

[R E P O R T]

정보통신공학전공
200301582
김성태



국립공주대학교

KONGJU NATIONAL UNIVERSITY

과제 7: 가상 네트워크에서 DHCP 구출 및 동작확인

1. 개요

가상 네트워크에서 DHCP 서버를 구축하고 동작을 확인 및 분석한다.

2. 수행할 과제 내용

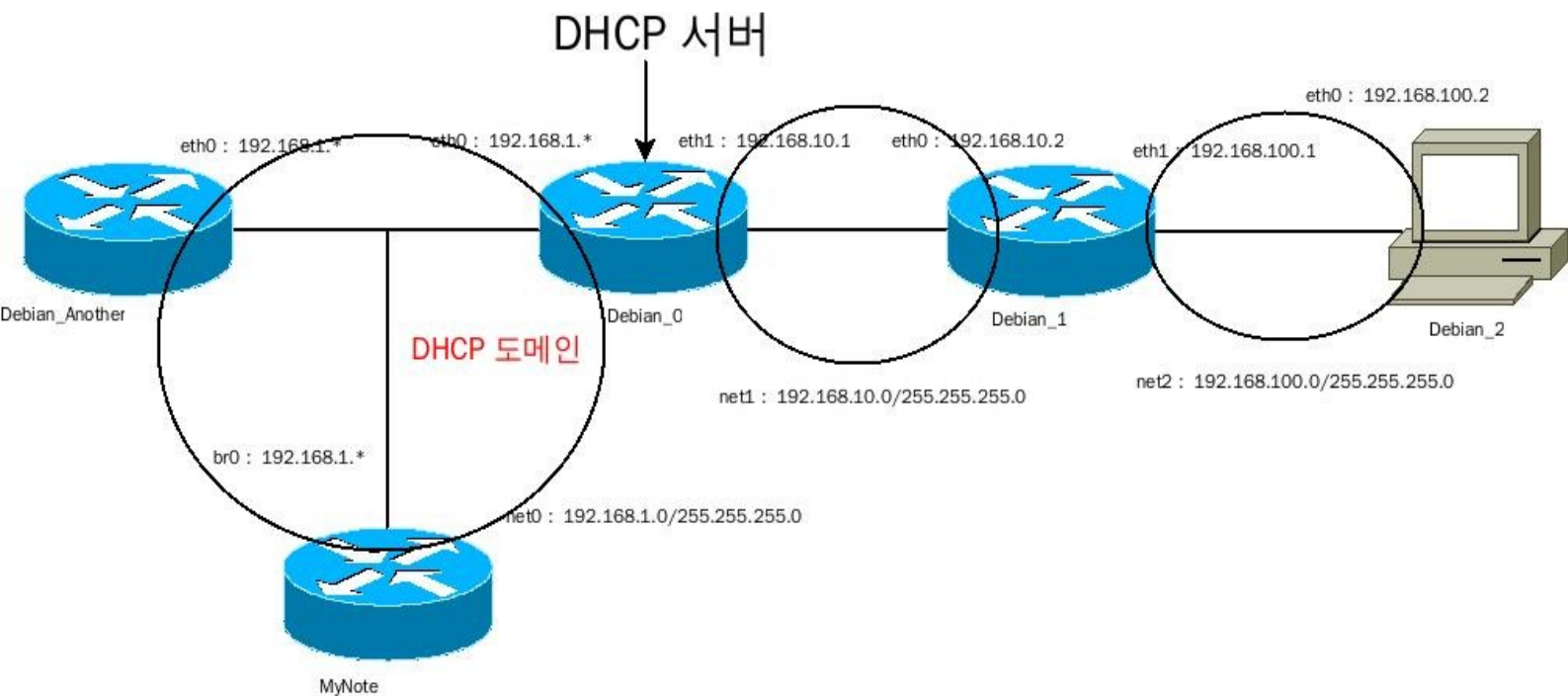
DHCP 서버 구축

주어진 자료를 이용하여 DHCP 서버를 구축

DHCP 동작 확인 및 분석

패킷 캡처 프로그램을 이용하여 DHCP 관련 메시지를 캡처하고, 주소공급 절차와 제공되는 정보, 예로 IP 주소, 게이트웨이 주소, DNS 서버 주소, 도메인 명 등이 어떻게 공급되는지 관찰하면서 전체의 흐름을 분석한다.

3. 네트워크의 구성



4. DHCP 동작 방식

DHCP는 한 네트워크의 모든 IP 주소를 서버에 저장해두고 네트워크내의 노드가 요청할때마다 서버에서 IP 주소를 할당해주는 프로토콜이다.

DHCP를 사용하면 IP 주소 공간을 더 효율적으로 사용할 수 있다. DHCP를 사용해서 클라이언트의 IP 주소와 할당하는 시간을 정하면 클라이언트가 컴(노드)를 사용하지 않을 때는 다른 컴(노드)에 IP 주소를 할당할 수 있다. 즉, 적은 IP 주소를 많은 클라이언트들이 사용한다. 그리고 DHCP를 사용하면 주소 충돌 문제를 원천적으로 막을 수 있다.

동작과정

- 클라이언트 부팅 시 자동으로 DHCP 검색 패킷을 브로드캐스트 한다. 브로드캐스트 패킷의 소스 주소는 0.0.0.0 이고 목적지 주소는 255.255.255.255 이다. 클라이언트는 자신의 MAC 주소를 포함해서 전송한다.
- DHCP 서버는 클라이언트에서 발생된 DHCP 탐색 패킷을 수신하면, 이에 대한 응답으로 DHCP OFFER 패킷을 전송한다. 이 패킷에는 클라이언트의 MAC 주소, DHCP 서버가 관리하는 IP 주소 중 대여할 IP 주소, IP 주소의 서브넷마스크, 대여 기간 등이 포함되어 있다.
- IP 중복을 막기 위해서 클라이언트는 OFFER 메시지 중 가장 처음 도착한 것을 선택하고 이 내용을 다시 브로드캐스트한다.
- DHCP 서버는 DHCP Ack 메시지를 사용해서 클라이언트가 이 IP 주소를 사용하는 것을 허락한다.

5. DHCP 관련 메시지

- DHCP Req

The image shows a Wireshark capture of network traffic. The packet list pane shows several packets, with Frame 57 (DHCP ACK) selected. The packet details pane shows the structure of the selected packet:

- Ethernet II**: Src: Dell_9a:53:74 (00:14:22:9a:53:74), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Address: Broadcast (ff:ff:ff:ff:ff:ff)
 -1 = IG bit: Group address (multicast/broadcast)
 -1. = LG bit: Locally administered address (this is NOT the factory default)
 - Source: Dell_9a:53:74 (00:14:22:9a:53:74)
 - Address: Dell_9a:53:74 (00:14:22:9a:53:74)
 -0 = IG bit: Individual address (unicast)
 -0. = LG bit: Globally unique address (factory default)
 - Type: IP (0x0800)
- Internet Protocol**: Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN: 0x00)

The packet bytes pane shows the raw data of the selected packet, including the Ethernet II header and the IP header.

- DHCP Ack

Filter: + Expression... 바꾸기(C) 적용(A)

No.	Time	Source	Destination	Protocol	Info
54	240.221302	192.168.3.188	224.0.0.22	IGMP	V3 Membership Report / Leave group 224.0.0.251
55	243.369348	192.168.3.188	224.0.0.22	IGMP	V3 Membership Report / Leave group 224.0.0.251
56	244.431745	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xabdbd150
57	244.444074	192.168.1.8	192.168.1.104	DHCP	DHCP ACK - Transaction ID 0xabdbd150
58	244.529310	192.168.1.104	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.251 for any sources
59	244.625376	192.168.1.104	224.0.0.251	MDNS	Standard query PTR _pgkey-hkp._tcp.local, "QM" question
60	244.765436	192.168.1.104	224.0.0.251	MDNS	Standard query ANY 4.7.3.5.a.9.e.f.f.f.2.2.4.1.2.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa, "QM" question ANY MyNote.
61	244.809378	192.168.1.104	224.0.0.251	MDNS	Standard query response PTR _workstation._tcp.local PTR MyNote [fa:db:9b:07:48:46]._workstation._tcp.local
62	245.017426	192.168.1.104	224.0.0.251	MDNS	Standard query ANY 4.7.3.5.a.9.e.f.f.f.2.2.4.1.2.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa, "QM" question ANY MyNote.
63	245.269443	192.168.1.104	224.0.0.251	MDNS	Standard query ANY 4.7.3.5.a.9.e.f.f.f.2.2.4.1.2.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa, "QM" question ANY MyNote.
64	245.469562	192.168.1.104	224.0.0.251	MDNS	Standard query response PTR_cache flush MvNote.local A_cache flush 192.168.1.104 PTR_cache flush MvNote.local HIN

Security: enipsec: 0

Bootp flags: 0x0000 (Unicast)
 0... .. = Broadcast flag: Unicast
 .000 0000 0000 0000 = Reserved flags: 0x0000
 Client IP address: 0.0.0.0 (0.0.0.0)
 Your (client) IP address: 192.168.1.104 (192.168.1.104)
 Next server IP address: 192.168.1.8 (192.168.1.8)
 Relay agent IP address: 0.0.0.0 (0.0.0.0)
 Client MAC address: Dell_9a:53:74 (00:14:22:9a:53:74)
 Server host name not given
 Boot file name not given
 Magic cookie: (OK)
 Option: (t=53,l=1) DHCP Message Type = DHCP ACK
 Option: (53) DHCP Message Type
 Length: 1

0030 d1 50 00 00 00 00 00 00 00 00 00 a8 01 68 c0 a8 .P.....a.l..
 0040 01 08 00 00 00 00 00 14 22 9a 53 74 00 00 00 00".St...
 0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 Your (client) IP address (bootp.ip.your), ... Packets: 75 Displayed: 75 Marked: 0 Profile: Default

- 정상적인 DHCP IP 할당 직후의 모습

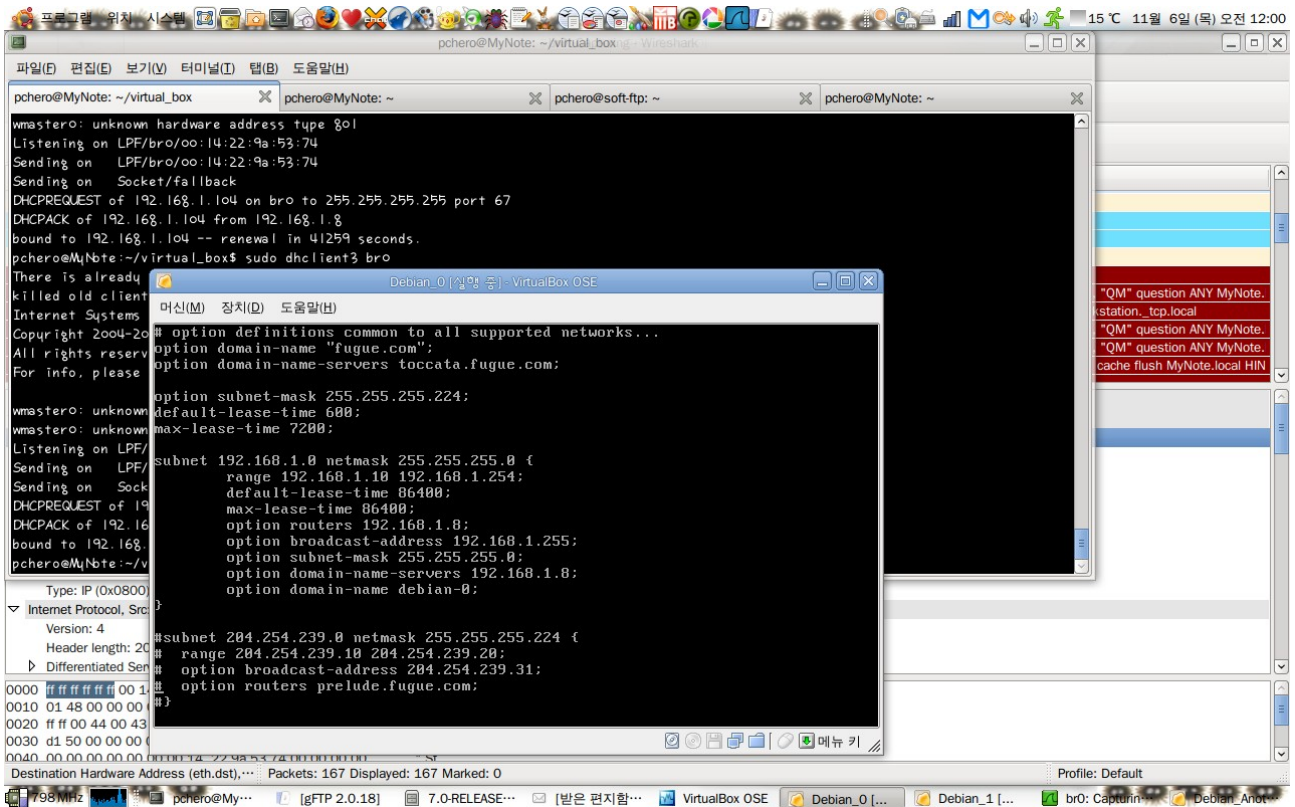
```

pchero@MyNote: ~/virtual_box
pchero@MyNote: ~
pchero@soft-ftp: ~
pchero@MyNote: ~

wmastero: unknown hardware address type 801
Listening on LPF/bro/oo:14:22:9a:53:74
Sending on LPF/bro/oo:14:22:9a:53:74
Sending on Socket/fallback
DHCPREQUEST of 192.168.1.104 on bro to 255.255.255.255 port 67
DHCPACK of 192.168.1.104 from 192.168.1.8
bound to 192.168.1.104 -- renewal in 41259 seconds.
pchero@MyNote:~/virtual_box$ sudo dhclient3 bro
There is already a pid file /var/run/dhclient.pid with pid 11607
killed old client process, removed PID file
Internet Systems Consortium DHCP Client V3.0.6
Copyright 2004-2007 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

wmastero: unknown hardware address type 801
wmastero: unknown hardware address type 801
Listening on LPF/bro/oo:14:22:9a:53:74
Sending on LPF/bro/oo:14:22:9a:53:74
Sending on Socket/fallback
DHCPREQUEST of 192.168.1.104 on bro to 255.255.255.255 port 67
DHCPACK of 192.168.1.104 from 192.168.1.8
bound to 192.168.1.104 -- renewal in 42817 seconds.
pchero@MyNote:~/virtual_box$
  
```

- dhcpd.conf 파일 내용



6. 메시지 분석 결과

- Req 메시지

Source Mac 주소 : Dell_9a:53:74(00:14:22:9a:53:74)

Source IP 주소 : 0.0.0.0

- Ack 메시지

Your (client) IP Address : 192.168.1.104(192.168.1.104)

Next Server IP Address : 192.168.1.8(192.168.1.8)

Server host name not given

- 정상적으로 서로의 Req 메시지와 Ack 메시지를 교환함을 알 수 있었다.