U-F9028W

사용자 매뉴얼

Release 1.2

Table of contents

로그인 5
로그인 페이지 5
개요 6
개요 6
인터페이스 관리 7
이더넷 상태 7
이더넷 상태 7
링크 집계 8
글로벌 8
링크 집계 9
스톰 컨트롤 9
흐름 제어 11
포트 격리 12
글로벌 12
포트 격리 12
고급 설정 13
VLAN 13
VLAN 요약 13
VLAN 글로벌 설정 14
VLAN 추가/삭제 14
VLAN 인터페이스 15

엑세스/트렁크 포트 15
VLAN 분류자 16
요약 16
규칙 17
그룹 17
용법 18
MAC 18
맥 주소 테이블 18
맥 전역 구성 19
맥 학습 19
정적 맥 테이블 20
블랙홀 맥 테이블 21
정적 보안 맥 22
Mirror 23
요약 23
글로벌 설정 25
미러 설정 25
LLDP 26
글로벌 설정 26
포트 설정 27
LLDP 이웃 27
스패닝 트리 28
STP 정보 28
STP 글로벌 28

STP Interface 30
MSTP 영역 32
ACL 33
Access Control List 33
클래스 맵 37
정책 맵 39
IP 라우팅 42
IPv4 경로 42
IPv4 정적 42
OSPF 경로 44
RIP 경로 45
멀티캐스트 46
IGMP 스누핑 46
IGMP 스누핑 정보 48
네트워크 관리 49
DHCP 클라이언트 49
DHCP 클라이언트 설정 49
DHCP 클라이언트 상태 50
SNMP 50
SNMP 트랩 51
보안 52
포트 보안 52
ARP 인터셉트 53
DDoS 인터셉트 54

현재 세션 55
사용자 관리 56
시스템 관리 57
파일 관리 57
시스템 설정 58
Load 설정 58
툴 59
핑 59
Traceroute 60
재시작/저장 60

로그인

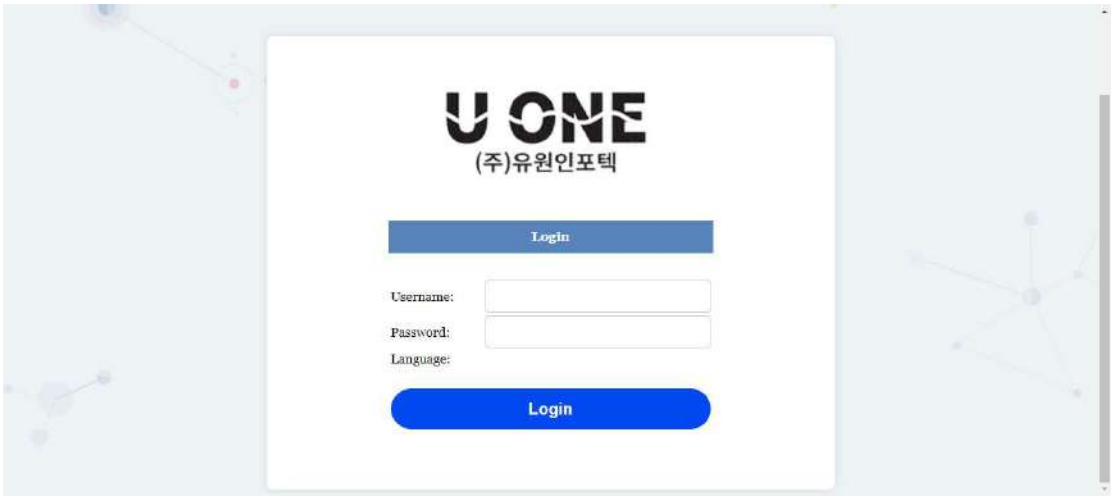
로그인 페이지

공장 출하시 기본 IP는 192.168.2.1입니다.

사용자 이름과 비밀번호를 입력한 후 로그인 버튼을 클릭하거나 Enter 키를 눌러 웹 구성 인터페이스로 들어갑니다.

- **Username** – admin
- **Password** – system

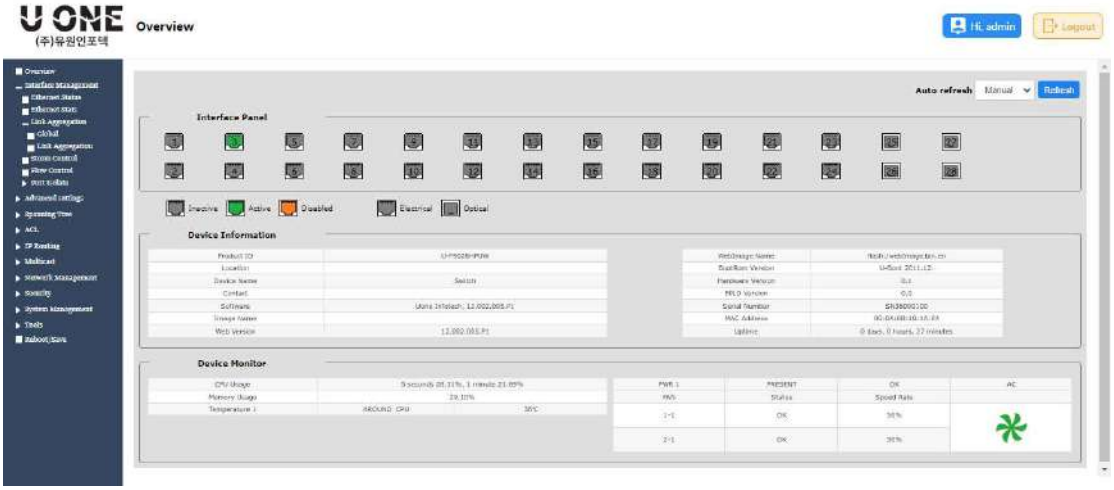
◆**Language** – Default English.



개요

개요

개요 페이지를 사용하면 정보를 표시하여 시스템을 식별할 수 있습니다.



인터페이스 관리

이더넷 상태

Interface Management > Ethernet Status

이 페이지는 포트 정보를 표시하는 페이지입니다.

이더넷 상태

Interface Management > Ethernet Stats

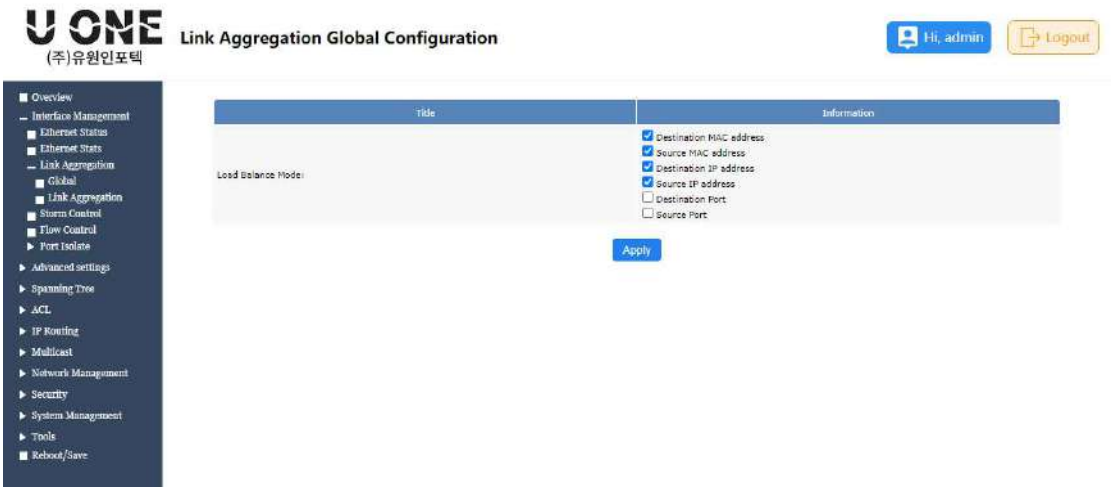
포트의 데이터 통계를 표시하는 페이지입니다.

링크 집계

글로벌

Interface Management > Link Aggregation> Global

이 페이지는 트렁크 그룹의 매개변수를 구성하는데 사용하는 페이지입니다.



◆**Destination MAC Address** – 동일한 대상 MAC 주소를 가진 모든 트래픽은 트렁크의 동일한 링크로 출력됩니다. 이 모드는 다음에 가장 적합합니다. 스위치를 통한 트래픽이 여러 다른 호스트로 향하는 스위치 간 트렁크 링크. 위치-라우터 트렁크 링크에는 이 모드를 사용하지 마십시오. 여기서 대상 MAC 주소는 모든 트래픽에 대해 동일합니다.

◆**Source MAC Address** – 소스 MAC 주소가 동일한 모든 트래픽은 트렁크의 동일한 링크로 출력됩니다. 이 모드는 스위치를 통한 트래픽이 다양한 호스트로부터 수신되는 스위치 간 트렁크 링크에 가장 적합합니다.

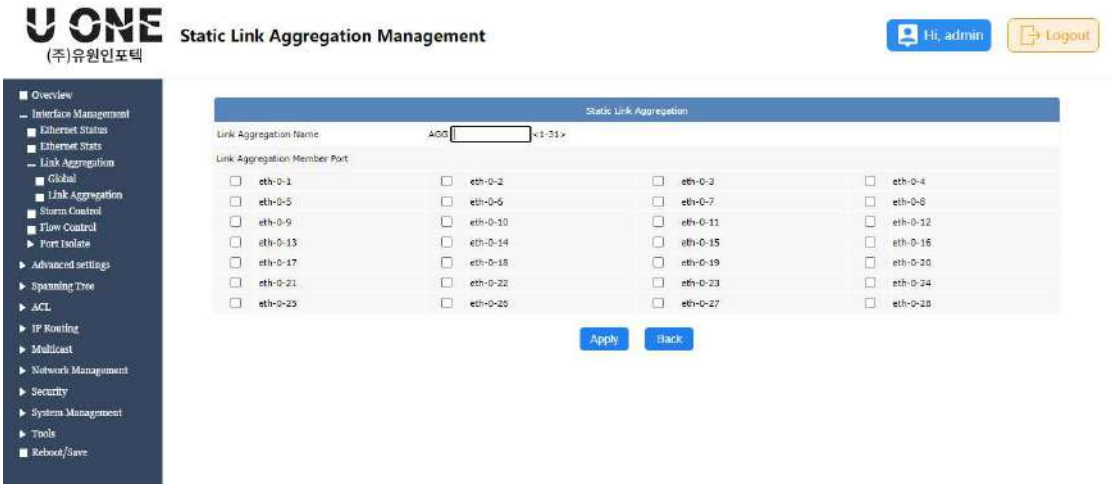
◆**Destination IP Address** – 동일한 대상 IP 주소를 가진 모든 트래픽은 트렁크의 동일한 링크로 출력됩니다. 이 모드는 스위치를 통한 트래픽이 다양한 호스트로 향하는 스위치-라우터 트렁크 링크에 가장 적합합니다. 모든 트래픽에 대해 대상 IP 주소가 동일한 스위치-서버 트렁크 링크에는 이 모드를 사용하지 마십시오.

◆**Source IP Address** – 동일한 소스 IP 주소를 가진 모든 트래픽은 트렁크의 동일한 링크로 출력됩니다. 이 모드는 스위치를 통한 트래픽이 다양한 호스트로부터 수신되는 스위치-라우터 또는 스위치-서버 트렁크 링크에 가장 적합합니다.

링크 집계

Interface Management > Link Aggregation> Link Aggregation

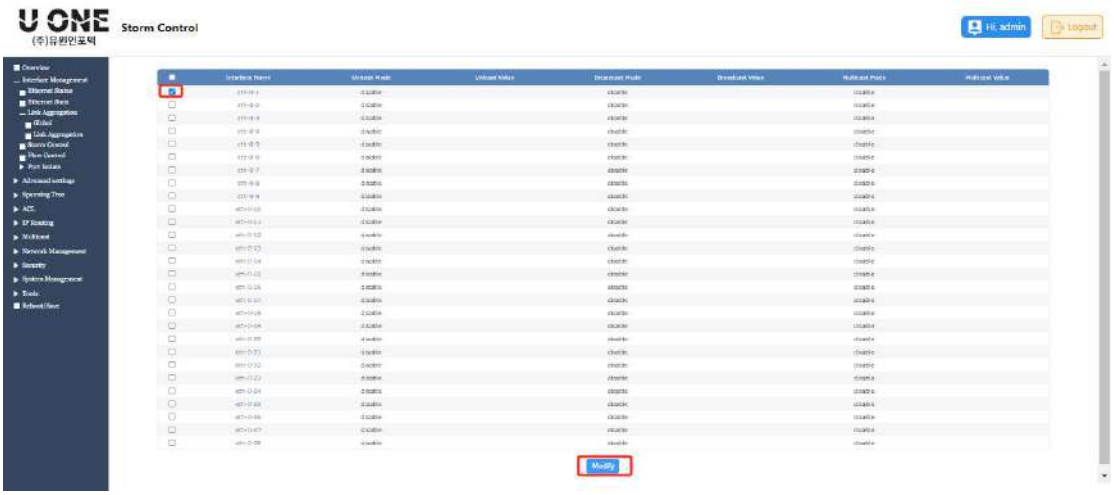
이 페이지는 정적 트렁크 그룹을 생성/삭제하는 페이지이며, 정적 그룹 구성원을 추가/삭제하는데 사용됩니다.



스톰 컨트롤

Interface Management >Storm Control

이 페이지는 브로드캐스트, 멀티캐스트 및 알 수 없는 유니캐스트 스톰 제어 임계값을 구성하는데 사용합니다.



포트를 선택하고 수정 버튼을 클릭하여 단일 또는 다중 포트에 대한 스톰 제어 구성 페이지로 들어갑니다.

◆**Interface Name** – 포트 목록을 표시합니다.

◆**Unicast Mode** – 알 수 없는 유니캐스트 트래픽에 대한 폭풍 제어를 지정합니다.

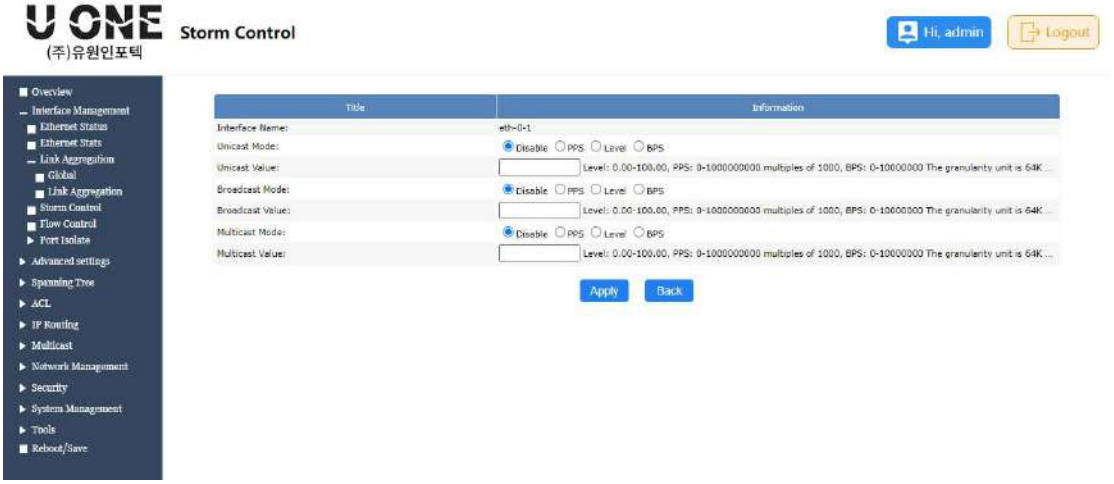
◆**Unicast Value** – 알 수 없는 유니캐스트 트래픽의 값을 구성합니다.

◆**Broadcast Mode** – 브로드캐스트 트래픽에 대한 폭풍 제어를 지정합니다.

◆**Broadcast Value** – 브로드캐스트 트래픽의 값을 구성합니다.

◆**Multicast Mode** – 멀티캐스트 트래픽에 대한 폭풍 제어를 지정합니다.

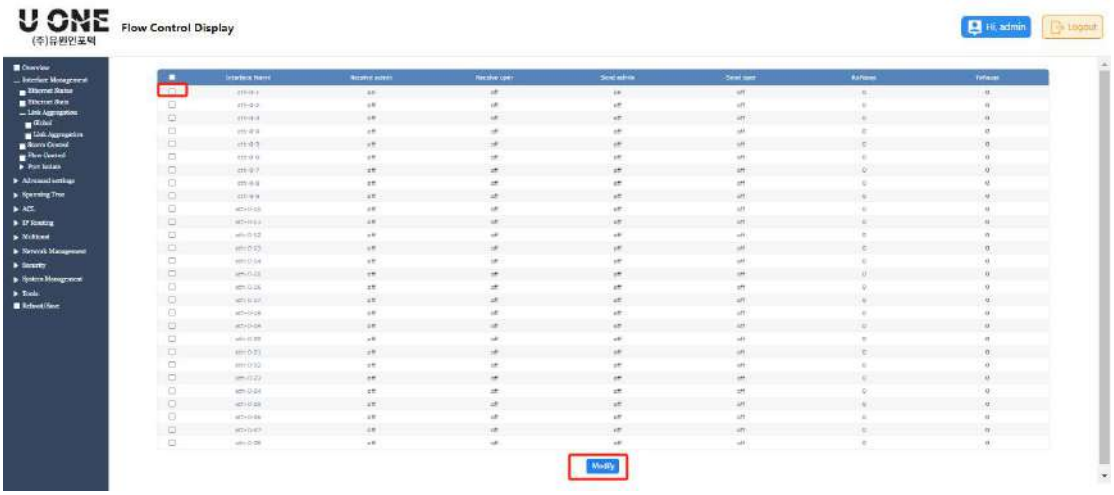
◆**Multicast Valie** – 멀티캐스트 트래픽 값을 구성합니다.



흐름 제어

Interface Management >Flow Control

이 페이지는 흐름 제어의 매개변수를 구성하는데 사용합니다.

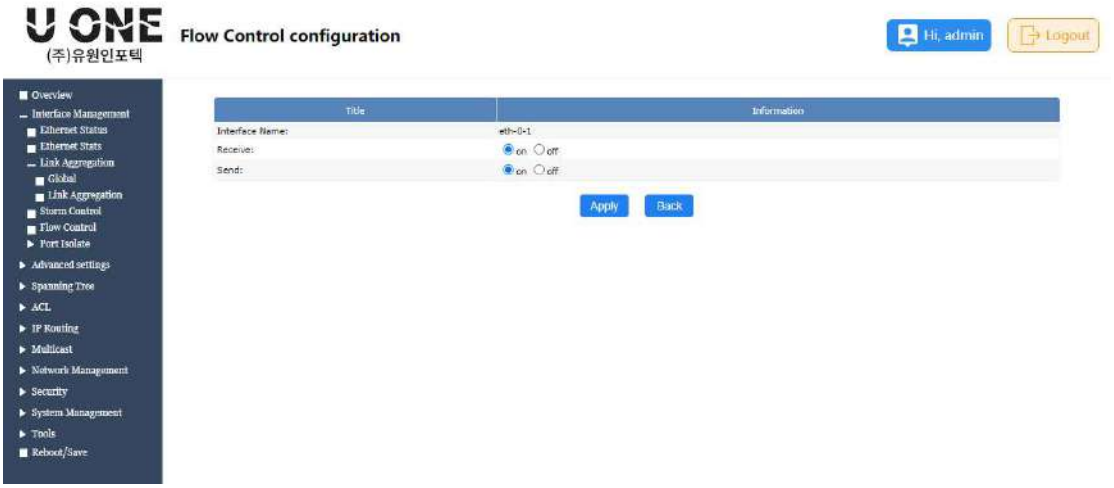


포트를 선택하고 수정 버튼을 클릭하여 단일 또는 다중 포트에 대한 흐름 제어 구성 페이지로 들어갑니다.

◆**Interface Name** – 포트 목록을 표시합니다.

◆**Receive** – 수신을 활성화하거나 비활성화합니다.

◆**Send** – 보내기를 활성화하거나 비활성화합니다.



포트 격리

글로벌

Interface Management > Port Isolate> Global

이 페이지는 포트 격리 모드를 구성하는데 사용됩니다.

◆**Port Isolate Mode** – L2: 레이어2 패킷만 격리합니다.

ALL: 모든 레이어2 패킷과 레이어3 패킷을 격리합니다.

포트 격리

Interface Management > Port Isolate> Port Isolate

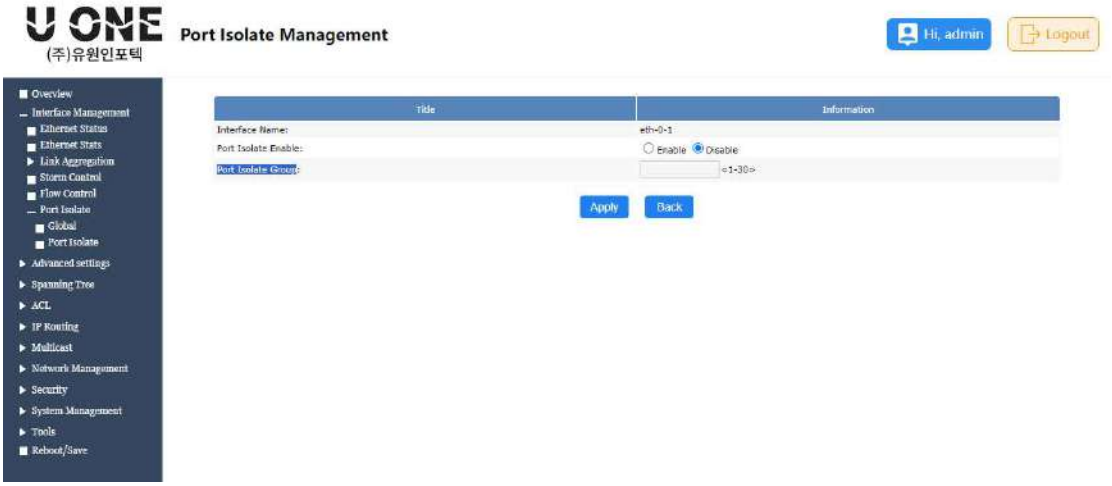
이 페이지는 포트에서 격리를 구성하는데 사용됩니다.

포트를 선택하고 수정 버튼을 클릭하여 단일 또는 다중 포트에 대한 포트 격리 구성 페이지로 들어갑니다.

◆**Interface Name** – 포트 목록을 표시합니다.

◆**Port Isolate Enable** – 포트 격리를 활성화하거나 비활성화합니다.

◆**Port Isolate Group** – 포트의 격리 그룹 번호를 지정하는 데 사용됩니다.



고급 설정

VLAN

VLAN 요약

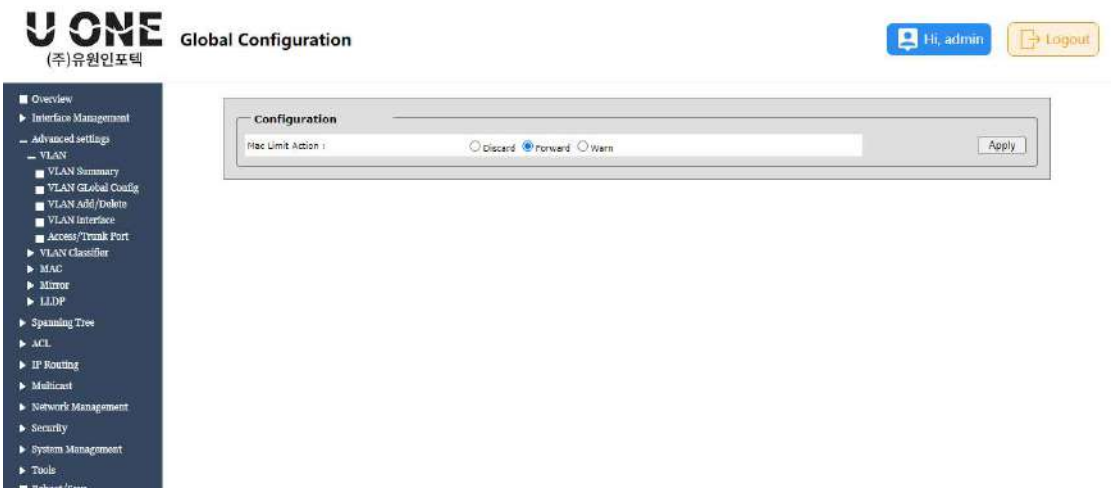
Advanced Settings> VLAN> VLAN Summary

이 페이지는 VLAN ID, 상태, DSCP 교체, MAC 학습, 제한, 맴버 포티 및 인터페이스를 포함하여 모든 VLAN의 관련 속성 정보를 표시하는데 사용됩니다.

VLAN 글로벌 설정

Advanced Settings> VLAN> VLAN Global Config

이 페이지는 VLAN에 대한 MAC 제한 작업을 구성하는데 사용됩니다.



VLAN 추가/삭제

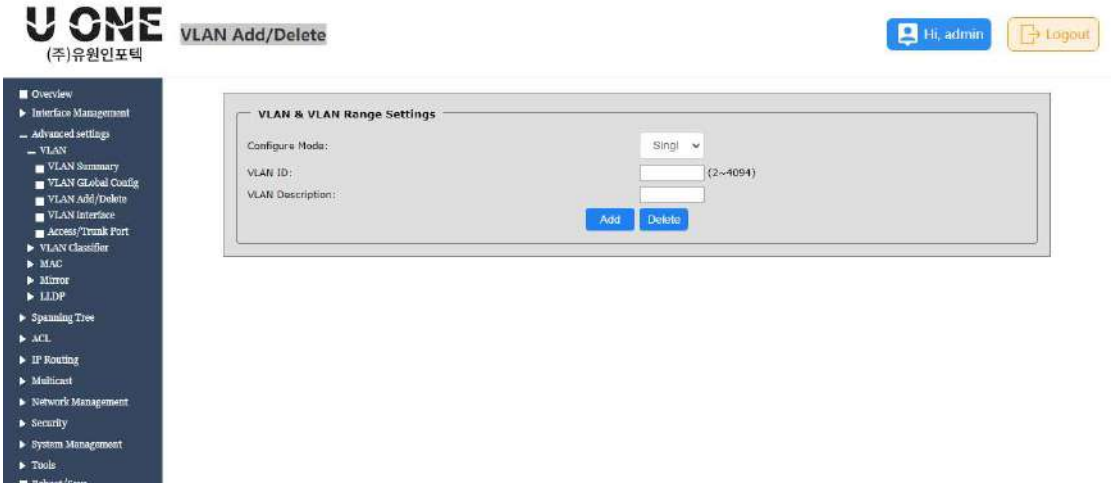
Advanced Settings> VLAN> VLAN Add/Delete

이 페이지는 VLAN을 추가하고 삭제하는데 사용됩니다.

◆**Configure Mode** – 단일 VLAN 또는 범위가 있는 다중 VLAN.

◆**VLAN ID** – VLAN의 ID 또는 VLAN 범위(2-4094)입니다.

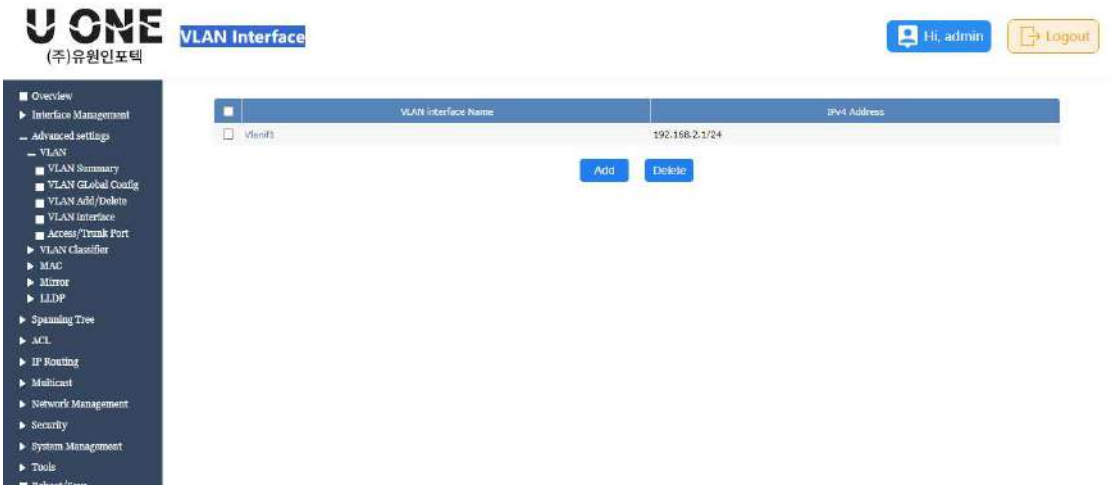
◆**VLAN Description** – VLAN의 이름입니다.



VLAN 인터페이스

Advanced Settings> VLAN> VLAN Interface

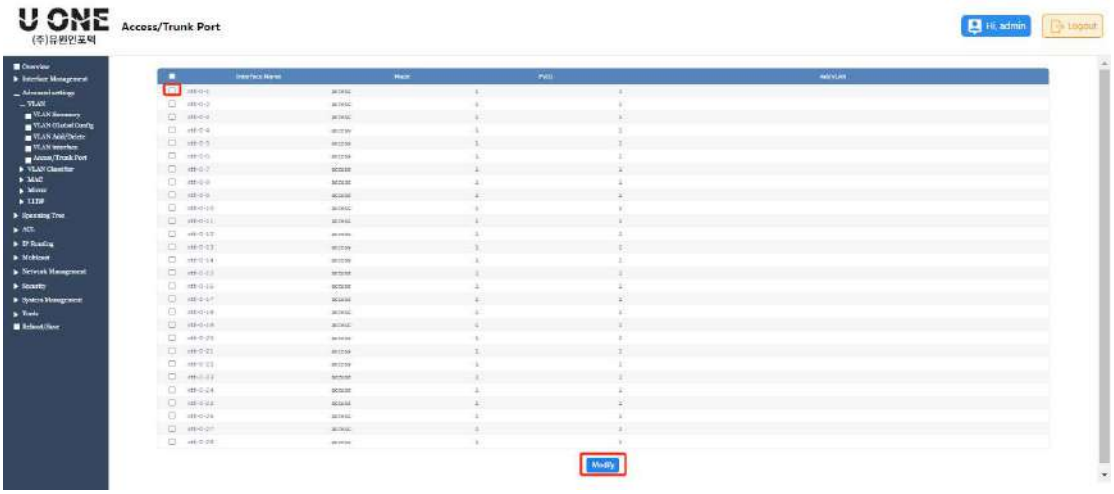
이 페이지는 VLAN의 IP 주소를 구성하는데 사용됩니다.



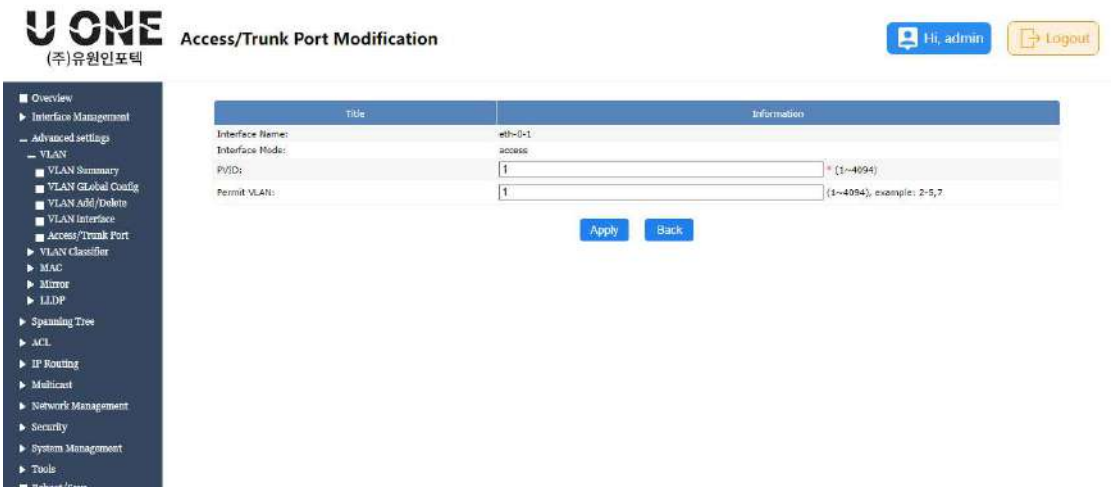
엑세스/트렁크 포트

Advanced Settings> VLAN> Access/Trunk Port

이 페이지는 포트 모드, PVID 및 수신 필터링을 포함하여 VLAN에 포트를 추가하는데 사용됩니다.



포트를 선택하고 수정 버튼을 클릭하여 단일 또는 다중 포트에 대한 액세스/트렁크 포트 수정 페이지로 들어갑니다.



VLAN **분류자**

요약

Advanced Settings> VLAN> VLAN classifier> Summary

이 페이지는 VLAN 분류자 규칙, VLAN 분류자 그룹, VLAN 분류자 사용 등 VLAN 분류자의 관련 속성 정보를 표시하는데 사용되며 페이지에서 추가하거나 삭제할 수 있습니다.

규칙

Advanced Settings> VLAN> VLAN classifier> Rules

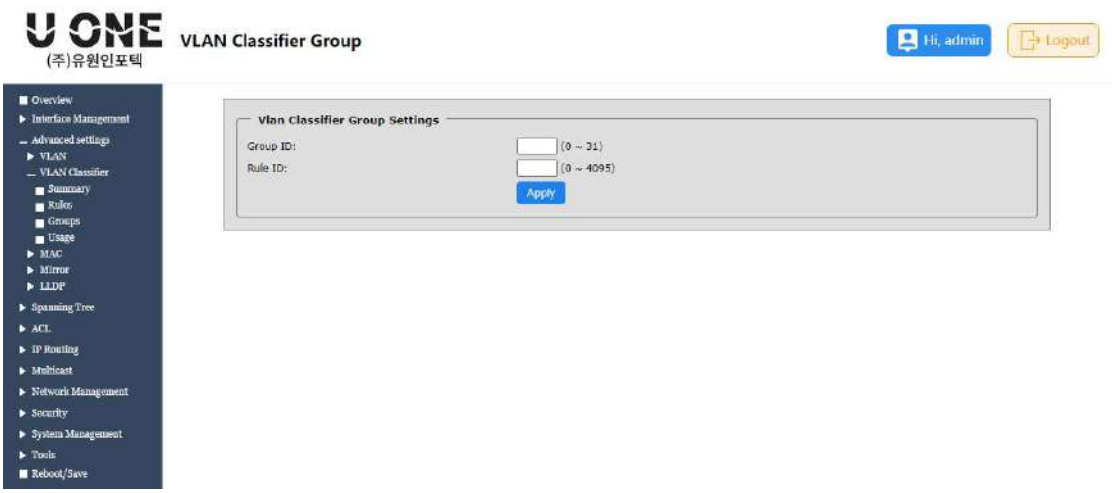
이 페이지는 VLAN 분류자 규칙을 추가하는데 사용됩니다.

◆**Rule Type** – IP 와 MAC과 protocol입니다.

그룹

Advanced Settings> VLAN> VLAN classifier> Groups

이 페이지는 VLAN 분류자 그룹을 추가하는데 사용됩니다.



용법

Advanced Settings> VLAN> VLAN classifier> Usage

이 페이지는 VLAN 분류자 규칙을 포트에 적용하는데 사용됩니다.

◆**Based Type** – IP와 MAC과 protocol 입니다.

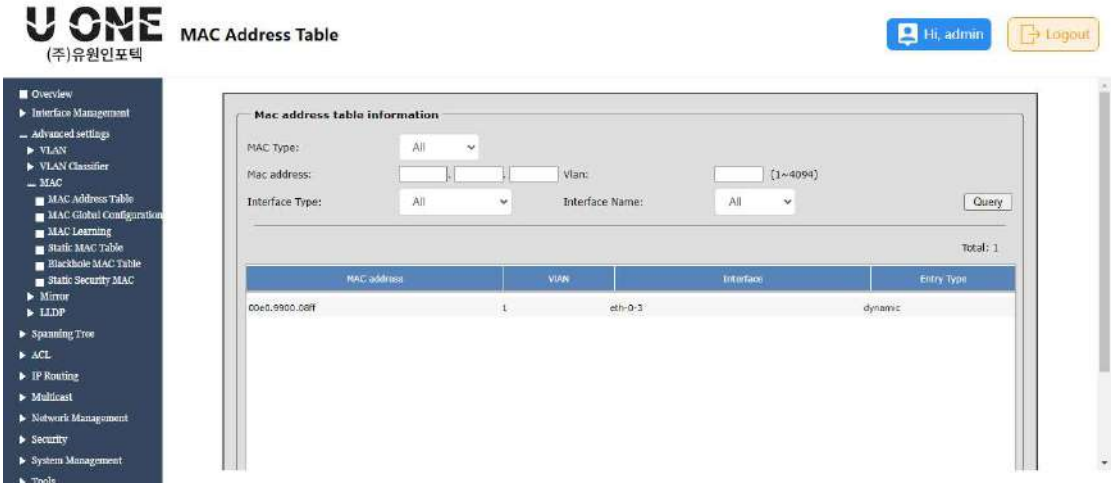
MAC

맥 주소 테이블

Advanced Settings> MAC> MAC Address Table

이 페이지는 동적 주소, 정적 주소 및 VLAN ID를 포함하여 각 포트에서 학습한 MAC

주소를 표시하는데 사용됩니다.



맥 전역 구성

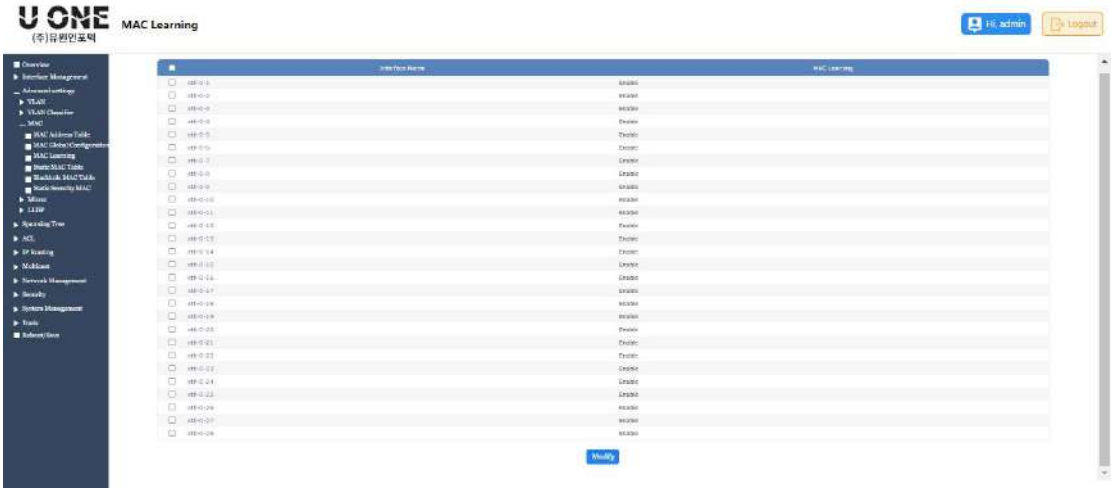
Advanced Settings> MAC> MAC Global Configuration

이 페이지는 MAC 주소 테이블의 에이징 시간을 구성하는데 사용되며 범위는 10-999999초입니다.

맥 학습

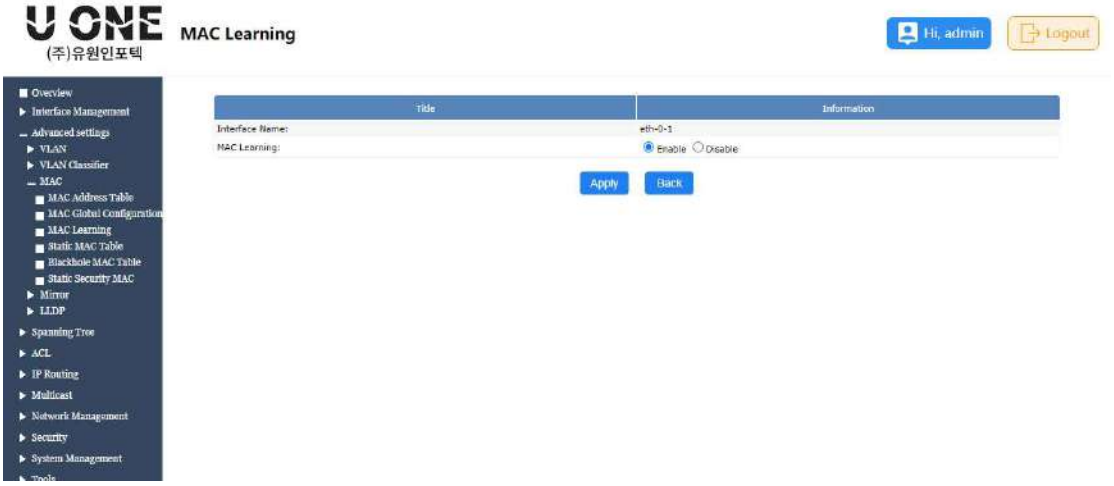
Advanced Settings> MAC> MAC Learning

이 페이지는 포트에서 MAC 학습을 활성화 및 비활성화하는데 사용됩니다.



포트를 선택하고 수정 버튼을 클릭하면 단일 또는 다중 포트에 대한 활성화/비활성화

MAC 학습 페이지로 들어갑니다.



정적 맥 테이블

Advanced Settings> MAC> Static MAC Table page is used to add and delete the static MAC address.

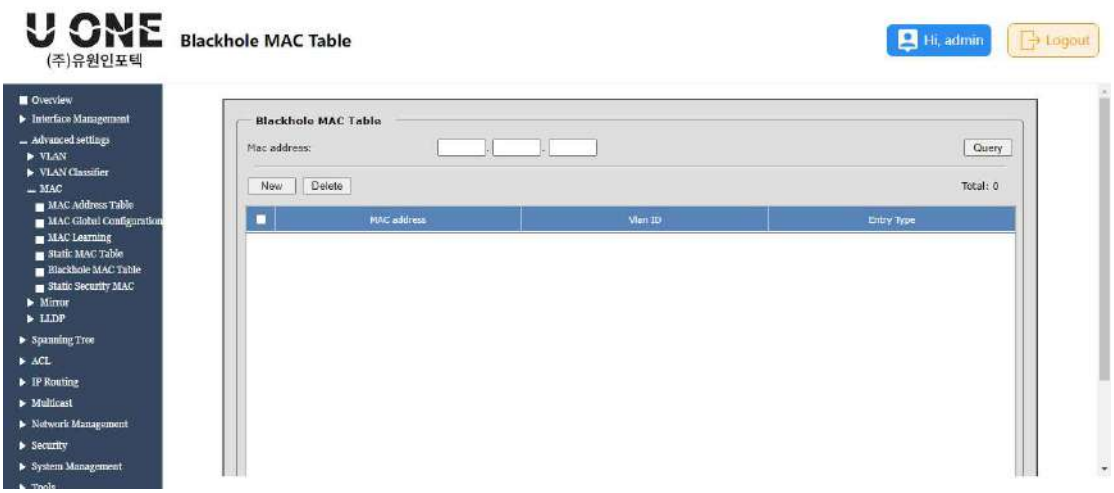
이 페이지는 고정 MAC 주소를 추가하고 삭제하는데 사용됩니다.

새로 만들기 버튼을 클릭하여 단일 포트 및 링크 집계 그룹에 대한 정적 MAC 주소 추가 페이지로 들어갑니다.

블랙홀 맥 테이블

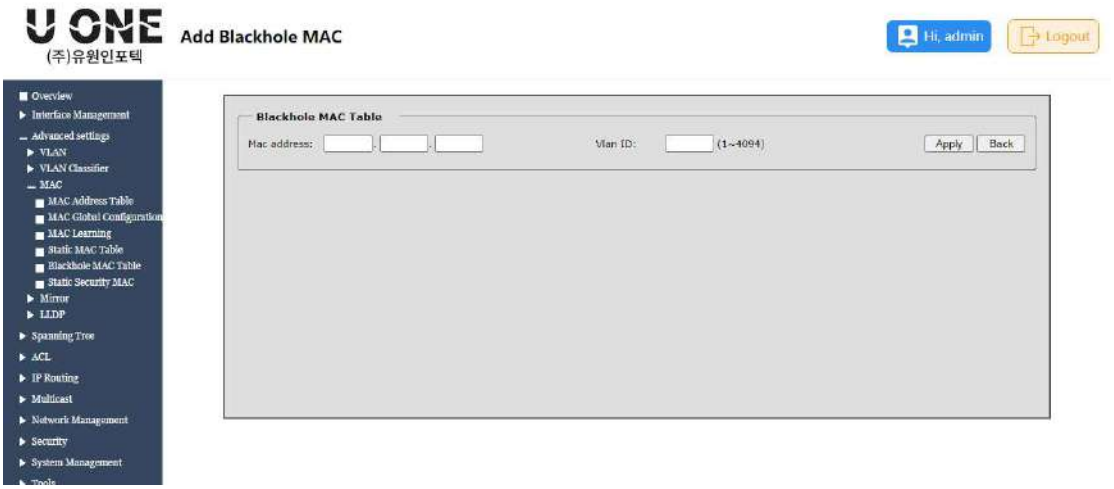
Advanced Settings> MAC> Blackhole MAC Table

이 페이지는 블랙홀 MAC 주소를 추가하고 삭제하는데 사용됩니다.



새로 만들기 버튼을 클릭하여 VLAN에 대한 블랙홀 MAC 주소 추가 페이지로

들어갑니다.

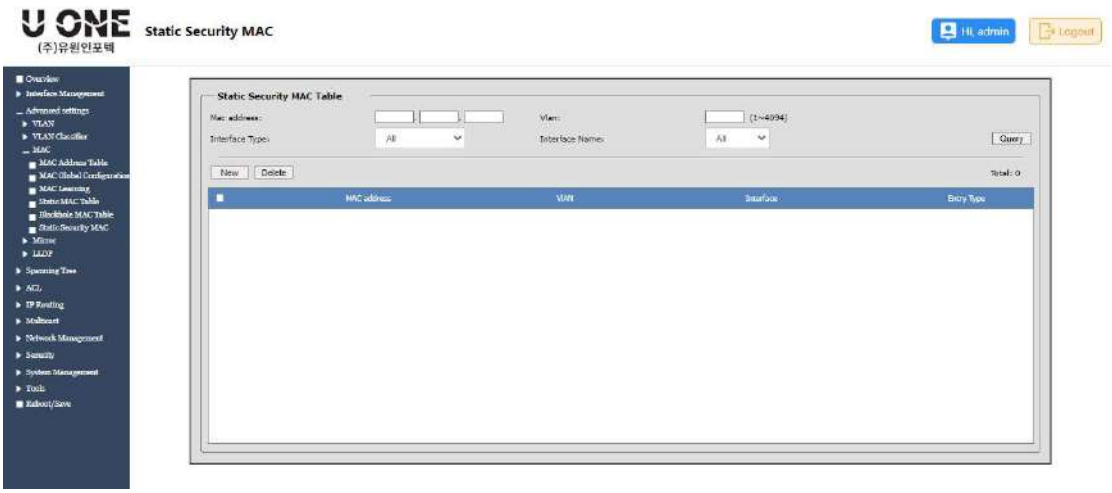


정적 보안 맥

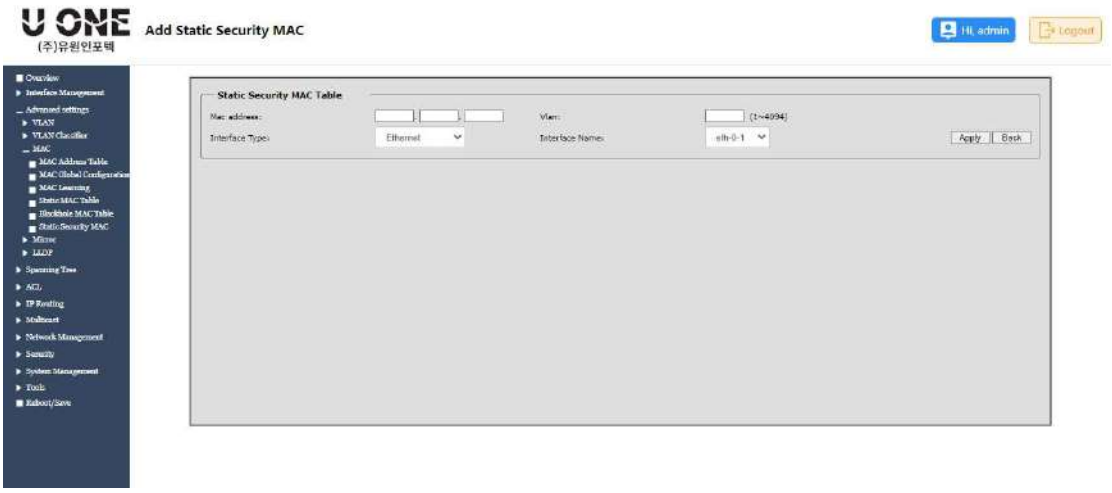
Advanced Settings> MAC> Static Security MAC

페이지는 Static Security MAC 주소를 추가하고 삭제하는 데 사용됩니다.

정적 보안 MAC 주소는 우선순위가 더 높으며 에이징 시간의 영향을 받지 않습니다.



새로 만들기 버튼을 클릭하여 단일 포트에 대한 블랙홀 MAC 주소 추가 페이지로 들어갑니다.

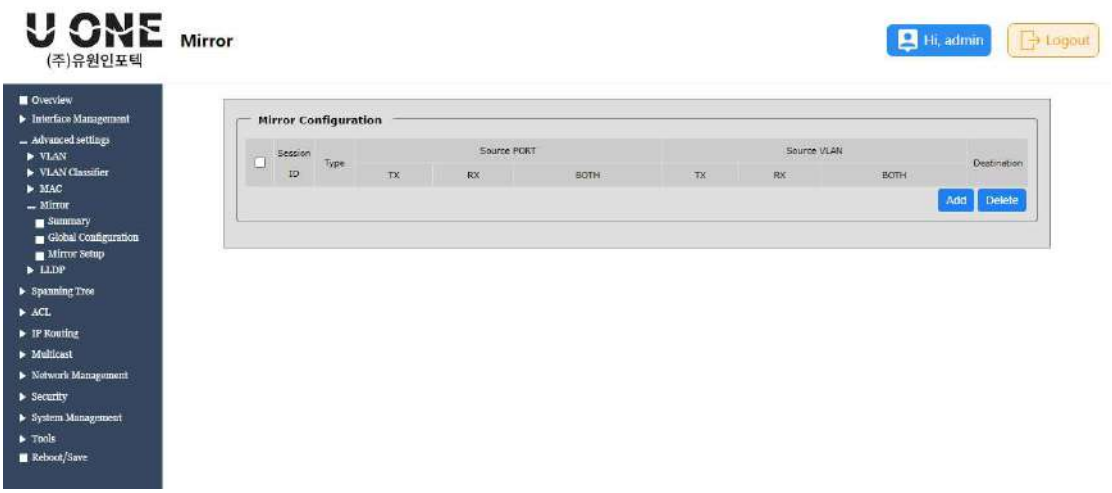


Mirror

요약

Advanced Settings> Mirror> Summary

이 페이지는 미러 항목을 추가하고 삭제하는데 사용됩니다.



추가 버튼을 눌러 미러 세션 설정 추가 페이지로 들어갑니다.

◆**Session ID** – 1~4.

◆**Source Port** – 트래픽을 모니터링할 포트입니다.

◆**Destination Port** – 소스 포트에서 미러링되는 트래픽을 모니터링할 대상 포트를 지정합니다.

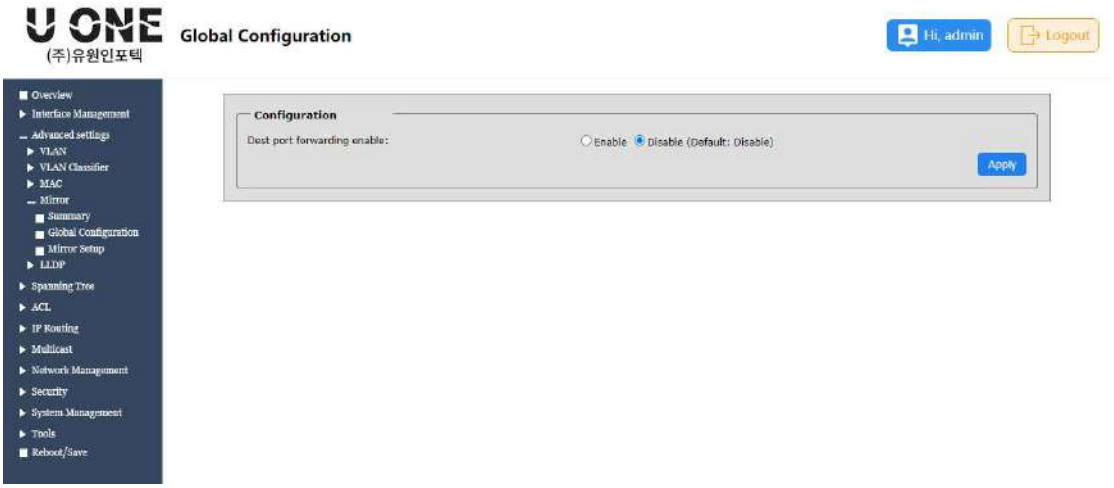
◆**Direction** – 대상 포트, Rx(수신), Tx(전송) 또는 둘 다에 미러링할 트래픽을 선택할 수 있습니다.

◆**Destination Type** – 로컬 및 원격 로컬 포트 미러는 실시간 분석을 위해 모든 소스 포트에서 대상 포트로 트래픽을 미러링하는 데 사용됩니다. RSPAN은 로컬 스위치의 대상 포트에서 분석을 위해 원격 스위치의 트래픽을 미러링하는 데 사용됩니다.

글로벌 설정

Advanced Settings> Mirror> Global Configuration

이 페이지는 미러 기능을 전체적으로 활성화 또는 비활성화하는데 사용됩니다.



미러 설정

Advanced Settings> Mirror> Mirror Setup

이 페이지는 미러 항목을 생성하는데 사용됩니다.

LLDP

글로벌 설정

Advanced Settings> LLDP> Global Configuration

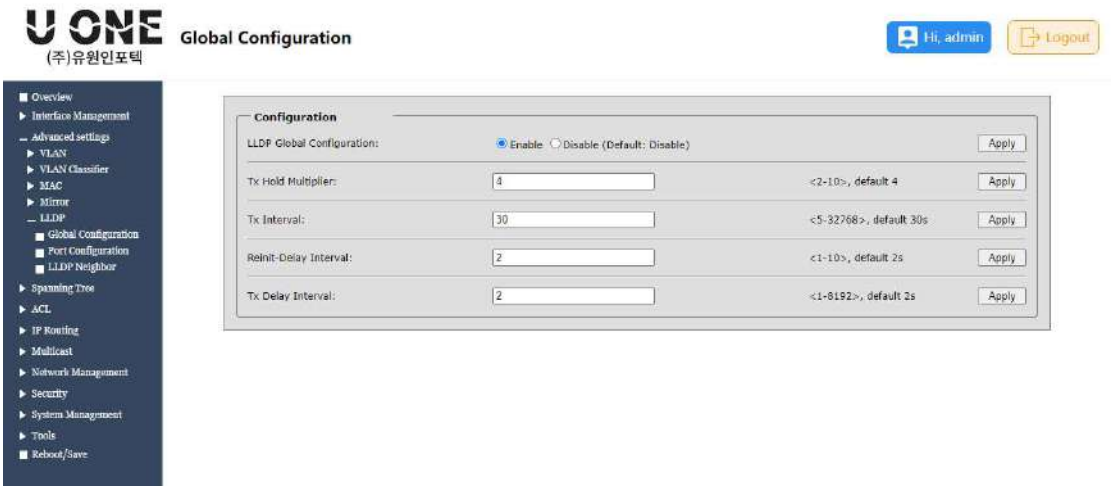
이 페이지는 LLDP 기능을 전역적으로 활성화 또는 비활성화하고 LLDP 매개변수를 구성하는 데 사용됩니다.

◆**Tx Hold Multiplier** – 이 객체는 이웃 장치 정보의 유지 시간 배율을 나타냅니다. 기본값은 4입니다.

◆**Tx Interval** – 이 객체는 LLDP 패킷 전송 간격(초)을 나타냅니다. 기본값은 30초입니다.

◆**Reinit-Delay Interval** – 이 객체는 LLDP 초기화 지연을 초 단위로 나타냅니다. 기본값은 2초입니다.

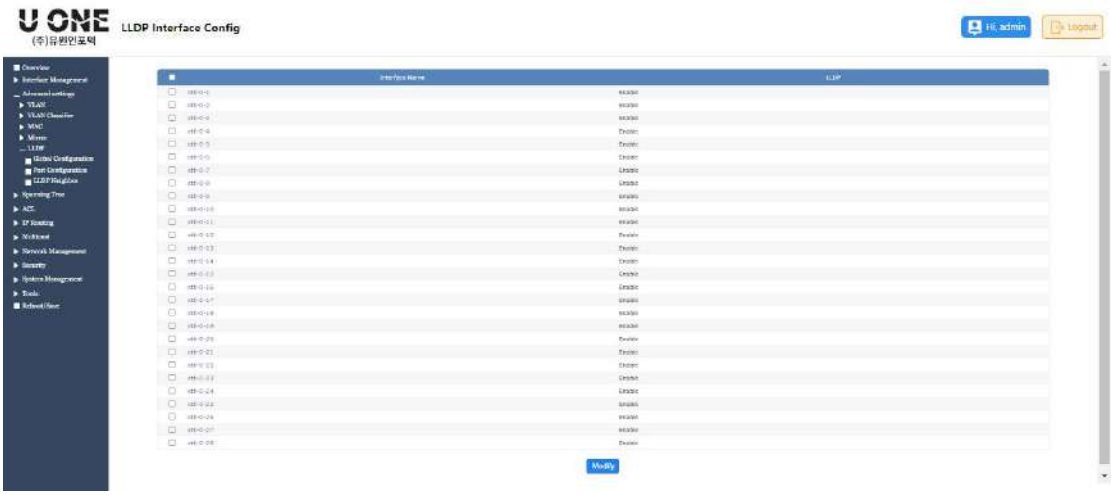
◆**Tx Delay Interval** – 이 객체는 LLDP 패킷 전송 지연을 초 단위로 나타냅니다. 기본값은 2초입니다.



포트 설정

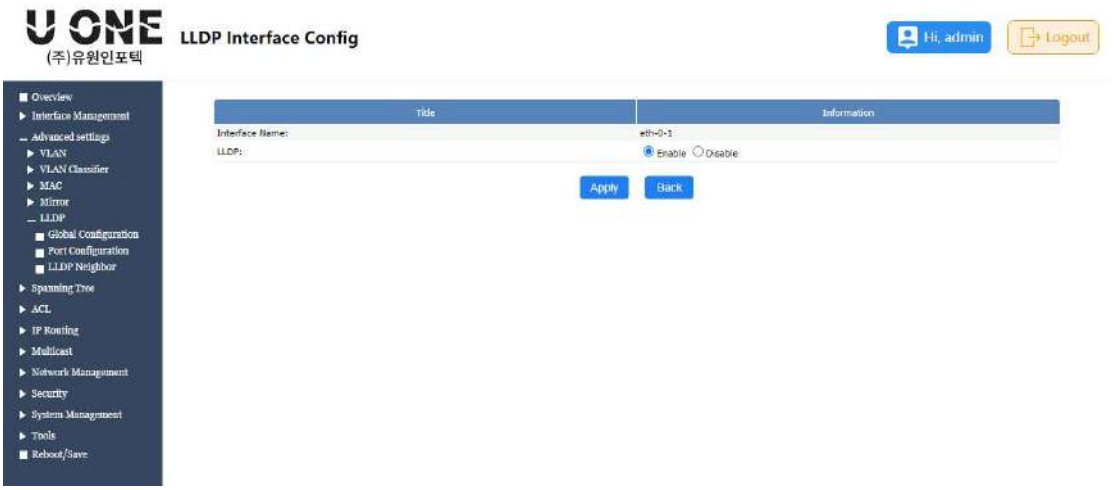
Advanced Settings> LLDP> Port Configuration

이 페이지는 포트의 LLDP 기능을 활성화하거나 빌활성화하는데 사용됩니다.



포트를 선택하고 수정 버튼을 클릭하여 단일 또는 다중 포트에 대한 LLDP

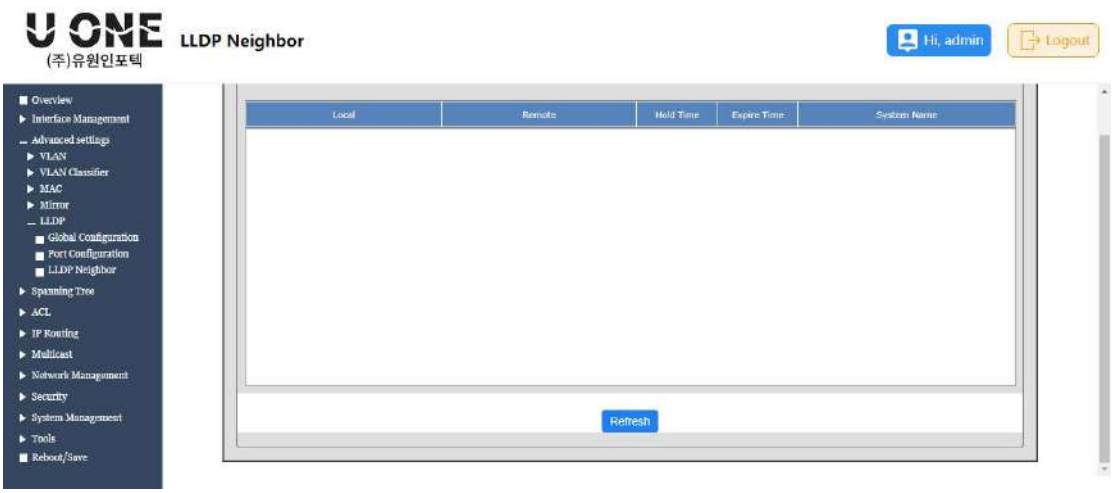
활성화/비활성화 페이지로 들어갑니다.



LLDP 이웃

Advanced Settings> LLDP> LLDP Neighbor

이 페이지는 LLDP 이웃 목록을 표시하는데 사용됩니다.



스패닝 트리

STP 정보

Spanning Tree > STP Information

이 페이지는 스패닝 트리의 매개변수를 표시하는데 사용됩니다.

STP 글로벌

Spanning Tree > STP Global

이 페이지는 STP 기능을 전체적으로 활성화 또는 비활성화하고 스패닝 트리의 매개

변수를 구성하는 데 사용됩니다.

◆**BPDU Guard** – 이 기능은 엣지 포트가 BPDU를 수신하지 못하도록 보호합니다. BPDU를 스패닝 트리 폐기 상태로 전환하는 대신 BPDU가 수신되면 에지 포트를 종료하여 루프를 방지합니다. 유효한 구성에서는 구성된 에지 포트가 BPDU를 수신해서는 안 됩니다. 엣지 포트가 BPDU를 수신하는 경우 승인되지 않은 장치에 대한 연결과 같은 잘못된 구성이 존재합니다. BPDU 보호 기능은 관리자가 수동으로 포트를 활성화해야 하기 때문에 잘못된 구성에 대한 보안 응답을 제공합니다.

◆**BPDU Filter** – BPDU 필터링을 사용하면 끝 노드에 연결된 구성된 에지 포트에서 BPDU 전송을 방지할 수 있습니다. 기본적으로 STA는 관리 Edge가 포트에서 활성화되었는지 여부에 관계없이 모든 포트에 BPDU를 보냅니다. BDPU 필터링은 포트별로 구성됩니다.

◆**Working Mode** – 스패닝 트리 프로토콜 모드: STP(Spanning Tree IEEE 802.1D), RSTP(Rapid Spanning Tree IEEE 802.1w), MSTP(Multiple Spanning Tree IEEE 802.1s)

◆**Pathcost Standard** – 경로 비용은 장치 간 최적의 경로를 결정하는 데 사용됩니다. 경로 비용 방법은 각 인터페이스에 할당할 수 있는 값의 범위를 결정하는 데 사용됩니다.

■Dot1t: 1~200,000,000 범위의 32비트 기반 값을 지정합니다. (이것이 기본값입니다.)

■Dot1d-1998: 1~65535 범위의 16비트 기반 값을 지정합니다.

◆**Max Age** – 장치가 재수렴을 시도하기 전에 구성 메시지를 수신하지 않고 기다릴 수 있는 최대 시간(초)입니다. 모든 장치 포트(지정된 포트 제외)는 정기적으로 구성 메시지를 수신해야 합니다. STA 정보(마지막 구성 메시지에 제공됨)가 만료된 모든 포트는 연결된 LAN에 대해 지정된 포트가 됩니다. 루트 포트인 경우 네트워크에 연결된 장치 포트 중에서 새로운 루트 포트가 선택됩니다. (이 섹션에서 "포트"는 "인터페이스"를

의미하며, 여기에는 포트와 그룹이 모두 포함됩니다.)

◆**Max Hops** – MST 영역의 최대 홉 수입니다.

◆**Hello Time** – 루트 장치가 구성 메시지를 전송하는 간격(초)입니다.

◆**Forward Time** – 인터페이스 상태 전환 시간입니다.

◆**Instance** – 스패닝 트리 인스턴스의 수를 지정합니다.

◆**Priority** – 스패닝 트리에서 스위칭 장치의 우선순위를 지정합니다. 값이 작을수록 스위치 우선순위가 높아집니다.

STP Interface

Spanning Tree > STP Interface

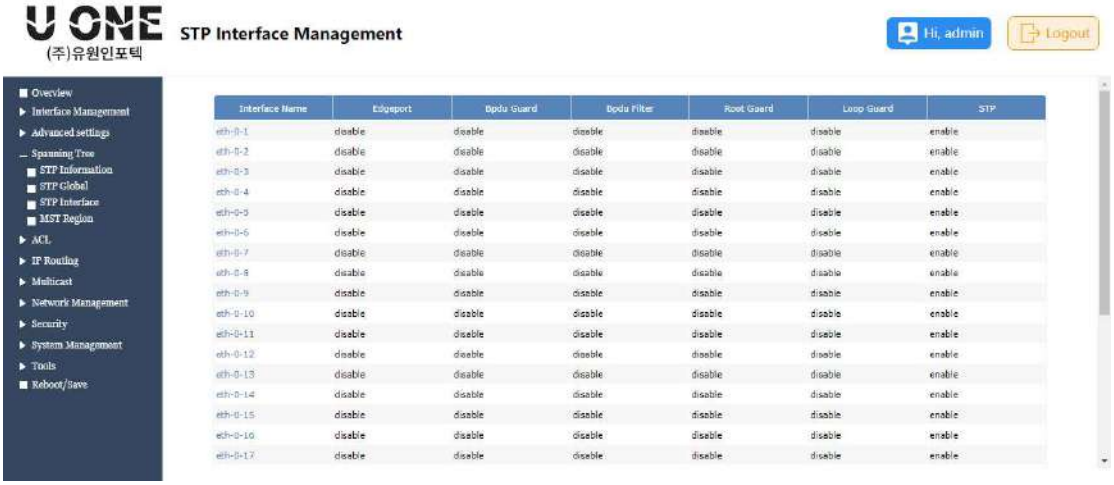
이 페이지는 스패닝 트리에 있는 포트나 그룹의 현재 상태를 표시하는 데 사용됩니다.

◆**Edge Port** – 끝 노드는 전달 루프를 일으킬 수 없으므로 스패닝 트리 전달 상태를 직접 통과할 수 있습니다. 에지 포트를 지정하면 워크스테이션이나 서버와 같은 장치에 대한 더 빠른 수렴을 제공하고 현재 전달 데이터베이스를 유지하여 재구성 이벤트 중 주소 테이블을 다시 작성하는 데 필요한 프레임 플러딩 양을 줄이고 인터페이스 상태가

변경될 때 스패닝 트리가 재구성을 시작하지 않습니다. 또한 다른 STA 관련 시간 초과 문제도 극복합니다. 하지만 엣지 포트는 엔드노드 장치에 연결된 포트에 대해서만 활성화되어야 한다는 점을 기억하세요.

◆**Root Guard** – STA는 더 낮은 브리지 식별자(또는 동일한 식별자와 더 낮은 MAC 주소)를 가진 브리지가 언제든지 루트 브리지 역할을 맡을 수 있도록 허용합니다. Root Guard는 루트 브리지가 최적이 아닌 위치에 형성되지 않도록 보장하는 데 사용될 수 있습니다. 루트 포트를 대신하고 새로운 스패닝 트리 토폴로지를 형성함으로써 느린 링크에 잠재적으로 과부하가 걸릴 수 있는 저속 브리지에 연결된 모든 지정된 포트에서 루트 가드를 활성화해야 합니다. 또한 루트 브리지가 허용되는 네트워크 부분 주위에 경계를 형성하는 데 사용될 수도 있습니다.

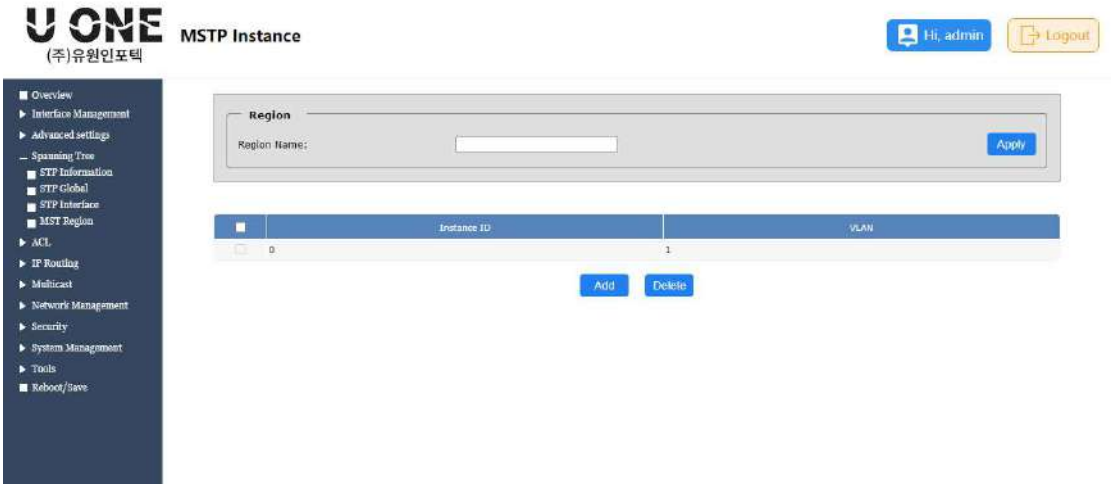
◆**Loop Guard** – 지정되지 않은 포트에서 루프 가드 기능이 활성화되고 max_age 시간 내에 BPDU 메시지가 수신되지 않으면 포트는 일련의 상태 전환을 수신, 학습 및 전달하는 대신 루프 불일치 차단 상태로 들어갑니다. 포트가 루프 불일치 상태에 들어가면 비즈니스 데이터를 전달할 수 없습니다.



MSTP 영역

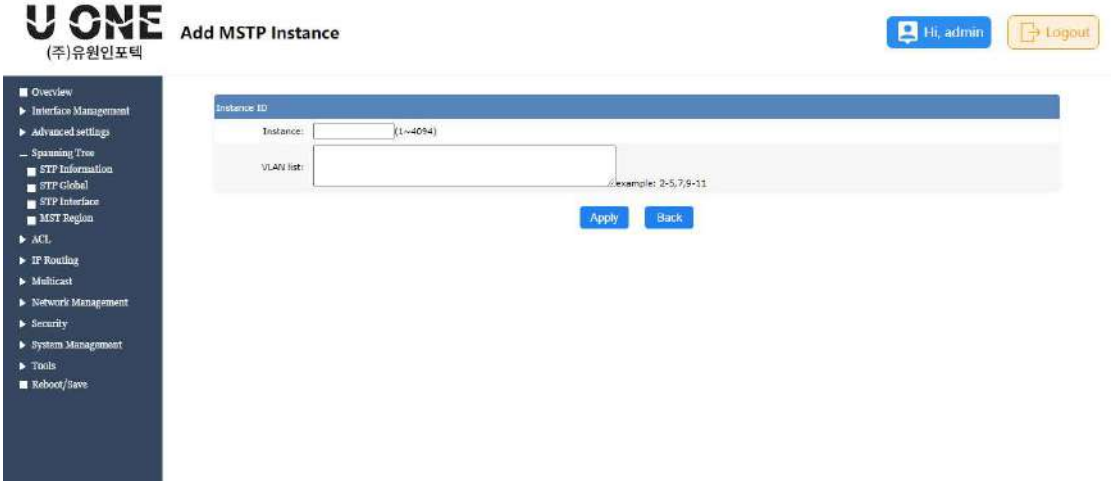
Spanning Tree > MSTP Region

이 페이지는 MSTP 인스턴스를 추가하고 삭제하는 페이지입니다.



추가 버튼을 클릭하여 MSTP 인스턴스 생성 페이지로 들어갑니다.

◆**VLAN list** – 이 MST 인스턴스에 할당할 VLAN입니다.



ACL

Access Control List

ACL > Access Control List

이 페이지는 ACL을 생성 및 삭제하고 ACL 규칙을 추가/삭제하는데 사용됩니다.

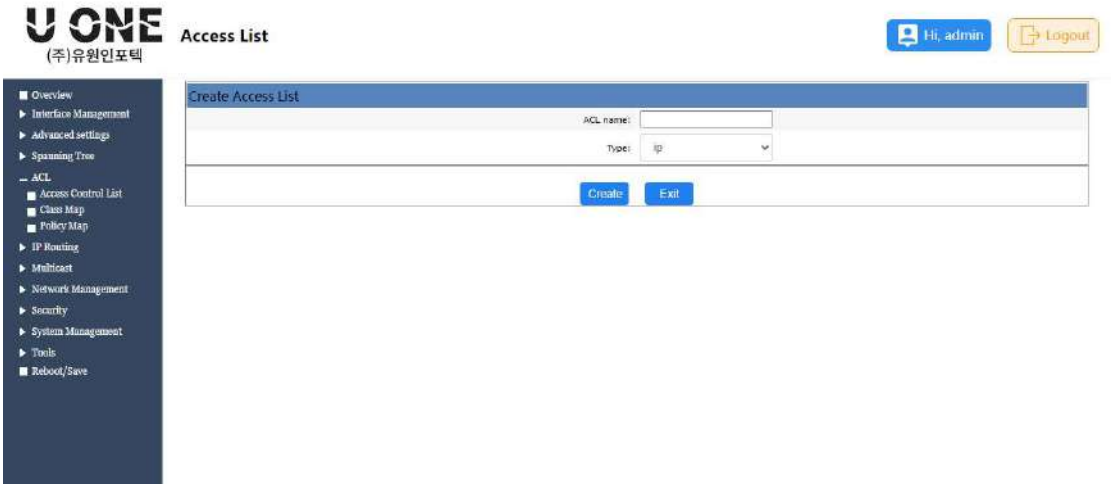
생성 버튼을 클릭하여 ACL 구성 페이지로 들어갑니다.

◆**ACL name** – ACL의 이름입니다.

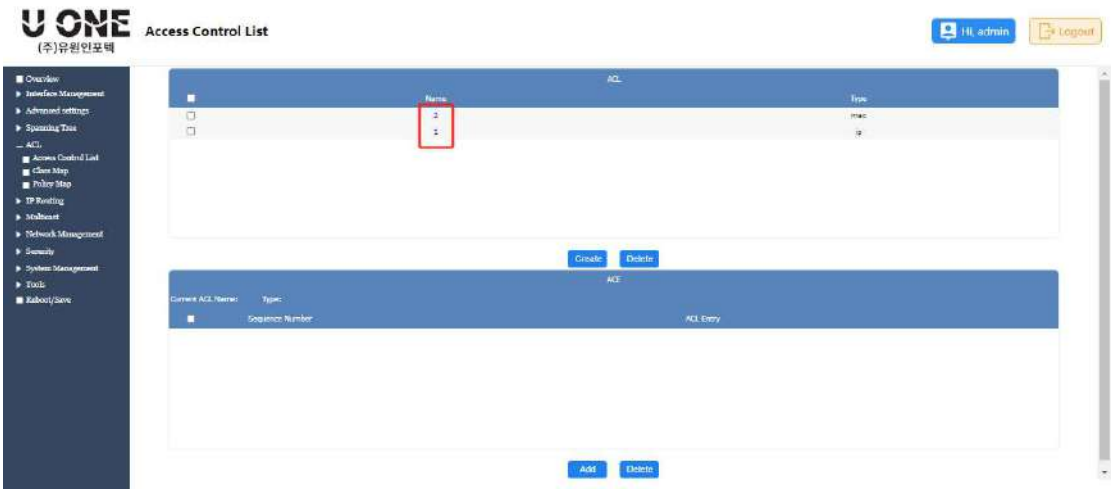
◆**Type** – 다음 필터 모드가 지원됩니다.

■**IP:** IPv4 ACL 모드는 소스 IPv4 주소를 기반으로 패킷을 필터링합니다.

■**MAC:** MAC ACL 모드는 소스 또는 대상 MAC 주소와 이더넷 프레임 유형을 기반으로 패킷을 필터링합니다.



ACL 이름을 생성한 후 생성된 ACL을 클릭한 후 추가 버튼을 클릭하여 ACL 규칙 구성 페이지로 들어갑니다.



ACL IP 규칙 구성 페이지.

◆**Sequence Number** – ACL 규칙의 시퀀스 번호입니다.

◆**Action** – ACL에는 허용 또는 거부 규칙의 조합이 포함될 수 있습니다.

◆**IP Protocol** – 일치시킬 프로토콜 유형을 TCP, UDP, ICMP, IGMP, 사용자 정의 또는 ANY로 지정합니다.

◆**Source IP Address** – 일치시킬 소스 IP 주소를 지정합니다.

◆**Source IP Address Wildcard Mask** – 일치시킬 소스 IP 주소 와일드카드 마스크를

지정합니다.

◆**Dest IP Address** – 일치시킬 대상 IP 주소를 지정합니다.

◆**Source IP Address Wildcard Mask** – 일치시킬 대상 IP 주소 와일드카드 마스크를 지정합니다.

◆**DSCP** – 차별화 서비스 코드 포인트 우선순위 레벨, 값이 높을수록 우선순위가 높아집니다.(범위: 0-63)

DSCP를 기반으로 ACL 규칙을 설정한 후 특정 유형의 트래픽에 대해 더 높은 대역폭 또는 더 낮은 대기 시간을 제공하는 등 다양한 DSCP 태그가 있는 패킷에 다양한 전달 정책을 적용할 수 있습니다. 이는 네트워크 리소스를 보다 효율적이고 유연하게 관리하는 데 도움이 됩니다.

◆**Routed** – 이 규칙은 라우터가 전달한 패킷에 적용되며, 처리되어 다른 네트워크로 전달할 준비가 된 패킷에만 영향을 미칩니다.

◆**Option** – IP 옵션과 패킷을 일치시킵니다.

ACL MAC 규칙 구성 페이지.

◆**Sequence Number** – ACL 규칙의 시퀀스 번호입니다.

◆**Action** – ACL에는 허용 또는 거부 규칙의 조합이 포함될 수 있습니다.

◆**Source MAC Address** – 일치시킬 소스 MAC 주소를 지정합니다.

◆**Source MAC Address Wildcard Mask** – 일치시킬 소스 MAC 주소 와일드카드 마스크를 지정합니다.

◆**Dest MAC Address** – 일치시킬 대상 MAC 주소를 지정합니다.

◆**Source MAC Address Wildcard Mask** – 일치시킬 대상 MAC 주소 와일드카드 마스크를 지정합니다.

◆**VLAN** – VLAN 필드는 MAC 주소 액세스 제어 목록 규칙이 적용되는 특정 VLAN을 지정하는 데 사용됩니다. 즉, 지정된 VLAN의 트래픽만 이 규칙의 영향을 받습니다.

◆**Untag Vlan** – 활성화 또는 비활성화합니다.

■**Enable:** 규칙은 태그가 지정되지 않은 VLAN 트래픽에 적용됩니다. 패킷에 VLAN 태그가 없더라도 다른 조건(예: 소스 MAC 주소, 대상 MAC 주소 등)을 충족하면 이 규칙의 영향을 받습니다.

■**Disable:** 규칙은 특정 VLAN 태그가 있는 패킷에만 적용됩니다. 태그가 지정되지 않은 VLAN 트래픽은 이 규칙의 영향을 받지 않습니다.

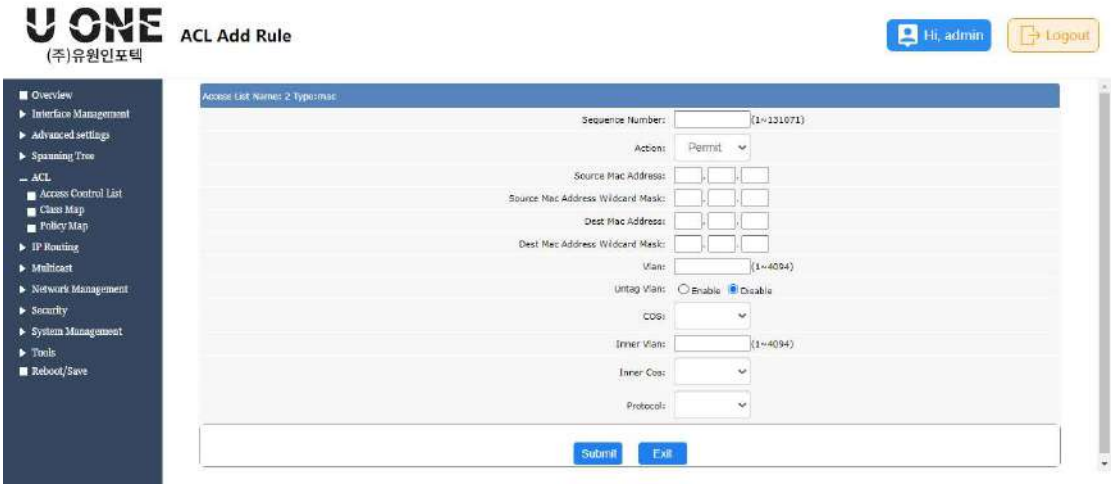
◆**COS** – 패킷의 우선순위를 설정하는 데 사용되는 서비스 클래스입니다. COS 값을 지정하면 다양한 유형의 트래픽을 분류하고 우선순위를 지정할 수 있습니다. 값이 높을수록 우선순위가 높아집니다.

◆**Inner Vlan** – "Inner Vlan"은 일반적으로 이중 태그 VLAN(Q-in-Q 또는 802.1Q-in-802.1Q) 구성의 내부 VLAN 태그를 나타냅니다. 이 설정을 사용하면 기존 태그 위에 추가 VLAN 태그를 추가할 수 있습니다.

◆**Inner Cos** – "Inner CoS"는 일반적으로 내부 VLAN 태그의 서비스 클래스 필드를

나타냅니다. 패킷 우선순위를 지정하는 데 사용되는 802.1Q VLAN 태그의 3비트 필드입니다.

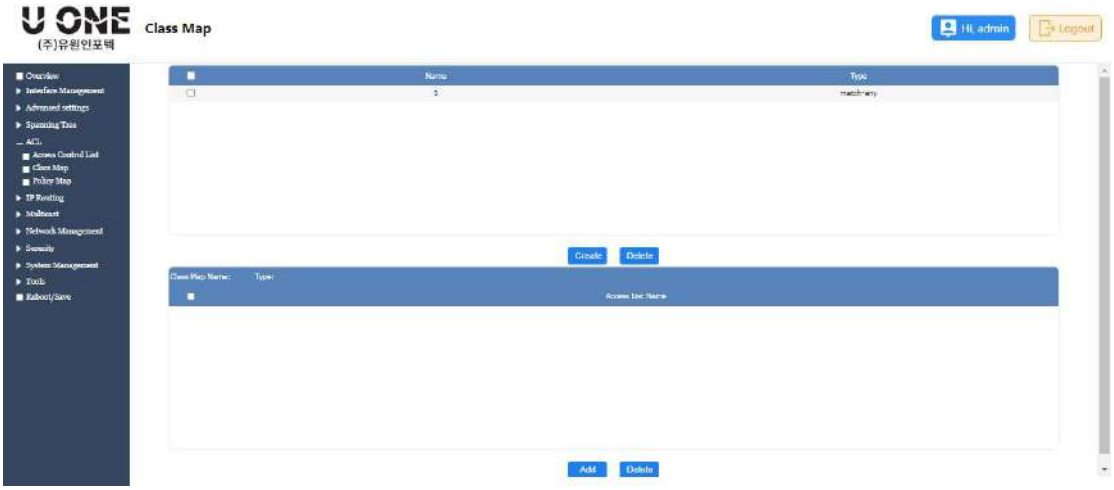
◆**Protocol** – "protocol" 필드는 일치하는 패킷에 대한 프로토콜 유형(ARP/RARP)을 지정합니다. 이 필드를 사용하면 특정 네트워크 계층 프로토콜을 기반으로 트래픽을 필터링할 수 있습니다.



클래스 맵

ACL > Class Map

이 페이지는 클래스 맵을 생성 및 삭제하고 ACL을 일치시키는 데 사용됩니다.



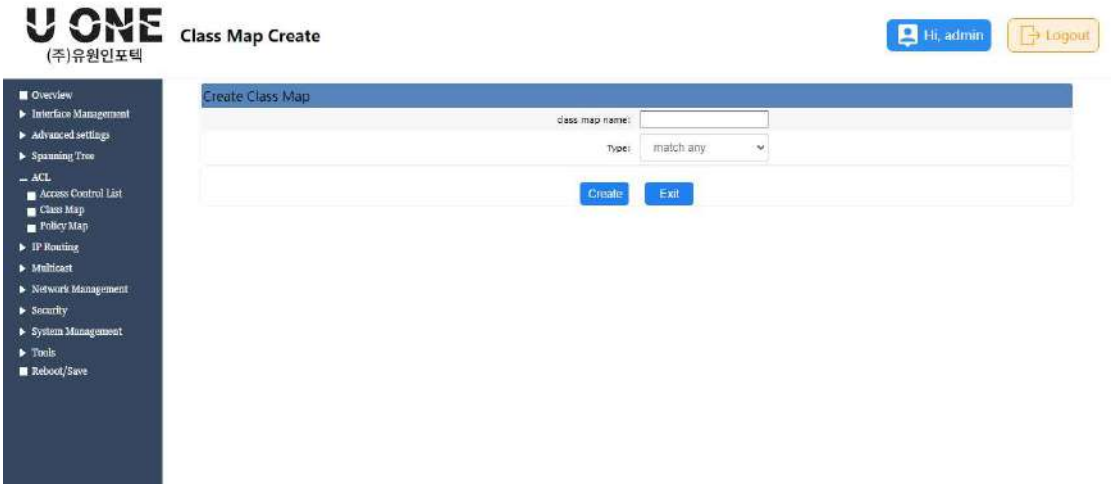
생성 버튼을 클릭하여 클래스 맵 구성 페이지로 들어갑니다.

◆**Class map name** – 클래스 맵의 이름입니다.

◆**Type** – match any 또는 match all 입니다.

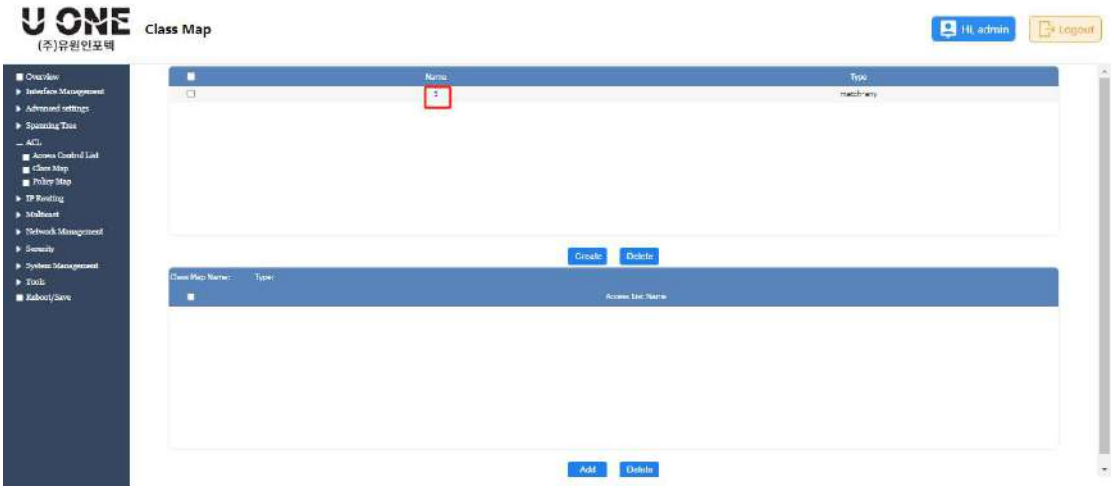
■**Match any:** 이는 조건 중 하나라도 충족되면 경기가 성공한다는 의미입니다.

■**Match all:** 이는 매치가 성공하려면 모든 조건이 동시에 충족되어야 함을 의미합니다.



클래스 맵 이름을 생성한 후 생성된 클래스 맵 이름을 클릭한 후 추가 버튼을 클릭하면

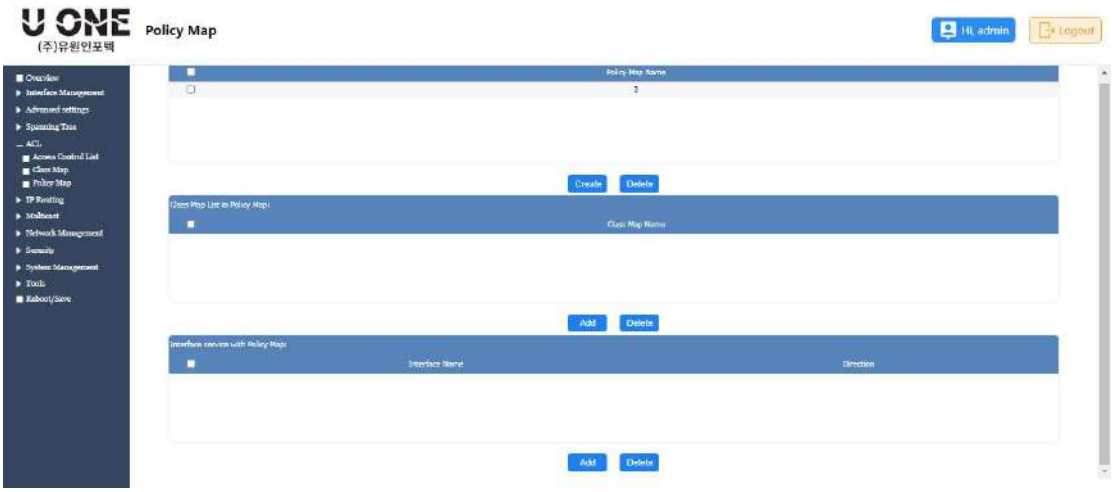
Class Map Match ACL 구성 페이지로 진입합니다.



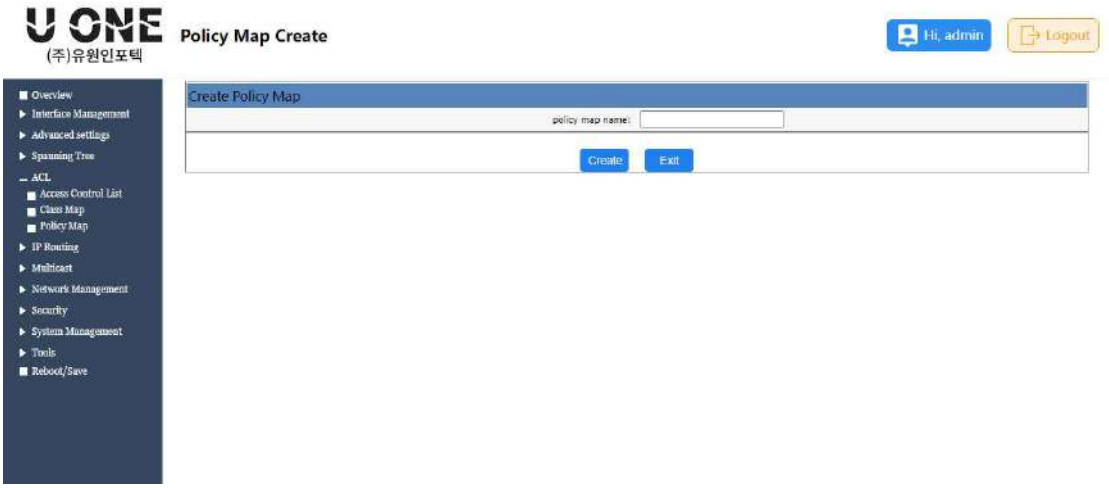
정책 맵

ACL > Policy Map

이 페이지는 정책 맵을 생성 및 삭제하고, 정책 맵을 적용하는 데 사용됩니다.



생성 버튼을 클릭하면 정책 맵 생성 구성 페이지로 들어갑니다.



정책 맵 이름을 생성한 후 생성된 정책 맵 이름을 클릭한 후 추가 버튼을 클릭하면 정책 맵 일치 클래스 맵 구성 페이지로 들어갑니다.

정책 맵이 특정 클래스 맵과 일치하도록 설정되면 클래스 맵에서 정의한 기준을 충족하는 모든 트래픽에 정책 맵이 적용된다는 의미입니다. 즉, 클래스 맵은 트래픽 유형을 식별하고 정책 맵은 해당 트래픽에 대한 특정 QoS 정책을 설정합니다.

◆**Class map name** – 클래스 기본 또는 기타 클래스 맵 이름입니다.

■**Class-default:** Class-default는 다른 클래스 맵에서 명시적으로 정의되지 않은 모든 트래픽을 일치시키는 기본 클래스 맵입니다. 다른 클래스 맵이 정의되지 않은 경우 모든 트래픽은 이 기본 범주에 속합니다.

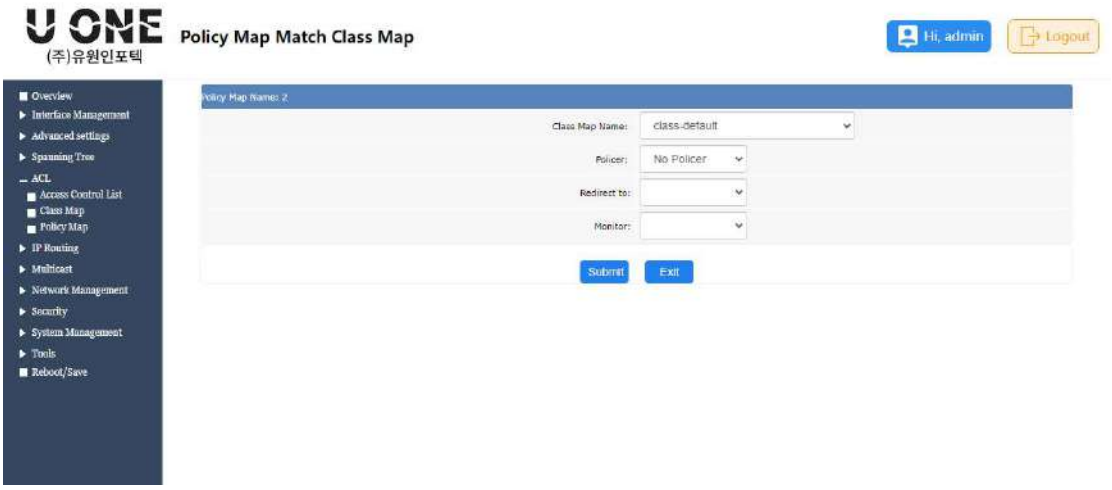
◆**Policer** – Policer가 아니거나 Policer입니다.

■**Policer:** Policer는 특정 트래픽의 속도를 제한하거나 제어하는 데 사용됩니다. 설정된 속도에 따라 데이터 흐름을 제한하고, 제한을 초과하는 패킷은 삭제, 표시 등으로 처리합니다.

◆**Redirect to** – "Redirect to"을 사용하면 특정 트래픽 범주를 지정된 인터페이스로 리디렉션할 수 있습니다.

◆**Monitor** – 세션1, 세션2 및 세션3. "Monitor"이 특정 세션(예: "세션1", "세션2" 또는

"세션3")과 함께 사용되는 경우 사전 정의된 모니터링 정책에 트래픽 범주를 할당한다는 의미입니다.



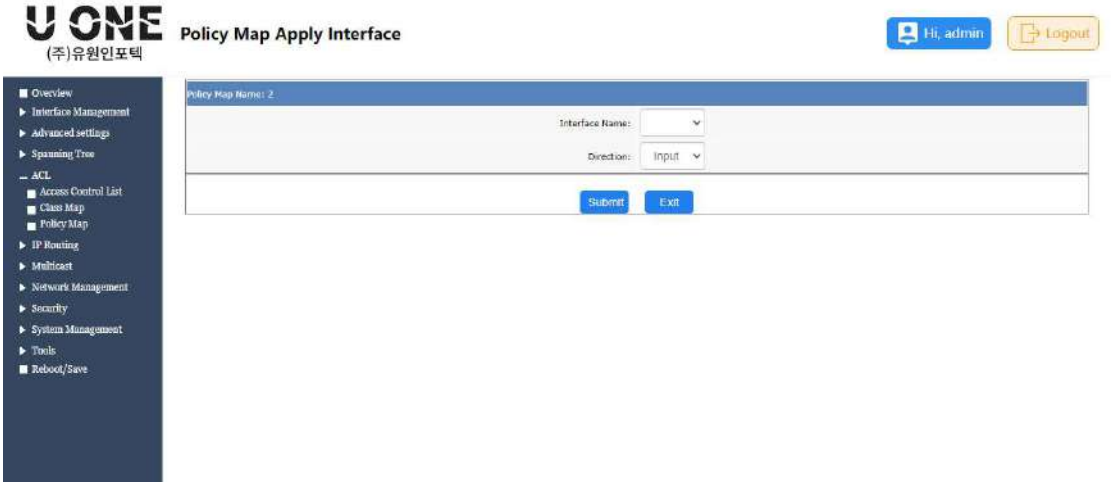
정책 맵 이름을 생성한 후 생성된 정책 맵 이름을 클릭한 후 페이지 하단의 추가 버튼을 클릭하면 정책 맵 일치 클래스 맵 구성 페이지로 진입합니다.

◆**Interface Name** – 특정 인터페이스에 정책 맵을 할당합니다.

◆**Direction** – Input 또는 Output입니다.

■**Input:** 특정 포트의 입력 방향에 정책 맵을 적용합니다.

■**Output:** 특정 포트의 출력 방향에 정책 맵을 적용합니다.

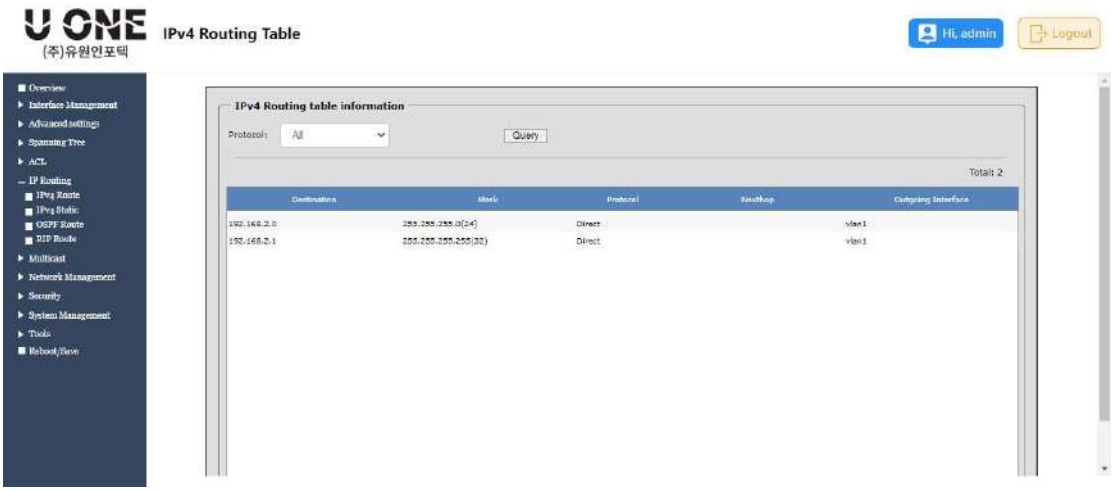


IP 라우팅

IPv4 경로

IP Routing > IPv4 Route

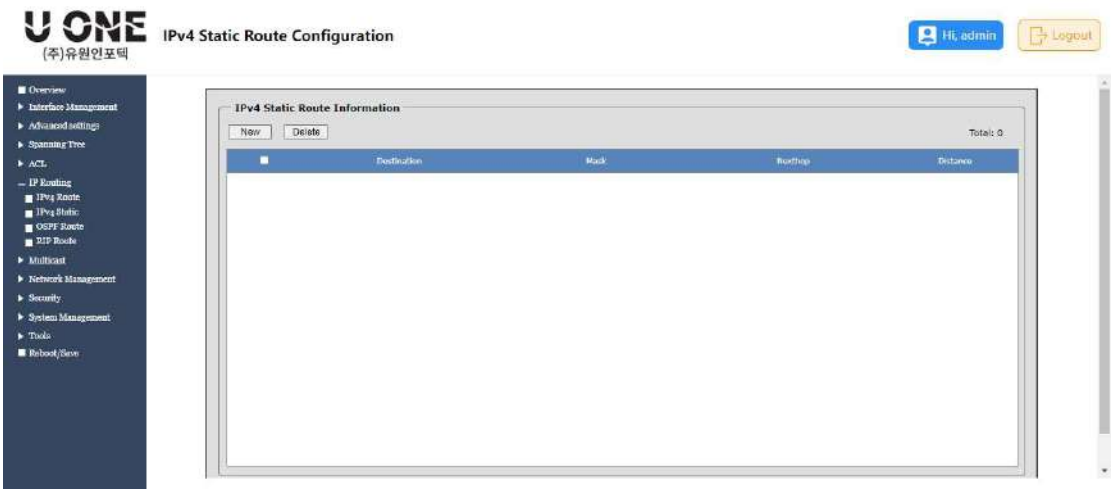
이 페이지는 BGP 경로 테이블, 직접 경로 테이블, OSPF 경로 테이블, RIP 경로 테이블 및 정적 경로 테이블을 포함한 라우팅 테이블을 표시하는 데 사용됩니다.



IPv4 정적

IP Routing > IPv4 Static

이 페이지는 IPv4 고정 경로 항목을 생성하거나 삭제하는 데 사용됩니다.



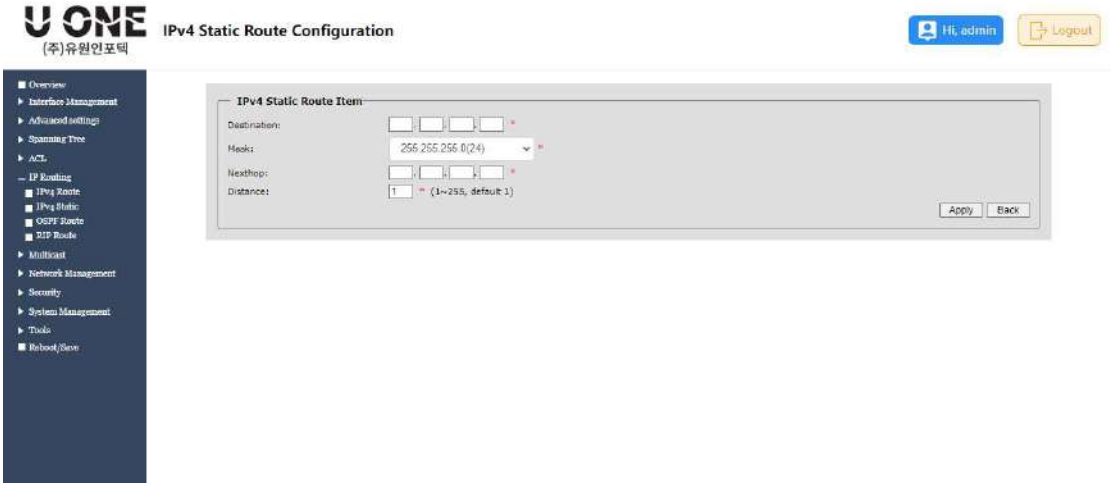
새로 만들기 버튼을 클릭하여 IPv4 고정 경로 항목 생성 페이지로 들어갑니다.

◆**Destination** – 대상 네트워크, 서브네트워크 또는 호스트의 IP 주소입니다.

◆**Mask** – 연결된 IP 서브넷의 네트워크 마스크입니다. 이 마스크는 특정 서브넷으로 라우팅하는 데 사용되는 호스트 주소 비트를 식별합니다.

◆**Nexthop** – 이 경로에 사용되는 다음 라우터 홉의 IP 주소입니다.

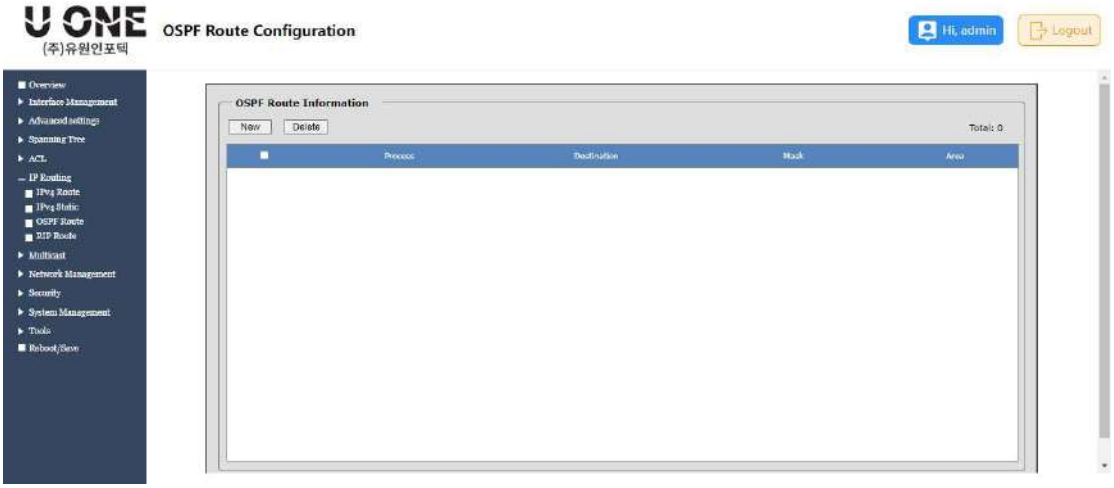
◆**Distance** – 동적 경로의 거리가 정적 경로에 대해 구성된 거리보다 작은 경우 이 경로가 동적 라우팅 정보로 재정의될 수 있음을 나타내는 관리 거리입니다. 동적 유니캐스트 라우팅 프로토콜에서 사용되는 기본 관리 거리는 OSPF의 경우 110, RIP의 경우 120, eBGP의 경우 20, iBGP의 경우 200입니다. (범위: 1~255, 기본값: 1)



OSPF 경로

IP Routing > OSPF Route

이 페이지는 IPv4 OSPF 경로 항목을 생성하거나 삭제하는 데 사용됩니다.



New 버튼을 클릭하여 OSPF Route Item 생성 페이지로 들어갑니다.

◆**Process** – OSPF 프로세스 ID를 나타냅니다. 매개변수를 지정하지 않으면 모든 OSPF 프로세스가 다시 시작됩니다.

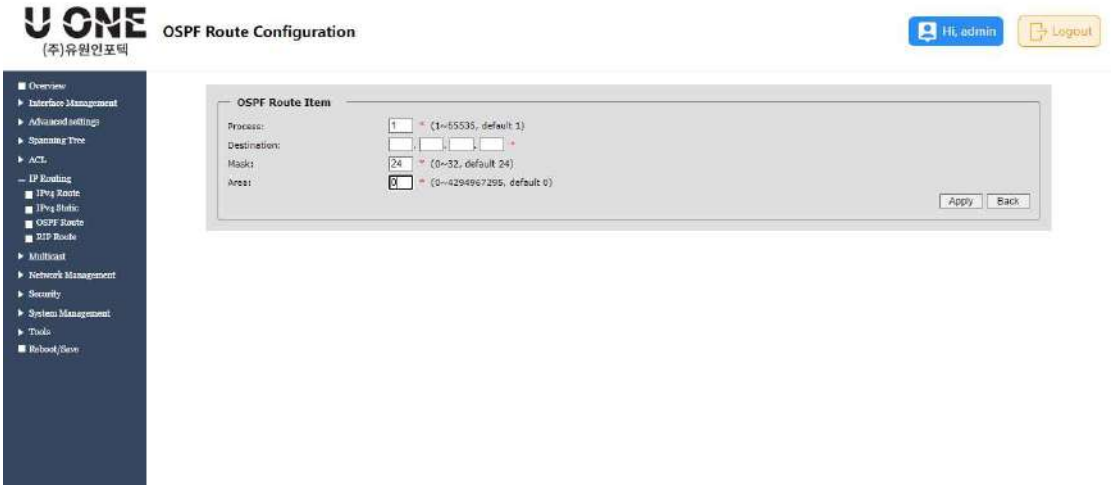
◆**Destination** – 대상 네트워크, 서브네트워크 또는 호스트의 IP 주소입니다.

◆**Mask** – 연결된 IP 서브넷의 네트워크 마스크입니다. 이 마스크는 특정 서브넷으로 라우팅하는 데 사용되는 호스트 주소 비트를 식별합니다.

◆**Area** – 네트워크의 논리적 분할을 나타내는 OSPF의 중요한 개념입니다. OSPF는 네트워크를 여러 영역으로 분할함으로써 전송되는 라우팅 정보의 양을 줄이고 네트워크 성능과 확장성을 향상시킬 수 있습니다.

OSPF 프로토콜에서 영역은 전체 네트워크를 여러 패치로 나누는 논리적 파티션입니다. 영역에는 백본 영역, 일반 영역, 스텁 영역의 세 가지 주요 유형이 있습니다. 백본영역은 가장 중요한 영역으로 식별번호가 0.0.0.0으로 모든 영역을 연결하고 영역 간 데이터 트래픽 전달을 담당한다. 백본 영역을 제외한 일반 영역의 다른 영역은 적어도 하나의

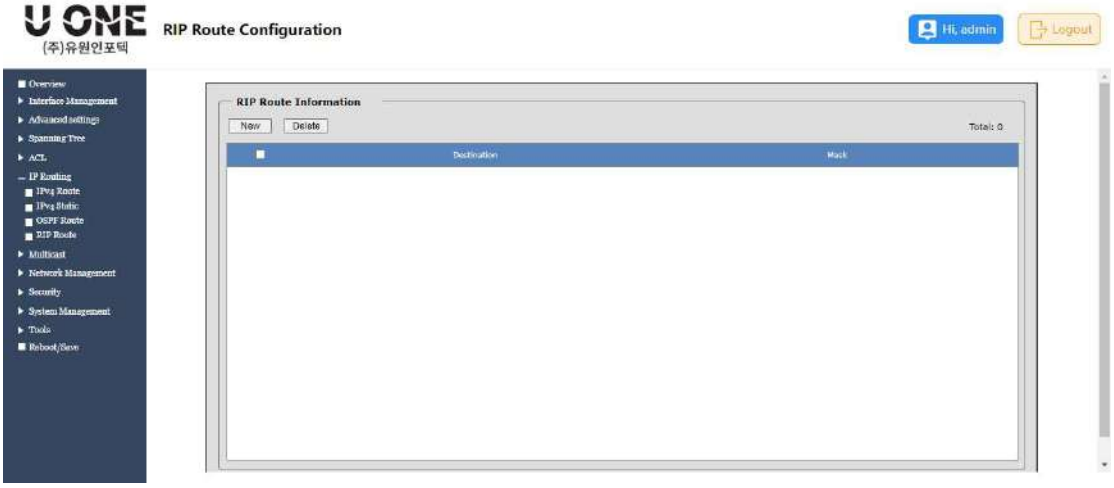
백본 영역과 연결되어야 다른 영역과의 통신 및 경로 계산이 가능합니다. 라우터 간 정보 교환을 단순화하고 네트워크 성능과 안정성을 향상시킵니다.



RIP 경로

IP Routing > RIP Route

이 페이지는 IPv4 RIP 경로 항목을 생성하거나 삭제하는 데 사용됩니다.

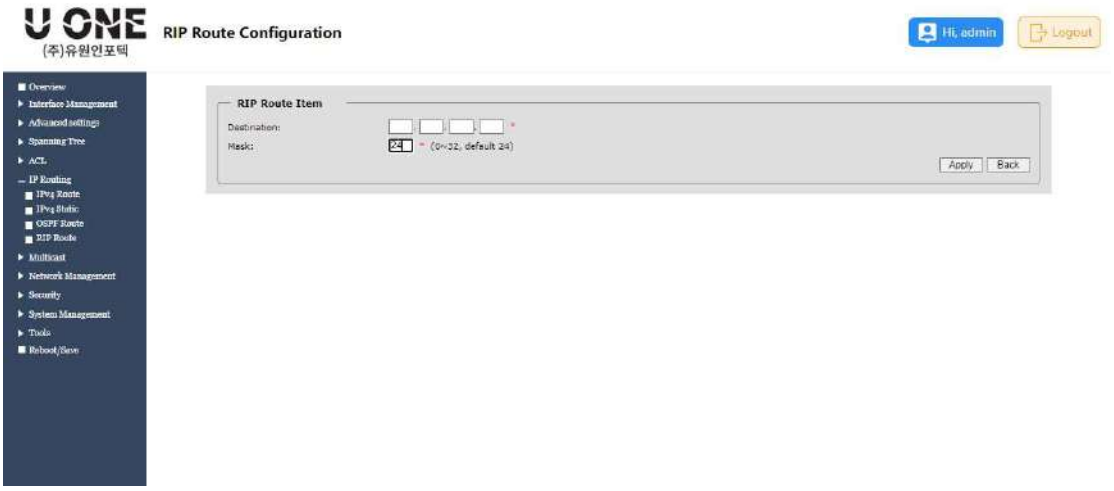


새로 만들기 버튼을 클릭하여 RIP 경로 항목 생성 페이지로 들어갑니다.

◆**Destination** – 대상 네트워크, 서브네트워크 또는 호스트의 IP 주소입니다.

◆**Mask** – 연결된 IP 서브넷의 네트워크 마스크입니다. 이 마스크는 특정 서브넷으로

라우팅하는 데 사용되는 호스트 주소 비트를 식별합니다.



멀티캐스트

IGMP 스누핑

Multicast >IGMP Snooping

이 페이지는 멀티캐스트 트래픽의 매개변수를 구성하는 데 사용됩니다.

◆**IGMP Snooping** – 활성화되면 스위치는 네트워크 트래픽을 모니터링하여 멀티캐스트 트래픽을 수신하려는 호스트를 결정합니다. 이를 IGMP 스누핑이라고 합니다.

◆**TCN Querier count** – IGMP 쿼리어의 견고성 계수는 패킷 재전송 횟수에 따라 네트워크 패킷 손실 가능성을 보상하기 위해 설정됩니다. 재전송이 많을수록 IGMP 쿼리기는 더욱 "강건"해지지만 필요한 멀티캐스트 그룹 시간 초과 시간은 길어집니다.

◆**Max Member Number** – IGMP 멀티캐스트 그룹의 최대 구성원 수입니다.

◆**TCN Querier Interval** – IGMP 쿼리어가 시작되면 "IGMP 쿼리 엔진 시작 쿼리 간격"의 시간 간격으로 "IGMP 쿼리 엔진 시작 쿼리 시간" IGMP 일반 그룹 쿼리 메시지를 보내 현재 네트워크에 멀티캐스트 그룹 구성원이 있는지 빠르게 확인합니다.

◆**Vlan Mode** – 모든 VLAN 또는 단일 VLAN.

◆**Vlan ID** – VLAN의 ID.

◆**Discard Unkonwn** – 등록되지 않은 멀티캐스트 트래픽을 삭제합니다.

◆**Report Suppression** – IGMPv1/v2 구성원 보고 메시지를 억제하도록 포트를 설정합니다. IGMP 스누핑이 v3 모드에서 작동하는 경우 구성원 보고 메시지는 억제되지 않습니다.

◆**Fast Leave** – 빠른 나가기가 구성된 후 쿼리자는 멀티캐스트 수신기 완료 메시지를 수신한 후 멀티캐스트 주소 특정 쿼리 메시지 또는 멀티캐스트 주소 및 소스 특정 쿼리 메시지를 보내지 않습니다. 대신 쿼리 수행자는 호스트가 멀티캐스트 그룹을 떠났다는 사실을 업스트림 멀티캐스트 장치에 직접 알립니다. 빠른 나가기 기능은 완료 메시지에 대한 응답 지연을 줄이고 네트워크 대역폭을 절약합니다.

◆**Version** – 네트워크의 다른 장치와의 호환성을 위해 프로토콜 버전을 설정합니다. 이는 스위치가 스누핑 보고서를 보내는 데 사용하는 IGMP 버전입니다. (범위: 1-3;기본값: 2)

◆**Last Member Query Interva** – 멀티캐스트 호스트가 그룹을 탈퇴하면 IGMP 탈퇴 메시지를 보냅니다.

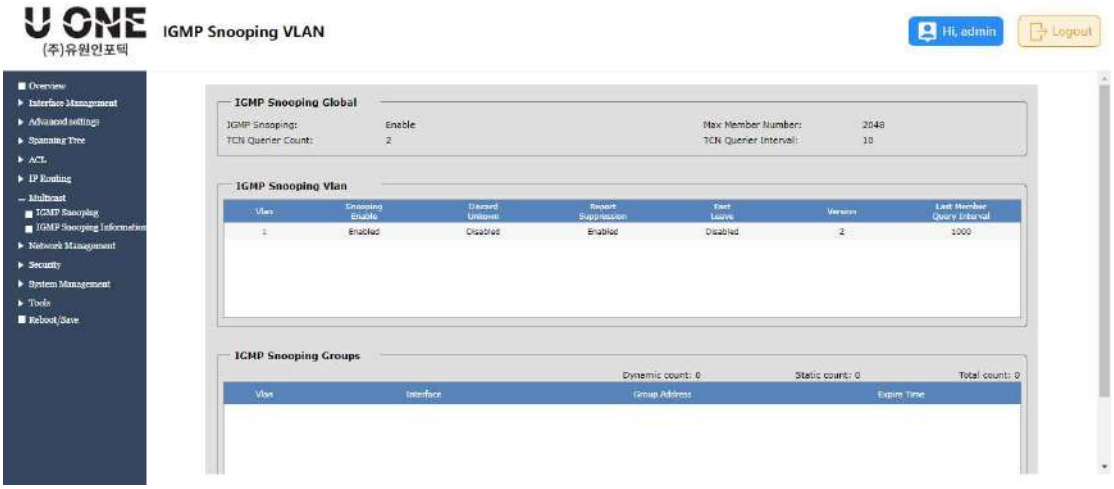
스위치는 탈퇴 메시지를 수신하면 IGMP 그룹별 또는 그룹 및 소스별 쿼리 메시지를 보내 해당 호스트가 마지막으로 그룹을 탈퇴했는지 확인하고 타이머를 시작합니다.

타이머가 만료되기 전에 보고서가 수신되지 않으면 그룹 기록이 삭제되고 보고서가 업스트림 멀티캐스트 라우터로 전송됩니다. 값을 줄이면 그룹 또는 소스의 마지막 구성원 손실을 감지하는 데 걸리는 시간이 줄어들지만 버스트 트래픽이 더 많이 발생할 수 있습니다. 이 속성은 IGMP 스누핑 프록시 보고가 활성화되거나 IGMP 쿼리기가 활성화된 경우에만 적용됩니다.

IGMP 스누핑 정보

Multicast >IGMP Snooping Information

이 페이지는 IGMP 스누핑 글로벌 상태, IGMP 스누핑 VLAN 및 IGMP 스누핑 그룹의 매개변수를 포함하여 IGMP 스누핑 상태를 표시하는 데 사용됩니다.



네트워크 관리

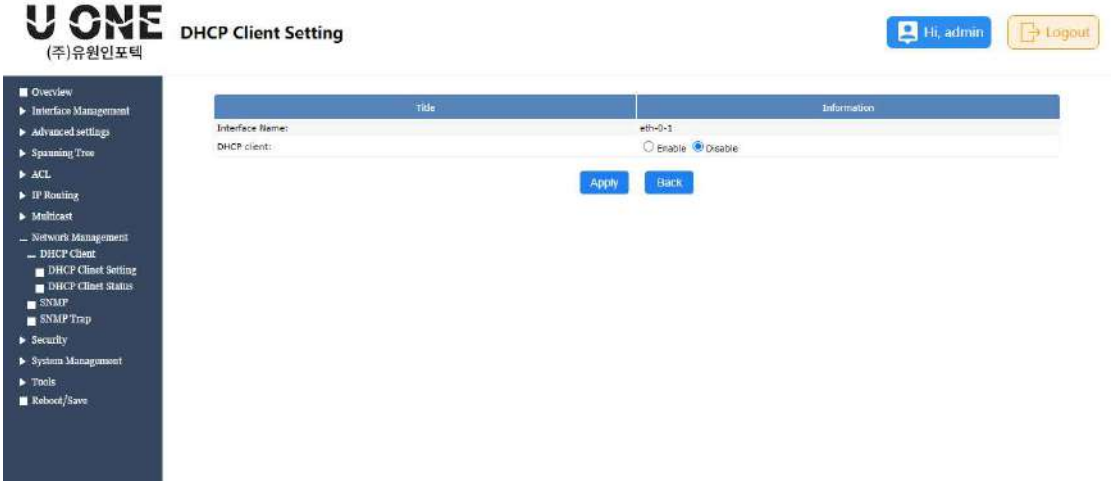
DHCP 클라이언트

DHCP 클라이언트 설정

Network management >DHCP Client >DHCP Client Setting

이 페이지는 포트에서 DHCP 클라이언트 기능을 활성화 또는 비활성화하는 데 사용됩니다.

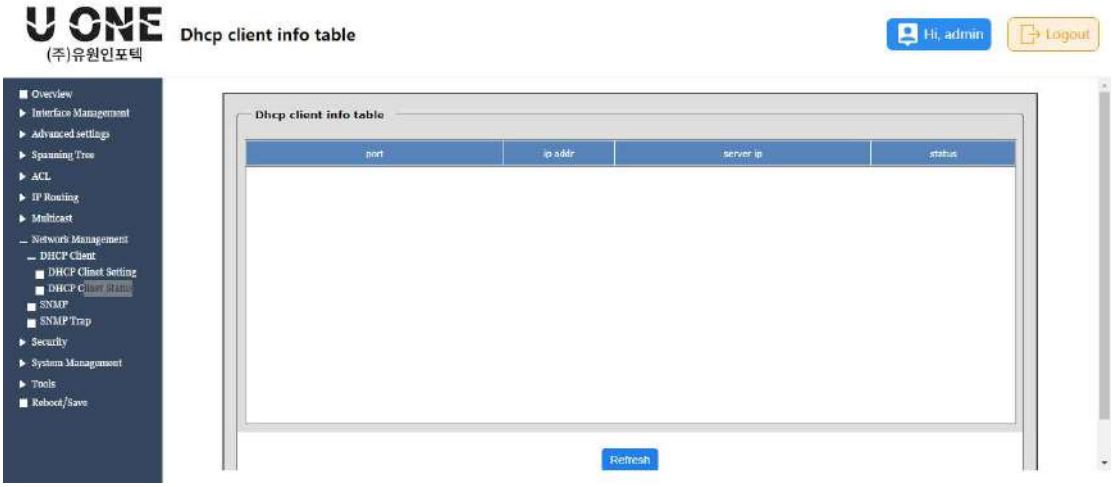
포트를 선택하고 수정 버튼을 클릭하면 단일 또는 다중 포트에 대한 DHCP 클라이언트 설정 페이지로 들어갑니다.



DHCP 클라이언트 상태

Network management >DHCP Client >DHCP Client Status

이 페이지는 포트, 포트의 IP 주소, DHCP 서버 IP 및 포트 상태를 포함한 DHCP 클라이언트 정보 테이블을 표시하는 데 사용됩니다.



SNMP

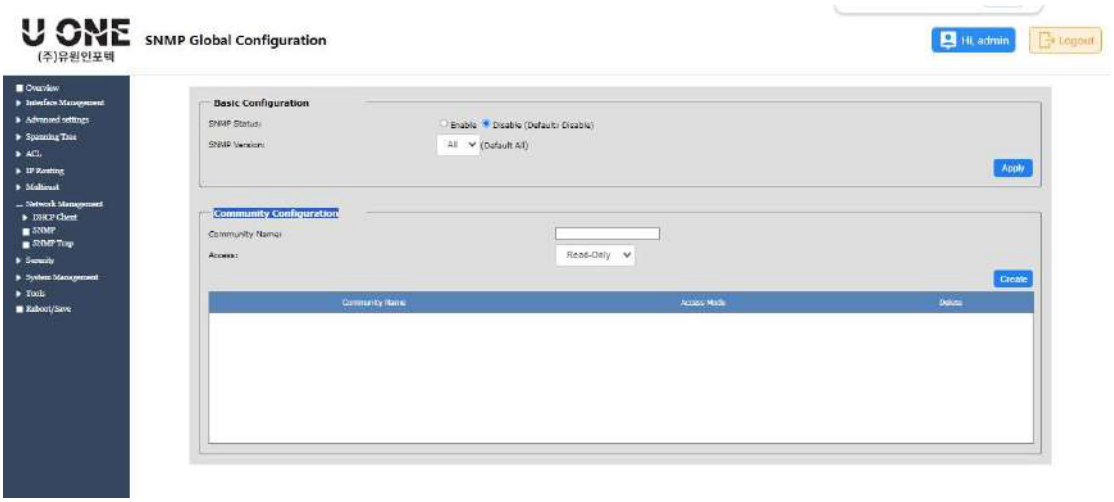
Network management >SNMP

이 페이지는 모든 관리 클라이언트(버전 All, 1, 2, 3)에 대해 SNMP 서비스를 활성화 또는 비활성화하고 커뮤니티 구성을 설정하는 데 사용됩니다.

◆**Access Mode** – 커뮤니티 문자열에 대한 액세스 권한을 지정합니다.

■**Read-Only** – 승인된 관리 스테이션은 MIB 개체만 검색할 수 있습니다.

■**Read/Write** – 승인된 관리 스테이션은 MIB 개체를 검색하고 수정할 수 있습니다.



SNMP 트랩

Network management >SNMP Trap

이 페이지는 Trap의 매개변수를 구성하는 데 사용됩니다.

◆**Coldstart Trap** – 스위치는 콜드 재시작 시 트랩을 SNMP 서버로 보냅니다.

◆**Warmstart Trap** – 스위치는 웜 재시작 시 트랩을 SNMP 서버로 보냅니다.

◆**Linkup Trap** – 스위치는 포트 연결 시 트랩을 SNMP 서버로 보냅니다.

◆**Linkdown Trap** – 스위치는 포트 연결이 끊어지면 트랩을 SNMP 서버로 보냅니다.

◆**System Trap** – 스위치는 시스템 예외가 발생하면 트랩을 SNMP 서버로 보냅니다.

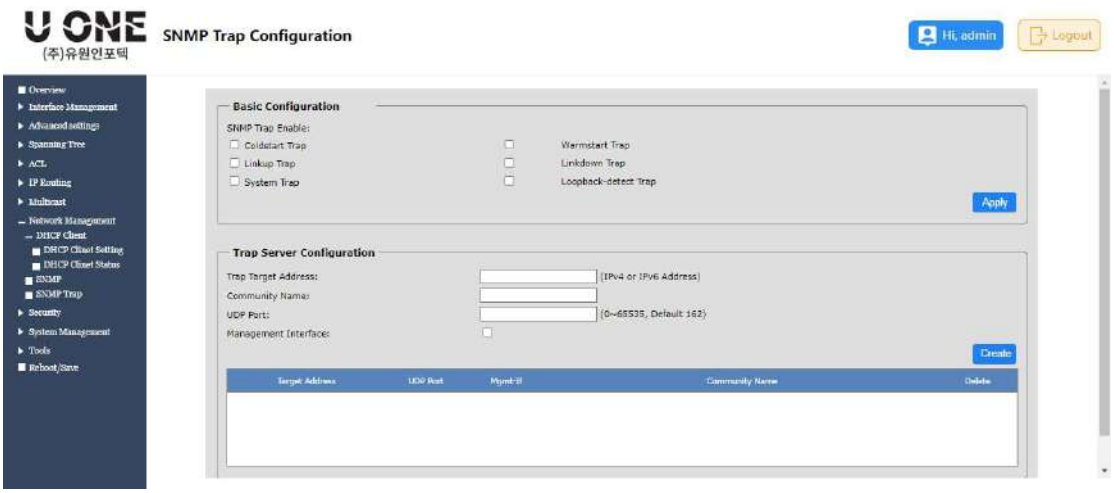
◆**Loopback-detect Trap** – 스위치는 루프가 감지되면 트랩을 SNMP 서버로 보냅니다.

◆**Community Name** – 새 트랩 관리자 항목에 대한 유효한 커뮤니티 문자열을 지정합니다.

◆**Trap Target Address** – 알림 메시지를 수신할 새 관리 스테이션의 IP 주소입니다.

◆**UDP Port** – 트랩 관리자가 사용하는 UDP 포트 번호를 지정합니다.

◆**Management Interface** – 관리 포트를 통해 SNMP 서버를 연결합니다.

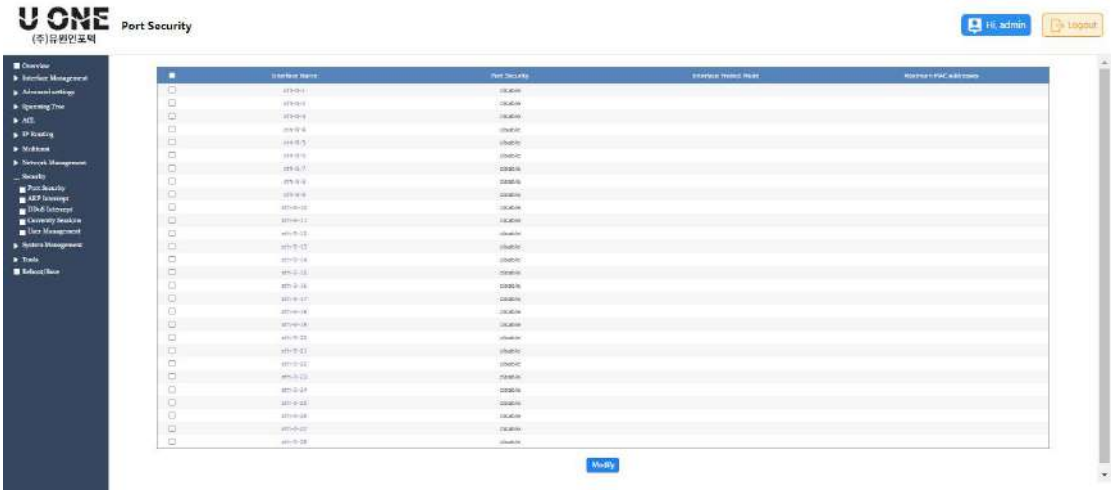


보안

포트 보안

Security >Port Security

이 페이지는 스위치 포트에서 학습할 수 있고 주소 테이블에 저장되며 네트워크 액세스 권한을 부여받을 수 있는 장치 MAC 주소의 최대 개수를 구성하는 데 사용됩니다.



포트를 선택하고 수정 버튼을 클릭하여 단일 또는 다중 포트에 대한 포트 보안 구성 페이지로 들어갑니다.

◆**Interface Name** – 포트 번호.

◆**Port Security** – 포트의 포트 보안을 활성화하거나 비활성화합니다.

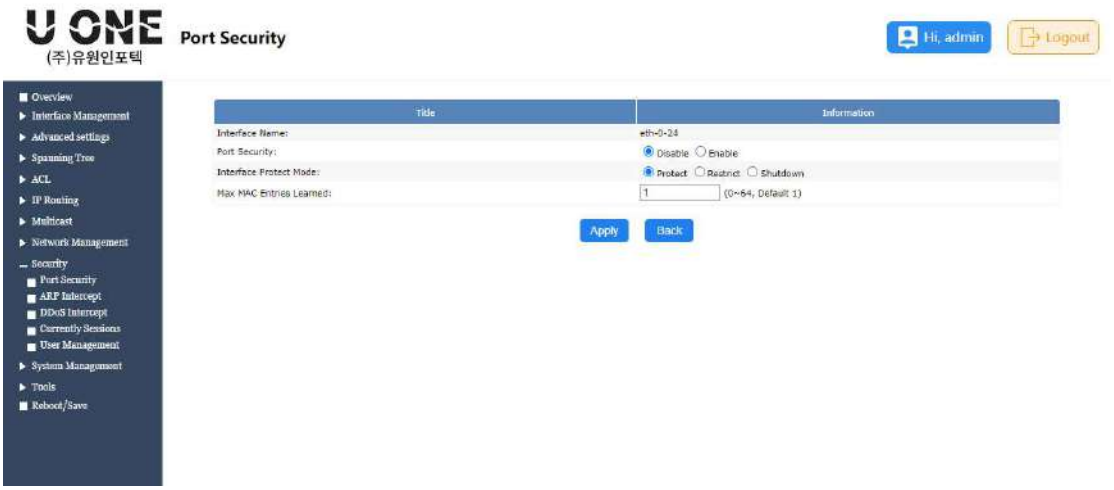
◆**Interface Protect Mode** – 보호, 제한 및 종료.

■**Protect** – 포트 보안 위반 시 패킷을 폐기합니다.

■**Restrict** – 포트 보안 위반 시 메시지를 삭제하고 로그를 인쇄합니다.

■**Shutdown** – 포트 보안 위반 시 포트를 비활성화합니다.

◆**Max MAC Entries Learned** – 포트에서 학습할 수 있는 최대 MAC 주소 수입니다.



ARP **인터셉트**

Security >ARP Intercept

이 페이지는 초당 수신되는 최대 ARP 패킷 수를 설정하는 데 사용됩니다. 이 수를

초과하면 ARP 공격을 방지하기 위해 폐기됩니다.

DDoS 인터셉트

Security >DDoS Intercept

이 페이지는 분산 서비스 거부 공격으로부터 보호하는 데 사용됩니다. DDoS 공격은 컴퓨터나 네트워크 리소스가 제공하는 서비스를 차단하려는 시도입니다.

◆**Smurf Attack Intercept** – 가해자가 브로드캐스트 대상 IP 주소(255.255.255.255)로 대량의 스푸핑된 ICMP 에코 요청 트래픽을 생성하는 공격으로, 모두 의도한 피해자의 스푸핑된 소스 주소를 사용합니다. ICMP Echo 응답 패킷을 보내는 데 필요한 많은 인터럽트로 인해 피해자는 충돌을 겪게 됩니다.

◆**Fraggle Attack Intercept** – 이 공격은 스머프 공격의 변형입니다. ICMP 패킷을 엄격하게 검사하는 방화벽을 회피하기 위해 더 이상 ICMP 요청 패킷을 브로드캐스트 주소로 보내지 않습니다. 대신 UDP 패킷을 사용합니다.

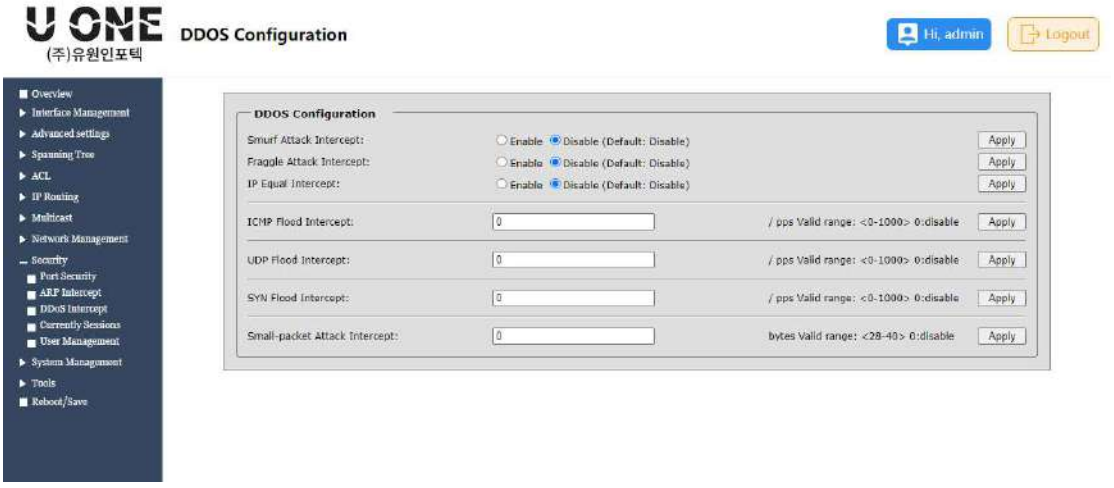
◆**IP Equal Intercept** – 소스 IP 주소와 일치하도록 대상 IP 주소를 스푸핑한 패킷을 활용하는 공격입니다.

◆**ICMP Flood Intercept** – ICMP 패킷으로 대상 IP를 넘치게 하면 사용 가능한 대역폭을 모두 사용하여 합법적인 트래픽을 차단합니다.

◆**UDP Flood Intercept** – 가해자가 원격 호스트의 임의 포트에 대량의 UDP 패킷(스푸핑된 소스 IP 유무에 관계없이)을 보내는 공격입니다. 대상은 애플리케이션이 해당 포트에서 수신 대기 중인지 확인하고 ICMP 목적지 도달 불가능 패킷으로 응답합니다. 많은 ICMP 패킷을 보내야 하므로 결국 다른 클라이언트가 해당 패킷에 연결할 수 없게 됩니다.

◆**SYN Flood Intercept** – 가해자가 연속적인 TCP SYN 요청(스푸핑된 소스 IP 유무에 관계없이)을 대상으로 보내고 ACK 패킷을 반환하지 않는 공격입니다. 이러한 반개방 연결은 대상의 리소스를 바인딩하고 새로운 연결을 만들 수 없으므로 서비스 거부가 발생합니다.

◆**Small-packet Attack Intercept** – IP 소형 패킷 공격에는 대상 시스템에 많은 수의 소형 패킷을 보내 해당 시스템의 리소스를 소비하는 작업이 포함됩니다.



현재 세션

Security >Currently Session

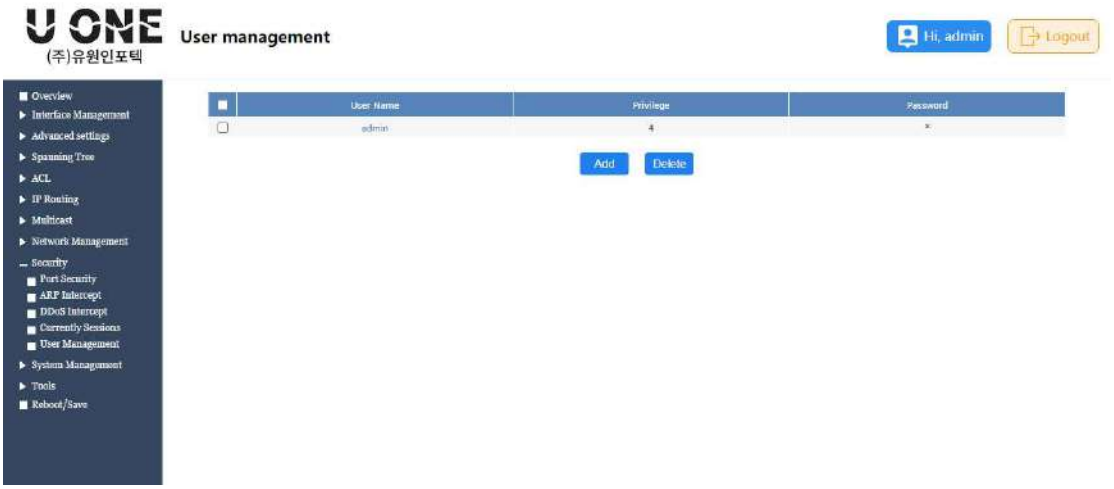
이 페이지는 활성 웹 세션의 매개변수를 표시하는 데 사용되며 이를 삭제하거나 사용자를 강제로 로그아웃시킬 수 있습니다.

사용자 관리

Security > User Management

수동으로 구성된 사용자 이름과 비밀번호를 기반으로 스위치에 대한 관리 액세스를

제어하는 페이지입니다.



추가 버튼을 클릭하여 사용자 구성 추가/수정 페이지로 들어갑니다.

◆**User Name** – 사용자의 이름입니다.

◆**Password** – 사용자 비밀번호를 지정합니다.

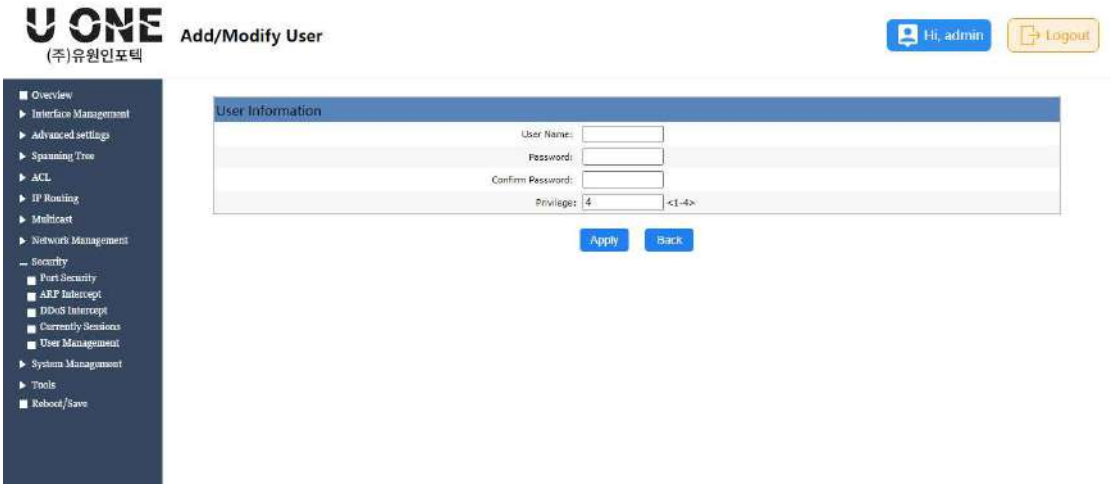
◆**Confirm Password** – 오류가 발생하지 않았는지 확인하려면 이전 필드에 입력한

문자열을 다시 입력하세요. 이 두 필드가 일치하지 않으면 스위치는 비밀번호를 변경하지

않습니다.

◆**Privilege** – 사용자 수준을 지정합니다. (옵션: 1 - 일반, 4 - 권한 있음)

일반 권한 수준은 스위치의 현재 상태를 표시하는 제한된 수의 명령과 여러 데이터베이스 지우기 및 재설정 기능에 대한 액세스를 제공합니다. 권한 수준은 모든 명령에 대한 전체 액세스를 제공합니다.



시스템 관리

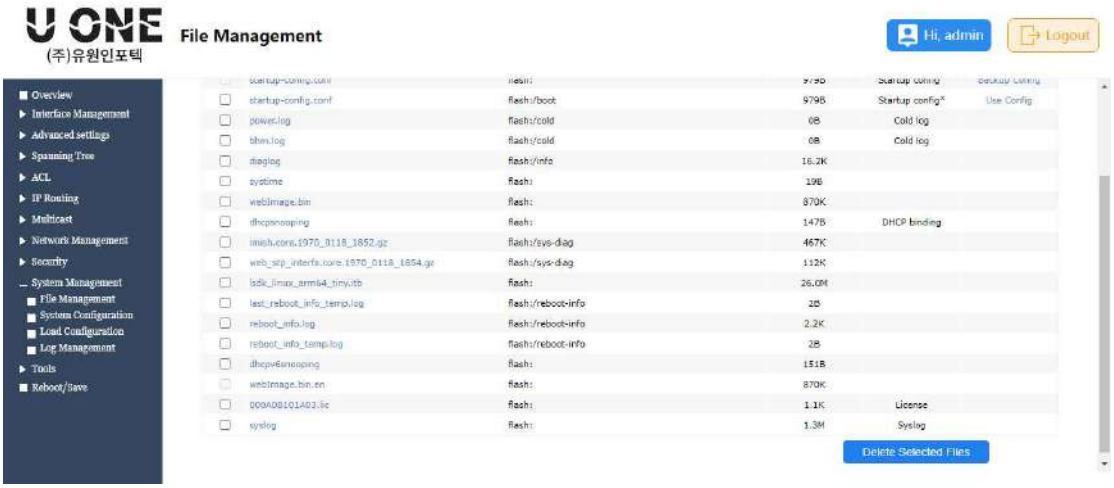
파일 관리

System Management > File Management

이 페이지는 장치의 파일을 관리하는 데 사용됩니다.

사용자는 구성 파일을 PC에 업로드하고 런타임 파일을 장치에 다운로드할 수 있습니다.

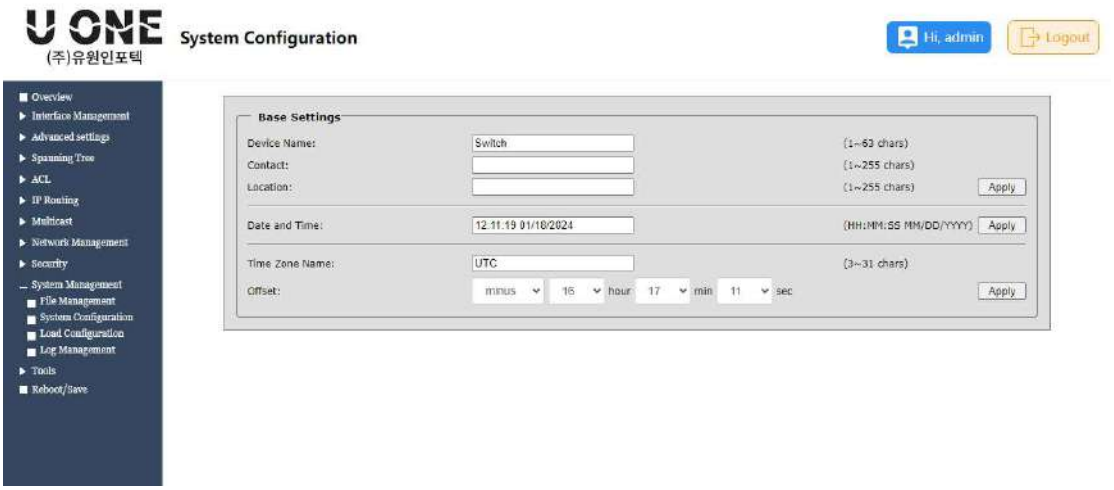
구성 파일을 다른 구성 파일에 복사하고 구성 파일을 삭제합니다.



시스템 설정

System Management > System Configuration

이 페이지는 스위치에 대한 설명과 시간을 구성하는 데 사용됩니다.



Load 설정

System Management > Load Configuration

이 페이지는 시스템 로그를 표시하고 삭제를 허용하는 데 사용됩니다.

◆**Level** – 0-emergency, 1-alert, 2-critical, 3-error, 4-warning, 5-notice, 6-information, 7-debug

툴

핑

Tools > Ping

이 페이지는 ICMP 에코 요청 패킷을 네트워크의 다른 노드로 보내는 데 사용됩니다.

(호환성을 위한 팁: IE 또는 Firefox를 사용하십시오)

◆**VRF ID** – 가상 라우팅 및 전달 ID는 단일 물리적 라우터 내에서 서로 다른 가상 라우팅 인스턴스를 구별하는 고유 식별자입니다. 각 VRF에는 자체 라우팅 테이블이 있어 동일한 장치에서 트래픽 격리와 여러 라우팅 도메인이 가능합니다. 이는 다중 테넌트 환경에서 트래픽을 분리하는 데 유용합니다.

◆**Destination IP** – ping 중인 IP 주소입니다.

Traceroute

Tools > Traceroute

이 페이지는 지정된 대상으로 이동하는 경로 패킷을 표시하는 데 사용됩니다. (호환성을 위한 팁: IE 또는 Firefox를 사용하십시오)

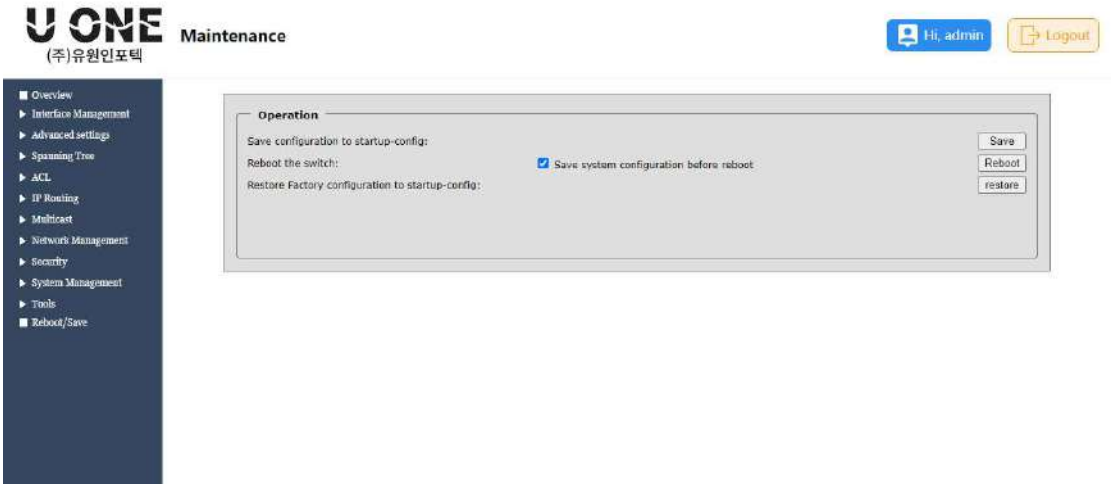
◆**Destination IP** – 추적 중인 IP 주소입니다.

재시작/저장

Reboot/Save

이 페이지는 스위치 구성을 저장하고, 스위치를 다시 시작하고, 장치를 공장 설정으로 복원하는 데 사용됩니다.

◆**Save** – 구성을 시작 구성에 저장하면 재부팅 후에도 구성이 유지됩니다.

◆**Reboot** – 스위치를 재부팅하십시오.

◆**Restore** – 스위치를 재부팅하고 공장 설정을 복원하십시오.