IPv6 포럼 코리아 기술문서 2001-006

인터넷 트래픽 수동적 측정 도구 Cflowd의 설치 및 설정방법

Installation & Configuration of Cflowd for Internet Traffic Passive Measurement (for Linux 2.4.5)

정재훈 (J. H. Jeong) ETRI
이승윤 (S. Y. Lee) ETRI
김용진 (Y. J. Kim) ETRI

목차

인터넷 트래픽 수동적 측정 도구 Cflowd의 설치 및 설정방법

Installation & Configuration of Cflowd for Internet Traffic Passive Measurement (for Linux 2.4.5)

정재훈 (J. H. Jeong) ETRI
이승윤 (S. Y. Lee) ETRI
김용진 (Y. J. Kim) ETRI

본 문서는 인터넷 트래픽 분석을 위한 수동적 측정에 대해 설명하고, Linux 2.4.5 운영체제를 이용하여 인터넷 트래픽을 분석할 수 있게 하는 대표적인 수동적 측정도구인 Cflowd에 대한 설치 및 운영방법에 대해 기술한다.

1. 수동적 측정

수동적 측정은 네트워크에 유통되는 패킷 정보를 수집하고 분석함으로써 이용자별, 시간대별, 프로토콜별, 응용별로 특정 네트워크을 출입한 패킷을 파악하여 그 네트워크의 트래픽 특성을 파악할 수 있게 한다. 인터넷 백본에서의 트래픽 유통량이나 사용 패턴의 분석은 그 백본 네트워크의 성능 파악은 물론 앞으로의 네트워크 링크 용량 증대에 유용한 정보를 제공한다[1].

기존에 수행되었던 인터넷 트래픽 패턴 분석의 연구에 의하면 대부분의 인터넷 패킷은 송신자와 수신자 사이의 연속적인 데이터 흐름을 이루고 있음이 밝혀졌다. 이러한 연구의 결과로 등장한 MPLS(Multi-Protocol Label Switching)는 인터넷 트래픽을 연속적인 패킷 흐름인 플로우(Flow)로 모델링하여 고정된 레이블(Label)을 이용하여 고속으로 패킷을 스위칭함으로써 IP 라우팅의 성능을 향상시킬 수 있다. IP 플로우는 다음과 같이 정의될 수 있다. IP 플로우는 응용의 주소 쌍(송신자 주소, 송신자 포트 번호, 수신자 주소, 수신자 포트 번호), 호스트 쌍(송신자 네트워크 주소, 수신자 네트워크 주소), AS 번호 쌍(송신자 AS 번호, 수신자 AS 번호)등으로 명세되는 제한된 시간내에 도착하는 IP 패킷들의 흐름이다. 이러한 플로우 모델은 Packet train 모델로 처음 제안되었다[2]. 플로우의 정의는 사람마다 다르다. 플로우 정의의 한 예를 들면, TCP 연결에서 송신자와 수신자의 주소와 포트 쌍으로 이루어진 플로우는 SYN과 ACK로 플로우의 시작과 끝을 구분할 수 있다. 플로우의 길이는 다양한데, 전자메일은 대부분 몇 개의 IP 패킷으로 플로우를 구성하지만, VOD와 같은 멀티미디어 서비스의 플로우는 많은 IP 패킷으로 플로우를 구성한다.

이러한 플로우 측정을 포함하는 대표적인 수동적인 측정 시스템 중 하나로써 Cisco의 NetFlow와 CAIDA 그룹의 Cflowd를 결합한 구조를 본 문서에서 설명한다.

1.1 NetFlow

Cisco의 네트워크 플로우는 송신자에서 수신자로의 일련의 단방향성 패킷의 흐름으로 정의된다[3]. Cisco의 NetFlow는 Cisco 라우터가 각 네트워크 인터페이스를 통해 지나가는 트래픽의 플로우 정보를 제공하는 기능이다. 플로우의 구분은 IP 주소와 포트 번호로 되는데, Cisco의 NetFlow는 플로우의 구분을 위해 IP Protocol type, Type of Service(TOS) 그리고 Input interface identifier도 같이 사용하면서 플로우의 정보를 제공한다. NetFlow는 NetFlow Cache를 이용하여 동작하는데, NetFlow Cache Software는 특정 패킷이 기존에 존재하는 플로우에 속하는지 여부에 따라 Cache에 새로운 플로우 엔트리를 생성할지를 결정한다. 또한 플로우 해제시간(Expire Time)이 지난 플로우들의 정보를 그림 1의 'NetFlow Export' UDP 데이터그램의 Payload에 담아서 플로우 정보 Export 네트워크 인터페이스로 전송한다. 그림 2는 Cisco NetFlow Version 5 Flow Header를 기술하고 있고, 그림 3은 Cisco NetFlow Version 5의 Flow Entry를 기술하고 있다.

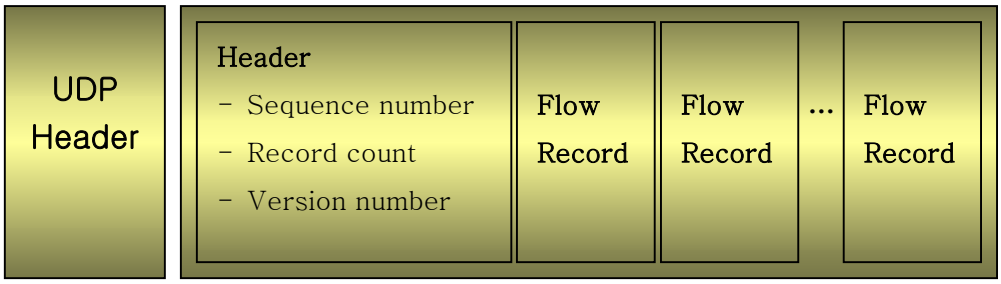

그림 1. NetFlow Export UDP 데이터그램 구조

version	count
sysUpTime	
unix seconds	
unix nano seconds	
flow sequence number	
engine type	engine ID	reserved

그림 2. Cisco NetFlow Version 5 Flow Header

source IP address			
detination IP address			
next hop IP address			
input interface index		output interface index	
packets			
bytes			
start time of flow			
end time of flow			
source port		destination port	
pad	TCP flags	IP protocol	TOS
source port		destination port	
src netmask len	det netmask len	padding	

그림 3. Cisco NetFlow Version 5 Flow Entry

1.2 Cflowd

Cflowd는 Cisco의 NetFlow를 이용한 스위칭 방법을 분석하기 위해 현재 사용되고 있는 플로우 분석 도구이다[4]. 현재 배포된 버전은 수집, 저장, 기본적인 분석 모듈을 포함하고 있다. arts++ 라이브러리를 이용하여 기본적인 분석 모듈을 만들었다[5]. 위의 분석 패키지는 ISP나 네트워크 엔지니어가 Capacity planning, Trends analysis 그리고 네트워크 서비스 환경에서 Workload의 특성을 파악할 수 있도록 데이터 수집과 분석 기능을 제공하고 있다. 그밖에도 Web hosting, Billing, Network planning, Network monitoring 그리고 Data warehousing/mining 등을 할 수 있게 한다. 그림 4는 Cflowd의 Data 흐름을 나타내고 있다.

그림 4와 같이 각 Cisco 라우터는 Flow-export 패킷을 cflowdmux와 cflowd를 실행하고 있는 호스트에 보낸다. 호스트의 cflowdmux는 UDP 데이터그램인 Flow-export 패킷을 수신하여 공유메모리 버퍼에 쓰고, 호스트의 cflowd는 공유메모리에 쓰여진 패킷을 읽어서 로컬 테이블에 저장한다. 최종 데이터 수집은 호스트의 cfdcollect에 의해 수행되는데, cfdcollect는 주기적으로 한번에 하나의 cflowd와 TCP 연결을 맺고 cflowd의 로컬 테이블로부터 데이블 데이터를 수집하여 ARTS라는 바이너리 파일로 저장한다. arts++ 유틸리티를 통해 ARTS 파일로부터 AS matrix와 Net matrix같은 여러 가지 통계정보를 얻을 수 있는데, 이 통계정보를 가지고 데이터를 수집한 네트워크의 트래픽을 분석할 수 있다.

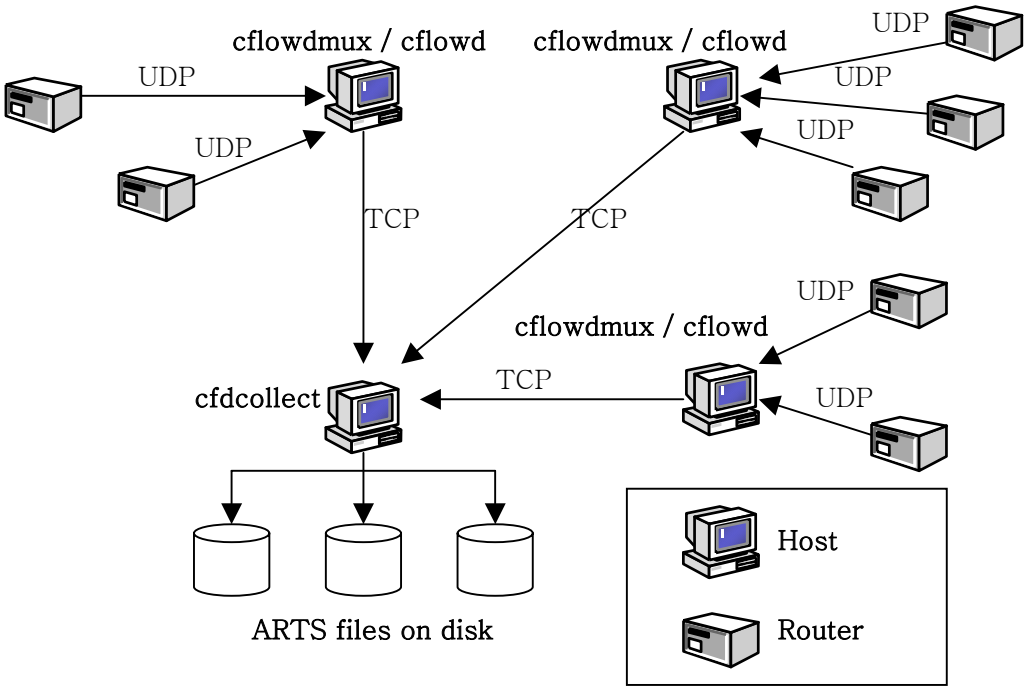

그림 4. Cflowd data flow

2. cflowd 설치

cflowd 관련 프로그램은 CAIDA 그룹의 Web-site(http://www.caida.org)에서 다운로드 받을 수 있다. 사용 OS(운영체제)로는 Linux Redhat 최신 버전(Linux 2.4.5)을 사용하기를 권장한다.

2.1 cflowd 관련 프로그램의 다운로드

cflowd와 arts++를 http://www.caida.org/tools/measurement/cflowd/에서 다운로드한다. cflowd 프로그램은 그림 5에서와 같이 ftp://ftp.caida.org/pub/cflowd/ 에서 cflowd-2-1-b1.tar.gz를 다운로드하여 얻을 수 있고, arts++ 유틸리티는 그림 6에서와 같이 arts++-1-1-a8.tar.gz를 다운로드하여 얻을 수 있다.

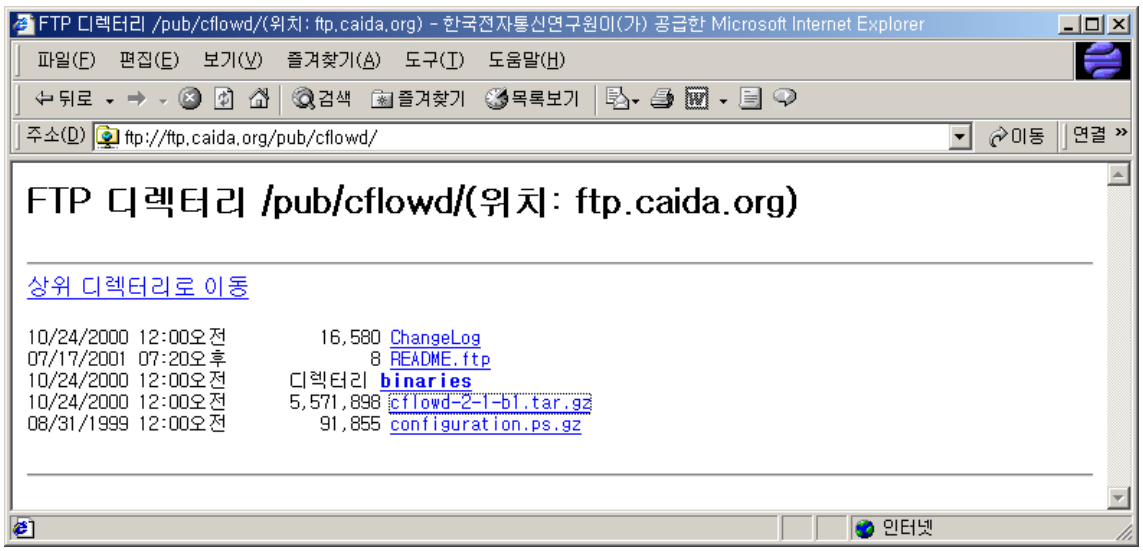

그림5. cflowd 프로그램 다운로드 페이지

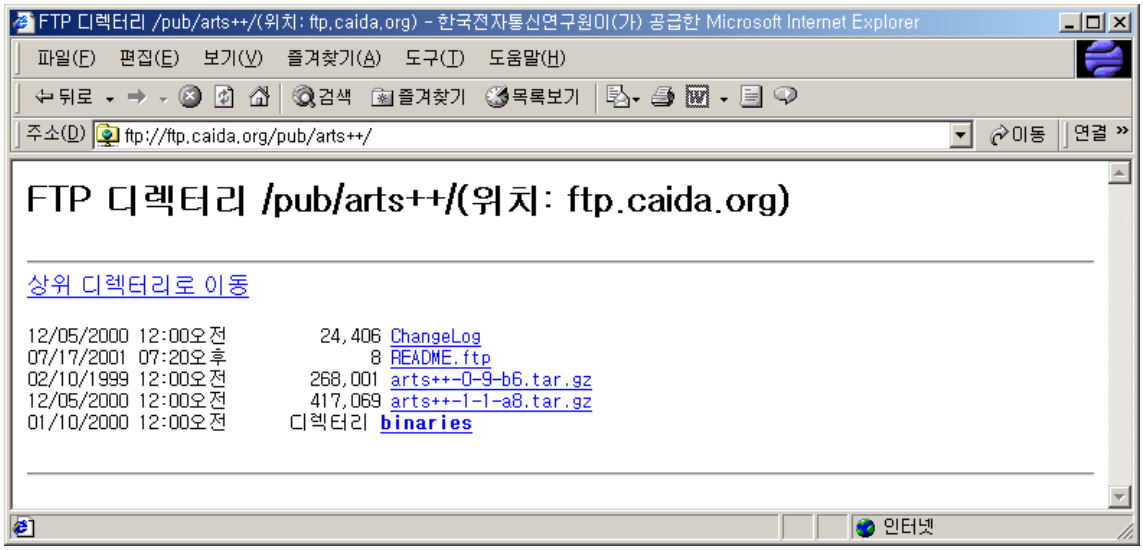

그림6. arts++유틸리티 다운로드 페이지

2.2 cflowd 관련 프로그램의 설치

arts++ 유틸리티는 cflowd가 필요로 하는 라이브러리를 제공하므로 arts++ 유틸리티를 먼저 설치하고, 그 다음으로 cflowd를 설치한다.

1) cflowd를 설치할 네트워크의 구성

그림 7은 cflowd 프로그램을 설치할 Host A(129.254.164.13)가 위치할 네트워크를 나타내고 있다. 그림 7과 같이 Host A에 cflowd, cflowdmux 그리고 cfdcollect를 모두 실행시킨다. 물론 그림 4와 같이 cflowd와 cflowdmux를 실행시킬 Host와 cfdcollect를 실행시킬 Host를 분리할 수도 있다.

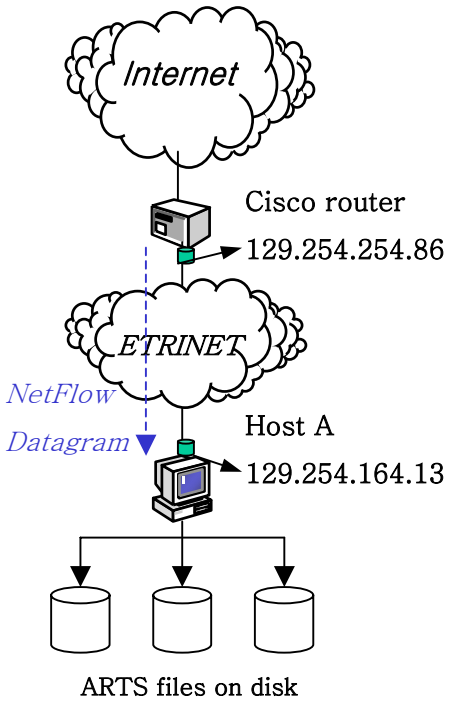

그림 7. 네트워크의 구성

2) arts++의 설치

arts++-1-1-a8.tar.gz를 /usr/local/에 복사해서 다음의 절차로 인스톨한다.

```
$ tar xvfz arts++-1-1-a8.tar.gz
$ cd arts++-1-1-a8
$ ./configure
$ make
$ make install
$ cd ..
```

arts++ 유틸리티를 위의 순서로 인스톨하면 arts++-1-1-a8과 같은 위치에 arts라는 디렉토리가 생성되어 있다. 이 디렉토리에 arts++ 유틸리티가 인스톨되어 있다.

3) cflowd의 설치

cflowd-2-1-b1.tar.gz를 /usr/local/에 복사해서 다음의 절차로 인스톨한다.

```
$tar xvfz cflowd-2-1-b1.tar.gz
$cd cflowd-2-1-b1.tar.gz
$./configure
$make
$make strip (optional)
$make install
$make install-lib (optional)
$cd ..
```

'make install'은 binary와 example configuration file들을 인스톨한다. 'make install-lib'는 사용자가 cflowd library를 사용하여 새로운 응용을 만들 때 필요한 header file과 cflowd library를 인스톨한다.

2.3 Cisco router의 Configuration 추가

1) Cisco router에 NetFlow 기능을 enable 시키기

Cisco route의 IP 주소가 129.254.254.85이라고 가정한다.

```
$telnet 129.254.254.85 #cisco router
User Access Verification

Password: xxxxxx
ipv6-gw>enable
Password: xxxxxx
ipv6-gw#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.   End with CNTL/Z.
ipv6-gw(config)#ip flow-cache timeout inactive 300
ipv6-gw(config)#ip flow-cache timeout active 1
ipv6-gw(config)#ip cef
ipv6-gw(config)#ip flow-export version 5 peer-as
ipv6-gw(config)#ip flow-export destination 129.254.164.13 2055
ipv6-gw#write
Building configuration...
[OK]
ipv6-gw#
```

Cisco router로부터 Flow information을 얻기 위해서 설정해야 할 Configuration은 다음과 같다.

ipv6-gw(config)#ip flow-cache timeout inactive 300는 Flow cache의 inactive flow timeout을 300초로 설정한다.

ipv6-gw(config)#ip flow-cache timeout active 1는 Flow cache의 active flow timeout을 1초로 설정한다.

ipv6-gw(config)#ip flow-export version 5 peer-as는 NetFlow의 Version을 5로 설정한다.

ipv6-gw(config)#ip flow-export destination 129.254.164.13 2055는 NetFlow Datagram을 받는 cflowdmux 프로세스가 실행되는 Host의 IP 주소가 129.254.164.13이고, 목적 UDP port번호가 2055임을 나타낸다.

ipv6-gw(config)#ip cef는 Cisco Express Forwarding 기능을 enable시켜서 NetFlow를

forwarding시킨다.

2)NetFlow기능을 enable시키고자 하는 Interface의 구성

NetFlow 기능을 enable시킬 Interface를 선택하여, 아래와 같이 Configuration한다.

```
ipv6-gw#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.   End with CNTL/Z.
ipv6-gw(config)#interface Ethernet1
ipv6-gw(config-if)#ip route-cache flow
ipv6-gw(config-if)#^Z
ipv6-gw#write
Building configuration...
[OK]
ipv6-gw#
```

ipv6-gw(config)#interface Ethernet1는 Interface Ethernet1를 선택한다.
ipv6-gw(config-if)#ip route-cache flow는 Ethernet1에 Flow-switching 기능을 enable시켜서, NetFlow datagram을 export하게 한다.

2.4 cflowd의 Configuration 파일 설정[6]

cflowd가 사용하는 Configuration 파일은 두개가 있다. (a) cflowd.conf와 (b) cfdcollect.conf이다.

1) cflowd.conf의 설정

cflowd, cflowdmux 그리고 cfdases와 cfdnets같은 local utility들은 'cflowd.conf' configuration file에서 초기화를 위한 정보를 얻는다. cflowd.conf는 디폴트로 /usr/local/arts/etc/ 디렉토리에 저장된다. 그런데, cflowd가 인스톨되었을 때의 파일 이름은 cflowd.conf.example이므로 아래와 같이 cflowd.conf 파일을 하나 복사한다.

```
$cd /usr/local/arts/etc/
$cp cflowd.conf.example cflowd.conf
```

cflowd.conf는 세 개의 절로 구성된다. (a) OPTIONS절, (b) CISCOEXPORTER절 그리고 (c) COLLECTOR절이다.
OPTION절은 cflowd 시스템 전역에 사용되는 값을 설정하며, CISCOEXPORTER절은 Data를 수집할 Cisco router에 대한 Configuration 값을 설정하고, COLLECTOR는 어떤 호스트들의 cfdcollect가 Data를 수집하는 cflowd에 연결할 수 있는지를 설정한다.

(1) OPTIONS절의 설정

OPTIONS절을 구성하는 항목은 표 1과 같다.

항 목	역 할
LOGFACILITY	cflowd와 cflowdmux의 logging을 위해 사용될 syslog facility를 설정한다.
TCPCOLLECTPORT	cflowd가 cfdcollect의 접속을 받아들이는데 사용될 Listen socket의 port번호를 지정한다.
PKTBUFSIZE	cflowdmux가 Netflow datagram을 수신하기 위해 사용하는 Shared memory를 구성하는 2개의 toggle buffer의 각각의 크기를 지정한다.
TABLESOCKETFILE	cfdases와 cfdnets같은 Local table client들이 cflowd에게 접속을 할 때 사용되는 cflowd의 Listen socket(Named stream socket)의 path를 나타낸다.
FLOWDIR	Raw flow file들이 저장될 디렉토리를 나타낸다. 이것은 CISCOEXPORTER절에 flows가 정의될 때 사용된다.
FLOWFILELEN	Raw flow file의 크기를 나타낸다. cflowd는 Raw flow file이 이 크기에 도달하게 될 때, 0의 크기로 조정되어 다시 증가하게 된다 (Roll over).
NUMFLOWFILES	Router당 사용될 Raw flow file의 수를 지정한다.
MINLOGMISSED	cflowd가 missed flow들에 대한 Message를 syslog하는데 사용할 Threshold를 지정한다.

표 1. OPTIONS절의 항목

cflowd를 인스톨했을 때 제공되는 OPTIONS절이 그림 8과 같이 설정이 되어 있는데, 그대로 이용하면 된다. 주의할 점은 FLOWDIR이 가리키는 디렉토리가 없다면, 사용자가 반드시 명시적으로 만들어주어야 한다. 이 디렉토리가 없으면 cflowd는 Flow 정보를 저장할 Raw flow file들을 생성할 수 없다. FLOWDIR가 그림 8에 제시된 값 (/usr/local/arts/etc/cflowd/flows)과 다른 디렉토리를 가리킬 수 있으나, 그 디렉토리가 존

재하지 않는다면, 사용자가 그 디렉토리를 명시적으로 만들어 주어야 한다.

```
OPTIONS {
LOGFACILITY:          local6
TCPCOLLECTPORT:       2056
PKTBUFSIZE:           2097152
PKTBUFSIZE:           2097152
TABLESOCKFILE:        /usr/local/arts/etc/cflowdtable.socket
FLOWDIR:              /usr/local/arts/data/cflowd/flows
FLOWFILELEN:          1000000
NUMFLOWFILES:         10
MINLOGMISSED:         1000
}
```

그림 8. OPTIONS절 항목 설정의 예

(2) CISCOEXPORTER절의 설정

NetFlow datagram을 전송할 Cisco router에 대한 설정에 사용되는 절로써 1개 이상의 CISCOEXPORTER절이 있을 수 있다. CISCOEXPORTER절을 구성하는 항목은 다음과 같다.

항 목	역 할
HOST	Cisco router의 IP 주소를 설정한다.
ADDRESSES	Cisco router가 갖고 있는 Interface들의 IP 주소를 설정한다.
CFDATAPORT	Cflowdmux가 Cisco router로부터의 Netflow datagram을 수신하는데 사용되는 UDP Socket의 Port번호를 명시한다. Cisco router에서 flow-export destination port로 지정한 것과 같아야 한다.
LOCALAS	Cisco router의 Local AS를 지정한다.
SNMPCOMM	Router로부터 Interface descriptions(ifDescr)와 IP 주소들(ipAdEntIfIndex)을 받아들일 때 사용되는 SNMP(v1) community name을 명시한다.
COLLECT	Cisco router의 Flow-export data(NetFlow datagram)로부터 추출하여 수집할 Data의 종류를 선정한다.

표 2. CISCOEXPORTER절의 항목

ADDRESSES에 지정된 Cisco router의 네트워크 인터페이스를 통과하는 트래픽 정보를 수집한다.

COLLECT의 Data 종류로는 asmatrix(AS matrix), netmatrix(net matrix), portmatrix(port matrix), ifmatrix(interface matrix), protocol(protocol table), nexthop(IP nexthop table), tos(TOS table), flows(raw flow data)가 있다. Matrix는 한쪽에서 다른쪽으로의 traffic 량을 packet수와 byte수로 나타낸 것이고, Table은 각각에 대한 packet 수와 byte 수를 나타낸 것이다. 예를 들면, asmatrix는 source ASes로부터 destination ASes로 가는 Traffic을 packet 수와 byte 수로 나타낸 것이고,protocol은 IP protocol별로 Traffic을 packet 수와 byte 수로 나타낸 것이다.

그림 9의 CISCOEXPORTER절을 구성된 네트워크에 맞게 설정한다. 그림 7을 보면, NetFlow Datagram을 export할 Cisco router의 IP 주소는 129.254.254.86이고, 트래픽 수집에 사용될 Interface는 하나이고 그것의 IP 주소도 129.254.254.86이다. Cisco router는 AS번호가 3748인 ETRINET에 포함되어 있다. 그림 9는 구성 네트워크의 정보를 CISCOEXPORTER절에 반영하고 있다.

```
CISCOEXPORTER {
   HOST:            129.254.254.86       #   IP address of Cisco sending data.
   ADDRESSES:      { 129.254.254.86 }   #   Addresses of interfaces on Cisco
                                          #     sending data.
   CFDATAPORT:    2055                  #   Port on which to listen for data.
   SNMPCOMM:       'public'              #   SNMP community name.
   LOCALAS:        3748                  #   Local AS of Cisco sending data
                                          #-> ETRINET
   COLLECT:        { protocol, portmatrix, ifmatrix, nexthop, netmatrix,
                     asmatrix, tos, flows }
}
```

그림 9. CISCOEXPORTER절 항목 설정의 예

(3) COLLECTOR절의 설정

cfdcollect를 실행하는 Host의 Configuration 값을 설정하는데 사용된다. cfdcollect가 여러 개 있을 수 있는데, 이러한 경우에는 COLLECTOR절이 두 개 이상 존재한다. 표 3은 COLLECTOR절의 항목을 나타낸다.

항 목	역 할
HOST	cfdcollect를 실행하는 Host의 IP 주소를 설정한다.
ADDRESSES	cfdcollect를 실행하는 Host가 갖고 있는 Interface들의 IP 주소를 설정한다.
AUTH	현재 사용되지 않는다.

표 3. COLLECTOR절의 항목

그림 10의 COLLECTOR절을 구성된 네트워크에 맞게 설정한다. 그림 7을 보면, 측정된 트랙픽 정보를 수집하는 cfdcollect가 실행되는 Host의 IP 주소는 129.254.164.13이고, 사용될 Interface는 하나이고 그 주소도 129.254.164.13이다. 그림 10은 구성 네트워크의 정보를 COLLECTOR절에 반영하고 있다.

```
COLLECTOR {
   HOST:          129.254.164.13   # IP address of central collector
   ADDRESSES:     { 129.254.164.13 }
   AUTH:          none
}
```

그림 10. COLLECTOR절 항목 설정의 예

2) cfdcollect.conf의 설정

cfdcollect는 'cfdcollect.conf' configuration file에서 초기화를 위한 정보를 얻는다. cfdcollect.conf는 디폴트로 /usr/local/arts/etc/ 디렉토리에 저장된다. 그런데, cflowd가 인스톨되었을 때의 파일 이름은 cfdcollect.conf.example이므로 아래와 같이 cfdcollect.conf 파일을 하나 복사한다.

```
$cd /usr/local/arts/etc/
$cp cfdcollect.conf.example cfdcollect.conf
```

cfdcollect.conf는 두 개의 절로 구성된다. (a) system절과 (b) cflowd절이다.
system절은 cfdcollect 전역에 사용되는 값을 설정하며, cflowd절은 Data를 수집할 cflowd의 각 Instance에 대한 정보를 설정한다.

(1) system절의 설정

표 4는 system절의 항목을 나타낸다.

항 목	역 할
logFacility	cfdcollect의 logging을 위해 사용될 syslog facility를 설정한다.
dataDirectory	각 Router의 ARTS file을 저장할 Top-level 디렉토리를 설정한다.
filePrefix	ARTS file 이름의 Prefix를 지정한다.
pidFile	cfdcollect의 Process ID를 저장하는 File의 절대경로를 설정한다.

표 4. system절의 항목

system절은 그림 11과 같이 디폴트로 설정된 것을 그대로 사용해도 된다. cfdcollect는 cflowd로부터 수집한 Flow 정보를 저장할 ARTS 파일 저장디렉토리를 dataDirectory (/usr/local/arts/data/cflowd) 안에 만든다. 디렉토리 이름은 cflowd.conf 파일의 CISCOEXPORTER절의 ADDRESSES에 명시된 네트워크 인터페이스의 IP 주소이다. ARTS 파일은 IP 주소를 이름으로 갖는 디렉토리에 저장되고, ARTS의 파일이름은 filePrefix(arts)에 년월일이 추가되어 만들어 진다.
예를 들어, 2001년 8월 17일 하루동안 129.254.254.86를 통과하는 트래픽 정보를 담은 ARTS파일의 이름은 arts20010817이고,이 파일은 /usr/local/arts/data/cflowd/129.254.254.86 디렉토리에 저장된다.

```
system {
   logFacility:          local6          #   Syslog to local6 facility.
   dataDirectory:        /usr/local/arts/data/cflowd
   filePrefix:           arts
   pidFile:              /usr/local/arts/etc/cfdcollect.pid
}
```

그림 11. system절 항목 설정의 예

(2) cflowd절의 설정

표 5는 cflowd절의 항목을 나타낸다.

항 목	역 할
host	cflowd를 실행하는 Host의 IP 주소를 나타낸다.
tcpCollectPort	cflowd의 Listen socket의 Port번호를 나타낸다. Cflowd.conf의 OPTION절의 TCPCOLLECTPORT항에 설정된 값과 같아야 한다.
minPollInterval	cflowd에 접속하여 Flow data를 수집하는 간격을 나타낸다.

표 5. cflowd절의 항목

host는 cfdcollect가 Flow 정보를 수집하기 위해 접속하는 cflowd가 실행되고 있는 호스트를 나타낸다.

```
cflowd {
   host:                129.254.164.13
# host:                localhost
   tcpCollectPort:      2056
   minPollInterval:     300 #unit: second
}
```

그림 12. cflowd절 항목 설정의 예

2.5 cflowd 프로그램의 실행

1) cflowd 관련 프로세스의 실행

아래와 같이 cflowdmux를 가장 먼저 실행하고, 그 다음으로 cflowd를 실행하고, 마지막으로 cfdcollect를 실행한다.

```
$cflowdmux /usr/local/arts/etc/cflowd.conf #또는 cflowdmux만 실행시켜도 됨.
$cflowd /usr/local/arts/etc/cflowd.conf #또는 cflowd만 실행시켜도 됨.
$cfdcollect /usr/local/arts/etc/cfdcollect.conf
```

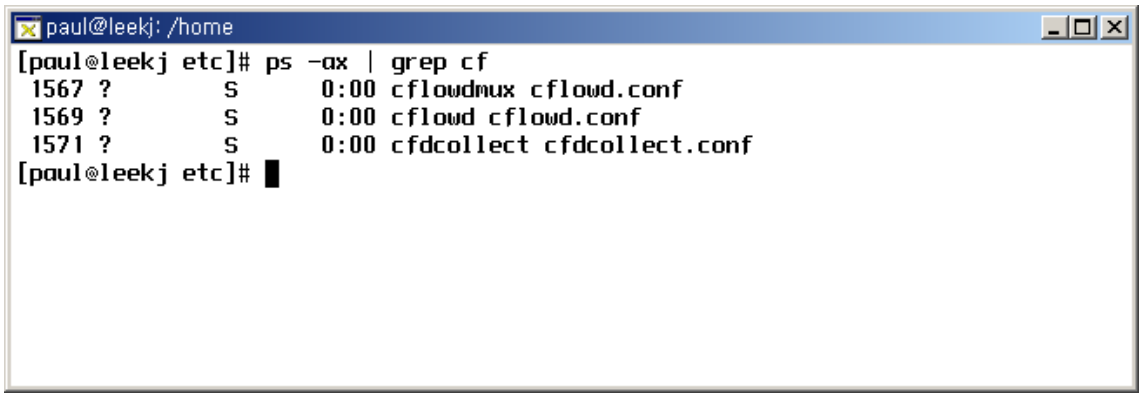

그림 13. cflowd 관련 프로세스의 동작 확인

2) Cflowd 작동 확인 및 문제 해결

'ps -ax | grep cf'를 실행하여 그림 13같이 세 개의 프로세스가 정상적으로 실행되고 있는지 확인한다. 다음으로 Cisco router로부터 NetFlow datagram을 제대로 받고 있는지 확인한다. 그림 14와 같이 Raw flow file들이 /usr/local/arts/data/cflowd/flows 디렉토리에 저장되기 시작하면, Cflowd 시스템이 정상적으로 동작하고 있다고 간주할 수 한다. 만약에 파일이 생성되지 않으면, 다음의 순서로 문제의 원인을 발견하여 해결할 수 있다.

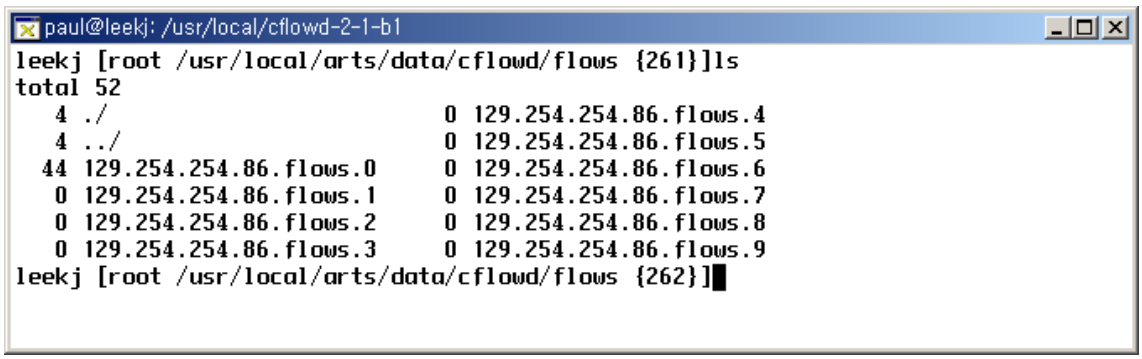

그림 14. Raw flow file의 생성

(1) cflowd 설정파일 확인

cflowd.conf와 cfdcollect.conf가 네트워크 구성에 맞게 정확하게 설정되어 있는지 확인한다. 2.4절의 'cflowd의 Configuration 파일 설정'을 참고한다.

(2) Router의 설정 확인

그림 15와 같이 tcpdump를 이용하여 NetFlow datagram이 오는지 살펴본다. Cisco

router(IP 주소: 129.254.254.86)가 NetFlow datagram을 포트 2055으로 cflowd가 실행되는 호스트(IP 주소: 129.254.164.13)에게 보내고 있는지 확인한다. 만약에 그림 15과 같이 NetFlow datagram이 수신되지 않는다면, 라우터 설정에 문제가 있을 수 있으므로, 2.3절의 'Cisco router의 Configuration 추가'를 참고하여 라우터 설정이 제대로 되어있는지 확인한다.

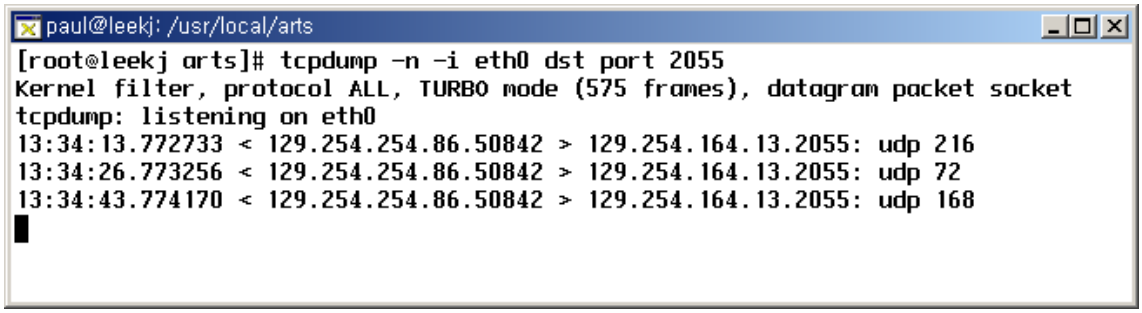

그림 15. tcpdump를 이용한 NetFlow datagram의 수신 확인

3. ARTS 파일의 가공 및 분석

cflowd 프로그램을 이용하여 ARTS 파일을 저장한 후, arts++ 패키지의 여러 유틸리티를 이용하여, Raw data인 ARTS 파일로부터 원하는 여러 가지 정보를 얻을 수 있다[7]. 예를 들면, ARTS 파일에 저장된 Flow 정보를 가지고 Protocol별로 트래픽 량을 알고 싶을 때, artsprotos 유틸리티를 이용하면 된다. 그림 16은 cfdcollect가 저장한 ARTS 파일을 보여주고 있고, 그림 17은 artsprotos 유틸리티를 이용하여 5분 단위로 Protocol별 트래픽 량을 볼 수 있다.

하루 단위로 Protocol별 트래픽 량을 볼려면, 먼저 그림 18과 같이 Aggregation 유틸리티인 artsprotoagg를 이용하여 ARTS 파일을 하루단위로 Aggregation한다. 그리고 나면, 그림 19와 같이 artsprotos 유틸리티로 하루 단위로 Protocol별 트래픽 량을 볼 수가 있다.

이와 같은 수동적 측정을 통해 얻은 정보로 측정된 네트워크의 트래픽 종류와 트래픽 양을 파악하여, 그 네트워크의 트래픽 특성을 파악할 수 있다. 측정된 트래픽 특성을 가지고 Network management, Billing, Network planning 그리고 Network monitoring 등을 할 수 있을 것이다.

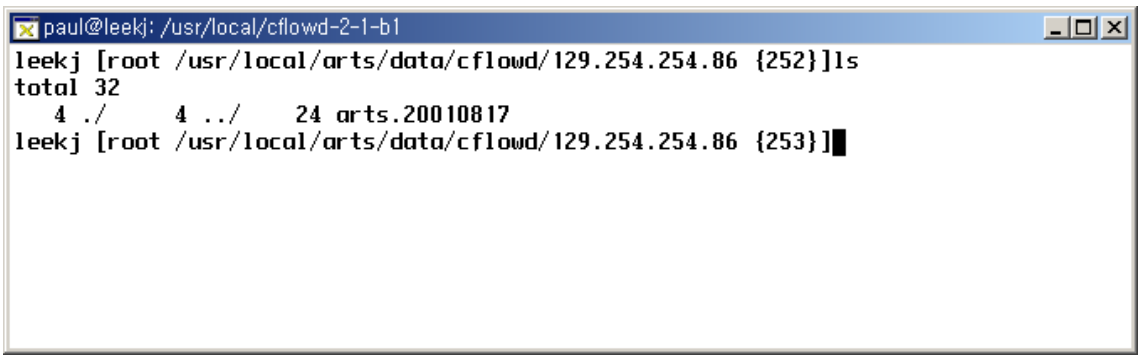

그림 16. ARTS 파일

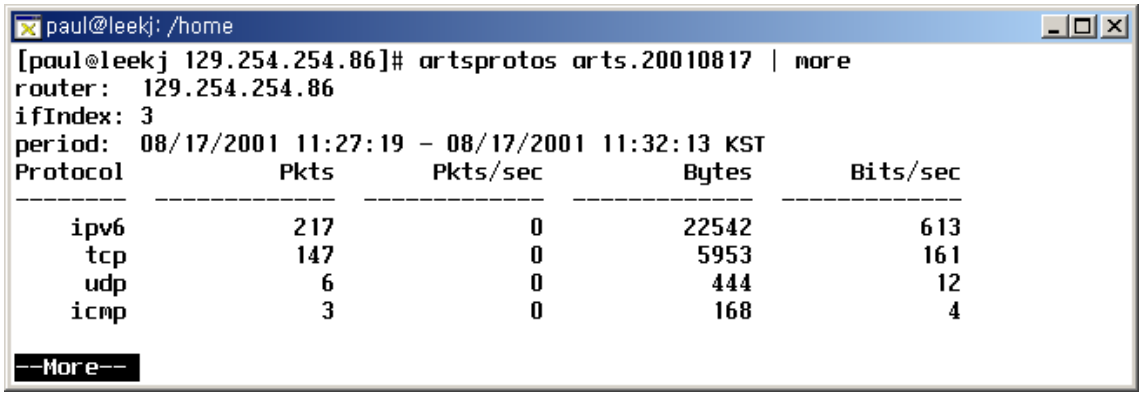

그림 17. 5분 단위의 Protocol별 트래픽 량

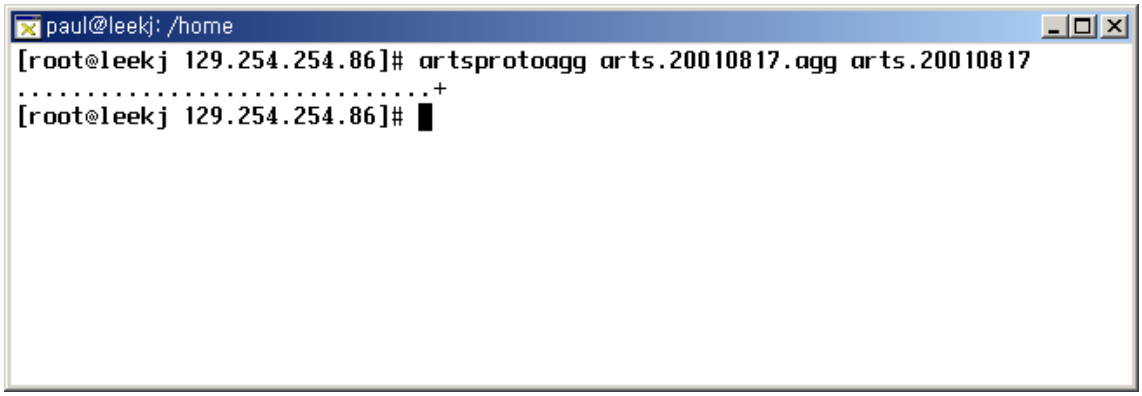

그림 18. ARTS 파일의 Aggregation(통합)

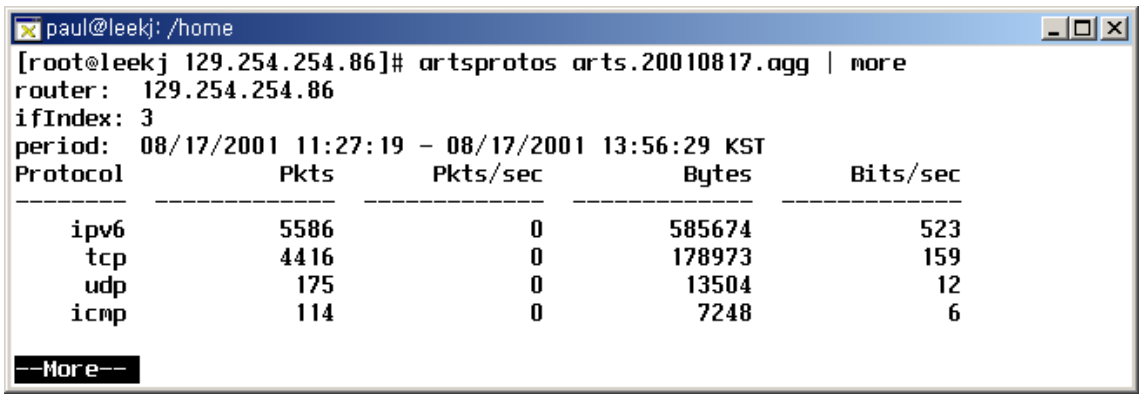

그림 19. 하루 단위의 Protocol별 트래픽 량

참고문헌

[1] 옥도민, “플로우 분류기를 이용한 인터넷 트래픽 측정 및 특성 분석”, 서울대학교 컴퓨터공학 석사논문, 2000년 2월.

[2] R. Jain and S. A. Routhier, “Packet Trains – Measurements and a New Model for Computer Network Traffic”, IEEE JSAC, Sep. 1986

[3] NetFlow, http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps_wp.htm

[4] cflowd, http://www.caida.org/tools/measurement/cflowd/

[5] arts++ Library, http://www.caida.org/tools/utilities/arts/

[6] cflowd configuration, http://www.caida.org/tools/measurement/cflowd/configuration/configuration.html

[7] arts++ Utility, http://www.caida.org/tools/utilities/arts/arts++/artsplusplus-4.html#ss4.2