김해중
KBS 보도기술국

실무 네트워크 Design - 12 : Windows OS의 Networking

이번 시간에는 먼저 windows OS에서 이용되는 네트워크 기본 명령과 세팅에 대해 자세히 알아보려고 합니다. 뒷부분은 windows에서 사용하는 공유기능에 대해서 자세히 다루도록 하겠습니다.

windows 네트워크 세팅

L3(IP) 관련

먼저 IP 세팅을 해보려고 합니다. 일반적으로 IPv6는 사용하지 않기에 비활성화를 권장합니다. IP를 세팅하는 방법에는 항상 고정된 IP를 사용하는 방법과 IP를 동적으로 할당하는 서버(DHCP 서버)로부터 IP를 할당받는 방식이 있습니다.

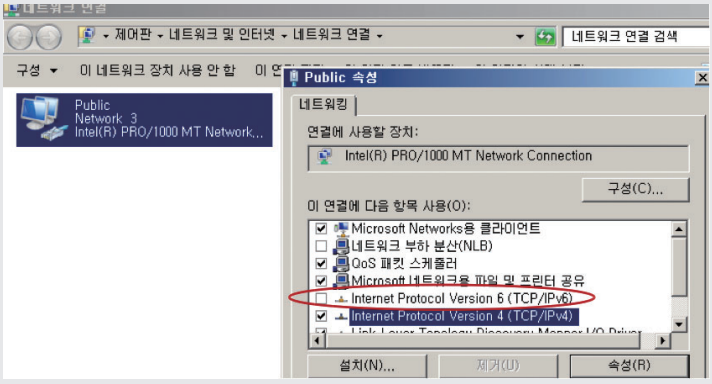
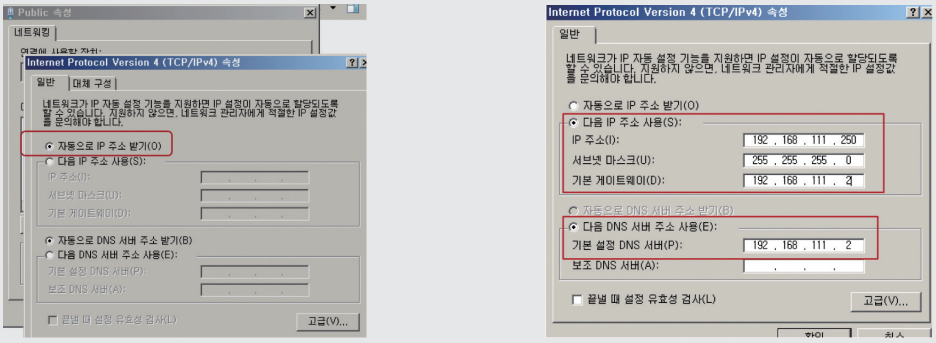


그림 1. 기업환경에서 IPv6는 사용하지 않으니 비활성화를 권장합니다



(a) dynamic(동적) IP 세팅　　(b) static(고정) IP 세팅

그림 2. IP 세팅 2가지 방법

ipconfig 명령을 통해 세팅된 IP 정보를 확인할 수 있으며, 자세한 정보를 얻으려면 ipconfig/all을 사용하면 됩니다.

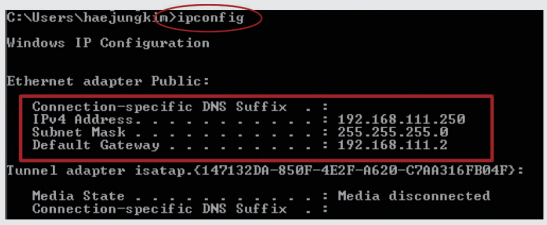


그림 3. ifconfig 명령을 이용해 세팅된 정보를 확인할 수 있다

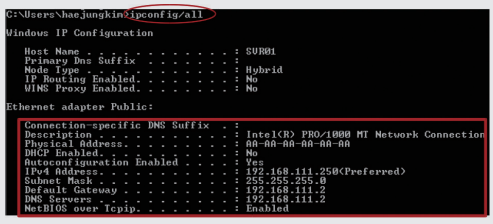


그림 4. ipconfig/all을 이용해 자세한 정보를 확인할 수 있다

만약 PC가 IP를 얻지 못하면, windows는 microsoft 사의 사설 IP 대역(169로 시작함)의 IP를 가지게 됩니다. 그럼 언제 IP를 얻지 못할까요? dynamic IP 세팅일 때는, IP를 할당하는 DHCP 서버를 찾지 못했을 때 발생하며, 이때는 DHCP 서버로 가는 경로에 문제가 없는지 확인해 보아야 합니다. static IP 세팅이라면, 다른 누군가가 자신이 입력한 IP를 미리 사용하고 있어서 IP 충돌이 발생했을 때입니다.

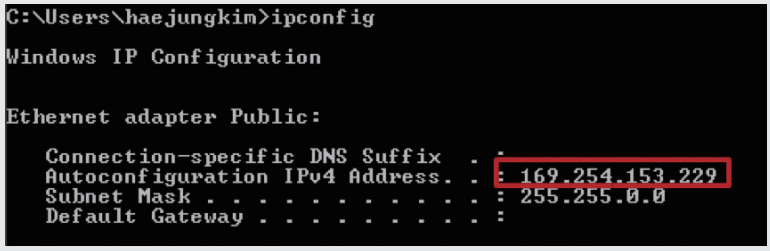


그림 5. 169점대의 IP를 할당받은 것은, IP 획득에 실패했음을 알려줍니다

ipconfig는 추가적으로 다양한 기능을 제공하는데, [표 1]을 참고하시면 됩니다.

명 령	특 징
ipconfig/release	동적으로 할당 받은 IP를 반납할 때 사용합니다.
ipconfig/renew	동적으로 할당받은 IP를 반납하면서, 다시 새로운 IP를 요청하는 기능입니다.
ipconfig/displaydns	DNS-cache table 정보를 보여줍니다.
ipconfig/flushdns	DNS-cache table 정보를 삭제합니다.

표 1. ipconfig의 다양한 기능

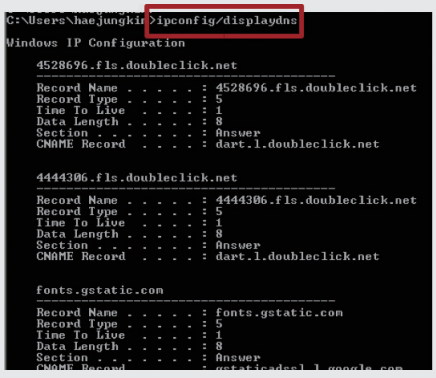


그림 6. ipconfig/displaydns는 DNS-cache 정보를 보여줍니다

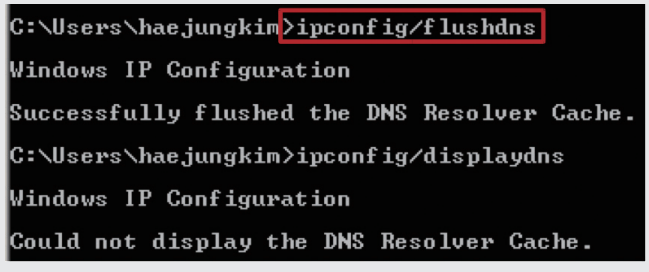


그림 7. ipconfig/flushdns는 DNS-cache 정보를 삭제합니다

김해중
KBS 보도기술국

LAN card의 MAC-address 변경은 장치 관리자에서 가능합니다.

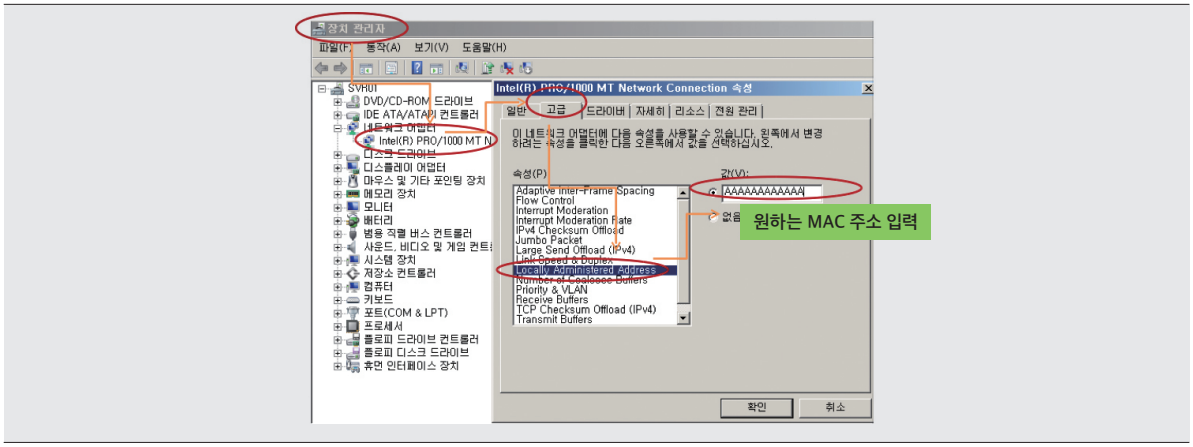


그림 8. 장치 관리자에서 LAN card의 MAC-address를 변경할 수 있습니다

ARP를 이용한 L2(mac-address) 정보 확인

arp -a 명령을 이용해 ARP cache table 정보를 알 수 있으며, arp -d 명령을 이용해 ARP cache table 정보를 삭제할 수 있습니다.

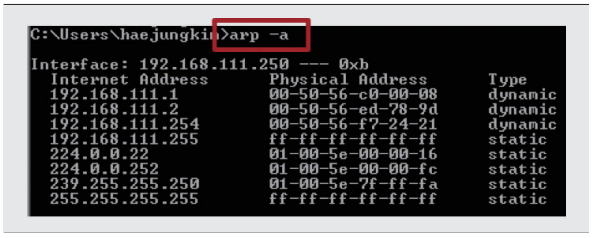


그림 9. arp -a 명령은 ARP cache table를 보여줍니다

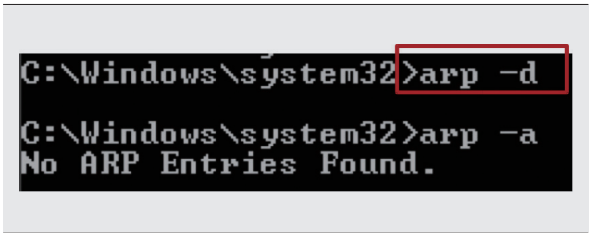


그림 10. arp -d 명령을 이용해 ARP cache table을 삭제할 수 있습니다

예1) arp -d 192.168.0.100	192.168.0.100에 대한 ARP cache table을 삭제합니다.
예2) arp -d	모든 ARP cache table을 삭제합니다.
예3) arp -s 192.168.0.200 aa-bb-cc-dd-ee-ff	수동으로 arp cache table을 만듭니다.

표 2. ARP 예제

참고로 원격지에 있는 PC의 mac 주소를 알고 싶을 때는, getmac 명령을 사용하면 됩니다. getmac은 RPC 프로토콜을 이용하여 상대방의 mac 주소를 알아내며, TCP 135와 2041번 port로 통신합니다. 사용방법은 getmac /S PC 이름(IP 주소, 도메인 네임)입니다.

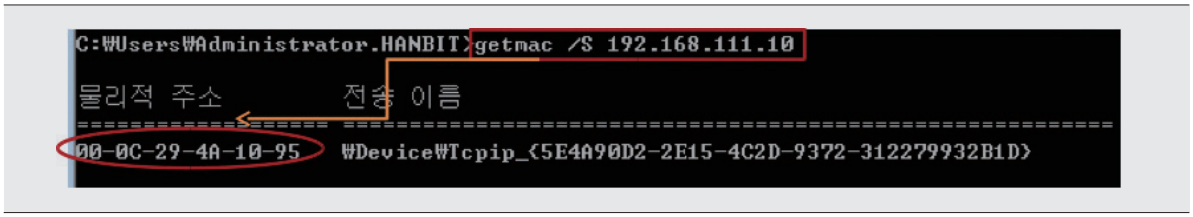


그림 11. getmac 명령을 통해 원격지에 있는 PC의 mac-address를 알 수 있습니다

L4(port) 정보 확인

PC에 연결 중(establish) 이거나 연결 대기 중인(listen) 상태의 TCP/UDP PORT 정보를 확인할 때는 netstat 명령을 이용합니다. netstat -an을 가장 많이 사용하며, -n은 number(숫자 형식)로 보여주며 -a는 all의 의미로 모든 연결(establish)과 수신대기(listen)를 보여줍니다.

참고로 TCPview 프로그램을 통해서도 자세한 정보를 얻을 수 있으며, TCPview는 인터넷에서 쉽게 구할 수 있습니다.

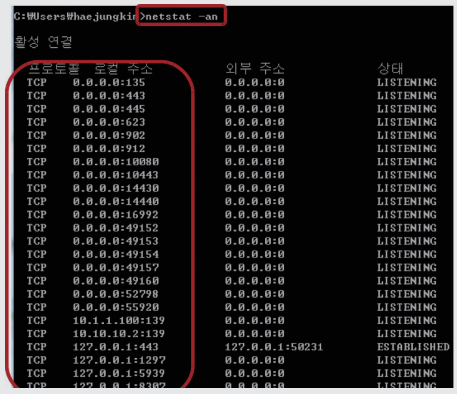


그림 12. netstat -an 명령을 통해서 L4(port) 정보를 확인할 수 있습니다

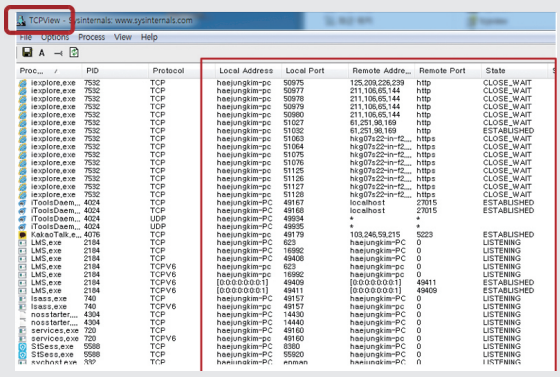
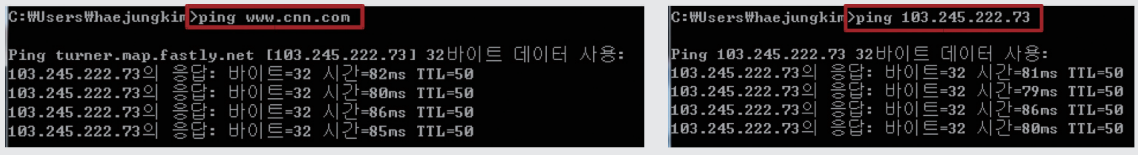


그림 13. TCPview를 이용해서 L4(port) 정보를 확인할 수 있습니다

Ping

ping은 원격지에 있는 컴퓨터가 동작하는지 확인하는 고전적인 도구입니다. 하지만 최근에는 많은 방화벽이 ping 서비스를 차단하고 있기에, ping을 실패했다고 해서 원격지에 있는 서버에 연결이 실패한다는 의미는 아닙니다.



(a) 도메인 네임 이용 (b) IP 주소 이용

그림 14. IP 주소와 도메인 이름을 이용해, Ping을 보낼 수 있습니다

ping -t 명령을 이용하면, ctrl c를 누를 때까지 계속 ping이 동작합니다. 서버나 네트워크에 특정 작업을 할 때, ping -t 명령을 통해 서비스가 끊어지지 않고 동작 중임을 체크할 수 있습니다.

그림 15. ping -t 명령을 이용하면, ctrl c를 누를 때까지 계속 ping이 동작합니다

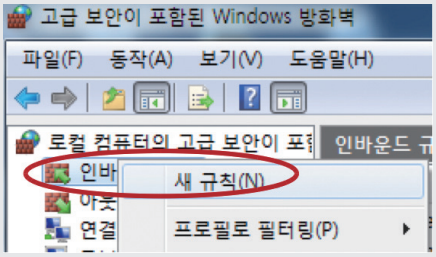
그림 16. 특정 회사(예 : 네이버)는 보안을 위해 Ping 서비스를 지원하지 않습니다

1) ping -n 10 domino.co.kr	ping 패킷을 10개만 전송합니다. (default는 4개 전송입니다.)
2) ping -i 10 domino.co.kr	ping 패킷을 보낼 때 TTL 값을 10으로 세팅한다. (default TTL은 128입니다.)
3) ping -l 2000 domino.co.kr	ping 패킷의 MTU를 2000byte로 설정하여 전송합니다. - 일반적으로 MTU가 1500byte라서, ping 패킷은 2개로 분할되어서 전송된다.
4) ping -f domino.co.kr	ping 패킷을 보낼 때, IP 헤더에 절대 패킷 분할이 안 되도록, DF 필드에 0을 세팅한다.

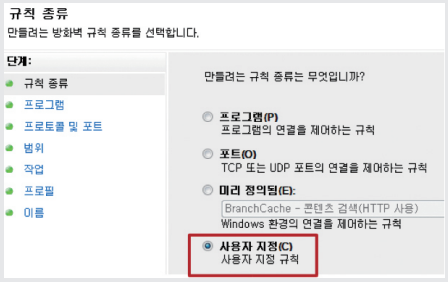
표 3. ping 예제

김해중
KBS 보도기술국

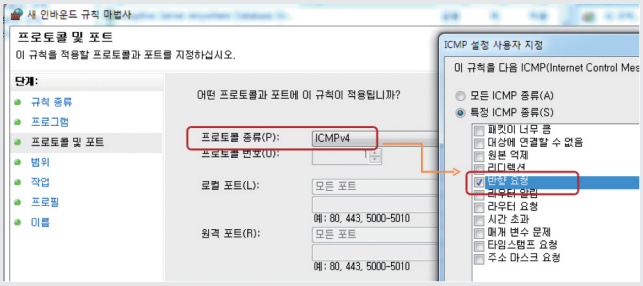
자신의 PC로 들어오는 Ping에 대해, reply 패킷을 보내지 않으려면 windows 방화벽을 사용하면 됩니다.



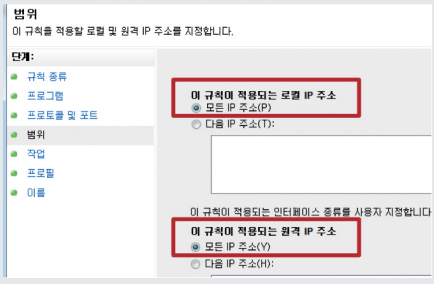
(a) 인바운드에서 새 규칙 선택하기



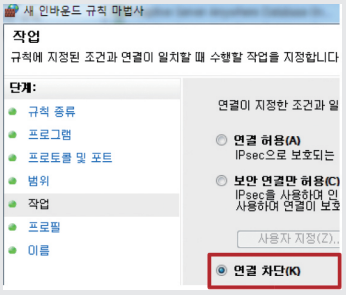
(b) 사용자 지정을 선택한다.



(c) ping과 관련 있는 ICMPv4(반향 요청)을 선택한다.

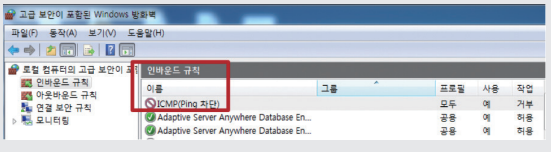


(d) 차단할 IP 대역을 선택한다



(e) "연결차단"을 선택한다.

(f) 알아보기 쉽게 이름을 할당한다.



(g) 만들어진 인바운드 규칙을 확인한다.

그림 17. windows 방화벽을 이용해 ping을 차단할 수 있다

tracert

tracert는 목적지까지의 경로를 상세히 확인하는데 사용하는 도구이며, 사용방법은 tracert IP 주소(도메인 네임)입니다. 하지만 이렇게만 하면 응답속도가 너무 느려서, 대부분의 사용자들은 -d option을 사용합니다. -d는 주소를 hostname으로 바꾸지 않는 옵션입니다. 보안상의 이유로, tracert를 비활성화 해놓은 구간에서는 * 혹은 request time out(요청시간이 만료되었습니다)으로 표시됩니다.

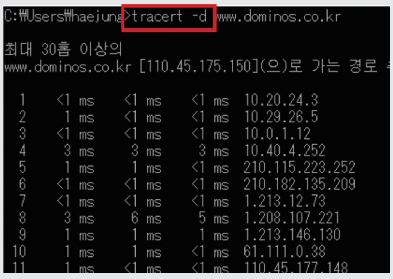


그림 18. tracert는 목적지까지의 경로를 상세히 확인하는데 사용하는 도구입니다

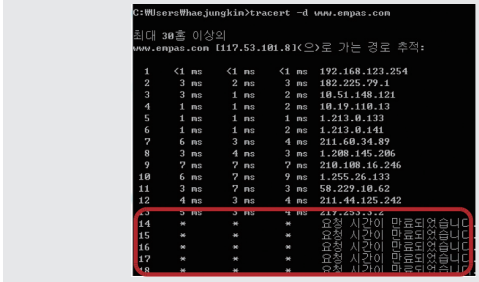


그림 19. 보안상의 이유로 tracert를 막아놓은 곳도 있다

PC 이름

windows에서는 3가지 명령을 통해 PC 이름을 알 수 있습니다.

(a) hostname (b) whoami (c) echo %computer$

그림 20. windows에서 PC 이름을 알아내는 3가지 명령어

windows의 AD(active directory)는 내부적으로 모든 개체(사용자, 그룹, computer)를 SID(security ID)를 통해서 구별합니다. 즉 모든 사용자, group, computer는 고유의 SID를 가지고 있어서, PC의 이름을 변경하더라도, SID는 변하지 않습니다. whoami 명령어에 /user를 추가하면, 사용자의 SID를 알 수 있습니다.

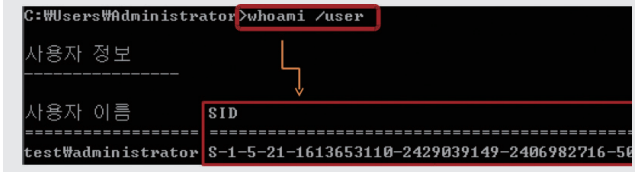
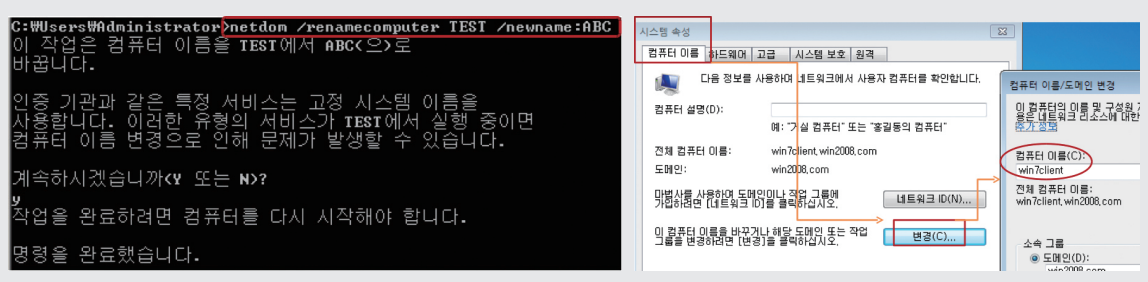


그림 21. whoami /user를 통해서 사용자의 SID를 알 수 있습니다

시스템 속성에서 PC 이름을 변경할 수도 있지만, netdom(domain manager의 약어) 명령을 통해서도 PC 이름을 변경할 수 있습니다.



(a) (b)

그림 22. PC 이름 변경

김해중
KBS 보도기술국

netsh 명령

netsh 명령을 이용해 네트워크 정보를 확인하고 세팅할 수 있습니다. 먼저 "netsh" 명령으로 네트워크를 설정할 수 있는 환경으로 들어가면 프롬프트가 netsh>로 변경됩니다. [그림 23]처럼 (interface ipv4 show interface) 명령을 입력하면, 해당 PC가 가지고 있는 모든 LAN card 정보를 보여 줍니다.

기능	명령어
PC의 LAN card 정보 확인	interface ipv4 show interface
Static IP 세팅	interface ipv4 set address name="색인번호" source=static address=IP mask=서브넷 마스크 gateway=gatewayIP
DNS 서버 세팅	interface ipv4 add dnsserver name="색인번호" address=IP index=1

표 4. netsh 명령어

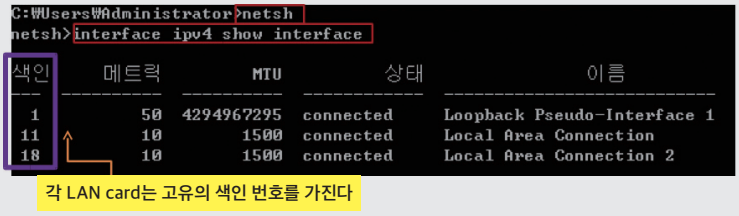


그림 23. interface ipv4 show interface 명령은 PC가 가지는 모든 LAN card 정보를 보여주며, 각 LAN card를 색인번호로 구분합니다

그림 24. 색인번호(18)인 LAN card에 IP를 세팅하고 있다

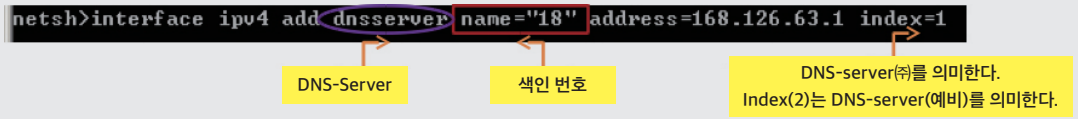
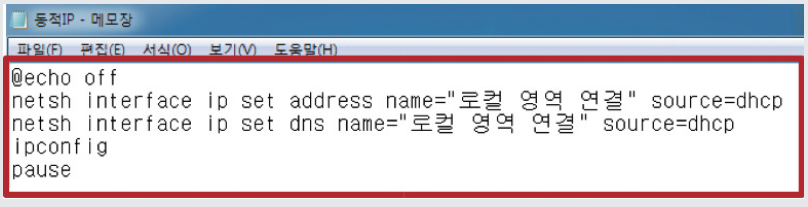
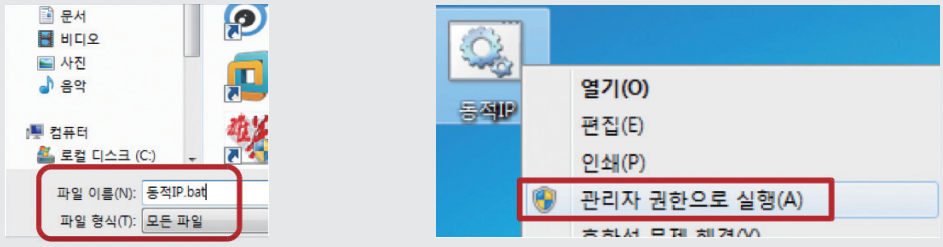


그림 25. 색인번호(18)인 LAN card에 DNS-server를 세팅하고 있다

만약 사용자가 고정 IP와 동적 IP를 번갈아 가면서 사용해야 하는 상황이라면, netsh 명령을 배치파일 형태로 만들어서, 배치파일만 클릭하면 IP를 변경할 수 있게 구성할 수 있습니다.



(a) 메모장에서 동적으로 IP를 받도록 세팅한다.



(b) 배치파일(확장자 bat)을 만든다. (c) 배치파일을 실행한다.

그림 26. 배치파일을 이용해서 동적으로 IP를 받도록 설정 변경하기

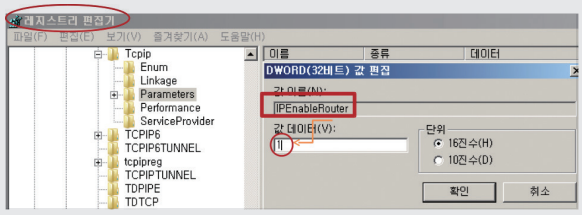
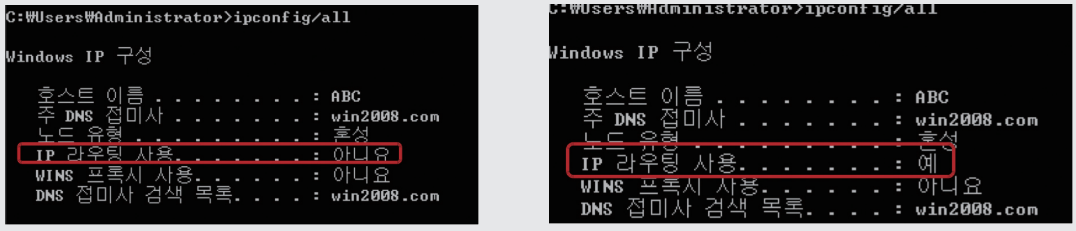


그림 27. 레지스트리를 수정해 routing 기능을 활성화 시킬 수 있습니다

PC를 router로 만들기

windows PC는 기본적으로 host(단말)로 동작하도록 되어 있어서, routing 기능이 기본적으로 비활성화되어 있습니다. 하지만 레지스트리를 수정하면 routing 기능을 활성화할 수 있습니다. 레지스트리 편집기의 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCP\Parameters에서 IPEnableRouter의 값을 0에서 1로 변경 후, 리부팅하면 routing 기능이 활성화됩니다.

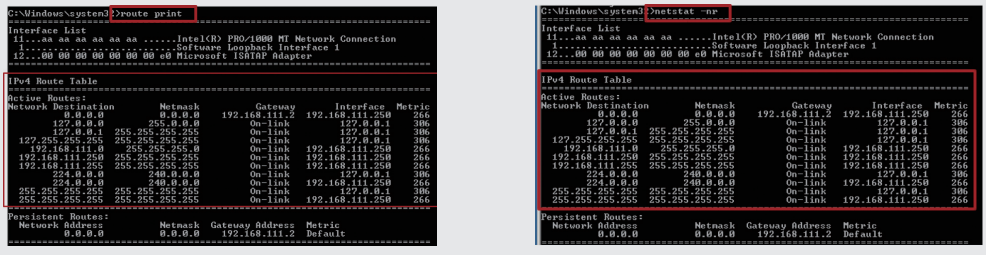


(a) routing 기능 off 상태 (b) routing 기능 on 상태

그림 28. ipconfig/all을 통해 routing 기능의 활성화 여부를 알 수 있습니다

PC의 routing table

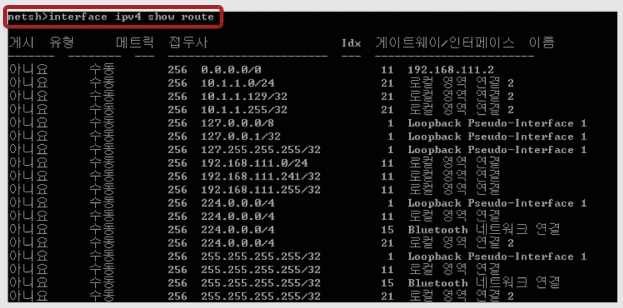
일반 PC도 router처럼 routing table을 가지고 있으며, 만약 여러 개의 LAN card를 가지고 있으면, router 역할을 할 수 있습니다. routing table 확인은 (route print), (netstat -nr), (netsh → interface ipv4 show route)로 가능하며, 일반적으로 route print 명령을 가장 많이 사용합니다.



(a) route print (b) netstat -nr

그림 29. routing table 확인하기

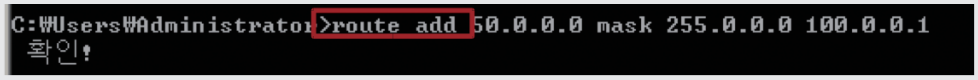
김해중
KBS 보도기술국



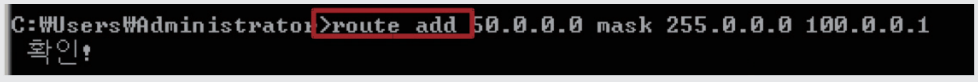
게시(publish) : router 역할여부를 의미하며, "아니오"는 router 역할이 비활성화 되었음을 의미한다.
유형(type) : 사용자 또는 응용프로그램에 의해 추가되면 "수동"이며, IP 계층에 의해 추가되면 "자동"이다.
메트릭(metric) : 목적지까지 가는 비용을 의미하는데, 가장 적은 값이 이용된다.
접두사(preifx) : 목적지 경로를 CIDR(classless inter-domain routing) 형식으로 보여준다.
Idx(index) : interface를 간단히 표현하기 위한 index입니다.
게이트웨이/인터페이스 이름 : 목적지까지 패킷을 전송할 local interface(outgoing interface)를 알려준다.

그림 30. routing table 분석

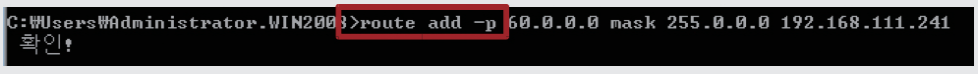
route 명령을 통해, routing table을 생성, 삭제, 변경할 수 있습니다.



(a) routing table 추가 (50.0.0.0/8 경로로 갈 때는 100.0.0.1 IP 가지는 LAN card 사용하라)



(b) routing table 추가 (-p 옵션을 사용하면, 리부팅해도 경로가 유지됩니다.)



(c) routing table 변경

(d) routing table 삭제 (50.1.0.0/16 경로 삭제)

그림 31. route 명령으로 routing table 생성/삭제/변경

공유 기능

windows 공유 (CIFS/SMB)

windows 환경에서는 파일 공유 프로토콜로 CIFS(common internet file system)를 주로 사용합니다. CIFS는 파일 공유 프로토콜인 SMB(server message block)에 기반을 두고, Microsoft에서 개발했습니다.

SMB 버전	운영 체제
SMB 1.0	win 2000/2003/2003 R2 /XP
SMB 2.0	window vista / 2008
SMB 2.1	window 7 / 2008 R2
SMB 3.0	window 8 / 2012

표 5. 운영체제별 SMB 버전

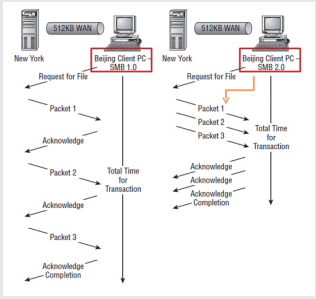


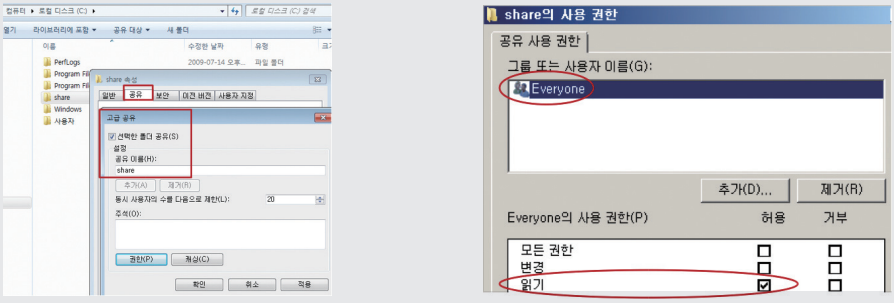
그림 32. SMB 2.0은 request compounding 기능을 통해서 전송 효율을 개선했습니다

SMB는 2.0이 현재 많이 이용되고 있으며, 한번에 여러 개의 packet을 전송하는 request compounding 기능을 통해서 전송 효율을 향상 시켰습니다.

CIFS 특징	운영 체제
client/server 기반 프로토콜	TCP 기반위에서 동작하며, 445번 port를 사용합니다.
DNS 사용	name-resolution(이름 해석)을 위해 DNS를 사용합니다.
special-locking	1명의 user가 작업하는 동안, 다른 user가 overwrite하는 것을 막아줍니다.
F.T(fault tolerance)	interrupt가 발생하면, 자동으로 연결을 복구하며, interrupt 전에 연결된 파일을 reopen 합니다.
stateful protocol	CIFS 서버는 연결된 모든 client에 대한 연결정보를 가지고 있습니다. 그래서 네트워크나 CIFS 서버에 장애 발생시, 모든 client는 연결이 끊겼다는 통지를 받게 되며, client는 재 연결을 시도할 수 있습니다.

표 6. CIFS 특징

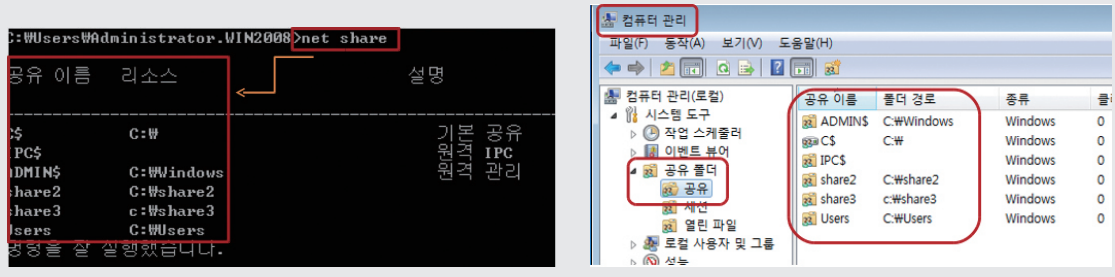
공유폴더는 윈도우 탐색기에서 쉽게 만들 수 있습니다. 공유폴더를 만들 때 권한을 할당하지 않으면, 기본적으로 Everyone-Read(읽기) 권한이 할당됩니다.



(a) (b)

그림 33. 탐색기에서 공유폴더를 만들 수 있으며, 기본권한은 Everyone에 읽기이다

로컬 PC에 존재하는 모든 공유 폴더 정보를 확인할 때는, net share 명령을 사용합니다. 물론 컴퓨터 관리에서도 확인할 수 있으며, compmgmt.msc 명령을 통해서도 컴퓨터 관리에 들어갈 수 있습니다.



(a) (b)

그림 34. 로컬 PC에 존재하는 공유폴더는 net share 명령이나 컴퓨터 관리에서 확인할 수 있습니다

김해중
KBS 보도기술국

windows는 관리목적으로 여러 가지 공유가 기본적으로 만들어져 있으며, 그중의 일부는 숨김 공유입니다. 숨김 공유는 공유 이름 뒤에 $ 표시가 붙어져 있습니다.

window 기본 공유	특 징
C$, D$	CD-ROM을 포함한 모든 드라이브는 숨김 공유를 가지고 있습니다.
ADMIN$	운영체제가 설치된 위치에, 기본적으로 매핑되는 숨김 공유입니다.
PRINT$	공유 프린터를 생성할 때마다, 시스템은 PRINT$ 공유폴더에 프린터 드라이버를 두어서. 클라이언트가 프린터에 접근할 때, 쉽게 드라이버를 다운로드 받게 합니다.
IPC$	서버 간 통신에 사용되는 공유입니다.
NETLOGON	DC(Domain Controller)에서 사용자의 logon을 처리할 때 사용합니다.
SYSVOL	그룹 정책 정보와 script 정보를 저장하는데 사용되며, DC(Domain Controller)는 항상 해당 정보를 가지고 있습니다.

표 7. windows의 기본 공유폴더

공유폴더는 net share 명령으로 만들 수 있습니다.

만들기	net share <공유이름=drive:path>
삭 제	net share 공유이름 /delete
예제 1)	net share myshare=C:\Users\Myname - C드라이브의 \users\Myname 폴더를 (myshare)라는 이름으로 공유
예제 2)	net share AAA=c:\aaa /grant:john,Full /grant:everyone,read - C드라이브의 aaa폴더를 (AAA)이름으로 공유하면서, john에게 Ful 권한을 할당하고, everyone에게 read 권한을 할당
예제 3)	net share c$ /delete - C드라이브 공유삭제
예제 4)	net share ABC=c:\abc /USRES=5 - 공유폴더에 동시에 최대 5명이 접속 가능
예제 5)	net share ABC=c:\abc /Unlimited - 공유폴더 인원 접속제한이 없다
예제 6)	net share ABC$=c:\abc - 공유 이름 뒤에 $를 붙이면 숨김 공유가 된다

표 8. net share 명령으로 공유 폴더를 관리할 수 있습니다

원격 PC에 있는 공유 폴더에 접근할 때는 UNC(universal naming convention) 방식을 사용합니다. UNC는 "\\server이름\공유이름"으로 표현하며, server 이름은 IP 주소, domain name, NETBIOS name 모두 가능합니다. 만약 공유이름을 입력하지 않고 server 이름만으로 접속하면(예) \\server이름), 해당 서버의 모든 공유 폴더를 보여줍니다.

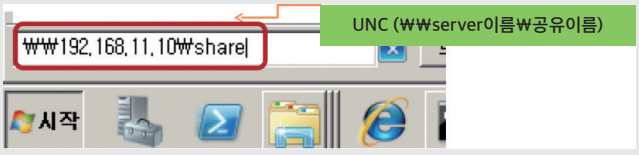


그림 35. 공유폴더에 접근할 때는 UNC(universal naming convention)를 사용합니다

(a) (b)

그림 36. 공유이름을 입력하지 않고, server 이름만으로 접속하면, 해당 서버의 모든 공유 폴더를 보여줍니다

특정 공유폴더에 계속 접근해야 한다면, 공유폴더에 드라이브 문자를 할당해서, 별도의 network 드라이브로 만들 수 있습니다. “로그온 할 때 다시 연결”을 체크하면, 부팅될 때마다 해당 드라이브에 자동으로 연결됩니다.

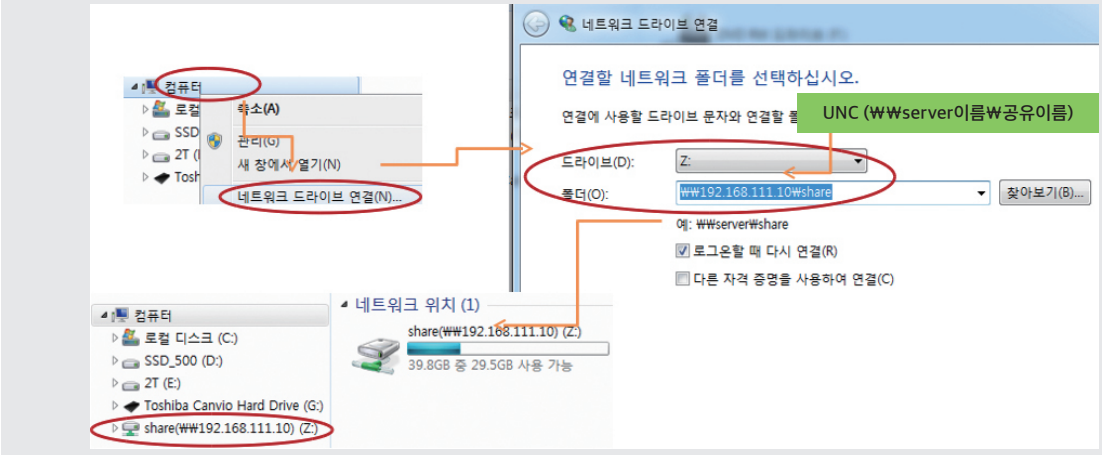


그림 37. 공유폴더에 계속 접근해야 한다면, 공유폴더에 네트워크 드라이브를 할당합니다

net use 명령을 통해 네트워크 드라이브를 만들고 삭제할 수 있습니다.

기능	명령어
네트워크 드라이브 만들기	net use drive이름 UNC(\\server이름\공유이름)
만들어진 네트워크 드라이브 확인	net use
네트워크 드라이브 연결 끊기	net use drive이름 /delete
모든 네트워크 드라이브 연결 끊기	net use * /delete
PC를 reboot하면 연결 끊어짐	net use z: \\10.1.1.1\share /persistent:no

표 9. net use 명령어를 이용해 네트워크 드라이브 세팅

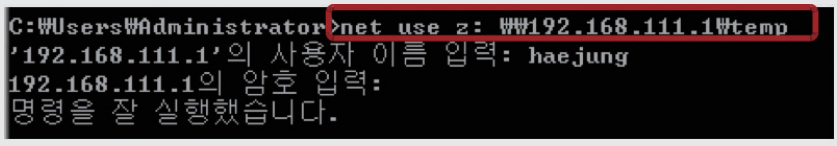


그림 38. net use 명령으로 네트워크 드라이브를 만들 수 있습니다

그림 39. net use 명령을 입력해, 존재하는 네트워크 드라이브를 확인합니다

김해중
KBS 보도기술국

NFS 공유 접근

일반적으로 window는 CIFS를 사용하고, linux는 NFS(network file system) 공유를 사용해서 서로 호환이 되지 않았습니다. 그래서 과거에 windows와 linux를 서로 연결할 때는, linux에 별도의 SAMBA 기능을 세팅해야 했었습니다. 하지만 windows 7의 enterprise/ultimate edition 또는 window 2008R2 이후 버전에서는, NFS에 직접 접근할 수 있는 NFS client를 내장하고 있습니다.

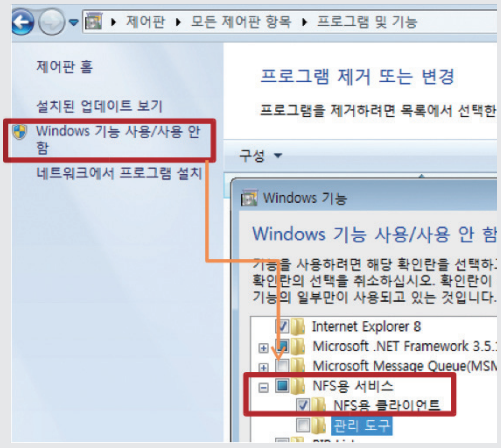


그림 40. window 7에서 NFS 공유에 접근하려면, NFS client를 설치해야 합니다

내용	명령어 사용법
NFS용 네트워크 드라이브 생성	mount\\컴퓨터이름\공유이름 드라이브명
NFS용 네트워크 드라이브 삭제	umount 드라이브이름

표 10. NFS용 네트워크 드라이브 관련 명령어

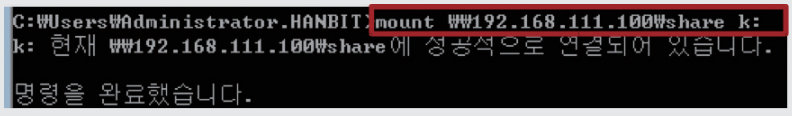


그림 41. mount 명령으로, NFS 접근 용도의 네트워크 드라이브를 생성할 수 있습니다

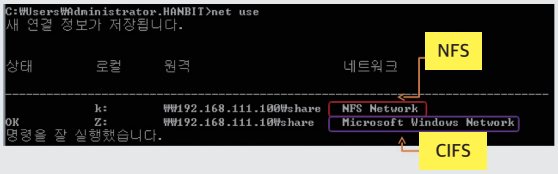


그림 42. net use 명령으로, 생성된 네트워크 드라이브를 확인할 수 있습니다

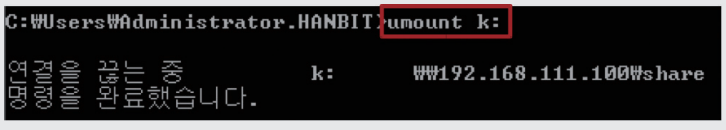


그림 43. umount 명령으로 NFS용 네트워크 드라이브를 삭제할 수 있습니다

요약

개 념	정 리
ipconfig	간단히 IP 정보를 보여줍니다.
ipconfig/all	IP에 관련된 세부 정보를 보여줍니다.
IP (169.x.x.x 대역)	Microsoft의 사설 IP 대역(PC가 IP를 받지 못 할 때 할당합니다.)
arp -a	arp cache table을 확인하는 명령어이다.
arp -d	arp cache table을 삭제하는 명령어이다.
getmac /s	원격지에 있는 PC의 MAC-address을 알고 싶을 때 사용하는 명령어이다.
netstat -an	PC에서 사용 중인 TCP/UDP port 정보를 보여준다.
ping	원격지에 있는 PC가 동작 중인지 확인하는 명령어이다.
ping -t	ctrl c를 누를 때 까지, 계속 ping 패킷을 전송한다.
tracert -d	목적지까지의 경로를 상세히 확인할 때 사용하는 명령어이다.
route print	PC에 존재하는 routing table을 확인하는 명령어이다.
route add/change/delete	outing table을 추가, 삭제, 변경할 때 사용한다.
CIFS	windows 환경에서 주로 사용하는 파일 공유 프로토콜이다.
숨김 공유	공유를 숨기고 싶을 때는, 공유이름 뒤에 $를 붙이면 된다.
UNC(universal naming convention)	공유폴더에 접근할 때 사용하는 경로명으로, [\\서버이름\공유이름]으로 표현한다.
net share	local PC의 공유 폴더에 대한 관리를 할 때 사용하는 명령어이다.
net use	네트워크 드라이브를 관리할 때 사용하는 명령어이다.
mount	windows에서 NFS 공유에 대한 네트워크 드라이브를 만들 때 사용하는 명령어이다. - window 7 enterprise/ultimate edition 또는 window 2008R2 이후 버전에서만 지원합니다.
umount	windows에서 NFS 공유에 대한 네트워크 드라이브를 삭제할 때 사용하는 명령어이다.