



유무선공유기 (RUSH-314N) 사용자설명서



유무선공유기 (RUSH-314N) 사용자설명서

이 안내서는 RUSH-314N을 구입하신 사용자에게 제품 설치 방법과 설치한 이후에 발생하는 문제점을 해결하는 방법을 알려드립니다. 사용자는 제품 취급전에 반드시 본 안내서를 잘 읽은 후 지침에 따라 제품을 바르게 사용해 주십시오.

- ※ 본 안내서의 내용과 그림 등은 제품의 기능 향상 및 그 밖의 이유로 별도의 공지 없이 변경될 수 있습니다.
- ※ 본 안내서의 내용은 (주)머큐리의 허가 없이 임의로 내용을 변경할 수 없습니다.



안전한 사용을 위한 주의사항	4
1. RUSH-314N AP 사양 및 구성품	5
1.1 설치하기 전 유의사항	5
1.2 RUSH-314N의 사양	6
1.3 제품 구성품	7
1.4 제품의 외관 및 각 부분의 명칭	7
2. RUSH-314N AP 설치 방법	11
2.1 RUSH-314N AP 기본 설치	12
2.2 RUSH-314N AP 설치 전 확인사항	12
2.3 RUSH-314N AP 랜케이블 연결방법	13
2.4 RUSH-314N AP 인터넷 연결방법	14
2.5 PC 환경 설정하기	15
3. RUSH-314N AP 기능 활용 방법	21
3.1 상태정보조회	21
3.1.1 인터넷 연결정보	23
3.1.2 DHCP 할당정보	24
3.1.3 시스템 로그	24
3.2 시스템 기본 설정	25
3.2.1 WAN 설정	26
3.2.2 LAN 설정	28
3.2.3 DHCP 설정	29
3.2.4 운영모드 선택	30
3.3 무선랜 설정	31
3.3.1 기본설정	32
3.3.2 고급설정	33
3.3.3 인증/암호화설정	34
3.3.4 MAC 주소 필터링	36
3.3.5 WDS	37
3.3.6 무선 연결 상태	38

3.4 고급설정	39
3.4.1 NAT 설정	39
1) 내부서버	40
2) 포트포워드	41
3) ALG	42
4) VPN	43
5) DMZ 설정	44
6) 비정규 FTP	45
3.4.2 보안설정	46
1) IP 필터링	46
2) MAC 필터링	47
3) DOS 방어설정	48
4) 트래픽제한설정	49
3.4.3 DNS	50
3.4.4 L2 스위치 설정	51
1) MAC 제한 설정	51
2) Storm 제어 설정	52
3.5 시스템 설정	53
3.5.1 업그레이드	53
3.5.2 비밀번호 변경	55
3.5.3 시스템 관리	56
3.5.4 로그아웃	58
4. 문제 해결	59
5. 부록	67
부록 A : 윈도우 XP에서 무선랜 연결방법	68
부록 B : 무상/유상 AS 기준	71

안전한 사용을 위한 주의사항

이 사용설명서는 RUSH-314N AP(Access Point)를 설치하고 사용하는데 필요한 기본적인 사항을 설명합니다. RUSH-314N 제품과 같은 종류의 무선랜 제품을 처음 사용하는 사용자는 물론 이전에 사용해 본 사용자도 반드시 본 설명서를 읽어보고 그 순서에 맞게 설치 작업을 수행하는 것이 좋습니다. 이 설명서는 사용자가 컴퓨터에 대해 기초지식을 가지고 제품을 사용한다는 가정 하에서 설명하고 있습니다. RUSH-314N 제품을 사용하기 전에 먼저 다음 주의 사항을 읽어보기 바랍니다. 다음 설명은 RUSH-314N 제품을 안전하고 올바르게 사용하여 사고나 위험을 사전에 방지하기 위한 사항이므로 반드시 지켜주시기 바랍니다.

- RUSH-314N AP는 전문가만이 제품을 수리할 수 있습니다. 문제가 생겼을 때에 전문가의 도움 없이 제품을 임의로 분해 및 변경을 하지 않도록 합니다.
- RUSH-314N AP 제품 수리 시 지정된 부품 이외의 다른 부품을 사용하지 않도록 합니다.
- RUSH-314N AP를 비롯한 모든 무선 장치들은 주파수 간섭을 받을 수 있고, 그 결과 제품 성능에 영향을 미칠 수도 있습니다.
- RUSH-314N AP의 전원 공급용 어댑터는 반드시 RUSH-314N AP 전용 제품을 사용하도록 합니다.
- RUSH-314N AP 제품에 물기가 닿지 않도록 주의하여야 합니다. RUSH-314N AP에 손상을 줄 수 있습니다.
- RUSH-314N AP 제품을 떨어뜨리거나 과도한 충격을 주지 않도록 합니다.
- 물기나 습기가 많은 곳, 온도 변화가 심한 곳, 너무 덥거나 추운 곳에서는 성능 저하나 고장의 원인이 될 수 있으므로, 사용을 가급적 피하시기 바랍니다.
- 연료나 화학약품과 가까운 곳 또는 폭발물이 있는 곳 등 위험이 발생할 수 있는 장소나 환경에서 RUSH-314N AP를 사용하지 않도록 합니다. RUSH-314N AP에 손상을 줄 수 있습니다.
- 무선 시스템의 특성상, AP의 전원이 단말 PC의 전원보다 항상 먼저 켜져야 올바르게 동작합니다.
- RUSH-314N AP의 설치 과정 중에 PC에 저장되어 있는 중요한 데이터를 손실할 수 있는 가능성을 배제하기 위해서 설치과정에 앞서 모든 중요한 데이터를 백업하는 것을 권장합니다.
- 데이터의 전송 도중에 AP의 서비스 영역 밖으로 이동하는 것은 전송되는 데이터의 손실을 가져올 수 있습니다.
- 전송되는 데이터의 손실을 방지하기 위해 RUSH-314N AP와의 연결을 끊을 때에는 먼저 모든 무선 데이터 전송을 중지하도록 합니다.

※ Microsoft Windows 관련 사항은 Microsoft Corporation의 등록 상표입니다. 다른 회사명이나 제품명은 해당회사 소유의 등록 상표입니다.

※ 본 사용설명서에 표시된 내용(외관, 디자인, 규격, 내용)은 제품의 품질 향상을 위하여 예고 없이 변경될 수 있습니다.

1. RUSH-314N AP

사양 및 구성품

본 장에서는 RUSH-314N AP의 소개와 각 부분의 명칭과 기능에 관하여 설명합니다.

- 설치하기전 유의 사항
- RUSH-314N 의 사양
- 제품 구성품
- 제품의 외관 및 각 부분의 명칭과 기능



1.1 설치하기 전 유의사항

RUSH-314N AP를 설치하기 전에 확인해야 할 사항들에 대해 알아봅니다. RUSH-314N AP는 IEEE 802.11n 무선랜 표준에 따르는 무선랜 장비로서 일반적인 유선랜 사용환경의 모든 편리성과 더불어 이동성의 자유를 함께 제공합니다.

RUSH-314N AP는 무선랜을 보다 안전하고 편리하게 사용 할 수 있도록 강력한 기능과 특징들을 보유하고 있습니다.

사용상의 장애를 방지하려면 RUSH-314N를 설치하기에 앞서 다음과 같은 제품 성능상 영향을 미치는 몇 가지 사항들에 유의하여야 합니다.

주의 사항	설 명
전파의 감쇄	무선랜 시스템의 전파는 사용되는 거리 또는 다른 기기로부터의 전파 간섭, 장애물 등에 의해서 영향을 받을 수 있습니다. 특히 영향을 주는 것들로는 콘크리트 벽, 금속 문, 전파를 방출하는 기기 (예: 전자레인지) 등이 있습니다. RUSH-314N 를 설치하거나 노트북 PC 등을 사용하기 위해 장소를 선정할 때는 이러한 영향에 대해 검토하여야 합니다.
RUSH-314N 전파출력의 크기	RUSH-314N 로부터의 전자파 방출이 강해야만 인터넷 접속이 용이하거나 빠른 데이터 전송률이 얻어진다고 볼 수만은 없습니다. 그 이유는 무선 연결의 품질이 클라이언트(예: 노트북 PC)에 사용되는 무선랜 카드로부터의 전파 세기에도 관계되기 때문입니다.
무선 채널	RUSH-314N 는 802.11n를 지원합니다. 그러나 각 표준은 국가마다 서로 다른 채널 범위에 대한 규격을 갖고 있습니다. 예를 들면 802.11n에서 한국과 중국 그리고 대부분의 유럽 국가에서는 13개의 채널을 사용하지만 미국에서는 11개의 채널을 사용합니다. 채널이 맞지 않는 무선랜 카드를 RUSH-314N 와 함께 사용할 경우 문제가 발생할 수 있습니다.

1.2 RUSH-314N 의 사양

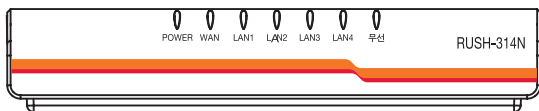
구분	사양
하드웨어	■ 인터페이스: RJ-45 LAN 포트 (이더넷, 10/100 Base-T) 4개, ■ RJ-45 WAN 포트(이더넷, 10/100 Base-T) 1개, 전원 공급용 커넥터 1개 ■ 초기화 스위치 ■ 상태표시 LED: 7개 ■ 온도 범위: -20 ~ 70 (oC) (보관온도), -10 ~ 50 (oC) (사용온도) ■ 상대 습도: 0 ~ 95 (%) / - 전원 공급 어댑터: 5V DC/2A
소프트웨어	■ IEEE 802.11b/g/n(physical) 성능의 무선 네트워크를 지원 ■ 유선랜 표준: IEEE 802.3 & 802.3u (이더넷, 10/100 Mbps) ■ NAT 기능 지원: ALG, DMZ, Firewall, VPN Pass-through 등 ■ HTTP (Web Manager) 를 이용한 원격 관리 ■ WMM (Wi-Fi Multi Media) 지원 ■ SNMP v1, v2c & MIB I, II ■ 무선 보안: 정적/동적인 64/128-bit WEP 암호화, WPA /WPA2(TKIP, AES-CCMP) 지원 ■ 자동 채널 선택 / - WDS 지원
무선	1. IEEE802.11n 사양 ■ 주파수 대역: 2.400~2.4835 GHz ■ Modulation : MIMO OFDM ■ 무선 출력: 11dBm at 54Mbps at 40MHz Occupied B/W ■ Antenna : 2.4GHz External Dipole Antenna 4dBi 2. IEEE802.11g 사양 ■ 주파수 대역: 2.400~2.4835 GHz ■ Modulation : OFDM (64QAM, 16QAM, QPSK, BPSK) ■ 무선 출력: 14dBm at 54Mbps ■ Antenna : 2.4GHz External Dipole Antenna 4dBi 3. IEEE802.11b 사양 ■ 주파수 대역: 2.400~2.4835 GHz ■ Modulation : DSSS (CCK, DQPSK, DBPSK) ■ 무선 출력: 20dBm at 11Mbps ■ Antenna : Dual Band External Dipole Antenna 4dBi

1.3 제품 구성품

- RUSH-314N 본체 1대 (안테나 2개 포함) / 이더넷 케이블 (RJ-45) 1개
- 전원 공급용 어댑터 (5V DC/2A) 1개
- 사용자 설명서

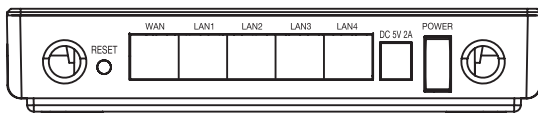
1.4 제품의 외관 및 각 부분의 명칭

1) 전면부 상태 표시등(LED) 설명



명칭	색상	기능
Power	적색	AP에 정상적으로 전원이 공급되면 켜짐.
WAN	녹색	인터넷 또는 모뎀과 연결 상태를 표시합니다. 정상적으로 연결되면 켜지며 데이터 전송이 일어나면 깜빡임
LAN1	녹색	PC와 연결 상태를 표시합니다. PC와 정상적으로 연결되면 켜지며 데이터 전송이 일어나면 깜빡임.
LAN2	녹색	PC와 연결 상태를 표시합니다. PC와 정상적으로 연결되면 켜지며 데이터 전송이 일어나면 깜빡임.
LAN3	녹색	PC와 연결 상태를 표시합니다. PC와 정상적으로 연결되면 켜지며 데이터 전송이 일어나면 깜빡임.
LAN4	녹색	PC와 연결 상태를 표시합니다. PC와 정상적으로 연결되면 켜지며 데이터 전송이 일어나면 깜빡임.
무선	녹색	무선랜 사용 상태를 표시합니다. 무선 정상적으로 동작되면 켜지며 데이터 전송이 일어나면 깜빡임.

2) 후면부 포트면 설명



인터페이스 명칭	표시명	기능
초기화 스위치 포트	RESET	AP을 공장 초기화 상태로 할 수 있음.
WAN 포트	WAN	인터넷 망과 연결하는 포트임.
LAN 포트	LAN1	PC와 연결하는 포트임.
LAN 포트	LAN2	PC와 연결하는 포트임.
LAN 포트	LAN3	PC와 연결하는 포트임.
LAN 포트	LAN4	PC와 연결하는 포트임.
전원입력 포트	DC 5V 2A	전원 어댑터로부터 5V 2A 의 전원을 공급 받음.
전원스위치	POWER	전원을 켜거나 꺼지게 함

이 페이지는 편집을 위한 공백입니다.

2. RUSH-314N AP

설치방법

본장에서는 RUSH-314N AP 를 설치하는 방법에 대해 알아봅니다.

- RUSH-314N AP의 기본 설치
- RUSH-314N AP 설치전 확인 사항
- RUSH-314N AP 랜케이블 연결방법
- RUSH-314N AP 인터넷 연결방법
- PC 환경 설정 방법



2.1 RUSH-314N AP 기본 설치

다음은 RUSH-314N AP를 설치하여 인터넷을 사용하는 기본적인 방법을 설명하며 설치 시 상세한 내용은 뒷장의 상세내용을 참고해 주시기 바랍니다.

1. RUSH-314N AP 와 ADSL, VDSL, 케이블 모뎀과 PC 연결하기

RUSH-314N AP의 WAN포트에 ADSL, VDSL, 케이블 모뎀을 연결(모뎀과 PC를 연결한 기존 랜케이블 사용)하고 RUSH-314N AP와 LAN포트에 PC를 연결합니다 (RUSH-314N AP와 함께 제공한 랜케이블 사용)

2. RUSH-314N AP LAN 포트에 연결된 PC 환경설정

RUSH-314N AP의 LAN 포트에 연결된 PC에서 <http://192.168.25.1/>에 접속되는 지 확인합니다. 접속되지 않으면 PC 네트워크 환경 설정을 변경해야 합니다.

3. RUSH-314N AP 인터넷 연결하기

RUSH-314N AP를 설정하기 전에 LAN포트에 연결된 PC가 인터넷 접속이 가능하면 설정을 끝냅니다. 인터넷 접속이 안되면 PC에서 RUSH-314N AP와 접속하여 설정하여야 합니다

2.2 RUSH-314N AP 설치 전 확인사항

현재 사용하고 있는 인터넷 서비스를 미리 확인하여야 합니다. 그 유형은 일반적으로 2가지 경우의 서비스가 제공되고 있습니다, 어떤 서비스를 사용하고 있는지 인터넷 서비스 업체에 확인 후 아래 설명을 확인하시기 바랍니다.

인터넷 서비스 유형	설 명
유동 IP 주소(DHCP)	VDSL 서비스, 광랜서비스, 케이블 인터넷 서비스 지역 유선방송 사업자가 함께 제공하는 인터넷서비스 접속 프로그램을 사용하지 않는 ADSL 서비스(예 : IP-ADSL등)
고정 IP 주소	인터넷 서비스 업체로부터 지정된 IP 주소 할당 사용

1. 유동 IP 주소(DHCP) 사용자 주의 사항

유동 IP 주소를 사용하는 고객의 경우 RUSH-314N AP에 랜케이블을 연결한 후 별도의 설정없이 자동으로 인터넷이 연결되어 사용할 수 있습니다. RUSH-314N AP는 유동 IP 연결방식의 인터넷서비스를 이용시 별도의 설정없이 인터넷을 사용할 수 있도록 기본값이 설정되어 있습니다. 그러므로 이런 경우 내부 PC의 환경설정만 확인 후 그대로 사용시면 됩니다.

단, 랜케이블 연결 후 자동으로 인터넷이 연결이 안되면 해당 인터넷 서비스 업체가 MAC 주소제한을 하고 있을 수 있습니다. 광랜의 경우에는 연결되는 PC나 유무선공유기의 MAC 주소가 변경이 되면 고객인증 절차를 거쳐야 인터넷을 사용할 수 있습니다.

2. 고정 IP 사용자 주의사항

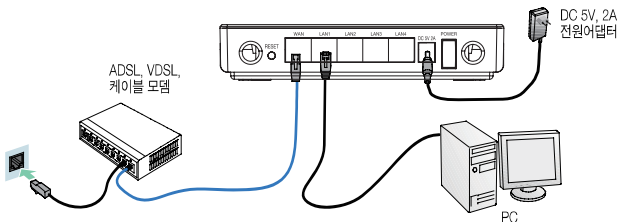
인터넷 서비스 업체에서 제공하는 다음 5가지 정보를 미리 확인하여 인터넷연결 설정시 입력하시기 바랍니다. IP주소, 서브넷마스크, 기본게이트웨이, 기본 DNS, 보조 DNS(일부 인터넷 서비스 업체에서는 제공하지 않을 수 있습니다.)

추가 사항은 사용자설명서의 상세 사항을 참조하시기 바랍니다.

2.3 RUSH-314N AP 랜케이블 연결방법

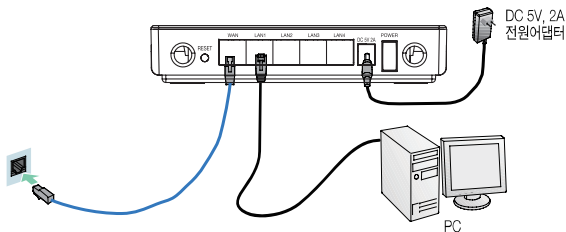
1. ADSL, VDSL, 케이블 모뎀 인터넷 서비스를 이용하는 경우

- ① ADSL, VDSL, 케이블 모뎀과 유무선 공유기를 연결한 랜케이블을 AP의 인터넷 포트에 연결합니다.
- ② AP와 함께 제공된 랜케이블을 AP의 LAN포트와 PC에 연결합니다.
- ③ AP를 설치한 후 모뎀, AP, PC순으로 켜다 켜야 정상적으로 인터넷에 연결됩니다.



2. 광랜과 같이 가정에 모뎀없이 랜케이블이 직접 들어오는 경우

가정내에 별도의 모뎀이 없이 랜케이블이 직접 들어오고 유무선공유기를 사용하지 않으셨다면 다음과 같이 설치합니다.



- ① 가정 내에 별도의 모뎀 없이 들어와 있는 랜케이블을 AP의 인터넷 포트에 연결합니다.
- ② AP와 함께 제공된 랜케이블을 AP의 LAN포트와 PC에 연결합니다.
- ③ AP를 설치한 후 모뎀, AP, PC순으로 켜야 정상적으로 인터넷에 연결됩니다.

2.4 RUSH-314N AP 인터넷 연결방법

RUSH-314N AP를 인터넷에 연결 하기 위해서는 사용하는 인터넷서비스 업체 따라 설정을 하여야 합니다.

주의 : LAN 포트에 연결된 PC가 인터넷 접속이 가능하면 PC 환경설정을 하지 않아도 됩니다.

1) RUSH-314N AP의 웹서버 들어가기

RUSH-314N AP는 제품내부의 설정변경을 위해서 웹서버 형태의 설정변경창을 지원합니다. 웹서버에 들어가시려면 다음과 같이 실행하시면 됩니다.

RUSH-314N AP의 LAN 포트에 연결된 PC에서 인터넷 익스플로러를 실행합니다. 인터넷 익스플로러 실행후 주소(D)창에 에서 <http://192.168.25.1/> (RUSH-314N AP의 기본설정 IP주소)를 입력한 후 Enter Key를 칩니다. RUSH-314N AP의 웹서버에 들어가면 아래와 같은 화면이 나옵니다.



MERCURY CORPORATION

Welcome to Mercury RGW

사용자ID :

암호 :

외부IP 주소 :

DNS 서버 :

연결 모드 :

연결 상태 :

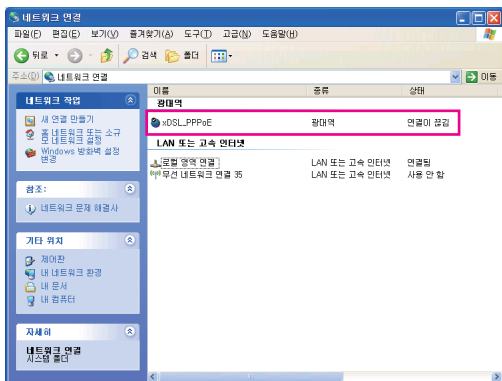
소프트웨어 버전 :

기본 시스템 사용자 이름에 admin, 암호에 admin (모두 소문자입니다.)를 입력한 후 사용자 환경에 맞추어 RUSH-314N AP의 설정을 변경할 수 있습니다. 만약 RUSH-314N AP Web Manager 화면이 나오지 않는다면 'PC 환경 설정하기'를 참고하시기 바랍니다.

2.5 PC 환경 설정하기

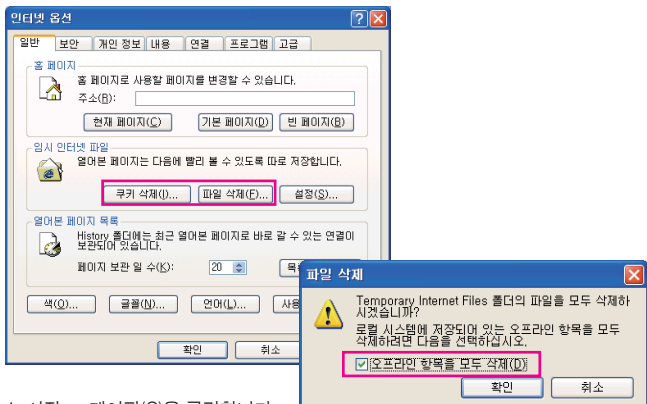
1) 광대역 연결 확인

아래 그림과 같이 사용자 환경이 윈도우XP일 경우 자체적으로 광대역 연결을 지원하지므로 윈도우 시작버튼 → 제어판(C) → 네트워크 연결에서 설치된 광대역을 삭제합니다.

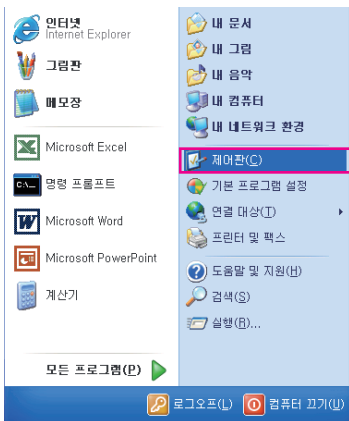


2) 윈도우 XP의 네트워크 설정하기

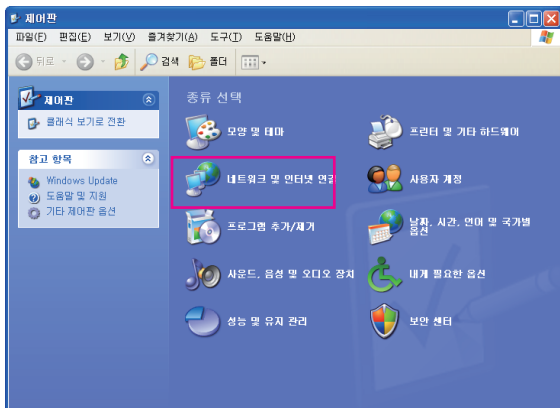
인터넷 익스플로러를 실행한 후 **도구(T) → 인터넷 옵션(O)**를 선택합니다. 쿠키와 파일을 삭제합니다. 파일 삭제 시에는 **오프라인을 모두 삭제(D)**해 주십시오.



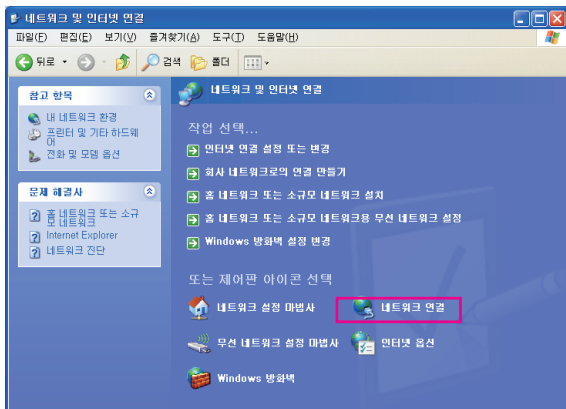
1. 시작 → 제어판(C)을 클릭합니다.



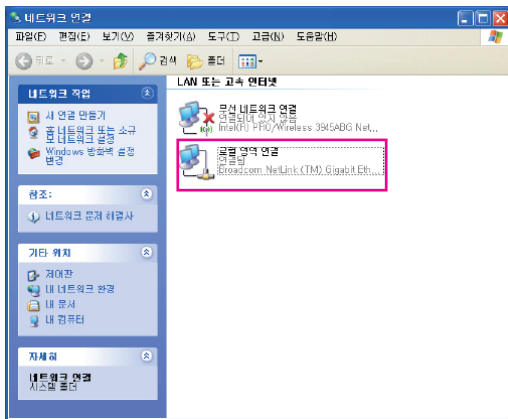
2. 제어판(C)에서 네트워크 및 인터넷 연결을 클릭합니다.



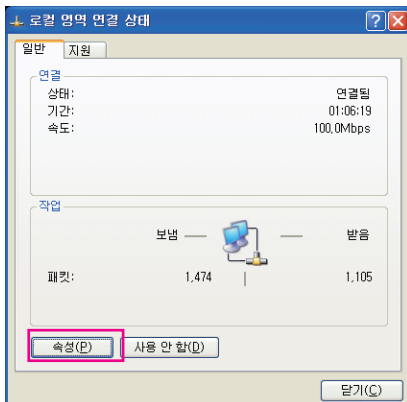
3. 네트워크 및 인터넷에서 네트워크 연결을 클릭합니다.



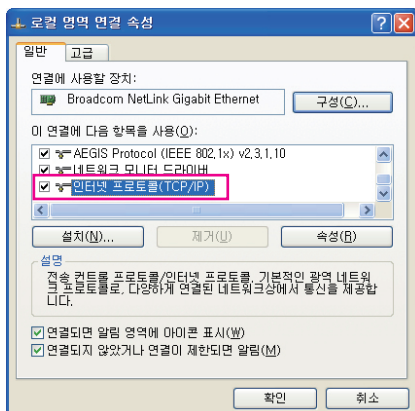
4. 네트워크 연결 → 로컬 영역 연결을 더블 클릭합니다.



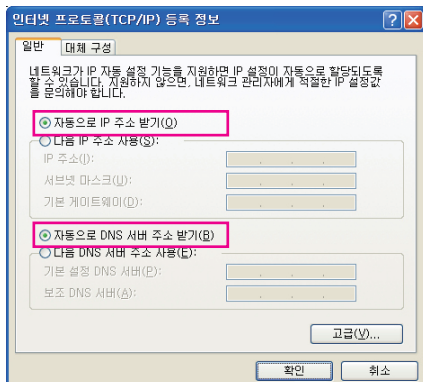
5. 로컬 영역 연결에서 속성(P)을 클릭합니다.



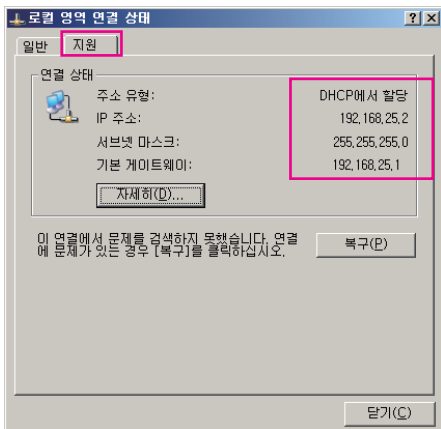
6. 로컬 영역 연결 속성에서 TCP/IP 항목을 더블 클릭합니다.



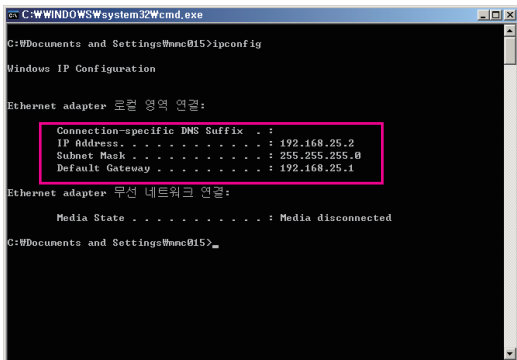
7. TCP/IP에서 자동으로 IP 주소 받기(O)와 자동으로 DNS 서버 주소 받기(B)를 선택한 후 확인 클릭합니다.



8. 로컬 영역 연결 상태 → 지원 탭으로 이동하여 IP 주소를 확인할 수 있습니다.
RUSH-314N AP로부터 IP를 할당 받기까지 최대 20~30초 정도 걸릴 수 있습니다.



9. 윈도우 시작 버튼 → 모든 프로그램(P) → 보조 프로그램 → 명령프롬프트를 실행
한 후 ipconfig 명령을 입력합니다.
아래 그림과 같이 PC의 네트워크 정보가 표시되어야 정상입니다.



3. RUSH-314N AP

기능 활용 방법

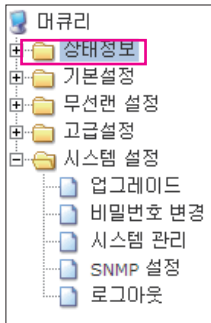
본 장에서는 RUSH-314N AP의 설정에 관하여 설명합니다. RUSH-314N AP의 특별한 설정 없이도 인터넷을 사용할 수 있습니다. 특정 기능 사용 시 참조하십시오.

- 상태정보조회
- 시스템 기본설정
- 무선랜 설정
- 고급설정
- 시스템설정



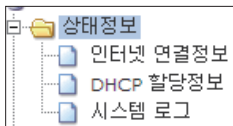
3.1 상태정보조회

AP의 상태 정보를 볼 수 있습니다. 상위메뉴에는 “상태정보”, “기본설정”, 무선랜설정”, “고급설정”, 시스템설정” 총 5가지 메뉴를 확인할 수 있으며, 사용자는 “상태정보”메뉴를 사용하여 접속상태를 확인할 수 있습니다.



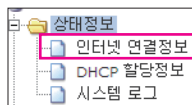
이 장은 상태정보 메뉴의 다음과 같은 내용으로 이루어집니다.

- ☐ 인터넷 연결정보
- ☐ DHCP 할당정보
- ☐ 시스템로그



운영모드를 Bridge로 선택시에는 DHCP 할당정보 메뉴는 선택 메뉴에서 사라집니다.

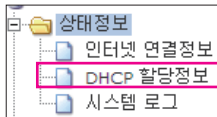
3.1.1 인터넷 연결정보



AP의 상태 정보를 볼 수 있습니다. 시스템, WAN 설정정보, LAN 설정정보, WLAN 설정정보를 간략하게 보여줍니다.

시스템 정보	
SDK 버전	1.02.02 (Nov 5 2009,14:49:18)
장비시간	Nov 5 16:54:59 2009
제조사	Mercury Co.
운용모드	Gateway Mode
WAN 설정정보	
연결방법	DHCP
WAN IP 주소	165.133.16.100
서브넷마스크	255.255.255.0
게이트웨이	165.133.16.254
DNS 서버1	168.126.63.1
DNS 서버2	165.133.1.13
하드웨어주소	00:C0:77:B0:06:70
LAN 설정정보	
Local IP 주소	192.168.1.254
Local 서브넷마스크	255.255.255.0
하드웨어주소	00:C0:77:B0:06:71
무선 설정정보	
무선 동작 설정	활성화
무선 모드	11b/g/n mixed mode
채널	Auto
BSSID	00:C0:77:B0:06:72
이더넷 포트상태	

3.1.2 DHCP 할당정보



DHCP 할당 정보는 LAN port를 통해서 동작하는 단말이 할당 받은 IP 주소와 하드웨어 주소를 확인할 수 있습니다. 또한 할당한 정보를 초기화 할 수 있습니다

할당 정보 초기화		적용
DHCP 할당		
하드웨어주소	IP 주소	할당된 상태
할당된 정보가 없습니다.		

3.1.3 시스템 로그

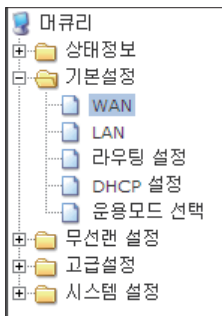
시스템 로그기능은 장비의 전반적인 동작상태에 대한 기록을 저장하는 기능입니다. 시스템 로그 기능은 “취소”버튼을 눌러서 로그 기능을 정지할 수 있으며 “적용” 기능을 눌러서 시작할 수 있습니다. 또한 로그 서버를 입력하여 로그화일을 입력한 원격 로그 서버로 보내는 동작을 수행합니다.

시스템로그 설정	
시스템로그 동작 설정	활성화
시스템로그 원격서버 IP	비활성화
적용	취소
다시보기 기록삭제	
시스템 로그	
<pre> Sep 1 18:04:53 Mercury_RGW user.info syslog: DHCP: IP 165.133.16.130 , lease time 240 Sep 1 18:04:51 Mercury_RGW user.info syslog: DHCP: Sending renew... Sep 1 18:02:53 Mercury_RGW user.info syslog: DHCP: IP 165.133.16.130 , lease time 240 Sep 1 18:02:51 Mercury_RGW user.info syslog: DHCP: Sending renew... Sep 1 18:01:43 Mercury_RGW daemon.warn SystemMgmt: LAN2 PORT UP Sep 1 18:00:53 Mercury_RGW user.info syslog: DHCP: IP 165.133.16.130 , lease time 240 Sep 1 18:00:51 Mercury_RGW user.info syslog: DHCP: Sending renew... Sep 1 17:58:53 Mercury_RGW user.info syslog: DHCP: IP 165.133.16.130 , lease time 240 Sep 1 17:58:51 Mercury_RGW user.info syslog: DHCP: Sending renew... Sep 1 17:56:54 Mercury_RGW user.info syslog: DHCP: IP 165.133.16.130 , lease time 240 Sep 1 17:56:51 Mercury_RGW user.info syslog: DHCP: Sending renew... Sep 1 17:54:53 Mercury_RGW user.info syslog: DHCP: IP 165.133.16.130 , lease time 240 Sep 1 17:54:50 Mercury_RGW user.info syslog: DHCP: Sending renew... Sep 1 17:52:52 Mercury_RGW user.info syslog: DHCP: IP 165.133.16.130 , lease time 240 </pre>	

3.2 시스템 기본 설정

시스템 기본 설정에서는 RUSH-314N 에 대한 기본적인 설정을 하는 MENU로서 이 장은 다음과 같은 내용으로 이루어집니다.

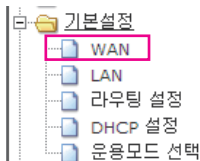
- WAN 설정
- LAN 설정
- 라우팅 설정
- DHCP 설정
- 운영모드 선택



Notice

운영모드를 Bridge로 선택시에는 DHCP 할당정보 메뉴는 DHCP Option82 메뉴로 바뀌어지며, 라우팅 설정 메뉴는 사라집니다

3.2.1 WAN 설정



아래 창에서 WAN 인터페이스는 네트워크 환경에 따라서 유동IP(DHCP), 고정IP 모드로 사용할 수 있습니다. 가입자의 네트워크 환경이 고정 IP인 경우 “Static Mode(fixed IP)”를 선택한 후 IP 주소와 서브넷 마스크, 게이트웨이 주소를 입력한 후 “적용” 버튼을 누릅니다.

가입자의 네트워크 환경이 DHCP 인 경우”DHCP(Auto config)”를 선택후 “적용” 버튼을 누르면 됩니다.

“WAN 포트 설정”항목은 상위 네트워크 장비의 포트설정에 따라서 설정해야 하며 특별한 경우가 아니면 변경하지 않아야 합니다.

1) DHCP 설정 메뉴

WAN 연결 모드:		DHCP(Auto config) ▼			
DHCP 모드					
하드웨어주소		00:C0:77:B0:06:7F			
총괄 IP 주소					
장비이름 (optional)		Mercury_RGW			
적용 취소					
MAC Clone					
Enabled		비활성화 ▼			
적용 취소					
WAN 포트 설정					
포트	Admin Status	포트상태	AutoNego	Speed	Duplex
wan	Up ▼	Connected	On ▼	100 Mbps ▼	Full Duplex ▼
적용					

2) STATIC IP 설정메뉴

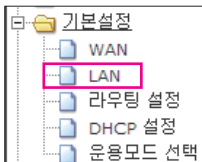
WAN 연결 모드:		Static Mode(fixed IP) ▼			
Static 모드					
IP 주소	165.133.31.16				
서브넷마스크	255.255.255.0				
게이트웨이	165.133.31.254				
하드웨어주소	00:C0:77:B0:06:7F				
총틀 IP 주소					
적용 취소					
MAC Clone					
Enabled	비활성화 ▼				
적용 취소					
WAN 포트 설정					
포트	Admin Status	포트상태	AutoNego	Speed	Duplex
wan	Up ▼	Connected	On ▼	100 Mbps ▼	Full Duplex ▼
적용					

3) MAC Clone

지정한 MAC주소로 변경하여, 통신하는 기능입니다

MAC Clone	
Enabled	활성화 ▼
하드웨어주소	00:00:00:00:00:00
MAC Address List	
Num	MAC Address
할당된 정보가 없습니다.	
적용 취소	

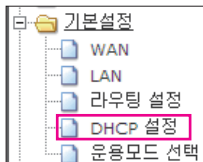
3.2.2 LAN 설정



LAN 인터페이스에 설정된 “192.168.25.1”는 PC의 default gateway로서 변경되어서는 안되며 “LAN 포트 설정” 항목 또한 특별한 경우가 아니면 변경하지 않아야 합니다. 부득이하게 LAN IP 주소를 변경하게 되는 경우에는 반드시 DHCP 설정에서 DHCP IP Range도 변경해야 합니다.

LAN 설정					
IP 주소	192.168.25.1				
서브넷마스크	255.255.255.0				
하드웨어주소	00:C0:77:B0:06:80				
적용 취소					
LAN 포트 설정					
포트	AdminStatus	AutoNegotiation	Speed	Duplex	
lan1	Up	Off	10 Mbps	Half Duplex	
적용					
LAN 포트 리셋					
포트	lan1				
적용					
LAN 포트 상태					
포트	Admin Status	포트상태	AutoNegotiation	Speed	Duplex
lan1	Up	Disconnected	On	10Mbps	Half
lan2	Up	Disconnected	On	10Mbps	Half
lan3	Up	Disconnected	On	10Mbps	Half
lan4	Up	Disconnected	On	10Mbps	Half

3.2.3 DHCP 설정



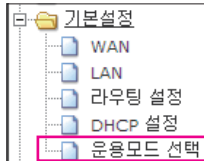
DHCP 설정은 LAN 인터페이스에서 동작하는 DHCP server에 대한 설정을 할 수 있습니다. “DHCP설정”을 누르면 현재 설정된 정보를 볼 수 있으며 변경을 원할 경우 시작주소, 마지막주소, 넷마스크, 게이트웨이, 임대시간에 대한 설정 값을 변경할 수 있습니다. LAN 인터페이스에 연결된 PC에 원하는 DNS IP를 고정으로 받고자 할 경우 “DNS 포워드 설정”항목을 DNS IP 로 선택하면 “기본 DNS 서버”, “보조 DNS 서버”항목이 추가되며 해당 값을 입력 후 아래의 “적용”을 누릅니다. 그외 Domain Name 은 IP가 아닌 문자형태 주소값입니다. PC에서 자동으로 IP 주소를 받고 있는 경우 DHCP 범위내에서 특정 IP 주소를 항상 같은 PC가 사용할 수 있도록 하여, 내부 PC의 IP주소 관리를 할 수 있습니다.

DHCP 서버 설정	
DHCP 설정	서버 ▼
시작 주소	192.168.25.2
마지막 주소	192.168.25.9
넷마스크	255.255.255.0
게이트웨이	192.168.25.1
임대 시간	3600
DNS 포워드 설정	☒ Not Used ☐ DNS IP ☐ Domain Name ☐ Both (DNS/DomainName)
고정 IP1	MAC: 00:00:00:00:00:00 IP : 0.0.0.0
고정 IP2	MAC: 00:00:00:00:00:00 IP : 0.0.0.0
적용 취소	



운영모드를 Bridge로 선택시에는 DHCP 할당정보 메뉴는 없어집니다.

3.2.4 운영모드 선택



NAT Enable(Gateway Mode) 및 NAT Disable(Bridge Mode)로 동작 할 수 있습니다. NAT Enable(Gateway Mode)은 LAN 인터페이스에 연결된 PC가 AP의 DHCP server로부터 사설 IP를 받아서 통신하는 것으로 AP의 기본 동작 모드입니다.

NAT Disable(Bridge Mode)은 LAN 인터페이스에 연결된 PC가 네트워크의 DHCP server로부터 공인 IP를 받아서 통신하는 모드입니다. 설정은 NAT Disable(Bridge Mode)을 선택 후 “적용”을 누릅니다.

NAT Disable(Bridge Mode)을 설정하면 AP가 네트워크의 DHCP server로부터 공인 IP를 받고, PC도 공인 IP를 받아서 공인 IP 2개를 소비하게 되며 경우에 따라서 네트워크의 DHCP server의 IP pool이 모자랄 경우 통신이 불가할 수도 있습니다. 따라서 NAT Enable(Gateway Mode)모드로 사용을 권장 합니다.

1) Gateway 모드

☐ Bridge:
br0(무선 + WAN 포트 + LAN 포트)로 구성된다.

☒ Gateway:
WAN 포트 + br0(무선+LAN 포트)로 구성된다
무선 AP 클라이언트를 WAN으로 구성하고, 무선 AP와 이더넷 포트를 LAN 포트에 구성한다.

NAT 설정 활성화 ▼

적용 취소

2) Bridge 모드

☒ Bridge:
br0(무선 + WAN 포트 + LAN 포트)로 구성된다.

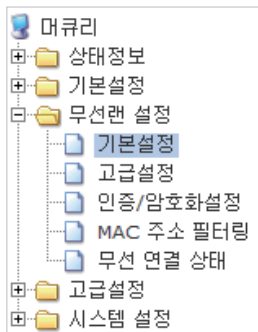
☐ Gateway:
WAN 포트 + br0(무선+LAN 포트)로 구성된다
무선 AP 클라이언트를 WAN으로 구성하고, 무선 AP와 이더넷 포트를 LAN 포트에 구성한다.

적용 취소

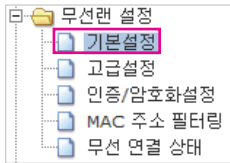
3.3 무선랜 설정

무선랜 설정에서는 다음과 같은 내용으로 이루어져 있습니다.

- 기본설정
- 고급설정
- 인증/암호화설정
- MAC 주소 필터링
- WDS
- 무선연결상태



3.3.1 기본설정

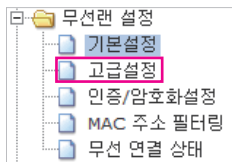


무선랜 AP의 기본 동작을 설정하는 기능입니다.

무선 기본 설정	
무선 동작 설정	☐ 중단 ☒ 사용
무선 모드	11g/n mixed mode ▼
SSID(네트워크이름)	SK_WLAN
SSID(네트워크이름) 알림	☐ 중단 ☒ 사용
BSSID	00:C0:77:B0:06:81
채널	Auto ▼ 채널 검색
채널 크기	☐ 20M ☒ 20/40M
확장 채널	Auto ▼
WMM 동작설정	☐ 중단 ☒ 사용
Data Rate	Auto ▼
TxStream	2 ▼
RxStream	2 ▼
적용 취소	

- 무선동작설정 : AP의 무선랜 사용여부를 결정합니다.
- 무선 모드 : 무선랜 모드를 결정합니다.
- SSID(네트워크이름) : 무선 네트워크의 이름을 설정합니다. 영문 및 특수문자를 입력할 수 있습니다.
- SSID(네트워크이름)알림 : SSID Hidden 기능 사용여부를 설정합니다.
- BSSID : 현재 무선랜이 사용하는 MAC 주소를 표시합니다.
- 채널 : 채널을 설정합니다.
- 채널검색 : 최적의 채널을 검색합니다. 채널 검색시 무선 연결이 끊길 수 있습니다.
- 채널 크기 : 11n에서 channel의 bandwidth를 설정합니다.
- WMM 동작설정 : 802.11e (WMM) 기능 사용여부를 설정합니다.
- Data Rate : 무선 연결시 data rate를 설정합니다.

3.3.2 고급설정



무선 고급설정은 무선 기능에 익숙한 고급사용자들을 위한 설정기능입니다.

무선 고급 설정	
Beacon 주기	100 ms (50~1024), default:100
Data Beacon Rate (DTIM)	1 ms (1~255), default:1
RTS Threshold	2347 bytes (1~2347), default:2347
Fragment Threshold	2346 bytes (256~2346), default:2346
BG Protection	자동 ▼
Frame Aggregation	☐ 중단 ☒ 사용
송신 파워	100 % (1~100), default:100
Short Slot	☐ 중단 ☒ 사용
Preamble 길이	☒ Long Preamble ☐ Short Preamble
최대 접속 단말	0 (0~255)
적용 취소 초기화	

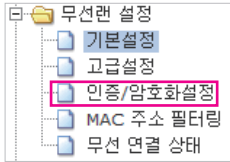
- Beacon 주기 : Beacon 송신 주기를 설정합니다.
- Data Beacon Rate(DTIM) : DTIM 주기를 설정합니다.
- RTS Threshold : 설정 값 이상의 길이를 가진 무선 데이터 전송시 RTS/CTS방식으로 데이터를 전송합니다.
- Fragment Threshold : 설정 값 이상의 길이를 가진 무선 데이터 전송시 설정값 크기로 데이터를 나누어 전송합니다.
- BG Protection : 11b와 11g 용 랜카드를 동시에 사용하는 경우 원활한 무선 통신을 위한 설정입니다.
- Frame Aggregation : 기능을 지원하는 Client 카드와 사용할 경우 무선 성능을 향상시킬 수 있습니다.
- 송신 파워 : 무선 송신 출력을 조정합니다.
- Short Slot : 11g로 연결된 무선Station의 성능을 향상시킬 수 있습니다.
- Preamble 길이 : 호환성을 위해서는 Long Preamble를 사용하는 것이 좋습니다.
- 최대 접속 단말 : 동시 접속가능한 단말의 수를 제한 합니다. 0으로 설정할 경우 제한하지 않습니다.



Notice

무선 성능에 영향을 줄 수 있으니 꼭 필요한 경우만 변경하기를 권장합니다.

3.3.3 인증/암호화설정



SSID별로 보안 및 인증기능을 설정할 수 있는 기능입니다.

무선 보안/인증 설정	
SSID(네트워크이름)	SK_WLAN ▼
인증방법	Auto ▼
암호화방법	WEP ▼
암호화 Key	WEP Index 1 ▼
	Key 종류 HEX ▼
	WEP Key 987654321b
적용 취소	

※ 공장출하시 기본 설정값은 WEP 암호화 방법이며 암호화 KEY값은 987654321b 입니다.

- SSID : 보안 기능을 설정할 SSID를 선택합니다.
- 인증방법 : 무선 인증 방법을 설정합니다.
- 암호화 방법 : 인증 방법에 해당하는 암호화 종류를 선택합니다.
- 암호화 Key : WEP, WPA-PSK, WPA2-PSK 계열의 암호화시 사용할 Key를 설정합니다.

WEP 설정 방법

1. 설정할 SSID를 선택합니다.
2. 인증 방법에서 Open, Shared, Auto 중 하나를 선택합니다.
 - ▣ OPEN (개방형시스템) : 모든 클라이언트에게 링크를 허용하되 AP와 동일한 WEP key를 사용하는 클라이언트와의 통신만 가능하도록 합니다.
 - ▣ Shared(공유키시스템) : 공유키로 설정된 클라이언트만이 AP와 동일한 WEP key를 사용하여 링크와 통신이 가능하도록 합니다.
 - ▣ Auto(자동) : 개방형 시스템과 공유키 시스템을 동시에 지원합니다.
3. 암호화방법에서 WEP을 선택합니다.
4. 암호화 Key 정보를 설정합니다.
 - ▣ WEP Index : 1~4 를 선택할 수 있습니다.
 - ▣ Key 종류 : ASCII, HEX 를 선택할 수 있습니다.
 - ▣ WEP Key : ASCII 인 경우 5 (64bit)또는 13 (128bit)character를 입력할 수 있습니다. HEX의 경우 10 (64bit)또는 26 (128bit)character를 입력할 수 있습니다. WEP Key의 길이가 길수록 암호화가 강화됩니다.

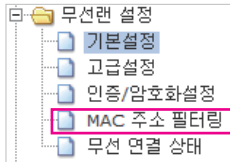
무선 보안/인증 설정

SSID(네트워크이름)	SK_WLAN ▼
인증방법	WPA-PSK ▼
암호화방법	TKIP/AES ▼
암호화 Key	PSK 987654321b

WPA-PSK 설정방법

1. 설정할 SSID를 선택합니다.
2. 인증방법에서 WPA-PSK, WPA2-PSK, WPA/WPA2-PSK 중 하나를 선택합니다.
 - ▣ WPA-PSK : WPA 방식으로 설정된 단말과 접속할 수 있습니다.
 - ▣ WPA2-PSK : WPA2 방식으로 설정된 단말과 접속할 수 있습니다.
 - ▣ WPA/WPA2-PSK : WPA 또는 WPA2 방식으로 설정된 단말과 접속할 수 있습니다.
3. 암호화 방법에서 TKIP, AES, TKIP/AES 중 하나를 선택합니다. TKIP/AES를 선택하면 두가지 암호화를 동시에 지원합니다.
4. 암호화 Key를 설정합니다. 8~64 character를 입력할 수 있습니다.

3.3.4 MAC 주소 필터링

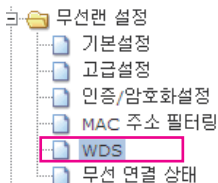


SSID별로 MAC 주소를 이용해서 AP에 접근하려는 무선 단말의 사용여부를 결정할 수 있습니다. 등록된 MAC에 대해서 모두허용, 등록된 주소만 허용, 등록된 주소만 차단의 세가지 정책중 하나를 이용하실 수 있습니다.

SSID(네트워크이름)	SK_WLAN ▼ 갱신
방법	☒ 모두허용 ☐ 등록된주소 허용 ☐ 등록된주소 차단
☐	등록된 MAC 정보가 없습니다 추가
등록가능 갯수:50 적용 취소 선택삭제	

- 모두 허용 : 모든 단말의 접속을 허용합니다.
- 등록된주소만 허용 : 등록된 MAC만을 접속할 수 있도록 설정합니다.
- 등록된주소만 차단 : 등록된 MAC을 접속할 수 없도록 설정합니다.

3.3.5 WDS



WDS(Wireless Distribution System) 기능을 설정합니다. WDS는 AP와 AP를 무선으로 연결해서 사용할 수 있습니다.

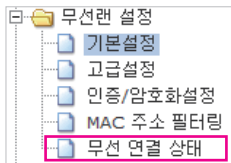
WDS Setup	
WDS Mode	Bridge(WDS Only) ▼
BSSID	00:C0:77:B0:06:81
암호화방법	NONE ▼
MAC 0	
MAC 1	
MAC 2	
MAC 3	
MAC 4	
MAC 5	
MAC 6	

- WDS Mode :
 - Disable - WDS 기능을 사용하지 않습니다.
 - 브릿지 - AP를 WDS 전용으로만 사용합니다. 이 모드에서 무선 단말은 접속할 수 없습니다.
 - 리피터 - WDS 및 AP 기능을 함께 사용합니다.
- MAC 0~7 : WDS 로 사용할 상대 AP의 MAC 주소를 입력합니다.



WDS 기능은 AP 및 사용 Chipset에 따라서 호환이 안될 수도 있습니다.

3.3.6 무선 연결 상태



무선 AP에 무선 단말이 연결되어 있는 경우 연결된 단말의 정보를 표시해줍니다.

SSID(네트워크이름)

SK_WLAN ▼ 갱신

☐	AID	MAC	IP	UserID	Mode	Rate	Signal	RX Bytes	TX Bytes	Conn Time
연결된 단말이 없습니다										

선택삭제

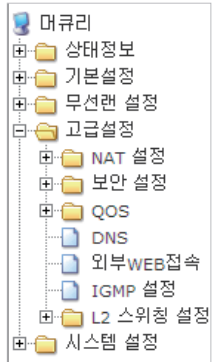
통계초기화

- 선택 삭제 : 연결된 단말을 강제로 접속을 끊습니다.(끊어진 후 무선 단말에 의해서 재접속이 시도될 수 있습니다.)
- 통계초기화 : 접속된 단말의 통계정보를 초기화합니다.

3.4 고급설정

고급설정에서는 다음과 같은 내용으로 이루어져 있습니다. 고급설정은 기본설정이 완료된 상태에서 추가적인 기능을 이용하고자 할 경우 설정하는 메뉴입니다.

- NAT설정
- 보안설정
- DNS
- 외부WEB접속



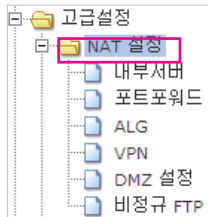
Notice

운영모드를 Bridge로 선택시 NAT설정 메뉴는 사라지고 VLAN 설정 메뉴가 추가됩니다.

3.4.1 NAT 설정

NAT설정은 다음과 같은 서브메뉴로 구성되어 있습니다.

- 내부서버
- 포트포워드
- ALG
- VPN
- DMZ 설정
- 비정규 FTP



Notice

운영모드를 Bridge로 선택시 NAT설정 메뉴는 사라집니다

1) 내부서버

내부서버 기능은 외부 네트워크 사용자가 내부 네트워크에 접속하고자 하는 경우 사용되는 어플리케이션의 포트번호를 내부 네트워크의 IP주소와 내부포트 번호로 연결시켜주는 기능으로서 AP의 내부 서버 설정 기능을 이용하면 내부 네트워크에 FTP서버, TFTP서버, WEB 서버, Telnet, 메일 서버, DNS 서버, PPTP 서버 등을 운용할 수 있습니다. 내부 서버를 사용하는 경우 내부 서버의 IP주소는 고정으로 할당하는 것이 편리하며 서버 프로그램에서는 표준 포트번호를 사용하여야 합니다.

내부서버 설정방법은 다음과 같습니다.

- 사용하고자 하는 내부서버의 “프로토콜”을 선택합니다.
- 내부서버의 주소를 입력합니다.
- “적용” 버튼을 누릅니다.

설정을 해제할 경우에는 해당 프로토콜의 선택을 해제한 후 적용버튼을 누르면 됩니다.

내부서버 설정				
프로토콜	내부서버 IP 주소	외부포트	내부포트	선택
FTP	192.168.25.0	21	21	비활성화 ▼
TFTP	192.168.25.0	69	69	비활성화 ▼
TELNET	192.168.25.0	23	23	비활성화 ▼
SSH	192.168.25.0	22	22	비활성화 ▼
HTTP	192.168.25.0	80	80	비활성화 ▼
SMTP	192.168.25.0	25	25	비활성화 ▼
POP3	192.168.25.0	110	110	비활성화 ▼
NEWS	192.168.25.0	119	119	비활성화 ▼
DNS	192.168.25.0	53	53	비활성화 ▼

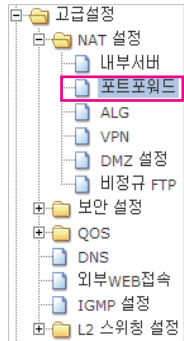
적용
취소

2) 포트포워드

NAT기능은 내부 네트워크 사용자가 외부 네트워크를 접속하고자 하는 경우 내부의 사설 IP주소를 외부의 공인 IP주소로 자동적으로 변경하여 줍니다.

그러나 외부 네트워크 사용자가 내부 네트워크를 접속하고자 하는 경우 외부 네트워크에서 접속을 요청한 Application Protocol의 Port 번호를 내부 네트워크의 사설 IP주소와 이에 따른 내부 Port 번호에 Mapping 하는 기능이 필요합니다.

포트포워드는 내부서버 설정 외에 고객이 이용하고자 하는 특별한 IP와 port번호를 설정 함으로서 외부 접속 요청에 내부 IP주소 및 port번호를 Mapping 할 수 있습니다.



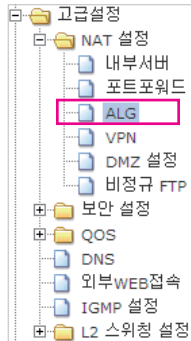
포트포워드 설정방법은 다음과 같습니다.

- “프로토콜”에 Protocol-Type을 선택합니다. TCP와 UDP, TCP/UDP 중 하나를 선택할 수 있습니다.
- “외부포트”는 외부에서 수신되는 Packet의 Destination Port 번호를 입력하는 항목입니다. 일반적인 경우 이 항목의 값에 따라 수신되는 Packet의 Application이 결정되어지므로 이 항목은 목적에 맞게 꼭 입력하여야 합니다.
- “포워딩 IP주소”는 외부에서 수신되는 Packet을 전달할 내부 PC IP 주소를 입력하는 항목입니다.
- “내부포트(option)”는 외부에서 수신되는 Packet을 전달할 내부 Destination Port 번호를 입력하는 항목입니다. 일반적으로 외부 사용 포트 범위와 같은 값을 입력하며 하나의 Port 번호를 입력합니다. Port 번호의 범위를 지정하면 Traffic에 따라 Load Balancing을 하게 됩니다.
- 위의 설정이 끝나면 “추가” 버튼을 누릅니다.

다른 포트포워드를 원하면 “추가”를 누른 후 위의 과정을 반복하고 설정된 포트포워드 기능을 원하지 않을 경우 해당 리스트를 선택한 후 “삭제” 버튼을 누르면 삭제됩니다.

포트 포워드 설정				
프로토콜	TCP ▼			
외부포트	-			
포워딩 IP 주소				
내부포트	-			
(The maximum rule count is 32.)				
추가 취소				
포트 포워드 리스트				
항목	프로토콜	외부포트	포워딩 IP 주소	내부포트
포트 포워드 리스트가 없습니다.				
전체선택 삭제 취소				

3) ALG



MSN 메신저에서 파일전송, 원격지원, 화상채팅, 웹캠등의 기능이 정상동작하기 위해서는 AP에서 적절한 포트가 개방되어야 합니다. 이와 같은 포트 포워딩 자동개방이 UPNPD의 기능입니다.

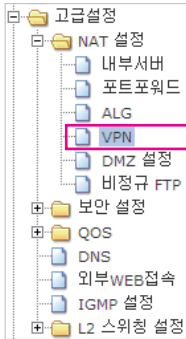
ALG 설정은 사용자들이 많이 사용하는 어플리케이션의 정상적인 동작을 위해 제공되는 기능입니다. ALG 설정을 사용하는 경우 내부 PC의 IP 주소는 고정으로 할당하는 것이 편리합니다.

ALG 설정은 다음과 같습니다.

- ▣ 사용하고자 하는 어플리케이션을 선택하고 해당 PC의 IP를 입력하고 활성화시킵니다.
- ▣ “적용” 버튼을 누릅니다.

UPNPD		활성화 v
적용 취소		
ALG	내부 IP 주소	선택
NETMEET	192.168.25.0	비활성화 v
BATTLE.NET(StarCraft,Diablo)	192.168.25.0	비활성화 v
WINAMP	192.168.25.0	비활성화 v
적용 취소		

4) VPN



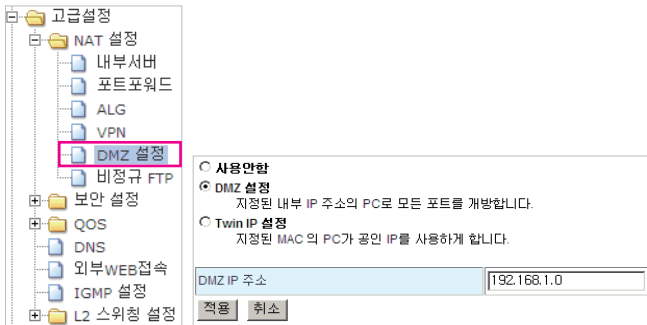
VPN Pass through 기능을 지원하며 PPTP, L2TP 및 IPSec을 사용하는 VPN(Virtual Private Networking) 서버에 접속하여 AP의 내부 PC를 사용할 수 있으며, VPN 서버에 접속하기 위해서는 해당 PC의 윈도우 운영 체제에서 가상 사설망 접속 어댑터를 설치하여야 합니다.

VPN 설정은 다음과 같습니다.

- ▣ 접속하고자 하는 VPN 서버의 프로토콜을 선택합니다.
- ▣ “적용” 버튼을 누릅니다.

VPN Pass Through	
L2TP Passthrough	비활성화 ▼
IPSec Passthrough	비활성화 ▼
PPTP Passthrough	비활성화 ▼

5) DMZ 설정



■ DMZ 설정시

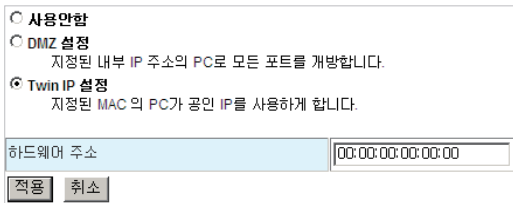
DMZ서버는 모든 TCP/UDP 포트들을 내부의 특정 IP 주소를 가지는 PC로 개방하는 기능입니다. 어플리케이션 포트번호를 알 수 없어 인터넷 공유가 정상적으로 이루어지지 않는 프로그램들은 DMZ 호스트 기능으로 해결할 수 있으며 설정방법은 다음과 같습니다.

- DMZ 설정을 선택합니다.
- PC의 IP를 입력하고 “적용” 버튼을 누릅니다.

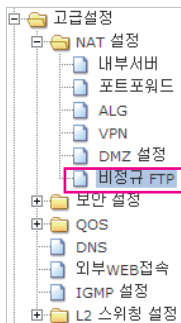
DMZ 기능을 해제하고자 할 경우에는 DMZ 선택을 해제한 후 적용버튼을 누르면 됩니다.

■ Twin IP 설정시

Twin IP(Super DMZ)서버로 지정된 PC는 WAN이 사용하는 공인 IP를 할당 받게 됩니다. Twin IP(Super DMZ)서버로 지정할 PC의 맥주소를 하단에 입력 후 “적용”을 클릭합니다.



6) 비정규 FTP

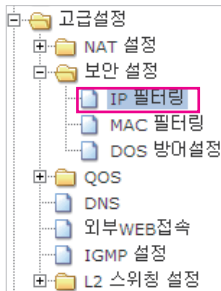


ISP나 내부 방화벽에 의하여 정규 포트(21번)이 차단되었을 때, 비정규 FTP 서버를 운영하는 경우 사용하는 기능입니다. 최대 4개의 비정규 FTP포트를 사용할 수 있습니다.

비정규 FTP 포트 설정		
서버 IP 주소	포트번호	선택
192.168.1.0	0	활성화 ▼
192.168.1.0	0	비활성화 ▼
192.168.1.0	0	활성화 ▼
192.168.1.0	0	비활성화 ▼
적용 취소		

3.4.2 보안설정

1) IP 필터링



IP Filter기능을 통해 발신/수신 패킷 필터로 특정 IP에서 시작하거나 도착하는 데이터를 TCP,UDP,ICMP 포트 등으로 Filtering을 할 수 있습니다.

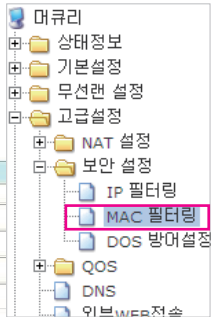
IP/Port 필터링 설정						
프로토콜	TCP					
발신IP/ MASK						
학신IP/ MASK						
발신포트						
학신포트						
허용/차단	차단					
(The maximum rule count is 32.)						
추가 취소						
IP/Port 필터링 리스트						
항목	프로토콜	발신IP	학신IP	발신포트	학신포트	허용/차단
필터링 리스트가 없습니다.						
전체선택 삭제 취소						

- 사용하고자 하는 프로토콜 항목을 선택/입력 합니다.
 - Protocol : ALL(모두), TCP, UDP, ICMP 선택
 - 발신 IP Address : 차단할 패킷의 소스 IP주소
 - 수신 IP Address : 차단 또는 허용할 목적지 IP주소
 - 발신포트 : 차단할 패킷의 소스 Port
 - 착신포트 : 차단 또는 허용할 목적지 Port
 - 허용/차단 : 허용, 차단 선택
- “추가” 버튼을 누릅니다.
- 다른 IP Filter를 원하면 “추가”를 누른 후 위의 과정을 반복하고 설정된 IP Filter 기능을 원하지 않을 경우 해당 리스트를 선택한 후 “삭제” 버튼을 누르면 삭제됩니다.

2) MAC 필터링

특정 내부 PC 및 외부 PC들의 통신을
PC의 MAC을 이용하여 각 포트별로
허용/차단 할 수 있습니다.

MAC 필터링 동작 설정			
포트	사용안함	허용	차단
LAN1	☒	☐	☐
LAN2	☒	☐	☐
LAN3	☐	☒	☐
LAN4	☐	☒	☐



MAC 필터링 설정	
소스 MAC주소	
포트 선택	lan1 ☐ lan2 ☐ lan3 ☐ lan4 ☐

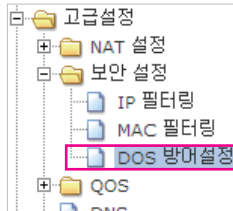
(The maximum rule count is 32.)

MAC 필터링 리스트						
항목	소스 MAC주소	Lan1	Lan2	Lan3	Lan4	허용/차단
1 ☐	00:00:C0:A8:01:02	-	-	*	-	Permit
2 ☐	00:00:C0:A8:01:04	-	-	*	*	Permit
3 ☐	00:C0:77:11:22:33	-	-	*	*	Permit
4 ☐	any	-	-	*	*	Drop

- 정책 : 차단 / 허용 중 선택합니다.
- 포트 선택 : LAN0 ~ 3 까지 개별적으로 선택 가능합니다.
- 다른 MAC 필터링을 원하면 “추가”을 누른 후 위의 과정을 반복하고 설정된 MAC Filter 기능을 원하지 않을 경우 해당 리스트를 선택한 후 “삭제” 버튼을 누르면 삭제됩니다.
- 정책이 허용인 경우에는 특정 맥 주소만 허용하는 것이므로 반드시 마지막에 해당 포트에 차단 정책을 추가해야 합니다.

3) DOS 방어설정

Denial of Service(DoS)는 한 사람이 공유자원을 모두 점유하여 다른 사람이 사용할 자원을 없애버리는 공격방식으로 AP는 DoS 방어설정 기능을 통해서 해당 공격에 방어를 할 수 있습니다. IP Filter List 설정은 다음과 같습니다.



DOS 방어 설정		
SYN Flooding	20 (Pkt/Sec) 비활성화	TCP Syn 공격 차단
Smurf	비활성화	Broadcast icmp 공격 차단
IP Source routing	비활성화	IP 소스 라우팅 차단
IP Spoofing	비활성화	IP 스푸핑 공격 차단
Port Scan	비활성화	협업 감지시 IP를 차단함. 다시 허용하려면 아래 차단 List를 보고 해제해야함.
ARP Spoofing	비활성화	ARP 스푸핑 공격 차단
Land Attack	비활성화	LAND 공격 차단
Tear Drop	비활성화	TearDrop 공격 차단
Ping Of Death	비활성화	Ping Of Death 공격 차단
UDP Bomb	비활성화	UDP Bomb 공격 차단
MAC Flood Guard	0 (Pkt/Sec) 0 (BlockTime:Sec) 비활성화	초당 CPU로 인입되는 패킷 수가 입력된 값을 넘을 경우 지정시간동안 차단한다.

적용 취소

차단된 IP 리스트

항목 차단 IP주소

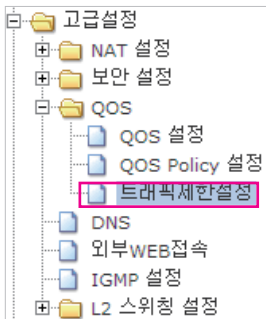
차단된 IP 리스트가 없습니다.

허용 IP주소

적용 취소

- 방어하고자 하는 DoS 공격의 종류를 선택하고 "활성화" 선택하고 "적용" 클릭합니다
- 선택된 DoS 공격을 해제하고자 할 경우 "비활성화" 선택하고서 "적용" 클릭합니다.
- DOS 방어 설정 후 외부에서 DOS 공격이 시도되면 해당 IP는 접근이 차단이 됩니다.
- 차단된 IP를 허용하려면 아래와 같이 해당 IP를 선택한 후 Allow IP "적용"버튼을 누르거나 AP를 리부팅하면 차단이 해제됩니다.
- 차단이 해제되더라도 해당 IP는 AP가 리부팅되기 전까지 Blocked IP List에 남아있게 됩니다.

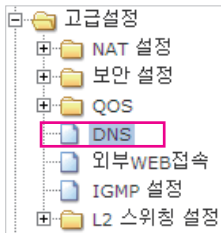
4) 트래픽제한설정



모든 포트에 대해 입력/출력 트래픽을 조절할 수 있으며, 특정 포트의 트래픽을 다른 포트의 트래픽 보다 우선순위를 높여 설정함으로써 물리적 포트에 대한 트래픽 보장 기능을 사용합니다. 무선 관련 MAC Filtering 기능에 대한 설정을 변경합니다.

포트별 우선순위 및 트래픽 제한 설정				
포트	흐름제어	입력 트래픽량 (단위:100Kbps)	출력 트래픽량 (단위:100Kbps)	포트우선순위
WAN	비활성화 ▼	1000	1000	비활성화 ▼
LAN0	비활성화 ▼	1000	1000	비활성화 ▼
LAN1	비활성화 ▼	1000	1000	비활성화 ▼
LAN2	비활성화 ▼	1000	1000	비활성화 ▼
LAN3	비활성화 ▼	1000	1000	비활성화 ▼
적용 취소				

3.4.3 DNS



DNS(Domain Name System)는 호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나 그 반대의 변환을 수행할 수 있도록 하는 것입니다. 기본 DNS 주소는 1차 DNS 서버 주소이며, 보조 DNS 주소는 2차 DNS 서버 주소에 해당 합니다. DNS 설정은 고정설정 및 자동설정이 있으며 어떠한 경우라도 사용자의 PC에 자동으로 설정된DNS IP를 내려보내 줍니다.

■ 고정설정의 경우

본 Manual의 5.4절 DHCP 설정에서 설명된 것처럼 사용자가 원하는 고정 DNS IP를 설정해서 PC가 DHCP를 통해서 자동으로 DNS IP를 받을 수 있습니다.

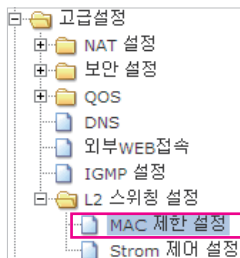
■ 자동설정의 경우

네트워크의 DHCP server로부터 받은 DNS IP를 PC에 자동으로 내려 보내줍니다. 이 경우 아래의 창에서와 같이 DNS-Setup에 DNS IP가 자동 설정됩니다.

DNS 설정	
고정 기본 DNS 서버	165.133.1.13
고정 보조 DNS 서버	168.126.63.1
유동 기본 DNS 서버	165.133.1.13
유동 보조 DNS 서버	168.126.63.1
적용 취소	

3.4.4 L2 스위치 설정

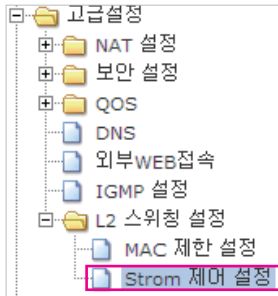
1) MAC 제한 설정



각 포트별 접속되는 단말의 개수를 제한합니다. 각 포트당 최대 4개까지 지원합니다.

포트별 MAC 주소 제한 설정	
포트	제한할 MAC 갯수
LAN0	0
LAN1	0
LAN2	0
LAN3	0
적용 취소	

2) Storm 제어 설정



비정상적인 패킷의 유입으로 CPU의 부하가 높아지는 것을 방지하기 위해 다음의 기능을 제공합니다. 각 포트별로 storm control 제어가 가능합니다.

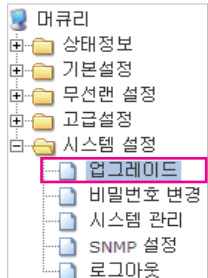
포트별 폭주 제어 기능 설정	
포트	폭주제어
WAN	비활성화 ▼
LAN0	비활성화 ▼
LAN1	비활성화 ▼
LAN2	비활성화 ▼
LAN3	비활성화 ▼
적용 취소	

3.5 시스템 설정

시스템 설정에서는 다음과 같은 내용으로 이루어져 있습니다.

시스템 설정은 업그레이드 시스템관리와 같이 장비 운영에 관한 부가적인 기능을 이용하고자 할 경우 설정하는 메뉴입니다.

- 업그레이드
- 비밀번호 변경
- 시스템 관리
- SNMP 설정
- 로그아웃



3.5.1 업그레이드

펌웨어는 이중화 되어 있기 때문에 펌웨어 1,2 로 나누어져 있으며 “펌웨어 정보”에는 버전 정보, 운용중인 펌웨어 사이드, 생성날짜를 보여줍니다.

펌웨어 정보	
펌웨어 1 버전정보	1.01.08
펌웨어 2 버전정보	0.00.01
현재 운용중인 펌웨어	1
이미지 생성날짜	Aug 31 2009,10:26:58
업그레이드	
펌웨어 업그레이드 형식	랜에 접속된 PC를 이용 ▼
업그레이드 적용위치	☐ 펌웨어 1 ☒ 펌웨어 2
RESET이후 로딩될 이미지	☐ 펌웨어 1 ☒ 펌웨어 2
펌웨어 위치	찾아보기...
적용	

- 펌웨어 업그레이드 방식 : 랜에 접속된 PC를 이용/ TFTP 서버를 이용한 업그레이드
- 업그레이드 적용위치 : 이미지 WRITE할 펌웨어 위치 설정
- RESET이후 로딩될 이미지 : 업그레이드 이후 RESET 했을때 시작될 이미지

1) 랜에 접속된 PC를 이용한 업그레이드

펌웨어 정보	
펌웨어 1 버전정보	1.01.08
펌웨어 2 버전정보	0.00.01
현재 운용중인 펌웨어	1
이미지 생성날짜	Aug 31 2009,10:26:58
업그레이드	
펌웨어 업그레이드 형식	랜에 접속된 PC를 이용 ▼
업그레이드 적용위치	☐ 펌웨어 1 ☒ 펌웨어 2
RESET이후 로딩될 이미지	☐ 펌웨어 1 ☒ 펌웨어 2
펌웨어 위치	찾아보기...
적용	

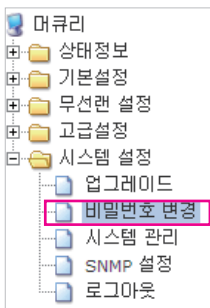
※ 펌웨어 위치는 랜에 접속된 로컬 PC의 디렉토리에서 찾을 수 있습니다.

2) TFTP 서버를 이용한 업그레이드

펌웨어 정보	
펌웨어 1 버전정보	1.01.08
펌웨어 2 버전정보	0.00.01
현재 운용중인 펌웨어	1
이미지 생성날짜	Aug 31 2009,10:26:58
업그레이드	
펌웨어 업그레이드 형식	TFTP 서버 이용 ▼
업그레이드 적용위치	☐ 펌웨어 1 ☒ 펌웨어 2
RESET이후 로딩될 이미지	☐ 펌웨어 1 ☒ 펌웨어 2
서버 주소	165.133.13.210
펌웨어 이름	test.bin
적용	

※ 서버주소는 tftp 서버주소이며, 펌웨어 이름은 tftp 서버에 있는 펌웨어 이름입니다.

3.5.2 비밀번호 변경

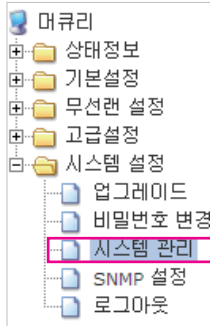


WEB을 통해서 시스템에 접속할 수 있는 계정은 “admin”이 있습니다.
 각 계정에 대한 비밀번호는 다음과 같습니다.

- admin 계정으로 WEB 접속시 비밀번호 : admin

관리자 설정	
사용자	
비밀번호	최대길이:16
비밀번호확인	
적용 취소	

3.5.3 시스템 관리



- 1) 시스템 재시작 : 장비를 재시작 합니다.
- 2) 시스템 초기화 : Factory default 값으로 초기화합니다.
- 3) 장비 이름 적용 : 장비이름을 지정합니다.
- 4) NTP 설정
전용 AP에서 사용할 현재 시간을 받아오는 타임서버와 시간 정책을 설정합니다.
 - 표준 시간대 : 나라별 시간대 적용
 - NTP 서버 : 서버를 지정합니다. 현재 default는 kriss.net입니다.
 - NTP 서버2 : default는 time.bora.net입니다.
 - DHCP 서버로부터 받은 NTP 서버 : DHCP에서 받은 ntp 서버입니다.DHCP 서버로부터 받은 NTP 서버에서 받은 정보가 제일 먼저 설정되고 실패하게 되면 NTP 서버, NTP 서버2가 그다음 우선순위가 됩니다.
- 5) DDNS 설정
DDNS 서비스란 유동 IP주소로도 서버를 운용할 수 있도록 유동 IP주소와 도메인을 매칭시켜주는 서비스입니다. 유동 IP주소가 변경되어도 변경된 IP주소는 항상 지정된 도메인과 매칭됨으로 전용AP 내부 PC에서 WEB, FTP서버를 운영하거나 전용 AP 원격 접속기능을 이용할 수 있습니다.

시스템 재시작

재시작

시스템 초기화

초기화

장비 이름 설정

Mercury_RGW

적용

취소

NTP 설정

현재시간

Sep 8 20:15:49 2009

표준 시간대

(GMT+09:00) Korean

NTP 서버

kriss.net

ex: kriss.net, time.bora.net, time.nist.gov
time.korserve.net, time.windows.com, asia.pool.ntp.org
ntp.apple.com, ntp.nasa.gov, kr.pool.ntp.org
time-a.netgear.com, time-b.netgear.com

NTP 서버2

time.bora.net

DHCP 서버로 부터 받은 NTP 서버

NTP Server Address From DHCP server
Best Priority,
Can Delete, Can't Change

적용

취소

DDNS 설정

DDNS 서버

ex: nameip.co.kr, ddns.co.kr, wowdns.com
dyndns.org, freedns.afraid.org, zoneedit.com
no-ip.com, codns.com, dnsserver.com

사용자

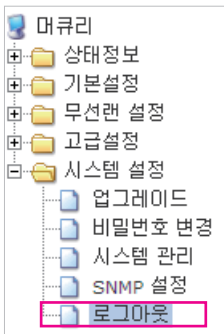
비밀번호

DDNS

적용

취소

3.5.4 로그아웃



현재 계정에서 로그아웃 하여 다른 계정 혹은 시스템 설정을 더 이상 하지 않을시에
사용하게 됩니다.



4. RUSH-314N AP 문제해결

본 장에서는 RUSH-314N AP의 문제 발생시 해결 방법에 대하여 설명합니다.



1. 문제 유형

- RUSH-314N AP 설치를 완료 후 인터넷 익스플로러가 동작하지 않습니다.
- 인터넷에 연결할 수 없습니다. RUSH-314N AP의 인터넷 상태표시등이 꺼져 있고 컴퓨터 상태표시등이 깜빡입니다.

해결 방안

인터넷에 연결할 수 없고, 인터넷 상태표시등이 꺼져 있으며 컴퓨터 상태표시 등이 깜빡이는 경우의 원인은 모뎀과 RUSH-314N AP가 정상적으로 연결되어 있지 않기 때문입니다.

- ① 모뎀과 RUSH-314N AP가 랜 케이블로 올바르게 연결되어 있는지 확인합니다. 케이블 모뎀 또는 ADSL 모뎀과 함께 제공된 랜케이블을 사용하는 것이 좋습니다. 랜케이블의 한 쪽 끝은 RUSH-314N AP의 인터넷 포트에 연결하고 다른 쪽 끝은 모뎀에 연결하여야 합니다.
- ② 케이블 모뎀 또는 ADSL 모뎀의 전원을 3분 동안 끈 다음 다시 연결합니다. 모뎀이 RUSH-314N AP를 정상적으로 인식하게 됩니다.
- ③ RUSH-314N AP의 전원을 10초 동안 껐다 다시 켭니다. RUSH-314N AP가 모뎀과 통신을 다시 시도합니다. 이 단계를 수행한 후에도 RUSH-314N AP의 인터넷 상태표시등이 켜지지 않는 경우 고객센터로 문의하십시오.
- ④ PC를 종료하고 다시 시작합니다.

2. 문제 유형

- RUSH-314N AP의 설치 완료 후 인터넷 익스플로러가 작동하지 않습니다.
- 인터넷에 연결할 수 없습니다. RUSH-314N AP 인터넷 상태표시등이 켜져 있고 컴퓨터 상태표시등이 깜빡입니다.

해결 방안

인터넷에 연결할 수 없고 인터넷 상태표시등이 켜져 있으며 컴퓨터 상태표시등이 깜빡이는 경우의 원인은 연결방식이 인터넷 서비스 업체와 일치하지 않기 때문일 수 있습니다.

- ① 수동 IP주소 연결방식을 사용하는 경우 인터넷 서비스 업체는 사용자에게 IP 주소, 서브넷 마스크 및 기본 게이트웨이 주소를 할당해야 합니다. 이 설정의 변경에 대한 자세한 내용은 '**RUSH-314N AP 인터넷 연결하기**' 항목을 참고하십시오.

3. 문제 유형

- RUSH-314N AP 설치 완료 후 인터넷 익스플로러가 작동하지 않습니다.
- 인터넷에 연결할 수 없습니다. RUSH-314N AP의 인터넷 상태표시등이 깜빡이고 컴퓨터 상태표시등이 켜져 있습니다.

해결 방안

인터넷 상태표시등이 깜빡이며 컴퓨터 상태표시등이 켜져 있지만 인터넷에 접속할 수 없는 경우 인터넷에 접속을 시도하는 PC에 타사 방화벽 소프트웨어가 설치되어 있기 때문일 수 있습니다.

타사 방화벽 프로그램으로는 ZoneAlarm, MyFireWall, Sygate Personal Firewall, McAfee Personal Firewall 및 하우리 바이로봇(방화벽 프로세서 내장) 등이 있습니다.

PC에 방화벽 소프트웨어가 설치되어 있는 경우 구성이 올바른지 확인하십시오. 방화벽 소프트웨어를 일시 해제하여 인터넷에 접속하지 못하게 할 지 여부를 결정할 수 있습니다. 만일 방화벽을 사용하지 않는 동안 인터넷 접속이 원활하게 작동되는 경우 방화벽 사용 시 올바르게 작동되도록 방화벽 설정을 변경해야 합니다.

인터넷 접속을 허용하는 방화벽 소프트웨어 구성방법은 해당 방화벽 소프트웨어 게시자가 제공하는 지침을 참고하십시오. 모든 방화벽 소프트웨어를 해제한 후에도 여전히 인터넷에 접속할 수 없는 경우 고객 센터에 문의하십시오.

4. 문제 유형

- 인터넷에 무선으로 연결할 수 없습니다.

해결 방안

무선 노트북에서 인터넷을 연결할 수 없는 경우 다음 항목을 확인합니다.

- ① RUSH-314N AP의 상태표시등을 확인합니다. 정상적인 경우 표시등의 상태는 다음과 같아야 합니다.
 - 전원 상태표시등이 켜져 있어야 합니다.
 - 무선/컴퓨터/인터넷 상태표시등이 켜져 있거나 깜빡이어야 합니다.
- ② 윈도우 화면 오른쪽 맨 아래의 시스템 트레이에 있는 무선 연결 프로그램 (WZC 혹은 인텔 PROSET/무선) 아이콘을 클릭하여 엽니다.
- ③ 열린 창은 무선 카드의 모델에 따라 다릅니다. 하지만 모든 유틸리티에는 연결 가능한 무선랜인 '사용 가능한 네트워크' 목록이 제공됩니다.

네트워크 이름(DATA)이 무선랜 검색결과에 나타납니까?

- 예, 내 네트워크 이름이 목록에 있습니다.

`인터넷에 무선으로 연결할 수 없지만, 내 네트워크 이름이 무선랜 검색결과에 있습니다.`라는 문제에 대한 해결 방법을 참조하십시오.

- 아니오, 내 네트워크 이름이 목록에 없습니다.

`인터넷에 무선으로 연결할 수 없고, 내 네트워크 이름이 무선랜 검색결과에 없습니다.`라는 문제에 대한 해결 방법을 참조하십시오.

5. 문제 유형

- 인터넷에 무선으로 연결할 수 없지만, 내 네트워크 이름이 무선랜 검색결과에 있습니다.

해결 방안

내 네트워크 이름이 “사용 가능한 네트워크” 목록에 있는 경우 무선으로 연결되도록 다음 과정을 수행합니다.

- ① “사용 가능한 네트워크” 목록에서 올바른 네트워크 이름을 클릭합니다.
- ② 무선랜 보안(암호화)을 설정한 경우 네트워크 키를 입력해야 합니다.
`윈도우 XP에서 무선랜 연결하기` 항목을 참고 하십시오.
- ③ 몇 초 내에 윈도우 화면 오른쪽 맨 아래에 있는 트레이 아이콘이 네트워크 연결을 의미하는 녹색으로 변해야 합니다.

6. 문제 유형

- 인터넷에 무선으로 연결할 수 없고 내 네트워크 이름이 무선랜 검색결과에 없습니다.

해결 방안

네트워크 이름이 무선 유틸리티의 “사용 가능한 네트워크” 목록에 없는 경우 다음 문제 해결 과정을 수행합니다.

- ① 가능하다면 일시적으로 RUSH-314N AP와 노트북의 거리를 1.5~3 미터가 되게 이동합니다. 무선 유틸리티를 닫았다가 다시 엽니다. 네트워크 이름이 사용 가능한 네트워크 목록에 나타난다면 범위나 간섭문제가 있을 수 있습니다.
- ② RUSH-314N AP와 랜케이블로 PC를 연결하고 Hide SSID 항목을 사용함으로 설정했는지 확인합니다. 이 설정은 본 사용자 설명서 `무선 네트워크 설정하기` 에서 확인할 수 있습니다.

※ 이 단계를 완료한 후에도 여전히 인터넷에 무선으로 연결할 수 없는 경우
고객센터에 문의하십시오.

7. 문제 유형

- 무선 네트워크 성능이 일정하지 않습니다.
- 데이터 전송속도가 느린 경우가 가끔 있습니다.
- 신호 세기가 약합니다.

해결 방안

무선랜 기술은 무선 통신을 기반으로 합니다. 무선 장치간 거리가 멀어지면 연결성 및 처리 성능이 떨어지게 됩니다. 신호 세기를 약화시키는 다른 요인으로 콘크리트 벽과 금속장치와 같은 장애물이 있습니다.

따라서 실내 환경에서 무선 장치를 사용할 수 있는 일반적인 범위는 30~60미터입니다. 또한 RUSH-314N AP에서 멀어질수록 연결속도는 느려집니다.

무선랜 관련 문제의 원인이 범위인지 확인하려면 가능하다면 일시적으로 RUSH-314N AP와 PC의 거리를 1.5~3미터가 되게 합니다.

■ 무선랜 채널변경

RUSH-314N AP의 무선 채널을 변경하면 주변 무선 트래픽 및 채널 간섭이 약해져서 성능 및 안전성이 증가할 수 있습니다. 다른 무선랜 채널 선택방법은 본 사용자 설명서의 **‘무선 네트워크 설정하기’** 항목을 참조하십시오.

■ 무선랜 전송속도 제한

- 무선랜 전송속도를 제한하면 최대 무선범위 및 연결 안전성이 증가할 수 있습니다.
- 대부분의 무선랜 카드에는 전송속도를 제한하는 기능이 있습니다. (기본적으로 무선랜 전송속도를 자동으로 조정하도록 설정되었습니다.)

무선랜 전송속도를 자동으로 조절하도록 설정해 두면 무선 신호가 매우 약해질 경우 연결이 주기적으로 끊어질 수 있습니다. 전송속도가 느릴수록 연결성이 증가합니다. 연결 속도를 달리 설정하여 사용자의 환경에 가장 적합한 전송속도를 찾아 봅니다.

8. 문제 유형

PC 무선랜 어댑터의 WPA(Wi-Fi Protected Access : 무선 보호 액세스) 보안을 설정하는데 문제가 있습니다.

해결방안

노트북 무선랜 어댑터에서 WPA 기능을 지원하는 소프트웨어가 제공되지 않는 경우 Microsoft에서 제공하는 '무선 보호 액세스용 Windows 지원 패치' 파일을 무료로 다운로드 할 수 있습니다.

<http://www.microsoft.com/downloads/details.aspx?displayang=kor&FamilyID=5039EF4A-61E0-4C44-94F0-C25C9DE0ACE9>

주의. Microsoft에서 제공하는 이 패치 파일은 윈도우 XP에서만 사용이 가능합니다. 그리고, 윈도우 XP 서비스팩 2에 이미 설치가 되어 있다면 다운로드가 필요하지 않습니다. 현재 다른 운영체제는 지원되지 않습니다. 무선랜 카드 제조업체가 WPA 기능을 지원하는지 확인하고 해당 제조업체의 지원 사이트에서 최신 드라이버를 다운로드 하여 설치했는지 확인해야 합니다.

- 지원되는 운영 체제
 - 윈도우 XP Professional
 - 윈도우 XP Home Edition
- WPA-PSK 사용법
 - ① 윈도우 XP에서 시작 버튼 -> 제어판(C) -> 네트워크 연결 순으로 차례로 클릭합니다.
 - ② 무선네트워크 연결 속성(R)에서 무선 네트워크 탭을 마우스 왼쪽 버튼으로 클릭하면 다음 화면이 나타납니다. Windows에서 무선 네트워크 구성(W) 확인란이 선택되어 있는지 확인합니다.
 - ③ 무선 네트워크 탭에서 추가(A) 버튼을 클릭하면 다음 화면이 표시됩니다.
 - ④ 네트워크 인증(A)에서 WPA-PSK를 선택합니다.
 - ⑤ 데이터 암호화(D)에서 TKIP이나 AES를 선택합니다. 이 설정은 RUSH-314N AP와 일치해야 합니다.
 - ⑥ 네트워크 키(K)와 네트워크 키 확인(O) 상자에 암호화 키를 입력합니다.

주의. 공유 키를 입력합니다. 이 키는 문자, 숫자, 또는 기호를 사용하여 8~63자로 구성 할 수 있습니다. 설정한 모든 클라이언트에 동일한 키를 사용해야 합니다.

- ⑦ 설정을 적용하려면 확인을 클릭합니다.

9. 문제 유형

- P2P, 온라인 게임 등을 할 수 없습니다.

해결 방안

RUSH-314N AP 내부에 연결된 PC는 RUSH-314N AP 내부 방화벽 밑에서 동작합니다.

그렇기 때문에 특정 포트를 사용하는 P2P, 온라인 게임 등 일정 프로그램이 사용이 원활하지 않을 수 있습니다. 이럴 경우 프로그램에서 사용하는 특정 포트를 열어 주어야 하며 방법은 다음과 같습니다.

- 특정 어플리케이션 설정
 - RUSH-314N AP 웹서버 고급 설정 -> NAT 설정 -> 포트 포워딩에서 특정 프로그램 포트를 열어줍니다. **프로그램 포트정보**는 프로그램 제조사에게 문의 하시길 바랍니다.
- DMZ 설정
 - RUSH-314N AP 고급설정 -> NAT 설정 -> DMZ설정에서 DMZ 기능을 설정합니다. DMZ 설정 시 바이러스 또는 해킹의 위험에 노출될 수 있습니다.
- RUSH-314N AP 컴퓨터 포트에 유무선 공유기 WAN 포트를 같이 사용할 경우
 - RUSH-314N AP 컴퓨터 포트에 유무선 공유기 WAN 포트가 연결되어 있을 경우 유무선 공유기의 NAT 설정을 해제해 주십시오.

NAT 설정을 해제하는 방법은 유무선 공유기 제조사에 문의 하시길 바랍니다.

이 페이지는 편집을 위한 공백입니다.

5. 부록

본 장에서는 RUSH-314N AP 사용상 무선랜 연결방법에 대해 기술합니다.

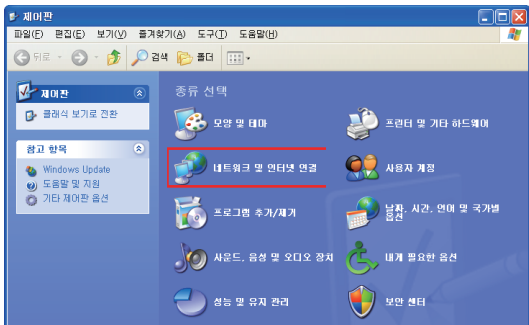
- 윈도우 XP에서 무선랜 연결방법



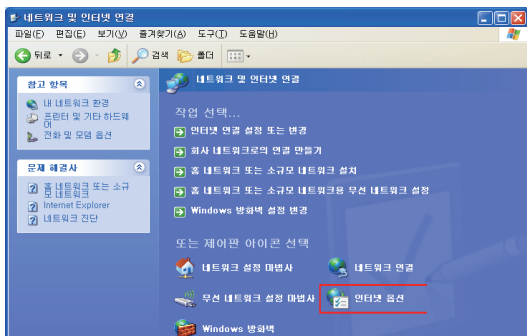
부록 A : 윈도우 XP에서 무선랜 연결방법

PC에서 무선랜 서비스를 이용하기 위해서는 PC, 노트북에 무선랜 카드가 설치되어 있어야 하고 윈도우 XP에서는 무선연결 프로그램(Zero Configuration)이 내장되어 있으며 윈도우98/ME/2000에서는 무선연결 프로그램을 지원하지 않으므로 무선랜 카드 제조사에서 제공하는 무선연결 프로그램(무선랜 드라이버)을 사용하시기 바랍니다. (무선랜 카드 사용설명서 참조 또는 무선랜 카드 제조사/판매사에게 문의 바랍니다.)

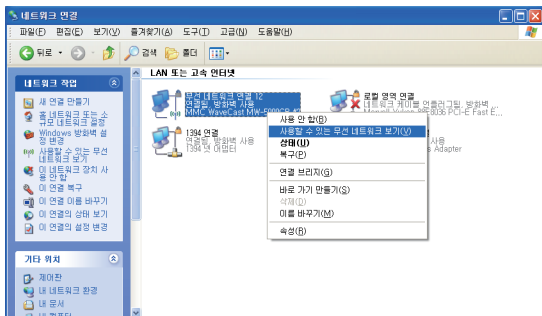
1. 제어판(C)에서 네트워크 및 인터넷 연결을 클릭합니다.



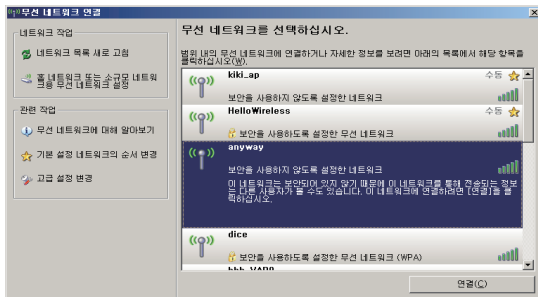
2. 네트워크 및 인터넷 연결에서 네트워크 연결을 클릭합니다.



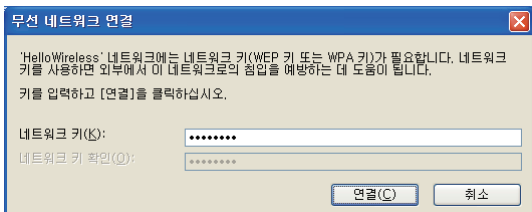
3. 네트워크 연결 -> 무선네트워크 연결을 선택 후 마우스 오른쪽 버튼을 클릭하여 사용할 수 있는 무선네트워크 보기(V)를 선택합니다.



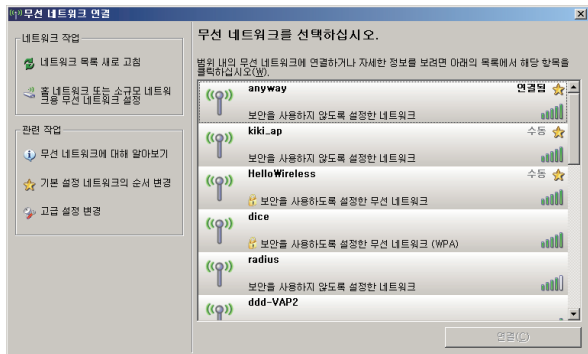
4. 사용 할 수 있는 무선네트워크에서 RUSH-314N AP의 네트워크 이름(SSID)인 “Anyway”를 누릅니다.



5. RUSH-314N AP에 암호화 기능이 설정되어 있을 경우 연결 시 암호를 확인해야 합니다. RUSH-314N AP에 설정한 암호와 동일한 정보를 입력하면 됩니다.



6. 정상적으로 연결이 되면 SSID 오른쪽에 연결됨 표시가 나옵니다.



(윈도우XP의 무선 네트워크 속성은 운영체제 패치 버전에 따라 화면형태가 다를 수 있습니다.)

부록 B : 무상/유상 AS 기준

유/무상 AS 및 타사인터넷망 사용방법 관련하여 아래 사항을 참고하시고, 문의는 근무시간중에 고객센터(1566-5202)로 하시기 바랍니다.

1. 무상AS

제품 보증기간 이내에 정상적인 사용중에 발생한 성능, 기능상의 고장 발생시 (택배비는 고객이 부담, 고객센터 1566-5202 (근무시간內)로 문의)

2. 유상AS

① 소비자 과실로 고장난 경우

- 사용 잘못 또는 취급 부주의로 인한 고장(낙하, 침수, 충격, 무리한 작동등)
- 당사 지정 서비스센터가 아닌 장소 및 사람이 수리하여 고장이 발생한 경우
- 소비자의 고의 또는 과실로 인한 고장인 경우
- 정품 이외의 부품이나 부속물 사용에 의한 고장이나 제품파손의 경우

② 그 밖의 경우

- 천재지변 (화재,염해,수해,이상전원 등)에 의한 고장 발생시
- 소모성 부품의 수명이 다한 경우 (배터리,안테나,램프류 및 각종 부착물)
- 사용설명서 내용과 다른 방법으로 설치한 경우

3. 환불기준

단말 구매후 14일 이내일 경우에 고객과실이 아닌 정상적인 사용상태에서 발생한 성능, 기능상의 하자 고장 발생에 대해서 장비의 부속품의 Full set를 반환할 경우에 만 환불이 가능합니다

4. 타사 인터넷 망에서 사용방법

본 장비는 SK브로드밴드 초고속인터넷망에서 최적의 상태로 동작하도록 설정이 되어 있으므로, SK브로드밴드의 초고속인터넷 서비스를 해지하고 타사 인터넷망에서 사용할 경우에는 SK브로드밴드의 Call센터(국번없이 106번의 2번 장애상담)에 연락하여 장비설정을 변경하시기 바랍니다.

제 품 보 증 서

(주)머큐리에서 생산, 판매한 제품은 제반 법규정과 표준을 준수하여 설계 및 제작되었으며 제품설명서에 명시된 내용에 따라 사용하시면 항상 최적의 상태와 최고의 성능을 보장 받으실 수 있습니다. (주)머큐리는 고객 여러분께서 제품을 구매한 날로부터 아래와 같은 내용으로 12개월 동안 무상 유지 보수를 보장합니다.

1. 보증 기간 - 구매 일로부터 12개월 동안 무상 유지보수

상기 기간 중 장비의 하드웨어 오류로 인한 장애가 발생할 경우에는 구매사(대리점)로부터 무상 수리 및 교환 서비스를 받으실 수 있습니다.

2. 보증기간 이후 서비스 보장

보증기간 이후에도 단종되지 않은 제품에 대해서는 계속적인 수리 및 교환 서비스를 유상으로 제공 받을 수 있습니다.

3. 고객 등록 카드 등록

아래의 제품 보증 고객 등록 카드를 기입하시고 당사로 등록하시면 보다 빠른 수리 및 교환 서비스를 제공 받으실 수 있고, 개선된 제품정보를 E-mail로 받으실 수 있습니다.

4. 예외 사항(하기 사항의 경우에는 유상으로 서비스가 제공됩니다.)

- 1) 천재지변(화재, 염해, 가스, 지진, 풍수해, 낙뢰 등) 시
- 2) 사용자의 부주의(사용 전원이상, 접속기기 불량) 시
- 3) 인가되지 않은 인력에 의한 수리개조 시

※ 구매일이 기입된 본 보증서를 제시하여야 서비스를 보장 받으실 수 있으니 잘 보관하시기 바랍니다.

제 품 명 :

제품번호 :

구 매 일 : 년 월 일

고객성명 :



- 올바르게 안전한 사용을 위하여 사용전에 사용설명서를 반드시 읽어 보시기 바랍니다.
- 사용설명서의 내용은 AP의 소프트웨어 버전에 따라 다를 수 있으며, 사용자에게 통보없이 일부 변경될 수 있습니다.

www.skbbroadband.com
SK브로드밴드 Call센터
(국번없이 106번의 2번 장애상담)