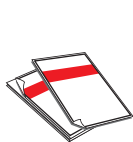


제품 구성물



제품 구성물 및 보증서

제품을 개봉하신 후 제품 구성물 및 보증서에 따라
제품 내용을 확인하여 주시기 바랍니다. (본 설명서)



사용설명서

IP 공유기 설정과 관리를 위한 Net-OS 사용설명 책자입니다.

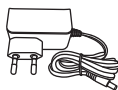
※ 설치하시기 전에 구성물이 아래와 같이 모두 있는지 확인하여 주시기 바랍니다.
※ 구성물의 모양이 아래 그림과 다를 수 있습니다.



〈 본체 〉



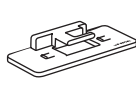
〈 제품구성물 및 보증서 /
사용설명서 〉



〈 어댑터 〉

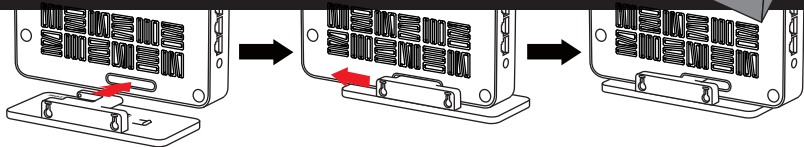


〈 랜선 〉



〈 크래들 〉

■ 크래들 결합 순서도



[제품 보증서 및 고객 지원]

제품 보증서

제품명 : 네트워크 공유기

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

보증 규약 내용

1. AS 보증 대상 기기 : ipTIME x6003
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)에프엠네트웍스 (직인 생략)

고객지원실 전화 번호 : 1544-8695
인터넷 고객지원실 : <http://www.ipitime.com>
휴무일 : 공휴일 / 토요일 / 일요일

[주의] 해당무선설비는 운용 중 전파혼신 가능성이 있으므로, 인명과 관련된 서비스는 할 수 없음. 이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 업무용 방송통신 기자재로 사용하는 것을 목적으로 합니다.

ipTIME 2WAN 설명서

문의 사항 및 고객 지원

Tel. 1544-8695
<http://www.iptime.com>

(주) 이에프엠네트웍스

사용자 설명서 보는 방법

- 설명서 1~3장은 공유기와 PC를 연결하는 방법, 공유기에 인터넷을 연결하는 방법이 기술되어 있습니다.
- 4장 ~ 10장은 ipTIME의 모든 기능을 설명하는 설명서입니다. 제품 사용시 필요한 기능에 해당하는 부분의 사용법을 참고하시기 바랍니다.

목차

1장 PC 환경 설정	6
1.1 윈도우 XP 설정	6
1.2 윈도우 VISTA 설정	9
1.3 윈도우 7 설정	14
1.3 윈도우 8.1 설정	19
2장 웹 설정 화면 이용하기	24
2.1 ipTIME 웹 서버 접속	24
2.2 도움말 기능	25
2.3 설정 저장 기능	26
3장 설정 마법사로 인터넷 연결	27
3.1 ipTIME 웹 서버 접속	28
3.2 ipTIME 설정 마법사 실행	29
3.3 자동 검색에 의한 PPPoE 연결 예	31
3.4 자동 검색에 의한 동적 IP 연결 예	34
3.5 수동 설정을 이용한 인터넷 연결 설정	37
4장 기본설정	43
4.1 시스템 요약 정보	43
4.2 인터넷 연결 설정	44
4.3 펌웨어 업그레이드	47

5장 네트워크 관리	50
5.1 인터넷 연결 정보	50
5.2 내부 네트워크 정보	51
5.3 인터넷 연결 설정	51
5.4 내부 네트워크 설정	52
6장 NAT/라우터 관리	55
6.1 포트포워드 설정	55
6.2 DMZ/Twin IP 설정	56
6.3 포트트리거 설정	58
6.4 기타기능 설정	59
6.5 라우팅 테이블 관리	60
7장 보안기능	61
7.1 인터넷 사용제한	61
7.2 네트워크 감시	64
7.3 공유기 접속 관리	67
7.4 기타 보안 설정	68
8장 특수기능	70
8.1 VPN 서버설정	70
8.2 DDNS 설정	85
8.3 WOL 기능	86
8.4 호스트검색	87
8.5 공지/광고 기능	89

9장 트래픽관리	90
9.1 분산정책 기본설정	90
9.2 분산정책 고급설정	93
9.3 QoS 설정	95
9.4 컨넥션 정보	98
9.5 컨넥션 검색	99
9.6 컨넥션 제어	102
9.7 링크설정/정보	103
10장 시스템관리	104
10.1 시스템 로그	104
10.2 관리자 설정	105
10.3 펌웨어 업그레이드	105
10.4 시스템 시간 설정	106
10.5 설정 백업/복구	106
10.6 기타 설정	107
부록 A. LAN Cable 규격	109
부록 B. IP 공유기 Ping 시험	110

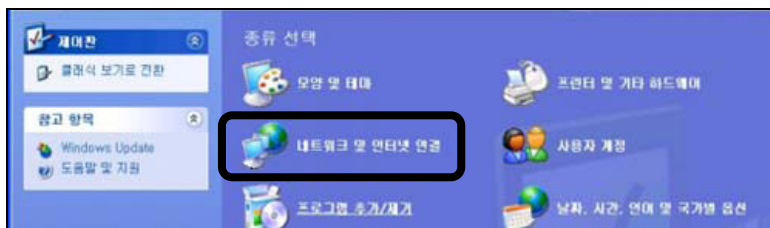
1장 PC 환경 설정

1.1 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 ipTIME에서 자동으로 IP 주소를 부여 받는지 확인하기 위해서는 윈도우를 설정하기 전에 PC와 ipTIME을 LAN 케이블로 연결하고 ipTIME을 켜두어야 합니다.

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



<네트워크 및 인터넷 연결 클릭>

- 네트워크 및 인터넷 연결에서 **네트워크 연결** 아이콘을 클릭합니다.



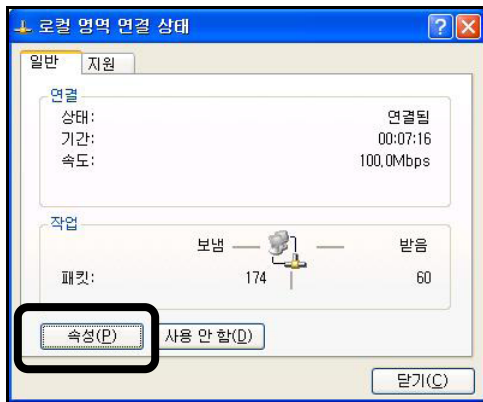
<네트워크 연결 클릭>

- 네트워크 연결에서 **로컬 영역 연결**을 더블 클릭하여 선택합니다.



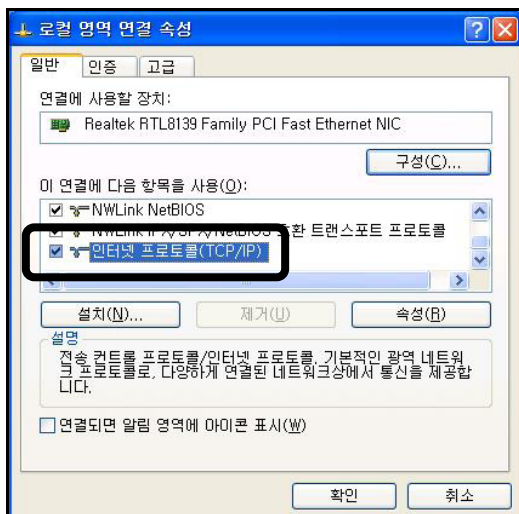
<로컬 영역 연결 클릭>

- 로컬 영역 연결 상태에서 **속성**을 클릭하여 선택합니다.

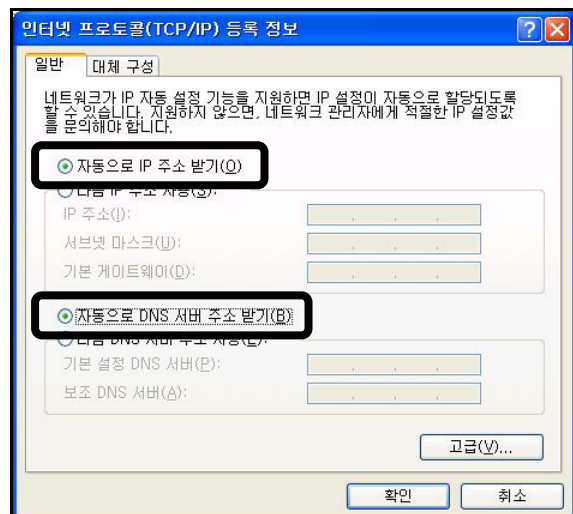


<속성 클릭>

- **인터넷 프로토콜 (TCP/IP)**를 더블 클릭하여 선택하고, **자동으로 IP 주소 받기(O)**와 **자동으로 DNS 서버 주소 받기(B)**를 선택합니다.



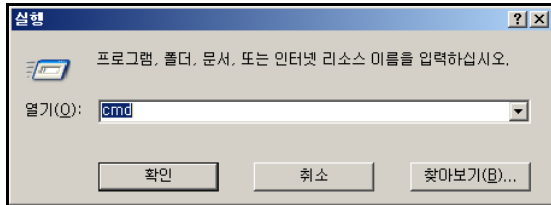
<TCP/IP 더블 클릭>



<자동 선택 후 확인 클릭>

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

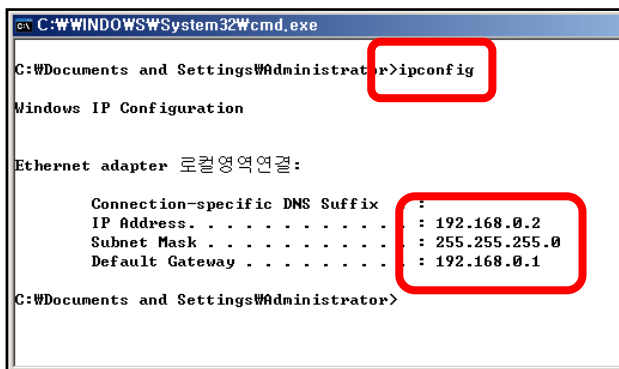
- IP 주소 자동 할당 확인은 명령 프롬프트의 **ipconfig** 명령으로 확인할 수 있습니다.
- 명령 프롬프트는 윈도우 화면 좌측 하단의 **[시작]** 버튼을 클릭한 뒤 **[실행]**을 선택하여 열기에 그림과 같이 “cmd”를 입력하고 확인 버튼을 클릭하면 실행됩니다.



<cmd 실행>

- 명령 프롬프트가 실행되면 아래 그림과 같이 “ipconfig” 명령을 입력하여 PC에 자동 할당 된 IP 주소, 서브네트마스크, 게이트웨이 등을 확인합니다.

[참고] ipTIME에 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 ipTIME사이의 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.com>)를 참고하여 IP 주소 수동 설정 방법으로 IP 주소를 설정하거나 ipTIME 고객센터(1544-8695)에 문의하시기 바랍니다.

PC 설정을 완료한 뒤 인터넷을 사용하기 위해서는 3장의 내용을 참고하여 설정합니다.

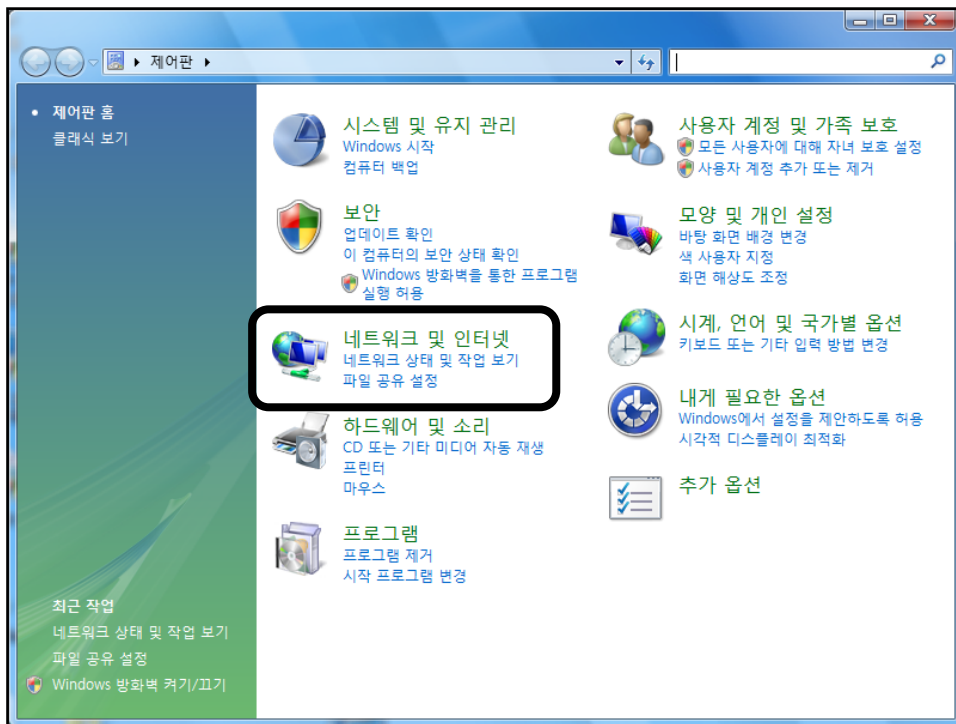
인터넷 연결 설정은 ipTIME에서 이루어지는 것이므로 모든 PC에서 설정할 필요는 없으며 한번만 설정하면 됩니다.

1.2 윈도우 VISTA 설정

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

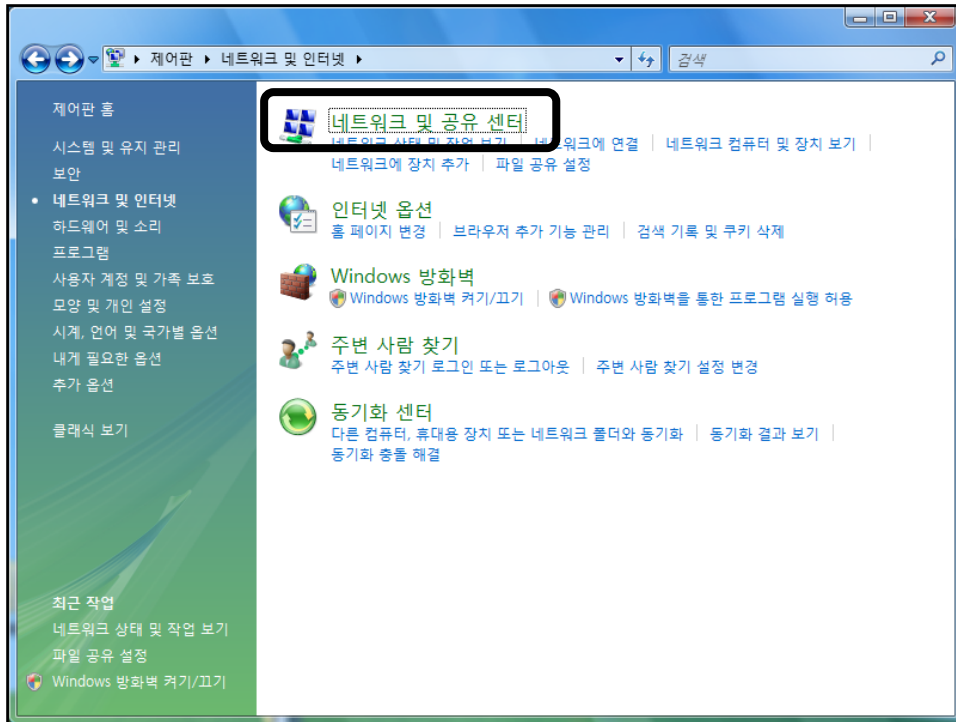
PC의 TCP/IP 설정이 완료된 후 ipTIME에서 자동으로 IP 주소를 부여 받는지 확인하기 위해서는 윈도우를 설정하기 전에 PC와 ipTIME을 LAN 케이블로 연결하고 ipTIME을 켜두어야 합니다.

- 윈도우 좌측 하단의 **윈도우 아이콘** 버튼을 클릭한 후 메뉴에서 **제어판**을 선택합니다.
- 제어판의 **네트워크 및 인터넷** 아이콘을 클릭합니다.



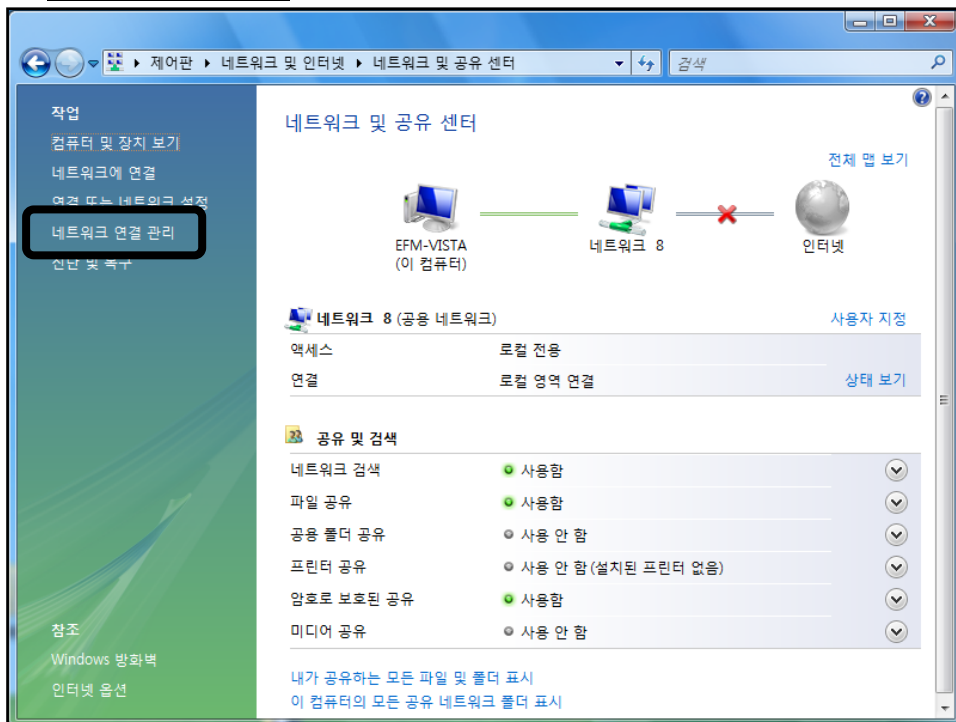
<네트워크 및 인터넷 클릭>

- 네트워크 및 인터넷 연결에서 **네트워크 및 공유 센터** 아이콘을 클릭합니다.



<네트워크 및 공유 센터 클릭>

- **네트워크 연결 관리**를 클릭합니다.



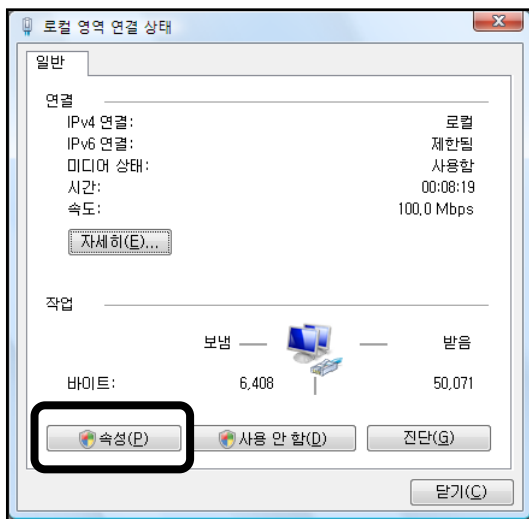
<네트워크 연결 관리 클릭>

- 네트워크 연결에서 **로컬 영역 연결**을 더블 클릭하여 선택합니다.



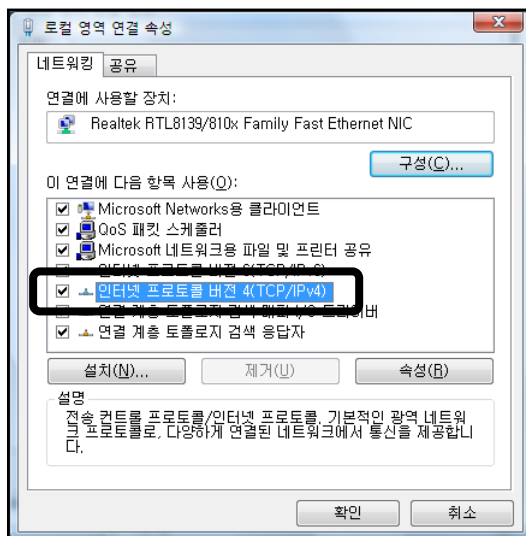
<로컬 영역 연결 더블 클릭>

- 로컬 영역 연결 상태에서 **속성**을 클릭하여 선택합니다.

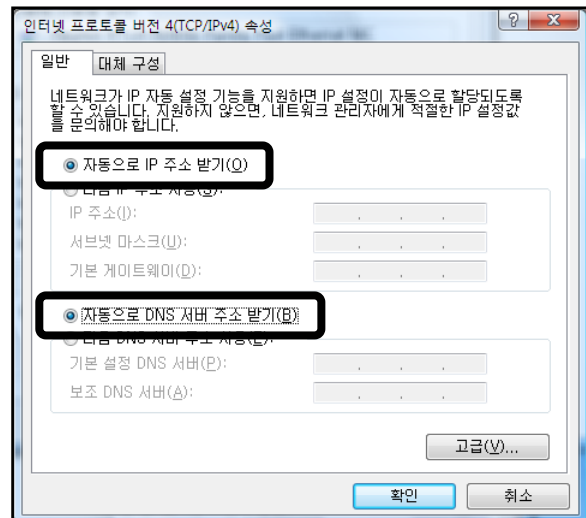


<속성 클릭>

- **인터넷 프로토콜 버전 4(TCP/IPv4)**를 더블 클릭하여 선택하고,
자동으로 IP 주소 받기(O)와 **자동으로 DNS 서버 주소 받기(B)**를 선택합니다.

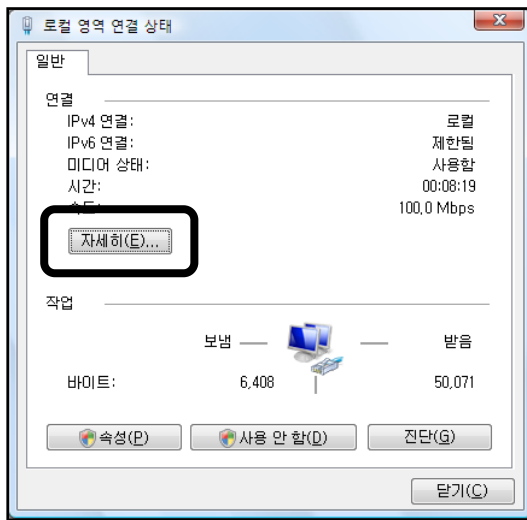


<TCP/IP 더블 클릭>



<자동 선택 후 확인 클릭>

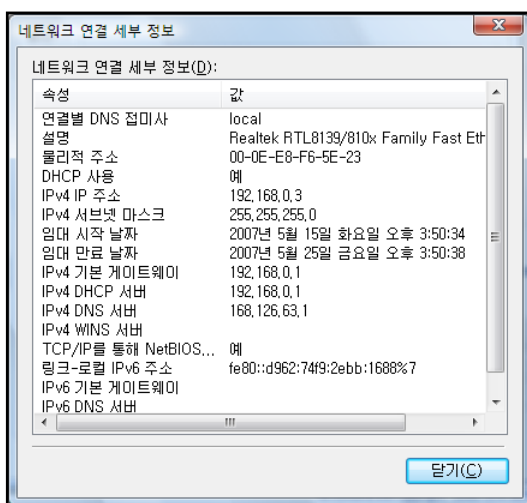
- 설정이 완료된 뒤 **[확인]** 버튼을 클릭하고 로컬 영역 연결 속성 창도 모두 닫아 줍니다.
- TCP/IP 설정을 완료하면 ipTIME에서 IP 주소를 자동으로 할당합니다.
자동할당을 위해서 PC와 ipTIME이 LAN 케이블로 연결되어야 합니다. 만일 케이블을 연결하지 않았다면 케이블을 연결한 뒤 PC를 다시 시작합니다.
- IP 주소 자동 할당 확인은 로컬 영역 연결 상태 창에서 **[자세히]** 버튼을 클릭하면 확인할 수 있습니다.



<자세히 클릭>

- **[자세히]** 버튼을 클릭하면 아래 그림과 같이 자동 할당된 IP 주소, 서브넷 마스크, 게이트웨이 등을 확인합니다.

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



<IP 주소 확인>

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

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

- PC와 ipTIME사이의 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.com>)를 참고하여 IP 주소 수동 설정 방법으로 IP 주소를 설정하거나 ipTIME 고객센터(1544-8695)에 문의하시기 바랍니다.

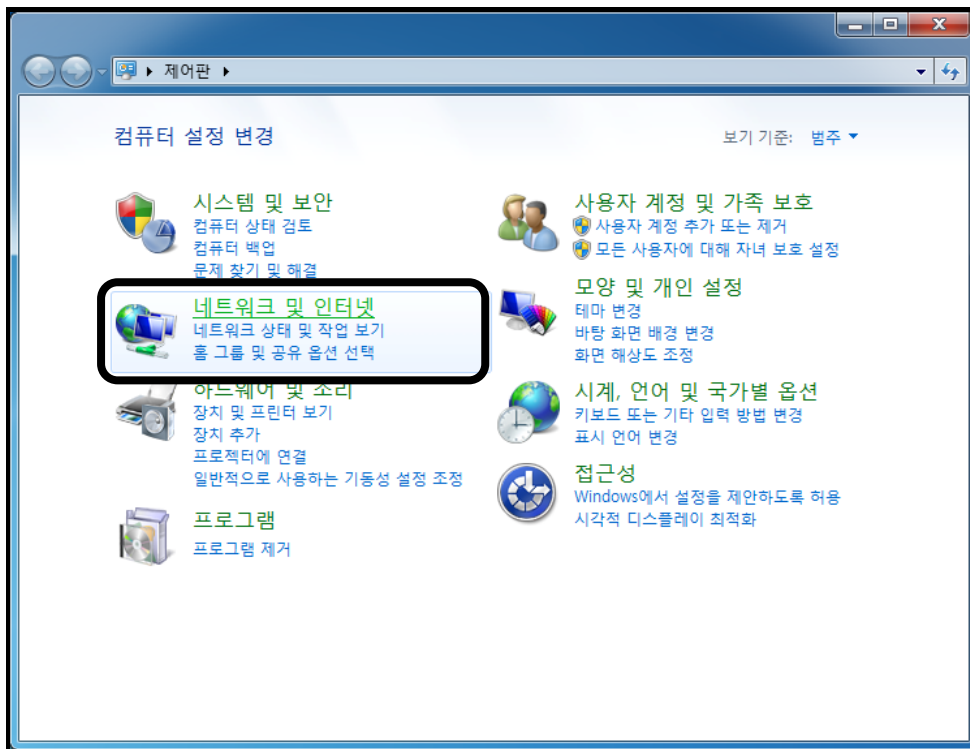
PC 설정을 완료한 뒤 인터넷을 사용하기 위해서는 3장의 내용을 참고하여 설정합니다. 인터넷 연결 설정은 ipTIME에서 이루어지는 것이므로 모든 PC에서 설정할 필요는 없으며 한번만 설정하면 됩니다.

1.3 윈도우 7 설정

이 과정은 윈도우7의 TCP/IP 설정을 초기값으로 복원하는 것입니다. PC에 윈도우가 처음 설치된 상태라면 변경은 없으며 다음 과정에 따라 모든 값이 정상적인지를 확인합니다.

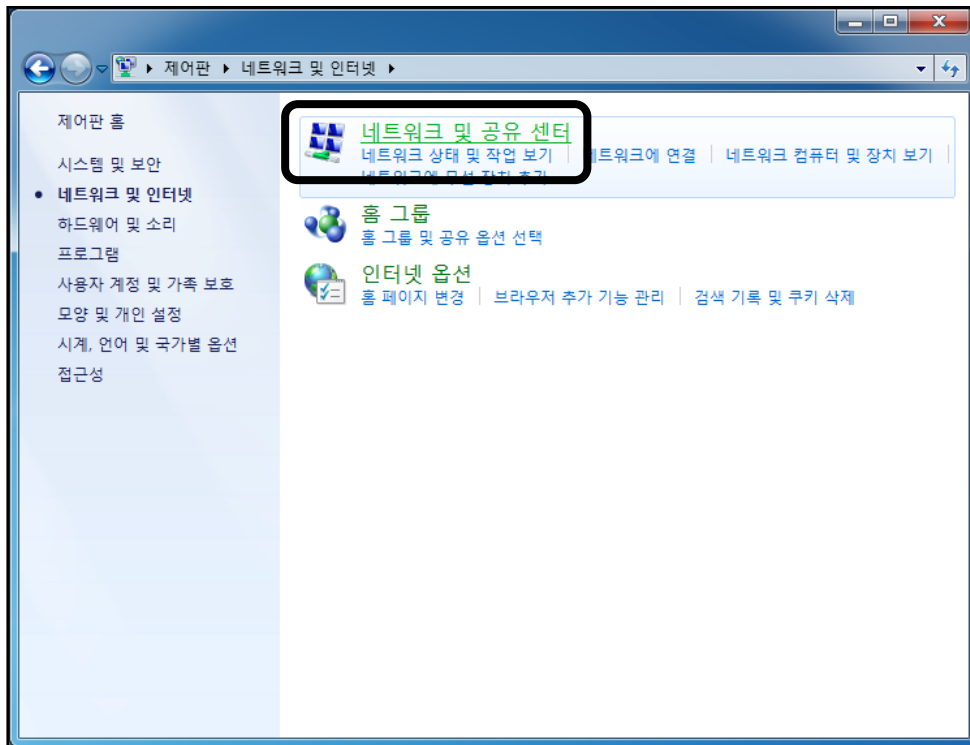
PC의 TCP/IP 설정이 완료된 후 ipTIME에서 자동으로 IP 주소를 부여 받는지 확인하기 위해서는 윈도우를 설정하기 전에 PC와 ipTIME을 LAN 케이블로 연결하고 ipTIME을 켜두어야 합니다.

- 윈도우 좌측 하단의 **윈도우 아이콘** 버튼을 클릭한 후 메뉴에서 **제어판**을 선택합니다.
- 제어판의 **네트워크 및 인터넷** 아이콘을 클릭합니다.



<네트워크 및 인터넷 클릭>

- 네트워크 및 인터넷 연결에서 **네트워크 및 공유 센터** 아이콘을 클릭합니다.



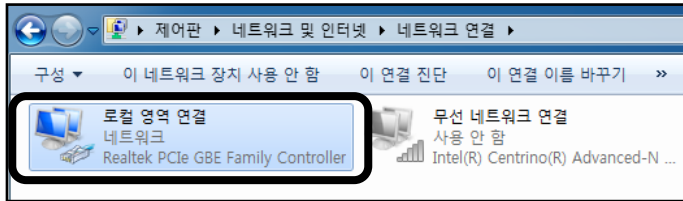
<네트워크 및 공유 센터 클릭>

- **어댑터 설정 변경**을 클릭합니다.



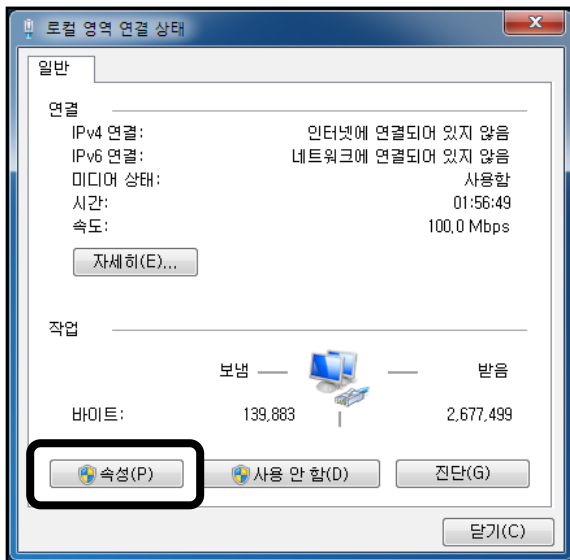
<어댑터 설정 변경 클릭>

- 네트워크 연결에서 **로컬 영역 연결**을 더블 클릭하여 선택합니다.



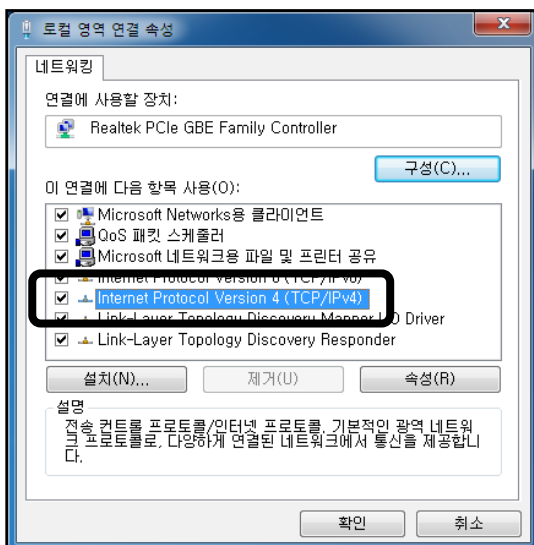
<로컬 영역 연결 더블 클릭>

- 로컬 영역 연결 상태에서 **속성**을 클릭하여 선택합니다.

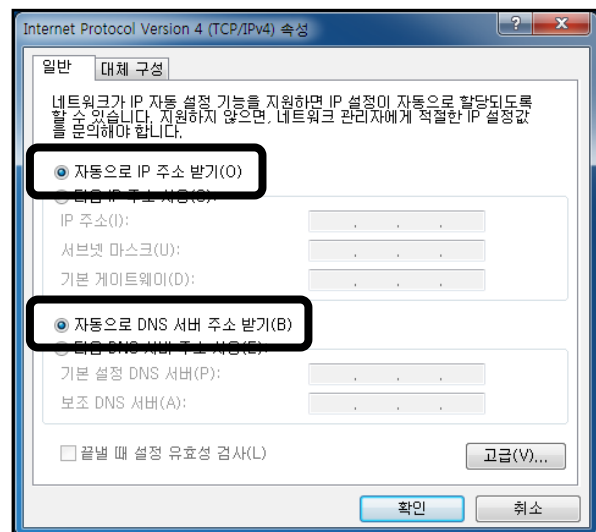


<속성 클릭>

- **Internet Protocol Version 4 (TCP/IPv4)**를 더블 클릭하여 선택하고
자동으로 IP 주소 받기(O)와 **자동으로 DNS 서버 주소 받기(B)**를 선택합니다.

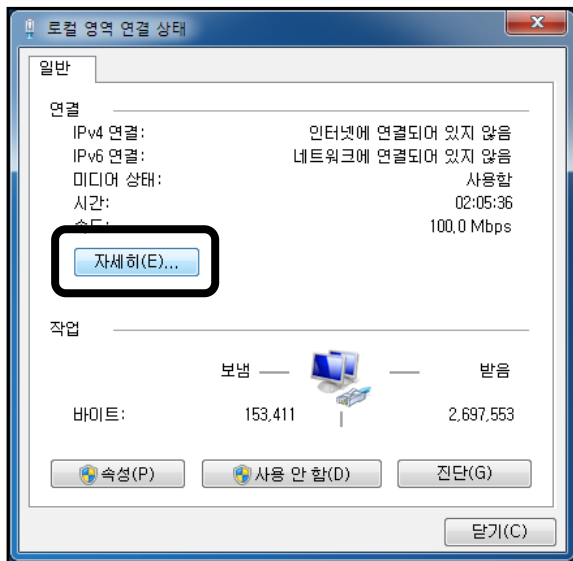


<TCP/IP 더블 클릭>



<자동 선택 후 확인 클릭>

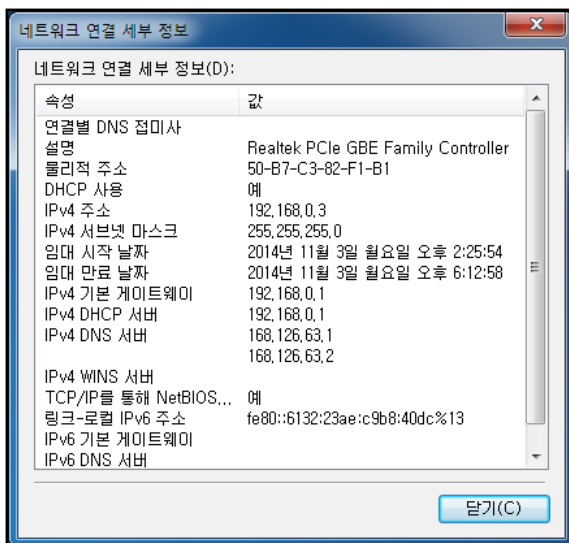
- 설정이 완료된 뒤 **확인** 버튼을 클릭하고 로컬 영역 연결 속성 창도 모두 닫아 줍니다.
- TCP/IP 설정을 완료하면 ipTIME에서 IP 주소를 자동으로 할당합니다.
자동할당을 위해서 PC와 ipTIME이 LAN 케이블로 연결되어야 합니다. 만일 케이블을 연결하지 않았다면 케이블을 연결한 뒤 PC를 다시 시작합니다.
- IP 주소 자동 할당 확인은 로컬 영역 연결 상태 창에서 **자세히** 버튼을 클릭하면 확인할 수 있습니다.



<자세히 클릭>

- **자세히** 버튼을 클릭하면 아래 그림과 같이 자동 할당된 IP 주소, 서브넷 마스크, 게이트웨이 등을 확인합니다.

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



<IP 주소 확인>

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

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

- PC와 ipTIME사이의 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.com>)를 참고하여 IP 주소 수동 설정 방법으로 IP 주소를 설정하거나 ipTIME 고객센터(1544-8695)에 문의하시기 바랍니다.

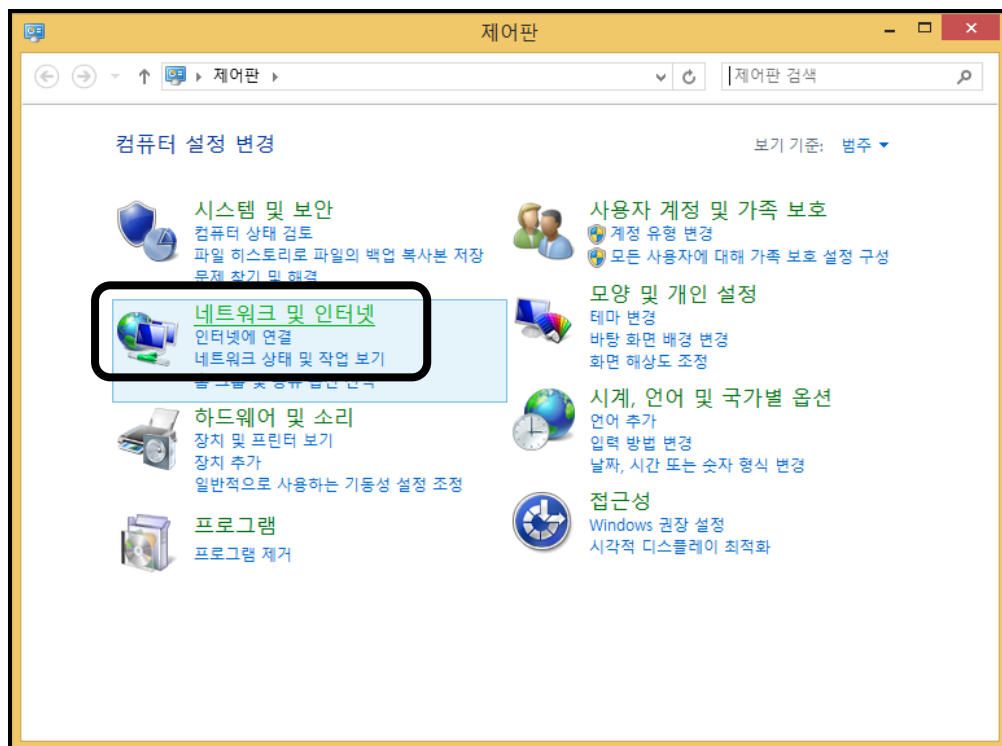
PC 설정을 완료한 뒤 인터넷을 사용하기 위해서는 3장의 내용을 참고하여 설정합니다. 인터넷 연결 설정은 ipTIME에서 이루어지는 것이므로 모든 PC에서 설정할 필요는 없으며 한번만 설정하면 됩니다

1.3 윈도우 8.1 설정

이 과정은 윈도우 8.1의 TCP/IP 설정을 초기값으로 복원하는 것입니다. PC에 윈도우가 처음 설치된 상태라면 변경은 없으며 다음 과정에 따라 모든 값이 정상적인지를 확인합니다.

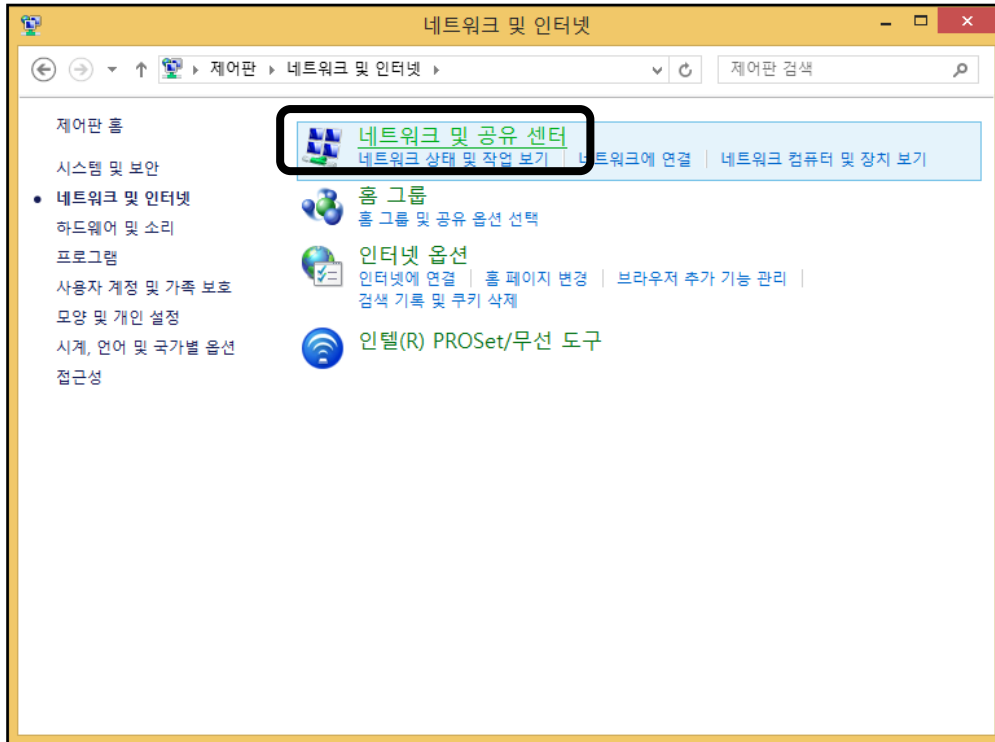
PC의 TCP/IP 설정이 완료된 후 ipTIME에서 자동으로 IP 주소를 부여 받는지 확인하기 위해서는 윈도우를 설정하기 전에 PC와 ipTIME을 LAN 케이블로 연결하고 ipTIME을 켜두어야 합니다.

- 윈도우 좌측 하단의 **윈도우 아이콘** 버튼을 마우스 오른쪽 버튼으로 클릭한 후 메뉴에서 **제어판**을 선택합니다.
- 제어판의 **네트워크 및 인터넷** 아이콘을 클릭합니다.



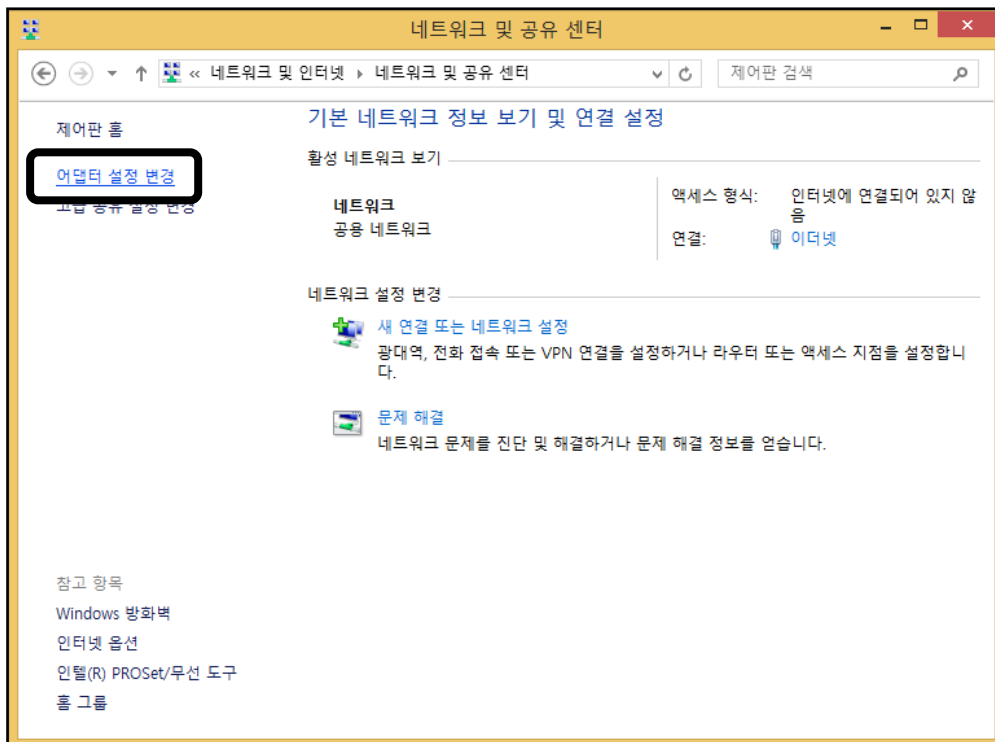
<네트워크 및 인터넷 클릭>

- 네트워크 및 인터넷 연결에서 **네트워크 및 공유 센터** 아이콘을 클릭합니다.



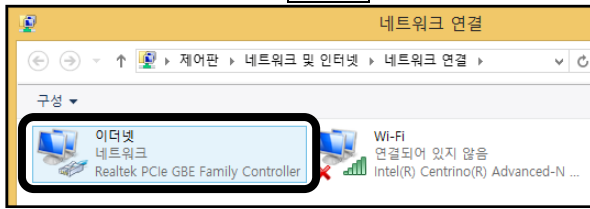
<네트워크 및 공유 센터 클릭>

- **어댑터 설정 변경**을 클릭합니다.



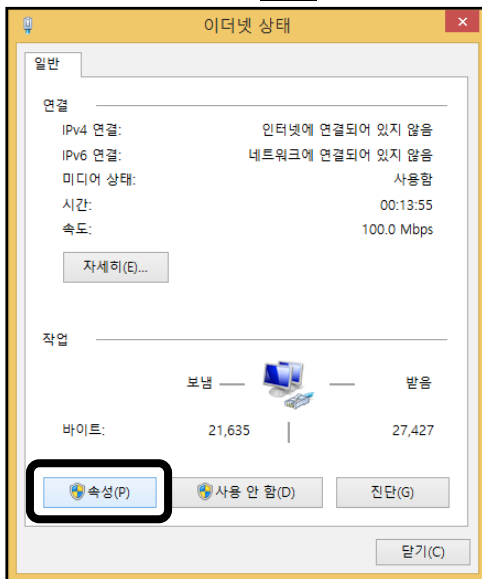
<어댑터 설정 변경 클릭>

- 네트워크 연결에서 **이더넷**을 더블 클릭하여 선택합니다.



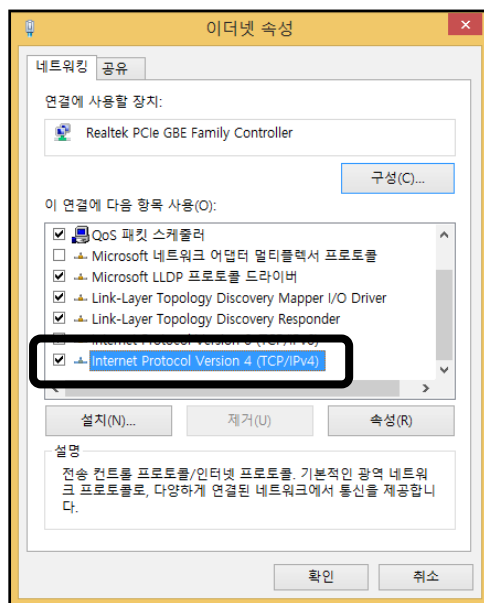
<이더넷 더블 클릭>

- 이더넷 상태에서 **속성**을 클릭하여 선택합니다.

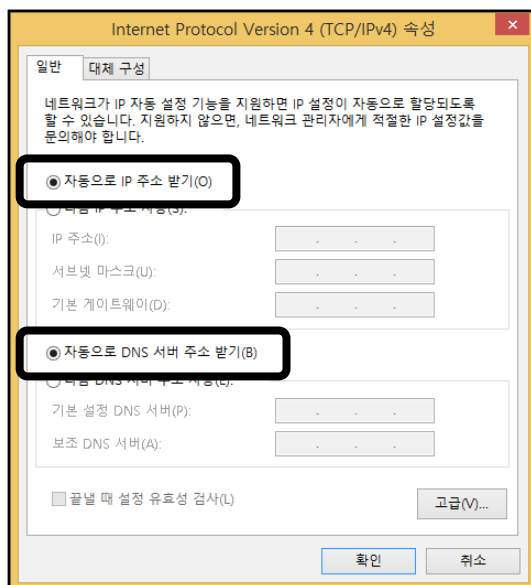


<속성 클릭>

- **Internet Protocol Version 4 (TCP/IPv4)**를 더블 클릭하여 선택하고
자동으로 IP 주소 받기(O)와 **자동으로 DNS 서버 주소 받기(B)**를 선택합니다.

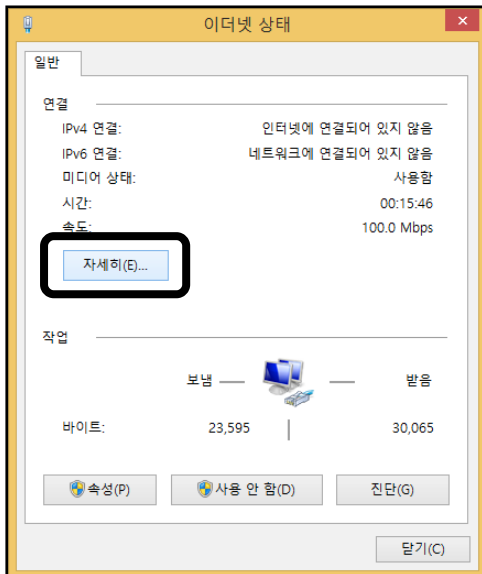


<TCP/IP 더블 클릭>



<자동 선택 후 확인 클릭>

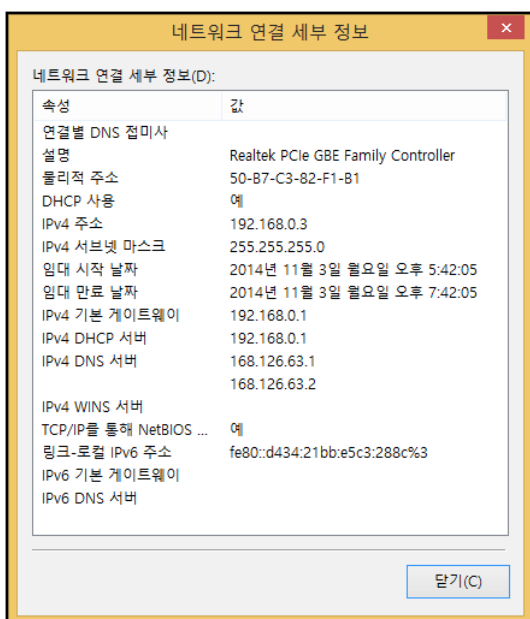
- 설정이 완료된 뒤 **확인** 버튼을 클릭하고 이더넷 속성 창도 모두 닫아 줍니다.
- TCP/IP 설정을 완료하면 ipTIME에서 IP 주소를 자동으로 할당합니다.
자동할당을 위해서 PC와 ipTIME이 LAN 케이블로 연결되어야 합니다. 만일 케이블을 연결하지 않았다면 케이블을 연결한 뒤 PC를 다시 시작합니다.
- IP 주소 자동 할당 확인은 이더넷 상태 창에서 **자세히** 버튼을 클릭하면 확인할 수 있습니다.



<자세히 클릭>

- **자세히** 버튼을 클릭하면 아래 그림과 같이 자동 할당된 IP 주소, 서브넷 마스크, 게이트웨이 등을 확인합니다.

[참고] ipTIME에 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 ipTIME사이의 LAN 케이블 연결
- TCP/IP의 설정 내용 확인
- ADSL 접속 프로그램(광대역 연결 아이콘)의 제거 여부

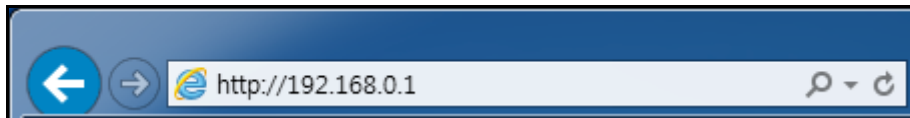
위의 사항을 확인하여도 IP 주소가 정상적으로 자동 할당되지 않는다면 당사 홈페이지 (<http://www.iptime.com>)를 참고하여 IP 주소 수동 설정 방법으로 IP 주소를 설정하거나 ipTIME 고객센터(1544-8695)에 문의하시기 바랍니다.

PC 설정을 완료한 뒤 인터넷을 사용하기 위해서는 3장의 내용을 참고하여 설정합니다. 인터넷 연결 설정은 ipTIME에서 이루어지는 것이므로 모든 PC에서 설정할 필요는 없으며 한번만 설정하면 됩니다

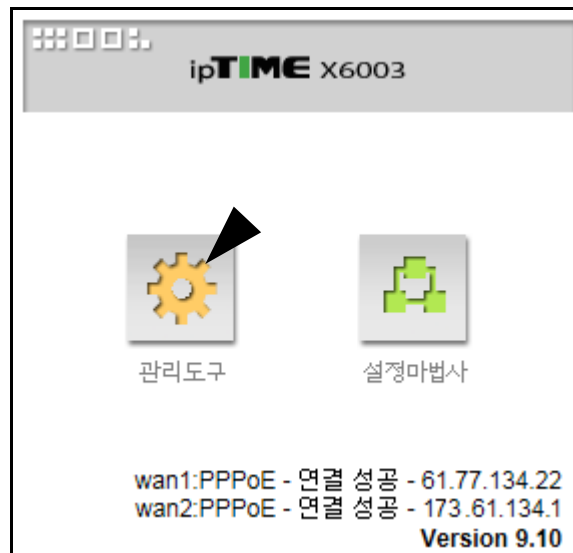
2장 웹 설정 화면 이용하기

2.1 ipTIME 웹 서버 접속

- ipTIME 웹 서버에 접속하여 관련된 설정을 변경하거나 동작 상태를 확인할 수 있습니다. ipTIME의 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 ipTIME의 주소인 192.168.0.1을 입력합니다.



- ipTIME에 접속되면 아래 그림과 같은 화면이 표시되며 이때 **관리도구** 버튼을 클릭하면 ipTIME 웹 설정 화면으로 접속됩니다.



<웹 설정 화면>

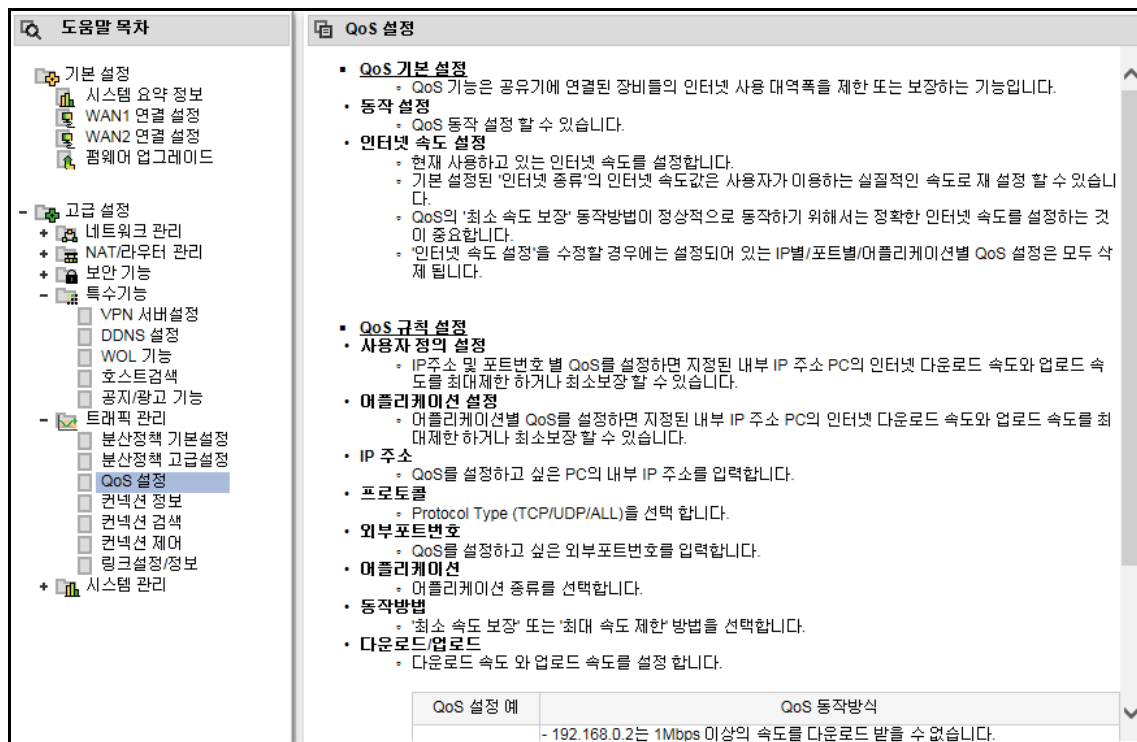
2.2 도움말 기능

- ipTIME은 모든 기능에 대한 도움말을 내장하고 있습니다. ipTIME 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 도움말 화면>

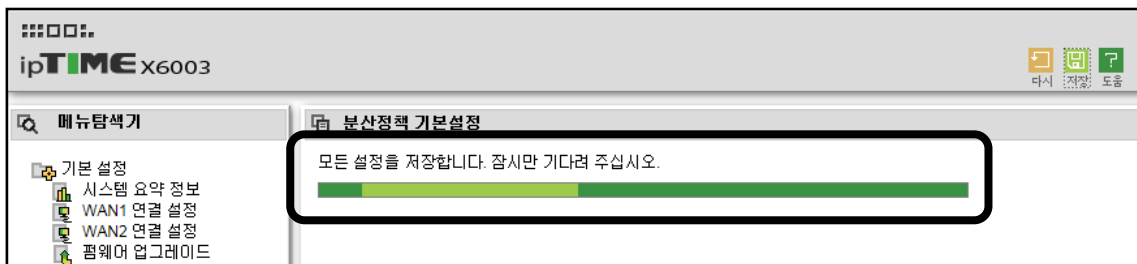
2.3 설정 저장 기능

- ipTIME 웹 설정 화면으로 설정 변경된 내용은 설정 저장을 하여야 영구적으로 저장됩니다. 설정 저장을 하지 않으면 변경된 설정 내용은 공유기의 전원을 OFF하면 모두 지워집니다. 설정 저장을 위해서는 웹 설정 화면 우측 상단의 설정 저장 메뉴를 클릭합니다.
- [시스템 관리] - [기타 설정]에서 자동설정 저장기능을 활성화/비활성화 할 수 있습니다.



<웹 설정 화면 우측 상단의 설정 저장 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.



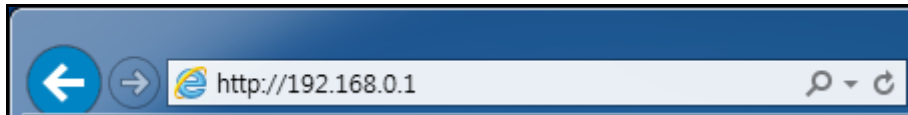
<설정 저장을 알리는 화면 메시지 내용>

3장 설정 마법사로 인터넷 연결

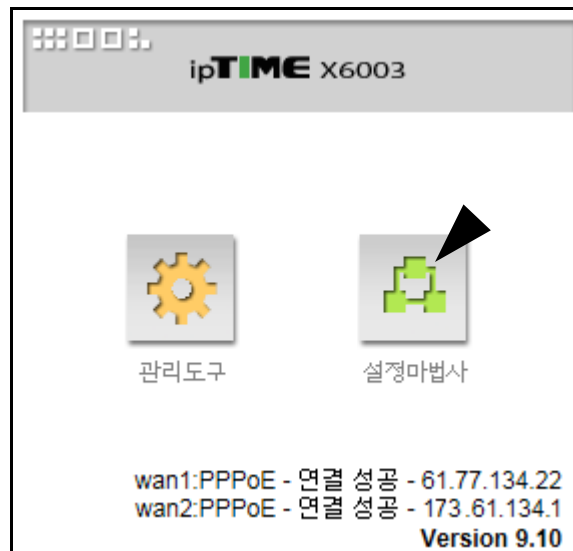
- 본 3장에서는 ipTIME을 인터넷에 연결하는 방법에 대해서 설명합니다. 인터넷 연결 설정은 내장된 웹 설정화면에 접속하여 이루어집니다. 그러므로 인터넷 연결 설정은 ipTIME과 연결된 PC 중 한 곳에서 한번만 실행하면 됩니다.
- ipTIME에 내장된 웹 서버에 접속하기 위해서는 PC를 정상적으로 설정하여야 합니다. PC의 설정 방법에 대해서는 본 설명서 1장을 참고하시면 됩니다.
- 인터넷 연결 설정은 ipTIME에 내장된 마법사를 이용하며, 자동 또는 수동 설정이 가능합니다. 3장에서는 이 마법사를 이용하여 인터넷 설정을 진행하는 방법을 설명합니다.
- 1장에서 3장까지의 내용에 따라 PC와 ipTIME의 설정을 완료하면 ipTIME과 연결된 PC에서 인터넷 사용이 가능합니다.
- 마법사를 사용하지 않고 인터넷 연결 설정을 진행하시려면 "4.2장 인터넷 연결 설정"을 참고합니다.
- 케이블 모뎀 방식의 인터넷 서비스 환경일 경우, 본 사용 설명서 1장을 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 3장의 내용을 진행합니다.

3.1 ipTIME 웹 서버 접속

- ipTIME에 내장된 웹 서버는 인터넷이 연결되어 있지 않아도 접속할 수 있습니다.
웹 서버에 접속하기 위해서는  Internet Explorer를 실행하여, 주소란에 ipTIME의 주소인 192.168.0.1을 입력합니다.



- ipTIME에 접속되면 아래 그림과 같은 화면이 표시되며 이때 **설정마법사** 버튼을 클릭하면 마법사를 시작합니다.



<웹 설정 화면>

3.2 ipTIME 설정 마법사 실행

- ipTIME 초기화면에서 설정 마법사 버튼을 클릭하여 아래 그림과 같이 마법사를 시작합니다.

WAN포트를 선택합니다.
마법사를 이용하여 설정할 WAN포트를 선택합니다.

☒ WAN1 포트
☐ WAN2 포트

설정할 WAN포트를 선택한 후 "다음" 버튼을 누릅니다.

다음 >

설정할 WAN 포트를 선택하고 **다음** 버튼을 클릭합니다.

인터넷 연결 마법사를 시작합니다.
마법사를 실행할 방법을 선택하십시오.
[WAN1 포트]

☒ 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.

< 이전 다음 >

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.

인터넷 회선 선택 기준

유 형	내 용
동적 IP 주소	FTTH, 광랜 서비스 VDSL 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

3.3 자동 검색에 의한 PPPoE 연결 예

Aceman Pro, WinPOET, XP 광대역 접속 프로그램 등을 사용하는 PPPoE 서비스 방식의 ADSL 환경에서 사용하는 경우 아래 순서로 인터넷 설정이 자동 진행됩니다.

[1] 자동 검색을 선택한 후 **다음** 버튼을 클릭합니다.

인터넷 연결 마법사를 시작합니다.
 마법사를 실행할 방법을 선택하십시오.
[WAN1 포트]

☒ 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.

< 이전

다음 >

[2] WAN포트 연결 및 모뎀에 대한 내용 확인하시고 **다음** 버튼을 클릭합니다.

WAN포트 연결 성공 - 모뎀 재시작
[WAN1 포트]

WAN포트가 정상적으로 연결되어 있습니다.

FTTH, 광랜 등의 서비스처럼 벽에서 직접 인터넷선(랜선)이 나오는 경우는,
 '다음' 버튼을 눌러 계속 진행합니다.

ADSL/VDSL/케이블모뎀 서비스 방식일 경우는 모뎀의 전원을 껐다 켜줍니다.
 일정 시간(최대 5분 이내)이 지난 후, 모뎀의 Link/Sync/Online 등의 LED의 상태를 확인합니다.
 해당 LED가 정상적으로 켜져 있으면, '다음' 버튼을 눌러 계속 진행합니다.

* 해당 LED가 지속적으로 깜박거리면, 인터넷 서비스 제공업체에 문의합니다.

< 이전

다음 >

[3] 인터넷 검색 중 화면이 나오는 동안 기다립니다.

인터넷 연결 검색 중
[WAN1 포트]
 인터넷 연결을 검색하고 있습니다.
 검색을 마친 후에는 자동으로 검색 결과를 보여줍니다.
 이 과정은 최대 2분까지 소요될 수 있습니다.

< 이 전
 다음 >

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

PPPoE 방식 검색됨
 사용자 계정 및 암호 입력
[WAN1 포트]
 PPPoE를 사용하는 ADSL 방식의 인터넷 연결이 검색되었습니다.
 이 연결 방식은 인터넷 서비스 제공업체로부터 부여받은 사용자 계정 및 암호가 필요합니다.
 사용자 계정 및 암호를 정확히 입력한 후 '다음' 버튼을 클릭합니다.

사용자 계정
 사용자 암호
 사용자 계정 및 암호를 분실하였을 경우에는 인터넷 서비스 제공업체로 문의합니다
 KT : 국번없이 100
 하나로통신 : 국번없이 106
 (하나로 통신에서는 기본계정으로 사용자이름:hanaro@hanaro, 암호:1 을 제공하고있습니다)

< 이 전
 다음 >

- 잘못된 암호/계정이라는 메시지가 나오는 경우 서비스 회사에 사용자 계정과 암호를 확인하여 다시 입력합니다.
- 정확한 암호/계정을 입력하여도 잘못된 암호/계정이라는 메시지가 나오면 10.5장을 참고하여 ipTIME을 공장 초기화한 후 다시 진행하여 보시기 바랍니다.

[5] 인터넷이 연결되면 할당 받은 IP 주소가 표시되며, **설정 저장 후 마법사 종료** 버튼을 클릭하여 마법사를 종료합니다.

인터넷 연결 성공
PPPoE 방식
[WAN1 포트]

PPPoE방식으로 인터넷에 연결되었습니다.
할당된 IP정보는 아래와 같습니다.

외부 IP 주소	61.77.134.22
서브넷 마스크	255.255.255.255
기본 게이트웨이	ppp1
기본 DNS 서버	168.126.63.1
보조 DNS 서버	168.126.63.2

현재의 인터넷 설정을 적용하려면 "설정 저장 후 마법사 종료" 버튼을 클릭합니다.
"마법사 재실행" 버튼을 누르면, 다른 WAN 포트에 대한 인터넷 연결 설정을 계속할 수 있습니다.

마법사 재실행

설정 저장 후 마법사 종료

3.4 자동 검색에 의한 동적 IP 연결 예

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

[1] 자동 검색을 선택한 후 **다음** 버튼을 클릭합니다.

인터넷 연결 마법사를 시작합니다.
 마법사를 실행시킬 방법을 선택하십시오.

☒ 자동으로 인터넷 연결을 검색하며 설정합니다.
 인터넷 연결 방법을 자동으로 감지하며 설정합니다.
 동적IP(DHCP) 또는 PPPoE 방식을 감지할 수 있습니다.

☐ 수동으로 인터넷 연결을 설정합니다.
 모든 인터넷 연결을 수동으로 설정하실 수 있습니다.

다음 >

[2] WAN포트 연결 및 모뎀에 대한 내용을 확인하시고 **다음** 버튼을 클릭합니다.

WAN포트 연결 성공 - 모뎀 재시작

WAN포트가 정상적으로 연결되어 있습니다.

 FTTH, 광랜 등의 서비스처럼 벽에서 직접 인터넷선(랜선)이 나오는 경우는,
 '다음' 버튼을 눌러 계속 진행합니다.

ADSL/VDSL/케이블모뎀 서비스방식일 경우는 모뎀의 전원을 껐다 켜줍니다.
 일정 시간(최대 5분 이내)이 지난 후, 모뎀의 Link/Sync/Online 등의 LED의 상태를 확인합니다.
 해당 LED가 정상적으로 켜져 있으면, '다음' 버튼을 눌러 계속 진행합니다.

* 해당 LED가 지속적으로 깜박거리면, 인터넷 서비스 제공업체에 문의합니다.

< 이전

다음 >

[3] 인터넷 검색 중 화면이 나오는 동안 기다립니다.

인터넷 연결 검색 중
[WAN1 포트]
 인터넷 연결을 검색하고 있습니다.
 검색을 마친 후에는 자동으로 검색 결과를 보여줍니다.
 이 과정은 최대 2분까지 소요될 수 있습니다.

< 이 전
 다음 >

[4] 동적 IP 방식으로 인터넷이 검색되면 아래 그림과 같이 설정이 종료되며, **설정 저장 후 마법사 종료** 버튼을 클릭하여 마법사를 종료합니다.

인터넷 연결 성공
 동적IP(DHCP) 방식

동적IP방식(DHCP)으로 인터넷에 연결되었습니다.
 할당된 IP정보는 아래와 같습니다.

외부 IP 주소	192.168.11.121
서브넷 마스크	255.255.255.0
기본 게이트웨이	192.168.11.254
기본 DNS 서버	168.126.63.1
보조 DNS 서버	168.126.63.2

현재의 인터넷 설정을 적용하려면 "설정 저장 후 마법사 종료" 버튼을 클릭합니다.

마법사 재실행
 설정 저장 후 마법사 종료

[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 한 대의 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 4장의 4.2.1 동적 IP 방식 설정의 그림과 같이 "사설 IP 할당 허용하기"를 반드시 체크하시고 하단의 적용을 눌러주시면 IP공유기의 연결도 사용할 수 있습니다.

3.5 수동 설정을 이용한 인터넷 연결 설정

마법사를 이용한 자동 인터넷 검색에 실패하였거나 인터넷 서비스의 종류를 정확히 알고 있는 경우, 그리고 인터넷 서비스 회사로부터 할당 받은 고정 IP 주소를 사용하는 My IP, Multi IP 등과 같은 서비스를 사용하는 경우, 수동 설정을 이용하여 인터넷을 연결합니다.

[1] 수동 설정을 선택한 후 **다음** 버튼을 클릭합니다.

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.

인터넷 연결방식 선택

☐ 동적으로 IP를 할당받는 방법(DHCP)
 FTTH,광랜,케이블모뎀,VDSL,IP ADSL,LAN방식등의 서비스에 적합합니다.
 이 방식은 DHCP 프로토콜을 이용하여 IP를 동적으로 할당받는 방법입니다.

☐ 사용자 계정과 암호를 필요로 하는 인터넷 연결(PPPoE)
 ADSL모뎀(PPPoE지원) 사용시 적합한 방식입니다.
 이 방식은 PPPoE 프로토콜을 이용하여 인터넷에 연결합니다.
 사용자 계정 및 암호는 인터넷 서비스 회사로부터 제공받습니다.

☒ 고정 IP를 사용하는 인터넷에 연결(Static IP)
 인터넷 서비스 제공업체로부터 할당받은 고정IP를 설정하는 방식입니다.
 IP주소,서브넷 마스크,게이트웨이,DNS 등의 주소를 직접 입력합니다.

< 이전 다음 >

- 고정 IP 서비스 방식의 경우 인터넷 서비스 회사에서 입력 받은 IP 주소와 게이트웨이 DNS 주소를 입력한 뒤 **다음** 버튼을 클릭합니다..

고정 IP를 사용하는 인터넷에 연결(Static IP)
IP주소, 서브넷마스크, 게이트웨이, DNS 서버를 입력

외부 IP 주소	61	77	128	253
서브넷 마스크	255	255	255	0
기본 게이트웨이	61	77	128	1
기본 DNS서버	168	126	63	1
보조 DNS서버	168	126	63	2

- 위에 입력한 IP주소 값은 임의 IP주소 값이므로 PC에 IP를 수동으로 입력한 값이나 인터넷 서비스 업체에서 준 계약서의 IP주소 값을 넣어 주셔야 합니다.

인터넷 연결 설정 확인

설정 될 내용이 다음과 같습니다.

연결방식	고정IP 방식
외부 IP 주소	61.77.128.253
서브넷 마스크	255.255.255.0
기본 게이트웨이	61.77.128.1
기본 DNS서버	168.126.63.1
보조 DNS서버	168.126.63.2

현재의 인터넷 설정을 적용하려면 "설정 저장 후 마법사 종료" 버튼을 클릭합니다.

[3] PPPoE 방식을 선택한 후 **다음** 버튼을 클릭합니다.

인터넷 연결방식 선택

☐ 동적으로 IP를 할당받는 방법(DHCP)
 FTTH,광랜,케이블모뎀,VDSL,IP ADSL,LAN방식등의 서비스에 적합합니다.
 이 방식은 DHCP 프로토콜을 이용하여 IP를 동적으로 할당받는 방법입니다.

☒ 사용자 계정과 암호를 필요로 하는 인터넷 연결(PPPoE)
 ADSL모뎀(PPPoE지원) 사용시 적합한 방식입니다.
 이 방식은 PPPoE 프로토콜을 이용하여 인터넷에 연결합니다.
 사용자 계정 및 암호는 인터넷 서비스 회사로부터 제공받습니다.

☐ 고정 IP를 사용하는 인터넷에 연결(Static IP)
 인터넷 서비스 제공업체로부터 할당받은 고정IP를 설정하는 방식입니다.
 IP주소,서브넷 마스크,게이트웨이,DNS 등의 주소를 직접 입력합니다.

- 사용자 계정 및 암호를 필요로 하는 PPPoE ADSL 방식의 경우 서비스 회사에서 부여 받은 사용자 계정 및 암호를 입력하고 **다음** 버튼을 클릭합니다.

사용자 계정과 암호를 필요로 하는 인터넷 연결(PPPoE)
 사용자 계정 및 암호 입력

사용자 계정 및 암호는 인터넷 서비스 제공 업체로부터 제공받습니다.

사용자 계정

사용자 암호

사용자 계정 및 암호를 분실하였을 경우에는 인터넷 서비스 제공업체로 문의합니다
 KT : 국번없이 100
 하나로통신 : 국번없이 106
 (하나로 통신에서는 기본계정으로 사용자이름:hanaro@hanaro, 암호:1 을 제공하고있습니다)

- 잘못된 암호/계정이라는 메시지가 나오는 경우 서비스 회사에 사용자 계정과 암호를 확인하여 다시 입력합니다.
- 정확한 암호/계정을 입력하여도 잘못된 암호/계정이라는 메시지가 나오면 10.5장을 참고하여 ipTIME을 공장 초기화한 후 다시 진행하여 보시기 바랍니다.

39

인터넷 연결 설정 확인

설정 될 내용이 다음과 같습니다.

연결방식	사용자계정 및 암호입력 방식(PPPoE)
사용자 계정	iptimeex
사용자 암호	*****

현재의 인터넷 설정을 적용하려면 "설정 저장 후 마법사 종료" 버튼을 클릭합니다.

< 이 전

설정 저장 후 마법사 종료

[4] 동적 IP 방식을 선택한 후 **다음** 버튼을 클릭합니다.

인터넷 연결방식 선택

☒ **동적으로 IP를 할당받는 방법(DHCP)**
FTTH,광랜,케이블모뎀,VDSL,IP ADSL,LAN방식등의 서비스에 적합합니다.
이 방식은 DHCP 프로토콜을 이용하여 IP를 동적으로 할당받는 방법입니다.

☐ **사용자 계정과 암호를 필요로 하는 인터넷 연결(PPPoE)**
ADSL모뎀(PPPoE지원) 사용시 적합한 방식입니다.
이 방식은 PPPoE 프로토콜을 이용하여 인터넷에 연결합니다.
사용자 계정 및 암호는 인터넷 서비스 회사로부터 제공받습니다.

☐ **고정 IP를 사용하는 인터넷에 연결(Static IP)**
인터넷 서비스 제공업체로부터 할당받은 고정IP를 설정하는 방식입니다.
IP주소,서브넷 마스크,게이트웨이,DNS 등의 주소를 직접 입력합니다.

- 정상 연결이 안될 경우 모뎀에서 이전 연결한 PC의 하드웨어 주소(MAC Address)를 저장하고 있어 연결이 되지 않는 경우가 있습니다.

동적으로 IP를 할당받는 방법(DHCP)
WAN포트의 MAC 주소 입력

WAN포트의 MAC 주소를 변경합니다.

☒ 현재 접속 되어 있는 PC의 MAC 주소를 자동으로 입력

☐ PC의 MAC 주소를 수동으로 입력
 - - - - -
 공유기를 사용하지 않고 인터넷을 사용했던 PC의 MAC 주소를 입력합니다.

☐ MAC 주소를 변경하지 않음.

☒ 사설 IP할당을 허용합니다.

- 정상 연결이 안될 경우 모뎀에서 이전 연결한 PC의 하드웨어 주소(MAC Address)를 저장하고 있어 연결이 되지 않는 경우가 있습니다.
 이러한 경우에는 모뎀과 공유기를 꺼주시고 모뎀부팅 후(약 1~2분) 공유기를 부팅하시고 (10초 후) 위 설정을 다시 시작 시작해 보시기 바랍니다.

인터넷 연결 설정 확인

설정 될 내용이 다음과 같습니다.

연결방식	동적IP 방식-DHCP사용
WAN포트의 MAC 주소	접속된 PC의 MAC 주소 : 00-13-8F-43-F2-10
사설IP할당	허용함

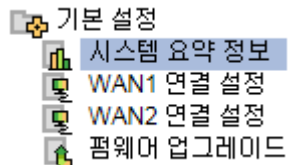
현재의 인터넷 설정을 적용하려면 "설정 저장 후 마법사 종료" 버튼을 클릭합니다.

< 이 전

설정 저장 후 마법사 종료

4장 기본설정

4.1 시스템 요약 정보



공유기의 인터넷 연결 정보, 내부 네트워크 정보, 펌웨어 정보 그리고 원격 관리 정보를 확인 할 수 있습니다.

WAN1 인터넷 정보

인터넷 연결 상태	인터넷에 정상적으로 연결됨 (인터넷 라인백업 동작중)		
인터넷 연결 방식	PPPoE 연결	외부 IP 주소	61.77.134.22
인터넷 연결 시간	0 시간 52 분 25 초		

WAN2 인터넷 정보

인터넷 연결 상태	WAN포트 연결안됨 (WAN1로 백업됨)		
인터넷 연결 방식	동적 IP 연결	외부 IP 주소	
인터넷 연결 시간	0 시간 0 분 0 초		

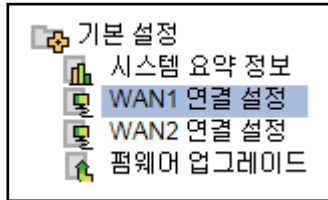
내부 네트워크 정보

내부 IP주소	192.168.0.1
DHCP 서버 상태	DHCP 서버 동작중
동적 IP 할당 범위	192.168.0.2 - 192.168.0.254

기타 정보

현재 펌웨어 버전	9.10
원격 관리 정보	원격 관리 포트가 설정되어 있지 않음 [공유기 접속 관리]에서 설정을 변경할 수 있습니다.
시스템 동작 시간	0 시간 53 분 31 초

4.2 인터넷 연결 설정

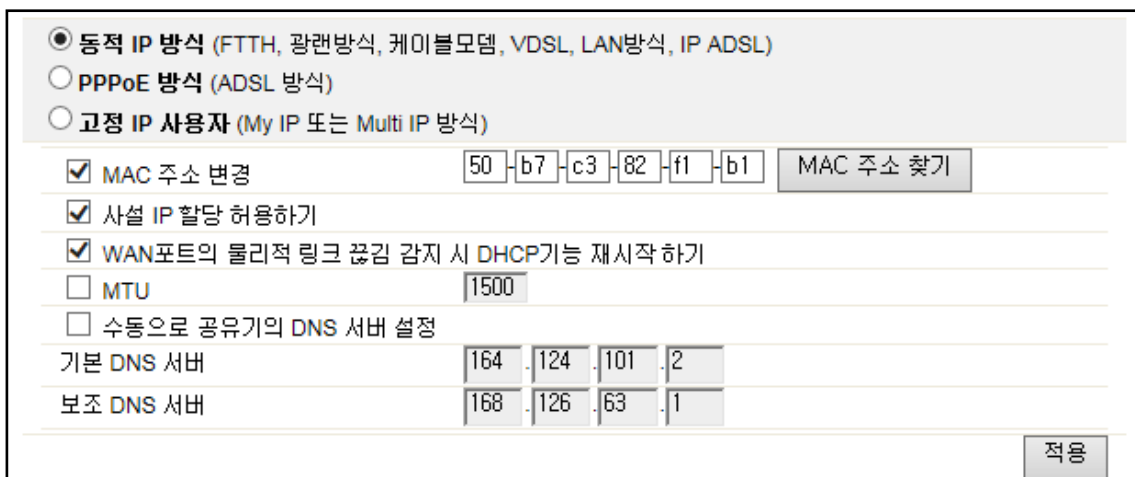


사용하시는 인터넷 서비스 방식을 선택하여 공유기를 인터넷에 연결할 수 있도록 설정하는 메뉴입니다.

('WAN2 연결 설정' 역시 동일하게 진행 하면 됩니다.)

4.2.1 동적 IP 방식 설정

FTTH, 광랜, 케이블 모뎀, VDSL, IP-ADSL (접속 프로그램 ADSL 모뎀 내장) 방식의 인터넷 서비스에 접속하는 경우 동적 IP 방식을 선택합니다. 일부 동적 IP 서비스 지역에서는 MAC 주소에 근거하여 서비스를 제한하는 경우가 있습니다. 이때는 모뎀 등에 연결하여 인터넷 사용이 가능한 것으로 확인되는 PC의 MAC 주소를 공유기에 입력해주어야 합니다.



☒ 동적 IP 방식 (FTTH, 광랜방식, 케이블모뎀, VDSL, LAN방식, IP ADSL)
☐ PPPoE 방식 (ADSL 방식)
☐ 고정 IP 사용자 (My IP 또는 Multi IP 방식)

☒ MAC 주소 변경 50 - b7 - c3 - 82 - f1 - b1 MAC 주소 찾기
☒ 사설 IP 할당 허용하기
☒ WAN포트의 물리적 링크 끊김 감지 시 DHCP기능 재시작하기
☐ MTU 1500
☐ 수동으로 공유기의 DNS 서버 설정

기본 DNS 서버 164 . 124 . 101 . 2
 보조 DNS 서버 168 . 126 . 63 . 1

적용

<동적 IP 방식 입력 화면>

동적 IP 방식 설정 항목 요약

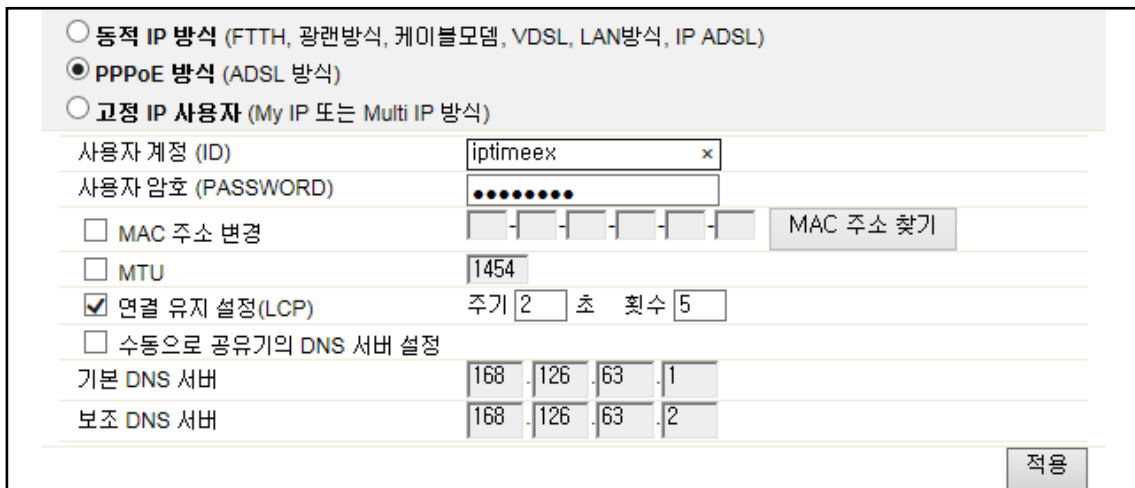
항목	내용
MAC 주소 변경	MAC 주소 변경에 check를 하면 현재 웹 설정 화면에 접속한 PC의 하드웨어 주소가 자동으로 복사됩니다.
사설 IP 할당 허용하기	WAN 을 사설 IP주소로 구성된 네트워크에 연결하고자 하는 경우 이 항목을 check합니다. 일반적으로 check하지 않고 사용합니다.
MTU	MTU 값은 공유기를 통해서 인터넷으로 전달되는 패킷 데이터의 최대 크기를 지정합니다. 일반적으로 1500을 사용하며 특정한 서비스 환경에서 업로드에 문제가 발생하는 경우 1300정도의 값을 입력하여 사용합니다
수동으로 DNS 서버 설정	인터넷 서비스 회사로부터 자동 할당 받는 DNS 서버를 사용하지 않고 사용자가 지정한 임의의 DNS 서버를 사용할 때 설정합니다.

동적 IP 방식의 WAN 설정 순서

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

4.2.2 PPPoE 방식 설정

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



<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.
수동으로 DNS 서버 설정	인터넷 서비스 회사로부터 자동 할당 받는 DNS 서버를 사용하지 않고 사용자가 지정한 임의의 DNS 서버를 사용할 때 설정 합니다.

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.

4.2.3 고정 IP 방식 설정

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

☐ 동적 IP 방식 (FTTH, 광랜방식, 케이블모뎀, VDSL, LAN방식, IP ADSL) ☐ PPPoE 방식 (ADSL 방식) ☒ 고정 IP 사용자 (My IP 또는 Multi IP 방식)					
외부 IP 주소	210	123	20	245	
서브넷 마스크	255	255	255	0	
기본 게이트웨이	210	123	201		
기본 DNS 서버	168	126	63	1	
보조 DNS 서버	168	126	63	2	
☐ MTU	1500				
☒ MAC 주소 변경	50	b7	c3	82	f1 b1
					MAC 주소 찾기
					적용

<고정 IP 방식 입력 화면>

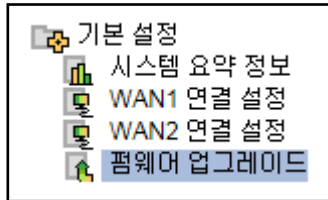
고정 IP 방식 설정 항목 요약

항목	내용
MAC 주소 변경	MAC 주소 변경에 check를 하면 현재 웹 설정 화면에 접속한 PC의 하드웨어 주소가 자동으로 복사됩니다.
MTU	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

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.

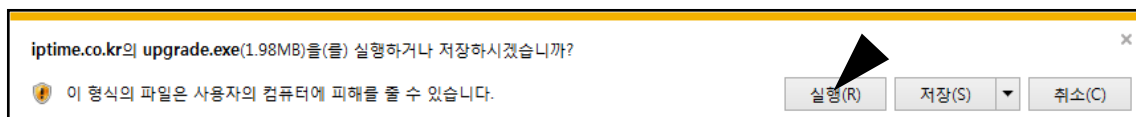
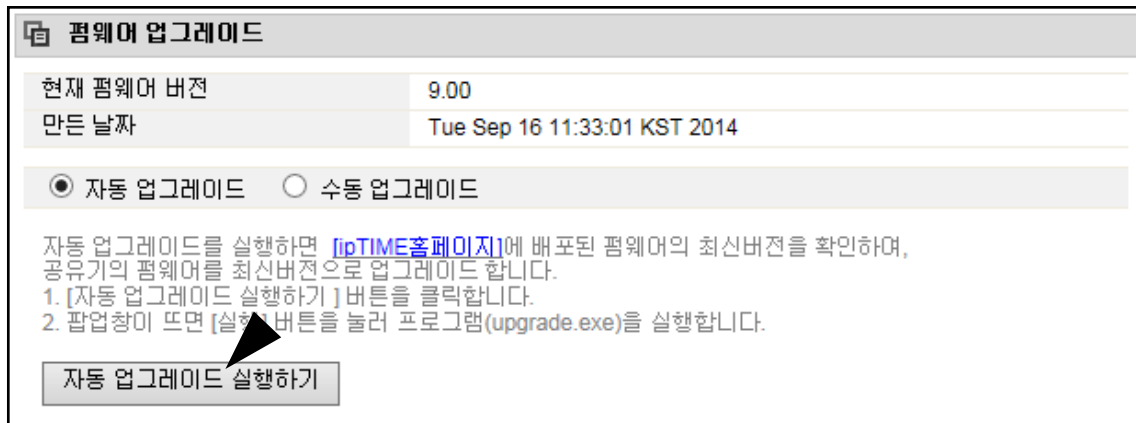
4.3 펌웨어 업그레이드



새로 배포되는 ipTIME 펌웨어를 해당 메뉴에서 업그레이드 할 수 있습니다.

자동 업그레이드

공유기가 인터넷에 정상적으로 연결된 경우에는 [자동 업그레이드 실행하기]를 클릭하고 해당 프로그램 [실행]을 선택하면 아래 그림과 같은 펌웨어 업그레이드 유틸리티가 실행되어 공유기의 최신 펌웨어로 자동 업그레이드 됩니다.



ipTIME 관리자 계정 및 암호 확인
ipTIME의 관리자 계정 및 암호 입력

ipTIME Upgrade




관리자 계정

관리자 암호 ☒ 암호 숨기기

ipTIME에 관리자 계정 및 암호가 설정되어 있습니다.
관리자 계정 및 암호를 입력후 '다음' 버튼을 클릭 합니다.

업그레이드
업그레이드 정보 확인

ipTIME Upgrade


Upgrade


공유기의 펌웨어를 최신 버전으로 업그레이드 합니다.
업그레이드를 진행할 공유기의 정보를 확인 후 업그레이드 버튼을 클릭합니다.

모델명	ipTIME X6003	IP 주소	192.168.0.1
현재 펌웨어	9.00	최신 펌웨어	9.10

☒ 선택하신 ipTIME의 펌웨어를 9.10 버전으로 업그레이드 합니다.

업그레이드 성공
ipTIME 펌웨어 업그레이드 성공

ipTIME Upgrade


SUCCESS


ipTIME의 펌웨어 업그레이드에 성공하였습니다.
'마침' 버튼을 클릭하여 ipTIME 업그레이드를 종료합니다.

수동 업그레이드

수동 업그레이드를 위해 <http://www.iptime.com>을 방문하여 **고객지원** > **다운로드** 에서 **다운로드 구분** > **제품군** > **모델명**을 클릭하여 제품 모델명을 선택한 후 해당 제품의 최신 펌웨어를 PC에 저장합니다.



번호	제목	날짜	조회
10	ipTIME x5007 펌웨어 버전 8.76	2013-11-12	2528
9	ipTIME X5007 펌웨어 버전 8.74	2013-10-07	1357
8	ipTIME X5007 펌웨어 버전 8.72	2013-08-06	1856
7	ipTIME X5007 펌웨어 버전 8.70	2013-07-04	1567
6	ipTIME X5007 펌웨어 버전 7.70	2011-08-16	5498
5	ipTIME X5007 펌웨어 버전 7.26	2010-08-18	3718

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

펌웨어 업그레이드

현재 펌웨어 버전

9.00

만든 날짜

Tue Sep 16 11:33:01 KST 2014

☐ 자동 업그레이드
 ☒ 수동 업그레이드

수동 업그레이드를 통해 공유기의 펌웨어를 업그레이드할 수 있습니다.

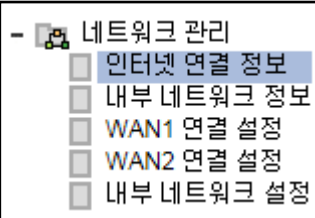
1. [ipTIME 홈페이지]에서 펌웨어를 다운로드합니다.
2. [찾아보기] 버튼을 누른 후, 다운로드받은 펌웨어파일을 선택합니다.
3. [업그레이드] 버튼을 클릭합니다.

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

업그레이드 버튼을 클릭하여 최신 버전의 펌웨어로 업그레이드를 시작합니다.

5장 네트워크 관리

5.1 인터넷 연결 정보



ipTIME의 인터넷 연결 상태 확인 할 수 있습니다.

인터넷 회선 상태를 반영하기 위하여 연결이 되지 않은 경우
5초마다 자동 갱신됩니다.

WAN1

연결 상태	인터넷에 정상적으로 연결됨 인터넷 라인백업 동작중
연결 방식	PPPoE 연결
외부 IP 주소	61.77.134.22
서브넷 마스크	255.255.255.255
기본 게이트웨이	61.77.134.22
기본 DNS 서버	168.126.63.1
보조 DNS 서버	168.126.63.2
MAC 주소	00-08-9F-12-51-AB

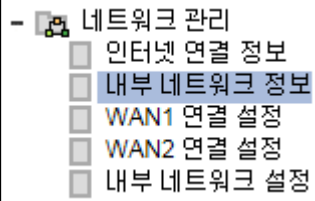
접속 해제

WAN2

연결 상태	WAN포트 연결안됨 WAN1로 백업됨
연결 방식	고정 IP 연결
외부 IP 주소	192.168.123.1
서브넷 마스크	255.255.255.0
기본 게이트웨이	192.168.123.254
기본 DNS 서버	164.124.101.2
보조 DNS 서버	
MAC 주소	00-08-9F-12-51-AC

위의 예는 WAN1 PPPoE 방식의 인터넷 연결과 WAN2 고정 IP 인터넷 연결 정보 입니다.

5.2 내부 네트워크 정보



ipTIME의 내부 네트워크 설정 정보, 내장된 DHCP서버가 할당한 동적 IP 할당 수 및 ipTIME과 연결되어 있는 PC들의 정보를 확인할 수 있습니다.

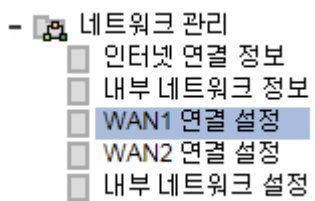
내부 네트워크 정보

내부 IP주소	192.168.0.1
서브넷 마스크	255.255.255.0
MAC 주소	00-08-9F-12-51-AA
동적 IP 할당 범위	192.168.0.2 ~ 192.168.0.254
동적 IP 할당 수	1

사용 중인 IP 주소 정보

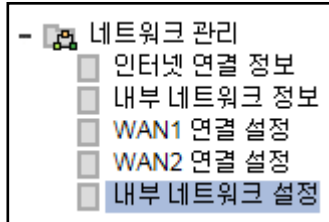
	IP 주소	MAC 주소	비고
1	192.168.0.3	50-B7-C3-82-F1-B1	유선 : 자동할당
2	192.168.0.34	00-E0-4C-37-2C-94	유선 : 수동설정

5.3 인터넷 연결 설정



사용하시는 인터넷 서비스 방식을 선택하여 공유기를 인터넷에 연결할 수 있도록 설정하는 메뉴입니다.
자세한 내용은 4.2장 기본설정의 인터넷 연결 설정을 참고하세요.

5.4 내부 네트워크 설정



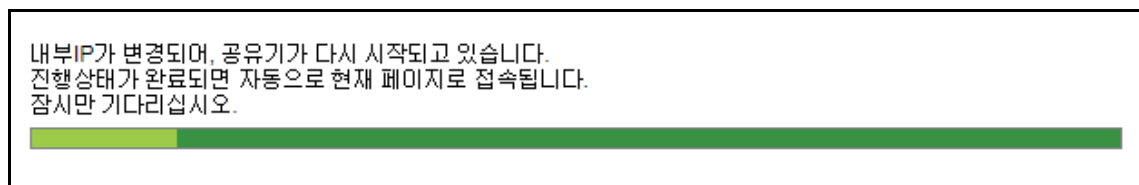
ipTIME의 내부 IP 설정, DHCP 서버의 설정 및 DHCP 서버의 수동 IP 할당 설정을 할 수 있습니다.

내부 IP 설정

ipTIME 의 기본 IP 주소는 192.168.0.1입니다. 이 IP 주소를 변경하고자 하는 경우 본 항목을 이용합니다

내부 IP 설정				
내부 IP주소	192	168	0	119
서브넷 마스크	255	255	255	0
적용 후 시스템 다시 시작				

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



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

DHCP 서버 상태/설정

DHCP 서버 설정에서 실행 또는 중지를 선택한 후 **[적용]** 버튼을 클릭하여 ipTIME의 DHCP 서버를 켜거나 끌 수 있습니다. DHCP 서버를 중지하면 ipTIME에서 PC로 IP주소를 자동 할당하지 않습니다.

DHCP 서버 상태/설정

DHCP 서버 설정

동적 IP 주소 범위

IP 대여 시간

☒ 실행
 ☐ 중지

192

168

0

2

~

192

168

0

254

7200 초

DNS Suffix

local x

☐ 내부네트워크에서 DHCP서버 발견시 공유기의 DHCP 서버기능을 중단
☐ IP를 할당받은 PC만 인터넷 접속을 허용

적용

무선 접속 정보화면에서 표시되는 내용은 다음과 같습니다.

동작 상태	무선 모듈의 동작상태
DHCP 서버 설정	DHCP 서버의 동작을 설정합니다.
DNS Suffix	DNS suffix를 정의하면 자동으로 클라이언트 이름 뒤에 도메인 이름이 붙게 됩니다. 예를 들어, DNS suffix를 'office.com'으로 지정한 후, 'abc' 라는 클라이언트 이름으로 ping 테스트를 하게 되면 "abc.office.com" 도메인 이름에 대한 DNS 쿼리가 송신됩니다.
동적 IP 주소 범위	DHCP 서버가 PC에 자동 할당해 줄 수 있는 IP 주소의 범위를 설정 할 수 있습니다. 예를 들어, '192.168.0.[10] ~ 192.168.0.[100]'으로 설정하면, PC들은 192.168.0.10부터 IP 주소를 자동할당 받게 됩니다.

정상적인 IP 주소 할당을 위해서는 DHCP 서버를 실행하여야 하며 DHCP 서버를 중단 시킨 경우라면 ipTIME에 연결하는 PC의 IP 주소는 수동으로 설정하여 사용하여야 합니다.

IP 주소 수동 설정 방법은 본사 홈페이지(<http://www.iptime.com>)의

[고객지원] > **[자주묻는질문]** 게시판에서 확인하시기 바랍니다.

내부네트워크에서 DHCP 서버 발견 시 공유기의 DHCP 서버기능을 중단합니다.

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

DHCP 서버에서 IP를 할당 받은 PC만 인터넷 접속을 허용합니다.

ipTIME에 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.

수동 IP 할당 설정

DHCP 서버가 특정PC에게 설정해 놓은 IP로만 할당 하게 합니다.

수동 IP 할당 설정

☐ 설정된 IP와 다른 IP를 가진 MAC주소 통신 차단
 ☐ 설정된 MAC주소 통신만 허용
 적용

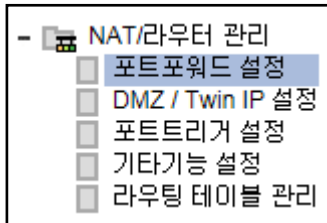
삭제	설정된 IP/MAC 주소	추가	검색된 IP/MAC 주소
☐		☐	
☐	192.168.0.47 / 00-08-9F-28-7D-C8	☐	192 . 168 . 0 . /
☐	192.168.0.57 / 00-63-00-00-04-74		
☐	192.168.0.210 / 00-08-9F-28-1A-28		
		☐	192.168.0.3/50-B7-C3-82-F1-B1 현재 접속된 PC

등록 가능한 최대 MAC 주소는 200개 입니다.

- 검색된 IP/MAC주소를 추가
 - 추가할 IP/MAC주소 좌측의 체크박스를 클릭
 - 추가 버튼 클릭
- 검색되지 않은 IP/MAC주소를 등록
 - 첫 번째 줄의 체크박스를 클릭한 후, IP/MAC주소를 입력
 - 추가 버튼 클릭
- 설정된 IP/MAC주소를 삭제
 - 삭제할 IP/MAC주소 좌측의 체크박스 클릭
 - 삭제 버튼 클릭

6장 NAT/라우터 관리

6.1 포트포워드 설정



공유기의 외부 네트워크 사용자가 내부 네트워크에 접속하고자 하는 경우 사용되는 어플리케이션의 포트번호를 내부 네트워크의 IP 주소와 내부포트 번호로 연결시켜주는 기능이 필요한데, 이런 기능을 포트포워드라고 합니다.

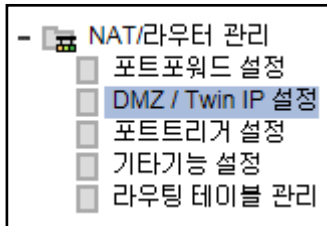
정의된 리스트	사용자정의 ▼	규칙이름				
내부 IP주소	192.168.0.1	☐ 현재 접속된 PC의 IP 주소로 설정(192.168.0.3)				
프로토콜	TCP ▼	외부 포트		~		
WAN	WAN1 ▼	내부 포트		~		
최대 120개의 규칙이 설정 가능합니다. 추가 취소						
낮은 번호일수록 우선순위가 높습니다. 규칙이름을 클릭하시면, 해당 규칙을 수정할 수 있습니다.						
동작	규칙이름	내부 IP	프로토콜	외부 포트	내부 포트	삭제
☐						☐
1 ☒	http	192.168.0.11	tcp	WAN1 80	80	☐
2 ☒	FTP	192.168.0.11	tcp	WAN1 21	21	☐
3 ☒	원격데스...	192.168.0.11	tcp	WAN2 3389	3389	☐

포트포워드 설정에 필요한 각각의 항목은 다음과 같습니다.

설정 항목	기능 설명
정의된 리스트	미리 정의된 규칙을 선택하거나 사용자가 임의로 정의 할 수 있습니다.
규칙이름	새로 입력하는 포트포워드 규칙의 이름을 입력합니다
내부IP주소	어플리케이션이 설치된 내부서버 또는 PC의 IP 주소를 입력합니다.
프로토콜	프로토콜의 종류를 선택합니다. (TCP 또는 UDP)
WAN	WAN 포트를 선택합니다.
외부포트	외부 인터넷에서 접속 시 사용되는 내부서버 또는 PC에 설치된 어플리케이션 포트범위를 설정합니다.
내부포트	내부서버 또는 PC에 설치된 어플리케이션 포트범위를 설정합니다 '외부포트'와 동일한 경우에는 입력하지 않아도 됩니다

- 위의 설정 예는 내부 IP 주소 192.168.0.11을 사용하는 PC의 HTTP 서버, FTP 서버 및 원격데스크톱 서비스를 외부 네트워크에서 접속 할 수 있도록 설정한 규칙 입니다.
- 먼저 입력된 낮은 번호의 규칙이 우선순위가 높습니다.
- 규칙이름을 클릭하시면 해당 규칙을 수정 할 수 있습니다.
- **[동작]** 체크박스를 해제하면 규칙은 남아 있으나 해당 규칙은 동작하지 않습니다.

6.2 DMZ/Twin IP 설정



DMZ 기능 또는 Twin IP 기능을 선택하여 설정 할 수 있습니다.

DMZ 설정

☐ 사용하지 않음
☒ **DMZ** (지정된 내부 IP 주소의 PC로 모든 포트를 개방합니다. 단, 포트포워드에 설정된 포트는 제외)
☐ **Twin IP** (지정된 MAC 주소의 PC가 공인 IP 주소를 사용하도록 합니다)

내부 IP 주소:

☐ 현재 접속된 PC의 IP 주소로 설정(192.168.0.3)

포트포워드에서 설정되어 있지 않은 모든 포트들을 내부의 특정 IP 주소를 가지는 PC로 개방하는 기능입니다. 어플리케이션 포트번호를 알 수 없어 인터넷 공유가 정상적으로 이루어지지 않는 프로그램들은 DMZ 호스트 기능으로 해결 할 수 있습니다.

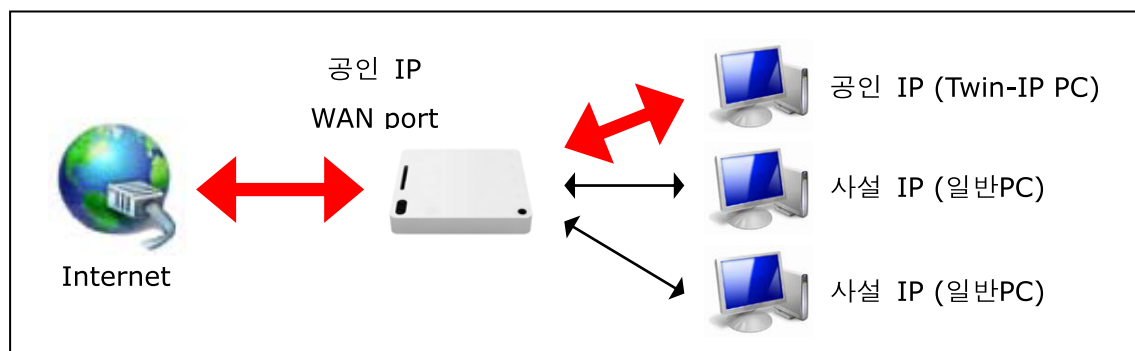
Twin IP 설정

☐ 사용하지 않음
☐ DMZ (지정된 내부 IP 주소의 PC로 모든 포트를 개방합니다. 단, 포트포워드에 설정된 포트는 제외)
☒ **Twin IP** (지정된 MAC 주소의 PC가 공인 IP 주소를 사용하도록 합니다)

MAC 주소: ☐ 현재 접속된 PC의 MAC주소로 설정

IP 갱신 시간: 초

Twin-IP는 인터넷 서비스 업체로 부여 받는 공인 IP주소를 공유기와 연결된 내부의 특정 PC 한 대에 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.



Twin-IP 설정 순서

- ① Twin-IP PC로 지정할 PC의 MAC 주소를 입력합니다.
- ② 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.
- ③ MAC 주소와 갱신 시간을 입력한 후 적용을 클릭합니다.
- ④ 설정 완료 후 해당 PC를 재시작 해야 Twin-IP 기능이 동작합니다.

- Twin-IP 기능은 DHCP 서버가 동작 상태에서 사용 가능합니다.
- 동일한 PC로 WAN1과 WAN2에 대해 모두 Twin-IP를 설정할 수 는 없습니다.

6.3 포트트리거 설정

-  NAT/라우터 관리
 -  포트포워드 설정
 -  DMZ / Twin IP 설정
 -  **포트트리거 설정**
 -  기타기능 설정
 -  라우팅 테이블 관리

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

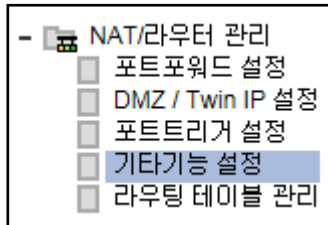
규칙이름											
포트트리거	프로토콜	TCP ▼									
	포트범위	~									
포트포워드	프로토콜	TCP ▼									
	포트범위										
최대 10개의 규칙이 설정 가능합니다. 추가											
<table border="1" style="width: 100%;"> <thead> <tr> <th>규칙이름</th> <th>포트트리거 조건</th> <th>포트포워드 조건</th> <th>☐ 삭제</th> </tr> </thead> <tbody> <tr> <td>1 트리거테스트</td> <td>[tcp] 8080</td> <td>[tcp] 80 8000 8001</td> <td>☐</td> </tr> </tbody> </table>				규칙이름	포트트리거 조건	포트포워드 조건	☐ 삭제	1 트리거테스트	[tcp] 8080	[tcp] 80 8000 8001	☐
규칙이름	포트트리거 조건	포트포워드 조건	☐ 삭제								
1 트리거테스트	[tcp] 8080	[tcp] 80 8000 8001	☐								

포트트리거 설정에 필요한 각각의 항목은 다음과 같습니다.

설정 항목	기능 설명
규칙이름	새로 입력하는 포트트리거 규칙의 이름을 입력합니다.
포트트리거-프로토콜	어플리케이션의 온라인 접속을 감지하기 위한 프로토콜의 종류를 선택합니다. 인터넷 어플리케이션 서버의 목적지 포트 프로토콜(TCP 또는 UDP 선택)
포트트리거-포트범위	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.

- 위의 설정 예는 TCP 8080포트를 사용하는 외부 서버에 접속을 요청하는 내부 IP 주소로 TCP 80, 8000, 8001번 포트를 자동으로 포트포워드 설정하는 규칙입니다..
- 먼저 입력된 낮은 번호의 규칙이 우선순위가 높습니다.
- 포트포워드의 포트범위 입력 시 구분은 '공백'으로 합니다.

6.4 기타기능 설정



FTP 비정규포트, 멀티캐스트 포워드, 인터넷 공유기능의 NAT 기타 기능을 설정 할 수 있습니다.

FTP 비정규포트

공유기 내부 또는 외부에 설치된 FTP 서버가 기본 포트 21번이 아닌 임의의 비정규 포트를 이용하여 운영되는 경우 FTP 비정규 포트 설정을 하여야 합니다

FTP 비정규포트	포트 번호						추가
	☐ 2121	☐ -	☐ -	☐ -	☐ -		삭제

- 2121번을 FTP 포트로 사용하는 경우에 설정한 예 입니다.

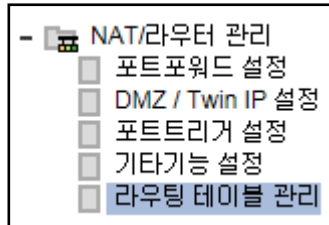
인터넷 공유 기능

인터넷 공유 기능을 중단시키면 공유기의 모든 기능이 중단되고 일반 라우터로 동작이 전환됩니다.

인터넷 공유 기능	☒ 실행 ☐ 중단	적용 후 시스템 다시 시작
	인터넷 공유 기능을 실행하거나 중단할 수 있습니다. 인터넷 공유 기능을 중단하면 관련된 기능이 자동으로 꺼집니다.	

6.5 라우팅 테이블 관리

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



Type	Target	Mask	Gateway
Net ▼			
추가 가능한 최대 주소는 20개 입니다.			
추가			
Type	Target	Mask	Gateway
1	NETWORK	192.168.10.0	255.255.255.0
삭제			

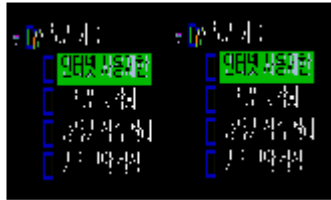
라우팅 테이블 설정에 필요한 각각의 항목은 다음과 같습니다.

설정 항목	기능 설명
Type	라우팅 테이블이 HOST 인지 NETWORK 인지를 설정합니다.
Target	입력할 라우팅 테이블의 Target IP주소 또는 네트워크 주소를 입력합니다.
Mask	Type이 NETWORK일 경우 Subnet mask를 결정합니다.
Gateway	Target으로 통신할 때 거쳐갈 Gateway주소를 입력합니다.

- 위의 설정 예는 192.168.10.0 network 을 목적지로 하는 모든 통신을 Gateway 192.168.0.20을 통하여 통신할 수 있도록 라우팅 테이블을 입력한 화면입니다.

7장 보안기능

7.1 인터넷 사용제한



IP 주소별/MAC 주소별로 인터넷을 차단/허용 할 수 있으며, 또는 어플리케이션의 포트 별로 인터넷을 차단/허용 할 수 있습니다. 설정방법은 `사용자 간단 설정`, `사용자 고급 설정`, `사이트 접속 차단 설정` 및 미리 등록된 어플리케이션 리스트(메신저, P2P, 게임)로 구분 됩니다. 그리고 각각 설정된 규칙들은 각각의 스케줄을 설정하여 정해진 요일과 시간에만 동작시킬 수도 있습니다.

사용자 간단 설정 화면

입력방법 선택	사용자 간단 설정 ▼		규칙이름	
시작지 IP 주소	☒ 192.168.0. ~ 192.168.0. ☐ 모든 IP 주소			
시작지 MAC 주소	☐ - - - - - MAC 주소 찾기			
허용/차단	차단 ▼		우선순위	0

사용자 고급 설정 화면

입력방법 선택	사용자 고급 설정 ▼		규칙이름	
방향	내부 -> 외부 ▼			
시작지 IP 주소	☒ 192.168.0. ~ 192.168.0. ☐ 모든 IP 주소			
시작지 MAC 주소	☐ - - - - - MAC 주소 찾기			
목적지 IP 주소	- - - ~ - - -			
프로토콜	▼		목적지 포트	~
허용/차단	차단 ▼		우선순위	0

사이트 접속 차단 설정 화면

입력방법 선택	사이트 접속 차단 설정 ▼		규칙이름	
시작지 IP 주소	☒ 192.168.0. ~ 192.168.0. ☐ 모든 IP 주소			
시작지 MAC 주소	☐ - - - - - MAC 주소 찾기			
차단할 사이트				
허용/차단	차단 ▼		우선순위	0

사용자 스케줄 설정 화면

☒ 사용자 스케줄 설정하기	
스케줄-요일	☐ 일 ☐ 월 ☐ 화 ☐ 수 ☐ 목 ☐ 금 ☐ 토 ☐ 매일
스케줄-시간	00:00 ~ 00:00 24시간 타임 ☐ 24시간
최대 200개의 설정을 추가 할 수 있습니다.	
추가 취소	

- `사용자 스케줄 설정하기` 항목을 체크하지 않으면 해당 규칙은 요일/시간과 무관하게 무조건 적용됩니다.

인터넷 사용제한 설정에 필요한 각각의 항목은 다음과 같습니다.

설정 항목	기능 설명	비고
입력방법선택	`사용자 간단 설정`, `사용자 고급 설정`, `사이트 접속 차단 설정` 및 미리 등록된 어플리케이션 리스트(메신저, P2P, 게임)를 선택합니다.	공통
규칙이름	새로 입력하는 규칙의 이름을 입력합니다.	공통
방향	내부->외부:공유기에 연결된 내부의 PC에서 외부로 통신 외부->내부:외부에서 공유기에 연결된 내부의 PC로 통신	고급
시작지 IP주소	내부->외부:내부PC의 IP 주소 (기본값) 외부->내부:외부PC의 IP 주소	공통
시작지 MAC 주소	내부->외부:내부PC의 MAC 주소 (기본값) 외부->내부:외부PC의 MAC 주소	공통
목적지 IP 주소	내부->외부:외부PC의 IP 주소 (기본값) 외부->내부:내부PC의 IP 주소	고급
프로토콜	TCP, UDP, ICMP를 선택합니다.	고급
목적지 포트	TCP, UDP 프로토콜을 선택 시 관련 목적지 포트번호를 입력합니다.	고급
차단할 사이트	접속을 차단하고자 하는 사이트의 문자열을 입력합니다. 예를들어, 'sex hangame porn' 이라고 입력하시면 다음의 사이트들이 차단 됩니다. www.sex.com , www.sex.co.kr , www.hangame.com , www.hangame.co.kr , www.porn.com , www.porn.co.kr	사이트차단
우선순위	새로 입력하는 규칙을 우선순위를 지정합니다. 입력하지 않는 경우에는 최하위 우선순위로 설정됩니다.	공통
허용/차단	새로 입력하는 규칙을 허용할지 차단할지를 결정합니다. `사이트 접속 차단`의 경우에는 차단으로 고정됩니다.	공통

다음은 설정된 규칙 예제들 입니다.

낮은 번호일수록 우선순위가 높습니다. 규칙이름을 클릭하시면, 해당 규칙을 수정할 수 있습니다.					
동작	규칙이름	스케줄	필터링 규칙	허용/차단	삭제
☐					☐
1 ☒	내부전용PC	매일 24시간	필터링 규칙 보기	차단	☐
2 ☒	차단사이트	매일 09:00 ~ 18:00	필터링 규칙 보기	차단	☐
3 ☒	네이트온	월 화 수 목 금 24시간	필터링 규칙 보기	차단	☐
[규칙이름] 네이트온 [방향] 내부 -> 외부 [시작지 IP 주소] 모든 IP 주소 [목적지 IP 주소] 모든 IP 주소 [프로토콜 1] tcp 5004 [차단할 사이트] prs.nate.com					

- 모든 IP 주소가 월~금, 09:00~18:00 사이에는 네이트온 메신저를 접속하지 못하도록 차단한 예제 입니다.
- 네이트온 메신저의 경우에는 미리 등록된 어플리케이션 리스트에서 선택하면 됩니다.

낮은 번호일수록 우선순위가 높습니다.
규칙이름을 클릭하시면, 해당 규칙을 수정할 수 있습니다.

동작	규칙이름	스케줄	필터링 규칙	허용/차단	삭제
☐					☐
1 ☒	내부전용PC	매일 24시간	필터링 규칙 보기	차단	☐
[규칙이름] 내부전용PC [방향] 내부 -> 외부 [시작지 IP 주소] 192.168.0.100 - 192.168.0.150 [목적지 IP 주소] 모든 IP 주소					
2 ☒	차단사이트	매일 09:00 ~ 18:00	필터링 규칙 보기	차단	☐
3 ☒	네이트온	월 화 수 목 금 24시간	필터링 규칙 보기	차단	☐

- 192.168.0.100 ~ 192.168.0.150 사이의 IP주소를 사용하는 PC들은 항상 인터넷을 차단하도록 설정한 예제입니다.

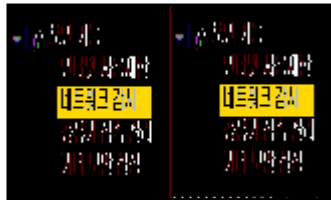
낮은 번호일수록 우선순위가 높습니다.
규칙이름을 클릭하시면, 해당 규칙을 수정할 수 있습니다.

동작	규칙이름	스케줄	필터링 규칙	허용/차단	삭제
☐					☐
1 ☒	내부전용PC	매일 24시간	필터링 규칙 보기	차단	☐
2 ☒	차단사이트	매일 09:00 ~ 18:00	필터링 규칙 보기	차단	☐
[시작지 IP 주소] 모든 IP 주소 [차단할 사이트] naver daum nate					
3 ☒	네이트온	월 화 수 목 금 24시간	필터링 규칙 보기	차단	☐

- 모든 IP 주소가 매일 09:00 ~ 18:00 사이에는 naver, daum, nate 문자가 포함되는 모든 사이트에 접속하는 것을 차단하는 설정 예제입니다.

- 먼저 입력된 낮은 번호의 규칙이 우선순위가 높습니다.
- **[동작]** 체크박스를 해제하면 규칙은 남아 있으나 해당 규칙은 동작하지 않습니다.
- `필터링 규칙 보기`를 클릭하셔야 자세한 필터링 규칙 정보를 볼 수 있습니다.
- 문자열 차단 규칙을 작성한 후에 차단 대상PC를 재부팅 해야 합니다.

7.2 네트워크 감시



악성 웹 바이러스나 P2P 프로그램의 경우 동시에 수천 개의 인터넷 연결을 발생시켜 인터넷 회선을 마비시킬 수 있습니다. ipTIME의 네트워크 감시 기능은 이와 같은 통신 폭주 프로그램을 찾아내어 사용자에게 경고 메시지를 전달하고 폭주 프로그램의 통신을 적절히 제한하는 기능을 제공합니다.

네트워크 감시 설정	
동작 설정	☒ 실행 ☐ 중단
감시대상	☐ 알려진 웹바이러스 통신 ☒ 모든 통신
감시수준	☒ 보통 ☐ 0 연결수/초
감지된 통신차단	☐ 아니오 ☒ 웹바이러스 통신만 차단
E-mail 통보정책	[관리자 E-mail을 설정] 하여야 E-mail 보고기능을 사용할수 있습니다.
적용	

네트워크 감시 내역					
E-mail 바로 보내기				모든 감시 내역 삭제	
최근감지시간	IP 주소	프로토콜	감지횟수	설명 [적색:사용자 경고 해제상태]	
2014/11/04 21:31:08	192.168.1.104	TCP/80	1	웹 과다 접속 감지 또는 웹바이러스 의심	

네트워크 감시의 동작을 위하여 설정할 항목은 다음과 같습니다.

항목	설명						
동작 설정	☒ 실행 또는 ☐ 중단 을 선택하여 네트워크 감시 동작을 설정합니다.						
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. 웹바이러스만 차단 옵션을 체크하면 바이러스 통신만을 차단합니다.						
E-mail 통보 정책	네트워크 감시의 감지 내역을 E-mail 통보하는 방법을 지정합니다.						

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.

항닫기

- 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
2014/11/04 08:39:20	ICMP	해당포트 웜바이러스 감염 의심됨	☐
2014/11/04 12:20:06	TCP/80	웹 과다 접속 감지 또는 웜바이러스 의심	☐

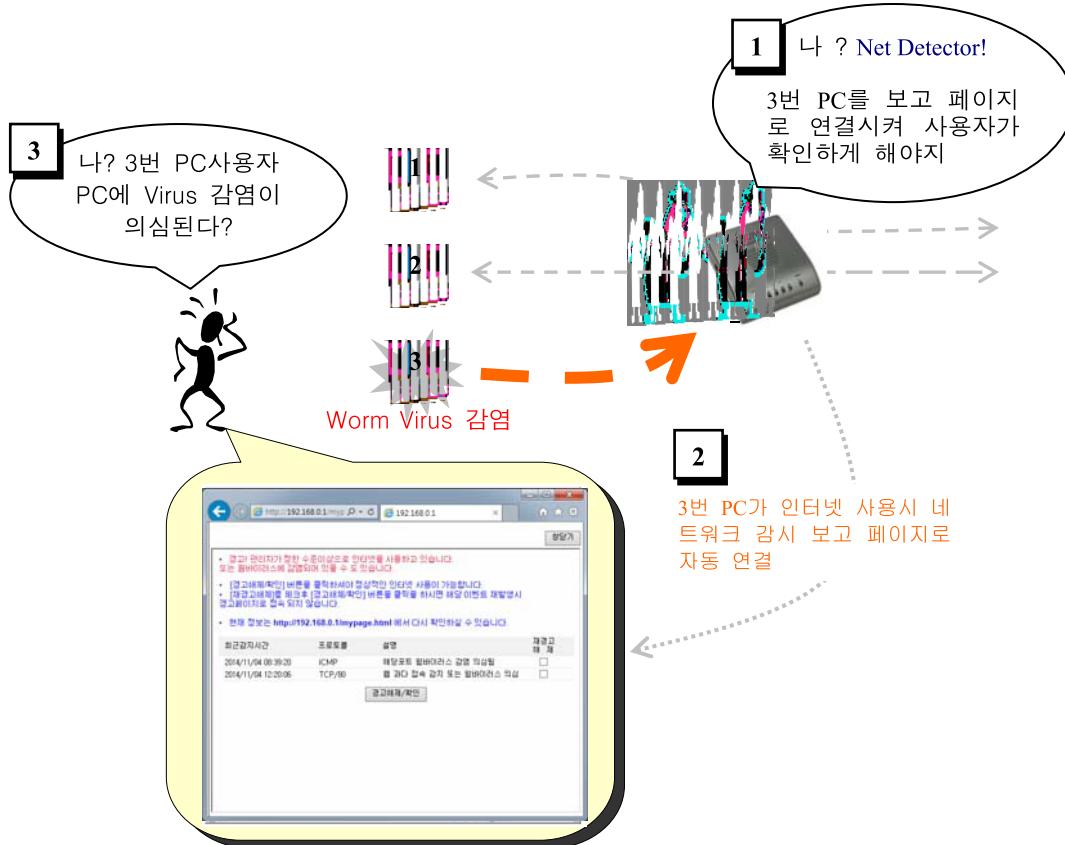
경고해제/확인

[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.

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

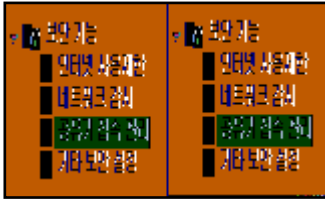
내용	통신 유형
SMTP 바이러스	TCP 25
Worm.Win32.Blaster / Win32 / Ralelka.worm 바이러스	TCP 135
Unknown worm 바이러스	TCP 139
Win32 / IRCBot.worm / Win32 / AgoBot.worm 바이러스	TCP 445
Worm.Win32.Welchina	TCP 707
Unknown worm 바이러스	UDP 137
SQL_Overflow 바이러스	UDP 1434
Unknown worm 바이러스	UDP 6677
소리 바다	TCP 7674 UDP 22321
당나귀	TCP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

- 네트워크 감시의 동작 개요는 다음과 같습니다.



- 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 한 PC 사용자 또는 관리자는 웹 경고 화면에 따라 바이러스 존재 가능성을 확인할 수 있고, 연동되는 하우리 Live call 로 바이러스를 치료 할 수 있다.

7.3 공유기 접속 관리



공유기 설정 웹 서버에 접속을 지정된 사용자만 가능하도록 설정 할 수 있습니다.

공유기 접속관리는 외부 접속과 내부 접속을 구분하여 관리 합니다.

외부 접속 보안

외부 접속 보안			
☒ 원격 관리 포트 사용	5454		
☒ 외부 접속 보안 사용	적용		
허용 할 IP 주소			
설명		추가	
추가 가능한 최대 주소는 10개 입니다.			
IP 주소	설명	삭제	
1 210.198.10.200	사무실A	☐	

- 외부 접속을 위해서는 반드시 원격 관리 포트 번호를 지정하셔야 합니다.
- 외부 접속 보안 사용을 체크하면 등록된 IP주소에서만 원격 관리 포트 번호를 통해서 공유기 설정 웹 서버로 접속 할 수 있습니다.
- 유동 IP 서비스의 경우 외부 IP주소가 자주 바뀌기 때문에 DDNS 기능과 연동하여 사용하시면 편리합니다.

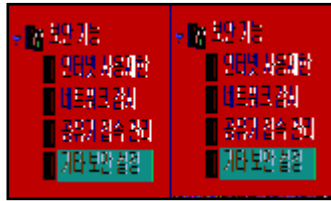
- 공유기의 접속은 웹 브라우저에 주소란에 `http://xxx.xxx.xxx.xxx:pppp`와 같이 URL을 입력하면 공유기 설정 화면에 접속이 가능합니다.(xxx.xxx.xxx.xxx : 외부 IP , pppp : 원격 관리 포트)
- 위의 예는 외부 IP 주소 210.198.10.200인 경우에만 원격 관리 포트 5454번을 통해 공유기 설정 웹 서버에 접속을 허용한 예제입니다.

내부 접속 보안

내부 접속 보안			
☒ 내부 접속 보안 사용	적용		
허용 할 IP 주소			
설명		추가	
추가 가능한 최대 주소는 10개 입니다.			
IP 주소	설명	삭제	
1 192.168.0.11	자동 항목	☐	
2 192.168.0.12	PC12	☐	

- 내부에서의 공유기 설정 웹 서버 접속은 기본적으로 공유기와 연결된 모든 PC에서 접속이 가능합니다.
- 내부 접속 보안을 사용을 체크하면 등록된 IP 주소에만 공유기 설정 웹 서버로 접속 할 수 있습니다.

7.4 기타 보안 설정



Denial of Service (DoS)는 한 사람이 공유자원을 모두 점유하여 다른 사람이 사용할 자원을 없애버리는 공격방식으로 해당 공격에 대해 방어설정을 할 수 있습니다.

기타 보안 설정	
SYN Flood	☒ 실행 ☐ 중단 TCP가 데이터를 보내기 전에 연결을 맺어야 하는 연결 지향(connection-oriented) 방식이라는 점을 착안하여 많은 수의 SYN bit이 설정 되어있는, 즉 연결을 요청하는 TCP 패킷을 호스트의 특정 포트에 보내어 포트의 대기 큐(backlog queue)를 가득 차게 하여 포트에 들어오는 연결 요청을 큐가 빌 때 까지(connection time out이 될 때 까지) 무시하도록 하게 끄는 공격방식.
Smurf	☒ 실행 ☐ 중단 ping의 목적지주소를 브로드캐스트 주소로 사용하는 공격방식. Smurf 공격은 Echo-request 패킷을 어떤 네트워크의 브로드캐스트 주소로 보내면 해당 네트워크의 모든 호스트가 request 패킷에 응답하느라 다른 일은 하지 못하도록 하는 공격방식.
IP source routing	☒ 실행 ☐ 중단 RFC 1122에 따르면 목적지의 경로에 대한 세부적인 내용을 담고 있는 IP Source Routing은 목적지 호스트에서도 같은 경로를 따라 반응을 해야 한다는 문제점이 있다. 크래커가 특정 네트워크에 Source Routing 패킷을 보낼 수 있다면 돌아오는 반응을 가로채서 상대방의 신뢰받은 호스트처럼 속일 수 있다.
IP Spoofing	☒ 실행 ☐ 중단 네트워크 시스템에서 서로 신뢰관계에 있는 A, B 두 시스템간에는 A 시스템의 계정을 가지고 B 시스템을 액세스 할 수 있다. 이는 네트워크에서 신뢰관계를 형성하는 서비스가 네트워크 주소에 기반하여 이를 인증하기 때문이다. 이로 인해 IP Spoofing이 가능해진다. IP Spoofing은 이 신뢰관계에 있는 두 시스템사이에서 해커의 호스트를 마치 하나의 신뢰관계에 있는 호스트인 것처럼 속이는 것이다.
ARP Virus 방어 기능	☒ 실행 ☐ 중단 초당 10 개의 ARP를 로 전송합니다. ARP Virus 방어 기능은 ARP를 통한 공격(ARP snoofing)을 방어하는 기능입니다.
인터넷으로부터 오는 ICMP(ping) 막기	☒ 실행 ☐ 중단
인터넷으로 나가는 ICMP(ping) 막기	☒ 실행 ☐ 중단
적용	

(1) DoS 공격의 종류 및 설명

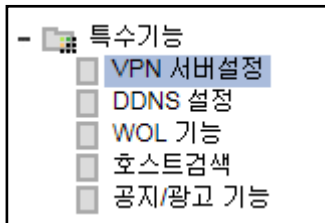
- ① SYN Flooding : TCP 가 데이터를 보내기 전에 연결을 맺어야 하는 연결 지향(connection-oriented) 방식이라는 점을 착안하여 많은 수의 SYN bit 이 설정 되어있는, 즉 연결을 요청하는 TCP 패킷을 호스트의 특정 포트에 보내어 포트의 대기 큐(backlog queue)를 가득 차게 하여 포트에 들어오는 연결 요청을 큐가 빌 때 까지(connection time out 이 될 때 까지) 무시하도록 하게 끄는 공격방식.

- 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 있습니다. Cracker 가 특정 네트워크에 Source Routing 패킷을 보낼 수 있다면 돌아오는 반응을 가로채서 상대방의 호스트와 신뢰받은 호스트처럼 속일 수 있습니다.
- ④ **IP Spoofing** : 네트워크 시스템에서 서로 신뢰관계에 있는 A, B 두 시스템간에는 A 시스템의 account 를 가지고 B 시스템을 액세스 할 수 있습니다. 이는 네트워크에서 신뢰관계를 형성하는 서비스가 네트워크 주소에 기반하여 이를 인증하기 때문이다. 이로 인해 IP Spoofing 이 가능해 집니다. IP Spoofing 은 이 신뢰관계에 있는 두 시스템 사이에서 Hacker 의 호스트를 마치 하나의 신뢰관계에 있는 호스트인 것처럼 속이는 것입니다..
- 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.

8장 특수기능

8.1 VPN 서버설정

해당 기능은 제품 모델에 따라 지원되지 않을 수 있습니다.



VPN 서버 기능을 이용하면 인터넷에 연결된 다수의 PC를 하나의 LAN에 연결된 것처럼 망을 구성할 수 있습니다.

VPN 서버에 연결된 PC 사이에 자유롭게 파일 공유 및 프린터 공유를 할 수 있으며 LAN 환경에서 사용되는 여러 프로그램들을 자유롭게 사용할 수 있습니다.

- ipTIME의 VPN 서버 기능은 최대 5명의 사용자까지 VPN 서버에 접속하여 LAN VPN 환경을 구성할 수 있습니다.
- VPN 서버에 접속하기 위해서는 해당 PC의 윈도우 운영 체제에서 가상 사설망 접속 어댑터를 설치하여야 합니다.

VPN(PPTP) 서버설정

동작 모드 ☒ 실행 ☐ 중단
 암호화(MPPE) ☐ 암호화 사용할 ☒ 암호화 없음

적용

VPN(PPTP) 계정 설정

VPN 접속 계정 test_1
 VPN 접속 암호 ●●●●
 할당 될 IP 주소 192 . 168 . 0 . 50

최대 5명의 사용자를 추가 할 수 있습니다.

추가

VPN 접속 계정	할당 될 IP 주소	연결 상태	연결끊기	삭제
test_1	192.168.0.50	연결되지않음	☐	☐

VPN 서버 설정을 위하여 설정할 항목은 다음과 같습니다.

항목	설명
동작 설정	실행 또는 중단 을 선택하여 VPN 기능 동작을 설정합니다.
암호화(MPPE)	MPPE 암호화 사용여부를 선택합니다.
VPN 접속 계정	VPN을 사용할 새로운 계정을 입력합니다.
VPN 접속 암호	VPN을 사용할 새로운 계정의 암호를 입력합니다.
할당할 IP 주소	VPN을 사용할 새로운 계정이 할당 받을 IP 주소를 지정합니다.

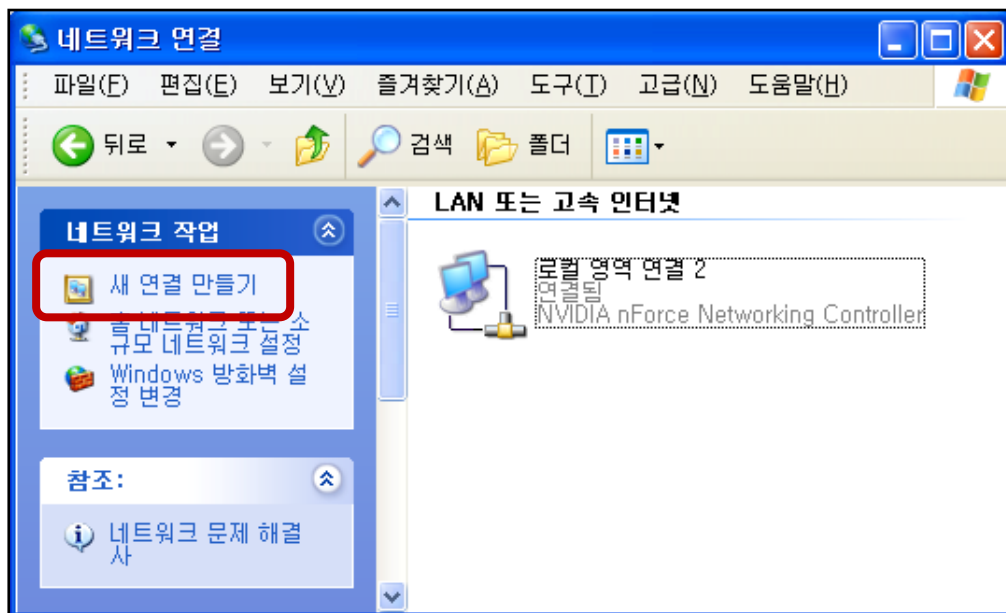
[참고] VPN을 구성하는 방법은 IPSec 또는 PPTP 등의 방법이 있으며, ipTIME은 PPTP 기반의 VPN을 지원한다.

8.1.1 Windows XP에서의 VPN 서버 접속

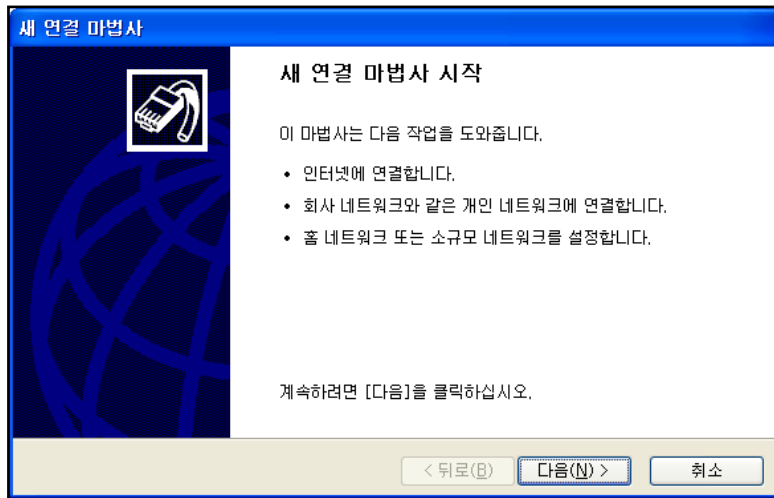
8.1장에서 설정한 VPN 서버로 Windows XP를 사용하는 VPN 클라이언트가 접속하는 과정입니다. VPN 서버에 접속하여 가상 사설망을 구축하기 위해서는 다음 (1),(2)의 설정을 진행하여 가상 사설망 어댑터를 설치 하여야 하며 한번 설정이 완료된 이후에는 (3)의 접속 방법을 통하여 연결합니다. (※ 가상 사설망 어댑터는 윈도우 운영 체제에서 제공됩니다.)

(1) 가상 사설망 어댑터 설치

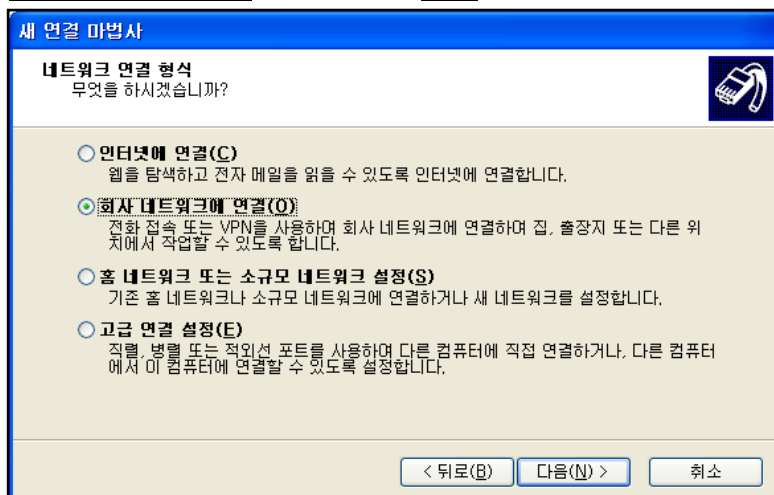
- 윈도우 좌측 하단의 **시작**을 클릭하고 **제어판** > **네트워크 및 인터넷 연결** > **네트워크 연결**로 접속하여, **새 연결 만들기**를 클릭합니다.



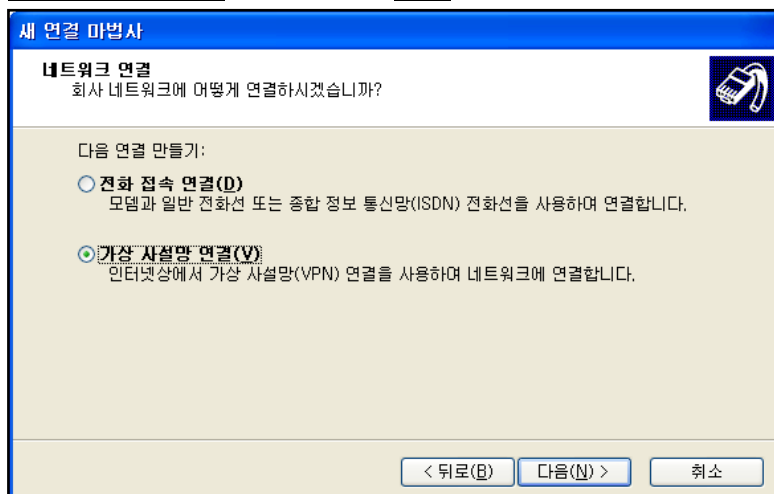
- 네트워크 연결 마법사가 실행되면 **[다음]** 버튼을 클릭합니다.



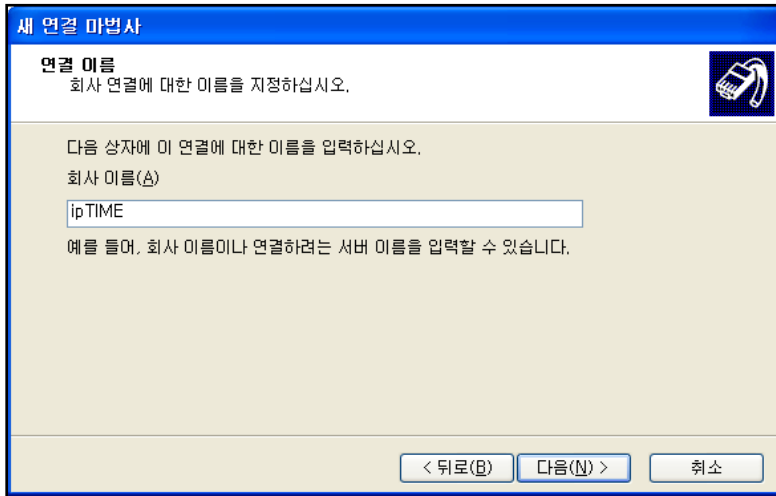
- **[회사 네트워크 연결]**을 선택하고, **[다음]** 버튼을 클릭합니다.



- **[가상 사설망 연결]**을 선택하고, **[다음]** 버튼을 클릭합니다.



- **회사이름**을 입력한 후, **다음** 버튼을 클릭합니다. (예. ipTIME, 임의입력 가능)



새 연결 마법사

연결 이름
회사 연결에 대한 이름을 지정하십시오.

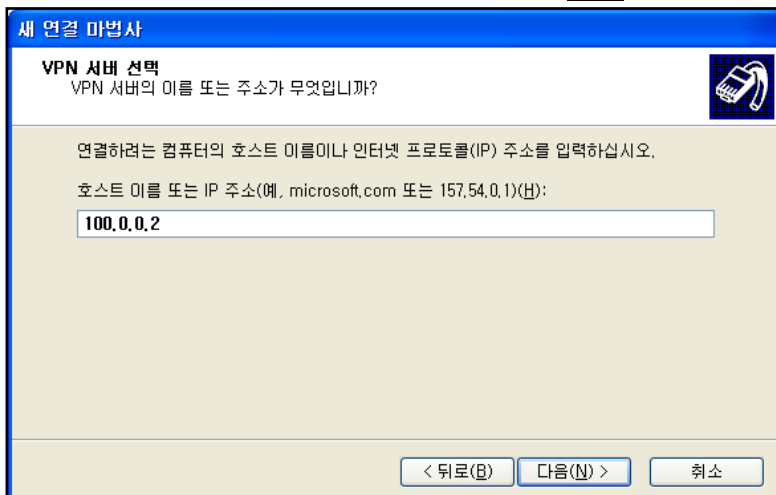
다음 상자에 이 연결에 대한 이름을 입력하십시오.
회사 이름(Δ)
ipTIME

예를 들어, 회사 이름이나 연결하려는 서버 이름을 입력할 수 있습니다.

< 뒤로(B) 다음(N) > 취소

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

- 연결하려는 VPN 서버의 IP 주소를 입력 후, **다음** 버튼을 클릭합니다.



새 연결 마법사

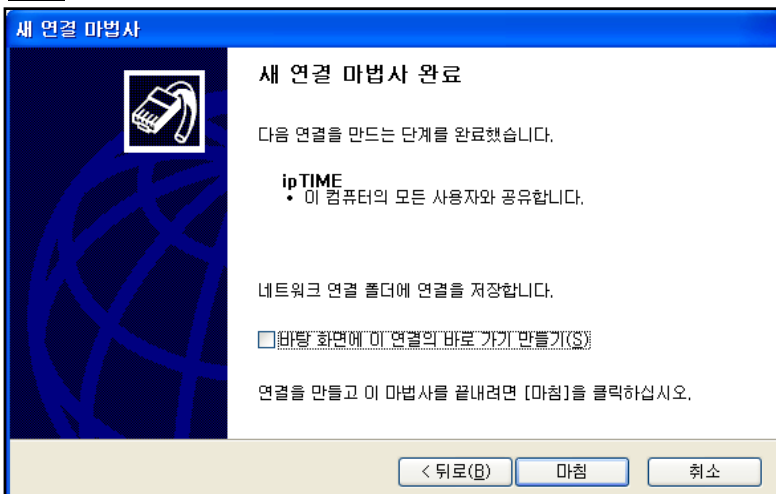
VPN 서버 선택
VPN 서버의 이름 또는 주소가 무엇입니까?

연결하려는 컴퓨터의 호스트 이름이나 인터넷 프로토콜(IP) 주소를 입력하십시오.
호스트 이름 또는 IP 주소(예, microsoft.com 또는 157.54.0.1)(H):
100.0.0.2

< 뒤로(B) 다음(N) > 취소

(본 예제에서는 VPN 서버 공유기의 외부IP인 100.0.0.2를 입력 하였습니다.)

- **마침** 버튼을 클릭하여 새 연결 마법사를 완료합니다.



새 연결 마법사

새 연결 마법사 완료

다음 연결을 만드는 단계를 완료했습니다.

ipTIME
• 이 컴퓨터의 모든 사용자와 공유합니다.

네트워크 연결 폴더에 연결을 저장합니다.

☐ **바탕 화면에 이 연결의 바로 가기 만들기(S)**

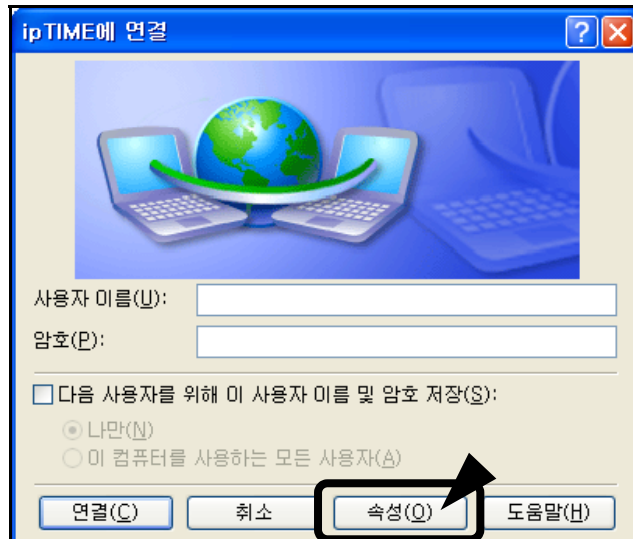
연결을 만들고 이 마법사를 끝내려면 [마침]을 클릭하십시오.

< 뒤로(B) 마침 취소

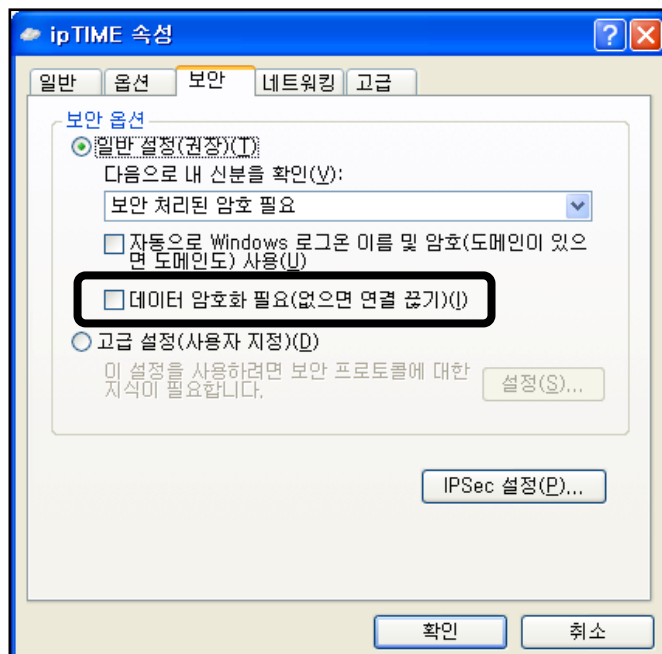
[참고] 바로 가기 생성 옵션을 선택하면 바탕화면에 접속 아이콘이 생성됩니다.

(2) 가상 사설 망 어댑터의 옵션 조정

- 생성된 연결을 실행하신 후, **속성** 버튼을 클릭합니다.

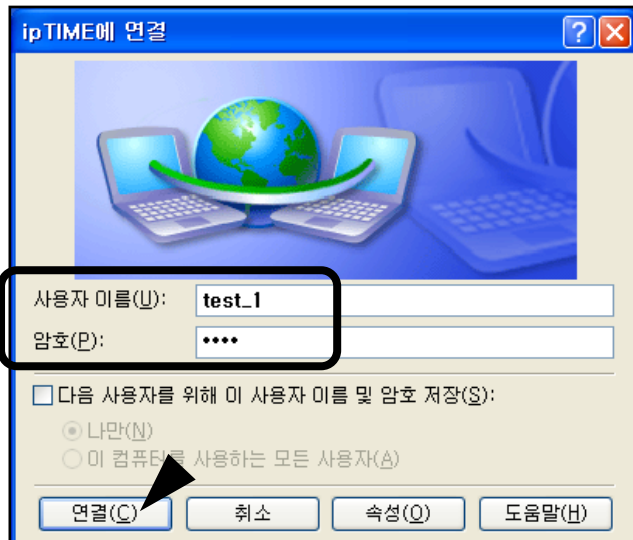


- **보안** 탭을 선택하고, **데이터 암호화 필요**의 체크를 해제 합니다.



(3) VPN 접속

- 바탕 화면의 단축 아이콘 또는 네트워크 등록 정보의 가상 사설망 어댑터 아이콘을 클릭합니다.
- 가상 사설 망 연결 프로그램이 실행되면 VPN 서버에 등록된 **사용자 이름**과 **암호**를 입력하고, **연결** 버튼을 클릭합니다.



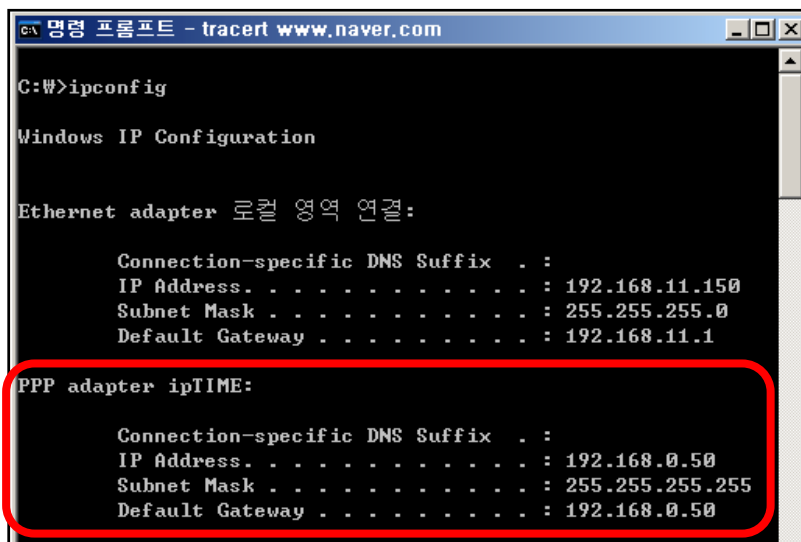
(예제에서는

- 사용자이름 : test_1,
 - 암호 :1234
- 를 사용하였습니다.

- 정상적으로 연결 되었다면 가상 사설망 연결이 아래와 같이 활성화 됩니다.



- VPN 서버로 사용할 공유기에 연결된 PC에서 윈도우 좌측 하단의 **시작** > **실행**을 클릭하고 "CMD"를 실행하여, 아래와 같이 ipconfig 명령어로 VPN 연결상태를 확인합니다.



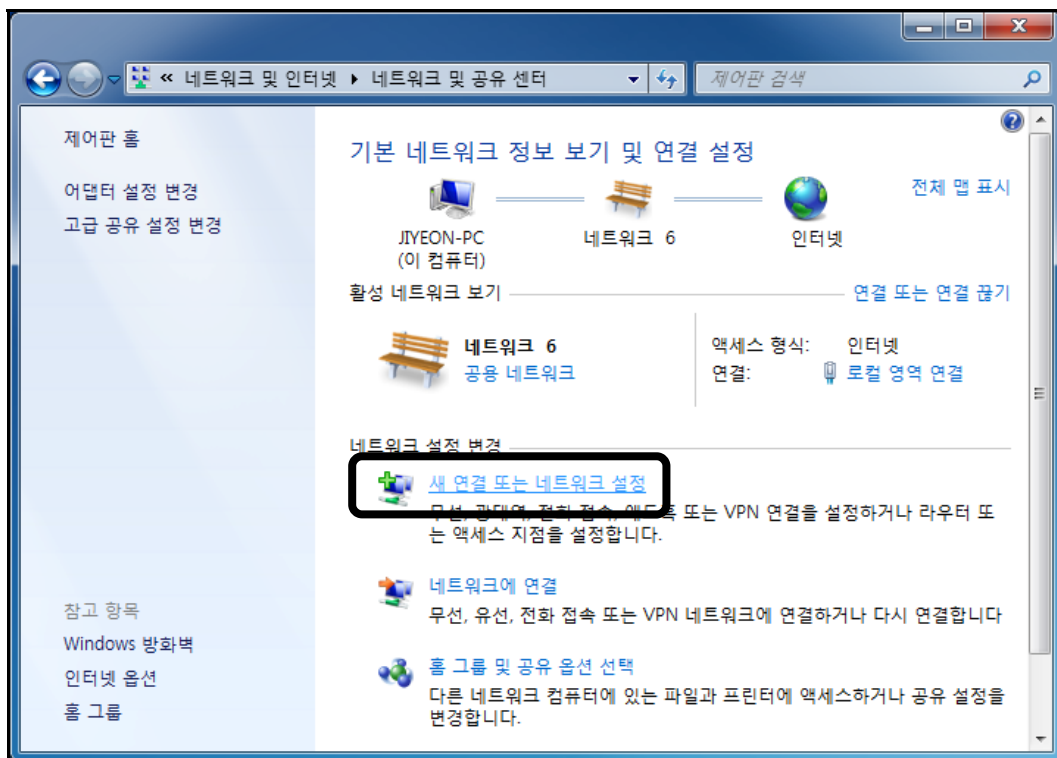
VPN Client의 네트워크에 PPP Adapter가 생성되어 VPN 서버에 설정한 IP인 192.168.0.50을 사용할 수 있음을 확인할 수 있습니다.

8.1.2 Windows 7에서의 VPN 서버 접속

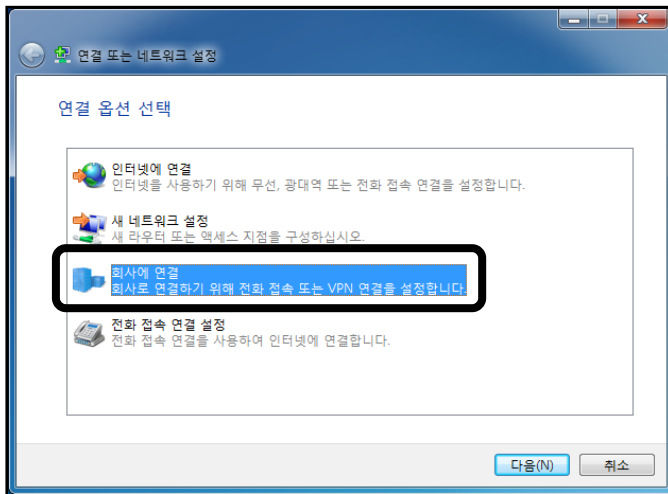
8.1장에서 설정한 VPN 서버로 Windows 7을 사용하는 VPN 클라이언트가 접속하는 과정입니다. VPN 서버에 접속하여 가상 사설망을 구축하기 위해서는 다음 (1)의 설정을 진행하여 가상 사설망 어댑터를 설치 하여야 하며 한번 설정이 완료된 이후에는 (2)의 접속 방법을 통하여 연결합니다. (※ 가상 사설망 어댑터는 윈도우 운영 체제에서 제공됩니다.)

(1) VPN 클라이언트 설정 및 연결

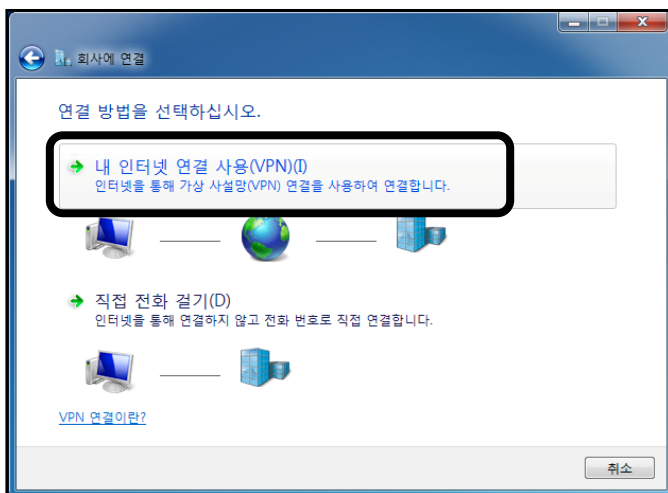
- 윈도우 좌측 하단의 [윈도우아이콘]을 클릭하고 [제어판] > [네트워크 및 인터넷] > [네트워크 및 공유 센터]로 접속하여, [새 연결 또는 네트워크 설정]을 클릭합니다.



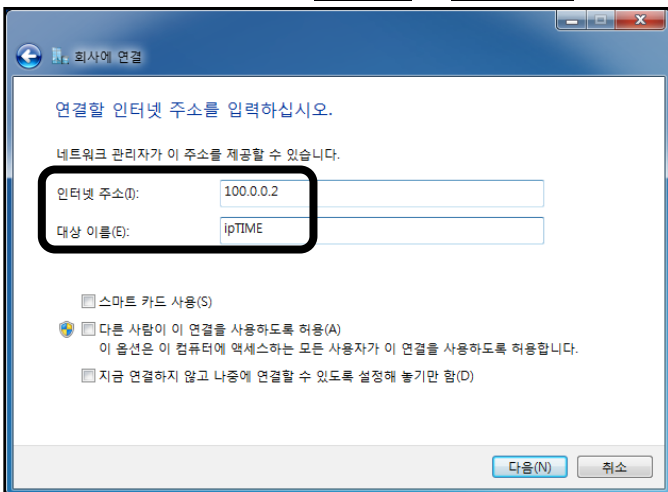
- 회사에 연결을 선택하고, 다음 버튼을 클릭합니다.



- 내 인터넷 연결 사용(VPN)을 선택합니다.



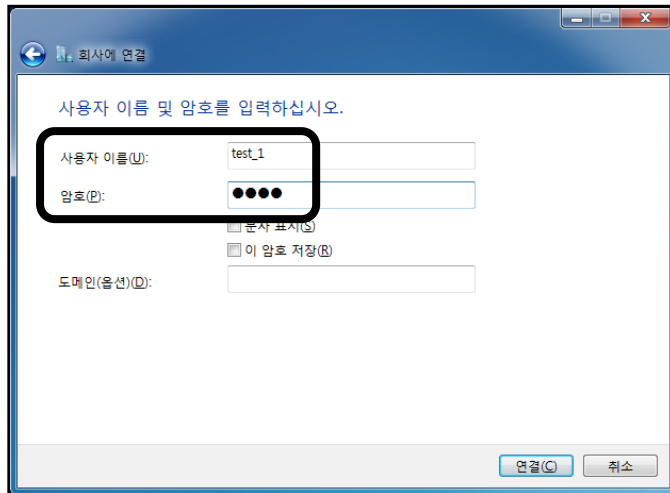
- 연결하려는 VPN 서버의 IP 주소와 대상 이름을 입력한 후, 다음 버튼을 클릭합니다.



(예제에서는 VPN 서버 공유기의 외부IP인 100.0.0.2를 입력 하였습니다.)

[참고] 대상 이름은 임의로 자유롭게 입력할 수 있으며, DDNS를 사용하면 DNS 이름으로 공유기에 접근할 수 있어 편리합니다.

- VPN 서버에 등록된 사용자 이름과 암호를 입력 하고, **연결** 버튼을 클릭합니다.



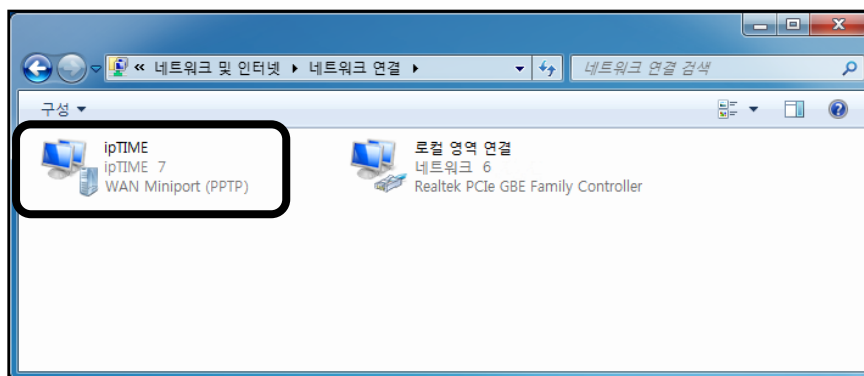
(예제에서는

- 사용자이름 : test_1,

- 암호 :1234

를 사용하였습니다.

- 정상적으로 연결 되었다면 WAN Miniport(PPTP) 아이콘이 아래와 같이 활성화 됩니다.

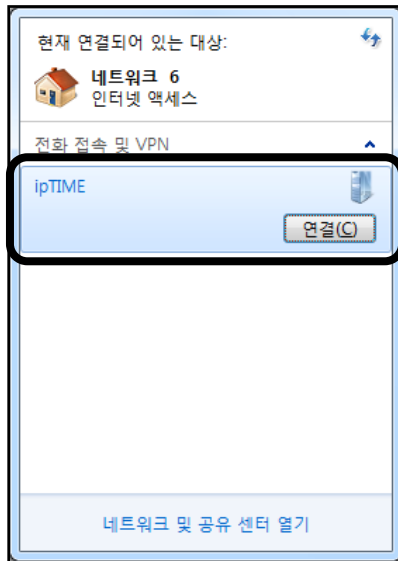


(2) VPN 접속

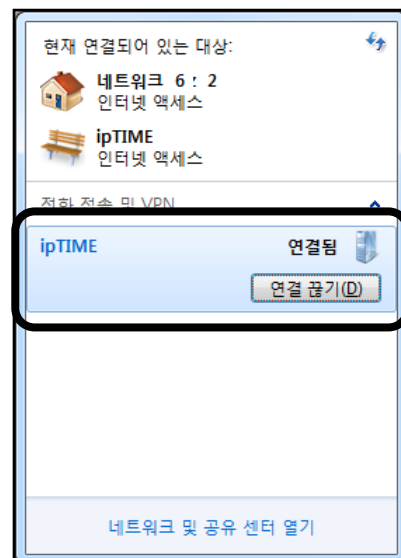
- 윈도우 우측 하단의 **네트워크 아이콘**을 클릭하여 **네트워크** 메뉴를 활성화 합니다.



- ipTIME을 선택하고 **연결** 버튼을 클릭합니다.



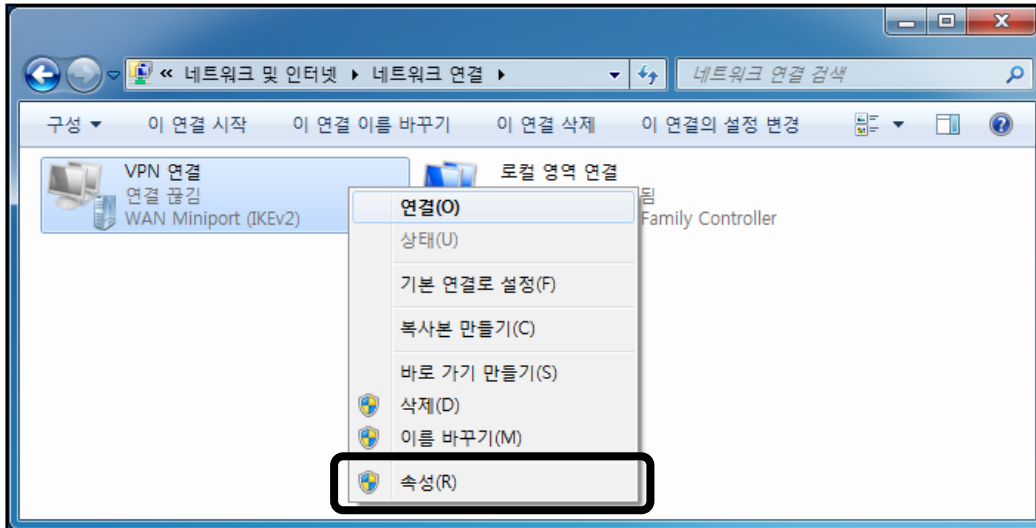
- VPN 서버에 등록된 사용자 이름과 암호를 입력 하고, **확인**버튼을 클릭합니다.
(예제에서는 사용자 이름 : test_1, 암호 : 1234를 사용하였습니다.)
- 정상적으로 연결되면 **연결됨**이라고 표시됩니다.



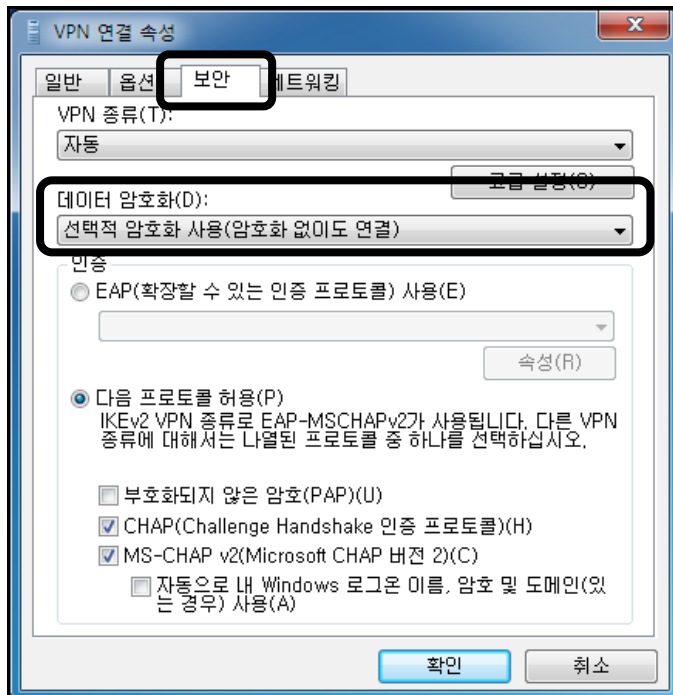
(3) 정상적으로 연결이 되지 않을 경우

- 윈도우 좌측 하단의 [윈도우 아이콘]을 클릭하고, [제어판] > [네트워크 및 인터넷] > [네트워크 연결] 메뉴로 이동합니다.

ipTIME 항목의 아이콘을 마우스 우측 버튼으로 클릭하여 [속성]을 선택합니다.



- 속성 창이 열리면 [보안] 탭으로 이동하여 [데이터 암호화] 항목을 아래와 같이 [선택적 암호화 사용(암호화 없이도 연결)]으로 선택하고 [확인] 버튼을 클릭합니다.

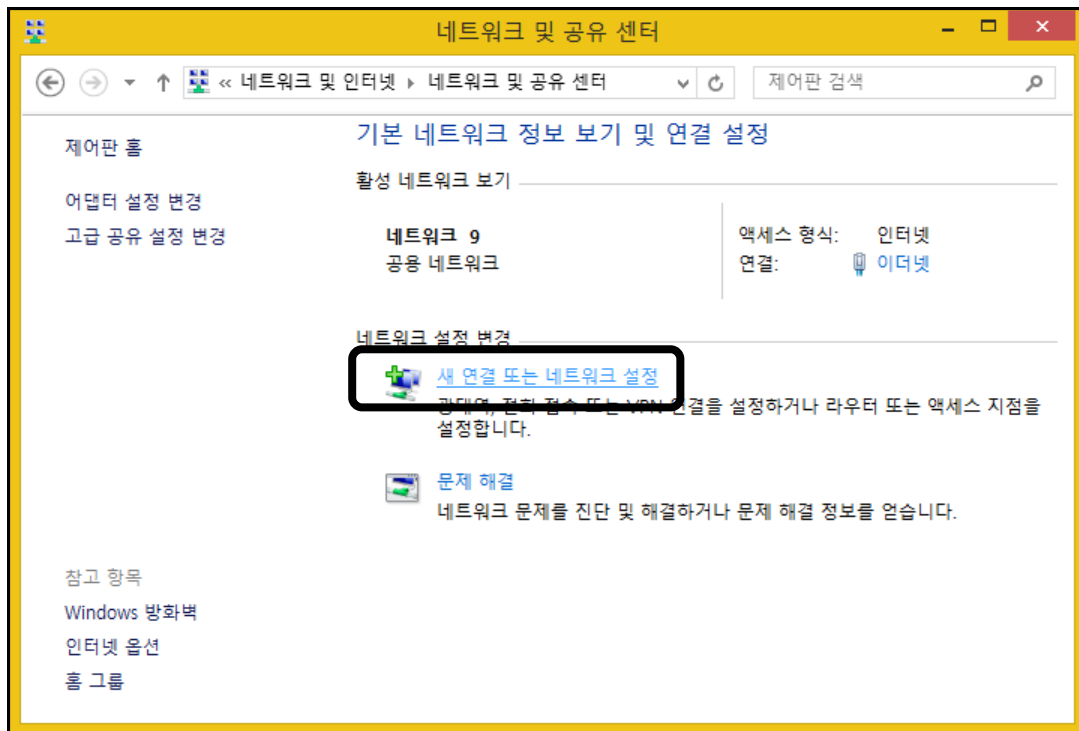


8.1.2 Windows 8.1에서의 VPN 서버 접속

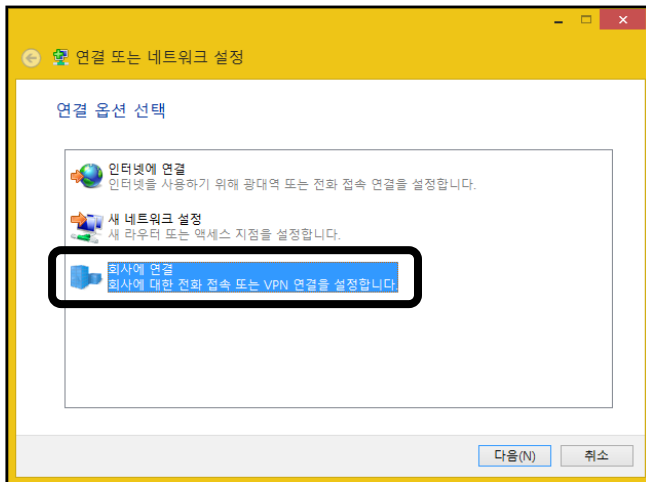
8.1장에서 설정한 VPN 서버로 Windows 8.1을 사용하는 VPN 클라이언트가 접속하는 과정입니다. VPN 서버에 접속하여 가상 사설망을 구축하기 위해서는 다음 (1)의 설정을 진행하여 가상 사설망 어댑터를 설치 하여야 하며 한번 설정이 완료된 이후에는 (2)의 접속 방법을 통하여 연결합니다. (* 가상 사설망 어댑터는 윈도우 운영 체제에서 제공됩니다.)

(1) VPN 클라이언트 설정 및 연결

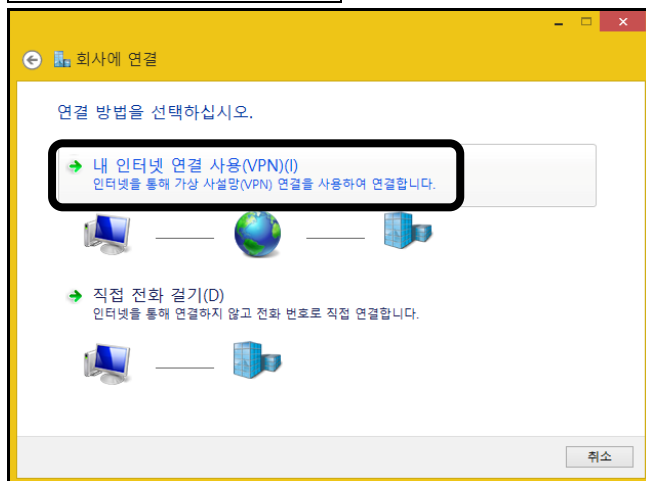
- 윈도우 좌측 하단의 **윈도우아이콘**을 마우스 오른쪽 버튼으로 클릭한 후, 메뉴에서 **제어판** > **네트워크 및 인터넷** > **네트워크 및 공유 센터**로 접속하여, **새 연결 또는 네트워크 설정**을 클릭합니다.



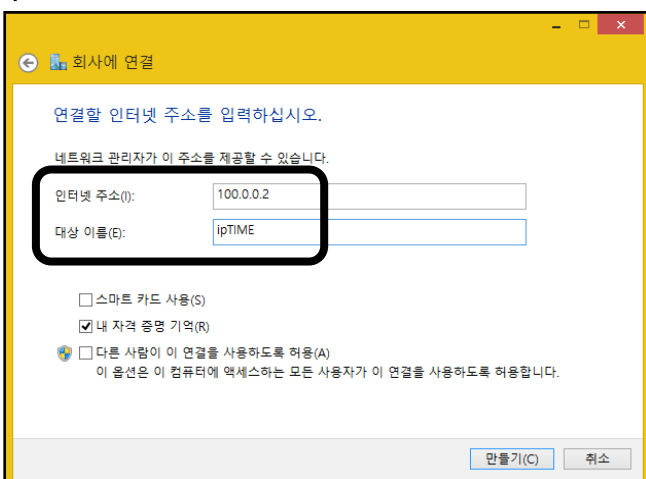
- 회사에 연결을 선택하고, 다음 버튼을 클릭합니다.



- 내 인터넷 연결 사용(VPN)을 선택합니다.



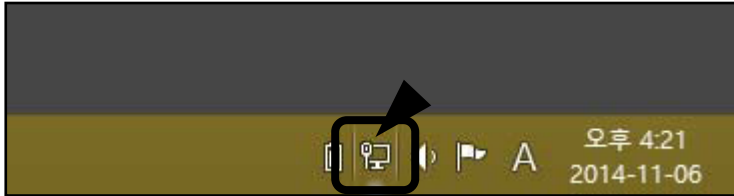
- 연결하려는 VPN 서버의 IP 주소와 대상 이름을 입력한 후, 만들기 버튼을 클릭합니다.
(본 예제에서는 VPN 서버 공유기의 외부IP인 100.0.0.2를 입력하였습니다.)



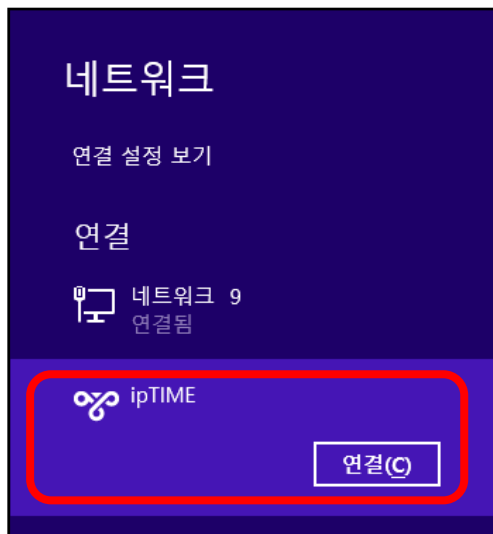
[참고] 대상 이름은 임의로 자유롭게 입력할 수 있으며, DDNS를 사용하면 DNS 이름으로 공유기에 접근할 수 있어 편리합니다.

(2) VPN 접속

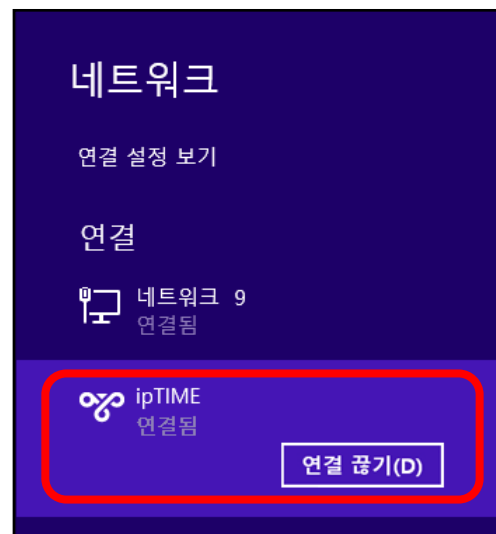
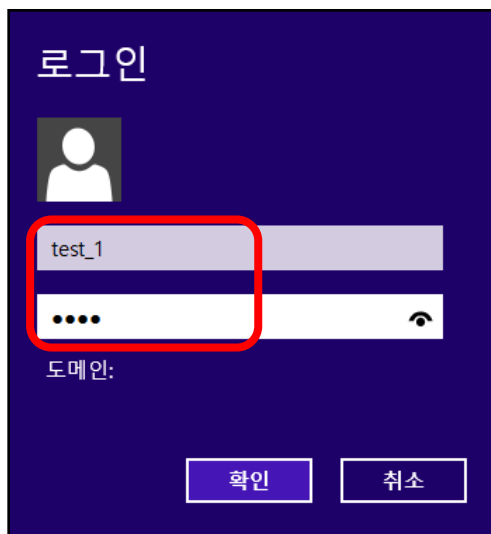
- 윈도우 우측 하단의 **네트워크 아이콘**을 클릭하여 **네트워크** 메뉴를 활성화 합니다.



- ipTIME을 선택하고 **연결** 버튼을 클릭합니다.



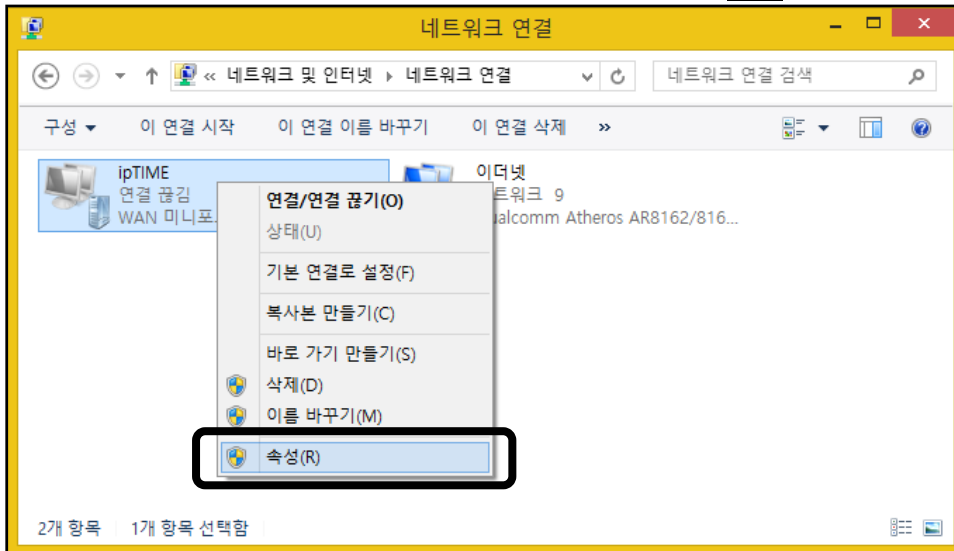
- VPN 서버에 등록된 사용자 이름과 암호를 입력 하고, **확인**버튼을 클릭합니다.
(예제에서는 사용자 이름 : test_1, 암호 : 1234를 사용하였습니다.)
- 정상적으로 연결되면 **연결됨**이라고 표시됩니다.



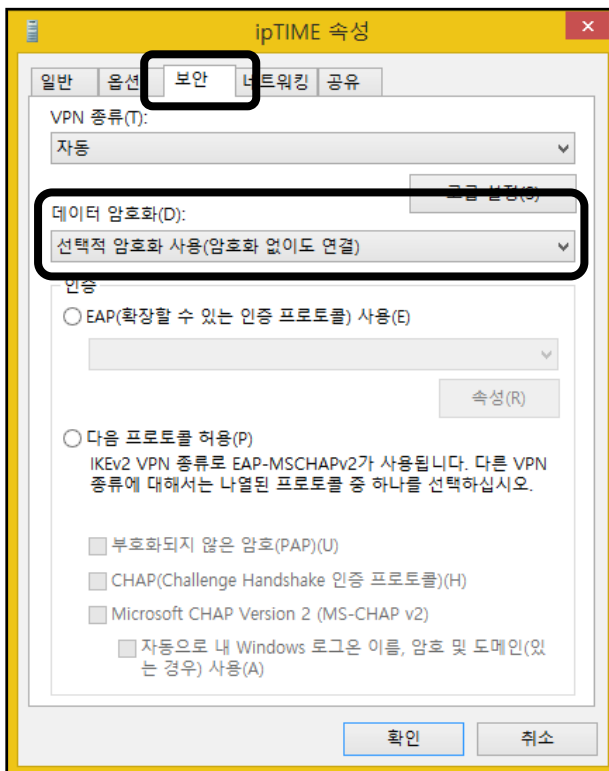
(2) 정상적으로 연결이 되지 않을 경우

- 윈도우 좌측 하단의 [윈도우 아이콘]을 클릭하고, [제어판] > [네트워크 및 인터넷] > [네트워크 연결] 메뉴로 이동합니다.

ipTIME 항목의 아이콘을 마우스 우측 버튼으로 클릭하여 [속성]을 선택합니다.



- 속성 창이 열리면 [보안] 탭으로 이동하여 [데이터 암호화] 항목을 아래와 같이 [선택적 암호화 사용(암호화 없이도 연결)]으로 선택하고 [확인] 버튼을 클릭합니다.



8.2 DDNS 설정

- 특수기능

- ☐ VPN 서버설정
- ☒ DDNS 설정
- ☐ WOL 기능
- ☐ 호스트검색
- ☐ 공지/광고 기능

유동 IP 주소에 도메인 이름을 지정하여 고정 IP 주소처럼 사용할 수 있습니다.

DDNS을 사용하면 매번 공유기의 외부 IP주소를 확인하지 않아도 편리하게 서버 운영을 할 수 도 있습니다.

- ipTIME에서는 ipTIME DDNS와 DynDNS를 지원합니다.
- ipTIME DDNS를 사용하기 위해서는 별도의 등록 절차 없이 공유기 설정만으로 사용할 수 있습니다.
- DynDNS 설정을 위해서는 먼저 www.dyndns.org 홈페이지에서 사용자 이름 및 도메인을 등록한 뒤 공유기를 설정하여야 합니다.

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

• ipTIME DDNS를 사용하실때에는 별도의 등록과정이 필요 없습니다.
 • 호스트이름은 iptime.org 로 끝나야 합니다. (예> testtest.iptime.org)
 • 사용자계정에는 E-mail주소를 입력해야 합니다.
 • 한 개의 호스트만 등록할 수 있습니다.

추가

호스트이름	기본 WAN	접속상태	접속상태 다시보기	갱신	삭제
ddnsiptime.iptime.org	wan1	등록 시도중		☐	☐

DDNS 동작을 위하여 설정할 항목은 다음과 같습니다.

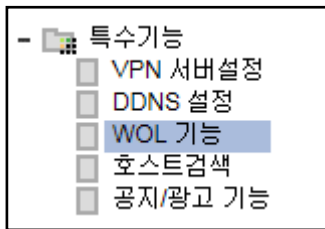
항목	설명
서비스 공급자	ipTIME DDNS 또는 DynDNS 서비스 공급자를 선택합니다.
호스트이름	DDNS 서비스에 사용할 호스트 이름을 설정 합니다.
사용자 계정	DDNS 서비스 이용을 위한 사용자 계정을 입력합니다. ipTIME DDNS를 사용할 경우에는 E-mail 주소를 사용자 계정으로 사용하셔야 합니다.
사용자 암호	DDNS 서비스 이용을 위한 사용자 계정의 암호를 입력합니다.
기본 WAN	DDNS에 등록될 IP주소의 WAN 포트를 선택합니다.

ipTIME DDNS 암호찾기

ipTIME DDNS 설정시 사용했던 E-mail주소를 입력 후 E-mail보내기 버튼을 클릭합니다.

- ipTIME DDNS 설정 시 사용자 계정으로 입력한 E-mail 주소를 입력한 후 **E-mail 보내기** 버튼을 클릭하시면 해당 메일주소로 암호가 발송 됩니다.

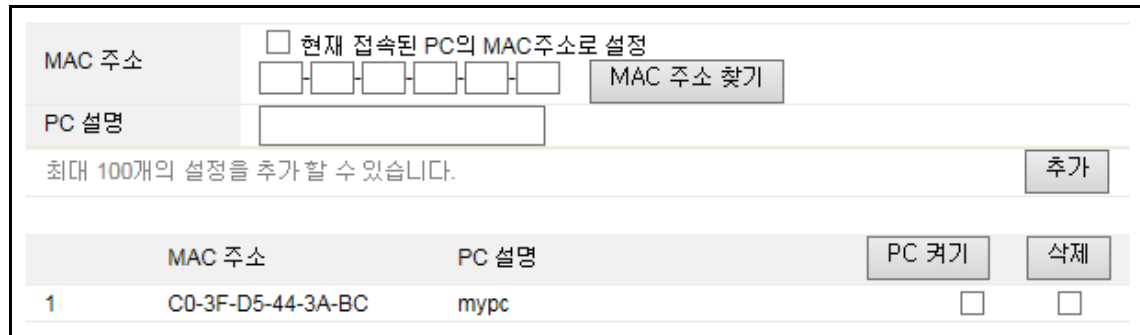
8.3 WOL 기능



WOL(Wake-up On Lan) 기능을 이용하면 공유기에 연결된 PC 전원을 켤 수 있습니다.

즉, WOL을 이용할 경우 인터넷을 통하여 공유기에 접속한 뒤 PC 전원을 켤 수 있기 때문에 사무실이나 가정에 설치된 PC를 외부 어디서든지 사용 하 실 수 있습니다.

- WOL을 이용하기 위해서는 PC에 WOL 기능을 제공하는 LAN 카드가 설치되어야 합니다
- 외부에서 PC를 사용하시기 위해서는 해당 PC에 Windows OS에서 제공하는 원격 데스크톱 기능(XP Professional 이상에서만 지원)을 활성화 하시거나, Remote Admin 또는 VNC 같은 어플리케이션을 이용하시면 됩니다.



	MAC 주소	PC 설명	PC 켜기	삭제
1	C0-3F-D5-44-3A-BC	mypc	☐	☐

WOL 동작을 위하여 설정할 항목은 다음과 같습니다.

항목	설명
MAC 주소	WOL 기능을 이용할 PC의 MAC 주소를 입력합니다.
PC 설명	해당 PC의 간단한 설명을 입력합니다..

- 등록된 리스트에서 'PC켜기' 항목을 체크하신 후에 **PC켜기** 버튼을 클릭하시면 해당 MAC 주소의 PC의 전원이 켜집니다.

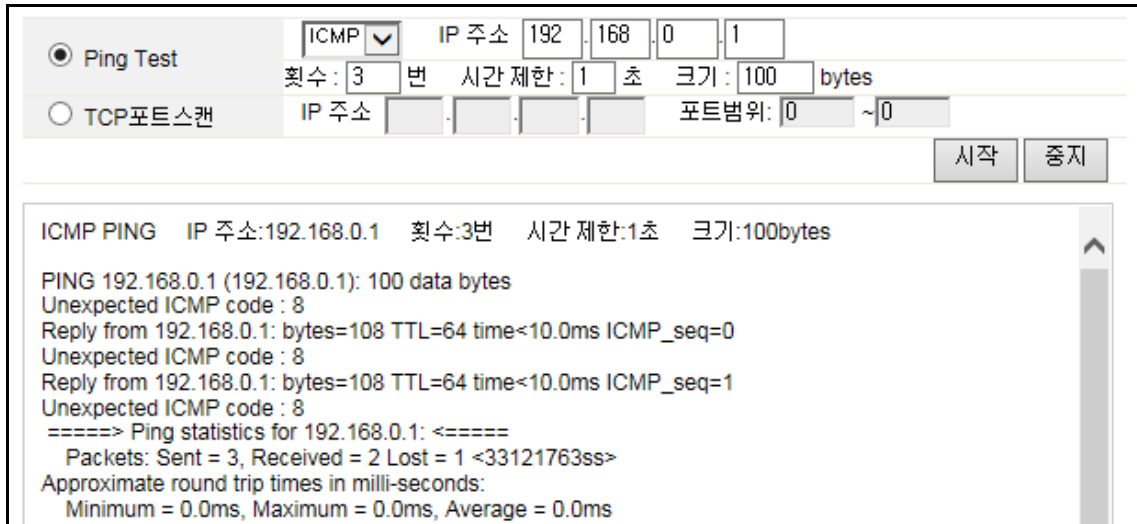
8.4 호스트검색

- 특수기능
 - ☐ VPN 서버설정
 - ☐ DDNS 설정
 - ☐ WOL 기능
 - ☒ 호스트검색
 - ☐ 공지/광고 기능

호스트 검색은 크게 Ping Test와 TCP포트스캔 두 가지 기능으로 나뉘며, Ping Test의 경우 [ICMP]와 [ARP]로 구분됩니다.

Ping Test - ICMP

Ping은 해당 컴퓨터에 소량의 패킷을 보내 되돌아 오는지를 확인하는 것으로 해당 단말(PC)과 지정한 단말(PC)간의 연결 상태를 확인할 수 있습니다.



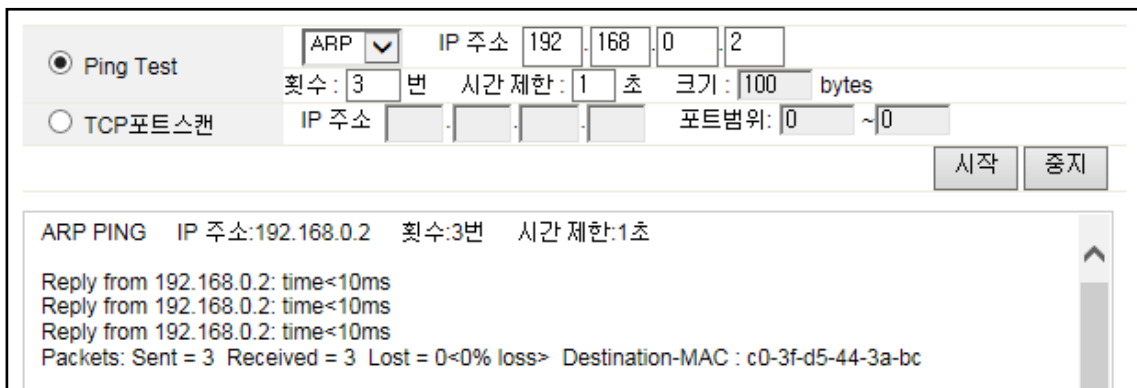
ICMP PING IP 주소:192.168.0.1 횟수:3번 시간 제한:1초 크기:100bytes

PING 192.168.0.1 (192.168.0.1): 100 data bytes
 Unexpected ICMP code : 8
 Reply from 192.168.0.1: bytes=108 TTL=64 time<10.0ms ICMP_seq=0
 Unexpected ICMP code : 8
 Reply from 192.168.0.1: bytes=108 TTL=64 time<10.0ms ICMP_seq=1
 Unexpected ICMP code : 8
 =====> Ping statistics for 192.168.0.1: <=====
 Packets: Sent = 3, Received = 2 Lost = 1 <33121763ss>
 Approximate round trip times in milli-seconds:
 Minimum = 0.0ms, Maximum = 0.0ms, Average = 0.0ms

- Ping Test항목에서 ICMP 선택하고 Test 대상의 IP주소를 입력한 후에 **시작** 버튼을 클릭하시면 됩니다.

Ping Test - ARP

지정한 IP주소를 가지고 있는 PC의 MAC 주소를 알아오는 테스트 방법입니다.



ARP PING IP 주소:192.168.0.2 횟수:3번 시간 제한:1초

Reply from 192.168.0.2: time<10ms
 Reply from 192.168.0.2: time<10ms
 Reply from 192.168.0.2: time<10ms
 Packets: Sent = 3 Received = 3 Lost = 0<0% loss> Destination-MAC : c0-3f-d5-44-3a-bc

- Ping Test항목에서 ARP 선택하고 Test 대상의 IP주소를 입력한 후에 **시작** 버튼을 클릭하시면 됩니다.

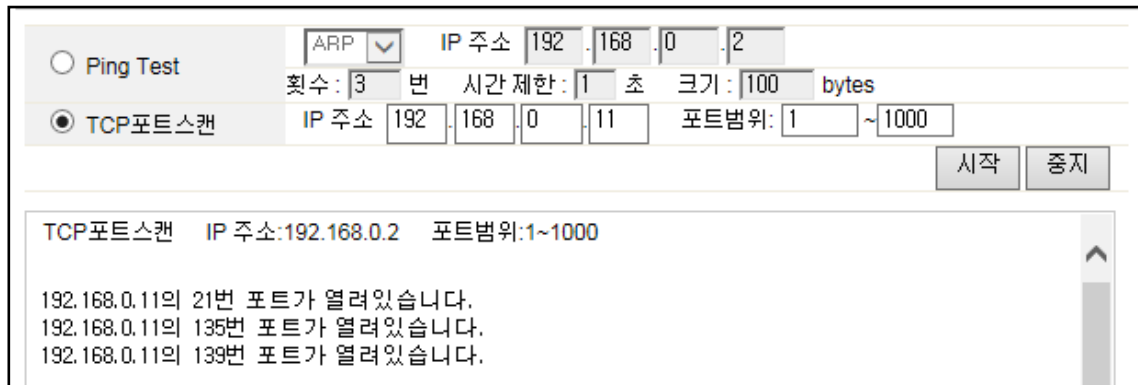
ARP 란?

Address Resolution Protocol의 약자로 상대방의 IP주소를 이용하여 IP주소가 가지고 있는 PC의 MAC 주소를 알아오는 주소 변환 프로토콜입니다.

서로 통신을 하기 위해서는 상대방 랜카드의 MAC 주소를 알고 있어야 하는데, 통신할 송신지(A)에서는 상대방의 MAC 주소를 알지 못하므로, 통신할 수신지(B)의 MAC 주소를 확인하기 위해, 브로드캐스트라는 통신 방법을 사용하여 상대방의 IP주소(B의 IP주소)로 ARP Request를 보내면, 그 IP주소를 가지고 있는 PC(B)가 ARP Response(응답)를 통해 송신지(A)에게 자신의 MAC 주소를 알려주는 과정입니다.

TCP포트스캔

지정한 IP 주소의 PC에서 어떤 TCP 포트가 개방되어 있는지 확인할 수 있는 기능입니다.



☐ Ping Test ☒ TCP포트스캔

ARP IP 주소: 192.168.0.2 횟수: 3 번 시간 제한: 1 초 크기: 100 bytes

IP 주소: 192.168.0.11 포트범위: 1 ~ 1000

시작 중지

TCP포트스캔 IP 주소:192.168.0.2 포트범위:1~1000

192.168.0.11의 21번 포트가 열려있습니다.
 192.168.0.11의 135번 포트가 열려있습니다.
 192.168.0.11의 139번 포트가 열려있습니다.

- TCP포트스캔 항목을 선택하고 IP주소를 지정하고 스캔 할 포트의 범위를 입력한 후에 **시작** 버튼을 클릭하시면 됩니다.

8.5 공지/광고 기능

- 특수기능

- ☐ VPN 서버설정
- ☐ DDNS 설정
- ☐ WOL 기능
- ☐ 호스트검색
- ☒ 공지/광고 기능

공지/광고 기능은 공유기에 최초로 연결된 사용자가 인터넷 익스플로러 실행 시에 설정된 URL로 자동으로 연결해 주는 기능입니다.

- 해당 URL로 접속된 후 하단의 확인 버튼을 누르면 정상적으로 인터넷 접속이 가능합니다.
- 10분 동안 인터넷을 사용하지 않으면, 최초로 연결된 사용자로 인식합니다.

공지/광고 페이지 설정

공지/광고 페이지 설정	
동작 설정	☒ 실행 ☐ 중단 http://www.iptime.com 공지/광고 할 페이지의 URL을 입력하시면 됩니다.
확인 버튼 사용자 문구	 (option) 공지/광고 페이지 확인 버튼에 사용 할 사용자 문구를 정의합니다.
확인 시 사용자 문구	 (option) 공지/광고 페이지 확인 시 사용 할 사용자 문구를 정의합니다.
확인 후 사용자 문구	 (option) 공지/광고 페이지 확인 후 사용 할 사용자 문구를 정의합니다.
White List	 (option) White List를 가져올 URL을 입력하시면 됩니다. ※ White List란 공지/광고 페이지에 연결되어 있는 다른 도메인 또는 IP주소에 대해서도 연결이 가능하도록 사전에 정의한 List를 의미합니다. ※ 입력 형태) http://advertise.domain.co.kr/whitelist ※ 응답 형태) www.facebook.com,111.112.113.114,211.212.213.0/24 도메인 또는 IP주소를 콤마(,)로 구분하여 나열하면 됩니다. 인터넷 접속을 요청한 사용자는 입력된 URL로 자동 연결이 되고, '확인' 버튼을 눌러야 정상적으로 인터넷 접속이 가능합니다.
적용	

실행을 선택하고, 지정하고자 하는 URL을 입력 후, **적용** 버튼을 클릭하여 설정내용을 적용합니다.

예외 기기

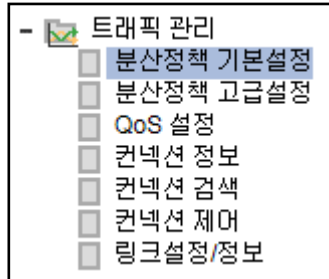
예외 기기에 등록한 IP주소를 사용하는 기기는 공지/광고 기능의 영향을 받지 않습니다.

예외 기기	
내부 IP주소	192 168 0 ~ 192 168 0
설명	
최대 10개의 설정을 추가 할 수 있습니다. 추가	

- 예외 기기의 IP주소를 입력하고, 설명을 입력한 후, **추가** 버튼을 클릭합니다.

9장 트래픽 관리

9.1 분산정책 기본설정



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.

분산 정책 설정에서는 두 개의 WAN 포트를 어떻게 사용할 것인가를 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 설정	WAN1, WAN2가 모두 인터넷에 연결되어 있는 경우 정해진 비율에 따라 인터넷 통신을 자동으로 분배하는 기능

라인 백업과 분산 정책에 따른 WAN1, WAN2의 인터넷 연결 경로

동작 조건				동작 설명
WAN 1	WAN 2	자동 분산 정책	자동 라인 백업	
ON	ON	ON	N.A	자동 분산 비율에 따라 WAN1/2 동시 통신 사용자 분산 정책은 정해진 경로로 통신
ON	ON	OFF	N.A	기본 분산 경로로만 통신 사용자 분산 정책이 있는 경우 별도 적용
ON	OFF	N.A	ON	모든 인터넷 WAN1으로 통신
ON	OFF	OFF	OFF	기본 분산 경로와 사용자 분산 정책이 WAN1인 경우만 인터넷 통신 가능
OFF	ON	N.A	ON	모든 인터넷 WAN2으로 통신
OFF	ON	OFF	OFF	기본 분산 경로와 사용자 분산 정책이 WAN2인 경우만 인터넷 통신 가능

[참고]

WAN을 하나만 연결하여 사용하시는 경우,

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

9.1.1 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	
기본 분산 경로	☒ WAN1 ☐ WAN2
적용	

<기본 분산 경로 입력 화면>

9.1.2 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	
동작 설정	☒ 실행 ☐ 중단
라인 백업 확인 주기	1 초 간격으로 3 회 검사
라인 백업 확인 방법	☒ ARP ☐ Ping ☐ DNS
자동 인터넷 라인 백업 기능을 동작시킵니다.	
적용	

<자동 인터넷 라인 백업 기능 설정 화면>

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

9.1.3 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.

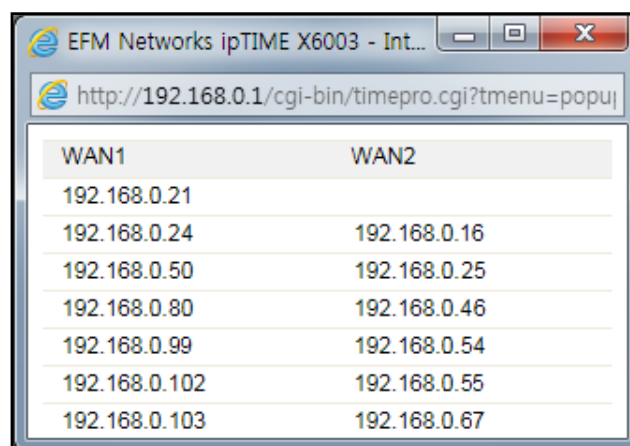
자동 분산 비율 설정			
동작 설정	☒ 실행 ☐ 중단		
분산 방법	☒ PC IP 주소 단위 분산 [STATUS]	WAN1	1
	☐ PC IP 주소 + 포트 단위 분산	WAN2	1
자동 분산 비율을 설정하는 경우라도 사용자정의 분산규칙은 우선적으로 적용됩니다.. 적용			

<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 선택 시 PC에서 발생하는 패킷의 목적지 포트에 따라 WAN1,2를 분산하여 통신하게 됩니다. 로그인이 필요한 웹 사이트 및 게임과 같은 경우 로그인을 다시 해야 하는 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.

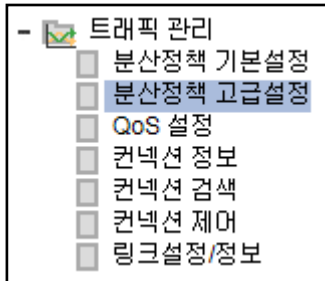


WAN1	WAN2
192.168.0.21	
192.168.0.24	192.168.0.16
192.168.0.50	192.168.0.25
192.168.0.80	192.168.0.46
192.168.0.99	192.168.0.54
192.168.0.102	192.168.0.55
192.168.0.103	192.168.0.67

<STATUS 화면>

단, 사용자정의 분산정책에서 'PC IP주소' 옵션값으로만 설정된 PC IP주소는 표시되지 않습니다.

9.2 분산정책 고급설정



분산정책 고급설정에서는 통신사별 분산 규칙과 사용자 정의 분산 정책을 어떻게 사용할 것인가를 결정합니다.

9.2.1 통신사(ISP)별 분산 규칙

목적지 IP주소를 관리하는 통신사(ISP)별로 분산 정책을 적용합니다.

사용 예

KT망에서 관리하는 목적지 IP주소로 통신하는 경우에는 WAN1으로,

SK브로드밴드망에서 관리하는 목적지 IP주소로 통신하는 경우에는 WAN2로 분산정책을 적용한 화면 입니다.

지정되지 않는 목적지 IP주소는 기본 분산 경로로 통신하게 됩니다.

통신사(ISP)별 분산규칙				
통신사(ISP)	☒ KT ☐ SK브로드밴드 ☐ 데이콤 ☐ 사용자정의 찾아보기...			
분산경로	☒ WAN1 ☐ WAN2			
최대 10개의 규칙이 설정 가능합니다.				추가
높은 번호일수록 우선순위가 높습니다.				
☐	동작	이름	분산경로	☐
☒	1	KT	WAN1	☐
☒	2	SK브로드밴드	WAN2	☐

<통신사(ISP)별 분산 규칙 화면>

9.2.2 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 분산규칙

규칙이름												
내부 IP 주소	192	168	0		~	192	168	0				
목적지 IP 주소					~							
프로토콜	any ▼											
시작지 포트		~						목적지 포트		~		
분산경로	☒ WAN1 ☐ WAN2										우선순위	

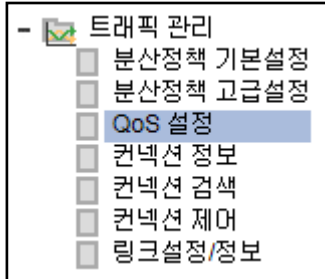
최대 60개의 규칙이 설정 가능합니다. 추가 취소

높은 번호일수록 우선순위가 높습니다.
규칙이름을 클릭하시면, 해당 규칙을 수정할 수 있습니다.

동작	규칙이름	분산 조건	분산경로	삭제
☐				☐
1 ☒	Group_A	내부 IP주소 192.168.0.2~192.168.0.100 목적지 IP any 프로토콜 any	WAN1	☐
2 ☒	Group_B	내부 IP주소 192.168.0.101~192.168.0.254 목적지 IP any 프로토콜 any	WAN2	☐

<사용자 정의 분산 정책 화면>

9.3 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 또는 어플리케이션 포트 번호에 근거하여 인터넷 대역폭을 제한하거나 보장할 수 있습니다.

QoS 기본설정

QoS 기본설정					
동작 설정	☐ 실행 ☒ 중단				적용
WAN1 Setup					
인터넷종류	사용자정의 ▼				
다운로드	0	Kbps ▼	업로드	0	Kbps ▼
					적용
WAN2 Setup					
인터넷종류	사용자정의 ▼				
다운로드	0	Kbps ▼	업로드	0	Kbps ▼
					적용
인터넷속도가 2.5Mbps인 경우에는 2500Kbps로 입력하세요. 소숫점단위로 설정할 수 없습니다. 정확한 인터넷 속도는 speed.nia.or.kr 에서 측정할 수 있습니다.					

QoS 기능의 정상적인 동작을 위해서는 공유기가 접속된 인터넷 속도에 대한 기본값을 정확히 설정합니다.

QoS 기본 설정을 위하여 설정할 항목은 다음과 같습니다.

항목	설명
동작 설정	실행 또는 중단 을 선택하여 QoS 동작을 설정합니다.
인터넷 종류 다운로드/업로드	해당 서비스의 다운로드와 업로드 속도가 자동으로 입력되며 인터넷 종류를 사용자 정의로 설정하면 다운로드 속도와 업로드 속도를 임의의 값으로 입력할 수 있습니다.

- QoS의 정확한 동작을 위해 <http://speed.nia.or.kr> 등의 속도 측정 사이트에서 정확한 인터넷 속도를 측정한 뒤 사용자 정의로 입력할 것을 권장합니다.
- 인터넷 속도를 수정하게 되면 이미 입력된 IP, 포트, 어플리케이션 별 QoS 설정 규칙이 무의미해지므로 설정된 규칙은 자동 삭제됩니다.

QoS 규칙설정

☒ 사용자 정의 설정 ☐ 어플리케이션 설정

동작 방법: 최대속도제한 ▼ 다운로드: 0 Kbps ▼ 업로드: 0 Kbps ▼

IP 주소: 192.168.0.0 ~ 192.168.0.0 ☐ IP 주소별 대역폭 개별할

☐ WAN1 Twin IP ☐ WAN2 Twin IP

WAN: WAN1 ▼

프로토콜: ----- ▼ 외부포트: ~

최대 31개의 규칙이 설정 가능합니다. 적용

☐ 사용자 정의 설정 ☒ 어플리케이션 설정

동작 방법: 최대속도제한 ▼ 다운로드: 0 Kbps ▼ 업로드: 0 Kbps ▼

IP 주소: 192.168.0.0 ~ 192.168.0.0 ☐ IP 주소별 대역폭 개별할

☐ WAN1 Twin IP ☐ WAN2 Twin IP

WAN: WAN1 ▼

어플리케이션: WWW(HTTP) ▼

최대 31개의 규칙이 설정 가능합니다. 적용

QoS 규칙 설정을 위하여 설정할 항목은 다음과 같습니다.

항목	설명
동작방법	최대속도제한: 과도한 인터넷 사용을 방지하기 위해 사용합니다. 최소속도보장: 일정한 수준 이상의 인터넷 속도가 보장되어야 하는 경우 사용합니다
다운로드/업로드	제한 또는 보장을 하기 위한 속도를 입력합니다.
IP 주소	규칙이 적용될 IP 주소를 입력합니다. 입력하지 않을 경우에는 모든 IP 주소가 적용 대상이 됩니다.
WAN	QoS 규칙을 적용할 WAN 포트를 선택합니다.
프로토콜/외부포트번호	규칙이 적용될 프로토콜과 해당 외부 포트번호를 입력합니다.
어플리케이션	규칙이 적용될 이미 정의된 어플리케이션을 선택합니다.

QoS 규칙설정 예제

* 최대 속도 제한

낮은 번호일수록 우선순위가 높습니다.
'최소속도보장'이 '최대속도제한' 보다 우선순위가 높습니다.

☒ 최대속도제한
 ☐ 최소속도보장

	IP 주소	조건	동작 방법	다운로드	업로드	삭제
						☐
1	192.168.0.4	[WAN1]	최대속도제한	2 Mbps	-----	☐
2	모든 IP 주소	[WAN2] WWW(HTTP)	최대속도제한	-----	512 Kbps	☐

QoS 설정 예	QoS 동작 방식
192.168.0.4 다운로드 2Mbps 최대 속도 제한	192.168.0.4는 WAN1로부터 2 Mbps 이상 다운 받을 수 없습니다. 다른 트래픽이 증가하면 다운로드의 속도는 2Mbps 이하가 될 수도 있습니다. 다른 트래픽이 없는 경우에도 다운로드의 속도는 2Mbps로 제한 됩니다
WWW(HTTP) 업로드 512Kbps 최대 속도 제한	WAN2로 512 Kbps 이상의 속도로 업로드 할 수 없습니다. 다른 트래픽이 증가하면 업로드의 속도는 512 Kbps 이하가 될 수도 있습니다. 다른 트래픽이 없는 경우에도 업로드의 속도는 512 Kbps로 제한 됩니다.

* 최소 속도 보장

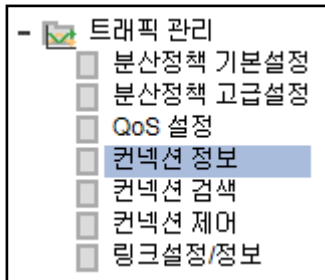
낮은 번호일수록 우선순위가 높습니다.
'최소속도보장'이 '최대속도제한' 보다 우선순위가 높습니다.

☐ 최대속도제한
 ☒ 최소속도보장

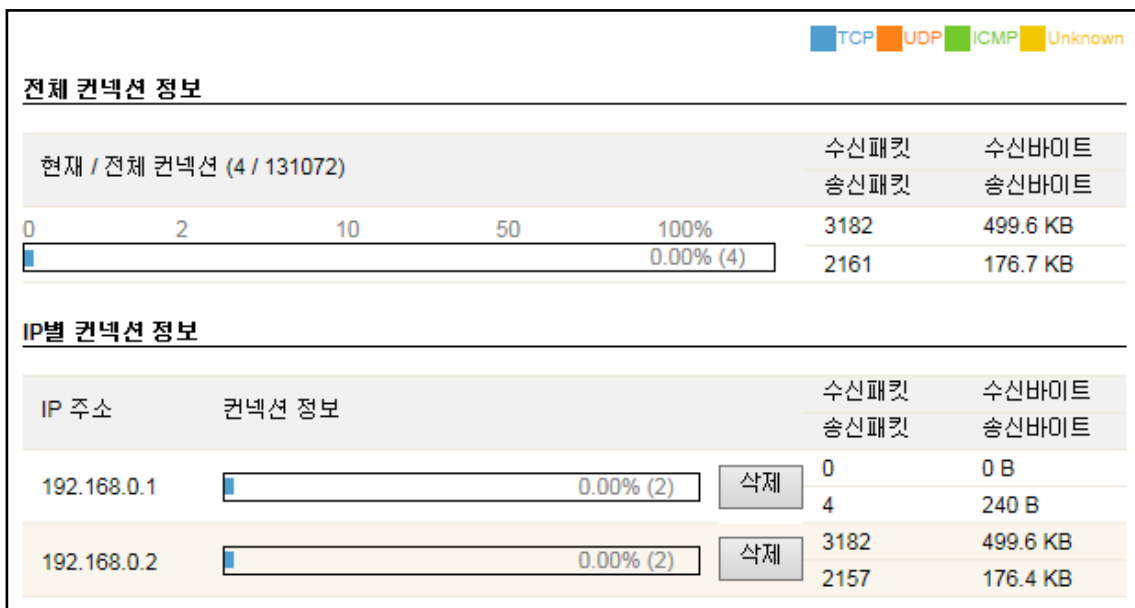
	IP 주소	조건	동작 방법	다운로드	업로드	삭제
						☐
1	192.168.0.100	[WAN1] TCP 8080	최소속도보장	3 Mbps	-----	☐

QoS 설정 예	QoS 동작 방식
TCP 8080 다운로드 3Mbps 최소 속도 보장	WAN1로부터 3 Mbps 이상의 속도로 다운로드 할 수 있습니다. 다른 트래픽이 증가해도 다운로드의 속도는 최소 3 Mbps 이상을 유지합니다. 다른 트래픽이 없는 경우 다운로드의 속도는 3Mbps 이상이 될 수 있습니다

9.4 컨넥션 정보



ipTIME에 연결되어 인터넷을 사용하는 PC들의 IP주소별로 사용되고 있는 컨넥션의 정보를 보여 줍니다.



전체 컨넥션 정보

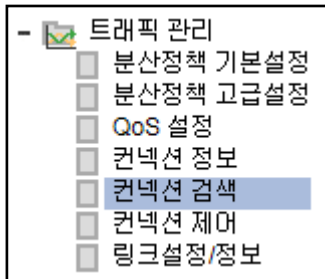
- 현재 통신하고 있는 모든 컨넥션의 개수를 알 수 있습니다.
- 전체 컨넥션의 수는 공유기가 가질 수 있는 최대 컨넥션 수를 나타냅니다.
- 현재 컨넥션 수가 전체 컨넥션 수와 같아지면 더 이상의 인터넷 연결을 할 수 없습니다.

IP 별 컨넥션 정보

- IP 주소란은 연결을 시작한 IP를 나타냅니다.
- 이 정보를 이용하여 과도한 컨넥션을 생성하는 PC를 찾아낼 수 있습니다
- IP 주소별 삭제 버튼을 클릭하시면 모든 컨넥션이 삭제됩니다. 만약 해당 IP 주소에서 파일 다운로드와 같은 통신을 하고 있다면 해당 통신은 끊어지게 됩니다.

항목	설명
TCP	대표적으로 HTTP 및 FTP에서 사용하는 프로토콜입니다.
UDP	P2P 검색 및 온라인 게임 등에서 많이 사용하는 프로토콜입니다.
ICMP	ping 명령어를 실행하였을 때 사용되는 프로토콜 입니다.
Unknown	3가지 프로토콜 이외의 다른 접속을 의미합니다.

9.5 컨넥션 검색



현재 통신하고 있는 모든 컨넥션을 필터링 옵션을 통해 검색할 수 있으며, 추가적으로 IP별/포트별/방향별로 분류하여 검색 할 수 있습니다.

필터링 옵션

항목	설명
내부 IP	설정된 내부 IP에 대한 컨넥션 정보를 검색합니다.
원격지 IP	설정된 원격지 IP에 대한 컨넥션 정보를 검색합니다.
프로토콜	설정된 IP Header의 프로토콜 번호에 대한 컨넥션 정보를 검색합니다.
TCP/UDP포트	IP Header의 프로토콜이 TCP/UDP일 경우, 설정된 포트 번호와 동일한 목적지 포트를 갖는 컨넥션 정보를 검색합니다.
컨넥션 방향	설정된 컨넥션 방향에 대한 컨넥션 정보를 검색합니다.
모든 TCP 연결 검색 하기	옵션이 꺼져 있는 경우에는 TCP 컨넥션 중, TCP연결 상태가 "ESTABLISHED"(연결됨)인 경우만 검색.
컨넥션 정보 자세히 보기	- 프로토콜/유지시간: 프로토콜이름(번호), 컨넥션 상태, 유지시간. - 시작 IP :포트(요청) : 최초에 연결을 요청한 IP및 포트번호. - 목적 IP :포트(요청) : 최초 연결 요청 시 목적지IP 및 목적지포트번호. - 방향 : 최초 연결 요청시의 방향을 나타냅니다.
속도/통신량 보기 옵션	- 속도(MB/s)보기:컨넥션의 데이터 통신 속도를 초당 Mega bytes 단위로 표시. - 통신량(Bytes)보기: 컨넥션의 데이터 통신량을 Byte단위로 표시.
초기 컨넥션 방향 별로 검색하기	[컨넥션 방향별 상태]를 검색 시, 컨넥션 생성 시, 최초 요청 방향별로 검색합니다.

전체 컨넥션 상태

통신중인 컨넥션에 대한 요약 정보를 표시합니다.

전체 컨넥션 상태 ▼ 검색 ☐ 필터링 옵션						
내부 IP	원격지 IP	프로토콜	포트	초기방향	다운로드 속도 (MB/s)	업로드 속도 (MB/s)
192.168.0.2	192.168.0.1	tcp(6)	80	LAN->MGMT	1.518	0.010
192.168.0.2	1.201.1.224	tcp(6)	5223	LAN->WAN1	0.000	0.000
192.168.0.2	120.50.133.141	tcp(6)	5004	LAN->WAN1	0.000	0.000

IP별 컨넥션 상태

특정 PC(IP)가 점유하고 있는 인터넷 대역폭(MB/s), 사용량(Bytes), 그리고 컨넥션 수를 검색할 수 있습니다.

IP별 컨넥션 상태 ▼ 검색 ☐ 필터링 옵션					
내부 IP	컨넥션 수	다운로드 속도 (MB/s)	업로드 속도 (MB/s)	다운로드 통신량 (Bytes)	업로드 통신량 (Bytes)
192.168.0.2	17	2.443	0.036	508,026	54,330

TCP/UDP 포트별 컨넥션 상태

특정 어플리케이션(프로토콜, 포트)이 점유하고 있는 인터넷 대역폭(MB/s), 사용량(Bytes), 컨넥션 수를 검색할 수 있습니다.

TCP/UDP 포트별 컨넥션 상태 ▼ 검색 ☐ 필터링 옵션						
프로토콜	포트	컨넥션 수	다운로드 속도 (MB/s)	업로드 속도 (MB/s)	다운로드 통신량 (Bytes)	업로드 통신량 (Bytes)
tcp(6)	80	10	2.213	0.036	188,264	4,116
tcp(6)	5004	1	0.000	0.000	97,103	40,392
tcp(6)	5223	1	0.000	0.000	9,699	5,273
udp(17)	53	1	0.000	0.000	1,952	1,272

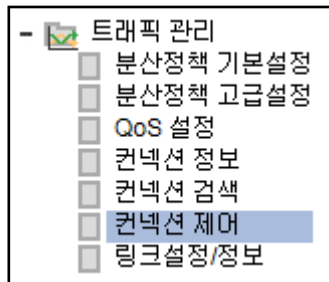
컨넥션 방향별 상태

컨넥션 방향별 상태 ▼ 검색 ☐ 필터링 옵션						
방향	컨넥션 수	다운로드 속도 (MB/s)	업로드 속도 (MB/s)	다운로드 통신량 (Bytes)	업로드 통신량 (Bytes)	
LAN <-> WAN1	13	0.000	0.000	112,340	49,355	
LAN <-> WAN2	0	0.000	0.000	0	0	
LAN <-> MGMT	2	2.751	0.037	187,016	2,707	
MGMT <-> WAN1	0	0.000	0.000	0	0	
MGMT <-> WAN2	0	0.000	0.000	0	0	
LAN<->MGMT	0	0.000	0.000	0	0	
MGMT<->LAN	0	0.000	0.000	0	0	

[컨넥션 방향 용어설명]

항목	설명
->	단방향
<->	양방향
LAN	내부 네트워크
WAN1,WAN2	외부 네트워크(WAN2:2 WAN제품군일 경우)
MGMT	공유기 자체 네트워크

9.6 컨넥션 제어



공유기가 NAT를 수행하기 위한 컨넥션 테이블을 관리할 수 있는 메뉴입니다.

이 기능은 네트워크 기술에 익숙한 전문가용 설정입니다.

컨넥션 수 제어

최대 컨넥션 수	131072	개 (0 : 제한 없음, 512 ~)
최대 UDP 컨넥션 수	100000	개 (0 : 제한 없음, 10 ~ 최대 컨넥션 수)
최대 ICMP 컨넥션 수	100000	개 (0 : 제한 없음, 1 ~ 최대 컨넥션 수)
PC별 최대 컨넥션 비율	0	% (0 : 제한 없음, 1 ~ 100)

최대 컨넥션 수 - 공유기가 관리할 수 있는 최대 컨넥션 수입니다. P2P 어플리케이션 등을 위해 컨넥션 수를 많이 필요로 하는 경우에 기본값 보다 큰 값을 사용하십시오.

최대 UDP컨넥션 수 - UDP 통신을 위한 최대 컨넥션 수를 설정합니다. 0 으로 설정할 경우에는 [최대 컨넥션 수] 만큼 컨넥션을 만들 수 있습니다.

최대 ICMP 컨넥션 수 - ICMP 통신을 위한 최대 컨넥션 수를 설정합니다. 0 으로 설정할 경우에는 [최대 컨넥션 수] 만큼 컨넥션을 만들 수 있습니다.

PC별 최대 컨넥션 비율 - 한 대의 PC가 모든 컨넥션을 독점하지 않도록, 한 대의 PC 당 컨넥션의 비율을 설정하는 기능입니다. 컨넥션의 비율은 [최대 컨넥션 수]를 기준으로 계산합니다. (예> 최대 컨넥션 수가 8196일 경우 25%로 설정하면, 한 대의 PC는 2048개 의 컨넥션을 만들 수 있습니다.)

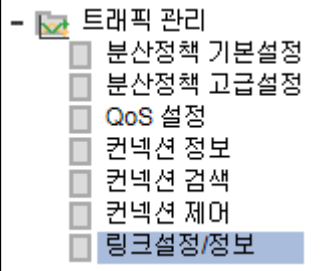
컨넥션 타임아웃 제어

TCP SYN SENT TIMEOUT	20	초	TCP SYN RECV TIMEOUT	60	초
TCP ESTABLISHED TIMEOUT	86400	초	TCP FIN WAIT TIMEOUT	120	초
TCP CLOSE WAIT TIMEOUT	60	초	TCP LAST ACK TIMEOUT	30	초
TCP TIME WAIT TIMEOUT	10	초	TCP CLOSE TIMEOUT	10	초
UDP TIMEOUT	30	초	UDP STREAM TIMEOUT	180	초
ICMP TIMEOUT	30	초	GENERIC TIMEOUT	600	초

컨넥션의 상태에 따른 타임 아웃 값을 조절 할 수 있습니다.

* 주의 : 이 기능은 네트워크 전문가용 설정입니다. 특별한 경우를 제외하고는 기본값을 사용하십시오.

9.7 링크설정/정보



WAN, LAN포트의 동작모드, 속도, Duplex 및 개별 포트의 통신량을 확인할 수 있으며, 특정 포트의 속도를 자동 또는 수동으로 결정 할 수 있습니다.

링크 설정					
포트 번호	동작 모드	속도	Duplex		
WAN1	자동 ▼	1Gbps ▼	FULL ▼	적용	
WAN2	자동 ▼	1Gbps ▼	FULL ▼	적용	
1	자동 ▼	1Gbps ▼	FULL ▼	적용	
2	자동 ▼	1Gbps ▼	FULL ▼	적용	
3	자동으로 고정				

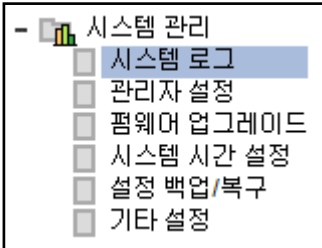
링크통계 정보					
포트 번호	WAN1	WAN2	1	2	3
Rx-Packets	270430	0	0	0	247571
Rx-Bytes	249459207	0	0	0	34834074
Rx-Broadcast	1518	0	0	0	1136
Rx-Multicast	1916	0	0	0	618
Rx-Error(CRC)	0	0	0	0	0
Rx-Error(Drop)	0	0	0	0	0
Rx-Pause	0	0	0	0	0
Tx-Packets	235548	0	0	0	249767
Tx-Bytes	34515642	0	0	0	281744386
Tx-Broadcast	211	0	0	0	38
Tx-Multicast	6	0	0	0	1639
Tx-Collision	0	0	0	0	0
Tx-Pause	0	0	0	0	0

통계정보 초기화

- ipTIME 모델마다 LAN포트의 수 및 지원되는 정보가 달라질 수 있습니다.

10장 시스템 관리

10.1 시스템 로그



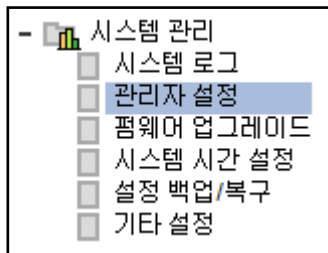
시스템 로그 기능을 이용하면 공유기의 동작 내역을 확인할 수 있으며 저장된 로그를 E-mail 로 전송할 수 있습니다.

최대 개수 400개가 초과하게 되면 가장 오래된 로그내역부터 삭제되고 최신 로그내역이 추가됩니다.

시스템 로그 설정	
로그 기능 설정	☒ 실행 ☐ 중지 적용
로그 기능 상태	로그갯수(최대갯수) : 14(400) 전체 삭제
E-mail 보고 기능	[관리자 E-mail을 설정] 하여야 E-mail 보고기능을 사용할수 있습니다.

시스템 로그 보기	
발생시간	로그 내용
2014/11/05 17:10:15	IP : 192.168.0.2 LOGIN 성공
2014/11/05 15:23:26	IP : 192.168.0.2 LOGIN 성공
2014/11/05 14:36:26	WAN1 인터넷 연결 복원
*****	PPP가 연결되어 IP를 받음: 61.77.134.65 (wan1)
*****	WAN1 인터넷 연결 끊김. WAN2로 백업
*****	관리자가 인터넷 설정을 변경함: 동적 IP -> PPPoE 방식
*****	IP : 192.168.0.2 LOGIN 성공
*****	DHCP 서버가 IP 할당함: 192.168.0.2 (MAC : C0-3F-D5-44-3A-BC)
*****	DHCP Server 응답없음 (wan1)
*****	시스템 재시작 (Version: 9.10)

10.2 관리자 설정



설정 웹 서버 접속 시 사용되는 관리자의 계정 및 암호를 설정할 수 있고 시스템 로그 및 네트워크 감시 보고서에서 사용할 수 있는 관리자 E-mail 주소를 설정 할 수 있습니다.

현재 계정 및 암호	계정 - 설정되지 않음	암호 - 설정되지 않음
새 계정		
새 암호		
새 암호 확인		
적용		

로그인 인증 방법 설정

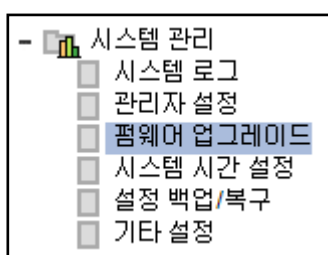
인증 방법	☒ 기본방식
	☐ 세션방식
	10 분간 미사용시 자동 로그 아웃
☐ 로그인시 문자열 입력(Captcha Code)	
적용	

관리자 E-Mail 설정

관리자 E-Mail	
메일서버(SMTP)	
보내는 E-Mail	
메일 서버 인증	☐ 사용할 ☒ 사용하지 않음
메일 서버 계정	
암호	
적용	

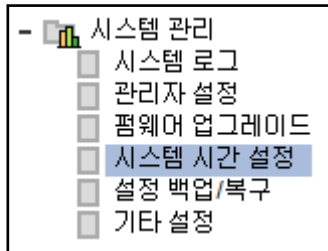
- 공장 출하 시 계정과 암호는 별도로 설정되어 있지 않습니다.
- 로그인 암호를 잊어버린 경우 리셋 스위치를 이용 공장초기화 방법으로 초기화합니다

10.3 펌웨어 업그레이드



새로 배포되는 ipTIME 펌웨어를 해당 메뉴에서 업그레이드 할 수 있습니다
자세한 내용은 4장 기본설정의 4.3절 펌웨어 업그레이드를 참고합니다.

10.4 시스템 시간 설정

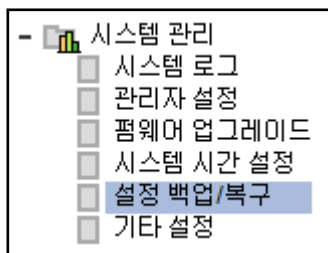


공유기가 인터넷에 연결되었을 때 시스템 시간을 얻어오는 서버와 표준 시간대를 입력합니다. 원하는 Time Server와 시간대를 선택한 후 적용 버튼을 클릭합니다.

현재 시스템 시간	2014년 11월 5일 수요일 18시 1분 1초	
Time Server 설정	time.windows.com ▼	time.windows.com
표준시간대	☐ 일광절약시간제 적용 (GMT+09:00) 서울, 도쿄 ▼	
적용		

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

10.5 설정 백업/복구



공유기의 설정을 PC로 저장하거나, PC에 저장해둔 설정파일을 공유기에 적용 할 수 있습니다. 또는 공장 초기화 상태로 설정을 복원할 수 도 있습니다.

설정 파일 백업	모든 설정을 설정파일로 저장하여 PC로 다운로드합니다. PC에 저장된 설정파일은 설정 복구시 사용됩니다.
찾아보기...	
설정 파일 복구	PC에 저장해둔 설정파일을 이용해 설정을 복구합니다.
초기 설정 복원	시스템의 모든 설정이 초기화된 후 다시 시작 됩니다.

항목	설명
설정 파일 백업	모든 설정을 설정파일로 저장하여 PC로 다운로드 합니다.
설정 파일 복구	PC에 저장해둔 설정파일을 이용해 설정을 복구합니다.
초기 설정 복원	시스템의 모든 설정이 초기화된 후 재시작 됩니다.

10.6 기타 설정

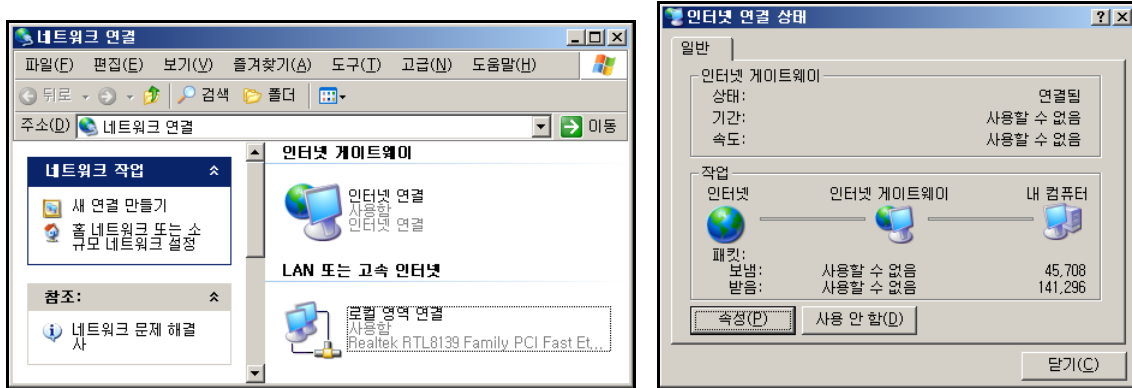
- 시스템 관리
 - 시스템 로그
 - 관리자 설정
 - 펌웨어 업그레이드
 - 시스템 시간 설정
 - 설정 백업/복구
 - 기타 설정**

공유기의 이름 설정 및 UPNP 설정 등의 기타 기능들의 동작여부를 설정할 수 있습니다.

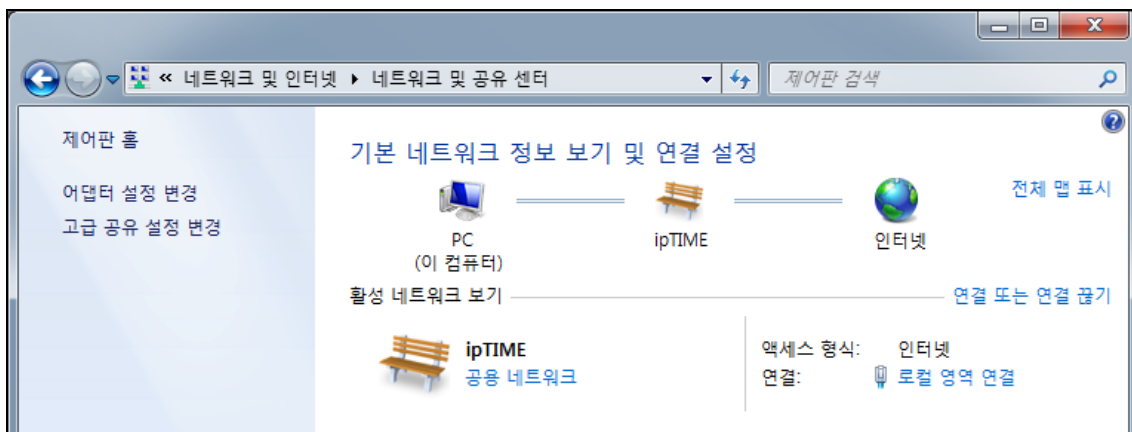
공유기 이름		적용
자동 설정 저장	☒ 실행 ☐ 중단	적용
설정 화면 자동 연결	☐ 실행 ☒ 중단 인터넷 끊김시 공유기 설정 화면으로 자동으로 연결되는 기능	적용
로그인 페이지 설정	☒ 설정 화면 접속시 로그인 페이지를 보여줍니다. ☐ 설정 화면 접속시 로그인 페이지를 보여주지 않습니다.	적용
관리도구 접속방법	☐ 팝업으로 새 창 띄움 ☒ 현재 창 사용	적용
UPNP 설정	☒ 실행 ☐ 중단 UPNP 포트포워딩 리스트	적용
나이트 LED모드	☒ 기본 모드 ☐ 항상 끄 ☐ 22시 부터 9시 까지 공유기의 LED를 끕니다. * 일부 LED는 꺼지지 않을 수 있습니다.	적용
HTTP URL TAG	☐ 실행 ☒ 중단	적용
공유기 다시 시작	공유기가 다시 시작된 후 "기타 설정" 페이지로 접속됩니다.	적용
원격 지원	☐ 실행 ☒ 중단	적용
서비스 네트워크	192 168 255 0	적용

항목	설명
공유기 이름	공유기 이름은 웹 설정 화면의 인터넷 탐색기 상단에 표시되는 Title입니다. 원하는 공유기 이름을 입력하고 적용 버튼을 클릭하면 이름이 변경됩니다. 또한, 로그파일을 관리자 메일로 전송 시 메일의 제목에 포함됩니다.
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.
로그인 페이지 설정	공유기의 웹 설정 화면에 접속하는 경우 최초 표시되는 로그인 화면을 보여줄지 여부를 결정합니다.
관리도구 접속방법	팝업으로 새 창 띄움 - 관리도구 클릭 시 새 창을 띄웁니다. 현재 창 사용 - 관리도구 클릭 시 현재 창으로 관리도구가 접속됩니다.
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.
공유기 다시 시작	공유기를 재시작 합니다. 만약 저장하지 않은 설정이 있다면 지워지게 됩니다.

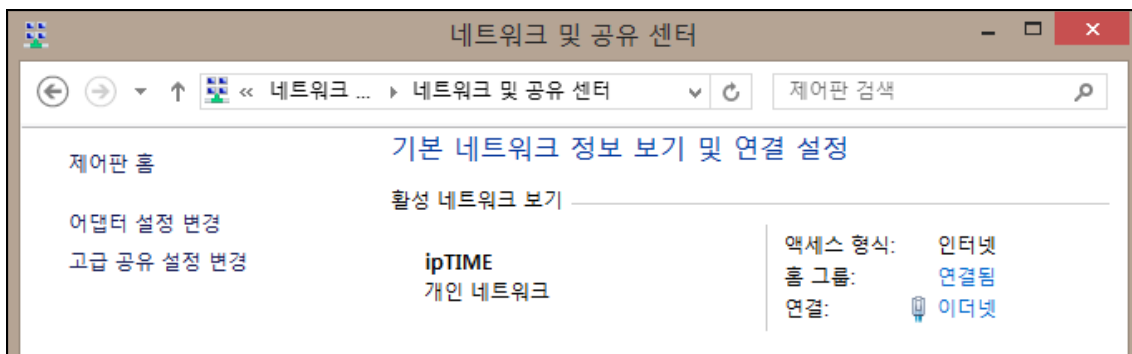
- UPnP가 동작하면 아래 그림처럼 인터넷 게이트 웨이를 인식하게 됩니다.



<윈도우 XP에서 UPnP를 통해서 인식된 IP 공유기 아이콘>



<윈도우 7에서 UPnP를 통해서 인식된 IP 공유기 아이콘>

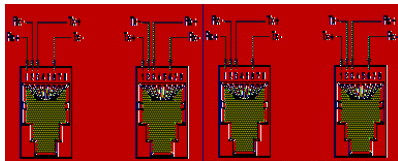
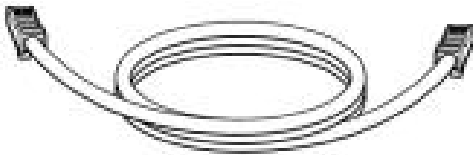


<윈도우 8.1에서 UPnP를 통해서 인식된 IP 공유기 아이콘>

부록 A. LAN Cable 규격

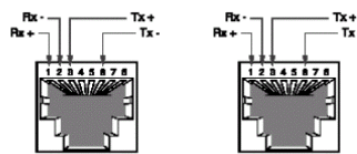
LAN Cable은 스트레이트 케이블(다이렉트 케이블)과 크로스 케이블이 있습니다.

ipTIME에는 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.



Pin No.		Pin No.
1	↔	1
2	↔	2
3	↔	3
4	---	4
5	---	5
6	↔	6
7	---	7
8	---	8

<다이렉트 케이블의 구성>



Pin No.		Pin No.
1	↔	1
2	↔	2
3	↔	3
4	---	4
5	---	5
6	↔	6
7	---	7
8	---	8

<크로스 케이블의 구성>

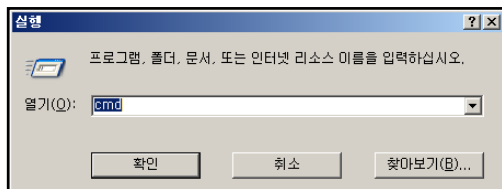
부록 B. IP 공유기 Ping 시험

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.

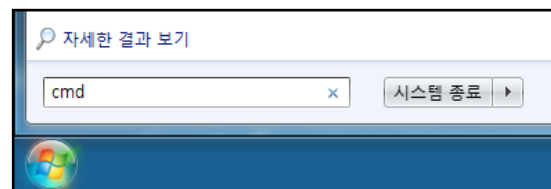
- Ping 시험을 하기 위해서는 명령 프롬프트를 실행합니다.

이의 실행을 위하여

- Windows XP의 경우, 윈도우 화면 좌측 하단의 **[시작]** 버튼을 클릭하고 **[실행]**을 선택합니다. 실행 창에 "CMD"를 입력하고, **[확인]**버튼을 클릭합니다.
- Windows 7의 경우, 윈도우 화면 좌측 하단의 **[윈도우 아이콘]** 버튼을 클릭하고, **[프로그램 및 파일검색]** 창에 "CMD"를 입력하고, 키보드의 **[Enter]** 키를 누릅니다.
- Windows 8 / 8.1의 경우, 화면 좌측 하단의 **[윈도우 아이콘]** 버튼을 마우스 오른쪽 버튼으로 클릭하고 실행을 선택합니다. 실행 창에 "CMD"를 입력하고, **[확인]**버튼을 클릭합니다.

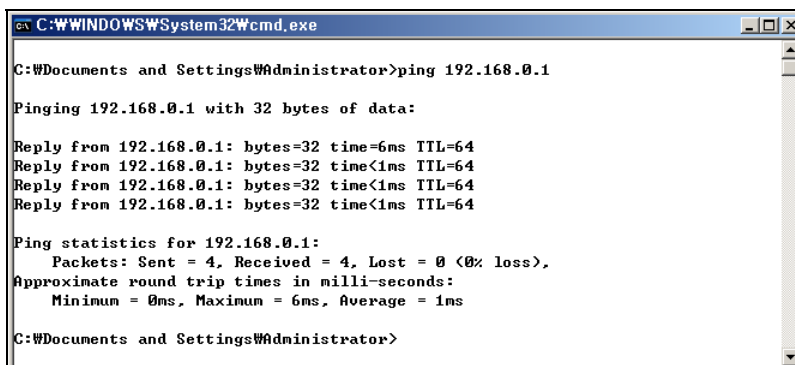


<윈도우 XP의 cmd 실행>



<윈도우 7의 cmd 실행>

- 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.

