DIVA-IAP-AX

IEEE802.11a/b/g/n/ac/ax 무선랜 표준

2.4/5GHz 무선랜 동시 지원

Access Point (Multiple SSIDs)

Ethernet to Wi-Fi Bridge

L2 Transparent Bridge

802.11s Mesh Point

2x2 MIMO Antenna (SMA Female)

35mm 딘레일, 벽면 장착

IEEE802.1at/af PoE 전원

9-30V DC 전원

A급 기기

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며
가정 외의 지역에서 사용하는 것을 목적으로 합니다.

목차

Chapter 1: 개요

기능

DIVA-IAP-AX 제품을 구매해 주셔서 감사합니다. DIVA-IAP-AX 제품은 다양한 산업 현장에서 무선랜 액세스 포인트, 무선 클라이언트(이더넷 브리지), 매쉬 포인트, 무선랜 검색 기능을 사용할 수 있도록 설계되어 있습니다.

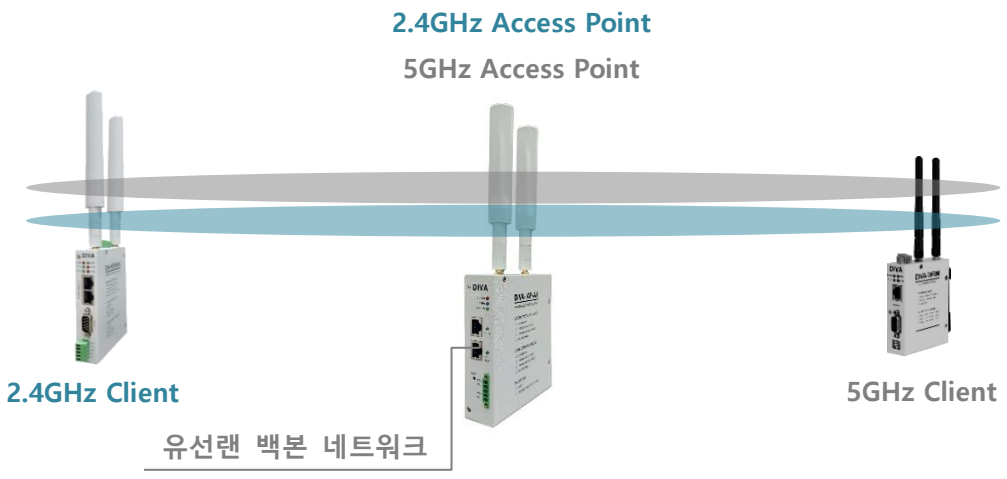
무선랜 액세스 포인트 기능은 기가비트 유선랜 포트에 연결된 백본 유선랜 네트워크와 IEEE 802.11a/b/g/n/ac/ax 무선랜 네트워크를 연결합니다. 액세스 포인트 모드로 동작하는 DIVA-IAP-AX 장치는 무선랜 네트워크에서 호스트 장치로 동작합니다. 따라서 표준 무선랜 클라이언트 모드로 동작하는 스마트 폰 및 노트북 컴퓨터, DIVA-IAP-AX, DIVA-AXP, DIVA-WRM, DIVA-WRM2 장치 등을 연결할 수 있습니다.

무선 클라이언트(이더넷 브리지) 기능은 기가비트 유선랜 포트에 연결된 이더넷 장치를 IEEE 802.11a/b/g/n/ac/ax 무선랜 네트워크에 연결합니다. DIVA-IAP-AX 장치는 Access Point 장치에 연결 시 무선랜 클라이언트 모드로 동작하며 유선랜 포트에 이더넷 스위치를 연결하여 여러 개의 장치를 무선랜 네트워크에 연결할 수 있습니다.

DIVA-IAP-AX 제품은 2.4GHz 무선랜 인터페이스와 5GHz 무선랜 인터페이스를 동시에 사용할 수 있습니다. 각각의 무선랜 인터페이스는 독립적인 동작 모드와 보안 방식을 지원합니다. 각각의 무선랜 인터페이스와 유선랜 인터페이스를 아래와 같이 설정하여 네트워크를 구성할 수 있습니다.

매쉬 포인트 기능은 802.11s 표준 프로토콜을 통해 무선 네트워크를 손쉽게 자동으로 연결하고 유선랜 포트에 연결된 장치들을 단일 네트워크로 연결합니다. 1개의 무선랜 인터페이스는 Mesh Point 용도로 사용하고 나머지 1개의 무선랜 인터페이스는 Access Point 모드로 사용하여 표준 와이파이 무선랜 장치들도 연결할 수 있습니다.

- **Dual Access Point 모드**
  2개의 무선랜 인터페이스를 모두 액세스 포인트 모드로 설정하여 2.4GHz 무선랜 네트워크와 5GHz 무선랜 네트워크를 구성합니다. 2개의 무선랜 인터페이스에 동일한 SSID 와 보안 방식을 설정하면 2.4GHz 무선랜과 5GHz 무선랜을 단일 무선 네트워크로 통합합니다.



- **Access Point (WDS), Client (WDS) 모드**

  Access Point (WDS) 와 Client (WDS) 모드로 동작하는 DIVA-IAP-AX 장치 사이에 MAC 주소를 이용한 연결 방식을 사용합니다. DIVA-IAP-AX 장치의 유선랜 포트에 연결된 장치들은 장치 유의 MAC 주소와 IP 주소를 기반으로 식별되고 데이터를 송수신합니다. WDS 방식은 PROFINET 장치와 같이 MAC 주소 기반의 통신 장비를 연결합니다.

DIVA-IAP-AX #1
Access Point (WDS) mode
IP 주소 192.168.1.1
MAC 주소 11:11:11:11:11:11

DIVA-IAP-AX #2
Client (WDS) mode
IP 주소 192.168.1.2
MAC 주소 22:22:22:22:22:22

PLC
유선랜 전용 장치
IP 주소 192.168.1.3
MAC 주소 33:33:33:33:33:33

ARP 테이블 정보

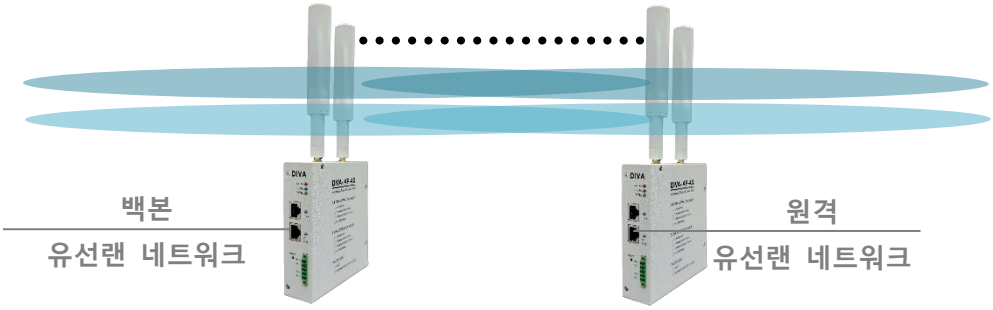
WDS 모드 사용 시	WDS 모드 미사용 시
192.168.1.1 - 11:11:11:11:11:11	192.168.1.1 - 11:11:11:11:11:11
192.168.1.2 - 22:22:22:22:22:22	192.168.1.2 - 22:22:22:22:22:22
192.168.1.3 - 33:33:33:33:33:33	192.168.1.3 - 22:22:22:22:22:22

- **Virtual Access Point 모드**

  각각의 무선랜 인터페이스에 최대 8개의 Virtual Access Point 모드를 등록할 수 있습니다. 각각의 Virtual Access Point 모드는 서로 다른 무선랜 네트워크 이름과 보안을 사용합니다. 백본 유선랜 네트워크와 원격 유선랜 네트워크, 각각의 가상 무선랜에 연결된 모든 무선 클라이언트 치들은 동일 서브넷 네트워크로 연결되며 각 장치들은 장치 고유의 MAC 주소를 사용할 수 있습니다.

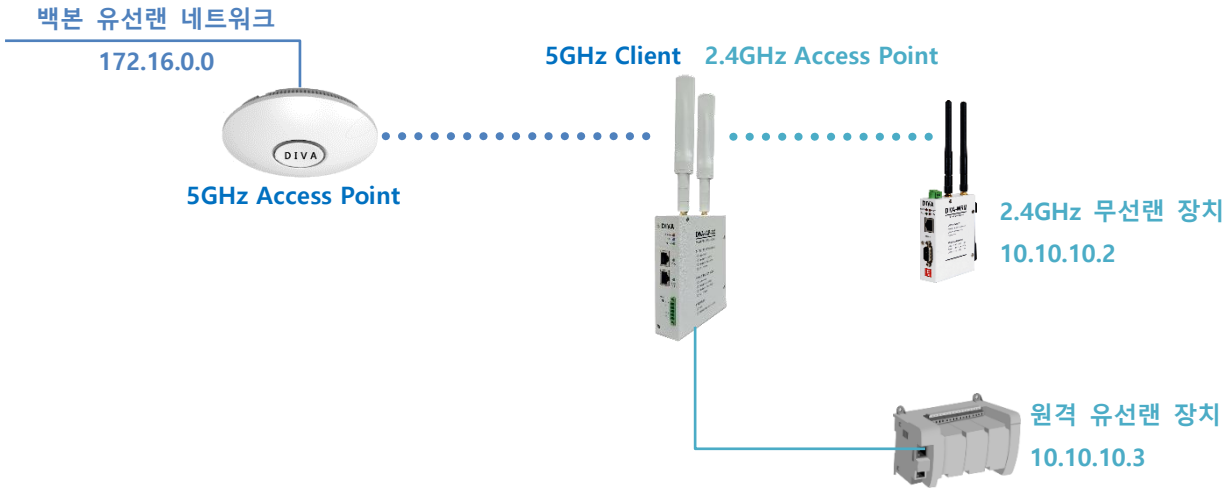
5GHz Access Point (WDS)
2.4GHz Virtual Access Point #1
2.4GHz Virtual Access Point #2

5GHz Client (WDS)
2.4GHz Virtual Access Point #1
2.4GHz Virtual Access Point #2



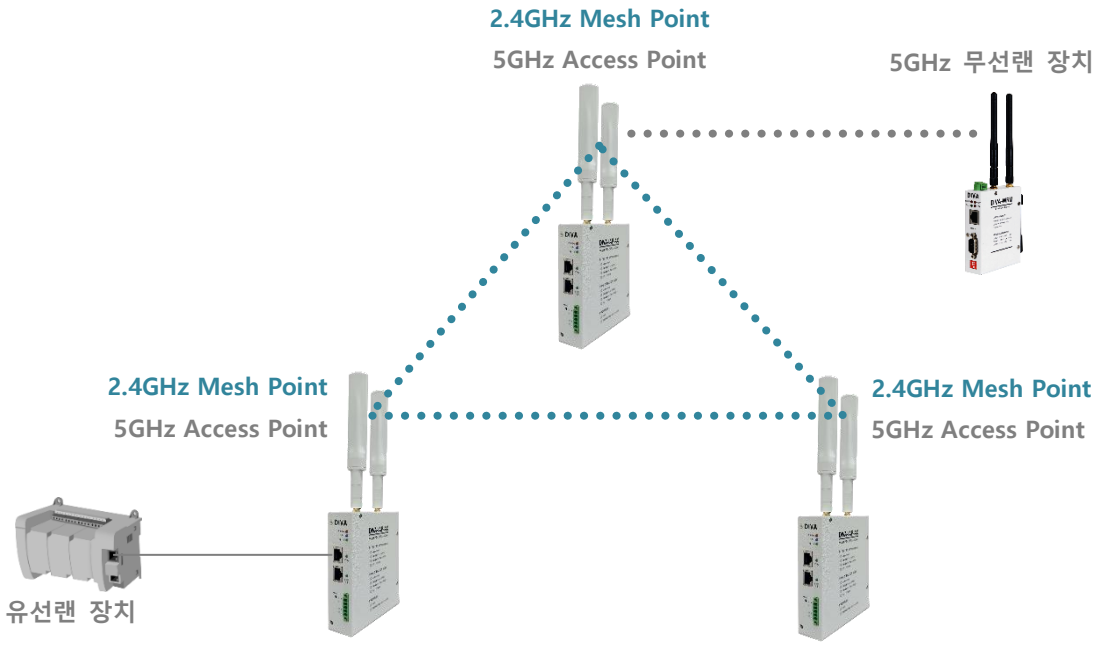
- **Client 모드**

  2개의 무선랜 인터페이스 중 1개의 인터페이스를 Client 모드로 사용하면, 나머지 1개의 무선랜 인터페이스와 2개의 유선랜 인터페이스는 액세스 포인트 장치와 다른 서브넷 네트워크를 사용합니다. 아래의 그림에서 백본 유선랜 네트워크와 액세스 포인트 장치, DIVA-IAP-AX 장치의 5GHz 무선랜 인터페이스는 172.16.0.0 네트워크로 연결되고, DIVA-IAP-AX 장치의 2.4GHz 인터페이스와 2개의 유선랜 인터페이스는 10.10.10.0 네트워크로 연결됩니다 10.10.10.0 네트워크 장치는 방화벽으로 보호되고, 포트 포워딩 기능으로 172.16.0.0 네트워크 장치가 접속할 수 있습니다.



- **802.11s 모드**

  802.11s 표준 프로토콜을 통해 무선 네트워크를 손쉽게 자동으로 연결/복구합니다. 1개의 무선랜 인터페이스는 Mesh Point 용도로 사용하고 나머지 1개의 무선랜 인터페이스는 Access Point 모드로 사용하여 표준 와이파이 무선랜 장치들도 연결할 수 있습니다.



주요 특징

- **고속 무선랜** : 5GHz 1201Mbps, 2.4GHz 573Mbps
- **2.4GHz 와 5GHz 동시 지원** : HD 영상 스트림과 같은 고속 어플리케이션은 가용 채널이 많고 간섭이 적은 5GHz 무선을 사용하고 일반 어플리케이션은 2.4GHz 무선을 사용하여 데이터 처리 효율 최적화
- **주파수 대역별 독립 운영 모드** : 2개 주파수 대역 동시 사용 가능, 1개 주파수 대역은 클라이언트 모드로 사용하고 나머지 1개 주파수 대역은 액세스 포인트 모드로 사용하여 고속 리피터 기능 응용
- **고출력 무선** : 최고 20dBm 송신 출력(국내 전파 규격 준수)을 제공하여 넓은 통신 반경 제공
- **강력한 무선랜 보안** : WPA/WPA2/WPA3 PSK & EAP, MAC-Filter, Isolate Clients, Firewall
- **다양한 동작 모드**
  - **표준 액세스 포인트** : 주파수 대역별로 최대 8개의 가상 SSID 설정
  - **WDS AP/Client** : PROFINET 장치 연결이 가능한 L2 트랜스패런트 네트워크
  - **Mesh Point** : 802.11s 매쉬 네트워크를 기반으로 유선랜 장치 연결
  - **산업용 IP 공유기** : 유무선 배본 네트워크 연결 지원, IPv4 & IPv6 DHCP 서버, 방화벽 설정
  - **Radius 클라이언트** : 1개의 IP 주소와 DMZ 설정으로 유선랜 장치를 MSCHAPv2 무선랜에 연결
- **무선랜 로밍** : 802.11r Fast Transition, 802.11k RRM, 802.11v, 신호 레벨이 낮은 클라이언트 장치 연결 차단
- **STP** Spanning Tree Protocol 기반으로 네트워크 루프 감지 및 자동 차단
- **편리한 상태 확인 및 관리** : 실시간 무선 채널/트래픽 분석, 웹/SSH/HTTPS 접속, 설정상태 파일 저장/복구
- **장착 방식** : 35mm 딘레일 또는 벽면
- **802.11at/af 표준 PoE** : 이더넷 케이블 하나로 전원 및 유선랜 네트워크 동시 연결

무선 간섭 환경

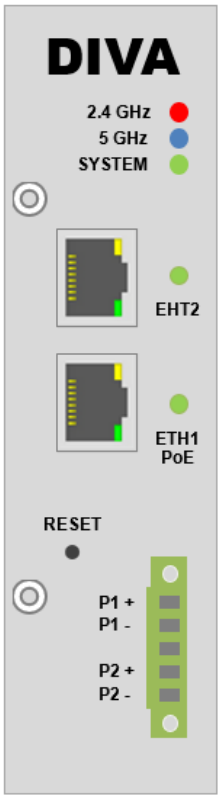
아래와 같은 장치 및 장소의 인접한 곳에서는 동일한 주파수 대역으로 인해 간섭이 발생하여 무선 통신에 서로 영향을 주기 때문에 DIVA-IAP-AX 장치를 사용을 신중히 검토하시기 바랍니다.

- 마이크로파를 사용하는 산업용/연구용/의료용 장치 (맥박조정장치 등...)
- 산업 현장에서 별도의 전파 허가 후 사용되는 무선 기지국
- 소형 라디오 방송국 (무허가)

일반적으로 휴대폰, TV, 라디오와 같은 장치는 DIVA-IAP-AX 제품과 다른 무선 주파수를 사용하기 때문에 문제가 발생하지 않습니다. 하지만 장치 성능 및 주변 환경에 따라 음향 장치 및 영상 장치에 노이즈가 발생할 수도 있습니다. DIVA-IAP-AX 장치는 목재 또는 유리를 통해 무선 통신을 연결할 수 있지만 철근 콘크리트, 금속 판넬 등이 중간에 위치할 경우 신호 감쇄로 인해 무선 통신이 불안정 할 수 있습니다.

사용자는 주변 무선 네트워크에 심각한 영향을 주지 않으면서 DIVA-IAP-AX 장치의 무선 성능을 최대화할 수 있도록 주변 무선 환경을 사전에 충분히 분석하시는 것이 좋습니다. 사용자는 국내 전파법에 위반되지 않도록 채널 및 무선 송신 출력, DFS 채널을 설정하여 사용할 책임이 있습니다. DIVA-IAP-AX 제품은 KC 인증을 획득한 제품으로서 국내 전파법 요구 사항을 준수합니다. 사용자는 반드시 채널 및 안테나에 따라 무선 송신 출력을 국내 전파법에 위배되지 않도록 사용해야 합니다. Network > Wireless > Device Configuration > Advanced Settings 설정에서 Country Code 항목을 "**KR-South Korea**" 값으로 설정하고 Wireless > Device Configuration > General Setup 메뉴의 "Maximum transmit power" 항목을 설정하여 사용하시기 바랍니다. 해외에서 제품을 사용하실 경우 Country Code 항목을 해당 국가로 설정하여 사용하시기 바랍니다.

LED 상태 표시



LED	색상	상태 표시
2.4GHz	●	액세스 포인트 모드에서 2.4GHz 미사용 설정 시 켜짐 클라이언트/매쉬 모드에서 2.4GHz 연결되지 않을 경우 꺼짐 무선 연결 후 데이터 송수신 시 깜빡임 Access Point 모드 사용 시, 연결된 클라이언트 장치가 없어도 비콘 메시지 전송으로 깜빡임
5GHz	●	액세스 포인트 모드에서 5GHz 미사용 설정 시 켜짐 클라이언트/매쉬 모드에서 5GHz 연결되지 않을 경우 꺼짐 무선 연결 후 데이터 송수신 시 깜빡임 Access Point 모드 사용 시, 연결된 클라이언트 장치가 없어도 비콘 메시지 전송으로 깜빡임
ETH2	●	ETH2 포트에 이더넷 링크 연결 시 켜짐 데이터 송수신 시 깜빡임
ETH1 PoE	●	ETH1 PoE 포트에 이더넷 링크 연결 시 켜짐 데이터 송수신 시 깜빡임
SYSTEM	●	PoE / DC 전원 입력 시 켜짐 부팅 완료 후 깜빡임 공장 초기화 설정 시 1초에 5회 깜빡임

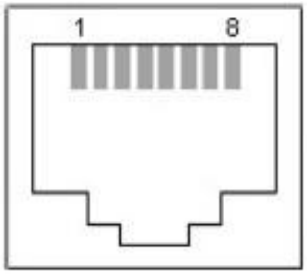
안테나 연결

DIVA-IAP-AX 모델은 외부 안테나를 연결할 수 있는 2개의 SMA Female 커넥터를 제공합니다. DIVA-IAP-AX 장치에 안테나를 직접 연결할 경우 SMA Male 커넥터로 제작된 안테나를 사용합니다. **안테나를 연결하거나 분리할 때 정전기 충격에 의해 무선랜 인터페이스 회로가 손상될 가능성이 있으니 반드시 제품 전원을 차단한 후 작업하시기 바랍니다.**

DIVA-IAP-AX 커넥터 (SMA Female)	안테나 커넥터 (SMA Male)
	

이더넷 케이블 연결

DIVA-IAP-AX 장치는 2개의 기가비트 유선랜 인터페이스를 제공하고 Auto MDI/MDIX 기능을 지원하기 때문에 다이렉트 또는 크로스 케이블을 모두 사용할 수 있습니다. **PoE 전원 품질 및 기가비트 고속 통신을 위하여 쉴드로 보호된 이더넷 케이블 사용을 권장**하며 실외 환경에 설치할 경우 적합한 규격의 실외용 케이블을 사용하시기 바랍니다.

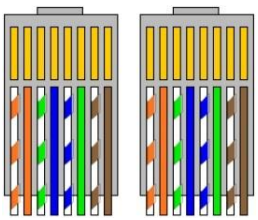


핀	10BASE-T	100BASE-T	1000BASE-T
1	TX+	TX+	BI_DA+
2	TX-	TX-	BI_DA-
3	RX+	RX+	BI_DB+
4	Not connected	Not connected	BI_DC+
5	Not connected	Not connected	BI_DC-
6	RX-	RX-	BI_DB-
7	Not connected	Not connected	BI_DD+
8	Not connected	Not connected	BI_DD-

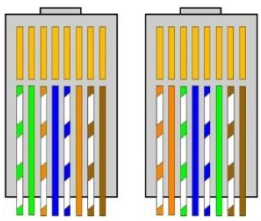
이더넷 케이블 규격에 따라 다음과 같은 통신 속도를 지원합니다.

카테고리	케이블 타입	지원 속도
CAT.5	UTP	100Mbps
CAT.5e	UTP	1Gbps
CAT.6	UTP, STP	1Gbps
CAT.6A	STP	10Gbps
CAT.7	S/FTP	10Gbps

일반적으로 다이렉트 케이블을 사용하여 DIVA-IAP-AX 장치와 유선랜 장치를 연결합니다. DIVA-IAP-AX 장치와 유선랜 장치 사이에 링크가 연결되지 않을 경우 크로스 케이블을 사용하시기 바랍니다. **아래의 순서로 케이블을 제작하지 않을 경우, PoE 전원의 극성이 변경되어 장치가 심각하게 손상될 수 있으며 유선랜 고속 통신이 지원되지 않습니다.**



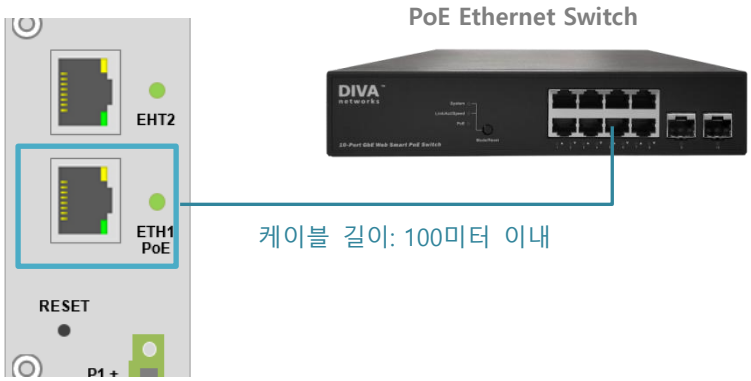
다이렉트 케이블



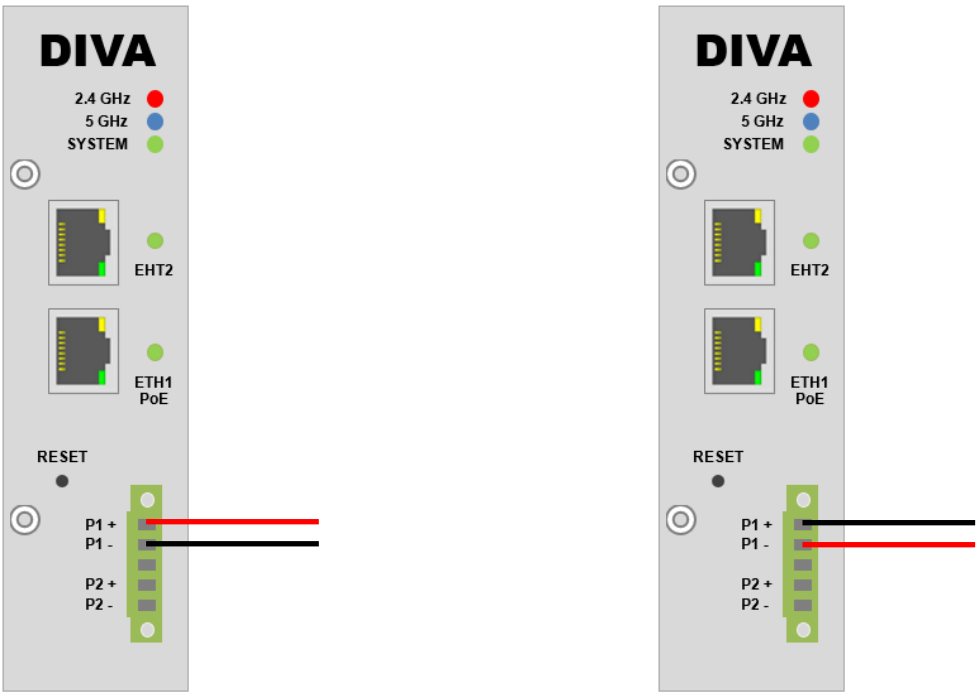
크로스 케이블

전원 연결

DIVA-IAP-AX 제품은 48V 규격의 표준 802.3at/af PoE 전원을 지원합니다. 반드시 표준 규격의 PoE 인젝터 제품이나 PoE 이더넷 스위치(홈페이지 참조)를 통해 전원을 공급하시기 바랍니다. PoE 전원이 정상적으로 입력될 경우 SYSTEM LED 와 ETH1 PoE LED가 켜집니다. **표준 규격의 유선랜 케이블을 사용하지 않을 경우 극성이 변경되어 장치가 손상될 수 있습니다.**



DIVA-IAP-AX 제품은 PoE 전원 외에도 9-30V 사이의 DC 전원을 터미널블록 커넥터에 연결하여 동작할 수 있습니다. 이때 **DC 전원과 PoE 전원을 동시에 연결하지 않도록 주의하시기 바랍니다. 동시 연결 시 제품이 손상됩니다**. DIVA-IAP-AX 제품은 역전압 보호 회로를 내장하여 + / - 전원을 반대로 연결하여도 시스템이 손상되지 않고 정상 동작합니다. 상단 P1+ 단자는 하단 P2+ 단자와 내부적으로 연결되어 있으며, P1- 단자는 P2- 단자와 내부적으로 연결되어 있습니다. 따라서 DIVA-IAP-AX 장치와 동일 규격의 전원을 사용하는 장치를 손쉽게 캐스케이드 방식으로 부착할 수 있습니다.



시스템 요구 사항

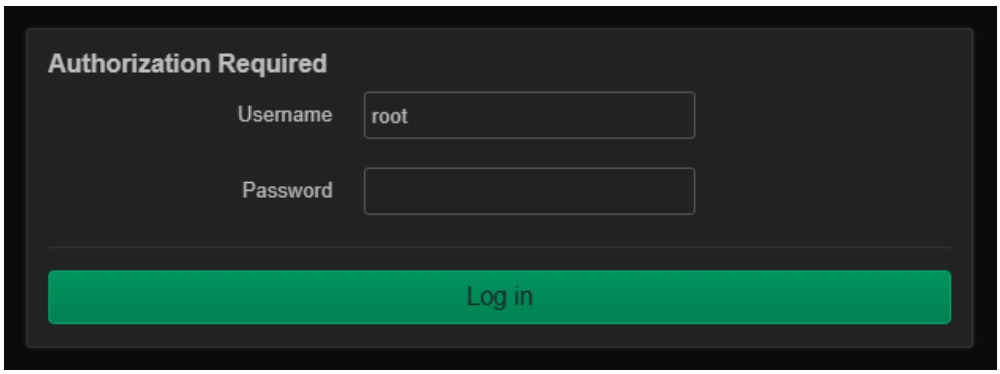
DIVA-IAP-AX 장치는 기능 설정 및 상태 확인을 위한 웹 서버를 내장하고 있습니다.

- Microsoft Windows 7 이상, Linux, Mac OS X
- 웹 브라우저: Mozilla Firefox, Apple Safari, Google Chrome, Microsoft Internet Explorer 8 이상

시작하기

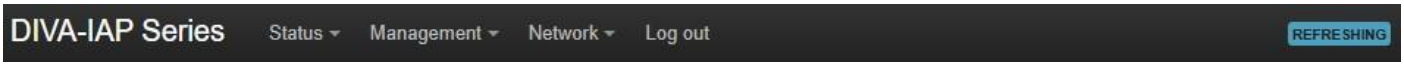
DIVA-IAP-AX 장치의 웹 설정 화면은 다음과 같은 단계로 접속합니다.

1. DIVA-IAP-AX 장치와 사용자 컴퓨터를 유선랜 케이블로 연결합니다.
2. DIVA-IAP-AX 장치에 전원을 입력한 후 시스템 부팅이 완료되면 SYSTEM LED가 깜빡입니다.
3. 사용자 컴퓨터의 IP 주소를 192.168.1.xxx (예: 192.168.1.100, 서브넷: 255.255.255.0) 값으로 설정합니다.
4. 웹 브라우저를 실행한 후 주소 창에 **192.168.1.1** 주소를 입력한 후 **Enter** 키를 누릅니다.
5. 로그인 화면이 표시됩니다. 사용자 이름 **root**, 비밀번호 **admin** (소문자)를 입력하고 **Login** 버튼을 클릭합니다.



시스템 및 네트워크 보안을 위하여 로그인 비밀번호를 변경하시고 사용하시기 바랍니다. 로그인 비밀번호는 상단 System 메뉴를 선택한 후 **Administration** 메뉴에서 변경하실 수 있습니다.

네비게이션



웹 설정 인터페이스는 다음과 같이 4개의 메인 웹 페이지로 구성되어 있으며 각각의 페이지에서 특정 기능을 변경하거나 설정값 및 동작 상태를 확인할 수 있습니다.

- **Status** 유무선 네트워크 설정 정보 및 연결 상태, 실시간 트래픽, 장치 정보를 표시합니다.
- **Management** 시스템 비밀번호 변경, 펌웨어 업데이트, 설정 저장/복구/초기화, 재부팅 프로세스를 실행합니다.
- **Network** IP 주소와 같은 네트워크 정보와 무선랜, DHCP 서버, 네트워크 진단, 방화벽 기능을 설정합니다.
- **Log out** 웹 서버 연결을 종료합니다.

각 페이지에서 설정을 변경하신 후 화면 하단의 **Save** 버튼을 클릭하면 변경된 설정이 임시 저장됩니다. 모든 설정을 변경한 후 화면 하단의 **Save & Apply** 버튼을 클릭하면 변경된 설정으로 장치가 동작합니다. **Management > Reboot** 메뉴를 실행하여 재부팅 후에도 변경된 설정으로 동작하는지 확인하실 것을 권장합니다.

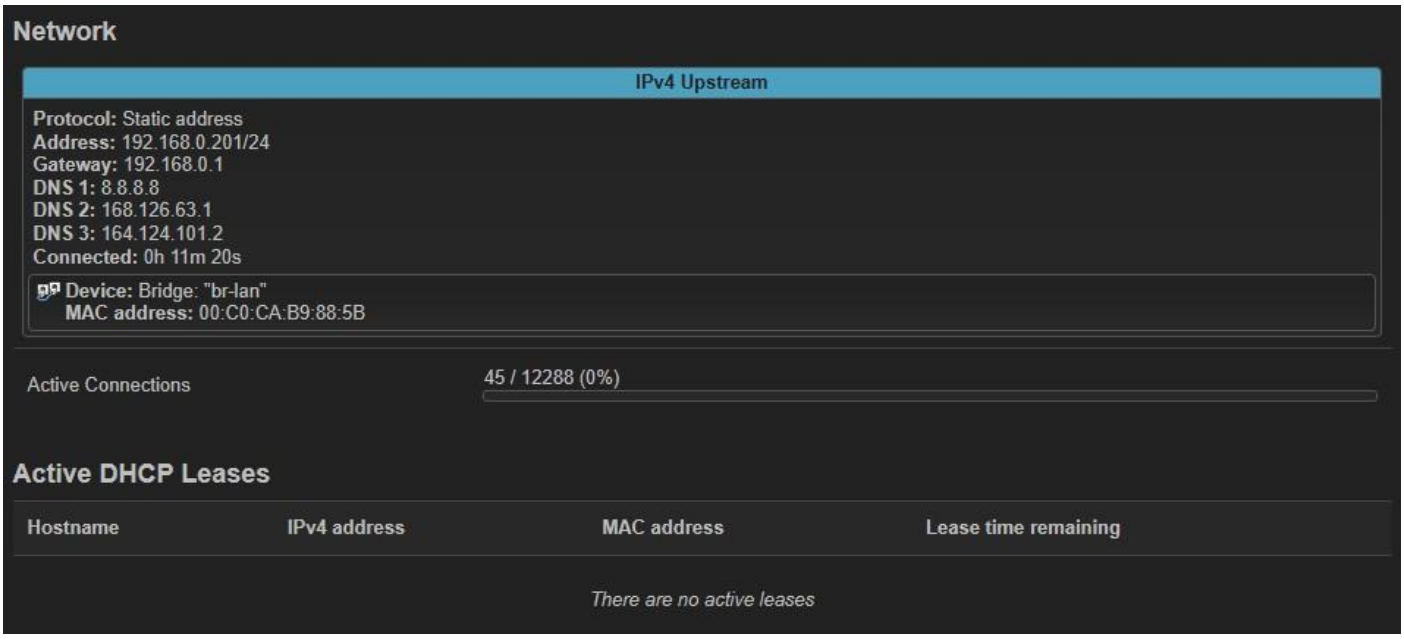
Chapter 2: Status

유무선 네트워크 연결 정보 및 실시간 트래픽 그래프, 장치 정보 등을 표시합니다.

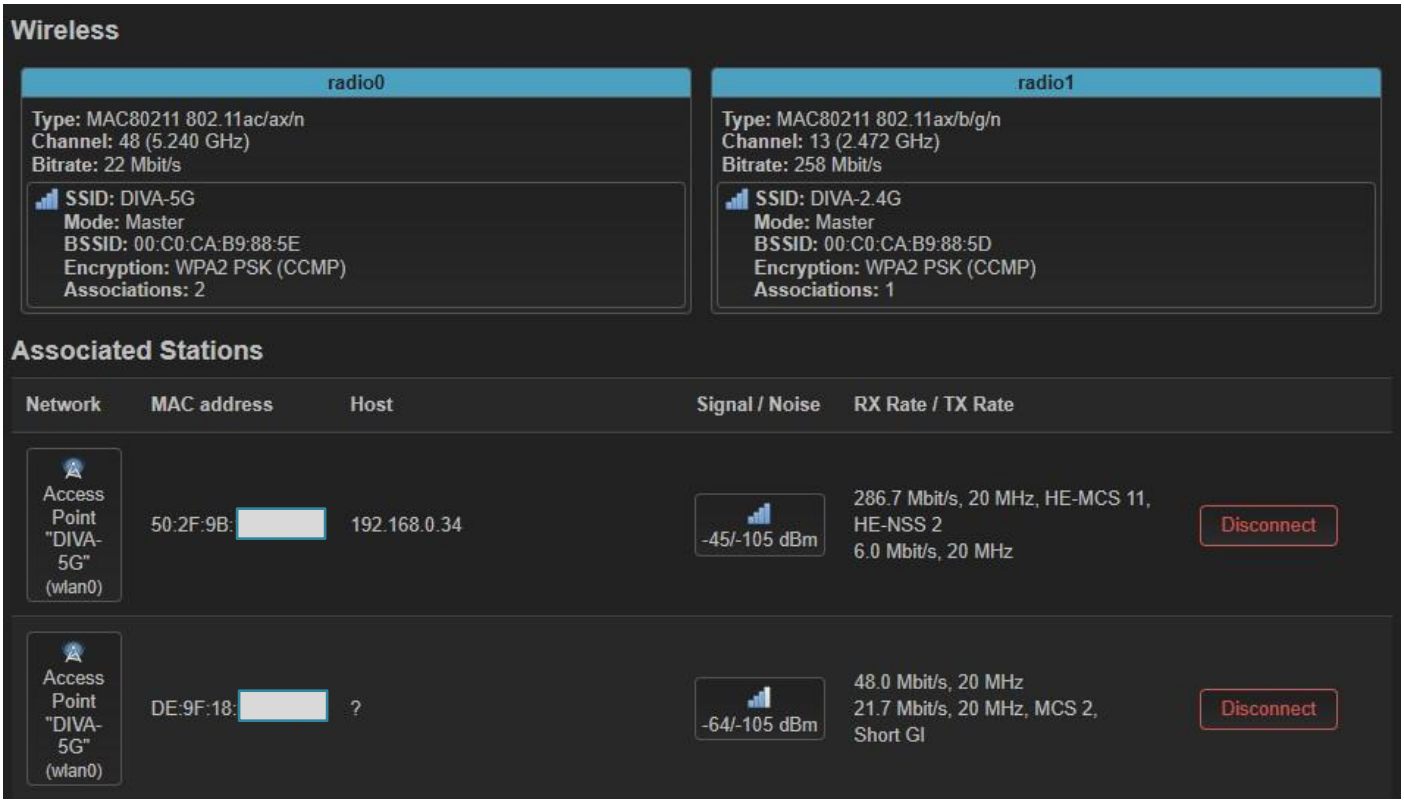
- **Overview** System, Network, Active DHCP Leases, Wireless, Associate Station 정보를 표시합니다.
- **System Log** 이벤트 로그 정보를 표시합니다. 로그 메시지 크기 및 이벤트 종류는 System > System > Logging 메뉴에서 변경할 수 있고, 로그 메시지 전송을 위한 원격 서버를 설정할 수 있습니다.
- **Channel Analysis** 주변 무선 네트워크에서 감지되는 2.4/5GHz 채널 정보를 표시합니다. 주변에 위치한 무선랜 장치와 채널 간섭이 발생하지 않도록 무선 채널을 충분히 검색한 후 사용할 채널을 선택하시기 바랍니다. 숨겨진 무선랜 장치까지 상세하게 검색할 경우, DIVA-IAP-AX 장치의 무선 인터페이스를 Monitor 모드로 설정하시기 바랍니다. Monitor 모드는 Interfaces > Wireless 메뉴로 접속한 후 radio0 / radio1 인터페이스의 Mode 항목에서 설정합니다.
- **Realtime Graphs** 시스템 부하 및 유무선 데이터 트래픽, 무선 신호 강도와 노이즈 레벨, 연결된 TCP/UDP 세션 정보를 실시간 그래프로 표시합니다.

2.1 Overview

- **Hostname** 유무선 네트워크에서 식별되는 장치 이름을 표시합니다. System > System > General Settings 탭에서 Hostname 값을 변경할 수 있습니다.
- **Model** 제품 모델명을 표시합니다.
  - DIVA-IAP-AX : 산업용 모델, 외장 안테나 장착형
  - DIVA-AXP : 지향성 안테나 일체형, IP66 방수/방진
- **Firmware Version** 펌웨어 버전을 표시합니다. System > Backup / Flash Firmware 메뉴에서 펌웨어를 업데이트 할 수 있습니다.
- **Local Time** 장치에서 사용되는 현재 시간을 표시합니다. 시스템 시간은 이벤트 로그 발생 시간을 기록하고, 특정 시간에만 동작하는 방화벽 기능에 사용됩니다. System > System > General Settings 및 Time Synchronization 메뉴에서 변경할 수 있습니다.
- **Uptime** 부팅 후 시스템 동작 시간을 표시합니다. 전원을 껐다 켜거나 Reboot 기능을 실행하면 초기화 됩니다.



- **Network** 네트워크와 연결된 인터페이스 정보를 표시합니다.
- **Active DHCP Leases** IPv4 DHCP 서버 기능 사용 시, 연결된 DHCP 클라이언트 장치 정보를 표시합니다.

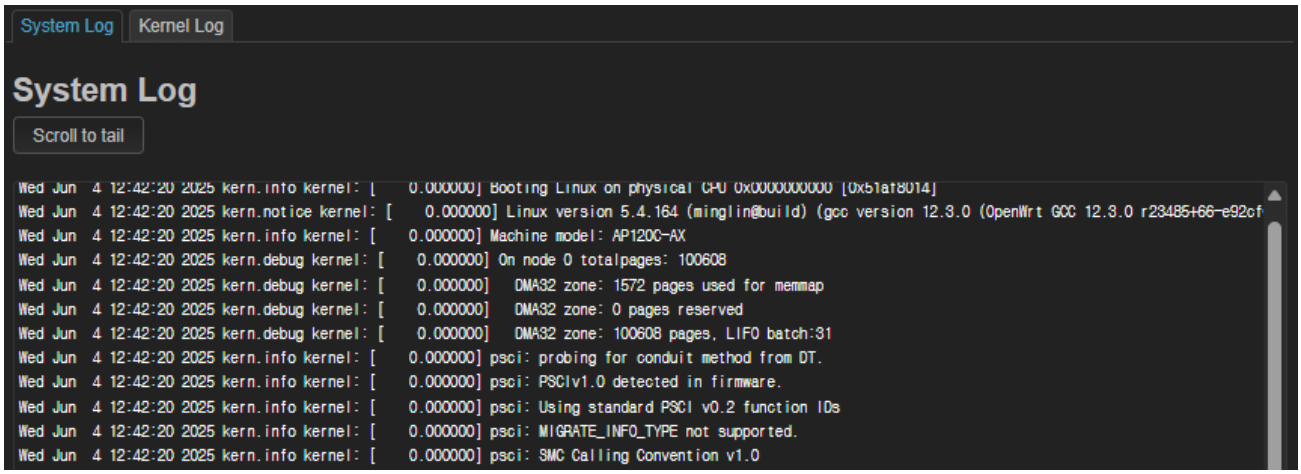


- **Wireless** 5GHz(radio0) 와 2.4GHz(radio1) 무선 인터페이스 상태를 표시합니다.
- **Associated Stations** 무선랜 연결 정보를 표시합니다. DIVA-IAP-AX 장치를 Access Point 모드로 사용 시, 우측에 **Disconnect** 버튼이 표시되고 버튼을 클릭하면 해당 클라이언트 장치의 무선 연결이 끊어집니다. 미확인 클라이언트 장치 연결을 해제할 때 사용되며, 해당 장치는 Access Point 장치를 재부팅 할 때까지 다시 연결할 수 없습니다.

2.2 System Log

2.2.1 System Log

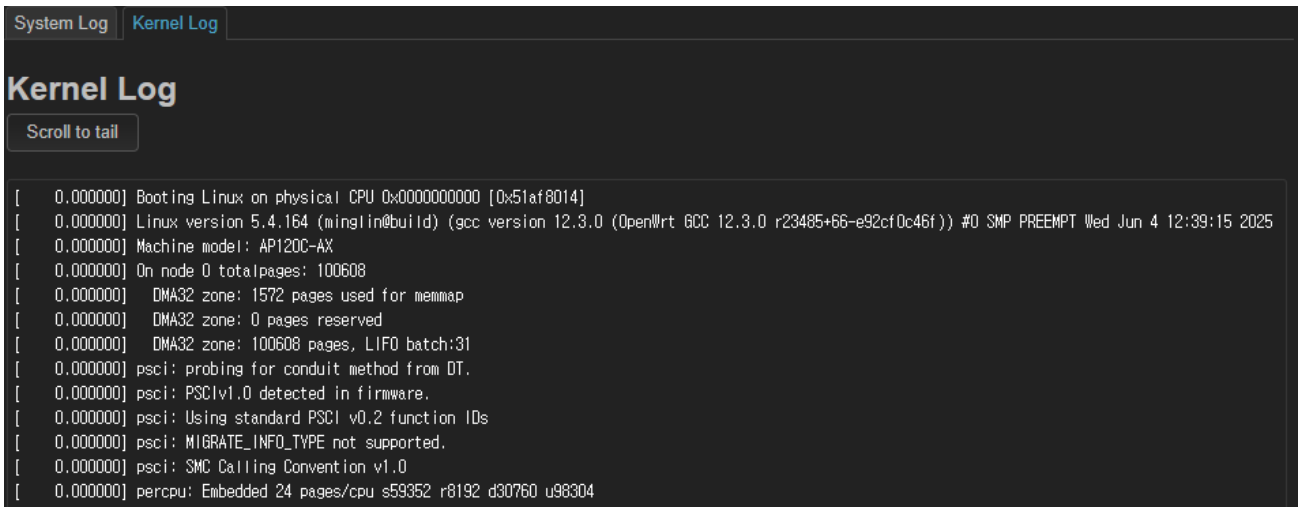
Wi-Fi 연결 문제나 DHCP/DNS, 방화벽, 서비스 재시작, 설정 오류 등을 확인할 때 사용합니다. 휘발성 메모리에 저장되고 재부팅 후 메시지는 자동 삭제됩니다. 표시되는 로그 메시지 크기 및 이벤트 종류는 **System > System > Logging** 메뉴에서 변경할 수 있고, 로그 메시지를 외부 네트워크 서버로 전송하도록 설정할 수 있습니다.



좌측에 표시되는 시간은 현재 장치에서 사용되는 시간 정보를 나타냅니다. 디버깅을 위해 정확한 시간 정보가 필요할 경우 **System > System > General Settings** 및 **Time Synchronization** 메뉴에서 시간 정보를 설정합니다.

2.2.2 Kernel Log

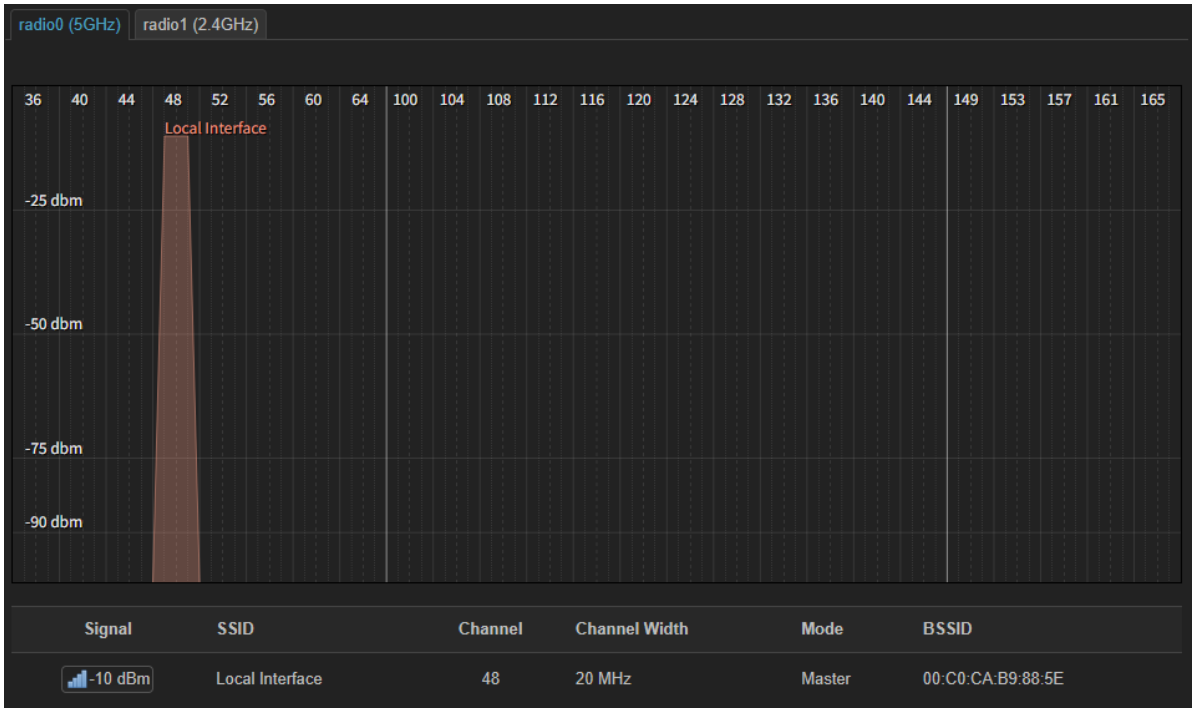
리눅스 커널에서 출력하는 로그 메시지로서 하드웨어, 네트워크 스택, 메모리 관련 메시지를 확인할 때 사용합니다. 부팅 문제, 네트워크 인터페이스 에러 등을 확인할 수 있으며 커널 로그 메시지는 내부적으로 시스템 로그 메시지로도 전달됩니다.



특정 장치의 연결 정보를 조회해야 할 경우, 'Ctrl + F' 키보드 버튼을 누른 후 해당 장치의 MAC 주소를 입력하여 검색합니다. 또는 authenticate, authentication, associated 등의 검색어를 통해 무선랜 연결 시간을 검색할 수 있습니다.

2.3 Channel Analysis

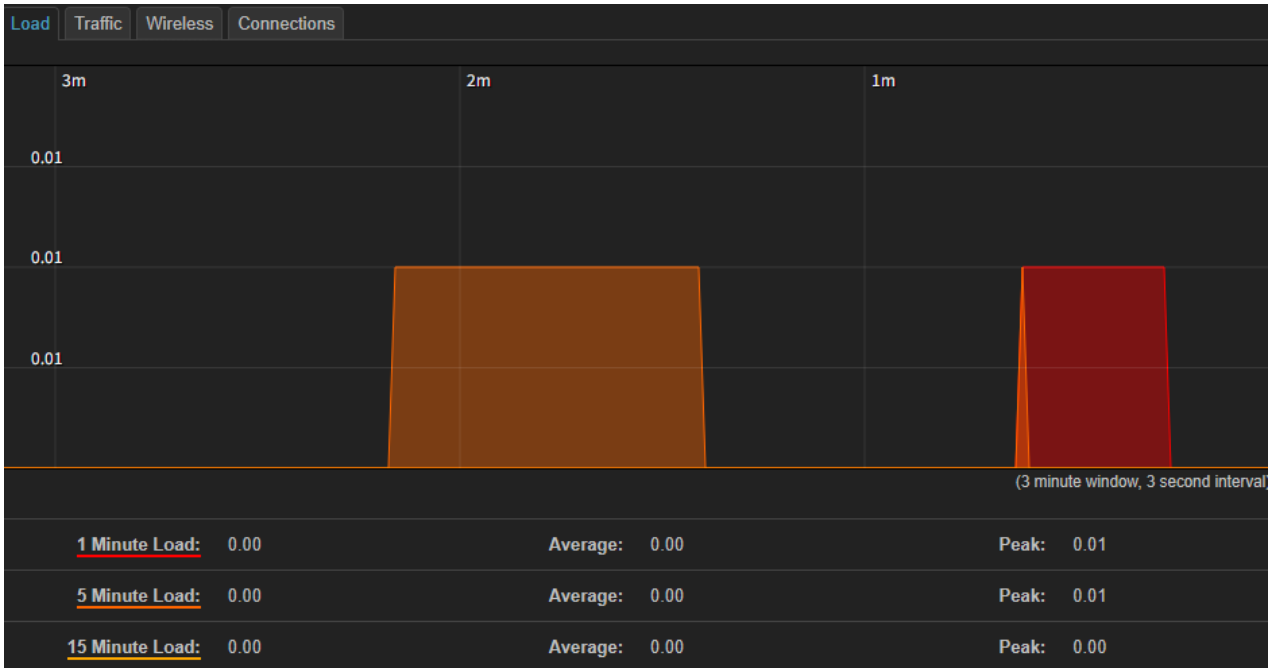
2.3.1 radio0 (5GHz) 5GHz 채널 검색 결과를 표시합니다. 간섭이 발생하지 않는 채널을 사용하시기 바랍니다.



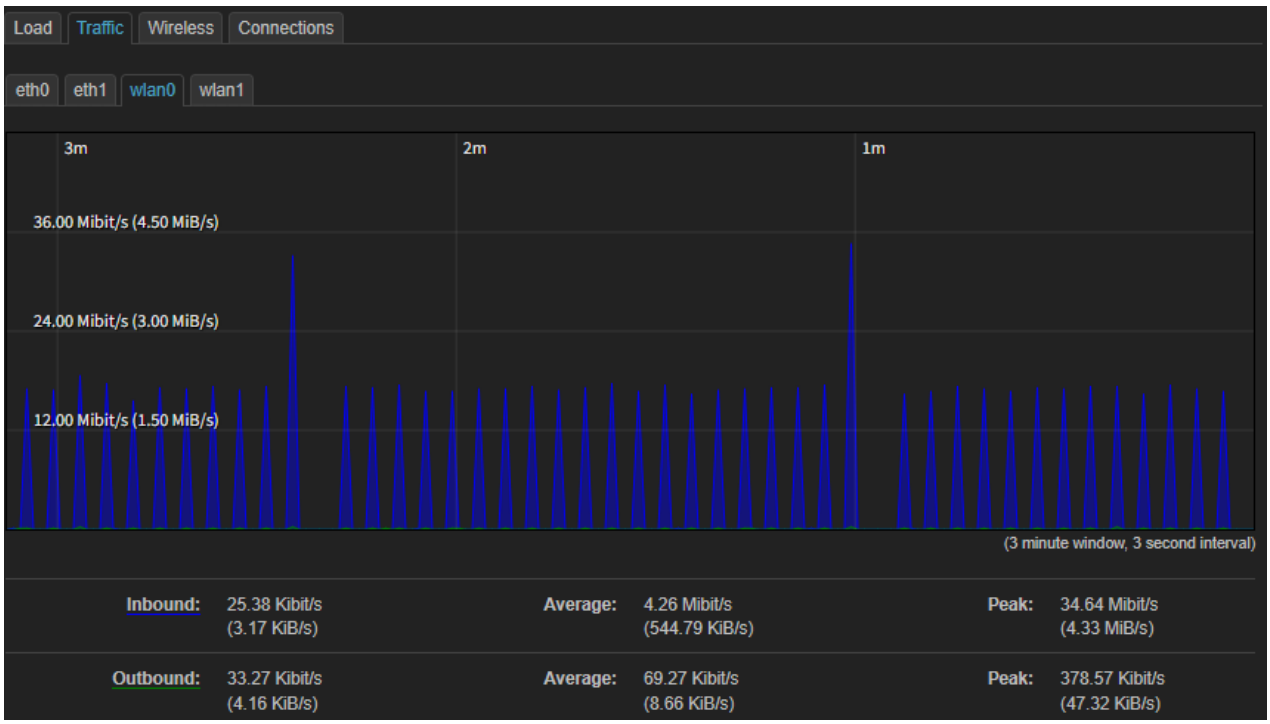
2.3.2 radio1 (2.4GHz) 2.4GHz 채널 검색 결과를 표시합니다. 간섭이 발생하지 않는 채널을 사용하시기 바랍니다.

2.4 Realtime Graphs

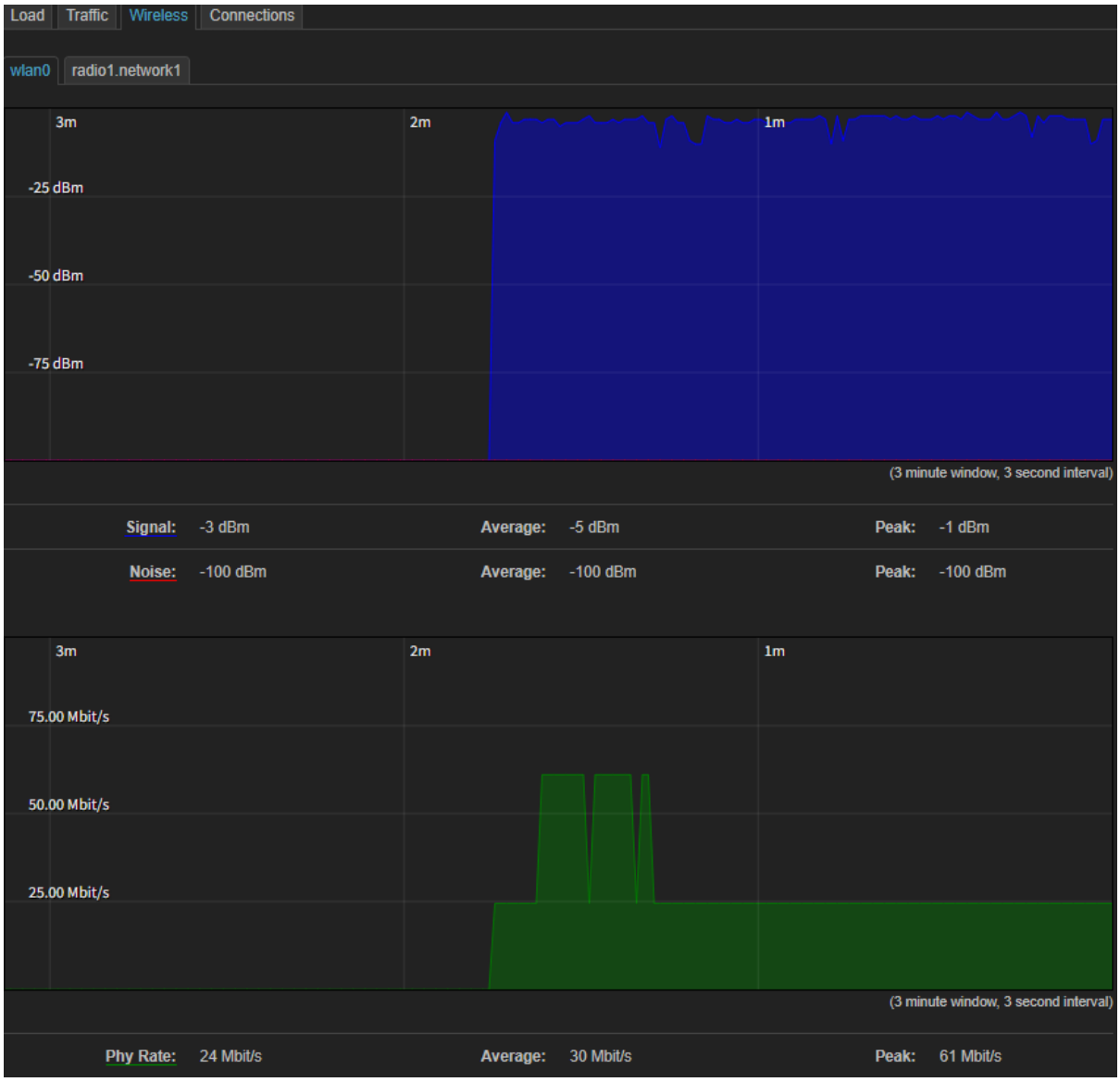
2.4.1 Load CPU 상태 정보를 표시하며 Average는 CPU에서 실행 중이거나 실행 대기 상태인 프로세스 수를 나타냅니다. DIVA-IAP-AX 제품은 4코어 CPU를 사용합니다. 0.0 ~ 2.8 수치는 정상 범위이고, 2.8 ~ 4.0 수치는 주의, 4.0 이상은 위험 단계를 나타냅니다. 부하가 발생할 경우 웹 접속이 느려지거나 SSH 입력 지연, 무선랜 끊김, NAT/라우팅 성능 저하, Watchdog 리부팅 현상이 발생할 수 있습니다.



2.4.2 Traffic 2개의 유선랜 포트와 2.4GHz 와 5GHz 무선랜을 통해 송수신 되는 트래픽 정보를 표시합니다.

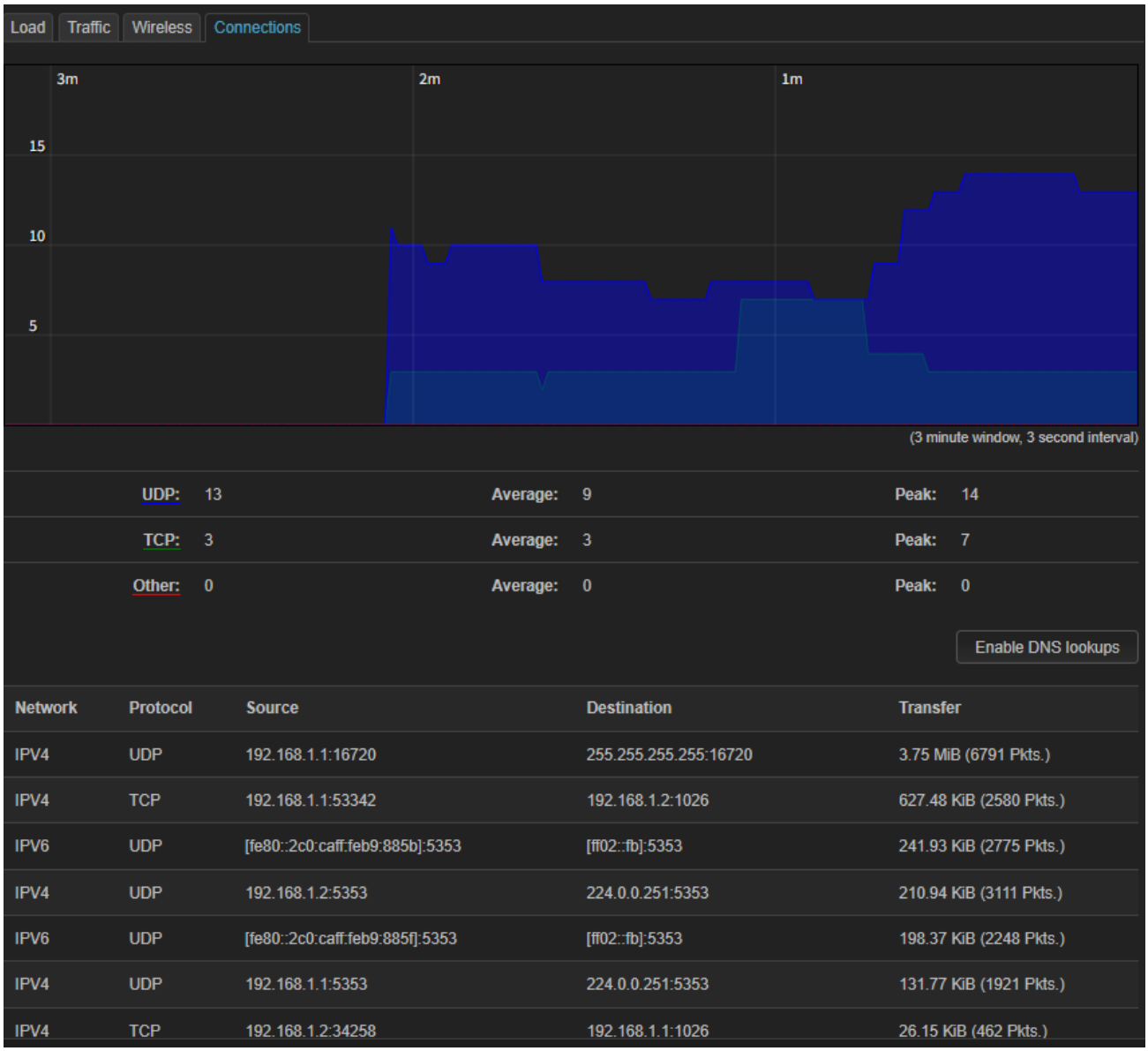


2.4.3 Wireless 2.4GHz 와 5GHz 무선 신호 강도 및 노이즈 레벨, 속도를 표시합니다.



- **Signal** 무선 장치 사이의 수신 신호 세기를 표시하며 0에 가까울수록 강한 신호를 의미합니다.
  - -30 ~ -50 : 매우 좋음 (최대 속도)
  - -50 ~ -60 : 좋음 (안정)
  - -60 ~ -70 : 보통 (속도 감소)
  - -70 ~ -80 : 나쁨 (끊김 가능)
- **Noise** 주변 환경에서 발생하는 전파 잡음 레벨을 표시합니다.
  - -95 ~ -100 : 매우 깨끗
  - -90 : 보통
  - -85 이상 : 혼잡/간섭
- **Phy Rate** 이론상 무선 전송 속도를 표시합니다. 실제 속도는 약 40~60% 이고 SNR, 20/4/80MHz 채널 폭, MCS 인덱스, 암호화 오버헤드 등의 영향을 받습니다. 수시로 값이 변동될 경우 채널 간섭과 무선 통신 거리를 확인합니다. Signal 레벨이 높아도 Noise 레벨이 높으면 속도가 낮아지고, 80MHz 채널 대역폭은 오히려 간섭 발생 가능성이 높아집니다.

2.4.4 Connections 연결된 TCP/UDP/ICMP 세션 정보를 표시합니다.



일반적으로 1개의 웹 서버에만 접속해도 수십 개의 세션 연결이 생성됩니다. 연결이 과다할 경우 CPU 부하가 높아지고 메모리가 부족해져 장치 성능이 저하될 수 있습니다. DIVA-IAP-AX 제품은 128MB 메모리를 장착하고 있으며 최대 8192개 이내의 동시 세션 사용을 권장합니다. 동시 세션이 증가할 경우 비정상적인 클라이언트 장치를 확인하시기 바랍니다. 일반적으로 비정상적인 클라이언트 장치에서는 P2P, 잘못된 IoT 펌웨어를 사용하거나 UDP flood, DNS loop, 외부 스캔 공격 등이 발생합니다.

동시 세션 개수 별 성능 (대략적 수치)

- ✓ 30% 미만 (2458개 미만) : 매우 안정
- ✓ 30 ~ 60% (2458 ~ 4915개) : 정상
- ✓ 60 ~ 80% (4915 ~ 6554개) : 주의
- ✓ 80% 이상 (6554개 이상) : 위험

Chapter 3: Management

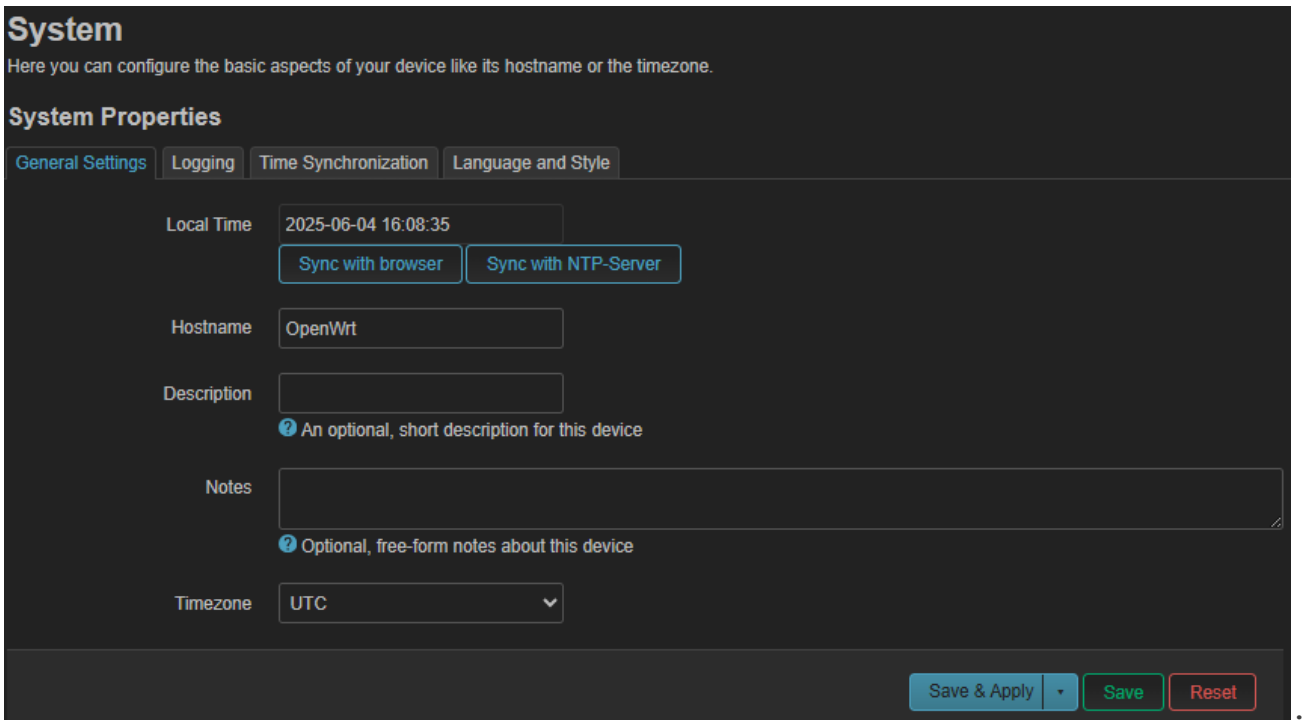
시스템 시간 및 로그인 비밀번호를 설정하고, 펌웨어 업데이트, 설정 초기화/저장/복구, 재부팅 작업을 실행합니다.

- **System** 시스템 시간 동기화, 로그 메시지 옵션 설정, 타임서버 설정
- **Administration** 로그인 비밀번호, SSH/HTTPS 접속 설정
- **Backup / Flash Firmware** 설정 저장/복구, 공장 초기화, 펌웨어 업데이트
- **Reboot** 시스템 재시작

3.1 System

3.1.1 General Settings

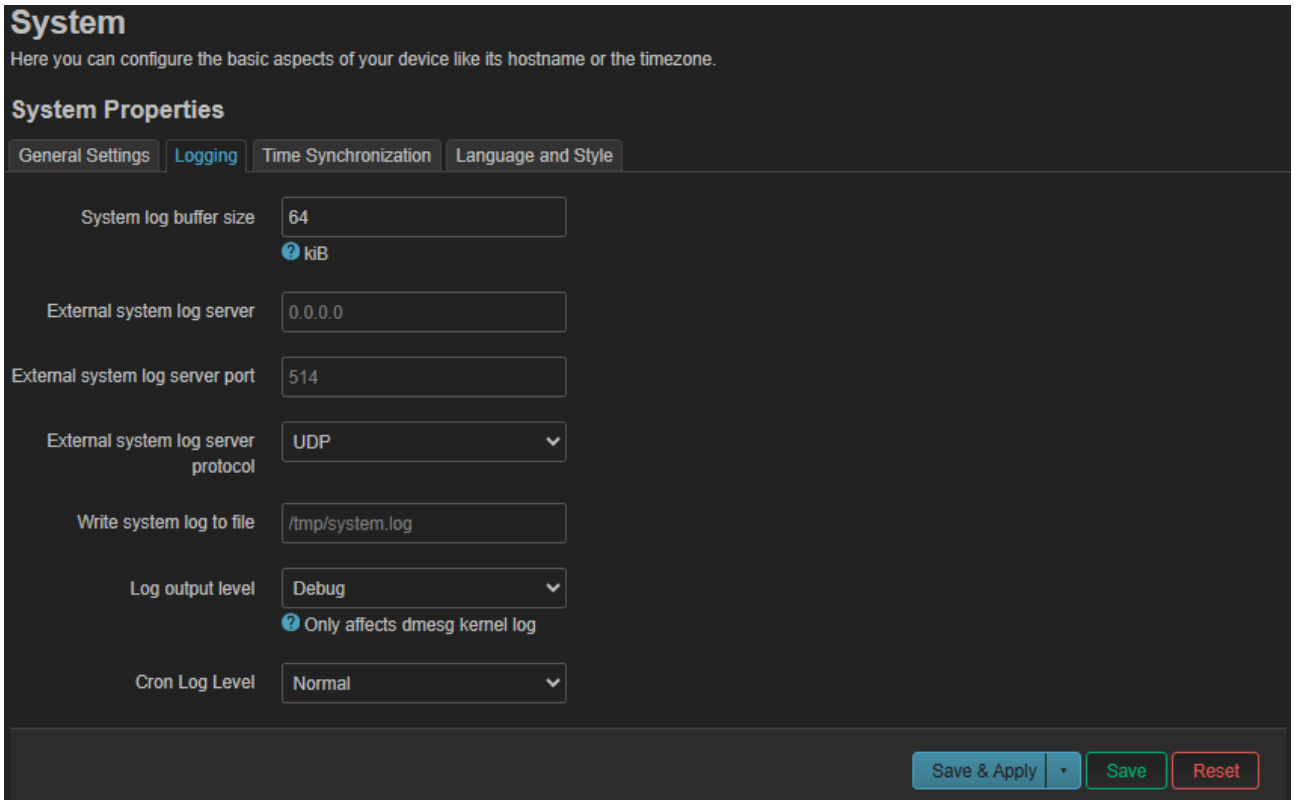
로그 메시지 및 방화벽에 사용되는 시간과 관리 목적을 위한 정보 등을 입력합니다.



- **Local Time** 시스템에서 현재 사용되는 시간을 표시합니다.
  - **Sync with browser** 접속한 사용자 컴퓨터의 웹 브라우저와 시간 정보를 동기화 합니다.
  - **Sync with NTP-Server** NTP 서버와 시간 정보를 동기화 합니다. (Time Synchronization 참조)
- **Hostname** 네트워크에서 식별되는 장치 이름을 설정합니다. (기본값 DIVA-AX Series)
- **Description** 관리 목적을 위해 장치 용도 및 기능 등을 입력합니다.
- **Notes** 관리 목적을 위해 장치에 대한 추가 정보를 입력합니다.
- **Timezone** 로컬 시간 지역을 선택합니다. (기본값 Asia/Seoul)

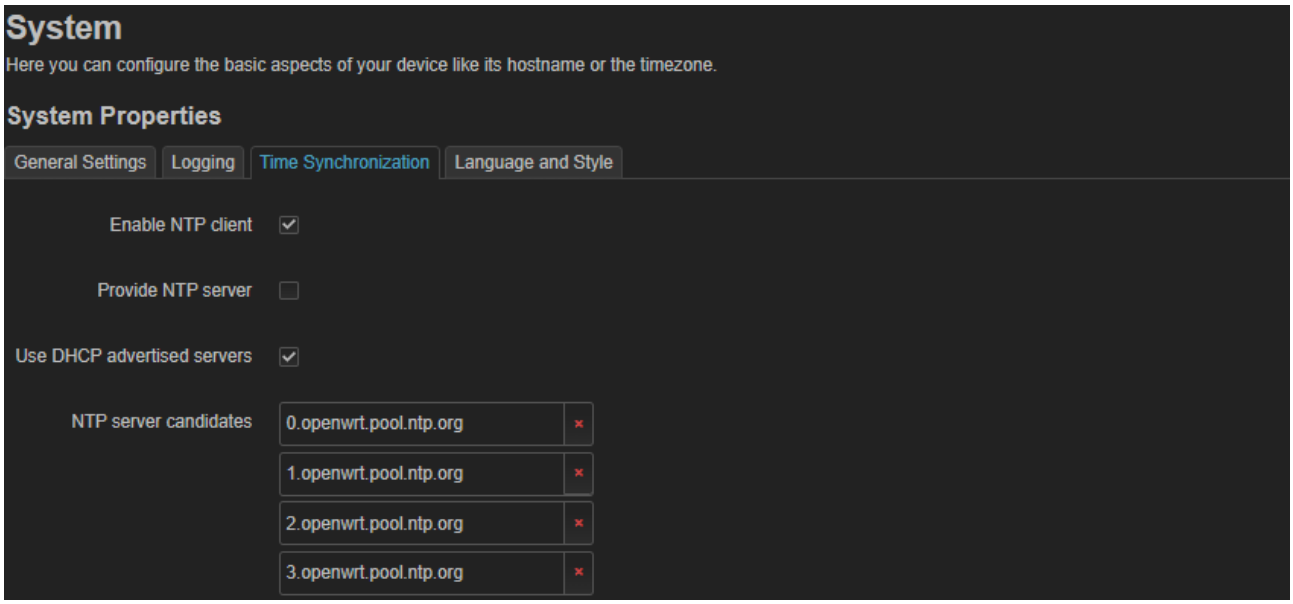
3.1.2 Logging

웹 서버에 표시되는 로그 메시지 버퍼 크기 및 로그 메시지 전송을 위한 외부 서버 정보 등을 설정합니다.



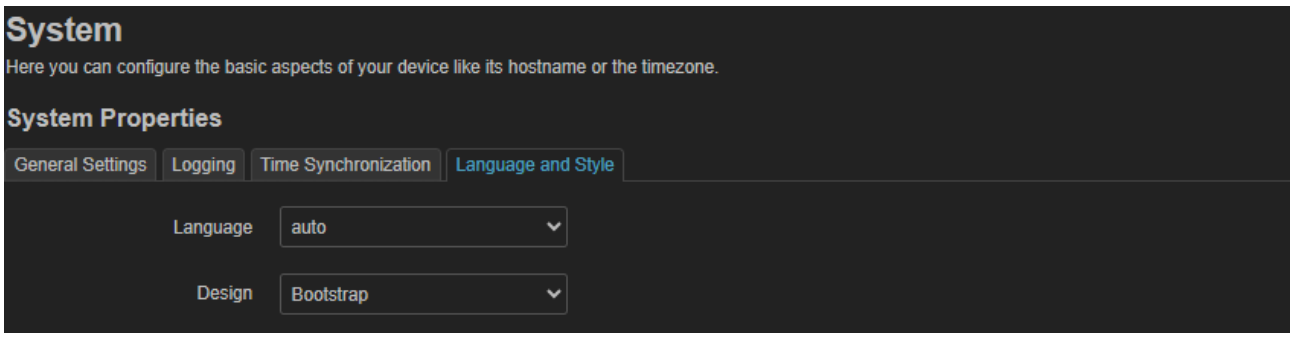
- **System log buffer size** Status > System Log 화면에 표시되는 메시지 버퍼 사이즈를 설정합니다.
- **External system log server** 로그 메시지를 수신하는 원격 서버의 IP 주소를 입력합니다.
- **External system log server port** 원격 로그 서버에서 사용되는 TCP/UDP 소켓 번호를 입력합니다.
- **External system log server protocol** 로그 서버와 세션 연결에 사용되는 TCP/UDP 프로토콜을 선택합니다.
- **Write system log to file** 장치 내부 메모리에 로그 메시지를 저장할 위치를 지정합니다.
- **Log output level** 웹 서버에 표시할 로그 메시지 종류를 선택합니다. 장애가 발생할 경우 Debug 레벨을 사용할 수 있지만 정상적인 상태에서는 Notice 또는 Warning 레벨 사용을 권장합니다. (기본값 Notice)
  - **Debug** 매우 상세한 디버그 메시지
  - **Info** 일반적인 정보 메시지, 어플리케이션의 정상적인 실행 흐름을 추적할 때 사용
  - **Notice** 정상적이지만 의미 있음 (권장)
  - **Warning** 경고 조건, 문제는 없지만 향후 문제가 될 수 있는 상황을 경고 (권장)
  - **Error** 오류 조건, 어플리케이션에서 문제 발생
  - **Critical** 위급한 상황
  - **Alert** 즉각적인 조치 필요
  - **Emergency** 시스템 사용 불가
- **Cron Log Level** 시스템 로그에 기록하는 정보의 범위 설정 (기본값 Normal)
  - **Normal** 명령어 실행 등 일반적인 정보 위주로 기록
  - **Disabled** 오류(Error) 메시지만 남기거나 로그 메시지 출력을 거의 차단(권장)
  - **Debug** 모든 디버그 메시지와 실행 내역을 출력

3.1.3 Time Synchronization



- **Enable NTP client** 체크 시 NTP 서버와 시간 정보를 자동으로 동기화 합니다.
- **Provide NTP server** 체크 시 DIVA-IAP-AX 장치를 NTP 서버로 사용합니다. (UDP 123포트)
  - **Bind NTP server** NTP 서버 기능을 제공하는 네트워크 인터페이스를 선택합니다.
- **Use DHCP advertised servers** DIVA-IAP-AX 장치가 DHCP 서버로부터 IP 주소를 할당 받을 때, DHCP 응답 메시지(옵션 42)에 포함된 NTP 서버 주소를 시스템 시간 동기화에 사용합니다. DIVA-IAP-AX 장치는 사용자가 NTP server candidates에 등록한 리스트 외에 DHCP 서버로부터 받은 NTP 서버 주소를 추가하여 시간 동기화를 시도합니다. 만약 기능을 체크하지 않으면 DHCP 서보로부터 전달받은 NTP 서버 정보를 무시하고, 사용자가 등록한 NTP server candidates 목록만 사용합니다.
- **NTP server candidates** 사용할 NTP 서버를 등록합니다.

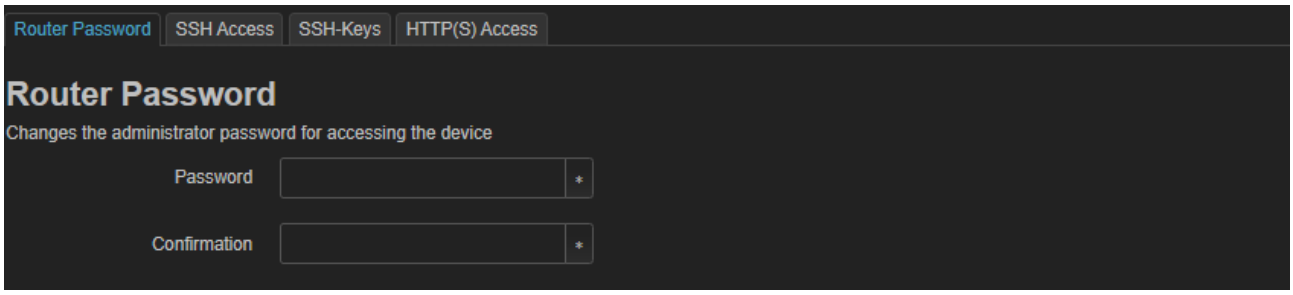
3.1.4 Language and Style



- **Language auto** 또는 **English** 중 사용할 언어를 선택합니다.
- **Design** 웹 서버 디자인을 선택합니다.
  - **Bootstrap** 사용자 브라우저 설정에 따라 자동으로 Dark/Light 모드로 전환
  - **BootstrapDark** 어두운 배경 모드
  - **BootstrapLight** 밝은 배경 모드

3.2 Administration

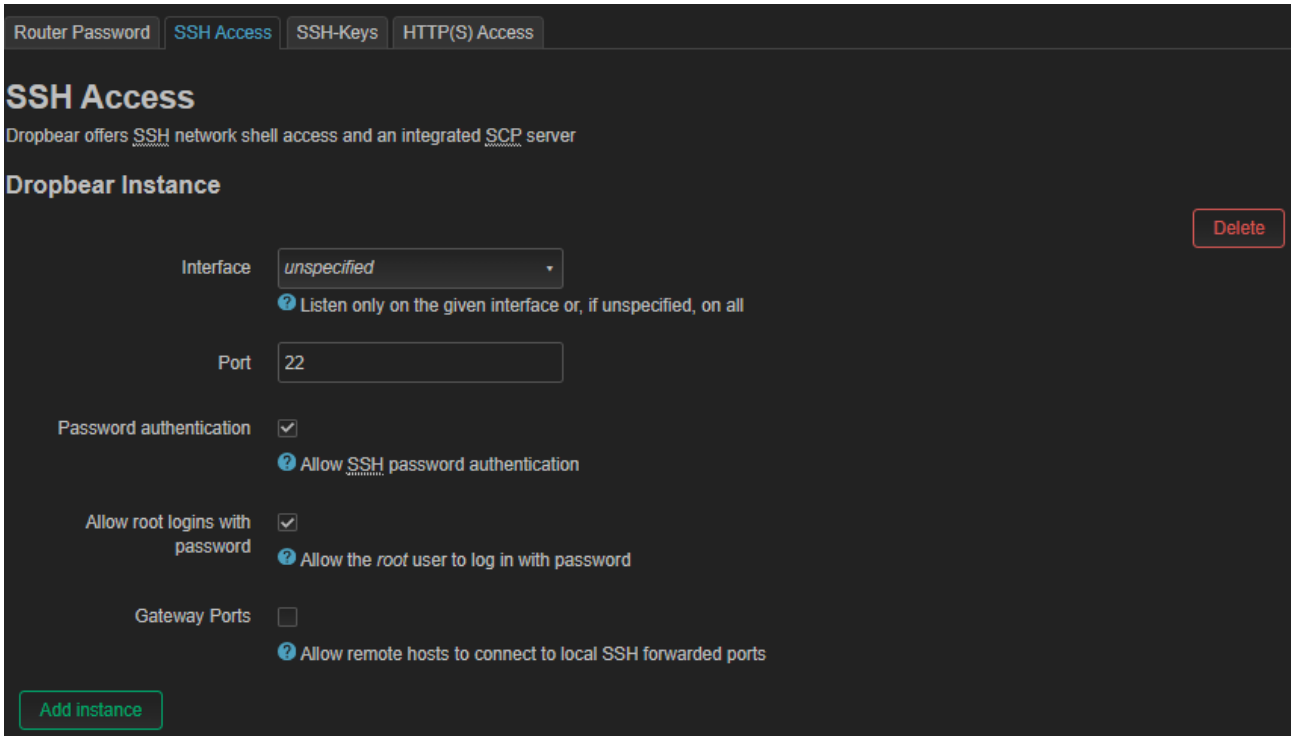
3.2.1 Router Password



- **Password** 6자리 이상의 비밀번호를 입력합니다. 값을 입력하면 하단에 비밀번호 강도가 표시됩니다.
- **Confirmation** 입력한 비밀번호 확인을 위해 다시한번 입력합니다.

비밀번호 분실 시 장치 접속이 불가능합니다. 리셋 스위치를 통해 모든 설정을 초기화하고 다시 설정해야 합니다. SYSTEM LED가 빠르게 깜빡일 때까지 RESET 스위치를 눌렀다 떼면 제품 설정이 초기화 됩니다.

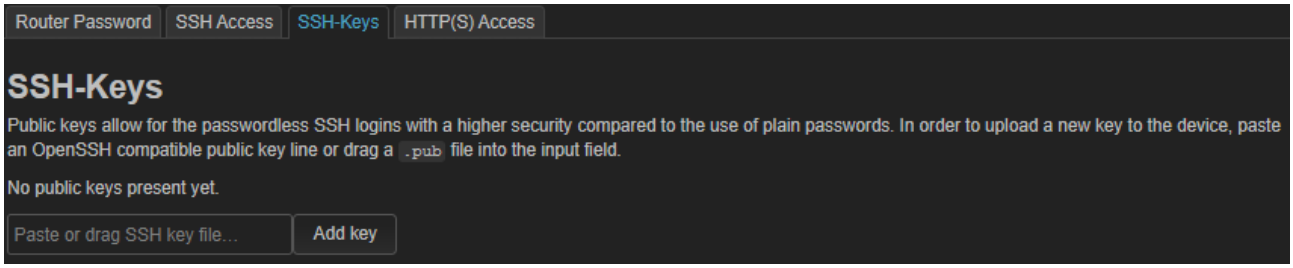
3.2.2 SSH Access



- **Interface** SSH 접속을 허가하는 네트워크 인터페이스를 선택합니다.
- **Port** 접속을 대기하는 포트 번호를 입력합니다.
- **Password authentication** 비밀번호 인증을 사용합니다.
- **Allow root logins with password** 비밀번호 인증 시 root 관리자 권한 접속을 허용합니다.
- **Gateway Ports** 원격 호스트 장치가 포트 포워딩으로 로컬 SSH로 접속하는 것을 허용합니다.
- **Delete** SSH 접속을 위한 Dropbear 인스턴스를 삭제합니다.
- **Add interface** SSH 접속을 위한 신규 Dropbear 인스턴스를 추가합니다.

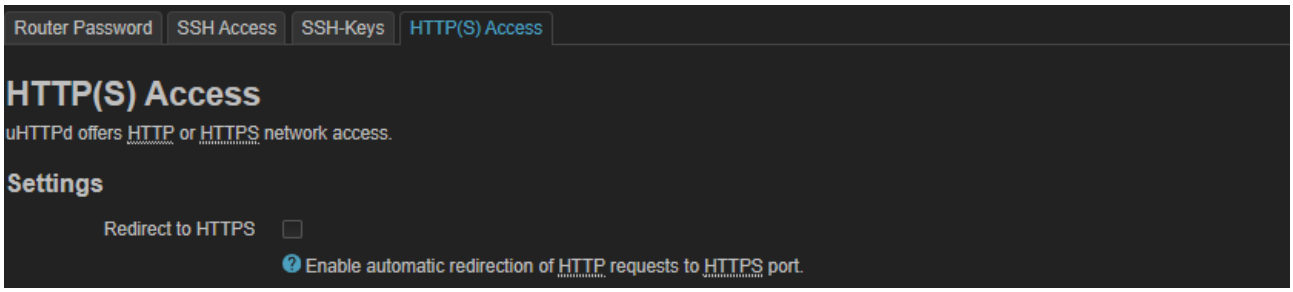
3.2.3 SSH-Keys

공개 키를 사용하면 암호 없이도 보안 수준이 높은 SSH 로그인이 가능합니다. DIVA-IAP-AX 장치에 신규 키를 업로드하려면 OpenSSH와 호환되는 공개 키 코드를 붙여 넣거나 .pub 파일을 입력 필드로 드래그 합니다.



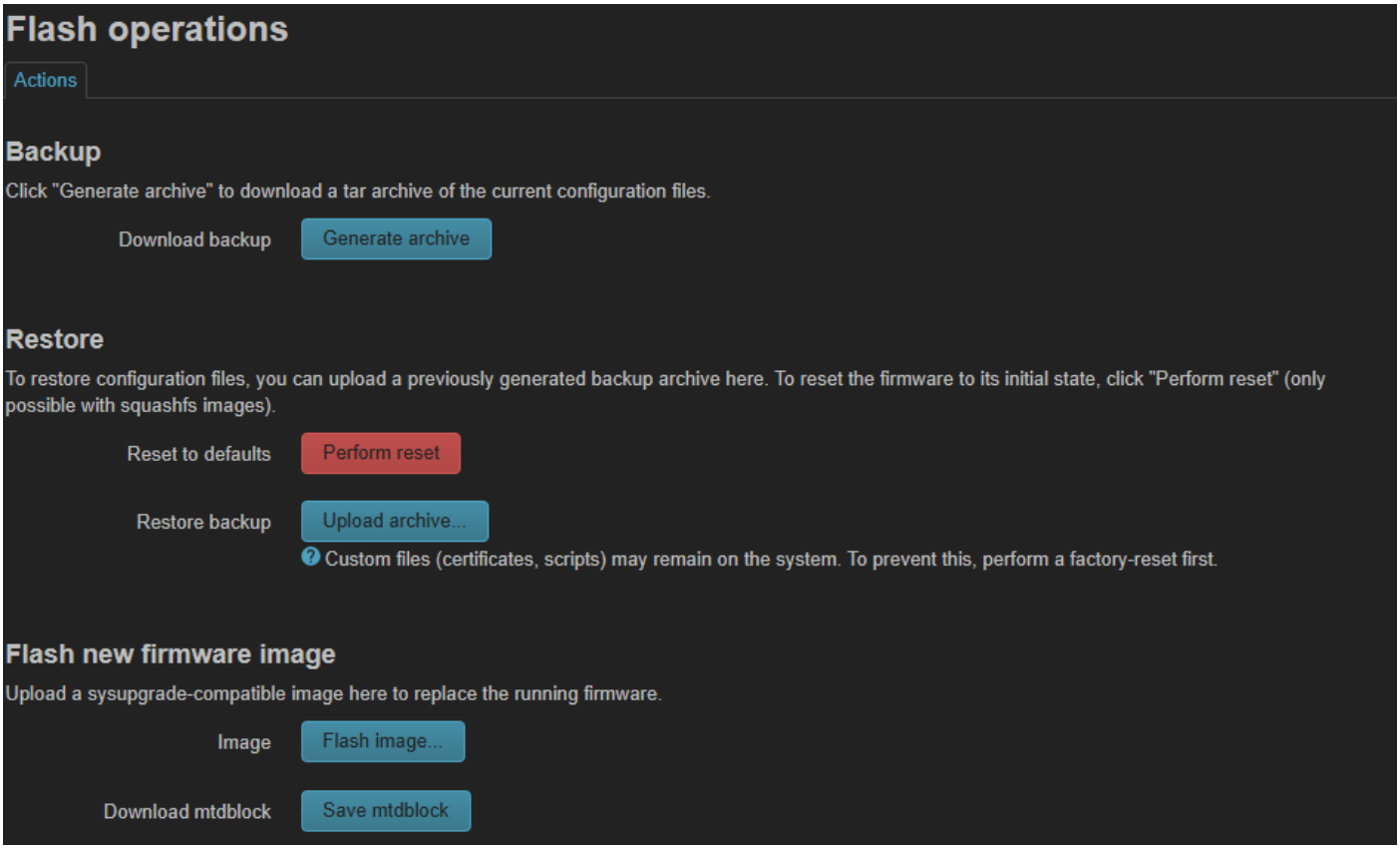
3.2.4 HTTP(S) Access

HTTP 또는 HTTPS 네트워크 접속을 설정합니다. 보안상의 이유로 외부(WAN) 접속은 기본적으로 차단되어 있으며, 내부(LAN) 접속만 허용됩니다.



- **Redirect to HTTPS** 체크 시 보안을 위해 모든 HTTP 접속을 HTTPS로 자동 전환

3.3 Backup / Flash Firmware



Backup

- **Generate archive** 현재 설정 상태를 파일로 PC에 다운로드 합니다.

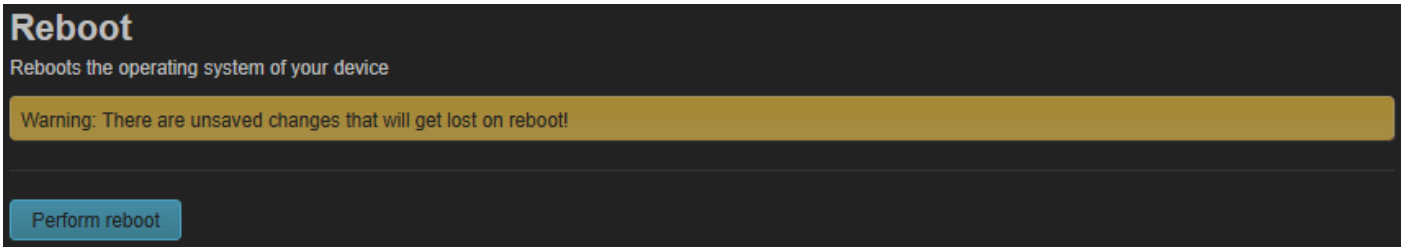
Restore

- **Perform reset** 모든 설정을 초기값으로 변경한 후 재부팅 합니다.
- **Upload archive...** PC에 저장된 설정 파일을 DIVA-IAP-AX 장치로 업로드하여 설정을 복구합니다.

Flash new firmware image

- **Flash image...** 펌웨어 버전을 확인하신 후 최신 버전으로 업그레이드 합니다.

3.4 Reboot



- **Perform reboot** 시스템을 재시작 합니다. 장치 설정을 변경한 후 Save & Apply 버튼을 클릭하면 변경된 설정 상태로 장치가 동작합니다. Reboot을 실행하여 설정이 변경된 것을 다시 한번 확인하실 것을 권장합니다.

Chapter 4: Network

유무선 인터페이스를 브리지로 구성하고 IP 주소 및 SSID, 보안과 같은 무선랜 파라미터, 방화벽을 설정합니다. DIVA-IAP-AX 장치는 네트워크 장치와 네트워크 인터페이스 개념을 통해 장치를 설정합니다.

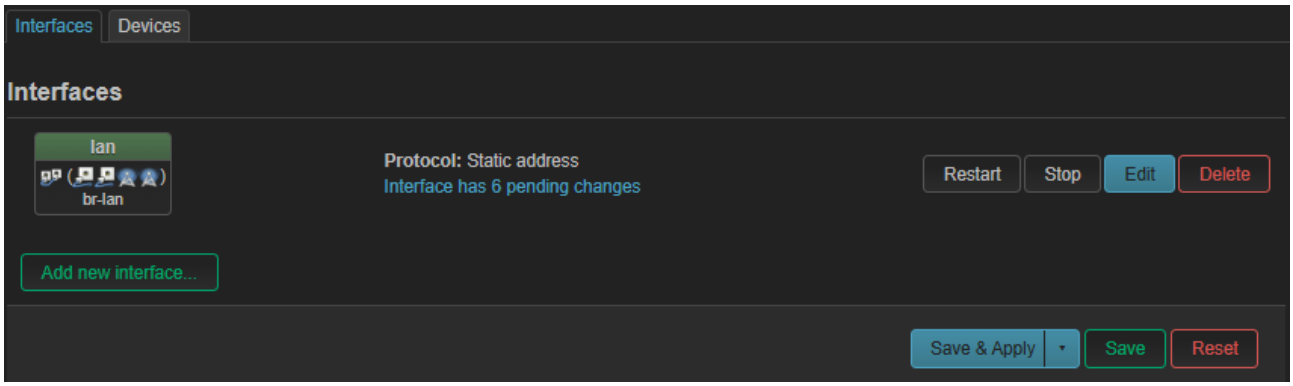
네트워크 장치는 DIVA-IAP-AX 장치에 물리적으로 존재하는 하드웨어 인터페이스 또는 이를 소프트웨어적으로 묶은 가상 장치를 의미합니다. OSI 7계층 중 L2 데이터 링크 계층에 해당하며 IP 주소를 직접 가지지 않습니다. DIVA-IAP-AX 장치에는 eth0, eth1, wlan0, wlan1 하드웨어 장치가 존재하고, 이를 가상 스위치로 연결한 브리지 장치(이름: br-lan)가 기본 제공됩니다. 각각의 하드웨어 장치를 가상랜으로 분할할 경우에도 VLAN 장치가 생성됩니다. (Network > Interfaces > Devices 설정 참조)

네트워크 장치를 논리적으로 연결하면 네트워크 인터페이스가 생성됩니다. OSI 7계층 중 L3 네트워크 계층에 해당하며 실제 IP 주소가 할당되는 항목입니다. 용도에 따라 eth0, eth1, wlan0, wlan1 네트워크 장치 중에서 LAN 과 WAN 역할로 네트워크 인터페이스를 구성할 수 있습니다. 즉 어떤 네트워크 장치를 사용하여 어떤 프로토콜로 외부 네트워크에 연결할 것인가를 정의하게 됩니다. DIVA-IAP-AX 제품은 브리지 장치(br-lan)에 "lan" 이름을 부여한 네트워크 인터페이스를 기본 제공합니다.
(Network > Interfaces > Interfaces 설정 참조)

4.1 Interfaces

일반적으로 Access Point, Access Point (WDS), Client (WDS), 802.11s 모드를 사용할 경우 모든 유무선 장치가 1개의 로컬 네트워크에 연결되기 때문에 기본 네트워크 인터페이스(lan)만 설정하여 사용할 수 있습니다. 하지만 DIVA-IAP-AX 장치를 IP 공유기처럼 사용할 경우, eth0/eth1 네트워크 장치 중 1개는 WAN(외부 네트워크) 연결을 위한 네트워크 인터페이스로 분리되고 나머지 3개의 네트워크 장치는 LAN(내부 네트워크) 연결을 위한 네트워크 인터페이스로 분리됩니다. Client 모드를 사용할 경우에도 wlan0/wlan1 네트워크 장치 중 1개는 WAN 연결을 위한 네트워크 인터페이스로 분리되고 나머지 3개의 네트워크 장치는 LAN 연결을 위한 네트워크 인터페이스로 분리됩니다.

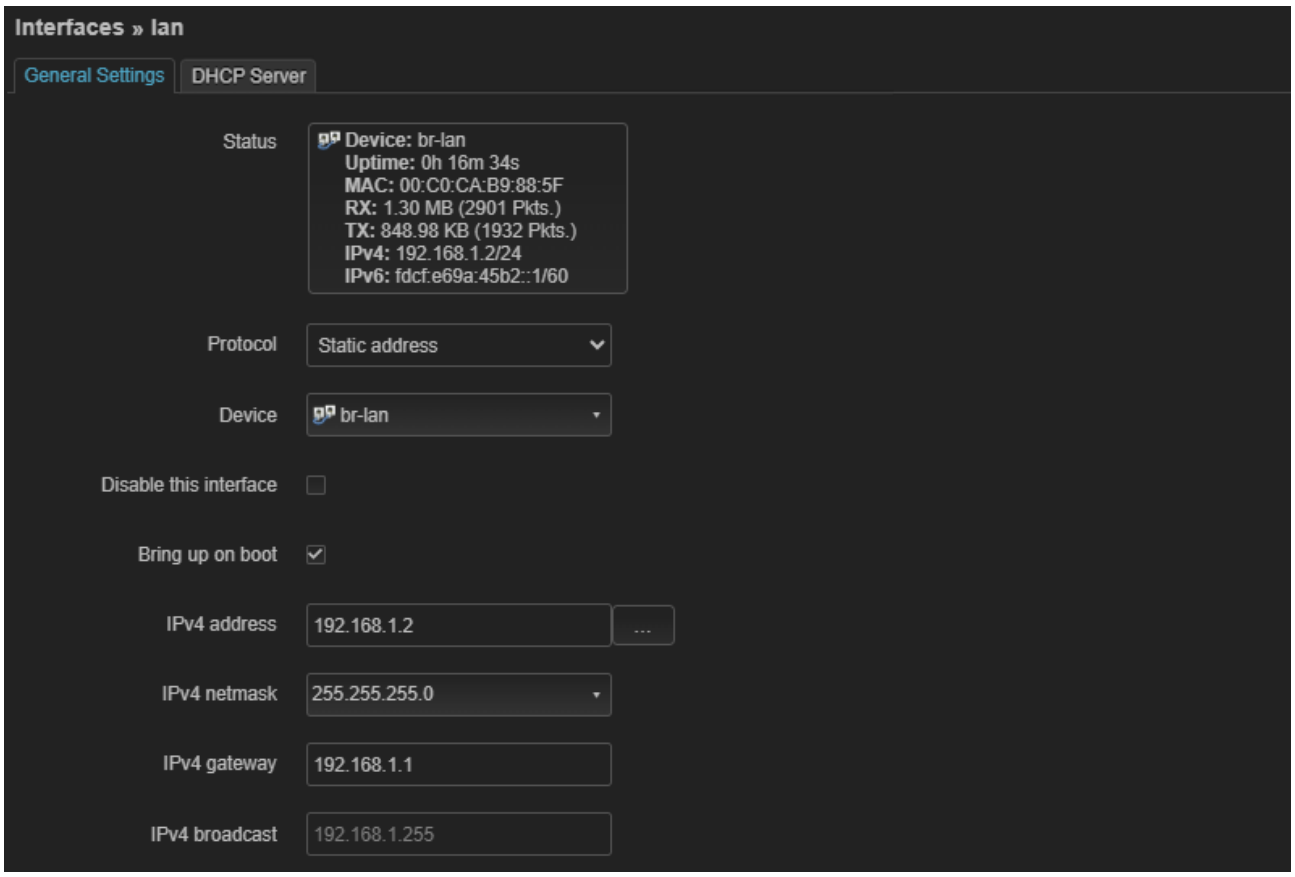
4.1.1 Interfaces 탭



- **Restart** Stop 버튼을 통해 중단된 해당 네트워크 인터페이스 프로세스를 재시작 합니다.
- **Stop** 설정 변경 및 점검을 위해 해당 네트워크 인터페이스 실행을 일시적으로 중단합니다.
- **Edit** 해당 네트워크 인터페이스 설정을 변경합니다. (다음 페이지 참조)
- **Delete** 해당 네트워크 인터페이스를 삭제합니다.
- **Add new interface...** 신규 네트워크 인터페이스를 추가합니다.

Edit 버튼을 클릭하여 해당 네트워크 인터페이스에 IP 주소를 포함한 L3 네트워크 정보를 설정합니다.

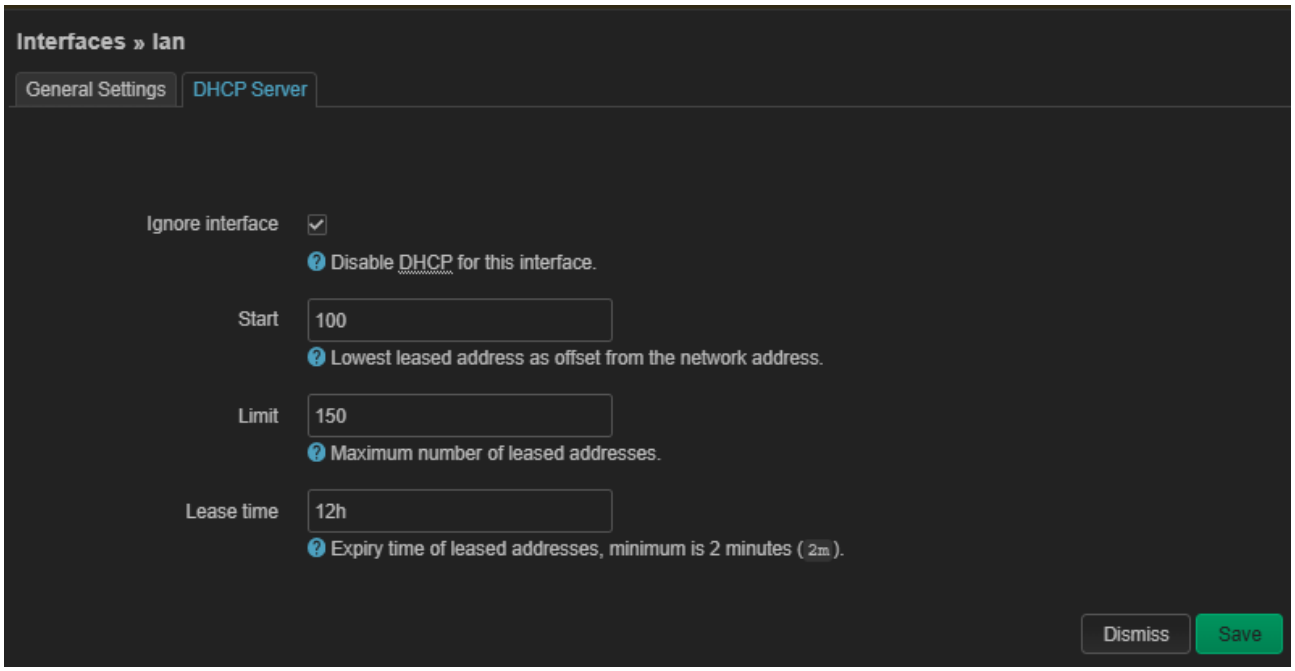
4.1.1.1 General Settings 탭



- **Force link** 물리적인 링크 상태와 관계없이 인터페이스를 항상 연결 상태로 유지합니다. 가상 브리지 인터페이스에서 WAN 케이블이 분리될 경우 방화벽/라우팅이 중단되는 것을 방지할 수 있습니다.
- **Status** 네트워크 인터페이스 설정 및 동작 상태를 표시합니다.
- **Protocol** IP 주소 사용 방식을 선택합니다.
  - **Static address** IPv4 또는 IPv6 방식의 고정 IP 주소를 사용하도록 설정합니다.
  - **DHCP client** IPv4 방식의 자동 IP 주소를 사용하도록 설정합니다.
- **Device** IP 주소가 사용되는 네트워크 장치를 선택합니다.
- **Disable this interface** 네트워크 인터페이스를 사용하지 않도록 설정합니다.
- **Bring up on boot** 시스템 부팅 시 네트워크 인터페이스가 자동 시작되도록 설정합니다.
- **IPv4 address** Static address 사용시 IP 주소를 설정합니다.
- **IPv4 netmask** Static address 사용시 네트워크 크기를 설정합니다.
- **IPv4 gateway** Static address 사용 시 게이트웨이 주소를 설정합니다.
- **IPv4 broadcast** Static address 사용 시 netmask 설정에 적합한 브로드 캐스트 주소를 설정합니다. 255.255.255.0 C 클래스 사용시 xxx.xxx.xxx.0 값은 네트워크 주소이고, xxx.xxx.xxx.255 값은 브로드 캐스트 주소입니다.
- **IPv6 address** IPv6 Static address 사용시 주소를 설정합니다.
- **IPv6 gateway** IPv6 Static address 사용 시 게이트웨이 주소를 설정합니다.
- **IPv6 routed prefix** DIVA-IAP-AX 장치를 IPv6 DHCP 서버로 사용할 경우, 내부 네트워크에 할당하는 주소 대역을 설정합니다.

- **Use default gateway** 해당 인터페이스에서 제공하는 게이트웨이를 시스템의 기본 라우팅 경로로 사용할지 여부를 설정합니다. 일반적으로 IP 공유기 기능을 사용할 때, WAN 인터페이스에서 설정하며 LAN 인터페이스에서는 설정하지 않습니다.
- **Use custom DNS servers** 해당 인터페이스에서 자동으로 할당 받은 DNS 서버를 무시하고, 사용자가 지정한 DNS 서버 주소를 사용합니다.
- **DNS search domains** 전용 내부망/사내망 이용 시, 짧은 호스트 이름을 DNS로 조회할 때 자동으로 뒤에 붙여서 검색할 도메인 목록을 설정합니다. 가정집, 소규모 사무실과 같은 일반적인 환경에서는 불필요한 DNS 질의가 증가하고 응답 지연이 발생할 수 있습니다.
- **DNS weight** 여러 인터페이스의 DNS 서버 중에서 어떤 인터페이스의 DNS를 우선적으로 사용할지 설정합니다. 값이 낮을수록 우선순위가 높아집니다. 내부 DNS 서버를 사용하거나 이중 WAN 환경에서 사용할 수 있습니다.
- **Use gateway metric** 여러 개의 기본 게이트웨이가 있을 때, 어떤 인터페이스의 게이트웨이를 우선적으로 사용할지 설정합니다. 값이 낮을수록 우선순위가 높아집니다. 이중 WAN 환경에서 사용할 수 있습니다.
- **Override IPv4 routing table** 해당 인터페이스의 IPv4 라우트를 기본(main) 테이블이 아닌, 지정한 별도의 라우팅 테이블로 변경합니다. 정책 라우팅, 고급 멀티 WAN을 구성할 때 사용될 수 있습니다. 고급 사용자를 위한 옵션으로 잘못 설정할 경우 외부 네트워크 연결이 불가능할 수 있습니다.
- **Override IPv6 routing table** 해당 인터페이스의 IPv6 라우트를 기본(main) 테이블이 아닌, 지정한 별도의 라우팅 테이블로 변경합니다. 정책 라우팅, 고급 멀티 WAN을 구성할 때 사용될 수 있습니다. 고급 사용자를 위한 옵션으로 잘못 설정할 경우 외부 네트워크 연결이 불가능할 수 있습니다.
- **Delegate IPv6 prefixes** WAN 인터페이스에 설정하는 옵션으로 해당 인터페이스를 통해 받은 IPv6 prefix를 다른 내부 인터페이스(LAN 등)에 분배할지 여부를 설정합니다. 체크할 경우, ISP 등으로부터 받은 IPv6 prefix를 LAN과 같은 다른 인터페이스에 재할당 가능하며 LAN에서는 IPv6 주소가 자동으로 생성됩니다. 체크하지 않을 경우 LAN에서 IPv6 주소가 자동으로 생성되지 않으며 내부 네트워크의 IPv6 상태가 비활성화 됩니다.
- **IPv6 assignment length** 상위 인터페이스(WAN)에서 위임받은 IPv6 prefix (Prefix Delegation, PD)를 해당 인터페이스에 어떤 길이로 할당할지 설정합니다. 일반적으로 LAN에서 60 또는 64 값을 사용하며, 값이 없으면 해당 인터페이스에 IPv6 prefix를 할당하지 않습니다. WAN 인터페이스에는 설정하지 않습니다.
  - **64** : 표준 LAN 설정 (SLAAC 정상 동작)
  - **60** : 더 큰 프리픽스 (하위 네트워크에 재분배 가능)
  - **disabled** : IPv6 비활성화
- **IPv6 assignment hint** 상위(WAN)에서 받은 IPv6 프리픽스 중에서 해당 인터페이스가 사용할 하위 프리픽스를 16진수 값으로 설정합니다. 인터페이스 순서가 변경되어도 항상 같은 IPv6 대역을 유지하거나 여러 개의 LAN을 명확히 구분할 때 사용될 수 있습니다. 단일 LAN 환경에서는 사용할 필요가 없습니다.
- **IPv6 prefix filter** 해당 인터페이스가 상위(WAN)에서 받은 여러 IPv6 프리픽스 중에서, 어떤 프리픽스만 선택하여 사용/위임할 지 제한합니다. 일부 인터넷 서비스 사업자나 상위 네트워크는 한 인터페이스에 여러 개의 IPv6 프리픽스를 동시에 제공할 수 있습니다. 원하지 않는 프리픽스가 LAN에 위임되거나 기본 라우트에 섞이는 것을 방지하기 위해 사용됩니다.
- **IPv6 suffix** 해당 인터페이스(주로 LAN)에서 사용할 IPv6 주소의 호스트 부분(하위 64비트)을 고정합니다. 보통 IPv6 주소는 [프리픽스 64비트] : [호스트 ID 64비트] 형태로 구성되며, 프리픽스는 ISP→WAN→LAN으로 자동할당 되고 호스트 ID는 랜덤(SLAAC) 또는 EUI-64 방식으로 구성됩니다. IPv6 suffix는 이 호스트 ID의 끝부분을 수동으로 지정하여 주소를 고정합니다.
- **IPv6 preference** 해당 인터페이스가 advertise 하거나 사용하는 IPv6 프리픽스/라우트의 선호도를 설정하여, 클라이언트 장치가 여러 IPv6 경로 중 선호도가 높은 경로를 우선 사용하도록 합니다.

4.1.1.2 DHCP Server 탭



- **Ignore interface** 박스를 체크하면 DIVA-IAP-AX 장치를 DHCP 서버로 사용하지 않습니다. 체크하지 않으면 DIVA-IAP-AX 장치는 네트워크에 연결된 유무선 DHCP Client 장치들에게 IP 주소를 자동으로 할당합니다. 유무선 네트워크에 설치된 다른 DHCP 서버와 충돌이 발생하지 않도록 주의하시기 바랍니다. (기본값 체크)

DHCP 서버로 사용할 경우 아래의 항목을 설정합니다.

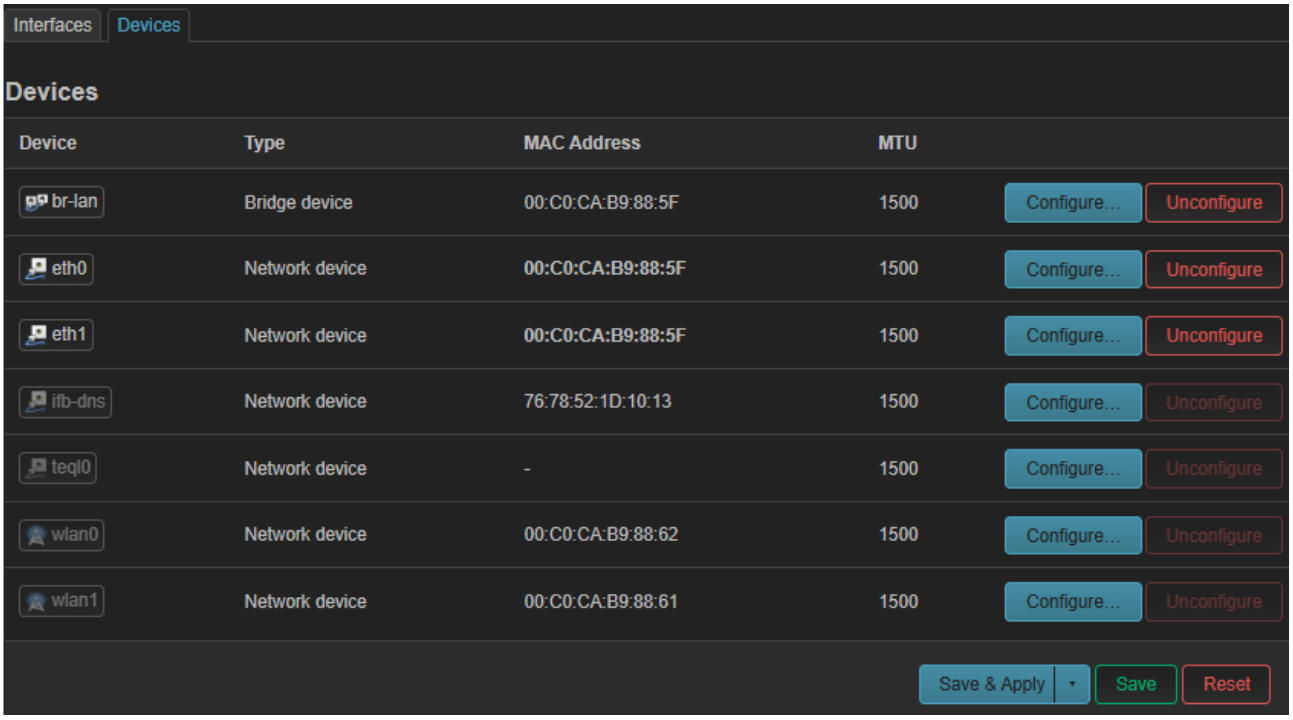
- **Start** DHCP 클라이언트 장치들에게 할당하는 IP 주소 범위의 시작 값을 입력합니다. 예를 들어 192.168.1.0 네트워크에서 100 값을 설정할 경우, DHCP 클라이언트 장치에게 192.168.1.100 IP 주소부터 할당합니다.
- **Limit** DHCP 클라이언트 장치들에게 할당할 수 있는 IP 주소의 개수를 입력합니다. 예를 들어 192.168.1.0 네트워크에서 150 값을 설정할 경우, DHCP 클라이언트 장치에게 192.168.1.100 부터 192.168.1.249 사이의 150개 IP 주소를 할당합니다.
- **Lease time** 할당된 IP 주소의 유효 시간을 분(m), 시간(h), 일(d) 단위로 설정합니다. 클라이언트 장치는 설정 시간이 경과한 후 IP 주소를 다시 할당 받아야 합니다.
  - 30m : 30분
  - 12h : 12시간
  - 1d : 1일
- **Dynamic DHCP** 해당 인터페이스에 DHCP/RA 설정을 자동으로 적용할지 선택합니다. 주로 IPv6 Prefix Delegation으로 만들어진 동적 내부 인터페이스에 적용됩니다. 체크하면 동적으로 생성된 인터페이스에 DHCPv6/RA 서버 설정을 자동으로 적용합니다. IPv4 사용 시 설정할 필요가 없습니다.
- **Force** DHCP 클라이언트 장치의 요청 여부와 상관없이 해당 인터페이스에 정의된 DHCP 옵션을 강제로 적용합니다. 일반적인 환경에서는 사용되지 않으며, DHCP 표준을 따르지 않는 일부 임베디드 장치, 오래된 네트워크 장치에 강제로 네트워크 설정을 전달합니다. 체크하지 않으면 표준 DHCP 서버로 동작하며 DHCP Discover / Request 메시지를 보낸 클라이언트 장치에게만 IP 주소와 옵션을 할당합니다.
- **IPv4-Netmask** DHCP 클라이언트 장치에 전달할 IPv4 서브넷 마스크를 수동으로 지정합니다. 대부분의 환경에서 수동으로 설정할 필요가 없습니다. 체크하지 않으면 해당 인터페이스의 IP 주소와 넷마스크 값을 기준으로 서브넷 마스크를 자동으로 생성합니다.

- **DHCP-Options** DHCP 서버가 클라이언트 장치에게 전달할 DHCP 옵션을 수동으로 지정합니다. DHCP 서버는 IP 주소 외에도 옵션 번호를 통해 여러 개의 네트워크 정보를 전달합니다. 잘못된 옵션 번호를 설정할 경우 네트워크 장애를 발생할 수 있으며, 기본 DHCP 서버 설정과 충돌할 수 있습니다.
  - **Option 1 :** Subnet Mask
  - **Option 3 :** Default Gateway
  - **Option 6 :** DNS Server
  - **Option 15 :** Domain Name
  - **Option 42 :** NTP Server
  - **Option 66 :** TFTP Server (PXE)
  - **Option 67 :** Boot Filename (PXE)
  - **Option 119 :** Domain Search
- **Designated master** 네트워크에 여러 개의 DHCP 서버가 있을 경우, 해당 DHCP 서버를 네트워크의 마스터(우선) DHCP 서버로 지정합니다. 단일 DHCP 서버 환경에서는 설정할 필요가 없습니다. 체크하면 DIVA 장치는 마스터 DHCP 서버로 선언하고 DHCP Discover에 더 적극적으로 응답하여 클라이언트가 해당 서버를 선택할 가능성을 높입니다. 하지만 다른 DHCP 서버와의 충돌 가능성을 차단할 수는 없으며 네트워크에서 단일 DHCP 서버만 사용할 것을 권장합니다.
- **RA-Service** 해당 인터페이스에서 IPv6 Router Advertisement(RA)를 어떻게 제공할지 선택합니다. RA는 IPv6에서 클라이언트가 IPv6 주소, 기본 게이트웨이, DNS 정보를 자동으로 설정하는 기능입니다.
  - **disabled** 해당 인터페이스에서 RA 보내지 않음. 클라이언트에서 IPv6 주소 생성 안됨, IPv4 네트워크
  - **server mode** DIVA 장치가 IPv6 RA 서버로 동작, 클라이언트가 SLAAC로 IPv6 주소 생성
  - **relay mode** 해당 인터페이스에서 RA를 생성하지 않고 상위 인터페이스(WAN)의 RA 중계
  - **hybrid mode** RA + DHCPv6 혼합 모드, SLAAC 주소와 DHCPv6 옵션 제공
- **Default router** IPv6 RA에서 기본 라우터(기본 게이트웨이) 광고 방식을 선택합니다.
  - **automatic** 가장 안전하고 일반적인 설정으로 해당 인터페이스에 정상적인 IPv6 연결이 있을 때만 기본 라우터로 자신을 자동 광고합니다.
  - **on available prefix** 업스트림 IPv6 경로가 완전히 준비되지 않아도 자신을 기본 라우터로 광고합니다. 내부 IPv6 통신 시험은 가능하지만 외부 IPv6 통신이 연결되지 않을 수 있습니다.
  - **forced** 업스트림 상태와 무관하게 항상 자신을 IPv6 기본 라우터로 광고합니다. IPv6 경로가 없어도 클라이언트 장치는 무조건 DIVA 장치로 IPv6 트래픽을 전송합니다.
- **Enable SLAAC** 해당 인터페이스에서 IPv6 주소를 SLAAC(Stateless Address Autoconfiguration) 방식으로 자동 생성하도록 허용할지 선택합니다. 체크하면 DIVA 장치는 RA에 Prefix Information Option(PIO)를 포함하여 전송하고, 클라이언트 장치는 자동으로 IPv6 주소를 생성합니다.
- **RA Flags** IPv6 RA 메시지에 포함되는 플래그 비트를 설정합니다. 플래그 비트는 클라이언트 장치가 IP 주소를 어떻게 받을지 지시합니다. 안드로이드 운영체제 기반의 클라이언트 장치는 DHCPv6 버전이 호환되지 않습니다. 일반적으로 DIVA 장치에 다양한 운영체제를 사용하는 장치들을 모두 연동하기 위하여 managed config (M) 설정은 체크하지 않고, other config (O) 설정은 체크합니다. 이러한 방식은 주소는 SLAAC, DNS 및 기타 정보는 DHCPv6 방식으로 할당 받도록 합니다.
  - **managed config (M)** 클라이언트 장치는 DHCPv6 서버로부터 IPv6 주소를 할당 받습니다.
  - **other config (O)** 클라이언트 장치는 DHCPv6 서버로부터 DNS 등 추가 정보만 받습니다.
- **NAT64 prefix** IPv4 주소를 IPv6 주소로 매핑할 때 사용되는 프리픽스를 설정합니다. IPv6 버전만 지원하는 클라이언트 장치가 IPv4 장치에 접근할 수 있도록 NAT64 prefix 정보를 RA 또는 DHCPv6를 통해 클라이언트 장치에 광고합니다.

- **Max RA interval** 주기적으로 전송되는 IPv6 RA 메시지 사이의 최대 전송 간격을 초단위로 설정합니다. 기본값 600은 600초, 즉 10분을 의미합니다. 실제 전송 간격은 트래픽 폭주를 방지하기 위하여 Min RA Interval ~ Max RA Interval 설정 값 사이에서 무작위로 결정됩니다. 설정 값이 너무 크면 클라이언트 장치가 IPv6 연결이 끊어진 것을 늦게 감지하는 문제가 발생할 수 있습니다. 일반적으로 기본값 600초 사용을 권장하며 이동/불안정한 네트워크에서는 30~120초 사이의 값을 사용할 수 있습니다.
- **Min RA interval** 주기적으로 전송되는 IPv6 RA 메시지 사이의 최소 전송 간격을 초단위로 설정합니다. 실제 전송 간격은 트래픽 폭주를 방지하기 위하여 Min RA Interval ~ Max RA Interval 사이에서 무작위로 결정됩니다.
- **RA Lifetime** 기본 라우터 유효 시간을 초단위로 설정합니다. IPv6 RA 메시지에서 DIVA 장치를 기본 게이트웨이로 신뢰해도 되는 시간을 의미하며 클라이언트 장치는 설정된 시간 동안 DIVA 장치를 IPv6 기본 게이트웨이로 유지하고, 신규 RA 메시지를 수신하면 타이머를 리셋합니다. 0 ~ 9000초 이내의 값을 사용할 수 있으며 일반적으로 Max RA Interval 설정 값의 3배 이상을 권장합니다.
- **RA MTU** IPv6 클라이언트 장치에게 해당 네트워크에서 사용할 MTU(Maximum Transmission Unit) 값을 통보합니다. 기본값 1500 사용을 권장합니다.
- **RA Hop Limit** 클라이언트 장치가 기본값으로 사용할 IPv6 Hop Limit (TTL에 해당) 값을 설정합니다. Linux 운영체제 장치는 기본값 64, Windows 장치는 기본값 128을 사용하며 일반적으로 64값이 가장 많이 사용됩니다.
- **DHCPv6-Service** IPv6 DHCP 서버 동작 모드를 선택합니다.
  - **disabled IPv6** DHCPv6 서버 비활성화, 주소/옵션을 제공하지 않음. SLAAC 만 가능
  - **server mode** DHCPv6 서버로 동작, IPv6 주소 및 DNS, NTP 등 옵션 제공
  - **relay mode** 해당 인터페이스에서 수신한 DHCPv6 요청을 다른 DHCPv6 서버로 중계
  - **hybrid mode** 주소는 SLAAC로 자동 생성하고, DNS, NTP 등의 추가 정보는 DHCPv6로 제공합니다. 실제 동작은 아래와 같이 설정한 것과 같습니다.
    - ✓ RA-Service: Server
    - ✓ Enable SLAAC: ON
    - ✓ RA Flags: other configuration check
    - ✓ DHCPv6-Service: Server
- **Announced IPv6 DNS servers** IPv6 환경에서 클라이언트 장치가 사용할 DNS 서버를 설정합니다. 값을 입력하지 않으면 해당 인터페이스의 IPv6 주소를 DNS로 광고하고 해당 DNS 요청을 상위 DNS로 포워딩합니다.
- **Local IPv6 DNS server** 해당 인터페이스의 IPv6 주소를 DNS로 광고하고 해당 DNS 요청을 상위 DNS로 포워딩합니다. Announced IPv6 DNS servers 설정과 상호 보완.
- **Announced DNS domains** 클라이언트 장치가 짧은 호스트 이름을 사용할 때 자동으로 붙여서 검색할 도메인 목록을 설정합니다. Local DNS, DNS 서버 옵션과의 관계는 다음과 같습니다.
  - Announced DNS domains : 자동으로 붙일 도메인 역할
  - Local IPv6 DNS server : DNS 서버 주소 역할
  - Announced IPv6 DNS servers : 어떤 DNS 서버를 사용할지 정보 제공
- **NDP-Proxy** IPv6 Neighbor Discovery Protocol을 해당 인터페이스에서 어떻게 처리할지 설정합니다.
  - **disabled** 기본값으로 NDP 프록시 사용 안함
  - **relay mode** 해당 인터페이스에서 받은 Neighbor Solicitation을 다른 인터페이스로 그대로 전달
  - **hybrid mode** 일부 주소는 직접 응답하고 일부 주소는 중계, 라우터 및 프록시 동시 수행
- **IPv6 Prefix Lifetime** IPv6 네트워크 주소 범위의 유효 시간 설정
- **Follow IPv4 Lifetime** IPv6 주소/프리픽스 유효 시간을 IPv4 DHCP 임대 시간과 자동으로 맞추는 옵션

4.1.2 Devices 탭

DIVA-IAP-AX 장치는 아래와 같이 7개의 기본 네트워크 장치를 제공합니다. 사용자 용도에 따라 사용하지 않는 장치를 제거할 수 있습니다.

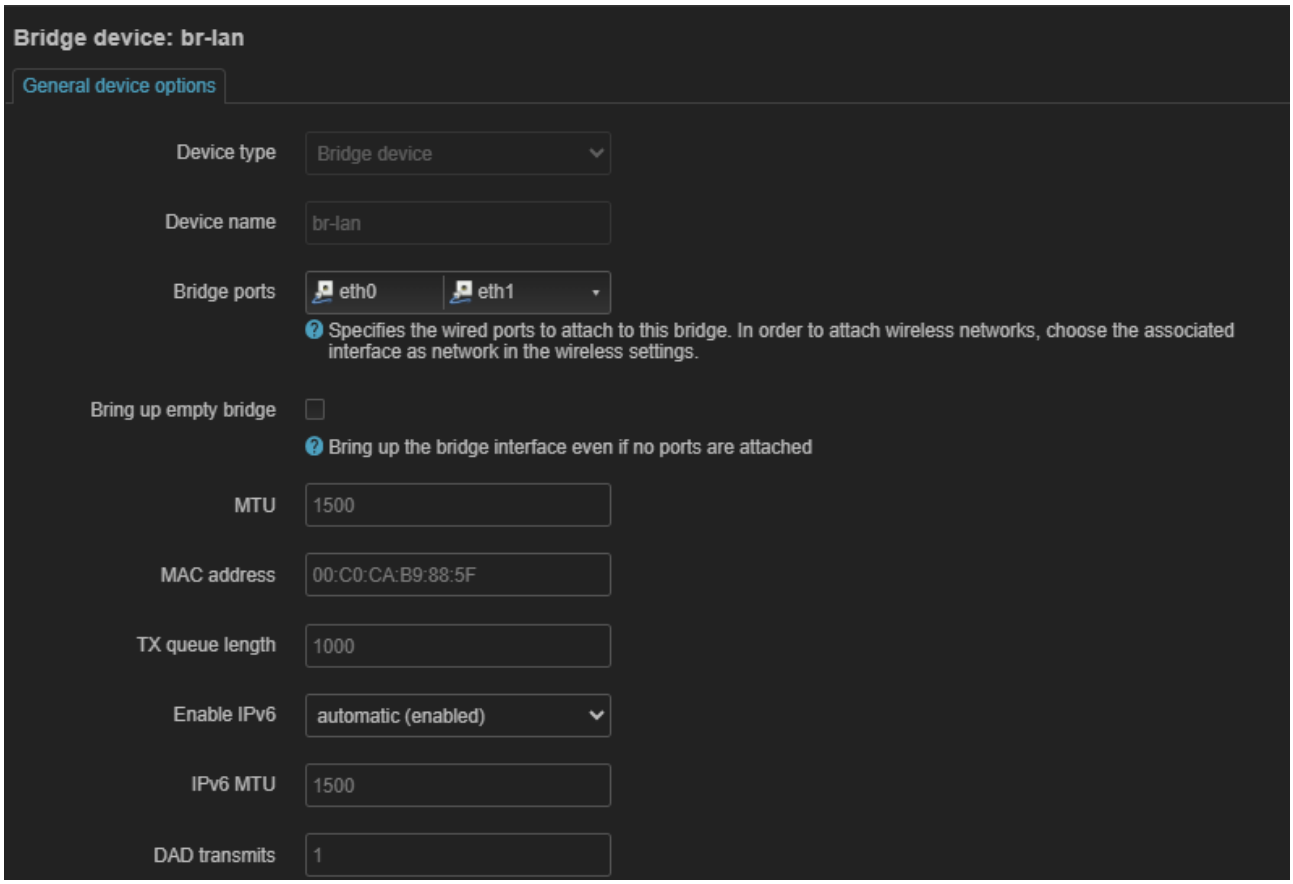


- **br-lan** 가상의 네트워크 장치로서 가상 스위치를 통해 eth0, eth1, radio0, radio1 네트워크 장치를 연결
- **eth0** 하드웨어 네트워크 장치로서 ETH1(PoE) 포트
- **eth1** 하드웨어 네트워크 장치로서 ETH2 포트
- **ifb-dns** 가상의 네트워크 장치로서 DNS 트래픽을 SQM/QoS 제어하거나 처리
- **teql0** 가상의 네트워크 장치로서 여러 네트워크 인터페이스를 라운드로빈 방식으로 묶어 트래픽을 분산
- **wlan0** 하드웨어 네트워크 장치로서 5GHz 무선랜 인터페이스
- **wlan1** 하드웨어 네트워크 장치로서 2.4GHz 무선랜 인터페이스

- **Configure...** 해당 네트워크 장치에 MAC 주소를 포함한 L2 네트워크 정보를 설정합니다.
- **Unconfigure** 해당 네트워크와 관련 설정을 삭제하고 장치를 제거합니다. ifb-dns, teql0, wlan0, wlan1 장치는 기본 네트워크 장치로서 삭제가 불가능합니다.

Configure... 버튼을 클릭하여 각각의 장치 설정을 변경할 수 있습니다.

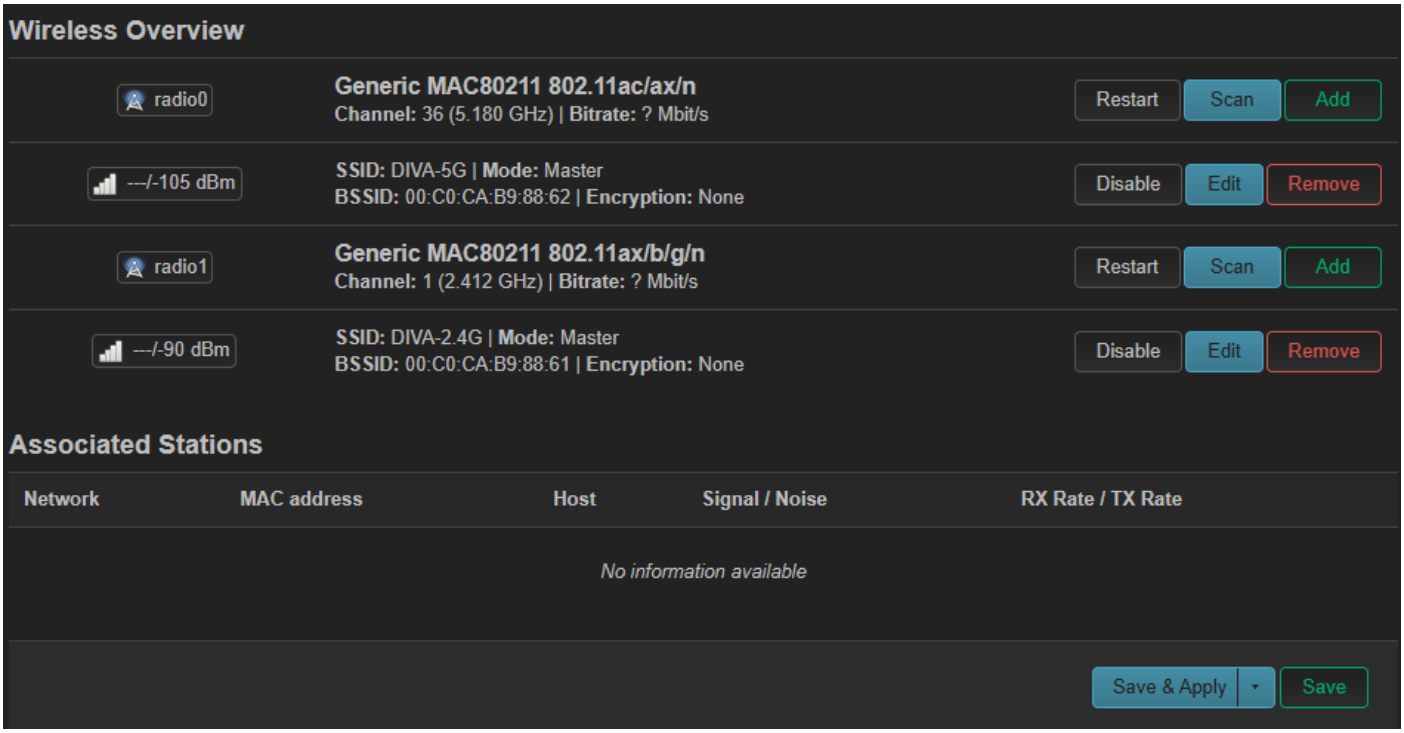
[페이지 계속]



- **Device type** 해당 네트워크 장치의 타입을 표시합니다.
  - **Bridge device** br-lan 브리지 장치, Spanning Tree Protocol 기반으로 네트워크 루프 감지 및 차단
  - **Network device** eth0, eth1, wlan0, wlan1, ifb-dns, teql0 네트워크 장치 해당
- **Device name** 네트워크 장치 이름을 표시합니다.
  - **br-lan** 브리지 네트워크 장치 이름
  - **eth0** ETH1(PoE) 유선랜 포트의 장치 이름, **eth1** ETH2 유선랜 포트의 장치 이름
  - **ifb-dns** SQM/QoS 트래픽 제어 가상 네트워크 장치 이름, **teql0** 트래픽 분산 가상 네트워크 장치 이름
  - **wlan0** 5GHz 무선랜 인터페이스 장치 이름, **wlan1** 2.4GHz 무선랜 인터페이스 장치 이름
- **Bridge ports** 가상 스위치로 무선랜과 연결할 장치 선택, 브리지 장치에서만 표시
  - **eth0** ETH1(PoE) 유선랜 포트, **eth1** ETH2 유선랜 포트
  - **Ethernet Adapter: "ifb-dns"** 트래픽 제어 가상 네트워크 장치
  - **Ethernet Adapter: "teql0"** 트래픽을 분산 가상 네트워크 장치
- **Bring up empty bridge** 부팅 시 브리지 장치에 아무 포트가 연결되어 있지 않아도 브리지 기능을 켭니다. 물리적인 포트가 빠지거나 링크 다운이 발생해도 IP 접속이 가능합니다. 브리지 장치에서만 표시 (기본값 체크)
- **Existing device** eth0, eth1, ifb-dns, teql0, wlan0, wlan1 장치 해당
- **MTU** 해당 네트워크 장치를 통해 전송할 수 있는 최대 데이터 크기를 설정합니다. (기본값 1500)
- **MAC address** 해당 네트워크 장치의 MAC 주소를 설정합니다. 기본값 사용 권장
- **TX queue length** 송신 큐에 쌓아 둘 수 있는 패킷 개수를 설정합니다. 기본값 사용 권장
- **Enable IPv6** IPv6 사용 여부를 설정합니다.
- **IPv6 MTU** IPv6 사용 시 MTU 값을 설정합니다.
- **DAD transmits** IPv6 사용 시 중복 주소 탐지를 위해 전송할 NS(Neighbor Solicitation) 패킷 개수를 설정합니다.

4.2 Wireless

무선랜 동작 모드 및 네트워크 이름, 보안 등을 설정합니다. radio0 인터페이스에서는 5GHz 무선랜을 설정하고, radio1 인터페이스에서는 2.4GHz 무선랜을 설정합니다.

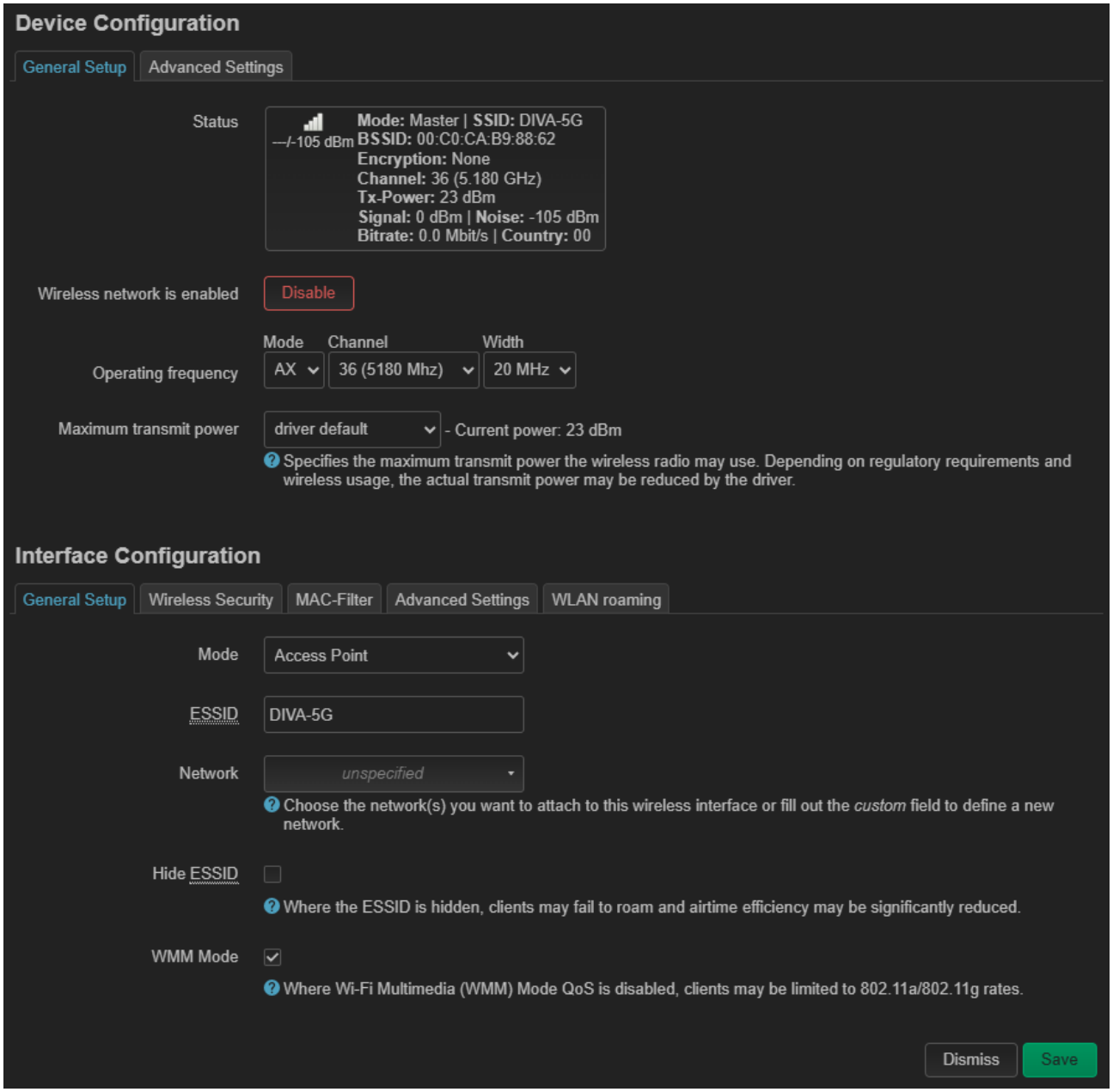


- **radio0**
  - **Restart** 5GHz 무선랜 하드웨어 인터페이스를 재시작 합니다.
  - **Scan** 5GHz 무선랜을 검색하고 연결합니다. 무선랜 검색 기능은 Client, Client (WDS), 802.11s, Monitor 모드에서 동작합니다. Edit 버튼을 클릭 후 Interface Configuration > General Setup > Mode 항목을 수정하시기 바랍니다.
  - **Add** 5GHz 대역에 최대 8개의 가상 무선 장치를 등록하여 사용할 수 있습니다. 등록된 장치 간에 네트워크 루프 및 충돌이 발생하지 않도록 사용하지 않는 가상 장치는 Disable 상태로 변경하시기 바랍니다.
    - ✓ **Access Point 모드** 최대 8개 등록, 8개 동시 동작 가능
    - ✓ **Client** 최대 8개 등록, 등록된 가상 장치 중 1개만 동작(Enable) 설정
    - ✓ **Access Point (WDS)** 최대 8개 등록, 등록된 가상 장치 중 1개만 동작(Enable) 설정
    - ✓ **Client (WDS)** 최대 8개 등록, 등록된 가상 장치 중 1개만 동작(Enable) 설정
    - ✓ **802.11s** 최대 8개 등록, 등록된 가상 장치 중 1개만 동작(Enable) 설정
  - **Disable** 해당 5GHz 무선 장치를 동작하지 않도록 설정합니다.
  - **Enable** 해당 5GHz 무선 장치를 동작하도록 설정합니다.
  - **Edit** 해당 5GHz 무선 장치 설정을 변경합니다.
  - **Remove** 해당 5GHz 무선 장치를 제거합니다.

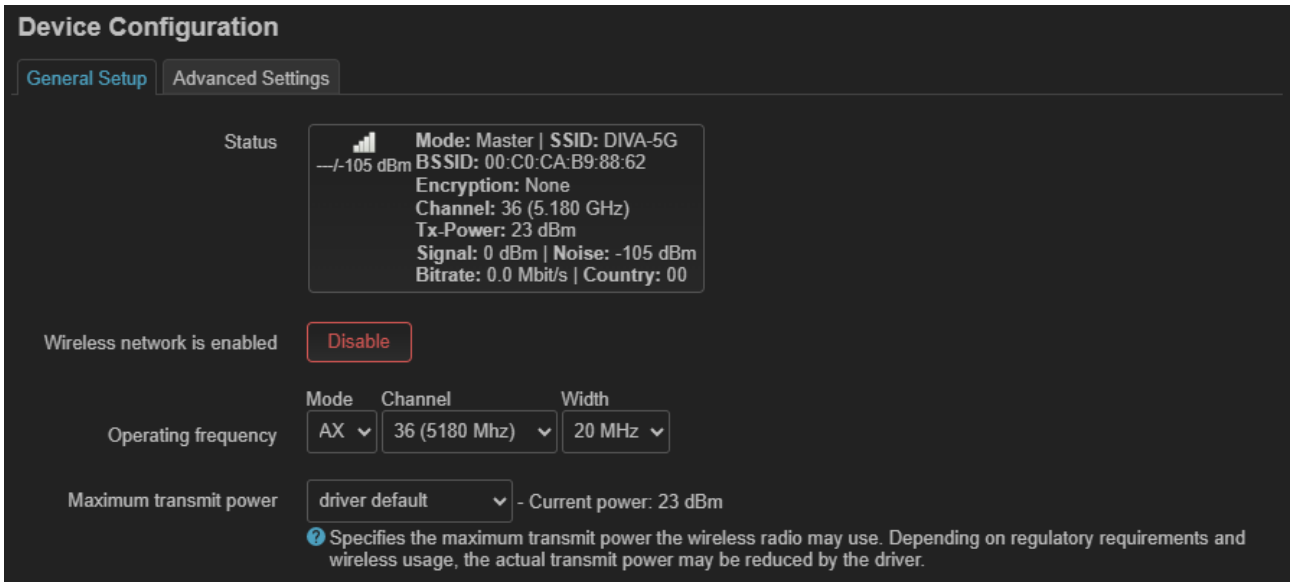
- **radio1**
  - **Restart / Scan / Add** radio0 버튼과 동일
  - **Disable / Enable / Edit / Remove** radio0 버튼과 동일

4.2.1 Edit (radio0 / radio1 공통)

상단 Device Configuration 섹션과 하단 Interface Configuration 섹션으로 설정이 구분됩니다. Device Configuration 섹션은 실제 하드웨어와 관련된 항목을 설정하고, Interface Configuration 섹션은 논리적인 동작 모드 및 보안 등을 설정합니다. 각각의 항목을 변경할 때마다 설정을 저장할 필요가 없으며 모든 항목을 변경한 후 하단 Save 버튼을 클릭하시기 바랍니다.

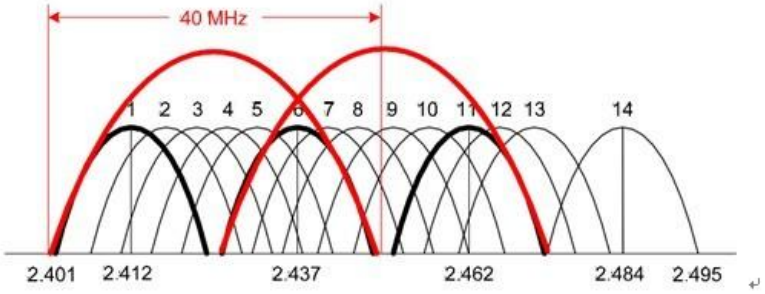


4.2.1.1 Device Configuration > General Setup

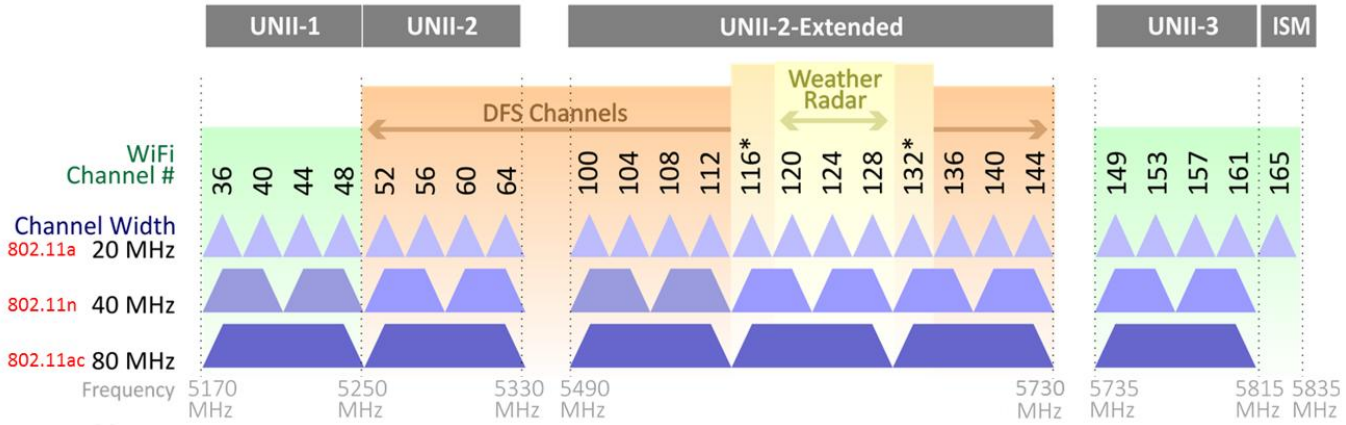


- **Status** 설정값 및 연결 상태를 표시합니다.
- **Wireless network is enabled** 해당 장치를 사용할 경우 'Wireless network is enabled' 상태 정보가 표시되고 장치 동작을 차단할 수 있도록 Disable 버튼이 표시됩니다. Disable 버튼을 클릭하면 'Wireless network is disabled' 상태로 변경되고 장치를 다시 동작 시킬 수 있도록 Enable 버튼이 표시됩니다.
- **Operating frequency** 주파수 관련 모드, 채널, 채널 대역폭을 설정합니다.
  - **Mode** 주파수에 따라 동작 모드를 설정합니다.
    - ✓ **radio0** 5GHz 대역에서 **N / AC / AX** 모드 중 선택, 모드에 따라 최대 전송 속도가 변경됩니다. 구형 무선랜 장비와 호환 문제가 발생할 경우 AX - AC - N 순서대로 모드를 변경하시기 바랍니다.
    - ✓ **radio1** 2.4GHz 대역에서 **Legacy / N / AX** 모드 중 선택, 모드에 따라 최대 전송 속도가 변경됩니다. 구형 무선랜 장비와 호환 문제가 발생할 경우 AX - N - Legacy 순서대로 모드를 변경합니다.
  - **Channel Auto** 설정을 사용하거나 특정 채널을 선택할 수 있습니다. 채널 간섭이 발생하지 않도록 주변 채널과 4-5채널 떨어진 채널을 사용합니다. Auto 설정 시, DIVA-IAP-AX 장치는 부팅 후 5GHz 또는 2.4GHz 대역의 모든 채널을 검색하여 사용률이 낮은 채널을 자동으로 사용합니다. Client 및 Client (WDS) 모드에서 채널을 직접 지정하면 선택한 채널만 탐색하여 검색 프로세스를 빠르게 완료할 수 있고 원하지 않는 액세스 포인트 장치들을 필터링 합니다. Auto 설정 시 SSID 가 같은 액세스 포인트 장치 중에서 신호 품질이 가장 우수한 액세스 포인트 장치로 자동 연결됩니다.

    2.4GHz 대역에서는 20MHz 채널 대역폭을 사용할 때 3개의 비중첩 채널만 사용할 수 있습니다. 40MHz 채널 대역폭을 사용할 경우 비중첩 채널로 무선 네트워크를 구성하는 것이 불가능합니다.

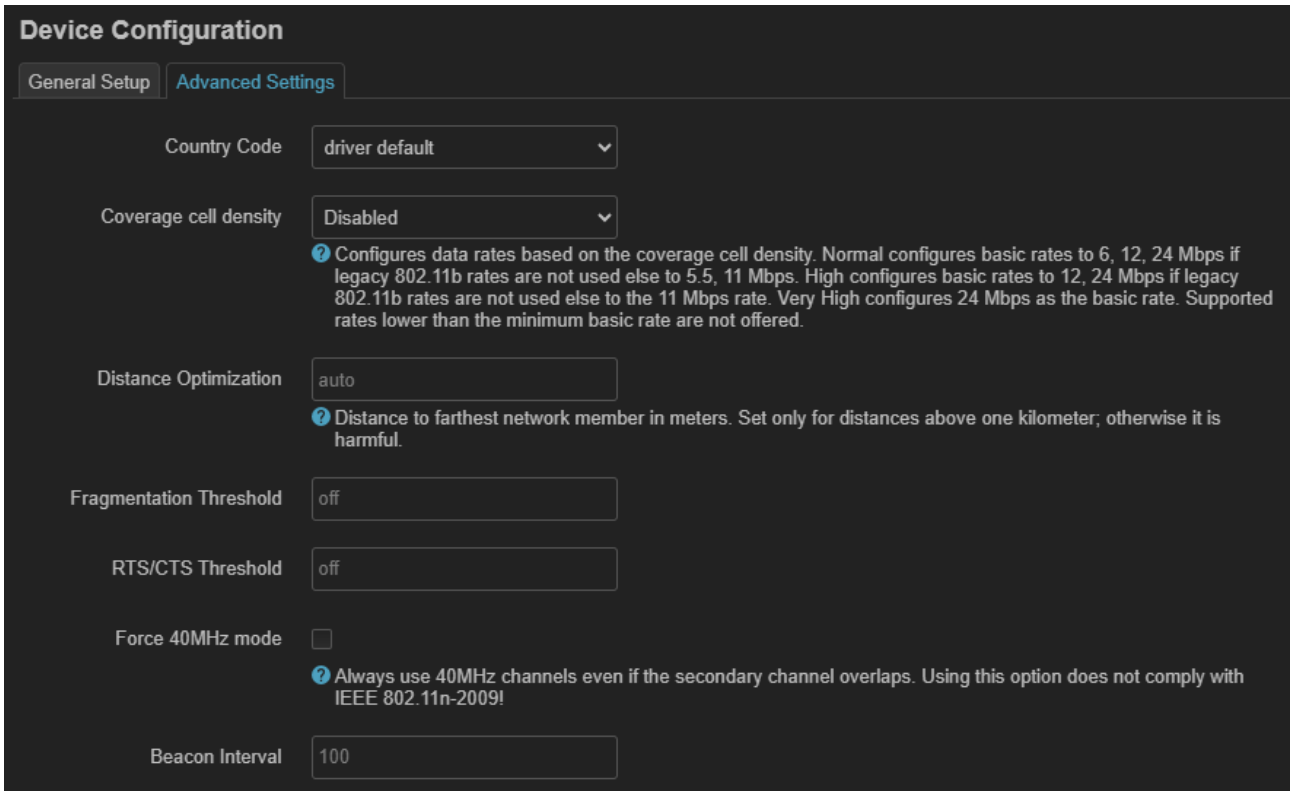


2.4GHz 대역과 달리 5GHz 대역은 비교적 많은 채널이 제공되어 채널이 중첩되지 않도록 무선랜 네트워크를 설계하는 것이 유리합니다. 실외에서 52번부터 140번 사이의 DFS 채널 사용 시 레이더 시스템 영향으로 1~10분간 무선 연결이 끊어질 수 있습니다.



- **Width** 채널 대역폭을 설정합니다. 채널 대역폭이 넓을 수록 고속 통신에 유리하지만, 채널 간섭 가능성도 증가하여 무선랜 성능이 떨어질 수 있습니다. 채널 대역폭이 작으면 비중첩 채널 수가 증가하여 네트워크 확장성을 높일 수 있고 채널 당 파워 스펙트럼 밀도가 증가하여 장거리 통신에 유리합니다.
  - ✓ **radio0** 5GHz 무선랜 인터페이스는 N 모드에서 **20MHz** 대역폭과 **40MHz** 대역폭을 사용할 수 있고, AC/AX 모드에서 **20, 40, 80MHz** 채널 대역폭을 사용할 수 있습니다.
  - ✓ **radio1** 2.4GHz 무선랜 인터페이스는 Legacy 모드에서 **20MHz**, N/AX 모드에서 **20MHz** 와 **40MHz** 채널 대역폭을 사용할 수 있습니다. 40MHz 채널 대역폭을 사용하면 비중첩 채널 설계가 불가능하여 결국 액세스 포인트 장치의 성능이 떨어지게 됩니다.
- **Maximum transmit power** 2.4/5GHz 대역의 무선 송신 출력을 설정합니다. 설정된 국가의 전파 규정에 따라 무선 송신 출력을 설정하시기 바랍니다. DIVA-IAP-AX 모델은 모드 및 채널 대역폭에 따라 17~23dBm 사이의 송신 출력을 제공합니다. 적합한 송신 출력을 확인할 수 없을 경우 **driver default** 값을 선택합니다. 케이블을 통해 안테나를 연결할 경우 케이블 손실을 감안하여 송신 출력을 설정합니다. ㈜하이링크에 문의하시면 케이블 길이 및 손실, 안테나 이득, 무선 통신 거리에 따른 송신 출력을 제안해 드립니다.

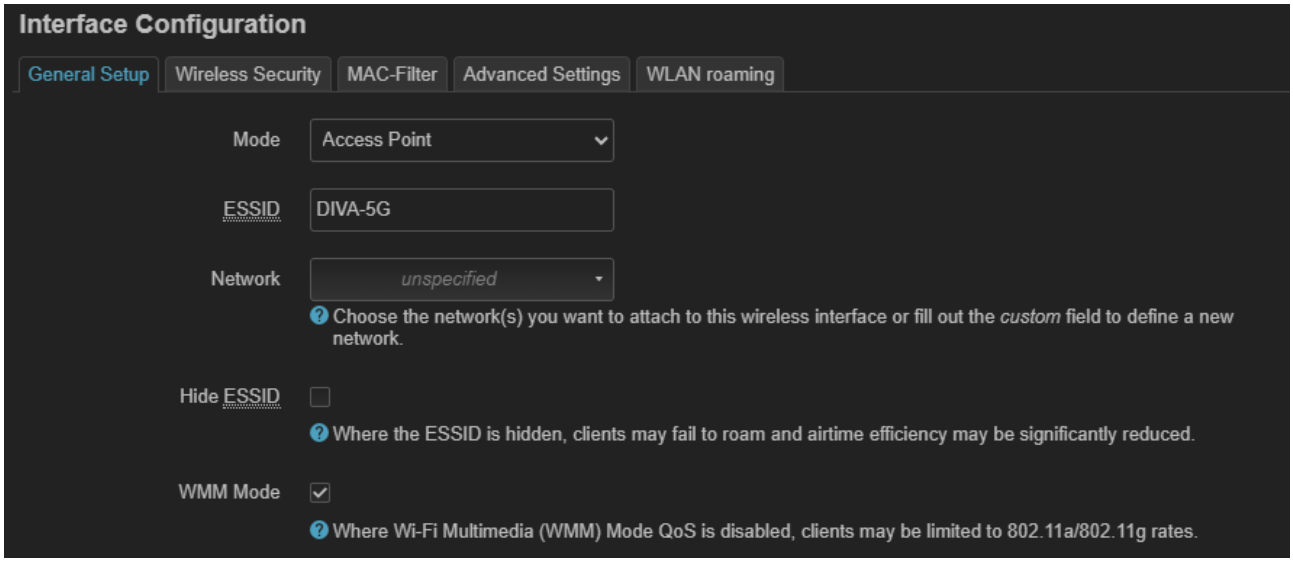
4.2.1.2 Device Configuration > Advanced Settings



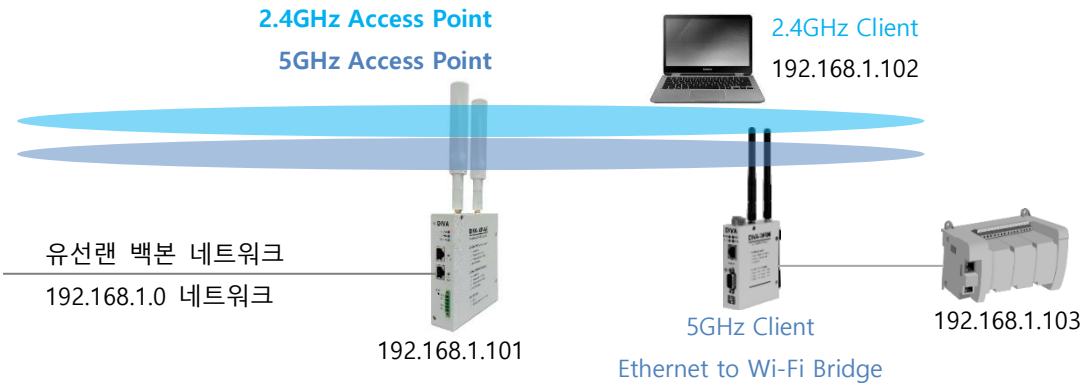
- **Country Code** 설치 지역의 국가 코드를 선택합니다. 국가 별로 사용 가능한 채널이 자동 변경됩니다.
- **Coverage cell density** 무선 환경의 장치 밀집도, 거리를 가정해 ACK 타이밍을 조정하는 옵션이며 넓은 공간에서 무선 신호 레벨이 양호한데도 재전송이 많고 끊김 현상이 발생할 때 사용할 수 있습니다. 전문가 외에는 Disabled 기본 설정을 사용하시기 바랍니다.
  - **Disabled** 기능을 사용하지 않음
  - **Normal** 일반적인 환경(소형 아파트, 단독 주택)
  - **High** 다수의 무전 장치 있음 (사무실)
  - **Very High** 매우 많은 무선 장치 밀집 (공장, 야외, 장거리 링크)
- **Distance Optimization** 무선 통신 거리가 1Km를 초과할 경우 가장 멀리 위치한 무선랜 클라이언트 장치까지의 거리를 미터 단위로 입력합니다. 전문가 외에는 **auto** 설정을 사용하시기 바랍니다.
- **Fragmentation Threshold** 프레임 크기가 설정값 보다 크면 여러 조각으로 분할하여 전송합니다. 256 ~ 2346 바이트 사이의 값을 설정할 수 있으며 **0** 값 설정 시 해당 기능을 사용하지 않습니다. 기본값 사용을 권장합니다.
- **RTS/CTS Threshold** 트래픽 흐름 제어를 위한 무선 전송 패킷 크기를 설정합니다. 패킷 크기는 1부터 2346 바이트 사이의 값을 설정할 수 있으며 기본값은 **off** 로 설정되어 있습니다. off 값을 사용할 경우 RTS Threshold 기능이 사용되지 않습니다. 802.11 무선 네트워크 프로토콜은 히든 노드에 의해 발생되는 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. 무선랜 클라이언트 장치는 액세스 포인트 장치로 RTS 프레임을 먼저 전송한 후 데이터 전송 허가를 위한 CTS 응답 프레임 수신을 대기합니다. 클라이언트 장치는 액세스 포인트 장치로부터 CTS 프레임을 수신한 후에 데이터 패킷을 전송합니다. 특정 클라이언트 장치가 데이터를 전송하는 동안 다른 클라이언트 장치들은 액세스 포인트 장치로 데이터를 전송할 수 없고 특정 클라이언트 장치가 데이터 전송을 완료할 때까지 대기합니다. 고급 사용자 외에는 기본값을 사용하시기 바랍니다.

- **Force 40MHz mode** 채널 간섭이 발생하는 환경에서도 40MHz 채널 대역폭을 강제로 사용하도록 설정합니다. 주변에 무선 장치가 없는 환경에서만 사용할 수 있는 옵션으로 대부분의 환경에서는 사용하지 않습니다. 간섭이 전혀 없는 특수 환경에서 테스트 용도로 사용합니다.
- **Beacon Interval** Access Point 및 Access Point (WDS) 모드에서 주기적으로 보내는 Beacon 프레임 간격을 ms 단위로 설정합니다. Beacon 프레임은 SSID 존재를 알리고, 타이밍 동기화, 절전 클라이언트 장치를 깨우는 역할을 합니다. 값을 늘리면 SSID 검색이 지연되고 로밍 기능이 떨어질 수 있습니다.
  - **일반적인 환경** 100ms 기본값
  - **무선랜 장치 밀집 지역** 200ms (Beacon 충돌로 인한 관리 프레임 오버헤드 증가 방지)
  - **저전력 IoT 네트워크** 200~300ms (무선 클라이언트 장치 배터리 효율 증가)
  - **실외용 장거리 연결** 150~200ms (무선 장치간 관리 트래픽 감소)

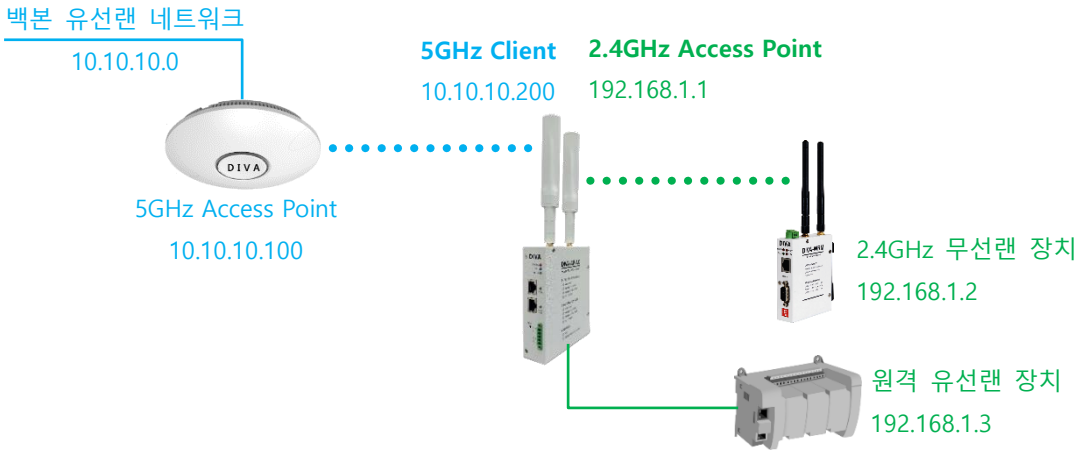
4.2.1.3 Interface Configuration > General Setup



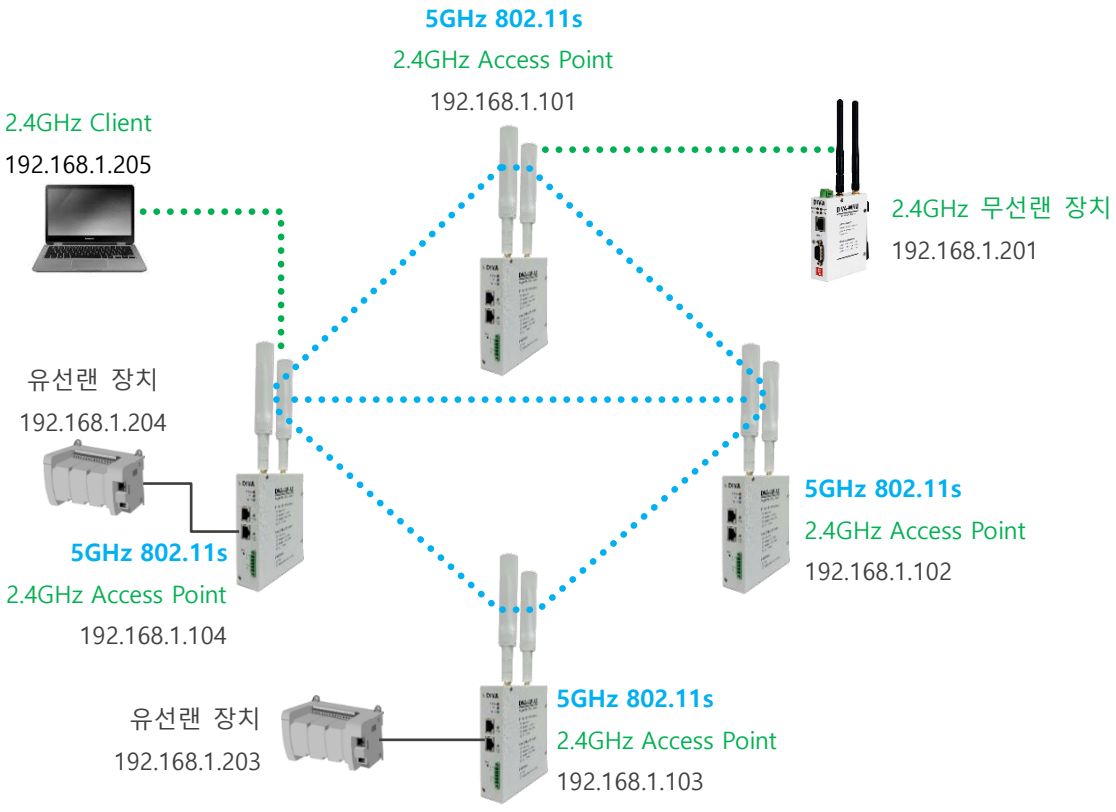
- **Mode** 사용 용도에 따라 장치 동작 모드를 선택합니다.
  - **Access Point** 일반적인 액세스 포인트 모드로 장치를 동작합니다. 무선랜을 통해 연결되는 장치와 유선랜을 통해 연결되는 장치들은 모두 동일 서브넷 네트워크로 연결됩니다.



- **Client** 1개의 무선랜 인터페이스를 통해 WAN 백본 네트워크에 연결하고, 나머지 1개의 무선랜 인터페이스와 2개의 유선랜 포트는 로컬 네트워크(LAN) 네트워크 장치들을 연결합니다. 액세스 포인트에 연결되는 무선랜 인터페이스는 액세스 포인트 장치와 동일 서브넷 네트워크를 사용하고, 나머지 1개의 무선랜 인터페이스와 2개의 유선랜 인터페이스에 연결되는 장치들은 자체 로컬 서브넷 네트워크를 사용합니다. NAT 및 Port Forward 기능을 사용하여 DIVA-IAP-AX 장치에 연결된 유무선 장치와 백본 네트워크를 연결합니다. L2 연결 방식의 클라이언트 브리지 장치를 사용해야 할 경우 DIVA-WRM, DIVA-WRM2 모델을 사용합니다.



- **802.11s** 표준 매쉬 프로토콜을 사용하여 무선 네트워크를 자동으로 구성합니다. 유무선 네트워크에 연결되는 모든 장치들은 동일 서브넷 네트워크로 연결됩니다.
  - ✓ **Mesh Id** 매쉬 네트워크 이름을 대소문자를 구분하여 설정합니다.
  - ✓ **Network** 매쉬 네트워크로 연결할 네트워크 인터페이스를 선택합니다.



- **Monitor** 주변의 모든 무선 프레임을 수신만 하는 모드로서 암호화 여부와 상관없이 전파로 송신되는 패킷을 그대로 캡쳐할 수 있습니다. 주변 무선랜 AP 탐색 및 패킷 분석 작업에 사용됩니다. Monitor 모드에서는 숨김 SSID 장치도 검색이 가능합니다. Monitor 모드로 동작하는 DIVA-IAP-AX 장치는 유선랜 접속만 가능합니다.

- **Access Point (WDS)** 무선랜 액세스 포인트 모드로 동작하고 Client (WDS) 모드로 동작하는 DIVA-IAP-AX 장치 사이에 MAC 주소를 이용한 연결 방식을 사용합니다. DIVA-IAP-AX 장치의 유선랜 포트에 연결된 네트워크 장치들은 동일 서브넷 네트워크로 연결되고 고유의 MAC 주소와 IP 주소를 기반으로 식별되고 데이터를 송수신합니다. WDS 방식은 PROFINET 장치와 같이 MAC 주소 기반의 통신 장비를 연결하는데 사용할 수 있습니다. DIVA-IAP-AX 및 DIVA-AXP 장치만을 사용하여 무선 네트워크를 구성할 때 사용하시기 바랍니다.
- **Client (WDS)** 무선랜 클라이언트 모드로 동작하고 Access Point (WDS) 모드로 동작하는 DIVA-IAP-AX 장치에 연결됩니다. DIVA-IAP-AX 장치의 유선랜 포트에 연결된 네트워크 장치들은 동일 서브넷 네트워크로 연결되고 고유의 MAC 주소와 IP 주소를 기반으로 식별되고 데이터를 송수신합니다.

Access Point (WDS) mode
IP 주소 192.168.1.1
MAC 주소 11:11:11:11:11:11

Client (WDS) mode
IP 주소 192.168.1.2
MAC 주소 22:22:22:22:22:22

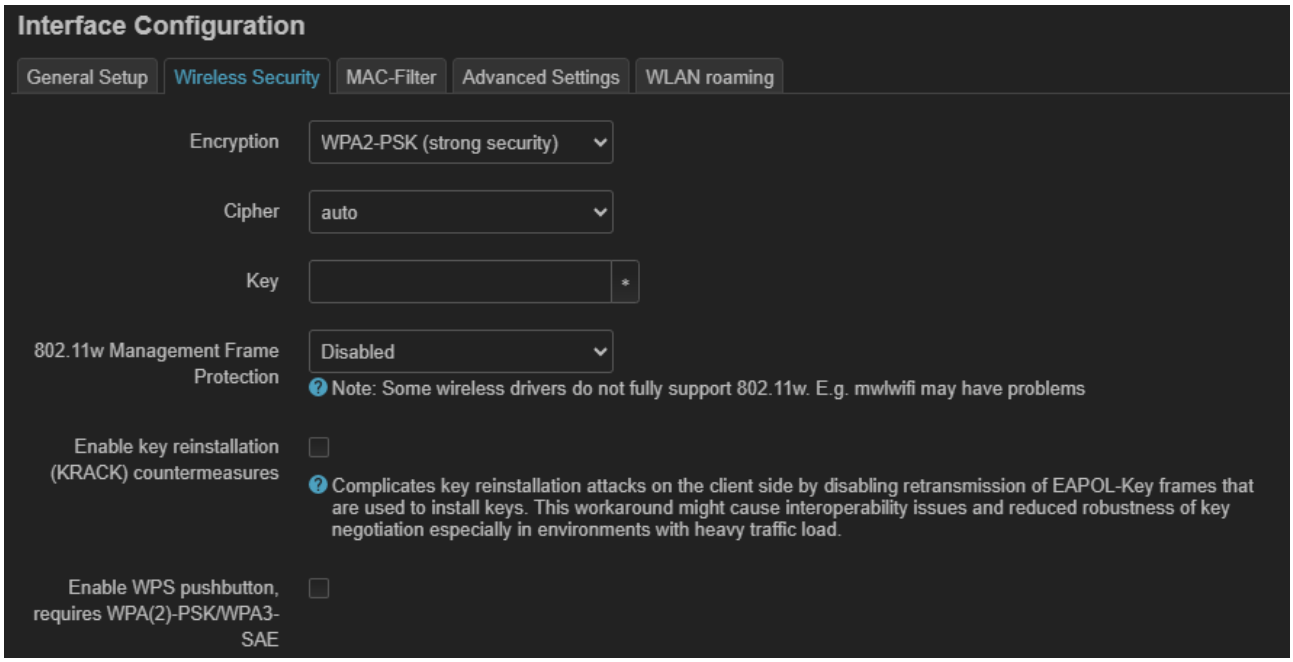
PLC 유선랜 장치
IP 주소 192.168.1.3
MAC 주소 33:33:33:33:33:33

ARP 테이블 정보

WDS 모드 사용 시	WDS 모드 미사용 시
192.168.1.1 - 11:11:11:11:11:11	192.168.1.1 - 11:11:11:11:11:11
192.168.1.2 - 22:22:22:22:22:22	192.168.1.2 - 22:22:22:22:22:22
192.168.1.3 - 33:33:33:33:33:33	192.168.1.3 - 22:22:22:22:22:22

- **ESSID** 무선랜 네트워크 이름을 대소문자를 구분하여 설정합니다. 무선랜으로 연결되는 액세스 포인트 및 클라이언트 장치들은 동일한 ESSID를 사용합니다.
- **Network** 무선랜에 연결할 네트워크 인터페이스를 선택합니다.
- **Hide ESSID** SSID 브로드 캐스트를 중단하여 주변 기기에서 무선랜 목록에 네트워크 이름이 보이지 않게 합니다. DIVA-IAP-AX 장치는 비콘 프레임의 SSID 필드를 비워서 전송합니다. 무인 물류 시스템과 같이 로밍 기능을 사용하는 네트워크에서는 연결 지연 및 자동 연결 실패 현상이 발생할 수 있습니다. Monitor 모드를 사용할 경우 숨겨진 무선랜 네트워크도 검색이 가능합니다.
- **WMM Mode** 802.11n/ac/ax 사용 시 트래픽 우선순위(QoS)를 기반으로 고속 무선랜을 구성합니다. 영상과 음성 품질을 향상 시기키 위해 기능 사용을 권장합니다. 802.11b/g 구형 장비와 호환성 문제가 발생할 경우에만 사용하지 않도록 설정합니다.

4.2.1.4 Interface Configuration > Wireless Security



- **Encryption** 무선랜 보안/인증을 선택합니다. 무선랜 장치들은 동일한 보안 설정을 통해 연결됩니다.
  - **WPA2-PSK** 가장 보편적으로 사용되는 무선랜 암호화 방식으로 소규모 네트워크 구성에 적합합니다. WPA2 암호화 표준을 사용하며 PSK (Pre-Shared Key, 공유 비밀번호) 하나로 모든 사용자가 접속합니다.
    - ✓ **Cipher** 암호화 알고리즘을 선택합니다. Force CCMP (AES) 사용을 권장합니다.
      - **auto** 액세스 포인트와 클라이언트 장치가 공통으로 지원하는 암호화 방식 자동 협상
      - **Force CCMP (AES)** CCMP (AES) 암호화를 강제로 사용합니다. (표준 권장)
      - **Force TKIP** TKIP 암호화를 강제로 사용합니다.
      - **Force TKIP and CCMP (AES)** 구형 장치 호환을 위해 TKIP 암호화도 강제로 허용합니다.
    - ✓ **Key** 8~63개 사이의 문자와 숫자를 조합하여 비밀번호를 구성합니다.
    - ✓ **802.11w Management Frame Protection** 무선랜 관리 프레임을 암호화/무결성 보호하여 Deauth 같은 무선 공격을 차단합니다. WPA3-SAE 방식에서는 강제 사항이지만 WPA2 또는 WPA2/WPA3 Mixed 방식에서는 옵션 사항입니다.
      - **Disabled** 사용 안함
      - **Optional** 지원 기기만 사용 (표준 권장)
      - **Required** 미지원 기기 접속 차단
    - ✓ **Enable key reinstallation** KRACK 공격을 차단합니다. 이 기능을 사용하면 DIVA-IAP-AX 장치는 Access Point 모드에서 이미 설치된 키를 다시 설치하려는 시도를 차단하고 비정상적인 핸드쉐이크 재설치 요청을 무시합니다. 구형 무선랜 장치와 연동할 경우 호환되지 않을 수 있습니다. (설정 권장)
    - ✓ **Enable WPS pushbutton** 설정할 필요 없음

- **WPA2-EAP** WPA2 Enterprise 또는 802.1x 보안 방식은 무선랜 클라이언트 장치가 Radius 서버와 액세스 포인트 장치를 통해서 백본 네트워크에 연결할 수 있도록 인증 프로세스를 제공합니다. 액세스 포인트 장치는 백본 네트워크로 접근하기 위한 게이트웨이 역할을 제공하며 인증이 실패할 경우 백본 네트워크에 접근하는 것이 불가능합니다. WPA2 Enterprise 인증 방식은 Access Point, Client 모드에서만 사용되며 Radius 서버 정보를 등록합니다. DIVA-IAP-AX 장치는 Client (WDS) 모드에서 트랜스패런트 브리지로 동작하기 때문에 WPA2 Enterprise 인증을 사용할 수 없습니다.
  - ✓ **Cipher** 암호화 알고리즘을 선택합니다. Force CCMP (AES) 사용을 권장합니다.
    - **auto** 액세스 포인트와 클라이언트 장치가 공통으로 지원하는 암호화 방식 자동 협상
    - **Force CCMP (AES)** CCMP (AES) 암호화를 강제로 사용합니다. (표준 권장)
    - **Force TKIP** TKIP 암호화를 강제로 사용합니다.
    - **Force TKIP and CCMP (AES)** 구형 장치 호환을 위해 TKIP 암호화도 강제로 허용합니다.
  - ✓ **RADIUS Authentication Server** Radius 서버의 IP 주소를 입력합니다.
  - ✓ **RADIUS Authentication Port** Radius 서버의 UDP 포트 번호를 입력합니다. 일반적으로 1812 소켓 번호가 사용되지만 서버 관리자에게 확인 후 설정하시기 바랍니다.
  - ✓ **RADIUS Authentication Secret** Radius 장치 사이의 통신 유효성을 확인할 때 사용되는 비밀 번호를 대소문자를 구분하여 입력합니다.
  - ✓ **RADIUS Accounting Server** 사용 이력을 기록하는 서버가 있을 경우 IP 주소를 입력합니다.
  - ✓ **RADIUS Accounting Port** 사용 이력을 기록하는 서버의 UDP 포트 번호를 입력합니다.
  - ✓ **RADIUS Accounting Secret** 사용 이력을 기록하는 서버와 통신 유효성을 확인할 때 사용되는 비밀 번호를 대소문자를 구분하여 입력합니다.
  - ✓ **RADIUS Access-Request attributes** Radius 서버로 인증 요청을 보낼 때, 추가로 어떤 정보를 같이 보낼지 설정합니다. (설정할 필요 없음)
  - ✓ **RADIUS Accounting-Request attributes** Radius 사용 이력 기록 서버로 데이터를 보낼 때, 추가로 어떤 세부 정보를 포함시킬지 설정합니다. (설정할 필요 없음)
  - ✓ **RADIUS Dynamic VLAN Assignment** 동일한 SSID를 사용하여 클라이언트 장치(사용자/그룹 단위)가 접속하여도 Radius 서버가 장치 별로 다른 VLAN에 연결되도록 설정합니다.
    - **Disabled** 사용 안함
    - **Optional** 지원 기기만 사용 (표준 권장)
    - **Required** 미지원 기기 접속 차단
  - ✓ **RADIUS Per STA VLAN** 무선 클라이언트 장치마다 개별 VLAN을 할당합니다.
  - ✓ **RADIUS VLAN Naming** Radius 서버가 숫자 형태의 VLAN 아이디 대신 VLAN 이름을 내려주면, 액세스 포인트로 동작하는 DIVA-IAP-AX 장치가 그 이름에 지정된 VLAN으로 트래픽을 보내는 기능 설정
  - ✓ **RADIUS VLAN Tagged Interface** 선택한 네트워크 장치로부터의 수신된 데이터는 액세스 포인트 장치에서 변경하지 않고 802.1Q 테그를 붙인 채 상위 네트워크로 전달합니다.
  - ✓ **RADIUS VLAN Bridge Naming Scheme** 동적 VLAN이 생길 때 내부 인터페이스 이름을 자동으로 어떻게 붙일지 규칙을 설정합니다.
  - ✓ **DAE-Client** DAE 서버 장치(Radius 서버)의 IP 주소를 입력합니다. Radius 서버가 AP 장치로 "지금 당장 이 사용자 차단/정책 변경하라"는 명령을 내일 수 있게 해주는 실시간 제어 기능입니다.
  - ✓ **DAE-Port** DAE 서버의 UDP 포트 번호를 입력합니다.
  - ✓ **DAE-Secret** DAE 서버 연결에 필요한 비밀 번호를 입력합니다.
  - ✓ **RSN Preauth** WPA2 기반의 보안 기능으로서 현재 연결된 AP를 통해 로밍 할 주변의 다른 AP와 미리 인증을 수행하는 기능을 설정합니다.
  - ✓ **802.11w Management Frame Protection** 무선랜 관리 프레임을 암호화/무결성 보호하여 Deauth 같은

무선 공격을 차단하는 보안 기능을 설정합니다. WPA3-SAE 방식에서는 강제 사항이지만 WPA2 또는 WPA2/WPA3 Mixed 방식에서는 옵션 사항입니다.

- **Disabled** 사용 안함
- **Optional** 지원 기기만 사용 (표준 권장)
- **Required** 미지원 기기 접속 차단

✓ **Enable key reinstallation (KRACK) countermeasures** KRACK 공격을 차단하는 보안 기능을 설정합니다. 이 기능을 사용하면 DIVA-IAP-AX 장치는 Access Point 모드에서 이미 설치된 키를 다시 설치하려는 시도를 차단하고 비정상적인 핸드쉐이크 재설치 요청을 무시합니다. 구형 무선랜 장치와 연동할 경우 호환되지 않을 수 있습니다. (설정 권장)

■ **WPA3-EAP** WPA3 Enterprise 또는 802.1x 보안 방식은 무선랜 클라이언트 장치가 Radius 서버와 액세스 포인트 장치를 통해서 백본 네트워크에 연결할 수 있도록 인증 프로세스를 제공합니다. 액세스 포인트 장치는 백본 네트워크로 접근하기 위한 게이트웨이 역할을 제공하며 인증이 실패할 경우 백본 네트워크에 접근하는 것이 불가능합니다. WPA3 Enterprise 인증 방식은 Access Point, Client 모드에서만 적용되며 Radius 서버 정보를 등록합니다. DIVA-IAP-AX 장치는 Client (WDS) 모드에서 트랜스패런트 브리지로 동작하기 때문에 WPA3 Enterprise 인증을 사용할 수 없습니다.

✓ **Cipher** 암호화 알고리즘을 선택합니다. Force CCMP (AES) 사용을 권장합니다.

- **auto** 액세스 포인트와 클라이언트 장치가 공통으로 지원하는 암호화 방식 자동 협상
- **Force CCMP (AES)** CCMP (AES) 암호화를 강제로 사용합니다. (표준 권장)
- **Force TKIP** TKIP 암호화를 강제로 사용합니다.
- **Force TKIP and CCMP (AES)** 구형 장치 호환을 위해 TKIP 암호화도 강제로 허용합니다.

✓ **RADIUS Authentication Server** Radius 서버의 IP 주소를 입력합니다.

✓ **RADIUS Authentication Port** Radius 서버의 UDP 포트 번호를 입력합니다. 일반적으로 1812 소켓 번호가 사용되지만 서버 관리자에게 확인 후 설정하시기 바랍니다.

✓ **RADIUS Authentication Secret** Radius 장치 사이의 통신 유효성을 확인할 때 사용되는 비밀 번호를 대소문자를 구분하여 입력합니다.

✓ **RADIUS Accounting Server** 사용 이력을 기록하는 서버가 있을 경우 IP 주소를 입력합니다.

✓ **RADIUS Accounting Port** 사용 이력을 기록하는 서버의 UDP 포트 번호를 입력합니다.

✓ **RADIUS Accounting Secret** 사용 이력을 기록하는 서버와 통신 유효성을 확인할 때 사용되는 비밀 번호를 대소문자를 구분하여 입력합니다.

✓ **RADIUS Access-Request attributes** Radius 서버로 인증 요청을 보낼 때, 추가로 어떤 정보를 같이 보낼지 설정합니다. (설정할 필요 없음)

✓ **RADIUS Accounting-Request attributes** Radius 사용 이력을 기록하는 서버로 데이터를 보낼 때, 추가로 어떤 세부 정보를 포함시킬지 설정합니다. (설정할 필요 없음)

✓ **RADIUS Dynamic VLAN Assignment** 동일한 SSID로 클라이언트 장치(사용자/그룹 단위)가 접속하여도 Radius 서버가 장치 별로 다른 VLAN에 연결되도록 설정합니다.

- **Disabled** 사용 안함
- **Optional** 지원 기기만 사용 (표준 권장)
- **Required** 미지원 기기 접속 차단

✓ **RADIUS Per STA VLAN** 무선 클라이언트 장치마다 개별 VLAN을 할당하는 기능 설정

✓ **RADIUS VLAN Naming** Radius 서버가 숫자 형태의 VLAN 아이디 대신 VLAN 이름을 내려주면, 액세스 포인트로 동작하는 DIVA-IAP-AX 장치가 그 이름에 지정된 VLAN으로 트래픽을 보내는 기능 설정

✓ **RADIUS VLAN Tagged Interface** 선택한 네트워크 장치로부터의 수신된 데이터는 액세스 포인트 장치에서 변경하지 않고 802.1Q 테그를 붙인 채 상위 네트워크로 전달합니다.

- ✓ **RADIUS VLAN Bridge Naming Scheme** 동적 VLAN이 생길 때 내부 인터페이스 이름을 자동으로 어떻게 붙일지 규칙을 설정합니다.
- ✓ **DAE-Client** DAE 서버 장치(Radius 서버)의 IP 주소를 입력합니다. Radius 서버가 AP 장치로 "지금 당장 이 사용자 차단/정책 변경하라"는 명령을 내일 수 있게 해주는 실시간 제어 기능입니다.
- ✓ **DAE-Port** DAE 서버의 UDP 포트 번호를 입력합니다.
- ✓ **DAE-Secret** DAE 서버 연결에 필요한 비밀 번호를 입력합니다.
- ✓ **RSN Preauth** WPA2 기반의 보안 기능으로서 현재 연결된 AP를 통해 로밍 할 주변의 다른 AP와 미리 인증을 수행하는 기능을 설정합니다.
- ✓ **802.11w Management Frame Protection** 무선랜 관리 프레임을 암호화/무결성 보호하여 Deauth 같은 무선 공격을 차단합니다. WPA3-SAE 방식에서는 강제 사항이지만 WPA2 또는 WPA2/WPA3 Mixed 방식에서는 옵션 사항입니다.
  - ◆ **Disabled** 사용 안함
  - ◆ **Optional** 지원 기기만 사용
  - ◆ **Required** 미지원 기기 접속 차단 (사용 권장)
- ✓ **802.11w maximum timeout** MFP 보호 관리 프레임 응답 대기 시간을 설정합니다.
- ✓ **802.11w retry timeout** MFP 보호 관리 프레임 전송이 실패할 경우, 재시도 대기 시간을 설정합니다.
- ✓ **Enable key reinstallation (KRACK) countermeasures** KRACK 공격을 차단합니다. 이 기능을 사용하면 DIVA-IAP-AX 장치는 Access Point 모드에서 이미 설치된 키를 다시 설치하려는 시도를 차단하고 비정상적인 핸드쉐이크 재설치 요청을 무시합니다. 구형 무선랜 장치와 연동할 경우 호환되지 않을 수 있습니다. (설정 권장)

■ **WPA2-EAP / WPA3-EAP Mixed** WPA2 Enterprise 방식과 WPA3 Enterprise 방식을 동시에 지원하는 모드입니다. 신형 클라이언트 단말은 WPA3-EAP, 구형 클라이언트 단말은 WPA2-EAP로 자동 선택하여 접속하는 방식입니다. 일부 구형 클라이언트 장치는 WPA3 IE 해석에 실패하여 연결이 불안정할 수 있습니다.

- ✓ **세부 항목 설정** WPA3-EAP 와 동일

■ **WPA3-SAE** 비밀번호 기반의 무선랜 취약점을 제거하고, 오프라인 사전 공격과 키 재사용을 원천 차단하는 최신 PSK 보안 방식입니다. 802.11s 모드에서는 WPA-SAE 보안만 사용할 수 있습니다.

- ✓ **Key** SAE 인증 과정에서 매 접속마다 새로 만들어지는 세션 암호 키를 입력합니다. 12~16자 이상의 문자와 숫자를 조합하여 비밀번호를 구성합니다.
- ✓ **802.11w Management Frame Protection** 무선랜 관리 프레임을 암호화/무결성 보호하여 Deauth 같은 무선 공격을 차단하는 보안 기능을 설정합니다. WPA3-SAE 방식에서는 강제 사항이지만 WPA2 또는 WPA2/WPA3 Mixed 방식에서는 옵션 사항입니다.
  - ◆ **Disabled** 사용 안함
  - ◆ **Optional** 지원 기기만 사용
  - ◆ **Required** 미지원 기기 접속 차단 (사용 권장)
- ✓ **802.11w maximum timeout** MFP 보호 관리 프레임 응답 대기 시간을 설정합니다.
- ✓ **802.11w retry timeout** MFP 보호 관리 프레임 전송이 실패할 경우, 재시도 대기 시간을 설정합니다.
- ✓ **Enable key reinstallation (KRACK) countermeasures** KRACK 공격을 차단하는 보안 기능을 설정합니다. 이 기능을 사용하면 DIVA-IAP-AX 장치는 Access Point 모드에서 이미 설치된 키를 다시 설치하려는 시도를 차단하고 비정상적인 핸드쉐이크 재설치 요청을 무시합니다. 구형 무선랜 장치와 연동할 경우 호환되지 않을 수 있습니다. (설정 권장)
- ✓ **Enable WPS pushbutton** 설정할 필요 없음

- **WPA2-PSK / WPA3-SAE Mixed** WPA2-PSK 방식과 WPA3-SAE 방식을 동시에 지원하는 모드입니다. 신형 클라이언트 단말은 WPA3-SAE, 구형 클라이언트 단말은 WPA2-PSK로 자동 선택하여 접속하는 방식입니다. WPA3 방식에서는 802.11w Management Frame Protection 설정을 required 값으로 설정하지만 Mixed 모드에서는 구형 클라이언트 장치와의 혼합 연동으로 인해 Optional 로 설정합니다.
  - ✓ **802.11w Management Frame Protection** Optional
  - ✓ **나머지 세부 항목 설정** WPA3-SAE 와 동일

- **WPA-PSK / WPA2-PSK Mixed** WPA-PSK 방식과 WPA2-PSK 방식을 동시에 지원하는 모드입니다. 신형 클라이언트 단말은 WPA2-PSK, 구형 클라이언트 단말은 WPA-PSK로 자동 선택하여 접속하는 방식입니다. TKIP 암호화 방식을 사용하여 802.11n/ac/ax 기능이 제한될 수 있으며 속도나 매우 낮아질 수도 있습니다. 보안 및 성능이 모두 취약한 모드로서 특별한 사유가 없다면 사용하지 않습니다.
  - ✓ **세부 항목 설정** WPA2-PSK 와 동일

- **WPA-EAP** WPA Enterprise 또는 802.1x 보안 방식은 무선랜 클라이언트 장치가 Radius 서버와 액세스 포인트 장치를 통해서 백본 네트워크에 연결할 수 있도록 인증 프로세스를 제공합니다. 액세스 포인트 장치는 백본 네트워크로 접근하기 위한 게이트웨이 역할을 제공하며 인증이 실패할 경우 백본 네트워크에 접근하는 것이 불가능합니다. WPA Enterprise 인증 방식은 Access Point, Client 모드에서만 적용되며 Radius 서버 정보를 등록합니다. DIVA-IAP-AX 장치는 Client (WDS) 모드에서 트랜스패런트 브리지로 동작하기 때문에 WPA Enterprise 인증을 사용할 수 없습니다.
  - ✓ **세부 항목 설정** WPA2-EAP 와 동일

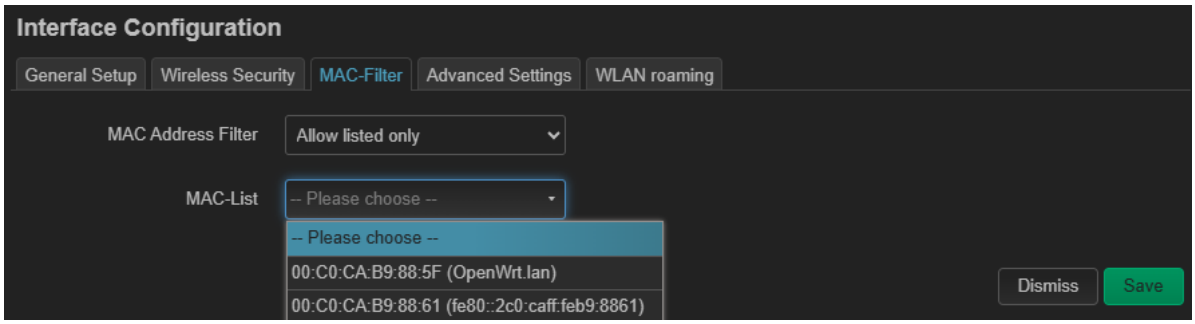
- **WPA-PSK** 매우 취약한 무선랜 암호화 방식으로 사용을 권장하지 않습니다. WPA 암호화 표준을 사용하며 PSK(Pre-Shared Key, 공유 비밀번호) 하나로 모든 사용자가 접속합니다.
  - ✓ **세부 항목 설정** WPA2-PSK 와 동일

- **OWE (open network)** 비밀번호 없이도 무선 트래픽을 자동으로 암호화하는 보안 방식입니다. 모든 클라이언트 장치가 인증 없이 접속할 수 있고 데이터는 암호화되는 방식으로 공공 무선랜에서 사용할 수 있습니다.
  - ✓ **802.11w Management Frame Protection** 무선랜 관리 프레임을 암호화/무결성 보호하여 Deauth 같은 무선 공격을 차단하는 보안 기능을 설정합니다. WPA3-SAE 방식에서는 강제 사항이지만 WPA2 또는 WPA2/WPA3 Mixed 방식에서는 옵션 사항입니다.
    - ◆ **Disabled** 사용 안함
    - ◆ **Optional** 지원 기기만 사용
    - ◆ **Required** 미지원 기기 접속 차단 (사용 권장)
  - ✓ **802.11w maximum timeout** MFP 보호 관리 프레임 응답 대기 시간을 설정합니다.
  - ✓ **802.11w retry timeout** MFP 보호 관리 프레임 전송이 실패할 경우, 재시도 대기 시간을 설정합니다.

- **No Encryption (open network)** 개방형 무선 네트워크를 구성할 때 설정합니다. 연결 인증 및 데이터 암호화를 사용하지 않기 때문에 보안에 취약하며 외부에 노출되지 않는 폐쇄 환경에서만 사용하시기 바랍니다.

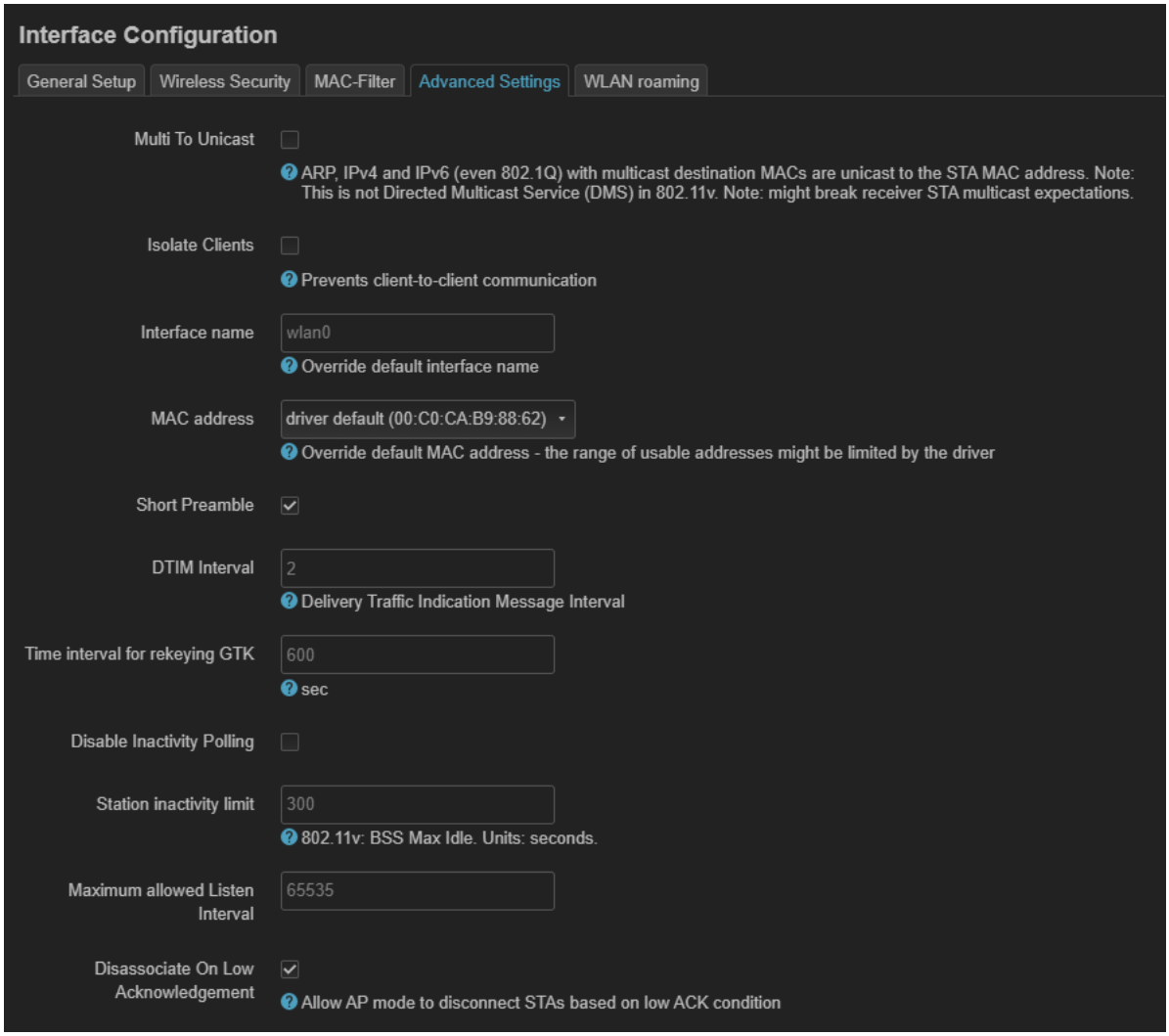
4.2.1.5 Interface Configuration > MAC-Filter

MAC 주소를 기반으로 네트워크 접속 허용/차단을 등록하는 필터링 기능을 설정합니다.



- **MAC Address Filter** 필터 기능을 선택합니다.
  - **disable** MAC 필터링 기능 사용 안함
  - **Allow listed only** 등록된 장치만 네트워크 접속 허용
  - **Allow all except listed** 등록된 장치만 네트워크 접속 차단
- **MAC-List** 표시되는 장치를 선택하거나 custom 메뉴를 통해 MAC 주소 직접 입력

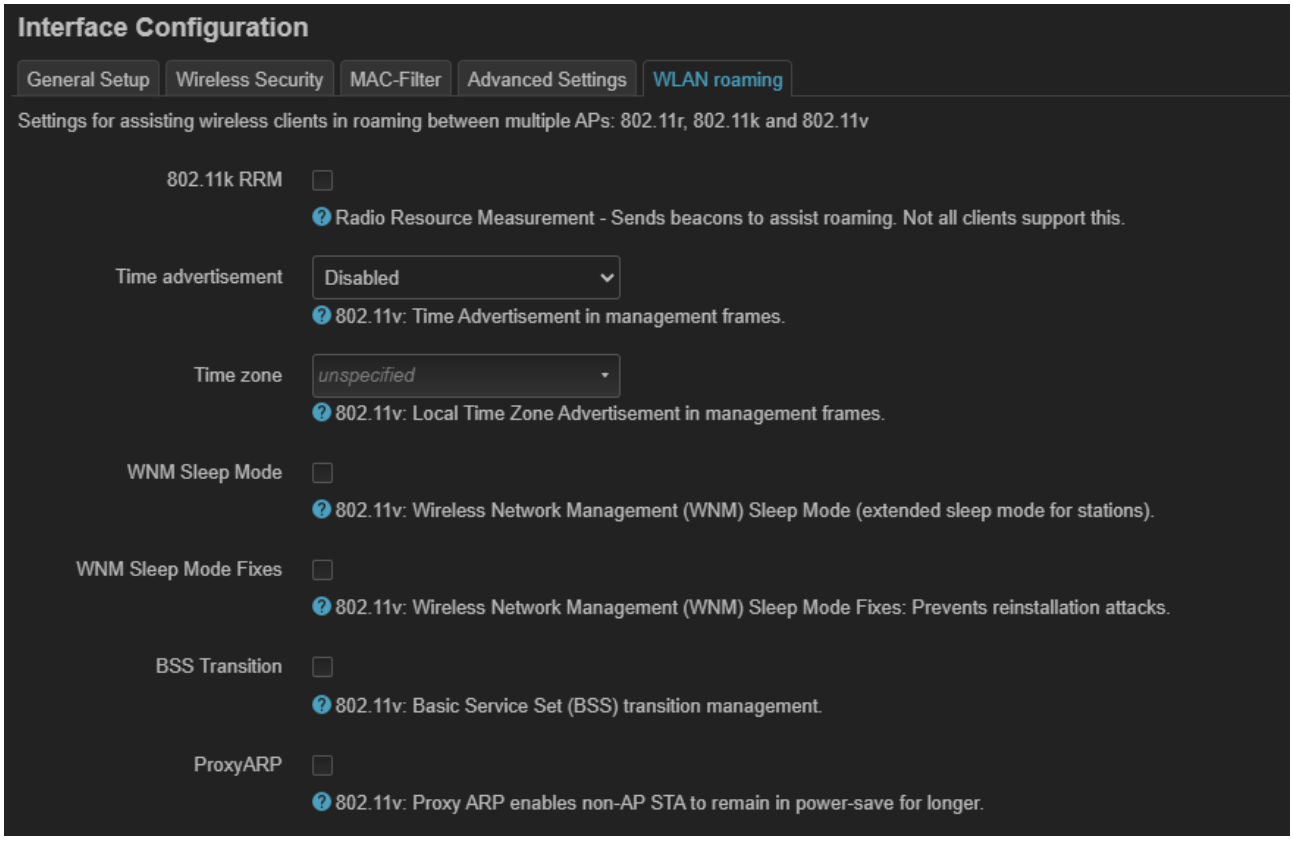
4.2.1.6 Interface Configuration > Advanced Settings



- **Multi To Unicast** 무선 네트워크에서 멀티캐스트/브로드캐스트 트래픽을 각 클라이언트 장치에게 유니캐스트로 변환해 전송합니다. IPTV 또는 미디어 스트리밍 품질을 개선할 수 있으나 무선랜 클라이언트 장치가 많은 환경에서는 사용하지 않습니다.
- **Isolate Clients** 유선랜 네트워크와 무선랜 클라이언트 장치 사이의 트래픽만 허용되며 액세스 포인트 장치에 연결된 무선랜 클라이언트 장치 사이의 트래픽은 차단됩니다. 공용 무선랜에서 사용자 사이의 공격/도청/오남용을 방지할 때 사용됩니다. 액세스 포인트 장치에 연결된 Client 장치 사이에 레이어2 레벨 연결이 지원되지 않으니 주의하시기 바랍니다.
- **Interface name** 해당 인터페이스 이름을 변경합니다.
- **MAC address** 해당 인터페이스에서 사용할 MAC 주소를 선택합니다.
  - **driver default** 제품 출고 시 기본값을 사용합니다.
  - **randomly generated** 임으로 생성한 MAC 주소를 사용합니다.
  - **custom** 사용자가 입력한 MAC 주소를 사용합니다.
- **Short Preamble** 802.11b 호환용 옵션으로 5GHz 인터페이스에서는 사용되지 않으며 2.4GHz에서 아래와 같은 조건에서 사용합니다.
  - 2.4GHz 802.11b 클라이언트 장치만 연결
  - 무선 클라이언트 장치가 Short Preamble 지원
  - 속도보다 무선랜 연결 유지가 중요할 경우
- **DTIM Interval** 절전 모드로 동작 중인 클라이언트 장치에게 멀티캐스트/브로드캐스트 데이터를 언제 전달할지 정하는 주기를 설정합니다. 클라이언트 장치는 비콘 프레임을 수신하다가 DTIM 비콘 프레임을 수신하면 절전 모드에서 해제됩니다. 설정 단위는 100ms이며 기본값 2 사용시 200ms 마다 DTIM 비콘 프레임을 전송합니다. 배터리 수명과 네트워크 반응성을 조절하여 변경하시기 바랍니다.
- **Time interval for rekeying GTK** 무선 네트워크에서 멀티캐스트/브로드캐스트 트래픽 보안을 유지하기 위해 사용하는 그룹 키 교체 주기를 초단위로 설정합니다. 변경 시 3600초 이내의 값 사용을 권장합니다.
- **Disable Inactivity Polling** 액세스 포인트 장치가 클라이언트 장치가 살아 있는지 주기적으로 확인하는 동작을 끕니다. 주로 절전/저트래픽 IoT 기기의 끊김 문제를 해결할 때만 선택적으로 사용됩니다.
- **Station inactivity limit** 무선 클라이언트 장치가 설정된 시간 동안 트래픽이 발생하지 않으면 비활성으로 판단해 무선 연결을 해제합니다.
- **Maximum allowed Listen Interval** 절전 모드로 동작 중인 무선 클라이언트 장치가 설정된 시간보다 오래 꺼져 있으면 연결이 끊어진 것으로 판단합니다. Listen Interval 은 무선 클라이언트 장치가 액세스 포인트 장치에게 전송하는 값으로, 설정된 값보다 큰 Listen Interval 값을 클라이언트 장치가 요청할 경우 액세스 포인트 장치는 연결을 거부하거나 제한합니다. 다음과 같은 수식으로 계산됩니다.
  최대 허용 시간 = 비콘 주기 x Maximum allowed Listen Interval
  예를 들어, 100ms 비콘 주기를 사용하면서 Max. Listen 주기가 20일 경우 2초(2000ms) 입니다.
- **Disassociate On Low Acknowledgement** 무선 클라이언트 장치가 액세스 포인트 프레임에 대해 ACK(응답)를 거의 보내지 못할 정도로 무선 연결 품질이 나빠지면, 액세스 포인트 장치는 해당 클라이언트 장치를 무선 연결을 강제로 해제합니다. 해당 클라이언트 장치는 로밍 기능을 지원하지 않아도 네트워크를 다시 스캔하여 더 신호 품질이 우수한 액세스 포인트 장치로 연결할 수 있습니다.

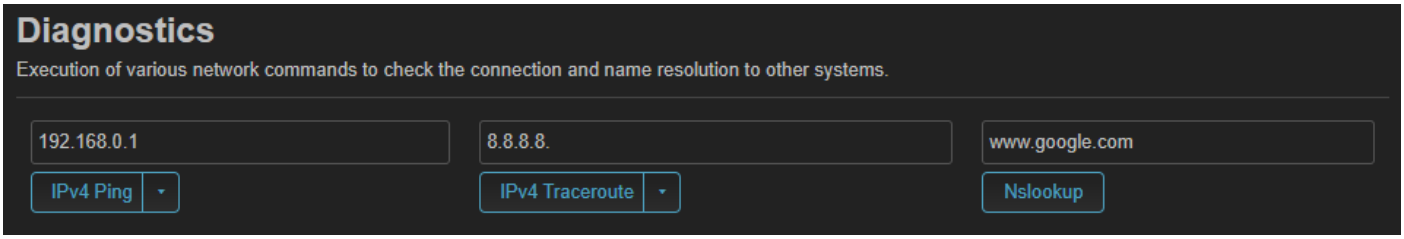
4.2.1.7 Interface Configuration > WLAN roaming

무선랜 클라이언트 장치가 제공하는 로밍 기능과 별개로 DIVA-IAP-AX 장치가 액세스 포인트 모드로 동작할 때 로밍 기능을 설정합니다. 연결되는 클라이언트 장치는 802.11k, 802.11v 프로토콜을 지원해야 합니다.



- **802.11k RRM** 액세스 포인트 장치가 무선 환경 정보를 클라이언트 장에게 제공하여 클라이언트 장치가 로밍을 하도록 기능을 제공합니다. 로밍 결정은 클라이언트 장치에 의해 결정되고 액세스 포인트 장치는 정보만 제공합니다. 액세스 포인트 장치는 다음과 같은 정보를 제공합니다.
  - **Neighbor Report** 주변 AP 목록, BSSID, 채널, PHY 정보
  - **Beacon Measurement** AP가 대신 측정하거나 클라이언트 장치가 측정한 결과 보고
  - **Channel Load / Noise** 채널 혼잡도 정보
- **Time advertisement** 액세스 포인트 장치가 Beacon / Action 프레임을 통해 기준 시간 정보를 제공하여 클라이언트 장치의 시간 동기화 및 인증, 전력효율을 개선하도록 합니다.
- **Time zone** Time advertisement 기능 사용 시 사용할 지역 시간대를 설정합니다. UTC 혹은 사용자가 지역 시간대를 입력할 수 있습니다.
- **WNM Sleep Mode** 무선 클라이언트 장치가 장시간 절전 모드로 들어갈 때, 액세스 포인트 장치에게 미리 알려 트래픽을 대신 처리/버퍼링 할 수 있도록 합니다.
- **WNM Sleep Mode Fixes** WNM Sleep Mode 기능을 제대로 구현하지 못한 클라이언트 장치로 인해 발생하는 연결 끊김, 재연결 실패, 트래픽 유실 같은 문제를 완화하고 수정하기 위한 호환성 보정 옵션을 사용합니다.
- **BSS Transition** 무선 클라이언트 장치에게 더 적합한 액세스 포인트 장치로 이동(로밍) 하도록 권고 메시지를 전송합니다. 무선 클라이언트 장치의 판단에 따라 로밍이 결정됩니다.
- **ProxyARP** 액세스 포인트 장치가 클라이언트 장치 대신 ARP에 응답해 무선 단말 간 직접 통신을 차단하고, 모든 트래픽을 중앙에서 제어하도록 합니다.

4.3 Diagnostics



- **Ping** 다른 장치로 Ping 테스트 메시지를 전송하여 네트워크 연결 상태를 확인하며 ICMP (Internet Control Message Protocol) 패킷을 사용하여 링크 품질과 네트워크 장치 사이의 전송 지연을 확인합니다. 입력창에 원격 호스트 시스템의 IP 주소나 URL 주소를 입력한 후 **Ping** 버튼을 클릭합니다. URL 주소를 입력할 경우 DIVA-IAP-AX 장치에 DNS 서버가 설정되어 있어야 합니다. DNS 서버는 Network > LAN Settings 메뉴에서 등록합니다. 테스트가 완료되면 송수신 패킷의 개수와 손실 수치를 표시하며 최소 왕복 송수신 시간, 평균 왕복 송수신 시간, 최대 왕복 송수신 시간을 ms 단위로 표시합니다.

```
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: seq=0 ttl=64 time=1.228 ms
64 bytes from 192.168.0.1: seq=1 ttl=64 time=0.874 ms
64 bytes from 192.168.0.1: seq=2 ttl=64 time=1.286 ms
64 bytes from 192.168.0.1: seq=3 ttl=64 time=1.013 ms
64 bytes from 192.168.0.1: seq=4 ttl=64 time=0.724 ms

--- 192.168.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.724/1.025/1.286 ms
```

- **Traceroute** DIVA-IAP-AX 장치로부터 지정한 호스트 이름이나 IP 주소를 가진 장치까지의 네트워크 경로를 추적합니다. Traceroute 툴은 ICMP 패킷을 전송하여 라우팅 경로를 확인합니다. 홉 호스트 마다 IP 주소와 왕복 송수신 시간이 표시되며 응답이 없을 경우 "*" 문자가 표시됩니다.

```
traceroute to 168.126.63.1 (168.126.63.1), 20 hops max, 46 byte packets
 1  192.168.0.1  1.221 ms
 2  *
 3  *
 4  10.19.216.5  1.478 ms
 5  1.213.5.113  1.993 ms
 6  100.92.1.5  3.456 ms
```

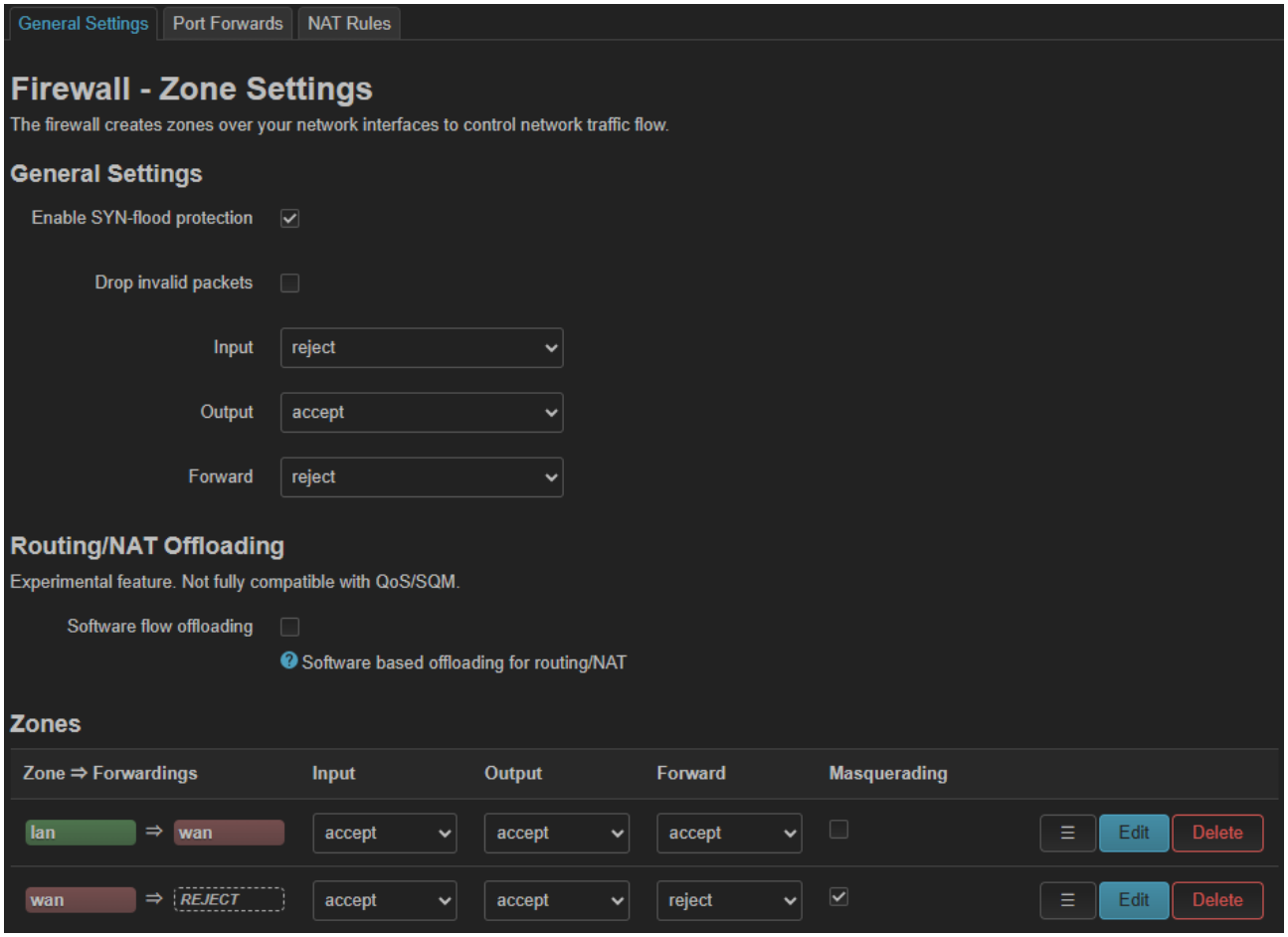
- **Nslookup** 인터넷 도메인의 IP 주소를 확인하는데 사용됩니다. DIVA-IAP-AX 장치에 DNS 서버가 설정되어 있어야 합니다.

```
Server:         127.0.0.1
Address:        127.0.0.1:53

Non-authoritative answer:
Name:   www.google.com
Address: 2404:6800:4005:81a::2004

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.199.68
```

4.4 Firewall

DIVA-IAP-AX 제품을 L2 네트워크 연결을 위한 Access Point, Access Point (WDS), Client (WDS), 802.11s 모드로 사용하실 경우, 별도의 방화벽 설정이 필요하지 않습니다. 유무선 네트워크 장치를 통해 서로 다른 서브넷을 사용하는 외부 배본 네트워크와 로컬 네트워크를 연결할 경우 방화벽 설정을 사용하시기 바랍니다.

4.4.1 General Settings



General Settings

- **Enable SYN-flood protection** 대량의 연결 요청 공격을 감지/차단하여 서버가 다운되는 것을 방지합니다.
- **Drop invalid packets** 잘못된 패킷을 차단합니다. 방화벽이 연결 상태를 추적했을 때 세션 정보가 없거나 비정상 순서 패킷, 스푸핑/스캔/깨진 패킷, 타임아웃 패킷 등이 잘못된 패킷으로 처리되며 보안상 대부분 차단 대상입니다. 일반적으로 drop 상태를 유지합니다.
  - **Input** 잘못된 수신 패킷에 대하여 reject / drop / accept 처리합니다.
  - **Output** 잘못된 송신 패킷에 대하여 reject / drop / accept 처리합니다.
  - **Forward** 잘못된 포워딩 패킷에 대하여 reject / drop / accept 처리합니다.
    - ✓ **reject** 거부 응답을 보내고 차단합니다. 연결 실패를 신속히 인지할 수 있지만 공격자에게 시스템 존재가 노출됩니다.
    - ✓ **drop** 패킷을 아무 반응 없이 폐기하고 DoS/스캔 공격자에게 정보를 제공하지 않습니다. (권장)
    - ✓ **accept** 잘못된 패킷이라도 허용하며 사실상 보안 기능을 끕니다.

Routing/NAT Offloading

- **Software flow offloading** 이미 설정된 네트워크 흐름을 내부적으로 빠르게 처리해서 라우팅 성능 및 속도를 개선합니다. 초기 패킷에 대해서만 방화벽/NAT 검사를 수행하고 이후 패킷은 우회 경로를 통해 바로 전달합니다. CPU 사용량이 감소하지만 SQM/QoS 트래픽 제어 기능과 완벽히 호환되지 않습니다.
- **Hardware flow offloading** 패킷 처리를 CPU가 아닌 스위치 칩으로 넘겨 최대 성능으로 가속합니다. 속도는 빠르지만 패킷이 방화벽을 완전히 우회하기 때문에 주의가 필요합니다. (Software flow offloading 체크 후 표시)

Zones

인터페이스마다 각각 방화벽 규칙을 만들면 매우 복잡하기 때문에 비슷한 보안 성격의 네트워크를 Zone으로 묶어 Zone과 Zone 사이의 통신 규칙을 설정합니다.

- **lan** br-lan 인터페이스가 포함된 내부 네트워크
- **wan** eth0, pppoe-wan 등이 포함된 외부 인터넷

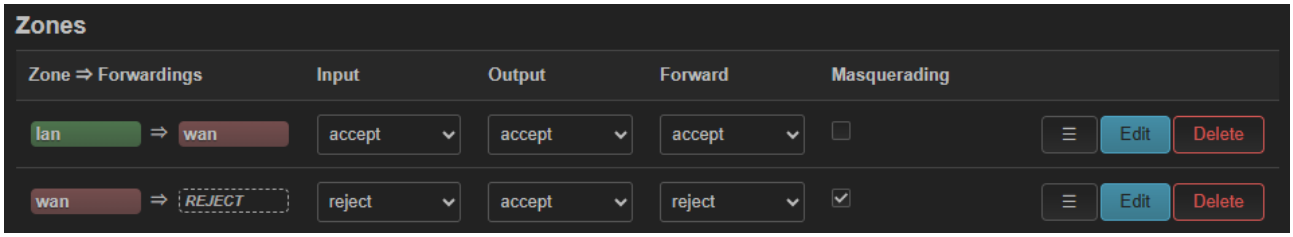
다음과 같이 Zone을 설계하시기를 권장합니다.

- LAN / WAN 기본 유지
- Guest / IoT / VPN은 반드시 별도 Zone 생성
- 신뢰도가 다르면 Zone 분리

Zone 에서는 패킷의 목적지에 따라 아래와 같이 3가지 트래픽 방향을 사용합니다.

- **Input** zone에서 DIVA-IAP-AX 장치로 입력되는 방향
  - SSH9(22), Web(80/443), Ping (ICMP), DNS, DHCP 요청 등
  - WAN에서 DIVA-IAP-AX 접속, LAN에서 DIVA-IAP-AX 관리
- **Output** DIVA-IAP-AX 장치에서 zone으로 출력되는 방향
  - NTP 시간 동기화, VPN 연결, DNS 쿼리
  - 대부분 zone에서 Output accept로 설정
- **Forward** Zone과 Zone 사이의 방향
  - LAN → WAN, Guest → WAN (인터넷 접속)
  - VPN → LAN
  - 클라이언트 간 통신 제어

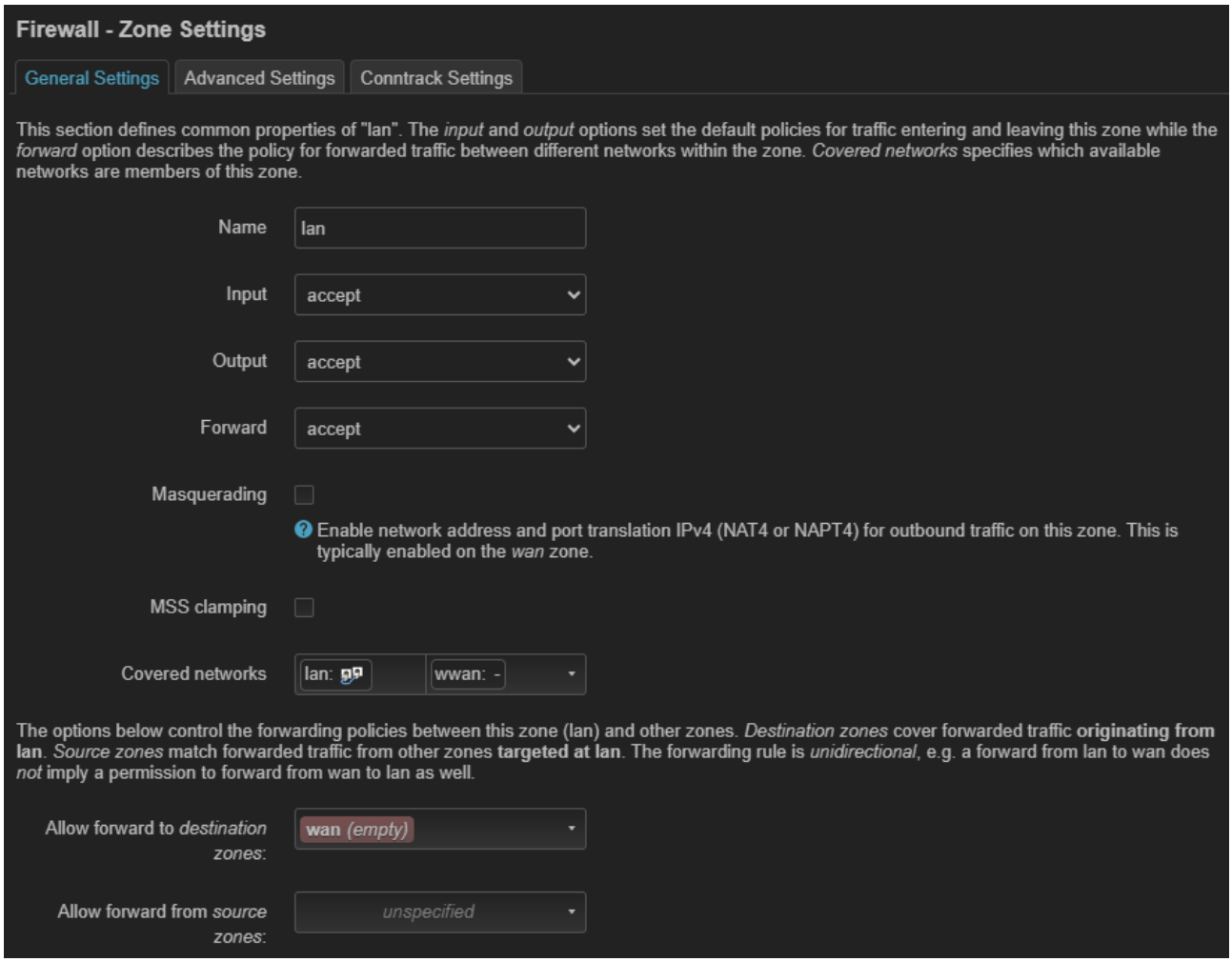
각 Zone 및 Zone과 Zone 사이에는 reject / accept / drop 정책을 설정할 수 있습니다.
아래와 같이 설정된 Zone 정책은 다음과 같이 동작합니다.



- **lan Zone** : 내부 사용자는 라우터/인터넷 모두 자유
- **wan Zone** : 인터넷에서 라우터 접근 차단, 외부로부터 내부 연결 차단

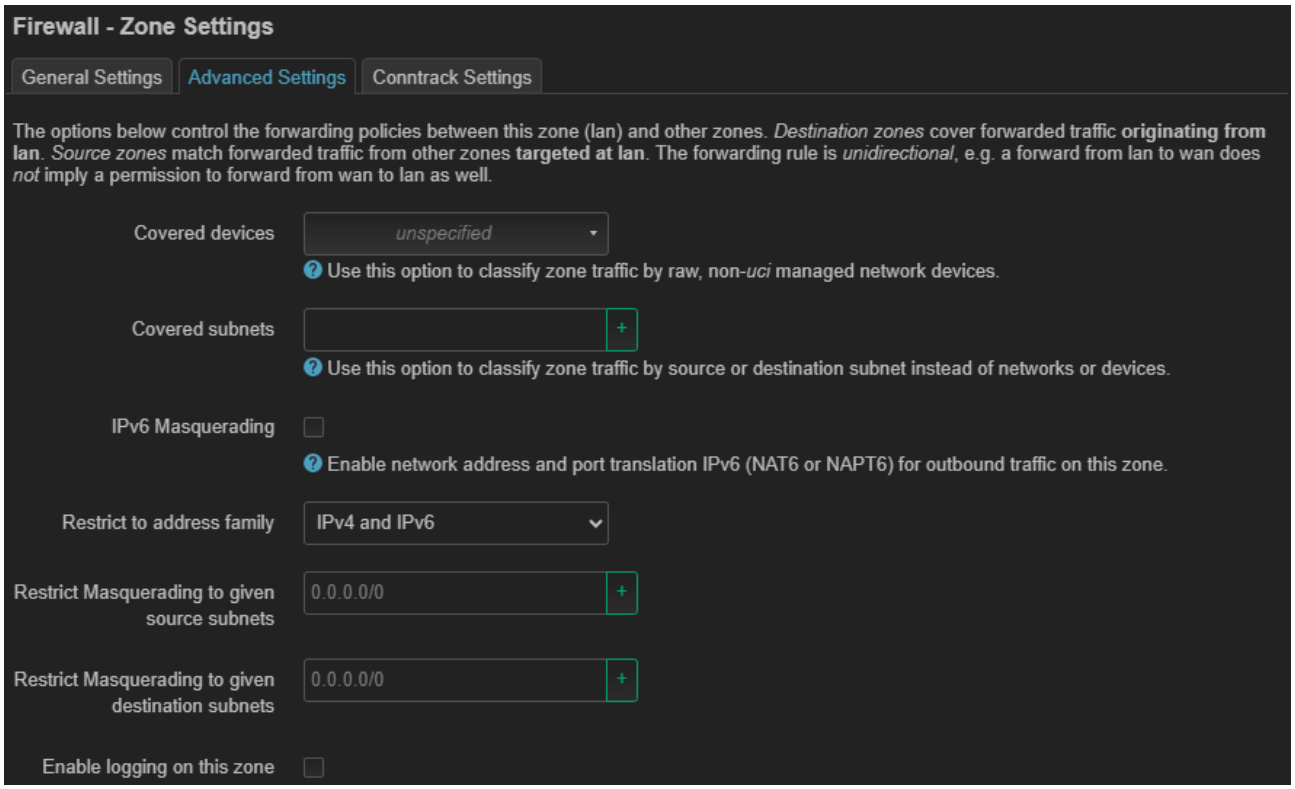
Edit 버튼을 클릭하여 상세 정책을 변경할 수 있습니다. [다음 페이지]

4.4.1.1 Zone > General Settings



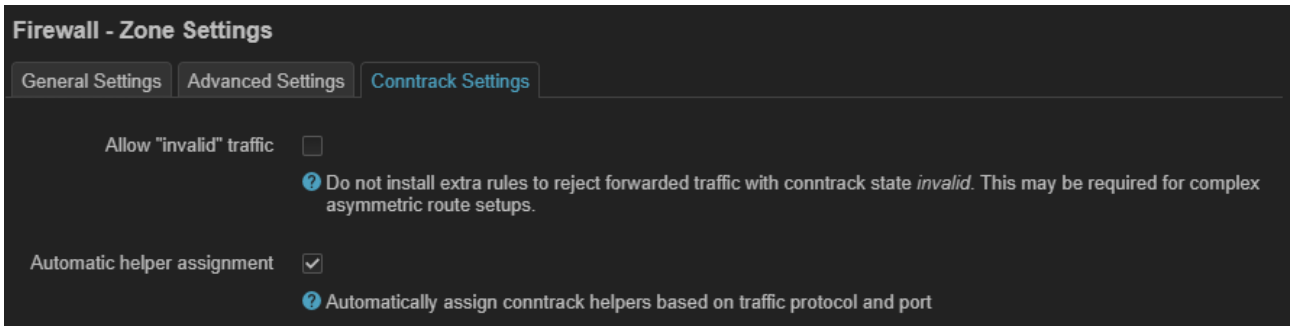
- **Name** Zone 이름을 설정합니다.
- **Input** 수신 방향에 대한 accept / drop / reject 규칙을 설정합니다.
- **Output** 송신 방향에 대한 accept / drop / reject 규칙을 설정합니다.
- **Forward** Zone과 Zone 사이의 포워딩에 대한 accept / drop / reject 규칙을 설정합니다.
- **Masquerading** 출발지 IPv4 주소를 WAN 인터페이스에 설정된 IP 주소로 변경합니다. 예를 들어 IP 공유기에서 내부 사설 IP 주소가 공유기의 공인 IP 주소로 변경되어 인터넷으로 나갑니다. 일반적으로 wan Zone에서 설정하며 lan Zone에서는 설정하지 않습니다.
- **MSS clamping** TCP 패킷의 MSS (Maximum Segment Size) 값을 MTU (Maximum Transmission Unit)에 맞게 줄입니다. VPN / VLAN / 터널링 환경에서는 MSS는 크고, MTU는 작아서 패킷 단편화 및 끊김 현상이 발생할 수 있습니다. 일반적으로 wan Zone에서 설정하며 lan Zone에서는 설정하지 않습니다.
- **Covered networks** 정책이 적용되는 네트워크 인터페이스를 설정합니다.
- **Allow forward to destination zones** 해당 Zone에서 출발한 트래픽이 선택한 Zone으로 전달(Forward)될 수 있도록 설정합니다. forward 정책은 기본적으로 허용/차단 기능을 제공하지만 Allow forward to 정책은 특정 목적지 예외를 허용합니다.
- **Allow forward from source zones** 선택한 Zone에서 들어오는 트래픽을 해당 Zone에 허용하도록 설정합니다.

4.4.1.2 Zone > Advanced Settings



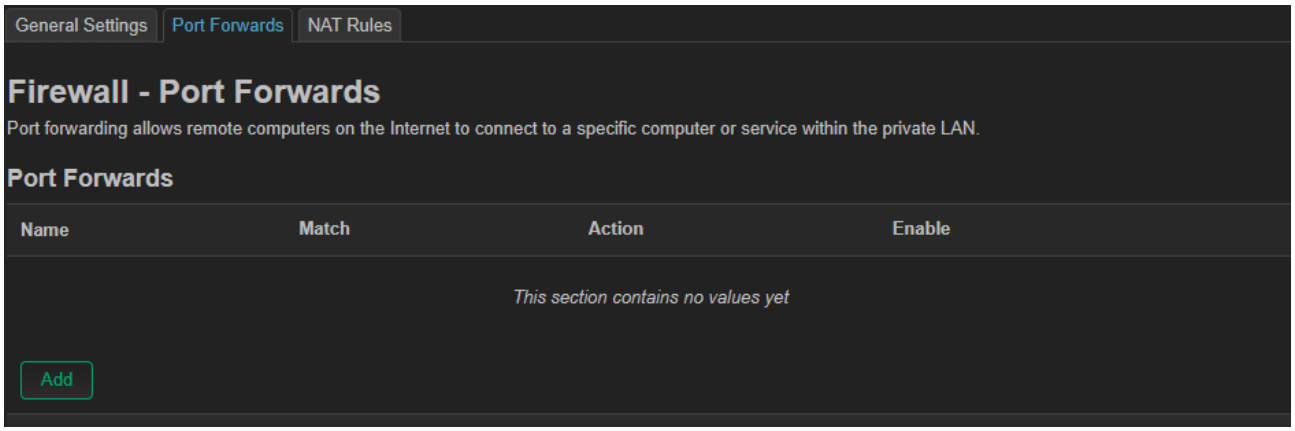
- **Covered devices** 해당 Zone에 어떤 네트워크 장치를 포함할지 선택합니다. 네트워크 인터페이스가 아닌 특정 네트워크 장치만 선택할 때 사용됩니다. 일반적으로 브리지에 포함되지 않은 포트를 보호하거나, 특수한 트래픽을 분리하기 위하여 wan 포트를 device 단위로 직접 Zone에 넣을 때 사용됩니다.
- **Covered subnets** 특정 IP 범위를 이 Zone의 정책 대상에 포함하도록 설정합니다. 특정 VLAN이나 네트워크를 논리적으로 나누지 않고 IP 기준으로 Zone에 포함하려고 할 때 사용될 수 있습니다. 192.168.2.0/24와 같이 CIDR 형식으로 입력합니다.
- **IPv6 Masquerading** IPv6 네트워크에서 NAT를 적용할지 선택합니다. IPv6는 주소가 기본적으로 글로벌 공개가 가능하여 NAT가 필요하지 않습니다. 하지만 내부 IPv6 주소를 외부에 노출하지 않기 위해 NAT66을 사용합니다. 내부 IPv6 주소가 글로벌 IPv6로 변환되고, 외부에서 들어오는 트래픽은 다시 내부 IPv6로 매핑됩니다.
- **Restrict to address family** 해당 Zone에서 처리할 IP 주소 종류를 선택합니다.
  - **IPv4 only** IPv4 트래픽만 처리, IPv6는 무시
  - **IPv6 only** IPv6 트래픽만 처리, IPv4는 무시
  - **IPv4 and IPv6** IPv4와 IPv6 모두 처리
- **Restrict Masquerading to given source subnets** 모든 내부 트래픽이 아니라 지정된 서브넷만 NAT 처리하도록 설정합니다.
- **Restrict Masquerading to given destination subnets** NAT를 적용할 목적지 IP 범위를 제한합니다. 즉, 출발지는 그대로 두고 NAT를 적용할 목적지 IP 주소 범위만 선택합니다.
- **Enable logging on this zone** 방화벽 활동 모니터링을 위해 해당 Zone을 통과하거나 관련 패킷 이벤트를 로그에 기록할지 여부를 설정합니다. Input/Output/Forward 정책 위반 패킷과 reject/drop 처리된 패킷 위주의 이벤트가 로그 기록 대상입니다.

4.4.1.3 Zone > Conntrack Settings



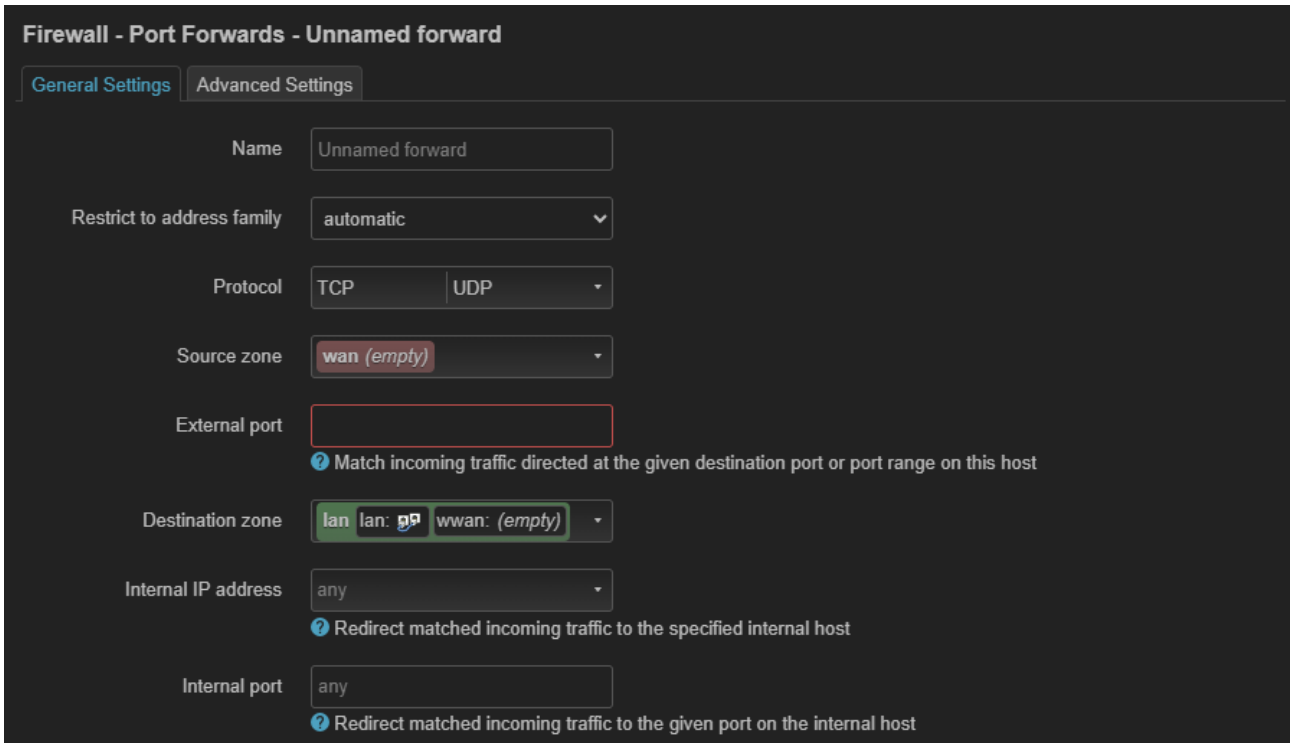
- **Allow "invalid" traffic** DIVA-IAP-AX 장치는 커넥션 추적 기능을 사용하여 각 패킷의 상태를 NEW, ESTABLISHED, RELATED, INVALID 상태로 지정합니다. INVALID 패킷은 커넥션 상태를 알 수 없거나 비정상적인 패킷을 의미하며 커넥션 추적 기능에서 INVALID 상태의 패킷을 허용할지 여부를 설정합니다. 설정을 체크하면 INVALID 패킷도 해당 Zone을 통과할 수 있으며 체크하지 않으면 INVALID 패킷을 차단합니다. (OFF 권장)
  - **NEW** 새 연결 시도
  - **ESTABLISHED** 기존 연결 패킷
  - **RELATED** 관련 연결 패킷 (예: FTP 데이터 채널)
  - **INVALID** 상태를 알 수 없는 패킷
- **Automatic helper assignment** 커넥션 추적에서 특정 프로토콜에 대한 Helper 모듈을 자동으로 적용할지 설정합니다. FTP, SIP, H.323 같은 일부 프로토콜은 다중 연결/포트를 사용하며, NAT 환경에서는 단순 패킷 포워딩만으로 데이터 채널을 추적할 수 없습니다. Helper 모듈은 프로토콜별 트래픽 분석기로서 NAT 포트 매핑 자동 처리를 지원합니다. 기능을 설정할 경우 방화벽이 필요 시 자동으로 helper 모듈을 적용합니다. 예를 들어, LAN에서 FTP를 열면 NAT + FTP helper 모듈이 자동 적용됩니다. 기능을 사용하지 않을 경우 **Conntrack helpers** 항목에서 필요한 모듈을 수동으로 지정할 수 있습니다. 수동 방식은 보안을 강화하고, 불필요한 helper 모듈 로딩을 방지하여 시스템 부하를 줄일 수 있습니다. 가능하면 설정을 해제하고 필요한 서비스만 수동으로 선택하시기 바랍니다. 네트워크 보안을 위해 wan Zone에서는 OFF 설정을 사용하시기 바랍니다. 수동을 선택 가능한 helper 모듈은 다음과 같습니다.
  - **Amanda backup and archiving proto**
  - **FTP passive connection tracking**
  - **RAS proto tracking**
  - **Q.931 proto tracking**
  - **IRC DCC connection tracking**
  - **NetBIOS name service broadcast tracking**
  - **PPTP VPN connection tracking**
  - **SANE scanner connection tracking**
  - **SIP VoIP connection tracking**
  - **SNMP monitoring connection tracking**
  - **TFTP connection tracking**
  - **RTSP connection tracking**

4.4.2 Port Forwards



NAT 기능을 사용할 경우 외부에서 들어오는 특정 포트 트래픽을 내부로 전달합니다. **Add** 버튼을 클릭하여 추가할 포트 포워딩 규칙을 생성합니다.

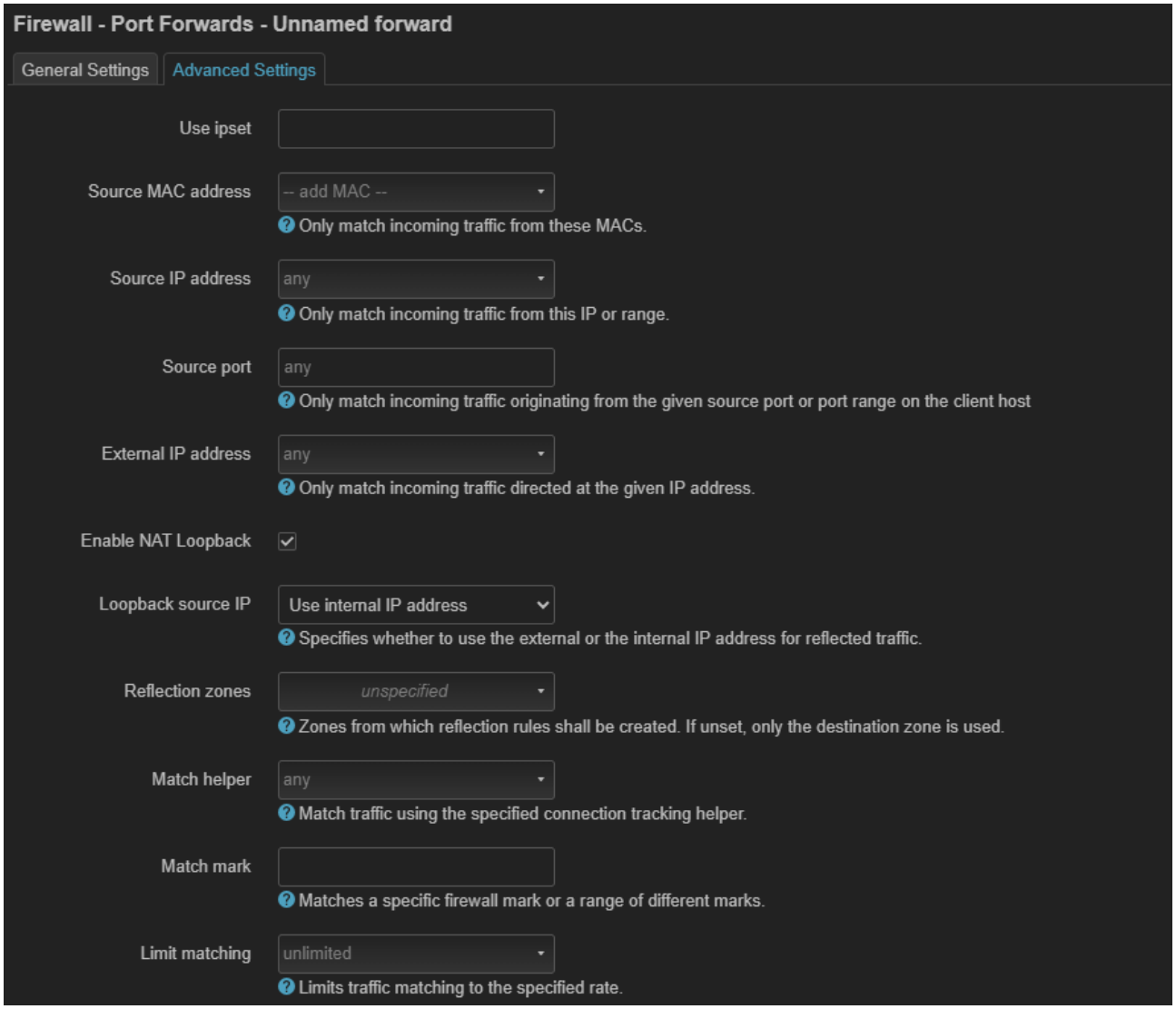
4.4.2.1 Port Forwards > General Settings



- **Name** 규칙 이름을 설정합니다.
- **Restrict to address family** 포트 포워딩 규칙이 적용될 IP 버전을 선택합니다.
  - **automatic** 자동
  - **IPv4 and IPv6** IPv4와 IPv6 패킷 모두 포워딩
  - **IPv4 only** IPv4 패킷만 포워딩, IPv6 패킷 포워딩 불가
  - **IPv6 only** IPv6 패킷만 포워딩, IPv4 패킷 포워딩 불가

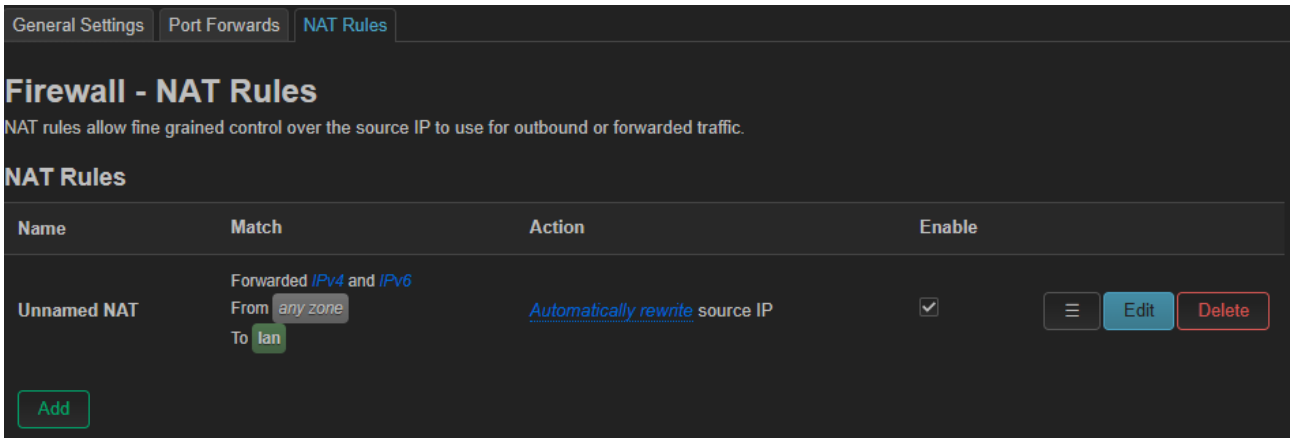
- **Protocol** 포워딩이 허용되는 프로토콜 종류를 선택합니다. (복수 선택 가능)
  - **Any** 모든 프로토콜 가능
  - **TCP** Transmission Control Protocol, 신뢰성 있는 연결 (HTTP, HTTPS, SSH 등)
  - **UDP** User Datagram Protocol, 비연결형 (VoIP, DNS, 게임, 스트리밍 등)
  - **ICMP** ping 네트워크 제어 메시지
  - **custom** 프로토콜 직접 지정 (GRE, ESP 등)
- **Source zone** 외부 트래픽이 들어오는 외부 방화벽 Zone 선택 (일반적으로 wan)
- **External port** 외부에서 접속할 포트 번호 설정
- **Destination zone** 트래픽이 전달되는 내부 Zone 선택 (일반적으로 lan)
- **Internal IP address** 트래픽을 실제 수신하는 내부 장치의 IP 주소
- **Internal port** 내부 장치에서 실제 사용하는 포트 번호
  다른 포트로 매핑 가능 : External port 8080, Internal port 80

4.4.2.2 Port Forwards > Advanced Settings



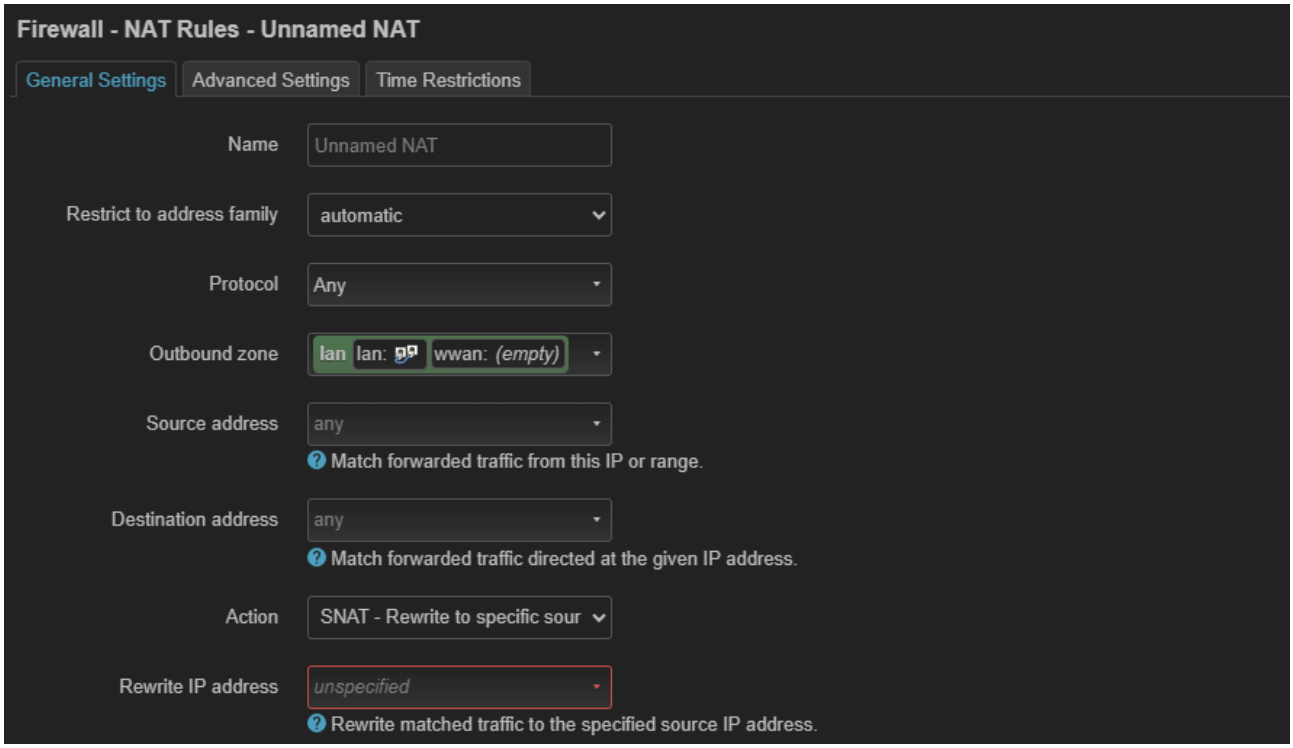
- **Use ipset** 특정 IP 그룹만 포트 포워딩을 적용합니다. (지원하지 않음)
- **Source MAC address** 설정된 MAC 주소 장치에서 들어오는 트래픽만 포워딩을 허용하고, 다른 장치의 트래픽은 무시합니다.
- **Source IP address** 설정된 IP 주소에서 들어오는 트래픽만 포트 포워딩을 허용하고, 다른 IP 장치의 트래픽은 무시합니다.
- **Source port** 포트 포워딩 규칙이 적용될 트래픽의 출발 포트(External Port와 달리 송신측 포트)를 제한합니다. 특정 출발 포트에서 오는 트래픽만 내부 장치로 포워딩 합니다.
- **External IP address** 여러 개의 WAN IP를 사용할 경우, 포트 포워딩 규칙이 적용될 WAN IP를 설정합니다.
- **Enable NAT Loopback** LAN 내부에서 외부 IP/도메인으로 접속 시, 포트 포워딩을 통해 자신이 호스팅하는 내부 서버에 접근하는 것을 허용합니다.
- **Loopback source IP** NAT Loopback 사용 시, 특정 내부 장치의 IP 주소를 등록하여 해당 장치에서 들어오는 트래픽만 허용합니다.
- **Reflection zones** NAT Loopback을 적용할 내부/외부 Zone을 지정합니다.
- **Match helper** 커넥션 추적에서 특정 프로토콜에 대한 Helper 모듈을 적용할지 설정합니다. FTP, SIP, H.323 같은 일부 프로토콜은 다중 연결/포트를 사용하며, NAT 환경에서는 단순 패킷 포워딩만으로 데이터 채널을 추적할 수 없습니다. Helper 모듈은 프로토콜별 트래픽 분석기로서 NAT 포트 매핑 자동 처리를 지원합니다. any 항목을 설정할 경우 방화벽이 필요 시 자동으로 helper 모듈을 적용합니다. 예를 들어, LAN에서 FTP를 열면 NAT + FTP helper 모듈이 자동 적용됩니다. 또한 항목에서 필요한 모듈을 수동으로 지정할 수 있습니다. 수동 지정 방식은 보안을 강화하고, 불필요한 helper 모듈 로딩을 방지하여 시스템 부하를 줄일 수 있습니다. 가능하면 설정을 해제하고 필요한 서비스만 수동으로 선택하시기 바랍니다. 선택 가능한 helper 모듈은 다음과 같습니다.
  - **Amanda backup and archiving proto**
  - **FTP passive connection tracking**
  - **RAS proto tracking**
  - **Q.931 proto tracking**
  - **IRC DCC connection tracking**
  - **NetBIOS name service broadcast tracking**
  - **PPTP VPN connection tracking**
  - **SANE scanner connection tracking**
  - **SIP VoIP connection tracking**
  - **SNMP monitoring connection tracking**
  - **TFTP connection tracking**
  - **RTSP connection tracking**
- **Match mark** 입력된 mark 값을 가진 패킷만 포트 포워딩 합니다. 사용자는 방화벽/iptables에서 0x0 ~ 0xFFFF 사이의 커넥션/패킷 마크를 지정해야 합니다.
- **Limit matching** 포트 포워딩 규칙에 대해 시간당 연결 수를 제한하여, DoS 공격이나 과도한 요청으로 내부 서버가 과부하 되는 것을 방지합니다. 지정된 조건을 초과하면 해당 트래픽 포워딩을 사용할 수 없습니다.
  - **Unlimited** 제한 없음
  - **10/second** 초당 10회
  - **60/minute** 분당 60회
  - **3/hour** 시간당 3회
  - **500/day** 하루 500회
  - **custom** 사용자 지정

4.4.3 NAT Rules



NAT 기능은 패킷의 소스 또는 목적지를 변환합니다. **Add** 또는 **Edit** 버튼을 눌러 규칙을 생성하거나 수정합니다.

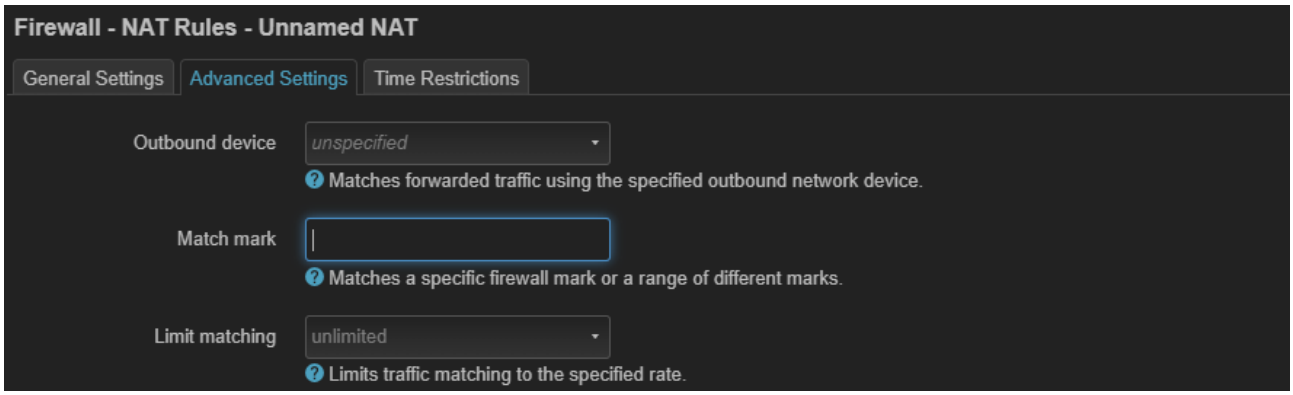
4.4.3.1 NAT Rules > General Settings



- **Name** NAT 규칙 이름을 설정합니다.
- **Restrict to address family** 포트 포워딩 규칙이 적용될 IP 버전을 선택합니다.
  - **automatic** 자동
  - **IPv4 only** IPv4 패킷만 NAT 규칙 적용, IPv6 패킷 불가
  - **IPv6 only** IPv6 패킷만 NAT 규칙 적용, IPv4 패킷 불가

- **Protocol** NAT 규칙이 적용되는 프로토콜 종류를 선택합니다. (복수 선택 가능)
  - **Any** 모든 프로토콜 가능
  - **TCP** Transmission Control Protocol, 신뢰성 있는 연결 (HTTP, HTTPS, SSH, FTP 제어, SMTP 등)
  - **UDP** User Datagram Protocol, 비연결형 (VoIP, DNS, 게임, 스트리밍 등)
  - **ICMP** ping, 오류 메시지
  - **custom** 프로토콜 직접 지정
- **Outbound zone** NAT 처리된 패킷이 전달되는 목적지 Zone 선택
- **Source address** NAT 규칙이 적용될 패킷의 출발지 IP 또는 서브넷을 입력합니다.
  - 단일 IP 설정 : 192.168.1.100 형태로 입력
  - 서브넷(CIDR) 설정 : 192.168.1.0/24
  - 복수 IP 설정 : 192.168.1.100-192.168.1.200
  - 모든 IP : any
- **Destination address** NAT 규칙이 적용될 패킷의 목적지 IP 또는 서브넷을 입력합니다.
  - 단일 IP 설정 : 192.168.1.100 형태로 입력
  - 서브넷(CIDR) 설정 : 192.168.1.0/24
  - 복수 IP 설정 : 192.168.1.100-192.168.1.200
  - 모든 IP : any
- **Action** NAT 규칙에 매칭된 트래픽을 어떻게 변환할지 선택합니다.
  - **SNAT** 출발지 IP를 지정한 IP로 고정 변환합니다. 고정 공인 IP 주소 환경에 적합합니다. Rewrite IP address 항목에 IP 사용할 IP 주소를 입력합니다.
  - **MASQUERADE** 가장 보편적으로 사용되는 방법으로 출발지 IP를 Outbound Zone 인터페이스 IP 주소로 변환합니다. 일반 가정과 같이 자동 IP 환경에 적합합니다.
  - **ACCEPT** NAT 예외 처리용으로 변화 없이 패킷을 그대로 전송합니다.
- **Rewrite IP address** NAT 규칙이 적용될 때, 패킷의 IP를 변경할 대상 IP 주소를 입력합니다. SNAT 방식에서 사용됩니다.

4.4.3.2 NAT Rules > Advanced Settings



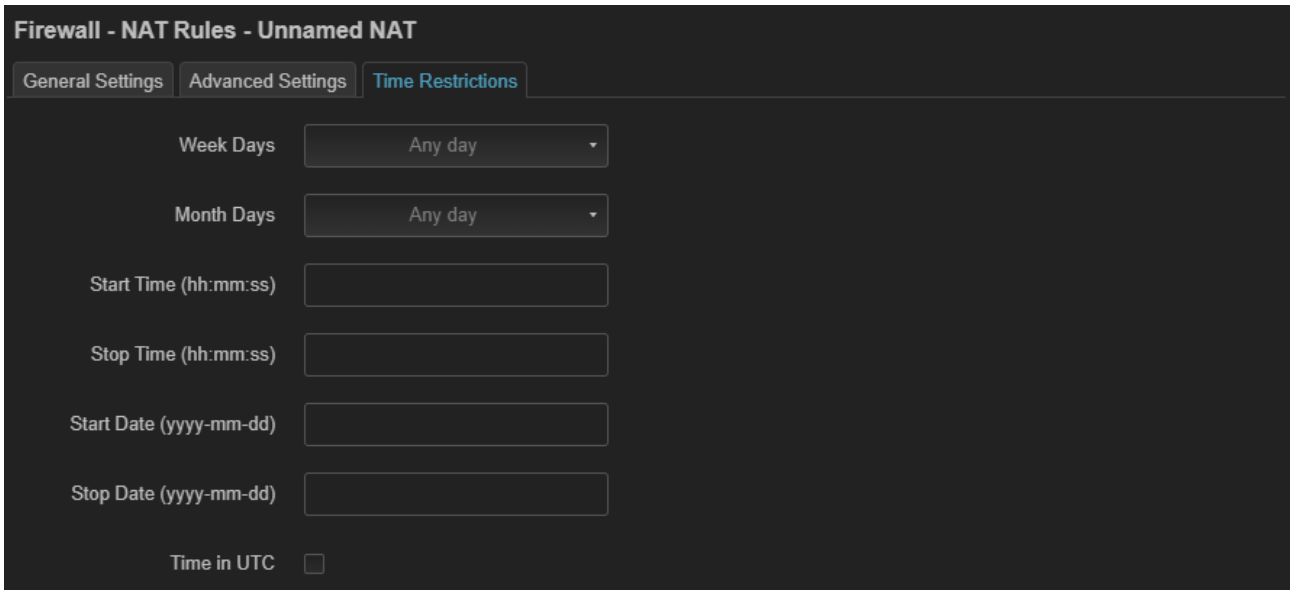
- **Outbound device** 내부 네트워크 트래픽이 외부로 나갈 때 사용하는 인터페이스를 선택합니다.
- **Match mark** 설정한 mark가 붙은 패킷만 NAT 규칙을 적용합니다. (지원하지 않음)

[다음 페이지]

- **Limit matching** NAT 규칙에 대해 시간당 연결 수를 제한하여, 과도한 연결, 오작동, 공격성 트래픽을 제어합니다. 지정된 조건을 초과하면 다음 NAT 규칙으로 넘어가거나 미적용 됩니다.
  - **Unlimited** 제한 없음
  - **10/second** 초당 10회
  - **60/minute** 분당 60회
  - **3/hour** 시간당 3회
  - **500/day** 하루 500회
  - **custom** 사용자 지정

4.4.3.3 NAT Rules > Time Restrictions

설정한 시간대에만 NAT 기능이 활성화되도록 설정합니다.



- **Week Days** 월요일부터 일요일을 중 사용할 요일을 선택합니다. (복수 선택 가능)
- **Month Days** 1일부터 31일 사이의 날짜를 선택합니다. (복수 선택 가능)
- **Start Time (hh:mm:ss)** 매일 시작 시간과 종료 시간을 지정하여 NAT 기능을 사용합니다.
- **Stop Time (hh:mm:ss)** 매일 시작 시간과 종료 시간을 지정하여 NAT 기능을 사용합니다.
- **Start Date (yyyy-mm-dd)** 시작 기간을 지정하여 NAT 기능을 사용합니다.
- **Stop Date (yyyy-mm-dd)** 시작 기간을 지정하여 NAT 기능을 사용합니다.
- **Time in UTC** 시스템 시간 기준을 선택합니다.

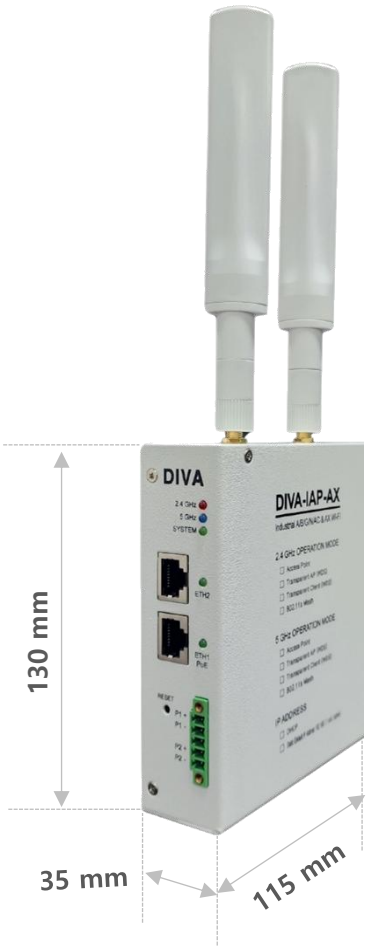
Appendix

무선랜 송신출력 및 수신감도

동작 모드	데이터 속도	최대 송신 출력 (dBm±2dB)		최고 수신 감도 (dBm)	
		2.4GHz	5GHz	2.4GHz	5GHz
802.11b	1 Mbps	23	-	-97	-
	2 Mbps	23	-	-95	-
	5.5 Mbps	23	-	-93	-
	11 Mbps	23	-	-91	-
802.11g 802.11a	6 Mbps	23	23	-95	-95
	9 Mbps	23	23	-93	-93
	12 Mbps	23	23	-91	-90
	18 Mbps	23	23	-89	-88
	24 Mbps	23	23	-86	-86
	36 Mbps	23	23	-83	-84
	48 Mbps	23	23	-80	-81
	54 Mbps	21	21	-78	-79
802.11n HT20 802.11n/ac VHT20	MCS 0	22	23	-95	-96
	MCS 1	22	23	-93	-94
	MCS 2	22	23	-91	-91
	MCS 3	22	23	-88	-89
	MCS 4	22	23	-85	-87
	MCS 5	22	23	-83	-85
	MCS 6	21	21	-81	-82
	MCS 7	20	20	-78	-79
	MCS 8	-	20	-	-76
802.11n HT40 802.11n/ac VHT40	MCS 0	21	23	-92	-93
	MCS 1	21	23	-90	-91
	MCS 2	21	23	-88	-88
	MCS 3	21	23	-85	-86
	MCS 4	21	23	-83	-84
	MCS 5	21	23	-81	-81
	MCS 6	20	21	-78	-78
	MCS 7	19	20	-75	-74
	MCS 8	-	20	-	-72
	MCS 9	-	19	-	-69
802.11ac VHT80	MCS 0	-	23	-	-90
	MCS 1	-	23	-	-88
	MCS 2	-	23	-	-85
	MCS 3	-	23	-	-83
	MCS 4	-	23	-	-80
	MCS 5	-	23	-	-78
	MCS 6	-	21	-	-75
	MCS 7	-	20	-	-72
	MCS 8	-	19	-	-69
	MCS 9	-	19	-	-66

동작 모드	데이터 속도	최대 송신 출력 (dBm±2dB)		최고 수신 감도 (dBm)	
		2.4GHz	5GHz	2.4GHz	5GHz
802.11ax HE20 802.11ax HE20	MCS 0	22	23	-95	-96
	MCS 1	22	23	-93	-94
	MCS 2	22	23	-90	-91
	MCS 3	22	23	-87	-89
	MCS 4	22	23	-84	-86
	MCS 5	22	23	-81	-83
	MCS 6	21	21	-79	-80
	MCS 7	20	20	-76	-77
	MCS 8	18	20	-73	-74
	MCS 9	18	19	-70	-71
	MCS 10	17	18	-68	-68
	MCS 11	17	18	-65	-66
802.11ax HE40 802.11ax HE40	MCS 0	21	23	-92	-93
	MCS 1	21	23	-90	-91
	MCS 2	21	23	-87	-88
	MCS 3	21	23	-85	-85
	MCS 4	21	23	-83	-82
	MCS 5	21	23	-79	-79
	MCS 6	20	21	-77	-77
	MCS 7	19	20	-74	-74
	MCS 8	18	20	-71	-71
	MCS 9	18	19	-68	-68
	MCS 10	17	18	-65	-65
	MCS 11	17	18	-63	-63
802.11ax HE80	MCS 0	-	23	-	-90
	MCS 1	-	23	-	-87
	MCS 2	-	23	-	-84
	MCS 3	-	23	-	-81
	MCS 4	-	23	-	-78
	MCS 5	-	23	-	-75
	MCS 6	-	21	-	-72
	MCS 7	-	20	-	-70
	MCS 8	-	20	-	-67
	MCS 9	-	19	-	-65
	MCS 10	-	18	-	-62
	MCS 11	-	18	-	-59

외관 및 크기

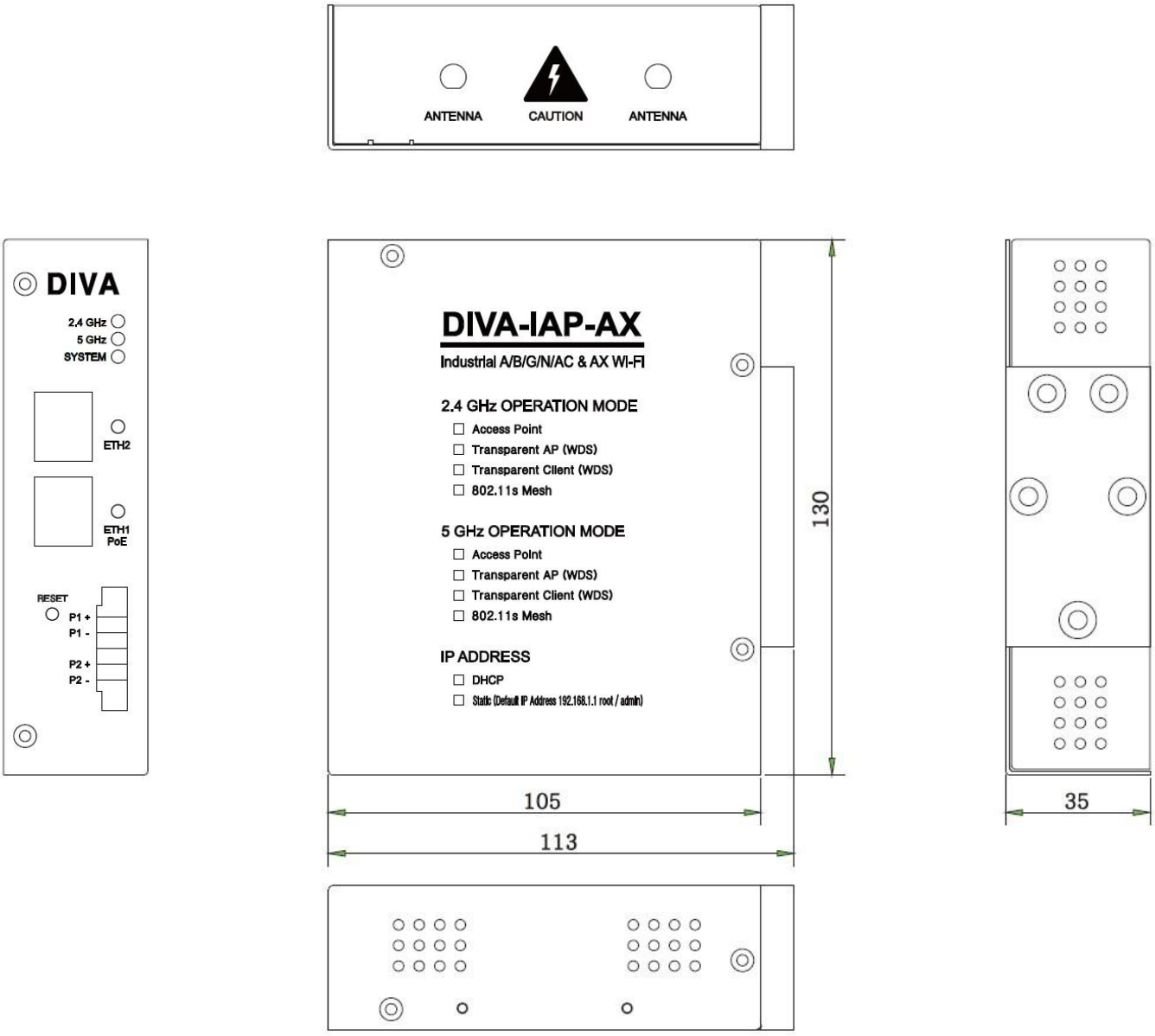


패널 브라켓 모델

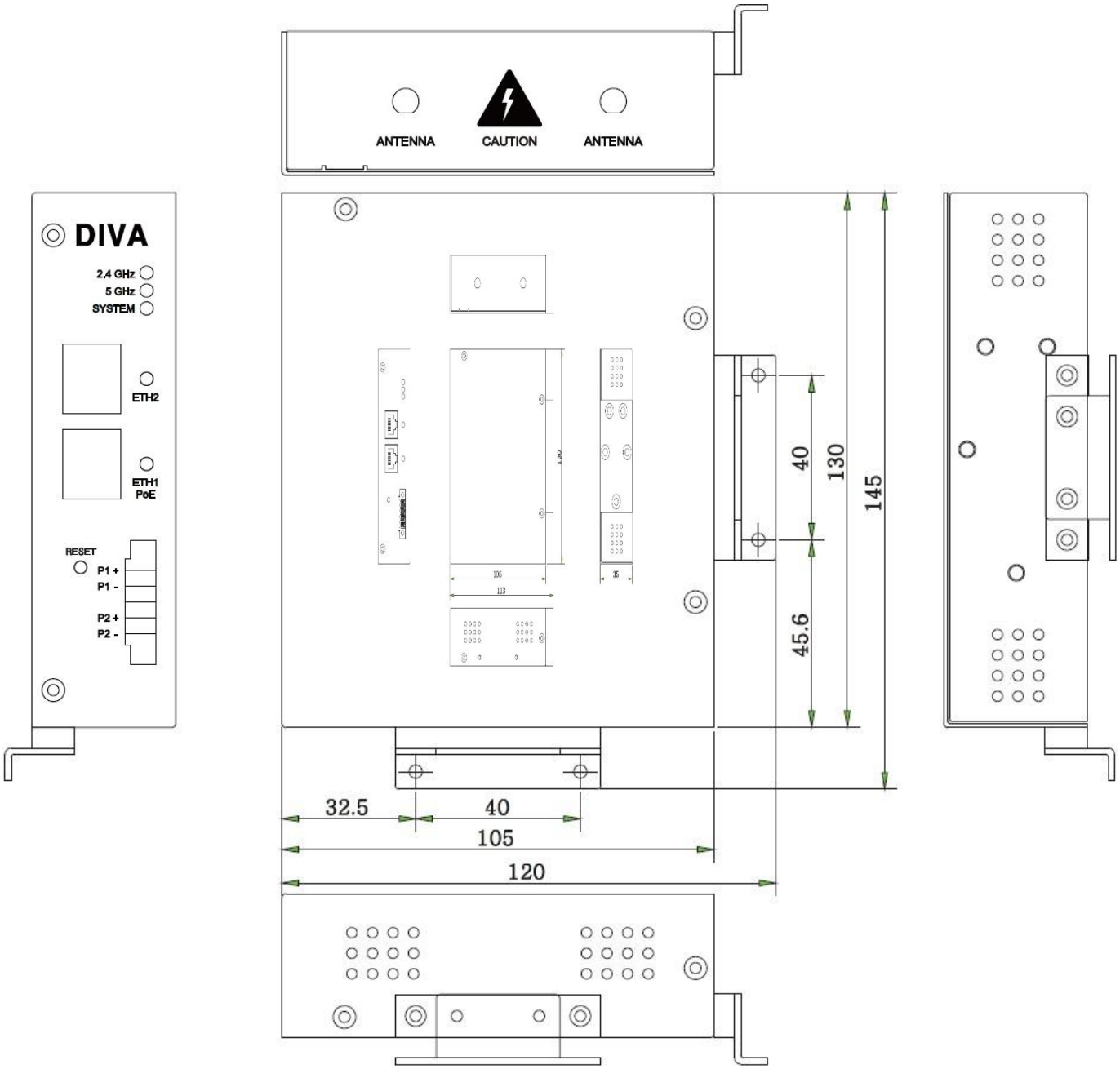
딘레일 브라켓 모델

장착 방식

DIN-Rail 장착



Panel/Wall 장착



제품 보증서

제품명: DIVA-IAP-AX
본 제품은 구입일로부터 1년간 품질을 보증하며 보상 규정은 아래와 같습니다.

보증 규약 내용

1. AS 보증 기간: 구입일로부터 1년간 (구입일 미확인 시 제조일로부터 14개월)
2. 무상 서비스: AS 보증 기간 내 제품의 하자 발생 시
3. 유상 서비스
   - AS 보증 기간이 경과된 제품의 하자 발생 시
   - 화재, 수재, 낙뢰 등의 천재 지변으로 인한 고장 발생 시
   - 임의 개조 또는 수리 등에 의한 하자 발생 시
   - 기타 사용자 과실에 의한 제품 하자 발생 시
4. AS 운송 처리
   - 당사에 직접 입고 원칙
   - 무상 AS 기간내 제품 입고 비용은 사용자 부담, 출고 비용은 당사 부담
   - 무상 AS 기간 이후의 제품 운송 비용은 입출고 모두 사용자 부담
   - 하자가 없는 제품의 입출고 비용은 모두 사용자 부담

주식회사 하이링크

기술문의

㈜하이링크
support@highlink.co.kr