

ipTIME X1005

사용자 설명서

Revision 1.0

사용자 설명서 보는 방법

- 1장 ~ 4장의 내용에 따라 PC를 설정하고 ipTIME X1005의 인터넷 연결을 설정하면 공유기에 연결된 PC에서 인터넷을 사용할 수 있으며 자동 백업과 자동 분산 기능을 이용하여 2개의 인터넷 회선을 연결할 수 있습니다.
- 5장 ~ 12장은 ipTIME X1005의 모든 기능을 설명하는 고급 기능 설명서입니다. 제품 사용시 필요한 기능에 해당하는 부분의 사용법을 참고하시기 바랍니다.

목차

사용자 설명서 보는 방법	2
목차	2
기본 기능	6
1장 제품 개요	7
1.1 제품 특징	7
1.2 제품 구성	8
1.3 제품 본체 기능 설명	9
2장 IPTIME X1005 연결	10
2.1 전원 어댑터 연결	10
2.2 모뎀의 연결	10
2.3 PC의 연결	10
3장 PC 환경 설정	11
3.1 윈도우 98/ME 설정	12
3.2 윈도우 2000 설정	15
3.3 윈도우 XP 설정	18

4장 인터넷 설정 마법사로 IPTIME X1005 인터넷 연결	22
4.1 IPTIME X1005 내장 웹서버 접속	23
4.2 IPTIME X1005 인터넷 설정 마법사 실행	24
4.3 자동 검색에 의한 PPPoE 연결 예	25
4.4 자동 검색에 의한 동적 IP 연결 예	27
4.5 수동 설정을 이용한 고정 IP 연결	29
4.6 수동 설정을 이용한 동적 IP 연결	31
4.7 수동 설정을 이용한 PPPoE 연결	33
5장 웹 설정 화면 이용하기	36
5.1 IPTIME X1005 내장 웹 서버 접속	36
5.2 도움말 기능	37
5.3 설정저장 기능	38
6장 시스템 정보	39
6.1 인터넷 연결 상태	39
6.2 내부 네트워크 정보	40
6.3 컨넥션 정보	41
7장 네트워크 설정	42
7.1 WAN1/WAN2 연결 설정	42
7.2 내부 PC 연결 설정	47
7.3 네트워크 감시 (NET DETECTOR)	52
7.4 링크 설정 정보	55
7.5 라우팅 테이블 관리	56
7.6 스위치 설정	57
8장 시스템 설정	58
8.1 관리자 설정	58
8.2 펌웨어 업그레이드	60
8.3 시스템 로그	63

8.4 기타 설정	64
9장 QoS 설정	68
9.1 QoS 기본 설정	68
9.2 IP 주소별 QoS 설정	70
9.3 어플리케이션별 QoS 설정	72
9.4 포트별 QoS 설정	74
10장 통신 정책 설정	76
10.1 분산 정책 설정	76
10.2 어플리케이션 설정	80
10.3 내부 서버 설정	82
10.3 포트포워드 설정	84
10.5 포트 트리거 설정	86
10.6 NAT ON/OFF 기능	88
11장 고급 설정	89
11.1 보안 설정	89
11.2 DDNS 설정	92
11.3 원격 PC 제어 (WOL)	94
11.4 사이트 접속 차단	95
11.5 원격 공유기 관리	96
11.6 사용 시간 제한	97
12장 VPN 서버 기능	99
12.1 VPN 서버 기능	99
12.2 VPN 서버 설정 방법	100
12.3 WINDOWS 98/ME에서의 VPN 서버 접속	101
12.4 WINDOWS 2000에서의 VPN 서버 접속	106
12.5 WINDOWS XP에서의 VPN 서버 접속	112
부록 A. LAN CABLE 규격	118

부록 B. IP 공유기 PING 시험	119
-----------------------------	------------

부록 C. 제품 사양	120
--------------------	------------

부록 D. 인터넷이 끊겼을 때의 확인사항	121
-------------------------------	------------

부록 E. 제품 보증서 및 고객 지원	124
-----------------------------	------------

기본 기능

- 1장 ~ 4장은 ipTIME X1005 환경에서 인터넷을 사용할 수 있도록 PC를 설정하고, ipTIME X1005의 인터넷 연결을 설정하는 방법을 설명하고 있습니다.
- ipTIME X1005를 설치하시는 경우 1장 ~ 4장의 내용을 숙지하고 제품을 설치하시기 바랍니다.

1장 제품 개요

1.1 제품 특징

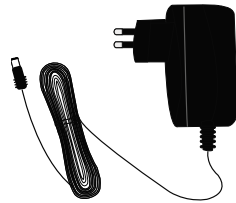
- ☐ 2 WAN 인터넷 접속
- ☐ 국내 모든 인터넷 환경 접속 가능
- ☐ Line backup / 트래픽 분산
- ☐ PPTP VPN 서버 내장
- ☐ 인터넷 속도 조절을 위한 QoS
- ☐ 105Mbps의 인터넷 공유 속도 지원
- ☐ 100Mbps 5 포트 스위치 허브 내장
- ☐ 케이블 자동 감지 기능
- ☐ 최대 253대 PC의 인터넷 연결 지원
- ☐ 어플리케이션 설정, 내부 서버 설정
- ☐ 공인 IP 주소를 그대로 사용할 수 있는 TWIN-IP 기능
- ☐ 사용 시간 제한 기능 및 기타 고급 기능 지원
- ☐ Multi Channel VPN Pass Through
- ☐ UPnP 지원

1.2 제품 구성

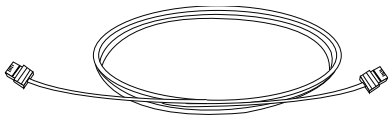
다음과 같은 내용물이 모두 들어 있는지 확인합니다.



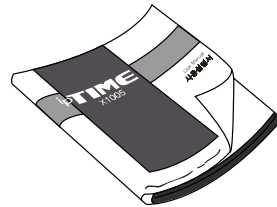
<그림 : 본체>



<그림 : 전원 어댑터>



<그림 : UTP 케이블>



<그림 : 사용설명서>



<그림 : CD>

1.3 제품 본체 기능 설명

LED 램프

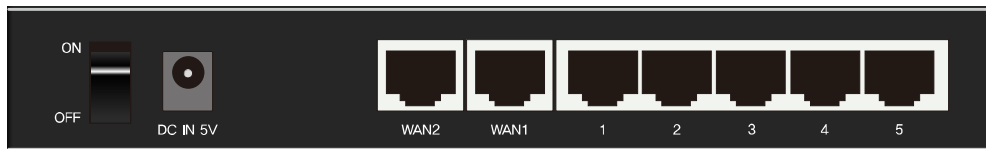
- PWR 램프: 전원 공급 상태를 나타냅니다. (전원 ON시 켜짐)
- CPU 램프 : 제품의 동작 상태를 나타냅니다. (정상 동작 시 1초 간격으로 깜박임)
- WAN 램프: 인터넷 모뎀 연결 상태를 나타냅니다. (연결 시 ON, 통신시 깜박임)
- LAN 램프 : PC 연결 상태를 나타냅니다. (연결 시 ON, 통신시 깜박임)



<ipTIME X1005 LED>

컨넥터

- 전원 스위치 : 스위치를 ON으로 하면 제품이 켜지며 OFF로 하면 꺼집니다.
- DC-IN : 전원 어댑터를 연결하는 컨넥터입니다.
- WAN 포트 : 인터넷 모뎀이 연결되는 RJ-45 컨넥터입니다.
- LAN 포트 : PC가 연결되는 RJ-45 컨넥터입니다.



<ipTIME X1005 후면>

리셋 스위치

- 시스템 리셋 : 동작 중 5초 이상 누르고 있으면 시스템이 재시작 됩니다.
- 공장 초기화 : 리셋을 누른 상태에서 전원 스위치를 OFF한 뒤 2초 후 다시 전원 스위치를 ON하고 약 10초간 기다리면 CPU 램프가 빠르게 점멸합니다. CPU 램프의 빠른 점멸이 중단되었을 때 리셋 스위치를 때면 시스템이 공장 출하 상태로 초기화됩니다.



<ipTIME X1005 전면>

2장 ipTIME X1005 연결

2.1 전원 어댑터 연결

- 전원 어댑터를 AC 단자에 연결하고 DC 컨넥터를 연결합니다.
- 전원 스위치를 켜면 모든 램프가 1초 정도 ON 후 OFF됩니다.
- 부팅이 완료되면 ipTIME X1005의 CPU 램프가 1초 정도의 간격으로 깜박입니다.

2.2 모뎀의 연결

- 모뎀의 LAN 단자(모뎀에 따라 표기 다름)와 ipTIME X1005의 WAN 1,2를 연결합니다.
- 주 회선을 WAN1, 보조 회선을 WAN2에 연결합니다.
- LAN 선이 정상 연결되면 WAN 램프가 ON되며 통신이 있는 경우 깜박입니다.

[참고] ipTIME X1005에는 케이블 자동 감지 기능이 있어 다이렉트(스트레이트), 크로스 케이블을 자유롭게 사용할 수 있습니다.

2.3 PC의 연결

- PC의 LAN 카드 또는 머더보드의 LAN 포트를 ipTIME X1005 LAN 1~5에 연결합니다.
- 정상 연결된 경우 해당 LAN 램프가 ON되며 통신 시 램프가 깜박입니다.

[참고]

- 허브의 UP-LINK로 연결하는 경우 UP-LINK 바로 옆 포트에는 사용할 수 없습니다.
- 허브와 공유기는 하나의 포트만 연결합니다. 2개 이상 연결 시 사용할 수 없습니다.
- ipTIME X1005에는 케이블 자동 감지 기능이 있어 다이렉트(스트레이트), 크로스 케이블을 자유롭게 사용할 수 있습니다.

3장 PC 환경 설정

이장에서는 PC의 네트워크 환경을 ipTIME X1005에 연결하여 사용할 수 있도록 설정하는 방법을 윈도우 운영 체제 종류에 따라 기술하고 있습니다.

윈도우와 같은 운영 체제에서 인터넷을 사용하기 위해서는 TCP/IP라는 프로토콜이 필요합니다. ipTIME X1005의 정상적인 사용을 위해서는 TCP/IP 프로토콜을 정상적으로 설정하여야 합니다.

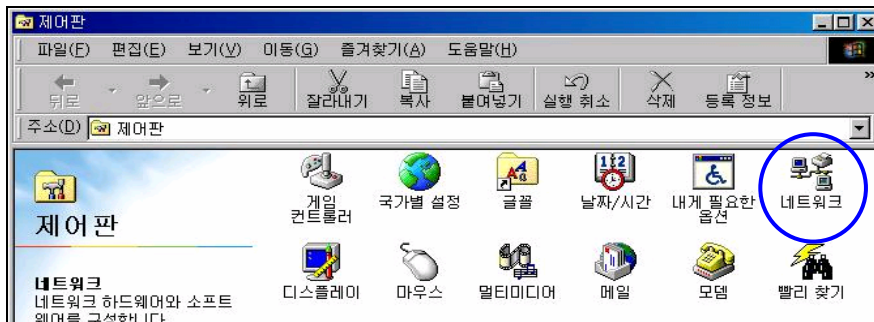
- 일반적인 경우 PC에 윈도우가 처음 설치된 상태가 바로 공유기를 사용할 수 있는 상태이며 이 상태에서는 별도의 TCP/IP 설정이 필요하지 않습니다.
- ADSL 서비스 환경에서 사용하던 컴퓨터는 ADSL 접속 프로그램(PPPoE 접속 프로그램)이 설치된 경우 공유기 환경에서 문제가 발생할 수 있으므로 이것을 먼저 삭제한 뒤 본 장의 내용에 따라 네트워크 환경을 설정합니다.
 - Windows 98/ME/2000의 경우 별도로 설치된 ADSL 접속 프로그램 삭제
 - Window XP의 경우 설치된 광대역 연결을 삭제
 - 삭제 방법은 본 사용설명서 20쪽을 참고합니다.
- LAN 방식, VDSL방식, IP-ADSL 방식, 케이블 모뎀 방식의 인터넷 서비스 환경에서 사용하던 컴퓨터의 경우 별도의 윈도우 환경 설정 변경 없이도 바로 공유기에 연결하여 사용할 수 있습니다.

3.1 윈도우 98/ME 설정

이 과정은 윈도우 98/ME의 TCP/IP 설정을 초기값으로 복원하는 것입니다. PC에 윈도우가 처음 설치된 상태라면 변경은 없으며 다음에 따라 모든 값이 정상적인지를 확인합니다.

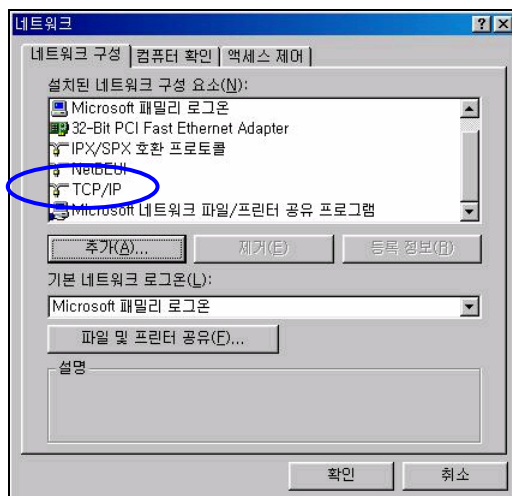
PC의 TCP/IP 설정이 완료된 후 ipTIME X1005에서 자동으로 IP 주소를 부여 받는지 확인하기 위해서는 윈도우를 설정하기 전에 2장의 내용에 따라 PC와 ipTIME X1005를 LAN 케이블로 연결하고 ipTIME X1005을 켜두어야 합니다.

- 윈도우 [시작] 버튼을 클릭한 후 메뉴에서 [설정] >> [제어판]을 선택합니다.
- 제어판 윈도우에서 [네트워크] 아이콘을 더블 클릭합니다.



<네트워크 아이콘 선택>

- 네트워크 구성 요소 중 TCP/IP를 더블 클릭하여 [자동으로 IP 주소지정]을 선택합니다.
- 전화 접속 어댑터에 연결된 TCP/IP는 무시하고 랜 카드 관련 TCP/IP만 설정합니다.

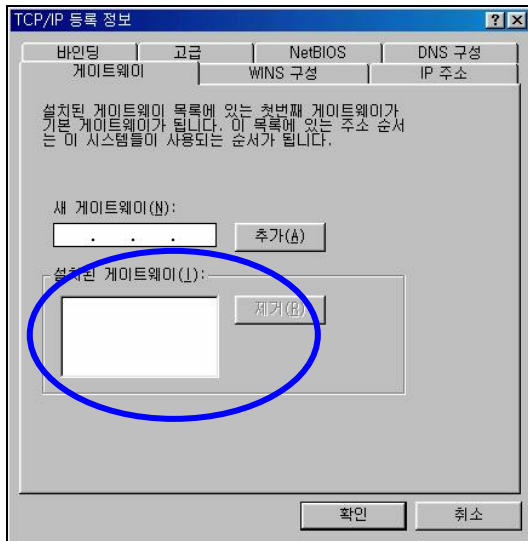


<TCP/IP 선택>

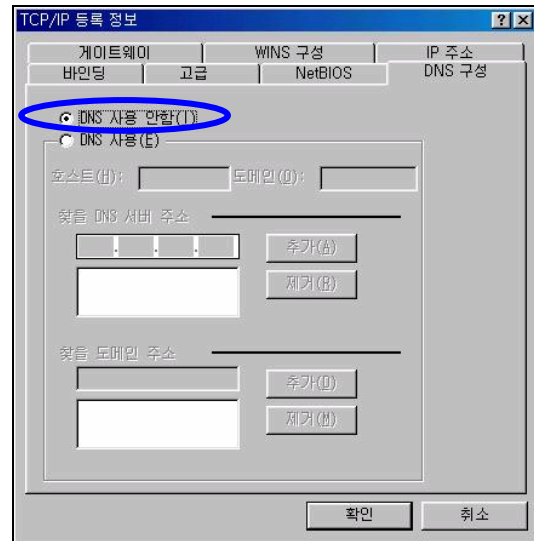


<자동 IP 주소 선택>

- 게이트웨이 항목에서 설치된 모든 게이트웨이를 제거합니다.
- DNS 구성에서 "DNS 사용 안함"을 선택합니다.

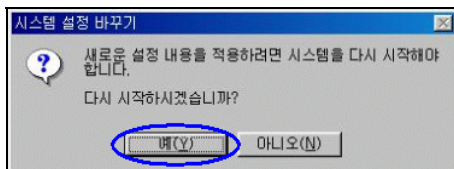


<게이트웨이 항목 전부 제거>



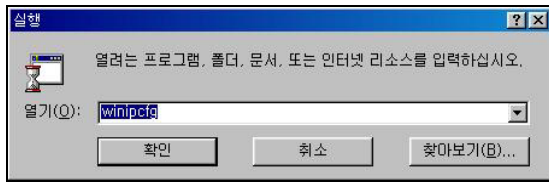
<DNS 사용 안함 선택>

- IP주소, 게이트웨이, DNS 구성의 3가지 항목에 대한 설정이 완료되면 확인 버튼을 클릭하여 TCP/IP 등록 정보 창을 닫습니다. 이후 "네트워크" 창이 표시되면 다시 확인을 클릭합니다.
- 윈도우98의 경우 네트워크와 관련된 설정이 변경되면 자동으로 시스템이 재시작 됩니다. 시스템 설정 바꾸기 화면이 표시되면 "예"를 선택하여 윈도우를 다시 시작합니다.



<시스템 재시작 확인>

- PC가 재시작되면 ipTIME X1005에서 IP 주소를 자동으로 할당합니다. 자동할당을 위해서 PC와 ipTIME X1005가 LAN 케이블로 연결되어야 합니다. 만일 케이블을 연결하지 않았다면 케이블을 연결한 후 PC를 다시 시작하여야 합니다.
- IP 주소 자동 할당 확인은 winipcfg 프로그램을 이용하여 확인할 수 있습니다.
- 윈도우 [시작] 버튼을 클릭한 후 메뉴에서 [실행]을 선택하여 열기 항목에 그림과 같이 "winipcfg"를 입력하고 확인 버튼을 클릭합니다.

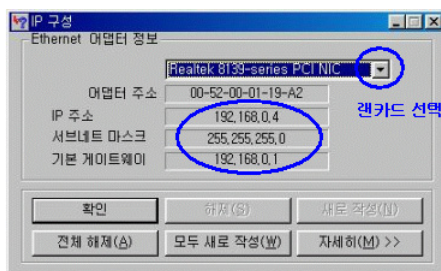


<winipcfg 실행>

- winipcfg의 IP 구성창에서 공유기와 연결하여 사용하는 랜카드 어댑터 (NDIS 5.0 또는 해당 랜카드 선택, PPP 어댑터는 선택하면 안됨)를 선택하여 PC의 IP 주소가 192.168.0.2 ~ 192.168.0.254 사이의 값으로 자동 할당되었는지를 확인합니다. 만일 랜카드 선택에서 PPP 어댑터 이외에 사용하는 랜카드가 보이지 않을 경우에는 랜카드 드라이버를 재설치하여야 합니다.

(랜카드 선택 후 "해제"버튼을 클릭 후 "모두 새로 작성" 또는 "모두 갱신"버튼을 클릭하여 IP할당 확인)

[참고] ipTIME X1005에 연결된 모든 PC는 각각 다른 IP 주소를 할당 받게 됩니다.



랜카드 선택 : NDIS 5.0 또는 해당 랜카드 선택
 어댑터 주소 : 어댑터마다 다른 값, 무시 가능
 IP 주소 : 192.168.0.2 ~ 192.168.0.254
 서브넷 마스크 : 255.255.255.0
 기본 게이트웨이 : 192.168.0.1

<IP 주소 확인>

[참고] PC의 IP 주소가 정상적으로 자동 할당되지 않는다면 다음 사항을 확인한 뒤 PC를 재시작하여 IP주소가 할당되는지 확인합니다.

- PC와 ipTIME X1005 사이의 LAN 케이블 연결
- TCP/IP의 설정 내용 확인
- ADSL 접속 프로그램의 제거 여부

위의 사항을 확인하여도 IP 주소가 정상적으로 자동 할당되지 않는다면 당사 홈페이지 (<http://www.iptime.co.kr>)를 참고하여 IP 주소 수동 설정 방법으로 IP 주소를 설정하거나 ipTIME 고객센터(070-7018-1199)로 문의하시기 바랍니다.

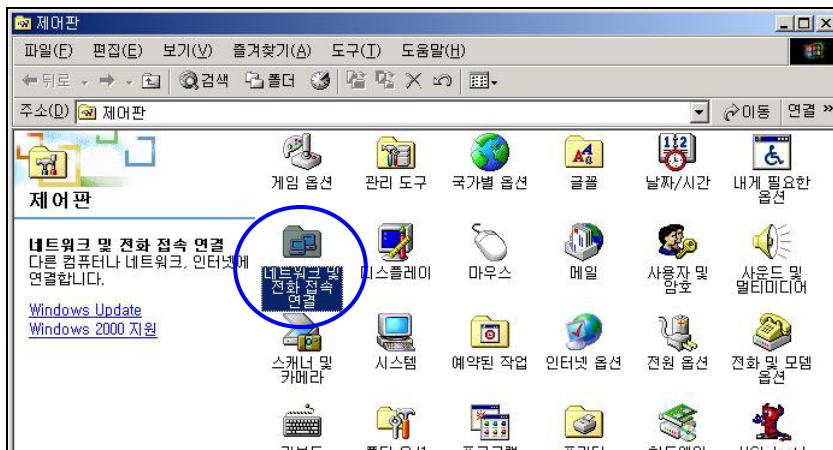
PC 설정을 완료한 뒤 인터넷을 사용하기 위해서는 4장의 내용을 참고하여 ipTIME X1005의 WAN 포트를 인터넷에 연결 설정합니다. 인터넷 연결 설정은 ipTIME X1005에서 이루어지는 것이므로 모든 PC에서 설정할 필요는 없으며 한번만 설정하면 됩니다.

3.2 윈도우 2000 설정

이 과정은 윈도우 2000의 TCP/IP 설정을 초기값으로 복원하는 것입니다. PC에 윈도우가 처음 설치된 상태가 아니거나 인터넷이 정상적으로 동작하지 않는다면 다음 과정에 따라 모든 값이 정상인지를 확인합니다.

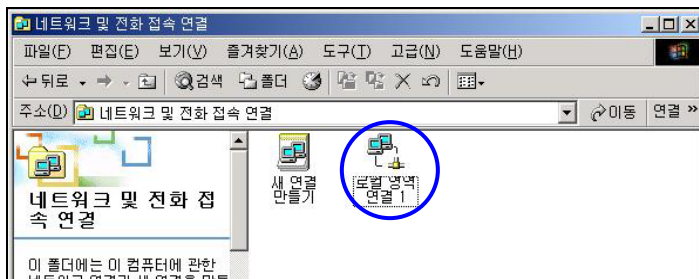
PC의 TCP/IP 설정이 완료된 후 ipTIME X1005에서 자동으로 IP 주소를 부여 받는지 확인하기 위해서는 윈도우를 설정하기 전에 2장의 내용에 따라 PC와 ipTIME X1005를 LAN 케이블로 연결하고 ipTIME X1005을 켜두어야 합니다.

- 윈도우 [시작] 버튼을 클릭한 후 메뉴에서 [설정] >> [제어판]을 선택한 뒤 “네트워크 및 전화 접속 연결” 아이콘을 더블 클릭합니다.



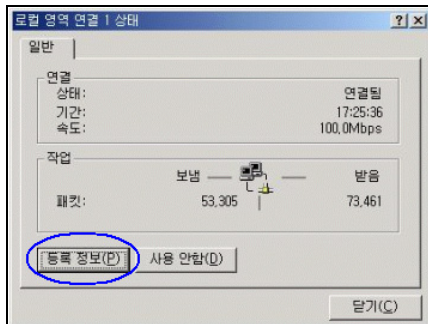
<네트워크 및 전화 접속 연결 더블 클릭>

- 네트워크 및 전화 접속 연결 윈도우에서 로컬 영역 연결 아이콘을 더블 클릭합니다.

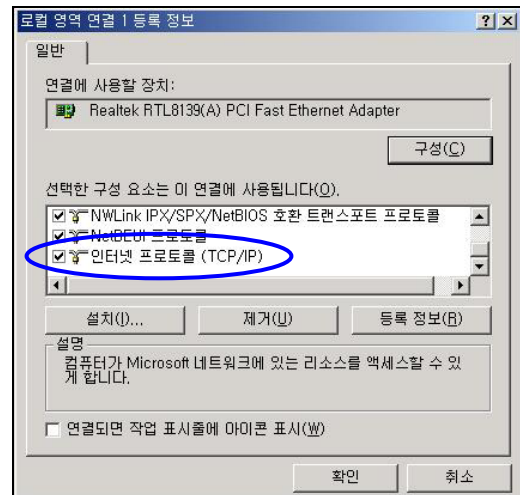


<로컬 영역 연결 더블 클릭>

- 로컬 영역 연결 윈도우에서 등록 정보를 클릭합니다.
- 등록 정보 윈도우에서 인터넷 프로토콜 (TCP/IP)을 더블 클릭합니다.

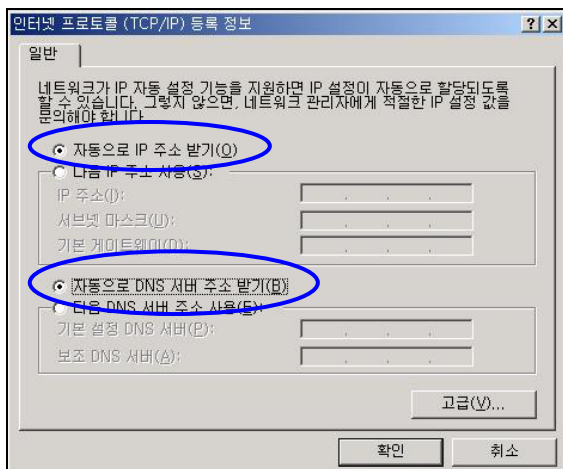


<등록 정보 선택>



<TCP/IP 더블 클릭>

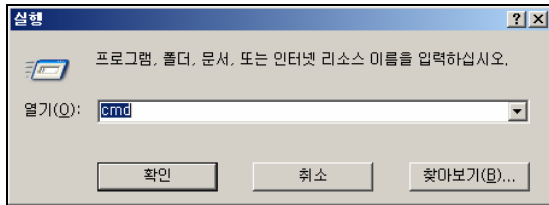
- “자동으로 IP 주소 받기”와 “자동으로 DNS 서버 주소 받기”를 선택합니다.



<자동 선택 후 확인 클릭>

- 설정완료 후 확인버튼을 클릭하고 네트워크 및 전화접속연결 창도 모두 닫습니다.
- TCP/IP 설정을 완료하면 ipTIME X1005에서 IP 주소를 자동으로 할당합니다. 자동 할당을 위해서 PC와 ipTIME X1005가 LAN 케이블로 연결되어야 합니다. 만일 케이블을 연결하지 않았다면 케이블을 연결한 뒤 PC를 다시 시작합니다.

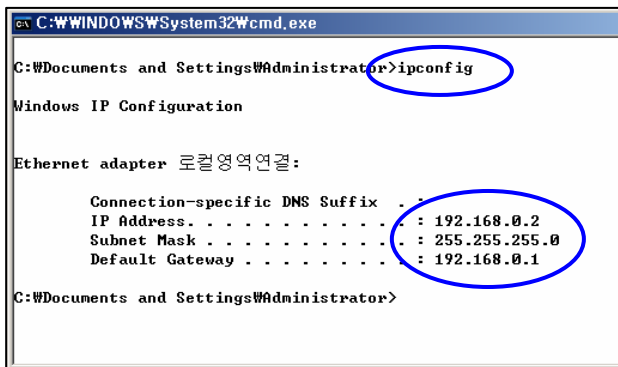
- IP 주소 자동 할당 확인은 명령 프롬프트의 **ipconfig** 명령으로 확인할 수 있습니다.
- 명령 프롬프트는 윈도우 화면 좌측 하단의 **[시작]** 버튼을 클릭한 뒤 **[실행]**을 선택하여 열기에 그림과 같이 **"cmd"**를 입력하고 확인 버튼을 클릭하면 실행됩니다.



<cmd 실행>

- 명령 프롬프트가 실행되면 아래 그림과 같이 **"ipconfig"** 명령을 입력하여 PC에 자동 할당된 IP 주소, 서브네트마스크, 게이트웨이 등을 확인합니다.

[참고] ipTIME X1005에 연결된 모든 PC는 각각 다른 IP 주소를 할당 받게 됩니다.



IP Address : 192.168.0.2~254
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.0.1

<IP 주소 확인>

[참고] PC의 IP 주소가 정상적으로 자동 할당되지 않는다면 다음 사항을 확인한 뒤 PC를 재시작하여 IP주소가 할당되는지 확인합니다.

- PC와 ipTIME X1005 사이의 LAN 케이블 연결
- TCP/IP의 설정 내용 확인
- ADSL 접속 프로그램의 제거 여부

위의 사항을 확인하여도 IP 주소가 정상적으로 자동 할당되지 않는다면 당사 홈페이지 (<http://www.iptime.co.kr>)를 참고하여 IP 주소 수동 설정 방법으로 IP 주소를 설정하거나 ipTIME 고객센터(070-7018-1199)에 문의하시기 바랍니다.

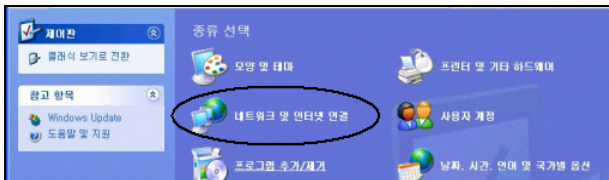
PC 설정을 완료한 뒤 인터넷을 사용하기 위해서는 4장의 내용을 참고하여 ipTIME X1005의 WAN 포트를 인터넷에 연결 설정합니다. 인터넷 연결 설정은 공유기에서 이루어지는 것이므로 모든 PC에서 설정할 필요는 없으며 한번만 설정하면 됩니다.

3.3 윈도우 XP 설정

이 과정은 윈도우 XP의 TCP/IP 설정을 초기값으로 복원하는 것입니다. PC에 윈도우가 처음 설치된 상태라면 변경은 없으며 다음 과정에 따라 모든 값이 정상적인지를 확인합니다.

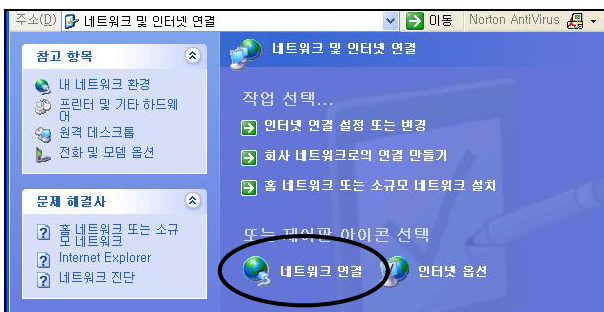
PC의 TCP/IP 설정이 완료된 후 ipTIME X1005에서 자동으로 IP 주소를 부여 받는지 확인하기 위해서는 윈도우를 설정하기 전에 2장의 내용에 따라 PC와 ipTIME X1005를 LAN 케이블로 연결하고 ipTIME X1005을 켜두어야 합니다.

- 윈도우 **시작** 버튼을 클릭한 후 메뉴에서 **설정** >> **제어판**을 선택합니다.
- 제어판의 **네트워크 및 인터넷 연결** 아이콘을 더블 클릭합니다.



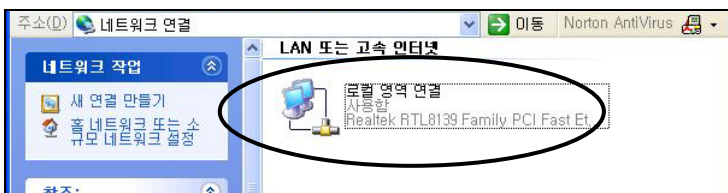
<네트워크 및 인터넷 연결 더블 클릭>

- 네트워크 및 인터넷 연결에서 네트워크 연결 아이콘을 더블 클릭합니다.



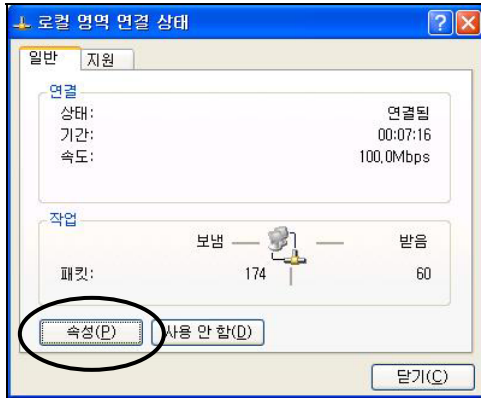
<네트워크 연결 더블 클릭>

- 네트워크 연결에서 로컬 영역 연결을 더블 클릭하여 선택합니다.



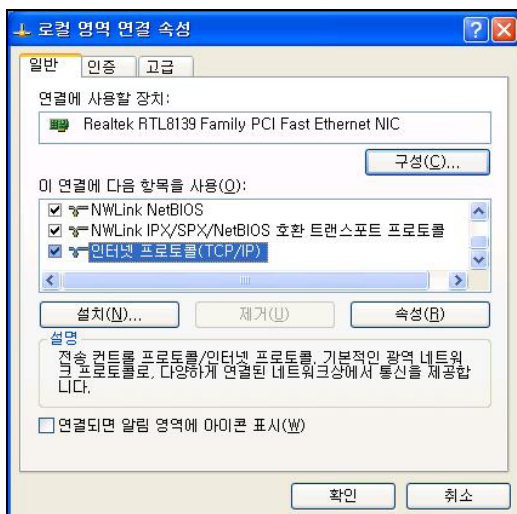
<로컬 영역 연결 더블 클릭>

- 로컬 영역 연결 상태에서 속성을 클릭하여 선택합니다.

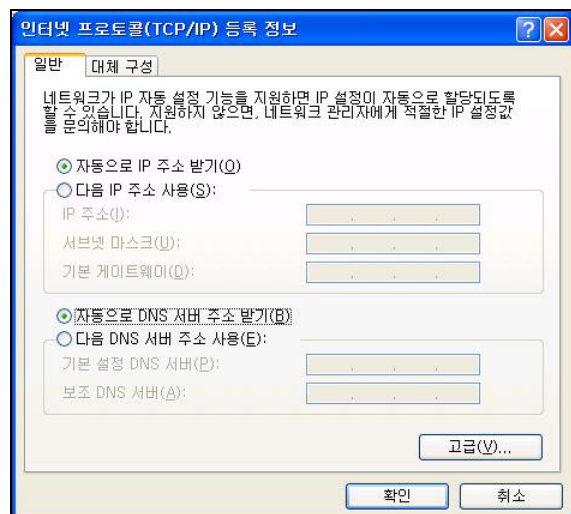


<속성 더블 클릭>

- 인터넷 프로토콜 (TCP/IP)를 더블 클릭하여 선택하고 자동으로 IP 주소 받기와 자동으로 DNS 서버 주소 받기를 선택합니다.



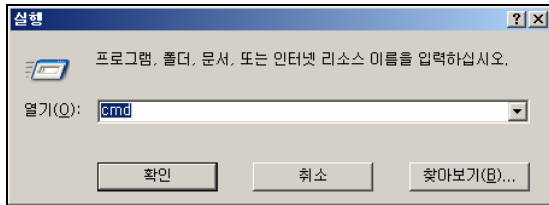
<TCP/IP 더블 클릭>



<자동 선택 후 확인 클릭>

- 설정이 완료된 뒤 확인 버튼을 클릭하고 로컬 영역 연결 속성 창도 모두 닫아 줍니다.
- TCP/IP 설정을 완료하면 ipTIME X1005에서 IP 주소를 자동으로 할당합니다. 자동 할당을 위해서 PC와 ipTIME X1005가 LAN 케이블로 연결되어야 합니다. 만일 케이블을 연결하지 않았다면 케이블을 연결한 뒤 PC를 다시 시작합니다.

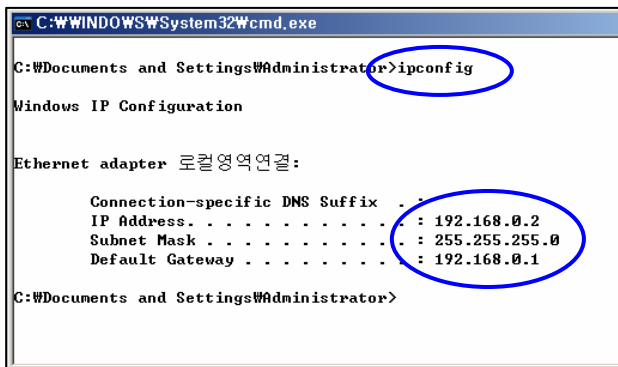
- IP 주소 자동 할당 확인은 명령 프롬프트의 **ipconfig** 명령으로 확인할 수 있습니다.
- 명령 프롬프트는 윈도우 화면 좌측 하단의 **[시작]** 버튼을 클릭한 뒤 **[실행]**을 선택하여 열기에 그림과 같이 **"cmd"**를 입력하고 확인 버튼을 클릭하면 실행됩니다.



<cmd 실행>

- 명령 프롬프트가 실행되면 아래 그림과 같이 **"ipconfig"** 명령을 입력하여 PC에 자동 할당된 IP 주소, 서브네트마스크, 게이트웨이 등을 확인합니다.

[참고] ipTIME X1005에 연결된 모든 PC는 각각 다른 IP 주소를 할당 받게 됩니다.



IP Address : 192.168.0.2~254
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.0.1

<IP 주소 확인>

[참고] PC의 IP 주소가 정상적으로 자동 할당되지 않는다면 다음 사항을 확인한 뒤 PC를 재시작하여 IP주소가 할당되는지 확인합니다.

- PC와 ipTIME X1005 사이의 LAN 케이블 연결
- TCP/IP의 설정 내용 확인
- ADSL 접속 프로그램(광대역 연결 아이콘)의 제거 여부

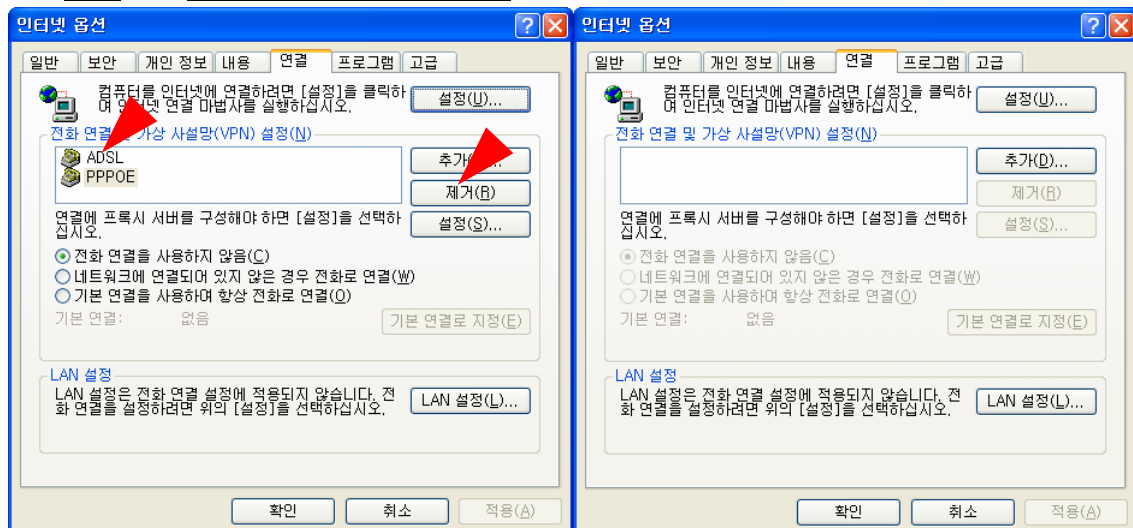
위의 사항을 확인하여도 IP 주소가 정상적으로 자동 할당되지 않는다면 당사 홈페이지 (<http://www.iptime.co.kr>)를 참고하여 IP 주소 수동 설정 방법으로 IP 주소를 설정하거나 ipTIME 고객센터(070-7018-1199)에 문의하시기 바랍니다.

PC 설정을 완료한 뒤 인터넷을 사용하기 위해서는 4장의 내용을 참고하여 ipTIME X1005의 WAN 포트를 인터넷에 연결 설정합니다. 인터넷 연결 설정은 공유기에서 이루어지는 것이므로 모든 PC에서 설정할 필요는 없으며 한번만 설정하면 됩니다.

[참고] ADSL 사용시 인터넷 접속 프로그램 삭제 방법 (windows 98/ME, 2000)

PPPoE 연결방식의 경우 Internet Explorer 실행시 접속프로그램의 자동실행으로 설정화면이 나오지 않는 경우가 발생합니다. 이러한 경우 반드시 자동 실행되게 하는 연결 아이콘을 삭제하셔야 합니다.

ADSL의 PPPoE 연결방식 사용자의 경우 프로그램추가/삭제에서 접속프로그램이 삭제되지 않았거나 프로그램을 찾기 어려울 경우 Internet Explorer의 **[도구] >> [인터넷 옵션] >> [연결]**에서 **[전화 연결 및 가상 사설망]**의 연결아이콘을 "제거"하여 줍니다



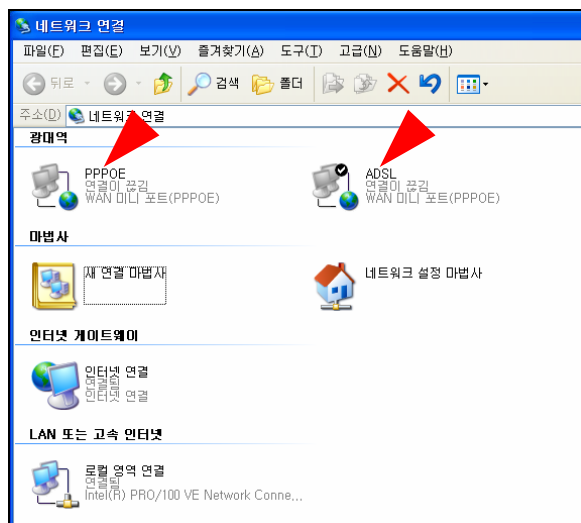
<ADSL의 연결 아이콘이 있는경우>

<전화접속 아이콘을 모두 삭제한 화면>

[참고] ADSL 사용시 Windows XP 광대역 연결 삭제 방법

바탕화면의 **[시작] - [제어판] - [네트워크 연결]**을 더블 클릭하여 나타나는 네트워크연결 창에서 광대역에 추가되어있는 아이콘을 마우스 오른쪽 클릭 "삭제"합니다.

삭제되지 않을 경우 마우스 오른쪽 클릭하여 "연결 끊기"를 클릭하신 후 "삭제"합니다.



<광대역의 PPPoE연결 아이콘 화면>

4장 인터넷 설정 마법사로 ipTIME X1005 인터넷 연결

본 4장에서는 ipTIME X1005를 인터넷에 연결하는 방법에 대해서 설명합니다. 인터넷 연결 설정은 내장된 웹 서버에 접속하여 이루어집니다. 그러므로 인터넷 연결 설정은 ipTIME X1005에 연결된 PC 중 한 곳에서 한번만 실행하면 됩니다.

ipTIME X1005에 내장된 웹 서버에 접속하기 위해서는 PC를 정상적으로 설정하여야 합니다. PC의 설정 방법에 관하여서는 본 설명서 3장과 부록 A, B의 내용을 참고합니다.

인터넷 연결 설정은 ipTIME X1005에 내장된 마법사를 이용하며, 자동 또는 수동 설정이 가능합니다. 4장에서는 이 마법사를 이용하여 인터넷 설정을 진행하는 방법을 설명합니다.

2장에서 4장까지의 내용에 따라 PC와 ipTIME X1005의 설정을 완료하면 연결된 PC에서 인터넷 사용이 가능하며 WAN1, WAN2의 인터넷 연결 상태에 따라 자동 Back-up 및 1:1의 비율에 근거한 트래픽 자동 분산이 이루어집니다.

마법사를 사용하지 않고 인터넷 연결 설정을 진행하시려면 7.1을 참고합니다.

케이블 모뎀 방식의 인터넷 서비스 환경일 경우, 본 사용 설명서 2장을 진행하신 뒤, 모뎀과 공유기의 전원을 모두 끄고, 먼저 모뎀을 켜서 약 1분 후에 링크가 잡히면, 공유기의 전원을 켜주시면 별도의 설정 없이도 인터넷 연결이 이뤄질 수 있습니다.

- 모뎀의 링크가 잡히면 CABLE, ONLINE, SYNC등의 램프는 점멸하다가 켜지게 됩니다.
- 사용 환경에 따라 바로 연결이 되지 않을 수 있으며, 본 4장의 내용을 진행합니다.

4.1 ipTIME X1005 내장 웹 서버 접속

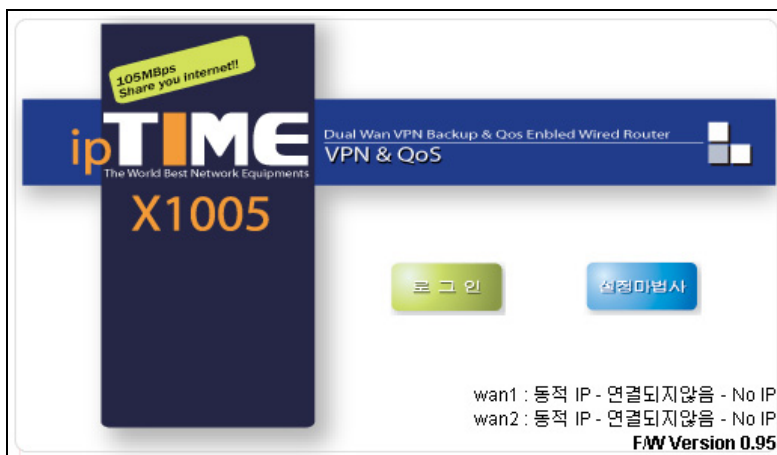
□ ipTIME X1005에 내장된 웹서버는 인터넷이 연결되어 있지 않아도 접속할 수 있습니다.

웹 서버에 접속하기 위해서는  Internet Explorer를 실행하여,
주소란에 ipTIME X1005의 주소인 192.168.0.1을 입력합니다.

주소(D)	http://192.168.0.1
-------	--------------------

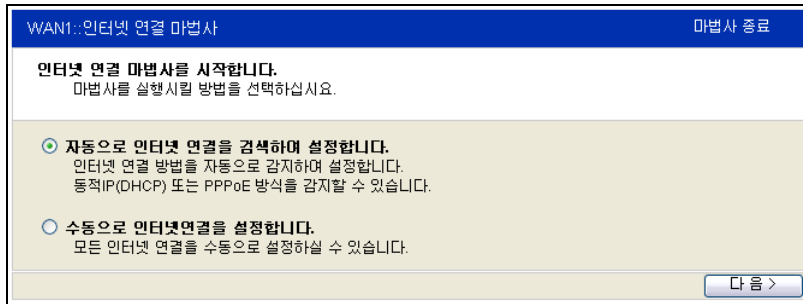
[참고] PC가 ipTIME X1005에 정상적으로 연결되었으나 인터넷이 연결되지 않은 경우 주소란에 별도 입력을 하지 않아도 자동으로 ipTIME X1005의 웹 서버로 연결됩니다. 이 기능은 특정 환경에서 동작하지 않을 수도 있습니다.

□ ipTIME X1005에 접속하면 다음과 같은 로그인 화면이 표시됩니다.



4.2 ipTIME X1005 인터넷 설정 마법사 실행

- ipTIME X1005에서 설정 마법사 버튼을 클릭하여 마법사를 시작합니다.



- 인터넷 회선을 확실히 알고 있는 경우 수동을 선택하며 인터넷 회선의 종류가 불확실한 경우 자동으로 선택하고 **다음** 버튼을 클릭합니다.
- 고정 IP 주소 서비스 사용자의 경우 자동 검색을 통하여 인터넷 설정을 할 수 없으므로 수동으로 인터넷 연결을 설정한 후 사용하여야 합니다.
- 마법사를 실행하면 먼저 WAN1에 대한 인터넷 설정을 진행하며 WAN1에 대한 인터넷 설정이 완료된 뒤 WAN2에 대한 인터넷 설정이 진행됩니다.
- WAN2을 별도로 연결하지 않는 경우에는 WAN1 설정을 완료한 후 **마침** 버튼을 클릭하여 인터넷 설정 마법사를 종료하면 됩니다.

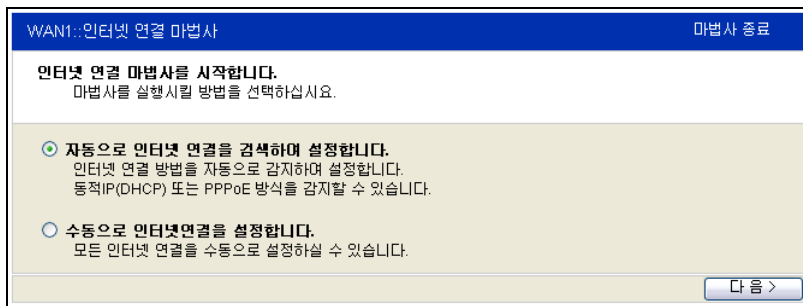
인터넷 회선 선택 기준

유 형	내 용
동적 IP 주소	VDSL 서비스 LAN 방식(100Mbps급 광랜) 서비스 ADSL이나 접속프로그램을 사용하지 않는 서비스 (IP-ADSL) 케이블 모뎀 서비스
PPPoE 방식	ADSL이며 접속시 사용자 이름과 암호를 입력하는 서비스 Aceman pro, WINPoET 등의 접속 프로그램 사용 XP의 경우 내장 광대역 접속 사용
고정 IP 주소	인터넷 서비스사로부터 지정된 IP 주소 할당 사용

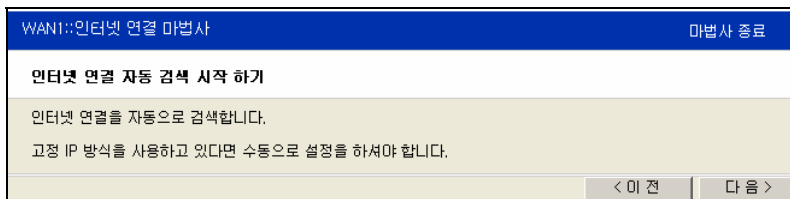
4.3 자동 검색에 의한 PPPoE 연결 예

WAN1 또는 WAN2가 Aceman Pro, WinPOET, XP 광대역 접속 프로그램등을 사용하는 PPPoE 서비스 방식의 ADSL이 연결된 경우 아래 순서로 인터넷 설정이 자동 진행됩니다.

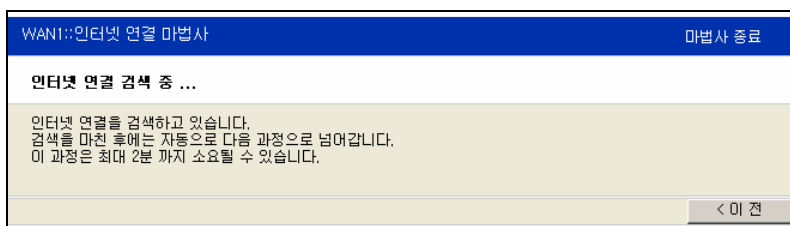
[1] 자동 검색을 선택한 후 **[다음]** 버튼을 클릭합니다.



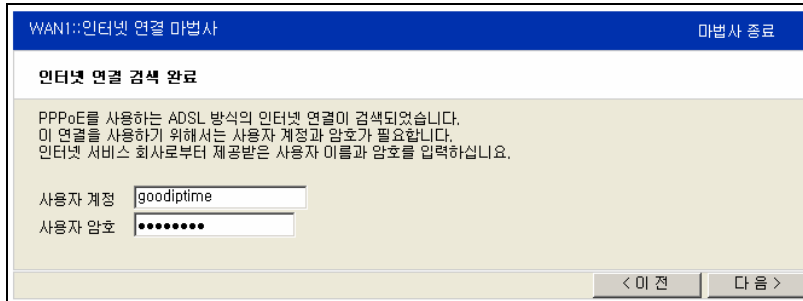
[2] **[다음]** 버튼을 클릭하여 자동 검색을 시작합니다.



[3] 인터넷 검색 중 화면이 나오는 동안 기다립니다.



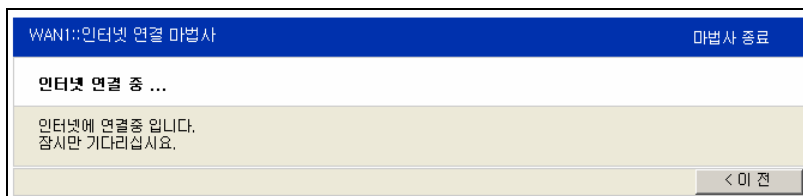
[4] PPPoE로 검색된 경우 사용자 계정과 암호를 입력하고 **[다음]** 버튼을 클릭합니다.



참고

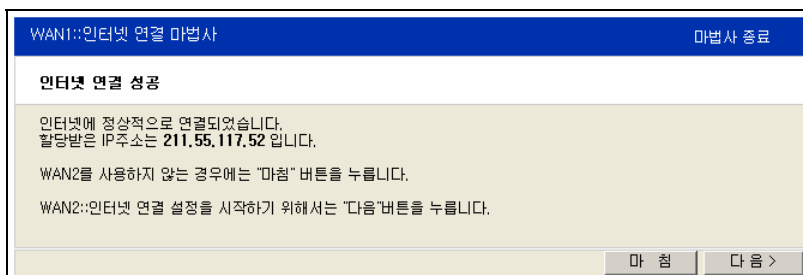
- 잘못된 암호/계정이라는 메시지가 나오는 경우 서비스 회사에 사용자 계정과 암호를 확인하여 다시 입력합니다.
- 정확한 암호/계정을 입력하여도 잘못된 암호/계정이라는 메시지가 나오면 1.3 장을 참고하여 ipTIME X1005를 공장 초기화한 후 다시 진행하여 보시기 바랍니다.

[5] 입력 받은 사용자 계정과 암호로 인터넷을 연결합니다.



[6] 인터넷이 연결되면 할당 받은 IP 주소가 표시되며, **[마침]** 버튼을 클릭하여 마법사를 종료합니다.

WAN2에 대한 인터넷 설정을 바로 진행하려면 **[다음]** 버튼을 클릭하여 진행합니다.



4.4 자동 검색에 의한 동적 IP 연결 예

WAN1 또는 WAN2에 동적 IP 방식 (DHCP 방식)의 서비스인 케이블 모뎀, VDSL, LAN, IP-ADSL에 연결된 경우 아래 순서로 인터넷 설정이 자동 진행됩니다.

[1] 자동 검색을 선택한 후 **다음** 버튼을 클릭합니다.

WAN2::인터넷 연결 마법사		마법사 종료
인터넷 연결 마법사를 시작합니다. 마법사를 실행시킬 방법을 선택하십시오.		
☒ 자동으로 인터넷 연결을 검색하여 설정합니다. 인터넷 연결 방법을 자동으로 감지하여 설정합니다. 동적IP(DHCP) 또는 PPPoE 방식을 감지할 수 있습니다.		
☐ 수동으로 인터넷 연결을 설정합니다. 모든 인터넷 연결을 수동으로 설정하실 수 있습니다.		
		다음 >

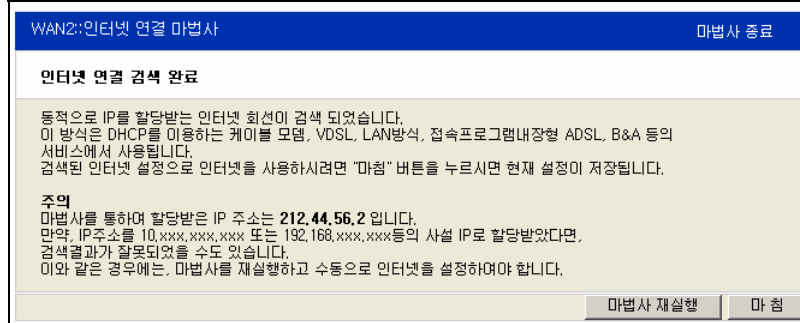
[2] **다음** 버튼을 클릭하여 자동 검색을 시작합니다.

WAN2::인터넷 연결 마법사		마법사 종료
인터넷 연결 자동 검색 시작 하기		
인터넷 연결을 자동으로 검색합니다. 고정 IP 방식을 사용하고 있다면 수동으로 설정을 하셔야 합니다.		
		< 이 전 다음 >

[3] 인터넷 검색 중 화면이 나오는 동안 기다립니다.

WAN2::인터넷 연결 마법사		마법사 종료
인터넷 연결 검색 중 ...		
인터넷 연결을 검색하고 있습니다. 검색을 마친 후에는 자동으로 다음 과정으로 넘어갑니다. 이 과정은 최대 2분 까지 소요될 수 있습니다.		
		< 이 전

[4] 동적 IP 방식으로 인터넷이 검색되면 아래 그림과 같이 설정이 종료되며, **[마침]** 버튼을 클릭하여 마법사를 종료합니다.



[참고]

- 동적 IP 방식을 자동으로 검색하는 경우 자동 검색을 실행한 PC의 하드웨어 주소(MAC Address)가 해당 WAN 포트에 자동 복사됩니다.
- PC의 하드웨어 주소(MAC Address)란 PC에 설치되어 있는 LAN 카드의 고유 번호이며, 동적 IP 방식 서비스의 경우 일부 인터넷 서비스 회사에서 하드웨어 주소를 확인하여 한대의 PC만 인터넷을 사용할 수 있도록 하고 있습니다. 이와 같은 경우 PC의 하드웨어 주소를 IP 공유기로 복사하면 하드웨어 주소 검사에 따른 제약 없이 IP 공유기를 사용할 수 있습니다.
- WAN 포트에 모뎀이나 랜방식의 회선이 아닌 IP공유기의 UTP-케이블을 연결하신 경우 검색 실패로 나옵니다.

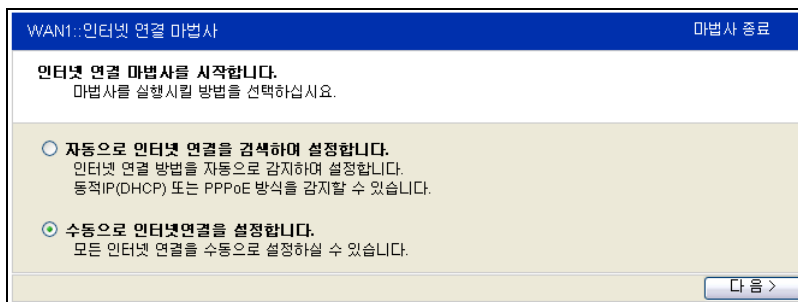
이러한 경우에는 7장의 **7.1.1 동적 IP 방식 설정**의 그림과 같이 "사설 IP 할당 허용하기"를 반드시 체크하시고 맨 하단의 적용을 눌러주시면 IP공유기의 연결도 사용할 수 있습니다.

4.5 수동 설정을 이용한 고정 IP 연결

WAN1 또는 WAN2가 인터넷 서비스 회사로부터 이미 할당 받은 고정 IP 주소를 사용하는 MyIP, Multi IP 등과 같은 서비스 방식에 접속하는 경우 아래와 같은 순서로 해당 WAN 포트의 인터넷 설정을 수동 진행합니다.

고정 IP 방식의 서비스는 자동 검색에 의한 인터넷 설정이 불가능하며 수동 설정을 통해서만 인터넷을 연결할 수 있습니다.

[1] 수동 설정을 선택한 후 **다음** 버튼을 클릭합니다.



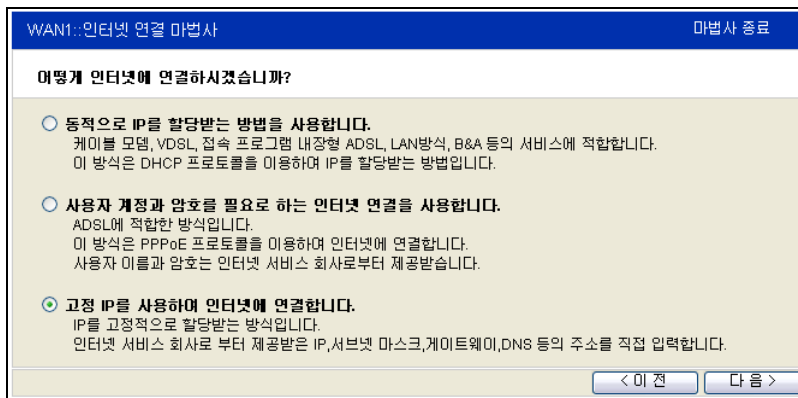
WAN1: 인터넷 연결 마법사 마법사 종료

인터넷 연결 마법사를 시작합니다.
마법사를 실행시킬 방법을 선택하십시오.

- ☐ 자동으로 인터넷 연결을 검색하여 설정합니다.
인터넷 연결 방법을 자동으로 감지하여 설정합니다.
동적IP(DHCP) 또는 PPPoE 방식을 감지할 수 있습니다.
- ☒ 수동으로 인터넷 연결을 설정합니다.
모든 인터넷 연결을 수동으로 설정하실 수 있습니다.

다음 >

[2] 고정 IP 방식을 선택한 후 **다음** 버튼을 클릭합니다.



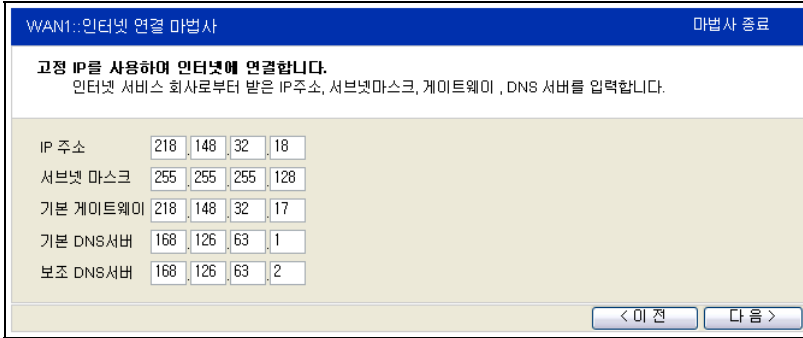
WAN1: 인터넷 연결 마법사 마법사 종료

어떻게 인터넷에 연결하시겠습니까?

- ☐ 동적으로 IP를 할당받는 방법을 사용합니다.
케이블 모뎀, VDSL, 접속 프로그램 내장형 ADSL, LAN방식, B&A 등의 서비스에 적합합니다.
이 방식은 DHCP 프로토콜을 이용하여 IP를 할당받는 방법입니다.
- ☐ 사용자 계정과 암호를 필요로 하는 인터넷 연결을 사용합니다.
ADSL에 적합한 방식입니다.
이 방식은 PPPoE 프로토콜을 이용하여 인터넷에 연결합니다.
사용자 이름과 암호는 인터넷 서비스 회사로부터 제공받습니다.
- ☒ 고정 IP를 사용하여 인터넷에 연결합니다.
IP를 고정적으로 할당받는 방식입니다.
인터넷 서비스 회사로부터 제공받은 IP, 서브넷 마스크, 게이트웨이, DNS 등의 주소를 직접 입력합니다.

< 이 전 **다음 >**

[3] 인터넷 서비스 회사에서 부여 받은 IP 주소와 게이트웨이, DNS 주소를 입력한 뒤 **다음** 버튼을 클릭합니다.

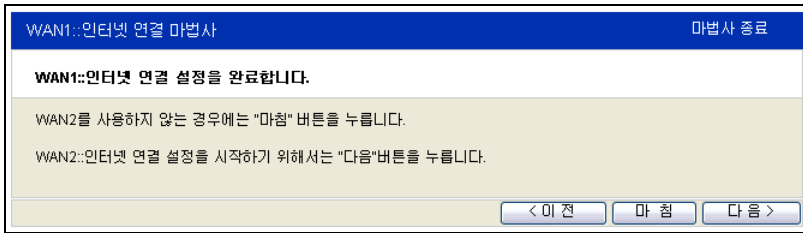


WAN1::인터넷 연결 마법사 마법사 종료

고정 IP를 사용하여 인터넷에 연결합니다.
인터넷 서비스 회사로부터 받은 IP주소, 서브넷마스크, 게이트웨이, DNS 서버를 입력합니다.

IP 주소	218	148	32	18
서브넷 마스크	255	255	255	128
기본 게이트웨이	218	148	32	17
기본 DNS서버	168	126	63	1
보조 DNS서버	168	126	63	2

[4] 설정이 완료되면 **마침** 버튼을 클릭하여 해당 WAN1에 대한 인터넷 설정을 종료합니다. WAN2에 대한 인터넷 설정을 바로 진행하려면 **다음** 버튼을 클릭하여 진행합니다.



WAN1::인터넷 연결 마법사 마법사 종료

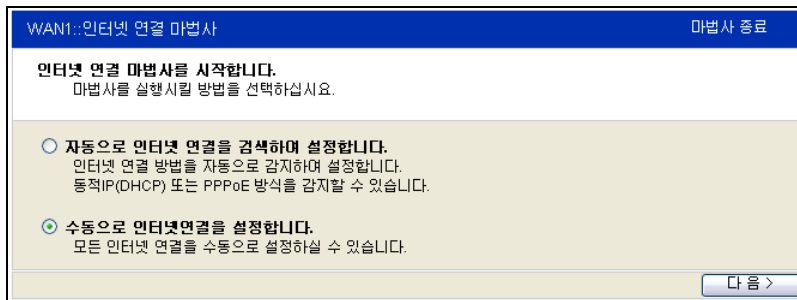
WAN1::인터넷 연결 설정을 완료합니다.

WAN2를 사용하지 않는 경우에는 "마침" 버튼을 누릅니다.
WAN2::인터넷 연결 설정을 시작하기 위해서는 "다음" 버튼을 누릅니다.

4.6 수동 설정을 이용한 동적 IP 연결

WAN1 또는 WAN2에 동적 IP 방식 (DHCP 방식)의 서비스인 케이블 모뎀, VDSL, LAN, IP-ADSL에 연결된 경우 아래와 같은 순서로 해당 WAN 포트의 수동 인터넷 설정을 진행합니다.

[1] 수동 설정을 선택한 후 **다음** 버튼을 클릭합니다.



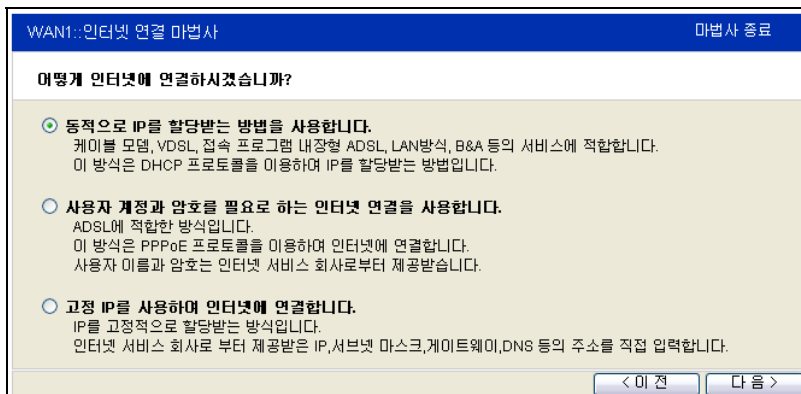
WAN1: 인터넷 연결 마법사 마법사 종료

인터넷 연결 마법사를 시작합니다.
마법사를 실행시킬 방법을 선택하십시오.

- ☐ 자동으로 인터넷 연결을 검색하여 설정합니다.
인터넷 연결 방법을 자동으로 감지하여 설정합니다.
동적IP(DHCP) 또는 PPPoE 방식을 감지할 수 있습니다.
- ☒ 수동으로 인터넷 연결을 설정합니다.
모든 인터넷 연결을 수동으로 설정하실 수 있습니다.

다음 >

[2] 동적 IP 방식을 선택한 후 **다음** 버튼을 클릭합니다.



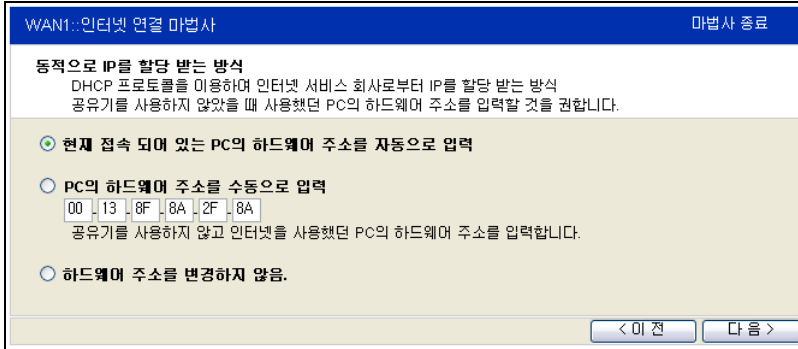
WAN1: 인터넷 연결 마법사 마법사 종료

어떻게 인터넷에 연결하시겠습니까?

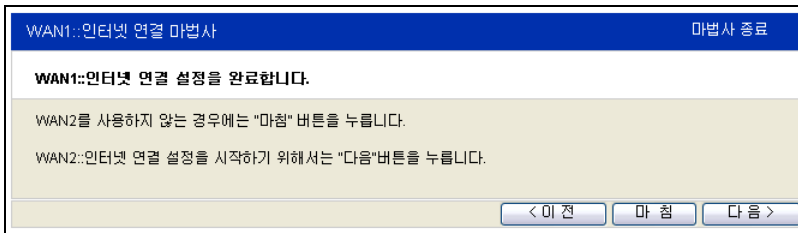
- ☒ 동적으로 IP를 할당받는 방법을 사용합니다.
케이블 모뎀, VDSL, 접속 프로그램 내장형 ADSL, LAN방식, B&A 등의 서비스에 적합합니다.
이 방식은 DHCP 프로토콜을 이용하여 IP를 할당받는 방법입니다.
- ☐ 사용자 계정과 암호를 필요로 하는 인터넷 연결을 사용합니다.
ADSL에 적합한 방식입니다.
이 방식은 PPPoE 프로토콜을 이용하여 인터넷에 연결합니다.
사용자 이름과 암호는 인터넷 서비스 회사로부터 제공됩니다.
- ☐ 고정 IP를 사용하여 인터넷에 연결합니다.
IP를 고정적으로 할당받는 방식입니다.
인터넷 서비스 회사로부터 제공받은 IP, 서브넷 마스크, 게이트웨이, DNS 등의 주소를 직접 입력합니다.

< 이전 **다음 >**

[3] 인터넷 서비스 회사에 따라 등록된 하드웨어 장비만 연결이 가능한 경우가 있으므로 이 경우 해당 서비스 방식에서 인터넷 사용이 가능한 PC 또는 장비의 하드웨어 주소를 입력한 뒤 **다음** 버튼을 클릭합니다.



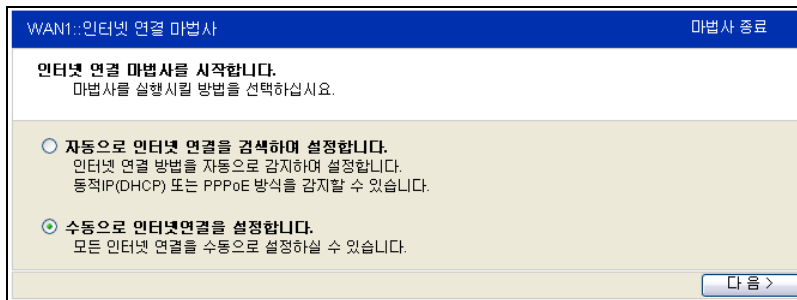
[4] 설정이 완료되면 **마침** 버튼을 클릭하여 해당 WAN1에 대한 인터넷 설정을 종료합니다. WAN2에 대한 인터넷 설정을 바로 진행하려면 **다음** 버튼을 클릭하여 진행합니다.



4.7 수동 설정을 이용한 PPPoE 연결

WAN1 또는 WAN2에 Aceman Pro, WinPOET, XP 광대역 접속 프로그램등을 사용하는 PPPoE 서비스 방식의 ADSL이 연결된 경우 아래와 같은 순서로 해당 WAN 포트의 인터넷 설정을 수동 진행합니다.

[1] 수동 설정을 선택한 후 **다음** 버튼을 클릭합니다.



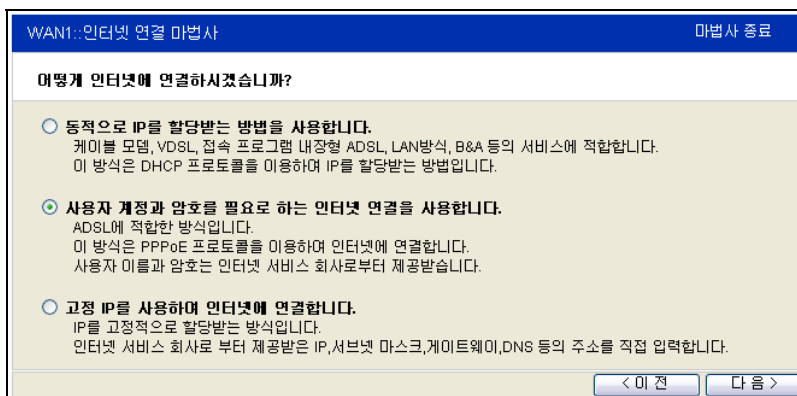
WAN1: 인터넷 연결 마법사 마법사 종료

인터넷 연결 마법사를 시작합니다.
마법사를 실행시킬 방법을 선택하십시오.

- ☐ 자동으로 인터넷 연결을 검색하여 설정합니다.
인터넷 연결 방법을 자동으로 감지하여 설정합니다.
동적IP(DHCP) 또는 PPPoE 방식을 감지할 수 있습니다.
- ☒ 수동으로 인터넷연결을 설정합니다.
모든 인터넷 연결을 수동으로 설정하실 수 있습니다.

다음 >

[2] 사용자 계정과 암호를 필요로 하는 PPPoE 방식을 선택한 후 **다음** 버튼을 클릭합니다.



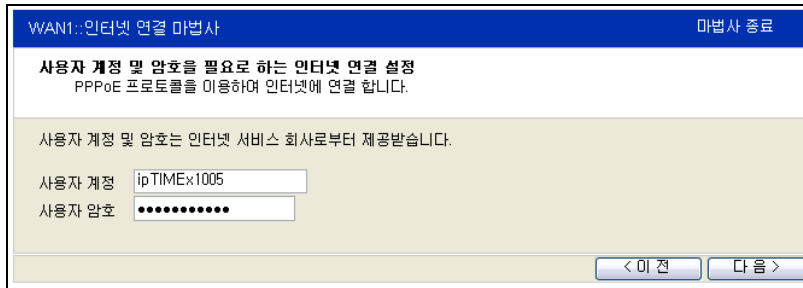
WAN1: 인터넷 연결 마법사 마법사 종료

어떻게 인터넷에 연결하시겠습니까?

- ☐ 동적으로 IP를 할당받는 방법을 사용합니다.
케이블 모뎀, VDSL, 접속 프로그램 내장형 ADSL, LAN방식, B&A 등의 서비스에 적합합니다.
이 방식은 DHCP 프로토콜을 이용하여 IP를 할당받는 방법입니다.
- ☒ 사용자 계정과 암호를 필요로 하는 인터넷 연결을 사용합니다.
ADSL에 적합한 방식입니다.
이 방식은 PPPoE 프로토콜을 이용하여 인터넷에 연결합니다.
사용자 이름과 암호는 인터넷 서비스 회사로부터 제공받습니다.
- ☐ 고정 IP를 사용하여 인터넷에 연결합니다.
IP를 고정적으로 할당받는 방식입니다.
인터넷 서비스 회사로부터 제공받은 IP, 서브넷 마스크, 게이트웨이, DNS 등의 주소를 직접 입력합니다.

< 이전 **다음 >**

[3] 서비스 접속에 사용하는 사용자 계정과 암호를 입력한 후 **다음** 버튼을 클릭합니다.



WAN1: 인터넷 연결 마법사 마법사 종료

사용자 계정 및 암호를 필요로 하는 인터넷 연결 설정
PPPoE 프로토콜을 이용하여 인터넷에 연결 합니다.

사용자 계정 및 암호는 인터넷 서비스 회사로부터 제공받습니다.

사용자 계정

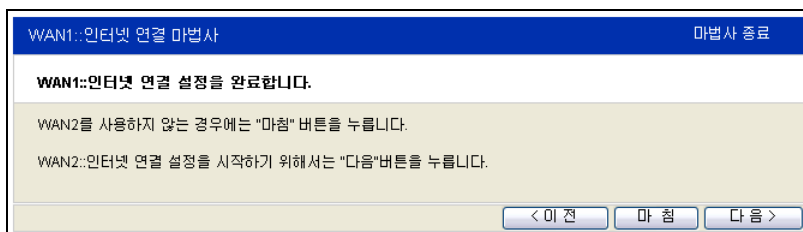
사용자 암호

< 이 전 다음 >

참고

- 잘못된 암호/계정이라는 메시지가 나오는 경우 서비스 회사에 사용자 계정과 암호를 확인하여 다시 입력합니다.
- 정확한 암호/계정을 입력하여도 잘못된 암호/계정이라는 메시지가 나오면 1.3 장을 참고하여 ipTIME X1005를 공장 초기화한 후 다시 진행하여 보시기 바랍니다.

[4] 설정이 완료되면 **마침** 버튼을 클릭하여 해당 WAN1에 대한 인터넷 설정을 종료합니다. WAN2에 대한 인터넷 설정을 바로 진행하려면 **다음** 버튼을 클릭하여 진행합니다.



WAN1: 인터넷 연결 마법사 마법사 종료

WAN1: 인터넷 연결 설정을 완료합니다.

WAN2를 사용하지 않는 경우에는 "마침" 버튼을 누릅니다.

WAN2: 인터넷 연결 설정을 시작하기 위해서는 "다음" 버튼을 누릅니다.

< 이 전 마 침 다음 >

고급 기능 편

- 5장 ~ 12장은 ipTIME X1005의 모든 기능을 설명하고 있는 고급 기능 설명서입니다.
- ipTIME X1005의 모든 기능을 원활하게 사용하기 위해서는 5장 ~ 12장의 내용을 숙지하여야 합니다.

5장 웹 설정 화면 이용하기

5.1 ipTIME X1005 내장 웹 서버 접속

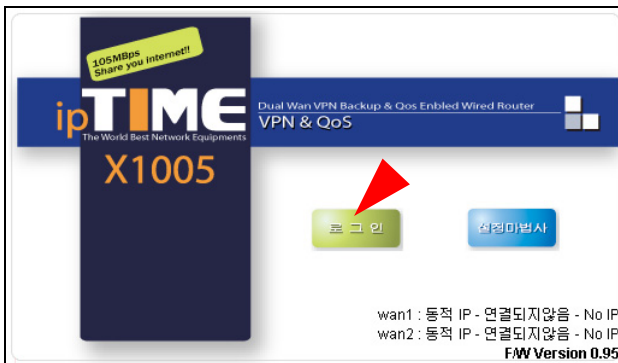
ipTIME X1005는 웹 서버에 접속하여 관련된 설정을 변경하거나 ipTIME X1005의 동작 상태를 확인할 수 있습니다. ipTIME X1005의 웹 설정 화면은 내부에 내장된 웹 서버를 이용하는 것이므로 인터넷이 연결되어 있지 않아도 접속할 수 있습니다.

웹 설정 화면에 접속하기 위해서는  Internet Explorer를 실행하여, 주소란에 ipTIME X1005의 주소인 192.168.0.1을 입력합니다.

주소(D)	http://192.168.0.1
-------	--------------------

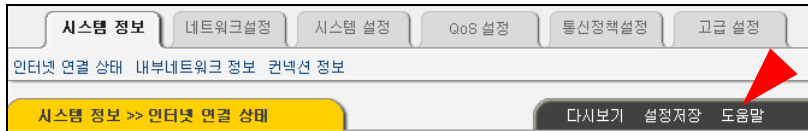
[참고] PC가 ipTIME X1005에는 연결되었으나 인터넷이 연결되지 않은 경우 주소란에 별도 입력을 하지 않아도 자동으로 ipTIME X1005의 웹 서버로 연결됩니다. 이 기능은 특정 환경에서 동작하지 않을 수 있습니다.

ipTIME X1005에 접속되면 아래 그림과 같은 화면이 표시되며 이때 **로그인** 버튼을 클릭하면 ipTIME X1005 웹 설정 화면으로 접속됩니다.



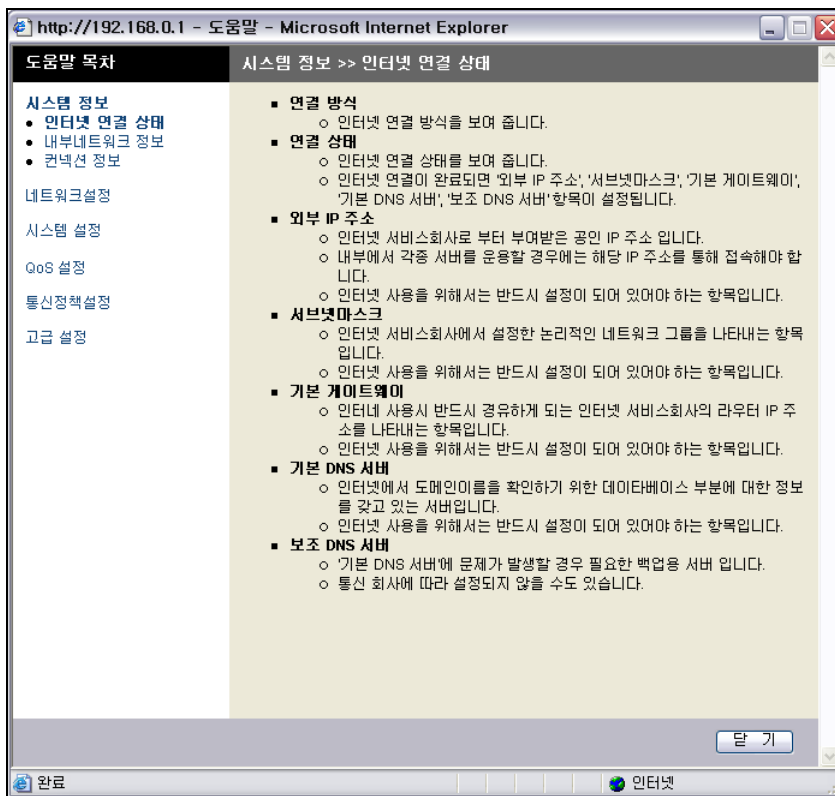
5.2 도움말 기능

ipTIME X1005은 모든 기능에 대한 도움말을 내장하고 있습니다. ipTIME X1005을 웹 설정 화면의 우측 상단의 도움말을 클릭하면 해당 웹 설정 화면에 대한 자세한 도움말을 볼 수 있습니다.



<웹 설정 화면 우측 상단의 도움말 메뉴>

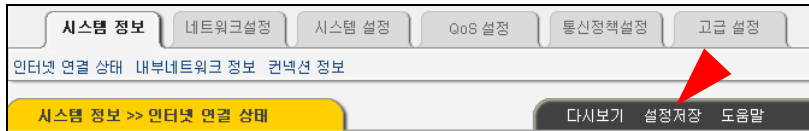
도움말 화면 좌측에는 전체 도움말의 목차가 링크되어 있으므로 필요한 경우 목차를 클릭하면 현재 화면 이외의 다른 기능에 대한 도움말도 확인할 수 있습니다.



<ipTIME X1005의 도움말 화면>

5.3 설정저장 기능

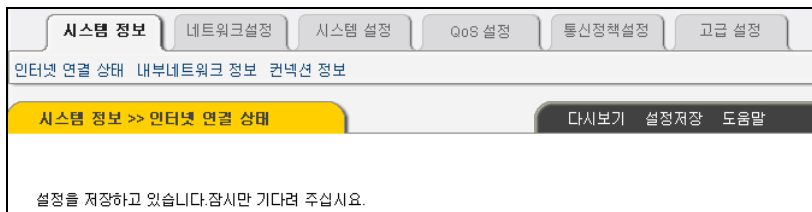
ipTIME X1005의 웹 설정 화면에서 변경된 설정 내용은 설정저장을 하여야 영구적으로 저장됩니다. 설정저장을 하지 않으면 변경된 설정 내용은 공유기의 전원을 OFF하면 모두 지워집니다. 설정저장을 위해서는 웹 설정 화면 우측 상단의 설정저장 메뉴를 클릭합니다.



<웹 설정 화면 우측 상단의 설정저장 메뉴>

설정저장 메뉴를 클릭하면 확인 창이 표시됩니다.

이때 확인을 클릭하면 아래 그림과 같이 설정저장 중임을 알리는 화면이 표시된 뒤 모든 설정 내용이 공유기 내부의 비휘발성 메모리에 기록됩니다.



<설정저장을 알리는 화면 메시지 내용>

6장 시스템 정보

6.1 인터넷 연결 상태

ipTIME X1005 설정 화면의 **시스템 정보** 메뉴를 클릭한 뒤 **인터넷 연결 상태** 메뉴를 클릭하면 ipTIME X1005의 WAN1과 WAN2의 인터넷 연결 상태를 확인할 수 있습니다. 이 화면은 인터넷 회선 상태를 반영하기 위하여 연결이 되지 않은 경우 5초마다 갱신되며 WAN1/WAN2가 전부 연결된 경우 30초마다 한번씩 자동 갱신됩니다.

공유기의 DNS 서버 정보 항목은 공유기 시스템에서 사용중인 DNS 서버 정보를 표시합니다.



시스템 정보 >> 인터넷 연결 상태

다시보기 설정저장 도움말

WAN1		WAN2	
연결 방식	PPPoE 연결	연결 방식	동적 IP 연결
연결 상태	인터넷에 정상적으로 연결됨 인터넷 라인백업 동작중	연결 상태	인터넷에 정상적으로 연결됨 인터넷 라인백업 동작중
하드웨어 주소	00-13-8F-8A-2F-8A	하드웨어 주소	00-08-9F-58-87-1A
외부 IP 주소	220 . 120 . 139 . 117	외부 IP 주소	203 . 142 . 178 . 246
서브넷 마스크	255 . 255 . 255 . 255	서브넷 마스크	255 . 255 . 255 . 0
기본 게이트웨이	220 . 120 . 139 . 117	기본 게이트웨이	203 . 142 . 178 . 1
기본 DNS 서버	168 . 126 . 63 . 1	기본 DNS 서버	168 . 126 . 63 . 1
보조 DNS 서버	168 . 126 . 63 . 2	보조 DNS 서버	
전속 해제		연결 해제	

공유기 DNS 서버 정보

DNS 서버 설정 방법	자동으로 공유기의 DNS 서버 설정
DNS 서버	168 . 126 . 63 . 1 , 168 . 126 . 63 . 2

<인터넷 연결 상태 화면>

6.2 내부 네트워크 정보

ipTIME X1005 설정 화면의 **시스템 정보** 메뉴를 클릭한 뒤 **내부네트워크 정보** 메뉴를 클릭하면 ipTIME X1005 내부 LAN 에 관련된 정보가 표시됩니다.

ipTIME X1005에 연결된 PC에서 IP를 할당 받은 후 통신이 이뤄지면,
할당된 IP 주소 정보 항목에서 연결된 PC의 정보를 확인할 수 있습니다.



시스템 정보 **네트워크 정보** 시스템 설정 QoS 설정 통신정책설정 고급 설정

인터넷 연결 상태 내부네트워크 정보 컨넥션 정보

시스템 정보 >> 내부네트워크 정보 다시보기 설정저장 도움말

내부 네트워크 정보

하드웨어 주소	00-08-9F-56-87-1A
내부 IP 주소	192 . 168 . 0 . 1
서브넷 마스크	255 . 255 . 255 . 0
동적 IP 할당 범위	192 . 168 . 0 . 2 - 192 . 168 . 0 . 254
동적 IP 할당 수	1

할당된 IP 주소 정보

번호	IP 주소	하드웨어 주소	비고
1	192.168.0.2 (jsh)	00:13:8F:8A:2F:8A	자동할당

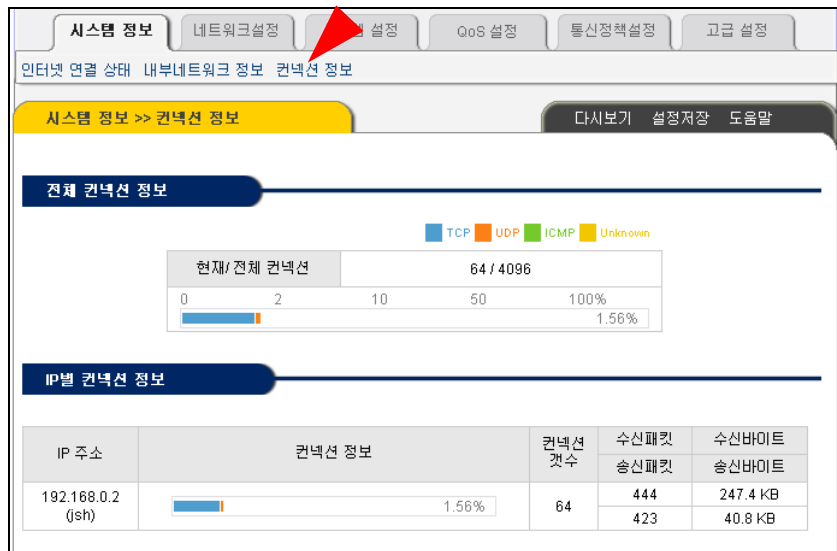
<내부 네트워크 정보 화면>

내부네트워크 정보 화면에서 표시되는 내용은 다음과 같습니다.

구분	이름	내용
내부 네트워크 정보	하드웨어 주소	ipTIME X1005의 LAN 하드웨어 주소
	내부 IP 주소	ipTIME X1005의 LAN IP 주소, 기본값 192.168.0.1
	서브넷 마스크	LAN의 서브넷 마스크, 기본값 255.255.255.0
	동적 IP 할당 범위	ipTIME X1005가 자동으로 할당할 IP 주소 범위
	동적 IP 할당 수	현재 ipTIME X1005가 자동으로 할당한 IP 주소 개수
할당된 IP 주소 정보	번호	ipTIME X1005에 연결되어 통신중인 PC의 일련 번호
	IP 주소	ipTIME X1005에 연결되어 통신중인 PC의 IP 주소
	하드웨어 주소	ipTIME X1005에 연결되어 통신중인 PC의 하드웨어 주소
	비고	자동 할당 : ipTIME X1005 자동으로 IP 주소를 부여함 수동 설정 : 사용자가 PC IP 주소를 수동 입력함

6.3 컨넥션 정보

현재 공유기에 연결되어 인터넷을 사용하는 PC가 외부와 접속하게 되면 컨넥션을 생성하게 됩니다. 공유기가 지원할 수 있는 전체 컨넥션에 각 PC의 컨넥션이 백분율로 나타납니다.



<컨넥션 정보 화면>

전체 컨넥션 정보

현재 통신하고 있는 모든 컨넥션의 개수를 알 수 있습니다.

전체 컨넥션의 수는 공유기가 가질 수 있는 최대 컨넥션 수를 나타냅니다.

현재 컨넥션 수가 전체 컨넥션 수와 같아지면 더 이상의 인터넷 연결을 할 수 없습니다.

IP 별 컨넥션 정보

IP 주소란은 연결을 시작한 IP를 나타냅니다.

이정보를 이용하여 과도한 컨넥션을 생성하는 PC를 찾아낼 수 있습니다.

구 분	내 용
TCP	보통 인터넷(http)에서 많이 사용하며 일부P2P에서 접속, 리스트 등에 사용하기도 합니다.
UDP	P2P에서 데이터를 전송하거나 온라인 게임등에서 많이 사용하는 프로토콜입니다.
ICMP	대표적으로 ping 명령어를 실행하였을 때 사용되는 프로토콜 입니다.
Unknown	3가지 프로토콜 이외의 다른 접속을 의미합니다.

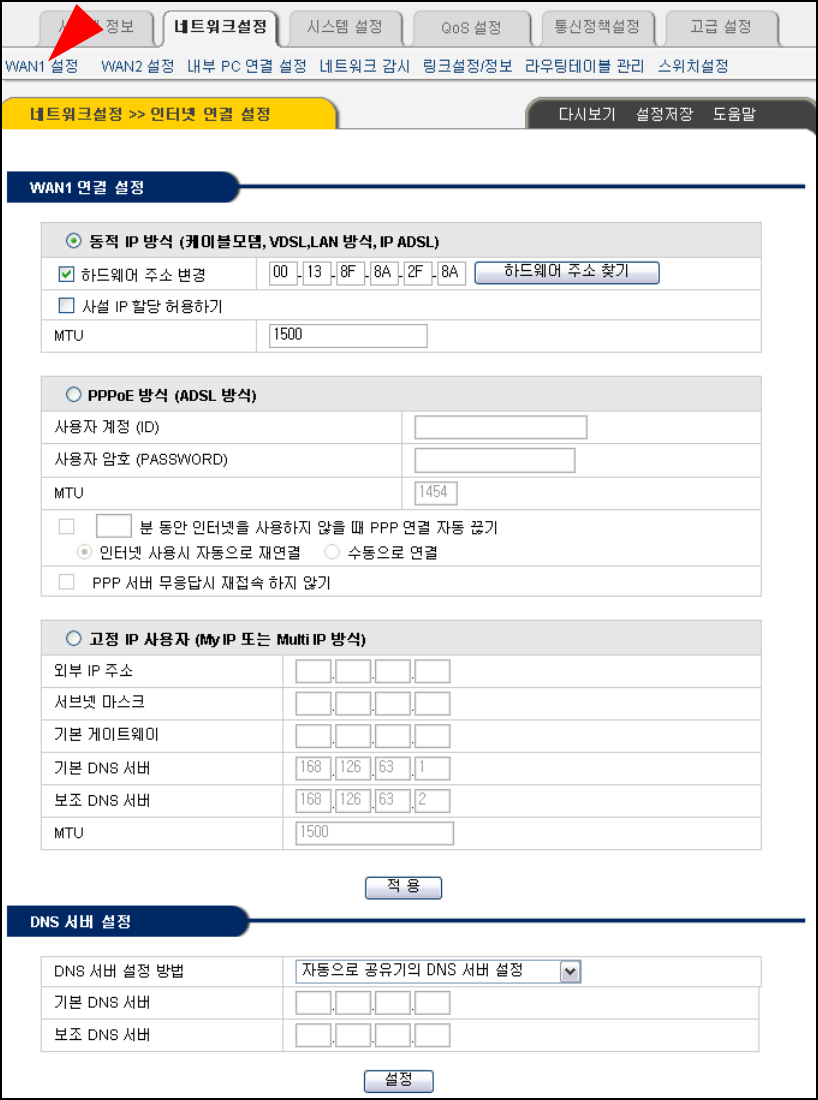
공유기를 통해 외부와 연결하기 위해 공유기에 남겨진 각 프로토콜별 접속량을 나타냅니다.

프로토콜의 자세한 내용은 포털 사이트에서 검색하여 보시면 자세하게 확인할 수 있습니다.

7장 네트워크 설정

7.1 WAN1/WAN2 연결 설정

웹 설정 화면의 **네트워크설정** 메뉴를 클릭한 뒤 **WAN1 설정** 또는 **WAN2 설정** 메뉴를 클릭하면 WAN1 또는 WAN2의 인터넷 연결 방식을 수동으로 설정할 수 있습니다.



네트워크설정 >> 인터넷 연결 설정

WAN1 연결 설정

동적 IP 방식 (케이블모뎀, VDSL, LAN 방식, IP ADSL)

☒ 하드웨어 주소 변경 00 13 8F 8A 2F 8A [하드웨어 주소 찾기](#)

☐ 사설 IP 할당 허용하기

MTU 1500

PPPoE 방식 (ADSL 방식)

사용자 계정 (ID)

사용자 암호 (PASSWORD)

MTU 1454

☐ ☐ 분 동안 인터넷을 사용하지 않을 때 PPP 연결 자동 끊기

☒ 인터넷 사용시 자동으로 재연결 ☐ 수동으로 연결

☐ PPP 서버 무응답시 재접속 하지 않기

고정 IP 사용자 (My IP 또는 Multi IP 방식)

외부 IP 주소

서브넷 마스크

기본 게이트웨이

기본 DNS 서버 168 126 63 1

보조 DNS 서버 168 126 63 2

MTU 1500

[적용](#)

DNS 서버 설정

DNS 서버 설정 방법 자동으로 공유기의 DNS 서버 설정 ▼

기본 DNS 서버

보조 DNS 서버

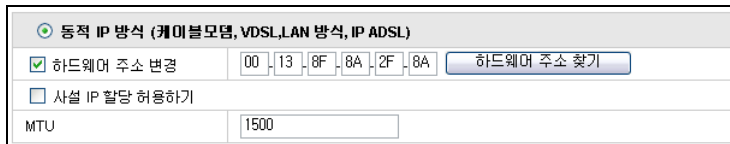
[설정](#)

<WAN 연결 설정 화면>

7.1.1 동적 IP 방식 설정

케이블 모뎀, VDSL, IP-ADSL (접속 프로그램 ADSL 모뎀 내장), 랜 방식의 인터넷 서비스에 접속하는 경우 동적 IP 방식을 선택합니다. 동적 IP 방식은 WAN 포트가 DHCP Client로 동작하며 인터넷 서비스 회사로부터 IP주소를 요청하여 할당 받는 방식입니다.

일부 동적 IP 서비스 지역에서는 하드웨어 주소에 근거하여 서비스를 제한하는 경우가 있습니다. 이때는 모뎀 등에 연결하여 인터넷 사용이 가능한 것으로 확인되는 PC의 하드웨어 주소를 공유기에 입력해 주어야 합니다.



<동적 IP 방식 입력 화면>

동적 IP 방식 설정 항목 요약

항목	내용
하드웨어 주소 변경	하드웨어 주소 변경 에 check를 하면 현재 웹 설정 화면에 접속한 PC의 하드웨어 주소가 자동으로 복사됩니다.
하드웨어 주소 찾기	하드웨어 주소 찾기 버튼을 클릭하면 현재 공유기에 연결된 PC의 하드웨어 주소 목록이 표시되므로 선택할 수 있습니다.
사설 IP 할당 허용하기	WAN을 사설 IP주소로 구성된 네트워크에 연결하고자 하는 경우 이 항목을 check합니다. 일반적으로 check하지 않고 사용합니다.

동적 IP 방식의 WAN 설정 순서

- ① 동적 IP 방식의 **⊙** 버튼을 마우스로 클릭하여 선택합니다.
- ② 하드웨어 주소 변경이 필요한 경우 적절히 입력합니다.
- ③ 하단의 **적용** 버튼을 클릭합니다.
- ④ 인터넷 연결이 확인되면 우측 상단의 **설정저장** 메뉴로 변경 상태를 저장합니다.

(5.3절 참고)

7.1.2 PPPoE 방식 설정

Aceman Pro, WinPOET, XP 광대역 접속 프로그램 등을 사용하여 접속하는 ADSL 인터넷 서비스가 PPPoE 방식입니다.

PPPoE 방식 (ADSL 방식)	
사용자 계정 (ID)	iptimex1005
사용자 암호 (PASSWORD)	*****
MTU	1454
☐ ☐ 본 동안 인터넷을 사용하지 않을 때 PPP 연결 자동 끊기 ☒ 인터넷 사용시 자동으로 재연결 ☐ 수동으로 연결	
☐ PPP 서버 무응답시 재접속 하지 않기	

<PPPoE 방식 입력 화면>

PPPoE 방식 설정 항목 요약

항목	내용
사용자 계정	인터넷 서비스 회사에서 전달 받은 사용자 계정
사용자 암호	인터넷 서비스 회사에서 전달 받은 사용자 암호
MTU	PPPoE 통신시 전달되는 Packet의 최대 크기 일반적으로 1454의 값을 사용하며 ADSL 선로 상태가 나빠 끊김이 자주 발생하는 경우 또는 특정 사이트가 접속되지 않는 경우 1300으로 줄여서 사용함.
PPPoE 자동 끊기	인터넷을 사용하지 않는 경우 PPPoE를 자동으로 종료함 일반적으로 사용하지 않음
PPP서버 재접속 않기	서비스 회사의 PPP 서버에 응답이 없는 경우 재접속하지 않음 일반적으로 사용하지 않음

PPPoE 방식의 WAN 설정 순서

- ① PPPoE 방식의 ☒ 버튼을 마우스로 클릭하여 선택합니다.
- ② 사용자 계정과 암호를 입력합니다.
- ③ 하단의 **적용** 버튼을 클릭합니다.
- ④ 인터넷 연결이 확인되면 우측 상단의 **설정저장** 메뉴로 변경 상태를 저장합니다.
(5.3절 참고)

7.1.3 고정 IP 방식 설정

인터넷 회사에서 고정된 IP 주소를 받아서 사용하는 서비스 방식으로 KT의 MY-IP, Multi-IP 등의 서비스가 있습니다.

● 고정 IP 사용자 (My IP 또는 Multi IP 방식)				
외부 IP 주소	219	236	43	18
서브넷 마스크	255	255	255	0
기본 게이트웨이	219	236	43	17
기본 DNS 서버	168	126	63	1
보조 DNS 서버	168	126	63	2
MTU	1500			

<고정 IP 방식 입력 화면>

고정 IP 방식의 WAN 설정 순서

- ① 고정 IP 방식의 ● 버튼을 마우스로 클릭하여 선택합니다.
 - ② 서비스 회사에서 받은 IP주소, 서브넷 마스크, 게이트웨이, DNS 등을 입력합니다.
 - ③ 하단의 **적용** 버튼을 클릭합니다.
 - ④ 인터넷 연결이 확인되면 우측 상단의 **설정 저장** 메뉴로 변경 상태를 저장합니다.
- (5.3절 참고)

[참고] MTU 값은 공유기를 통해서 인터넷으로 전달되는 패킷 데이터의 최대 크기를 지정합니다. 일반적으로 1500을 사용하며 특정한 서비스 환경에서 업로드에 문제가 발생하는 경우 1300정도의 값을 입력하여 사용합니다.

7.1.4 DNS 서버 설정

공유기의 시스템에서 사용되는 DNS 서버를 사용자가 임의로 선택/설정할 수 있습니다.

설정 항목	기능 설명
자동으로 공유기의 DNS 서버 설정	WAN1 및 WAN2의 DNS서버를 자동으로 선택
WAN 1의 DNS를 공유기의 DNS로 사용	WAN1의 DNS 서버 사용
WAN 2의 DNS를 공유기의 DNS로 사용	WAN2의 DNS 서버 사용
수동으로 공유기의 DNS 서버 설정	사용자가 임의로 DNS 서버를 입력

DNS 서버 설정

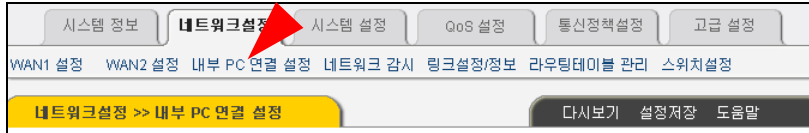
DNS 서버 설정 방법	자동으로 공유기의 DNS 서버 설정 ▼
기본 DNS 서버	
보조 DNS 서버	

설정

<DNS 서버 설정 화면>

7.2 내부 PC 연결 설정

웹 설정 화면의 **네트워크설정** 메뉴를 클릭한 뒤 **내부 PC 연결 설정** 메뉴를 클릭하면 ipTIME X1005의 내부 네트워크(LAN)에 관련된 설정을 변경할 수 있습니다.



<내부 PC 연결 설정 화면>

내부 PC 연결 설정으로는 내부 IP 주소, DHCP 서버, Twin-IP 기능 등과 같이 ipTIME X1005의 LAN 주소와 관련된 모든 설정할 수 있습니다. 각 기능에 대한 간단한 설명은 아래의 표를 참고합니다.

기능	내용 설명
내부 IP 변경	ipTIME X1005의 기본 IP 주소는 192.168.0.1입니다. 이 IP 주소를 변경하고자 하는 경우 본 항목을 이용합니다. 자세한 내용은 7.2.1을 참고합니다.
DHCP 서버 상태/설정	ipTIME X1005에 연결된 PC로 IP 주소를 자동 할당하는 기능을 DHCP 서버 기능이라고 합니다. 이 항목을 이용하면 DHCP 서버에서 자동 할당하는 IP 주소의 범위와 특정 PC에 대한 특정 IP 주소 할당을 지정할 수 있습니다. 자세한 내용은 7.2.2를 참고합니다.
Twin-IP 설정	ipTIME X1005의 경우 WAN1과 WAN2에 할당된 공인 IP 주소를 지정한 PC에 직접 할당하는 Twin IP 기능을 제공합니다. 이 기능으로 공인 IP 주소가 할당된 PC는 공유기로 인하여 발생할 수도 있는 제약이 없는 상태로 인터넷을 사용할 수 있습니다. 자세한 내용은 7.2.3을 참고합니다.
인터넷 사용 PC 제한	설정된 PC의 갯수 만큼 인터넷 사용이 가능합니다. 자세한 내용은 7.2.4를 참고합니다.

<내부 PC 연결 설정 항목>

7.2.1 내부 IP 주소 변경

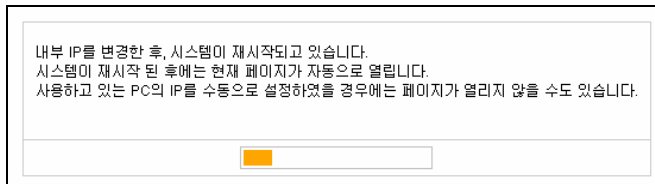
내부 IP 주소 변경 항목에서 변경하고자 하는 새로운 IP 주소를 입력한 뒤 **변경** 버튼을 클릭합니다.



내부 IP 주소	192	168	0	1
서브넷 마스크	255	255	255	0
변경				

<내부 IP 변경 항목>

변경 버튼을 클릭하면 공유기의 IP 주소가 변경되며 아래 화면과 같이 변경 IP 주소 적용을 위한 공유기 재시작 화면이 표시된 후 내부 IP 주소가 변경됩니다.



내부 IP를 변경한 후, 시스템이 재시작되고 있습니다.
 시스템이 재시작 된 후에는 현재 페이지가 자동으로 열립니다.
 사용하고 있는 PC의 IP를 수동으로 설정하였을 경우에는 페이지가 열리지 않을 수도 있습니다.

[참고] 내부 IP 주소 변경은 별도 설정저장 없이도 자동으로 저장됩니다.

7.2.2 DHCP 서버 상태/설정

DHCP 서버 상태/설정

DHCP 서버 상태	DHCP 서버 동작중
DHCP 서버 설정	실행 ▼
동적 IP주소 범위	192.168.0.2 - 192.168.0.254
☐ 수동 DNS 설정	168.126.63.1, 168.126.63.2
☒ 내부네트워크에서 DHCP서버 발견시 공유기의 DHCP 서버기능을 중단 합니다. ☐ DHCP서버에서 IP를 할당받은 PC만 인터넷 접속을 허용합니다.	
적용	

IP 할당 수동 지정

☒ 현재 네트워크에 있는 주소에서 추가하기
☐ 수동으로 추가하기

할당할 IP 주소	지정할 하드웨어 주소
☐ 192.168.0.2	00-13-8F-8A-2F-8A

추가

할당할 IP 주소	지정할 하드웨어 주소	삭제
192.168.0.45	00-a0-0c-c8-68-09	삭제
192.168.0.44	00-01-80-53-c9-b2	삭제

[1]

<DHCP 서버 상태 설정 화면>

DHCP 서버 끄고 켜기

DHCP 서버 설정에서 실행 또는 중지를 선택한 후 적용 버튼을 클릭하여 ipTIME X1005의 DHCP 서버를 켜거나 끌 수 있습니다. DHCP 서버를 끄면 ipTIME X1005에서 PC로 IP주소를 할당하지 않습니다. 정상적인 IP 주소 할당을 위해서는 DHCP 서버를 실행하여야 하며 DHCP 서버를 중단 시킨 경우라면 ipTIME X1005에 연결하는 PC의 IP 주소는 수동으로 설정하여 사용하여야 합니다.

IP 주소 수동 설정 방법은 본사 홈페이지(<http://www.iptime.co.kr>)에서 고객지원 >> 네트워크 >> 자주묻는질문 게시판에서 확인하시기 바랍니다.

내부네트워크에서 DHCP 서버 발견시 공유기의 DHCP 서버기능을 중단합니다.

공유기 내부 네트워크에 다른 DHCP 서버가 발견되면 공유기는 DHCP 기능을 중단하게 되며, DHCP가 다시 발견되지 않으면 공유기는 자동으로 DHCP 기능을 실행하게 됩니다.

DHCP 서버에서 IP를 할당받은 PC만 인터넷 접속을 허용합니다.

공유기에 연결된 PC 랜카드의 TCP/IP 설정이 자동으로 IP 주소 받기로 설정되어 있는 PC만 인터넷 접속을 허용하는 기능입니다. TCP/IP 설정이 수동으로 구성되어 있는 경우 인터넷 접속이 차단됩니다.

IP 할당 수동 지정

IP 주소를 수동 지정하면 지정한 하드웨어 주소의 PC에 항상 동일한 IP 주소를 자동 설정할 수 있습니다. 현재 할당된 IP 주소 리스트에서 선택 또는 수동으로 입력 후 추가 버튼을 클릭합니다. IP 주소 수동 지정은 DHCP 서버가 동작 중인 경우 사용 가능합니다.

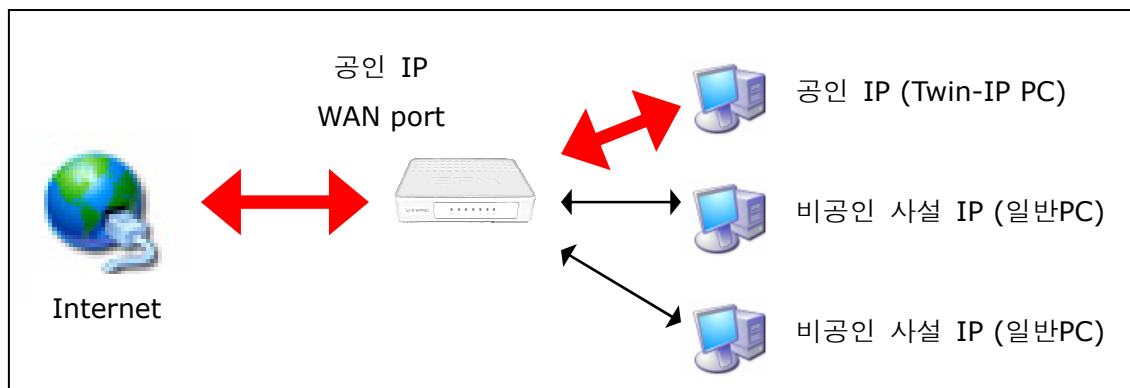
[참고] DHCP 서버 상태/설정에서 변경된 내용을 영구적으로 저장하려면 설정 화면 우측 상단의 **설정저장** 메뉴를 클릭합니다. (5.3 참조)

7.2.3 Twin IP 설정

Twin-IP 기능에 대한 간단한 설명

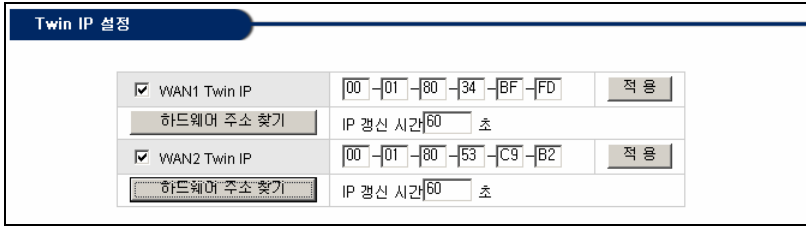
Twin IP는 인터넷 서비스 업체(ISP)로 부여받는 공인 IP주소를 ipTIME 인터넷 공유기와 연결된 내부의 특정 PC한대에 동시 설정하여 사용할 수 있는 기능입니다. 즉, Twin IP기능이 설정된 PC의 경우에는 내부 사설 IP주소가 아닌 공인 IP주소를 가지고 공유기를 사용하지 않는 환경과 동일하게 인터넷을 이용하실 수 있는 기능입니다.

ipTIME X1005에는 2개의 WAN이 존재하므로 2대의 PC를 Twin-IP PC로 지정할 수 있습니다.



<Twin-IP 망 구성도>

Twin-IP 설정은 다음과 같은 순서로 진행합니다.



Twin IP 설정 화면의 상세 내용:

☒ WAN1 Twin IP	00-01-80-34-BF-FD	적용
하드웨어 주소 찾기	IP 갱신 시간 60 초	
☒ WAN2 Twin IP	00-01-80-53-C9-B2	적용
하드웨어 주소 찾기	IP 갱신 시간 60 초	

<Twin-IP 설정 화면>

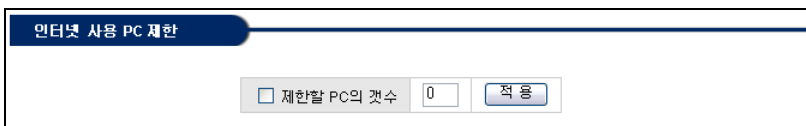
Twin-IP 설정 순서

- ① Twin-IP를 check하면 웹 설정 화면에 접속한 PC의 하드웨어 주소가 자동 입력됩니다.
- ② 하드웨어 주소 찾기 버튼을 클릭하면 다른 PC를 Twin-IP PC로 지정할 수 있습니다.
- ③ WAN의 IP 주소가 변경된 경우 IP 주소 갱신 시간이 지나면 Twin-IP PC의 IP 주소가 변경된 WAN IP 주소로 수정됩니다. 일반적인 경우 60초를 추천하며 WAN IP 주소가 바뀌게 되면 60초 이내에 Twin-IP PC로 변경된 IP 주소가 전달됩니다.
- ④ 하드웨어 주소와 갱신 시간을 입력한 후 적용을 클릭합니다.
- ⑤ 웹 설정 완료 후 해당 PC를 재시작하여야 Twin-IP 기능이 동작합니다.

[참고] Twin-IP 기능은 DHCP 서버가 동작 상태에서 사용 가능합니다. Twin-IP 설정 항목에서 변경된 내용을 영구적으로 저장하려면 설정 화면 우측 상단의 **설정저장** 메뉴를 클릭합니다. (5.3 참조)

7.2.4 인터넷 사용 PC 제한

MAC Address(랜카드 고유의 일련 번호) 를 기준으로 PC 갯수를 판단하며, 설정한 PC의 갯수 만큼 동시에 인터넷 사용이 가능합니다.



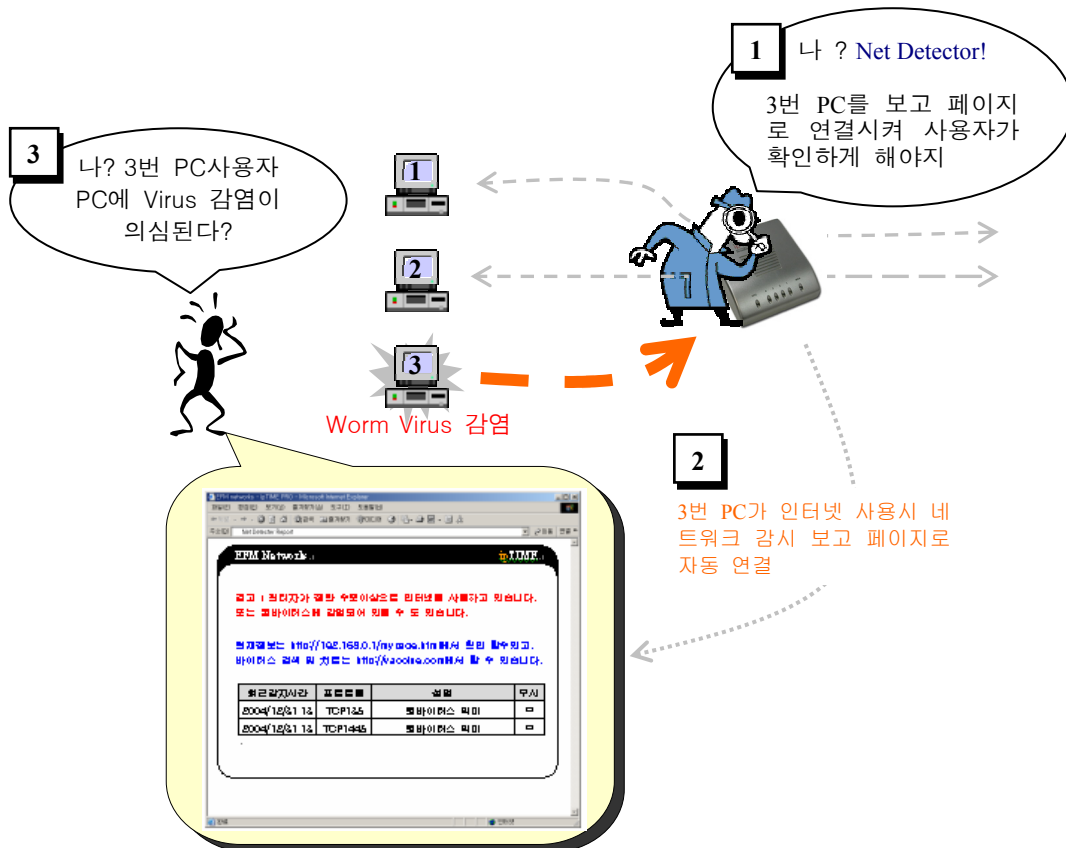
인터넷 사용 PC 제한 화면의 상세 내용:

☐ 제한할 PC의 갯수	0	적용
-------------------------------------	---	----

<인터넷 사용 PC 제한 화면>

7.3 네트워크 감시 (Net Detector)

악성 웜바이러스나 P2P 프로그램의 경우 동시에 수천개의 인터넷 연결을 발생시켜 인터넷 회선을 마비시킬 수 있습니다. ipTIME X1005의 네트워크 감시 기능은 이와 같은 통신 폭주 프로그램을 찾아내어 사용자에게 경고 메시지를 전달하고 폭주 프로그램의 통신을 적절히 제한하는 기능을 제공합니다.



<네트워크 감시 기능 동작의 도식화>

위의 그림은 네트워크 감시 기능을 도식화한 것으로 네트워크 감시 기능은 아래와 같은 순서에 따라 동작한다.

- ① 사용자가 웹 설정 화면에서 네트워크 감시 기능을 활성화 하면 네트워크 감시 모듈은 PC에서 발생시키는 인터넷 통신 데이터를 분석한다.
- ② 특정 PC에서 인터넷을 마비 시킬 수준으로 통신을 발생 시키는 경우 웹 설정 화면과 특정 PC 사용자의 웹 화면으로 경고 메시지를 출력하고 사용자가 지정한 수준 이하로 해당 통신량을 제한하여 인터넷이 사용될 수 있게 한다.
- ③ PC 사용자 또는 관리자는 웹 경고 화면에 따라 바이러스 존재 가능성을 확인할 수 있고 연동되는 하우리 Live call로 바이러스를 치료할 수 있다.

네트워크 감시 설정은 웹 설정 화면의 **네트워크 설정** 메뉴를 클릭한 뒤 **네트워크 감시** 메뉴를 클릭하면 해당 기능 설정 화면으로 접속하게 됩니다.



<네트워크 감시 설정 화면>

네트워크 감시의 동작을 위하여 설정할 항목은 다음과 같습니다.

항목	설명						
동작 설정	중단 또는 실행 버튼을 눌러 네트워크 감시를 활성화 시킵니다						
감시 수준	<table border="1"> <tr> <td>낮음</td><td>초당 300개 이상의 동시 통신 감시</td></tr> <tr> <td>보통</td><td>초당 150개 이상의 동시 통신 감시</td></tr> <tr> <td>높음</td><td>초당 50개 이상의 동시 연결 감시</td></tr> </table> 감시 대상이 되는 통신 수준을 결정합니다. 사용자가 이 수치를 직접 정의할 수도 있으며 일반적으로 보통 수준의 감시 사용을 권장합니다. 설정된 수준을 넘어서는 통신이 감지되는 경우 로그를 기록하며 설정에 따라 초과하는 트래픽을 제한할 수 있습니다.	낮음	초당 300개 이상의 동시 통신 감시	보통	초당 150개 이상의 동시 통신 감시	높음	초당 50개 이상의 동시 연결 감시
낮음	초당 300개 이상의 동시 통신 감시						
보통	초당 150개 이상의 동시 통신 감시						
높음	초당 50개 이상의 동시 연결 감시						
감지된 통신 차단	감시 수준을 넘어서는 통신에 대해서 차단 여부를 결정합니다. 웬바이러스만 차단 옵션을 체크하면 바이러스 통신만을 차단합니다.						
E-mail 통보 정책	네트워크 감시의 감지 내역을 E-mail 통보하는 방법을 지정합니다.						

미리 정의된 웹 바이러스 또는 어플리케이션 통신 내용은 아래 표와 같습니다.

내용	통신 유형
SMTP 바이러스	TCP 25
Worm.Win32.Blaster / Win32 / Ralelka.worm 바이러스	TCP 135
Unknown worm 바이러스	TCP 139
Win32 / IRCBot.worm / Win32 / AgoBot.worm 바이러스	TCP 445
Worm.Win32.Welchima	TCP 707
Unknown worm 바이러스	UDP 137
SQL_Overflow 바이러스	UDP 1434
Unknown worm 바이러스	UDP 6677
소리 바다	TCP 7674 UDP 22321
당나귀	TCP 4662 UDP 4672
V-Share	TCP 8404 UDP 8402
Win-MX	TCP 6699
FileGuri	TCP 9493
KaZaA	TCP 3531 UDP 3531

과도한 통신 트래픽이나 바이러스 트래픽이 유발 시키는 PC가 감지되면, 관리자에게 E-mail 보고와 로그 기록 이외에 해당 PC 사용자에게도 동일한 내용이 웹을 통해 보고됩니다. 해당 PC에서 웹 접속을 시도하는 경우에 '네트워크 감시'의 보고 페이지로 바뀌어 접속됩니다. 웹 보고 페이지는 다음과 같습니다.

보고서
 바이러스검사
 바이러스치료
 창닫기

- 경고 관리자가 정한 수준이상으로 인터넷을 사용하고 있습니다.
또는 웜바이러스에 감염되어 있을 수 도 있습니다.
- [경고해제/확인] 버튼을 클릭하셔야 정상적인 인터넷 사용이 가능합니다.
- [재경고해제]를 체크후 [경고해제/확인] 버튼을 클릭을 하시면 해당 이벤트 재발생시 경고페이지로 접속 되지 않습니다.
- 현재 정보는 <http://192.168.0.1/mypage.html> 에서 다시 확인하실 수 있습니다.

	최근감지시간	프로토콜	설명	재경고 해 제
NEW	2005/05/13 17:39:20	ICMP	해당포트 웜바이러스 감염 의심됨	☐
NEW	2005/05/13 17:38:06	TCP/80	웹 과다 접속 감지 또는 웜바이러스 의심	☐

경고해제/확인

[무시] 항목을 체크하고 확인을 하는 경우에는, 해당되는 통신에 의해 트래픽이 감지되어도 웹 보고 페이지로 접속되지 않습니다. 단, 이외의 다른 통신에 의해 감지되는 경우에는 웹 보고 페이지로 접속이 됩니다. 관리자는 [모든 감시 내역 삭제]시에만 개인별 [무시]항목 설정을 해제 할 수 있습니다.

[참고] 네트워크 감시 설정에서 변경된 내용을 영구적으로 저장하려면 설정 화면 우측 상단의 **설정저장** 메뉴를 클릭합니다. (5.3 참조)

7.4 링크 설정 정보

링크 설정/정보 기능은 공유기에 연결된 WAN1, WAN2, LAN 1~ 5 포트의 연결 상태, 속도, Duplex 상태 및 개별 포트의 통신량을 확인할 수 있으며, 특정 포트의 속도를 자동 또는 수동으로 결정 할 수 있습니다. 링크설정/정보 기능은 웹 설정 화면의 **네트워크 설정** 메뉴를 클릭한 뒤 **링크설정/정보** 메뉴를 클릭하면 해당 기능 설정 화면으로 접속하게 됩니다.



The screenshot shows the EFM web interface with the '링크설정/정보' (Link Settings/Information) page selected. The page has a top navigation bar with tabs: 시스템 정보, 네트워크설정, 시스템 설정, QoS 설정, 통신정책설정, 고급 설정. Below this is a sub-navigation bar with: WAN1 설정, WAN2 설정, 내부 PC 연결 설정, 네트워크 감시, 링크설정/정보 (highlighted), 라우팅테이블 관리, 스위치설정. The main content area is titled '링크 설정' and contains three sections: '링크 설정' (Link Settings), '링크 상태 정보' (Link Status Information), and '링크 통계 정보' (Link Statistics Information).

Port	Mode	Speed	Duplex	적용
WAN1	자동	10Mbps	HALF	적용
WAN2	자동	10Mbps	HALF	적용
1	자동	10Mbps	HALF	적용
2	자동	10Mbps	HALF	적용
3	자동	10Mbps	HALF	적용
4	자동	10Mbps	HALF	적용
5	자동으로 고정			

Port	WAN1	WAN2	1	2	3	4	5
Link	On	On	Off	Off	On	Off	Off
Speed	100 Mbps	100 Mbps	-	-	100 Mbps	-	-
Duplex	Full	Full	-	-	Full	-	-

Port	WAN1	WAN2	1	2	3	4	5
Rx-Packets	9	28	0	0	2557	0	0
Rx-Broadcast	8	9	0	0	136	0	0
Tx-Packets	3	20	0	0	3348	0	0

Clear

<링크 설정/정보 화면>

링크 설정/정보 사용 방법

- ① 링크 설정에서는 개별 포트의 속도를 변경할 수 있습니다.
- ② 링크 상태 정보는 개별 포트의 연결 상태, Speed, Duplex 정보를 표시합니다.
- ③ 링크 통계 정보는 개별 포트의 통신량을 표시합니다.

[참고] 화면 우측 상단 **설정저장** 을 클릭하여 변경 내용을 영구 저장합니다. (5.3 참조)

7.5 라우팅 테이블 관리

기능

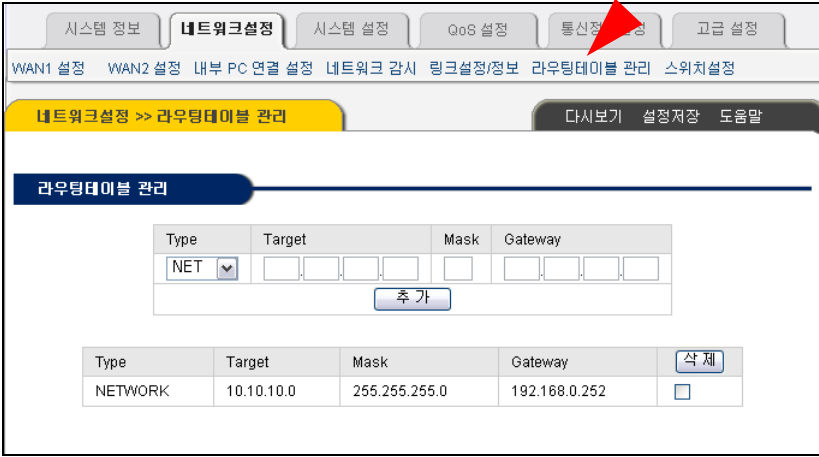
라우팅 테이블 관리 기능은 라우팅 테이블을 직접 입력할 수 있게 하는 기능입니다.

사용 방법

- ① **네트워크 설정** >> **라우팅테이블 관리**를 클릭합니다.
- ② **Type** 은 입력할 라우팅 테이블이 **HOST** 인지 **NETWORK** 인지를 설정합니다.
- ③ **Target**은 입력할 라우팅 테이블의 **Target IP**주소 또는 네트워크 주소를 입력합니다.
- ④ **Mask**는 **Type**이 **NETWORK**일 경우 **Subnet mask**를 결정합니다.
- ⑤ **Gateway**는 **Target**으로 통신할 때 거쳐갈 **Gateway**주소를 입력합니다.

사용 예

아래의 그림은 10.10.10.0 network 을 Destination으로 하는 모든 Traffic을 Gateway 192.168.0.252을 통하여 통신할 수 있도록 라우팅 테이블을 입력한 화면입니다.



Type	Target	Mask	Gateway	
NET				

추가

Type	Target	Mask	Gateway	삭제
NETWORK	10.10.10.0	255.255.255.0	192.168.0.252	☐

<라우팅테이블 관리 설정 화면>

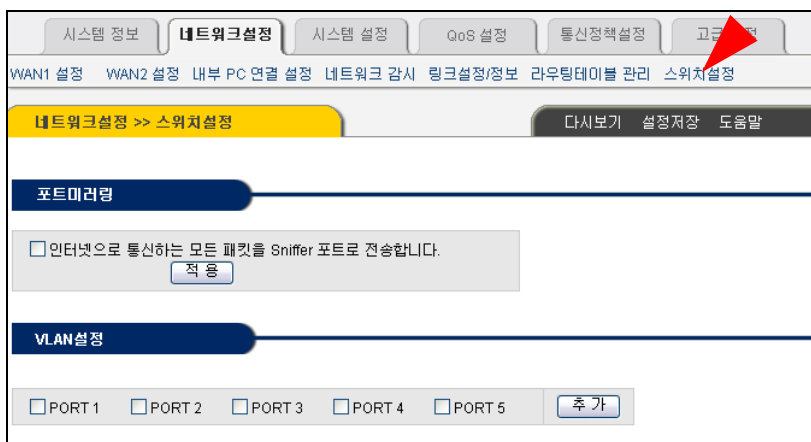
[참고] 화면 우측 상단 **설정저장** 을 클릭하여 변경 내용을 영구 저장합니다. (5.3 참조)

7.6 스위치 설정

스위치설정은 VLAN(Virtual LAN)의 기술을 이용하여 물리적 배치와 상관없이 논리적으로 LAN을 구분할 수 있는 기술입니다.

VLAN의 주된 사용 이유는 트래픽을 줄이고, 여러 워크그룹과 리소스를 분리하고, 허용된 사용자만 접속하도록 제한함과 네트워크의 보안 강화입니다.

스위치설정은 웹 설정 화면의 **네트워크설정** 메뉴를 클릭한 뒤 **스위치설정** 메뉴를 클릭하면 해당 기능 설정 화면으로 접속하게 됩니다.



<스위치설정 화면>

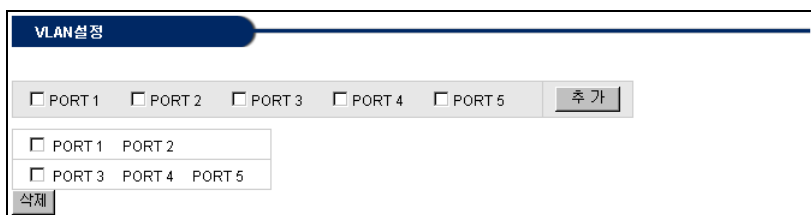
포트 미러링

- 인터넷 통신을 하는 모든 패킷을 Sniffer Port로 전송합니다.
- LAN 포트간의 통신은 전송되지 않습니다.

VLAN 설정

- 최대 5개의 Port 기반의 VLAN을 지원합니다.
- VLAN을 만들고자하는 포트를 선택한 후 추가 버튼을 누릅니다.

사용 예



< LAN 1,2(A 네트워크)와 LAN 3,4,5(B 네트워크)를 논리적으로 구분한 화면 >

8장 시스템 설정

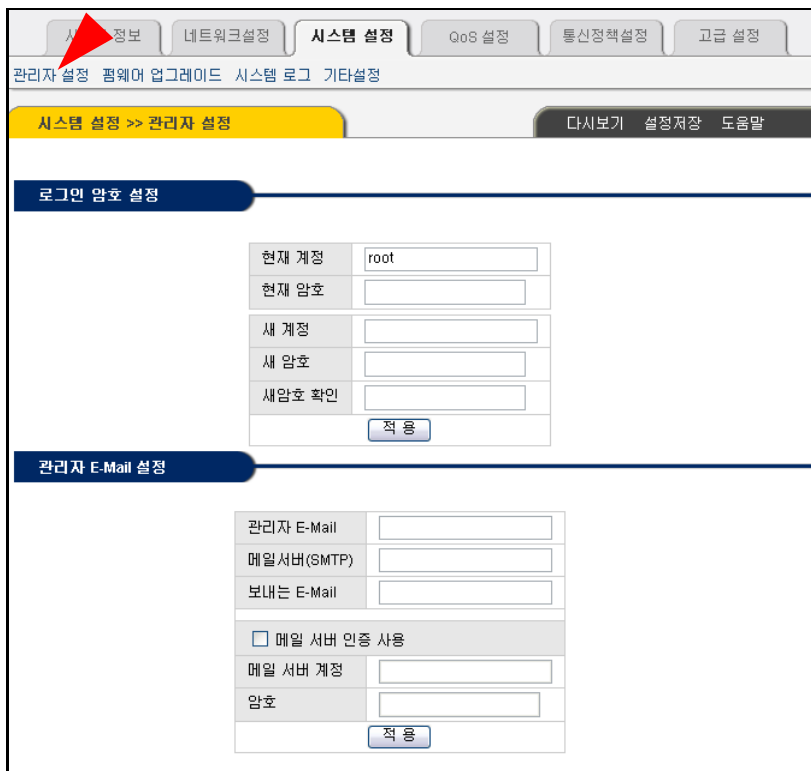
8.1 관리자 설정

로그인 암호 설정 방법

시스템설정 >> **관리자 설정** 메뉴를 클릭한 뒤 현재의 계정 및 암호, 새로 바꿀 계정 및 암호를 함께 입력한 후 적용을 누릅니다.

관리자 E-mail 설정 방법

로그를 전달 받고자 하는 관리자의 E-mail 계정과 이 계정이 등록된 메일 서버 및 서버 계정을 입력합니다.



The screenshot shows the EFM system configuration interface. At the top, there are tabs for 'System Settings', 'Network Settings', 'QoS Settings', 'Policy Settings', and 'Advanced Settings'. The 'System Settings' tab is selected, and a red arrow points to the 'Administrator Settings' sub-tab. Below the tabs, there are links for 'Administrator Settings', 'Firmware Upgrade', 'System Log', and 'Other Settings'. The 'Administrator Settings' sub-tab is active, showing two sections: 'Login Password Setting' and 'Administrator E-Mail Setting'. The 'Login Password Setting' section has fields for 'Current Account' (root), 'Current Password', 'New Account', 'New Password', and 'Confirm New Password', with an 'Apply' button. The 'Administrator E-Mail Setting' section has fields for 'Administrator E-Mail', 'Mail Server (SMTP)', 'Sending E-Mail', a checkbox for 'Use Mail Server Authentication', 'Mail Server Account', and 'Password', with an 'Apply' button.

<관리자 설정 화면>

참고

- ① 암호를 설정하기 위해서는 현재의 계정 및 암호를 정확하게 알고 계셔야 합니다.
- ② 변경된 암호는 "설정저장"을 누르지 않아도 저장이 됩니다.
- ③ 공장 출하 시 계정과 암호는 별도로 설정되어 있지 않습니다.
- ④ 로그인 암호를 잊어버린 경우 리셋 스위치를 이용 공장초기화 방법으로 초기화합니다.

(1.3장 참고)

8.2 펌웨어 업그레이드

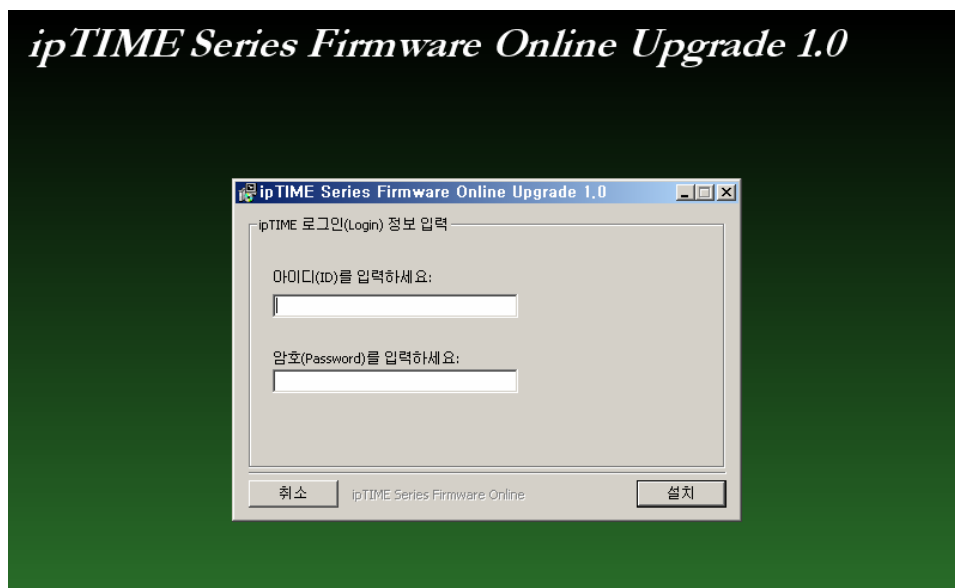
펌웨어 업그레이드 메뉴 이동

시스템설정 >> 펌웨어 업그레이드 메뉴를 클릭하면 공유기 펌웨어 업그레이드 화면으로 이동할 수 있습니다.



자동 업그레이드 유틸리티를 통한 업그레이드

공유기가 인터넷에 정상적으로 연결된 경우에는 [자동 업그레이드 유틸리티 다운 받기]를 클릭하고 해당 프로그램 열기를 선택하면 아래 그림과 같은 펌웨어 업그레이드 유틸리티가 실행되고 공유기의 최신 펌웨어로 자동 업그레이드 됩니다.



[참고] 업그레이드 도중 공유기와 인터넷을 끄면 안됩니다.

수동 업그레이드

인터넷이 연결되지 않거나 보다 안정적인 업그레이드를 위해서는 수동 업그레이드를 진행할 수 있습니다. 수동 업그레이드를 위해 <http://www.iptime.co.kr>을 방문하여 **고객지원** >> **네트워크** >> **다운로드** >> **펌웨어 수동 업데이트**를 클릭하여 제품 모델명을 ipTIME X1005로 선택한 후 해당 제품의 최신 펌웨어를 PC에 저장합니다.

[참고]

파일 1 : 한글 버전 펌웨어

파일 2 : 영문 버전 펌웨어



EFM network & multimedia

회사소개 공지/뉴스 제품소개 **고객지원** 제품구입 제품소개 바로가기

멀티미디어 • 네트워크 기술자료

ip TIME Q104 펌웨어 다운로드

펌웨어 자동 업데이트 펌웨어 수동 업데이트 제품 설명서 다운로드 유틸리티 다운로드

제품 모델명 선택 하세요

번호	제목	날짜	조회
13	ipTIME Q104 펌웨어 버전 2.28	2006/06/13	2740
12	ipTIME Q104 펌웨어 버전 2.26	2006/05/03	3957
11	ipTIME Q104 펌웨어 버전 2.24	2006/04/24	2040
10	ipTIME Q104 펌웨어 버전 2.22 (베타)	2006/03/22	2435
9	ipTIME Q104 펌웨어 버전 2.20	2006/02/07	4222
8	ipTIME Q104 펌웨어 버전 2.18	2006/01/19	2102
7	ipTIME Q104 펌웨어 버전 2.14	2005/12/28	2036
6	ipTIME Q104 펌웨어 버전 2.12	2005/11/22	2193
5	ipTIME Q104 펌웨어 버전 2.10	2005/09/15	2770
4	ipTIME Q104 펌웨어 버전 2.08	2005/08/29	1451
3	ipTIME Q104 펌웨어 버전 2.04	2005/07/12	1932
2	ipTIME Q104 펌웨어 버전 2.02	2005/06/28	1090
1	ipTIME Q104 펌웨어 버전 2.00	2005/06/27	980

페이지선택 1

☐ 이름 ☒ 제목 ☐ 내용

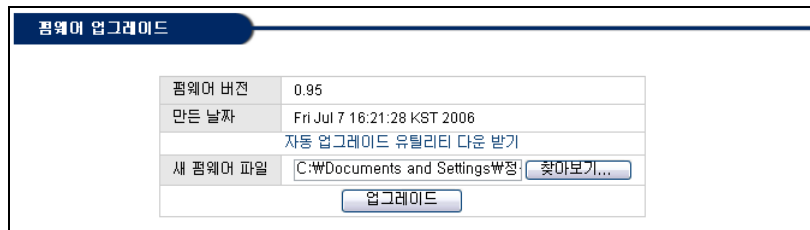
검색시작

Copyright 1999-2006 Zeroboard

<ipTIME 홈페이지 펌웨어 다운로드, 홈페이지 외관은 당사 사정에 따라 변동될 수 있음>

공유기 설정 화면에서 **찾아보기** 버튼을 클릭하여 다운 받은 펌웨어를 선택합니다.

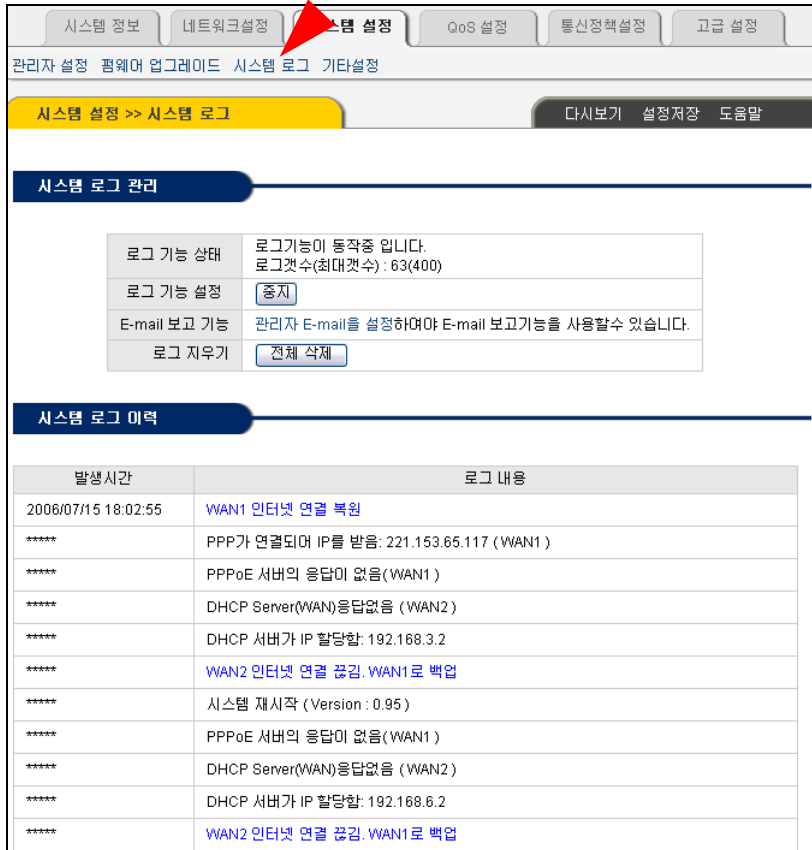
업그레이드 버튼을 클릭하여 최신 버전의 펌웨어로 업그레이드를 시작합니다.



[참고] 펌웨어 업그레이드가 완료되기 까지는 대략 3분 정도의 시간이 소요되며 만일 펌웨어 업그레이드 중 오류가 발생하여도 5분 이상 기다린 후 제품을 재시작합니다. 재시작 후에도 오류 해결이 되지 않는다면 본 설명서 1.3장을 참고하여 공유기를 공장초기화 방법으로 초기화 한 후 펌웨어를 수동으로 재업그레이드하여 정상적으로 완료한 후 사용하시기 바랍니다.

8.3 시스템 로그

시스템 로그 기능을 이용하면 공유기의 동작 내역을 확인할 수 있으며 저장된 로그를 E-mail 등으로 전송할 수 있습니다. 시스템 로그는 **시스템 설정** >> **시스템 로그** 메뉴를 선택하면 확인할 수 있습니다.



The screenshot shows the 'System Settings' (시스템 설정) menu with a red arrow pointing to the 'System Log' (시스템 로그) option. Below the menu, the 'System Log Management' (시스템 로그 관리) section displays the current log status and settings. The log is currently enabled, with a maximum of 63 log entries. The 'E-mail Report Function' (E-mail 보고 기능) is disabled, and a note indicates it must be enabled to use the E-mail report function. The 'Log Clear' (로그 지우기) button is set to 'Delete All' (전체 삭제).

The 'System Log History' (시스템 로그 이력) section shows a table of log entries:

발생시간	로그 내용
2006/07/15 18:02:55	WAN1 인터넷 연결 복원
*****	PPP가 연결되어 IP를 받음: 221.153.65.117 (WAN1)
*****	PPPoE 서버의 응답이 없음(WAN1)
*****	DHCP Server(WAN)응답없음 (WAN2)
*****	DHCP 서버가 IP 할당함: 192.168.3.2
*****	WAN2 인터넷 연결 끊김. WAN1로 백업
*****	시스템 재시작 (Version : 0.95)
*****	PPPoE 서버의 응답이 없음(WAN1)
*****	DHCP Server(WAN)응답없음 (WAN2)
*****	DHCP 서버가 IP 할당함: 192.168.6.2
*****	WAN2 인터넷 연결 끊김. WAN1로 백업

<시스템 로그 화면>

8.4 기타 설정

기타 설정은 공유기의 이름, 초기 설정 복원과 설정 파일 백업 및 시스템 재시작, 공유기 시스템 시간, UPnP 동작 설정, 설정화면 자동 연결, 로그인 페이지 설정과 관련된 내용을 변경할 수 있습니다. **시스템 설정** >> **기타 설정** 메뉴를 클릭하면 기타 설정 화면에 접속할 수 있습니다.



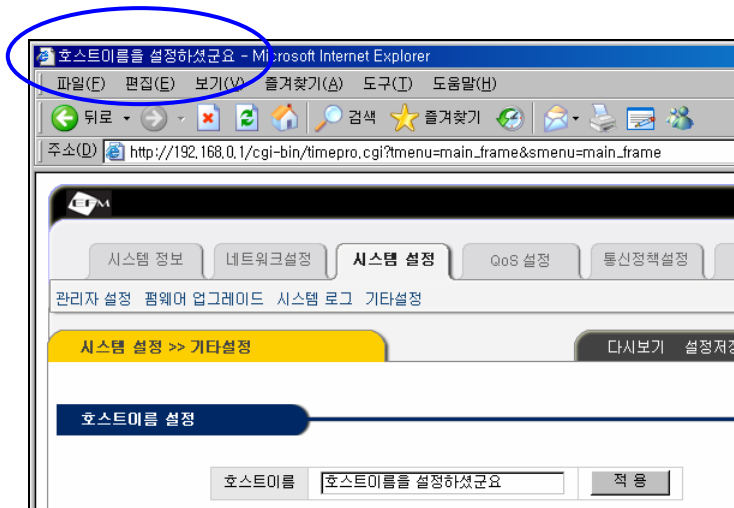
<기타 설정 화면 접속>

8.4.1 호스트 이름 설정

호스트 이름은 웹 설정 화면의 Internet Explorer 상단에 표시되는 Title입니다. 원하는 공유기 이름을 입력하고 **적용** 버튼을 클릭하면 호스트 이름이 변경됩니다. 변경 내용을 영구적으로 저장하기 위해서는 우측 상단의 **설정저장** 메뉴를 클릭합니다. (5.3 참조)



<호스트이름 설정 화면>



<호스트이름 설정을 설정하여 웹 설정 화면의 Title을 적용한 화면 >

8.4.2 설정 관리 및 재시작

설정 파일 백업을 클릭하면 공유기의 설정 상태를 PC에 파일로 저장할 수 있습니다.

설정 파일 복구를 클릭하면 PC에 저장된 파일로 공유기 설정을 복구할 수 있습니다.

초기 설정 복원을 클릭하면 공유기가 공장 출하 상태로 초기화됩니다. 1.3의 내용에 따라 리셋 스위치를 이용한 공장 초기화도 가능합니다.

설정 관리 및 재시작	
설정 파일 백업	저장되어 있는 모든 설정을 파일로 다운로드합니다.
찾아보기... 설정 파일 복구	설정 파일을 선택한 후 설정을 복구합니다. 잘못된 설정 파일은 복구 되지 않습니다.
초기 설정 복원	시스템의 모든 설정이 초기화된 후 재시작 됩니다.
시스템 재시작	시스템이 재시작됩니다. 저장 하지 않은 설정값은 지워질 수 있습니다.

<설정 관리 및 재시작 화면>

8.4.3 시스템 시간 설정

공유기가 인터넷에 연결되었을 때 시스템 시간을 얻어오는 서버와 표준 시간대를 입력합니다. 원하는 Time Server와 시간대를 선택한 후 적용 버튼을 클릭합니다. 변경 내용을 영구적으로 저장하기 위해서는 우측 상단의 **설정저장** 메뉴를 클릭합니다. (5.3 참조)

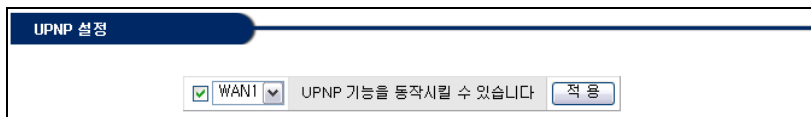
시스템 시간 설정	
현재 시스템 시간	2006년 7월 15일 토요일 12시 4분 27초
Time Server 설정	☒ time.nist.gov
	☐
	☐ 일광절약시간제 적용
표준시간대	(GMT+09:00) 서울, 도쿄
적용	

<시스템 시간 설정 화면>

[참고] 인터넷이 연결되어 있지 않거나 Time Server가 동작하지 않는 경우 1970년으로 시간이 표시될 수 있습니다.

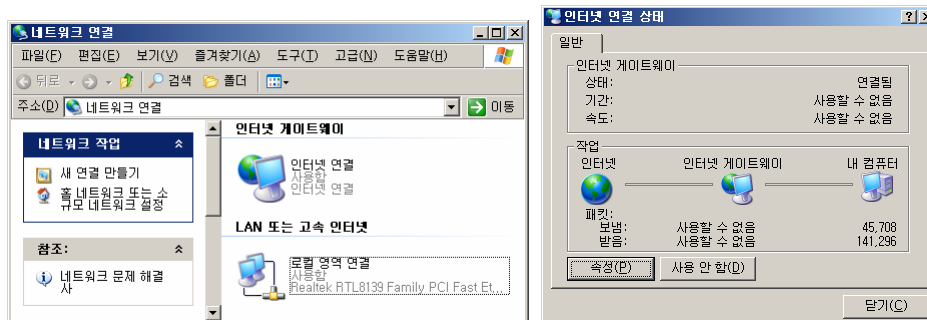
8.4.4 UPnP 설정

UPnP는 Universal Plug and Play의 약자로 MSN등 MS 윈도우 관련 제품에서 공유기의 존재 여부를 확인하여 여러 가지 서버 프로그램이 정상적으로 수행될 수 있도록 하는 프로토콜입니다. UPnP를 동작 시키기 위해서는 사용할 WAN 포트를 선택하고 체크한 뒤 **적용** 버튼을 클릭합니다.



<UPnP 설정 화면>

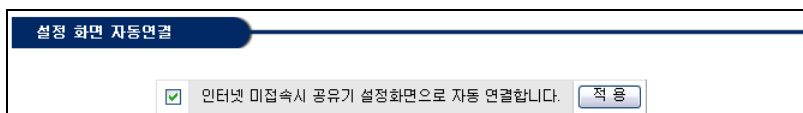
UPnP가 동작하면 XP 윈도우는 아래 그림과 같은 인터넷 게이트웨이를 인식하게 됩니다.



<윈도우 XP에서 UPnP를 통해서 인식된 IP 공유기 아이콘>

8.4.5 설정 화면 자동 연결

설정 화면 자동 연결 기능을 활성화하면 공유기가 인터넷에 연결되지 않은 경우 모든 인터넷 화면을 공유기 설정 화면으로 전환합니다. 이 기능을 이용하면 인터넷이 끊기면 바로 공유기 화면이 접속되어 인터넷 연결 상태를 쉽게 확인할 수 있습니다. 변경 내용을 영구적으로 저장하기 위해서는 우측 상단의 **설정저장** 메뉴를 클릭합니다. (5.3 참조)



<설정 화면 자동연결 설정 화면>

8.4.6 로그인 페이지 설정

공유기의 웹 설정 화면에 접속하는 경우 최초 표시되는 로그인 화면을 보여줄지 여부를 결정합니다. 변경 내용을 영구적으로 저장하기 위해서는 우측 상단의 **설정저장** 메뉴를 클릭합니다. (5.3 참조)

로그인 페이지 설정	
☒ 처음 접속할때 로그인 페이지를 보여줍니다.	적용
☐ 처음 접속할때 로그인 페이지를 보여주지 않습니다.	

<로그인 페이지 설정 화면>

9장 QoS 설정

QoS를 이용하면 공유기에 연결된 PC의 인터넷 속도를 원하는 대역만큼 제한하거나 보장할 수 있습니다. QoS를 이용하기 위해서는 먼저 QoS 기본 설정을 통하여 사용되는 인터넷의 대역폭을 정의한 뒤 IP 주소, Application 또는 L4 port 번호에 근거하여 인터넷 대역폭을 제한하거나 보장할 수 있습니다.

9.1 QoS 기본 설정

QoS 기능은 공유기에 연결된 장비들의 인터넷 사용 대역폭을 제한 또는 보장하는 기능입니다. QoS 기능의 정상적인 동작을 위해서는 공유기가 접속된 인터넷 속도에 대한 기본값을 정확히 설정합니다.



<QoS 기본 설정 화면>

사용 방법

- ① 공유기 설정 화면에 접속한 뒤 **QoS 설정** >> **QoS 기본설정**을 클릭합니다.
- ② QoS를 동작 시키기 위해서는 QoS 기능 설정의 **실행** 버튼을 클릭합니다.
- ③ 인터넷 속도의 입력은 인터넷의 종류를 선택하면 해당 서비스의 다운로드와 업로드 속도가 자동으로 입력되며 인터넷 종류를 사용자 정의로 설정하면 다운로드 속도와 업로드 속도를 임의의 값으로 입력할 수 있습니다.
- ④ QoS의 정확한 동작을 위해 **<http://speed.nca.or.kr>** 등의 속도 측정 사이트에서 정확한 인터넷 속도를 측정한 뒤 사용자 정의로 입력할 것을 권장합니다.
- ⑤ 인터넷 속도를 수정하게 되면 기 입력된 IP, 포트, 어플리케이션 별 QoS 설정 규칙이 무의미해지므로 기 설정된 규칙은 삭제됩니다.
- ⑥ 인터넷 속도는 WAN1, WAN2를 전부 입력하여야 합니다.

[참고]

설정 상태를 영구 저장하기 위해서는 화면 우측 상단의 **설정저장** 버튼을 클릭합니다.

9.2 IP 주소별 QoS 설정

IP 주소별 QoS를 설정하면 지정된 내부 IP 주소 PC가 WAN1, WAN2 포트에 다운로드 받거나 업로드하는 인터넷 속도의 최대 속도를 제한하거나 최소 속도를 보장할 수 있습니다.

최대 속도 제한은 영화 파일 다운로드 등 과도한 인터넷 사용을 방지하기 위해 사용하며, **최소 속도 보장**은 인터넷 강의 등과 같이 일정한 수준 이상의 인터넷 속도가 보장되어야 하는 경우 사용합니다.

사용 방법

- ① 공유기 설정 화면에 접속한 뒤 **QoS 설정** >> **IP 주소별 설정**을 클릭합니다.
 - ② 속도를 제어하고자 하는 PC의 IP주소와 해당 WAN 포트를 입력합니다.
 - ③ 동작 방법에서 최대 속도 제한 또는 최소 속도 보장을 선택합니다.
 - ④ 다운로드 속도와 업로드 속도를 입력합니다.
 - ⑤ 업/다운 로드 중 한가지 속도만 제어하는 경우 원하는 쪽의 속도만 입력합니다.
 - ⑥ IP 주소별 QoS 규칙은 15개까지 입력할 수 있습니다.
- [참고] 설정 상태를 영구 저장하기 위해서는 화면 우측 상단의 **설정저장** 버튼을 클릭합니다.



IP 주소	WAN	동작방법	다운로드	업로드	삭제
192.168.0.2	WAN1	최대 속도 제한	1 Mbps	-----	☐
192.168.0.3	WAN1	최소 속도 보장	2 Mbps	-----	☐

<IP 주소별 QoS 설정 화면>

앞의 그림에서 입력된 IP 주소별 QoS 설정 내역은 다음과 같습니다.

QoS 설정 예	QoS 동작 방식
192.168.0.2 WAN1 다운로드 1Mbps로 최대 속도 제한	192.168.0.2는 WAN1으로 1Mbps 이상 다운 받을 수 없다 다른 트래픽이 증가하면 다운로드가 1Mbps 이하가 될 수도 있다. 다른 트래픽이 없는 경우에도 다운로드는 1Mbps로 제한 된다.
192.168.0.3 WAN1 다운로드 2Mbps로 최소 속도 보장	192.168.0.3은 WAN1으로 2Mbps 이상 다운 받을 수 있도록 한다. 다른 트래픽이 증가하여도 다운로드는 최소 2Mbps 이상을 유지한다. 다른 트래픽이 없는 경우 다운로드는 2Mbps 이상으로 증가할 수 있다.

9.3 어플리케이션별 QoS 설정

어플리케이션 QoS 설정하면 WAN1, WAN2를 다운로드/업로드되는 특정 어플리케이션의 속도를 최대 속도 제한 또는 최소 속도 보장할 수 있습니다.

사용 방법

- ① 공유기 설정 화면에 접속한 뒤 **QoS 설정** >> **어플리케이션별 설정**을 클릭합니다.
- ② 속도를 제어하고자 하는 어플리케이션 - WAN 포트에 check 합니다.
- ③ 동작 방법에서 최대 속도 제한 또는 최소 속도 보장을 선택합니다.
- ④ 다운로드 속도와 업로드 속도를 입력합니다.
- ⑤ 업/다운 로드 중 한가지 속도만 제어하는 경우 원하는 쪽의 속도만 입력합니다.
- ⑥ 입력 후 **적용** 버튼을 클릭하여 입력한 내용을 적용합니다.

[참고]

설정 상태를 영구 저장하기 위해서는 화면 우측 상단의 **설정저장** 버튼을 클릭합니다.



QoS 기본 설정 IP주소별 설정 어플리케이션별 설정 포트별 설정

QoS 설정 >> 어플리케이션별 설정

다시보기 설정저장 도움말

어플리케이션 설정

WAN1 인터넷 연결 속도	다운로드 8 Mbps	업로드 512 Kbps
WAN2 인터넷 연결 속도	다운로드 8 Mbps	업로드 4 Mbps

종 류	WAN	동작방법	다운로드	업로드
WWW(HTTP)	☐ WAN1	최대 속도 제한 ▼	0 Kbps ▼	0 Kbps ▼
	☐ WAN2	최대 속도 제한 ▼	0 Kbps ▼	0 Kbps ▼
소리바다	☒ WAN1	최대 속도 제한 ▼	3 Mbps ▼	0 Kbps ▼
	☐ WAN2	최대 속도 제한 ▼	0 Kbps ▼	0 Kbps ▼
구루구루	☒ WAN1	최소 속도 보장 ▼	0 Kbps ▼	128 Kbps ▼
	☐ WAN2	최대 속도 제한 ▼	0 Kbps ▼	0 Kbps ▼
WinMX	☐ WAN1	최대 속도 제한 ▼	0 Kbps ▼	0 Kbps ▼
	☐ WAN2	최대 속도 제한 ▼	0 Kbps ▼	0 Kbps ▼
eDonkey	☐ WAN1	최대 속도 제한 ▼	0 Kbps ▼	0 Kbps ▼
	☐ WAN2	최대 속도 제한 ▼	0 Kbps ▼	0 Kbps ▼
MS Streaming	☐ WAN1	최대 속도 제한 ▼	0 Kbps ▼	0 Kbps ▼
	☐ WAN2	최대 속도 제한 ▼	0 Kbps ▼	0 Kbps ▼

적용

<어플리케이션별 QoS 설정 예>

앞의 그림에서 설정된 어플리케이션 별 QoS는 다음과 같습니다.

QoS 설정 예	QoS 동작 방식
소리바다 WAN1 다운로드 3Mbps로 최대 속도 제한	소리바다 서버에서 3Mbps 이상의 속도로 다운 받을 수 없다. 다른 트래픽이 증가하면 소리바다 서버에서 다운로드는 3Mbps 이하가 될 수 있다. 다른 트래픽이 없는 경우에도 소리바다 서버에서 다운로드하는 3Mbps로 제한 된다.
구루구루 WAN1 업 로드 128Kbps로 최소 속도 보장	외부의 구루구루 서버로 128Kbps 이상의 속도로 업로드할 수 있도록 한다. 다른 트래픽이 증가하여도 구루구루 업로드는 최소 128Kbps 이상을 유지한다. 다른 트래픽이 없는 경우 구루구루 업로드는 128Kbps 이상이 될 수 있다.

9.4 포트별 QoS 설정

포트별 QoS에서 정의하는 포트번호는 WAN1, WAN2로 연결되어 있는 인터넷 서버의 포트 번호입니다.

포트별 QoS를 설정하면 WAN1, WAN2로 연결된 인터넷 서버로의 다운로드 및 업로드를 최대 속도 제한하거나 최소 속도 보장할 수 있습니다.

사용 방법

- ① 공유기 설정 화면에 접속한 뒤 **QoS 설정** >> **포트별 설정**을 클릭합니다.
- ② 속도를 제어하고자 하는 포트번호, 프로토콜 종류, WAN 포트를 선택합니다.
- ③ 동작 방법에서 최대 속도 제한 또는 최소 속도 보장을 선택합니다.
- ④ 다운로드 속도와 업로드 속도를 입력합니다.
- ⑤ 업/다운 로드 중 한가지 속도만 제어하는 경우 원하는 쪽의 속도만 입력합니다.
- ⑥ 입력 후 **적용** 버튼을 클릭하여 입력한 규칙을 추가합니다.

[참고] 설정 상태를 영구 저장하기 위해서는 화면 우측 상단의 **설정저장** 버튼을 클릭합니다.



포트번호	프로토콜	WAN	동작방법	다운로드	업로드	삭제
80	TCP	WAN1	최대 속도 제한	2 Mbps	-----	☐
80	TCP	WAN1	최소 속도 보장	-----	256 Kbps	☐

<포트별 QoS 설정 화면 예>

앞의 그림에서 설정된 포트별 QoS는 다음과 같습니다.

QoS 설정 예	QoS 동작 방식
TCP 80 포트 WAN1 다운로드 2Mbps로 최대 속도 제한	외부 서버의 80 포트에서 2Mbps 이상으로 다운 받을 수 없다 즉 외부의 HTTP 서버에서 2Mbps 이상으로 다운 받을 수 없다. 다른 트래픽이 증가하면 외부 HTTP 서버에서 다운로드하는 2Mbps 이하가 될 수도 있다. 다른 트래픽이 없는 경우에도 192.168.0.2의 다운로드는 2Mbps로 제한된다.
TCP 80 포트 WAN1 업 로드 256Kbps로 최소 속도 보장	외부 서버의 80 포트로 256Kbps 이상으로 업로드할 수 있도록 한다. 즉 외부 HTTP 서버로는 항상 256Kbps 이상 업로드할 수 있도록 한다. 다른 트래픽이 증가하여도 외부 HTTP 서버 업로드는 최소 256Kbps 이상을 유지한다. 다른 트래픽이 없는 경우 외부 HTTP 서버 업로드는 256Kbps 이상이 될 수 있다.

10장 통신 정책 설정

통신 정책 설정에서는 2 WAN에 백업, 통신 분산 정책과 공유기에 연결된 PC의 특정 서버 프로그램과 이와 유사한 응용 프로그램을 사용할 수 있도록 하는 공유기 설정 메뉴를 제공합니다.

10.1 분산 정책 설정

분산 정책 설정에서는 ipTIME X1005의 두 개의 WAN 포트를 어떻게 사용할 것인지를 결정합니다.

용어 정의

용어	설명
기본 분산 경로	자동 분산과 사용자 정의 분산이 별도로 설정되지 않은 경우 인터넷 접속에 사용하는 WAN 포트
자동 인터넷 라인 백업	WAN1, WAN2 중 하나의 포트가 끊긴 경우 모든 인터넷 연결을 끊기지 않는 WAN 포트를 사용하도록 하는 기능
자동 분산 비율	WAN1, WAN2가 모두 인터넷에 연결되어 있는 경우 정해진 비율에 따라 인터넷 통신을 자동으로 분배하는 기능
사용자 정의 분산 정책	사용자가 정의하는 분산 경로로 WAN1과 WAN2 중에서 어느 쪽으로 인터넷을 연결할지를 규정함

라인 백업과 분산 정책에 따른 WAN1, WAN2의 인터넷 연결 경로

WAN1	WAN2	자동 분산 정책	자동 라인 백업	동작
ON	ON	ON	X	자동 분산 비율에 따라 WAN1/2 동시 통신 사용자 분산 정책은 정해진 경로로 통신
ON	ON	OFF	x	기본 분산 경로로만 통신 사용자 분산 정책이 있는 경우 별도 적용
ON	OFF	x	ON	모든 인터넷 WAN1으로 통신
ON	OFF	OFF	OFF	기본 분산 경로와 사용자 분산 정책이 WAN1 인 경우만 인터넷 통신 가능
OFF	ON	x	ON	모든 인터넷 WAN2으로 통신
OFF	ON	OFF	OFF	기본 분산 경로와 사용자 분산 정책이 WAN2 인 경우만 인터넷 통신 가능

[참고]

ipTIME X1005 제품은 백업 공유기로 Dual WAN을 제공합니다.

WAN을 하나만 연결하여 사용하시는 경우,

자동 분산 비율 설정 및 자동 인터넷 라인 백업 기능은 비활성화하여 사용하시기 바랍니다.

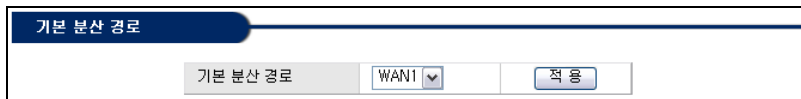
통신 정책 설정에서는 자동 인터넷 라인 백업 기능과 트래픽 분산 기능을 설정합니다. 분산 정책 설정을 위해서는 공유기 웹 설정 화면에 접속한 뒤 **통신정책설정** >> **분산정책설정** 메뉴를 클릭합니다.



<분산 정책 설정 메뉴 접속 화면>

10.1.1 기본 분산 경로

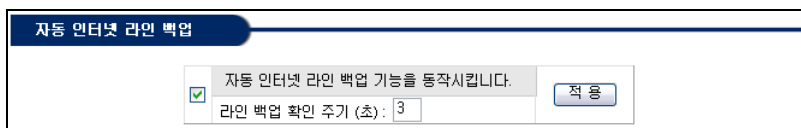
사용자가 별도의 트래픽 분산 규칙을 입력하지 않았을 경우 사용하게 되는 인터넷 연결 경로입니다. 기본 인터넷 회선이 연결되어 있는 WAN 포트를 선택하여 사용하는 것을 권장합니다. WAN1이 기본 설정 값입니다.



<기본 분산 경로 입력 화면>

10.1.2 자동 인터넷 라인 백업

자동 인터넷 라인 백업 기능은 WAN1 또는 WAN2의 인터넷이 단절되었을 경우 단절되지 않는 WAN 포트를 이용하여 모든 인터넷 통신이 이루어지도록 자동 백업하는 기능입니다. 기본 설정 값은 자동 인터넷 라인 백업 ON이며, 라인 백업 확인 주기는 3초입니다. 기능을 해제하고자 하는 경우 좌측 check를 풀고 적용을 클릭합니다.



<자동 인터넷 라인 백업 기능 설정 화면>

[참고] 자동 백업이 해제된 경우 WAN1/2하나가 단절되면 단절된 WAN 포트로 분산 설정된 인터넷 연결은 사용할 수 없습니다. 일반적인 경우라면 자동 인터넷 라인 백업을 활성화시키고 사용할 것을 권장합니다.

10.1.3 자동 분산 비율 설정

자동 분산 비율 정책을 활성화하면 인터넷을 접속하며 발생하는 TCP/UDP 컨넥션을 입력한 비율에 따라 WAN1과 WAN2로 분산하여 맺어주므로 WAN1과 WAN2의 인터넷 대역폭을 입력한 비율에 따라 나누어 쓸 수 있게 됩니다. 자동 분산 비율을 설정하면 자동 인터넷 라인 백업도 같이 활성화 됩니다.



<자동 분산 비율 설정 화면>

설정 항목	기능 설명
PC IP 주소 단위 분산	PC의 IP를 기준으로 통신을 시작하는 순서에 따라 WAN1, WAN2로 자동 분산됩니다.
PC IP 주소 단위 분산 + 포트 단위 분산	본 기능의 선택시 PC에서 발생하는 패킷의 목적지 포트에 따라 WAN1,2를 분산하여 통신하게 됩니다. 로그인이 필요한 웹 사이트 및 게임과 같은 경우 로그인을 다시 해야하는 경우가 발생할 수 있으므로 주의하시기 바랍니다.

PC IP 주소 단위 분산 설정하여 **STATUS** 버튼을 클릭하시면

아래 그림처럼 WAN1, WAN2에 각각 분산되어 통신중인 IP 정보를 확인할 수 있습니다.



<STATUS 화면>

10.1.4 사용자 정의 분산 정책

사용자 정의에 따른 분산 정책을 입력합니다. 분산 정책을 적용하고자 하는 PC의 IP 주소와 프로토콜 번호 및 경로(WAN1/WAN2)를 입력합니다.

사용 예

아래의 그림은 group A에 속한 IP를 사용하는 PC는 WAN1으로 통신하고, Group B에 속한 IP를 사용하는 PC는 WAN2로 통신하도록 사용자정의 분산정책을 입력한 화면입니다.

사용자정의 분산정책

규칙 이름					
내부 PC IP 주소	☒ 192.168.0.1		넷마스크		
	☐ 192.168.0.1		-		
목적지 IP 주소	☒		넷마스크		
	☐		-		
프로토콜	any				
시작지 포트		~		목적지 포트	
					~
분산경로	WAN1				
현재 접속되어 있는 PC의 IP는 192.168.0.2 입니다.					
추가					

규칙 이름	IP 주소	프로토콜	포트번호	분산경로	삭제
group A	192.168.0.2 - 192.168.0.100 -> any	any	any -> any	WAN1	☐
group B	192.168.0.101 - 192.168.0.254 -> any	any	any -> any	WAN2	☐

<사용자 정의 분산 정책 화면>

10.2 어플리케이션 설정

기능

어플리케이션 설정을 이용하면 버디버디, 원애플방송, 구루구루 등과 같은 서버의 특징을 갖는 어플리케이션 프로그램을 지정된 IP 주소의 PC에서 정상적으로 사용할 수 있게 합니다. ipTIME X1005는 WAN1과 WAN2가 있으므로 2개의 다른 PC에서 개별 어플리케이션을 운영할 수 있습니다.

사용 방법

웹 설정 화면에 접속한 뒤 **통신정책설정** >> **어플리케이션 설정**을 클릭한 뒤 사용할 어플리케이션 및 WAN 포트에 check하고 어플리케이션을 운영할 PC의 IP 주소를 입력한 뒤 하단의 **적용** 버튼을 클릭합니다.



어플리케이션	WAN1 :: 내부 IP주소	WAN2 :: 내부 IP주소
버디버디	☐ 192.168.0.	☐ 192.168.0.
원애플방송	☐ 192.168.0.	☐ 192.168.0.
구루구루	☐ 192.168.0.	☐ 192.168.0.
넷미팅	☐ 192.168.0.	☐ 192.168.0.
WinMx	☐ 192.168.0.	☐ 192.168.0.
Windows XP/2000 원격 데스크톱 연결	☐ 192.168.0.	☐ 192.168.0.
네트워크 드라이브 연결	☐ 192.168.0.	☐ 192.168.0.
H.323 인터넷 전화기	☐ 192.168.0.	☐ 192.168.0.
소리바다2	☐ 192.168.0.	☐ 192.168.0.
☐ 멀티캐스트 포워드	멀티캐스트 데이터를 송수신하는 경우에 사용합니다.	
현재 접속되어 있는 PC의 IP는 192.168.0.2 입니다.		
적용		

<어플리케이션 설정 화면>

[참고] 설정 상태를 영구 저장하기 위해서는 화면 우측 상단의 **설정저장** 버튼을 클릭합니다.

아래 표는 어플리케이션의 포트 번호입니다.

어플리케이션	설 명	사용포트
버디버디	외부 사용자로부터의 파일 수신 기능	TCP 812, TCP 987
원애플 방송	외부 사용자대상으로 원애플 방송 서버 운용	TCP 8000
구루구루	외부 사용자대상으로 구루구루 서버 운용	TCP 9292 TCP 9999
넷미팅	외부 사용자대상으로 넷미팅 전화 받기	TCP 1720
WinMX	파일 업로드 기능	TCP 6699 UDP 6257
원격데스크 탐연결	외부 사용자대상으로 원격데스크탑 서버 접속	TCP 3389 UDP 3389

FTP 비정규 포트 설정

기능

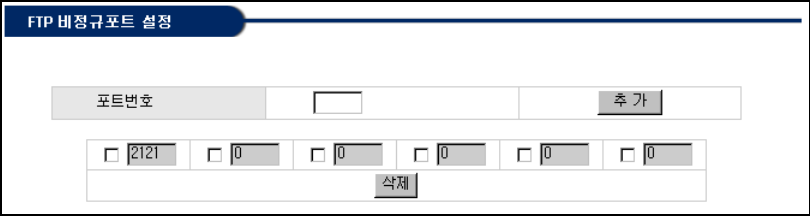
공유기 내부 또는 외부에 설치된 FTP 서버가 비정규 포트를 이용하여 운영되는 경우 FTP 비정규 포트 설정을 하여야 합니다.

사용 방법

어플리케이션 설정 화면 하단의 FTP에 사용되는 비정규 포트 번호를 입력합니다.

사용 예

FTP 기본 포트인 21번이 아닌 2121을 이용하여 운영되는 경우, FTP 비정규 포트를 적용한 화면입니다.



[참고] 설정 상태를 영구 저장하기 위해서는 화면 우측 상단의 **설정저장** 버튼을 클릭합니다.

10.3 내부 서버 설정

기능

내부 서버 설정 기능을 이용하면 내부 네트워크에 WEB 서버, Telnet 서버, 메일 서버, DNS 서버, PPTP 서버 (Windows NT등의 사설 망 기능), DMZ 호스트를 운용할 수 있습니다. ipTIME X1005는 WAN1, WAN2가 있어 각 WAN 포트에 대하여 내부 서버를 설정할 수 있습니다. 내부 서버를 사용하는 경우 내부 서버의 IP 주소는 수동으로 고정 할당하면 편리하며 서버 프로그램에서는 표준 포트 번호를 사용하여야 합니다

사용 방법

- ① 내부 서버 설정을 위해 공유기의 설정화면에 접속한 뒤 **통신 정책 설정** >> **내부 서버 설정** 메뉴를 클릭합니다.
- ② 내부 서버에 따라 프로토콜이 표시되며 프로토콜에 따른 서버를 운용하기 위해서는 좌측의 Check Box을 클릭하여 선택합니다. 프로토콜에 따른 서버의 기능은 아래 표를 참고합니다.

Protocol	Server
DNS	DNS 서버
SMTP	송신 메일 서버
POP3	수신 메일 서버
HTTP	웹 서버
News	뉴스 서버
FTP	FTP 서버
Telnet	Telnet 서버
PPTP	VPN (Windows NT등) 서버

- ③ 내부 서버 WAN1과 WAN2의 IP 주소 항목에는 운용하고자 하는 내부 서버의 내부 IP 주소를 입력합니다. 내부 서버를 운용하는 경우 서버의 비공인 IP 주소는 수동으로 할당하는 것이 편리합니다.
- ④ 외부 사용 포트에는 외부에서 해당 서버를 접속할 때 외부에서 접속되는 Port 번호를 지정합니다. 외부 사용 포트 번호의 기본 값은 well-known Port 번호로 일반적인 경우 항목은 수정하지 않도록 합니다. **외부 사용 Port 번호를 변경하는 경우라도 내부 서버의 포트 번호는 표준 포트 번호(well-known port)를 유지합니다.**
- ⑤ DMZ 호스트 설정기능은 내부 어플리케이션, 내부서버, 포트포워드에서 설정되어 있지 않은 모든 포트들을 내부의 특정 IP 주소를 가지는 PC로 전달하는 기능입니다. 어플리케이션 포트번호를 알 수 없어 인터넷 공유가 정상적으로 이루어지지 않는 프로그램들은 DMZ 호스트 기능을 사용하여, 지정된 IP 주소의 PC에서 정상적으로 사용할 수 있습니다.

시스템 정보 네트워크 설정 **보안 설정** QoS 설정 통신정책설정 고급 설정

분산정책 설정 어플리케이션 설정 내부 서버 설정 포트포워드 설정 포트 트리거 NAT On/Off

통신정책설정 >> 내부 서버 설정 다시보기 설정저장 도움말

내부 서버 설정

프로토콜	WAN1 :: 내부 서버 IP 주소	외부 포트 (내부 포트)	WAN2 :: 내부 서버 IP 주소	외부 포트 (내부 포트)
DNS	☐ 192.168.0.0	53 (53)	☐ 192.168.0.0	53 (53)
SMTP	☐ 192.168.0.0	25 (25)	☐ 192.168.0.0	25 (25)
POP3	☐ 192.168.0.0	110 (110)	☐ 192.168.0.0	110 (110)
HTTP	☐ 192.168.0.0	80 (80)	☐ 192.168.0.0	80 (80)
News	☐ 192.168.0.0	119 (119)	☐ 192.168.0.0	119 (119)
FTP	☐ 192.168.0.0	21 (21)	☐ 192.168.0.0	21 (21)
Telnet	☐ 192.168.0.0	23 (23)	☐ 192.168.0.0	23 (23)
SSH	☐ 192.168.0.0	22 (22)	☐ 192.168.0.0	22 (22)
PPTP	☐ 192.168.0.0	1723	☐ 192.168.0.0	1723

현재 접속되어 있는 PC의 IP는 192.168.0.2 입니다.

DMZ 호스트 설정

☐ WAN1 DMZ 192.168.0.0 ALL

☐ WAN2 DMZ 192.168.0.0 ALL

현재 접속되어 있는 PC의 IP는 192.168.0.2 입니다.

<내부 서버 설정 화면>

[참고] PPTP 서버를 설정하면 ipTIME X1005에 내장된 VPN 서버를 사용할 수 없습니다.
 설정 상태를 영구 저장하기 위해서는 화면 우측 상단의 **설정저장** 버튼을 클릭합니다.

10.3 포트포워드 설정

공유기의 외부 네트워크 사용자가 내부 네트워크를 접속하고자 하는 경우 외부 네트워크에서 접속을 요청한 Application Protocol의 Port 번호를 내부 네트워크의 비공인 IP 주소와 이에 따른 내부 Port 번호에 Mapping하는 기능이 필요합니다. 포트포워드 설정으로 외부 접속 요청에 내부 IP 주소 및 Port 번호를 Mapping 할 수 있습니다

사용 방법

- ① 공유기 설정 화면에 접속한 뒤 **통신 정책 설정** >> **포트포워드 설정**을 클릭합니다.
- ② 포트포워드 규칙을 구성하는 항목과 이에 따른 설명은 아래 표를 참고 합니다.

설정 항목	기능 설명
규칙 이름	새로 입력하는 포트포워드 규칙의 이름을 입력합니다 예 : "구루구루", "SQL" 등 자유롭게 입력
프로토콜	포트포워드를 원하는 프로토콜의 종류를 선택합니다. (TCP 또는 UDP 선택)
외부 사용 포트 범위	WAN1/WAN2를 선택하고 수신되는 Destination Port 번호를 입력합니다. 포트포워드를 원하는 Port가 1개일 경우 시작 값만 입력합니다.
내부PC IP주소 범위	WAN 포트로 수신된 패킷을 전달할 내부 PC의 IP 주소를 입력합니다.
내부 포트 사용 범위	WAN 포트로 수신된 패킷을 전달할 내부 PC의 포트 번호를 입력합니다. 수신된 Port와 같은 포트로 전달을 원하는 경우 입력하지 않아도 됩니다.

- ③ 규칙을 입력한 뒤 **추가** 버튼을 클릭하면 입력한 규칙이 추가됩니다.
 - ④ 규칙을 삭제하고자 하는 경우 해당 규칙의 우측 **check box**를 클릭한 뒤 **삭제** 버튼을 클릭합니다.
 - ⑤ 규칙을 때에 따라 활성화/비활성화 와 같이 동작을 변경하시려면 규칙 왼쪽 **check box**를 조정한 후 **동작** 버튼을 사용하여 수정합니다.
 - ⑥ 규칙 이름을 클릭하면 해당 규칙을 수정할 수 있습니다.
- [참고] 설정 상태 영구 저장을 위해서는 화면 우측 상단의 **설정저장** 버튼을 클릭합니다.

사용 예

A,B PC에서 각각 프루나를 사용할 수 있도록 프루나 포트를 각각 달리하여 포트포워드 설정한 화면입니다.



통신정책설정 >> 포트포워드 설정

다시보기 설정저장 도움말

포트포워드 설정

규칙 이름: 프로토콜: TCP

외부 사용 포트 범위: WAN1 -

내부 PC IP 주소: 192.168.0.

내부 사용 포트 범위: -

현재 접속되어 있는 PC의 IP는 192.168.0.2입니다.

동작	규칙 이름	프로토콜	외부 사용 포트 범위	내부 PC IP	내부 사용 포트 범위	삭제
☒	pruna01_PCA	tcp	[WAN1] 4662	192.168.0.2		☐
☒	pruna02_PCA	udp	[WAN1] 4672	192.168.0.2		☐
☒	pruna01_PCB	tcp	[WAN1] 4663	192.168.0.3		☐
☒	pruna02_PCB	udp	[WAN1] 4673	192.168.0.3		☐

<포트포워드 설정 화면>

10.5 포트 트리거 설정

인터넷을 사용하는 어플리케이션에서 사용하는 TCP/UDP 포트 번호를 감지하여 해당 어플리케이션에 필요한 포트를 현재 사용 중인 PC로 자동 포트포워딩 시켜주는 기능을 포트 트리거 기능이라고 합니다.

사용 방법

- ① 공유기 설정 화면에 접속한 뒤 **통신 정책 설정** >> **포트 트리거**를 클릭합니다.
- ② 포트포워드 규칙을 구성하는 항목과 이에 따른 설명은 아래 표를 참고 합니다.

설정 항목	기능 설명
규칙 이름	새로 입력하는 포트 트리거 규칙의 이름을 입력합니다 예 : "버디버디", "MY RULE" 등 자유롭게 입력
포트트리거 프로토콜	어플리케이션의 온라인 접속을 감지하기 위한 프로토콜의 종류를 선택합니다. 인터넷 어플리케이션 서버의 목적지 포트 프로토콜(TCP 또는 UDP 선택)
포트트리거 포트 범위	어플리케이션의 온라인 접속을 감지하기 위한 포트범위를 입력합니다. 인터넷 어플리케이션 서버의 목적지 포트 번호
포트포워드 프로토콜	어플리케이션 사용을 위한 포트포워드 프로토콜의 종류를 선택합니다.
포트포워드 포트범위	어플리케이션 사용을 위한 포트포워드 포트를 입력합니다. 다수개의 포트 번호 입력시 구분은 "공백"으로 합니다.

- ③ 규칙을 입력한 뒤 **추가** 버튼을 클릭하면 입력한 규칙이 추가됩니다.
 - ④ 규칙을 삭제하고자 하는 경우 해당 규칙의 우측 check box를 클릭한 뒤 **삭제** 버튼을 클릭합니다.
- [참고] 설정 상태 영구 저장을 위해서는 화면 우측 상단의 **설정저장** 버튼을 클릭합니다.

시스템 정보 네트워크 설정 시스템 설정 QoS 설정 **통신정책설정** 고급 설정

분산정책 설정 어플리케이션 설정 내부 서버 설정 포트포워드 설정 포트 트리거 NAT On/Off

통신정책설정 >> 포트 트리거

다시보기 설정저장 도움말

포트트리거 설정

규칙이름		
포트트리거	프로토콜	TCP ▼
	포트범위	-
포트포워드	프로토콜	TCP ▼
	포트범위	

추가

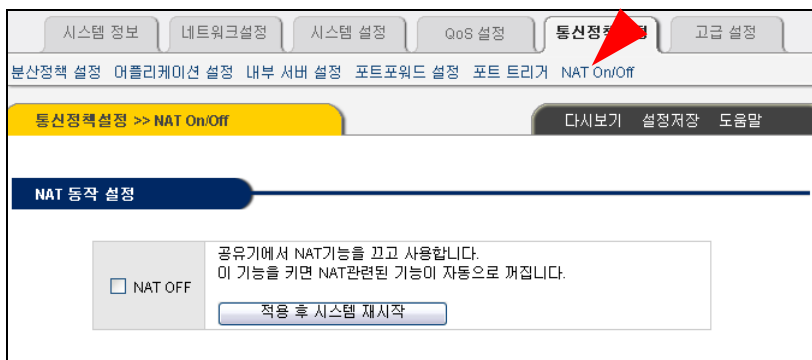
규칙이름	포트트리거 조건	포트포워드 조건	삭제
------	----------	----------	----

<포트 트리거 설정 화면>

10.6 NAT On/Off 기능

ipTIME X1005의 NAT 기능을 중지 시켜 일반 라우터로 사용하기 위한 기능입니다.
NAT 기능을 중지시키면 IP 공유기로 사용을 중단하게 되며 일반 라우터 모드로 동작합니다.

ipTIME X1005를 IP공유기로 동작시키기 위해서는 NAT On 모드에서 사용하여야 합니다.
라우터나 네트워크에 대한 자세한 사용을 숙지하고 NAT Off 모드를 이용하여야 합니다.



<NAT On/Off 설정 화면>

[참고] NAT기능을 OFF하시게 되면 일반적인 IP공유기로서의 정상적인 사용이 불가능합니다. 일반라우터 모드로 사용하시려면 반드시 라우터와 네트워크의 충분한 기술을 숙지하시고 사용하셔야 합니다.

11장 고급 설정

11.1 보안 설정

기능

- Denial of Service (DoS)는 한 사람이 공유자원을 모두 점유하여 다른 사람이 사용할 자원을 없애버리는 공격방식으로 해당 공격에 대해 방어설정을 할 수 있습니다.
- 보안 설정 기능을 이용하면 특정 내부 PC 들 및 외부 PC 들의 통신을 차단 또는 허용할 수 있습니다.

사용 방법

(1) DoS 공격의 종류 및 설명

- ① SYN Flooding : TCP 가 데이터를 보내기 전에 연결을 맺어야 하는 연결 지향(connection-oriented) 방식이라는 점을 착안하여 많은 수의 SYN bit 이 설정되어있는, 즉 연결을 요청하는 TCP 패킷을 호스트의 특정 포트에 보내어 포트의 대기 큐(backlog queue)를 가득차게 하여 포트에 들어오는 연결 요청을 큐가 빌 때 까지(connection time out 이 될 때 까지) 무시하도록 하게 끔 하는 공격방식.
- ② Smurf : ping 의 목적지주소를 브로드캐스트 주소로 사용하는 공격 방식. Smurf 공격은 Echo-request 패킷을 어떤 네트워크의 브로드캐스트 주소로 보내면 해당 네트워크의 모든 호스트가 request 패킷에 응답하느라 다른 일은 하지 못하도록 하는 공격방식
- ③ IP Source Routing : RFC 1122 에 따르면 목적지의 경로에 대한 세부적인 내용을 담고 있는 IP Source Routing 은 목적지 호스트에서도 같은 경로를 따라 반응을 해야 한다는 문제점이 있다. Cracker 가 특정 네트워크에 Source Routing 패킷을 보낼 수 있다면 돌아오는 반응을 가로채서 상대방의 호스트와 신뢰받은 호스트처럼 속일 수 있다
- ④ IP Spoofing : 네트워크 시스템에서 서로 신뢰관계에 있는 A, B 두 시스템간에는 A 시스템의 account 를 가지고 B 시스템을 액세스 할 수 있다. 이는 네트워크에서 신뢰관계를 형성하는 서비스가 네트워크 주소에 기반하여 이를 인증하기 때문이다. 이로 인해 IP Spoofing 이 가능해진다. IP Spoofing 은 이 신뢰관계에 있는 두 시스템 사이에서 Hacker 의 호스트를 마치 하나의 신뢰관계에 있는 호스트인 것처럼 속이는 것이다.
- ⑤ 인터넷으로부터 오는 ICMP(ping) 막기를 설정하면 공유기는 인터넷에서 수신되는 Ping 요청에 응답하지 않습니다.

- ⑥ 인터넷으로 나가는 ICMP(ping) 막기를 설정하면 공유기에 연결된 PC 가 송신하는 모든 Ping 요청을 차단하여 공유기에 연결된 PC 는 공유기에 대한 ping 과 인터넷에 존재하는 다른 장비에 대한 ping 시험을 할 수 없게 됩니다. 이 기능을 설정하면 바이러스에 걸린 내부 PC 가 과도한 ping 요청으로 공유기와 인터넷에 존재하는 다른 장비를 공격하는 것으로 보호해줍니다.

(2) 개별 보안 정책 설정

- ① 설정 화면에 접속한 뒤 **고급 설정** >> **보안 설정**을 클릭합니다.
- ② 보안 설정을 위한 규칙 입력 항목은 아래 표를 참고 합니다.

설정 항목	기능 설명																				
방향	외부 -> 내부 : 공유기 외부 인터넷에서 내부 LAN으로 통신 내부 -> 외부 : 공유기 내부 LAN에서 외부 인터넷으로 통신																				
하드웨어주소	공유기에 연결된 PC 등의 하드웨어 주소																				
시작지 IP 주소	외부 -> 내부의 경우 : 보안 설정을 하는 인터넷 상의 특정 IP 주소 내부 -> 외부의 경우 : 보안 설정을 하는 내부 LAN 의 IP 주소 추가적인 넷마스크를 설정하면 IP 주소 범위를 지정할 수 있다.																				
목적지 IP 주소	외부 -> 내부의 경우 : 보안 설정을 하는 내부 LAN 의 IP 주소 내부 -> 외부의 경우 : 보안 설정을 하는 인터넷 상의 특정 IP 주소 추가적인 넷마스크를 설정하면 IP 주소 범위를 지정할 수 있다.																				
넷 마스크	시작지/목적지 IP 주소 입력 시 넷 마스크를 입력하면 IP 주소 범위를 지정할 수 있다 넷 마스크에 따른 IP 범위 (C class 기준) <table><tr><th>넷마스크</th><th>IP 네번째 값</th><th>넷마스크</th><th>IP 네번째 값</th></tr><tr><td>31</td><td>0 ~ 1</td><td>27</td><td>1 ~ 31</td></tr><tr><td>30</td><td>1 ~ 3</td><td>26</td><td>1 ~ 63</td></tr><tr><td>29</td><td>1 ~ 7</td><td>25</td><td>1 ~ 127</td></tr><tr><td>28</td><td>1 ~ 15</td><td>24</td><td>1 ~ 254</td></tr></table>	넷마스크	IP 네번째 값	넷마스크	IP 네번째 값	31	0 ~ 1	27	1 ~ 31	30	1 ~ 3	26	1 ~ 63	29	1 ~ 7	25	1 ~ 127	28	1 ~ 15	24	1 ~ 254
넷마스크	IP 네번째 값	넷마스크	IP 네번째 값																		
31	0 ~ 1	27	1 ~ 31																		
30	1 ~ 3	26	1 ~ 63																		
29	1 ~ 7	25	1 ~ 127																		
28	1 ~ 15	24	1 ~ 254																		
프로토콜	Protocol-Type을 선택합니다. TCP, UDP, ICMP, any 중 택일 Any를 선택하는 경우 설정한 IP 주소의 모든 포트에 대한 보안 규칙이 지정됩니다.																				
목적지 포트	외부 -> 내부의 경우 : 보안 설정 내부 LAN 의 목적지 포트 번호 내부 -> 외부의 경우 : 보안 설정 인터넷 목적지 포트 번호																				
허용 차단	위와 같이 설정한 규칙에 적용되는 packet에 대해 허용/차단을 정의합니다																				

사용 예

192.168.0.2 ~ 192.168.0.99 IP를 사용하는 PC는 TCP 80 포트를 차단하여 인터넷 사용을 할 수 없고, 192.168.0.200 IP를 사용하는 PC는 모든 포트를 차단하여, 모든 통신이 차단되도록 보안 설정이 적용된 화면입니다.



DoS 방어설정

☒ SYN Flooding
 ☒ Smurf
 ☒ IP source routing
 ☒ IP Spoofing

☒ 인터넷으로부터 오는 ICMP(ping) 막기
☐ 인터넷으로 나가는 ICMP(ping) 막기

보안 설정

방향: 내부 -> 외부
 내부PC 하드웨어 주소: [] [] [] [] [] [] 하드웨어 주소 찾기
 시작지 IP 주소: ☒ [] [] [] [] 넷마스크 []
☐ [] [] [] [] - [] [] [] []
 목적지 IP 주소: ☒ [] [] [] [] 넷마스크 []
☐ [] [] [] [] - [] [] [] []
 프로토콜: any 목적지 포트: [] ~ []
 허용/차단: 허용
 추가

방향	시작지 IP 주소	목적지 IP 주소	프로토콜	목적지 포트	허용/차단	수정	삭제
내부 -> 외부	IP: 192.168.0.2 - 192.168.0.99	모든 IP주소	tcp	80	차단	☐	☐
내부 -> 외부	IP: 192.168.0.200	모든 IP주소	any		차단	☐	☐

<보안 설정 화면>

11.2 DDNS 설정

기능

PPPoE 또는 DHCP 방식의 유동 IP 환경에서 공유기 하단에 FTP, Web 서버 등을 운영하는 경우 공유기의 외부 IP 주소를 매번 확인하여야 하는 불편함이 발생합니다. 공유기에서 제공하는 ipTIME DDNS 또는 DynDNS Client 기능을 이용하면 유동 IP 주소를 도메인 이름으로 자동 변경하므로 매번 공유기의 외부 IP주소를 확인하지 않아도 편리하게 서버 운영을 할 수 있습니다.

[참고]

- ipTIME DDNS를 사용하기 위해서는 별도의 등록 없이 공유기 설정만으로 사용할 수 있습니다.
- DynDNS 설정을 위해서는 먼저 dyndns.org에 사용자 이름 및 도메인을 등록한 뒤 공유기를 설정하여야 합니다.

사용 방법 - ipTIME DDNS

- (1) 공유기 설정 화면에 접속한 뒤 **고급 설정** >> **DDNS 설정**을 클릭합니다.
 - (2) **호스트 이름** 항목에 사용할 도메인(호스트이름)을 입력합니다.
ex : x1005.iptime.org
 - (3) 사용자 계정 및 암호를 입력한 후 **추가** 버튼을 클릭합니다.
사용자 계정 : 주로 사용하시는 웹 메일 (ex : x1005@iptime.co.kr)
사용자 암호 : 사용자 계정에 등록한 E-mail 의 암호
 - (4) 접속 상태 항목이 "정상등록"이라고 표시되면 모든 설정이 완료된 상태입니다.
- [참고] 설정 상태 영구 저장을 위해서 화면 우측 상단의 **설정저장** 버튼을 클릭합니다.

사용 방법 - dyndns.org(DynDns)

- (1) 공유기 설정 화면에 접속한 뒤 **고급 설정** >> **DDNS 설정**을 클릭합니다.
 - (2) 서비스 공급자를 **dyndns.org(DynDns)**로 선택합니다.
 - (3) **호스트 이름** 항목에 DynDNS.org 에 등록된 도메인(호스트이름)을 입력합니다.
 - (4) 사용자 계정 및 암호를 입력한 후 **추가** 버튼을 클릭합니다.
사용자 계정 : dyndns.org(DynDns) 로그인 계정
사용자 암호 : dyndns.org(DynDns) 로그인 암호
 - (5) 접속상태 항목이 "정상등록"이라고 표시되면 모든 설정이 완료된 상태입니다.
- [참고] 설정 상태 영구 저장을 위해서 화면 우측 상단의 **설정저장** 버튼을 클릭합니다.

사용 예 (ipTIME DDNS)

(1) 공유기 설정 화면



시스템 정보 네트워크설정 시스템 설정 QoS 설정 통신정책설정 고급 설정

보안 설정 DDNS설정 원격PC제어(WOL) 사이트 접속 차단 원격 공유기 관리 사용 시간 제한 VPN 설정

고급 설정 >> DDNS설정 다시보기 설정저장 도움말

DDNS 동작/계정 설정

호스트이름	서비스 공급자	사용자 계정	사용자 암호	기본 WAN
	ipTIME DDNS			WAN1

- ipTIME DDNS를 사용하실때에는 별도의 등록과정이 필요하지 않습니다.
- 호스트이름은 iptime.org 로 끝나야 합니다. (예> testtest.iptime.org)
- 사용자계정에는 E-mail주소를 입력하셔야 합니다.
- 한개의 호스트이름만 사용하실 수 있습니다.

추가

호스트이름	서비스 공급자	사용자 계정	기본 WAN	접속상태	갱신	삭제
x1005.iptime.org (168.126.129.26)	ipTIME DDNS	x1005@iptime.co.kr	wan1	정상 등록	☐	☐

ipTIME DDNS 암호찾기

등록시 사용한 E-mail 주소를 입력하세요.

보내기

(2) 아래 그림처럼 등록된 도메인으로 “ping” 테스트를 합니다.

```
C:\W>ping x1005.iptime.org
Pinging x1005.iptime.org [168.126.129.26] with 32 bytes of data:
Reply from 168.126.129.26: bytes=32 time<1ms TTL=255
Reply from 168.126.129.26: bytes=32 time<1ms TTL=255
Reply from 168.126.129.26: bytes=32 time<1ms TTL=255
Reply from 168.126.129.26: bytes=32 time<1ms TTL=255

Ping statistics for 168.126.129.26:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\W>
```

(3) 도메인 이름으로 Ping이 정상적으로 수행되면 DDNS 설정이 완료된 것입니다.

11.3 원격 PC 제어 (WOL)

기능

원격 PC 제어 (WOL : Wake-up On Lan) 기능을 이용하면 공유기에 연결된 PC 의 전원을 공유기를 통하여 Power On 할 수 있습니다. WOL을 이용하기 위해서는 PC에 WOL 기능을 제공하는 LAN card가 설치되어야 합니다.

원격 PC 제어 기능을 이용할 경우 인터넷을 통하여 공유기에 접속한 뒤 PC Power-On이 가능하므로 사무실이나 가정에 설치된 PC를 어디서든지 켤 수 있습니다. 인터넷을 통한 공유기 접속은 원격 공유기 관리 기능의 사용법을 참고합니다.

사용 방법

- ① 공유기 설정 화면에 접속한 뒤 **고급 설정** >> **원격 PC 제어** 메뉴를 클릭 합니다.
- ② WOL을 실행하고자 하는 PC의 이름과 하드웨어 주소를 입력합니다.
- ③ **추가** 버튼을 클릭하면 하단에 PC 리스트에 PC 내용이 추가됩니다.
- ④ 개별 PC 항목에 **PC 켜기** 버튼을 클릭하면 해당 PC가 Power On됩니다.
- ⑤ 개별 PC 항목에 **삭제** 버튼을 클릭하면 PC 리스트가 삭제됩니다.



The screenshot shows the '고급 설정 >> 원격PC제어(WOL)' page. At the top, there are tabs for '시스템 정보', '네트워크', '시스템 설정', 'QoS 설정', '통신정책설정', and '고급 설정'. The '고급 설정' tab is active. Below the tabs, there are sub-tabs: '보안 설정', 'DDNS설정', '원격PC제어(WOL)', '사이트 접속 차단', '원격 공유기 관리', '사용 시간 제한', and 'VPN 설정'. The '원격PC제어(WOL)' sub-tab is selected. Below the sub-tabs, there is a yellow bar with '고급 설정 >> 원격PC제어(WOL)' and a grey bar with '다시보기', '설정저장', and '도움말'. The main content area is titled '내부 PC 등록'. It contains a form with 'PC 이름' and '하드웨어 주소' fields. The '하드웨어 주소' field has a dropdown menu set to '자동' and a '하드웨어 주소 찾기' button. Below the form is a '추가' button. At the bottom, there is a table with columns: 'PC 이름', '하드웨어 주소', 'PC 켜기', and '삭제'. The table contains one entry: 'TEST_PC01' with hardware address '00:13:8F:8A:2F:8A'. The 'PC 켜기' button is labeled 'PC 켜기' and the '삭제' button is labeled '삭제'.

<원격 PC 제어 설정 화면>

[참고] 설정 상태 영구 저장을 위해 화면 우측 상단의 **설정저장** 버튼을 클릭합니다.

11.4 사이트 접속 차단

기능

사이트 접속 차단 기능은 특정 문자열을 갖는 사이트 주소에 대한 접속을 제한하는 기능입니다. 가정에서 청소년을 위한 유해 사이트의 접속 차단에 사용될 수 있습니다.

사용 방법

- (1) 공유기 설정 화면에 접속한 뒤 **고급 설정** >> **사이트 접속 차단**을 클릭합니다.
- (2) 사이트 접속 차단을 가동하기 위해서는 동작 설정의 **실행** 버튼을 클릭합니다.
- (3) 사이트 접속 차단의 중지를 위해서는 동작 설정의 **중단** 버튼을 클릭합니다.
- (4) 접속을 차단할 IP주소 또는 하드웨어 주소를 입력합니다.
- (5) 접속을 차단하고자 하는 사이트의 URL 문자열을 입력합니다.
- (6) 차단이 설정된 URL을 해제하기 위해서는 해당 URL의 **삭제** 버튼을 클릭합니다.
- (7) 문자열 입력란에 " " (스페이스)로 구분하여 여러 개의 문자열을 입력할 수 있습니다.

ex : sex cyworld naver

사용 예

192.168.0.100 ~ 192.168.0.200 IP를 사용하는 PC에서 www.sex.com, www.sexpage.com 등 sex 단어가 들어가는 모든 도메인으로의 접속을 차단합니다.

192.168.0.2 ~ 192.168.0.254 IP를 사용하는 PC에서 리니지 프로그램의 접속을 차단합니다.



시스템 정보 네트워크설정 시스템 설정 QoS 설정 통신정책설정 고급 설정

보안 설정 DDNS설정 원격PC제어(WOL) 사이트 접속 차단 원격 공유기 관리 사용 시간 제한 VPN 설정

고급 설정 >> 사이트 접속 차단 다시보기 설정저장 도움말

접속 차단 관리

동작 상태 동작중
동작 설정 중단

IP주소 192.168.0.192.168.0
하드웨어주소 00.00.00.00.00.00 하드웨어 주소 찾기
문자열 입력 Messenger
추가

차단될 주소	Filter String/Application	삭제
IP 주소:192.168.0.100 - 192.168.0.200	sex	삭제
IP 주소:192.168.0.2 - 192.168.0.254	[리니지]	삭제

<사이트 접속 차단 설정 화면>

11.5 원격 공유기 관리

기능

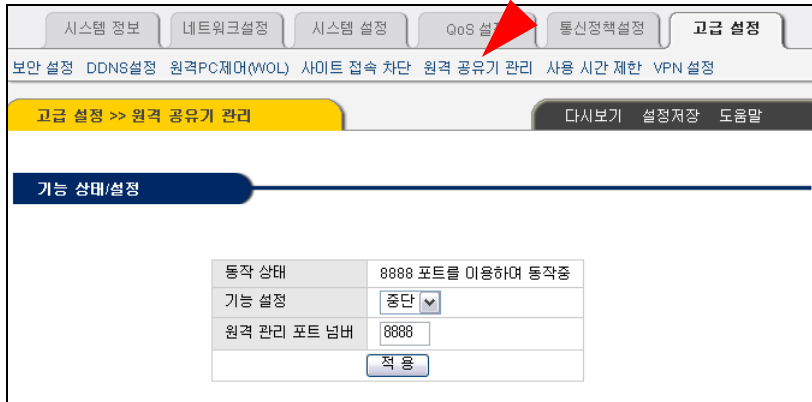
원격 ipTIME 관리 기능은 외부(인터넷)에서 공유기의 설정 화면에 접속할 수 있게 합니다.

사용 방법

- (1) 공유기 설정 화면에 접속한 뒤 **고급 설정** >> **원격 공유기 관리** 메뉴를 클릭합니다.
- (2) 원격 관리 기능의 사용을 위해 기능 설정을 **실행**으로, 외부에서 공유기에 접속하고자 하는 포트 번호는 사용자의 선택에 따라 입력한 뒤 **적용** 버튼을 클릭합니다.
- (3) 원격 관리 기능을 중지하려면 기능 설정을 **중단**으로 선택한 뒤 **적용**을 클릭합니다.
- (4) 원격 관리 기능 활성화 후 외부(인터넷)에서 공유기의 접속은 웹 브라우저에 주소란에 `http://xxx.xxx.xxx.xxx:pppp`와 같이 URL을 입력하면 공유기 설정 화면에 접속이 가능합니다. xxx.xxx.xxx.xxx는 공유기의 WAN1 또는 WAN2 IP주소이며 pppp는 사용자가 임의로 설정한 원격 관리 포트 넘버입니다.

사용 예

8888번 포트로 외부(인터넷)에서 공유기 접속이 가능하도록 설정한 예



동작 상태	8888 포트를 이용하여 동작중
기능 설정	중단 ▼
원격 관리 포트 넘버	8888
적용	

< 원격 공유기 관리 설정 화면 >

참고

- 설정 상태를 영구 저장하기 위해서는 화면 우측 상단의 **설정저장** 버튼을 클릭합니다.
- 유동 IP 서비스의 경우 외부 IP가 자주 바뀌기 때문에 DDNS 기능과 연동하여 사용하면 편리합니다

11.6 사용 시간 제한

기능

사용자가 정의한 특정 요일 및 시간대에 지정한 PC 또는 모든 PC의 인터넷 사용을 제한할 수 있습니다.

사용 방법

- (1) 공유기 설정 화면에 접속한 후 **고급 설정** >> **사용 시간 제한**을 클릭합니다.
- (2) 인터넷 사용을 제한할 특정요일을 설정합니다.
- (3) 인터넷 사용을 제한할 시간대를 설정합니다. 하루 24시간 형태로 설정이 가능하며, '22:00 ~ 03:00'와 같이 양일간의 형태로는 설정할 수 없습니다.
예1) 오후 8시부터 오후 12까지 제한할 때 -> '20:00 ~ 00:00'로 설정
예2) 새벽 0시부터 오전 6까지 제한할 때 -> '00:00 ~ 06:00'로 설정
- (4) 인터넷 사용을 제한할 PC의 주소를 설정합니다.
 - IP 주소 : 인터넷 사용을 제한할 PC의 IP 주소를 설정합니다.
 - 넷 마스크 : 마스크를 통해 IP주소의 범위를 지정할 수 있습니다. (C클래스 기준)
 - 하드웨어주소: 인터넷 사용을 제한할 PC의 하드웨어 주소를 설정합니다.
: 선택시 현재 사용중인 PC의 하드웨어 주소가 자동설정 됩니다
- (5) 모든 설정이 완료되었으면, **추가** 버튼을 클릭합니다.

사용 예

모든 PC를 매일 오전9시~12시와 오후 1시~6시의 인터넷을 제한한 예



제한할 요일	제한할 시간대	제한할 주소	삭제
일 월 화 수 목 금 토	09:00 ~ 12:00	ALL IP	☐
일 월 화 수 목 금 토	13:00 ~ 18:00	ALL IP	☐

<사용 시간 제한 설정 화면>

[참고]

- 시스템설정 >> 기타 설정에서 설정한 Time Server 로 부터 현재시간을 얻어오지 못하는 경우에는 정상 동작하지 않습니다.
- 사용 시간 제한 설정 기능을 사용할 때에는 시스템설정 >> 관리자 설정에서 암호를 설정하기를 권장합니다.

12장 VPN 서버 기능

12.1 VPN 서버 기능

ipTIME X1005의 VPN 기능은 windows 운영 체제에서 기본적으로 제공되는 가상 사설망 어댑터를 이용한 PPTP 기반의 VPN 서버 기능입니다.

VPN 서버 기능을 이용하면 인터넷에 연결된 다수의 PC를 하나의 LAN에 연결된 것처럼 망을 구성할 수 있어 VPN 서버에 연결된 PC 사이에 자유롭게 파일 공유 및 프린터 공유를 할 수 있으며 LAN 환경에서 사용되는 여러 프로그램들을 자유롭게 사용할 수 있습니다.

VPN 서버를 사용하기 위해서는 고급 설정에서 VPN 서버 상태를 동작 중으로 변경하고 접속을 허용할 VPN 계정을 만들어 주어야 합니다. 또한 VPN 서버에 접속하기 위해서는 해당 PC의 윈도우 운영 체제에서 가상 사설망 접속 어댑터를 설치하여야 합니다.

ipTIME X1005의 VPN 서버 기능은 최대 5명의 사용자까지 VPN 서버에 접속하여 LAN VPN 환경을 구성할 수 있습니다.

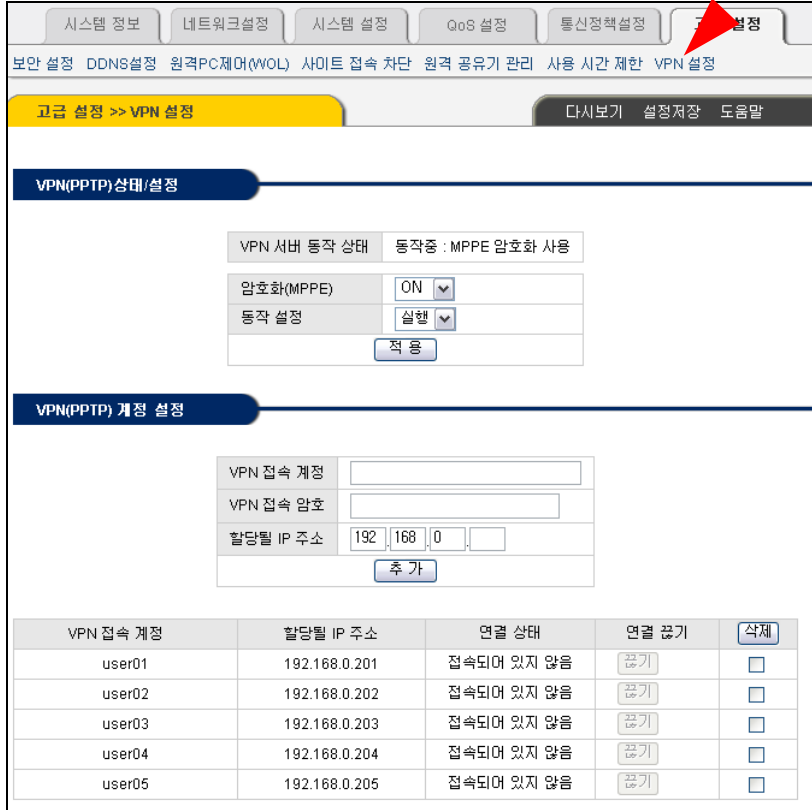
참고 : VPN에 대한 기본 설명

사무실이나 연구실과 같이 LAN 환경에서 익숙해진 컴퓨터 사용자의 경우, 인터넷이 연결된 다른 장소에서도 익숙해진 LAN 환경에 접속하여 파일 서버, 프린터를 이용하고, LAN 내부의 여러 PC들과 자료를 공유할 수 있습니다.

VPN을 구성하는 방법은 IPSec 또는 PPTP 등의 방법이 있으며, ipTIME X1005는 PPTP 기반의 VPN을 지원한다. PPTP 기반의 VPN 구성을 위해서는 사무실 LAN 환경에서는 PPTP 서버가 원격지 PC에는 가상 사설망 어댑터가 설치되어야 합니다.

PPTP 서버와 가상 사설망 어댑터를 이용 VPN을 구성하게 되면 논리적으로 원격지 PC는 사무실 LAN에 연결된 상태가 유지됩니다. 이와 같은 원리로 VPN으로 접속된 PC는 LAN 환경에서 수행되는 모든 어플리케이션을 인터넷을 통하여 수행할 수 있습니다.

12.2 VPN 서버 설정 방법



VPN(PPTP)상태/설정

VPN 서버 동작 상태 : 동작중 : MPPE 암호화 사용

암호화(MPPE) : ON

동작 설정 : 실행

적용

VPN(PPTP) 계정 설정

VPN 접속 계정 :

VPN 접속 암호 :

할당될 IP 주소 : 192.168.0.0

추가

VPN 접속 계정	할당될 IP 주소	연결 상태	연결 끊기	삭제
user01	192.168.0.201	접속되어 있지 않음	끊기	☐
user02	192.168.0.202	접속되어 있지 않음	끊기	☐
user03	192.168.0.203	접속되어 있지 않음	끊기	☐
user04	192.168.0.204	접속되어 있지 않음	끊기	☐
user05	192.168.0.205	접속되어 있지 않음	끊기	☐

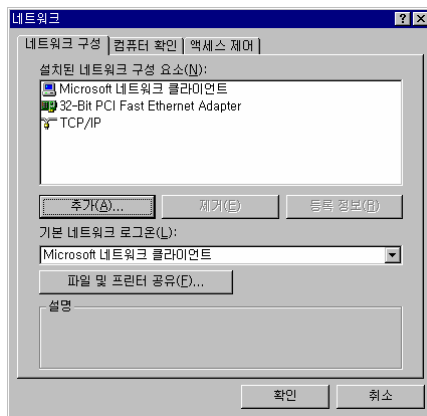
- ① 공유기 웹 설정 화면에 접속한 뒤 **고급 설정** >> **VPN 설정**을 클릭합니다.
- ② 암호화(MPPE)기능 사용여부를 선택한다. 만약 암호화 기능을 사용한다면, PC에서 클라이언트 설정 시 "데이터 암호화"를 설정해야 합니다.
- ③ VPN 접속 계정을 아래와 같은 과정으로 추가합니다.
 - VPN 접속 계정에 VPN 서버 사용자 이름을 입력합니다.
 - VPN 접속 암호에 사용자에게 해당 암호를 입력합니다.
 - VPN 접속 시 할당될 IP 주소를 입력합니다.
 - **추가** 버튼을 클릭하여 VPN 사용자 계정을 추가합니다.
- ④ VPN(PPTP) 상태/설정의 **실행** 버튼을 클릭하여 VPN 서버를 동작시킵니다. VPN을 동작시키면 공유기가 재시작된 뒤 VPN 기능이 동작합니다.

12.3 Windows 98/ME에서의 VPN 서버 접속

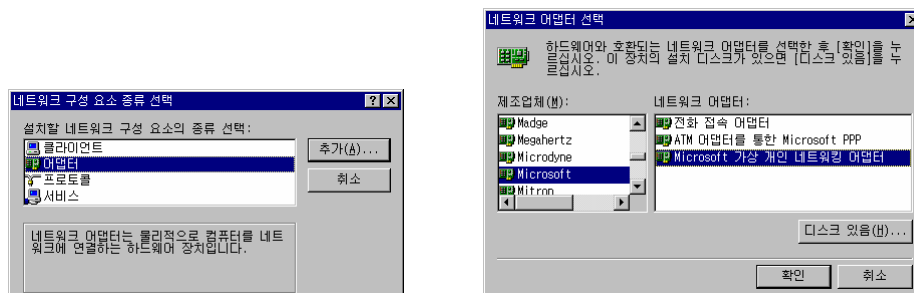
VPN 서버에 접속하여 가상 사설망을 구축하기 위해서는 먼저 가상 사설망 어댑터를 설치합니다. 가상 사설망 어댑터는 윈도우 운영 체제에서 제공됩니다. 가상 사설망 이용을 위해서는 다음 (1) 의 설정을 진행하여야 하며 한번 설정이 완료된 이후에는 (2) 접속 방법을 통하여 연결하면 된다.

(1) 가상 사설망 어댑터 설치

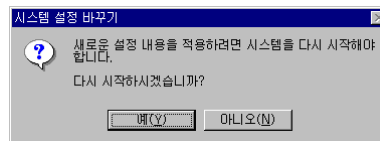
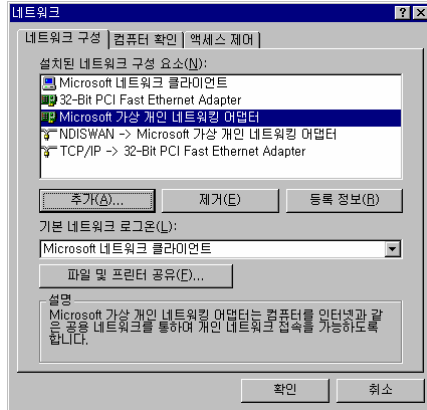
- 윈도우 바탕 화면의 네트워크 환경을 마우스 우측 버튼으로 클릭한 뒤 "등록 정보"를 선택합니다.
- VPN 어댑터 추가를 위하여 추가 버튼을 클릭합니다.



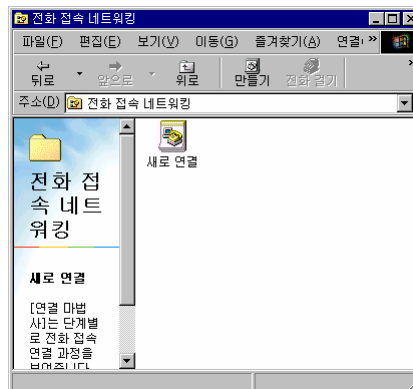
- 네트워크 구성 요소 중 어댑터를 선택한 뒤 추가 버튼을 클릭하여 Microsoft의 VPN 어댑터를 선택합니다.



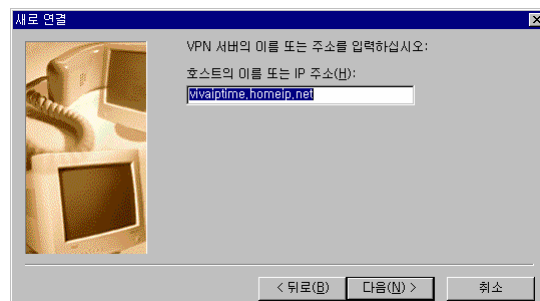
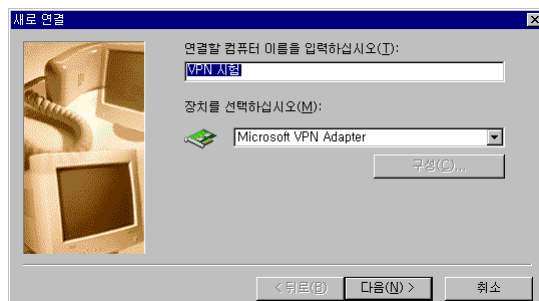
- 확인을 선택하면 가상 개인 네트워킹 어댑터가 추가된 것을 확인할 수 있고 확인을 클릭하면 시스템이 재 시작됩니다.



- 시스템이 재 시작된 뒤 바탕 화면의 내 컴퓨터를 더블 클릭하고 이 중 전화 접속 네트워킹을 클릭합니다.

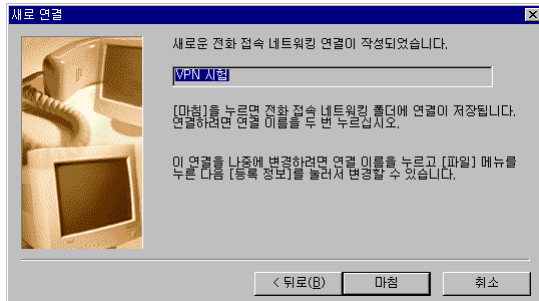


- 새로 연결을 구성하고자 하는 VPN망의 이름과 VPN 서버의 주소를 입력합니다.



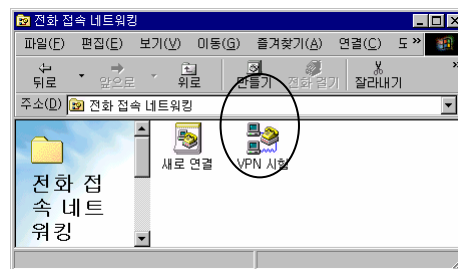
[참고] VPN 망 이름은 임의로 자유롭게 입력할 수 있으면 DDNS를 사용하면 DNS 이름으로 공유기에 접근할 수 있어 편리합니다.

- 마침을 클릭하여 VPN 구성을 완료 합니다.

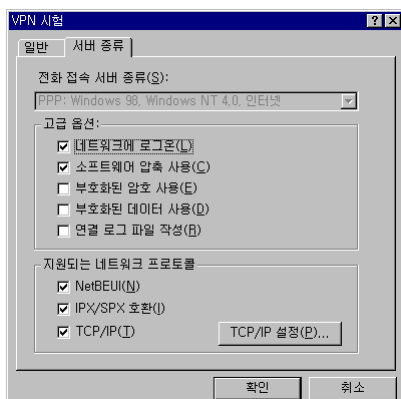


(2) 가상 사설망 어댑터의 옵션 조절

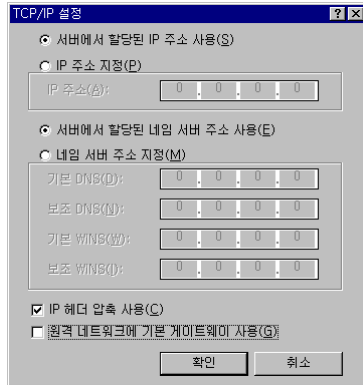
- 바탕 화면의 내 컴퓨터를 더블 클릭하고 이 중 전화 접속 네트워킹을 마우스 우측 버튼으로 클릭하여 등록 정보를 선택합니다.



- 서버 종류 항목을 선택하여 암호와 관련 옵션을 조정한다. 공유기 설정에서 암호화 (MPPE)를 사용하는 것으로 설정하였다면, “무호화된 데이터 사용”에 체크합니다.



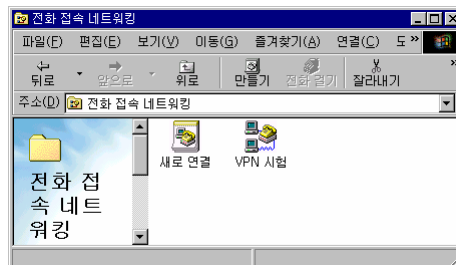
- TCP/IP 설정을 선택하여 원격네트워크 기본 게이트웨이 사용이 체크되지 않도록 합니다.



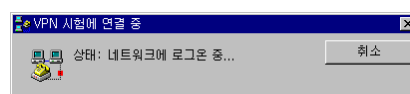
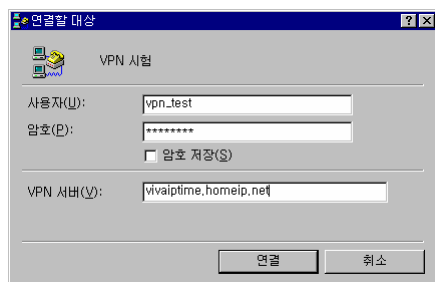
- 확인을 클릭하여 등록 정보 수정을 완료합니다.

(2) VPN 접속

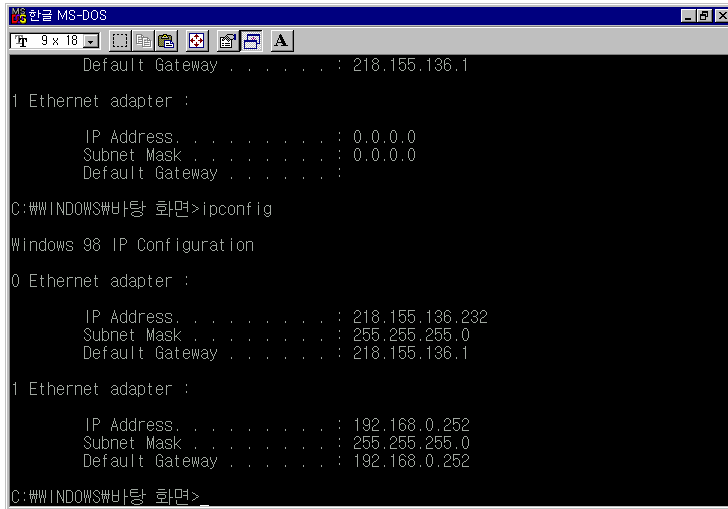
- VPN 접속을 위해서 바탕 화면의 내 컴퓨터를 더블 클릭하고 이 중 전화 접속 네트워킹을 클릭합니다.



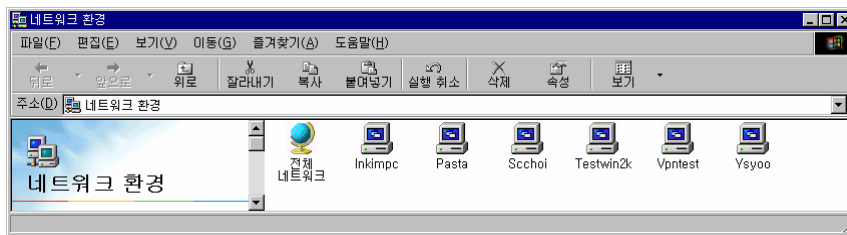
- 새로 생성된 VPN 접속 아이콘을 클릭하여 VPN 사용자 계정과 암호를 입력하면 VPN 접속이 완료됩니다.



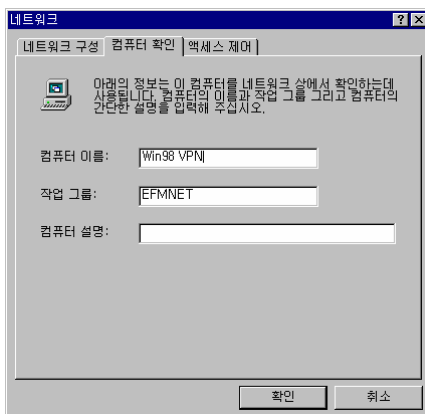
□ VPN 접속 상태는 명령 프롬프트의 ipconfig 명령으로 확인할 수 있습니다.



□ 네트워크 환경을 검색하면 가상 사설망 LAN으로 연결된 PC를 확인할 수도 있습니다.



[참고] VPN 접속 시 LAN 상의 모든 자원을 자유롭게 공유하기 위해서는 네트워크 환경에서 작업 그룹을 연결하고자 하는 VPN 망의 작업 그룹과 동일하게 설정하여야 합니다.

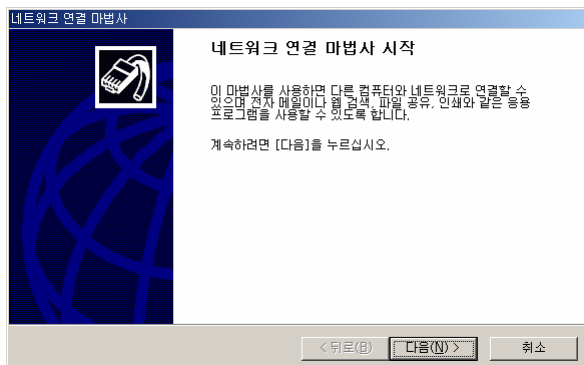


12.4 Windows 2000에서의 VPN 서버 접속

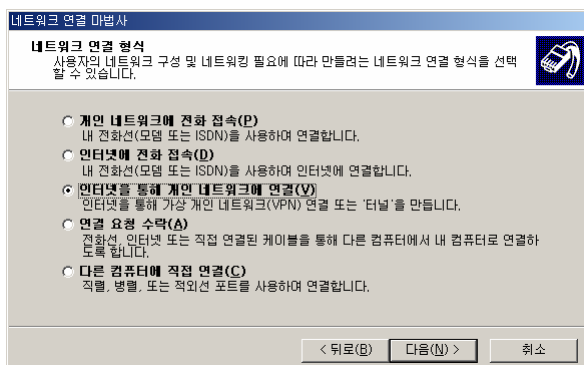
VPN 서버에 접속하여 가상 사설망을 구축하기 위해서는 먼저 가상 사설망 어댑터를 설치합니다. 가상 사설망 어댑터는 윈도우 운영 체제에서 제공됩니다. Windows 2000 운영 체제에서 가상 사설망 이용을 위해서는 다음 (1) ~ (3)까지의 설정을 진행하여야 하며 한번 설정이 완료된 이후에는 (4) 접속 방법을 통하여 연결합니다.

(1) 가상 사설망 어댑터 설치

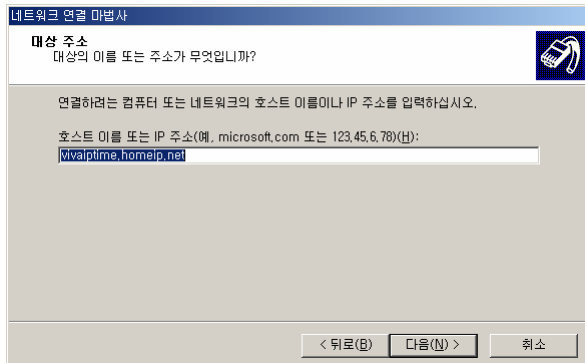
- 윈도우 시작 버튼을 클릭하여 **설정**>>**네트워크 및 전화 접속 연결**>>**새 연결 만들기**를 선택한 후 네트워크 연결 마법사가 실행되면 다음을 클릭합니다.



- 네트워크 연결 형식은 VPN을 선택한 후 다음을 클릭합니다.

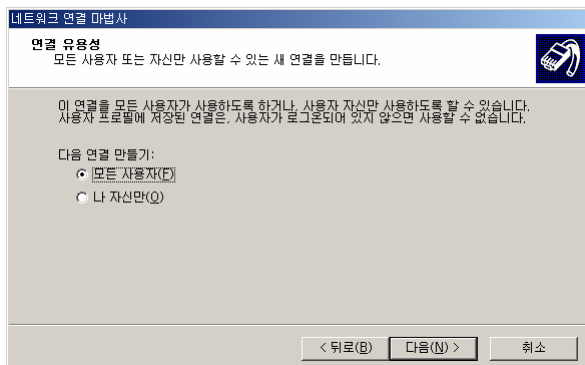


- 연결하고자 하는 VPN 서버 (공유기)의 주소를 입력한 후 다음을 클릭합니다.



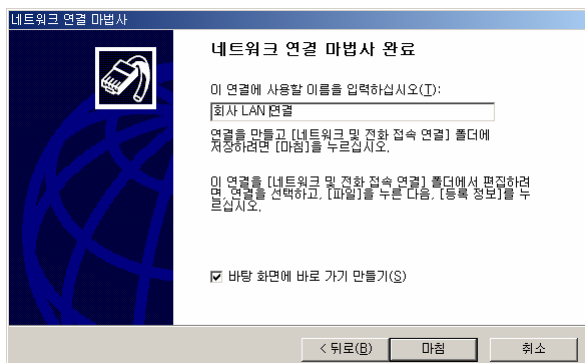
- [참고] DDNS를 사용하면 DNS 이름으로 공유기에 접근할 수 있어 편리합니다.

- 설치된 가상 사설망 어댑터를 사용할 수 있는 사용자를 선택한 후 다음을 클릭합니다.



- [참고] 별도의 사용자 관리를 하지 않는 경우 모든 사용자를 선택합니다.

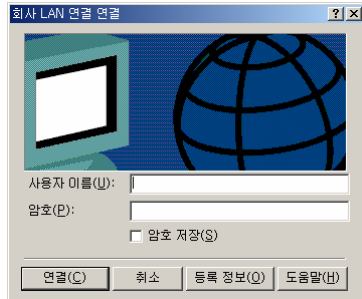
- 설치된 가상 사설망의 이름을 입력하고 확인을 클릭하면 어댑터 설치가 완료됩니다.



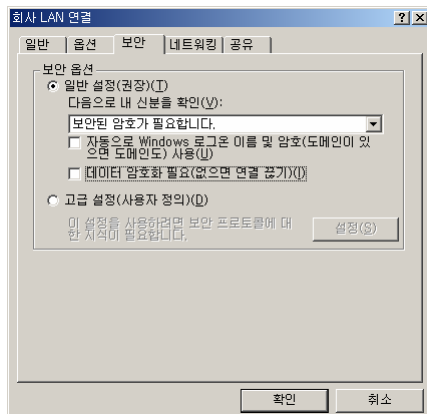
- [참고] 사설망의 이름은 임의로 입력하면 되며 하단의 단축 아이콘 생성 옵션을 선택하면 바탕 화면에 가상 사설망 접속 아이콘이 생성됩니다.

(2) 가상 사설 망 어댑터의 옵션 조정

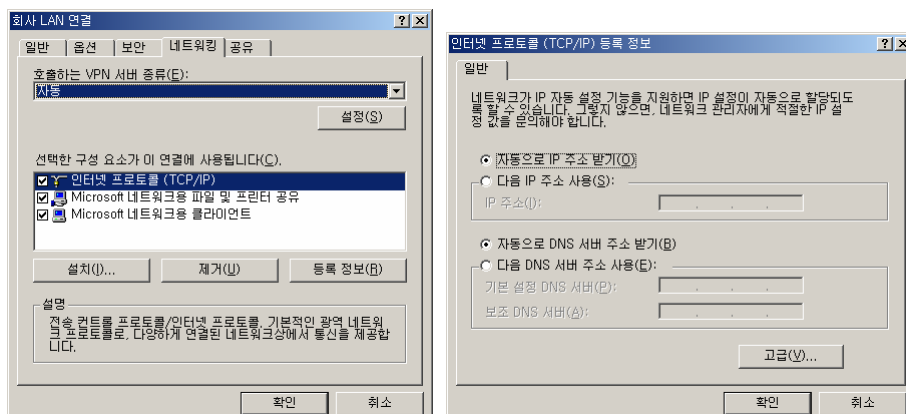
- 가상 사설망 어댑터 접속 프로그램이 실행되면 등록 정보 버튼을 클릭합니다.



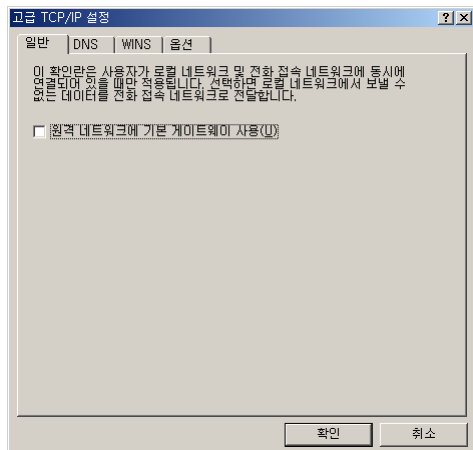
- 보안 항목을 설정하며 "데이터 암호화 필요"의 체크 상태를 확인합니다. 만약, 공유기의 설정에서 암호화 (MPPE)를 사용하는 것으로 설정하였다면, "데이터 암호화필요"에 체크를 하셔야 됩니다.



- 네트워크 항목 중 TCP/IP 항목을 더블 클릭합니다.



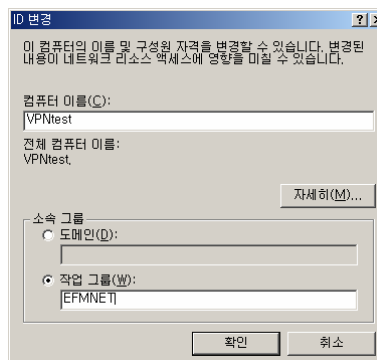
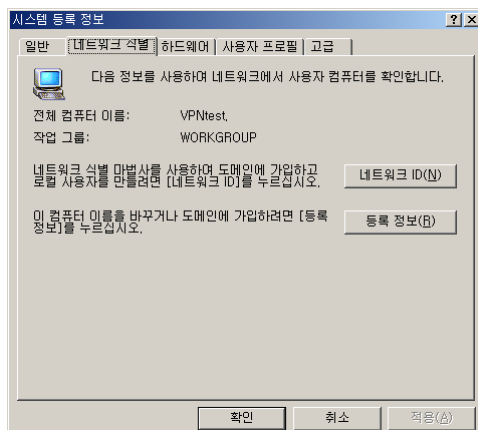
- 고급 버튼을 클릭하여 원격 네트워크에 기본 게이트웨이 사용에 체크가 해제되었는지 확인합니다.



- 암호화 설정과 원격 게이트웨이에 대한 설정을 확인한 뒤 확인 버튼을 클릭하여 등록 정보 창을 닫습니다.

(3) 워크 그룹 이름의 확인

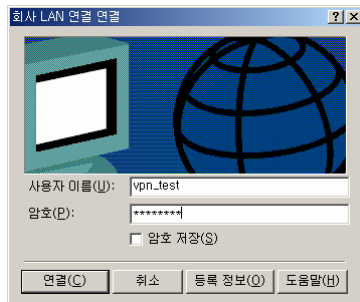
- VPN 서버에 접속한 뒤 정상적인 윈도우 공유 시스템을 위해서는 LAN 환경에 PC 및 가상 사설망으로 접속하는 모든 PC는 동일한 워크 그룹 이름을 갖고 있어야 합니다.
- 컴퓨터의 워크 그룹 이름 변경을 위하여 바탕 화면의 내 컴퓨터를 마우스 우측 버튼으로 클릭한 뒤 등록 정보를 클릭하고 네트워크 식별 항목을 선택하고 등록 정보 버튼을 클릭합니다.
- 작업 그룹 이름을 가상 사설망으로 연결하고자 하는 LAN의 그룹 이름과 동일하게 수정합니다.



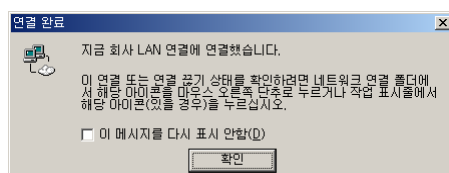
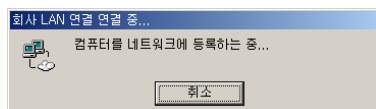
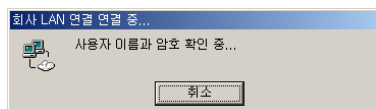
[참고] 워크 그룹 이름이 다른 경우 윈도우 환경에서 공유가 정상적으로 수행되지 않습니다.

(4) VPN 접속

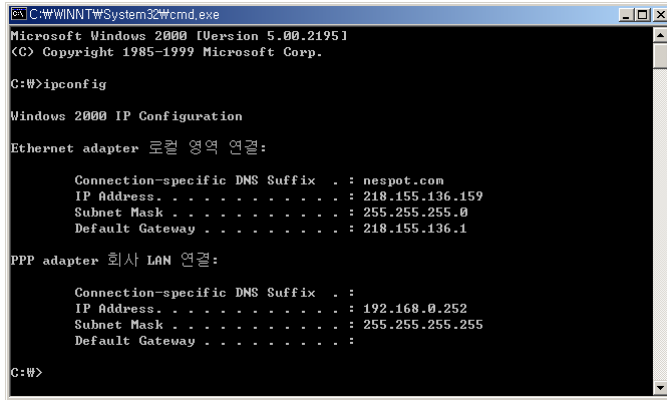
- 바탕 화면의 단축 아이콘 또는 네트워크 등록 정보의 가상 사설망 어댑터 아이콘을 클릭합니다.
- 가상 사설 망 연결 프로그램이 실행되면 등록된 사용자 이름과 암호를 입력한 뒤 연결을 클릭합니다.



- VPN 서버와 정상으로 접속되는 경우 아래와 같은 메시지가 표시됩니다.



- VPN 접속 상태는 명령 프롬프트의 ipconfig 명령으로 확인할 수 있습니다.



```

C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\W>ipconfig

Windows 2000 IP Configuration

Ethernet adapter 로컬 영역 연결:

    Connection-specific DNS Suffix  . : nespot.com
    IP Address. . . . . : 218.155.136.159
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 218.155.136.1

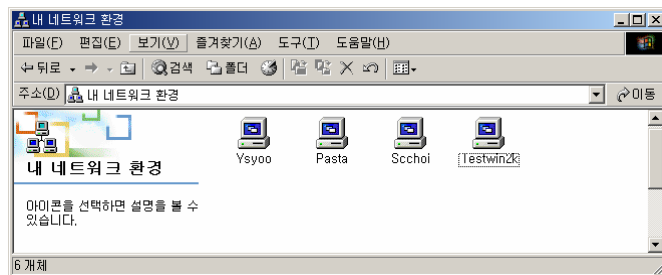
PPP adapter 회사 LAN 연결:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 192.168.0.252
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . :

C:\W>

```

- 또 네트워크 환경을 검색하면 가상 사설망을 통하여 LAN으로 연결된 PC를 확인할 수도 있습니다.



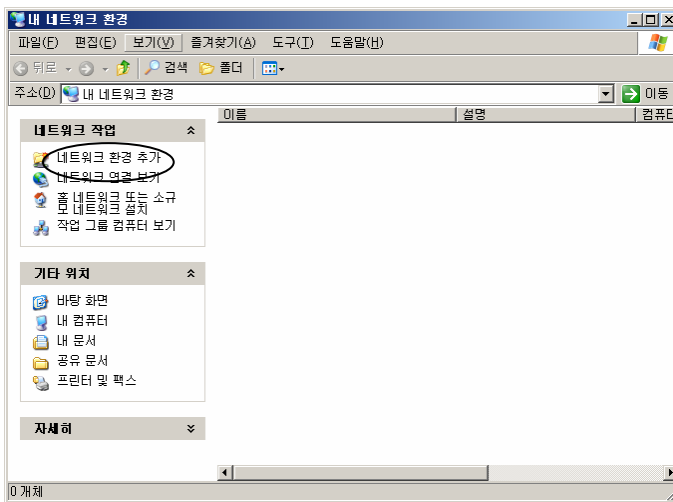
- VPN 서버와 연결이 완료되면 LAN 상의 모든 자원을 자유롭게 공유할 수 있습니다.

12.5 Windows XP에서의 VPN 서버 접속

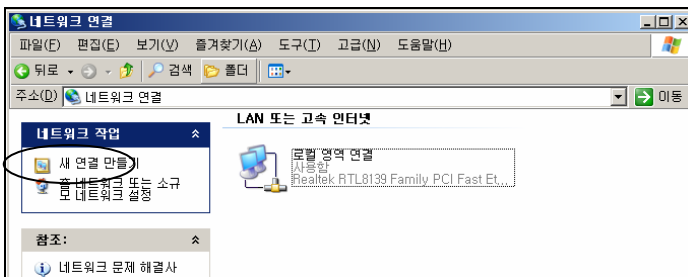
VPN 서버에 접속하여 가상 사설망을 구축하기 위해서는 먼저 가상 사설망 어댑터를 설치합니다. 가상 사설망 어댑터는 윈도우 운영 체제에서 제공됩니다. 가상 사설망 이용을 위해서는 다음 (1) ~ (3)까지의 설정을 진행하여야 하며 한번 설정이 완료된 이후에는 (4) 접속 방법을 통하여 연결합니다.

(1) 가상 사설망 어댑터 설치

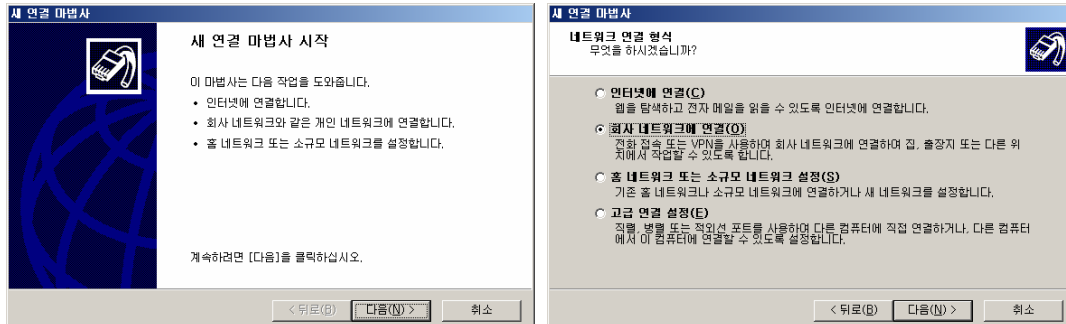
- 윈도우 **[시작]** 버튼을 클릭하여 **[내 네트워크 환경]**을 선택한 뒤 **[네트워크 연결 보기]**를 선택합니다.



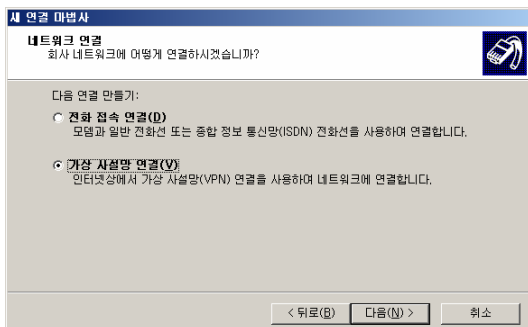
- 새 연결 만들기를 클릭하여 새 연결 마법사를 실행합니다.



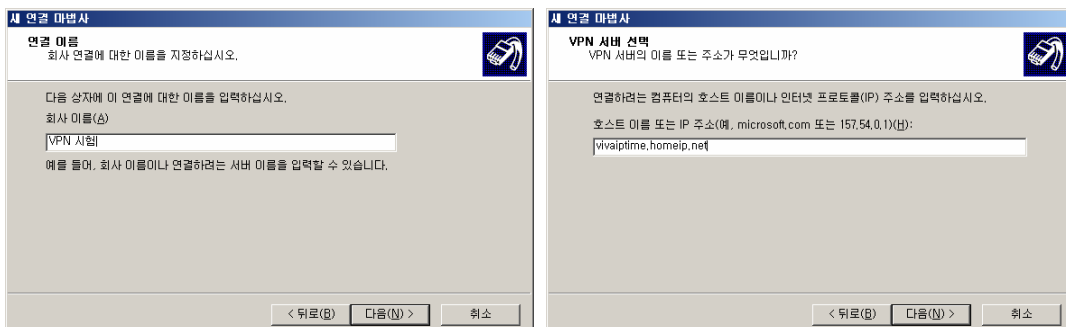
- 네트워크 연결 마법사가 실행되면 다음을 클릭하고 연결 형식에서는 회사 네트워크 연결을 선택합니다.



- 네트워크 연결 방법은 VPN 연결을 선택합니다.

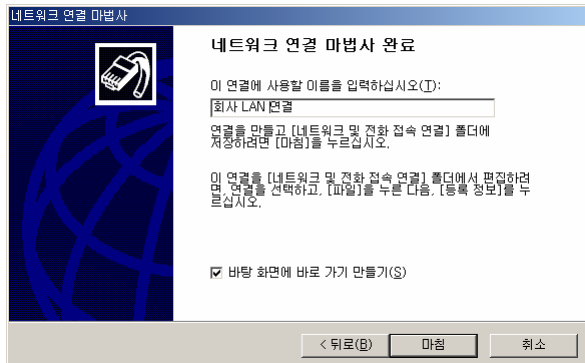


- VPN 망의 이름을 입력한 뒤 접속하고자 하는 VPN 서버 (공유기)의 주소를 입력합니다.



[참고] VPN 망 이름은 임의로 자유롭게 입력할 수 있으면 DDNS를 사용하면 DNS 이름으로 공유기에 접근할 수 있어 편리합니다.

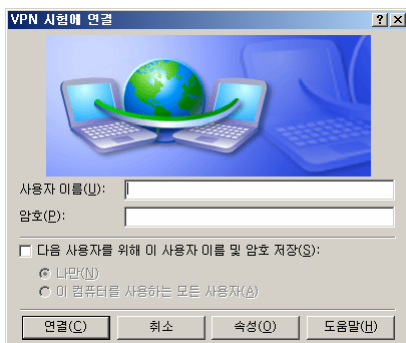
- 마지막으로 마침을 클릭하면 가상 사설망 어댑터 설치가 완료됩니다.



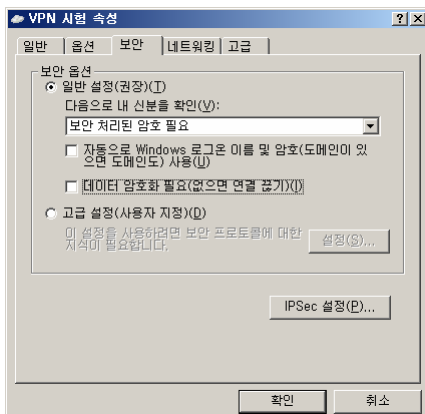
- [참고] 단축 아이콘 생성 옵션을 선택하면 바탕화면에 접속 아이콘이 생성됩니다.

(2) 가상 사설 망 어댑터의 옵션 조정

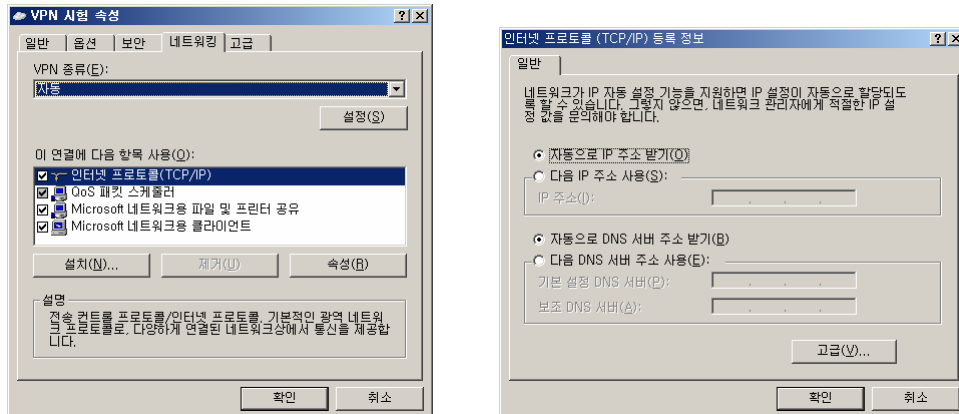
- 가상 사설망 어댑터 접속 프로그램이 실행되면 속성 버튼을 클릭합니다.



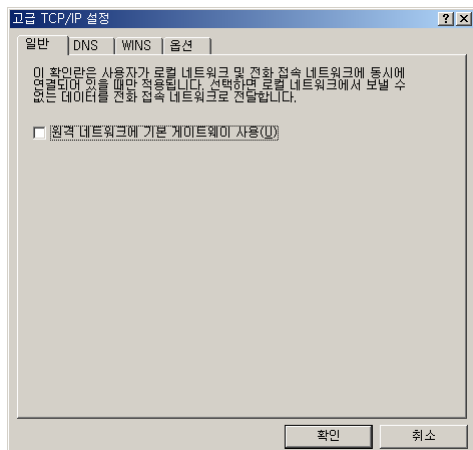
- 보안 항목을 설정하며 "데이터 암호화 필요"의 체크상태를 확인합니다. 공유기의 설정에서 암호화 (MPPE)를 사용하는 것으로 설정하였다면, "데이터 암호화필요"에 체크를 하여야 합니다.



- 네트워크 항목 중 TCP/IP 항목을 더블 클릭합니다.



- 고급 버튼을 클릭하여 원격 네트워크에 기본 게이트웨이 사용에 체크가 해제되었는지 확인합니다.

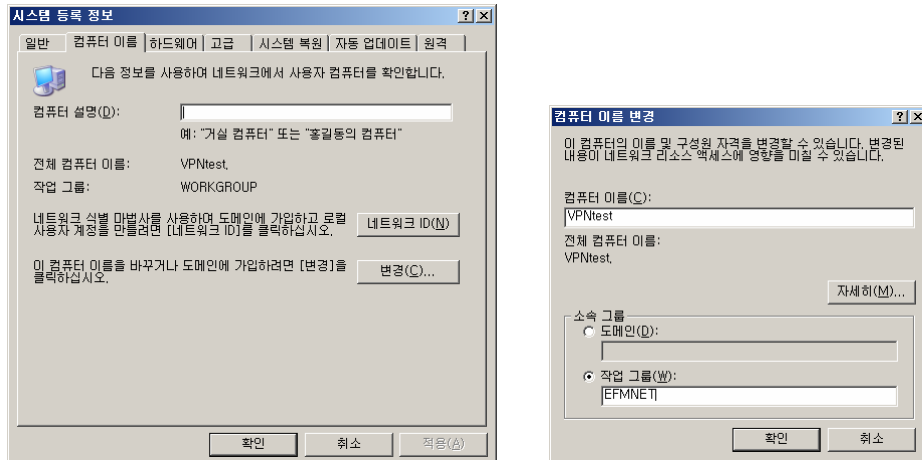


- 암호화 설정과 원격 게이트웨이에 대한 설정을 확인한 뒤 확인 버튼을 클릭하여 등록 정보 창을 닫습니다.

(3) 워크 그룹 이름의 확인

- VPN 서버에 접속한 뒤 정상적인 윈도우 공유 시스템을 위해서는 LAN 환경에 PC 및 가상 사설망으로 접속하는 모든 PC는 동일한 워크 그룹 이름을 갖고 있어야 합니다.
- 컴퓨터의 워크 그룹 이름 변경을 위하여 시작 메뉴의 내 컴퓨터를 마우스 우측 버튼으로 클릭한 뒤 속성을 클릭하고 컴퓨터 이름 항목을 선택하고 변경 버튼을 클릭합니다.

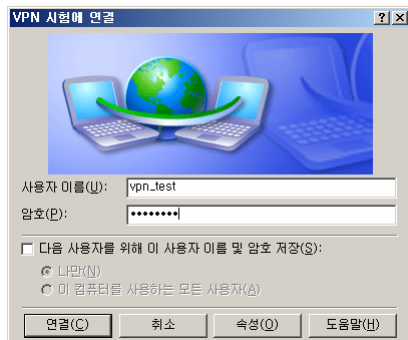
- 작업 그룹 이름을 가상 사설망 LAN의 그룹 이름과 동일하게 합니다.



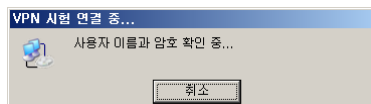
[참고] 워크 그룹 이름이 다른 경우 윈도우 환경에서 공유가 정상적으로 수행되지 않습니다.

(4) VPN 접속

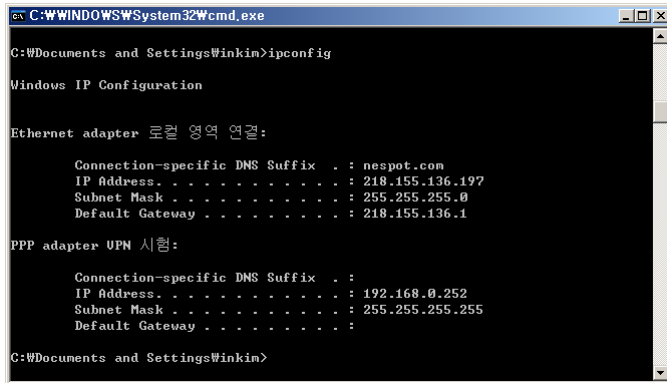
- 바탕 화면의 단축 아이콘 또는 네트워크 등록 정보의 가상 사설망 어댑터 아이콘을 클릭합니다.
- 가상 사설 망 연결 프로그램이 실행되면 등록된 사용자 이름과 암호를 입력한 뒤 연결을 클릭합니다.



- VPN 서버와 정상으로 접속되는 경우 아래와 같은 메시지가 표시됩니다.



- VPN 접속 상태는 명령 프롬프트의 ipconfig 명령으로 확인할 수 있습니다.



```

C:\WINDOWS\System32\cmd.exe
C:\Documents and Settings\inkin>ipconfig

Windows IP Configuration

Ethernet adapter 로컬 영역 연결:

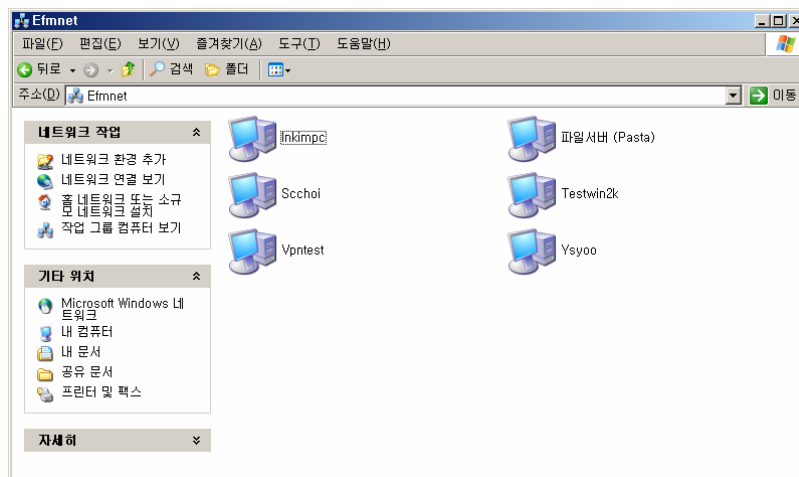
    Connection-specific DNS Suffix  . : nespot.com
    IP Address. . . . . : 218.155.136.197
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 218.155.136.1

PPP adapter UPN 시험:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 192.168.0.252
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . :

C:\Documents and Settings\inkin>
  
```

- 네트워크 환경을 검색하면 가상 사설망을 통하여 LAN으로 연결된 PC를 확인할 수도 있습니다.

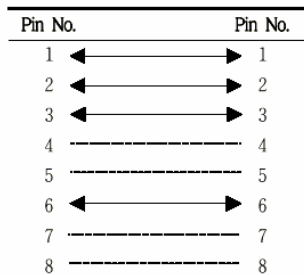
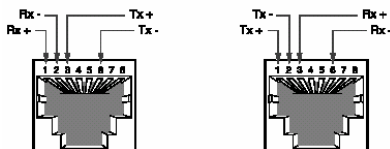
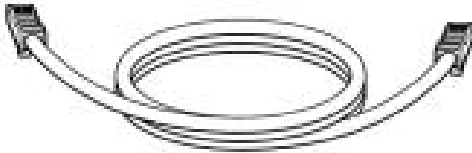


- VPN 서버와 연결이 완료되면 LAN 상의 모든 자원을 자유롭게 공유할 수 있습니다.

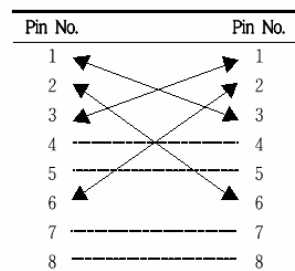
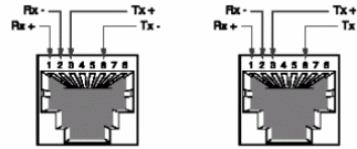
부록 A. LAN Cable 규격

LAN Cable은 스트레이트 케이블(다이렉트 케이블)과 크로스 케이블이 있습니다.

ipTIME X1005에는 케이블 자동 감지 기능이 있어 이 두 가지 케이블 중 어떤 케이블을 사용하여도 됩니다. 그러나 규정에 따라 1-2, 3-6 번 선의 꼬임상이 유지되지 않은 케이블을 사용하면 정상적인 통신이 불가능하므로 꼭 규정에 맞도록 케이블을 제작하시거나 구입하여 사용하시기 바랍니다.



<다이렉트 케이블의 구성>

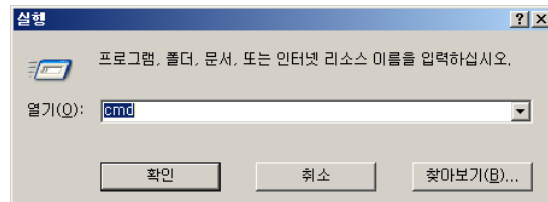
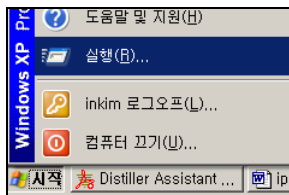


<크로스 케이블의 구성>

부록 B. IP 공유기 Ping 시험

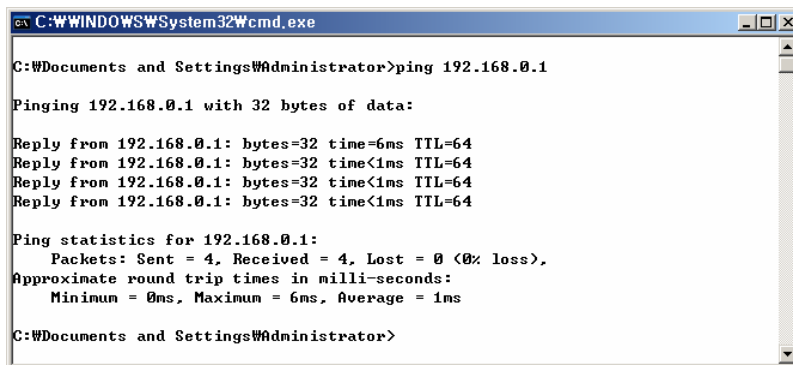
PC가 IP 공유기에 정상 연결되어 있는지 여부는 PC에서 공유기로 Ping 시험을 하면 알 수 있습니다. IP공유기 공유기로 Ping 시험을 하기 전에 PC의 IP 주소가 정상인지를 확인하여야 합니다. PC의 IP 주소 확인은 자동으로 설정한 경우 본 설명서 3장의 내용을 참고하고 수동으로 설정하는 경우 본 설명서 부록 A의 내용을 참고합니다.

- Ping 시험을 하기 위해서는 Win98/ME의 경우 MS-DOS를, Windows 2000/XP의 경우 명령 프롬프트를 실행합니다. 이의 실행을 위하여 윈도우 화면 좌측 하단의 “시작” 버튼을 클릭하고 “실행”을 선택합니다.
- 열기 윈도우에서 98/ME의 경우 “command”를 2000/XP의 경우 “cmd”를 입력하고 확인 버튼을 클릭하여 MS-DOS 또는 명령프롬프트를 실행합니다.



<command 또는 cmd 실행>

- MS-DOS 또는 명령프롬프트 윈도우에서 “ping 192.168.0.1” 명령을 입력합니다.



<Ping 192.168.0.1 명령 실행과 그 결과>

위의 그림과 같이 “Reply from....” 4개 메시지가 확인되면 IP 공유기와 PC가 정상적으로 연결되어 있어 통신에 문제가 없는 것을 확인할 수 있습니다.

부록 C. 제품 사양

제품 사양

항목	사양
제품 규격	크기 : 184 x 130 x 27 (mm) 무게 : 1300g
동작 온도	0 ~ 50도
전원	제공되는 정격 어댑터
인터페이스	WAN x 2 : 100Base-TX LAN x 5 : 100Base-TX

MIC 인증

A급 기기 (업무용 정보 통신 기기)

이 기기는 업무용으로 전자기파 적합 등록을 한 기기이니 판매자 또는 사용자는 이점을 주의 하시기 바랍니다.

부록 D. 인터넷이 끊겼을 때의 확인사항

1. 외장형 모뎀의 상태를 확인합니다.

- 케이블, VDSL, ADSL 모뎀의 Link 램프가 들어와 있는지 확인합니다.

2. ipTIME X1005의 LED를 상태를 확인합니다.

- CPU 램프가 약 1초 간격으로 천천히 깜박거리는지 확인합니다.
(CPU 램프가 계속 꺼져 있거나, 켜져 있으면 공유기의 전원을 껐다 켜봅니다.)
- WAN의 램프가 들어와 있는지 확인합니다.
- LAN 1,2,3,4,5 번 포트 중 PC가 연결된 포트의 램프가 들어와 있는지 확인합니다.

3. PC의 IP 주소를 확인합니다.

- Windows 98/ME 의 경우는 [시작 -> 실행]에서 [winipcfg] 명령을 입력해서 [IP 주소] 창이 나오면 [IP 주소]를 확인합니다.
- Windows 2000/XP의 경우는 [명령프롬프트]를 실행시킨 후, [ipconfig] 명령을 입력하여 [IP address]를 확인합니다.

4. IP 주소가 정상적이지 않을 때는 - PC의 IP 주소를 수동으로 설정합니다.

IP주소가 정상적인 주소일 때는 - 5번 항목으로 이동합니다.

- Windows 95/98/ME의 경우
 - ① [시작 -> 제어판 -> 네트워크]를 실행하여, 랜카드에 대한 [TCP/IP]의 등록정보를 클릭합니다.
 - ② [할당된 IP 주소 사용]에 체크를 하고, [IP 주소]는 [192.168.0.100]으로 입력하고, [서브네트 마스크]는 [255.255.255.0]으로 입력합니다.
 - ③ [게이트웨이]를 선택한 후 [새 게이트웨이]에 [192.168.0.1]을 입력하고, [추가] 버튼을 클릭합니다.
 - ④ [DNS 구성]을 선택한 후 [DNS 사용]을 체크 하고, [호스트]에는 임의의 이름을 입력하고, [찾을 DNS 서버 주소]에는 한국 통신의 경우 [168.126.63.1]을 하나로 통신의 경우 [210.220.163.82]를 입력하고, [추가] 버튼을 클릭합니다.
(타 통신 업체의 경우는 [168.126.63.1]로 입력합니다.)
 - ⑤ [확인] 버튼을 클릭하고, [네트워크 등록 정보] 창도 [확인] 버튼을 클릭하여 [시스템 설정 바꾸기] 창이 나오면 [확인]을 클릭하여 PC를 재 부팅 합니다.

- Windows 2000의 경우

- ① [시작 -> 제어판 -> 네트워크 및 전화 접속 연결]을 실행하여, [로컬 영역 연결] 을 더블클릭 하고, [등록정보]를 클릭합니다. 구성 요소 중 [인터넷 프로토콜(TCP/IP)]의 등록정보를 클릭합니다.
- ② [다음 IP 주소 사용]을 클릭합니다.
- ③ [IP 주소]는 [192.168.0.100]으로 입력하고, [서브네트 마스크]는 [255.255.255.0]으로 입력하고, [기본 게이트웨이]는 [192.168.0.1]로 입력합니다.
- ④ [다음 DNS 서버 주소 사용]을 클릭합니다.
- ⑤ [기본 설정 DNS 서버]에는 한국 통신의 경우 [168.126.63.1], 하나로 통신의 경우 [210.220.163.82]를 입력하고, [보조 DNS 서버]에는 한국 통신의 경우 [168.126.63.2], 하나로 통신의 경우 [210.94.0.7]을 입력합니다.
- ⑥ [확인] 버튼을 클릭합니다. [로컬영역 연결 등록정보] 창도 [확인]을 클릭합니다.

- Windows XP 경우

- ① [시작 -> 제어판 -> 네트워크 및 인터넷 연결]을 실행하여, [로컬영역 연결] 을 더블클릭 하고, [속성]를 클릭합니다. 구성 요소 중 [인터넷 프로토콜(TCP/IP)]의 등록정보를 클릭합니다.
- ② [다음 IP 주소 사용]을 클릭합니다.
- ③ [IP 주소]는 [192.168.0.100]으로 입력하고, [서브네트 마스크]는 [255.255.255.0]으로 입력하고, [기본 게이트웨이]는 [192.168.0.1]로 입력합니다. [22 페이지 둘째 그림 참조]
- ④ [다음 DNS 서버 주소 사용]을 클릭합니다.
- ⑤ [기본 설정 DNS 서버]에는 한국 통신의 경우 [168.126.63.1], 하나로 통신의 경우 [210.220.163.82]를 입력하고, [보조 DNS 서버]에는 한국통신의 경우 [168.126.63.2], 하나로 통신의 경우 [210.94.0.7]을 입력합니다.
(타 통신 업체의 경우는 [168.126.63.1], [168.126.63.2]로 입력합니다.)
- ⑥ [확인] 버튼을 클릭합니다. [로컬영역 연결 속성] 창도 [확인]을 클릭합니다.

5. [한글 MS-DOS] 또는 [명령프롬프트]를 실행시킨 후 [192.168.0.1]로 ping 테스트를 합니다. [ping 192.168.0.1] 명령을 실행하였을 때,
[Reply from 192.168.0.1: bytes=32 time=1ms TTL=64] 의 메시지가 나와야 합니다.
Ping 테스트가 정상적으로 나오지 않으시면 고객센터로 문의하시기 바랍니다.

6. Internet Explorer를 실행하여 ipTIME X1005 의 웹 설정 화면에 로그인 한 뒤 공유기 설정 화면의 인터넷 연결 상태를 확인해봅니다.

7. 외장형 모뎀과 ipTIME X1005의 전원을 껐다 켜봅니다.

8. 계속 인터넷이 연결되지 않는다면 ipTIME X1005를 제거하신 후 외장형 모뎀에 PC를 직접 연결하여 인터넷이 되는지 확인 합니다.

9. 위의 내용을 모두 진행하신 후에도 문제 해결이 되지 않는다면 고객센터로 문의하여 주시기 바랍니다.

고객지원실 운영 안내

고객지원실 전화 번호 : 070-7018-1199

인터넷 고객센터 : <http://www.iptime.co.kr>

평일 : 10:00 ~ 22:00 전화 및 인터넷 게시판 상담

토요일 : 10:00 ~ 13:00 인터넷 게시판 상담만 운영

공휴일 : 휴무

부록 E. 제품 보증서 및 고객 지원

제품 보증서

제품명 : 인터넷 공유기

모델명 : ipTIME X1005

본 제품은 구입일로부터 2년간 품질을 보증하며 보상 규정은 아래와 같습니다.

보증 규약 내용

1. AS 보증 대상 기기 : ipTIME X1005
2. AS 보증 기간 : 구입일로부터 2년간 (구입일 미확인 시 제조일로부터 27개월)
3. 무상 서비스
 - AS 보증 기간 내 제품의 하자 발생 시
4. 유상 서비스
 - AS 보증 기간이 경과된 제품의 하자 발생 시
 - 화재, 수재, 낙뢰 등의 천재 지변으로 인한 고장 발생 시
 - 임의 개조 또는 수리 등에 의한 하자 발생 시
 - 기타 소비자 과실에 의한 제품 하자 발생 시
5. AS 운송 처리
 - 당사에 직접 입고 원칙
 - 무상 AS 기간내 제품 입고 비용은 사용자 부담, 출고 비용은 당사 부담
 - 무상 AS 기간 이후의 제품 운송 비용은 입출고 모두 사용자 부담
 - 하자가 없는 제품의 입출고 비용은 모두 사용자 부담

(주)이에프엠네트웍스 (직인 생략)

고객지원실 운영 안내

고객지원실 전화 번호 : 070-7018-1199

인터넷 고객지원실 : <http://www.iptime.co.kr>

평일 : 10:00 ~ 22:00 전화 및 인터넷 게시판 상담

토요일 : 10:00 ~ 13:00 인터넷 게시판 상담만 운영

공휴일 : 휴무