ACKSYS
COMMUNICATIONS & SYSTEMS

WAVEOS
USER GUIDE

[적용모델]

	RuggedAir 시리즈		AirLink
	RailBox 시리즈		AirBox 시리즈
	AirXroad		EmbedAir 시리즈
	WaveNet-Ex		AirWan

Since 2007
WITree
INDUSTRIAL WIRELESS LEADER

ACKSYS
COMMUNICATIONS & SYSTEMS

10, rue des Entrepreneurs
Z.A. Val Joyeux
78450 VILLEPREUX - France

Phone:	**+33 (0)1 30 56 46 46**
Fax:	**+33 (0)1 30 56 12 95**
Web site:	**www.acksys.fr**
Hotline:	**support@acksys.fr**
Sales:	**sales@acksys.fr**

목 차

I INTRODUCTION

이 가이드는 다음 제품에 적용됩니다:

- ❖ RAILBOX, RAILTRACK family, all models
- ❖ Airlink & Airbox series, all models
- ❖ AirWan, all models
- ❖ AirXroad, all models
- ❖ EmbedAir series, all models
- ❖ RuggedAir series, all models
- ❖ WaveNet-Ex series, all models

이 문서에서 특정 제품의 지칭 없이 "제품"을 언급하는 경우 위 목록에 있는 제품 중 하나를 의미합니다.
제품 패키지에 포함된 빠른 시작 가이드와 함께 제품 설치, 구성 및 사용, Wi-Fi 프로토콜에 대한 일반 정보를 다룹니다.
이 참조 가이드에서는 WaveOS 버전을 설명합니다.4.16.9.1.

- 제품에 이전 버전이 포함되어 있는 경우 인터넷 웹 사이트에서 펌웨어 업데이트를 다운로드 할 수 있습니다.
- 제품에 최신 버전이 포함된 경우 당사 웹 사이트에서 설명서 업데이트를 다운로드 할 수 있습니다.

펌웨어 변경 로그(ACKSYS 웹사이트에서 다운로드 가능)는 펌웨어 버전에 따라 어떤 기능을 사용 할 수 있는지 설명합니다.
전원 공급 장치, 안테나 및 연결 케이블과 같은 장비 설치에 대한 모든 권장 사항은 각 제품별 빠른 설치 가이드에 문서화되어 있습니다.

Regulatory information / Disclaimers

이 무선 LAN 장치의 설치 및 사용은 제품과 함께 제공된 사용 설명서에 포함된 지침을 엄격히 준수해야 합니다. 제조업체가 명시적으로 승인하지 않은 이 장치의 변경 또는 수정(안테나 포함)은 장비 작동에 대한 사용자의 권한을 무효화 할 수 있습니다. 제조업체는 이 장치의 무단 개조 또는 제조업체가 지정하지 않은 연결 케이블 및 장비의 교체로 인해 발생하는 라디오 또는 TV 간섭에 대해 책임을 지지 않습니다. 이러한 무단 수정, 대체 또는 부착으로 인해 발생하는 간섭을 수정하는 것은 사용자의 책임입니다.

이 문서의 정보는 예고 없이 변경될 수 있으며 ACKSYS 측의 책무에 해당되지 않습니다.

ACKSYS 는 특정 목적을 포함하되 이에 국한되지 않는 어떠한 종류의 명시적 또는 묵시적 보증 없이 이 문서를 "있는 그대로" 제공하며 수익성이나 사용자 요구 사항에 대한 장비의 적합성에 대해 책임을 지지 않습니다.
ACKSYS 는 언제든지 이 설명서에 설명된 제품 및 프로그램을 개선, 변경할 수 있는 권리를 보유합니다.
이 설명서에 제공된 정보는 정확하고 신뢰할 수 있도록 작성되었습니다.
단, ACKSYS 는 그 사용으로 인해 발생할 수 있는 제 3 자의 권리 침해에 대해 책임을 지지 않습니다.
이 제품에는 의도하지 않은 기술 또는 인쇄상의 오류가 포함될 수 있습니다. 이러한 오류를 수정하기 위해 여기에 있는 정보가 주기적으로 변경되며 이러한 변경 사항은 간행물의 새 판에 통합됩니다.

II PRODUCTS LINE OVERVIEW

II.1 Products goals

이 제품은 이더넷 장치에 Wi-Fi 연결을 제공합니다. 구성에 따라 다양한 토폴로지를 만들 수 있습니다. 자세한 내용은 *Wireless topologies examples* 를 참조하세요.

II.2 Features common to all products

많은 기능이 이 제품 군의 모든 제품에 공통적입니다.

Networking:

Layer 2 software bridging, VLAN, Tunneling, STP/RSTP, 802.1p and 802.11e QOS.
Layer 3 routing with DSCP retagging, NAT, firewall, Diffserv QOS, Multicast routing
DHCP server or client, DNS relay

Configuration and maintenance:

HTTP and HTTPS Web browser configuration
Acksys WaveManager compatibility
SNMP agent for status and configuration
Events handler, alarms
Browser-based firmware upgrades
Emergency upgrade mode
Performance graph trace

Wi-Fi capabilities:

Radio:

- Dual band (2.4 GHz and 5 GHz)
- Support either 802.11n, 20 or 40 MHz channel width or 802.11ac, 20, 40 or 80 MHz channel width
- Backward compatible with 802.11a, b, g, n

Wireless Roles:

- Access point, bridging client, 802.11s Mesh, ad-hoc, RogueAP
- Access point: Client isolation, 802.11x authenticator, slow bit rates lockout, clients MAC filtering
- Client modes: 4 addresses, MAC translation, cloning

Security (depending on the mode):

- WPA2, 802.1x (RADIUS)
- A/B/G compatible security: WPA, WEP

Long-distance Wi-Fi
WME/WMM configuration support
Miscellaneous: 802.11h, 802.11d, client 802.11r support.

II.3 Extra features per product model

이 섹션에서는 특정 소프트웨어 구성과 관련된 기능에 중점을 둡니다. 다른 특징은 각 제품의 빠른 설치 가이드를 참조하세요.

Configuration and maintenance:

C-Key configuration backup
LED status
Hardware alarm contactor, digital output and digital input

Wide area radio networks:

2G/3G/4G data communications, 2 SIM slots
Multi-constellation satellite positioning (GNSS)

Ethernet capabilities:

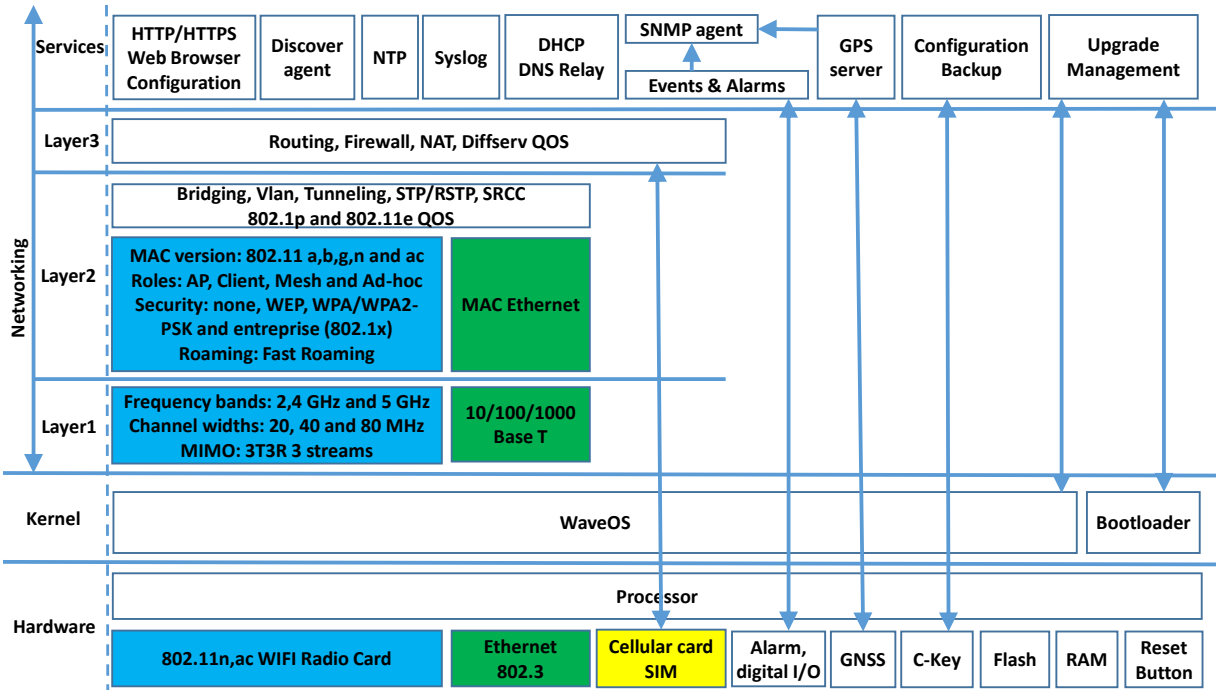
10/100/1000 base T
Auto-crossing (MDX)
Automatic speed and duplex selection

일부 기능은 Radio Card 유형 (802.11n or 802.11ac or 802.11ax)에 따라 다릅니다.

Radio card type / Feature	802.11n	802.11ac	802.11ac Wave 2	802.11ax
802.11 max modulation rate	450 Mbps	1300 Mbps	1730 Mbps	4083 Mbps
Max remote clients per access point	124	128	128	512
Fast Roaming	✓			
Connect Before Break Roaming	✓	✓	✓	
Scanning/roaming cluster	✓	As scanner	As scanner	
Mesh	✓			
Line Topology Repeater	✓			
Multiple roles per radio (AP, client, repeater, portal)	✓	✓	✓	16
Dual radio repeater	✓	✓	✓	✓
VLAN-tagged frames forwarding	✓	✓	✓	✓
SRCC support[1]		✓	✓	✓

1. SRCC 는 첫 번째 무선 카드의 802.11ac 에서만 작동합니다: **RuggedAir/1000** and **Railbox/2x**

II.4 System design



II.5 Products settings compatibility

제품 설정은 웹 인터페이스를 통해 파일로 백업하거나 C-KEY 에서 백업할 수 있습니다. 이 백업은 모든 제품군과 호환되지 않습니다.

이 섹션은 제품 간의 백업 호환성을 보여줍니다.

Backup from	Backup can be loaded in
RailBox/10*	RailBox/10*
RailBox/11*	RailBox/11*
RailBox/22*	RailBox/22*
RailBox/20*	RailBox/20*
RailBox/24*	RailBox/27*
RailBox/27*	RailBox/24*

III DEVICE INSTALLATION

이 매뉴얼을 보기 전에 핵심적인 내용을 살펴볼 수 있도록 제품 박스 내 quick start guide 를 먼저 확인해 주시기 바랍니다.

III.1 Power supply

빠른 시작 가이드는 제품의 최대 전력 소비를 제공합니다. 이 값을 전원 공급 장치에서 제공해야 하는 최소값으로 고려해야 합니다. 또한 고려해야 할 추가 사항이 있습니다. 이러한 제품에는 무선 통신 중에 빠른 전력 서지를 유발할 수 있는 Wi-Fi 라디오 카드가 포함되어 있습니다. 이러한 서지는 빠른 시작에서 제공하는 전력 소비에 포함되지만 전원 공급 장치가 너무 느려 전원을 공급할 수 없는 경우 제품 재부팅 또는 예측할 수 없는 동작이 발생할 수 있습니다.

III.2 Antenna types

다음 섹션에서는 가장 일반적으로 사용되는 안테나 유형과 설치 방법에 대해 설명합니다.

이러한 설명은 복사 패턴이 나타내는 것을 잘 살펴봐야 합니다. 내용이 어려우면 먼저 다음 링크를 참조하세요. *http://www.antenna-theory.com/basics/radPattern.html*.

다음 섹션에 표시된 방사 패턴은 각 안테나 유형의 고유한 특성을 더 잘 이해할 수 있도록 예시로만 제공됩니다.

III.2.1 Omnidirectional antenna (무지향성 안테나)

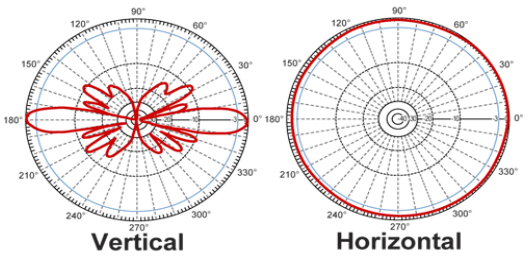
방사 전력은 모든 수평 방향에서 균일합니다. 안테나 축(수직) 방향에 접근하면서 전력이 점진적으 로 떨어집니다. 해당 방사 패턴도 함께 참조하세요.

이 유형의 안테나는 안테나 주변의 넓은 영역을 커버하는 데 사용됩니다.

안테나 사용 시 같은 평면에 배치되어 있는지 확인하세요.

Antenna

Radiation pattern

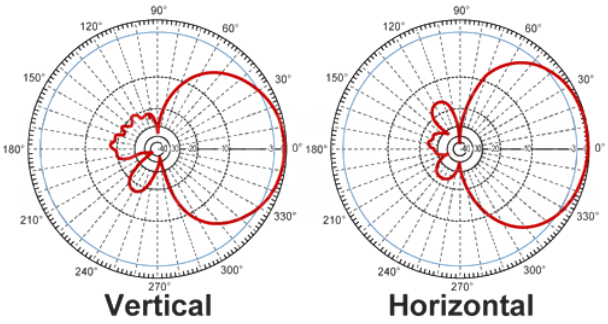


III.2.2 Patch antenna

패치 안테나는 한쪽에 방사를 집중시킵니다. 이를 통해 벽에 방사선을 낭비하지 않고 벽에 장착할 수 있습니다. 이득은 일반적으로 7dBi 와 9dBi 사이로 구성됩니다.

Antenna

Radiation pattern

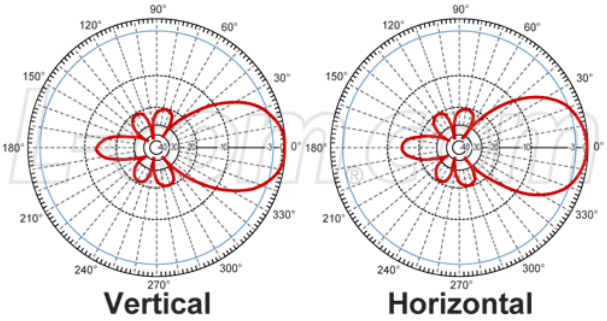


III.2.3 Yagi antenna

야기 안테나는 한쪽에 방사를 집중시킵니다. 이득은 일반적으로 11dBi ~ 15dBi 이며 패치 안테나 보다 높습니다.

Antenna

Radiation pattern

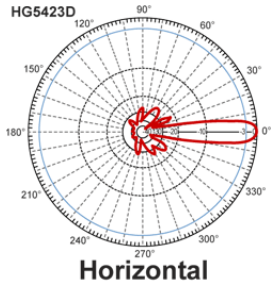


III.2.4 Dish antenna

접시 안테나는 방사를 한 지점에 집중시킨 다음 매우 높은 이득(>20dBi)값을 얻을 수 있습니다.

Antenna

Radiation pattern



III.2.5 MIMO antenna

안테나 제조업체는 앞에서 설명한 각 안테나 유형의 MIMO 버전을 제공합니다. MIMO 안테나는 기본적으로 single enclosure 에 결합된 여러 표준 안테나 세트(보통 2 개 또는 3 개)입니다.

제조사의 안테나 데이터 시트를 참조하여 안테나의 방사 패턴과 내부 레이아웃을 참조해보시기 바랍니다.

III.3 Antenna installation

무선 커넥터는 SMA, RPSMA, QMA, N-Type 등 여러 종류가 있습니다. SMA 와 RPSMA 는 비슷해 보이지만 중앙의 핀이나 모양이 거꾸로 되어 있습니다. RPSMA 는 Wi-Fi 용도로만 사용됩니다. GPS 또는 셀룰러 라디오와 같은 용도는 SMA 커넥터를 사용합니다.

Wi-Fi 안테나 설치 시 크게 두 가지 고려해야 할 사항이 있습니다.

III.3.1 Legacy 802.11a/b/g case

수 백 미터까지 Wi-Fi 링크를 설정할 수 있지만 몇 가지 주의가 필요합니다:

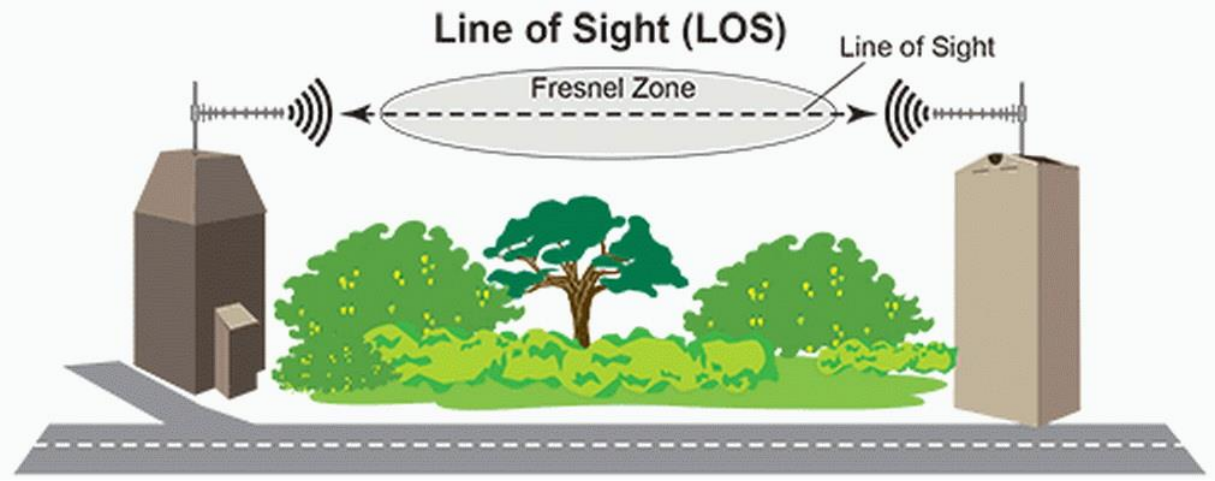
기기 간의 거리와 장애물에 따라 제품의 EIRP 를 조정해야 합니다(단, 현지 규정 범위 내에서 유지해야 함). EIRP (Effective Istropically Radiated Power, 실효 출력).

신호세기 RSSI 는 충분히 높아야 합니다. 그렇지 않으면 환경 변화(기후 조건 변화 또는 공간 재구성) 시 링크가 끊어질 수 있습니다.

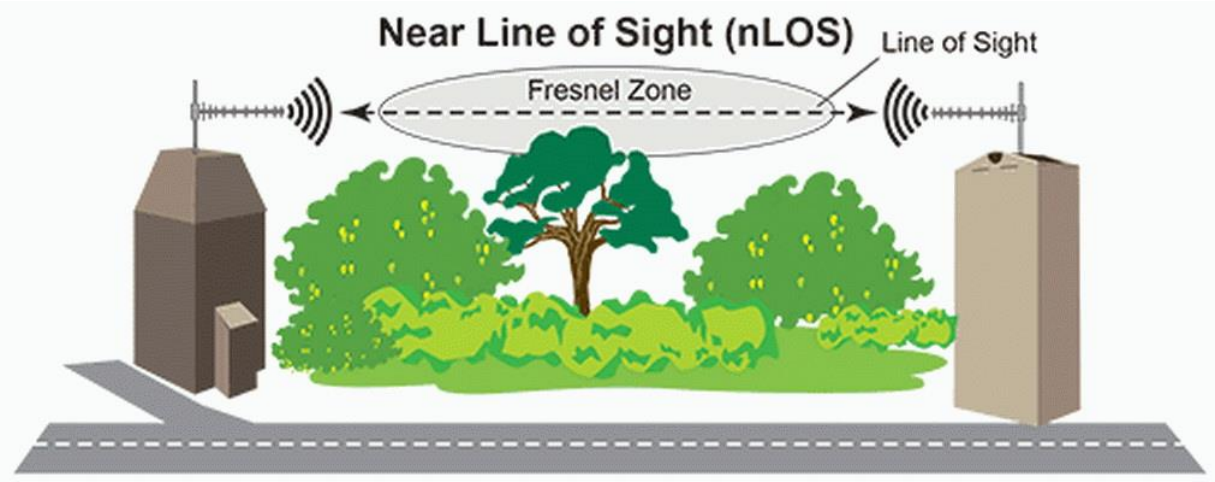
EIRP 를 높이려면 다음 중 하나를 수행할 수 있습니다:

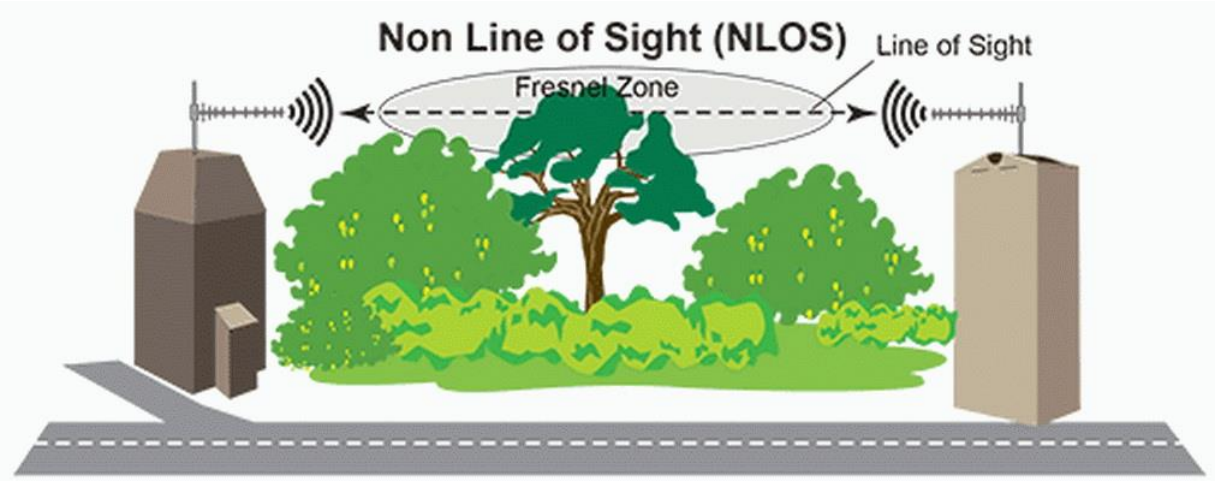
- 더 큰 이득값을 가진 안테나를 사용하고,
- 더 큰 무선 출력을 가진 제품을 사용하며,
- 그리고 더 좋은 품질의 커넥터와 무선 케이블을 사용하세요.

실외 링크의 경우 제품은 다른 제품과 가시거리 (Line of sight)가 확보되어야 합니다. 이것은 필수조건이며 주의 깊게 고려해야 합니다. 아래 그림은 가시거리가 의미하는 바를 설명합니다.



비가시선(NLOS) 및 근거리 가시선은 일반적으로 가장 안쪽 프레넬 영역의 물리적 물체에 의해 부분적으로 차단된 경로를 통한 무선 전송입니다.





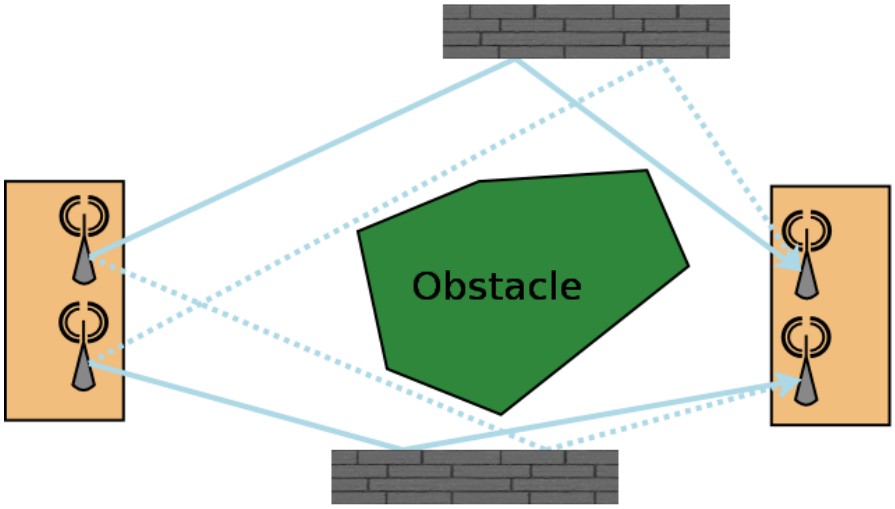
Near Line Of Sight 는 일반적으로 더 나은 안테나를 사용하여 처리할 수 있지만 Non Line Of Sight 에는 일반적으로 대체 경로 또는 다중 경로 전파 방법이 필요합니다.

일반적으로 NLOS 상태를 일으키는 장애물에는 건물, 나무, 언덕, 산 등이 있습니다.

III.3.2 802.11n/ac/ax

이러한 제약을 보완할 802.11n/ac/ax 는 MIMO(다중 입력 다중 출력) 기술을 활용하고 다중 안테나를 사용함으로써 어느 정도의 장애물이 있다 하더라도 통신이 가능합니다.

802.11a/b/g 제품은 이미 하나 이상의 안테나를 사용하지만 다이버시티 모드(한 번에 하나의 안테나만 전송)로 제한되었습니다. 또한 벽이나 기타 장애물에 부딪히면 수신기를 혼동시키는 여러 경로가 발생합니다.



802.11n/ac 는 이러한 바운스를 사용하여 여러 independent streams(2~4)을 동시에 보내고 식별할 수 있 습니다. 수신기는 해당 패턴을 사용하여 자체 보정하고 각 안테나의 전송 채널을 특성화합니다.

이 정보를 사용하여 수신기는 어떤 스트림이 어떤 안테나에 속하는지 계산할 수 있습니다.

이 경우 전송될 스트림당 적어도 하나의 안테나가 있어야 합니다. 여분의 안테나는 추가 공간 정보를 전송하는 데 사용됩니다.

802.11n/ac 는 바운스를 사용하여 대역폭을 늘리므로 가시선이 확보된 실외 어플리케이션의 경우는 바운스가 전혀 없기 때문에 실내 어플리케이션에 비해 성능이 떨어집니다. 이 문제는 편광된 전파를 서로 직교하게 보내면 해결할 수 있습니다. "Slant Antennas" 는 실제로 단일 케이스에 결합된 2 개의 편파된 안테나로 만들어집니다.

III.3.3 Cellular antennas

안테나를 하나만 사용하는 경우 "main" 안테나 커넥터에 연결되어 있는지 확인하세요. "diversity" 커넥터는 수신을 증가시키는데만 사용됩니다.

다이버시티 안테나를 사용하는 경우에는 메인 안테나에서 최소 30cm 이상 떨어져서 동축 케이블 이 잘 분리되도록 하세요.

최상의 성능을 위한 준비 :

- 안테나를 지면과 수직으로 유지하고,
- 금속 물체에 둘러싸여 있지 않도록 하며
- 다이버시티 안테나는 편파와 메인 편파가 일치하지 않도록 배치합니다.

III.3.4 GNSS antennas

GNSS 는 GPS, GALILEO 및 유사한 위성 위치 확인 시스템의 일반적인 약어입니다. GNSS 안테나는 active 또는 passive 의 두 가지 유형이 있습니다. active 안테나에는 안테나 케이블을 통해 전원이 공급되는 내장 전치 증폭기가 있습니다.

active 입력 커넥터에 passive 안테나를 연결하면 전원 공급 장치가 수명이 단축될 수 있습니다. passive 입력 커넥터에 active 안테나를 연결하면 수신이 약해집니다. 항상 입력 커넥터에 적합한 올바른 유형의 안테나를 사용하세요.

GNSS 신호는 미약합니다. 케이블은 가능한 한 짧게 유지하세요. GNSS 무선 주파수에 방해될 수 있는 불투명한 유리창을 조심하세요.

III.4 802.11 radio channel choice

Wi-Fi 표준 호환 제품은 두 개의 RF 대역을 사용할 수 있습니다.

- 2.4 GHz 대역은 802.11b/g/n 표준과 호환되는 채널을 포함하며,
- 5 GHz 대역은 802.11a/n/ac 표준과 호환되는 채널을 포함합니다.

최적의 성능을 위해 무선 채널을 선택할 때 몇 가지 사항을 고려해야 합니다.

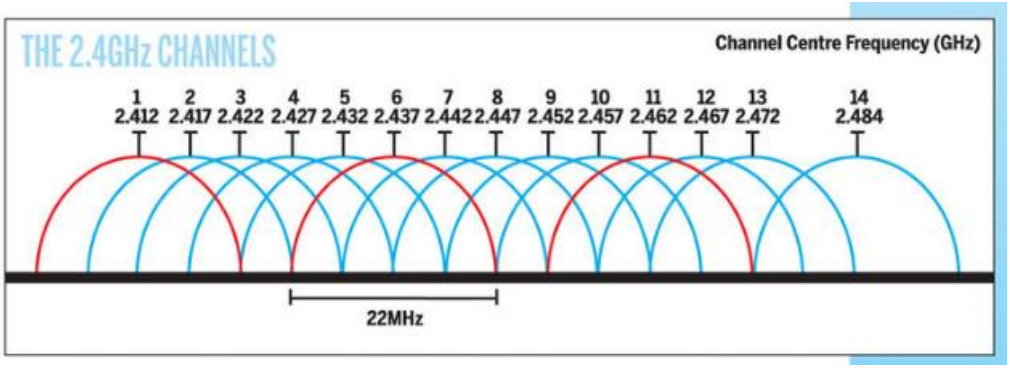
- 우선, 일부 채널 사용을 금지하거나 제한할 수 있는 현지 규제 규칙
- 법률 및 하드웨어에 의해 제한될 수 있는 각 채널의 전송 전력
- 동일한 채널에서 작동하는 다른 Wi-Fi 장치 또는 전자레인지, 무선전화기, 블루투스 장치, 기타 무선장치와 같은 Wi-Fi 가 아닌 장치에서 발생하는 무선 잡음 및 간섭
- 시스템의 모든 액세스 포인트가 동일한 채널을 사용할 때 “hidden station” 영향으로 인한 충돌

대역별 안테나를 구매하기 전에 과부하된 무선 채널을 감지하기 위해 예비 사이트 조사는 필수입니다. 과부하된 채널은 성능에 큰 영향을 줄 수 있으므로 AP 가 적게 분포된 채널을 사용하는 것이 좋습니다.

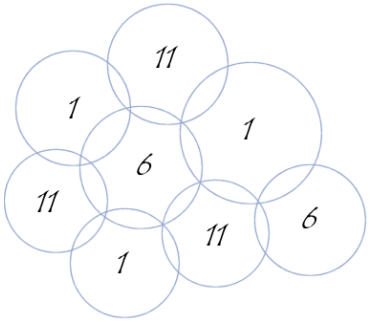
Wi-Fi 성능은 또한 무선 링크 품질(RSSI 라고도 함)에 따라 크게 달라집니다. RSSI 가 좋을수록 처리량은 증대되고 오류율이 더 적어질 수 있습니다. 신호 품질은 거리, 장애물, 좁은 통로, 습도 및 안테나 방향 등에 따라 달라질 수 있습니다.

III.4.1 2.4GHz overlapping radio channels

무선 채널은 사용 중인 중심 주파수의 표시입니다. 변조는 채널을 20-22MHz 대역으로 확장합니다. 여러 Wi-Fi 셀이 2.4GHz(5GHz 채널이 겹치지 않음)에서 서로 가까이 있을 때 이를 고려해야 합니다. 그렇지 않으면 간섭으로 인해 효과적인 성능이 저하됩니다. 이 지점은 여러 액세스 지 점이 있는 지리적 영역을 커버하려고 할 때 특히 중요합니다.



'비중첩' 채널 1, 6, 11 의 사용은 제품이 너무 가까울 때 제한이 있지만 1-6-11 가이드라인은 장점 이 있습니다. 송신기 채널이 채널 1, 6 및 11(예: 1, 4, 7 및 10)보다 더 가깝게 선택되는 경우 채널 간의 중첩으로 인해 신호 품질 및 처리량이 허용할 수 없을 정도로 저하될 수 있습니다.



Picture III-1: 겹치지 않는 채널의 예시

III.5 802.11 regulatory domain rules

Wi-Fi 라디오 채널 사용을 제어하기 위해 전 세계적으로 널리 사용되는 3 가지 주요 규제 규칙이 있습니다.

- ETSI: 유럽 국가용
- FCC: 미국 국가용
- MKK/TELEC: 아시아 국가용

특정 규제 영역(프랑스, 브라질, 한국, 호주 ...)은 몇 가지 수정을 거쳐 주요 규제 규칙에서 파생됩니다.

규제 영역은 각 RF 대역을 사용하는 규칙을 제공합니다.

현지 법률을 준수하려면 Wi-Fi 카드를 활성화하기 전에 제품을 설치할 국가를 선택해야 합니다.

III.5.1 Antenna gain and RF output power

고이득 안테나를 사용할 계획이라면, 사용할 국가에서 허용되는 EIRP 를 초과할 수 있습니다. 이 경우 제품의 무선 전송 전력을 수동으로 줄여야 합니다 (see *Advanced Settings tab* in section *VI.1.1.1 Wireless/Radio*).

다음 섹션에서는 제품 전송 전력을 사용된 안테나에 적용하기 위한 FCC 및 ETSI 규칙을 찾을 수 있습니다.

용어 정의:

RF Output power: 안테나 없이 ACKSYS 무선기기에서 방사되는 RF 전력

EIRP: 안테나가 있는 ACKSYS 무선기기에서 방사되는 RF 전력

EIRP = RF OUTPUT POWER + ANTENNA GAIN (dBi)

III.5.2 FCC rules for 2.4 GHz band

2.4 GHz point to multipoint: MAX EIRP = +36 dBm (4 Watts)				
MAX RF Output POWER dBm	(mW)	MAX Gain dBi	MAX EIRP dBm	(W)
30	(1000)	6	36	(4)
27	(500)	9		
24	(250	12		
21	(125)	15		
18	(62.5)	18		
15	(32)	21		
12	(16)	24		

이득이 6dBi 이상인 안테나를 사용할 경우, 6dBi 이상의 이득이 1dBi 일 때마다 MAX RF 출력을 1dB 줄여야 합니다.

2.4 GHz point to point: MAX EIRP = special rules				
MAX RF Output POWER dBm	(mW)	MAX Gain (dBi)	MAX EIRP dBm	(W)
30	(1000)	6	36	(4)
29	(800)	9	38	(6.3)
28	(630)	12	40	(10)
27	(500)	15	42	(16)
26	(400)	18	44	(25)
25	(316)	21	46	(39.8)
24	(250)	24	48	(63)
23	(200)	27	50	(100)
22	(160)	30	52	(158)

6dBi 보다 높은 이득을 가진 안테나를 사용할 때, 6dBi 를 초과하는 3dBi 이득마다 MAX RF 출력 전력은 1dB 감소해야 합니다.

III.5.3 FCC rules for 5 GHz band

5 GHz point to multipoint: MAX EIRP = special rules						
BAND	Freq. (GHz)	Channels	Location	MAX RF output POWER (dBm/mW)	MAX Gain (dBi)	MAX EIRP (dBm/mW)
UNII	5.15-5.25	36, 40, 44, 48	Indoor & outdoor	16 / 40	6(1)	22 / 160
UNII-2	5.25-5.35	52, 56, 60, 64	Indoor & outdoor	23 / 200	6(1)	29 / 800
UNII-2 ext.	5.470-5.725	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Indoor & outdoor	23 / 200	6(1)	29 / 800
UNII-3	5.725-5.825	149 to 165	outdoor	29 / 800	6(1)	35 / 3.2 W

(1) 6dBi 이상의 이득이 있는 안테나를 사용하는 경우 6dBi 이상의 안테나 이득이 1dBi 증가할 때마다 MAX RF 출력 POWER 의 1dB 감소가 필요합니다.

5 GHz point to point: MAX EIRP = special rules						
BAND	Freq. (GHz)	Channels	Location	MAX RF output POWER (dBm/mW)	MAX Gain (dBi)	MAX EIRP (dBm/mW)
UNII	5.15-5.25	36, 40, 44, 48	Indoor	16 / 40	6	22 / 160
UNII-2	5.25-5.35	52, 56, 60, 64	Indoor & outdoor	23 / 200	6	29 / 800
UNII-2 ext.	5.470-5.725	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Indoor & outdoor	23 / 200	6	29 / 800
UNII-3	5.725-5.825	149 to 165	outdoor	30 / 1 W	23(2)	53 / 200 W

(2) 23dBi 이상의 이득이 있는 안테나를 사용하는 경우 23dBi 이상의 안테나 이득이 1dBi 증가할 때마다 MAX RF 출력 POWER 의 1dB 감소가 필요합니다.

일부 채널에는 DFS 지원이 필요합니다. 섹션 참조 "*Radars detection overview (DFS)*".

III.5.4 ETSI rules for 2.4 GHz band

2.4 GHz point to multipoint: MAX EIRP = +20 dBm (100 mWatts)						
BAND	Freq. (GHz)	Channels	Location	MAX RF output POWER (dBm/mW)	MAX Gain (dBi)	MAX EIRP (dBm/mW)
ISM	2.4-2.483	1 to 13	Indoor/ outdoor	NA	NA	20 / 100

III.5.5 ETSI rules for 5GHz band

5 GHz point to multipoint: MAX EIRP = special rules						
BAND	Freq. (GHz)	Channels	Location	MAX RF output POWER dBm (mW)	MAX Gain (dBi)	MAX EIRP (dBm/mW)
UNII	5.15-5.25	36, 40, 44, 48	Indoor	NA	NA	23 / 200
UNII-2	5.25-5.35	52, 56, 60, 64	Indoor	NA	NA	If TPC 23 / 200 Else 20 / 100
UNII-2 ext.	5.470-5.725	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Indoor & outdoor	NA	NA	If TPC 30 / 1000 Else 27 / 500
UNII-3	5.725-5.825	149 to 165	Forbidden	NA	NA	NA

TPC 는 송신 전력 제어를 의미합니다. 통신을 시작하는 2 개의 장치는 서로 인지할 수 있을 만큼 각각의 전력 레벨이 최대한 낮도록 협상하는 메커니즘 입니다.

일부 채널에는 DFS 지원이 필요합니다. 섹션 참조 "*Radars detection overview (DFS)*".

III.5.6 Radars detection overview (DFS)

일부 지역에서는 무선 장비가 5GHz 대역의 특정 레이더 시스템을 방해하지 않는지 확인하는 것이 중요합니다. 레이더가 감지되면 무선 네트워크는 자동으로 레이더 시스템을 방해하지 않는 채널로 전환합니다. 레이더가 감지될 때 채널을 해제하는 것을 DFS(동적 주파수 선택)라고 합니다.

레이더 감지는 마스터 장치(AP, 메시 노드, Ad-hoc)에만 필요합니다. 슬레이브 장치(클라이언트) 의 경우 레이더 감지는 필요하지 않지만 장치는 수동 스캔을 사용해야 합니다(네트워크에 가입할 때만 수신). 수동 스캔은 숨겨진 SSID 에 대한 연결을 허용하지 않습니다(능동 스캔이 필요함). 실 제로 클라이언트는 숨겨진 SSID AP 를 식별하기 위해 프로브(액티브 스캔)를 보내야 합니다.

레이더 탐지는 거리, 에코 및 기타 위험에 의해 무선 신호가 왜곡될 수 있기 때문에 확률론적 활동 입니다. 무선 하드웨어는 무선 신호를 알려진 레이더 패턴과 비교합니다. 이 메커니즘은 본질적으 로 두 가지 방식으로 실패할 수 있습니다.

- 왜곡되어 실제 레이더 패턴을 감지하지 못합니다.
- 다른 무선 신호가 왜곡되어 레이더 신호와 유사한 결과를 가져오기 때문에 존재하지 않는 레이더 패턴을 감지합니다. 이를 오탐지라고 합니다.

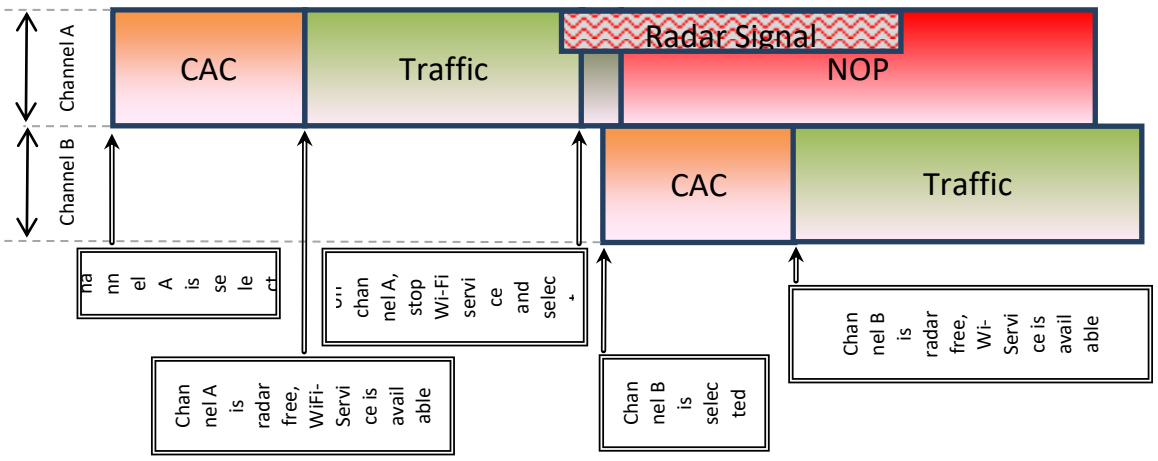
탐지기는 이러한 함정을 피하기 위함이지만 100% 정확한 탐지를 보장할 수는 없습니다. 그리고 실제로 표준은 100% 탐지하는 것을 요구하지 않습니다. 이로 인해 잘못된 감지가 발생하고 경우에 따라 예기치 않은 채널 전환이 발생할 수 있습니다.

ACKSYS 제품은 적용 가능한 모든 채널의 데이터베이스를 유지하며, 각 채널은 "Radar Free", "Radar detected", "No radar detection"으로 표시됩니다. 제품은 "Radar free" 또는 "No radar detection"으로 표시된 채널만 선택할 수 있습니다.

선택한 채널에 DFS 메커니즘이 필요한 경우 제품은 CAC(채널 가용성 확인) 기간을 시작합니다. 이 기간 동안 제품은 채널에 레이더가 없는지 확인하기 때문에 Wi-Fi 서비스를 사용할 수 없습니 다. CAC 기간 동안 레이더가 감지되면 해당 채널은 "Radar detected"으로 표시되고 제품은 다른 채널을 선택합니다.

선택한 채널이 "radar free"인 경우 제품이 작동할 수 있습니다. 작동 중 제품은 스펙트럼을 지속 적으로 모니터링하여 레이더 패턴을 검색합니다. 레이더가 감지되면 Wi-Fi 서비스를 중지하고 다 른 채널을 선택합니다.

레이더 감지 후 채널은 NOP(채널 회피 기간) 동안 "Radar detected"으로 표시됩니다. 이 기간 동안 제품은 이 채널을 선택할 수 없습니다.



ETSI 또는 FCC 표준에 따라 두 가지 일반적인 레이더 파형 목록을 감지해야 합니다. 기본적으로 일반적인 레이더 파형은 다음과 같은 다양한 매개변수로 정의됩니다.

- Pulse Width
- Number of pulses per radar burst
- Time between pulses (Pulse Repetition Frequency or Pulse Repetition Interval)
- Number of bursts

DFS 가 필요한 채널 목록은 다음과 같습니다.

DFS in FCC			
Channels	BAND	CAC period	NOP period
36, 40, 44, 48	UNII	DFS is not required	
52, 56, 60, 64	UNII-2	1 min	30 min
100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	UNII-2 ext.	1 min	30 min
149 to 165	UNII-3	DFS is not required	

DFS in ETSI			
Channels	BAND	CAC period	NOP period
36, 40, 44, 48	UNII	DFS is not required	
52, 56, 60, 64	UNII-2	1 min	30 min
100, 104, 108, 112	UNII-2 ext.	1 min	30 min
116,120, 124, 128		10 min	30 min
132, 136, 140		1 min	30 min

CAC 및 NOP 기간은 최소값입니다.

참고: Slave device(Client)가 레이더 감지를 지원하지 않는 경우 EIRP 는 23dBm 으로 제한됩니다.

III.5.7 Specific DFS features for ACKSYS products range

ACKSYS 제품은 AP, 메시 노드 및 AD-HOC 의 세 가지 마스터 역할을 지원합니다. AP 역할만 DFS 를 지원합니다. 따라서 두 개의 다른 마스터 역할(메시 노드, ad-hoc)은 비 DFS 채널만 사용할 수 있습니다.

슬레이브 모드에서 ACKSYS 제품은 수동 스캔 모드를 사용하기 때문에 레이더 감지를 지원하지 않지만 DFS 요구 사항을 충족합니다. EIRP 는 항상 23dBm 보다 낮아야 합니다.

채널 116 에 대한 ETSI 모드의 CAC 기간은 10 분으로 강제되는 반면 최소 권장 값은 1mn 입니다. 이를 통해 채널 116/120 이 있는 HT40 및 채널 116/120/124/128 이 있는 HT80 을 지원할 수 있 습니다.

ACKSYS 제품이 감지한 레이더 파형 목록은 다음과 같습니다.

- ETSI EN 301 893 표준. 지원되는 릴리스는 제품의 DFS 테스트 보고서/CE 선언에 언급되어 있습니다. 모든 버전에 새로운 레이더 펄스가 추가됩니다.
- FCC 파트 15 하위 파트 E. 지원되는 릴리스는 DFS 테스트 보고서에 언급되어 있습니다.

IV ADMINISTRATION OVERVIEW

IV.1 Web interface

제품을 설정하는 주요 방법은 웹 브라우저 인터페이스에서 진행됩니다. *Web Interface reference* 부분 참조.

제품에 액세스하려면 먼저 IP 주소를 설정해야 합니다. 이 작업은 Acksys Wave Manager software 를 사용하여 진행해도 됩니다.

Microsoft Internet Explorer 11 을 제외한 모든 최신 브라우저를 사용할 수 있습니다.

IV.2 Reset pushbutton

RESET 푸시버튼은 세 가지 용도로 사용됩니다.

- 짧게(< 2 초) 누르면 제품이 재부팅됩니다. 재부팅이 되면 제품이 작동할 때까지 DIAG LED 가 빨간색으로 계속 켜집니다.
- 제품이 실행되는 동안 길게 누르면 공장 초기화로 재설정됩니다. DIAG LED 가 빨간색으로 바뀔 때까지 재설정 버튼을 누르고 있으면 됩니다.
- 시작할 때 길게 누르면(전원을 켤 때나 재부팅 직후에) "Emergency upgrade" 모드가 활성화됩니다. 모드가 활성화되면 DIAG LED 가 빠르게 깜박입니다. 이 모드는 Acksys WaveManager 로 펌웨어를 다시 로드 하거나 푸쉬 버튼을 다시 눌러 공장 초기화로 재설정할 수 있습니다.(위 참조)

IV.3 Acksys WaveManager

Acksys WaveManager 는 Acksys 제품을 탐색하고, 설정값을 확인할 수 있으며 IP 주소를 세팅할 수 있습니다. 또한 SSID, WiFi 주파수도 설정 가능합니다.

Acksys WaveManager 는 제품이 "Emergency upgrade" 모드일 때 펌웨어를 다시 로드하는 것도 가능합니다.

IV.4 Emergency upgrade

푸시 버튼을 통해 "긴급 업그레이드" 모드로 들어갑니다. 정기적인 펌웨어 업그레이드 중에 제품 의 전원이 꺼지거나 제품이 완전히 작동하지 않는 상태인 경우 복구할 수 있습니다.

"Emergency upgrade" 모드는 챕터에 자세히 설명되어 있습니다. *VIII Firmware Upgrade*

IV.5 SNMP agent

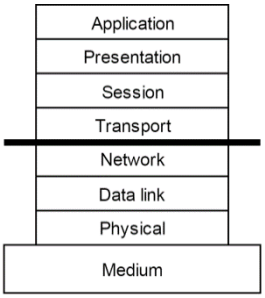
제품에는 Acksys WaveManager, HP OpenView™ 또는 net-snmp 명령과 같은 SNMP manager 에서 구성 및 모니터링을 허용하는 SNMP agent 가 포함되어 있습니다.
SNMP 에이전트는 해당 장에 자세히 설명되어 있습니다.

V TECHNICAL REFERENCE

V.1 Networking components

V.1.1 OSI model

네트워킹 기능에 대한 논의는 OSI(Open Systems Interconnection) 모델을 참조합니다. ISO 에서 표준화한 통신 시스템의 개념적 관점입니다. 추가 설명을 위한 다음 링크를 참조하세요. *http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html*



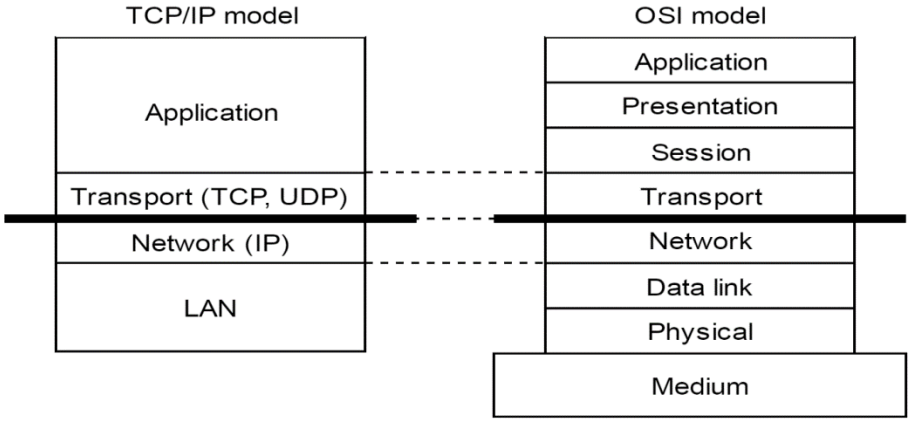
Picture V-1: The OSI layers

이 사용자 가이드는 모델의 세 가지 하위 계층인 물리적, 데이터 링크 및 네트워크에 중점을 둡니다.

V.1.2 TCP/IP model

TCP/IP 는 인터넷과 대부분의 인트라넷에서 사용하는 프로토콜 스택입니다.

TCP/IP 네트워크에 참여하는 장치에는 4 개의 소프트웨어 계층이 있습니다. Application layer, Transport layer (TCP 또는 UDP), Network layer (IP), LAN layer (Ethernet, Wi-Fi, point-to-point 등). TCP/IP 모델은 OSI 보다 오래되었지만 OSI 의 모델 중 하나이기 때문에 상관관계가 있습니다.



Picture V-2: TCP/IP 모델과 OSI 모델의 비교

각 계층에는 고유한 목적과 주소 지정 체계가 있습니다.

LAN layer address 는 동일한 LAN 에 연결된 다른 장치로 데이터를 보낼 수 있도록 합니다. 그러나 라우터를 통해 다른 LAN 에 연결된 장치에 보낼 LAN 주소 정보가 충분하지 않습니다.

Network (IP) address 는 라우팅 대상이 될 수 있는 주소를 정의하여 이 문제를 해결합니다. 소스 장치와 대상 장치가 동일한 LAN 에 있지 않은 경우 소스 장치는 중간 라우터(게이트웨이라고도 함)로 데이터를 보낼 수 있습니다. 라우터에는 다른 게이트웨이를 통해 대상 장치로 데이터를 전달할 수 있는 라우팅 테이블이 있습니다.

Transport layer address, "port"라고도 함. 대상 장치 내부에서 올바른 응용 프로그램 프로세스에 데이터를 전달하는 데 사용됩니다.

패킷을 변경하지 않고 MAC 주소에 따라 두 물리적 링크 간에 패킷을 이동할 수 있습니다. 이를 bridging 또는 switching 이라고 합니다. IP 주소에 따라 대상을 선택하여 LAN 간에 패킷을 이동할 수 있습니다. 이를 routing 이라고 합니다. 라우팅은 IP 주소를 가장하거나 라우팅을 선택적으로 비 활성화할 수 있는 가능성과 같은 추가 기능을 제공합니다. 이것이 방화벽입니다.

V.1.3 LAN layer: network interfaces

TCP/IP 네트워크의 맥락에서 네트워크 인터페이스는 다른 컴퓨터와 통신하는 방법입니다. 이 방법은 이더넷 LAN 과 같은 하드웨어 및 소프트웨어 드라이버 또는 두 컴퓨터의 COM 포트를 연결하는 한 쌍의 모뎀이 될 수 있습니다. PABX, Wi-Fi 인프라 또는 이중화를 위해 쌍을 이루는 이더넷과 같은 전체 하위 시스템일 수도 있습니다.

WaveOS 에서 네트워크 인터페이스는 통신 포트를 개념화하는 소프트웨어 개체로 구현됩니다. 다음과 같은 사이의 통신을 제공합니다.

- IP 네트워킹 계층이나 브리지와 같은 상위 소프트웨어 계층,
- 물리적 미디어, 터널, Wi-Fi "roles" 또는 브리지와 같은 하위 통신 인터페이스.

브리지 내에서 호환 가능한 네트워크 인터페이스를 그룹화할 수 있습니다. 액세스 포인트는 일반적으로 이더넷 LAN 과 브리지되어 Wi-Fi 클라이언트에 대한 이더넷 액세스를 제공합니다. IP 프로토콜은 브리지가 외부 하드웨어 스위치인 것처럼 브리지를 단일 IP 주소를 가진 단일 인터페이스로 봅니다.

네트워크 인터페이스에 IP 주소를 부여하면 IP 계층에 연결됩니다.

V.1.4 Physical interface

물리적 인터페이스는 이더넷 카드나 WiFi 무선 카드와 같은 하드웨어 장치에 의존하는 소프트웨어 개체입니다.

0 매개변수를 변경한 후에는, **Save** 를 눌러 영구적인 메모리에 기록합니다. 이 경우 변경 사항은 즉시 적용되지 않고, 재시작 후 또는 **Save & Apply** 후에만 적용됩니다.

Save & Apply 를 누르게 되면 지금까지 모든 페이지에서 수행한 모든 구성 변경 사항을 적용하게 됩니다.

Reset (사용 가능한 경우) 을 눌러 양식의 데이터를 이전 값(마지막 저장 **save** 후 표시되는 값)으로 되돌립니다.

Physical interfaces 하위 메뉴는 물리적 인터페이스를 구성합니다.

V.1.5 Network segment

네트워크 세그먼트는 두 대 이상의 컴퓨터를 상호 연결하고 물리적 "signals"를 교환할 수 있도록 하는 하드웨어 어셈블리입니다. (예: RJ45 케이블, 동축 이더넷 또는 이더넷 허브로 연결된 RJ45 케이블).

이더넷 호환 네트워크에서 네트워크 세그먼트의 개념은 "collision domain"과 유사합니다. 전송된 프레임을 항상 수신하는 장치와 미디어에 액세스하기 위해 동기화해야 하는 장치를 나타냅니다.

네트워크 스위치는 포트 사이의 프레임을 필터링하기 때문에 네트워크를 여러 세그먼트로 분할합니다. 반대로 레거시 네트워크 허브는 포트 간에 충돌이 발생할 수 있으므로 단일 세그먼트를 공유하는 몇몇 포트의 속성을 유지합니다.

V.1.6 Virtual interface

가상 인터페이스는 데이터 프레임에 대한 특수 목적 처리를 구현하고 물리적 인터페이스 또는 다른 가상 인터페이스와 연결되는 소프트웨어 개체입니다.

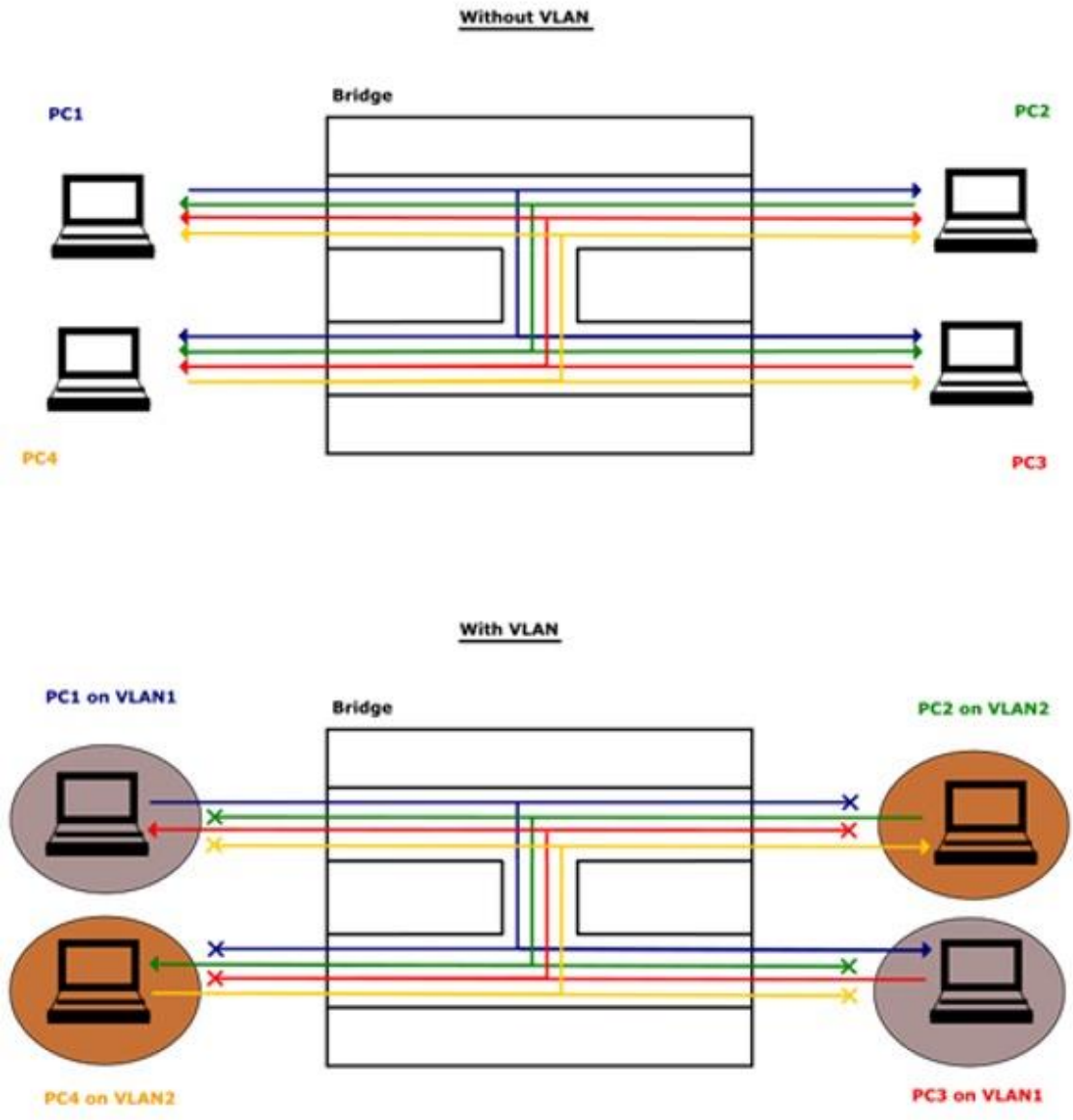
가상 장치는 일반적으로 터널을 생성하거나 VLAN 을 사용하여 하나의 매체를 통해 관련 없는 여러 흐름을 다중화하는 데 사용됩니다.

Cellular 하위 메뉴는 가상 인터페이스를 구성합니다.

V.1.7 VLAN

VLAN(가상 LAN) 개념은 각 하위 도메인에 VLAN 식별 번호, VLAN_ID 를 할당함으로써 데이터 링크 계층의 브로드캐스트 도메인을 여러 개의 하위 도메인으로 분할 할 수 있게 합니다.

VLAN 에는 여러 가지 장점이 있습니다. 브로드캐스트 프레임의 대상을 하위 도메인으로 줄이고 동일한 물리적 네트워크를 공유하면서 관련 없는 호스트를 격리하며 브리지가 VLAN ID 를 기반으로 다른 전달 결정을 내릴 수 있도록 합니다.



Picture V-3: 컴퓨터는 동일한 VLAN 에 있는 컴퓨터에서만 수신합니다.

V.1.7.1 Frame tagging

네트워크 세그먼트가 여러 VLAN 에 대한 프레임을 전달해야 하는 경우 프레임에는 해당 VLAN_ID 가 태그로 지정됩니다.

V.1.7.2 Vlan interface

VLAN 인터페이스는 물리적 인터페이스에서 수신 트래픽의 VLAN_ID 를 필터링한 다음 VLAN_ID 를 제거하여 태그를 해제하는 가상 인터페이스입니다. 반대로 VLAN 인터페이스의 모든 나가는 트래픽은 VLAN_ID 로 태그가 지정됩니다.

VLAN 인터페이스는 하위 메뉴의 VIRTUAL INTERFACES/802.1Q TAGS 로 구현됩니다.

참조: *VI.1.2.1 802.1q Tagging*

V.1.8 Bridge

브리지는 2 개 이상의 802.1 호환 네트워크 세그먼트를 연결하고 프레임을 선택적으로 전달하는 장치입니다. 브리징은 OSI 모델의 레이어 2(데이터 링크 레이어)에서 수행됩니다. 프레임은 라우터와 달리 IP 주소가 아닌 이더넷 주소를 기반으로 전달됩니다. 전달은 레이어 2 에서 이루어지기 때문에 모든 레이어 3 프로토콜은 브리지를 통해 투명하게 이동할 수 있습니다.

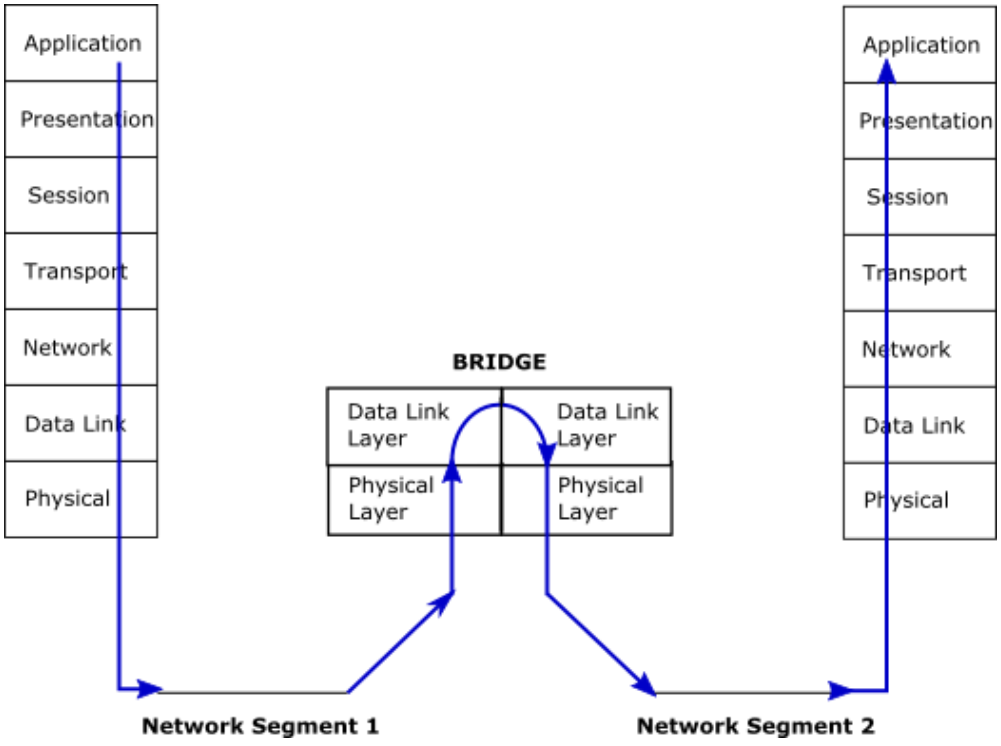
각 네트워크 세그먼트는 포트를 통해 브리지에 연결됩니다. 포트는 물리적 또는 가상 인터페이스 일 수 있습니다.

브리지는 연결된 각 네트워크 세그먼트에서 사용 중인 MAC 주소의 내부 목록을 작성합니다. 프레임을 전달할 때 브리지는 테이블에서 대상을 찾아 주소가 있는 포트로만 전달합니다. 대상 주소가 테이블에서 발견되지 않으면 프레임이 복제되어 원래 포트를 제외한 모든 포트에서 전달됩니다.

브리지는 "switch"라는 별개의 하드웨어로 나타날 수 있습니다. 또는 라우터는 레이어 3 에서 구성할 단일 레이어 2 인터페이스의 여러 포트를 그룹화하는 "software bridge"를 포함할 수 있습니다.

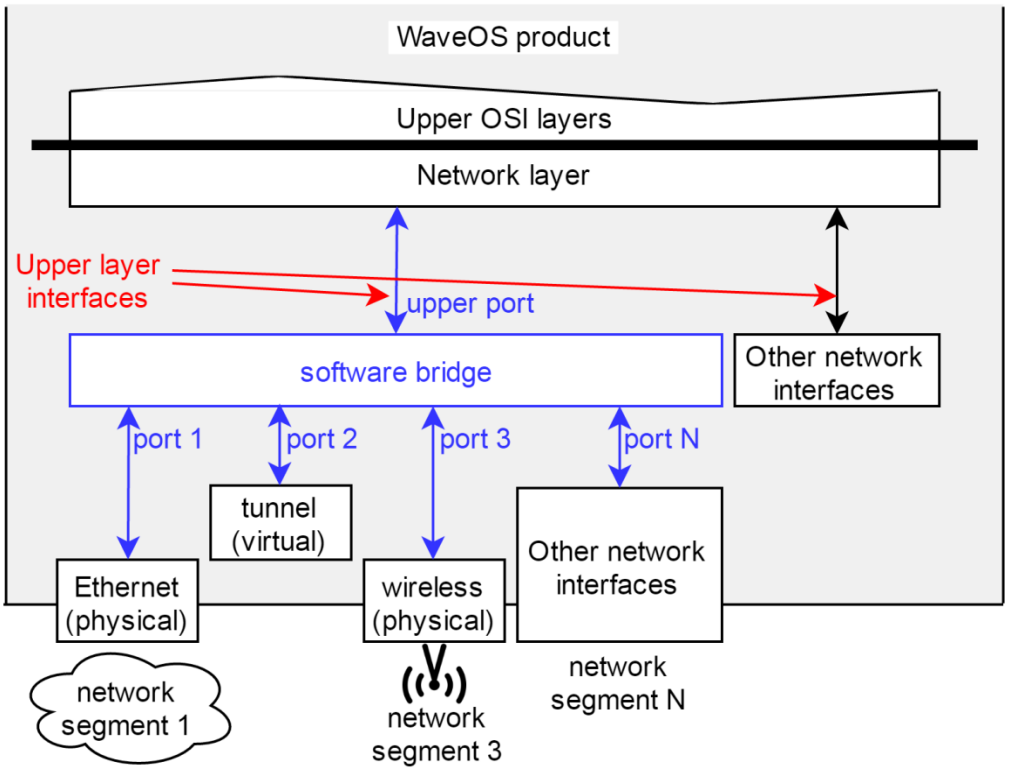
Picture V-4: An 8-ports switch

인터페이스를 함께 브리지 하려면 *VI.1.3.1 Network configuration* 과 Interfaces Settings 하위 메뉴를 참조하세요.



V.1.8.1 Bridge upper layer interface

라우터에 통합된 소프트웨어 브리지에는 네트워크 상위 계층 서비스가 데이터를 기본 네트워크 세그먼트로 라우팅하거나 브리지 자체를 구성할 수 있는 전용 포트가 하나 있습니다. 이 특별한 포트를 upper layer interface 라고 합니다.



Picture V-5: 소프트웨어 브리지의 상위 계층 인터페이스

V.1.8.2 Vlan bridging

WaveOS 에는 2 가지 유형의 브리지가 있습니다.

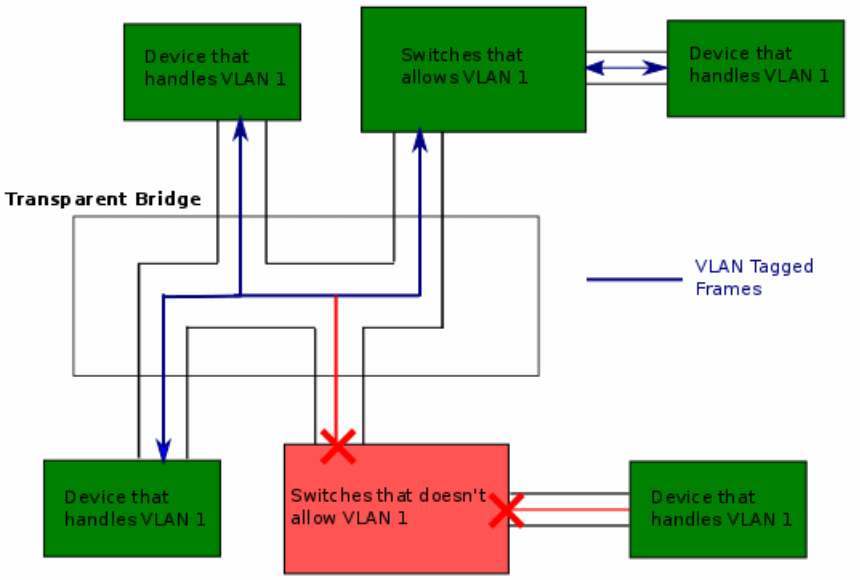
- Transparent Bridge: VLAN 을 처리하지 않는 브리지.
- Bridge-VLAN: VLAN 을 처리하는 브리지.

Transparent bridges 는 덜 강력하지만 설정하기 쉽습니다. 제한된 형태의 VLAN 필터링을 사용하도록 조정할 수 있습니다.

a. Transparent Bridge

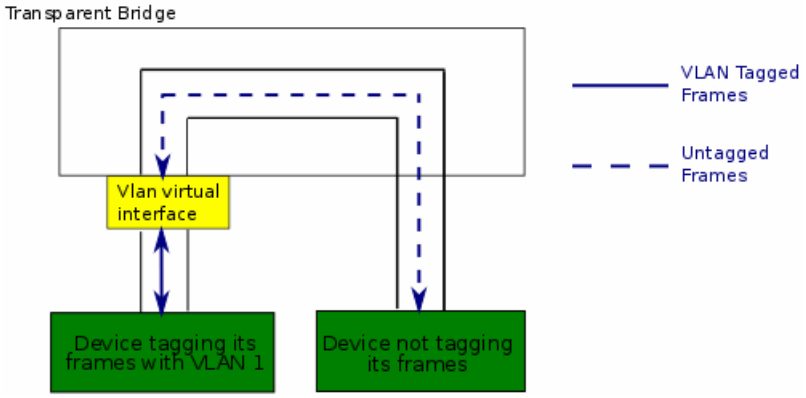
Transparent bridge 는 프레임에서 VLAN 또는 VLAN 태그를 고려하지 않습니다. 프레임은 대상 주소에 따라 모든 브리지 포트로 전달됩니다. 수신 프레임에 VLAN 태그가 포함되어 있으면 변경되지 않고 송신됩니다.

따라서 브리지 포트는 잠재적으로 태그가 지정된 프레임과 태그가 지정되지 않은 프레임을 모두 출력할 수 있습니다. 이 브리지에 연결된 관리 가능한 외부 스위치는 계획된 VLAN 태그 또는 태그가 지정되지 않은 프레임을 필터링하거나 통과 하도록 신중하게 설정해야 합니다. 다음 그림을 참조하세요.



Picture V-6: Transparent bridge forwards tagged frames unmodified

그러나 VLAN 인터페이스를 생성하고(위 참조) 브리지 포트에 연결할 수 있습니다. 이렇게 하면 태그 사용이 시행되고 한 VLAN 에서 다른 VLAN 으로 변환할 수 있습니다.



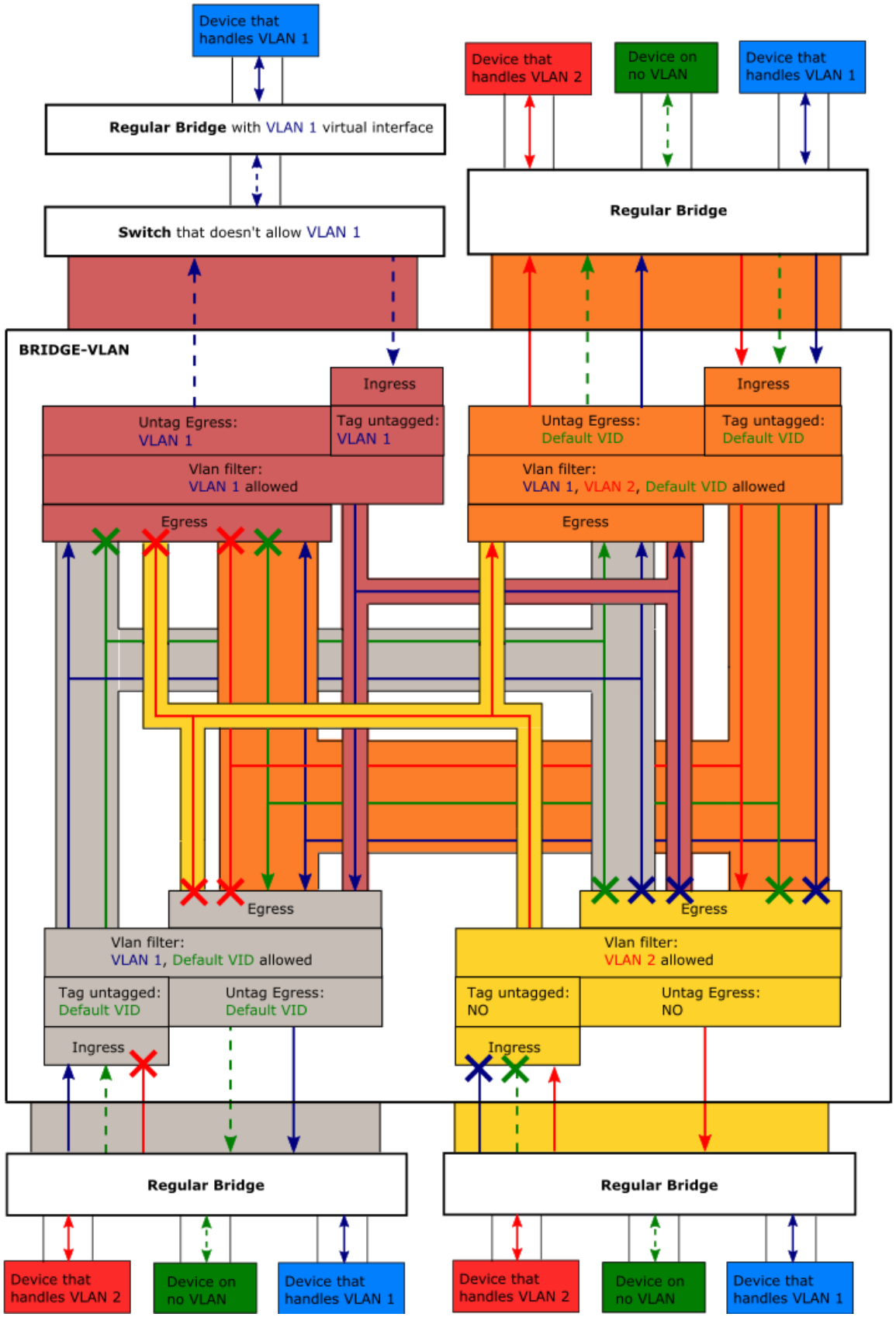
Picture V-7: VLAN tag conversion using a virtual interface

VLAN 인터페이스는 태그가 지정되지 않았거나 잘못 태그가 지정된 수신 프레임을 삭제합니다. 브리지로 전달하기 전에 적절하게 태그가 지정된 수신 프레임의 태그를 해제합니다. 다른 방향에서는 송신 트 래픽에 태그를 지정합니다.

b. Bridge-VLAN

Bridge-VLAN 에서 각 인터페이스에는 승인된 VLAN 목록이 있습니다. 이 목록에 없는 VLAN 은 이 인터페이스를 통해 전달할 수 없습니다.

태그가 지정되지 않은 수신 트래픽은 브리지에서 전달되지 않고 삭제됩니다. 대신 구성 가능한 기본 VLAN_ID 로 태그를 지정할 수 있으므로 브리지에서 전달할 수 있습니다. 송신 트래픽에 태그하거나 언태그 할 수 있습니다.



Bridge-VLAN 은 BRIDGING / VLAN MANAGEMENT 메뉴를 통해 설정가능합니다.

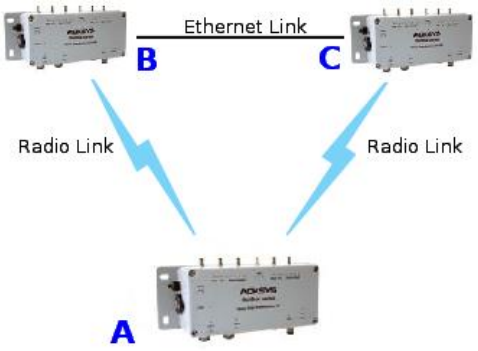
참조: Vlan Management

V.1.8.3 Spanning Tree Protocols (STP, RSTP)

a. Spanning Tree overview

Incentive

LAN 에서 다양한 스위치 장치와 MAC 브리지를 상호 연결하면 네트워크 루프가 발생할 수 있 습니다. 예를 들어(아래 그림 참조) 3 개의 브리지 A, B, C 가 있고, A 와 B 사이에 직접(이더넷 또는 Wi-Fi) 연결이 있고, B 와 C 사이에 다른 연결이 있고, C 와 A 사이에 다른 연결이 있다고 가정합니다. 그런 다음 A 에 연결된 장치가 브로드캐스트를 보내면 A 에서 B 와 C 로 다시 보내고, B 는 C 로 다시 보내고, C 는 A 로 다시 보냅니다. 브로드캐스트 프레임은 loop 가 형성되어 많은 대역폭이 소모되는 "브로드캐스트 스톰(broadcast storm)"을 초래합니다.



하지만 loop 는 링크가 끊겼을 때 백업경로를 만드는 데 유용할 수 있습니다.

참조: Point-to-point redundancy with dual band

Topology model and related terms

STP/RSTP 토폴로지는 브리지로 상호 연결된 물리적 네트워크 링크에 구축됩니다. 전체 구조는 Bridged LAN 이라고 합니다. 브리지의 예로는 이더넷 스위치, 관리 가능한 스위치 및 제품에 포함된 소프트웨어 브리지가 있습니다.

하나의 물리적 네트워크 링크는 여러 end stations 과 여러 브리지를 함께 연결될 수 있습니다.. 이러한 링크의 예는 legacy Coaxial Ethernet, Twisted Pair Ethernet hub 또는 무선 액세스 포인트입니다. 링크로 정확히 2 개의 브리지가 연결되어 있는 경우 STP/RSTP 관점에서 "point-to-point"라고 합니다. Point-to-point 는 두 개의 브리지 외에 종단 스테이션을 연결할 수 있습니다.

브리지와 물리적 네트워크 링크 사이의 인터페이스를 port 라 합니다. 브리지에는 여러 포트가 있으며 주요 기능은 한 포트에서 다른 포트로 프레임을 전달하는 것입니다.

브리지된 LAN 에서 이중화를 제공하는 방법에는 두 가지가 있습니다. 첫째, 브리지에는 포트 오류를 방지하기 위해 동일한 물리적 네트워크 링크에 연결된 여러 포트가 있을 수 있습니다. 둘째, 브리지 그룹은 브리지 장애를 방지하기 위해 루프(메쉬)를 형성할 수 있습니다.

Operation

STP 프로토콜이 상호 연결된 여러 브리지에서 활성화되면 한 지점에서 다른 지점으로 프레임을 전송하는 고유한 경로에 동의하기 위해 정보를 교환합니다.

브리지는 트리 구조를 설정하도록 조정되어 루프를 방지하고 이 트리는 링크가 끊어지면 자동으로 재정렬할 수 있습니다.

STP 는 LAN 루프에 참여하는 모든 브리지에서 활성화되어야 합니다. 대체 프로토콜 RSTP 는 경우에 따라 끊어진 링크에 더 빠르게 반응하여 끊어진 링크 복구를 가속화하는 STP 의 진화된 프로토콜 입니다.

브리지에 무선 인터페이스가 포함된 경우, STP/RSTP 의 적절한 기능을 수행하기 위해 몇 가지 주의를 기울여야 합니다.

- 무선인터페이스가 Access Point 인 경우: Access Point 에 연결된 클라이언트의 수는 1 로 제한되어야 합니다.
- 무선 인터페이스가 클라이언트인 경우: 브리징 모드는 "4 address format (WDS)"이어야 합니다(ARPNAT 은 non-IP STP 프레임을 처리할 수 없음). 이것은 로밍 기능이 Connect before break 모드로 설정된 경우에만 STP/RSTP 와 호환됩니다.

b. RSTP overview

RSTP 는 브리지된 LAN(무선 인터페이스를 위한 WDS 사용)에서 loop-free 토폴로지를 수행하는 표준 802.1d 에 정의된 네트워크 프로토콜입니다. 또한 네트워크 토폴로지에 대체 경로 및 백업 포트를 포함할 수 있습니다. RSTP 는 연결을 빠르게 복구하여 프레임 손실을 최소화합니다. BPDU 라고 하는 패킷은 브리지 간의 RSTP 협상 및 토폴로지 변경에 사용됩니다.

Protocol outlines

Root election

RSTP 는 네트워크 토폴로지를 Spanning Tree (an inverted tree)로 정의합니다. 먼저 Ethernet/Wireless 가 다른 스위치를 연결하는 부분에서 Root bridge 를 선택합니다. 루트 브리지가 선택된 후 네트워크의 서로 다른 브리지는 2 가지 유형의 링크를 갖습니다.

- **Upper links**: 루트 브리지로 연결되는 링크
- **Lower links**: 루트 브리지로 연결되지 않는 링크

그런 다음 각 브리지가 인접 라우터와 비교하여 하위 링크에 연결된 포트(Designated ports)와 상위 링크에 연결된 포트를 지정합니다. 이렇게 해서 하나의 포트가 Root port 로 선택됩니다.

Port roles

브리지의 여러 포트에 상위 링크가 있다면 루프를 방지하기 위해 RSTP 는 이러한 포트를 두 가지 중 하나로 지정합니다. 루트 포트와 동일한 장치를 공유하는 경우에는 백업으로, 다른 장치에 있는 경우에는 대체 포트로 지정합니다. 이 작업은 포트 성능 파라미터에 따라 수행됩니다.

루트 및 지정 포트만 패킷 전달이 허용되고 대체 및 백업 포트는 전달이 허용되지 않습니다. 루트 포트에 장애가 발생한 경우 RSTP 는 대체 또는 백업 포트를 루트 포트로 변경합니다.

따라서 RSTP 는 브리지에 대한 5 가지 포트 역할을 정의합니다.

- **Root**
- **Designated**
- **Alternate**
- **Backup**
- **Disabled (**no link).

Port states

RSTP 포트 역할 정의 중 루프를 방지하기 위해 포트는 트래픽을 전달하거나 MAC 주소를 취할 수 없습니다. 역할을 할당한 후 포트는 MAC 주소를 취할 수 있지만 아직 트래픽을 전달할 수는 없습니다. 결국 포트는 전달 상태로 전환됩니다.

RSTP 에서 포트는 3 가지 상태가 있습니다.

- **Discarding**: 트래픽을 전달할 수 없습니다.
- **Learning**: 트래픽을 전달할 수 없지만 MAC 주소를 취할 수 있습니다.
- **Forwarding**: 트래픽을 전달할 수 있고, MAC 주소를 취할 수 있습니다.

Topology change propagation

RSTP 에서 루트 또는 지정된 포트가 포워딩 상태로 이동하면 토폴로지 변경이 생성됩니다. 모든 브리지(루트 및 비루트 브리지)는 BPDU 를 통해 토폴로지 변경 정보를 생성하여 네트워크의 상위 및 하위 링크로 전달할 수 있으므로 RSTP 가 STP 보다 빠른 처리가 가능합니다.

Performance Improvements

Convergence speed

전달 상태로의 전환 속도를 높이고 기능적인 네트워크를 갖기 위해 RSTP 는 몇 가지 성능 매개변수를 정의합니다.

The Edge port type: 다른 브리지가 연결되지 않은 LAN 에 연결된 포트입니다. RSTP 는 에지 포 트를 전달 상태로 직접 전환합니다.

The Point-to-Point link type: 두 브리지를 직접 연결(허브와 같은 중간 장비없이). 이렇게 하면 지정된 포트가 전달 상태로 더 빨리 전환됩니다.

The forward delay: 루트와 지정된 포트를 전달 상태로 전환하는데 걸리는 시간입니다.

Failure recovery speed

일부 파라미터는 브리지 장애가 발생한 경우 연결이 복구되는 속도에 영향을 줍니다.

Hello period: 각 브리지는 지정된 포트에서 BPDU 를 "Hello time" (기본값 = 2s), RSTP 와 실제 루트를 주변 브리지에 알립니다. 하위 링크 브리지는 3 개의 연속 BPDU(기본적으로 3x2s = 6s)를 수신하지 않은 경우 상위 링크와 연결이 끊어진 것으로 간주합니다.

Hello 시간을 줄이면 브리지 장애 시 복구 속도가 빨라지지만 BPDU 에 더 많은 대역폭이 사용됩니다.

Best path enforcement

루트 브리지의 자동 선택은 트래픽 흐름에 대한 차선의 경로로 이어질 수 있습니다. 따라서 RTSP 가 알려진 최상의 경로를 사용하도록 우선 순위를 설정할 수 있습니다.

Bridge priority: 먼저 브리지 우선 순위를 비교하여 루트 브리지를 선택하고 두 번째로 MAC 주소를 브리지합니다. 사용자는 원하는 루트 브리지를 선택하도록 브리지 우선 순위 를 설정하여 알려진 최상의 경로를 적용할 수 있습니다.

Port path cost and Port priority: 브리지에 여러 개의 상위 링크가 있는 경우 이 매개변수를 통해 브리지의 루트 포트와 대체 포트 또는 백업 포트를 선택할 수 있습니다.

Backward compatibility with STP:

RSTP 는 STP BPDU 의 레거시 버전이 해당 포트에서 감지되면 인터페이스에서 레거시 STP 로 되돌아갑니다. 이로 인해 성능이 저하될 수 있습니다. 따라서 LAN 의 모든 브리지는 RSTP 를 사용해야 하지만 LAN 은 여전히 STP 를 사용하여 덜 빠르게 복구됩니다.

V.1.9 Tunneling

터널링은 데이터 프레임을 캡슐화하여 주소 공간이 호환되지 않거나 프로토콜이 호환되지 않는 네트워크를 통과할 수 있도록 하는 방법입니다.

Generic Routing Encapsulation (GRE) tunnels 은 unicast/multicast 트래픽을 캡슐화할 수 있는 터널입니다.

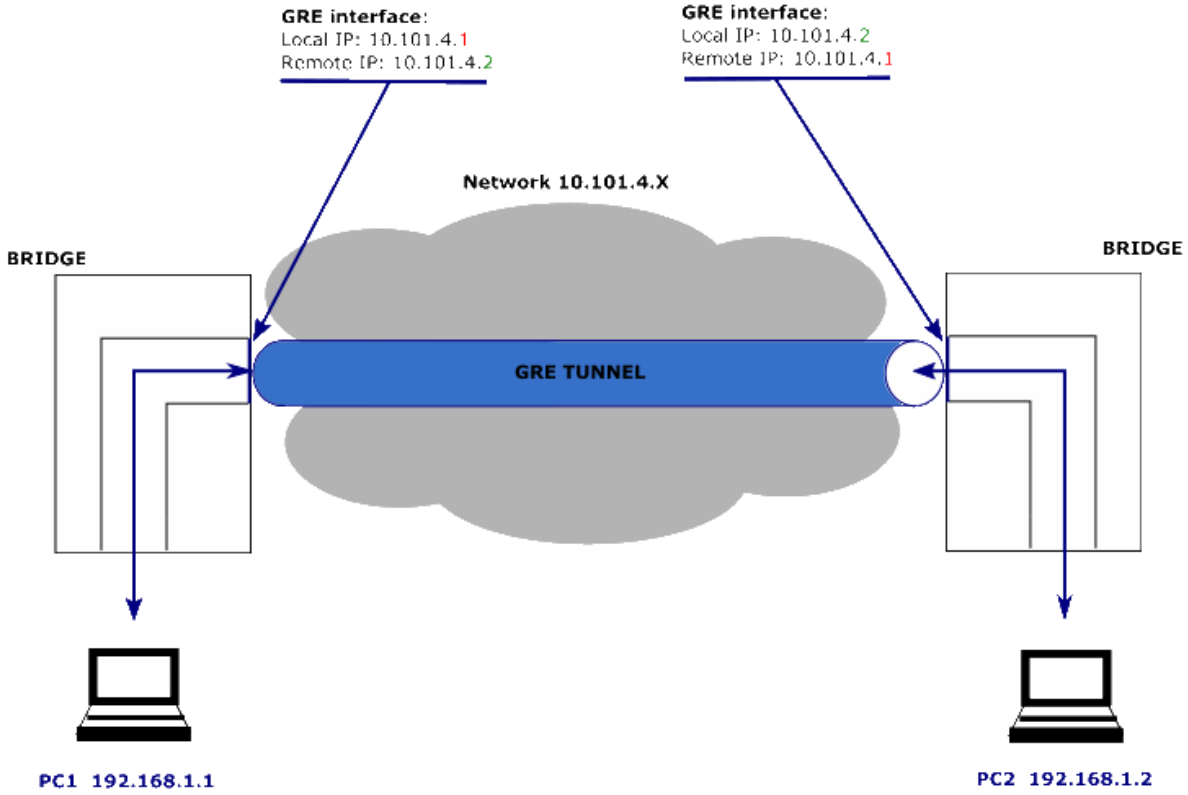
GRE 는 한 쌍의 끝점(네트워크 장치) 간에 양방향 터널을 만듭니다. 소스 지점은 패킷을 캡슐화하고 캡슐화를 해제할 대상 지점으로 리디렉션하므로 GRE 터널은 가상 지점 간 링크로 작동합니다. 소스 및 대상 지점은 GRE 터널의 양쪽에 있는 GRE 가상 인터페이스를 통해 구성됩니다. 각 GRE 인터페이스에는 터널 반대편의 IP 주소가 포함되어 있습니다.

캡슐화되어 특정 목적지로 전달되어야 하는 패킷(payload packets)는 GRE 패킷으로 캡슐화되고, GRE 패킷은 다른 프로토콜(delivery protocol)로 캡슐화 된 후 전달합니다.

페이로드 패킷의 프로토콜 유형은 ETHER TYPES 중 하나가 될 수 있습니다. (참조 RFC1700). WaveOS 는 delivery protocol 로써 IPV4 를 지원합니다.

GRE 터널은 임시적으로 형성되고, 대상 엔드포인트에 연결할 수 없는 경우 소스 엔드포인트를 종료할 수 없습니다.

WaveOS 는 물리적 인터페이스를 GRE 터널 인터페이스와 연결하여 GRE 를 통한 layer 2 터널링을 지원합니다.



Layer 2 tunneling over GRE 는 **VIRTUAL INTERFACES/L2 TUNNELS** 로 구성할 수 있습니다.

참고*: VI.1.2.4 L2 Tunnels*

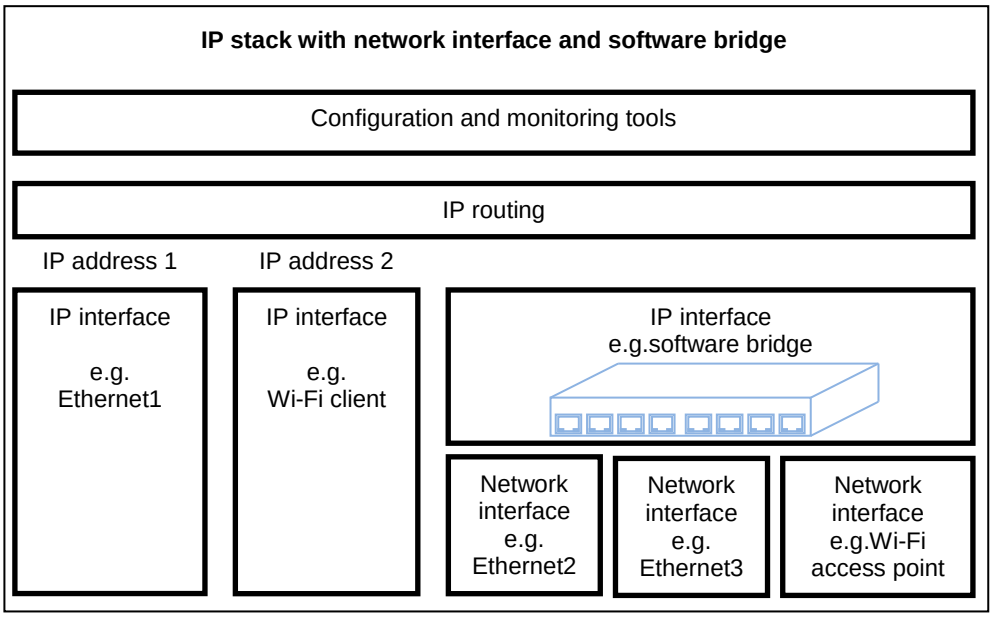
V.1.10 Unicast Routing in IP networks

라우팅은 패킷이 이동할 수 있는 한 위치에서 다른 위치로의 경로를 찾는 행위입니다. 동일한 로컬 네트워크에 있지 않은 호스트가 서로 통신할 수 있도록 합니다.

라우터는 자신을 목표로 하지 않는 패킷을 수신하고 그 주소를 기반으로 다음 중간 라우터 또는 최종 목적지로 패킷을 전달할 경로를 선택합니다. 경로 선택을 달성하기 위해 라우터는 자동으로 또는 사용자가 구축한 라우팅 테이블을 사용합니다.

라우팅은 OSI 모델의 layer 3 에서 수행됩니다.

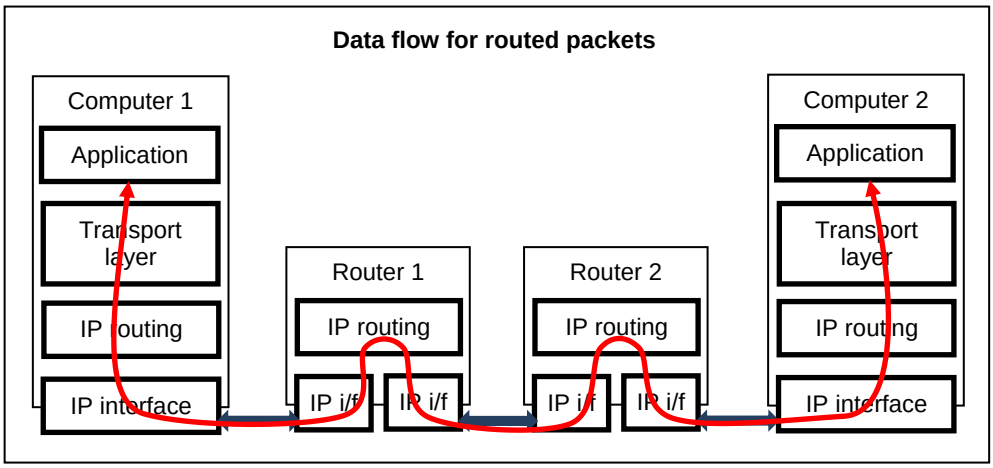
IP 는 컴퓨터 주소와 라우팅을 관리하는 TCP/IP 스택의 일부입니다. 한 컴퓨터 내에서 IP 프로토콜은 각 네트워크 인터페이스를 별도의 LAN 으로 봅니다. 각 LAN 에는 "192.168.1.2"와 같은 IP 주소가 있어야 IP 에서 사용할 수 있습니다. 따라서 네트워크 인터페이스는 하나의 네트워크 하드웨어 인터페이스를 구동하는 소프트웨어 일부입니다.



Picture V-8: Example of combined routing/bridging setup

라우터를 통해 함께 통신할 수 있는 모든 LAN 집합은 "internetwork"입니다. 인터넷 자체가 그러한 개념의 한 예입니다. 라우터 자체는 여러 네트워크 연결이 장착되어 있고 특별히 패킷을 라우팅 하는 데 사용되는 장치입니다.

다음은 2 개의 라우터를 통과하는 데이터 패킷이 뒤따르는 경로입니다. 각 라우팅 포인트에서 변경되는 MAC 주소와 달리 소스 및 대상 IP 주소는 전송 중에 변경되지 않습니다.



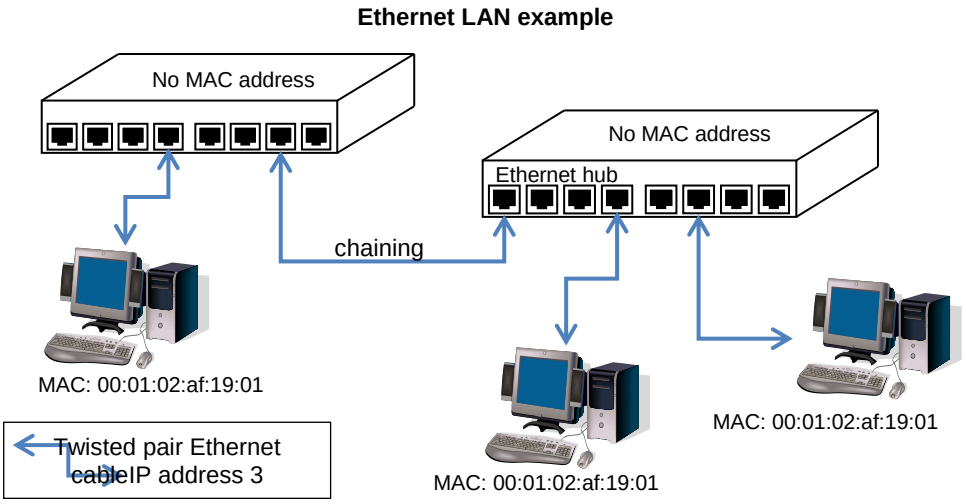
WaveOS 에서 라우팅은 여러 네트워크 인터페이스가 구성되었을 때 수행됩니다. ROUTING/ FIREWALL 서브메뉴에서 자세한 내용을 확인할 수 있습니다. 참조: *Routing / Firewall*

V.1.11 Addressing in the Data Link Layer (OSI layer 2)

V.1.11.1 Ethernet Address

이더넷 주소는 하드웨어 주소 또는 MAC 주소라고도 합니다. 처음 세 바이트는 하드웨어 제조업체를 식별합니다(예: ACKSYS 제품의 경우 Hex 00:09:90). 마지막 3 바이트는 각 제품에서 변경됩니다. 이 주소는 공장에서 할당되며 변경하면 안됩니다.

이더넷 LAN 은 허브, 스위치, 브리지로 구성될 수 있습니다. 이들은 변경 없이 데이터 패킷을 재전송합니다. 허브는 단순한 전기 증폭기로 생각할 수 있고, 스위치는 필터링 허브로 생각할 수 있습니다. IP 라우터와 혼동해서는 안됩니다.



V.1.11.2 Wi-Fi MAC Address

Wi-Fi 프로토콜은 이더넷 주소 형식을 사용하여 무선 카드를 식별하고 동일한 카드의 다양한 기능을 구별합니다. 이러한 주소는 무선 카드 제조업체에서 공장에서 할당하거나 동적으로 계산됩니다. 예: 동일한 무선 카드가 두 개의 액세스 포인트 기능(2 개의 무선랜)을 알릴 때.

Wi-Fi MAC 주소는 Wi-Fi 기술만 사용하여 함께 통신할 수 있는 스테이션을 구분하는 식별자인 BSSID 로도 사용할 수 있습니다. 예: TCP/IP 또는 이더넷이 아닌 액세스 포인트 사용.

V.1.12 Addressing in the IP layer (OSI layer 3)

V.1.12.1 IP addresses

이 섹션에서는 IPv4 addresses 에 중점을 둡니다.

IP 주소는 네트워크의 각 장치에 고유한 4 바이트(또는 32 비트) 숫자로 호스트가 통신하는 데 사용합니다. IP 주소는 일반적으로 점으로 구분된 4 바이트 각각의 10 진수 값으로 표시됩니다.

IP 주소는 네트워크와 호스트의 두 부분으로 나뉩니다. 이 분할의 주요 목적은 라우팅 프로세스를 용이하게 하는 것입니다. 네트워크 부분을 구성하는 비트 집합은 "네트워크

마스크"로 식별됩니다. 예를 들어, 마스크 255.255.255.0 은 주소의 상위 24 비트를 네트워크 주소로 선택하고 하위 8 비트를 호스트 주소로 선택합니다.

넷마스크를 지정하는 또 다른 방법은 그들 모두가 가장 중요하다고 가정할 때 '1'의 비트 수를 표시하는 것입니다. 예를 들어, **192.168.1.0/24** 에서 **/24** 부분의 의미는 **netmask 255.255.255.0** 입니다.

Example: Class C network address and netmask

1	1	0	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	0	0	0
193								168								1								200							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
255								255								255								0							

과거 사용에서는 **Class A** 네트워크를 1.x.x.x/8 ~ 127.x.x.x/8 네트워크, **Class B** 네트워크를 128.0.x.x/16 ~ 191.255.x.x/16 네트워크, **Class C** 네트워크를 192.0.0.x/24 ~ 223.255.255.x/24 네트워크라고 했습니다.

모든 비트가 1 로 설정된 호스트 부분은 브로드캐스트 주소이며, "모든 장치에 대한"을 의미합니다. 모든 비트가 0 으로 고정된 호스트 부분은 네트워크 전체를 다룬다(예: 라우팅 항목). 224.0.0.0 이상의 주소는 멀티캐스트 주소 지정에 사용됩니다.

V.1.12.2 IP addresses IPv6

WaveOs 4.18.0.1 IPv6 의 주요 신기능

- "Stateless Address Autoconfiguration"(SLAAC)을 통한 호스트 자동 구성
- SLAAC를 통해 장치는 DHCP 서버 없이 자체 IP 주소를 생성할 수 있습니다.
- 많은 주소 – 호스트 기반 NAT를 사용할 필요 없음

IPv4 와 마찬가지로 일부 IPv6 주소 풀은 특정 서비스 및 사용 사례를 위해 예약되어 있습니다. 아래 표는 IPv6 주소로 작업하고 할당하거나 IPv4 와 비교하여 각 IPv6 주소가 할당되거나 사용되는 방식을 이해하려고 할 때 유용합니다.

IPv6 주소 타입

Prefix	주소 타입	IPv4와 동등점	명칭 및 설명
2000::/3	**Global Unicast**	동등한 단일 블록 없음	이 표에 설명된 예외 외에 이러한 주소를 사용하는 네트워크 운영자는 레지스트리에 나열된 RIR의 Whois 서버를 사용하여 찾을 수 있습니다. 위치: https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml

IPv6 주소 타입

Prefix	주소 타입	IPv4와 동등점	명칭 및 설명
fe80::/10	**Link-Local Addresses**	169.254.0.0/16 (RFC3927)	이러한 주소는 단일 링크 또는 이더넷 LAN과 같은 라우팅되지 않은 일반 액세스 네트워크에서 사용됩니다. 해당 링크 외부에서 고유할 필요는 없습니다. 링크 로컬 주소는 IPv6 패킷의 소스 또는 대상으로 나타날 수 있습니다. 소스 또는 대상에 링크 로컬 주소가 포함된 경우 라우터는 IPv6 패킷을 전달하지 않아야 합니다. 링크 로컬 주소는 IPv6 패킷의 소스 또는 대상으로 나타날 수 있습니다. 소스 또는 대상에 링크-로컬 주소가 포함된 경우 라우터는 IPv6 패킷을 전달하지 않아야 합니다.
ff00::/8	**Multicast**	224.0.0.0/4	이 주소는 멀티캐스트 그룹을 식별하는 데 사용됩니다. 발신지 주소가 아닌 대상 주소로만 사용해야 합니다.
fc00::/7	**Unique Local Addresses (ULAs)**	Private, or RFC1918 address space: 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	이러한 주소는 가정 및 기업 환경에서 로컬 사용을 위해 예약되어 있으며 공용 주소 공간이 아닙니다. 이러한 주소는 고유하지 않을 수 있으며 정식 주소 등록이 없습니다. 소스 또는 대상 필드에 이러한 주소가 있는 패킷은 공용 인터넷에서 라우팅하기 위한 것이 아니라 기업 또는 조직 내에서 라우팅하기 위한 것입니다. 자세한 내용은 RFC4193을 참조하세요.

V.1.12.3 IPv6 Autoconfiguration

IPv6 노드는 SLAAC 를 사용한다.

- IP 주소
- 기본 게이트웨이
- (선택 사항) DNS 리졸버

SLAAC 는 링크 로컬 멀티캐스트 라우터 광고(RA)를 전송하는 라우터에서 작동합니다.

RA 메시지에는 다음을 포함할 수 있는 정보가 포함됩니다:

- 선호/유효 수명이 있는 On-link prefix(es)

- 링크 최대 전송 단위(MTU) ; 일반적으로 이더넷의 경우 1500
- DHCPv6의 가용성 표시; M = 상태 저장 DHCPv6 사용 가능, O = 상태 비저장 DHCPv6 사용 가능
- A-flag; A = 1 은 SLAAC로 주소 구성을 의미합니다. A = 0은 SLAAC로 주소를 구성하지 않음을 의미합니다.
- (선택 사항) DNS 리졸버

(선택사항) DNS 리졸버 정보(RFC 8106)

V.1.12.4 Public and private addresses

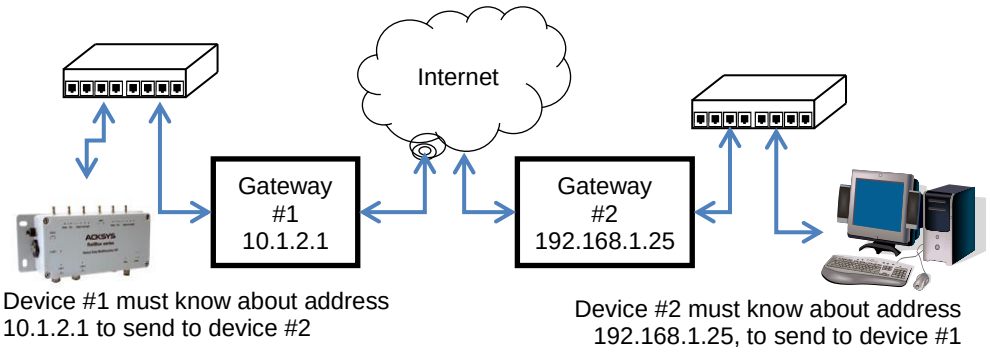
IP 주소는 개인 또는 공용일 수 있습니다. 공용 장치는 인터넷과 같은 공용 네트워크를 통해 데이터를 전송해야 하는 장치에 예약되어 있습니다. 일반적으로 로컬 ISP 에서 구입하거나 임대합니다.

이상적으로 세계의 각 장치는 항상 함께 통신할 수 있도록 자체 IP 주소를 가지고 있어야 합니다. 실제 환경에서는 대부분의 조직이 자체 IP 주소 공간을 독립적으로 관리하므로 한 조직에서 다른 조직으로 중복됩니다. 두 가지 규칙은 충돌을 방지하는 데 도움이 됩니다.

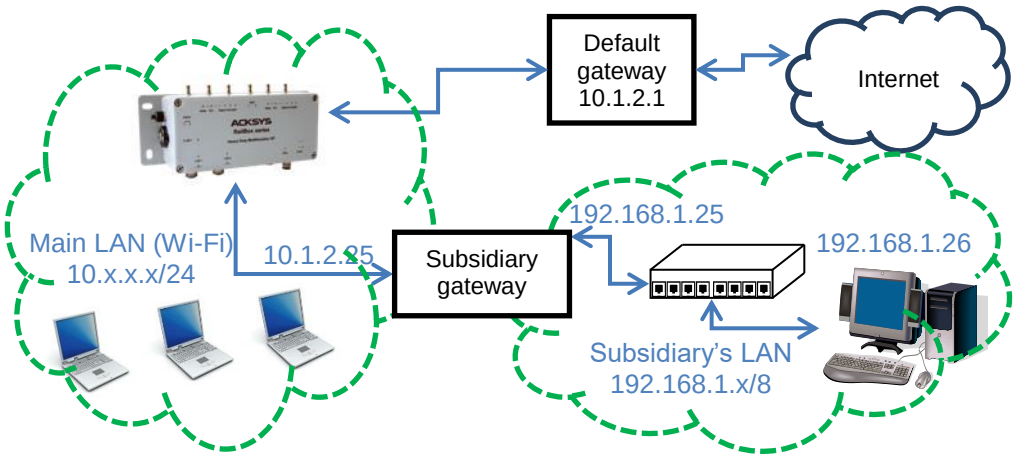
- 내부적으로 조직은 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 형태의 개인 주소를 사용합니다.
- 개인 영역과 인터넷 사이의 라우터는 내부 개인 주소를 자체 인터넷 공용 주소로 변환하여 전 세계가 조직의 모든 컴퓨팅 리소스를 보유하고 있는 컴퓨터는 한 대뿐이라고 취급합니다. 이 변환을 NAT(Network Addresses Translation, 네트워크 주소 변환)이라고 합니다.

V.1.12.5 Routers (a.k.a. gateways)

라우터를 통해 통신하는 각 네트워크 장치는 가장 가까운 게이트웨이의 IP 주소를 알고 있어야 합니다. 이 게이트웨이를 사용하여 데이터를 더 먼 LAN 으로 전달합니다. 장치가 게이트웨이를 모르는 경우 데이터를 수신할 수 있지만 응답을 반환하지 않을 수 있습니다. 예를 들어, PING 요청이 장치로 전달되더라도 PING 에 응답하는 것을 금지할 수 있습니다.



단일 LAN 에서 여러 대의 라우터를 사용하여 다양한 원격 LAN 에 액세스할 수 있는 경우, LAN 의 네트워크 장치는 각 라우터의 자체 주소와 라우터가 유도하는 원격 네트워크 주소에 대해 알아야 합니다. 일반적으로 라우터 중 하나는 "default"로 지정되고 다른 라우터는 이 기본 경로에 대한 예외로 처리됩니다.



네트워크 장치는 DHCP 프로토콜을 사용하여 IP 주소를 가져옵니다. DHCP 서버는 로컬 라우터의 주소를 동시에 제공할 수 있습니다. Acksys 제품을 DHCP 클라이언트로 설정하려면 섹션 VI.1.10.1 DHCP 서버를 참조하세요.

V.1.13 Multicast routing

멀티캐스트 트래픽은 단일 데이터 패킷을 여러 수신자에게 배포하는 데 사용됩니다. 예를 들어 비디오 방송(보내는 사람 하나, 받는 사람 다수) 또는 원격 회의(보내는 사람 다수, 받는 사람 다수)가 있습니다. 멀티캐스트 트래픽은 일반적으로 UDP 전송 프로토콜을 사용합니다.

멀티캐스트 라우팅은 최소 비용으로 선택된 수신자에게 데이터 흐름을 브로드캐스트하는 것을 목표로 합니다. 이 목표를 달성하려면 다음과 같이 하세요.

- 브리지는 로컬 수신기가 있거나 IP 라우터가 필요한 네트워크 세그먼트로만 멀티캐스트 프레임을 전송해야 합니다.
- IP 라우터는 로컬 수신기가 있거나 IP 라우터가 필요한 네트워크 인터페이스에만 멀티캐스트 패킷을 전송해야 합니다.
- IP 라우터는 데이터 전송자에서 모든 수신기로의 최적의 경로를 선택해야 합니다. 네트워크의 총 호스트 수에 비해 수신자의 수가 많은 것으로 알려져 있을 때, 멀티캐스트 트래픽은 네트워크 전체에 걸쳐 과도하게 넘쳐날 수 있습니다. 이러한 "dense mode"는 간단하지만 많은 네트워크 리소스가 필요하고 확장 가능하지 않습니다. 일반적으로 수신기의 수는 제한되어 있으며, 이를 "sparse mode"라고 합니다. 트래픽을 제한하려면 두 가지 기능이 필요합니다.
- 수신자는 수신하려는 의지를 알려야 합니다.
- 중간 라우터는 최적의 분배 트리를 구축해야 합니다. 예를 들어, 두 개의 수신기가 아닌 동일한 LAN 상의 라우터에 데이터의 복사본 하나만 전송되고, 하나의 라우터만이 하나의 주어진 LAN 에 멀티캐스트 흐름을 분배합니다.

V.1.13.1 Multicast addresses

멀티캐스트 주소는 일반적으로 네트워크 내의 특정 위치를 가리키지 않기 때문에 "group"이라고 합니다.

a. Ethernet Data link layer

이더넷 호환 네트워크(Wi-Fi 포함)에서 그룹 주소는 첫 번째 바이트의 최하위 비트가 1 로 설정됩니다(프레임에서 전송되는 첫 번째 비트입니다). 이러한 의미에서 브로드캐스트 주소는 멀티캐스트이기도 합니다.

b. Network layer

IPv4 는 멀티캐스트를 위해 이진 "1110"으로 시작하는 모든 32 비트 주소를 예약합니다. 여기에는 그룹 범위 224.0.0.0 ~ 239.255.255 가 포함됩니다.

224.0.0.0 ~ 224.0.0.255 범위의 그룹은 LAN 전달용으로 예약되어 있으며 LAN 외부로 라우팅할 수 없습니다.

c. Conversion between layers

이더넷 네트워크에서 IP 멀티캐스트가 전송되면 이더넷이 프레임을 멀티캐스트하기 위해 IP 그룹이 이더넷 멀티캐스트 주소로 변환됩니다.

IPv4 그룹은 그룹의 "01:00:5E:" + 23 하위 비트로 변환됩니다.

IPv6 그룹은 그룹의 "33:33:" + 32 하위 비트로 변환됩니다.

따라서 장치에서는 두 개의 서로 다른 그룹을 하나만 수신할 수 있습니다. 수신 네트워크 계층이 예기치 않은 그룹을 필터링해야 합니다.

V.1.13.2 PIM-SM

WaveOS 는 PIM-SM(Protocol Independent Multicast – Sparse Mode)을 구현하여 멀티캐스트 트래픽에 필요한 라우팅 테이블을 설정합니다. PIM 은 데이터 소스와 수신기 사이의 모든 중간 라우터에서 실행되어야 합니다. PIM-SM 의 주요기능 입니다.

- 지정된 멀티캐스트 흐름에 대한 중앙 배포 지점인 “rendezvous point (랑데부 지점)” (RP) 라우터를 관리합니다.
- 로컬 멀티캐스트 소스를 식별하고 관리합니다.
- 로컬 수신기를 식별합니다.
- 멀티캐스트 흐름에 대한 경로를 찾습니다.
- 멀티캐스트 라우팅 테이블을 관리합니다.
- 랑데부 지점 중복을 처리합니다.
- 라우터 중복을 처리합니다.

a. Routers redundancy

로컬 네트워크에서 여러 멀티캐스트 라우터가 사용 가능할 때, 그들은 자동으로 협상하고 이 네트워크에 대한 멀티캐스트를 처리할 "Designated Router"(DR)를 선택합니다. 정기적인 메시지를 통해 DR 실패를 감지하여 새 선택을 트리거할 수 있습니다.

b. Local sources management

멀티캐스트 소스는 멀티캐스트 배포를 트리거하는 프로토콜이 필요하지 않습니다. 그것은 단지 자신들의 데이터를 보냅니다. 스위치 및 브리지는 멀티캐스트 트래픽을 로컬 자체 보급 수신기와 로컬 라우터 모두에 전달합니다.

c. Local receivers management

처음에, 라우터는 로컬 수신기가 "IGMP join" 메시지를 브로드캐스트하여 자신을 광고할 때까지 로컬 네트워크에서 멀티캐스트 트래픽을 전달하지 않습니다. 이렇게 하면 외부 환경에서 로컬 네트워크로 요청된 멀티캐스트 흐름의 라우팅이 트리거됩니다.

가능한 수신기 오류와 IGMP 프레임 손실을 설명하기 위해 멀티캐스트 라우터는 주기적으로 "IGMP global query"를 전송하여 로컬 멀티캐스트 수신기에 대한 정보를 새로 고칩니다.

로컬 네트워크의 중간 스위치와 브리지는 "IGMP snooping"을 사용하여 로컬 멀티캐스트 트래픽을 최적화할 수 있습니다. 이를 위해 "IGMP global query"를 직접 발행할 수 있습니다. 이 메시지는 라우터의 메시지와 두 가지 점에서 다릅니다.

- 소스 IP 주소는 0.0.0.0 입니다.
- 이 주소를 기반으로 하여, 수신 브리지는 발신자를 멀티캐스트 라우터로 간주하지 않으므로 멀티캐스트 데이터를 그 주소로 포워드 하지 않습니다.

모든 로컬 수신기가 그룹에 대한 쿼리에 응답하지 않으면 라우터는 LAN 에서 이 그룹 포워딩을 중지합니다.

d. Rendezvous points functions

멀티캐스트 흐름에 대해 가능한 각 소스로 네트워크의 각 라우터를 구성하는 것을 피하기 위해, 각 멀티캐스트 그룹에는 이 그룹의 "rendezvous point"로 알려진 하나의 멀티캐스트 라우터가 할당됩니다.

멀티캐스트 소스의 데이터는 캡슐화되어 로컬 라우터(송신자의 DR)에 의해 유니캐스트의 rendezvous point 으로 전송됩니다.

수신기의 요청은 멀티캐스트 라우터에 의해 랑데부 지점으로 라우팅됩니다.

초기 통신 설정 후, 랑데부 지점은 경로를 최적화하여 멀티캐스트 트래픽이 소스에서 대상으로 직접 흐르도록 할 수 있습니다.

e. Rendezvous points selection

모든 멀티캐스트 라우터는 정적 구성에 의해 그룹의 랑데부 지점으로 지정될 수 있습니다. 그 후, 다른 라우터는 다음 중 하나를 통해 그 존재를 알게 됩니다.

- 다른 라우터의 정적 구성
- BSR (Bootstrap router)과의 동적 협상

중복성을 위해 여러 랑데부 지점이 동일한 그룹에 서비스를 제공할 수 있습니다. 우선 순위를 적용할 수 있으며, 우선 순위가 동일한 경우 알고리즘은 모든 라우터에서 동일한 랑데부 지점을 사용하도록 보장합니다.

f. BSR election

랑데부 지점이 동적으로 설정되면 부트스트랩 라우터(BSR)가 현재 활성 랑데부 지점의 테이블을 주기적으로 브로드캐스트하도록 지정됩니다.

정적 구성에 의해 모든 멀티캐스트 라우터를 네트워크의 BSR 로 지정할 수 있습니다. 중복성을 위해 여러 BSR 을 다양한 우선순위로 정의할 수 있습니다. 이 경우 마스터 BSR 이 자동으로 선택됩니다.

g. Multicast route selection

유니캐스트를 라우팅할 때 라우터는 패킷을 수신하고 대상 주소를 추출하고 대상에 따라 전달합니다. 반대로, 멀티캐스트를 라우팅할 때, 라우터는 소스 주소(랑데부 지점 중 하나)로 변환된 그룹에 대한 요청을 수신합니다. 라우터는 요청을 원본으로 향하는 역방향 경로로 전송해야 합니다. 이를 역방향 경로 전달(RPF)이라고 합니다. 요청

경로에 있는 라우터는 멀티캐스트 데이터가 반대 방향으로 이동하도록 전달 테이블을 설정합니다.

지정된 LAN 에는 여러 라우터가 존재할 수 있습니다. LAN 이 동일한 그룹에 대해 중복 패킷을 수신하지 않도록 DR(Designated Router)이 선택됩니다. 또한 PIM 은 라우터 간의 중복 경로를 확인하고 정리합니다.

V.1.13.3 Multicast pitfalls and solutions

많은 세부 정보가 있어 멀티캐스트 트래픽을 전달할 때 보기 좋은 구성이 실패할 수 있습니다. 여기서는 가장 일반적인 문제를 설명하고 해결 방법을 제시합니다.

a. Router misconfiguration

멀티캐스트 라우터는 RPF 및 SSM 경로를 계산하고 다른 라우터에 가입하기 위해 로컬 유니캐스트 라우팅 테이블을 최대한 활용합니다. 따라서 유니캐스트 작동을 위해 IP 테이블과 경로를 올바르게 설정해야 합니다.

Solution: 전제 조건으로 각 라우터가 유니캐스트 작동을 위해 올바르게 구성되었는지 확인합니다.

b. Sender misconfiguration

송신자가 유니캐스트 작동을 위해 올바르게 구성되어야 합니다. 첫째,

송신자의 소스 IP 가 잘못된 경우, 로컬 DR 이 멀티캐스트 트래픽을 수락하지 않습니다.

그러나 인증되지 않은 UDP 트래픽이므로 송신자는 멀티캐스트 트래픽을 내보냅니다. 둘째,

송신자는 멀티캐스트 전달 경로를 알고 있어야 합니다.

일반적으로 송신자의 네트워크 구성에는 기본 경로가 포함되며 멀티캐스트는 기본 경로가 있는 네트워크 인터페이스를 통해 출력됩니다.

Solution: 송신자 IP 주소를 DR 과 동일한 서브넷에 설정하고, 그룹 주소를 로컬 네트워크 인터페이스와 연결하거나, 기본 유니캐스트 라우터가 아닌 동일한 LAN 에 DR 을 갖도록 주의를 기울입니다.

c. Small TTL

멀티캐스트 트래픽에는 실수 가능성을 제한하기 위해 네트워크를 플러딩하는 기능이 있습니다.

대부분의 표준 멀티캐스트 전송자는 기본 TTL 1 을 사용

이는 특히 Videolan VLC, IPERF 및 JPERF 와 같이 네트워크 튜닝 및 테스트에 일반적으로 사용되는 소프트웨어의 경우입니다.

IP 프로토콜에 따라 TTL 매개 변수는 패킷이 통과할 수 있는 로컬 네트워크의 수를 제한합니다. 따라서 TTL= "1"은 "로컬 전송만"을 의미합니다.

Solution: 더 큰 TTL 을 사용하도록 전송 소프트웨어를 구성합니다.

최소값은 RP 를 통과하거나 직접 통과하는 소스와 가장 먼 대상 사이의 최단 경로를 고려해야 합니다.

잘못된 값을 설정하면 배포 경로를 따라 특정 라우터에 의해 패킷이 자동으로 손실됩니다.

d. MTU and DON'T_FRAGMENT option

이것은 멀티캐스트에만 국한되지 않지만 UDP 가 일반적으로 사용되기 때문에 두드러집니다. 패킷이 배포 경로에 있는 하위 네트워크의 MTU 보다 크면 관련 라우터가 패킷을 단편화해야 합니다. 하지만,

대부분의 전송자는 기본적으로 IP Don't Fragment 플래그 사용

이것은 특히 Linux 커널의 경우이며, 결과적으로 Linux 에서 실행되는 모든 애플리케이션 소프트웨어가 이 IP 옵션을 재설정할 수 있는 수단을 제공하지 않는 경우입니다.

큰 패킷 크기를 사용하면 일반적으로 배포 경로를 따라 특정 라우터에 의해 패킷이 자동으로 손실됩니다. RP 에 대한 트래픽을 캡슐화하여 MTU 를 줄여야 하기 때문에 종종 전송자의 DR 이 됩니다.

Solution: 단편화가 필요하지 않은 최대 프레임 크기를 사용하도록 응용프로그램을 구성하거나, 단편화를 하지 않는 플래그를 지우도록 전송자를 구성합니다.

e. Wireless slow multicast traffic

802.11 인프라 모드는 본질적으로 비대칭적입니다. 액세스 포인트는 스테이션에 데이터를 전송할 때 이 스테이션에 적합한 데이터 속도를 사용합니다.
멀티캐스트에서와 같이 많은 스테이션으로 전송할 때, 802.11 은 다음과 같이 기술합니다.

AP 는 가능한 가장 낮은 속도를 사용하여 멀티캐스트를 전송

무선 대역에 따라 1 Mbps 또는 6 Mbps 입니다.

스테이션이 멀티캐스트 프레임을 AP 로 전송할 때, 최상의 전송 속도를 사용하지만 프레임을 다른 스테이션에서 사용할 수 있도록 하기 위해 AP 는 즉시 가장 낮은 전송 속도로 프레임을 다시 브로드캐스트합니다.

이렇게 하면

- 무선으로 멀티캐스트 트래픽이 매우 느림
- 다른 트래픽에 대한 대역폭 낭비가 큼

Solution: 터널에 캡슐화된 상태에서 멀티캐스트 트래픽이 무선 링크를 통과하도록 합니다. 예를 들어 이 용도로 구성된 GRE 터널일 수도 있고, 송신자의 DR 과 RP 사이의 캡슐화를 활용할 수도 있습니다(이 경우 RP 가 터널을 우회하는 최단 경로로 전환되는 것을 금지해야 함).

f. Wireless transmitting traffic permanently

라디오 채널은 희박한 자원입니다. 다른 한편으로는,

멀티캐스트 송신자는 조건 없이 DR 로 송신

그리고 이 DR 은 무작정 RP 로 전송합니다(수신자가 없을 때 RP 가 일시 중단을 요청하는 것은 제외).

Solution: 송신자와 DR 사이의 경로가 무선 LAN 을 통과해서는 안 됩니다. 송신자와 RP 사이의 경로는 무선 LAN 을 통과해서는 안 되지만, 이 요구 사항은 덜 엄격합니다.

이전의 위험한 항목을 참조하는 경우, 최적의 시스템은 송신자와 RP 를 무선 LAN 의 동일한 쪽에 두고 GRE 터널을 사용하여 멀티캐스트 데이터를 다른 쪽으로 전송합니다.

g. Wireless transmitting unwanted multicast traffic

이더넷 세그먼트에 연결된 액세스 포인트는 개념적으로 이더넷을 관련 스테이션으로 확장합니다.

이더넷에서 AP 에 도달하는 원치 않는 멀티캐스트는 매우 느린 속도로 스테이션에 전송되어 대역폭을 낭비

WaveOS 에서 AP 가 다른 인터페이스와 함께 브리지에 추가될 경우 이러한 현상이 발생할 수 있습니다.

Solution: 일부 멀티캐스트 그룹에 관심이 있는 무선 스테이션이 없는 경우 브리지 필터를 설정하여 나가는 멀티캐스트 트래픽을 금지할 수 있습니다. 참조 : *Bridge filter*

h. Access points and multicast routers

멀티캐스트 라우터가 시작되면 사용 가능한 네트워크 인터페이스를 열거합니다.

멀티캐스트 라우터 중 하나가 액세스 포인트인 경우, 이 AP 가 채널을 검색하도록 구성되었거나(ACS 기능) 선택한 채널이 DFS 지연(CAC 또는 NOP)의 영향을 받기 때문에 아직 시작되지 않은 것일 수 있습니다. 이 경우 멀티캐스트 라우터는 다양한 협상을 수립할 수 없으며, 이 네트워크 인터페이스는 영원히 무시됩니다.

액세스 포인트는 ACS 및 DFS 에 의해 지연

Solution: AP 를 단독으로 자체 브리지에 배치합니다. 멀티캐스트 라우터는 AP 상태에 관계없이 브리지 자체가 사용 가능한 것으로 간주합니다.

i. Long delays at startup

실행 중인 멀티캐스트 라우터는 다양한 이벤트에 적시에 반응합니다. 그러나 사용자는 WaveOS 가 시작되면 예상외로 오랜 지연을 겪게 됩니다.

이러한 정상 동작은 다음과 같은 경우에 발생합니다.

- 여러 프로토콜 (IGMP, DR 선택, BSR 선택, RP 선택, RPF 설정),
- 동시에 시작,
- 각각에 의존,
- 재시도 타이머

PIM(5 초)에 사용된 타이머의 분해능은 이 효과를 복합시킵니다.

Solution: 여기서는 광범위한 징후만 제공할 수 있습니다. 그러나 문제는 시작 시에만 발생한다는 것을 참고해주시기 바랍니다.

한편으로는 다양한 타이머(IGMP 쿼리어, HELLO 및 RD-Candidate 메시지), 네트워크에 가해지는 추가 부하 및 외부 멀티캐스트 라우터와의 호환성, 그리고 다른 한편으로는 정적 RP 목록 구성과 추가 관리 부담 사이에서 균형을 유지해야 합니다.

j. Associating VRRP and PIM

VRRP 라우터를 멀티캐스트 라우터로 사용할 때 VRRP 는 마스터 또는 백업인 VRRP 상태에 따라 PIM 라우터를 재개하거나 일시 중단합니다. 이 동작은 VRRP 와 동일한

인터페이스에서 PIM 을 사용하지 않는 경우 *VRRP configuration page* 에서 VRRP 를 멀티캐스트 라우팅에 연결하여 구성할 수 있습니다.

복잡한 구성을 다룰 때는 몇 가지 사항을 염두에 두어야 합니다.

1) 멀티캐스트 라우터는 모두 또는 없음입니다. 구성된 모든 인터페이스를 실행하고 관리하거나, 중지하고 관리하지 않습니다. 네트워크 인터페이스의 일부가 VRRP 와 관련이 없는 경우 VRRP 가 백업 상태로 전환될 때 이러한 인터페이스는 관리되지 않습니다.
2) VRRP 백업이 마스터 상태로 전환되면 PIM 이 다시 시작됩니다. 이는 테이크오버 지연이 시작과 동일하다는 것을 의미하며, 이는 유니캐스트 트래픽보다 멀티캐스트 트래픽이 훨씬 더 길다는 것을 의미합니다.

V.1.14 Firewall

Network 인터페이스는 공통 관리 정책을 할당하기 위해 개념적으로 "zones"으로 그룹화될 수 있습니다. *Firewall*

방화벽은 각 패킷에 적용되는 규칙을 설정하여 패킷을 전달할지 차단할지 결정할 수 있습니다.

WaveOS 에서는 하위 메뉴인 ROUTING/FIREWALL/NETWORK ZONES 에서 방화벽 기능을 조정할 수 있습니다.

참조: *Firewall*

V.1.15 Zones and Network Address Translation (NAT)

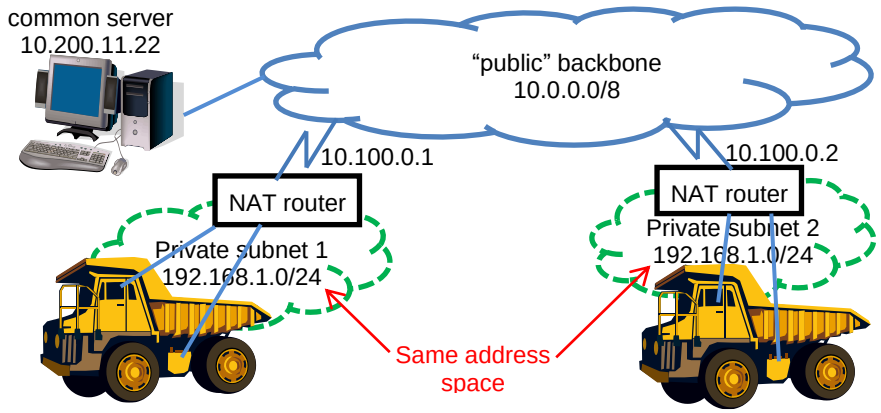
라우터에서 네트워크 인터페이스 간의 트래픽을 선택적으로 차단하거나 허용해야 할 수 있습니다. 영역은 일반적인 추가 처리를 지정하기 위해 여러 IP 인터페이스를 그룹화하는 관리 개념입니다.

- Firewall 규칙
- IP 주소 변환 규칙 (NAT 구현)

V.1.15.1 NAT/PAT (Network/Port Addresses Translation) routers

글로벌 네트워크가 독립 관리자가 운영하고 함께 연결된 여러 네트워크로 구성된 경우 하위 네트워크 내에 동일한 IP 주소가 할당될 수 있습니다. 이것은 일반적으로 여러 회사의 개인 네트워크를 연결하는 중추 역할을 하는 인터넷에서 볼 수 있습니다. 이는 동일한 하위 네트워크를 많이 설정하고 루트 백본에 연결해야 할 경우에도 사용할 수 있습니다.

이러한 종류의 설정에서 각 하위 네트워크에는 하위 네트워크로 들어오고 나가는 게이트웨이인 라우터가 있습니다. 라우터는 백본에 의해 상호 연결됩니다. IP 주소가 중복되는 것을 방지하기 위해 라우터는 하위 네트워크 IP 주소를 백본 IP 주소로 변환하여 "NAT"라는 이름을 사용합니다.



NAT/PAT 라우터의 경우 네트워크는 두 개의 "zones"으로 분할됩니다. 즉, 백본에 의해 구현되는 퍼블릭 영역과 중앙 관리에서 "public" IP 주소를 제공하는 퍼블릭 영역, 그리고 관리자가 외부의 IP 주소를 인식하지 않고도 IP 주소를 할당할 수 있는 프라이빗 영역으로 분할됩니다.

그런 다음 NAT/PAT 라우터는 모든 발신(프라이빗에서 퍼블릭으로) IP 데이터그램을 변경하여 소스 프라이빗 IP 주소를 고유한 퍼블릭 IP 주소로 위장합니다. 또한 라우터의 공용 주소인 대상 주소를 개인 네트워크에 있는 일부 장치의 전용 IP 주소로 대체하여 수신(공용에서 전용으로) IP 데이터그램을 변경합니다. 퍼블릭 측면에서 볼 때 넓은 주소 공간을 계속 제공하기 위해 NAT/PAT 라우터는 포트 번호를 IP 주소의 확장자로 사용합니다. 따라서 NAT/PAT 은 주로 UDP 및 TCP 와 함께 작동하며 일반 ICMP 라우팅을 처리할 수 없으며 최대 하나의 개인 장치로만 작동합니다.

NAT/PAT 라우터는 들어오는 연결 호출과 나가는 연결 호출을 관리해야 합니다. 두 가지 주요 변환 테이블을 사용합니다.

- 수신 호출에서 선택한 대상 포트에 개인 대상 IP 를 할당하는 구성 가능한 테이블입니다.

- 나가는 데이터그램에 대해 어떤 포트(전용 IP, 전용 포트)가 할당되었는지 추적하는 내부 변환 테이블입니다.

이와 관련된 다양한 처리로 인해 NAT/PAT 라우터의 성능은 일반 라우터의 성능보다 낮으며, 이는 단순한 소프트웨어 브리지의 성능보다 낮습니다.

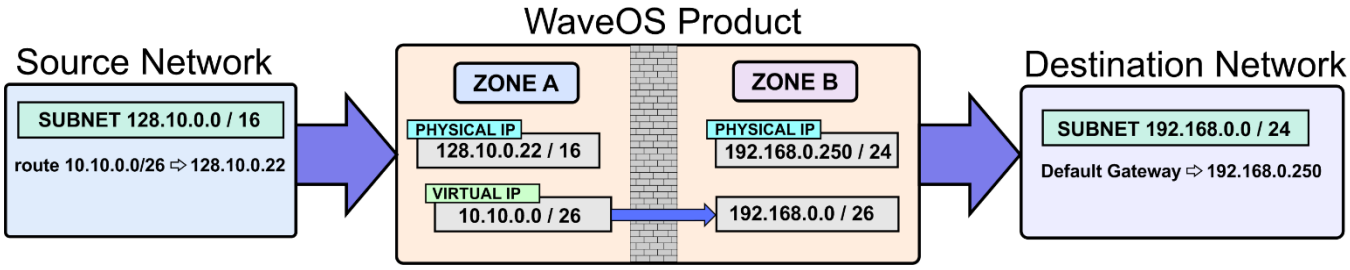
V.1.15.2 NAT 1:1

1:1 NAT 의 경우, 변환은 여전히 서로 다른 영역 간의 라우팅을 통해 수행되지만 더 이상 프라이빗 및 퍼블릭 영역에 대한 개념이 없습니다. 지정된 영역(소스 영역)과 연결된 가상 서브넷을 생성하고 이러한 가상 서브넷에서 다른 영역(대상 영역)의 실제 서브넷으로 변환을 수행하는 것입니다. 따라서 고유한 IP 주소 또는 전체 서브넷을 변환할 수 있습니다.

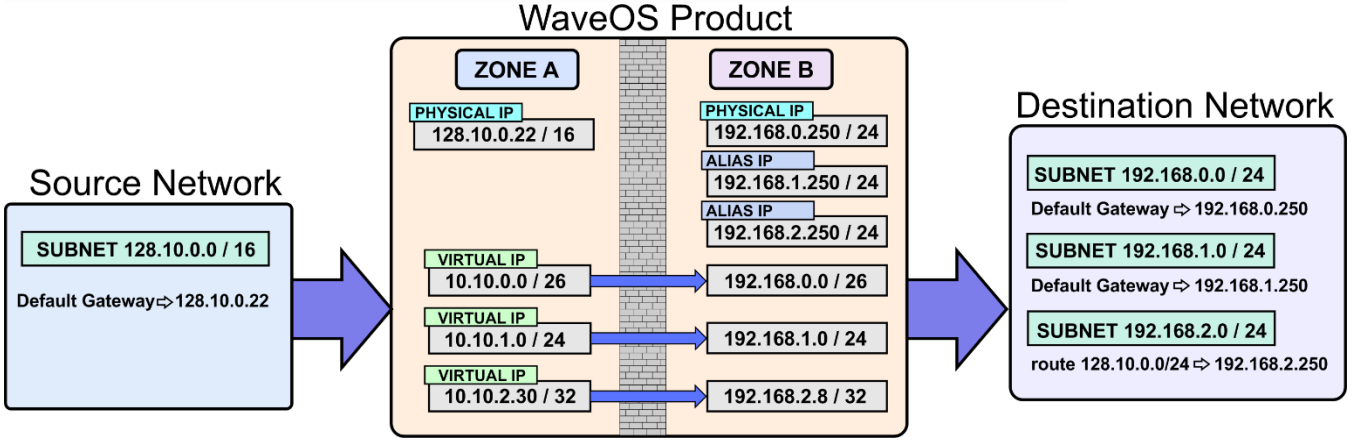
다음 예제에서는 서브넷 128.10.0.0/16 에 소스 네트워크가 있고 서브넷 192.168.0.0/24 에 대상 네트워크가 있습니다.

소스 네트워크에서 대상 네트워크의 서브넷 192.168.0.0 의 하위 주소 64 개(192.168.0.0 ~ 192.168.0.63)에 액세스하려고 합니다.

이를 위해, 우리는 정적 경로를 통해 소스 네트워크에서 정의될 영역 A(소스 영역)에 가상 서브넷을 만듭니다. 그러면 WaveOS 제품에서 이 가상 서브넷을 대상 네트워크의 물리적 주소로 변환하는 규칙을 정의할 수 있습니다. 서브넷의 처음 64 개 주소로 변환을 제한하려면 가상 IP 의 서브넷 마스크가 255.255.255.192(또는 /26 CIDR 표기)여야 합니다.



이제 전체 192.168.1.0 서브넷에 대한 액세스를 추가하고 고유한 192.168.2.0 서브넷 주소에 연결하려면 가상 주소를 추가하고 적절한 변환 규칙을 정의하기만 하면 됩니다. 그러나 정적 경로 또는 기본 게이트웨이를 통해 반환 경로를 정의할 수 있으려면 대상 인터페이스에서 각 서브넷에 대한 제품의 IP 주소 별칭을 만들어야 합니다.



V.1.15.3 NAT 66

NAT66 기능은 IPv6 메시지의 IPv6 주소 접두사를 다른 IPv6 주소 접두사(셀룰러 사용 사례)로 변환하는 데 사용되는 IPv6 네트워크 기반 주소 변환 기술인 WaveOs 에서 사용할 수 있습니다.

가장 간단한 형태로 NAT66 장치는 두 개의 네트워크 링크에 연결되며, 그 중 하나는 단일 관리 도메인 내의 리프 네트워크에 연결된 "내부" 네트워크 링크이고 다른 하나는 연결이 있는 "외부" 네트워크입니다. 글로벌 인터넷으로. 내부 네트워크의 모든 호스트는 로컬로 라우팅된 단일 접두사의 주소를 사용하며 IP 패킷이 NAT66 장치를 통과할 때 해당 주소는 전역 라우팅 가능한 접두사의 주소로/에서 주소로 변환됩니다.

V.2 Wireless concepts in 802.11

V.2.1 Wireless architectures

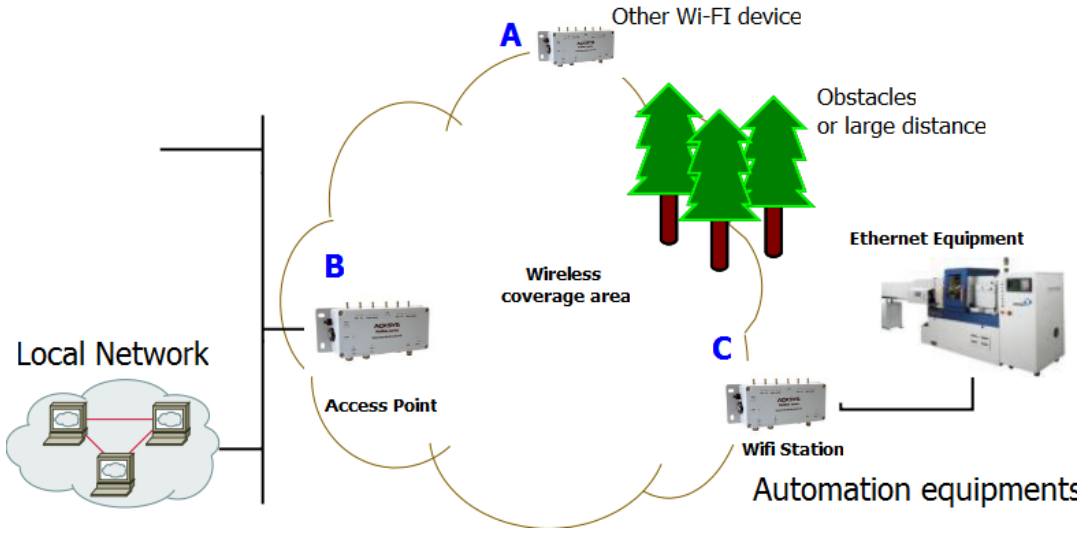
무선 LAN(WLAN)은 Wi-Fi 지원 스테이션의 그룹입니다. 이들은 주어진 아키텍처에 지정된 규칙을 따라 서로 통신합니다.
그룹의 스테이션에는 WLAN 을 식별하는 무선 네트워크 이름이 공통적으로 있습니다. IEEE 802.11 규범은 Wi-Fi 스테이션 간에 통신하기 위한 세 가지 아키텍처를 정의합니다.

- Infrastructure (AP 가 모든 트래픽을 릴레이하는 클라이언트/서버)
- Ad-hoc (피어 투 피어 멀티포인트 통신, 릴레이 없음)
- Mesh network (모든 스테이션이 트래픽 릴레이에 관여)

V.2.1.1 Infrastructure Mode

인프라 네트워크에는 두 가지 종류의 장치(스테이션이라고 함)가 있습니다.

- Access Points
- 다른 Wi-Fi 장치 또는 LAN 장치에 액세스하기 위해 액세스 지점에 연결하는 Client Wi-Fi 장치(클라이언트 스테이션)



제품 **A**, **B**, **C** 는 각각 서로 통신 가능
제품 **B** 는 **A** 와 **C** 간에 데이터를 중계
제품 **B** 는 LAN 과 제품 **A** 와 **C** 사이에서 데이터를 중계

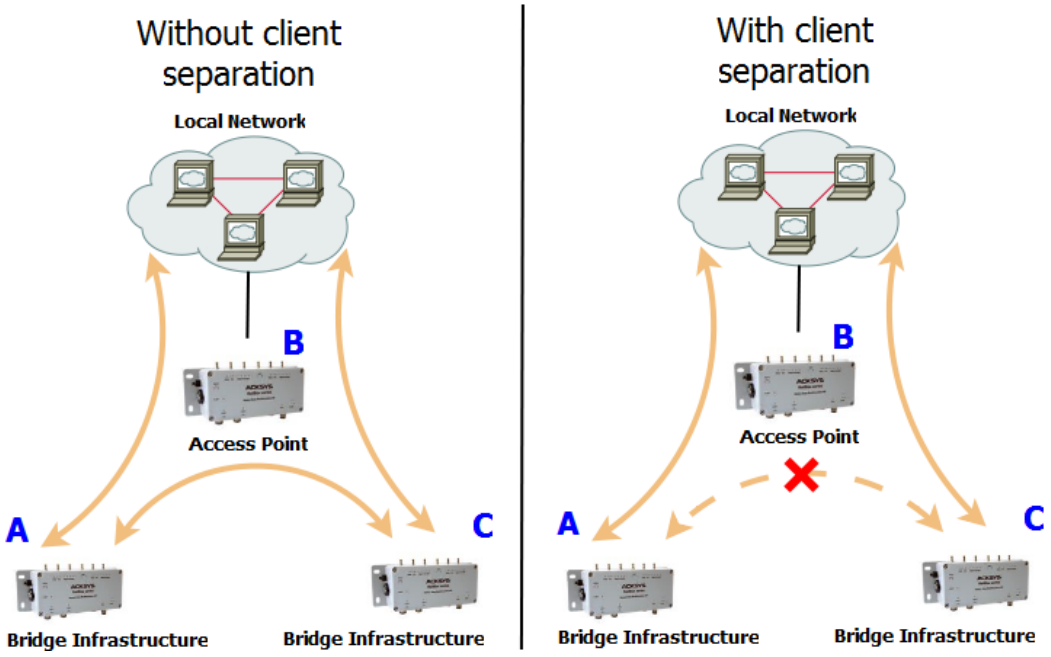
인프라 모드는 WLAN 클라이언트에 중앙 연결 지점을 제공하며 AP 는 이를 유선 네트워크에 연결할 수도 있습니다. 통신하기 전에 클라이언트는 하나의 액세스 지점을 선택하고 암호화 키를 인증하고 설정함으로써 WLAN(무선 LAN)에 참여해야 합니다.

AP 및 관련 클라이언트는 AP 에 의해 자동으로 구축된 MAC 주소의 형태로 BSSID 로 식별되는 BSS(기본 서비스 세트)를 형성합니다. 더 많은 AP 를 WLAN 에 추가하여 인프라의 도달 범위를 늘리고 임의의 수의 무선 클라이언트를 지원할 수 있습니다. 전체 WLAN 은 1~32 bytes 문자열로 구성된 일반적으로 사람이 읽을 수 있는 텍스트 SSID 로 식별됩니다. 동일한 WLAN 에 있는 모든 무선 스테이션과 AP 는 동일한 SSID 를 사용하도록 구성해야 합니다.

WLAN 의 AP 는 무선 클라이언트가 예를 들어 인터넷 연결이나 프린터에 액세스할 수 있도록 공통 유선 LAN 에 케이블로 연결됩니다.

Ad-hoc 무선 네트워크에 비해 infrastructure mode 네트워크는 확장성, 중앙 집중식 보안 관리 및 향상된 도달 범위라는 이점을 제공합니다.

1.4.2 버전 이후 펌웨어는 AP 가 클라이언트 간의 통신을 차단할 수 있는 "clients isolation" 기능을 구현합니다. 이 경우 제품 A 는 제품 B 및 "local network"와 통신할 수 있지만 제품 C 와는 통신할 수 없습니다(아래 그림 참조). C 제품은 또한 B 제품과 "로컬 네트워크"와 통신할 수 있지만 A 제품과는 통신할 수 없습니다. 이 그림에서는 분리 클라이언트 옵션이 있는 액세스 지점과 없는 액세스 지점 동작을 보여 줍니다.



Infrastructure 모드 개념에서 클라이언트는 단일 유닛이어야 합니다. 그러나 무선 클라이언트는 여러 이더넷 장치를 AP 쪽으로 BSS 로 브리지할 수 있으며, MAC 주소를 즉시 변환하여 여전히 하나의 장치로 나타납니다. (참조: *V.2.6 Wired to wireless bridging in infrastructure mode*).

V.2.1.2 Ad-hoc Mode

무선 컴퓨터 네트워크에서 ad-hoc 모드는 무선 장치가 서로 직접 통신하는 방법입니다. ad-hoc 모드에서 작동하면 중앙 액세스 지점(광대역 무선 라우터에 내장된 액세스 지점 포함) 없이 서로 범위 내에 있는 모든 무선 장치가 서로를 보고 피어 투 피어 방식으로 통신할 수 있습니다.

ad-hoc 네트워크를 설정하려면 각 무선 어댑터를 infrastructure 모드가 아닌 ad-hoc 모드로 구성해야 합니다.

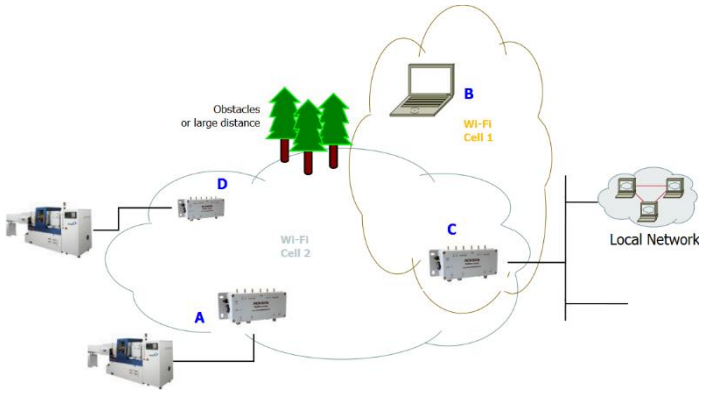
또한 ad-hoc 네트워크의 모든 무선 어댑터는 동일한 SSID 와 동일한 채널 번호를 사용해야 합니다.

Ad-hoc 네트워크는 매우 가까운 환경에 있는 장치들을 소규모로 그룹화하려는 특징을 가지고 있으며, 모든 통신 장치는 동일한 셀을 공유해야 합니다. 그래서 이 네트워크 환경에서는 원격에 있는 장치들을 연결하기 위한 방법이 없습니다.

보안을 사용하지 않으면, Ad-hoc 은 802.11abgn/ac 모드로 작동합니다.

WEP 보안을 사용하면, Ad-Hoc 은 802.11abg 모드로 작동합니다.

Ad-Hoc 모드는 WPA/WPA2 보안을 지원하지 않습니다.



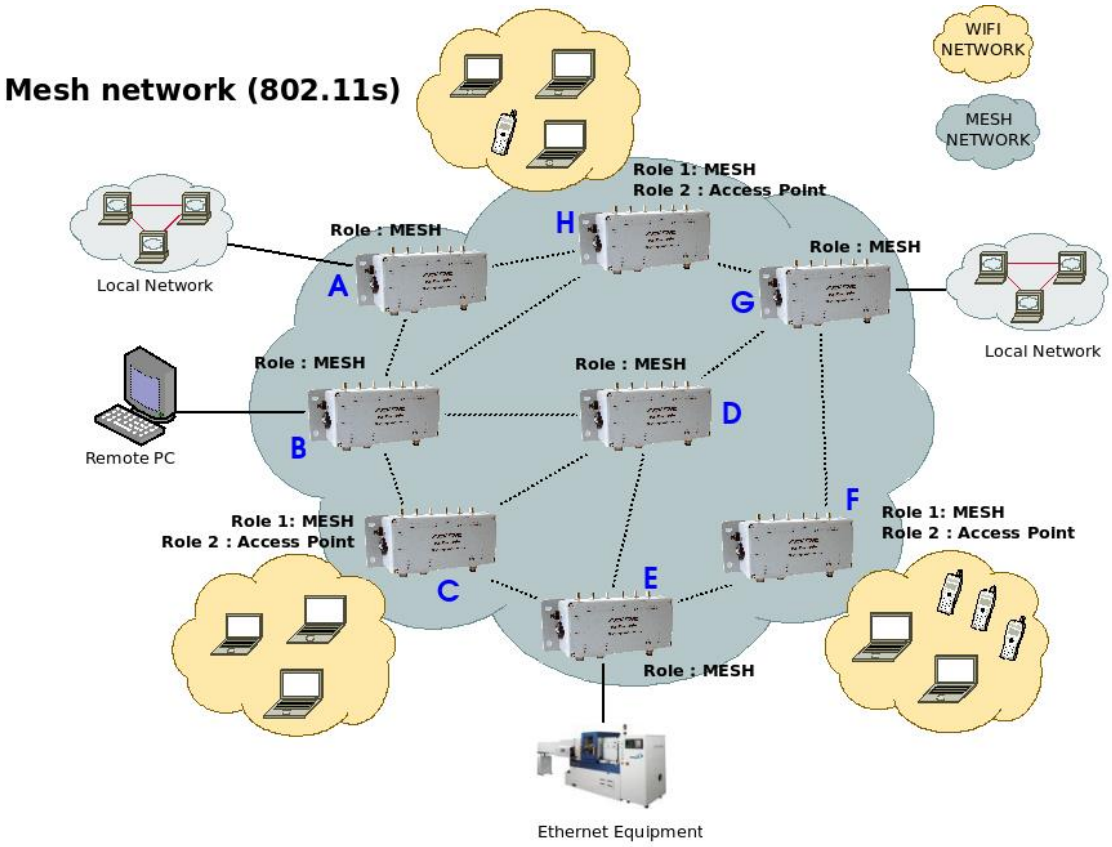
제품 **A**, **C**, **D** 서로 통신할 수 있습니다.
제품 **B**, **C** 서로 통신할 수 있습니다.
제품 **B**, **D** 방해물로 인해 서로 통신할 수 없습니다.
제품 **A**, **B** 너무 멀어서 서로 통신할 수 없습니다.
제품 **C** 는 **A, D** 에서 **B** 로 전달할 수 없습니다.

V.2.1.3 Mesh (802.11s) Mode

802.11s 메쉬 네트워크에는 3 가지 종류의 장치가 있습니다. 이들은 모두 패킷 릴레이 프로세스에 참여합니다.

- **mesh station** 에는 자체적인 기능이 있습니다(예 : 랩톱 컴퓨터).
- **mesh access point** 는 "메쉬" 및 "기본 액세스 포인트" 기능을 모두 제공하여 메시가 아닌 Wi-Fi 장치를 메시 네트워크에 연결합니다.
- **mesh portal** 을 사용하면 다른 네트워크 유형을 메쉬 네트워크에 브리지할 수 있습니다. 예를 들어, 포털은 이더넷을 Wi-Fi 메시에 연결합니다.

ACKSYS 제품은 현재 "스테이션" 및 "포털" 기능을 구현하고 있습니다. 두 개의 무선 카드가 장착된 제품은 메시 액세스 포인트로 사용할 수 있습니다.



제품 **A** 부터 **H** 까지 서로 통신할 수 있습니다.
제품 **A, B, D, E, G** 는 메쉬 포털 기능을 제공합니다.
제품 **C, F, H** 는 메쉬 AP 기능을 제공합니다.

Routing protocols

두 메시 지점 사이의 전송 경로를 결정하려면 라우팅 프로토콜이 네트워크를 분석해야 합니다. 802.11s 는 HWMP 를 필수 프로토콜로 정의하고 다른 타사 라우팅 프로토콜을 연결하기 위한 준비를 합니다. ACKSYS 제품은 HWMP 를 구현합니다.

Security protocols

802.11s 네트워크는 보안이 없거나 *V.2.5.7 Mesh Secure Authentication of Equals (SAE)* 섹션에서 설명된 WPA3-PSK (SAE-Personnal) 보안을 사용할 수 있습니다. 이 보안은 infrastructure WPA/PSK 와 유사합니다.

V.2.1.4 Wireless Network Name

SSID 는 무선 네트워크에서 식별자 역할을 합니다.

SSID 는 사용자가 액세스하려는 특정 802.11 무선 LAN 을 식별하는 데 사용되는 이름입니다. 클라이언트 장치는 범위 내의 모든 액세스 포인트로부터 브로드캐스트 메시지를 수신하여 자신의 SSID 를 알리고, 범위 내의 SSID 목록을 표시한 후 사용자에게 SSID 를 선택하도록 요청하여 연결할 SSID 를 선택할 수 있습니다.

Wi-Fi 통신에 참여하는 장치는 모두 동일한 SSID 를 사용해야 합니다. 사용 가능한 무선 네트워크를 검색할 때 이 이름이 목록에 나타납니다. 보안을 위해 미리 구성된 네트워크 이름을 변경하는 것이 좋습니다.

802.11s 메쉬 모드에서 사용되는 SSID 를 "메쉬 ID"라고 합니다. Infrastructure SSID 와 동일한 형식을 취하지만 별도의 매개 변수입니다. Infrastructure SSID 와 메시 ID 에 동일한 문자열을 사용하는 경우 두 개의 다른 WLAN 으로 간주됩니다.

V.2.1.5 Virtual AP (multi-SSID) and multifunction cards

이 제품은 단일 무선 카드에서 여러 가상 기능(인터페이스)을 구현할 수 있습니다. 예를 들어, 하나의 무선 장치를 사용하여 여러개의 SSID 를 브로드캐스팅하여 하나의 메시 지점과 함께 여러 실제 AP 를 동시에 시뮬레이션할 수 있습니다.

하나의 무선 카드가 동시 가상 인터페이스를 지원하는 경우 모두 동일한 채널로 설정해야 합니다(따라서 클라이언트 검색은 선택한 채널로 제한되어야 하며 다중 채널 로밍은 불가능합니다). 채널 대역폭은 모든 인터페이스에서 공유됩니다.

다기능 제한은 웹 인터페이스의 "Setup / Physical interfaces Overview" 페이지에 표시됩니다.

V.2.1.6 Wireless repeater

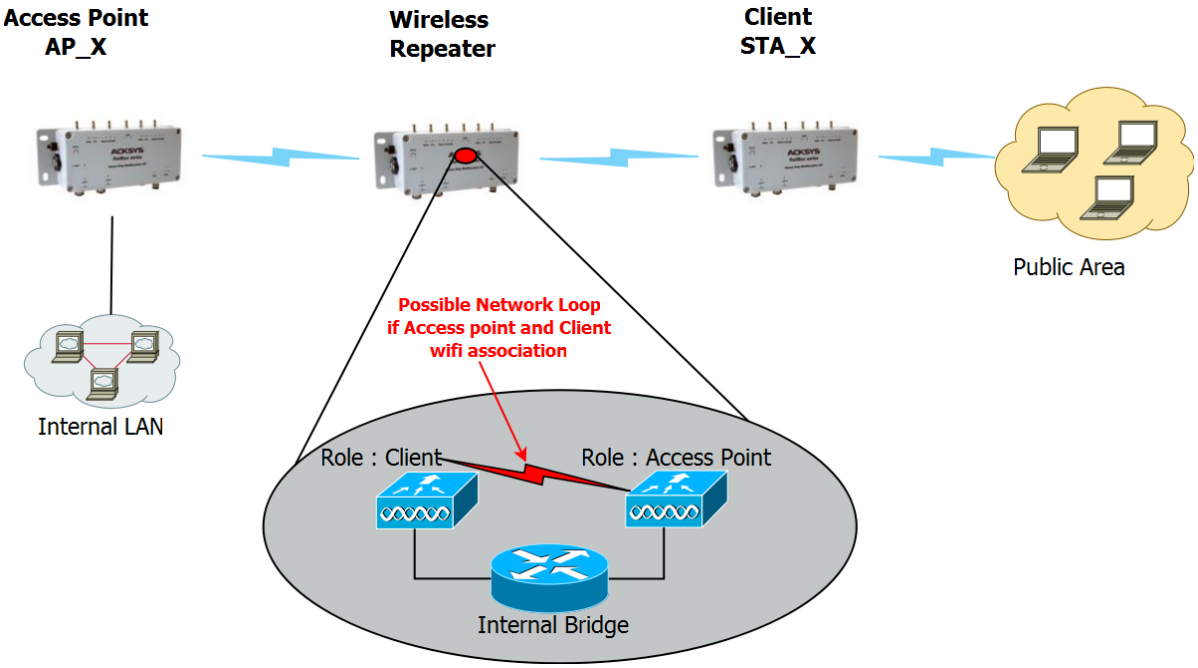
액세스 포인트 AP_X 와 무선 스테이션 STA_X 사이의 거리가 너무 길어 직접 연결할 수 없는 경우 무선 중계기를 사용하여 갭을 메웁니다.

무선 중계기는 2 가지 역할을 합니다.

➔ 액세스 포인트 AP_X 에 데이터를 전달하는 클라이언트 역할.

➔ 무선 스테이션 STA_X 에 데이터를 전달하는 액세스 포인트 역할.

이 두 역할은 동일한 스위치에서 함께 브리지됩니다. 따라서, 리피터에 대해 여러 가지 구성이 가능합니다.



리피터를 구성할 때 클라이언트 리피터가 액세스 포인트 리피터와 연결되지 않도록 각별히 주의해야 합니다(SSID 가 동일한 경우). 그러면 네트워크 루프가 생성됩니다.

네트워크 루프를 방지하는 두 가지 방법

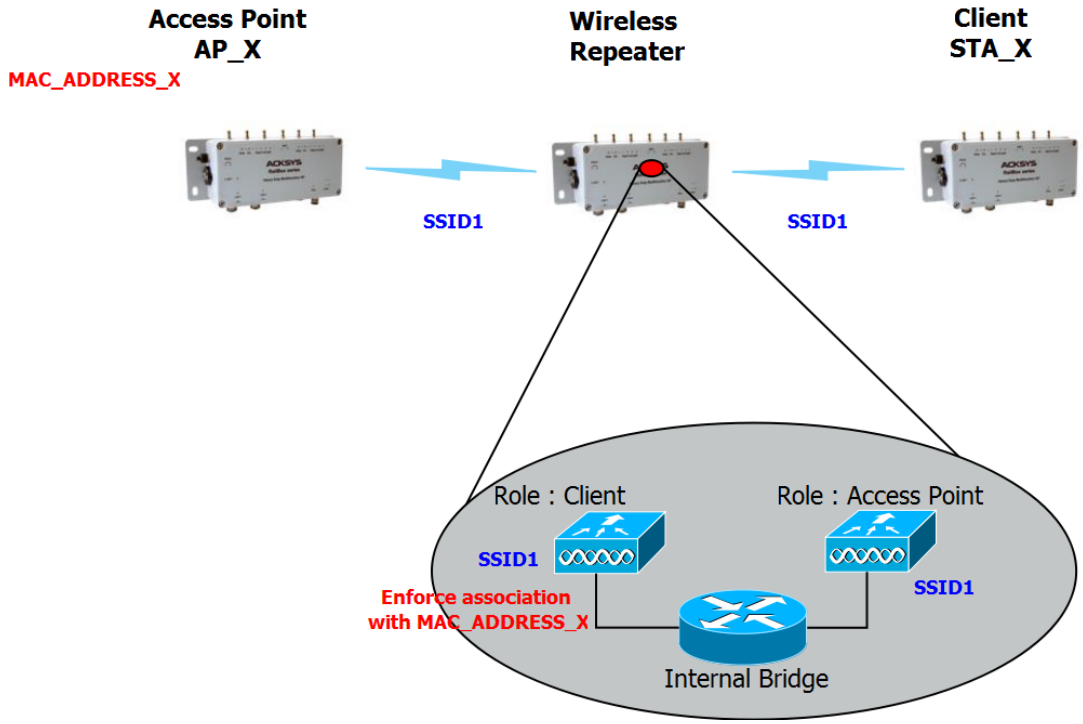
➔ 클라이언트 역할과 리피터의 액세스 포인트 역할에서 동일한 SSID 를 설정하지만 클라이언트 역할이 AP_X 의 BSSID 와 연결되도록 강제합니다. 클라이언트 역할의 "multiple SSID" 기능을 사용하여 BSSID 구성의 잠금을 해제합니다.

장점:

서비스 연속성: 중계기가 동일한 SSID 로 현재 네트워크를 확장합니다. 따라서 최종 사용자는 모든 네트워크 위치에서 동일한 SSID 를 유지할 수 있습니다.

단점:

AP_X 가 교체되면 리피터의 클라이언트 역할이 새 BSSID 에만 연결되도록 재구성해야 합니다.



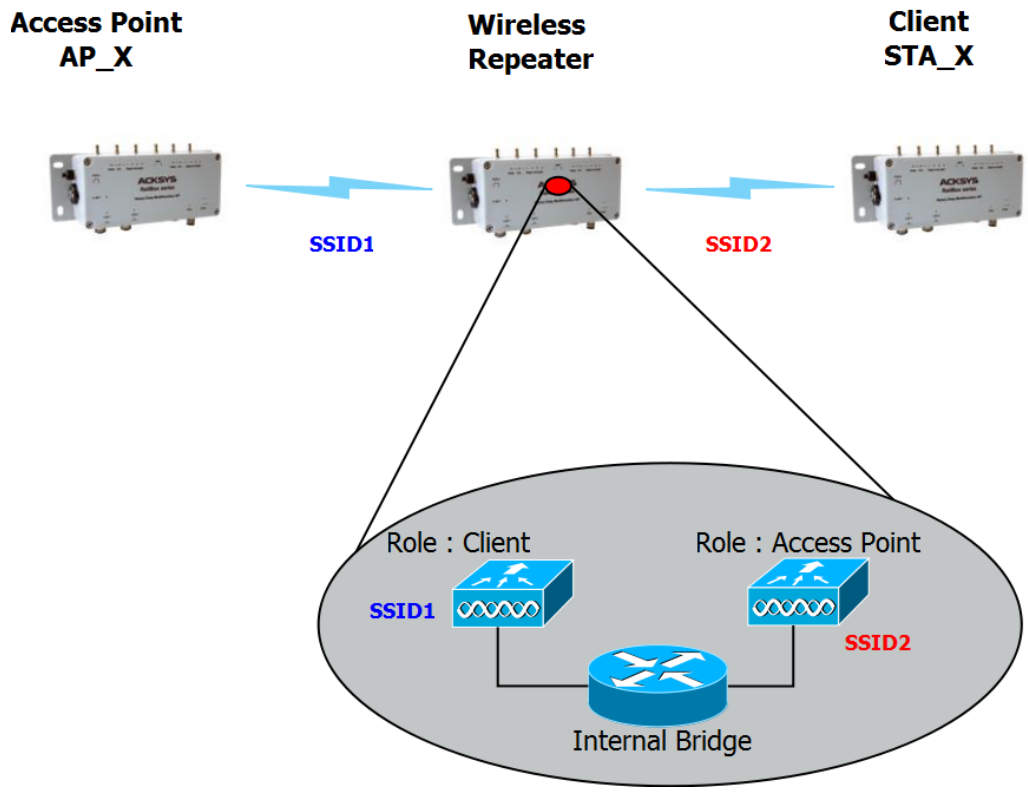
➔ 클라이언트 역할과 리피터의 액세스 포인트 역할에서 다른 SSID 를 설정합니다.

장점:

AP_X 를 변경해도 리피터를 재구성할 필요가 없습니다.

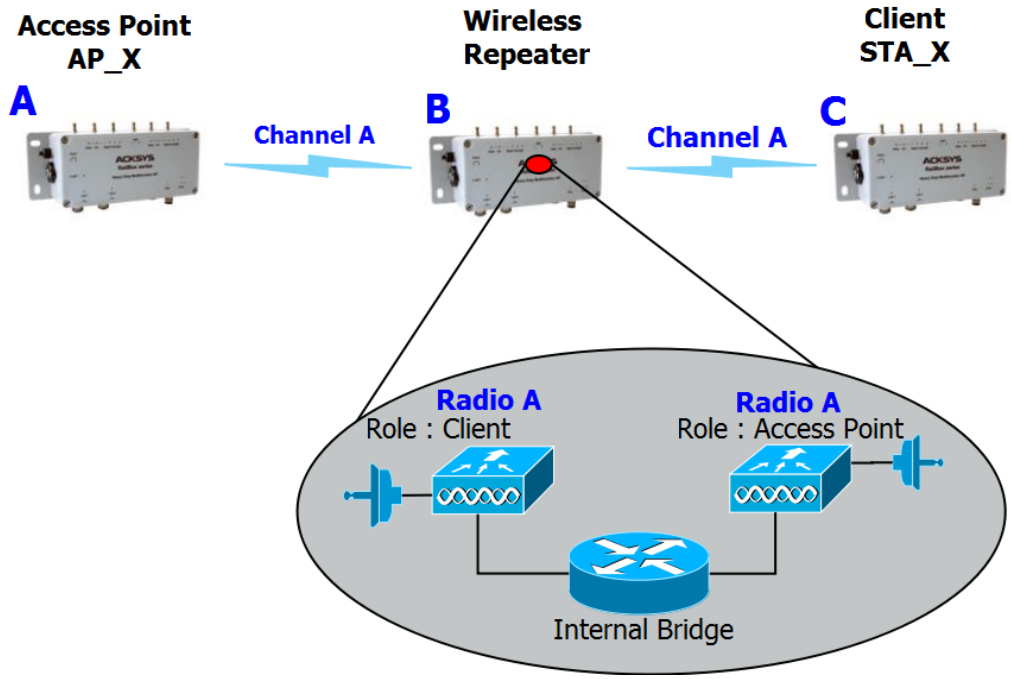
단점:

확장된 네트워크에 다른 SSID 가 있으므로 사용자는 여러 SSID 를 사용해야 하는 불편함이 발생합니다.



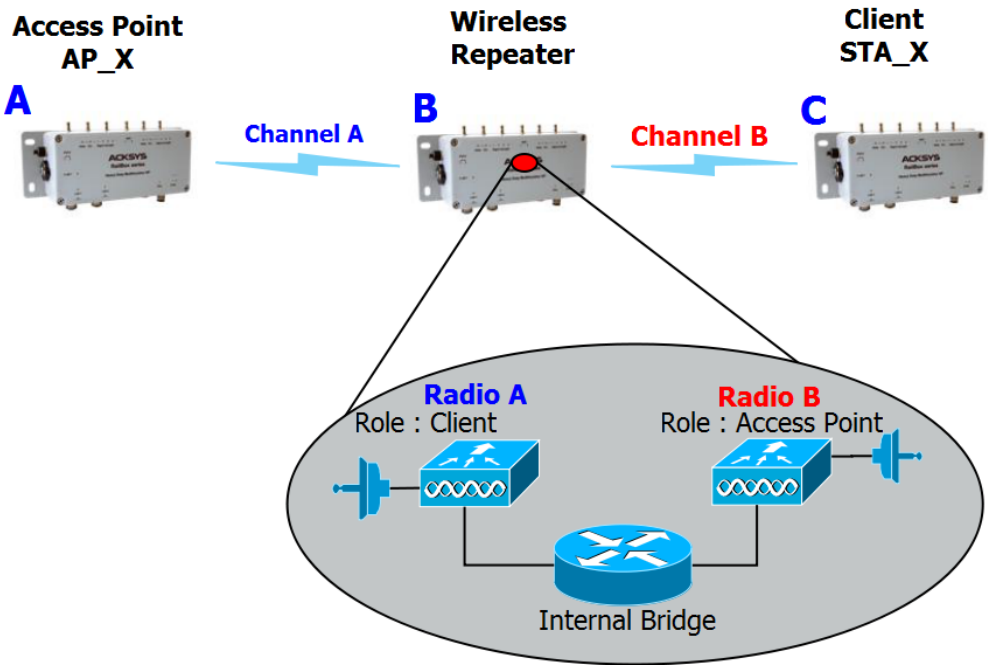
처리량에 미치는 영향:

리피터는 하나의 무선 카드를 사용하여 클라이언트+액세스 포인트라는 두 가지 역할을 수행하고 AP X 에서 리피터로, 그리고 리피터에서 STA X 로(또한 그 반대) 전송을 수행합니다. 라디오 카드가 하나만 있는 리피터는 동시에 수신과 전송을 할 수 없기 때문에 처리량이 50% 이상 감소합니다.



고성능 리피터:

처리량을 향상시키기 위해, 듀얼 무선 중계기는 각 무선 카드의 다른 채널을 사용하여 AP 역할을 위해 하나의 라디오를 사용하고 클라이언트 역할을 위해 다른 라디오를 사용할 수 있으므로 동시에 송수신할 수 있습니다.



장점:
사용 가능한 대역폭을 두 배로 늘리고 루프 문제도 해결합니다.
단점:
최종 사용자는 SSID 를 찾기 위해 여러 채널을 검색해야 합니다.

V.2.2 Hardware

휴대 전화 인터페이스는 휴대 전화의 데이터 서비스와 기능적으로 동일합니다. 보조 Wi-Fi 인터페이스를 대체합니다. 하나 또는 두 개의 안테나가 필요합니다. 두 번째 안테나를 사용하면 통신 품질이 향상됩니다.

세 번째 안테나 커넥터가 있으면 위성 위치 지정에 사용됩니다(GNSS 에 대한 다음 섹션 참조).

셀룰러 인터페이스는 공용 모바일 네트워크에 연결됩니다. 이렇게 하려면 적절한 공용 통신사의 계정이 필요합니다. 이 계정은 제품에 설치된 SIM 카드의 형태입니다. 2 개의 SIM 카드를 설치할 수 있으므로 2 개 중 1 개의 통신사를 선택할 수 있습니다.

V.2.3 Modulation and coding

5 가지 무선 전송 형식을 사용할 수 있습니다: 802.11b, 802.11g, 802.11a, 802.11n 및 802.11ac.

V.2.3.1 802.11b

802.11b 는 예전 장치와의 호환성을 위해 지원됩니다. 802.11b 는 처리량이 적기 때문에 802.11b 를 사용하면 무선 범위의 모든 장치에 대한 처리량이 줄어듭니다.

Op. Frequency	Typical throughput	Bit Rate (Max)
2.4 GHz	4.5 Mbit/s	11 Mbit/s

참고: 실제 처리량 및 비트 전송률은 스테이션 간의 거리, 안테나 품질 및 무선 조건에 따라 달라집니다.

802.11b 의 최대 데이터 전송 속도는 11 Mbit/s 이며 표준에 정의된 액세스 방법을 사용합니다. 802.11b 장치는 2.4GHz 대역에서 작동하는 다른 제품의 간섭을 받습니다. 2.4GHz 범위에서 작동하는 장치에는 전자레인지, 블루투스 장치 및 오래된 무선 전화등이 포함됩니다.

V.2.3.2 802.11g

이 전송 표준은 2.4GHz 대역(802.11b 와 같이)에서 작동하지만 최대 54Mbit/s 의 데이터 속도 또는 약 20Mbit/s 의 평균 처리량으로 작동합니다. 802.11g 하드웨어는 802.11b 하드웨어와 호환이 가능합니다.

Op. Frequency	Typical throughput	Bit Rate (Max)
2.4 GHz	20 Mbit/s	54 Mbit/s

참고: 실제 처리량 및 비트 전송률은 스테이션 간의 거리, 안테나 품질 및 무선 조건에 따라 달라집니다.

802.11b 와 마찬가지로 802.11g 장치는 2.4GHz 대역에서 작동하는 다른 제품의 간섭을 받습니다. 2.4GHz 범위에서 작동하는 장치에는 전자레인지, 블루투스 장치 및 오래된 무선 전화등이 포함됩니다.

V.2.3.3 802.11a

802.11a 는 5GHz 대역에서 작동하고, 최대 데이터 속도는 54Mbit/s 이며, 20Mbit/s 중반의 현실적인 평균 처리량을 산출합니다.

Op. Frequency	Typical throughput	Bit Rate (Max)
5 GHz	20Mbit/s	54Mbit/s

참고: 실제 처리량 및 비트 전송률은 스테이션 간의 거리, 안테나 품질 및 무선 조건에 따라 달라집니다.

2.4GHz 대역은 포화 상태인 경우가 많기 때문에 상대적으로 사용되지 않는 5GHz 대역을 사용하면 802.11a 에 상당한 이점이 있습니다. 그러나 이 높은 주파수는 다음과 같은 약간의 단점도 있습니다. 802.11a 의 전체 유효 범위는 802.11b/g 보다 약간 낮습니다. 802.11a 신호는 벽 및 기타 장애물에 의해 더 쉽게 흡수되기 때문에 802.11b 보다 통신거리가 짧습니다.

V.2.3.4 802.11n

802.11n 은 2.4GHz 또는 5GHz 대역에서 작동할 수 있습니다. 선택한 항목에 따라 범위 및 밴드 포화도에 대한 위의 참고 사항도 적용됩니다.

또한 802.11n 에서는 20MHz 또는 40MHz 의 채널 폭을 사용하여 대역폭을 두 배로 늘릴 수 있습니다. "HT20"은 표준 단일 채널 작동을 의미하며, "HT40"은 확장된 이중 채널 작동을 의미합니다.

802.11n 하드웨어는 두 개 이상의 데이터 스트림("공간 스트림")을 동시에 전송할 수 있습니다. 스트림이 서로 간섭하지 않으려면 무선 신호가 장애물에 대해 다양한 방향으로 튕겨야 하거나 안테나가 편광되어야 합니다. 두 경우 모두 전력 손실로 인해 범위가 낮지만 전송 속도가 빨라집니다.

공간 스트림의 수와 안테나 수를 혼동하면 안 됩니다. 또한 안테나는 방출 또는 수신 전용일 수 있습니다. 따라서 802.11n 무선 사양에는 송신기 수, 수신기 수, 공간 스트림 수 이렇게 세 가지 숫자가 포함되어야 합니다.

무선 조건에 자동으로 적응하기 위해 802.11n 은 스트림 수, 변조, 채널 폭 등 다양한 전송 매개 변수를 사용합니다. 결과 전송 형식은 MCS(Modulation and Coding Scheme)라고 합니다. ACKSYS 제품은 모델에 따라 1~3 개의 스트림을 처리합니다. 다음은 1 개, 2 개 및 3 개의 스트림으로 달성할 수 있는 물리적 비트 전송률입니다.

Maximum bit rate (Mbps)

Channel width	20 MHz	40 MHz
1 stream		
MCS 0	7.2	15
MCS 1	14.4	30
MCS 2	21.7	45
MCS 3	28.9	60
MCS 4	43.3	90
MCS 5	57.8	120
MCS 6	65.0	135
MCS 7	72.2	150
2 streams		
MCS 8 = 2xMSC0	14.4	30
MCS 9 = 2xMCS1	28.9	60
MCS 10 = 2xMCS2	43.3	90
MCS 11 = 2xMCS3	57.8	120
MCS 12 = 2xMCS4	86.7	180
MCS 13 = 2xMCS5	115.6	240
MCS 14 = 2xMCS6	130.0	270
MCS 15 = 2xMCS7	144.4	300
3 streams		
MCS 16 = 3xMCS0	21.7	45
MCS 17 = 3xMCS1	43.3	90
MCS 18 = 3xMCS2	65.00	135
MCS 19 = 3xMCS3	86.7	180
MCS 20 = 3xMCS4	130	270
MCS 21 = 3xMCS5	173.3	360
MCS 22 = 3xMCS6	195	405
MCS 23 = 3xMCS7	216.7	450

참고 1: Peer station 이 짧은 guard interval 을 처리할 수 없는 경우 비트 전송률이 약 10% 감소합니다. Guard interval 은 802.11n 기능으로 전송 중 유휴 시간을 단축할 수 있습니다.
참고 2: 위의 표에서 추론할 수 있듯이 비트 전송률은 스트림 수에 비례합니다. 3 streams 무선은 최대 450Mbps 까지 전송할 수 있습니다.
참고 3: 실제 비트 전송률과 처리량은 스테이션 간 거리, 안테나 품질 및 무선 상태에 따라 달라집니다.

MCS, 비트 전송 속도, 최대 전송 전력 및 수신기 감도에 대한 자세한 정보는 각 제품의 퀵 스타트 가이드를 참조하세요.

V.2.3.5 802.11ac

802.11n 과 비교하여 802.11ac 은 80MHz 채널 크기(광범위 채널 증가 속도), 256-QAM 변조(스트림당 2 개의 새로운 MCS)를 추가하고 5GHz 대역만 지원합니다.

다음은 1, 2, 3 스트림으로 달성할 수 있는 물리적 비트 전송률입니다.

Maximum bit rate (Mbps)

Channel width	20 MHz	40 MHz	80 MHz
1 stream			
MCS 0	7.2	15	32.5
MCS 1	14.4	30	65
MCS 2	21.7	45	97.5
MCS 3	28.9	60	130
MCS 4	43.3	90	195
MCS 5	57.8	120	260
MCS 6	65	135	292.5
MCS 7	72.2	150	325
MCS 8	86.7	180	390
MCS 9	n/a	200	433.3
2 streams			
MCS 0	14.4	30	65
MCS 1	28.9	60	130
MCS 2	43.3	90	195
MCS 3	57.8	120	260
MCS 4	86.7	180	390
MCS 5	115.6	240	520
MCS 6	130.3	270	585
MCS 7	144.4	300	650
MCS 8	173.3	360	780
MCS 9	n/a	400	866.7
3 streams			
MCS 0	21.7	45	97.5
MCS 1	43.3	90	195
MCS 2	65	135	292.5
MCS 3	86.7	180	390
MCS 4	130	270	585
MCS 5	173.3	360	780
MCS 6	195	405	n/a
MCS 7	216.7	450	975
MCS 8	260	540	1170
MCS 9	288.9	600	1300

V.2.4 Radio channels and national regulation rules

무선 네트워크는 2.4GHz 또는 5GHz 라디오 스펙트럼의 특정 채널을 사용하여 스테이션 간의 통신을 처리합니다. 해당 지역의 일부 채널에서 다른 전자 장치의 간섭이 발생할 수 있습니다. 무선 네트워크의 성능과 적용 범위를 최적화하는 데 도움이 되는 가장 명확한 채널을 선택합니다.

Region/country

모든 국가에서 사용 가능한 무선 주파수를 제어하고 제한합니다. 현재 사용되고 있는 802.11 2.4GHz 및 5GHz 대역은 다른 무선 장치(레이더, 기상 장치)와 공유할 수 있도록 더욱 제한됩니다. 제품을 운영할 국가를 설정하면 메뉴에서 제안하는 채널이 선택한 국가에서 사용할 수 있는 채널로 제한됩니다.
"AP" 역할에서 제품은 802.11d 프로토콜에서 요구하는 대로 국가 규칙을 비콘에 삽입합니다. "클라이언트" 역할에서 제품은 802.11d 프로토콜을 사용하여 AP 에서 제공하는 국가 규칙을 사용합니다.

무선 규제 영역에 대한 자세한 내용은 *802.11 regulatory domain rules*, *Appendix – 802.11 Radio channels* 이 부분을 참고하세요.

Automatic channel selection

액세스 포인트 모드에서는 제품이 목록 중 또는 해당 국가에서 사용 가능한 모든 채널 중에서 가장 적합한 채널을 선택할 수 있습니다. 시작 시(이는 한 번만 발생함) AP 는 측정된 노이즈와 가능한 각 채널의 점유율에 따라 최적의 채널을 선택합니다. 이 노이즈 분석은 분석된 채널당 약 0.5 초 동안 제품의 정상가동 시간을 지연시킵니다.

AP 이외의 역할은 이 옵션을 인식하지 못합니다. 리피터, 메시 및 애드혹 역할의 경우 채널을 하나만 설정해야 합니다. 클라이언트 역할의 경우 사전 로밍 모드를 선택한 경우를 제외하고 사용 가능한 모든 채널이 검색됩니다.

V.2.5 Wireless security

무선 네트워크 침입을 방지하기 위해 사용할 수 있는 많은 기술이 있지만 현재 절대적으로 안전한 방법은 없습니다. 가장 좋은 전략은 여러 보안 조치를 결합하는 것입니다.

무선 네트워크 보안을 위한 단계

1. 모든 무선 LAN 장치를 보호해야 합니다.
2. 무선 네트워크의 모든 사용자는 무선 네트워크 보안에 대한 교육을 받아야 합니다.
3. 모든 무선 네트워크를 적극적으로 모니터링 하여 취약점 및 위반 여부를 확인해야 합니다.

사용 가능한 무선 보안 보호

SSID 를 브로드캐스트 하지 않음 (액세스포인트 전용 기능)
WEP encryption
Enhanced Open (WPA3-OWE)
WPA, WPA2 or WPA3 – PSK (*Pre-Shared Key*)
WPA, WPA2 or WPA3 – Enterprise, 802.1x 또는 RADIUS 라고도 함.
OSEN

WEP encryption vs. WPA and WPA2 encryption

암호화는 무선 토폴로지에 따라 다릅니다. 애드혹 모드에서는 WPA 가 암호화 키를 설정하기 위해 포인트 투 포인트 링크가 필요하기 때문에 WEP 암호화만 사용할 수 있습니다. 인프라 모드에서는 각 스테이션과 관련된 액세스 포인트 사이에 포인트 투 포인트 링크가 있으며, WEP 또는 WPA/WPA2 를 사용할 수 있습니다.

V.2.5.1 WEP encryption

WEP 는 무선 통신을 위해 데이터를 암호화하는 방법이며 유선 네트워크와 동일한 수준의 개인 정보를 제공하기 위한 것입니다. 그러나 암호화 기술의 발전으로 인해 **WEP 는 더 이상 안전하지 않으며, 802.11N/AC 모드와 함께 사용할 수 없습니다.** WEP 네트워크에 액세스하려면 키를 알고 있어야 합니다. 키는 사용자가 생성하는 일련의 문자입니다. WEP 를 사용할 때는 암호화 수준을 결정해야 합니다. 암호화 유형에 따라 키 길이가 결정됩니다. 128 비트 암호화에는 64 비트 암호화보다 긴 키가 필요합니다.

키는 HEX(16 진수 - 0-9, A-F 문자 사용) 또는 ASCII(미국 정보 교환 표준 코드 - 영숫자 문자) 형식으로 문자열을 입력하여 정의합니다.

기억하기 쉬운 문자열을 입력할 수 있도록 ASCII 형식이 제공됩니다. ASCII 문자열은 네트워크에서 사용할 수 있도록 16 진수로 변환됩니다. 키를 쉽게 변경할 수 있도록 4 개의 키를 정의할 수 있습니다. 네트워크에서 사용할 기본 키가 선택됩니다.

V.2.5.2 WEP authentication

WEP 방식은 *Open System authentication* 과 *Shared Key authentication* 두 가지 인증 방법을 사용할 수 있습니다.

Open System authentication 인증 방법에서 WLAN 클라이언트는 인증 중에 액세스 포인트에 자격 증명을 제공할 필요가 없습니다. 따라서 모든 클라이언트는 WEP 키에 관계없이 액세스 포인트로 자신을 인증하고 연결을 시도할 수 있습니다. 사실상 인증이 발생하지 않습니다. 인증 및 연결 후 WEP 는 데이터 프레임을 암호화 하기 위하여 사용될 수 있습니다. 이때 클라이언트는 올바른 키를 가지고 있어야 합니다.

Shared Key authentication 인증 방법에서 WEP 는 인증에 사용됩니다. 4 방향 challenge-response handshake 가 사용됩니다.

1) 클라이언트는 액세스 포인트로 인증 요청을 보냅니다.
2) 액세스 포인트는 clear-text challenge 를 다시 보냅니다.
3) 클라이언트는 구성된 WEP 키를 사용하여 challenge text 를 암호화하고 다른 인증 요청으로 다시 전송해야 합니다.
4) 액세스 포인트는 정보를 해독하고 보낸 clear-text 와 비교합니다. 이 비교 결과에 따라 액세스 포인트는 긍정 또는 부정 응답을 반환합니다. 인증 및 연결 후 WEP 를 사용하여 데이터 프레임을 암호화할 수 있습니다.

언뜻 보면 공유 키 인증이 개방형 시스템 인증보다 더 안전한 것처럼 보일 수 있습니다. 이는 공유 키 인증이 실제 인증을 제공하지 않기 때문입니다. 하지만, 그것은 정반대입니다. 공유 키 인증에서 4 개의 핸드셰이크 프레임을 캡처하여 정적 WEP 키를 도출할 수 있습니다. 따라서 WEP 인증에는 공유 키 인증보다 개방형 시스템 인증을 사용하는 것이 좋습니다. **두 인증 모두 메커니즘이 취약하여 현재는 사용되지 않습니다.**

V.2.5.3 Enhanced Open (WPA3-OWE)

Wi-Fi Enhanced Open 은 OWE(Opportunistic Wireless Encryption)를 기반으로 하는 공용 네트워크의 새로운 보안 표준입니다. 커피숍, 호텔, 식당 및 도서관 등의 개방된 비암호 보호 네트워크를 통해 암호화 및 개인 정보를 제공합니다. Enhanced Open 은 인증을 제공하지 않습니다.

V.2.5.4 WPA/WPA2/WPA3 encryption

WPA/WPA2/WPA3 는 기존 및 미래의 Wi-Fi 네트워크에서 무선 데이터 보호 및 액세스 제어 수준을 크게 향상시킵니다. 802.11 표준의 원래 기본 보안 메커니즘인 WEP(Wired Equivalent Privacy)의 알려진 모든 약점을 해결합니다.

WPA/WPA2/WP3 는 WEP 의 취약점을 해결하기 위해 강력한 데이터 암호화를 제공할 뿐만 아니라 WEP 에서 크게 누락되었던 사용자 인증을 추가합니다. WPA2 는 802.11b, 802.11a 및 802.11g, 다중 대역 및 다중 모드를 포함한 모든 버전의 802.11 장치를 보호하도록 설계되었습니다.

WPA 는 암호화 기술의 발전으로 인해 더 이상 안전하지 않은 오래된 표준입니다.

WPA2 는 더 강력한 IEEE 802.11i 보안 표준을 보다 최근에 구현한 것입니다.

WPA3 는 보다 강력한 암호 기반 인증을 제공하여 개별 사용자에게 더 나은 보호를 제공하는 최신 구현입니다. 이 기능은 WPA2-Personal 의 PSK(Pre-shared Key)를 대체하는 SAE(Simultaneous Authentication of Equals)를 통해 활성화됩니다.

WPA3 에는 보안 취약성으로 인해 서로 호환되지 않는 세 가지 버전이 있습니다. WaveOS 는 2019 년 8 월 이후 최신 버전을 사용합니다.

암호 유형은 데이터 통신을 보호하는 데 사용되는 암호화 알고리즘입니다.

TKIP (*Temporal Key Integrity Protocol*) 는 WEP 를 기반으로 패킷별 키 생성을 제공합니다.

AES (*Advanced Encryption Standard*) 는 매우 안전한 블록 기반 암호화입니다.

다음 세 가지 보안 옵션 중에서 선택할 수 있습니다(WPA 는 권장되지 않습니다).

WPA Mode	Cipher Type	Security solution
WPA	RC4	RC4-TKIP
WPA2	AES	AES-CCMP
WPA3	AES	AES-GCMP-256

a. Pre-shared key mode (PSK)

PSK(Pre-Shared Key Mode, personal mode 라고도 함)에서 각 액세스 포인트 클라이언트는 네트워크에 액세스하려면 암호를 제공해야 합니다. 암호는 8~63 자의 인쇄 가능한 ASCII 문자일 수 있습니다. 대부분의 운영 체제에서는 다시 입력할 필요가 없도록 암호를 저장할 수 있습니다. 또한 암호는 Wi-Fi 액세스 지점에 저장된 상태로 유지되어야 합니다.

Wi-Fi 셀의 모든 Wi-Fi 장치는 동일한 Pre-Shared Key 를 가지고 있어야 합니다.

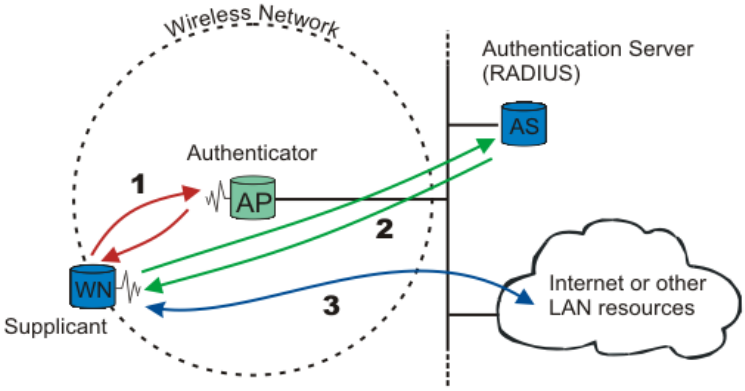
b. Enterprise mode (802.1x, RADIUS)

WPA/WPA2-Enterprise 또는 802.1x 는 액세스 지점을 통해 전용 네트워크에 연결하거나, 액세스 지점을 LAN 리소스에 대한 게이트웨이로 설정하거나, 인증에 실패할 경우 해당 장치에서 액세스를 차단하려는 장치에 인증을 제공합니다.

참고: 리피터 연결에서 가장 먼 리피터들은 802.1X 서버에 접근하기 위해 가장 가까운 리피터들에 의존하기 때문에, 이 보안은 리피터 모드에서는 사용할 수 없습니다. WPA/WPA2-PSK 는 사용할 수 있습니다.

인증 프로세스는 다음과 같은 여러 에이전트로 구성됩니다.

- supplicant 또는 Wireless Node (WN)라고도 하는 사용자,
- Wireless access point or authenticator,
- Authentication server, 즉 RADIUS (Remote Authentication Dial-In User Service) server,
- Authentication 방식.



Wireless node(WN)가 LAN 리소스에 대한 액세스를 요청할 때 첫 번째 단계는 클라이언트와 액세스 지점 간의 물리적 연결로, 이른바 "access port"(도표의 1 번)를 정의합니다.

Access point(AP)는 WN 의 ID 를 요청합니다. 그런 다음 WN 과 인증 서버 사이에 포인트 투 포인트 EAP 터널을 설정합니다(도표의 2 번). WN 이 인증될 때까지("포트"가 닫힐 때까지) EAP 이외의 다른 트래픽은 허용되지 않습니다. 인증될 때까지 클라이언트는 LAN 에 액세스할 수 없습니다.

인증 서버가 인증자에게 WN 이 인증되었음을 알리면 LAN 으로의 트래픽이 허용됩니다(그림의 3 번). "port"가 열려 있습니다. 그렇지 않으면 "port"가 닫힌 상태로 유지됩니다.

참고: 802.1x 는 통신을 암호화하고 무결성을 확인하는 데 사용될 키를 교환하는 시스템을 제공합니다.

Authentication modus operandi

802.1x 는 EAP(Extensible Authentication Protocol) 방법 중 하나를 사용합니다. 가장 일반적으로 사용되는 것은 다음과 같습니다.

- EAP-PEAP
- EAP-TLS
- EAP-TTLS

사용되는 EAP 방법은 액세스 지점에 대해 알기 쉽습니다. 반면 브리지와 같은 액세스 포인트 클라이언트는 인증 방법을 알고 있어야 합니다. 방법을 선택할 때는 서버/클라이언트의 기능과 필요한 보안 수준을 고려해야 합니다.

예를 들어 윈도우즈 10 클라이언트는 다음을 허용합니다.

- 로그인과 암호(MSCHAP V2 라 불리는)를 사용한 PEAP 인증
- 인증서 사용.

Preauthentication

클라이언트는 현재 연결된 AP 를 통해 새로운 AP 로 인증할 때 사전 인증을 요청합니다. 802.1x 프로토콜의 중요한 오버헤드를 제거하기 때문에 클라이언트가 사전 인증된 AP 로 로밍하기로 결정할 때 연결 시간을 단축하는 것을 목표로 합니다.

클라이언트가 사전 인증을 사용할 수 있도록 하려면 AP 에서 사전 인증을 활성화해야 합니다. 이러한 제품의 클라이언트 역할은 AP 가 제공할 때 항상 사전 인증을 사용합니다.

사전 인증은 클라이언트가 통신 키를 필요하기 전에 저장하도록 합니다. 클라이언트는 802.1x 프로토콜을 다시 실행하지 않고도 한 AP 에서 다른 AP 로 로밍을 허용하면서 많은 키를 미리 보관할 수 있습니다.

클라이언트에서 키는 수명이 구성 가능한 캐시 테이블에 보관됩니다.

V.2.5.5 Protected management frame (802.11w)

이 기능은 해커 DoS(서비스 거부) 공격으로부터 장치를 보호합니다.

기본적으로 관리 프레임은 보호되지 않습니다. 누구나 클라이언트 또는 AP 에 DEAUTH 프레임을 보낼 수 있습니다.

이 경우 해커는 Wi-Fi 스니퍼를 사용하여 AP 정보를 수집한 다음 AP MAC 주소가 포함된 DEAUTH 프레임을 레거시 클라이언트에 전송할 수 있습니다. 클라이언트는 이 프레임을 수신한 다음 AP 와의 연결을 닫습니다.

802.11w 는 프레임에 필드를 추가하여 프레임 전송자를 인증합니다.

Wi-Fi 장비가 올바르지 못한 전송자로부터 관리 프레임을 수신하면 해당 프레임은 폐기됩니다.

WPA3 에서는 보호된 관리 프레임이 항상 활성화되어 있어야 합니다.

WPA2/WP3 혼합 모드를 선택하면 WaveOS 가 자동으로 보호 관리를 enabled/optional 로 설정하여 이 옵션을 지원하지 않는 WPA2 피어와의 연결을 인증합니다.

V.2.5.6 OSU Server-Only Authenticated L2 Encryption Network (OSEN)

이 보안 모드는 Hotspot 2.0 r2 암호용으로 사용됩니다.

V.2.5.7 Mesh Secure Authentication of Equals (SAE)

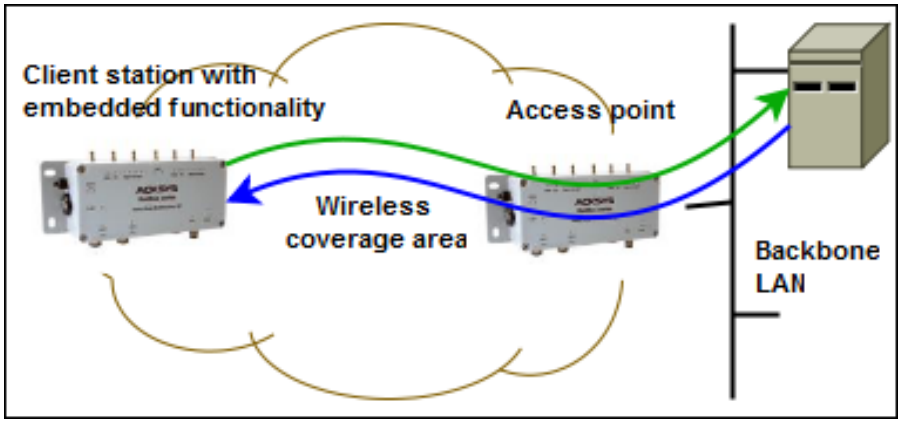
802.11s 메쉬 모드에서는 특별한 식별 역할이 있는 메쉬 노드가 없으며 모든 노드가 권한에서 동일한 것으로 간주됩니다. SAE 를 사용하는 경우 모든 노드에 사전 설정된 공통 키가 있어야 합니다. 노드가 동일한 메쉬의 다른 노드에 도달할 때마다 피어 노드가 키를 알고 있는지 확인합니다. 암호화는 WPA2 프로토콜 제품군(AES/CCMP)을 사용합니다.

암호 키는 8~63 자의 인쇄 가능한 ASCII 문자일 수 있습니다. 동일한 암호가 모든 메쉬 노드에 저장되어 있어야 합니다.

V.2.6 Wired to wireless bridging in infrastructure mode

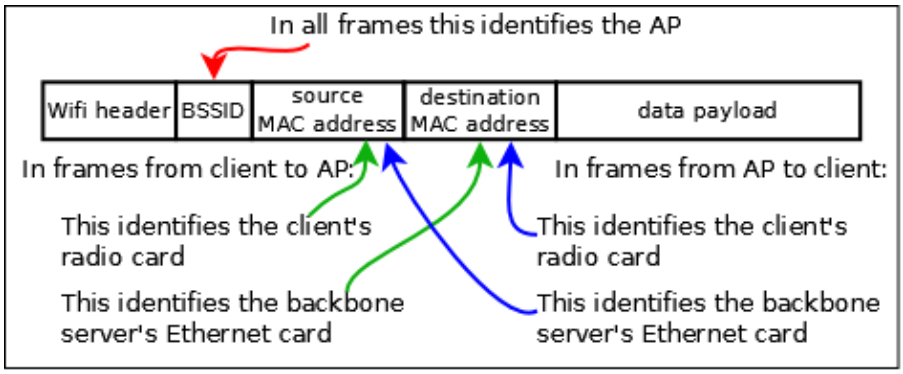
V.2.6.1 The problem

섹션 *V.2.1.1* 에 설명된 대로 802.11 표준에서 **infrastructure 클라이언트는 단일 MAC 주소를 가진 단일 장치여야** 합니다. AP 는 클라이언트 또는 유선 장치로 데이터를 전달합니다. 이 점에서 AP 는 이더넷 스위치와 유사합니다.



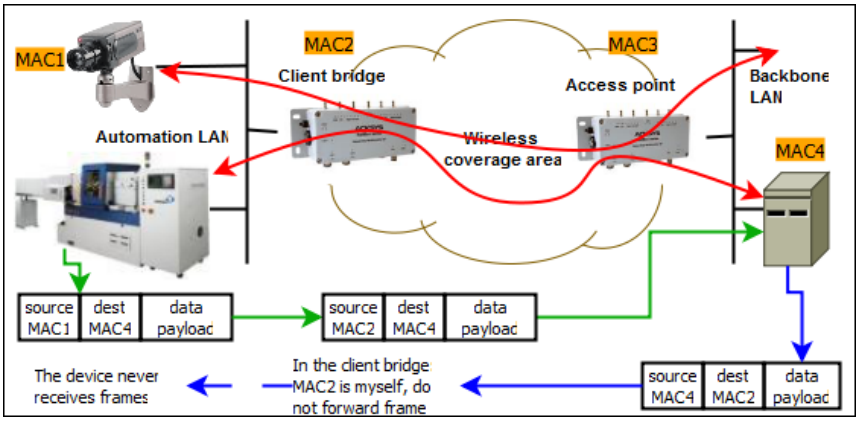
단일 무선 클라이언트로 여러 장치 연결

AP 가 데이터를 전달할 수 있도록 각 프레임에는 소스 MAC 및 대상 MAC 이 포함됩니다.



표준 infrastructure 데이터 프레임 (3 addresses)

클라이언트 스테이션을 사용하여 유선 네트워크를 AP 에 브리지할 때는 상황이 다릅니다. AP 에 단일 MAC 주소(무선 카드 주소)를 가진 단일 장치로 표시되는 것은 여러 유선 장치를 숨기는 것이며, 각 장치는 고유한 MAC 주소를 가지고 있습니다. AP 에 대한 연결 프로세스에 참여하지 않고 인증하지 않았기 때문에 AP 는 MAC 주소를 포함하는 프레임을 소스로 받아들이지 않습니다. 클라이언트가 소스 MAC 주소를 자체 MAC 주소로 변경하면 다른 문제가 나타납니다. 아래 그림을 참조하세요.



단일 무선 클라이언트를 사용하여 여러 장치를 연결하는 문제 예시

V.2.6.2 The solutions

이러한 한계를 극복하고 클라이언트 뒤에 있는 장치를 브리징할 수 있는 4 가지 방법이 있습니다.

- Routing. 클라이언트 측의 유선 LAN 을 IP 하위 네트워크로 하고 클라이언트를 라우터 또는 NAT 로 합니다. 이것은 매우 깨끗한 솔루션이지만 하위 네트워크를 관리해야 합니다. 엄밀히 말하면, 이것은 브리징(layer 2 networking)이 아니라 라우팅(layer 3 networking)입니다.
- Masquerading. 클라이언트가 유선 장치의 MAC 주소를 자체 MAC 주소와 "Level 2.5 NAT" 또는 "ARPNAT"로 변경할 수 있도록 합니다. **"client (infrastructure)"** 모드의 기본 동작입니다. 자세한 내용은 아래 섹션에서 *Masquerading (ARPNAT)* 설명합니다.
- Cloning. 클라이언트가 유선 장치의 MAC 주소를 사용하도록 합니다. 이것은 하나의 유선 장치로 제한됩니다.
- 보다 정교한 프레임 형식을 포함하는 **"client (infrastructure)"** 및 **"4 addresses format"** 브릿징 모드를 사용합니다. 802.11 표준은 이러한 종류의 문제를 해결하기 위해 "4-addresses" 프레임 형식을 제공하지만 완전히 명시하지는 않습니다. 따라서 이 모드는 클라이언트와 다른 공급업체의 AP 간에 항상 호환되는 것은 아닙니다. ACKSYS 제품은 물론 여러 Linux 기반 클라이언트 및 AP 에서도 아래 섹션 b 에 설명된 이 모드를 지원합니다.

  메쉬 모드(인프라 모드가 아님)도 브릿징을 허용합니다.

a. Masquerading (ARPNAT)

브릿징 문제에 대한 이 솔루션에서 클라이언트 브릿지는 장치의 MAC 주소를 IP 주소로 변환하거나 IP 주소에서 변환하는 테이블을 유지합니다.

AP 로 전송된 프레임에서 브릿지는 장치 소스 MAC 주소를 자체 MAC 주소로 교체하고 프레임의 MAC/IP 대응을 기억합니다.

프레임이 AP 에서 돌아올 때 대상 MAC 주소는 브릿지 주소입니다. 브릿지는 프레임에서 IP 주소를 찾고 해당 장치 MAC 주소를 찾아 프레임의 대상 MAC 에 넣어 유선 LAN 측에 전송합니다.

이 솔루션은 모든 처리가 클라이언트 측에서 이루어지기 때문에 모든 타사 AP 와 호환됩니다. 그러나 다음과 같은 특별한 행동을 유념해야 합니다.

1) 변환 테이블은 MAC/IP 변환만 처리합니다. 즉, **TCP/IP 프로토콜 제품군**(TCP, UDP, IP, ICMP, ARP, DHCP 등)만 브릿지할 수 있습니다.

2) 변환 테이블은 LAN 에서 Wi-Fi 로 프레임별로만 업데이트됩니다. 데이터를 전송하기 전에 브로드캐스트 ARP 요청/응답 교환이 이루어져야 하므로 이는 일반적으로 문제가 되지 않습니다. 그러나 클라이언트 브릿지의 전원이 꺼진 경우 다시 켜질 때 ARP 교환이 백본 측 장치에 의해 재시작될 필요는 없습니다. 그런 다음 브릿지가 AP 로부터 데이터 프레임을 수신하면 변환 테이블이 비어 프레임이 전달되지 않습니다. 이 경우 브릿지 자체가 프레임에 언급된 대상 IP 주소에 대한 ARP 를 시작하여 LAN 장치에서 테이블을 업데이트하는 응답을 트리거하여 다음 프레임이 전달될 수 있습니다.

3) **백본의 장비는 제품이 게이트웨이이고 대상 서브넷이 제품에 의해 직접 라우팅 가능한 경우를 제외하고 클라이언트 LAN 측에 위치한 IP 게이트웨이(라우터 또는 NAT)를 사용할 수 없습니다.** 그 이유는 AP 에서 수신한 프레임의 대상 IP 주소가 게이트웨이의 주소가 아니라 게이트웨이보다 더 멀리 있는 장비의 주소이기 때문입니다. 그러나 필요한 MAC 주소는 게이트웨이의 주소입니다. 따라서 주소 변환이 불가능합니다.

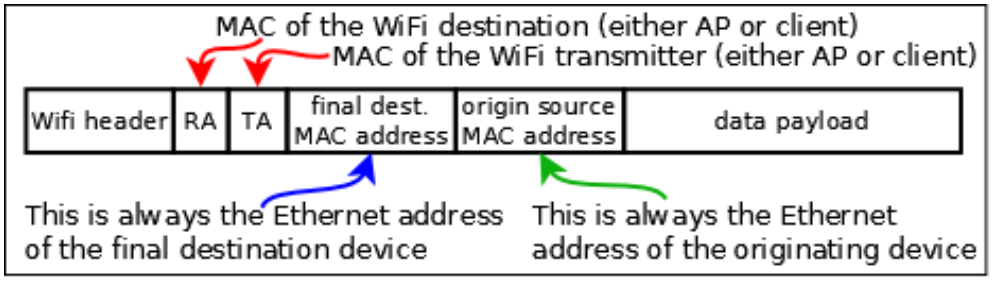
4) DHCP 는 IP 주소를 설정하는 데 사용되는 프로토콜입니다. 유선 장치 MAC 주소는 DHCP 프레임 헤더뿐만 아니라 데이터 페이로드에서도 전송됩니다. 주소 변환으로 인해 DHCP 서버에서 주소가 일치하지 않습니다. DHCP 서버 요구 사항을 충족하기 위해 브릿지는 자신을 DHCP 릴레이 에이전트로 통지하여 불일치를 해결합니다. 이렇게 하려면 **AP 쪽에 위치한 DHCP 서버가 유니캐스트 IP 패킷을 브릿지로 전송할 수 있어야 합니다.** 즉, 브릿지 뒤에 있는 장치에 IP 주소를 제공하기 전에 브릿지에 DHCP 서버에서 연결할 수 있는 IP 주소가 있어야 합니다.

5) ARP 는 MAC 주소를 검색하는 데 사용되는 프로토콜입니다. ARP 프레임은 헤더와 데이터 모두에 MAC 주소를 포함합니다. 이러한 프레임을 변환하기 위해 브릿지에서 특수 처리가 수행됩니다.
CISCO 및 기타 제품은 AP 에 "proxy ARP server"를 설정할 수 있습니다. 이는 AP 자체가 백본 장비를 대신하여 IP 주소를 MAC 주소로 변환한다는 것을 의미합니다. 브릿지된 LAN 의 모든 장치가 MAC 주소(브릿지 무선 카드 중 하나)는 같지만 IP 주소가 다른 것처럼 보이기 때문에 프록시 ARP 서버가 혼동될 수 있습니다. 해결책은 **AP 측에서 프록시 ARP 서버를 비활성화**하는 것입니다. CISCO 제품에서는 이를 "passive client mode"라고 합니다.

6) 보다 일반적으로 백본 측에서 실행되며 MAC 주소에 의존하여 장치를 식별하는 응용 프로그램 또는 프로토콜은 이 모드에서 문제가 발생합니다. 다행히도, 그러한 소프트웨어는 거의 사용되지 않습니다.

b. Infrastructure client using 4 addresses format (WDS)

클라이언트가 4 개의 주소 형식 브릿징 모드인 경우 Wi-Fi 및 LAN MAC 주소가 모두 표시되는 특수 프레임 헤더를 사용합니다. 이를 "4-addresses frame format"이라고 합니다. 무선 프레임에서 클라이언트 MAC 과 유선 장치 MAC 을 모두 전송함으로써 클라이언트는 Wi-Fi 프레임을 LAN 으로 올바르게 라우팅할 수 있으며 AP 는 인증된 클라이언트에 보내는 것을 알 수 있습니다.



4-addresses frame format

브릿징 문제에 대한 이 솔루션에서 클라이언트 브릿지와 AP 는 데이터와 이더넷 MAC 주소를 모두 Wi-Fi 프레임에 캡슐화하여 AP 와 클라이언트 Wi-Fi MAC 주소를 모두 추가합니다. 따라서 프레임이 Wi-Fi 대상에 도달할 수 있으므로 Wi-Fi 주소가 제거되고 원래 프레임이 변경되지 않은 상태로 검색됩니다. 두 가지 방법으로 동일한 프로세스가 수행됩니다.

이 솔루션은 layer 3 IP 주소와 독립적입니다.

1) 이 모드는 TCP/IP 이외의 프로토콜을 브릿지할 수 있습니다.
2) DHCP 및 ARP 프레임을 변경하지 않고 전송하여 프록시 ARP 또는 DHCP 서버와 같은 AP 측의 대부분의 검증 문제를 방지합니다.
3) AP 측 또는 브릿지 측에서 IP 게이트웨이를 사용할 수 있으며, 어느 쪽에서든 액세스할 수 있습니다.

그러나 이 솔루션은 지정되지 않은 802.11 기능에 의존하므로 동일한 브랜드 또는 범위의 제품 간 또는 AP 와 클라이언트가 호환되는 소프트웨어를 사용하는 것을 알고 있는 경우에만 사용해야 합니다.

4-addresses 프레임 형식은 로밍 기능과 호환되지 않습니다.

참고: 4-addresses 프레임 형식을 WDS(wireless distribution system, 무선 분배 시스템)라고 부르기도 합니다. 이 약어는 다양한 방법으로 사용할 수 있는 프레임 형식을 지정합니다. 특정 Wi-Fi 아키텍처(infrastructure 또는 mesh)를 지정하지 않습니다.

Configuration

액세스 포인트 역할(AP)은 항상 표준 ARPNAT 및 4-Addresses 클라이언트를 동시에 지원합니다. 클라이언트 브릿지는 ARPNAT 또는 4-addresses 형식으로 설정할 수 있습니다.

c. Cloning

ARPNAT 솔루션은 프레임을 무선 인터페이스에 브릿징할 때 유선 장치에서 MAC 주소 정보를 손실합니다. 대부분의 장치는 layer 3 의 IP 프로토콜을 사용하고 ARPNAT 이 IP 주소를 처리하기 때문에 MAC 주소 대체에 상관이 없습니다.

그러나 일부 장치는 layer 3 (Profinet 장비, LAN 비디오 카메라 등)에서 IP 를 사용하지 않으며 MAC 주소는 장비를 올바르게 식별할 수 있는 고유 ID 입니다.

복제 기능을 통해 제품은 무선 인터페이스의 소스 MAC 주소로 유선 장비의 MAC 주소를 사용할 수 있습니다. 복제된 주소는 연결, 인증 및 데이터 교환과 같은 모든 무선 트랜잭션에 사용됩니다. 무선 카드의 원래 MAC 주소는 무시됩니다.

무선 MAC 주소를 설정하기 위해 제품은 재부팅 후 첫 번째 수신 프레임 또는 구성된 MAC 주소를 복제합니다. 따라서 제품의 LAN 에 연결된 장치가 **하나만** 있어야 합니다.

IP 가 없는 장치를 다른 IP 장치와 혼합하는 경우 제품이 올바른 MAC 주소를 복제하도록 제품이 켜진 후 IP 가 없는 장치가 첫 번째 프레임을 전송하도록 해야 합니다. PROFINET 장비에서 이 문제를 방지하려면 "PROFINET cloning"를 사용해야 합니다. 이 경우 첫 번째 PROFINET 프레임 소스의 MAC 주소가 복제에 사용됩니다.

V.2.7 Fast roaming features

빠르게 이동하는 차량에 클라이언트 제품이 설치되어 있을 때 네트워크 연결을 유지하기 위해 일부 구성 매개 변수를 조정할 수 있습니다. fast roaming 기능은 4-addresses 형식과 호환되지 않으므로 STP/RSTP 와 호환되지 않습니다.

V.2.7.1 Mono-channel vs. multichannel roaming

클라이언트 역할은 한 채널에서만 AP 를 찾거나 여러 채널을 검색할 수 있습니다. 각각의 방법에는 장단점이 있습니다.

Mono-channel

모든 AP 는 무선 미디어를 놓고 경쟁하므로 모든 클라이언트와 AP 에 대해 사용 가능한 대역폭이 줄어듭니다. 그러나 클라이언트는 항상 AP 의 존재와 상태를 알고 있으며, 항상 현재 AP 와 통신할 수 있습니다. 또한 AP 중 하나가 선택한 채널의 간섭 소스 근처에 있으면 모든 AP 를 다른 채널로 전환해야 합니다.

Multi-channel

서로 무선 범위에 있는 AP 가 서로 다른 채널을 사용하도록 설정할 수 있습니다. 이런 식으로 그들은 공중 대역폭을 놓고 경쟁하지 않을 것입니다. 서로 너무 가까운 채널은 간섭할 수 있으므로 선택하지 마세요.

클라이언트는 선택한 각 채널을 차례대로 스캔해야 합니다. 이 경우 현재 연결된 AP 의 채널을 떠나 짧은 시간 동안 "off-channel"로 전환해야 합니다. 이 시간 동안에는 데이터를 교환할 수 없습니다. 그런 다음 데이터는 특정 제한에 따라 버퍼링됩니다. 이렇게 하면 클라이언트의 데이터 처리량이 줄어듭니다.

Configuration

Proactive roaming 기능을 활성화한 후 클라이언트에서 검색한 채널 목록을 조정해야 합니다. 하나 이상의 채널을 선택할 수 있습니다.

Proactive roaming 로밍이 활성화되지 않은 경우 국가에서 허용되는 모든 채널이 검색되므로 일치하는 AP 를 찾을 가능성은 최대화되지만 데이터 전송 속도는 느려집니다.

V.2.7.2 Proactive roaming vs. reactive roaming

Reactive

클라이언트가 더 이상 AP 와 통신할 수 없을 때 reactive roaming 이 발생합니다. 장애가 너무 많이 발생하면 클라이언트는 현재 AP 에서 연결을 끊고 새 AP 를 검색하기 시작합니다. 이 경우 구성할 항목이 없으므로 reactive roaming 이 기본 모드입니다. 이 모드에서는 데이터 전송 중에 채널 스캔(일명 "foreground scan"이라고도 함)이 수행되지 않으므로 데이터 전송에 사용할 수 있는 대역폭이 모두 유지되지만, 로밍

프로세스는 느리고(스캔이 끝날 때까지 기다려야 함) 이 시간 동안에는 데이터를 전송할 수 없습니다. 클라이언트가 AP 에 연결할 수 없을 때마다 reactive roaming 을 시작합니다.

Proactive

Proactive roaming 은 신호 레벨이 너무 낮아 많은 오류가 발생할 수 있기 전에 클라이언트가 다른 AP 를 검색하고 선택하고 전환한다는 것을 의미합니다. 적절한 매개 변수를 선택하면 데이터 처리량에 영향을 미치기 전에 한 AP 에서 다른 AP 로 변경이 이루어지며, 새 AP 가 충분한 무선 범위에 있으면 재연결 프로세스가 빨라집니다. 따라서 손실되는 데이터는 거의 없습니다.

Proactive roaming 을 활성화하려면 클라이언트는 이미 연결되어 있고 잠재적으로 데이터를 교환하는 동안 AP 를 검색해야 합니다. 이 프로세스를 "background scan"이라고 하며 데이터 처리량을 다소 줄입니다.

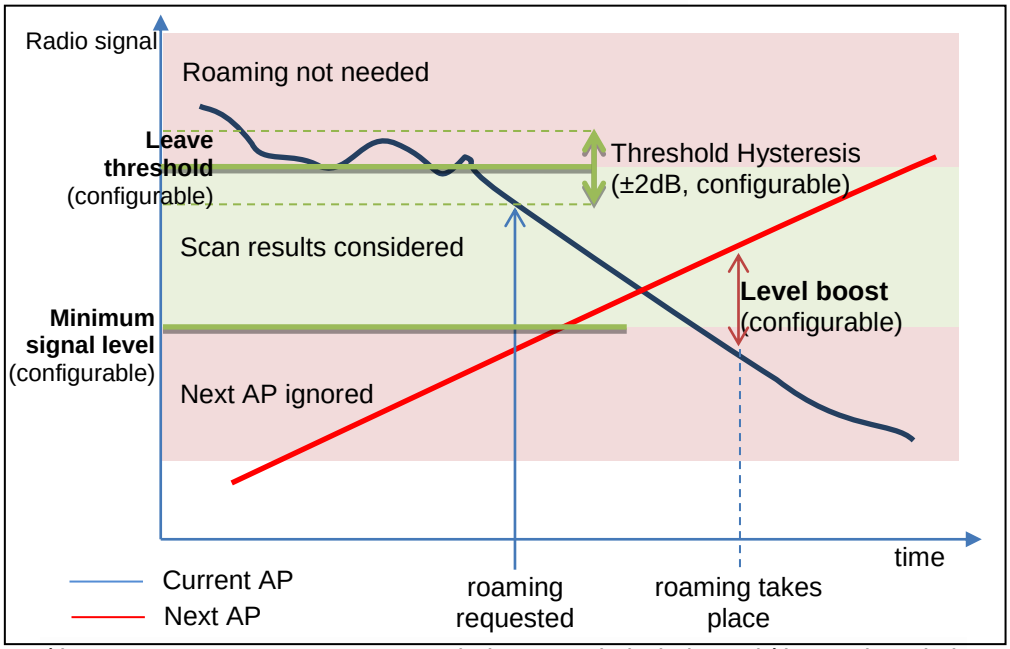
Configuration

링크 품질이 처리량 요구 사항에 불충분하다고 간주되는 무선 신호 레벨 임계값을 구성해야 합니다.

그러나 무선 신호 수신 수준은 안정적인 측정이 아닙니다. 예측하지 못한 많은 매개 변수(이동 물체, 습도 등)에 따라 달라집니다. AP 신호가 임계값에 가까울 때, 한계치 근처를 왔다 갔다 할 수 있습니다. 이러한 재연결 기간 동안에는 데이터를 전송할 수 없으므로 AP 에서 AP 로 너무 자주 전환하지 않는 것이 좋습니다. 이를 설명하기 위해, 한계를 넘으면 "required level boost"(default: 6dB)라고 하는 이력(hysteresis)이 적용됩니다.

마지막으로, 임계값을 초과하더라도 신호세기가 더 좋지 않은 AP 와 다시 연결하려는 것은 아니지만, 현재 연결되어 있는 신호세기가 약한 AP 를 잃는 것도 원하지 않습니다. "required level boost" 구성 매개 변수는 재연결을 시작하기 위해 얼마나 개선된 새 AP 를 원하는지 지정합니다.

이 그림에는 다양한 파라미터의 효과가 나와 있습니다.



참고: Threshold Hysteresis 는 버전 2.2.7 이상에서 구성할 수 있습니다. 이전 펌웨어에서는 "leave threshold"를 "minimum level"이라고 합니다.

V.2.7.3 What happens when the current AP fails

유선 LAN 과 달리 Wi-Fi 미디어는 폭, 간섭원 또는 장애물에 제한되지 않습니다. 따라서 현장 내 물체 이동, 기후 변화, AP 전원 차단 등으로 인해 현재 연결된 AP 가 클라이언트의 "sight"에서 갑자기 사라질 수 있습니다.

클라이언트는 AP 를 사용할 수 있는지 확인하는 네 가지 방법이 있습니다.

- AP 로 부터 비콘이 정기적으로 수신되고 있는지 확인하고,
- 데이터를 수신하고 있는지,
- 전송된 데이터에 대해 확인을 수신하는지,
- 전송된 시도에 대한 응답을 수신하는지 입니다.

오류가 오래 지속되지 않으면 데이터가 재전송되고 일부 누락된 비콘이 허용됩니다. 반대로, 신호 또는 데이터 ACK 가 오랫동안 없으면 연결이 끊어집니다. 이전에 탐지된 다른 AP 가 여전히 주변에 있으면 클라이언트는 해당 AP 로 전환하고, 그렇지 않으면 클라이언트는 reactive roaming 을 시작합니다. Long-lived 장애와 short-lived 장애를 적절히 구분하기 위해 이 프로세스는 구성에 따라 proactive roaming 보다 더 느리게 반응합니다.

Configuration
클라이언트 측에서 로밍 프로세스를 트리거하는 누락된 비콘의 수를 구성할 수 있습니다. 지연은 AP 에 구성된 비콘 주파수에 따라 달라집니다. Wi-Fi 는 한두 개의 프레임을 잃어버리는 경우가 매우 흔하며, 누락된 비콘 수는 3 이하로 설정해서는 안 된다는 점을 기억하시기 바랍니다.

AP 측에서 비콘 간격을 설정할 수 있습니다. 간격이 작을수록 장애는 더 빠르게 감지되지만, 비콘은 허용된 가장 낮은 비트 전송 속도로 전송되고 데이터 프레임보다 더 많은 대역폭을 소비합니다.

V.2.7.4 Scanning

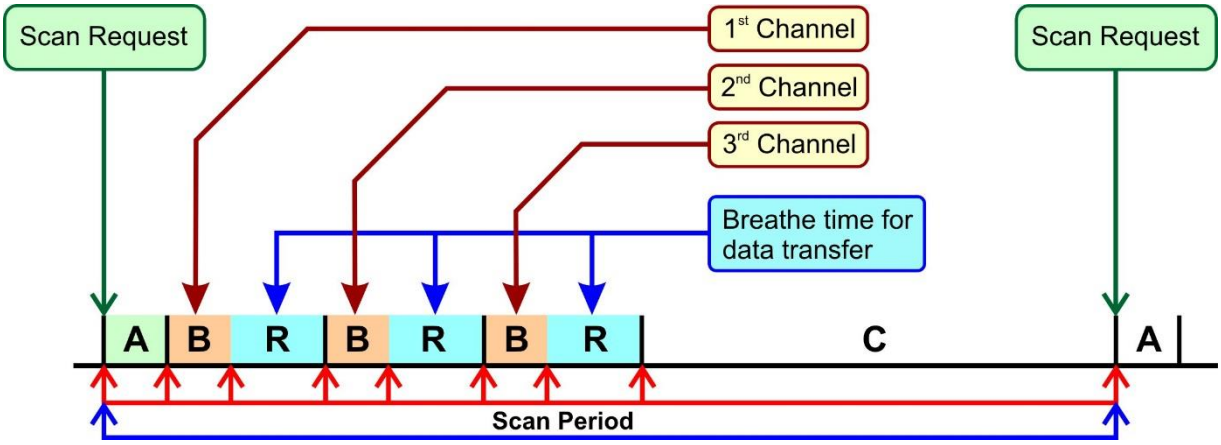
스캐닝은 클라이언트 스테이션이 AP 중 하나와 연결하기 위해 주변의 AP 를 찾는 데 사용하는 프로세스입니다. 스캐닝이 주기적으로 수행됩니다. 각 기간 동안 클라이언트는 구성된 스캔 채널로 연속적으로 전환하고 브로드캐스트 "probe request" 프레임을 보낸 후 응답을 기다립니다.

프로브 요청에는 다른 데이터 중 SSID 가 포함되어 있습니다. 이 SSID 를 제공할 수 있는 AP 가 응답합니다. 응답이 수신되는 신호 품질은 최상의 AP 를 선택하는 데 사용됩니다.

스캔한 채널이 현재 AP 의 채널이 아닌 경우 클라이언트는 "off-channel"로 간주되며 이 시간 동안 데이터를 전송하거나 수신할 수 없습니다. 데이터는 버퍼링됩니다. AP 에 수신할 수 없음을 알리기 위해 클라이언트는 오프 채널로 가기 전에 AP 에 "power save mode" 표시를 전송하여 AP 가 그 동안 프레임을 버퍼링할 수 있도록 합니다. 너무 많은 검색 채널을 구성하면 처리량이 손실되거나 데이터가 손실됩니다. 버퍼링된 데이터가 넘치기 충분한 시간을 허용하기 위해 두 검색 기간 사이의 지연을 구성할 수 있습니다.

Configuration
두 가지 스캔 파라미터는 스캔 채널 목록과 스캔 간 지연입니다. 경고합니다! 이 지연은 스캔 주기가 아니라, 스캔 주기가 늘어납니다. 백그라운드 스캔 예시 참조(C 파라미터).

참고: 클라이언트가 AP 에 연결되어 있지 않은 경우(클라이언트 재시작 후 또는 현재 AP 가 갑자기 사라진 경우), 교환할 데이터가 없으므로 대기 시간 "R"이 0 으로 단축되어 스캔 주기가 약간 빨라집니다.

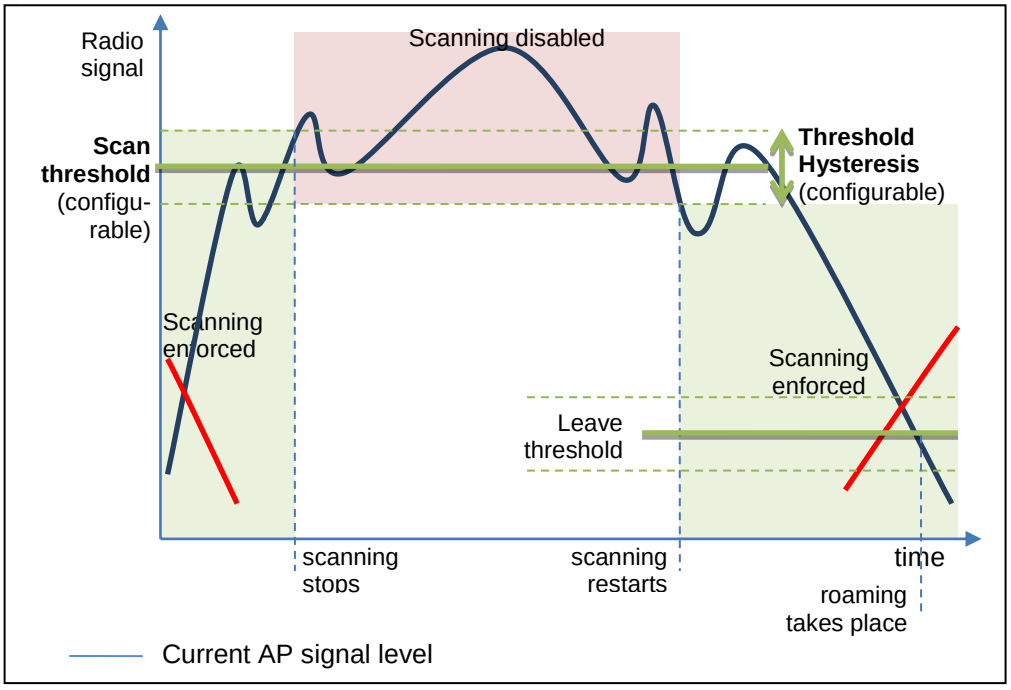


A: Initialization = a few ms
B: Channel scan = 56ms
C: Padding = configurable by steps of 4 ms
R: Breathe time = 200ms
(C 는 웹 인터페이스에서 두 개의 연속된 검색 주기 사이의 지연)
Reactive (foreground) 스캔 사이클에서 'R' 지연이 제거되므로 클라이언트가 AP 에 연결되어 있지 않은 동안에는 지연 시간이 단축됩니다.
참고: 'B' 지연은 버전 2.4.3 이상에서 구성할 수 있습니다. 다음 섹션을 참조하세요.

스캐닝 자체는 일반적으로 무조건 수행됩니다. 신호 레벨이 양호할 때 추가 처리량을 얻으려면 "scan threshold"을 구성할 수 있습니다. 이 파라미터는 로밍이 필요하지 않다고 추정하는 신호 레벨을 설정합니다. "scan threshold"을 0 으로 설정하면 이 기능이 비활성화됩니다(기본값).

설정된 경우, 스캔 임계값은 현재 AP 에서 수신한 신호세기와 비교됩니다. 신호세기가 임계값보다 크면 다음 검색 기간에 검색 프로세스가 중지됩니다. 수신된 신호세기가 임계값보다 낮으면 스캔 프로세스가 다시 시작됩니다.

수신되는 신호세기로 인해 임계값 주변에서 빠르게 변화하는 진동 효과를 방지하기 위해 hysteresis (이력)가 구현됩니다. 이 값은 "leave threshold"에 사용되는 히스테리시스와 동일합니다.



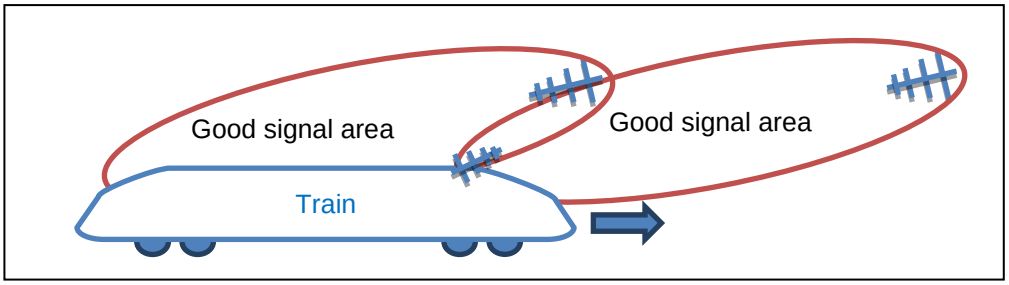
참조: Scan threshold 는 버전 2.2.7 이상에서 구현 가능합니다.

V.2.7.5 Advanced Roaming settings

기본 로밍 설정이 충분하지 않은 경우가 있습니다. 여기에는 지향성 안테나 처리, 평균 신호 감쇠율 미세 조정 및 스캔에 사용되는 대역폭 미세 조정이 포함됩니다.

a. Directional AP handling

Wi-Fi 클라이언트가 열차에 내장되어 있고 지향성 안테나가 지붕에 고정되어 있는 경우(그림 참조), 신호 레벨이 높으면 AP 가 곧 지향성 안테나의 다른 쪽에 위치하게 되므로 수신 레벨이 낮은 다른 AP 로 로밍하기에 좋은 시기입니다.



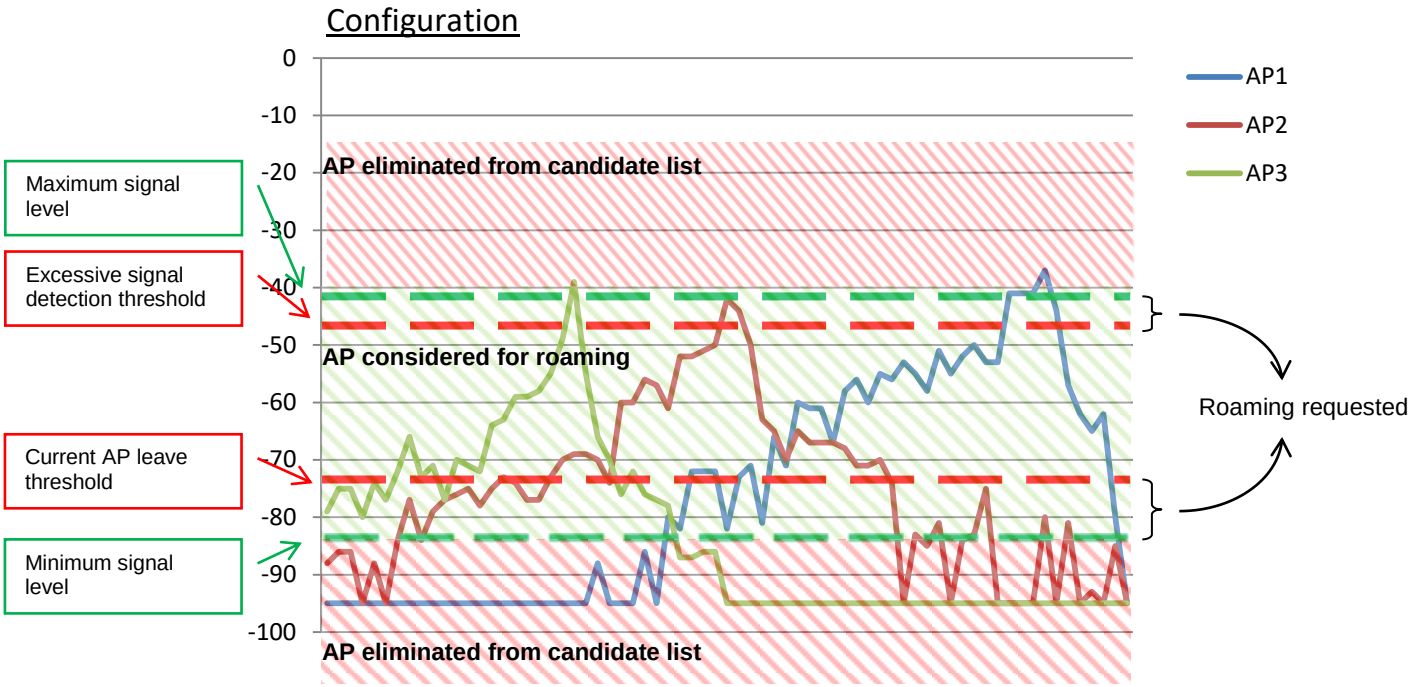
신호가 양호하더라도 열차가 이동하기 때문에 곧 현재 AP 와 연결이 끊기게 됩니다.

이 경우 AP 가 높은 신호 레벨로 표시될 때 클라이언트는 다음 몇 초 안에 연결을 잃을 수 있습니다.

Excessive signal detection threshold 파라미터는 레벨이 너무 높을 때 현재 AP 를 동적으로 떠나도록 결정합니다. **Maximum signal level** 파라미터는 다음 연결 후보로 높은 신호 레벨을 가진 AP 의 정적 제거를 유도합니다. 검사는 각 스캔 후에 수행됩니다.

안정성이 좋으면 다음 파라미터에 몇 가지 제약이 따릅니다.

- 두 파라미터를 모두 사용할 경우 임계값 레벨을 최대 레벨보다 낮게(강력하지 않음) 설정해야 합니다.
- 이러한 파라미터는 높은 신호 레벨 AP 를 관리하는 또 다른 방법인 **Current AP scan threshold** 와 호환되지 않습니다.
- 과도한 임계값은 **Threshold hysteresis** 매개 변수도 사용합니다.
- 연결 후 첫 번째 스캔 중에는 방금 연결된 현재 AP 와 연결이 끊어지지 않게 하기 위해서 최대 레벨을 확인하지 않습니다.



스캔 프로세스가 끝나면 제품이 후보 AP 를 선택합니다. 후보 AP 는 로밍이 요청될 경우 로밍할 AP 입니다.

마지막 연결 이후 **Minimum roaming interval** 이 경과하기 전에는 로밍이 발생하지 않습니다. 신호 품질이 거의 동일한 여러 AP 가 수신되는 영역에서 이 매개 변수는 약간의 신호 변동으로 인한 잦은 로밍을 방지하는 데 도움이 됩니다.

No-return delay 가 경과하기 전에 최근에 남겨진 AP 에서는 로밍이 발생하지 않습니다. 이 매개 변수는 신호 바운스로 인해 이전 AP 가 일시적으로 더 신호가 좋게 나타나더라도 AP 의 순차적인 로밍을 적용하는 데 도움이 됩니다.

b. Smoothing factor (RSSI decay rate)

다양한 파라미터는 이벤트를 트리거하기 위한 것입니다.

- scan threshold
- leave threshold
- excessive signal detection threshold

임계값 교차 검출을 위해, 이 모든 파라미터는 현재 AP 의 RSSI 와 비교됩니다.

현재 AP 의 RSSI 는 현재 AP 로부터 수신된 가장 최근의 비콘에 대해 계산된 지수 이동 평균으로 정의됩니다. 따라서 현재 신호 레벨이 아니라 평균과 비교됩니다. 비콘 신호 레벨은 안정적인 비트 전송률과 신호세기 레벨로 전송되고 동일한 수신 감도로 수신되므로 비콘 신호 레벨만 사용됩니다.

계산된 RSSI 평균의 이전 비콘에 비해 최근 비콘을 더 선호하기 위해 이동 평균의 지수 계수를 설정할 수 있습니다. 이 요인을 "RSSI smoothing factor"이라고 합니다. 계산에서 가장 최근의 비콘에 연결된 백분율을 나타냅니다.

Smoothing factor 는 1/16th 단계의 0 과 1 사이의 값입니다. 예를 들어 3/16 값은 이전 비콘의 신호세기 레벨이 다음과 같이 사용됨을 의미합니다.

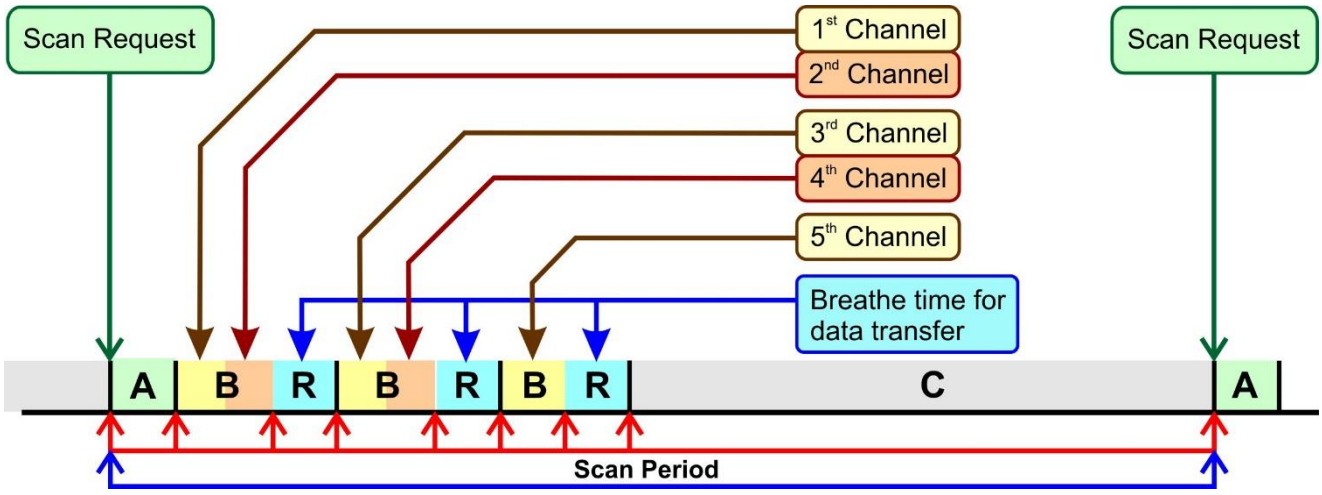
- 가장 최근 비콘, $\frac{3}{16} = 18.75\%$ of the signal value,
- 두 번째 비콘, $\frac{3}{16} \times \frac{13}{16} = 15\%$,
- 세 번째 비콘, $\frac{3}{16} \times \frac{13}{16} \times \frac{13}{16} = 12\%$,
- 계속 진행...

Configuration
브라우저 인터페이스에서 요인은 마지막 비콘에 연결된 백분율로 표시됩니다. 극단적인 경우 100% (또는 16/16th) 를 사용한다는 것은 가장 최근의 신호만 비교에 사용된다는 것을 의미합니다.

c. Off-channel configuration

Off-channel 프로브 요청/응답 시퀀스의 지속 시간을 단축할 수 있습니다("scan period" 사진의 'B' 파라미터). 이를 통해 대용량 데이터 흐름이 AP 에 진입하고 있지만 다른 채널을 스캔 중이기 때문에 클라이언트에 전달할 수 없고 AP 에 버퍼가 부족한 상황을 해결할 수 있습니다. 'B' 지연은 (B1) 전환 지연(매우 빠름), (B2) 동기화 지연(프로브가 채널의 다른 송신기와 충돌하지 않도록 보장), (B3) 프로브 요청 전송(사용 가능한 최저 속도로), (B4) 응답 대기 지연의 합계입니다.

또한 스캐너는 현재 채널로 돌아가지 않고 채널 간에 전환할 수 있습니다. 다음 그림에서는 5 개의 채널을 스캔해야 합니다. 하나의 스캔 시퀀스 'B' 동안 파라미터 "Maximum time off-channel" 또는 현재 AP 비콘 간격이 모두 사용될 때까지 데이터 채널로 돌아가지 않고 지연(B2)-(B3)-(B4)이 반복됩니다. 이 동작은 전환 지연(B1)의 일부를 절약하고 즉각적인 처리량을 희생하여 평균 처리량을 향상시킵니다.



Configuration
항목(B2)은 "Off channel adaptation delay"로, (B4)는 "Per channel probe response delay"로 구성할 수 있으며, "Maximum time off-channel" 파라미터로 하나의 'B' 스캔 시퀀스의 전체 오프 채널 지속 시간을 정의할 수 있습니다. 이 모든 파라미터는 ±4ms 로 정의됩니다.

Default values
기본 파라미터에서는 그림에 표시된 것처럼 스캔 시퀀스당 2 개의 채널을 프로빙할 수 있습니다. 기본 "maximum time off-channel"은 125ms 이지만, 대부분의 AP 는 100ms 의 비콘 주기를 가지고 있기 때문에 이 파라미터는 일반적으로 100ms 로 자동 감소됩니다. 다른 두 기본 파라미터는 30ms 로 설정되지만 실제로는 28ms 로 내림됩니다.

채널 목록에 DFS 채널이 포함된 경우, "Maximum Time off-channel"에 표시된 지연은 DFS 의 경우 "채널별 프로브 응답 지연"의 최소값을 고려해야 합니다.

For example, if we scan channel 36 (not DFS) and 52 (DFS):
"Maximum time off-channel"은 "Offchannel adaptation delay" +108 이상이어야 합니다. 이 파라미터를 비워 두면 배경에 125 가 표시되지만 125 + " Offchannel adaptation delay"으로 자동 조정됩니다.
"Off channel adaptation delay" = 30(28 로 내림), "Per channel probe response" = 30(28 로 내림), "Maximum time off-channel" = 150 의 경우, 검색 주기는 채널 36(약 56ms)에서 작동 채널(200ms), 채널 52(약 138ms)로 돌아간 다음 "Delay between two successive scan cycles"으로 다시 시작합니다. 최대 지연 시간인 150ms 는 절대 최대값으로 사용되지 않으며, 최대 서비스 중단 시간은 138ms 입니다.
138 보다 조금 큰 값을 설정하면 라우터의 CPU 사용을 최대치로 끌어 올릴 수 있습니다. 예를 들어 멀티캐스트 라우팅, 암호화된 VPN 등을 동시에 수행하는 경우입니다. 실제로 이 예에서는 최대 138 + 56 + (56-4) = 246ms 까지 스캔 주기가 동일합니다.

2 개 채널을 연속으로 스캔하려면 "Offchannel adaptation delay" = 30(28 로 내림), "Per channel probe response delay" = 30(28 로 내림), "Maximum time off-channel" = 200(즉, 138 + 56 + 6ms 마진)을 설정할 수 있습니다. 스캔 주기는 다음과 같습니다. 채널 36(약 56ms) 다음 직접 채널 52(약 138ms) "Delay between two successive scan cycles"를 표시하고 다시 시작합니다.

V.2.7.6 Authentication speed up

연결 작업에서 AP 와 클라이언트는 여러 프레임을 교환해야 합니다. 프레임 수는 보안 수준에 따라 증가합니다.

WPA 프로토콜에서 PMK(Pairwise Master Key)는 데이터를 암호화하는 데 사용될 임시 키를 생성하는 데 사용됩니다.

- WPA/WPA2-PSK: PMK 는 Pre-Shared Key 에서 파생됩니다.
- WPA/WPA2-EAP: PMK 는 Radius server 에 의해 배포됩니다.

보안 수준에 따른 프레임 수

Security policy	Number of frame
Open (without security)	4 frames - 4 Authentication frames
WEP	4 frames - 4 Authentication frames
WPA/WPA2-PSK	8 frames - 4 Authentication frames - 4 Key exchange frames
WPA/WPA2-EAP (with radius server)	> 8 frames - 4 Authentication frames - Several radius authentication frames - 4 key exchange frames

"4 Authentication frames"은 802.11 프로토콜에 의해 필수입니다.

임시 키를 교환하려면 "4 Key exchange frames"이 필요합니다.

Wi-Fi 클라이언트를 Radius 서버로 인증하려면 "several radius authentication frames" 이 필요합니다. 프레임 수는 인증방법에 따라 다릅니다.

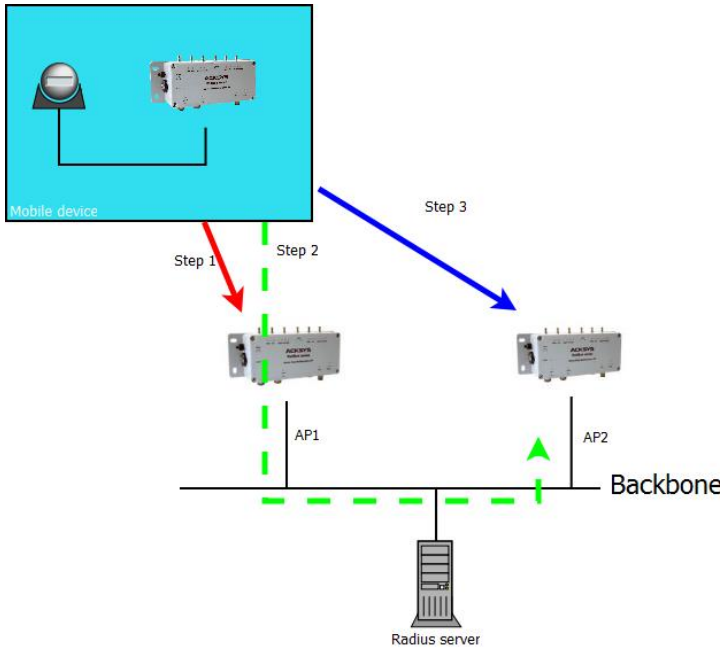
a. Pre-authentication / PMK caching

이 기능을 사용하면 PSK 모드처럼 WPA/WPA2-EAP 정책을 사용한 인증이 8 프레임으로 줄어듭니다.

AP 비콘은 사전 인증/PMK 캐싱 기능을 제공합니다. 고객은 지원되는 기능을 선택하여 사용할 수 있습니다.

제품은 두 가지 기능을 모두 지원하며 로밍이 활성화된 경우 자동으로 사용합니다.

아래 그림은 사전 인증 프로세스의 3 단계를 보여줍니다.



Step 1: Wi-Fi 클라이언트가 처음으로 AP1 과 연결됩니다. 이 단계에서 클라이언트는 전체 인증을 수행합니다. Radius 서버는 PMK 를 AP1 과 Wi-Fi 클라이언트 모두에 전송합니다. AP1 및 Wi-Fi 클라이언트는 PMK 를 로컬 캐시에 저장합니다.

이 단계가 끝나면 Wi-Fi 클라이언트가 AP1 에 연결됩니다.

Step 2: Wi-Fi 클라이언트는 스캔 프로세스로 AP2 를 검색합니다. AP1 의 보안 링크를 사용하여 AP2 의 사전 인증을 처리합니다. 이 단계에서 Radius 서버는 PMK 를 AP2 및 Wi-Fi 클라이언트로 전송합니다. 둘 다 PMK 를 로컬 캐시에 저장합니다.

이 단계가 끝나면 Wi-Fi 클라이언트는 AP1 에 계속 연결됩니다.

Step 3: Wi-Fi 클라이언트가 AP2 로 로밍합니다. AP2 와 Wi-Fi 클라이언트 모두 로컬 캐시의 PMK 가 올바른지 확인합니다.

PMK 가 올바르면 AP2 는 Wi-Fi 클라이언트와 WPA 핸드셰이크를 시작합니다.

PMK 가 올바르지 않으면 AP 가 Radius 인증을 시작합니다.

이 단계가 끝나면 Wi-Fi 클라이언트가 AP2 에 연결됩니다.

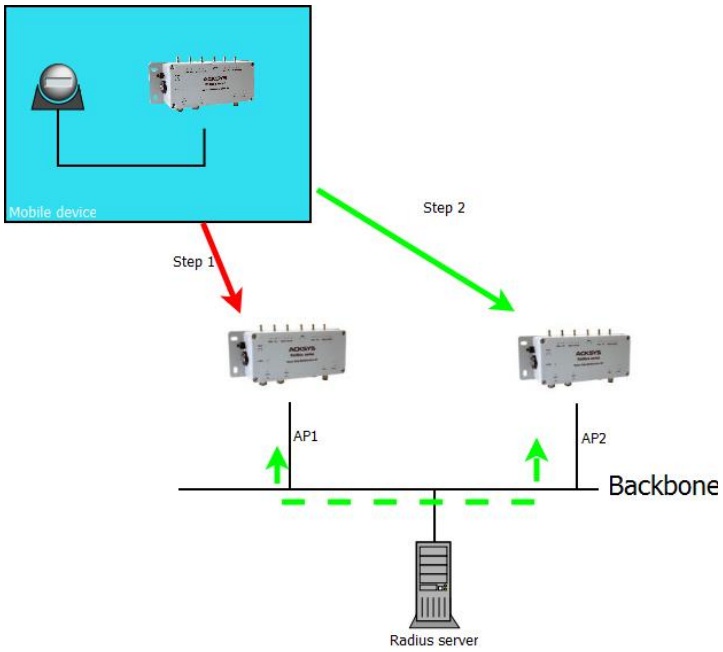
b. Fast Transition Support (802.11r)

이 기능을 사용하면 모든 WPA/WPA2 정책에 대한 인증이 4 프레임으로 줄어듭니다(오픈 모드와 같이).

802.11r 에서는 임시 키가 백본(back bone)을 통해 서로 다른 AP 간에 분산됩니다.

제품은 클라이언트 모드에서만 802.11r 을 지원합니다.

아래 그림은 802.11r 인증 단계를 보여줍니다.



Step 1: Wi-Fi 클라이언트는 AP1 로 전체 인증을 수행합니다. AP1 은 PMK 및 임시 키를 저장합니다. 이 전체 인증 프로세스는 Wi-Fi 클라이언트가 다음 단계를 위해 저장할 데이터를 생성합니다.

Step 2: Wi-Fi 클라이언트는 AP2 를 로밍하고 인증 요청에서 이전 단계에서 저장된 데이터를 사용합니다. 이 데이터를 통해 AP2 는 이 Wi-Fi 클라이언트가 AP1 로 성공적으로 인증되었음을 알 수 있습니다. AP2 는 (back bone 사용) AP1 에서 임시 키를 직접 요청합니다. AP1 이 AP2 에 필요한 모든 키를 제공하면 Wi-Fi 클라이언트는 AP2 와의 연결 프로세스를 완료할 수 있습니다. 다른 경우에는 Wi-Fi 클라이언트가 AP2 로 전체 인증을 시작합니다.

V.2.7.7 Connect before break

앞서 살펴본 바와 같이, 로밍 프로세스는 두 개의 무선 카드를 사용하는 경우에도 Wi-Fi 클라이언트가 다음 AP 에 다시 연결할 수 있기 전에 항상 현재 AP 에서 물리적으로 연결을 끊는다는 것을 의미합니다. 이는 클라이언트가 네트워크에서 완전히 연결이 끊기는 시간이 반드시 존재함을 의미하며, 이 기간 동안 패킷 전송을 중지하기 위해 시행된 메커니즘은 패킷 손실이 없음을 완전히 보장할 수 없습니다.

핸드오버 중 패킷 손실이 중요한 특정 애플리케이션의 요구를 충족하기 위해 Acksys 는 "Connect Before Break"라고 하는 특정 로밍 모드를 개발했습니다. 이 모드를 사용하면 패킷 손실률을 획기적으로 줄일 수 있으며 데이터 처리량도 상당히 줄일 수 있습니다.

Connect Before Break 의 작동원리는 'ghost' WiFi 클라이언트 사용을 기반으로 하여 주변 액세스 포인트를 감지 (스캐닝)하는 기능을 수행합니다. 이 'ghost' WiFi 클라이언트는 데이터 교환을 하는 대신 동일한 액세스 포인트에 연결하여 나중에 연결될 액세스 포인트와 병렬로 작동하는 실제로 효과적인 클라이언트의 클론입니다. 따라서 언제든지 완벽하게 동일한 두 개의 클라이언트가 있습니다. 하나는 AP 로 트래픽을 제공하는 **active client** 이고 다른 하나는 호환되는 액세스 포인트를 검색하여 환경을 분석하는 **passive client** 입니다.

현재 AP 의 신호 레벨이 로밍 임계값 아래로 떨어지면, **passive client** 가 로밍 기준을 충족하는 새로운 AP 를 감지하는 즉시, 현재 AP 를 떠나 이 새로운 AP 에 대한 연결 프로세스를 시작합니다. 이 시간 동안 **active client** 는 현재 AP 에 연결된 상태를 유지하고 데이터 패킷을 계속 교환할 수 있습니다. **passive client** 가 새로운 AP 와의 연결을 확립했을 때, 전체 네트워크에 핸드오버 요청한 후, ARP 교환을 통해, 그리고 현재 AP 와 **active client** 의 버퍼가 비어 있는지 확인한 후에만 현재 AP 와 연결이 끊어집니다.

active client 의 연결이 끊어지면 두 클라이언트가 역할을 바꿉니다. **passive client** 가 **active client** 가 되고 그 반대의 경우도 마찬가지입니다.

제품이 NAT 라우터로 구성되지 않은 경우 Connect Before Break 에는 4 addresses format (WDS)이 필요합니다. 이것은 제품이 연결할 수 있는 액세스 포인트가 WaveOS Acksys 제품만 될 수 있음을 의미합니다.

또한 Connect Before Break 은 단일 라디오 카드에서 작동할 수 있지만, 이 경우 하나의 채널만 사용할 수 있습니다.

Connect before Break 구현 시 어플리케이션 노트 *APNUS0016 Connect Before Break* 를 참조하세요.

V.2.7.8 Connect Before Break with Predictive Linear Handover

Predictive Linear Handover (PLH)는 Connect Before Break 로밍의 특정 작동 모드입니다. PLH 알고리즘은 모바일 장비가 새로운 AP 앞에서 연속적인 선형으로 이동하는 경우에 적합하도록 설계되었습니다. 다음과 같은 경우에 적합합니다.

- 선형 경로로 이동하는 차량 (전차, 기차, 일부 버스 노선)
- 경로에 일정한 간격으로 배치된 액세스 포인트
- 어떤 AP 도 경로와 가까운 두 섹터를 커버하지 않는 경우 (블록 주위를 도는 버스의 경우는 적합하지 않음).
- 안테나의 배열은 한 방향을 선호 (방향성이 있거나 차량이 한 방향으로 전파를 방해함)

목표는 안테나가 한 방향을 가리키는 "back lobes"를 피하는 것입니다. PLH 는 일련의 AP 안테나에 점차 접근하거나 점차 멀어지는 상황을 위해 고안되었습니다.

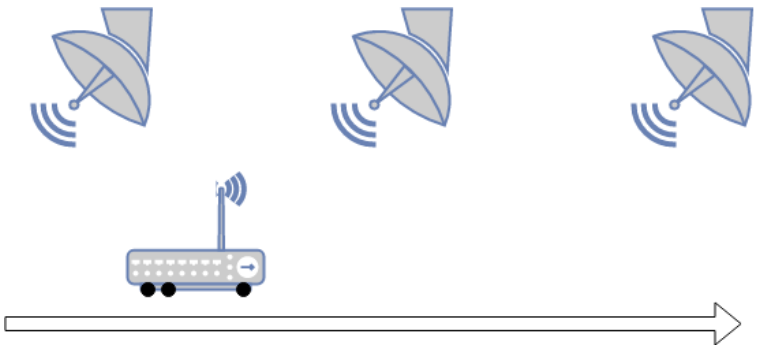
알고리즘에 대한 자세한 내용

세 가지 기본 규칙

1. 신호 레벨이 사전 정의된 범위[min, max]에 있고 증가 또는 감소 중인 경우 AP 는 "후보"(다음 연결로 사용)입니다.
2. 데이터 링크(active AP)에 사용되는 AP 는 사전 정의된 임계값 범위를 벗어나 범위 내에 후보 AP 가 있는 경우에만 삭제됩니다.
3. Active AP 가 사전 정의된 "긴급" 임계값 미만으로 떨어지고 후보 AP 가 없는 경우 비상 상태가 발생합니다(단, 상의해야 함).

WiFi 클라이언트(PLH 를 실행하는)를 차량의 앞쪽에 배치하는지 뒷쪽에 배치하는지에 따라 2 가지 경우가 있습니다.

FRONT PLH

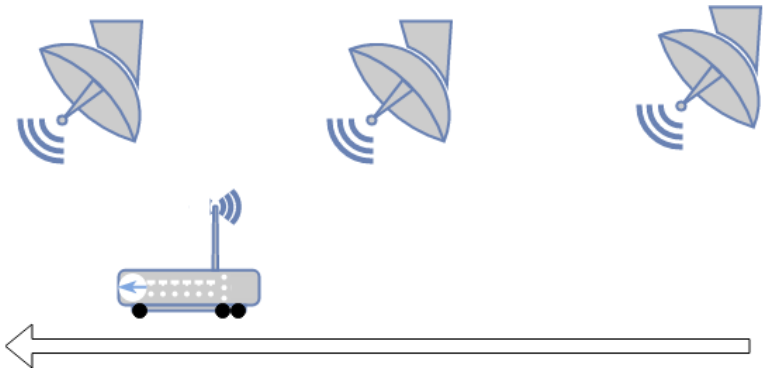


이 경우는 신호 레벨이 감소하는 AP 를 거부하는 것입니다. 그것들은 차량에 의해 지나가게 되어 있습니다. 더 정확히 말하면, PLH 는 AP 가 계속 보이는 한 시간 제한 없이 신호 레벨이 이전 값 중 하나보다 낮은 AP 를 거부합니다.

또한 신호가 너무 높은 AP 는 매우 가깝고 오버런이 임박했다는 가정 하에 거부됩니다.

Rear PLH (REAR)

클라이언트의 안테나가 이동의 반대 방향을 가리키고 AP 가 이동 방향을 가리키고 있다고 가정합니다.



그 경우는 신호가 증가하는 AP 를 거부하는 것입니다. 더 정확히 말하면, PLH 는 AP 가 계속 보이는 한 시간 제한 없이 신호가 이전 값 중 하나보다 큰 AP 를 거부합니다.

또한 신호가 너무 높은 AP 는 매우 가깝고 잠재적으로 여전히 후방 로브에 있다는 가정 하에 거부됩니다.

"Emergency" 상태

다음은 비상 상태를 조건화하는 테스트 목록입니다.

- 활성 인터페이스가 아직 없습니다.
- 활성 인터페이스가 연결되어 있지 않습니다.
- 활성 인터페이스의 신호레벨이 비상 임계값보다 낮습니다.
- 후방 로브 상태에 있습니다. FRONT= 활성 AP 에 거의 도달했거나 초과했습니다. REAR= 활성 AP 가 다가오고 있습니다. (일반적으로 이러한 경우 다른 무선으로 전환했어야 합니다. 그렇지 않은 경우, 다른 라디오의 연결이 원활하지 않습니다.)

비상 상태는 SNMP OID *statusRoamingUrgent* 를 사용하여 참조할 수 있습니다.

V.2.8 WLAN Association Controller

WAC(WLAN Association Controller) 기능은 액세스 포인트에서 로드 밸런싱, 밴드 스티어링 및 클라이언트 로밍 제어를 담당하는 WaveOS 모듈입니다.

V.2.8.1 Load balancing

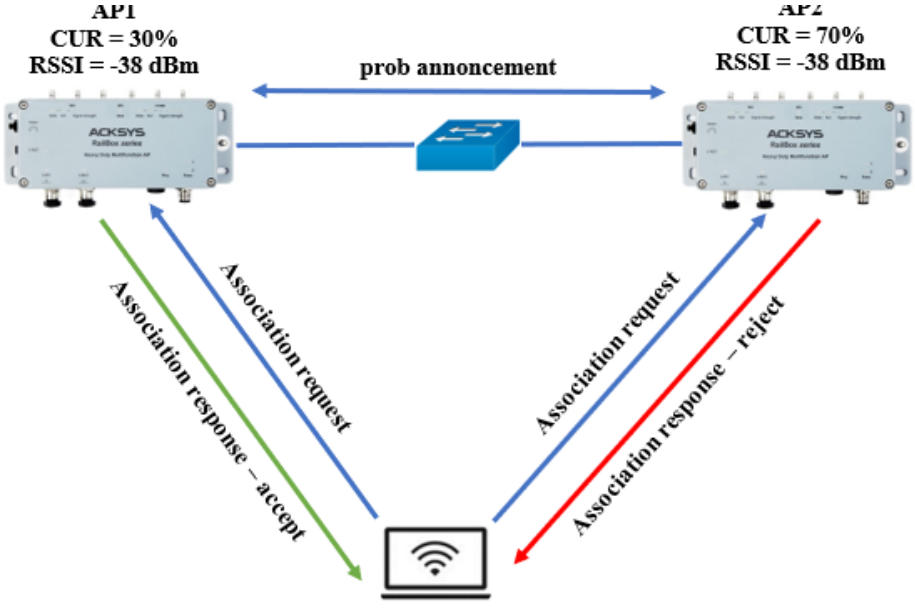
로드 밸런싱을 사용하면 두 개 이상의 AP 와 WLAN 내에서 가능한 AP 간에 STA 를 공평하게 연결하는 방식으로 WiFi Stations 또는 STA 연결을 제어할 수 있습니다.

각 액세스 포인트는 최적의 AP 인지 여부를 판단하고, 최적의 AP 인 경우 프로브 요청에 응답하고 연결 요청을 수락합니다. AP 가 최상의 AP 가 아닐 경우 프로브 요청에 응답하지 않고 연결 요청을 거부합니다.

WAC 는 RSSI 와 함께 CUR(Channel Usage Rate) 표시기를 사용하여 최상의 AP 를 선택합니다. AP 의 CUR 는 AP 당 허용되는 최대 STA 수에 대한 관련 STA 수의 비율을 나타냅니다. 따라서 각 AP 는 CUR 와 RSSI 를 기반으로 STA 에 대한 연결 점수를 계산합니다. AP 는 STA 당 관련 STA 수와 RSSI 를 교환하고, 새로운 STA 를 수락해야 하는 AP 를 분산 스키마에서 결정합니다.

각 프로브 요청 시 AP 의 WAC 데몬은 멀티캐스트 "프로브 공지" 메시지를 멀티캐스트 그룹에 속한 AP 로 보냅니다. 프로브 공지사항에는 AP 의 MAC 주소, 연결된 STA 의 수 및 STA 의 RSSI 가 포함됩니다. 프로브 공지 수신 시, 수신 AP 는 다음 다이어그램과 같이 특정 STA 에 대한 최상의 AP 를 업데이트합니다.

마지막으로, 스테이션은 가장 높은 점수로 AP 에 연결됩니다.

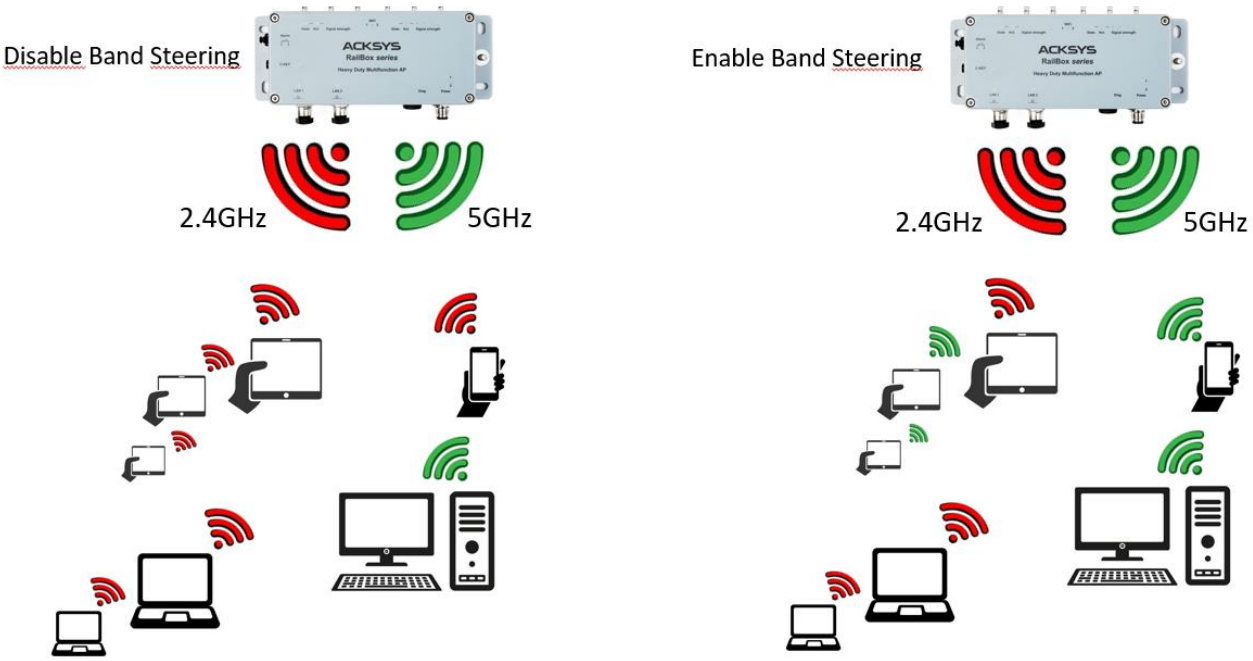


V.2.8.2 Band steering

Band steering 을 통해 듀얼 대역이 가능한 STA 는 AP 의 덜 혼잡한 대역(일반적으로 5GHz)으로 이동할 수 있습니다.

Wi-Fi 장치의 "Dual-band"의 발전으로, 이제 장치는 2.4GHz 또는 5GHz Wi-Fi 네트워크에 연결할 수 있습니다. 그러나 대부분의 소비자 라우터 및 많은 액세스 지점에 연결할 때 클라이언트 장치가 연결할 대역을 결정합니다. 클라이언트 장치가 연결되도록 허용하면 2.4GHz WiFi 네트워크 및 5GHz 대역에서 Wi-Fi 장치가 매우 불균형하게 분산될 수 있습니다.

밴드 스티어링을 활성화하면 듀얼 밴드 장치가 5GHz WiFi 네트워크에 연결됩니다. 5GHz 지원 장치를 해당 대역에 자동으로 전달함으로써 두 대역의 전반적인 연결 품질을 낮추고 개선할 것입니다.



V.2.8.3 Roaming control

로드 밸런싱 및 밴드 스티어링 외에도 ACKSYS AP 는 관련 스테이션별 RSSI 를 모니터링하도록 구성할 수 있습니다. 로밍 제어는 RSSI 가 허용 임계값 미만으로 떨어질 경우 스테이션 연결을 해제하는 것으로 구성됩니다. 따라서 이 임계값보다 낮은 RSSI 와의 연결 요청은 거부됩니다. 그러나 엄격한 모드를 사용하지 않는 한 동일한 클라이언트의 두 번째 연결 요청은 무조건 수락됩니다.

V.2.9 Hotspot 2.0

WaveOS 는 *Passpoint* 로 알려진 Hotspot 2.0 을 지원합니다. 이것은 공용 Wi-Fi 핫스팟에 더 쉽고 안전하게 연결할 수 있도록 설계된 새로운 무선 표준입니다.

Hotspot 2.0 네트워크의 목표는 Wi-Fi 네트워크를 위한 셀룰러 유형의 "roaming"을 제공하는 것입니다. 전 세계를 여행할 때 장치가 사용 가능한 공개 핫스팟에 자동으로 투명하게 연결됩니다. 여기에는 몇 가지 이점이 있습니다.

- 공용 핫스팟에 대한 액세스 용이성과 보안성을 향상시킵니다.
- 네트워크 공급자는 함께 그룹화하고 다른 공급자와 제휴할 수 있는 옵션이 있습니다.
- 현재 많은 공용 Wi-Fi 액세스 지점이 열려 있고 안전하지 않은 Wi-Fi 네트워크인 Hotspot 2.0 네트워크에는 엔터프라이즈급 WPA2 암호화 기능이 필요합니다.

WiFi 클라이언트는 Acksys 액세스 포인트의 ID, 위치 및 네트워크 유형에 대한 일반적인 정보를 수신할 수 있습니다. 또한 클라이언트는 네트워크에서 사용 가능한 IP 주소 유형(IPv4 또는 IPv6), 지원되는 로밍 파트너 및 인증 방법에 대한 정보를 액세스 포인트로부터 요청하고 액세스 포인트 정보 요소에서 이 정보를 받을 수 있습니다.

V.2.9.1 Generic Advertisement Service (GAS) Queries

OI(Organization Identifier)는 서비스 공급자가 IEEE 등록 기관에 등록할 때 할당되는 고유 식별자입니다. Acksys 액세스 포인트는 서비스 공급자의 OI 를 비콘에 포함하고 클라이언트의 답변을 조사할 수 있습니다. 클라이언트가 AP 의 OI 를 인식하는 경우 이 서비스 공급자와 관련된 보안 자격 증명을 사용하여 이 AP 와 연결을 시도합니다.

클라이언트가 AP 의 OI 를 인식하지 못하면 클라이언트가 AP 에 GAS(Generic Advertisement Service) 요청을 전송하여 연결 전에 네트워크에 대한 추가 정보를 요청할 수 있습니다.

V.2.9.2 Access Network Query Protocol (ANQP) elements

ANQP 정보 요소(IE)는 AP 에서 클라이언트로 전송하여 AP 네트워크 및 서비스 공급자를 식별할 수 있는 추가 데이터입니다. 클라이언트가 GAS 요청을 통해 이 정보를 요청하면 핫스팟 AP 는 후속 IE 에 대한 지원을 나타내는 ANQP 기능 목록을 GAS 초기 프레임에 전송합니다. 클라이언트가 특정 IE 에 대한 요청으로 응답하면 AP 는 구성된 ANQP IE 정보가 포함된 GAS 응답 프레임을 전송합니다.

- 장소 이름: 플레이스 이름 IE 는 플레이스 그룹 및 플레이스 유형을 정의합니다.
- Domain Name: 이 IE 는 AP 의 도메인 이름을 지정합니다.
- 네트워크 인증 유형: 네트워크에 ASRA(Additional Step Required for Access)가 있는 경우 이 프로파일은 핫스팟 네트워크에서 사용하는 인증 유형을 정의합니다.
- 로밍 컨소시엄 목록: 로밍 컨소시엄의 IE 에는 네트워크와 서비스 공급자를 식별하는 정보가 포함되어 있으며, 보안 자격 증명을 사용하여 이 요소를 전송하는 AP 를 인증할 수 있습니다.
- IP 주소 가용성: 이 IE 는 클라이언트에 AP 핫스팟과 연결된 후 이러한 클라이언트에 할당할 수 있는 버전 및 IP 주소 유형에 대한 정보를 제공합니다.

- NAI 영역: AP 의 NAI 영역 프로파일은 AP 를 사용하여 연결할 수 있는 NAI(Network Access Identifier) 도메인과 NAI 도메인이 인증에 사용하는 방법을 식별하고 설명합니다.
- 3GPP 셀룰러 네트워크 데이터: 셀룰러 운영자와 로밍 관계를 갖는 핫스팟을 위한 3 세대 셀룰러 파트너십 프로젝트(3GPP) 네트워크에 대한 정보를 정의합니다.
- 연결 기능: IE ANQP 로 보낼 핫스팟 프로토콜 및 포트 기능을 정의합니다.
- 작동 클래스: 이 프로필을 사용하여 핫스팟이 작동할 수 있는 채널을 정의합니다.
- 운영자 이름: 연산자를 식별하고 위치에 대한 정보를 제공할 수 있는 자유 텍스트 필드입니다.
- WAN 메트릭: 핫스팟 클라이언트에 링크 상태, 인터넷에 대한 WAN 링크의 용량 및 속도와 같은 액세스 네트워크 특성에 대한 정보를 제공합니다.

V.2.9.3 Passpoint Profile Types

통과점을 쉽게 구성할 수 있도록 구성은 별도로 저장되며 무선 인터페이스와는 거의 독립적입니다. 구성은 여러 개의 통과점 구성 프로파일로 구성되며, 각 통과점 구성 프로파일의 옵션은 동일한 목적을 공유합니다.

Passpoint 구성 프로필은 두 가지 유형으로 요약할 수 있습니다. HS20 프로파일과 ANQP 프로파일입니다. HS20 프로파일은 핫스팟 2.0 기능을 구성하고 ANQP 프로파일은 ANQP 802.11u 기능을 구성합니다.

다양한 구성 프로파일에 대한 설명은 Setup(설정) 메뉴 섹션 (*Passpoint Config Profiles*). 에서 찾을 수 있습니다. 이러한 서로 다른 프로필을 작성하는 데 필요한 정보는 서비스 공급자가 제공해야 합니다.

Profil	Description
HS20 Operator Friendly Name	이 프로필을 사용하여 장치에서 보내는 이름을 정의합니다.
HS20 Connection Capability	이 프로파일을 사용하여 핫스팟 프로토콜 및 포트 기능을 지정합니다.
HS20 WAN Metrics	이 프로파일을 사용하여 핫스팟의 WAN 상태 및 링크 메트릭을 지정합니다.
HS20 Operating Class	이 프로필을 사용하여 핫스팟이 작동할 수 있는 채널을 지정합니다.
HS20 OSU Provider, Passpoint Icon	이 프로파일을 사용하여 OSU 공급자를 정의합니다.
ANQP Venue	GAS 요청 응답에서 IE ANQP 에 보낼 위치 그룹 및 위치 유형을 지정하려면 이 프로필을 사용합니다.
ANQP Roaming Consortium	로밍 컨소시엄의 IE 에는 네트워크와 서비스 공급자를 식별하는 정보가 포함되어 있으며, 보안 자격 증명을 사용하여 이 요소를 전송하는 AP 를 인증할 수 있습니다.

ANQP Network Authentication Type	네트워크에 ASRA(Additional Step Required for Access)가 있는 경우 이 프로필은 핫스팟 네트워크에서 사용하는 인증 유형을 정의합니다.
ANQP IP Address Availability	액세스 포인트 네트워크에서 사용할 수 있는 IPv4 및 IPv6 주소 유형을 지정하려면 이 프로필을 사용합니다.
ANQP Domain Name	이 프로파일을 사용하여 핫스팟 운영자의 도메인 이름을 지정합니다.
ANQP 3GPP Cell Net	이 프로파일을 사용하여 셀룰러 운영자와 로밍 관계를 가진 액세스 포인트가 사용하는 3 세대 파트너십 프로젝트(3GPP) 셀룰러 네트워크에 대한 우선 순위 정보를 설정합니다.
ANQP NAI Realm	AP 의 NAI 도메인 프로파일은 AP 를 사용하여 액세스할 수 있는 NAI(Network Access Identifier) 도메인을 식별하고 설명하며 NAI 도메인이 인증에 사용하는 방법을 설명합니다.
ANQP Override Element	임의 값을 가진 추가 ANQP 요소는 내용을 페이로드 16 진수로 지정하여 정의할 수 있습니다. 이러한 값은 구성 매개 변수의 상위 계층에서 지정될 수 있는 ANQP 요소의 내용을 재정의합니다.

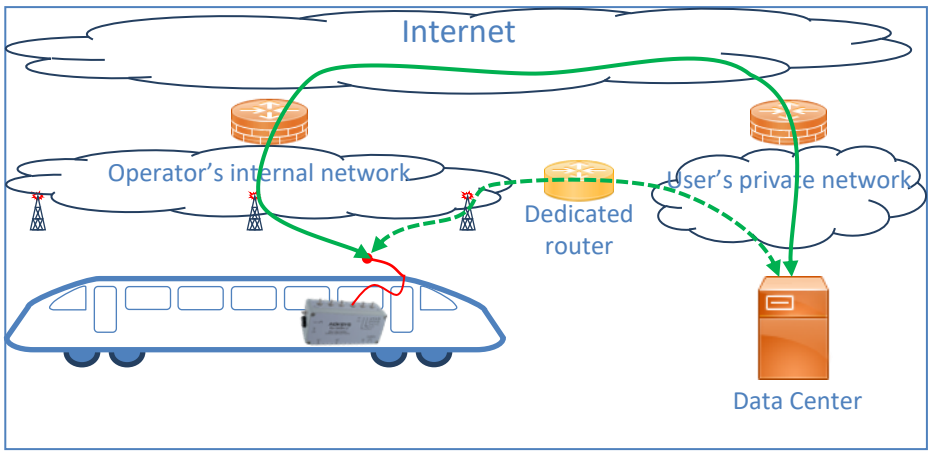
V.3 Cellular interface option

V.3.1 Networking model

활성화된 경우 셀룰러 인터페이스는 선택한 SIM 의 지정된 공급자에 자동으로 연결됩니다. 운영자는 셀룰러 인터페이스에 IP 주소를 할당해야 합니다. 따라서, 셀룰러 인터페이스는 특정 IP 주소, VLANS, 레이어 2 브리지에 포함, 무선 채널 선택, 무선 프로토콜 등과 같은 링크 계층 세부 사항으로 직접 구성할 수 없습니다.

연결 후 제품은 운영자의 개인 네트워크에 액세스한 다음 원격 IP 네트워크로 다시 라우팅됩니다.

- 일반 개인 계정을 사용할 때 원격 IP 네트워크는 인터넷입니다. 인터넷 액세스는 일반적으로 운영자가 관리하는 NAT 게이트웨이를 통해 제공되므로 제품의 셀룰러 인터페이스를 원격 노드에서 직접 호출할 수 없습니다.
- 회사 차원의 계정을 사용할 때 운영자는 전용 링크 또는 VPN 을 통해 회사의 데이터 센터 시설에 대한 액세스를 직접 라우팅할 수 있습니다.



셀룰러 통신을 사용할 때는 다음 두 가지 중요한 기능을 처리해야 합니다.

- 개인 정보 보호: 제품과 데이터 센터 간의 통신은 첫 번째 단계에서 공기(매우 가벼운 개인 정보 보호)를 통해 그리고 두 번째 단계에서는 인터넷(일반적인 이슈)을 통해 이루어집니다. 허용 가능한 개인 정보를 얻으려면 제품과 데이터 센터 간에 암호화 VPN 을 설정하는 것이 좋습니다(운영자가 경로의 일부에서 개인 정보를 제공하는 경우에도).
- 로컬 장치에 대한 액세스 제공: 제품의 LAN 에 있는 다른 장치가 제품을 인터넷 또는 데이터 센터에 대한 라우터로 사용하려면 운영자의 중간 NAT 에 대응해야 합니다. 실제로 운영자의 NAT 은 원격 소스에서 수신한 로컬 장치 주소를 라우팅하는 방법을 알지 못합니다. 이 문제를 해결하려면 제품의 셀룰러(공용) 인터페이스에 NAT 을 설정해야 합니다.

V.3.2 Configuration

설치 시 보안을 강화하기 위해 셀룰러 인터페이스는 기본적으로 비활성화되어 있으므로 반드시 활성화해야 합니다. 대부분의 로우 레벨 구성은 SIM 모듈에서 제공합니다.

그 외에 NAT 또는 VPN 을 설정해야 하는지 결정해야 합니다.

VPN 이 없으면 이더넷 또는 Wi-Fi 링크의 장치가 인터넷에 액세스할 수 있도록 하기 위해 NAT 이 필요할 수 있습니다. VPN 을 사용하는 경우 NAT 이 있는지 여부는 VPN 의 로컬 끝과 원격 끝 모두에서 사용하는 주소 지정 방식에 따라 달라집니다.

추가 방화벽 규칙을 설정하기 위해 셀룰러 인터페이스를 네트워크 영역에 배치할 수 있습니다.

일반적으로 연결이 설정되면 셀룰러 인터페이스가 기본 경로가 되고 구성된 DNS 서버는 운영자가 제공한 서버로 대체됩니다. 이러한 동작은 일반적으로 필수적이지만 사용하지 않도록 설정할 수 있습니다.

V.4 Satellite positioning (GNSS) option

셀룰러 인터페이스와 함께 제공되는 GNSS 구성 요소는 GPS(미국), 갈릴레오(유럽), GLONASS(러시아), 베이두(중국)의 네 가지 기존 위성 시스템을 자동으로 사용합니다.

위치를 획득("고정")하려면 위성으로부터 좋은 수신이 필요합니다. GNSS 안테나는 막힘이 없는 하늘을 향해 꽂혀 있어야 합니다. 다시 시작하거나 위치를 잃은 후 최소 4 개의 위성이 GNSS 안테나를 볼 수 있는 경우 장치를 복구하는 데 약 30 초가 걸립니다.

다음 네 가지 방법으로 현재 위치를 검색할 수 있습니다.

- 웹 인터페이스 "Device Information" 페이지에 표시합니다.
- Acksys SNMP MIB(service Status 섹션)에서 읽는 중입니다. 위치 데이터는 2 초마다 자동으로 새로 고쳐지며 positionValid 또는 gnssAllPositions 중 하나를 읽을 때 새로 고쳐집니다. GNSS 장치는 **초당 한 번만** 위치를 획득하므로 더 높은 주파수에서 값을 읽을 필요가 없습니다.
- 활성화된 경우 시스템 로그를 주기적으로 읽습니다.
- 활성화된 경우 내장된 "gpsd" 서버에 연결합니다. 사용된 프로토콜에 대한 자세한 내용 참조 *http://www.catb.org/gpsd/gpsd_json.html*.

시스템 로그에 표시되는 문자열과 'qnssAllPositions' SNMP OID 를 통해 얻은 문자열의 형식은 동일합니다. 다음 순서로 열로 구분된 일련의 값으로 구성됩니다.

Valid flag	위치가 정의되지 않은 경우 1, 다음 데이터가 유효한 경우 2
Dimension	위도/경사만 알려진 경우 2, 고도가 유효한 경우 3, 위치를 알 수 없는 경우 0 또는 1
Date	마지막 수정 날짜 YYMMDD(년, 월, 일) 또는 유효하지 않은 경우 비어 있음
Time	마지막 수정 시간. 시간이 가능한 경우: HHMMSS.ddd (hour, minute, second, dot, milliseconds). 시간을 사용할 수 없는 경우: 제품에 알려진 sssssssss (1/1/1970 이후 최대 시간). 항상 1000000 보다 큼
Latitude	적도에서 ±DD.dddddd degrees, 소수점 6 자리, 마이너스 기호는 적도 남쪽을 의미
Longitude	Greenwich 에서 ±DD.dddddd degrees, 소수점 6 자리, 마이너스 기호는 Greenwich 서쪽을 의미
Altitude	HHH.hhhhhh 위의 높이는 미터 단위로 표시된 레벨을 의미
Speed	kkk.vvvvvv 수평 변위 속도 (Km/h), 소수점 6 자리
Direction	True north 에서 DDD.dddddd degrees, 소수점 6 자리, DDD 범위는 0~359

위 목록은 끝에 추가하여 확장될 수 있습니다.

예:

2:2:180131:095959.000:48.817204:2.007647:0.000000:0.000000

V.5 High availability features

V.5.1 Router redundancy with VRRP

Wi-Fi 링크를 사용하여 지상과 통신하는 운송 시스템(기차, 트램웨이 등)과 같은 네트워크에서 중복 라우팅을 통해 이중 경로, 주 및 보조 경로를 설정하고 주 경로의 고장을 감지하여 보조 경로를 활성화할 수 있습니다. 주 경로가 정상적으로 작동하는 동안 보조 경로는 중요하지 않은 데이터를 전송하거나 정적 로드 밸런싱을 구현하는 데에도 사용될 수 있습니다.

제품이 IP 라우터 모드에서 사용되는 경우 보조 제품이 백업 라우터 역할을 하도록 설정할 수 있습니다. 이 기능은 VRRP 프로토콜을 사용하여 지정된 시간에 트래픽을 라우팅하는 제품을 결정합니다. 일반적으로 "master"(또는 "primary") 라우터가 사용되며 마스터가 실패할 경우 "slave"(또는 "backup", 또는 "secondary") 라우터가 사용됩니다.

주변 장치에서는 게이트웨이 주소가 하나만 설정됩니다. 가용성에 따라 이 게이트웨이 IP 주소는 마스터 또는 슬레이브 라우터를 주소 지정합니다. 그들은 함께 "virtual router"라고 불리는 클러스터를 형성합니다.

또한 두 개의 게이트웨이 주소 A 와 B 에 해당하는 두 개의 가상 라우터를 설정하고 한 라우터를 A 의 마스터로 지정하고 B 의 백업으로 지정한 후 다른 라우터를 B 의 마스터로 설정하고 A 의 백업으로 설정하면 고가용성 load-sharing 을 제공할 수 있습니다.

감지된 장애에는 이더넷 케이블 렌치, 이더넷 커플러 번아웃, 무선 카드 장애, 원격 액세스 포인트 장애(클라이언트 모드) 및 마스터의 전원 장애가 포함됩니다. 두 원격 노드 간의 네트워크 손상(예: 제품에 간접적으로 연결된 두 원격 스위치)이 감지되지 않으므로 나머지 네트워크도 중복되어야 합니다.

감지된 장애는 백업 라우터를 다음과 같이 만듭니다.

- 기존 연결을 이어받습니다.
- IP 게이트웨이의 MAC 주소가 변경되었음을 원격 디바이스에 알립니다.

마스터에서 기본값이 고정되어 있으면 기본값이 다시 시작되어 백업 라우터에서 라우팅을 다시 가져옵니다.

페일오버를 지원하기 위해 세 가지 서비스가 협력합니다. VRRP 는 오류를 감지하고 주소 지정을 전환합니다. 연결 추적은 주 라우터와 백업 라우터 간의 TCP 연결을 동기화합니다. 이벤트 관리자는 오류를 보고합니다.

V.5.1.1 VRRP

VRRP 서비스는 하드웨어 장애 감지 및 경로 전환을 처리합니다. 약간의 변경으로 RFC3768 을 구현합니다. VRRP 프로토콜은 간단합니다. VRRP 마스터는 VRRP 백업을 억제하는 주기적인 알림 프레임을 멀티캐스트합니다. 백업은 알림 수신을 중지하면 ARP 를 사용하여 네트워크에 게이트웨이 IP 주소의 새 위치를 알립니다. 그런 다음 새로운 "master"로서 주기적으로 "advertisement" 프레임을 보냅니다.

마스터가 복구되면 알림 프레임을 통해 백업과 협상하고 실제 마스터가 라우팅 기능을 다시 가져옵니다.

따라서 마스터 라우터에서 VRRP 서비스는 하드웨어 장애를 감지하고 슬레이브에서는 마스터의 상태도 모니터링합니다.

백업은 마스터의 존재를 탐지할 수 있지만 마스터는 비활성 백업의 존재를 탐지할 수 없습니다. 네트워크 하드웨어가 절반만 작동하는 경우(예: 마스터의 이더넷 링크는 프레임을 수신할 수 있지만 전송할 수 없음) 시스템이 동일한 주소에 두 개의 활성 라우터를 가질 수 있기 때문에(마스터에서 기본값이 표시되지 않고 마스터로부터 알림을 수신하지 않으므로 백업이 활성화됨) 매우 중요합니다. 이에 대한 해결책은 인스턴스 그룹화입니다.

백업 실패와 테이크오버 사이의 기간은 다음과 같은 여러 매개 변수에 따라 달라집니다.

- Time to detect the failure (이더넷 링크 다운의 경우 1~2 초, Wi-Fi 장애의 경우 로밍 매개 변수에 따라 다름)
- Advertisement interval. 백업은 인계받기 전에 최대 4 배의 간격을 기다립니다.
- 백업에서 연결을 다시 로드하는 시간(수 ms)입니다.
- 스위치와 호스트가 게이트웨이 IP 주소에 연결된 새 MAC 주소를 알 수 있도록 "gratuitous ARP" 프레임을 네트워크에 브로드캐스트할 시간입니다.
- 트래픽 부하. 네트워크 트래픽이 많으면 테이크오버 속도가 현저히 느려질 수 있습니다.

VRRP Instances

VRRP 인스턴스는 하나의 라우터에서 하나의 게이트웨이 IP 주소를 관리하는 독립체입니다. 하나의 서브넷에 바인딩되어 있습니다.

이 정의에 따르면 VRRP 인스턴스는 다음과 같은 속성을 가집니다.

- ID — 마스터 및 백업에 공통인 가상 주소 식별 번호입니다. IP 와 연결된 ID 는 서브넷에서 고유해야 합니다(VRRP 를 사용하는 고유한 게이트웨이가 여러 개인 경우).
- Virtual IP address — 인스턴스에서 관리하는 주소입니다. 디바이스에 할당된 다른 IP 주소(정적 또는 DHCP 제공)와 달라야 합니다.
- Netmask — 가상 IP 주소에 대한 라우팅 정보입니다.
- Network interface — 가상 IP 주소가 바인딩된 물리적(이더넷...) 또는 논리적(브릿지...) 서브넷입니다.

인스턴스가 속한 그룹에는 우선 순위(백업 상태), 마스터 알림 기간(마스터 상태) 및 초기 상태와 같은 몇 가지 속성이 상속됩니다.

네트워크 인터페이스는 여러 IP 주소에 바인딩될 수 있습니다. 일반적으로 하나는 정적이며 관리 목적(라우터를 구성하고 모니터링하는 데)으로 사용되며 다른 하나는 호스트에서 패킷을 다른 서브넷으로 라우팅하는 데 사용되는 가상 게이트웨이 주소입니다.

VRRP Groups

IP 라우터는 여러 서브넷(LANs)을 상호 연결합니다. 연결된 모든 서브넷의 원격 호스트가 라우터 사용을 중지하도록 하려면 한 서브넷의 장애를 다른 서브넷에도 보고해야 합니다. 이를 위해 VRRP 서비스는 상호의존적인 서브넷 그룹을 관리합니다. 그룹에서 하나의 서브넷이 실패하면 모든 서브넷이 실패한 것처럼 작동하고 그룹화된 모든 서브넷에서 알림을 중지합니다.

쉽게 구성하기 위해 일부 인스턴스 속성은 그룹 수준에서 정의됩니다.

- Name — 게이트웨이 식별 문자열은 백업에 사용되는 동일한 그룹 이름과 다를 수 있습니다. 그러나 사용자 오류로 이어지므로 다른 이름을 사용하지 않는 것이 좋습니다.
- Initial state — 서비스 시작 시 모든 인스턴스의 상태를 통해 초기 상태 안정화 속도가 빨라집니다. 일반적으로 마스터는 처음에 마스터이고 백업은 처음에 백업이지만 필수 사항은 아닙니다.
- Advertisement period — 이 VRRP 매개 변수는 그룹의 VRRP 인스턴스에 제공됩니다.
- VRRP instances list — 그룹의 일부인 인스턴스입니다.
- Connection tracking — 라우터가 NAT/PAT 인 경우 백업이 활성화될 때 VRRP 가 연결을 동기화해야 합니다. 연결 추적 서비스를 사용하도록 설정하고 별도로 구성해야 합니다.

그룹 속성은 초기 상태를 제외하고 마스터와 백업에서 동일해야 합니다.

RFC changes

RFC3768 에는 다음과 같은 세 가지 향상된 기능이 추가되었습니다.

- 타이머는 seconds 가 아닌 centiseconds 단위로, 이 기능은 VRRP V3(RFC5798)에서 가져온 것입니다.
- 새로운 "fault" 상태를 통해 부분적인 하드웨어 장애를 추적할 수 있습니다. 진정한 VRRP 프로토콜은 완전한 라우터 종료만 처리합니다.
- 마스터 라우터와 백업 라우터의 MAC 주소가 서로 다릅니다. 즉, 가상 MAC 주소는 지원되지 않습니다. 따라서 가상 라우터를 사용하는 장치는 전부는 아니더라도 IP 네트워크 장치의 대부분인 ARP 프로토콜을 처리해야 합니다.

V.5.1.2 Connection tracking

"connection tracking" 서비스는 오히려 "connection tracking and replication" 서비스입니다. 라우터가 NAT/PAT 모드일 때, 연결 추적 서비스는 마스터와 슬레이브 간의 연결 정보를 동기화합니다. 연결 정보는 가능한 한 빨리 마스터에서 슬레이브로 전송됩니다(크기 순서는 수십 밀리초이지만 실제 수치는 제품 및 네트워크 로드에 따라 다릅니다). 장애 직전에 열린 연결이 백업 라우터로 전송되지 않을 가능성이 약간 있습니다. 사용자의 응용 프로그램 소프트웨어가 이를 준비하고 연결을 다시 시도해야 합니다.

전용 네트워크 링크를 사용하여 연결 데이터(예: 일부 제품에서 사용 가능한 보조 이더넷)를 전송할 수 있습니다.

TCP 연결을 설정하거나 해제할 때마다 또는 UDP 흐름이 안정화될 때마다 서비스가 활성화됩니다. 사용자의 애플리케이션에 따라 이러한 이벤트가 많이 발생할 수 있습니다. 이러한 파일은 함께 그룹화되어 UDP 멀티캐스트 패킷으로 연결 목록을 복제하는 백업 시스템으로 전송됩니다. 그룹화는 많은 연결이 있을 때 네트워크의 오버플로우를 방지하지만 복제에 약간의 지연을 초래합니다.

V.5.1.3 Failures reporting

라우터가 상태를 변경하면 내부 이벤트가 생성되며, 일반 "alarms/events" 서비스로 다양한 작업을 생성하도록 이벤트를 설정할 수 있습니다. 지정된 인스턴스 또는 그룹이 지정된 상태로 들어가거나 나갈 때 작업을 트리거할 수 있습니다. 이벤트 및 작업을 연결할 때 SNMP 작업을 전파하려면 작동 서브넷이 필요하다는 것을 기억해야 합니다.

V.5.1.4 Force routing via the BACKUP

예를 들어 마스터를 즉시 재구성해야 하는 경우처럼 의도적으로 MASTER 에서 백업으로 전환하는 것이 유용할 수 있습니다. 이를 위해 그룹의 우선 순위 수준에서 재생할 수 있습니다. 기본적으로 MASTER 그룹의 우선 순위는 230 으로 고정되고 BACKUP 그룹의 우선 순위는 200 으로 고정됩니다. SNMP 명령을 사용하면 일시적으로 MASTER 의 우선 순위를 0 으로 낮추어 강제로 백업을 대신할 수 있습니다. 이렇게 하려면 Alter VRRP action (참조 섹션 Alarms/events)을 사용하여 이벤트 트리거 SNMP Trigger 를 프로그래밍해야 하며, 인수로서 MASTER 그룹의 이름과 우선 순위 값에 적용할 오프셋(예: 기본값을 유지한 경우 -230)을 지정해야 합니다.

OID adminEventEnable 을 SNMP 로 전송하면 트리거 이름을 인수로 지정하여 정의된 오프셋을 MASTER 그룹의 우선 순위에 적용할 수 있습니다(예: 230-230=0). 그러면 즉시 BACKUP 으로의 전환이 트리거되므로 우선 순위가 더 높습니다.

그러면 OID adminEventDisable 을 보내면 오프셋이 취소되고 결과적으로 MASTER 그룹의 우선 순위를 복원할 수 있으므로 MASTER 가 다시 이어받습니다.

V.5.1.5 Miscellaneous questions

a. Access points configuration

액세스 포인트는 클라이언트가 여러 IP 주소를 사용하고 수시로 변경할 수 있도록 허용해야 합니다. **이 요구 사항은 일부 형식의 프록시 ARP 를 제외합니다.**

b. Throughput

로드 공유에서는 테이크오버 후 모든 데이터가 하나의 라우터에 의해서만 라우팅되는 실패 가능성을 고려해야 합니다. 따라서 이러한 구성에서는 처리량을 허용 처리량의 절반으로 제한하는 것이 좋습니다.

시간 초과를 줄이면 시스템이 더 빨리 반응하지만 CPU 와 네트워크에 추가 부하가 걸리기 때문에 유용한 처리량이 줄어듭니다.

c. Wi-Fi bandwidth occupation

VRRP 및 연결 추적은 MULTICAST 프레임에 의존합니다. 공기 대역폭에 미치는 영향을 고려해야 합니다.

1. 모든 VRRP 프레임은 공기를 통해 3 회 전송됩니다. Master(Wi-Fi 클라이언트) → AP 방향으로 두 번 전송됩니다. UNICAST 에서 AP 로 한 번 전송되어 AP 의 다른 잠재적 클라이언트에 (저비트 속도로) 재전송됩니다.
2. AP → Backup (Wi-Fi 클라이언트) 방향으로 낮은 비트 전송률로 한 번 브로드캐스트 됩니다.
3. AP 의 멀티캐스트/브로드캐스트 프레임은 사용 가능한 가장 낮은 변조 속도(2.4GHz 대역에서 1Mbps 또는 5GHz 대역에서 6Mbps)로 전송됩니다. 가장 낮은 비트 전송률을 비활성화하여 멀티캐스트 속도를 높일 수 있습니다(문서 참조).
4. 앞서 서술한 바와 같이 연결 추적 및 복제에는 와이파이를 사용하지 않는 것이 좋습니다. 대역폭은 이를 피하는 또 다른 이유입니다.

VRRP 기간이 짧을수록 대역폭이 더 많이 점유될수록 유용한 데이터 교환에 사용할 수 있는 대역폭이 줄어듭니다.

d. Influence of Wi-Fi handover (roaming) on VRRP takeover delay

"클라이언트" Wi-Fi 기능에서 로밍 모드가 활성화되면 두 가지 종류의 짧은 전송 중단이 발생합니다. 이러한 중단 시간은 VRRP "Advertisement periods"을 구성할 때 반드시 고려되어야 하며, 따라서 고장이 아닌 로밍 지연으로 인해 원치 않는 테이크오버가 발생하지 않습니다.

1. 다중 채널 스캔으로 인한 중단

   "advanced roaming" 탭의 Maximum time off-channel, Offchannel adaptation delay, Per channel probe response delay 이라는 세 가지 파라미터를 사용하여 일부 제한 내에서 구성할 수 있습니다. 표준 AP 와 기본 파라미터의 경우, 중단은 65ms 를 초과하지 않습니다.

2. 한 AP 에서 다른 AP 의 핸드오버로 인한 중단

   이 경우 중단 기간은 보안 매개 변수의 종류, AP 성능 및 AP 신속성과 같은 많은 요인에 따라 달라집니다. 다양한 요인에 따라 기간은 14ms(보안 없음, fast

AP)에서 300ms(WPA, RADIUS dialog, 인증서 제어, slow AP 등)까지 다양할 수 있습니다.

핸드오버 프로세스는 VRRP 서비스에 의한 Wi-Fi 연결 끊김 감지를 억제합니다. 다른 AP 를 빠른 로밍에 사용할 수 있는 경우, 다른 AP 에 대한 연결이 빠르게 이어진다는 가정 하에 연결 끊김 감지가 비활성화됩니다. 빠른 재연결이 실패하면 타이머가 만료되고 VRRP 가 연결을 처리하도록 합니다. 현재 AP 의 손실과 VRRP 페일오버 결정 사이의 최대 시간을 나타내는 타이머는 다음과 같이 계산됩니다.

- 스캔 주기 기간이 2 초보다 큰 경우:

  Timer = (scan interval parameter) + 2s.

- 2 초보다 작은 경우:

  Timer = 2 × (scan interval parameter)

e. Influence of the priority field on VRRP takeover delay

VRRP 는 둘 이상의 백업을 처리하도록 설계되었습니다. "priority" 필드는 잠재적으로 많은 백업 간의 우선 순위를 조정합니다. 마스터의 오류를 탐지하는 타이머는 이 우선 순위 필드에 따라 달라집니다. 우선 순위가 높을수록 테이크오버(인수)가 더 빠릅니다. 그러나 우선 순위 협상에서 안정성 이유로 VRRP 인스턴스의 각 장치에 할당된 값 간(즉, 마스터와 백업 간)에는 큰 간격을 사용하는 것이 좋습니다. 마스터의 "advertisement" 프레임 대기 시간은 다음과 같이 계산됩니다.

Timeout (in ms) = ((256 – priority) / 256) × 1000 + 3 x AdvertisementPeriod

예를 들어, 제품의 초기 역할이 "backup"이고, Advertisement period = 100 ms 이면 default timeout 은 다음과 같습니다.

(256 – 200)/256 × 1000 + 3 x 100 = 519 ms (±4 ms)

f. Takeover caused by a Ethernet link loss

사용되는 소프트웨어 및 하드웨어 구성 요소의 제한으로 인해 이더넷 링크 손실을 감지하는 데 최대 2 초가 걸릴 수 있습니다. 분명히 이 경우 인수는 지연 전에 이루어질 수 없습니다.

g. Packets are not routed from wireless to wired interfaces! What is wrong?

Advanced settings/bridging mode setting 은 ARPNAT 모드로 유지되었습니다. 섹션 *V.2.6.2a* 에 설명된 대로 브리지되지 않은 무선 인터페이스만 수신 데이터를 라우팅할 수 있습니다. 무선 인터페이스를 유지하는 "network"는 non-bridging 으로 설정되거나 클라이언트 브리징 모드가 4-addresses 여야 합니다.

h. SNMP

VRRP 구성에 대해 SNMP OIDs 가 아직 정의되지 않았습니다. 따라서 SNMP 를 사용하여 VRRP 를 구성할 수 없습니다.

그러나 SNMP 트랩은 정의되어 있으며 구성 및 전송할 수 있습니다.

V.5.1.6 Link layer redundancy with RSTP

WaveOS 는 STP 및 RSTP 프로토콜을 지원합니다. 링크 계층 프로토콜로 브리지 구성요소에서 처리됩니다. 참조 *V.1.8.3 Spanning Tree Protocols (STP, RSTP)*

V.6 SNMP agent and ACKSYS MIB

SNMP 프로토콜은 관리 스테이션과 SNMP 에이전트 간의 통신 내용을 정의합니다. SNMP 에이전트는 각 관리되는 시스템에서 실행되고 SNMP 를 통해 관리 시스템에 정보를 보고합니다.

SNMP 를 통해 다음 작업 수행

- 장치 상태 확인
- 제품의 설정 변경
- 이벤트 관리

V.6.1 SNMP security

V.6.1.1 SNMP V1 and V2c

SNMP V1 과 V2c 에서, 보안은 **Community String** 에 매핑된 IP 기반 액세스 제어에 따릅니다. 클라이언트의 인증은 **community string** 을 사용하여 수행되며, 패스워드 형식의 일반 텍스트로 전송됩니다.

SNMP V1/V2c 커뮤니티는 SNMP AGENT 하위 메뉴에서 구성할 수 있습니다. 참고: *SNMP Agent*

V.6.1.2 SNMP V3

SNMP v3 프로토콜은 SNMP v1 및 SNMP v2c 보다 더 정교한 보안 메커니즘을 제공합니다. SNMP v3 는 에이전트와 해당 관리자 간에 전송된 요청을 인증 및 암호화하고 사용자 기반 액세스 제어를 제공하는 USM(사용자 기반 보안 모델)을 구현합니다.

SNMP V3 는 보안을 인증/암호화 및 권한 부여의 두 부분으로 나눕니다.

a. The User based Security Model (USM):

USM 은 인증 및 개인 정보 보호(암호화) 기능을 제공하며 메시지 수준에서 작동합니다.

USM 에서 관리자는 다음 사용자 목록을 만들 수 있습니다.

- 각 사용자에게는 데이터 암호화를 위한 이름(Security Name), 인증 유형(NONE, MD5 또는 SHA) 및 개인 정보 프로토콜(NONE, DES 또는 AES)이 있습니다.

WAVEOS 는 AES128 을 AES 암호화로 지원합니다.

USM 에 대한 자세한 내용은 "RFC 3415"를 참조하세요.

SNMP V3 사용자는 SNMP AGENT 하위 메뉴에서 구성할 수 있습니다.

참고: *SNMP Agent*

b. The View based Access Control Model (VACM):

VACM 은 사용자가 특정 기능을 수행하기 위해 MIB 개체에 액세스할 수 있는지 여부를 결정하고 PDU 수준에서 작동합니다.

VACM 에서 관리자는 다음을 수행할 수 있습니다.

- 각 사용자 (또는 SNMPv1/v2c communities)에 보안모델 할당
  - **V1** 커뮤니티 기반 보안 모델
  - **V2c** 커뮤니티 기반 보안 모델
  - **USM**

  그리고 **"Security Model, Security Name"**의 각 쌍에 그룹 이름을 할당합니다.
- MIB 하위 트리를 포함하거나 제외할 수 있는 MIB 개체 집합을 포함하는 "**Views**"를 정의합니다.
- 각 그룹에 대한 액세스 정책 설정: 지정된 보기에 대한 읽기/쓰기 권한
  - 각 **"Group Name, Context Name, Security Model, Security Level"**은 지정된 보기에 대한 읽기/쓰기 권한을 할당할 수 있습니다.
  - **Security Level**:
    - No authentication.
    - Authentication and no privacy (data encryption).
    - Authentication and privacy (data encryption).

보안모델 V1 and V2c 는 security level 을 "No authentication"으로 합니다.

WAVEOS 에서 사용하는 컨텍스트 이름은 항상 빈 문자열인 기본 컨텍스트 이름입니다 (SNMP 컨텍스트에 대한 자세한 내용은 RFC 5343 참조).

VACM 에 대한 자세한 내용은 "RFC 3415"를 참조하세요.

SNMP AGENT 하위 메뉴에서 사용자의 액세스 권한을 구성할 수 있습니다.

참조: *SNMP Agent*

V.6.2 Access methods

SNMP 에이전트에 대한 요청은 WAVOS 에 구성된 SNMP 보안 규칙에 따라 SNMP V1, V2c 또는 V3 을 사용할 수 있습니다.
SNMP V1 및 V2C 의 경우 "public" 커뮤니티는 기본적으로 읽기/쓰기로 구성되며 웹 인터페이스를 통해 커뮤니티를 관리할 수 있습니다.

Recommended tools

- Net-SNMP 참고 사이트: *http://www.net-snmp.org/*
- Ireasoning™ MIB browser 참고 사이트: *http://ireasoning.com/mibbrowser.shtml* (JAVA 필요)

V.6.3 Using the Acksys MIB

Obtaining the MIB

Acksys MIB 는 www.acksys.com 의 다운로드 섹션에서 제공되는 펌웨어 업데이트 패키지에 포함되어 있습니다. ACKSYS MIB 파일은 자체 문서화되어 있습니다. OID 설명서를 읽으려면 텍스트 파일 편집기 또는 MIB 브라우저를 사용하세요.

Relevant OIDs

Acksys MIB 는 다양한 장치를 지원합니다. 따라서 모든 OID 는 WaveOS 와 관련이 없습니다. 모든 OID 설명에는 이 OID 와 관련된 펌웨어를 식별하는 펌웨어 태그가 포함되어 있습니다. "WaveOS 펌웨어 버전 2.8.0.1"과 같이 필요한 펌웨어 유형과 최소 버전이 태그에 포함됩니다.

아래에 설명된 모든 OIDs 는 Acksys MIB root 와 관련이 있습니다.

- .1.3.6.1.4.1.28097
- iso.org.dod.internet.private.enterprises.acksys

다음 OID 는 WaveOS 에 유용합니다. 각 항목에 대한 수치 OID 값과 구체적인 설명은 MIB 를 참조하세요.

acksysProductID	제품 모델 식별 코드
acksysProductSerialNumber	제품에 할당된 고유 식별자
network-product.administration	핵심 관리 기능: adminReset, adminSave, adminApply, adminResetFactory
c-key-management	C-KEY 에서 구성을 지우거나 저장/복원하고 영구적으로 C-KEY 의 상태 LED 를 off 시키며, C-KEY 의 설정을 무시하는 기능. Acksys 제품에 대해 예약된 테스트 유틸리티 제공.
networkStatus	현재 실행중인 네트워크 상태, 참조: *V.6.4*
networkConfiguration	인근에 구성된 제품의 네트워크 파라미터, 참조: *V.6.5*
serviceStatus	현재 실행중인 서비스 상태
servicesConfiguration	인근에 구성된 제품의 서비스 구성, 참조: *V.6.6*

Changing the configuration

networkConfiguration 또는 servicesConfiguration 의 항목이 변경되면 변경 내용이 영구 메모리에 저장되지 않습니다. adminSave OID 를 읽으면 보류 중인(저장되지 않은) 변경 사항이 있는지 알 수 있습니다. saveNotRequired 는 저장되지 않은 변경 사항이 없음을 의미합니다. saveRequired 는 보류 중인 변경 사항이 있음을 의미합니다. adminSave 에 '1'을 적어 영구 메모리에 저장할 수 있습니다.

adminResetFactory 를 '1'로 설정하면 저장 여부에 관계없이 이전 구성이 삭제되고 제품이 재부팅되므로 공장 설정으로 재설정됩니다. 그러나 펌웨어 버전은 변경되지 않은 상태로 유지됩니다.

Applying the configuration

현재 저장된 변경 내용을 적용하려면 adminApply 를 'enable'(제품을 재부팅하지 않음)으로 설정하거나 adminReset 을 '1'(제품을 재부팅함)로 설정할 수 있습니다. 경고: 제품 네트워킹 하위 시스템이 중지되었다가 다시 시작되었기 때문에 네트워크 구성 변경 사항을 적용하면 에이전트에서 응답을 받지 못할 수 있습니다. SNMP 클라이언트에서 수정된 새 네트워크에 연결할 수 없는 경우 에이전트에서 응답을 받을 수 없습니다. 이것은 오류로 간주되지 않습니다.

V.6.4 Understanding network status tables

제품의 현재 네트워크 상태는 아래에 요약되어 있습니다.

- statusIfWlanTable: 실행 중인 무선 인터페이스 상태(예: BSSID, 채널, 보안 정보, 연결 상태, 신호 수준 등)를 나열합니다.
  statusIfWlanChannel OID 는 무선 인터페이스에서 사용되는 현재 채널을 표시합니다. 채널 "-1"은 채널 선택 프로세스가 진행 중임을 나타냅니다. *statusIfWlanFrequency* OID 의 주파수와 0(MHz)은 동일합니다.
  기본적으로 *statusIfWlanPreSharedKey* OID 가 SNMP V3 의 보호를 받는 경우 admin acksys group 만 결과를 볼 수 있습니다. 물론 SNMP AGENT 하위 메뉴에서 이 구성을 수정할 수 있습니다. 참조: *SNMP Agent*
- statusPhyWifiTable: 라디오 카드 레이블, 활성화/비활성화 상태, 클러스터 모드 등과 같은 라디오 카드의 현재 상태를 표시합니다.
- statusPhyWifiScanTable: Acksys MIB 는 *statusPhyWifiScanTableStart* OID 에 '1'을 입력하여 무선 검색 서비스를 제공합니다. 검색을 시작한 후 *statusPhyWifiScanUpdateTbl* OID 를 읽어 현재 검색이 완료되었는지 확인할 수 있습니다. inprogress 는 아직 검색이 완료되지 않았음을 의미하며, available 은 검색이 중지되었음을 의미하고, *statusPhyWifiScanTable* 에서 결과를 확인할 수 있습니다.
  StatusPhyWifiScanTable 은 액세스 포인트, 메시 포인트 또는 애드혹 스테이션과 같은 모든 무선 채널에서 사용 가능한 모든 무선 장치를 요약합니다. 이 표에서는 SSID, BSSID, 신호 수준, 주파수(MHz), 보안 등과 같은 유용한 정보를 찾을 수 있습니다. StatusPhyWifiScanSignal OID 는 프로브 및 비콘 프레임에서 가져온 신호 레벨을 dBm 단위로 표시하며, 이 신호 레벨은 사용 가능한 최저 속도로 전송됩니다. 일반적으로 이러한 프레임에 대해 발견된 신호 수준은 데이터 프레임의 신호 수준보다 높습니다.
- statusSpanningTreeTable: 제품에 STP/RSTP 가 활성화된 브리지가 있는 경우 STP/RSTP 브리지의 현재 상태를 표시합니다.
- statusSpanningTreePortTable:
  이 표에는 상태 SpanningTreeTable 과 스패닝 트리 포트에 대한 추가 정보가 포함되어 있습니다.

V.6.5 Managing network configuration tables

네트워크 구성 관리는 OSI 모델의 3 계층인 IP 계층(tcp/ip), 데이터 링크 계층(netif) 및 물리 계층(netphy)을 나타내는 3 가지 부분으로 구성됩니다. 각 계층에서 관련 OID 를 찾을 수 있습니다.

이 기능은 공통 매개 변수를 가진 AP 와 STA(클라이언트)의 조합이므로 "repeater" 테이블은 없습니다.

관련 테이블 중 하나에 행을 삽입하려면 만들 인덱스에 의해 색인화된 'rowStatus' 항목을 'createAndGo'로 설정해야 합니다. 행을 제거하려면 삭제할 인덱스의 'rowStatus' 항목을 'destroy'하도록 설정해야 합니다.

CAVEATS:

- SNMP 및 웹 인터페이스와 동시에 구성을 변경하지 않는 것이 좋습니다. 이러한 두 서비스 중 하나에서 다른 서비스로 변경 내용을 전파하는 데 몇 초가 걸릴 수 있습니다.
- SNMP 에이전트는 웹 인터페이스로 만든 리피터를 인식하지 못합니다. 해결 방법은 아래 예제에 나와 있습니다.
- WEB 인터페이스는 AP 용 WPA/WPA2 PSK 혼합을 제외하고 WPA 혼합(WPA/WPA2 혼합)을 지원하지 않습니다. 또한 WPA 암호 모드 tkip, aes 또는 tkip+aes 를 지원하지 않습니다. SNMP 를 통해 이러한 모드 중 하나를 구성하면 WEB 인터페이스에 "No encryption"이 표시됩니다.
- AP 의 기본 WPA 암호는 WPA2-PSK 및 WPA2-EAP 모드의 경우 AES 이고 WPA-PSK 및 WPA-EAP 모드의 경우 TKIP+AES 입니다. 클라이언트의 경우 기본 암호는 WPA/WPA2-EAP-TLS 모드의 경우 AES 이고 다른 모드의 경우 TKIP+AES 입니다. 다른 WPA 암호를 구성할 수도 있지만 WEB 인터페이스에 유의해야 합니다.

V.6.6 OIDs relevant to IP layer

IP 계층과 관련된 OID 는 IP 설정, 라우팅 및 방화벽 관리에 관한 것입니다. 아래 설명된 OID 테이블에서 사용자는 SNMPV2c 절차를 사용하여 행을 삽입하거나 삭제할 수 있습니다.

- configIpSubnetTable: IP 설정이 있는 구성 가능한 네트워크 인터페이스를 나열합니다. 기본적으로 네트워크 인터페이스는 *configIpSubnetInterface* 을 사용하여 무선 인터페이스, 이더넷 인터페이스, 가상 인터페이스 또는 L2 tunnel GRE 인터페이스 중 하나의 인터페이스만 지정할 수 있습니다.
  네트워크에 다중 인터페이스를 추가하려면 configIpSubnetBridgeEnable OID 에 '2'를 적어 네트워크를 브리지로 설정한 다음 configInterfaceTable 을 관리하여 인터페이스를 추가해야 합니다 (참조 *configInterfaceDepends* in *section OIDs relevant to Data Link Kayer*).
- configIpZonesTable: 사용자 정의 network zones 의 일반 설정입니다. 이 표에서는 NAT/PAT(IP Masquerading)를 활성화한 후 configIpNatIpForwardTable 로 이동하여 추가 구성을 수행할 수도 있습니다.
- configIpNatIpForwardTable: configIpZoneNAT 이 활성화된 경우 한 영역의 입력 트래픽을 private zone 의 장치로 리디렉션할 수 있습니다.
- configIpFirewallTable: 지정된 영역에서 통합 방화벽 규칙을 관리하는 데 사용됩니다. 방화벽은 선택한 영역에서 다른 디바이스 또는 영역으로 입력 트래픽을 drop, reject 또는 forward 할 수 있습니다.

- configIpRoutesTable: 정적 경로 목록입니다. 정적 경로는 특정 호스트 또는 네트워크에 연결할 수 있는 인터페이스 및 게이트웨이를 나타냅니다.
- configIpZoneForwardTable: 영역 간 전달 규칙 목록입니다. 한 영역과 다른 영역 간에 전달 정책을 설정할 수 있습니다. 이 테이블은 IP Masquerading 을 비활성화하는 영역에만 사용됩니다.
- configIpDscpTaggingTable: 들어오는 각 프레임에 적용된 DSCP 태그 규칙 목록입니다. 이 테이블의 모든 규칙과 일치하는 수신 프레임은 DSCP 태그에 태그가 지정됩니다. 한 IP 네트워크에서 다른 IP 네트워크로 전달된 라우팅된 프레임만 태그를 지정할 수 있습니다.

Acksys MIB 는 DOS 보호 관리 기능도 제공: 기본적으로 활성화되어 있음

- synfloodprotection: SYN-flood protection 활성화/비활성화
- dropinvalidpacket: 활성 연결이 없는 잘못된 프레임을 삭제/수락

V.6.7 OIDs relevant to Data Link layer

무선 인터페이스, 가상 인터페이스 및 브리지에 대한 구성 세부 정보는 데이터 링크 계층과 관련이 있습니다. configInterfaceTable 을 제외한 다음 설명된 OID 테이블에서 사용자는 SNMPV2c 절차를 사용하여 행을 삽입하거나 삭제할 수 있습니다.

- configFilterGroupTable: 계층 2 브리지 필터 그룹을 관리할 수 있습니다. 자세한 필터 규칙 정보는 configFilterGroupRuleTable 을 참조하세요.
- configFilterGroupRuleTable: 모든 필터 그룹의 필터 규칙을 나열합니다. 각 필터 그룹에는 하나 이상의 필터 규칙이 포함될 수 있습니다. 하나 이상의 규칙과 일치하는 프레임이 삭제됩니다.
- configInterfaceTable: 모든 논리 인터페이스가 이 테이블에 나열됩니다. 행은 다음 표에 따라 에이전트에 의해 고정됩니다. 사용자는 행을 삽입하거나 삭제할 수 없습니다. configInterfaceDepends OID 를 사용하여 이러한 인터페이스 간의 네트워크 관계를 관리할 수 있습니다. 네트워크 관계는 하나의 브리지 인터페이스와 하나 이상의 비 브리지 인터페이스 간의 종속성입니다. configInterfaceDepends OID 에서 무선 인터페이스, 이더넷 인터페이스, L2 터널 GRE 인터페이스 또는 VLAN 인터페이스와 같은 하나 이상의 비브릿지 유형 인터페이스 아래에 브리지를 지정할 수 있습니다. 이 규칙을 준수하지 않으면 SNMP 에이전트가 오류 메시지를 보내 사용자의 구성을 거부합니다.
- 또한 configInterfaceFilterGroupIndex 와 configInterfaceFilterGroupDir OID 을 설정하여 각 인터페이스에서 필터 그룹을 구성할 수 있습니다.
- configInterfaceTable 에 나열된 모든 인터페이스는 다음 표에서 제공됩니다. 추가 구성은 여기에서 확인할 수 있습니다.
- configIfMeshTable: 구성 가능한 메쉬 포인트 목록입니다. 현재 메시 포인트는 보안 모드로 SAE 만 지원합니다.
- configIfBridgeTable: MAC 브리지 네트워크 목록입니다. STP/RSTP 가 활성화된 브리지에 대해 STP/RSTP 를 구성할 수 있습니다.
  configIfVlanTable: 구성 가능한 VLAN 인터페이스 목록입니다.
- configIfStaTable: 인프라 클라이언트 목록입니다. 이 표에서 클라이언트의 일반 구성, 보안 및 로밍의 고급 구성을 찾을 수 있습니다.
  각 보안 모드에는 전용 구성이 있습니다. 보안 모드를 정의할 때 이러한 구성을 설정해야 하며 다른 보안 모드의 구성을 무시해야 합니다. 다음은 지정된 보안 구성에 대한 요약입니다.

SECURITY	SPECIFIED CONFIGURATION	DESCRIPTION
WEP	configIfStaWepKey1 - 4	HEX (characters 0-9, A-F) or ASCII 형식 문자열로 정의된 WEP KEY #1- #4
	configIfStaWepKey	4 개의 WEP keys 중 현재 선택된 키
WPA(2)-PSK	configIfStaKey	사전 공유키의 길이는 8 to 63 자. 길이가 64 자인 경우 16 진주 형식으로 사용됨
	configIfStaFastBSSTransitionActivated	Fast transition support (802.11r)
WPA(2)-EAP	configIfStaKey	Password TLS mode: 선택한 개인 키에 연결된 암호
	configIfStaEapType	EAP method: TLS, PEAP, LEAP
	configIfStaFastBSSTransitionActivated	Fast transition support (802.11r)
	configIfStaIdentity	LEAP/PEAP mode 에 대해서만 식별됨
	configIfStaPrivateKey	SNMP-SET 에서 개인 키 파일의 내용을 PEM 형식(TLS 모드에서만)으로 업로드 가능 결과는 SNMP-GET 으로 표시: 0 : key not set 1 : key is uploaded
	configIfStaCACert	SNMP-SET 를 통해 CA-Certificate 파일의 내용을 PEM 형식(TLS 모드에서만)으로 업로드 가능 결과는 SNMP-GET 으로 표시: 0 : key not set 1 : key is uploaded
	configIfStaUserCert	업로드한 사용자 인증서 파일의 내용을 SNMP-SET 에서 PEM 형식(TLS 모드에서만)으로 업로드 가능 결과는 SNMP-GET 으로 표시: 0 : key not set 1 : key is uploaded
	configIfStaAuthentication	PEAP 모드에서만 단계 2 에 대한 인증 유형
	configIfStaWpaKeyCacheLifeTime	클라이언트가 이미 인증된 AP 로 로밍하는 경우 인증키가 유지되는 시간(초)

다음 OID 는 로밍 모드 전용 구성으로, 로밍 클라이언트를 추가로 구성하는 데 도움이 될 수 있습니다. 클라이언트가 로밍을 사용할 경우에만 해당됩니다.

OID NAME	DESCRIPTION
configIfStaRoamingEnable	클라이언트 로밍 모드 활성화 *[아래의 모든 OID 는 '2'로 설정된 경우에만 해당됩니다.]*
configIfStaRoamingEnableDBM	현재 AP 의 RSSI 가 이 값(dBm) 아래로 떨어지면 클라이언트는 현재 AP 를 떠나 다른 AP 로 로밍을 시도합니다.
configIfStaRoamingRequiredBoost	로밍은 잠재적 AP 신호가 현재 AP 에 이 값을 더한 값(dBm) 이상인 경우에만 발생합니다.
configIfStaRoamingScanPeriod	두 번의 연속 검색 주기 사이의 지연 시간 (millisecond)
configIfStaRoamingRssiSmoothingFactor	현재 AP 의 RSSI 는 수신된 마지막 몇 개의 비콘에 대해 계산된다. 이전 비콘과 비교하여 마지막 비콘의 중요도를 선택합니다. RSSI 평활 계수는 1 과 16 사이의 값으로 1/16 의 단계를 나타냅니다.(예: 3/16, 5/16, 16/16). *WEB 인터페이스에서는 백분율 형태로 표시: 6%(1), 13%(2), 19%(3), 25%(4), 31%(5), 38%(6), 44%(7), 50%(8), 56%(9), 63%(10), 69%(11), 75%(12), 81%(13), 88%(14), 94%(15), 100%(16)* *Default:19%(3)*
configIfStaRoamingBeaconTimeout	비콘 간격 단위
configIfStaRoamingCurrentApScanThreshold	현재 AP 신호가 이 수준(dBm)을 초과하면 클라이언트가 검색을 중지합니다. 무조건 검색하려면 0 으로 설정합니다. *configIfStaRoamingMaxSignalLevel 과 호환되지 않음*
configIfStaRoamingMinimumStaLevel	AP 의 신호는 이 수준(dBm)보다 낮으며 로밍 후보는 아니지만 현재 AP 또는 더 나은 AP 가 없는 경우에도 사용됩니다. 이 구성을 사용하지 않도록 설정하려면 '0'
configIfStaRoamingAboveLevelThreshold	현재 AP 의 인식된 신호 수준이 이 제한(dBm)을 초과하면 클라이언트는 다른 AP 로 로밍을 시도합니다. 이 구성을 사용하지 않도록 설정하려면 '0'
configIfStaRoamingMaxSignalLevel	이 수준(dBm)보다 높은 AP 는 로밍할 다음 AP 를 선택할 때 우선 순위가 낮습니다.
configIfStaRoamingMinRoamDelay	마지막 연결 이후 지연 시간(ms)이 경과하기 전에는 로밍이 수행되지 않습니다.
configIfStaRoamingNoReturnDelay	최근에 떠난 AP 는 로밍이 발생하지 않습니다. (ms, 최대 180000ms)
configIfStaRoamingThresholdHysteresis	이 값(dBm)은 해당 임계값 히스테리시스 간격을 설정하기 위해 각 임계값에 추가 및 감산됩니다.
configIfStaRoamingOffChanMaxDelay	연결된 AP 에서 데이터를 버퍼링해야 하는 최대 채널 끄기 지연 시간(ms)
configIfStaRoamingOffChanProbeDelay	채널 전환 후 프로브 요청을 전송하기 전 충돌 방지를 위한 지연 시간(ms)
configIfStaRoamingPerChanProbeDelay	AP 의 응답을 기다리는 시간(ms)

- configIfAPTable: 구성 가능한 액세스 지점 목록입니다. 일반 AP 설정, 보안, MAC 필터 및 프레임 필터에 대한 모든 구성은 표에서 확인할 수 있습니다.
  configIfStaTable 에서와 마찬가지로 각 보안에는 지정된 구성이 있습니다. 선택한 보안 구성에 초점을 맞추고 다른 보안 구성은 무시합니다.

SECURITY	SPECIFIED CONFIGURATION	DESCRIPTION
WEP	configIfAPWepKey1 - 4	HEX (문자 0-9, A-F) 또는 ASCII 형식 문자열로 정의된 WEP KEY #1- #4
	configIfAPWepAuthentication	WEP type: open, share
	configIfAPWepKey	현재 사용되는 WEP 키, 4 개의 WEP 키 중 하나를 선택하여 나타내는 1 과 4 사이의 값
WPA(2)-PSK	configIfAPKey	사전 공유 키(8~63 자)입니다. 길이가 64 자인 경우 16 진수 형식으로 직접 사용됨
	configIfAPPreAuthentication	802.11w 보안기능 활성화
	configIfAPWpaGroupRekey	GTK(브로드캐스트/멀티캐스트 암호화 키) 키 재생성을 위한 시간 간격(초)
	configIfAPWpaPairRekey	PTK(유니캐스트 암호화 키) 키 재생성을 위한 시간 간격(초)
	configIfAPWpaMasterRekey	GMK(GTK 를 생성하기 위해 내부적으로 사용되는 마스터 키)의 키 재생성을 위한 시간 간격(초)
WPA(2)-EAP	configIfAPKey	8~63 자 길이의 공유 암호
	configIfAPPreAuthentication	802.11w 보안기능 활성화
	configIfAPWpaGroupRekey	GTK(브로드캐스트/멀티캐스트 암호화 키) 키 재생성을 위한 시간 간격(초)
	configIfAPWpaPairRekey	PTK(유니캐스트 암호화 키) 키 재생성을 위한 시간 간격(초)
	configIfAPWpaMasterRekey	GMK(GTK 를 생성하기 위해 내부적으로 사용되는 마스터 키)의 키 재생성을 위한 시간 간격(초)
	configIfAPRadiusIndex	configRadiusTable 항목의 선택된 인덱스

- configRadiusTable: AP 보안 구성을 위해 준비된 Radius 서버의 하위 테이블입니다. 여러 Radius 서버를 포함할 수 있습니다. AP 용 Radius 서버를 하나 선택할 수 있습니다.

  AP 에 대한 Radius 서버의 선택은 웹 인터페이스와 SNMP 에이전트 간에 다릅니다. 두 서비스 모두에서 Radius 서버를 변경하면 웹 인터페이스가 우선합니다. SNMP 에 의해 설정된 Radius 구성을 복구하려면 먼저 웹 인터페이스를 사용하여 AP 를 비 Radius 모드로 변경합니다.
- configDetailsNasId: Radius 서버의 NAS 공통 식별자입니다. WPA-EAP 모드에서 AP 에 사용됩니다.

V.6.7.1 OIDs relevant to Physical layer

configPhyWifiTable 무선 카드에 대한 모든 물리적 매개변수를 수집합니다. 사용자는 행을 삽입하거나 삭제할 수 없습니다. 행 수는 제품에 설치된 라디오 카드에 따라 다릅니다.

configPhyWifiChannel 의 '0'은 라디오 카드가 여러 채널 또는 자동 채널 선택에 대해 구성되었음을 나타냅니다. 자세한 채널 정보는 configPhyWifiChannelList 를 참조하세요. configPhyWifiChannelList 는 공백으로 구분된 하나 이상의 채널을 포함할 수 있습니다. configPhyWifiChannelList 의 'auto' 또는 '0'은 자동 채널 선택을 나타냅니다.

무선 카드가 클라이언트 로밍 모드로 구성되어 있고 configPhyWifiChannel 및 configPhyWifiChannelList 가 무시되는 경우 대신 configIfStaScanChannels 를 참조하세요.

V.6.8 Integrity check management

무결성 검사 서비스는 SNMP 에서 사용할 수 있습니다. MIB 에는 이를 위한 두 가지 요소가 포함되어 있습니다.

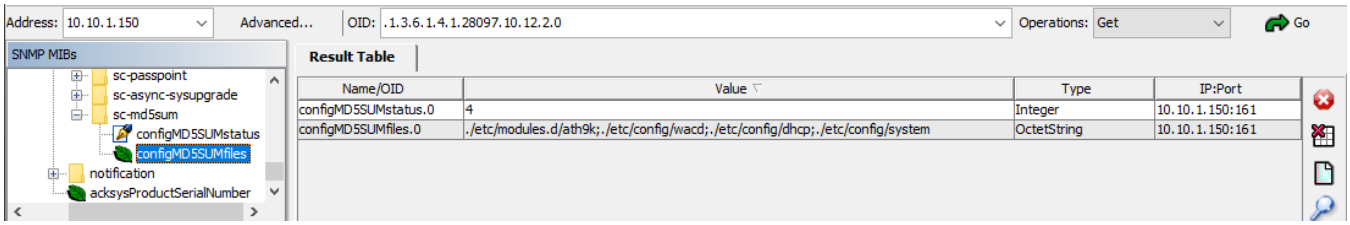
serviceConfiguration/configMD5SUMstatus

OID configMD5SUMstatus 집합은 제품을 구성하는 모든 파일에 대해 무결성 계산을 트리거합니다. get 은 Acksys 에서 제공한 원래 마이크로코드와 비교하여 장치에서 수정된 파일 수를 반환합니다. 수정된 파일 목록은 configMD5SUMfiles OID 를 사용하여 얻을 수 있습니다.

serviceConfiguration/configMD5SUMfiles

OID confiMD5SUM 파일은 Acksys 에서 제공한 원래 마이크로코드와 비교하여 수정된 파일의 목록을 반환하며 수정된 파일은 세미콜론으로 구분됩니다.

예:*/usr/bin/ls;/usr/bin/cat;/usr/bin/ssh*



V.6.9 Managing service configuration tables

서비스 구성 관리는 웹 서버, DHCP 서버, DNS 릴레이에 대한 서비스 매개 변수를 수집합니다.

Web server: 이 파트에서는 HTTP 및 HTTPS 서버를 활성화하고 구성할 수 있습니다.

DHCP: DHCP 서비스는 네트워크별로 별도로 제공됩니다. 각 네트워크 인터페이스에 대해 독립적이고 설정할 준비가 된 하나의 DHCP 서버가 마련되어 있습니다. 정적 리스 테이블을 사용하면 클라이언트 MAC 주소에 따라 항상 동일한 미리 정의된 IP 주소를 할당할 수 있습니다.

DNS relay: DNS 보호 공격의 활성화에 관한 것입니다.

V.6.10 Using SNMP notifications (traps)

제품은 SNMP V2c 트랩을 지원합니다 (notifications 이라고도 함).

Acksys MIB 는 사용 가능한 SNMP 트랩을 OID .1.3.6.1.4.1.28097.11 (notification) 아래에 나열합니다.

트랩을 사용하려면 이벤트의 트랩 설정을 구성해야 합니다 (웹 인터페이스의 "*Alarms/events*" 참조).

아래 표에는 이벤트와 트랩 간의 매핑이 나와 있습니다.

Event name	Notification name	OID
LAN link	linkAlarm	.1.3.6.1.4.1.28097.11.1
Wireless link	linkAlarm	.1.3.6.1.4.1.28097.11.1
Input power	powerAlarm	.1.3.6.1.4.1.28097.11.3
Digital input	digitalInput	.1.3.6.1.4.1.28097.11.4
Temperature limit	tempExceededAlarm	.1.3.6.1.4.1.28097.11.5
Wireless client assoc.	clientLinkAlarm	.1.3.6.1.4.1.28097.11.6
VRRP state change	vrrpAlarm	.1.3.6.1.4.1.28097.11.7

변수들은 이벤트에 대한 상세한 정보를 제공하기 위해 알림에 바인딩될 수 있다. 영향을 받는 각 이벤트에 대해 사용 가능한 변수가 MIB 에 나열됩니다. 이러한 변수는 OID.1.3.6.1.4.1.28097.11.255(notificationBindings)에서 찾을 수 있습니다.

V.6.11 Examples

이러한 예제 스크립트는 SNMP-SET(Linux net-snmp 패키지에 제공됨)를 사용합니다. 그것들은 리눅스에서 실행되도록 되어 있습니다. 다른 경우에 대한 지침으로 사용하세요.

이 스크립트는 제품 IP 주소를 변경하고 변경 내용을 적용합니다.

```
# define a shell macro for snmpset
alias CFGSET="snmpset -m ACKSYS-WLG-MIB -c public -v2c"
# configure it with a new address and netmask
CFGSET 192.168.1.253 configIpSubnetIPv4Addr.\"lan\" a 10.0.1.2
CFGSET 192.168.1.253 configIpSubnetIPv4Mask.\"lan\" a 255.0.0.0
# save and apply without rebooting
CFGSET 192.168.1.253 adminSave.0 i 1
CFGSET 192.168.1.253 adminApply.0 i 2
```

다음 스크립트는 무선 A 의 factory-defined AP 인터페이스를 내부 브리지에 연결된 Wi-Fi 클라이언트로 대체하고 WPA-PSK 키를 설정합니다.

```
# define a shell macro for snmpset
alias CFGSET="snmpset -m ACKSYS-WLG-MIB -c public -v2c"
# delete existing AP interface
CFGSET 192.168.1.253 configIfAPRowStatus.\"radio0w0\" i 6
# add a client interface
CFGSET 192.168.1.253 configIfStaRowStatus.\"radio0w0\" i 4
# configure it with WPA/WPA2-PSK
CFGSET 192.168.1.253 configIfStaSsid.\"radio0w0\" s myNewSsid
CFGSET 192.168.1.253 configIfStaSecurityMode.\"radio0w0\" i 3
CFGSET 192.168.1.253 configIfStaWpaVersion.\"radio0w0\" i 1
CFGSET 192.168.1.253 configIfStaWpaCipher.\"radio0w0\" i aestkip
CFGSET 192.168.1.253 configIfStaKey.\"radio0w0\" s "shared psk key"
# set bridge type to L25NAT (therefore, not WDS)
CFGSET 192.168.1.253 configIfStaWds.\"radio0w0\" i disable
# save and apply without rebooting
CFGSET 192.168.1.253 adminSave.0 i 1
CFGSET 192.168.1.253 adminApply.0 i enable
```

다음은 factory-defined AP 로 시작하는 리피터와 동등한 것을 생성합니다.

```
# define a shell macro for snmpset
alias CFGSET="snmpset -m ACKSYS-WLG-MIB -c public -v2c"
# configure the existing AP interface
CFGSET 192.168.1.253 configIfStaWds.\"radio0w0\" i enable
# add a client interface
CFGSET 192.168.1.253 configIfStaRowStatus.\"radio0w1\" i 4
# configure it
CFGSET 192.168.1.253 configIfStaSsid.\"radio0w1\" s "acksys"
CFGSET 192.168.1.253 configIfStaSecurityMode.\"radio0w1\" i none
CFGSET 192.168.1.253 configIfStaWds.\"radio0w1\" i enable
# set MAC address of next AP
CFGSET 192.168.1.253 configIfStaBssid.\"radio0w1\" x 90a4de214f85
# save and apply without rebooting
CFGSET 192.168.1.253 adminSave.0 i 1
CFGSET 192.168.1.253 adminApply.0 i enable
```

V.7 C-KEY handling

제품 라인의 일부 제품에는 C-KEY 가 장착될 수 있습니다.

Warning: "WLg" 제품 시리즈와 달리 C-KEY 는 자동으로 저장되거나 업데이트되지 않습니다.

V.7.1 Factory settings

이 상태(출고 시 상태)에서는 C-KEY LED 가 꺼지고 C-KEY 에 사용할 수 없는 데이터가 포함되어 있습니다.
C-KEY 가 초기화된 후에는 이 상태로 C-KEY 를 되돌릴 방법이 없습니다.

V.7.2 Understanding configurations and their signature

C-Key 에는 다음이 포함됩니다.

- 제품 모델 식별자
- 모델에 적합한 구성 파일의 보관
- 아카이브에 대한 서명(C-Key 서명, MD5 sum).

제품은 C-Key 를 제거한 상태에서도 작동할 수 있도록 구성 파일의 내부 복사본을 유지합니다. 내부 복사본에는 서명(내부 서명)도 있으며, 다음과 같은 3 가지 경우에 업데이트됩니다.

- 제품이 factory 설정으로 재설정되면 재부팅하기 전에 내부 서명이 삭제됩니다.
- 사용자가 내부 구성을 C-Key 에 복사하면 내부 서명이 새로 생성된 C-Key 서명과 동일하도록 다시 계산됩니다.
- 부팅 시 C-Key 서명이 내부 서명과 다른 경우 C-Key 구성 및 해당 서명이 내부 구성으로 복사됩니다(웹 인터페이스 또는 SNMP 를 사용하여 이 복사본을 비활성화할 수 있음).

이 절차에는 몇 가지 결과가 있습니다.

- 출고 시 설정으로 재설정 작업을 수행한 후 제품이 재부팅되고 C-Key 내용이 유효한 경우 내부 구성으로 복사되어 즉시 사용됩니다. 이 경로는 제품이 C-Key 구성을 사용하고 있는지 확인하는 확실한 경로입니다.
- 내부 구성을 변경하는 경우 내부 서명이 변경되지 않으므로 다음 재부팅은 C-Key 에서 로드되지 않습니다. 대신 변경된 구성을 사용합니다. 이 상황은 웹 인터페이스에 경고와 함께 표시됩니다. 실험실 테스트에 유용합니다.
- C-Key 를 다른 구성(따라서 다른 서명)이 포함된 다른 구성으로 교체하면 다음 번 전원을 켤 때 내부 구성이 지워지고 교체됩니다. 이전에 C-Key 기능을 비활성화한 경우에는 이러한 문제가 발생하지 않습니다.

V.7.3 Not using the C-Key

C-Key 를 사용하지 않도록 하려면 C-Key 를 비워 두어야 합니다("erase" 구성 기능). 그러면 C-Key LED 가 빨간색으로 켜집니다. 이 LED 를 비활성화하도록 구성할 수 있습니다.

V.7.4 Replacing a product on the field

설치되어 사용 중인 제품과 해당 구성이 C-Key 에 백업되어 있다고 가정해 보겠습니다. 이제 제품이 손상되어 교체가 필요하다고 가정해 보겠습니다. 다음은 손상된 제품 "DP"에서 새 제품 "NP"로 구성을 전송하는 절차입니다.

요구 사항: C-Key 를 분리하고 다시 꽂을 수 있는 소형 스크루드라이버.

1) NP 의 C-Key(있는 경우)를 제거하고 분리합니다.
2) DP 의 전원을 끄고 케이블을 분리한 후 지지대에서 나사를 풉니다.
3) DP 에서 C-Key 를 분리합니다.
4) C-Key 를 NP 에 꽂고 나사를 조입니다.
5) NP 를 해당 위치에 장착하고 케이블을 다시 연결합니다.

   NP 가 이전에 사용된 적이 있고 구성이 C-Key 를 비활성화하는지 여부를 확신할 수 없는 경우:

6) NP 전원을 켜고 "Diag" LED 가 녹색으로 바뀔 때까지 기다립니다.
7) "Diaq" LED 가 빨간색으로 바뀔 때까지 최소 3 초 동안 재설정 버튼을 계속 누릅니다. 그러면 제품이 출고 시 설정으로 재설정됩니다. "Diag" 및 "C-Key" LED 가 모두 녹색으로 바뀔 때까지 기다립니다.

V.7.5 Working with the C-Key in the lab

실습에서는 내부 구성이나 C-Key 내용을 정확히 알지 못할 수 있습니다.

C-Key 를 꽂거나 꽂지 않은 상태에서 제품을 사용할 수 있습니다. C-Key 를 연결하거나 분리하기 전에 항상 제품의 전원을 끄십시오.

다양한 구성을 테스트하는 동안 C-Key 를 비활성화하고 마운트 상태로 두는 것이 좋습니다. 구성이 만족스러우면 C-Key 에 저장할 수 있습니다. "C-Key disable" 플래그 자체는 C-Key 에 저장되지 않습니다.

출고 시 설정으로 재설정하면 "C-Key disable" 플래그가 지워집니다.

구성 작업(저장 또는 지우기)만 C-Key 내용을 변경합니다.

V.7.6 Programming a set of identical C-Keys

전용 제품을 사용하여 구성을 준비하고 C-Key 를 프로그래밍합니다.

1) 전원이 꺼진 제품에서 C-Key 를 제거합니다.
2) 재부팅하고 필요에 따라 제품을 구성합니다.
3) "Tools/Set config/C-Key management"에서 "Ignore C-Key settings" 및 "save option"을 선택합니다.
4) Save 및 power off
5) C-Key 를 설치하고 전원을 켭니다. 진단 LED 가 녹색으로 바뀔 때까지 기다립니다. 재부팅 후 제품은 새 IP 주소를 사용합니다.
6) " Tools/Set config/C-Key management " 메뉴에서 "copy"를 클릭합니다.
7) 제품의 전원을 끄고 프로그래밍된 C-Key 를 제거한 후 5 단계로 돌아갑니다.

V.8 QOS Traffic Class Management

V.8.1 Traffic Classification

트래픽 분류는 네트워크 계층에 의한 트래픽을 여러 트래픽 클래스로 분류하는 것에 해당합니다. 각각의 결과 트래픽 클래스는 사용자에게 암시되는 서비스를 구별하기 위해 다르게 처리될 수 있습니다.

제품은 특정 프로토콜의 패킷 헤더의 일부 내용에 기초하여 트래픽 스트림의 패킷을 패킷 출력 측면에서 서로 다른 우선순위를 갖는 분리된 개별 흐름과 큐로 분류하는 네트워크 스케줄러 역할을 할 것입니다.

이 제품은 이더넷 계층에서 표준 IEEE 802.1p(Vlan 우선 순위)에 정의된 트래픽 클래스를, IP 계층에서 DiffServ 표준 및 IEEE 802.11e 표준의 WMM 에서 IEEE 802.11 네트워크(WLAN)에 대해 관리합니다.

V.8.2 802.1p traffic classes

IEEE 802.1p 표준은 IEEE 802.1Q 표준에서 정의한 대로 VLAN 태그 프레임을 사용할 때 이더넷 프레임 헤더 내의 PCP(Priority Code Point)라는 3 비트 필드로 서비스 클래스(CoS)를 정의합니다. QoS 규칙에서 트래픽을 구별하는 데 사용할 수 있는 0 과 7 사이의 우선 순위 값을 지정합니다.

PCP	Traffic Types	Product Internal Traffic classes
0	Best Effort	Diffserv 에 따라 다름 (아래 참조)
1	Background	1
2	Spare	2
3	Excellent Effort	3
4	Controlled Load	4
5	Video	5
6	Voice	6
7	Network Control	7

이 제품은 IEEE 802.1p 우선 순위 → 7 을 내부 트래픽 classes 1 → 7 에 매핑합니다.

IEEE 802.1p 우선 순위 0 은 우선 순위가 설정되지 않은 것으로 간주되고, Diffserv 우선 순위가 대신 사용됩니다.

V.8.3 DiffServ traffic classes

DiffServ 는 패킷 분류 목적으로 IP 헤더의 8 비트 Differentiated Services Field (DS 필드)에 있는 6 비트 Differentiated Services Code Point (DSCP)를 사용합니다. DS 필드와 ECN 필드는 오래된 IPv4 TOS 필드를 대체합니다.

제품은 DiffServ 의 Class Selector 를 나타내는 DS 필드의 처음 3 비트만 사용하여 내부 트래픽 클래스 0 → 7 에 매핑합니다.

IEEE 802.1p 우선 순위 > 0 이 있는 경우 Diffserv 우선 순위는 사용되지 않습니다.

Class Selector Values		Product Internal Traffic classes
DS field	Class	
000XXXXX	CS0	0
001XXXXX	CS1	1
010XXXXX	CS2	2
011XXXXX	CS3	3
100XXXXX	CS4	4
101XXXXX	CS5	5
110XXXXX	CS6	6
111XXXXX	CS7	7

V.8.4 WMM Traffic Classes

WMM 은 QoS 데이터 트래픽을 처리하기 위해 802.11 네트워크(WLAN)에 대해 4 개의 액세스 범주를 정의합니다. 4 개의 우선 순위는 0 → 3 (0 이 가장 높은 우선 순위, 3 이 가장 낮은 우선 순위)입니다.

WMM Access Categories	Priority
AC_BK (background)	3
AC_BE (best effort)	2
AC_VI (video)	1
AC_VO (voice)	0

또한 WMM 은 LAN 의 계층 2(802.1d) 서비스 클래스와 WLAN 의 WMM 액세스 범주 간의 매핑을 지정합니다.

802.1p PCP	WMM Access Categories	
	WMM Access Categories	Priority
0	AC_BE (best effort)	2
1	BK (background)	3
2	BK (background)	3
3	AC_BE (best effort)	2
4	AC_VI (video)	1
5	AC_VI (video)	1
6	AC_VO (voice)	0
7	AC_VO (voice)	0

이 제품은 LAN 의 Layer 3 Diffserv 필드와 WLAN 의 WMM 액세스 범주 사이에 다음 매핑을 추가합니다. 이 매핑은 802.1p 우선 순위 = 0 일 때, 그리고 VLAN 은 없지만 Diffserv 필드가 있을 때 사용됩니다.

Diffserv Class	WMM Access Categories	
	WMM Access Categories	Priority
CS0	AC_BE (best effort)	2
CS1	BK (background)	3
CS2	BK (background)	3
CS3	AC_BE (best effort)	2
CS4	AC_VI (video)	1
CS5	AC_VI (video)	1
CS6	AC_VO (voice)	0
CS7	AC_VO (voice)	0

V.8.5 Traffic Class to Queue Mapping

V.8.5.1 Queue definition

네트워크 스케줄러는 트래픽 정체로 인해 나갈 수 없는 패킷을 분류하려고 할 때 해당 패킷을 대기열에 넣습니다.

제품의 각 인터페이스에는 패킷이 전송되기 전에 저장되는 대기열이 있습니다.

각 대기열은 패킷 송신 측면에서 고유한 우선 순위를 가집니다.

우선 순위가 더 높은 큐의 패킷이 먼저 전송됩니다.

V.8.5.2 Queues of Ethernet Interfaces

이더넷 인터페이스는 8 개의 큐를 병렬로 관리합니다. 큐 0-7(우선 순위 0-7)은 0 이 가장 높고 7 이 가장 작습니다.

V.8.5.3 Queues of Wireless interfaces

무선 인터페이스는 4 개의 대기열을 병렬로 관리합니다. 대기열 0-3 은 우선 순위가 0-3 이고, 0 은 우선 순위가 가장 높고 3 은 가장 작습니다.

V.8.5.4 Queue mapping

큐 매핑은 트래픽 클래스와 큐 우선 순위 간의 연결을 정의합니다.

대기열 우선 순위를 통해 네트워크 스케줄러는 패킷이 네트워크로 전송되는 순서를 알 수 있습니다.

무선 인터페이스의 경우 WMM 은 트래픽 클래스를 큐 매핑에 적용합니다. 대기열 우선 순위는 WMM 액세스 범주 우선 순위에 해당합니다.

V.8.6 Queue Management

동일한 큐에 있는 것처럼 여러 트래픽 클래스를 가질 수 있으며, 트래픽 클래스에서 여러 개의 서로 다른 원본 스트림을 가질 수 있고, 동일한 큐 내의 대역폭 공유도 처리하기 위해 관리가 필요합니다.

큐 관리는 동일한 큐의 트래픽을 처리하는 방법에 해당합니다.

The product offers 2 types of queue management:

- **FIFO** Queue: 패킷은 대역폭 공유와 관계없이 입력된 순서와 동일한 순서로 큐에서 나옵니다.
- **FAIR** Queue: 큐 내부의 트래픽이 여러 흐름으로 분할된 다음 모든 흐름이 출구에 대해 공정하게 처리됩니다.

V.8.7 GRE Tunnels

이 제품은 GRE 터널에 의해 캡슐화된 패킷의 트래픽 클래스 상속을 관리합니다.

GRE 터널이 VLAN 을 VLAN 우선 순위(PCP)가 0 보다 큰 상태로 캡슐화하는 경우 캡슐화된 VLAN 우선 순위를 IP 패킷에 대한 DiffServ 클래스로 변환합니다.

VLAN 우선 순위(PCP) = 0 이거나 캡슐화된 패킷이 VLAN 이 아닌 경우 캡슐화된 Diffserv 필드를 상속합니다.

V.9 Train Communication Network (TCN)

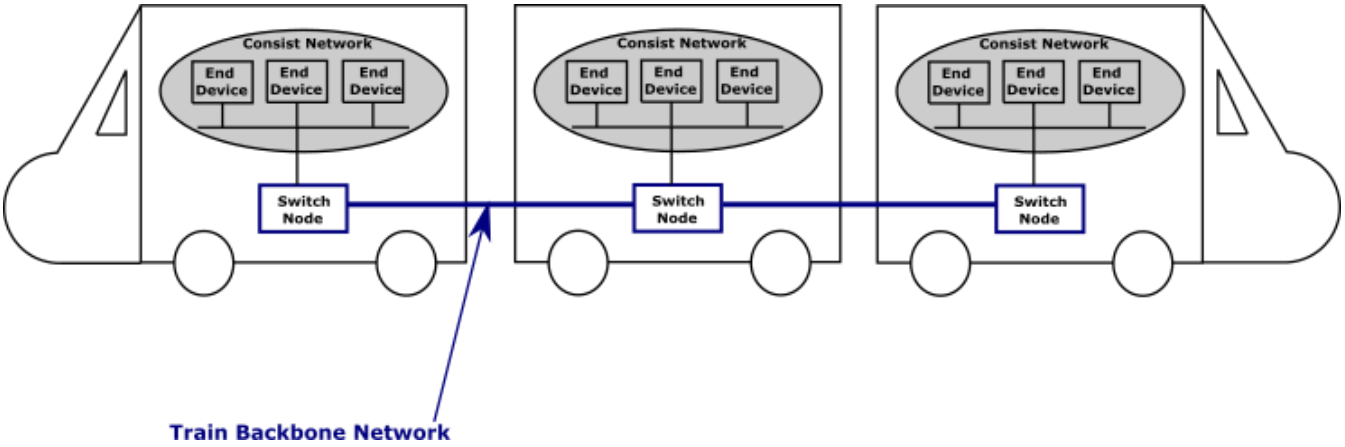
Train communication network (TCN, 열차 통신 네트워크)는 열차 내 디지털 통신을 위한 완전한 네트워크를 정의합니다.

참고: 이 섹션에서 "coach"와 "carriage"라는 단어의 의미는 동일합니다.

V.9.1 Train backbone

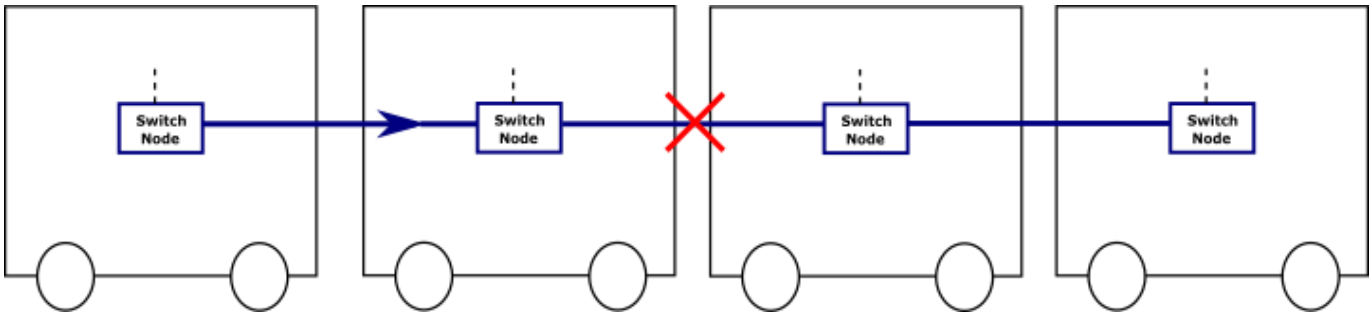
열차 통신 네트워크는 선형 토폴로지로 배열된 일련의 노드(스위치)로 대표되는 열차 백본 네트워크로 구성됩니다.

각 스위치 노드는 하위 네트워크(Consist 네트워크)를 열차 백본에 연결합니다.



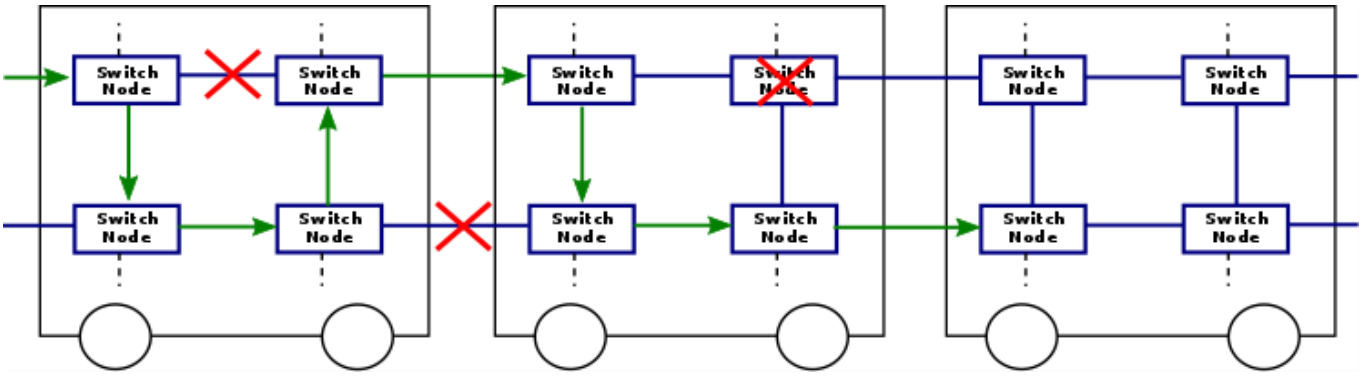
V.9.2 Link failure in linear topology

선형 토폴로지에서 링크 장애가 발생하면 열차의 양쪽 사이의 통신이 끊어집니다.



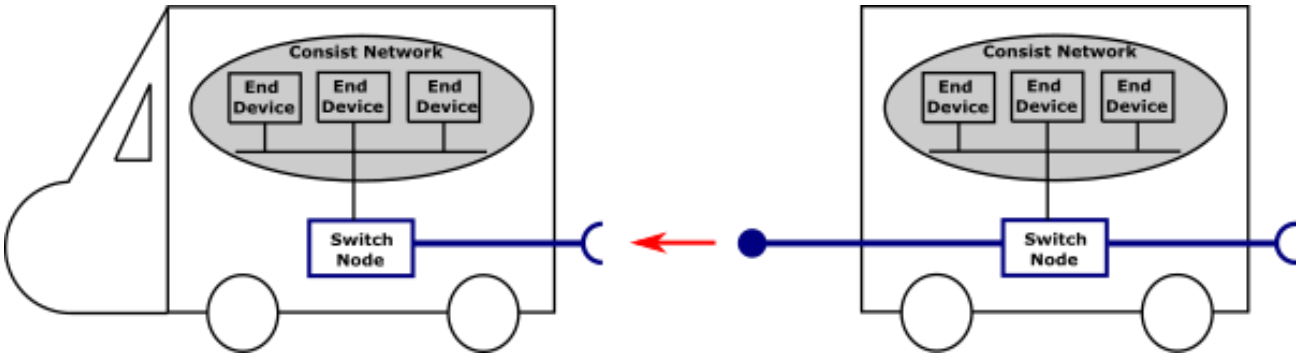
V.9.3 Ring topology

링 토폴로지를 사용하면 링크 장애 시 대체 경로를 제공하여 중복 네트워크를 구축할 수 있습니다.



V.9.4 Carriage coupling

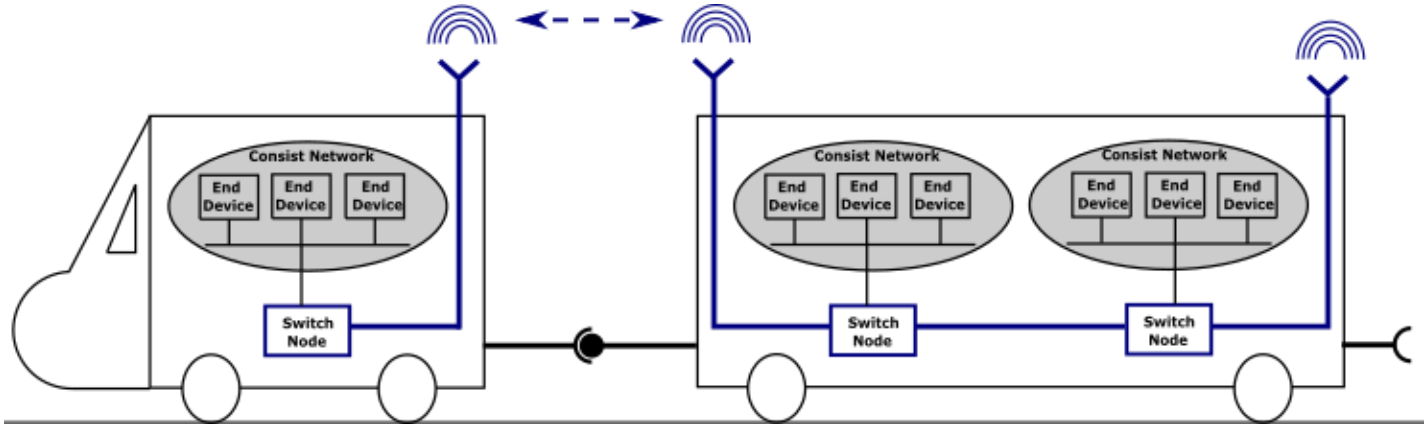
캐리지 커플링은 열차 내 철도 차량을 연결하는 메커니즘입니다.



특히 노후화되거나 품질이 떨어지는 커넥터로 인해 보수 작업 시 객차 간 네트워크 배선이 어렵거나 불가능한 경우가 많기 때문에 WiFi 는 중복성, 신뢰성 및 고속 네트워킹을 가능하게 함으로써 가장 효율적인 솔루션으로 자연스럽게 정착되었습니다.

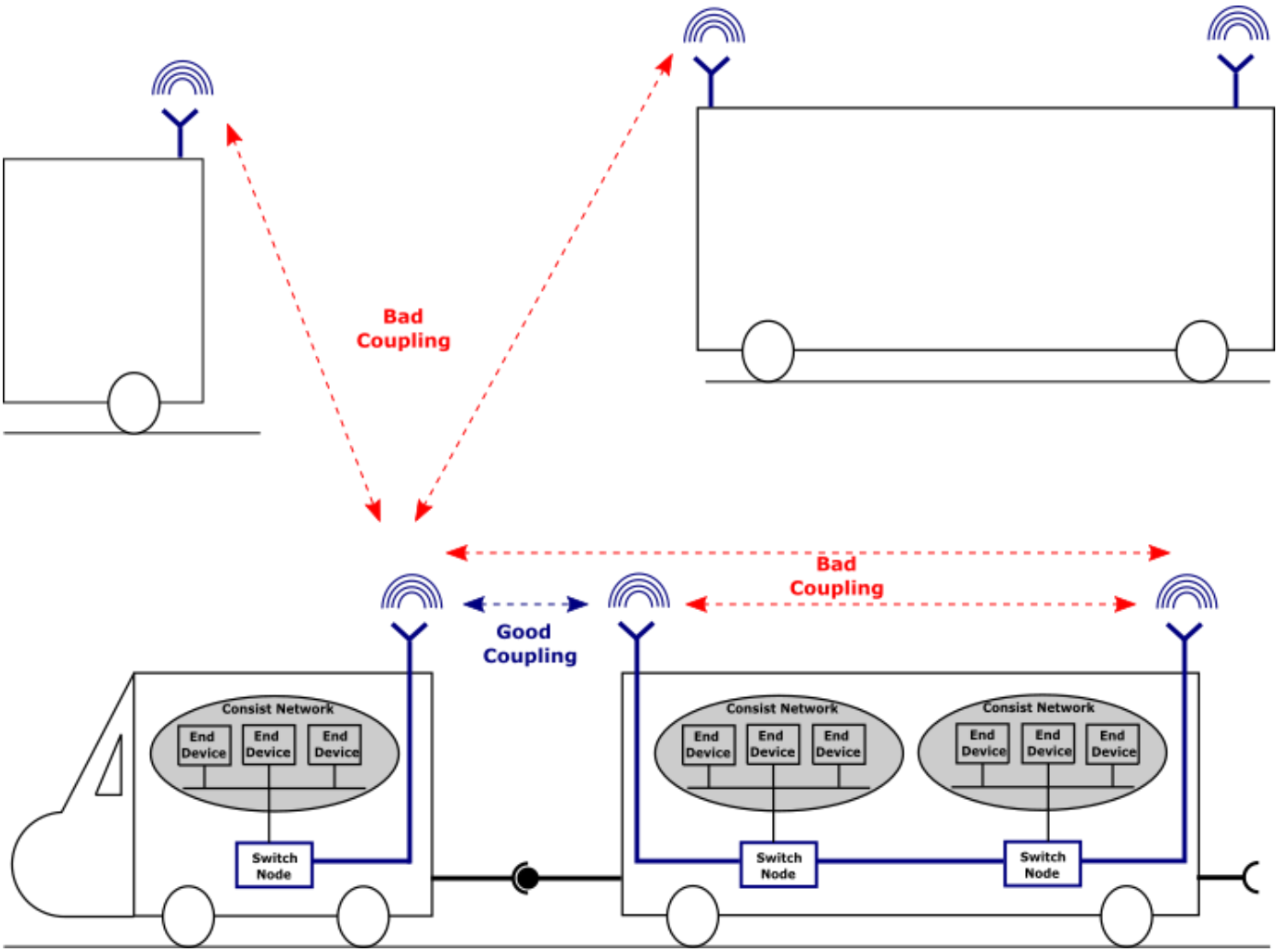
V.9.5 Wireless carriage coupling

무선 캐리지 커플링은 탐색 및 인접 캐리지와의 연결을 기반으로 구성됩니다.



V.9.6 Neighbor discovery

무선 브로드캐스트로 인해 물리적 인접 네트워크가 아닌 노드에서도 프레임이 수신되기 때문에 무선 채널을 통한 인접 네트워크 검색은 무선 매체의 브로드캐스트 특성으로 인해 어려워집니다.



잘못된 커플링을 방지하려면 각 스위치 노드가 가장 가까운 유효한 스위치 노드에서만 신호를 수신하는지 확인해야 합니다.

다음 방법을 사용하여 위 규칙을 준수할 수 있습니다.

- 원하는 객차에 방사를 집중시키기 위해 지향성 안테나를 사용합니다.
- 가능한 저이득 안테나 또는 RF 감쇠기를 사용합니다.
- 두 열차 사이의 공간을 늘립니다.
- 링크 설정 임계값을 사용하여 원하지 않는 스위치 노드를 제외합니다(SRCC 매개 변수 참조).

이러한 모든 방법을 사용하면 불량 커플링 문제를 제거할 수 있습니다. 그럼에도 불구하고 객차의 유형이 다양하기 때문에 최상의 결과를 얻기 위해서는 시스템 보정을 수행하고 방법의 조합과 최적의 매개 변수 값을 찾는 것이 필수입니다.

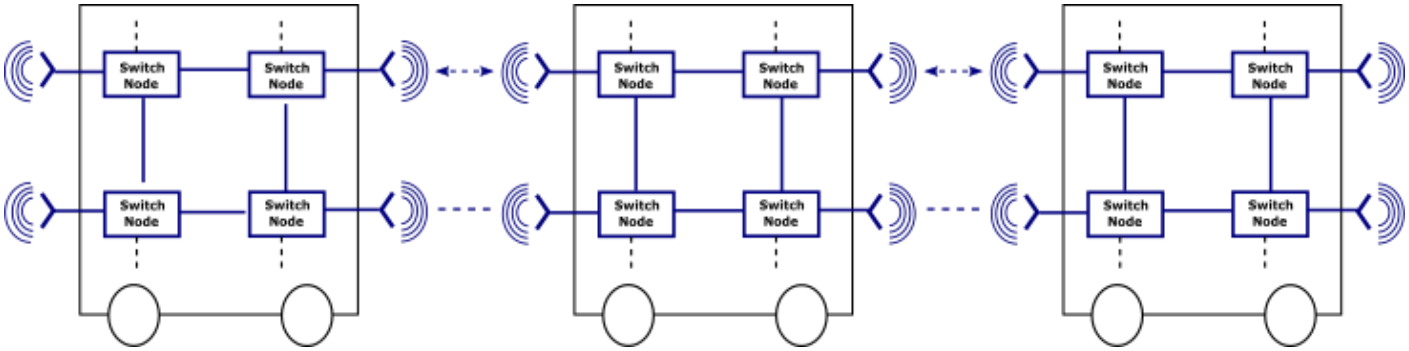
동일한 객차의 잘못된 커플링을 방지하려면 모든 스위치 노드가 캐리지의 내부 노드와의 연결을 방지하기 위해 자체 내부 토폴로지를 인식해야 합니다.

V.9.7 Topology discovery

토폴로지 검색은 캐리지의 다른 모든 내부 노드의 각 노드에 의한 탐지로 구성되며 인접 노드 검색 단계보다 선행되어야 합니다.

V.9.8 ACKSYS's Smart Redundant Carriage Coupling (SRCC)

SRCC(Smart Redundant Carry Coupling)는 보안된 Wi-Fi 연결 및 이더넷 링크를 사용하여 중복 *link-layer* 백본을 설정하기 위해 인접 캐리지의 무선 커플링을 자동화하는 서비스입니다.



Picture V-9: SRCC 로 구성된 이중화 이더넷 백본의 예시

SRCC 구성 참조: *SRCC configuration*

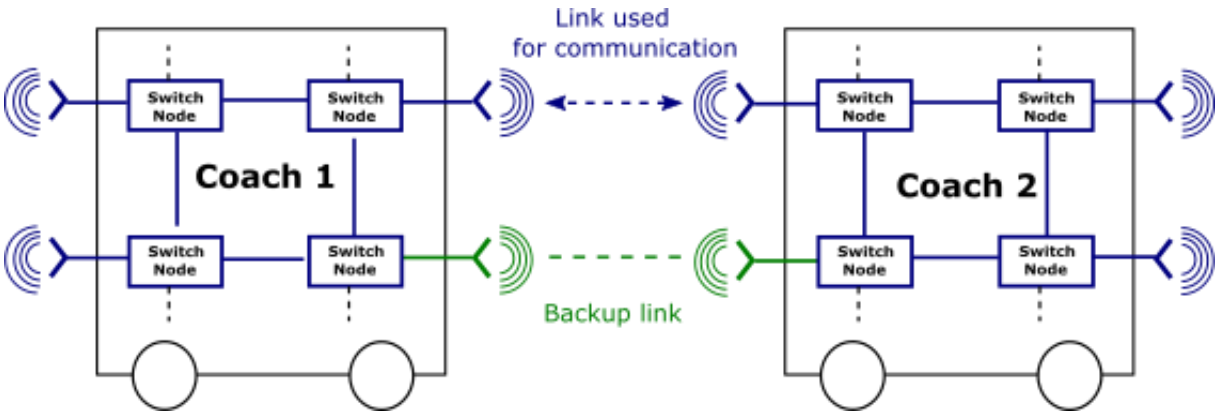
V.9.9 Operating mode

SRCC 는 각 캐리지의 내부 토폴로지를 검색하는 것으로 시작한 다음 두 번째 단계에서 인접 캐리지를 검색합니다. 주변의 모든 잠재적 장치 중에서 커플링에 적합한 파트너를 자동으로 선택합니다.

파트너가 선정되면 SRCC 는 두 객차의 내부 네트워크를 연결하는 두 장치 사이에 보안 링크를 자동으로 설정합니다.

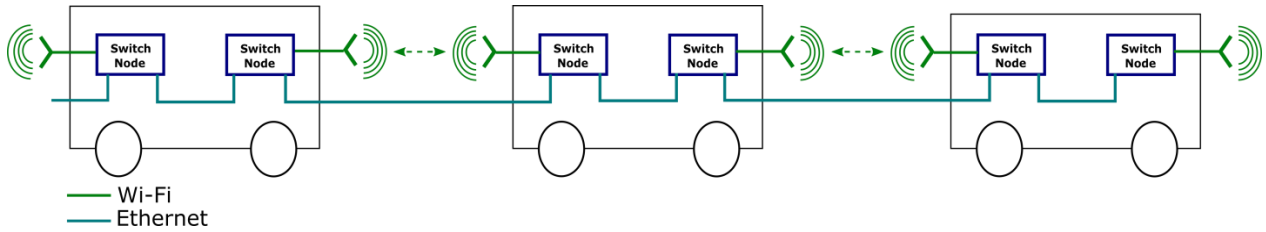
나중에 객차가 분리된 경우 SRCC 는 RF 링크의 드롭을 감지하고 양쪽에서 링크를 닫고 감지 프로세스를 다시 시작합니다.

인접한 객차 간에 2 개의 무선 링크가 가능한 경우, SRCC 는 하나는 통신용으로, 다른 하나는 백업용으로 설정하여 객차 간에 중복 링크를 달성합니다.



V.9.10 Redundant mixed mode

이 모드는 또 다른 인기 있는 아키텍처입니다. 이 경우 객차 간에 이더넷 연결을 사용할 수 있습니다. 이 이더넷 링크는 무선 링크로 보호됩니다.



Picture V-10: SRCC 이중화 혼합 모드

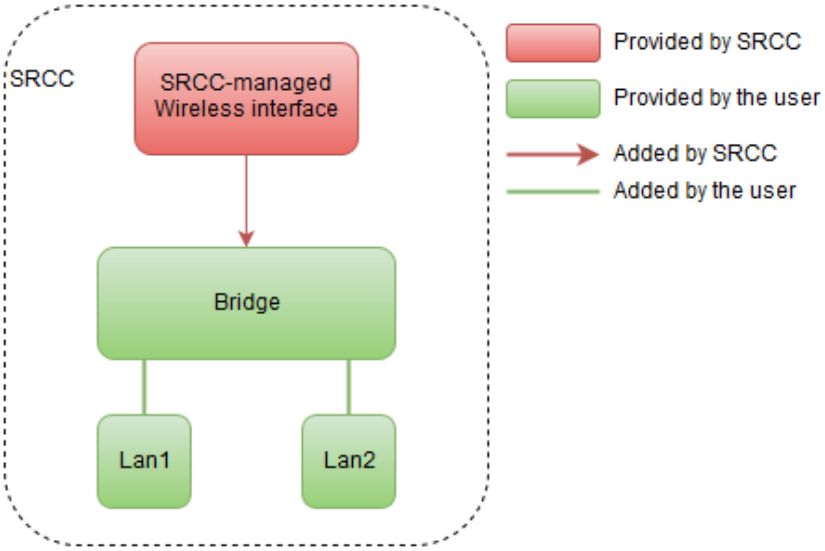
이중화는 링 토폴로지만큼 가득 차지 않지만, 캐리지 간 링크 장애 또는 무선 장애를 허용합니다.

또한 이 아키텍처는 스위치 노드가 이더넷 바이패스 기능을 내장할 때 특히 중요합니다. 이렇게 하면 스위치 노드에 장애가 발생해도 아키텍처가 중단되지 않습니다.

약점은 내부 이더넷 링크입니다. 이 링크는 시스템이 장애에 탄력적으로 대처하기 위해 매우 낮은 장애율을 필요로 합니다.

V.9.10.1 Prerequisites

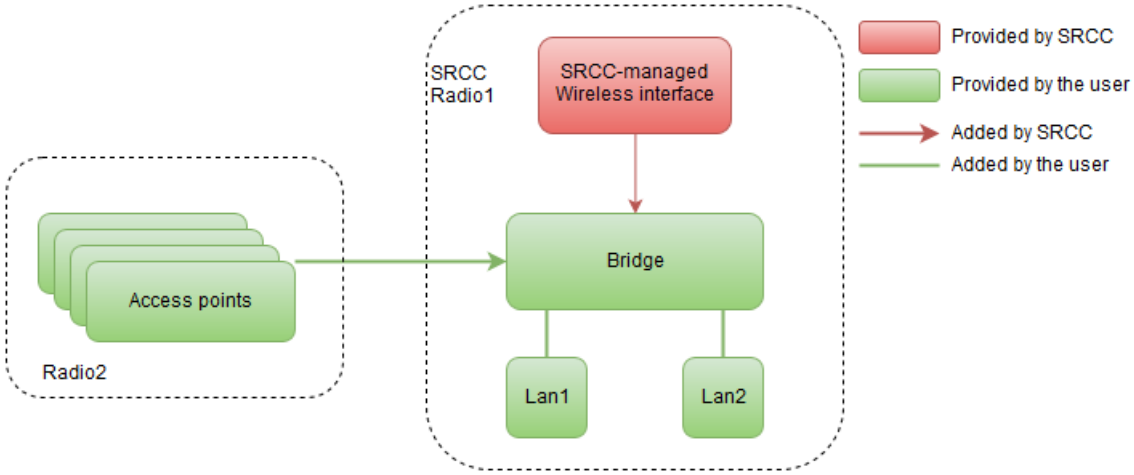
SRCC 가 올바르게 작동하려면 몇 가지 사전 구성이 필요합니다. 기본적으로 사용자는 브리지를 만들고 이더넷 인터페이스를 추가해야 합니다. **중복 토폴로지 또는 링 토폴로지에서는 이 브리지에 대해 RSTP 를 활성화해야 합니다.**



Picture V-11: Internal structure of the SRCC switch

제품에 두 개의 무선 카드가 장착된 경우, 두 번째 역할은 일부 역할(AP 또는 클라이언트)을 구현한 다음 이들을 백본에 연결하기 위해 브리지에 추가할 수 있습니다.

이를 통해 예를 들어 SRCC 덕분에 첫 번째 무선이 백본 전용인 동안 두 번째 무선에서 온보드 서비스 액세스 포인트(VLAN 포함 또는 없음)를 사용할 수 있습니다. 아래 다이어그램은 이러한 가능성을 보여줍니다.



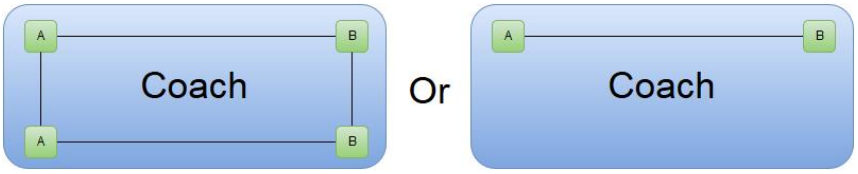
Picture V-12: 서비스 AP 가 있는 내부 구조

V.9.10.2 Topology discovery

시작 시 각 스위치 노드에 있는 SRCC 서비스는 구성 가능한 기간 동안 객차 내부의 다른 스위치 노드에 대한 토폴로지 검색을 수행합니다. 그러면 각 SRCC 제품이 객차 구조를 인식하게 됩니다. 존재하지 않거나 결함이 있는 장치는 이 단계에서 감지됩니다.

성공적인 객차 매핑을 수행하기 위해 SRCC 는 사전 구성된 객차 엔드 유형(예: End A 및 End B)을 사용하여 2 개의 스위치 노드가 지정된 객차의 동일한 측에 있는지 여부를 확인합니다.

객차의 같은 끝에 있는 두 장치는 객차의 끝 유형이 같아야 하고, 객차의 반대편에 있는 두 장치는 객차의 끝 유형이 반대여야 합니다.



중복 혼합 모드의 경우 객차 엔드 유형은 관련이 없습니다. 이 모드에서, 캐리지 간 이더넷 링크는 열차의 모든 장치를 한 번에 검색할 수 있는 방법을 제공합니다. 토폴로지 검색이 끝나면 각 제품에는 열차의 모든 장치 목록이 표시됩니다. 자체 열차의 제품을 알면 SRCC 는 무선 링크를 설정할 때 나열되지 않은 제품(즉, 다른 열차의 제품)을 제외할 수 있습니다.

객차의 모든 제품은 동시에 전원이 켜져야 합니다. 그렇지 않은 경우, 최근에 전원이 켜진 일부 제품은 파트너에 의해 존재하지 않는 것으로 간주될 수 있습니다. 특정 전원 켜기 시퀀스를 수용하기 위해 토폴로지 검색 단계 기간을 줄이거나 연장할 수 있습니다.

이 단계에서는 SRCC 관련 라디오 카드에 무선 인터페이스가 생성되거나 허용되지 않습니다.

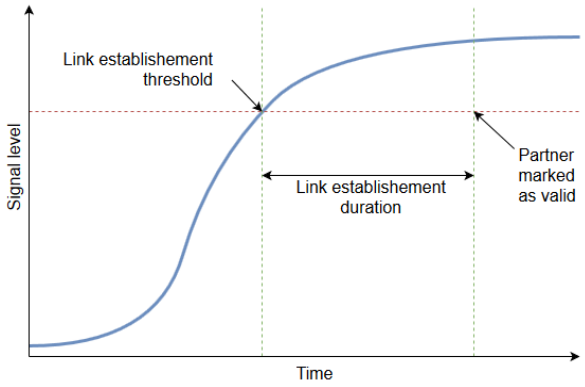
Terminal product

이더넷 토폴로지 검색 프로세스는 객차의 다른 쪽 끝에서 하나 이상의 제품을 찾을 것으로 예상합니다. 그렇지 않으면 자동으로 열차의 마지막 객차에 설치된 것으로 간주됩니다. 이는 고객 라우팅/제어 장치가 열차의 각 끝에 중복으로 설치되어 있고 두 개의 SRCC 제품이 객차의 같은 끝에 고장이 발생할 경우 추가적인 중복성을 제공할 수 있습니다.

V.9.10.3 Neighbor discovery

토폴로지 검색이 완료되면 SRCC 가 무선 탐지 프로세스를 시작합니다. 탐지가 완료되면 모든 유효한 잠재적 파트너 중에서 최종 파트너가 선택됩니다.

파트너는 지정된 기간(링크 설정 기간) 이상 동안 신호 수준이 지정된 임계값(링크 설정 임계값)보다 강한 경우 유효한 것으로 간주됩니다.



Picture V-13: Partner validation process

사용 가능한 모든 파트너 간의 선택은 대부분 모든 스테이션과 장치 정보 간의 신호 수준에 기초합니다(즉, 직접 신호 수준에만 기초하는 것은 아님).

중복 혼합 모드의 경우 토폴로지 검색에 의해 설정된 목록에 제품이 있으면 "boost" 계수가 적용됩니다. 이렇게 하면 목록에 있는 제품이 강화되고 선택될 가능성이 높아집니다(다른 철도 선로의 열차에서 장치 제외).

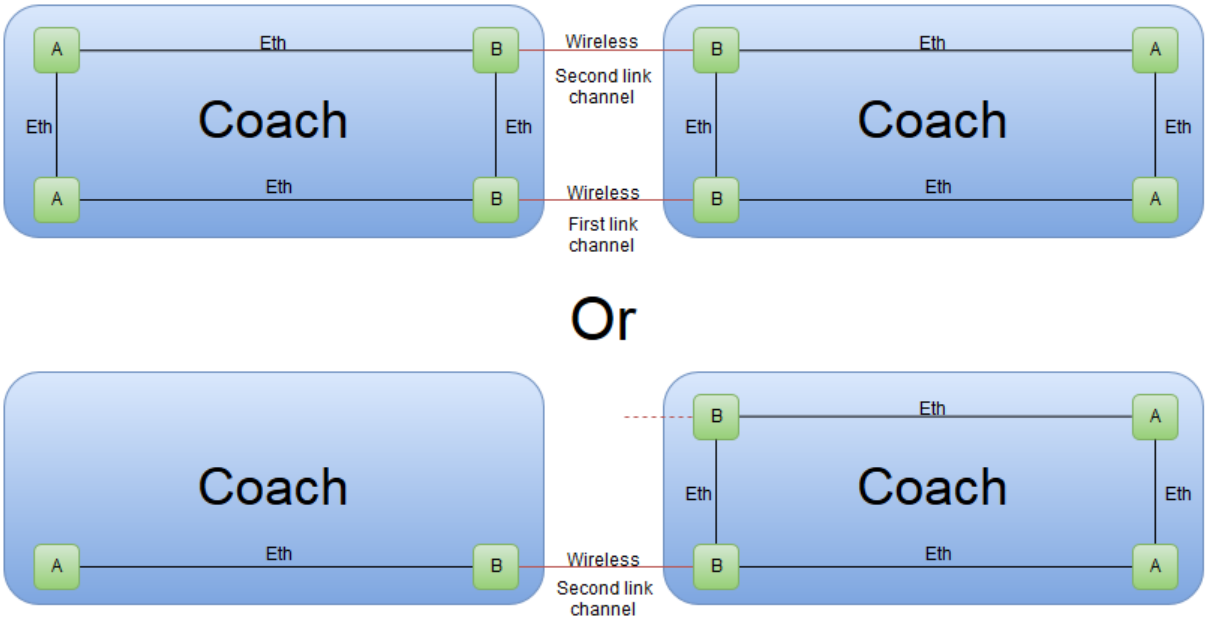
토폴로지 검색 중에 인터캐리지 링크에 결함이 있는 경우 검색되지 않은 장치는 부스트만 활용하지 않습니다.

하지만 이것은 체계적이지 않습니다. 따라서 토폴로지 검색 중에 다른 캐리지의 제품이 누락된 경우에도 RF 신호 수준이 양호하기 때문에 열차에서 더 멀리 탐지된 다른 제품보다 선택된 무선 파트너가 될 수 있습니다.

V.9.10.4 Link establishment

모든 파트너가 식별되면 각 스위치 노드에 무선 역할(액세스 포인트 또는 클라이언트)이 할당됩니다. 이러한 장치는 개인 정보 보호를 위해 고유한 SSID 와 강력하고 고유한 키를 사용하여 최대 2 개의 무선 AP-Client 링크를 생성합니다.

사용자는 가능한 각 링크에 대해 하나씩 두 개의 채널(첫 번째 링크 채널 및 두 번째 링크 채널)을 제공해야 합니다. SRCC 에서 임의 순서로 사용합니다. 링크 간 채널 할당은 예측할 수 없으며 SRCC 의 내부 계산 결과입니다.



Picture V-14: Example of channel allocation among wireless links

장치 내부에서 무선 링크는 이더넷 네트워크와 연결되어 한 객차에서 다른 객차로 데이터를 전송할 수 있습니다.

장치는 링크가 손실되지 않는 한 이 상태를 유지합니다(아래 참조). 장치가 이 모드로 유지되는 한 링크가 설정되고 데이터가 객차를 통해 흐를 수 있습니다.

V.9.10.5 Summary: initialization outline

SRCC 초기화 시퀀스에서 메인 스트림(즉, 설정이 안정적이고 선택이 명백한 경우 처리)은 다음과 같습니다. 아래 단계는 시스템 로그에 나타나는 대로 번호가 매겨집니다.

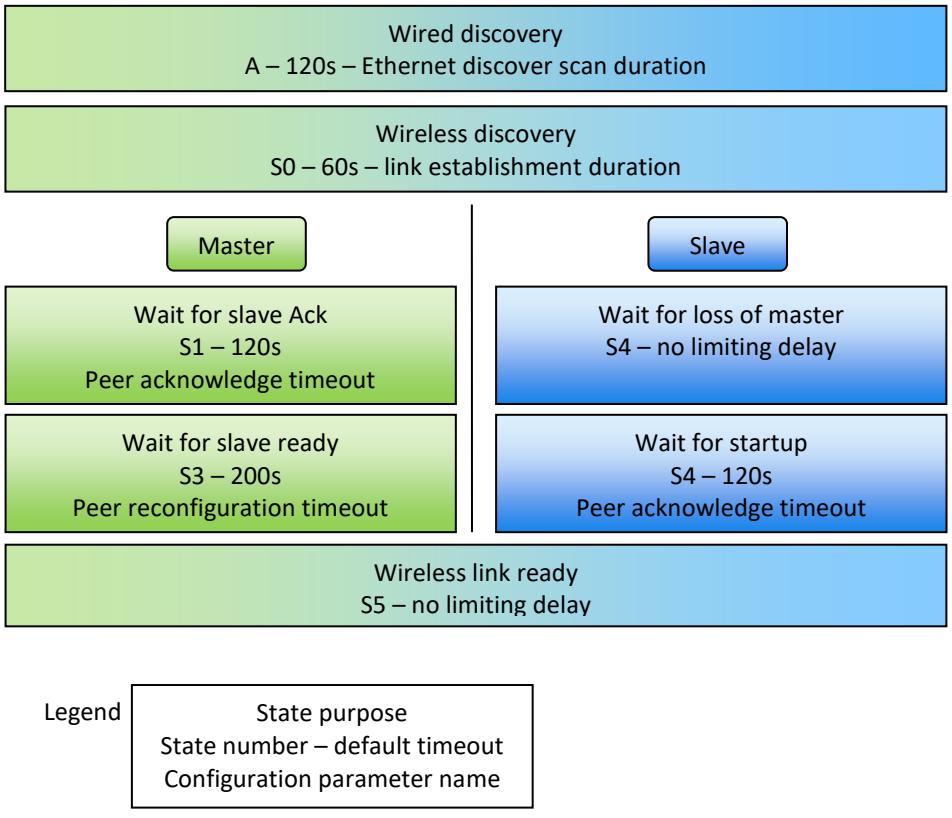
무선 링크의 두 제품(각 객차에 하나씩)은 자체 유선 네트워크를 점검하여 객차에서 파트너를 찾습니다(A 단계).

그런 다음 두 제품 모두 무선 비콘을 브로드캐스트하여 유선 네트워크를 다른 객차의 제품에 알립니다(S0 단계). 각 제품은 다른 객차의 피어 무선 제품과 마스터(액세스 포인트) 또는 슬레이브(클라이언트) 쌍에서의 역할을 학습합니다.

마스터는 슬레이브의 확인을 기다린 다음 시작 메시지를 보냅니다(S1 단계). 그런 다음 슬레이브가 시작될 때까지 기다린 후(S3 단계), AP 역할(S5 단계)에서 자동으로 시작됩니다.

한편, S0 에 이어 슬레이브는 마스터로부터 시작 메시지를 기다리는 것을 확인합니다(S4 단계). 도착하면 슬레이브는 클라이언트 역할에서 스스로 시작합니다(S5 단계).

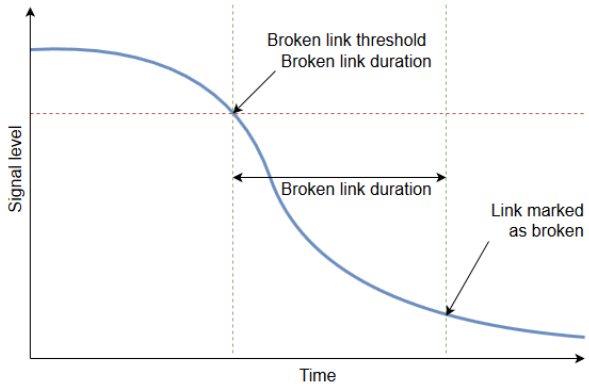
약한 신호, 피어 불일치 또는 시간 초과(S2 및 S6 단계)로 인해 이 초기화 프로세스를 중단하는 다양한 이유가 있습니다. 이러한 경우 초기화는 S0 또는 S1 단계에서 다시 시작됩니다.



V-1 smooth 초기 개요

V.9.10.6 Partner loss

열차가 분리되면 객차가 서로 멀어지면서 양쪽 사이의 신호가 떨어지게 됩니다. SRCC 는 이 신호 레벨을 추적하며 지정된 기간(중단된 링크 기간) 이상 동안 지정된 임계값(중단된 링크 임계값) 아래로 떨어지면 링크가 중단된 것으로 간주됩니다. 다음 다이어그램은 이 단계를 보여줍니다.



Picture V-15: 무선 링크간 채널 할당 예시

링크가 끊어진 것으로 표시되는 즉시 장치는 인접 탐색 단계를 다시 시작하고 잠재적인 새 파트너를 다시 찾으려고 합니다.

V.10 Security Management

제품에 대한 네트워크 액세스가 안전한지 확인하여 해커의 무단 액세스를 방지해야 합니다. 이를 위해 제품에 대한 액세스를 네트워크 세그먼트 또는 인증된 사용자 그룹으로 제한하도록 제품을 구성해야 합니다.

V.10.1 HTTP/HTTPS server

암호를 사용하여 웹 인터페이스에 대한 액세스를 보호할 수 있습니다.

- Username: root
- Password: 기본적으로 암호가 설정되어 있지 않습니다.

서버와의 데이터 교환이 암호화되도록 HTTPS 서버를 활성화할 수도 있습니다.

보안 수준이 낮은 자체 서명 인증서를 제공하지 않으면 기본 자체 서명 인증서가 사용됩니다.

자체 인증서를 업로드하는 것이 좋습니다(인증서와 암호화되지 않은 개인 키가 모두 포함된 PEM 파일이어야 함).

제품 구성 시 참조: *Web Server*

V.10.2 Bridge mode

브리지 모드에서 브리지 VLAN 관리를 사용하여 제품에 대한 액세스를 제어할 수 있습니다.

인증된 사용자가 포함된 네트워크 세그먼트에서 제품의 구성 관리에 VLAN 을 사용합니다.

이 네트워크 세그먼트에 연결된 포트와 브리지 상위 계층 인터페이스에서만 이 VLAN 을 허용합니다.

제품 구성 시 참조: *VLAN description:*

VLAN 에 대한 설명이나 이름을 입력합니다.

VLAN ID:

VLAN ID 를 입력합니다.

Default VLAN ID:

이 옵션을 체크하면 태그가 지정되지 않은 모든 수신 트래픽이 VLAN 에 배치됩니다.
포트당 하나의 VLAN 만 기본값이 될 수 있습니다.

Default priority:

우선 순위를 선택합니다. 이 옵션은 기본 VLAN ID 가 선택된 경우에만 사용할 수 있습니다.

Egress untagged:

이 옵션을 체크하면 포워딩 하기 전에 VLAN 태그가 프레임에서 제거됩니다.

Interface:

VLAN 설정을 적용할 포트를 선택합니다.
관련된 VLAN 은 전부, 브리지의 모든 인터페이스에 구성되어야 합니다.

Enable the Bridging VLAN

V.10.3 Router mode

라우터 모드에서 다음을 사용하여 제품에 대한 액세스를 제어할 수 있습니다.

로컬 서비스에 대한 수락 정책입니다. 인증된 사용자가 포함되지 않은 네트워크 영역에 대해서는 사용 안 함으로 설정해야 합니다.

제품으로 전송되는 입력 트래픽을 차단하는 방화벽입니다.

제품 구성 시 참조: *Routing/FireWall*

V.10.4 SNMP access

기본적으로 SNMP 에이전트에서 활성화된 보안은 없으며 모든 SNMP v1/v2c 사용자가 모든 공용 및 개인 OIDs 에 액세스할 수 있습니다.

SNMP 액세스를 보호하려면 예를 들어 "view" 읽기/쓰기 권한을 특정 OIDs 로 제한하여 SNMP 액세스 구성을 변경해야 합니다.

SNMP v3 보안 사용자를 생성할 수도 있습니다.

제품 구성 시 참조: *SNMP Agent*

V.11 Rogue AP detector

V.11.1 Rogue Access Point concept

악성 액세스 포인트는 선의의 직원이 추가하든 악의적인 공격자가 추가하든 로컬 네트워크 관리자의 명시적 권한 없이 보안 네트워크에 설치된 무선 액세스 포인트입니다.

악성 액세스 포인트와 해당 클라이언트는 인근 지역의 모든 사용자 또는 클라이언트가 네트워크에 무단으로 액세스할 수 있도록 허용하여 기업 네트워크의 보안을 손상시킵니다. 또한 악성 액세스 포인트는 기업 네트워크의 작동을 방해할 수 있습니다.

악성 액세스 포인트는 다음과 같은 방법으로 무선 네트워크에 영향을 줄 수 있습니다.

- 네트워크에 보안 취약점을 만들 수 있습니다.
  - 해커가 "man-in-the-middle" 공격을 수행할 수 있도록 함으로써 공격자는 피해자와 독립적으로 연결하고 메시지를 릴레이하여 피해자가 사적인 연결을 통해 서로 직접 대화하고 있다고 믿게 만듭니다. 실제로 전체 대화는 공격자에 의해 제어됩니다.
  - 무료 인터넷 연결과 같은 매력적인 기능을 광고하는 가짜 SSID 를 보냅니다. 사용자가 연결하면 가짜 SSID 가 클라이언트의 무선 구성에 추가되고 클라이언트가 가짜 SSID 를 브로드캐스트하기 시작하여 다른 클라이언트를 감염시킵니다.
  - 회사 정보의 도용을 위한 통로를 제공합니다.
- WiFi 성능에 부정적인 영향을 미칠 수 있습니다.
  - 관리되지 않는 RF 경합 또는 간섭을 적용합니다.
  - 네트워크에 불필요한 데이터를 가득 채워서 서비스 거부를 생성합니다.
  - WAN 포트 대신 LAN 으로 연결하면 네트워크에 DHCP 를 주입하여 문제를 일으킬 수 있습니다.
  - 사용자가 액세스 지점이 유효하지 않다고 생각하고 연결하려고 할 때 VLAN 차이로 인해 적절한 리소스에 연결할 수 없으며, 이로 인해 IT 부서에 많은 점검 요청이 발생할 수도 있습니다.

V.11.2 Rogue Access Point attack

Rogue Access Point 는 선의의 직원이 추가하든 악의적인 공격자가 추가하든 로컬 네트워크 관리자의 명시적인 권한 없이 보안 네트워크에 설치됩니다.

악성 액세스 포인트는 종종 "Evil Twin"으로 불립니다. 와이파이를 위한 IEEE 802.11 표준에서는 사용자가 AP 를 인식할 수 있는 두 개의 식별자가 있습니다 (Service Set Identifier(SSID)와 Basic Service Set Identifier(BSSID)). 그러나 이러한 식별자는 쉽게 속일 수 있습니다. 합법적인 AP 를 복제하면 Evil Twin AP 가 생성됩니다.

Evil Twins 또는 RAP 는 두 가지 형태로 존재할 수 있습니다.

- Coexistence (공존)
- Replacement (대체)

두 경우 모두 RAP 는 허용된 AP 와 동일한 SSID 를 사용합니다.

Coexistence(공존)에는 합법적인 AP 와 Evil Twin 이 같은 장소에 공존합니다. IEEE 802.11 표준은 WLAN 클라이언트가 가장 강력한 신호로 AP 에 연결해야 한다고 명시하고 있으므로 공격자는 RAP 의 신호 강도를 높여 사용자가 연결하도록 합니다.

"Replacement" 유형에서 Evil Twin 은 합법적인 액세스 포인트에 대한 적극적인 공격으로 인해 해당 액세스 포인트를 종료하여 대체합니다. 공격받는 대상자가 탐지하지 못하도록 하려면 RAP 에 유효한 인터넷 연결(또는 액세스 지점과 동일한 네트워크에 대한 연결)이 있어야 하며, 전자의 경우 후자에 연결할 수 있는 한 합법적인 AP 를 통해 패킷을 릴레이할 수 있습니다.

V.11.3 Rogue Access Point Detector

악성 액세스 포인트 탐지는 무선 네트워크를 보호하는 데 중요한 구성 요소입니다. 악성 액세스 포인트 탐지는 탐지와 경고의 두 가지 작업을 수행합니다. 네트워크에 설치하기로 결정한 사항이 무엇이든 간에 RF 설계 초기부터 악성 액세스 지점을 탐지하고 네트워크 관리자에게 알릴 수 있는 기능이 있어야 합니다.

RAP 탐지 모듈은 SSID 및 예상되는 BSSID 에 대한 구성 프로필의 정보를 사용하는 고전적인 화이트리스트 접근 방식을 사용합니다.

RAP 디텍터에서 스캔한 파라미터는 다음과 같습니다:

- SSID,
- BSSIDs,
- Channel,
- Encryption,
- Signal strength.

SSID 또는 BSSID 는 바이패스될 가능성이 높기 때문에(BSSID 스푸핑: 합법적인 ap 와 동일한 SSID 및 MAC 주소를 전송하는 RAP) 액세스 포인트에서 사용되는 암호화 유형도 비교합니다. (OPEN = Open, WEP = Wired Equivalent Privacy, WPA = Wi-Fi Protected Access version 1, 2 and 3).

검출 모듈에 의해 구현된 또 다른 비교점은 신호 강도의 변화입니다. 이 알고리즘은 인증된 AP 에 대해 사용자가 예상하는 인증된 RSSI(auth_rssi)를 사용하며, 읽기 RSSI 값은 허용 가능한 [auth_rssi - delta; auth_rssi + delta] 범위 내에 있어야 합니다(델타값은 15db). RSSI 읽기가 이 간격을 벗어날 때 경고가 트리거됩니다.

V.12 Internet Protocol V6 – IPv6

V.12.1 What is IPv4?

IPv4 는 인터넷 프로토콜 버전 4 를 의미합니다. IPv4 는 우리 장치를 웹에 연결할 수 있게 해주는 기본 기술입니다. 장치가 인터넷에 액세스할 때마다 99.48.227.227 과 같은 고유한 숫자 IP 주소가 할당됩니다. 웹을 통해 한 컴퓨터에서 다른 컴퓨터로 데이터를 보내려면 네트워크를 통해 두 장치의 IP 주소를 포함하는 데이터 패킷이 전송되어야 합니다.

V.12.2 What is IPv6?

현재 많은 인터넷 서비스에서 여전히 사용하고 있는 IPv4 프로토콜 보완하고 대체하기 위해, 차세대 인터넷 프로토콜(IP) 주소 표준으로 개발된 프로토콜이 IPv6입니다. 인터넷에 연결된 모든 컴퓨터, 휴대폰, 홈 오토메이션 구성 요소, IoT 센서 및 기타 장치는 다른 장치 간에 통신하기 위해서는 각각의 IP 주소가 필요합니다.

V.12.3 Why Support IPv6?

IPv4 에는, IPv6 와 다른 한 가지 중요한 차이점이 있습니다. 바로 128 비트 IP 주소를 사용한다는 것입니다. 수많은 연결 장치 확산으로 인해, 이러한 한정된 크기로는 할당할 주소가 부족합니다.

IPv4 는 인터넷 주소로 32 비트 주소를 사용합니다. 즉, 총 약 42 억 9 천만 개의 2^32 IP 주소를 지원할 수 있습니다. 많아 보일 수 있지만, 현재 42 억 9 천만 개의 IP 주소가 모두 할당된 상태라, 오늘날 우리가 직면하고 있는 주소 부족 문제로 이어지고 있습니다.

IPv6 는 128 비트 인터넷 주소를 사용합니다. 따라서 2^128 개의 인터넷 주소(정확히 340,282,366,920,938,463,463,374,607,431,768,211,456 개)를 지원할 수 있습니다. IPv6 주소의 수는 IPv4 주소의 수보다 1028 배 더 많습니다. 따라서 IPv6 의 주소 개수는, 향후 인터넷 장치가 계속 확장되기에 충분합니다.

IPv6 의 주요 이점은 다음과 같습니다.

- 더 이상 NAT (Network Address Translation, 네트워크 주소 변환)을 할 필요가 없습니다.
- 자동 구성 기능
- 더 이상 사설 주소간에 충돌이 없습니다.
- 향상된 멀티캐스트 라우팅
- 더 간단한 헤더 형식
- 간소화되고 보다 효율적인 라우팅
- 진정한 QoS (quality of service, flow labeling 라고도 부름) 지원
- 내장된 인증 및 개인정보 보호 지원
- 유연한 옵션 및 확장
- broadcast 을 하지 않습니다.

주요 이점 요약 :

IPv6 의 이점	IPv4	IPv6
IPv6 는 많은 양의 주소를 가지고 있습니다.	4.29 x 109 = 43 억 개의 주소를 가지고 있습니다. 지구에 있는 모든 사람이 한 사람씩 IP 주소도 할당할 수 없을 정도로 부족합니다.	3.4 x 1038 = 340 조 1000 조 개의 주소를 가지고 있습니다. 지구 표면의 평방 밀리미터당 약 670 조 개의 주소입니다.
IPv6 는 관리하기 쉽고 저렴합니다.	네트워크는 수동이나 DHCP 를 사용하여 구성해야 합니다. IPv4 에는 인터넷 성장을 처리하기 위한 많은 오버레이가 있어, 유지 관리에 많은 노력이 필요합니다.	IPv6 네트워크는 자동 네트워크 구성 기능을 제공합니다. 특히 대규모 설치의 경우 더 간단하고 관리하기 쉽습니다.
IPv6 는 end-to-end 간 투명성을 복원합니다.	NAT 의 광범위한 사용은, 단일 NAT 주소가 라우팅할 수 없는 수천 개의 주소를 마스킹할 수 있어, end-to-end 간 무결성을 달성할 수 없습니다.	광대한 주소 공간으로 인해 직접 주소 지정이 가능합니다. 네트워크 주소 변환 장치가 필요하지 않습니다.
IPv6 는 보안 기능이 향상되었습니다.	보안은 애플리케이션에 달려 있습니다. IPv4 는 보안을 염두에 두고 설계되지 않았습니다.	IPv6 에는 적합한 키 인프라와 함께 사용할 수 있는 IPSEC 이 내장되어 있습니다.
IPv6 는 향상된 이동성을 제공합니다.	상대적으로 제한된 네트워크 토폴로지는, IPv4 인터넷의 이동성 및 상호 운용성 기능을 제한합니다.	IPv6 는 이미 네트워크 장치에 널리 내장된 상호 운용성 및 이동성 기능을 제공합니다.
IPv6 는 혁신을 장려합니다.	IPv4 는 전송 및 통신 매체로 설계되었으며, IPv4 는 제약 조건을 우회하는 방법을 찾습니다.	IPv6 의 주소 수, 확장성 및 유연성을 감안할 때, IPv6 는 혁신을 촉발하고 협업을 지원하며 무한한 잠재력을 가지고 있습니다.

V.12.4 IPv6 address format introduction

IPv6 주소의 텍스트 형식은 **'aaaa:bbbb:cccc:dddd:eeee:ffff:gggg:hhhh'**이며, 각 문자는 4 비트를 나타내는 16 진수입니다. 선행에 있는 0 은 생략할 수 있습니다. 이중 콜론(::)은 주소의 텍스트 형식에서 한 번만 사용하여 임의의 수의 0 비트를 지정할 수 있습니다.

하기는 예시입니다.

- **aaaa:bbbb:cccc** 는 사이트 접두어입니다. 공용 토폴로지는 ISP 또는 RIR 에 의해 사이트에 할당됩니다.
- **dddd** 는 서브넷 ID: 개인 토폴로지(사이트 토폴로지: 사이트 내부)입니다. IPv4 와 동일한 개념, 단일 HW 링크와 연결된 서브넷입니다.
- **eeee:ffff:gggg:hhhh** 는 인터페이스 ID 입니다. 인터페이스의 MAC 주소 또는 EUI-64 형식(Extended Unique Identifier)으로부터 자동으로 구성됩니다.

주소를 단순화하기 위해 00 을 생략할 수 있습니다.
2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b ⇔ 2001:db8:3c4d:15::1a2f:1a2b

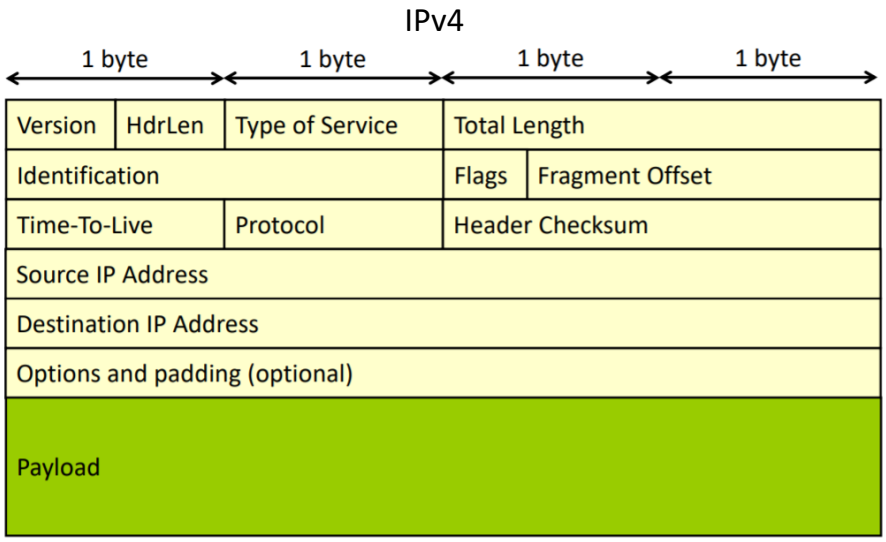
참고: 선행 0 만 생략됩니다. 후행 0 은 생략되지 않습니다.

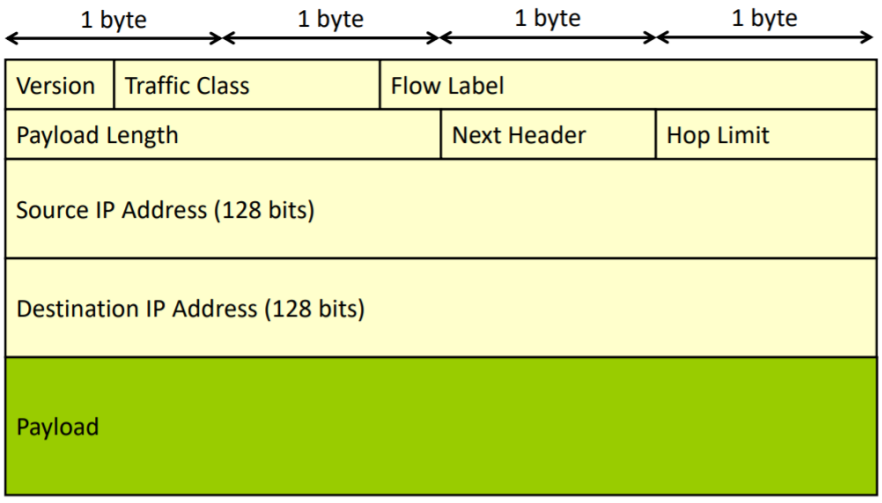
2001:0db8:**0012**::/48 = 2001:db8:12::/48
2001:db8:**1200**::/48 ≠ 2001:db8:12::/48

참고: 일부 특수 IPv6 접두사는 예약되어 있습니다.

- 2002:: /16→ IPv6 에서 IPv4 로 라우팅
- fe80:: /10 → 링크 로컬 주소
- ff00:: /8 → 멀티캐스트 주소

요약하면 각각의 IP v4 및 v6 데이터그램을 비교할 수 있습니다.





V.12.5 Class of IPv6 address

IPv6 주소에는 두 가지 일반적인 클래스가 있습니다:

- Unicast
  - IPv4와 동일하지만 링크 로컬 주소가 추가되었습니다.
- Multicast
  - IPv6 프로토콜 고유, 특히 ND(Neighbor Discovery)(RFC 4861)
  - 모든 멀티캐스트 주소는 ff00::/8에 속합니다.
  - IPv6에는 IP 서브넷 브로드캐스트 주소가 없습니다.
  - 대신 서브넷 내에서 링크 로컬 멀티캐스트를 사용합니다.

V.12.6 IPv6 address types

V.12.6.1 Unicast Address

링크 로컬 주소 (⇔ LAN):

로컬 네트워크에서만 유효하며 외부에서는 유효하지 않습니다.

예시 : 링크 로컬 주소, Acksys MAC 주소 00:09:90:00:5a:db

- FE80::290:E8FF:FE00:5ADB

글로벌 유니캐스트 주소: 인터넷에서 유일합니다.

- 예시 : [2001:db8::1]:80 or URL: http://[2001:db8::1]:80

예시 : 사이트 접두사로 글로벌 유니캐스트 계산 = aaaa:bbbb:cccc:
Subnet ID=0 and IPv4 = 10.11.16.1 (=0x0A0B1001)

- AAAA:BBBB:CCCC::A0B:1001

V.12.6.2 Multicast Address

알림: FF00:: /8 는 멀티캐스트 주소입니다.

8 bits	4 bits	4 bits	122 bits
11111111	Lifetime	Scope	Network prefix .. Group ID
ff00	*0 or 1*	*1,2,5,8,e*	*Multicast ID*

1 – Node (interface local scope)
2 – Link local scope
5 – Site local scope
8 – Organisation local scope
e – Global scope

0 – Permanently, globally assigned, well-known IANA
1 – Non-permanently assigned muticast address (dynamically assigned)

- 영구적인 IPv6 멀티캐스트 주소 (FLGS = 0)
- 0x00000001 ~ 0x3FFFFFFF 범위의 그룹 ID
- 영구적인 IPv6 멀티캐스트 그룹 식별자 (FLGS = 0)
- 범위 0x40000000 ~ 0x7FFFFFFF

예시:

NTP(Network Time Protocol) 가 ID 0x40404040 에 할당되었습니다.

- 동적 IPv6 멀티캐스트 주소 (FLGS = 3)

  예시: RFC 3307 참조

  FF02::1 = 모든 호스트 멀티캐스트 주소 (로컬 네트워크), FF05::1 (사이트)

  FF02::2 = 모든 라우터 멀티캐스트 주소 (로컬 네트워크)

V.12.7 Services supporting IPV6 addressing

- *제품 웹 인터페이스용 HTTP/HTTPS*
- *Syslog 푸시*
- *클라이언트 모드 NTP*
- *SNMP*
- *IPv6 에서 원격 인증 서버 주소 지정을 가능하게 하여 RADIUS 인증*
- *고정 라우팅*
- *방화벽*
- *라우팅*
- *브리지*
- *브리지 WIFI(ARPNAT 및 WDS)*

V.13 Asynchronous System Upgrade

고객은 운영 팀이 근무하지 않는 시간에 라우터의 펌웨어를 업그레이드할 때도 있습니다. (예: 라우터를 업그레이드하려면 열차를 중지해야 함)
대역폭 과부하를 피하기 위해 수백 개의 업그레이드(파일 업로드)를 동시에 하기는 어렵습니다.
운영자는 비동기식 업그레이드 기능을 사용하여, 다음을 수행할 수 있습니다.

- 인터넷에 액세스할 수 있는 한은, 기차가 운행 중이거나 차고에 있을 때에도 Firmware 를 업로드합니다.
- 기차가 더 이상 운행하지 않을 때에만 Firmware 를 업그레이드하여 라우터를 다시 지정할 수 있습니다.

목표는 펌웨어 전송과 업그레이드 자체를 분리하는 것입니다. 사용자는 펌웨어를 다운로드하고 나중에 시스템 업그레이드를 수행할 수 있습니다. 시스템 업그레이드를 위한 몇 가지 옵션이 있습니다.

- 프로그램 즉시 실행
- 특정 날짜 및 시간에 업그레이드 예약

파일 서버에서 라우터로 펌웨어 전송하는 것은 시스템 업그레이드 기능과 무관합니다. 전송에 사용된 방법에 관계없이, 업그레이드 기능은 파일이 유효한지 여부를 확인합니다.

참고:
Railbox V2 를 사용하면, 시스템 업데이트를 예약했을 때, 펌웨어가 즉시 eMMC 에 저장되어 제품에 전원이 공급되지 않을 때 데이터를 보존할 수 있습니다.
다른 제품의 경우 펌웨어를 RAM 에만 저장할 수 있으므로 다시 시작하면 예약되었거나 보류 중인 업데이트가 손실됩니다.

V.14 System Integrity Check

WaveOS 는 보안 개선 목적으로, 무결성 검증 시스템을 통합시켰습니다. 무결성 검증 시스템은, 운영 체제를 구성하는 파일의 무결성을 검사할 수 있게 해주는 운영 체제의 기술 구성 요소입니다. 이 기능을 통해 고객은 제품이 의도적으로 또는 실수로 손상되거나 수정되지 않았는지 알 수 있습니다.

파일 시스템의 무결성 검사는, 이를 구성하는 각 파일의 'checksums'또는 'fingerprint ' 계산을 기반으로 합니다. WaveOS 를 컴파일하는 동안 모든 'checksums '은 참조 파일에 저장되며, 무결성 확인 프로세스는 각 파일의 'fingerprint '을 참조와 비교합니다.

- checksums 이 동일하면 제품의 무결성이 ACKSYS 에서 생산했을 때와 동일함을 보장합니다.
- 만약 결과가 다르면 제품이 손상된 것일 수 있습니다.

파일의 해시(condensate)를 계산하기 위해, 해시 함수가 콘텐츠에 적용됩니다. 이것은 MD5 계산 알고리즘(1992 년 RFC 1321 준수)을 기반으로 고유한 디지털 해시를 계산하는 함수입니다. 이 무결성 검사는 HIDS(기계 침입 탐지 시스템)에서 요청하는 많은 기능 중 하나이며,파일이 인에 의해 악의적으로 수정되지 않았는지 알 수 있습니다.

무결성 검사 기능은 SNMP 인터페이스를 통해 제공되며, 이를 통해 고객은 원격으로 이 검사를 수행할 수 있습니다.

참고: SSH 또는 직렬 포트를 통해서도 명령 확인이 가능합니다.

검증은 다음 3 가지 작업을 통해서 이루어집니다.:

- md5sum 으로 현재 파일 분석을 유지합니다.
- SNMPD 인터페이스에서 객체 식별자 OID(Object Identifier, 객체 식별자)를 정의합니다.
    - 요청에 따라 분석 시작
    - 분석 진행 상황 확인 가능
- 시스템 로그 파일에 다음과 같은 형식으로 결과 기록:
    - 변경된 파일마다 메시지를 하나씩 기록하며, 메시지에는 특정 문자열의 시작 부분과 변경된 파일의 이름과 그 해시값이 포함됩니다.
    - 분석 결과를 나타내는 메시지가 있으며, 이는 특정 문자열의 시작 부분과 결과입니다.

일반적인 사용 사례로는, SNMP 명령을 통해 대상 플랫폼에서 WaveOS 파일이 수정되지 않았는지 확인하는 것입니다.

VI WEB INTERFACE REFERENCE

VI.1 Setup Menu

이 메뉴를 사용하여 무선 인터페이스 및 네트워킹 속성을 구성할 수 있습니다. 대부분의 **SETUP** 페이지 하단에는 2 개 또는 3 개의 버튼이 있습니다.

매개변수를 변경한 후에는, **Save** 를 눌러 영구적인 메모리에 기록합니다. 이 경우 변경 사항은 즉시 적용되지 않고, 재시작 후 또는 **Save & Apply** 후에만 적용됩니다.

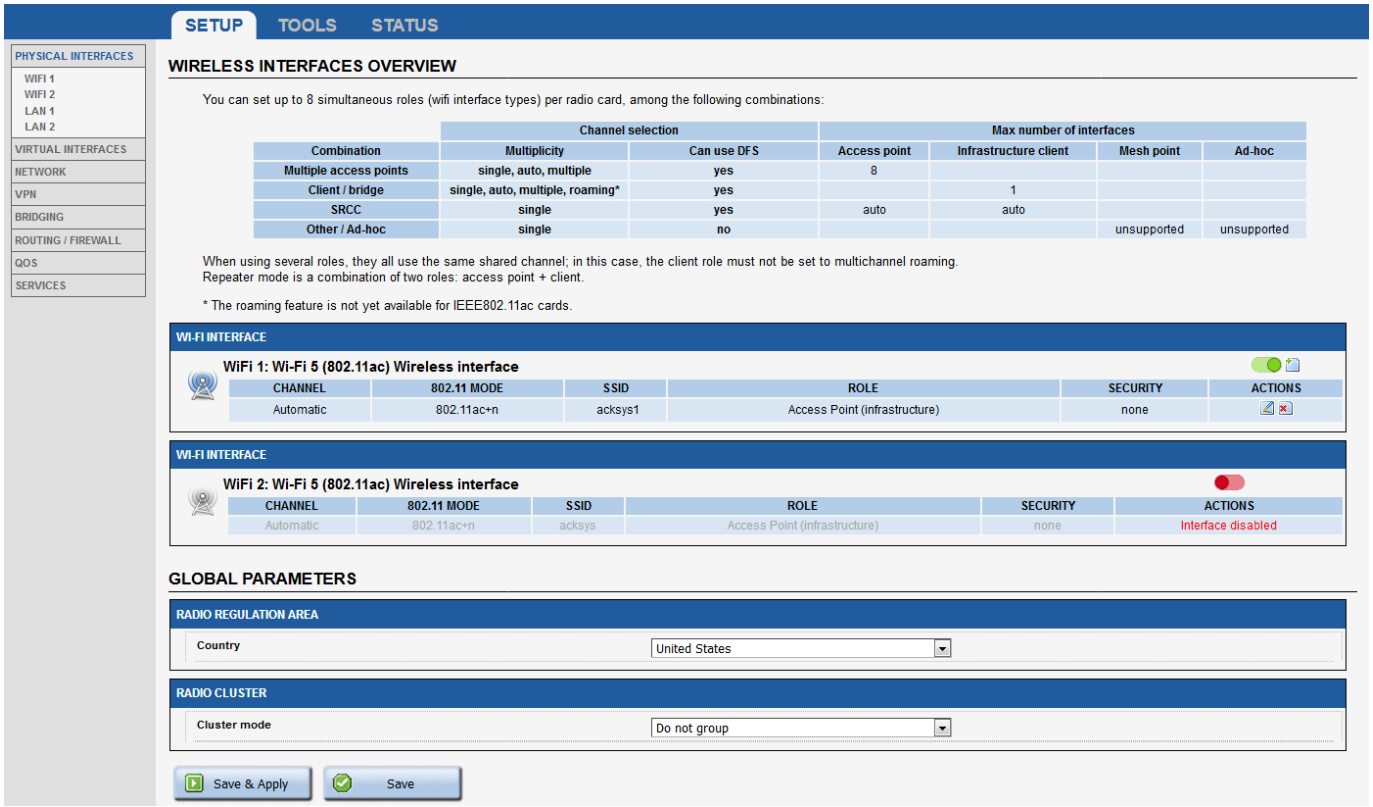
Save & Apply 를 누르게 되면 지금까지 모든 페이지에서 수행한 모든 구성 변경 사항을 적용하게 됩니다.

Reset (사용 가능한 경우) 을 눌러 양식의 데이터를 이전 값(마지막 저장 **save** 후 표시되는 값)으로 되돌립니다.

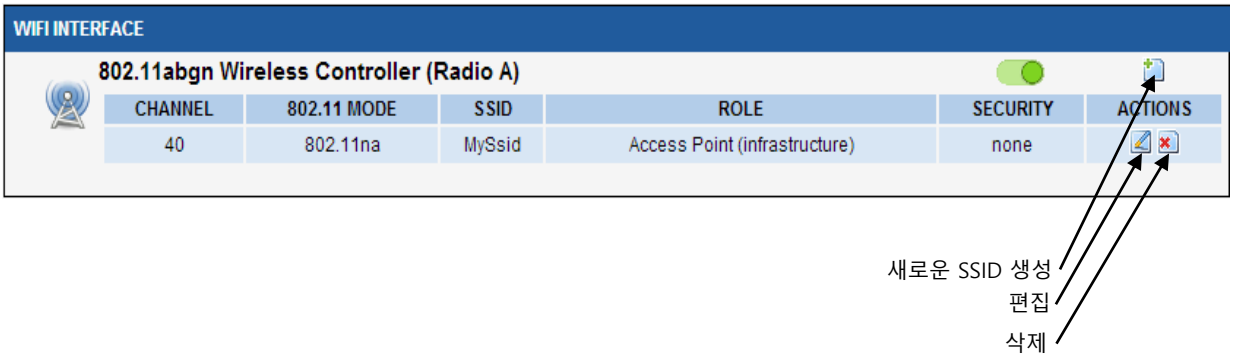
VI.1.1 Physical interfaces

Wireless overview section:

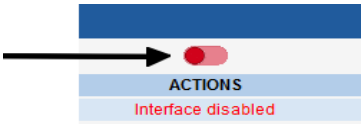
이 페이지에서는, 구성된 라디오 카드의 가장 중요한 속성을 SSID 별로 보여줍니다. 페이지 하단에서는 global Wi-Fi 속성을 변경할 수 있습니다.



WIFI INTERFACE 프레임은 각 WiFi 인터페이스의 주요 설정을 요약합니다.



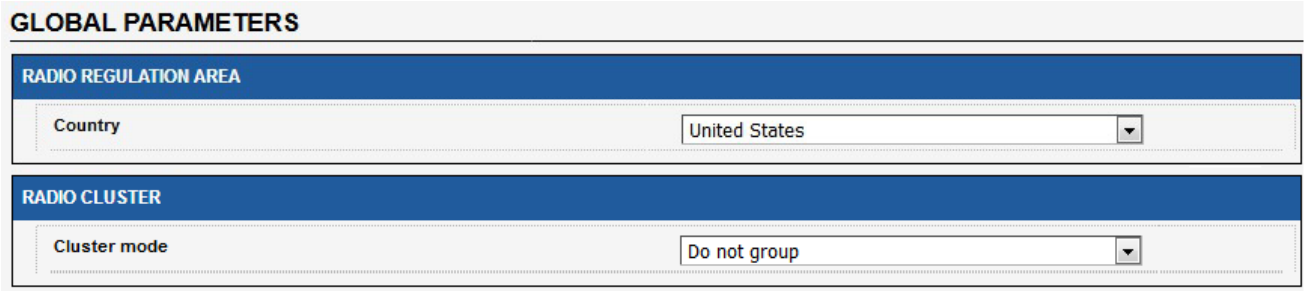
기본적으로(초기 설정), 무선 기능은 비활성화 되어 있습니다.
사용하려면 직접 버튼을 활성화 해야 합니다.



라디오 카드 활성화/비활성화는 **Save & apply** 후에만 적용됩니다.

SSID 를 삭제하려면 **Remove** 버튼을 클릭하세요. 그리고 **Edit** 버튼을 통해 라디오 창을 열어 SSID 설정을 편집합니다.

Global parameters section:



Country:

선택한 국가의 규제 규칙에 따라, 사용할 수 있는 채널과 전송 전력이 결정됩니다. 또한 클라이언트 역할에서 제품은 beacons 에서 AP 가 제공하는 국가를 사용합니다.

Cluster mode:

라디오 카드를 클러스터링하여, 하나의 라디오가 여러 채널을 스캔하고 다른 라디오가 AP 에 연결되어 데이터를 전송하도록 구성할 수 있습니다. 이 모드에서 스캔 프로세스는 데이터 전송을 방해하진 않지만, 스캐너 라디오는 이 용도로 예약됩니다.

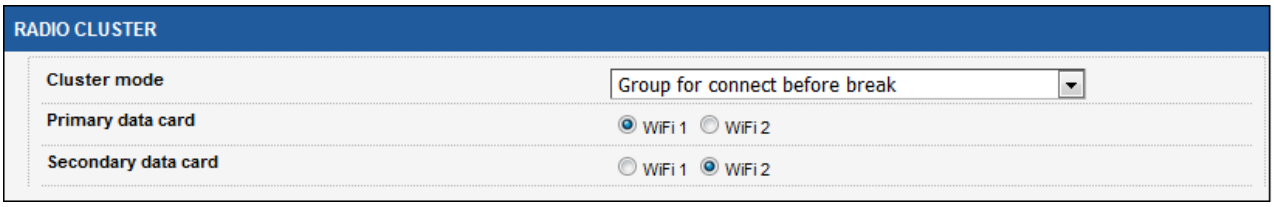
Group for scanning 을 선택하면, 하나의 라디오 카드에서 AP 에 대한 스캔이 발생합니다. 결과는 로밍 목적에 가장 적합한 AP 를 선택할 수 있도록 다른 라디오 카드에 제공됩니다. 이는 AP 신호 레벨이 두 카드에 대해 동일해야 함을 의미합니다. 따라서 안테나 위치, 극성 및 케이블 연결은 서로 매우 가까워야 합니다. 차이를 고려하여 로밍 트리거 레벨 부스트를 너무 작게 설정해서는 안 됩니다.

이 모드에서 로밍 매개변수는 데이터 전송에 사용되는 라디오 카드 구성에서 가져옵니다.

Group for scanning 을 선택하면, **Scanner card** 라디오 버튼으로 스캔에 사용할 카드를 선택할 수 있습니다.

Group for connect before break 를 선택하면, 두 라디오 카드의 작동 방식은 ***Group for scanning*** 와 유사하지만, 로밍이 발생할 때마다 두 카드의 기능이 교환됩니다. 이 기능은 Connect before break 섹션에 자세히 설명되어 있습니다.

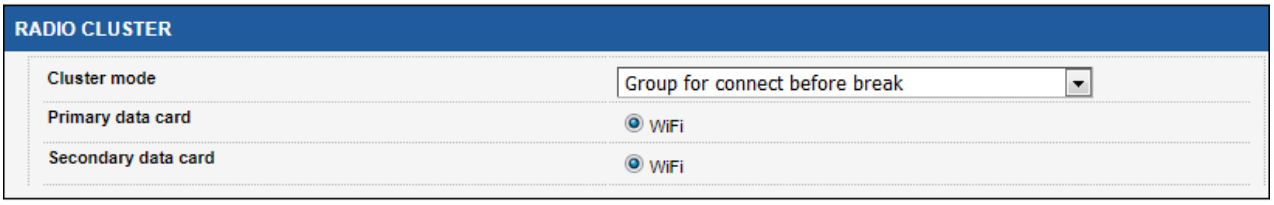
기본적으로 WiFi 1 인터페이스가 기본 카드로 선택되지만, 이는 일시적인 상태이므로 대부분의 경우 작동에 영향을 미치지 않습니다.



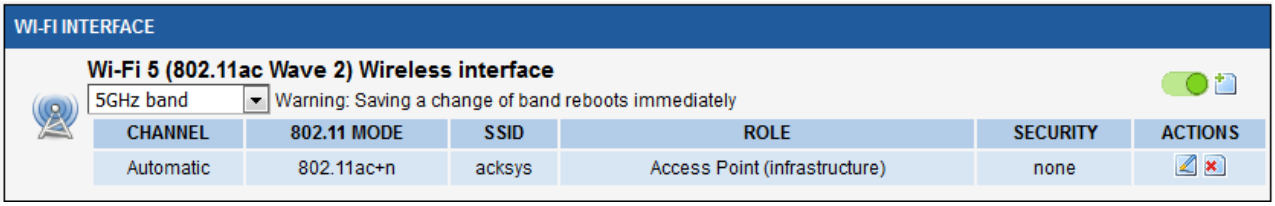
이 모드에서는 동일한 라디오 카드에 두 가지 기능을 모두 수행하도록 요청할 수 있지만, 로밍은 싱글 무선 채널에서만 가능합니다.

듀얼 무선 제품의 경우 두 기능에 대해 동일한 라디오 카드를 선택하기만 하면 됩니다.

단일 무선 제품 구성 :



Case of 802.11ac Wave 2 products:



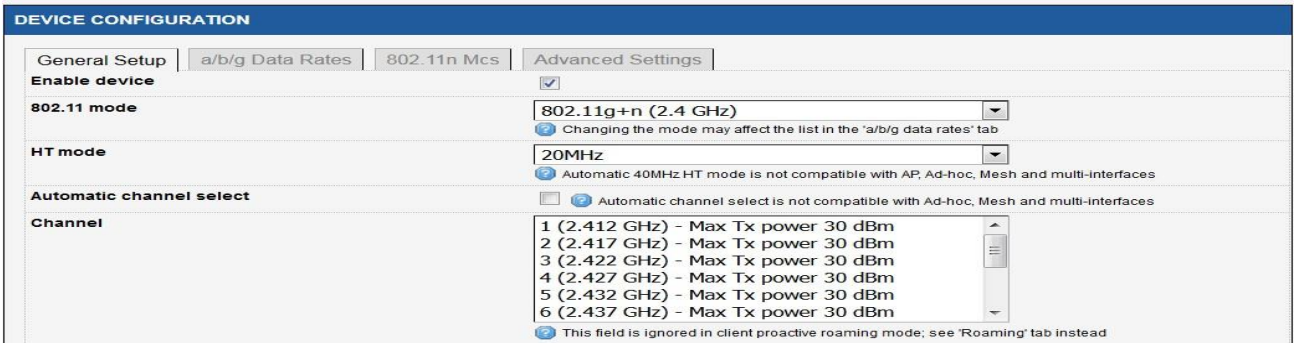
802.11ac Wave 2 라디오가 장착된 Railbox/6xA0 과 같은 제품의 경우 무선 구성을 진행하기 전에 주파수 대역(5GHz 또는 2.4GHz)을 선택해야 합니다.

VI.1.1.1 Wireless/Radio

a. SETUP/PHYSICAL INTERFACES/WIRELESS SETTINGS/DEVICE CONFIGURATION

General Setup tab:

이 섹션에서는 라디오 카드에서 생성할 수 있는 각 SSID 에 대한 공통적인 모든 설정을 할 수 있습니다.



Enable device:

이 체크박스에 체크하면, 라디오 카드가 활성화되고 통신할 수 있습니다. 체크하지 않으면, 무선모듈이 비활성화 되어 무선통신이 불가능해집니다.

802.11ode:

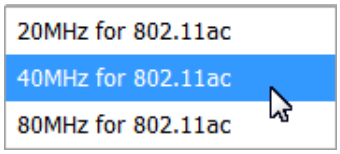
- 802.11g+n 모드는 2.4GHz 대역(802.11g)에서 작동하며, 802.11g 및 802.11n 장치와 호환됩니다.
- 802.11a+n 모드는 5GHz 대역(802.11a/h)에서 작동하며, 802.11a/h 및 802.11n 장치와 호환됩니다.
- 802.11ac+n 모드는 5GHz 대역에서 작동하며, 802.11ac, 802.11a/h 및 802.11n 장치와 호환됩니다.

참고: 802.11a+n/ac+n 으로 구성된 제품은 서로 다른 주파수 범위를 사용하기 때문에 802.11g+n 으로 구성된 다른 제품과 통신할 수 없습니다.

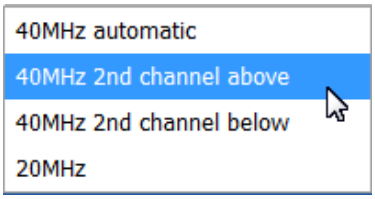
HT (High Throughput) mode:

802.11n 및 802.11ac 모드에서는 기본 HT20 모드를 사용할 수 있습니다. 이 모드는 기존의 802.11a 및 802.11g 모드와 마찬가지로 단일 20MHz 채널을 사용합니다. 그러나 대역폭을 늘리려면 40MHz(HT40) 또는 80MHz(HT80) 채널에서 각각 작동하도록, 2 개 또는 4 개의 연속 20MHz 채널을 통합할 수 있습니다.

802.11ac 모드에서는 2 개 또는 4 개의 20MHz 채널을 통합할 수 있습니다. 기본 채널은 AP 가 신호 자체에 beacons 을 전송하는 채널로 자동 결정됩니다.



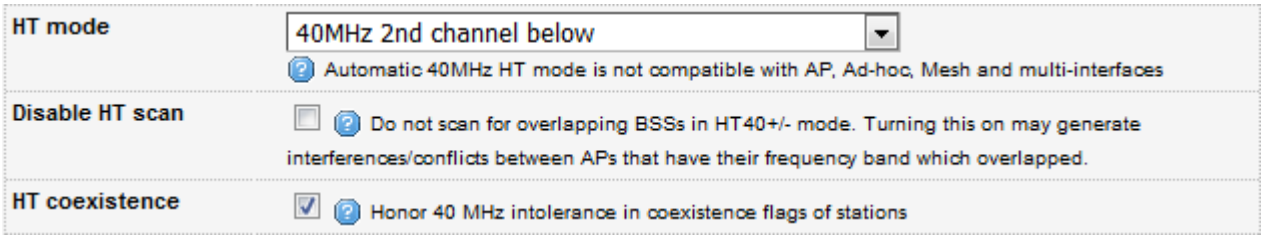
802.11n 모드에서는 인접한 20MHz 채널 두 개만 집계하여, 40MHz 채널에서 작업할 수 있습니다.



기본 채널은 채널 섹션에서 선택됩니다.(아래 참조) 보조 채널은 기본 채널 바로 위 또는 아래로 고정하도록 선택할 수 있습니다. 또한 40MHz 를 자동으로 설정하고 선택하도록 할 수 있습니다.

자동 40MHz 모드는 Ad-hoc, Mesh 및 다중 인터페이스와 호환되지 않습니다.

HT40 모드를 선택하면 두 가지 추가 옵션이 나타납니다.



Disable HT scan:

이 옵션이 활성화되면 시스템은 운영 채널의 40MHz 폭에서 다른 AP 의 존재를 감지하지 않고 통신하게 되며, 이로 인해 간섭이 발생하고 통신 품질이 저하될 수 있습니다.

HT coexistence:

이 옵션을 사용하면, 시스템은 다른 AP 들이 보조 채널을 사용하고 있을 경우, 데이터 전송을 위해 여러 채널을 집계(aggregation) 하지 않고, 보조 채널을 해제합니다. 이를 통해 다른 AP 의 신호와의 간섭을 줄이고 통신 품질을 향상시킬 수 있습니다.

Automatic channel select (ACS):

제품의 역할에 따라 채널을 자동으로 선택할 수 있습니다.

- AP 역할 : AP 를 시작할 때, 해당 국가에서 허용되는 모든 채널 중에서 채널을 선택합니다. 특정 채널로 선택을 제한하려면, ACS 를 체크하지 않고 채널 다중 선택 상자를 사용하세요.
- Client 역할 : 클라이언트는 해당 국가에서 허용되는 모든 채널을 검색합니다. 채널 검색 목록을 제한하려면, ACS 를 선택하지 말고 채널 다중 선택 상자를 사용하세요. 클라이언트가 로밍 모드로 설정된 경우, 이 채널 목록은 로밍 탭의 채널 목록으로 대체됩니다.
- 기타 역할 : 기타 역할(mesh, ad-hoc) 은 하나의 채널만 지원하며, 이 매개변수는 사용할 수 없으며 드롭다운 상자에서 채널을 선택해야 합니다.

참고 : "40 MHz second channel below" 모드에서는 ACS 를 사용할 수 없습니다.

Channel:

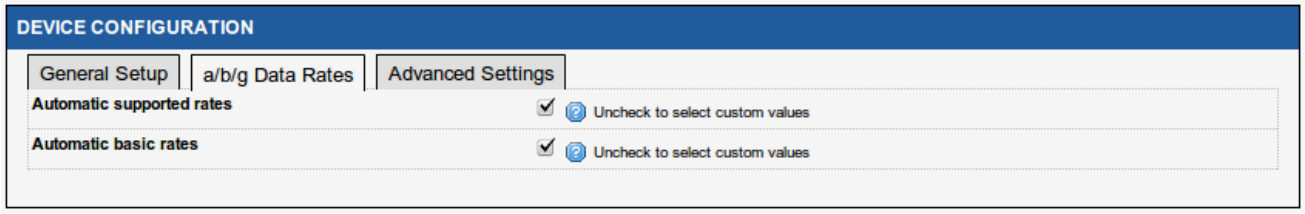
선택한 802.11 모드 및 선택한 국가의 규정 규칙에 따라 채널 목록을 선택할 수 있습니다. 이는 인프라 클라이언트 모드에 사용되지 않습니다. 스캔에 허용된 모든 채널을 사용하기 때문입니다(로밍 매개변수에 의해 제한될 수 있음).

경우에 따라 단일 무선 카드가 여러 Wi-Fi 역할을 동시에 처리할 수 있습니다. 이 경우 "클라이언트" 기능은 공통 채널만 스캔 하도록 설정해야 합니다. 더 자세한 내용은 섹션 *V.2.1.5 Virtual AP (multi-SSID) and multifunction cards* 와 *Appendix – 802.11 Radio channels* 을 참고하세요.

AP 가 가장 포화도가 없는 채널을 선택하고, 현재 채널에서 레이더가 감지되면 다른 채널로 전환할 수 있도록 여러 채널을 선택할 수 있습니다. 브라우저에서 여러 채널을 선택하려면 Ctrl+클릭 단축키를 사용하세요.

참고: DFS 대상 채널은 사용하기 전에 확인 지연(CAC 시간)이 발생됩니다. 더 자세한 정보는 *V.2.4 Radio channels and national regulation rules* 섹션을 참고하세요.

a/b/g Data Rates tab:



Automatic supported rates:

이 옵션을 체크하면, AP 에서 Client 에게 알리는 속도를 제한할 수 있습니다.

Automatic basic rates:

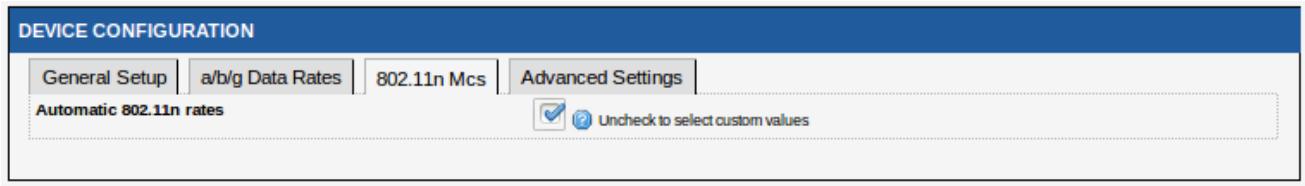
이 옵션은 다른 기기가 액세스 포인트와 통신하기 위해 지원해야 하는 속도를 수정할 수 있는 설정입니다. **경고: 모든 기본 rate 는 지원되는 rate set 에 포함되어야 합니다.**

최저 rates 에서 변경할 때의 참고사항 :

관리, 브로드캐스트 및 멀티캐스트 프레임은 선택된 최저 기본 속도를 사용하여 전송됩니다. 이러한 프레임의 성능을 높이려면, 기본값보다 높은 속도만 선택하게끔 설정하여 성능을 개선할 수 있지만, 이는 지역 커버리지에 영향을 미칩니다(product Quick Start guide 에 제공된 출력 전력 표를 참조하십시오).

무선 카드는 낮은 속도는 시도하지 않기 때문에, 재전송(프레임이 손실된 경우)이 더 빨리 발생하고 더 적은 대역폭을 사용합니다. 액세스 포인트와 연결되면, 자동 적응 속도 제어 알고리즘(MINSTREL 알고리즘)도 더 빠르게 수렴됩니다.

802.11n MCS tab:

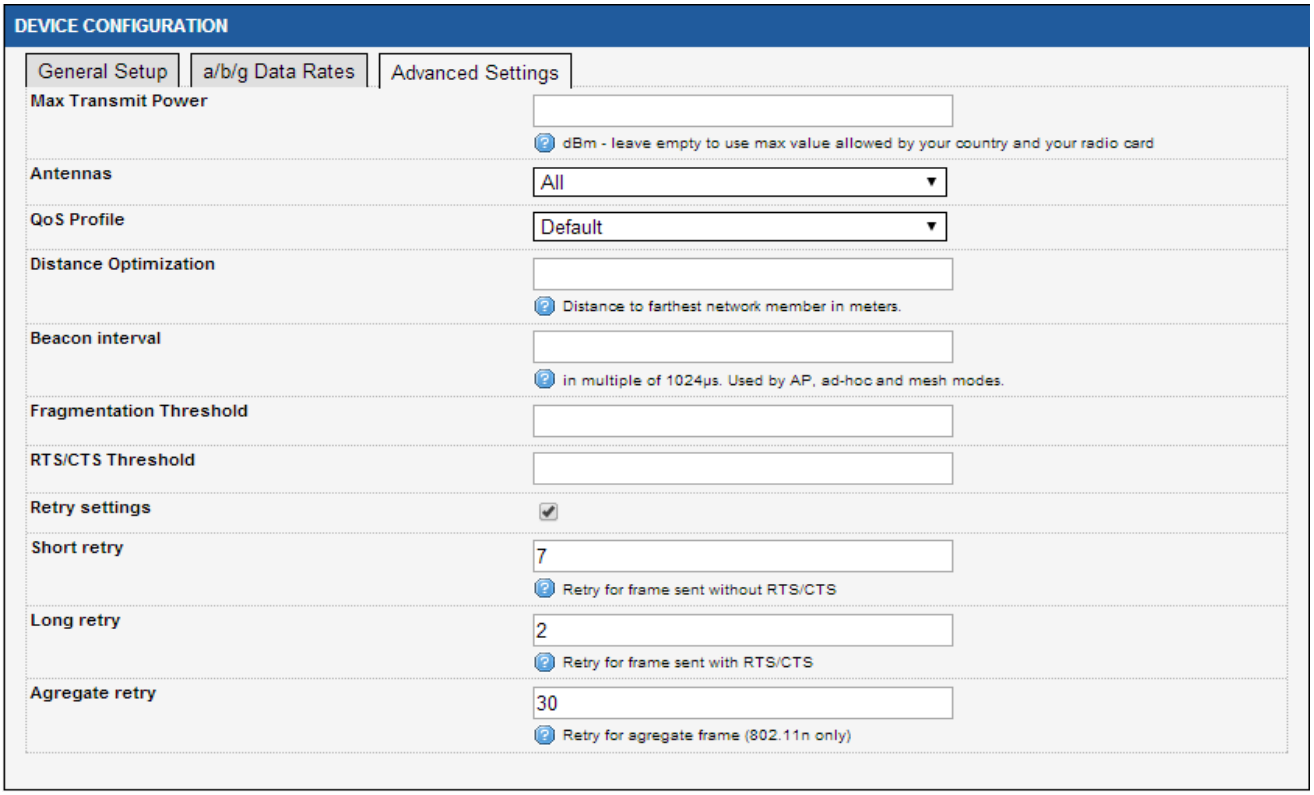


이 옵션은 액세스 포인트에서 클라이언트에게 지원되는 MCS(Modal Coding and Scheme)를 제한할 수 있는 옵션입니다.

a/b/g 속도와 마찬가지로, 스트림에서 가장 높은 MCS 만 선택하면 브로드캐스트 및 멀티캐스트 프레임의 성능을 향상시킬 수 있습니다. 그러나 이 경우 a/b/g 와 동일한 단점이 있습니다.

이 옵션은 802.11ac 라디오 카드에서는 사용할 수 없습니다.

Advanced Settings tab:



Max transmit power:

송신 출력은 일반적으로 주어진 채널의 규정, 규칙 및 라디오 카드의 기능에 따라 자동으로 계산됩니다. 이 옵션은 송신 출력에 대한 상한을 설정합니다. 송신 출력은 구성된 안테나 간에 분배됩니다.

Antennas:

사용되지 않는 안테나는 여기에서 비활성화할 수 있으며, 이로 인해 전송 출력을 남은 안테나에 집중시킬 수 있습니다. 세 번째 안테나 또는 두 번째와 세 번째를 모두 비활성화할 수 있습니다. 802.11n 다중 공간 스트림을 활용하려면, 최소한 공간 스트림 수와 동일한 수의 안테나를 사용해야 합니다. 송신 출력은 구성된 안테나 간에 분배됩니다.

QoS Profile:

이 옵션에서는, SETUP/QOS/WMM 페이지에 정의된 두 가지 QoS 프로필 중에서 선택할 수 있습니다.

- Default : 모든 WMM(Wi-Fi MultiMedia) 매개변수에 대해 공장 초기 기본값을 사용합니다.
- User : 사용자가 정의한 WMM(Wi-fi MultiMedia) 매개변수를 사용합니다.

Distance Optimization:

링크의 길이가 300m 보다 긴 경우 이 옵션을 사용하십시오. 이 옵션은 Wi-Fi 내부 제한 시간 몇 가지를 업데이트하지만, 송신 출력을 증가하거나 감소시키지는 않습니다. 가장 먼 장치까지의 거리를 기입해야 합니다.

Beacon interval:

이 옵션을 사용하면, 두 개의 beacon 프레임 간격을 구성할 수 있습니다.

Beacon 은 AP, 메시 노드 및 애드혹(Ad-hoc) 스테이션에서 다른 장치에게 자신의 기능 및 설정 (HT 모드, SSID 등)을 알리기 위해 사용됩니다.

기본 설정은 802.11 모드에 따라 다릅니다.

Beacon 간격을 줄이면 채널에서 더 많은 대역폭을 사용하므로, 전체 Wi-Fi 성능이 저하될 수 있지만, 연결 손실을 더 빨리 감지할 수 있습니다.

Fragmentation Threshold:

이 옵션은 802.11a/b/g 모드에서, 최대 802.11 프레임 크기를 바이트 단위로 구성합니다. 이 임계값을 초과하는 프레임은 분할됩니다.

RTS/CTS Threshold:

채널에 간섭이 많고 Wi-Fi 성능이 좋지 않은 경우 CTS/RTS 를 사용합니다. 이 옵션은 대상인 802.11 a/b/g 프레임의 크기를 정의합니다. 이 크기를 초과하는 프레임은 CTS/RTS 프로토콜로 전송됩니다. 또는 숨겨진 스테이션이 있는 경우(예: 스테이션 A 와 B 사이의 교환에서, A 는 볼 수 있지만 B 는 볼 수 없는 세 번째 스테이션이므로, A 로 보낼 때 B 를 방해함)에도 사용합니다. 그 외에도 이 보호 기능이 global Wi-Fi 성능을 저하시키는 경우도 있습니다.

Retry settings:

일반적으로 특정 수신장치로 보내는 데이타 프레임은 확인 응답을 받습니다. 송신자가 확인 응답을 받지 못하면 프레임을 다시 보내야 합니다.

802.11n 에서는 여러 프레임을 하나의 큰 프레임으로 집합화한 A-MPDU(Aggregation Multi-PDU)로 보낼 수 있습니다. 독립적인 프레임은 개별 ACK 프레임에 의해 확인 응답을 받으며, A-MPDU 프레임은 A-MPDU 내의 각 서브프레임에 대한 하나의 확인 응답을 포함하는 단일 "block acknowledge" 프레임에 의해 확인 응답을 받습니다. 확인되지 않은 프레임은 나중에 A-MPDU 에서 재전송됩니다.

이 옵션을 선택하면, 재시도 횟수를 제어할 수 있습니다.

Short retry:

이 옵션은 물리 데이터 프레임 (단일 또는 A-MPDU)에 대한 재시도 횟수를 설정합니다.

Long retry:

이 옵션은 RTS/CTS 프로토콜로 전송된 물리 데이터 프레임(단일 또는 A-MPDU)의 재시도 횟수를 설정합니다.

Aggregate retry:

이 옵션은 A-MPDU 로 집계된 프레임(각각의 802.11 프레임이 A-MPDU 프레임으로 보내진 경우)에 대한 재시도 횟수를 설정합니다.

b. SETUP/PHYS. INTERFACES/WIRELESS SETTINGS/INTERFACE CONFIGURATION

이 섹션은 각 SSID 에 대해 복제됩니다. 설정은 선택한 SSID 에만 적용됩니다.

참고 : **Interface configuration** 섹션의 여러 역할에는 **Advanced settings** 탭이 있으며, 이를 **Device configuration** 섹션의 **Advanced settings** 과 혼동해서는 안됩니다.

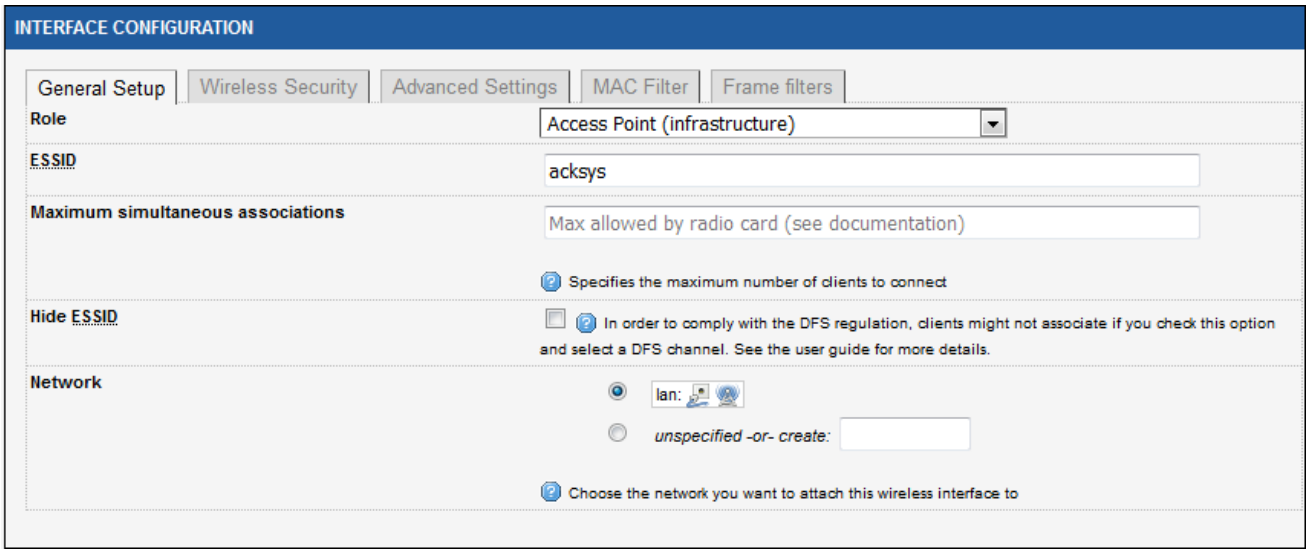
Loops pitfall in products with more than one radio

두 개 이상의 무선 카드가 장착된 제품에서는, 하나의 라디오를 일부 SSID 로 액세스 포인트로 활성화하고, 다른 라디오를 동일한 SSID 로 클라이언트로 설정하여, 무선 루프 문제가 생길 수 있습니다.

초기 기본값은, 두 무선을 내부적으로 함께 연결하고 동일한 SSID 를 가진 AP 역할로 설정하는 것이므 로, 두 무선을 모두 활성화하고 그 중 하나를 AP 역할에서 클라이언트 역할로 변경하면 이러한 루프가 생깁니다.

제품은 우선 순위가 높은 데이터 전송 (radio 1->wireless->radio 2->internal bridge->radio 1) 순으로 빠르게 전송됩니다. 복구할 수 있는 유일한 방법은 제품을 공장 초기화 후 재설정하는 것입니다.

General Setup, Access Point Mode



Role: 지원되는 roles 는 다음과 같습니다.

- Access point
- Isolating Access Point
- Client (connecting to an Access Point)
- RogueAP (WIDS)
- Mesh (802.11s)
- Point to multipoint station (ad-hoc)
- SRCC

ESSID:

무선 네트워크 이름을 설정합니다. 더 자세한 설정은 *V.1.15.1 Wireless architectures* 을 참고하세요.

Maximum simultaneous associations:

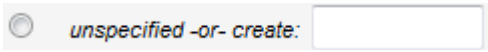
Access Point(무선 액세스 포인트)에서 동시에 연결 가능한 최대 클라이언트 수를 설정하는 것이며, 만약 로드 밸런싱 서비스가 활성화되어 있다면, 동시에 연결 가능한 최대 클라이언트 수를 정의해야 합니다.

Hide ESSID:

이 옵션은 네트워크에서 SSID 를 브로드캐스트하지 않도록합니다. 이는 스캐닝에서 AP 의 SSID 를 찾을 수 없기 때문에, 클라이언트가 미리 SSID 를 알고 있어야 한다는 것을 의미합니다. 숨겨진 SSID 및 DFS 고려 사항에 대한 자세한 내용은 *Radars detection overview (DFS)* 섹션을 확인하세요.

Network:

이 옵션을 사용하면 인터페이스가 추가된 네트워크를 선택할 수 있습니다. 초기 설정에서는 모든 물리 인터페이스(이더넷 및 무선 포트)가 **lan** 네트워크에 브리지되어 있습니다. 

만약 오른쪽 필드를 채우고 

유효성을 검사하면, 새 네트워크가 생성됩니다. 이 경우, 무선 인터페이스는 자동으로 이 새로운 네트워크에 추가되고 현재 네트워크에서 제거됩니다. 따라서, 매우 명확한 목적이 있는 경우에만 이 기능을 사용하고, 주의해서 사용해야 합니다. 더 자세한 설정은 *Network* 섹션을 참고하세요.

Mesh ID (only in Mesh mode):

Mesh 모드가 선택되면, 이 옵션은 ESSID(Extended Service Set Identifier)를 대체합니다. 이 필드에는 Mesh 이름을 기입합니다.

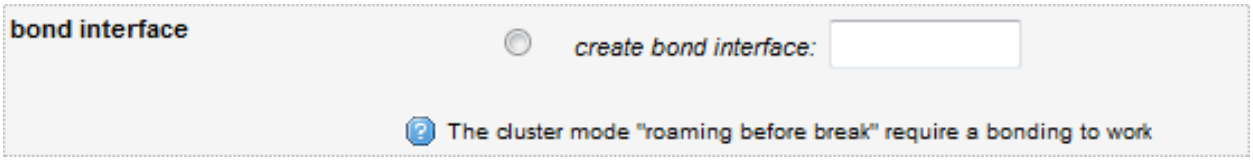
General Setup tab, Client mode

Multiple ESSIDs:

이 옵션을 선택하면, 단일 ESSID 항목이 Wireless network nicknames 항목으로 전환됩니다. 여러 개의 SSID 와 보안 매개변수를 선택할 수 있으며, 클라이언트는 이러한 조합 중 하나를 신호를 알리는 AP 에 연결합니다. 범위 내에 일치하는 AP 가 여러개인 경우, 우선 순위에 따라 SSID 를 선택할 수 있습니다.

이 기능을 사용하면 로밍 기능을 사용할 수 없으며, 보안은 해당 ESSID 와 별도의 메뉴에서 정의됩니다. 자세한 내용은 Wireless SSIDs 섹션을 참고하세요.

Global Parameters 의 **Cluster mode** 에서 **CBB(Connect before Break)** 를 선택하면, **Network** 필드가 **bond interface** 로 대체됩니다. 이 인터페이스에 이름을 지정해야 합니다.

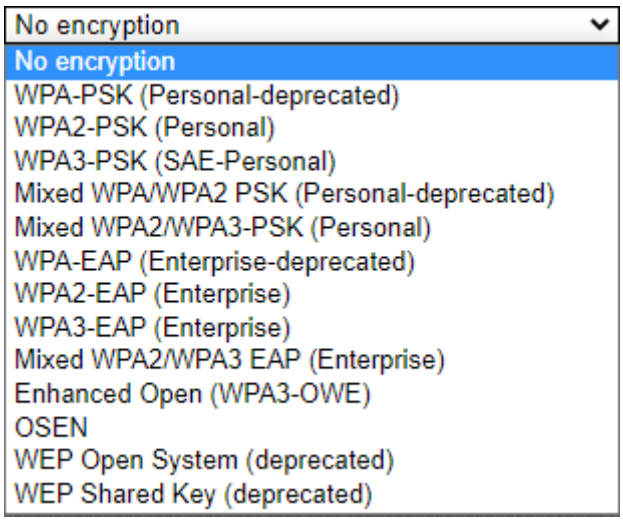


Wireless Security tab:

이 메뉴를 사용하면 해당 SSID 에 적용할 무선 보안 유형을 선택할 수 있습니다. 다른 보안 체계는 *Wireless security* 섹션에 설명되어 있습니다.

Security:

지원되는 모드는 우측 그림과 같습니다:



참고 1: 엔터프라이즈 클라이언트는 EAP-TLS 방법을 사용하는 WPA2-Enterprise 액세스 포인트를 제외하고는, 모든 유형의 WPA/WPA2 엔터프라이즈 액세스 포인트에 자동으로 적응합니다. EAP-TLS 방법을 사용하여 WPA2-Enterprise 을 사용하는 경우에는 CCMP 프로토콜의 사용이 강제되며, CCMP 를 제공하는 WPA2-Enterprise 액세스 포인트에만 연결됩니다.

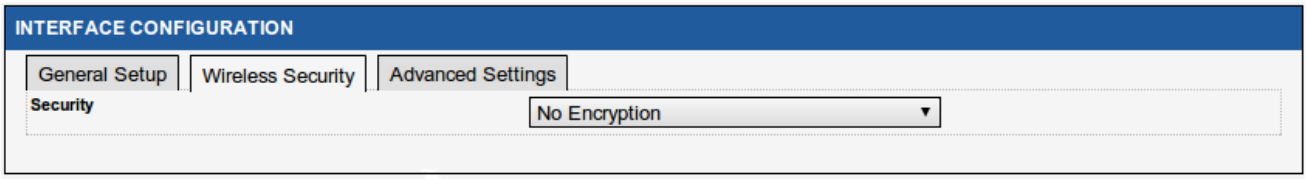
선택한 항목에 따라 일부 속성이 나타나거나 사라질 수 있습니다.

Fast Transition Support (802.11r):

이 상자는 WPA/WPA2 모드의 클라이언트에 대해서만 나타납니다. AP 에 대해 802.11r 프로토콜 사용을 허용하려면, 이 체크박스를 선택하세요. 로밍 시 인증에 필요한 시간을 줄일 수 있습니다.

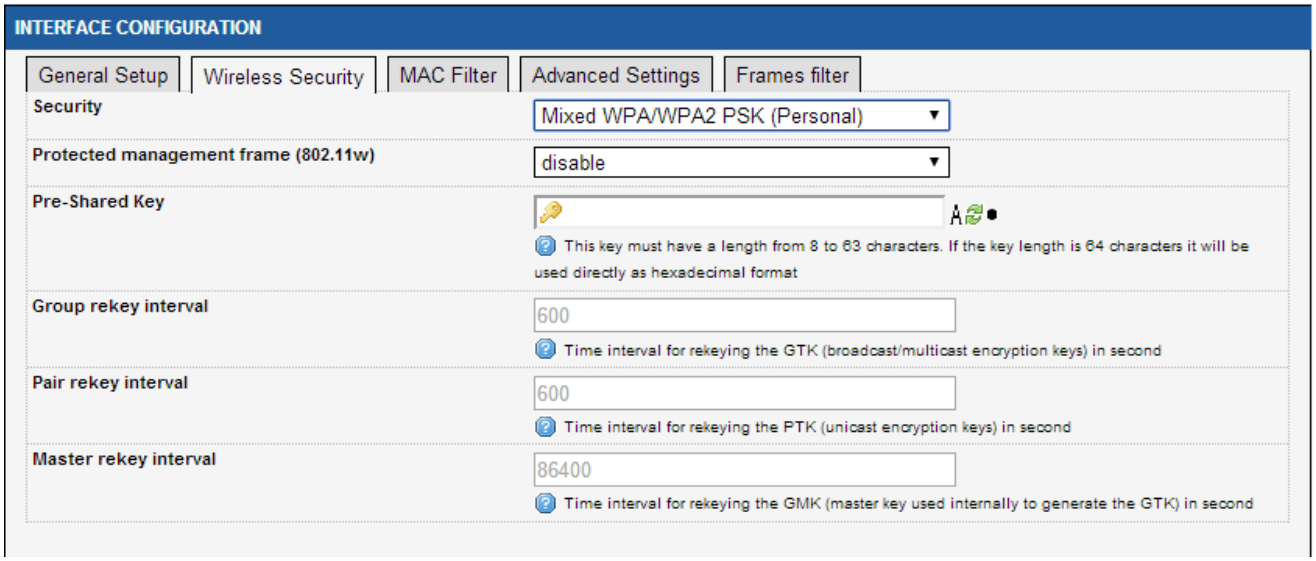
이 기능을 활용하려면 AP, 이동성 도메인 및 NAS ID 를 적절하게 구성해놔야 합니다.

Wireless Security tab, No Encryption mode:



여기에서는 설정할 항목이 없습니다

Wireless Security tab, WPA-PSK, WPA2-PSK, WPA3-PSK & PSK Mixed Modes:



Protected management frame (802.11w):

802.11w 보안 기능을 활성화/비활성화합니다. 이 옵션은 WPA3-PSK 및 혼합 WPA2/WPA3-PSK 에 숨겨져 있습니다. 더 자세한 정보는 *Protectedmanagement frame (802.11w)* 섹션을 참고하세요.

Pre-Shared-Key:

pre-shared (사전에 공유된) key 는 8~63 개의 ASCII 문자 또는 64 개의 16 진수(256 비트)일 수 있습니다. 오른쪽에 있는 녹색 화살표 아이콘을 사용하면 키를 입력하는 동안 일반 텍스트로 키를 표시할 수 있습니다.

Group rekey (AP mode only):

Interval : GTK(브로드캐스트/멀티캐스트 암호화 키) 키를 갱신하기 위한 간격(초) 입니다.

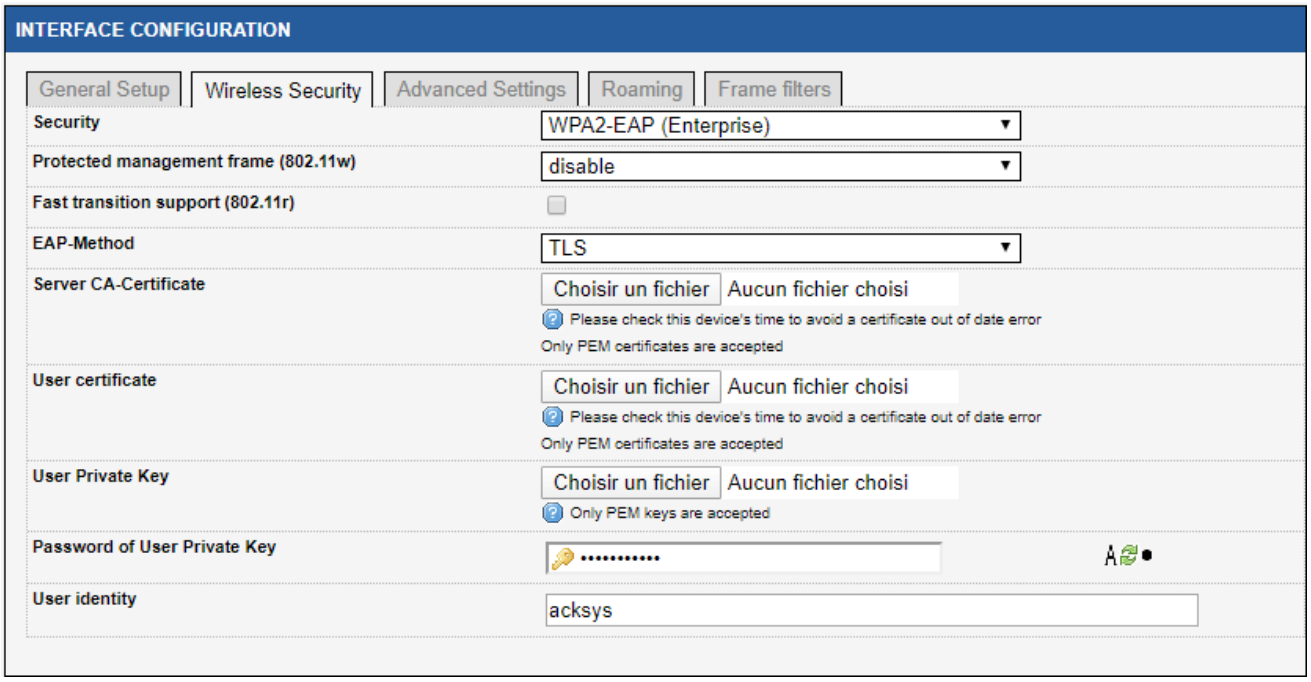
Pair rekey interval (AP mode only):

PTK(유니캐스트 암호화 키) 키를 갱신하기 위한 시간 간격(초)입니다.

Master rekey interval (AP mode only):

GMK(GTK 를 생성하기 위해 내부적으로 사용되는 마스터 키) 키를 갱신하기 위한 간격(초)입니다.

Wireless Security tab, WPA-EAP, WPA2-EAP, WPA3-EAP & EAP Mixed in Client Mode:



Protected management frame (802.11w):

802.11w 보안 기능을 활성화/비활성화합니다. 이 옵션은 WPA3-EAP 및 혼합 WPA2/WPA3-EAP 에 숨겨져 있습니다. 더 많은 정보는 *Protected management frame (802.11w)* 섹션을 참고하세요.

Fast Transition Support (802.11r):

WPA/WPA2 모드에서 이 항목을 체크하면, 802.11r 프로토콜을 지원하는 AP 에 해당 프로토콜을 사용할 수 있으므로, 로밍 시 인증시간이 단축됩니다.

잘 활용하기 위해서는 AP, mobility domain, NAS ID 를 적절하게 구성해야 합니다. 더 자세한 정보는 *Fast Transition Support (802.11r)* 섹션을 참고하세요.

Server CA-Certificate:

업로드할 CA 인증서 파일 위치를 선택합니다. 인증서와 키는 PEM(Privacy Enhanced Mail : 개인정보가 강화된 메일) 형식으로 제공되어야 합니다. 이 형식은 OpenSSL 프로젝트에서 정의합니다. "BEGIN"으로 시작하는 첫 줄과 base64 메서드를 사용하여 인코딩된 이진 데이터로 식별 가능한 텍스트 파일입니다.

EAP-Method:

이 항목은 사용할 EAP (Extensible Authentication Protocol)를 나타냅니다.

선택 가능한 방법은 TLS, PEAP, LEAP 입니다.

> 참고 1: 엔터프라이즈 클라이언트는 EAP-TLS 방법을 사용하는 WPA2-Enterprise 액세스 포인트를 제외하고는, 모든 유형의 WPA/WPA2 엔터프라이즈 액세스 포인트에 자동으로 적응합니다. EAP-TLS 방법을 사용하여 WPA2-Enterprise 을 사용하는 경우에는 CCMP 프로토콜의 사용이 강제되며, CCMP 를 제공하는 WPA2-Enterprise 액세스 포인트에만 연결됩니다.

EAP-Method TLS:

User certificate:

업로드할 사용자 인증서 파일의 위치를 선택합니다. PEM((Privacy Enhanced Mail: 개인정보가 강화된 메일) 형식으로 제공되어야 합니다.

User Private Key:

업로드할 개인 키 파일의 위치를 선택합니다. PEM 개인 키만 허용됩니다.

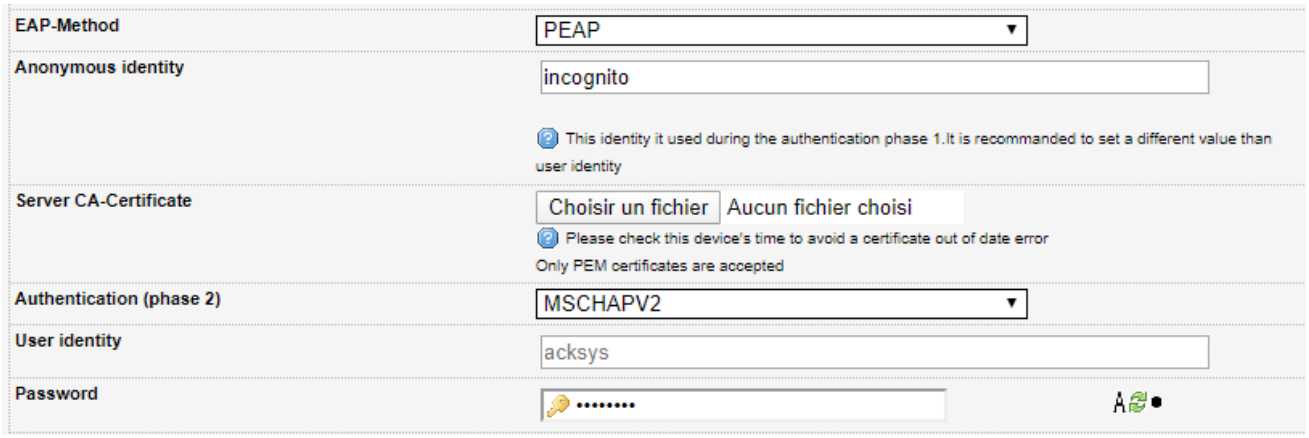
Password of User Private Key:

선택한 개인 키에 연결된 암호입니다.

User identity:

EAP-TLS 인증 중 사용할 로그인을 제공합니다. 이 인증 방법에서 이 필드는 RADIUS 서버에서는 거의 사용되지 않습니다. 기본값은 acksys 입니다.

EAP-Method PEAP:



Anonymous identity:

이 값을 사용하면 프로토콜의 1 단계에서 전송할 ID 를 구성할 수 있습니다. 이 값은 RADIUS 서버에서는 사용되지 않지만 TLS 터널을 설정하는 데 필요한 요소입니다. 이 필드는 네트워크에서 노출될 수 있으므로, 보안상 인증에 사용되는 로그인과 다른 값을 설정하는 것이 좋습니다.

이 필드를 비워 둔 경우, 인증 방법에 사용되는 ID(사용자 ID)가 사용됩니다.

Authentication (phase 2):

이 필드에는 인증 방법이 포함됩니다. 현재까지는 MSCHAPV2 만 사용할 수 있습니다.

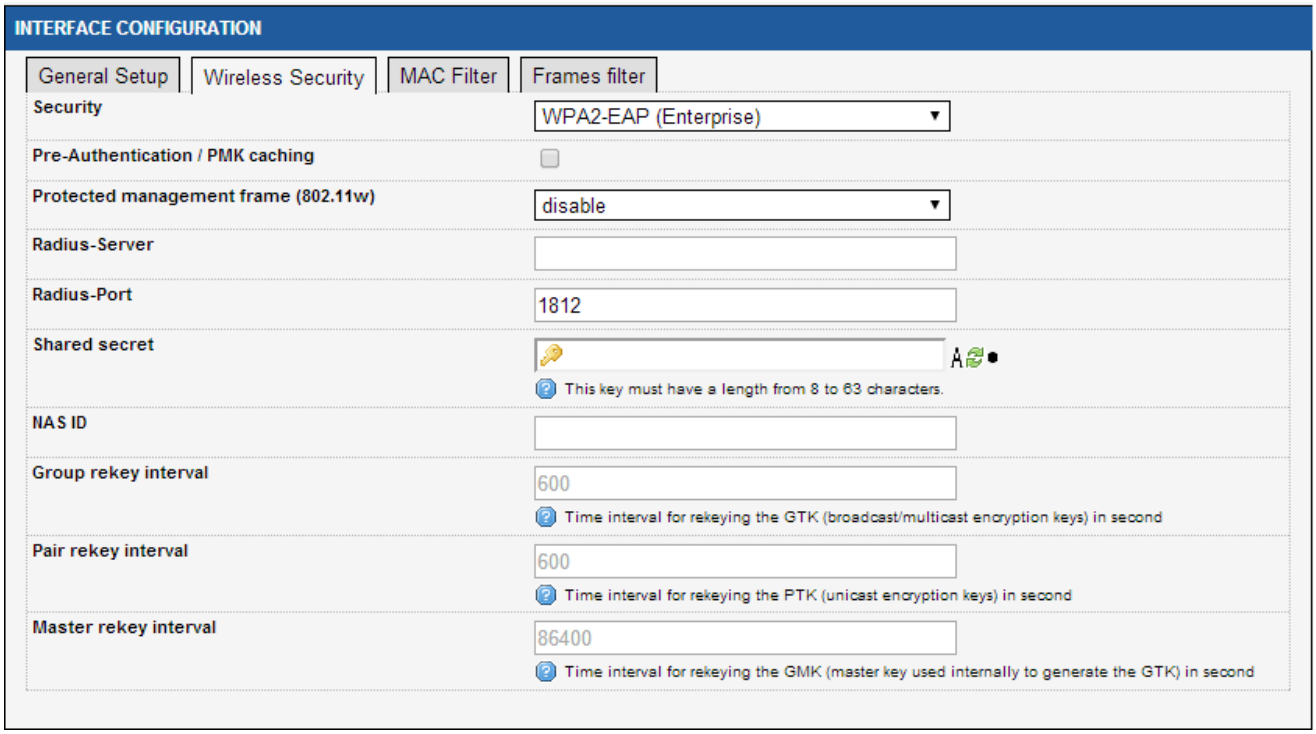
User identity:

인증에 사용되는 ID 입니다.

Password:

사용자 ID 에 대한 암호입니다.

Wireless Security tab, WPA-EAP, WPA2-EAP, WPA3-EAP & EAP Mixed in AP Mode:



Pre-Authentication / PMK caching :

WPA/WPA2-EAP 모드에서 사전 인증/PMK 캐싱 사용을 허용하려면 이 체크박스를 선택합니다. 더 많은 정보를 보려면 *Pre-authentication / PMK caching* 섹션을 참고하세요.

Protected management frame (802.11w) :

802.11w 보안 기능을 활성화/비활성화합니다. 이 옵션은 WPA3-EAP 및 혼합 WPA2/WPA3-EAP 에 숨겨져 있습니다. 더 자세한 정보는 *Protected management frame (802.11w)* 섹션을 참고하세요.

Radius-Server : Radius(Remote Aunthentication Dial In User Service) 서버의 IP 주소 또는 URI(Uniform Resource Identifier)를 기입합니다.

Radius-Port : Radius 서버의 UDP 포트를 기입합니다.

Shared secret : AP 와 radius 서버간에 공유되는 비밀번호로 8~63 자 여야 합니다.

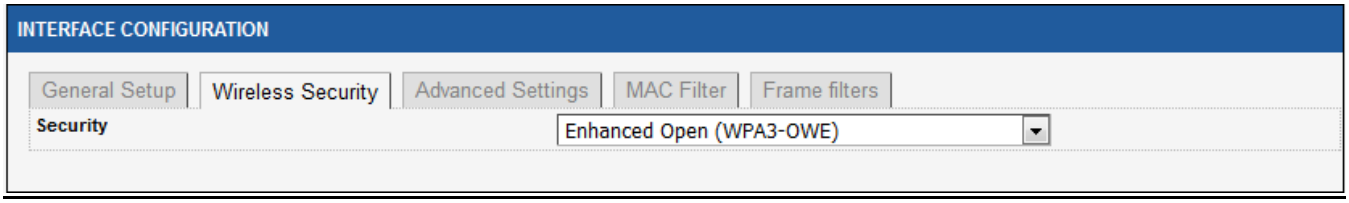
NAS ID : Network Access Server ID 로, 이 값은 IP 주소 대신 Radius 서버에서 사용될 수 있습니다.

Group rekey interval : GTK (브로드캐스트/멀티캐스트 암호화 키)를 갱신하기 위한 시간 간격입니다. (단위: 초)

Pair rekey interval : PTK (유니캐스트 암호화 키)를 갱신하기 위한 시간 간격입니다. (단위: 초)

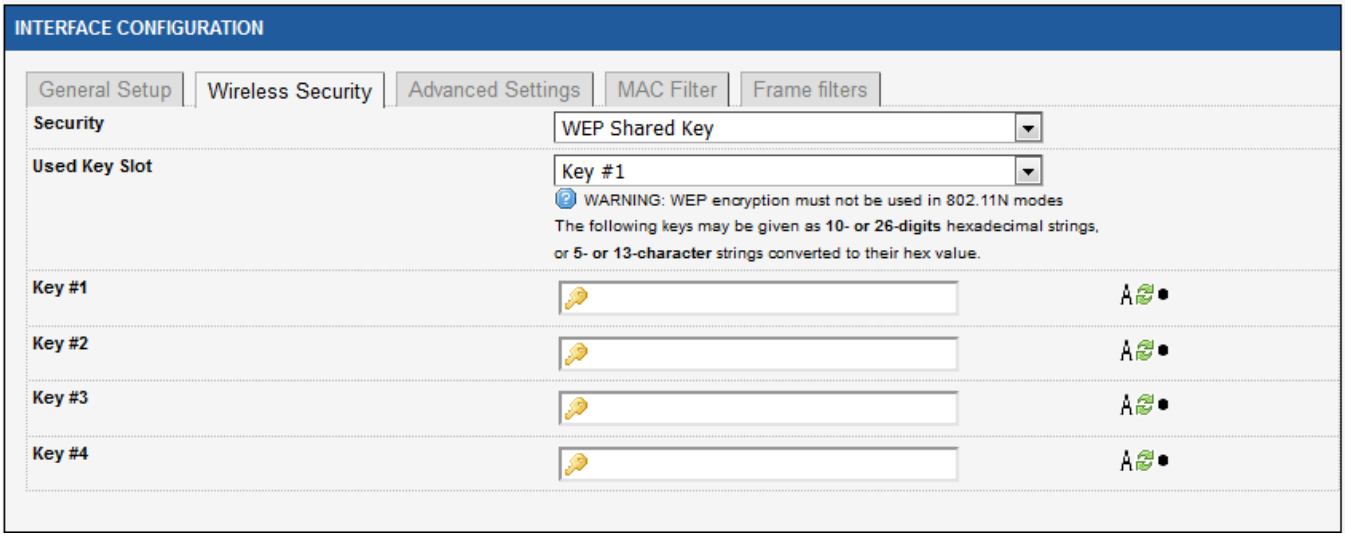
Master rekey interval : GMK (마스터 키를 사용하여 GTK 를 생성)를 갱신하기 위한 시간 간격입니다. (단위: 초)

Wireless Security tab, Enhanced Open (WPA3-OWE):



여기에서는 설정할 것이 없습니다.

Wireless Security tab, WEP Open System & WEP Shared Key:



Use Key Slot:

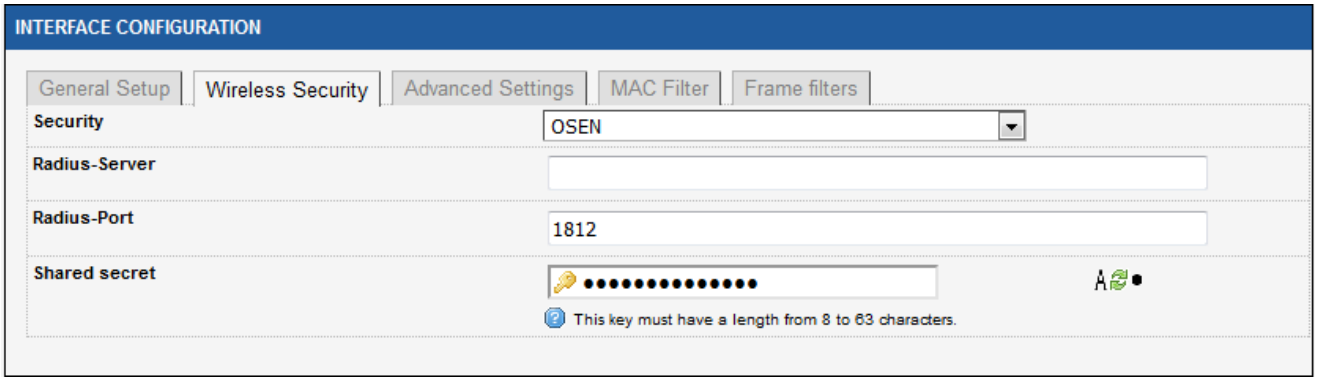
이 필드는 최근에 사용 중인 WEP 키를 선택합니다.

Key #1 to #4:

WEP 키가 포함되어 있습니다. 키는 HEX(16 진수 - 문자 0-9, A-F 사용) 또는 ASCII(영숫자 문자) 형식의 문자열을 입력하여 정의됩니다.

ASCII 형식은 기억하기 쉬운 문자열을 입력하는것을 제공합니다. ASCII 문자열은 네트워크에서 사용할 수 있도록 HEX 로 변환됩니다. 4 개의 키를 정의하여 쉽게 키를 변경할 수 있습니다. 네트워크에서 사용할 기본 키가 선택됩니다.

Wireless Security tab, OSEN:



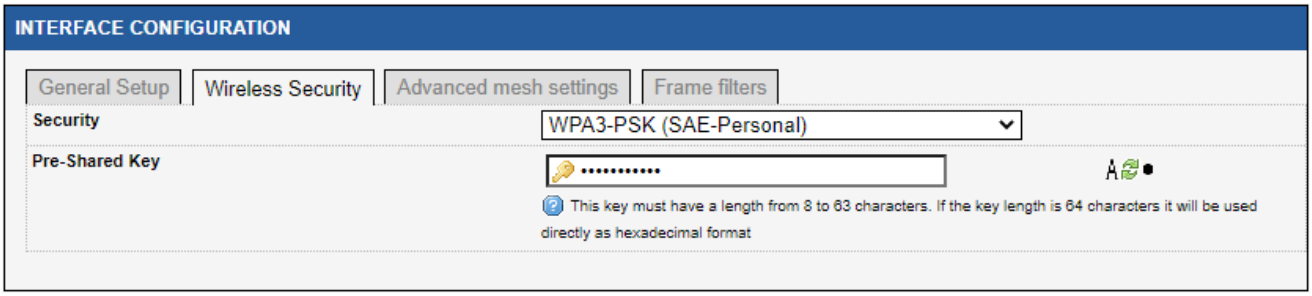
Osen 보안 모드는 Hotspot 2.0 r2 모드용으로 예약되어 있습니다.

Radius-Server: Radius 서버의 IP 주소 또는 URI 입니다.

Radius-Port: Radius 서버의 UDP 포트입니다.

Shared secret: 액세스 포인트와 Radius 서버 간에 공유되는 암호입니다.

Wireless Security tab, SAE Mode (in mesh mode):



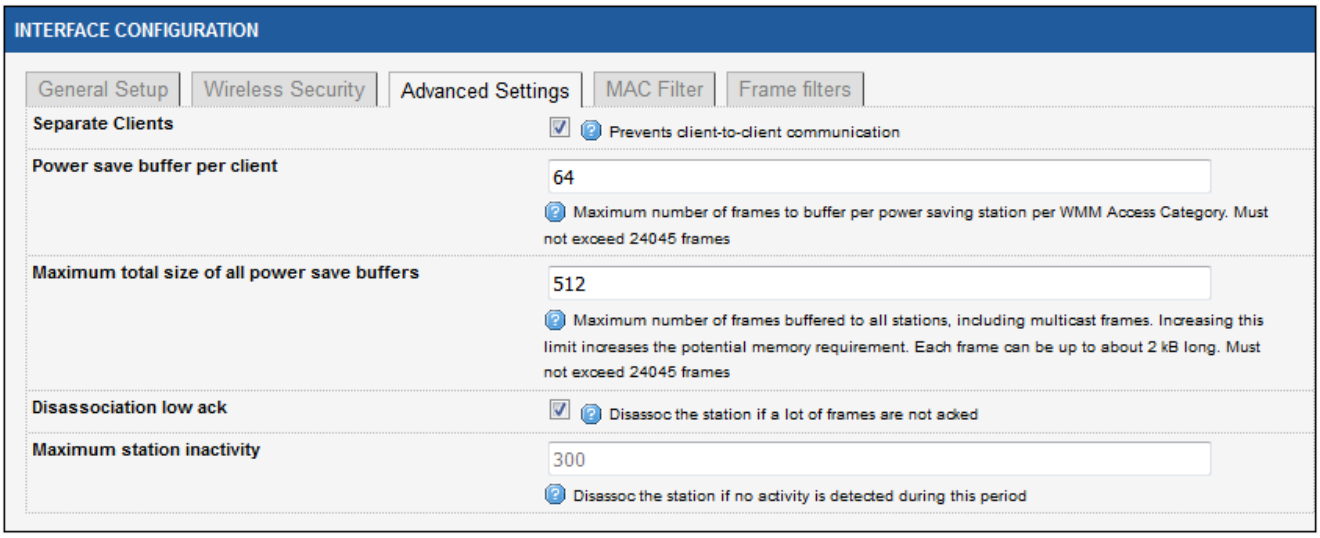
Security:

암호화 없음과 WPA3-PSK 중에서 선택하세요.

Pre-Shared key:

여기에 MESH 네트워크 공유 키를 입력하세요.

Advanced settings tab in Access point mode



Separate Clients:

이 옵션은 **Isolating Access Point** 역할을 선택한 경우에만 사용할 수 있습니다. 이 옵션을 체크하게 되면 클라이언트끼리 통신하는 것을 제한합니다. (이는 **Access point** 모드에서는 불가능합니다) 더 자세한 정보는 Infrastructure Mode 섹션을 참고하세요.

Power Save buffer per client:

각 클라이언트에 대해 대기할 수 있는 최대 프레임 수를 지정합니다. WMM (Wi-Fi Multimedia) 액세스 범주 및 절전 스테이션 당 버퍼링 할 최대 프레임 수입니다. 24,213 프레임을 초과해서는 안됩니다.

Maximum total size of all power save buffers:

모든 스테이션에 대해 버퍼링할 수 있는 최대 프레임 수를 지정합니다. 이 제한을 늘리면, 잠재적인 메모리 요구 사항이 증가합니다. 각 프레임은 최대 약 2KB 까지 가능합니다. 24,213 프레임을 초과해서는 안됩니다.

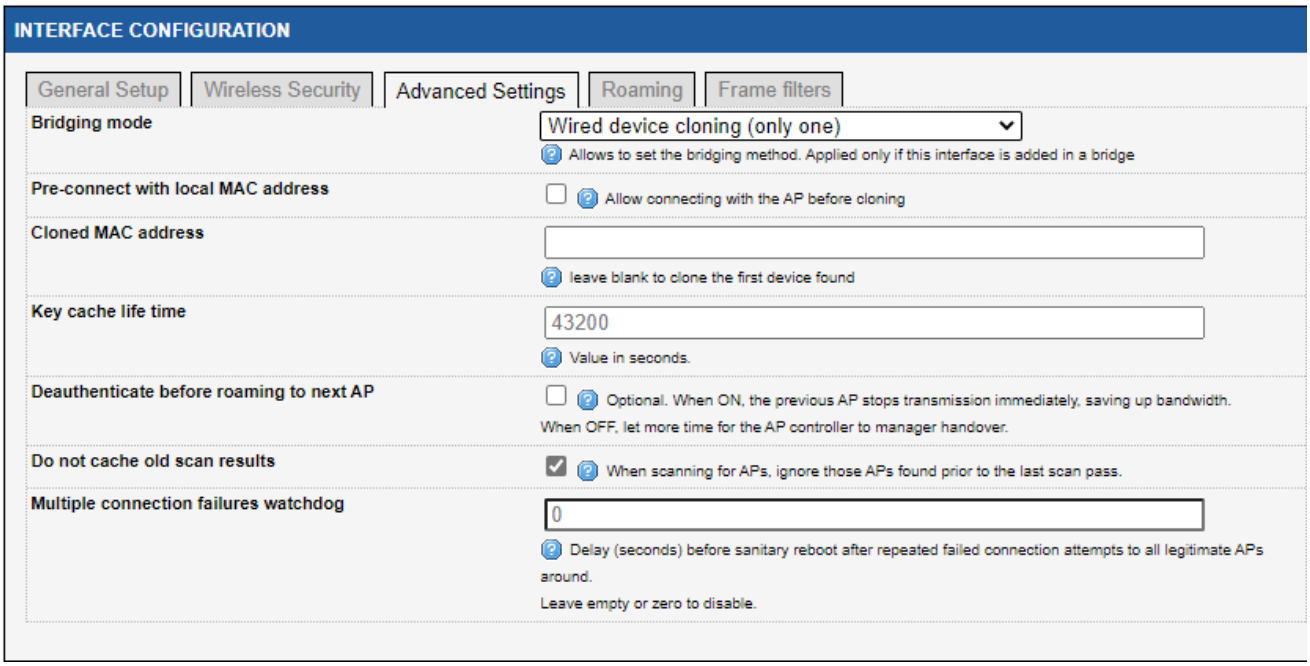
Disassociation low ack:

이 옵션을 설정하면, AP 에서 보낸 패킷이 50 개 이상 클라이언트에서 응답 확인되지 않으면, 클라이언트와의 연결이 끊어집니다. 대부분의 프레임에 응답이 없으면, 스테이션을 분리하세요.

Maximum station inactivity:

클라이언트의 연결이 끊어지기 전에 대기해야하는 시간(초)입니다. 기본값은 300 초(5 분)입니다. 이 시간동안 클라이언트가 활성화되지 않으면, 스테이션을 분리하세요.

Advanced settings tab in Client mode



Bridging mode:

이 옵션을 사용하면 이 인터페이스가 브리지에 추가되는 경우(자세한 내용은 *Network* 섹션 참고), 사용될 브리징 방법(자세한 내용은 *Wired to wireless bridging in infrastructure mode* 섹션 참고)을 선택할 수 있습니다.
사용 가능한 방법은 다음과 같습니다.

- ARPNAT (pseudo L2 NAT): 논리적인 IP 주소 (망 계층)를 물리적인 MAC 주소 (데이터 링크 계층)로 할당 및 매핑하는 주소 변환 방식으로 기본값으로 ARPNAT 가 선택되어 있습니다.
- 4 addresses format (WDS) : 무선과 유선 MAC 을 통해 무선 네트워크를 확장
- Wired device cloning
- PROFINET device cloning.

Cluster mode 에서 **Global Parameters** 로부터 **Connect before Break** 를 선택한 경우 4 개의 주소 형식(WDS)를 선택해야 합니다. Cloning 모드에 대한 자세한 정보는 *Cloning* 섹션을 참고하세요.

Pre-connect with local MAC address:

이 옵션은 유선 장치 또는 Profinet 장치 Cloning 에서만 사용 가능합니다. 체크하면, 이더넷 또는 Profinet 장비가 감지되지 않을 때, 로컬 무선 어댑터 MAC 주소를 사용하여 제품을 AP 에 연결할 수 있습니다. 이 경우 일정 시간이 지난 후 Ethernet 또는 Profinet 장비에 대한 Cloning 이 발생하면, 원격 장치의 ARP 테이블이 더 이상 유효하지 않게됩니다. 따라서 이러한 원격 장치는 ARP 테이블을 새로 고칠 때까지, 제품에 액세스할 수 없습니다.

Cloned MAC addr:

이 옵션은 유선 장치 또는 Profinet 장치 Cloning 에서만 사용 가능합니다. Cloning 에 사용되는 MAC 주소를 강제 적용하려면 이 필드에 입력하고, 검색된 첫 번째 장치를 Cloning 하려면 비워 두세요.

Key cache life time:

WPA/WPA2 EAP 에서만 사용 가능합니다. AP 가 OKC(Opportunistic Key Caching) 또는 Pre-authentication(사전 인증)을 지원하는 경우, 이 옵션을 사용하여 각 PMK 의 라이프 타임을 구성할 수 있습니다. 기본값은 43200 초(12 시간)입니다.
참고 : OKC 는 802.11 보안의 PMK 캐싱 기능을 기반으로 구축된 빠른 로밍 기능입니다. OKC 를 사용하면 여러 AP 가 PMK 를 공유할 수 있으며 클라이언트가 사전 인증을 수행하지 않고도 인증되지 않은 AP 로 로밍할 수 있습니다.

Deauthenticate before roaming to next AP:

이 옵션을 선택하면, 클라이언트가 다음 액세스 포인트로 로밍하기 전에 클라이언트가 현재 액세스 포인트를 인증 해제할 수 있으므로, 주파수가 더 빨리 해제됩니다. 이 옵션을 체크하지 않으면, AP 컨트롤러가 전송을 처리하는데 더 많은 시간을 할애합니다. 또한 이전 버전의 WaveOS 와의 호환성을 보장할 수 있습니다.

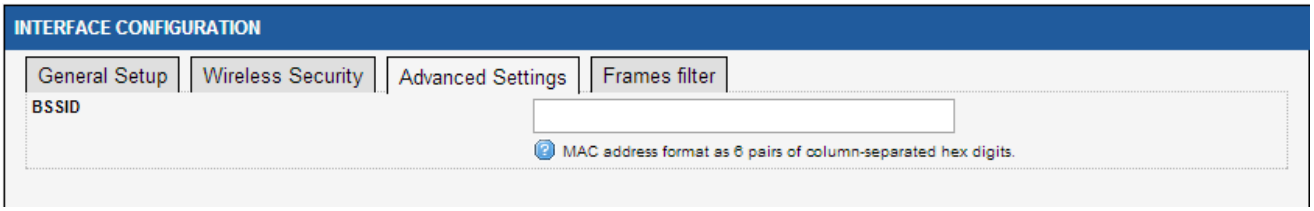
Do not cache old scan results:

이 항목을 체크하면, 이전 스캔 사이클의 스캔 결과가 현재 스캔 사이클의 결과와 병합되지 않습니다. 이 옵션은 기본적으로 선택되어 있습니다.

Multiple connection failures watchdog:

이 옵션을 사용하면, 범위 내에 후보 AP 가 있을 때, 액세스 포인트에 대한 연결이 시스템적으로 실패하는 경우, 장비를 재부팅하게끔 설정할 수 있습니다. 값은 초 단위로 표시됩니다.

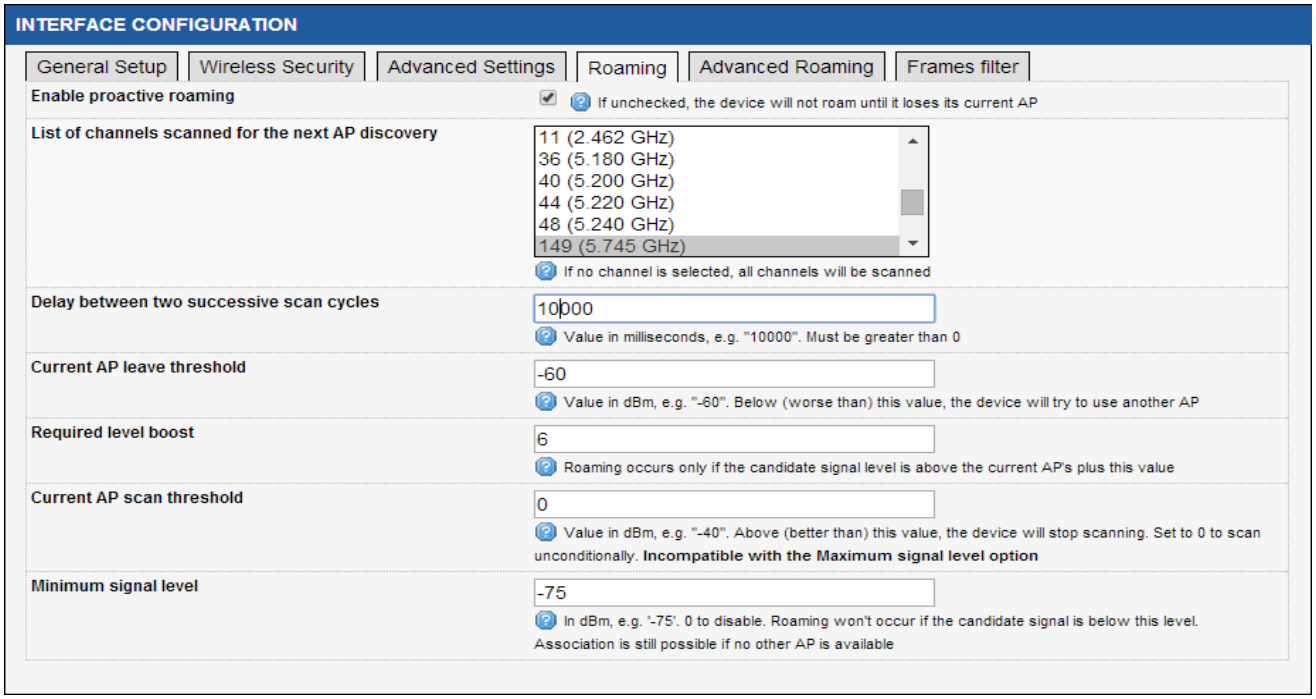
Advanced settings tab in Point to multipoint station (ad-hoc)



BSSID:

이 옵션을 사용하면, 이 인터페이스의 BSSID 를 MAC 주소 형식으로 설정할 수 있습니다. 형식은 6 쌍의 열로 구분된 16 진수 숫자(예: 12:34:56:78:9A:BC)입니다.

Roaming tab (only in Client mode):



브리징 모드가 '**4 addresses format (WDS)**' 로 설정된 경우에는 로밍 기능을 사용할 수 없기 때문에 이 탭이 나타나지 않습니다. 또한, Connect before Break 모드를 선택한 경우에만 Proactive Roaming 을 활성화해야 합니다.

Enable proactive roaming:

로밍 기능을 사용하려면, 이 항목을 체크하세요.

List of channels scanned for the next AP discovery:

AP 검색을 위해 스캔할 채널을 선택하세요. 이 선택은 위의 장치 구성 상자 채널 목록을 대체합니다. 두 개 이상의 채널을 사용하면 AP 가 서로 간섭하지 않으므로 밀도 있게 배치할 수 있습니다. 그러나 듀얼 라디오 제품을 사용하지 않는 한 클라이언트의 데이터 처리량이 감소하게 되는데, 스캔 프로세스는 AP 채널을 벗어나 다른 채널을 스캔하기 위해 주기적으로 전송을 중지해야 하기 때문입니다. 따라서 단일 무선 제품의 경우, 처리량을 최대치로 끌어올리려면 하나의 채널만 사용하시는 것이 좋습니다.

Delay between two successive scan cycles:

스캔 사이클 사이의 시간 (milliseconds)을 기입합니다.

Current AP leave threshold:

현재 AP 의 RSSI 값이 기입한 값 (dBm)보다 떨어지면 클라이언트는 현재 AP 를 떠나고 다른 AP 로 로밍을 시도합니다. 조건없이 스캔하려면 0 으로 설정하세요. 최대 신호 레벨 옵션과 호환되지 않습니다. *참고: 이전 버전에서는 이 매개변수의 이름이 Current AP minimum signal level 이었습니다.*

Required level boost:

새로운 AP 가 이전 AP 보다 얼마나 더 나은 신호 수신 성능을 보여야, 로밍이 실제로 발생할 수 있는지에 대한 최소한의 기준입니다. 현재 AP 의 신호레벨과 이 값을 더해 초과해야만 새로운 AP 로의 로밍이 발생합니다

Current AP scan threshold:

현재 AP 신호가 이 수준 (dBm) 이상이면 클라이언트는 더 나은 AP 에 대한 스캔을 중지합니다. 조건없이 스캔하려면 0 으로 설정하세요. 최대 신호 레벨 옵션과 호환되지 않습니다.

Minimum signal level:

로밍 대상이 아니라고 판단되는 AP 의 최소 신호 레벨 수치 (dBm)를 기입합니다. 로밍될 AP 후보의 신호가 이 레벨보다 낮으면 로밍이 발생하지 않습니다. 하지만 현재 연결된 AP 도 없고, 다른 AP 를 사용할 수 없다면 연결이 가능할 수도 있습니다. '-75' 또는 0 으로 표시하면 비활성화 됩니다.

Advanced Roaming tab (only Client with proactive roaming enabled):

INTERFACE CONFIGURATION

General Setup | Wireless Security | Advanced Settings | Roaming | Advanced Roaming | Frame filters

Excessive signal detection threshold
0
In dBm, e.g. '-30'. Leave empty or 0 to disable. Roaming will occur when the current AP signal crosses and exceeds this value, and there is an acceptable candidate around.
This allows elimination of approaching AP antennas that will be soon overtaken

Maximum signal level
0
In dBm, e.g. '-30'. Leave empty or 0 to disable. Must be greater or equal to the 'Excessive signal detection threshold'. Roaming will occur whenever the current AP signal is above this value, and there is an acceptable candidate around. When selecting the next AP, the ones above this value are considered last

Maximum time above maximum level
0
In number of scan cycles. Leave empty or 0 to disable. Maximum time allowed with a signal level superior to Maximum without a disconnection when no other APs are available for roaming. Furthermore, when this option is activated, the client will not connect to any AP superior to Maximum.

Maximum time under minimum level
0
In number of scan cycles. Leave empty or 0 to disable. Maximum time allowed with a signal level inferior to Minimum without a disconnection when no other APs are available for roaming. Furthermore, when this option is activated, the client will not connect to any AP inferior to Minimum.

Minimum roaming interval
0
In ms. Leave empty or 0 to disable. Roaming won't occur before this delay has elapsed since the last association

No-return delay
0
In ms. Leave empty or 0 to disable, max 180000 (3 mn). Roaming won't occur to an AP that was left recently (before this delay gos elapsed). The delay is cleared for APs that are not around anymore

Threshold hysteresis
2
Value in dBm, e.g. "2". Hysteresis used for all thresholds. This value will be added and substracted to each threshold to set the corresponding threshold hysteresis interval

RSSI smoothing factor
Last beacon weight: 19%
The RSSI of the current AP is computed over the last few beacons received. Select the importance of the last beacon relative to older ones. This value commands a decaying factor. Default: 19%

Beacon timeout
7
Value in beacon interval units

Probe on beacon timeout
☑ When beacon time out occurs, probe the current AP for the last time in the hope that deauthentication won't be needed if the AP answers.

Maximum time off-channel
125
In ms. Maximum delay offchannel (during which data must be buffered by the associated AP). Several channels will be scanned without returning to the base channel, until this delay is exhausted. An upper limit of 10 times the beacon interval of the current AP is enforced

Offchannel adaptation delay
30
In ms. Adaptation delay after a channel switch, before sending the probe request or accepting beacons. Reducing below 30 ms speeds up scanning but decreases AP detection likelihood

Per channel probe response delay
30
In ms. Time to wait for an answer from the access points.
For DFS channels, where probes are forbidden, a floor value of 108 ms is enforced to ensure beacon detection

Roaming log info
- ☐ Display scan process while associated
- ☐ Display scan process while un-associated
- ☐ Display best bssid selection comparison
- ☐ Display roaming parameters
- ☐ Log filtered table of APs used to select the best AP (limited to line buffer available space)
- ☐ Include unfiltered APs in the above table (show all APs seen)
- ☐ Rise log level used to display reasons for filtering out APs
- ☐ Display roaming state changes

Select the roaming log info will show in product log.
To show the log you must to set the wireless client log level to roaming or more and general log level to notice or more in 'log settings' section.

Excessive signal detection threshold:

현재 AP 의 인식된 신호 레벨 (dBm)이 이 한계치를 초과하면, 클라이언트는 다른 AP 로 로밍을 시도합니다. 비활성화 하려면 비워 두거나 0 으로 설정하세요.

Maximum signal level:

이 수준 (dBm)이상의 AP 는 로밍할 다음 AP 를 선택할 때 우선 순위가 낮습니다. 'Excessive signal detection threshold' 보다 크거나 같아야 합니다. 비활성화 하려면 비워 두거나 0 으로 설정하세요.

Maximum time above maximum level:

다른 AP 가 로밍할 수 없는 경우, 연결 끊김 없이 최대한으로 인지 신호 수준을 유지할 수 있는, 최대 시간(스캔 주기 수)입니다. 이 옵션을 활성화하면, 클라이언트는 Maximum 이상의 AP 에 연결하지 않습니다.

Maximum time under minimum level:

다른 AP 가 로밍할 수 없는 경우, 연결 끊김 없이 최소한으로 인지 신호 수준을 유지할 수 있는, 최대 시간(스캔 주기 수)입니다. 이 옵션을 활성화하면, 클라이언트는 Minimum 이하의 AP 에 연결하지 않습니다.

Minimum roaming interval:

모든 AP 가 동일하게 매우 낮은 레벨일 경우, 더 이상 로밍하지 않으려면, 두 개의 연속 로밍 프로세스 사이에 최소 지연시간 (ms)을 적용할 수 있습니다. 비활성화 하려면 비워 두거나 0 으로 설정하세요.

No-return delay:

벽이 많은 지역에서 너무 멀리 떨어져 있는 AP 가 무선 전파의 튕기는 성질때문에 잠시동안 신호가 매우 좋아 보일 수 있습니다. 이런 종류의 AP 로 다시 로밍하지 않으려면, 이 항목에 지연시간 (ms)을 추가할 수 있습니다. 비활성화 하려면 비워 두거나 0 으로 설정하세요. 최대치는 180000ms (3 분)입니다.

Threshold hysteresis:

측정된 수신 신호가 불안정 할 때 진동하는 동작을 피하기 위해 스캔, 탈락 및 과도한 한계값은 폭 ± 이력(履歷)현상으로 해석됩니다. dBm 단위로 표시(예: "2")하며 모든 한계값에 사용되는 이력을 나타냅니다. 이 값은 해당되는 한계값 이력 간격을 설정하기 위해 각 한계값에 가감됩니다.

RSSI smoothing factor:

한계값은 현재 AP 로부터 수신된 beacon 의 평균 출력과 비교됩니다. 평활 요소는 이동 평균 계산에서 이전 beacon 이 사라지는 속도를 조정합니다. 현재 AP 의 RSSI 는 수신된 마지막 몇 개의 beacon 들로 계산됩니다. (기본값: 19%)

Beacon timeout:

연결을 해제하고, 새 AP 를 검색하는 현재 AP 에서, 연속적으로 누락된 beacon 의 수입니다. 해당 기간은 AP 에 설정된 beacon 간격에 따라 다릅니다.

Probe on beacon timeout:

beacon 누락으로 인해 연결이 해제되기 전에, 클라이언트는 짧은 데이터 프레임을 보내고, 이 프레임이 승인되면 연결을 해제하지 않습니다.

Maximum time off-channel:

관련 AP 에 의해 데이터가 버퍼링 되어야 하는 기간입니다. 클라이언트가 다른 채널을 스캔할 때, 현재 AP 는 클라이언트가 AP 의 채널로 돌아올 때까지 들어오는 데이터를 버퍼링하라는 요청을 받습니다. 일부 AP 는 그 동안 버퍼가 부족해서 데이터가 손실됩니다. 이 매개변수는 스캐너가 다른 채널을 스캔하는 기간을 제한하므로, AP 버퍼가 소진되기 전에 AP 채널로 돌아가게끔 할 수 있습니다. 이 기간은 다음 두 매개변수의 합보다 크게 설정해야 합니다. 이 기간은 AP beacon 간격의 지속 기간으로 자동 줄어듭니다. 정밀도는 약 10ms 입니다.

이 매개변수가 충분히 크면 스캐너는 현재 AP 채널로 돌아가기 전에, 채널을 전환하고 여러 번 프로브를 보낼 수 있습니다.

Off-channel adaptation delay:

채널 전환 후 프로브 요청을 보내거나 beacon 을 수락하기 전에, 충돌을 피하기 위한 지연시간입니다. (ms) 30ms 이하로 감소하면 스캔 속도가 빨라지지만, AP 감지 가능성이 감소합니다.

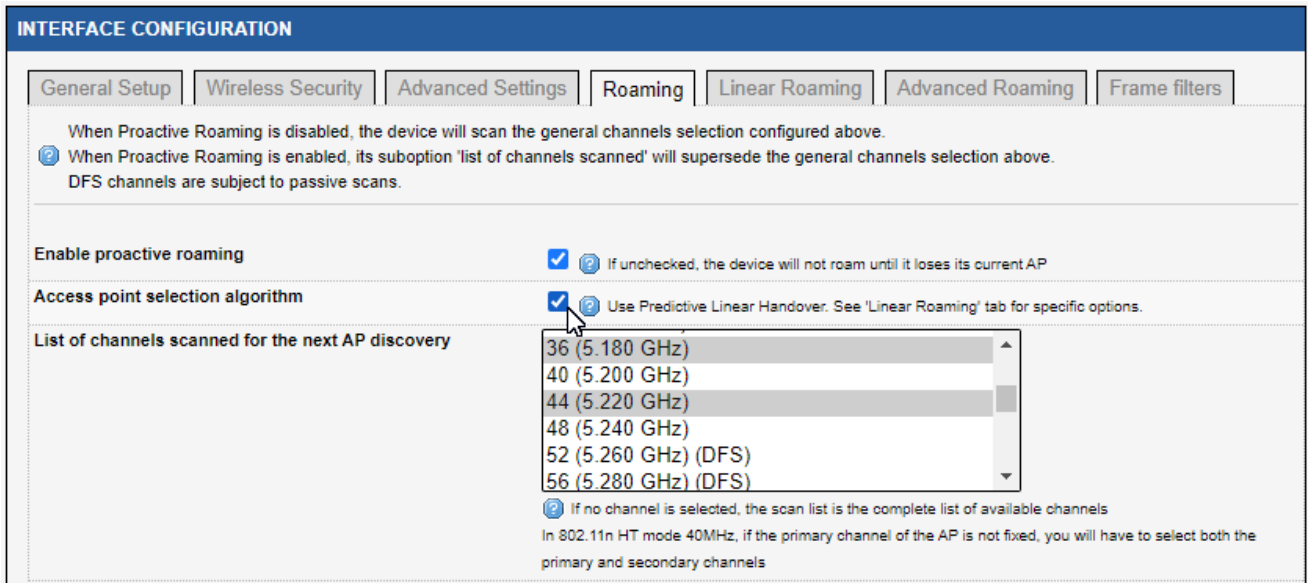
Per channel probe response delay:

AP 로부터 응답을 기다리는 시간입니다. (ms)
프로브 요청을 보내고 프로브 또는 beacon 을 기다린 후, 스캐너가 스캔된 채널에 머무는 시간입니다. 이 매개변수를 조정하려면 프로브 요청에 응답할 때, 채널 트래픽과 AP(또는 해당 컨트롤러)의 신속성을 고려해야 합니다.
프로브가 금지된 DFS 채널의 경우, beacon 감지를 보장하기 위해 108ms 의 최소값이 적용됩니다.

Roaming log info:

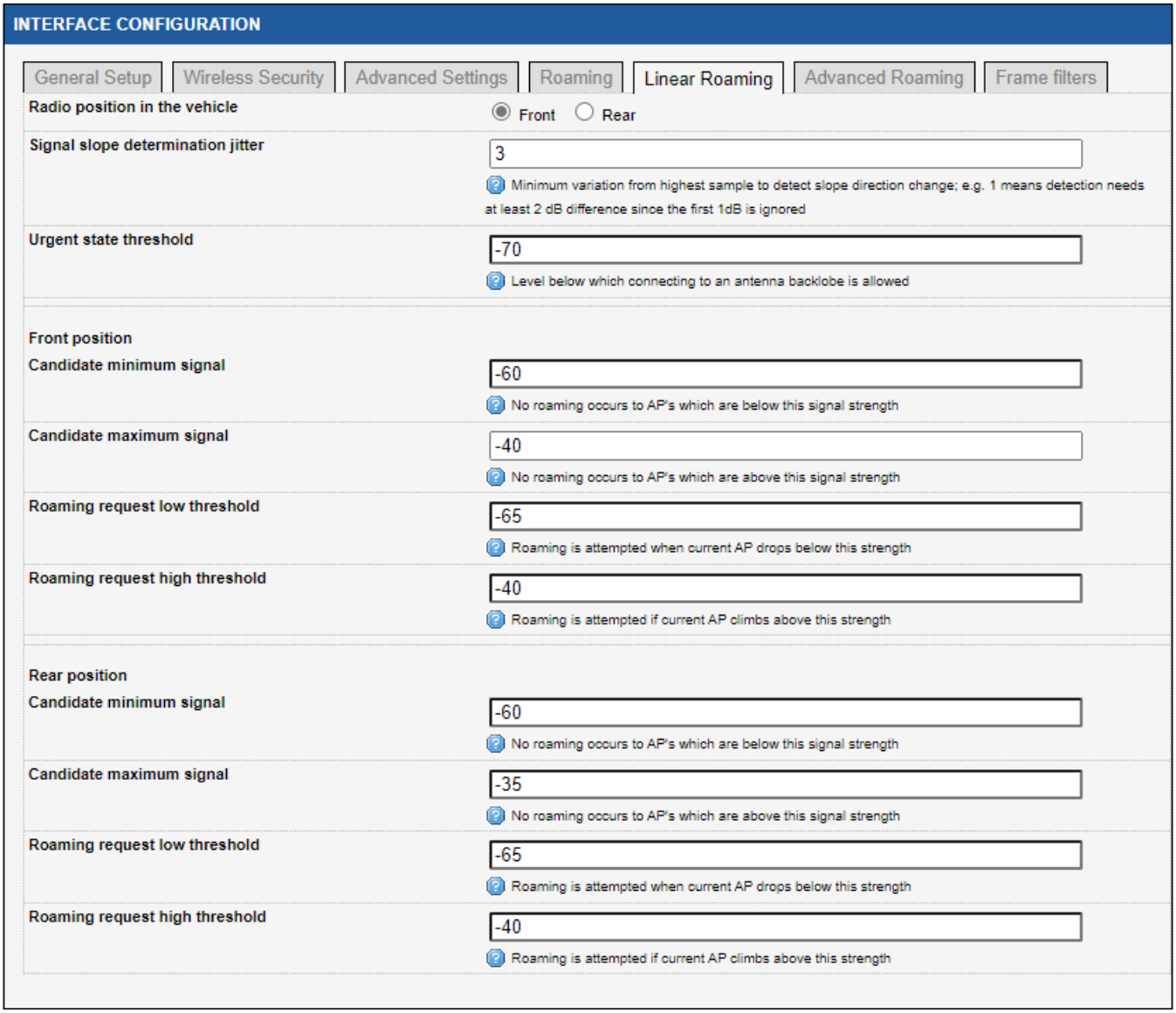
로그에 표시해야 하는 로밍 정보를 선택하세요. 무선 로그 수준은, 로밍 수준 이상으로 설정해야 합니다. (섹션 Log settings 참고)

Roaming tab with CBB (only in Client mode):



AP 알고리즘 선택 상자는, Connect Before Break 를 선택한 경우에만 나타납니다.
선택하면 **Linear Roaming** 이라는 새 탭이 표시됩니다.

Linear Roaming (Only in Client mode with CBB):



Radio position in the vehicle:

제품이 차량의 전면에 장착되었는지 뒷면에 장착되었는지 여부를 여기에 표시하십시오. 이를 통해 소프트웨어가 신호 강도의 변화에 맞게 분석할 수 있습니다.

Urgent state threshold:

이것은 안테나 backlobe(안테나에서 발생하는 신호의 반사로 인해 발생하며, 안테나의 후방으로 향하는 방향으로 나가는 신호입니다.)에 연결을 허용하는, 최대 신호 레벨입니다.

Signal Slope determination jitter:

경사 방향 변화를 감지하기 위해, 가장 높은 샘플과 비교한 최소 변화 수치를 여기에 기입하세요. 여기서 주의할 점은, 첫 번째 dB 는 무시되므로, 값 1 의 경우 감지하려면 최소 2dB 의 차이가 필요합니다.

Do not roam if current AP is the best candidate:

서로 다른 임계값의 구성으로 인해 현재 AP 가 최상의 후보일 때 알고리즘이 로밍을 유발할 수 있습니다. 이 옵션을 사용하면 이 동작을 피할 수 있으므로 불필요한 로밍 횟수를 제한할 수 있으며, 대부분의 경우 동일한 AP 에서 다시 로밍됩니다.

Candidate minimum signal (Front position & Rear position):

AP 로밍이 허용되려면, 이 AP 의 신호 강도는 이 값과 동일하거나 커야 합니다.

Candidate maximum signal (Front position & Rear position):

AP 로밍이 허용되려면, 이 AP 의 신호 강도는 이 값과 동일하거나 작아야 합니다.

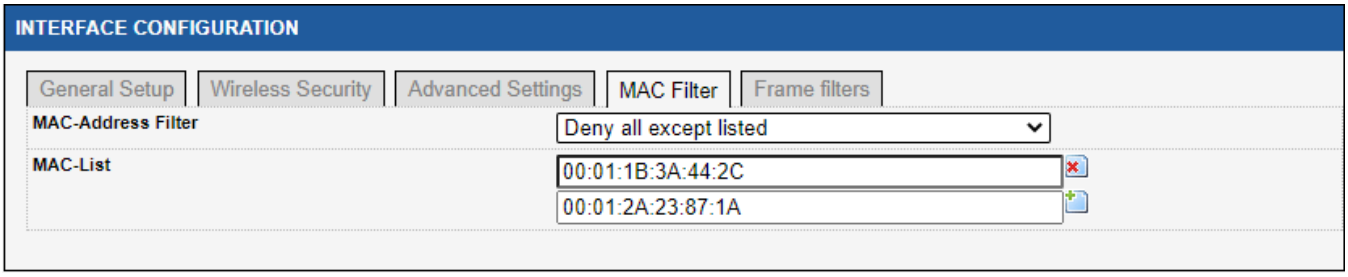
Roaming request low threshold (Front position & Rear position):

현재 AP 의 신호 강도가, 이 값 아래로 떨어지면 로밍이 허용됩니다.

Roaming request high threshold (Front position & Rear position):

현재 AP 의 신호 강도가, 이 값 이상이면 로밍이 허용됩니다.

MAC filter tab (only in Access Point modes):



MAC-Address filter:

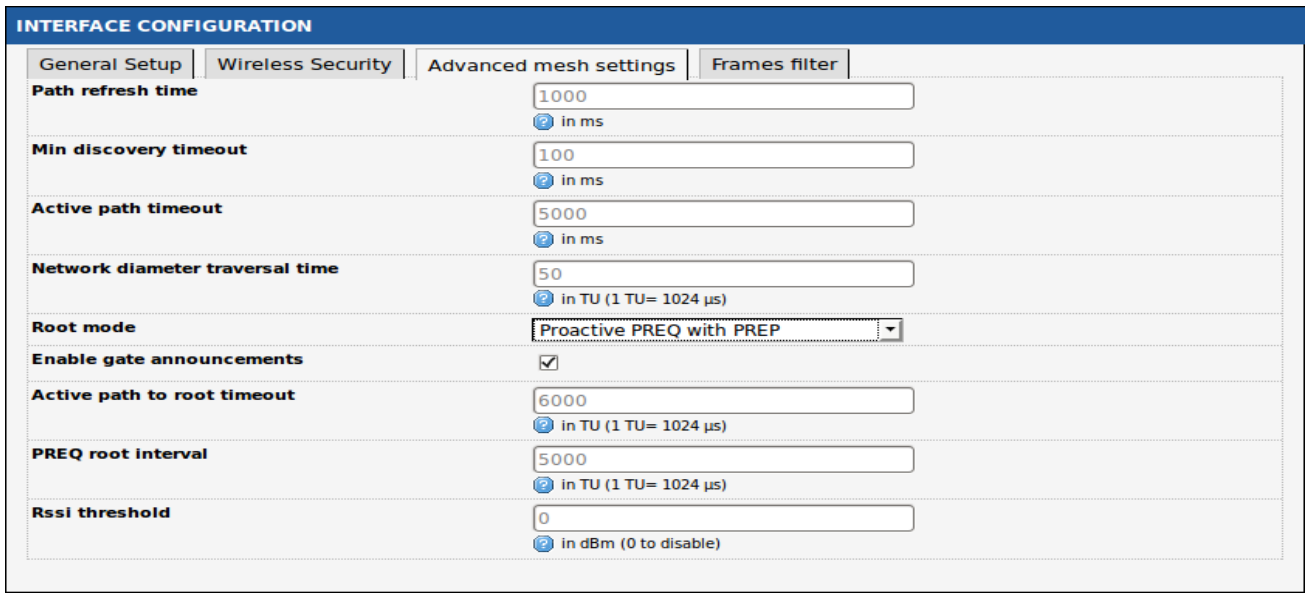
허용 또는 거부할 클라이언트 MAC 주소 목록을 지정할 수 있습니다. 필요하지 않은 경우 필터를 비활성화하세요. 다만 주의할 점은, MAC 주소는 쉽게 조작할 수 있기 때문에 이 기능만으로는 보안 역할을 할 수 없습니다.

MAC-List:

허용 또는 거부할 클라이언트 MAC 주소를 입력하세요. MAC 주소는 두 자리씩 콜론(:)으로 구분된, 16 진수 문자열로 입력합니다.

마지막 필드 오른쪽의 추가 아이콘 을 클릭하여 새 주소를 추가할 수 있습니다. 필드 오른쪽의 제거 아이콘 을 클릭하여, 주소를 제거할 수 있습니다.

Advanced mesh settings tab (only in 802.11s mode):



Path refresh time:

이전에 검색된 경로를 통해 데이터를 전송할 때, 해당 경로가 *path refresh time* 보다 빨리 만료될 경우, 만료되기 전에 미리 검색을 시작하여 경로가 만료될 때 이미 갱신되도록 합니다. 이렇게하면 데이터 대기 시간이 줄어들게 됩니다. *path refresh time* 은, *active path timeout* 보다 작아야합니다. (ms)

Min discovery timeout:

경로 검색 요청이 전송될 때, **min discovery timeout** 후 응답이 수신되지 않으면 경로 검색 요청이 재전송됩니다. 이 검색 시간초과는 같은 경로에 대해 연속적으로 시간초과가 발생하면 두 배로 증가합니다. 이 값은 'network diameter traversal time' 의 두 배 이상이어야 하므로, 시간 초과는 네트워크에서 가능한 최대 경로를 통과하는, 요청과 응답을 모두 포함하도록 해야 합니다. (ms)

Active path timeout:

이것은 경로가 유효하다고 간주되는 지연 시간입니다. 즉, 경로 갱신이 강제로 되기 전에, 캐시 테이블에 보관하고 사용될 수 있습니다. 경로 검색 대상은, 응답에 이 값을 삽입합니다. 요청자는 최대 이 시간 동안 경로를 사용할 수 있으며 그 후에는 검색을 갱신해야 합니다. (대상이 이동한 경우)

Network diameter traversal time:

HWMP 프레임이 메쉬를 통해 전파되는 데 필요한 예상 시간입니다.

Rssi threshold:

이미 연결되었거나 프로세스를 시작할 수 없는 경우, 이 한계값 미만이면 플링크 (plink)가 닫힙니다. 또한 설정되지 않으면 피어링 프로세스를 시작할 수 없는 dBm 임계값입니다. 이 기능을 사용하지 않으려면 0 을 입력하세요.

Root mode:

이것은 이 스테이션이 루트 노드인지 여부와 이 사실을 다른 스테이션에 알리는 방법을 나타냅니다. 루트 노드는 주기적으로 브로드캐스트를 해서 다른 모든 노드에 자신의 존재를 알립니다. 이렇게 하면 라우팅 결정 속도가 빨라질 수 있습니다. 여러

스테이션을 같은 메시에 루트 모드로 설정할 수 있지만, 브로드캐스트 메시지 오버헤드는 사용 가능한 대역폭을 줄입니다. 여기에서는 세 가지 루트 모드를 사용할 수 있습니다. 자세한 내용은 IEEE 802.11-2012 standard, chapter 13 을 참조하세요.

- Proactive PREQ : 루트 스테이션은, 모든 노드에서 루트로 데이터 경로를 설정하는 브로드캐스트 HWMP PREQ 프레임을 주기적으로 보냅니다.
- Proactive PREQ with PREP: 루트 스테이션은, 모든 노드에서 루트로 데이터 경로를 설정하는 브로드캐스트 HWMP PREQ 프레임을 주기적으로 전송하고, 루트에서 모든 노드로의 역 데이터 경로를 설정하는 HWMP PREP 프레임으로 응답하도록 요구합니다.
- Proactive RANN: 루트 스테이션은, 주기적으로 브로드캐스트 HWMP RANN 프레임을 보내 자신의 주소를 알립니다. (수신 스테이션은 유니캐스트 PREQ 를 사용하여 루트에 대한 경로를 요청합니다.)

다음 매개변수는 정확한 루트 모드에 따라 다릅니다.

Enable gate announcements (root mode only):

메시 외부의 네트워크에 액세스 할 수 있는 경우, 설정해야하는 플래그입니다. 이 경우에 네트워크는 브리지 기능을 갖고 있기 때문에 항상 true 입니다. 이 플래그는 다른 모든 노드에게 전송되어, 해당 루트 노드를 통해 메시 외부의 MAC 주소에 액세스 할 수 있음을 알리는 역할을 합니다.

Active path to root timeout (root mode only):

이 값은 proactive PREQ 에 의해 보내지는 값으로, Active path timeout 과 동일하지만, 이 루트 노드에서만 사용됩니다.

PREQ root interval (PREQ root modes only):

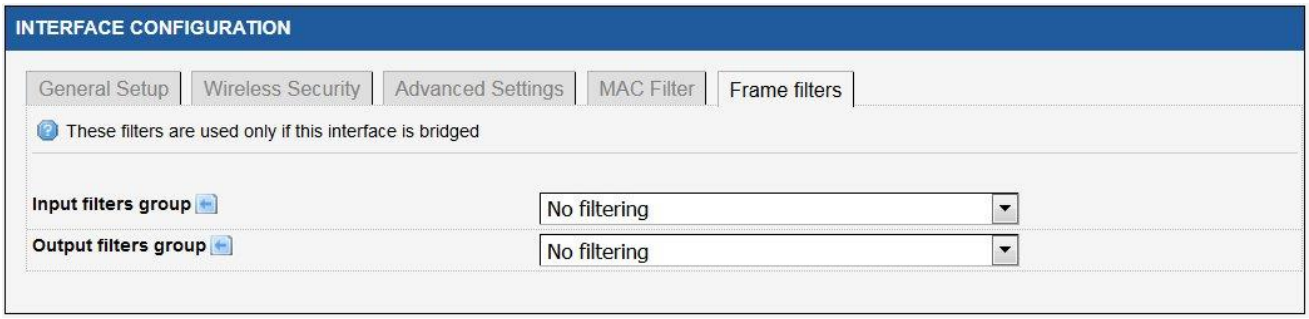
이 값은 proactive PREQ 브로드캐스트간의 시간 간격을 나타냅니다.

RANN root interval (RANN root mode only):

이 값은 proactive RANN 브로드캐스트간의 시간 간격을 나타냅니다.

Frames filter tab:

브리지 형식 네트워크 인터페이스에 포함된 무선 인터페이스는, 프레임이 통과할 때 필터링할 수 있습니다.



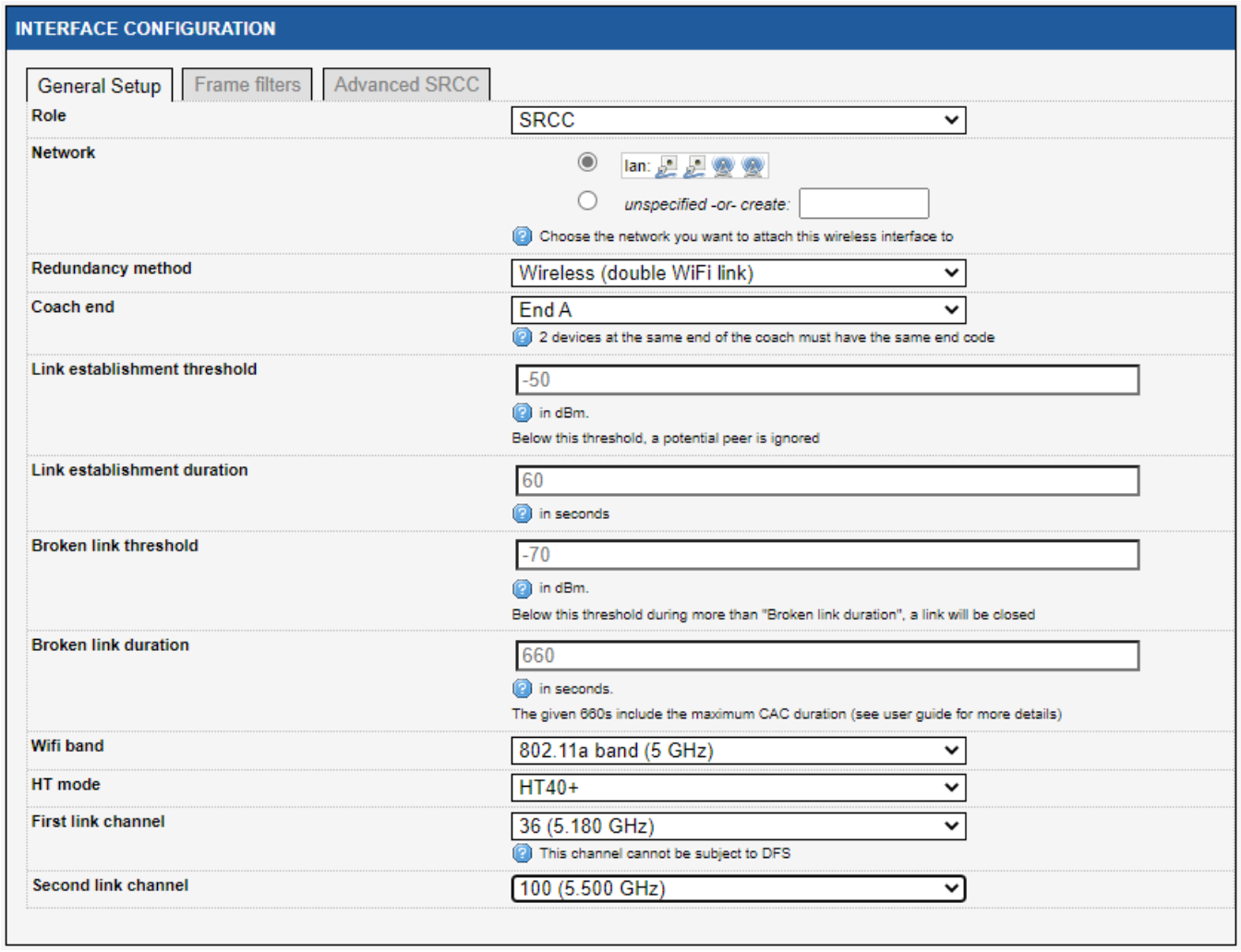
Input filter group/Output filter group:

routing/firewall/bridge 필터 섹션에서, 준비된 필터 중 하나를 선택하세요.
더 많은 정보를 보려면 Bridge filter 섹션을 참고하세요.

SRCC configuration

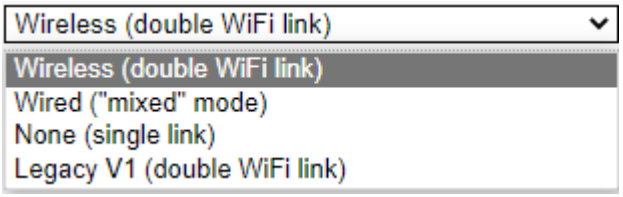
SRCC 가 올바르게 작동하려면, 두 섹션의 (Coach end type 을 제외한) 모든 매개변수가, 기차의 모든 제품에서 동일해야 합니다.

General Setup:



Network: SRCC 가 추가할 무선 네트워크입니다.

Redundancy method: 다음 중 적절한 모드를 선택하세요.



Coach end: 동일한 코치 엣지의 모든 제품은, Coach end type 이 동일해야 합니다. 즉, End A 또는 End B 여야 합니다.

Link establishment threshold & Link establishment duration:
신호 수신 강도가 링크 설정 기간 동안 링크 설정 임계값을 초과하는 경우, 잠재적인 파트너는 유효한 것으로 간주됩니다.

Broken link threshold and Broken link duration:
끊어진 링크 기간 이상 동안, 설정된 링크의 신호가 임계값 아래로 떨어지면, 링크가 끊어진 것으로 간주되고, SRCC 는 무선 감지 프로세스를 재시작합니다.

끊어진 링크 기간에는 DFS CAC 시간이 포함됩니다. 기본값은 660s 로, 600s(날씨 채널을 위한 유럽 CAC 시간)와 60s(깨진 링크 기간 자체)로 이루어져 있습니다. 현재 DFS CAC 시간에 따라 이 값을 줄일 수 있습니다. 일반적인 값은 *III.5.6 Radars detection overview (DFS)* 섹션을 참고하세요. 위의 마지막 4 개 매개변수에 대한 자세한 내용은 *V.9.8 ACKSYS's Smart Redundant Carriage Coupling (SRCC)* 섹션을 참고하세요. 아래 매개변수를 통해 사용자는 최종 무선 링크를 구성할 수 있습니다.

Wi-fi band:

최종 링크의 Wi-Fi 주파수 범위입니다. 5GHz 대역에는 802.11a 를 선택하고, 2.4GHz 대역에는 802.11g 를 선택하세요. 802.11ac Wave 2 제품인 Railbox/66A0 은 SRCC 에 2.4GHz 무선 대역을 사용할 수 없습니다.

HT mode:

애플리케이션 요구 사항에 따라 HT80 ieee80211.ac 모드를 선택하여, 링크 대역폭을 크게 늘릴 수 있습니다.

First link channel:

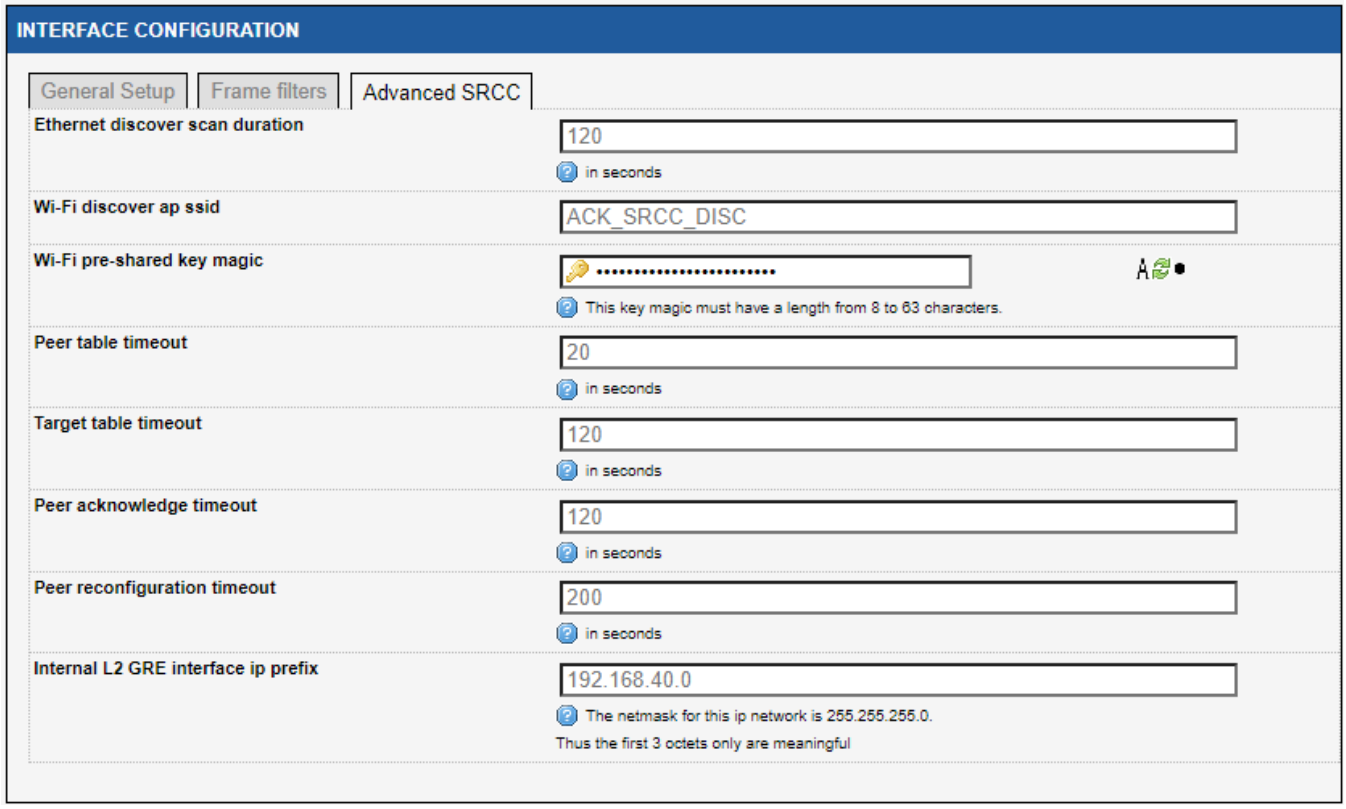
첫 번째 SRCC 최종 링크와 관련된 무선 채널입니다. SRCC 가 무선 검색에 DFS 채널을 사용하기 때문에, DFS 채널은 목록에서 제거되었습니다. 이렇게 하면 검색 프로세스가 DFS 이벤트에 의해 중지되지 않습니다.

Second link channel:

이것은 두 번째 SRCC 최종 링크와 연결된 무선 채널입니다. 제품이 비중복 토폴로지로 구성되어 있더라도 두 채널 모두 필요합니다.

Advanced SRCC parameters:

이러한 설정은 매우 주의해서 변경해야 하기 때문에, 숙련된 사용자가 사용하는 것이 좋습니다.



Ethernet discover scan duration:

이것은 이더넷 토폴로지 검색 스캔의 global 기간입니다. technical reference 섹션에서 설명한 것처럼, 동일한 코치의 모든 SRCC 장치는 동시에 전원을 켜야 합니다. 그렇지 않은 경우, 이 매개변수는 모든 SRCC 장치가 전원을 켜는 동안 서로를 스캔할 수있는 시간을 조정하는 데 도움이됩니다.

Wi-Fi discover ap ssid:

무선 검색 프로세스에서, 다른 잠재적인 파트너를 발견하기 위해 사용되는 SSID 입니다.

Wi-Fi pre-shared key magic:

이 키를 사용하면 사용자가 자신의 키를 정의할 수 있으므로, 각 사용자마다 다른 키를 사용할 수 있습니다.

Peer table timeout:

무선 검색 프로세스 중 잠재적인 파트너의 신호 강도가 올바르게 유지(링크 설정 임계값 이상)되다가 갑자기 사라지면, 이 파트너는 Peer table timeout 기간 이후에 파트너 (peer) 목록에서 삭제됩니다.

Target table timeout:

이것은 peer table timeout 과 동일하지만, 전체 셀(다른 캐리지에 있는 무선 peer 그룹)에 대해 표현됩니다. 자세한 내용은 SRCC 기술 참조를 참조하세요. 셀이 대상 table timeout 보다 유효하지 않으면 목록에서 제거됩니다.

Peer acknowledge timeout:

Master 가 제안한 셀 아키텍처를 보낸 후, 모든 파트너로부터 응답을 기다리는 시간입니다.

Peer reconfiguration timeout:

마스터가, 모든 파트너가 최종 역할로 전환하기를 기다리는 시간입니다.

Internal L2 GRE interface IP prefix:

SRCC 의 내부는 GRE L2 터널을 사용합니다. 이 GRE 인터페이스는 C 클래스 IPV4 주소로 구성됩니다. 이 매개변수는 기본 IP 주소와 사용자의 네트워크 간 충돌이 발생한 경우 IP 를 사용자 정의 할 수있는 방법을 제공합니다.
이 매개변수는 GRE 인터페이스 IP 접두사를 나타냅니다. 마지막 숫자는 무선 파트너의 최종 역할이 AP 인 경우 1 로 대체되고, 클라이언트 최종 역할인 경우 2 로 대체됩니다.

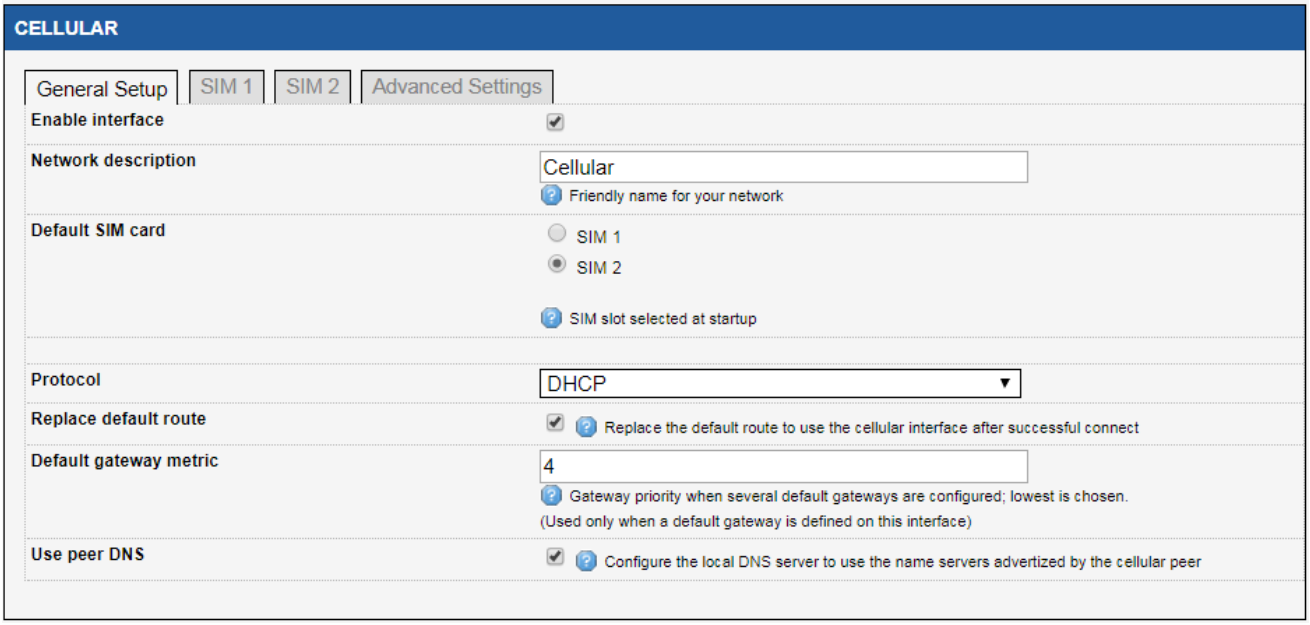
예시:

User prefix: A.B.C.D

Final role	IP
AP	**A.B.C.1**
Client	A.B.C.2

VI.1.1.2 Cellular (on some models)

General Setup:



Enable interface:

셀룰러 인터페이스는 초기 설정에서는 비활성화되어 있습니다. 인터페이스를 사용하려면 이 체크박스를 선택하세요.

Network description:

네트워크에 대한 설명이나 이름을 입력합니다.

Default SIM card:

시작 시 처음 선택되는 SIM 슬롯입니다.

Protocol:

IPv4 에 대해서는 DHCP 만 지원됩니다. 운영자는 DHCP 서버를 통해 IP 주소를 제공해야 합니다.

Replace default route:

체크하면, DHCP 에서 제공하는 기본 게이트웨이는, 연결시 기존 게이트웨이를 덮어씁니다.

Default gateway metric:

DHCP 에서 제공하는 기본 게이트웨이의 우선순위입니다.

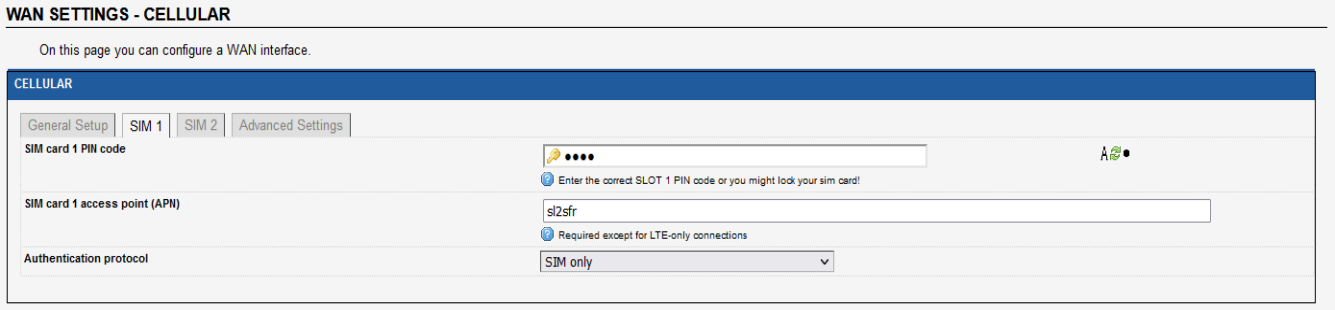
두 개의 기본 경로가 가능한 경우, 'replace default route' 를 사용할 때 셀룰러 경로만 유지됩니다. 'default gateway metric' 을 사용하면 두 경로가 모두 유지되지만, 가장 낮은 메트릭을 가진 경로만 경로만 사용됩니다.

Use peer DNS:

보통 DHCP 에서 가져온 DNS 주소는, 미리 구성된 DNS 에 추가됩니다. 체크를 해제하면 운영자가 제공하는 DNS 대신, 다른 소스(예: LAN 서버)를 사용할 수 있습니다.

SIM 1 / SIM 2:

두 탭은 각각 SIM 슬롯을 구성합니다. 슬롯에 SIM 이 있는지 여부에 관계없이 둘 다 작성 가능합니다.



SIM card PIN code:

PIN 코드입니다. 우측 더블 화살표 아이콘을 클릭하면 암호가 평문으로 표시됩니다.

SIM card 2 access point (APN):

운영자가 제공하는 APN 입니다.

Authentication protocol:

운영자가 제공하는 인증 정보입니다. SIM 은 해당 SIM 에 내장된 인증 토큰을 사용합니다. 다른 방식은 명시적인 사용자 이름/비밀번호가 필요합니다. (하기 내용 참조)

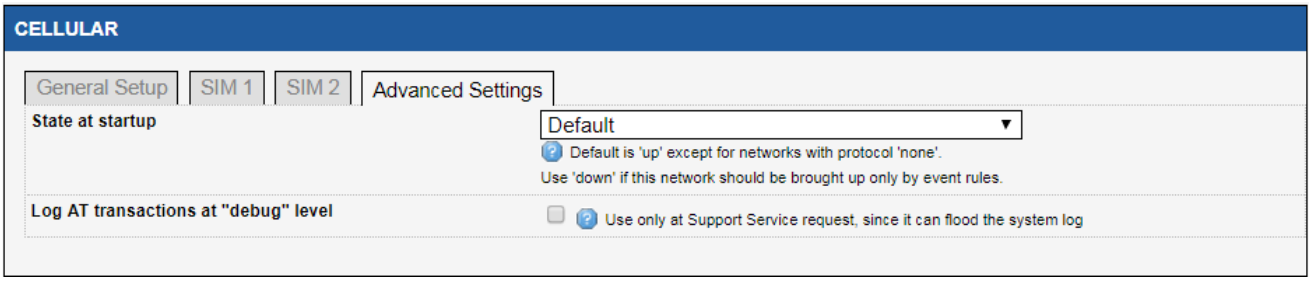
PAP/CHAP user name (only in PAP, CHAP or PAP/CHAP mode):

모바일 장비를 인증하는 사용자 이름입니다.

Password (only in PAP, CHAP or PAP/CHAP mode):

사용자 이름과 관련된 비밀번호입니다. 더블 화살표 아이콘을 클릭하면 암호가 평문으로 표시됩니다.

Cellular Advanced Settings:



State at startup:

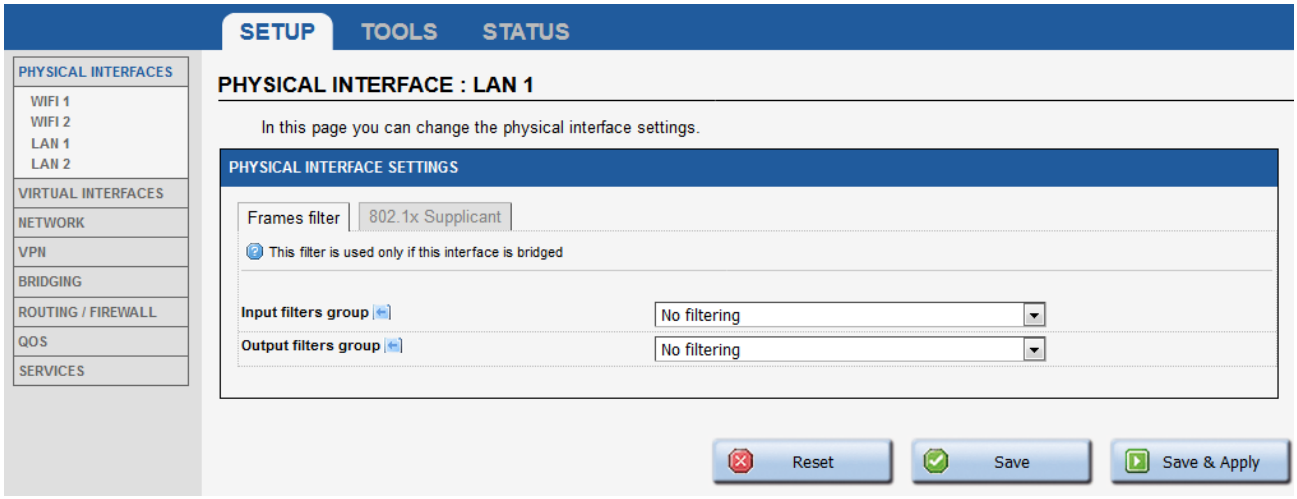
'down' 을 선택하면 셀룰러는 부팅 후 운영자에게 연결을 시도하지 않으며, 시작하려면 이벤트/알람 서비스의 특정 작업이 필요합니다.

Log AT transactions at “debug” level:

WaveOS 와 셀룰러 카드 간의 자세한 구성 및 상태 트랜잭션을 로그에 기록합니다. 지원 서비스 요청 시에만 사용하세요.

VI.1.1.3 Physical Interface: LAN

Frames filter



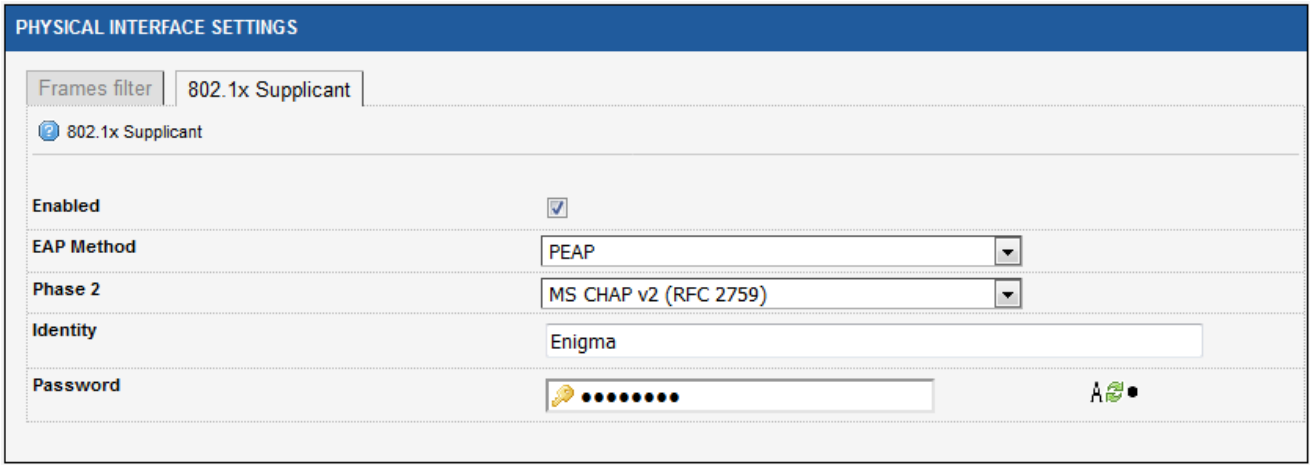
이 페이지에서는 이더넷 인터페이스에 입력/출력 필터를 적용할 수 있습니다.

Input/Output filters group:

routing/firewall/bridge 필터 섹션에서, 준비된 필터 중 하나를 선택합니다. 필터 그룹에 대한 더 자세한 정보를 보려면, Bridge filter 섹션을 참고하세요.

802.1x Supplicant

이 탭에서는 이더넷 포트에서 801.1x 인증을 활성화할 수 있습니다. 현재까지는 서플리컨트 모드만 지원됩니다.



EAP-Method:

사용할 EAP 방법(PEAP 또는 TLS)을 선택합니다.

Phase 2:

이 필드에는 인증 방법이 포함됩니다. MSCHAPV2 만 사용할 수 있습니다.

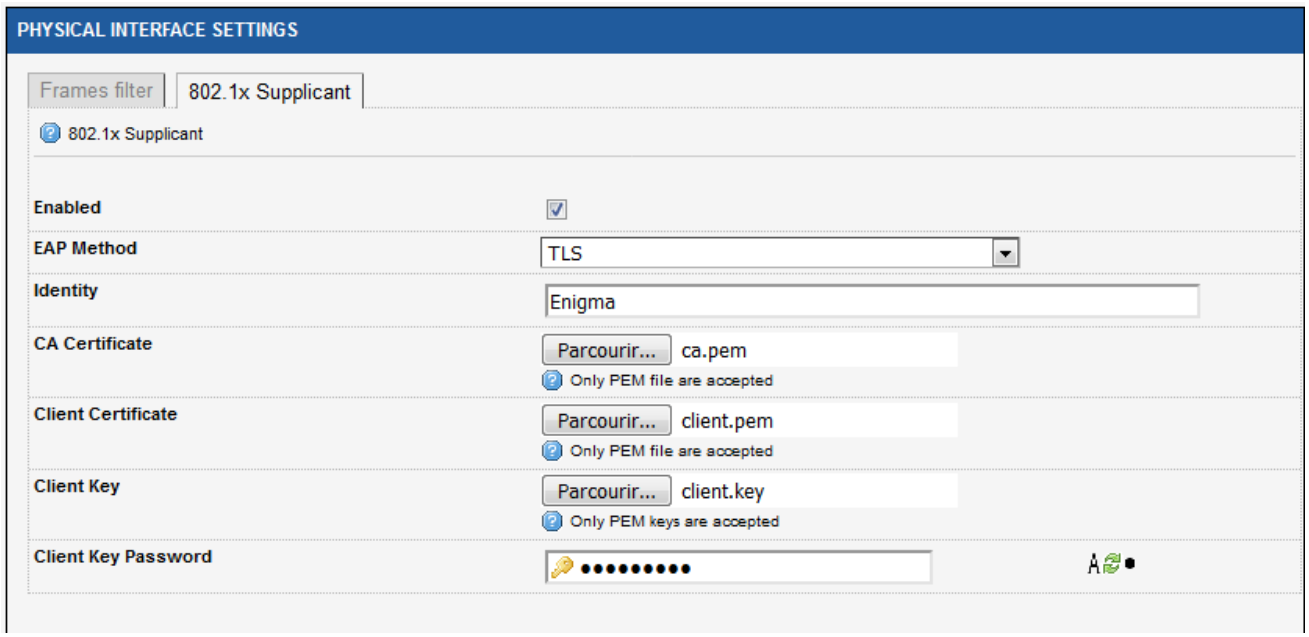
Identity:

인증에 사용되는 ID 입니다.

Password:

사용자 ID 와 연관된 암호입니다.

EAP-Method TLS:



Identity:

이 필드는 EAP-TLS 인증 중 사용할 로그인 정보를 제공합니다.

CA-Certificate:

업로드할 CA 인증서 파일의 위치를 선택합니다. 인증서와 키는 PEM 형식으로 제공되어야 합니다. (하기 내용 참조)

Client certificate:

업로드할 클라이언트 인증서 파일의 위치를 선택합니다. PEM 형식으로 제공되어야 합니다.

Client Key:

업로드할 키 파일의 위치를 선택합니다. PEM 개인 키만 허용됩니다.

Client Key password:

클라이언트 키와 관련된 비밀번호를 기입합니다.

참고: PEM 형식은 OpenSSL 프로젝트에서 정의된 것입니다. 첫 줄이 "-----BEGIN"으로 시작하고 이진 데이터가 base64 방식으로 인코딩된 이진 데이터로, 식별 가능한 텍스트 파일입니다.

VI.1.2 Virtual interfaces

이 섹션에서는 가상 인터페이스를 관리할 수 있습니다. 가상 인터페이스는 물리적 인터페이스에 연결됩니다. 하나의 물리적 인터페이스에 여러 가상 인터페이스를 추가할 수 있습니다. 802.1q 태깅의 경우, 가상 인터페이스는 송신 트래픽에 802.1q 태그를 추가하고, 수신 트래픽에서 태그를 제거합니다.

VI.1.2.1 802.1q Tagging

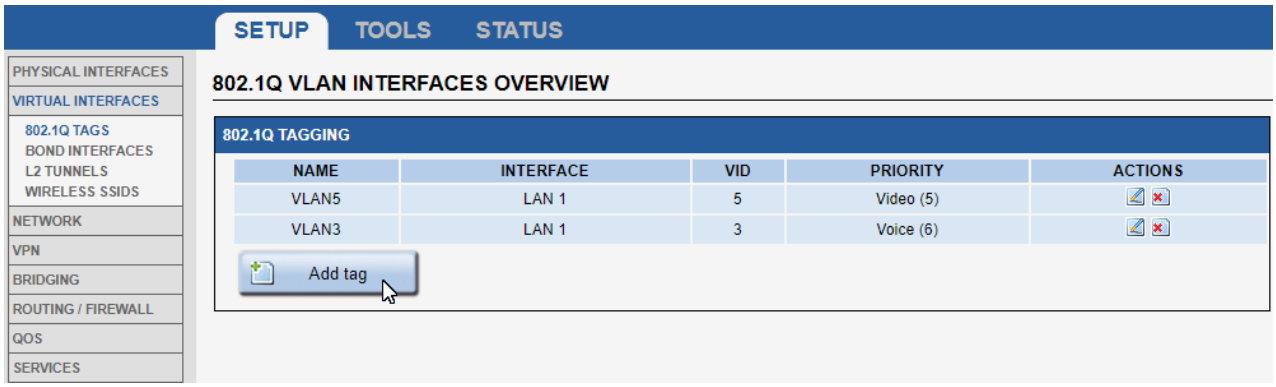
802.1q 태그는, 장치 그룹과 관련된 트래픽을 격리하기 위해, 공통 물리적 링크를 여러 가상 LAN(VLAN)으로 분할하는 데 사용됩니다. 각 그룹은 각각의 다른 VLAN ID 를 부여받으며, 이는 그룹 내에서 교환되는 데이터 프레임을 표시하는 데 사용됩니다. 그런 다음 VLAN 태그를 사용하도록 구성된 장치만 그룹 내의 다른 장치와 통신할 수 있습니다.

제품 내 물리적 LAN 인터페이스에서는, 독립적인 물리적 LAN 인터페이스와 마찬가지로, 사용되는 가상 인터페이스를 정의할 수 있습니다.

가상 인터페이스를 생성한 후 이를 사용하려면, 네트워크에 추가해야 합니다.

VLAN Interfaces overview:

이 페이지에는 생성된 실제 가상 인터페이스 목록이 표시됩니다..

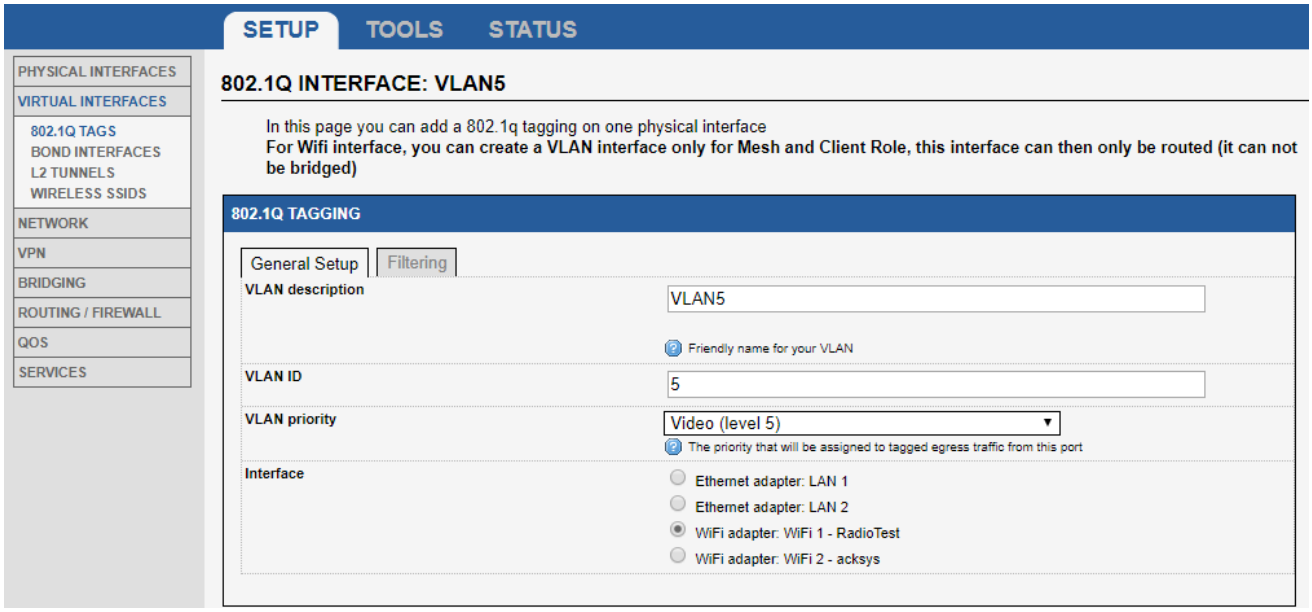


Remove 버튼을 클릭하여 가상 인터페이스를 제거합니다.

Edit 버튼을 클릭하여 가상 인터페이스 설정을 수정합니다.

Add tag 버튼을 클릭하여 새 가상 인터페이스를 생성합니다.

VLAN configuration:



VLAN description

VLAN 에 대한 설명이나 이름을 기입합니다. (선택 사항)

VLAN ID

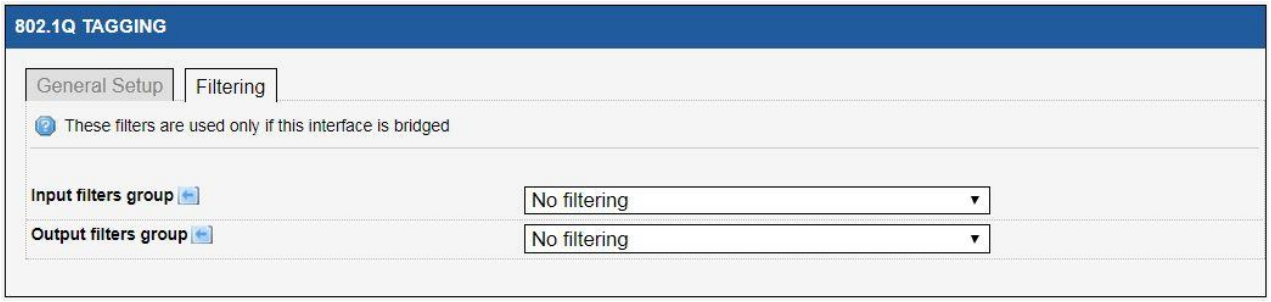
가상 인터페이스의 ID 를 입력하세요. 동일한 물리 인터페이스 위에 여러 VLAN ID 를 생성해야하는 경우, 공백 문자(스페이스바)를 사용하여 ID 를 구분할 수 있습니다. (예 : 5 10 120)

VLAN priority

이 포트에서, 태그가 지정된 출력 트래픽에 할당될 우선 순위를 선택합니다.

Interface

가상 인터페이스를 생성할 물리 인터페이스를 선택하세요. Wi-Fi 인터페이스의 경우, Mesh 및 Client 역할에 대해서만 VLAN 인터페이스를 생성할 수 있습니다. 이 인터페이스는 라우팅 될 수는 있지만, 다른 인터페이스와 브리지될 수는 없습니다.

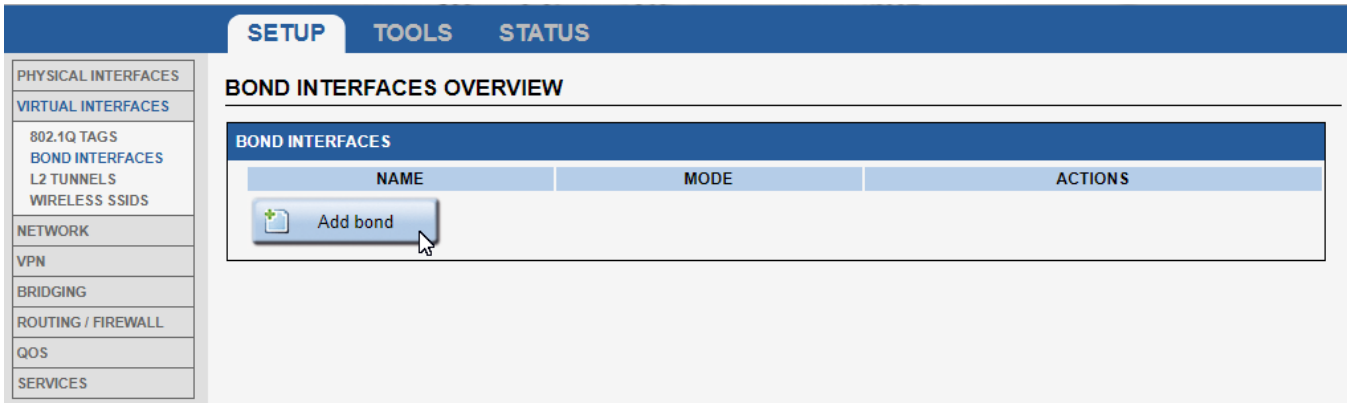


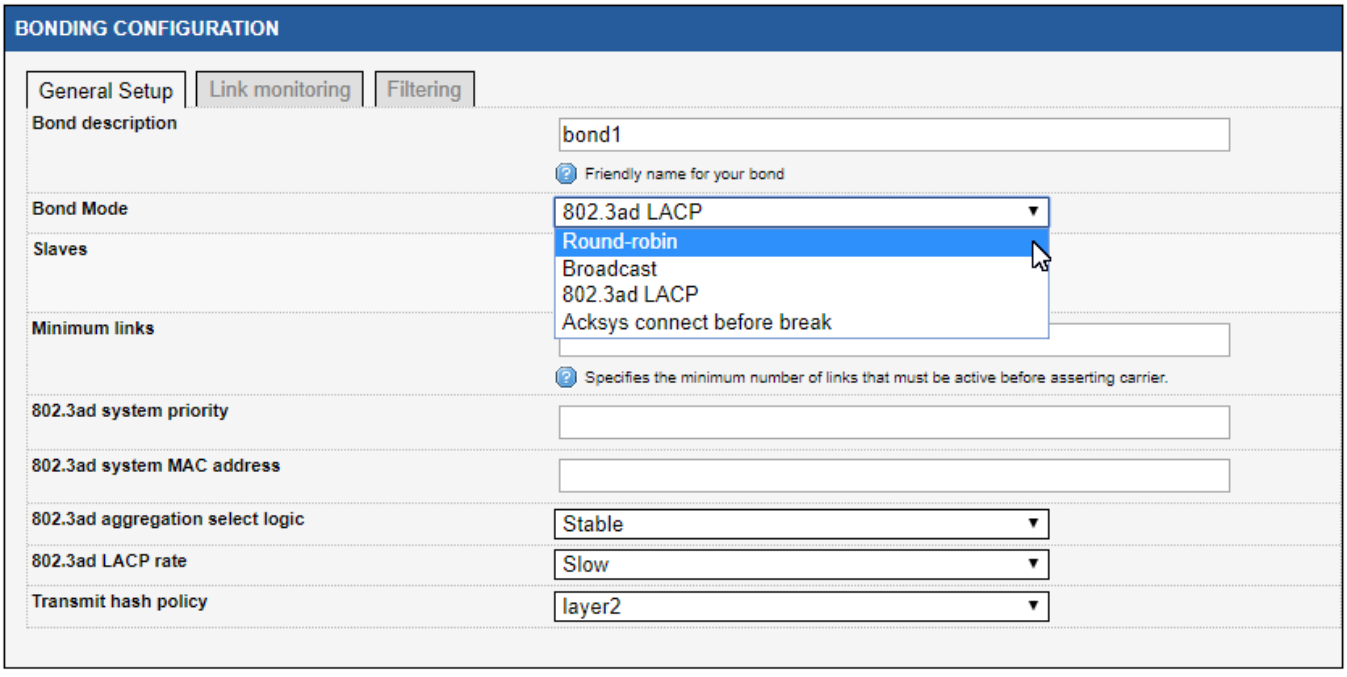
Input filter group/Output filter group:

라우팅/방화벽/브리지 필터 섹션에서, 준비된 필터 중 하나를 선택합니다. 더 많은 정보를 보려면, Bridge filter 섹션을 참고하세요.

VI.1.2.2 BOND INTERFACES

본딩을 사용하면, 여러 네트워크 카드를 통합하여 대역폭을 늘릴 수 있어 가용성이 높아집니다. CBB(Connect Before Break) 모드를 사용할 때에도 본딩 인터페이스가 자동으로 생성됩니다. **Add bond** 를 클릭하여 새로운 본딩 인터페이스를 추가할 수 있습니다.





Bond description:

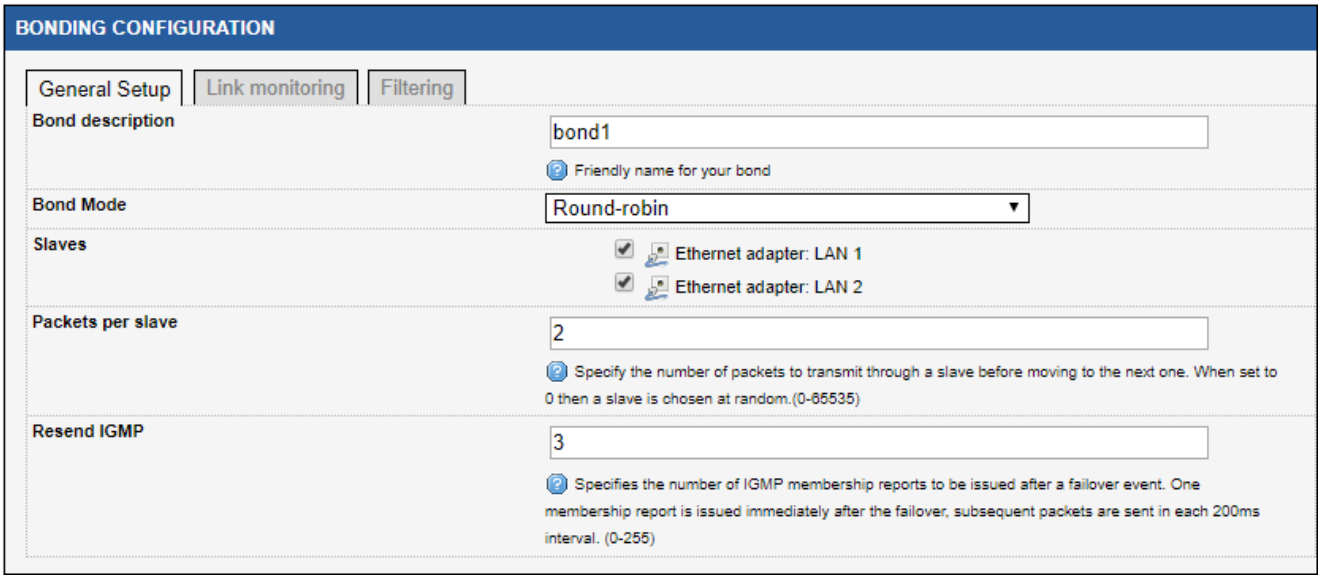
본딩 인터페이스에 대한 설명이나 이름을 기입합니다.

Bond Mode:

필요한 본딩 모드를 선택하세요. Round Robin, Broadcast, 803.3ad LACP, Connect before break 모드가 있습니다. 이러한 모드에 대한 설명은 다음 페이지에서 제공됩니다.

Round-Robin Mode

Round-Robin 모드는 로드 밸런싱에 사용됩니다. 패킷 전송은, 집합체 내에서 활성화된 각 카드에서 순차적으로 수행됩니다. 이 모드는 대역폭을 늘리고, 오류 허용성을 관리합니다.



Slaves:

두 개의 이더넷 인터페이스(LAN 1,LAN 2)를 선택해야 합니다.

Packets per slave:

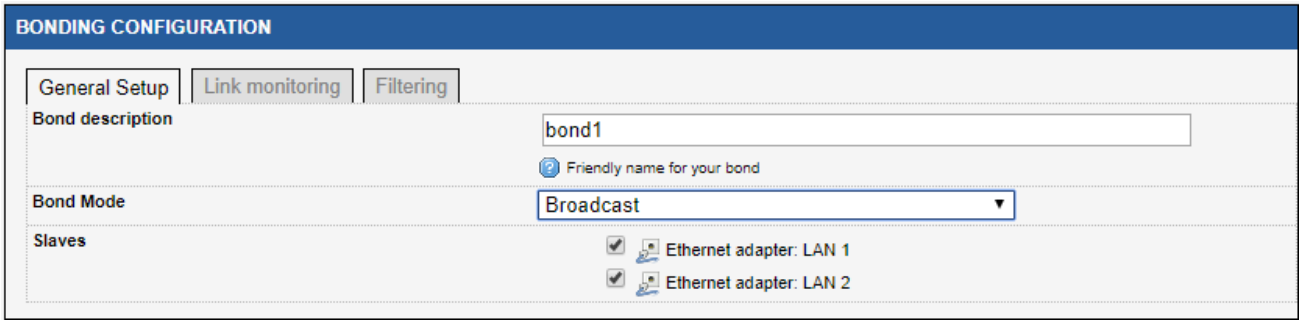
네트워크 카드에서, 다음으로 이동하기 전에 보내는 패킷 수를 지정합니다. 값은 1 에서 65535 까지 다양할 수 있습니다. 기본값은 1 입니다. 0 을 입력하면 값이 무작위로 선택됩니다.

Resend IGMP:

장애 조치 이벤트 후 발행되는 IGMP 멤버십 보고서의 수를 지정합니다. 장애 조치 후 즉시 하나의 멤버십 보고서가 발행되며, 이후 패킷은 각 200ms 간격으로 전송됩니다. (0-255)

Broadcast Mode

이 방법은, 모든 슬레이브 인터페이스에 모든 것을 전송하는 브로드캐스트 정책에 기반을 두고 있습니다. 이는 오류 허용성을 제공합니다. 이는 특정 용도로만 사용할 수 있습니다.

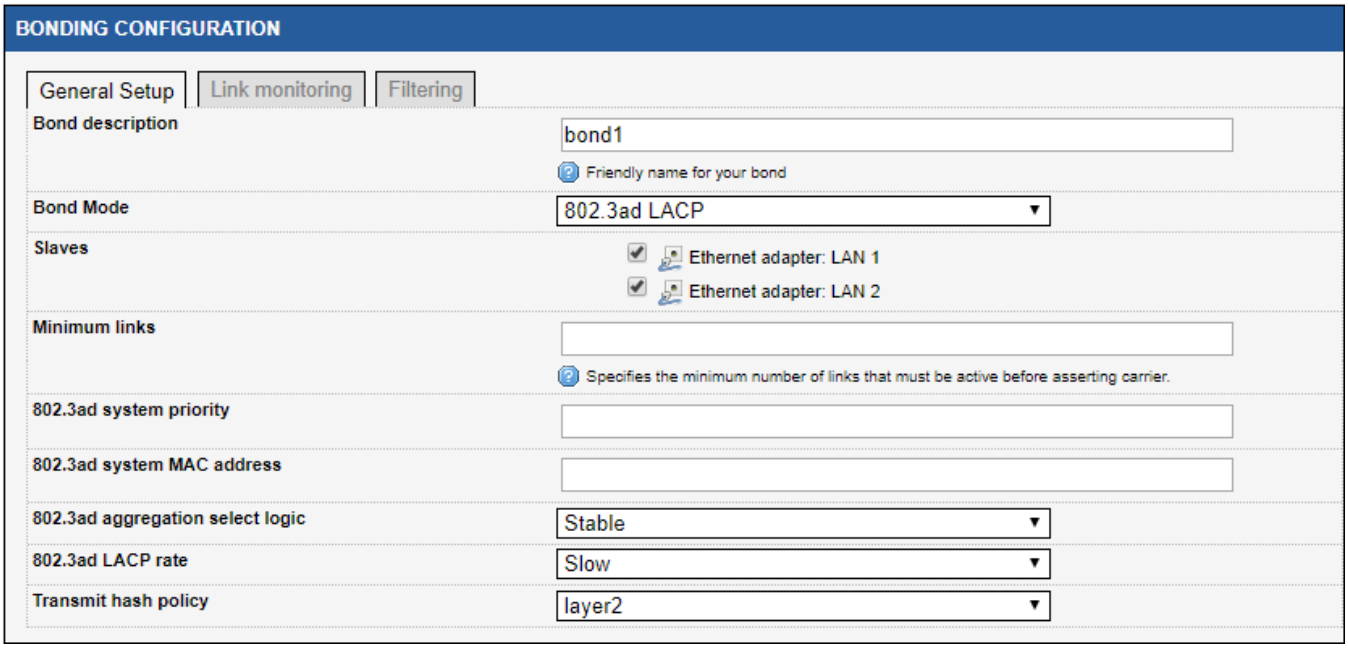


Slaves:

두 개의 이더넷 인터페이스(LAN 1,LAN 2)를 선택해야 합니다.

802.3ad LACP

이 모드는 동적 링크 집합 모드로 알려져 있으며, 동일한 속도를 가진 집합체를 생성합니다. IEEE 802.3ad 동적 링크를 지원하는 스위치가 필요합니다. 대상에 대한 슬레이브 선택은, 전송 해시 함수에 기반합니다.



Minimum links:

장착할 본딩 인터페이스 캐리어에 대해, 활성화되어야 하는 물리적 링크의 최소 수를 지정합니다. 기본값은 1 이며, 1 로 유지되어야 합니다.

802.3ad system priority:

802.3ad 스위치에서, 관리할 링크의 우선 순위를 설정할 수 있습니다. 가장 높은 우선 순위는 1 이고, 가장 낮은 우선 순위는 65535 입니다. 기본값은 65535 입니다.

802.3ad system MAC address:

기본적으로 본딩 인터페이스의 가상 MAC 주소가 사용됩니다. 이 필드를 사용하여 다른 값을 정의할 수 있습니다.

802.3ad aggregation select logic:

802.3ad aggregation 로직을 지정합니다. 가능한 값과 그 효과는 다음과 같습니다.

Stable 가장 큰 집계 대역폭에 따라, 활성 집합체가 선택됩니다. 활성 집합체의 모든 슬레이브가 다운되거나, 활성 집합체가 슬레이브를 가지고 있지 않을 때에만, 활성 집합체 재선택이 발생합니다.

Bandwidth 가장 큰 집계 대역폭에 따라, 활성 집합체가 선택됩니다. 하기 상황일 때 재선택이 발생됩니다.

- 활성 집합체에 슬레이브가 추가/제거될 때
- 모든 슬레이브의 링크 상태 변경
- 슬레이브의 링크 상태/802.3ad 연관 상태가 변경될 때
- 본딩의 관리 상태가 'up'으로 변경될 때

Count 가장 많은 수의 포트(슬레이브)에 의해 선택됩니다. 재선택은 위의 'bandwidth' 설정에서 설명한 대로 발생합니다.

대역폭 및 포트 수 선택 정책은, 802.3ad 집계가 일부 실패할 경우, 장애조치(failover)를 허용합니다. 이렇게 하면 항상 가용성이 가장 높은 집계자(대역폭 또는 포트 수 중 높은 값)가 활성 상태를 유지합니다.

802.3ad LACP rate:

802.3ad 모드에서, 링크 파트너에게 LACPDU 패킷을 전송할 속도를 지정하는 옵션입니다. 가능한 값은 다음과 같습니다.

- **Slow :** 링크 파트너에게 LACPDUs 를 30 초마다 전송하도록 요청합니다.
- **Fast :** 링크 파트너에게 LACPDUs 를 1 초마다 전송하도록 요청합니다.

Transmit hash policy:

이 매개변수를 사용하면, 각 교환 유형에 대해 포트를 선택할 때 사용할 전략을 정의할 수 있습니다.

Layer2 데이터 흐름이 다른 소스 MAC 주소 또는 다른 대상 MAC 주소의 패킷으로 구성된 경우 모든 본딩 포트가 사용됩니다.

Layer2+3 데이터 흐름이 다른 소스 MAC 주소 또는 다른 대상 MAC 주소, 다른 소스 IP 주소 또는 다른 대상 IP 주소의 패킷으로 구성된 경우 모든 본딩 포트가 사용됩니다.

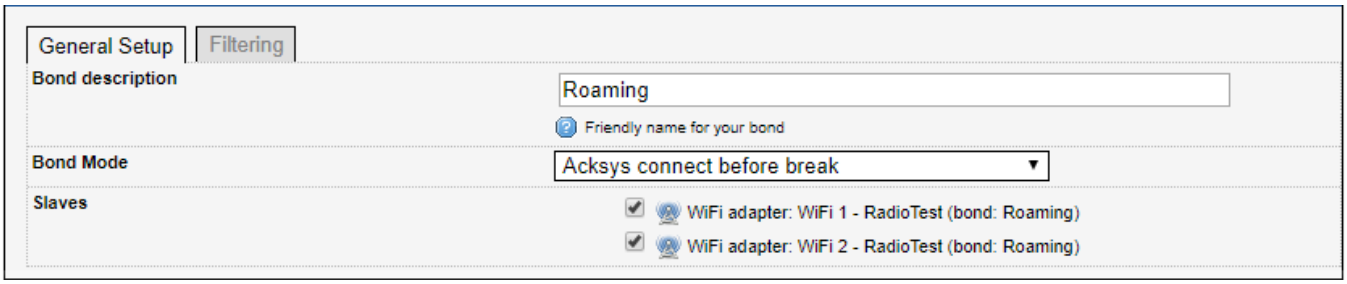
Layer3+4 데이터 흐름이 다른 MAC 소스 주소 또는 다른 MAC 주소 대상, 다른 소스 IP 주소 또는 다른 대상 IP 주소, 다른 소스 포트 또는 다른 대상 포트의 패킷으로 구성된 경우 모든 본딩 포트가 사용됩니다.

Encap2+3 Layer 2+3 과 동일하지만 패킷이 터널 프로토콜(예: GRE)로 캡슐화되어 있음을 감지하면, 터널에서 데이터를 추출하여 처리합니다.

Encap3+4 Layer 3+4 와 동일하지만 패킷이 터널 프로토콜(예: GRE)로 캡슐화되어 있음을 감지하면, 터널에서 데이터를 추출하여 처리합니다.

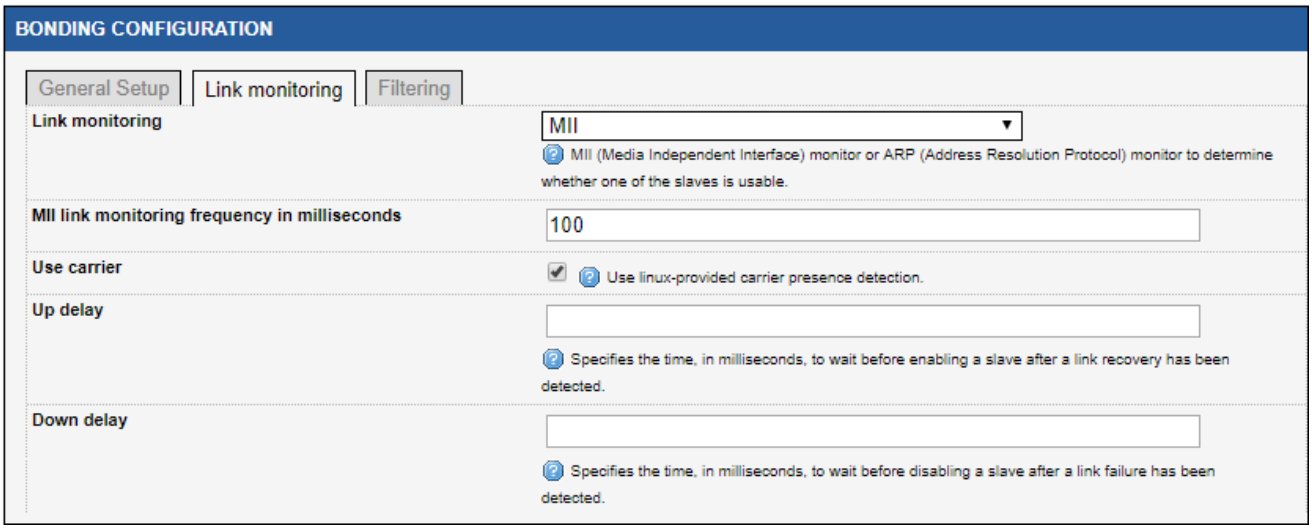
Connect before break

중단 전 연결을 위한 bond 는, 일반적으로 설정/물리적 인터페이스 페이지를 통해 생성됩니다. Global parameters/Cluster 모드를 참고하세요.



Link monitoring using MII

링크 모니터링 탭은, 본딩 인터페이스의 슬레이브 포트 링크를 모니터링하기 위한 매개변수를 정의하는 데 사용됩니다. MII 옵션을 선택하면, 인터페이스의 물리적 링크가 테스트됩니다.



MII link monitoring frequency in milliseconds:

각 포트의 물리적 링크가 테스트되는 빈도를 정의합니다. 기본값은 100ms 입니다.

Up delay:

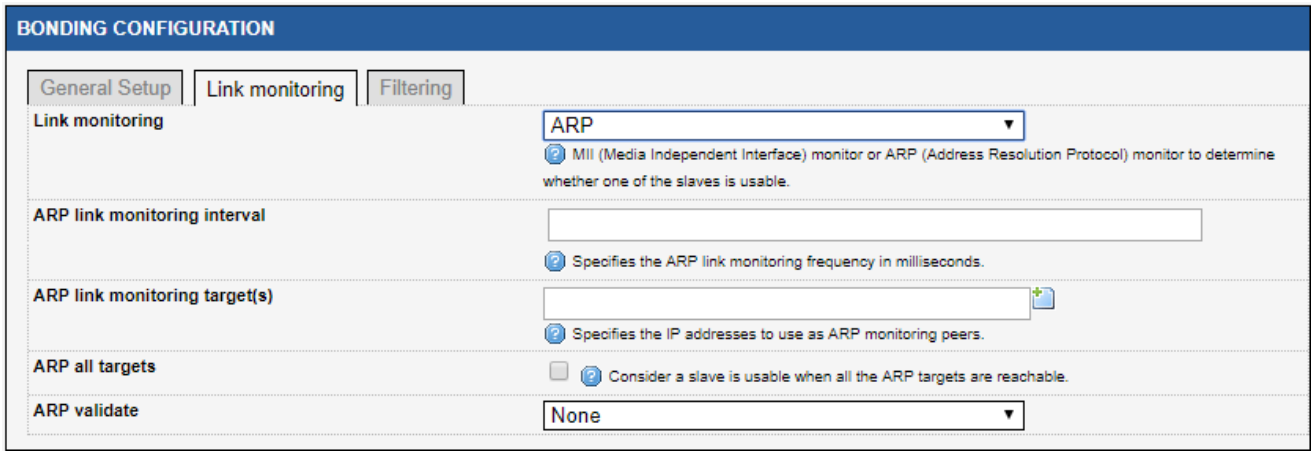
물리적 링크 복구 감지 후, 슬레이브 포트를 활성화하기 전에 대기할 시간(밀리초)을 지정합니다.

Down delay:

물리적 링크 장애 감지 후, 슬레이브 포트를 비활성화하기 전에 대기하는 시간(밀리초)을 지정합니다.

Link monitoring using ARP (only in Round Robbin or Broadcast mode)

이 경우, 링크의 연속성 제어는, ARP 트래픽을 기반으로 합니다.



ARP link monitoring interval:

ARP 요청이 전송되는 시간 간격을, 밀리초 단위로 지정합니다.

ARP link monitoring target(s):

여기에서, 링크를 모니터링하기 위해, ARP 요청을 보내야 하는 IP 주소를 정의합니다.

ARP all targets:

이 체크박스를 선택한 경우, 모든 지정된 IP 주소가 ARP 요청에 응답해야만, 사용 가능한 슬레이브로 간주됩니다.

ARP validate:

이곳에서는 인터페이스가 사용 가능한지 결정하는 기준을 정의합니다. MAC 주소를 보내는 슬레이브 인터페이스는 ***active interface*** 로, 다른 슬레이브는 ***backup interfaces*** 로 부릅니다. 다음은 다른 옵션들입니다.

None: (기본값): 인터페이스에서 최근 들어오고 나가는 ARP 트래픽이 있는지 확인하여, 사용 가능한지 확인합니다.

Active: 인터페이스에서 최근에 들어오고 나가는 ARP 트래픽이 있는지 확인하고, 액티브 인터페이스의 경우 들어오고 나가는 ARP 의 내용도 검사합니다.

Backup: 인터페이스에서 최근에 들어오고 나가는 ARP 트래픽이 있는지 확인하고, 백업 인터페이스의 경우 들어오고 나가는 ARP 의 내용도 검사합니다.

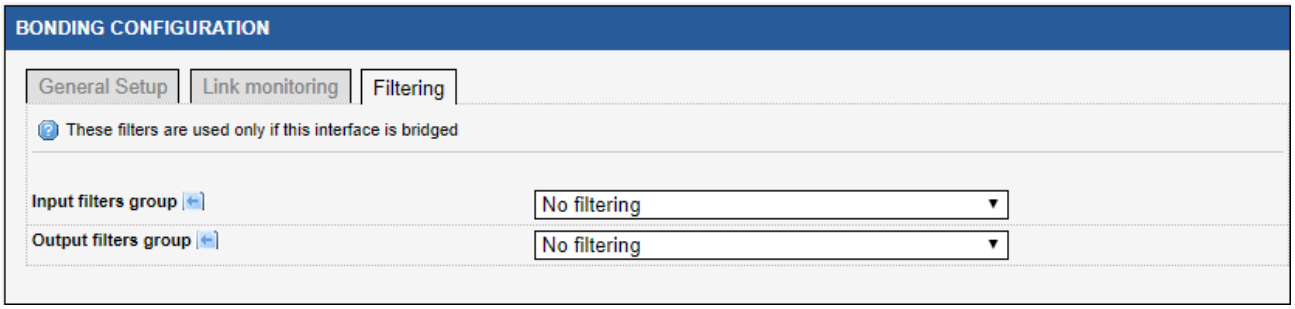
All: 모든 본딩 인터페이스의 ARP 를 모두 조사하여, 사용 가능한지 확인합니다.

Filter: 인터페이스에 최근 들어오는 ARP 트래픽이 있는지 확인하여, 사용 가능한지 확인합니다.

Filter active: 인터페이스에 최근 들어오는 ARP 트래픽이 있는지 확인하고, 액티브 인터페이스의 경우 들어오고 나가는 ARP 의 내용도 검사합니다.

Filter backup: 인터페이스에 최근 들어오는 ARP 트래픽이 있는지 확인하고, 백업 인터페이스의 경우 들어오고 나가는 ARP 의 내용도 검사합니다.

Filtering tab



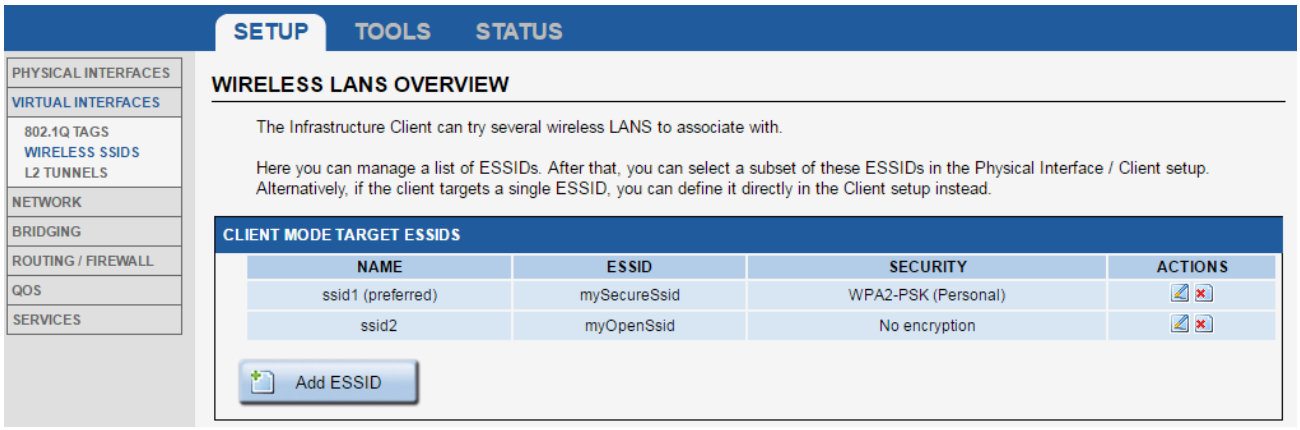
Input filter group/Output filter group:

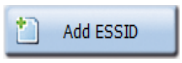
routing/firewall/bridge 필터 섹션에 준비된 필터 중 하나를 선택합니다. 더 많은 정보를 보려면 Bridge filter 섹션을 참고하세요.

VI.1.2.3 Wireless SSIDs

무선 SSID 섹션은, 여러 SSID 를 구성하고 무선 인터페이스의 클라이언트 역할에서 이를 활성화하는데 사용됩니다.

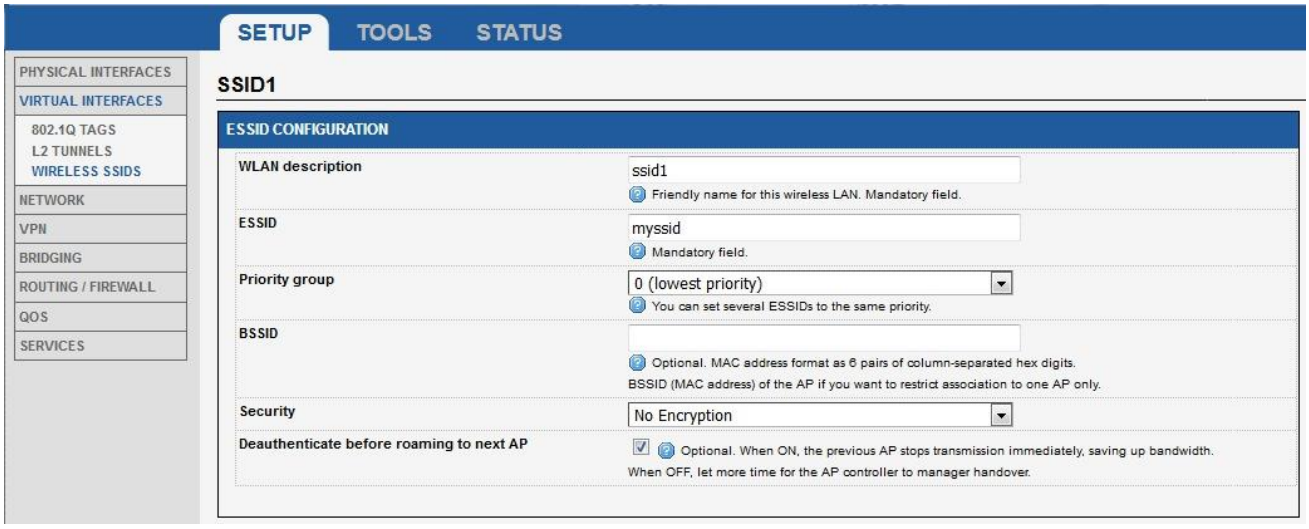
Wireless SSID overview





버튼을 사용하여 SSID 사양을 추가합니다.  버튼을 사용하여 매개변수를 편집합니다.  버튼을 사용하여 SSID 사양을 삭제합니다.

Wireless SSID configuration



WLAN description (optional):

SSID 에 대한 설명이나 이름을 기입합니다. (선택사항)

ESSID:

네트워크 이름 (필수사항/SSID 로도 불림)

Priority group:

스캔 프로세스는, 우선 순위가 가장 높은 SSID 를 가진 AP 를 선택합니다. 동일한 우선 순위의 SSID 를 갖는 AP 가 여러 개 있는 경우, 신호가 가장 좋은 AP 가 선택됩니다.

BSSID (optional):

하나의 AP 로만 연결을 제한하려면, AP 의 BSSID(MAC 주소 형식)를 설정합니다.

Security:

보안 정책을 선택합니다. 더 자세한 내용은 *Wireless Security tab* 섹션을 참고하세요.

VI.1.2.4 L2 Tunnels

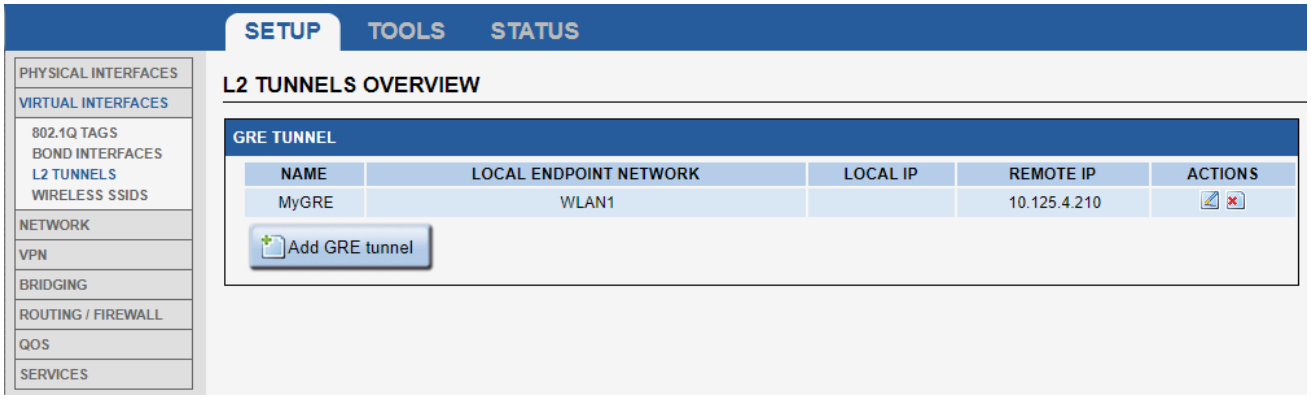
이 섹션에서는 GRE(Generic Routing Encapsulation: 일반 라우팅 캡슐화)를 사용한 Layer 2 터널링을 구성할 수 있습니다. GRE 캡슐화는 원본 L2 프레임에, L2, L3 및 GRE 헤더를 추가합니다. 이 오버헤드는 네트워크 MTU (Maximum Transmit Unit: 최대전송단위)를 줄일 수 있습니다. (802.3 네트워크에서 L2 프레임은 1524 옥텟으로 제한됩니다.)

참고: 참고: 802.11 네트워크는 802.3 네트워크보다 더 큰 프레임을 지원합니다. GRE 터널이 802.11 네트워크만 통과하는 경우, 원래 L2 프레임에 대해 최대 802.3 MTU 를 사용할 수 있도록, GRE 인터페이스 및 802.11 물리적 인터페이스가 포함된 네트워크의 MTU 를 늘리는 것이 좋습니다.

예를 들어 GRE 및 WiFi 인터페이스 MTU 를 2000 으로 설정하면, 최대 802.3 MTU 까지 프레임 크기를 캡슐화하기에 충분합니다.

L2 TUNNELS Overview

이 페이지에서 GRE 터널을 생성할 수 있습니다:



버튼을 사용하여 GRE 인터페이스를 추가하세요.

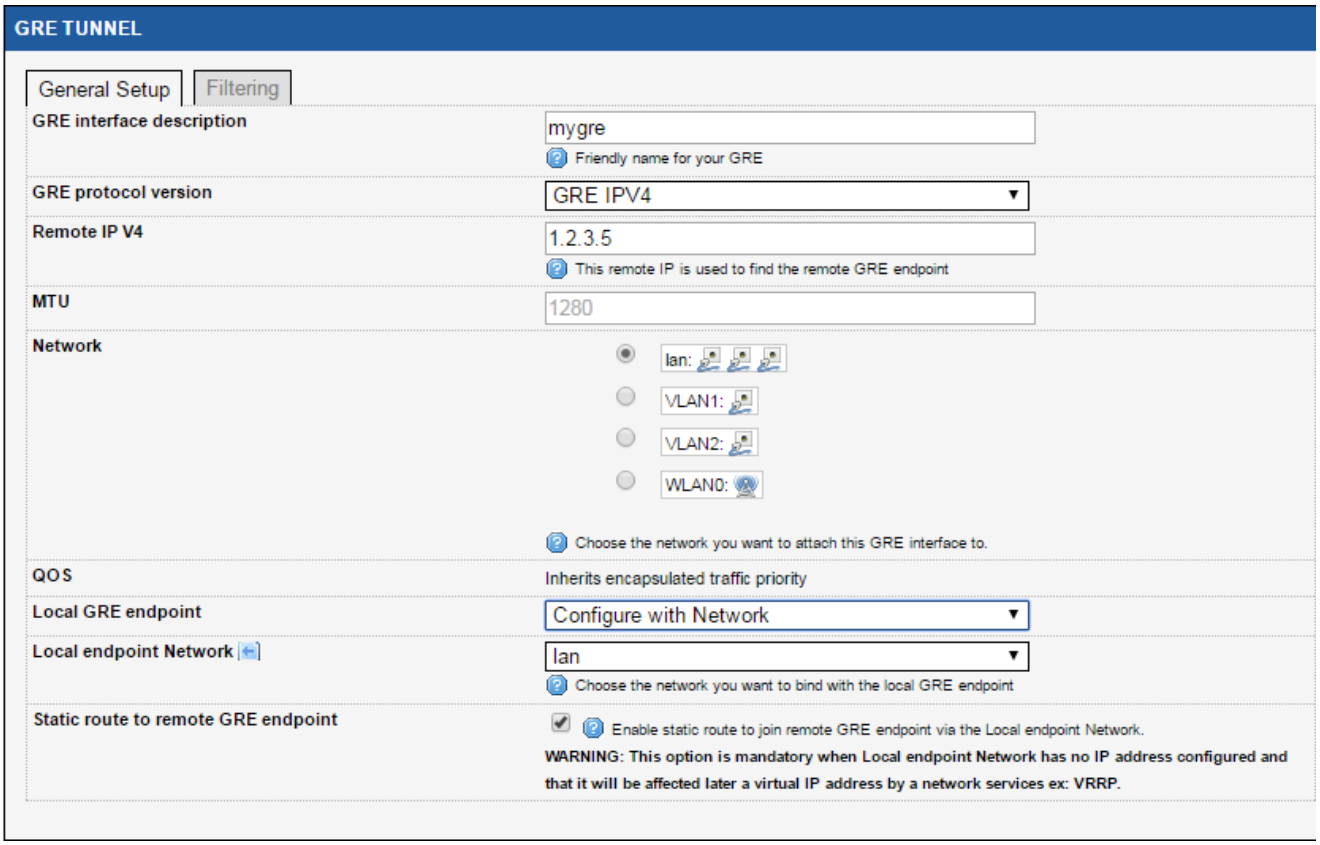

버튼을 사용하여 GRE 터널 매개변수를 편집하세요.


버튼을 사용하여 GRE 터널을 삭제하세요.

GRE TUNNEL configuration page

이 페이지에서는 GRE 터널을 구성할 수 있습니다.

General Setup tab



GRE interface description

GRE 인터페이스에 대한 설명이나 이름을 기입합니다.

GRE protocol version

항상 GRE IPV4 를 사용합니다.

GRE Remote IPV4

터널 원격 종단점의 IP 를 입력합니다.

MTU (Maximum transmit unit)

GRE 터널에서 캡슐화된 L2 프레임의 최대 크기를 설정합니다.

Network

선택한 네트워크에 GRE 터널 인터페이스를 추가합니다.

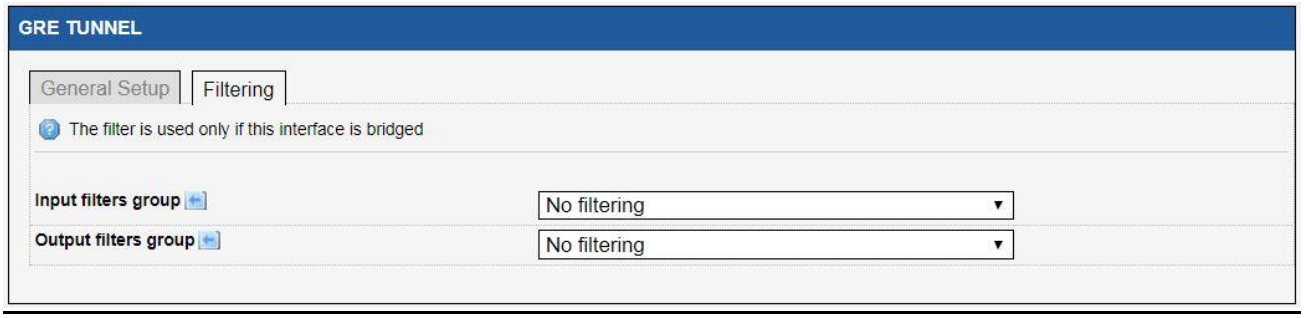
.

Local GRE endpoint

하기 내용 중에서 선택하세요.

- **Configure with IPV4 address:**
  - **Local IP V4:** 이 로컬 IP 를 이용하여, 로컬 GRE 종단점을 찾습니다. 만약 이 IP 가 GRE 인터페이스를 생성할 때 유효하지 않은 경우, 터널은 기본 게이트웨이를 통해 라우팅됩니다. 이러한 경우, 무선 인터페이스나 GRE 터널 이후에 생성된 가상 인터페이스와 같은 인터페이스에 해당하는 IP 를 사용하지 않고, 아래 섹션에서 설명하는 대로, 주어진 인터페이스와 IP 가 포함된 네트워크에 로컬 종단점을 바인딩 하는 것이 좋습니다.
- **Configure with Network:**
  - **Local endpoint Network:** 로컬 GRE 종단점과 바인딩 할 네트워크를 선택합니다.
  - **Static route to remote GRE endpoint:** 로컬 종단점 네트워크를 통해, 원격 GRE 종단점에 대한 고정 경로를 연결할 수 있습니다. 단, 로컬 종단점 네트워크에 IP 주소가 구성되어 있지 않은 경우나, 이후에 네트워크 서비스(ex.VRRP)에 의해 가상 IP 주소가 할당될 경우, 이 옵션은 필수로 활성화해야 합니다.

Filtering tab

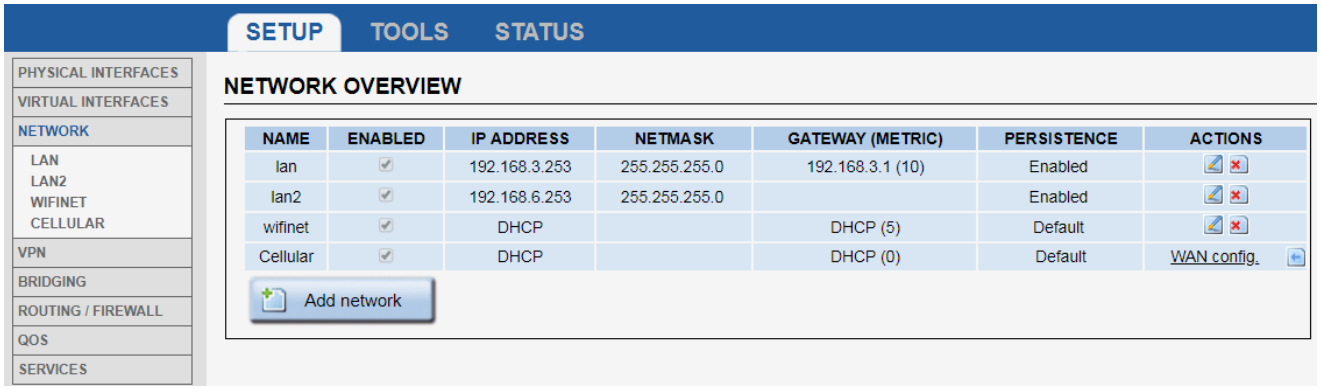


Input filter group/Output filter group:

routing/firewall/bridge 필터 섹션에 준비된 필터 중 하나를 선택합니다. 더 많은 정보를 보려면 Bridge filter 섹션을 참고하세요.

VI.1.3 Network

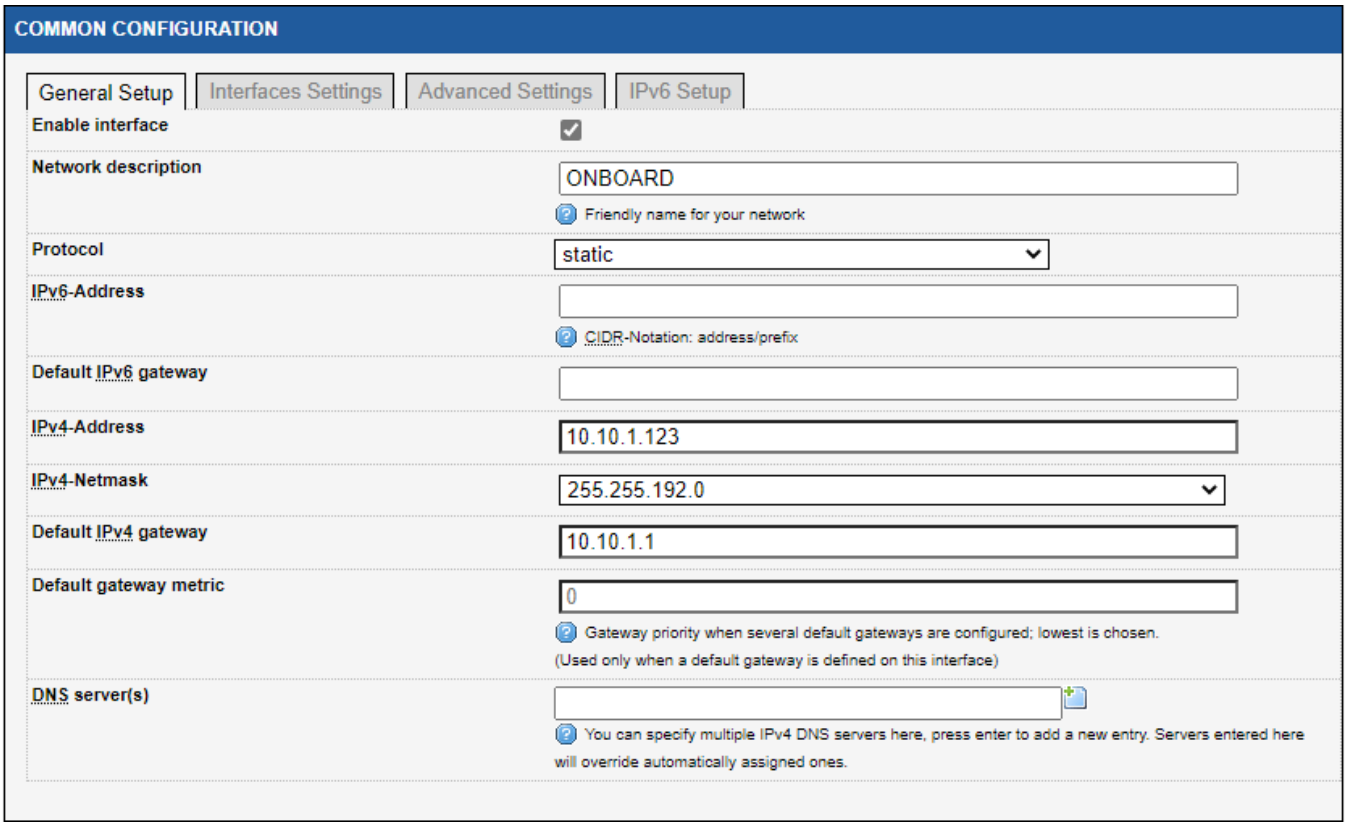
이 페이지는 현재 네트워크 구성을 표시합니다.



Remove 버튼을 클릭하여 네트워크를 제거합니다.
Edit 버튼을 클릭하여 네트워크 설정을 편집합니다.
Add network 버튼을 클릭하여 네트워크를 새로 추가합니다.

VI.1.3.1 Network configuration

General setup:



Enable interface

이 체크박스를 선택하면, LAN 인터페이스를 일시적으로 비활성화할 수 있습니다. 이때 구성은 유지됩니다.

Network description

네트워크에 대한 설명이나 이름을 기입합니다.

Protocol

네트워크에 DHCP 서버가 있고, 장치에 IP 주소를 할당하려는 경우 'DHCP'를 선택하세요. 이 경우 DNS 서버를 제외하고, 위에 표시된 필드를 채우지 않아도 됩니다.

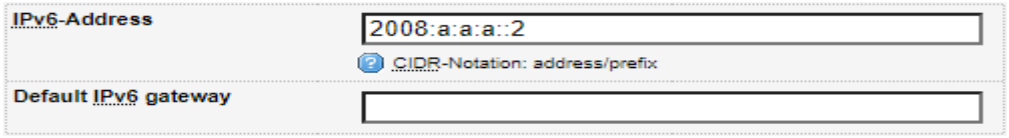
네트워크에 DHCP 서버가 없거나, 다른 이유로 인해 인터페이스에 고정 주소를 할당해야하는 경우에는 'static'을 선택하세요. 이 경우 아래 표시된 필드를 구성해야 합니다.

DHCP 페이지(SETUP > SERVICES > DHCP/DNS RELAY)에서 'DHCP Server' 옵션을 활성화 한 경우, 'DHCP'를 선택할 수 없습니다. AP 는 DHCP 클라이언트와 DHCP 서버가 동시에 될 수 없습니다.

장치가 DHCP 서버 없이 자체 IP 주소를 생성할 수 있도록 하려면 SLAAC 를 선택하세요.

IPV6 address and Default IPV6 gateway:

이러한 필드를 통해 IPV6 주소 및 게이트웨이를 일부 서비스에 추가하고 CIDR 유형 주소 구문을 허용할 수 있습니다.



Delegated prefix length (for ULA Addresses)

1~128 사이의 IPv6 네트워크 주소 접두사

IPv4-Address (only in static mode)

근거리 통신망에 있는 AP 의 IP 주소입니다. LAN 에 사용 가능한 IP 주소 범위에서 사용하지 않는 IP 주소를 할당합니다. 예: 192.168.0.1.

IPv4-Netmask

근거리 통신망의 서브넷 마스크입니다.

Default IPv4-Gateway

LAN 에 있는 라우터의 IP 주소입니다. 게이트웨이가 정의되지 않은 경우 0.0.0.0 을 사용하세요.

Default Gateway Metric

자체 게이트웨이를 사용하여 여러 네트워크가 구성된 경우 기본 게이트웨이 메트릭을 통해 이러한 게이트웨이 간에 우선 순위를 도입할 수 있습니다. Metric 이 가장 낮은 게이트웨이가 선택됩니다.

DNS-Server:

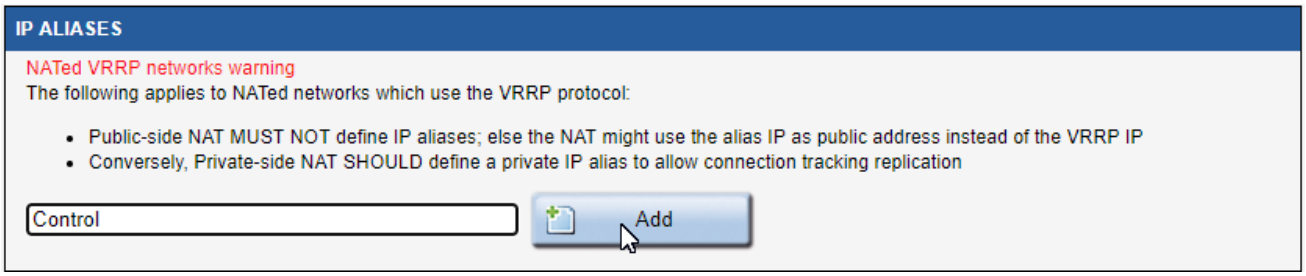
사용하려는 DNS 서버의 IP 주소입니다. DHCP 프로토콜을 선택한 경우, TOOLS/System 메뉴에 정의된 값을 사용하도록 선택하거나 이 네트워크에 특정 새 호스트 이름을 정의할 수 있습니다.

IPV6 Global configuration:

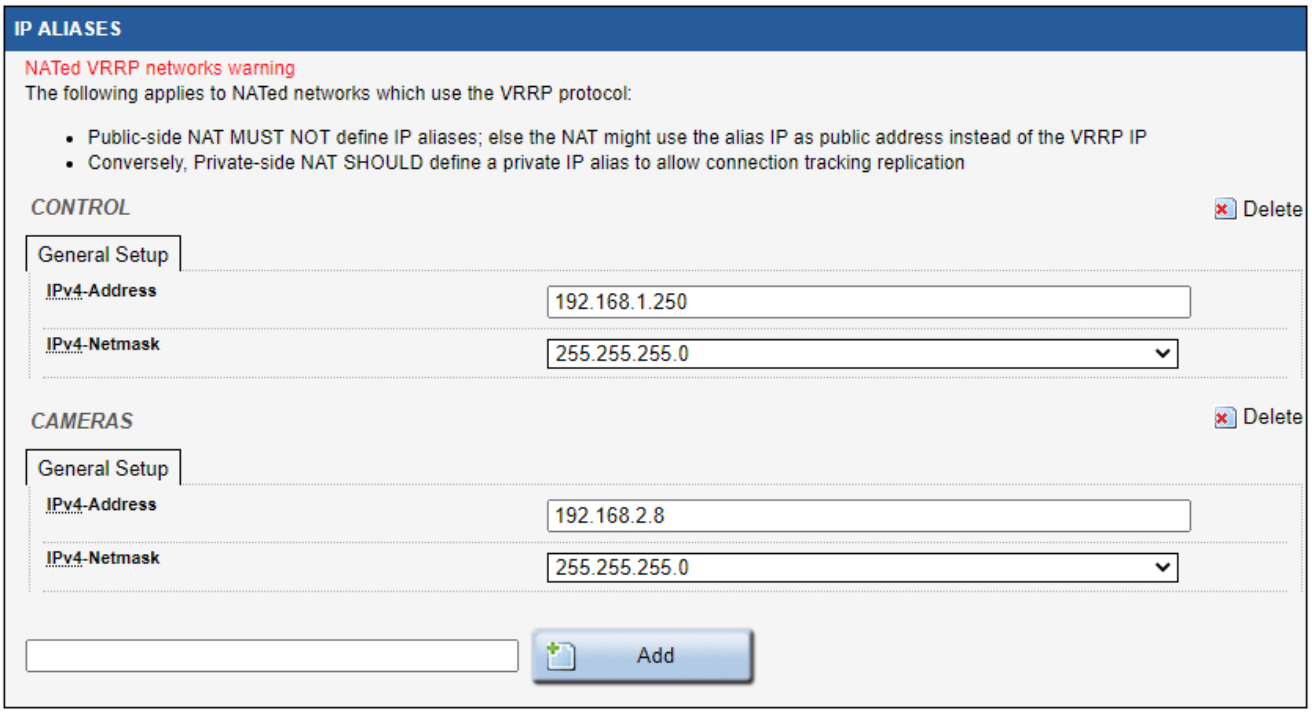
이 필드는 IPv6 ULA 접두사를 허용하고 개인 네트워크에 고유한 로컬 주소를 추가할 수 있습니다.

IP Alias:

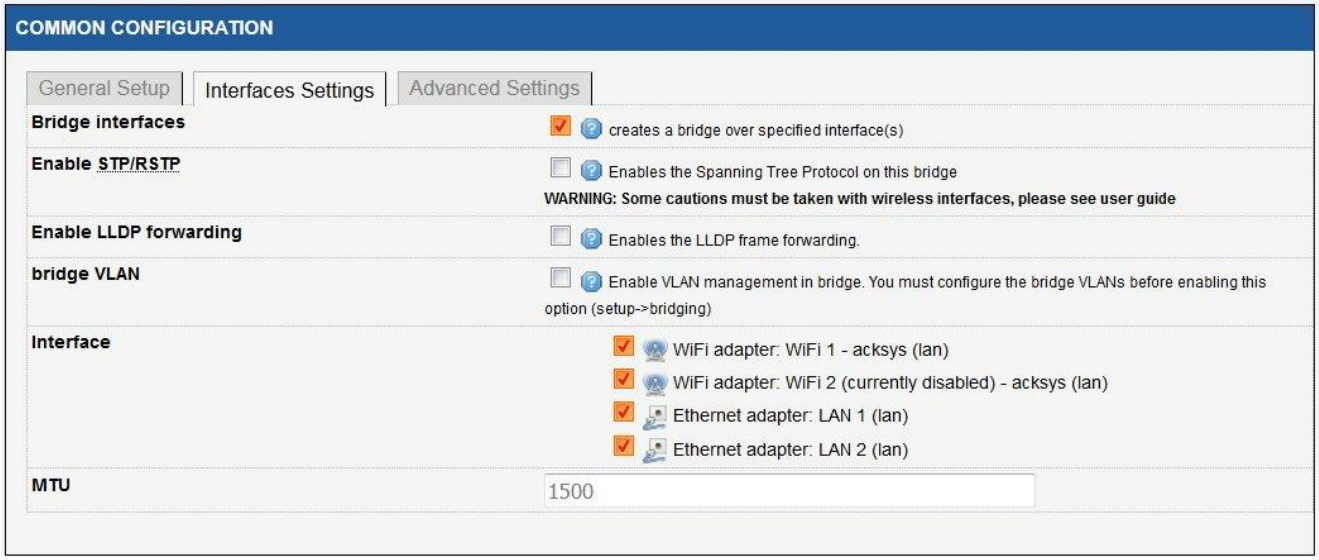
IP 별칭은 여러 네트워크에서 장치에 액세스해야하는 경우 유용합니다. 예를 들어, 제품이 라우터 모드로 구성되어 다른 하위 네트워크의 게이트웨이로 작동하는 경우입니다.



IP 별칭을 추가하려면 mnemonic 을 입력 후, 추가를 클릭한 다음 원하는 IP 주소와 연관된 서브넷 마스크를 입력하세요.



Interfaces Settings:



Bridge interfaces:

이 기능을 선택하면 네트워크의 모든 인터페이스는 이더넷 스위치와 동등한 소프트웨어로 연결됩니다.

Enable STP/RSTP:

STP/RSTP (Spanning Tree Protocol) 기능이 활성화됩니다. 이 기능을 사용하지 않는다면 네트워크 루프를 피하기 위해 장치를 직접 설정해야 합니다.

무선 인터페이스와 함께 사용 시 주의사항이 있으니, *Spanning Tree Protocols (STP, RSTP)* 를 참조하세요.

Enable LLDP forwarding:

이 체크박스를 선택하면, 내부 브릿지가 LLDP(Link Layer Discovery Protocol) 멀티캐스트 프레임을 전달합니다.

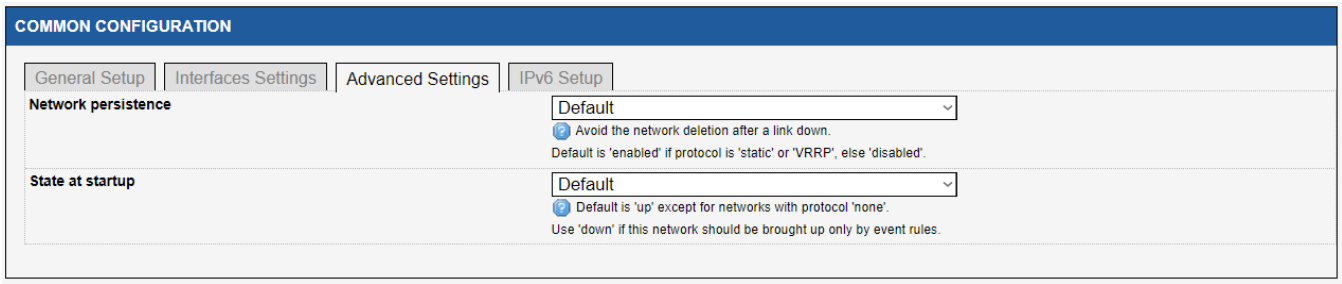
Bridge VLAN:

브리지에서 VLAN 관리를 활성화합니다. 이 옵션을 활성화하기 전에 SETUP > BRIDGING 에서 브리지 VLAN 을 구성해야 합니다. 자세한 내용은 *Vlan Management* 를 참조하세요.

Interface:

사용 가능한 네트워크 인터페이스 목록입니다. 비활성화된(회색으로된) 인터페이스는 이미 다른 네트워크에서 사용 중입니다. 브릿지 네트워크의 경우, 구성 중인 LAN 으로 함께 브릿지할 모든 인터페이스를 선택하세요. 단순한 네트워크의 경우, 구성할 하나의 인터페이스를 선택하세요.

Advanced Settings:



Network Persistence:

이 옵션이 활성화되면 물리적 인터페이스의 연결이 끊어져도 IP 설정(라우팅, 게이트웨이, 가상 인터페이스 등)이 지속됩니다. 예를 들어 인터페이스에서 링크가 끊어졌을 때 DHCP 요청을 시스템적으로 보내는 것을 방지할 수 있습니다.
static 프로토콜(고정 IP)의 기본값은 활성화되며, 다른 모든 프로토콜(DHCP, VRRP)의 기본값은 비활성화됩니다.

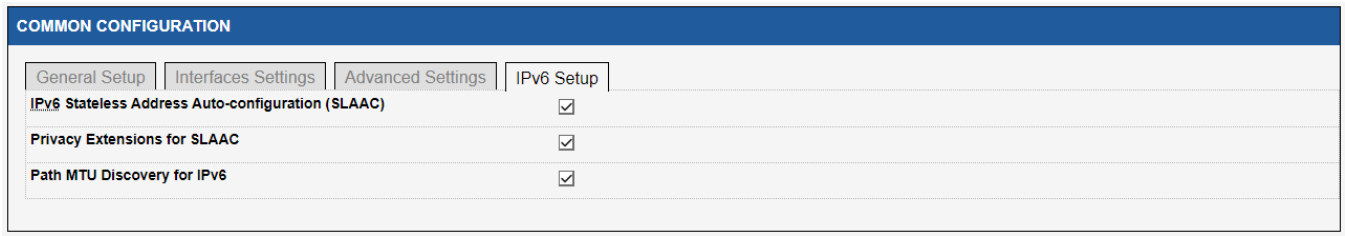
Cellular (on some models)

이 옵션은, 'Physical interfaces' 하위 메뉴에서 Cellular 구성을 가리키는 별칭 항목입니다. 이 항목에 대해서는 해당 섹션의 Cellular 을 참조하세요.

State at startup

시작 시, 네트워크 상태를 나타냅니다. 프로토콜이 'none'인 경우를 제외하고 기본 상태는 'Up'입니다. 이 네트워크가 이벤트에 의해 활성화될 경우에만 'Down'을 사용합니다.

IPv6 Setup:



IPv6 Stateless Address Auto-configuration (SLAAC):

이 옵션이 활성화되면, 네트워크 인터페이스는 자신을 인터페이스 식별자로 정의하고, IPv6 주소로 변환됩니다. (네트워크에서 라우터가 활성화된 경우)

Privacy Extensions for SLAAC:

인터페이스 MAC 주소의 마지막 48 비트에 무작위 비트를 생성하여, 개인 탐색을 활성화합니다.

Path MTU Discovery for IPv6:

호스트가 ICMPv6 유형 2 패킷(패킷이 너무 큰 경우)을 감지하면, Path MTU Discovery 프로토콜을 활성화하여, 원래 호스트(메시지를 분할할 대상의 소스)에게 올바른 패킷 크기를 알려줍니다.

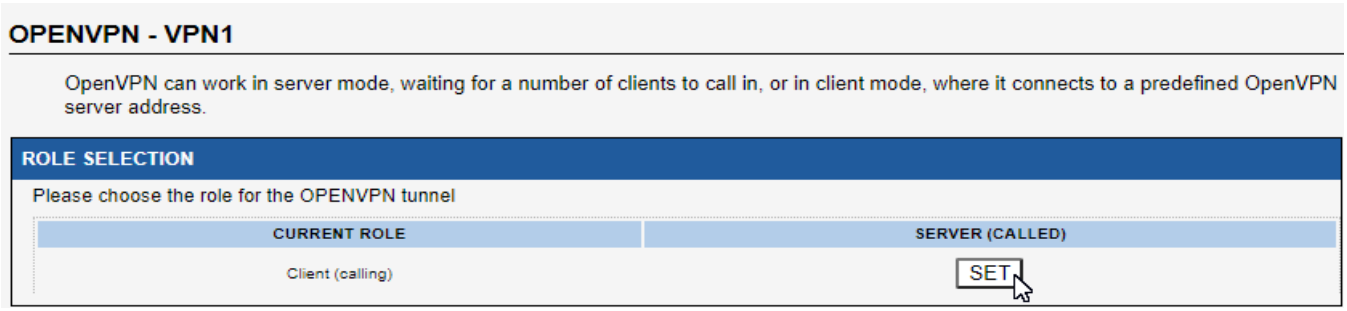
VI.1.4 VPN

VPN 구성 섹션에는 OPENVPN 및 IPSEC 를 구성할 수 있는 장치에 현재 존재하는 VPN 인스턴스가 나열됩니다.

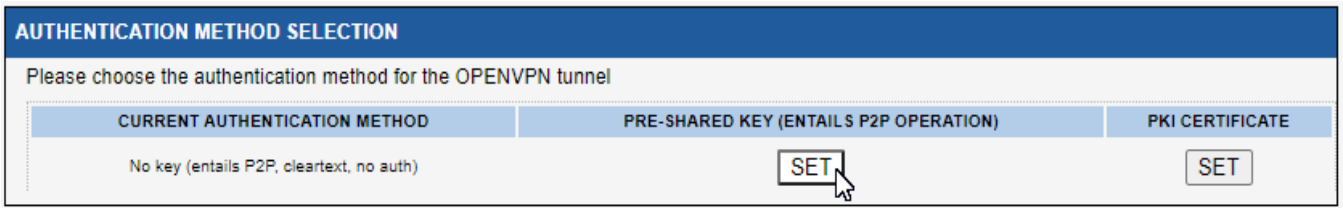
VI.1.4.1 OPENVPN

이 페이지에서는 OPENVPN 또는 IPSEC VPN 인터페이스를 만들 수 있습니다.

새 VPN 인스턴스를 생성하려면, **Add instance** 를 클릭해야 OpenVPN 구성 페이지가 열립니다.



ROLE SELECTION 섹션에서는 클라이언트에서 서버로 또는 그 반대로 역할을 변경할 수 있습니다.



인증 방법 또는 역할을 변경하면, 그에 따라 다음 섹션이 업데이트되니 주의 바랍니다.

CONFIGURATION

Basic settings | Advanced settings

Enable virtual network	☑
OpenVPN instance description	vpn1 Friendly name for this VPN instance
Remote OpenVPN server address	110.25.250.16 Remote OpenVPN server address
VPN subnet local tunnel endpoint IP address	10.8.0.2 IP address of the local VPN tunnel endpoint, not used in TLS client mode since it is pulled from server
VPN subnet mask	255.255.255.0 Subnet mask of the VPN tunnel subnet, not used in TLS client mode
VPN subnet remote tunnel endpoint IP address	10.8.0.1 IP address of the remote VPN tunnel endpoint This IP will be used as default gateway to route via the VPN tunnel. This is not the system default gateway, but default gateway to use in routes created by openvpn and where gateway is not filled.

OPENVPN - VPN1

OpenVPN can work in server mode, waiting for a number of clients to call in, or in client mode, where it connects to a predefined OpenVPN server address.

CONFIGURATION

Tunnel settings | Auth/Crypto | Client settings

Enable virtual network	☑
State at startup	Default Default is 'up' except for networks with protocol 'none'. Use 'down' if this network should be brought up only by event rules.
OpenVPN instance description	vpn1 Friendly name for this VPN instance
Role	Client (calling)
Protocol	UDP Favor UDP, as TCP leads to potential conflicts in the TCP over TCP redundancy mechanisms
Listener port	1194 UDP or TCP port that the server will listen to, and that the client will call
Data channel compression	☐ Use fast LZO compression
Tunnel type	L3 (IP) tunnel Only L3 tunnels are supported
VPN subnet local IP address	10.8.0.1 IP address of the local VPN endpoint, not used in TLS client mode since it is pulled from server
VPN subnet mask	255.255.255.0 Subnet mask of the VPN subnet, not used in TLS client mode
Tunnel MTU	1500 Encapsulated MTU, adjust to avoid fragmentation; the default of 1419 allows the default SHA1 digest
Keepalive period	10 Keepalive period (seconds). Every such time, a packet is sent to each peer to elicit a response.
Keepalive timeout	30 Keepalive timeout (seconds). Connection terminates if no traffic is received from the peer for such time.

State at startup
시작할 때 VPN 네트워크 상태를 제공합니다. 프로토콜이 'none'인 네트워크를 제외하고, 기본 상태는 "Up"입니다. 이 네트워크가 이벤트 규칙에 의해서만 활성화되어야 하는 경우, 'Down'을 사용하세요.

OpenVPN instance description
VPN 인스턴스에 대한 설명이나 이름을 기입합니다.

Role
역할은 서버 또는 클라이언트가 될 수 있습니다. 서버는 클라이언트의 호출을 기다리며, 클라이언트는 서버를 호출하여 연결을 시작합니다.

Protocol
프로토콜은 UDP 또는 TCP 를 선택할 수 있습니다. TCP 는 TCP over TCP 중복 메커니즘에서 잠재적인 충돌로 이어질 수 있으므로, UDP 를 선호합니다. 클라이언트와 서버 사이의 라우터가, 선택한 형식의 패킷을 승인하기 위해 필요한 포트를 열어야 합니다.

Listener port
이것은 서버가 대기하며, 클라이언트의 호출을 기다리는 UDP 또는 TCP 포트입니다. 기본값은 1194 입니다.

Data channel compression
이 옵션을 선택하면, 터널을 통해 전달되는 데이터를 압축합니다. Fast LZO 압축이 사용됩니다.

Tunnel Type
L3 터널만 지원됩니다.

VPN subnet local IP address
이 VPN 종단점의 가상 IP 주소입니다.

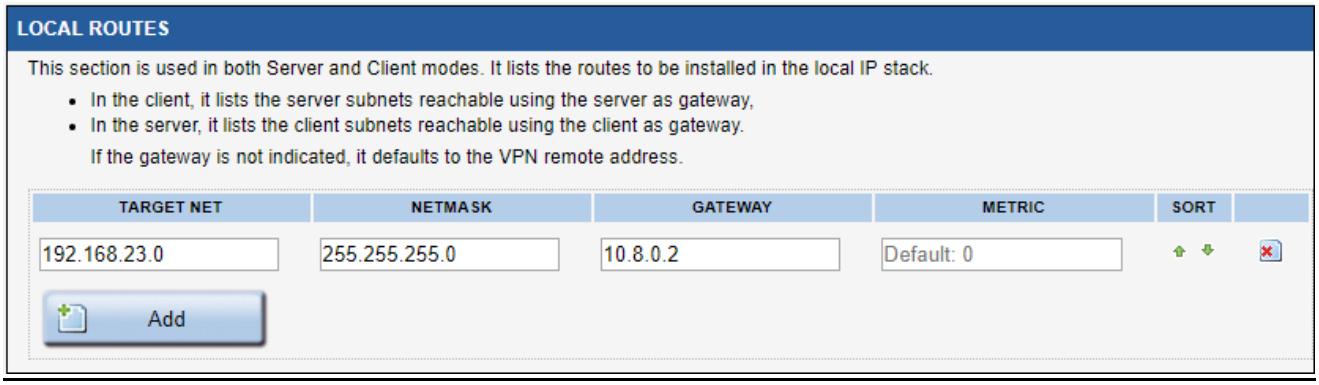
VPN subnet mask
이 VPN 종단점 IP 주소에 연결된 서브넷 마스크입니다.

Tunnel MTU
캡슐화된 MTU 는 조각화를 방지하기 위해 조정되어야 합니다. 기본값은 1419 바이트이며, 기본 SHA1 다이제스트가 허용됩니다.

Keepalive period
Keepalive 메커니즘은 VPN 링크가 항상 유효한지 확인합니다. 이 매개변수로 정의된 주기로 각 피어에서 프로브가 전송됩니다. Keepalive 주기는 초 단위로 지정됩니다.

Keepalive timeout
이것은 Keepalive 제한 시간 값(초)입니다. 이 시간보다 긴 시간 동안 패킷이 수신되지 않으면 연결이 닫힙니다. **Keepalive timeout** 제한 시간 값은 **Keepalive period** 기간보다 커야 합니다.

LOCAL ROUTES



이 섹션에서는 로컬 IP 스택에 설치할 경로를 정의할 수 있습니다.

TARGET NET:
대상 서브넷입니다.

NETMASK:
대상 서브넷 마스크입니다.

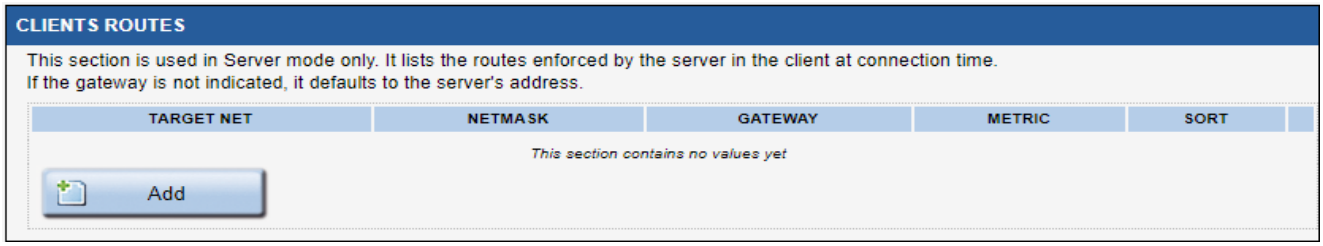
GATEWAY:
대상 네트워크에 도달하기 위해 사용해야 하는 게이트웨이입니다. 비워두면 게이트웨이는 VPN 원격 주소로 기본 설정됩니다.

METRIC:
이 경로에 대한 메트릭을 설정합니다.

USERS VALIDATION

이 섹션은 서버 모드에서만 사용됩니다. 이 VPN 인스턴스에 연결할 수 있는 사용자를 표시합니다. 선택적으로 서버에서 클라이언트측 서브넷으로의 라우팅을 활성화 할 수 있습니다..

CLIENTS ROUTES

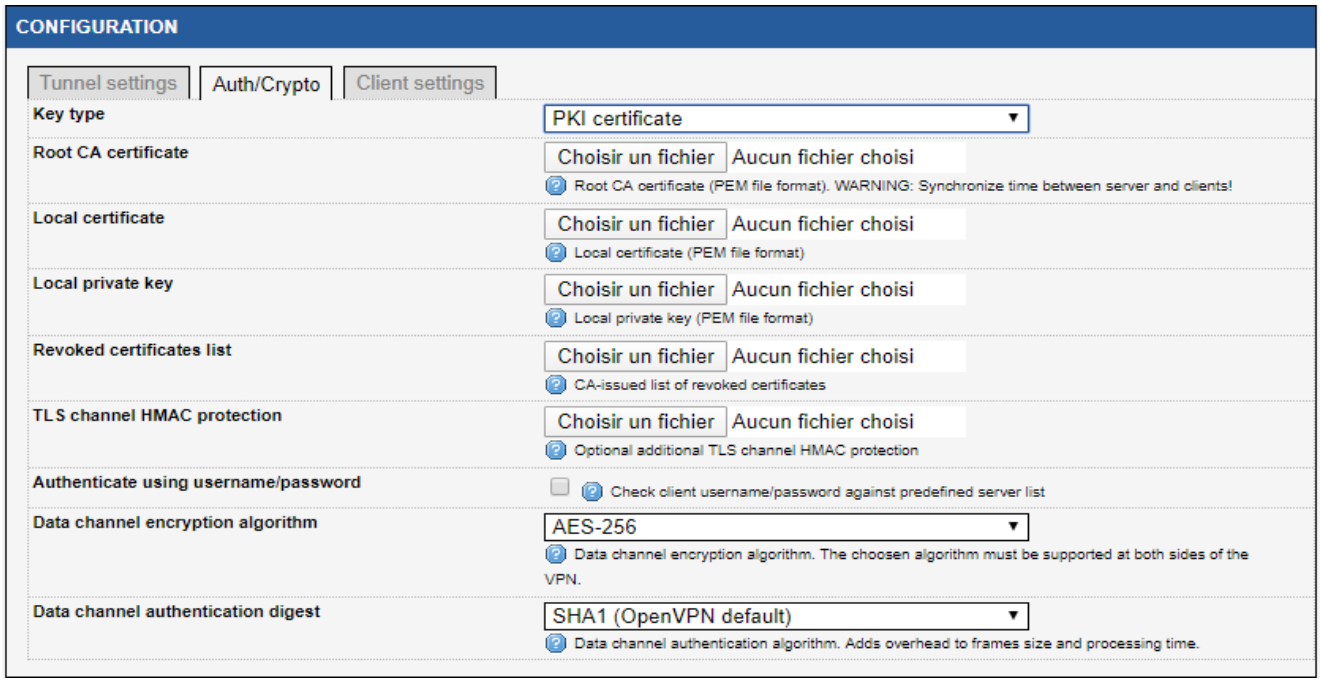


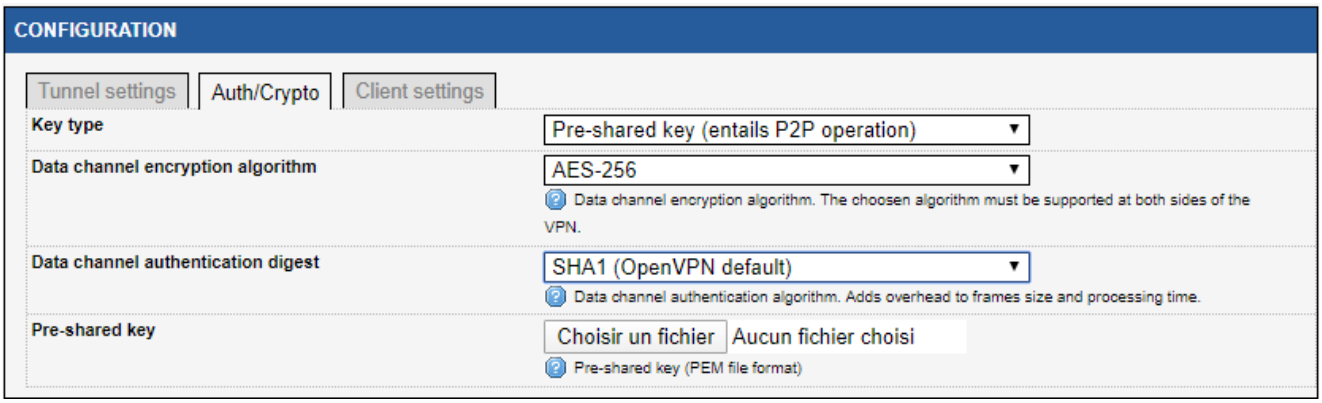
이 섹션은 서버 모드에서만 사용됩니다. 연결 시 클라이언트의 서버에서 적용되는 경로를 표시합니다. 게이트웨이가 표시되지 않으면, 기본적으로 서버 주소가 사용됩니다.

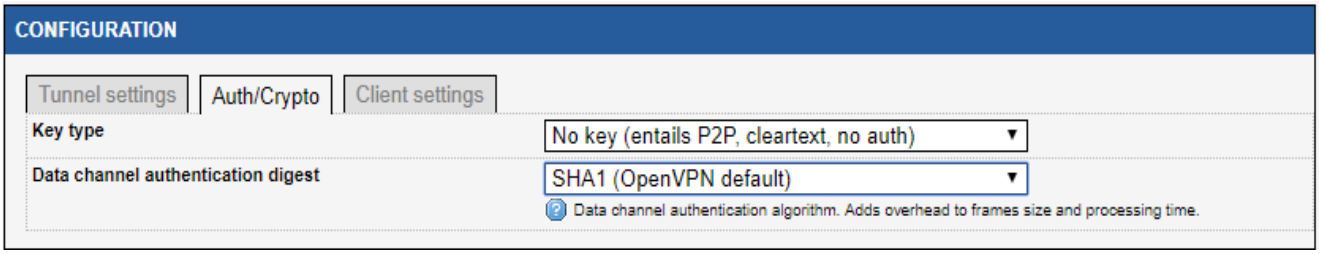
경고: 경로는 TLS VPN 인증을 사용하는 서버에서만 시행할 수 있습니다. 아래에 설명된 'Auth/Crypto' 탭에서 PKI 인증서를 선택해야 합니다.

AUTH/CRYPTO

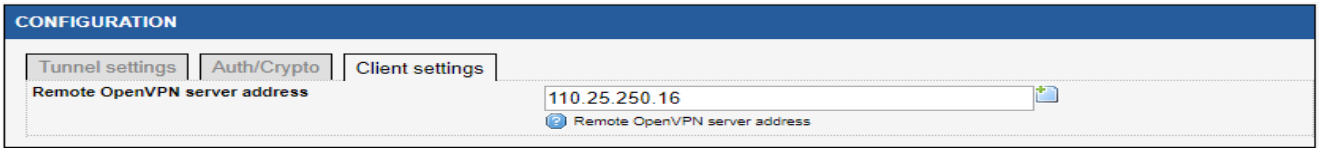
이 페이지에서는 VPN 터널에 대한 자격 증명, 암호화 및 인증 방법을 정의할 수 있습니다. 이러한 필드의 정의에 대한 자세한 내용은 OpenVPN 설명서를 참조하세요.
https://community.openvpn.net/openvpn/wiki/SecurityOverview







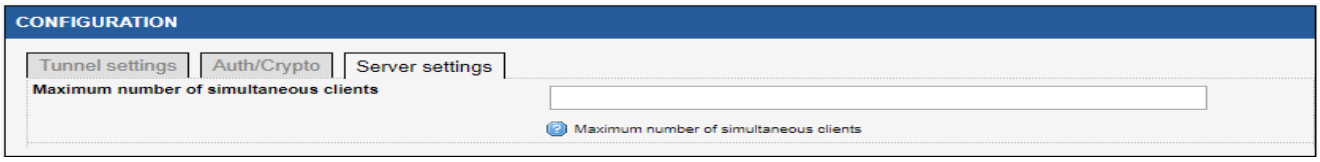
Client settings



Remote OpenVPN server address:

원격 OpenVPN 서버 주소입니다.

Server settings

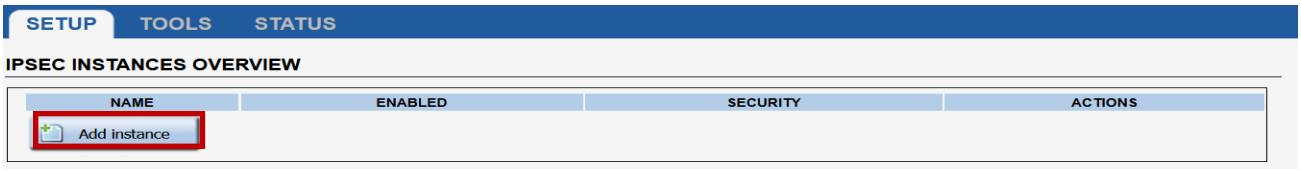


Maximum number of simultaneous clients:

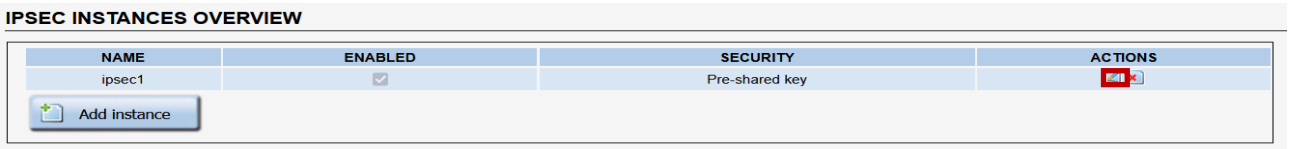
이 설정을 사용하면, 서버에 동시에 연결할 수 있는 클라이언트 수를 제한할 수 있습니다. 이를 통해 제품의 물리적 리소스 사용을 최적화할 수 있습니다.

VI.1.4.2 IPSEC

새 IPSEC 인스턴스를 생성하려면 "추가" 인스턴스를 클릭하면 IPsec 버튼이 열립니다.

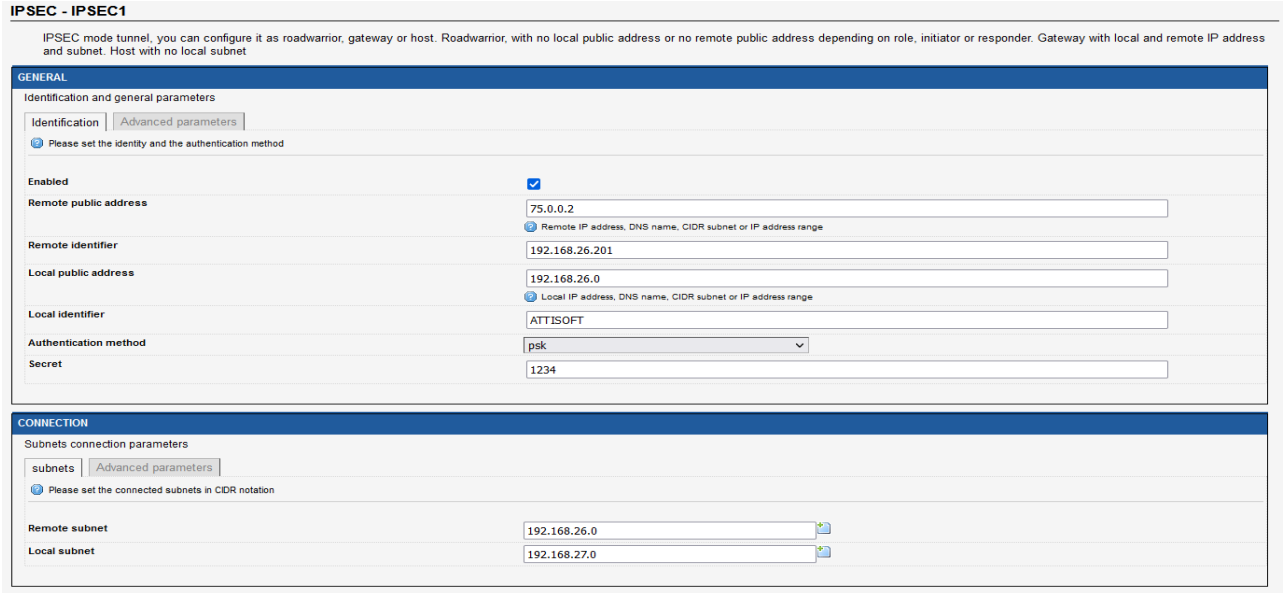


새로 생성된 인스턴스 옆에 있는 "편집" 버튼을 클릭합니다.

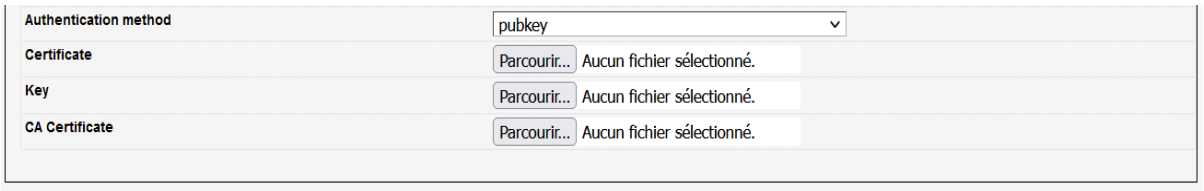


IPV4 또는 IPV6 주소로 인스턴스를 구성할 수 있는 인스턴스의 구성 페이지로 리디렉션합니다.

일반 설정 섹션은 기본 IPsec 매개변수를 구성하는 데 사용됩니다. 일반 및 연결 설정 섹션에 있는 구성 필드에 대한 정보는 아래 표를 참조하세요



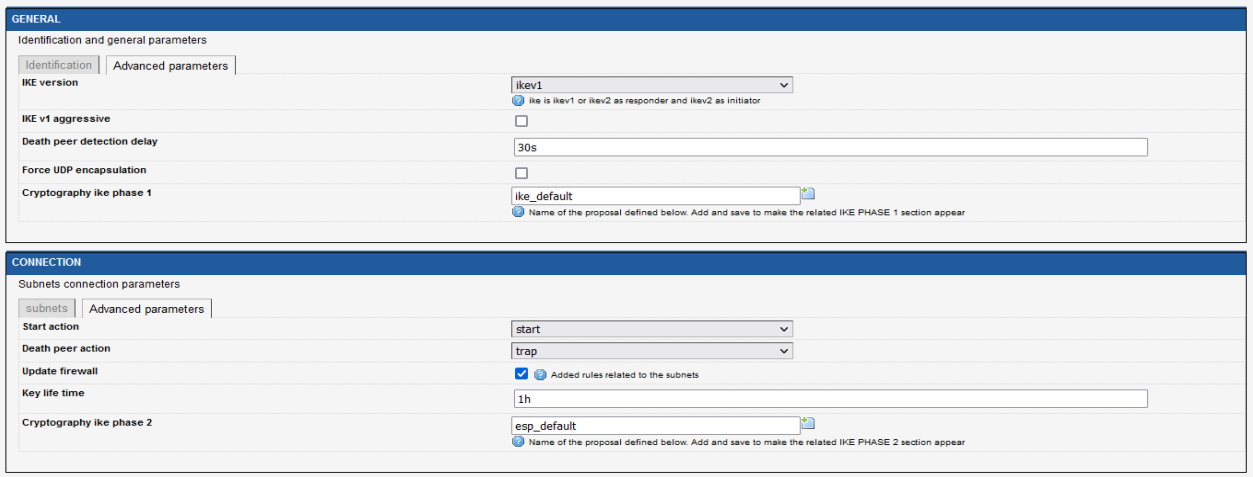
공용키



필드	값	설명
Enable	off | on; default: **on**	IPsec 인스턴스를 켜거나 끕니다.
Remote public address	host | ip; default: **none**	원격 IPsec 인스턴스의 IP 주소 또는 호스트 이름입니다.
Remote identifier	ip | string; default: **none**	인증 중에 올바른 참가자를 식별하는 방법을 정의합니다. • **IP** - 인터넷 프로토콜 주소 **FQDN** - 정규화된 도메인 이름으로 정의된 ID입니다. 호스트의 완전한 도메인 이름입니다.
Local public address	ip | string; default: **none**	인증 중에 사용자(왼쪽 참가자)를 식별하는 방법을 정의합니다. • **IP** - 인터넷 프로토콜 주소 **FQDN** - 정규화된 도메인 이름으로 정의된 ID입니다. 호스트의 완전한 도메인 이름입니다.
Local identifier		
Authentication method	Pre-shared key | X.509; default: **Pre-shared key**	인증 방법을 지정합니다. 사전 공유 키와 X.509 인증서 중에서 선택합니다.
Pre-shared key: Pre shared key	string; default: **psk**	보안 채널이 설정되기 전에 IPsec 피어 간의 인증에 사용되는 공유 암호입니다.
X.509: Key	.pem file; default: **none**	공개 키 파일
X.509: Local Certificate	.pem file; default: **none**	로컬 인증서 파일
X.509: CA Certificate	.pem file; default: **none**	인증 기관 파일

Advance settings

고급 설정 섹션은 아래 표를 참조하여 IPsec 연결의 고급 기본 매개변수를 구성하는 데 사용됩니다.



필드	값	설명
IKE v1 aggressive	off | on; default: **off**	발신 연결에 대해 aggressive 모드를 켜거나 끕니다. Aggressive 모드는 대부분의 데이터를 첫 번째 교환에 저장하므로 Main 모드(총 6개 메시지)보다 적은 수의 교환(총 4개 메시지)을 수행합니다. 공격적 모드에서는 보안 채널이 있기 전에 정보가 교환되므로 주 모드보다 덜 안전하지만 더 빠릅니다. aggressive 모드는 IKEv1에서만 사용할 수 있습니다. IKEv2가 선택된 경우 이 필드는 숨겨집니다..
Force encapsulation	off | on; default: **off**	"NAT 없음" 상황이 감지되더라도 ESP 패킷에 대해 UDP 캡슐화를 강제합니다.
Local firewall	off | on; default: **on**	이 장치에서 이 IPsec 인스턴스의 트래픽을 허용하는 데 필요한 방화벽 규칙을 추가합니다.
Update firewall	off | on; default: **on**	이 장치에서 반대쪽 IPsec 인스턴스의 트래픽을 허용하는 데 필요한 방화벽 규칙을 추가합니다.
Key live time	integer; default: **none**	트래픽을 보내거나 받지 않은 경우 CHILD_SA가 닫히는 시간 초과 간격을 정의합니다.
Dead Peer Detection	off | on; default: **off**	IKE(Internet Key Exchange) 중에 " dead " 피어를 감지하는 데 사용되는 기능입니다. 상대 피어가 사용할 수 없을 때 메시지 수를 최소화하고 장애 조치 메커니즘으로 트래픽을 줄이는 데 사용됩니다.
Dead Peer Detection: DPD action	Start | Trap | Clear | None; default: **Restart**	IPsec 피어의 활성 상태를 확인하기 위해 알림 메시지가 주기적으로 전송되는 Dead Peer Detection 프로토콜의 사용을 제어합니다.
Dead Peer Detection: DPD Delay	integer; default: **none**	R_U_THERE 메시지 또는 INFORMATIONAL 교환을 동료에게 보내는 빈도
Dead Peer Detection: DPD Timeout	integer; default: **none**	비활성 시 피어에 대한 모든 연결이 삭제되는 제한 시간 간격을 정의합니다.

VI.1.5 Bridging

이 섹션에서는 통합된 브리징 서비스를 구성할 수 있습니다.

VI.1.5.1 STP/RSTP

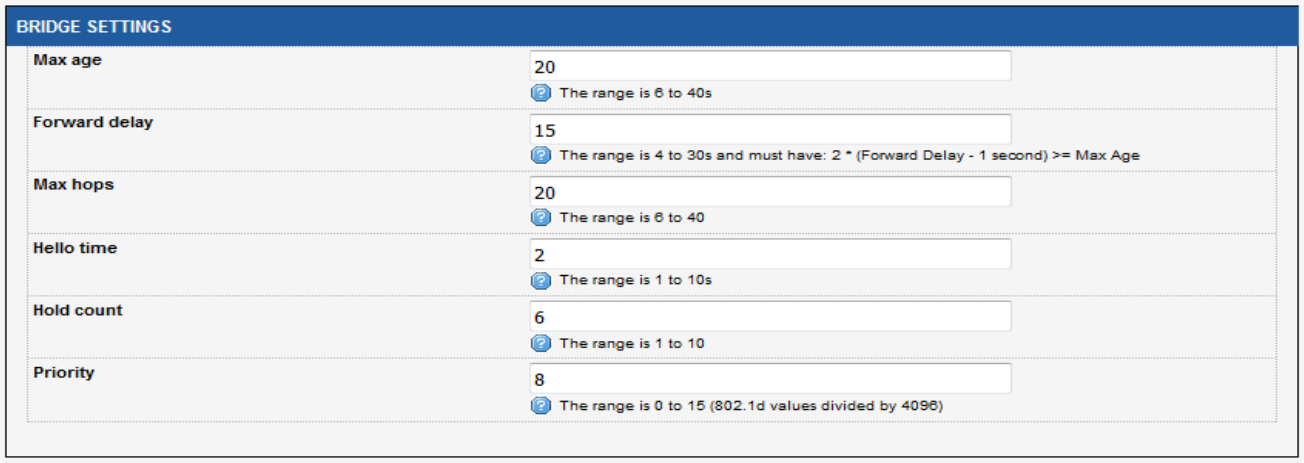
이 섹션에서는 네트워크 포트 및 브리지에 대한 STP/RSTP 를 구성할 수 있습니다. 특정 네트워크에 대해 STP/RSTP 를 구성하려면, Bridge 를 활성화해야 합니다.

STP/RSTP overview

NETWORK	BRIDGE STATUS	STP/RSTP STATUS	BRIDGED INTERFACE	ACTIONS
lan	Enabled	Disabled	WiFi adapter: WiFi 1 - Acksys WiFi adapter: WiFi 2 - Service Ethernet adapter: LAN 1 Ethernet adapter: LAN 2	

브리지 네트워크에 대한 STP/RSTP 설정을 변경하려면, 우측 편집 버튼을 클릭하세요

STP/RSTP Bridge settings



Max age

루트 브리지에 의해 전송되는 정보의 최대 수명입니다. (입력 범위는 6 ~ 40s)

Forward delay

루트 및 지정 포트를, 차단상태에서 학습상태 또는 학습상태에서 전달 상태로 전환할 때의 지연 정도를 말합니다.
(입력 범위는 4 ~ 30s), 2 * (Forward Delay - 1 second) >= Max Age)

Max hops

BPDU(Bridge Protocol Data Unit)가 전달할 수 있는 최대 홉 수 (입력 범위는 6 ~ 40)

Hello time

지정된 포트별 구성 메시지의 주기적인 전송 간격입니다. (입력 범위는 1 ~ 10s)

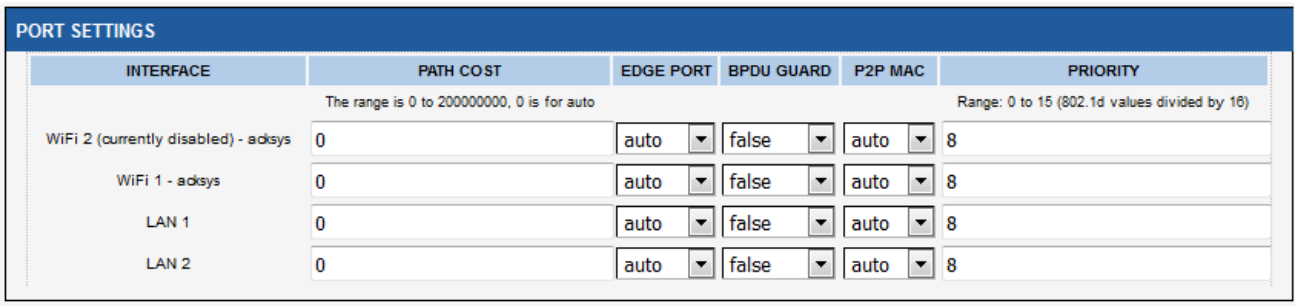
Hold count

1 초 동안 보낼 수 있는 최대 BPDU 수를 말합니다.

Priority

STP/RSTP 토폴로지의 브리지 우선순위 범위는 0~15 이며, 0 이 가장 높은 우선순위이고 15 가 가장 작은 우선순위입니다. 루트 브리지를 선택할 수 있습니다.

STP/RSTP Port settings


PORT SETTINGS

INTERFACE	PATH COST	EDGE PORT	BPDU GUARD	P2P MAC	PRIORITY
	The range is 0 to 200000000, 0 is for auto				Range: 0 to 15 (802.1d values divided by 16)
WiFi 2 (currently disabled) - acksys	0	auto	false	auto	8
WiFi 1 - acksys	0	auto	false	auto	8
LAN 1	0	auto	false	auto	8
LAN 2	0	auto	false	auto	8

Path Cost

루트 포트 일 때, 루트 브리지에 도달하는 데 필요한 경로 비용입니다.

0 으로 설정하면 포트 속도에 따라 값이 자동으로 계산됩니다.
루트 브리지에 가장 낮은 비용을 제공하는 포트가 루트 포트가 되고, 다른 모든 중복 경로는 차단 상태가 됩니다.

Edge Port

Edge 포트(다른 브리지가 연결되지 않은 LAN 에 연결된 포트)의 초기 상태입니다.

true 로 설정하면 초기 상태는 Edge 포트로 설정되고, false 로 설정하면 초기 상태는 non-edge 포트로 설정되며, auto 로 설정하면 제품이 자동으로 포트 유형을 감지합니다.
RSTP 는 Edge 포트를 포워딩 상태로 직접 전환합니다.

BPDU Guard

BPDU 수신 시 포트를 비활성화하려면, Edge 포트(다른 브리지가 연결되지 않은 LAN 에 연결된 포트)에서 true 로 설정해야 합니다.

P2P Mac

이 설정을 통해 초기 point to point 링크 상태를 설정할 수 있습니다.

true 로 설정하면 초기 링크 상태는 point-to-point 링크(두 브리지 사이의 직접 링크(두 브리지 사이에 허브와 같은 중간 장비 없음))로 설정되어, 지정된 포트가 포워딩 상태로 빠르게 전환되도록 도와줍니다.
자동으로 설정하면 제품이 링크 유형을 자동으로 감지합니다.

Priority

브리지 내부의 포트 우선 순위입니다.

브리지에서 여러 포트가 동일한 경로 비용을 제공하는 경우, STP/RSTP 는 포트 우선 순위를 사용하여 루트 포트를 선택합니다.
범위는 0~15 까지이며, 0 이 가장 높은 우선 순위이고 15 가 가장 작은 우선 순위입니다.

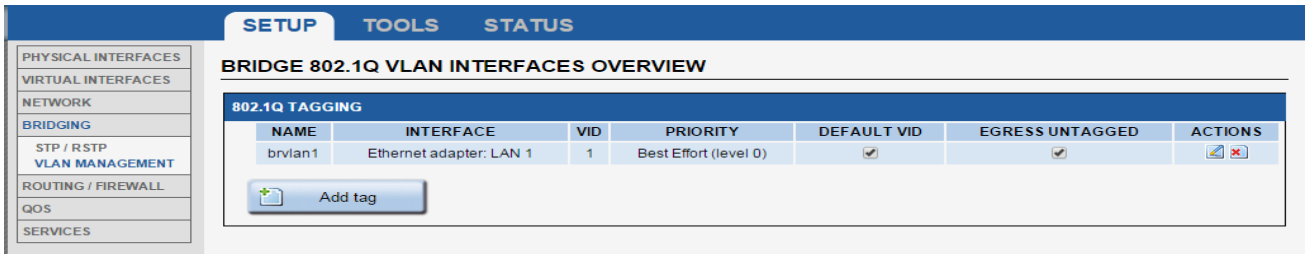
VI.1.5.2 Vlan Management

이 페이지에서는 브리지된 포트의 802.1q 태그를 관리할 수 있습니다.

브리지에 포함된 각 인터페이스에 대해 지원되는 VLAN 을 지정할 수 있습니다.

VLAN Interfaces overview

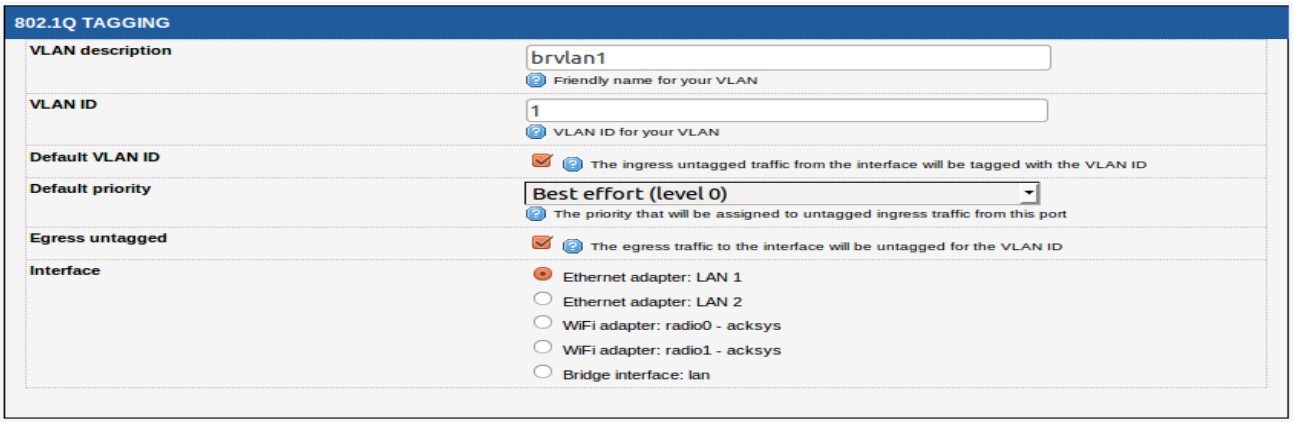
overview 에서는 구성된 모든 포트 및 VLAN 조합을 리스트 형태로 확인할 수 있습니다.



Add tag 버튼을 클릭하면, 하나의 포트에 VLAN 구성을 추가할 수 있습니다.

편집 버튼을 클릭하여 VLAN 속성을 정의하거나 변경합니다.

Port configuration page



VLAN description:

VLAN 에 대한 설명이나 이름을 입력합니다.

VLAN ID:

VLAN ID 를 입력합니다.

Default VLAN ID:

이 옵션을 체크하면 태그가 지정되지 않은 모든 수신 트래픽이 VLAN 에 배치됩니다.
포트당 하나의 VLAN 만 기본값이 될 수 있습니다.

Default priority:

우선 순위를 선택합니다. 이 옵션은 기본 VLAN ID 가 선택된 경우에만 사용할 수 있습니다.

Egress untagged:

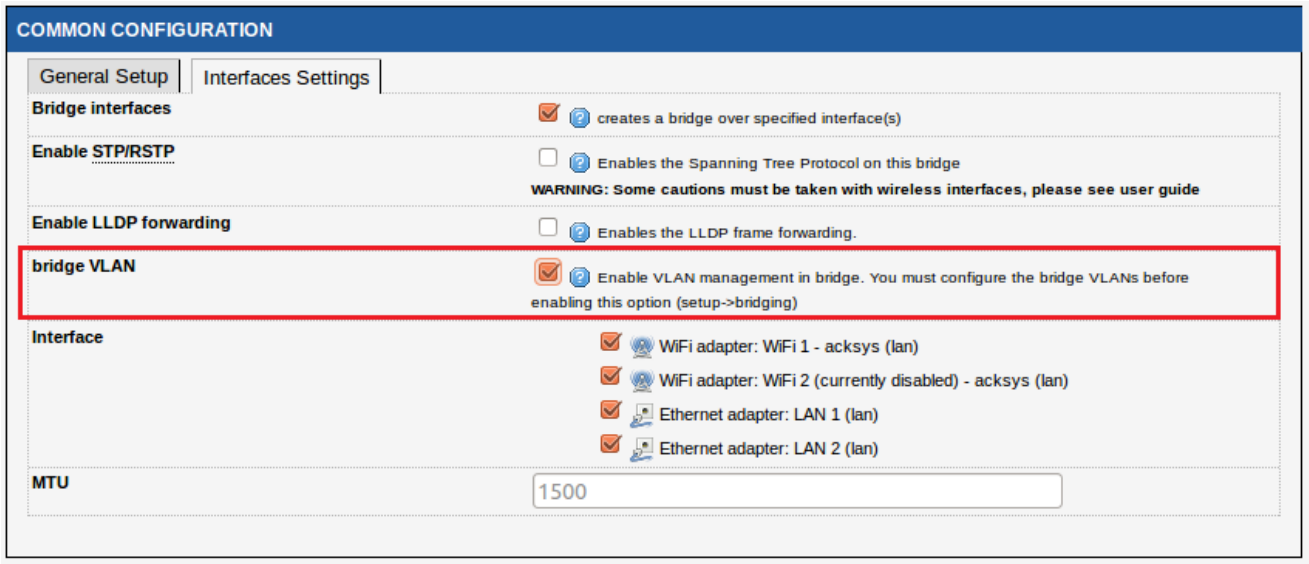
이 옵션을 체크하면 포워딩 하기 전에 VLAN 태그가 프레임에서 제거됩니다.

Interface:

VLAN 설정을 적용할 포트를 선택합니다.
관련된 VLAN 은 전부, 브리지의 모든 인터페이스에 구성되어야 합니다.

Enable the Bridging VLAN

NETWORK/Interface Settings 하위 메뉴에서 브리지 VLAN 을 활성화 할 수 있습니다.



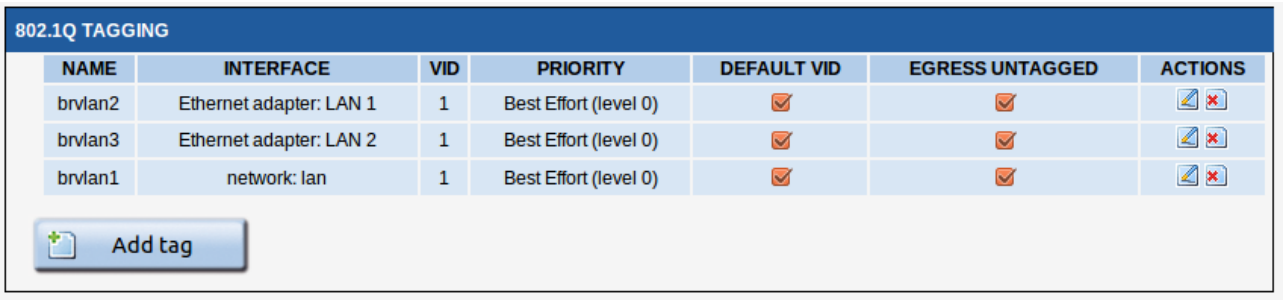
브리지 VLAN 을 활성화하면, 보안상의 이유로 태그가 지정되지 않은 프레임이 삭제됩니다. 태그가 지정되지 않은 모든 프레임은, 원래 포트에서 기본 VLAN 을 구성하여 특정 VLAN 에 배치해야 합니다.

VLAN 태그가 없는 포트를 통해 제품에 액세스하려는 경우에는, **Bridge interface** 자체(브리지 상위 계층 인터페이스)에 VLAN 을 추가한 후 **default VID** 를 확인하고, 필수 포트에서 **egress untagged** 옵션을 체크 해야 합니다.

제품에 액세스하려는 모든 인터페이스에 동일한 VLAN 을 추가하고, **default VID** 와 egress untagged 옵션을 확인하세요.

이 VID 값은 다른 VLAN 에서 사용 중인 값이 아니어야 합니다. (또는 해당 트래픽이, VLAN 이 설정되어 있지 않은 트래픽과 혼합되는 값이 아니어야 합니다.)

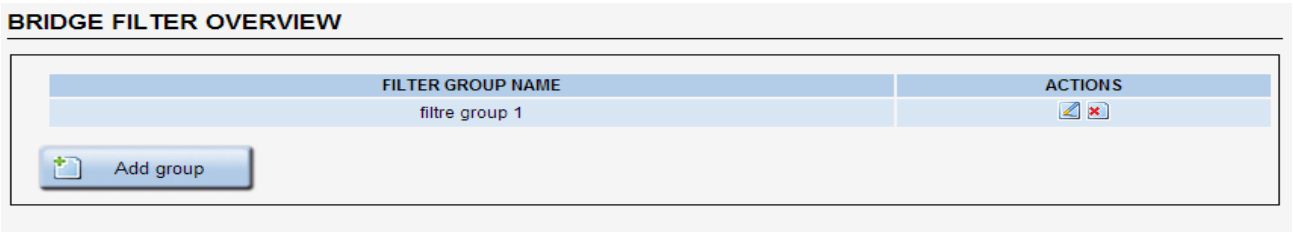
아래 그림은 VLAN 없이 LAN1 또는 LAN2 에서 제품에 액세스하는 간단한 구성을 보여줍니다.



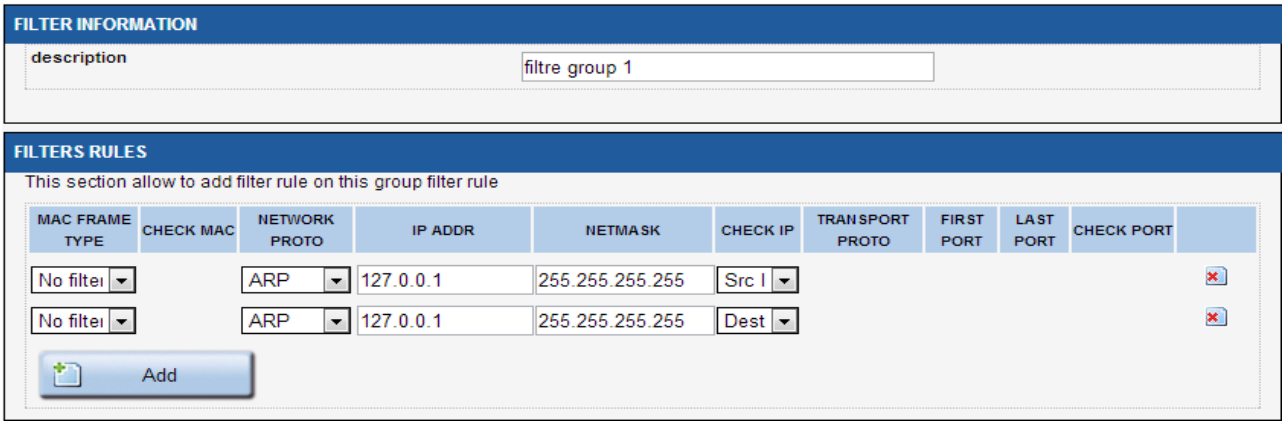
VI.1.5.3 Bridge filter

이 섹션에서는 layer2(링크 수준) 필터 그룹을 관리할 수 있습니다. 각 필터 그룹은 여러 규칙을 포함할 수 있으며, 만약 인터페이스가 브리지에 포함된 경우 하나 이상의 이더넷 또는 무선 인터페이스에 영향을 미칠 수 있습니다. 필터는 그룹에서 하나의 규칙이 일치하면 프레임을 drop 시킵니다.

Add group



Edit group



Description:

그룹에 대한 설명이나 이름을 입력합니다.

Mac frame type:

layer2 프레임 유형을 선택합니다.

- No filter : 필터를 적용하지 않습니다.
- Unicast : 프레임이 유니캐스트인지 확인합니다.
- Broadcast : 프레임이 브로드캐스트 유형인지 확인합니다.
- Multicast : 프레임이 멀티캐스트인지 확인합니다.

Check MAC:

이 필드는 Mac 프레임 유형이 'No filter'와 다른 경우에만 표시됩니다.

- Src Addr : 소스 MAC 주소 필드에서 프레임 유형을 확인합니다.
- Dest Addr : 대상 MAC 주소의 프레임 종류를 확인합니다.

Network Proto:

layer3 프로토콜을 선택합니다.

- No filter : 필터를 적용하지 않습니다.
- ARP : ARP(Address Resolution Protocol) 프레임인지 확인합니다.
- IP : IP 프레임인지 확인합니다.
- Custom : 프로토콜 번호를 입력합니다. 예를 들어, IP 프레임의 경우 0x800 입니다.

IP addr & Netmask

이 필드는 Layer3 프로토콜이 IP 또는 ARP 로 설정된 경우에만 표시됩니다. 이 필드를 사용하여 IP 주소의 일부를 선택할 수 있습니다.

IP address	Netmask	Result
192.168.1.3	255.255.255.255	IP 주소가 192.168.1.3 인 프레임에 대해서만 일치하는 프레임
10.10.0.0	255.255.0.0	10.10.x.x 네트워크의 모든 IP 주소와 일치하는 프레임
127.0.0.1	255.255.255.255	이 인터페이스에서 제품에 할당된 IP 주소에 대해 일치하는 프레임

Check IP:

이 필드는 Layer3 프로토콜이 IP 또는 ARP 로 설정된 경우에만 표시됩니다.

- Dest IP : 프레임의 대상 IP (받는 사람) 필드를 확인하세요. ARP 프로토콜의 경우 대상 IP 주소 필드가 사용되었습니다.
- Src IP : 프레임의 소스 IP (보낸 사람) 필드를 확인하세요. ARP 프로토콜의 경우 소스 IP 주소 필드가 사용되었습니다.

Transport proto:

이 필드는 레이어 3 프로토콜이 IP 로 설정된 경우에만 표시됩니다.

- UDP : 전송 프로토콜이 UDP 인지 확인합니다.
- TCP : 전송 프로토콜이 TCP 인지 확인합니다.
- ICMP : 전송 프로토콜이 ICMP 인지 확인합니다.

First port & Last port

이 필드는 전송 프로토콜(layer4)이 UDP 또는 TCP 로 설정된 경우에만 표시됩니다. 프레임이 첫 번째 포트와 마지막 포트 사이의 포트를 사용했는지 확인하세요.

Check Port

이 필드는 전송 프로토콜(layer4)이 UDP 또는 TCP 로 설정된 경우에만 표시됩니다.

- Src : 소스 포트를 확인합니다.
- Dest : 대상 포트를 확인합니다.

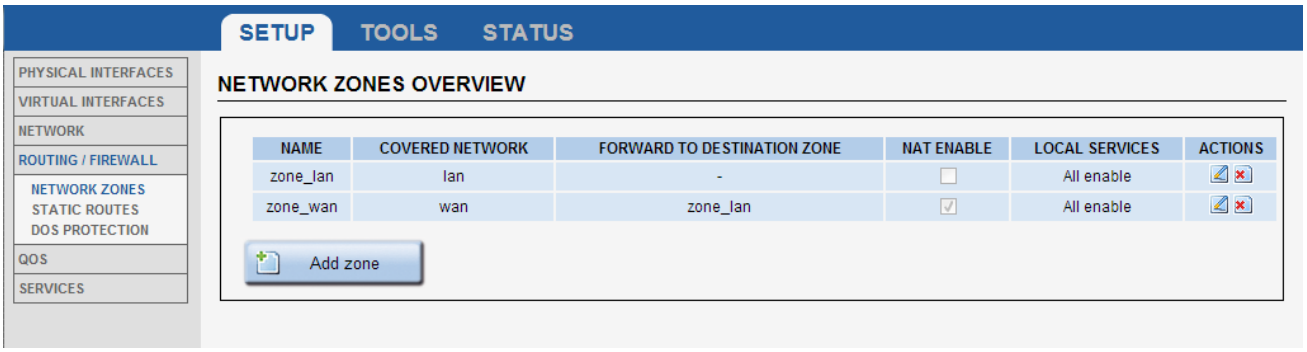
VI.1.6 Routing / Firewall

VI.1.6.1 Network zones

라우팅 규칙은 네트워크 zone 에 적용됩니다. zone 은 동일한 전달 규칙을 공유하는 네트워크의 집합입니다. zone 을 정의하고 zone 간 네트워크를 분산시킬 수 있습니다. 각 네트워크 zone 에서 다음을 수행할 수 있습니다:

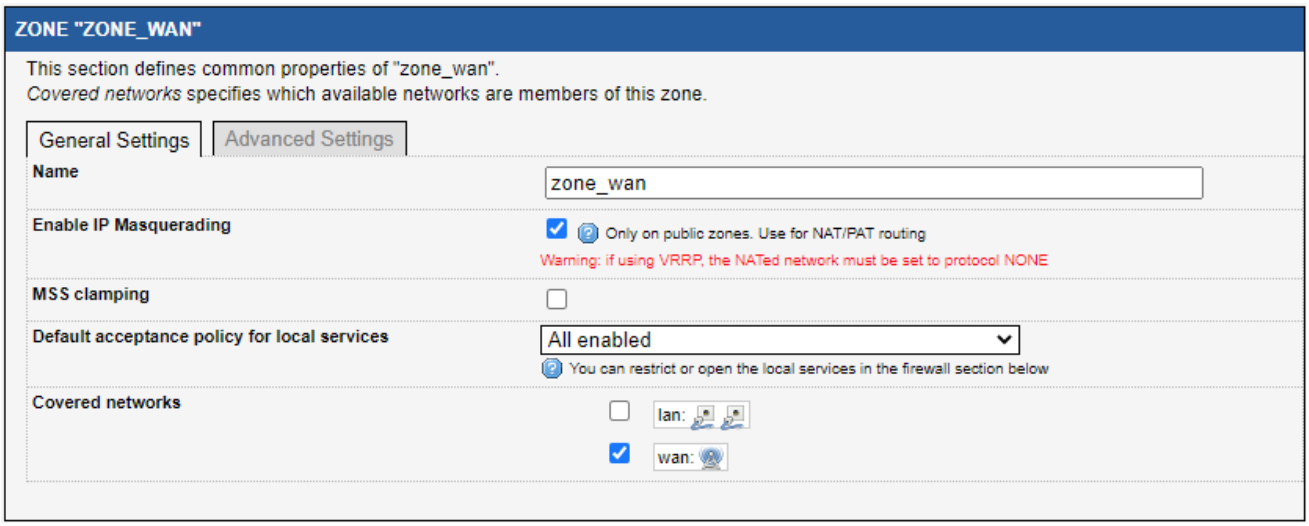
- 다른 zone 으로 전달 규칙 설정
- NAT/PAT 필터링 규칙 설정
- NAT 1:1 변환 규칙 설정
- 방화벽 규칙 설정

Zones Overview



Add zone 버튼을 클릭하여 새 zone을 만듭니다.
Edit 버튼을 클릭하여 zone 설정 페이지를 엽니다.
Remove 버튼을 클릭하여 zone 을 제거합니다.

General Zones settings



Name:
zone 에 대한 설명이나 이름을 입력합니다.

Enable IP Masquerading:
이 zone 에서 NAT/PAT 를 활성화합니다. 이 옵션은 공용 인터페이스가 포함된 zone 에서만 선택하세요.

MSS clamping:
인터페이스가 더 작은 MTU 를 사용하는 경우 MSS(최대 세그먼트 크기)를 줄입니다.

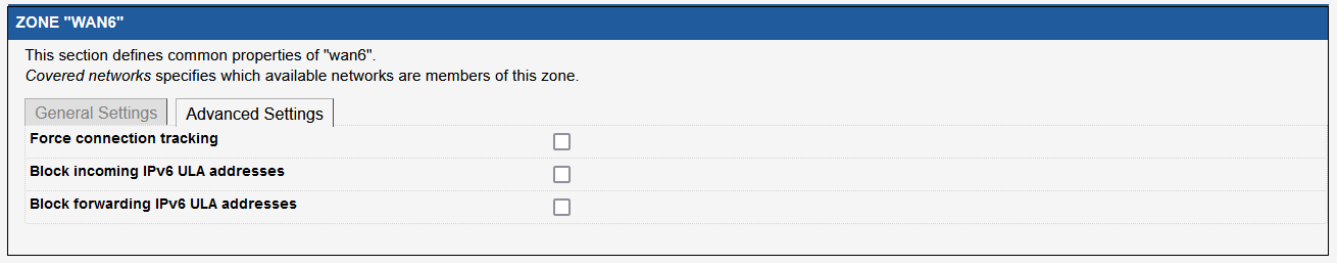
Default acceptance policy for local services:

이 zone 에서 로컬 서비스를 활성화/비활성화합니다. 방화벽 섹션에서 로컬 서비스를 제한하거나 열 수 있습니다.

Covered networks:

이 zone 에 포함되는 네트워크를 선택합니다.

Advanced Settings



Force connection tracking:

기본적으로 방화벽은 NAT/PAT(IP Masquerading)가 활성화되지 않은 경우 영역에 대한 연결 추적을 비활성화합니다. 연결 추적을 비활성화하면 라우팅 성능이 향상됩니다. 이 영역에서 연결 추적을 활성화하려면 이 옵션을 선택하십시오. 이를 필요로 하는 사용자 정의 버전의 펌웨어에서만 이 작업을 수행해야 합니다.

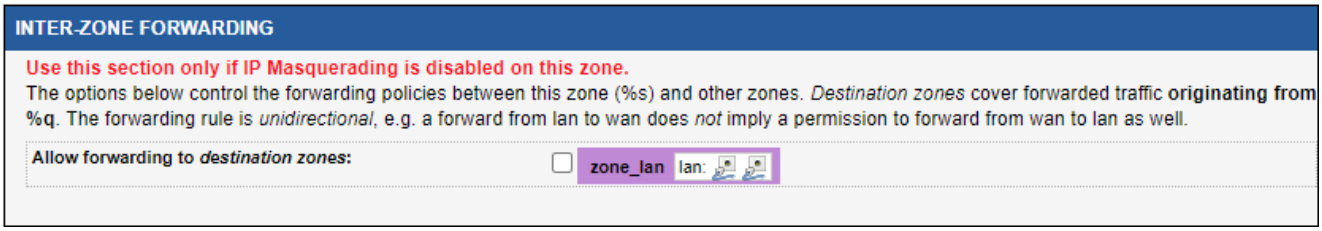
Block incoming IPv6 ULA addresses:

기본적으로 NAT/PAT(IP Masquerading)가 활성화되지 않은 경우 방화벽은 영역에 대한 IPv6 ULA 주소를 비활성화합니다.

Block forwarding IPv6 ULA addresses:

기본적으로 방화벽은 NAT/PAT(IP Masquerading)가 활성화되지 않은 경우 영역에 대한 IPv6 ULA 주소 전달을 비활성화합니다.

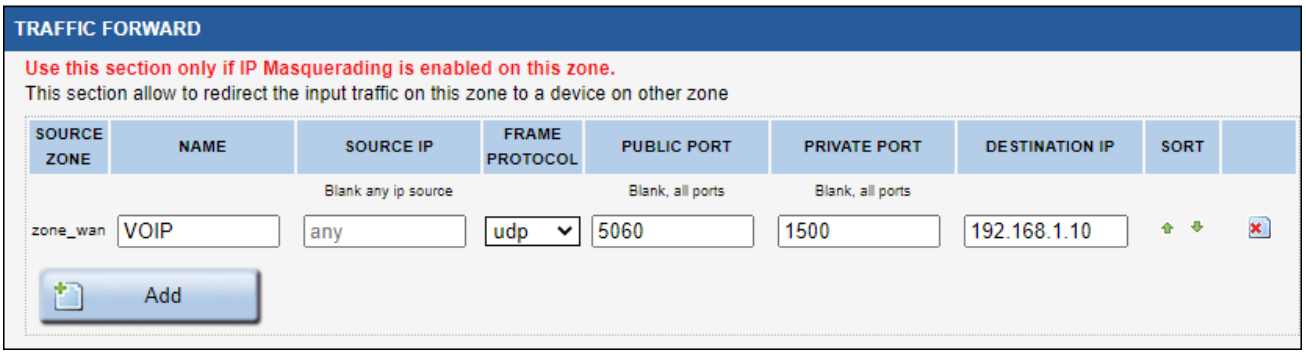
Inter-zone forwarding



이 섹션은 NAT/PAT(IP Masquerading)이 비활성화된 경우에만 사용됩니다.

선택된 zone 의 모든 트래픽이 제한 없이 전달되는 zone 을 선택합니다. 트래픽의 일부만 전달하려면 방화벽 섹션을 사용하세요.

Traffic forwarding



NAT/PAT(IP Masquerading)를 활성화할 때, 사설 영역으로 트래픽을 전달하려면 이 섹션을 사용하세요.

이 zone 에서 수신한, 소스 IP, 프레임 프로토콜 및 공용 대상 포트가 일치하는 각 프레임에 대해, 프레임의 대상 포트 및 대상 IP 주소가 지정된 대로 다시 작성됩니다.

Name:

규칙 이름을 입력하세요. 규칙에 기호 이름을 지정할 수 있습니다.

Source IP:

S 입력 프레임의 예상 소스 IP 를 설정합니다. 이 필드가 비어 있으면 모든 IP 가 일치합니다.

Frame Protocol:

예상되는 프로토콜 유형을 설정합니다. (UDP, TCP, TCP & UDP 또는 all)

Public port:

이 zone 에서 입력 프레임의 예상 대상 포트를 설정합니다. 단일 포트 또는 포트 범위를 지정할 수 있습니다. (포트 범위 지정 시 시작 포트와 끝 포트 사이에 대시 "-" 사용) 이 필드가 비어 있으면 모든 포트가 일치합니다.

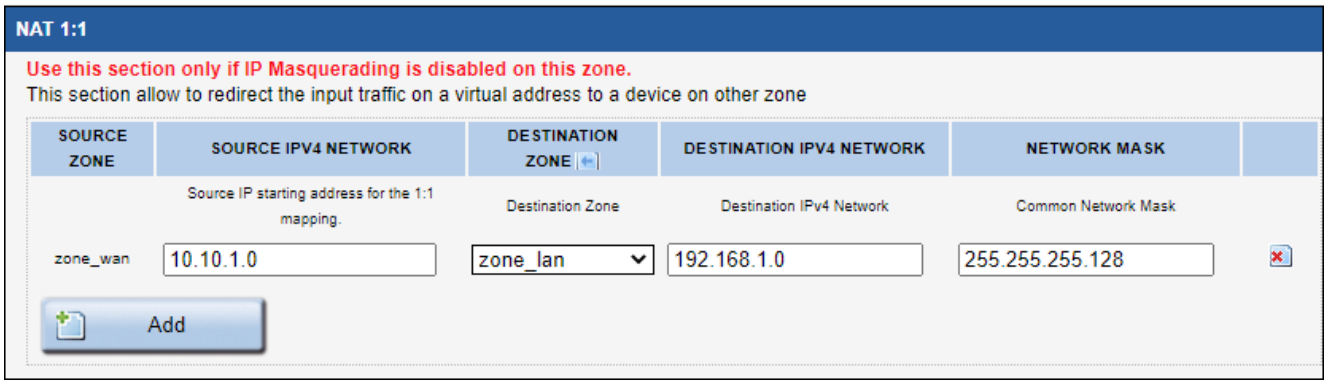
Private Port:

NAT/PAT 는 사설영역에 전송하기 전에, 원래 대상 포트를 프레임의 이 사설 포트로 대체합니다. 이 필드가 비어 있으면 포트(또는 포트 범위)는 변경되지 않습니다. 공용 포트 범위를 사용하는 경우 사설 포트는 동일 너비 포트 범위여야 합니다.

Destination IP:

NAT/PAT 는 사설영역에 전송하기 전에, 원래 대상 IP 주소를 프레임의 이 사설 IP 주소로 대체합니다. **이 필드는 비워 둘 수 없습니다**.

NAT 1:1



이 섹션을 사용하여, 소스 영역에서부터 정의된 대상 영역 네트워크로 트래픽을 전달하는 데 사용할, 가상 IPV4 네트워크를 정의합니다. NAT1:1 을 사용하려면 IP Masquerading 을 비활성화해야 합니다

Source IPV4 Network:

1:1 매핑에 사용되는 소스 가상 주소를 정의합니다.

Destination Zone:

대상 zone 을 여기에서 선택합니다.

Destination IPV4 Network:

물리적 대상 IPV4 네트워크를 정의합니다. 이 서브넷은 대상 영역에서 액세스 할 수 있어야 합니다.

Network Mask:

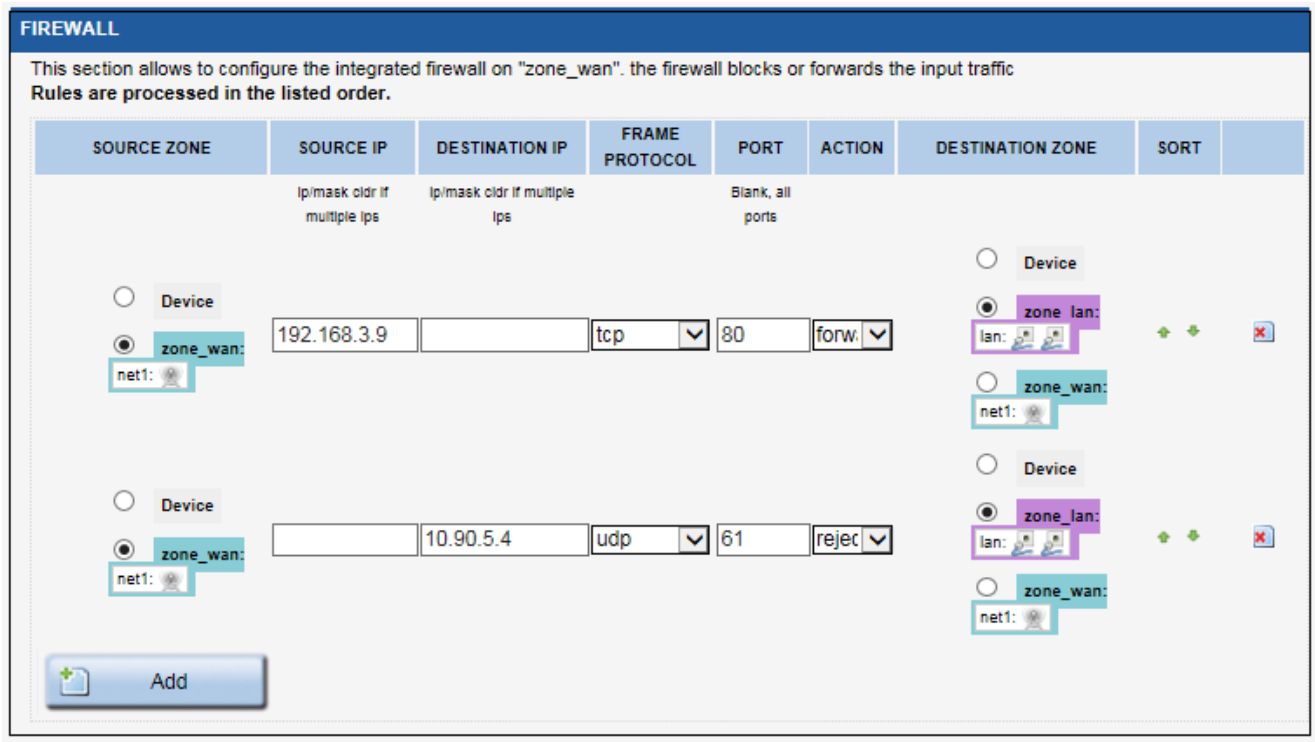
Network Mask 는 변환된 네트워크의 크기를 정의합니다:

255.255.255.255	⇨	1 translated IP addresses
255.255.255.192	⇨	64 translated IP addresses
255.255.255.128	⇨	128 translated IP addresses
255.255.255.0	⇨	256 translated IP addresses
255.255.0.0	⇨	65 536 translated IP addresses
255.0.0.0	⇨	16 777 216 translated IP addresses

원본 네트워크에서 대상 영역의 변환된 서브넷에 액세스하려면, 라우터를 기본 게이트웨이로 정의하거나, 라우터에 대한 고정 경로를 만들어야 합니다.

대상 네트워크에서 원본 네트워크로의 반환 경로도 같은 방식으로 정의해야 합니다. 이를 위해 IP 별칭 생성이 필요할 수 있습니다.

Firewall



이 섹션은 로컬 장치 또는 다른 영역에서 제공되는 서비스의 사용을 제한하거나 허용합니다.

Source IP:

필터링할 패킷의 소스 IP 주소입니다.

Destination IP:

필터링할 패킷의 대상 IP 주소입니다.

Frame protocol:

프로토콜 유형 (TCP, UDP, TCP & UDP, ICMP, GRE, all)

Port:

트래픽의 대상 포트입니다. 포트는 서비스를 식별합니다.

Action:

One of:

Forward : 대상 영역 또는 장치로 트래픽을 전달합니다.

Reject : 패킷을 삭제하고 트래픽 소스에 ICMP 메시지를 보냅니다.

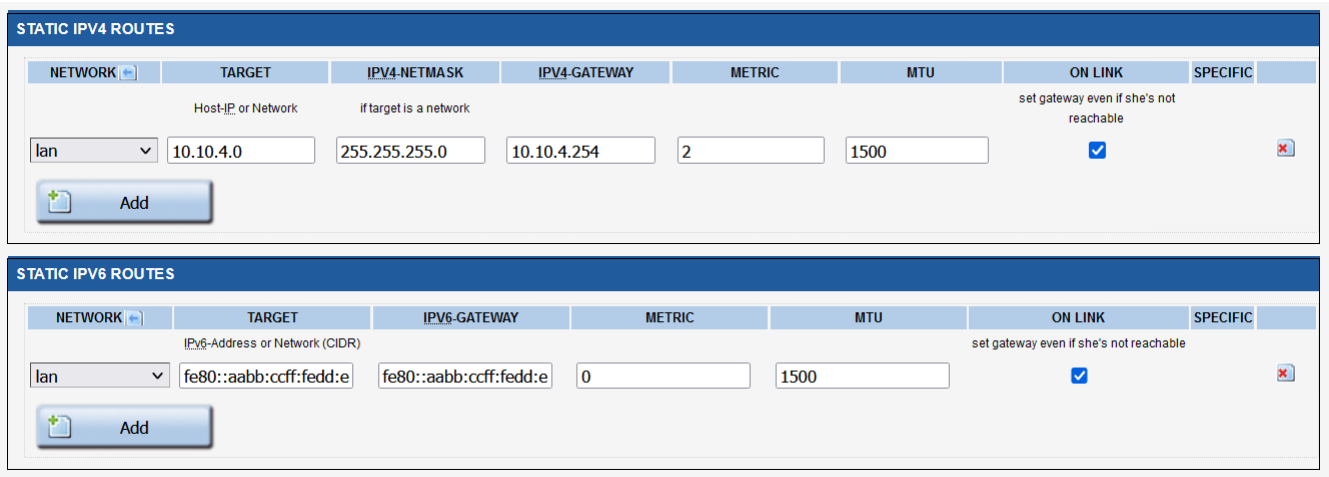
Drop : ICMP 메시지 없이 패킷을 삭제합니다.

Destination zone:

트래픽이 전달되는 영역입니다.

VI.1.6.2 Static routes

이 섹션에서는 장치에 고정 경로를 추가할 수 있습니다.



Target:

대상 호스트 또는 네트워크 IP 주소.

IPv4-netmask:

대상이 네트워크인 경우, 이 필드를 올바른 Netmask 로 설정해야 합니다.

대상이 호스트인 경우에는 이 필드를 공백으로 둘 수 있습니다.

Metric:

이 경로에 대한 메트릭을 설정합니다. 기본값인 64 를 사용하려면 비워두세요.

MTU:

이 경로의 MTU 를 설정합니다. 계산된 값을 사용하려면 비워두세요.

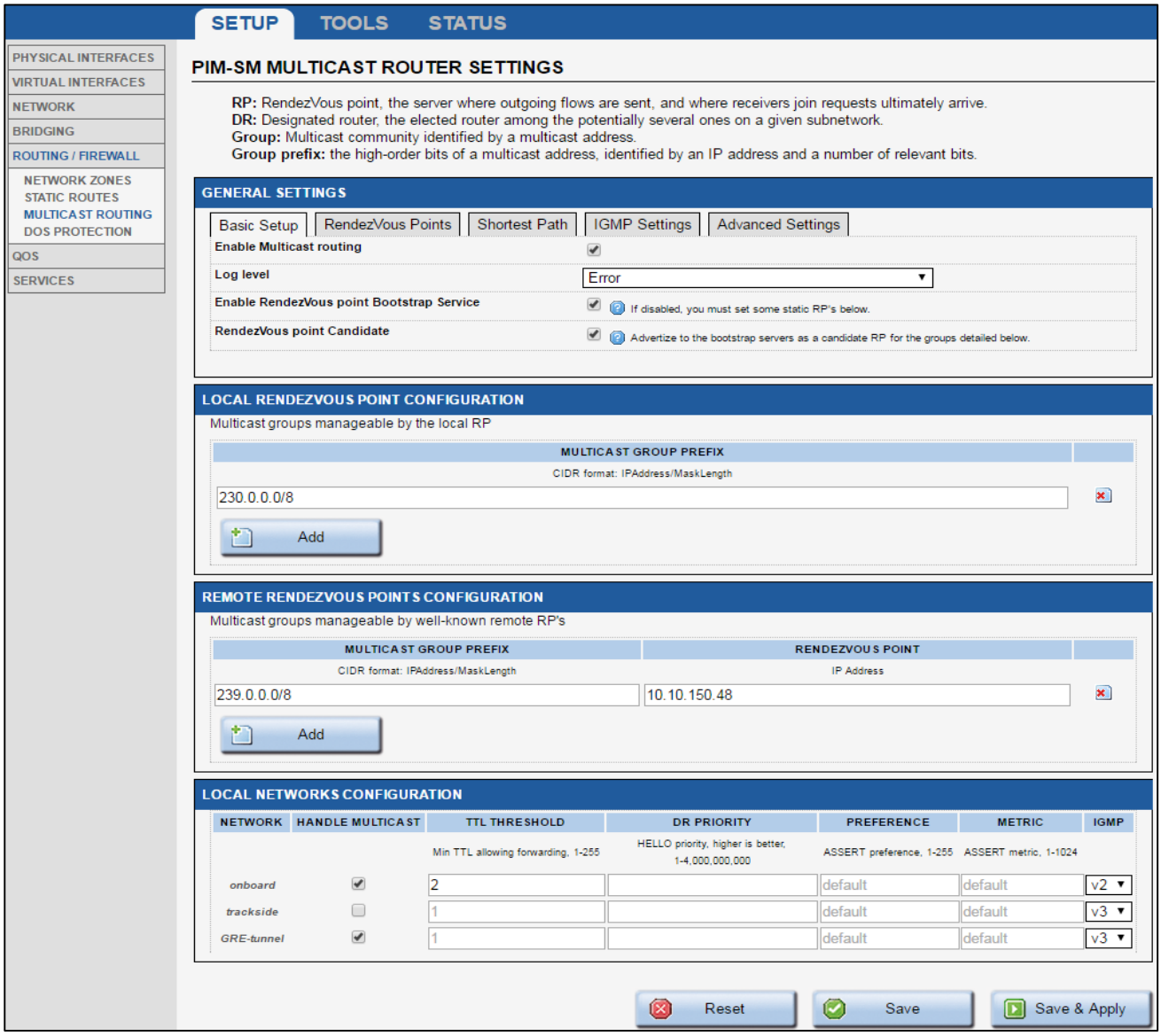
Specific:

이 컬럼은 네트워크 서비스에서 자동으로 생성되는 고정 경로를 나타냅니다.

경고: SPECIFIC 으로 표시된 경로를 수정/삭제하면, 해당 서비스가 제대로 작동하지 않을 수 있습니다.

VI.1.6.3 Multicast routing

이 페이지에서 PIM-SM 멀티캐스트 라우터를 구성합니다.



General settings 은 다양한 라우터 옵션을 설정합니다.

Local rendezvous points configuration 은 이 장치가 랑데부 포인트로 처리할 멀티캐스트 그룹 목록을 설정합니다.

Remote rendezvous points configuration 은 그룹을 원격 랑데부 포인트 주소에 연결하므로 이 연결을 제공하기 위해 이 장치에 BSR 이 필요하지 않습니다.

Local networks configuration 은 멀티캐스트 라우팅에 사용할 수 있는 로컬 네트워크 인터페이스가 나열됩니다. **setup/network overview** 에 있는 목록의 미러입니다. 일부 인터페이스를 비활성화하거나 다양한 성능 세부 정보를 변경할 수 있습니다.

General settings Basic setup tab

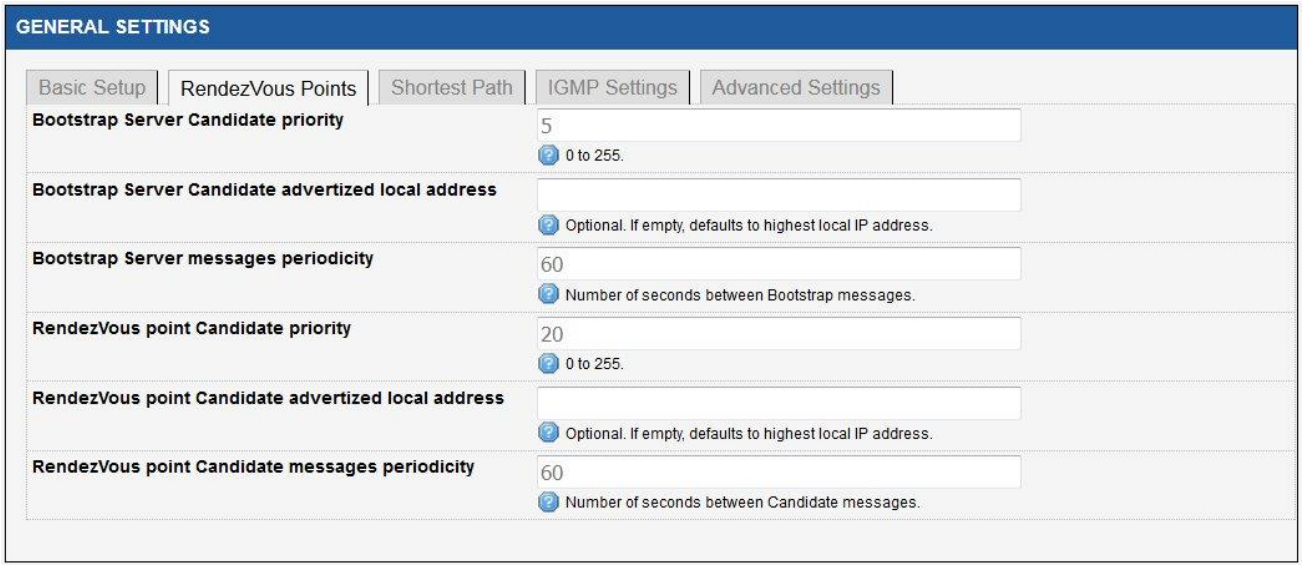
Enable multicast routing:
멀티캐스트 라우터 및 모든 종속 기능을 활성화하려면 선택하세요.

Log level:
시스템 로그에 전송될 메시지의 양을 지정합니다. 메시지를 처리하려면 시스템 로그를 최소한 동일 레벨로 설정해야 합니다.

Enable Bootstrap Service:
이 장치를 BSR 후보로 허용하려면 체크합니다.

RendezVous Point candidate:
이 장치가 **local rendezvous point configuration** 섹션에 나열된 그룹의 RP 로 되도록 하려면 체크합니다.

Rendezvous Points tab



BSR(BootStrap Server) candidate priority:
후보가 여러 명일 경우 선정 과정에 우선 순위를 부여합니다.

BSR(BootStrap Server) local address:
라우터는 멀티 홈이며 여러 IP 주소를 가집니다. 이것은 BSR 프로토콜의 목적을 위해 사용될 IP 주소입니다. 기본값(활성화 인터페이스의 가장 높은 IP 주소)을 사용하려면 공백으로 둡니다.

BSR(BootStrap Server) message periodicity:
'BS_Period' 라고도 합니다. 멀티캐스트 그룹과 해당 RP 간의 연결은 라우터에 캐시됩니다. 이 캐시의 지속 시간은 일반적으로 RP 메시지 주기성의 2.5 배입니다. (3 회 동안 2 개의 메시지가 손실될 수 있음) 그러나 이 기간이 'BS_Period'보다 작으면 RFC5059 제약 조건을 준수하기 위해 2.5 x [BS_Period]로 조정됩니다.

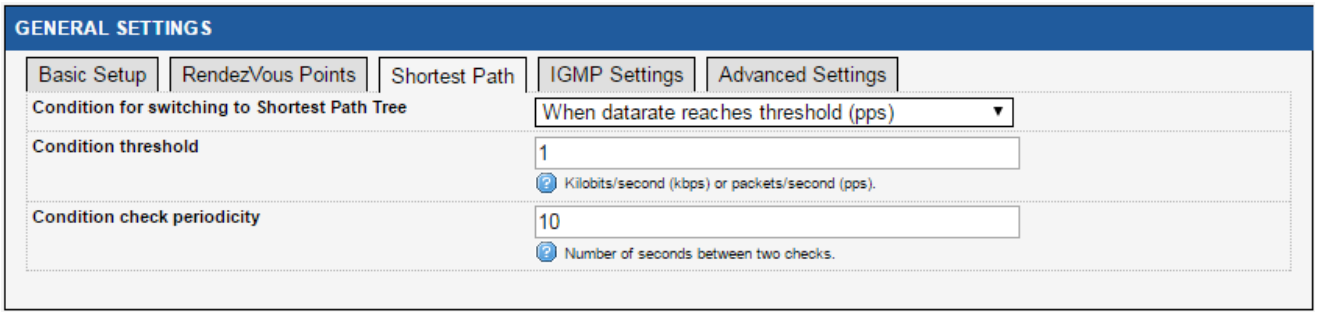
RP(RendezVous Point) candidate priority:
후보가 여러 명일 경우 선정 과정에 우선 순위를 부여합니다. (우선순위가 높을수록 순위가 높다.)

RP(RendezVous Point) local address:
라우터는 멀티 홈이며 여러 IP 주소를 가집니다. 이것은 BSR 프로토콜에서 RP 선택에 사용될 IP 주소입니다. 기본값(활성화 인터페이스의 가장 높은 IP 주소)을 사용하려면 공백으로 둡니다.

RP(RendezVous Point) candidate messages periodicity:

두 개의 연속적인 **RP-Cand** 및 PIM 메시지 사이의 지속 기간

Shortest path tab



Condition for switching:

처리량이 구성된 값을 초과하면 경로를 RP 트래버셜에서 최단 경로로 전환할 수 있습니다. 트리거 유형을 선택하면 "Never"(전환 없음), 초당 패킷 수 또는 초당 비트 수로 표현할 수 있습니다.

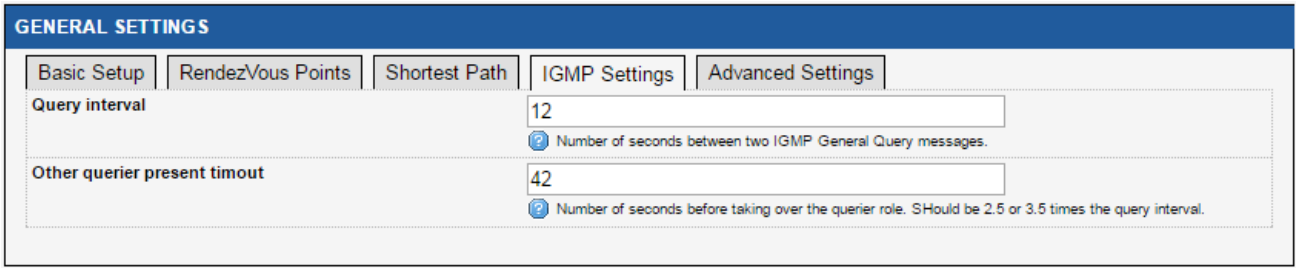
Condition threshold:

처리량에 따라 SPT 로의 전환이 트리거됩니다. 단위는 위의 항목 선택에 따라 다릅니다.

Condition check periodicity:

트리거 조건이 참이 되는 시간과, SPT 스위치가 시작되는 시간 사이의 최대 지연 정도입니다.

IGMP settings tab



Condition threshold:

SPT 로의 전환을 트리거합니다. 단위는 위의 선택에 따라 다릅니다.

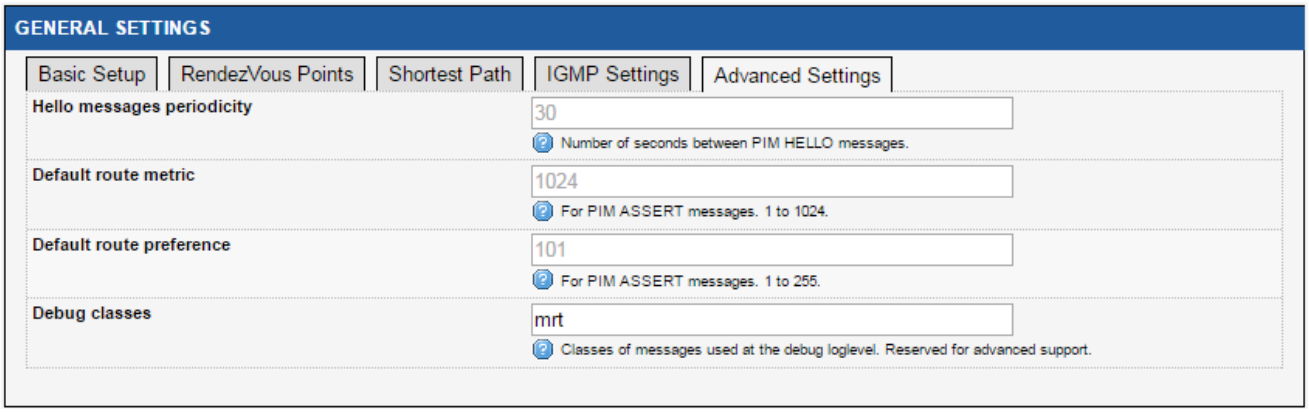
Query interval:

두 개의 연속적인 IGMP 쿼리 사이의 지연 정도입니다.

Other querier present timeout:

이전 쿼리가 다운되었다는 가정 하에, 네트워크 인터페이스에서 마지막 IGMP 쿼리가 나타난 후, 이 라우터가 이 인터페이스에서 IGMP 쿼리 역할을 인수하기 전까지의 지연 정도입니다.

Advanced settings tab



Hello periodicity:

두 개의 연속적인 "HELLO" PIM 메시지(PIM 라우터의 존재 및 우선 순위 알림) 사이의 지속 시간입니다.

Default route metric:

ASSERT 가 전송되는 네트워크 인터페이스에 대한 메트릭이 설정되지 않은 경우, ASSERT 메시지에서 전송되는 경로 메트릭 값입니다.

Default route preference:

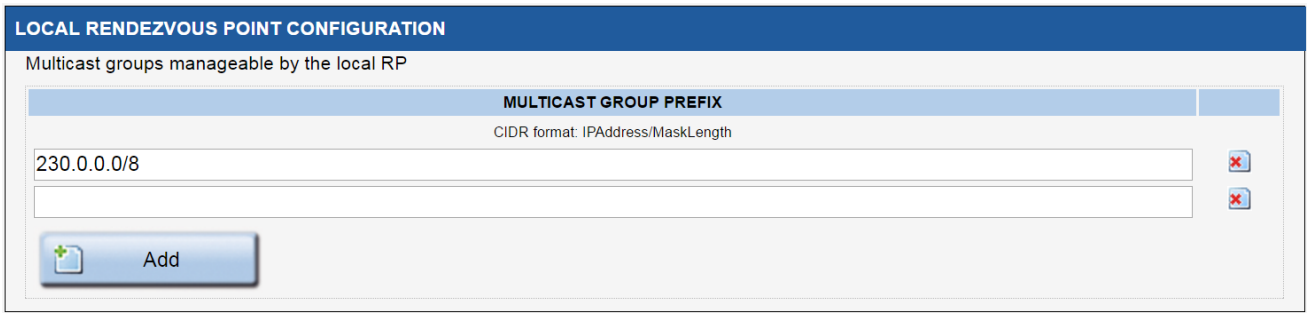
ASSERT 가 전송되는 네트워크 인터페이스에 대해 기본 설정이 지정되지 않은 경우, ASSERT 메시지에서 전송되는 기본 설정 메트릭 값입니다.

Debug classes:

로그 수준이 "Debug"로 설정된 경우, 이 쉼표로 구분된 필드는 로그로 전송된 디버그 메시지의 클래스를 나타냅니다. 이 필드는 고급 기술 지원을 위해 제한되어 있습니다.

Local rendezvous point configuration

여기에 이 라우터가 랑데부 포인트 역할을 하는 그룹 목록을 입력합니다.



ADD button:

새 그룹을 추가하려면 클릭하세요.

Red cross buttons:

그룹을 삭제하려면 클릭하세요.

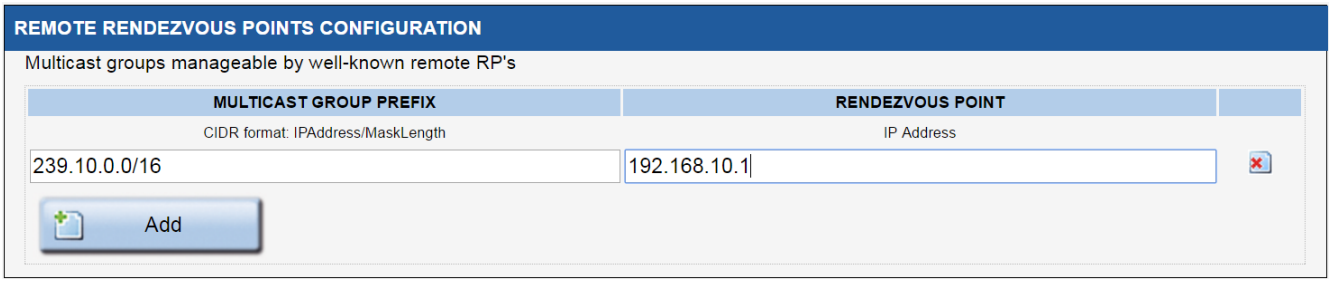
Multicast group prefix:

각 줄에 그룹 IP 주소의 접두사(공통 시작 부분)와 "/", 접두사의 유효 비트 수를 기입합니다.

이 라우터는 목록의 접두사 중 하나로 시작하는 모든 그룹을 처리합니다.

Remote rendezvous points configuration

원격 RP 로 처리되지만 BSR 을 사용할 수 없는 그룹이 나열됩니다. BSR 은 여전히 다른 그룹에 사용됩니다.



ADD button:
새 그룹을 추가하려면 클릭하세요.

Red cross buttons:
그룹을 삭제하려면 클릭하세요.

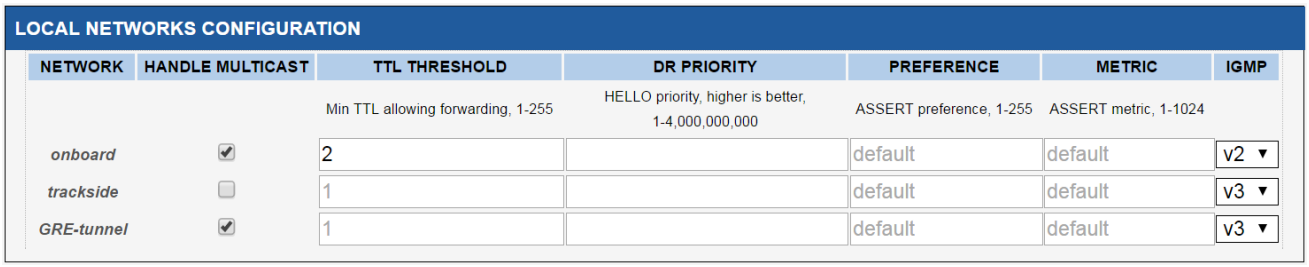
Multicast group prefix:
그룹 IP 주소의 공통 시작, "/" 및 접두사의 유효 비트 수가 뒤에 옵니다.

Rendezvous point:
이 그룹 블록을 관리하는 랑데부 포인트의 주소를 입력하세요.

이 라우터는 시작 시 목록을 미리 로드하고, 이러한 연결을 사용하여 지정된 그룹에 대한 원격 RP 를 찾습니다. RP 선정을 위해 이러한 고정 연결의 우선 순위는 1(가장 높음)입니다.

Local networks configuration

여기에서 각 네트워크 인터페이스와 관련된 매개변수를 제공합니다.



Network: 네트워크 인터페이스 이름.

Handle multicast:
PIM 라우터가 이 네트워크를 무시할지 여부.

TTL threshold:
TTL 이 낮은 발신 멀티캐스트 데이터를 삭제합니다.

DR priority:
이 네트워크에서 지정 라우터 선택을 위한 이 라우터의 우선 순위.

Preference:
ASSERT 메시지로 전송된 기본 설정 메트릭 값입니다. **advanced settings** 탭에서 설정한 값이 기본값입니다.

Metric:

ASSERT 메시지로 전송된 경로 메트릭 값이 라우터와 대상 RP 사이의 거리를 나타냅니다. **advanced settings** 탭에서 설정한 값으로 기본 설정됩니다.

IGMP: IGMPv2 호환성을 적용하려면 v2 로 설정하십시오.

VI.1.6.4 Denial Of Service (DOS) protection

Enable SYN-flood protection:

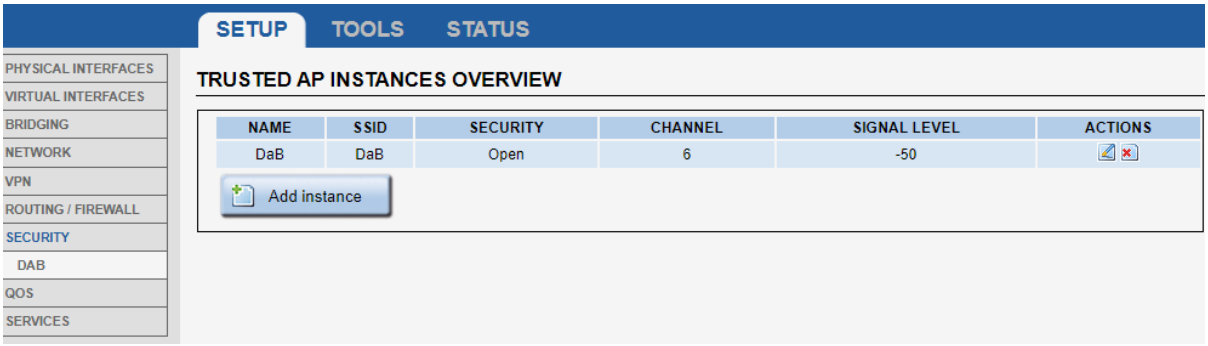
The syn-flood 공격은 반쯤 오픈된 연결을 많이 생성하여, 피해자의 리소스를 취하는 것입니다. http://en.wikipedia.org/wiki/SYN_flood 에 자세히 설명되어 있습니다.

Drop invalid packets:

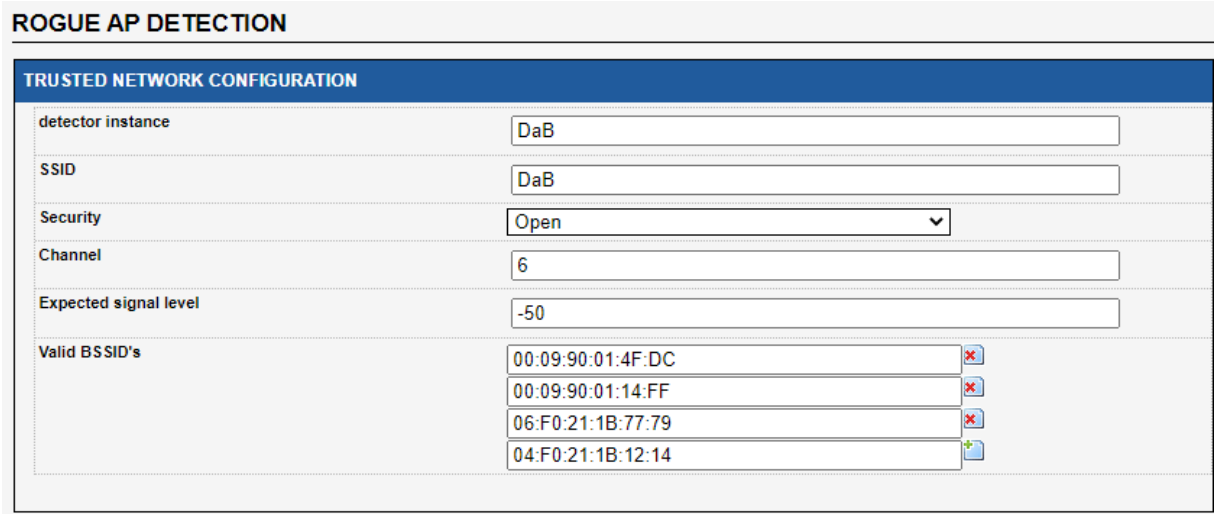
유효하지 않은 프레임 또는 활성화된 연결이 없는 프레임을 삭제합니다.

VI.1.7 Security

이 페이지에서는 Rogue AP Detector 개체를 생성할 수 있습니다.



새 Rogue AP 감지 개체를 생성하려면 **Add instance** 를 클릭하세요. 이렇게 하면 Rogue AP 감지 구성 페이지가 열립니다.



Detector Instance

Rogue AP Detector 개체 이름을 기입합니다.

SSID

모니터링 할 SSID 를 기입합니다.

Security

SSID 에 적용된 보안 모드를 선택합니다.

Channel

모니터링 할 채널을 기입합니다.

Expected signal level

모니터링 무선 카드가 측정해야 하는 최소 신호 수준을 기입합니다.

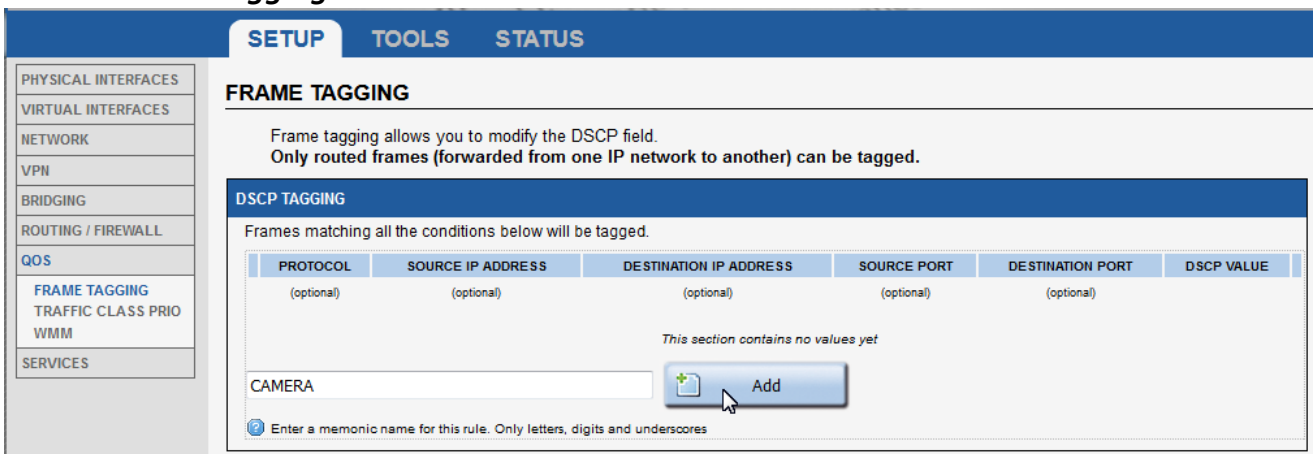
Valid BSSID's

이 SSID 를 내보내도록 허용된, 모든 AP 의 BSSID(MAC 주소) 목록입니다.

이 기능에 대한 자세한 내용은 Rogue AP detector 섹션을 참조하세요.

VI.1.8 QOS

VI.1.8.1 Frame tagging



DSCP 태그는 다음 기준과 일치하는 각 수신 프레임(모든 인터페이스에서)에 적용됩니다:

PROTOCOL

IP 프로토콜 유형입니다. TCP, UDP 또는 ICMP 를 선택합니다.

SOURCE IP ADDRESS

수신 프레임의 소스 IP 주소입니다. Wildcard 는 허용되지 않습니다.

DESTINATION IP ADDRESS

수신 프레임의 목적지 IP 주소입니다. Wildcard 는 허용되지 않습니다.

SOURCE PORT

수신 프레임의 소스 포트. 이 매개변수는 TCP 및 UDP 프로토콜에만 유효합니다. 단일 포트 또는 포트 범위를 지정할 수 있습니다. (시작 및 끝 포트 사이에 대시 "-" 사용)

DESTINATION PORT

수신 프레임의 목적지 포트. 이 매개변수는 TCP 및 UDP 프로토콜에만 유효합니다. 단일 포트 또는 포트 범위를 지정할 수 있습니다. (시작 및 끝 포트 사이에 대시 "-" 사용)

DSCP VALUE

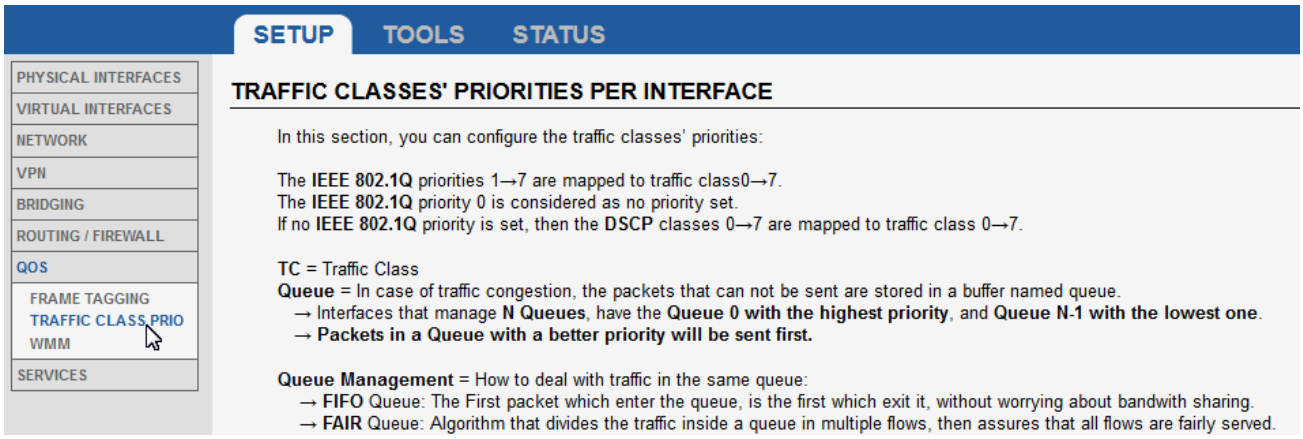
IP 프레임의 DSCP 필드(6 비트)에 기록할 값입니다.

하기 표를 사용하여 WMM 유효 태그를 설정할 수 있습니다:

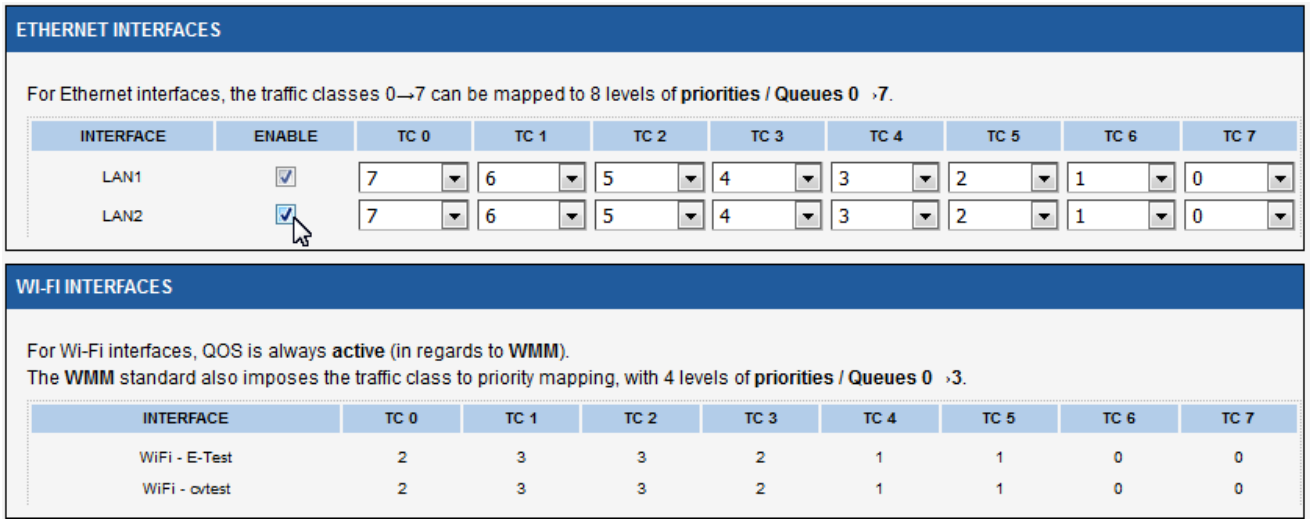
WMM valid tags	
DSCP field value	***WMM Queue***
8 or 16	Background (BK)
0 or 24	Best effort (BE)
32 or 40	Video (VI)
48 or 56	Voice (VO)

VI.1.8.2 Traffic Class Priorities

이 메뉴에서는 QoS(Quality of Service: 통신 서비스 품질) 트래픽 클래스 관리 구성을 설정할 수 있습니다.

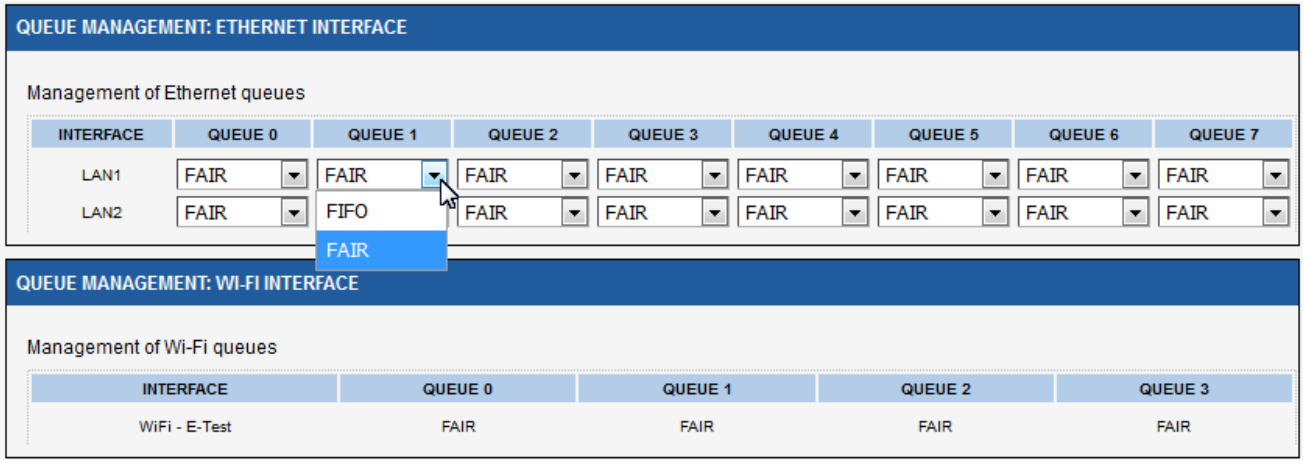


Traffic Class to queue mapping



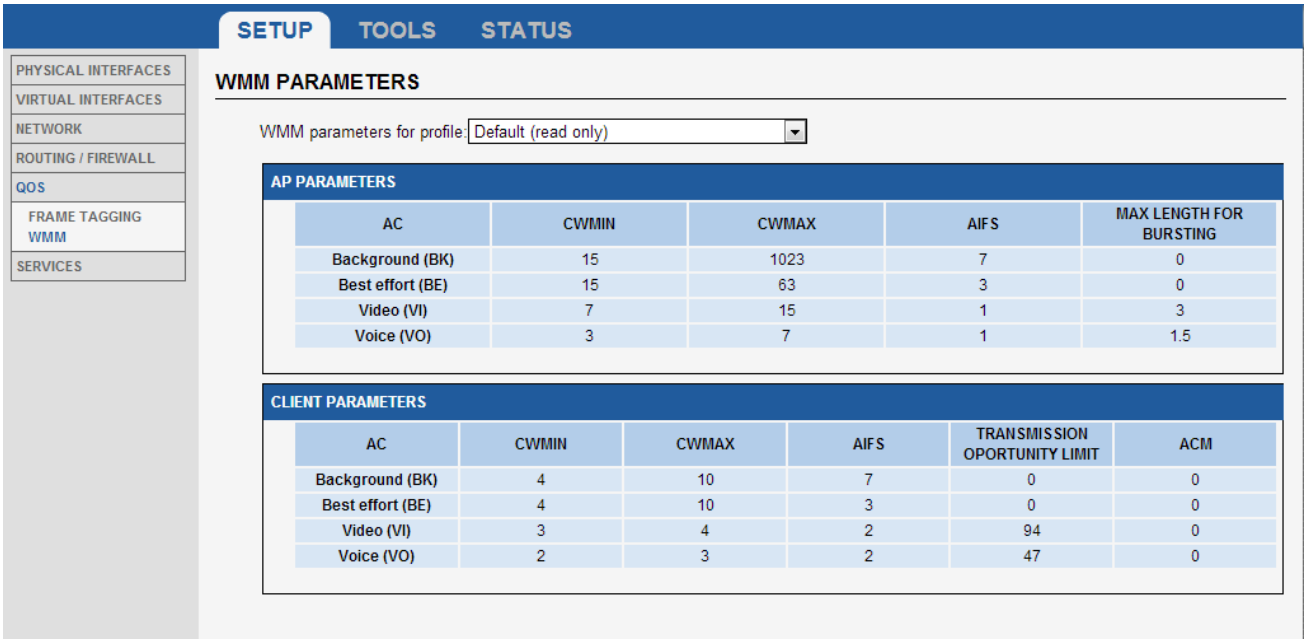
트래픽 클래스를 지정된 queue(대기열)/priority(우선 순위)에 매핑하려면, 각 TCx 트래픽 클래스에 대한 queue 번호를 선택합니다. Wi-Fi 인터페이스의 경우 WMM 이 항상 활성 상태이며, queue 매핑이 적용되며 변경할 수 없습니다

Queue management



queue 관리 유형(FIFO or FAIR)을 선택하려면, 각 QUEUE x 에 대한 대기열 유형을 선택하세요.

VI.1.8.3 WMM



이 페이지에는 선택한 프로필에 대한 WMM 매개변수가 표시됩니다. WMM(a.k.a. WME)은 항상 사용할 수 있습니다.

WMM parameters for profile

이 리스트에서 **User** 또는 **Default** QoS 매개변수를 선택할 수 있습니다.

기본 QoS 매개변수는 참조용으로 제공되며 수정할 수 없습니다.

AP PARAMETERS:

이 테이블에서는 4 개의 AP Tx queue(BK, BE, VI, VO)에 대한 WMM 매개변수를 변경할 수 있습니다.

CWMIN

최소 윈도우 크기 (시간 슬롯의 수로 표시).

허용값은 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023

CWMAX

최대 윈도우 크기 (시간 슬롯의 수로 표시)

허용값은 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023.

AIFS

현재 queue 크기(시간 슬롯 수로 표시)에 대한 조정 프레임 간격 값. 허용값은 0~255

MAX LENGTH FOR BURSTING

최대 버스트 길이(0.1 밀리 초 단위로 표시)

허용값은 0~100000ms

CLIENT Parameters:

이 테이블을 사용하면 관리 프레임에서 CLIENT 가 보낸 WMM 매개변수를 변경할 수 있습니다.

CWMIN

최소 윈도우 크기(시간 슬롯의 수로 표시)

허용값은 0~12

CWMAX

최대 윈도우 크기 (시간 슬롯의 수로 표시)

허용값은 0~12

AIFS:

현재 queue 크기 (시간 슬롯 수로 표시)에 대한 조정 프레임 간격 값

허용값은 1~255

TXOP_LIMIT:

tx 기회제한기간을 정의합니다. (시간 슬롯의 수로 표시)

허용값은 0~65535

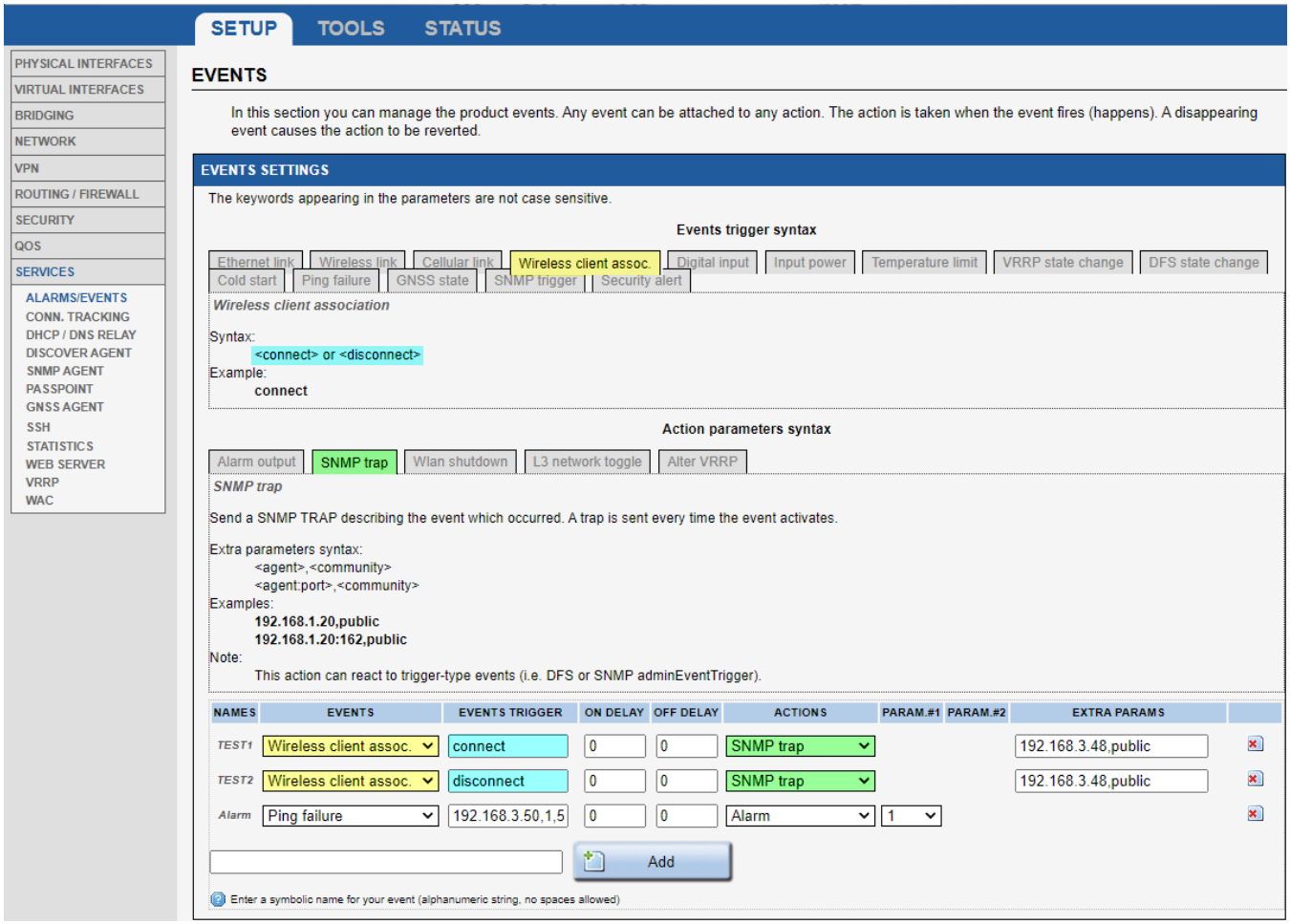
ACM:

현재 queue 에 허용값을 정의합니다. 허용값은 0 과 1.

VI.1.9 Services

VI.1.9.1 Alarms / events

해당 탭을 통해 다양한 이벤트 및 트리거를 설정할 수 있습니다. **Add** 버튼을 클릭하여 여러 개의 트리거를 생성하고, 이름을 지정할 수 있습니다. 트리거를 생성한 후 이벤트 소스 및 관련 설정을 할 수 있습니다. 이벤트 소스와 작업에는 유형에 따라 추가 매개변수가 필요할 수 있습니다. 또한 상단에 이벤트 테이블에 대한 도움말 요약이 표시됩니다.



이벤트의 상징적인 이름을 입력하고 추가 버튼을 클릭하여 새 항목을 추가하세요.

Events:

Ethernet link : 이더넷이 연결되면 활성화 됩니다.

Wireless link (in Access Point mode): Clinet 가 AccessPoint 에 연결되면 활성화 됩니다.

Wireless link (in Client mode): 브리지가 하나의 액세스 포인트에 연결되면 활성화됩니다.

Cellular link (LTE 지원 제품): Cellular 링크가 연결되면 활성화 됩니다.

Wireless client assoc: 해당 이벤트는 오직 **SNMP trap** 기능만 지원됩니다. Client 가 AccessPoint 에 연결되거나 해제될 때 알림을 보냅니다.

Digital input (digital input 지원 제품): 값이 1 이 될 경우 디지털 입력이 활성화 됩니다. Airbox 와 같은 일부 제품에는 여러 개의 디지털 입력이 있습니다.

Input Power (전원이 2 개인 제품): 전원이 인가되면 활성화 됩니다.

Temperature limit: 온도가 트리거를 초과하면 이벤트가 활성화 됩니다.

VRRP state change: VRRP 상태가 변경되거나 종료되면 이벤트가 활성화 됩니다.

DFS state change: DFS 상태가 변경되면 이벤트가 활성화 됩니다.

Cold start: 제품의 부팅이 완료되면 이벤트가 활성화 됩니다.

Pinger: ICMP ECHO (ping)요청은 정기적으로 원격 호스트로 전송됩니다. 연속적으로 여러 시간 동안 ICMP ECHO 의 응답이 없을 경우 이벤트가 활성화 됩니다.

GNSS state (LTE 지원 제품): GNSS 위치가 안정화 되면 이벤트가 트리거 되며 위치 정보가 손실될 경우 비활성화 됩니다.

SNMP trigger: 이벤트는 다음 SNMP OIDs 에 의해 활성화 됩니다:

adminEventEnable 는 지정된 경보를 활성화 합니다

adminEventDisable 는 지정된 경보를 비활성화 합니다

adminEventTrigger 원샷 경보를 활성화 합니다

지정된 알람의 이름은 event 를 생성할 때 지정한 이름입니다. ("NAMES" 열).

Security alert: 보안 위협이 탐지될 경우 사용자에게 전달합니다. 해당 기능은 **Rogue AP detection** 만 지원됩니다. 해당 이벤트는 비활성화 되지 않으며 필요할 때 마다 자동으로 활성화 됩니다.

제품 모델에 따라 일부 이벤트 소스는 사용할 수 없음으로 표시될 수 있습니다.

사용할 수 없음 이벤트 소스로 생성된 이벤트/알람은 트리거되지 않습니다.

Actions:

Alarm output: Airbox 와 같은 일부 제품에는 알람으로 프로그래밍할 수 있는 여러 디지털 출력이 있습니다. 트리거되면 제품 빠른 설치 가이드에 지정된 대로 알람 접점이 활성화됩니다..

SNMP: SNMP 트랩 작업이 트리거되면 지정된 커뮤니티를 사용하여 지정된 관리자 주소로 관련 트랩을 보냅니다.

Wlan shutdown: **Wlan shutdown** 이벤트가 활성화 되면 무선 인터페이스가 종료됩니다.

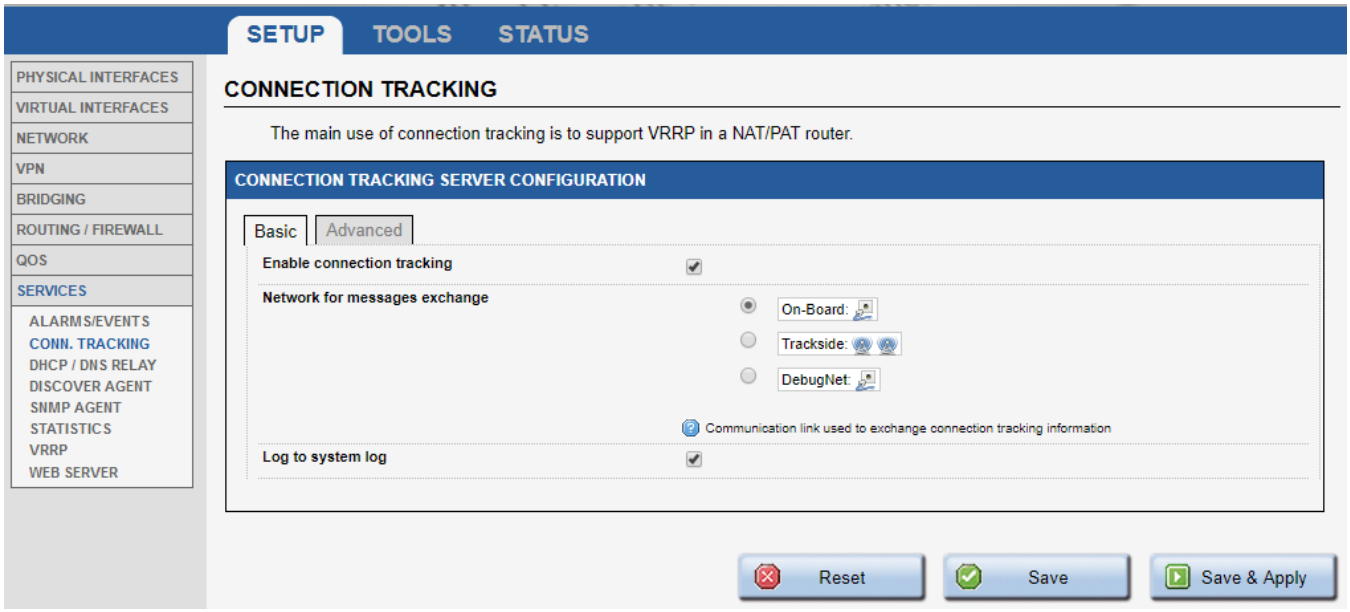
L3 network toggle: 지정된 네트워크를 활성화 또는 비활성화 합니다.

Alter VRRP: VRRP 그룹의 현재 우선 순위에 오프셋 설정을 적용하여 VRRP 그룹의 우선 순위를 변경할 수 있으며 마스터에서 백업으로 전환될 수 있습니다. 원칙적으로 SNMP 트리거에 의해 트리거됩니다.

VI.1.9.2 Connection tracking

해당 페이지를 통해 연결 추적 및 복제 기능을 활성화 할 수 있습니다.

VRRP 설정 페이지에서 연결 추적이 필요한 경우 해당 페이지에서 설정해야 합니다.



Basic tab

Enable connection tracking:

체크박스 활성화 시 연결 복제 기능을 활성화 합니다.

Network for messages exchange:

백업 라우터에 연결 정보를 보낼 인터페이스입니다. VRRP 에서 사용되는 서브넷 또는 전용 네트워크를 사용할 수 있습니다. 해당 링크는 무선 링크보다 유선 링크가 선호됩니다.

Log to system log:

이벤트 메시지는 시스템 로그로 전송됩니다.

Advanced tab

Multicast IPv4 address:

연결 복제 메시지를 보내는 데 사용되는 멀티캐스트 대상 주소입니다. 다른 사용자가 동일한 멀티캐스트 주소를 사용하는 경우 변경할 수 있습니다.

Conntrack group:

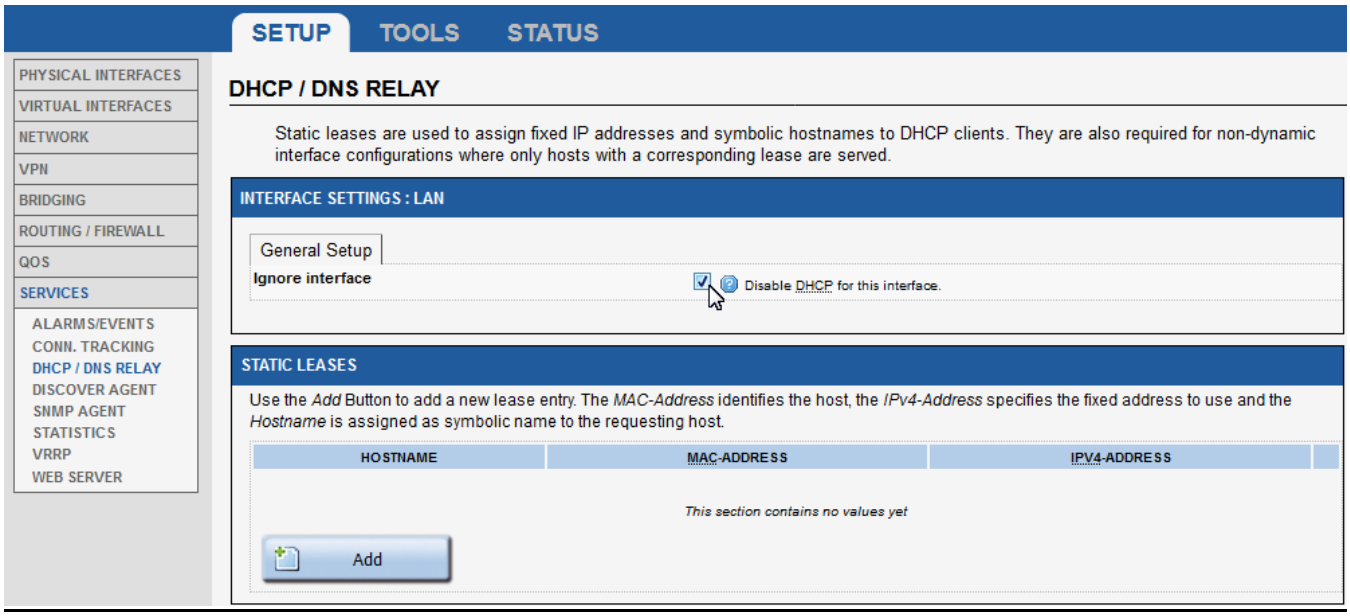
복제 서비스는 conntrack 이라는 표준 프로토콜을 사용합니다. 동일한 서브넷에 여러 인스턴스가 있을 경우 "group number" 를 지정하여 백업 메시지에 태그를 지정할 수 있습니다.

Process priority:

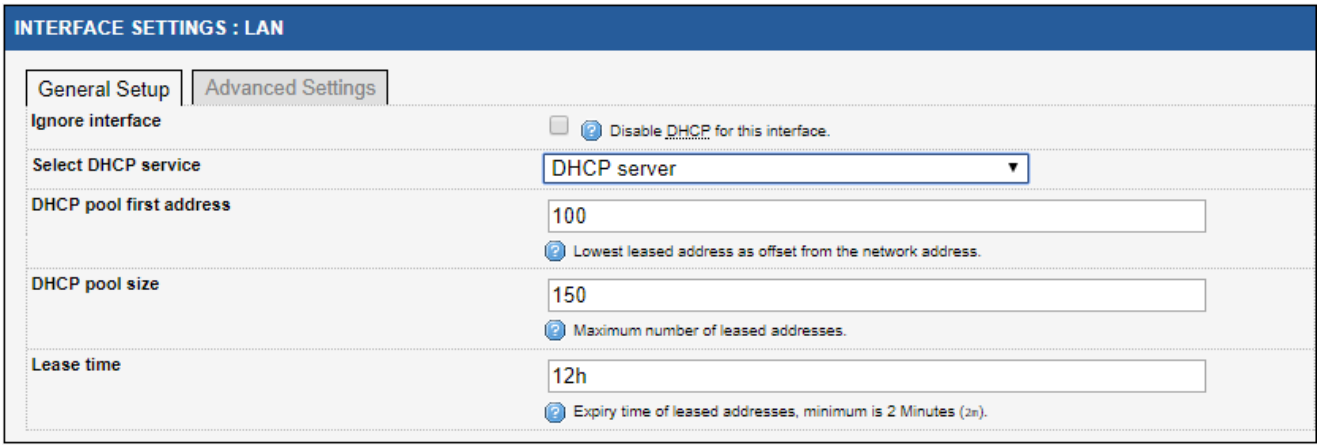
우선 순위가 높을수록 복제 속도가 빨라지지만 복제 전용 네트워크 부하도 높아집니다. 또한 많은 연결이 있는 높은 우선 순위는 로밍 지연에 악영향을 미칠 수 있습니다.

VI.1.9.3 DHCP/DNS RELAY

DHCP 서버 및 DHCP 릴레이를 활성화 하려면 **Ignore Interface** 의 체크 박스를 비활성화 해야 합니다:



Interface settings: DHCP 서버 General Setup:



Select DHCP service:

DHCP 서버 또는 DHCP 릴레이를 선택할 수 있습니다. (기본값 : DHCP server)

DHCP pool first address:

DHCP 서버가 할당 가능한 IP 주소의 범위를 정의합니다. 이 범위는 네트워크 주소를 기준으로 상대적인 위치를 나타내며, 첫 번째 IP 주소는 그 위치에서의 첫 번째 주소를 의미합니다.

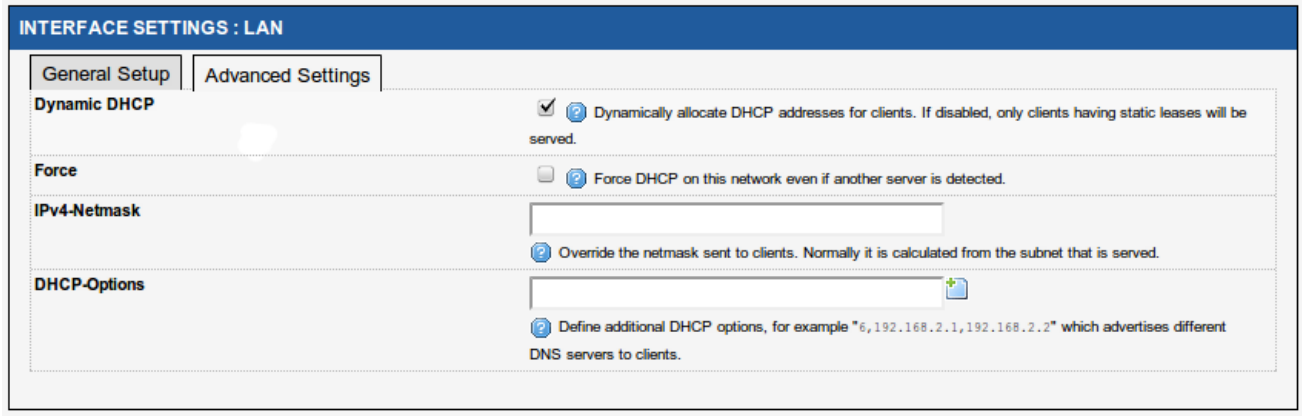
DHCP pool size:

IP 주소의 최대 수.

Lease time:

Client 의 지정된 IP 주소가 유지되는 시간. 해당 시간 이후의 Client 는 재갱신됩니다.

Interface settings: DHCP Server Advanced Settings:



Dynamic DHCP:

해당 옵션을 선택하지 않을 경우 **static leases** 만 승인됩니다.

Force:

기본적으로 네트워크에 다른 DHCP 서버가 있는 것을 감지하면 DHCP 서비스가 시작되지 않습니다. 해당 옵션을 선택하면 DHCP 서버는 시작하기 전에 다른 서버의 존재를 확인하지 않습니다.

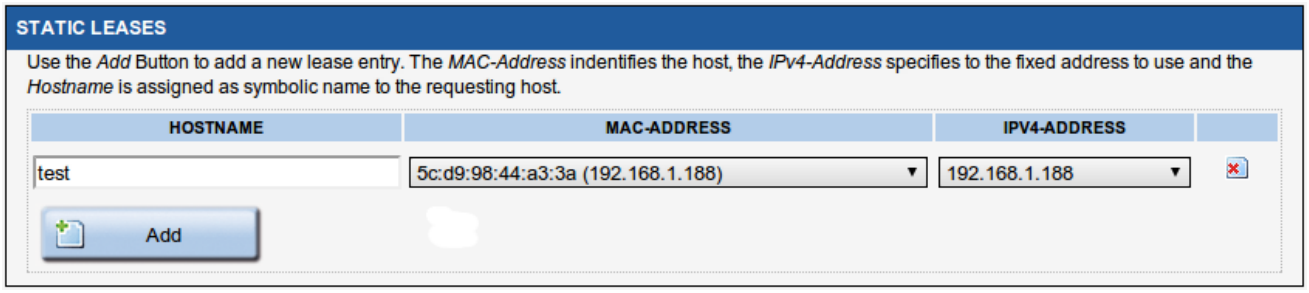
Ipv4-Netmask:

해당 옵션을 통해 DHCP 클라이언트로 전송된 기본 넷마스크 값을 설정할 수 있습니다.

DHCP-Options:

해당 필드에서는 추가 DHCP 옵션을 설정할 수 있습니다 (따옴표 " 로 묶음). 명령어는 옵션 자체에 따라 달라집니다. DHCP 옵션에 대한 자세한 내용은 DHCP RFC 를 참조하세요.

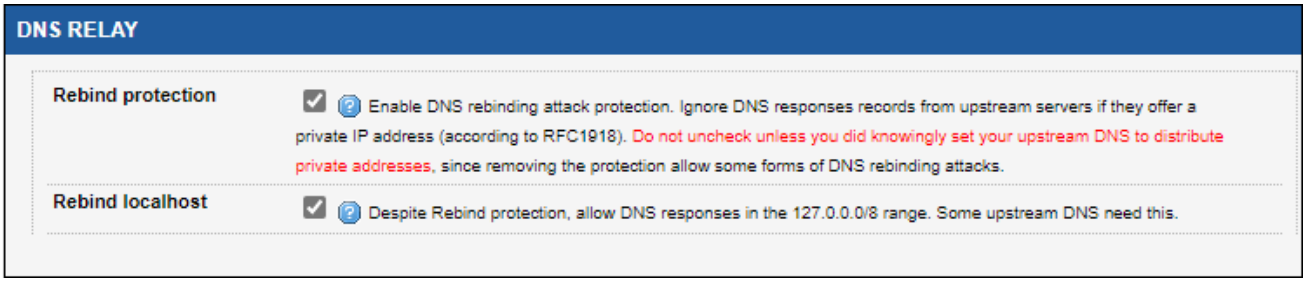
STATIC LEASES:



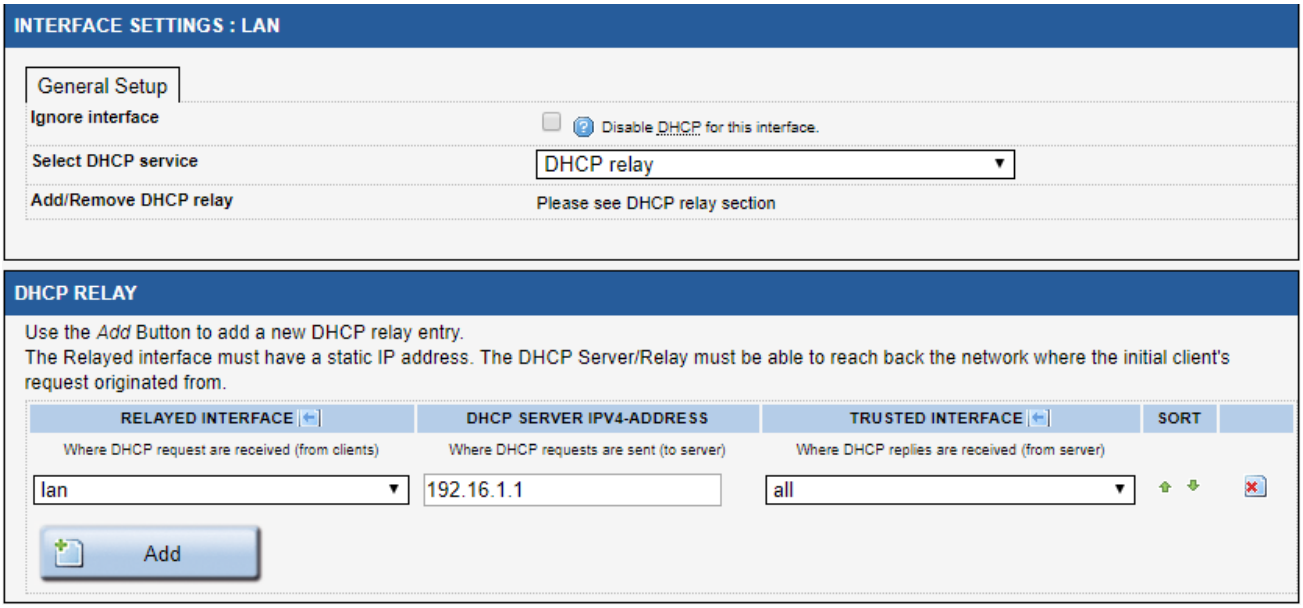
해당 옵션을 사용하면 지정된 클라이언트의 MAC 주소를 입력하여 미리 IP 를 지정할 수 있습니다. 또한 해당 모드는 DHCP 서버에서만 동작됩니다.

DNS relay

해당 옵션을 통해 DNS 공격 보호 기능을 활성화 합니다.



DHCP RELAY



Add 버튼을 클릭하여 새로운 DHCP RELAY 를 생성합니다.

RELAYED INTERFACE

DHCP Client 가 연결되는 인터페이스 (SETUP-NETWORK). 해당 인터페이스를 통해 DHCP 요청이 수신됩니다.

DHCP SERVER IPV4-ADDRESS

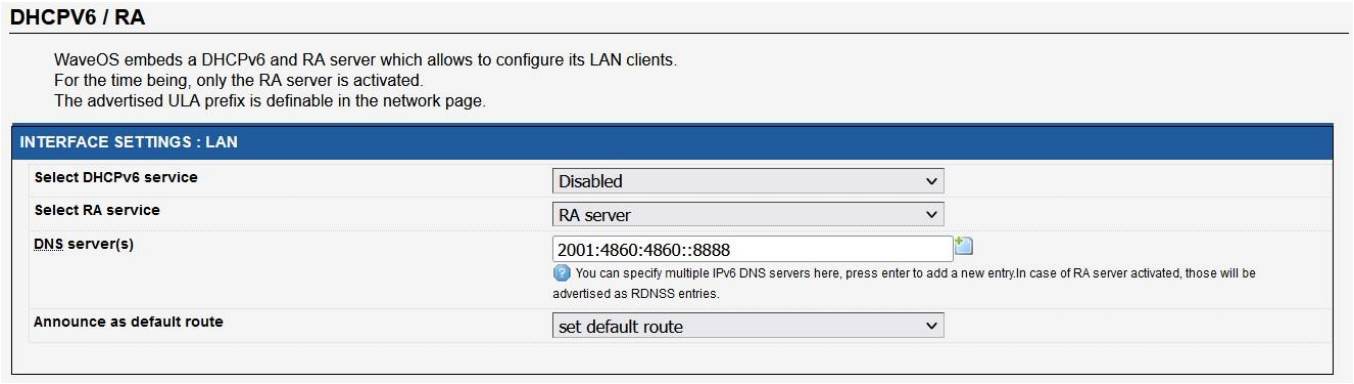
DHCP server 의 IP 주소입니다. Client 의 DHCP 요청이 해당 주소로 전달됩니다

TRUSTED INTERFACE

DHCP 요청에 대한 응답 수신을 승인하는 인터페이스 (SETUP-NETWORK) 입니다. 일반적인 경우 "all" 을 선택합니다.

VI.1.9.4 DHCPv6

DHCPv6 및 RA 서버는 LAN 클라이언트 구성을 허용하지만 이 버전에서는 RA 서버 기능만 활성화할 수 있습니다.



Select DHCPv6 service

서비스 DHCP 서버를 활성화 또는 비활성화할 수 있지만 이 릴리스에서는 이 기능이 비활성화되어 있습니다.

Select RA service

서비스 RA(Router Advertisement) 서버를 활성화 또는 비활성화할 수 있습니다.

DNS server(s)

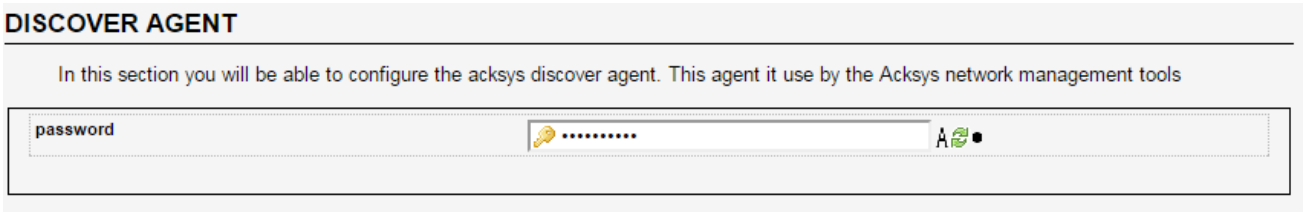
RA 서버가 알리는 DNS 서버

Announce as default route

기본 라우터 구성 허용: 기본 경로 설정 |GUA 접두사가 없으면 무시|항상 무시(기본값= 기본 경로)

VI.1.9.5 Discover Agent

해당 페이지를 통해 WaveOS 에 포함된 Discover Agent 를 설정할 수 있습니다. Acksys Network Device Manager 에서 ACKSYS 제품을 자동으로 찾기 위해 사용되는 에이전트입니다.



Password

해당 패스워드는 ACKSYS WaveManager 와 같은 NMS 소프트웨어에서 설정을 변경할 때 사용됩니다.

VI.1.9.6 Passpoint

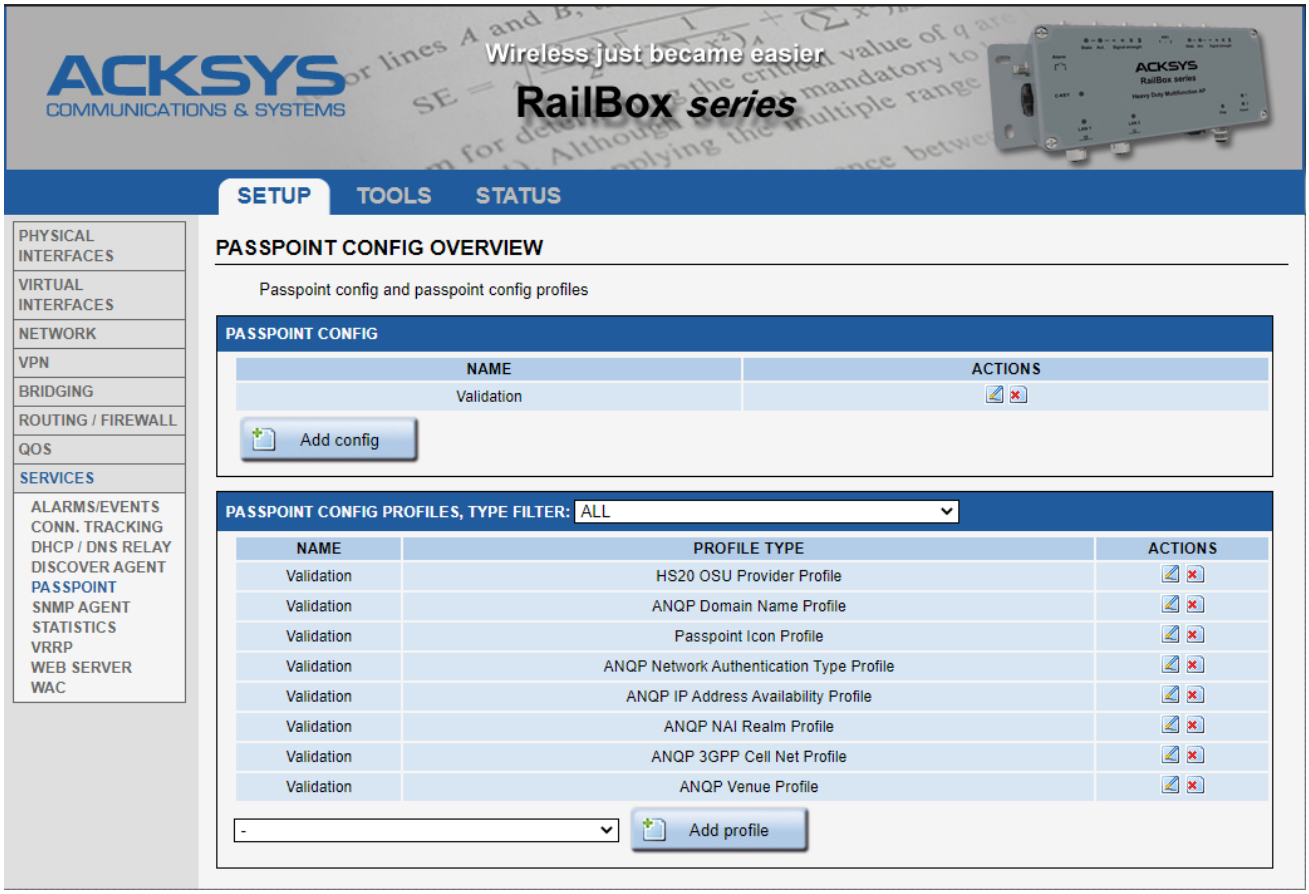


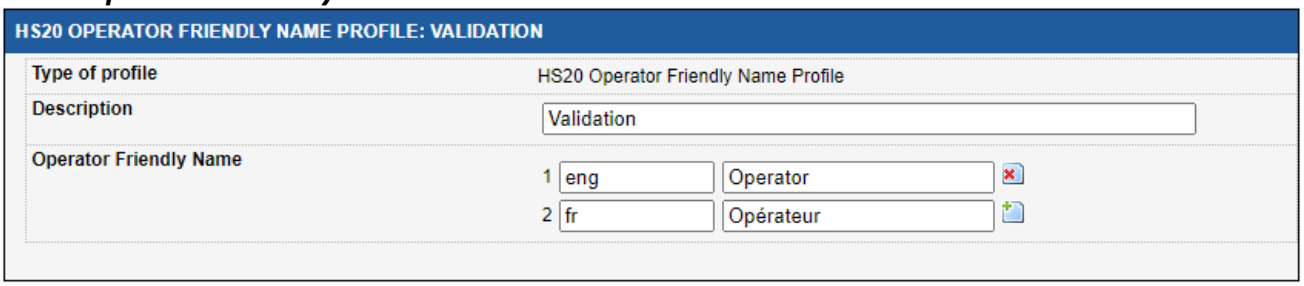
Figure 2: 페이지 Passpoint 구성 개요

Passpoint 구성을 추가하기 전에 사용할 프로필을 정의해야 합니다. 필요한 모든 정보는 제공자가 제공해야 합니다.

Passpoint Config Profiles

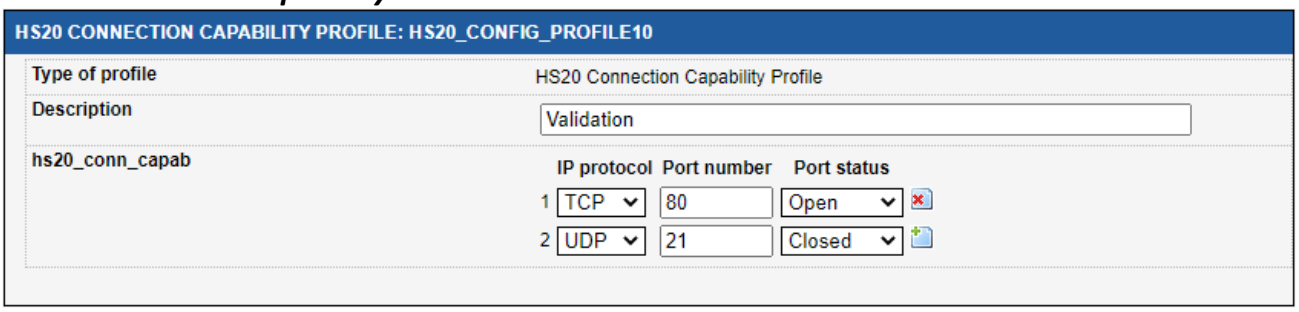
Passpoint 설정 프로필은 HS20 프로필 및 ANQP 프로필로 설정할 수 있습니다. HS20 프로필을 Hotspto2.0 기능을 설정하고, ANQP 프로필은 ANQP 802.11u 기능을 설정합니다.

HS20 Operator Friendly Name



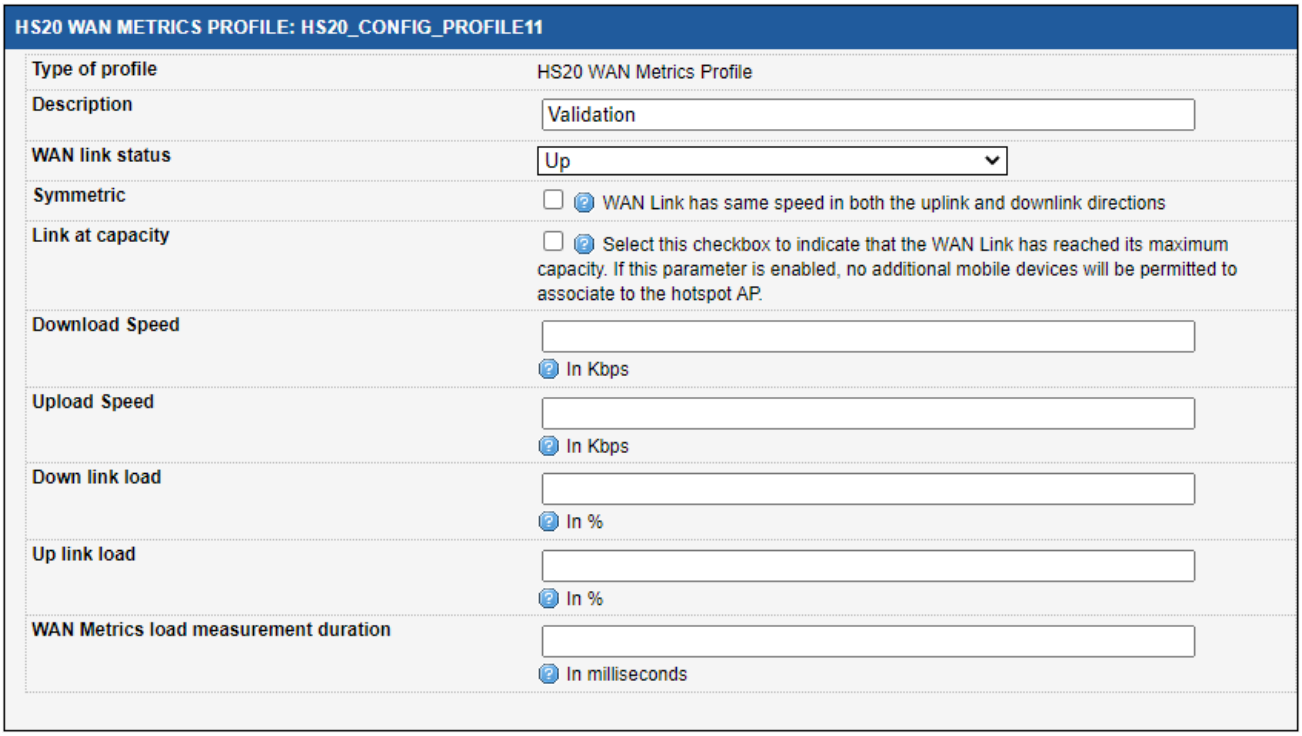
Operator friendly name: 해당 설정을 사용하여 하나 이상의 운영자에게 이름을 지정할 수 있습니다. 각 항목에는 두 개 또는 세 개의 문자 언어 코드(ISO-639) 와 연산자 이름 문자열이 있습니다.

HS20 connection capability



Hs20_conn_capab: Hotspot 에서 보낼 수 있는 IP 트래픽 유형을 공개할 수 있습니다. (firewall allowing/blocking protocols/ports).

HS20 WAN metrics



Symmetric: WAN 링크의 업링크 및 다운링크 방향 속도가 모두 동일할 경우 해당 체크 박스를 활성화 합니다.

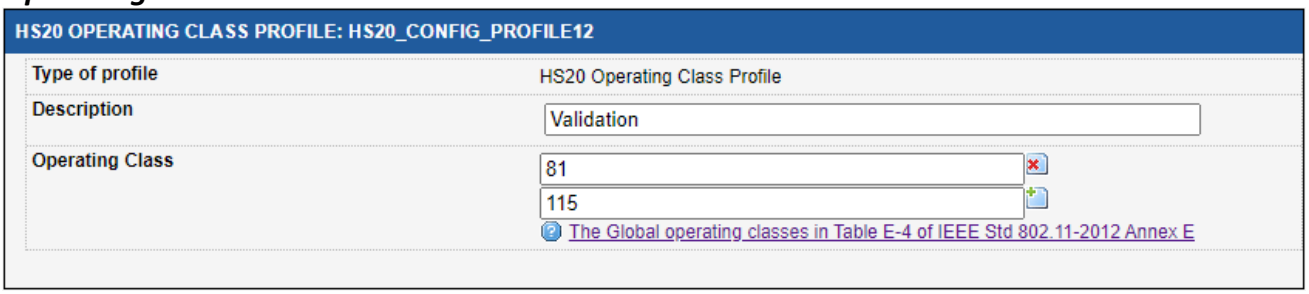
Link at capacity: WAN 링크가 최대 용량에 도달했음을 표시하려면 해당 체크 박스를 활성화 합니다. 해당 설정이 활성화되면 추가 모바일 장치가 Hotspot AP 에 연결되지 않습니다.

Download/Upload speed: 현재 WAN down/up link 의 속도 (단위 : kbps).

Down/Up link load: down/up Link WAN 연결의 전류 부하

WAN metrics load measurement duration: downlink/next load 측정 시간 (단위 : ms). 로드를 확인할 수 없을 경우 0 으로 표시됩니다.

Operating class



Operating class: 해당 SSE 에서 BSS 가 사용하는 운영 클래스의 목록입니다. *IEEE 802.11-2012* 의 부록 E-4 글로벌 등급이 표준입니다. (https://tinyurl.com/yxs4ctde)

예를 들어 81 과 115 는 채널 1~13 과 36, 40, 44, 48 을 사용하는 AP 를 표시합니다. 아래의 표를 참조하세요.

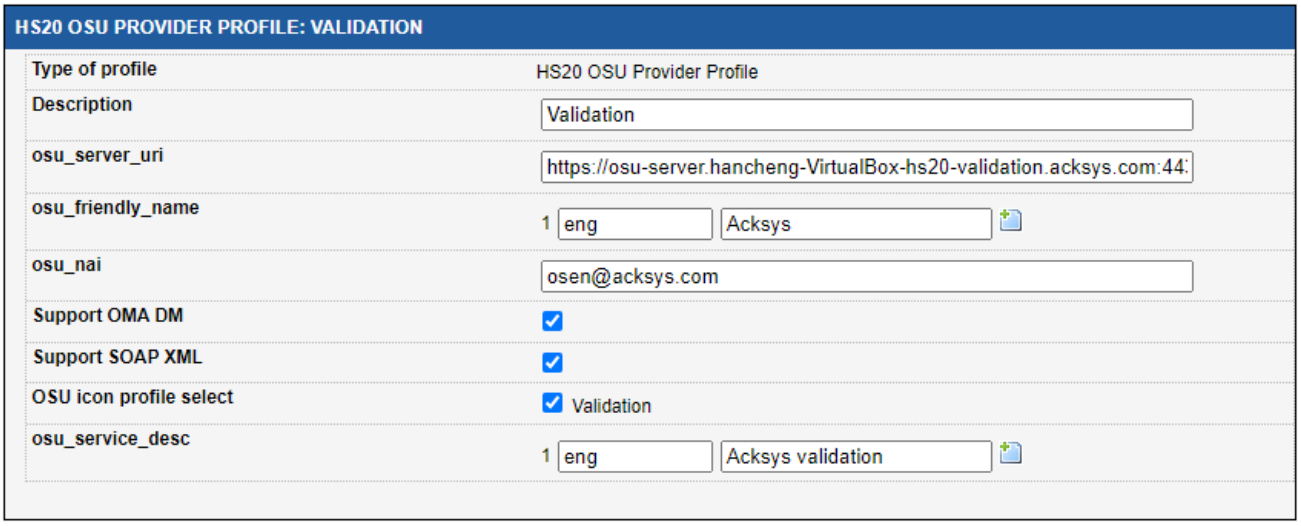
Table E-4—Global operating classes

Operating class	Nonglobal operating class(es)	Channel starting frequency (GHz)	Channel spacing (MHz)	Channel set	Behavior limits set
1–80		Reserved	Reserved	Reserved	Reserved
81	E-1-12, E-2-4, E-3-30	2.407	25	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	
82	E-3-31	2.414	25	14	

Table E-4—Global operating classes *(continued)*

Operating class	Nonglobal operating class(es)	Channel starting frequency (GHz)	Channel spacing (MHz)	Channel set	Behavior limits set
111	E-3-25,26,27,28,29	4.0025	5	182, 183, 184, 185, 186, 187, 188, 189	
112	E-3-2,3,4,5,6	5	20	8, 12, 16	
113	E-3-12,13,14,15	5	10	7, 8, 9, 10, 11	
114	E-3-21,22,23,24	5.0025	5	6, 7, 8, 9, 10, 11	
115	E-1-1, E-2-1, E-3-1	5	20	36, 40, 44, 48	
116	E-1-22, E-2-5, E-3-36	5	40	36, 44	PrimaryChannelLowerBehavior

HS20 OSU PROVIDER



OSU server URI: 클라이언트가 해당 OSU (*Online Signup Server*) Provider 를 선택할 경우 해당 URI 를 등록하여 사용할 수 있습니다.

OSU friendly name: OSU Provider 의 식별자.

OSU NAI: Client 가 Passpoint 설정에 의해 OSEN AP 에 연결 하는데 사용되는 식별자.

OMA DM: OSU 서버는 OMA DM (Open Mobile Alliance Device Management) 프로토콜을 지원합니다. (Hotspot_2.0_Specification_v2.0: 8.3 Provisioning using OMA DM)

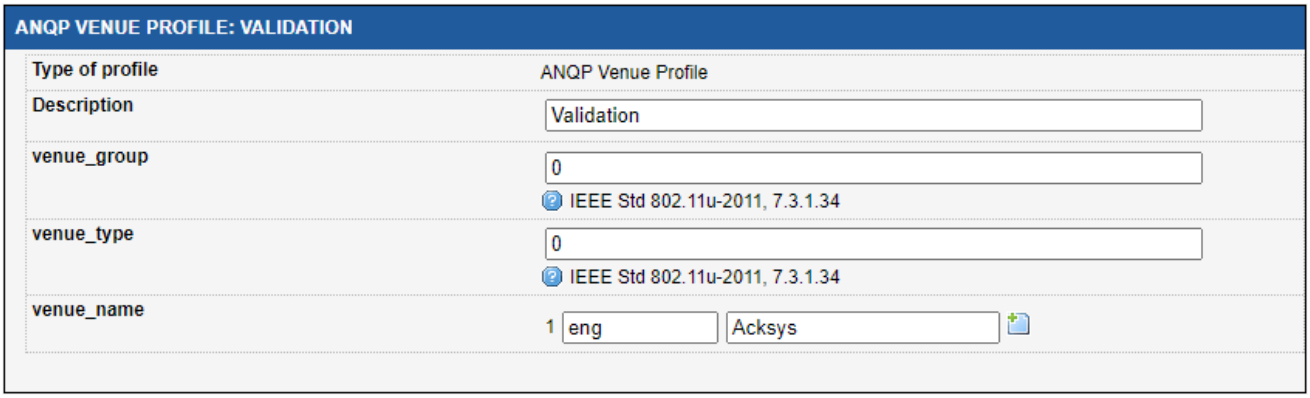
SOAP XML: OSU 서버는 SOAP XML (Simple Object Access Protocol XML) 프로토콜을 지원합니다. (Hotspot_2.0_Specification_v2.0: 8.4 Provisioning using SOAP XML)

OSU icon: OSU 이름을 기재합니다.

OSU service desc: 서비스에 대한 설명을 입력합니다.

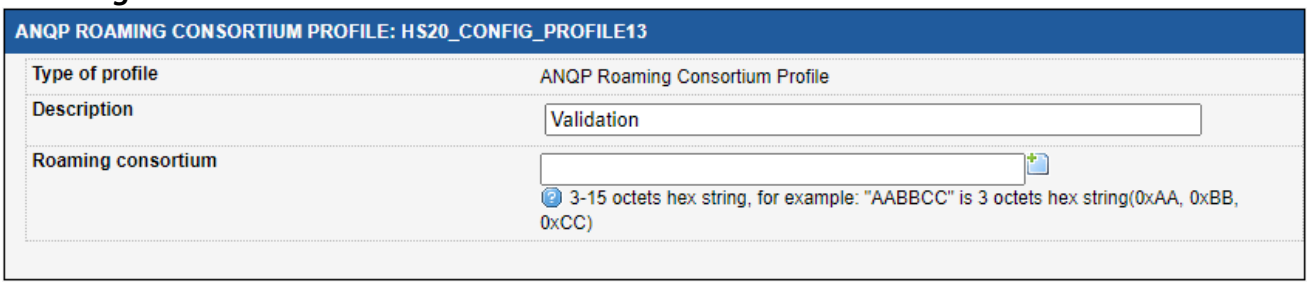
Passpoint 설정에는 여러 OSU 제공자의 프로필이 포함될 수 있습니다.

ANQP Venue



venue group 과 **venue type** 는 AP 의 경로를 지정합니다. 해당 설정 값과 설명은 *IEEE std 802.11u-2011* 섹션의 7.3.1.34 에서 확인할 수 있습니다.

Roaming Consortium

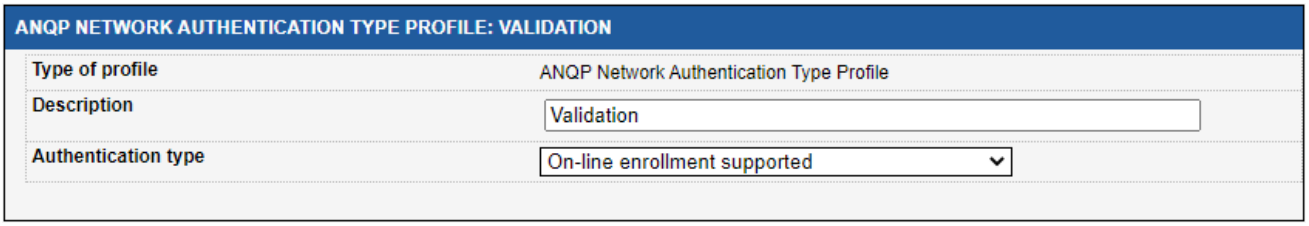


Roaming consortium: roaming consortium 는 OI (Organization Identifier)의 목록입니다. 식별자는 IEEE 가 할당한 24 비트 번호입니다. 해당 번호는 MAC 주소에서 제조업체 또는 조직을 고유하게 식별합니다. 네트워크 인터페이스의 MAC 주소의 첫 3 바이트는 OUI 입니다.

해당 필드는 hexdump 형식으로 입력해야 합니다. 예를 들어 10 진수로 1000, 16 진수로 0x3E8, 16 진수 덤프는 03E8 입니다.

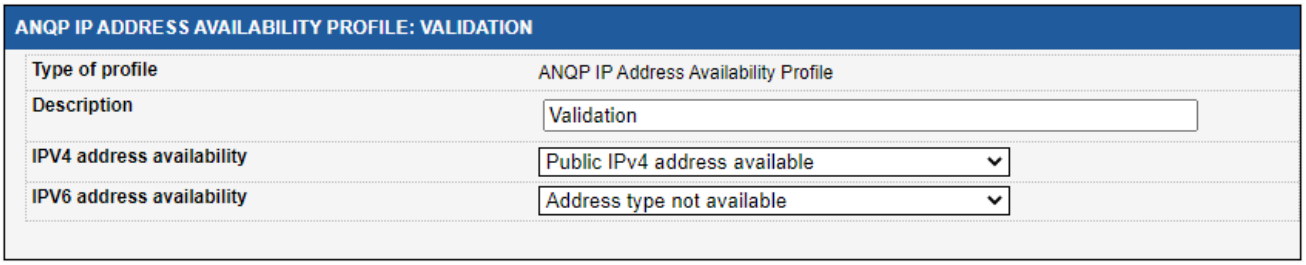
Acksys 의 OI 는 000990XXXXXXXXXXXXXXXXXXXXXX 입니다.

ANQP Network Authentication Type



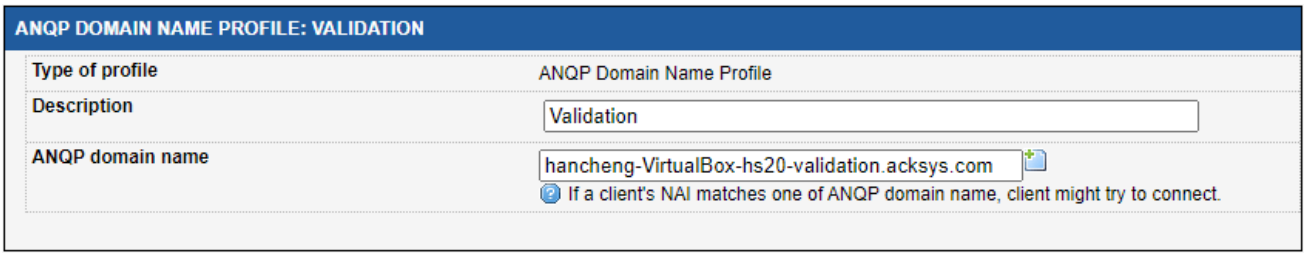
Authentication type: 패스포인트가 ASRA (Additional Step Required for Access)로 설정된 경우 해당 구성에 적용하려면 ANQP 네트워크 인증 유형 프로필이 필수로 필요합니다.

ANQP IP Address Availability



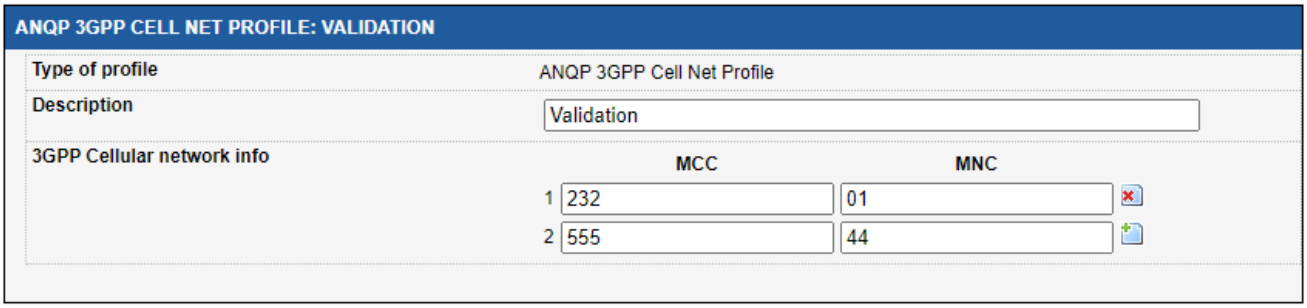
해당 프로필을 사용하여 AccessPoint 네트워크에서 사용할 수 있는 IPv4 및 IPv6 주소 유형을 설정합니다.

ANQP Domain name



도메인의 이름 항목은 IEEE 802.11 네트워크를 운영하는 엔티티의 하나 이상의 도메인 이름 목록을 제공합니다. Client 의 NAI 는 ANQP 도메인 이름 중 하나에 해당되며 Client 도 해당 AccessPoint 에 연결을 시도합니다.

ANQP 3GPP Cell Net

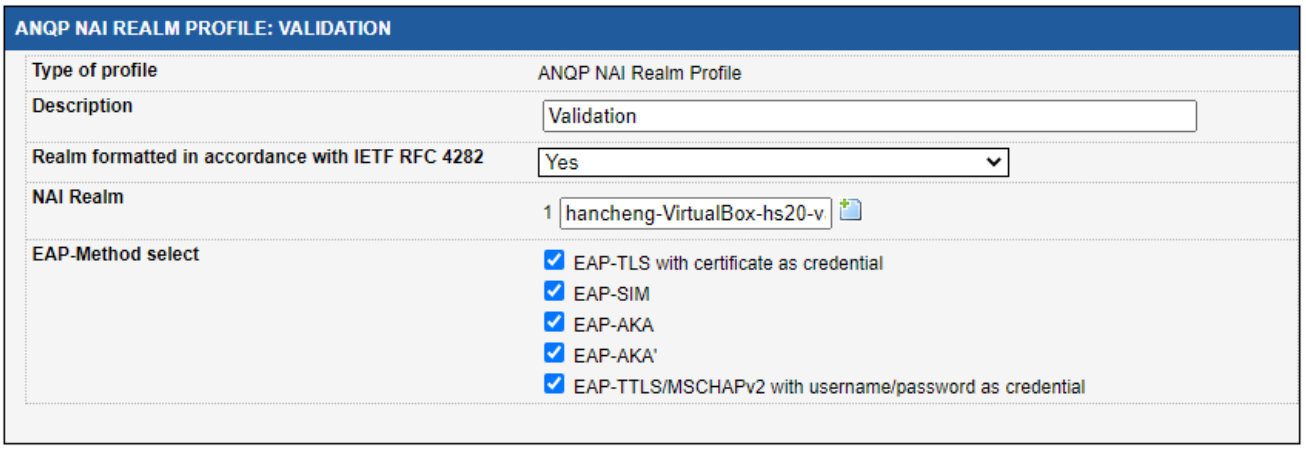


3GPP cellular network info 는 MMC 와 MNC 로 구성된 중복 목록으로 연산자를 식별하는데 사용됩니다.

MMC: MMC(모바일 국가 코드)는 국제전기통신연합(ITU) 이 권고사항 E.212 에서 표준화한 3 자리 국가코드로, 특히 GSM 과 UMTS 기술에서 사용됩니다. (예:프랑스의 MMC 는 208 입니다.)

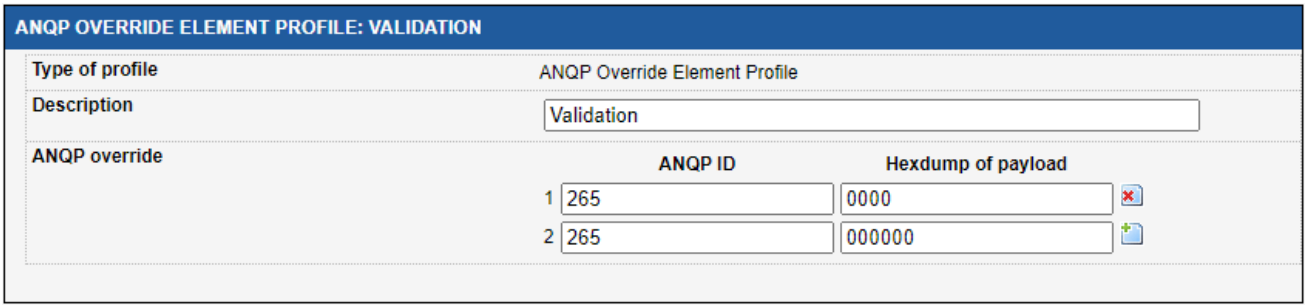
MNC: MNC(모바일 네트워크 코드)는 GSM, CDMA, TETRA, UMTS, LTE 및 특정 모바일 위성 네트워크를 사용하는 모바일 네트워크 운영자의 네트워크를 명확하게 식별하기 위해 MCC 와 함께 사용됩니다. (예:Orange 의 3gpp 코드는 MCC = 208, MNC = 01)

ANQP NAI Realm



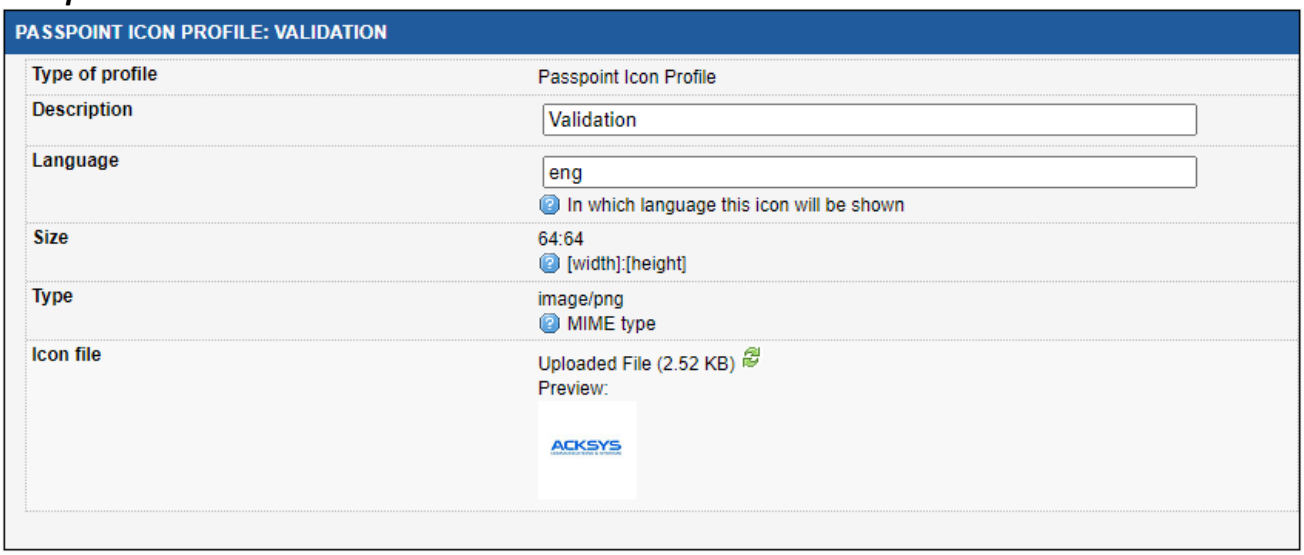
각 **NAI Realm** 은 선택적으로 EAP 와 연결될 수 있습니다. 각각의 EAP 방식은 선택적으로 인증 값의 세트와 통합될 수 있습니다. NAI 도메인 정보는 STA 가 IEEE 802.1x RSN 환경에서 연결을 설정하는데 사용됩니다. STA 가 NAI 도메인을 인식하면 EAP 방식이 다르게 설정되어도 인증을 시도할 수 있습니다. Passpoint 설정에서 여러 개의 ANQP NAI 영역 프로필을 활성화 할 수 있습니다.

ANQP Override Element



Hexdump 형식으로 내용을 지정하여 임의 값을 가진 추가 ANQP 요소를 설정할 수 있습니다. 해당 값은 상위 계층의 ANQP 요소의 내용을 입력합니다.

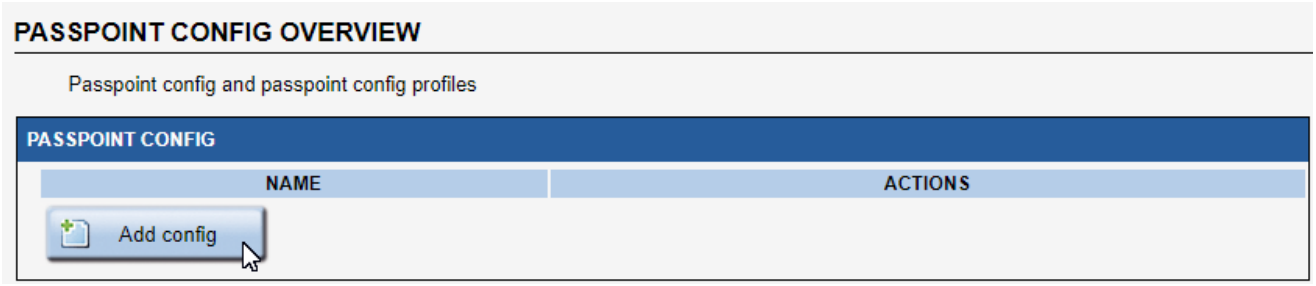
Passpoint icon

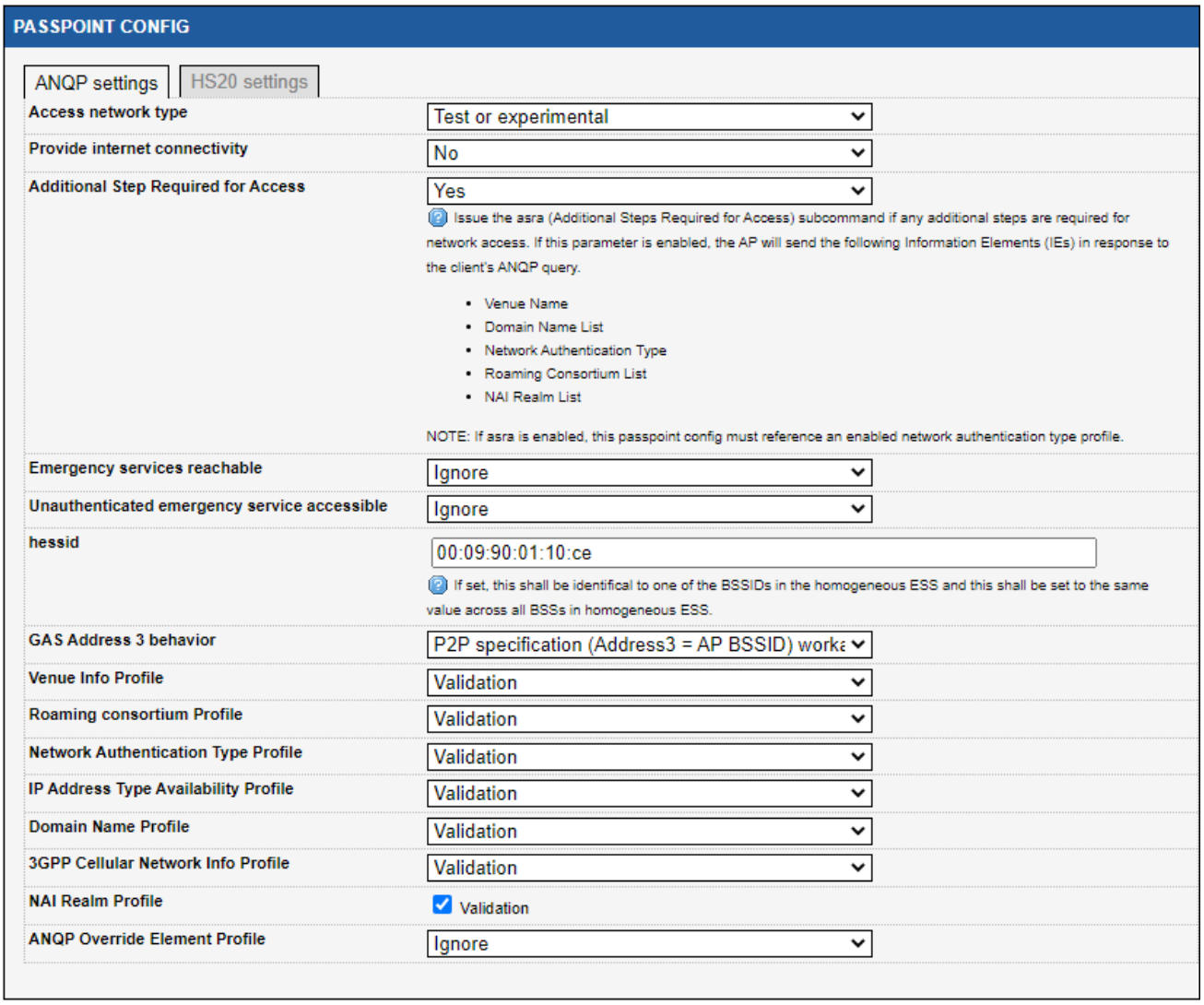


다른 프로필에서 참조할 아이콘 파일을 다운로드 합니다.

Passpoint Config

Passpoint 설정은 여러 개의 "passpoint config profiles" 로 구성됩니다. 따라서 Passpoint 설정을 진행하기 전에 프로필을 설정해야 합니다.





Access network type: 해당 옵션은 연결 후 연결될 네트워크의 유형을 나타냅니다. 사용 가능한 유형은 다음과 같습니다:

- Private network
- Private network with guest access
- Chargeable public network (paying public network)
- Free public network
- Personal device network
- Emergency services only network
- Test or experimental
- Wildcard (general network)

Provide internet connectivity: 페어링 후 인터넷을 사용할 수 있는지 여부.

Additional Step Required for Access (ASRA): 네트워크 연결에 대한 추가 조치가 필요한 경우. 해당 옵션이 활성화 된 경우 올바른 "Network authentication type" 프로필도 적용되어야 합니다.

Emergency services reachable: emergency services 에 연결할 수 있는지 확인합니다.

Unauthenticated emergency service accessible: 인증되지 않은 emergency services 에 연결할 수 있는지 확인합니다.

HESSID: Homogeneous ESS 식별. HESS 의 BSSID 중 하나와 동일하게 설정되어야 하며 HSSE 는 모든 SSE 에서 동일한 값을 설정해야 합니다.

GAS Address 3 behavior: "Address 3"에 대한 GAS 프레임에 대해 취해야 할 조치. Address 3 은 802.11 프레임 헤더에 삽입된 세 번째 MAC 주소입니다. MAC 프레임 형식에는 네 개의 주소 필드가 있습니다. 해당 필드는 기본 서비스 세트 식별자(BSSID), 소스 주소(SA), 대상 주소(DA), 송신 STA(TA)의 주소 및 수신 STA(RA)의 주소를 표시하는 데 사용됩니다. 일부 프레임은 일부 주소 필드를 포함하지 않을 수 있습니다.
옵션은 다음과 같습니다:

- P2P 사양(Address3 = AP BSSID) 해결 방식은 GAS 요청 Address3 에 따라 기본적으로 활성화됩니다: 응답 프레임의 Address 3 은 액세스 포인트의 BSSID 또는 와일드카드(FF:FF:FF:FF:FF:FF)로 채워져야 합니다.
    - GAS 초기 요청의 BSSID 가 브로드캐스트되는 경우 IEEE 802.11 std 를 수행합니다.
    - 그렇지 않은 경우, 응답의 주소 3 을 AP 의 BSSID 와 동일하게 합니다.
- GAS 요청 Address 3 에 관계없이 IEEE802.11 표준 준수 : GAS 의 초기 프레임의 Address 3 이 무엇이든 항상 802.11 표준을 준수합니다.
- Force non-compliant behavior: 항상 GAS 요청에 대한 초기 응답의 Address 3 이 AccessPoint 의 BSSID 인지 확인합니다.

Venue info profile: 해당 옵션을 무시하려면 “Venue info” 프로필을 선택하거나 “ignore” 를 선택합니다.

Roaming consortium Profile: 해당 옵션을 무시하려면 ”Roaming consortium” 프로필을 선택하거나 “ignore” 를 선택합니다.

Network Authentication Type Profile: 해당 옵션을 무시하려면 “Network Authentication Type” 프로필을 선택하거나 “ignore” 를 선택합니다.

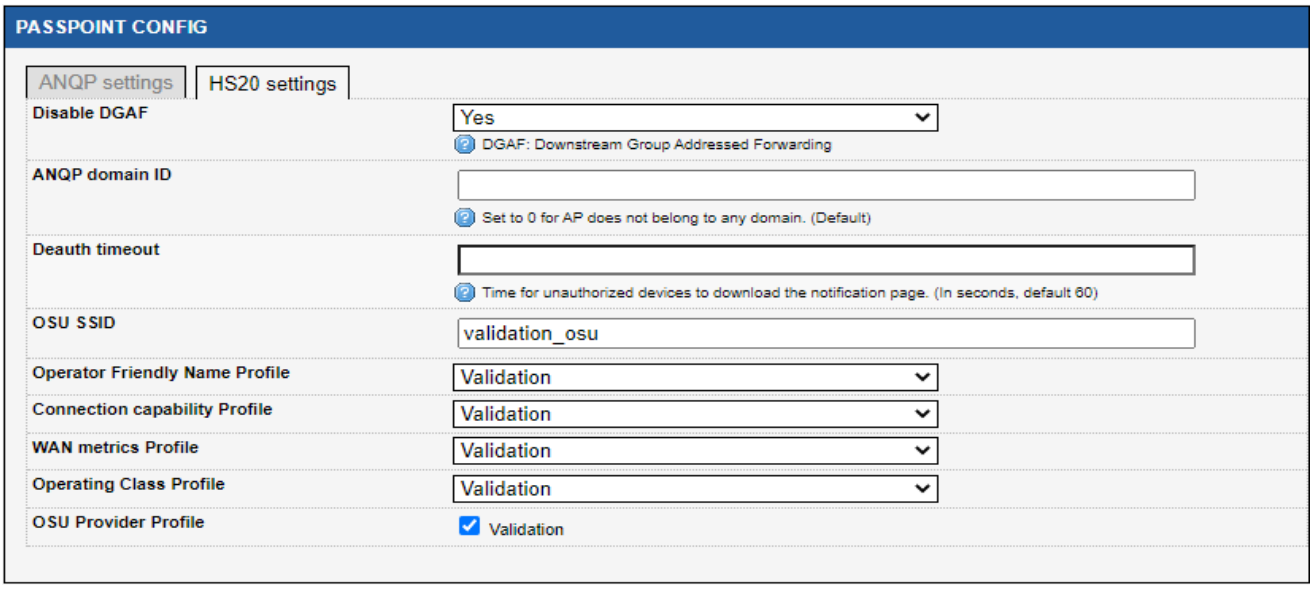
IP Address Type Availability Profile: 해당 옵션을 무시하려면 “IP Address Type Availability” 프로필을 선택하거나 “ignore” 를 선택합니다.

Domain Name Profile: 해당 옵션을 무시하려면 "Domain Name Profile" 을 선택하거나 "ignore" 를 선택합니다.

3GPP Cellular Network Info Profile: 해당 옵션을 무시하려면 “3GPP Cellular Network Info” 을 선택하거나 "ignore" 를 선택합니다.

NAI Realm Profile: 하나 이상의 “NAI Realm” 프로필을 선택하거나 해당 옵션을 무시할 내용을 남겨두지 마세요.

ANQP Override Element Profile: 해당 옵션을 무시하려면 "ANQP Override Element" 을 선택하거나 "ignore" 를 선택합니다.



Disable DGAF: DGAF(Disable Downstream Group-Addressed Forwarding) 를 사용하지 않도록 설정합니다. 그룹에서 지정된 주소의 프레임이 허용되지 않는 네트워크를 설정하는 데 사용됩니다. AccessPoint 는 그룹 주소 프레임을 스테이션으로 전송하지 않으며, 관련 스테이션이 BSS 내의 다른 스테이션으로 프레임을 위조하는 것을 방지하기 위해 각 스테이션에 대해 GTK 가 발행됩니다.

ANQP domain ID: 동일한 공통 ANMQP 정보를 공유하는 SSE 의 AccessPonit 집합에 대한 식별자 (0 – 65535). 기본값은 0 이며, 일부 ANMQP 정보가 해당 AccessPoint 에 포함됨을 의미합니다. (기본값)

Deauth timeout: RADIUS 서버가 스테이션이 BSS/ESS 에 연결할 수 있는 권한이 없음을 표시하는 경우, AccessPoint 는 스테이션이 알림 페이지(메시지에 포함된 URL) 를 다운로드 하도록 허용할 수 있습니다. 해당 설정의 지연은 초 단위로 진행됩니다. 기본값은 60 입니다.

OSU SSID: 표시된 모든 OSU 공급자의 OSU 연결에 사용되는 SSID 입니다.

Operator Friendly Name Profile: 해당 옵션을 무시하려면 “Operator Friendly Name” 프로필을 사용하거나, “ignore” 를 선택해서 무시하세요.

Connection capability Profile: 해당 옵션을 무시하려면 “Connection capability” 을 선택하거나 "ignore" 를 선택해서 무시하세요.

WAN metrics Profile: 해당 옵션을 무시하려면 “WAN metrics” 을 선택하거나 "ignore" 를 선택해서 무시하세요.

Operating Class Profile: 해당 옵션을 무시하려면 "Operating Class" 을 선택하거나 "ignore" 를 선택해서 무시하세요.

OSU Provider Profile: 하나 이상의 “OSU Provider” 프로필을 확인하거나 해당 옵션을 무시할 내용을 남겨두지 마세요.

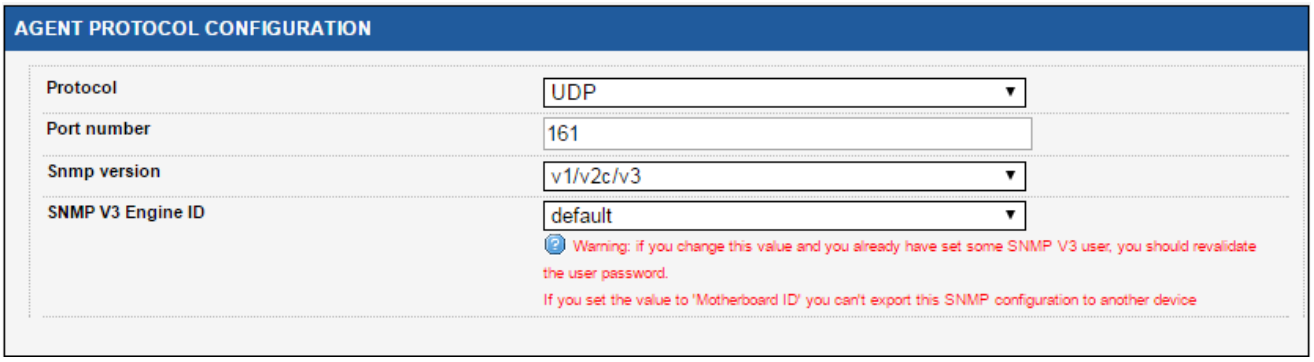
VI.1.9.7 SNMP Agent

SNMP Agent 는 기본적으로 활성화되며 **public** community 를 사용하여 MIB-II 및 ACKSYS MIB 에 대한 읽기/쓰기 권한을 허용합니다.

ACKSYS MIB 파일은 자체 문서화되어 있습니다. OID 설명서를 읽으려면 텍스트 파일 편집기 또는 MIB 브라우저를 사용하세요.

SNMP 사용자 및 액세스 권한을 구성하기 전에 SNMP 보안 장을 읽으세요: V.6.1 SNMP security

AGENT PROTOCOL CONFIGURATION



Protocol:

에이전트 연결 방식 (UDP/TCP)

Port number:

에이전트 포트 번호

SNMP version:

- **v1/v2c**: **security model v1**, **v2c, usm** 을 사용할 수 있습니다.
- **v3**: **usm security model** 만 허용됩니다.

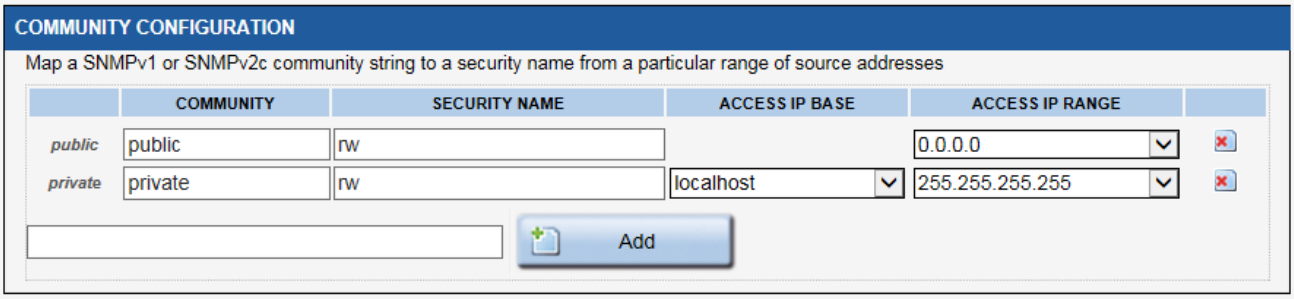
SNMP V3 Engine ID

- **Default:** 모든 장치의 기본 Engine ID 는 동일합니다. 해당 설정을 통해 여러 장치 간에 SNMP 설정을 공유할 수 있습니다. SNMP V3 사용자가 이미 있는 상태에서 해당 값을 변경할 경우 각 장치에서 사용자 암호를 다시 확인해야 합니다.
- **MotherboardID:** Motherboard ID 를 EngineID 로 사용합니다. 해당 ID 는 고유하므로 해당 설정을 가진 각 장치의 Engine ID 가 다릅니다. 해당 설정에서는 여러 제품 간에 SNMP 설정을 공유할 수 없습니다. 각 장치에서 사용자 암호를 다시 확인해야 합니다.

COMMUNITY CONFIGURATION

해당 섹션에서는 커뮤니티 목록, 커뮤니티 액세스 권한 및 커뮤니티 사용자에 대한 제한 사항을 확인할 수 있습니다. SNMP v1/v2c **community based security model** 기반의 보안 모델에 의존합니다.

주의: 공용 커뮤니티 속성을 변경할 경우 SNMP 클라이언트가 적절하게 설정되었는지 확인해야 합니다. 예를 들어, Acksys WaveManager 소프트웨어에는 장치 별로 커뮤니티를 변경할 수 있는 메뉴가 있습니다.



액세스 권한 규격을 추가하려면 규격의 닉네임을 입력한 후 **Add** 버튼을 클릭합니다. 닉네임은 문자, 숫자 및 밑줄로 설정되어야 합니다. 닉네임은 커뮤니티 이름이 아닌 **access rights specification** 이름입니다.

기본적으로 **private** 커뮤니티는 과거의 호환성을 위해 동작되지만 변경할 수 없습니다. 기본 커뮤니티를 원하는 대로 재설정 할 수 있습니다.

Community:

SNMP Client 가 에이전트에 대해 식별하기 위해 제공해야 하는 식별자. 필요한 경우 닉네임과 동일하게 사용할 수 있습니다.

Security Name:

VACM 섹션에서 액세스 권한을 설정하는 데 사용할 보안 이름.

Access IP base:

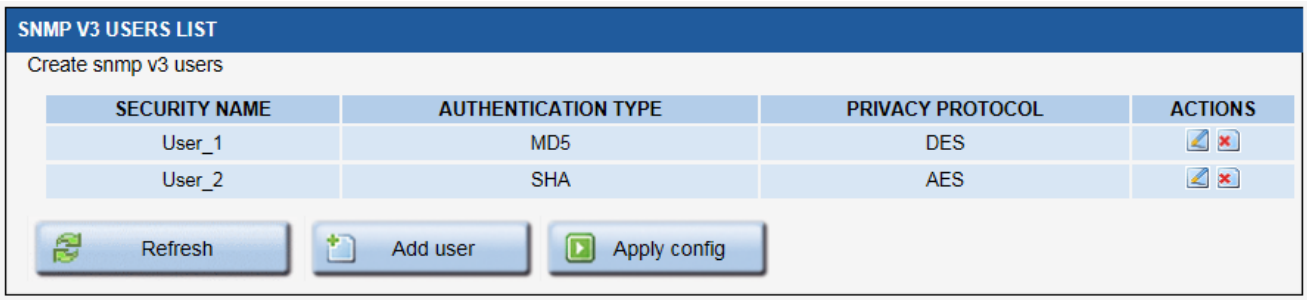
해당 규격을 사용할 수 있는 IP 주소입니다. DNS 서버가 SETUP-Network 페이지에서 입력 되었거나 DHCP 서버에서 가져온 경우 호스트 이름 (FQDN)을 입력할 수 있습니다.

Access IP range:

허용된 Client IP 주소의 전체 범위를 결정하기 위한 IP 마스크 입니다.

SNMP V3 USM user administration

USM 보안 모델에 따라 **SNMP v3** 사용자의 보안 설정을 생성, 삭제 또는 수정할 수 있습니다.

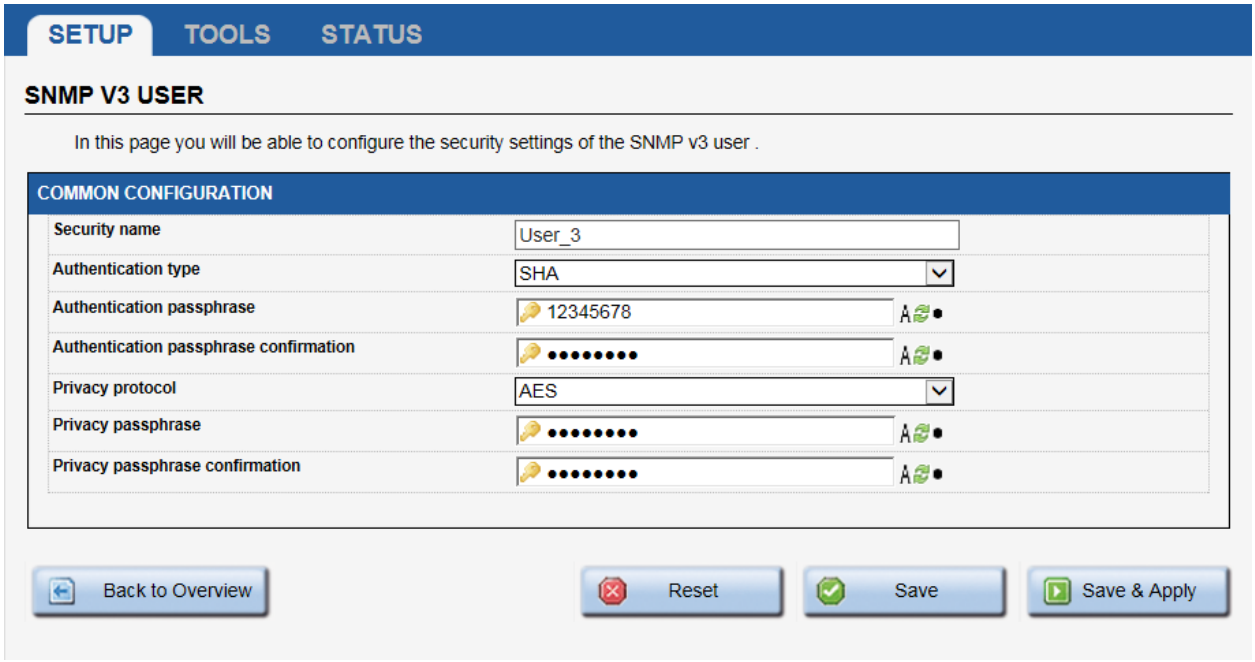


Refresh button:

Refresh 버튼을 클릭하여 SNMP Agent 의 사용자 데이터베이스와 동기화 합니다 (SNMP v3 에서는 명령을 통한 원격으로 사용자를 생성할 수 있습니다). 또한 저장된 변경 내용도 SNMP 설정에 적용됩니다.

Add user button:

Add 버튼을 클릭하여 새 SNMP v3 사용자를 생성합니다.



해당 섹션을 통해 사용자 인증 정보를 설정할 수 있습니다.

보안상의 이유로 저장된 암호는 나중에 확인할 수 없습니다.

Authentication type:

지원되는 인증 유형은 SHA-512, SHA-384, SHA-256 및 SHA-224 입니다.

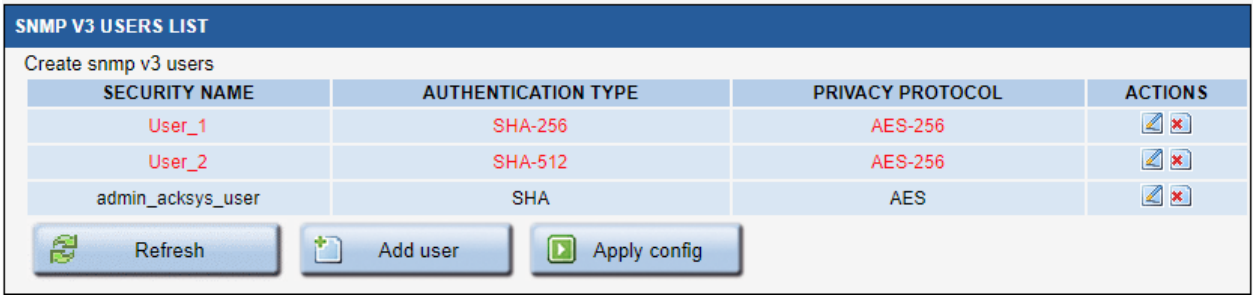
지원되는 프라이버시 프로토콜은 AES-256, AES-192 및 AES 입니다.

SHA1, MD5 및 DES 도 호환성을 위해 지원되지만 안전하지 않은 것으로 표시됩니다.

향후 버전에서는 확실히 제거될 것이므로 사용하지 않는 것이 좋습니다.

Apply config button:

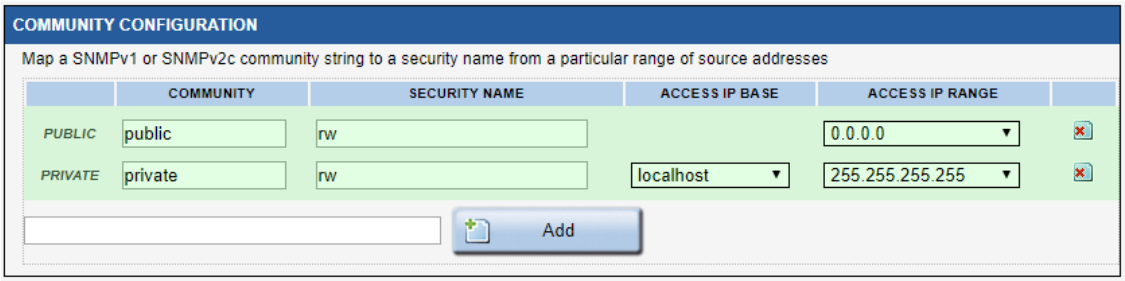
해당 버튼을 클릭하면 변경 사항이 적용됩니다. 아직 SNMP v3 사용자 목록에 적용되지 않은 변경 사항은 빨간색으로 표시됩니다.

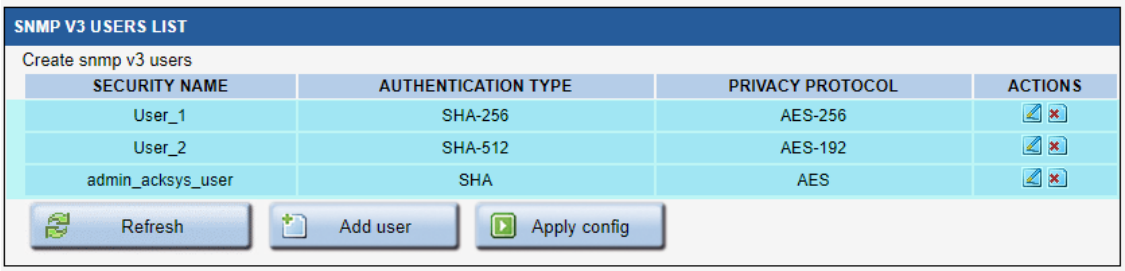


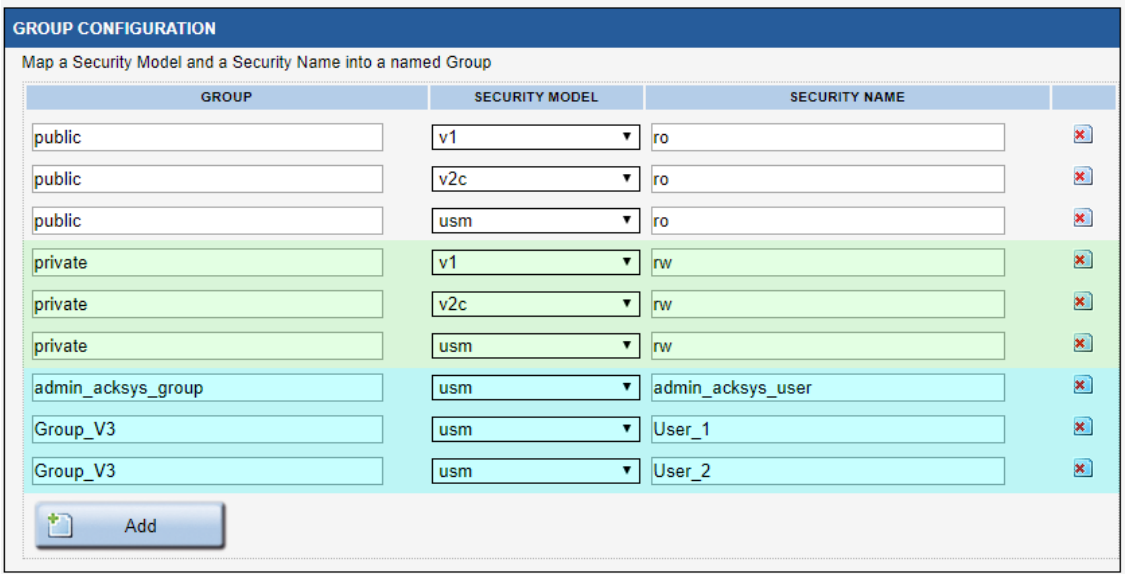
Access control administration (VACM)

해당 섹션을 통해 SNMP v3 사용자 또는 SNMP v1/v2c 커뮤니티의 액세스 권한을 관리할 수 있습니다.

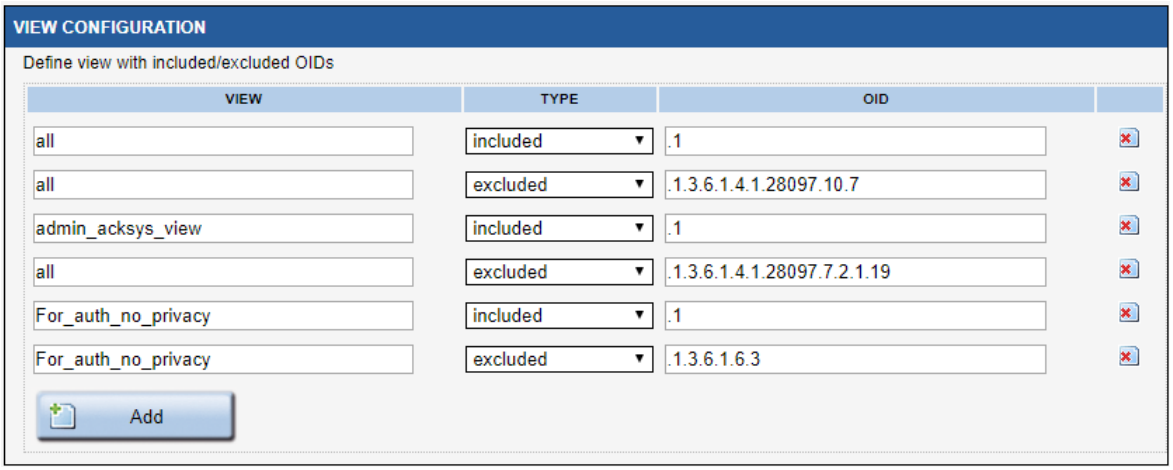
1) 보안 모델을 사용하여 **Group** 에 사용자 추가



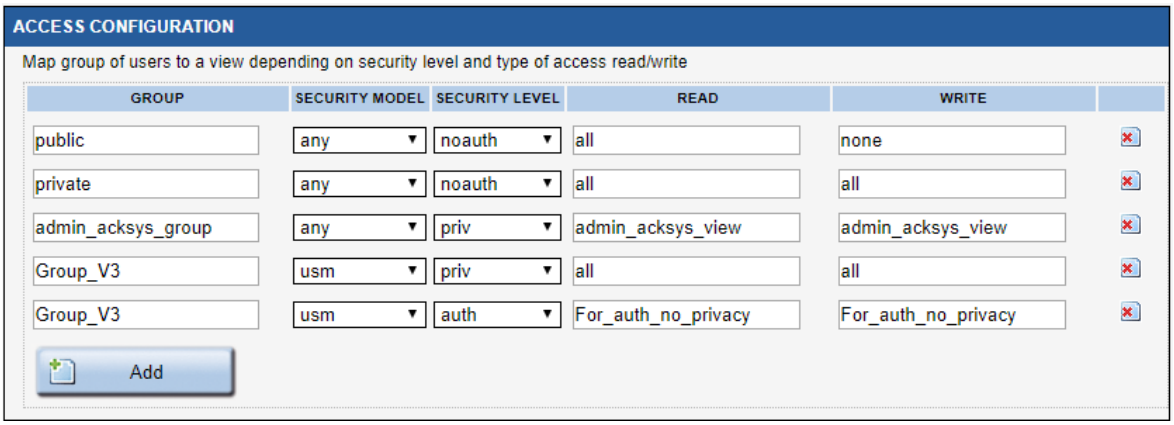




2) OID 에 권한이 필요한 보기 생성



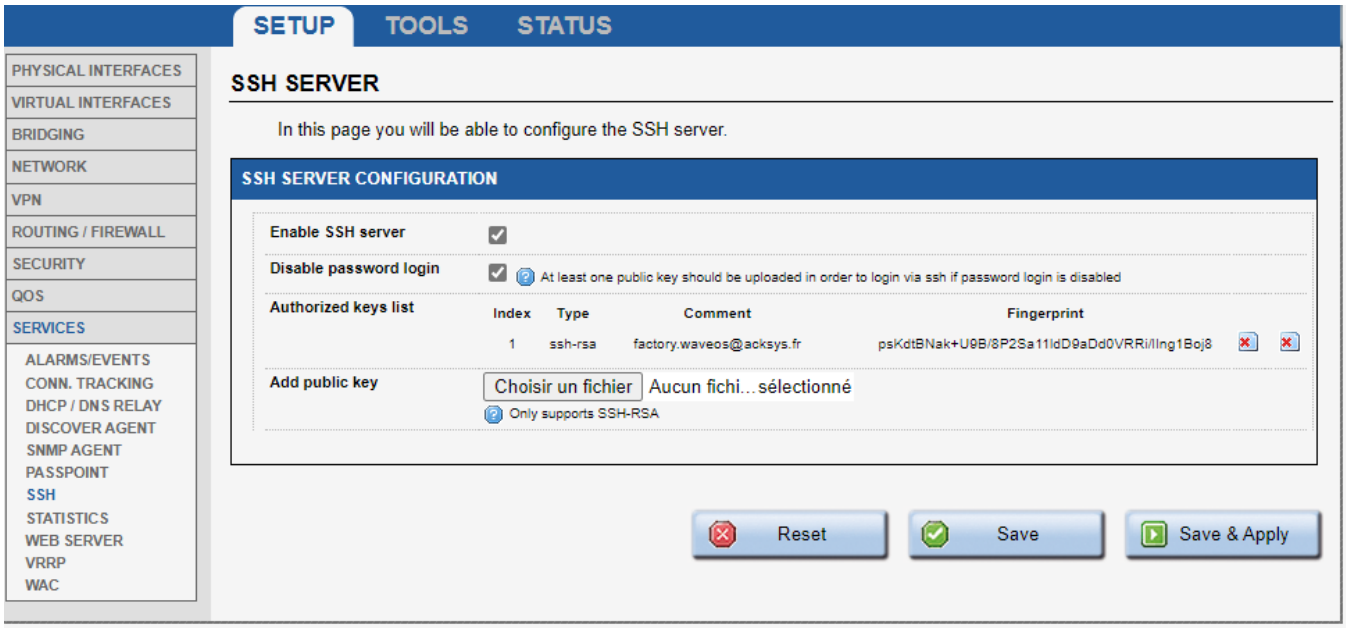
3) 사용자 보안 모델 및 보안 수준에 따라 그룹에 대한 보기의 액세스 권한 설정



VI.1.9.8 SSH Server

해당 페이지를 통해 제품에 내장된 SSH Server 기능을 활성화 할 수 있습니다.

경고 : 해당 기능은 개발자용으로 제품에 손상이 발생할 수 있습니다.



Enable SSH server

해당 기능을 활성화 하지 않으면 SSH 서버가 종료됩니다.

Disable password login

해당 옵션을 선택/선택 취소 하여 암호 로그인을 활성화/비활성화 할 수 있습니다.

주의 : 암호 로그인이 비활성화 된 경우 RSA 키만 SSH 서버에 연결할 수 있습니다.

Authorized keys list

제품에 내장된 모든 인증 키가 표시됩니다.

Index : 0 부터 시작하는 저장된 키의 인덱스 입니다.

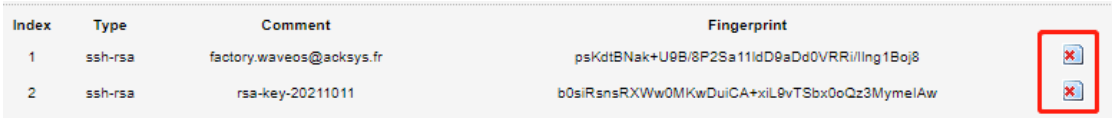
Type : 저장된 키의 유형입니다. 현재는 RSA 키만 지원됩니다.

Comment : 저장된 키의 설명입니다.

주의: 동일한 두 키는 서로 다른 식별자를 가질 수 있고 서로 다른 두 키는 동일한 식별자를 가질 수 있으므로 키의 식별 정보를 간주하지 마세요.

Fingerprint : 저장된 키의 짧은 식별, 지문을 비교하여 두 개의 키가 동일한지 비교할 수 있습니다.

키를 삭제하려면 각 행의 오른쪽 삭제 버튼을 클릭합니다.



Index	Type	Comment	Fingerprint
1	ssh-rsa	factory.waveos@acksys.fr	psKdtBNak+U9B/8P2Sa11ldD9aDd0VRRi/Ing1Boj8
2	ssh-rsa	rsa-key-20211011	b0siRsnsRXWw0MKwDuiCA+xiL9vTSbx0oQz3MymeIAw

Add public key

생성된 키를 일반 텍스트 파일에 다음 형식으로 붙여 넣어야 합니다:

ssh-rsa[space][AAAA….(key content)][space][key comment]

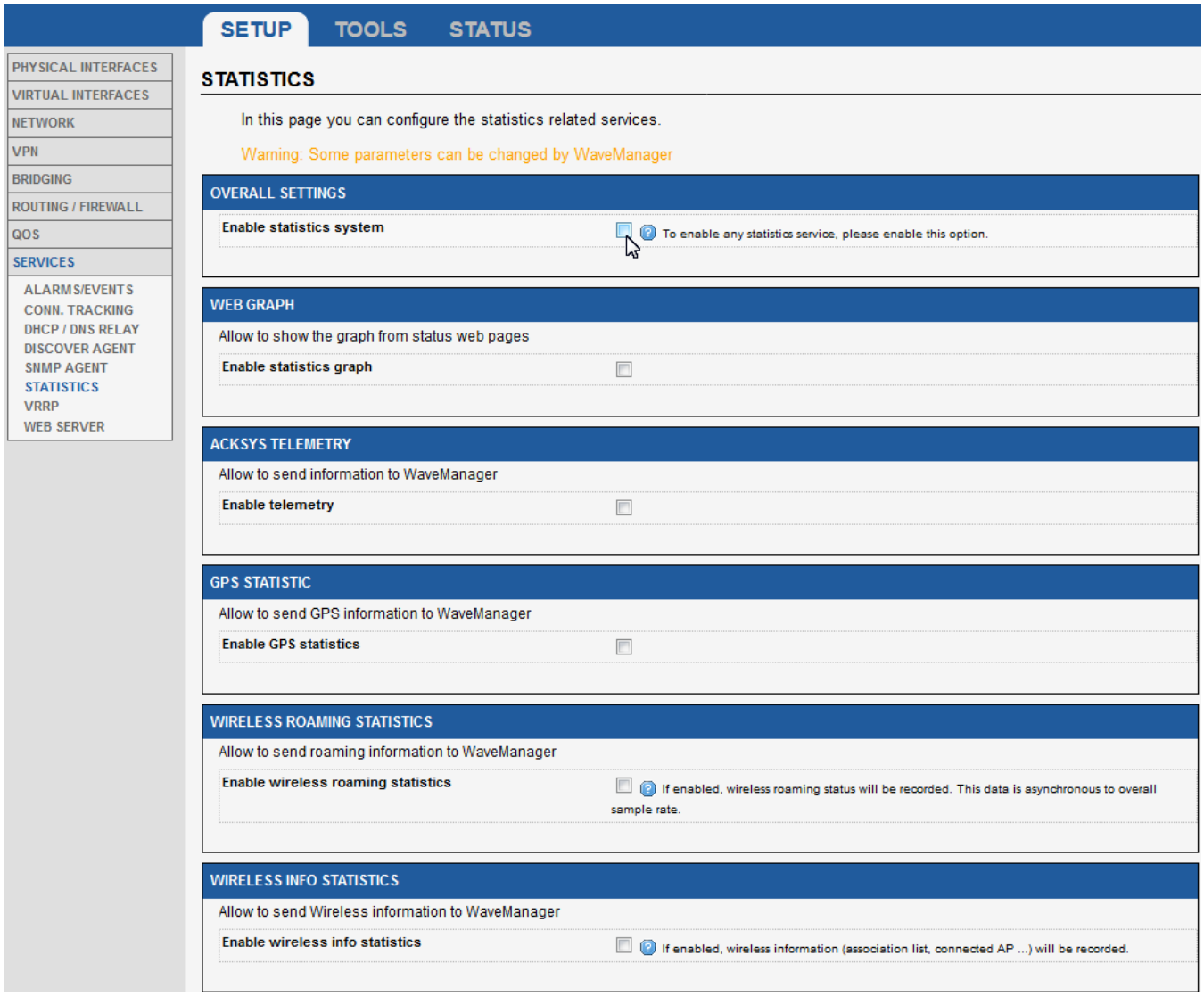
예시:

ssh-rsa
AAAB3NzaC1yc2EAAAADAQABAAABAQCWOmRA3qIcY7lWjSg4psIaULpB7Usl6obkRveOxj8TCzcK9UsNzknGiSOIG2R
C0uZ2J5QR7B/ijLNLySkOpt/oVvM/30jWtpDNlX9n14AVmnNwwwT1xzNXzMt1qahg3TBpI6qGoEEuTZF24qu8Q8NL5y
f9N+tQS2HyYfSsJitf93PaRTH8hxYwmi41qCTVHXeqrI554YYzIkArYT7zXbUWsiQzrtz9QOk7s2lavF6gk+ZT1j1dbTqBjTfP
EfwknGpWdFTn257hJ6pEsK+Fx0KJhkzXIyMf1nLaTjRbtaZDmWD542r0eK7pHUGKfOpUem9dpFR9qrHupt9P1p2NBap
F rsa-key-20211011

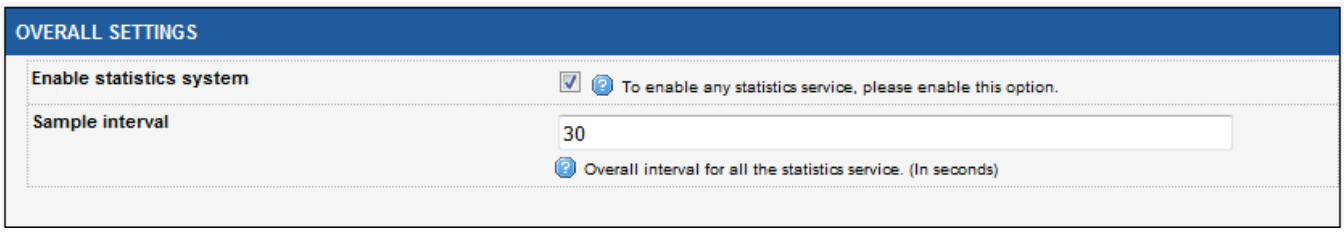
한 줄에 하나의 키가 포함된 파일을 업로드 하여 여러 개의 키를 한 번에 추가할 수도 있습니다. 형식과 일치하지 않는 파일은 거부됩니다.

VI.1.9.9 Statistics

주기적으로 데이터를 수집하여 제품 성능을 그래프로 표시합니다.

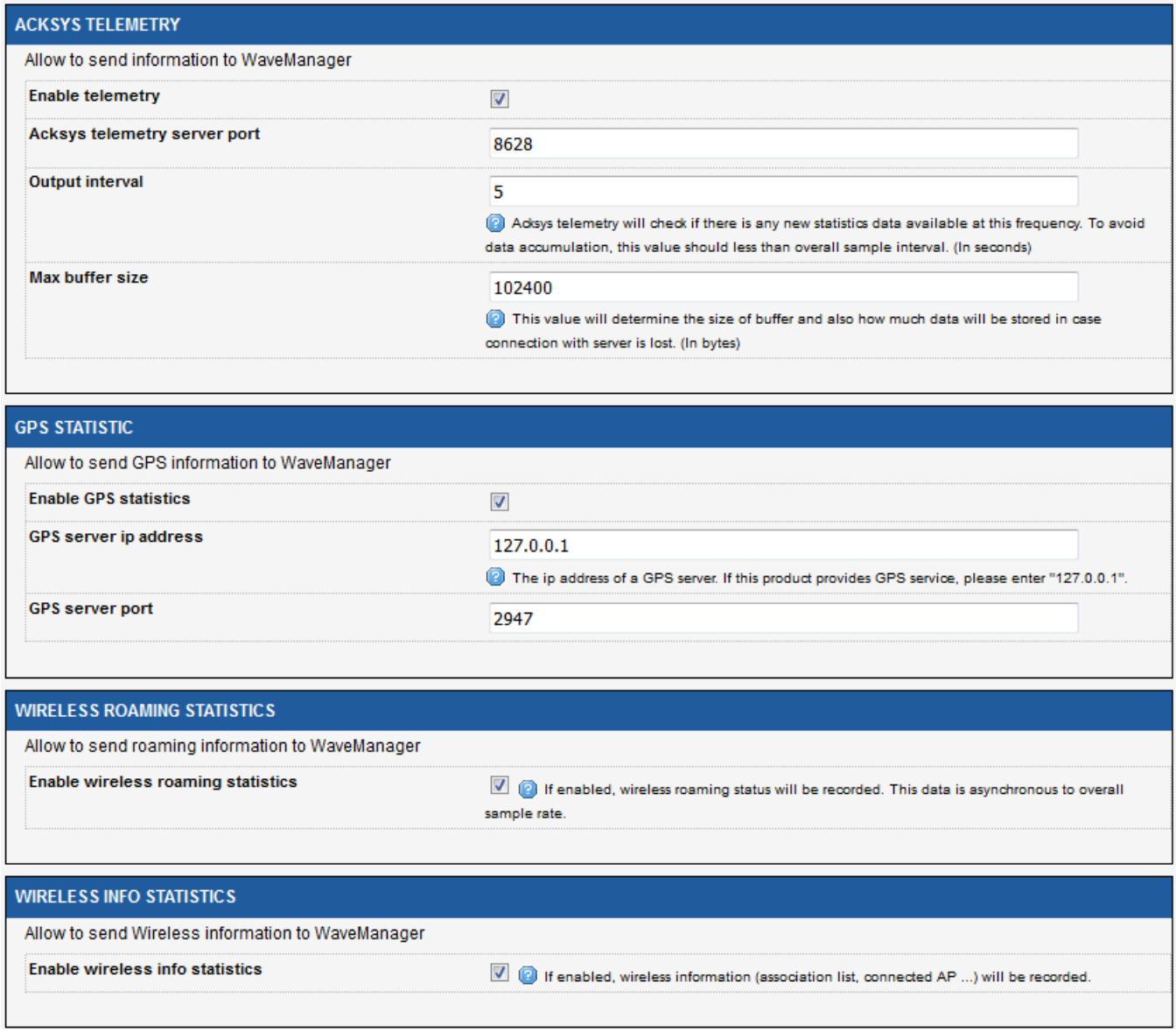


Statistic 관련 기능은 기본적으로 비활성화 되어있습니다. OVERALL SETTINGS 에서 Statistic 기능을 활성화 할 수 있습니다.



Statistic 기능이 활성화 된 경우 데이터 수집 간격을 설정할 수 있습니다. (기본값 : 30 초 간격)

그래프가 활성화 되면 제품은 무선 Client 가 AccessPoint 로부터 수신한 무선 신호 레벨과 네트워크 인터페이스의 Tx/Rx 트래픽 데이터를 실시간으로 수집합니다. STATUS 탭에서 수집된 데이터를 다양한 표시 기간과 함께 그래픽 형식으로 표시할 수 있습니다. (섹션 VI.3.2 Network, VI.3.6.1 Associated 참고)

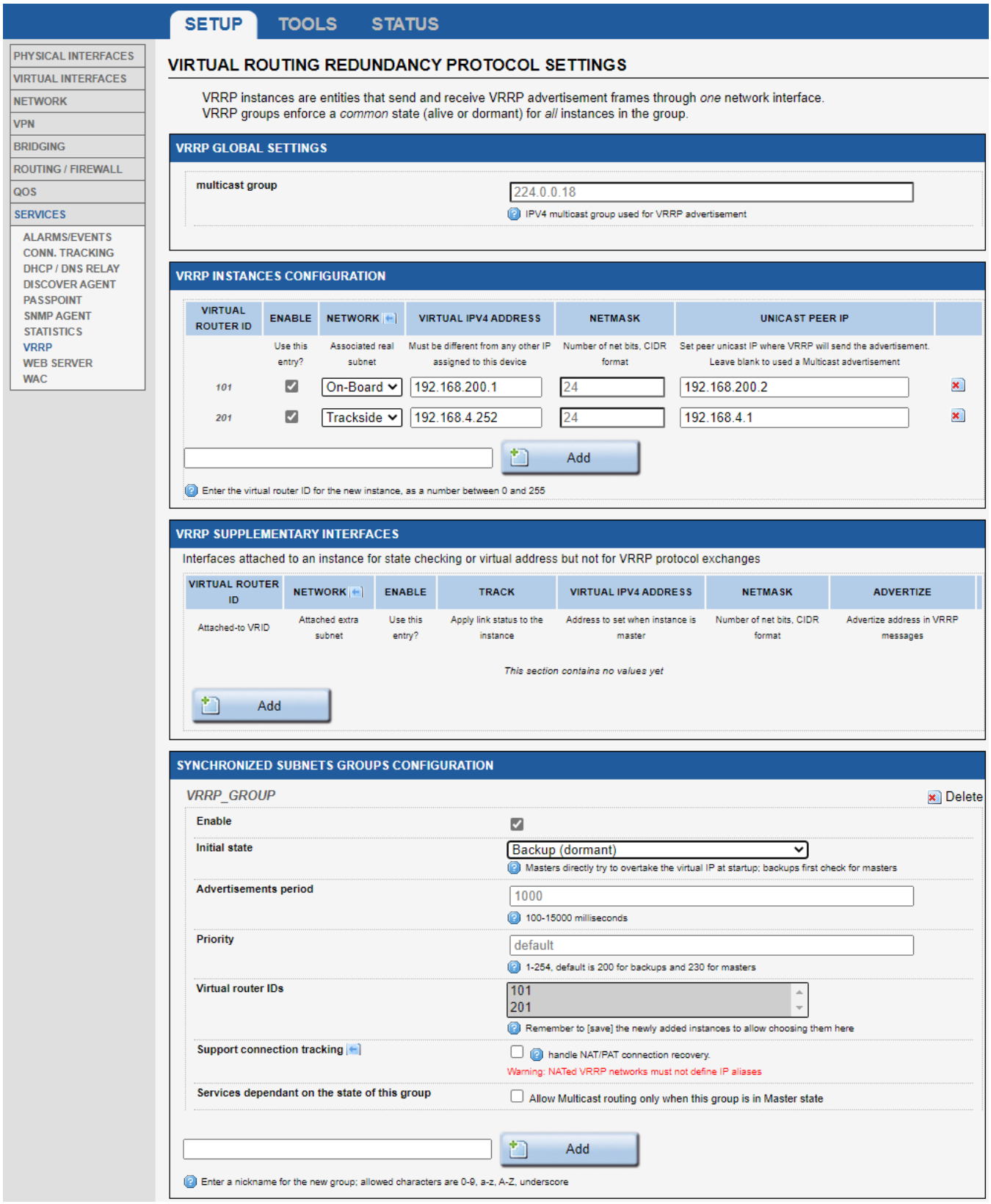


원격 측정 정보, GPS 통계, 로밍 통계 및 GPS 통계 수집은 WaveManager 소프트웨어가 실행되거나 해당 서비스가 활성화 될 때 자동으로 설정됩니다. 해당 서비스는 로컬에서 비활성화 할 수 있습니다.

VI.1.9.10 VRRP

이 탭을 통해 VRRP 인스턴스 및 관련 가상 IP 의 주소를 추가할 수 있으며 VRRP 그룹을 생성하고 해당 인스턴스와 모든 인스턴스에 공통되는 속성을 표시합니다.

인스턴스를 생성하기 위해서는 SETUP – NETWORK 탭에서 서브넷과 설정을 적용해야 합니다. 또한 NAT 또는 PAT 라우터를 사용하는 경우 **connecting tracking service** 기능을 활성화 해야 합니다. (Connection tracking 섹션 참고)



Subsection: VRRP global settings

Multicast group:
VRRP 인스턴스가 알림 메시지를 보내는 멀티캐스트 그룹을 설정합니다. 기본 그룹을 사용하려면 공란으로 두시기 바랍니다.

Subsection: VRRP INSTANCES CONFIGURATION

각 가상 IP 주소는 1 에서 255 사이의 숫자로 식별됩니다. 인스턴스를 생성하기 위해 첫 번째 하위 섹션의 맨 아래의 입력상자에 유효한 숫자를 입력한 후 **Add** 버튼을 클릭합니다. 인스턴스가 생성되면 아래의 기능을 설정할 수 있습니다.

Enable:
인스턴스를 사용하기 위해 활성화 합니다. 또한 사용하지 않는 인스턴스는 비활성화 할 수 있습니다.

Networks:
가상 IP 와 연결할 네트워크 인터페이스를 선택합니다. 인터페이스는 네트워크 장치 또는 소프트웨어 브리지일 수 있지만 손상된 링크는 소프트웨어 브리지에서 감지되지 않습니다.

Virtual IPV4 address:
해당 서브넷에 대한 라우터의 가상 IP 주소를 설정합니다.

Netmask:
가상 주소의 넷마스크를 설정합니다. (24 는 255.255.255.0 넷마스크와 동일합니다)

Unicast peer IP:
VRRP 는 멀티캐스트 대신 유니캐스트 알림을 사용할 수 있습니다. 마스터가 알림을 보내는 동안 유니캐스트 IP 주소를 사용하도록 설정해야 합니다. 멀티캐스트 알림을 사용하려면 공백으로 두십시오.

Red cross:
빨간색 **X** 아이콘을 클릭하여 인스턴스를 삭제할 수 있습니다.

Subsection: SYNCHRONIZED SUBNETS GROUPS CONFIGURATION

각 인스턴스 그룹에는 문자, 숫자, 밑줄로 구성된 이름이 지정됩니다. 하단 박스에 유효한 이름을 입력한 후 Add 버튼을 클릭하면 그룹이 생성되며 속성을 설정할 수 있습니다:

Red cross:
빨간색 **X** 아이콘을 클릭하여 그룹을 삭제할 수 있습니다.

Enable:
그룹을 활성화하거나 테스트용으로 비활성화 할 수 있습니다.

Initial state:
t 해당 그룹에 대한 제품의 의도된 역할을 반영해야 합니다.

Advertisements period:
백업으로 전송되는 두 메시지 간의 간격. 작은 값은 오류 감지를 가속화 하지만 네트워크의 부하는 증가합니다.

Priority:

여러 개의 백업을 설정할 때 협상에 사용됩니다. 기본값은 초기 역할에 따라 적절한 값을 할당합니다.

Virtual router IDs:

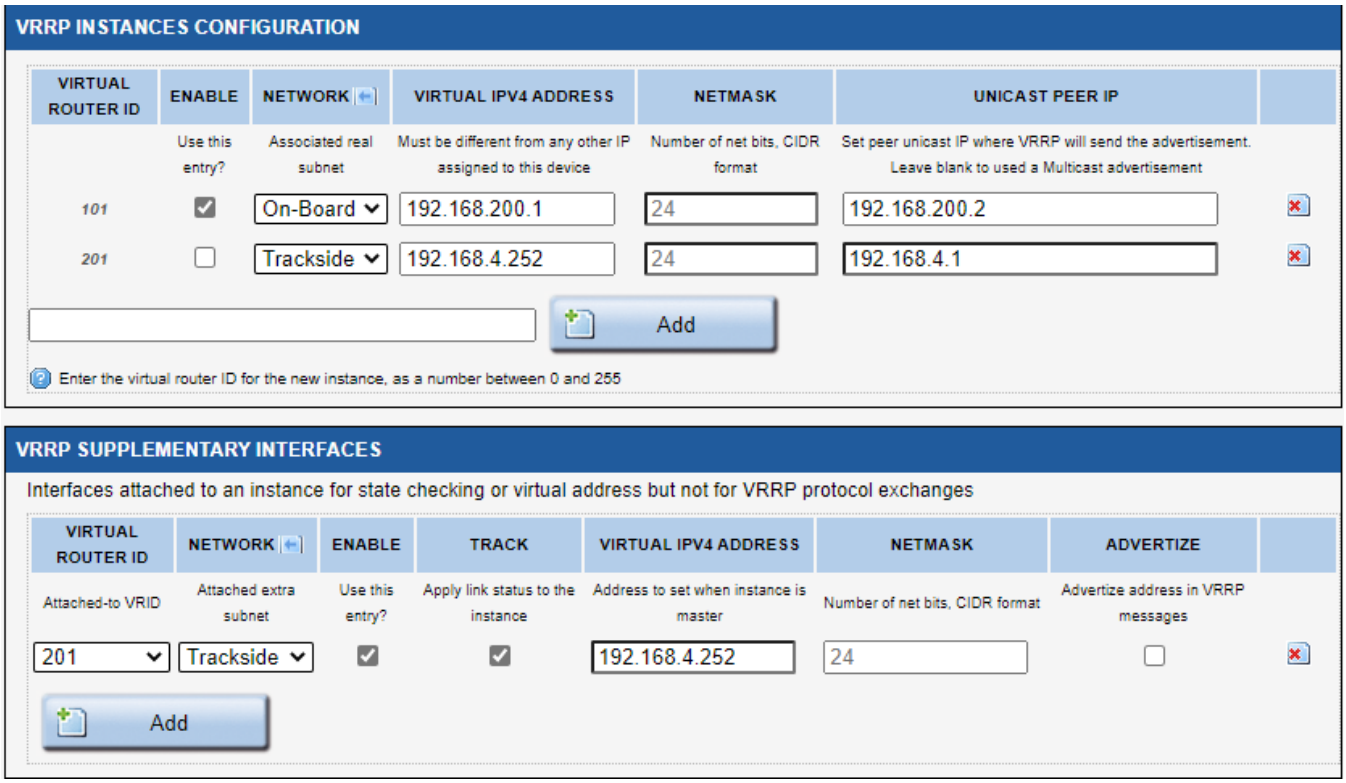
그룹에서 인스턴스를 선택할 수 있는 다중 선택 박스입니다.

Support connection tracking:

활성 라우터에서 비활성 라우터로 연결 정보를 전송하려면 선택합니다.

Subsection: SYNCHRONIZED SUBNETS GROUPS CONFIGURATION

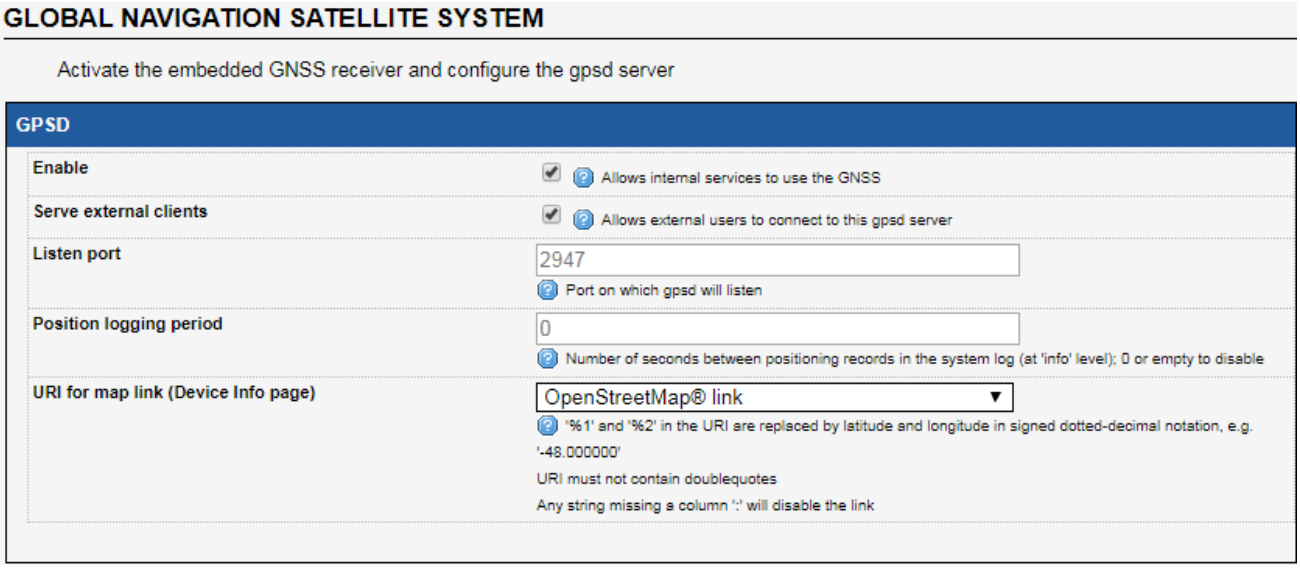
이 섹션에서는 상태 확인 또는 가상 주소를 위해 인스턴스에 연결된 추가 인터페이스를 정의할 수 있지만 프로토콜 교환에는 사용되지 않습니다. 이것은 특히 특정 인터페이스에서 광고를 보내는 것을 방지합니다. 예를 들어 여기서는 On-Board 인터페이스에만 광고를 보내고 Trackside 인터페이스는 더 이상 이 목적으로 사용되지 않습니다.



ID 201 모델에 광고 없는 추가 인터페이스를 생성한 후 구성 섹션에서 제거할 수 있습니다. 그러나 적어도 테스트 단계에서는 단순히 비활성화(활성화 확인란)하는 것이 유용할 수 있으며 이 경우 그룹의 가상 라우터 ID(동기화된 서브넷 그룹 구성 섹션)에서 ID 101 만 선택합니다.

VI.1.9.11 GNSS Agent (on some models)

GNSS agent 에 대한 설정을 변경할 수 있습니다.



Enable

location service 의 사용을 허용합니다.

Serve external clients

외부 장치가 GPSD 프로토콜을 사용하여 위치를 쿼리 할 수 있도록 합니다. 비활성화된 경우에도 SNMP 를 사용하여 위치를 쿼리 하거나 STATUS-Device Inforamtaion 페이지에 표시 또는 외부 로그 서버에 기록할 수 있습니다.

Listen port

외부 Client 의 TCP 서버 포트를 변경합니다.

Position logging period

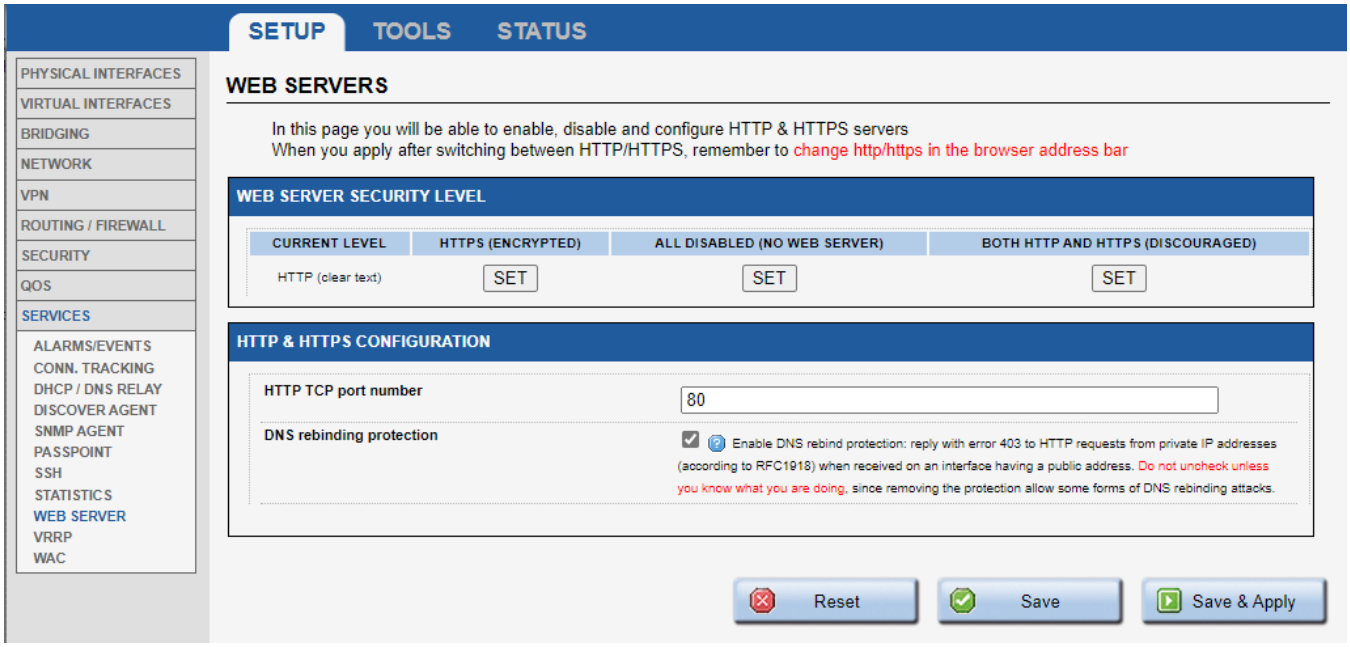
시스템 Log 에 현재 위치를 표시하는 항목을 주기적으로 추가합니다.

URI for map link

STATUS-Device Information 페이지에 표시되는 현재 위치는 웹 링크에 포함되어 있습니다. 예)외부 서비스를 사용하여 지도 표시. 또한 공공 서비스 중에서 선택하거나 선호하는 웹 서버에 대한 링크를 설정할 수 있습니다. 링크를 완전히 비활성화 하려면 사용자를 선택하고 대시(-) 또는 해시 마크를 입력합니다. %1 는 위도 %2 는 경도로 표시됩니다.

VI.1.9.12 Web Server

이 메뉴를 통해 HTTP 및 HTTP 서버를 설정할 수 있습니다. (기본값 : **HTTP)**:



HTTP TCP port number

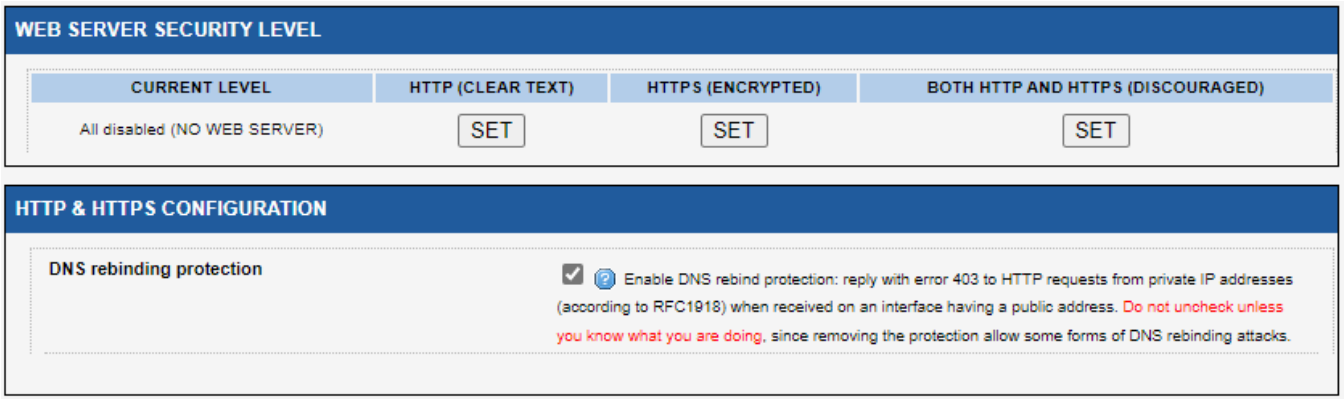
포트 번호를 변경할 수 있습니다. (기본값 : **80**)

DNS rebinding protection

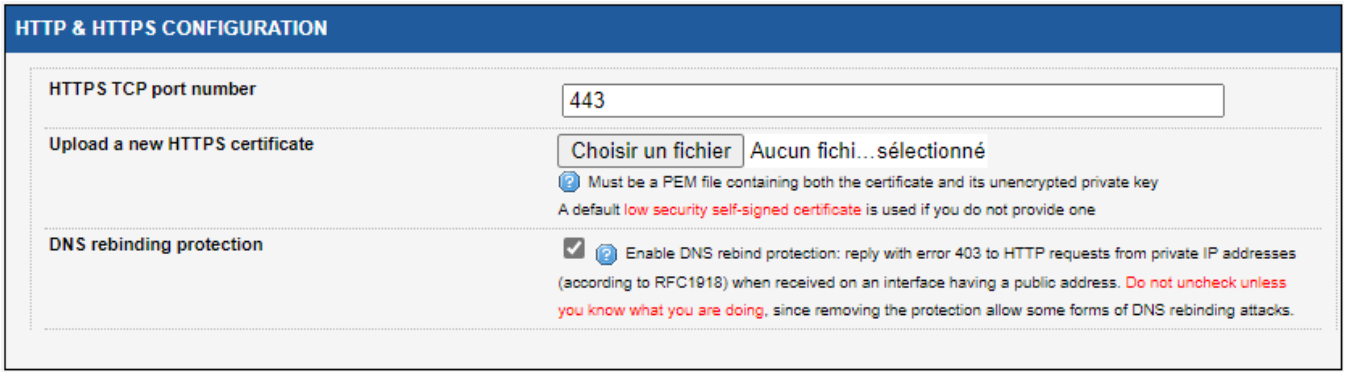
DNS rebinding protection option 을 체크하면 WEB 서버에 대한 private 주소의 연결을 금지하는 RFC 1918 기능을 사용할 수 있습니다. 예를 들어 제품이 public 주소 82.128.0.30 으로 설정되어 있을 경우, priate 주소 192.168.1.40 에서 이 제품의 WEB 페이지를 확인할 수 없으며 403 오류가 발생합니다.

SET 버튼을 클릭하여 다른 옵션을 선택할 수 있습니다:

All disabled (NO WEB SERVER)



HTTPS (암호화)



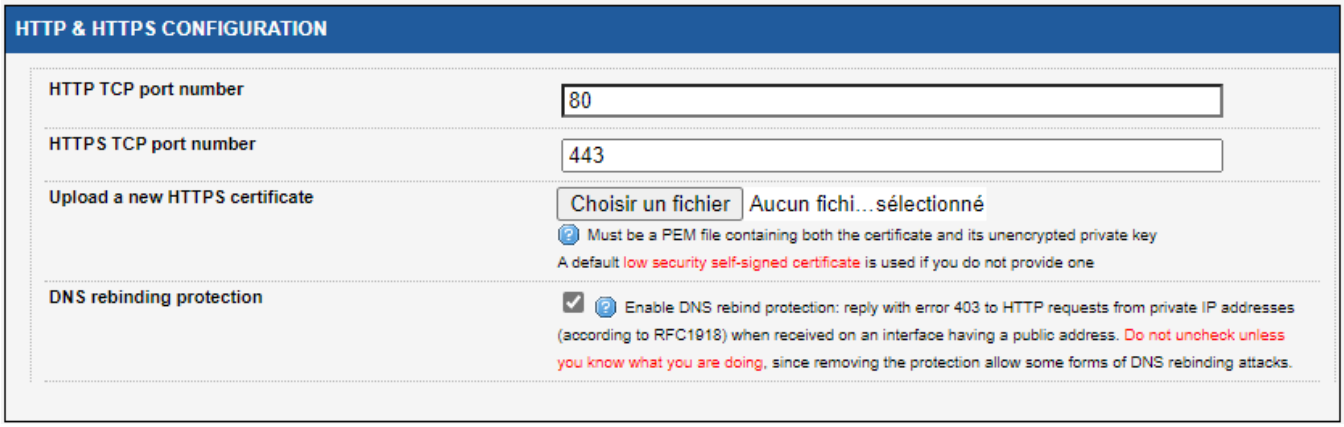
HTTPS TCP port number

HTTP 인증서를 업로드 할 수 있으며 다른 포트를 사용할 수 있습니다. (기본값 : **443**)

Upload a new HTTPS certificate

HTTPS 서버의 경우 PEM 형식의 웹 인증서 파일을 업로드 할 수 있습니다. Save 또는 Save & Apply 버튼을 클릭하면 인증서 파일이 적용 및 업로드 됩니다.

Both HTTP and HTTPS (discouraged)



HTTP TCP port number

기본 포트 및 다른 포트를 설정할 수 있습니다. (기본값 : 80)

HTTPS TCP port number

기본 포트 및 다른 포트를 설정할 수 있으며 HTTPS 인증서를 업로드 할 수 있습니다. (기본값 : 443)

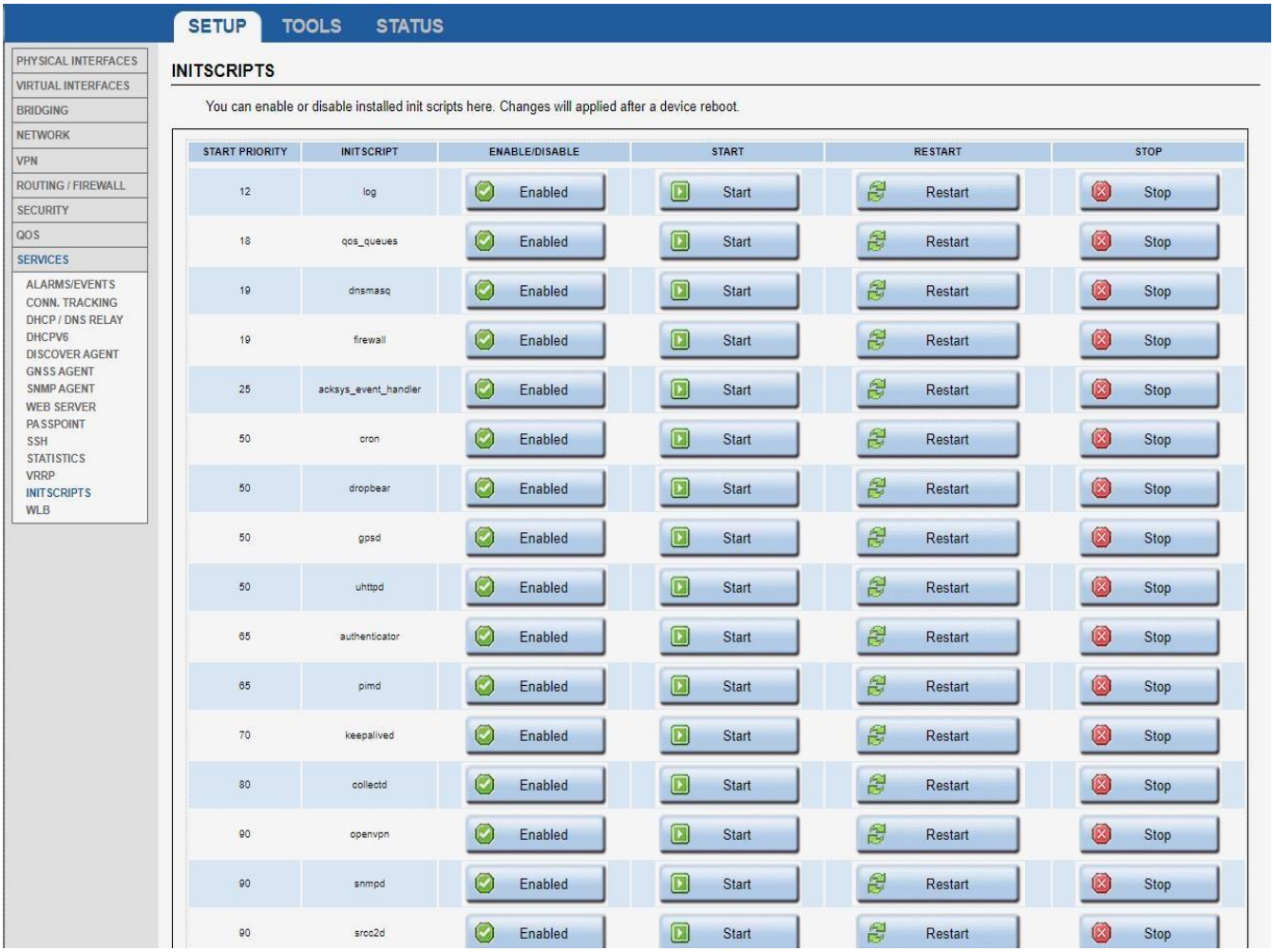
Upload a new HTTPS certificate

HTTPS 서버의 경우 PEM 형식의 웹 인증서 파일을 업로드 할 수 있습니다. Save 또는 Save & Apply 버튼을 클릭하면 인증서 파일이 적용 및 업로드 됩니다.

VI.1.9.13 INIT SCRIPTS

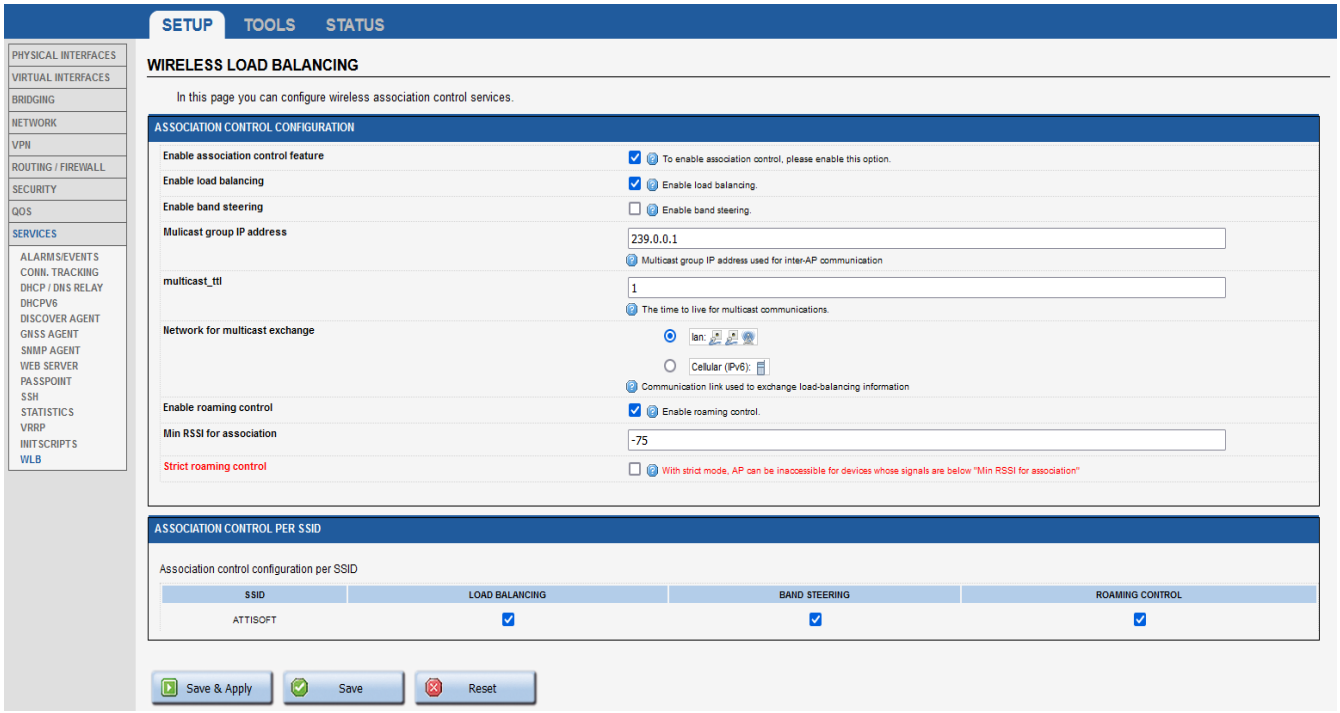
SERVICES/INIT SCRIPTS 메뉴를 사용하면 다음과 같이 설치된 일부 필수 스크립트를 관리하고 모니터링할 수 있습니다.

- 서비스 우선 순위 보기
- 서비스명 보기
- 서비스 활성화/비활성화
- 서비스 시작/재시작/중지



VI.1.9.14 WLB

SERVICES/WAC 메뉴를 통해 WLAN 의 연결 및 제어 시스템을 설정할 수 있습니다.



ASSOCIATION CONTROL CONFIGURATION

Enable association control feature

해당 체크 박스를 체크하면 WAC 설정을 위한 설정 화면이 표시됩니다.

Enable load balancing

해당 체크 박스를 체크하면 load balancing 기능을 활성화 할 수 있습니다:

Multicast group IP address

AP 는 동일한 Multicast 그룹에 속한 다른 AP 에 프로브 데이터를 전송합니다. 사용자는 Multicast 그룹 IP 주소를 설정할 수 있습니다. (기본값 : 239.0.0.1)

Multicast_TTL

기본적으로 프로브는 멀티캐스트에서 LAN 으로 전송됩니다. (기본값 : TTL=1) 또한 ***probe announcements*** traverse 라우터, 다른 LAN 에 속하는 AP 를 생성하도록 TTL 을 구성할 수 있습니다.

Network for multicast exchange

probe announcements 가 advertised 될 네트워크를 선택하세요.

load balancing 기능을 사용할 경우, General Setup, Access Point Mode 페이지의 **Maximum simultaneous associations** 를 설정해야 합니다.

Enable band-steering

해당 체크 박스를 체크하면 밴드 스티어링을 활성화 할 수 있습니다. 해당 기능을 사용하면 듀얼 밴드를 지원하는 STA 가 혼잡하지 않은 대역으로 이동됩니다.

Enable roaming control

해당 체크 박스를 체크하면 로밍 설정을 위한 설정 화면이 표시됩니다:

Min RSSI for association

roaming control 이 활성화 되어 있을 경우, STA 가 연결되어 있지 않은 RSSI 임계값을 설정해야 합니다. 연결 요청은 설정된 RSSI 임계값을 초과할 때만 적용됩니다.

Strict roaming control

Strict 모드는 로밍 동작에 영향을 줄 수 있습니다:

Association with Strict mode enabled:

무선 장치가 **Min RSSI for association** 보다 낮으면 연결되지 않습니다.

Association with Strict mode disabled:

AP 는 **Min RSSI for association** 보다 낮은 RSSI 값을 가진 Client 의 첫 번째 연결 시도를 거부합니다. 또한 장치가 동일한 AP 에 두 번째로 연결할 경우 AP 는 연결 시도를 무조건 수락합니다. 이러한 장치를 **insited 장치**라고 부릅니다.

De-association with Strict mode enabled:

Min RSSI for associaation 보다 작은 5 개의 샘플 신호가 연속적으로 발생할 경우 AP 는 즉시 장치의 연결을 해제합니다.

De-association with Strict mode disabled:

- AP 는 연속된 5 개의 샘플 신호 중 하나라도 **Min RSSI for association** 보다 낮은 경우 무조건 적으로 장치와의 연결을 유지합니다.
- 마지막 5 개의 샘플 신호가 **Min RSSI for association** 보다 높을 경우 **insited 장치**는 제거됩니다.
- **non-insited 장치 (일반 장치)** 의 경우, 5 개의 샘플 신호가 모두 **Min RSSI for association** 보다 낮으면 연결을 해제합니다.

샘플 신호는 3 초의 주기로 통신됩니다.

ASSOCIATION CONTROL PER SSID

Load balancing, band-steering, roaming control 은 SSID 별로 적용됩니다. 따라서 각 기능을 SSID 별로 활성화 및 비활성화 할 수 있습니다.

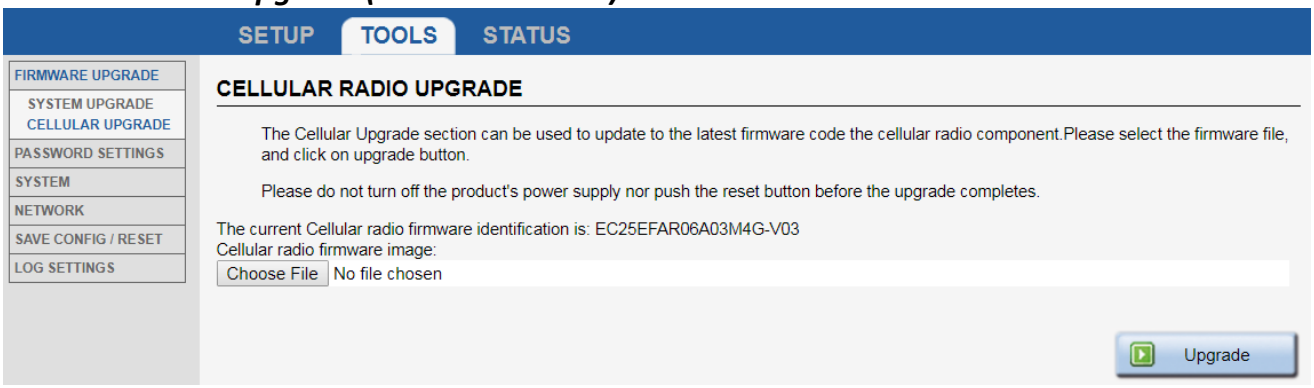
VI.2 Tools Menu

TOOLS 탭을 통해 제품을 관리 할 수 있습니다:

VI.2.1 Firmware upgrade

펌웨어 업그레이드에 대한 자세한 설명은 *Firmware Upgrade* 에서 확인이 가능합니다.

VI.2.1.1 Cellular upgrade (on some models)

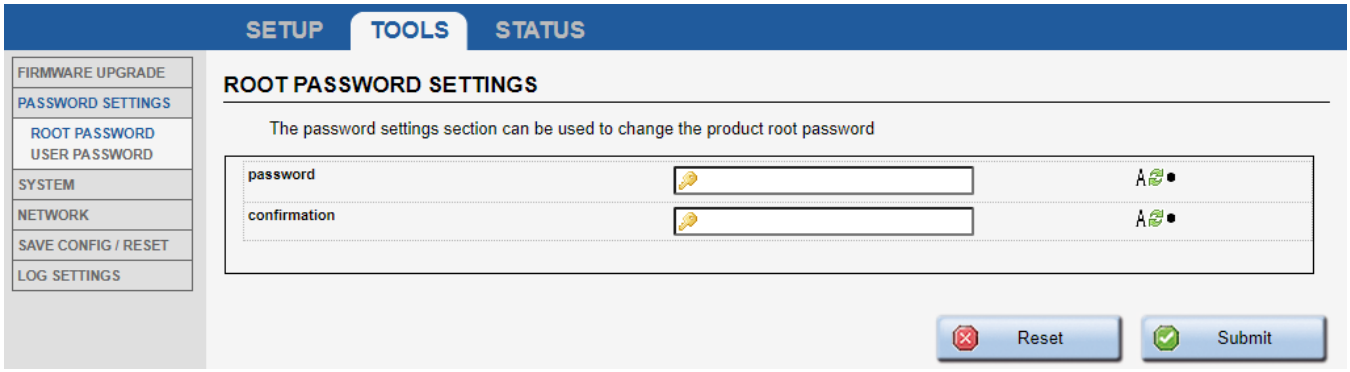


Cellular 모듈이 내장된 제품의 펌웨어 업그레이드를 할 수 있습니다.

당사 홈페이지 및 엔지니어의 지원을 받지 않고 Cellular 펌웨어를 업데이트 하지 마세요. 또한 제품에 맞는 Cellular 펌웨어 ID 를 확인하시기 바랍니다.

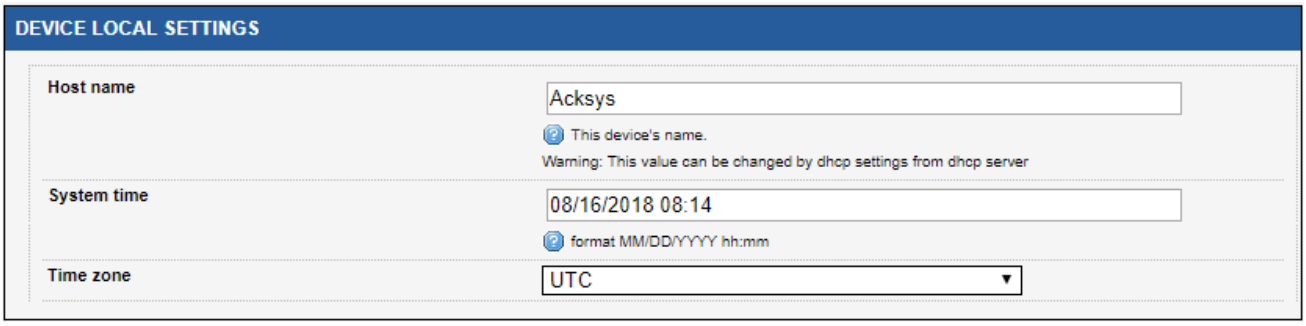
VI.2.2 Password Settings

이 메뉴를 통해 제품의 암호를 설정할 수 있습니다. USER 는 STATUS 페이지만 접속할 수 있습니다. ROOT 는 모든 설정 페이지 (SETUP, TOOLS, STATUS) 에 접속할 수 있습니다.



VI.2.3 System

VI.2.3.1 Device Local settings



Host Name:

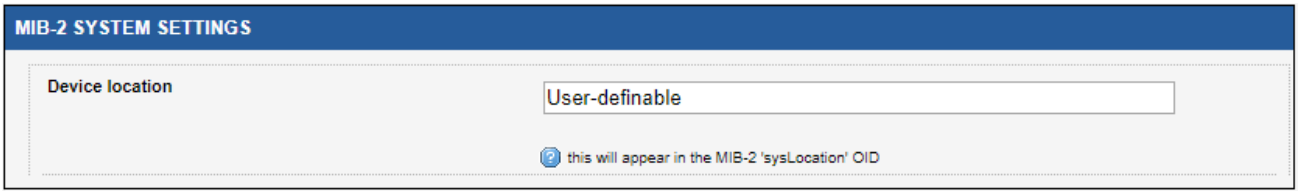
장치의 이름을 설정할 수 있습니다. 해당 이름은 STATUS 페이지에서 표시됩니다. 또한 DHCP Client 장치가 구성되면 DHCP 설정을 변경할 수 있습니다.

System time and Time Zone:

현재 시간을 설정하고 Time Zone 표준 시간을 선택할 수 있습니다.

주의 : 제품을 재부팅할 때마다 로컬 시간 설정이 손실됩니다. 필요한 경우 타임서버를 사용해주시기 바랍니다.

VI.2.3.2 MIB-2 System Settings



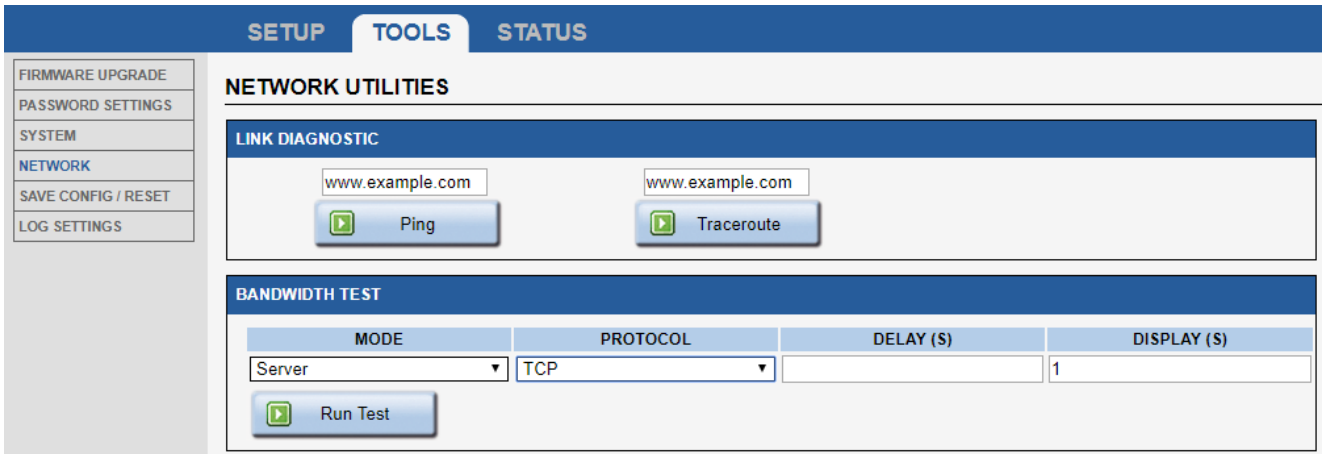
Device Location:

이 텍스트는 WaveManager 소프트웨어의 **Location** 열, SNMP **sysLocation** 값, Browser caption 에 표시됩니다.

VI.2.3.3 Network Timer Server

네트워크에서 NTP 서버에 연결할 수 있는 경우, 이 메뉴를 통해 로컬 시간을 구성할 수 있습니다. IP 주소와 도메인 이름을 사용할 수 있습니다. 도메인 이름을 사용하려면 Network configuration 탭에서 하나 이상의 DNS 서버 주소를 입력해야 합니다.

VI.2.4 Network Utilities



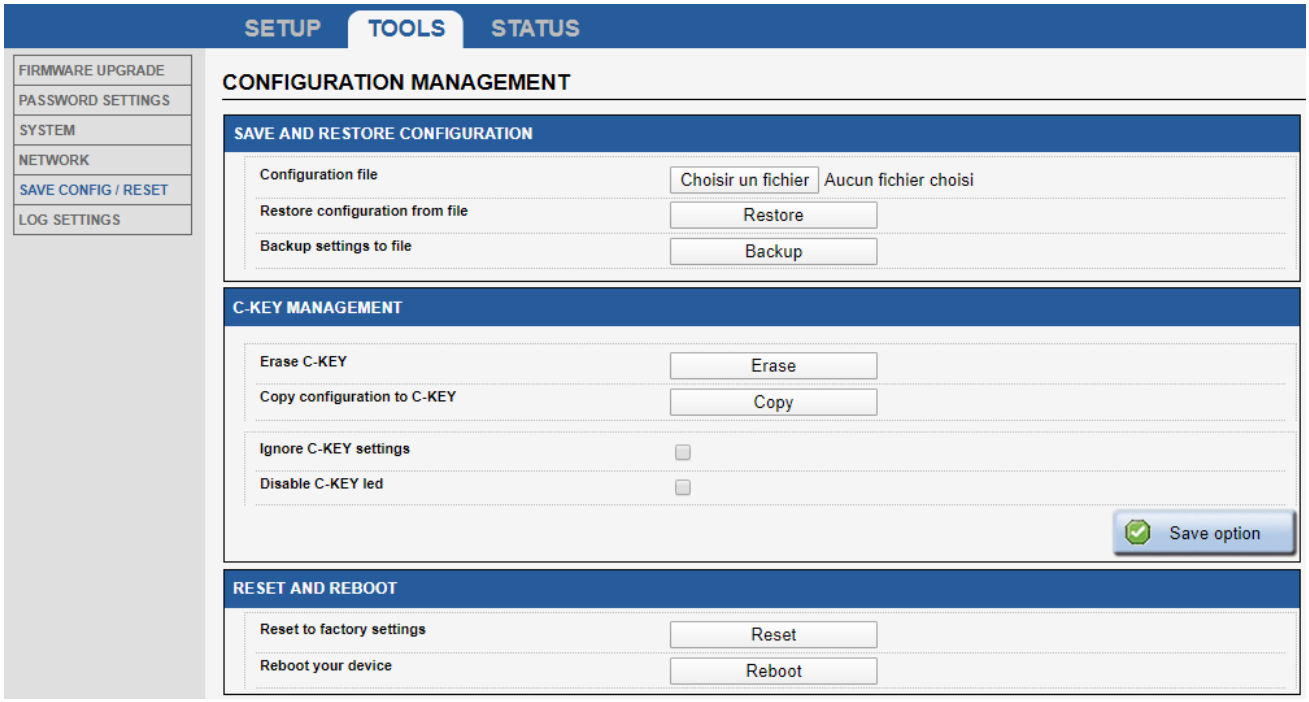
LINK DIAGNOSTIC:

표준 UNIX 도구인 Ping 과 Traceroute 를 입력한 후 버튼을 클릭하면 해당 상태 값이 아래의 프레임에 표시됩니다. IP 주소와 도메인 이름을 사용할 수 있습니다. 도메인 이름을 사용하려면 Network configuration 탭에서 하나 이상의 DNS 서버 주소를 입력해야 합니다.

BANDWIDTH TEST:

TCP 또는 UDP 프로토콜을 사용하여 서버 또는 클라이언트 모드에서 iPERF 테스트를 할 수 있습니다. **DELAY** 탭은 테스트 간격을 초 단위로 설정할 수 있으며 **DISPLAY** 탭은 상태 표시 간격을 초 단위로 설정할 수 있습니다.

VI.2.5 Save Config / Reset



Save And Restore Configuration:

backup settings to file 버튼을 클릭하여 제품의 설정 파일을 생성하여 다운로드 받을 수 있습니다. 또한 **Restore configuration from file** 버튼을 클릭하여 이전에 저장한 설정 파일을 업로드 하여 적용할 수 있습니다.

C-KEY Management:

Erase C-KEY:

이 옵션을 사용하면 해당 제품의 C-KEY 의 내용이 전부 지워집니다. 설정값을 C-KEY 에 처음으로 저장 하기 전에 이 작업을 수행해야 합니다.

Copy configuration to C-KEY:

이 옵션을 사용하면 현재 설정값이 C-KEY 에 저장됩니다. 이전에 저장되어 있던 데이터는 백업으로 보관되며 새 설정값이 손상된 경우 백업이 대신 로드 됩니다.

WARNING: WPA 키와 다양한 인증서(802.1x, HTTPS)도 복사됩니다. 관리 암호가 정의되지 않은 경우, C-키를 소유한 사람은 누구나 이 정보를 추출할 수 있습니다.

Ignore C-KEY setting:

이 옵션을 사용하면 제품 부팅 시 C-KEY 의 설정값을 읽어오지 않습니다. 또한 제품 부팅 시 C-KEY 의 내부 설정값을 덮어씁니다(기본값)

Disable C-KEY led:

이 옵션을 선택하면 C-KEY 의 Status LED 가 영구적으로 꺼집니다. 이 기능은 C-KEY 가 없을 때 표시되는 LED 를 표시하지 않을 때 유용하며 소비 전력을 약간 줄이는데도 사용할 수 있습니다.

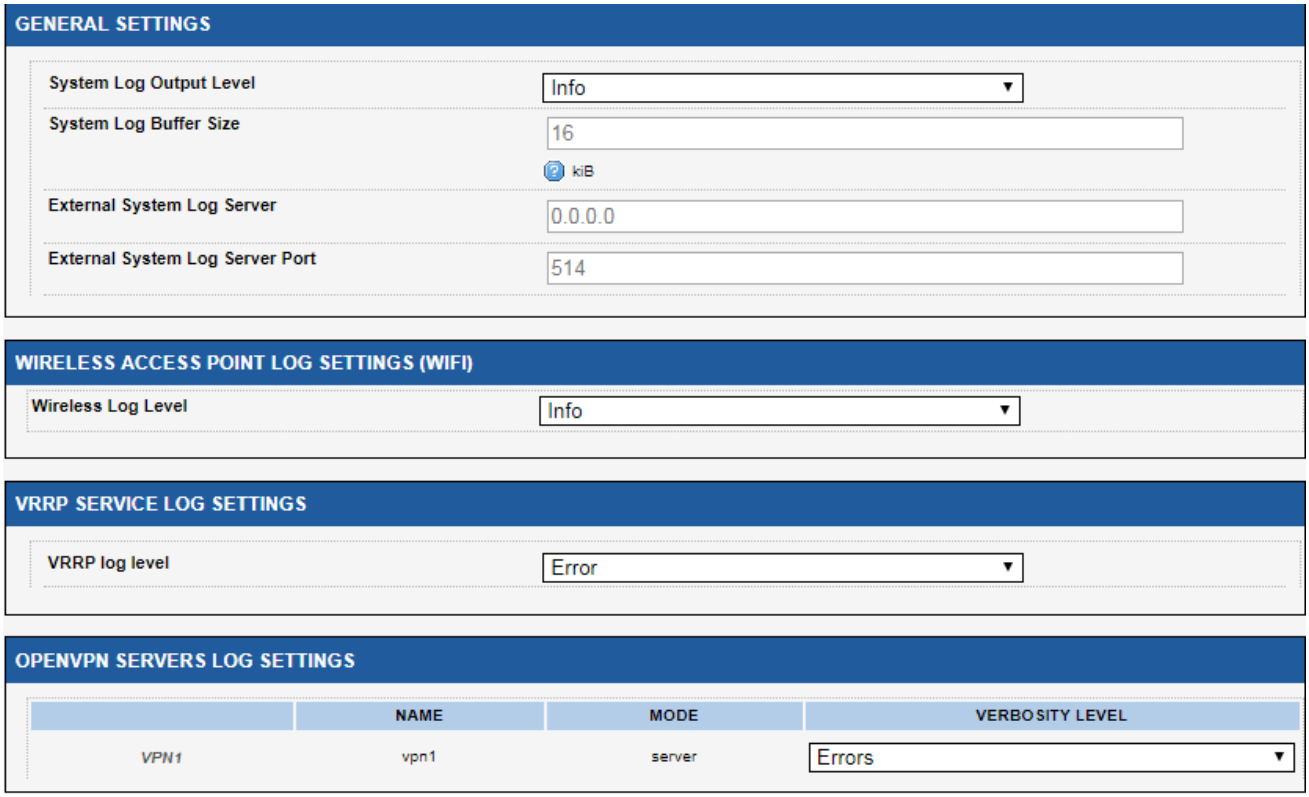
Reset And Reboot:

Reset to factory settings:
현재 동작 중인 제품이 기본 설정 값으로 복원됩니다.

Reboot your device:
현재 동작 중인 제품이 재 부팅됩니다.

VI.2.6 Log Settings

이 페이지에서 Log 구성을 설정할 수 있습니다.



General settings:

이 탭에서는 시스템 로그에 대한 설정을 할 수 있습니다.

System Log Output Level:

system log 에 대한 로그 메시지의 최소 심각도를 설정할 수 있습니다.

External System Log Server and Port:

원격 로그 서버에 대한 설정을 할 수 있습니다. syslog 프로토콜을 사용하여 로그 메시지를 보낼 IP 주소와 UDP 포트 입니다. 이 기능을 사용하지 않을 경우 공란으로 두세요.

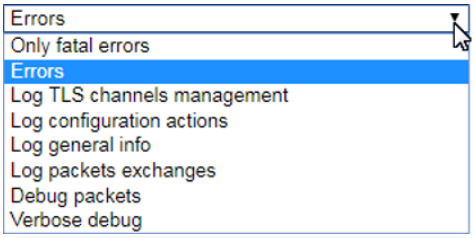
Log settings:

이 탭에서는 다양한 로그 메시지의 종류를 설정할 수 있습니다. 심각도가 설정된 수준 이상일 경우 메시지가 system log 로 전송됩니다.

따라서 로그 메시지는 각각 특정서비스 및 syslog 서비스 이 두 가지의 필터링 단계를 거칩니다. system log 가 모든 메시지를 표시할 수 있을 만큼 충분한지 확인하세요.

Verbosity Level:

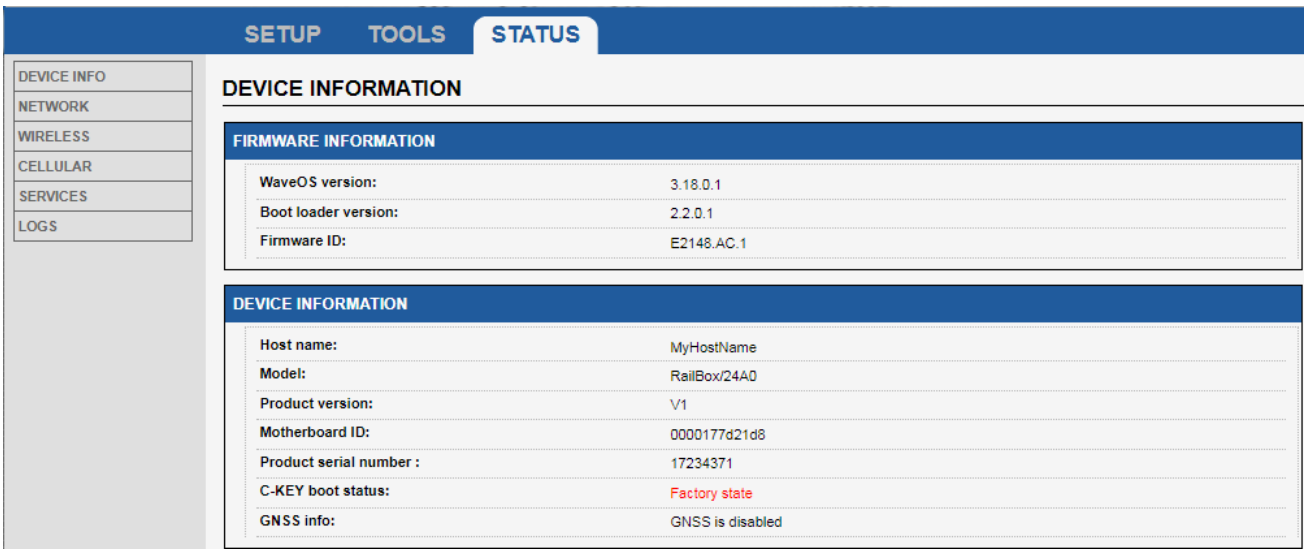
system log 00 에 삽입할 수 있는 OpenVPN 서버와 관련된 메시지의 최소 심각도를 설정합니다.



VI.3 STATUS Menu

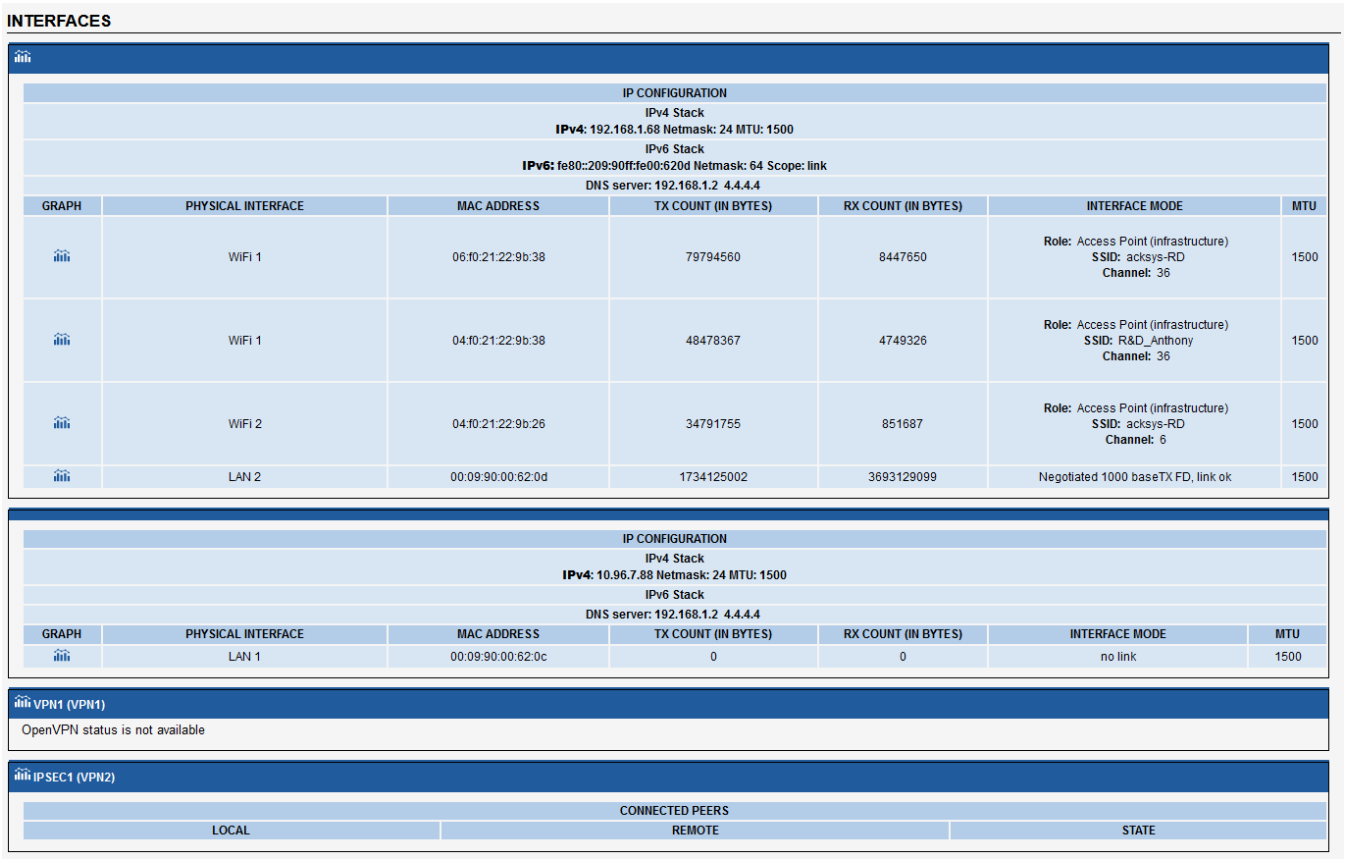
VI.3.1 Device Info

이 페이지를 통해 제품에 대한 다양한 정보를 확인할 수 있습니다.



VI.3.2 Network

이 페이지는 네트워크 인터페이스의 구성이 요약되어 있으며 데이터 패킷을 확인할 수 있습니다.

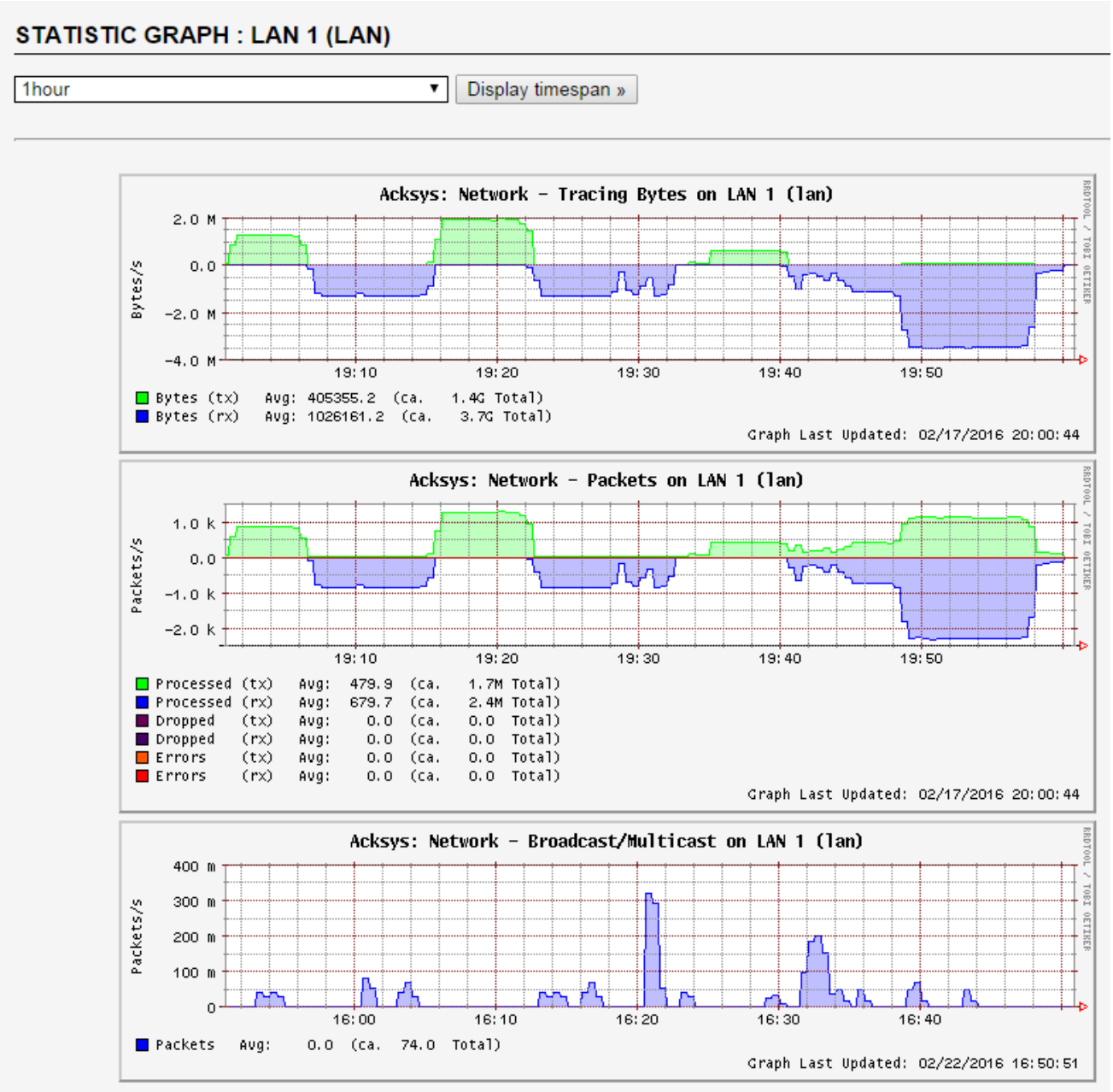


Graph:

: SETUP 메뉴 (SERVICES/COUNTER GRAPHS) 에서 그래프 기능이 비활성화 되어 있을 경우 히스토리 그래프를 사용할 수 없습니다.

: 인터페이스의 히스토리 그래프를 사용할 수 있습니다.

: 브릿지된 네트워크의 히스토리 그래프를 사용할 수 있습니다.



이 페이지는 인터페이스 LAN 1 의 기록 그래프를 표시합니다:

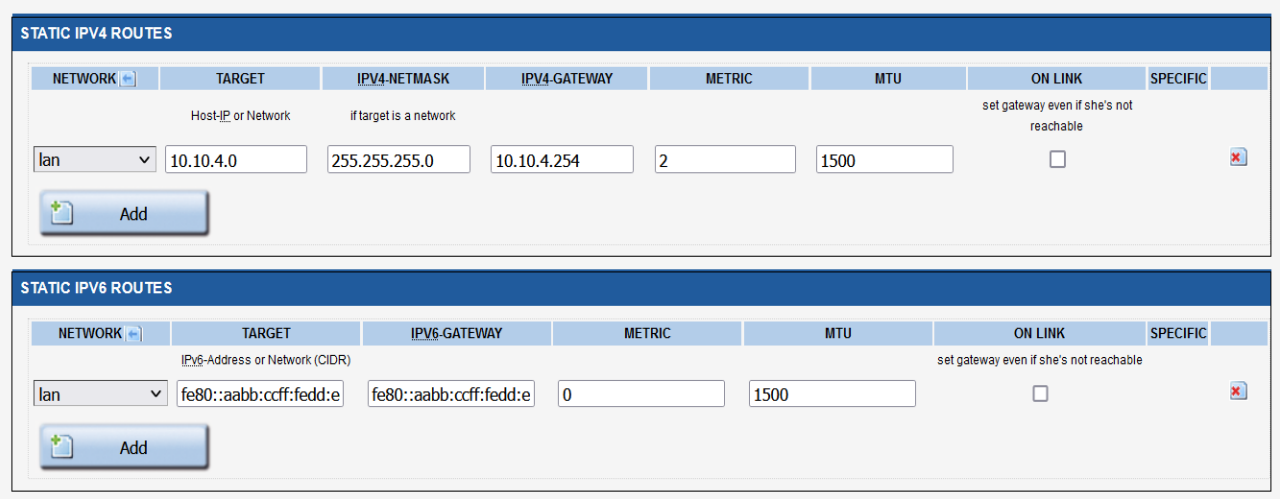
Tracing bytes graph: 데이터 송수신 패킷 표시

Packets graph: 데이터 송수신 처리, 삭제, 오류의 패킷 표시

Broadcast/Multicast graph: broadcast/multicast 의 패킷 표시

또한 표시 기간을 10 분, 1 시간, 1 일, 1 주, 1 개월 단위로 설정할 수 있습니다.

VI.3.3 Routes

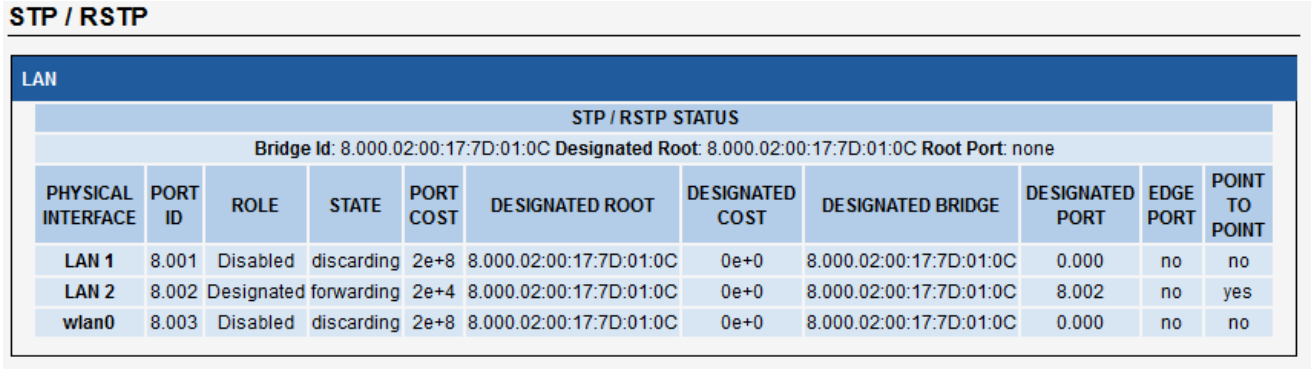


이 페이지는 제품에서 활성화된 활성 IPV4 경로 및 IPV6 경로를 표시합니다.

	필드 이름	샘플 값	설명
1.	Network	loopback	사용된 네트워크 인터페이스
2.	Target	0:0:0:0:0:0:0:0/0	특정 IP 주소를 가진 TCP/IP 패킷이 전달되어야 하는 위치를 나타냅니다.
3.	IPv6-Gateway	0:0:0:0:0:0:0:0/0	TCP/IP 패킷이 전달되어야 하는 게이트웨이를 나타냅니다.
4.	Metric	FFFFFFFF	사용의 인터페이스 우선 순위를 나타내는 메트릭 번호

VI.3.4 Bridges

STP/RSTP 가 활성화 된 Bridge 가 있는 경우 STP/RSTP 의 포트 상태가 표시 됩니다.



Physical interface: Bridge 의 포트

Port Id: 지정된 포트의 식별 ID 로써 포트 우선 순위와 인터페이스 번호로 구성됩니다.

Role: Rapid Spanning Tree 기능은 각 Bridge 포트에 Root 포트, Designated 포트, Alternate 포트, Backup 포트, Disabled 포트 중 하나를 할당합니다. Disabled 포트는 포트가 동작되지 않거나 관리자에 의해 제외된 경우에 할당됩니다.

State: port forwarding 상태:

For RSTP: discarding, learning or forwarding 을 할 수 있습니다.

For STP: disabled, blocking, listening, learning or forwarding 을 할 수 있습니다.

Port Cost: 기본적으로 포트 속도에 따라 STP/RSTP 에서 설정할 수 있습니다.

Designated Root: Spanning tree 의 Root 브리지 입니다. root 브리지의 우선 순위 및 기본 MAC 주소를 사용하여 설정합니다.

Designated Bridge: 지정 포트를 포함하는 브리지 입니다. 이 주소는 해당 브리지의 우선 순위(Priority) 및 기본 MAC 주소로 구성됩니다.

Designated port: LAN 에 연결된 모든 브리지 포트 중 지정된 역할을 가진 포트(현재 포트 및 인접 브리지 포트 포함)입니다. 포트 우선 순위와 포트의 인터페이스 번호로 구성됩니다.

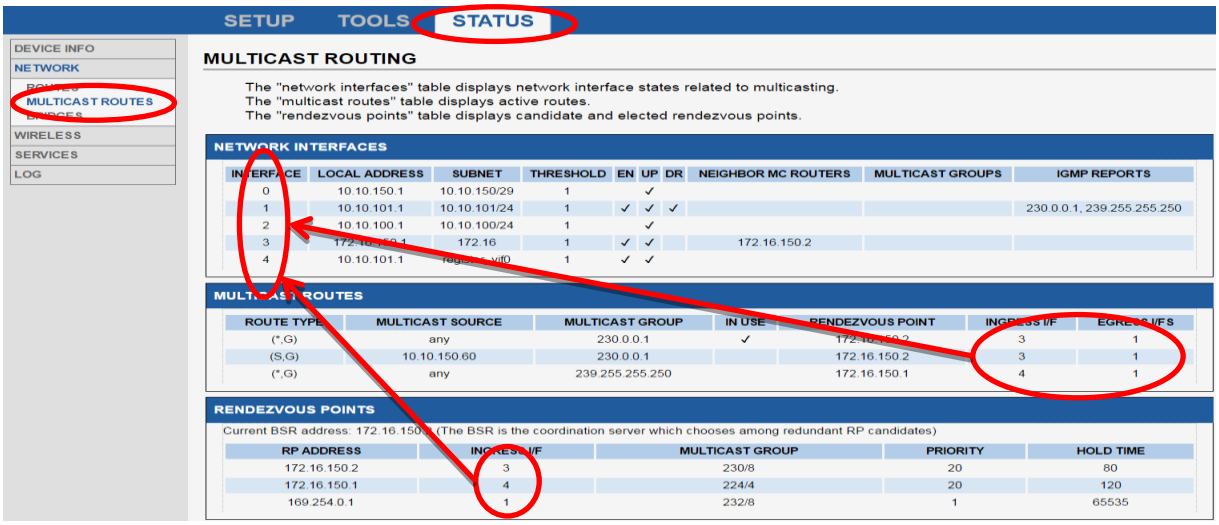
Designated Cost: 지정 포트를 통해 루트 브리지의 Path cost (지정 포트 및 루트 브리지 간의 각 브리지에 대한 루트 포트의 port cost 합계)

Edge port: 포트가 토폴로지의 엔드스테이션 위치 유무에 따라 true 및 false 로 설정합니다.

Point to Point: 포트가 지점간 미디어 (케이블을 사용하는 다른 스위치에 직접 연결됨)에 연결되어 있을 경우 true 로 설정되며 그렇지 않을 경우 false 로 설정됩니다.

VI.3.5 Multicast routes

이 페이지를 통해 현재 실행 중인 PIM 멀티 캐스트 라우터 인스턴스의 사용 가능한 모든 정보가 표시됩니다.



a. Network interfaces section

Interface: ingress/egress 열에서 참조되는 네트워크 번호 입니다.

Local address: Setup/Network 페이지에서 네트워크에 할당된 Unicast IP 주소. (Unicast: 특정 수신자에게 송신)

Subnet: 해당 인터페이스에 연결되는 서브넷 및 서브넷 비트 수, register_vif0 서브넷은 송신자가 캡슐화된 데이터를 rendezvous point 로 전송하는 특수 인터페이스입니다.

Threshold: 인터페이스에 데이터를 전달하는 데 필요한 최소 TTL

EN: 해당 인터페이스에서 멀티캐스팅을 사용할 수 있습니다.

UP: 해당 인터페이스를 사용할 수 있습니다 (예 : RJ45 커넥터가 연결됨)

DR: 해당 라우터는 해당 네트워크에 의해 설계

Neighbor MC routers: 별도의 PIM 라우터가 해당 네트워크에 직접 연결 되어있습니다.

Multicast groups: 해당 인터페이스에서 처리된 PIM-SSM 그룹.

IGMP reports: 수신자가 해당 로컬 네트워크에서 가입 요청을 보내는 그룹의 목록

b. Multicast routes section

Route type: *, G: 그룹화 할 소스, S, G 그룹화 할 특정 소스

Multicast source: 수신자가 요청한 소스 : 임의 또는 특정 IP 주소

Muticast group: 경로 진입과 관련된 그룹

In use: 해당 항목은 데이터 전달에 적극적으로 사용됩니다.

Rendezvous point: 그룹에 대해 계산된 IP 주소입니다.

Ingress I/F: 멀티캐스트 데이터가 도착할 것으로 예상되는 인터페이스

Egress I/F: 멀티캐스트 데이터가 전달되어야 하는 인터페이스 목록

c. Rendezvous points section

RP address: 해당 그룹 블록에 대한 **Rendezvous point** 의 IP 주소 입니다.

Ingress I/F: 데이터가 수신되는 RP 에 대한 인터페이스

Multicast group: 해당 RP 와 연결된 그룹 블록

Priority: RP 의 우선 순위. 로컬로 구성된 그룹의 우선 순위는 1 입니다.

Hold time: 일정 시간 동안 갱신되지 않으면 해당 항목이 무효화 되는 지연 시간

- SSM 라우팅을 관리하기 위해 내부적으로 사용되는 IP 주소 169.254.0.1

VI.3.6 Wireless

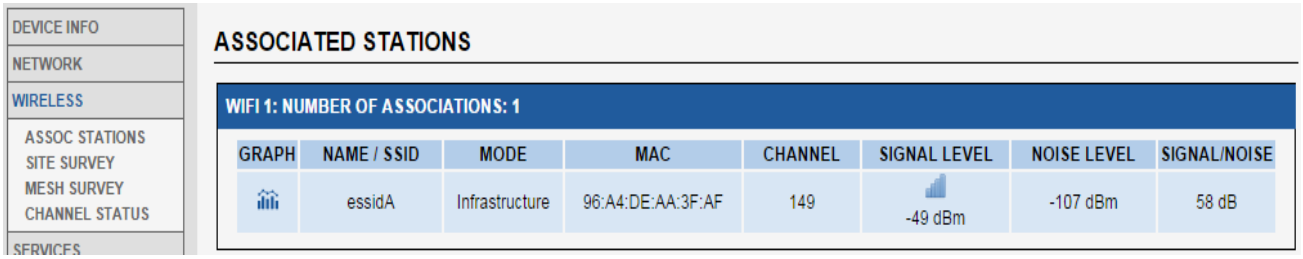
VI.3.6.1 Associated Stations

AP 모드인 경우, 현재 연결되어 있는 Client 와 RF 신호 및 정보를 확인할 수 있습니다.

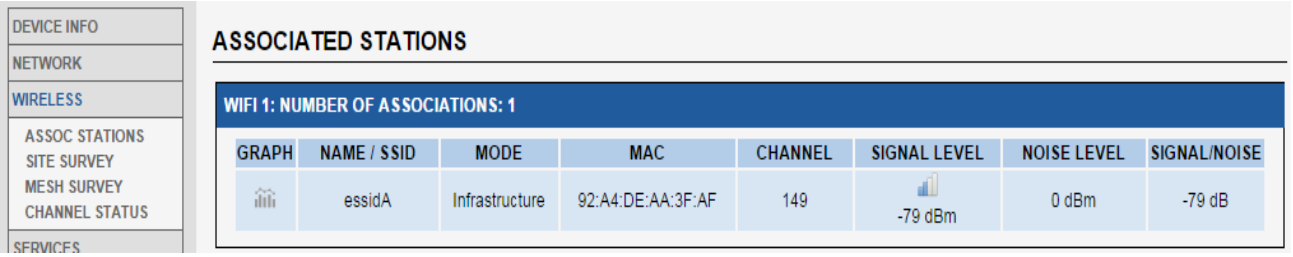
Client 모드인 경우, AP 와 연결되면 해당 RF 세부 정보가 나옵니다. 또한 Signal level 은 트래픽에 따라 많이 변경될 수 있습니다.

표시되는 신호 레벨은 유형(데이터 또는 관리) 또는 변조 종류에 관계없이 수신된 마지막 프레임에서 얻은 것입니다. 따라서 프로브 프레임과 비콘 프레임에만 해당하는 사이트 조사에 나타나는 값과 비교할 수 없습니다.

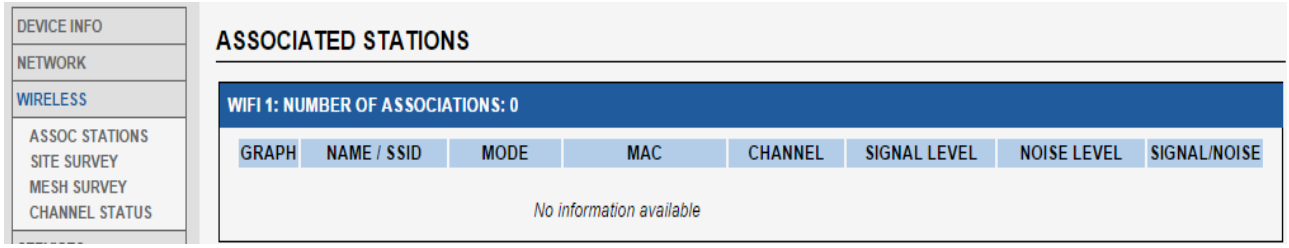
또한 신호 수준은 트래픽에 따라 많이 달라질 수 있습니다. 높은 MCS 값으로 데이터가 수신되면 일반적인 송신기가 고속에서 덜 강력하기 때문에 신호가 낮을 수 있습니다. 데이터가 수신되지 않으면 저속 비콘에서 가져오기 때문에 신호가 발생할 수 있습니다.



Client 모드에서의 AccessPoint 와 연결 예시

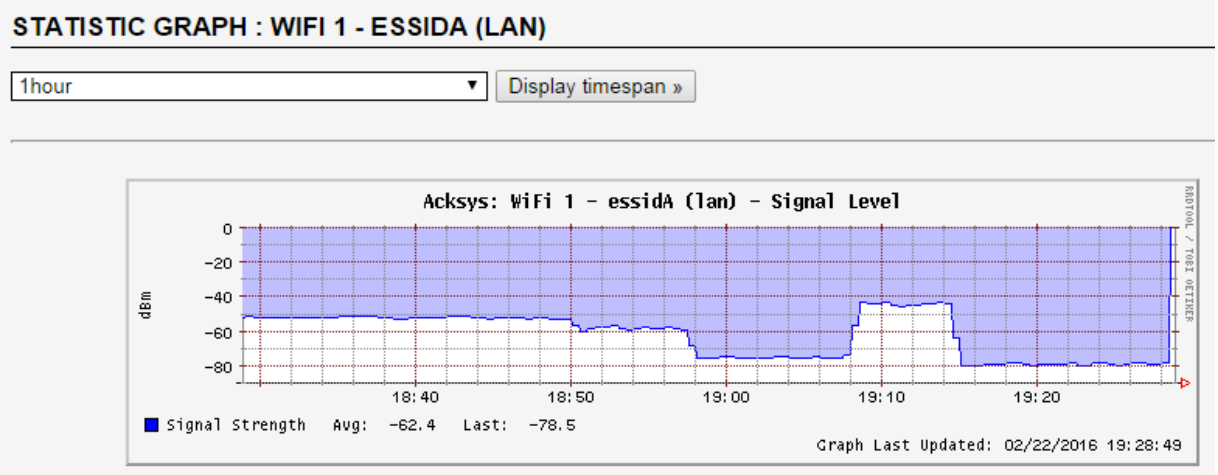


AccessPoint 모드에서의 Client 와 연결 예시



연결되지 않을 때 화면

통계 그래프 아이콘 을 클릭하여 신호 강도에 대한 통계 그래프를 표시할 수 있습니다. 또한 통계 그래프는 **Client 모드에서만** 사용할 수 있습니다. AccessPoint 모드로 설정되어 있으면 통계 그래프 아이콘이 비활성화 됩니다.



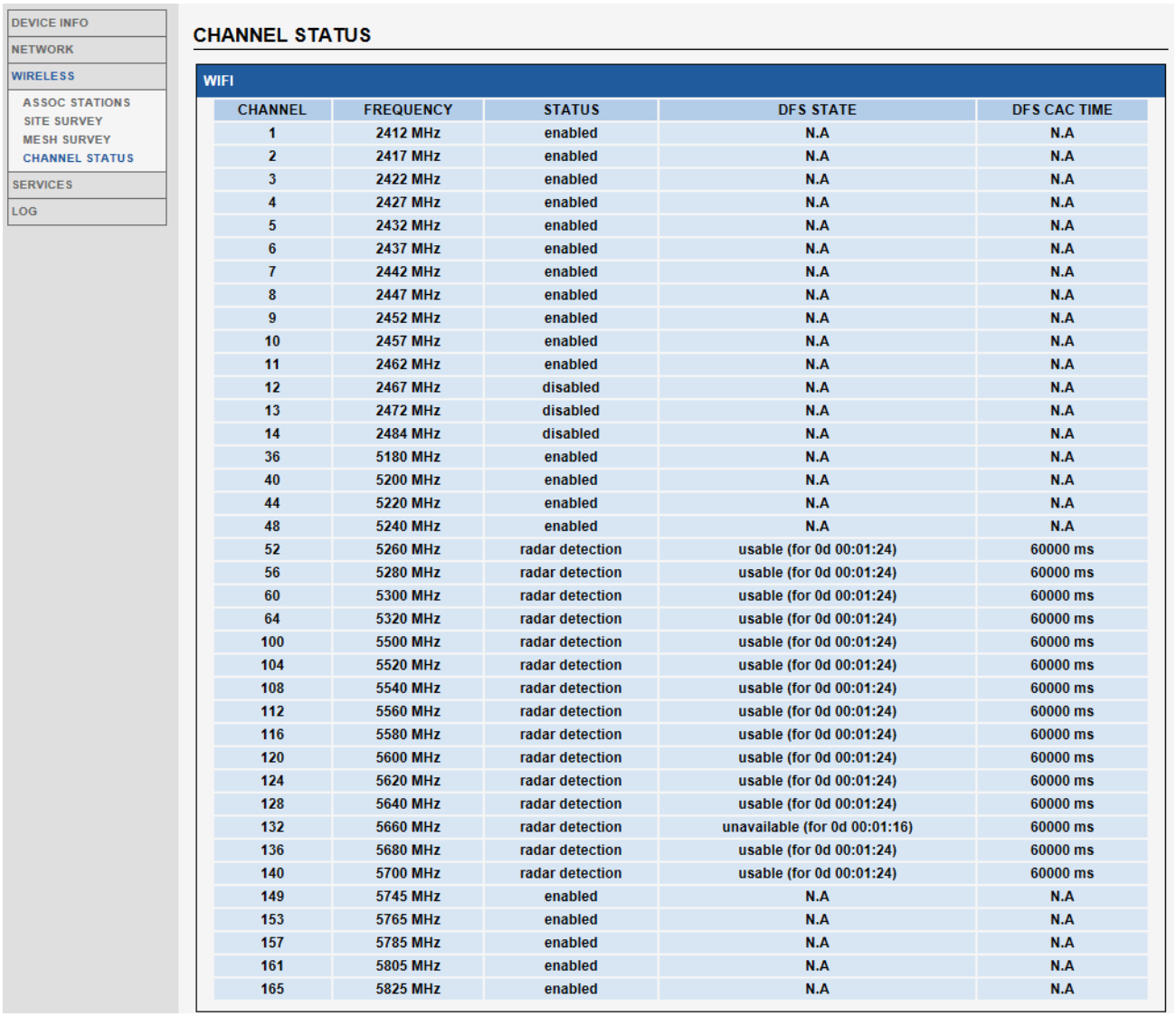
이 그래프를 통해 무선 인터페이스의 신호 세기 값을 실시간으로 확인할 수 있습니다:

Signal Level graph: 무선 인터페이스에 대한 신호 레벨을 실시간으로 dBm 으로 표시합니다.

또한 표시 기간을 10 분, 1 시간, 1 일, 1 주, 1 개월 단위로 설정할 수 있습니다.

VI.3.6.2 Channel Status

사용 가능한 채널 및 주파수가 표시됩니다.



CHANNEL	FREQUENCY	STATUS	DFS STATE	DFS CAC TIME
1	2412 MHz	enabled	N.A	N.A
2	2417 MHz	enabled	N.A	N.A
3	2422 MHz	enabled	N.A	N.A
4	2427 MHz	enabled	N.A	N.A
5	2432 MHz	enabled	N.A	N.A
6	2437 MHz	enabled	N.A	N.A
7	2442 MHz	enabled	N.A	N.A
8	2447 MHz	enabled	N.A	N.A
9	2452 MHz	enabled	N.A	N.A
10	2457 MHz	enabled	N.A	N.A
11	2462 MHz	enabled	N.A	N.A
12	2467 MHz	disabled	N.A	N.A
13	2472 MHz	disabled	N.A	N.A
14	2484 MHz	disabled	N.A	N.A
36	5180 MHz	enabled	N.A	N.A
40	5200 MHz	enabled	N.A	N.A
44	5220 MHz	enabled	N.A	N.A
48	5240 MHz	enabled	N.A	N.A
52	5260 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
56	5280 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
60	5300 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
64	5320 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
100	5500 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
104	5520 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
108	5540 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
112	5560 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
116	5580 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
120	5600 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
124	5620 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
128	5640 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
132	5660 MHz	radar detection	unavailable (for 0d 00:01:16)	60000 ms
136	5680 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
140	5700 MHz	radar detection	usable (for 0d 00:01:24)	60000 ms
149	5745 MHz	enabled	N.A	N.A
153	5765 MHz	enabled	N.A	N.A
157	5785 MHz	enabled	N.A	N.A
161	5805 MHz	enabled	N.A	N.A
165	5825 MHz	enabled	N.A	N.A

Status: 현재 무선 규제 구역에 대한 채널 제약 조건

- Enabled: 해당 채널은 무선 규제 구역에 의해 사용할 수 있습니다.
- Disabled: 해당 채널은 무선 규제 규역에 의해 사용할 수 없습니다.
- Radar detection: 해당 채널은 현재 규제 구역의 일부로써 레이더 상태를 모니터링 합니다.

DFS state: 채널의 동적 주파수 선택 상태

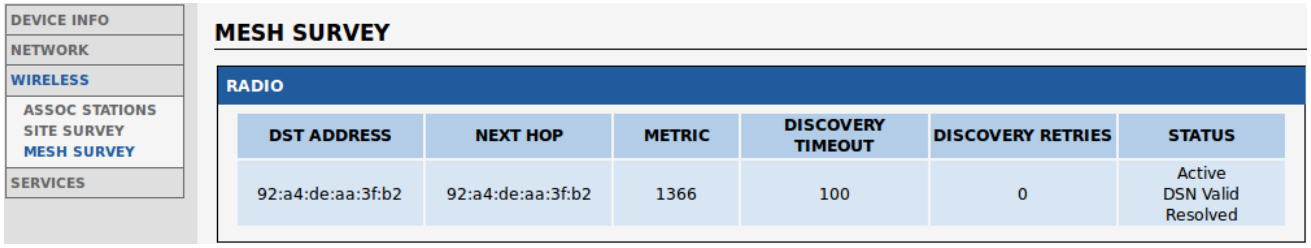
- Usable: 채널을 사용할 수 있지만, 채널 가용성 점검(CAC)은 사용 전에 수행해야 합니다.
- Unavailable: 채널에서 레이더가 감지되었으며 규제 정의 비 점유 기간 (NOP)에는 사용할 수 없습니다.
- Available: 채널이 CAC 를 확인했으며 해당 채널을 사용할 수 있습니다.

DFS CAC time:

채널을 사용 가능으로 간주하기 전에 레이더의 존재를 확인하는 기간입니다.

VI.3.6.3 MESH Survey

해당 패널을 통해 현재 사용 가능한 모든 802.11s 메쉬 포인트의 상태를 확인 할 수 있습니다.



DST Address:
최종 대상의 MAC 주소

Next Hop:
“DST Address” 에 도달하기 위한 다음 Mesh 노드의 MAC 주소

Metric:
해당 메쉬 경로의 총 cost 를 표시합니다. (값이 낮을수록 유리함)

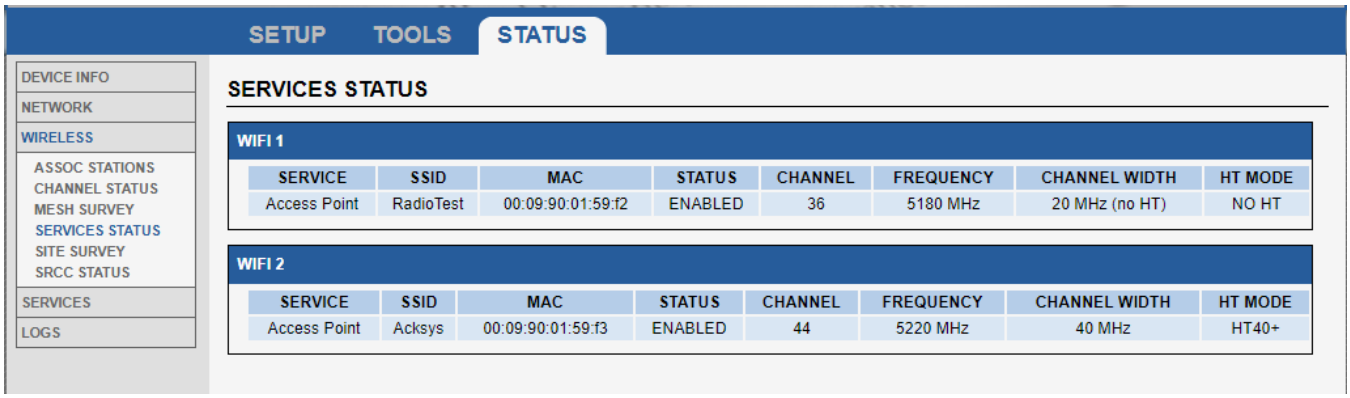
Discovery Timeout:
해당 메쉬 경로의 초과 검색 시간을 표시합니다. (단위 : ms)

Discovery retries:
재 검색 횟수를 표시합니다.

Status:
현재 MESH 경로의 상태를 표시합니다.

- Active : 해당 메쉬 경로를 포워딩 할 수 있음
- Resolving : 해당 메쉬 경로를 검색 중
- Resolved : 검색이 성공적으로 종료됨
- DSN Valid : 메쉬 경로에 유효한 시퀀스 번호가 포함됨

VI.3.6.4 Service status



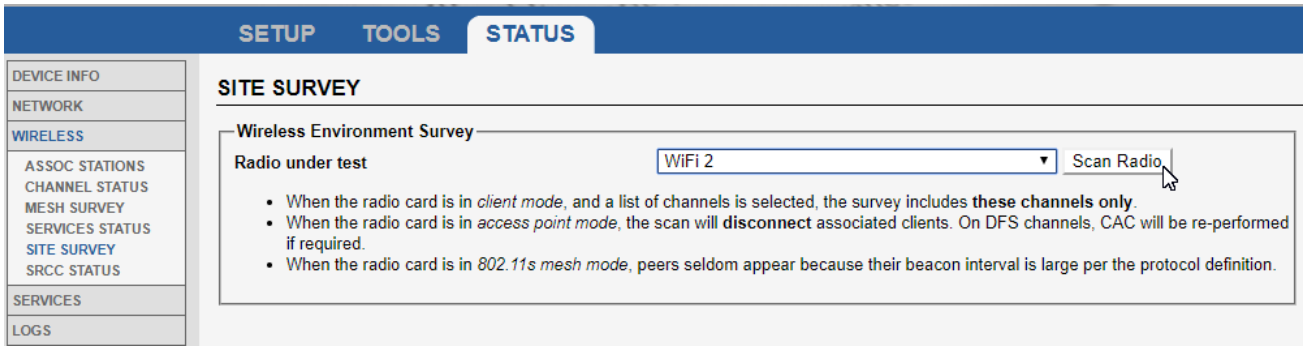
Service status 탭에서는 현재 무선 인터페이스에 대한 정보를 표시합니다. 또한 DFS 채널이 설정되어 있을 경우 해당 상태를 표시합니다.

VI.3.6.5 Site Survey

해당 기능을 통해 무선 모듈이 위치한 범위 내의 위치한 모든 AP 를 스캔 할 수 있습니다. 검색 결과는 무선 모듈이 설정된 모드에 따라 다르게 표시될 수 있습니다:

- Client 모드의 **Roaming** 기능을 사용하고 있을 경우 Roaming 탭에서 선택한 채널만 스캔 됩니다.
- AccessPonit 모드로 설정되어 있을 경우 스캔 간 현재 연결되어 있는 Client 의 통신이 해제됩니다.
- 802.11s 메쉬 모드로 설정되어 있을 경우 스캔 타임이 짧기 때문에 피어가 정상적으로 표시되지 않을 가능성이 있습니다.

Dual Radio 가 탑재된 제품의 경우 스캔 할 무선 모듈을 선택할 수 있습니다. **Scan Radio** 버튼을 클릭하여 스캔을 시작합니다. 해당 작업은 환경에 따라 몇 분 정도 소요될 수 있습니다.

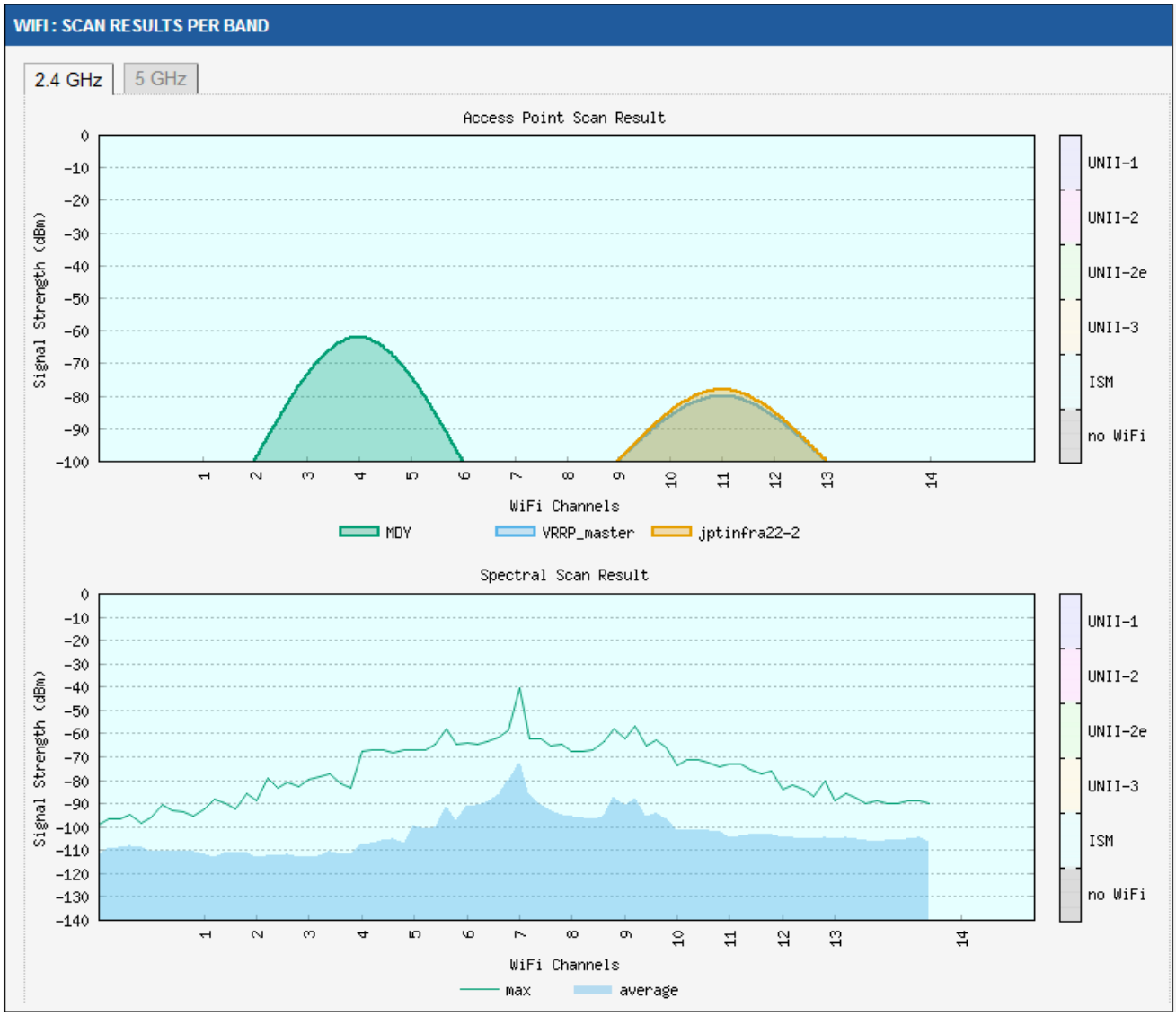


SITE SURVEY 가 동작되는 동안에는 설정된 무선 기능을 동작할 수 없습니다. 예를 들어 AccessPoint 모드로 설정된 경우 현재 연결된 모든 Client 의 연결이 해제됩니다. 또한 무선이 비활성화 되어 있는 경우에는 SITE SURVEY 가 동작되지 않습니다.

주의, 교란된 환경은 특정 액세스 포인트의 감지를 방해할 수 있으므로 두 개의 연속적인 사이트 조사 사이에 크게 다른 결과가 나타나는 것은 비정상적인 것이 아닙니다.

첫 번째 패널에는 감지된 액세스 포인트의 레이더 보기가 표시되며 측정된 전자기 노이즈 수준 아래에 있습니다. 각 탭을 클릭하여 2.4GHz 대역 또는 5GHz 대역을 표시할 수 있습니다.

아래 예에서 채널 7 주파수 주변에 전자기 노이즈가 있음을 볼 수 있습니다. 이 노이즈는 이 주파수에 액세스 포인트가 없기 때문에 Wi-Fi 가 아닙니다.



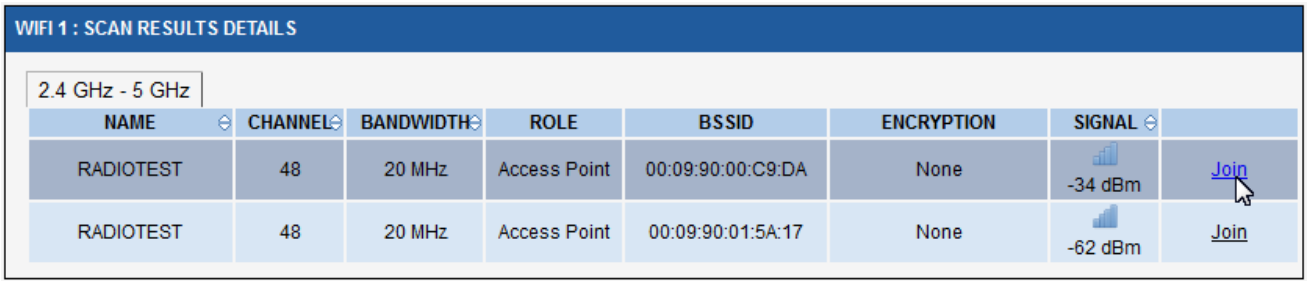
아래 표와 같이 탐지할 수 있는 모든 AccessPonit 를 스캔 할 수 있습니다.

WIFI 1 : SCAN RESULTS DETAILS

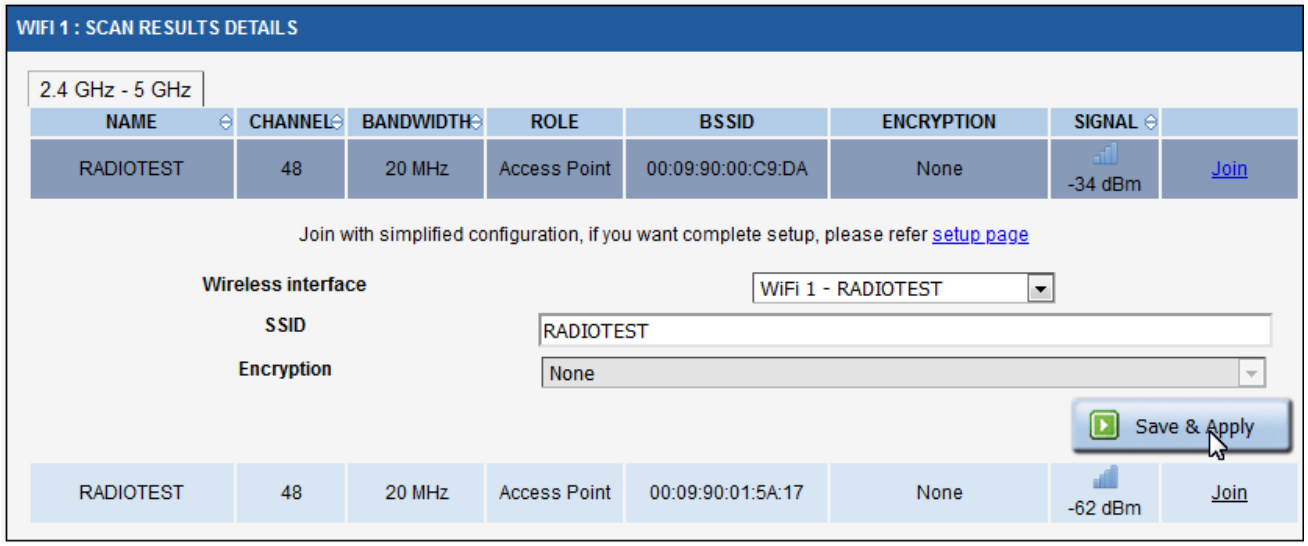
2.4 GHz - 5 GHz

NAME	CHANNEL	BANDWIDTH	ROLE	BSSID	ENCRYPTION	SIGNAL	
MDY	4	20 MHz	Access Point	00:1C:F0:08:CF:10	WPA2 PSK	-34 dBm	Join
VRRP_master	48	20 MHz	Access Point	04:F0:21:2C:6C:E3	None	-62 dBm	Join
jptinfra22-2	11	20 MHz	Access Point	04:F0:21:19:EB:95	WPA2 PSK	-75 dBm	Join
RADIOTEST	48	20 MHz	Access Point	00:09:90:00:C9:DA	None	-74 dBm	Join
RADIOTEST	48	20 MHz	Access Point	00:09:90:01:5A:17	None	-80 dBm	Join

SITE SURVEY 는 가장 낮은 속도의 비콘 프레임을 전송합니다. 따라서 실제 SIGNAL 값은 해당 표에 표시되어 있는 SIGNAL 값보다 더 양호합니다.



SSID 가 숨겨져 있을 경우 해당 표의 오른쪽 **Join** 버튼이 표시되지 않습니다. Join 버튼을 클릭할 경우 해당 AccessPoint 와 연결할 수 있습니다.



Wireless interface 를 사용하면 기존 설정을 변경하거나 무선 모듈에 새로운 설정을 추가할지 선택할 수 있습니다. 이미 Client 로 설정 되어 있을 경우에는 해당 옵션을 사용할 수 없습니다. (라디오에서 둘 이상의 Client 역할을 가질 수 없음)

VI.3.6.6 SRCC Status

해당 페이지를 통해 SRCC 인터페이스의 상태를 확인할 수 있습니다.

다음은 SRCC 초기화의 여러 단계를 설명하는 몇 가지 예입니다.

Coach topology discovery

SRCC STATUS		
STATE: COACH TOPOLOGY DISCOVERY		

SRCC DISCOVER RESULT		
COACH SWITCH NODE LIST		
	MAC ADDRESS	SRCC TYPE

Wi-Fi neighbor discovery

SRCC STATUS		
STATE: WIFI NEIGHBOR DISCOVERY		

SRCC DISCOVER RESULT		
COACH SWITCH NODE LIST		
	MAC ADDRESS	SRCC TYPE
WIFI NEIGHBOR LIST		
	MAC ADDRESS	SIGNAL

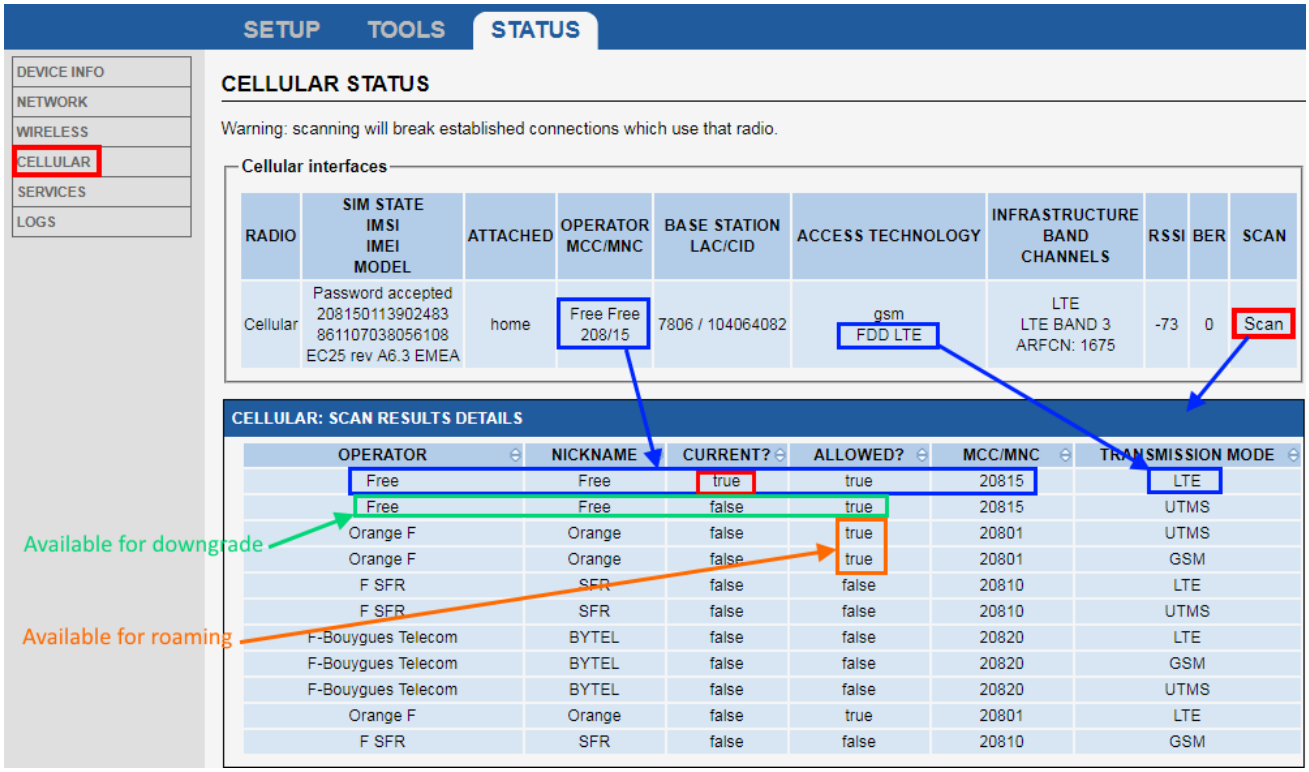
Configuration complete

SRCC STATUS		
STATE: LINK CONFIGURED		
COACH CONFIGURATION		
POSITION IN COACH	MAC ADDRESS	SRCC TYPE
Local switch node	00:09:90:00:5a:f7	a

LINK CONFIGURATION	
MAC ADDRESS	ROLE
00:09:90:00:5a:db	AP
00:09:90:00:5a:f7	CLIENT

VI.3.7 Cellular

해당 페이지를 통해 Cellular 무선 동작에 대한 정보를 확인할 수 있습니다.



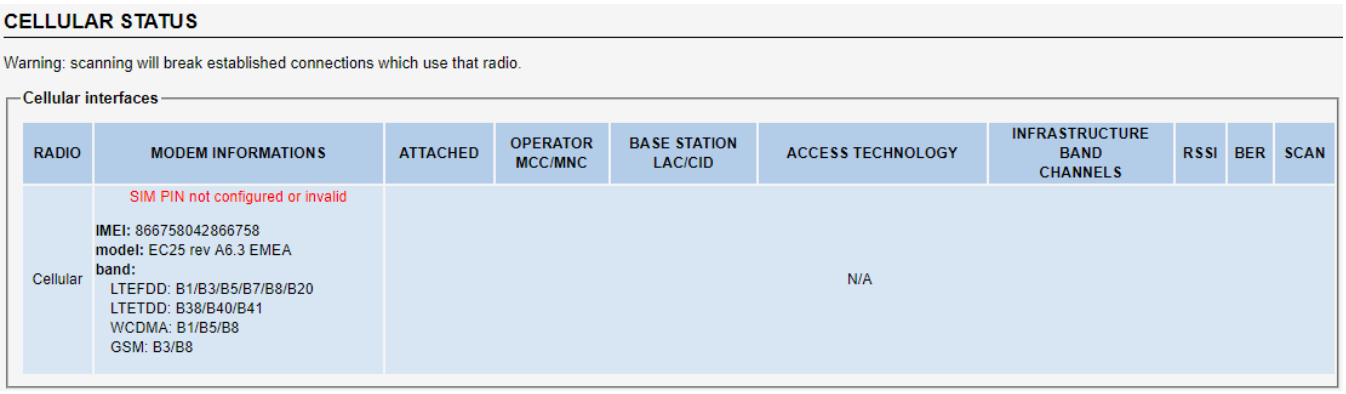
Cellular interfaces

- Radio 네트워크 인터페이스 이름
- SIM state PIN 코드 상태
- IMSI SIM77777 의 고유 식별자
- IMEI Radio Client 의 고유 식별자
- Model 무선 카드 모델, 버전, 지역
- Attached "home"은 SIM 네이티브 값을 사용하고, "Roaming"은 허용된 값을 사용합니다
- Operator 운영자 이름, MCC / MNC
- LAC/CID 기지국 위치 및 ID (통신사별)
- Access technology – GSM or CDMA
- RSSI 신호 품질 측정
- BER 비트 오류율 측정, 10000 bit 당 예상 오류 수 (see 3GPP TS 45.008)
- Scan 스캔을 통해 주변에 사용 가능한 인터페이스를 탐지합니다.

Scan results details

- Current? 현재 무선이 연결되어 있는 운영자 및 모드
- Allowed? 무선이 로밍될 수 있는 운영자

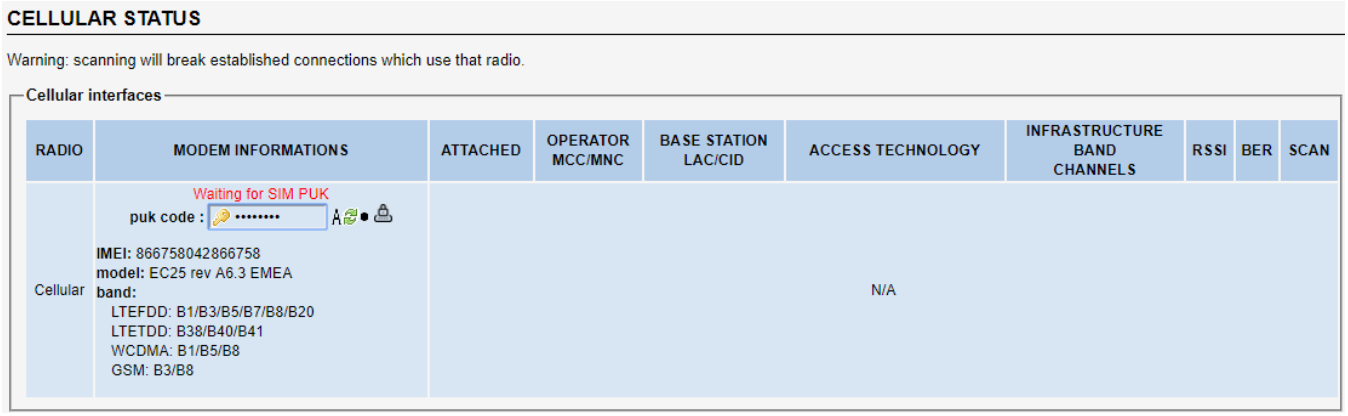
SIM PIN not configured or invalid



해당 메시지가 표시될 경우 PIN 코드가 입력되지 않았거나 잘못되었음을 의미합니다. 또한 해당 상황에서 접속 시도를 3 번 이상 할 경우 SIM 카드가 잠길 수 있습니다.

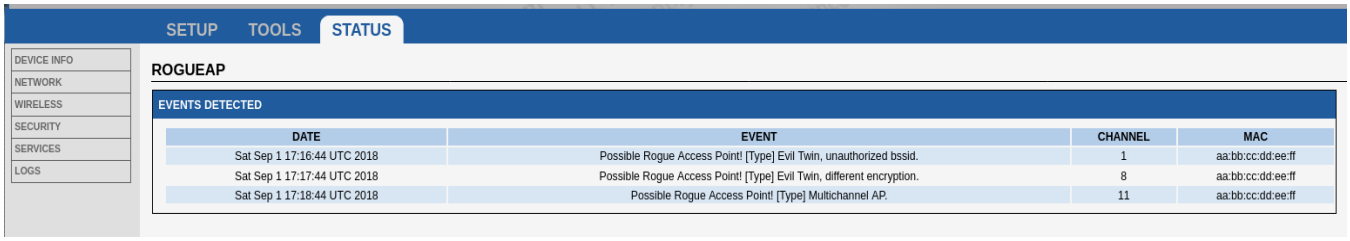
Unlocking the SIM card with the PUK code

LTE 인터페이스가 PUK 코드를 요청할 경우 (예: SIM 이 잠길 경우) PUK 코드를 입력할 수 있는 입력 창이 표시됩니다. PUK 코드를 변경할 때 PIN 코드를 지정해야 함으로 SIM 카드 슬롯에 설정된 PIN 코드를 입력해야 합니다.



VI.3.8 Security

해당 패널을 통해 보안 경고 목록을 확인할 수 있습니다.



- Wi-Fi 인터페이스 wlan xx 에서 RogueAP detector service 가 동작 됨
- **Evil Twin, different encryption.**

  무선 보안 설정이 예상 값과 다름.
- **Multichannel AP.**

  SSID 가 해당 인스턴스에 대해 설정된 채널과 다른 채널에서 감지됨
- **Evil Twin, unauthorized BSSID.**

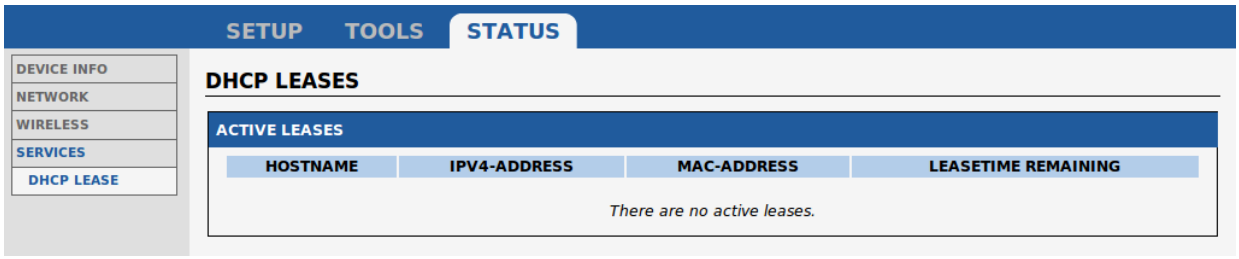
  BSSID 가 허용된 BSSID 리스트에 적용되어 있지 않음
- **Strange RSSI.**

  RSSI 값이 해당 SSID 에 대해 예상되는 RSSI 의 범위를 벗어남

VI.3.9 Services

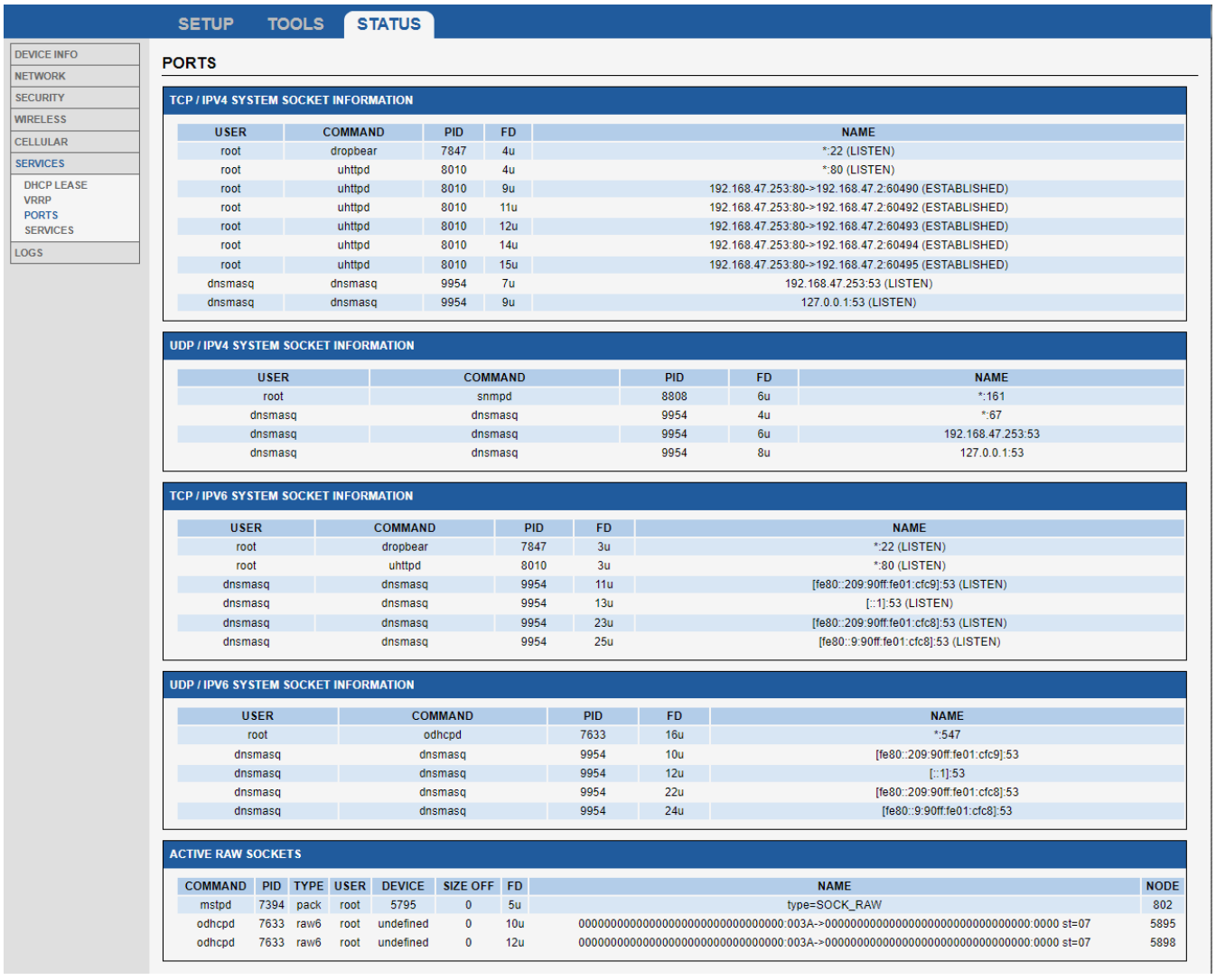
VI.3.9.1 DHCP Lease

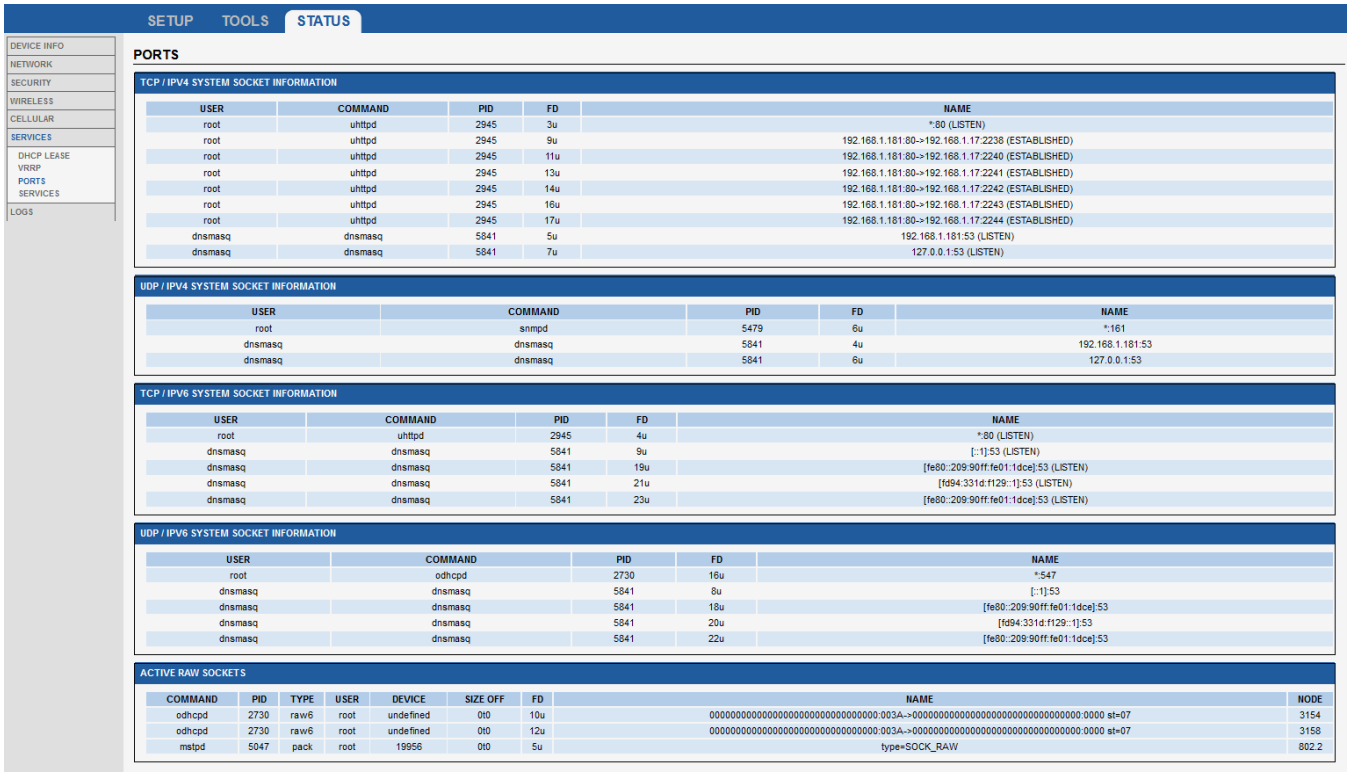
DHCP Lease 의 상태가 요약되어 있습니다.



VI.3.9.2 PORT

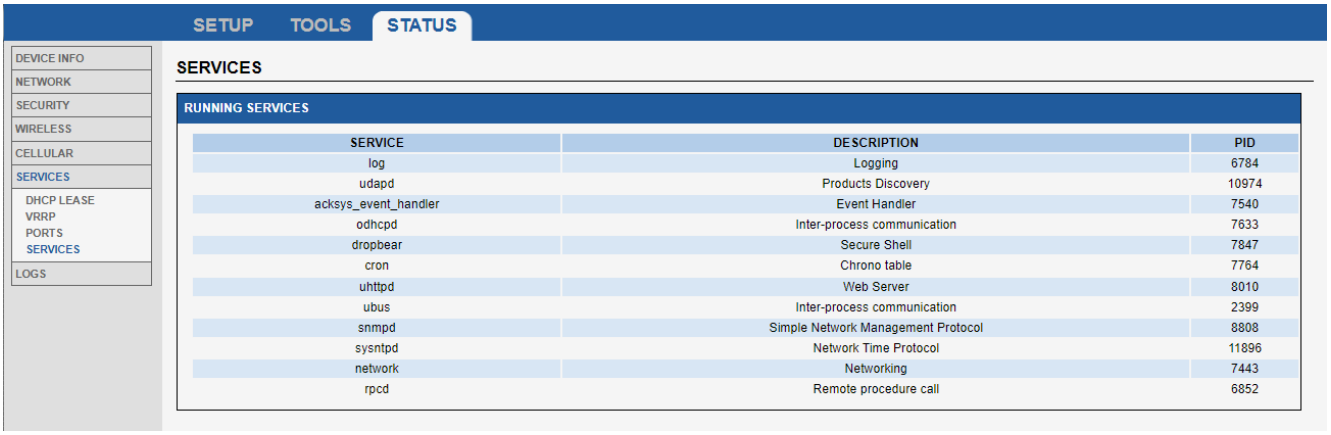
이 화면에서는, 활성 클라이언트에 대한 TCP 포트 인스턴스를 모니터링하기 위해 서비스당 현재 열려 있는 포트를 표시합니다.





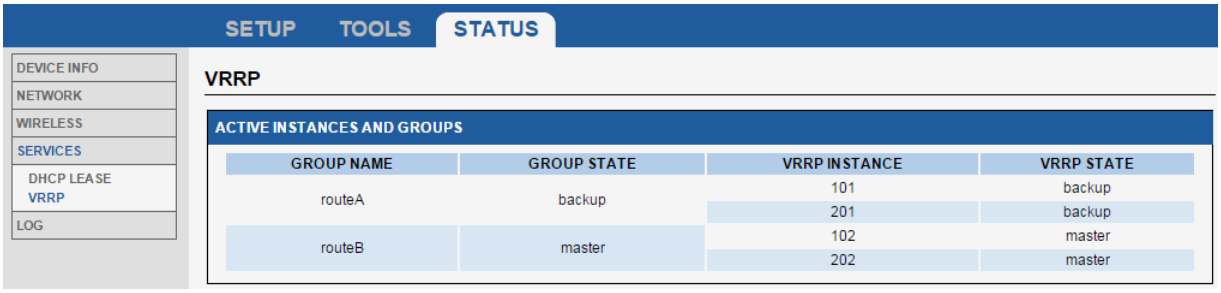
VI.3.9.3 SERVICES

이 패널에는 IT 팀이 실행 중인 서비스를 알고 보안 위반이 감지된 경우 중지할 수 있는 서비스 목록이 표시됩니다.



VI.3.9.4 VRRP

제품에 설정된 VRRP 상태 및 그룹의 현재 상태가 표시됩니다.



예시) 위 표를 통해 제품의 두 개의 게이트웨이가 설정되어 있는 것을 확인할 수 있습니다. 첫 번째는 “routeA” 로 표시되며 가상 인터페이스 101 과 201 을 그룹화합니다. 마스터가 두 인터페이스에서 모두 스캔 되었기 때문에 현재 비활성 상태 입니다.

가상 게이트웨이 “routeB” 가 현재 가상 인터페이스 102 와 202 사이에서 패킷을 라우팅 하고 있습니다.

VI.3.10 Logs

해당 탭을 통해 제품의 Log 를 확인할 수 있습니다.

Config log 는 설정에 문제가 없는지 확인할 수 있습니다.

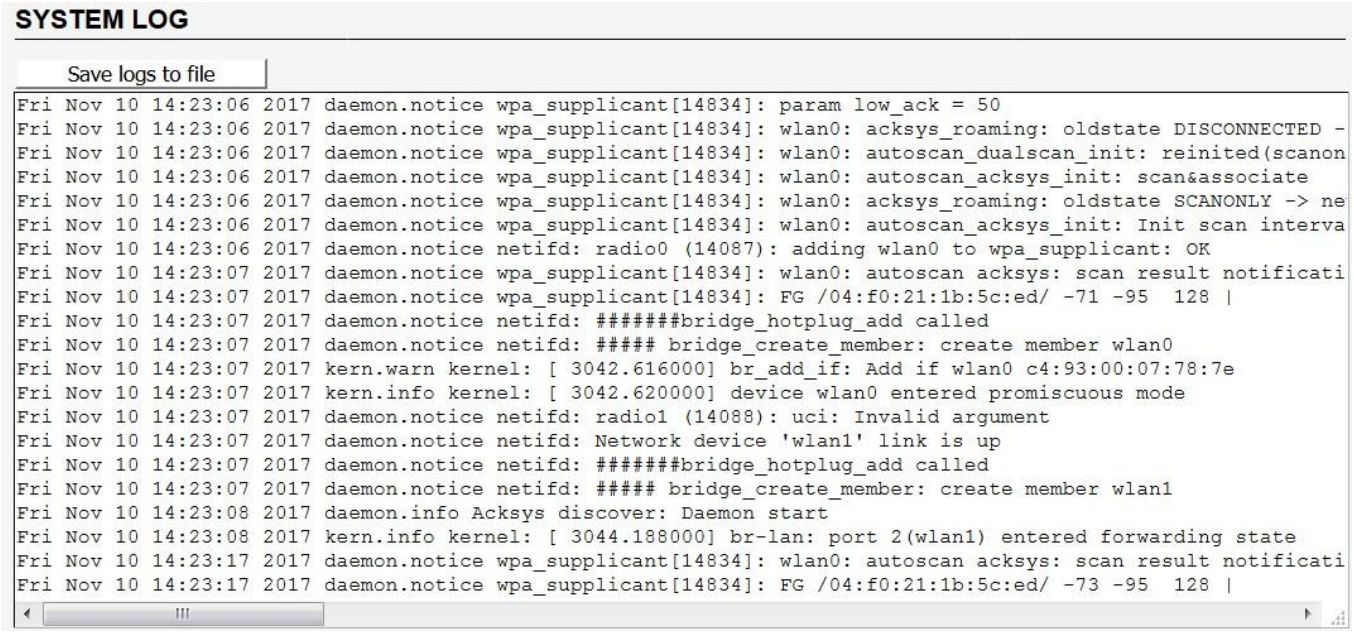
kernel log 에는 Linux kernel 로그 메시지만 표시됩니다. 또한 kernel 에서 보낸 모든 메시지는 필터링 되지 않습니다.

system log 는 kernel log 와 현재 실행 중인 서비스의 로그 메시지를 모두 표시합니다. The 해당 로그의 메시지는 SETUP/TOOLS/LOG 설정 페이지에서 설정된 우선 순위로 제한됩니다.

Client 모드에서는 로밍 프로세스와 관련된 메시지를 system log 에 선택적으로 표시할 수 있습니다. 해당 메시지에 표시되는 BSSID (MAC address) 를 둘러싼 기호의 설명은 다음 표를 참고하세요:

[B1:B2:B3:B4:B5:B6**]**	*현재 AP 의 BSSID*
B1:B2:B3:B4:B5:B6	*다음 로밍에 대해 선택한 AP 의 BSSID*
/B1:B2:B3:B4:B5:B6**/**	*'matching SSID' 테스트에 의해 삭제된 AP*
tB1:B2:B3:B4:B5:B6**t**	*'no return' 테스트에 의해 삭제된 AP*
mB1:B2:B3:B4:B5:B6**m**	*'minimum signal level'로 확보된 AP*
MB1:B2:B3:B4:B5:B6**M**	*'maximum signal level' 테스트를 통해 확보된 AP*

참고: 다른 선택의 여지가 없는 경우, '대기중인' AP 를 계속 사용할 수 있습니다.



KERNEL LOG

Save logs to file

```
[     0.000000] Linux version 3.18.9 (cv@devRD) (gcc version 4.8.3 (OpenWrt/Linaro GCC 4.8-2014.04 r43290) )
[     0.000000] bootconsole [early0] enabled
[     0.000000] CPU0 revision is: 00019750 (MIPS 74Kc)
[     0.000000] SoC: Qualcomm Atheros QCA9558 ver 1 rev 0
[     0.000000] Determined physical RAM map:
[     0.000000]  memory: 08000000 @ 00000000 (usable)
[     0.000000] User-defined physical RAM map:
[     0.000000]  memory: 08000000 @ 00000000 (usable)
[     0.000000] Initrd not found or empty - disabling initrd
[     0.000000] Zone ranges:
[     0.000000]   Normal   [mem 0x00000000-0x07ffffff]
[     0.000000] Movable zone start for each node
[     0.000000] Early memory node ranges
[     0.000000]   node   0: [mem 0x00000000-0x07ffffff]
[     0.000000] Initmem setup node 0 [mem 0x00000000-0x07ffffff]
[     0.000000] On node 0 totalpages: 32768
[     0.000000] free_area_init_node: node 0, pgdat 8039e250, node_mem_map 81000000
[     0.000000]   Normal zone: 256 pages used for memmap
[     0.000000]   Normal zone: 0 pages reserved
[     0.000000]   Normal zone: 32768 pages, LIFO batch:7
[     0.000000] Primary instruction cache 64kB, VIPT, 4-way, linesize 32 bytes.
[     0.000000] Primary data cache 32kB, 4-way, VIPT, cache aliases, linesize 32 bytes
[     0.000000] pcpu-alloc: s0 r0 d32768 u32768 alloc=1*32768
[     0.000000] pcpu-alloc: [0] 0
[     0.000000] Built 1 zonelists in Zone order, mobility grouping on.  Total pages: 32512
[     0.000000] Kernel command line:  board=42 console=ttyS0,115200 mtdparts=ar934x-nfc:3M(uboot),2M(uboot-en
[     0.000000] ack_ethaddr_setup: ethaddr 00:09:90:00:8b:5f,c4:93:00:07:78:80
[     0.000000] eth0 => mac 00:09:90:00:8b:5f
[     0.000000] eth1 => mac c4:93:00:07:78:80
[     0.000000] eth2 => mac 00:00:00:00:00:00
[     0.000000] eth3 => mac 00:00:00:00:00:00
[     0.000000] eth4 => mac 00:00:00:00:00:00
[     0.000000] PID hash table entries: 512 (order: -1, 2048 bytes)
[     0.000000] Dentry cache hash table entries: 16384 (order: 4, 65536 bytes)
[     0.000000] Inode-cache hash table entries: 8192 (order: 3, 32768 bytes)
[     0.000000] Writing ErrCtl register=00000000
[     0.000000] Readback ErrCtl register=00000000
[     0.000000] Memory: 125748K/131072K available (2870K kernel code, 127K rwdata, 412K rodata, 164K init, 18
[     0.000000] SLUB: HWalign=32, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
[     0.000000] NR_IRQS:51
[     0.000000] Clocks: CPU:720.000MHz, DDR:600.000MHz, AHB:200.000MHz, Ref:40.000MHz
[     0.000000] Calibrating delay loop... 359.42 BogoMIPS (lpj=718848)
[     0.028000] pid_max: default: 32768 minimum: 301
[     0.028000] Mount-cache hash table entries: 1024 (order: 0, 4096 bytes)
[     0.028000] Mountpoint-cache hash table entries: 1024 (order: 0, 4096 bytes)
[     0.028000] NET: Registered protocol family 16
[     0.028000] MIPS: machine is Acksys EmbedAir1000
[     0.032000] registering PCI controller with io_map_base unset
[     0.032000] ar724x-pci ar724x-pci.1: PCIe link is down
[     0.032000] registering PCI controller with io_map_base unset
[     0.032000] ath79_device_reset_set: SGMII dbg register is good (07560710)=> skip reset
[     0.136000] ath79_device_reset_clear: SGMII_DEBUG value 0756070f
[     0.240000] usbcore: registered new interface driver usbfs
```

CONFIG LOG

Save logs to file

```
####################################        DEVICE LIST         ####################################
Device_label  Device_name  Interface_name
------------  -----------  --------------
LAN 1         eth0         eth0
LAN 2         eth1         eth1
WiFi 1        phy0         radio0
WiFi 2        phy1         radio1


####################################          WIFI LIST         ####################################
Interface_label                Interface_name       Network_included_in
-----------------              --------------       -------------------
WiFi 1.RADIOTEST               radio0w0             bond1
WiFi 2.RADIOTEST               radio1w0             bond1


####################################       Check VLAN LIST      ####################################
Nothing to report
####################################          VLAN LIST         ####################################
vlan_description     vlan_name  Interface_attached_to  vid   Network_included_in  interface_name
----------------     ---------  ---------------------  ---   -------------------  --------------


####################################   Check GRE/NETWORK LIST   ####################################
Nothing to report
####################################          GRE LIST          ####################################
gre_description      gre_name   gre_network  local_endpoint_type  tunlink
---------------      --------   -----------  -------------------  -------


####################################        NETWORK LIST        ####################################
network_description  network_name  network_proto network_type         network_ifname
-------------------  ------------  ------------- ------------         --------------
loopback             loopback      static                             lo
lan                  lan           static        bridge               eth0 eth1
bond1                bond1                       bond                 ***N/A***
```

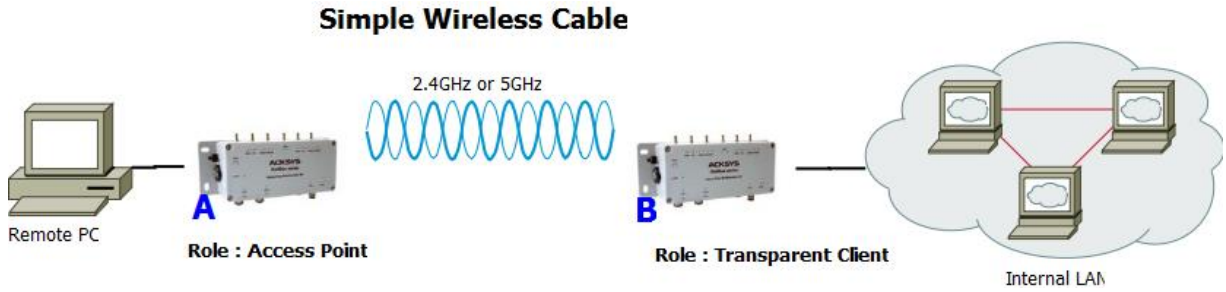
VII WIRELESS TOPOLOGIES EXAMPLES

이 제품군에는 다중 무선 토폴로지로 구성 가능한 장치가 있습니다. 다음 섹션에서는 가장 많이 사용되는 항목에 대해 설명합니다.

모든 토폴로지에 대해 이 토폴로지의 특성 매개변수는 빨간 글씨로 작성됩니다.

VII.1 Simple “Wireless cable”

해당 모드는 AccessPoint 와 Infrastructure Client 를 유선을 대체하여 무선으로 연결합니다.



Configuration summary:

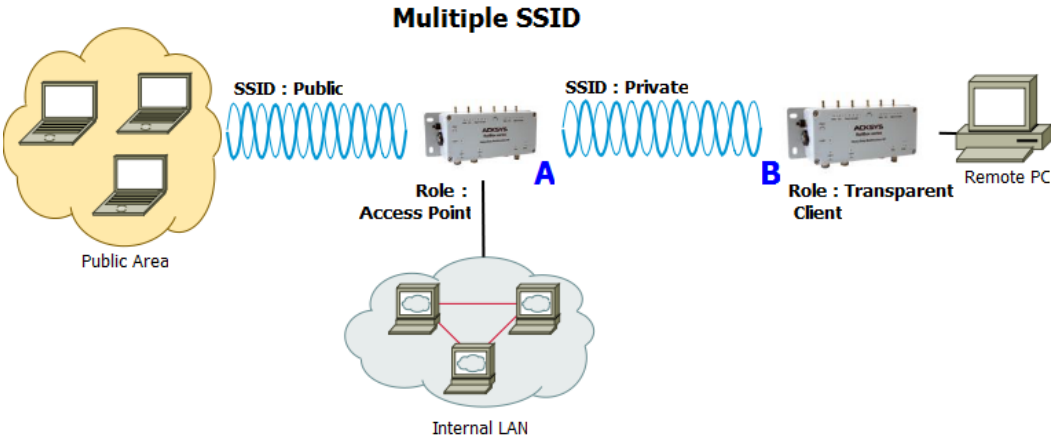
다음 예시는 20MHz HT 모드, 채널 36, 국가 코드 FR 및 ACKSYS 를 ESSID 로 사용하는 802.11a 를 사용하고 있습니다.

Product A	
Device Configuration	
Parameter	***Value***
Enable device	on
802.11 mode	802.11a
HT mode	20MHz
Channel	36
Country code	FR
Interface Configuration 1	
Parameter	***Value***
Role	Access Point
ESSID	ACKSYS

Product B	
Device Configuration	
Parameter	***Value***
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	any
Interface Configuration 1	
Parameter	***Value***
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A

VII.2 Multiple SSID

해당 모드에서 단일 AccessPoint 는, 각 SSID 에 대해 서로 다른 네트워크 별 보안 체계를 허용하기 위해, 여러 개의 SSID 를 동시에 제공할 수 있습니다.



Configuration summary:

다음 예시는 HT 모드보다 40MHz 높은 802.11na, 채널 36, 국가 코드 FR, 개인용 ESSID 로 ACKSYS, 공용 ESSID 로 SYSKCA 를 사용하고 있습니다.

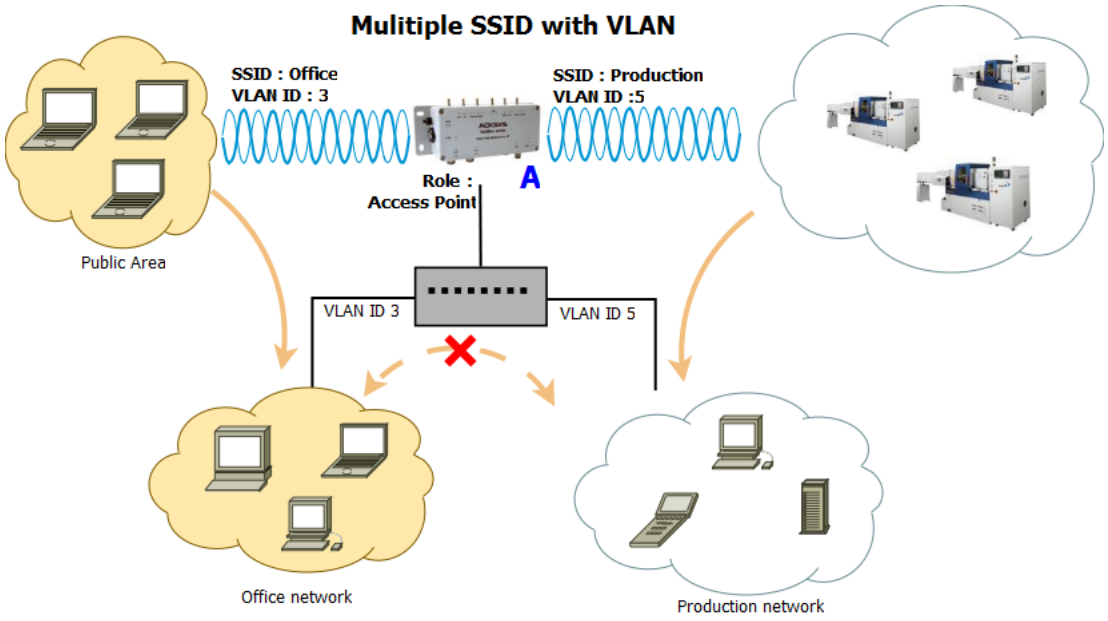
Product A	
Device Configuration	
Parameter	***Value***
Enable device	on
802.11 mode	802.11na
HT mode	40 MHz above
Channel	36
Country code	FR
Interface Configuration 1 (Public)	
Parameter	***Value***
Role	Access point
ESSID	SYSKCA
Interface Configuration 2 (Private)	
Parameter	***Value***
Role	Access point
ESSID	ACKSYS

Product B	
Device Configuration	
Parameter	***Value***
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	any
Interface Configuration 1	
Parameter	***Value***
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A private ESSID

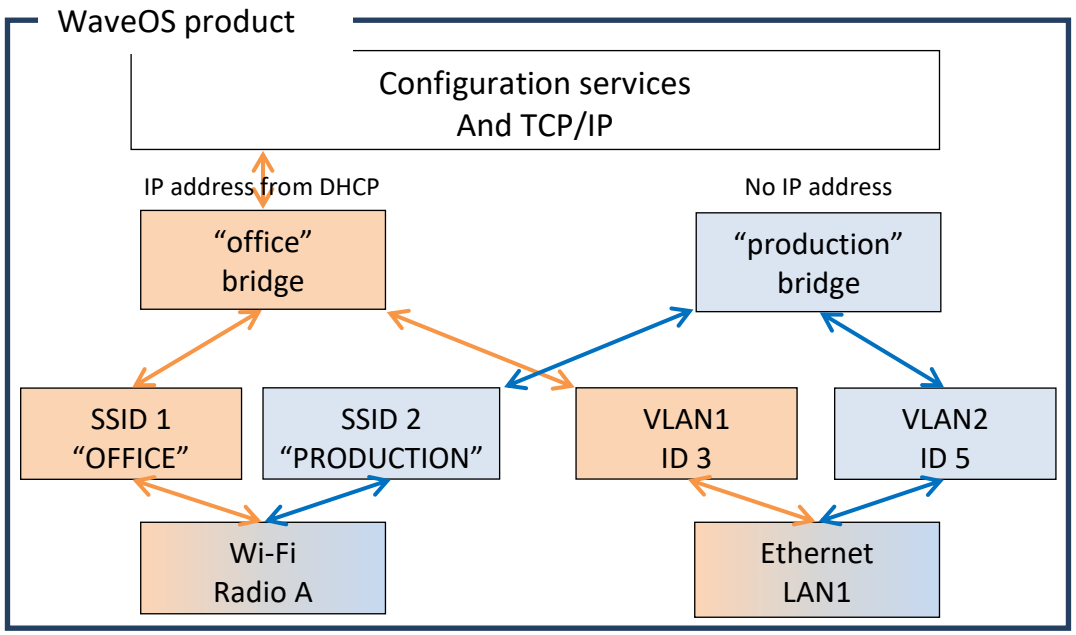
VII.3 Multiple SSID with VLAN

한 개의 AccessPoint 를 통해 서로 다른 여러 개의 SSID 를 동시에 설정하여 연결할 수 있습니다. 또한 모든 SSID 트래픽은 동일한 LAN 인터페이스를 공유하며 VLAN 을 사용하여 LAN 에서 SSID 트래픽을 서로 분리할 수 있습니다.

해당 모드는 LAN 으로 전송되는 프레임에 802.1q 태그를 추가하고 수신 LAN 프레임에 있는 태그를 사용하여 연결된 SSID 로 데이터를 전달합니다. 또한 태그 자체는 Wi-Fi 링크를 통해 전송되지 않습니다.



이 설정을 지원하는 제품 "A"의 내부 구조입니다:



Configuration summary:

Product A	
Device Configuration	
Parameter	***Value***
Enable device	on
802.11 mode	802.11na
HT mode	40 MHz above
Channel	36
Country code	FR
Interface Configuration 1 (Office)	
Parameter	***Value***
Role	Access point
ESSID	OFFICE
Interface Configuration 2 (Production)	
Parameter	***Value***
Role	Access point
ESSID	PRODUCTION

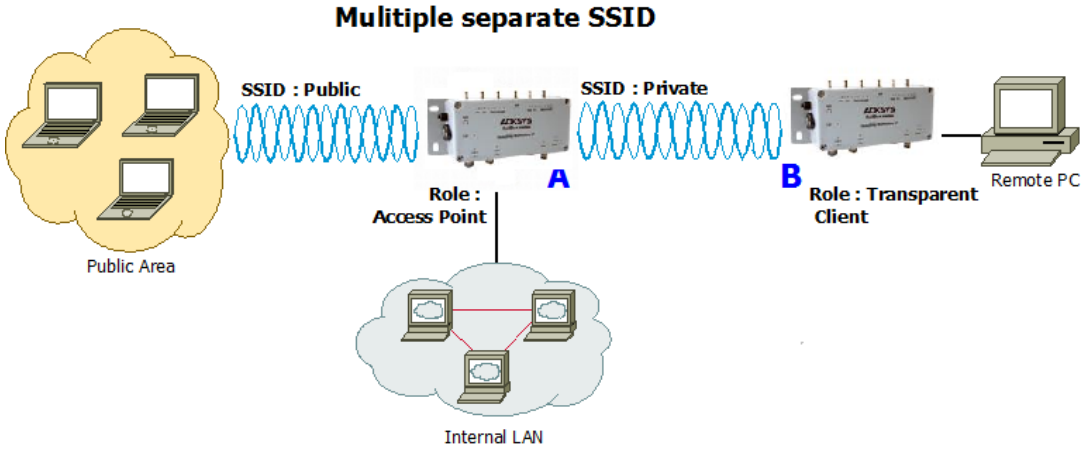
Virtual interface (VLAN 3)	
Parameter	***Value***
VLAN ID	3
Interface	LAN
Virtual interface (VLAN 5)	
VLAN ID	5
Interface	LAN
Network (office)	
Protocol	DHCP
Bridge interfaces	Checked
Interfaces	LAN.3 and “office” Wi-Fi adapter
Network (Production)	
Protocol	None
Bridge interface	Checked
Interfaces	LAN.5 and “production” Wi-Fi adapter

웹 인터페이스를 통해 해당 설정을 변경할 수 있습니다:

- “virtual interfaces” 메뉴에서 이더넷 LAN 위에 VLAN 인터페이스를 생성합니다
- “physical interfaces” 메뉴에서 무선 설정을 완료한 후 필요한 SSID 당 하나의 “access point” 인터페이스를 생성합니다
- “network” 메뉴에서 가상 네트워크 당 하나의 네트워크를 생성한 후 Ethernet 의 VLAN 과 Wireless Radio 의 SSID 를 연결합니다.

VII.4 Multiple separate SSID

해당 모드에서 두 개의 무선 모듈을 가진 제품을 사용하여 중계기 기능을 사용할 수 있습니다. (예: 공용 액세스용 채널 하나와 SCADA 용 채널 하나)



Configuration summary:
해당 모드는 두 가지로 구성할 수 있습니다. (무선 카드당 하나씩)

For Radio A (Public side):
Mode: 802.11na, HT mode: 40MHz above, channel: 36, country code: FR, ESSID: ACKSYS.

For Radio B (Private side):
Mode: 802.11na, HT mode: 40MHz above, channel: 44, country code: FR, ESSID: SYSKCA.

Product A

Device Configuration 1 (Radio A)

Parameter	*Value*
Enable device	on
802.11 mode	802.11na
HT mode	40 MHz above
Channel	36
Country code	FR

Interface Configuration 1 (Radio A)

Parameter	*Value*
Role	Access point
ESSID	Private

Device Configuration 2(Radio B)

Parameter	*Value*
Enable device	on
802.11 mode	802.11na
HT mode	40 MHz above
Channel	44
Country code	FR

Interface Configuration 2 (Radio B)

Parameter	*Value*
Role	Access point
ESSID	Public

Product B

Device Configuration

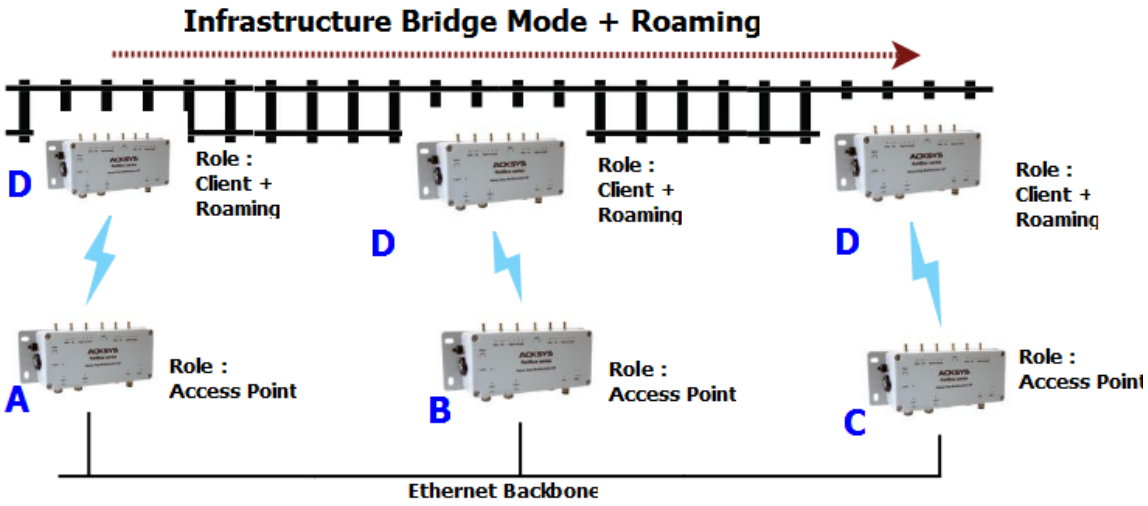
Parameter	*Value*
Enable device	on
802.11 mode	802.11na
HT mode	40 MHz above
Channel	44
Country code	FR

Interface Configuration 1

Parameter	*Value*
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A private ESSID

VII.5 Infrastructure bridge + Roaming

해당 모드를 통해 Client 는 Infrastructure biridge 의 연결을 해제하지 않고 다음 Access Point 로 절체할 수 있습니다.



Configuration summary:

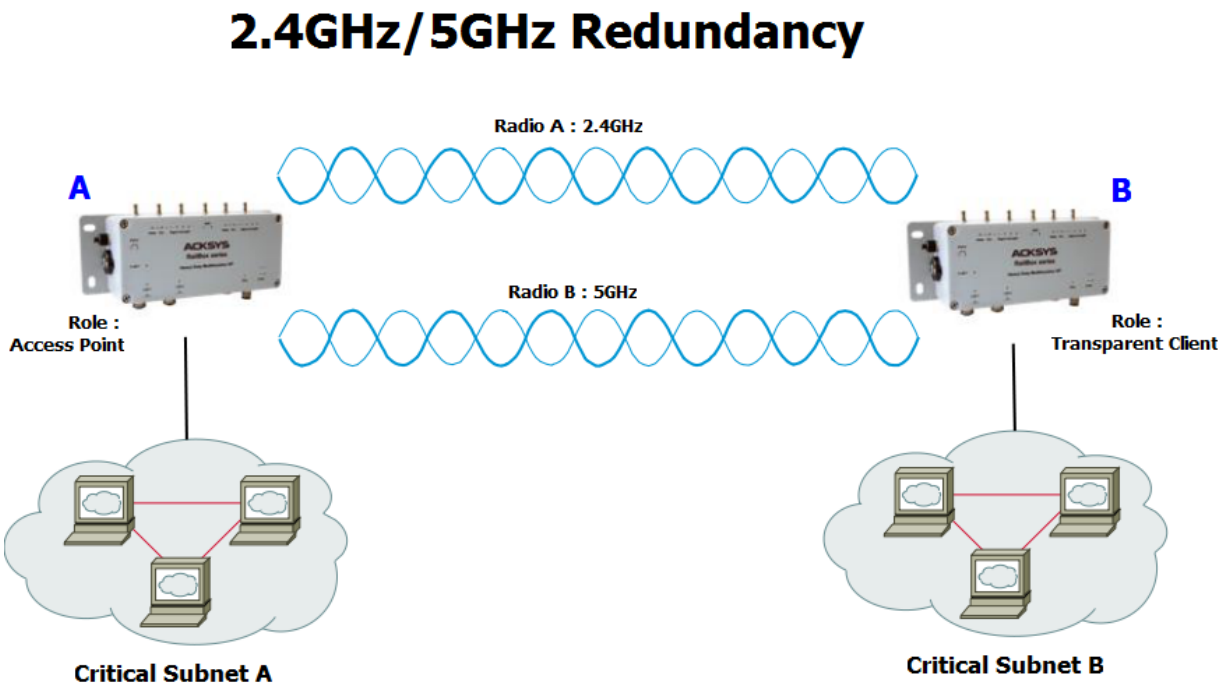
다음 예시에서는, 로밍 임계값을 -60dBm 으로 설정하고 스캔 주기 기간을 5 초로 설정하여 이전과 동일한 매개변수를 사용하고 있습니다.

Products A, B, C	
Device Configuration	
Parameter	***Value***
Enable device	on
802.11 mode	802.11na
HT mode	40MHz above
Channel	36
Country code	FR
Interface Configuration 1	
Parameter	***Value***
Role	Access point
ESSID	ACKSYS

Product D	
Device Configuration	
Parameter	***Value***
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	any
Interface Configuration 1	
Parameter	***Value***
Role	Client
ESSID	same as product A
Roaming	
Parameter	***Value***
Enable proactive roaming	on
Channel	same as product A
Current AP minimum level	-60
Delay between 2 successive scan cycle	5000

VII.6 Point-to-point redundancy with dual band

해당 모드를 통해 Dual Radio 를 보유한 무선 모듈을 서로 다른 채널로 설정하여 이중화 링크를 형성할 수 있습니다. 한번에 하나의 링크만 데이터를 전송할 수 있으며 두 링크 중 하나가 문제가 발생할 경우 두 번째 링크로 절체됩니다.



Configuration summary:

다음 예시에서는 두 가지 다른 구성(무선 카드당 하나)이 있습니다.

라디오 A 의 경우:

모드: 802.11ng, HT 모드: 20MHz, 채널: 11, 국가 코드: FR, ESSID: ACKSYS1.

라디오 B 의 경우:

모드: 802.11na, HT 모드: 20MHz, 채널: 36, 국가 코드: FR, ESSID: ACKSYS2.

주의: 이 토폴로지는 네트워크 루프를 생성합니다. STP 또는 RSTP 를 사용하여 두 Wi-Fi 링크 중 하나를 끊어야 루프 발생이 되지 않습니다. STP 기능은 펌웨어 1.4.0 부터 제공되며, 연결된 모든 제품에서 각각 활성화되어야 합니다. 자세한 내용은 "스패닝 트리 프로토콜(STP, RSTP)" 섹션을 참고하세요.

Product A

Device Configuration (Radio A)

Parameter	*Value*
Enable device	on
802.11 mode	802.11ng
HT mode	20MHz
Channel	11
Country code	FR

Interface Configuration 1(Radio A)

Parameter	*Value*
Role	Access point
ESSID	ACKSYS1

Device Configuration (Radio B)

Parameter	*Value*
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR

Interface Configuration 1(Radio B)

Parameter	*Value*
Role	Access point
ESSID	ACKSYS2

Product B

Device Configuration (Radio A)

Parameter	*Value*
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	any

Interface Configuration 1 (Radio A)

Parameter	*Value*
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A

Device Configuration (Radio B)

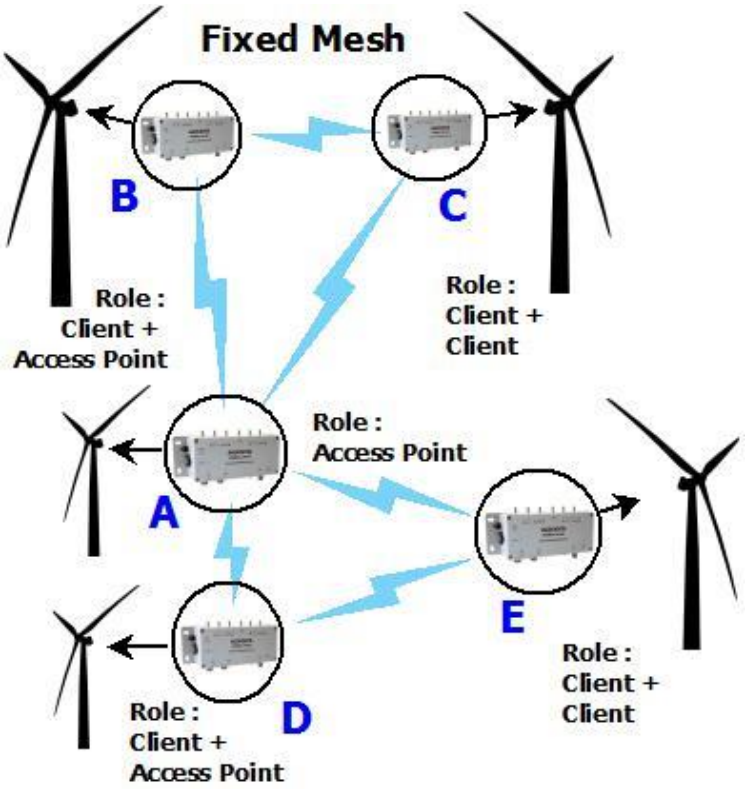
Parameter	*Value*
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	any

Interface Configuration 1 (Radio B)

Parameter	*Value*
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A

VII.7 Fixed Mesh

해당 기능을 통해 고정된 환경에서의 MESH 네트워크 망을 형성할 수 있습니다.



Configuration summary:.

Mode (Product **A** and Radio A for Products **B**, **C**, **D**, **E**,): 802.11na, HT mode: 20MHz , channel: 36, country code: FR, ESSID: ACKSYS.

Mode (Radio B for Products **B**, **C**): 802.11na, HT mode: 20MHz, channel: 40, country code: FR, ESSID: ACKSYS2.

Mode (Radio B for Products **D**, **E**): 802.11na, HT mode: 20MHz, channel: 60, country code: FR, ESSID: ACKSYS3.

주의: 해당 기능은 네트워크 루프를 생성할 가능성이 있습니다. 따라서 제품의 STP 및 RSTP 기능을 활성화를 권고 드립니다. 펌웨어 1.4.0 부터 STP 를 제공하며, 각 제품에서 STP 를 활성화해야 합니다. 자세한 내용은 VI.1.4.1 Network configuration 섹션을 참고하세요.

Product A

Device Configuration

Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR

Interface Configuration

Parameter	Value
Role	Access point
ESSID	ACKSYS

Product B

Device Configuration (Radio A)

Parameter	Value
Enable device	on
802.11 mode	Same as product A
HT mode	Same as product A
Channel	Same as product A
Country code	any

Interface Configuration (Radio A)

Parameter	Value
Role	Client
Bridging mode	4 address format
ESSID	ACKSYS

Device Configuration (Radio B)

Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	40
Country code	FR

Interface Configuration (Radio B)

Parameter	Value
Role	Access Point
ESSID	ACKSYS2

Product C

Device Configuration (Radio A)

Parameter	Value
Enable device	on
802.11 mode	Same as product A
HT mode	Same as product A
Channel	Same as product A
Country code	any

Interface Configuration (Radio A)

Parameter	Value
Role	Client
Bridging mode	4 address format
ESSID	ACKSYS

Device Configuration (Radio B)

Parameter	Value
Enable device	on
802.11 mode	Same as product B (Radio B)
HT mode	Same as product B (Radio B)
Channel	Same as product B (Radio B)
Country code	any

Interface Configuration (Radio B)

Parameter	Value
Role	Client
Bridging mode	4 address format
ESSID	Same as product B (Radio B)

Product D

Device Configuration (Radio A)

Parameter	*Value*
Enable device	on
802.11 mode	Same as product A
HT mode	Same as product A
Channel	Same as product A
Country code	any

Interface Configuration (Radio A)

Parameter	*Value*
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	ACKSYS

Device Configuration (Radio B)

Parameter	*Value*
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	60
Country code	FR

Interface Configuration (Radio B)

Parameter	*Value*
Role	Access Point
ESSID	ACKSYS3

Product E

Device Configuration (Radio A)

Parameter	*Value*
Enable device	on
802.11 mode	Same as product A
HT mode	Same as product A
Channel	Same as product A
Country code	any

Interface Configuration (Radio A)

Parameter	*Value*
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	ACKSYS

Device Configuration (Radio B)

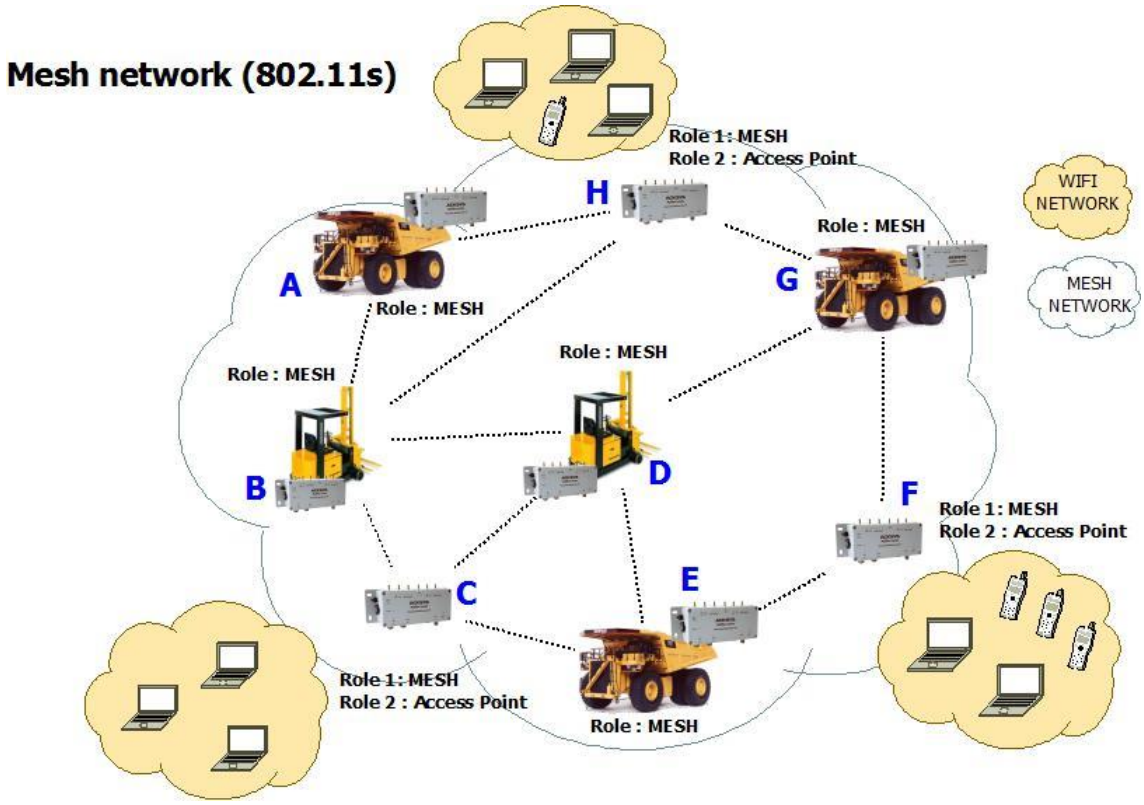
Parameter	*Value*
Enable device	on
802.11 mode	Same as product D (Radio B)
HT mode	Same as product D (Radio B)
Channel	Same as product D (Radio B)
Country code	any

Interface Configuration (Radio B)

Parameter	*Value*
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	Same as product D (Radio B)

VII.8 802.11s Mesh

해당 기능은 IEEE 802.11s 표준을 사용하며, MESH 네트워크 망을 형성할 수 있습니다. (V.2.1.3 Mesh (802.11s) Mode 섹션 참고)



Configuration summary:

Mode (Products **A**, **B**, **E**, **D**, **G** and Radio A for Products **C**, **F**, **H**): 802.11na, HT mode: 20MHz, channel: 36, country code: FR, MESHID: ACKSYS.

Mode (Radio B for Products **C**): 802.11na, HT mode: 20MHz, channel: 40, country code: FR, ESSID: ACKSYS1.

Mode (Radio B for Products **F**): 802.11na, HT mode: 20MHz, channel: 44, country code: FR, ESSID: ACKSYS2.

Mode (Radio B for Products **H**): 802.11na, HT mode: 20MHz, channel: 48, country code: FR, ESSID: ACKSYS3.

Product A, B, E, D, G

Device Configuration

Parameter	*Value*
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR

Interface Configuration

Parameter	*Value*
Role	Mesh (802.11s)
MESHID	ACKSYS

Product C

Device Configuration (Radio A)

Parameter	*Value*
Enable device	on
802.11 mode	Same as Product A
HT mode	Same as Product A
Channel	Same as Product A
Country code	any

Interface Configuration (Radio A)

Parameter	*Value*
Role	Mesh (802.11s)
MESHID	ACKSYS

Device Configuration (Radio B)

Parameter	*Value*
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	40
Country code	FR

Interface Configuration (Radio B)

Parameter	*Value*
Role	Access Point
ESSID	ACKSYS1

Product F

Device Configuration (Radio A)

Parameter	*Value*
Enable device	on
802.11 mode	Same as Product A
HT mode	Same as Product A
Channel	Same as Product A
Country code	any

Interface Configuration (Radio A)

Parameter	*Value*
Role	Mesh (802.11s)
MESHID	ACKSYS

Device Configuration (Radio B)

Parameter	*Value*
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	44
Country code	FR

Product H

Device Configuration (Radio A)

Parameter	*Value*
Enable device	on
802.11 mode	Same as Product A
HT mode	Same as Product A
Channel	Same as Product A
Country code	any

Interface Configuration (Radio A)

Parameter	*Value*
Role	Mesh (802.11s)
MESHID	ACKSYS

Device Configuration (Radio B)

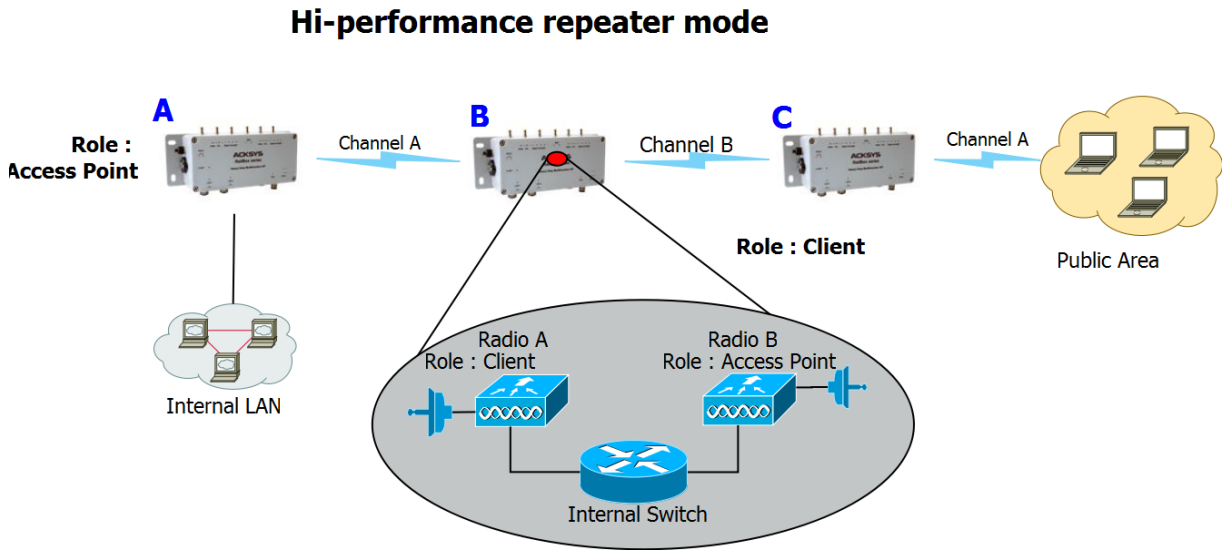
Parameter	*Value*
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	48
Country code	FR

Interface Configuration (Radio B)	
Parameter	***Value***
Role	Access Point
ESSID	ACKSYS2

Interface Configuration (Radio B)	
Parameter	***Value***
Role	Access Point
ESSID	ACKSYS3

VII.9 High performance repeater

듀얼 무선 모듈을 통해 고성능 리피터 기능을 사용할 수 있습니다.



Configuration summary:

Mode (Product **A** to Product **B**): 802.11na, HT mode: 20MHz, channel: 36, country code: FR, ESSID: ACKSYS1.

Mode (Product **B** to Product **C**): 802.11na, HT mode: 20MHz, channel: 44, country code: FR, ESSID: ACKSYS2.

해당 설정을 사용하면 Wi-Fi 채널을 공유할 수 없습니다. 해당 예시에서 제품 **B** 의 라디오 **A** 는 제품 **A** 와만 통신하는 반면, 제품 B 의 라디오 **B** 는 제품 **C** 와만 통신합니다.

주의: Radio **A** 와 Radio **B** 는 서로 다른 채널을 선택해야 합니다.

Product A

Device Configuration (Radio A)	
Parameter	***Value***
Enable device	on
802.11 mode	802.11na
HT mode	40MHz above
Channel	36
Country code	FR

Interface Configuration 1(Radio A)	
Parameter	***Value***
Role	Access point
ESSID	ACKSYS1

Product B

Device Configuration (Radio A)	
Parameter	***Value***
Enable device	on
802.11 mode	802.11na
HT mode	40MHz above
Channel	36
Country code	FR

Interface Configuration 1(Radio A)	
Parameter	***Value***
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	ACKSYS1

Device Configuration (Radio B)	
Parameter	***Value***
Enable device	on
802.11 mode	802.11ng
HT mode	40MHz above
Channel	44
Country code	FR

Interface Configuration 1(Radio B)	
Parameter	***Value***
Role	Access point
ESSID	ACKSYS2

Product C

Device Configuration (Radio A)	
Parameter	***Value***
Enable device	on
802.11 mode	802.11na
HT mode	40MHz above
Channel	44
Country code	FR

Interface Configuration 1(Radio A)	
Parameter	***Value***
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	ACKSYS2

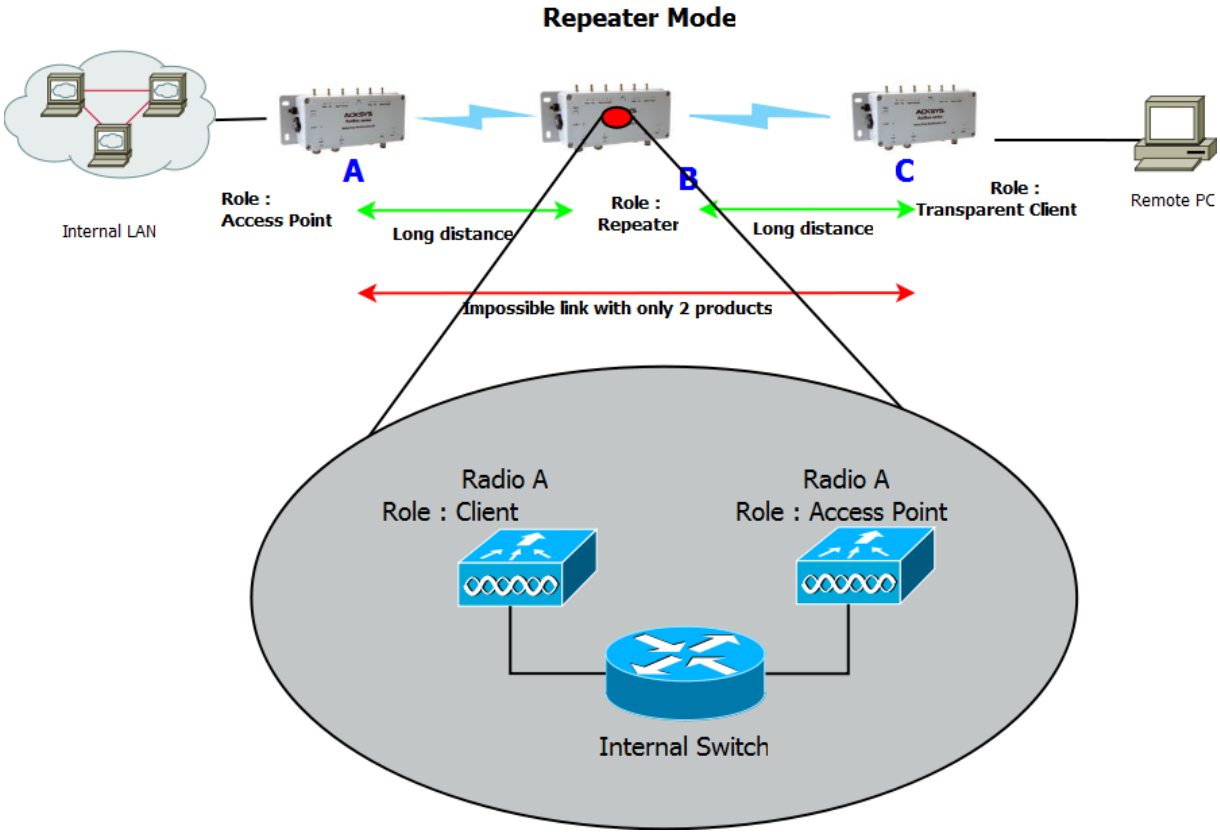
Device Configuration (Radio B)	
Parameter	***Value***
Enable device	on
802.11 mode	802.11ng
HT mode	40MHz above
Channel	36
Country code	FR

Interface Configuration 1(Radio B)	
Parameter	***Value***
Role	Access point
ESSID	ACKSYS1

VII.10 Line topology repeater (single radio card)

해당 모드로 하나 이상의 리피터를 추가 하여, 링크의 거리를 확장할 수 있습니다.

(*0* for supporting products 섹션 참고)



Configuration summary:

Mode: 802.11na, HT mode: 20MHz, channel: 36, country code: FR, ESSID: ACKSYS.

Repeater 모드에서는 하나의 무선 카드로, 두 개의 인터페이스를 생성하여 동작합니다. (예시: 상단 구성도에서 **B** 는 **A** 의 Client, **C** 의 AccessPoint 로 동시에 동작합니다.)

이 때, **A** 와 **B** 모두 동일한 SSID 로 설정해야 합니다. 또한 repeater 는 연관시켜야 하는 액세스 포인트(이 예에서는 제품 A)의 BSSID 를 알아야 합니다.

제품 C 는 4-주소 브리징 모드로 설정됩니다. 다른 모드(예: ARPNAT)도 작동하지만 주의 사항이 있습니다. 자세한 내용은 V.2.6 Wired to wireless bridging in infrastructure mode 에서 유선-무선 브리징을 참조하세요.

Product A

Device Configuration (Radio A)

Value	*Parameter*
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR

Interface Configuration 1(Radio A)

Value	*Parameter*
Role	Access point
ESSID	ACKSYS

Product C

Device Configuration (Radio A)

Value	*Parameter*
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR

Interface Configuration 1 (Radio A)

Parameter	*Value*
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A

Product B

Device Configuration (Radio A)

Parameter	*Value*
Enable device	on
802.11 mode	same as product A
HT mode	same as product A
Channel	same as product A
Country code	any

Interface Configuration 1 (Radio A)

Parameter	*Value*
Role	Client
Bridging mode	4 addresses format (WDS)
Multiple ESSIDs	on
Wireless Network Nicknames	SSID_ACKSYS

ESSID Configuration (SSID_ACKSYS)

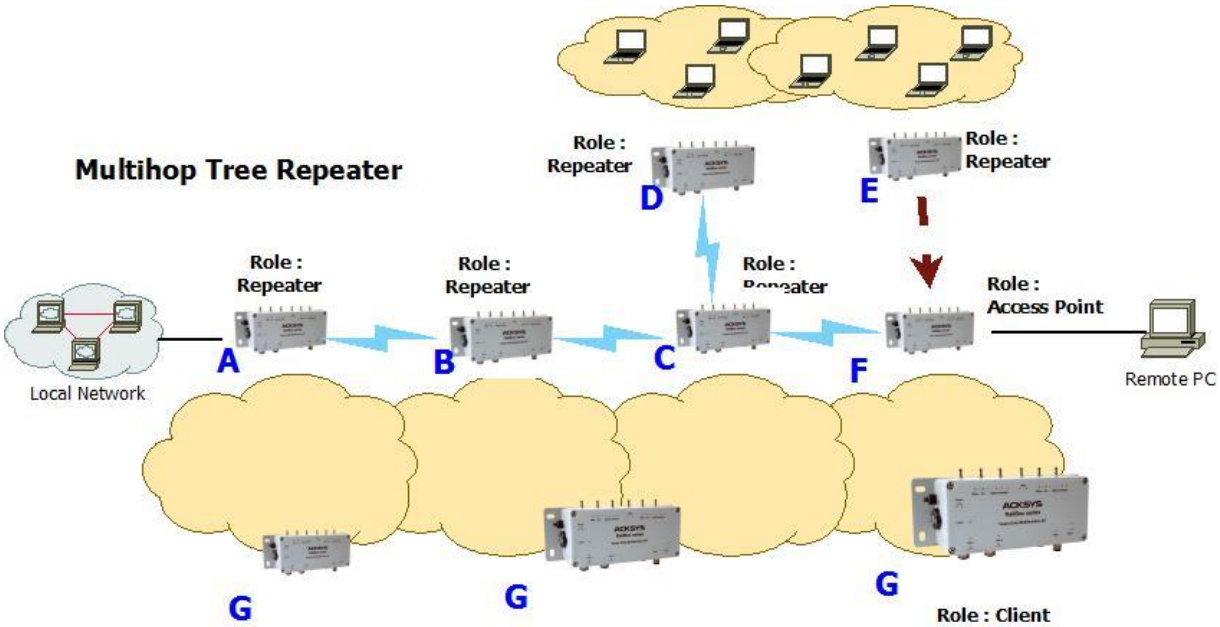
Parameter	*Value*
WLAN description	SSID_ACKSYS
ESSID	same as product A
Priority group	7
BSSID	Product A radio card MAC address

Interface Configuration 2 (Radio A)

Parameter	*Value*
Role	Access point
ESSID	same as product A

VII.11 Multihop tree repeater

하나 이상의 리피터 모듈을 추가하여, 무선 커버리지 영역을 여러 방향으로 확장하고 전체 통신 연결을 유지할 수 있습니다.



Configuration summary:

Mode: 802.11na, HT mode: 20MHz, channel: 36, country code: FR, ESSID: ACKSYS.

해당 구성은 Repeater 간의 연결 제한이 없습니다.

중계기 상호 연결은 트리 구조로 제한됩니다. 그러나 이는 트리의 두 장치 간에 발생할 수 있는 데이터 교환은 제한하지 않습니다.

F(트리의 마지막 라우터)는 액세스 포인트 모드로 설정해야 합니다. 이론적으로 F 는 리피터 모드에서 구성할 수 있지만, 리피터의 클라이언트 부분은 연결하려고 시도하는 무선 대역폭을 소비합니다.

Product A

Device Configuration

Parameter	*Value*
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR

Interface Configuration 1 (Radio A)

Parameter	*Value*
Role	Client
Bridging mode	4 addresses format (WDS)
Mutiple ESSIDs	on
Wireless Network Nicknames	SSID_ACKSYS

ESSID Configuration (SSID_ACKSYS)

Parameter	*Value*
WLAN description	SSID_ACKSYS
ESSID	ACKSYS
Priority group	7
BSSID	Product B radio card MAC address

Interface Configuration 2 (Radio A)

Parameter	*Value*
Role	Access point
ESSID	ACKSYS

Product B

Device Configuration

Parameter	*Value*
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR

Interface Configuration 1 (Radio A)

Parameter	*Value*
Role	Client
Bridging mode	4 addresses format (WDS)
Mutiple ESSIDs	on
Wireless Network Nicknames	SSID_ACKSYS

ESSID Configuration (SSID_ACKSYS)

Parameter	*Value*
WLAN description	SSID_ACKSYS
ESSID	same as product A
Priority group	7
BSSID	Product C radio card MAC address

Interface Configuration 2 (Radio A)

Parameter	*Value*
Role	Access point
ESSID	same as product A

Product C

Device Configuration

Parameter	*Value*
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR

Interface Configuration 1 (Radio A)

Parameter	*Value*
Role	Client
Bridging mode	4 addresses format (WDS)
Mutiple ESSIDs	on
Wireless Network Nicknames	SSID_ACKSYS

ESSID Configuration (SSID_ACKSYS)

Product D

Device Configuration

Parameter	*Value*
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR

Interface Configuration 1 (Radio A)

Parameter	*Value*
Role	Client
Bridging mode	4 addresses format (WDS)
Mutiple ESSIDs	on
Wireless Network Nicknames	SSID_ACKSYS

ESSID Configuration (SSID_ACKSYS)

Parameter	Value
WLAN description	SSID_ACKSYS
ESSID	same as product A
Priority group	7
BSSID	Product F radio card MAC

Interface Configuration 2 (Radio A)

Parameter	Value
Role	Access point
ESSID	same as product A

Parameter	Value
WLAN description	SSID_ACKSYS
ESSID	same as product A
Priority group	7
BSSID	Product C radio card MAC

Interface Configuration 2 (Radio A)

Parameter	Value
Role	Access point
ESSID	same as product A

Product E

Device Configuration

Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR

Interface Configuration 1 (Radio A)

Parameter	Value
Role	Client
Bridging mode	4 addresses format (WDS)
Mutiple ESSIDs	on
Wireless Network Nicknames	SSID_ACKSYS

ESSID Configuration (SSID_ACKSYS)

Parameter	Value
WLAN description	SSID_ACKSYS
ESSID	same as product A
Priority group	7
BSSID	Product F radio card MAC

Interface Configuration 2 (Radio A)

Parameter	Value
Role	Access point
ESSID	same as product A

Product F

Device Configuration

Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR

Interface Configuration

Parameter	Value
Role	Access Point
ESSID	same as product A

Product G

Device Configuration

Parameter	Value
Enable device	on
802.11 mode	802.11na
HT mode	20MHz
Channel	36
Country code	FR

Interface Configuration	
Parameter	***Value***
Role	Client
Bridging mode	4 addresses format (WDS)
ESSID	same as product A

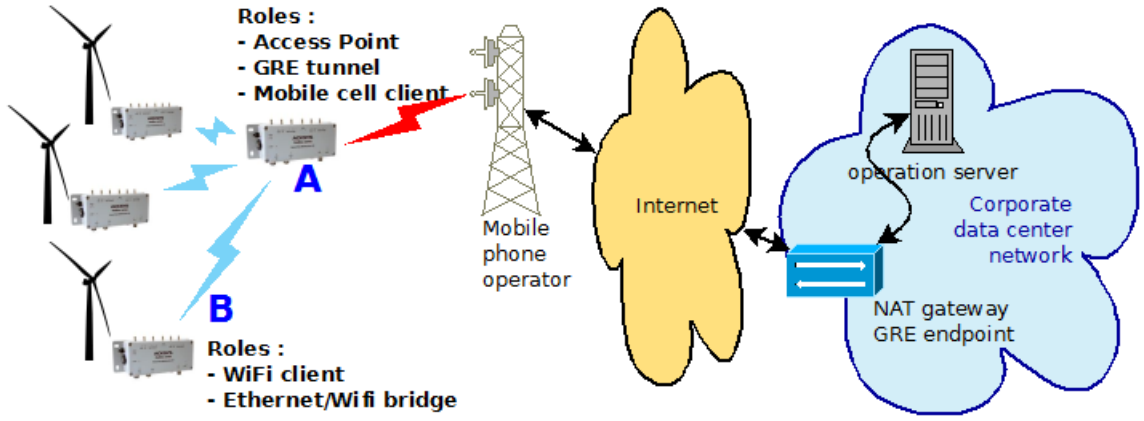
Roaming	
Parameter	***Value***
Enable proactive roaming	on
Channel	same as product A
Current AP minimum level	-60
Delay between 2 successive scan cycle	5000

VII.12 Cellular communication

VII.12.1.1 Simple connection from product to Internet

이 설정에서는 제품 자체만 인터넷 서버에 액세스할 수 있습니다. 제품 LAN 또는 WLAN 의 장치는 연결을 사용할 수 없으며, 원격 컴퓨터에서 제품에 대한 액세스를 요청할 수 없습니다.

예를 들어 제품이 공개적으로 액세스할 수 있는 로그 서버 또는 GRE 터널 끝점에는 연결할 수 있습니다.



이 설정에서는 제품 'A'(플랜트 게이트웨이)의 구성만 제공됩니다. 제품 'B'와 운영 서버는 동일한 IP 범위(192.168.0.0/24)에서 가상 LAN 을 공유하며, 제품 'B'는 192.168.0.100~192.168.0.249 범위에서 DHCP 를 통해 주소를 공급받습니다. 운영 서버는 192.168.0.1 과 같은 주소를 가져야 합니다.

'B' 제품에는 제품 'A'가 기본 게이트웨이로 지정되지만 다음 두 가지 이유로 사용할 수 없습니다.

첫째, 구성 아래에 zone 전달이 설정되어 있지 않기 때문입니다.

둘째, phone 네트워크의 NAT 는 개별 'B' 제품으로 다시 라우팅할 방법을 알지 못하기 때문입니다.

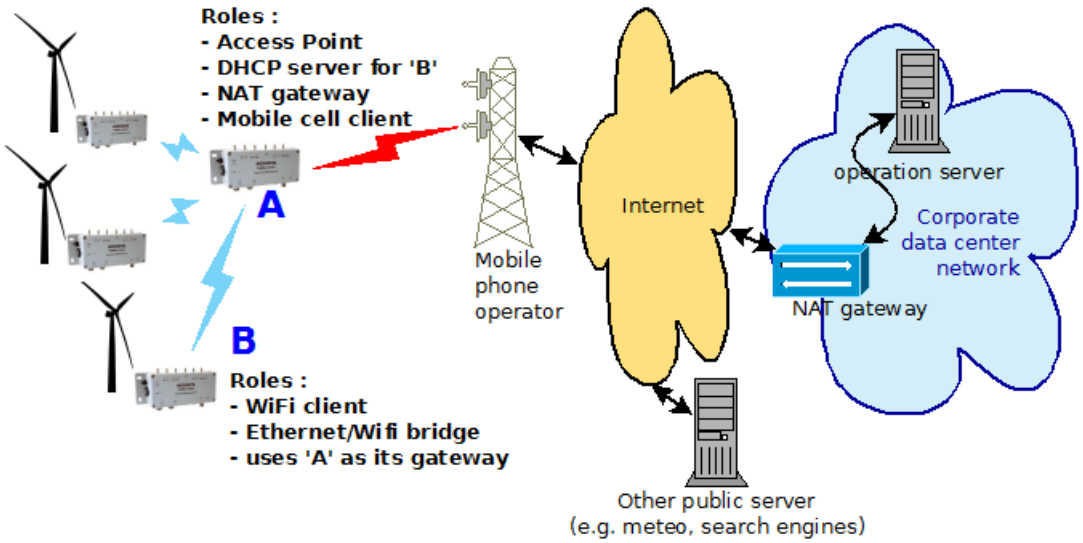
그림에서 GRE 엔드포인트는 NAT 게이트웨이에 설치되어 있지만, NAT 가 해당 장치로 전달 규칙을 갖고 있다면 다른 장치에 설치할 수 있습니다.

Product A	
Device Configuration (WiFi)	
Parameter	***Value***
Enable device	on
802.11 mode	802.11ac+n
HT mode	20 MHz
Channel	36
Country code	FR
Interface Configuration (WiFi)	
Parameter	***Value***
Role	Access point
ESSID	MySsid
Network Configuration (Cellular)	
Parameter	***Value***
Enable interface	on
Replace default route	on
Use peer DNS	on
SIM1 (or SIM2) pin code	Operator provided value
Country code	FR

Product A (continued)		
Network Configuration (LAN)		
Parameter	***Value***	
Enable interface	on	
IPv4 address	192.168.0.1	
IPv4 Netmask	255.255.255.0	
DHCP Service		
Parameter	***Value***	
Ignore interface	off	Client
Virtual interfaces/L2 tunnels		
Remote IP v4	Public address of data center NAT gateway	
Network	LAN	
Local Endpoint network	Cellular	
Static route to remote	on	
Corporate NAT gateway/GRE endpoint		
NAT	Redirect GRE to private GRE endpoint	
Important note:	configuration of the data center gateway cannot be shown here since it depends on its manufacturer and model.	

VII.12.2 NAT/PAT gateway between LAN and Internet

이 설정에서 LAN 의 모든 장치는 제품을 게이트웨이로 사용하는 경우 인터넷에 액세스할 수 있습니다.



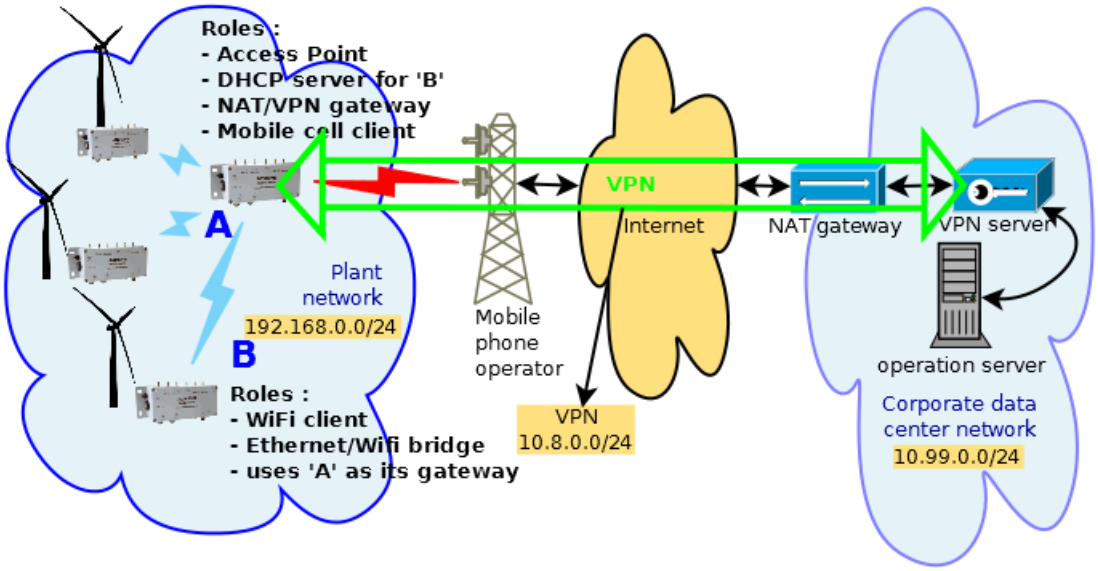
큰 그림은 위와 같지만 A 제품의 셀룰러 인터페이스는 NAT/PAT 로 설정해야 합니다. 전체 인터넷에 대한 액세스가 허용되므로 GRE 터널은 제외됩니다:

Product A		**Products B**	
Device Configuration (WiFi)		*Device Configuration (WiFi)*	
Parameter	***Value***	***Parameter***	***Value***
Enable device	on	Enable device	on
802.11 mode	802.11ac+n	802.11 mode	802.11ac+n
HT mode	20 MHz	HT mode	20 MHz
Channel	36	Channel	36
Country code	FR	Country code	FR
Interface Configuration (WiFi)		*Interface Configuration (WiFi)*	
Parameter	***Value***	***Parameter***	***Value***
Role	Access point	Role	Client
ESSID	MySsid	ESSID	MySsid
Network Configuration (LAN)		*Network Configuration (LAN)*	
Parameter	***Value***	***Parameter***	***Value***
Enable interface	on	Enable interface	on
IPv4 address	192.168.0.1	Protocol	DHCP
IPv4 Netmask	255.255.255.0	Interfaces settings tab:	
Network Configuration (Cellular)		Bridge interfaces	on
Parameter	***Value***	Interface	Wifi, LAN 1, LAN 2
Enable interface	on	*Corporate NAT gateway*	
Replace default route	on	*Important note:* the data center gateway may require extra configuration, e.g. NAT/PAT forwarding rules. It cannot be shown here since it depends on the gateway's manufacturer and application specifics.	
Use peer DNS	on		
SIM1 (or SIM2) pin code	Operator provided value		
Country code	FR		
DHCP Service			
Parameter	***Value***		
Ignore interface	off		
Firewall – public zone			
Name	Public		
Enable NAT/PAT	on		
Default acceptance policy	All disabled		
Covered networks	Cellular		
Traffic forward	As required by application		
Firewall – private zone			
Name	Private		
Enable NAT/PAT	off		
Default acceptance policy	All enabled		
Covered networks	lan		
Inter-zone forwarding	Allow to "public"		

Client

VII.12.3 Secure gateway LAN-to-private data center through Internet

이 설정에서 제품 LAN 의 모든 장치는 인터넷을 통한 VPN 을 통해 원격 회사 데이터 센터에 액세스할 수 있습니다.



'B' 장치는 게이트웨이 'A'와 데이터 센터의 VPN 서버 모두에서 라우팅 테이블이 허용하는 IP 주소에만 액세스할 수 있습니다. 게이트웨이 제품 'A'는 일반적으로 모든 트래픽을 VPN 서버로 전달하도록 설정됩니다. 그러나 VPN 외부의 특정 인터넷 위치에 대한 액세스를 허용하는 예외가 포함될 수 있습니다. VPN 서버(데이터 센터에 있는)는 일반적으로 선택된 운영 서버 그룹으로 전달을 제한하여, 원격 장치가 승인되지 않은 컴퓨터에 액세스하는 것을 금지하고, 그 반대의 경우도 마찬가지입니다.

Authentication mode

명확성을 위해 아래 구성에서는 PSK 인증을 사용합니다. 실제 설치는 인증서를 사용해야 합니다. 인증서는 더 안전하며 서버에서 여러 클라이언트를 동시에 수락할 수 있습니다. 또한 연결 시 서버에서 클라이언트로 추가 라우팅 구성을 푸시할 수 있습니다. 다음 명령을 사용하여 Linux 컴퓨터에서 PSK 를 생성할 수 있습니다:

```
openvpn --genkey --secret static.key
```

Corporate OpenVPN server configuration

전체 구성은 회사 인프라에 따라 다릅니다. 여기서는 지침만 제공할 수 있습니다.

B 제품의 구성은 이전 예시와 동일합니다.

Product A

Device Configuration (WiFi)

Parameter	Value
Enable device	on
802.11 mode	802.11ac+n
HT mode	20 MHz
Channel	36
Country code	FR

Interface Configuration (WiFi)

Parameter	Value
Role	Access point
ESSID	MySsid

Network Configuration (LAN)

Parameter	Value
Enable interface	on
IPv4 address	192.168.0.1
IPv4 Netmask	255.255.255.0

Network Configuration (Cellular)

Parameter	Value
Enable interface	on
Replace default route	on
Use peer DNS	on
SIM1 (SIM2) pin code	Operator provided value
SIM1 (SIM2) APN	Operator provided value

DHCP Service (LAN)

Parameter	Value
Ignore interface	off

Firewall – public zone

Name	Public
Enable NAT/PAT	on
Default acceptance policy	All disabled
Covered networks	Cellular
Traffic forward / Firewall	As required by application

Firewall – private zone

Name	Private
Enable NAT/PAT	off
Default acceptance policy	All enabled
Covered networks	lan
Inter-zone forwarding	Allow to “vpn2corp”
Firewall	As required by application

Product A (continued)

Firewall – vpn2corp zone

Parameter	Value
Name	vpn2corp
Enable NAT	on
Default acceptance policy	All enabled
Covered networks	vpn1
Traffic forward / Firewall	As required by application

VPN (vpn1)

Parameter	Value
Enable virtual network	on
Listener port	1194 Set to port redirected by corporate NAT to the VPN server
VPN local address	10.8.0.2 VPN server’s local address plus 1
Local routes	
Target net	10.99.0.0
Netmask	255.255.255.0
Gateway	10.8.0.1
Auth/Crypto key type	Pre-shared key
Auth/Crypto key	Upload a PEM key
Client settings/Remote OpenVPN server address	IP of corporate gateway

Client

Corporate NAT gateway / VPN server

Important note: the data center gateway may require extra configuration, e.g. NAT forwarding rules. It cannot be shown here since it depends on the gateway’s manufacturer and application specifics.

Sample OpenVPN server configuration file

```
secret /etc/openvpn/certificates/vpn1/secret
mode p2p
auth SHA1
cipher AES-256-CBC
comp-lzo no
dev tun
ifconfig 10.8.0.1 255.255.255.0
keepalive 10 30
port 1194
proto udp
route-gateway 10.8.0.2
route 192.168.0.0 255.255.255.0
topology subnet
```

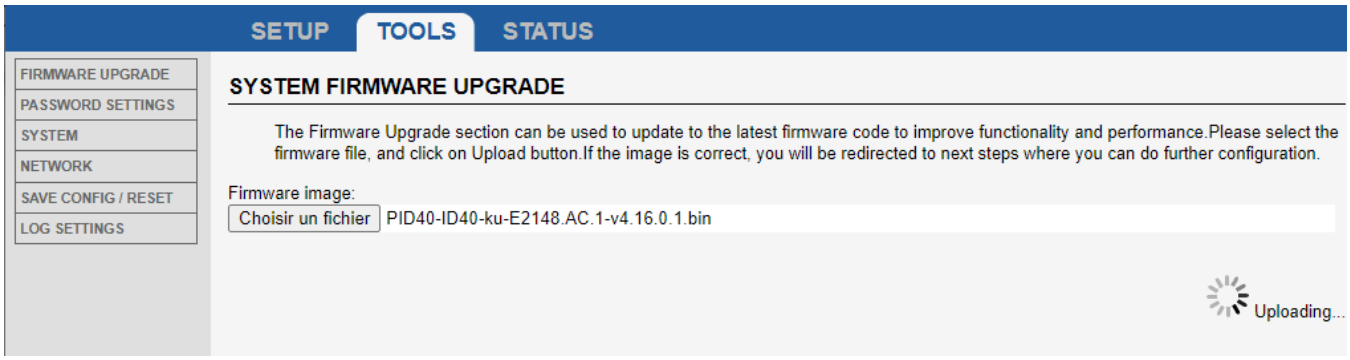
VIII FIRMWARE UPGRADE

VIII.1 Standard upgrade

VIII.1.1 Firmware file upload

웹 인터페이스를 통해 새로운 펌웨어 버전을 쉽게 업로드 할 수 있습니다.

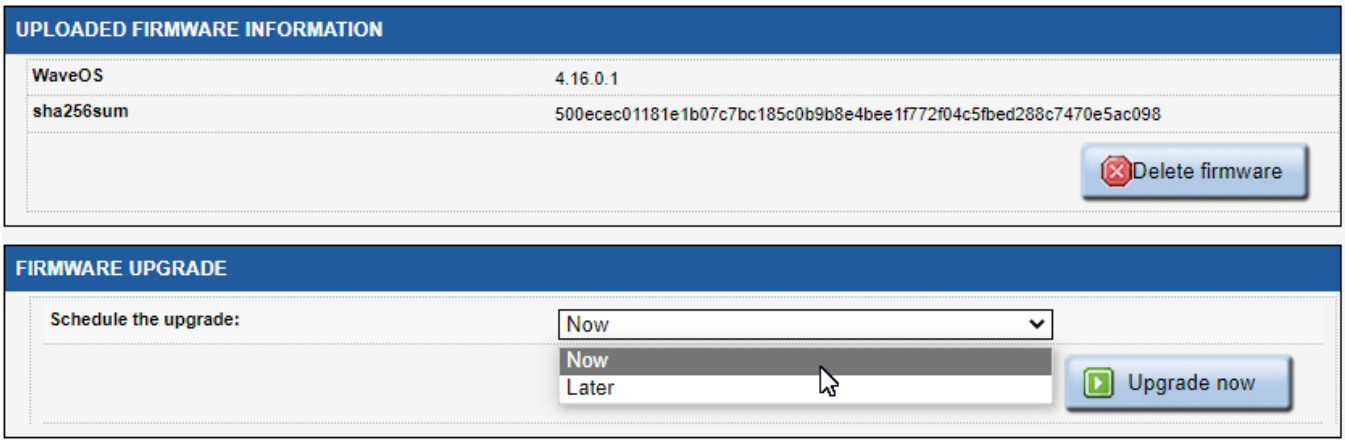
TOOLS→FIMWARE UPGRADE→SYSTEM UPGRADE



업로드가 완료되면 업그레이드 메뉴가 표시됩니다.

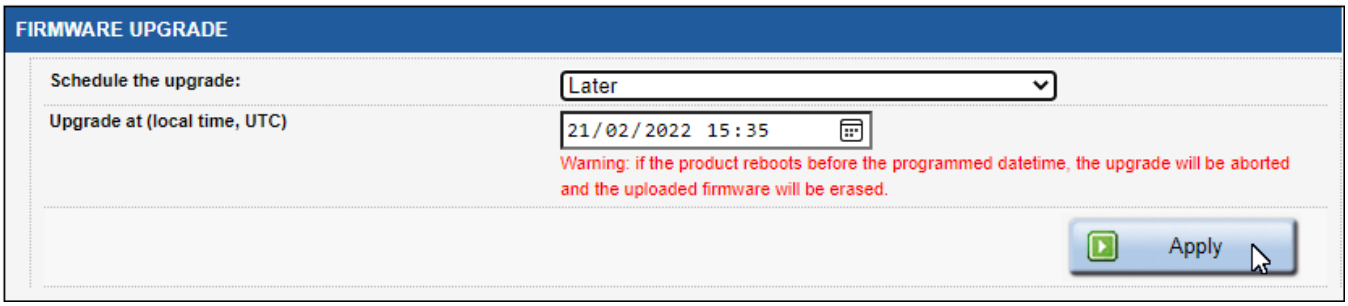
VIII.1.2 Firmware immediate upgrade

Upgrade now 버튼을 클릭하여 펌웨어를 즉시 업그레이드 할 수 있습니다. 업그레이드가 진행된 후 재 부팅 됩니다.



VIII.1.3 Firmware scheduled upgrade

펌웨어 업그레이드를 시작할 날짜와 시간을 예약할 수도 있습니다. 기본적으로 라우터 날짜 및 시간은 agenda 에 표시됩니다. 또한 과거의 날짜로 선택 할 경우 '현재 날짜와 같거나 이후여야 한다'는 경고 메시지가 표시됩니다.

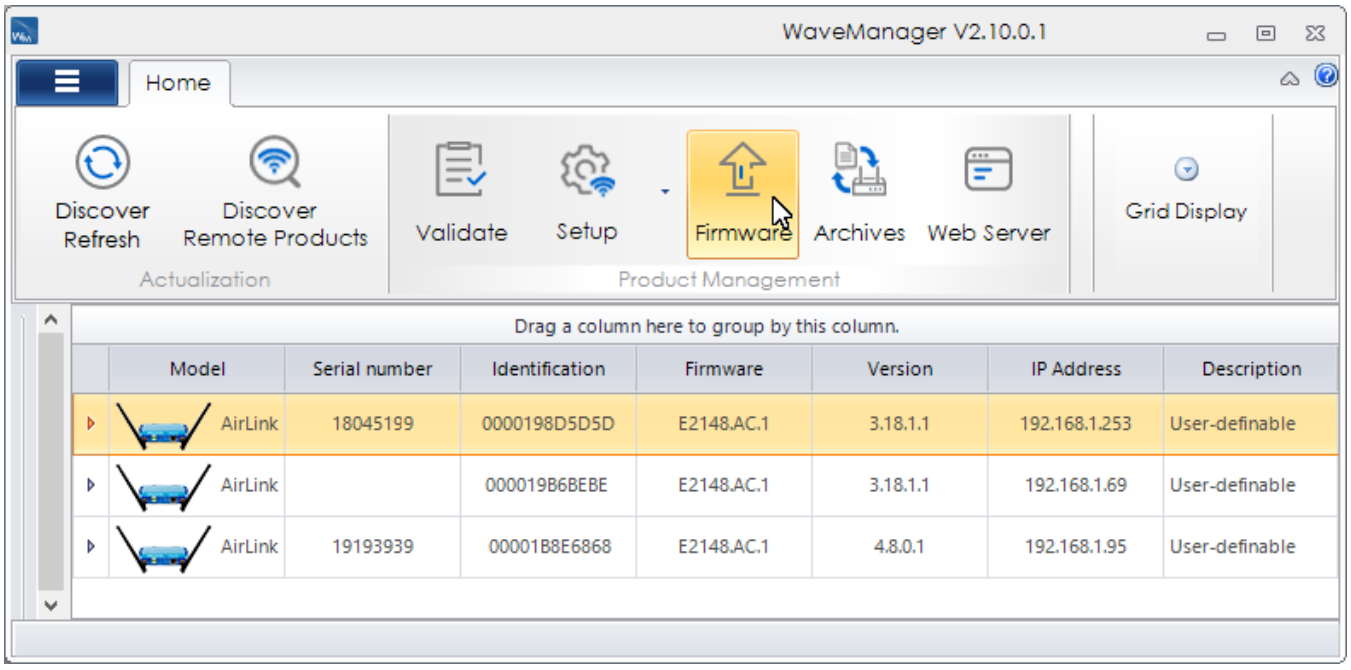


펌웨어 업그레이드와 상관없이 이전의 모든 설정은 변경되지 않고 유지됩니다.

VIII.2 Upgrade in WaveManager

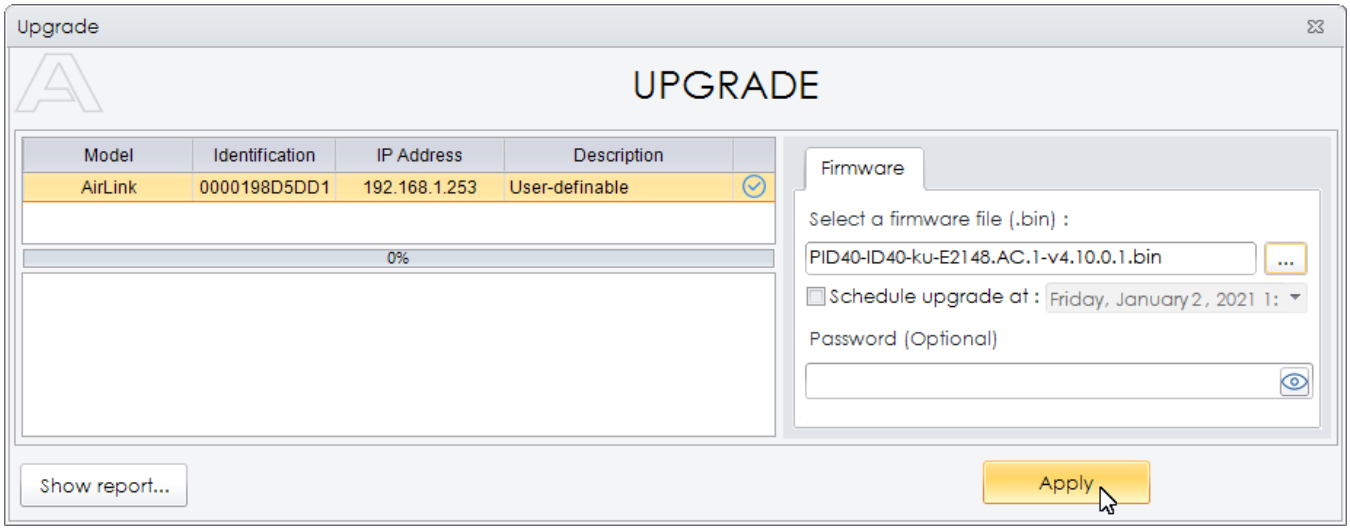
WaveManager 소프트웨어를 통해서도 펌웨어를 업데이트 할 수 있으며, 여러 대의 제품을 동시에 업그레이드 시킬 수 있습니다.

제품 목록에서 업그레이드 할 제품을 선택하고 **Firmware** 버튼을 클릭합니다.

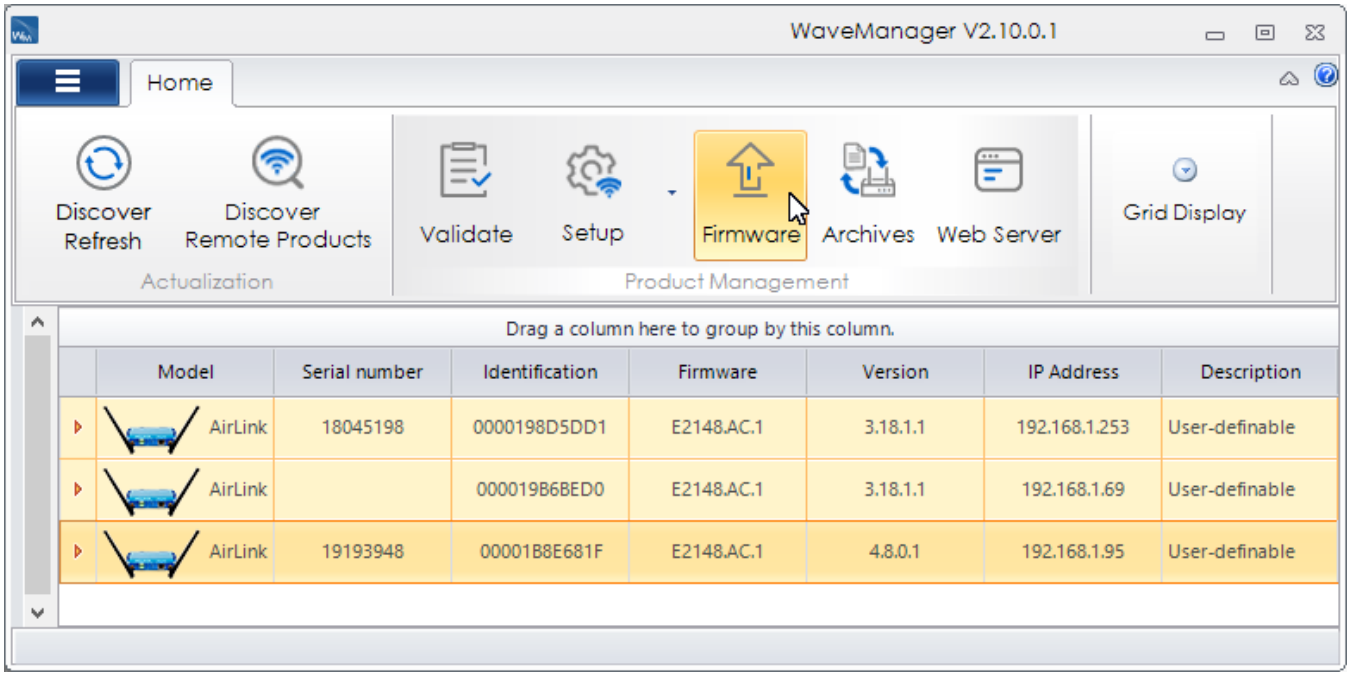


제품의 서브넷이 PC 의 IP 와 서브넷과 일치하지 않을 경우 소프트웨어를 통해 제품의 IP 및 서브넷을 변경 한 후 펌웨어를 업그레이드 할 수 있습니다.

Upgrade 창이 표시되면 업그레이드 할 펌웨어를 선택 한 후, 관리자 암호를 입력하고 (필요한 경우), **Apply** 버튼을 클릭합니다



메인 리스트에서 여러 제품 (동일한 모델)을 다중 선택하여 동시에 여러 대의 제품을 업그레이드 할 수 있습니다:



해당 소프트웨어의 상세 자료는 WaveManager user's guide 를 참고하여 주시기 바랍니다.

VIII.3 Bootloader upgrade

부트로더는 제품 부팅 및 긴급 업그레이드를 처리하는 별도의 모듈입니다. 매우 중요한 업그레이드이며 이 업그레이드 중에 정전이 발생하면 제품이 손상될 수 있습니다. 따라서 제품 반품을 피하기 위해 ACKSYS 에서 요청한 경우에만 부트로더를 업그레이드해야 합니다.

다음 권장 사항을 준수하세요:

- 강력한 전원 공급 장치를 사용하세요.
- 생산라인보다 조용한 책상을 선택하세요.
- 웹 페이지 새로 고침을 시도하기 전에 제품이 완전히 재부팅될 때까지 기다리세요.
- 질문이 있으면 주저하지 말고, ㈜와이트리(tech@witree.co.kr)에 문의 바랍니다.

제품에 해당하는 부트로더 패키지를 얻으려면 Acksys 기술 지원에 문의하세요. 내부 웹 인터페이스의 TOOLS/FIRMWARE UPGRADE 페이지를 사용하여 부트로더 업그레이드를 적용할 수 있습니다. 절차는 일반 펌웨어 업그레이드와 동일한 업그레이드 프로세스를 사용합니다:

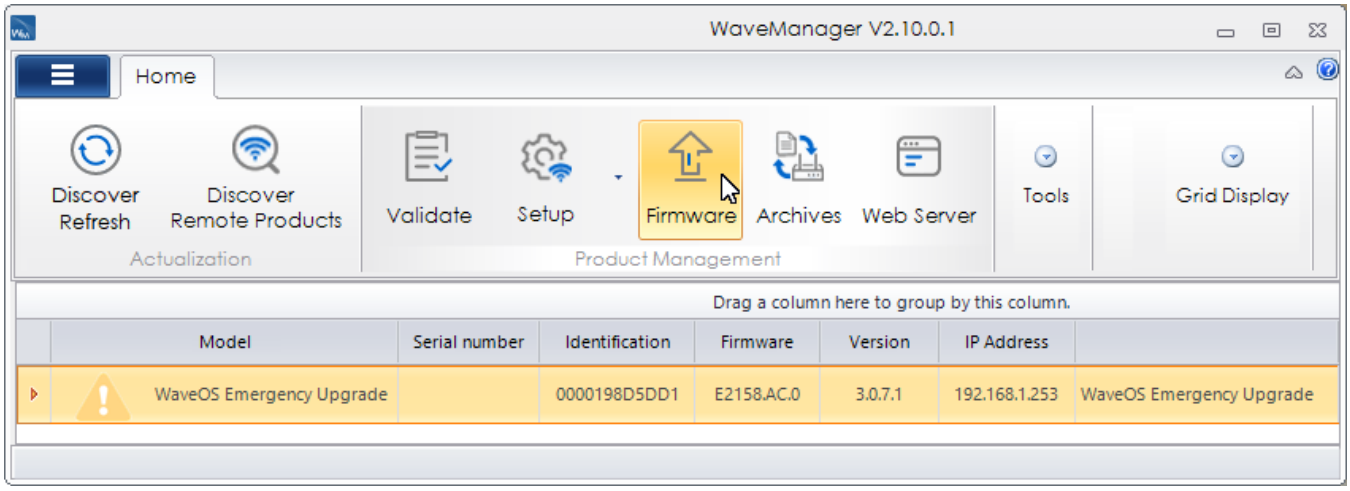
- 업그레이드 파일을 선택하려면 찾아보기 버튼을 클릭합니다.
- 업그레이드를 수행하려면 실행 버튼을 클릭하세요.

VIII.4 Fallback after an interrupted upgrade operation

예를 들어 플래시 EPROM 프로그래밍 중에, 예기치 않은 전원 공급 장치 오류로 업그레이드가 실패되었을 경우, 자동으로 장애 복구 모드로 전환됩니다.

다음에 재 부팅 시, 펌웨어가 불완전함이 확인되면 자동으로 긴급 업그레이드 모드를 시작합니다. DIAG LED 가 빠르게 깜박이면 장애 복구 모드 상태를 뜻합니다. (정상 작동 모드에서는 이 LED 가 녹색이거나 꺼져 있습니다). 그 후 ACKSYS WaveManager 소프트웨어에서 펌웨어 업로드만 허용되게끔 전환됩니다.

간단한 재설정만으로는 충분하지 않은 경우, Wavemanage 에서 펌웨어를 업데이트해야 합니다. 긴급 업그레이드 모드의 제품은 WaveManager 에서 명확하게 식별할 수 있습니다. 목록에서 장치를 선택한 다음 펌웨어를 클릭하고 위의 VIII.1 장에 표시된 대로 장치를 업그레이드합니다.



제품이 긴급 업그레이드 모드일 때 리셋 버튼을 2 초 이상 누르면 공장 초기화가 가능합니다.

자발적으로 긴급 업그레이드 모드로 들어갈 수 있습니다. 제품 시작 중에 Diag LED 가 깜박이기 시작할 때까지 재설정 버튼을 길게 누릅니다.

IX TROUBLESHOOTING

해당 섹션을 통해 제품이 이상 동작 할 경우에 대한 해결 방법을 확인할 수 있습니다.

네트워크 스니퍼는 네트워크 연결을 디버깅할 때 매우 유용할 수 있습니다.

Windows 및 Linux 에서 작동하는 무료 스니퍼인 WireShark 를 권장합니다.

IX.1 Basic checks

Check power supply LED(s)

Power LED 가 OFF 되어 있는 경우, 전원이 올바르게 연결되어 있는지 확인하고, 공급된 전류와 전압이 허용 가능 범위 인지 확인합니다. 또한 이중 전원을 지원하는 제품의 경우, 하나의 전원만으로도 동작할 수 있습니다.

Check Diag LED

Diag LED 는 부팅 후 약 30~50 초 후에 적색에서 녹색으로 변경됩니다. 영구적으로 적색으로 표시 될 경우에는 고장일 가능성이 있습니다. 또한 빠르게 깜박이면 Emergency Upgrade 모드로 동작됩니다.

Check State LEDs

무선 인터페이스가 비활성화 될 경우 State LED 가 꺼집니다. 제품이 연결을 시도하거나 연결을 대기할 때 깜박거립니다. 제품이 연결될 경우 State LED 는 계속 켜져 있습니다.

제품이 Client 로 설정되어 있을 경우 AccessPoint 에 연결을 시도하며 WLAN LED 가 청색으로 깜박입니다.

- AccessPoint 가 범위 내에 있는지 확인합니다.
- AccessPoint 의 설정값이 Client 와 동일한지 확인합니다.

Check WLAN LEDs

- WLAN LED 는 프레임을 전송하거나 수신할 때마다 깜박입니다. 데이터 전송이 진행되지 않는 경우에도 관리 프레임이 해당 LED 를 깜박이게 할 수 있습니다.

IX.2 Network configuration checks

Check IP address

IP 주소 확인: 다음은 모든 네트워크 장치가 동일한 LAN(테스트에 사용되는 컴퓨터, 제품, 원격 장치)에 있다고 가정합니다:

- 모든 네트워크 장치의 IP 서브넷은 동일해야 합니다.(RFC 950 참고)
  예를 들어, 192.168.1.253/24 와 192.168.1.10/24 는 동일한 서브넷에 있지만, 192.168.1.253/24 와 128.1.1.10/24 는 동일하지 않습니다.
- 모든 네트워크 장치의 넷마스크가 동일해야 합니다.
- 한 장치의 IP 주소를 변경할 때, 다른 장치는 ARP 캐시에서 몇 분 동안 이전 주소를 유지합니다. CMD 에서 "arp –d" (윈도우 OS) 명령어를 사용하거나 캐싱 장치의 전원을 종료하면 삭제됩니다.
- OS 의 방화벽이 통신에 영향을 줄 수 있습니다.
- 웹 인터페이스 (TOOLS / NETWORK 메뉴)를 통해 ping 명령을 웹 페이지에서 표시할 수 있습니다.

Check security parameters

초기 무선 설정 시 보안을 제외하고 설정합니다. 제품이 올바르게 동작하는 것을 확인한 이후 보안을 설정 하는 것을 권고 드립니다.

Check Wi-Fi parameters

모든 Wi-Fi 제품의 무선 설정 값은 서로 동일해야 합니다. SSID, 채널, 802.11 모드, 무선 모드(Infrastructure, Mesh, Repeater, AD-hoc 등)를 확인합니다. 확실하지 않은 경우에는 모든 통신 장치에 동일한 고정 채널을 설정하고, 4-addresses bridging 모드를 사용하지 마세요. 이 형식은 일부 AP 와는 호환되지 않을 수 있습니다.

IX.3 Cellular configuration checks

Check Status LED

꺼져 있으면 장치를 활성화하지 않은 것입니다.(상태/네트워크/셀룰러)
깜박이면 SIM 카드 또는 안테나에 문제가 있는 것입니다.

Check SIM

올바른 PIN 코드를 입력했는지 확인하세요. 선택한 SIM 이 SIM 이 삽입된 슬롯과 일치하는지 확인합니다.

시스템 로그 및 셀룰러 서비스를 "정보" 수준으로 설정하고 시스템 로그에서 "PIN 코드 이벤트" 메시지를 확인하세요.

Check antenna(s)

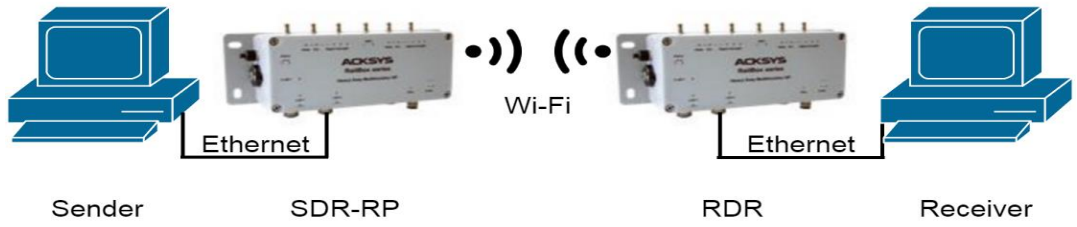
메인 안테나가 연결되어 있고 중간에 있는 모든 SMA 커넥터가 단단히 고정되어 있는지 확인하세요. RPSMA 가 아닌 SMA 커넥터를 사용하고 있는지 확인하세요. 적절한 안테나를 사용하고 있는지 확인하세요. Wi-Fi 안테나는 작동하지 않습니다.

Check Operator subscription

사용할 준비가 되었나요? 유료인가요? 일반 휴대전화에 SIM 을 삽입하여 가입 가능 여부와 해당 지역의 무선 신호 존재 여부를 확인하세요.

IX.4 Multicast router checks

이 섹션에서는 다음 참조 구성이 사용됩니다:



Sender 멀티캐스트 트래픽을 보냅니다..

SDRRP 멀티캐스트 라우터, 오른쪽 이더넷의 지정된(단독) 라우터 및 멀티캐스트 그룹의 랑데뷰 포인트(발신자 측 지정 라우터 및 랑데뷰 포인트)입니다.

RDR 멀티캐스트 라우터로 왼쪽 이더넷에 지정된(유일한) 라우터(Receive side Designated Router)입니다.

Receiver 발신자가 보낸 멀티캐스트 트래픽을 읽는 소프트웨어를 실행합니다.

Check unicast configuration

- Receiver 에서 RDR, SDRRP, Sender 각각에 대해 ping 을 수행할 수 있습니까?
- Sender 에서 SDRRP, RDR, Receiver 각각에 대해 ping 을 수행할 수 있습니까?
- RDR 에서 Receiver, SDRRP, Sender 각각에 대해 ping 을 수행할 수 있습니까?
- SDRRP 에서 Receiver, RDR, Sender 각각에 대해 ping 을 수행할 수 있습니까?

Run software

발신자와 수신자 소프트웨어를 지금 실행하세요.

Check multicast configuration in SDRRP

- "Enable multicast", "Enable bootstrap" 및 "Rendezvous point Candidate" 체크박스가 모두 체크되어 있나요?
- "로컬 랑데뷰 포인트 구성"에 적절한 그룹 접두어가 포함되어 있나요?
- 두 개의 네트워크 인터페이스가 이더넷에 도달하고 Wi-Fi 가 멀티캐스트를 처리할 수 있도록 설정되어 있나요? 지금은 다른 매개변수에 대한 기본값을 그대로 둡니다.

이제 SDRRP 에서 멀티캐스트 로그 수준이 디버그로 설정된 경우 10 초마다 다음 메시지를 볼 수 있습니다:

```
daemon.debug pimd[nnn]: move_kernel_cache: SG
```

또한 "상태/네트워크/멀티캐스트 경로"는 때때로 멀티캐스트 경로 섹션의 발신자 주소를 간략하게 표시할 수 있습니다. 이는 수신기의 가입 요청이 아직 SDRRP 에 도달하지 않았음을 나타냅니다.

발신자 주소가 안정적이고 멀티캐스트 경로 섹션에서 "사용 중"이면, 발신자 확인 아래를 참조하세요.

- SDRRP 에서 "Status/network/multicast route"를 보세요.
  - "network interfaces" 섹션에서 예상 라인의 "Neighbor MC routers" 열에 RDR 의 IP 주소가 표시되나요? 그렇지 않으면 Wi-Fi 링크에 대해 RDR 이 활성화되지 않았거나 링크가 설정되지 않았습니다.
  - "Rendezvous points" 섹션에서 귀하의 그룹이 보이나요? SDRRP 의 주소와 연결되어 있나요? BSR 주소가 RDR 또는 SDRRP 중 하나인가요?

Check multicast configuration in RDR

- RDR 에서 "상태/네트워크/멀티캐스트 경로"를 확인합니다.
  - "network interfaces" 섹션에서 수신기 측 이더넷 인터페이스에 대한 "DR" 확인란이 표시되어 있나요? 그렇지 않으면 이 네트워크에 다른 PIM 라우터가 있습니다.
  - "network interfaces" 섹션에서 예상 라인의 "Neighbor MC routers" on the 열에 SDRRP 의 IP 주소가 표시되나요?
  - "network interfaces" 섹션에서 예상 라인의 "IGMP reports" 열에 멀티캐스트 그룹이 표시되나요? 그렇지 않으면 수신기에 문제가 있습니다. 멀티캐스트 대신 유니캐스트 주소를 사용하거나 224.0.0.X/24 범위의 멀티캐스트를 사용하거나 IGMPv3 를 사용하고 IGMPv2 를 구성했을 수 있습니다.
  - "multicast routes" 섹션에 그룹에 대한 경로가 표시되나요? "RP address" 는 SDRRP 의 주소인가요? 수신 인터페이스가 수신기가 연결된 인터페이스인가요?
  - "Rendezvous points" 섹션에서 귀하의 그룹이 보이나요? SDRRP 주소와 연결되어 있나요? BSR 주소가 RDR 또는 SDRRP 중 하나인가요? 그렇지 않으면 BSR 이 없고, 랑데부 포인트가 잘못 구성되어 있습니다.

Check IP options in Sender

이러한 확인은 사용하는 소프트웨어에 따라 다릅니다.

- Sender 가 사용하는 TTL 을 다시 확인하세요. 가능하면 "tcpdump"(Linux) 또는 "Wireshark"(Windows 및 Linux)로 이더넷 트래픽을 덤프하세요. 나가는 프레임의 TTL 을 표시합니다.
- 프레임의 크기를 다시 확인하세요. 가능하면 첫 번째 시도에서 줄이세요. 1000 바이트는 아무데나 통과해야 합니다. "iperf" 또는 "jperf"를 사용하여 알려진 프레임 크기로 멀티캐스트 트래픽을 생성할 수 있습니다.

Check UDP options in Sender and Receiver

- 동일한 UDP 포트를 사용합니까? 동일한 데이터 형식인가요?

X FREQUENTLY ASKED QUESTIONS

이 섹션에서는 제품 작동의 다양한 측면에 대한 질문과 답을 확인할 수 있습니다.

X.1 장치를 공장 초기화 하는 방법?

웹 인터페이스를 통해 공장 초기값으로 설정할 수 있으며 경우에 따라 하드웨어의 리셋 버튼을 사용하여 재설정 할 수 있습니다. 재설정 버튼의 위치는 제품 설명서를 참조하세요. 초기화 절차는 다음과 같습니다:

DIAG LED 가 빨간색으로 바뀔 때까지 리셋 버튼을 3 초 이상 계속 누르고 있다가 버튼에서 손을 뗍니다. DIAG LED 가 다시 녹색으로 바뀔 때까지 기다린 다음 WaveManager 를 사용하여 장치의 IP 주소가 공장 기본값 192.168.1.253 으로 재설정되었는지 확인하세요.

X.2 Transparent Client mode 를 찾을 수 없습니다.

Transparent Client 모드는 **Client (infrastructure)** 와 다르며 Interface – Advanced settings 탭에서 Bridging 모드를 4-address format(WDS) 로 변경해야 합니다.

X.3 Wi-Fi bit 전송률은 어떻게 선택됩니까?

프레임 전송에 사용되는 비트 전송률은 몇 가지 고려 사항에 따라 달라지며, 두 장치 간의 처리량과 다른 장치에 남겨진 대역폭 모두에 큰 영향을 미칠 수 있습니다.

일부 프레임은 항상 사용 가능한 최저 비트 전송률로 전송됩니다. 브로드캐스트 및 멀티캐스트는 모든 스테이션을 향하므로, 가능한 가장 먼 거리에 도달해야 합니다. 관리 프레임이 중요하며 가능한 많은 수신이 보장되어야 합니다.

구성된 최저 비트 전송률만큼은 항상 전송되어야 합니다. 이 비트 전송률은 연결 후 시작 값으로 사용됩니다. 그런 다음 MINSTREL 이라는 동적 적응 알고리즘이 사용되어 다른 속도에서 더 나은 처리량을 주기적으로 확인하면서 최적의 속도로 빠르게 수렴합니다. MINSTREL 알고리즘은 다음에 설명되어 있습니다:
http://linuxwireless.org/en/developers/Documentation/mac80211/RateControl/minstrel/

X.4 WMM, WME, IEEE802.11e 의 차이점?

QoS 기능의 다양한 이름입니다. IEEE802.11e 는 WME QoS 의 확장으로, APSD(자동 절전 전달) 및 드물게 사용되는 프로토콜인 HCCA 를 추가합니다.(QoS Wi-Fi 는 일반적으로 EDCA 를 사용함) 이 제품은 IEEE802.11e 의 필수 기능으로 구성된 WME 를 지원합니다. WMM 은 WME 의 다른 이름입니다.
WME 기능은 4 개의 우선 순위 클래스(최선, 백그라운드, 비디오, 음성)로 구성됩니다. 전송된 각 프레임은 하나의 클래스에 속하며 에어 미디어의 경합/충돌 해결을 위한 매개 변수는 클래스에 따라 미세 조정될 수 있습니다.

X.5 Multicast

X.5.1 웹 인터페이스에서 멀티캐스트 경로가 불안정합니다.

멀티캐스트 그룹을 구성하고 해당 멀티캐스트 발신자를 시작한 후 웹 인터페이스, 페이지 상태/네트워크/멀티캐스트 경로 목록에서 경로가 들어오고 나가는 것을 테스트할 수 있습니다.

가장 자주 발생하는 원인은, 라우터가 멀티캐스트 흐름을 수신하지만 나가는 인터페이스가 구성되지 않았기 때문입니다.

설정/라우팅/멀티캐스트 라우팅 페이지의 "local networks configuration" 섹션에서 관련 인터페이스를 확인하세요.

수신기의 IGMP 보고서에 예상되는 멀티캐스트 그룹이 포함되어 있는지 확인하세요. (아래의 다음 FAQ 참조).

X.5.2 Receiver device 가 IGMP 보고서에서 멀티캐스트 그룹을 보내지 않습니다.

Linux 장치에서 IGMP 메시지는 다음과 같은 라우팅 테이블(적절한 라우팅 항목을 포함해야 하는)에 의해 정의된 인터페이스에서만 전송됩니다.

```
$ route -n
Destination  Gateway   Genmask     Flags Metric Ref    Use Iface
(…)
224.0.0.0    0.0.0.0   240.0.0.0   U     0      0      0 eth0
```

X.6 CISCO 액세스 포인트가 내 클라이언트 브리지랑 연결이 안됩니다.

SSID, 채널 및 보안이 올바르게 설정되어있다고 가정합니다. LAN 을 CISCO AP 에 연결하려면 프록시 ARP 서버가 비활성화되도록 CISCO AP 에서 "수동 모드"를 사용해야 합니다. 섹션 *V.2.6.2a Masquerading (ARPNAT)* 을 참조하세요.

X.7 Fast roaming 기능

아래 제공된 수치는 펌웨어 버전 2.2.0 에 대해 정확하며 이 문서의 향후 릴리스에서 필요에 따라 업데이트됩니다.

X.7.1 사전 로밍이 활성화된 경우 스캔 기간은 어떻게 됩니까?

클라이언트가 연결되면 능동적 로밍이 활성화된 채널을 순환합니다. 각 채널은 약 56ms 동안 스캔되며, 이 기간 동안 라디오는 "오프 채널"로 간주되어 데이터가 흐를 수 없습니다. 그런 다음 데이터 전송을 허용하기 위해 각 채널 스캔 사이에 200ms 일시 중지가 발생되고, CPU 사용량과 오프 채널 시간을 줄여 처리량을 향상시키기 위해 주기 사이에 추가 지연을 구성할 수 있습니다.
200ms 일시 정지는 스캔할 채널이 현재 사용 중인 채널인 경우 발생하지 않습니다.
예를 들어, 지연이 3000ms 로 구성된 4 채널 스캔의 경우 스캔 기간은 56ms + 0ms + 56ms + 200ms + 56ms + 200ms + 56ms + 3000ms = 3464ms 입니다. 라디오는 오프 채널일 때 통신할 수 없습니다. 이 경우에는 (3x56)/3464 = 시간의 4,8%입니다. 그에 따라 처리량이 줄어듭니다.
이 수치는 근사치일 뿐이며 부하가 매우 높을 경우에는 달라질 수 있습니다.

X.7.2 현재 액세스 포인트가 갑자기 사라질 때 로밍 지연은 무엇입니까?

예를 들어 터널의 모퉁이를 돌 때 큰 장애물이 갑자기 전파를 방해할 때 발생할 수 있습니다. 이는 AP 의 전원이 꺼져 있거나, 어떤 이유로든 실패하는 경우에 발생할 수 있습니다. 클라이언트 제품에는 여러 가지 방법이 있습니다:
- 클라이언트가 AP 로 데이터를 보내고 AP 가 더 이상 이를 승인하지 않으면 클라이언트는 승인되지 않은 50 프레임 후에 연결을 끊습니다. 각 프레임은 관련 재시도 절차 및 적절한(구성 가능) 지원 속도를 사용하여 재시도됩니다.
- 클라이언트가 데이터를 보내지 않으면 AP 에서 받은 비콘에 의존합니다. 클라이언트는 여러 개의 연속된 비콘이 누락된 경우를 감지합니다. 그런 다음 두 개의 추가 제어 프레임(각각 10 회 재시도)을 전송하여 AP 를 추가로 조사합니다. AP 가 여전히 응답하지 않으면 클라이언트는 연결을 끊습니다. 누락된 비콘의 수는 구성 가능합니다.
이 절차의 총 기간은 구성된 수, AP 구성에 설정된 비콘 간격 기간 및 가장 낮게 구성된 기본 속도(제어 프레임과 관련된 프로브의 경우)에 따라 다릅니다.

X.8 GRE tunnel 가 데이터를 전달하지 않습니다.

터널의 양쪽 끝에서 GRE 끝점 IP 주소가 정확하고, 각 측면에서 서로 ping 할 수 있는 경우에는 코너 케이스에서 다음과 같이 발생할 수 있습니다.

- GRE 터널 로컬 엔드포인트는 무선 액세스 포인트 인터페이스를 사용합니다.

- AP 가 ACS 또는 DFS 지연으로 인해 빠르게 초기화할 수 없는 방식으로 구성됩니다.

이 경우 시작 시 GRE 터널은 원격 끝점으로 나가는 경로를 검색하지만, 아직 존재하지 않기 때문에 찾을 수 없습니다. 잘못된 방향을 가리키는 기본 경로로 되돌아갑니다.

해결 방법은 AP 설정을 변경하거나 AP 네트워크 인터페이스를 브리지에 포함하는 것입니다. 소프트웨어 브리지에는 시작 지연이 없으므로, GRE 터널은 항상 브리지를 찾을 수 있습니다.

X.9 RA 서버에서 IPv6 주소를 가져오기 위해 SLAAC 에서 LAN 을 구성하는 방법

4.18.0.1 버전의 WaveOS 는 DHCPv6 가 아닌 RA 서버를 지원하여 인프라 모드에서 호스트 주소를 지정합니다. 이 장은 IPv6 및 RA 서버 섹션의 개요입니다.

X.10 NAT router 를 통한 FTP

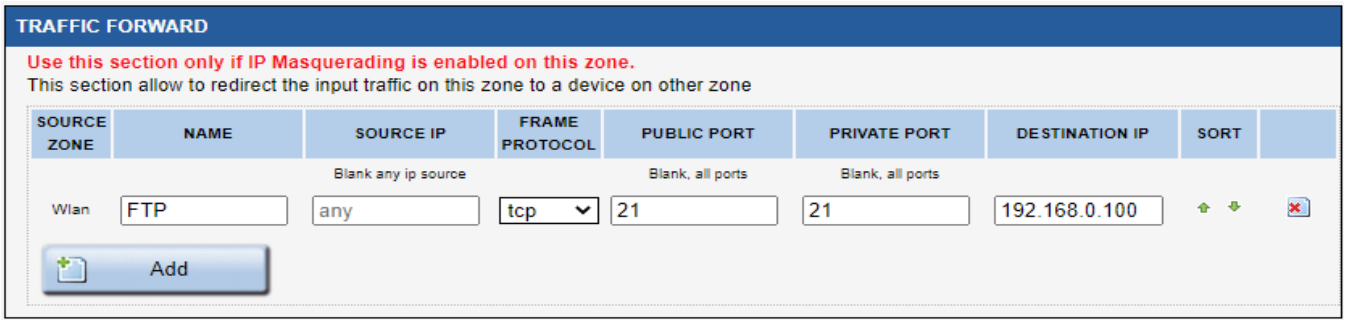
FTP 전송에는 일반적으로 두 개의 TCP 연결이 포함됩니다. 첫 번째 제어 연결은 FTP 클라이언트에서 FTP 서버의 포트 21 로 이동합니다. 이 연결은 로그온에 사용되며 엔드포인트 간에 명령 및 응답을 전송합니다. 데이터 전송("ls" 및 "dir" 명령의 출력 포함)에는 두 번째 데이터 연결이 필요합니다.

FTP 클라이언트는 2 가지 모드로 작동할 수 있습니다.

Passive Mode: 클라이언트가 PASV 명령을 내립니다. 이 명령을 수신하면 서버는 동적으로 할당된 포트에서 수신 대기한 다음 클라이언트에 PASV 응답을 보냅니다. PASV 응답은 서버가 수신 대기 중인 IP 주소와 포트 번호를 제공합니다. 그런 다음 클라이언트는 해당 IP 주소 및 포트 번호에 대한 두 번째 연결을 엽니다.

Active Mode: 클라이언트는 동적으로 할당된 포트에서 수신한 다음 서버에 PORT 명령을 보냅니다. PORT 명령은 클라이언트가 수신 대기 중인 IP 주소와 포트 번호를 제공합니다. 그런 다음 서버는 해당 IP 주소 및 포트 번호에 대한 연결을 엽니다.

데이터 전송이 NAT 라우터를 통과해야 하는 경우, 공개 영역에서 로컬 대상 IP, 포트 21 로 FTP 흐름의 리디렉션을 보장하기 위해, NAT 영역의 정방향 트래픽 테이블을 입력해야 합니다.



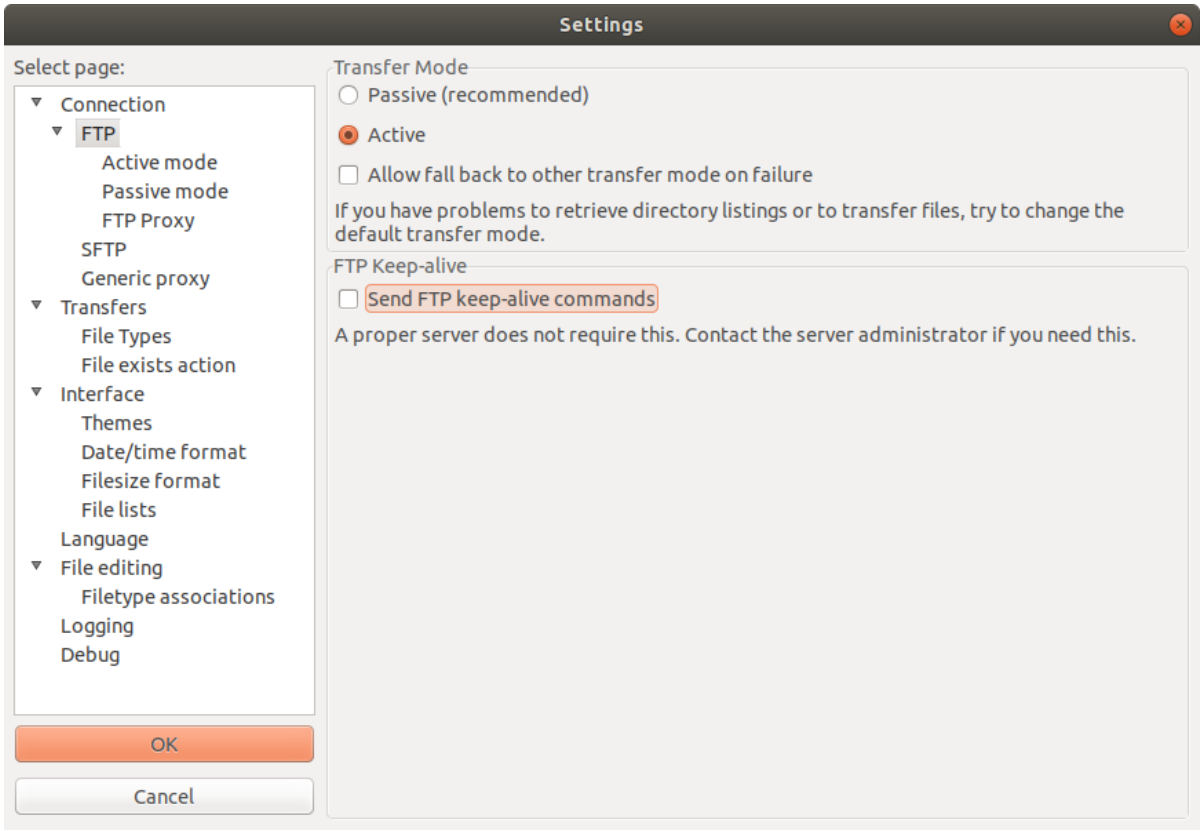
FTP 서버가 공용 영역에 있는 경우 FTP 클라이언트는 수동 모드로 구성되어 FTP DATA 연결의 소스가 됩니다. (FileZilla 의 기본 모드)

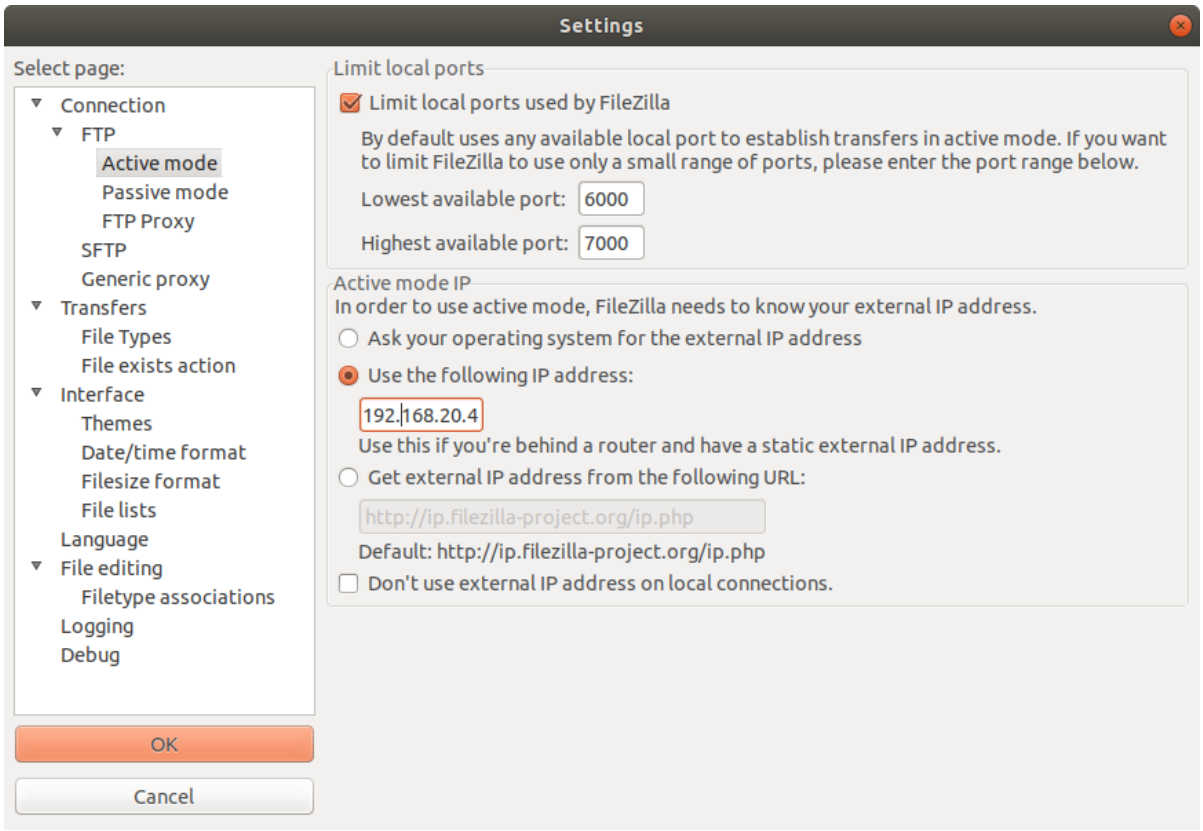
서버가 비공개 영역에 있는 경우 FTP 클라이언트가 활성 모드로 구성되어 FTP DATA 연결의 소스가 되어야 합니다. 활성 모드에서 FileZilla FTP 클라이언트를 구성하는 방법은 다음과 같습니다.

- 클라이언트 설정 섹션의 FTP 페이지에서 활성 모드를 선택합니다.

- 활성 모드 페이지에서 FileZilla 에서 사용하는 로컬 포트 제한 상자를 선택합니다. 무료인 경우 기본 범위를 그대로 두거나 고유한 범위를 정의할 수 있습니다.

- 다음 IP 주소 사용 체크 후 공유기의 공인 IP 주소를 입력합니다.


Settings
Select page:
Connection
FTP
Active mode
Passive mode
FTP Proxy
SFTP
Generic proxy
Transfers
File Types
File exists action
Interface
Themes
Date/time format
Filesize format
File lists
Language
File editing
Filetype associations
Logging
Debug
OK
Cancel
Transfer Mode
Passive (recommended)
Active
Allow fall back to other transfer mode on failure
If you have problems to retrieve directory listings or to transfer files, try to change the default transfer mode.
FTP Keep-alive
Send FTP keep-alive commands
A proper server does not require this. Contact the server administrator if you need this.


Settings
Select page:
Connection
FTP
Active mode
Passive mode
FTP Proxy
SFTP
Generic proxy
Transfers
File Types
File exists action
Interface
Themes
Date/time format
Filesize format
File lists
Language
File editing
Filetype associations
Logging
Debug
OK
Cancel
Limit local ports
Limit local ports used by FileZilla
By default uses any available local port to establish transfers in active mode. If you want to limit FileZilla to use only a small range of ports, please enter the port range below.
Lowest available port: 6000
Highest available port: 7000
Active mode IP
In order to use active mode, FileZilla needs to know your external IP address.
Ask your operating system for the external IP address
Use the following IP address:
192.168.20.4
Use this if you're behind a router and have a static external IP address.
Get external IP address from the following URL:
http://ip.filezilla-project.org/ip.php
Default: http://ip.filezilla-project.org/ip.php
Don't use external IP address on local connections.

XI 부록 – 용어집 및 두문자어

802.11	무선 LAN 의 네트워크 계층 1 및 2 의 여러 변형을 설명하는 IEEE 표준
802.11s	무선 메시 네트워크를 설명하는 IEEE 802.11 표준의 일부
AP	액세스 포인트
A-MPDU	Aggregated MAC 프로토콜 데이터 단위. 여러 개의 MAC 프레임이 하나의 큰 프레임에 연결되어 하나의 청크로 전송하기 위해 물리 계층으로 전달됩니다.
BSR	부트스트랩 라우터는 RP 와 멀티캐스트 그룹 간 매핑의 동적 선택 및 배포를 담당하는 멀티캐스트 라우터입니다.
BSS	하나의 AP 와 클라이언트로 구성된 네트워크인 기본 서비스 세트
Bridge	무선 애플리케이션의 맥락에서 브리지는 LAN(이더넷) 프레임을 WLAN(Wi-Fi) 미디어로 또는 그 반대로 전송하는 네트워크 구성 요소입니다. WLAN 이 인프라 모드에 있을 때 "브리지"라는 용어는 AP 의 클라이언트에 사용되지만 기술적으로는 AP 도 브리지입니다. 더 넓은 네트워킹 맥락에서 브리지는 레벨 3 라우팅에 의존하지 않고 하나의 물리적 인터페이스에서 다른 물리적 인터페이스로 레이어 2 프레임을 전송합니다. 예를 들어 이더넷 스위치는 하드웨어 브리지이며 제품에는 이더넷, 여러 WLAN 클라이언트 또는 AP, 메시 등과 같은 다양한 인터페이스 간의 소프트웨어 브리지가 포함됩니다.
BSSID	BSS 식별자, 일반적으로 AP 의 MAC 주소 또는 그 파생어
GNSS	GPS(미국), GLONASS(러시아어), Galileo(유럽어) 또는 BeiDou(중국어) 중 하나인 글로벌 내비게이션 위성 시스템
IPv4	인터넷 프로토콜 버전 4, 올바른 대상 컴퓨터로의 패킷 전달을 담당하는 TCP/IP 프로토콜 스택의 네트워크 계층. IPv4 는 "192.168.1.1"과 같은 32 비트 크기의 주소를 사용합니다.
IPv6	인터넷 프로토콜 버전 6(IPv6)은 2 세대 네트워크 계층 프로토콜입니다. IETF(Internet Engineering Task Force)에서 설계한 IPv6 은 인터넷 프로토콜 버전 4(IPv4)의 업그레이드 버전입니다.
LAN	근거리 통신망(Local Area Network) 장치가 서로 통신하기 위해 MAC(OSI 계층 2) 주소를 직접 사용할 수 있는 네트워크의 일부
MCC	셀룰러 네트워크의 고유 국가 식별자인 모바일 국가 코드
MCS	Modulation and Coding Scheme, 비트가 802.11n 에서 전파로 인코딩되는 방식
MNC	모바일 네트워크 코드, 지정된 국가의 셀룰러 네트워크 사업자 식별자
OSI	네트워킹 시스템을 특수 계층으로 구성하는 ISO 표준 참조 모델인 Open Systems Interconnection
PSK	링크의 양쪽 끝에서 동일한 키가 사용되는 대칭 암호화 시스템인 사전 공유 키. 이는 키가 사전에 한쪽 끝에서 다른 쪽 끝으로 별도의 방식으로 전송되어야 함을 의미합니다.(이 방식은 공격 대상이 될 수 있습니다.)

Repeater	소프트웨어 브리지에서 함께 연결된 동일한 라디오의 결합된 클라이언트+AP. AP 또는 이더넷 LAN 에서 수신한 데이터는 클라이언트를 통해 원격 AP 로 전달되어 체인을 설정할 수 있습니다.
RP	Rendezvous Point 는 지정된 멀티캐스트 그룹의 배포를 담당하는 멀티캐스트 라우터입니다.
RTS/CTS	다음 데이터 프레임을 보내기에 충분한 시간 동안 공기 매체를 예약하는 작은 RTS 프레임을 보내야 하는 선택적 MAC 프로토콜. 수신자는 동일한 예약을 하는 CTS 프레임을 보냄으로써 응답합니다. 따라서 송신기와 수신기의 무선 범위에 있는 모든 무선 스테이션은 발생할 데이터 전송에 대해 알립니다.
SSID	Service Set Identifier 는 AP 그룹과 해당 클라이언트로 구성된 무선 네트워크를 식별하는 문자열입니다.
SSM	소스별 멀티캐스트는 수신자가 송신자의 주소를 알고 있으므로 RP 를 거칠 필요가 없는 멀티캐스트 라우팅의 변형입니다.
USM	사용자 기반 보안 모델은 사용자별로 SNMP 액세스 권한을 정의하는 방법입니다..
VLAN	가상 LAN, VLAN 의 각 프레임에 VLAN 태그를 추가하여 다른 LAND 에 터널링된 LAN
Wi-Fi™	”Wireless Fidelity”. 이 설명서에서 이 용어는 802.11 의 동의어로 사용됩니다.
WLAN	무선 LAN 은 서로 정보를 교환하기 위해 공통 네트워크 이름(SSID 또는 Mesh ID)과 공통 인증 방법을 공유하는 Wi-Fi 스테이션 그룹입니다.
RA	라우터 알림에는 호스트가 라우터와 동일한 링크(온링크)에 있는지 확인하는 데 사용되는 서브넷 접두사 목록이 포함되어 있습니다.

XII 부록 – 802.11 RADIO CHANNELS

XII.1 11b/g (2.4GHz)

해당 네트워크는 [2.3995-2.4965] 주파수에서 ISM (Industrial Scientific and Medical) 무선 대역을 사용합니다.

Channel (25 MHz)	Central frequency (GHz)	Allowed by
1	2,412	Asia MKK, Europe ETSI, US FCC
2	2,417	Asia MKK, Europe ETSI, US FCC
3	2,422	Asia MKK, Europe ETSI, US FCC
4	2,427	Asia MKK, Europe ETSI, US FCC
5	2,432	Asia MKK, Europe ETSI, US FCC
6	2,437	Asia MKK, Europe ETSI, US FCC
7	2,442	Asia MKK, Europe ETSI, US FCC
8	2,447	Asia MKK, Europe ETSI, US FCC
9	2,452	Asia MKK, Europe ETSI, US FCC
10	2,457	Asia MKK, Europe ETSI, US FCC
11	2,462	Asia MKK, Europe ETSI, US FCC
12	2,467	Asia MKK, Europe ETSI
13	2,472	Asia MKK, Europe ETSI
14	2,484	Asia MKK

각 채널의 중심 주파수를 지정하는 것 외에도 802.11 은 각 채널에서 허용되는 전력 분배를 정의하는 스펙트럼 마스크(17 절)도 지정합니다. 마스크는 채널이 효과적으로 22MHz 폭이 되도록 신호가 중심 주파수에서 ±11MHz 의 피크 에너지에서 최소 30dB 감쇠되어야 합니다. 스테이션이 겹치지 않고 매 5 번째 채널(일반적으로 아메리카에서는 1, 6, 11, 유럽에서는 1-13 등)만 사용할 수 있습니다. 예를 들어 할당은 영국의 경우 2400-2483.5, 미국의 경우 2402-2483.5 등입니다.

스펙트럼 마스크는 중심 주파수에서 최대 ±22MHz 까지만 50dB 감쇠되는 전력 출력 제한을 정의하므로, 채널의 에너지가 이러한 제한보다 더 확장되지 않는다고 가정하는 경우가 많습니다. 채널 1, 6, 11 사이의 분리를 감안할 때 모든 채널의 신호는 충분히 감쇠되어 다른 채널의 송신기와 간섭을 최소화해야 한다고 말하는 것이 더 정확합니다. 근거리 문제로 인해 송신기는 "중첩되지 않는" 채널의 수신기에 영향을 미칠 수 있지만, 피해자 수신기에 가깝거나(미터 이내) 허용된 전력 수준 이상으로 작동하는 경우에만 가능합니다.

XII.2 802.11a/h (5 GHz)

해당 네트워크는 5GHz 무선 대역 UN-II 를 사용합니다.

UN-II 는 4 개의 개별 하위 대역을 사용합니다: UN-II-1, 2, 2e and 3

Band	Channel (20 MHz)	Central frequency (GHz)	Allowed by
UNII 1	34	5,170	Japan TELEC
	36	5,180	Europe ETSI, US FCC
	38	5,190	Japan TELEC
	40	5,200	Europe ETSI, US FCC
	42	5,210	Japan TELEC
	44	5,220	Europe ETSI, US FCC
	46	5,230	Japan TELEC
	48	5,240	Europe ETSI, US FCC
UNII 2	52	5,260	Europe ETSI, US FCC
	56	5,280	Europe ETSI, US FCC
	60	5,300	Europe ETSI, US FCC
	64	5,320	Europe ETSI, US FCC
UNII 2e	100	5,500	Europe ETSI, US FCC
	104	5,520	Europe ETSI, US FCC
	108	5,540	Europe ETSI, US FCC
	112	5,560	Europe ETSI, US FCC
	116	5,580	Europe ETSI, US FCC
	120	5,600	Europe ETSI, US FCC
	124	5,620	Europe ETSI, US FCC
	128	5,640	Europe ETSI, US FCC
	132	5,660	Europe ETSI, US FCC
	136	5,680	Europe ETSI, US FCC
	140	5,700	Europe ETSI, US FCC
	144	5,720	Europe ETSI, US FCC
UNII 3	149	5,745	US FCC
	153	5,765	US FCC
	157	5,785	US FCC
	161	5,805	US FCC
	165	5,825	US FCC

요약:

Europe (ETSI): 19 channels

- UN-II 1 : 4 channels 36, 40, 44, 48
- UN-II-2 : 4 channels 52, 56, 60, 64
- UN-II-2e : 11 channels : 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140

US and Canada (FCC): 23 channels

- UN-II 1 : 4 channels 36, 40, 44, 48
- UN-II-2 : 4 channels 52, 56, 60, 64
- UN-II-2e : 11 channels : 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
- UN-II-3 : 4 channels : 149, 153, 157, 161, 165

Japan (TELEC): 4 channels

- UN-II-1 : 4 channels : 34, 38, 42, 46