

[ITBANK Andylec 주말 리눅스 2 과정]

■오늘의 수업내용(1일차)

수업 OT

실습환경 구축

리눅스 네트워크

■PC 로그인

-ITBANK 계정으로 로그인

-402호 강의장은 Master(관리자) 계정은 막아 놓았음

※인터넷 되는지 확인하기

■수강동의

온라인 출석부 사이트(<http://mgr.eduitbank.com>)에 로그인 하셔서

수강동의 를 체크해 주시기 바랍니다.

나의정보(오른쪽상단)-출석정보(왼쪽메뉴)-과목명 클릭-수강동의 확인버튼 클릭

■출석확인

■강사 게시판

<http://car2100.ivyro.net/hs1>

사용자 : start

암호 : unix

■수업 준비사항

1. 윈도우 탐색기 실행
2. 2_주말반 폴더 생성후 그 안에 "공용" 폴더 생성(폴더 있으면 생략)
3. 2_주말반 폴더 안에 자신이 사용할 폴더 생성
(폴더 이름은 자신의 이름으로 지정)

예)

D:\2_주말반

D:\2_주말반\공용

D:\2_주말반\홍길동

■자료 다운

탐색기 실행 후 자신의 컴퓨터에서 아래 파일을 찾아보고

없으면 강의장 임시 서버에서

알FTP 이용하여 D:\주말반\공용 폴더에 다운받기

(파일 있으면 다운 생략하고 그 파일을 자신의 폴더로 복사해서 사용하면 됨)

XP_2013.alz

Cent6.4.alz

■수업OT

■First 서버 준비

1. vmware 설치 확인
2. Cent6.4.alz 를 자신의 폴더에 압축풀기
3. vmware 실행하기
4. 리눅스 가상머신을 vmware 에서 불러와서 실행하기
vmware 메뉴 표시줄-File-Open
폴더 이동
Cent6.4.vmx 선택 후 열기 버튼 누르기
start 버튼(> 녹색 화살표 아이콘) 누르기
copy, move 질문 나오면 "I copied it" 선택 후 ok 누르기
5. 부팅후
사용자 : root
암호 : andylec
입력하고 로그인 하기
6. 터미널 실행하기
바탕화면-마우스 오른쪽 버튼-터미널 열기 선택
7. 해상도 변경 : gnome-display-properties

■가상머신 이름 변경하기

vmware 메뉴표시줄-VM-Settings-Options 선택

Virtual Maching Name : First_WeekendPM3

■인터넷을 하기 위한 네트워크 정보(4가지)

1. 아이피 주소(IP Address)
2. 서브넷 마스크(Subnet Mask)

3. 게이트웨이(Gateway)

4. DNS(Domain Name Server) 정보

■보안 설정 확인

방화벽 설정 비활성화

selinux 설정 비활성화

```
#service iptables status
```

```
#sestatus
```

---> 비활성화 확인

---> 리눅스 2 수업은 방화벽과 selinux 를 비활성화 시켜 놓은 상태에서 실습을 해야함

```
////////////////////////////////////
```

방화벽 비활성화 설정 :

```
lokit --disabled
```

selinux 비활성화 설정 :

/etc/sysconfig/selinux 파일에서

SELINUX=disabled 설정 후 리부팅

```
////////////////////////////////////
```

■VMnet8 Switch 의 서브넷 확인

VMWARE 메뉴-Edit-Virtual Network Editor

Name	Subnet Address
------	----------------

VMnet8	192.168.x.0
--------	-------------

--->VMnet8 의 서브넷을 확인후 리눅스 네트워크 설정시

동일한 서브넷으로 설정해야 함

■랜카드 인터페이스명 설정

```
#cd /etc/udev/rules.d
```

```
#vi 70-persistent-net.rules
```

```
:set nu
```

8 번 라인 # 처리

11 번 라인에서 eth1 을 eth0 으로 변경

8 #SUBSYSTEM

11 NAME="eth0"

저장후 종료(esc :wq)

////////////////////////////////////

마지막 라인은 # 으로 시작하면 안 되고 그 위의 라인은 모두

#으로 시작하게 설정

마지막 라인의 NAME 을 eth0 으로 변경

////////////////////////////////////

#reboot

■네트워크 설정 명령어

setup

system-config-network

system-config-network-tui

#system-config-network

장치 설정 선택후 엔터 입력

eth0 선택 후 엔터 입력

이름 : eth0

장치 : eth0

DHCP 사용 : [] ---> 스페이스바를 눌러서 * 표 해제

고정 IP : 192.168.x.10

넷 마스크 : 255.255.255.0

기본 게이트웨이 IP : 192.168.x.2

첫번째 DNS 서버 : 192.168.x.2

두번째 DNS 서버 : 168.126.63.1

OK

저장

종료

■네트워크 시작/중지 스크립트

```
/etc/init.d/network
/etc/rc.d/init.d/network
/etc/init.d/network stop
/etc/init.d/network start
/etc/init.d/network restart
```

```
#service network restart
```

■ifconfig

아이피 확인

(도스창에서는 ipconfig)

```
#ifconfig
```

```
////////////////////////////////////
```

네트워크 설정후 service network restart 로 적용한 다음

ifconfig 로 보았을 때 아이피가 출력 안 되면

아래와 같이 해 본다.

```
#cd /etc/sysconfig/network-scripts
#ls
#vi ifcfg-eth0 또는 gedit ifcfg-eth0
```

```
#HWADDR
```

```
#UUID
```

```
ONBOOT=yes
```

--->HWADDR, UUID 는 주석처리(라인 앞에 # 입력)

--->ONBOOT=no 로 되어 있으면 ONBOOT=yes 로 변경

```
#service network restart
```

```
#ifconfig
```

```
////////////////////////////////////
```

■ping

네트워크 점검 명령어

상대 호스트가 살아 있는지 확인

```
#ping 168.126.63.1
```

64 bytes 로 나오면 정상

ctrl + c 로 중단

```
#ping -c 3 www.yahoo.co.kr
```

(네이버와 다음은 핑을 막아 놓아서 핑테스트 하면 안 됨)

-c 는 count 옵션

-c 3 은 패킷을 3 개 보내는 옵션

안 될경우

/etc/resolv.conf 에

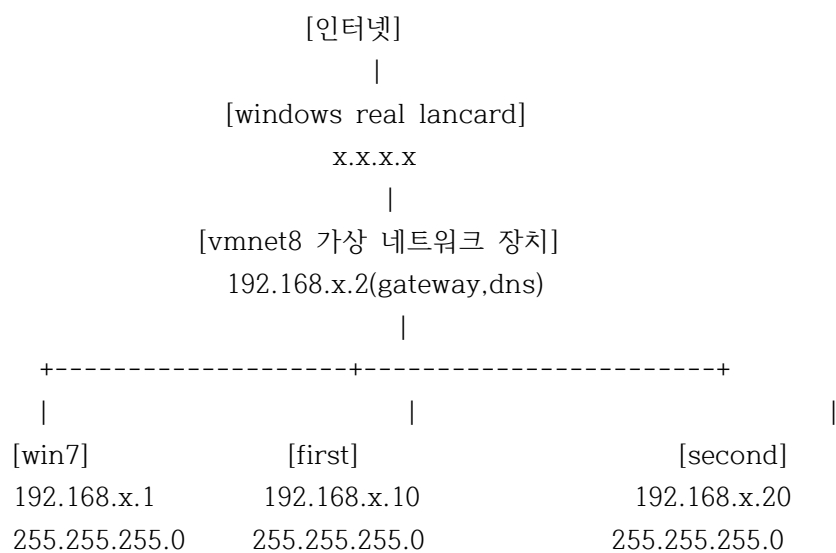
```
nameserver 192.168.x.2
```

또는

```
nameserver 168.126.63.1
```

등록 후 테스트

■실습환경



vmnet8 의 서브넷을 확인후

리눅스 아이피 설정시 동일하게 적어야 한다.

■Second 리눅스 네트워크 설정 실습

1. 자신의 폴더에 Second 폴더 만들고 Cent6.4.alz 를 그 안에 압축풀기
(D:\2_주말반\자신의폴더\Second)
2. vmware 에서 second 리눅스 open(불러오기)한 후 부팅시키기
3. 방화벽 해제, selinux 해제
4. 랜카드 인터페이스명 eth0 설정

////////////////////////////////////

```
#cd /etc/udev/rules.d
```

```
#vi 70-persistent-net.rules
```

마지막 라인만 빼고 모두 # 처리(라인 앞에 # 입력)

마지막 라인의 eth1 을 eth0 으로 변경

마지막 라인만 # 으로 시작하면 안 되고 그 위의 라인은 모두 #으로 시작하게 설정

```
#reboot
```

////////////////////////////////////

5. setup 또는 system-config-network 로 네트워크 정보 입력

아이피 : 192.168.x.20

넷마스크 : 255.255.255.0

게이트웨이 : 192.168.x.2

DNS 1 : 192.168.x.2

DNS 2 : 168.126.63.1

6. service network restart 로 적용

7. ifconfig 로 확인

////////////////////////////////////

아이피 적용이 안 되면

/etc/sysconfig/network-scripts/ifcfg-eth0 파일을 vi 로 연 후

ONBOOT=no 설정이 있으면 ONBOOT=yes 로 변경

HWADDR, UUID 는 # 처리(라인 앞에 # 입력)

```
#HWADDR
```

```
#UUID
```

저장후 종료

service network restart 로 다시 확인

////////////////////////////////////

8. ping 테스트

9. www.yahoo.co.kr 로 핑테스트한 화면을 캡춰하여 실습게시판에 제출

■리눅스(레드햇)의 네트워크 설정파일

1. /etc/sysconfig/network-scripts/ifcfg-*

각 NIC 설정 파일

아이피, 서브넷 마스크, 게이트웨이 등록 파일

파일명 예)ifcfg-eth0, ifcfg-eth1

NIC(Network Interface Card) : 랜카드

컴퓨터에 장착되는 네트워크를 하기위한 부품

LAN(랜) : LocaL Area Network(근거리 통신망)

Ethernet(이더넷) : 보통 UTP 케이블을 이용하며 랜(LAN)에서 사용되는

가장 일반적인 통신 방식

MAC(맥) 주소 : Media Access Control Address

랜카드에 할당되어 있는 고유한 주소

Hardware Address(하드웨어 주소),

Physical Address(물리적 주소) 라고도 한다.

////////////////////////////////////

ifcfg-eth번호 파일의 항목

DEVICE : 네트워크 인터페이스 장치명(eth0, eth1)

HWADDR : 랜카드의 물리적 주소인 MAC(맥) 어드레스(00:0C:29:9D:9F:E3)

ONBOOT : 부팅시 해당 디바이스 활성화 유무(yes | no)

TYPE : 데이터링크 계층의 타입(주로 이더넷 사용)

BOOTPROTO : 프로토콜 지정(none | static | dhcp)

DNS1 : 첫번째 네임서버 지정

DNS2 : 두번째 네임서버 지정

IPADDR : IP 주소 지정(192.168.10.15)

NETMASK : 서브넷 마스크 지정(255.255.255.0)

GATEWAY : 게이트웨이 지정

리눅스 버전, 네트워크 설정 프로그램에 따라서

ifcfg-* 파일에 등록되는 내용이 차이가 남

////////////////////////////////////

2. /etc/resolv.conf

DNS 서버 주소 설정 파일

한국통신 DNS 서버 : 168.126.63.1

DNS(Domain Name Service) : 문자 주소를 아이피로 변환해 주는 서비스

형식)

nameserver 아이피주소

3. /etc/hosts

IP 주소와 컴퓨터 이름(호스트 이름)을 매칭시켜 놓은 파일

형식)

IP주소 호스트네임 별칭

```
#vi /etc/hosts
```

```
127.0.0.1    linux1.andylec.com    localhost    localhost.localdomain    localhost4
localhost4.localdomain4
```

```
:::1            localhost localhost.localdomain localhost6 localhost6.localdomain6
```

```
192.168.x.2    vmgw
```

---> 1번 라인에 linux1.andylec.com 추가

linux1.andylec.com 은 설치할 때 지정한 컴퓨터 이름 임

---> 3번 라인 추가 후 저장 및 종료(192.168.x.2 vmgw)

esc :wq

```
#ping -c3 vmgw
```

4. /etc/sysconfig/network

네트워크 기본 설정 파일

네트워킹, 컴퓨터 이름(호스트 네임) 등록 파일

■ifconfig

아이피 확인, 인터페이스(랜카드) 비활성화 및 활성화 할 때 사용

1. 비활성화(사용안함 설정)

```
ifconfig eth0 down
```

다운 된 인터페이스는 ifconfig 로 출력 안 되고 ifconfig -a 옵션으로 확인

2. 활성화(사용함 설정)

```
ifconfig eth0 up
```

3. ifconfig 를 이용한 아이피 설정(일회성)

```
#ifconfig
```

```
#ifconfig eth0 down
```

---> 랜카드 비활성화

```
#ifconfig
```

```
#ifconfig eth0 up
```

```
#ifconfig eth0 192.168.1.155 netmask 255.255.255.0
```

---> 1회성 아이피 설정

```
#ifconfig
```

```
#ifconfig eth0
```

```
#service network restart
```

[ITBANK Andylec 주말 리눅스 2 과정]

■오늘의 수업내용(2일차)

원격 접속 서비스(Remote Login Service)

■실습준비

수업용 FTP 서버 900.가상머신 폴더에서 win2003.alz 를
D:\2_주말반\공용 폴더에 다운받고 자신의 폴더에 압축풀기
(윈도우 탐색기 실행후 자신의 컴퓨터에 파일이 있으면 다운 생략)

<용어 정리>

☞서버(Server)

- 회사에서 1년 내내 동작시키는 성능 좋은 컴퓨터를 의미하기도 하고
- 수업에서는 운영체제 상에서 특정 역할을 하는 프로그램을 의미한다.
- 서버프로그램이 동작하고 있는 컴퓨터가 서버 컴퓨터이다.
- 컴퓨터를 서버로 사용할 수 있도록 해 주는 운영체제 중의 하나가 리눅스이다.
- ▷웹서버 : 클라이언트에게 홈페이지 서비스를 제공하는 프로그램 또는 컴퓨터
- ▷ftp 서버 : 클라이언트에게 파일전송 서비스(업로드,다운로드)를 제공하는 프로그램 또는 컴퓨터

☞클라이언트(Client)

- 사전적 의미는 고객이지만 수업에서는 서버 컴퓨터를 이용하는 컴퓨터 또는 프로그램을 의미한다.
- 주로 윈도우 7 이 설치된 컴퓨터가 해당되며 윈도우 7 상의 웹브라우저, alftp 도 클라이언트라고 부른다.

☞포트 : 항구라고 비유할 수 있으며 네트워크를 사용하는 서비스 프로그램은 포트를 사용하며 프로그램 마다 포트번호가 틀리다.

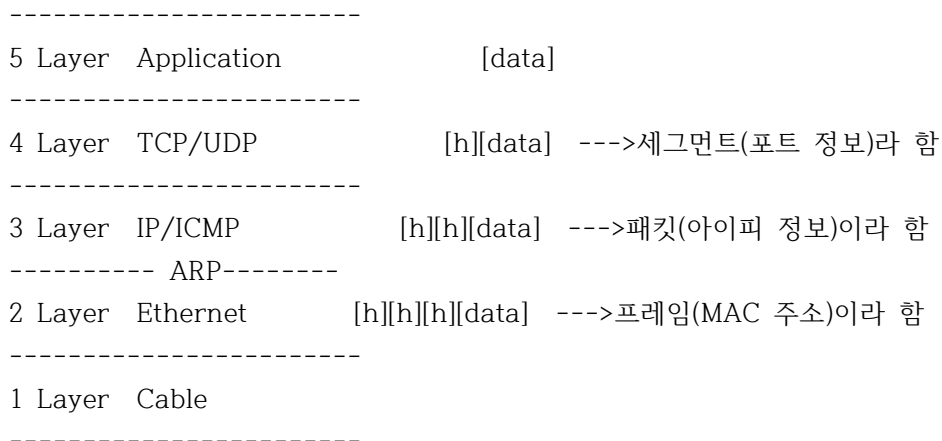
[win7]	[linux]
웹브라우저	-----> 192.168.x.10:80 (아이피:포트)
알FTP	-----> 192.168.x.10:21
Putty	-----> 192.168.x.10:22

☞프로토콜(Protocol)

- 프로토콜은 통신을 하기위한 약속이다.
- 컴퓨터간의 데이터가 전송되기 위해서는 프로토콜이 필요하다.

■TCP/IP 5 Layer Model

인터넷에 구현된 프로토콜 모델

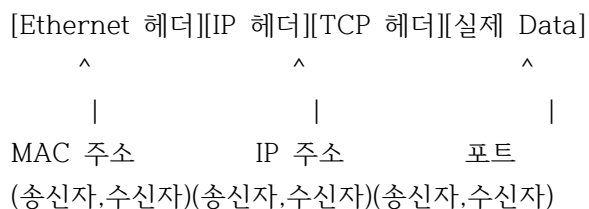


h 는 header(헤더,부가정보) 를 의미

■택배전송

[송장번호][주소][이름][선물]

■이더넷 프레임 전송



--->케이블을 통해 데이터가 전송되는 형식이 위와 같다.

<패킷 캡취 예>

04/07-15:09:24.767704 0:D0:CB:2C:B0:E -> 0:30:67:4:4D:DC type:0x800 len:0x42
192.168.33.1:57407 -> 192.168.33.10:1234 TCP TTL:122 TOS:0x0 ID:16740 IpLen:20
DgmLen:52 DF

*****S* Seq: 0x3A3C7F0B Ack: 0x0 Win: 0x2000 TcpLen: 32
TCP Options (6) => MSS: 1460 NOP WS: 8 NOP NOP SackOK

+++++

04/07-15:09:24.767750 0:30:67:4:4D:DC -> 0:D0:CB:2C:B0:E type:0x800 len:0x42
192.168.33.10:1234 -> 192.168.33.1:57407 TCP TTL:64 TOS:0x0 ID:0 IpLen:20
DgmLen:52 DF

***A**S* Seq: 0x21CE87B9 Ack: 0x3A3C7F0C Win: 0x16D0 TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 7

+++++

04/07-15:09:24.789263 0:D0:CB:2C:B0:E -> 0:30:67:4:4D:DC type:0x800 len:0x3C
192.168.33.1:57407 -> 192.168.33.10:1234 TCP TTL:122 TOS:0x0 ID:16741 IpLen:20
DgmLen:40 DF

A* Seq: 0x3A3C7F0C Ack: 0x21CE87BA Win: 0x100 TcpLen: 20

+++++

04/07-15:09:24.802541 0:30:67:4:4D:DC -> 0:D0:CB:2C:B0:E type:0x800 len:0x5B
192.168.33.10:1234 -> 192.168.33.1:57407 TCP TTL:64 TOS:0x0 ID:30793 IpLen:20
DgmLen:77 DF

AP Seq: 0x21CE87BA Ack: 0x3A3C7F0C Win: 0x2E TcpLen: 20

54 65 73 74 20 2D 2D 2D 20 53 61 74 20 41 70 72 Test --- Sat Apr
20 30 37 20 31 35 3A 30 39 3A 32 34 20 4B 53 54 07 15:09:24 KST
20 32 30 31 32 2012

+++++

04/07-15:09:24.802902 0:30:67:4:4D:DC -> 0:D0:CB:2C:B0:E type:0x800 len:0x44
192.168.33.10:1234 -> 192.168.33.1:57407 TCP TTL:64 TOS:0x0 ID:30794 IpLen:20
DgmLen:54 DF

***AP**F Seq: 0x21CE87DF Ack: 0x3A3C7F0C Win: 0x2E TcpLen: 20

0A 0D 0A 4C 69 6E 75 78 20 54 65 73 74 0A ...Linux Test.

+++++

```
04/07-15:09:24.814600 0:D0:CB:2C:B0:E -> 0:30:67:4:4D:DC type:0x800 len:0x3C
192.168.33.1:57407 -> 192.168.33.10:1234 TCP TTL:122 TOS:0x0 ID:16742 IpLen:20
DgmLen:40 DF
```

```
***A*** Seq: 0x3A3C7F0C Ack: 0x21CE87EE Win: 0x100 TcpLen: 20
```

[illegible]

```
04/07-15:09:24.817553 0:D0:CB:2C:B0:E -> 0:30:67:4:4D:DC type:0x800 len:0x3C
192.168.33.1:57407 -> 192.168.33.10:1234 TCP TTL:122 TOS:0x0 ID:16743 IpLen:20
DgmLen:40 DF
```

```
***A***F Seq: 0x3A3C7F0C  Ack: 0x21CE87EE  Win: 0x100  TcpLen: 20
```

[illegible]

```
04/07-15:09:24.817585 0:30:67:4:4D:DC -> 0:D0:CB:2C:B0:E type:0x800 len:0x36
192.168.33.10:1234 -> 192.168.33.1:57407 TCP TTL:64 TOS:0x0 ID:0 IpLen:20
DgmLen:40 DF
```

```
***A**** Seq: 0x21CE87EE  Ack: 0x3A3C7F0D  Win: 0x2E  TcpLen: 20
```

=+++++

```
netstat(network status)
```

라우팅 테이블 및 네트워크 연결 상태, 열린 포트를 확인하는 명령어

사용 옵션)

-n : 10진수의 수치정보로 결과 출력(number, numeric)

-r : 라우팅 정보를 출력

-t : tcp 프로토콜의 정보출력

- u : udp 프로토콜의 정보출력

-1 : 현재 listen 되고 있는 소켓정보 출력

-p : 프로세스 정보출력

-a : all

-s : 통계

👉 사 용 예

```
#netstat -ntlp
```

```
#netstat -nulp
```

```
#netstat -atn
```

```
#netstat -r
#netstat -rn
#netstat -s
```

//

<http://linux.die.net/man/8/netstat>

Output

Active Internet connections (TCP, UDP, raw)

Proto

The protocol (tcp, udp, raw) used by the socket.

Recv-Q

The count of bytes not copied by the user program connected to this socket.

Send-Q

The count of bytes not acknowledged by the remote host.

Local Address

Address and port number of the local end of the socket. Unless the --numeric (-n) option is specified, the socket address is resolved to its canonical host name (FQDN), and the port number is translated into the corresponding service name.

Foreign Address

Address and port number of the remote end of the socket. Analogous to "Local Address."

State

The state of the socket. Since there are no states in raw mode and usually no states used in UDP, this column may be left blank. Normally this can be one of several values:

ESTABLISHED

The socket has an established connection.

//

■데몬

1. 메모리에 계속 상주하면서 특정 역할을 하는 프로그램(서비스, 서버 프로그램)

2. 서버 컴퓨터에는 클라이언트가 요청한 서비스를 제공하기 위해 서비스 프로세스(데몬)가 동작

3. 데몬은 메모리를 할당받아 사용되므로 효율적 관리가 필요

4. 데몬의 동작방식(서비스의 요청 빈도에 따라 구분)

1) standalone type(독립 방식)

서비스 프로그램인 데몬이 메모리에 계속 상주하는 방식

2) xinetd type(수퍼서버 방식)

매니저 프로그램인 xinetd(수퍼 서버라고도 함)만 실행되어 있고 서비스 프로그램은 필요할 때 로딩하는 방식

<xinetd>

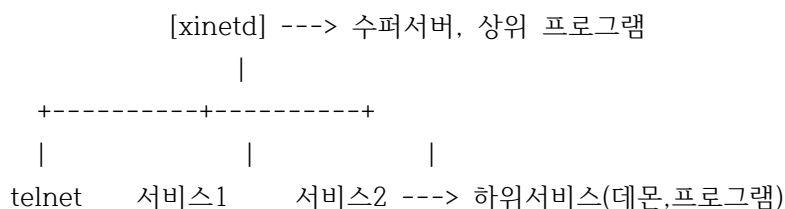
수퍼서버 방식

평상시에는 xinetd 프로그램만 실행되어서

포트를 관리하다가 클라이언트의 요청이 있으면

특정 포트에 해당하는 프로그램을 메모리로 로딩해서 서비스하고

서비스 종료후 메모리에서 프로그램을 언로딩하는 방식



[first]

패키지)

xinetd

---> 수퍼서버 프로그램

telnet

---> telnet 클라이언트 프로그램

telnet-server

---> telnet 서버 프로그램


```
#rpm -qa | grep xinetd
#rpm -qa | grep telnet
```

패키지가 없을 경우 yum 으로 설치하기

```
#yum -y install xinetd telnet-server telnet
```

■xinetd 서비스 설정파일 형식

xinetd 주설정 파일 : /etc/xinetd.conf

--->하위 서비스에 공통적으로 적용되는 설정파일

defaults

{

log_type = SYSLOG daemon info

로깅 설정

log_on_failure = HOST

로그인 실패시 로그에 호스트이름 기록

log_on_success = PID HOST DURATION EXIT

로그인 성공시 로그에 프로세스 번호, 호스트 이름 등을 기록

cps = 50 10

초당 접속 제한수를 50 으로 하고 넘으면 10초 기다렸다가 다시 구동

instances = 50

데몬의 최대갯수

}

includedir /etc/xinetd.d

하위 서비스 설정파일 디렉토리

■xinetd 하위 서비스 설정파일 위치 : /etc/xinetd.d/

형식

service 서비스이름

{

속성 = 값

}

☞서비스 이름은 /etc/services 파일에 등록된 서비스이름을 사용해야 한다.

☞서비스에 따라 설정 파일에서 대소문자를 구분하는 경우도 있고 안 하는 경우도 있으므로 미리 적혀있는 샘플대로 설정하면 된다.

■속성 설명

flags

소켓같은 자원을 재사용하는 설정

socket_type

stream : tcp 기반의 서비스

dgram : udp 기반의 서비스

wait

단일 쓰레드, 멀티쓰레드에 대한 설정

tcp 서비스는 반드시 no 로 설정되어야 정상 서비스 된다.

udp 서비스는 yes 로 설정

no : 접속시 프로세스를 생성하여 처리한다.(대기시간이 없다)

yes : 1 개의 프로세스를 이용한다.(대기시간이 필요하다)

user

프로세스를 실행할 수 있는 사용자를 지정

server

xinetd 수퍼서버가 실행할 실제 서비스 프로그램 경로 및 이름

log_on_failure

로그에 남기는 설정

disable

telnet 서비스를 활성화 하려면 no 로 설정

////////////////////////////////////

#man xinetd

NAME

xinetd - the extended Internet services daemon

xinetd starts the appropriate server.

Because of the way it operates, xinetd (as well as inetd) is also referred to as a super-server.

☞telnet 패키지명

CentOS 5 버전

krb5-workstation

/etc/xinetd.d/krb5-telnet

CentOS 6 버전

telnet-server

/etc/xinetd.d/telnet

////////////////////////////////////

<telnet 서비스>

원격지에서 리눅스 머신으로 로그인하여 명령어 작업을 할 수 있도록 해 주는 서비스

동작 방식 : xinetd 방식(수퍼 서버 방식)

telnet 설정파일 : /etc/xinetd.d/telnet

데몬 파일 : /usr/sbin/in.telnetd

서비스 시작 : service xinetd start 또는 /etc/init.d/xinetd start

서비스 종료 : service xinetd stop 또는 /etc/init.d/xinetd stop

서비스 재시작 : service xinetd restart 또는 /etc/init.d/xinetd restart

서비스 상태 : service xinetd status 또는 /etc/init.d/xinetd status

☞telnet 서버 접속 방법

1)윈도즈에서는 Putty, Secure CRT 사용 또는 telnet 명령 사용

2)리눅스 터미널에서는 telnet 명령 사용

형식)

telnet [아이피 또는 문자주소] 포트

[first]

```
#netstat -ntlp | grep 23
```

telnet 서비스 포트 : 23

```
#cd /etc/xinetd.d
```

```
#vi telnet
```

```
disable = no
```

로 변경

```
#service xinetd status
```

```
#service xinetd restart
```

```
#service xinetd status
```

```
#netstat -ntlp | grep 23
```

```
#ps -ef | grep telnet
```

---> 수퍼 서버 방식이므로 검색 안 됨

```
#passwd apple
```

1234

1234

---> 테스트 계정 암호 설정

[second]

```
#yum -y install telnet
```

---> 텔넷 클라이언트 프로그램 설치

```
////////////////////////////////////
```

yum 사용시 lock 메시지가 출력되면

```
#rm /var/run/yum.pid 한 후 다시 실행해 본다.
```

```
////////////////////////////////////
```

#telnet 첫번째리눅스아이피

접속 중단은 ctrl +]

telnet>quit 입력

apple login

\$who

접속 종료는 exit 입력

☞Putty 사용하기

☞telnet 루트 로그인 허용(권장 안함)

[first]

#cd /etc/pam.d

#vi remote

2번 라인 주석처리

#auth required pam_securetty.so

---> 서버 설정 파일이 아니므로 service ~ restart 를 하지 않는다.

[second]

테스트

#telnet 첫번째리눅스아이피

root login test

■실습

1. Second 리눅스에서 Telnet 서버 구축하기
2. First 리눅스에서 Second 리눅스로 Telnet 서비스 이용하여 apple 계정으로 로그인하기
3. \$who 실행한 화면을 캡처하여 실습게시판에 제출

////////////////////////////////////

Telnet 응용 항목(/etc/xinetd.d/telnet 파일에 설정)

only_from : 접속을 허용할 곳 지정

no_access : 접속을 허용하지 않을 호스트나 네트워크 지정

access_times : 접근 가능 시간 지정(시간은 0~23, 분은 0~59)

banner : 접속시 표시 될 파일 지정

예))

```
only_from = 192.168.10.20
```

```
access_times = 0:00-23:59
```

```
////////////////////////////////////
```

```
////////////////////////////////////
```

[second]

```
#yum -y install xinetd telnet-server
```

```
#cd /etc/xinetd.d
```

```
#vi telnet
```

```
disable = no 로 변경
```

```
#service xinetd restart
```

```
#netstat -ntlp | grep 23
```

```
#passwd apple
```

```
1234
```

```
1234
```

[first]

```
#telnet 아이피
```

배너(접속시 메시지) 출력

접속 시간 제한(PM 3시 ~ PM 8시 까지만 접속 허용)

[second]

```
#cd /etc/xinetd.d
```

```
#vi telnet
```

```
service telnet
```

```
{
```

```
    기존 설정 그대로 두고 아래 내용 추가
```

```
    access_times = 시간:분-시간:분
```

```
    banner = /work/telnet.txt
```

```
}  
#mkdir /work  
#vi /work/telnet.txt
```

Second Telnet Server

```
#service xinetd restart
```

```
////////////////////////////////////
```

▣원격 접속 서비스(Remote Service)

1. TELNET

포트 : 23, 비암호화, 텍스트 방식

2. SSH

포트 : 22, 암호화, 텍스트 방식

3. VNC

그래픽(GUI 환경) 환경

▣암호화 방식

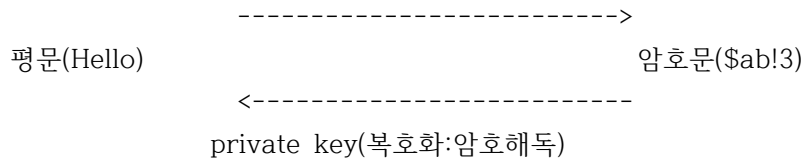
대칭키 방식과 비대칭키 방식이 있다.

1. 대칭키 방식 : 암호화 할 때와 복호화(암호해독) 할 때의 키가 똑같은 방식

```
                key1(암호화)  
                ----->  
평문(안녕)                                암호문(@#%^&*)  
                <-----  
                key2(해독)  
key1 = key2
```

2. 비대칭키 방식(OpenSSH 가 사용하는 방식)

public key(암호화)



public key 와 private key 는 동일하지 않다.

공개키 : public key

개인키(비밀키,사설키) : private key, secret key

평문 : Hello 와 같이 암호화 이전의 데이터

암호문 : \$ab!3 과 같이 변환된 데이터(암호화는 수신자의 공개키로 한다.)

참조)

http://ko.wikipedia.org/wiki/RSA_%EC%95%94%ED%98%B8

■SSH(Secure SHell)

암호화 통신을 하는 리모트 로그인 서비스

1. 패키지명 : openssh

#rpm -qa | grep openssh

패키지가 없으면 설치 : #yum -y install openssh

2. 디렉토리 : /etc/ssh

3. 서버 설정 파일 : sshd_config

4. 클라이언트 설정 파일 : ssh_config

5. 데몬 스크립트 : /etc/init.d/sshd

데몬 스크립트 : 서비스 프로그램을 시작 및 종료 시키는 역할을 하는 파일

<sshd_config 파일 항목>

#으로 시작하는 라인은 주석(설명) 또는 디폴트값을 뜻한다.

버전에 따라 라인 번호는 틀려질 수 있으므로 내용을 확인한다.

13 #Port 22

ssh 포트

15 #ListenAddress 0.0.0.0

서비스에 사용할 주소 설정

21 Protocol 2

ssh 버전 설정

25 # HostKeys

암호화에 사용되는 키파일 위치 지정

30 #KeyRegenerationInterval

동일한 키를 오랫동안 사용하지 않도록 하기 위한 서버의 키 재생성시간 설정

31 #ServerKeyBits

서버 키의 비트 수를 정의

36 SyslogFacility

로깅 facility(로그 기록 방식)

AUTHPRIV : 인증 절차에 관련된 메시지

37 #LogLevel

로깅 레벨(로그 기록 수준)

emerg : 시스템이 다운되는 수준

crit : 서브시스템을 종료해야 하는 수준

warning : 경고 메시지 수준

info : 정보를 제공하는 수준

41 #LoginGraceTime 2m

로그인 허용 대기시간-디폴트로 2분

10 으로 적으면 10초

42 #PermitRootLogin yes

루트 로그인 허용 설정

43 #StrictModes

로그인 전에 파일모드, 홈디렉토리 소유권 등을 체크하는 설정

44 #MaxAuthTries 6

로그인 실패시 재시도 허용 횟수

48 #PubkeyAuthentication yes

공개키 인증 허용 여부

49 #AuthorizedKeysFile .ssh/authorized_keys

공개키 인증 사용시 공개키가 저장되어 있는 파일

64 #PasswordAuthentication

패스워드 인증 설정

65 #PermitEmptyPasswords

패스워드 인증을 할 때 빈 패스워드 사용 설정

112 #PrintMotd

로그인 시에 /etc/motd 를 출력

129 #Banner none

접속시 보여줄 메시지 파일

<ssh 서비스 관리>

telnet 은 xinetd 이용

#ls /etc/init.d

/etc/init.d/sshd [start|stop|restart]

start //프로그램 시작

stop //프로그램 종료

restart //재시작, 종료후 시작

reload //설정파일을 다시 읽기

condrestart //프로그램이 실행중인 경우에만 재시작

status //프로그램 실행 여부 확인

1. 중지

```
service sshd stop  
/etc/init.d/sshd stop
```

2. 시작

```
service sshd start  
/etc/init.d/sshd start
```

3. 상태확인

```
service sshd status  
/etc/init.d/sshd status
```

<ssh 클라이언트 명령어>

윈도우에서는 Putty, CRT 같은 프로그램을 사용할 수 있고
리눅스 터미널에서는 ssh 명령어를 이용할 수 있다.

1. ssh 192.168.x.10
현재 로그인한 계정으로 접속

2. ssh cent.andylec.com
현재 로그인한 계정으로 접속

3. ssh apple@192.168.x.10
apple 계정으로 접속

4. ssh -l apple 192.168.x.10
apple 계정으로 접속

<ssh 서버 테스트>

[first]

```
#netstat -ntlp | grep sshd  
#netstat -ntlp | grep 22
```

```
#cd /etc/ssh  
#vi sshd_config  
:set nu
```

```
130 Banner /work/ssh.banner
```

```
#mkdir /work
```

```
#vi /work/ssh.banner
```

First SSH Server

```
#service sshd restart
```

리눅스 서비스의 경우 설정 파일이 변경되면
서비스를 재시작 해 주어야 한다.

[second]

```
#ssh 첫번째리눅스아이피
```

질문에 yes 입력

루트 암호 입력

접속 종료는 exit 입력

```
#ssh apple@첫번째리눅스아이피
```

apple 암호 입력

접속 종료는 exit 입력

☞루트 로그인 제한

[first]

```
#cd /etc/ssh
```

```
#vi sshd_config
```

```
42 PermitRootLogin no
```

---> 라인 앞의 # 을 없애고 yes 를 no 로 수정

```
#service sshd restart
```

```
#netstat -ntlp | grep sshd
```

```
#ps -ef | grep sshd
```

[second]

```
#ssh 첫번째리눅스아이피
```

결과 확인 후 Root Login Allow 설정하기

☞배너(Banner)

1. 로그인 전 배너

1)시스템 배너

/etc/issue : 로컬 로그인 배너

/etc/issue.net : 네트워크 로그인 배너(Telnet 사용, SSH 사용 안 함)

2)서비스 자체 배너

Telnet : /etc/xinetd/telnet 파일에 설정

SSH : /etc/ssh/sshd_config 파일에 설정

2. 로그인 후 배너

/etc/motd

---> Telnet, SSH 둘다 사용

[first]

#cat /etc/issue

#cat /etc/issue.net

#mkdir /backup

#cp /etc/iss* /backup

#vi /etc/issue

Local Login Banner

#vi /etc/issue.net

Remote Login Banner

#vi /etc/motd

Hello User !

Enjoy Linux

[ITBANK Andylec 주말 리눅스 2 과정]

■오늘의 수업내용(3일차)

VNC

DHCP

■실습준비

수업용 FTP 서버 900.가상머신 폴더에서 Win2008.alz 를
D:\2_주말반\공용 폴더에 다운받고 자신의 폴더에 압축풀기
(윈도우 탐색기 실행후 자신의 컴퓨터에 파일이 있으면 다운 생략)

■VNC 서비스

VNC

-Virtual Network Computing

-그래픽(GUI) 리모트 로그인(Remote) 환경을 제공하는 서비스이다.

-일반 계정은 하나의 연결만 가능

☞필요한 패키지

vnc-server : 서버 프로그램

vnc : 클라이언트 프로그램(vnc 서버를 이용하는 프로그램, 리눅스용)

☞서비스 관리

/etc/init.d/vncserver start|stop|restart

service vncserver start|stop|restart

☞서버 설정

[first]

#rpm -qa | grep vnc

vnc-server 설치되어 있는지 확인

패키지 없으면 yum 으로 설치

#yum -y install tigervnc-server

[first]

#cd /etc/sysconfig

```
#ls
```

```
#vi vncservers
```

마지막에 추가

```
VNCSERVERS="1:root"
```

---> VNCSERVERS 는 대문자로 설정

---> 라인이 # 으로 시작하면 안 됨

```
////////////////////////////////////
```

"1:root" 에서 1은 디스플레이 번호이고 일반적으로 1 을

사용한다.

root 는 로그인 할 때 사용할 계정을 의미한다.

"2:root" 로 설정하면 클라이언트에서 접속할 때 번호를 2로

지정해야 한다.

여러 계정을 사용하려면

```
VNCSERVERS="1:apple 2:orange 3:mango"
```

위와 같이 등록하면 된다.

/etc/sysconfig/vncservers 파일에 등록하는 계정은

adduser 또는 useradd 로 미리 계정을 추가해 주어야 한다.

```
////////////////////////////////////
```

```
////////////////////////////////////
```

/etc/sysconfig/vncservers 를 수정한 후에는

```
#su - 계정명
```

형식으로 vncservers 파일에 등록한 계정으로 전환후

vncpasswd 명령어를 이용하여 암호 설정을 해 주어야 한다.

그러면 계정 홈디렉토리 안에 .vnc 디렉토리가 생기고

암호 파일이 생성된다.

```
////////////////////////////////////
```

```
#vncpasswd
```

---> 루트 계정이므로 su - 를 할 필요가 없음

---> vnc 서비스로 로그인 할 때 사용할 암호 지정(6자 이상 입력)

```
#cd /root/.vnc
```

passwd (암호가 저장된 파일이 생성된다.)

```
#ls
```

```
#cat passwd
```

인코딩(암호화)되서 실제 패스워드는 알 수 없다.

```
#service vncserver start
```

서비스가 시작되면서 /root/.vnc 안에 로그파일과 xstartup 파일 등 이 생성된다.

(vnc 포트 확인)

```
#netstat -ntlp | grep vnc
```

☞클라이언트 설정

[win2003]

administrator 암호는 andy

2003 에서 웹브라우저 실행하고 아래 사이트 접속

<http://www.tightvnc.com>

TightVNC is a free remote control software package. With TightVNC, you can see the desktop of a remote machine and control it with your local mouse and keyboard, just like you would do it sitting in the front of that computer.

왼쪽 메뉴에서 Download Now 클릭

TightVNC:

Home

Download (v1.3) ---> 클릭

Self-installing package for Windows

---> 클릭해서 다운받기

<tightvnc 설치>

1. tightvnc-x.x.x-setup.exe 실행
2. welcome 화면-next 클릭
3. Information-next 클릭
4. 설치경로-next 클릭(디폴트값 사용)
5. 구성요소(Select Components)

- []TightVNC Server 체크 해제
- [v]TightVNC Viewer 체크
- [v]Web pages and documentation
- 6. 메뉴폴더-next 클릭(디폴트값 사용)
- 7. Select Additional Tasks
 - 디폴트값 그대로 사용-Next 클릭
- 8. Next 클릭
- 9. Install 클릭
- 10. Finish 클릭

시작메뉴에서 "프로그램-TightVNC" 를 찾아간 후
TightVNC Viewer 를 실행시킨다.

VNC sever : [첫번째리눅스아이피:1]

리눅스 머신의 아이피만 적으면 접속이 안 됨
아이피:1 을 입력하고 Connect 버튼을 누른다.
암호를 입력하면 로그인 할 수 있다.

```
[second]
#rpm -qa | grep vnc
#yum -y install tigervnc
---> vnc 클라이언트 프로그램 설치
```

리눅스에서 다른 vncserver 로 접속할 때는
vncviewer 를 입력하면 된다.

#vncviewer 또는 #vncviewer 아이피:디스플레이번호

[첫번째리눅스아이피:디스플레이번호] 입력
[암호] 입력후 엔터 누르기

■TSClient

```
[first]
#yum -y install tsclient
```

```
#tsclient
```

■ftp 명령어

- FTP(File Transfer Protocol, 파일 전송 서비스) 클라이언트 프로그램
- 디렉토리는 다운 받을 수 없고
- 동일한 파일을 다시 받으면 덮어쓰기 된다.
- 한글지원 안 됨

[second]

```
#yum -y install ftp
#ftp
ftp>help
ftp>help get
ftp>help mget
ftp>help put
ftp>help mput
ftp>by
```

```
////////////////////////////////////
ftp>help(도움말)
ftp>get(1개 파일 다운)
ftp>mget(여러개 파일 다운)
ftp>put(1개 파일 업로드)
ftp>mput(여러개 파일 업로드)
ftp>ls(서버쪽 목록 출력)
ftp>!ls(자신의 컴퓨터 목록 출력)
!명령어 : 자신의 컴퓨터에서 명령이 실행됨
ftp>cd(서버쪽 디렉토리 이동)
ftp>lcd(자신의 컴퓨터 디렉토리 이동)
ftp>by(접속 종료) 또는 bye 또는 quit
////////////////////////////////////
```

☞ftp 명령어 테스트

[second]

#ftp FTP서버아이피
Name : 사용자 아이디 입력
Password : 암호 입력, 입력시 안 보임

////////////////////////////////////
로그인 실패시에는 아래와 같이 하면 된다.

ftp>by
#ftp FTP서버아이피

////////////////////////////////////

ftp>pwd
---> 서버쪽 경로
ftp>!pwd
---> 자신의 컴퓨터 경로(로컬 경로)

ftp>ls (서버쪽 목록 출력)
ftp>!ls (자신의 컴퓨터 목록 출력)

ftp>cd /100.UPLOAD (서버쪽 디렉토리 이동)
ftp>pwd (서버쪽 경로 확인)
ftp>lcd /tmp (자신의 컴퓨터 디렉토리 이동)
ftp>!pwd (자신의 컴퓨터 경로 확인)

ftp>cd /120.UPLOAD2
ftp>ls
ftp>ls *.rpm
ftp>mget open* gftp*(서버쪽 파일 다운로드, 질문에 엔터 입력)
ftp>by
#ls /tmp

////////////////////////////////////
[FTP 서버] [FTP 클라이언트]
pwd !pwd
cd lcd (영문 엘)
ls !ls

다운로드)

```
ftp>get a.txt
ftp>mget *.txt
```

업로드)

```
ftp>put b.txt
ftp>mput *.txt
```

////////////////////////////////////

■실습

- second 리눅스에서 VNC 서버 구축
- 계정은 root, apple 지정
- win2003 에서 apple 계정 이용하여 second 리눅스 vnc 서버에 접속한 화면을 캡춰한 후 실습게시판에 제출

■실습

1. /down 폴더 생성, /upload 폴더 생성 및 이동
2. 자신의 영문이니셜 또는 닉네임을 이용한 파일을 /upload 폴더에 생성 (이름이 홍길동이면 hkd.txt 로 만들면 됨)
3. ftp 명령 이용하여 수업용 FTP 서버에 접속후 /100.UPLOAD 폴더에 자신의 파일을 업로드
4. 수업용 FTP 서버 120.UPLOAD2 폴더에서 확장자가 html 인 파일을 /down 폴더에 다운받기

```
[리눅스가상머신]----->[FTP Server]
/upload
/down
```

■DHCP(Dynamic Host Configuration Protocol)

Dynamic Host Configuration Protocol 을 의미하며 같은 네트워크 상의 클라이언트 컴퓨터에게 IP 를 자동으로 할당해주는 서비스이다.

클라이언트 컴퓨터는 부팅시에 IP, Subnet Mask, Gateway, DNS 정보를 DHCP 서버에 요청하고 DHCP 서버는 이 요청에 응답을 해서 아이피 할당이 처리된다.

DHCP 를 사용하면 사용자는 아이피 충돌로 인하여 관리자에게 아이피를 문의해야 하는 일이 없어진다.

네트워크 관리자가 조직내의 IP 주소를 중앙에서 관리하고 할당해 줄 수 있도록 해주는

프로토콜이므로 관리자 입장에서는 아이피 주소관리의 부담
(아이피 충돌 문제, 네트워크 정보 변경 문제)이 줄어든다.

DHCP 를 사용하지 않을 경우에는 각 컴퓨터마다 IP 주소를 수동으로 입력해 주어야 한다.

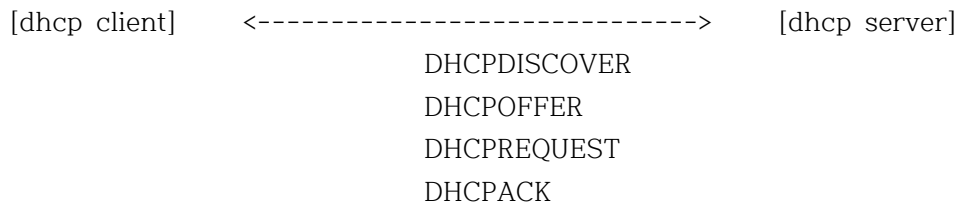
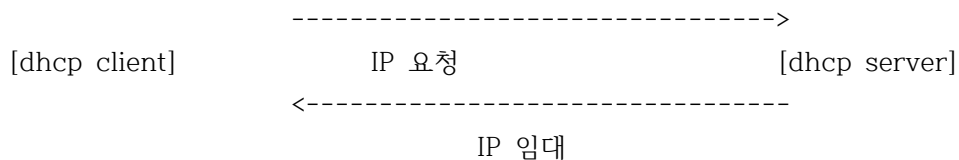
기본적으로 DHCP 서버는 DHCP 클라이언트와 같은 네트워크에 있어야 한다.
클라이언트가 아이피가 없기 때문이다.

☞BOOTP(Bootstrap Protocol)

초기에 사용되던 통신 규약

DHCP 의 기반이 됨

☞DHCP 동작 과정



1)1 단계 : IP Lease Request

메시지 - DHCPDISCOVER

클라이언트는 DHCP 서버를 모르기 때문에

출발지 주소는 0.0.0.0 , 목적지 주소는 255.255.255.255(브로드캐스트) 형태로 보내고

여기에는 클라이언트의

MAC Address(하드웨어 주소)도 포함되어 있다.

2)2 단계 : IP Lease Offer

메시지 - DHCPOFFER

DHCP 서버는 클라이언트에게 사용가능한 아이피 정보등을 브로드 캐스트로 보내
사용 제안을 한다.

DHCPOFFER 메시지 내용 :

클라이언트의 MAC 주소

제안하는 IP

임대기간

서버아이피

3)3 단계 : IP Lease 선택

메시지 - DHCPREQUEST

클라이언트는 DHCP 로 부터 제안받은 아이피 주소를 선택하고
임대 요청을 브로드캐스트로 보낸다.

4)4 단계 : IP Lease 응답

메시지 - DHCPACK

DHCP 서버는 클라이언트 메시지에 긍정 응답을 하고
클라이언트에게 아이피를 할당한다.

<참고>

tcpdump 명령어를 이용한 패킷 캡취 결과)

reading from file /work/dhcp.txt, link-type EN10MB (Ethernet)

07:50:11.753934 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from 00:0c:29:bc:c0:f9,

length: 300

---> 컴퓨터가 DHCP 서버를 찾는 패킷

07:50:12.002536 IP 192.168.x.25.bootps > 192.168.x.233.bootpc: BOOTP/DHCP, Reply,

length: 300

---> 서버가 아이피를 제안하는 패킷

07:50:12.010524 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 00:0c:29:bc:c0:f9,

length: 300

---> 컴퓨터가 아이피 사용 요청하는 패킷

07:50:12.024001 IP 192.168.x.25.bootps > 192.168.x.233.bootpc: BOOTP/DHCP, Reply, length: 300

---> 서버가 아이피가 사용허락을 응답하는 패킷

📁 관련 파일

[DHCP Server]

포트 : 67(서버)

언트)

[DHCP Client]

포트 : 68(클라이

프로토콜 : UDP

데몬 : /usr/sbin/dhcpd

데몬 스크립트 : /etc/init.d/dhcpd

설정파일 :

/etc/dhcp/dhcpd.conf(서버 설정 파일)

클라이언트는 네트워크 설정에서 프로토콜을 dhcp 로 해 주면 된다.

IP임대로그파일 : /var/lib/dhcpd/dhcpd.leases

※시간 동기화

[first]

#rdate -s time.bora.net

#date

[second]

#rdate -s time.bora.net

#date

<DHCP 서버 설정>

[first]

아래와 같이 나오면 yum 이용하여 DHCP 서버 프로그램을 설치한다.

```
#rpm -qa | grep dhcp
dhcp-common
```

```
#yum -y install dhcp*
```

```
#rpm -qa | grep dhcp
dhcp-common
dhcp-devel
dhcp (서버 프로그램)
```

DHCP 포트 확인

```
#grep bootp /etc/services
```

```
#cat /etc/dhcp/dhcpd.conf
```

---> 서버 설정에 기본적으로 내용이 없다.

```
////////////////////////////////////
DHCP 서비스 설정 파일
```

CentOS 5 버전 : /etc/dhcpd.conf

CentOS 6 버전 : /etc/dhcp/dhcpd.conf

```
////////////////////////////////////
```

샘플 파일 :

```
/usr/share/doc/dhcp-버전/dhcpd.conf.sample
```

---> 샘플 파일을 복사해서 사용할 수도 있다.

```
#cat /usr/share/doc/dhcp*/dhcpd.conf.sample
```

📄 DHCP 서버 설정 파일 형식

```
subnet 네트워크주소 netmask 서브넷마스크 {
    option routers 게이트웨이 ;
    option subnet-mask 서브넷마스크 ;
```



```
option domain-name 도메인이름 ;
option domain-name-servers DNS서버주소 ;
range dynamic-bootp 시작아이피 마지막아이피 ;
default-lease-time 임대시간(단위는 초) ;
max-lease-time 최대임대시간(단위는 초) ;
}

host ns { ---> 클라이언트에게 특정 아이피를 지정할 때 사용하는 항목
    hardware Ethernet 맥주소 ;
    fixed-address 특정아이피 ;
}
```

default-lease-time time;

Time should be the length in seconds that will be assigned to a lease if the client requesting the lease does not ask for a specific expiration time.

max-lease-time time;

Time should be the maximum length in seconds that will be assigned to a lease. The only exception to this is that Dynamic BOOTP lease lengths, which are not specified by the client, are not limited by this maximum.

참조)

<http://www.fis.unipr.it/pub/linux/redhat/9/en/doc/RH-DOCS/rhl-cg-ko-9/s1-dhcp-configuring-server.html>

```
#cd /etc/dhcp
```

--->아래는 first 리눅스 아이피가 192.168.1.10 인 경우이므로
아이피가 틀린 경우에는 자신의 아이피를 적고 테스트하면 된다.

```
#vi dhcpd.conf
```

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    option routers 192.168.1.2; (게이트웨이)
    option subnet-mask 255.255.255.0; (서브넷 마스크)
    option domain-name "andytest.com";
    option domain-name-servers 168.126.63.1; (DNS 서버)
    range 192.168.1.71 192.168.1.80; (아이피범위)
    default-lease-time 7200; (임대기간, 단위는 초)
    max-lease-time 86400;
}
```

////////////////////////////////////
위에서 괄호() 안의 내용은 설명이므로 적는 것이 아님

임대시간 예)

30분 : 30분 x 60초 = 1800

1시간 : 60분 x 60초 = 3600

2시간 : 120분 x 60초 = 7200

////////////////////////////////////

인터넷을 하기 위한 정보 일부(DNS, 게이트웨이)가 생략되어도
서비스는 시작되지만
디폴트값으로 설정되지는 않는다.

////////////////////////////////////
설정 예)

```
subnet 192.168.10.0 netmask 255.255.255.0 {
# --- default gateway
option routers 192.168.10.2;
option subnet-mask 255.255.255.0;

# option nis-domain "domain.org";
option domain-name "example.com";
```

```
option domain-name-servers 192.168.x.x;

# option ntp-servers 192.168.1.1;
# option netbios-name-servers 192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
# option netbios-node-type 2;

range dynamic-bootp 192.168.10.100 192.168.10.199;
default-lease-time 21600;
max-lease-time 43200;

# # we want the nameserver to appear at a fixed address
# host ns {
#   next-server marvin.redhat.com;
#   hardware ethernet 12:34:56:78:AB:CD;
#   fixed-address 207.175.42.254;
# }
}

host fedora {
option host-name "fedora.example.com";
hardware ethernet 00:A0:78:8E:9E:AA;
fixed-address 192.168.1.4;
}

////////////////////////////////////
```

☞ 서비스 관리

```
/etc/init.d/dhcpd stop|start|restart
service dhcpd stop
service dhcpd start
service dhcpd restart
```

```
#service dhcpd start
#netstat -nulp | grep dhcp
```

```
udp          0          0 0.0.0.0:67      0.0.0.0:*
16770/dhcpd
#
```

```
////////////////////////////////////
포트가 열리지 않았으면 -d 옵션 이용하여 오류를 찾은 후
오류를 해결하고 service 시작 시키기
#dhcpd -d
////////////////////////////////////
```

<DHCP 클라이언트 설정>
[second]
#dmesg | grep eth
인터페이스 장치명 확인(eth0)

```
#system-config-network
장치설정 선택
위의 dmesg | grep eth 명령어에서 출력된 장치명 선택(eth0)
DHCP 사용 [*]
```

스페이스 바를 눌러서 * 체크를 한 후 저장후 종료

```
#service network restart
--->리부팅을 해서 확인 할 수도 있다.
```

아이피 확인)
#ifconfig

DNS 확인)
#cat /etc/resolv.conf

게이트웨이 확인)
#route
#route -n

```
#cd /var/lib/dhclient/  
#ls  
dhclient~.leases  
---> DHCP 클라이언트 정보 파일
```

```
[first]  
#cd /var/lib/dhcpd/  
#ls  
dhcpd.leases  
---> DHCP 서버 임대 기록 파일
```

※first 와 second 고정아이피 방식으로 다시 설정

[first]	[second]
192.168.x.10	192.168.x.20

[ITBANK Andylec 주말 리눅스 2 과정]

■오늘의 수업내용(4일차)

FTP 서버

NFS 서버

■FTP Service

File Transfer Protocol : 파일 전송 서비스

☞FTP 서비스 이용 계정 종류

1)시스템에 등록된 사용자

adduser 로 추가하고 passwd 로 암호 설정을 해 준 계정
자신의 홈디렉토리에 업로드와 다운로드 가능

2)익명 계정(Anonymous)

다수의 사용자들에게 자료를 공유하기 위해서 사용하는 계정
업로드는 보통 금지되어 있다.

접속시 사용자에는 anonymous 를 입력하고

암호에는 보통 자신의 이메일을 입력한다.(빈 암호도 가능)

■FTP 서버 프로그램 : vsftpd

☞vsftpd 특징

1)UNIX 계열에서 사용할 수 있는 Free FTP 서버 프로그램

2)Redhat 리눅스 계열에서 기본으로 채택 된 프로그램

3)standalone, xinetd 지원

4)전송 대역폭 조절 기능

5)IP 제한 기능

[first]

```
#rpm -qa | grep vsftpd
```

프로그램이 없으면 #yum -y install vsftpd 로 설치해 준다.

▷서버 데몬 :

/usr/sbin/vsftpd

▷데몬관리 스크립트(서비스 시작, 종료 시키는 파일) :

```
#file /etc/init.d/vsftpd
/etc/init.d/vsftpd: Bourne-Again shell script text executable
#
```

```
#ll /etc/init.d
/etc/init.d 는 /etc/rc.d/init.d 의 링크 파일이다.
```

```
#cat /etc/init.d/vsftpd
C 나 Java 의 switch 문 형식으로 되어 있어서
start 인자가 입력되면 데몬을 메모리에 로딩하고
stop 인자가 입력되면 메모리에서 데몬을 내리는 형식으로 되어 있다.
```

▷설정파일

```
#file /etc/vsftpd/vsftpd.conf
/etc/vsftpd/vsftpd.conf: ASCII English text
#
```

▷사용자 접근제한 파일

```
#cd /etc/vsftpd
#ls
ftpusers user_list
(기본적으로 접속 불가능한 사용자 설정 파일)
```

🔖vsftpd.conf 의 주요 항목

형식)

변수이름=값

--->변수 이름은 대소문자를 구분함

--->값은 대소문자 구분 안 함

--->변수이름과 값 사이에 공백이 있으면 안 됨

anonymous_enable=YES

anonymous 사용자의 접속 허용 여부 (default = YES)

local_enable=YES

로컬 계정 접속 허용 여부

write_enable=YES

write 명령어 허용 여부(업로드 가능 여부)

anon_upload_enable=YES

anonymous 사용자가 파일을 업로드 할 수 있는지 여부

anon_mkdir_write_enable=YES

anonymous 사용자의 디렉토리 생성 허용 여부

xferlog_enable=YES

파일 전송 로그를 남길 것인지 여부

connect_from_port_20=YES

데이터 전송 포트 지정

xferlog_file=/var/log/vsftpd.log

로그파일을 지정(디폴트는 /var/log/xferlog)

xferlog_std_format=YES

표준 포맷으로 로그를 기록할 지 설정

vsftpd 로그 방식은 표준 방식보다 상세한 기록을 남긴다.

idle_session_timeout=600

사용자가 FTP 접속후 아무 작업도 하지 않을 때 접속을 끊을 시간 설정

단위는 초(10분 x 60초)

ftpd_banner=vsftpd 버전

ftp 서버 접속할 때 메시지

session_support=YES

로그인 로그 남기기 여부

chroot_local_user=YES

사용자가 자신의 home directory를 벗어나지 못하도록 설정

---> apple 계정이 ftp 로 로그인 하면 apple 의 홈디렉토리 /home/apple 으로

이동하는 데 자신의 홈디렉토리를

최상위 디렉토리(루트디렉토리) 로 전환(chroot) 시키는 설정이다.

자신의 홈디렉토리가 / (루트) 가 되면

더 이상 올라갈 데가 없으므로 상위 디렉토리로 이동이 불가능하게 된다.

chroot_list_enable=YES

상위로 이동하는 것에 대한 예외 설정

chroot_list_file=/etc/vsftpd/chroot_list

위의 디렉토리 이동제한에 이용되는 사용자 목록 파일

chroot_local_user=YES 항목이 없을 경우 이 파일의 사용자는 상위로 이동 불가

userlist_enable=YES

사용자 접근제한 기능 사용여부

userlist_deny=YES

사용자 목록을 거부자 목록으로 이용할지, 허용자 목록으로 이용할지 결정

anon_max_rate=0

익명 접속시 전송속도 제한항목

(0은 제한없다는 의미, 단위는 초당 bytes)

local_max_rate=0

/etc/passwd 에 등록된 사용자 전송속도 제한항목

(0은 제한없다는 의미, 단위는 초당 bytes)

max_clients=10

최대 접속자 수 제한

max_per_ip=3

하나의 IP당 접속 수 제한 설정

listen=YES

수퍼서버(xinetd) 방식이 아닐 때 YES 사용(Standalone 방식일 때)

tcp_wrappers=YES

TCP Wrappers 접근제한 프로그램 사용 여부

☞ FTP 서버 포트 및 동작 모드

포트 21 번 사용

평상시에는 21번 포트가 열려 있고 데이터 전송시 추가로 포트가 열린다.

active mode(활성모드) : 명령어는 21번 포트 사용,
데이터 포트는 20번 사용

passive mode(수동모드) : 방화벽이 포트 제한을 할 때 사용하며
명령어는 21번 포트 사용,
데이터 포트는 임의로 지정되는 모드

▷ Active Mode(Default)

- 1)FTP Client opens command channel to server; tells server second port number to use
- 2)FTP Server acknowledges
- 3)FTP Server opens data channel to clients second port as instructed
- 4)FTP Client acknowledges and data flows

FTP 클라이언트 : 알FTP, 리눅스 ftp 명령어

Active 모드 동작 예 :

FTP 클라이언트 FTP 서버

Port(3000)----->Port(21)

Data 포트 알림

Data 채널

Port(3001)-----Port(20)

----->

Data 전송

▷ Passive Mode

- 1)FTP Client opens command channel to FTP server and requests "passive" mode.
- 2)FTP Server Allocates port for the data channel and transmits the port number to use for the data transmission
- 3)FTP Client opens the data channel on the specified port
- 4)FTP Server responds with okay to transmit and data begins to flow

Passive 모드 동작 예 :

FTP 클라이언트

FTP 서버

Port(5000)----->Port(21)

PASV 요청

<-----

2000

Port(5001)----->Port(2000)

<-----

Data

<FTP 서버 테스트>

👉ftp 서버도 기본적으로 루트 로그인인 안 된다.

☞ 서버 설정파일(vsftpd.conf)이 변경되면 서비스를 재시작 해 주어야 반영된다.

```
#netstat -ntlp | grep ftp
```

---> 21번 포트가 없으면 리눅스 머신이 FTP 서버로 동작하고 있지 않다는 의미이다.

포트 번호와 서비스 이름은 `/etc/services` 를 참조하면 된다.

```
#grep '^ftp' /etc/services
```

👉 vsftpd 시작

```
#/etc/init.d/vsftpd
```

(---> /etc/rc.d/init.d/vsftpd 와 동일)

사용법: /etc/init.d/vsftpd {start|stop|restart|condrestart|status}

```
#/etc/init.d/vsftpd start
```

(service vsftpd start 와 동일)

```
#netstat -ntlp | grep vsftpd
```

```
tcp      0      0 0.0.0.0:21          0.0.0.0:*          LISTEN
        2537/vsftpd
```

테스트 계정 생성 및 암호 설정

```
#adduser grape
```

```
#passwd grape
```

1234

1234

[윈도우]

알FTP 이용하여 리눅스 머신으로 grape 계정 로그인

FTP 주소 : 리눅스아이피 입력

사용자 ID : grape

비밀번호 : 1234

포트 : 21

☞테스트 항목

1)배너 설정

2)최대 접속자수 제한

3)디렉토리 이동 제한

4)루트 로그인

[first]

```
#cd /etc/vsftpd
```

```
#vi vsftpd.conf
```

86 ftpd_banner=First FTP Server Test (1번 설정)

---> 라인 앞의 # 제거하고 입력

121 max_clients=2 (2번 설정)

96 chroot_local_user=YES (3번 설정, # 제거)

97 chroot_list_enable=YES (3번 설정, # 제거)

99 chroot_list_file=/etc/vsftpd/chroot_list (3번 설정, # 제거)

```
#touch /etc/vsftpd/chroot_list (3번 설정)
```

```
#service vsftpd restart
```

▷4번 설정

FTP 루트 로그인 허용 설정

```
#cd /etc/vsftpd
#vi ftpusers
2 #root
--->2번 라인앞에 # 입력해서 주석처리하고 저장후 종료
```

```
#vi user_list
7 #root
--->7번 라인앞에 # 입력해서 주석처리하고 저장후 종료
```

▷디렉토리 이동제한 예외 설정

```
#cd /etc/vsftpd
#ls
#cat chroot_list
#echo root >> chroot_list
#cat chroot_list
```

--->루트는 상위 디렉토리 이동이 가능하도록 설정

☞FTP 서버 실습(second 리눅스에서 실습)

1. second 리눅스 ftp 서버 접속시 계정에 상관없이 상위로 이동하지 못하도록 설정 (root 는 예외 설정)
2. 배너 메시지 변경하기(파일로 설정하기)
 - 1) ftp 서버 설정파일에 banner_file=/work/ftptest.txt 항목 추가
 - 2) /work 폴더 생성
 - 3) /work/ftptest.txt 파일 작성
3. black 계정 추가 및 암호 설정하고 black 계정은 ftp 로그인인 안 되도록 설정 (ftpusers 또는 user_list 파일에 계정 등록)
4. 윈도우 에서 ftp 접속 해서 결과 확인하기

서버 설정이 변경되면 서비스 재시작한 후 결과 확인

■익명(Anonymous) FTP 사용하기

사용자 ID : anonymous(또는 ftp)

비밀번호 : 이메일(또는 엔터)

-익명 접속시 리눅스 서버에서는 ftp 계정으로 처리되므로

/etc/passwd 의 ftp 계정의 홈디렉토리로 이동된다.

-익명 접속을 허용 안하려면 vsftpd.conf 를 수정(anonymous_enable=NO)후
서비스를 재시작 하면 된다.

```
#grep grape /etc/passwd
#grep ftp /etc/passwd
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
```

```
#ls /var/ftp
#cp /etc/hosts /var/ftp
```

윈도우에서 anonymous(익명 접속) FTP 테스트

■NFS

NFS : Network File System

- ▷Sun 사에서 서버 자원 공유를 위해 개발 됨
- ▷리눅스 및 유닉스 운영체제간에 디렉토리 단위로 공유하는 서비스
- ▷서버 한대를 파일공유 서버로 만들어서 여러 클라이언트가 자료를 이용할 수 있도록 하는 목적으로 사용 될 수 있다.

☞NFS 접속 구조

서버-클라이언트 구조로 사용된다.

- ▷NFS 서버 : 파일을 공유시켜 놓은 컴퓨터
- ▷NFS 클라이언트 : NFS 서버를 이용하는 컴퓨터

[NFS 클라이언트]

[NFS 서버]

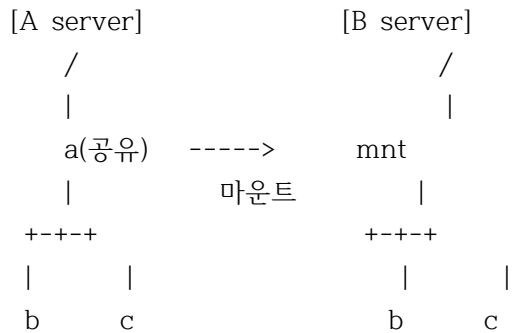
레드햇 리눅스 <-----

공유된

데비안 리눅스 <-----

자료

유닉스 <-----



A 서버에서 a 디렉토리를 공유하면 하위 디렉토리 b, c 도 공유가 된다.
 B 서버에서는 A 서버의 a 디렉토리를 mnt 에 마운트하면
 자신의 디렉토리처럼 b c 에 접근할 수 있다.
 (연결 디렉토리 mnt 는 임의로 지정할 수 있다.)

☞패키지 확인

1) NFS 관련 패키지

[first]

```
#rpm -qa | grep nfs
nfs-utils
nfs-utils-lib
```

2) RPC 관련 패키지

[first]

```
#rpm -qa | grep rpcbind
```

☞RPC(Remote Procedure Call) :

원격 함수 호출, 자신의 컴퓨터에서 원격지 컴퓨터의 함수 또는 프로그램을 실행시키는 것
 서비스마다 포트가 틀리고 자주 사용하는 서비스는 포트가 고정되어 있다.

포트는 한정된 자원이므로 프로그램에 따라서는 고정된 포트가 아니라
 동적으로 할당된 포트를 이용하기도 한다.

동적으로 포트가 할당된 경우 클라이언트에서는
 그 포트를 알지 못하므로 직접 접속할 수가 없고
 RPC 를 통해서 해당 서비스의 포트를 확인 한 후
 그 포트를 서비스를 이용하게 된다.

NFS 는 대표적인 RPC 서비스이다.

서버쪽에서는 부팅시에 portmapper 가 실행되면서 mountd 데몬의
포트를 동적으로 할당한다.

클라이언트가 마운트 요청을 하면 서버쪽의 portmapper 가
클라이언트에게 mountd 데몬의 포트를 알려주고
클라이언트가 그 포트를 이용하여 mountd 와 통신을 하게 된다.

portmapper(CentOS 6 버전에서는 rpcbind 로 서비스 이름이 변경 됨) :
RPC 서비스들의 포트를 관리하는 프로그램

<NFS Server 설정>

▷공유 설정 파일 : /etc/exports

▷exports 파일 형식

공유디렉토리 아이피 or 문자주소(옵션)

▷옵션

ro // read only (디폴트, 읽기 전용)

rw // read, write(읽기,쓰기)

root_squash // 루트 무시(디폴트, 클라이언트의 루트로 접근해도 익명 계정으로 처리
된다.)

no_root_squash // 클라이언트에게 서버측 루트 권한 주기

all_squash // 클라이언트 측에서 사용자로 접근 요청 했을 때 익명 계정으로 연결
을 허용

(디폴트는 no_all_squash)

anonuid=UID // 클라이언트 측에서 익명으로 접근 요청시 지정한 UID 로 연결

anongid=GID // 클라이언트 측에서 익명으로 접근 요청시 지정한 GID 로 연결

wdelay // 작업시 지연설정(디폴트,여러 클라이언트가 동시에
이용할 수 도 있으므로 약간의 시간을 두고 처리하게 된다.)

////////////////////////////////////

squash

1 짓누르다:눌러 찌그러뜨리다(crush):짜다, 납작하게 만들다

2 (좁은 곳에) 밀어 넣다, 쑤셔 넣다 《into》

3 <반란 등을> 진압하다:《구어》 <사람을> 꺾소리 못하게 하다

1 찌부러지다, 납작해지다

2 철썩 떨어지다

squash

1【식물】 호박 《덩굴식물 및 열매》

////////////////////////////////////

☞ NFS 서버 데몬

nfsd // 데이터 전송 처리

rpc.mountd // 마운트 처리

rpc.statd, rpc.lockd // 클라이언트가 공유된 자원의 동시 접속시
발생하는 파일 locking 처리를 담당하는 데몬

☞ 데몬 스크립트 : /etc/init.d/nfs

☞ 공유목록 확인 : exportfs (-v)

-v 공유 설정을 자세히 출력하는 옵션

exportfs -ra(NFS 데몬 재시작 없이 변경된 내용 적용)

☞ portmap 확인

NFS 서비스는 동적으로 포트를 할당받는 RPC(Remote Procedure Call)서비스 이다.

NFS 서비스는 portmap(rpcbind) 데몬이 먼저 동작하고 있어야 한다.

rpcinfo : rpc 서비스들의 정보를 확인하는 명령어

-p : 포트 출력 옵션

[first]

#/etc/init.d/rpcbind status

(service rpcbind status 와 동일)

#ps -ef | grep rpcbind

#rpcinfo -p

<NFS Client>

클라이언트는 mount 명령을 이용해서 NFS 자원을 이용한다.

▷ 서버측 공유목록 확인

showmount -e [아이피 or 문자주소]

▷ 마운트 형식

mount -t nfs [서버아이피 or 문자주소:공유디렉토리] 마운트디렉토리

(-t nfs 는 생략 가능)

<NFS 테스트 환경>

아래와 같이 네트워크 설정

[first]	[second]
192.168.x.10	192.168.x.20
NFS 서버	NFS 클라이언트

[first]
NFS server

#cat /etc/exports
---> 공유 설정 파일

#mkdir /nfs_server1 /nfs_server2
---> 공유할 폴더 생성
#ls /

#vi /etc/exports
/nfs_server1 192.168.x.20(rw,no_root_squash)
/nfs_server2 192.168.x.0/255.255.255.0(rw,sync)

////////////////////////////////////
위 파일의 첫번째 줄은 first 리눅스의 /nfs_server1 디렉토리를 192.168.x.20 컴퓨터에게
읽기,쓰기,루트권한주기 옵션으로 공유하는 설정

/nfs_server1 *(rw,root_squash) 처럼 공유하면 모든 컴퓨터에서 이용가능하게 된다.

192.168.0.*(192.168.0.1, 192.168.0.2 ...)로 접근제한을 하려면
192.168.0.0/24 또는 192.168.x.0/255.255.255.0 으로 /etc/exports 에 등록하면 된다.
(24 는 192.168.0 까지의 비트수를 의미한다.)

sync : 동기화 처리(디폴트)
async : 비동기 처리, sync 와 반대

async This option allows the NFS server to violate the NFS protocol
and reply to requests before any changes made by that request

have been committed to stable storage (e.g. disc drive).

Using this option might improve performance with version 2 only,
but at the cost that an unclean server restart (i.e. a crash)
can cause data to be lost or corrupted.

sync Reply to requests only after the changes have been committed to
stable storage (see async above).

////////////////////////////////////

▷rpcbind(portmapper)

RPC 서비스 포트관리 프로그램

NFS 클라이언트가 NFS 서버의 공유디렉토리를 마운트하려고 할 때
먼저 서버측의 111 번 포트의 portmapper 에게 마운트를 담당하는
mountd 의 포트를 물어보고 그 다음에 클라이언트가
서버측의 mountd 포트로 접속을 해서 마운트 처리가 완료된다.

[서버]

[클라이언트]

portmap(111번 포트) <----- mount 요청

----->

mountd 의 포트 전송

rpc.mountd(포트 랜덤 할당) <----- mount 처리

nfsd ----->

데이타 전송

[first]

NFS 서비스 시작 및 확인

```
#service nfs start
```

```
#ps -ef | grep nfs
```

```
#ps -ef | grep mountd
```

---> 메모리에 실행된 프로세스 확인

#rpcinfo -p

프로그램	버전	원형	포트	
100000	2	tcp	111	portmapper
100000	2	udp	111	portmapper
100024	1	udp	32768	status
100024	1	tcp	32769	status
100011	1	udp	728	rquotad
100011	2	udp	728	rquotad
100011	1	tcp	731	rquotad
100011	2	tcp	731	rquotad
100003	2	udp	2049	nfs
100003	3	udp	2049	nfs
100003	4	udp	2049	nfs
100003	2	tcp	2049	nfs
100003	3	tcp	2049	nfs
100003	4	tcp	2049	nfs
100021	1	udp	32770	nlockmgr
100021	3	udp	32770	nlockmgr
100021	4	udp	32770	nlockmgr
100021	1	tcp	32770	nlockmgr
100021	3	tcp	32770	nlockmgr
100021	4	tcp	32770	nlockmgr
100005	1	udp	757	mountd
100005	1	tcp	760	mountd
100005	2	udp	757	mountd
100005	2	tcp	760	mountd
100005	3	udp	757	mountd
100005	3	tcp	760	mountd

#

서비스 재시작)

#service nfs stop

#service nfs start

또는

#service nfs restart

포트 변경 확인)

#rpcinfo -p

프로그램	버전	원형	포트	
100000	2	tcp	111	portmapper
100000	2	udp	111	portmapper
100024	1	udp	32768	status
100024	1	tcp	32769	status
100011	1	udp	849	rquotad
100011	2	udp	849	rquotad
100011	1	tcp	852	rquotad
100011	2	tcp	852	rquotad
100003	2	udp	2049	nfs
100003	3	udp	2049	nfs
100003	4	udp	2049	nfs
100003	2	tcp	2049	nfs
100003	3	tcp	2049	nfs
100003	4	tcp	2049	nfs
100021	1	udp	32770	nlockmgr
100021	3	udp	32770	nlockmgr
100021	4	udp	32770	nlockmgr
100021	1	tcp	32771	nlockmgr
100021	3	tcp	32771	nlockmgr
100021	4	tcp	32771	nlockmgr
100005	1	udp	861	mountd
100005	1	tcp	864	mountd
100005	2	udp	861	mountd
100005	2	tcp	864	mountd
100005	3	udp	861	mountd
100005	3	tcp	864	mountd

#

---> NFS 서비스를 재시작하면 mountd 포트가 변경되는 것을 알 수 있다.

(이러한 서비스가 RPC 서비스이다.)

NFS 서버를 이용하는 클라이언트 입장에서는 mountd 의 포트를 알 필요는 없고

111 번 포트를 이용하는 portmapper 에게 먼저 물어보면 mountd 의

포트를 알 수 있으므로 그 포트를 이용하여 통신을 하게 된다.

////////////////////////////////////

#man portmap

PORTMAP(8)

BSD System Manager's Manual

PORTMAP(8)

NAME

portmap - DARPA port to RPC program number mapper

SYNOPSIS

portmap [-d] [-l] [-v]

DESCRIPTION

Portmap is a server that converts RPC program numbers into DARPA protocol port numbers. It must be running in order to make RPC calls.

When an RPC server is started, it will tell portmap what port number it is listening to, and what RPC program numbers it is prepared to serve.

When a client wishes to make an RPC call to a given program number, it will first contact portmap on the server machine to determine the port number where RPC packets should be sent.

Portmap must be started before any RPC servers are invoked.

////////////////////////////////////

공유 디렉토리 확인)

#exportfs

---> /etc/hosts 에 문자주소가 등록되어 있으면 아이피 대신 문자로 출력된다.

#exportfs -v

-v 설정내용을 자세히 출력시키는 옵션

테스트 파일 생성)

#cd /nfs_server1

```
#pwd
#touch first_첫번째리눅스아이피.txt
#ls
```

```
////////////////////////////////////
```

NFS 4 UID 맵핑 설정

[first]

```
#vi /etc/idmapd.conf
```

```
6 Domain = linux1.andylec.com
```

```
#service nfs restart
```

[second]

```
#vi /etc/idmapd.conf
```

```
6 Domain = linux1.andylec.com
```

```
#/etc/init.d/rpcidmapd restart
```

또는 service rpcidmapd restart

```
////////////////////////////////////
```

클라이언트 설정 및 테스트)

[second]

NFS client

```
#ifconfig
```

```
#showmount 첫번째리눅스아이피
```

---> -e 옵션을 지정해야 공유목록을 확인할 수 있다.

```
#showmount -e 첫번째리눅스아이피
```

Export list for x.x.x.x:

--->다른 컴퓨터의 공유 목록 확인

☞ 테스트 환경

[서버]

/nfs_server1

/nfs_server2

[클라이언트]

/nfs_client1

/nfs_client2

----->

마운트

테스트 1

[second]

```
#mkdir /nfs_client1
```

```
#mount -t nfs 첫번째리눅스아이피:/nfs_server1 /nfs_client1
```

또는

```
#mount -t nfs first:/nfs_server1 /nfs_client1
```

---> /etc/hosts 에 first 가 등록되어 있는 경우

```
#df -h
```

```
#df -T
```

```
#cd /nfs_client1
```

```
#ls
```

```
#touch second.txt
```

```
#ls -l
```

테스트 2

[second]

```
#mkdir /nfs_client2
```

```
#mount -t nfs 첫번째리눅스아이피:/nfs_server2 /nfs_client2
```

```
#df -h
```

```
#cd /nfs_client2
```

```
#pwd
```

```
#ls
```

```
#touch redhat.txt
```

---> X

---> NFS 서버 설정에서 rw 로 쓰기 권한까지 주었지만

디렉토리 퍼미션의 권한이 없어서 파일이 만들어 지지 않는다.

[first]

```
#ls -ld /nfs_server2
```

```
#chmod 777 /nfs_server2
```

```
#ls -ld /nfs_server2
```

[second]

```
#pwd
```



```
/nfs_client2
#touch redhat.txt
#ll
---> first NFS 서버에서 디렉토리 퍼미션에 쓰기 권한을 주어서
      파일이 만들어진다.
---> 파일의 소유자와 그룹이 특정 계정으로 나타나게 하려면
      NFS 서버 공유 설정에서 anonuid, anongid 를 이용하면 된다.
---> NFS 클라이언트 루트에게 루트권한을 주려면 no_root_squash 옵션을 이용하면 된다.
```

```
마운트 해제하기)
[second]
#umount /nfs_client2
---> busy 라고 나오면 다른 디렉토리로 이동후 마운트 해제
#pwd
#cd
#pwd
/root
```

```
#umount /nfs_client2
#ls /nfs_client2
#df -h
```

```
#umount /nfs_client1
#ls /nfs_client1
#df -h
```

■실습

1. second 리눅스를 NFS 서버로 설정
 - 1) /share1, /share2 디렉토리 생성
 - 2) /share1 은 루트권한을 주고, 읽기, 쓰기 옵션으로 공유 설정
 - 3) /share2 는 루트권한 무시, 읽기, 쓰기, 익명사용자는 apple 계정(UID 500번), apple 그룹(GID 500번) 으로 처리 설정

2. first 리눅스에서 테스트

```
////////////////////////////////////
```

```
[second]
#mkdir /share1 /share2
```

```
#vi /etc/exports
/share1      *(rw,no_root_squash,sync)
/share2      *(rw,root_squash,anonuid=500,anongid=500,sync)
#chmod 777 /share2
#service rpcbind restart
#service nfs restart
```

```
[first]
#mkdir /my1 /my2
#rpcinfo -p 두번째리눅스아이피
#showmount -e 192.168.x.20
--->두번째리눅스 아이피 입력
#mount -t nfs 192.168.x.20:/share1 /my1
#mount -t nfs 192.168.x.20:/share2 /my2
#df -h
```

////////////////////////////////////

[ITBANK Andylec 주말 리눅스 2 과정]

■오늘의 수업내용(5일차)

Autofs

Samba

■공지사항

-다음 달 수강신청을 해 주시기 바랍니다.

■Autofs

-사용시점에 파일 시스템을 자동으로 마운트하고

일정시간 사용하지 않으면 언마운트 해 주는 데몬

-주로 NFS 나 자주 사용되지 않는 장치를 마운트 할 때 사용

☞패키지

[first]

```
#rpm -qa | grep autofs
```

```
q //query
```

```
a //all
```

```
rpm -qa //리눅스에 설치된 프로그램(패키지) 모두 출력
```

```
rpm -qa | grep autofs //설치된 프로그램중에 autofs 들어간 프로그램만 출력
```

```
yum -y install 패키지명(프로그램이름) //인터넷의 패키지 서버에 해당 프로그램을 다운받아 설치
```

☞데몬

```
/usr/sbin/automount
```

☞데몬 스크립트

```
/etc/init.d/autofs
```

☞테스트 환경

[first]

NFS 서버

[second]

Autofs

☞autofs 서버 설정

서버에서는 NFS 설정만 해 주면 된다.(/etc/exports)

☞autofs 클라이언트 설정

[second]

1. /etc/sysconfig/autofs

autofs 데몬에 대한 설정 파일

6 #MASTER_MAP_NAME="auto.master"

자동마운트에 사용될 주설정 파일 지정

10 TIMEOUT=300

자동마운트된 자원을 사용하지 않을 때 언마운트할 시간(5분, 단위 초)

32 BROWSE_MODE="yes"

auto.master 에서 지정한 파일을 브라우징 시킬 지 여부

autofs 를 사용하려면 yes 로 수정해야 함

2. /etc/auto.master

자동마운트할 대상 디렉토리 마스터 설정 파일

/misc /etc/auto.misc

/misc 디렉토리를 /etc/auto.misc 파일을 적용하여 사용하겠다는 의미

/etc/auto.misc 에서 설정한 디렉토리가 /misc 하위에 자동 생성되어 마운트 된다.

3. /etc/auto.misc

auto.master 파일에 설정해 준 디렉토리 하위에

실제 마운트 될 mount point 설정 파일

☞마운트 옵션

suid, nosuid // SetUID 허용 여부

bg // nfs 마운트를 처음에 실패할 경우 백그라운드 실행

retry=숫자 // 포기할 때까지 마운트 재시도 횟수(기본값은 일만번, 10000)

timeo=숫자 // 마운트 시도 시 타임아웃 시간을 설정(단위는 1/10 초)

soft, hard // 재시도 횟수가 끝 났을 때 연결을 계속 할 지 결정(hard 는 무한 재 시도, soft 는 타임아웃 될 때 까지 시도)

retrans=숫자 // 숫자 만큼 요구를 재전송하는 것으로 기본은 3번

```
intr                // 정지 프로세스를 죽이기 위한 인터럽트를 허용
rsize=숫자          // nfs 서버에 있는 읽기 버퍼의 크기(바이트 단위)
wsize=숫자          // nfs 서버에 있는 쓰기 버퍼의 크기(바이트 단위)
```

☞autofs 테스트

1. NFS 자동마운트

[first]

---> NFS 서버 설정

```
#mkdir /nfs_share
#chmod 777 /nfs_share
```

```
#vi /etc/exports
```

---> NFS 공유 설정 파일

기존 내용은 모두 삭제하고 아래 내용 입력

```
/nfs_share          *(rw,sync)
```

```
#service rpcbind restart
```

```
#service nfs restart
```

```
#exportfs
```

공유목록 확인

```
#exportfs -v
```

-v 자세히 출력

[second]

---> Autofs 사용

```
#showmount -e 첫번째리눅스아이피
```

--->공유목록 확인

```
#vi /etc/sysconfig/autofs
```

```
33 BROWSE_MODE="yes"
```

---> no 를 yes 로 수정

```
#cat /etc/auto.master
```

자동 마운트될 베이스 디렉토리(상위 디렉토리)가 /misc 로 되어 있음

```
#vi /etc/auto.misc
```

```
first_share      -rw,soft,intr   첫번째리눅스아이피:/nfs_share
```

```
////////////////////////////////////
```

--->첫번째리눅스아이피:/nfs_share 에서 / 를 빼면 안 됨

형식)

자동마운트할디렉토리 마운트옵션 마운트할자원

---> /etc/auto.master 파일에 /misc 디렉토리가 정의되어 있으므로

/misc/first_share 디렉토리를 찾아갈 때 자동마운트가 된다.

```
////////////////////////////////////
```

```
#ps -ef | grep auto
```

부팅 중에 실행된 automount 가 출력 됨

```
#service autofs restart
```

[first]

```
#cd /nfs_share
```

```
#touch first.txt
```

[second]

```
#df -h
```

```
#cd /misc
```

```
#ls
```

```
#cd first_share
```

```
#ls
```

```
#df -h
```

```
////////////////////////////////////
```

/etc/auto.master 파일 : /misc 디렉토리 등록 되어 있음

/etc/auto.misc 파일 : first_share 디렉토리 등록 되어 있음

cd 를 이용하여 /misc/first_share 디렉토리를 찾아갈 때

첫번째리눅스의 /nfs_share 가 autofs 에 의해 자동 마운트 됨

////////////////////////////////////

2. NFS, Autofs, FTP 응용

[first]

```
#adduser -u 2001 candy1
```

```
#adduser -u 2002 candy2
```

```
#cd /nfs_share
```

```
#mkdir candy1 candy2
```

```
#chown candy1:candy1 candy1
```

```
#chown candy2:candy2 candy2
```

```
#ll
```

[second]

```
#adduser -u 2001 candy1
```

```
#adduser -u 2002 candy2
```

```
#passwd candy1
```

```
1234
```

```
1234
```

```
#passwd candy2
```

```
1234
```

```
1234
```

```
#grep candy /etc/passwd
```

```
#usermod -d /misc/first_share candy1
```

```
#usermod -d /misc/first_share candy2
```

```
#grep candy /etc/passwd
```

```
#yum -y install vsftpd
```

---> FTP 서버 프로그램 설치

```
#service vsftpd restart
```

---> FTP 서비스 시작

```
#netstat -ntlp | grep vsftpd
---> FTP 서비스 포트 21 확인
```

테스트 환경

[first]	[second]
NFS 서버	Autofs, FTP 서버
	^
	[윈도우]

[win7]
알FTP 이용 second 로 ftp 로그인 테스트(candy1, candy2)

---> 윈도우에서 두번째리눅스로 FTP 로그인 할 때
첫번째리눅스의 디렉토리가 자동마운트 됨(서버 응용 예)

■실습

1. first 리눅스에서 /nfs_share2 디렉토리 NFS 공유 설정
2. second 리눅스에서 /misc/first 디렉토리로 이동시
first 리눅스의 /nfs_share2 디렉토리가 자동마운트 되도록 설정
3. second 리눅스에 bank1, bank2 계정 생성 및 암호 설정하기
4. 윈도우에서 second 리눅스로 bank1, bank2 계정으로 알FTP 접속할 때
first 리눅스의 /nfs_share2 디렉토리가 사용되도록 설정하기
(2번 autofs 사용)

[first]	[second]
NFS 서버	Autofs, FTP 서버
/nfs_share2 ----->	/misc/first

[윈도우]
알FTP

////////////////////////////////////


```
[first]
#mkdir /nfs_share2
#chmod 777 /nfs_share2
#touch /nfs_share2/first.txt
#vi /etc/exports
/nfs_share2 *(rw,no_root_squash,sync)
#service rpcbind restart
#service nfs restart
#rpcinfo -p
#exportfs
#adduser -u 3001 bank1
#adduser -u 3002 bank2
```

```
[second]
#vi /etc/auto.misc
first -rw,soft,intr 첫번째리눅스아이피:/nfs_share2
#service autofs restart
#showmount -e 첫번째리눅스아이피
#cd /misc/first
#ls
#df -h
#adduser -u 3001 bank1
#adduser -u 3002 bank2
#passwd bank1
1234
1234
#passwd bank2
1234
1234
#usermod -d /misc/first bank1
#usermod -d /misc/first bank2
////////////////////////////////////
```

■SAMBA

삼바는 리눅스머신과 윈도우머신간에 MS 윈도우 방식으로 자료를 공유할 수 있는 서비스이다.

```
[windows] <-----> [Linux]
                Data Share
```

☞홈페이지 : <http://www.samba.org>

Samba is the standard Windows interoperability suite of programs for Linux and Unix.

Samba is an important component to seamlessly integrate Linux/Unix Servers and Desktops

into Active Directory environments using the winbind daemon

☞삼바 관련 용어

NetBIOS :

넷바이오스는 컴퓨터 상에 있는 응용프로그램들이 LAN(근거리 통신망) 내에서 서로 통신 할 수 있게 해 주는 프로그램 이다. 초창기 PC 네트워크를 위해 IBM 에 의해 개발 되었으며, 마이크로소프트에 의해 채택되었고, 산업계 표준이 되었다. 일반적으로 윈도우 사용자에게는 공유 서비스로 이해되고 파일과 프린트 서비스, 호스트 도메인과 워크그룹의 구분, 호스트 브라우징, 브로드캐스팅과 네임 서비스를 포함한 폭넓고 다양한 기능을 정의하고 있다.

SMB :

Server Message Block

다른 시스템의 디스크나 프린터 자원 공유를 위한 프로토콜
TCP/IP 기반하의 NetBIOS 프로토콜 이용

CIFS :

Common Internet File System

윈도우와 유닉스 환경을 동시 지원하는 인터넷 표준 파일 규약 프로토콜
SMB 파일 공유 프로토콜의 확장 버전

참조)

http://www.codefx.com/CIFS_Explained.htm

What is CIFS?

The Common Internet File System (CIFS), also known as Server Message Block (SMB),

is a network protocol whose most common use is sharing files on a Local Area Network (LAN).

☞ 윈도우 2003 확인 사항

- 1)vmware 에서 win2003 을 Open 하기
- 2)win2003 부팅시키기
- 3)질문나오면 "I copied it " 선택
- 4)로그인 화면 에서 Ctrl + alt + insert 를 누르고 암호는 andy 입력

[win2003]

1)제어판-시스템 클릭

컴퓨터 이름-변경 클릭

컴퓨터 이름 : win2003

작업 그룹 : ANDYLEC

위와 같이 수정후 확인 클릭

질문에 확인-확인 클릭

리부팅 은 아니오 클릭

--->실제 머신이라면 윈도우 컴퓨터 이름을 각각 다르게 설정해야 함

2)탐색기 실행후 C:\SambaShare 폴더 생성(폴더 이름에 공백 있으면 안 됨)

C:\SambaShare 폴더 를 마우스로 클릭한 후 마우스 오른쪽 버튼 누르고

메뉴 마지막 "속성" 을 클릭하기

공유 탭에서 공유 설정하기

[일반][공유][보안][사용자 지정]

|

"(*)이 폴더를 공유" 선택-확인 클릭

3)리부팅 하기

<테스트 1>

윈도우의 공유자원을 리눅스에서 접근하기(삼바서버 필요 없음)

[리눅스]

[윈도우]

디렉토리 <----- 공유폴더
CIFS 방식 마운트

[win2003]

도스창 실행

C:\>net share

---> \$ 로 끝난 자원은 hidden 공유를 의미

[first]

NFS 로 마운트된 디렉토리 있으면 마운트 해제하기

#df -h

#umount 마운트디렉토리

▷윈도우 머신의 공유목록 확인

1) smbclient -L 컴퓨터이름(또는 아이피)

---> 리눅스에서 윈도우 XP 공유 자원 확인 할 때

2) smbclient -L 컴퓨터이름(또는 아이피) -U 로그인사용자이름

암호는 로그인사용자의 암호 입력

#smbclient -L 2003아이피

암호는 엔터 입력

---> X (공유 자원 출력 안 됨)

2003 에서는 아래와 같이 입력

#smbclient -L 2003아이피 -U administrator

암호 andy 입력

#vi /etc/hosts

마지막 라인에 추가

원2003아이피 win2003

---> win2003 은 윈도우 컴퓨터의 이름과 동일하게 적어야 함

```
#smbclient -L win2003 -U administrator
```

형식)

```
mount -t cifs -o user=윈도우사용자명 윈도우아이피:공유폴더 리눅스마운트디렉토리
```

---> 윈도우 XP 를 이용하여 테스트할 경우에는 user 를 지정할 필요가 없음

```
#mkdir /win
```

```
#mount -t cifs -o user=administrator 윈2003아이피:SambaShare /win
```

Password: 계정의 암호 입력

또는

```
#mount -t cifs -o user=administrator //윈2003아이피/SambaShare /win
```

```
#df -h
```

```
#df -T
```

```
#cd /win
```

```
#pwd
```

```
/win
```

```
#ls
```

마운트 해제하기

```
#cd
```

```
#pwd
```

```
/root
```

```
#umount /win
```

```
#df -h
```

<테스트 2>

익명 공유 방식 삼바 테스트

리눅스의 공유 자원을 윈도우에서 이용할 때(삼바 서버 필요)

[리눅스]

공유폴더(디렉토리)

삼바서버 실행

----->

[윈도우]

리눅스의 공유자원 접근

☞삼바 관련 파일

1. 설정파일 디렉토리 : /etc/samba/
2. 설정파일 : /etc/samba/smb.conf
3. 데몬 스크립트 : /etc/init.d/smb start
(service smb start 와 동일)
4. 데몬 : smbd
5. 사용 포트 : 139, 445

#man smbd

smbd - server to provide SMB/CIFS services to clients
smbd is the server daemon that provides filesharing and printing services to Windows clients.

#man nmbd

nmbd - NetBIOS name server to provide NetBIOS over IP naming services to clients

nmbd is a server that understands and can reply to NetBIOS over IP name service requests

[first]

#rpm -qa | grep samba

#yum -y install samba

#rpm -qa | grep samba

samba-common (공통파일-라이브러리, 설정파일 등)

samba-client (삼바 클라이언트 프로그램)

samba (삼바 서버 프로그램)

[first]

#cd /etc/samba

#ls

lmhosts (/etc/hosts 와 비슷한 역할)

smb.conf (삼바 설정 파일)

```
#vi smb.conf
```

```
14 # Any line which starts with a ; (semi-colon) or a # (hash)
```

```
15 # is a comment and is ignored.
```

; 나 # 으로 시작되는 라인은 주석(설명) 이다.

삼바 설정은 global 영역과 share 영역으로 구성된다.

1)global 영역

프로그램 버전에 따라 왼쪽 라인 번호는 차이가 날 수 있다.

```
74 workgroup = ANDYLEC (윈도우의 작업 그룹과 동일하게 설정)
```

```
75 server string = First Samba Server %v
```

컴퓨터 설명에 해당

%v 는 버전으로 변환되어 나타난다.

```
77 netbios name = FirstSamba
```

; 를 제거하고 수정하기(윈도우 네트워크 환경에서 사용되는 컴퓨터이름 설정)

```
80 ;hosts allow = 127. 192.168.12. 192.168.13.
```

---> 접근제한 설정(수업에서는 기본값 그대로 사용)

192.168.12. 은 192.168.12.* 컴퓨터에서 이용할 수 있다는 의미이다.

```
89 log file = /var/log/samba/%m.log
```

---> 삼바 로그 파일

/var/log/samba/변환된파일명 에 접속 기록을 저장한다.

%L //서버의 netbios 이름

%m //접속하는 컴퓨터 이름(machine name)을 의미

%R //통신에 사용되는 프로토콜(LANMAN1, LANMAN2, NT1 ...)

%I //클라이언트 머신의 IP 주소

```
91 max log size = 50
```

---> 로그파일 사이즈(단위 KB)

```
101 security = share
```

---> 인증 설정(user 에서 share 로 변경)

//

<삼바 인증 설정>

user

삼바 서버에 접속하는 클라이언트는 윈도우에
로그인한 사용자명과 암호를 확인한 후에
삼바 서버 접속이 이루어진다.

share

유효한 사용자명과 암호로 삼바 서버에 로그인하지
않아도 접속이 되는 방식이다.

server

다른 삼바 서버에서 사용자명과 암호를 전달하여
확인하는 방식이다.

//

2)share 영역(실제 공유할 디렉토리 설정 영역)

246 #=====Share Definitions=====

[homes] ---> 홈디렉토리 설정(인증모드를 사용자로 할 때 사용)

browseable = no

---> 윈도우에서 홈디렉토리가 보이게 할지를 결정하는 항목

writable = yes

---> 쓰기 권한 설정 항목

[공유자원명] ---> 윈도우에서 접근 가능한 공유 목록

path ---> 실제 공유 디렉토리 경로

public ---> 모든 사용자에게 접근 허용

browseable = yes

writable = no

마지막에 아래 추가

[first_work]

comment = Samba test


```
path = /work
writable = no
browseable = yes
guest ok = yes
```

저장후 종료하기

```
////////////////////////////////////
//
```

<samba 공유디렉토리 지정 옵션>

comment	---	> 설명
path	---	> 공유 디렉토리를 절대경로로 지정
writable, write ok	---	> 쓰기 허용
read only	---	> 읽기 전용
browseable	---	> 공유 디렉토리 목록을 보여줄 지를 지정
public, guest ok	---	> 공유 디렉토리를 다른 사용자들이 이용하게 할지를 지정
valid users	---	> 공유 디렉토리를 로그인 할 수 있는 사용자 지정
create mask, create mode	---	> 파일 생성시 기본권한 설정
write list	---	> 쓰기 가능한 특정 사용자 지정

```
////////////////////////////////////
//
```

```
#mkdir /work
#ls -ld /work
755 퍼미션 확인(drwxr-xr-x)
#cd /work
#vi first_samba.txt
```

Samba Server Test

위와 같이 입력하고 저장후 종료

```
#testparm
--->삼바 설정 체크 명령
```

```
#service smb start
#ps -ef | grep smbd
#netstat -ntlp | grep smbd
```

☞ 윈도우 에서 리눅스의 공유자원 접근하기

[win2003]

시작버튼-실행-[\\삼바서버아이피]

--->텍스트 박스에 \\리눅스아이피 를 입력하고 엔터 누르기

```
////////////////////////////////////
[first]
#service nmb restart
nmbd : netbios 이름 서비스 데몬
////////////////////////////////////
```

<사용자 인증 공유 방식 삼바 테스트>

- 1)삼바유저(User)로 사용할 계정을 시스템에 생성
 - 2)smbpasswd 이용하여 삼바유저 생성 및 암호 설정
- 로컬 계정의 암호와 삼바 계정의 암호는 별개 임

```
////////////////////////////////////
[리눅스]          <-----삼바----->          [윈도우]
```

시스템 계정	삼바계정
(/etc/passwd)	

시스템암호	삼바암호
(/etc/shadow)	

```
////////////////////////////////////
```

```
[first]
#adduser samba1
--->시스템 계정 생성
```

```
#smbpasswd -h
```

도움말 확인

```
#smbpasswd -a samba1
```

```
1234
```

```
1234
```

--->삼바 계정 생성

삼바 사용자는 passdb.tdb 파일에 저장되며

이 파일은 데이터베이스 파일이므로 삼바 사용자는 아래 명령어로 확인을 한다.

```
#net lookup name samba1
```

--->삼바 계정 확인

```
#cd /etc/samba
```

```
#vi smb.conf
```

```
[global]
```

```
#----- Standalone Server Options -----
```

```
101 security = user (share 에서 user 로 변경)
```

```
102 passdb backend = tdbsam
```

새로운 공유 자원 추가)

아래 내용 마지막에 추가

```
[public]
```

```
comment = samba public dir
```

```
path = /samba
```

```
browseable = yes
```

```
guest ok = yes
```

```
writable = yes
```

저장후 종료

```
#mkdir /samba
```

```
#chmod 777 /samba
```

```
#service smb restart
```

```
[win2003]
```

시작-실행-[\\리눅스아이피 입력]

로그인창 나오면 아이디와 암호 입력

아이디는 samba1

암호는 samba1 의 암호 입력

samba 접속 종료

도스창 실행

C:\>net use

C:\>net use \\아이피\IPC\$ /delete

---> 세션(연결정보) 삭제

C:\>net use

■실습

1. win2003 에서 C:\MyDATA 폴더를 공유하고 second 리눅스에서 CIFS 방식으로 마운트 테스트
2. second 리눅스에서 아래 조건을 만족하도록 samba 서버구축
 - 1) 사용자 인증 방식(계정은 samba2 암호는 1234 사용)
 - 2) 공유 디렉토리 : /work
 - 3) win2003 에서 /work 폴더에 쓰기가 가능하도록 설정

////////////////////////////////////

[second]

#yum -y install samba

#cd /etc/samba

#vi smb.conf

74 workgroup = ANDYLEC

75 server string = Second Samba Server

77 netbios name = Secondsamba

101 security = user

마지막 부분에 아래 추가

[second_work]

comment = Samba test

path = /work

writable = yes

browseable = yes

guest ok = yes

#mkdir /work

```
#chmod 777 /work
#adduser samba2
#smbpasswd -a samba2
1234
1234
#net lookup name samba2
#service smb start
```

////////////////////////////////////

[ITBANK Andylec 주말 리눅스 2 과정]

■오늘의 수업내용(6일차)

Apache

PHP

MySQL

■실습준비

1. 수업용 FTP 서버 120.UPLOAD2 폴더에서
jpg 파일을 first 의 /var/www/html 로 다운받기

[first]

```
#yum -y install ftp
```

```
#cd /var/www/html
```

```
#ftp 서버아아피
```

```
Name : 아이디 입력
```

```
Password : 암호 입력
```

```
ftp>cd 120.UPLOAD2
```

```
ftp>ls
```

```
ftp>mget *.jpg
```

질문나오면 엔터 또는 y 입력(mget 은 여러 개 파일 다운받는 명령)

```
ftp>by
```

```
#
```

```
#ls
```

```
test.jpg
```

```
#file test.jpg
```

리눅스 메뉴표시줄-프로그램-그래픽-gThumb 그림보기

---> 이미지(그림) viewer 프로그램

```
#gthumb
```

2. 윈도우 웹브라우저 설정 아래와 같이 변경

웹브라우저 메뉴-도구-인터넷 옵션

검색 기록 : [설정] 버튼 클릭

임시 인터넷 파일 :

저장된 페이지의 새 버전 확인 :

(*) 웹페이지를 열 때마다

확인

---> 웹서버 테스트시 웹브라우저가 자체적으로 캐쉬해 놓은
이전 홈페이지가 보여지는 경우가 있으므로 위와 같이
변경하고 테스트를 한다.

■Apache

☞웹서버(Web Server)

윈도우 웹브라우저 주소창에서 아이피나 문자주소를 입력했을 때
홈페이지가 보이도록 서비스해 주는 프로그램
리눅스에서는 Apache 를 주로 사용하고
윈도우 서버에서는 IIS 를 주로 사용한다.
Apache 와 IIS 는 서버 프로그램 이름이다.

☞HTTP(Hypertext Transfer Protocol)

HTTP 는 웹 상에서 파일(텍스트, 이미지, 사운드, 비디오, 기타 파일)을
주고 받는데 필요한 프로토콜로서
TCP/IP 와 관련된 응용 프로토콜(Application, 응용 프로그램이 사용하는 프로토콜)이다.

☞HTTP 특징

HTTP 는 World Wide Web(WWW) 에서 사용되는 프로토콜이다.

HTTP 는 비상태기반(Stateless Protocol) 프로토콜이다.

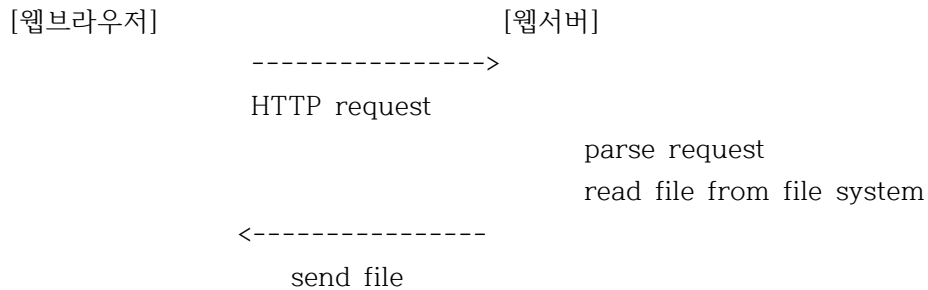
클라이언트 요청과 서버측 응답으로 구성된다.

요청과 응답은 3 부분으로 구성된다.

- 1)요청코드(Request Method)/응답 코드(Response Code)
- 2)헤더(Header)
- 3)바디(Body)

☞웹서버의 동작방식 :

- 1)클라이언트는 웹브라우저를 통해 HTTP 요청을 한다.
- 2)웹서버는 요청에 대한 내용을 분석한다.
- 3)웹서버는 파일 시스템의 파일정보를 읽어 들인다.
- 4)웹서버가 클라이언트에게 파일을 보낸다.



☞패키지 확인

[first]

```
#rpm -qa | grep httpd
```

httpd-버전 (웹서버 메인 프로그램)

프로그램이 검색 되지 않으면 yum 으로 설치

```
#yum -y install httpd
```

☞웹서버 설정파일 : /etc/httpd/conf/httpd.conf

☞웹서버 데몬 관리 스크립트 : /etc/init.d/httpd

☞서비스 관리

```
/etc/init.d/httpd start|stop|restart
```

```
service httpd start|stop|restart
```

☞Apache 웹서버 주요 항목

```
#cd /etc/httpd/conf
```

```
#vi httpd.conf
```

```
:set nu
```

44 ServerTokens OS

서버 HTTP 응답 헤더를 설정, 오류문 등 서버 메시지에
출력되는 정보 설정

Full : 아파치 서버 버전, 운영체제, 모듈 정보 등을 모두 출력
OS : 아파치 서버 버전과 운영체제 정보만을 출력
Prod : 아파치 서버 정보만을 출력

57 ServerRoot "/etc/httpd"

웹서버 base 디렉토리

(웹서버와 관련된 파일과 sub 디렉토리가 모여 있는 디렉토리)

65 PidFile run/httpd.pid

프로세스 아이디 파일

아파치 웹서버가 실행 될 때 PID 를 기록하는 파일을 지정

경로명이 run/httpd.pid 이므로 /etc/httpd/run/httpd.pid 로 생성 됨

70 Timeout 60

클라이언트의 요청을 받고 응답해 주기까지의 시간

76 KeepAlive Off

한 번 연결된 연결을 유지할 것인가를 결정하는 지시자

92 ##Server-Pool Size Regulation (MPM specific)

서버 프로세스 수

아파치 2.x 에서는 다중처리모듈(MPM) 이라는 교체할 수 있는 동기화 모듈 지원

RPM 패키지 사용시 prefork MPM 으로 설정 됨

96 #prefork MPM

#StartServers: number of server processes to start

아파치 웹서버를 실행 할 때의 프로세스 갯수 지정

메인 프로세스 한 개와 startservers 에 설정된 프로세스 갯수가 동작

#MaxClients: maximum number of server processes allowed to start

클라이언트들이 동시에 최대로 접속했을 경우 실행 가능한 최대 프로세스 수

136 Listen 80

웹서버가 사용하는 포트

242 User apache

243 Group apache

웹서버가 사용하는 유저와 그룹(웹서버가 홈페이지를 찾아갈 때 리눅스 운영체제는
웹서버가 사용하는 apache 계정이 접근하는 것으로 판단한다.)

메인 프로세스는 root 로 실행, 자식 프로세스는 apache 권한 으로 실행

262 ServerAdmin root@localhost

서버에 문제가 생겼을 경우 시스템 관리자에게 메일을 보낼 수 있도록
관리자 이메일 지정

#ServerName www.example.com:80

클라이언트에게 다시 돌려 보내줄 호스트 이름 설정

기본도메인네임(www.kcr2.pe.kr) 지정

292 DocumentRoot "/var/www/html"

가상호스트를 사용 안할 경우 기본도메인 또는 서버 아이피를 입력했을 때
보여줄 홈페이지가 있는 디렉토리

<Directory />

Options FollowSymLinks

AllowOverride None

</Directory>

디렉토리 접근 설정

아파치 서버가 접근하는 디렉토리에 대해서 어떠한 서비스나

기능을 사용할 수 있도록 허용, 거부 설정

////////////////////////////////////

웹문서 디렉토리 설정 옵션(Options)

FollowSymLinks : 디렉토리의 심볼릭 링크를 따를 것인지 결정

AllowOverride None

웹문서 디렉토리의 접근제한 설정 파일인 .htaccess 파일이 있을 경우

어떠한 설정을 재정의 할 수 있는 지를 결정

////////////////////////////////////

366 UserDir disable

373 #UserDir public_html

일반계정은 웹서버가 클라이언트에게 홈페이지를 보여주려고 할 때
일반계정 홈디렉토리 안의 public_html 을 찾아가므로 웹문서를 이 디렉토리에
저장시켜야 한다. (변경할 수 도 있다.)

402 DirectoryIndex index.html index.html.var

웹브라우저에서 www.kcr2.pe.kr(또는 192.168.x.10)이라고 입력했을 때
가장 먼저 보여줄 파일 지정

484 ErrorLog logs/error_log

에러가 나면 /etc/httpd/logs/error_log 에 저장

CustomLog logs/access_log common

웹서버에 접근한 로그 기록

ServerSignature On

시스템 메시지 출력

아파치 서버가 만들어 내는 문서들에 웹서버 버전, 가상 호스트 이름을
마지막 라인에 추가

Alias /icons/ "/var/www/icons/"

알리아스 기능

743 LanguagePriority en ca cs da de el

언어의 우선 순위 부여

759 AddDefaultCharset UTF-8

문자셋 지정(한글은 EUC-KR)

참조)

<http://httpd.apache.org/docs/2.2/>

☞ 웹서버 테스트

[first]

```
#cd /var/www/html
```

```
#vi index.html
```

---> 웹서버가 가장 먼저 찾는 파일이 index.html 이므로
파일명을 index.html 로 저장한다.

```
<html>
```

```
<body>
```

```
<br>
```

```
<center>
```

```
<h1>
```

자신의 이름 영문 이니셜

Linux Web Server


```
</h1>
```

```
<hr color=orange>
```

```
<p>
```

```
<img src=test.jpg width=600 height=400><p>
```

```
<img src=test2.jpg width=600 height=400><p>
```

```
<img src=test3.jpg width=600 height=400><p>
```

```
</center>
```

```
</body>
```

```
</html>
```

////////////////////////////////////

HTML

(Hyper Text Markup Language)

웹문서를 만드는 언어

<html> 로 시작해서 </html>로 끝남

<body></body>는 웹문서 본문 정의

 개행 태그

<h1></h1> 헤드라인 태그

<hr> 수평선 태그

 이미지 태그

<p> 문단 태그

<center></center> 중앙 정렬 태그

////////////////////////////////////

서비스 시작)

#service httpd restart

#netstat -ntlp | grep httpd

80 포트 확인

[windows]

http://리눅스아이피

<일반 사용자 홈페이지 사용하기>

주소형식)

http://아이피또는문자주소/~계정명

[first]

#cd /etc/httpd/conf

#vi httpd.conf

:set nu

아래와 같이 설정

366 #UserDir disable

373 UserDir public_html

저장후 종료

```
#service httpd restart
```

```
#cd ~apple
```

```
#pwd
```

```
/home/apple
```

```
#mkdir public_html
```

```
#cd public_html
```

```
#pwd
```

```
/home/apple/public_html
```

```
#vi index.html
```

```
<html>
```

```
<body>
```

```
<h1>
```

```
Apple's Homepage
```

```
</h1>
```

```
<h3>
```

```
Linux Web Server
```

```
</h3>
```

```
</body>
```

```
</html>
```

```
[windows]
```

```
http://리눅스아이피/~apple
```

```
--->Forbidden ?
```

```
[first]
```

```
#ps -ef | grep httpd
```

```
#cd /home
```

```
#ll
```

```
웹서버(apache 계정 사용) ---> /home/apple 디렉토리 접근
```

```
#ls -ld /home/apple
```

```
#chmod 755 /home/apple
```

```
#ls -ld /home/apple
```

```
[windows]
```

```
http://리눅스아이피/~apple
```

■PHP

▷Professional HyperText Preprocessor

▷서버에서 해석되는 HTML 에 내장되어 동작하는 스크립트 언어

▷C, JAVA, Perl 등에서 문법을 차용해 옴

▷웹브라우저 등으로 실제 코드를 볼 수 없는 보안상 이점

▷대부분의 데이터베이스 지원

[first]

▷패키지 확인 및 설치

```
#rpm -qa | grep php
```

```
#yum -y install php php-mysql
```

▷설정파일 : /etc/php.ini

▷서비스 관리 : 웹서비스 이용

PHP 는 독립적인 서비스가 아니라 웹서버가 실행시 메모리에 부품(모듈)형태로 적재시킨후 사용을 한다.

PHP 모듈

웹서버

[메모리]

```
#service httpd restart
```

```
#netstat -ntlp | grep httpd
```

▷PHP 문법

1. PHP 코드는 <?php 로 시작해서 ?> 로 끝남
2. 변수는 \$ 기호로 시작
3. 변수 선언 없이 사용가능
4. 한 문장은 ; 로 끝남
5. echo 는 출력 함수
6. 변수이름은 대소문자 구분
7. 함수이름은 대소문자 구분 안 함
8. // 는 한 줄 주석
9. 여러 줄 주석은 /* ~ */
/*

여기는 설명 1 입니다.

여기는 설명 2 입니다.

*/

예제 1)

```
#cd /var/www/html
```

```
#vi info.php
```

```
<?php
```

```
phpinfo();
```

```
//phpinfo() 는 php 정보 출력 함수
```

```
?>
```

실행방법)

웹브라우저 실행

http://아이피/info.php

예제 2)

```
#pwd
```

```
/var/www/html
```

```
#vi hello.php
```

```
<html>
```

```
<head>
```

```
<title>PHP TEST</title>
```

```
</head>
```

```
<body>
```

```
<?php
```

```
echo "<h1>Hello World</h1>";
```

```
//echo 는 PHP 출력 함수
```

```
$num1 = 100;
```

```
$num2 = 200;
```

```
echo $num1 + $num2;
```

```
?>
```

```
</body>
```

```
</html>
```

☞ PHP 처리 과정

HTML : 웹문서를 만드는 언어(동적인 처리 불가)

PHP : 웹프로그래밍 언어(동적인 처리 가능)

1. 웹브라우저가 웹서버에게 PHP 파일 요청
2. 웹서버 프로그램이 PHP 모듈에게 처리 부탁
3. PHP 모듈이 PHP 처리후 결과를 HTML 형태로 웹서버에게 전달
4. 웹서버가 웹브라우저에게 결과를 전달
5. 결과적으로 웹브라우저에서는 PHP 코드는 안 보이고 HTML 형태만 보임

[웹서버]

[웹브라우저]

Apache + PHP

<http://리눅스아이피/hello.php>

PHP 모듈

웹서버 데몬

[웹서버 메모리]

예제 3)

#pwd

/var/www/html

#vi for.php

<?php

for(\$i=1;\$i<=9;\$i++) {

 \$result=2 * \$i;

 echo "2 x \$i = \$result
";

}

?>

////////////////////////////////////

for 문은 반복문(조건을 만족 할 때까지 반복)

for(초기치 ; 조건 ; 증감식) {

 문장;

}

실행순서 : 조건을 만족할 때 까지 반복

1)초기치

2)조건

3)문장

4)증감식

5)조건

6)문장

....

////////////////////////////////////

■실습

아래와 같은 홈페이지가 출력되도록 두번째리눅스 웹서버 구축

1. http://두번째리눅스아이피

2. http://두번째리눅스아이피/~itbank

3. http://두번째리눅스아이피/gugudan.php

---> 구구단 9 단 출력

itbank 계정을 추가후 홈페이지를 만들어야 함

■MySQL

▷데이타베이스 :

자료를 효율적으로 저장하는 공간

table 단위

▷DBMS :

데이타베이스를 관리하는 시스템

사용자 <-----> Application <-----> DBMS <-----> 데이타베이스

▷DBMS 종류

1. MySQL

공개형 오픈소스 데이타베이스

중소형급의 강력한 DB 서버

PHP 및 각종 언어와 연결이 쉽고 간편

2. Oracle, SQL Server

엔터프라이즈급의 대형 DB 서버

////////////////////////////////////

Table(테이블) 자료 형태)

번호	이름	이메일	주소	전화번호
1	aaa	aaa@aa.com	Seoul	11-22-33
2	bbb	bbb@aa.com	Pusan	11-22-44
3	ccc	ccc@aa.com	Daegu	11-22-55

레코드 : 한 행(라인, 줄) 을 의미

컬럼(column) : 열(각 라인의 항목) 을 의미, 필드(field) 라고도 함

////////////////////////////////////

[first]

```
#rpm -qa | grep mysql-server
```

---> 서버 프로그램 확인

프로그램 없으면 yum 으로 설치

```
#yum -y install mysql-server
```

▷설정 파일 : /etc/my.cnf

▷서비스 시작

```
#service mysqld start
```

```
#netstat -ntlp | grep mysqld
```

3306 포트 확인

▷MySQL 접속

mysql : mysql 서버에 접속하는 클라이언트 명령어 프로그램

```
mysql -u 사용자 -p 또는 mysql -u사용자 -p암호
```

[first]

```
#mysql -u root -p
```

암호는 엔터 입력

--->여기서 root 는 MySQL 관리자 계정을 의미

--->리눅스 시스템의 관리자 계정 root 가 아님

ctrl + l(엘) ---> 화면 clear

▷MySQL 접속 끊기

```
mysql>quit
```

▷버전 및 날짜 확인

```
mysql>select version(), current_date();
```

▷데이터베이스 목록 보기

```
mysql>show databases;
```

▷데이터베이스 생성

```
mysql>create database 디비이름;
```

(이름은 한글 사용 불가)

```
mysql>create database linux1;
```

```
mysql>create database linux2;
```

```
mysql>show databases;
```

▷데이터베이스 삭제

```
mysql>drop database 디비이름;
```

```
mysql>drop database linux1;
```

```
mysql>show databases;
```

▷데이터베이스 선택

```
mysql>use 디비이름;
```

```
mysql>use linux2;
```

```
mysql>select database();
```

```
mysql>show tables;
```

테이블 예)

bbs1 ---> 테이블 이름

번호 이름 ---> 필드 이름(field name) 또는 컬럼 이름(column name)

1	apple
2	banana

bbs2

번호	이름	이메일	내용
1	apple	apple@a.com	test
2	banana	banana@b.com	test2

▷테이블 생성

mysql>create table 테이블이름(필드이름 자료형, 필드이름2 자료형 ...);

(테이블 이름 한글사용 불가)

mysql>create table bbs1(num int, name varchar(20));

mysql>create table bbs2(num int not null auto_increment primary key,
name varchar(20),
email varchar(30),
content varchar(50));

mysql>show tables;

////////////////////////////////////
/////

MySQL 자료형)

int : 숫자(정수) 를 의미하는 자료형

not null : 널값 허용 안함

auto_increment : 자동 증가 속성

primary key : 중복방지 속성

num int not null auto_increment primary 는 숫자가 자동으로 증가하는 설정

varchar : 가변길이 문자형, varchar(10) 은 최대 10문자 까지 입력받을 수 있다는 의미

////////////////////////////////////
/////

bbs1

num	name

1	apple
2	orange

▷테이블 구조 확인

```
mysql>show tables;
```

```
mysql>desc bbs1;
```

```
mysql>explain bbs1;
```

▷레코드(자료) 입력

```
mysql>insert into 테이블이름 values(값1, 값2 ...);
```

```
mysql>insert into bbs1 values(1,'apple');
```

```
mysql>insert into bbs1 values(2,'banana');
```

숫자는 그대로 사용하고 문자열은 작은따옴표로 감싸 주어야 한다.

▷자료 검색

```
mysql>select * from 테이블이름;
```

```
mysql>select * from bbs1;
```

```
mysql>select num from bbs1;
```

▷레코드(자료) 수정

```
mysql>update 테이블이름 set 필드이름=수정값, 필드이름2=수정값 ... where 조건;
```

```
mysql>update bbs1 set name='candy' where num=2;
```

---> where 절이 없으면 모든 행이 수정 됨

```
mysql>select * from bbs1;
```

▷레코드(자료) 삭제

```
mysql>delete from 테이블이름 where 조건;
```

```
mysql>delete from bbs1 where num=1;
```

---> where 절이 없으면 모든 행이 삭제 됨

```
mysql>select * from bbs1;
```

▷테이블 삭제

```
mysql>drop table 테이블이름;
```

```
mysql>drop table bbs1;
```

```
mysql>show tables;
```

▷MySQL 루트 암호 설정

```
mysql>quit
```

```
#mysqladmin -uroot password '1234'
```

---> mysql 관리자 계정 root 의 암호를 1234 로 설정

```
#mysql -uroot -p
```

암호입력

■실습 준비

수업용 FTP 서버 120.UPLOAD2 폴더 에서 zb4p19.zip 파일을 /var/www/html 에 다운받기

[first]

```
mysql>quit
```

```
#yum -y install ftp
```

```
#cd /var/www/html
```

```
#ftp 서버아이피
```

Name : 아이디

Password : 암호

```
ftp>cd 120.UPLOAD2
```

```
ftp>mget zb*
```

```
ftp>by
```

```
#
```

■Zero Board

오픈 소스 게시판

1)

[first]

```
#cd /var/www/html
#unzip zb4pl9.zip
--->압축 해제
```

```
#service mysqld restart
```

```
////////////////////////////////////
MySQL 루트 암호 설정 확인
#mysqladmin -uroot password '1234'
---> mysql 접속 계정 root 의 암호를 1234 로 설정
```

```
////////////////////////////////////
```

```
#mysql -uroot -p
암호입력
```

```
mysql>create database zero_board;
mysql>show databases;
mysql>quit
```

2)

[first]

```
#service httpd restart
```

[windows]

웹브라우저 실행

<http://첫번째리눅스아이피/bbs/install.php>

위의 화면에서 글자가 깨질 경우

아래처럼 웹서버의 언어 설정을 변경하고

제로보드 설치시 파일이 생성될 수 있도록 디렉토리 쓰기 권한 설정을 해 준다.

[first]

```
#vi /etc/httpd/conf/httpd.conf
```

httpd.conf 의 759 라인 UTF-8 을 EUC-KR 로 변경

```
759 AddDefaultCharset EUC-KR
```



```
#vi /etc/php.ini
아래 항목 On 으로 설정
229 short_open_tag = On
693 register_globals = On
703 register_long_arrays = On

#service httpd restart

#chmod 707 /var/www/html/bbs
```

3)
<http://첫번째리눅스아이피/bbs/install.php>
[v]라이선스 동의 체크
{설치 시작} 클릭

MySQL DB 설정)
Host Name : localhost
SQL User ID : root
Password : 1234
DB Name : zero_board

{설정 완료} 클릭

4)
관리자 정보(제로보드 관리자 설정 정보 입력)
ID : admin
Password : 1234
Confirm password : 1234
Name : andylec

{정보 입력 완료} 클릭

5)
관리자 로그인
<http://첫번째리눅스아이피/bbs/admin.php>

User ID : admin
Password : 1234

6)

관리자 화면

왼쪽의 [새 그룹 추가] 클릭

그룹 이름 : Test

오른쪽 하단 Confirm 클릭

왼쪽 메뉴

[게시판 관리 | 추가]

--->추가 클릭

게시판 이름 : linux

오른쪽 하단 Confirm 클릭

[first]

```
#mysql -uroot -p
```

```
mysql>use zero_board;
```

```
mysql>show tables;
```

```
mysql>select * from zetyx_board_linux;
```

```
mysql> select no,name,subject,ip from zetyx_board_linux;
```

```
+-----+-----+-----+-----+
```

```
| no | name | subject | ip |
```

```
+-----+-----+-----+-----+
```

```
| 1 | andy | test | 192.168.1.1 |
```

```
| 2 | andy | test | 192.168.1.1 |
```

```
| 3 | andy | test3 | 192.168.1.1 |
```

```
+-----+-----+-----+-----+
```

```
3 rows in set (0.00 sec)
```

```
mysql>
```

■실습

second 리눅스에 APM 서버 구축 및 제로보드 설치

////////////////////////////////////

[second]

1)프로그램 설치

```
#yum -y install php php-mysql mysql-server
```

2)설정 변경

```
#vi /etc/httpd/conf/httpd.conf
```

```
292 DocumentRoot "/var/www/html"
```

```
759 AddDefaultCharset EUC-KR
```

```
#vi /etc/php.ini
```

```
229 번 라인 On 으로 설정
```

```
693, 703 라인 On 설정 확인
```

```
229 short_open_tag = On
```

```
693 register_globals = On
```

```
703 register_long_arrays = On
```

3)서비스 시작

```
#service httpd restart
```

```
#service mysqld restart
```

4)암호 변경

```
#mysqladmin -uroot password '1234'
```

---> mysql 접속 계정 root 의 암호를 1234 로 설정

5)제로보드용 데이터베이스 생성

```
#mysql -uroot -p
```

```
mysql>create database zero_board;
```

```
mysql>show databases;
```

```
mysql>quit
```

6)제로보드 다운

```
#cd /var/www/html
```

제로보드 다운

```
#unzip zb4pl9.zip
```

--->압축 해제

```
#chmod 707 /var/www/html/bbs
```

7)제로보드 설치

<http://두번째리눅스아이피/bbs/install.php>

////////////////////////////////////

[ITBANK Andylec 주말 리눅스 2 과정]

■오늘의 수업내용(7일차)

DNS

■Domain Name Service(DNS)

인터넷에 있는 서버의 아이피를 기억하기는 어려우므로
문자주소를 사용한다.

그러나 실제 컴퓨터는 아이피 주소로 통신을 하므로
네임서버에서 문자주소를 아이피로 변경해 주어야 한다.

DNS 서비스란 ?

문자주소를 아이피 주소로

또는

아이피 주소를 문자주소로 변환 시켜주는 서비스

DNS 서비스를 하는 컴퓨터를 네임서버(Name Server)

또는 DNS 서버라고 한다.

www.andylec.com ---> IP : 정방향 설정(문자 주소 ---> 아이피 주소)

IP ---> www.andylec.com : 역방향 설정(아이피 주소 ---> 문자 주소)

■FQDN

호스트 이름과 도메인을 함께 표기하여 시스템을 지칭하는 완전한 이름

FQDN(Fully Qualified Domain Name) : www.andylec.com

www ---> 호스트 네임(host name)

andylec.com ---> 도메인 네임(domain name)

[ns.andylec.com] [ftp.andylec.com] [www.andylec.com]

192.168.0.10 192.168.0.20 192.168.0.30

andylec.com

■DNS UTIL

nslookup, dig : DNS lookup utility

nslookup 은 DNS query(질의하다) 유틸리티 명령어

```
////////////////////////////////////
```

```
#man nslookup
```

```
NSLOOKUP(1)
```

```
NAME
```

```
nslookup - query Internet name servers interactively
```

```
////////////////////////////////////
```

```
[first]
```

```
#nslookup
```

```
>www.nice.co.kr
```

```
>exit
```

```
#nslookup www.nice.co.kr
```

```
#nslookup ns.nice.co.kr
```

```
#dig
```

```
---> 루트 네임서버 목록이 출력 됨
```

```
#dig www.nice.co.kr
```

```
dig @네임서버 문자주소 타입(ANY,A,MX 등)
```

```
#dig @168.126.63.1 www.nice.co.kr A
```

■도메인체계-tree 구조(분산구조)

www.andylec.com

. 루트도메인
|
com 1차 도메인
|
andylec 2차 도메인
|
www 3차 도메인

1. 도메인 주소(문자주소)는 대소문자 구분 안 함
2. 네임서버 설정 파일의 단어(레코드)도 대소문자 구분 안 하지만 알아보기 쉽도록 보통 대문자 사용

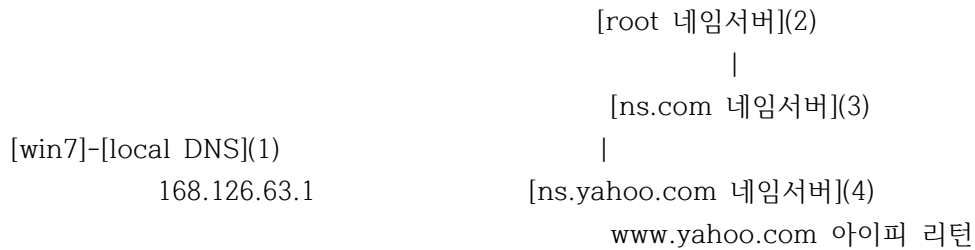
. (루트 도메인, 루트 네임서버)
|
+-----+-----+-----+-----+
com net kr jp

▷ win7 웹브라우저에서 www.yahoo.com 이라고 입력했을 때 아이피가 변환되는 과정

1. 네임서버로 지정된 168.126.63.1 서버에 query
2. 네임서버는 자신이 데이터를 갖고있지 않다면 루트 네임서버에게 ns.com 서버를 query

루트네임서버에는 com 네임서버, net 네임서버등의 목록을 갖고있다.
ns.com 네임서버는 com으로 끝나는 네임서버 목록을 갖고 있다.
ns 는 네임서버를 뜻함

3. ns.com 은 ns.yahoo.com 의 아이피를 리턴
4. ns.yahoo.com 네임서버는 yahoo.com으로 끝나는 목록(www.yahoo.com, ftp.yahoo.com ..)을 갖고 있다.
그 중에 www.yahoo.com 이 200.200.200.200 이라면 클라이언트한테 그 아이피를 리턴한다.
5. 클라이언트는 200.200.200.200 아이피를 가지고 서버를 찾아간다.



리눅스의 경우 /etc/resolv.conf 에 설정된 네임서버가 local DNS 가 된다.

■네임서버 설정 파일 주요 항목

1) /etc/named.conf

```
options {
    directory "/var/named"; ---> 존파일을 저장할 디렉토리
};
```

```
zone "." IN {
    type hint;
    file "named.ca";
};
```

--->zone은 도메인을 구분하는 단위

--->zone 이 . 이면 루트 네임서버를 뜻한다.

--->type 은 루트네임서버인지, 1차 네임서버인지, 2차 네임서버인지를 지정한다.

hint // 루트네임서버

master // 1차 네임서버

slave // 2차 네임서버 ---> 1차 서버의 자료를 Copy 해서 저장

---> master , slave 는 리눅스 가상머신의 이름이 아님

--->file "named.ca" 는 루트 네임서버의 목록을 저장하고 있는
파일이 named.ca 라는 의미

2) /etc/named.rfc1912.zones

☞정방향 설정 : 문자주소를 아이피로 변환할 때 사용하는 설정
(여러 개 설정할 수 있다.)


```
zone "kcr2.pe.kr" IN { ---> 정방향 설정
    type master;
    file "kcr2.zone"; ---> kcr2.pe.kr 도메인 설정을
                        저장할 파일이름이
                        /var/named 에 존재해야 한다.
    allow-update { none; }; ---> 외부 업데이트 금지
};
```

☞역방향 설정 : 아이피를 문자주소로 변환할 때 사용하는 설정
(1개만 설정할 수 있다.)
자신의 아이피대역을 거꾸로 등록

아이피가 192.168.30.10 이면
10.30.168.192.in-addr.arpa 로 등록(CentOS 6 버전 기준)

```
zone "x.x.x.x.in-addr.arpa" IN { ---> 역방향 설정
    type master;
    file "kcr2.rev"; ---> 역방향 설정을 저장할 파일명
    allow-update { none; };
};
```

■존파일의 레코드 설명

1) kcr2.zone 파일

\$TTL 86400 ---> TTL
(Time to Live, DNS 데이터의 수명, 초단위, 86400은 하루)

24시간*60분*60초=86400

@ IN SOA ns.kcr2.pe.kr. root.ns.kcr2.pe.kr. (

--->@ // Origin 도메인을 의미
--->IN // Internet Class
--->SOA // Start Of Authority, 관리도메인 지정
--->ns.kcr2.pe.kr. 에서 마지막의 점은 루트 도메인을 의미
--->root.ns.kcr2.pe.kr. 관리자 이메일을 뜻함
--->root@ns.kcr2.pe.kr 을 root.ns.kcr2.pe.kr. 으로 표시

세미콜론은 주석을 뜻함

년도월일 ; serial ---> 일련번호, 보통 날짜 지정

3H ; refresh ---> 2차 네임서버가 1차 네임서버 데이터를
재확인할 시간 간격
3H는 3시간(Hour)

15M ; retry ---> 1차 네임서버가 다운시 2차 네임서버가
접속을 시도할 시간간격
15M은 15분(Minute)

1W ; expiry ---> dns 데이터 만료기간(1차 네임서버가 다운시
2차 네임서버가 데이터를 사용할 기간)
1W 는 1주일(Week)

1D) ; minimum ---> negative caching ttl, NXDOMAIN 정보를 캐시에 저장할 시간, 1D
는 하루(Day)

NXDOMAIN : no-such-domain, 조회한 도메인의 정보가 없을 때 받게 되는 응답(존재하지
않는 도메인)

IN NS ns.kcr2.pe.kr.

---> NS 는 네임서버 지정(A 레코드로 아이피를 지정해 주어야 한다.)

IN A x.x.x.x

---> A는 address, A 다음에는 반드시 아이피가 나와야 한다.

ns IN A x.x.x.x

www IN A x.x.x.x

--->클라이언트가 www.kcr2.pe.kr 를 query 하면
아이피 x.x.x.x 를 리턴

2) kcr2.rev 파일

\$TTL 86400

@ IN SOA ns.kcr2.pe.kr. root.ns.kcr2.pe.kr. (

년도월일 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H) ; minimum

--->정방향 설정과 동일한 의미

```
NS      @
A        x.x.x.x
PTR     ns.kcr2.pe.kr.
```

---> 역방향 설정에서는 PTR(포인터 레코드) 다음에 문자주소를 적는다.

nslookup 으로 x.x.x.x 를 query 하면
ns.kcr2.pe.kr 을 리턴한다.

■테스트 시나리오

first 리눅스 서버를 네임서버로 만들고
www.kcr2.pe.kr 을 입력하면 first 리눅스의 아이피가 출력되게 한다.

리눅스의 네임서버 : BIND

네임서버 설정파일

1. /etc/named.conf
2. /etc/named.rfc1912.zones
3. /var/named 디렉토리의 존파일들

데몬 스크립트 : /etc/init.d/named

--->네임서버 시작 및 종료 시키는 파일

네임서버 포트 : 53

(참고)

자신의 리눅스 아이피를적어서 테스트해야 함

■네임서버 설정하기

[first]

패키지 확인 및 설치

```
#rpm -qa | grep "^bind"
```

bind-utils

bind-libs

```
#yum -y install bind bind-devel
```

1. /etc/named.conf 수정하기(접근제한 설정 해제)

```
#vi /etc/named.conf
```

```
10 options {
11     listen-on port 53 { any; }; // 수정
12     listen-on-v6 port 53 { ::1; };
13     directory "/var/named";
14     dump-file "/var/named/data/cache_dump.db";
15     statistics-file "/var/named/data/named_stats.txt";
16     memstatistics-file "/var/named/data/named_mem_stats.txt";
17     allow-query { any; }; // 수정
```

2. named.rfc1912.zones 수정하기

```
#vi /etc/named.rfc1912.zones
```

---> 기존내용은 그대로 두고 마지막에 아래 내용 추가
버전에 따라 라인 번호는 차이가 날 수 있음

```
43 zone "kcr2.pe.kr" IN {
44     type master;
45     file "kcr2.zone";
46     allow-update { none; };
47 };
48
49 zone "x.x.x.x.in-addr.arpa" IN {
50     type master;
51     file "kcr2.rev";
52     allow-update { none; };
53 };
```

```
////////////////////////////////////
43번 라인에서 www.kcr2.pe.kr 로 적으면 안 됨
49번 라인에서 리눅스 아이피가 192.168.30.10 이면
10.30.168.192.in-addr.arpa 로 적어야 한다.
////////////////////////////////////
```

3. 존파일 생성하기

존(zone) : 도메인 구분단위(kcr2.pe.kr, andylec.com)

```
#cd /var/named
#pwd
/var/named
#ls
```

```
#vi kcr2.zone
```

(kcr2.zone 파일명은 /etc/named.rfc1912.zones 의 존설정에서
file 다음에 지정해 준 이름으로 생성해야 한다.

file "kcr2.zone"; ---> /etc/named.rfc1912.zones 의 설정내용)

왼쪽의 숫자는 라인번호로 타이핑하지 않는다.

년도월일 은 한글로 적는 것이 아니고 현재날짜를 적으면 된다.

```
1 $TTL 86400
2 @ IN SOA ns.kcr2.pe.kr. root.ns.kcr2.pe.kr. (
3                                     20140125 ; serial
4                                     3H      ; refresh
5                                     15M     ; retry
6                                     1W      ; expiry
7                                     1D )    ; minimum
8     IN NS ns.kcr2.pe.kr.
9     IN A  x.x.x.x
10 ns  IN  A  x.x.x.x
11 www  IN  A  x.x.x.x
12 ftp  IN  A  x.x.x.x
////////////////////////////////////
---> 리눅스 아이피가 192.168.30.5 이면 x.x.x.x 에 192.168.30.5 를 적는다.
---> ; 은 주석을 의미한다.
---> 1W ; expiry 에서 W 는 영문대문자(1 Week)
---> 7번 라인에서 1D 는 숫자 1, 영문 대문자 D
---> IN NS ns.kcr2.pe.kr. 라인(8번~9번 라인)은 반드시 공백으로 시작해야 한다.
---> ns IN A x.x.x.x 라인(10번~12번 라인)은 적을 때 공백으로 시작하면 안 된다.
////////////////////////////////////
```

named-checkzone : 존파일 설정 체크 명령어

형식)

named-checkzone 도메인 존파일명

```
#pwd
/var/named
#named-checkzone kcr2.pe.kr kcr2.zone
```

```
#pwd
/var/named
(경로 확인)
```

```
#vi kcr2.rev
$TTL 86400
@ IN SOA ns.kcr2.pe.kr. root.ns.kcr2.pe.kr. (
                                20140125 ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum

    NS      @
    A       x.x.x.x
    PTR     ns.kcr2.pe.kr.
```

////////////////////////////////////

x.x.x.x 에는 리눅스아이피를 적는다.(거꾸로 적는 것이 아님)

A 다음에는 네임서버로 설정하고 있는 리눅스 아이피 적기

파일 작성할 때 공백 주기

////////////////////////////////////

```
#pwd
/var/named
#named-checkzone kcr2.pe.kr kcr2.rev
존파일 체크하기
```

4. 소유권 변경

```
#pwd
/var/named
#chmod 660 /var/named/kcr2*
#chown root:named /var/named/kcr2*
#ls -l
```

🖨️named-checkconf : 네임서버 주설정파일 체크 명령어

```
////////////////////////////////////  
#man named-checkconf  
  
NAME  
named-checkconf - named configuration file syntax checking tool  
  
-z Perform a check load the master zonefiles found in named.conf.  
////////////////////////////////////  
  
#named-checkconf -z /etc/named.conf
```

5. 네임서버 테스트

- 1)DNS 클라이언트 설정 파일 변경(/etc/resolv.conf)
- 2)네임서버 시작
- 3)nslookup 으로 테스트

```
////////////////////////////////////  
본사  
|  
서울지사                대구지사                부산지사  
|  
서울강남지점  서울강북지점
```

[고객이사는동네상점]-----고객

```
////////////////////////////////////
```

[first]

```
#vi /etc/resolv.conf
```

```
nameserver 192.168.x.10(---> 첫번째리눅스의 아이피를 적는다.)
```

```
nameserver 168.126.63.1
```

```
#service named restart
```

```
#netstat -ntlp | grep named  
---> 네임서버는 53번 포트를 사용함
```

```
#cat /etc/services | grep domain  
domain          53/tcp          # name-domain server  
domain          53/udp
```

```
#ps -ef | grep named  
---> 메모리에 실행된 네임서버 검색
```

```
테스트 1)  
[first]  
#nslookup www.kcr2.pe.kr  
#nslookup 192.168.x.10  
--->첫번째리눅스의 아이피 입력
```

```
테스트 2)  
[first]  
#service httpd restart  
#netstat -ntlp | grep httpd
```

[first]	[2003]
웹서버	웹브라우저
네임서버	
192.168.x.10	

```
[win2003]  
네트워크 설정에서 네임서버를 첫번째리눅스 아이피 192.168.x.10 으로 변경  
웹브라우저  
http://www.kcr2.pe.kr
```

```
[second]  
#vi /etc/resolv.conf  
  
nameserver 192.168.x.10 (---> 첫번째리눅스 아이피로 설정)  
nameserver 168.126.63.1
```

```
#nslookup www.kcr2.pe.kr
```


second 리눅스 웹브라우저 실행후
http://www.kcr2.pe.kr 입력해서 홈페이지 출력 확인

테스트 3)

[first]	[second]	[win2003]
네임서버	웹서버	클라이언트
192.168.x.10	192.168.x.20	

```
[first]
#cd /var/named
#vi kcr2.zone
```

```
www IN A 192.168.x.20
---> 위와 같이 변경
```

```
#service named restart
#nslookup www.kcr2.pe.kr
---> 두번째리눅스 아이피 출력 확인
```

```
[second]
#cd /var/www/html
#vi index.html
<html>
<body>
<h1>
Second Linux Web Server <br>
IP : 192.168.x.20 <br>
</h1>
</body>
</html>
```

```
/etc/httpd/conf/httpd.conf 파일의 292 번 라인 확인
292 DocumentRoot "/var/www/html"
```

```
#service httpd restart
```

[win2003]

웹브라우저 실행후 http://www.kcr2.pe.kr 입력
두번째리눅스 홈페이지가 나와야 정상
첫번째리눅스홈페이지가 나오면
도스창 실행(시작-실행-cmd)후 아래 입력후 테스트
C:\>ipconfig /flushdns

■실습

second 리눅스 네임서버에 자신의 도메인을 설정
(자신의 영문이름이니셜 또는 자신의 닉네임 사용)

nslookup 으로 테스트하면 second 리눅스 아이피가 리턴되도록 설정하시오
--->정방향 설정(zone "kcr2.pe.kr")은 여러 개 할 수 있고
역방향 설정(zone "x.x.x.x.in-addr.arpa")은 하나만 할 수 있다.

#nslookup 자신의도메인

////////////////////////////////////
-네임서버 패키지 확인 및 설치
-접근제한 해제
-존 등록(/etc/named.rfc1912.zones)
-존 파일 생성(/var/named 폴더 안)
-소유권 변경(#chown root:named 존파일)
-네임서버 시작
-/etc/resolv.conf 변경
-nslookup 으로 테스트
////////////////////////////////////

■가상호스트 실습준비

[first]

#netstat -ntlp | grep named
53 번 포트확인하고 없으면 서비스 시작시키기
#service named restart

#nslookup www.kcr2.pe.kr

아이피 출력되는지 확인
---> 첫번째리눅스 아이피가 출력되도록 수정

/etc/resolv.conf 에서 아래 내용 확인

nameserver 첫번째리눅스아이피

nameserver 168.126.63.1

#vi /etc/named.rfc1912.zones

andylec2.net 존 설정 확인

zone "kcr2.pe.kr" IN { ---> 없으면 추가하기

type master;

file "kcr2.zone";

allow-update { none; };

};

zone "x.x.x.x.in-addr.arpa" { ---> 새로 추가하면 안 됨, x.x.x.x.in-addr.arpa 설정은 하나만 있어야 한다.

type master;

file "kcr2.rev";

allow-update { none; };

};

zone "andylec2.net" IN { ---> 없으면 마지막 부분에 새로 추가하기

type master;

file "andylec2.zone";

allow-update { none; };

};

#cd /var/named

#ls

andylec2.zone 파일 있으면 아래 명령 생략

////////////////////////////////////

#cp kcr2.zone andylec2.zone

#vi andylec2.zone

:%s/kcr2.pe.kr/andylec2.net/g (--->vi 치환기능 사용)

--->kcr2.pe.kr 을 andylec2.net 으로 치환하고 저장후 종료하기

#chown root:named andylec2.zone

---> 소유권 변경

////////////////////////////////////

```
#service named restart
```

```
#cat /etc/resolv.conf
```

```
nameserver 첫번째리눅스아이피
```

```
nameserver 168.126.63.1
```

--->위와 같은지 확인

설정후 테스트 결과

```
#nslookup www.andylec2.net
```

---> 첫번째리눅스 아이피 출력 확인

```
#nslookup www.kcr2.pe.kr
```

---> 첫번째리눅스 아이피 출력 확인

---> 두번째리눅스 아이피로 나오면 첫번째리눅스 아이피로 변경

■가상호스트(VirtualHost)란 ?

호스트는 컴퓨터를 뜻하며 가상으로 컴퓨터가 여러 개 있는 효과를 내는 웹서버의 기능을 가상호스트 기능이라 한다.

회사에서 운영하려고 하는 홈페이지가 2 개이고 서버가 2대이면

각 서버에 서로 다른 홈페이지가 나오도록 설정할 수 있지만

서버가 한 대 이어도 가상호스트를 이용하면 서버가

2대 인 것처럼 홈페이지를 여러 개 운영할 수 있다.

실제 웹호스팅 업체에서 사용되고 있는 방식이다.

◆서버가 2 대일 때

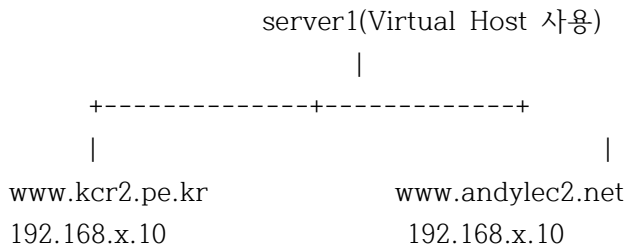
[server1]

[server2]

www.kcr2.pe.kr

www.andylec2.net

◆서버가 1대이고 가상호스트 이용할 때



두 도메인에 대해서 서로 다른 디렉토리를
찾아갈 수 있도록 웹서버가 지원한다.
네임서버는 두 도메인 대해서 server1 의 아이피가
동일하게 리턴되도록 설정되어 있어야 한다.

◆가상호스트 설정하기

[first]

```
#cd /etc/httpd/conf
```

```
#vi httpd.conf
```

shift + g 를 누르면 마지막 라인으로 이동한다.

라인번호는 차이가 날 수 있으므로 내용을 확인해서 수정하기

991 라인을 # 제거후 아래와 같이 수정하기

```
991 NameVirtualHost 192.168.x.10
```

```
////////////////////////////////////
```

--->#을 제거하고 첫번째리눅스 아이피를 적는다.

--->192.168.0.10:80 으로 적으면 하위 설정에서도 동일하게 적어야 한다.

```
////////////////////////////////////
```

마지막 라인에 아래 추가

```
<VirtualHost 192.168.x.10>
```

```
    ServerName www.kcr2.pe.kr
```

```
</VirtualHost>
```

```
<VirtualHost 192.168.x.10>
```

```
    ServerAdmin root@ns.andylec2.net
```

```
    DocumentRoot /home/polo/public_html
```

```
    ServerName www.andylec2.net
```

```
    ErrorLog logs/www.andylec2.net-error_log
```

```
CustomLog      logs/www.andylec2.net-access_log  common
</VirtualHost>
////////////////////////////////////////////////////////////
--->ErrorLog 와 CustomLog 다음에는 log 가 아니고 logs 로 적어야 한다.
    ErrorLog, CustomLog 에서 logs 는 rpm 버전일 때
    /etc/httpd/logs(=> /var/log/httpd) 디렉토리를 뜻한다.
    그러므로 log/www.andylec2.net-error_log 라고 적으면
    로그파일을 만들 수 없어서 웹서버가 시작되지 않는다.
////////////////////////////////////////////////////////////
```

```
#cd /etc/httpd
#ls
conf  conf.d  logs  modules  run
#ll
lrwxrwxrwx  1 root root   19  2월 12 09:45 logs -> ../../var/log/httpd
```

(/etc/httpd/logs 는 실제로는 /var/log/httpd 디렉토리이다.)

◆가상호스트 설정 설명

```
NameVirtualHost x.x.x.x
---> 가상호스트 사용할 아이피 지정
---> 가상호스트의 네임서버 역할
---> 이 설정이 없으면 이름 기반 가상호스트가 적용 안 됨
```

```
<VirtualHost x.x.x.x>
    ServerName www.kcr2.pe.kr
</VirtualHost>
---> 기본 도메인에 대한 가상호스트 설정(Default 설정)
---> /var/www/html 를 찾아감
---> 이 설정이 없으면 아래 가상호스트와 똑같이 나온다.
---> 첫번째 적은 도메인 주소가 디폴트로 설정 됨
```

```
<VirtualHost x.x.x.x> ---> 가상호스트 설정 시작
ServerAdmin root@ns.andylec2.net
---> 관리자 이메일 지정
```

DocumentRoot /home/polo/public_html

---> 홈페이지 문서가 저장된 디렉토리 지정

ServerName www.andylec2.net

---> 가상호스트 적용할 도메인 지정

즉 www.andylec2.net 을 요청받으면 DocumentRoot 로 찾아가서
웹페이지를 보여준다.

ErrorLog logs/www.andylec2.net-error_log

---> 에러를 기록할 파일지정

/var/log/httpd 에 저장됨

CustomLog logs/www.andylec2.net-access_log common

---> 정상적인 접속을 기록할 파일 지정, common 은 로그타입을 의미

</VirtualHost> ---> 가상호스트 설정 끝

■테스트 계정 및 홈페이지 생성하기

#adduser polo

#cd ~polo

#cd public_html (디렉토리 없으면 #mkdir public_html 입력해서 생성하기)

#pwd

/home/polo/public_html

#ls

index.html

#vi index.html

1 <html>

2 <body>

3 <h1>

4 <i>

5 Polo's Homepage

6 </i>

7 </h1>

8 www.andylec2.net

9 </body>

10 </html>

---> 왼쪽 숫자는 라인 번호이므로 타이핑하지 않는다.

#apachectl configtest

Syntax OK ---> 문법 검사 결과 OK

```
#apachectl -S
```

--->가상호스트 설정 확인(OK 로 출력되어야 함)

```
#service httpd restart
```

■ 테스트 환경

```
[first] <-----> [second]
```

웹서버 클라이언트(웹브라우저)

네임서버

www.kcr2.pe.kr

www.andylec2.net

[second]

```
#vi /etc/resolv.conf
```

nameserver x.x.x.x (---> first 리눅스의 아이피로 변경)

```
nameserver 168.126.63.1
```

```
#nslookup www.kcr2.pe.kr
```

```
#nslookup www.andylec2.net
```

second 리눅스 웹브라우저 실행(/etc/resolv.conf 변경후 테스트)

<http://www.kcr2.pe.kr>

<http://www.andylec2.net>

--->Forbidden 으로 출력되면 first 리눅스에서 아래 명령 실행 후 테스트

```
#chmod 755 /home/polo
```

--->똑같이 보인다면 새로고침 버튼을 눌러본다.

(그래도 똑같이 나온다면 가상호스트 설정이 잘못된 것이다.)

[ITBANK Andylec 주말 리눅스 2 과정]

■오늘의 수업내용(8일차)

로그(Log)

방화벽(Firewall)

■로그란?

- 시스템에 접속한 사용자들의 행위들을 저장해 놓은 기록
- 시스템에서 발생한 메시지들의 기록
- 문제 발생시 그 해결 방안을 제시해 주는 가장 기본적인 자료

■로그 분석의 필요성

1. 시스템의 오류나 사용자의 취향 등을 분석할 수 있는 정보제공
2. 보안 사고 발생시 추적자료
3. 문제 발생 전 사전 징후 포착
4. 로그 분석을 위해

로그 파일의 경로,

로그 파일명,

로그 파일을 확인하는 명령어 를 알 필요가 있다.

■리눅스 로그

<rsyslog>

rsyslog

시스템 로깅을 담당하는 데몬

로깅 데몬 : rsyslogd

데몬스크립트 : /etc/init.d/rsyslog

로깅 데몬 설정 파일 : /etc/rsyslog.conf

---> 주요 시스템 로그 파일의 위치를 지정

리눅스 시스템 대부분의 로그파일 저장되어 있는 디렉토리 : /var/log

#ls /var/log

messages : 시스템 운영에 대한 전반적인 메시지 저장

secure : 사용자들의 원격로그인 정보기록

maillog : 메일과 관련된 기록

cron : 시스템 정기 작업에 대한 로그
boot.log : 부팅 관련 메시지를 기록
---> 위 파일들은 /etc/rsyslog.conf 에 등록된 로그 파일

```
#cat /var/log/messages
#tail /var/log/messages
#tail /var/log/secure
#tail /var/log/maillog
#tail /var/log/cron
```

rsyslog 처리 과정)

- 1)서비스 ---> 메시지 발생
- 2)rsyslogd ---> 설정 파일에 따라 메시지 기록

```
#ps -ef | grep syslog
#ls /etc/init.d/rsys*
```

```
#egrep 'log|Level' --color /etc/ssh/sshd_config
SyslogFacility AUTHPRIV
#LogLevel INFO
```

---> SSH 접속시 로그메시지를 발생시키는 설정

```
#cat /etc/rsyslog.conf
```

- 1) rsyslog.conf 설정형식

Facility.Level	logfile-location
(a) (b)	(c)

--->a에 대하여 b의 경우에 해당하는 로그 메시지가 발생하였을 때에
c에 그 기록을 저장하라는 의미
모든 Facility 와 모든 Level 를 나타낼 때는 * 를 사용하고
여러 메시지를 기록할 때는 ; 로 메시지를 구분해 준다.

- 2) Facility 종류(로그메시지를 발생시키는 개체)

```
#man 3 syslog
```

auth

로그인과 같이 사용자 인증에 관한 메시지

authpriv(현재는 auth 대신에 authpriv 를 사용)

로그인과 같이 사용자 인증에 관한 메시지

cron

cron 데몬, at 데몬에 의해 발생하는 메시지

daemon

telnet,ftp 데몬에 의한 메시지

kern

kernel 에 의한 메시지

lpr

프린터 데몬인 lpd 에 의한 메시지

mail

sendmail 등의 메일에 의한 메시지

news

뉴스서비스에 의한 메시지

uucp

uucp 에 의한 메시지

local0 ~ local7

사용자가 정의해서 이용

3) Level 종류(메시지의 중요도)

#man syslog

emerg

시스템 다운으로 인한 서비스 불가로 가장 높은 level

자주 발생한다면 시스템 점검이 반드시 필요

alert

경고 수준의 레벨로 해당 데몬 및 프로그램 종료 후 보안조치 필요

crit

유틸리티나 서브시스템을 종료해야 하는 수준

err

error 수준의 레벨로 주기적인 모니터링 필요

warn

단순 경고 메시지로 주의요망

notice

시스템에서 발생하는 주의 정도의 로그

info

정보를 제공하는 메시지

debug

세부적인 정보 출력으로 문제 해결에 도움을 주는 레벨

none

로그하지 않음

SSH 서비스 로그 처리 과정)

/etc/rsyslog.conf 설정 내용 :

authpriv.* /var/log/secure

[리눅스 서버]

SSH 서비스 <-----


[윈도우]

putty 접속

AUTHPRIV.INFO 메시지 발생

Syslog 가 설정 파일 참조하여 기록

<로그인 관련 로그>

 /var/run/utmp


시스템에 현재 로그인한 사용자들에 대한 상태를 기록하는 파일

텍스트 파일이 아닌 바이너리 파일

vi, cat, tail 명령어로 내용 확인 불가

who, w, users 명령어를 이용하여 정보 확인

```
#ls /var/run
#file /var/run/utmp
#cat /var/run/utmp
#who
#w
#users --help
#users
```


 /var/log/wtmp

사용자들의 로그인, 로그아웃 정보
바이너리 형태의 파일
사용자들의 로그인, 로그아웃 히스토리를 누적 형태로 저장
시스템의 셧다운, 부팅 히스토리까지 포함
해킹 피해 시스템 분석시 매우 중요한 로그 기록
last 명령어로 분석

```
#ls /var/log
#file /var/log/wtmp
#cat /var/log/wtmp
```

프롬프트가 깨지면 터미널을 종료후 다시 실행

```
#last
#last apple
---> apple 계정 로그인 히스토리 출력
#last -5
---> 출력 라인수 설정
```

 /var/log/lastlog

각 사용자가 최근에 로그인한 시간과 접속 장소가 기록되는 파일
사용자가 시스템에 로그인 할 때마다 갱신 됨
바이너리 파일
lastlog 명령어로 분석

```
#lastlog
/etc/passwd 파일에 정의되어 있는 모든 계정의 최근 접속 정보를 확인
#lastlog -u 계정명
```

<FTP 로그>

 /var/log/xferlog

FTP 파일 전송에 관련된 로그 기록

#cat /var/log/xferlog

접근날짜와 시간

접속한 IP

전송한 파일 사이즈

전송한 파일

파일의 종류

b : 바이너리

a : ascii 파일

취해진 해동 분석

_ 아무일도 발생하지 않았음

C 압축파일

서버에서 파일 행동 방식

i : incoming, 업로드

o : outgoing, 다운로드

d : delete, 삭제

사용자 접근 방식

r : real, 인증된 사용자

a : anonymous, 익명 사용자

로그인한 ID

서비스 방법(ftp)

인증에 사용된 방법(0)

인증에 사용된 ID(*)

전송상태

c : complete, 전송 성공

i : incomplete, 전송 실패

<프로세스 관련 로그>

 psacct(process account)

-사용자가 로그인 한 후 로그아웃 할 때까지 입력한 command 와 시간,

작동된 tty(터미널) 등을 저장

-바이너리 형태의 파일

[first]

#rpm -qa | grep psacct

패키지가 없으면 yum 으로 설치

```
#yum -y install psacct
```

```
#service psacct restart
```

/var/account/pacct 바이너리 파일 생성

lastcomm 명령어를 통해 정보 출력

```
#lastcomm
```

```
#lastcomm 계정명
```

S //Superuser 가 사용한 명령임을 의미

F //다른 프로세스에 의해 fork 된 후에 사용된 명령

<logwatch>

로그 파일을 하루 단위로 종합적으로 정리해서 메일로 보내주는 스크립트 프로그램

```
#rpm -qa | grep logwatch
```

```
#yum -y install logwatch
```

```
#ls /etc/cron.daily/
```

0logwatch 파일이 Cron 데몬에 의해서 매일 실행 됨

logwatch 설정 파일 :

```
/usr/share/logwatch/default.conf/logwatch.conf
```

```
#cd /usr/share/logwatch/default.conf/
```

```
#vi logwatch.conf
```

27 로그 디렉토리

35 메일을 보낼 계정

44 메일제목

65 Range(범위)

72 Detail

```
#/etc/cron.daily/0logwatch
```

---> logwatch 수동 실행

mail 명령어를 통해 확인

#mail

&번호

---> 특정 번호 메일 확인

&h

---> 메일 목록 출력

&q

---> 저장후 종료(x 는 저장하지 않고 종료)

#

메일 삭제 : d

&d 5

---> 5번 메일 삭제

&d 6-10

---> 6번에서 10번 메일 삭제

(메일 삭제후 x 로 종료하면 저장되지 않으므로

#mail 을 입력했을 때 다시 나타나고

q 로 종료하면 삭제가 저장된다.)

<리눅스 로그 정리>

1. rsyslog(시스템 로그)

/var/log 안의 파일 확인

2. 로그인 관련 로그

who, last, lastlog 명령어로 확인

3. ftp(파일 전송 관련) 로그

/var/log/xferlog 파일 확인

4. 프로세스 관련 로그

lastcomm 명령어로 확인

5. logwatch 이용하여 mail 명령어로 확인

■실습

1. telnet 접속 로그를 /mylog/telnet.log 에 기록하기

(/etc/rsyslog.conf 에 authpriv.* 등록)
2. ftp 로그 파일을 /var/log/vsftpd.log 로 변경
(/etc/vsftpd/vsftpd.conf 파일
56 xferlog_std_format=NO 로 변경후
서비스 재시작하고 테스트)

[first] [second]
Telnet 서버 <----- telnet 접속

AUTHPRIV 메시지 발생
Syslog 가 처리

////////////////////////////////////

[first]
1)
#vi /etc/rsyslog.conf
마지막 라인에 추가
authpriv.* /mylog/telnet.log
#mkdir /mylog
#service rsyslog restart
#ls /mylog
#service xinetd restart
#netstat -ntlp | grep xinetd
23 번 텔넷 포트 확인

[second]
첫번째리눅스로 telnet 접속 테스트

2)
[first]
#vi /etc/vsftpd/vsftpd.conf
56 xferlog_std_format=NO
#service vsftpd restart

윈도우에서 알FTP 이용하여 first 리눅스로 ftp 접속후 파일 전송

[first]
#cat /var/log/vsftpd.log

////////////////////////////////////

■방화벽(firewall)

설정된 규칙(rule, 룰)에 따라 패킷(데이터)을
차단시키거나 통과시키는 프로그램 또는 장비

netfilter // iptables 가 방화벽 기능을 구현할 수 있게
프레임워크(framework)를 제공

iptables // 방화벽 규칙 설정 및 확인 명령어

참조)

http://navercast.naver.com/contents.nhn?rid=122&contents_id=7838

<리눅스 방화벽의 구조>

3개의 기본 테이블(작업공간)로 구성

각 table은 chain(패킷의 이동통로)으로 구성

1. filter table // 접속 허용, 차단 판단

1)FORWARD // 방화벽을 통과하는 패킷의 이동통로

2)INPUT // 방화벽 자체 서비스로 들어오는 패킷의 이동통로

3)OUTPUT // 방화벽 자체에서 외부로 나가는 패킷의 이동통로

2. nat table : 주소 변환 설정

1)OUTPUT

2)POSTROUTING

3)PREROUTING

외부 ----- firewall ----- 내부
(<---)postrouting prerouting(--->)

3. mangle table : 패킷의 속성(ttl,tos 등) 변경

1)FORWARD

2)INPUT

3)OUTPUT

4)POSTROUTING

5)PREROUTING

☞방화벽 분류

호스트 기반 방화벽(서버 방화벽)은 FORWARD를 이용하지 않는다.
(INPUT과 OUTPUT만 이용)

(1) 호스트 기반 방화벽(Host Based)

[client] ----- [웹서버 and 방화벽]

(2) 네트워크 기반 방화벽

[client] ----- [only 방화벽] -----+----- [웹서버]
|
+----- [네임서버]
|
+----- [DB서버]

■iptables 형식

iptables -t 테이블이름 command 체인이름 파라미터 옵션 ...

테이블이름

table // filter, nat, mangle

command

-L // 규칙 목록, List
-A // 규칙추가(마지막에 추가), Append
-F // 규칙 모두 삭제, Flush
-D 체인명 규칙번호 // 특정 번호 규칙 삭제, Delete
-I // 규칙입력(첫번째 규칙으로 추가), Insert
-I 체인명 2 // 2번째 규칙으로 입력
-R 체인명 규칙번호 // 특정 번호 규칙 교체, Replace

체인이름

chain // INPUT, OUTPUT, FORWARD, 사용자 체인

파라미터

-p 프로토콜 // 규칙에 영향을 받는 프로토콜 지정(icmp, tcp, udp, all)

옵션

target // DROP, REJECT, ACCEPT

포트를 여러 개 지정할 경우는 -m multiport 를 사용한 후 --sports, --dports, --ports
다음에

포트를 , 로 지정

예) -m multiport -p tcp --dports 10,20,30

포트범위 지정은 : 을 사용

예) -p tcp --dport 10:100

특정 포트와 아이피를 제외할 경우에는 ! 연산자 사용

예) ! -s 192.168.x.1

-p tcp ! --dport 23

웹서버 동작시키기

[first]

#service httpd restart

#netstat -ntlp | grep httpd

[windows]

웹브라우저 실행

http://리눅스아이피

---> O (홈페이지 출력 확인)

[first]

#service iptables status

#service iptables start

#service iptables status

---> ?

☞ 리눅스 방화벽 동작시키는 방법

1) lokkit

2) setup

3) system-config-firewall

4) system-config-firewall-tui

☞ 리눅스 방화벽 규칙설정 방법

1) setup, system-config-firewall, system-config-firewall-tui

2) iptables 를 이용한 설정

[first]

```
#lokit --enabled
#service iptables status
#lokit --disabled
#service iptables status
```

```
#setup
방화벽 설정 선택
```

```
#system-config-firewall
---> GUI 환경
```

```
#system-config-firewall-tui
---> TUI 환경
```

모듈(module) : 메모리에 로딩해서 특정 기능을 사용하는 부품 개념
lsmod : 모듈 확인
modinfo : 모듈 정보 확인

```
#lsmod
iptables 모듈 확인
#modinfo ip_tables
#modinfo pcnet32
---> 랜카드 드라이버
```

```
#iptables -L
-L(대문자) 규칙 목록 출력
```

```
#service iptables status
```

웹브라우저 설정 확인)

[windows]

웹브라우저 실행후 도구-인터넷 옵션 클릭
일반-검색 기록-설정 클릭

저장된 페이지의 새버전 확인:

(*)웹페이지를 열 때마다

확인 클릭

--->방화벽으로 차단 설정을 해도 웹브라우저 캐시가 보여지므로
위와 같이 설정을 변경함

http://리눅스아이피

---> X (방화벽이 차단해서 홈페이지 출력 안 됨)

[first]

#iptables -F

-F (flush) 규칙 모두 삭제

#iptables -L

[windows]

http://리눅스아이피

---> O (방화벽 규칙을 삭제했으므로 홈페이지 출력 됨)

[first]

#service iptables restart

#iptables -L

---> 방화벽 규칙 이 다시 나타난다.

☞방화벽 설정에서 웹서비스만 allow 설정하기

[first]

#setup

1)방화벽 설정 실행

2)탭키 또는 화살표키 이용하여 커서를 Customize(사용자 설정) 로 이동시킨 후
엔터 입력

3)스페이스바 이용하여

[*]www(HTTP)에 체크하고 빠져 나온다.

#netstat -ntlp | egrep 'httpd|vsftpd'

21, 80 포트 확인하고 없으면 서비스 시작 시키기

[second]

http://첫번째리눅스아이피

---> O

#ftp 첫번째리눅스아이피

---> X (호스트로 갈 루트가 없음 출력)

리눅스 방화벽의 각 테이블 확인

[first]

#iptables -L -t filter

---> iptables -L 과 같다.

디폴트가 filter 테이블이다.

iptables -t filter -L 로 실행해도 된다.

#iptables -L -t nat

#iptables -L -t mangle

-L 리스트

-t 테이블 지정

#cat /etc/sysconfig/iptables

부팅할 때 또는 iptables 서비스가 restart 될 때 이 파일 내용으로
방화벽규칙이 초기화 된다.

iptables -F(방화벽 규칙 삭제) 한 다음

리부팅하거나 service 를 재시작해도 위의 파일로 초기화 되지 않고
자신이 설정한 내용이 저장되게 하려면 설정파일을 수정해야 한다.

#mkdir /backup

#cp /etc/sysconfig/iptables /backup

기존 규칙 백업

#iptables -L

기본적으로 filter 테이블이 보여진다.

#iptables -F

```
#iptables -L
```

```
#reboot
```

루트 로그인

```
#iptables -L
```

기본적으로 설정된 규칙이 다시 나타남

☞사용자가 설정한 규칙이 저장(Save)되도록 설정 변경하기

```
#vi /etc/sysconfig/iptables-config
```

--->iptables 설정파일

19,25 라인 yes 로 변경

```
IPTABLES_SAVE_ON_STOP="yes"
```

```
IPTABLES_SAVE_ON_RESTART="yes"
```

```
#iptables -F
```

```
#iptables -L
```

```
#service iptables restart
```

```
#iptables -L
```

---> 서비스를 restart 해도 초기화 되지 않는다.

☞방화벽 규칙 설정 예

대소문자 구분함

[first]

```
#iptables -A INPUT -t filter -s 아이피 -j DROP
```

필터 테이블의 INPUT 체인에 출발지 아이피 패킷은 drop(접속무시)시키라는 rule

아이피는 second 리눅스 아이피로 설정

-A Append, 추가

INPUT 입력체인

-t 테이블(테이블을 생각하면 필터 테이블이 적용된다.)

filter 필터 테이블

-s source 출발지 주소

-d destination 목적지 주소

-j jump target 처리할 작업

DROP 패킷 버림

REJECT 접속 거부하면서 메시지 리턴
ACCEPT 패킷 통과

#iptables -L

[second]

#ftp 첫번째리눅스아이피

---> X

Ctrl + c 로 중단

#ssh 첫번째리눅스아이피

---> X

특정서비스만 접속 차단

[first]

#iptables -F

#iptables -A INPUT -s 두번째리눅스아이피 --dport 23 -j REJECT

---> 포트 지정시 프로토콜을 생략하면 규칙 추가 안됨

#iptables -A INPUT -s 두번째리눅스아이피 -p tcp --dport 23 -j REJECT

--->second 에서 first 로 telnet 접속 차단

-s 출발지 아이피 ---> 클라이언트 아이피

-d 목적지 아이피 ---> 리눅스 서버

-p 프로토콜 지정(tcp : tcp 프로토콜, udp, icmp)

--sport (source port) 출발지 포트 ---> 클라이언트 포트

--dport (destination port) 목적지 포트--->리눅스 서버측 포트

23 telnet 포트

#iptables -L

#iptables -nL

n : 숫자로 출력

first 리눅스에서 telnet 서버, ftp 서버 동작 시키기

#service xinetd restart

#service vsftpd restart

#netstat -ntlp | egrep 'xinetd|vsftpd'

21 번, 23 번 포트 확인

[second]

#telnet 첫번째리눅스아이피

---> X

#ftp 첫번째리눅스아이피

---> O

<iptables 옵션 및 관련 명령어 사용하기>

[first]

#cd

#pwd

/root

#iptables -nL --line-number

라인번호 출력

#iptables-save

#iptables-save > firewall.rule

룰을 파일로 저장

#ls

#cat firewall.rule

#iptables -F

#iptables -L

#iptables-restore < firewall.rule

파일로 된 룰을 다시 적용하기

#iptables -L

☞ 특정 룰 삭제

#iptables -F 는 모든 체인의 규칙을 삭제하며

특정 체인의 규칙만 삭제하려면

#iptables -F OUTPUT 과 같이 체인명을 뒤에 지정해 주면 된다.

```
#iptables -F
#iptables -A INPUT -s 172.16.1.1 -j DROP
#iptables -A INPUT -s 172.16.1.2 -j DROP
#iptables -A INPUT -s 172.16.1.3 -j DROP
```

--->규칙이 여러 개 있을 때 top-down(위에서 아래로) 방식으로 처리된다.

```
#iptables -L
#iptables -nL --line-number
또는 iptables -nL --line-numbers
```

```
#iptables -D INPUT 2
---> 두번째 규칙 삭제
---> -D 옵션 // 규칙 삭제
```

```
#iptables -nL --line-number
```

☞ 룰 insert 하기

```
#iptables -I INPUT -s 172.16.1.30 -j DROP
I //Insert , 첫번째 룰로 입력된다.
```

```
#iptables -nL --line-number
```

```
#iptables -I INPUT 2 -s 172.16.1.40 -j DROP
두번째 룰로 입력하기
```

```
#iptables -nL --line-number
```

☞ 룰 replace 하기

```
#iptables -R INPUT 2 -s 172.16.1.77 -p udp --dport 53 -j DROP
--->INPUT 체인에서 2번째 규칙을 교체
```

R //Replace , 교체

```
#iptables -nL --line-number
```

<IPTABLES 실습>

second 리눅스에서 방화벽을 동작시키고 규칙 모두 삭제후 테스트하기
#lokit --enabled

21, 22, 23, 80 포트 확인

포트가 없으면 서비스 시작시키기(프로그램 없으면 yum 으로 설치)

service vsftpd restart, service xinetd restart, service httpd restart
#iptables -F

Q1)

iptables 이용하여 first 에서 second 로 ftp 접속 차단
win2003 은 접속되어야 함

Q2)

현재 룰을 모두 지우고

win2003 에서 second 로 웹접속, telnet 접속 차단(멀티포트 이용),
first 에서 second 로 ssh 접속 차단하기

////////////////////////////////////

A1)

#iptables -A INPUT -s 첫번째리눅스아이피 -p tcp --dport 21 -j DROP
#iptables -L

A2)

#iptables -F

#iptables -A INPUT -s 윈도우2003아이피 -p tcp --dport 80 -j DROP

#iptables -A INPUT -s 윈도우2003아이피 -p tcp --dport 23 -j DROP

#iptables -A INPUT -s 첫번째리눅스아이피 -p tcp --dport 22 -j DROP

#iptables -nL

또는

#iptables -A INPUT -s 윈도우2003아이피 -m multiport -p tcp --dports 23,80 -j
DROP

#iptables -A INPUT -s 첫번째리눅스아이피 -p tcp --dport 22 -j DROP

////////////////////////////////////

작 성 자 : 김 흥 량 강사, 참 조 자 : 김 찬 중 강사

작 성 자 : 김 흥 량 강사, 참 조 자 : 김 찬 중 강사