



RM5

IEEE802.11a/n Wi-Fi
Ethernet to Wi-Fi Bridge

A급 기기

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의 하시기 바라며 가정외의 지역에서 사용하는 것을 목적으로 합니다.

목차

Chapter 1: 개요	-----	1
소개	-----	1
네트워크 모드	-----	1
무선 모드	-----	2
시스템 요구 사항	-----	2
시작하기	-----	2
네비게이션	-----	2
Chapter 2: MAIN	-----	3
Status	-----	3
Monitor	-----	7
Chapter 3: 로고	-----	17
airMAX Settings	-----	17
airSelect	-----	19
airView	-----	20
Chapter 4: WIRELESS	-----	24
Basic Wireless Settings	-----	25
Wireless Security	-----	30
Chapter 5: NETWORK	-----	34
Network Role	-----	34
Configuration Mode	-----	36
Management Network Settings (Bridge)	-----	37
Management Network Settings (Router, SOHO)	-----	38
WAN Network Settings	-----	38
LAN Network Settings	-----	42
DHCP Address Reservation	-----	44
Port Forwarding	-----	45
Multicast Routing Settings	-----	45
Interfaces	-----	46
IP Aliases	-----	46
VLAN Network	-----	46
Bridge Network	-----	47
Firewall	-----	48
IPv6 Firewall	-----	49
Static Routes	-----	50
IPv6 Static Routes	-----	50
Traffic Shaping	-----	51

Chapter 6: ADVANCED	-----	52
Advanced Wireless Settings	-----	53
Advanced Ethernet Settings	-----	54
Signal LED Thresholds	-----	55
Chapter 7: SERVICES	-----	55
Ping Watchdog	-----	56
SNMP Agent	-----	56
Web Server	-----	56
SSH Server	-----	57
Telnet Server	-----	57
NTP Client	-----	57
Dynamic DNS	-----	58
System Log	-----	58
Device Discovery	-----	58
Chapter 8: SYSTEM	-----	59
Firmware Update	-----	60
Device	-----	60
Date Settings	-----	60
System Accounts	-----	61
Miscellaneous	-----	61
Location	-----	61
Device Maintenance	-----	62
Configuration Management	-----	62
Chapter 9: Tools	-----	63
Align Antenna	-----	63
Site Survey	-----	64
Discovery	-----	64
Ping	-----	65
Traceroute	-----	66
Speed Test	-----	66
airView	-----	67
기술문의 연락처	-----	67

Chapter 1: 개요

소개

RM5 제품은 다음과 같은 강력한 무선 기능을 제공합니다.

- airMAX 프로토콜 지원
- 장거리 Point-to-Point (PtP) 연결 모드
- 다양한 채널 대역폭 설정 (제품 모델에 따라 차이가 있음)
- 자동 채널 설정
- 송신 출력 제어 (Transmit Power Control): 자동/수동
- 자동 거리 조정 (ACK Timing)

또한 사용자 편의를 제공하기 위하여 아래와 같은 기능이 추가되었습니다.

- IPv6 지원
- VLAN 을 위한 QoS
- 원격 시스템 로그인을 위한 TCP 지원
- WPA-AES, WPA2-AES 보안 지원 (WEP 보안은 AP-Repeater 모드에서만 사용)
- 5GHz 대역에서 airMAX 모드 사용 시 5 MHz 채널 대역폭 사용 가능

네트워크 모드

다음과 같은 네트워크 모드를 지원합니다.

- Transparent Layer 2 Bridge
- Router
- SOHO Router

무선 모드

다음과 같은 무선 모드를 지원합니다.

- Access Point
- Station / Client
- AP-Repeater

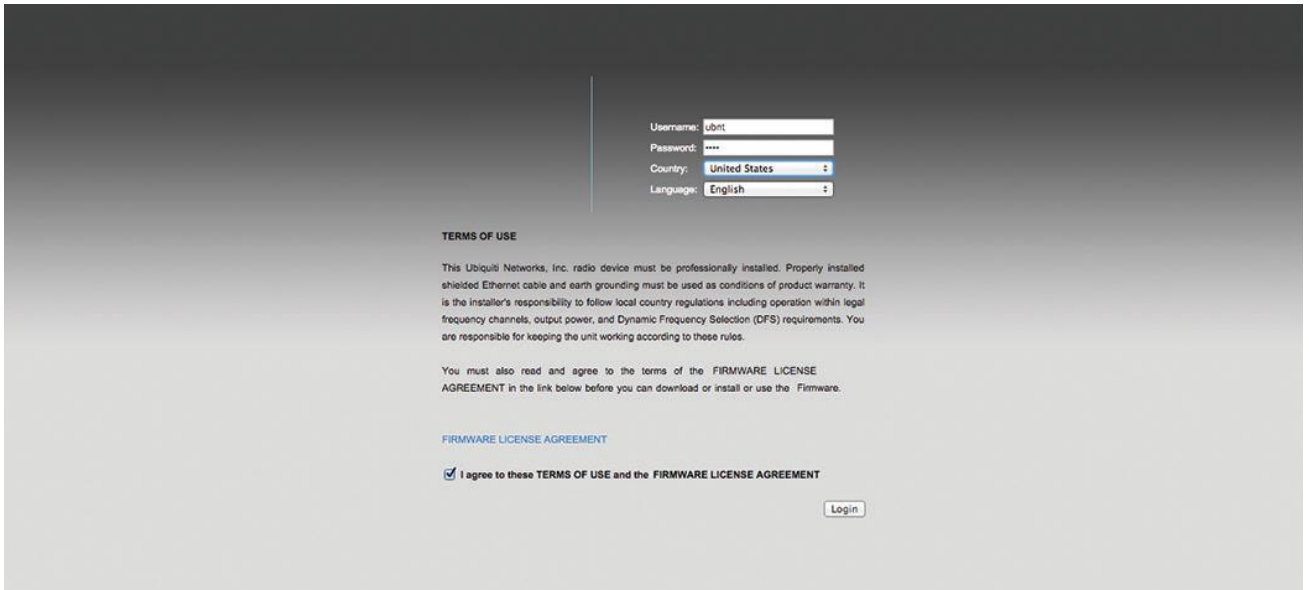
시스템 요구 사항

- Microsoft Windows 7, Windows 8, Windows 10; Linux; Mac OS X
- Java Runtime Environment 1.6 이상
- 웹 브라우저: Mozilla Firefox, Apple Safari, Google Chrome, Microsoft Internet Explorer 8 이상

시작 하기

설정 화면은 다음과 같은 단계로 접속합니다.

1. 사용자 컴퓨터의 IP 주소를 192.168.1.xxx (예: 192.168.1.100, 서버넷: 255.255.255.0) 서버넷으로 설정합니다.
2. 웹 브라우저를 실행한 후 주소 창에 **https://192.168.1.20** 를 입력한 후 **Enter** 키를 누릅니다.
3. 사용 약관 (Terms of Use)과 함께 초기 로그인 화면이 표시됩니다. Username 과 Password 항목에 **ubnt** 를 입력하고 사용 국가(Country) 와 표시 언어(Language) 를 선택합니다. "I agree to these terms of use" 앞에 위치한 박스를 체크한 후 **Login** 버튼을 클릭합니다.



4. 초기 로그인 단계에서 사용 약관에 동의하면 이후 접속 화면에서는 Username 과 Password 항목만 표시되며 아이디와 비밀번호를 입력하고 **Login** 버튼을 클릭합니다.
시스템 및 네트워크 보안을 위하여 초기 아이디와 비밀번호를 반드시 변경하시고 사용하시기 바랍니다.

네비게이션

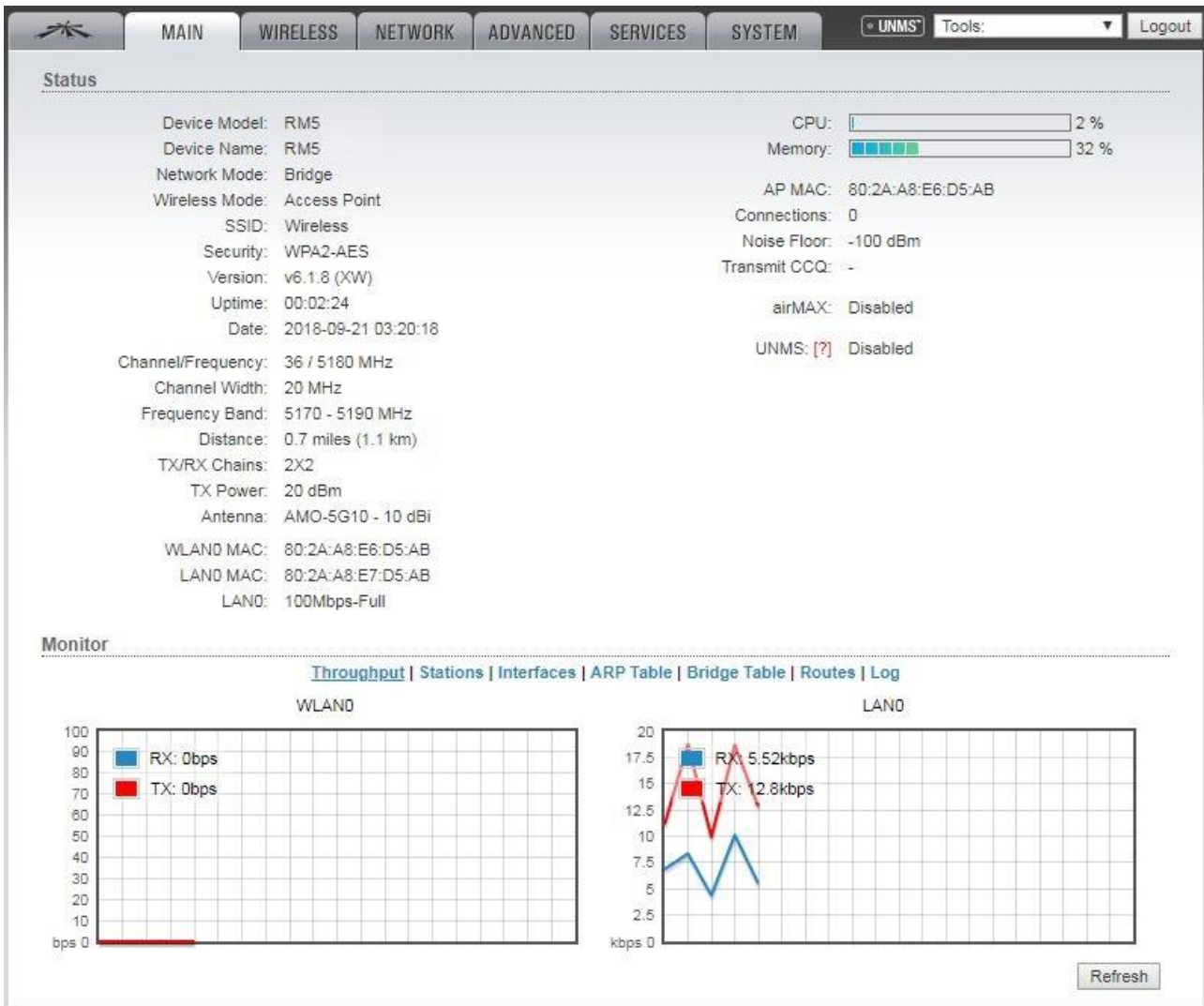
설정 인터페이스는 다음과 같이 7개의 메인 웹 페이지로 구성되어 있으며 각각의 페이지에서 특정 기능을 변경하거나 설정 및 동작 상태를 확인할 수 있습니다.

- **좌측 로고** airMAX, airView, airSelect 와 같이 독창적인 기술을 제어합니다. **MAIN** 장치 상태 및 통계 데이터, 네트워크 모니터링 링크를 표시합니다.
- **WIRELESS** 무선 모드, 무선 네트워크 이름(SSID), 802.11 모드, 채널, 주파수, 송신 출력, 데이터 변조 방식, 무선 보안 등 기본적인 무선 기능을 설정합니다.
- **NETWORK** 네트워크 운영 모드 및 IP 설정, IP 에일리어스, VLAN, 패킷 필터링, 브리징, 라우팅 경로, 트래픽 성형과 같은 기능을 설정합니다.
- **ADVANCED** 고급 무선 설정, 고급 이더넷 설정, 시그널 LED 제어 기능을 제공합니다.
- **SERVICES** Ping Watchdog, SNMP, 웹/SSH/텔넷 서버, NTP 클라이언트, 시스템 로그, 장치 검색 등의 서비스를 설정합니다.
- **SYSTEM** 시스템 관리 루틴, 관리자 계정 설정, 설치 위치 관리, 펌웨어 업데이트, 설정 백업 등의 기능을 제공합니다.

모든 페이지 우측 상단에는 네트워크 관리 및 모니터링 툴이 제공되며 다음과 같은 기능을 수행합니다.

- Align Antenna, Site Survey, Discovery, Ping, Traceroute, Speed Test, airView

Chapter 2: MAIN



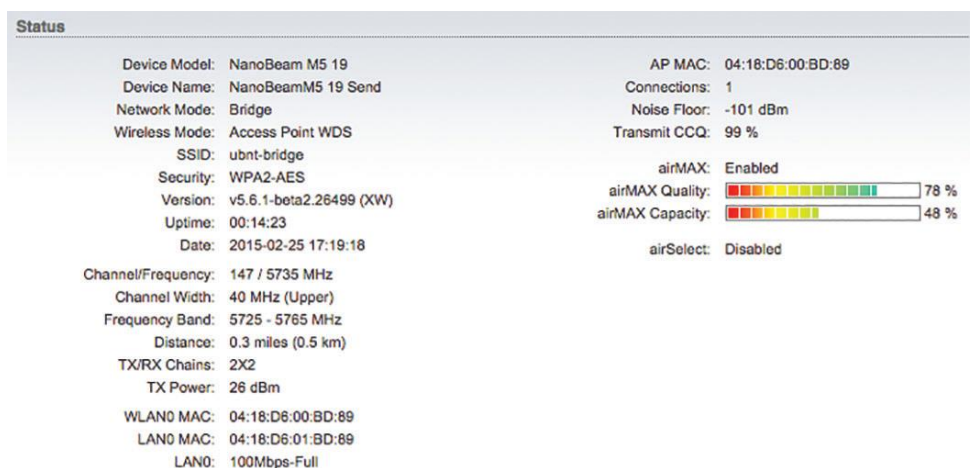
MAIN 메시지는 연결 상태 정보와 기본 설정값, 네트워크 설정 정보, 트래픽 정보 등을 표시합니다.

Status

Device Model 장치 모델명을 표시합니다.

Device Name 호스트 이름과 동일한 의미로서 장치 이름을 표시하며 사용자가 이름을 변경할 수 있습니다. 등록 화면 및 장치 검색 틀에서 장치 식별을 위해 사용됩니다.

Network Mode 네트워크 동작 모드 (Bridge, Router, SOHO Router)를 표시합니다. 상단 **NETWORK** 탭에서 동작 모드를 설정할 수 있습니다.



Wireless Mode 무선 인터페이스 동작 모드(Station, Access Point, AP-Repeater)를 표시합니다. 상단 **WIRELESS** 탭에서 무선 모드를 변경할 수 있으며 Station 또는 Access Point 모드를 선택한 상태에서 WDS(Wireless Distribution System) 모드를 추가로 설정할 수 있습니다.

RM5 제품은 airView 스펙트럼 분석 모드를 지원하며 무선 분석 기능을 사용하는 동안에는 모든 무선 연결이 종료됩니다. airView 모드는 우측 상단 **Tools** 메뉴에서 airView 를 선택하거나 상단 좌측 로고 페이지에서 **Launch airView** 메뉴를 클릭하면 실행됩니다. airView 모드를 종료하면 무선 연결이 자동으로 시작됩니다. RM5 제품은 동시에 여러 가지의 모드를 실행할 수 없으며 1가지 모드만 동작합니다. 예를 들어 Access Point 모드로 동작하는 장치에서 Station 모드를 동시에 동작 시킬 수 없습니다.

SSID 선택한 무선 모드에 따라 무선 네트워크 이름(SSID)을 표시합니다.

- Station 모드에서는 연결된 AP 장치의 SSID를 표시합니다.
- Access Point 모드에서는 **WIRELESS** 탭에서 설정한 SSID를 표시합니다.

Security 무선 장치에서 사용되는 무선 보안 모드를 표시합니다. 해당 무선 네트워크에서 보안을 사용하지 않을 경우 None 상태로 표시되고 RADIUS MAC 인증을 사용할 경우에도 None 상태로 표시됩니다.

Version 소프트웨어 버전 정보를 표시합니다.

Uptime 전원 연결 후 장치 동작 시간(일, 시간, 분, 초)을 표시합니다.

Date 현재 시스템 날짜 및 시간을 표시합니다. 시스템 날짜 및 시간은 NTP (Network Time Protocol) 프로토콜을 사용하여 인터넷을 통해 자동 설정이 가능합니다. NTP 클라이언트 기능은 상단 **SERVICES** 탭에서 설정할 수 있습니다. RM5 제품은 내부 클럭을 제공하지 않기 때문에 NTP 클라이언트 기능을 사용하지 않거나 인터넷에 연결되어 있지 않을 때 정확한 날짜와 시간을 표시할 수 없습니다.

Channel/Frequency 데이터 송수신에 사용되는 무선 채널 번호와 해당 채널의 중심 주파수를 표시합니다. 사용 가능한 채널과 주파수는 각 국가의 전파 규정에 따라 달라질 수 있습니다. DFS 문구가 표시될 경우 무선 장치가 DFS(Dynamic Frequency Selection) 채널을 사용하는 것을 나타냅니다.

Channel Width 장치에서 사용되는 무선 채널의 스펙트럼 폭을 표시합니다. RM5 제품은 3, 5, 7, 8, 10, 14, 20, 25, 28, 30, 40 MHz 스펙트럼 폭을 지원하며 제품 모델에 따라 사용 가능한 채널 폭이 다릅니다. Station 동작 모드에서 스펙트럼 폭은 Auto 20/40 MHz 기본값으로 설정됩니다.

Frequency Band 실제 장치에서 사용하는 주파수 범위를 표시합니다. 상단 **WIRELESS** 탭에서 설정한 주파수, 채널폭, 확장 채널 설정에 따라 주파수 범위가 다르게 표시됩니다.

Distance ACK 프레임을 위한 무선 장치 사이의 거리를 킬로미터/마일 단위로 표시합니다. 장치 사이의 거리를 변경하면 ACK (Acknowledgement) 타임아웃 값도 거리에 따라 자동으로 변경됩니다. 무선 송신 장치는 무선 수신 장치로 무선 데이터 프레임을 전송한 후 데이터 수신 확인 프레임을 대기합니다. ACK 타임아웃 시간동안 데이터 수신 확인 프레임을 받지 못하면 에러가 발생한 것으로 판단하고 데이터 프레임을 재전송합니다. 사용자는 무선 장치 사이의 거리를 상단 **ADVANCED** 탭에서 직접 입력하거나 자동으로 설정할 수 있습니다.

TX/RX Chains 1개의 무선 채널을 기반으로 데이터를 동시에 송수신할 때 사용되는 독립적인 무선 데이터 스트림 개수를 표시합니다. 체인 개수는 MIMO(Multiple-Input Multiple-Output) 기술을 사용하는 802.11n 장치의 특성에 따라 차이가 있습니다. TX/RX 체인은 안테나 사양에 따라 달라지기 때문에 사용하는 모델에 따라 다르게 표시됩니다.

Antenna External 안테나 타입을 표시합니다.

WLAN0 MAC 무선 네트워크에서 식별되는 장치의 MAC 주소를 표시합니다

LAN0 MAC 유선 네트워크에서 식별되는 장치의 MAC 주소를 표시합니다.

LAN1 MAC WAN 인터페이스에서 식별되는 장치의 MAC 주소를 표시합니다.

LAN0/LAN1 이더넷 포트 속도와 1000 Mbps-Full 또는 100 Mbps-Full 과 같은 이중 모드를 표시합니다. 속도 및 이중 모드가 정상적으로 표시되지 않을 경우 케이블 연결 상태를 확인하시기 바랍니다.

AP MAC Access Point 또는 AP-Repeater 모드에서는 장치 자체의 MAC 주소를 표시하고, Station 모드에서는 연결된 AP 장치의 MAC 주소를 표시합니다.

Signal Strength Station 모드에서만 표시되는 항목으로서 클라이언트 측에서 수신되는 AP 장치의 무선 신호 레벨을 그래픽막대로 표시합니다. 사용자는 장치에 내장된 안테나 조정 톨을 사용하여 무선 장치 사이의 링크 품질을 확인하고 최상의 신호 강도가 수신될 수 있도록 방향을 조정할 수 있습니다. 신호 강도는 dBm 단위로 표시되며 $\text{dBm} = 10 \log_{10}(P/1\text{mW})$ 기준으로 계산됩니다. 예를 들어 0dBm 값은 1mW 값을 기준으로 계산되고 -72dBm 값은 0.0000006mW 값을 기준으로 계산됩니다. 사용자는 최소 -80dBm 이상의 신호 강도가 수신될 수 있도록 무선 장치 사이를 연결해야 하며 -50부터 -70dBm 사이의 신호 강도로 연결하는 것이 안정적입니다.

Chain 또는 Horizontal/Vertical 또는 External/Internal (Vertical) Station 모드에서만 표시되는 항목으로서 각 신호의 레벨을 dBm 단위로 표시합니다. 안테나가 내장된 모델은 Chain 대신 Horizontal/Vertical 값이 표시됩니다. Chain 값이 표시될 경우 장치 모델에 따라 체인 개수가 다르게 표시됩니다.

Connections Access Point 또는 AP-Repeater 모드에서만 표시되는 항목으로서 AP 장치에 현재 연결되어 있는 무선 클라이언트 장치 개수를 표시합니다.

Noise Floor 동작 주파수에서 간섭으로 인해 발생하는 환경 노이즈 값을 dBm 단위로 표시합니다. RM5 제품은 신호 품질 (SNR:Signal-to-Noise, RSSI) 값을 계산할 때 Noise Floor 값을 사용합니다.

Transmit CCQ 무선 클라이언트 연결 품질(CCQ: Client Connection Quality)을 평가합니다. 완벽한 연결 상태를 100% 라고 가정했을 때의 상대적인 값을 퍼센트 단위로 표시합니다.

TX Rate/RX Rate Station 모드에서만 표시되는 항목으로서 현재의 802.11 데이터 전송 속도 및 수신 속도를 표시합니다.

airMAX airMAX 상태를 표시합니다. airMAX 기능을 사용할 경우 airMAX 기능을 사용하는 클라이언트 장치들만 airMAX AP 장치에 연결할 수 있습니다. airMAX 기능은 고급 QoS 자동감지 기능을 지원합니다.

airMAX Priority airMAX 기능을 사용하는 Station 장치에서만 표시되는 항목으로서 상단 좌측 **로고** 탭에서 airMAX Priority 값을 설정합니다. AP 장치는 기본적으로 연결된 모든 클라이언트 장치들에게 동일한 전송 시간을 부여합니다. 하지만 클라이언트 장치들이 서로 다른 우선권으로 설정되어 있을 경우 우선권 설정에 따라 특정 클라이언트에 더 많거나 적은 전송 시간을 부여합니다.

airMAX Quality airMAX 기능을 사용할 경우 물리적 연결 품질 및 재시도 회수에 따라 AMQ(airMAX Quality) 값을 표시합니다. 간섭이 발생하면 표시되는 값이 낮아지기 때문에 사용 주파수를 다른 채널로 변경해야 합니다. 80% 이상의 값이 표시될 경우 사용 채널을 변경할 필요가 없습니다.

airMAX Capacity airMAX 기능을 사용할 경우 무선 전송 효율에 따라 AMC(airMAX Capacity) 값을 표시합니다. 예를 들어 저속으로 1대의 클라이언트 장치가 연결되어 있거나 2x2 MIMO 클라이언트 장치와 함께 1x1 장치(DIVA-WDS 제품)를 사용할 경우 동일한 크기의 데이터를 전송하는데 보다 많은 전송 시간(Slot)이 소요되기 때문에 다른 클라이언트 장치들의 효율도 함께 저하시키게 됩니다. AMC 값이 낮아질수록 AP 장치의 효율도 낮아집니다. 1개의 클라이언트 장치만 연결되어 있을 경우에는 문제가 되지 않지만 30개 이상의 많은 클라이언트 장치들을 연결할 경우에는 AMC 값이 매우 중요합니다. AMC 값이 가능한 높아지도록 무선 네트워크를 구성하시기 바랍니다.

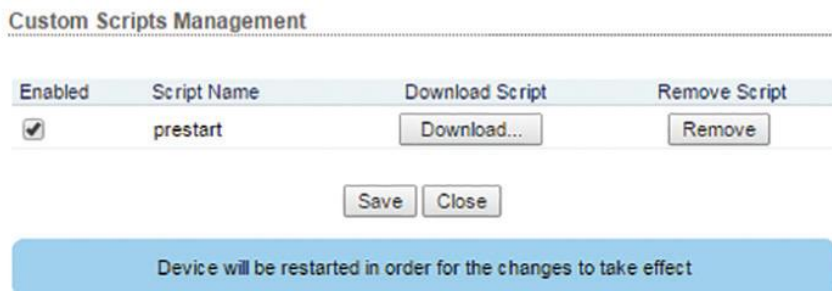
클라이언트 장치에서 AMC 값은 완벽한 링크 품질에서의 최대 성능을 기반으로 퍼센트 값을 표시합니다. 무선 효율이 낮은 클라이언트 장치는 데이터를 전송하는데 많은 시간을 필요로 하기 때문에 다른 클라이언트 장치의 효율도 저하시킬 수 있습니다. 예를 들어 A 클라이언트 장치가 이론적으로 MCS 15 (130Mbps) 속도를 사용할 수 있지만 낮은 신호 품질로 인해 MCS 12 (78Mbps) 속도를 사용한다고 가정합니다. 이때 AMC 값은 60% (현재속도 / 최대속도)로 표시됩니다. 동일한 방식으로 1x1 장치는 2x2 장치의 절반 성능을 제공하기 때문에 최대 MAC 값의 50% 를 표시하게 됩니다.

AP 장치에서 AMQ 및 AMC 항목은 모든 클라이언트 장치 값의 평균 값으로 표시됩니다. AP 장치의 AMC 값이 낮게 표시될 경우 전체 효율을 저하시키는 클라이언트 장치를 추적해야 합니다. 각 클라이언트 장치에 접속하여 전송 효율을 확인하시기 바랍니다. 효율이 낮은 클라이언트 장치는 이득이 높은 안테나로 업그레이드하여 전송 속도를 높일 수 있으며 1x1 장치는 2x2 장치로 업그레이드 하실 것을 권장합니다.

airSelect Access Point 또는 AP-Repeater 모드에서만 표시되는 항목으로서 airSelect 사용 상태를 표시합니다. airSelect 기능을 사용할 경우 airSync 기능을 함께 사용할 수 없습니다. airSelect 기능은 상단 좌측 **로그** 탭에서 설정합니다.

Hop Interval airSelect 기능을 사용할 경우 표시되는 항목으로서 다른 주파수로 사용 채널을 변경하기 전까지의 채널 사용 시간을 ms 단위로 표시합니다.

Custom Scripts 장치에 설정한 사용자 스크립트가 표시됩니다. 사용자 스크립트가 실행되면 **MAIN** 페이지에 Detected 로 옵션 상태가 표시되고 **Manage** 버튼도 표시됩니다.



- **Enabled** 실행할 사용자 스크립트를 선택합니다.
- **Script Name** 스크립트 이름을 표시합니다.
- **Download Script** 버튼을 클릭하면 선택한 사용자 스크립트를 다운로드 합니다.
- **Remove Script** 버튼을 클릭하면 선택한 사용자 스크립트를 제거합니다.
- **Save** 버튼을 클릭하면 변경된 사항을 저장한 후 시스템이 자동으로 재부팅됩니다.
- **Close** 버튼을 클릭하면 **Custom Scripts Management** 창이 종료됩니다.

airMAX Gateway airMAX 장치가 airMAX Gateway에 연결된 CPE 장치일 경우 표시됩니다. **Connected (Click to manage)** 링크를 클릭하면 원격 airGateway 장치에 접속할 수 있습니다.

Status	
Device Model:	Rocket M5 GPS
Device Name:	Rocket M5 GPS
Network Mode:	Router
Wireless Mode:	Station
SSID:	ubnt
Security:	none
Version:	v5.6-beta.21238
Uptime:	00:18:36
Date:	2014-02-25 11:08:29
Channel/Frequency:	157 / 5785 MHz
Channel Width:	20 MHz
Frequency Band:	5775 - 5795 MHz
Distance:	0.7 miles (1.1 km)
TX/RX Chains:	2X2
WLAN0 MAC:	00:27:22:9C:DA:C7
LAN0 MAC:	00:27:22:9D:DA:C7
LAN1 MAC:	02:27:22:9D:DA:C7
LAN0 / LAN1:	100Mbps-Full / Unplugged
AP MAC:	Not Associated
Signal Strength:	-
Chain 0 / Chain 1:	0 / 0 dBm
Noise Floor:	-
Transmit CCQ:	-
TX/RX Rate:	- / -
airMAX:	-
GPS Signal Quality:	<input type="text" value="0"/> 0 %
Latitude / Longitude:	- / -
Altitude:	-
airMAX Gateway:	Connected (Click to manage)

CPE 기능은 페어링 호환을 위하여 v5.5.8 이상의 펌웨어 버전에서 지원됩니다. CPE 장치에서 아래와 같이 설정하시기 바랍니다.

1. 상단 WIRELESS 탭에서 Wireless Mode 를 **Station** 으로 설정합니다.
2. 상단 NETWORK 탭에서 Network Mode 를 **Router** 로 설정합니다.
3. Configuration 모드를 **Advanced** 로 설정합니다.
4. Bridge Network 섹션을 확인합니다. 모든 포트를 제거한 후 Bridge 를 제거합니다. (WAN Network Settings 참조)
5. LAN Network Settings 섹션에서 **LAN0** 를 추가하고 나머지 항목을 설정합니다. LAN0 에서 192.168.1.x 서브넷을 사용하지 않도록 주의하시기 바랍니다.
6. **Change** 버튼을 클릭합니다.

다음과 같이 airGateway 장치와 페어링을 설정합니다.

1. airGateway 장치 설정을 초기화 합니다. airGateway 장치와 이미 연결되어 있을 경우 airMAX 장치와 airGateway 장치를 모두 재부팅합니다.
2. airGateway Quick Start Guide 매뉴얼을 참조하여 airGateway 장치를 CPE 장치에 연결합니다.
3. CPE 장치의 웹 설정 인터페이스에 접속합니다.
4. MAIN 페이지에서 Connected (Click to manage) 링크를 클릭하면 airGateway 장치에 접속됩니다.

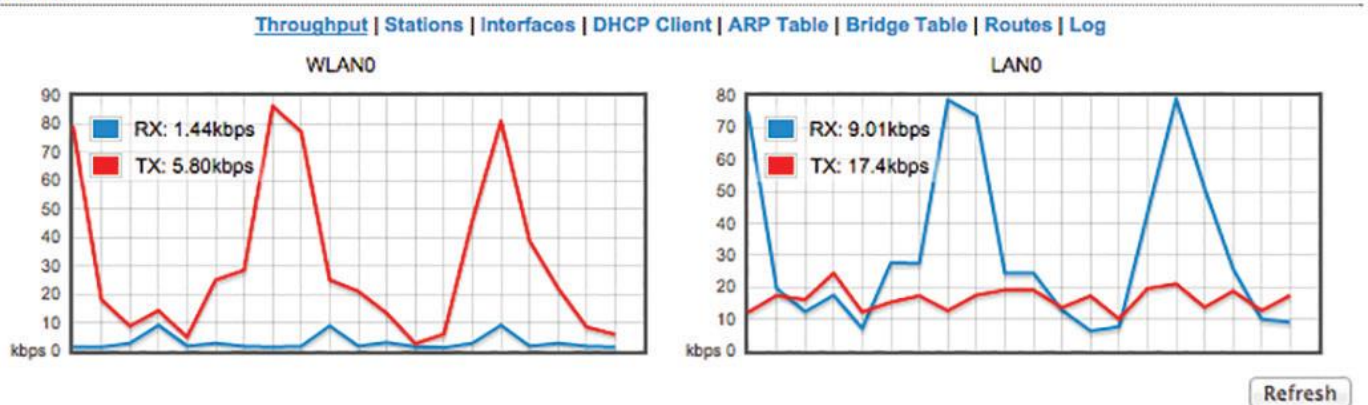
Monitor

MAIN 페이지에는 다양한 모니터링 톨로 연결되는 링크들을 제공합니다. MAIN 페이지에 접속하면 Throughput 항목이 기본으로 표시됩니다.

Throughput

현재 LAN 과 WLAN 인터페이스를 통해 발생하는 데이터 트래픽을 그래픽 이미지와 수치 데이터로 표시합니다. 평균 트래픽 값에 따라 차트 범위 및 처리량 크기(Bps, Kbps, Mbps) 가 자동으로 변경되고 통계 자료가 자동으로 업데이트 됩니다.

Monitor



Refresh 자동 업데이트에 지연이 발생할 경우 Refresh 버튼을 클릭하여 수동으로 통계 수치를 업데이트 합니다.

Stations

Access Point 및 AP-Repeater 모드에서만 표시되는 항목으로서 장치에 연결된 Station 정보를 표시합니다.

Monitor

[Throughput](#) | [Stations](#) | [Interfaces](#) | [DHCP Client](#) | [ARP Table](#) | [Bridge Table](#) | [Routes](#) | [Log](#)

Station MAC	Device Name	TX Signal, dBm Chain0/Chain1	RX Signal, dBm Combined	Noise, dBm	Latency, ms	Distance, miles	TX/RX, Mbps	CCQ, %	Connection Time	Last IP	Action
04:18:D6:00:BB:6D	NanoBeamM5 19 Rec	-74 / -72	-65	-101	1	0.3	108 / 162	94	00:14:05	10.0.2.193	kick

[Refresh](#)

Station MAC 연결된 Station 장치의 MAC 주소를 표시합니다. MAC 주소를 클릭하면 Station 장치에 대한 추가 정보를 확인할 수 있습니다.

Station 04:18:D6:00:BB:6D [1]

Device Name: NanoBeamM5 19 Rec	Negotiated Rate	Last Signal, dBm
Product: NanoBeam M5 19	MCS0	N/A
Firmware: XW.ar934x.v5.6.1-beta2.26499.150225.1705	MCS1	N/A
Connection Time: 00:14:28	MCS2	N/A
RX Signal: -66 dBm	MCS3	N/A
TX Signal: -69 dBm	MCS4	-72
Noise Floor: -101 dBm	MCS5	N/A
Distance: 0.3 miles (0.5 km)	MCS6	N/A
CCQ: 99%	MCS7	N/A
TX Power: 26 dBm	MCS8	N/A
airMAX Priority: None	MCS9	N/A
airMAX Quality: 76%	MCS10	N/A
airMAX Capacity: 45%	MCS11	-70
Last IP: 10.0.2.193	MCS12	-70
TX/RX Rate: 162 Mbps / 81 Mbps	MCS13	N/A
TX/RX Bit Rate: 31.48 kbps / 2.78 kbps	MCS14	N/A
TX/RX Packets: 11196 / 1408	MCS15	N/A
TX/RX Packet Rate, pps: 1 / 1		
Bytes Transmitted: 3415497 (3.42 MBytes)		
Bytes Received: 302136 (302.14 kBytes)		

Kick
Refresh
Close

- **Station** 연결된 station 장치의 MAC 주소를 표시합니다.
- **Device Name** station 장치의 호스트 이름을 표시합니다.
- **Product** 장치의 모델명을 표시합니다.
- **Firmware** 펌웨어 버전을 표시합니다.
- **Connection Time** Station 장치가 AP에 연결된 총 시간을 일/시간/분/초 단위로 표시합니다.
- **RX Signal** 마지막으로 수신한 무선 신호 레벨을 dBm 단위로 표시합니다.
- **TX Signal** 마지막으로 송신한 무선 신호 레벨을 dBm 단위로 표기합니다.
- **Noise Floor** 동작 주파수에서 간섭으로 인한 환경 노이즈 값을 dBm 단위로 표시합니다. RM5 제품은 신호 품질 (SNR:Signal-to-Noise, RSSI) 값을 계산할 때 Noise Floor 값을 사용합니다.

- **Distance** 상단 ADVANCED 탭의 Advanced Wireless 페이지에서 Auto Adjust 기능을 설정할 경우 표시됩니다. ACK 프레임에 대한 무선 장치 사이의 거리를 마일 또는 킬로미터 단위로 표시합니다. **miles** 링크를 클릭하면 km 단위로 거리를 표시하고 **km** 링크를 클릭하면 다시 miles 단위로 거리를 표시합니다. Auto Adjust 기능을 사용하면 auto-acknowledgement timeout 알고리즘에 따라 프레임 ACK 타임아웃 값을 자동으로 최적화합니다.
- **CCQ** AP 장치와의 무선 연결 품질 (CCQ: Client Connection Quality)을 평가합니다. 완벽한 연결 상태를 100% 라고 가정했을 때의 상대적인 값을 퍼센트 단위로 표시합니다.
- **TX Power** Station 장치의 무선 송신 출력을 dBm 단위로 표시합니다.
- **airMAX Priority** 다른 Station 장치와 비교하여 해당 Station 장치의 airMAX Priority를 표시합니다.
- **airMAX Quality** airMAX 기능을 사용할 경우 물리적 연결 품질 및 재시도 회수에 따라 AMQ(airMAX Quality) 값을 표시합니다. 간섭이 발생하면 표시되는 값이 낮아지기 때문에 사용 주파수를 다른 채널로 변경해야 합니다. 80% 이상의 값이 표시될 경우 사용 채널을 변경할 필요가 없습니다.
- **airMAX Capacity** 완벽한 링크 품질에서의 최대 성능을 기준으로 현재 지원되는 최대 속도를 퍼센트 단위로 표시합니다. 무선 효율이 낮은 Station 장치는 데이터를 전송하는데 많은 시간을 필요로 하기 때문에 다른 Station 장치의 효율도 저하시킬 수 있습니다.
- **Last IP** Station 장치의 최근 IP 주소를 표시합니다. IP 주소를 클릭하면 Station 장치에 접속합니다.
- **TX/RX Rate** 최근 송수신한 패킷을 기반으로 실제 802.11n 데이터 속도를 Mbps 단위로 표시합니다. 실제 데이터 속도는 변조 방식 및 동작 모드, 프로토콜에 따라 제한됩니다.
- **TX/RX Bit Rate** 마지막 순간에 송수신한 비트 수를 기반으로 사용자 데이터, 트래픽 부하, 데이터 스트림, 처리량의 비트 속도를 bps 단위로 표시합니다.
- **TX/RX Packets** AP 장치와 연결된 후 Station 장치가 송수신 한 총 패킷 개수를 표시합니다.
- **TX/RX Packet Rate, pps** 송수신 패킷 속도의 평균 값을 표시합니다.
- **Bytes Transmitted** AP 장치와 연결된 후 Station 장치가 송신한 총 데이터량을 바이트 단위로 표시합니다.
- **Bytes Received** AP 장치와 연결된 후 Station 장치가 수신한 총 데이터량을 바이트 단위로 표시합니다.
- **Negotiated Rate/Last Signal, dBm** 최근 수신한 패킷의 데이터 속도와 함께 무선 신호 레벨을 dBm 단위로 표시합니다. N/A 로 표시되는 항목은 해당 데이터 속도로 수신한 패킷이 없음을 표시합니다.
- **Kick** 버튼을 클릭하면 해당 Station 과 AP 연결이 해제됩니다.
- **Refresh** 버튼을 누르면 Station 정보가 업데이트 됩니다.
- **Close** 버튼을 클릭하면 Station 정보 창이 종료됩니다.

Device Name Station 장치의 호스트 이름을 표시합니다. 호스트 이름은 상단 SYSTEM 탭에서 변경할 수 있습니다.

TX Signal, dBm Station 장치로 최근 송신한 무선 신호 레벨을 표시합니다. **Combined** 링크를 클릭하면 Chain0 와 Chain1 신호값을 각각 표시합니다. **Chain0/Chain1** 링크를 클릭하면 결합된 신호 값을 표시합니다. 안테나 일체형 모델은 Chain 대신 **Horizontal/Vertical** 링크가 표시됩니다. 사용자는 장치 모델에 따라 Chain 개수가 다르게 표시됩니다.

RX Signal, dBm Station 장치로부터 마지막 수신한 무선 신호 레벨을 표시합니다. **Combined** 링크를 클릭하면 Chain0 와 Chain1 신호값을 각각 표시합니다. **Chain0/Chain1** 링크를 클릭하면 결합된 신호 값을 표시합니다. 안테나 일체형 모델은 Chain 대신 **Horizontal/Vertical** 링크가 표시됩니다. 사용자는 장치 모델에 따라 Chain 개수가 다르게 표시됩니다.

Noise, dBm 노이즈 레벨을 표시합니다.

Latency 상단 ADVANCED 탭의 Advanced Wireless 페이지에서 Auto Adjust 기능을 설정할 경우 표시됩니다. 무선 프레임에 대한 전송 지연 시간을 ms 단위로 표시합니다.

Distance 상단 ADVANCED 탭의 Advanced Wireless 페이지에서 Auto Adjust 기능을 설정할 경우 표시됩니다. ACK 프레임에 대한 무선 장치 사이의 거리를 마일 단위로 표시합니다. miles 링크를 클릭하면 km 단위로 거리를 표시하고 km 링크를 클릭하면 다시 miles 단위로 거리를 표시합니다. Auto Adjust 기능을 사용하면 auto-acknowledgement timeout 알고리즘에 따라 프레임 ACK 타임아웃 값을 자동으로 최적화합니다.

TX/RX, Mbps TX 값은 마지막으로 송신한 패킷에 대한 데이터 속도를 Mbps 단위로 표시하고 RX 값은 마지막으로 수신한 패킷에 대한 데이터 속도를 Mbps 단위로 표시합니다.

CCQ, % 무선 클라이언트 연결 품질 (CCQ: Client Connection Quality)을 평가합니다. 완벽한 연결 상태를 100% 라고 가정했을 때의 상대적인 값을 퍼센트 단위로 표시합니다.

Connection Time Station 장치가 AP 연결된 시간을 일/시간/분/초 단위로 표시합니다.

Last IP Station 장치의 최근 IP 주소를 표시합니다. IP 주소를 클릭하면 해당 장치로 접속합니다.

Action Station 장치에 대한 옵션을 표시합니다. 예를 들어 **kick** 링크를 클릭하면 Station 장치의 연결을 해제합니다.

Refresh 버튼을 클릭하면 표시된 정보가 업데이트 됩니다.

AP Information

Station 모드에서만 표시되는 항목으로서 연결된 AP 장치의 정보를 표시합니다.

Monitor

[Throughput](#) | [AP Information](#) | [Interfaces](#) | [DHCP Client](#) | [ARP Table](#) | [Bridge Table](#) | [Routes](#) | [Log](#)

Access Point 04:18:D6:00:BD:89	
Device Name: NanoBeamM5 19	Negotiated Rate Last Signal, dBm
Product: NanoBeamM5 19	MCS0 N/A
Firmware: v5.5.9	MCS1 N/A
Connection Time: 00:03:33	MCS2 N/A
TX Signal: -63 dBm	MCS3 N/A
RX Signal: -61 dBm	MCS4 -65
Noise Floor: -99 dBm	MCS5 N/A
Distance: 0.3 miles (0.5 km)	MCS6 N/A
CCQ: 95%	MCS7 N/A
Last IP: 10.0.2.196	MCS8 N/A
TX/RX Rate: 54 Mbps / 81 Mbps	MCS9 N/A
TX/RX Bit Rate: 26.36 kbps / 35.73 kbps	MCS10 N/A
TX/RX Packets: 1403 / 4143	MCS11 -64
TX/RX Packet Rate, pps: 12 / 25	MCS12 -64
Bytes Transmitted: 701810 (701.81 kBytes)	MCS13 N/A
Bytes Received: 951405 (951.41 kBytes)	MCS14 N/A
	MCS15 N/A

[Reconnect](#) [Refresh](#)

Access Point 연결된 AP 장치의 MAC 주소를 표시합니다.

Device Name 연결된 AP 장치의 호스트 이름을 표시합니다.

Product AP 장치의 모델명을 표시합니다.

Firmware AP 장치의 펌웨어 버전을 표시합니다.

Connection Time Station 장치가 해당 AP 장치에 연결된 총 시간을 일/시간/분/초 단위로 표시합니다.

RX Signal 마지막으로 수신한 무선 신호 레벨을 dBm 단위로 표시합니다.

TX Signal 마지막으로 송신한 무선 신호 레벨을 dBm 단위로 표시합니다.

Noise Floor 동작 주파수에서 간섭으로 인해 발생하는 환경 노이즈 값을 dBm 단위로 표시합니다. 신호 품질(SNR:Signal-to-Noise, RSSI) 값을 계산할 때 Noise Floor 값을 사용합니다.

Distance 상단 ADVANCED 탭의 Advanced Wireless 페이지에서 Auto Adjust 기능을 설정할 경우 표시되고 ACK 프레임을 위한 무선 장치 사이의 거리를 마일 또는 킬로미터 단위로 표시합니다. **miles** 링크를 클릭하면 km 단위로 거리를 표시합니다. Auto Adjust 기능은 auto-acknowledgement timeout 알고리즘에 따라 프레임 ACK 타임아웃 값을 자동으로 최적화합니다.

CCQ AP 장치와의 무선 연결 품질 (CCQ: Client Connection Quality)을 평가합니다. 완벽한 연결 상태를 100% 라고 가정했을 때의 상대적인 값을 퍼센트 단위로 표시합니다.

Last IP AP 장치의 최근 IP 주소를 표시합니다. IP 주소를 클릭하면 AP 장치에 접속합니다.

TX/RX Rate 최근 송수신한 패킷을 기반으로 실제 802.11n 데이터 속도를 Mbps 단위로 표시합니다. 실제 데이터 속도는 변조 방식 및 동작 모드, 프로토콜에 따라 제한됩니다.

TX/RX Bit Rate 마지막 순간에 송수신한 비트 수를 기반으로 사용자 데이터, 트래픽 부하, 데이터 스트림, 처리량의 비트 속도를 bps 단위로 표시합니다.

TX/RX Packets Station 장치와 연결된 후 AP 장치가 송수신 한 모든 패킷 개수를 표시합니다.

TX/RX Packet Rate, pps 송수신 패킷 속도의 평균 값을 표시합니다.

Bytes Transmitted AP 장치와 연결된 후 AP 장치가 송신한 총 데이터량을 바이트 단위로 표시합니다.

Bytes Received AP 장치와 연결된 후 AP 장치가 수신한 총 데이터량을 바이트 단위로 표시합니다.

Negotiated Rate/Last Signal, dBm 최근 수신한 패킷의 데이터 속도와 함께 무선 신호 레벨을 dBm 단위로 표시합니다. N/A 로 표시되는 항목은 해당 데이터 속도로 수신한 패킷이 없음을 표시합니다.

Reconnect 버튼을 클릭하면 해당 AP 장치와 무선을 재연결 합니다.

Refresh 버튼을 누르면 Station 정보가 업데이트 됩니다.

Interfaces

장치 인터페이스들에 대한 이름, MAC 주소, MTU, IP 주소, 트래픽 정보를 표시합니다.

Monitor

[Throughput](#) | [Stations](#) | [Interfaces](#) | [DHCP Client](#) | [ARP Table](#) | [Routes](#) | [Port Forward](#) | [DHCP Leases](#) | [Log](#)

Interface	MAC Address	MTU	IP Address	RX Bytes	RX Errors	TX Bytes	TX Errors
BRIDGE0	00:15:6D:5A:02:07	1500	192.168.25.1	16.3M	0	90.0M	0
LAN0	00:15:6D:5B:02:07	1500	24.43.98.84	95.3M	0	15.0M	0
LAN1	02:15:6D:5B:02:07	1500	0.0.0.0	17.3M	0	90.4M	0
WLAN0	00:15:6D:5A:02:07	1500	0.0.0.0	469K	0	1.12M	0

Refresh

Interface 각각의 인터페이스 이름을 표시합니다.

MAC Address 해당 인터페이스의 MAC 주소를 표시합니다.

MTU 해당 인터페이스를 통해 송수신 가능한 최대 프레임 크기를 바이트 단위로 표시합니다. (기본값: 1500 바이트)

IP Address 해당 인터페이스의 IP 주소를 표시합니다. IPv6 를 사용할 경우 "192.168.1.20 FE80::227:22FF:FEFC:F770/64" 형태와 같이 2가지 IP 주소가 표시됩니다.

RX Bytes 해당 인터페이스를 통해 수신한 총 데이터 수를 바이트 단위로 표시합니다.

RX Errors 해당 인터페이스에서 발생한 수신 에러 개수를 표시합니다.

TX Bytes 해당 인터페이스를 통해 송신한 총 데이터 수를 바이트 단위로 표시합니다.

TX Errors 해당 인터페이스에서 발생한 전송 에러 개수를 표시합니다.

Refresh 버튼을 클릭하면 표시 정보가 업데이트 됩니다.

DHCP Client

Router 또는 SOHO Router 모드에서만 표시되는 항목으로서 장치가 외부 DHCP 서버의 클라이언트 모드로 동작할 때 WAN 측 IP 주소와 넷마스크, DNS 서버, 게이트웨이 정보 등을 표시합니다.

Monitor

[Throughput](#) | [Stations](#) | [Interfaces](#) | [DHCP Client](#) | [ARP Table](#) | [Routes](#) | [Port Forward](#) | [DHCP Leases](#) | [Log](#)

DHCP Client Information	
Interface: LAN0	DHCP Server: 76.85.238.35
IP Address: 24.43.98.84	Domain: social.rr.com
Netmask: 255.255.255.192	Total Lease Time: 11:33:14
Gateway: 24.43.98.65	Remaining Lease Time: 10:04:55
Primary DNS IP: 209.18.47.61	<input type="button" value="Renew"/> <input type="button" value="Release"/>
Secondary DNS IP: 209.18.47.62	
<input type="button" value="Refresh"/>	

Interface WAN 네트워크에 연결된 인터페이스 이름을 표시합니다.

IP Address 외부 DHCP 서버가 WAN 인터페이스에 할당한 IP 주소를 표시합니다. 외부 DHCP 서버로부터 IP 주소를 할당받지 못하면 WAN Network Settings > DHCP Fallback IP 항목에 설정된 IP 주소가 사용됩니다.

Netmask 외부 DHCP 서버가 WAN 인터페이스에 할당한 넷마스크 값을 표시합니다. 외부 DHCP 서버로부터 넷마스크 값을 할당받지 못하면 WAN Network Settings > DHCP Fallback Netmask 항목에 설정된 넷마스크 값이 사용됩니다.

Gateway 외부 DHCP 서버가 WAN 인터페이스에 할당한 게이트웨이 주소를 표시합니다.

Primary/Secondary DNS IP 외부 DHCP 서버가 할당한 DNS IP 주소를 표시합니다. DNS (Domain Name System)는 인터넷에서 전화번호부와 같은 역할을 제공하며 도메인 이름을 IP 주소로 변환합니다.

DHCP Server 장치의 WAN IP 주소를 할당하는 외부 DHCP 서버의 IP 주소를 표시합니다.

Domain 도메인 이름을 표시합니다.

Total Lease Time 외부 DHCP 서버로부터 할당 받은 IP 주소의 총 사용 시간을 표시합니다.

Remaining Lease Time 외부 DHCP 서버로부터 할당 받은 IP 주소의 남은 유효 시간을 표시합니다.

Renew 버튼을 클릭하면 외부 DHCP 서버로 IP 주소를 재요청합니다.

Release 현재 사용 중인 IP 주소를 외부 DHCP 서버에 반환합니다. Release 버튼을 클릭하면 장치의 IP 주소가 변경되기 때문에 연결된 관리 세션도 함께 종료됩니다.

Refresh 버튼을 클릭하면 표시되는 정보가 업데이트 됩니다.

ARP Table

장치에 현재 기록된 ARP (Address Resolution Protocol) 테이블 정보를 표시합니다. ARP 테이블은 네트워크에서 각각의 IP 주소를 장치 고유의 하드웨어 MAC 주소와 연결합니다. 따라서 각각의 MAC 주소마다 서로 다른 IP 주소가 할당되어야 하며 IP 주소가 중첩될 경우 네트워크 라우팅에 문제가 발생할 수 있습니다.

Monitor

[Throughput](#) | [Stations](#) | [Interfaces](#) | [DHCP Client](#) | [ARP Table](#) | [Routes](#) | [Port Forward](#) | [DHCP Leases](#) | [Log](#)

IP Address	MAC Address	Interface
192.168.25.217	00:27:22:60:06:9E	BRIDGE0
192.168.25.161	AC:81:12:74:7C:5C	BRIDGE0
24.43.98.65	00:01:5C:3D:FA:41	LAN0
192.168.25.145	00:27:22:60:00:12	BRIDGE0
192.168.25.133	E8:9A:8F:4C:DD:FF	BRIDGE0
192.168.25.185	00:27:22:12:B3:92	BRIDGE0
192.168.25.160	28:CF:DA:E5:61:66	BRIDGE0
192.168.25.158	00:27:22:60:00:02	BRIDGE0
192.168.25.157	90:27:E4:F6:34:43	BRIDGE0

Refresh

IP Address 네트워크 장치에 할당된 IP 주소를 표시합니다.

MAC Address 장치의 MAC 주소를 표시합니다.

Interface 장치가 연결된 인터페이스를 표시합니다.

Refresh 버튼을 클릭하면 표시되는 정보가 갱신됩니다.

Bridge Table

브리지는 장치 내부에서 유무선 인터페이스 및 VLAN 네트워크 인터페이스(브리지 포트) 사이를 연결합니다. Bridge Table 항목은 Bridge 모드를 설정해야 표시되며 브리지 인터페이스에서 감지된 모든 MAC 주소를 표시합니다.

Monitor

[Throughput](#) | [Stations](#) | [Interfaces](#) | [ARP Table](#) | [Bridge Table](#) | [Routes](#) | [GPS Details](#) | [Log](#)

Bridge	MAC Address	Interface	Aging Timer
BRIDGE0	70:cd:60:f1:68:7e	LAN1	0.19

Showing 1 to 1 of 1 entries

<< < 1 > >>

Refresh

Bridge 브리지 이름을 표시합니다.

MAC Address 해당 브리지 포트에서 감지된 장치의 MAC 주소를 표시합니다.

Interface MAC 주소가 위치한 브리지 포트의 네트워크 인터페이스를 표시합니다. 장치의 특정 포트로만 패킷을 전달하여 트래픽 효율을 최적화 합니다.

Aging Timer 각각의 주소를 위한 테이블 유지 시간을 초단위로 표시합니다. 표시된 시간이 지난 후에 해당 주소를 가진 장치로부터의 패킷이 확인되지 않으면 브리지 테이블에서 해당 주소가 삭제됩니다.

Refresh 버튼을 클릭하면 표시되는 정보가 갱신됩니다.

Routes

시스템 라우팅 테이블에 등록된 모든 항목을 표시합니다.

Monitor

[Throughput](#) | [Stations](#) | [Interfaces](#) | [ARP Table](#) | [Bridge Table](#) | [Routes](#) | [GPS Details](#) | [Log](#)

IPv4 Routes			
Destination	Gateway	Netmask	Interface
192.168.1.0	0.0.0.0	255.255.255.0	BRIDGE0
169.254.0.0	0.0.0.0	255.255.0.0	BRIDGE0
0.0.0.0	192.168.1.1	0.0.0.0	BRIDGE0

IPv6 Routes		
Destination	Gateway	Interface
fe80::/64	::	LAN0
fe80::/64	::	wifi0
fe80::/64	::	BRIDGE0
fe80::/64	::	WLAN0
ff00::/8	::	LAN0
ff00::/8	::	wifi0
ff00::/8	::	BRIDGE0
ff00::/8	::	WLAN0

Refresh

RM5 제품은 데이터 패킷에서 데이터를 수신할 장치의 IP 주소를 확인한 후 라우팅 설정에 따라 패킷을 적절한 인터페이스로 전달합니다. 라우팅 테이블은 자동으로 설정되며 사용자가 직접 테이블을 구성할 수도 있습니다.

IPv4 라우팅 테이블

Destination 데이터를 수신하는 네트워크 또는 호스트 장치의 IP 주소를 표시합니다.

Gateway 게이트웨이 IP 주소를 표시합니다.

Netmask 데이터 수신 네트워크를 위한 넷마스크를 표시합니다. 255.255.255.255 값은 호스트를 위해 사용되며 0.0.0.0 값은 기본 라우팅을 위해 사용됩니다. 기본 라우팅은 테이블에서 라우팅 정보가 없을 경우에 사용됩니다.

Interface 데이터 전송에 사용되는 인터페이스를 표시합니다.

Refresh 버튼을 클릭하면 표시되는 정보가 갱신됩니다.

IPv6 라우팅 테이블

IPv6 주소를 위해 RM5 제품은 ::(더블 콜론) 기호를 사용합니다. 더블 콜론 기호는 인접한 16-비트 블록을 대체합니다. 예를 들어 2001:db8::1 값은 2001:db8:0000:0000:0000:0000:0000:0001 주소가 됩니다.

Destination 데이터를 수신하는 네트워크 또는 호스트의 IP 주소를 표시합니다.

Gateway 게이트웨이 IP 주소를 표시합니다.

Interface 데이터 전송에 사용되는 인터페이스를 표시합니다.

Refresh 버튼을 클릭하면 표시되는 정보가 갱신됩니다.

Firewall

상단 NETWORK 탭에서 방화벽 기능을 설정하면 표시됩니다.

Monitor

[Throughput](#) | [Stations](#) | [Interfaces](#) | [DHCP Client](#) | [ARP Table](#) | [Routes](#) | [Firewall](#) | [Port Forward](#) | [DHCP Leases](#) | [Log](#)

Firewall Rules

Chain FIREWALL (2 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	DROP	all	--	*	*	192.168.25.2	20.222.222.222	

Refresh

Firewall Rules Bridge 모드로 장치를 사용할 경우 표준 ebttables 필터 테이블에 포함된 방화벽 체인 항목을 표시하고 Router 모드로 장치를 사용할 경우에는 표준 iptables 필터 테이블에 포함된 방화벽 항목을 표시합니다. RM5 제품에 적용된 IP/MAC 레벨 접속 제어 및 패킷 필터링 기술은 ebttables 과 iptables 방화벽을 사용하여 외부 네트워크로부터 비허가 시스템의 내부 접속을 차단하고 네트워크 통신을 필터링합니다.

Refresh 버튼을 클릭하면 표시되는 정보가 갱신됩니다.

Port Forward

Router 및 SOHO Router 모드에서만 표시되는 항목으로서 포트 포워딩 규칙은 FTP 서버나 웹 서버와 같은 특정 서비스 연결에 사용됩니다. 방화벽/NAT 기능을 통해 외부 WAN 네트워크와 내부 LAN 네트워크 사이에 터널을 생성한 후 내부 시스템에서 동작하는 서비스에 접속할 수 있습니다.

Monitor

[Throughput](#) | [Stations](#) | [Interfaces](#) | [DHCP Client](#) | [ARP Table](#) | [Routes](#) | [Port Forward](#) | [DHCP Leases](#) | [Log](#)

Port Forward Rules

Chain PORTFORWARD (1 references)									
pkts	bytes	target	prot	opt	in	out	source	destination	
0	0	DNAT	tcp	--	eth0	*	192.168.25.3	20.222.222.222	tcp dpt:80 to:1

Refresh

Port Forward Rules Router 모드로 동작하는 장치에서 표준 iptables nat table 의 PREROUTING 체인 항목을 표시합니다.

Refresh 버튼을 클릭하면 표시되는 정보가 갱신됩니다.

DHCP Leases

Router 및 SOHO Router 모드로 동작하는 장치에서 DHCP 서버 기능을 사용할 경우 표시됩니다. 장치에서 동작하는 내부 DHCP 서버가 로컬 클라이언트 장치에 할당한 IP 주소와 상태 정보를 제공합니다.

Monitor

[Throughput](#) | [Stations](#) | [Interfaces](#) | [DHCP Client](#) | [ARP Table](#) | [Routes](#) | [Port Forward](#) | [DHCP Leases](#) | [Log](#)

MAC Address	IP Address	Remaining Lease	Hostname
90:27:E4:F6:34:43	192.168.25.157	00:09:50	
28:CF:DA:E5:61:66	192.168.25.160	00:06:25	
00:27:22:60:00:02	192.168.25.158	00:05:55	
00:27:22:60:06:9E	192.168.25.217	00:05:58	
AC:81:12:74:7C:5C	192.168.25.161	00:06:18	UBNT-Main
00:27:22:60:00:12	192.168.25.145	00:06:33	UBNT
00:27:22:12:B3:92	192.168.25.185	00:07:01	Office

Refresh

MAC Address 클라이언트 장치의 MAC 주소를 표시합니다.

IP Address 클라이언트 장치의 IP 주소를 표시합니다.

Remaining Lease 클라이언트 장치에 할당된 IP 주소의 남은 유효 시간을 표시합니다.

Hostname 클라이언트 장치의 이름을 표시합니다.

Refresh 버튼을 클릭하면 표시되는 정보가 갱신됩니다.

Log

로그 기능을 설정하면 표시되는 항목으로서 등록된 시스템 이벤트 정보들을 표시합니다.

Monitor

[Throughput](#) | [Stations](#) | [Interfaces](#) | [ARP Table](#) | [Bridge Table](#) | [Routes](#) | [GPS Details](#) | [Log](#)

System Log

```
Dec 2 18:45:17 Rocket M5 GPS syslog.info syslogd started: BusyBox v1.11.2
Dec 2 18:45:18 Rocket M5 GPS user.notice system: Start
Dec 2 18:45:18 Rocket M5 GPS daemon.info init: starting pid 1441, tty '/dev/null': '/bin/lighttpd -D -
Dec 2 18:45:18 Rocket M5 GPS daemon.info init: starting pid 1439, tty '/dev/null': '/bin/syslogd -n -S
Dec 2 18:45:18 Rocket M5 GPS daemon.info init: starting pid 1438, tty '/dev/null': '/bin/infctld -m -c
Dec 2 18:45:18 Rocket M5 GPS daemon.info init: starting pid 1440, tty '/dev/null': '/usr/bin/iwevent -
Dec 2 18:45:18 Rocket M5 GPS daemon.info init: starting pid 1442, tty '/dev/null': '/bin/dropbear -F -
Dec 2 18:45:18 Rocket M5 GPS daemon.info init: starting pid 1443, tty '/dev/null': '/usr/bin/ubnt-gps-
Dec 2 18:45:18 syslogd started: BusyBox v1.11.2
Dec 2 18:45:18 dropbear[1442]: Not backgrounding
Dec 2 18:45:28 Rocket M5 GPS daemon.info wireless: ath0 Scan request completed
```

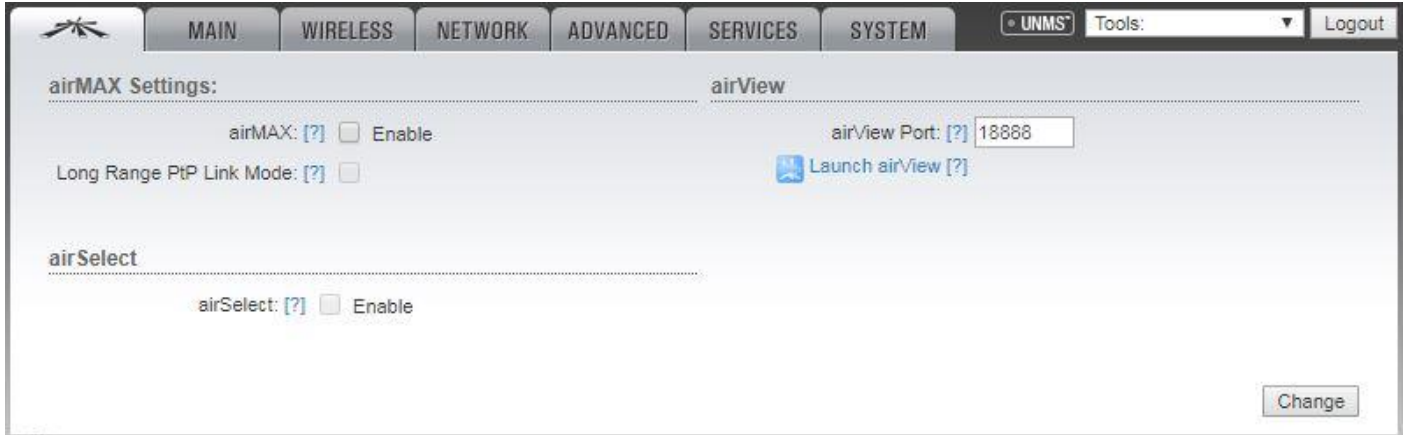
Clear Refresh

Clear 버튼을 클릭하면 시스템 로그에 등록된 모든 이벤트 기록을 삭제합니다.

Refresh 버튼을 클릭하면 최근 로그 정보를 업데이트 합니다.

Chapter 3: 좌측 로고

상단 좌측 로고 페이지에서는 다음과 같은 제조사 고유 기능을 설정합니다.



- **airMAX®** 부하가 많은 무선 환경에서도 저지연 기술을 사용하여 우수한 무선 성능을 제공하고 Access Point 에 보다 많은 클라이언트 장치를 연결할 수 있습니다.
- **airSelect®** 무선 간섭 영향을 최소화 할 수 있도록 무선 채널을 자동으로 변경합니다.
- **airView®** 정확한 무선 환경 분석을 위한 스펙트럼 분석 소프트웨어를 제공합니다.

Change 버튼을 클릭하여 변경된 사항을 저장하거나 테스트합니다.

- **Apply** 변경된 사항을 곧바로 저장합니다.
- **Test** 변경된 사항을 저장하지 않고 사전 테스트를 진행합니다. 테스트 후 변경된 사항을 저장하려면 Apply 버튼을 클릭합니다. 180 초 이내에 Apply 버튼을 클릭하지 않으면 설정 변경이 취소됩니다.
- **Discard** 설정 변경을 취소합니다.

airMAX Settings

airMAX 기능은 TDMA (Time Division Multiple Access) 폴링 특허 기술입니다. airMAX 기능은 전송 지연 시간을 줄여 데이터 속도를 높이고 노이즈가 많은 환경에서 간섭을 제거하여 Point-to-Point 와 Point-to-Multipoint 구조의 무선 네트워크 성능을 향상시킵니다. 또한 airMAX 특징을 기반으로 보다 많은 무선 클라이언트 장치를 Access Point 장치에 연결할 수 있습니다.

airMAX 기능은 히든 노드 문제를 해결하기 위하여 각각의 장치마다 통신을 위한 타임 슬롯을 할당합니다. Access Point 장치는 무선 노드들을 탐지할 수 있지만 Access Point 장치에 연결된 무선 노드 사이에 서로를 탐지할 수 없을 경우 히든 노드 문제가 발생하게 됩니다.

또한 airMAX 기능은 고급 QoS (Quality of Service) 자동감지 설정을 제공합니다. QoS 규칙을 적용할 때 트래픽 타입을 식별하고 분류할 수 있도록 TOS (Type of Service) 범위와 IP Header DSCP (Differentiated Services Code Point) 필드 세트에 특수 값이 포함되어야 합니다. 트래픽을 최초로 발생시키는 소프트웨어 및 하드웨어 장치가 특수 값을 설정해야 하며 airMAX 기능은 이러한 특수 값이 설정된 트래픽을 우선적으로 처리합니다.

QoS 규칙이 적용되는 트래픽은 다음과 같이 4개의 WME (Wireless Multimedia Enhancement) 카테고리 분류되며 Best Effort 에서 Voice 항목으로 갈수록 우선권이 높아집니다.

- Best Effort > Background > Video > Voice

기본적으로 모든 트래픽은 Best Effort 카테고리로 분류되기 때문에 우선권이 적용되지 않습니다. 카테고리들은 아래의 테이블 정보를 기반으로 분류될 수 있습니다.

802.11p Class of Service	TOS Range	DSCP Range	WME Category
0 - Best Effort	0x00 – 0x1f	0 – 7	Best Effort
1 - Background	0x20 – 0x3f	8 – 15	Background
2 - Spare	0x40 – 0x5f	16 – 23	Background
3 - Excellent Effort	0x60 – 0x7f	24 – 25, 28 – 31	Best Effort
4 - Controlled Load	0x80 – 0x9f	32 – 39	Video
5 - Video (<100ms latency)	0xa0 – 0xbf	04 – 45	Video
6 - Voice (<10ms latency)	0x68, 0xb8, 0xc0 – 0xdf	26 – 27, 46 – 47, 48 – 55	Voice
7 - Network Control	0xe0 – 0xff	56 – 63	Voice

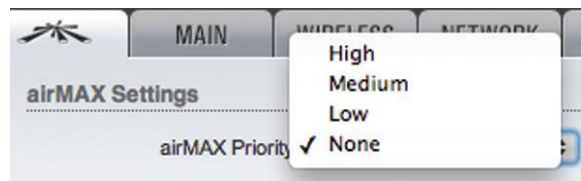
airMAX Access Point 및 AP-Repeater 모드에서만 표시되는 항목으로서 airMAX 기능의 사용 여부를 선택합니다. airMAX 모드로 동작하는 장치는 airMAX 모드로 동작하는 장치와만 연결될 수 있습니다. Station 모드로 동작하는 장치는 airMAX AP 장치에 연결할 때 airMAX 기능을 자동으로 설정합니다. **airMAX 기능을 사용할 경우 휴대용 컴퓨터, 테블릿, 스마트폰과 같은 표준 Wi-Fi 장치와 통신할 수 없습니다.**

Long Range PtP Link Mode Access Point 및 AP-Repeater 모드에서만 표시됩니다. ACK 타임아웃 설정은 사용하는 장치 모델에 따라 제한됩니다. Point-to-Point 방식의 무선 네트워크를 구성할 경우에만 설정하시기 바랍니다. 아래의 두가지 조건을 만족할 경우 Long Range PtP Link Mode 를 사용할 수 있습니다.

- 1개의 Station 또는 클라이언트 장치만 Point-to-Point 방식으로 Access Point 장치에 연결할 경우
- 무선 통신 거리가 하드웨어 ACK 타임아웃을 초과할 경우
 - 27 킬로미터 (40 MHz 모드)
 - 51 킬로미터 (20 MHz 모드)

Long Range PtP Link Mode 를 설정하면 상단 ADVANCED 탭에 있는 Auto Adjust 기능을 사용할 수 없습니다. 여러 개의 Station 장치나 클라이언트를 Access Point 장치에 연결할 경우 Long Range PtP Link Mode 대신 상단 ADVANCED 탭에 있는 Auto Adjust 기능을 사용하시기 바랍니다.

airMAX Priority Station 모드에서만 표시되는 항목으로서 각각의 클라이언트에 할당되는 타임 슬롯 개수(무선 전송 시간)를 설정합니다. 기본적으로 Access Point 장치는 모든 클라이언트 장치에게 동일한 전송 시간을 부여합니다. 하지만 장치에 설정된 우선권에 따라 특정 클라이언트 장치에게 더 많은 전송 시간을 부여하거나 더 적은 전송 시간을 부여할 수 있습니다. 전송 우선권은 여러 개의 Station 또는 클라이언트 장치에 airMAX Priority 기능이 설정되었을 경우에만 동작합니다.



- **High** 4회 슬롯 (4:1 비율)
- **Medium** 3회 슬롯 (3:1 비율)
- **Low** 2회 슬롯 (2:1 비율)
- **None** 1회 슬롯 (1:1 비율, 클라이언트 기본값)

높은 우선권을 가진 클라이언트 장치는 AP 장치의 무선 전송 시간을 더 많이 부여받기 때문에 다른 클라이언트 장치보다 빠른 속도와 저지연 통신을 사용할 수 있습니다. 예를 들어 3개의 클라이언트 장치가 각각 None, Medium, High 로 우선권이 설정되어 있다고 가정합니다. 이때 None 클라이언트 장치는 1회, Medium 클라이언트 장치는 3회, High 클라이언트 장치는 4회의 전송 타임 슬롯을 부여받게 됩니다.

airSelect

The screenshot shows the 'airSelect' configuration panel. At the top, there is a title 'airSelect' and a status 'airSelect: [?] Enable'. Below this, there are three main configuration items:

- 'Frequency List: [?]' followed by an empty text input field and an 'Edit...' button.
- 'Hop Interval: [?]' followed by a text input field containing '3000' and the unit 'milliseconds'.
- 'Announce Count: [?]' followed by a text input field containing '30'.

airSelect 기능을 사용할 경우 airSync 기능을 함께 사용할 수 없으며 Access Point 모드에서만 지원됩니다. airSelect 기능은 무선 간섭을 회피하여 전송 속도를 향상시키는 기술입니다. airSelect 기능은 현재 사용 중인 무선 채널을 Frequency List 에 포함된 채널 중에서 자주 사용되지 않는 무선 채널로 지정된 시간 내에 주기적으로 변경합니다. Frequency List 및 호핑 간격은 사용자가 설정할 수 있으며 호핑 간격은 ms 단위로 설정합니다. airSelect 기능은 사용되는 각 채널의 간섭 레벨을 추적하여 간섭이 적은 채널로 변경합니다.

airSelect 기능 사용 여부를 설정합니다. airSelect 기능을 사용하면 Access Point 장치 및 연결된 클라이언트 장치들이 채널 간섭을 회피하기 위하여 채널을 빠르게 변경하면서 통신합니다.

Frequency List airSelect 기능을 설정할 경우 사용 가능합니다. **Edit** 버튼을 클릭한 후 Access Point 에서 사용할 채널을 선택합니다. 선택 가능한 채널은 장치 모델에 따라 달라질 수 있습니다.

Hop Interval airSelect 기능을 사용할 경우 설정합니다. Access Point 장치는 설정한 시간 동안 특정 채널을 사용한 후 다음 채널로 변경합니다. 설정 시간은 ms 단위로 입력합니다. (기본값 3000 ms = 3초)

Announce Count airSelect 기능을 사용할 경우 설정합니다. Access Point 장치는 설정한 회수 만큼 클라이언트 장치들에게 다음 채널 정보를 브로드캐스팅합니다. 예를 들어 Hop Interval 시간을 3000 ms 로 설정하고 Announce Count 값을 30회로 설정할 경우 Access Point 장치는 100 ms (3000ms / 30회) 마다 클라이언트 장치들에게 다음 홉 정보를 전송합니다. Announce Count 사이의 시간 간격과 Hop Interval 시간이 커질수록 홉 동기화 오류 발생 가능성도 높아집니다. 기본값을 사용하시거나 Access Point 장치가 100 ms 마다 채널 정보를 전송할 수 있도록 Announce Count 값을 Hop Interval 시간의 1/100 값으로 설정하실 것을 권장합니다. 예를 들어 Hop Interval 값을 10000 ms 로 설정할 경우 Announce Count 값은 100 회로 설정하시면 됩니다.

airView

무선 노이즈 환경을 분석하고 Point-to-Point airMAX 링크를 구성할 때 최적의 주파수를 선택할 수 있도록 airView 스펙트럼 분석 툴을 사용할 수 있습니다.

airView Port airView 세션에 사용되는 TCP 포트를 설정합니다.

Launch airView airView 스펙트럼 분석 툴을 사용하려면 다음과 같은 2가지 시스템 요구 사항을 필요로 합니다.

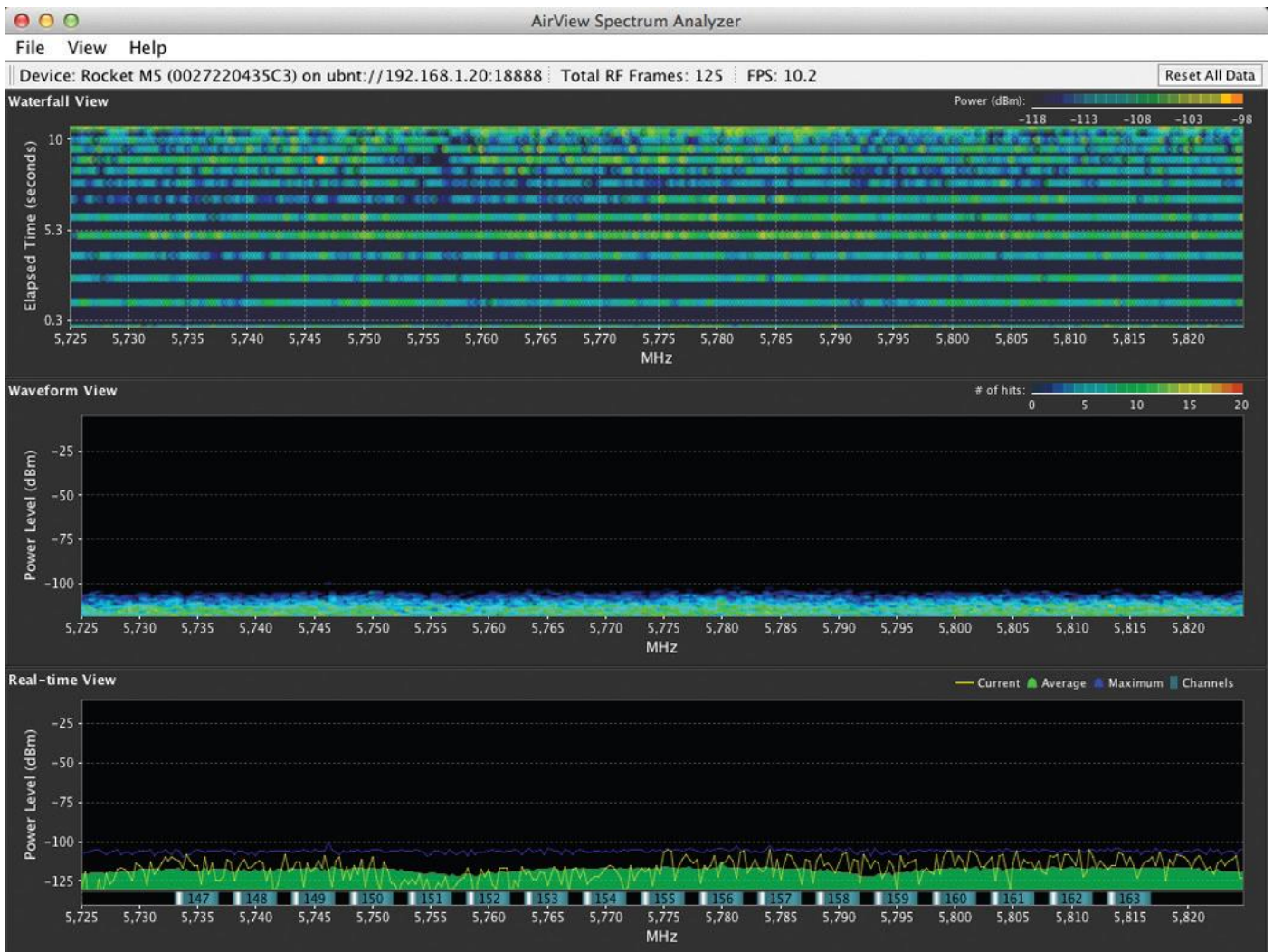
- 장치와 사용자 시스템 (PC)을 인터넷으로 연결해야 합니다. airView 기능을 실행하면 Access Point 와 무선 클라이언트 장치들 사이의 모든 무선 연결이 끊어집니다.
- 사용자 시스템에 Java Runtime Environment 1.6 이상의 버전이 설치되어 있어야 합니다.

Launch airView 링크를 클릭하면 airView 스펙트럼 분석 툴이 실행됩니다. airView 스펙트럼 분석 툴을 처음 실행할 경우 다음과 같은 창이 표시됩니다.



- **Do NOT warn me about this in the future** airView 스펙트럼 툴을 실행할 때 이 창을 표시하지 않으려면 박스를 체크합니다.
- **Launch airView** 클릭하면 jnlp (Java Network Launch Protocol) 파일을 사용자 시스템에 다운로드한 후 프로그램이 자동으로 실행됩니다.





Main 보기

Device: Rocket M5 (0027220435C3) on ubnt://192.168.1.20:18888 | Total RF Frames: 125 | FPS: 10.2 Reset All Data

Device 장치 모델명과 MAC (Media Access Control) 주소, IP 주소를 표시합니다.

Total RF Frames airView 세션이 시작되거나 Reset All Data 버튼을 클릭한 이후 수집된 총 RF 프레임 개수를 표시합니다.

FPS airView 세션이 시작되거나 Reset All Data 버튼을 클릭한 이후 초당 수집된 RF 프레임 개수를 표시합니다.

Reset All Data 수집된 데이터를 삭제합니다. 주로 위치를 변경하여 스펙트럼 분석을 다시 시작할 경우 사용됩니다.

File 메뉴

airView 세션을 종료하려면 **Exit** 를 클릭합니다.

View 메뉴

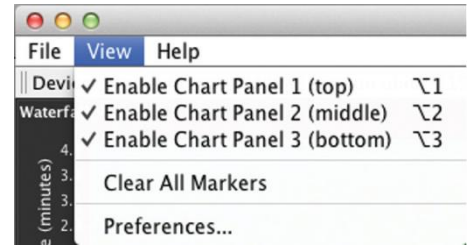
Enable Chart Panel 1 (top) Preferences 설정에 따라 Waterfall 또는 Channel Usage 차트를 Chart Panel 1 위치에 표시합니다. airView 세션이 시작된 시점부터 주파수 별 측정 에너지나 채널 사용 데이터를 시간축을 기준으로 누적하여 보여줍니다.

Enable Chart Panel 2 (middle) Waveform 차트를 Chart Panel 2 위치에 표시합니다. airView 세션이 시작된 시점부터 노이즈 환경의 RF 신호를 시간축을 기준으로 누적하여 보여줍니다. 파란색 계열의 차가운 색상은 낮은 에너지 레벨을 표시하고 노랑, 주황, 빨간색과 같은 따뜻한 계열의 색상은 높은 에너지 레벨을 의미합니다.

Enable Chart Panel 3 (bottom) 일반적인 스펙트럼 분석기와 유사한 형태의 실시간 차트를 Chart Panel 3 위치에 표시합니다. 주파수 별로 실시간으로 측정되는 신호 세기와 평균값, 최대값을 dBm 단위로 표시합니다.

Clear All Markers 표시된 모든 마커들을 제거합니다. 실시간 차트에서 특정 포인트를 클릭하면 주파수에 대응하는 마커가 생성됩니다.

Preferences 클릭하면 아래와 같은 airView Spectrum Analyzer 창이 표시되고 차트 활성화/비활성화, 트레이스, 주파수 간격과 같은 설정을 변경할 수 있습니다.



Charts

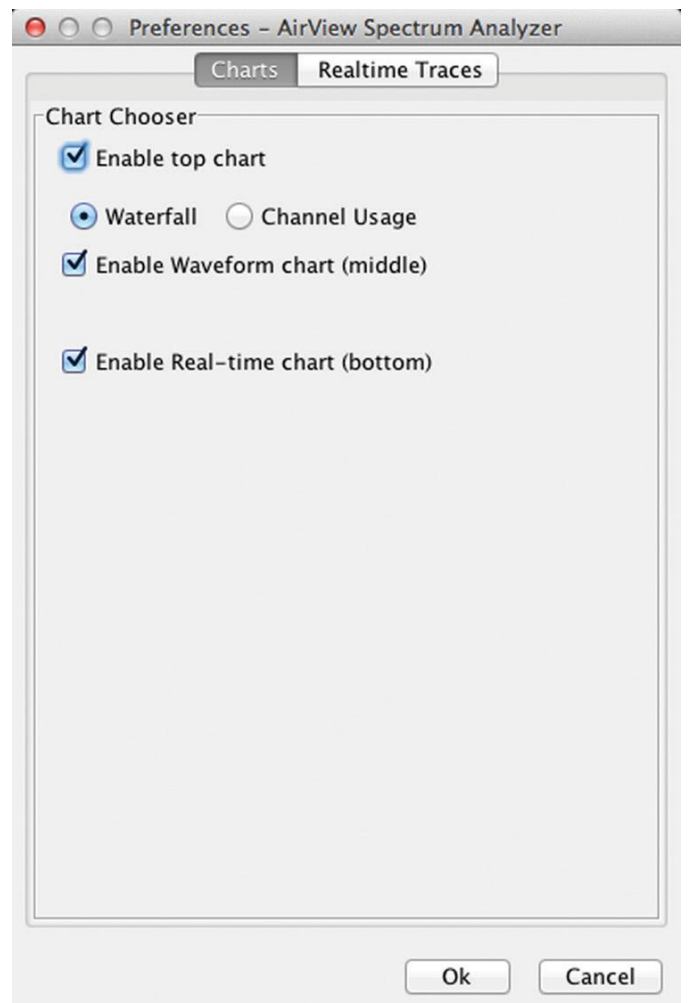
Enable top chart 박스를 체크하면 상단 차트를 사용합니다. 상단 차트 패널에 표시할 차트를 선택합니다.

- **Waterfall** airView 세션이 시작되는 시점부터 각 주파수별로 측정된 에너지를 시간축을 기준으로 표시하고 색상을 통해 에너지 세기를 나타냅니다. 우측 상단에는 dBm 단위의 파워 레벨이 표시됩니다. 좌측 끝에는 계산된 최저 노이즈 레벨이 표시되고 우측 끝에는 airView 세션이 시작되는 시점부터 측정된 신호 중 가장 높은 레벨을 표시합니다.
- **Channel Usage** 각각의 Wi-Fi 무선 채널에 대하여 막대 그래프를 통해 특정 채널의 혼잡도를 % 단위로 표시합니다. airView 스펙트럼 분석 툴은 airView 세션이 시작되는 시점부터 특정 채널들의 RF 에너지 강도와 빈도를 분석하여 백분율 값을 계산합니다.

Enable Waveform chart (middle) 박스를 체크하면 중간 차트를 사용합니다. airView 세션이 시작된 시점부터 노이즈 환경의 RF 신호를 시간축을 기준으로 누적하여 보여줍니다.

Enable Real-time chart (bottom) 박스를 체크하면 하단 차트를 사용합니다. 주파수 별로 실시간으로 측정되는 신호 세기와 평균값, 최대값을 dBm 단위로 표시합니다.

- **Current (노란색)** 실시간 에너지 값을 표시합니다.
- **Average (초록색)** 평균 에너지 값을 표시합니다.
- **Maximum (파란색)** 최대 에너지 값을 표시합니다.



Realtime Traces

아래의 설정은 실시간 차트에만 적용됩니다.

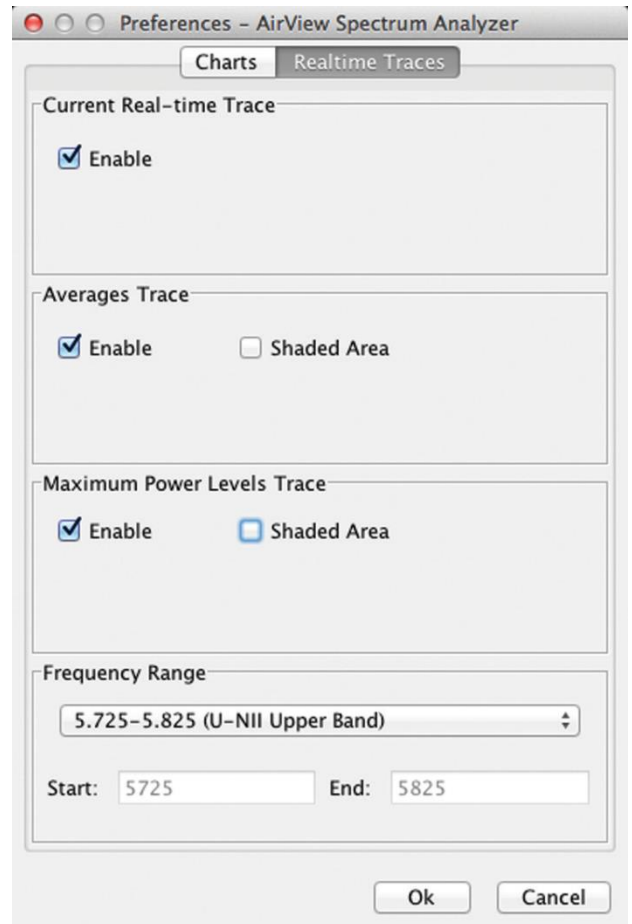
Current Real-time Trace Enable 박스를 체크하면 실시간 트레이스 기능을 사용합니다. 실시간 차트에서 노란색은 해당 주파수의 신호 세기를 표시합니다. 데이터 갱신 속도는 FPS 설정에 따라 달라집니다.

Averages Trace Enable 박스를 체크하면 평균 트레이스 기능을 사용합니다. 실시간 차트에서 녹색 영역으로 표시되며 airView 세션이 시작된 시점부터 수신된 신호의 평균 레벨을 나타냅니다. Shaded Area 박스를 체크하지 않으면 평균 레벨이 영역이 아닌 선으로만 표시됩니다.

Maximum Power Levels Trace Enable 박스를 체크하면 최대 신호 트레이스 기능을 사용합니다. 실시간 차트에서 파란색 영역으로 표시되며 airView 세션이 시작된 시점부터 수신된 신호의 최대 레벨을 나타냅니다. Shaded Area 박스를 체크하면 최대 신호 레벨이 선이 아닌 영역으로 표시됩니다.

Frequency Range 스캔한 주파수 범위를 선택합니다. 선택할 수 있는 주파수 범위는 사용하는 장치 모델에 따라 달라질 수 있습니다. 주로 사용되는 주파수 범위를 리스트에서 선택하거나 **Custom Range** 를 선택한 후 **Start** 와 **End** 필드에 스캔할 주파수 범위를 직접 입력할 수도 있습니다.

OK 버튼을 클릭하면 변경된 설정이 저장되고 **Cancel** 버튼을 클릭하면 설정 변경이 취소됩니다.



Help 메뉴

클릭하면 airView 스펙트럼 분석 툴 버전 정보를 표시합니다.

Chapter 4: WIRELESS

무선 모드, SSID, 주파수 및 채널, 송신 출력, 데이터 속도, 보안 등 무선 연결과 관련된 모든 항목을 설정합니다.

Change 설정을 변경한 후 우측 하단의 **Change** 버튼을 클릭하여 변경된 사항을 적용합니다. Change 버튼을 클릭하면 우측 상단에 아래와 같은 3가지 옵션이 표시되며 다음과 같은 작업을 수행할 수 있습니다.

- **Apply** 버튼을 클릭하면 변경된 설정이 곧바로 적용됩니다.
- **Test** 버튼을 클릭하면 변경된 사항을 저장하지 않고 테스트만 시도합니다. 180 초 이내에 Apply 버튼을 클릭하지 않으면 변경된 설정이 저장되지 않고 이전 설정으로 복구됩니다. Test 버튼을 클릭하면 180초 동안 화면에 카운트다운이 표시됩니다.
- **Discard** 변경된 설정을 저장하지 않고 취소합니다.

Basic Wireless Settings

무선 모드 및 SSID, 국가 코드, 802.11 모드, 송신 출력, 속도와 같은 기본적인 무선 파라미터를 설정합니다.

Basic Wireless Settings

Wireless Mode:

WDS (Transparent Bridge Mode): Enable

SSID: Hide SSID

Country Code:

IEEE 802.11 Mode:

Channel Width:[?]

Frequency, MHz:

Extension Channel:

Frequency List, MHz: Enable

Auto Adjust to EIRP Limit: Enable

Antenna Gain: dBi Cable Loss: dB

Output Power: dBm

Data Rate Module:

Max TX Rate, Mbps: Automatic

Wireless Mode 장치의 무선 모드를 설정합니다. 제품 모델에 따라 설정할 수 있는 모드와 네트워크 구조가 제한됩니다. RM5 제품은 다음과 같은 무선 모드를 지원합니다.

- **Station** AP 장치에 무선으로 연결되는 클라이언트 장치를 Station 모드로 설정합니다. Station 장치의 유선랜 포트에 연결된 네트워크 장치들은 AP 장치에 연결된 유무선 네트워크 장치들과 통신할 수 있습니다. Station 장치의 무선 인터페이스를 통해 수신된 모든 트래픽은 유선랜 인터페이스에 연결된 장치들로 전달되고 유선랜 인터페이스를 통해 수신된 모든 트래픽도 무선랜 인터페이스를 통해 AP 장치로 전달됩니다. WDS (트랜스패런트 브리지 모드) 기능을 사용하지 않으면 ARP/NAT 기술을 사용하기 때문에 트랜스패런트 브리지 역할을 제공할 수 없습니다. 트랜스패런트 브리지 기능을 사용하려면 Station 모드와 WDS 기능을 함께 사용하시기 바랍니다.
- **Access Point** 1개의 장치로 AP를 구성할 경우 Access Point 모드로 설정합니다. AP 장치에는 Station 및 노트북과 같은 여러 개의 클라이언트 장치들을 연결할 수 있습니다. 1개의 AP 장치에만 유선랜을 연결할 수 있고 여러 개의 AP 장치들을 사용하여 무선 신호를 확장하려면 AP-Repeater 모드를 사용합니다. WDS Access Point 모드를 사용하려면 Access Point 모드를 선택한 후 WDS 기능을 설정합니다.
- **AP-Repeater** 여러 개의 AP 장치들을 AP-Repeater 모드로 설정하여 WDS 무선 인프라스트럭처 네트워크를 구성합니다. Auto 옵션을 설정하면 모든 AP 장치들이 동일한 AP-Repeater 모드와 SSID를 자동으로 사용하여 WDS 연결을 구성합니다. 클라이언트 장치들은 AP 장치 뿐만 아니라 AP-Repeater 모드로 동작하는 장치들에도 연결할 수 있습니다. 단, AP-Repeater 모드를 사용할 경우 WPA/WPA2 보안 방식을 사용할 수 없으며 보안을 사용하지 않거나 WEP 보안 방식을 사용해야 합니다. 보안 방식을 사용하지 않아도 RADIUS MAC 인증과 MAC ACL 기능을 사용하여 네트워크 보안을 유지할 수 있습니다.

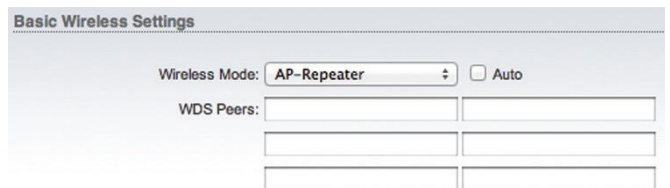
WPA 또는 WPA2 보안은 AP 구성에서 Authenticator 또는 Supplicant 와 같은 서로 다른 역할을 요구합니다.

WDS (Transparent Bridge Mode) Access Point 및 Station 모드에서만 사용할 수 있습니다. WDS 기능은 트랜스패런트 레이어 2 트래픽을 지원하기 때문에 대부분 WDS 사용을 권장합니다. WDS 기능을 사용하려면 박스를 체크합니다. WDS 프로토콜은 비표준 방식으로서 제조사에 따라 상호 호환되지 않을 수 있습니다.

- **Station (WDS)** Access Point (WDS) 모드로 동작하는 AP 장치에 연결하는 클라이언트 장치를 Station (WDS) 모드로 설정합니다.
- **Access Point (WDS)** Access Point (WDS) 모드는 Station (WDS) 모드와 레이어 2 브리지 연결을 지원합니다.

Station (WDS) 모드로 동작하는 장치를 Access Point (WDS) 모드로 동작하는 장치에 연결할 경우 WPA/WPA2 암호화 방식을 포함하여 모든 보안 방식을 사용할 수 있습니다.

Auto AP-Repeater 모드에서만 설정할 수 있습니다. 박스를 체크하면 AP-Repeater 모드로 동작하는 AP 장치 사이에 WDS 연결을 자동으로 구성합니다. Auto 로 설정된 AP-Repeater 장치는 SSID 설정 값을 기반으로 AP-Repeater 모드로 동작하는 WDS Peers 장치를 선택합니다. AP-Repeater 모드로 동작하는 모든 AP 장치(WDS Peers)들은 채널 번호와 채널 대역폭, 보안 방식을 모두 동일하게 설정해야 합니다.



WDS Peers AP-Repeater 모드에서만 설정할 수 있습니다. Auto 옵션을 사용하지 않을 경우 AP-Repeater 모드로 동작하는 AP 장치들을 직접 설정합니다. WDS Peers 필드에 AP-Repeater 장치들의 MAC 주소를 입력합니다. Point-to-Point 방식으로 1개의 장치만 연결할 경우에는 1개의 MAC 주소만 입력합니다. Point-to-Multipoint 방식으로 여러 개의 AP-Repeater 장치들을 연결할 경우 최대 6개의 MAC 주소를 입력할 수 있습니다.

SSID 무선 장치를 Access Point 또는 AP-Repeater 모드로 사용할 경우 무선랜 서비스에 사용되는 무선 네트워크 이름(SSID: Service Set Identifier)을 설정합니다. AP 장치의 무선 신호를 수신할 수 있는 모든 클라이언트 장치들은 AP 장치가 브로드캐스팅 하는 메시지를 통해 SSID를 확인할 수 있습니다. 무선 장치를 Station 모드로 사용할 경우에는 연결할 AP 장치의 SSID를 설정합니다. 트래픽 분산 및 음영 지역 해소를 위해 동일한 서비스 범위 내에서 동일한 SSID를 사용하는 여러 개의 AP 장치를 사용할 수도 있습니다.

Select Station 모드에서만 지원되는 항목으로서 연결 가능한 AP 장치 리스트를 표시하며 **Select** 버튼을 클릭하여 연결할 AP 장치를 선택합니다. Site Survey 툴을 사용하면 장치가 지원하는 모든 채널의 무선 네트워크를 검색한 후 사용자가 선택하여 연결할 수 있도록 합니다. Site Survey 툴은 없어지거나 새로 추가된 무선 네트워크만 스캔하는 기능을 제공하기 때문에 보다 효율적인 검색 결과를 제공합니다. 선택한 무선 네트워크가 암호화 보안을 사용할 경우 **WIRELESS** 페이지에서 보안 항목을 추가로 설정해야 합니다.

- **Lock to AP** 리스트에서 AP 장치를 선택한 후 **Lock to AP** 버튼을 클릭하면 스테이션 장치는 다른 AP 장치로는 연결하지 않고 선택한 MAC 주소를 가진 AP 장치로만 항상 연결합니다.
- **Select** 리스트에서 연결할 AP를 선택합니다.
- **Scan** Scan 버튼을 클릭하면 사용 가능한 무선 네트워크 리스트가 갱신됩니다. 선택할 SSID는 채널 대역폭과 보안 설정이 호환되어야 합니다.

Frequency List option 을 설정하면 Site Survey 툴에서 스캔할 주파수 리스트를 선택할 수 있습니다.

Lock to AP MAC Station 모드에서만 지원되는 항목으로서 스테이션 장치가 특정 MAC 주소를 가진 AP 장치로만 연결되게 합니다. 이 설정은 동일한 SSID로 설정된 여러 개의 AP 장치를 사용하는 환경에서 유용하게 사용될 수 있습니다.

Hide SSID Access Point 및 AP-Repeater 모드에서만 지원되는 항목으로서 SSID 가 클라이언트 장치로 브로드캐스팅 되는 것을 차단합니다.

Country Code 국가 별로 무선 송신 출력 및 사용 주파수가 제한될 수 있습니다. 장치가 사용되는 해당 국가의 전파 관리 규정을 준수할 수 있도록 올바른 국가를 선택하시기 바랍니다. 국가를 선택하면 해당 국가의 전파 관리 규정에 따라 IEEE 802.11 모드, 채널, 주파수, 송신 출력이 제한됩니다.

IEEE 802.11 Mode 장치에서 사용할 무선 표준을 선택합니다. 802.11n 기술은 802.11a/b/g 기술보다 빠른 속도와 우수한 성능을 제공합니다.

- **A/N mixed** 5 GHz 기반의 802.11a 또는 802.11n 모드를 사용합니다.
- **B/G/N mixed** 2.4 GHz 기반의 802.11b 또는 802.11g, 802.11n 모드를 사용합니다.

DFS 5 GHz 기반의 모델에서만 사용할 수 있으며 설정한 **Country Code** 에 따라 달라질 수 있습니다. 레이더 시스템은 5 GHz 대역의 특정 주파수를 사용하며 DFS(Dynamic Frequency Selection) 기술은 이러한 레이더 신호의 간섭을 회피하기 위하여 사용됩니다. DFS 채널을 사용하는 장치는 해당 국가의 주파수에 따라서 1분에서 10분 정도 사이의 CAC (Channel Availability Check) 시간이 소요된 후 사용이 가능할 수도 있습니다. 특히 5600~5650 MHz 사이의 기상 레이더 대역에서 많은 시간이 소요됩니다. 무선 장치가 레이더 주파수 신호를 감지하면 해당 주파수를 사용하지 않도록 30분 동안 블랙 리스트에 추가합니다. 만약 단 1개의 주파수만 주파수 리스트에 등록된 상태에서 해당 주파수의 레이더 신호를 감지하게 된다면 30~40분 동안 무선 통신이 불가능하게 됩니다. 또한 200mW 이상의 EIRP (Equivalent Isotropic Radiated Power) 신호를 사용하는 무선 장치도 레이더 신호를 감지하면 30분간 통신이 불가능하게 됩니다.

Channel Width 무선 채널 대역폭을 표시합니다. 사용자는 무선 연결에 사용되는 대역폭을 설정할 수 있습니다. 높은 대역폭을 사용하면 데이터 속도를 높일 수 있으며 사용 대역폭이 낮아지면 다음과 같은 특징을 제공합니다.

- 채널 크기에 따라 데이터 속도가 낮아집니다. 예를 들어 40MHz 대역폭을 사용하면 20MHz 대역폭을 사용할 때 보다 속도를 2배 높일 수 있지만 10MHz 대역폭을 사용하면 20MHz 대역폭 속도의 절반으로 줄어듭니다.
- 비중첩 채널 수가 증가하여 네트워크 확장성을 높일 수 있습니다.
- 채널 당 파워 스펙트럼 밀도(PSD: Power Spectral Density)가 증가하여 무선 통신 거리를 확장합니다.

채널 대역폭은 사용하는 제품 모델에 따라 차이가 있으며 다음과 같은 채널 대역폭을 사용할 수 있습니다.

- **3 MHz**
- **5 MHz** Quarter-Rate 모드
- **7 MHz**
- **8 MHz**
- **10 MHz** Half-Rate 모드
- **14 MHz**
- **20 MHz** 기본 설정값
- **25 MHz**
- **28 MHz**
- **30 MHz**
- **40 MHz**
- **Auto 20/40 MHz** Station 모드에서만 설정 가능, 높은 호환성을 제공함

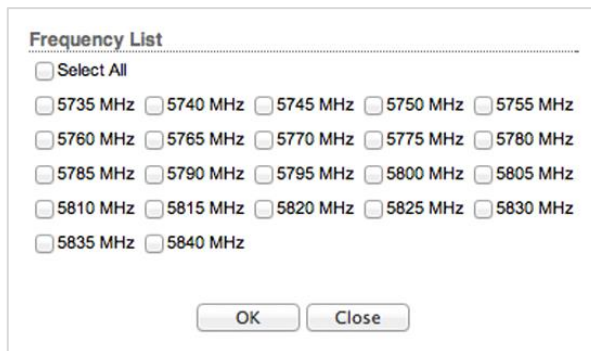
Channel Shifting 해당 기능은 5 GHz 제품 모델에서는 지원하지 않고 2.4 GHz 제품 모델에서만 사용할 수 있습니다. 표준 802.11 채널과 다른 채널 오프셋을 사용하기 때문에 표준 Wi-Fi 무선랜 제품과 호환되지 않습니다. 표준 802.11b/g/n 채널로부터 중심 주파수를 2 MHz 이동하여 사용하기 때문에 다른 Wi-Fi 장치로부터 감지되지 않아 보안을 강화할 수 있고 별도의 사설 무선 네트워크를 구성할 수 있습니다.

Frequency, MHz 리스트에서 사용할 채널을 선택합니다. Auto 옵션을 설정하면 장치가 부팅할 때 사용할 채널을 자동으로 선택합니다. Frequency List 옵션을 사용하면 리스트에 표시되는 채널을 변경할 수 있습니다. 5.25~5.725 GHz 사이의 UNII-2 대역을 기반으로 하는 DFS 채널을 사용해야 하지만 리스트에는 표시되지 않을 수도 있습니다. 사용 가능한 DFS 채널을 표시하려면 상단 **SYSTEM** 탭을 선택한 후 **Miscellaneous** 항목에서 **UNII-2 Band** 를 **Enable** 로 설정하시기 바랍니다.

Extension Channel Access Point 및 AP-Repeater 모드에서 40 MHz 채널 대역폭을 사용할 경우에만 해당 옵션을 설정할 수 있습니다. 40 MHz 채널은 2개의 20 MHz 채널을 함께 사용하여 구성됩니다. Extension Channel 설정은 기존 채널에 추가되는 채널을 상위 채널로 사용할 것인지 하위 채널로 사용할 것인지 선택합니다. 예를 들어 5805 MHz (40 MHz 채널) 기준 채널과 Lower 를 선택할 경우 무선 장치는 5795~5815 MHz 기준 채널과 하위에 있는 5775~5795 MHz 채널을 추가하여 40 MHz 채널을 구성합니다. 5805 MHz (40 MHz 채널) 기준 채널과 Upper 를 선택할 경우에는 5795~5815 MHz 기준 채널에 상위에 위치한 5815~5835 MHz 채널을 추가하여 40 MHz 채널을 구성합니다.

Frequency List, MHz Access Point 및 AP-Repeater 모드에서만 설정할 수 있습니다. AP 장치는 인접한 AP 장치들에서 발생하는 간섭을 줄이기 위하여 여러 개의 운영 채널을 선택할 수 있습니다. 채널 리스트는 Country Code 및 IEEE 802.11 Mode, Channel Width, Channel Shifting 설정에 따라 다릅니다. Auto 옵션은 Frequency List 에 등록된 채널 중에서 운영 채널을 사용하도록 제한합니다. **Enable** 박스를 체크하고 **Edit** 버튼을 클릭하면 Frequency List 창이 표시됩니다.

사용할 채널들을 선택한 후 **OK** 버튼을 클릭합니다. 아무런 채널도 선택하지 않으려면 **Close** 버튼을 클릭합니다.



Frequency Scan List, MHz Station 모드에서만 설정할 수 있습니다. 옵션에서 선택한 채널만 검색하도록 제한하여 스테이션 장치가 검색 프로세스를 빠르게 완료할 수 있고 불필요한 AP 장치들을 필터링합니다. Site Survey 툴은 이 옵션에서 선택된 채널만 검색합니다. **Enable** 박스를 체크하고 **Edit** 버튼을 클릭하면 Frequency List 창이 표시됩니다. 검색할 채널들을 선택한 후 **OK** 버튼을 클릭합니다. 아무런 채널도 선택하지 않으려면 **Close** 버튼을 클릭합니다.

Calculate EIRP Limit Enable 박스를 체크하면 설정된 국가의 전파 규정에 따라 무선 송신 출력이 자동으로 제한됩니다. 무선 채널 별로 최대 송신 출력 및 사용할 수 있는 안테나 이득이 국가마다 다르기 때문에 해당 규정을 확인하기 어려우시면 옵션을 설정하여 사용하시기 바랍니다. Calculate EIRP Limit 기능을 사용하지 않으려면 상단 **ADVANCED** 탭의 **Advanced Wireless Settings** 항목에서 **Installer EIRP Control** 기능을 해제해야 합니다.

Antenna 여러 개의 안테나 이득 옵션을 제공하는 모델에서만 설정할 수 있으며 내장 안테나를 사용하는 모델은 Antenna 필드가 표시되지 않습니다. RM5 제품은 모델에 따라 다음과 같이 안테나 옵션을 선택합니다.

Antenna Gain 안테나 이득을 dBi 단위로 입력합니다. Calculate EIRP Limit 옵션을 사용할 경우 해당 국가의 규정 및 안테나 이득에 따라 무선 송신 출력이 자동으로 제한됩니다. Antenna Gain 설정은 Cable Loss 설정과 연동하여 무선 송신 출력에 영향을 줍니다.

Cable Loss 외부 안테나 커넥터를 제공하는 제품에서만 사용할 수 있는 옵션으로서 케이블 손실을 dB 단위로 입력합니다. 케이블 손실이 많을 경우 무선 송신 출력을 높여야 합니다. Cable Loss 설정은 Antenna Gain 설정과 연동하여 무선 송신 출력에 영향을 줍니다.

Output Power 최대 무선 송신 출력을 dBm 단위로 설정합니다. 슬라이더를 사용하거나 출력 값을 직접 입력할 수 있으며 해당 국가의 전파 규정을 확인하신 후 설정하시기 바랍니다. 안테나 내장형 제품을 사용하실 경우 Output Power 신호가 내부 안테나에 직접 전달됩니다.

Data Rate Module 무선 연결에 사용되는 데이터 속도 알고리즘 (**Default** 또는 **Alternative**)을 선택합니다. Default 설정이 정상적으로 동작하지 않을 경우 Alternative 로 설정을 변경하여 개별 환경에 적합한 데이터 속도 알고리즘을 사용하시기 바랍니다. Alternative 알고리즘은 데이터 속도를 가능한 높게 유지하면서 동시에 패킷 에러 카운트를 지속적으로 모니터링합니다. Alternative 알고리즘은 보다 안정적인 데이터 속도를 제공하지만 환경 및 설정 상태에 따라 Default 및 Alternative 알고리즘을 선택하여 사용하셔야 합니다. 예를 들어 Default 알고리즘을 사용하는 무선 연결에서 트래픽 안정성 문제가 발생할 경우 Alternative 알고리즘으로 변경하여 상황이 개선되지는 확인할 수 있습니다. Data Rate Module 설정은 송신 속도에만 영향을 주고 수신 속도에는 영향을 주지 않습니다. 또한 연결된 AP 장치 및 다른 Station 장치에서 사용하는 알고리즘과 상관없이 현재 설정하는 장치에만 적용됩니다.

Max TX Rate, Mbps 무선 패킷 전송에 사용되는 최대 속도를 Mbps 단위로 설정합니다. 사용자는 MCS 0 부터 MCS 15 사이의 속도를 설정할 수 있습니다. 일반적으로 연결 장애 및 고속 통신에서 데이터 손실이 발생할 경우 Automatic 옵션 사용을 권장합니다. Automatic 옵션을 사용하면 자동으로 속도를 하향 조정하여 이러한 문제점들을 해결할 수도 있습니다. 20 MHz 채널 대역폭을 사용할 경우 MCS 15 - 130/144.4 Mbps 최고 속도를 사용할 수 있고 40 MHz 채널 대역폭을 사용할 경우에는 MCS 15 - 270/300 Mbps 최고 속도를 사용할 수 있습니다.

- **Automatic** 옵션을 사용하면 속도 알고리즘을 기반으로 무선 품질에 따라 최적의 데이터 속도가 자동으로 설정됩니다. 고속 통신에서 데이터 손실이 발생하거나 링크가 정상적으로 연결되지 않을 경우 Automatic 옵션을 사용하면 자동으로 속도를 하향 조정하여 문제를 해결할 수 있습니다. 보다 자세한 정보는 상단 **ADVANCED** 탭의 **Advanced Wireless Settings** 항목을 참고하시기 바랍니다.

속도 알고리즘은 GI (Guard Interval) 값을 자동으로 선택하며 이로 인해 MAX TX Rate 범위도 달라집니다. 800 ns Normal GI 값이 사용될 경우 데이터 속도는 낮아지고, 400 ns Short GI 값이 사용될 경우 데이터 속도가 높아집니다.

Wireless Security

Access Point 또는 AP-Repeater 모드로 동작하는 AP 장치에서 설정하는 무선 보안은 연결되는 스테이션 장치에서도 동일하게 사용됩니다. Station 모드로 동작하는 클라이언트 장치는 연결되는 AP 장치와 동일한 보안 설정을 적용합니다. 각각의 무선 모드 별로 다음과 같은 보안 방식을 제공합니다.

보안 방식	Access Point	AP-Repeater	Station
none	√ ¹	√ ¹	√
WEP		√ ²	
WPA-AES	√		√
WPA2-AES	√		√

1. 별도의 암호화 방식을 사용하지 않을 경우 네트워크 보안에 문제가 발생할 수 있습니다. 하지만 RADIUS MAC 인증 및 MAC ACL 방법을 함께 사용하여 취약한 보안 문제점을 보완할 수 있습니다.
2. WEP 암호화 방식은 보안에 취약하지만 MAC ACL 방법을 함께 사용하여 보안을 강화할 수 있습니다.

Security 다음과 같은 무선 보안 방식을 지원합니다.

- **none** 개방형 무선 네트워크를 구성할 때 설정합니다. 연결 인증 및 데이터 암호화를 사용하지 않기 때문에 외부에 노출되지 않는 폐쇄 환경에서만 사용됩니다. RADIUS MAC 인증 및 MAC ACL 방법을 사용하여 취약한 보안 문제점을 보완할 수 있습니다.
- **WEP** 최소한의 보안 알고리즘으로서 WEP (Wired Equivalent Access) 방식은 자주 사용되지 않습니다.
- **WPA-AES** WPA (Wi-Fi Protected Access) 보안 모드는 AES (Advanced Encryption Standard) 암호화 방식만 지원합니다. CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) 로 알려진 AES 알고리즘을 사용합니다.
- **WPA2-AES** WPA2 보안 모드는 AES 암호화 방식만 지원합니다. WPA2 방식은 WPA 방식을 강화한 버전으로서 안전한 무선 네트워크 구성을 위해 WPA2-AES 보안 사용을 권장합니다.

WPA Authentication 2가지 WPA 키 선택 방법 중에서 1가지를 선택합니다.

- **PSK** Pre-shared Key 방법
- **EAP** EAP (Extensible Authentication Protocol) IEEE 802.1x authentication 방법. 일반적으로 엔터프라이즈 네트워크에서 사용되며 RADIUS 서버 연동을 필요로 합니다.

None

RADIUS MAC Authentication MAC 주소를 사용하여 장치를 인증합니다.

MAC Format 적합한 MAC 주소 형식을 선택합니다.

Use Empty Password 비밀번호 없이 MAC 주소를 서버에 전송하려면 **Enable** 박스를 체크합니다.

Auth Server IP/Port 첫번째 필드에 RADIUS 인증 서버의 IP 주소를 입력합니다. RADIUS 프로토콜은 네트워크 접속 및 서비스 사용을 위해 AAA (Authentication, Authorization, Accounting) 기능을 제공합니다. 두번째 필드에는 RADIUS 인증 서버의 UDP 포트 번호를 입력합니다. 일반적으로 1812 포트가 사용되며 RADIUS 서버 관리자에게 포트 번호를 확인하시기 바랍니다.

Auth Server Secret Access Point 와 RADIUS 서버 사이의 통신을 인증하는데 사용되는 비밀 번호를 입력합니다. 입력하는 문자는 반드시 대소문자를 구분하여 입력하시기 바랍니다.

Show 박스를 체크하면 비밀 번호를 올바르게 입력하였는지 확인할 수 있습니다.

Accounting Server 과금 서버를 사용할 경우 **Enable** 박스를 체크합니다,.

Acct Server IP/Port 과금 서버를 사용할 경우 첫번째 필드에 과금 서버의 IP 주소를 입력합니다. 두번째 필드에는 RADIUS 과금 서버의 UDP 포트 번호를 입력합니다. 일반적으로 1813 포트가 사용되며 RADIUS 서버 관리자에게 포트 번호를 확인하시기 바랍니다.

Acct Server Secret 과금 서버를 사용할 경우 Access Point 와 RADIUS 서버 사이의 통신을 인증하는데 사용되는 비밀 번호를 입력합니다. 입력하는 문자는 반드시 대소문자를 구분하여 입력하시기 바랍니다.

Show 박스를 체크하면 비밀 번호를 올바르게 입력하였는지 확인할 수 있습니다.

MAC ACL Enable 박스를 체크하면 MAC address Access Control List 옵션을 사용합니다. 자세한 사항은 37 페이지의 **MAC ACL** 항목을 참고하시기 바랍니다.

WEP

Wireless Security

Security:

Authentication Type: Open Shared Key

WEP Key Length: Key Type:

WEP Key: Key Index:

MAC ACL: Enable

Policy:

Authentication Type 아래의 인증 방식 중 한가지를 선택합니다.

- **Open** AP 장치가 Station 장치를 자동으로 인증합니다.
- **Shared Key** AP 장치가 생성한 챌린지 교환 후 Station 장치를 인증합니다.

WEP Key Length WEP 보안 키 길이를 설정합니다. 아래의 두가지 옵션 중 한가지를 선택합니다.

- **64-bit** 10개의 16진수 문자 또는 5개의 ASCII 문자로 구성됩니다.
- **128-bit** 26개의 16진수 문자 또는 13개의 ASCII 문자로 구성됩니다.

Key Type WEP 키 문자 형식을 설정합니다.

- **HEX** 0-9 사이의 숫자와 A-F 사이의 대문자 또는 a-f 사이의 소문자를 사용합니다.
- **ASCII** 표준 알파벳 문자와 숫자를 사용합니다.

WEP Key 적절한 WEP 암호화 키를 입력합니다.

타입	HEX	ASCII
64-bit	10개의 16진수 문자로 구성 (0-9, A-F, a-f) 예: 00112233AA	5개의 ASCII 문자로 구성 예: ubnt1
128-bit	26개의 16진수 문자로 구성 (0-9, A-F, a-f) 예: 00112233445566778899AABBCC	13개의 ASCII 문자로 구성 예: ubntproducts1

Key Index 사용할 WEP 키 색인 번호를 선택합니다. 최대 4개의 WEP 키를 장치에 등록해 놓은 후 1가지 WEP 키를 선택하여 사용할 수 있습니다.

MAC ACL Enable 박스를 체크하면 MAC address Access Control List 옵션을 사용합니다. 자세한 사항은 37 페이지의 **MAC ACL** 항목을 참고하시기 바랍니다.

WPA-AES 또는 WPA2-AES

WPA-AES 와 WPA2-AES 설정 방법은 동일하며 WPA2-AES 방식이 보다 강력한 보안 성능을 제공합니다.

WPA Authentication 아래의 WPA 키 선택 방식 중에서 한가지를 선택합니다.

- **PSK** Pre-shared Key 방식 (기본값)
- **EAP** IEEE 802.1x 인증 방식. EAP(Extensible Authentication Protocol) 방식은 주로 엔터프라이즈 네트워크에서 사용됩니다.

Wireless Security

Security: WPA2-AES

WPA Authentication: PSK

WPA Preshared Key: [] Show

MAC ACL: Enable

PSK

WPA Preshared Key 패스프레이즈(패스워드보다 긴 문자열로 된 비밀 번호)를 입력합니다. 패스프레이즈 키는 최소 8개 이상 63개 이내의 문자와 숫자를 조합하여 구성할 수 있습니다.

Show 버튼을 클릭하면 입력한 문자열을 확인할 수 있습니다.

EAP

EAP - Station 모드

아래의 옵션은 Station 모드에만 적용됩니다.

EAP-TTLS / EAP-PEAP AP에서 사용되는 인증 프로토콜을 선택합니다. 내부 인증 프로토콜은 MSCHAPV2가 사용됩니다.

WPA Anonymous Identity 암호화되지 않은 EAP 인증에서 사용되는 자격증명을 입력합니다.

WPA User Name EAP 인증에 사용되는 아이디를 입력합니다.

WPA User Password EAP 인증에서 사용되는 비밀번호를 입력합니다.

Show 클릭하면 입력한 문자열을 확인할 수 있습니다.

Wireless Security

Security: WPA2-AES

WPA Authentication: EAP, EAP-TTLS, MSCHAPV2

WPA Anonymous Identity: []

WPA User Name: []

WPA User Password: [] Show

EAP - Access Point 모드

아래의 옵션은 Access Point 또는 AP-Repeater 모드에만 적용됩니다.

Auth Server IP/Port 첫번째 필드에 RADIUS 서버의 IP 주소를 입력합니다. RADIUS 네트워크 프로토콜은 네트워크 서비스 및 시스템에 연결하기 위한 인증/허가/과금(AAA) 중앙 관리 기능을 제공합니다. 두번째 필드에는 RADIUS 인증 서버의 UDP 포트 번호를 입력합니다. 일반적으로 1812 소켓 번호가 사용되지만 RADIUS 서버 관리자에게 확인 후 설정하시기 바랍니다.

Auth Server Secret RADIUS 장치 사이의 통신 유효성을 확인할 때 사용되는 비밀번호를 대소문자를 구분하여 입력합니다. **Show** 박스를 클릭하면 입력한 문자열을 확인할 수 있습니다.

Accounting Server 과금 서버를 사용할 경우 옵션을 선택합니다.

Acct Server IP/Port 과금 서버 옵션을 설정할 경우 서버 IP 주소를 입력합니다. 일반적으로 1813 포트가 사용되지만 RADIUS 서버 관리자에게 확인 후 설정하시기 바랍니다.

Acct Server Secret 과금 서버 옵션을 설정할 경우 비밀번호를 입력합니다. RADIUS 장치 사이의 통신 유효성을 확인할 때 사용되는 비밀번호를 대소문자를 구분하여 입력합니다. **Show** 박스를 클릭하면 입력한 문자열을 확인할 수 있습니다.

MAC ACL Enable 박스를 체크하면 MAC address Access Control List 옵션을 사용합니다. 자세한 사항은 37 페이지의 **MAC ACL** 항목을 참고하시기 바랍니다.

Wireless Security

Security: WPA2-AES

WPA Authentication: EAP

Auth Server IP/Port: [] 1812

Auth Server Secret: [] Show

Accounting Server: Enable

Acct Server IP/Port: [] 1813

Acct Server Secret: [] Show

MAC ACL: Enable

MAC ACL

아래의 옵션은 Access Point 및 AP-Repeater 모드에서만 사용할 수 있습니다.

Wireless Security

Security: **WPA2-AES** ▾

WPA Authentication: **PSK** ▾

WPA Preshared Key: Show

MAC ACL: Enable

Policy: **Allow** ▾ **ACL...**

MAC ACL MAC address Access Control List (ACL) 기능은 클라이언트 장치의 MAC 주소를 기반으로 AP 장치에 연결되는 것을 허용하거나 차단합니다. WPA, WPA2 암호화 방식과 MAC ACL 기능을 함께 사용할 경우 무선 네트워크 보안을 더욱더 강화할 수 있습니다. **Enable** 박스를 체크하면 아래의 추가 옵션을 설정할 수 있습니다.

Policy 클라이언트 장치에 적용할 정책 타입을 선택합니다.

- **Allow** 리스트에 등록된 무선 클라이언트 장치의 접속을 허용합니다. 리스트에 포함되지 않은 클라이언트 장치는 AP 장치에 연결할 수 없습니다.
- **Deny** 리스트에 등록된 무선 클라이언트 장치의 접속을 차단합니다. 리스트에 포함되지 않은 클라이언트 장치는 AP 장치에 연결할 수 있습니다.
- **ACL** 무선 클라이언트 장치의 MAC 주소를 추가하려면 버튼을 클릭합니다.

MAC ACL

Enabled	MAC	Comment	Action
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Add

■ **Enabled** 무선 클라이언트에

적용된 정책을 표시합니다.

- **MAC** xx:xx:xx:xx:xx:xx 형태로 클라이언트 장치의 MAC 주소를 입력합니다.
- **Comment** 무선 클라이언트 장치에 대한 설명을 입력합니다.
- **Action** 입력한 무선 클라이언트 장치의 MAC 주소를 리스트에 추가하려면 **Add** 버튼을 클릭합니다. 무선 클라이언트 장치의 MAC 주소를 리스트에서 제거하려면 **Del** 버튼을 클릭합니다. 등록된 MAC 주소를 수정하려면 **Edit** 버튼을 클릭합니다.

Chapter 5: NETWORK

브리지 또는 라우터 기능과 IP 주소를 설정합니다.

Change 설정을 변경한 후 우측 하단의 **Change** 버튼을 클릭하여 변경된 사항을 적용합니다. Change 버튼을 클릭하면 우측 상단에 아래와 같은 3가지 옵션이 표시되며 다음과 같은 옵션 작업을 수행할 수 있습니다.

- **Apply** 버튼을 클릭하면 변경된 설정이 곧바로 적용됩니다.
- **Test** 버튼을 클릭하면 변경된 사항을 저장하지 않고 테스트만 시도합니다. 180 초 이내에 Apply 버튼을 클릭하지 않으면 변경된 설정이 저장되지 않고 이전 설정으로 복구됩니다. Test 버튼을 클릭하면 180 초 동안 화면에 카운트다운이 표시됩니다.
- **Discard** 변경된 설정을 저장하지 않고 취소합니다.

Network Role

RM5 제품은 브리지와 라우터, SOHO 라우터 모드를 지원합니다.

Network Mode 네트워크 모드를 선택합니다. 브리지 모드는 주로 매우 작은 네트워크를 구성할 때 사용됩니다. 도메인 내부의 대용량 브로드캐스팅 트래픽을 관리하고 네트워크 과부하를 방지하도록 네트워크를 구성할 경우 라우터 모드나 SOHO 라우터 모드를 사용합니다. 라우터 모드나 SOHO 라우터 모드는 브로드캐스팅 트래픽을 도메인 내부에서만 처리하며 네트워크 전체에 모든 트래픽이 전달되어 과부하가 발생하는 것을 차단합니다.

- **Bridge** 관리형 스위치와 같이 레이어2 레벨로 동작하며 트랜스퍼런트 브리지로 동작합니다. 무선 장치는 관리 목적을 위한 1개의 IP 주소만 사용합니다.
- **Router** 무선 인터페이스로 외부 네트워크(WAN)를 연결하고 유선 인터페이스로 내부 네트워크(LAN)을 연결할 때 사용합니다. 유선과 무선 인터페이스는 각각 서로 다른 IP 주소를 사용하게 됩니다.
- **SOHO Router** SOHO (Small Office/Home Office) 라우터 모드는 라우터 모드를 기반으로 동작합니다. <...> 라벨이 표시된 메인 이더넷 포트는 외부 네트워크(WAN)에 연결되고 무선 인터페이스와 나머지 이더넷 포트는 내부 네트워크(LAN)에 연결됩니다. 외부와 내부 네트워크 연결에 사용되는 유무선 인터페이스에는 각각 관리 목적으로 사용되는 IP 주소가 할당됩니다.

브리지 모드와 라우터 모드, SOHO 라우터 모드는 다음과 같은 차이점을 제공합니다.

- **브리지 모드**
 - 별도의 라우팅 설정 없이 유선 네트워크 인터페이스로부터 수신한 모든 데이터 패킷을 무선 네트워크 인터페이스로 전달하고 반대로 무선 네트워크로부터 수신한 모든 트래픽을 유선 네트워크로 전달합니다.
 - 별도의 네트워크 세그먼트를 사용하지 않으며 동일한 브로드캐스팅 도메인을 사용합니다. 브리지 모드는 모든 브로드캐스팅 또는 멀티캐스팅 트래픽을 차단하지 않고 전송합니다. 사용자는 레이어2 패킷 필터링 및 접속 제어를 위하여 방화벽 기능을 설정할 수 있습니다.
 - 유선과 무선 인터페이스가 동일한 네트워크 세그먼트에 위치하며 동일한 IP 주소를 사용합니다. 브리지 장치에 설정되는 IP 주소는 무선 장치를 관리하기 위한 목적으로만 사용됩니다.
- **라우터 모드**
 - 라우팅과 네트워크 세그먼트를 위해 레이어3 레벨로 동작합니다. 무선 클라이언트 장치들과 외부 네트워크(WAN)는 다른 IP 서브넷에 위치합니다. 라우터 모드는 브로드캐스트 트래픽을 차단하고 멀티캐스트 트래픽 전송은 허용합니다. 레이어3 패킷 필터링 및 접속 제어를 위하여 방화벽 기능을 설정할 수 있습니다.
 - 무선 장치는 DHCP 서버로 동작하면서 NAT (Network Address Translation) 기능을 제공할 수 있습니다. NAT 기능은 LAN과 WAN 네트워크 사이에 방화벽 기능을 제공합니다.
 - 유선과 무선 인터페이스는 각각 WAN과 LAN 네트워크에 포함된 IP 주소를 사용합니다.

● SOHO 라우터 모드

- 라우팅과 네트워크 세그먼트를 위해 레이어3 레벨로 동작합니다. 무선 클라이언트 장치들과 외부 네트워크 (WAN)는 다른 IP 서브넷에 위치합니다. SOHO 라우터 모드는 브로드캐스트 트래픽을 차단하고 멀티캐스트 트래픽은 허용합니다. 레이어3 패킷 필터링 및 접속 제어를 위하여 방화벽 기능을 설정할 수 있습니다.
- 무선 장치는 DHCP 서버로 동작하면서 NAT (Network Address Translation) 기능을 제공할 수 있습니다. NAT 기능은 LAN과 WAN 네트워크 사이에 방화벽 기능을 제공합니다.
- 일반적으로 메인 이더넷 포트는 ISP (인터넷 서비스 사업자)가 제공하는 모뎀에 연결됩니다.
- 1개의 이더넷 포트를 가진 장치를 Access Point 또는 AP-Repeater 모드로 사용할 경우 SOHO 라우터 모드는 라우터 모드와 유사하게 동작합니다. 라우터 모드와 달리 SOHO 라우터 모드는 유선 인터페이스가 외부 네트워크(WAN)에 연결되고 무선 인터페이스가 내부 네트워크에 연결됩니다. 여러 개의 유선 인터페이스를 제공하는 모델은 메인 유선랜 포트가 WAN 네트워크에 연결되고 나머지 유선랜 포트와 무선 인터페이스가 LAN 네트워크에 연결됩니다. Station 모드로 동작하는 장치는 SOHO 라우터 모드를 사용할 수 없습니다. Station 모드와 SOHO 라우터 모드를 동시에 설정할 경우 장치에 접속할 수 없습니다. 장치 접속이 불가능 할 경우에는 Reset 버튼을 8초 이상 누르고 있다가 때어 초기화 하시기 바랍니다.

Disable Network WLAN, LAN0 또는 LAN1 인터페이스를 사용할 수 없도록 설정합니다. 사용 불가능 상태로 설정한 인터페이스를 통해 레이어2 또는 레이어3 연결을 하지 않도록 주의하시기 바랍니다.

Configuration Mode

상단 **NETWORK** 탭은 Configuration Mode 를 Simple 또는 Advanced 로 설정하는 것에 따라 설정 옵션을 다르게 표시합니다.



Simple 아래와 같은 기본적인 항목을 설정할 수 있으며 고급 설정 옵션은 표시되지 않습니다.

- Network Role
- Configuration Mode
- Management Network Settings (Bridge 모드에서만 표시)
- WAN Network Settings (Router 또는 SOHO Router 모드에서만 표시)
- LAN Network Settings (Router 또는 SOHO Router 모드에서만 표시)
- Port Forwarding (Router 또는 SOHO Router 모드에서만 표시)
- Multicast Routing Settings (Router 또는 SOHO Router 모드에서만 표시)
- DHCP Address Reservation (Router 또는 SOHO Router 모드에서만 표시)

Advanced 기본적인 설정 항목 외에도 다음과 같은 추가 설정 옵션을 제공합니다.

- Interfaces
- IP Aliases
- VLAN Network
- Bridge Network
- Firewall
- IPv6 Firewall
- Static Routes
- Traffic Shaping
- Management Network Settings (Router 또는 SOHO Router 모드에서만 표시)
- IPv6 Static Routes (Router 또는 SOHO Router 모드에서만 표시)

Management Network Settings

Bridge 모드

Management Network Settings

Management Interface:

Management IP Address: DHCP Static

DHCP Fallback IP:

DHCP Fallback NetMask:

Auto IP Aliasing: Enable

IPv6: Enable

IPv6 Address: Static SLAAC

IPv6 Address:

IPv6 Netmask:

Management Interface Advanced 옵션에서 표시되는 항목으로서 장치 관리에 사용되는 인터페이스를 선택합니다.

Management IP Address DHCP 서버로부터 IP 정보를 자동으로 할당 받을 경우 DHCP 를 선택하고, 고정 IP 주소를 사용할 경우 Static 을 선택합니다.

- **DHCP** DHCP 서버로부터 IP 주소, 게이트웨이 IP 주소, DSN 주소를 자동으로 할당 받습니다.
 - **DHCP Fallback IP** DHCP 서버로부터 IP 주소를 할당받지 못할 경우 사용할 IP 주소를 입력합니다.
 - **DHCP Fallback Netmask** DHCP 서버로부터 넷마스크 값을 할당받지 못하면 사용할 netmask 값을 입력합니다.
- **Static** 장치에서 사용할 고정 IP 정보를 입력합니다. 연결되는 네트워크 세그먼트와 같은 IP 정보를 입력합니다.

- **IP Address** 장치에서 사용할 IP 주소를 입력합니다. IP 주소는 장치를 관리하기 위한 목적으로 사용되며 네트워크 세그먼트에 속한 다른 장치의 IP 주소와 중복되지 않아야 합니다.

- **Netmask** 넷마스크 값을 입력합니다. 사용자는 바이너리 형태의 넷마스크 값을 기반으로 IP 주소의 범위와 호스트 장치들이 사용하는 주소의 범위를 확인할 수 있습니다. 넷마스크 값은 장치 네트워크 세그먼트의 주소 범위를 정의하는데 사용됩니다. 일반적으로 사용되는 255.255.255.0 넷마스크는 C 클래스 네트워크를 의미합니다.

- **Gateway IP** 게이트웨이 장치의 IP 주소를 입력합니다. 일반적으로 호스트 라우터 장치의 IP 주소로서 인터넷에 연결할 때에는 인터넷과 연결된 xDSL 모뎀, 케이블 모뎀, WISP 게이트웨이 라우터 장치의 IP 주소를 입력합니다. 무선 장치는 로컬 네트워크에 연결되어 있지 않는 외부 장치로 데이터를 전송할 경우에 게이트웨이로 데이터 패킷을 전달합니다. 브리지 모드에서 게이트웨이 IP 주소는 관리상의 목적으로만 사용되며 동일한 네트워크 세그먼트에 속한 IP 주소로 설정되어야 합니다.

- **Primary DNS IP** 주 DNS (Domain Name System) 서버의 IP 주소를 입력합니다.

- **Secondary DNS IP** 보조 DNS 서버의 IP 주소를 입력합니다. 보조 DNS IP 설정은 옵션 항목으로서 주 DNS 서버가 응답하지 않을 경우에만 사용됩니다.

Management Network Settings

Management IP Address: DHCP Static

IP Address:

Netmask:

Gateway IP:

Primary DNS IP:

Secondary DNS IP:

MTU:

Management VLAN: Enable

VLAN ID:

Auto IP Aliasing: Enable

STP: Enable

MTU Simple 옵션에서 표시되는 항목으로서 MTU 값을 바이트 단위로 입력합니다. MTU (Maximum Transmission Unit) 값은 네트워크 인터페이스를 통해 송수신할 수 있는 최대 프레임 크기를 나타냅니다.

Management VLAN Simple 옵션에서 표시되는 항목으로서 관리형 가상랜(VLAN: Virtual Local Area Network)을 자동으로 생성할 때 **Enable** 박스를 체크합니다. 이 옵션을 사용하면 Untagged VLAN을 포함하여 다른 VLAN 으로부터 무선 장치에 접근할 수 없습니다.

- **VLAN ID** 2부터 4094 값 사이의 고유 VLAN ID 를 입력합니다.

Auto IP Aliasing WLAN/LAN 인터페이스에 해당하는 IP 주소를 자동으로 생성할 경우 체크합니다. 169.254.X.Y 대역의 B 클래스(netmask 255.255.0.0) IP 주소를 생성합니다. 자동으로 생성되는 169.254.X.Y IP 주소에서 X, Y 부분은 무선 장치의 MAC 주소를 사용합니다. 예를 들어 장치의 MAC 주소가 00:15:6D:A3:04:FB 일 경우, 169.254.4.251 주소가 자동으로 생성됩니다. 사용자는 제품 설정을 잘못하거나 IP 주소를 기억하지 못할 경우에도 장치의 MAC 주소를 확인할 수 있다면 장치에 접속할 수 있습니다.

STP STP 기능을 사용할 경우 체크합니다. 내부 네트워크에 연결된 여러 개의 브리지 장치는 대형 네트워크를 생성합니다. STP (Spanning Tree Protocol) 기능은 네트워크에서 최단 경로를 탐색하여 네트워크 루프를 차단합니다. 브리지 장치는 다른 네트워크 장치와 BPDU (Bridge Protocol Data Units) 기반으로 통신합니다. LAN 네트워크에서 브리지 장치를 1대만 사용하거나 네트워크에서 루프 발생 가능성이 없을 경우에는 STP 기능을 사용할 필요가 없습니다.

IPv6 IPv6 주소를 사용할 경우 **Enable** 박스를 체크합니다.

- **Static** IP 정보를 직접 입력할 경우 Static 을 선택합니다.
 - **IPv6 Address** IPv6 주소를 입력합니다.
 - **IPv6 Netmask** IPv6 넷마스크 값을 입력합니다. 기본값: 64
- **SLAAC** IPv6를 사용할 경우 SLAAC (Stateless Address Auto-Configuration) 설정이 기본 선택되며 장치가 스스로 IPv6 주소를 할당합니다.

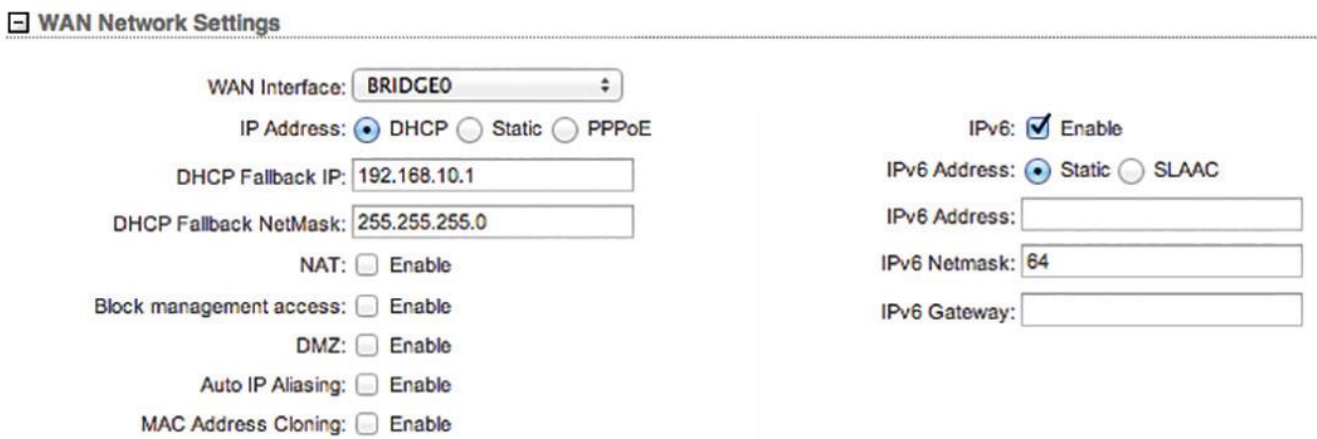
Router 또는 SOHO Router 모드

Management Interface Advanced 옵션에서 표시되는 항목으로서 장치 관리 용도로 사용되는 인터페이스를 선택합니다.



WAN Network Settings

라우터 또는 SOHO 라우터 모드에서만 설정할 수 있습니다.



WAN Interface 외부 네트워크나 인터넷 연결에 사용되는 인터페이스를 선택합니다.

WAN IP Address 외부 네트워크에 연결되는 WAN 인터페이스의 IP 주소를 설정합니다. 설정되는 IP 주소는 라우팅과 장치 관리 용도로 사용됩니다. IP 주소는 DHCP, Static, PPPoE 방식으로 설정할 수 있습니다.

WAN IP Address 를 DHCP 방식으로 설정할 경우

DHCP 서버로부터 IP 주소, 게이트웨이 IP 주소, DNS 주소를 자동으로 할당 받습니다.

DHCP Fallback IP DHCP 서버로부터 IP 주소를 할당받지 못할 경우 장치가 사용할 기본 IP 주소를 입력합니다.

DHCP Fallback Netmask DHCP 서버로부터 넷마스크 값을 할당받지 못할 경우 사용할 기본 넷마스크 값을 입력합니다.

MTU Simple 옵션에서 표시되는 항목으로서 네트워크 인터페이스를 통해 송수신할 수 있는 프레임의 최대 크기를 바이트 단위로 입력합니다. 기본값 1500

NAT NAT (Network Address Translation) 기술은 WAN 인터페이스에 설정된 1개의 공인 IP 주소를 사용하여 LAN 인터페이스에 사설 IP 네트워크를 생성합니다. 외부 WAN 네트워크로부터 내부 LAN 네트워크로의 접속을 차단하기 때문에 방화벽 기능을 제공하며 내부와 외부 네트워크의 연결 정보를 테이블에 자동으로 저장합니다. NAT 기능을 사용하지 않을 경우 패킷 전송을 위한 라우팅을 수동으로 설정하여 사용합니다.

- **NAT Protocol** 내부 네트워크에 연결된 장치는 외부 네트워크에 연결된 장치와 트랜스퍼런트 연결이 지원되지 않습니다. NAT 기능을 사용할 경우 데이터 패킷을 변형하여 특정 패킷이 외부 장치와 연결되게 합니다. SIP, PPTP, FTP, RTSP 와 같은 패킷이 변형되는 것을 방지하려면 해당 항목의 박스를 체크하지 않습니다.

Block management access WAN 인터페이스를 통해 외부 네트워크로부터 무선 장치에 접속하는 것을 차단합니다. 무선 장치가 공인 IP 주소를 사용하면서 라우터나 SOHO 라우터 모드로 사용될 경우 보안을 강화할 수 있습니다.

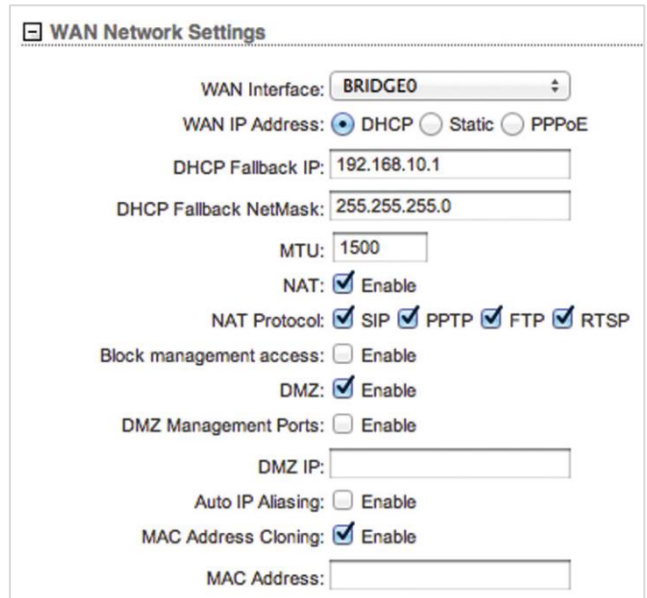
DMZ 1:1 NAT 연결 용도로 사용되며 외부 공인 네트워크로부터 연결되는 모든 통신을 NAT 내부 네트워크에 위치한 1개의 컴퓨터 혹은 장치로 전달합니다.

- **DMZ Management Ports** DMZ IP 주소를 사용하는 장치가 마치 호스트 장치인 것처럼 외부 네트워크로부터의 모든 요청에 응답합니다. 기본적으로 DMZ Management Ports 기능은 사용되지 않기 때문에 WAN 포트를 통해서 RM5 무선 장치에 접속할 수 있습니다. DMZ Management Ports 기능을 설정하면 내부 LAN 네트워크에서만 RM5 무선 장치의 관리 포트에 접속할 수 있습니다. RM5 무선 장치는 네트워크 및 장치 관리를 목적으로 다음과 같은 포트를 사용합니다.
 - HTTP/HTTPS: 80/443 TCP, SSH: 22 TCP, Telnet: 23 TCP, SNMP: 161 UDP, Discovery: 10001 UDP, airView: 18888 TCP
- **DMZ IP** 로컬 호스트 네트워크 장치의 IP 주소를 입력합니다. 외부 네트워크 장치는 DMZ 호스트 장치의 모든 포트로 접속할 수 있습니다.

Auto IP Aliasing WLAN/LAN 인터페이스에 해당하는 IP 주소를 자동으로 생성할 경우 체크합니다. 169.254.X.Y 대역의 B 클래스(netmask 255.255.0.0) IP 주소를 생성합니다. 자동으로 생성되는 169.254.X.Y IP 주소에서 X, Y 부분은 무선 장치의 MAC 주소를 사용합니다. 예를 들어 장치의 MAC 주소가 00:15:6D:A3:04:FB 일 경우, 169.254.4.251 주소가 자동으로 생성됩니다. 사용자는 제품 설정을 잘못하거나 IP 주소를 기억하지 못할 경우에도 장치의 MAC 주소를 확인할 수 있다면 장치에 접속할 수 있습니다.

MAC Address Cloning 무선 장치가 네트워크에서 특정 MAC 주소를 사용해야 할 경우 무선 장치의 MAC 주소를 사용자가 변경할 수 있습니다.

- **MAC Address** 사용할 MAC 주소를 입력합니다.



WAN IP Address 를 Static 방식으로 설정할 경우

무선 장치에 고정 IP 주소를 설정합니다.

IP Address 무선 장치의 IP 주소를 입력합니다. 입력하는 IP 주소는 장치 관리 목적으로만 사용됩니다.

Netmask 네트워크 세그먼트의 주소 범위를 설정합니다. 일반적으로 사용되는 255.255.255.0 값은 C 클래스 네트워크를 구성합니다.

Gateway IP 게이트웨이 장치의 IP 주소를 입력합니다. 무선 장치는 로컬 네트워크에 연결되어 있지 않는 외부 장치로 데이터를 전송할 경우에 게이트웨이로 데이터 패킷을 전달합니다.

Primary DNS IP 주 DNS (Domain Name System) 서버의 IP 주소를 입력합니다.

Secondary DNS IP 보조 DNS 서버의 IP 주소를 입력합니다. 보조 DNS IP 설정은 옵션 항목으로서 주 DNS 서버가 응답하지 않을 경우에만 사용됩니다.

MTU Simple 옵션에서 표시되는 항목으로서 네트워크 인터페이스를 통해 송수신할 수 있는 최대 프레임 크기를 바이트 단위로 입력합니다. 기본값 1500

NAT NAT (Network Address Translation) 기술은 WAN 인터페이스에 설정된 1개의 공인 IP 주소를 사용하여 LAN 인터페이스에 사설 IP 네트워크를 생성합니다. 외부 WAN 네트워크로부터 내부 LAN 네트워크로의 접속을 차단하기 때문에 방화벽 기능을 제공하며 내부와 외부 네트워크의 연결 정보를 테이블에 자동으로 저장합니다. NAT 기능을 사용하지 않을 경우 패킷 전송을 위한 라우팅을 수동으로 설정하여 사용합니다.

- **NAT Protocol** 내부 네트워크에 연결된 장치는 외부 네트워크에 연결된 장치와 트랜스퍼런트 연결이 지원되지 않습니다. NAT 기능을 사용할 경우 데이터 패킷을 변형하여 특정 패킷이 외부 장치와 연결되게 합니다. SIP, PPTP, FTP, RTSP 와 같은 패킷이 변형되는 것을 방지하려면 해당 항목의 박스를 체크하지 않습니다.

Block management access WAN 인터페이스를 통해 외부 네트워크에서 무선 장치에 접속하는 것을 차단합니다. 무선 장치가 공인 IP 주소를 사용하면서 라우터 모드로 사용될 경우 보안을 강화할 수 있습니다.

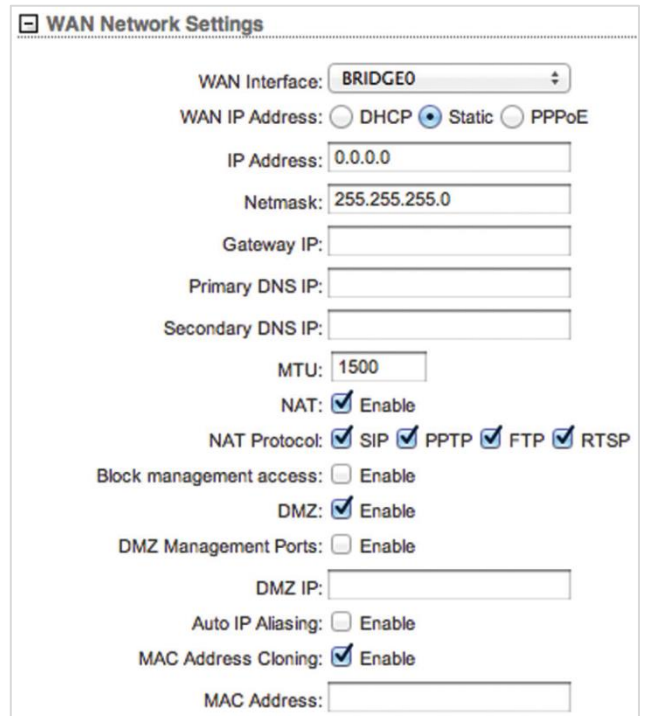
DMZ 1:1 NAT 연결 용도로 사용되며 외부 공인 네트워크로부터 연결되는 모든 통신을 NAT 내부 네트워크에 연결된 1개의 컴퓨터 혹은 장치로 전달합니다.

- **DMZ Management Ports** DMZ IP 주소를 사용하는 장치가 마치 호스트 장치인 것처럼 외부 네트워크로부터의 모든 요청에 응답합니다. 기본적으로 DMZ Management Ports 기능은 사용되지 않기 때문에 WAN 포트를 통해서 RM5 무선 장치에 접속할 수 있습니다. DMZ Management Ports 기능을 설정하면 내부 LAN 네트워크에서만 RM5 무선 장치의 관리 포트에 접속할 수 있습니다. RM5 무선 장치는 네트워크 및 장치 관리를 목적으로 다음과 같은 포트를 사용합니다.
 - HTTP/HTTPS: 80/443 TCP, SSH: 22 TCP, Telnet: 23 TCP, SNMP: 161 UDP, Discovery: 10001 UDP, airView: 18888 TCP
- **DMZ IP** 로컬 호스트 네트워크 장치의 IP 주소를 입력합니다. 외부 네트워크 장치는 DMZ 호스트 장치의 모든 포트 로 접속할 수 있습니다.

Auto IP Aliasing WLAN/LAN 인터페이스에 해당하는 IP 주소를 자동으로 생성할 경우 체크합니다. 169.254.X.Y 대역의 B 클래스(netmask 255.255.0.0) IP 주소를 생성합니다. 자동으로 생성되는 169.254.X.Y IP 주소에서 X, Y 부분은 무선 장치의 MAC 주소를 사용합니다. 예를 들어 장치의 MAC 주소가 00:15:6D:A3:04:FB 일 경우, 169.254.4.251 주소가 자동으로 생성됩니다. 제품 설정을 잘못하거나 IP 주소를 기억하지 못할 경우에도 장치의 MAC 주소를 확인할 수 있다면 장치에 접속할 수 있습니다.

MAC Address Cloning 특정 MAC 주소를 사용해야 할 경우 무선 장치의 MAC 주소를 사용자가 변경할 수 있습니다.

- **MAC Address** 사용할 MAC 주소를 입력합니다.



WAN IP Address 를 PPPoE 방식으로 설정할 경우

PPPoE (Point-to-Point over Ethernet) 연결은 2개의 시스템 사이에 보안 연결을 사용하여 데이터를 전송하며 WAN 인터페이스에만 PPPoE 클라이언트를 설정할 수 있습니다. PPPoE 연결이 성공하면 PPPoE 서버로부터 IP 주소와 게이트웨이 IP, DNS 서버 IP 주소를 할당받게 됩니다. PPPoE 연결이 완료되면 PPP 인터페이스의 IP 주소가 MAIN 탭 다음에 위치한 PPP 인터페이스 통계 화면에 표시됩니다. 터널이 연결이 되지 않으면 Not Connected 메시지와 Reconnect 버튼이 표시됩니다. PPPoE 터널을 재연결 하려면 **Reconnect** 버튼을 클릭합니다.

Username PPPoE 연결에 사용되는 사용자 ID를 입력합니다.

Password PPPoE 연결에 사용되는 비밀번호를 입력합니다. 입력한 비밀번호를 확인하려면 **Show** 버튼을 클릭합니다.

Service Name PPPoE 서비스 이름을 입력합니다.

Fallback IP 무선 장치가 PPPoE 서버로부터 IP 주소를 할당받지 못할 경우 사용할 IP 주소를 입력합니다.

Fallback Netmask 무선 장치가 PPPoE 서버로부터 넷마스크 값을 할당받지 못할 경우 사용할 넷마스크 값을 입력합니다.

MTU/MRU PPP 터널을 통해 데이터를 전달할 때 데이터 캡슐화에 사용되는 MTU(최대 송신 단위) 및 MRU(최대 수신 단위) 값을 바이트 단위로 입력합니다. 기본값 1492

Encryption MPPE (Microsoft Point-to-Point Encryption) 암호화 사용 여부를 설정합니다.

NAT WAN 인터페이스에 설정된 1개의 공인 IP 주소를 사용하여 LAN 인터페이스에 사설 IP 네트워크를 생성합니다. 외부 WAN 네트워크로부터 내부 LAN 네트워크로의 접속을 차단하기 때문에 방화벽 기능을 제공하며 내부와 외부의 연결 정보를 테이블에 자동으로 저장합니다. NAT 기능을 사용하지 않을 경우 패킷 전송을 위한 라우팅을 수동으로 설정하여 사용합니다.

- **NAT Protocol** 내부 네트워크에 연결된 장치는 외부 네트워크에 연결된 장치와 트랜스패런트 연결이 지원되지 않습니다. NAT 기능을 사용할 경우 데이터 패킷을 변형하여 특정 패킷이 외부 장치와 연결되게 합니다. SIP, PPTP, FTP, RTSP 와 같은 패킷이 변형되는 것을 방지하려면 해당 항목의 박스를 체크하지 않습니다.

Block management access WAN 인터페이스를 통해 외부 네트워크 장치가 무선 장치에 접속하는 것을 차단합니다.

DMZ 1:1 NAT 연결 용도로 사용되며 외부 네트워크로부터 연결되는 모든 통신을 NAT 내부 네트워크에 위치한 1개의 컴퓨터 혹은 장치로 전달합니다.

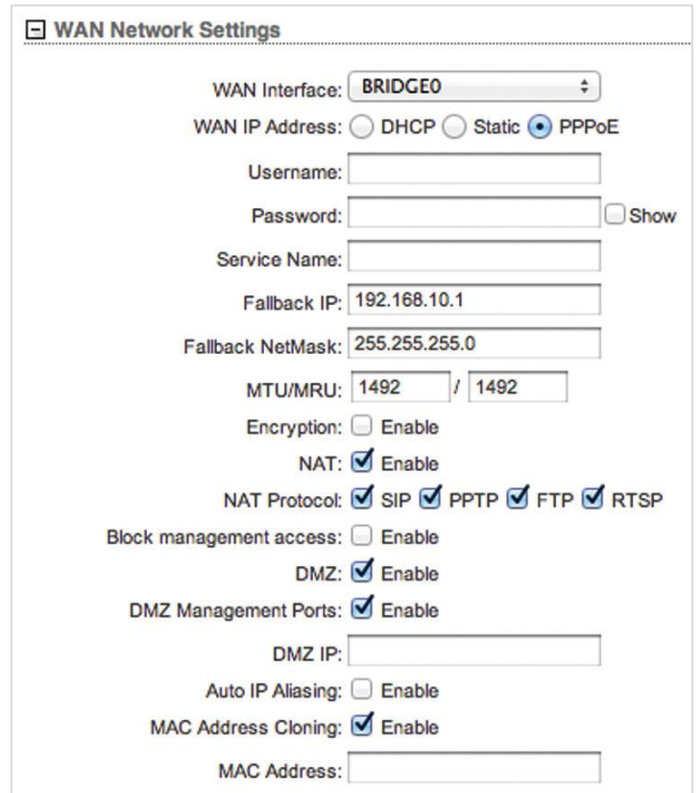
- **DMZ Management Ports** DMZ IP 주소를 사용하는 장치가 마치 호스트 장치인 것처럼 외부 네트워크로부터의 모든 요청에 응답합니다. 기본적으로 DMZ Management Ports 기능은 사용되지 않기 때문에 WAN 포트를 통해서 RM5 무선 장치에 접속할 수 있습니다. DMZ Management Ports 기능을 설정하면 내부 LAN 네트워크에서만 RM5 무선 장치의 관리 포트에 접속할 수 있습니다. RM5 무선 장치는 네트워크 및 장치 관리를 목적으로 다음과 같은 포트를 사용합니다.
 - HTTP/HTTPS: 80/443 TCP, SSH: 22 TCP, Telnet: 23 TCP, SNMP: 161 UDP, Discovery: 10001 UDP, airView: 18888 TCP

- **DMZ IP** 로컬 호스트 네트워크 장치의 IP 주소를 입력합니다.

Auto IP Aliasing WLAN/LAN 인터페이스에 해당하는 IP 주소를 자동으로 생성할 경우 체크합니다. 169.254.X.Y 대역의 B 클래스(netmask 255.255.0.0) IP 주소를 생성합니다. 자동으로 생성되는 169.254.X.Y IP 주소에서 X, Y 부분은 무선 장치의 MAC 주소를 사용합니다. 예를 들어 장치의 MAC 주소가 00:15:6D:A3:04:FB 일 경우, 169.254.4.251 주소가 자동으로 생성됩니다.

MAC Address Cloning 특정 MAC 주소를 사용해야 할 경우 무선 장치의 MAC 주소를 사용자가 변경할 수 있습니다.

- **MAC Address** 사용할 MAC 주소를 입력합니다.



IPv6 IPv6 주소를 사용할 경우 **Enable** 박스를 체크합니다.

- **Static** PPPoE 모드에서는 사용할 수 없습니다.
 - **IPv6 Address** IPv6 주소를 입력합니다.
 - **IPv6 Netmask** IPv6 넷마스크 값을 입력합니다. 기본값: 64
 - **IPv6 Gateway** 로컬 게이트웨이 장치의 주소를 입력합니다.
- **SLAAC** SLAAC (Stateless Address Auto-Configuration) 을 선택하면 장치가 스스로 IPv6 주소를 할당합니다.
- **DHCPv6** 외부 DHCP 서버가 유동 IP 주소 및 게이트웨이 주소, DNS 주소를 무선 장치에 할당합니다.

IPv6: <input checked="" type="checkbox"/> Enable IPv6 Address: <input checked="" type="radio"/> Static <input type="radio"/> SLAAC <input type="radio"/> DHCPv6 IPv6 Address: <input type="text"/> IPv6 Netmask: <input type="text" value="64"/> IPv6 Gateway: <input type="text"/>
IPv6: <input checked="" type="checkbox"/> Enable IPv6 Address: <input type="radio"/> Static <input checked="" type="radio"/> SLAAC <input type="radio"/> DHCPv6
IPv6: <input checked="" type="checkbox"/> Enable IPv6 Address: <input type="radio"/> Static <input type="radio"/> SLAAC <input checked="" type="radio"/> DHCPv6

LAN Network Settings

라우터 또는 SOHO 라우터 모드에서만 설정할 수 있습니다.

LAN Network Settings

LAN Interface: WLAN0 Del IP Address: <input type="text" value="192.168.1.1"/> Netmask: <input type="text" value="255.255.255.0"/> DHCP Server: <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled <input type="radio"/> Relay UPnP: <input type="checkbox"/> Enable	IPv6: <input checked="" type="checkbox"/> Enable IPv6 Address: <input type="text"/> IPv6 Netmask: <input type="text" value="64"/> IPv6 DHCP Server: <input checked="" type="radio"/> Disabled <input type="radio"/> Stateless <input type="radio"/> Stateful
Add LAN: <input type="text"/> Add	

LAN Interface Simple 옵션에서는 LAN 네트워크 연결에 사용할 인터페이스가 표시됩니다. **Del** 버튼을 클릭하여 인터페이스를 제거할 수 있고, 표시되는 인터페이스가 없을 경우 **Add LAN** 콤보박스에서 인터페이스를 선택하고 **Add** 버튼을 클릭합니다.

IP Address LAN 인터페이스에서 사용할 IP 주소를 입력합니다. LAN 인터페이스가 브리지로 사용될 경우 이더넷 및 WLAN 인터페이스와 같은 모든 브리지 포트는 로컬 네트워크 인터페이스로 취급됩니다. 입력하는 IP 주소는 로컬 네트워크의 라우팅에 사용되며 로컬 네트워크에 연결되는 모든 장치들의 게이트웨이 IP 주소로 사용됩니다.

Netmask IP 주소의 범위를 설정합니다. 일반적으로 사용되는 255.255.255.0 넷마스크 값은 C 클래스 네트워크를 구성할 수 있습니다. C 클래스 넷마스크 값 (/24)은 24 비트를 네트워크 식별에 사용하고 나머지 8 비트를 사용하여 호스트를 식별합니다. 넷마스크는 IP 주소가 속한 서브넷을 식별하는데 사용됩니다.

MTU Simple 옵션에서만 표시되는 항목으로서 네트워크 인터페이스를 통해 송수신 할 수 있는 최대 프레임 크기를 바이트 단위로 입력합니다. 기본값 1500

DHCP Server 무선 장치에 내장된 DHCP 서버 기능을 사용하여 LAN 인터페이스에 연결된 클라이언트 장치들에게 IP 주소를 자동으로 할당할 수 있습니다.

- **Disabled** 클라이언트 장치들에게 자동으로 로컬 IP 주소를 할당하지 않습니다.
- **Enabled** 무선 장치가 로컬 네트워크에 연결된 클라이언트 장치들에게 자동으로 IP 주소를 할당합니다.
 - **Range Start** DHCP 서버가 자동으로 할당하는 IP 범위의 시작 주소를 입력합니다.
 - **Range End** DHCP 서버가 자동으로 할당하는 IP 범위의 끝 주소를 입력합니다.
 - **Netmask** IP 주소 범위를 입력합니다. 일반적으로 사용되는 255.255.255.0 넷마스크 값은 C 클래스 네트워크를 구성할 수 있습니다. C 클래스 넷마스크 값 (/24)은 24 비트를 네트워크 식별에 사용하고 나머지 8 비트를 사용하여 호스트를 식별합니다.

- **Lease Time** DHCP 서버가 할당하는 IP 주소의 유효 시간을 초단위로 설정합니다. 유효 시간을 길게 설정할 경우 통신 중간에 IP 주소가 변경될 가능성이 낮아지지만 IP 자원이 쉽게 고갈될 수 있습니다. 반대로 유효 시간을 짧게 설정할 경우 사용 가능한 IP 주소를 효율적으로 관리할 수 있지만 클라이언트 장치의 IP 주소가 자주 변경될 수도 있습니다.
- **DNS Proxy** 설정할 경우 무선 장치가 DNS 프록시 서버로 동작합니다. 따라서 로컬 네트워크에 연결된 호스트 장치들이 전송하는 DNS 요청을 실제 DNS 서버로 전달합니다.
 - ◆ **Primary DNS** 주 DNS 서버의 IP 주소를 입력합니다.
 - ◆ **Secondary DNS** 보조 DNS 서버의 IP 주소를 입력합니다.

LAN Network Settings

LAN Interface: **WLAN0** Del

IP Address:

Netmask:

DHCP Server: Disabled Enabled Relay

Range Start:

Range End:

Netmask:

Lease Time:

DNS Proxy: Enable

UPnP: Enable

Add LAN: Add

- **Relay** DHCP 클라이언트와 서버 사이에 DHCP 메시지를 릴레이합니다. 무선 장치는 DHCP 서버 기능을 제공하지 않으며 백본 네트워크에 연결된 DHCP 서버가 무선 장치에 연결된 클라이언트 장치에 IP 주소를 할당합니다.
 - **DHCP Server IP** 백본 네트워크에 연결된 DHCP 서버의 IP 주소를 입력합니다.
 - **Agent-ID** DHCP 릴레이 에이전트의 아이디를 입력합니다.

LAN Network Settings

LAN Interface: **WLAN0** Del

IP Address:

Netmask:

DHCP Server: Disabled Enabled Relay

DHCP Server IP:

Agent-ID:

UPnP: Enable

Add LAN: Add

UPnP 게임 및 영상, 채팅, 회의 등의 어플리케이션에 사용되는 UPnP (Universal Plug-and-Play) 네트워크 프로토콜 사용 여부를 설정합니다.

Add LAN Advanced 옵션에서 표시되는 항목으로서 인터페이스를 선택한 후 **Add** 버튼을 클릭합니다.

IPv6 IPv6 주소를 사용할 경우 **Enable** 박스를 체크합니다.

- **IPv6 DHCP Server** Access Point 및 AP-Repeater 모드에서는 내장된 DHCPv6 서버를 사용하여 연결되어 있는 유무선 클라이언트 장치들에게 IPv6 주소를 할당합니다. 무선 장치가 Station 모드로 동작할 경우에는 내장된 DHCPv6 서버를 사용하여 유선랜 인터페이스에 연결된 장치들에게만 IPv6 주소를 할당합니다.
 - **Disabled** IPv6 주소 및 다른 네트워크 정보를 클라이언트 장치에게 자동으로 할당하지 않습니다.
 - **Stateless** DHCP 클라이언트 장치가 자신의 IPv6 주소를 직접 선택합니다. DHCPv6 서버는 IP 주소를 제외한 나머지 네트워크 정보를 DHCP 클라이언트 장치에게 할당합니다.
 - ◆ **DNS Proxy** Stateless 를 선택할 경우 DNS Proxy 가 자동으로 설정됩니다. DNS Proxy 서버는 로컬 네트워크에 연결된 호스트 장치가 전송한 DNS 요청을 DNS 서버로 전달합니다.
 - ◆ **Preferred DNS** DNS Proxy 를 설정하지 않을 경우 DNS 서버 주소를 직접 입력합니다.

IPv6: Enable

IPv6 DHCP Server: Disabled Stateless Stateful

DNS Proxy: Enable

IPv6: Enable

IPv6 DHCP Server: Disabled Stateless Stateful

DNS Proxy: Enable

Preferred DNS:

- **Stateful** DHCPv6 서버가 IP 주소 및 다른 네트워크 정보를 DHCP 클라이언트 장치에게 할당합니다.
 - ◆ **DNS Proxy** Stateless 또는 Stateful 을 선택할 경우 DNS Proxy 가 자동으로 설정됩니다. DNS Proxy 서버는 로컬 네트워크에 연결된 호스트 장치가 전송한 DNS 요청을 DNS 서버로 전달합니다.

IPv6: Enable
 IPv6 DHCP Server: Disabled Stateless Stateful
 DNS Proxy: Enable
 - ◆ **Preferred DNS** DNS Proxy 를 설정하지 않을 경우 DNS 서버 주소를 직접 입력합니다.
- **IPv6 Address WAN Network Settings** 에서 IPv6 를 위한 DHCPv6 기능을 설정할 경우 표시됩니다.
 - **Static** IPv6 네트워크 정보를 직접 설정합니다.
 - ◆ **IPv6 Address** 장치의 IPv6 주소를 입력합니다.
 - ◆ **IPv6 Netmask** 장치의 넷마스크 값을 입력합니다.
 - ◆ **IPv6 DHCP Server** 47 페이지 **IPv6 DHCP Server** 항목을 참고하시기 바랍니다.

IPv6: Enable
 IPv6 Address: Static Prefix Delegation
 IPv6 Address:
 IPv6 Netmask:
 IPv6 DHCP Server: Disabled Stateless Stateful
 - **Prefix Delegation** 서비스 사업자가 운영하는 DHCPv6 서버가 자동으로 IPv6 주소를 할당합니다.
 - ◆ **IPv6 Prefix Length** DHCPv6 서버가 제공하는 위임 프리픽스 길이를 입력합니다. 일반적으로 인터넷 서비스 사업자가 제공하는 값을 입력합니다. 기본값 64
 - ◆ **IPv6 DHCP Server** 47 페이지 **IPv6 DHCP Server** 항목을 참고하시기 바랍니다.

IPv6: Enable
 IPv6 Address: Static Prefix Delegation
 IPv6 Prefix Length: [?]
 IPv6 DHCP Server: Disabled Stateless Stateful

DHCP Address Reservation

DHCP 서버 기능이 설정된 라우터 및 SOHO 라우터 모드에서만 사용할 수 있습니다. DHCP 서버는 DHCP 클라이언트 장치들에게 유동 IP 주소를 할당하지만 클라이언트 장치의 MAC 주소를 기반으로 고정 IP 주소를 할당할 수도 있습니다. + 버튼을 클릭하면 아래와 같은 DHCP Address Reservation 섹션이 표시됩니다.

DHCP Address Reservation

Enabled	Interface	MAC Address	IP Address	Comment	Action
	BRIDGE0 ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>	Add

Enabled 특정 DHCP 주소 예약 기능을 사용합니다.

Interface 적절한 인터페이스를 선택합니다.

MAC Address DHCP 클라이언트 장치의 MAC 주소를 입력합니다.

IP Address DHCP 클라이언트 장치에 할당될 IP 주소를 입력합니다.

Comment 해당 주소 예약 기능에 대한 목적 및 설명을 입력합니다.

Action 다음과 같은 옵션 작업을 수행할 수 있습니다.

- **Add** 입력한 DHCP 주소 예약 설정을 추가합니다.
- **Edit** 등록된 DHCP 주소 예약 설정을 수정합니다. 수정 후 **Save** 버튼을 클릭하여 변경된 설정을 저장합니다.
- **Del** 선택한 DHCP 주소 예약 설정을 삭제합니다.

Port Forwarding

라우터 및 SOHO 라우터 모드에서만 지원되는 항목으로서 외부 네트워크(WAN) 장치가 로컬 네트워크에 연결되어 있는 호스트 시스템의 특정 포트에 연결할 수 있도록 합니다. FTP 서버, VoIP, 게임과 같은 호스트 시스템은 일반적으로 IP 주소와 함께 범용적인 포트 번호를 사용하기 때문에 포트 포워딩 기술을 유용하게 사용할 수 있습니다. + 버튼을 클릭하면 아래와 같은 Port Forwarding 섹션이 표시됩니다.

Port Forwarding

Enabled	Interface	Private		Type	Source IP/mask		Public		Comment	Action
		IP	Port		IP/mask	Port				
<input type="checkbox"/>	LAN0 ▾	<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Add

Enabled 특정 포트 포워딩 규칙을 사용하도록 설정합니다.

Interface 포트 포워딩 규칙을 적용할 인터페이스를 선택합니다.

Private IP 외부 네트워크로부터 접속이 필요한 로컬 호스트 장치의 IP 주소를 입력합니다.

Private Port 로컬 호스트 장치에서 실행되는 어플리케이션의 TCP, UDP 포트 번호를 입력합니다. 외부 네트워크 장치는 입력된 포트로 접속할 수 있습니다.

Type 로컬 네트워크로부터 포워딩되는 레이어3 프로토콜 (IP) 타입을 선택합니다.

Source IP/mask 데이터 송신 장치의 IP 주소와 넷마스크 값을 입력합니다.

Public IP/mask 내부 네트워크로 연결을 포워딩할 외부 네트워크 장치의 공인 IP 주소와 넷마스크 값을 입력합니다.

Public Port 외부 네트워크로부터 연결이 포워딩되는 로컬 호스트 장치의 TCP, UDP 포트 번호를 입력합니다.

Comment 웹 서버, FTP 서버, 게임 서버와 같이 포트 포워딩 규칙에 대한 설명을 입력합니다.

Action 다음과 같은 추가 작업을 수행할 수 있습니다.

- **Add** 입력한 포트 포워딩 규칙을 추가합니다.
- **Edit** 선택한 포트 포워딩 규칙을 수정합니다. **Save** 버튼을 클릭하면 변경된 설정이 저장됩니다.
- **Del** 선택한 포트 포워딩 규칙을 삭제합니다.

Multicast Routing Settings

라우터 및 SOHO 라우터 모드에서만 표시되는 항목으로서 멀티캐스트 네트워크를 설계할 때 데이터를 수신할 컴퓨터들을 그룹으로 지정한 후 패킷을 전송할 수 있습니다. 이 기술은 수신 장치마다 데이터를 전송하는 것이 아니라 수신 장치들을 그룹화하여 패킷을 전송합니다. 따라서 패킷 수신을 필요로 하는 호스트 장치들에게만 패킷을 전달합니다. 일반적인 라우터 장치는 로컬과 외부 네트워크 사이에서 모든 브로드캐스트(멀티캐스트) 트래픽을 차단하지만 멀티캐스트 라우팅 설정을 사용하여 멀티캐스트 트래픽을 전송할 수 있습니다. + 버튼을 클릭하면 아래와 같은 Multicast Routing Settings 섹션이 표시됩니다.

Multicast Routing Enable 박스를 체크하면 라우터 모드로 동작하는 장치에서 로컬과 외부 네트워크 사이에 멀티캐스트 패킷 전송을 허용합니다. 멀티캐스트 패킷 전송은 IGMP (Internet Group Management Protocol) 기술을 사용합니다.

Multicast Upstream 멀티캐스트 트래픽의 소스(송신 인터페이스)를 선택합니다.

Multicast Downstream 멀티캐스트 트래픽을 수신하는 인터페이스를 입력합니다.

- **Add** 멀티캐스트 트래픽을 수신하는 인터페이스를 추가합니다.
- **Del** 등록된 멀티캐스트 트래픽 수신 인터페이스를 삭제합니다.

Multicast Routing Settings

Multicast Routing: Enable

Multicast Upstream: BRIDGE0 ▾

Multicast Downstream:

Add ▾ Del

Interfaces

Advanced 옵션에서 표시되는 항목으로서 네트워크 인터페이스를 통해 송수신할 수 있는 최대 프레임 크기를 바이트 단위로 설정합니다. 인터페이스마다 서로 다른 MTU 값을 설정할 수 있으며 + 버튼을 클릭하면 Interfaces 섹션이 표시됩니다.

Interface 인터페이스 이름을 표시합니다.

MTU 제품 모델에 따라 하드웨어 성능이 제한될 수 있으며 일반적으로 2024 바이트 MTU 값을 사용합니다. 기본값: 1500

Action MTU 값을 변경하려면 **Edit** 버튼을 클릭합니다. 변경된 설정을 저장하려면 **Save** 버튼을 클릭하고 변경을 취소하려면 **Cancel** 버튼을 클릭합니다.

Interfaces		
Interface	MTU	Action
BRIDGE0	1500	Save Cancel
LAN0	1500	Edit
LAN1	1500	Edit
WLAN0	1500	Edit

IP Aliases

Advanced 옵션에서 표시되는 항목으로서 관리 목적을 위하여 네트워크 인터페이스의 IP 에일리어스를 설정합니다. 예를 들어 1개의 장치에서 1개의 공인 IP 주소와 1개의 사설 IP 주소를 사용할 수 있습니다. PPPoE 방식을 사용하는 CPE 장치는 공인 PPPoE 주소를 할당받지만 네트워크 관리자는 내부 IP 에일리어스를 장치에 부여합니다. 따라서 네트워크 관리자는 PPPoE 서버를 경유하지 않고 내부적으로 장치를 관리할 수 있습니다. + 버튼을 클릭하면 IP Aliases 섹션이 표시됩니다.

IP Aliases

Enabled	Interface	IP Address	Netmask	Comment	Action
	BRIDGE0				Add

Enabled 특정 IP 에일리어스를 사용하도록 설정합니다. 추가된 모든 IP 에일리어스는 시스템 설정 파일에 저장되고 Enabled 로 설정한 IP 에일리어스만 장치에서 사용됩니다.

Interface 적절한 인터페이스를 선택합니다.

IP Address 인터페이스의 대체 IP 주소를 표시합니다. 입력 값은 라우팅 및 장치 관리를 위해 사용됩니다.

Netmask IP 에일리어스를 위한 네트워크 주소 범위 식별자를 입력합니다.

Comment IP 에일리어스 용도에 대한 설명을 입력합니다.

Action IP 에일리어스는 추가 및 변경 및 제거 작업이 가능합니다.

- **Add** IP 에일리어스를 추가할 경우 클릭합니다.
- **Edit** IP 에일리어스를 변경합니다. 변경 후 **Save** 버튼을 클릭합니다.
- **Del** IP 에일리어스를 제거합니다.

VLAN Network

Advanced 옵션에서 표시되는 항목으로서 여러 개의 가상랜을 생성할 수 있습니다. + 버튼을 클릭하면 VLAN Network 섹션이 표시됩니다.

VLAN Network

Enabled	Interface	VLAN ID	Comment	Action
	LAN0			Add

Enabled 특정 VLAN을 활성화 할 때 옵션을 선택합니다. 추가된 모든 VLAN은 시스템 설정 파일에 저장되고 활성화된 VLAN 만 장치에서 사용됩니다.

Interface VLAN에 사용할 인터페이스를 선택합니다.

VLAN ID 다른 VLAN과 중복되지 않는 아이디를 입력합니다. 각각의 VLAN 마다 서로 다른 VLAN ID를 사용합니다. VLAN ID는 2부터 4094 사이의 값을 사용할 수 있습니다.

Comment VLAN 용도에 대한 설명을 입력합니다.

Action 아래와 같은 옵션 작업을 수행할 수 있습니다.

- **Add** VLAN을 생성하려면 Add 버튼을 클릭합니다.
- **Edit** VLAN 설정을 수정합니다. 변경된 설정을 저장하려면 **Save** 버튼을 클릭합니다.
- **Del** VLAN을 삭제합니다. (관리 인터페이스로 설정된 VLAN 은 삭제할 수 없습니다.)

Bridge Network

Advanced 옵션에서 표시되는 항목으로서 1개 이상의 레이어2 트랜스패런트 브리지 네트워크를 생성할 수 있습니다. 이더넷 스위치 사용과 유사한 방식으로 VLAN 및 IP 주소와 상관없이 브리지 장치의 한쪽 포트를 통해 입력된 모든 트래픽이 다른 포트를 통해 출력됩니다. 예를 들어 장치의 무선과 유선 인터페이스에 동일한 IP 서브넷을 사용하려고 할 때 브리지 네트워크를 생성합니다. + 버튼을 클릭하면 Bridge Network 섹션이 표시됩니다.

Bridge Network

Enabled	Interface	STP	Ports	Comment	Action
<input checked="" type="checkbox"/>	BRIDGE0	<input type="checkbox"/>	<div style="border: 1px solid gray; padding: 2px;"> LAN0 WLAN0 LAN1 </div>		Del
<div style="display: flex; justify-content: flex-end; gap: 10px;"> Add Del </div>					
<div style="display: flex; justify-content: flex-end; gap: 10px;"> Add </div>					

Enabled 특정 브리지 네트워크를 활성화할 때 선택합니다. 추가된 모든 브리지 네트워크는 시스템 구성 파일에 저장되고 활성화된 브리지 네트워크만 사용할 수 있습니다.

Interface 자동으로 인터페이스 이름을 표시합니다.

STP 802.1d STP 기능을 사용할 경우 선택합니다. 다중으로 연결된 브리지들은 대규모 네트워크를 생성하게 됩니다. STP (Spanning Tree Protocol) 기능은 네트워크에서 최단 경로를 검색하여 네트워크 루프를 제거합니다. STP 옵션을 선택하면 BPDU (Bridge Protocol Data Units) 송수신을 통해 다른 네트워크 장치와 통신합니다. LAN 네트워크에서 해당 장치가 유일한 브리지 장치이거나 네트워크에서 루프가 발생할 가능성이 없을 경우에는 STP 기능을 사용할 필요가 없습니다.

Ports 브리지 네트워크에 적합한 포트를 선택합니다. 만약 VLAN을 생성하였을 경우 가상 포트를 선택하는 것도 가능합니다.

- **Add** 사용 가능한 포트를 선택한 후 Add 버튼을 클릭합니다.
- **Del** 제거할 포트를 선택한 후 Del 버튼을 클릭합니다.

Comment 브리지 네트워크 용도에 대한 설명을 입력합니다.

Action 다음과 같은 추가 작업을 수행할 수 있습니다.

- **Add** 버튼을 클릭하면 브리지 네트워크를 생성합니다.
- **Del** 브리지 네트워크를 삭제합니다. 관리 인터페이스로 설정된 브리지는 삭제할 수 없습니다.

Firewall

Advanced 옵션에서 표시되는 항목으로서 네트워크 인터페이스에 방화벽 규칙을 설정합니다. Bridge 모드로 장치를 사용할 경우 ebtables 필터 테이블의 FIREWALL 체인에 모든 방화벽 항목들이 저장되고, Router 및 SOHO 라우터 모드로 장치를 사용할 경우에는 iptables 필터 테이블에 방화벽 항목들이 저장됩니다. ebtables 테이블은 브리지 인터페이스에서 사용되는 트랜스패런트 링크 레이어 필터링 도구로서 브리지를 통해 전달되는 네트워크 트래픽을 필터링합니다. 여러 개의 방화벽 규칙은 특정 패킷에 순차적으로 적용됩니다. + 버튼을 클릭하면 Firewall 섹션이 표시됩니다.

Firewall

Enable

Enabled	Target	Interface	IP Type	Source			Destination			Action		
Comment				!	IP/Mask	!	Port	!	IP/Mask	!	Port	
	<input type="text" value="DROP"/>	<input type="text" value="ANY"/>	<input type="text" value="IP"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Add"/>
<input type="text"/>												

Enable 방화벽 기능을 사용하려면 선택합니다.

Enabled 특정 방화벽 규칙을 사용하려면 선택합니다. 모든 방화벽 규칙은 시스템 설정 파일에 적용되며 사용자가 선택한 방화벽 규칙만 장치에서 사용됩니다.

Target 방화벽을 통과하는 패킷은 **ACCEPT**를 선택하고 방화벽에서 차단할 패킷은 **DROP**을 선택합니다.

Interface 방화벽 규칙을 적용할 인터페이스를 선택합니다. 모든 인터페이스에 방화벽을 적용하려면 **ANY**를 선택합니다.

IP Type IP, ICMP, TCP, UDP 와 같이 필터링이 적용될 레이어3 프로토콜 타입을 표시합니다.

! Source IP/Mask, Source Port, Destination IP/Mask, Destination Port 필터링 항목에 대하여 입력 값을 제외한 모든 범위에 방화벽 규칙을 적용할 경우 체크합니다. 예를 들어 Source Port 에 2500번 포트를 입력하고 ! 박스를 체크하면 2500번 포트에서 송신된 패킷을 제외한 모든 패킷에 대하여 방화벽 규칙이 적용됩니다.

Source IP/Mask 일반적으로 패킷을 송신하는 호스트 시스템의 IP 정보로서 패킷 헤더에 포함되어 있는 송신 IP를 입력합니다. 넷마스크 값은 CIDR 방식(슬래시 표기법)을 사용하여 입력합니다. 예를 들어 192.168.1.0/24 값을 입력하는 것은 192.168.1.0 부터 192.168.1.255 범위의 주소를 입력하는 것과 같습니다.

Source Port 일반적으로 패킷을 송신하는 호스트 시스템 어플리케이션의 포트 번호로서 패킷 헤더에 포함되어 있는 송신 포트 번호를 입력합니다.

Destination IP/Mask 일반적으로 패킷을 수신하는 시스템의 IP 정보로서 패킷 헤더에 포함되어 있는 수신 IP를 입력합니다. 넷마스크 값은 CIDR 방식(슬래시 표기법)을 사용하여 입력합니다. 예를 들어 192.168.1.0/24 값을 입력하는 것은 192.168.1.0 부터 192.168.1.255 범위의 주소를 입력하는 것과 같습니다.

Destination Port 일반적으로 패킷을 수신하는 호스트 시스템 어플리케이션의 포트 번호로서 패킷 헤더에 포함되어 있는 수신 포트 번호를 입력합니다.

Comment 방화벽 규칙에 대한 설명을 입력합니다.

Action 방화벽 규칙에 대하여 아래의 옵션 작업을 수행할 수 있습니다.

- **Add** 버튼을 클릭하면 새로운 방화벽 규칙을 생성합니다.
- **Edit** 방화벽 규칙을 수정합니다. 변경된 방화벽 규칙을 저장하려면 **Save** 버튼을 클릭합니다.
- **Del** 방화벽 규칙을 삭제합니다.

IPv6 Firewall

Advanced 옵션에서 표시되는 항목으로서 IPv6 네트워크 인터페이스에 방화벽 규칙을 설정합니다. + 버튼을 클릭하면 IPv6 Firewall 섹션이 표시됩니다.

IPv6 Firewall

Enable

Enabled	Target	Interface	IP Type	Source			Destination			Action		
Comment				!	IP/Mask	!	Port	!	IP/Mask	!	Port	
	ACCEPT	ANY	IP	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	Add
<input type="text"/>												

Enable 방화벽 기능을 사용하려면 선택합니다.

Enabled 특정 방화벽 규칙을 사용하려면 선택합니다. 모든 방화벽 규칙은 시스템 설정 파일에 적용되며 사용자가 선택한 방화벽 규칙만 장치에서 사용됩니다.

Target 방화벽을 통과하는 패킷은 **ACCEPT**를 선택하고 방화벽에서 차단할 패킷은 **DROP**을 선택합니다.

Interface 방화벽 규칙을 적용할 인터페이스를 선택합니다. 모든 인터페이스에 방화벽을 적용하려면 **ANY**를 선택합니다.

IP Type IP, ICMP, TCP, UDP 와 같이 필터링이 적용될 레이어3 프로토콜 타입을 표시합니다.

! Source IP/Mask, Source Port, Destination IP/Mask, Destination Port 필터링 항목에 대하여 입력 값을 제외한 모든 범위에 방화벽 규칙을 적용할 경우 체크합니다. 예를 들어 Source Port 에 2500번 포트를 입력하고 ! 박스를 체크하면 2500번 포트에서 송신된 패킷을 제외한 모든 패킷에 대하여 방화벽 규칙이 적용됩니다.

Source IP/Mask 일반적으로 패킷을 송신하는 호스트 시스템의 IP 정보로서 패킷 헤더에 포함되어 있는 송신 IP를 입력합니다. 넷마스크 값은 CIDR 방식(슬래시 표기법)을 사용하여 입력합니다. 예를 들어 2001:db8::/64 값을 입력하는 것은 2001:0db8:0000:0000:0000:0000:0000:0000 부터 2001:0db8:0000:0000:ffff:ffff:ffff:ffff 사이의 주소를 입력하는 것과 같습니다.

Source Port 일반적으로 패킷을 송신하는 호스트 시스템 어플리케이션의 포트 번호로서 패킷 헤더에 포함되어 있는 송신 포트 번호를 입력합니다.

Destination IP/Mask 일반적으로 패킷을 수신하는 시스템의 IP 정보로서 패킷 헤더에 포함되어 있는 수신 IP를 입력합니다. 넷마스크 값은 CIDR 방식(슬래시 표기법)을 사용하여 입력합니다. 예를 들어 2001:db8::/64 값을 입력하는 것은 2001:0db8:0000:0000:0000:0000:0000:0000 부터 2001:0db8:0000:0000:ffff:ffff:ffff:ffff 사이의 주소를 입력하는 것과 같습니다.

Destination Port 일반적으로 패킷을 수신하는 호스트 시스템 어플리케이션의 포트 번호로서 패킷 헤더에 포함되어 있는 수신 포트 번호를 입력합니다.

Comment 방화벽 규칙에 대한 설명을 입력합니다.

Action 방화벽 규칙에 대하여 아래의 옵션 작업을 수행할 수 있습니다.

- **Add** 버튼을 클릭하면 새로운 방화벽 규칙을 생성합니다.
- **Edit** 방화벽 규칙을 수정합니다. 변경된 방화벽 규칙을 저장하려면 **Save** 버튼을 클릭합니다.
- **Del** 방화벽 규칙을 삭제합니다.

Static Routes

Advanced 옵션에서 표시되는 항목으로서 시스템 라우팅 테이블에 고정 라우팅 규칙을 수동으로 추가합니다. 따라서 사용자는 수신 IP 주소나 네트워크 범위에 따라 특정 게이트웨이를 경유하도록 설정할 수 있습니다. + 버튼을 클릭하면 Static Routes 섹션이 표시됩니다.

Static Routes

Enabled	Target Network IP	Netmask	Gateway IP	Comment	Action
					Add

Enabled 특정 라우팅 규칙을 활성화 할 경우 체크합니다. 추가된 고정 라우팅 규칙은 시스템 설정 파일에 저장되며 활성화된 규칙만 장치에서 사용됩니다.

Target Network IP 패킷 수신 IP 주소를 입력합니다.

Netmask 패킷 수신 네트워크의 넷마스크를 입력합니다.

Gateway IP 게이트웨이 IP 주소를 입력합니다.

Comment 고정 라우팅 규칙에 대한 설명을 입력합니다.

Action 고정 라우팅 규칙에 대하여 다음과 같은 추가 작업을 수행할 수 있습니다.

- **Add** 고정 라우팅 규칙을 추가할 때 클릭합니다.
- **Edit** 고정 라우팅 규칙을 수정합니다. 변경된 라우팅 규칙을 저장하려면 **Save** 버튼을 클릭합니다.
- **Del** 생성된 고정 라우팅 규칙을 삭제합니다.

IPv6 Static Routes

라우터 및 SOHO 라우터 모드로 동작하는 장치의 Advanced 옵션에서 표시되는 항목으로서 시스템 라우팅 테이블에 IPv6 고정 라우팅 규칙을 수동으로 추가합니다. 따라서 사용자는 수신 IP 주소나 네트워크 범위에 따라 특정 게이트웨이를 경유하도록 설정할 수 있습니다. + 버튼을 클릭하면 IPv6 Static Routes 섹션이 표시됩니다.

IPv6 Static Routes

Enabled	Target Network IP	Netmask	Gateway IP	Comment	Action
					Add

Enabled 특정 라우팅 규칙을 활성화 할 경우 체크합니다. 추가된 고정 라우팅 규칙은 시스템 설정 파일에 저장되며 활성화된 규칙만 장치에서 사용됩니다.

Target Network IP 패킷 수신 IP 주소를 입력합니다.

Netmask 패킷 수신 네트워크의 넷마스크를 입력합니다. 넷마스크 값은 CIDR 방식(슬래시 표기법)을 사용하여 입력합니다. 예를 들어 2001:db8::/64 값을 입력하는 것은 2001:0db8:0000:0000:0000:0000:0000:0000 부터 2001:0db8:0000:0000:ffff:ffff:ffff:ffff 사이의 범위를 입력하는 것과 같습니다.

Gateway IP 게이트웨이 IP 주소를 입력합니다.

Comment 고정 라우팅 규칙에 대한 설명을 입력합니다.

Action 고정 라우팅 규칙에 대하여 다음과 같은 추가 작업을 수행할 수 있습니다.

- **Add** 고정 라우팅 규칙을 추가할 때 클릭합니다.
- **Edit** 고정 라우팅 규칙을 수정합니다. 변경된 라우팅 규칙을 저장하려면 **Save** 버튼을 클릭합니다.
- **Del** 생성된 고정 라우팅 규칙을 삭제합니다.

Traffic Shaping

Advanced 옵션에서만 표시되는 항목으로서 트래픽 성형(Traffic Shaping)은 클라이언트 관점에서 대역폭을 제어합니다. Station 모드에서 버스팅(Bursting)은 사용자가 웹 사이트와 같은 작은 파일을 빠르게 다운로드 할 수 있게 하지만 영상 스트리밍과 같이 대역폭을 초과하는 대용량 파일 다운로드를 차단합니다. 레이어3 QoS 정책을 기반으로 사용자가 지정한 제한 속도에 따라 인터페이스 트래픽을 제한할 수 있습니다. 각각의 인터페이스에는 다음과 같이 2가지 타입의 트래픽이 존재합니다.

- **Ingress** 인터페이스를 통해 들어오는 트래픽
- **Egress** 인터페이스를 빠져나가는 트래픽

인터페이스를 통해 들어오는 트래픽을 제어하는 것보다 인터페이스를 통해 빠져나가는 트래픽을 제어하는 것이 보다 효율적입니다. 인터페이스를 통해 짧은 시간에 많은 인그레스 트래픽이 수신되는 경우 혼잡이 발생하고 패킷 분실이 발생할 확률이 높지만 인터페이스를 통해 송신되는 이그레스 트래픽은 제어가 가능합니다. 버스팅은 사용자가 설정한 최대 대역폭보다 대역폭이 급등하는 것을 짧은 시간 동안에 허용합니다. 최대 대역폭에 도달하면 사용자가 설정한 인그레스 및 이그레스 속도(최대 대역폭)에 따라 데이터 처리 속도를 하향 조정합니다.

예를 들어 이그레스 버스트가 2048KB, 이그레스 속도가 512Kbit/s 이고 실제 최대 대역폭은 1024Kbit/s 라고 가정합니다. 버스팅은 512kbit/s로 속도를 낮추기 전에 잠시동안 2048KB가 1024Kbit/s 속도로 전송되게 합니다. Traffic Shaping 섹션을 클릭하면 다음과 같은 화면이 표시됩니다.

Traffic Shaping

Enable

Enabled	Interface	Ingress			Egress			Action
		Enable	Rate, kbit/s	Burst, kBytes	Enable	Rate, kbit/s	Burst, kBytes	
	WLAN0	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

Enable 장치에서 대역폭 제어 기능을 사용할 경우 체크합니다.

Enabled 특정 규칙을 사용할 경우 체크합니다. 추가된 모든 규칙은 시스템 설정 파일에 저장되며 체크한 규칙만 장치에서 활성화됩니다.

Interface 규칙을 적용할 인터페이스를 선택합니다.

Ingress

- **Enable** 인그레스 규칙을 사용하려면 체크합니다.
- **Rate, kbit/s** 지정한 인터페이스를 통해 입력되는 최대 대역폭을 설정합니다.
- **Burst, kBytes** 인그레스 최대 대역폭을 적용하기 전에 허용되는 최대 데이터 볼륨을 입력합니다.

Egress

- **Enable** 이그레스 규칙을 사용하려면 체크합니다.
- **Rate, kbit/s** 지정한 인터페이스를 통해 출력되는 최대 대역폭을 설정합니다.
- **Burst, kBytes** 이그레스 최대 대역폭을 적용하기 전에 허용되는 최대 데이터 볼륨을 입력합니다.

Action 생성된 트래픽 성형 규칙에 대하여 아래의 추가 옵션 작업을 수행할 수 있습니다.

- **Add** 트래픽 성형 규칙을 추가할 경우 클릭합니다.
- **Edit** 트래픽 성형 규칙을 수정합니다. 변경된 성형 규칙을 저장하려면 **Save** 버튼을 클릭합니다.
- **Del** 선택한 트래픽 성형 규칙을 제거합니다.

Chapter 6: ADVANCED

상단 ADVANCED 탭에서 고급 라우팅 및 무선, LED 신호 설정을 변경할 수 있습니다. ADVANCED 항목은 해당 분야의 고급 기술과 충분한 기술적 이해를 가진 사용자만 변경하시기 바랍니다. 잘못된 설정은 장치 및 유무선 네트워크 성능을 오히려 저하시킬 수 있습니다.

The screenshot shows the 'Advanced' configuration page in the HighLink web interface. The navigation tabs at the top are MAIN, WIRELESS, NETWORK, ADVANCED (selected), SERVICES, and SYSTEM. The user is logged in as 'UNMS' and has access to 'Tools' and 'Logout' options.

Advanced Wireless Settings

- RTS Threshold: [?] 2346 Off
- Distance: [?] 0.4 miles (0.6 km) Auto Adjust
- Aggregation: [?] 32 Frames 50000 Bytes Enable
- Multicast Data: [?] Allow
- Multicast Enhancement: [?] Enable
- Installer EIRP Control: [?] Enable
- Extra Reporting: [?] Enable
- Client Isolation: [?] Enable
- Sensitivity Threshold, dBm: [?] -96 Off

Advanced Ethernet Settings

- LAN0 Speed: [?] 10/100 Auto

Signal LED Thresholds

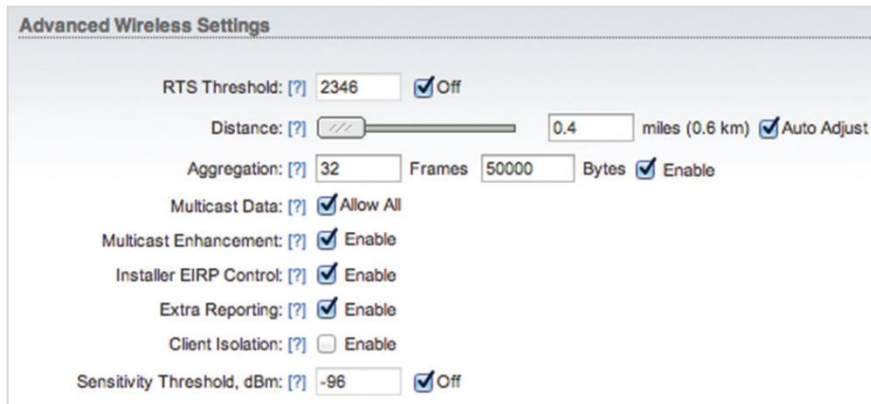
	LED1	LED2	LED3	LED4
Thresholds, dBm: [?]	-94	-80	-73	-65

A 'Change' button is located at the bottom right of the settings area.

Change 설정을 변경한 후 우측 하단의 **Change** 버튼을 클릭하여 변경된 사항을 적용합니다. Change 버튼을 클릭하면 우측 상단에 아래와 같은 3가지 옵션이 표시되며 다음과 같은 옵션 작업을 수행할 수 있습니다.

- **Apply** 버튼을 클릭하면 변경된 설정이 즉시 적용됩니다.
- **Test** 버튼을 클릭하면 변경된 사항을 저장하지 않고 테스트만 시도합니다. 180 초 이내에 Apply 버튼을 클릭하지 않으면 변경된 설정이 저장되지 않고 이전 설정으로 복구됩니다. Test 버튼을 클릭하면 180 초 동안 화면에 카운트다운이 표시됩니다.
- **Discard** 변경된 설정을 저장하지 않고 취소합니다.

Advanced Wireless Settings



RTS Threshold airMAX 기능을 설정하였을 경우 RTS Threshold 항목을 설정할 필요가 없습니다. RTS Threshold 기능을 사용하지 않을 경우 **Off** 박스를 체크합니다. 트래픽 흐름 제어를 위한 무선 전송 패킷 크기를 설정합니다. 패킷 크기는 0부터 2346 바이트 사이의 값을 설정할 수 있으며 기본값은 2346 바이트로 설정되어 있습니다. 기본값을 그대로 사용할 경우 RTS Threshold 기능을 사용하지 않는 것과 같습니다. 802.11 무선 네트워크 프로토콜은 히든 노드에 의해 발생하는 프레임 충돌을 감소시키기 위하여 802.11 무선 네트워킹 RTS(Request to Send) / CTS(Clear to Send) 메커니즘을 사용합니다. 무선 장치가 전송하려는 패킷 크기가 설정된 값보다 클 경우 RTS/CTS 제어 프레임을 사전에 교환한 후 데이터를 전송합니다. Station과 같은 무선 클라이언트 장치는 AP 장치로 RTS 프레임을 먼저 전송한 후 데이터 전송 허가를 위한 CTS 응답 프레임 수신을 대기합니다. 클라이언트 장치는 AP 장치로부터 CTS 프레임을 수신한 후에 데이터 패킷을 전송합니다. 특정 클라이언트 장치가 데이터를 전송하는 동안 다른 클라이언트 장치들은 AP 장치로 데이터를 전송할 수 없고 특정 클라이언트 장치가 데이터 전송을 완료할 때까지 대기합니다. 클라이언트 장치가 전송하려는 패킷 크기가 설정된 값보다 작거나 같을 경우에는 AP 장치로 RTS 프레임을 전송하지 않고 해당 데이터 패킷을 즉시 전송합니다.

Distance AP 장치와 Station 장치 사이의 거리를 슬라이더를 사용하여 설정하거나 직접 입력할 수 있습니다. 설정하는 거리에 따라 ACK 타임아웃 값이 자동으로 변경되며 무선 장치의 신호 강도 및 전송 속도도 자동으로 조정됩니다. 1개의 AP 장치에 여러 개의 Station 장치를 연결할 경우 가장 멀리 위치한 Station 장치를 기준으로 거리를 설정합니다.

Auto Adjust Station 장치는 AP 장치로 데이터 프레임을 전송할 때마다 AP 장치로부터 ACK 프레임 수신을 대기합니다. 만약 Station 장치가 설정된 타임아웃 시간동안 AP 장치로부터 ACK 프레임을 수신하지 못하면 Station 장치는 데이터 프레임을 AP 장치로 재전송합니다. ACK 타임아웃 시간이 너무 짧거나 길게 설정되어 데이터 프레임 재전송이 자주 발생하면 무선 네트워크 성능이 낮아질 수밖에 없습니다. M 시리즈 제품은 자동 ACK 타임아웃 알고리즘을 사용하여 타임아웃 시간을 실시간으로 최적화합니다. Auto Adjust 기능은 802.11n 기반의 장거리 링크를 연결할 때 유용하게 사용될 수 있습니다.

Aggregation 무선 장치가 여러 개의 다중 프레임을 1개의 대형 프레임으로 전송할 수 있도록 합니다. 무선 장치는 동일한 물리적 소스와 수신 장치, QoS 트래픽 클래스 속성을 가진 여러 개의 작은 프레임을 공통 MAC 헤더를 가진 1개의 대형 프레임으로 변환합니다. 슬라이더를 사용하여 대형 프레임으로 변환할 소형 프레임의 개수를 설정합니다.

- **Frames** 대형 프레임으로 변환할 프레임 개수를 입력합니다.
- **Bytes** 대형 프레임 크기를 바이트 단위로 입력합니다.
- **Enable** Aggregation 옵션을 사용할 경우 박스를 체크합니다.

Multicast Data 멀티캐스트 패킷 전송을 허용합니다.

Multicast Enhancement Access Point 및 AP-Repeater 모드에서만 설정할 수 있습니다. 클라이언트 장치들이 IGMP (Internet Group Management Protocol) 메시지를 전송하지 않으면 멀티캐스트 트래픽 수신자에 등록되지 않습니다. Multicast Enhancement 옵션은 IGMP snooping 기술을 사용하여 멀티캐스트 수신자에 등록되지 않은 클라이언트 장치들로부터 멀티캐스트 트래픽을 분리한 후 등록되어 있는 클라이언트 장치들로 멀티캐스트 트래픽을 고속으로 전송합니다. 따라서 Point to Multipoint 방식의 네트워크에서 트래픽 부하를 감소시킬 수 있으며 재전송 메커니즘을 통해 멀티캐스트 트래픽 전송의 신뢰성을 향상시킬 수 있습니다. 만약 클라이언트 장치들이 IGMP 메시지를 송신하지 않지만 멀티캐스트 트래픽을 수신해야 한다면 Multicast Enhancement 옵션을 사용하시기 바랍니다.



Installer EIRP Control Enable 박스를 체크하면 무선 송신 출력을 사용자가 변경할 수 있으며 상단 **WIRELESS** 탭에 포함된 **Calculate EIRP Limit** 설정에서 제어할 수 있습니다.

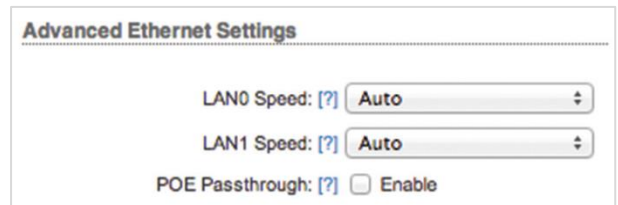
Extra Reporting Enable 박스를 체크하면 802.11 관리 프레임에 포함된 장치 이름과 같은 추가 정보를 제공합니다. 이러한 추가 정보는 시스템 식별 및 Discovery 유틸리티에서 상태 정보를 제공하고 라우터 운영체제에서 사용됩니다.

Client Isolation Access Point 및 AP-Repeater 모드에서만 사용할 수 있습니다. **Enable** 박스를 체크하면 동일한 AP 장치에 연결된 Station 장치 사이에 레이어2 MAC 또는 레이어3 IP 레벨의 데이터 통신을 할 수 없습니다. 클라이언트 장치는 AP 장치의 백본 네트워크에 연결된 장치들과만 데이터를 송수신할 수 있습니다.

Sensitivity Threshold, dBm AP 장치가 클라이언트 장치로부터 연결 요청 메시지를 수신하였을 때 연결을 허용할 수 있는 클라이언트 장치의 최소 신호 레벨을 dBm 단위로 입력합니다. AP 장치와 연결된 클라이언트 장치의 신호가 나중에 감소되어도 클라이언트 장치는 AP 장치에 계속 연결을 유지할 수 있습니다.

Advanced Ethernet Settings

LAN0/1 Speed 기본값 Auto 설정을 사용하면 유선랜 포트에 연결된 장치와 속도 및 이중모드와 같은 전송 파라미터를 자동으로 조정합니다. 자동 협상 과정에서 네트워크 장치들은 네트워크 사양 정보를 교환한 후 양측에서 공유할 수 있는 최고 전송 모드를 선택합니다. Auto 설정을 사용하지 않을 경우 속도 및 이중모드를 직접 선택할 수도 있습니다. RM5 제품은 **100 Mbps-Full, 100 Mbps-Half, 10 Mbps-Full, 10 Mbps-Half** 전송 모드를 지원합니다. 장치와 장치 사이에 100 미터를 초과하는 이더넷 케이블을 사용할 경우 10 Mbps 속도를 사용하는 것이 안정적입니다. Full-duplex 모드는 양방향 통신을 지원하며 송신과 수신을 동시에 처리할 수 있습니다. Half-duplex 모드는 양방향 통신을 지원하지 않지만 송신과 수신을 동시에 처리할 수 없고 한순간에 한방향으로만 데이터를 전송할 수 있습니다.



Signal LED Thresholds

각 필드에 설정된 값을 기반으로 수신한 무선 신호 레벨에 따라 장치에 부착된 LED 상태를 제어할 수 있습니다. 따라서 사용자는 무선 장치에 접속하지 않아도 LED 상태를 확인하면서 안테나 방향을 조정하거나 무선 연결 상태를 확인할 수 있습니다.

Signal GPS 기능을 지원하는 모델에서만 사용할 수 있으며 무선 또는 GPS 신호 타입을 설정합니다.

Thresholds, dBm 신호 강도가 설정된 값에 도달하면 해당 LED가 켜집니다. MAIN 탭에서 표시되는 신호 강도가 -63 dBm 값을 기준으로 조금씩 변화하면 4개의 LED에 대한 Threshold 값을 -70, -65, -62, -60 값으로 설정할 수 있습니다. '-' 문자는 입력 필드 외부에 위치해 있으며 필드 내부에 입력하지 않도록 주의하시기 바랍니다.

Chapter 7: SERVICES

Ping Watchdog, SNMP, 서버(웹, SSH, 텔넷), NTP, DDNS, 시스템 로그, 장치 탐색과 같은 시스템 관리 서비스를 설정합니다.

The screenshot displays the 'SERVICES' configuration page in the HighLink web interface. The navigation bar at the top includes 'MAIN', 'WIRELESS', 'NETWORK', 'ADVANCED', 'SERVICES', and 'SYSTEM'. The 'SERVICES' section is active, showing the following configurations:

- Network Management System:** UNMS is disabled. Key can be edited.
- Ping Watchdog:** Enabled. IP Address To Ping, Ping Interval (300 seconds), Startup Delay (300 seconds), Failure Count To Reboot (3), and Save Support Info are configured.
- SNMP Agent:** Enabled. SNMP Community is 'public'. Contact and Location fields are empty.
- Web Server:** Enabled. Secure Connection (HTTPS) is enabled. Secure Server Port is 443, Server Port is 80, and Session Timeout is 15 minutes.
- SSH Server:** Disabled. Server Port is 22. Password Authentication is enabled. Authorized Keys can be edited.
- Telnet Server:** Disabled. Server Port is 23.
- NTP Client:** Disabled. NTP Server is 0.ubnt.pool.ntp.org.
- Dynamic DNS:** Disabled. Service is dyndns.org. Host Name, User Name, and Password fields are empty.
- System Log:** System Log is enabled. Remote Log is disabled. Remote Log IP Address and Remote Log Port (514) are configured. TCP Protocol is disabled.
- Device Discovery:** Discovery and CDP are both enabled.

A 'Change' button is located at the bottom right of the configuration area.

Change 설정을 변경한 후 우측 하단의 **Change** 버튼을 클릭하여 변경된 사항을 적용합니다. Change 버튼을 클릭하면 우측 상단에 아래와 같은 3가지 옵션이 표시되며 다음과 같은 옵션 작업을 수행할 수 있습니다.

- **Apply** 버튼을 클릭하면 변경된 설정이 즉시 적용됩니다.
- **Test** 버튼을 클릭하면 변경된 사항을 저장하지 않고 테스트만 시도합니다. 180 초 이내에 Apply 버튼을 클릭하지 않으면 변경된 설정이 저장되지 않고 이전 설정으로 복구됩니다. Test 버튼을 클릭하면 180 초 동안 화면에 카운트다운이 표시됩니다.
- **Discard** 변경된 설정을 저장하지 않고 취소합니다.

Ping Watchdog

Ping Watchdog 기능은 원격 호스트 장치와의 연결 상태를 확인하기 위하여 사용자가 설정한 IP 주소로 Ping 테스트를 지속적으로 실행하고 응답이 오지 않으면 장치를 자동으로 재부팅합니다. 장치에 내장된 Ping 틀은 ICMP 에코 요청 패킷을 원격 호스트에 주기적으로 전송하고 ICMP 에코 응답 메시지의 수신을 대기합니다. 사용자가 설정한 개수 만큼 응답 메시지를 수신하지 못할 경우 무선 장치를 자동으로 재부팅합니다.

Ping Watchdog 기능을 사용할 경우 **Enable** 박스를 체크합니다.

IP Address To Ping 연결 상태를 모니터링 할 상대편 장치의 IP 주소를 입력합니다.

Ping Interval ICMP 에코 요청 메시지를 전송하는 시간 간격을 초 단위로 입력합니다. 기본값 300초

Startup Delay 부팅 완료 후 첫번째 Ping 메시지를 전송하는 시점까지의 대기 시간을 입력합니다. 네트워크 인터페이스 및 무선 연결에 소요되는 시간을 감안하여 최소 60초 이상의 값을 설정해야 합니다.

Failure Count to Reboot 입력한 개수만큼 Ping 응답 메시지를 연속하여 수신하지 못하면 자동으로 재부팅됩니다.

Save Support Info 체크할 경우 Ping Watchdog 에 의해 장치를 재부팅할 때 지원 정보 파일을 생성합니다.

SNMP Agent

SNMP (Simple Network Management Protocol)는 어플리케이션 레이어 프로토콜로서 네트워크 장치 사이에 관리 정보를 교환하는데 사용됩니다. 네트워크 관리자는 SNMP를 사용하여 네트워크에 연결된 장치들을 모니터링하고 제어할 수 있습니다. SNMP 에이전트를 내장한 장치는 장치 관리에 사용되는 네트워크 인터페이스를 제공하고 SNMP 관리 어플리케이션과 통신합니다. 네트워크 관리자는 네트워크 성능을 모니터링하거나 네트워크 문제를 해결하는데 SNMP 프로토콜을 사용할 수 있습니다. 장치 식별 정보 및 연락처, 위치 정보를 SNMP 에이전트에 설정합니다.

SNMP Agent SNMP 에이전트 기능을 사용할 경우 **Enable** 박스를 체크합니다.

SNMP Community MIB(Management Information Base) 객체 접근 인증에 필요하고 임베디드 패스워드로 사용되는 SNMP 커뮤니티 문자열을 입력합니다. RM5 장치는 읽기 전용 커뮤니티 문자열을 지원하며 인증된 관리 스테이션은 커뮤니티 문자열을 제외한 모든 MIB 객체에 대한 읽기 권한을 가지게 됩니다. RM5 장치는 SNMP v1 버전을 지원합니다.

Contact 긴급 상황에서 연락 받을 연락처 이름을 입력합니다.

Location 장치를 설치한 위치 정보를 입력합니다.

Web Server

웹 서버 파라미터를 관리합니다.

Web Server HTTP 서비스를 사용할 경우 **Enable** 박스를 체크합니다.

Secure Connection (HTTPS) HTTPS 보안 모드를 사용할 경우 체크합니다.

- **Secure Server Port** HTTPS 보안 모드를 사용할 경우 웹 서버의 TCP/IP 포트 번호를 입력합니다. 기본값 443

Server Port HTTP 모드를 사용할 경우 웹 서버의 TCP/IP 포트 번호를 입력합니다. 기본값 80

Session Timeout 최대 세션 종료 시간을 설정합니다. 세션이 종료되면 아이디와 패스워드를 재입력 후 로그인해야 합니다.

SSH Server

SSH 서버 파라미터를 설정합니다.

SSH Server SSH 접속을 사용할 경우 **Enable** 박스를 체크합니다.

Server Port SSH 서버의 TCP/IP 포트 접속 번호를 입력합니다. 기본값 22

Password Authentication **Enable** 박스를 체크할 경우 관리자 자격증명을 사용하여 접속합니다. 체크하지 않으면 인증 키를 사용해야 합니다.

Authorized Keys 관리자 패스워드 대신 공인키 파일을 사용하여 접속할 경우 **Edit** 버튼을 클릭합니다. Edit 버튼 클릭하면 다음과 같은 화면이 표시됩니다.

SSH Server

SSH Server: Enable

Server Port:

Password Authentication: Enable

Authorized Keys:

SSH Authorized Keys

Import Public Key File: No file chosen

Enabled	Type	Key	Comment	Action
<input type="button" value="Save"/> <input type="button" value="Close"/>				

- **Choose File** 신규 키 파일 위치를 탐색하여 선택합니다. 파일을 선택한 후 **Open** 버튼을 클릭합니다.
- **Import** SSH 접속을 위한 파일을 등록합니다.
- **Enabled** 특정 키 파일을 사용할 경우 선택합니다. 추가된 모든 키 파일은 시스템 설정 파일에 저장되고 선택한 키 파일만 장치에서 사용됩니다.
- **Type** 키 타입을 표시합니다.
- **Key** 키를 표시합니다.
- **Comment** 키에 대한 설명을 입력할 수 있습니다.
- **Action** 등록된 키 파일에 대하여 다음과 같은 작업을 수행할 수 있습니다.
 - **Remove** 등록된 공인키 파일을 삭제합니다.
- 변경된 설정을 저장하려면 **Save** 버튼을 클릭하고 취소하려면 **Close** 버튼을 클릭합니다.

Telnet Server

텔넷 서버 파라미터를 설정합니다.

Telnet Server 장치에 텔넷 접속을 허용할 경우 **Enable** 박스를 체크합니다.

Server Port 텔넷 서버 접속에 사용되는 TCP/IP 포트 번호를 입력합니다. 기본값 23

Telnet Server

Telnet Server: Enable

Server Port:

NTP Client

NTP (Network Time Protocol) 프로토콜은 데이터 네트워크를 통해 시스템 시간을 동기화합니다. System Log 기능을 사용할 경우 설정된 시스템 시간 다음에 시스템 이벤트 로그가 등록됩니다.

NTP Client **Enable** 박스를 체크할 경우 인터넷 타입의 서버를 통해 장치의 시스템 시간을 설정합니다.

NTP Server NTP 서버의 IP 주소나 도메인 이름을 입력합니다.

NTP Client

NTP Client: Enable

NTP Server:

Dynamic DNS

DNS(Domain Name System)은 도메인 이름을 IP 주소로 변환하며 인터넷에 연결된 각각의 DNS 서버는 이러한 매핑 정보를 데이터 베이스에 저장하고 있습니다. 다이나믹 DNS는 실시간으로 장치의 IP 주소를 확인해 주는 서비스입니다. 장치의 IP 주소가 변경되어 도 도메인 이름을 통해 IP 주소를 확인하고 접속할 수 있습니다.

Dynamic DNS DDNS 서버와 장치를 연동할 경우 체크합니다.

Service 리스트에서 DDNS 서비스를 선택합니다.

DDNS 서비스 목록: dynnds.org changeip.com zoneedit.com free.edit.com no-ip.com noip.com freedns.afraid.org he.net easydns.com dnsmax.com thatip.com dnsdynamic.org dnsexit.com ovh.com dnsomatic.com 3322.org namecheap.com

Host Name DDNS 서버에 업데이트되는 장치의 호스트 이름을 입력합니다. 예: sample.ddns.com

Username DDNS 계정의 사용자 이름을 입력합니다.

Password DDNS 계정의 비밀번호를 입력합니다.

Show 입력한 비밀번호를 확인할 경우 클릭합니다.

System Log

모든 로그 메시지에는 시스템 시간과 함께 이벤트를 발생시킨 특정 서비스 이름이 포함되어 있습니다. 서비스 종류에 따라 로그 메시지 형태가 다르고 정보 레벨도 차이가 있습니다. 일반적으로 에러, 경고, 시스템 서비스 메시지가 제공되며 보다 상세한 디버그 레벨 메시지도 제공됩니다. 상세한 시스템 메시지를 표시할 경우 전체 로그 메시지 크기가 커집니다.

System Log 체크하면 시스템 로그 (syslog) 메시지 루틴을 실행합니다.

Remote Log syslog 메시지를 원격 서버에 전송할 경우 체크합니다.

Remote Log IP Address syslog 메시지를 수신하는 서버의 IP 주소를 입력합니다. 서버는 syslog 프로토콜을 지원해야 합니다.

Remote Log Port syslog 메시지를 수신하는 서버의 TCP/IP 포트 번호를 입력합니다. 기본값 514

TCP Protocol 체크하면 TCP 프로토콜을 사용하여 시스템 로그 메시지를 전송합니다.

Device Discovery

장치 검색에 사용되는 파라미터를 설정합니다.

Discovery 장치 검색 툴을 사용하여 장치를 검색할 경우 체크합니다. 장치 검색 툴은 support@highlink.co.kr 이메일로 요청하시면 제공해 드립니다.

CDP 장치 정보를 공유하기 위해 Cisco Discovery Protocol을 사용하여 CDP 패킷을 전송할 경우 체크합니다.

Chapter 8: SYSTEM

System 페이지는 다양한 관리자 옵션을 제공합니다. 장치를 재부팅 하거나 초기값으로 리셋할 수 있으며 펌웨어 업데이트, 설정 저장 및 복구, 관리자 계정 등을 수정합니다.

The screenshot shows the 'SYSTEM' configuration page with the following sections and controls:

- Firmware Update:** Firmware Version: XW.v6.1.8, Build Number: 32774. Upload Firmware: 파일 선택 (선택된 파일 없음). Check for Updates: Enable, Check Now button.
- Device:** Device Name: RMS, Interface Language: English.
- Date Settings:** Time Zone: (GMT-12:00) International, Startup Date: Enable, Startup Date: [calendar icon].
- System Accounts:** Administrator User Name: ubnt, Read-Only Account: Enable.
- Miscellaneous:** Reset Button: [?] Enable.
- Location:** Latitude: [input], Longitude: [input].
- Device Maintenance:** Reboot Device: Reboot..., Support Info: Download...
- Configuration Management:** Back Up Configuration: Download..., Upload Configuration: 파일 선택 (선택된 파일 없음), Reset to Factory Defaults: Reset....

A 'Change' button is located at the bottom right of the configuration area.

Change 설정을 변경한 후 우측 하단의 **Change** 버튼을 클릭하여 변경된 사항을 적용합니다. Change 버튼을 클릭하면 우측 상단에 아래와 같은 3가지 옵션이 표시되며 다음과 같은 옵션 작업을 수행할 수 있습니다.

- **Apply** 버튼을 클릭하면 변경된 설정이 즉시 적용됩니다.
- **Test** 버튼을 클릭하면 변경된 사항을 저장하지 않고 테스트만 시도합니다. 180 초 이내에 Apply 버튼을 클릭하지 않으면 변경된 설정이 저장되지 않고 이전 설정으로 복구됩니다. Test 버튼을 클릭하면 180 초 동안 화면에 카운트다운이 표시됩니다.
- **Discard** 변경된 설정을 저장하지 않고 취소합니다.

Firmware Update

장치 펌웨어를 업데이트 합니다. 펌웨어 업데이트 후 기존 설정이 변경되지 않지만 펌웨어 업데이트 전에 현재 설정을 저장해 두실 것을 권장합니다.

Firmware Version 현재 탑재된 펌웨어 버전을 표시합니다.

Build Number 펌웨어 버전의 빌드넘버를 표시합니다.

Check for Updates Enable 박스를 체크하면 자동으로 펌웨어 업데이트 여부를 확인합니다.

Check Now 버튼을 클릭하면 수동으로 펌웨어 업데이트 여부를 확인합니다. 신규 업데이트가 검색될 경우 **Download** 버튼을 클릭하여 최신 펌웨어 파일을 PC에 다운로드하고 취소할 경우 **Dismiss** 버튼을 클릭합니다.

Upload Firmware PC에 다운로드한 최신 펌웨어 파일을 **Choose File** 버튼을 사용하여 선택한 후 **Open** 버튼을 클릭합니다. 장치에 업로드된 펌웨어 파일 버전이 표시되고 다음과 같은 두가지 옵션 작업을 수행할 수 있습니다.

- **Update** 클릭하여 펌웨어 업데이트를 시작합니다. 장치가 재부팅 된 후 펌웨어 업데이트 프로세스가 완료됩니다.
- **Discard** 펌웨어 업데이트를 취소합니다.

펌웨어 업데이트가 진행되는 동안 펌웨어 업데이트 창을 닫을 수 있지만 업데이트 작업이 취소되는 것은 아닙니다. 펌웨어 업데이트 작업은 3~7분 정도가 소요됩니다. 업데이트가 진행되는 동안에는 장치에 접속할 수 없습니다.

주의: 펌웨어 업데이트 프로세스가 진행되는 동안 전원이 꺼지지 않도록 주의하시기 바랍니다. 업데이트 중간에 전원이 차단될 경우 치명적인 시스템 손상이 발생합니다.

Device

장치 이름 또는 호스트 이름은 주로 네트워크에서 장치를 식별하는데 사용되며 SNMP 에이전트는 장치 이름을 인증된 관리 스테이션에 전달합니다. 또한 장치 이름은 일반적인 라우터 운영 시스템, 등록 스크린, 탐색 툴에서도 사용됩니다.

Device Name 장치 이름 또는 호스트 이름을 입력합니다.

Interface Language 웹에서 사용되는 언어를 선택합니다.

Date Settings

Time Zone 그리니치 표준시 (GMT) 시각대를 선택합니다.

Startup Date Enable 박스를 클릭하면 부팅 후 장치 동작이 시작되는 날짜를 설정할 수 있습니다. **달력 모양의 아이콘**을 클릭하여 날짜를 선택합니다.

System Accounts

허가받지 않는 사용자가 장치에 접속하여 설정을 변경할 수 없도록 관리자 아이디와 비밀번호를 변경합니다. 최초 장치를 설정하실 때 비밀번호를 변경하시기 바랍니다.

Administrator User Name 관리자 아이디를 입력합니다.

열쇠 아이콘 관리자 계정의 비밀번호를 변경하려면 열쇠 모양의 아이콘을 클릭합니다.

- **Current Password** 현재 사용 중인 관리자 비밀번호를 입력합니다. 비밀번호나 아이디를 변경할 경우 관리자 확인을 위해 현재의 비밀번호를 입력해야 합니다.
- **New Password** 관리자 계정의 신규 비밀번호를 입력합니다. 비밀번호는 4~63 문자 이내로 설정할 수 있으며 최소 8자 이상의 값을 설정하시기 바랍니다. 사용자가 입력한 비밀번호의 길이가 4자 미만일 경우 Too short (갈색) 메시지를 표시합니다. 또한 입력한 비밀번호의 보안 레벨을 Weak(갈색), Normal(주황색), Strong(녹색) 단계로 표시합니다.
- **Verify New Password** 입력한 신규 비밀번호 확인을 위해 신규 비밀번호를 다시 입력합니다.

Read-Only Account Enable 박스를 체크하면 읽기 전용 계정을 생성합니다. 읽기 전용 계정은 장치의 설정 상태를 변경하지 못하고 MAIN 페이지에서 설정 상태만 확인할 수 있습니다.

- **Read-Only Account Name** 읽기 전용 계정 이름을 입력합니다.
- **열쇠 아이콘** 클릭하면 읽기 전용 계정의 비밀번호를 변경합니다.
 - **New Password** 신규 비밀번호를 입력합니다.
 - **Show** 체크하면 입력한 비밀 번호를 표시합니다.

Miscellaneous

Reset Button 원격 PoE 스위치 및 아답터에서 장치를 초기화하는 기능을 사용할 경우 **Enable** 박스를 체크합니다. System 페이지의 **Reset to Factory Defaults** 메뉴에서도 장치 설정을 초기화할 수 있습니다.

UNII-2 Band DFS(Dynamic Frequency Selection) 주파수 대역을 사용하도록 설정합니다.

Location

장치가 설치된 위도 및 경도 위치를 입력합니다.

Latitude -90 ~ +90 사이의 위도 값을 입력합니다.

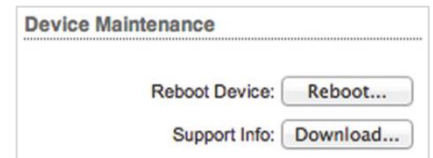
Longitude -180 ~ +180 사이의 경도 값을 입력합니다.

Device Maintenance

장치를 재부팅하거나 기술지원에 사용되는 정보 파일을 다운로드합니다.

Reboot Device 전원 OFF/ON 처럼 **Reboot** 버튼을 클릭하면 장치를 재부팅합니다.

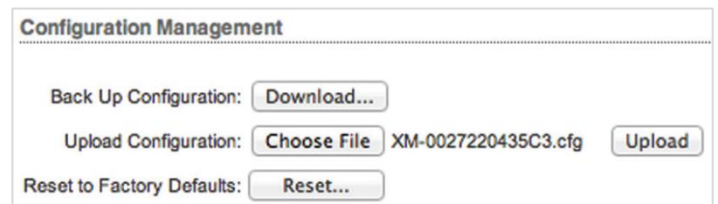
Support Info 기술 지원 시 엔지니어가 요청할 경우 **Download** 버튼을 클릭하여 지원 정보 파일을 PC에 다운로드 합니다.



Configuration Management

장치 설정 상태를 cfg 파일로 다운로드하거나 PC에 저장된 설정 파일을 장치에 업로드하여 설정을 복구합니다. 또한 설정 상태를 공장 출하 시 초기 상태로 리셋할 수 있습니다.

Back Up Configuration 현재의 시스템 설정 상태를 PC에 파일로 저장하려면 **Download** 버튼을 클릭합니다. 설정 파일은 WPA2 인증키와 같은 중요한 내용을 포함하고 있기 때문에 보안상 안전한 곳에 보관하시기 바랍니다.



Upload Configuration PC에 저장되어 있는 설정 파일을 장치에 업로드하여 설정을 복구합니다. **Choose File** 버튼을 클릭하여 설정 파일이 저장되어 있는 위치로 이동한 후 설정 파일을 선택하고 **Open** 버튼을 클릭합니다. 현재 설정 상태로 다시 복구할 필요가 있을 경우 현재의 설정 상태를 미리 저장하시기 바랍니다.

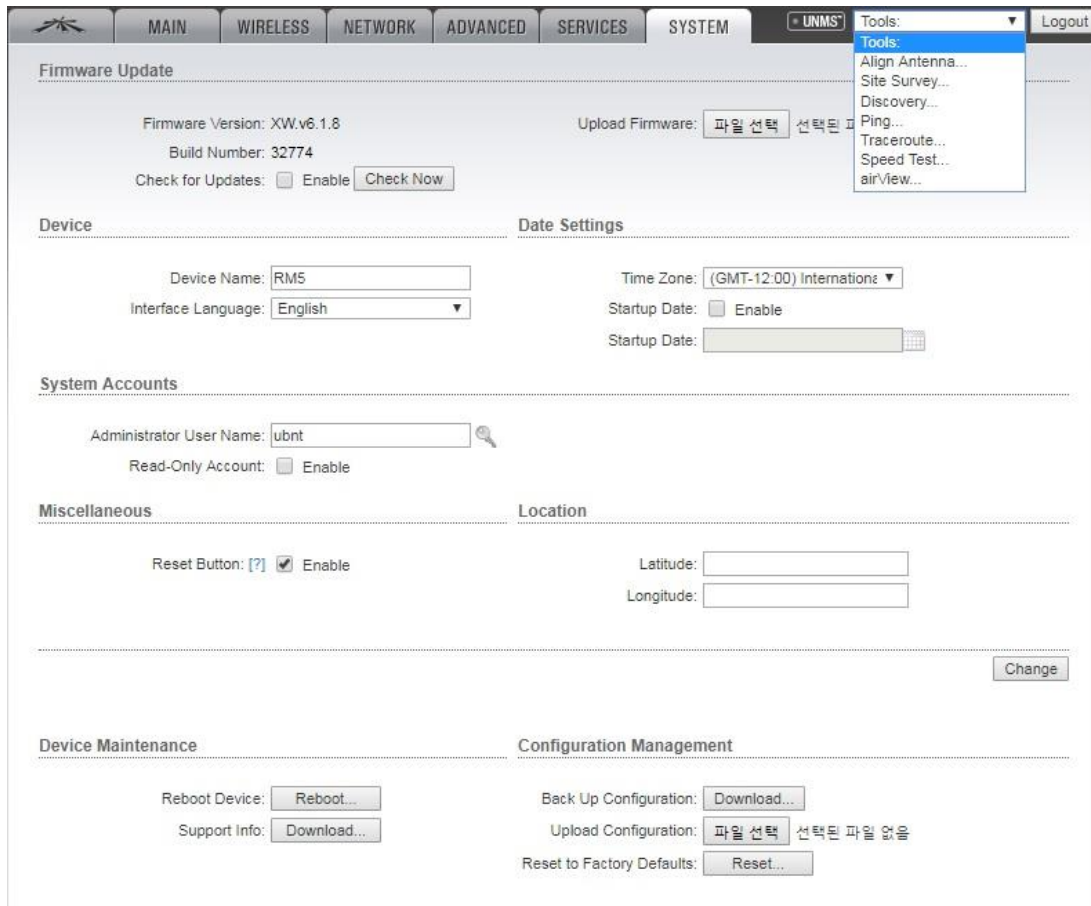
업로드할 설정 파일이 표시되고 다음과 같은 두가지 작업을 수행할 수 있습니다.

- **Apply** 선택한 설정 파일을 업로드하려면 Apply 버튼을 클릭합니다. 설정 파일 업로드가 완료되면 장치가 자동으로 재부팅하며 변경된 설정을 웹 페이지에서 확인하시기 바랍니다.
- **Discard** 설정 변경을 취소합니다.

Reset to Factory Defaults 장치 설정 상태를 공장 출하 시 초기값으로 변경하려면 **Reset** 버튼을 클릭합니다. 초기화가 적용되면 장치가 자동으로 재부팅되며 모든 설정값이 초기화됩니다. 초기화 진행 전에 현재의 설정값을 저장하시길 권장합니다.

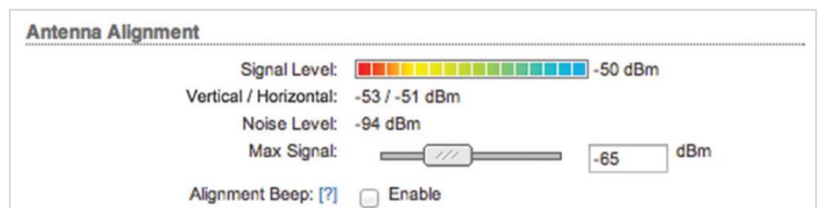
Chapter 9: Tools

웹 페이지 우측 상단에 Tools 페이지로 연결되는 링크를 제공합니다.



Align Antenna

지향성 안테나를 사용할 경우 최상의 신호 품질로 링크될 수 있도록 안테나 위치 및 방향을 조정합니다. 표시되는 신호 레벨은 1초마다 갱신됩니다.



Signal Level 마지막으로 수신한 무선 패킷의 신호 강도를 표시합니다. 붉은색 색상은 가장 약한 신호 레벨을 나타내고 파란색 색상은 가장 강한 신호 레벨을 나타냅니다.

Vertical / Horizontal 1개 이상의 편파가 사용될 경우 각 편파의 무선 신호 레벨을 dBm 단위로 표시합니다.

Noise Level 무선 신호를 수신할 때 백그라운드 노이즈 레벨을 dBm 단위로 표시합니다.

Max Signal 최대 신호 강도를 dBm 단위로 표시합니다. 변동되는 신호에 민감하게 반응할 수 있도록 슬라이더를 사용하여 Signal Level 계측 범위를 조정할 수 있습니다. 슬라이더는 최대 계기 값의 오프셋을 변경합니다.

Alignment Beep 소리를 통해 안테나 방향을 조정할 수 있습니다. 음이 높아질수록 강한 신호를 나타냅니다.

Site Survey

Site Survey 톨은 무선 장치가 지원하는 모든 주파수 대역의 무선 네트워크를 검색합니다.

Site Survey

Scanned Frequencies:

5.735GHz 5.74GHz 5.745GHz 5.75GHz 5.755GHz 5.76GHz 5.765GHz 5.77GHz 5.775GHz 5.78GHz 5.785GHz 5.79GHz 5.795GHz 5.8GHz 5.805GHz 5.81GHz 5.815GHz 5.82GHz 5.825GHz 5.83GHz 5.835GHz 5.84GHz

MAC Address	SSID	Device Name	Radio Mode	Encryption	Signal / Noise, dBm	Frequency, GHz / Channel
00:27:22:9C:DB:55	ubnt	RM5	802.11n	NONE	-73 / -91	5.755 / 151
DE:9F:DB:1B:BE:5E	UBNT-Guest		802.11n	NONE	-65 / -93	5.825 / 165
B8:C7:5D:06:6F:55	Grimm		802.11n	WPA2	-89 / -91	5.785 / 157
DC:9F:DB:1B:BE:5E	UBNT-OC		802.11n	WPA	-65 / -93	5.825 / 165

Scan

Scanned Frequencies 스캔한 주파수 리스트를 표시합니다. Station 모드를 사용할 경우 스캔할 주파수 리스트를 선택할 수 있습니다. 28 페이지 **Frequency Scan List, MHz** 항목을 참고하시기 바랍니다.

MAC Address 무선 장치의 MAC 주소를 표시합니다.

SSID 무선 네트워크 이름을 표시합니다.

Device Name 호스트 이름 또는 장치 식별 이름을 표시합니다.

Radio Mode 장치에서 사용되는 무선 기술을 표시합니다. airMAX 장치는 airMAX 로 표시됩니다.

Encryption 사용되는 암호화 방식을 표시합니다.

Signal/Noise, dBm 신호 강도와 노이즈 값을 표시합니다.

Frequency, GHz 장치에서 사용되는 주파수를 표시합니다.

Scan 사이트 검색 결과를 다시 업데이트 할 경우 Scan 버튼을 클릭합니다.

Discovery

네트워크에 연결되어 있는 모든 RM5 장치를 검색합니다. 검색 후 다음과 같은 정보를 표시합니다.

Device Discovery

Search:

MAC Address	Device Name	Mode	SSID	Product	Firmware	IP Address
00:27:22:60:07:12	UVC Dome	STA		UVC Dome	v3.1	192.168.25.172
00:27:22:60:06:9E	UVC Dome	STA		UVC Dome	v3.1	192.168.25.220
00:15:6D:5A:02:07	NanoBeamM5 19	AP	UBNT	NanoBeamM5 19	v5.5-beta6	192.168.25.1
00:27:22:60:00:12	UBNT	STA		AC	v1.0	192.168.25.147
00:27:22:60:00:02	UBNT	STA		AC	v1.0	192.168.25.160

Showing 1 to 5 of 5 entries

<< < 1 > >>

Scan

Search 키워드를 입력하면 자동으로 필터링하여 검색된 장치를 표시합니다.

MAC Address 장치의 MAC 주소나 하드웨어 식별자를 표시합니다.

Device Name 호스트 이름이나 장치 식별자 이름을 표시합니다.

Mode 무선 장치의 AP 또는 STA(스테이션) 동작 모드를 표시합니다.

SSID 무선 네트워크 이름을 표시합니다.

Product 제품 모델명을 표시합니다.

Firmware 장치의 펌웨어 버전을 표시합니다.


IP Address 장치의 IP 주소를 표시합니다. 웹 인터페이스를 통해 해당 장치에 접속하려면 IP 주소를 클릭합니다.

Scan 장치 검색 결과를 다시 업데이트 할 경우 Scan 버튼을 클릭합니다.

Ping

다른 장치로 Ping 테스트 메시지를 전송하여 네트워크 연결 상태를 확인할 수 있습니다. Ping 툴은 ICMP(Internet Control message Protocol) 패킷을 사용하여 링크 품질과 네트워크 장치 사이의 전송 지연을 확인하는데 사용됩니다.


Network Ping

Select Destination IP:  Packet Count: 5

Packet Size: 56

Host	Time	TTL
0 of 0 packets received, 0% loss		
Min: 0 ms		Max: 0 ms
Avg: 0 ms		

Select Destination IP 두가지 옵션을 사용할 수 있습니다.

- 자동으로 생성된 리스트에서 Ping 메시지를 전송할 원격 시스템의 IP를 선택합니다. 우측에 위치한  버튼을 클릭하면 원격 시스템의 IP 주소가 업데이트 됩니다.
- **specify manually** 를 선택한 후 아래에 위치한 입력란에 IP 주소를 직접 입력합니다.

Packet Count Ping 테스트에서 전송할 패킷 개수를 입력합니다.

Packet Size 패킷 크기를 입력합니다.

Start 버튼을 클릭하면 테스트를 시작합니다.

테스트가 완료되면 전송된 패킷에 대하여 아래와 같은 정보가 표시됩니다.

Host 원격 호스트 시스템의 IP 주소를 표시합니다.

Time ms 단위로 왕복 송수신 시간을 표시합니다.

TTL 데이터 유효 시간 (TTL: Time To Live)을 표시하며 Ping 테스트가 실패하기 전까지의 홉 카운트 값을 표시합니다.

Packets Received 수신한 총 패킷 개수를 표시합니다.

RESULTS 테스트 결과에 따라 패킷 손실 수치 및 왕복 송수신 시간을 표시합니다.

Loss 패킷 손실률을 표시합니다.

Min 최소 왕복 송수신 시간을 ms 단위로 표시합니다.

Avg 평균 왕복 송수신 시간을 ms 단위로 표시합니다.

Max 최대 왕복 송수신 시간을 ms 단위로 표시합니다.

Traceroute

장치로부터 지정한 호스트 이름이나 IP 주소를 가진 장치까지의 홉을 추적합니다. Traceroute 툴은 ICMP 패킷을 전송하여 라우팅 경로를 확인합니다.

Network Traceroute

Destination Host: Resolve IP Addresses

#	Host	IP	Responses

Destination Host 경로를 추적할 대상 장치의 호스트 이름이나 IP 주소를 입력합니다.

Resolve IP Addresses 옵션을 체크하면 홉 IP 주소를 숫자 형태가 아닌 상징적인 형태로 표시합니다.

Start 버튼을 클릭하면 테스트를 시작합니다.

테스트가 완료되면 각각의 홉에 대하여 아래와 같은 정보가 표시됩니다.

홉 번호를 표시합니다.

Host 홉 호스트의 이름, 식별자 또는 IP 주소를 표시합니다.

IP 홉 호스트의 IP 주소를 표시합니다.

Responses 무선 장치에서 테스트 장치까지의 왕복 송수신 시간을 표시합니다. 홉마다 패킷이 3회 전송되기 때문에 3개의 왕복 송수신 시간이 표시됩니다. 홉 호스트로부터 5초 타임아웃 시간동안 응답이 없을 경우 "*" 문자가 표시됩니다.

Speed Test

2개의 RM5 장치 사이에 무선 연결 속도를 테스트합니다. Speed Test 툴을 사용하여 두 네트워크 장치 사이의 실제 데이터 송수신 속도를 확인할 수 있습니다. 2개의 장치에서 트래픽 성형 기능을 사용할 경우 테스트 결과가 제한될 수 있습니다.

Network Speed Test

Select Destination IP:

User:

Password:

Remote WEB Port:

Show Advanced Options

Direction:

Duration: seconds

Test Results


RX: N/A

TX: N/A

Total: N/A

Warning! If traffic shaping is enabled on either device the speed test results will be limited accordingly.

Select Destination IP 2가지 입력 옵션을 제공합니다.

- 자동으로 생성된 리스트에서 원격 시스템의 IP 를 선택합니다. 우측에 위치한  버튼을 클릭하면 원격 시스템의 IP 주소가 업데이트 됩니다.
- **specify manually** 를 선택한 후 아래에 위치한 입력란에 IP 주소를 직접 입력합니다.

User 원격 RM5 장치의 관리자 아이디를 입력합니다.

Password 원격 RM5 장치의 관리자 비밀번호를 입력합니다.

Remote WEB port TCP/IP 기반의 속도 테스트를 연결할 원격 RM5 장치의 웹 포트 번호를 입력합니다. 예를 들어 원격 RM5 장치가 HTTPS 기술을 사용할 경우 443 포트 번호를 입력하고 HTTP 기술을 사용할 경우 80번 포트를 입력합니다.

Show Advanced Options 추가적인 속도 테스트 옵션을 설정할 경우 체크합니다.

Direction 아래의 3가지 모드 중 1가지를 선택합니다.

- **duplex** 수신(RX) 및 송신(TX) 속도를 동시에 테스트합니다.
- **receive** 수신(RX) 속도만 테스트합니다.
- **transmit** 송신(TX) 속도만 테스트합니다.

Duration 테스트 지속 시간을 초 단위로 설정합니다. 기본값 30초

Run Test 버튼을 클릭하면 테스트를 시작합니다.

테스트가 완료되면 다음과 같은 정보가 표시됩니다.

RX 평균 수신 속도를 표시합니다.

TX 평균 송신 속도를 표시합니다.

Total 총 송수신 속도를 표시합니다.

airView

스펙트럼 분석 기능을 제공합니다. 주파수 대역별로 노이즈 신호를 확인한 후 간섭을 최소화 하도록 무선 네트워크를 설계하여 RF 성능을 최적화 할 수 있습니다. airView 툴은 상단 좌측 로고 탭의 **airView** 항목에서도 실행할 수 있습니다. 자세한 사용법은 20 페이지 airView 항목을 참고하시기 바랍니다.

견적/기술 문의 연락처

주식회사 하이링크

경기도 용인시 기흥구 흥덕1로 13 흥덕아이티밸리 콤플렉스동 516호 (ZIP 16954)

TEL: 031-8065-6994

E-mail: support@highlink.co.kr