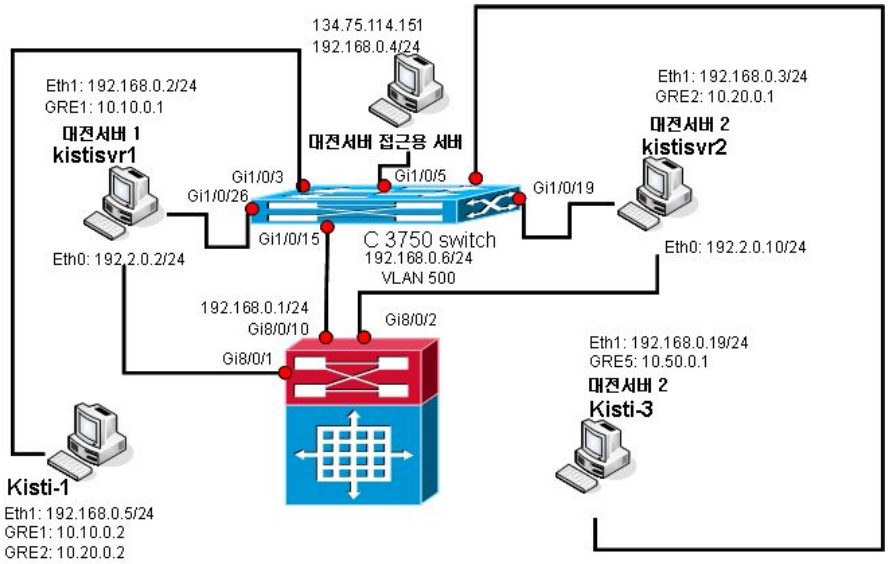

Figure 2. Basic VLSR Test Network Topology

이러한 설정을 위해 먼저 각각의 시스템에 DRAGON 소프트웨어를 2장의 절차에 맞게 설치한다. 물론 CSA1과 CSA2 시스템에는 do_build.sh 를 이용한 자동 컴파일 시에 csa 옵션을 주고, VLSR1에는 vlsr 옵션을 주되, Switch Vendor/Model number (Default: AutoDetect): 은 디폴트인 AutoDetect로 엔터키만 누르면 된다.

DRAGON 소프트웨어의 설지가 끝나면, 각각의 시스템 별로 설정파일을 편집한 후 DRAGON 소프트웨어를 기동하면 된다. 3장의 각 절에서는 이러한 세부적인 설정에 대해 설명한다.

3.1 GRE 터널링 설정

DRAGON 은 제어 평면과 데이터 평면을 분리하고 있으며, 자동설정을 위한 모든 제어 패킷들은 제어 평면상에서만 이동한다. 이러한 제어 평면을 구성하기 위해, 각각의 시스템은 제어 평면을 위한 네트워크 인터페이스 카드와 데이터 평면을 위한 네트워크 인터페이스 카드 적어도 두 개의 네트워크 카드가 필요한 것이다.

DRAGON 소프트웨어의 핵심인 제어평면에서의 제어 프로토콜은 데이터 평면과 다른 독자적인 네트워크를 구성한다. 이를 위해 DRAGON 은 GRE 터널링을 도입한다. 제어평면의 프로토콜 데이터들은 이 GRE 터널을 통해서 이동한다.

DRAGON의 제어평면 프로토콜인 OSPF-TE와 RSVP-TE가 동작하기 위해 이들이 설치되어 있는 시스템은 서로 GRE 터널로 연결되어 있어야 한다. Figure 2에서 종단 시스템이 모두 CSA 라는 것은 Peer-to-Peer 모델로 종단 사용자 시스템이 직접 라우팅에 참여 한다는 것을 의미한다.

따라서, Figure 2의 네트워크 구성에서는 두 개의 GRE 터널이 필요하다. 하나는 CSA1로부터 제어 시스템인(VLSR)으로 연결된 gre1이고 다른 하나는 CSA2로부터 제어 시스템인(VLSR)으로 연결된 gre2이다. 라우팅과 시그널링 메시지는 GRE 터널을 통해 CSA1에서 CSA2로 전달된다.

Linux 시스템인 CSA1, CSA2은 물론 그 반대 VLSR1에서도 이를 위해 각 시스템에서 다음의 설정을 해주어야 한다. del 명령은 gre1이 기존에 존재하였다면, 이를 지우기 위한 명령어로 새로 생성할 경우 실행하지 않아도 된다.

1) CSA1

```
[root@kistisvr1 sbin]# /sbin/modprobe ip_gre
[root@kistisvr1 sbin]# /sbin/ip tunnel del gre1
[root@kistisvr1 sbin]# /sbin/ip tunnel add gre1 mode gre remote 192.168.0.5 local 192.168.0.2 ttl 255
[root@kistisvr1 sbin]# /sbin/ip link set gre1 up
[root@kistisvr1 sbin]# /sbin/ip addr add 10.10.0.1/30 dev gre1
[root@kistisvr1 sbin]# /sbin/ip route add 10.10.0.2 dev gre1
```

2) CSA2

```
[root@kistisvr2 sbin]# /sbin/modprobe ip_gre
[root@kistisvr2 sbin]# /sbin/ip tunnel del gre2
[root@kistisvr2 sbin]# /sbin/ip tunnel add gre2 mode gre remote 192.168.0.5 local 192.168.0.3 ttl 255
[root@kistisvr2 sbin]# /sbin/ip link set gre2 up
[root@kistisvr2 sbin]# /sbin/ip addr add 10.20.0.1/30 dev gre2
[root@kistisvr2 sbin]# /sbin/ip route add 10.20.0.2 dev gre2
```

3) VLSR1

```
[root@kisti-1 sbin]# /sbin/modprobe ip_gre
[root@kisti-1 sbin]# /sbin/ip tunnel add gre1 mode gre remote 192.168.0.2 local 192.168.0.5 ttl 255
[root@kisti-1 sbin]# /sbin/ip link set gre1 up
[root@kisti-1 sbin]# /sbin/ip addr add 10.10.0.2/30 dev gre1
[root@kisti-1 sbin]# /sbin/ip route add 10.10.0.1 dev gre1
```

```
[root@kisti-1 sbin]# /sbin/ip tunnel add gre2 mode gre remote 192.168.0.3 local
192.168.0.5 ttl 255
[root@kisti-1 sbin]# /sbin/ip link set gre2 up
[root@kisti-1 sbin]# /sbin/ip addr add 10.20.0.2/30 dev gre2
[root@kisti-1 sbin]# /sbin/ip route add 10.20.0.1 dev gre2
```

이들이 제대로 설정되어 있는지 확인하기 위해서는 다음의 명령어를 치면 된다.

```
[root@kistisvr1 sbin]# ip tunnel show
gre0: gre/ip  remote any  local any  ttl inherit  nopmtudisc
gre1: gre/ip  remote 192.168.0.5  local 192.168.0.2  ttl 255

[root@kistisvr2 sbin]# ip tunnel show
gre0: gre/ip  remote any  local any  ttl inherit  nopmtudisc
gre2: gre/ip  remote 192.168.0.5  local 192.168.0.3  ttl 255

[root@kisti-1 sbin]# ip tunnel show
gre0: gre/ip  remote any  local any  ttl inherit  nopmtudisc
gre1: gre/ip  remote 192.168.0.2  local 192.168.0.5  ttl 255
gre2: gre/ip  remote 192.168.0.3  local 192.168.0.5  ttl 255
```

반드시, remote 와 local 의 ip 가 제대로 되어 있는지 확인해야 한다. 또한 동작이 제대로 되는 지 확인하기 위해서는 각 시스템에서 GRE 터널에서 부여한 GRE IP 로 상대방 시스템에 ping 을 해서 확인한다. DRAGON 시스템이 동작이 제대로 되지 않는 가장 잦은 실수 중 하나가 네트워크 토폴로지가 복잡할 경우 GRE 설정을 제대로 못했을 때이다.

3.2 DRAGON 소프트웨어 설정 파일

각 시스템에는 DRAGON 소프트웨어가 동작하는 데 필요한 설정파일들이 있다. 이들은 시스템이 설치 될 때 자동적으로 /usr/local/dragon/etc 디렉토리에 *.*.sample의 확장자로 설치된다. 우리는 이 sample 파일들을 제대로 편집해서 *.conf 파일로 만들어 주어야 한다.
본 절에서는 이들 기본 설정파일들을 어떻게 설정하는지 설명한다.

3.2.1 CSA1 설정 파일

CSA1에서 동작을 위해 설정해 주어야 하는 파일은 dragon.conf, ospfd.conf, RSVPD.conf, zebra.conf 로 모두 4개이다. 다음은 각각의 설정 파일에 대한 설정이다.

1) dragon.conf

dragon.conf 파일은 DRAGON 소프트웨어 실행 시 dragon 데몬이 참조하는 파일이다. password 는 lsp 설정을 위해 dragon vty 에 접속할 때 필요한 설정이며, hostname 은 vty의 prompt 로 표시된다.

```
! -*- dragon -*-
!
! DRAGON sample configuration file
!
hostname csa1-dragon
password dragon
```

2) ospfd.conf

```
! -*- ospf -*-
!
! OSPFd sample configuration file
!
hostname csa1-ospf
password dragon
enable password dragon
log stdout
log file /var/log/ospfd.log
!
! NOTE: max. bandwidth parameters are in bytes/sec, for example:
!    1 Gbps = 125000000 bytes/sec
!   10 Gbps = 1250000000 bytes/sec
!
! -*- sample ospf configuration for a dragon VLSR controlling a Layer2 Ethernet switch -*-
!

interface gre1
 description GRE tunnel between csa1(kistisvr1) and vlsr1(kisti-1)
 ip ospf network point-to-point
!
router ospf
 ospf router-id 192.168.0.2
 network 10.10.0.0/30 area 0.0.0.0
 ospf-te router-address 192.168.0.2
 ospf-te interface gre1
       level gmpls
       data-interface ip 10.1.10.1
       swcap l2sc encoding ethernet
       max-bw 125000000
       max-rsv-bw 125000000
       max-lsp-bw 0 125000000
       max-lsp-bw 1 125000000
       max-lsp-bw 2 125000000
       max-lsp-bw 3 125000000
       max-lsp-bw 4 125000000
```

```
      max-lsp-bw 5 125000000
      max-lsp-bw 6 125000000
      max-lsp-bw 7 125000000
      vlan 100 to 200
      metric 10
 exit
!
line vty
!
```

3) RSVPD.conf

RSVPD 데몬 프로세스가 기동 시 참조하는 파일로 시그널링을 위한 GRE 인터페이스를 설정할 수 있다.

```
interface gre1 tc none mpls
api 4000
```

4) zebra.conf

zebra.conf 는 zebra 데몬 프로세스가 기동 시 참조하는 파일로 라우팅 시 사용되는 인터페이스를 설정할 수 있다. zebra 데몬 프로세스는 실제 DRAGON 소프트웨어에서 불필요해 보이지만, ospfd 가 LSA를 보내 수집한 정보를 라우팅 테이블에 업데이트 하는 것은 ospfd가 아니라 zebra 프로세스이며, 이 라우팅 테이블에 있는 인터페이스 정보도 zebra.conf에서 얻어온다. ospfd에도 GRE 인터페이스에 대한 설정이 있지만, 이 설정은 인터페이스에 대한 속성을 정의하는 것이다. 따라서, zebra.conf 파일에는 반드시 라우팅에 사용하는 모든 인터페이스가 기술되어 있어야 한다. 따라서, CSA1의 설정은 다음과 같다.

```
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.14 1999/02/19 17:26:38 developer Exp $
!
hostname csa1-zebra
password zebra
enable password zebra
!
! Interface's description.
!
interface lo
interface gre1
!
line vty
log file /var/log/zebra.log
```

3.2.2 CSA2 설정 파일

CSA2도 CSA1과 마찬가지로 동작을 위해 설정해 주어야 하는 파일은 dragon.conf, ospfd.conf, RSVPD.conf, zebra.conf 로 모두 4개이다. 설정의 내용은 CSA1과 같고, CSA2에 맞는 hostname, IP 등만 설정해 주면 된다. 다음은 각각의 설정 파일에 대한 설정이다.

1) dragon.conf

```
! -*- dragon -*-
!
! DRAGON sample configuration file
!
hostname csa2-dragon
password dragon
```

2) ospfd.conf

```
! -*- ospf -*-
!
! OSPFd sample configuration file
!
hostname csa2-ospf
password dragon
enable password dragon
log stdout
log file /var/log/ospfd.log
!
! NOTE: max. bandwidth parameters are in bytes/sec, for example:
!    1 Gbps = 125000000 bytes/sec
!   10 Gbps = 1250000000 bytes/sec
!
! -*- sample ospf configuration for a dragon VLSR controlling a Layer2 Ethernet switch -*-
!

interface gre2
 description GRE tunnel between csa2(kistisvr2) and vlsr1(kisti-1)
 ip ospf network point-to-point
!
router ospf
 ospf router-id 192.168.0.3
 network 10.20.0.0/30 area 0.0.0.0
 ospf-te router-address 192.168.0.3
 ospf-te interface gre2
      level gmpls
      data-interface ip 10.1.10.6
      swcap l2sc encoding ethernet
```

```
      max-bw 125000000
      max-rsv-bw 125000000
      max-lsp-bw 0 125000000
      max-lsp-bw 1 125000000
      max-lsp-bw 2 125000000
      max-lsp-bw 3 125000000
      max-lsp-bw 4 125000000
      max-lsp-bw 5 125000000
      max-lsp-bw 6 125000000
      max-lsp-bw 7 125000000
      vlan 100 to 200
      metric 10
 exit
!
line vty
!
```

3) RSVPD.conf

```
interface gre2 tc none mpls
api 4000
```

4) zebra.conf

```
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.14 1999/02/19 17:26:38 developer Exp $
!
hostname kistisvr2
password zebra
enable password zebra
!
! Interface's description.
!
interface lo
interface gre2
!
line vty
log file /var/log/zebra.log
```

3.2.2 VLSR1 설정 파일

VLSR1도 CSA1과 마찬가지로 동작을 위해 설정해 주어야 하는 파일은 dragon.conf, ospfd.conf, RSVPD.conf, zebra.conf 로 모두 4개이다. 그러나, 설정의 내용은 CSA들과

다르다. VLSR은 자신이 제어하고 있는 스위치의 포트 정보에 대해 알고 있어야 한다. 다음은 각각의 설정파일의 내용이다.

1) dragon.conf
dragon.conf의 내용은 CSA1이나 CSA2와 다르지 않다. prompt 에 vlsr 임을 명시하기 위해 hostname을 vlsr로 설정하였다.

```
! -*- dragon -*-
!
! DRAGON sample configuration file
!
hostname vlsr-dragon
password dragon
```

2) ospfd.conf
VLSR1의 ospfd.conf는 CSA의 그것과 다르다. 먼저 CSA1, CSA2 양쪽 인터페이스 GRE를 모두 명시해야 한다. 또한 각 ospf-te interface gre1, interface gre2의 data-interface 설정에 실제 스위치의 ip 와 port 정보가 포함되어 있다. 이 중 switch-port 는 정수로만 입력할 수 있으므로, 주의를 요한다. 각 스위치 마다 이 정수를 해석하는 방법은 다르다.

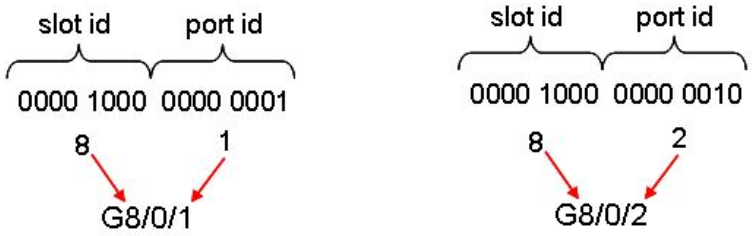

Figure 3. Cisco 7609 Port Conversion

Figure 3는 Cisco 7609 가 2049와 2050을 G8/0/1과 G8/0/2로 해석하는 방법을 보여 준다. 이 파일에 정의되어 있는 2049, 2050 포트는 실제 G8/0/1과 G8/0/2 이다. 2049는 이진수로 0000 1000 0000 0001 이고, 2050은 이진수로 0000 1000 0000 0010 이다. 다른 포트를 data-interface 에 정의하고자 할 때도 cisco 7609의 경우 위의 룰을 따라 정수로 port id를 정수로 바꾸어 설정해 주어야 한다.

```
! -*- ospf -*-
!
! OSPFd sample configuration file
!
hostname vlsr1-ospf
password dragon
enable password dragon
log stdout
```

```
log file /var/log/ospfd.log
!
! NOTE: max. bandwidth parameters are in bytes/sec, for example:
!    1 Gbps = 125000000 bytes/sec
!   10 Gbps = 1250000000 bytes/sec
!
! -*- sample ospf configuration for a dragon VLSR controlling a Layer2 Ethernet switch -*-
!
interface gre1
 description GRE tunnel between csa1(kistisvr1) and vlsr1(kisti-1)
 ip ospf network point-to-point
!
interface gre2
 description GRE tunnel between csa2(kistisvr2) and vlsr(kisti-1)
 ip ospf network point-to-point
!

router ospf
 ospf router-id 192.168.0.5
 network 10.10.0.0/30 area 0.0.0.0
 network 10.20.0.0/30 area 0.0.0.0
 ospf-te router-address 192.168.0.5
 ospf-te interface gre1
        level gmpls
        swcap l2sc encoding ethernet
        data-interface ip 10.1.10.2 protocol snmp switch-ip 192.168.0.1 switch-port 2049
        max-bw 125000000
        max-rsv-bw 125000000
        max-lsp-bw 0 125000000
        max-lsp-bw 1 125000000
        max-lsp-bw 2 125000000
        max-lsp-bw 3 125000000
        max-lsp-bw 4 125000000
        max-lsp-bw 5 125000000
        max-lsp-bw 6 125000000
        max-lsp-bw 7 125000000
        metric 10
 exit
 ospf-te interface gre2
        level gmpls
        swcap l2sc encoding ethernet
        data-interface ip 10.1.10.5 protocol snmp switch-ip 192.168.0.1 switch-port 2050
        max-bw 125000000
        max-rsv-bw 125000000
        max-lsp-bw 0 125000000
        max-lsp-bw 1 125000000
```

```
        max-lsp-bw 2 125000000
        max-lsp-bw 3 125000000
        max-lsp-bw 4 125000000
        max-lsp-bw 5 125000000
        max-lsp-bw 6 125000000
        max-lsp-bw 7 125000000
        metric 10
 exit
!
line vty
!
```

3) RSVPD.conf
두 CSA 들과의 시그널링 인터페이스를 모두 기술해 준다.

```
interface gre1 tc none mpls
interface gre2 tc none mpls
api 4000
```

4) zebra.conf
두 CSA 들과의 인터페이스를 모두 기술해 준다.

```
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.14 1999/02/19 17:26:38 developer Exp $
!
hostname vlsr1-zebra
password zebra
enable password zebra
!
! Interface's description.
!
interface lo
interface gre1
interface gre2
!
line vty
log file /var/log/zebra.log
```

3.3 스위치 준비

모든 설정이 끝나 DRAGON 소프트웨어를 기동하기 전, 한 가지 확인하여야 할 사항이 있

다. 스위치는 접근할 수 있는 ip 가 설정되어 있어야 하고, 또한 DRAGON 소프트웨어에 참여하는 모든 시스템들이 스위치에 access 할 수 있어야 한다.(방화벽이 있을 경우, access list 에 추가). 이외에도, snmp를 위한 서버 설정과 vlan 에 대한 준비가 필요하다.

3.3.1 SNMP server 설정

VLSR들은 SNMP를 통해 정보를 얻어가므로, 각 스위치 별로 snmp 설정을 해 주어야 한다. 본 절에서는 그 예로 Cisco 7609과 Force10 c300스위치의 snmp server 설정을 보여 준다.

1) Cisco 7609

```
DJ-C7609S_Antlab>en
Password:
DJ-C7609S_Antlab#
DJ-C7609S_Antlab#
DJ-C7609S_Antlab#
DJ-C7609S_Antlab#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
DJ-C7609S_Antlab(config)#snmp-server community dragon rw
DJ-C7609S_Antlab(config)#
```

2) Force10 c300

```
C300#config
C300(config)# snmp-server community dragon rw
C300(config)#
```

3.3.2 VLAN 설정

VLSR이 제어하는 실제 이더넷 스위치들은 자동 VLAN 설정을 위해, 다음의 몇 가지 사항을 확인하여야 한다. cisco 7609의 경우 사용할 VLAN id를 먼저 VLAN 데이터베이스에 등록해 두어야 한다. 그렇지 않을 경우, NARB 없이 단독으로 수행하는 DRAGON 소프트웨어의 경우 현재 데이터 베이스에 존재하는 VLAN ID 중 아무도 사용하지 않는 ID를 사용하거나, 새로운 VLAN ID를 만들어 사용한다. cisco 7609는 다음 네 개의 VLAN ID를 디폴트로 생성하여 특정 프로토콜을 위해 사용하는데, 이 VLAN ID에는 어떤 포트도 아직 할당되어 있지 않기 때문에, 사용하고자 하는 VLAN을 만들어 놓지 않으면, 이들 중 하나를 사용할 수도 있다. 그럴 경우, CSA1 과 CSA2는 통신이 되지 않는다.

```
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

VLAN 100을 사용하고자 할 때, cisco 7609에서 VLAN ID를 등록하는 방법은 다음과 같다.

1) VLAN 100이 있는지 확인한다.

```
DJ-C7609S_Antlab>show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi8/0/6
20   VLAN0020                         active    Gi8/0/7, Gi8/0/8, Gi8/0/9
30   VLAN0030                         active    Gi8/0/12, Gi8/0/13, Gi8/0/14
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----  ---------- ----- ------ ------ -------- ---- -------- ------
------
1    enet  100001     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
---


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

2) enable 모드로 들어가서, vlan 데이터 베이스 설정 편집 모드에 들어간다.

```
DJ-C7609S_Antlab>en
Password:
DJ-C7609S_Antlab#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.
```

3) vlan 100을 추가한다.

```
DJ-C7609S_Antlab(vlan)#vlan 100
VLAN 100 added:
```

Name: VLAN0100

4) vlan 데이터 베이스 설정 편집 모드에서 빠져 나온 다음, vlan 100 이 추가되었는지 확인한다.

```
DJ-C7609S_Antlab(vlan)#exit
APPLY completed.
Exiting....
DJ-C7609S_Antlab#show vlan

VLAN Name                            Status    Ports
---- ------------------------------  --------  ---------------------------------
1    default                         active    Gi8/0/6
20   VLAN0020                        active    Gi8/0/7, Gi8/0/8, Gi8/0/9
30   VLAN0030                        active    Gi8/0/12, Gi8/0/13, Gi8/0/14
100  VLAN0100                        active
1002 fddi-default                    act/unsup
1003 token-ring-default              act/unsup
1004 fddinet-default                 act/unsup
1005 trnet-default                   act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary    Secondary Type              Ports
-------    --------- ----------- ---------------------------------------
```

Force10의 경우 특별한 조치를 취하지 않아도 DRAGON 소프트웨어를 사용하는 데에 문제가 없다.

3.4 DRAGON 소프트웨어 기동과 종료

GRE 설정과 configuration 파일의 설정이 끝나면, 스크립트 파일로 DRAGON 소프트웨어를 기동시킬 수 있다. /usr/local/dragon/bin 에는 이를 위한 쉘 스크립트 파일인 dragon.sh 가 있다. 각 시스템의 기능에 맞도록 DRAGON 소프트웨어를 기동하면 된다.

Peer-to-Peer 모드로 동작하는 CSA는 라우팅에 참여하므로 하나의 VLSR 과 같이 기동한다. 따라서, CSA1과, CSA2, VLSR1은 모두 동일한 아래의 명령으로 기동할 수 있다.

```
[root@kistisvr2 bin]#./dragon.sh start-vlsr
```

명령을 실행하고 나면, 제대로 기동하였는지 확인하여야 한다. 리눅스 명령어를 사용하면, 다음과 같이 모두 4개의 프로세스가 떠 있음을 확인할 수 있다.

```
[root@kisti-1 bin]# ps -ef | grep dragon
root       5440 32160  0 14:31 pts/0    00:00:00 grep dragon
root       22320       1   0 Apr15 ?          00:00:00 /usr/local/dragon/sbin/zebra -d -f
/usr/local/dragon/etc/zebra.conf
root       22322       1   0 Apr15 ?          00:00:23 /usr/local/dragon/sbin/ospfd -d -f
/usr/local/dragon/etc/ospfd.conf
root       22324       1   0 Apr15 ?          00:00:00 /usr/local/dragon/bin/RSVPD -c
/usr/local/dragon/etc/RSVPD.conf -d -o /var/log/RSVPD.log -L select,ref,packet
root       22328       1   0 Apr15 ?          00:00:00 /usr/local/dragon/bin/dragon -d -f
/usr/local/dragon/etc/dragon.conf
```

이들 DRAGON 소프트웨어의 모든 프로세스를 종료하려면, 역시 dragon.sh를 사용하면 된다.

```
[root@kistisvr2 bin]#./dragon.sh stop
```

3.5 LSP의 설정

모든 설정이 끝나고, DRAGON 소프트웨어의 기동이 끝나면, LSP를 설정한다. LSP의 설정은 dragon vty 에 접속하여 수행한다. LSP 설정을 시작하기 전, CSA1에서 CSA2까지 데이터 평면에서 스위치 연결이 없음을 확인하기 위하여, ping 을 수행해 본다. 물론 ping 은 데이터 평면 IP로 서로에게 수행한다. LSP 설정 전 이 두 시스템은 데이터 평면의 연결이 없으므로, ping은 실패할 것이다.

```
[root@kistisvr1 bin]# ping 192.2.0.10          // CSA1
[root@kistisvr2 bin]# ping 192.2.0.2           //CSA2
```

다음으로 CSA1의 dragon 데몬 vty에 접속한다.

```
[root@kistisvr1 ~]# telnet 192.168.0.2 2611
Trying 192.168.0.2...
```

```
Connected to 192.168.0.2.
Escape character is '^]'.


 ____
|  _ ₩ _ __ __ _  __ _  ___  _ __
| | | | '__/ _` |/ _` |/ _ ₩| '_ ₩
| |_| | | | (_| | (_| | (_) | | | |
|____/|_|  ₩__,_|₩__, |₩___/|_| |_|
                 |___/
(D)ynamic (R)esource (A)llocation via
(G)MPLS (O)ptical (N)etworks
Based on Zebra (version 0.94).
Copyright 1996-2002 Kunihiro Ishiguro.
Copyright 2003-2004 the Dragon Team.


User Access Verification

Password:
csa1-dragon>
```

성공적으로 vty 에 접속되면, LSP csa를 만든다. 여기서 csa는 LSP를 구분하는 하나의 아이디로 사용자가 임의로 명명할 수 있으나, 현재 존재하지 않는 것이어야 한다.

```
csa1-dragon> edit lsp csa
csa1-dragon> set source ip-address 192.168.0.2 lsp-id 1000 destination ip-address 192.168.0.3 tunnel-id 2000
csa1-dragon> set bandwidth gige swcap l2sc encoding ethernet gpid ethernet
csa1-dragon> set vtag 100
csa1-dragon> exit
csa1-dragon> commit lsp csa
```

LSP가 제대로 생성되었는지 확인하기 위해서는 현재의 프롬프트 상에서 show lsp를 수행해 본다. show lsp는 현재 존재하는 lsp의 내용을 요약해서 보여준다. 제대로 수행이 되었다면, LSP csa 는 in-service 상태여야 한다.

```
csa1-dragon> show lsp
                        **LSP status summary**

Name         Status      Dir    Source (IP/LSP ID)  Destination (IP/Tunnel ID)
-------------------------------------------------------------------------
csa          in-service  <=>    192.168.0.2         192.168.0.3
                                1000                2000
csa1-dragon>
```

LSP 설정이 성공하면, 각 CSA에서 다시 한번 ping을 수행해 본다.

```
[root@kistisvr1 bin]# ping 192.2.0.10
PING 192.2.0.10 (192.2.0.10) 56(84) bytes of data.
64 bytes from 192.2.0.10: icmp_seq=1 ttl=64 time=0.109 ms
64 bytes from 192.2.0.10: icmp_seq=2 ttl=64 time=0.125 ms
64 bytes from 192.2.0.10: icmp_seq=3 ttl=64 time=0.125 ms
64 bytes from 192.2.0.10: icmp_seq=4 ttl=64 time=0.083 ms

[root@kistisvr2 bin]# ping 192.2.0.2
PING 192.2.0.2 (192.2.0.2) 56(84) bytes of data.
From 192.2.0.10 icmp_seq=1 Destination Host Unreachable
From 192.2.0.10 icmp_seq=2 Destination Host Unreachable
From 192.2.0.10 icmp_seq=3 Destination Host Unreachable
64 bytes from 192.2.0.2: icmp_seq=4 ttl=64 time=1.26 ms
64 bytes from 192.2.0.2: icmp_seq=5 ttl=64 time=0.121 ms
64 bytes from 192.2.0.2: icmp_seq=6 ttl=64 time=0.122 ms
64 bytes from 192.2.0.2: icmp_seq=7 ttl=64 time=0.132 ms
```

4. Intra-domain NARB 설정 및 시험

3장에서는 기본적인 VLSR 의 기능을 시험할 수 있는 간단한 예제를 살펴보았다. 본 장에서는 KISTI 가 확장 개발한 cisco7609와 Force10 C300을 지원하는 모듈을 이용하여, cisco7609와 Force10 C300 간의 이 기종 이더넷 스위치 장비에 대해, 하나의 NARB를 가진 도메인 내에서의 LSP 설정을 시험한다. Figure 4는 이를 위한 네트워크 토폴로지를 보여준다. 기본 설정에서와 같이 C3750 스위치는 스위칭 허브로 사용되었고, CSA1은 cisco7609의 Gi8/0/1 포트에 CSA2는 Force10 c300 장비의 Gi1/3 포트에 연결되어 있다. 이 두 이더넷 스위치는 다시 Gi8/0/11 과 Gi0/1 포트로 서로 연결되어 있다. 전체 시스템들은 NARB1과 모두 연결되어 있다. 그러나, VLSR1만이 GRE 터널을 통해 OSPF-TE 통신을 수행한다. 하나의 NARB로 관리하고 있는 네트워크 내의 모든 VLSR이 NARB 와 OSPF-TE를 수행할 필요는 없다. 그 네트워크의 모든 라우팅 정보는 각각의 VLSR 내에 모두 존재하므로 NARB에 이러한 정보를 전달하기 위해 우리는 하나의 VLSR을 선택하여 GRE 터널을 NARB와 연결해 준다. 이 VLSR을 border VLSR이라 한다. 또한, 3장에서와 달리 두 대의 종단 시스템은 CSA가 아니라 Proxy로 동작한다. 카메라나 다른 dummy 연결 시스템 대신 실제 데이터 평면의 종단 시스템을 Proxy 장비의 나머지 네트워크 인터페이스를 활용하여 시험하였다.

4.1 GRE 설정

한층 복잡해진 네트워크 토폴로지는 제어 평면을 위해 여러 개의 GRE 터널을 요구한다. GRE1은 CSA1과 VLSR1의 제어평면 통신을 위해, GRE2는 VLSR1과 VLSR2, GRE3는 VLSR2와 CSA2, GRE5는 border VLSR인 VLSR1과 NARB1의 제어평면 통신을 위해 필

요하다. 각각의 장비에서는 이들 GRE를 설정해 주어야 한다. GRE 설정을 잘못하면, DRAGON 소프트웨어가 정상적으로 기동하였다 할지라도 동작하지 않기 때문에 매 설정마다 local ip 와 remote ip를 확인하여 ping 을 통해 반드시 제대로 되었는지에 대한 검증을 수행하여야 한다.

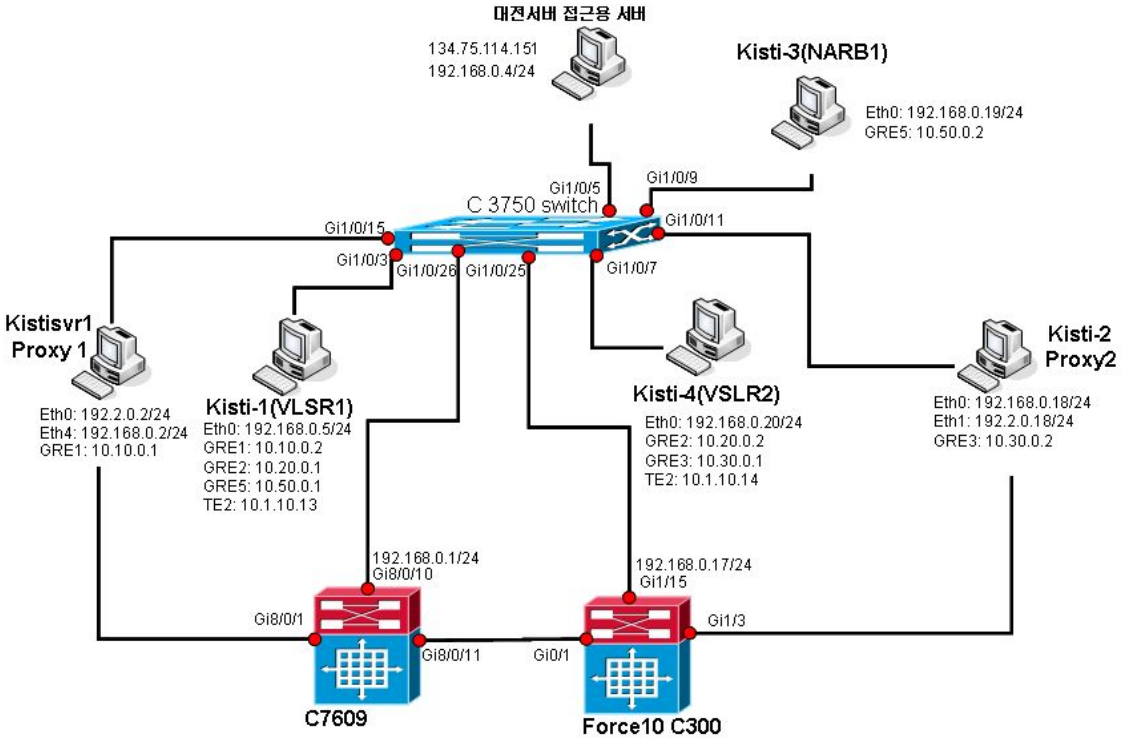

Figure 4. Intra-domain Test Network Topology

4.1.1 GRE1 설정

1) CSA1 (kistisvr1)

```
[root@kistisvr1 sbin]# /sbin/modprobe ip_gre
[root@kistisvr1 sbin]# /sbin/ip link set gre1 down
[root@kistisvr1 sbin]# /sbin/ip tunnel del gre1
[root@kistisvr1 sbin]# /sbin/ip tunnel add gre1 mode gre remote 192.168.0.5 local 192.168.0.2 ttl 255
[root@kistisvr1 sbin]# /sbin/ip link set gre1 up
[root@kistisvr1 sbin]# /sbin/ip addr add 10.10.0.1/30 dev gre1
[root@kistisvr1 sbin]# /sbin/ip route add 10.10.0.2 dev gre1
```

2) VLSR1 (kisti-1)

```
[root@kisti-1 sbin]# /sbin/modprobe ip_gre
[root@kisti-1 sbin]# /sbin/ip link set gre1 down
[root@kisti-1 sbin]# /sbin/ip tunnel del gre1
[root@kisti-1 sbin]# /sbin/ip tunnel add gre1 mode gre remote 192.168.0.2 local 192.168.0.5 ttl 255
```

```
[root@kisti-1 sbin]# /sbin/ip link set gre1 up
[root@kisti-1 sbin]# /sbin/ip addr add 10.10.0.2/30 dev gre1
[root@kisti-1 sbin]# /sbin/ip route add 10.10.0.1 dev gre1
```

4.1.2 GRE2 설정

1) VLSR1 (kisti-1)

```
[root@kisti-1 sbin]# /sbin/modprobe ip_gre
[root@kisti-1 sbin]# /sbin/ip link set gre2 down
[root@kisti-1 sbin]# /sbin/ip tunnel del gre2
[root@kisti-1 sbin]# /sbin/ip tunnel add gre2 mode gre remote 192.168.1.20 local
192.168.0.5 ttl 255
[root@kisti-1 sbin]# /sbin/ip link set gre2 up
[root@kisti-1 sbin]# /sbin/ip addr add 10.20.0.1/30 dev gre2
[root@kisti-1 sbin]# /sbin/ip route add 10.20.0.2 dev gre2
```

2) VLSR2 (kisti-4)

```
[root@kisti-4 sbin]# /sbin/modprobe ip_gre
[root@kisti-4 sbin]# /sbin/ip link set gre2 down
[root@kisti-4 sbin]# /sbin/ip tunnel del gre2
[root@kisti-4 sbin]# /sbin/ip tunnel add gre2 mode gre remote 192.168.0.5 local
192.168.1.20 ttl 255
[root@kisti-4 sbin]# /sbin/ip link set gre2 up
[root@kisti-4 sbin]# /sbin/ip addr add 10.20.0.2/30 dev gre2
[root@kisti-4 sbin]# /sbin/ip route add 10.20.0.1 dev gre2
```

4.1.3 GRE3 설정

1) VLSR2(kisti-4)

```
[root@kisti-4 sbin]# /sbin/ip link set gre3 down
[root@kisti-4 sbin]# /sbin/ip tunnel del gre3
[root@kisti-4 sbin]# /sbin/ip tunnel add gre3 mode gre remote 192.168.0.18 local
192.168.0.20 ttl 255
[root@kisti-4 sbin]# /sbin/ip link set gre3 up
[root@kisti-4 sbin]# /sbin/ip addr add 10.30.0.1/30 dev gre3
[root@kisti-4 sbin]# /sbin/ip route add 10.30.0.2 dev gre3
```

2) CSA2 (kisti-2)

```
[root@kisti-2 sbin]# /sbin/modprobe ip_gre
[root@kisti-2 sbin]# /sbin/ip link set gre3 down
[root@kisti-2 sbin]# /sbin/ip tunnel del gre3
[root@kisti-2 sbin]# /sbin/ip tunnel add gre3 mode gre remote 192.168.0.20 local
192.168.0.18 ttl 255
[root@kisti-2 sbin]# /sbin/ip link set gre3 up
[root@kisti-2 sbin]# /sbin/ip addr add 10.30.0.2/30 dev gre3
[root@kisti-2 sbin]# /sbin/ip route add 10.30.0.1 dev gre3
```

4.1.4 GRE5 설정

1) VLSR1 (kisti-1)

```
[root@kisti-2 sbin]# /sbin/modprobe ip_gre
[root@kisti-2 sbin]# /sbin/ip link set gre5 down
[root@kisti-2 sbin]# /sbin/ip tunnel del gre5
[root@kisti-2 sbin]# /sbin/ip tunnel add gre5 mode gre remote 192.168.0.19 local 192.168.0.5 ttl 255
[root@kisti-2 sbin]# /sbin/ip link set gre5 up
[root@kisti-2 sbin]# /sbin/ip addr add 10.50.0.1/30 dev gre5
[root@kisti-2 sbin]# /sbin/ip route add 10.50.0.2 dev gre5
```

2) NARB1 (kisti-3)

```
[root@kisti-3 sbin]# /sbin/modprobe ip_gre
[root@kisti-3 sbin]# /sbin/ip tunnel del gre5
[root@kisti-3 sbin]# /sbin/ip tunnel add gre5 mode gre remote 192.168.0.5 local 192.168.0.19 ttl 255
[root@kisti-3 sbin]# /sbin/ip link set gre5 up
[root@kisti-3 sbin]# /sbin/ip addr add 10.50.0.2/30 dev gre5
[root@kisti-3 sbin]# /sbin/ip route add 10.50.0.1 dev gre5
```

4.2 소프트웨어 설정 파일

NARB 를 포함하는 네트워크 토폴로지는 설정파일에도 몇 가지 다른 설정이 필요하다. 3장에서 설명한 부분과 중복되는 부분도 있겠지만, 전체 파일 설정을 보여 주기 위해 본 장에서는 전체 장비에서의 설정 파일 하나하나를 모두 보여줄 것이다.

4.2.1 Proxy1 설정 파일

1) dragon.conf

3장에서의 설정과 다르지 않다. 다만, UNI CSA 모델[1]로 Proxy로 동작하는 시스템은 LSP 설정을 요청할 때, 자신이 연결된 port 가 아니라 실제 데이터를 받을 시스템이 연결되어 있는 port를 알고 있어야 한다. 이를 위한 local-id 설정을 추가하였다. 여기서의 port 도 역시 정수로만 설정 가능하며, 3장의 cisco 7609 시스템의 포트변환 규칙을 따른다. 만일 Proxy가 다른 이더넷 스위치에 연결되어 있다면, 그 스위치에 맞는 포트변환 규칙에 따라 포트 아이디를 포트 번호로 변환해서 설정하여야 한다.

```
! -*- dragon -*-
!
! DRAGON sample configuration file
!
hostname proxy1-dragon
password dragon
set local-id port 2049
```

2) ospfd.conf
UNI CSA[3] 모드로 작동하는 Proxy1은 라우팅에 참여하지 않는다. 따라서, ospfd 데몬 프로세스는 기동하지 않으며, ospfd.conf 의 설정도 필요하지 않다.

3) RSVPD.conf
Proxy1의 RSVPD 데몬 프로세스는 데이터 평면에 연결된 실제 종단 시스템을 위해 대신 시그널링을 시작한다. 따라서, 설정 파일은 Proxy를 위한 RSVPD의 역할을 명시하여야 한다. p/2049는 dragon.conf에서 지정한 2049 포트에 실제 데이터가 연결되어 있고 이 시스템을 대신해 시그널링을 하라는 의미이다.

```
interface gre1 tc none mpls p/2049
api 4000
```

4) zebra.conf
3장의 zebra.conf와 같다.

```
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.14 1999/02/19 17:26:38 developer Exp $
!
hostname csa1-zebra
password zebra
enable password zebra
!
! Interface's description.
!
interface lo
interface gre1
!
line vty
log file /var/log/zebra.log
```

4.2.2 CSA2 설정 파일

1) dragon.conf
Proxy1과 마찬가지로 실제 데이터 평면의 종단 시스템을 위한 설정이 필요하다. Proxy2의 종단 시스템은 Force10 c300에 연결되어 있으므로, Force10 c300의 포트변환 규칙을 따라 Gi1/3을 변환한다. Force10 c300의 변환 규칙은 다음과 같다.

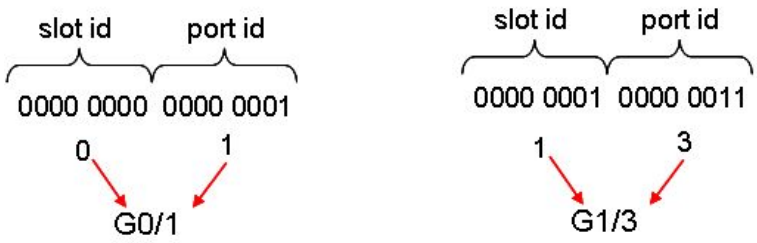

Figure 5. Force10 C300/E300/E600 Port Conversion

따라서, Gi1/3은 259로 변환하여 설정한다.

```
! -*- dragon -*-
!
! DRAGON sample configuration file
!
hostname kisti2-dragon
password dragon
set local-id port 259
```

2) ospfd.conf

UNI CSA[3] 모드로 작동하는 Proxy1은 라우팅에 참여하지 않는다. 따라서, ospfd 데몬 프로세스는 기동하지 않으며, ospfd.conf 의 설정도 필요하지 않다.

3) RSVPD.conf

Proxy1과 마찬가지로 실제 데이터 평면의 종단 시스템을 위한 설정이 필요하다.

```
interface gre3 tc none mpls p/259
api 4000
```

4) zebra.conf

```
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.14 1999/02/19 17:26:38 developer Exp $
!
hostname kisti2-zebra
password zebra
enable password zebra
!
! Interface's description.
!
interface lo
interface gre3
```

```
!
line vty
log file /var/log/zebra.log
```

4.2.3 VLSR1 설정 파일

1) dragon.conf

local-id를 통해 종단 데이터 평면 장비가 연결된 포트들을 명시한다. 또한, NARB 와의 통신을 위한 IP와 port 정보를 추가한다.

```
! -*- dragon -*-
!
! DRAGON sample configuration file
!
hostname vlsr-dragon
password dragon
set local-id port 2049
configure narb intra-domain ip-address 192.168.0.19 port 2609
```

2) ospfd.conf

VLSR1은 CSA1, VLSR2, NARB1 모두 세 개의 GRE 인터페이스를 가진다. proxy1과의 interface 인 gre1은 OSPF-TE 라우팅에 참여하지 않는 인터페이스이다. 따라서, 이를 passive-interface 로 지정한다. 또한, NARB와의 인터페이스인 gre5는 라우팅 정보는 주고 받지만, LSP 설정을 하거나 데이터 인터페이스가 필요한 것은 아니다. 따라서, gre2에 대해서만, ospf-te 인터페이스로 지정하고 이를 대한 정보를 명시한다. gre2는 VLSR1과 VLSR2를 위한 제어채널이고, 이를 통해 VLSR1이 관리하는 cisco7609 스위치와 Force10 c300 스위치와의 정보를 주고 받는다. 따라서, 이 후 LSP를 설정할 때, VLSR1이 관리하는 cisco 7609 스위치내의 어떤 포트가 Force10 c300 스위치와 연결되는 지에 대한 포트 정보와 이를 연결하는 LSP를 위한 데이터 인터페이스 정보를 정의한다.
vlan 100, vlan 200은 이 인터페이스를 위해 사용할 수 있는 vlan 을 명시한 것이다.

```
! -*- ospf -*-
!
! OSPFd sample configuration file
!
hostname vlsr1-ospf
password dragon
enable password dragon
log stdout
log file /var/log/ospfd.log
!
! NOTE: max. bandwidth parameters are in bytes/sec, for example:
!    1 Gbps = 125000000 bytes/sec
```

```
!  10 Gbps = 1250000000 bytes/sec
!
! -*- sample ospf configuration for a dragon VLSR controlling a Layer2 Ethernet switch -*-
!
interface gre1
 description GRE tunnel between vlsr1(kisti-1) and csa1(kistisvr1)
 ip ospf network point-to-point
!
interface gre2
 description GRE tunnel between vlsr1(kisti-1) and vlsr2(kisti-4)
 ip ospf network point-to-point
!
interface gre5
 description GRE tunnel between narb-server(kisti-3) and vlsr1(kisti-1)
 ip ospf network point-to-point
!
router ospf
 ospf router-id 192.168.0.5
 network 10.10.0.0/30 area 0.0.0.0
 network 10.20.0.0/30 area 0.0.0.0
 network 10.50.0.0/30 area 0.0.0.0
 ospf-te router-address 192.168.0.5
 passive-interface gre1
 ospf-te interface gre2
        level gmpls
        swcap l2sc encoding ethernet
        data-interface ip 10.1.10.13 protocol snmp switch-ip 192.168.0.1 switch-port 2059
        max-bw 125000000
        max-rsv-bw 125000000
        max-lsp-bw 0 125000000
        max-lsp-bw 1 125000000
        max-lsp-bw 2 125000000
        max-lsp-bw 3 125000000
        max-lsp-bw 4 125000000
        max-lsp-bw 5 125000000
        max-lsp-bw 6 125000000
        max-lsp-bw 7 125000000
        vlan 100
        vlan 200
        metric 10
 exit
!
line vty
!
```

3) RSVPD.conf

RSVPD.conf 에는 시그널링을 위한 모든 gre 인터페이스를 기술한다. gre1 에 대해서는 이 인터페이스가 local-id를 사용하는 UNI CSA[3]의 proxy와 연결되어 있고, 그 proxy가 대신하는 시그널링이 2049 포트에 관한 것이라는 것을 명시한다. 또한 NARB에 ERO를 요구하기 위한 NARB의 IP 와 port 정보도 포함한다.

```
interface gre1 tc none mpls p/2049
interface gre2 tc none mpls
interface gre5 tc none mpls
api 4000
narb 192.168.0.19 2609
```

4) zebra.conf

존재하는 모든 GRE 인터페이스를 정의한다.

```
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.14 1999/02/19 17:26:38 developer Exp $
!
hostname vlsr1-zebra
password zebra
enable password zebra
!
! Interface's description.
!
interface lo
interface gre1
interface gre2
interface gre5
!
line vty
log file /var/log/zebra.log
```

4.2.4 VLSR2 설정 파일

1) dragon.conf

VLSR2는 border VLSR 이 아니므로 VLSR1과 같은 NARB 정보가 필요없다. 그러나, VLSR1과 마찬가지로 proxy로 동작하고 있는 proxy2와의 연결 시에 필요한 local-id 정보는 설정해 주어야 한다. 이 정보는 proxy2의 dragon 설정과 맞아야 한다.

```
! -*- dragon -*-
!
! DRAGON sample configuration file
```

```
!
hostname kisti4-vlsr
password dragon
set local-id port 259
```

2) ospfd.conf

VLSR2 가 제어하는 장비는 Force10 c300 스위치이다. 따라서, VLSR1과 마찬가지로 VLSR1와 VLSR2가 연결된 포트와 데이터 인터페이스를 명시해야 한다. Force10 c300의 다음과 같은 메커니즘으로 정수로 변환할 수 있다. 이에 따라, Gi0/1을 1로 변환하였다. 또한 proxy2와의 인터페이스인 gre3는 라우팅 정보 교환에 사용하지 않으므로 passive-interface로 정의하였다.

```
! -*- ospf -*-
!
! OSPFd sample configuration file
!
hostname vlsr-ospf
password dragon
enable password dragon
log stdout
log file /var/log/ospfd.log
!
! NOTE: max. bandwidth parameters are in bytes/sec, for example:
!    1 Gbps = 125000000 bytes/sec
!   10 Gbps = 1250000000 bytes/sec
!
! -*- sample ospf configuration for a dragon VLSR controlling a Layer2 Ethernet switch -*-
!
interface gre2
 description GRE tunnel between vlsr1(kist-1) and vlsr2(kisti-4)
 ip ospf network point-to-point
!
interface gre3
 description GRE tunnel between csa2(kist-2) and vlsr2(kisti-4)
 ip ospf network point-to-point
!
router ospf
 ospf router-id 192.168.0.20
 network 10.20.0.0/30 area 0.0.0.0
 network 10.30.0.0/30 area 0.0.0.0
 ospf-te router-address 192.168.0.20
 passive-interface gre3
 ospf-te interface gre2
        level gmpls
        data-interface ip 10.1.10.14 protocol snmp switch-ip 192.168.0.17 switch-port 1
```

```
        swcap l2sc encoding ethernet
        max-bw 125000000
        max-rsv-bw 125000000
        max-lsp-bw 0 125000000
        max-lsp-bw 1 125000000
        max-lsp-bw 2 125000000
        max-lsp-bw 3 125000000
        max-lsp-bw 4 125000000
        max-lsp-bw 5 125000000
        max-lsp-bw 6 125000000
        max-lsp-bw 7 125000000
        vlan 100
        vlan 200
        metric 10
      exit
!
line vty
!
```

2) RSVPD.conf

VLSR2는 border VLSR 이 아니므로 dragon.conf 와 마찬가지로 NARB의 IP와 port 에 대한 정보를 요하지 않는다.

```
nterface gre2 tc none mpls
interface gre3 tc none mpls p/259
interface gre6 tc none mpls
api 4000
```

3) zebra.conf

```
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.14 1999/02/19 17:26:38 developer Exp $
!
hostname kisti4-vlsr2
password zebra
enable password zebra
!
! Interface's description.
!
interface lo
interface gre2
interface gre3
!
```

```
line vty
log file /var/log/zebra.log
```

4.2.5 NARB1 설정 파일

NARB를 기동하기 위해서는 narb.conf, ospfd-intra.con, ospfd-inter.conf, zebra.conf, rce.conf가 필요하다. 또한 rce 데몬 프로세스의 정상적인 동작을 위해 schema_combo.rsd.sample 을 schema_combo.rsd로 복사해 둔다.

1) narb.conf

narb.conf 는 narb 데몬 프로세스가 기동 시 참조하는 파일이다.

domain-id 는 그 도메인을 표현한다. Figure 4와 같이 현재 NARB1이 관리하고 있는 도메인은 192.168.0.0 도메인이다. domain-id를 표현하는 다른 방법은 참조문헌 [3]을 참조한다. 현재 NARB1은 하나의 도메인만 관장할 뿐 다른 어떤 NARB와의 연결도 가지지 않는다. 따라서, intra-domain-ospfd 에 관한 정보만 명시한다. originate-interface 는 VLSR1의 ospfd 데몬과 네트워크 토폴로지 정보를 교환하기 위해 사용하고 있는 GRE 인터페이스의 IP 주소를 의미한다. area 는 도메인 내부이므로 0.0.0.0 으로 설정한다.

router 는 네트워크 토폴로지를 추상적으로 기술한다. 도메인 내부에서만 NARB의 동작이 이루어질 경우 내부 도메인 토폴로지 정보는 내부의 ospfd 정보 교환만으로 충분하기 때문에, 굳이 기술할 필요는 없다. 그러나 본 문서에서는 네트워크 토폴로지 정보의 기술방법을 예시하기 위해 기술한다. 마지막으로 cli 는 CLI를 통해 narb vty 에 접속할 때 필요한 정보를 설정한다.

```
!
domain-id {ip 192.168.0.0}
!
intra-domain-ospfd {address localhost port 2617
        originate-interface 10.50.0.2 area 0.0.0.0}
!
router {id 192.168.0.5
        inter-domain link to vlsr2
        link {id 192.168.0.20 type 1
                max_bw 1250.0 max_rsv_bw 1250.0
                unrsv_bw0 1250.0 unrsv_bw1 1250.0 unrsv_bw2 1250.0 unrsv_bw3 1250.0
unrsv_bw4 1250.0 unrsv_bw5 1250.0 unrsv_bw6 1250.0 unrsv_bw7 1250.0
                enc_type 2 sw_type 51
                metric 10
                local_if 10.1.10.13  remote_if 10.1.10.14
                vlan_tags(100:100)
        }
}
!
inter-domain-te-link {id 10.2.10.14 narb-peer 10.80.0.2 port 2609}
!
```

```
cli {host kisti3-narb password dragon}
!
```

2) ospfd-intra.conf

ospfd-intra.conf는 도메인 내부의 네트워크 토폴로지 정보를 교환하기 위해 VLSR1의 ospfd 데몬 프로세스와 통신하는 NARB의 ospfd 데몬 프로세스가 기동 시 참조하는 파일이다. 인터페이스 정보와 라우팅에 필요한 기본 정보만 포함하고 있다.

```
! Intra-domain ospfd configuration for narb
!   2005/03/11 16:32:10
!
hostname kisti3-ospf-intra
password dragon
log stdout
!
!
!
interface gre5
  description GRE tunnel between kisti3-narb and kisti1-vlsr
  ip ospf network point-to-point
!
router ospf
  ospf router-id 192.168.0.19
  network 10.50.0.0/30 area 0.0.0.0
   ospf-te router-address 192.168.0.19
!
line vty
```

3) ospfd-inter.conf

다른 NARB와의 도메인 간 연결이 없으므로 필요한 파일은 아니다. 그러나 NARB 시스템 기동 시 inter-domain 을 위한 ospfd 데몬 프로세스가 실행되므로, 기본적인 호스트 이름과 패스워드만 포함한 파일로 존재해야 한다.

```
!
hostname kisti3-ospf-inter
password dragon
log stdout
!
```

4) zebra.conf

ospfd 데몬 프로세스에게 인터페이스 정보를 주고, 라우팅 정보를 업데이트 하기 위해 기동하는 zebra 데몬 프로세스가 기동 시 참조하는 파일이다. 다른 VLSR 이나 proxy 에서처럼 인터페이스를 기술해 주면 된다.

```
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.14 1999/02/19 17:26:38 developer Exp $
!
hostname kisti3-zebra
password zebra
enable password zebra
!
! Interface's description.
!
interface lo
interface gre5
!
line vty
log file /var/log/zebra.log
```

5) rce.conf
Resource Computation Engine 인 rce 데몬 프로세스가 기동 시 참조하는 파일이다.
도메인 아이디와 트래픽 엔지니어링 테이블을 위한 스키마 파일에 대한 설정이 필요하다.

```
!
domain-id {ip 192.168.0.0}
!
include-tedb-schema {path /usr/local/dragon/etc/schema_combo.rsd}
!
```

4.3 스위치 준비

3장에서와 같이 사용하고자 하는 VLAN id를 cisco7609의 데이터베이스에 등록해 둔다. Force10 c300의 경우, 이러한 데이터베이스 등록을 따로 하지 않더라도, LSP 설정에 문제가 없다.

4.4 DRAGON 소프트웨어 기동과 종료

UNI CSA[3] 모드로 동작하는 proxy는 라우팅에 참여하지 않으므로, UNI 를 통한 RSVP 시그널링과 설정을 위한 vty만 필요하다. 따라서, Proxy1과, Proxy2는 아래의 명령으로 기동할 수 있다.

```
[root@kistisvr1 bin]#./dragon.sh start-uni
```

명령을 실행하고 나면, 제대로 기동하였는지 확인하여야 한다. 리눅스 명령어를 사용하면,

다음과 같이 모두 3개의 프로세스가 떠 있음을 확인할 수 있다.

```
[root@kistisvr1 bin]# ps -ef | grep dragon
root          6441        1    0  15:28  ?              00:00:00  /usr/local/dragon/bin/RSVPD  -c
/usr/local/dragon/etc/RSVPD.conf -d -o /var/log/RSVPD.log -L select,ref,packet
root          6444        1    0  15:28  ?              00:00:00  /usr/local/dragon/bin/dragon  -d  -f
/usr/local/dragon/etc/dragon.conf
root          6446        1    0  15:28  ?              00:00:00  /usr/local/dragon/bin/node_agent  -d  -c
/usr/local/dragon/etc/node_agent.conf
root       6448  5778  0 15:29 pts/4     00:00:00 grep dragon
[root@kistisvr1 bin]#
```

3장과 다른 점은 ospfd 대신 node_agent 데몬 프로세스가 기동하였다는 점이다.

VLSR1과 VLSR2는 3장에서와 같이 dragon.sh 의 start-vlsr 옵션으로 기동하면 된다.
NARB1은 다음의 명령으로 실행가능하다.

```
[root@kisti-3 bin]# ./dragon.sh start-narb
```

프로세스들의 정상적인 기동을 알아보기 위해 ps 명령어를 실행하면 된다.

```
[root@kisti-3 bin]# ps -ef | grep dragon
root        13185        1    0  15:43  ?              00:00:00  /usr/local/dragon/sbin/zebra  -d  -f
/usr/local/dragon/etc/zebra.conf
root       13187       1   0 15:43 ?         00:00:00 /usr/local/dragon/sbin/ospfd -d -I -P 2614
-f /usr/local/dragon/etc/ospfd-inter.conf
root       13189       1   0 15:43 ?         00:00:00 /usr/local/dragon/sbin/ospfd -d -P 2604 -f
/usr/local/dragon/etc/ospfd-intra.conf
root        13203        1    0  15:43  ?              00:00:00  /usr/local/dragon/sbin/rce  -d  -f
/usr/local/dragon/etc/rce.conf
root        13207        1    0  15:43  ?              00:00:00  /usr/local/dragon/sbin/narb  -d  -f
/usr/local/dragon/etc/narb.conf
root       13209 12398   0 15:43 pts/0     00:00:00 grep dragon
```

NARB는 narb, rce, ospfd 의 라우팅 정보를 갱신하고 인터페이스 정보를 전달하기 위한 zebra 와 두 개의 ospfd(intra-domain, inter-domain) 모두 5개의 데몬 프로세스를 실행하고 있다. 이들의 자세한 기능은 []를 참조한다.

이들 DRAGON 소프트웨어의 모든 프로세스를 종료하려면, 역시 dragon.sh를 사용하면 된다.

4.4 설정 확인

복잡한 네트워크 토폴로지 일수록 설정이 프로세스의 기동과 설정이 제대로 이루어 졌는지

에 대한 검증이 필요하다. 본 절에서는 LSP 설정 전 검증을 위해 확인할 수 있는 여러 가지 사항들을 기술한다.

4.4.1 ospf 확인

ospfd 의 vty 에 직접 접속하여 OSPF-TE 정보가 제대로 등록되어 있는지 확인할 수 있다. 먼저 telnet으로 원하는 VLSR의 ospfd 포트인 2604에 접속한 다음 show ip ospf-te database detail 명령을 통해 현재 구성된 OSPF-TE 데이터베이스를 확인하여 도메인 내부 네트워크 토롤로지가 제대로 구성되었는지 확인할 수 있다. 도메인 내에 존재하는 VLSR1인 192.168.0.5 와 VLSR2인 192.168.0.20 각각의 라우터 정보와 이들 사이의 링크 정보를 확인할 수 있다. 또한 ospfd.conf에서 설정한 사용가능한 vlan id도 확인할 수 있다. 이들 정보 중 자신의 VLSR에 대한 정보는 ospfd.conf에서 얻지만, 다른 VLSR 에 대한 정보와 링크 정보들은 OSPF-TE의 LSA를 통해 얻어진다.

```
[root@kisti-1 ~]# telnet localhost 2604
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Hello, this is zebra (version 0.94).
Copyright 1996-2002 Kunihiro Ishiguro.

User Access Verification

Password:
vlsr1-ospf> show ip ospf-te database detail
OSPF-TE link state database, area 0.0.0.0
Type    ID       Adv Rtr Seq      Age      Cksum    Len
Area-Router ID TLV       1.168.0.5       192.168.0.5     0x8000  0       0xd13b  28
  Router-Address: 192.168.0.5

Area-Router ID TLV       1.168.0.20      192.168.0.20    0x8000  1       0x7768  28
  Router-Address: 192.168.0.20

Area-Link TLV    1.0.0.10        192.168.0.20    0x8000  1       0x160c  184
  Link: 160 octets of data
  Link-Type: Point-to-point (1)
  Link-ID: 192.168.0.5
  Local Interface IP Address(es): 10.1.10.14
  Remote Interface IP Address(es): 10.1.10.13
  Traffic Engineering Metric: 10
  Maximum Bandwidth: 1.25e+08 (Bytes/sec)
  Maximum Reservable Bandwidth: 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 0): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 1): 1.25e+08 (Bytes/sec)
```

```
    Unreserved Bandwidth (pri 2): 1.25e+08 (Bytes/sec)
    Unreserved Bandwidth (pri 3): 1.25e+08 (Bytes/sec)
    Unreserved Bandwidth (pri 4): 1.25e+08 (Bytes/sec)
    Unreserved Bandwidth (pri 5): 1.25e+08 (Bytes/sec)
    Unreserved Bandwidth (pri 6): 1.25e+08 (Bytes/sec)
    Unreserved Bandwidth (pri 7): 1.25e+08 (Bytes/sec)
    Interface Switching Capability Descriptor: l2sc ethernet
    Max LSP Bandwidth 0: 1.25e+08 (Bytes/sec)
    Max LSP Bandwidth 1: 1.25e+08 (Bytes/sec)
    Max LSP Bandwidth 2: 1.25e+08 (Bytes/sec)
    Max LSP Bandwidth 3: 1.25e+08 (Bytes/sec)
    Max LSP Bandwidth 4: 1.25e+08 (Bytes/sec)
    Max LSP Bandwidth 5: 1.25e+08 (Bytes/sec)
    Max LSP Bandwidth 6: 1.25e+08 (Bytes/sec)
    Max LSP Bandwidth 7: 1.25e+08 (Bytes/sec)
    -- L2SC specific information--
      --> Available VLAN tag set: 100 200
      --> Allocated VLAN tag set:
Area-Link TLV    1.0.0.12          192.168.0.5       0x8000   0         0xad71   184
  Link: 160 octets of data
  Link-Type: Point-to-point (1)
  Link-ID: 192.168.0.20
  Local Interface IP Address(es): 10.1.10.13
  Remote Interface IP Address(es): 10.1.10.14
  Traffic Engineering Metric: 10
  Maximum Bandwidth: 1.25e+08 (Bytes/sec)
  Maximum Reservable Bandwidth: 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 0): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 1): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 2): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 3): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 4): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 5): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 6): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 7): 1.25e+08 (Bytes/sec)
  Interface Switching Capability Descriptor: l2sc ethernet
  Max LSP Bandwidth 0: 1.25e+08 (Bytes/sec)
  Max LSP Bandwidth 1: 1.25e+08 (Bytes/sec)
  Max LSP Bandwidth 2: 1.25e+08 (Bytes/sec)
  Max LSP Bandwidth 3: 1.25e+08 (Bytes/sec)
  Max LSP Bandwidth 4: 1.25e+08 (Bytes/sec)
  Max LSP Bandwidth 5: 1.25e+08 (Bytes/sec)
  Max LSP Bandwidth 6: 1.25e+08 (Bytes/sec)
  Max LSP Bandwidth 7: 1.25e+08 (Bytes/sec)
  -- L2SC specific information--
    --> Available VLAN tag set: 100 200
```

```
    --> Allocated VLAN tag set:

vlsr1-ospf>
```

4.4.2 RCE 확인

NARB의 RCE는 TE 데이터베이스와 제약조건을 고려한 최적의 라우팅 경로를 계산하여 돌려준다. 따라서, RCE가 네트워크 토폴로지를 제대로 구성하고 있는지 확인할 필요가 있다. RCE가 데이터베이스를 구성하는 과정은 참조문헌[4]를 참조한다. 본 절에서는 구성된 네트워크 토롤로지를 확인하는 방법을 보여준다. 먼저 NARB 시스템의 IP에 2688 포트로 telnet 접속을 한다. show topology intra domain을 수행하면 rce의 정보를 알 수 있다. 만일 도메인간 연결된 NARB가 있다면, show topology inter domain 을 통해 확인 가능하다.

```
[root@kisti-3 ~]# telnet localhost 2688
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.


 ____
|  _ ₩ _ __ __ _  __ _  ___  _ __
| | | | '__/ _` |/ _` |/ _ ₩| '_ ₩
| |_| | | | (_| | (_| | (_) | | | |
|____/|_|  ₩__,_| ₩__, | ₩___/|_| |_|
                  |___/
(D)ynamic (R)esource (A)llocation via
(G)MPLS (O)ptical (N)etworks
Copyright 2003-2005 the Dragon Team.

password:
rce:cli>

rce:cli>show topology intradomain
                .......Router ID Opaque LSA.......
Adv_router (192.168.0.5), Router_id (192.168.0.5)
Adv_router (192.168.0.20), Router_id (192.168.0.20)
                .......TE Link Opaque LSA.......
Adv_router (192.168.0.5), Link_id (10.20.0.0), IfAddrs[10.1.10.13-0.0.0.0]
Adv_router (192.168.0.5), Link_id (192.168.0.20), IfAddrs[10.1.10.13-10.1.10.14]
Adv_router (192.168.0.20), Link_id (192.168.0.5), IfAddrs[10.1.10.14-10.1.10.13]
                .......The End.......
```

4.4.3 경로 검증 테스트

LSP 설정을 통해 실제 스위치에 접근하여 하나의 LSP를 만들기 전에 narb에 ERO를 요청함으로써 경로 검증이 가능하다. narb와 직접 연결된 시스템에서는 테스트 가능하다. 그러

나, narb_test 라는 프로그램은 narb-sw내에 포함되어 있기 때문에 이를 설치해야 테스트가 가능하다.

```
[root@kisti-1 sbin]# ./narb_test -H 192.168.0.19 -S 192.168.0.5 -D 192.168.0.20
NARB@[2008/04/03 13:44:27] : Request successful! ERO returned...
NARB@[2008/04/03 13:44:27] : HOP-TYPE [strict]: 10.1.10.13
NARB@[2008/04/03 13:44:27] : HOP-TYPE [strict]: 10.1.10.14
```

4.5 LSP의 설정

모든 설정이 끝나고, DRAGON 소프트웨어의 기동이 끝나면, LSP를 설정한다. LSP의 설정은 dragon vty 에 접속하여 수행한다. LSP 설정을 시작하기 전, proxy 이자 종단 더미 장비인 proxy1에서 데이터 평면의 종단 아이피인 192.2.0.2에서 192.2.0.18까지 스위치 연결이 없음을 확인하기 위하여, ping 을 수행해 본다. 반대의 경우도 테스트 해본다. LSP 설정 전 이 두 시스템은 데이터 평면의 연결이 없으므로, ping은 실패할 것이다.

```
[root@kistisvr1 bin]# ping 192.2.0.2
[root@kisti-2 bin]# ping 192.2.0.18
```

다음으로 proxy1의 dragon 데몬 vty에 접속한다.

```
[root@kistisvr1 ~]# telnet 192.168.0.2 2611
Trying 192.168.0.2...
Connected to 192.168.0.2.
Escape character is '^]'.


 ___
|   _ ₩ _ __ __ _   __ _   ___   _ __
| | | | '__/ _` |/ _` |/ _ ₩| '_ ₩
| |_| | | | (_| | (_| | (_) | | | |
|____/|_|  ₩__,_|₩__, |₩___/|_| |_|
                  |___/
(D)ynamic (R)esource (A)llocation via
(G)MPLS (O)ptical (N)etworks
Based on Zebra (version 0.94).
Copyright 1996-2002 Kunihiro Ishiguro.
Copyright 2003-2004 the Dragon Team.


User Access Verification

Password:
csa1-dragon>
```

성공적으로 vty 에 접속되면, vlan 100으로 LSP test1을 만든다. proxy 모드일 때, LSP의 설정은 CSA가 하나의 VLSR과 같이 라우팅에 참여할 때와 다르다. source 와 destinaion은 종단 시스템의 IP가 아니라 종단 시스템이 연결된 VLSR의 IP이다. 또한, lsp-id 와 tunnel-id가 아니라 그들이 연결된 스위치의 포트를 설정한다.

```
proxy1-dragon> edit lsp test1
proxy1-dragon(edit-lsp-test1)# set uni client ingress implicit egress implicit
proxy1-dragon(edit-lsp-test1)# set source ip-address 192.168.0.5 port 2049 destination ip-address 192.168.1.20 port 259
proxy1-dragon(edit-lsp-test1)# set bandwidth gige swcap l2sc encoding ethernet gpid ethernet
proxy1-dragon(edit-lsp-test1)# set vtag 100
proxy1-dragon(edit-lsp-test1)# exit
proxy1-dragon> commit lsp test1
proxy1-dragon> show lsp
                        **LSP status summary**

Name         Status      Dir    Source (IP/LSP ID)  Destination (IP/Tunnel ID)
-------------------------------------------------------------------------------
test1        Commit      <=>    192.168.0.5         192.168.1.20
                                2049                259
proxy1-dragon> show lsp
                        **LSP status summary**

Name         Status      Dir    Source (IP/LSP ID)  Destination (IP/Tunnel ID)
-------------------------------------------------------------------------------
test1        In service <=>    192.168.0.5         192.168.0.20
                               2049                259
proxy1-dragon>
```

LSP가 제대로 생성되었는지 확인하기 위해서는 현재의 프롬프트 상에서 show lsp를 수행해 본다. show lsp는 현재 존재하는 lsp의 내용을 요약해서 보여준다. 제대로 수행이 되었다면, LSP csa 는 in-service 상태여야 한다.

LSP 설정이 성공하면, 각 스위치에서 vlan이 제대로 설정되었는지 확인한다.

1) cisco 7609

```
DJ-C7609S_Antlab#show vlan id 100

VLAN Name                             Status     Ports
---- -- ------------------------ ------- --------------------------------

100  VLAN0100                         active     Gi8/0/1, Gi8/0/11

VLAN Type  SAID     MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
```

```
---- ---- -------- ----- ----- ----- -------- ---- -------- ------ ------
100  enet 100100   1500    -     -     -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary  Type              Ports
------- --------- ------------- ----------------------------------------

DJ-C7609S_Antlab#
```

2) Force10 c300

```
C300#show vlan

Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged

    NUM     Status     Description                Q Ports
*   1       Active                                U Gi 1/0-2,4-14,16-47
    100     Active                                U Gi 0/1
                                                  U Gi 1/3
C300#
```

마지막으로 이러한 설정이 제대로 되었는지 종단 시스템에서 ping으로 확인한다.

```
[root@kistisvr1 ~]# ping 192.2.0.18
PING 192.2.0.18 (192.2.0.18) 56(84) bytes of data.
64 bytes from 192.2.0.18: icmp_seq=1 ttl=64 time=0.145 ms
64 bytes from 192.2.0.18: icmp_seq=2 ttl=64 time=0.122 ms
64 bytes from 192.2.0.18: icmp_seq=3 ttl=64 time=0.148 ms
64 bytes from 192.2.0.18: icmp_seq=4 ttl=64 time=0.127 ms

[root@kisti-2 ~]# ping 192.2.0.2
PING 192.2.0.2 (192.2.0.2) 56(84) bytes of data.
64 bytes from 192.2.0.2: icmp_seq=1 ttl=64 time=0.162 ms
64 bytes from 192.2.0.2: icmp_seq=2 ttl=64 time=0.169 ms
64 bytes from 192.2.0.2: icmp_seq=3 ttl=64 time=0.108 ms
64 bytes from 192.2.0.2: icmp_seq=4 ttl=64 time=0.154 ms
```

5. Inter-domain NARB 설정 및 시험

4장까지 우리는 독립적인 도메인 내에서 LSP를 프로비저닝하였다. 본 장에서는 두 개의 도

메인에 걸쳐 있는 LSP를 설정하는 시험을 함으로써 보다 복잡한 네트워크 환경에서 VLSR을 시험하는 기본적인 예를 보여 주고자 한다. Figure 6는 시험 네트워크의 토폴로지를 보여준다. 4장에서와 달리 NARB는 각각의 도메인을 위해 하나씩 총 두 개 존재한다. 다른 도메인이라는 것은 데이터 평면을 의미하는 것이 아니다. 데이터 평면의 IP는 layer2 상에서 VLAN 으로 하나의 LSP를 설정하기 때문에 오히려 동일한 도메인 내에 있어야 한다. 이 때문에 Proxy1의 더미 시스템 대신 사용되고 있는 네트워크 인터페이스의 IP는 192.2.0.2/24 이고, Proxy2의 IP는 192.2.0.18/24 이다. 제어평면에서, Proxy1과 Proxy2는 다름 도메인에 위치한다. 각각의 도메인을 NARB1과 NARB2가 관장하고 있다. NARB1의 도메인은 192.168.0.0 도메인이고, NARB2의 도메인은 192.168.1.0 도메인이다.

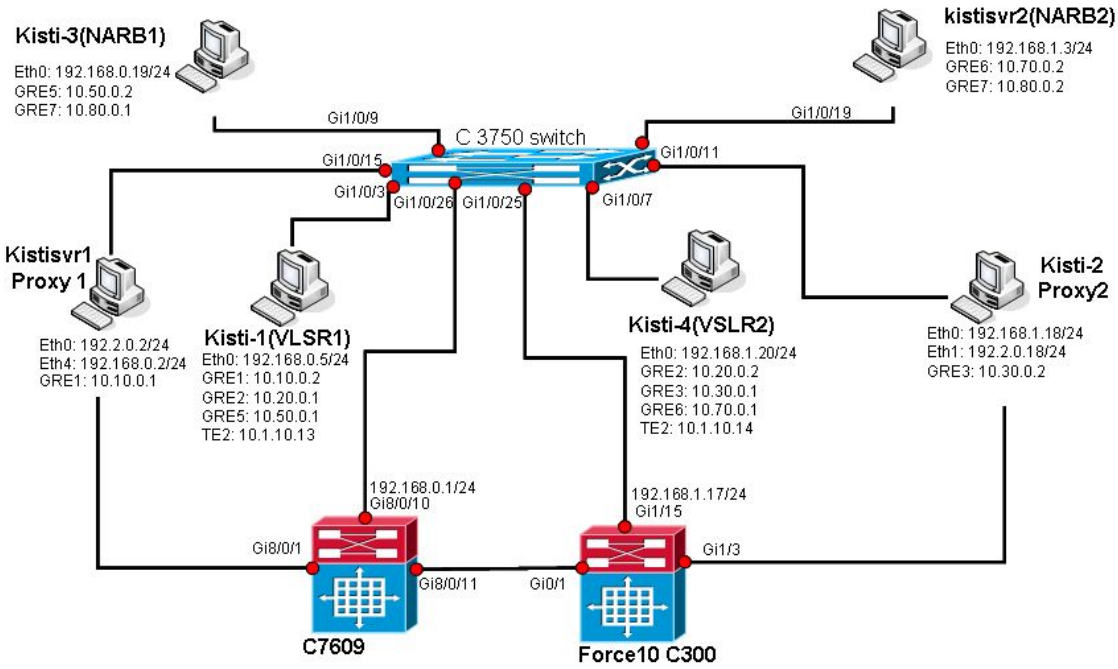

Figure 6. Inter-domain Test Network Topology

5.1 GRE 설정

Figure 6와 4.1절을 참고하여 각각의 시스템에서 GRE 터널을 설정한다. 4.1과 달리 Proxy2 와 NARB2간의 GRE 터널인 gre6와 NARB1과 NARB2와의 GRE 터널인 gre7이 추가적으로 더 필요하다.

5.2 소프트웨어 설정 파일

두 개의 NARB를 포함하는 네트워크 토폴로지는 대부분의 설정 파일이 4장과 유사하다. 그러나, 도메인이 달라져 IP에 유의하여야 한다. NARB1과 NARB2는 서로 다fms 도메인 간의 통신을 위해 많은 부분이 추가되어야 한다.

5.2.1 Proxy1 설정 파일

1) dragon.conf

```
! -*- dragon -*-
!
! DRAGON sample configuration file
!
hostname proxy1-dragon
password dragon
set local-id port 2049
```

2) ospfd.conf
UNI CSA 모드로 작동하는 Proxy1은 라우팅에 참여하지 않는다. 따라서, ospfd 데몬 프로세스는 기동하지 않으며, ospfd.conf 의 설정도 필요하지 않다.

3) RSVPD.conf
Proxy1의 RSVPD 데몬 프로세스는 데이터 평면에 연결된 실제 종단 시스템을 위해 대신 시그널링을 시작한다. 따라서, 설정 파일은 Proxy를 위한 RSVPD의 역할을 명시하여야 한다. p/2049는 dragon.conf에서 지정한 2049 포트에 실제 데이터가 연결되어 있고 이 시스템을 대신해 시그널링을 하라는 의미이다.

```
interface gre1 tc none mpls p/2049
api 4000
```

4) zebra.conf
3장의 zebra.conf와 같다.

```
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.14 1999/02/19 17:26:38 developer Exp $
!
hostname proxy1-zebra
password zebra
enable password zebra
!
! Interface's description.
!
interface lo
interface gre1
!
line vty
log file /var/log/zebra.log
```

5.2.2 Proxy2 설정 파일

1) dragon.conf

```
! -*- dragon -*-
!
! DRAGON sample configuration file
!
hostname proxy2-dragon
password dragon
set local-id port 259
```

2) ospfd.conf

UNI CSA 모드로 작동하는 Proxy1은 라우팅에 참여하지 않는다. 따라서, ospfd 데몬 프로세스는 기동하지 않으며, ospfd.conf 의 설정도 필요하지 않다.

3) RSVPD.conf

Proxy1과 마찬가지로 실제 데이터 평면의 종단 시스템을 위한 설정이 필요하다.

```
interface gre3 tc none mpls p/259
api 4000
```

4) zebra.conf

```
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.14 1999/02/19 17:26:38 developer Exp $
!
hostname proxy2-zebra
password zebra
enable password zebra
!
! Interface's description.
!
interface lo
interface gre3
!
line vty
log file /var/log/zebra.log
```

5.2.3 VLSR1 설정 파일

1) dragon.conf

```
! -*- dragon -*-
!
```

```
! DRAGON sample configuration file
!
hostname vlsr-dragon
password dragon
set local-id port 2049
configure narb intra-domain ip-address 192.168.0.19 port 2609
```

2) ospfd.conf

다른 설정은 4.2.3 절과 동일하나 VLSR1과 VLSR2는 더 이상 동일한 도메인 내에 있지 않으므로 LSA를 교환할 필요가 없다. 따라서, proxy와의 인터페이스와 마찬가지로 VLSR2와의 제어 채널인 gre2도 passive-interface 로 설정한다. 그러나, gre2에 ospf-te 정보로 OSPF-TE의 데이터 인터페이스 정보와 포트 정보등 연결에 대한 정보는 그대로 유지 하여야 한다.

```
! -*- ospf -*-
!
! OSPFd sample configuration file
!
hostname vlsr1-ospf
password dragon
enable password dragon
log stdout
log file /var/log/ospfd.log
!
! NOTE: max. bandwidth parameters are in bytes/sec, for example:
!    1 Gbps = 125000000 bytes/sec
!   10 Gbps = 1250000000 bytes/sec
!
! -*- sample ospf configuration for a dragon VLSR controlling a Layer2 Ethernet switch -*-
!
interface gre1
 description GRE tunnel between vlsr1(kisti-1) and csa1(kistisvr1)
 ip ospf network point-to-point
!
interface gre2
 description GRE tunnel between vlsr1(kisti-1) and vlsr2(kisti-4)
 ip ospf network point-to-point
!
interface gre5
 description GRE tunnel between narb-server(kisti-3) and vlsr1(kisti-1)
 ip ospf network point-to-point
!
router ospf
 ospf router-id 192.168.0.5
 network 10.10.0.0/30 area 0.0.0.0
```

```
 network 10.20.0.0/30 area 0.0.0.0
 network 10.50.0.0/30 area 0.0.0.0
 ospf-te router-address 192.168.0.5
 passive-interface gre1
 passive-interface gre2
 ospf-te interface gre2
        level gmpls
        swcap l2sc encoding ethernet
        data-interface ip 10.1.10.13 protocol snmp switch-ip 192.168.0.1 switch-port 2059
        max-bw 125000000
        max-rsv-bw 125000000
        max-lsp-bw 0 125000000
        max-lsp-bw 1 125000000
        max-lsp-bw 2 125000000
        max-lsp-bw 3 125000000
        max-lsp-bw 4 125000000
        max-lsp-bw 5 125000000
        max-lsp-bw 6 125000000
        max-lsp-bw 7 125000000
        vlan 100
        vlan 200
        metric 10
 exit
!
line vty
!
```

3) RSVPD.conf

RSVPD.conf 에는 시그널링을 위한 모든 gre 인터페이스를 기술한다. gre1 에 대해서는 이 인터페이스가 local-id를 사용하는 UNI CSA의 proxy와 연결되어 있고, 그 proxy가 대신하는 시그널링이 2049 포트에 관한 것이라는 것을 명시한다. 또한 NARB 에 ERO를 요구하기 위한 NARB의 IP 와 port 정보도 포함한다.

```
interface gre1 tc none mpls p/2049
interface gre2 tc none mpls
interface gre5 tc none mpls
api 4000
narb 192.168.0.19 2609
```

4) zebra.conf

존재하는 모든 GRE 인터페이스를 정의한다.

```
! -*- zebra -*-
!
```

```
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.14 1999/02/19 17:26:38 developer Exp $
!
hostname vlsr1-zebra
password zebra
enable password zebra
!
! Interface's description.
!
interface lo
interface gre1
interface gre2
interface gre5
!
line vty
log file /var/log/zebra.log
```

5.2.4 VLSR2 설정 파일

1) dragon.conf

VLSR2는 도메인 2의 border VLSR 이다. 따라서, VLSR1과 같이 NARB2의 정보를 추가해야 한다.

```
! -*- dragon -*-
!
! DRAGON sample configuration file
!
hostname kisti4-vlsr2
password dragon
set local-id port 259
configure narb intra-domain ip-address 192.168.1.3 port 2609
```

2) ospfd.conf

VLSR과 마찬가지로 VLSR1과의 제어채널인 gre2를 passive-interface로 정의한다.

```
! -*- ospf -*-
!
! OSPFd sample configuration file
!
hostname vlsr2-ospf
password dragon
enable password dragon
log stdout
log file /var/log/ospfd.log
```

```
!
! NOTE: max. bandwidth parameters are in bytes/sec, for example:
!    1 Gbps = 125000000 bytes/sec
!   10 Gbps = 1250000000 bytes/sec
!
! -*- sample ospf configuration for a dragon VLSR controlling a Layer2 Ethernet switch -*-
!
interface gre2
 description GRE tunnel between vlsr1(kist-1) and vlsr2(kisti-4)
 ip ospf network point-to-point
!
interface gre6
 description GRE tunnel between narb-server(kist-1) and vlsr2(kisti-4)
 ip ospf network point-to-point
!
router ospf
 ospf router-id 192.168.1.20
 network 10.20.0.0/30 area 0.0.0.0
 network 10.70.0.0/30 area 0.0.0.0
  ospf-te router-address 192.168.1.20
  passive-interface gre3
  passive-interface gre2
  ospf-te interface gre2
        level gmpls
        data-interface ip 10.1.10.14 protocol snmp switch-ip 192.168.1.17 switch-port 1
        swcap l2sc encoding ethernet
        max-bw 125000000
        max-rsv-bw 125000000
        max-lsp-bw 0 125000000
        max-lsp-bw 1 125000000
        max-lsp-bw 2 125000000
        max-lsp-bw 3 125000000
        max-lsp-bw 4 125000000
        max-lsp-bw 5 125000000
        max-lsp-bw 6 125000000
        max-lsp-bw 7 125000000
        vlan 100
        vlan 200
        metric 10
      exit
!
line vty
!
```

2) RSVPD.conf

VLSR2도 역시 border VLSR이므로, NARB2의 정보와 NARB2와의 제어채널인 gre6를 명시해 준다.

```
nterface  gre2 tc none mpls
interface gre3 tc none mpls p/259
interface gre6 tc none mpls
api 4000
narb 192.168.1.3 2609
```

3) zebra.conf
NARB2와의 제어 채널인 gre6 인터페이스를 추가해 준다.

```
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.14 1999/02/19 17:26:38 developer Exp $
!
hostname kisti4-vlsr2
password zebra
enable password zebra
!
! Interface's description.
!
interface lo
interface gre2
interface gre3
interface gre6
!
line vty
log file /var/log/zebra.log
```

5.2.5 NARB1 설정 파일

NARB를 기동하기 위해서는 narb.conf, ospfd-intra.con, ospfd-inter.conf, zebra.conf 이 필요하다.

1) narb.conf
NARB1은 내부 도메인 뿐 아니라 NARB2와 통신함으로써, 도메인간 라우팅의 책임을 지고 있다. 따라서, 내부 도메인만 관리 할 때 보다 많은 추가 적인 정보가 필요하다. 먼저 intra-domain-ospfd 에 대한 정보가 필요하다. originate-interface 는 NARB2와의 제어 채널 인터페이스인 gre7의 IP 주소이다. 또한 외부 도메인이므로 area 가 0.0.0.1 인 것에 주의한다. 네트워크 토포롤지 정보도 함께 기술한다. 마지막으로 inter-domain-te-link 에

대한 정보를 추가한다. inter-domain-te-link는 연결할 상대편 도메인의 TE 링크에 대한 정보이다. id는 NARB1의 도메인 마지막에 위치한 VLSR1이 NARB2의 VLSR2와 연결할 때 사용하는 TE 링크에 데이터 인터페이스 ip 이다. 다시 말해 VLSR2의 ospfd,conf에 있는 ospf-te interface gre2 의 data-interface ip와 일치해야 한다. narb-peer는 NARB1과 NARB2와의 제어 채널인 gre7에 부여된 NARB2의 ip 이다. 여기서는 10.80.0.2 이다.

```
!
domain-id {ip 192.168.0.0}
!
intra-domain-ospfd {address localhost port 2617
        originate-interface 10.50.0.2 area 0.0.0.0}
!
inter-domain-ospfd {address localhost port 2607
        originate-interface 10.80.0.1 area 0.0.0.1}
!
router {id 192.168.0.5
        inter-domain link to vlsr2
        link {id 192.168.1.20 type 1
                max_bw 1250.0 max_rsv_bw 1250.0
                unrsv_bw0 1250.0 unrsv_bw1 1250.0 unrsv_bw2 1250.0 unrsv_bw3 1250.0
unrsv_bw4 1250.0 unrsv_bw5 1250.0 unrsv_bw6 1250.0 unrsv_bw7 1250.0
                enc_type 2 sw_type 51
                metric 10
                local_if 10.2.10.13  remote_if 10.2.10.14
                vlan_tags(100:100)
        }
}
!
inter-domain-te-link {id 10.1.10.14 narb-peer 10.80.0.2 port 2609}
!
cli {host kisti3-narb password dragon}
!
```

2) ospfd-intra.conf

ospfd-intra.conf는 도메인 내부의 네트워크 토폴로지 정보를 교환하기 위해 VLSR1의 ospfd 데몬 프로세스와 통신하는 NARB의 ospfd 데몬 프로세스가 기동 시 참조하는 파일이다. 인터페이스 정보와 라우팅에 필요한 기본 정보만 포함하고 있다.

```
! Intra-domain ospfd configuration for narb
!   2005/03/11 16:32:10
!
hostname kisti3-ospf-intra
password dragon
log stdout
```

```
!
interface gre5
  description GRE tunnel between kisti3-narb and kisti1-vlsr
  ip ospf network point-to-point
!
router ospf
  ospf router-id 192.168.0.19
  network 10.50.0.0/30 area 0.0.0.0
   ospf-te router-address 192.168.0.19
!
line vty
```

3) ospfd-inter.conf

NARB2와의 인터페이스인 gre7을 추가하고, NARB2의 intra-domain ospfd 와의 통신을 위해 router ospf 정보도 추가한다. 단 여기서 network은 외부 도메인이므로 area 가 0.0.0.1 인 것을 주의한다.

```
!
hostname kisti3-ospf-inter
password dragon
log stdout
!
interface gre7
 description GRE tunnel between this narb server(kisti-3) and a peer narb server(kistisvr2)
 ip ospf network point-to-point
!
router ospf
 ospf router-id 192.168.0.19
 network 10.80.0.0/30 area 0.0.0.1
  ospf-te router-address 192.168.0.19
!
line vty
!
```

4) zebra.conf

NARB2와의 제어채널인 gre7을 인터페이스에 추가해 준다.

```
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.14 1999/02/19 17:26:38 developer Exp $
!
```

```
hostname kisti3-zebra
password zebra
enable password zebra
!
! Interface's description.
!
interface lo
interface gre5
interface gre7
!
line vty
log file /var/log/zebra.log
```

5) rce.conf

Resource Computation Engine 인 rce 데몬 프로세스가 기동 시 참조하는 파일이다.
도메인 아이디와 트래픽 엔지니어링 테이블을 위한 스키마 파일에 대한 설정이 필요하다.
도메인 아이디는 narb.conf와 일치해야 한다.

```
!
domain-id {ip 192.168.0.0}
!
include-tedb-schema {path /usr/local/dragon/etc/schema_combo.rsd}
!
```

5.2.6 NARB2 설정 파일

1) narb.conf

NARB1과 다른 domain-id 를 가진다.

```
!
domain-id {ip 192.168.1.0}
!
intra-domain-ospfd {address localhost port 2617
        originate-interface 10.70.0.2 area 0.0.0.0}
!
inter-domain-ospfd {address localhost port 2607
        originate-interface 10.80.0.2 area 0.0.0.1}
!
router {id 192.168.1.20
        inter-domain link to vlsr1
        link {id 192.168.0.5 type 1
                max_bw 1250.0 max_rsv_bw 1250.0
                unrsv_bw0 1250.0 unrsv_bw1 1250.0 unrsv_bw2 1250.0 unrsv_bw3 1250.0
unrsv_bw4 1250.0 unrsv_bw5 1250.0 unrsv_bw6 1250.0 unrsv_bw7 1250.0
                enc_type 2 sw_type 51
```

```
                metric 10
                local_if 10.2.10.14   remote_if 10.2.10.13
                vlan_tags(100:100)
        }
}
!
inter-domain-te-link {id 10.1.10.13 narb-peer 10.80.0.1 port 2609}
!
cli {host kistisvr2-narb password dragon}
!
```

2) ospfd-intra.conf

```
! Intra-domain ospfd configuration for narb
!   2005/03/11 16:32:10
!
hostname kistisvr2-ospf-intra
password dragon
log stdout
!
!
!
interface gre6
  description GRE tunnel between narb(kistisvr2) and vlsr2(kisti-4)
  ip ospf network point-to-point
!
router ospf
  ospf router-id 192.168.1.3
  network 10.70.0.0/30 area 0.0.0.0
   ospf-te router-address 192.168.1.3
!
line vty
!
```

3) ospfd-inter.conf

```
!
hostname kistisvr2-ospf-inter
password dragon
log stdout
!
interface gre7
 description GRE tunnel between this narb server(kistisvr2) and a peer narb server(kisti-3)
 ip ospf network point-to-point
!
router ospf
 ospf router-id 192.168.1.3
```

```
 network 10.80.0.0/30 area 0.0.0.1
   ospf-te router-address 192.168.1.3
!
line vty
!
```

4) zebra.conf

```
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.14 1999/02/19 17:26:38 developer Exp $
!
hostname kistisvr2
password zebra
enable password zebra
!
! Interface's description.
!
interface lo
interface gre6
interface gre7
!
line vty
log file /var/log/zebra.log
```

5) rce.conf

narb.conf와 동일한 domain-id로 설정해야 한다.

```
!
domain-id {ip 192.168.1.0}
!
include-tedb-schema {path /usr/local/dragon/etc/schema_combo.rsd}
!
```

5.3 DRAGON 소프트웨어 기동과 종료

4장과 같이 proxy, vlsr, narb등 기능에 맞게 dragon.sh 를 실행한다. NARB2 시스템에서는 NARB1과 마찬가지로 start-narb 옵션을 사용해 기동한다.

5.4 설정 확인

5.4.1 ospf 확인

4장에서와 달리 하나의 VLSR이 하나의 도메인을 구성하고 있으므로 표현되는 정보는 매우 간단하다.

```
[root@kisti-1 etc]# telnet localhost 2604
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Hello, this is zebra (version 0.94).
Copyright 1996-2002 Kunihiro Ishiguro.


User Access Verification

Password:
vlsr1-ospf> show ip ospf-te database detail
OSPF-TE link state database, area 0.0.0.0
Type      ID          Adv Rtr Seq       Age       Cksum     Len
Area-Router ID TLV        1.168.0.5         192.168.0.5       0x8000   0         0x44fc 28
  Router-Address: 192.168.0.5

Area-Link TLV     1.0.0.17          192.168.0.5       0x8000   0         0xcd21   176
  Link: 152 octets of data
  Link-Type: Point-to-point (1)
  Link-ID: 10.20.0.0
  Local Interface IP Address(es): 10.2.10.13
  Traffic Engineering Metric: 10
  Maximum Bandwidth: 1.25e+08 (Bytes/sec)
  Maximum Reservable Bandwidth: 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 0): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 1): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 2): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 3): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 4): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 5): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 6): 1.25e+08 (Bytes/sec)
  Unreserved Bandwidth (pri 7): 1.25e+08 (Bytes/sec)
  Interface Switching Capability Descriptor: l2sc ethernet
  Max LSP Bandwidth 0: 1.25e+08 (Bytes/sec)
  Max LSP Bandwidth 1: 1.25e+08 (Bytes/sec)
  Max LSP Bandwidth 2: 1.25e+08 (Bytes/sec)
  Max LSP Bandwidth 3: 1.25e+08 (Bytes/sec)
  Max LSP Bandwidth 4: 1.25e+08 (Bytes/sec)
  Max LSP Bandwidth 5: 1.25e+08 (Bytes/sec)
  Max LSP Bandwidth 6: 1.25e+08 (Bytes/sec)
  Max LSP Bandwidth 7: 1.25e+08 (Bytes/sec)
  -- L2SC specific information--
```

```
    --> Available VLAN tag set: 100 200
    --> Allocated VLAN tag set:

vlsr1-ospf>
```

5.4.2 narb 확인

NARB가 다른 NARB 시스템과 제대로 연결되어 있는지 확인 가능하다. NARB 시스템 IP에 2626 포트로 telenet 접속을 하고, show module 명령어를 실행하면 된다. intRA-domain OSPFd는 listner 이므로, 반드시 connected 될 필요는 없다. Next-domain NARB의 상태가 online 이고, Connection 정보가 올바로 되어 있는지 확인한다. 또한 narb 에서도 내부 도메인 네트워크 토폴로지는 확인 가능하다. show topology 명령을 통해 확인할 수 있다.

```
[root@kisti-3 etc]# telnet localhost 2626
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.


 ____
|  _ ₩ _ __ __ _  __ _  ___  _ __
| | | | '__/ _` |/ _` |/ _ ₩| '_ ₩
| |_| | | | (_| | (_| | (_) | | | |
|____/|_|  ₩__,_|₩__, |₩___/|_| |_|
                  |___/
(D)ynamic (R)esource (A)llocation via
(G)MPLS (O)ptical (N)etworks
Copyright 2003-2005 the Dragon Team.

password:
password:
narb:cli>show module
                    **NARB Module Status**

Module                  IP/Port              Status          Connection
intER-domain OSPFd    localhost/2607           online         connected
intRA-domain OSPFd    localhost/2617           online         disconnected
resource comp engine  localhost/2678           online
Next-domain  NARB      10.80.0.2/2609           online         via 10.2.10.14

narb:cli>

narb:cli>show topology
                    .......Router ID Opaque LSA.......
[on] Opaque ID (5), Adv_router (192.168.0.5), Router_id (192.168.0.5), Rt_type (0)
```

.....TE Link Opaque LSA.....
[on] Opaque ID (6), Adv_router (192.168.0.5), Router_id (192.168.1.20), IfAddr[10.2.10.13-10.2.10.14]
.....The End.....

5.4.2 rce 확인

inter domain, intra domain 네트워크 토폴로지 모두 확인 가능하다.

```
[root@kisti-3 etc]# telnet localhost 2688
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.


 ____
|  _ ₩ _ __ __ _  __ _  ___  _ __
| | | | '__/ _` |/ _` |/ _ ₩| '_ ₩
| |_| | | | (_| | (_| | (_) | | | |
|____/|_|  ₩__,_|₩__, |₩___/|_| |_|
                |___/
(D)ynamic (R)esource (A)llocation via
(G)MPLS (O)ptical (N)etworks
Copyright 2003-2005 the Dragon Team.

password:
rce:cli>show topology intradomain
                .....Router ID Opaque LSA.....
Adv_router (192.168.0.5), Router_id (192.168.0.5)
                .....TE Link Opaque LSA.....
Adv_router (192.168.0.5), Link_id (10.20.0.0), IfAddrs[10.2.10.13-0.0.0.0]
                .....The End.....

rce:cli>show topology interdomain
                .....Router ID Opaque LSA.....
Adv_router (192.168.0.5), Router_id (192.168.0.5)
Adv_router (192.168.1.20), Router_id (192.168.1.20)
                .....TE Link Opaque LSA.....
Adv_router (192.168.0.5), Link_id (192.168.1.20), IfAddrs[10.2.10.13-10.2.10.14]
Adv_router (192.168.1.20), Link_id (192.168.0.5), IfAddrs[10.2.10.14-10.2.10.13]
                .....The End.....

rce:cli>
```

5.4.1 경로 검증 테스트

narb_test 를 통해 LSP 설정 전 narb와 rce의 기능을 검증한다. 일반적으로 디폴트가 all-strict-hop 이므로 HOP-TYPE은 strict 여야 한다. 만일 내부 경로에 loose 가 있을 경우 narb.conf 나 rce.conf 의 설정 중 domain-id 정보를 확인해 보아야 한다.

```
[root@kisti-1 etc]# /usr/local/dragon/sbin/narb_test -H 192.168.0.19 -S 192.168.0.5 -D 192.168.1.20
NARB@[2008/04/10 14:31:35] : Request successful! ERO returned...
NARB@[2008/04/10 14:31:35] : HOP-TYPE [strict]: 10.2.10.13
NARB@[2008/04/10 14:31:35] : HOP-TYPE [strict]: 10.2.10.14
[root@kisti-1 etc]#
```

5.5 LSP 설정

Proxy 시스템의 dragon vty에 접속하여 LSP를 설정하고 show lsp 명령을 실행하여 최종 상태가 In service 인지 확인한다.

```
[root@kistisvr1 ~]# telnet localhost 2611
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.


 ____
|  _ ₩ _ __ __ _  __ _  ___  _ __
| | | | '__/ _` |/ _` |/ _ ₩| '_ ₩
| |_| | | | (_| | (_| | (_) | | | |
|____/|_|  ₩__,_|₩__, |₩___/|_| |_|
                |___/
(D)ynamic (R)esource (A)llocation via
(G)MPLS (O)ptical (N)etworks
Based on Zebra (version 0.94).
Copyright 1996-2002 Kunihiro Ishiguro.
Copyright 2003-2004 the Dragon Team.


User Access Verification

Password:
proxy1-dragon> edit lsp test1
proxy1-dragon(edit-lsp-test1)# set uni client ingress implicit egress implicit
proxy1-dragon(edit-lsp-test1)# set source ip-address 192.168.0.5 port 2049 destination ip-address 192.168.1.20 port 259
proxy1-dragon(edit-lsp-test1)# set bandwidth gige swcap l2sc encoding ethernet gpid ethernet
proxy1-dragon(edit-lsp-test1)# set vtag 100
```

```
proxy1-dragon(edit-lsp-test1)# exit
proxy1-dragon> commit lsp test1
proxy1-dragon> show lsp
                        **LSP status summary**

Name         Status      Dir    Source (IP/LSP ID)  Destination (IP/Tunnel ID)
-------------------------------------------------------------------------------
test1        Commit      <=>    192.168.0.5          192.168.1.20
                            2049                 259
proxy1-dragon> show lsp
                        **LSP status summary**

Name         Status      Dir    Source (IP/LSP ID)  Destination (IP/Tunnel ID)
-------------------------------------------------------------------------------
test1        In service <=>    192.168.0.5          192.168.1.20
                               2049                 259
proxy1-dragon>
```

LSP의 최종상태를 확인하고 나면, 스위치 설정이 제대로 되어 있는지 확인한다. 먼저 cisco 7609 스위치를 확인한다.

```
DJ-C7609S_Antlab#show vlan id 100

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
100  VLAN0100                         active    Gi8/0/1, Gi8/0/11

VLAN Type  SAID       MTU   Parent  RingNo  BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
100  enet  100100     1500        -      -        -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

DJ-C7609S_Antlab#
```

Force10 c300 스위치를 확인한다. 도메인간 UNI CSA 모드로 동작할 때, 스위치 간을 연결하는 포트는 Tagged port 여야 한다. 따라서, cisco 7609와 연결된 Gi 0/1 포트 앞에 Tagged를 명시하는 T를 확인한다.

```
C300#show vlan
```

```
Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged

    NUM     Status      Description                 Q Ports
*   1       Active                                  U Gi 1/0-2,4-14,16-47
    100     Active                                  T Gi 0/1
                                                    U Gi 1/3
C300#
```

ping 을 통해 실제 연결이 이루어졌는지 확인한다.

```
[root@kistisvr1 ~]# ping 192.2.0.18
PING 192.2.0.18 (192.2.0.18) 56(84) bytes of data.
64 bytes from 192.2.0.18: icmp_seq=1 ttl=64 time=0.145 ms
64 bytes from 192.2.0.18: icmp_seq=2 ttl=64 time=0.122 ms
64 bytes from 192.2.0.18: icmp_seq=3 ttl=64 time=0.148 ms
64 bytes from 192.2.0.18: icmp_seq=4 ttl=64 time=0.127 ms
64 bytes from 192.2.0.18: icmp_seq=5 ttl=64 time=0.111 ms
64 bytes from 192.2.0.18: icmp_seq=6 ttl=64 time=0.129 ms
64 bytes from 192.2.0.18: icmp_seq=7 ttl=64 time=0.155 ms
64 bytes from 192.2.0.18: icmp_seq=8 ttl=64 time=0.135 ms

--- 192.2.0.18 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 6999ms
rtt min/avg/max/mdev = 0.111/0.134/0.155/0.013 ms
[root@kistisvr1 ~]#


[root@kisti-2 ~]# ping 192.2.0.2
PING 192.2.0.2 (192.2.0.2) 56(84) bytes of data.
64 bytes from 192.2.0.2: icmp_seq=1 ttl=64 time=0.162 ms
64 bytes from 192.2.0.2: icmp_seq=2 ttl=64 time=0.169 ms
64 bytes from 192.2.0.2: icmp_seq=3 ttl=64 time=0.108 ms
64 bytes from 192.2.0.2: icmp_seq=4 ttl=64 time=0.154 ms
64 bytes from 192.2.0.2: icmp_seq=5 ttl=64 time=0.143 ms
64 bytes from 192.2.0.2: icmp_seq=6 ttl=64 time=0.132 ms
64 bytes from 192.2.0.2: icmp_seq=7 ttl=64 time=0.124 ms

--- 192.2.0.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 5999ms
rtt min/avg/max/mdev = 0.108/0.141/0.169/0.024 ms
[root@kisti-2 ~]#
```

5.6 LSP 삭제

dragon vty에서 delete 명령을 통해 삭제 가능하다. 삭제는 설정시 지정하였던 lsp name으로 해야 한다.

```
proxy1-dragon> show lsp
                        **LSP status summary**

Name         Status      Dir    Source (IP/LSP ID)  Destination (IP/Tunnel ID)
------------------------------------------------------------------------------
test1        In service <=>   192.168.0.5          192.168.1.20
                              2049                 259
proxy1-dragon> delete lsp test1
proxy1-dragon> show lsp
                        **LSP status summary**

Name         Status      Dir    Source (IP/LSP ID)  Destination (IP/Tunnel ID)
------------------------------------------------------------------------------
proxy1-dragon>
```

삭제 후 스위치에서 제대로 제거 되었는지 확인한다. DRAGON 소프트웨어는 삭제 시 VLAN 데이터베이스에서도 VLAN id를 제거한다.

```
DJ-C7609S_Antlab#show vlan id 100
VLAN id 100 not found in current VLAN database
DJ-C7609S_Antlab#

C300#show vlan

Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged

    NUM     Status     Description                  Q Ports
*   1       Active                                  U Gi 0/1
                                                    U Gi 1/0-14,16-47
C300#
```

다시 한 번 ping 으로 연결이 제거되었는지 확인한다.

```
[root@kisti-2 ~]# ping 192.2.0.2
```

```
PING 192.2.0.2 (192.2.0.2) 56(84) bytes of data.
From 192.2.0.18 icmp_seq=2 Destination Host Unreachable
From 192.2.0.18 icmp_seq=3 Destination Host Unreachable
From 192.2.0.18 icmp_seq=4 Destination Host Unreachable

--- 192.2.0.2 ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 3999ms
, pipe 3
[root@kisti-2 ~]#

[root@kistisvr1 ~]# ping 192.2.0.18
PING 192.2.0.18 (192.2.0.18) 56(84) bytes of data.
From 192.2.0.2 icmp_seq=2 Destination Host Unreachable
From 192.2.0.2 icmp_seq=3 Destination Host Unreachable
From 192.2.0.2 icmp_seq=4 Destination Host Unreachable

--- 192.2.0.18 ping statistics ---
6 packets transmitted, 0 received, +3 errors, 100% packet loss, time 4999ms
, pipe 3
[root@kistisvr1 ~]#
```

6. 결론

이상에서 우리는 Cisco 7609와 Force10 c300장비를 지원하도록 확장 개발한 DRAGON 소프트웨어의 설치와 시험을 진행하였다. 개발한 모듈은 cisco7609는 물론 Force10의 새로운 제품인 c300 스위치에도 잘 적용이 되었으며, 간단하지만, 도메인 내부, 도메인 간 설정 시험을 통해 DRAGON 소프트웨어의 동작에 대해서도 살펴보았다. 본 문서에서의 시험은 이 후 이들 이더넷 스위치로 구성된 망에서 DRAGON 소프트웨어를 도입하는데 유용할 것으로 보인다.

7. 참고문헌

[1] "Virtual Label Swtiching Router Implementation Guide, version 2.1a" December, 2007.
[2] "NARB and RCE Architecture", December 2007, http://dragon.east.isi.edu
[3] "NARB Design and User Manual", December, 2007, http://dragon.east.isi.edu
[4] "RCE Design and User Manual", December 2007, http://dragon.east.isi.edu
[5] "GNU Zebra Routing Protocol Suite", http://www.zebra.org
[6] Mark Meijerink, Rob Prickaerts, "Generalized MPLS, The DRAGON Project implementation at SARA", July 2006.
[7] "DRAGON Workshop Lab Exercises", Designing and Engineering Dynamic Circuit Services: A Hands-On Workshop, 2007,
http://events.internet2.edu/2007/DCS/materials/WorkshopLabMasterv2.1.doc