

[R E P O R T]

정보통신공학전공
200301582
김성태



국립공주대학교

KONGJU NATIONAL UNIVERSITY

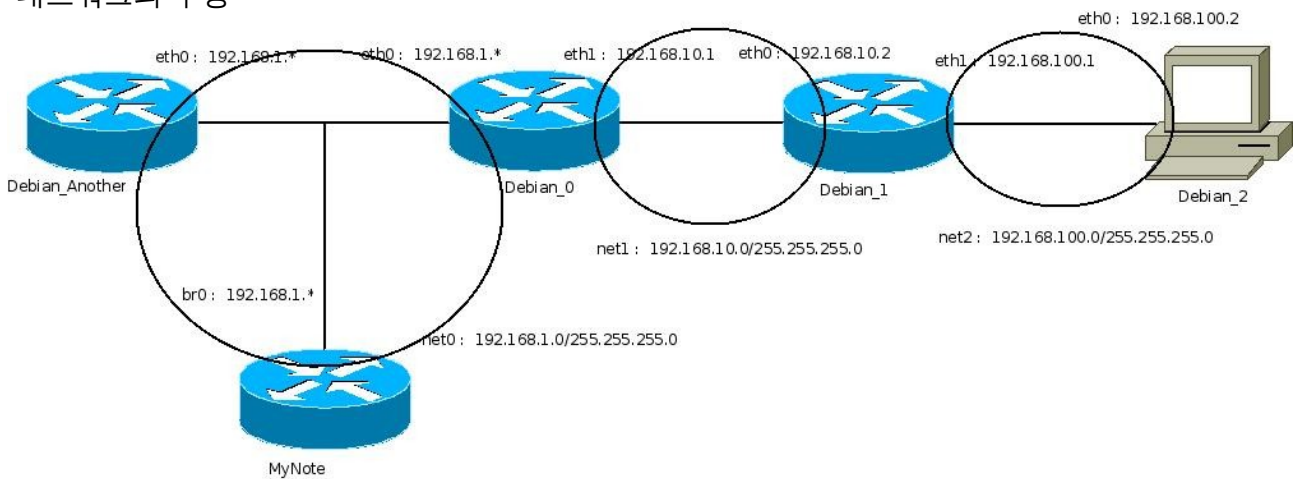
개요 :

4계층으로 구성되는 가상 네트워크에서 DNS 체제를 구축하고 동작을 확인 및 분석한다.

수행할 과제 내용

1. VMWare 내에 5대의 리눅스를 구축한 후, 각 리눅스에 IP 주소를 설정한 후 네임버서, 클라이언트 등의 구체적 역할을 할당한다. 물론 5대의 리눅스는 동적 라우팅 작업을 통해 상호간에 통신이 되어야 한다.
2. Kongju 계층의 이름을 본인의 학번 끝 3자리로 한다.
3. 리눅스 5대를 지원할 만큼 성능이 좋지 않을 경우 ac 계층을 없애도 좋다.

네트워크의 구성



DNS 동작 부분

dig kr

```
파일(F) 편집(E) 보기(V) 터미널(T) 탭(B) 도움말(H)
pchero@MyNote:~$ dig kr
; <<> DiG 9.4.2-P2 <<> kr
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29279
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;kr.                IN      A

;; ANSWER SECTION:
kr.                 10     IN      A      192.168.10.2

;; AUTHORITY SECTION:
kr.                 10     IN      NS     kr.

;; ADDITIONAL SECTION:
kr.                 10     IN      A      192.168.10.2

;; Query time: 32 msec
;; SERVER: 192.168.10.2#53(192.168.10.2)
;; WHEN: Thu Oct 30 04:34:56 2008
;; MSG SIZE rcvd: 66
pchero@MyNote:~$
```

dig ac.kr

```
파일(F) 편집(E) 보기(V) 터미널(T) 탭(B) 도움말(H)
pchero@MyNote: ~
pchero@MyNote: ~/virtual_box
pchero@MyNote:~/virtual_box$ dig ac.kr
; <<> DiG 9.4.2-P2 <<> ac.kr
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11135
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;ac.kr.             IN      A

;; ANSWER SECTION:
ac.kr.              10     IN      A      192.168.100.2

;; AUTHORITY SECTION:
ac.kr.              10     IN      NS     ac.kr.

;; ADDITIONAL SECTION:
ac.kr.              10     IN      A      192.168.100.2

;; Query time: 2 msec
;; SERVER: 192.168.10.2#53(192.168.10.2)
;; WHEN: Thu Oct 30 04:43:25 2008
;; MSG SIZE rcvd: 69
pchero@MyNote:~/virtual_box$
```

dig kongju.ac.kr

```
파일(F) 편집(E) 보기(V) 터미널(T) 탭(B) 도움말(H)
pchero@MyNote: ~
pchero@MyNote: ~/virtual_box
pchero@MyNpte:~/virtual_box$ dig kongju.ac.kr

; <<>> DiG 9.4.2-P2 <<>> kongju.ac.kr
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63467
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;kongju.ac.kr.                IN      A

;; ANSWER SECTION:
kongju.ac.kr.                10      IN      A      192.168.1.101

;; AUTHORITY SECTION:
kongju.ac.kr.                10      IN      NS     kongju.ac.kr.

;; ADDITIONAL SECTION:
kongju.ac.kr.                10      IN      A      192.168.1.101

;; Query time: 35 msec
;; SERVER: 192.168.10.2#53(192.168.10.2)
;; WHEN: Thu Oct 30 04:43:52 2008
;; MSG SIZE rcvd: 88

pchero@MyNpte:~/virtual_box$
```

#dig 200301582.kongju.ac.kr

```
파일(F) 편집(E) 보기(V) 터미널(T) 탭(B) 도움말(H)
pchero@MyNote: ~
pchero@MyNote: ~/virtual_box
pchero@MyNpte:~/virtual_box$ dig 200301582.kongju.ac.kr

; <<>> DiG 9.4.2-P2 <<>> 200301582.kongju.ac.kr
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15722
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;200301582.kongju.ac.kr.      IN      A

;; ANSWER SECTION:
200301582.kongju.ac.kr.      10      IN      A      192.168.1.101

;; AUTHORITY SECTION:
kongju.ac.kr.                10      IN      NS     kongju.ac.kr.

;; ADDITIONAL SECTION:
kongju.ac.kr.                10      IN      A      192.168.1.101

;; Query time: 6 msec
;; SERVER: 192.168.10.2#53(192.168.10.2)
;; WHEN: Thu Oct 30 04:44:35 2008
;; MSG SIZE rcvd: 108

pchero@MyNpte:~/virtual_box$
```

패킷 캡처 부분

dig kr 명령시 패킷 캡처

The screenshot shows a Wireshark packet capture of a DNS response. The packet list pane shows a packet at time 357.914190 from source 192.168.1.104 to destination 192.168.1.104, identified as a DNS Standard query response A for 'kr'. The packet details pane shows the following structure:

- Ethernet II, Src: Dell_9a:53:74 (00:14:22:9a:53:74), Dst: CadmusCo_8f:91:0a (08:00:27:8f:91:0a)
- Internet Protocol, Src: 192.168.1.104 (192.168.1.104), Dst: 192.168.10.2 (192.168.10.2)
- User Datagram Protocol, Src Port: 35831 (35831), Dst Port: domain (53)
- Domain Name System (query)
 - Response In: 259
 - Transaction ID: 0xeb45
 - Flags: 0x0100 (Standard query)
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 08 00 27 8f 91 0a 00 14 22 9a 53 74 08 00 45 00  ..St.E.
0010 00 30 00 00 40 00 40 11 ae 02 c0 a8 01 68 c0 a8  .O.@. ....h..
0020 0a 02 8b f7 00 35 00 1c 86 1a eb 45 01 00 00 01  .....E....
0030 00 00 00 00 00 02 6b 72 00 00 01 00 01  .....k r....
0040 01
```

dig ac.kr 명령시의 패킷

The screenshot shows a Wireshark packet capture of a DNS response for 'ac.kr'. The packet list pane shows a packet at time 382.758979 from source 192.168.1.104 to destination 192.168.1.104, identified as a DNS Standard query response A for 'ac.kr'. The packet details pane shows the following structure:

- Ethernet II, Src: Dell_9a:53:74 (00:14:22:9a:53:74), Dst: CadmusCo_8f:91:0a (08:00:27:8f:91:0a)
- Internet Protocol, Src: 192.168.1.104 (192.168.1.104), Dst: 192.168.10.2 (192.168.10.2)
- User Datagram Protocol, Src Port: 52370 (52370), Dst Port: domain (53)
- Domain Name System (query)
 - Response In: 285
 - Transaction ID: 0x2b7f
 - Flags: 0x0100 (Standard query)
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 08 00 27 8f 91 0a 00 14 22 9a 53 74 08 00 45 00  ..St.E.
0010 00 33 00 00 40 00 40 11 ad ff c0 a8 01 68 c0 a8  .3.@. ....h..
0020 0a 02 cc 92 00 35 00 1f a6 d7 2b 7f 01 00 00 01  .....5. .+....
0030 00 00 00 00 00 02 61 63 02 6b 72 00 00 01 00  .....a c.kr....
0040 01
```

dig kongju.ac.kr 명령시의 패킷 캡처

The image shows a Wireshark packet capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. A filter bar is present with a dropdown menu and buttons for 'Expression...', '비우기(C)', and '적용(A)'. The main display area is divided into three sections: a packet list, a packet details pane, and a packet bytes pane.

No.	Time	Source	Destination	Protocol	Info
315	409.944958	192.168.1.101	192.168.10.2	DNS	Standard query response A 192.168.1.101
312	409.941755	192.168.10.2	192.168.1.101	DNS	Standard query A kongju.ac.kr
300	409.944695	192.168.1.101	192.168.10.2	DNS	Standard query A kongju.ac.kr

The packet details pane for the selected packet (No. 315) shows the following structure:

- [Frame is marked: False]
- [Protocols in frame: eth:ip:udp:dns]
- [Coloring Rule Name: UDP]
- [Coloring Rule String: udp]
- Ethernet II, Src: CadmusCo_8f:91:0a (08:00:27:8f:91:0a), Dst: CadmusCo_fb:dc:1d (08:00:27:fb:dc:1d)
 - Destination: CadmusCo_fb:dc:1d (08:00:27:fb:dc:1d)
 - Source: CadmusCo_8f:91:0a (08:00:27:8f:91:0a)
 - Type: IP (0x0800)
- Internet Protocol, Src: 192.168.10.2 (192.168.10.2), Dst: 192.168.1.101 (192.168.1.101)
- User Datagram Protocol, Src Port: 46380 (46380), Dst Port: domain (53)
 - Source port: 46380 (46380)
 - Destination port: domain (53)
 - Length: 49
 - Checksum: 0x9662 [correct]
- Domain Name System (query)
 - [Response In: 316]
 - Transaction ID: 0xd5e6
 - Flags: 0x0000 (Standard query)
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 1
 - Queries

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 08 00 27 fb dc 1d 08 00 27 8f 91 0a 08 00 45 00  ..?.....E.
0010 00 45 00 00 40 00 3f 11 ae f0 c0 a8 0a 02 c0 a8  .E.@.?.....
0020 01 65 b5 2c 00 35 00 31 96 62 d5 e6 00 00 00 01  .e...5.1.b....
0030 00 00 00 00 00 01 06 6b 6f 6e 67 6a 75 02 61 63  .....k ongju.ac
0040 02 6b 72 00 00 01 00 01 00 00 29 10 00 00 00 00  _kr .....
```

At the bottom, the status bar indicates: br0: <live capture in progress> File: /tm... Packets: 339 Displayed: 339 Marked: 0 Profile: Default