사용자 가이드

10G 포트가 있는 Omada VPN 공유기

콘텐츠

이 가이드 정보

본 사용자 가이드는 Omada VPN 라우터 관리를 위한 정보를 제공합니다. 작동하기 전에 이 가이드를 주의 깊게 읽어주세요.

대상 독자

이 가이드는 IT 개념과 네트워크 용어에 익숙한 네트워크 관리자를 대상으로 합니다.

컨벤션

이 가이드를 사용할 때 SafeStream 시리즈 제품에서 사용할 수 있는 기능은 모델 및 소프트웨어 버전에 따라 다를 수 있다는 점에 유의하세요. SafeStream 시리즈 제품의 사용 가능 여부는 지역 또는 ISP에 따라 다를 수 있습니다. 이 가이드의 모든 이미지, 단계 및 설명은 예시일 뿐이며 실제 사용 환경을 반영하지 않을 수 있습니다.

이 가이드에 소개된 일부 모델은 해당 국가 또는 지역에서 제공되지 않을 수 있습니다. 현지 판매 정보는 https://www.tp-link.com 에서 확인하세요.

본 문서의 정보는 사전 통지 없이 변경될 수 있습니다. 본 문서의 작성 과정에서 내용의 정확성을 보장하기 위해 모든 노력을 기울였으나, 본 문서의 모든 진술, 정보 및 권장 사항은 명시적이든 묵시적이든 어떠한 종류의 보증도 구성하지 않습니다. 사용자는 제품 적용에 대한 전적인 책임을 져야 합니다.

이 가이드에서는 다음과 같은 규칙이 사용됩니다:

- 기호는 노트를 나타냅니다. 노트에는 장치를 더 잘 활용하는 데 도움이 되는 제안이나 참고 자료가 포함되어 있습니다.
- **메뉴 이름 > 하위 메뉴 이름 > 탭** 페이지는 메뉴 구조를 나타냅니다. 상태 **> 트래픽 통계 > 인터페이스** 통계는 상태 메뉴 아래에 있는 트래픽 통계 메뉴 옵션 아래의 인터페이스 통계 페이지를 의미합니다.
- **굵은** 글꼴은 버튼, 도구 모음 아이콘, 메뉴 또는 메뉴 항목을 나타냅니다.

자세한 정보

- 최신 소프트웨어 및 문서는 다운로드 센터(https://www.tp-link.com/support)에서 확인할 수 있습니다.
- 설치 가이드(IG)는 이 가이드를 찾을 수 있는 곳이나 라우터 패키지 내부에서 찾을 수 있습니다.
- 사양은 제품 페이지(https://www.tp-link.com)에서 확인할 수 있습니다.
- TP-Link 사용자 또는 엔지니어에게 질문하고, 답변을 찾고, 소통하려면 https://community.tp-link.com 를 방문하여 TP-Link 커뮤니티에 가입하세요.
- 기술 지원 연락처 정보는 기술 지원 문의 페이지(https://www.tp-link.com/support)에서 확인할 수 있습니다.

파트 1

라우터에 액세스하기

챕터

1 Det 관리 방법 결정

네트워크를 구축하기 전에 실제 네트워크 상황에 따라 적절한 라우터 관리 방법을 선택하세요. 라우터는 두 가지 구성 옵션을 지원합니다: 독립형 모드 또는 컨트롤러 모드.

■ 컨트롤러 모드

액세스 포인트, 스위치, 게이트웨이와 같은 대규모 디바이스로 구성된 대규모 네트워크를 중앙에서 구성하고 관리하려면 컨트롤러 모드를 사용하는 것이 좋습니다. 컨트롤러 모드에서는 Omada Pro SDN 컨트롤러를 통해 라우터를 중앙에서 구성하고 모니터링할 수 있습니다.

Omada Pro SDN 컨트롤러 관리를 위해 라우터를 준비하려면 컨트롤러 설정을 참조하세요. 이러한 상황에서의 네트워크 토폴로지에 대한 자세한 지침과 Omada Pro SDN 컨트롤러 사용 방법은 Omada Pro SDN 컨트롤러 사용자 가이드를 참조하세요. 이 가이드는 공식 웹사이트의 다운로드 센터(https://www.tp-link.com/support/download/)에서 찾을 수 있습니다.

■ 독립 실행형 모드

네트워크 규모가 비교적 작고 관리해야 할 장치가 하나 또는 소수에 불과한 경우, 독립형 모드를 권장합니다. 독립 실행형 모드에서는 GUI(그래픽 사용자 인터페이스, 이 글에서는 웹 인터페이스라고도 함)를 사용하여 라우터에 액세스하고 관리할 수 있습니다. 라우터는 사용자 인증을 위해 두 개의 내장 웹 서버, 즉 HTTP 서버와 HTTPS 서버를 사용합니다.

이 사용자 가이드는 독립 실행형 모드에서 라우터를 구성하고 모니터링하는 방법을 소개합니다.

참고:

라우터가 컨트롤러에 의해 관리되는 동안에는 GUI에 액세스할 수 없습니다. 라우터를 다시 독립 실행형 모드로 전환하고 GUI에 액세스하려면 컨트롤러에서 라우터를 잊어버리거나 라우터를 초기화하면 됩니다.

2 W eb 인터페이스 액세스

다음 예는 웹 브라우저를 통해 로그인하는 방법을 보여줍니다.

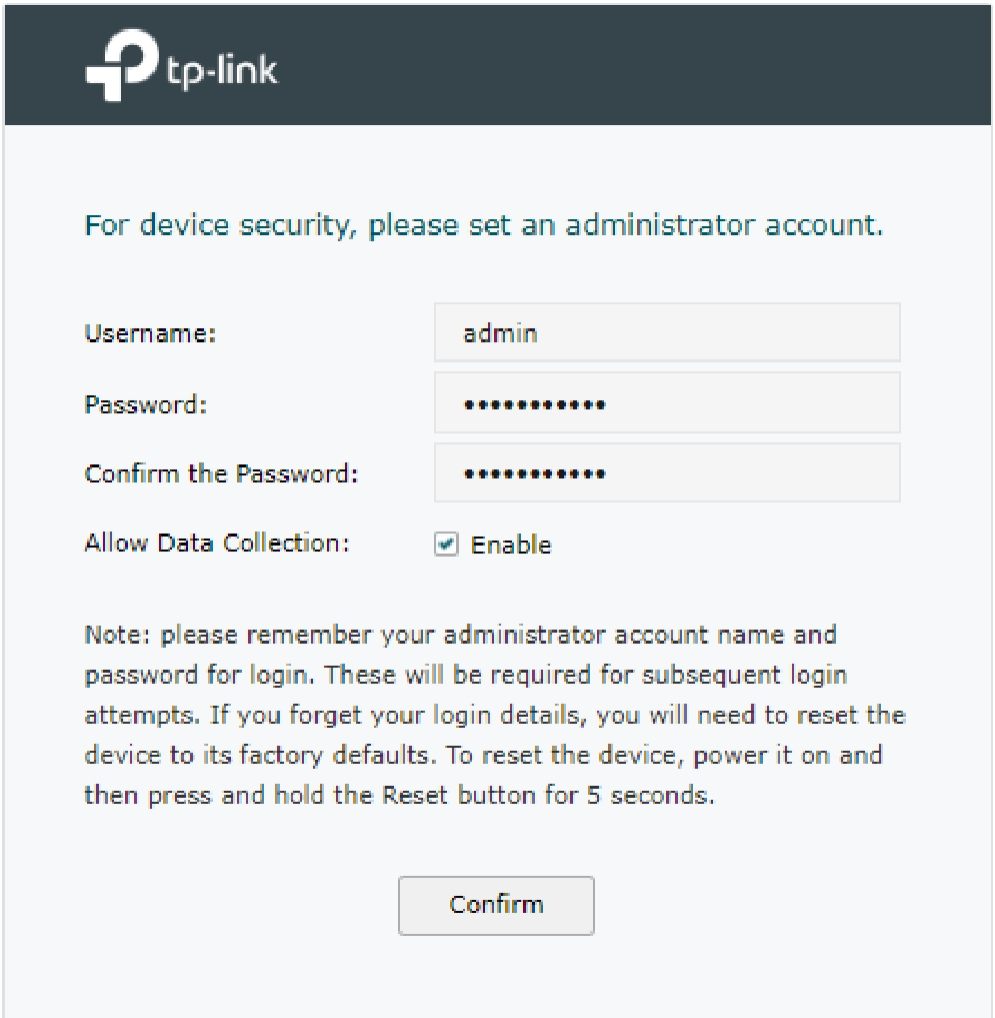
1) RJ45 포트가 있는 라우터의 LAN 포트에 PC를 올바르게 연결합니다. 컴퓨터가 고정 IP 주소로 구성된 경우 "자동으로 IP 주소 받기"로 변경합니다.

2) 웹 브라우저를 열고 브라우저의 주소 필드에 http://192.168.0.1 을 입력한 다음 Enter 키를 누릅니다.

그림 2-1 브라우저에서 라우터의 IP 주소 입력하기

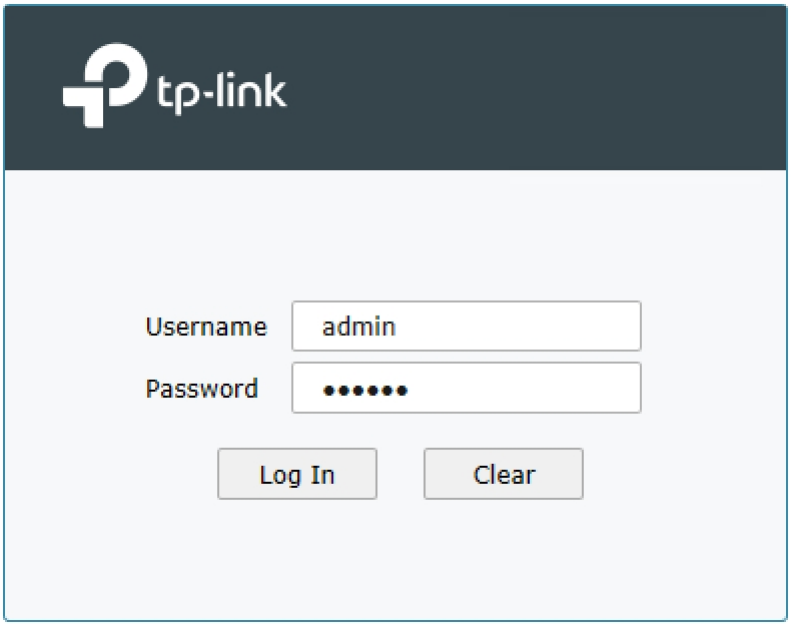
3) 이후 로그인 시도를 위한 사용자 아이디와 비밀번호를 생성합니다.

그림 2-2 사용자 이름 및 비밀번호 만들기



4) 위에 설정한 사용자 아이디와 비밀번호를 사용하여 웹페이지에 로그인합니다.

그림 2-3 로그인 인증



5) 로그인에 성공하면 메인 페이지가 나타나고, 화면 왼쪽의 설정 메뉴를 클릭하여 기능을 구 성할 수 있습니다.

파트 2

상태 정보 보기

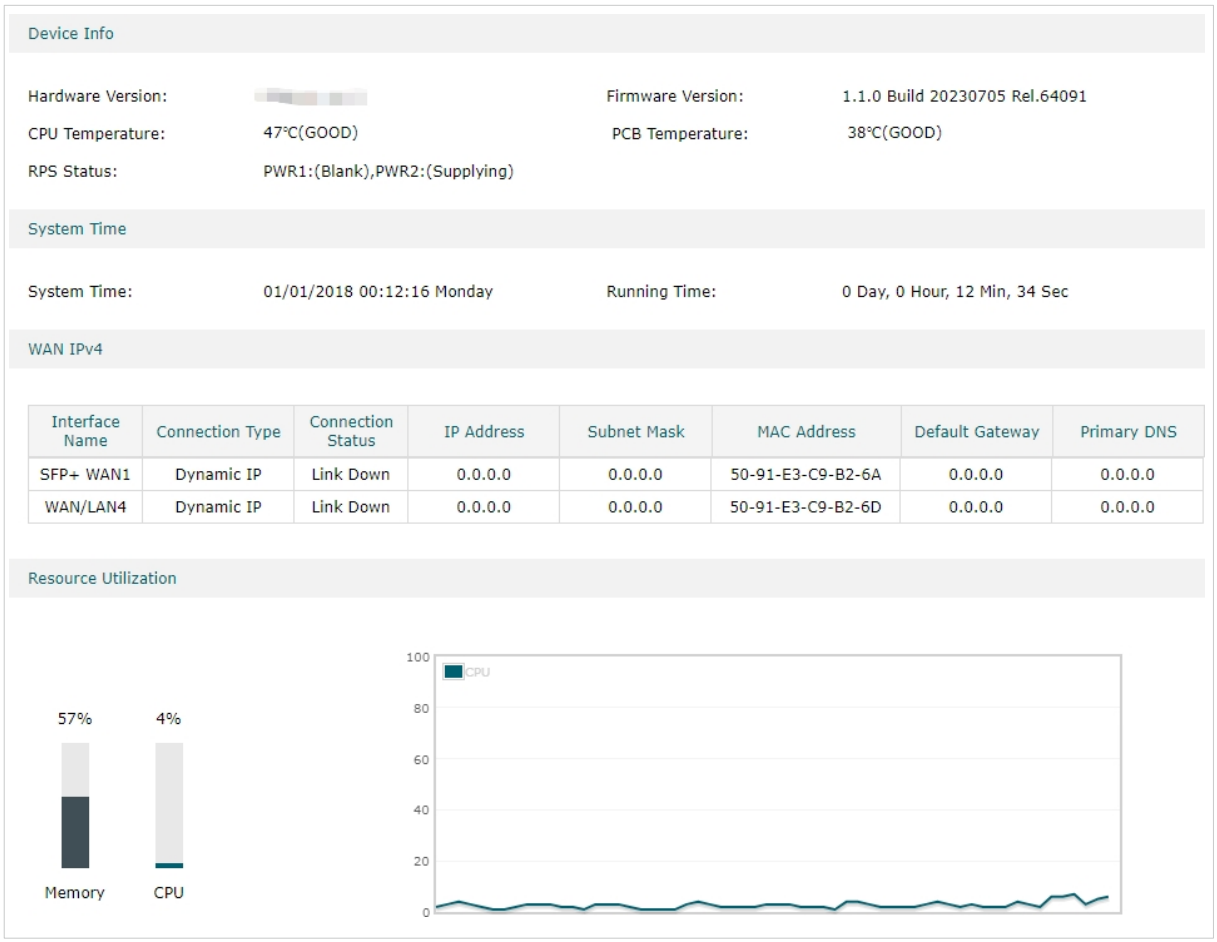
챕터

1 S 시스템 상태

시스템 상태 페이지에는 기본 시스템 정보(하드웨어 버전, 펌웨어 버전, 시스템 시간 등)와 실행 중인 정보(WAN 인터페이스 상태, 메모리 사용률, CPU 사용률 등)가 표시됩니다.

상태 **> 시스템 상태 > 시스템 상태** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 1-1 시스템 상태



2 Tr affic 통계

트래픽 통계에는 인터페이스 및 IP 주소의 데이터 트래픽과 관련된 자세한 정보가 표시됩니다. 이 정보에 따라 트래픽을 모니터링하고 결함을 찾을 수 있습니다.

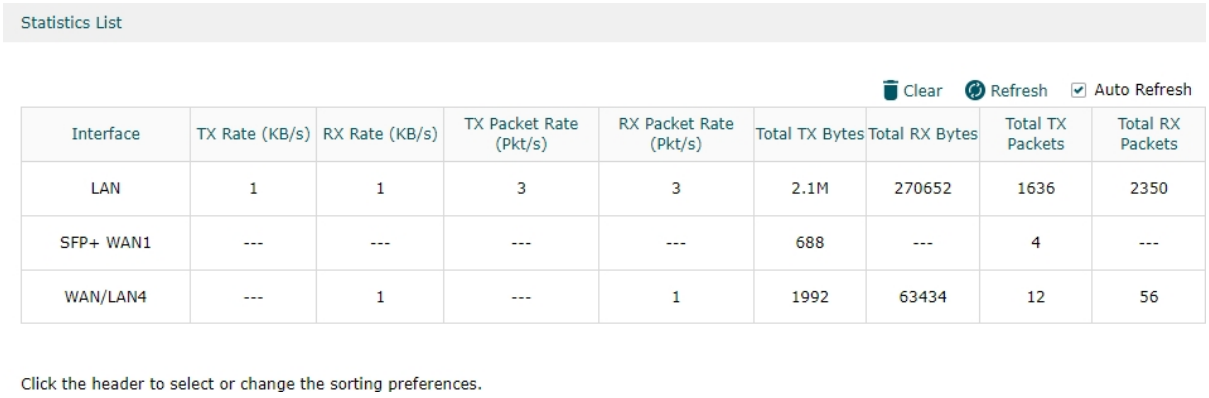
트래픽 통계 기능을 사용하면 가능합니다:

- 각 인터페이스의 트래픽 통계를 확인합니다.
- IP 주소 범위를 지정하고 해당 범위에 있는 IP 주소의 트래픽 통계를 볼 수 있습니다.

2.1 인터페이스 통계 보기

상태 **> 트래픽 통계 > 인터페이스 통계** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 2-1 인터페이스 통계



통계 목록에서 각 인터페이스의 자세한 트래픽 정보를 볼 수 있습니다.

TX 속도(KB/s)	데이터 전송 속도를 초당 킬로바이트 단위로 표시합니다. RX 속
도(KB/s)	데이터 수신 속도를 초당 킬로바이트 단위로 표시합니다.
TX 패킷 전송률 (Pkt/s)	초당 패킷 단위로 데이터를 전송하는 속도를 표시합니다.
RX 패킷 전송률 (Pkt/s)	데이터 수신 속도를 초당 패킷 단위로 표시합니다.
총 TX 바이트	인터페이스에서 전송된 패킷의 바이트를 표시합니다. 총 RX
바이트	인터페이스에서 수신된 패킷의 바이트를 표시합니다.

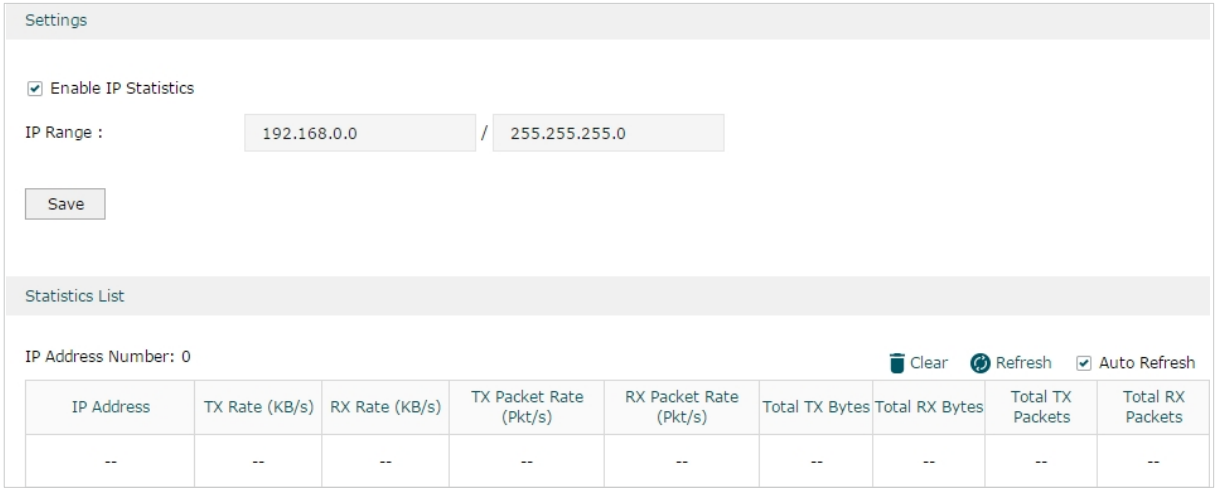
총 TX 패킷 수	인터페이스에서 전송된 패킷 수를 표시합니다. 총 RX 패킷 수
	인터페이스에서 수신된 패킷 수를 표시합니다.

자동 새로 고침을 사용 설정하거나 **새로 고침을** 클릭하여 최신 통계 정보를 가져오거나 **지우기를** 클릭하여 현재 통계 정보를 지울 수 있습니다.

2.2 IP 통계 보기

상태 **> 트래픽 통계 > IP 통계** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 2-2 IP 통계



특정 IP 주소의 트래픽 통계를 보려면 다음 단계를 따르세요:

1) **설정** 섹션에서 IP 통계를 사용 설정하고 모니터링할 IP 범위를 지정합니다.

IP 통계 사용	IP 통계를 사용하려면 확인란을 선택합니다.
IP 범위	IP 범위를 지정합니다. 게이트웨이는 소스 IP 주소 또는 대상 IP 주소가 이 범위에 속하는 패킷을 모니터링하고 통계 목록에 통계 정보를 표시합니다.

2) **통계 목록** 섹션에서 IP 주소의 자세한 트래픽 정보를 확인할 수 있습니다.

IP 주소 번호	IP 주소가 지정된 IP 범위에 있는 활성 사용자 수를 표시합니다.
TX 속도(KB/s)	데이터 전송 속도를 초당 킬로바이트 단위로 표시합니다. RX 속
도(KB/s)	데이터 수신 속도를 초당 킬로바이트 단위로 표시합니다.
TX 패킷 전송률 (Pkt/s)	초당 패킷 단위로 데이터를 전송하는 속도를 표시합니다.

RX 패킷 전송률 (Pkt/s)	데이터 수신 속도를 초당 패킷 단위로 표시합니다.
총 TX 바이트	IP 주소를 소유한 사용자가 전송한 패킷의 바이트를 표시합니다. 총 RX 바이트
	IP 주소를 소유한 사용자가 수신한 패킷의 바이트를 표시합니다.

자동 새로 고침을 사용 설정하거나 **새로 고침을** 클릭하여 최신 통계 정보를 가져오거나 **지우기를** 클릭하여 현재 통계 정보를 지울 수 있습니다.

파트 3

네트워크 구성

챕터

7. VLAN 구성

8. IPv6 구성

1 Ov erview

네트워크 모듈은 WAN 연결, DHCP 서비스, VLAN 등 기본적인 라우터 기능을 제공합니다.

1.1 지원되는 기능

WAN

WAN 포트는 인터넷에 연결됩니다. 네트워크에 여러 개의 WAN 포트를 구성할 수 있습니다. 각 WAN 포트에는 고유한 연결 유형과 매개변수가 있으며, ISP의 요구 사항에 따라 구성해야 합니다.

LAN

라우터의 LAN 포트가 로컬 네트워크 장치에 연결되면 라우터는 해당 장치가 인터넷에 연결할 수 있도록 하는 게이트웨이 역할을 합니다.

IPTV

ISP(인터넷 서비스 제공업체)에서 제공하는 인터넷/IPTV/전화 서비스를 사용하도록 IPTV 설정을 구성합니다.

MAC

필요에 따라 WAN 포트의 기본 MAC 주소를 변경할 수 있습니다.

스위치

라우터는 포트 미러, 속도 제어, 흐름 제어 및 포트 협상과 같은 몇 가지 기본 스위치 포트 관리 기능을 지원하여 트래픽을 모니터링하고 네트워크를 효과적으로 관리할 수 있도록 도와줍니다.

VLAN

VLAN을 사용하면 LAN을 여러 개의 논리적 네트워크로 나누고 편리하고 유연한 방식으로 네트워크 간의 트래픽을 제어할 수 있습니다. LAN은 지리적 위치에 관계없이 부서, 애플리케이션 또는 사용자 유형에 따라 논리적으로 세분화할 수 있습니다.

IPv6

IPv6는 IPv4의 뒤를 잇는 차세대 네트워크 프로토콜입니다. ISP가 IPv6를 지원하는 경우 라우터에 대해 IPv6 네트워크를 구성할 수 있습니다. IPv6 네트워크는 현재 사용 중인 IPv4 네트워크와 충돌을 일으키지 않습니다.

2 W AN 구성

WAN 포트는 인터넷에 연결됩니다. 네트워크에 여러 개의 WAN 포트를 구성할 수 있습니다. 각 WAN 포트에는 고유한 연결 유형과 매개변수가 있으며, ISP의 요구 사항에 따라 구성해야 합니다.

WAN 구성을 완료하려면 다음 단계를 따르세요:

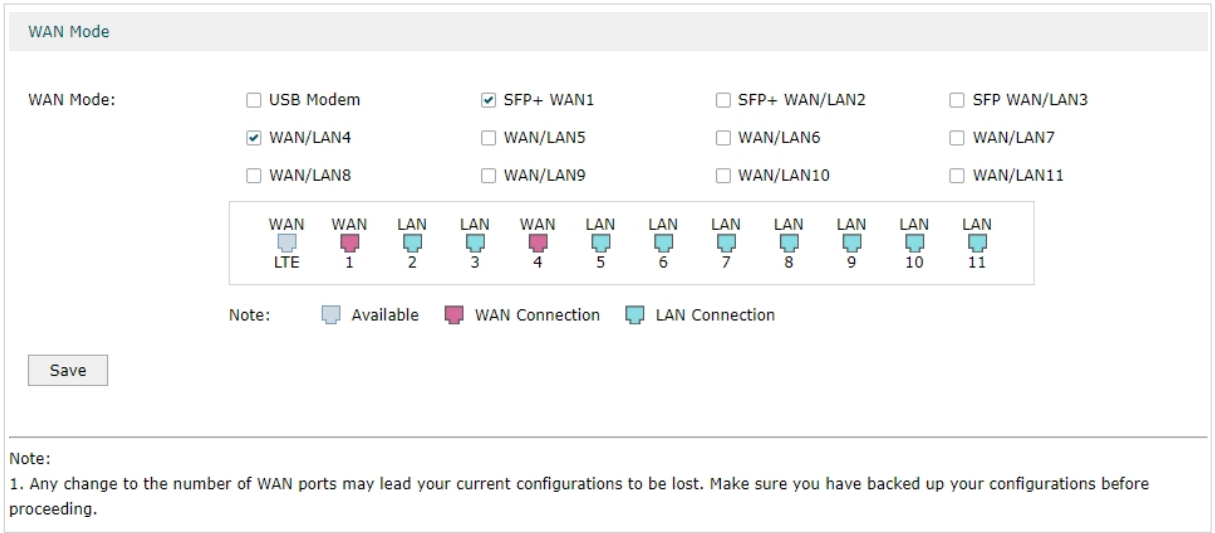
1) WAN 모드에서 필요에 따라 WAN 포트 수를 결정합니다.

2) WAN / SFP WAN 포트에 대한 WAN 연결을 구성합니다.

2.1 WAN 포트 수 구성

네트워크 > **WAN** > **WAN 모드** 메뉴를 **선택하면** 다음 페이지가 로드됩니다.

그림 2-1 WAN 모드 구성하기



WAN 모드	필요에 따라 WAN 포트 수를 결정합니다. 포트를 WAN 포트로 사용하려면 원하는 포트의 확인란을 선택합니다. 여러 개의 WAN 포트를 구성하려면 해당 포트를 활성화합니다. WAN, WAN/LAN, SFP WAN(특정 장치용) 및 USB 모뎀만 WAN 포트로 작동할 수 있습니다.

참고:

WAN 포트 수를 변경하면 현재 구성이 손실될 수 있습니다. 계속 진행하기 전에 구성을 백업했는지 확인하세요.

2.2 WAN 연결 구성

라우터는 5가지 연결 유형을 지원합니다: **고정 IP, 동적 IP, PPPoE, L2TP, PPTP** 중 ISP의 요구사항에 따라 하나를 선택할 수 있습니다.

고정 IP: ISP에서 고정 IP 주소를 제공한 경우 이 유형을 선택합니다. **동적 IP**: ISP가 자동으로 IP 주소를 할당하는 경우 이 유형을 선택합니다. **PPPoE**: ISP에서 PPPoE 계정을 제공한 경우 이 유형을 선택합니다.

L2TP: ISP에서 L2TP 계정을 제공한 경우 이 유형을 선택합니다.

PPTP: ISP에서 PPTP 계정을 제공한 경우 이 유형을 선택합니다.

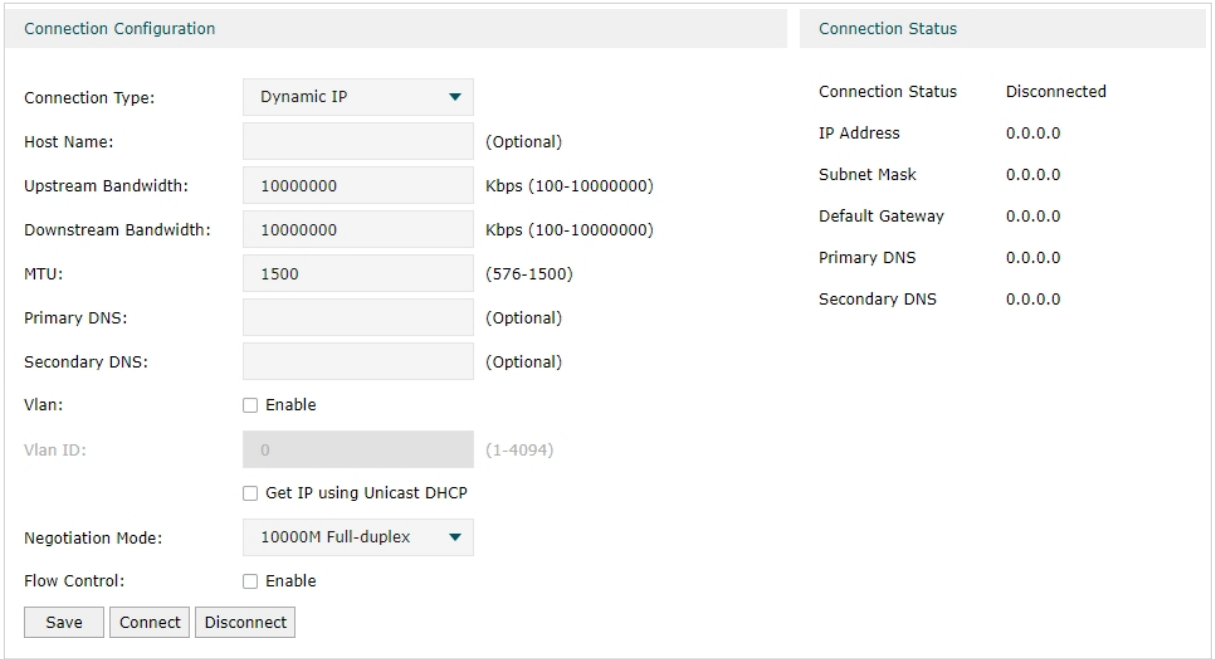
참고:

구성 가능한 WAN 포트의 수는 WAN 모드에 따라 결정됩니다. WAN 모드를 구성하려면 다음을 참조하세요. WAN 포트 수 구성하기.

■ 동적 IP 구성

네트워크 > **WAN** > **SFP+ WAN1** 메뉴를 **선택하면** 다음 페이지가 로드됩니다.

그림 2-2 동적 IP 구성하기



연결 구성 섹션에서 연결 유형을 동적 IP로 선택합니다. 해당 매개 변수를 입력하고 **저장을** 클릭합니다.

연결 유형	ISP가 고정 IP 주소를 제공한 경우 연결 유형을 동적 IP로 선택합니다.
호스트 이름	(선택 사항) 라우터의 이름을 입력합니다. 기본적으로 null입니다.

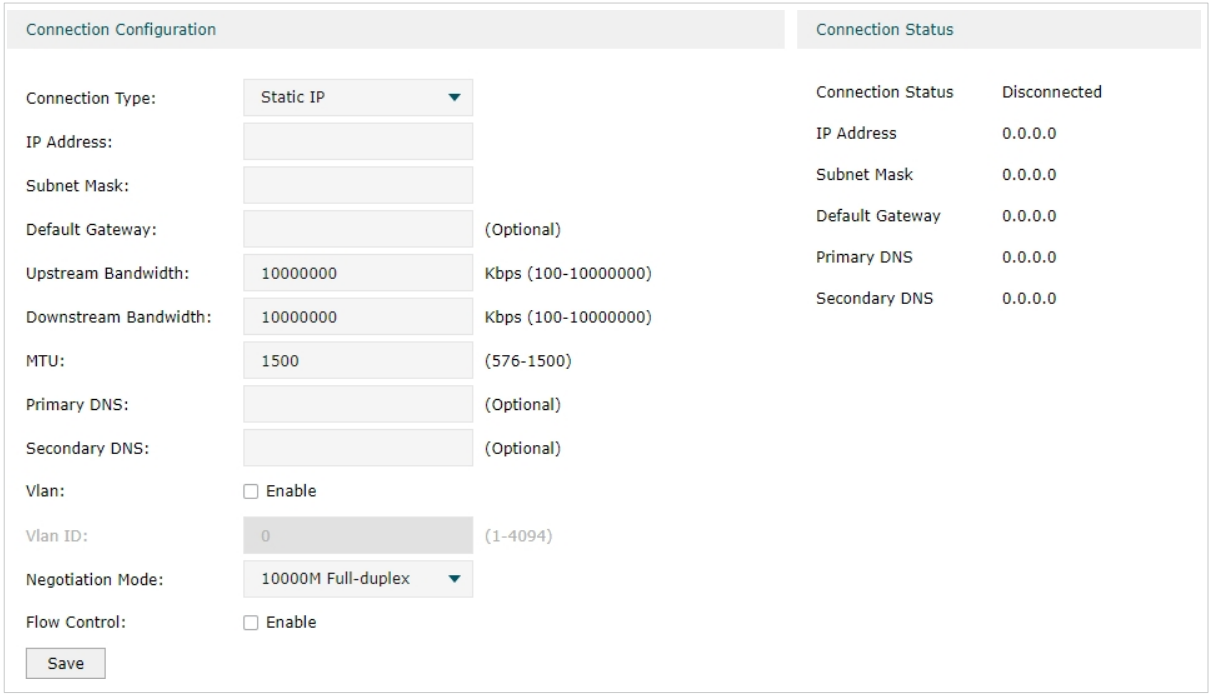
업스트림 대역폭	WAN 포트의 업스트림 대역폭을 지정합니다. 이 값은 **전송 > 대역폭 제어** 페이지의 최대 업스트림 대역폭의 상한입니다. 또한 이 값은 **전송 > 부하 분산 > 기본 설정** 페이지에서 대역폭 기반 균형 라우팅을 활성화한 후 각 WAN 포트의 대역폭 비율을 결정합니다.

다운스트림 대역폭	WAN 포트의 다운스트림 대역폭을 지정합니다. 이 값은 **전송 > 대역폭 제어** 페이지의 최대 다운스트림 대역폭의 상한입니다. 또한 이 값은 **전송 > 부하 분산 > 기본 설정** 페이지에서 대역폭 기반 균형 라우팅을 활성화한 후 각 WAN 포트의 대역폭 비율을 결정합니다.
MTU	WAN 포트의 MTU(최대 전송 단위)를 지정합니다. MTU는 물리적 네트워크에서 전송되는 최대 데이터 단위입니다. 동적 IP를 선택한 경우 MTU는 576~1500바이트 범위에서 설정할 수 있습니다. 기본값은 1500입니다.
기본/보조 DNS	(선택 사항) ISP에서 제공한 DNS 서버의 IP 주소를 입력합니다.
VLAN	WAN 포트를 VLAN에 추가합니다. 일반적으로 ISP에서 요구하지 않는 한 수동으로 구성할 필요가 없습니다.
VLAN ID	WAN 포트에 대한 VLAN이 활성화된 경우 VLAN ID를 입력해야 합니다. 그러면 WAN 포트가 자동으로 VLAN에 할당됩니다. 기본적으로 VLAN의 송신 규칙은 UNTAG이므로 패킷은 VLAN 태그 없이 WAN 포트를 통해 전송됩니다. WAN 포트가 VLAN 태그가 있는 패킷을 전송하도록 하려면 송신 규칙을 TAG로 구성해야 합니다. VLAN을 구성하려면 **네트워크 > VLAN > VLAN으로** 이동합니다.
유니캐스트 DHCP를 사용하여 IP 얻기	일부 ISP에서는 브로드캐스팅 요구 사항을 지원하지 않을 수 있습니다. 일반적인 DHCP 프로세스에서 ISP로부터 IP 주소를 얻을 수 없는 경우 이 옵션을 선택합니다. 이 옵션은 일반적으로 필요하지 않습니다.
협상 모드	이 포트의 속도 모드를 지정합니다.
흐름 제어	흐름 제어 기능을 활성화하려면 확인란을 선택합니다. 흐름 제어는 수신자에게 과부하가 걸리지 않도록 발신자의 데이터 전송을 관리하는 프로세스입니다.
연결/연결 해제	버튼을 클릭하여 연결을 활성화/종료합니다.

■ 고정 IP 구성

네트워크 > WAN > SFP+ WAN1 메뉴를 **선택하면** 다음 페이지가 로드됩니다.

그림 2-3 고정 IP 구성하기



연결 구성 섹션에서 연결 유형을 고정 IP로 선택합니다. 해당 매개 변수를 입력하고 **저장을** 클릭합니다.

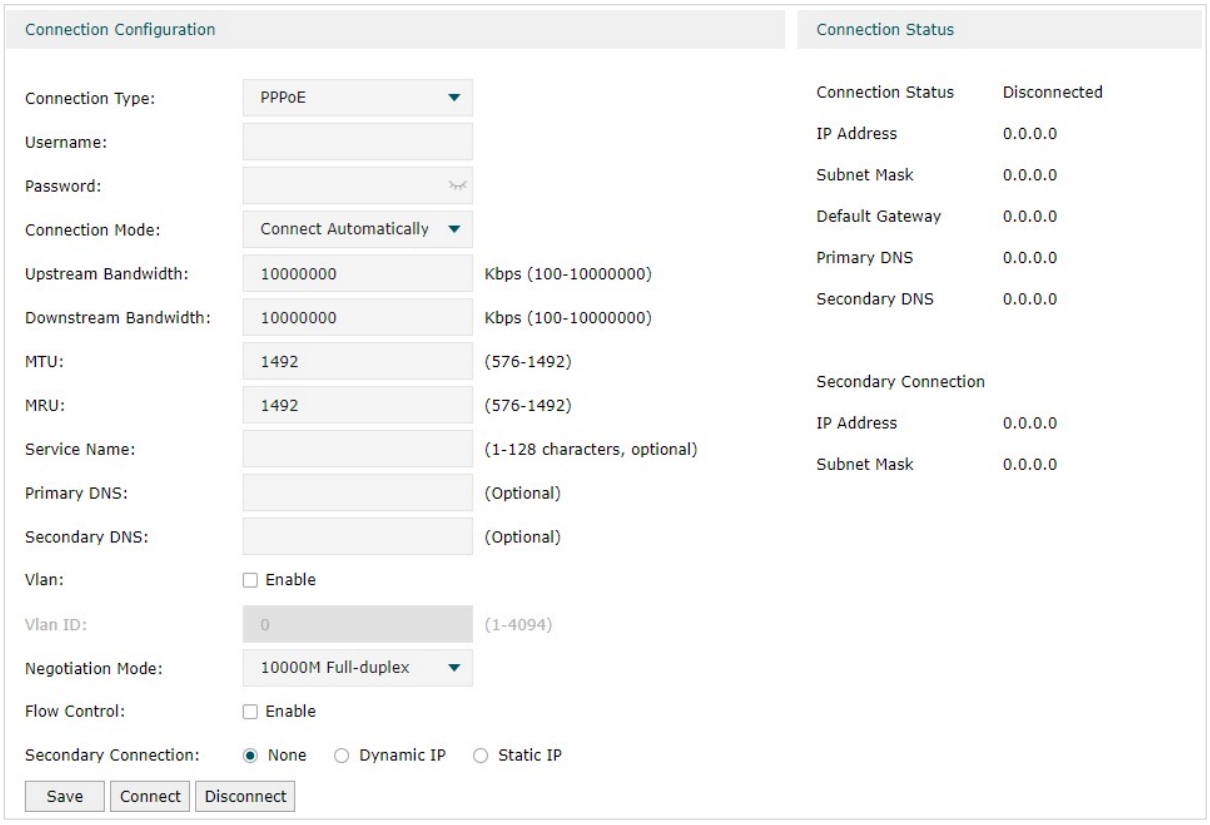
연결 유형	ISP가 고정 IP 주소를 제공한 경우 연결 유형을 고정 IP로 선택합니다.
IP 주소	ISP에서 제공한 IP 주소를 입력합니다. 서브넷 마
스크	ISP에서 제공한 서브넷 마스크를 입력합니다. 기
본 게이트웨이ISP에서 제공한 기본 게이트웨이를 입력합니다.	
업스트림 대역폭	WAN 포트의 업스트림 대역폭을 지정합니다. 이 값은 **전송 > 대역폭 제어** 페이지의 최대 업스트림 대역폭의 상한입니다. 또한 이 값은 **전송 > 부하 분산 > 기본 설정** 페이지에서 대역폭 기반 균형 라우팅을 활성화한 후 각 WAN 포트의 대역폭 비율을 결정합니다.
다운스트림 대역폭	WAN 포트의 다운스트림 대역폭을 지정합니다. 이 값은 **전송 > 대역폭 제어** 페이지의 최대 다운스트림 대역폭의 상한입니다. 또한 이 값은 **전송 > 부하 분산 > 기본 설정** 페이지에서 대역폭 기반 균형 라우팅을 활성화한 후 각 WAN 포트의 대역폭 비율을 결정합니다.
MTU	WAN 포트의 MTU(최대 전송 단위)를 지정합니다. MTU는 물리적 네트워크에서 전송되는 최대 데이터 단위입니다. 고정 IP를 선택한 경우 MTU는 576~1500바이트 범위에서 설정할 수 있습니다. 기본값은 1500입니다.

기본/보조 DNS	(선택 사항) ISP에서 제공한 DNS 서버의 IP 주소를 입력합니다.
VLAN	WAN 포트를 VLAN에 추가합니다. 일반적으로 ISP에서 요구하지 않는 한 일반적으로 WAN 포트에 대해 VLAN을 사용하도록 설정할 필요가 없습니다.
VLAN ID	WAN 포트에 대한 VLAN이 활성화된 경우 VLAN ID를 입력해야 합니다. 그러면 WAN 포트가 자동으로 VLAN에 할당됩니다. 기본적으로 VLAN의 송신 규칙은 UNTAG이므로 패킷은 VLAN 태그 없이 WAN 포트를 통해 전송됩니다. WAN 포트가 VLAN 태그가 있는 패킷을 전송하도록 하려면 송신 규칙을 TAG로 구성해야 합니다. VLAN을 구성하려면 **네트워크 > VLAN > VLAN으로** 이동합니다.
협상 모드	이 포트의 속도 모드를 지정합니다.
흐름 제어	흐름 제어 기능을 활성화하려면 확인란을 선택합니다. 흐름 제어는 수신자에게 과부하가 걸리지 않도록 발신자의 데이터 전송을 관리하는 프로세스입니다.

■ PPPoE 구성

네트워크 > WAN > SFP+ WAN1 메뉴를 **선택하면** 다음 페이지가 로드됩니다.

그림 2-4 PPPoE 구성하기



연결 구성 섹션에서 연결 유형을 PPPoE로 선택합니다. 해당 매개변수를 입력하고 **저장을** 클릭합니다.

연결 유형	ISP에서 PPPoE 계정을 제공한 경우 연결 유형을 PPPoE로 선택합니다.
사용자 이름	ISP에서 제공한 PPPoE 사용자 이름을 입력합니다.
비밀번호	ISP에서 제공한 PPPoE 비밀번호를 입력합니다.
연결 모드	**자동 연결**, **수동 연결** 등 연결 모드를 선택합니다. 및 **시간 기반.** **자동 연결: 라우터가** 재부팅되거나 연결이 끊어지면 라우터가 자동으로 연결을 활성화합니다. **수동으로 연결:** 수동으로 연결을 활성화하거나 종료할 수 있습니다. **시간 기반:** 지정된 기간 동안 라우터가 자동으로 연결을 활성화합니다.
시간	자동 연결할 시간 범위를 선택합니다. 시간 범위를 만들려면 다음으로 이동합니다. **환경설정** > **시간 범위 > 시간 범위를 선택합니다**.
업스트림 대역폭	WAN 포트의 업스트림 대역폭을 지정합니다. 이 값은 **전송 > 대역폭 제어** 페이지의 최대 업스트림 대역폭의 상한입니다. 또한 이 값은 **전송 > 부하 분산 > 기본 설정** 페이지에서 대역폭 기반 균형 라우팅을 활성화한 후 각 WAN 포트의 대역폭 비율을 결정합니다.
다운스트림 대역폭	WAN 포트의 다운스트림 대역폭을 지정합니다. 이 값은 **전송 > 대역폭 제어** 페이지의 최대 다운스트림 대역폭의 상한입니다. 또한 이 값은 **전송 > 부하 분산 > 기본 설정** 페이지에서 대역폭 기반 균형 라우팅을 활성화한 후 각 WAN 포트의 대역폭 비율을 결정합니다.
MTU	WAN 포트의 MTU(최대 전송 단위)를 지정합니다. MTU는 물리적 네트워크에서 전송되는 최대 데이터 단위입니다. PPPoE를 선택한 경우 MTU는 576-1492바이트 범위에서 설정할 수 있습니다. 기본값은 1492입니다.
MRU	WAN 포트의 MRU(최대 수신 단위)를 지정합니다. MRU는 라우터가 네트워크에 있는 컴퓨터가 수신할 수 있는 최대 패킷 크기입니다. PPPoE를 선택한 경우 MRU는 576-1492바이트 범위에서 설정할 수 있습니다. 기본값은 1492입니다.
서비스 이름	(선택 사항) 서비스 이름을 입력합니다. 이 매개 변수는 ISP에서 제공하지 않는 한 필요하지 않습니다. 기본적으로 null입니다.
기본/보조 DNS	(선택 사항) ISP에서 제공한 DNS 서버의 IP 주소를 입력합니다.

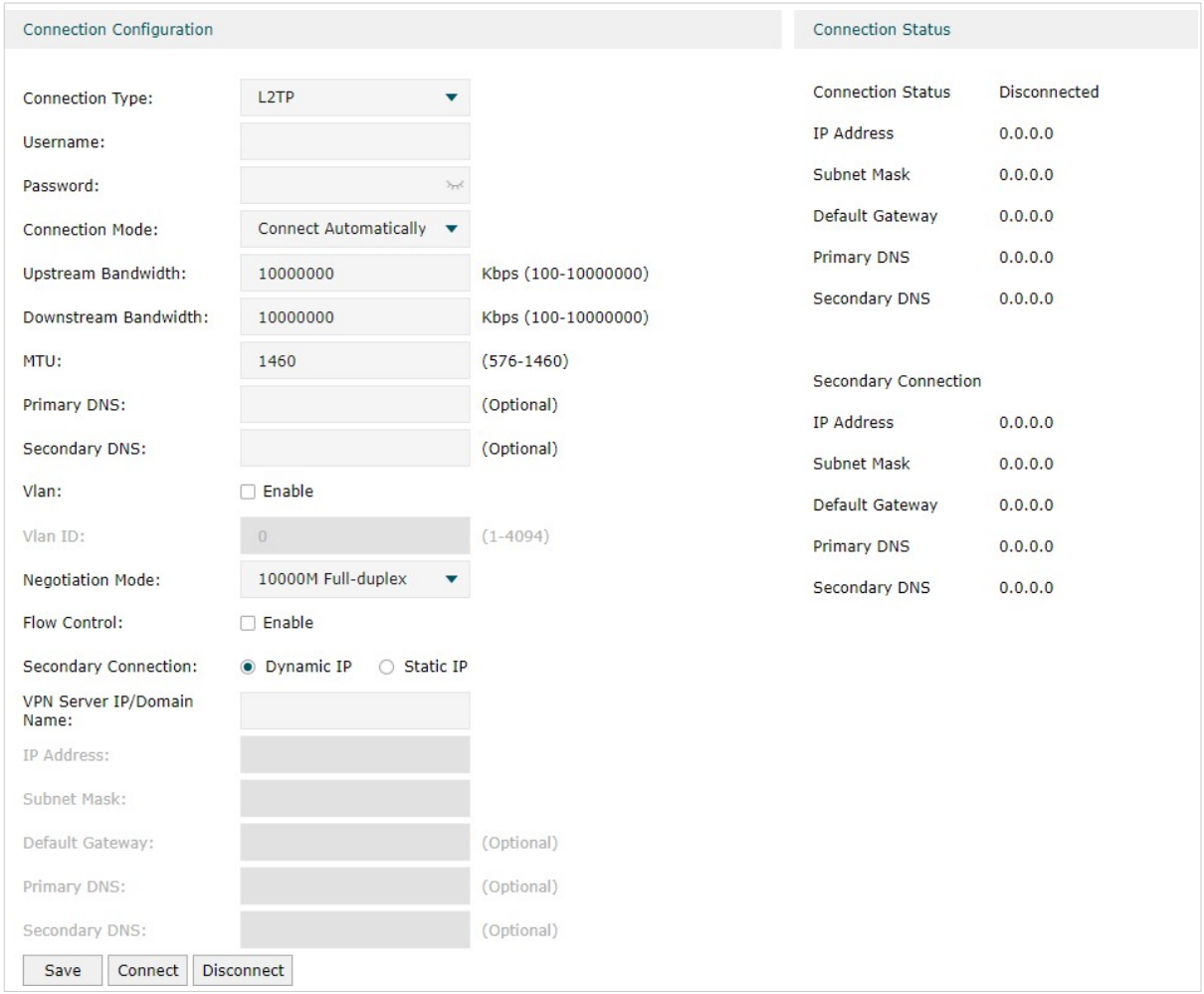
VLAN	WAN 포트를 VLAN에 추가합니다. 일반적으로 ISP에서 요구하지 않는 한 일반적으로 WAN 포트에 대해 VLAN을 사용하도록 설정할 필요가 없습니다.

VLAN ID	WAN 포트에 대한 VLAN이 활성화된 경우 VLAN ID를 입력해야 합니다. 그러면 WAN 포트가 자동으로 VLAN에 할당됩니다. 기본적으로 VLAN의 송신 규칙은 UNTAG이므로 패킷은 VLAN 태그 없이 WAN 포트를 통해 전송됩니다. WAN 포트가 VLAN 태그가 있는 패킷을 전송하도록 하려면 송신 규칙을 TAG로 구성해야 합니다. VLAN을 구성하려면 **네트워크 > VLAN > VLAN으로** 이동합니다.
협상 모드	이 포트의 속도 모드를 지정합니다.
흐름 제어	흐름 제어 기능을 활성화하려면 확인란을 선택합니다. 흐름 제어는 수신자에게 과부하가 걸리지 않도록 발신자의 데이터 전송을 관리하는 프로세스입니다.
보조 연결	일부 ISP에서는 보조 연결이 필요합니다. ISP에서 요구하는 연결 유형을 선택합니다. 없음**:** ISP에서 보조 연결이 필요하지 않은 경우 이 옵션을 선택합니다. **동적 IP:** ISP에서 보조 연결에 대한 IP 주소와 서브넷 마스크를 자동으로 할당하는 경우 이 옵션을 선택합니다. **고정 IP:** ISP에서 보조 연결을 위한 고정 IP 주소와 서브넷 마스크를 제공한 경우 이 옵션을 선택합니다.
연결/연결 해제	버튼을 클릭하여 연결을 활성화/종료합니다.

■ L2TP 구성

네트워크 > **WAN** > **SFP+ WAN1** 메뉴를 **선택하면** 다음 페이지가 로드됩니다.

그림 2-5 L2TP 구성하기



연결 구성 섹션에서 연결 유형을 L2TP로 선택합니다. 해당 매개 변수를 입력하고 **저장을** 클릭합니다.

연결 유형ISP에서 L2TP 계정을 제공한 경우 연결 유형을 L2TP로 선택합니다. 사용자 이름	ISP에서 제공한
L2TP 사용자 아이디를 입력합니다.	
비밀번호	ISP에서 제공한 L2TP 비밀번호를 입력합니다.
연결 모드	**자동 연결**, **수동 연결** 등 연결 모드를 선택합니다. 및 **시간 기반.** **자동 연결: 라우터가** 재부팅되거나 연결이 끊어지면 라우터가 자동으로 연결을 활성화합니다. **수동으로 연결:** 수동으로 연결을 활성화하거나 종료할 수 있습니다.

시간 기반: 지정된 기간 동안 라우터가 자동으로 연결을 활성화합니다.

시간	자동 연결할 시간 범위를 선택합니다. 시간 범위를 만들려면 다음으로 이동합니다. **환경설정 > 시간 범위 > 시간 범위를 선택합니다**.
업스트림 대역폭	WAN 포트의 업스트림 대역폭을 지정합니다. 이 값은 **전송 > 대역폭 제어** 페이지의 최대 업스트림 대역폭의 상한입니다. 또한 이 값은 **전송 > 부하 분산 > 기본 설정** 페이지에서 대역폭 기반 균형 라우팅을 활성화한 후 각 WAN 포트의 대역폭 비율을 결정합니다.
다운스트림 대역폭	WAN 포트의 다운스트림 대역폭을 지정합니다. 이 값은 **전송 > 대역폭 제어** 페이지의 최대 다운스트림 대역폭의 상한입니다. 또한 이 값은 **전송 > 부하 분산 > 기본 설정** 페이지에서 대역폭 기반 균형 라우팅을 활성화한 후 각 WAN 포트의 대역폭 비율을 결정합니다.
MTU	WAN 포트의 MTU(최대 전송 단위)를 지정합니다. MTU는 물리적 네트워크에서 전송되는 최대 데이터 단위입니다. L2TP를 선택한 경우 MTU는 576~1460바이트 범위에서 설정할 수 있습니다. 기본값은 1460입니다.
기본/보조 DNS	(선택 사항) ISP에서 제공한 DNS 서버의 IP 주소를 입력합니다.
VLAN	WAN 포트를 VLAN에 추가합니다. 일반적으로 ISP에서 요구하지 않는 한 일반적으로 WAN 포트에 대해 VLAN을 사용하도록 설정할 필요가 없습니다.
VLAN ID	WAN 포트에 대한 VLAN이 활성화된 경우 VLAN ID를 입력해야 합니다. 그러면 WAN 포트가 자동으로 VLAN에 할당됩니다. 기본적으로 VLAN의 송신 규칙은 UNTAG이므로 패킷은 VLAN 태그 없이 WAN 포트를 통해 전송됩니다. WAN 포트가 VLAN 태그가 있는 패킷을 전송하도록 하려면 송신 규칙을 TAG로 구성해야 합니다. VLAN을 구성하려면 **네트워크 > VLAN > VLAN으로** 이동합니다.
협상 모드	이 포트의 속도 모드를 지정합니다.
흐름 제어	흐름 제어 기능을 활성화하려면 확인란을 선택합니다. 흐름 제어는 수신자에게 과부하가 걸리지 않도록 발신자의 데이터 전송을 관리하는 프로세스입니다.
보조 연결	ISP의 요구 사항에 따라 보조 연결 유형을 선택합니다. 보조 연결은 L2TP 연결에 필요합니다. 보조 연결이 성공하면 라우터는 몇 가지 필요한 정보를 얻습니다. 이 정보는 L2TP 연결 과정에서 사용됩니다. **동적 IP:** 보조 연결 유형을 동적 IP로 선택하면 라우터가 보조 연결을 동적으로 설정합니다.

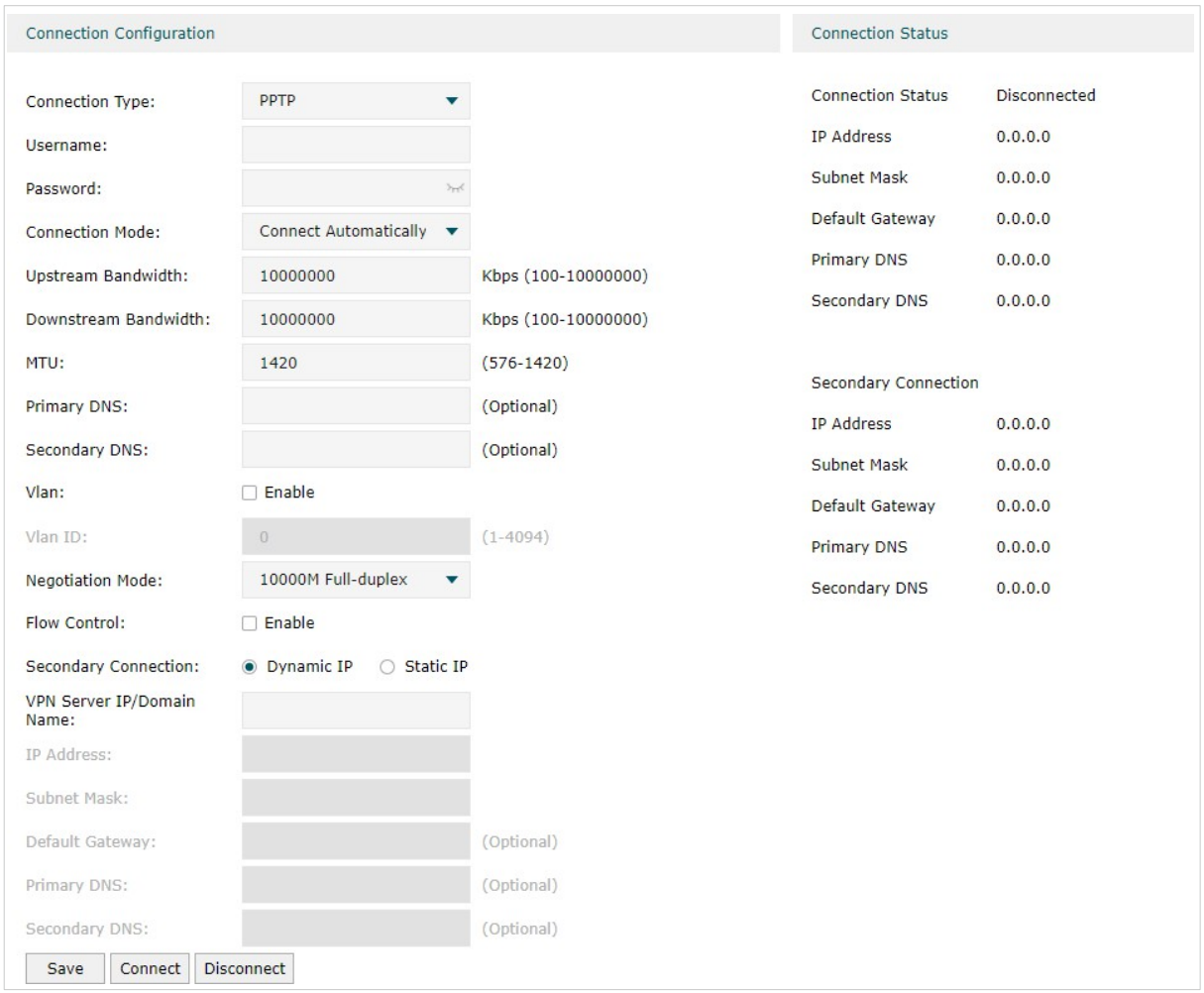
고정 IP:		보조 연결 유형을 고정 IP로 선택한 경우 보조 연결에 대한 IP 주소, 서브넷 마스크, 기본 게이트웨이, 기본/보조 DNS를 구성해야 합니다.
	VPN 서버/ 도메인 이름	ISP에서 제공한 VPN 서버/도메인 이름을 입력합니다.
	IP 주소	보조 연결을 위해 ISP에서 제공한 IP 주소를 입력합니다.

서브넷 마스크	보조 연결에 대해 ISP에서 제공한 서브넷 마스크를 입력합니다. 기본 게이트웨이
	ISP에서 제공하는 보조 연결용 기본 게이트웨이를 입력합니다.
기본/보조 DNS	보조 연결을 위해 ISP에서 제공한 기본/보조 DNS를 입력합니다.
연결/연결 해제	버튼을 클릭하여 연결을 활성화/종료합니다.

■ PPTP 구성

네트워크 > **WAN** > **SFP+ WAN1** 메뉴를 **선택하면** 다음 페이지가 로드됩니다.

그림 2-6 PPTP 구성하기



연결 구성 섹션에서 연결 유형을 PPTP로 선택합니다. 해당 매개변수를 입력하고 **저장을** 클릭합니다.

연결 유형	ISP에서 PPTP 계정을 제공한 경우 연결 유형을 PPTP로 선택합니다.
사용자 이름	ISP에서 제공한 PPTP 사용자 아이디를 입력합니다.

비밀번호	ISP에서 제공한 PPTP 비밀번호를 입력합니다.

연결 모드	**자동 연결**, **수동 연결** 등 연결 모드를 선택합니다. 및 **시간 기반.** **자동 연결: 라우터가** 재부팅되거나 연결이 끊어지면 라우터가 자동으로 연결을 활성화합니다. **수동으로 연결:** 수동으로 연결을 활성화하거나 종료할 수 있습니다. **시간 기반:** 지정된 기간 동안 라우터가 자동으로 연결을 활성화합니다.
시간	자동 연결할 시간 범위를 선택합니다. 시간 범위를 만들려면 다음으로 이동합니다. **환경설정** > **시간 범위 > 시간 범위를 선택합니다**.
업스트림 대역폭	WAN 포트의 업스트림 대역폭을 지정합니다. 이 값은 **전송 > 대역폭 제어** 페이지의 최대 업스트림 대역폭의 상한입니다. 또한 이 값은 **전송 > 부하 분산 > 기본 설정** 페이지에서 대역폭 기반 균형 라우팅을 활성화한 후 각 WAN 포트의 대역폭 비율을 결정합니다.
다운스트림 대역폭	WAN 포트의 다운스트림 대역폭을 지정합니다. 이 값은 **전송 > 대역폭 제어** 페이지의 최대 다운스트림 대역폭의 상한입니다. 또한 이 값은 **전송 > 부하 분산 > 기본 설정** 페이지에서 대역폭 기반 균형 라우팅을 활성화한 후 각 WAN 포트의 대역폭 비율을 결정합니다.
MTU	WAN 포트의 MTU(최대 전송 단위)를 지정합니다. MTU는 물리적 네트워크에서 전송되는 최대 데이터 단위입니다. PPTP를 선택한 경우 MTU는 576~1420바이트 범위에서 설정할 수 있습니다. 기본값은 1420입니다.
기본/보조 DNS	(선택 사항) ISP에서 제공한 DNS 서버의 IP 주소를 입력합니다.
VLAN	WAN 포트를 VLAN에 추가합니다. 일반적으로 ISP에서 요구하지 않는 한 WAN 포트에 대해 VLAN을 사용하도록 설정할 필요는 없습니다.
VLAN ID	WAN 포트에 대한 VLAN이 활성화된 경우 VLAN ID를 입력해야 합니다. 그러면 WAN 포트가 자동으로 VLAN에 할당됩니다. 기본적으로 VLAN의 송신 규칙은 UNTAG이므로 패킷은 VLAN 태그 없이 WAN 포트를 통해 전송됩니다. WAN 포트가 VLAN 태그가 있는 패킷을 전송하도록 하려면 송신 규칙을 TAG로 구성해야 합니다. VLAN을 구성하려면 **네트워크 > VLAN > VLAN으로** 이동합니다.
협상 모드	이 포트의 속도 모드를 지정합니다.
흐름 제어	흐름 제어 기능을 활성화하려면 확인란을 선택합니다. 흐름 제어는 수신자에게 과부하가 걸리지 않도록 발신자의 데이터 전송을 관리하는 프로

세스입니다.

보조 연결	ISP의 요구 사항에 따라 보조 연결 유형을 선택합니다. 보조 연결은 PPTP 연결에 필요합니다. 보조 연결이 성공하면 라우터는 몇 가지 필요한 정보를 얻습니다. 이 정보는 PPTP 연결 프로세스에서 사용됩니다. **동적 IP:** 보조 연결 유형을 동적 IP로 선택하면 라우터가 보조 연결을 동적으로 설정합니다. **고정 IP:** 보조 연결 유형을 고정 IP로 선택한 경우 보조 연결에 대한 IP 주소, 서브넷 마스크, 기본 게이트웨이, 기본/보조 DNS를 구성해야 합니다.
VPN 서버/ 도메인 이름	ISP에서 제공한 VPN 서버/도메인 이름을 입력합니다.
IP 주소	보조 연결을 위해 ISP에서 제공한 IP 주소를 입력합니다. 서브넷 마스크
	보조 연결에 대해 ISP에서 제공한 서브넷 마스크를 입력합니다. 기본 게이트웨이
	ISP에서 제공하는 보조 연결용 기본 게이트웨이를 입력합니다.
기본/보조 DNS	보조 연결을 위해 ISP에서 제공한 기본/보조 DNS를 입력합니다.
연결/연결 해제	버튼을 클릭하여 연결을 활성화/종료합니다.

3 L AN 구성

LAN 포트는 LAN 클라이언트에 연결하는 데 사용되며, 이러한 클라이언트의 기본 게이트웨이로 작동합니다. LAN 클라이언트에 대한 DHCP 서버를 구성할 수 있으며, IP 주소 획득 방법이 '자동으로 IP 주소 획득'으로 설정되어 있으면 클라이언트에 자동으로 IP 주소가 할당됩니다.

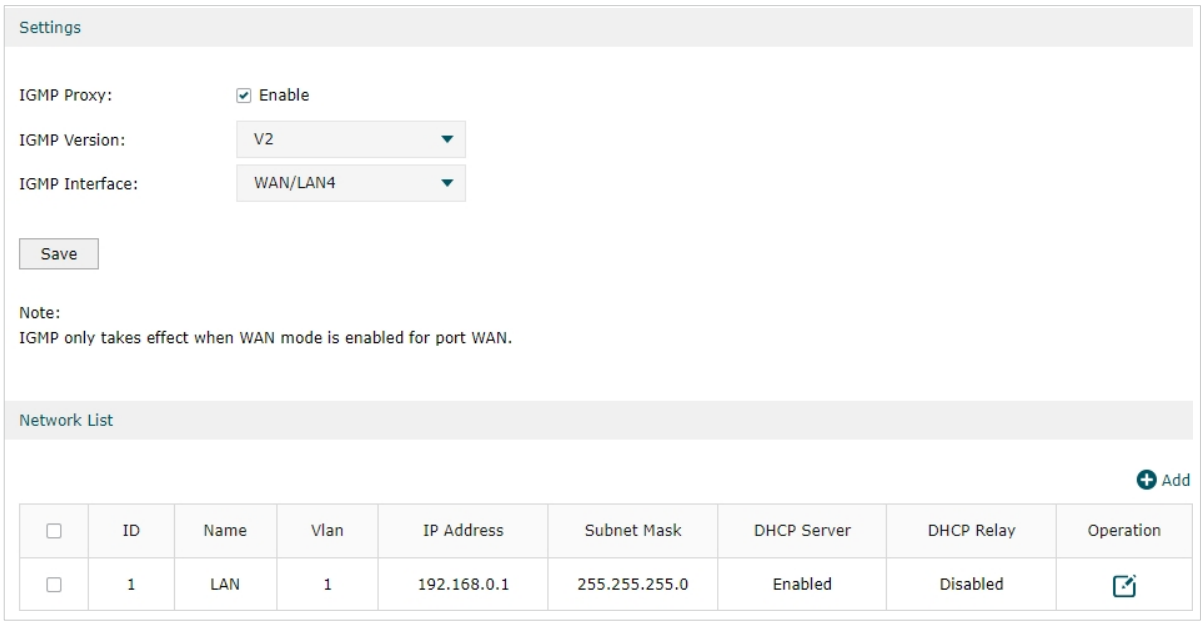
LAN 구성의 경우 가능합니다:

- LAN 포트의 IP 주소를 구성합니다.
- DHCP 서버를 구성합니다.
- 특정 LAN 클라이언트를 위한 IP 주소 예약

3.1 IGMP 프록시 구성

네트워크 > **LAN** > **LAN** 메뉴를 **선택하면** 다음 페이지가 로드됩니다.

그림 3-1 LAN IP 주소 구성하기



설정 섹션에서 IGMP 프록시를 사용하도록 설정하고 해당 매개변수를 선택한 후 다음을 클릭합니다. **저장**.

IGMP 프록시	로컬 네트워크 장치가 인터넷에서 멀티캐스트 데이터를 수신하도록 하려면 이 확인란을 선

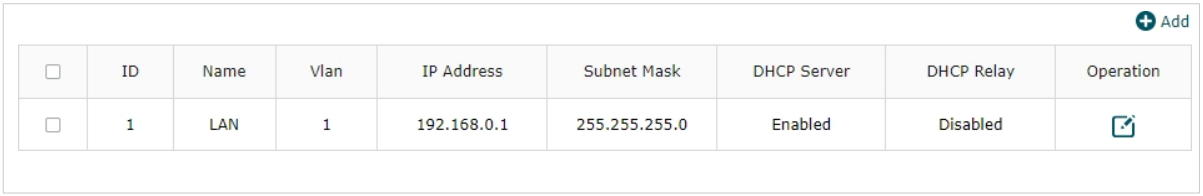
	택하여 IGMP 프록시를 활성화합니다. 이 기능은 LAN 포트에 연결된 멀티캐스트 멤버가 있는지 감지하는 데 사용됩니다.
IGMP 버전	ISP에 따라 IGMP 버전을 V2 또는 V3로 구성합니다.

IGMP 인터페이스	IGMP 프록시가 적용되는 인터페이스를 선택합니다.

참고:

- IGMP는 포트 WAN에 대해 WAN 모드가 활성화된 경우에만 적용됩니다.

그림 3-2 LAN 네트워크 구성하기



네트워크 목록 섹션에서 LAN 네트워크를 설정하거나 추가를 클릭하여 새 네트워크를 추가하고 관련 매개변수를 구성합니다.

이름	을 클릭하여 LAN 네트워크를 설정하거나 추가를 클릭하여 새 네트워크를 추가하고 관련 매개변수를 구성합니다.
IP 주소	LAN 포트의 IP 주소를 입력합니다. 로컬 네트워크 장치를 인터넷에 연결하려면 LAN 포트의 IP 주소를 해당 장치의 기본 게이트웨이로 설정해야 합니다.
서브넷	마스크랜 포트의 서브넷 마스크를 입력합니다(기본값은 255.255.255.0). LAN 포트에 연결되는 모든 장치의 IP 주소는 LAN 포트의 IP 주소와 동일한 서브넷에 있어야 합니다.
VLAN	LAN 포트의 VLAN을 지정하면 지정된 VLAN에 있는 장치만 게이트웨이에 액세스하고 관리할 수 있습니다.

DHCP 모드 -- DHCP 서버

DPCP 서버를 DHCP 모드로 선택하면 게이트웨이의 DHCP 서버가 LAN 클라이언트에 IP 주소를 할당합니다. 다음 매개변수를 구성합니다.

상태: 확인란을 선택하면 DHCP 서버가 활성화됩니다.

시작 IP 주소/끝 IP 주소: DHCP 서버의 IP 풀의 시작 IP 주소와 종료 IP 주소를 입력합니다. IP 풀은 LAN 클라이언트에 할당할 수 있는 IP 주소의 범위를 정의합니다. 시작 IP 주소와 종료 IP 주소는 LAN 포트의 IP 주소와 동일한 서브넷에 있어야 합니다.

임대 시간: DHCP 클라이언트의 임대 시간을 지정합니다. 임대 시간은 클라이언트가 DHCP 서버에서 할당된 IP 주소를 사용할 수 있는 기간을 정의합니다. 일반적으로 클라이언트는 임대가 만료되기 전에 DHCP 서버에 자동으로 임대 시간 연장을 요청합니다. 요청이 실패하면 클라이언트는 임대가 최종적으로 만료되었을 때 해당 IP 주소의 사용을 중지하고 다른 DHCP 서버에서 새 IP 주소를 얻으려고 시도해야 합니다.

기본 게이트웨이: (선택 사항) DHCP 서버에서 할당된 기본 게이트웨이를 입력합니다. LAN 포트의 IP 주소를 입력하는 것이 좋습니다.

기본 도메인: (선택 사항) 네트워크의 도메인 이름을 입력합니다.

기본 DNS/보조 DNS: (선택 사항) ISP에서 제공한 DNS 서버 주소를 입력합니다. 확실하지 않은 경우 ISP에 문의하세요.

옵션60: (선택 사항) DHCP 옵션 60의 값을 입력합니다. DHCP 클라이언트는 이 필드를 사용하여 DHCP 클라이언트의 공급업체 유형 및 구성을 선택적으로 식별합니다. 주로 AP가 필요에 따라 서로 다른 서버에서 서로 다른 IP 주소를 신청하는 시나리오에서 사용됩니다. 자세한 내용은 공급업체에 문의하세요. TP-Link의 경우, 이 항목은 TP-Link여야 합니다.

옵션60: (선택 사항) DHCP 옵션 60의 값을 입력합니다. DHCP 클라이언트는 이 필드를 사용하여 DHCP 클라이언트의 공급업체 유형 및 구성을 선택적으로 식별합니다. 주로 AP가 필요에 따라 서로 다른 서버에서 서로 다른 IP 주소를 신청하는 시나리오에서 사용됩니다. 자세한 내용은 공급업체에 문의하세요. TP-Link의 경우, 이 항목은 TP-Link여야 합니다.

Option138: (선택 사항) DHCP 옵션 138의 값을 입력합니다. 이 값은 Omada 컨트롤러가 장치를 검색할 때 사용됩니다.

옵션150: (선택 사항) DHCP 옵션 150의 값을 입력합니다. 이 옵션은 TFTP 서버 정보를 지정하고 여러 TFTP 서버 IP 주소를 지원합니다.

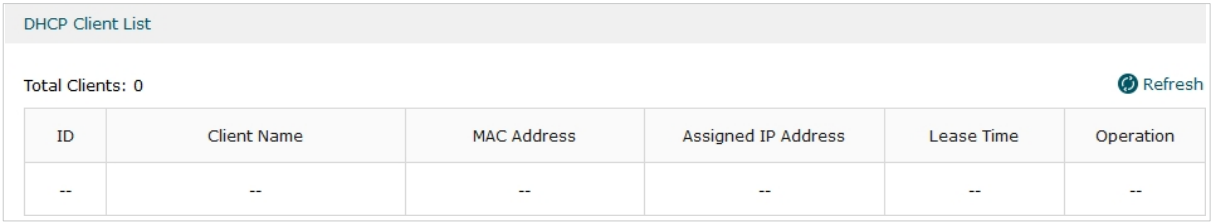
Option159: (선택 사항) DHCP 옵션 159의 값을 입력합니다. 이 옵션은 공유 IPv4 주소에 바인딩된 포트 집합을 구성하는 데 사용됩니다.	**옵션160:** (선택 사항) DHCP 옵션 160의 값을 입력합니다. 이 옵션은 DHCP 캡티브 포털을 구성하는 데 사용됩니다. **Option176:** (선택 사항) DHCP 옵션 176의 값을 입력합니다. 이 옵션은 IP 전화기의 매개변수를 구성하는 데 사용됩니다. **옵션242:** (선택 사항) DHCP 옵션 242의 값을 입력합니다. 이 옵션은 TMS 주소를 자동으로 제공하는 데 사용됩니다.

DHCP 모드 -- DHCP 릴레이	DHCP 릴레이를 DHCP 모드로 선택하면 게이트웨이가 LAN 클라이언트의 DHCP 요청을 다른 네트워크의 DHCP 서버로 릴레이합니다. 그러면 DHCP 서버가 LAN 클라이언트에 IP 주소를 할당합니다. 다음 매개변수를 구성합니다. **상태:** 확인란을 선택하면 DHCP 릴레이가 활성화됩니다. **서버 주소:** DHCP 서버의 IP 주소를 입력합니다.

3.2 DHCP 클라이언트 목록 보기

네트워크 > **LAN** > **DHCP 클라이언트 목록** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 3-3 DHCP 클라이언트 목록 보기



여기에서 DHCP 클라이언트 목록을 볼 수 있습니다.

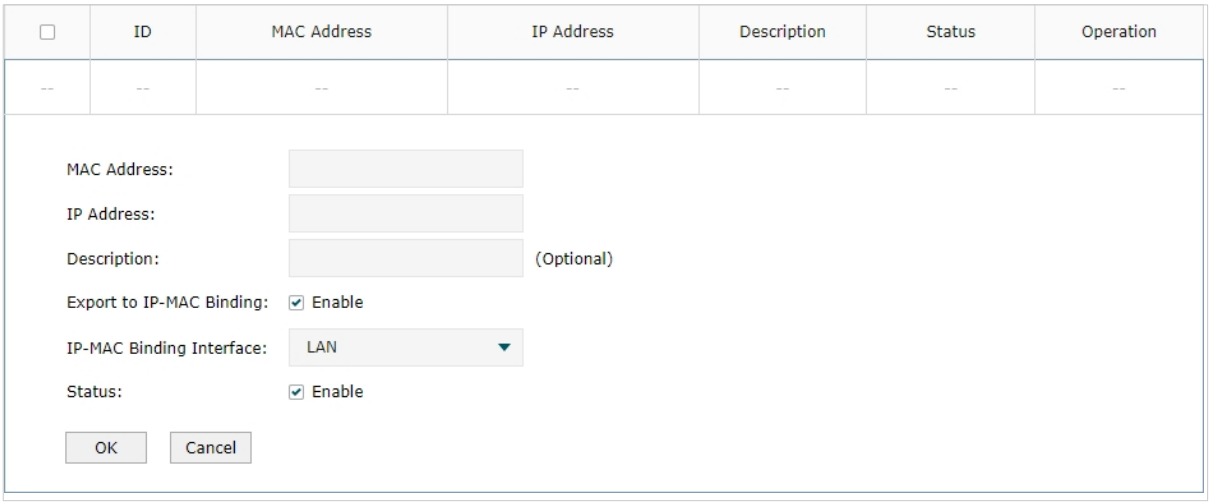
클라이언트 이름	DHCP 클라이언트의 호스트 이름을 표시합니다. 숫자, 영문자, 대시 및 밑줄로만 구성되어야 합니다.
MAC 주소	클라이언트의 MAC 주소를 표시합니다.
할당된 IP 주소	클라이언트에 할당된 IP 주소를 표시합니다.
임대 시간	할당된 IP 주소의 남은 임대 시간을 표시합니다. 임대가 만료되면 IP 주소가 다시 할당됩니다.

3.3 주소 예약 구성

- 주소 예약 구성

네트워크 > **LAN** > **주소 예약** 메뉴를 선택하고 추 가 를 클릭하면 다음 페이지가 로드됩니다.

그림 3-4 주소 예약 구성하기



MAC 주소, IP 주소 등 주소 예약 항목의 매개변수를 구성한 다음 **확인을** 클릭합니다.

MAC 주소	클라이언트의 MAC 주소를 입력합니
다. IP 주소	예약할 IP 주소를 입력합니다.
설명	(선택 사항) 항목에 대한 간단한 설명을 입력합니다. 최대 32자까지 입력할 수 있습니다.
IP로 내보내기- MAC 바인딩	(선택 사항) 이 바인딩 항목을 IP-MAC 바인딩 목록으로 내보내려면 확인란을 선택합니다. **방화벽 > ARP 스푸핑 방지 > IP-MAC 바인딩** 페이지.
상태	이 항목을 활성화하려면 확인란을 선택합니다.

4 IPT V 구성

ISP(인터넷 서비스 제공업체)에서 제공하는 인터넷/IPTV/전화 서비스를 사용하도록 IPTV 설정을 구성합니다.

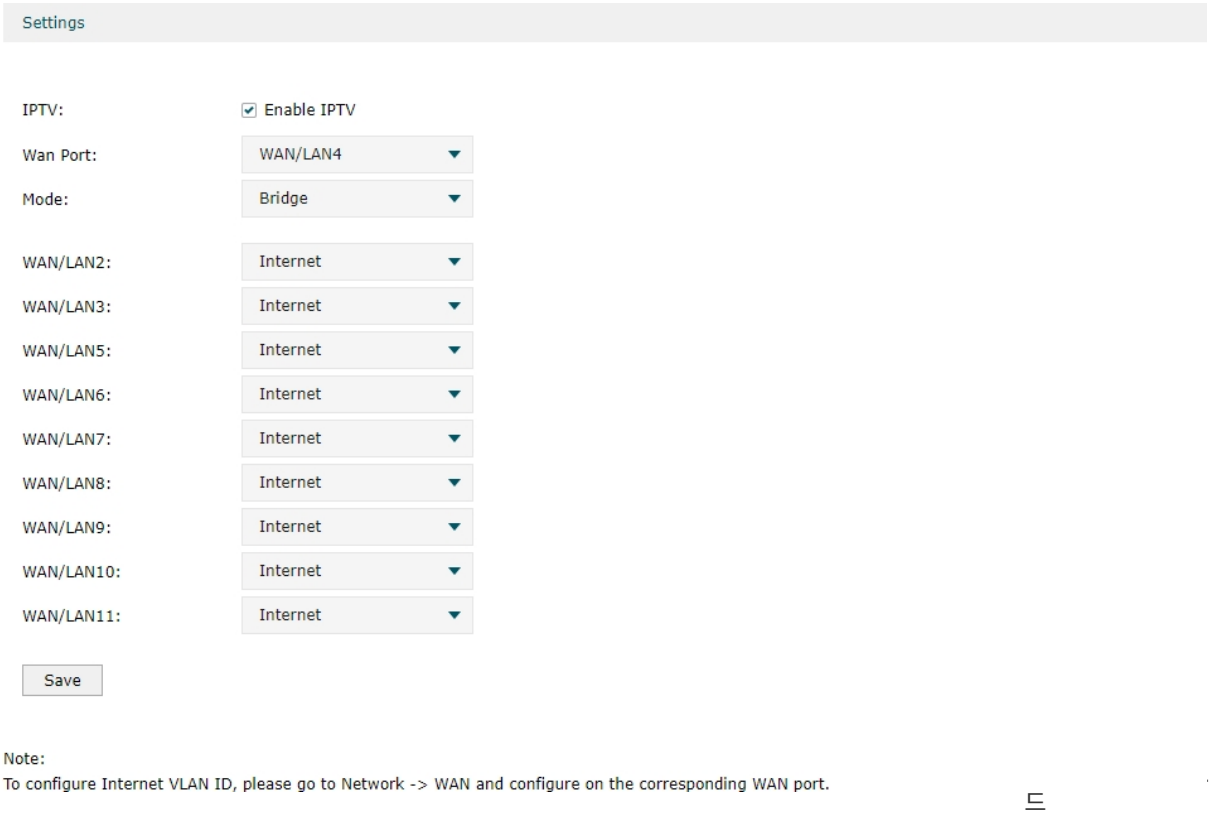
IPTV 구성을 완료하려면 다음 단계를 따르세요.

1) 전 세계에서 IPTV를 사용하도록 설정합니다.
2) ISP에 따라 WAN 포트를 선택합니다.
3) ISP에 따라 적절한 모드를 선택합니다.
4) 포트 모드를 선택하면 IPTV 서비스, IP-전화 서비스 또는 인터넷 서비스를 지원하는 데 사용되는 포트를 결정할 수 있습니다.
5) **저장을** 클릭합니다.

4. 1 IPTV 구성하기

네트워크 > **IPTV** > **IPTV** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 4-1 IPTV 구성하기



드

설정 섹션에서 IPTV를 활성화하고 해당 매개변수를 구성한 다음, 다음을 클릭합니다.

저장.

IPTV	전 세계에서 IPTV를 사용하도록 설정합니다.
완 포트	ISP에 따라 WAN 포트를 선택합니다.
모드	ISP에 따라 적절한 모드를 선택합니다. **브리지**: ISP에서 다른 매개 변수를 요구하지 않는 경우 이 모드를 선택합니다. **사용자 지정**: ISP에서 필요한 매개변수를 제공하는 경우 이 모드를 선택하고 ISP의 요구 사항에 따라 매개변수를 구성합니다.
포트 모드	LAN 포트의 적절한 포트 모드를 선택하여 인터넷 서비스 또는 IPTV 서비스를 지원하는 데 사용되는 포트를 결정합니다.

참고:

인터넷 VLAN ID를 구성하려면 WAN 구성으로 이동하여 해당 WAN 포트에서 구성하세요.

5 MA C 구성

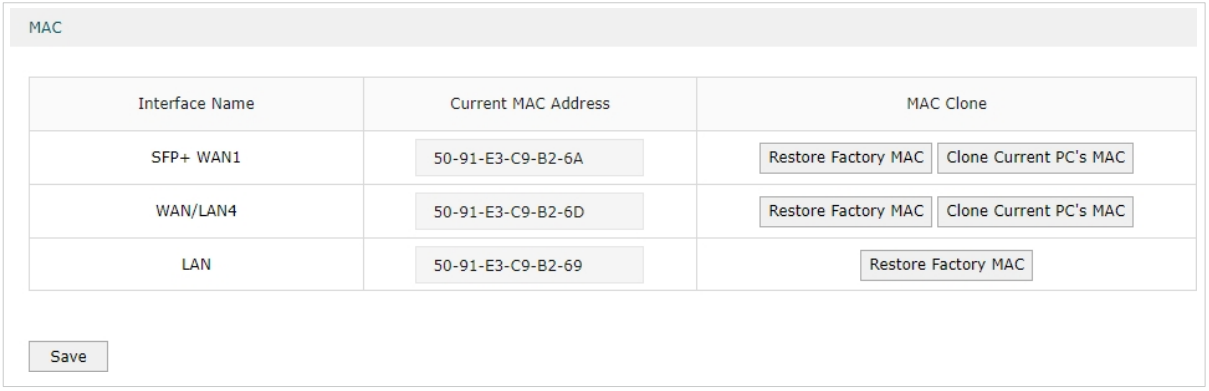
일반적으로 MAC 주소는 변경할 필요가 없습니다. 하지만 다음과 같은 상황에서는 WAN 포트의 MAC 주소를 변경해야 할 수 있습니다.

ISP가 전화 접속 장치의 MAC 주소에 계정을 바인딩한 상태에서 전화 접속 장치를 이 라우터로 교체하려는 경우, 이 라우터의 WAN 포트의 MAC 주소를 이전 전화 접속 장치의 MAC 주소와 동일하게 설정하면 정상적인 인터넷 연결이 가능합니다.

5.1 MAC 주소 구성

네트워크 > **MAC** > **MAC** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 5-1 MAC 주소 구성



필요에 따라 WAN 포트의 MAC 주소를 구성한 다음 **저장을** 클릭합니다.

인터페이스 이름	WAN 포트와 LAN 포트를 표시합니다.
현재 MAC 주소	WAN 포트의 MAC 주소를 구성합니다.
MAC 복제	MAC 클론은 MAC 주소를 변경하는 지름길을 제공합니다. **공장 출하 시 MAC 복원**: 이 버튼을 클릭하면 MAC 주소를 공장 출하 시 기본값으로 복원할 수 있습니다. **현재 PC의 MAC 복제**: 현재 라우터를 구성하는 데 사용 중인 PC의 MAC 주소를 복제하려면 이 버튼을 클릭하세요. WAN 포트에서만 사용할 수 있습니다.

참고:

WAN 포트에서 큐렌트된 관리 호스트의 MAC을 복제할 때는 관리 PC를 LAN 포트에 연결해야 합니다.

WAN 포트의 연결 유형이 PPPoE, L2TP 또는 PPTP인 경우, WAN 포트의 MAC 주소를 변경하면 연결이 종료되거나 다시 설정될 수 있습니다.

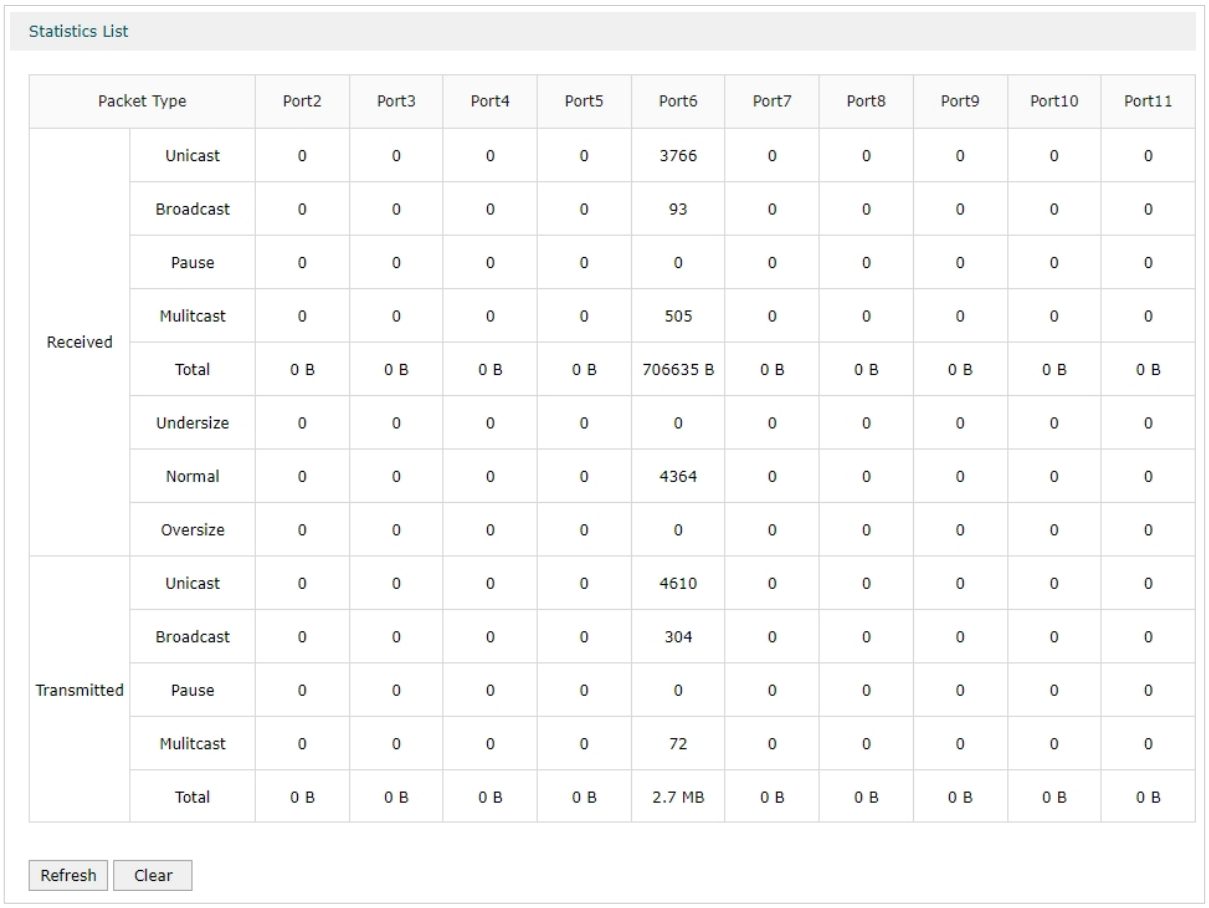
6 S 마녀 구성

라우터는 **통계**, **포트 미러**, **속도 제어**, **포트 구성**, 포트 **상태** 및 **DDM 상태를** 포함한 몇 가지 기본적인 스위치 포트 관리 기능을 제공합니다.

6.1 통계 보기

네트워크 > **스위치** > **통계** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 6-1 통계 보기



각 포트의 자세한 트래픽 정보를 볼 수 있어 트래픽을 모니터링하고 네트워크를 효과적으로 관리할 수 있습니다.

유니캐스트	포트에서 수신 또는 전송된 일반 유니캐스트 패킷의 수를 표시합니다. 브로드캐스트
	포트에서 수신 또는 전송된 일반 브로드캐스트 패킷의 수를 표시합니다. Pause 포트에
서 수신 또는 전송된 흐름 제어 프레임의 수를 표시합니다.	
멀티캐스트	포트에서 수신 또는 전송된 일반 멀티캐스트 패킷의 수를 표시합니다.

총	수신 또는 전송된 패킷의 총 바이트 수(오류 프레임 포함)를 표시합니다.

크기 미만	길이가 64바이트(오류 프레임 포함) 미만인 수신 패킷의 수를 표시합니다.
보통	길이가 64바이트에서 최대 프레임 길이(오류 프레임 포함) 사이인 수신된 패킷 수를 표시합니다.
오버사이즈	최대 프레임 길이(오류 프레임 포함)보다 큰 길이를 가진 수신 패킷 수를 표시합니다.
새로 고침	각 포트의 최신 트래픽 통계를 보려면 새로 고침을 클릭합니다.
지우기	모든 트래픽 통계를 지우려면 지우기를 클릭합니다.

참고:

오류 프레임: 잘못된 체크섬이 있는 프레임입니다.

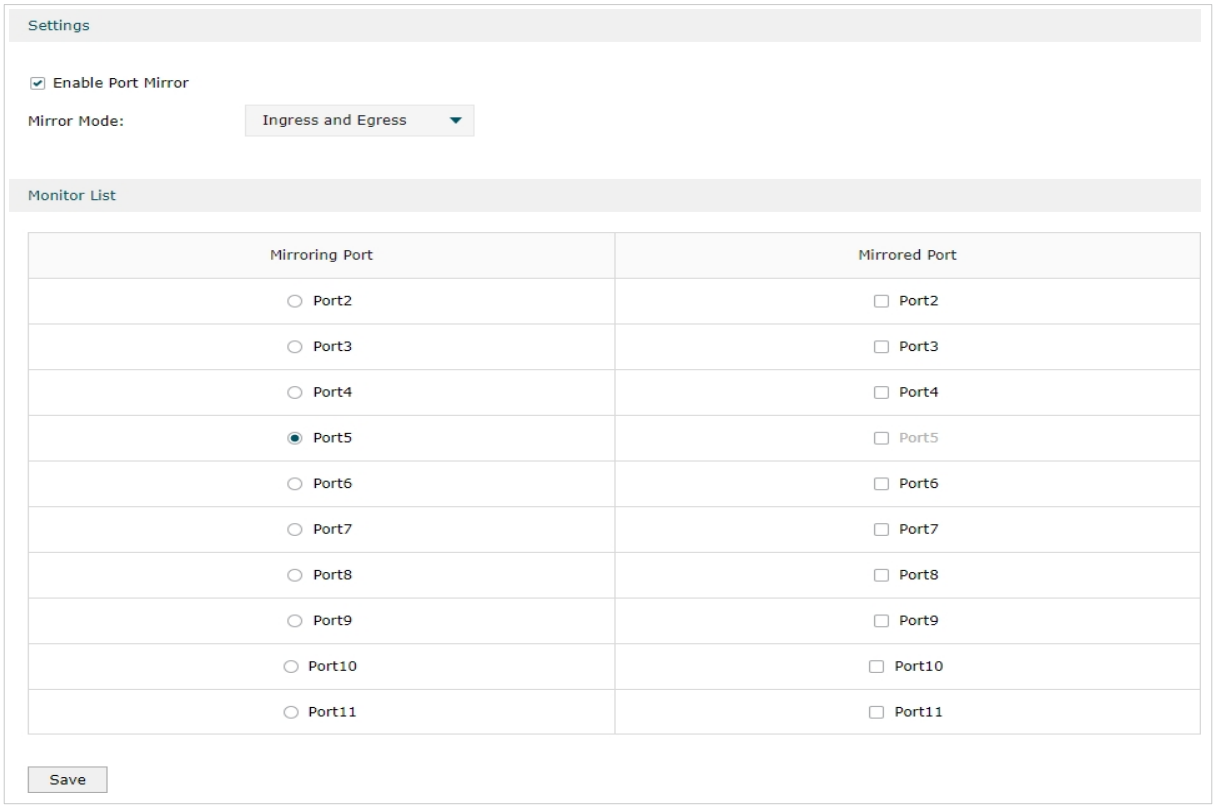
최대 프레임 길이: 라우터에서 지원하는 최대 프레임 길이입니다. 태그가 지정되지 않은 프레임의 경우 1518 바이트, 태그가 지정된 패킷의 경우 1522바이트입니다.

6.2 포트 미러 구성

포트 미러 기능을 사용하면 라우터가 모니터링되는 포트의 패킷 복사본을 특정 모니터링 포트로 전달할 수 있습니다. 그러면 복사된 패킷을 분석하여 네트워크 트래픽을 모니터링하고 네트워크 문제를 해결할 수 있습니다.

네트워크 > **스위치** > **미러** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 6-2 포트 미러 구성


Settings
Enable Port Mirror
Mirror Mode:
Ingress and Egress
Monitor List
Mirroring Port
Mirrored Port
Port2
Port3
Port4
Port5
Port6
Port7
Port8
Port9
Port10
Port11
Save

포트 미러를 구성하려면 다음 단계를 따르세요:

1) **설정** 섹션에서 포트 미러 기능을 활성화하고 미러 모드를 선택합니다.

포트 미러 사용	포트 미러 기능을 활성화하려면 확인란을 선택합니다.
미러 모드	**수신**, **송신** 및 **수신과 송신을** 포함하는 미러 모드를 선택합니다. **인그레스:** 미러링된 포트에서 수신한 패킷이 미러링 포트에 복사됩니다. **송신:** 미러링된 포트에서 보낸 패킷이 미러링 포트에 복사됩니다. **수신 및 송 신 :** 미러링된 포트를 통해 수신 및 발신되는 패킷이 모두 미러링 포트에 복사됩니다.

2) **모니터 목록** 섹션에서 미러링 포트와 미러링된 포트를 설정한 다음 다음을 클릭합니다. **저장**.

미러링 포트	미러링 포트를 통과하는 패킷은 이 포트로 복사됩니다. 일반적으로 미러링 포트는 네트워크 모니터링 및 문제 해결을 위해 미러링된 패킷을 분석하는 데 사용되는 데이터 진단 장치에 연결됩니다.
미러링 포트	이 포트를 통과하는 패킷은 미러링 포트로 복사됩니다. 일반적으로 미러링된 포트가 모니터링 대상 포트입니다.

6.3 속도 제어 구성

속도 제어를 사용하면 각 포트의 특정 패킷에 대한 트래픽 속도 제한을 설정하여 네트워크의 트래픽 흐름을 관리할 수 있습니다.

네트워크 > **스위치** > 속도 **제어** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 6-3 속도 제어 구성

Settings

Port	Ingress Limit	Ingress Frame Type	Ingress Rate(Mbps)	Egress Limit	Egress Rate(Mbps)
Port2	Enable	All Frames	10000	Enable	10000
Port3	Enable	All Frames	1000	Enable	1000
Port4	Enable	All Frames	1000	Enable	1000
Port5	Enable	All Frames	1000	Enable	1000
Port6	Enable	All Frames	1000	Enable	1000
Port7	Enable	All Frames	1000	Enable	1000
Port8	Enable	All Frames	1000	Enable	1000
Port9	Enable	All Frames	1000	Enable	1000
Port10	Enable	All Frames	1000	Enable	1000
Port11	Enable	All Frames	1000	Enable	1000

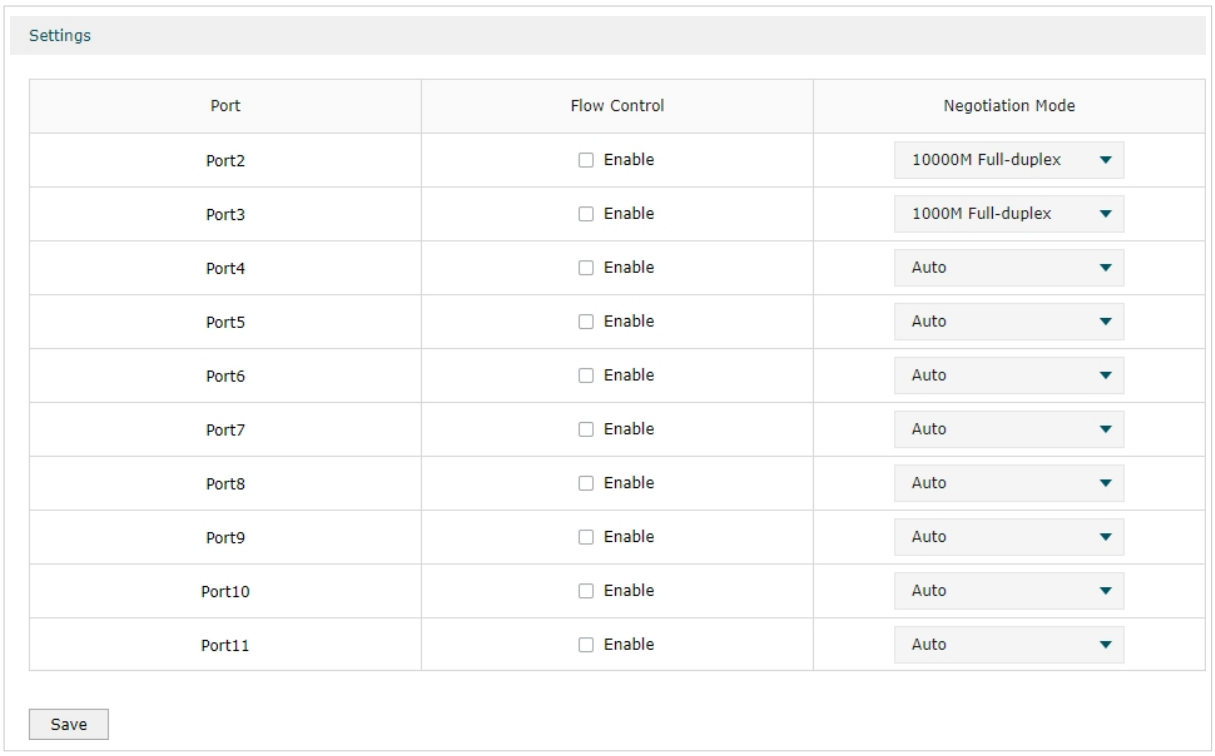
Save

포트를 선택하고 수신 프레임 또는 송신 프레임 제한을 구성한 다음 다음을 클릭합니다. **저장**.

인그레스 제한	인그레스 제한 기능을 활성화하려면 확인란을 선택합니다.
인그레스 프레임 유형	제한할 수신 프레임 유형을 지정합니다. 기본값은 모든 프레임입니다. **모든 프레임**: 모든 프레임의 수신률이 제한됩니다. **브로드캐스트**: 생방송 프레임의 수신률이 제한되어 있습니다. **브로드캐스트 및 멀티캐스트**: 브로드캐스트 및 멀티캐스트 프레임의 수신 속도가 제한됩니다.
인그레스 속도(Mbps)	수신 패킷의 제한 속도를 지정합니다.
송신 제한	송신 제한 기능을 활성화하려면 확인란을 선택합니다.
송신 속도(Mbps)	송신 패킷의 제한 속도를 지정합니다.

6.4 포트 구성 구성

포트의 흐름 제어 및 협상 모드를 구성할 수 있습니다. **네트워크** > **스위치** > **포트 구성** 메뉴를 선택하면 다음 페이지가 로드됩니다. 그림 6-4 흐름 제어 및 협상 구성하기



포트의 흐름 제어 및 협상 모드를 구성합니다.

흐름 제어	흐름 제어 기능을 활성화하려면 확인란을 선택합니다. 흐름 제어는 수신자에게 과부하가 걸리지 않도록 발신자의 데이터 전송을 관리하는 프로세스입니다.
협상 모드	포트의 협상 모드를 선택합니다. 포트 11의 경우 자동(자동 협상)을 선택하거나 속도 및 양면 모드를 수동으로 선택할 수 있습니다.

6.5 포트 상태 보기

네트워크 > 스위치 > 포트 상태 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 6-5 포트 상태 보기

상태	포트 상태를 표시합니다. **링크 다운**: 포트가 연결되지 않았습니다. **연결**: 포트가 정상적으로 작동합니다.
속도(Mbps)	포트 속도를 표시합니다.
양면 모드	포트의 양면 모드를 표시합니다. 흐름 제
어	흐름 제어가 활성화되어 있는지 표시합니

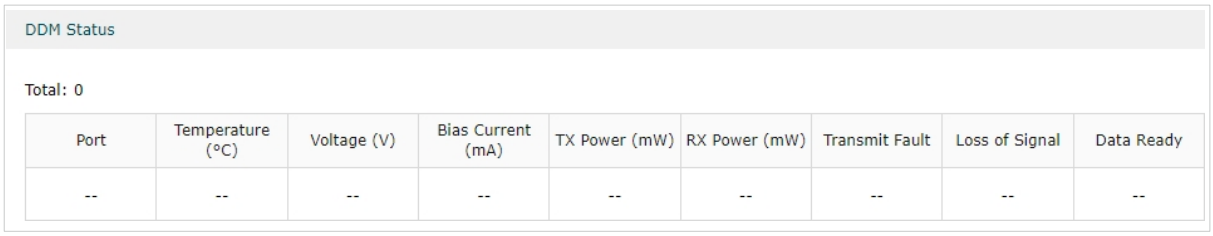
다.

6.6 DDM 상태 보기

DDM(디지털 진단 모니터링) 기능은 스위치의 SFP 포트에 삽입된 SFP 모듈의 상태를 모니터링하는 데 사용됩니다. 사용자는 지정된 매개변수가 알람 임계값 또는 경고 임계값을 초과할 때 모니터링되는 SFP 포트를 자동으로 종료하도록 선택할 수 있습니다. 모니터링되는 매개변수에는 다음이 포함됩니다: 온도, 전압, 바이어스 전류, 송신 전력 및 수신 전력.

네트워크 > **스위치** > **DDM 상태** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 6-6 포트 상태 보기



7 VL AN 구성

VLAN을 사용하면 LAN을 여러 개의 논리적 네트워크로 나누고 편리하고 유연한 방식으로 네트워크 간의 트래픽을 제어할 수 있습니다. LAN은 지리적 위치에 관계없이 부서, 애플리케이션 또는 사용자 유형에 따라 논리적으로 세분화할 수 있습니다.

VLAN 구성의 경우 가능합니다:

- VLAN을 생성하고 원하는 포트를 VLAN에 추가합니다.
- 포트의 PVID를 구성합니다.

7.1 VLAN 만들기

네트워크 > **VLAN** > **VLAN** 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 7-1 VLAN 만들기

VLAN을 생성하고 포트를 VLAN에 추가한 다음 **확인을** 클릭합니다.

VLAN ID	VLAN ID를 입력합니다. 값의 범위는 1에서 4094까지
입니다. 이름	쉽게 식별할 수 있도록 VLAN의 이름을 지정합니다.
포트	확인란을 선택하여 원하는 포트를 VLAN에 추가하고 지정된 VLAN의 포트 유형을 지정합니다. 포트는 두 가지 유형으로 나눌 수 있습니다: 태그 또는 태그 없음. **태그**: 포트에서 전송되는 패킷의 송신 규칙에 태그가 지정됩니다. **UNTAG**: 포트에서 전송되는 패킷의 송신 규칙은 태그가 지정되지 않은 상태입니다. 포트에 연결된 디바이스가 PC나 서버와 같은 최종 디바이스인 경우, 최종 디바이스는 태그가 지정된 패킷을 인식하지 못하므로 포트 유형은 UNTAG이어야 합니다.
설명	(선택 사항) 간편한 관리 및 검색을 위해 간단한 설명을 입력합니다.

VLAN 목록에서 라우터에 존재하는 모든 VLAN을 볼 수 있습니다.

VLAN ID	VLAN ID를 표시합니다.
이름	VLAN 이름을 표시합니다.
포트	해당 VLAN에 속하는 포트를 표시합니다. 설명 VLAN에

대한 설명을 표시합니다.

참고:

VLAN 목록에는 라우터에 존재하는 모든 VLAN이 포함되어 있습니다. 이 중 일부는 사용자가 수동으로 생성하며 편집하거나 삭제할 수 있습니다. 일부는 관리 VLAN과 같은 일부 특수한 시나리오를 위해 라우터에서 자동으로 생성 및 참조되며, 이러한 VLAN은 편집하거나 삭제할 수 없습니다.

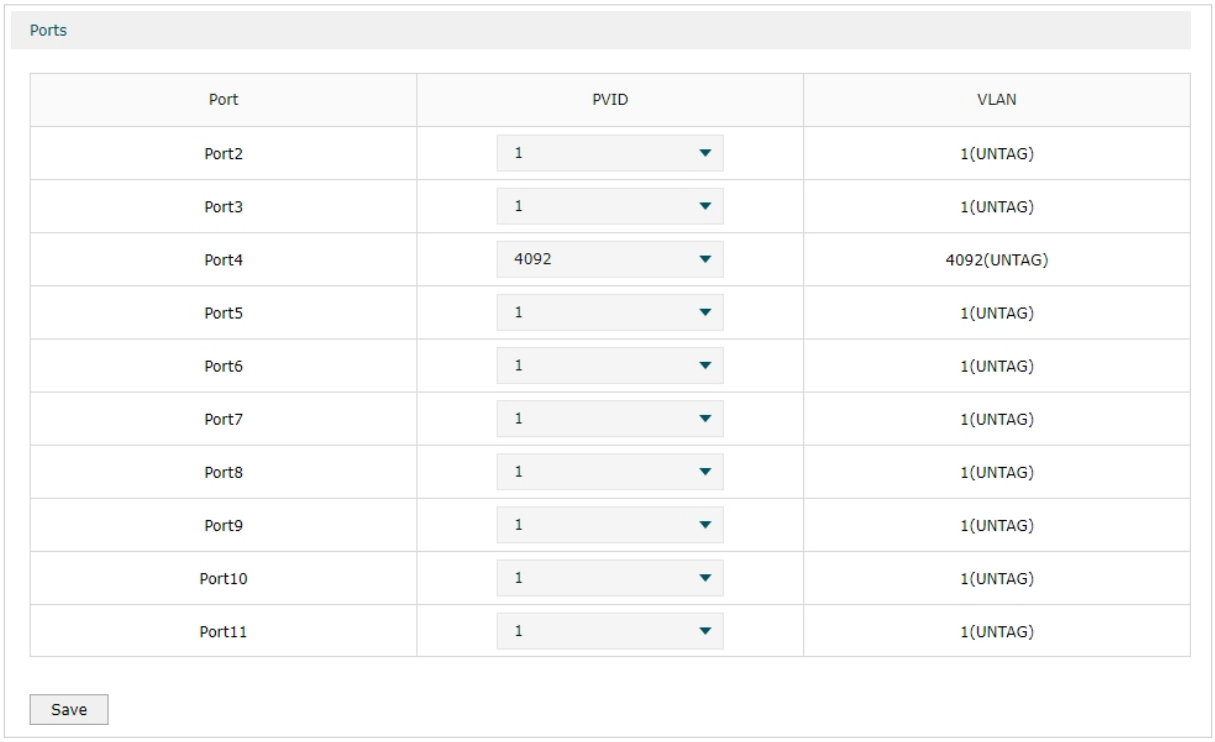
7.2 포트의 PVID 구성

PVID는 해당 포트의 기본 VLAN을 나타냅니다. 포트에서 수신되는 태그가 지정되지 않은 패킷은 PVID로 태그가 지정된 후 해당 VLAN 내에서 전송됩니다.

예를 들어 포트 2가 VLAN 10과 VLAN 20에 모두 있고 포트의 PVID가 10인 경우, 포트 2가 PC에서 태그가 없는 패킷을 수신하면 이 패킷은 VLAN 10 내에서 전송되지만 VLAN 20에 직접 도달할 수 없습니다.

포트의 PVID를 구성하려면 **네트워크** > **VLAN** > **포트** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 7-2 PVID 구성하기



포트의 PVID를 구성한 다음 **저장을** 클릭합니다.

포트	포트를 표시합니다.
PVID	포트의 PVID를 지정합니다. PVID는 해당 포트의 기본 VLAN을 나타냅니다.
VLAN	포트가 속한 VLAN을 표시합니다.

8 IP v6 구성

IPv6는 IPv4의 뒤를 잇는 차세대 네트워크 프로토콜입니다. ISP가 IPv6를 지원하는 경우 라우터에 대해 IPv6 네트워크를 구성할 수 있습니다. IPv6 네트워크는 현재 사용 중인 IPv4 네트워크와 충돌을 일으키지 않습니다.

IPv6 네트워크를 구성하려면 가이드라인을 따르세요:

- LAN에 IPv6를 구성합니다.
- WAN/SFP WAN 포트에 대해 IPv6를 구성합니다. 여러 WAN에 대해 IPv6를 구성할 수 있으며, 각 WAN 포트에는 고유한 인터넷 연결 유형과 매개변수가 있습니다.

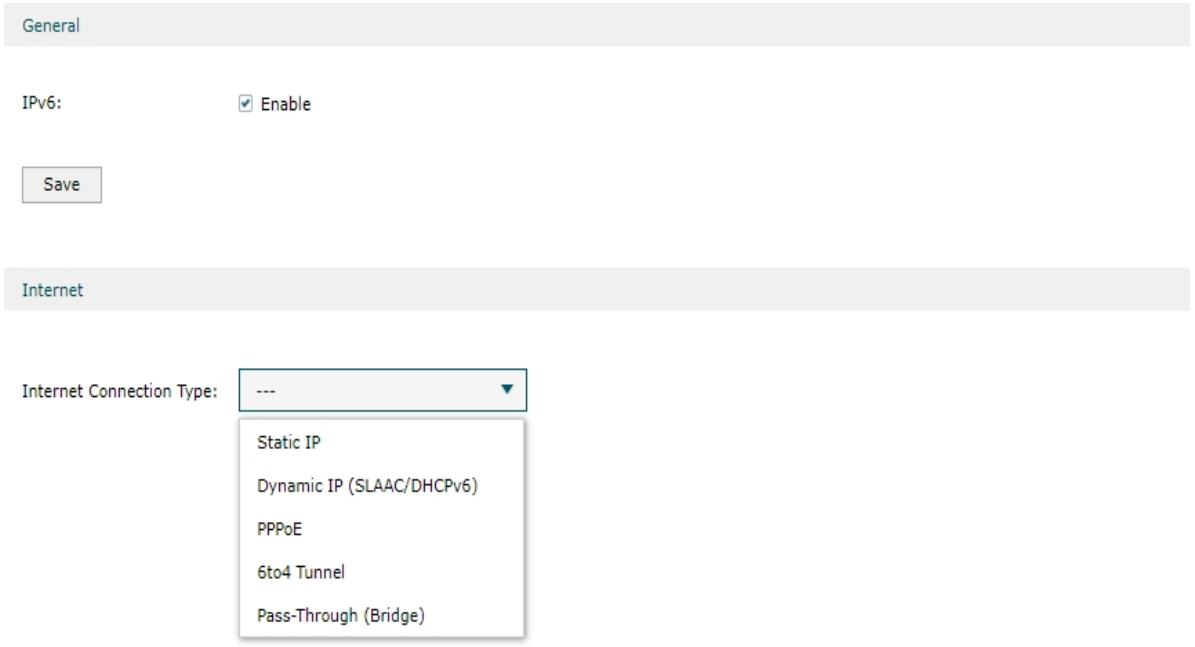
8.1 WAN/SFP WAN 포트에 IPv6 구성하기

네트워크 > **IPv6** > **SFP+ WAN1** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 8-1 IPv6 사용

일반 섹션에서 IPv6를 활성화하고 **저장을** 클릭합니다.

그림 8-2 인터넷 연결 유형 선택


General
IPv6:
Enable
Save
Internet
Internet Connection Type:

Static IP
Dynamic IP (SLAAC/DHCPv6)
PPPoE
6to4 Tunnel
Pass-Through (Bridge)

인터넷 섹션에서 적절한 인터넷 연결 유형을 선택하고 ISP의 요구 사항에 따라 매개변수를 구성합니다. 그런 다음 **저장을** 클릭합니다.

인터넷 연결 유형	ISP의 요구 사항에 따라 적절한 인터넷 연결 유형을 선택하세요.

8.2 WAN 연결 구성

라우터는 5가지 연결 유형을 지원합니다: **고정 IP, 동적 IP(SLAAC/DHCPv6), PPPoE, 6to4 터널, PPTP,** ISP가 제공하는 서비스에 따라 하나를 선택할 수 있습니다.

고정 IP: ISP에서 고정 IP 주소와 해당 매개변수를 제공하는 경우 고정 IP를 선택합니다.

동적 IP(SLAAC/DHCPv6): ISP가 IP 주소와 해당 매개변수를 자동으로 할당하는 경우 동적 IP를 선택합니다.

PPPoE: ISP가 PPPoE 계정을 제공한 경우 PPPoE를 선택합니다.

6to4 터널: ISP가 주소 할당에 6to4 배포를 사용하는 경우 이 유형을 선택합니다.

통과(브리지): ISP가 통과(브리지) 네트워크 배포를 사용하는 경우 이 유형을 선택합니다.

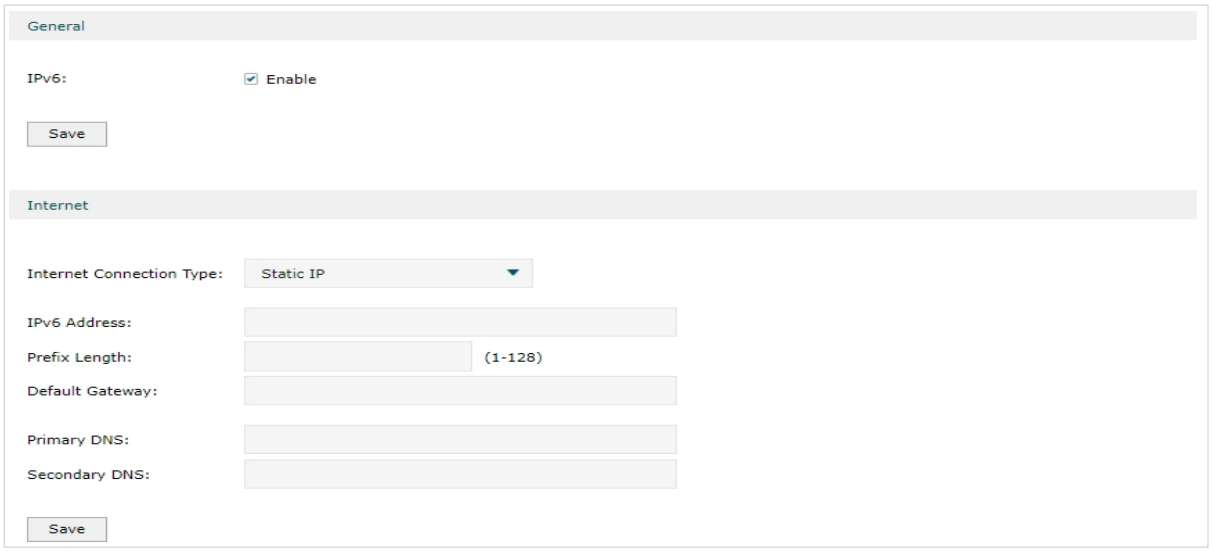
참고:

WAN/SFP WAN의 인터넷 연결 유형을 패스스루(브리지)로 선택한 경우, LAN 포트와 다른 WAN 포트의 IPv6 매개변수를 구성할 수 없습니다.

■ 고정 IP 구성

네트워크 > **IPv6** > **SFP+ WAN1** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 8-3 고정 IP 구성하기



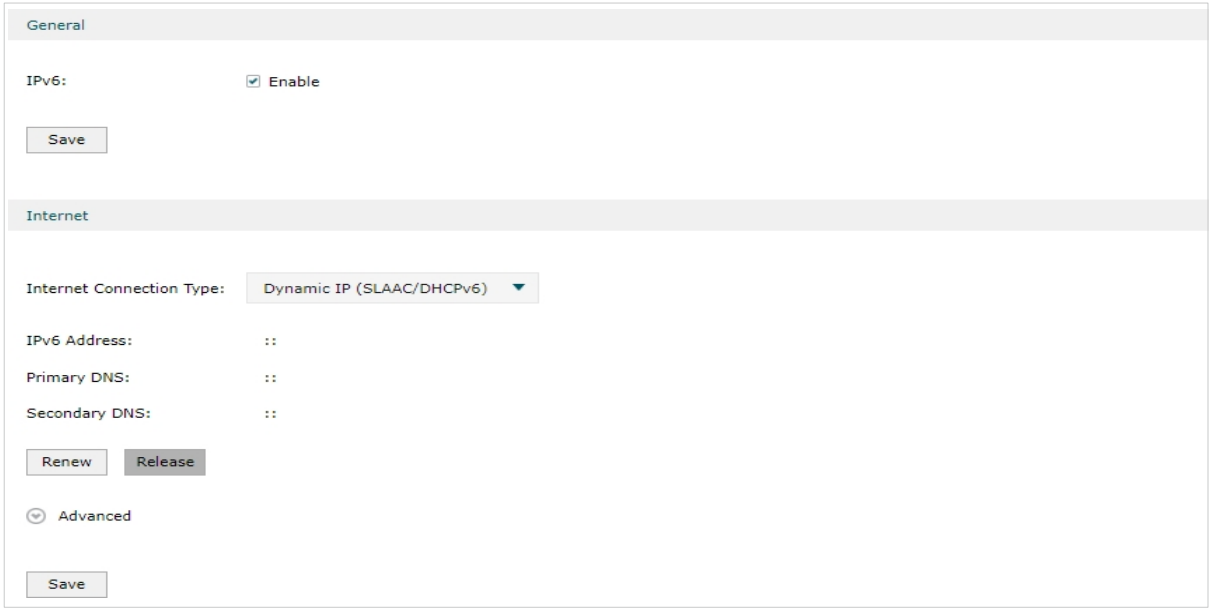
인터넷 섹션에서 연결 유형을 고정 IP로 선택합니다. 해당 매개변수를 입력하고 **저장을** 클릭합니다.

IPv6 주소/ 접두사 길이/ 기본 게이트웨이/ 기본 DNS/ 보조 DNS	ISP에서 제공한 매개변수를 입력합니다.

■ 동적 IP(SLAAC/DHCPv6) 구성하기

네트워크 > **IPv6** > **SFP+ WAN1** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 8-4 다이매닉 IP 구성하기(SLAAC/DHCPv6)



인터넷 섹션에서 연결 유형을 동적 IP(SLAAC/DHCPv6)로 선택합니다. 해당 매개변수를 입력하고 **저장을** 클릭합니다.

IPv6 주소/ 기본 DNS/ 보조 DNS	이러한 매개변수는 ISP에서 자동으로 할당합니다.	
갱신	이 버튼을 클릭하면 ISP에서 새 IPv6 매개변수를 할당받습니다. 해제	
	ISP에서 할당된 모든 IPv6 주소를 해제하려면 이 버튼을 클릭합니다.	
IP6 주소	받기ISP가 게이트웨이에 IP6 주소를 할당하는 적절한 방법을 선택합니다.	자동
	자동으로 IPv6 주소를 받으려면 자동을 선택합니다.	
DHCPv6	ISP는 DHCPv6를 사용하여 IPv6 주소와 DNS 서버 주소를 포함한 기타 매개변수를 게이트웨이에 할당합니다.	
SLAAC+무정형 DHCP	ISP가 게이트웨이에 IPv6 주소 접두사를 할당하면 게이트웨이가 자동으로 자체 IPv6 주소를 생성합니다. 또한, ISP는 DNS 서버 주소를 비롯한 기타 파라미터를 DHCPv6을 사용하여 게이트웨이에 할당합니다.	
접두사 위임	ISP로부터 LAN 포트의 주소 접두사를 받으려면 사용을 선택하고, LAN 포트의 주소 접두사를 수동으로 지정하려면 사용 안 함을 선택합니다. LAN의 클라이언트는 이 접두사가 포함된	

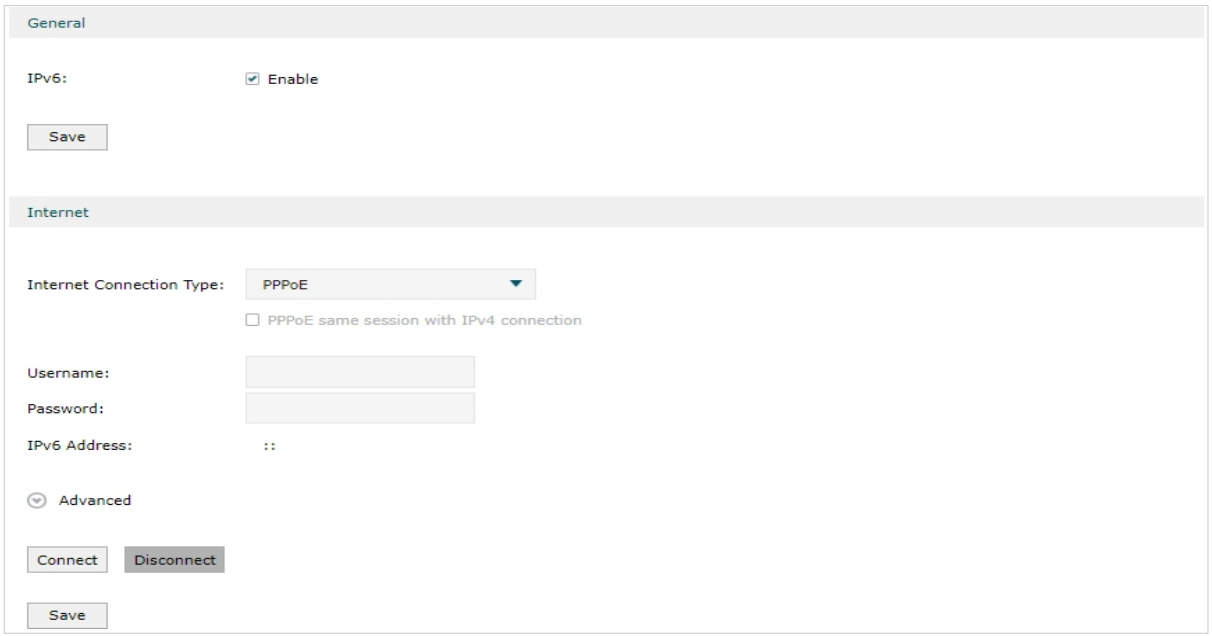
	IPv6 주소를 받게 됩니다.
접두사 위임 크기	접두사 위임이 활성화된 상태에서 접두사 위임 크기를 입력하여 주소 접두사의 길이를 결정합니다. 이 값은 ISP에서 얻을 수 있습니다.
DNS 주소	ISP에서 DNS 주소를 동적으로 가져올지 아니면 수동으로 DNS 주소를 지정할지 선택합니다.

ISP로부터 동적으로 받기	ISP는 게이트웨이에 동적으로 DNS 주소를 할당합니다.
다음 DNS 주소를 사용합니다.	ISP에서 제공한 DNS 주소를 수동으로 입력해야 합니다.
기본 DNS/보조 DNS	DNS 주소를 직접 입력하거나 ISP에서 할당된 DNS 주소를 표시합니다.

■ PPPoE 구성

네트워크 > **IPv6** > **SFP+ WAN1** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 8-5 PPPoE 구성하기



인터넷 섹션에서 연결 유형을 PPPoE로 선택합니다. 해당 매개변수를 입력하고 **저장을** 클릭합니다.

IPv4 연결과 동일한 세션의 PPPoE	이 옵션을 활성화하면 IPv6는 IPv4와 동일한 PPPoE 세션을 사용합니다.
사용자 이름/비밀번호:	ISP에서 제공하는 대로 이러한 매개변수를 입력합니다.
IPv6 주소이 주소는	사용자 이름과 비밀번호를 입력하고 **연결을 클릭하면** ISP에서 자동으로 할당합니다.
연결	인터넷에 연결하려면 이 버튼을 클릭합니다. 연결

해제	인터넷 연결을 끊으려면 이 버튼을 클릭합니다.	
IP6 주소	받기ISP가 게이트웨이에 IP6 주소를 할당하는 적절한 방법을 선택합니다. 자동	자동으

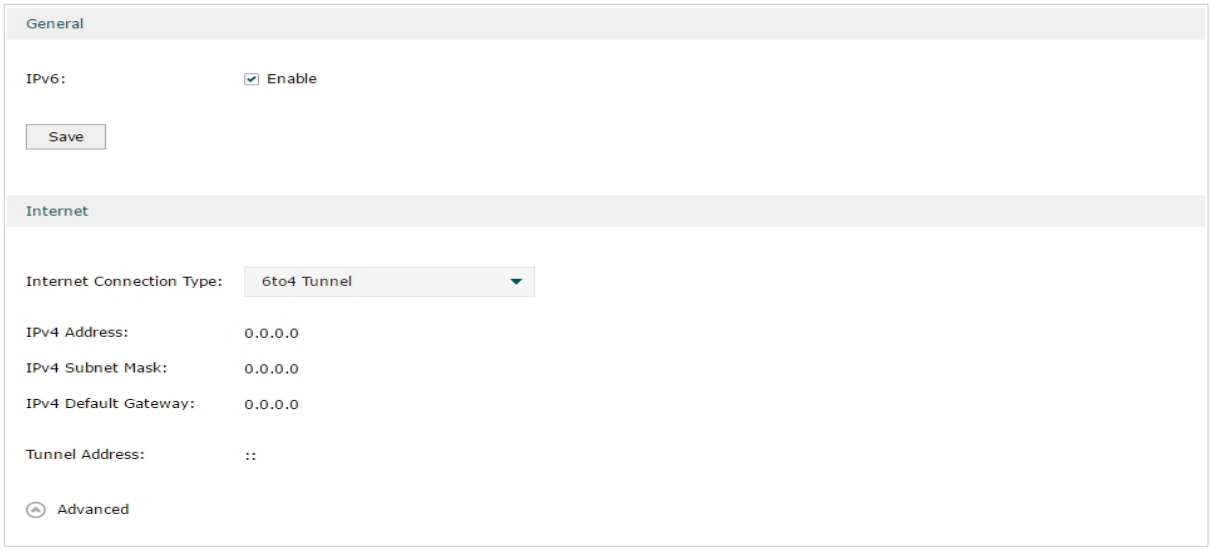
로 IPv6 주소를 받으려면 자동을 선택합니다.

DHCPv6	ISP는 DHCPv6을 사용하여 IPv6 주소와 DNS 서버 주소를 포함한 기타 매개변수를 게이트웨이에 할당합니다.
SLAAC+무정형 DHCP	ISP가 게이트웨이에 IPv6 주소 접두사를 할당하면 게이트웨이가 자동으로 자체 IPv6 주소를 생성합니다. 또한, ISP는 DNS 서버 주소를 비롯한 기타 매개변수를 DHCPv6을 사용하여 게이트웨이에 할당합니다.
ISP에서 지정	ISP에서 제공한 IPv6 주소를 직접 입력해야 합니다.
접두사 위임	ISP로부터 LAN 포트의 주소 접두사를 받으려면 사용을 선택하고, LAN 포트의 주소 접두사를 수동으로 지정하려면 사용 안 함을 선택합니다. LAN의 클라이언트는 이 접두사가 포함된 IPv6 주소를 받게 됩니다.
접두사 위임 크기	접두사 위임이 활성화된 상태에서 접두사 위임 크기를 입력하여 주소 접두사의 길이를 결정합니다. 이 값은 ISP에서 얻을 수 있습니다.
DNS 주소	ISP에서 DNS 주소를 동적으로 가져올지 아니면 수동으로 DNS 주소를 지정할지 선택합니다.
ISP로부터 동적으로 받기	ISP는 DNS 주소와 게이트웨이를 동적으로 할당합니다.
다음 DNS 주소를 사용합니다.	ISP에서 제공한 DNS 주소를 수동으로 입력해야 합니다.
기본 DNS/보조 DNS	DNS 주소를 직접 입력하거나 ISP에서 할당된 DNS 주소를 표시합니다.
연결	인터넷에 연결하려면 이 버튼을 클릭합니다. 연결
해제	인터넷 연결을 끊으려면 이 버튼을 클릭합니다.

■ 6to4 터널 구성

네트워크 > **IPv6** > **SFP+ WAN1** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 8-6 6to4 터널 구성하기


General
IPv6:
Enable
Save
Internet
Internet Connection Type:
6to4 Tunnel
IPv4 Address:
0.0.0.0
IPv4 Subnet Mask:
0.0.0.0
IPv4 Default Gateway:
0.0.0.0
Tunnel Address:
::
Advanced

인터넷 섹션에서 연결 유형을 6to4 터널로 선택합니다. 해당 매개변수를 입력하고 **저장을** 클릭합니다.

IPv4 주소/ IPv4 서브넷 마스크/ IPv4 기본 게이트웨이/ 터널 주소	IPv4 주소/IPv4 서브넷 마스크/IPv4 기본 게이트웨이/터널 주소: 이러한 매개변수는 연결을 클릭한 후 WAN 포트의 IPv4 정보에 따라 동적으로 생성됩니다.
다음 DNS 서버 사용	상자를 클릭하여 ISP에서 제공한 기본 DNS 및/또는 보조 DNS를 수동으로 입력합니다.
연결	인터넷에 연결하려면 이 버튼을 클릭합니다. 연결
해제	인터넷 연결을 끊으려면 이 버튼을 클릭합니다.

■ 패스스루(브리지) 구성하기

네트워크 > **IPv6** > **SFP+ WAN1** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 8-7 패스스루(브리지) 구성하기

인터넷 섹션에서 연결 유형을 통과(브리지)로 선택합니다. 이 연결 유형에는 구성이 필요하지 않습니다.

8.3 LAN 포트에 대한 IPv6 구성

네트워크 > **IPv6** > **LAN** > **작동** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 8-8 할당된 유형 선택

일반 섹션에서 로컬 네트워크에 있는 클라이언트의 호환성에 따라 결정되는 적절한 할당 유형을 선택하고 ISP의 요구 사항에 따라 매개변수를 구성합니다. 그런 다음 **확인을** 클릭합니다.

할당 유형	게이트웨이가 로컬 네트워크의 클라이언트에 IPv6 주소를 할당하는 방법을 결정합니다. 일부 클라이언트는 이러한 할당 유형 중 일부만 지원할 수 있으므로 로컬 네트워크에 있는 클라이언트의 호환성에 따라 선택해야 합니다.

참고:

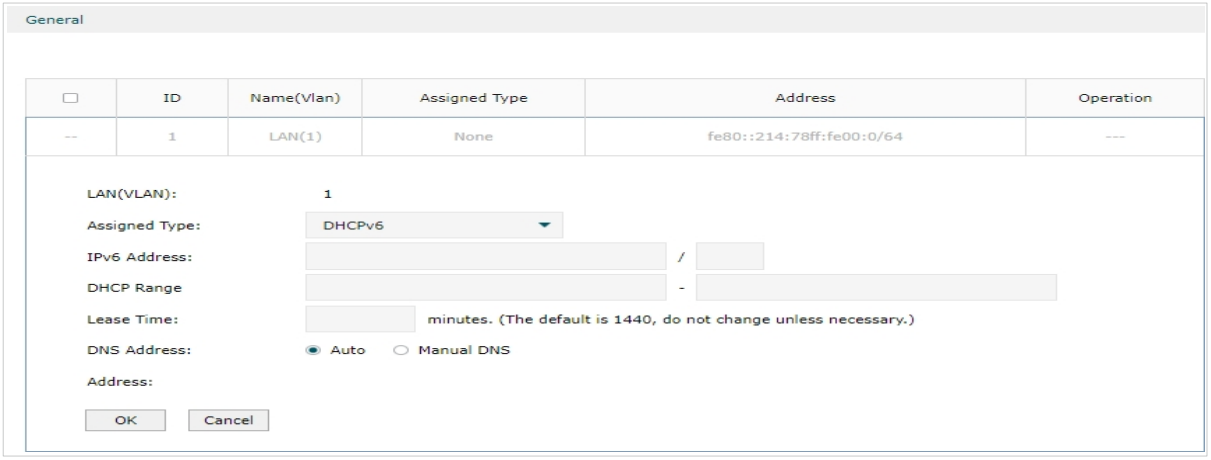
- WAN/SFP WAN의 인터넷 연결 유형을 패스스루(브리지)로 선택한 경우, LAN 포트와 다른 WAN 포트의 IPv6 매개변수를 구성할 수 없습니다.

- WAN/SFP WAN의 접두사 위임이 활성화된 경우, LAN의 주소 접두사는 ISP에 의해 자동으로 할당되며 수동으로 주소 접두사를 지정할 수 없습니다.

■ DHCPv6 구성

네트워크 > **IPv6** > **LAN** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 8-9 DHCPv6 구성하기



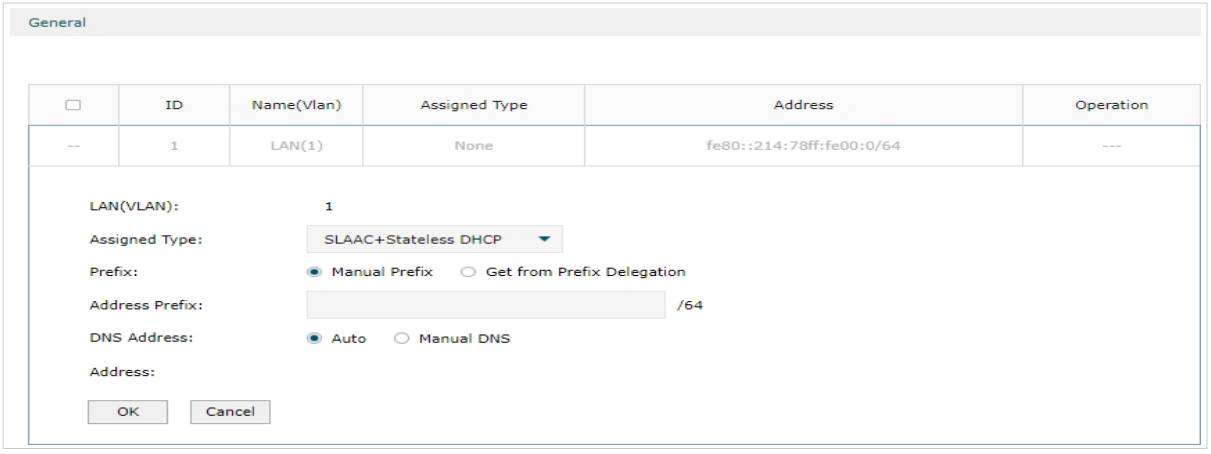
할당된 유형 섹션에서 연결 유형을 DHCPv6으로 선택합니다. 해당 매개변수를 입력하고 **확인을** 클릭합니다.

IPv6 주소	IPv6 주소와 접두사 길이(서브넷 마스크)를 입력합니다.
파일 접미사파일 접미사를 입력하여	파일 형식을 지정합니다. Enter 키, 스페이스 키, "," 또는 ";"을 사용하여 서로 다른 파일 접미사를 구분할 수 있습니다. 선택한 IP 그룹의 호스트는 인터넷에서 이러한 유형의 파일을 다운로드할 수 없습니다.
DHCP 범위	시작 및 종료 IP6 주소를 입력하여 DHCPv6 서버가 동적 IP6 주소를 할당할 범위를 정의합니다.
임대 시간	할당된 IPv6 주소가 유효한 상태로 유지되는 기간(분)입니다. 기본값인 1440분을 유지하거나 필요한 경우 변경합니다.
DNS 주소	LAN의 DNS 서버를 구성하는 방법을 선택합니다. 자동을 선택하면 DNS 서버 주소가 자동으로 가져옵니다. 수동 DNS를 선택한 상태에서 ISP가 제공한 기본 및 보조 DNS 서버 주소를 수동으로 입력합니다.
주소	LAN 포트의 IPv6 주소를 표시합니다.

■ SLAAC+상태 비저장 DHCP 구성하기

네트워크 > **IPv6** > **LAN** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 8-10 SLAAC+상태 비저장 DHCP 구성하기



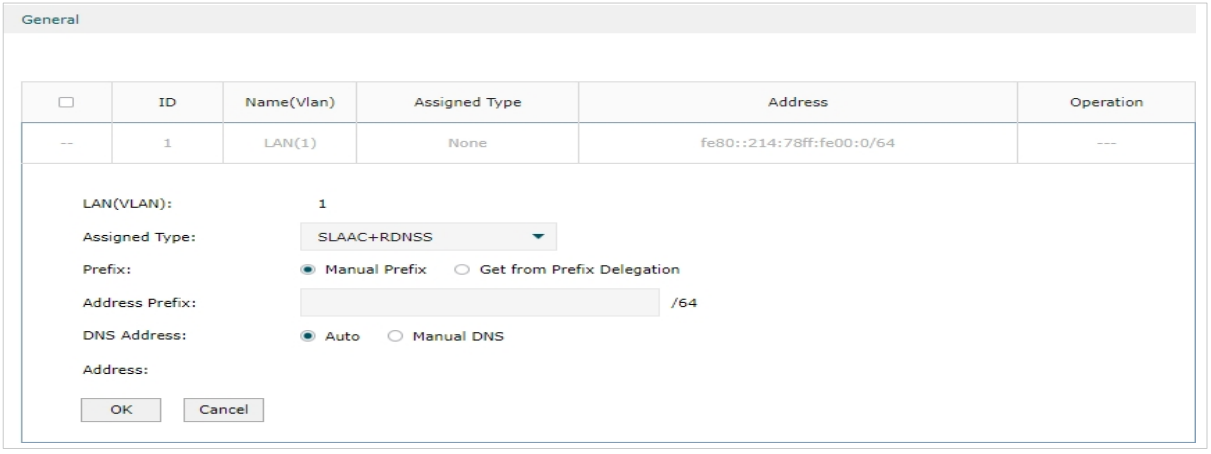
할당된 유형 섹션에서 연결 유형을 SLAAC + 상태 비저장 DHCP로 선택합니다. 해당 매개변수를 입력하고 **확인을** 클릭합니다.

접두사	로컬 네트워크의 각 클라이언트에 대한 IPv6 주소 접두사를 구성합니다. 수동 접두사를 선택한 상태에서 주소 접두사 필드에 접두사를 입력합니다. 접두사 위임에서 가져오기를 선택한 상태에서 IPv6 접두사 위임 WAN 포트를 선택하고 ISP로부터 접두사 위임을 가져올 IPv6 접두사 ID를 입력합니다.
IPv6 접두사 위임 WAN	ISP로부터 접두사 위임을 받으려면 IPv6 접두사 위임 WAN 포트와 IPv6 접두사 ID를 입력합니다.
IPv6 접두사 ID접두사	위임에서 가져오기를 선택한 상태에서 /64 서브넷을 얻기 위해 접두사에 추가할 접두사 ID를 입력합니다. IPv6 접두사 ID의 범위는 접두사 위임 크기와 접두사 길이에 의해 결정됩니다.
DNS 주소	LAN의 DNS 서버를 구성하는 방법을 선택합니다. 자동을 선택하면 DNS 서버 주소가 자동으로 가져옵니다. 수동 DNS를 선택한 경우 ISP에서 제공한 기본 및 보조 DNS 서버 주소를 수동으로 입력합니다.
주소	접두사에 의해 자동으로 생성된 IPv6 주소를 표시합니다.

■ SLAAC+RDNSS 구성하기

네트워크 > **IPv6** > **LAN** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 8-11 SLAAC+RDNSS 구성하기



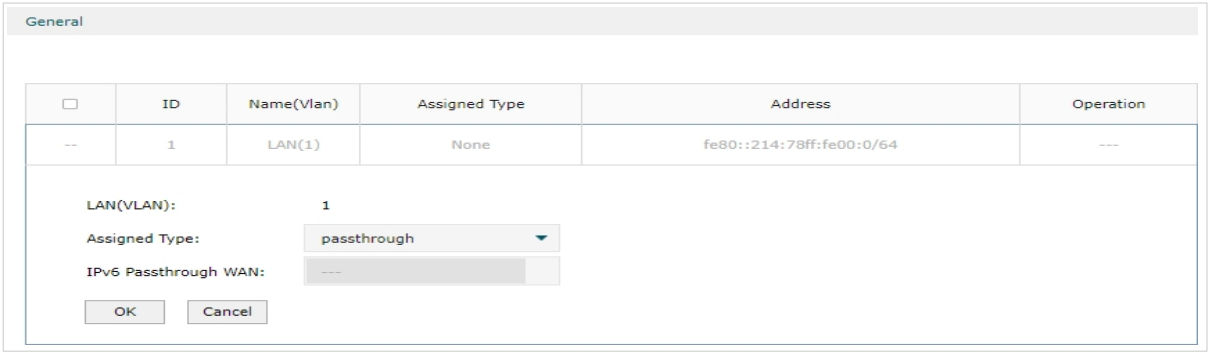
할당된 유형 섹션에서 연결 유형을 SLAAC+RDNSS로 선택합니다. 해당 매개변수를 입력하고 **확인을** 클릭합니다.

접두사	로컬 네트워크의 각 클라이언트에 대한 IPv6 주소 접두사를 구성합니다. 수동 접두사를 선택한 상태에서 주소 접두사 필드에 접두사를 입력합니다. 접두사 위임에서 가져오기를 선택한 상태에서 IPv6 접두사 위임 WAN 포트를 선택하고 ISP로부터 접두사 위임을 가져올 IPv6 접두사 ID를 입력합니다.
IPv6 접두사 위임 WAN	ISP로부터 접두사 위임을 받으려면 IPv6 접두사 위임 WAN 포트와 IPv6 접두사 ID를 입력합니다.
IPv6 접두사 ID접두사	위임에서 가져오기를 선택한 상태에서 /64 서브넷을 얻기 위해 접두사에 추가할 접두사 ID를 입력합니다. IPv6 접두사 ID의 범위는 접두사 위임 크기와 접두사 길이에 의해 결정됩니다.
DNS 주소	LAN의 DNS 서버를 구성하는 방법을 선택합니다. 자동을 선택하면 DNS 서버 주소가 자동으로 가져옵니다. 수동 DNS를 선택한 경우 ISP에서 제공한 기본 및 보조 DNS 서버 주소를 수동으로 입력합니다.
주소	접두사에 의해 자동으로 생성된 IPv6 주소를 표시합니다.

■ 패스스루 구성

네트워크 > **IPv6** > **LAN** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 8-12 패스스루 구성하기



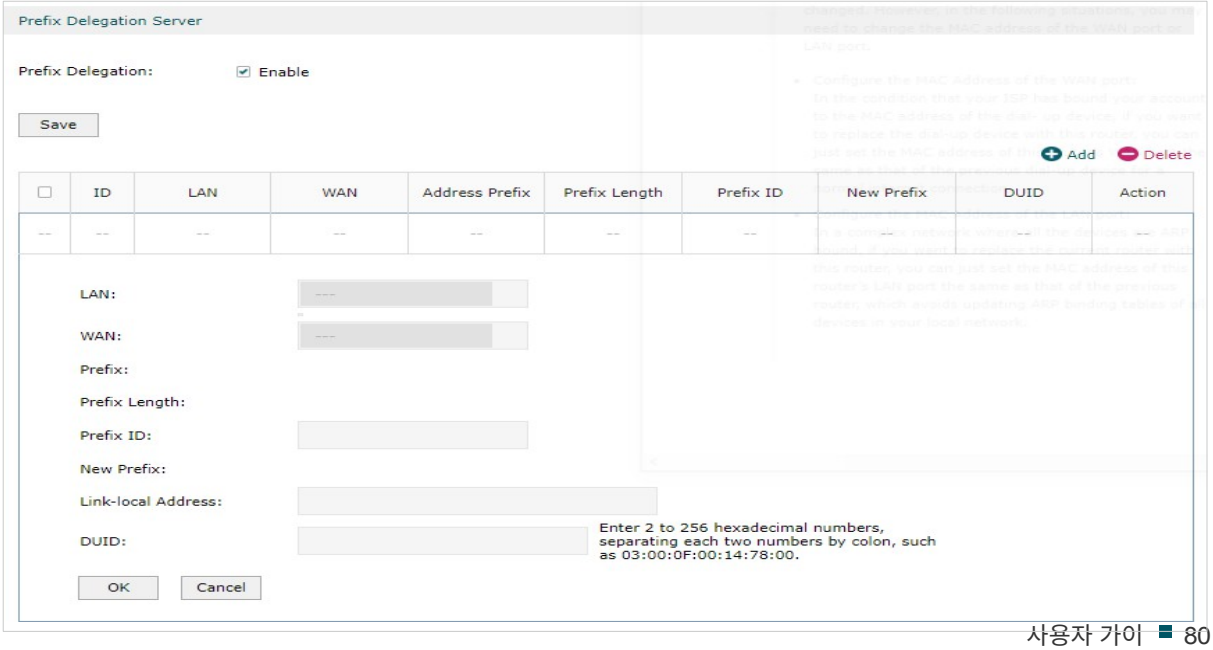
할당된 유형 섹션에서 연결 유형을 통과로 선택합니다. 해당 매개변수를 입력하고 **확인을** 클릭합니다.

IPv6 패스스루 WAN	IPv6 연결에 패스스루(브리지)를 사용하여 WAN 포트를 선택합니다.

참고:

- WAN/SFP WAN의 인터넷 연결 유형을 통과(브리지)로 선택하면 LAN 포트와 다른 WAN 포트의 IPv6 매개변수를 구성할 수 없습니다.
- WAN/SFP WAN의 접두사 위임이 활성화된 경우, LAN의 주소 접두사는 ISP에 의해 자동으로 할당되며 수동으로 주소 접두사를 지정할 수 없습니다.

3) **접두사 위임 서버** 섹션에서 확인란을 선택하여 접두사 **위임을** 사용하도록 설정하고 추가를 클릭하여 접두사 위임 서버를 추가합니다. 그런 다음 **확인을** 클릭합니다.



LAN	요청하는 라우터가 연결할 LAN 포트를 지정합니다.

WAN	위임된 접두사를 가져올 WAN 포트를 선택합니다.
접두사	선택한 WAN 포트에서 위임한 접두사를 표시합니다. (참고: 해당 WAN 포트에 대해 접두사 위임을 사용하도록 설정해야 합니다. 다음 단계를 따르세요: 네트워크 > IPV6 > WAN으로 이동하여 인터넷 연결 유형을 동적 IP로 설정하고 고급에서 접두사 위임을 사용하도록 설정합니다).
접두사 길이	적용할 접두사의 길이를 표시합니다. (참고: 접두사 길이를 설정하려면 네트워크 > IPV6 > WAN으로 이동하여 인터넷 연결 유형을 동적 IP로 설정한 다음 고급에서 접두사 위임 크기를 설정하세요.)
접두사 ID	구성된 접두사 길이가 원래 WAN 포트에서 할당된 접두사 길이보다 큰 경우 나머지 비트의 값을 지정합니다.
새 접두사	적용할 접두사를 표시합니다.
링크-로컬 주소	접두사를 적용할 장치의 링크-로컬 IPv6 주소를 지정합니다.
DUID	접두사를 적용할 디바이스의 ID입니다.

파트 4

USB

챕터

1 Ov erview

USB 모뎀 기능은 3G/4G USB 모뎀을 USB 포트에 연결한 후 ISP(인터넷 서비스 제공업체)의 3G/4G 네트워크에 WAN 연결로 연결하는 데 사용됩니다.

참고:

- LTE USB의 경우, 이 장치의 미국 버전은 2020년 이후 미국에서 생산된 USB 동글, 모바일 핫스팟 및 와이파이 장치와 AT&T, Verizon 및 T-Mobile 제품과 호환되는 장치와 호환됩니다. 이 장치는 또한 Android 테더링 및 플러그 앤 플레이 기능을 지원합니다. Android 휴대폰을 모뎀으로 사용하려면 USB 케이블로 LTE USB 포트에 연결하기만 하면 됩니다.
- 연결/연결 해제를 클릭하여 USB LTE 기능을 활성화/비활성화하거나 필요에 따라 업로드/다운로드 대역폭을 구성할 수 있습니다.

2 U SB 모뎀 구성

USB 모뎀 기능은 3G/4G USB 모뎀을 USB 포트에 연결한 후 ISP(인터넷 서비스 제공업체)의 3G/4G 네트워크에 WAN 연결로 연결하는 데 사용됩니다.

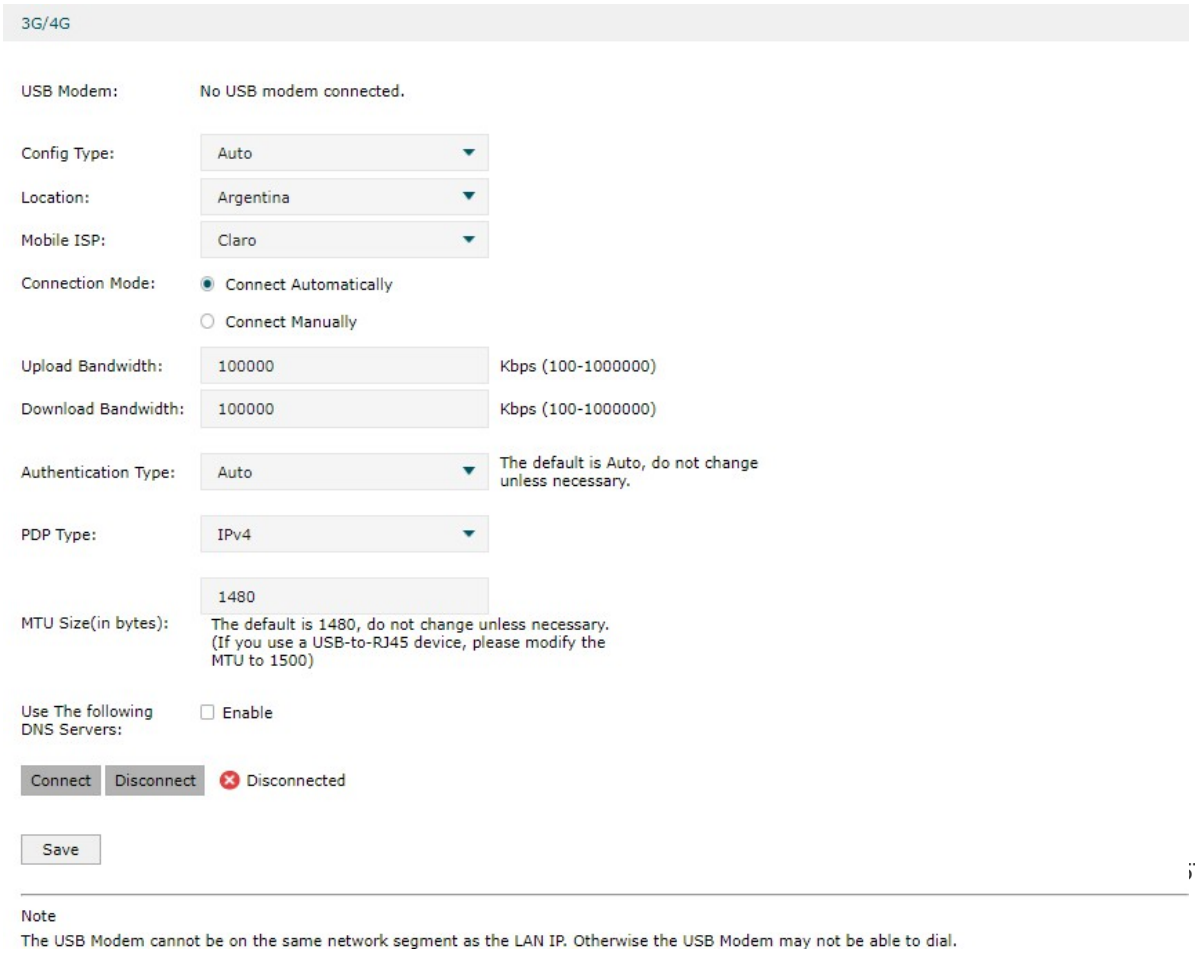
USB 모뎀을 구성하려면 다음 단계를 따르세요:

1) USB 모뎀이 USB 포트에 제대로 연결되어 있는지 확인합니다.
2) ISP 정보를 지정합니다. 위치 및 ISP를 지정하거나 다이얼 번호, APN, 사용자 이름 및 비밀번호를 수동으로 설정할 수 있습니다.
3) 연결 모드를 선택하고 ISP의 요구 사항에 따라 매개변수를 구성합니다.
4) 저장을 클릭합니다.

2.1 USB 모뎀 자동 구성

USB > USB 모뎀 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 2-1 USB 모뎀 자동 구성하기



3G/4G 섹션에서 구성 유형을 자동으로 선택합니다. 해당 매개 변수를 입력하고 **저장을** 클릭합니다.

USB 모뎀	3G/4G USB 모뎀의 상태를 표시합니다.
위치	USB 모뎀과 SIM 카드가 성공적으로 식별되면 자동으로 지역을 선택하고 표시합니다. 그렇지 않은 경우 드롭다운 메뉴에서 지역을 선택합니다.
모바일 ISP	3G/4G 네트워크의 ISP를 표시합니다. 자동으로 감지되지 않는 경우 드롭다운 메뉴에서 ISP를 선택합니다.
번호, APN, 사용자 이름 및 비밀번호 수동으로 다이얼하기	모바일 ISP 목록에 ISP가 없는 경우 이 확인란을 선택하고 ISP에서 제공하는 다이얼 번호, APN(액세스 포인트 이름), 사용자 이름 및 비밀번호를 입력합니다.
연결 모드	연결 모드를 선택하고 ISP의 요구 사항에 따라 매개변수를 구성합니다. **자동 연결:** 이 모드에서는 인터넷 연결이 끊어질 때마다 자동으로 다시 연결됩니다. **수동으로 연결:** 이 모드에서는 연결 또는 연결 해제 버튼을 클릭하여 인터넷 연결을 수동으로 제어할 수 있습니다.
업로드 대역폭	USB 모뎀의 업스트림 대역폭을 지정합니다. 이 값은 **전송 > 대역폭 제어** 페이지의 최대 업스트림 대역폭의 상한입니다. 또한 이 값은 **전송 > 부하 분산 > 기본 설정** 페이지에서 대역폭 기반 균형 라우팅을 활성화한 후 USB 모뎀과 WAN 포트의 대역폭 비율을 결정합니다.
대역폭 다운로드	USB 모뎀의 다운스트림 대역폭을 지정합니다. 이 값은 **전송 > 대역폭 제어** 페이지의 최대 다운스트림 대역폭의 상한입니다. 또한 이 값은 **전송 > 부하 분산 > 기본 설정** 페이지에서 대역폭 기반 균형 라우팅을 활성화한 후 USB 모뎀과 WAN 포트의 대역폭 비율을 결정합니다.
인증 유형	인증 유형을 선택합니다. 기본값은 자동입니다. 일부 ISP는 특정 인증 유형을 요구하므로 ISP에 확인하거나 기본 설정을 유지하세요. **자동:** 자동(기본값)을 선택하면 라우터가 ISP에서 사용하는 인증 유형을 자동으로 결정합

니다. **PAP:** PAP(암호 인증 프로토콜)인 경우, 라우터는 두 번의	핸드셰이크를 사용하여 피어를 인증합니다. ISP에서 이 인증 유형을 요구하는 경우 이 옵션을 선택합니다. **CHAP:** CHAP(챌린지 핸드셰이크 인증 프로토콜)인 경우, 라우터는 세 번의 핸드셰이크를 사용하여 피어를 인증하고 주기적으로 피어의 신원 확인을 확인합니다. ISP에서 이 인증 유형을 요구하는 경우 이 옵션을 선택합니다.

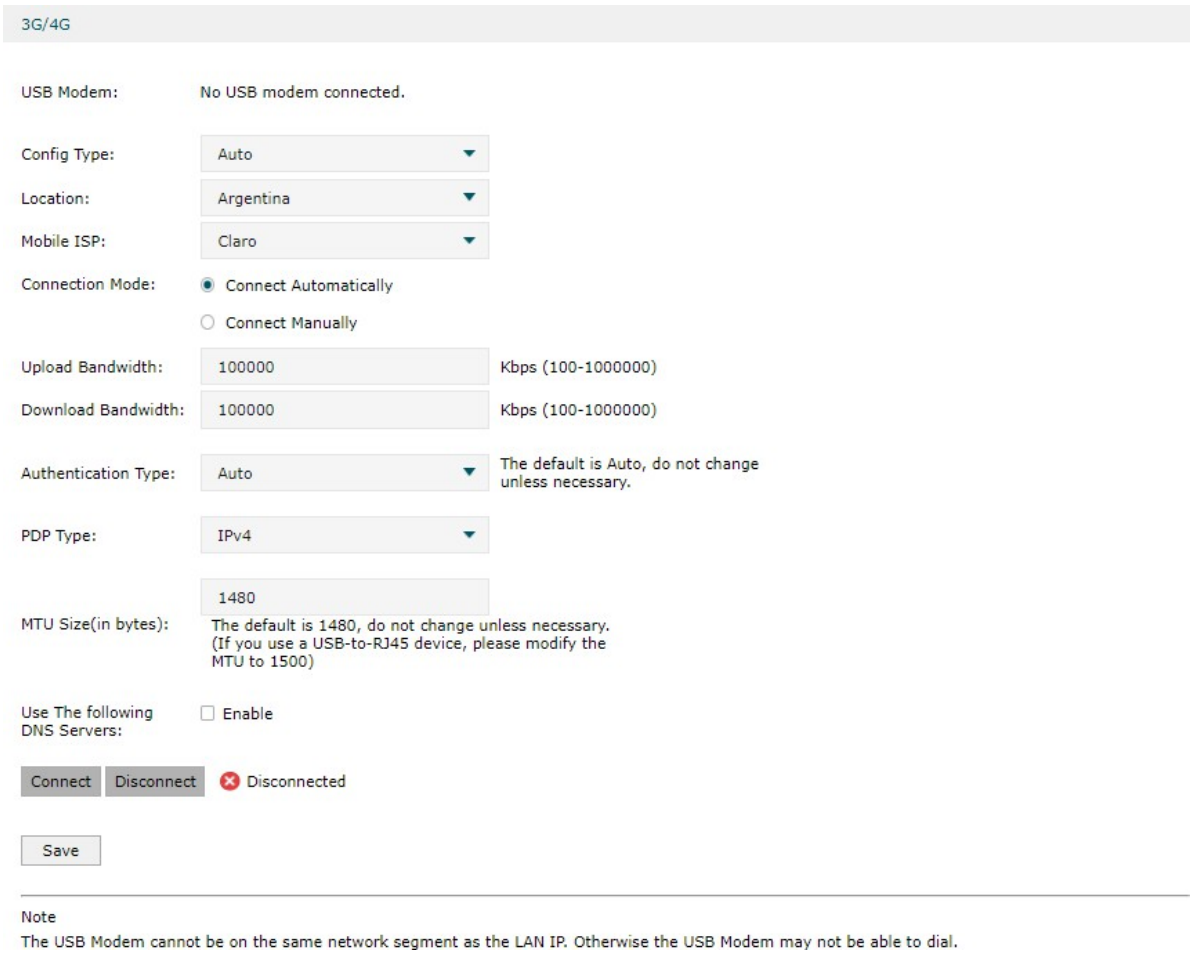
MTU 크기기본 MTU(최대 전송 단위) 크기는 1480바이트입니다. ISP에서 요구하지 않는 한 변경하지 마세요.

다음 DNS 서버 사용	ISP에서 DNS 서버 IP 주소를 제공하는 경우 이 확인란을 선택하고 아래에 기본 DNS 및 보조 DNS(선택 사항) IP 주소를 입력합니다. 그렇지 않으면 DNS 서버가 ISP에 의해 동적으로 할당됩니다. **기본 DNS:** ISP에서 제공한 DNS IP 주소를 점으로 구분된 십진수 표기법으로 입력합니다. **보조 DNS:** (선택 사항) ISP에서 제공한 다른 DNS IP 주소를 점으로 구분하여 소수점 이하 숫자로 입력합니다.

2.2 USB 모뎀 수동 구성하기

USB > USB 모뎀 메뉴를 선택하면 다음 페이지가 로드됩니다...

그림 2-2 USB 모뎀 수동 구성하기



3G/4G 섹션에서 구성 유형을 수동으로 선택합니다. 해당 매개 변수를 입력하고 **저장을** 클릭합니다.

USB 모뎀	3G/4G USB 모뎀의 상태를 표시합니다.

번호, APN, 사용자 이름 및 비밀번호 수동으로 다이얼하기	모바일 ISP 목록에 ISP가 없는 경우 이 확인란을 선택하고 ISP에서 제공하는 다이얼 번호, APN(액세스 포인트 이름), 사용자 이름 및 비밀번호를 입력합니다.
연결 모드	연결 모드를 선택하고 ISP의 요구 사항에 따라 매개변수를 구성합니다. **자동 연결:** 이 모드에서는 인터넷 연결이 끊어질 때마다 자동으로 다시 연결됩니다. **수동으로 연결:** 이 모드에서는 연결 또는 연결 해제 버튼을 클릭하여 인터넷 연결을 수동으로 제어할 수 있습니다.
업로드 대역폭	USB 모뎀의 업스트림 대역폭을 지정합니다. 이 값은 **전송 > 대역폭 제어** 페이지의 최대 업스트림 대역폭의 상한입니다. 또한 이 값은 **전송 > 부하 분산 > 기본 설정** 페이지에서 대역폭 기반 균형 라우팅을 활성화한 후 USB 모뎀과 WAN 포트의 대역폭 비율을 결정합니다.
대역폭 다운로드	USB 모뎀의 다운스트림 대역폭을 지정합니다. 이 값은 **전송 > 대역폭 제어** 페이지의 최대 다운스트림 대역폭의 상한입니다. 또한 이 값은 **전송 > 부하 분산 > 기본 설정** 페이지에서 대역폭 기반 균형 라우팅을 활성화한 후 USB 모뎀과 WAN 포트의 대역폭 비율을 결정합니다.
인증 유형	인증 유형을 선택합니다. 기본값은 자동입니다. 일부 ISP는 특정 인증 유형을 요구하므로 ISP에 확인하거나 기본 설정을 유지하세요. **자동:** 자동(기본값)을 선택하면 라우터가 ISP에서 사용하는 인증 유형을 자동으로 결정합니다. **PAP:** PAP(암호 인증 프로토콜)인 경우, 라우터는 두 번의 핸드셰이크를 사용하여 피어를 인증합니다. ISP에서 이 인증 유형을 요구하는 경우 이 옵션을 선택합니다. **CHAP:** CHAP(챌린지 핸드셰이크 인증 프로토콜)인 경우, 라우터는 세 번의 핸드셰이크를 사용하여 피어를 인증하고 주기적으로 피어의 신원 확인을 확인합니다. ISP에서 이 인증 유형을 요구하는 경우 이 옵션을 선택합니다.
MTU 크기	기본 MTU(최대 전송 단위) 크기는 1480바이트입니다. ISP에서 요구하지 않는 한 변경하지 마세요.
다음 DNS 서버 사용	ISP에서 DNS 서버 IP 주소를 제공하는 경우 이 확인란을 선택하고 아래에 기본 DNS 및 보조 DNS(선택 사항) IP 주소를 입력합니다. 그렇지 않으면 DNS 서버가 ISP에 의해 동적으로 할당됩니다. **기본 DNS:** ISP에서 제공한 DNS IP 주소를 점으로 구분된 십진수 표기법으로 입력합니다.

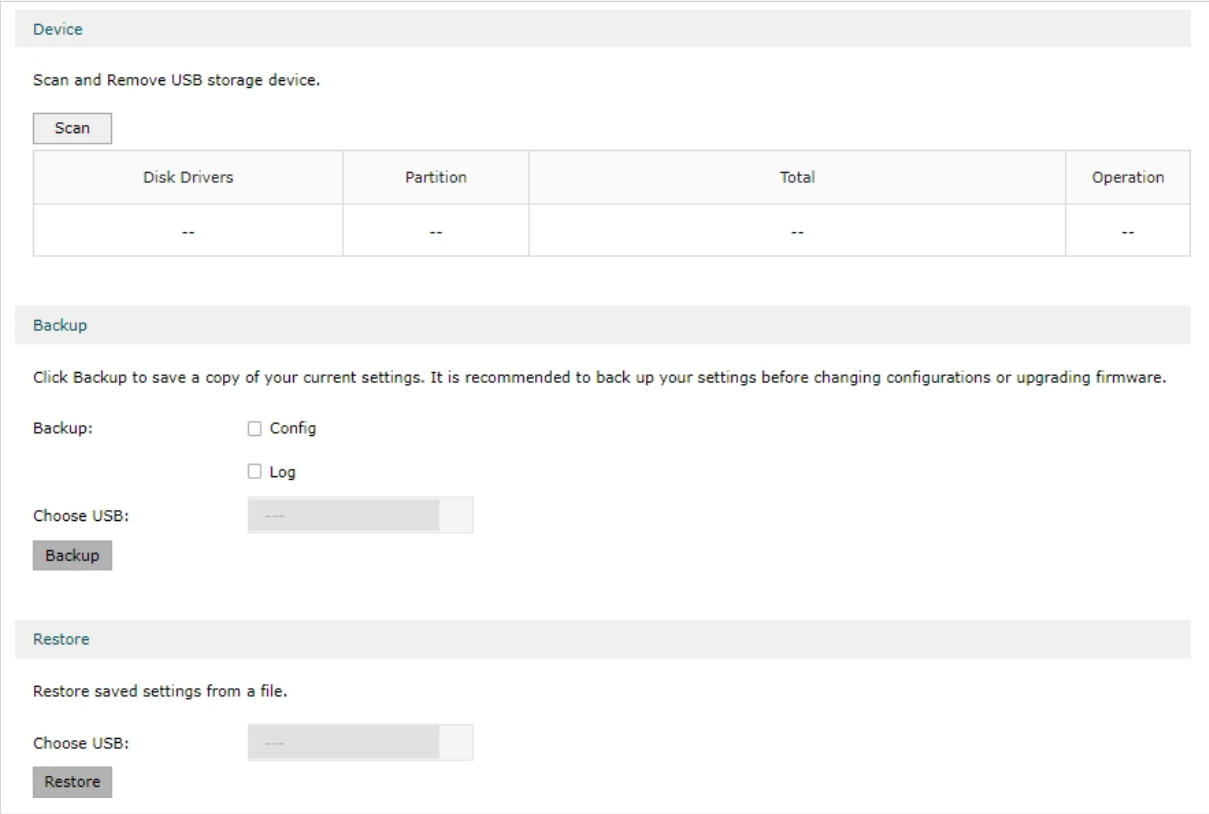
보조 DNS: (선택 사항)	ISP에서 제공한 다른 DNS IP 주소를 점으로 구분된 소수점 표기로 입력합니다.

3 U SB 스토리지

3.1 USB 스토리지 관리

USB > USB 저장소 **> USB 저장소** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 3-1 USB 스토리지 관리하기



USB 장치를 USB 포트에 꽂으면 됩니다:

1) **장치** 섹션에서 스캔을 클릭하여 USB 저장소 정보를 확인합니다.

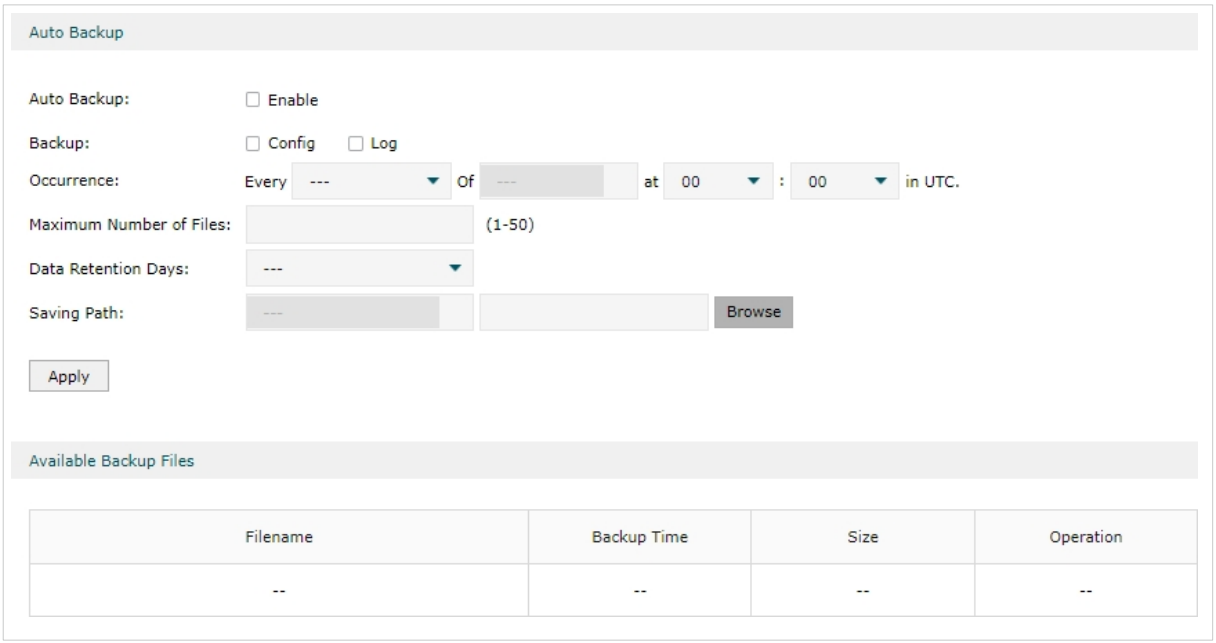
2) **백업** 섹션에서 백업을 클릭하여 현재 설정의 사본을 저장합니다. 구성을 변경하거나 펌웨어를 업그레이드하기 전에 설정을 백업하는 것이 좋습니다.

3) **복원** 섹션에서 **복원을** 클릭하여 저장된 설정을 파일 형태로 복원합니다.

3.2 자동 백업

USB > USB 저장소 **> 자동 백업** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 3-2 자동 백업 관리

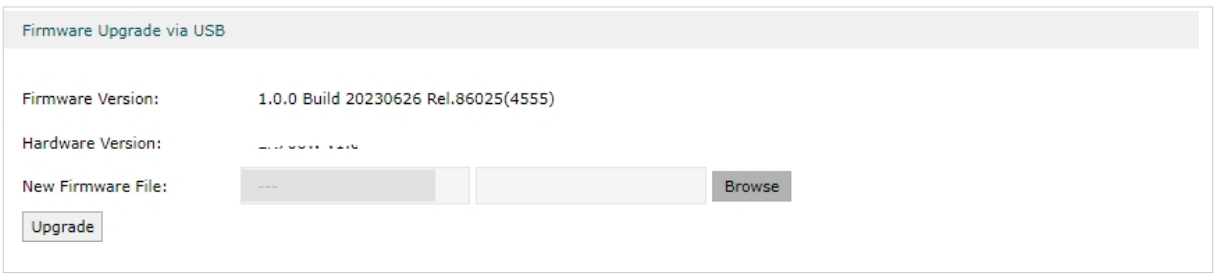


1) 자동 백업을 활성화합니다.
2) USB 저장 장치에 저장할 콘텐츠를 선택합니다. 현재 설정을 업그레이드하거나 수정하기 전에 백업하는 것이 좋습니다.
3) 백업 빈도를 설정합니다.
4) 자동 백업할 수 있는 최대 파일 수를 지정합니다.
5) 백업을 보관할 기간을 설정합니다.
6) 백업 저장 경로를 선택합니다.
7) 적용을 클릭하여 설정을 저장합니다.

3.3 USB를 통한 펌웨어 업그레이드

USB > USB 저장소 > USB를 통한 펌웨어 업그레이드 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 3-3 USB를 통한 펌웨어 업그레이드 관리



1) 찾아보기를 클릭하여 USB에서 파일을 선택합니다.

2) 업그레이드를 클릭하여 펌웨어를 업그레이드합니다.

파트 5

환경 설정 구성

챕터

1 Ov erview

IP 그룹, 시간 범위, IP 풀 및 서비스 유형과 같은 특정 환경설정을 미리 설정할 수 있습니다. 이러한 기본 설정은 일부 기능의 해당 매개변수를 구성할 때 선택할 수 있는 옵션으로 표시됩니다. 예를 들어, 여기에서 구성한 IP 그룹은 대역폭 제어, 세션 제한 , 정책 라우팅 등의 기능에 대한 유효 IP 주소를 구성할 때 옵션으로 표시됩니다.

여기에서 환경설정을 구성하면 여러 기능에 적용할 수 있으므로 구성하는 동안 시간을 절약할 수 있습니다. 예를 들어, **환경설정에서** 시간 범위를 구성한 후
> 시간 범위 > 시간 범위 페이지에서 이 시간 범위를 대역폭 제어 규칙, 링크 백업 규칙, 정책 라우팅 규칙 등의 유효 시간으로 사용할 수 있습니다.

2 IP 그룹 구성

IP 그룹에서는 대역폭 제어, 세션 제한, 정책 라우팅과 같은 일부 기능의 관련 매개변수를 구성할 때 선택할 수 있는 옵션으로 표시되는 IP 그룹을 미리 설정할 수 있습니다. 항목을 생성한 후에는 여러 구성에 적용할 수 있으므로 동일한 정보를 반복적으로 설정하지 않아도 됩니다.

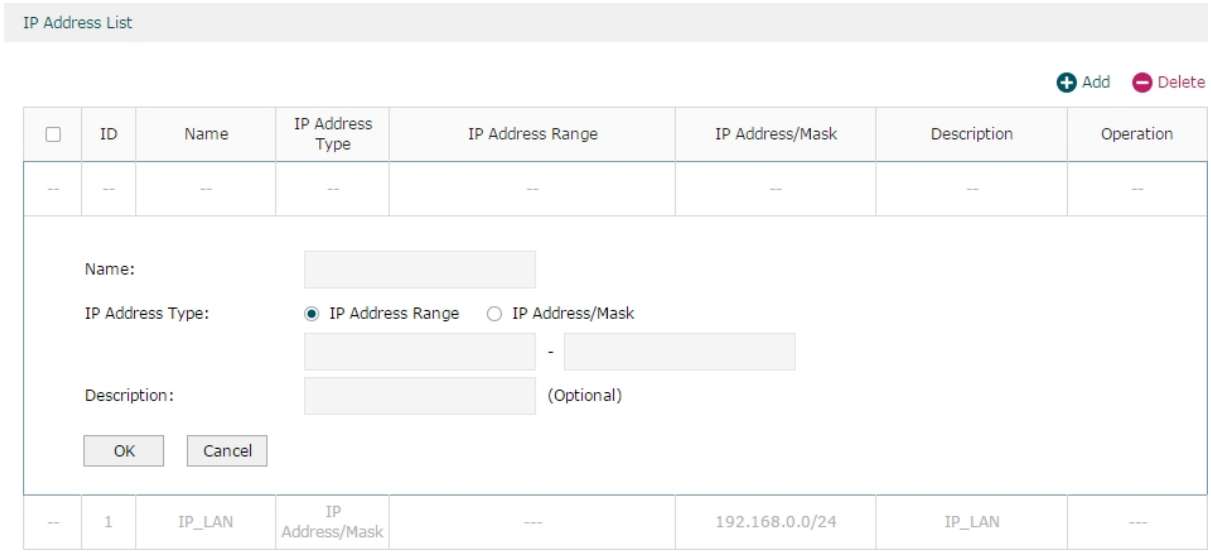
IP 그룹 구성을 완료하려면 다음 단계를 따르세요:

1) 추가를 클릭하여 새 IP 그룹을 추가합니다.
2) 이름을 입력하고 미리 설정된 IP 주소 항목을 선택한 다음 새 항목에 해당하는 매개변수를 구성합니다.
3) 대역폭 제어, 세션 제한 및 정책 라우팅과 같은 관련 구성에서 생성된 IP 그룹 항목을 선택합니다.

2.1 IP 주소 항목 추가

환경설정 > IP 그룹 > IP 주소 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 2-1 IP 주소 항목 추가



IP 주소 항목을 추가하려면 다음 단계를 따르세요:

1) 이름을 입력하고 IP 주소 범위를 지정합니다.

이름	IP 주소 항목의 이름을 입력합니다. 문자, 숫자 또는 밑줄만 사용할 수 있습니다.

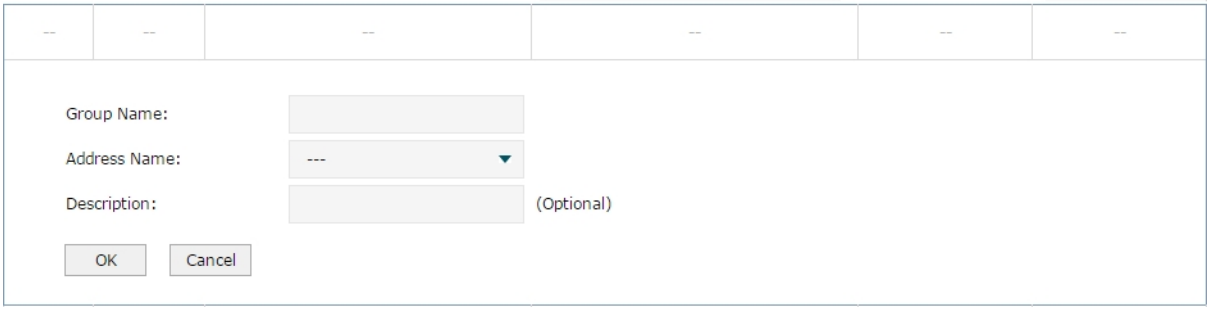
IP 주소 유형	IP 주소 항목의 유형을 지정합니다. 두 가지 유형이 제공됩니다: **IP 주소 범위**: 시작 IP 주소와 종료 IP 주소를 지정합니다. IP 주소 항목을 참조하는 규칙은 해당 항목의 범위 내에 있는 IP 주소에 적용됩니다. **IP 주소/마스크**: 네트워크 주소와 서브넷 마스크를 지정합니다. IP 주소 항목을 참조하는 규칙은 해당 항목의 범위 내에 있 는 IP 주소에 적용됩니다.
설명	관리를 용이하게 하기 위해 IP 주소 항목에 대한 간단한 설명을 입력합니다. 최대 50자까지 입력할 수 있습니다.

2) **확인을** 클릭합니다.

2.2 IP 주소 항목 그룹화

환경설정 > IP 그룹 > IP 그룹 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 2-2 IP 그룹 만들기



다음 단계에 따라 IP 그룹을 만들고 그룹에 IP 주소 항목을 추가합니다:

1) 이름을 지정하고 범위를 구성하여 IP 주소 범위를 추가합니다.

그룹 이름	IP 그룹의 이름을 입력합니다. 문자, 숫자 또는 밑줄만 사용할 수 있습니다.
주소 이름	IP 주소 항목을 선택하며, 하나의 IP 그룹에 대해 두 개 이상의 항목을 선택할 수 있습니다. IP 그룹을 참조하는 규칙은 그룹의 모든 IP 주소에 적용됩니다.
설명	주소 그룹을 쉽게 관리할 수 있도록 간단한 설명을 입력합니다. 최대 50자까지 입력할 수 있습니다.

2) **확인을** 클릭합니다.

참고:

규칙에서 참조한 IP 그룹은 규칙이 더 이상 해당 IP 그룹을 참조하지 않는 한 삭제할 수 없습니다.

IP 그룹은 null일 수 있으며, 이는 IP 그룹에 IP 주소가 포함되어 있지 않음을 의미합니다. 주소 그룹을 참조하는 규칙은 어떤 IP 주소에도 적용되지 않습니다.

3 IP v6 그룹 구성

IPv6 그룹에서는 대역폭 제어, 세션 제한, 정책 라우팅과 같은 일부 기능의 관련 매개변수를 구성할 때 선택할 수 있는 옵션으로 표시되는 IPv6 그룹을 미리 설정할 수 있습니다. 항목을 생성한 후에는 여러 구성에 적용할 수 있으므로 동일한 정보를 반복적으로 설정하지 않아도 됩니다.

IPv6 그룹 구성을 완료하려면 다음 단계를 따르세요:

3) 추가를 클릭하여 새 IPv6 그룹을 추가합니다.

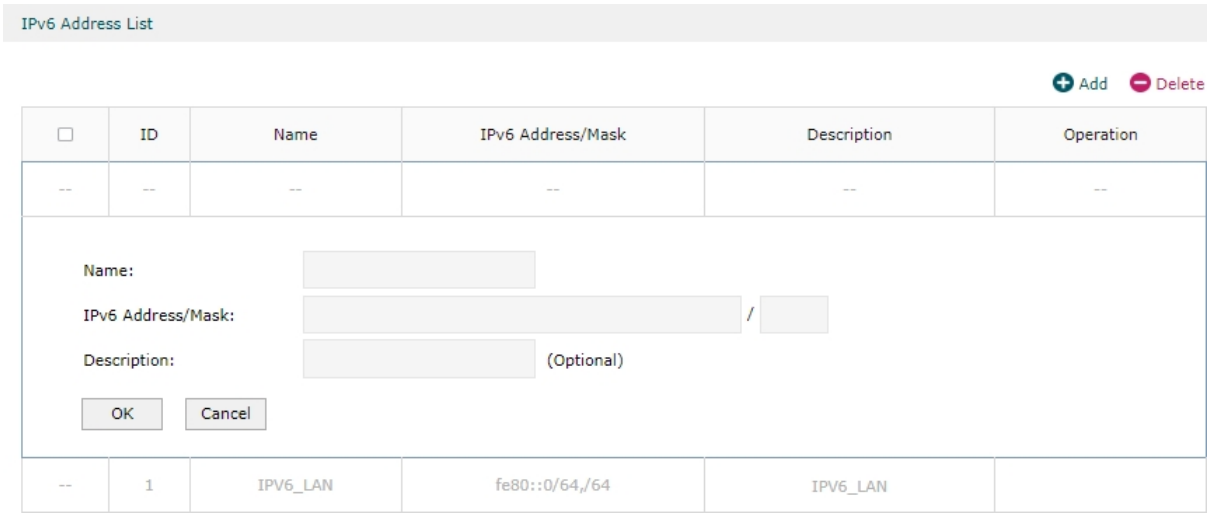
4) 이름을 입력하고 미리 설정된 IPv6 주소 항목을 선택한 다음 새 항목에 해당하는 매개변수를 구성합니다.

5) 대역폭 제어, 세션 제한 및 정책 라우팅과 같은 관련 구성에서 생성된 IPv6 그룹 항목을 선택합니다.

3.1 IP 주소 항목 추가

환경설정 > IPv6 그룹 > IPv6 주소 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 3-1 IPv6 주소 항목 추가하기



IPv6 주소 항목을 추가하려면 다음 단계를 따르세요:

1) 이름을 입력하고 IPv6 주소 범위를 지정합니다.

이름	IPv6 주소 항목의 이름을 입력합니다. 문자, 숫자 또는 밑줄만 사용할 수 있습니다.

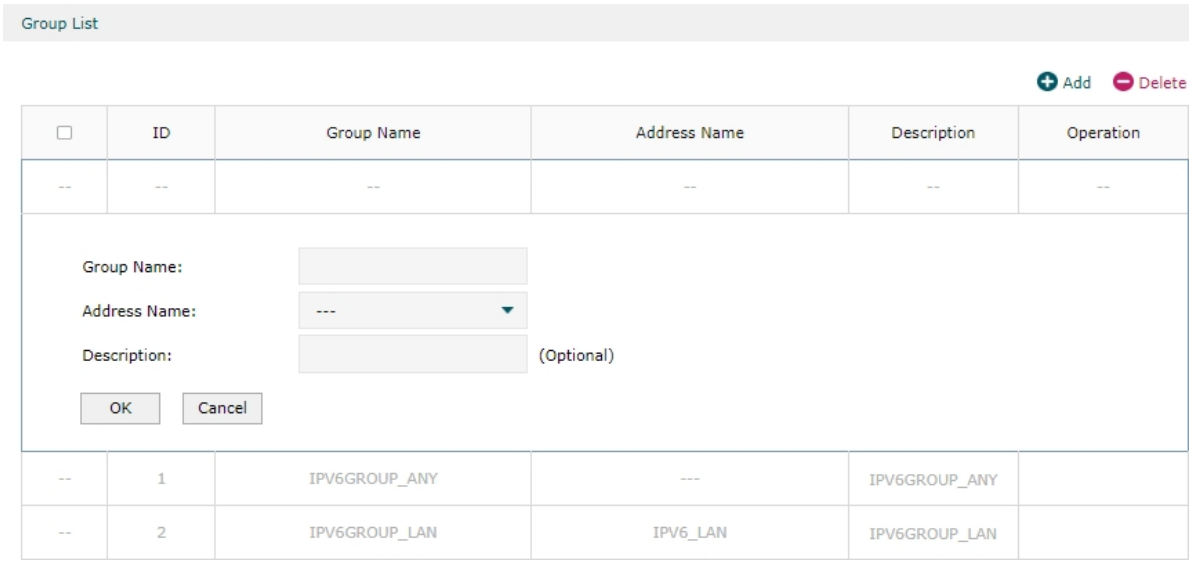
IPv6 주소/마스크:	네트워크 주소와 서브넷 마스크를 지정합니다. IP v6address 항목을 참조하는 규칙이 해당 항목의 범위 내에 있는 IPv6 주소에 적용됩니다.
설명	관리를 용이하게 하기 위해 IP 주소 항목에 대한 간단한 설명을 입력합니다. 최대 50자까지 입력할 수 있습니다.

2) **확인을** 클릭합니다.

3.2 IP 주소 항목 그룹화

환경설정 > IPv6 그룹 > IPv6 그룹 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 3-2 IPv6 그룹 만들기



다음 단계에 따라 IPv6 그룹을 만들고 그룹에 IPv6 주소 항목을 추가합니다:

1) 이름을 지정하고 범위를 구성하여 IPv6 주소 범위를 추가합니다.

그룹 이름	IPv6 그룹의 이름을 입력합니다. 문자, 숫자 또는 밑줄만 사용할 수 있습니다. 주소 이
름	IPv6 주소 항목을 선택하며, 하나에 대해 두 개 이상의 항목을 선택할 수 있습니다. IPv6 그룹. IPv6 그룹을 참조하는 규칙은 그룹의 모든 IPv6 주소에 적용됩니다.
설명	주소 그룹을 쉽게 관리할 수 있도록 간단한 설명을 입력합니다. 최대 50자까지 입력할 수 있습니다.

2) **확인을** 클릭합니다.

참고:

규칙이 더 이상 IPv6 그룹을 참조하지 않는 한 규칙에서 참조한 IPv6 그룹은 삭제할 수 없습니다.

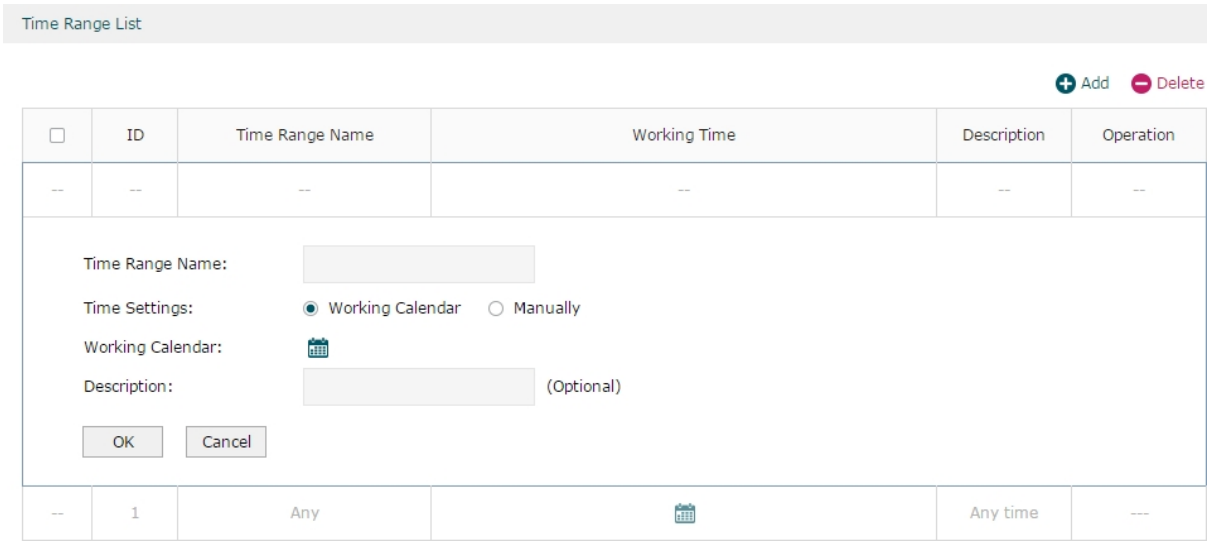
IPv6 그룹은 null일 수 있으며, 이는 IPv6 그룹에 IPv6 주소가 포함되어 있지 않음을 의미합니다. 주소 그룹을 참조하는 규칙은 어떤 IPv6 주소에도 적용되지 않습니다.

4 시간 범위 구성

시간 범위 구성에서는 일 단위 기간과 주 단위 요일을 지정하여 시간 범위를 정의할 수 있습니다. 여기서 설정한 시간 범위는 대역폭 제어, 링크 백업, 정책 라우팅 등과 같은 여러 기능의 유효 시간으로 사용할 수 있습니다.

환경설정 > 시간 범위 > 시간 범위 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 4-1 시간 범위 항목 추가



시간 범위 항목을 추가하려면 다음 단계를 따르세요:

1) 시간 범위 항목의 이름을 입력합니다.

시간 범위 이름	시간 범위 항목의 이름을 입력합니다. 문자, 숫자 또는 밑줄만 사용할 수 있습니다.

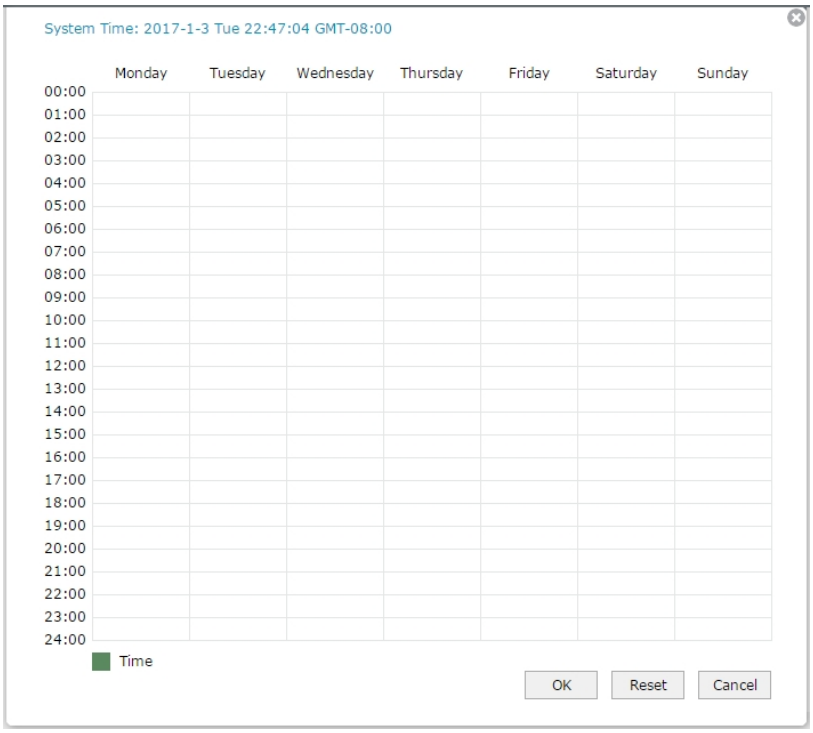
2) 모드를 선택하여 시간 범위를 설정합니다. 두 가지 모드가 제공됩니다: 작업 캘린더와 수동으로.

■ 업무 일정

작업 캘린더 모드에서는 캘린더에서 시간 범위를 설정할 수 있습니다. 이 모드에서는 유효 시간을 시간 단위로 정확하게 설정할 수 있습니다.

업무용 캘린더 모드를 선택하고 을 클릭하면 다음 페이지가 로드됩니다.

그림 4-2 작업 일정 모드



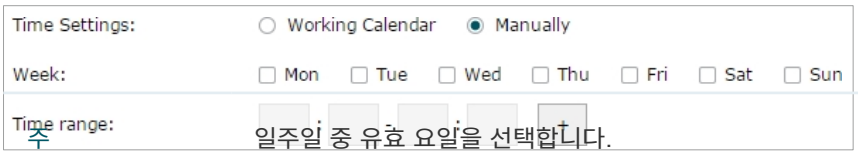
시간 조각을 선택하고 **확인을** 클릭하여 시간 범위를 설정합니다. 시간 조각을 클릭하거나 영역을 드래그하여 시간 조각을 선택하거나 선택 취소할 수 있습니다.

■ 수동으로

수동 모드에서는 시간 범위를 입력하고 일주일 중 유효 요일을 수동으로 선택할 수 있습니다. 이 모드에서는 유효 시간을 분 단위로 정확하게 설정할 수 있습니다.

수동 모드를 선택하면 다음 페이지가 로드됩니다.

그림 4-3 수동 모드



주 일주일 중 유효 요일을 선택합니다.

시간 범위	시작 및 종료 시간을 입력합니다. 유효 시간이 불연속적인 경우 + 을 클릭하여 다른 시간 범위를 추가합니다.

3) (선택 사항) 이 기간에 대한 간단한 설명을 입력하여 쉽게 식별할 수 있도록 합니다.

4) **확인을** 클릭합니다.

참고:

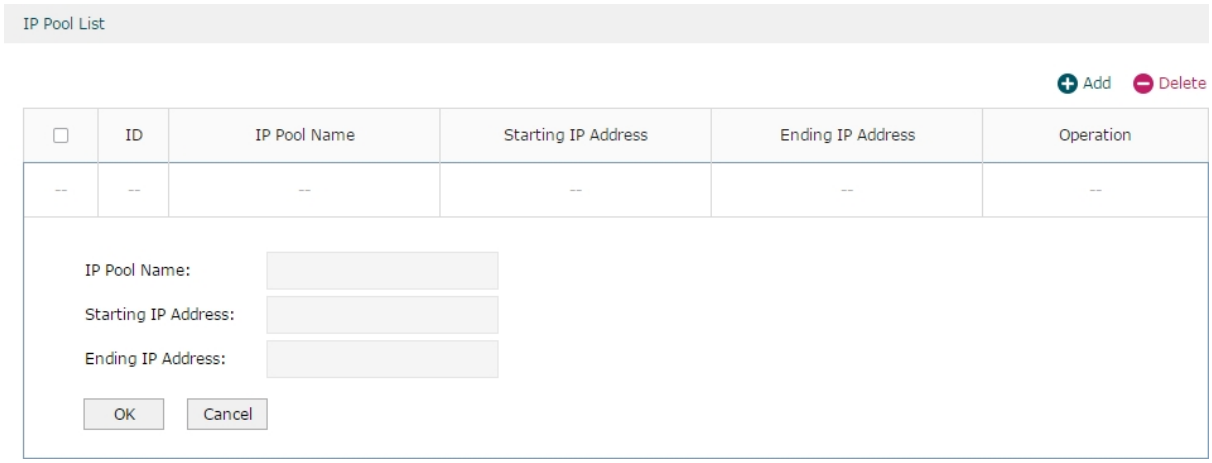
규칙에서 참조하는 시간 범위 항목은 삭제할 수 없습니다.

5 VPN IP 풀 구성

VPN IP 풀에서는 L2TP VPN 및 PPTP VPN을 구성할 때 선택할 수 있는 옵션으로 표시되는 VPN IP 풀을 미리 설정할 수 있습니다. 항목을 생성한 후 다른 규칙에 적용할 수 있으므로 동일한 정보를 반복적으로 설정하지 않아도 됩니다.

환경설정 > VPN IP 풀 > VPN IP 풀 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 5-1 IP 풀 항목 추가



IP 풀을 추가하려면 다음 단계를 따르세요:

1) 이름을 입력하고 IP 풀의 시작 및 종료 IP 주소를 지정합니다.

IP 풀 이름	IP 풀의 이름을 입력합니다. 문자, 숫자 또는 밑줄만 사용할 수 있습니다.
시작 IP 주소/종료 IP 주소	시작 및 종료 IP 주소를 지정합니다. IP 풀의 범위는 기존 IP 풀과 겹칠 수 없습니다.

2) **확인을** 클릭합니다.

참고:

새로 생성된 IP 풀의 범위는 DHCP 풀 및 다른 기존 VPN IP 풀의 IP 범위와 겹칠 수 없습니다.

규칙에서 참조한 VPN IP 풀 항목은 규칙이 더 이상 해당 항목을 참조하지 않는 한 삭제할 수 없습니다.

6 Ser 바이스 유형 구성

서비스 유형에서는 방화벽에서 액세스 제어 규칙을 구성할 때 선택할 수 있는 일치 조건으로 표시되는 서비스 유형 항목을 정의할 수 있습니다. 회색으로 표시된 항목은 시스템에서 미리 정의한 서비스 유형이며 편집하거나 삭제할 수 없습니다. 사용 중인 서비스 유형이 목록에 없는 경우 다른 항목을 추가할 수 있습니다.

환경설정 **> 서비스 유형 > 서비스 유형** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 6-1 서비스 유형 목록

Service Type List

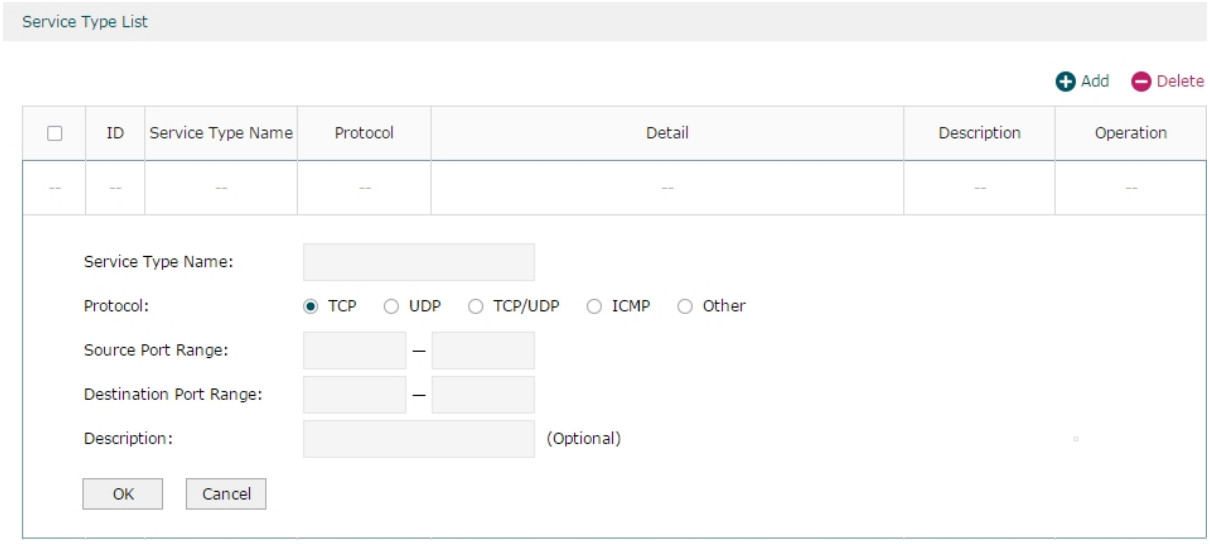
Add Delete

	ID	Service Type Name	Protocol	Detail	Description	Operation
--	1	ALL	0-255	---	ALL	---
--	2	FTP	TCP	Source Port = 0-65535; Destination Port = 21-21	FTP	---
--	3	SSH	TCP	Source Port = 0-65535; Destination Port = 22-22	SSH	---
--	4	TELNET	TCP	Source Port = 0-65535; Destination Port = 23-23	TELNET	---
--	5	SMTP	TCP	Source Port = 0-65535; Destination Port = 25-25	SMTP	---
--	6	DNS	UDP	Source Port = 0-65535; Destination Port = 53-53	DNS	---
--	7	HTTP	TCP	Source Port = 0-65535; Destination Port = 80-80	HTTP	---
--	8	POP3	TCP	Source Port = 0-65535; Destination Port = 110-110	POP3	---
--	9	SNTP	UDP	Source Port = 0-65535; Destination Port = 123-123	SNTP	---
--	10	H.323	TCP	Source Port = 0-65535; Destination Port = 1720-1720	H.323	---
--	11	ICMP_ALL	ICMP	Type =255; Code = 255	icmp	---
--	12	HTTPS	TCP	Source Port = 0-65535; Destination Port = 443-443	---	---

회색으로 표시된 항목은 시스템에서 미리 정의한 서비스 유형입니다. 서비스 유형이 목록에 없는 경우 다른 항목을 추가할 수 있습니다.

추가를 클릭하여 다음 페이지를 로드합니다.

그림 6-2 서비스 유형 항목 추가



서비스 유형 항목을 추가하려면 다음 단계를 따르세요:

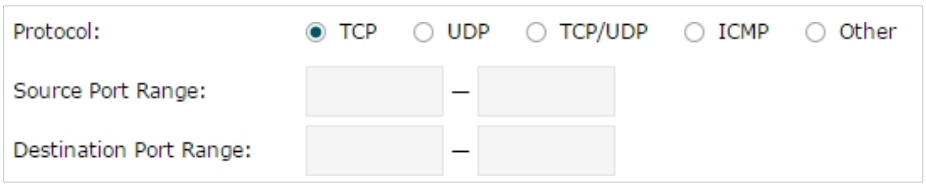
1) 서비스 유형의 이름을 입력합니다.

서비스 유형 이름	서비스 유형의 이름을 입력합니다. 문자, 숫자 또는 밑줄만 사용할 수 있습니다.

2) 서비스 유형에 맞는 프로토콜을 선택합니다. 미리 정의된 프로토콜에는 **TCP**, **UDP**, **TCP/UDP** 및 **ICMP가** 포함됩니다. 다른 프로토콜의 경우 **기타** 옵션을 선택합니다.

TCP, **UDP** 또는 TCP/UDP를 선택하면 다음 페이지가 표시됩니다.

그림 6-3 TCP/UDP 프로토콜



소스 포트 범위/대상 포트 범위	TCP 또는 UDP 패킷의 소스 포트와 대상 포트의 범위를 지정합니다. 소스 포트와 대상 포트가 모두 범위 내에 있는 패킷을 대상 패킷으로 간주합니다.

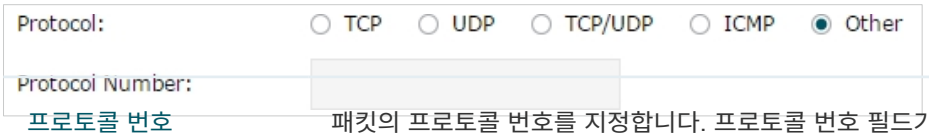
ICMP를 선택하면 다음 페이지가 표시됩니다.

그림 6-4 ICMP 프로토콜

유형/코드	ICMP 패킷의 유형과 코드를 지정합니다. 유형과 코드 필드가 모두 일치하는 ICMP 패킷을 대상 패킷으로 간주합니다.

기타를 선택하면 다음 페이지가 나타납니다.

그림 6-5 기타 프로토콜



프로토콜 번호	패킷의 프로토콜 번호를 지정합니다. 프로토콜 번호 필드가 일치하는 패킷을 대상 패킷으로 간주합니다.

3) (선택 사항) 서비스 유형을 쉽게 식별할 수 있도록 이 서비스 유형에 대한 간단한 설명을 입력합니다.

4) **확인을** 클릭합니다.

참고:

규칙에서 참조하는 서비스 유형 항목은 규칙이 더 이상 해당 항목을 참조하지 않는 한 삭제할 수 없습니다.

파트 6

전송 구성

챕터

7. 라우팅 구성

8. 구성 예제

1 Tr 입학

1.1 개요

전송 기능은 네트워크에 대한 다양한 트래픽 제어 수단을 제공합니다. 실제 필요에 따라 전송 기능을 구성할 수 있습니다.

1.2 지원되는 기능

전송 모듈에는 NAT, 대역폭 제어, 세션 제한, 부하 분산 및 라우팅이 포함됩니다.

NAT

NAT(네트워크 주소 변환)는 프라이빗 IP와 퍼블릭 IP 간의 변환입니다. NAT는 여러 사설 호스트가 동시에 하나의 공용 IP를 사용하여 공용 네트워크에 액세스할 수 있는 방법을 제공하여 IP 주소 부족을 완화합니다. 또한, NAT는 LAN 호스트의 주소가 인터넷에 절대 나타나지 않기 때문에 LAN(로컬 영역 네트워크) 보안을 강화합니다. 공유기는 다음과 같은 NAT 기능을 지원합니다:

- 일대일 NAT

일대일 NAT는 개인 IP 주소와 공인 IP 주소 간의 관계를 생성합니다. 프라이빗 IP 주소가 있는 디바이스는 그에 해당하는 유효한 공용 IP 주소를 통해 액세스할 수 있습니다.

- 가상 서버

로컬 네트워크에 서버를 구축하여 인터넷에서 공유하려는 경우, 가상 서버는 서비스를 구현하여 인터넷 사용자에게 제공할 수 있습니다. 동시에 가상 서버는 다른 서비스가 인터넷에서 보이지 않기 때문에 로컬 네트워크를 안전하게 유지할 수 있습니다.

- 포트 트리거링

포트 트리거링은 특정 포트의 트래픽을 로컬 네트워크의 특정 서버로 동적으로 전달하는 데 사용되는 기능입니다. 로컬 네트워크의 호스트가 트리거링 포트에 대한 연결을 시작하면 후속 연결을

위해 모든 외부 포트가 열립니다. 라우터는 호스트의 IP 주소를 기록할 수 있으며, 인터넷의 데이터가 외부 포트로 돌아오면 라우터는 이를 해당 호스트로 전달할 수 있습니다. 포트 트리거링은 주로 온라인 게임, VoIP, 비디오 플레이어 등에 적용됩니다.

- NAT-DMZ

로컬 네트워크에서 PC를 DMZ(비무장지대) 호스트로 설정하면 인터넷에 완전히 노출되어 내부 호스트와 외부 호스트 간의 무제한 양방향 통신을 실현할 수 있습니다. DMZ 호스트는 모든 포트가 열린 가상 서버가 됩니다. IP 카메라 및 데이터베이스 소프트웨어와 같은 일부 특수 애플리케이션에서 어떤 포트를 열어야 할지 명확하지 않은 경우 PC를 DMZ 호스트로 설정할 수 있습니다.

- ALG

FTP, H.323, SIP, IPSec 및 PPTP와 같은 일부 특수 프로토콜은 ALG(애플리케이션 계층 게이트웨이) 서비스가 활성화된 경우에만 제대로 작동합니다.

대역폭 제어

대역폭 제어 기능을 사용하면 다양한 데이터 흐름을 제한하는 규칙을 구성할 수 있습니다. 이를 통해 대역폭을 합리적으로 활용하여 네트워크 성능을 최적화할 수 있습니다.

서비스 품질

서비스 품질에서는 다양한 데이터 흐름을 제한하는 규칙을 구성할 수 있습니다.

세션 제한

세션 제한 기능은 특정 소스가 사용할 수 있는 세션 수를 제한합니다. 이 기능을 사용하면 한 번에 너무 많은 세션을 사용하는 일부 호스트로 인해 네트워크 리소스와 대역폭이 고갈되는 것을 방지하여 네트워크 성능을 최적화할 수 있습니다.

부하 분산

WAN 포트의 트래픽 공유 모드를 구성하여 서버의 리소스 사용률과 처리 능력을 최적화할 수 있습니다. 라우터는 항상 온라인 네트워크를 유지하기 위해 끊긴 회선의 모든 새 세션을 자동으로 다른 회선으로 전환합니다.

라우팅

정책 라우팅 규칙 및 정적 라우팅을 구성할 수 있습니다.

정책 라우팅은 네트워크 관리자가 정의한 정책에 따라 라우팅을 보다 정확하게 제어할 수 있는 방법을 제공합니다.

정적 라우팅은 라우팅 테이블에 에이징되지 않은 항목을 추가하여 수동으로 구성하는 라우팅의 한 형태입니다. 수동으로 구성된 라우팅 정보는 라우터가 데이터 패킷을 특정 목적지로 전달하도록 안내합니다.

2 NA T 구성

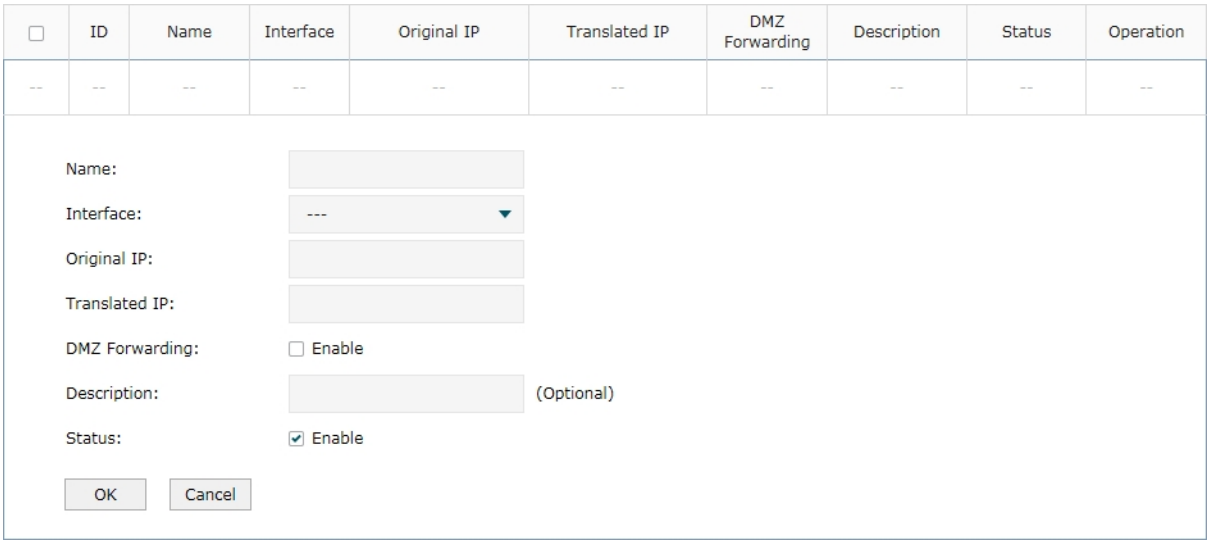
NAT 구성을 사용하면 가능합니다:

- 일대일 NAT를 구성합니다.
- 가상 서버를 구성합니다.
- 포트 트리거링을 구성합니다.
- NAT-DMZ를 구성합니다.
- ALG를 구성합니다.

2.1 일대일 NAT 구성

전송 > NAT > 일대일 NAT 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로 드 됩 니 다 .

그림 2-1 일대일 NAT 구성하기



일대일 NAT를 구성하려면 다음 단계를 따르세요:

1) 일대일 NAT 규칙의 이름을 지정하고 기타 관련 매개변수를 구성합니다.

인터페이스	연결 유형이 고정 IP인 경우에만 규칙의 유효 인터페이스를 지정합니다. 여러 포트를

	선택하면 선택한 모든 포트에 해당 항목이 동시에 적용됩니다.
원래 IP	규칙의 개인 IP 주소를 지정합니다. 원래 IP 주소는 브로드캐스트 주소와 LAN 인터페이스의 IP 주소가 될 수 없습니다.

번역된 IP	규칙의 공인 IP 주소를 지정합니다. 변환된 IP 주소는 브로드캐스트 주소와 WAN 인터페이스의 IP 주소가 될 수 없습니다.
DMZ 포워딩	DMZ 포워딩을 사용하려면 이 확인란을 선택합니다. DMZ 포워딩이 활성화된 경우 변환된 IP 주소로 전송된 패킷은 원래 IP 주소의 호스트로 전달됩니다.
설명	(선택 사항) 관리를 쉽게 할 수 있도록 규칙에 대한 간단한 설명을 입력합니다. 상
태	확인란을 선택하면 규칙이 활성화됩니다.

2) **확인을** 클릭합니다.

참고:

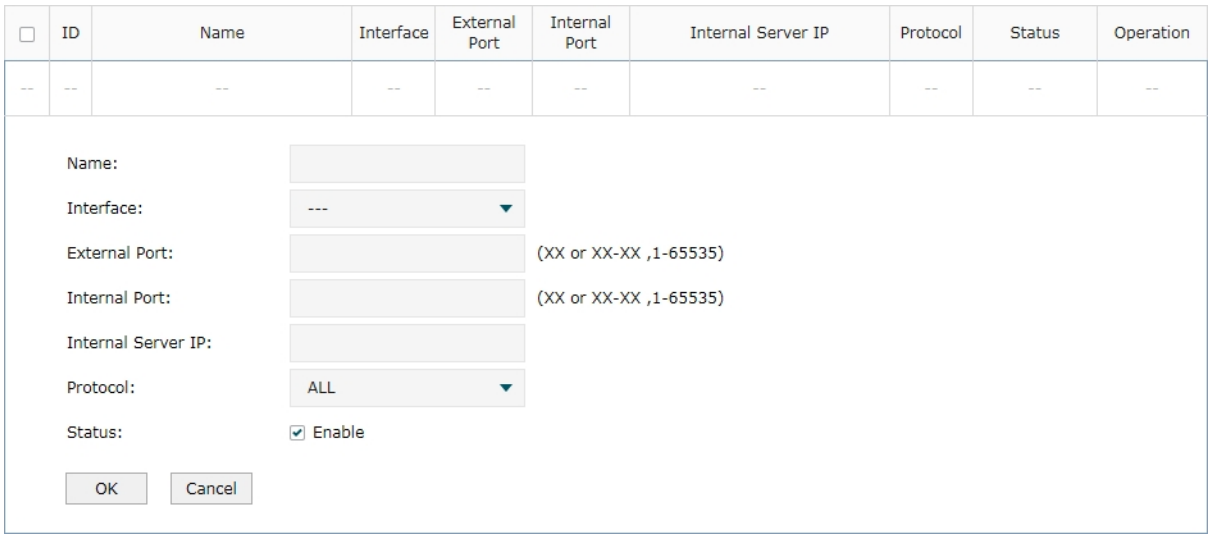
일대일 NAT는 WAN의 연결 유형이 고정 IP인 경우에만 적용됩니다.

NAT를 위한 개방형 포트를 설정할 때, 예약 포트(1723/1701은 PPTP/L2TP를 위해 예약된 포트, 1194는 OpenVPN을 위해 예약된 포트 및 예약한 특정 포트)를 선택하지 마세요.

2.2 가상 서버 구성

전송 > NAT > 가상 서버 메뉴를 선택하고 추가를 클릭하면 다음 페이지가 로드됩니다.

그림 2-2 가상 서버 구성하기



가상 서버를 구성하려면 다음 단계를 따르세요:

1) 가상 서버 규칙의 이름을 지정하고 기타 관련 매개변수를 구성합니다.

인터페이스	규칙의 유효 인터페이스를 지정합니다. 여러 포트를 선택하면 선택한 모든 포트에 해당 항목이 동시에 적용됩니다.
외부 포트	외부 네트워크 액세스를 위한 라우터의 서비스 포트 또는 포트 범위를 입력합니다. 포트 또는 포트 범위는 다른 가상 서버 규칙의 포트 또는 포트 범위와 겹칠 수 없습니다.

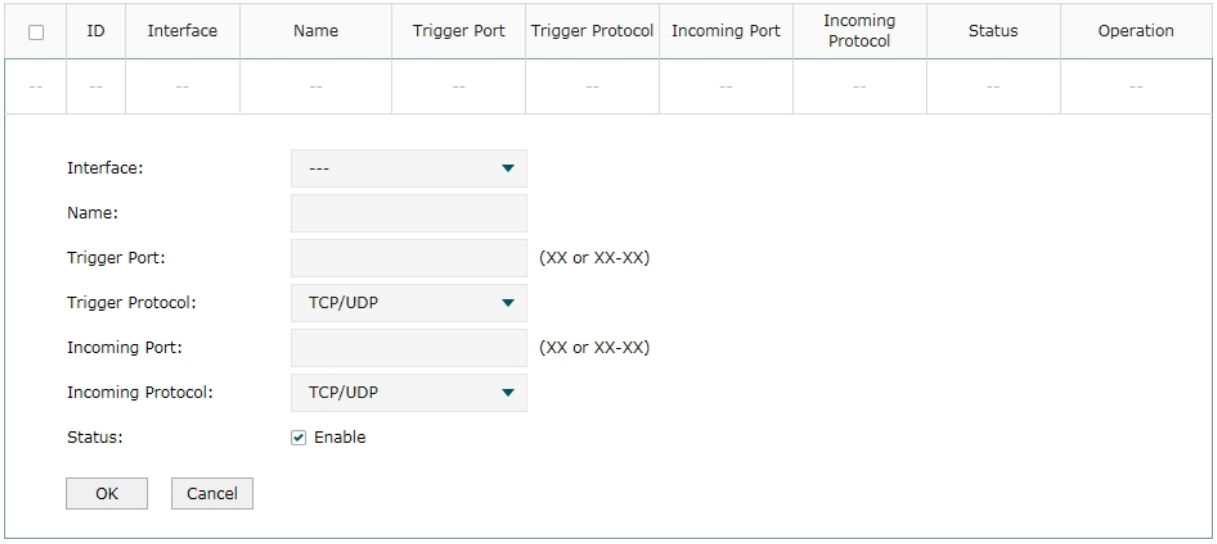
내부 포트	외부 네트워크 액세스를 위한 라우터의 서비스 포트 또는 포트 범위를 입력합니다. 포트 또는 포트 범위는 다른 가상 서버 규칙의 포트 또는 포트 범위와 겹칠 수 없습니다.
내부 서버 IP	항목에 대해 지정된 내부 서버의 IP 주소를 입력합니다. 인터넷에서 지정된 LAN 포트로의 모든 요청이 이 호스트로 리디렉션됩니다.
프로토콜	규칙에 사용되는 프로토콜을 지정합니다. **모두:** 데이터 패킷은 TCP 또는 UDP 프로토콜을 기반으로 전송됩니다. **TCP:** 데이터 패킷은 TCP 프로토콜을 기반으로 전송됩니다. **UDP:** 데이터 패킷은 UDP 프로토콜을 기반으로 전송됩니다.
상태	규칙을 활성화하려면 확인란을 선택합니다.

2) **확인을** 클릭합니다.

2.3 포트 트리거링 구성

전송 > NAT > 포트 트리거링 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 2-3 포트 트리거링 구성하기



포트 트리거링을 구성하려면 다음 단계를 따르세요:

1) 포트 트리거링 규칙의 이름을 지정하고 기타 관련 파라미터를 구성합니다.

인터페이스	규칙의 유효 인터페이스를 지정합니다. 여러 포트를 선택하면 선택한 모든 포트에 해당 항목이 동시에 적용됩니다.
트리거 포트	데이터가 흘러나오는 트리거 포트 또는 포트 범위를 입력합니다. 각 항목은 최대 5개의 트리거 포트 그룹을 지원합니다. 예를 들어 1 또는 1-2를 입력할 수 있습니다. 포트 또는 포트 범위는 다른 포트 트리거링 규칙의 포트 또는 포트 범위와 겹칠 수 없습니다.

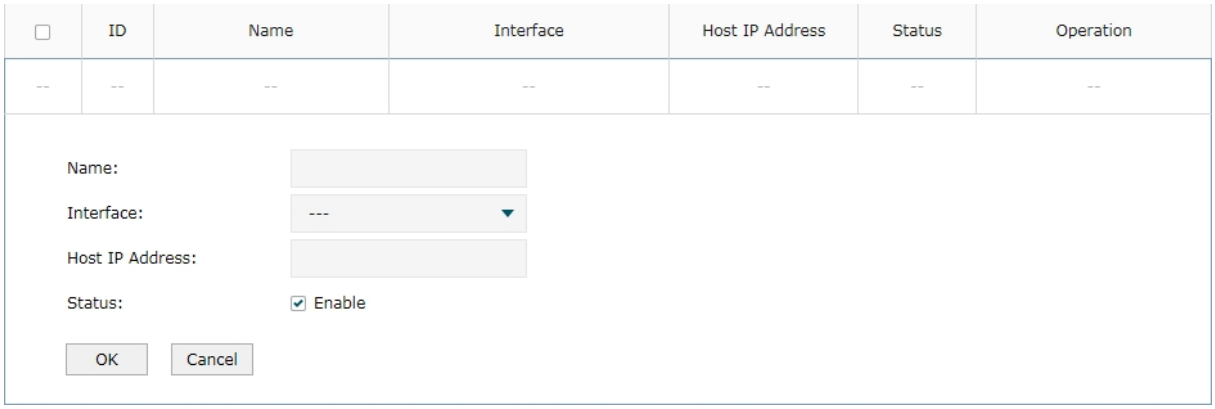
트리거 프로토콜	트리거 포트의 프로토콜을 지정합니다. **모두:** 데이터 패킷은 TCP 또는 UDP 프로토콜을 기반으로 전송됩니다. **TCP:** 데이터 패킷은 TCP 프로토콜을 기반으로 전송됩니다. **UDP:** 데이터 패킷은 UDP 프로토콜을 기반으로 전송됩니다.
수신 포트	데이터를 수신하는 수신 포트 또는 포트 범위를 입력합니다. 각 항목은 최대 5개의 수신 포트 그룹을 지원합니다. 예를 들어 1-2 또는 11-12를 입력할 수 있습니다. 포트 또는 포트 범위는 다른 포트 트리거링 규칙의 포트 또는 포트 범위와 겹칠 수 없습니다.
수신 프로토콜	수신 포트의 프로토콜을 지정합니다. **모두:** 데이터 패킷은 TCP 또는 UDP 프로토콜을 기반으로 전송됩니다. **TCP:** 데이터 패킷은 TCP 프로토콜을 기반으로 전송됩니다. **UDP:** 데이터 패킷은 UDP 프로토콜을 기반으로 전송됩니다.
상태	규칙을 활성화하려면 확인란을 선택합니다.

2) **확인을** 클릭합니다.

2.4 NAT-DMZ 구성

전송 > NAT > NAT-DMZ 메뉴를 선택하고 추가를 클릭하면 다음 페이지가 로드됩니다.

그림 2-4 NAT-DMZ 구성하기



NAT-DMZ를 구성하려면 다음 단계를 따르세요:

1) NAT-DMZ 규칙의 이름을 지정하고 기타 관련 매개변수를 구성합니다.

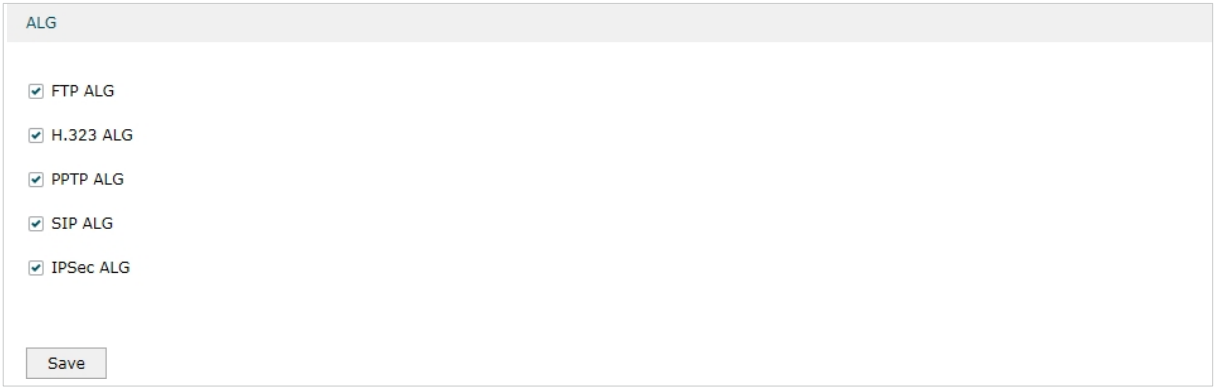
인터페이스	규칙의 유효 인터페이스를 지정합니다. 호스
트 IP 주소	NAT-DMZ의 호스트 IP 주소를 지정합니다. 상태 규
	칙을 사용하려면 확인란을 선택합니다.

2) **확인을** 클릭합니다.

2.5 ALG 구성

전송 > NAT > ALG 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 2-5 ALG 구성하기



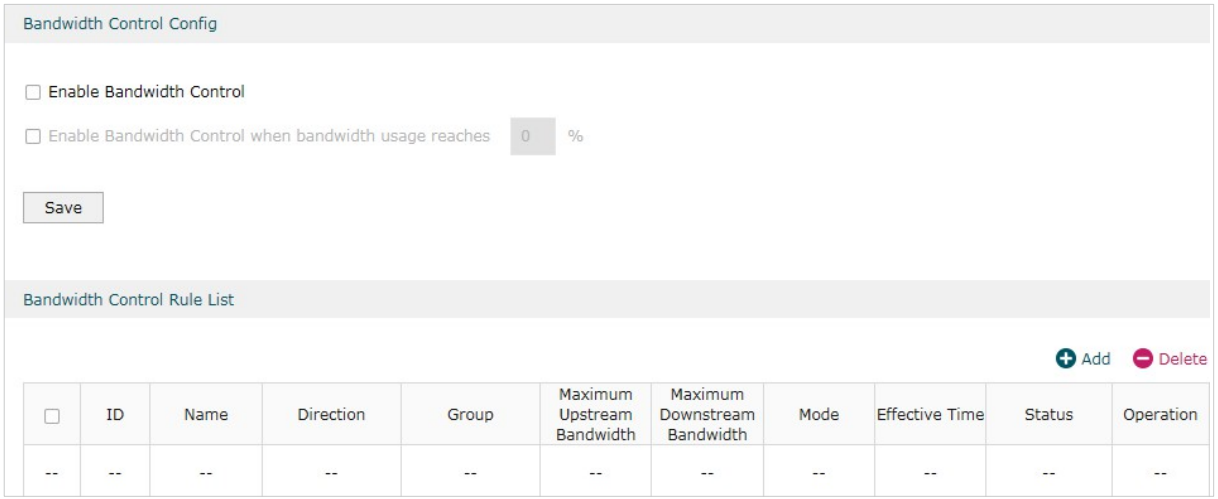
필요에 따라 관련 ALG를 활성화하고 **저장을** 클릭합니다.

3 대역폭 제어 구성

대역폭 제어는 다양한 데이터 흐름을 제한하는 규칙을 구성하여 대역폭을 제어하는 기능입니다. 이를 통해 네트워크 대역폭을 합리적으로 분배하고 활용할 수 있습니다.

전송 > 대역폭 제어 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 3-1 대역폭 제어 구성하기



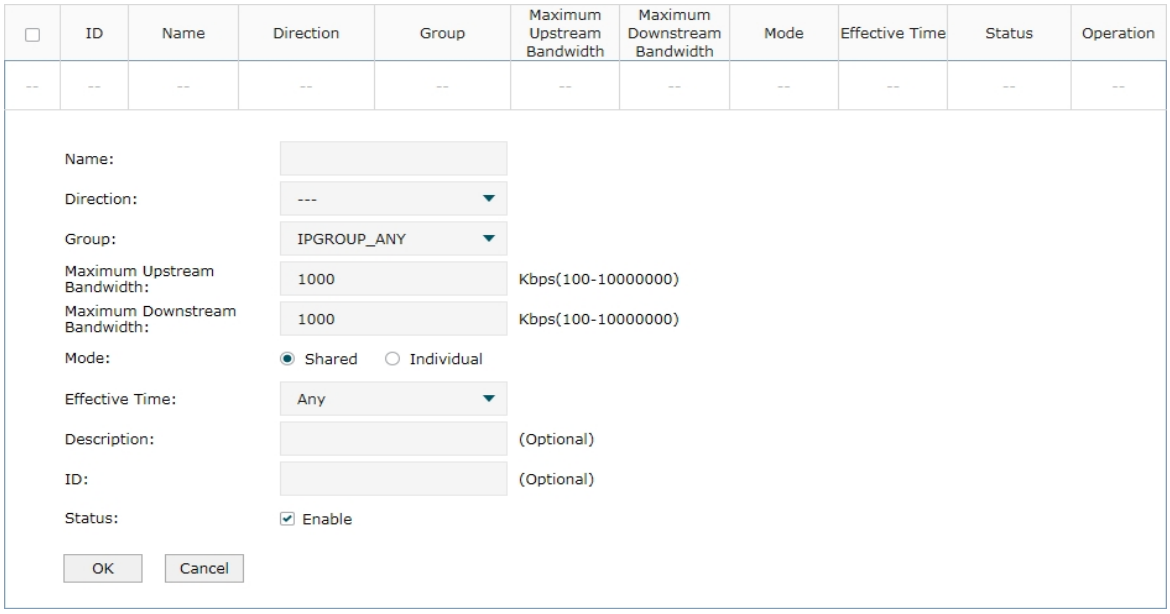
대역폭 제어 규칙을 구성하려면 다음 단계를 따르세요:

1) **대역폭 제어 구성** 섹션에서 대역폭 제어 기능을 전역으로 활성화합니다.

대역폭 제어 활성화	확인란을 선택하면 전역적으로 대역폭 제어를 활성화할 수 있습니다.
대역폭 제어 임계값	"대역폭 제어 활성화"를 선택하면 백분율을 지정할 수 있으며, 대역폭 사용량이 지정한 백분율에 도달할 때만 대역폭 제어가 적용됩니다.

2) **대역폭 제어 규칙 목록** 섹션에서 추가를 클릭하여 다음 페이지를 로드합니다.

그림 3-2 대역폭 제어 규칙 추가



대역폭 제어 규칙의 이름을 지정하고 기타 관련 매개변수를 구성합니다. 그런 다음 **확인을** 클릭합니다.

방향	규칙의 데이터 스트림 방향을 지정합니다.
그룹	드롭다운 목록에서 생성한 IP 그룹을 선택합니다. IPGROUP_ ANY를 선택하면 모든 클라이언트에 규칙이 적용됩니다. 원하는 IP 그룹이 생성되지 않은 경우 **환경설정 > IP 그룹** 페이지로 이동하여 생성합니다.
최대 업스트림 대역폭	특정 사용자가 라우터를 통해 인터넷으로 트래픽을 전송할 수 있는 업스트림 대역폭의 한도를 지정합니다.
최대 다운스트림 대역폭	특정 사용자가 라우터를 통해 인터넷에서 트래픽을 수신할 수 있는 다운스트림 대역폭의 한도를 지정합니다.
모드	컨트롤러 사용자의 대역폭 제어 모드를 선택합니다. **공유: 공유:** 모든 사용자의 총 대역폭이 업스트림 및 다운스트림 대역폭에서 지정된 값과 동일합니다. **개인:** 각 사용자의 대역폭은 업스트림 및 다운스트림 대역폭에서 지정된 값과 동일합니다 .
유효 시간	규칙이 적용되는 시간을 지정합니다. 아무거나 선택하면 항상 적용됩니다. 원하는 시간 범위가 구성되지 않은 경우 **환경설정 > 시간 범위** 페이지로 이동하여 시간 범위를 만듭니다.

설명	규칙에 대한 간단한 설명을 입력합니다.
ID	규칙에 번호를 지정하여 목록을 재정렬합니다.
상태	규칙을 활성화하려면 확인란을 선택합니다.

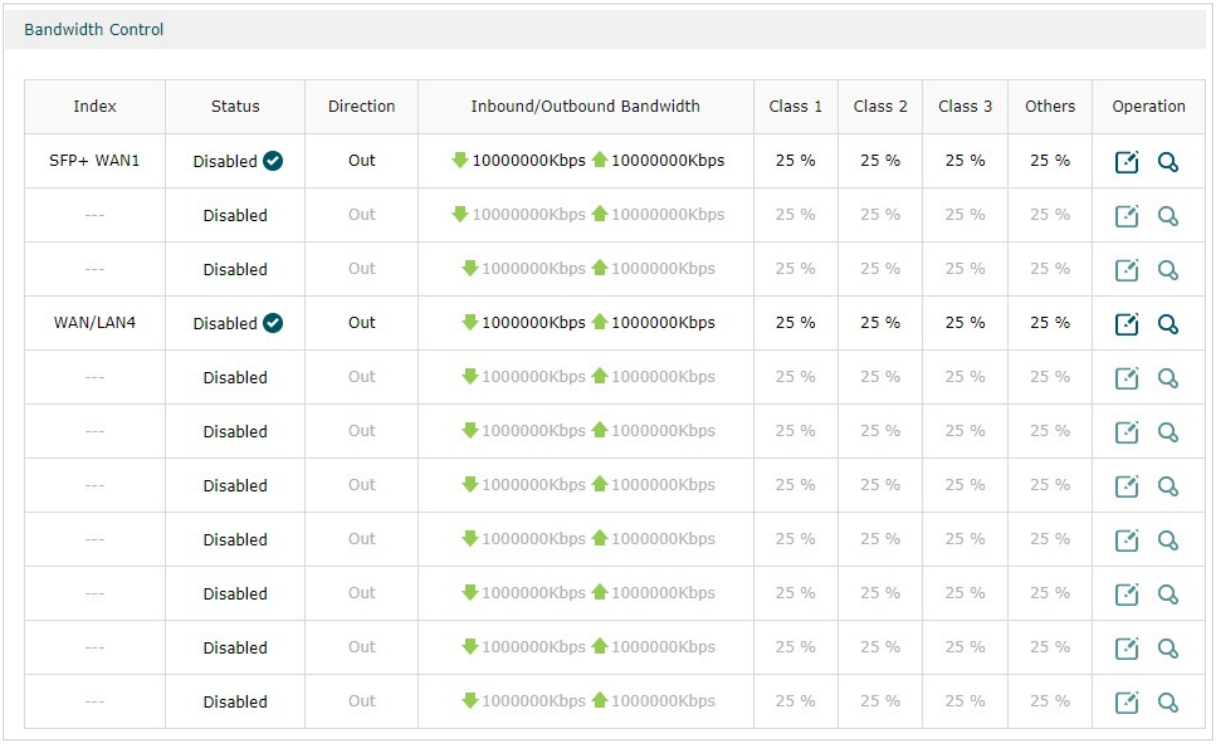
4 서비스 품질 구성

4.1 대역폭 제어 구성

대역폭 제어를 사용하면 다양한 데이터 흐름을 제한하는 규칙을 구성할 수 있습니다. 이렇게 하면 대역폭을 합리적으로 활용하여 네트워크 성능을 최적화할 수 있습니다.

전송 > 서비스 품질 > 대역폭 제어 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 4-1 대역폭 제어 구성하기

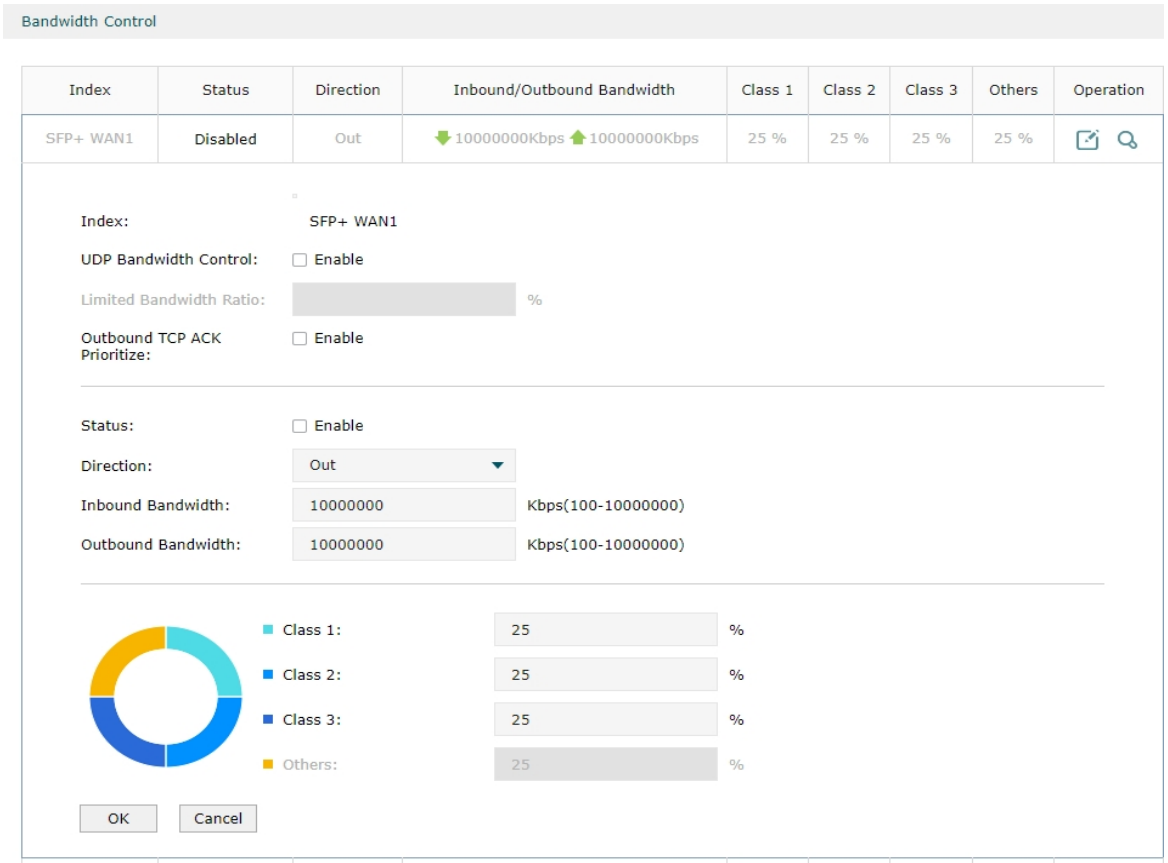


대역폭 제어 규칙을 구성하려면 다음 단계를 따르세요:

1) WAN 인터페이스를 선택하고 **대역폭 제어** 기능을 활성화합니다.

2) **작업** 열에서 수정을 클릭하여 다음 페이지를 로드합니다.

그림 4-2 대역폭 제어 규칙 편집



관련 매개변수를 구성합니다. 그런 다음 **확인을** 클릭합니다.

색인	WAN 포트를 표시합니다. 포트가 활성화된 경우에만 WAN 포트에 대한 QoS 규칙을 구성할 수 있습니다.
UDP 대역폭 제어	UDP 대역폭 제어를 사용하려면 확인란을 선택합니다.
제한된 대역폭 비율	UDP 대역폭 제어가 활성화된 경우 각 클래스에서 UDP 트래픽에 허용되는 최대 대역폭 비율을 지정합니다.
아웃바운드 TCP ACK 우선순위 지정	이 확인란을 선택하면 아웃바운드 TCP ACK 패킷의 우선순위를 지정할 수 있습니다.
상태	현재 항목에 대해 QoS를 사용하거나 사용하지 않도록 설정합니다.
방향	제어되는 트래픽의 방향을 지정합니다. "Out"은 패킷을 보내는 제어를 의미합니다. "In"은 패킷 수신을 의미합니다. "모두"는 둘 다 제어됨을 의미합니다.
인바운드/	아웃바운드 대역폭

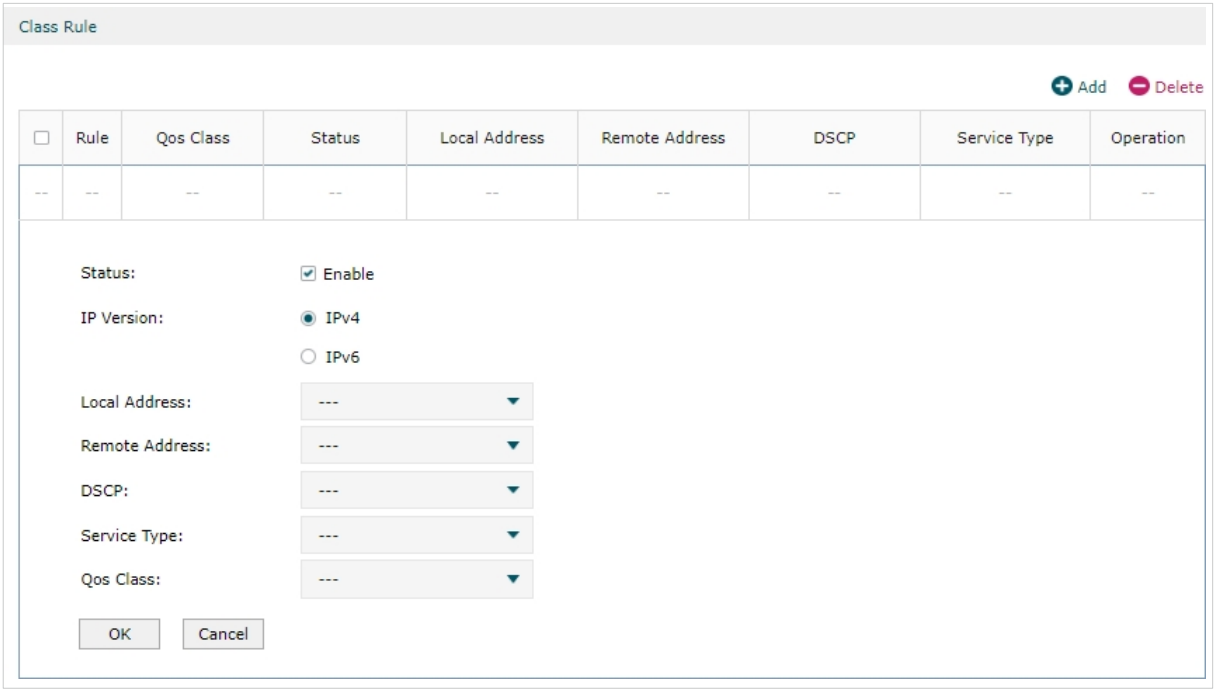
인바운드/아웃바운드	대역폭의 최대 임계값을 입력합니다.
클래스1/클래스2/클래스3/기타	클래스1, 클래스2, 클래스3 및 WAN 포트를 통해 흐르는 기타 트래픽에 할당된 WAN 대역폭의 비율을 지정합니다.

4.2 클래스 규칙 구성

클래스 규칙에서는 클래스 규칙을 추가하거나 삭제할 수 있습니다. 규칙은 규칙 시퀀스 번호에 따라 위에서 아래로 매칭됩니다. 트래픽이 규칙과 일치하면 해당 클래스에 할당되며 계속 아래로 일치하지 않습니다.

전송 > 서비스 품질 > 클래스 규칙 메뉴를 선택하고 **추가를** 클릭하여 다음 페이지를 로드합니다.

그림 4-3 클래스 규칙 구성하기



관련 매개변수를 구성합니다. 그런 다음 **확인을** 클릭합니다.

상태	확인란을 선택하여 규칙을 활성화합니다.
IP 버전	프로토콜 버전을 지정합니다: IPv4 또는 IPv6.
로컬 주소	트래픽의 소스 IP 주소와 일치합니다. IPv4 프로토콜의 경우 환경설정 > IP 그룹 모듈에서 구성된 IP 그룹 개체를 사용할 수 있습니다. IPv6 프로토콜의 경우 환경설정 > IPv6 그룹 모듈에서 구성된 IPv6 그룹 개체를 사용할 수 있습니다. QoS는 LAN > LAN의 트래픽에는 적용되지 않습니다. 클래스 규칙을 구성할 때 로컬 주소와 원격 주소는 LAN 측에서 동시에 IPGROUP을 선택할 수 없습니다.
원격 주소	트래픽의 대상 IP 주소를 일치시킵니다. IPv4 프로토콜의 경우 환경설정 > IP 그룹 모듈에서 구성된 IP 그룹 개체를 사용할 수 있습니다. IPv6 프로토콜의 경우 환경설정 > IPv6 그룹 모듈에서 구성된 IPv6 그룹 개체를 사용할 수 있습니다. QoS는 LAN >

LAN의 트래픽		에는 적용되지 않습니다. 클래스 규칙을 구성할 때 로컬 주소와 원격 주소는 LAN 측에서 동시에 IPGROUP을 선택할 수 없습니다.
	DSCP	트래픽의 DSCP 값과 일치합니다.

서비스 유형	트래픽의 포트 번호와 일치시킵니다. 기본 설정 > 서비스 유형 모듈에 정의된 서비스 유형 개체를 선택합니다.
QoS 클래스	규칙을 충족하는 트래픽 카테고리를 선택합니다.

4.3 VoIP 우선순위 설정 구성

VoIP SIP/RTP 트래픽에 대해 최우선 순위를 설정할 수 있습니다.

전송 > 서비스 품질 > VoIP 우선순위 지정 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 4-4 VoIP 우선순위 설정 구성하기

관련 매개변수를 구성합니다. 그런 다음 **저장을** 클릭합니다.

VoIP SIP/RTP에 최우선 순위 사용 설정하기	확인란을 선택하면 VoIP 트래픽 우선 순위 지정이 활성화됩니다.
SIP UDP 포트	VoIP 트래픽의 UDP 포트 ID를 입력합니다.

4.4 태그 우선순위 설정 구성

서로 다른 클래스의 트래픽에 대해 DSCP 또는 우선순위 값을 추가할 수 있습니다.

전송 > 서비스 품질 > 아웃바운드 트래픽 태그 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 4-5 태그 우선순위 설정 구성하기

원하는 클래스의 확인란을 선택하고 DSCP 또는 우선순위 값을 선택합니다. 그런 다음 **저장을** 클릭합니다.

5 세션 제한 구성

세션 제한 구성을 완료하려면 다음 단계를 따르세요:

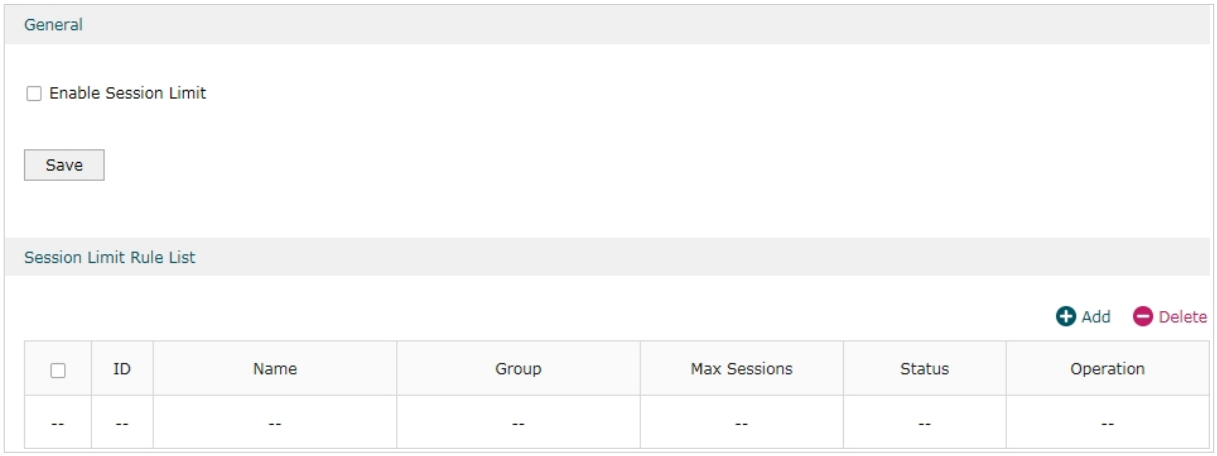
1) 세션 제한을 구성합니다.

2) 세션 제한 정보를 확인합니다.

5.1 세션 제한 구성

전송 > 세션 제한 > 세션 제한 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 5-1 세션 제한 구성하기

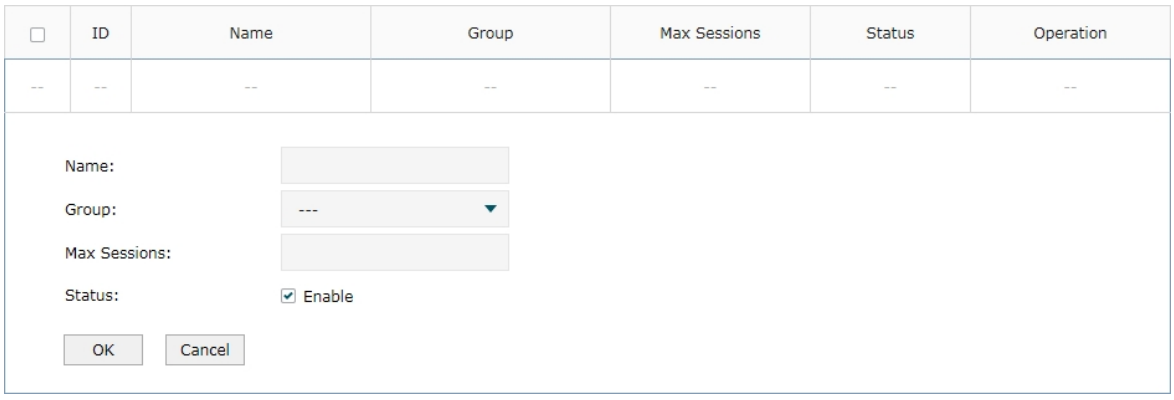


세션 제한 규칙을 구성하려면 다음 단계를 따르세요:

1) **일반** 섹션에서 세션 제한 기능을 전역으로 활성화합니다.

2) **세션 제한 규칙 목록** 섹션에서 추가를 클릭하여 다음 페이지를 로드합니다.

그림 5-2 세션 제한 규칙 추가



세션 제한 규칙의 이름을 지정하고 기타 관련 매개변수를 구성합니다. 그런 다음 **확인을** 클릭

합니다.

그룹	규칙이 적용될 주소 그룹을 지정합니다. 여기서 참조하는 IP 그룹은 **환경설정 > IP 그룹** 페이지에서 만들 수 있습니다.
최대 세션	LAN 호스트가 사용할 수 있는 최대 세션 수를 입력합니다. 소스의 세션 수가 최대값을 초과하면 라우터가 세션을 제한합니다.
상태	규칙을 활성화하려면 확인란을 선택합니다.

5.2 세션 제한 정보 보기

전송 > 세션 제한 > 세션 모니터 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 5-3 세션 제한 정보 보기

세션 제한이 설정된 호스트의 세션 제한 정보를 확인합니다. 세션 제한이 설정된 호스트의 **새로** 고침 버튼을 눌러 최신 정보를 확인합니다.

6 L oad 밸런싱 구성

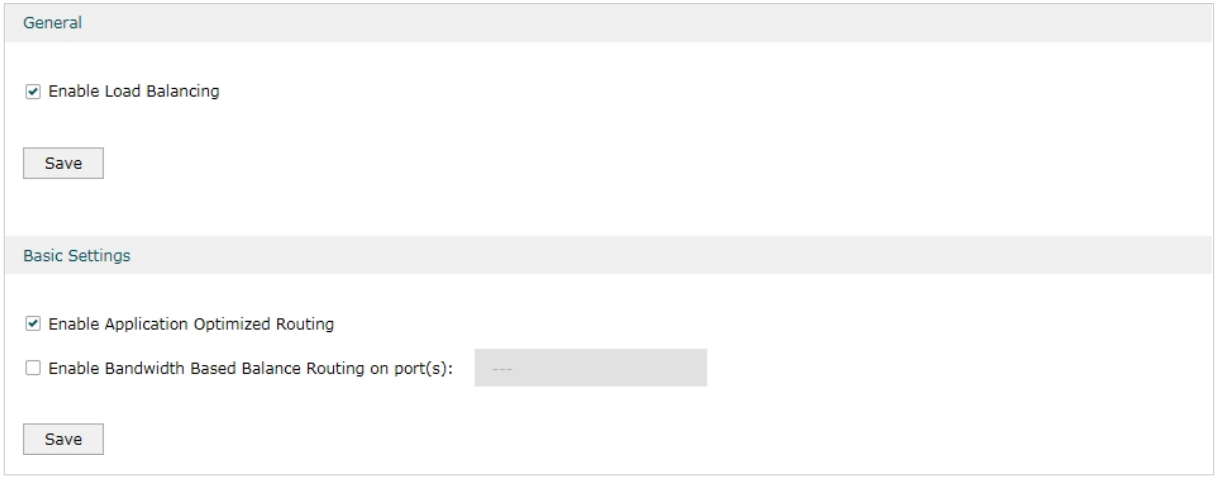
로드 밸런싱 구성을 사용하면 가능합니다:

- 부하 분산 구성
- 링크 백업 구성
- 온라인 탐지 구성

6.1 부하 분산 구성

전송 > 부하 분산 > 기본 설정 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 6-1 부하 분산 구성



부하 분산을 구성하려면 다음 단계를 따르세요:

1) **일반** 섹션에서 로드 밸런싱 기능을 전역으로 활성화하고 **저장을** 클릭합니다.

2) **기본 설정** 섹션에서 로드 밸런싱에 적합한 방법을 선택하고 **저장을** 클릭합니다.

애플리케이션 최적화 라우팅 사용	애플리케이션 최적화 라우팅을 활성화하면 라우터는 패킷의 소스 IP 주소와 목적지 IP 주소(또는 목적지 포트)를 전체적으로 고려하고 패킷이 통과하는 WAN 포트를 기록합니다. 그런 다음 소스 IP 주소와 목적지 IP 주소(또는 목적지 포트)가 동일한 패킷은 기록된 WAN 포트로 전달됩니다. 이 기능은 다중 연결된 애플리케이션이 제대로 작동하도록 보장합니다.

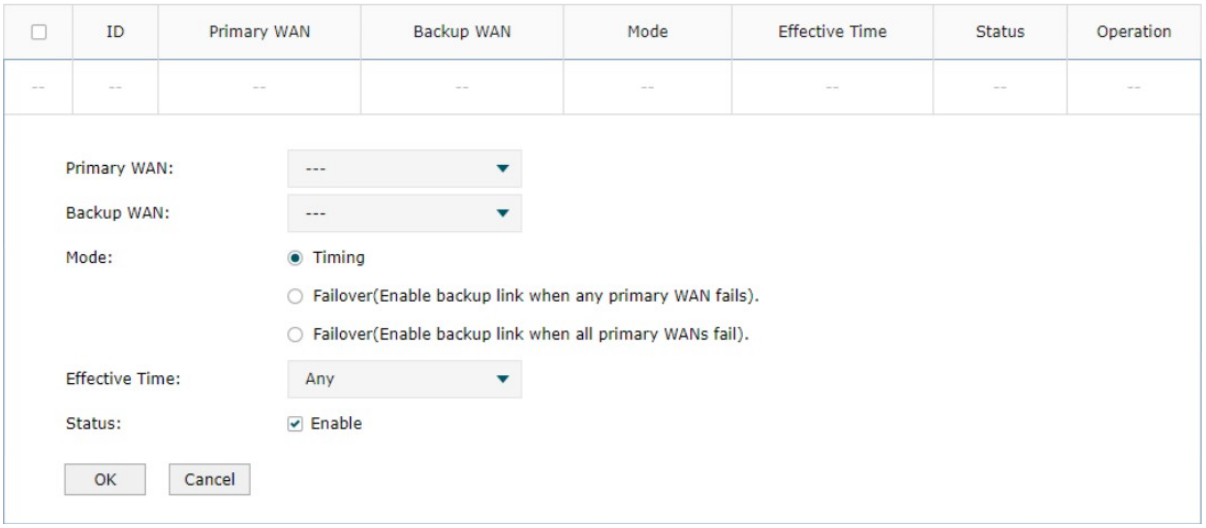
포트에서 대역폭 기반 밸런스 라우팅 활성화	드롭다운 목록에서 대역폭 기반 밸런스 라우팅을 사용할 WAN 포트를 선택합니다.

6.2 링크 백업 구성

링크 백업 기능을 사용하면 라우터가 끊긴 회선의 모든 새 세션을 자동으로 다른 회선으로 전환하여 항상 온라인 네트워크를 유지합니다.

전송 > 부하 분산 > 링크 백업 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 6-2 링크 백업 규칙 구성하기



이 페이지에서 다음 매개변수를 구성하고 **확인을** 클릭합니다.

기본 WAN	기본 WAN 포트를 지정합니다. 하나의 기본 WAN 포트를 선택하거나 여러 개의 기본 WAN 포트를 선택하여 부하 분산을 수행할 수 있습니다.
백업 WAN	지정한 조건에서 기본 WAN 포트의 트래픽을 백업할 백업 WAN 포트를 지정합니다.
모드	모드를 타이밍 또는 장애 조치로 지정합니다. **타이밍**: 지정된 유효 시간에 도달하면 링크 백업이 활성화됩니다. 기본 WAN의 모든 트래픽은 유효 시간이 시작될 때 백업 WAN으로 전환되고, 백업 WAN의 트래픽은 유효 시간이 종료될 때 기본 WAN으로 전환됩니다. **장애 조치(기본 WAN에 장애가 발생하면 백업 링크 사용)**: 기본 WAN에 장애가 발생하면 링크 백업이 활성화됩니다. 백업 WAN에서 로드 밸런싱이 활성화됩니다. 장애가 발생한 기본 WAN이 정상적으로 작동하면 백업 WAN의 트래픽이 기본 WAN으로 전환됩니다. **장애 조치(모든 기본 WAN이 실패할 때 백업 링크 사용)**: 모든 기본 WAN에 장애가 발생한 경우에만 링크 백업이 활성화됩니다. 기본 WAN의 모든 트래픽이 백업 WAN으로 전환됩니다. 모든 기본 WAN이 정상적으로 작동하면 백업 WAN의 트래픽이 기본 WAN으로 전환됩니다.

발효 시간 규칙이 발효될 시간을 지정합니다. 임의는 언제든지 적용됨을 의미합니다. 원하는 시간 범위를 구성하지 않은 경우 **환경설정 > 시간 범위** 페이지로 이동하여 생성하세요.

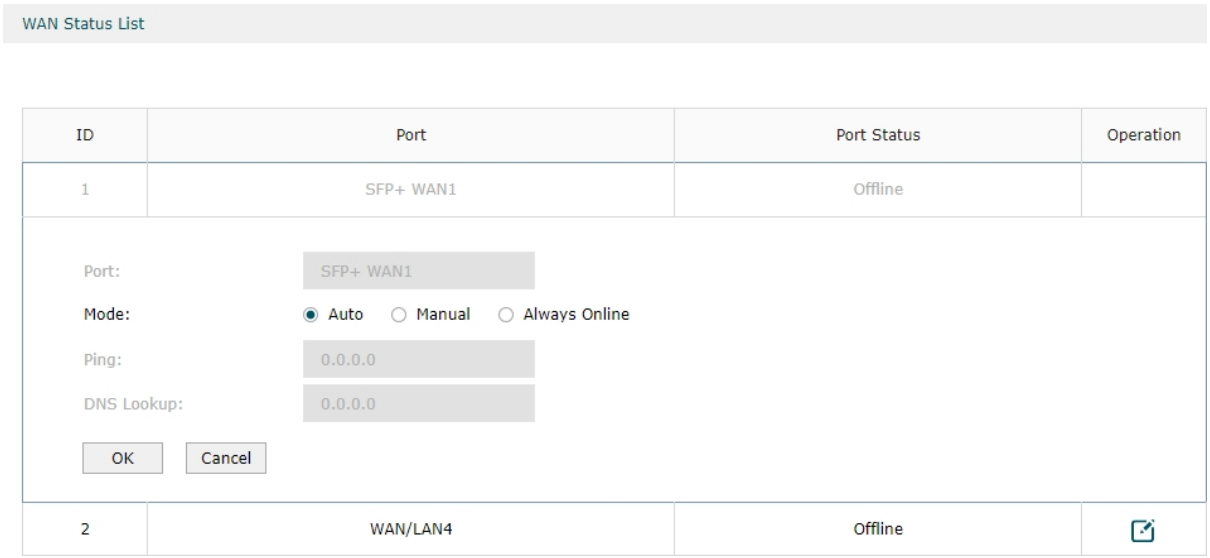
상태	규칙을 활성화하려면 확인란을 선택합니다.

6.3 온라인 탐지 구성

온라인 감지 기능을 사용하면 WAN 포트의 온라인 상태를 감지할 수 있습니다.

전송 > 부하 분산 > 온라인 탐지 메뉴를 선택하고 을 클릭하면 다음 페이지가 로드됩니다.

그림 6-3 온라인 탐지 구성하기



이 페이지에서 다음 매개변수를 구성하고 **확인을** 클릭합니다.

포트	WAN 포트의 이름을 표시합니다.
모드	온라인 감지 모드를 선택합니다. **자동:** 자동 모드에서는 WAN이 온라인 상태인지 여부를 감지하기 위해 WAN 포트의 DNS 서버가 DNS 조회 대상으로 선택됩니다. **수동:** 수동 모드에서는 PING 및 DNS 조회의 대상 IP 주소를 수동으로 구성하여 WAN이 온라인 상태인지 여부를 감지할 수 있습니다. **항상 온라인:** 항상 온라인 모드에서는 포트의 상태가 항상 온라인 상태가 됩니다.
Ping	"수동 모드"를 선택한 상태에서 Ping의 대상 IP를 지정합니다. 해당 포트는 해당 IP 주소를 Ping하여 WAN 포트가 온라인 상태인지 여부를 감지합니다. 0.0.0.0은 Ping 감지가 비활성화됨을 의미합니다.

DNS 조회수동	모드를 선택한 상태에서 DNS 서버의 IP 주소를 지정합니다. 해당 포트는 기본 도메인 이름을 사용하여 DNS 조회를 수행하여 WAN 포트가 온라인 상태인지 여부를 감지합니다. 0.0.0.0은 DNS 조회가 비활성화됨을 의미합니다.

7 R 외출 구성

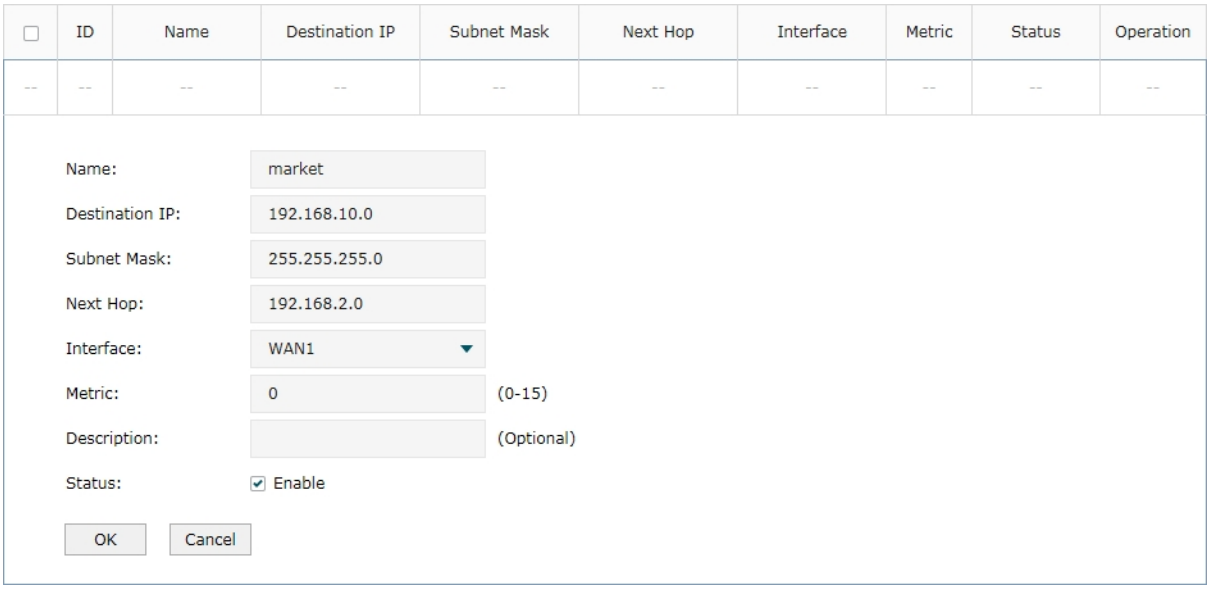
라우팅 구성을 사용하면 가능합니다:

- 정적 라우팅 구성
- 정책 라우팅 규칙 구성
- 라우팅 테이블 보기
- RIP 구성
- OSPF 구성

7.1 정적 라우팅 구성

전송 > 라우팅 > 정적 경로 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 7-1 정적 라우팅 구성하기



고정 경로 항목의 이름을 지정하고 기타 관련 매개변수를 구성합니다. 그런 다음 **확인을** 클릭합니다.

목적지 IP	경로가 연결되는 대상 IP 주소를 지정합니다. 서브넷 마

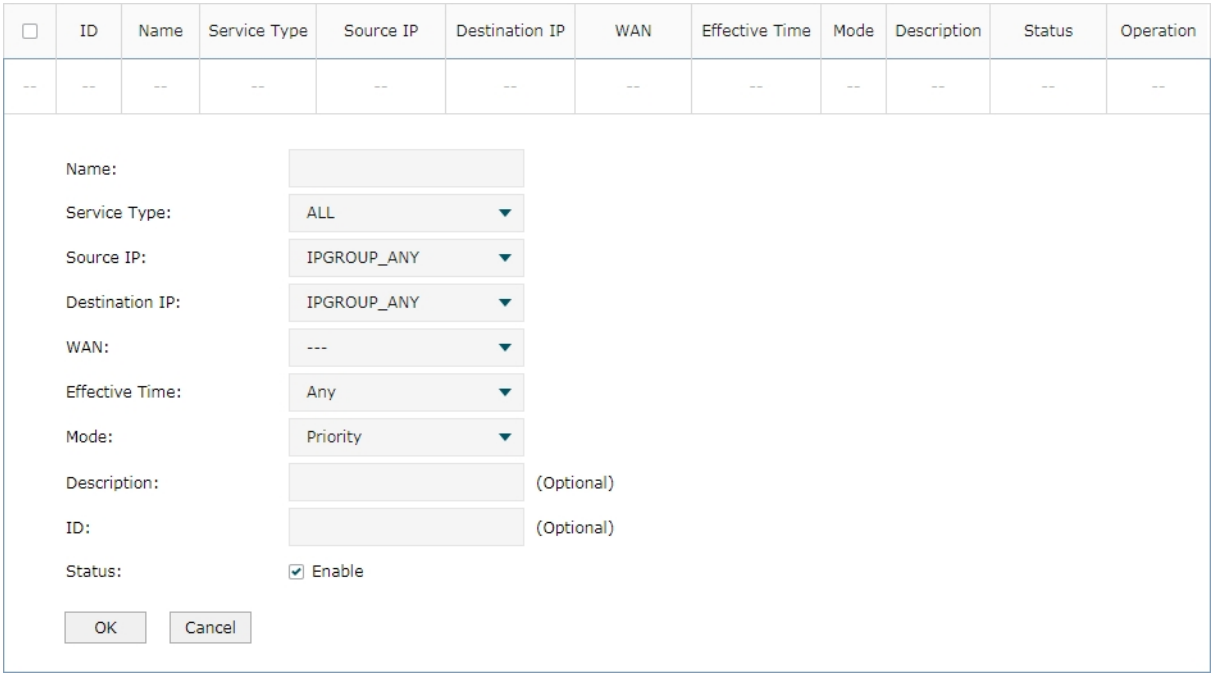
스크	대상 네트워크의 서브넷 마스크를 지정합니다.
다음 홉	다음에 패킷을 전송할 IP 주소를 지정합니다.

인터페이스	이 경로에 액세스할 수 있는 물리적 네트워크 인터페이스를 지정합니다.
메트릭	경로의 우선순위를 정의합니다. 값이 작을수록 우선순위가 높습니다. 기본값은 0입니다. 기본값을 유지하는 것이 좋습니다.
설명	규칙에 대한 간단한 설명을 입력합니
다. 상태	규칙을 사용하려면 확인란을 선택합니
다.	

7.2 정책 라우팅 구성

전송 > 라우팅 > 정책 라우팅 메뉴를 선택하고 추가를 클릭하면 다음 페이지가 로드됩니다.

그림 7-2 정책 라우팅 구성하기



정책 라우팅 항목의 이름을 지정하고 기타 관련 매개변수를 구성합니다. 그런 다음 **확인을** 클릭합니다.

서비스 유형	규칙에 대한 서비스 유형을 지정합니다.
소스 IP	규칙의 소스 IP 범위를 입력합니다. 0.0.0.0 - 0.0.0.0은 모든 IP가 허용됨을 의미합니다.
대상 IP	규칙의 대상 IP 범위를 입력합니다. 0.0.0.0 - 0.0.0.0은 모든 IP가 허용됨을 의미합니다.
WAN	규칙의 수신 포트를 지정합니다. 여러 포트를 선택하면 선택한 모든 포트에 동시에 항목이

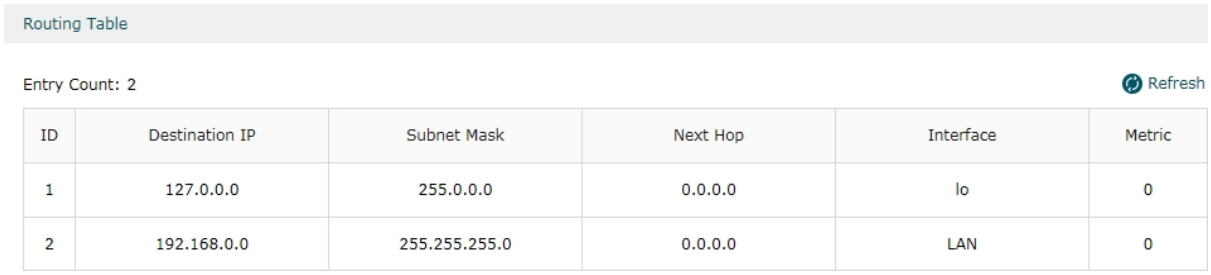
	적용됩니다.
유효 시간	규칙의 유효 시간을 지정합니다.

모드	규칙의 정책 라우팅 모드를 지정합니다. 우선순위: 우선순위 모드에서 규칙은 온라인 검색 결과에 따라 달라집니다. 지정한 WAN 포트가 온라인 상태이면 규칙이 적용됩니다. 지정한 모든 WAN 포트가 오프라인인 경우 규칙이 적용되지 않습니다. Only: 전용 모드에서는 WAN 포트 상태 또는 온라인 감지 결과에 관계없이 규칙이 항상 적용됩니다.
설명	규칙에 대한 간단한 설명을 입력합니
다. 상태 다.	규칙을 사용하려면 확인란을 선택합니

7.3 라우팅 테이블 보기

전송 > 라우팅 > 라우팅 테이블 메뉴를 선택하여 다음 페이지를 로드합니다.

그림 7-3 라우팅 테이블



라우팅 테이블에는 현재 경로 항목의 정보가 표시됩니다.

목적지 IP	경로가 연결되는 대상 IP 주소를 표시합니다. 서브넷 마스
크	대상 네트워크의 서브넷 마스크를 표시합니다.
다음 홉	패킷을 다음에 전송할 게이트웨이 IP 주소를 표시합니다. 인터페이스 이 경로
에 액세스할 수 있는 물리적 네트워크 인터페이스를 표시합니다.	
메트릭	대상 IP 주소에 도달하기 위한 메트릭을 표시합니다.

8 구성 예시

8.1 NAT 구성 예시

8.1.1 네트워크 요구 사항

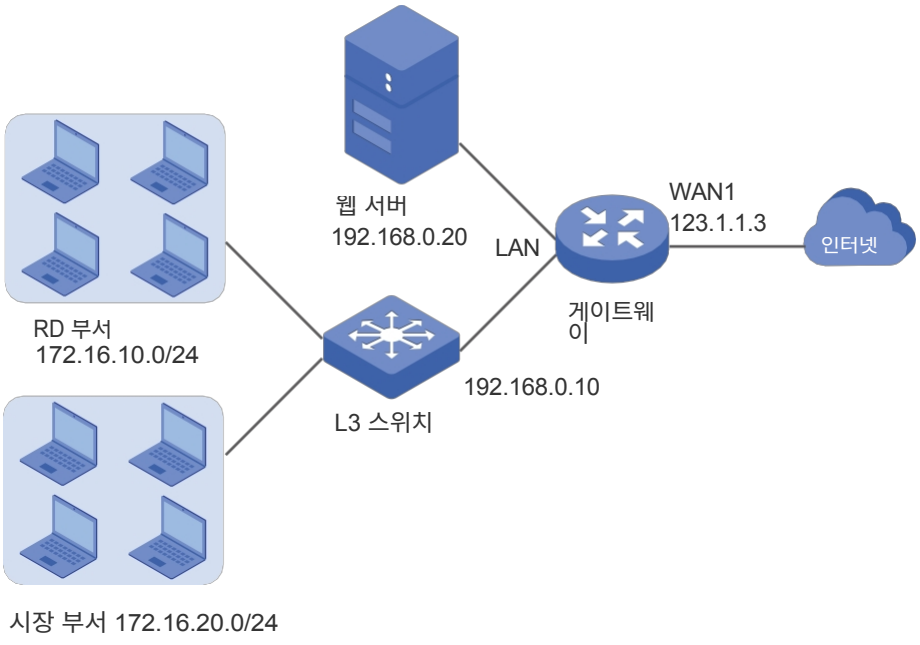
회사에는 두 개의 부서가 있습니다: 마케팅 부서와 R&D 부서입니다. 각 부서는 개별 서브넷에 할당됩니다. 회사에는 다음과 같은 요구 사항이 있습니다:

1) 두 부서는 동일한 라우터를 통해 인터넷에 액세스해야 합니다.

2) 이 회사에는 인터넷에서 사용자가 액세스해야 하는 웹 서버가 있습니다.

8.1.2 네트워크 토폴로지

그림 8-1 네트워크 토폴로지



8.1.3 구성 체계

첫 번째 요구 사항을 충족하려면 게이트웨이에서 정적 라우팅을 구성하여 라우터가 패킷을 다른 서브넷(172.16.10.0/24, 172.16.20.0/24)의 IP 주소로 전달할 위치를 알 수 있도록 합니다.

두 번째 요구 사항을 충족하려면 라우터에 웹 서버에 대한 일대일 NAT 항목을 추가하여 개인 IP

주소가 있는 웹 서버가 해당 유효한 공용 IP 주소에서 액세스할 수 있도록 합니다. 일대일 NAT는 WAN 포트의 연결 유형이 고정 IP인 경우에만 적용됩니다.

8.1.4 구성 절차

아래 단계에 따라 라우터에서 NAT를 구성하세요:

■ 정적 라우팅 구성

1) **전송 > 라우팅 > 정적 경로** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다.

2) 두 부서에 각각 고정 경로를 추가합니다: 항목 이름을 RD/ Market으로 지정하고, 대상 IP로 172.16.10.0/172.16.20.0을 입력한 다음, 다음 홉으로 L3 스위치의 VLAN 1 인터페이스 IP를 지정하고, 인터페이스를 WAN1으로 선택합니다. 이 항목의 상태를 **사용으로** 유지합니다. **확인을** 클릭합니다.

그림 8-2 RD 부서에 대한 정적 라우팅 구성

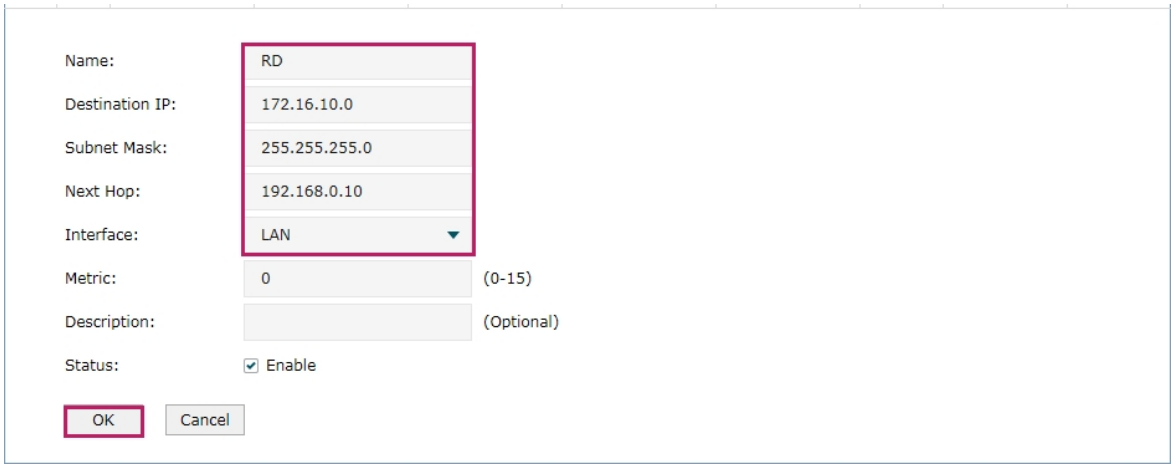
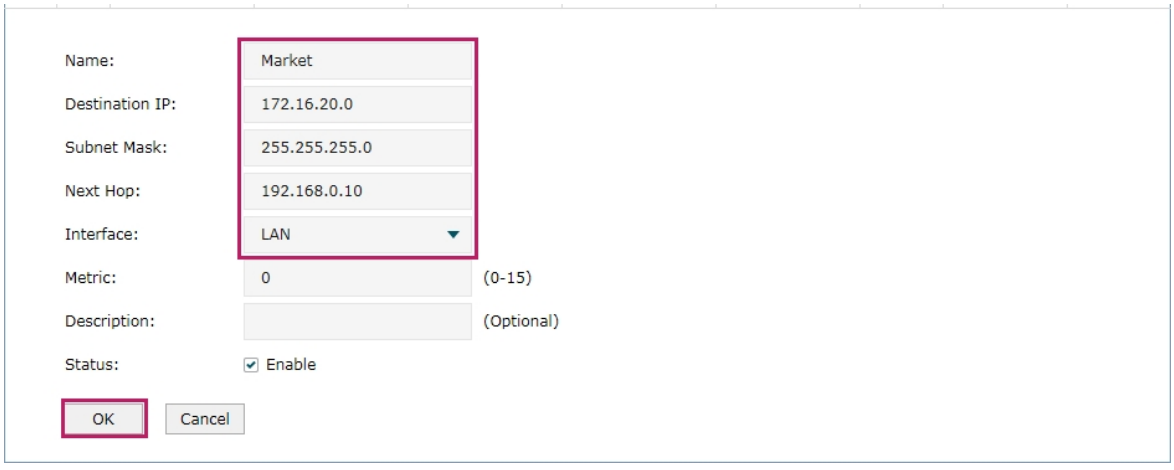


그림 8-3 마켓 부서에 대한 정적 라우팅 구성하기



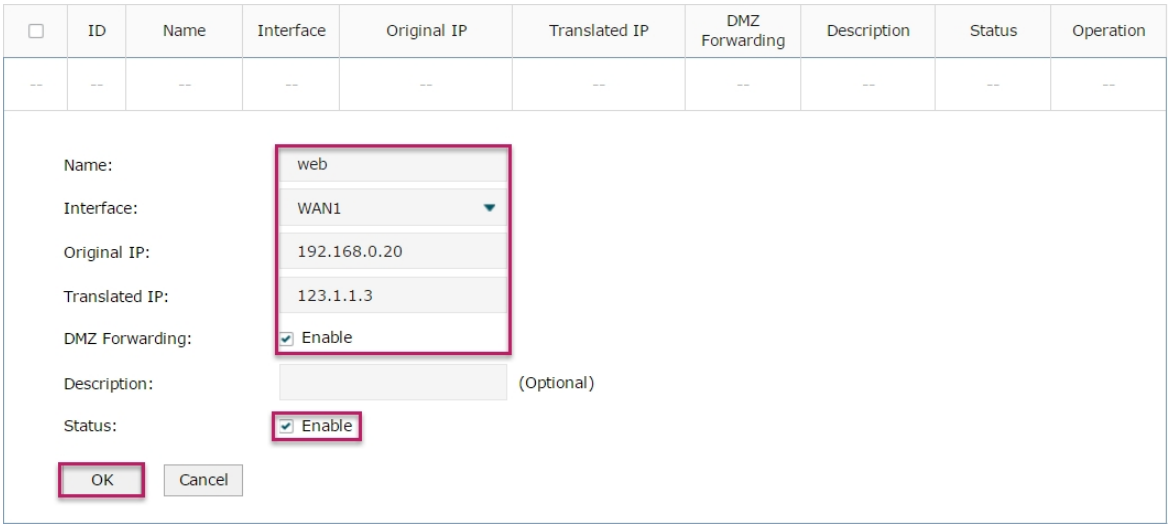
■ 일대일 NAT 구성

1) **전송 > NAT > 일대일 NAT** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다.

2) 웹 서버에 대한 일대일 NAT 항목을 추가합니다: 항목 이름을 web으로 지정하고 인터페이스를 WAN1으로 선택한 다음 원본 IP를 번역된 192.168.0.20으로 입력합니다.

IP를 123.1.1.3으로 설정합니다. DMZ 포워딩을 사용하도록 설정한 다음 이 항목의 상태를 **사용으로** 유지합니다. 클릭
OK.

그림 8-4 RD 부서에 대한 다중 네트워크 항목 추가



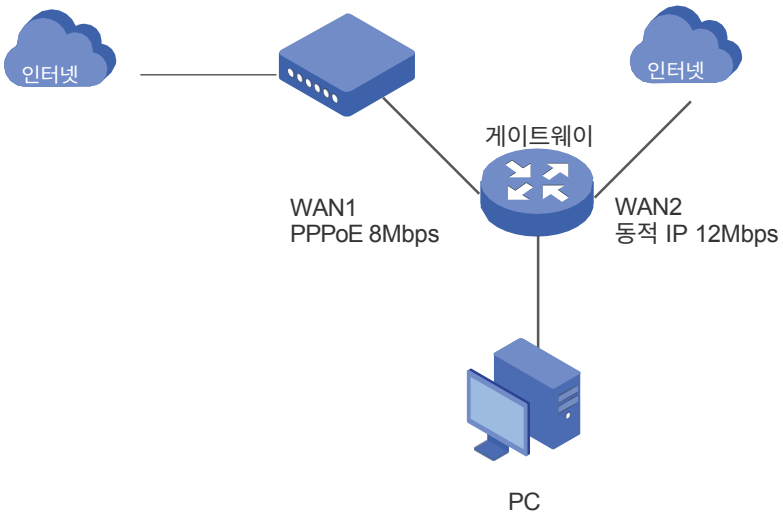
8.2 부하 분산 구성 예제

8.2.1 네트워크 요구 사항

대역폭을 효율적으로 활용하기 위해 네트워크 관리자는 로드 밸런싱을 사용하여 두 개의 WAN 링크를 바인딩하기로 결정합니다.

8.2.2 네트워크 토폴로지

그림 8-5 네트워크 토폴로지



8.2.3 구성 체계

요구 사항을 충족하려면 라우터에서 두 개의 WAN 링크가 제대로 작동하고 인터넷에 액세스할 수 있도록 WAN 매개변수를 구성한 다음 라우터에서 두 개의 WAN 링크를 집계하도록 로드 밸런싱을 구성합니다.

8.2.4 구성 절차

아래 단계에 따라 라우터에서 부하 분산을 구성하세요:

- WAN 매개변수 구성

  WAN1 포트의 경우 연결 유형을 PPPoE로 구성하고 ADSL 대역폭에 따라 이 링크의 업스트림 및 다운스트림 대역폭을 지정합니다(대역폭 정보는 인터넷 서비스 제공업체에 문의할 수 있습니다).

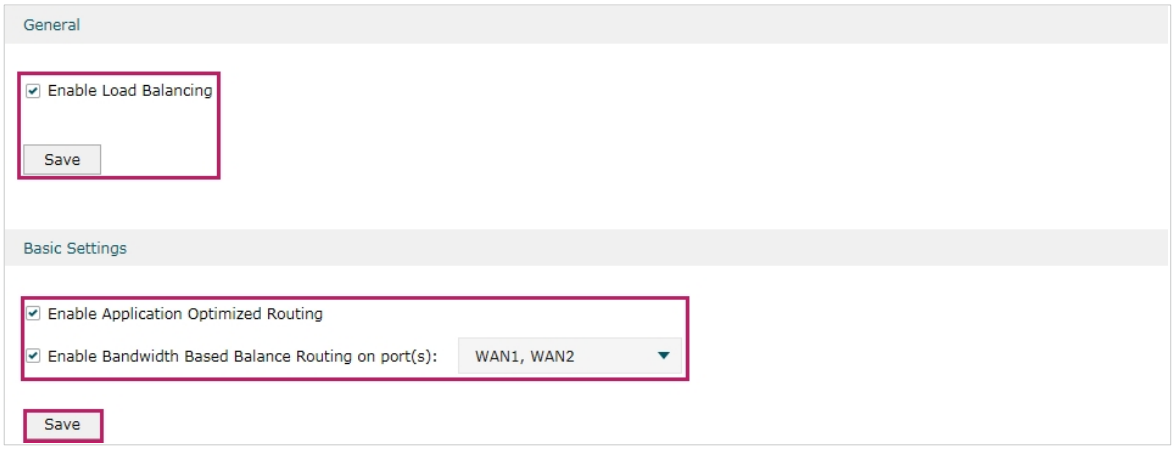
  WAN2 포트의 경우 연결 유형을 동적 IP로 구성하고 ISP가 제공하는 데이터에 따라 이 링크의 업스트림 및 다운스트림 대역폭을 지정합니다.

  두 개의 WAN 링크가 제대로 작동하고 인터넷에 액세스할 수 있는지 확인하세요.

- 부하 분산 구성

  전송 > 부하 분산 > 기본 설정 메뉴를 선택하여 구성 페이지를 로드합니다. 로드 밸런싱을 전역으로 활성화하고 **저장을** 클릭합니다. 애플리케이션 최적화 라우팅을 사용하도록 설정하고 WAN1 포트 및 WAN2 포트에서 대역폭 기반 밸런싱 라우팅을 사용하도록 설정합니다. **저장을** 클릭합니다.

그림 8-6 부하 분산 구성



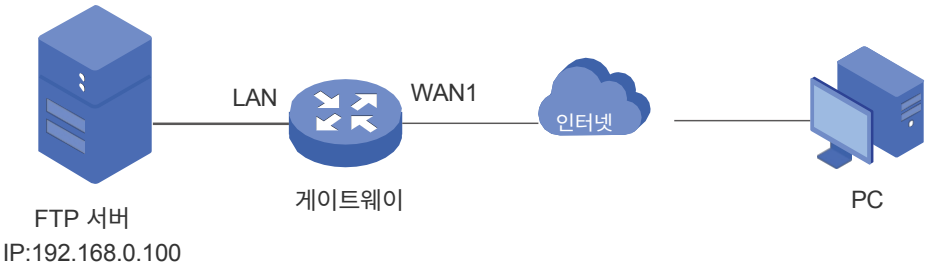
8.3 가상 서버 구성 예제

8.3.1 네트워크 요구 사항

네트워크 관리자가 로컬 네트워크에 FTP 서버를 구축하여 인터넷에서 공유하려고 합니다.

8.3.2 네트워크 토폴로지

그림 8-7 네트워크 토폴로지



8.3.3 구성 체계

이 시나리오에서는 가상 서버와 DMZ 호스트 모두 요구 사항을 충족하도록 구성할 수 있습니다. 여기서는 가상 서버를 구성하는 것을 예로 들었는데, 그 이유는 DMZ 호스트의 경우 모든 포트가 열려 있기 때문에 안전하지 않을 수 있기 때문입니다. 인터넷 사용자가 FTP 서버에 액세스할 수 있도록 라우터에서 FTP 서버를 가상 서버로 구성합니다.

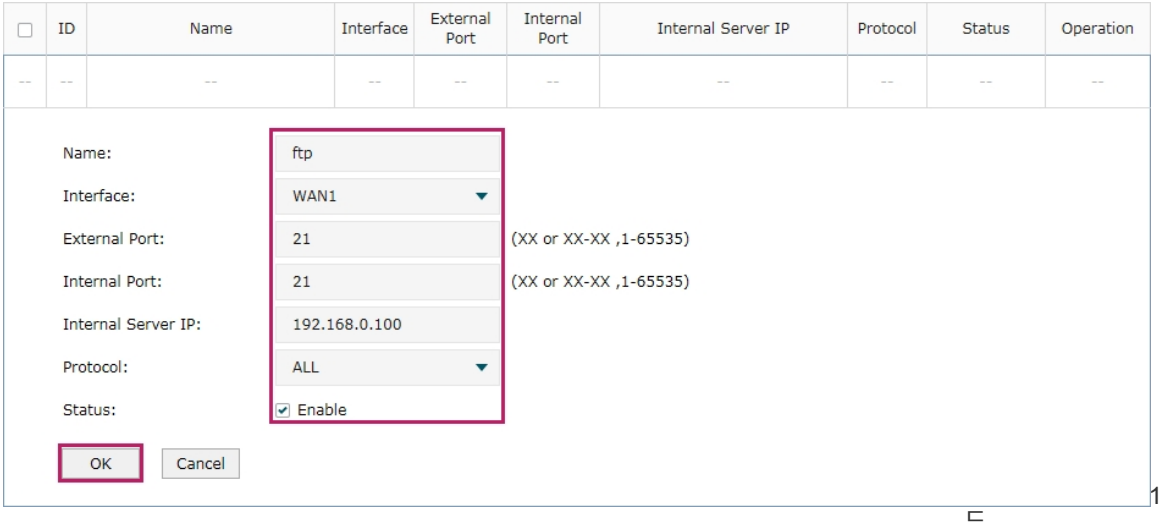
8.3.4 구성 절차

아래 단계에 따라 라우터에서 가상 서버를 구성하세요:

1) **전송 > NAT > 가상 서버** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다.

2) 항목 이름을 ftp로 지정하고 인터페이스를 WAN1로 선택한 다음 내부/외부 포트를 21로 지정하고 내부 서버 IP로 FTP 서버의 IP 주소(192.168.0.100)를 입력합니다. 프로토콜을 모두로 선택한 다음 이 항목의 상태를 **사용으로** 유지합니다. **확인을** 클릭합니다.

그림 8-8 가상 서버 구성하기



8.4 정책 라우팅 구성 예제

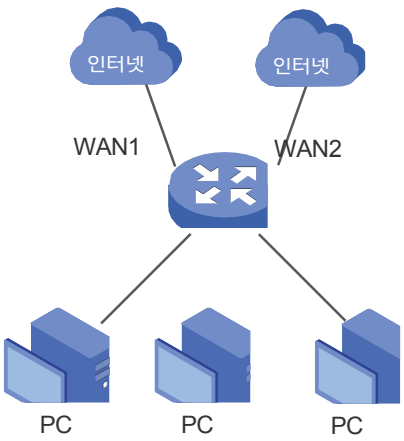
8.4.1 네트워크 요구 사항

네트워크 관리자는 3대의 컴퓨터(192.168.0.2-192.168.0.4)가 LAN 측에 연결된 라우터를 가지고 있으며, 모든 컴퓨터는 WAN1 포트와 WAN2 포트를 통해 인터넷으로 라우팅되며, 요구 사항은 다음과 같습니다:

- WAN2 링크는 항상 온라인 네트워크를 유지하기 위해 WAN1 링크를 백업하는 데 사용됩니다.
- IP 주소가 192.168.0.2 및 192.168.0.3인 두 대의 컴퓨터는 웹 서핑에는 WAN1을, 기타 인터넷 활동에는 WAN2를 사용해야 합니다.

8.4.1 네트워크 토폴로지

그림 8-9 네트워크 토폴로지



8.4.2 구성 체계

첫 번째 요구 사항을 충족하려면 라우터에서 링크 백업을 구성합니다. 두 번째 요구 사항을 충족하려면 192.168.0.2 및 192.168.0.3을 사용하는 두 대의 컴퓨터에 대한 정책 라우팅 규칙을 구성합니다. 링크 백업 규칙은 정책 라우팅 규칙보다 우선순위가 높다는 점에 유의하세요.

8.4.3 구성 절차

아래 단계에 따라 라우터에서 링크 백업 및 정책 라우팅을 구성하세요:

■ 링크 백업 구성

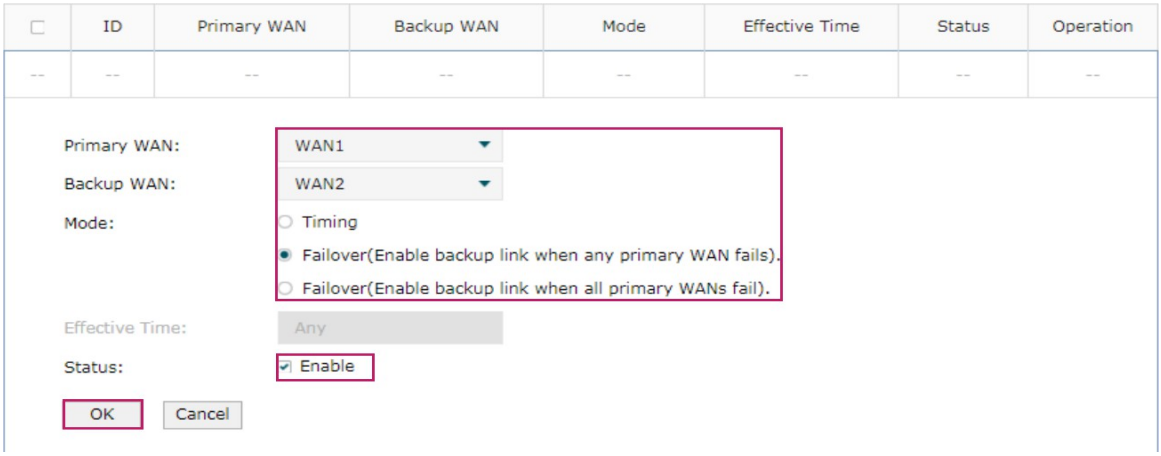
1) **전송 > 로드 밸런싱 > 링크 백업** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다.

2) 기본 WAN을 WAN1로, 백업 WAN을 WAN2로, 모드를 다음과 같이 지정합니다.

   장애 조치(기본 WAN에 장애가 발생할 경우 백업 링크를 사용하도록 설정), 백업 WAN이

기본 WAN이 실패하면 활성화됩니다. 이 항목의 상태를 사용으로 유지합니다. 클릭 **OK**.

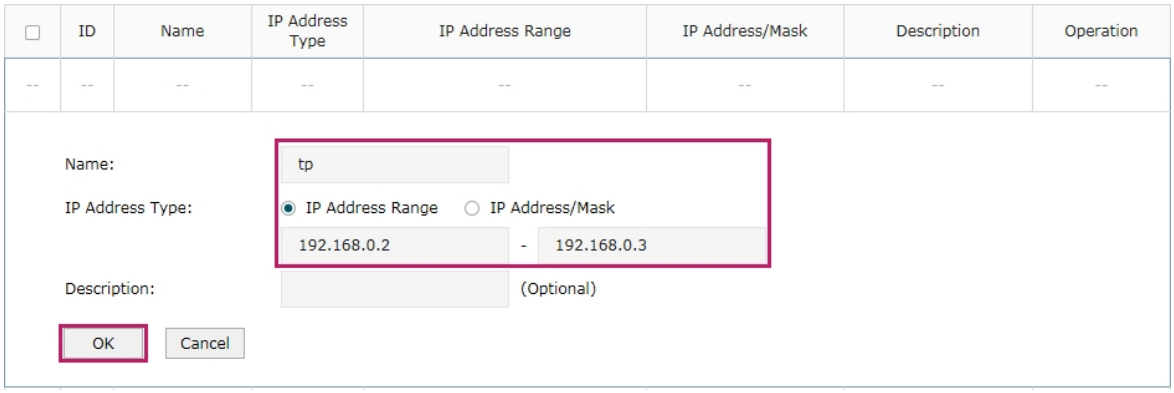
그림 8-10 링크 백업 구성하기



■ 정책 라우팅 규칙 구성하기

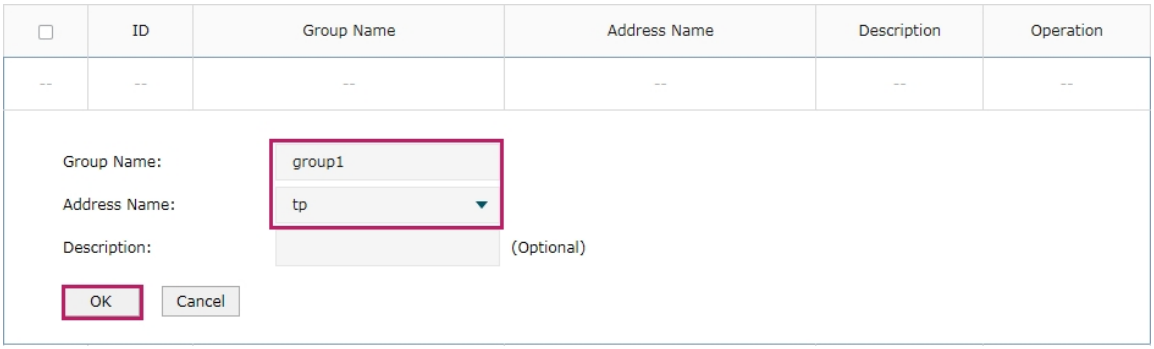
1) **환경설정 > IP 그룹 > IP 주소** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다. IP 주소 이름은 tp로, IP 주소 유형은 IP 주소 범위(192.168.0.2-192.168.0.3)로 지정합니다. **확인을** 클릭합니다.

그림 8-11 IP 주소 구성하기



2) **환경설정 > IP 그룹 > IP 주소** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다. IP 그룹 이름을 group1로 지정하고, 생성한 IP 주소를 참조할 수 있도록 IP 주소 이름을 tp로 지정합니다. **확인을** 클릭합니다.

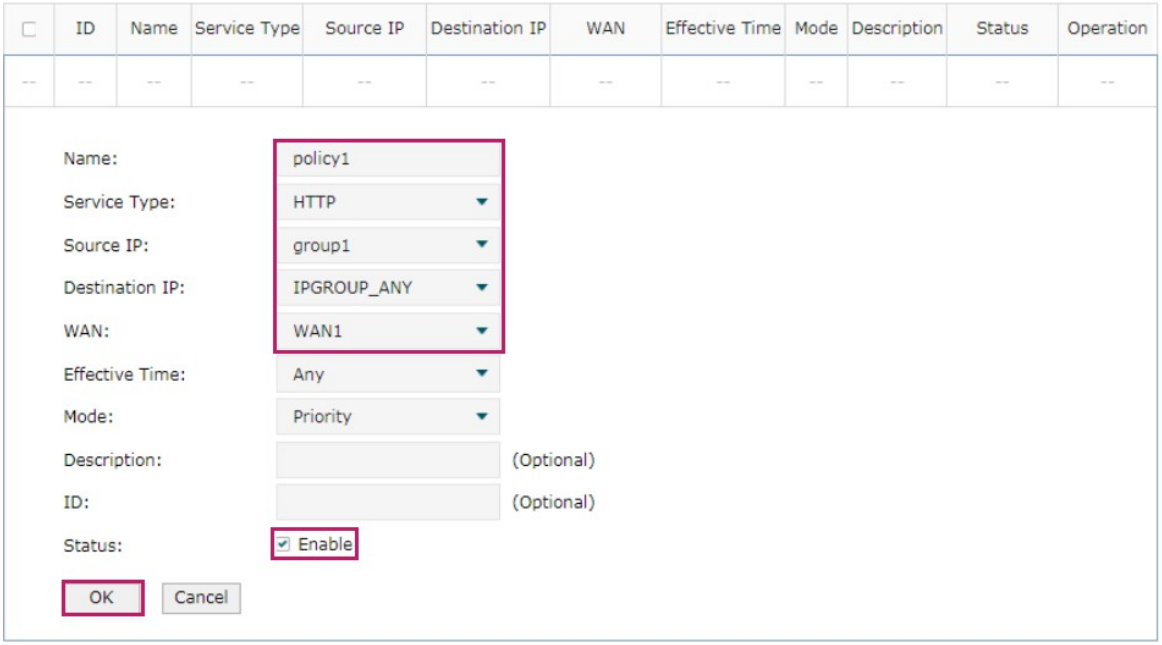
그림 8-12 IP 그룹 구성하기


ID
Group Name
Address Name
Description
Operation
Group Name:
group1
Address Name:
tp
Description:
(Optional)
OK
Cancel

3) **전송 > 라우팅 > 정책 라우팅** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다.

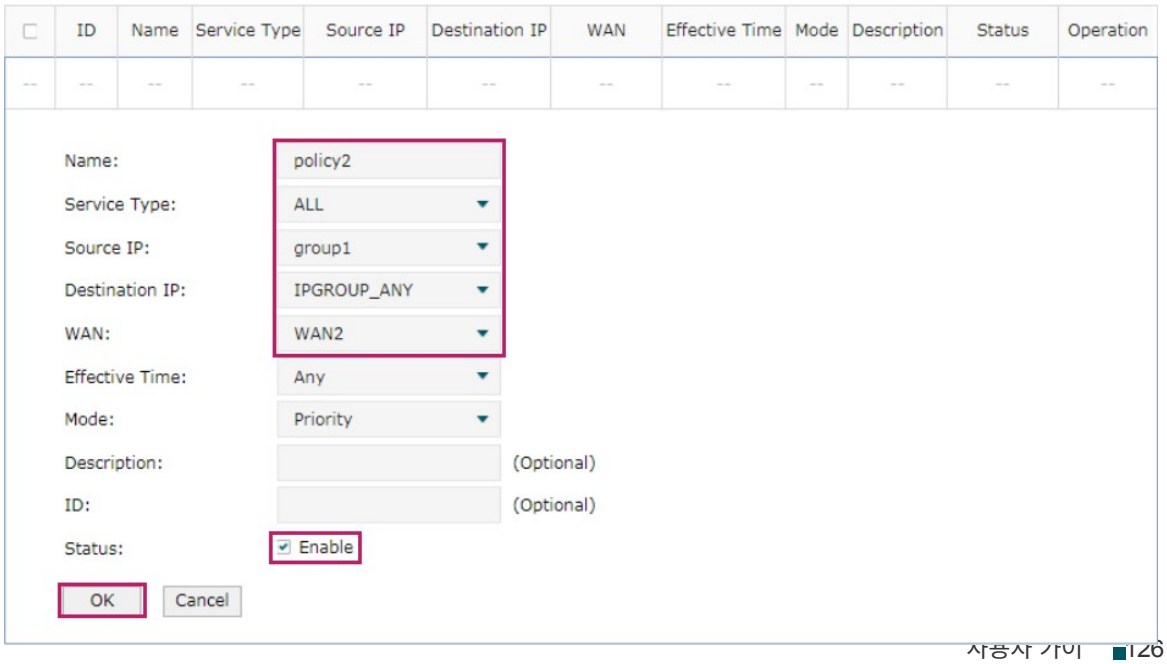
정책 라우팅 규칙 이름을 policy1로 지정하고, 서비스 유형을 HTTP로 지정하고, 소스 IP를 group1로 지정하고, 대상 IP를 제한이 없음을 의미하는 IPGROUP_ANY로 지정합니다. WAN1을 선택하고 이 항목의 상태를 **사용으로** 유지합니다. **확인을** 클릭합니다.

그림 8-13 정책 라우팅 규칙 구성 1



정책 라우팅 규칙 이름을 policy2로 지정하고, 서비스 유형을 ALL로 지정하며, 소스 IP를 group1로 지정하고, 대상 IP를 제한이 없음을 의미하는 IPGROUP_ANY로 지정합니다. WAN2를 선택하고 이 항목의 상태를 **사용으로** 유지합니다. **확인을** 클릭합니다.

그림 8-14 정책 라우팅 규칙 구성 2



파트 7

방화벽 구성

챕터

1. 방화벽
2. 방화벽 구성
3. 구성 예제

1 Fir ewall

1.1 개요

방화벽은 네트워크 보안을 강화하는 데 사용됩니다. 방화벽은 외부 네트워크 위협이 내부 네트워크로 확산되는 것을 방지하고, ARP 공격으로부터 내부 호스트를 보호하며, 내부 사용자의 외부 네트워크 액세스를 제어할 수 있습니다.

1.2 지원되는 기능

방화벽 모듈은 네 가지 기능을 지원합니다: ARP 스푸핑 방지, 공격 방어, 액세스 제어.

ARP 스푸핑 방지

ARP(주소 확인 프로토콜)는 패킷이 목적지로 전달될 수 있도록 IP 주소를 해당 MAC 주소에 매핑하는 데 사용됩니다. 하지만 ARP는 모든 호스트와 라우터를 신뢰할 수 있다는 전제하에 구현되기 때문에 실제 복잡한 네트워크에서는 보안 위험이 높습니다. 공격자가 잘못된 IP 주소와 MAC 주소의 매핑 항목이 포함된 ARP 스푸핑 패킷을 전송하면 디바이스는 잘못된 ARP 패킷을 기반으로 ARP 테이블을 업데이트하고 잘못된 매핑 항목을 기록하여 정상적인 통신이 중단됩니다.

ARP 스푸핑 방지 기능은 ARP 스푸핑 공격으로부터 네트워크를 보호할 수 있습니다. 이 기능은 IP-MAC 바인딩 항목을 기반으로 작동합니다. 이 항목은 IP 주소와 MAC 주소 간의 올바른 일대일 관계를 기록합니다. 라우터는 ARP 패킷을 수신할 때 IP-MAC 바인딩 항목과 일치하는지 확인합니다. 일치하지 않으면 라우터는 ARP 패킷을 무시합니다. 이러한 방식으로 라우터는 올바른 ARP 테이블을 유지합니다.

또한 라우터는 다음 두 가지 하위 기능을 제공합니다:

- IP-MAC 바인딩 항목과 일치하는 패킷만 허용하고 다른 패킷은 삭제합니다.
- ARP 공격을 감지하면 호스트에 GARP 패킷을 보냅니다. GARP 패킷은 호스트에게 올바른

ARP 테이블을 알려주어 ARP 스푸핑 패킷에 의해 ARP 테이블이 위조되는 것을 방지할 수 있습니다.

공격 방어

네트워크 장치에 대한 공격은 장치 또는 네트워크 마비를 일으킬 수 있습니다. 공격 방어 기능을 사용하면 라우터는 CPU로 전송되는 다양한 공격 패킷을 식별하여 삭제하고 패킷 수신 속도를 제한할 수 있습니다. 이러한 방식으로 라우터는 악의적인 공격으로부터 자신과 연결된 네트워크를 보호할 수 있습니다.

라우터는 두 가지 유형의 공격 방어 기능을 제공합니다: 플러드 방어와 패킷 이상 방어. 플러드 방어는 특정 유형의 패킷 수신 속도를 제한하고 패킷 이상 방어는 불법 패킷을 직접 삭제합니다.

MAC 필터링

MAC 필터링은 라우터를 통과하는 특정 디바이스의 패킷을 디바이스의 MAC 주소에 따라 삭제하거나 허용할 수 있습니다. MAC 필터링 정책과 MAC 필터링 목록이 구성되면 라우터는 MAC 주소와 일치하는 패킷에 필터 정책을 적용하여 네트워크 트래픽을 제한하고 네트워크 액세스 동작을 관리합니다.

액세스 제어

액세스 제어는 액세스 제어 규칙에 따라 라우터를 통과하는 패킷을 필터링할 수 있습니다. 액세스 제어 규칙에는 필터 정책과 서비스 유형, 수신 인터페이스, 유효 시간 등 몇 가지 조건이 포함됩니다. 라우터는 이러한 조건과 일치하는 패킷에 필터 정책을 적용하여 네트워크 트래픽을 제한하고 네트워크 액세스 동작을 관리하는 등의 작업을 수행합니다.

액세스 제어는 TCP(전송 제어 프로토콜) 및 ICMP(인터넷 제어 메시지 프로토콜) 패킷에 대한 공격 등 다양한 네트워크 공격을 방지할 수 있으며, 인터넷 액세스 제어 등 네트워크 액세스 동작을 관리할 수도 있습니다.

2 전나무 이월 구성

방화벽 모듈에서는 다음 기능을 구성할 수 있습니다:

- ARP 스푸핑 방지
- 공격 방어
- MAC 필터링
- 액세스 제어

2.1 ARP 스푸핑 방지

ARP 스푸핑 방지 구성을 완료하려면 두 단계가 있습니다. 먼저 IP-MAC 바인딩 목록에 IP-MAC 바인딩 항목을 추가합니다. 그런 다음 해당 항목에 대해 안티 ARP 스푸핑을 사용 설정합니다.

참고:

ARP 스푸핑 방지 기능으로 인해 현재 연결된 디바이스에 액세스 문제가 발생할 경우, ARP 스푸핑 방지 기능을 활성화하기 전에 먼저 IP-MAC 바인딩 항목을 추가하고 확인하는 것이 좋습니다.

2.1.1 IP-MAC 바인딩 항목 추가

수동 및 ARP 스캔을 통해 두 가지 방법으로 IP-MAC 바인딩 항목을 추가할 수 있습니다.

- 수동으로 IP-MAC 바인딩 항목 추가하기

네트워크에 있는 호스트의 관련 정보가 있다는 전제하에 IP 주소, MAC 주소 및 인터페이스를 수동으로 함께 바인딩할 수 있습니다.

- ARP 스캔을 통해 IP-MAC 바인딩 항목 추가하기

ARP 스캐닝을 사용하면 라우터는 특정 IP 필드가 포함된 ARP 요청 패킷을 호스트에 보냅니다.

ARP 응답 패킷을 수신하면 라우터는 호스트의 IP 주소, MAC 주소, 연결된 인터페이스를 확인할 수 있습니다.

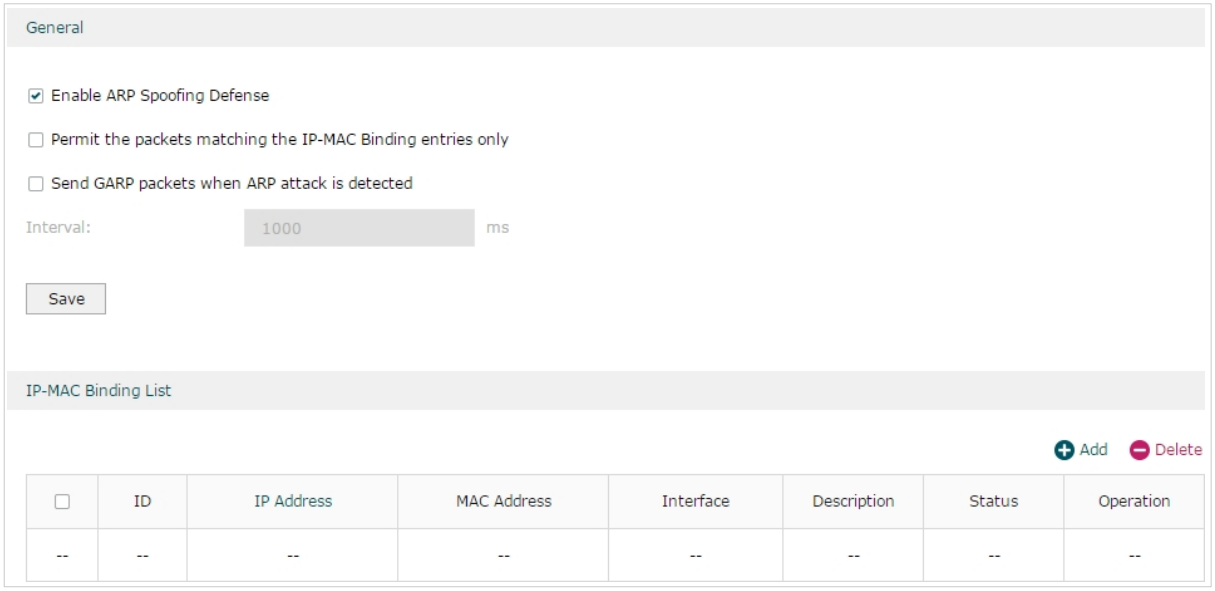
다음 섹션에서는 이 두 가지 방법을 자세히 소개합니다.

수동으로 IP-MAC 바인딩 항목 추가하기

항목을 수동으로 추가하기 전에 네트워크에 있는 호스트의 IP 주소와 MAC 주소를 가져와서 정확한지 확인하세요.

방화벽 > ARP 스푸핑 방지 > IP-MAC 바인딩 메뉴를 선택하면 다음 페이지가 로드됩니다.

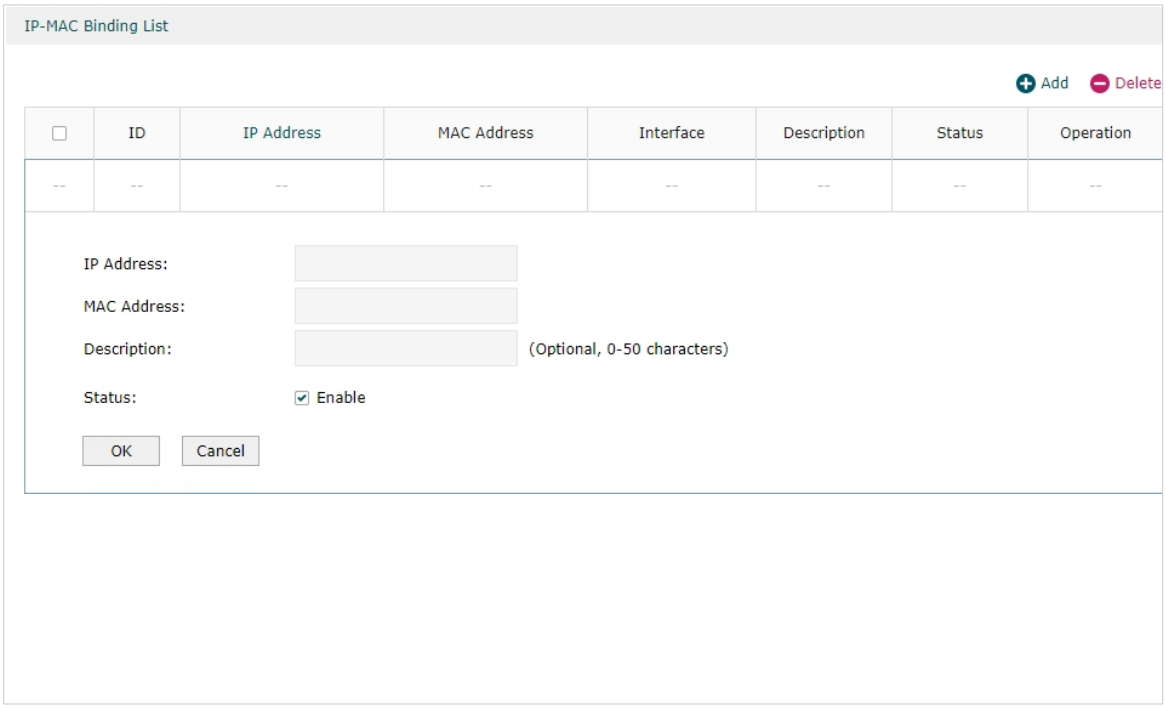
그림 2-1 IP-MAC 바인딩 페이지



IP-MAC 바인딩 항목을 수동으로 추가하려면 아래 단계를 따르세요. 이 항목은 LAN 인터페이스에 적용됩니다.

1) **IP-MAC 바인딩 목록** 섹션에서 추가를 클릭하여 다음 페이지를 로드합니다.

그림 2-2 IP-MAC 바인딩 항목을 수동으로 추가하기



2) 이 페이지에서 다음 매개 변수를 구성합니다.

IP 주소	바인딩할 IP 주소를 입력합니다.
MAC 주소	바인딩할 MAC 주소를 입력합니다.
인터페이스	항목이 적용될 인터페이스를 선택합니다.
설명	식별을 위한 설명을 입력합니다.
DHCP 주소 예약으로 내보내기	IP-MAC 바인딩 목록을 주소 예약 목록으로 내보낼지 여부입니다.
상태	이 항목을 활성화합니다. 상태가 활성화인 경우에만 이 항목이 적용됩니다.

3) 확인을 클릭하면 추가된 항목이 목록에 표시됩니다.

ARP 스캔을 통해 IP-MAC 바인딩 항목 추가하기

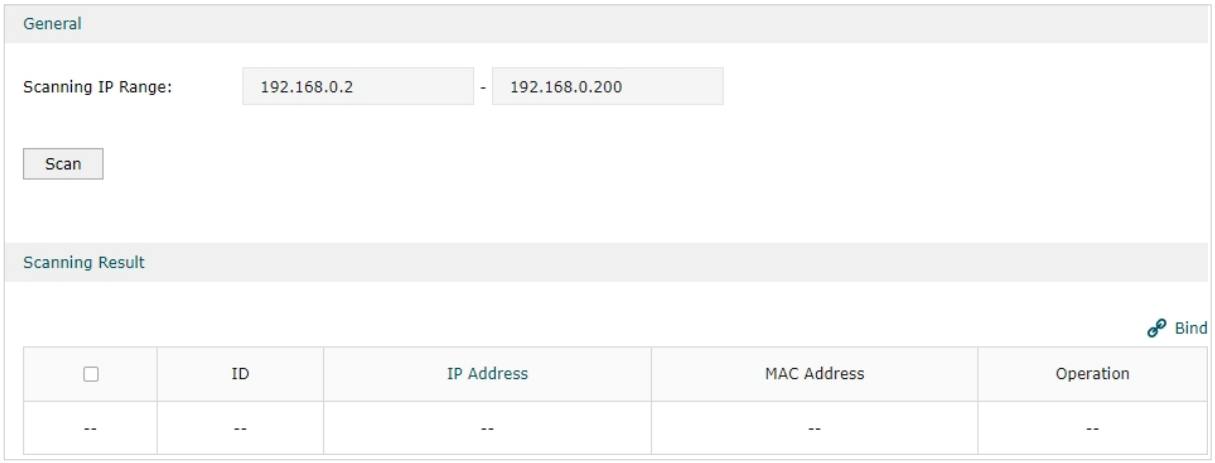
호스트의 IP 주소와 MAC 주소를 빠르게 얻으려면 ARP 스캔을 사용하여 작업을 용이하게 할 수 있습니다.

참고:

이 기능을 사용하기 전에 네트워크가 안전한지, 호스트가 현재 ARP 공격을 받고 있지 않은지 확인하세요. 그렇지 않으면 잘못된 IP-MAC 바인딩 항목을 얻을 수 있습니다. 네트워크가 공격을 받고 있는 경우 항목을 수동으로 바인딩하는 것이 좋습니다.

방화벽 > ARP 스푸핑 방지 > ARP 스캐닝 메뉴를 선택하면 다음 페이지가 로드됩니다.

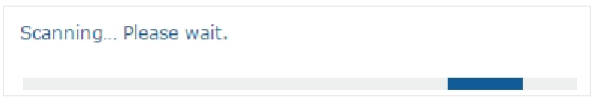
그림 2-3 ARP 스캔을 통한 IP-MAC 바인딩 시도 추가



ARP 스캔을 통해 IP-MAC 바인딩 항목을 추가하려면 아래 단계를 따르세요.

1) 스캔을 클릭하면 다음 창이 나타납니다.

그림 2-4 ARP 스캔 프로세스



2) 아무 조작 없이 잠시 기다리세요. 스캔 결과가 표로 내보냅니다. 🔗 을 클릭하여 해당 항목을 IP-MAC 바인딩 테이블로 내보내거나, 여러 항목을 선택하고 🔗 Bind 을 클릭하여 해당 항목을 일괄적으로 IP-MAC 바인딩 테이블로 내보냅니다.

그림 2-5 ARP 스캔 결과

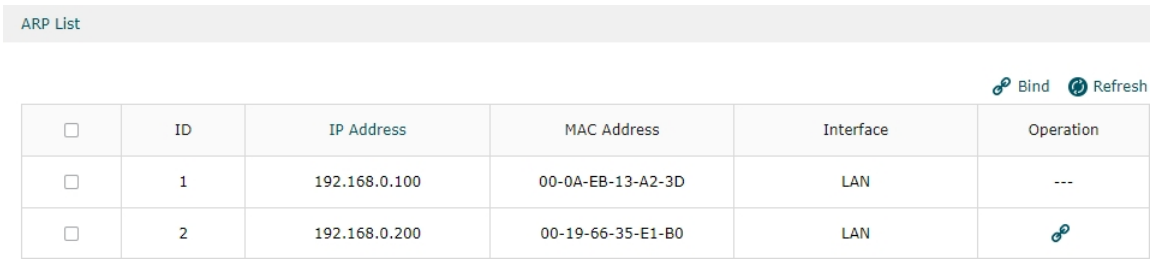
Scanning Result

Bind

	ID	IP Address	MAC Address	Operation
☐	1	192.168.0.100	00-0A-EB-13-A2-3D	
☐	2	192.168.0.200	00-19-66-35-E1-B0	
☐	3	192.168.0.73	00-0A-EB-00-13-01	
☐	4	192.168.0.37	00-0A-EB-03-12-A4	

또한 **방화벽 > ARP 스푸핑 방지 > ARP 목록으로** 이동하여 ARP 스캐닝 항목을 보고 바인딩할 수 있습니다. ARP 스캐닝 목록에는 과거에 스캔한 모든 항목이 표시됩니다. 을 클릭하여 해당 항목을 IP-MAC 바인딩 테이블로 내보내거나 여러 항목을 선택합니다.
를 클릭하고 Bind 을 클릭하여 항목을 IP-MAC 바인딩 테이블로 일괄 내보냅니다.

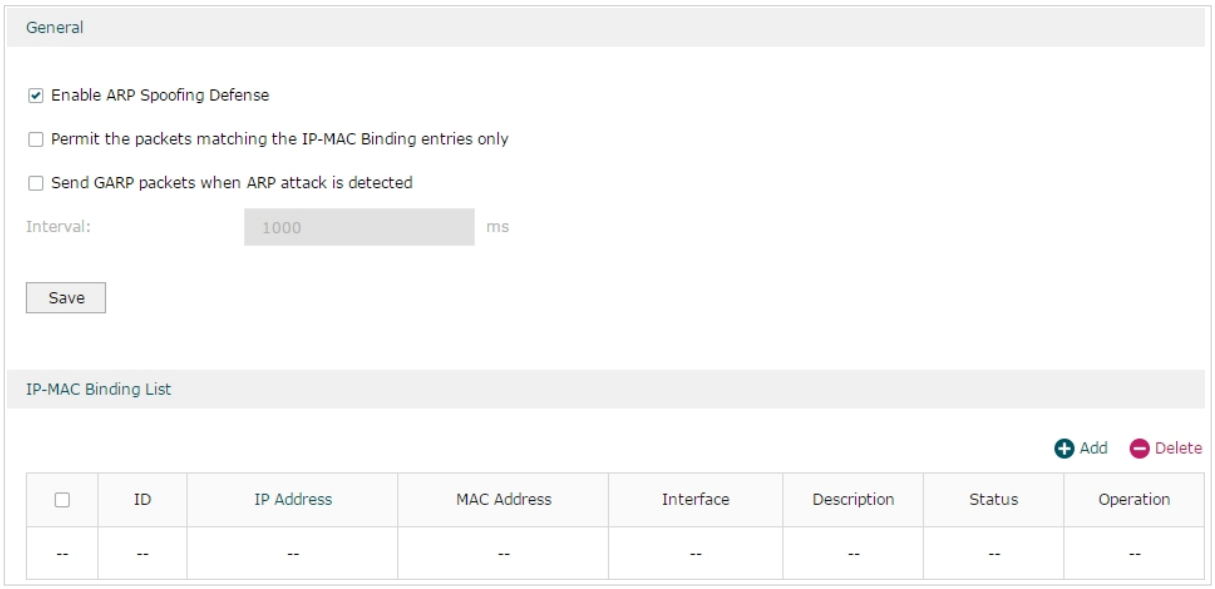
그림 2-6 ARP 목록



2.1.2 ARP 스푸핑 방지 활성화

방화벽 > ARP 스푸핑 방지 > IP-MAC 바인딩 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 2-7 IP-MAC 바인딩-일반 구성



아래 단계에 따라 ARP 스푸핑 방지 규칙을 구성할 수 있습니다:

1) **일반** 섹션에서 ARP 스푸핑 방어를 전역적으로 사용 설정합니다. 이 옵션을 활성화하면 라우터가 ARP 스푸핑 패킷에 의해 ARP 테이블이 위조되지 않도록 보호할 수 있습니다.

2) 두 가지 하위 기능을 활성화할지 여부를 선택합니다.

IP-MAC 바인딩 항목과 일치하는 패킷만 허용합니다.	이 옵션을 활성화하면 패킷을 수신할 때 라우터는 IP 주소, MAC 주소 및 수신 인터페이스가 IP-MAC 바인딩 항목과 일치하는지 확인합니다.

일치하는 패킷만 전달됩니다.

ARP 공격이 감지되면 GARP 패킷 보내기	이 옵션을 활성화하면 라우터는 네트워크에서 ARP 스푸핑 패킷을 감지하면 호스트에 GARP 패킷을 보냅니다. GARP 패킷은 호스트에 올바른 ARP 정보를 알려주며, 이 정보는 호스트의 잘못된 ARP 정보를 대체하는 데 사용됩니다.
간격	**ARP 공격이 감지되면 GARP 패킷 보내기** 옵션이 활성화된 경우 GARP 패킷을 전송할 시간 간격을 구성합니다. 유효한 값은 1~10,000밀리초입니다.

3) **저장을** 클릭합니다.

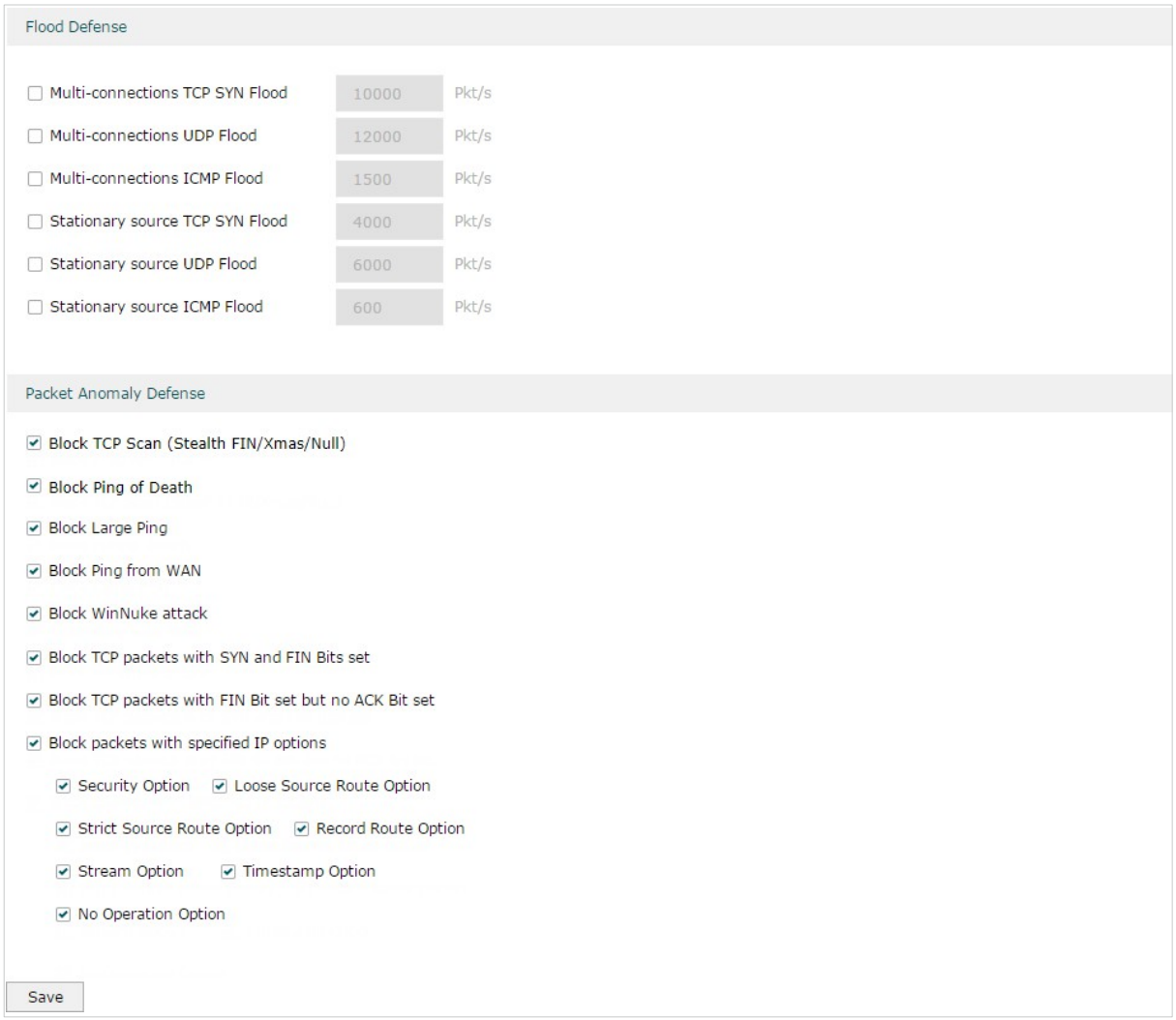
참고:

"IP-MAC 바인딩 항목과 일치하는 패킷만 허용"을 활성화하기 전에 관리 호스트가 IP-MAC 바인딩 목록에 있는지 확인해야 합니다. 그렇지 않으면 라우터의 웹 관리 페이지에 로그인할 수 없습니다. 이 경우 라우터를 공장 출하 시 기본값으로 복원하고 기본 로그인 자격 증명을 사용하여 로그인하세요.

2.2 공격 방어 구성

방화벽 > 공격 방어 > 공격 방어 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 2-8 공격 방어



아래 단계에 따라 공격 방어 기능을 구성하세요.

1) **홍수 방어** 섹션에서 확인란을 선택하고 해당 매개변수를 구성하여 원하는 기능을 사용하도록 설정합니다. 기본적으로 모든 옵션은 비활성화되어 있습니다. 자세한 내용은 다음 표를 참조하세요:

다중 연결 TCP SYN 폭주	이 기능을 활성화하면 이러한 종류의 패킷 수가 지정된 임계값에 도달하면 라우터가 후속 TCP SYN 패킷을 필터링합니다. 유효한 임계값 범위는 100에서 99999까지입니다.

다중 연결 UDP 폭주	이 기능을 활성화하면 이러한 종류의 패킷 수가 지정된 임계값에 도달하면 라우터가 후속 UDP 패킷을 필터링합니다. 유효한 임계값 범위는 100에서 99999까지입니다.
다중 연결 ICMP 폭주	이 기능을 활성화하면 이러한 종류의 패킷 수가 지정된 임계값에 도달하면 라우터가 후속 ICMP 패킷을 필터링합니다. 유효한 임계값 범위는 100에서 99999까지입니다.

고정 소스 TCP SYN 플러드	이 기능을 활성화하면 라우터는 이러한 종류의 패킷 수가 지정된 임계값에 도달하면 이후의 고정 소스 TCP SYN 패킷을 필터링합니다. 유효한 임계값 범위는 100에서 99999까지입니다.
고정 소스 UDP 플러드	이 기능을 활성화하면 라우터는 이러한 종류의 패킷 수가 지정된 임계값에 도달하면 이후의 고정 소스 UDP SYN 패킷을 필터링합니다. 유효한 임계값 범위는 100에서 99999까지입니다.
고정 소스 ICMP 플러드	이 기능을 활성화하면 라우터는 이러한 종류의 패킷 수가 지정된 임계값에 도달하면 이후의 고정 소스 ICMP SYN 패킷을 필터링합니다. 유효한 임계값 범위는 100에서 99999까지입니다.

2) **패킷 이상 방어** 섹션에서 직접 확인란을 선택하여 원하는 기능을 사용하도록 설정합니다. 기본적으로 모든 옵션이 활성화되어 있습니다. 자세한 내용은 다음 표를 참조하세요:

TCP 스캔 차단(스텔스 FIN/Xmas/Null)	이 옵션을 활성화하면 라우터가 스텔스 핀, 크리스마스, Null의 TCP 스캔 패킷을 필터링합니다.
죽음의 핑 차단	이 옵션을 활성화하면 라우터가 죽음의 핑 공격을 차단합니다. 죽음의 핑 공격이란 공격자가 65535바이트보다 큰 비정상적인 핑 패킷을 전송하여 대상 컴퓨터에서 시스템 충돌을 일으키는 것을 의미합니다.
대형 핑 차단	이 옵션을 활성화하면 라우터가 대형 핑 공격을 차단합니다. 대용량 핑 공격이란 공격자가 1500바이트보다 큰 핑 패킷을 여러 개 전송하여 대상 컴퓨터에서 시스템 충돌을 일으키는 것을 의미합니다.
WAN에서 핑 차단	이 옵션을 활성화하면 라우터가 WAN으로부터의 ICMP 요청을 차단합니다.
WinNuke 공격 차단	이 옵션을 활성화하면 라우터가 WinNuke 공격을 차단합니다. WinNuke 공격은 Windows 95 및 Windows N과 같은 일부 Windows 운영 체제에 영향을 미치는 원격 서비스 거부 공격(DoS)을 말합니다. 공격자는 TCP 포트 137, 138 또는 139를 통해 대상 컴퓨터로 일련의 OOB(대역 외) 데이터를 전송하여 시스템 충돌 또는 블루 스크린을 유발합니다.
SYN 및 FIN 비트가 설정된 TCP 패킷 차단	이 옵션을 활성화하면 라우터는 SYN 비트와 FIN 비트가 모두 설정된 TCP 패킷을 필터링합니다.
FIN 비트는 설정되어 있지만 ACK 비트가 설정	되어 있지 않은 TCP 패킷 차단

이 옵션을 활성화하면 라우터는	FIN 비트가 설 정 되 어 있지만 ACK 비트가 설정되어 있지 않은 TCP 패킷을 필터링합니다.
지정된 IP 옵션으로 패킷 차단	이 옵션을 활성화하면 라우터가 지정된 IP 옵션으로 패킷을 필터링합니다. 필요에 따라 옵션을 선택할 수 있습니다.

3) **저장을** 클릭하여 설정을 저장합니다.

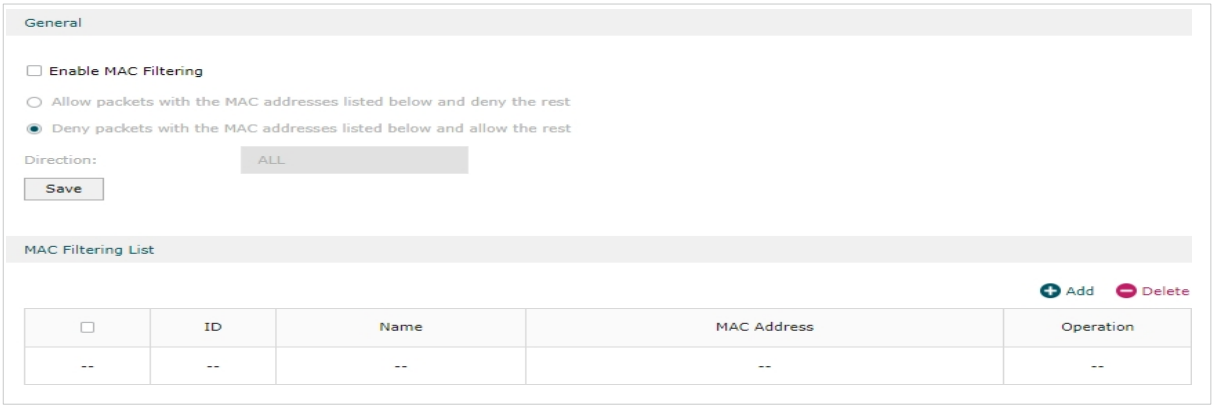
2.3 MAC 필터링 구성

MAC 필터링은 디바이스의 MAC 주소에 따라 라우터를 통과하는 특정 디바이스의 패킷을 삭제하거나 허용할 수 있습니다. MAC 필터링 정책 및 MAC 필터링 후

목록이 구성되면 라우터는 MAC 주소와 일치하는 패킷에 필터 정책을 적용하여 네트워크 트래픽을 제한하고 네트워크 액세스 동작을 관리합니다.

방화벽 > MAC 필터링 > MAC 필터링 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 2-9 MAC 필터링



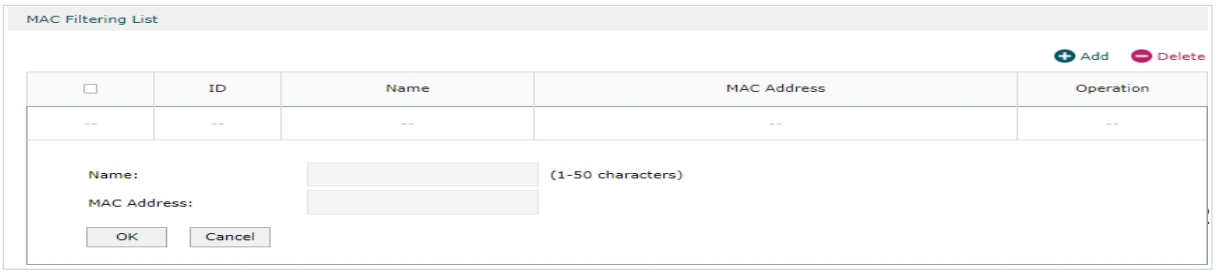
아래 단계에 따라 MAC 필터링을 구성할 수 있습니다.

1) **일반** 섹션에서 확인란을 선택하여 MAC 필터링 기능을 활성화하고 해당 매개변수를 구성한 다음 **저장을** 클릭합니다.

아래 나열된 MAC 주소를 가진 패킷은 허용하고 나머지는 거부합니다.	나열된 MAC 주소를 가진 패킷은 라우터를 통과하도록 허용하고 다른 MAC 주소를 가진 패킷은 삭제하려면 선택합니다.
아래 나열된 MAC 주소의 패킷은 거부하고 나머지는 허용합니다.	나열된 MAC 주소를 가진 패킷을 삭제하려면 선택하면 다른 MAC 주소를 가진 패킷은 라우터를 통과할 수 있습니다.
방향	LAN에서 LAN으로의 트래픽과 LAN에서 WAN으로의 트래픽 모두에 정책을 적용하려면 모두를 선택합니다. LAN에서 WAN으로의 트래픽에만 정책을 적용하려면 LAN -> WAN을 선택합니다.

2) **MAC 필터링 목록** 섹션에서 추가를 클릭하여 다음 페이지를 로드합니다.

그림 2-10 MAC 필터링



3) MAC 이름과 주소를 지정하고 **확인을** 클릭합니다.

MAC 주소	디바이스의 MAC 주소를 지정하면 해당 MAC 주소를 가진 트래픽에 MAC 필터링 정책이 적용됩니다.

2.4 액세스 제어 구성

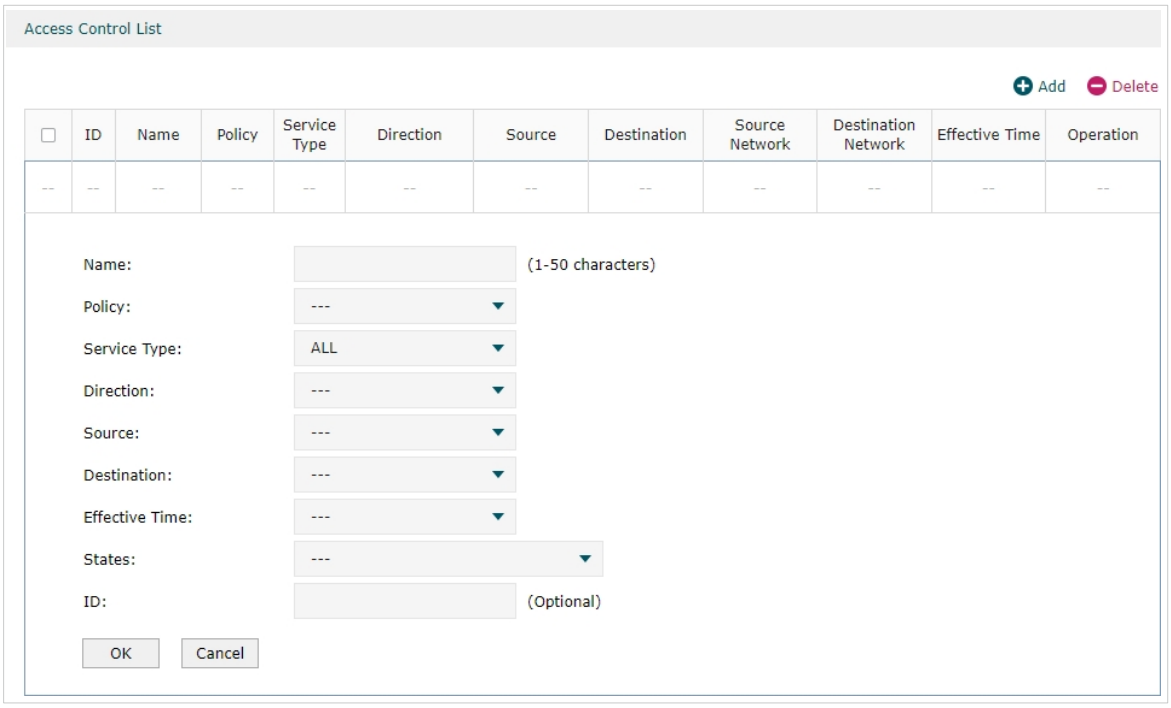
방화벽 > 액세스 제어 > 액세스 제어 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 2-11 액세스 제어

이 표에는 접근 제어 항목이 표시됩니다. 새 액세스 제어 항목을 추가하려면 아래 단계를 따르세요.

1) 추가를 클릭하면 다음 페이지가 나타납니다.

그림 2-12 액세스 제어



2) 필요한 매개변수를 구성하고 **확인을** 클릭합니다:

이름	규칙의 이름을 지정합니다. 최대 50자까지 입력할 수 있습니다. 각 항목의 이름은 반복할 수 없습니다.
정책	규칙과 일치하는 패킷의 네트워크 액세스를 차단할지 허용할지 선택합니다.
서비스 유형	규칙에 적용할 서비스를 선택합니다. 여기서 참조하는 서비스는 **환경설정 > 서비스 유형** 페이지에서 만들 수 있습니다.

방향	규칙의 효과적인 트래픽 방향을 선택합니다.

소스	규칙의 소스 주소 범위를 지정할 IP 그룹을 선택합니다. 여기서 참조하는 IP 그룹은 **환경설정 > IP 그룹** 페이지에서 만들 수 있습니다.
대상	규칙의 대상 주소 범위를 지정하려면 IP 그룹을 선택합니다. 여기서 참조하는 IP 그룹은 **환경설정 > IP 그룹** 페이지에서 만들 수 있습니다.
유효 시간	규칙의 유효 시간을 선택합니다. 여기서 참조하는 유효 시간은 **환경설정 > 시간 범위** 페이지에서 만들 수 있습니다.
상태	상태 저장 ACL 규칙의 유형을 결정합니다. 기본값인 자동 유형을 사용하는 것이 좋습니다. 신규 - 초기 상태의 연결과 일치합니다. 예를 들어 SYN 패킷이 TCP 연결로 도착하거나 라우터가 한 방향의 트래픽만 수신하는 경우입니다. 설정됨 - 설정된 연결을 일치시킵니다. 즉, 방화벽이 이 연결의 양방향 통신을 확인했다는 뜻입니다. 관련 - FTP 데이터 채널에 대한 연결과 같이 주 연결의 관련 하위 연결을 일치시킵니다. 유효하지 않음 - 예상대로 작동하지 않는 연결을 일치시킵니다.
ID	규칙 ID를 지정합니다. ID가 작을수록 우선 순위가 높습니다. 이 값은 선택 사항이며, 이 값을 구성하지 않고 새로 추가된 규칙은 모든 규칙 중에서 가장 큰 ID를 가지게 되므로 새로 추가된 규칙의 우선 순위가 가장 낮습니다.

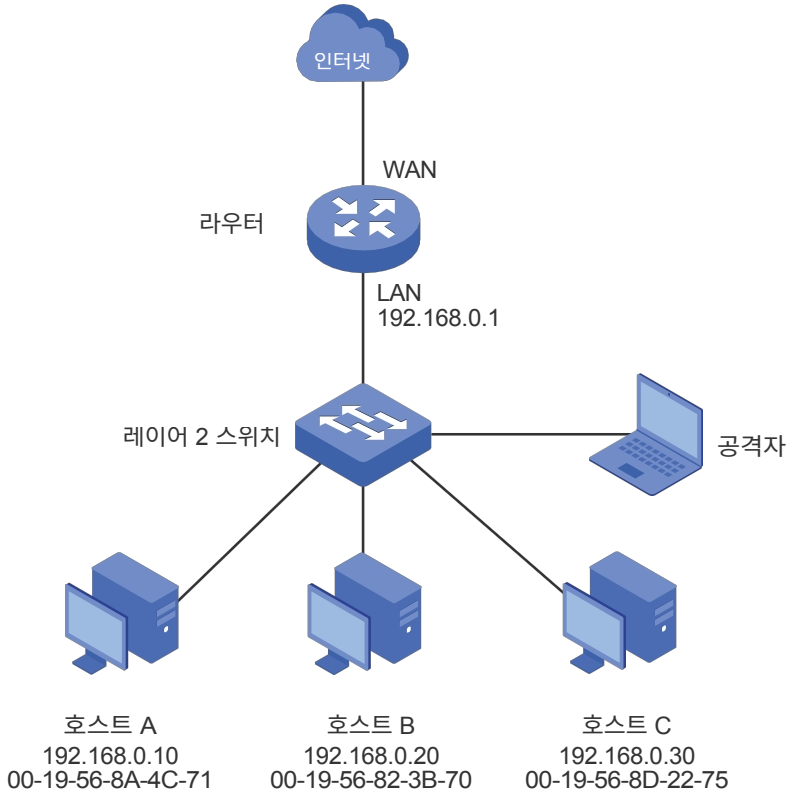
3 구성 예시

3.1 ARP 스푸핑 방지 예제

3.1.1 네트워크 요구 사항

아래 다이어그램에서 여러 호스트가 레이어 2 스위치를 통해 네트워크에 연결되어 있으며 라우터는 이 네트워크의 게이트웨이입니다. 공격자가 일련의 ARP 공격을 실행할 가능성이 존재하므로 라우터와 터미널 호스트를 ARP 공격으로부터 보호하도록 라우터를 구성해야 합니다.

그림 3-1 네트워크 토폴로지



3.1.2 구성 체계

공격자는 라우터 속이기, 게이트웨이 모방, 터미널 호스트 속이기 등 세 가지 유형의 ARP 공격을 실행할 수 있습니다. 다음 섹션에서는 세 가지 ARP 공격과 이에 대응하는 솔루션을 소개합니다.

- 부정 행위 게이트웨이

부정 게이트웨이 공격은 라우터를 대상으로 합니다.

공격자는 합법적인 터미널 호스트로 가장하여 라우터로 가짜 ARP 패킷을 전송하여 라우터가 호스트의 잘못된 ARP 맵을 기록하도록 속입니다. 그 결과 게이트웨이의 패킷이 호스트로 올바르게 전송되지 않습니다. 이러한 종류의 공격으로부터 라우터를 보호하기 위해 라우터에서 ARP 스푸핑 방지를 구성할 수 있습니다.

- 게이트웨이 및 부정 호스트 모방하기

이 두 가지 공격은 터미널 호스트를 대상으로 합니다.

게이트웨이 모방이란 공격자가 게이트웨이를 모방하여 호스트에 가짜 ARP 패킷을 보내는 것을 의미합니다. 결과적으로 호스트는 게이트웨이의 잘못된 ARP 맵을 기록하여 라우터에 패킷을 올바르게 보낼 수 없습니다.

치팅 호스트는 공격자가 합법적인 호스트인 것처럼 가장하여 다른 호스트에게 가짜 ARP 패킷을 보내는 것을 의미합니다. 그 결과, 치팅 호스트는 합법적인 호스트의 잘못된 ARP 맵을 기록하여 합법적인 호스트로 패킷을 올바르게 보낼 수 없게 됩니다.

위의 공격으로부터 호스트를 보호하려면 아래의 두 가지 예방 조치를 모두 취하는 것이 좋습니다
.

"호스트에서 방화벽 기능을 구성합니다.

" 라우터가 ARP 공격을 감지할 때 호스트에 GARP 패킷을 보내도록 라우터를 구성합니다. GARP 패킷은 호스트에 올바른 ARP 맵을 알려주며, 호스트의 잘못된 ARP 맵은 올바른 맵으로 교체됩니다.

결론적으로, ARP 공격으로부터 네트워크를 보호하려면 라우터와 호스트 모두에 관련 ARP 방어 기능이 구성되어 있는지 확인해야 합니다. 여기에서는 라우터에서 ARP 스푸핑 방지를 구성하는 방법을 소개합니다. 크게 세 단계로 구성되어 있습니다:

1) 합법적인 호스트의 IP 및 MAC 주소를 가져와서 IP-MAC 바인딩 목록에 바인딩합니다.

2) ARP 스푸핑 방지 기능을 활성화합니다.

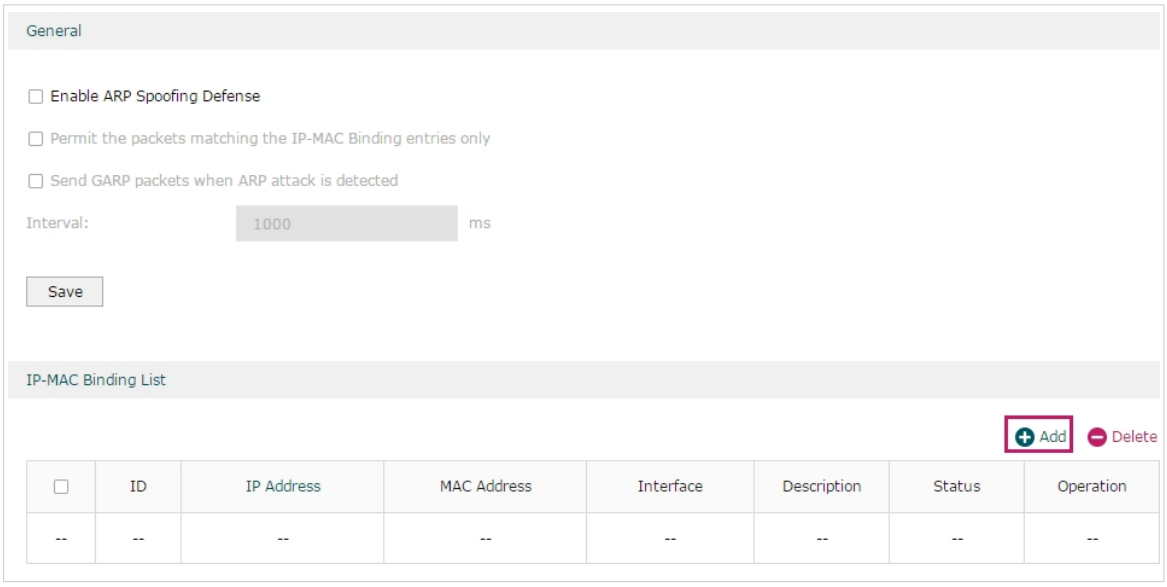
3) ARP 공격이 감지되면 GARP 패킷을 보내도록 라우터를 구성하세요.

3.1.3 구성 절차

아래 단계에 따라 라우터에서 ARP 스푸핑 방지를 구성하세요:

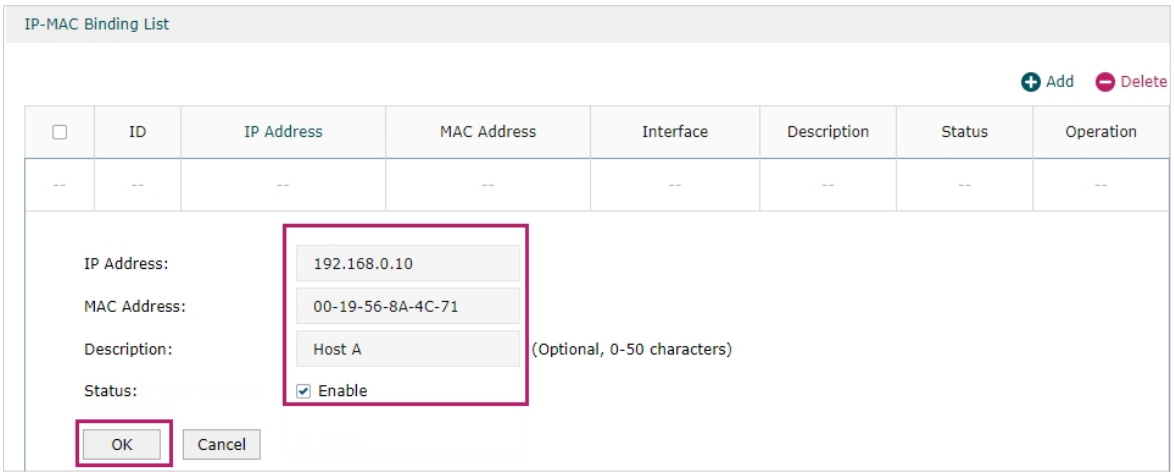
1) **방화벽 > ARP 스푸핑 방지 > IP-MAC 바인딩** 메뉴를 선택하면 다음 페이지가 로드됩니다. **IP-MAC 바인딩 목록** 섹션에서 **추가를** 클릭합니다.

그림 3-2 ARP 스푸핑 방지 페이지



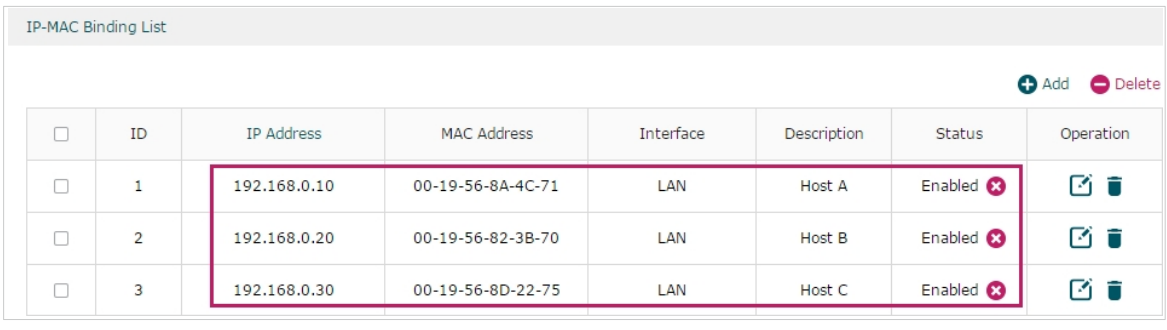
2) 다음 페이지가 나타납니다. 호스트 A의 IP 주소와 MAC 주소를 입력하고 이 항목에 대해 "호스트 A"라는 설명을 입력합니다. 이 항목의 **상태를** "사용"으로 유지합니다. **확인을** 클릭합니다.

그림 3-3 IP-MAC 바인딩 항목 추가하기



3) 위에서 소개한 대로 호스트 B 및 호스트 C에 대한 IP-MAC 바인딩 항목을 추가하고 구성을 확인합니다.

그림 3-4 IP-MAC 바인딩 전체 확인



4) 같은 페이지의 **일반** 섹션에서 ARP **스푸핑 방어를** 사용하도록 설정하고 **ARP 공격이 감지되면 GARP 패킷 보내기 확인란을 선택하고** 간격을 1000밀리초로 유지합니다. **저장을** 클릭합니다.

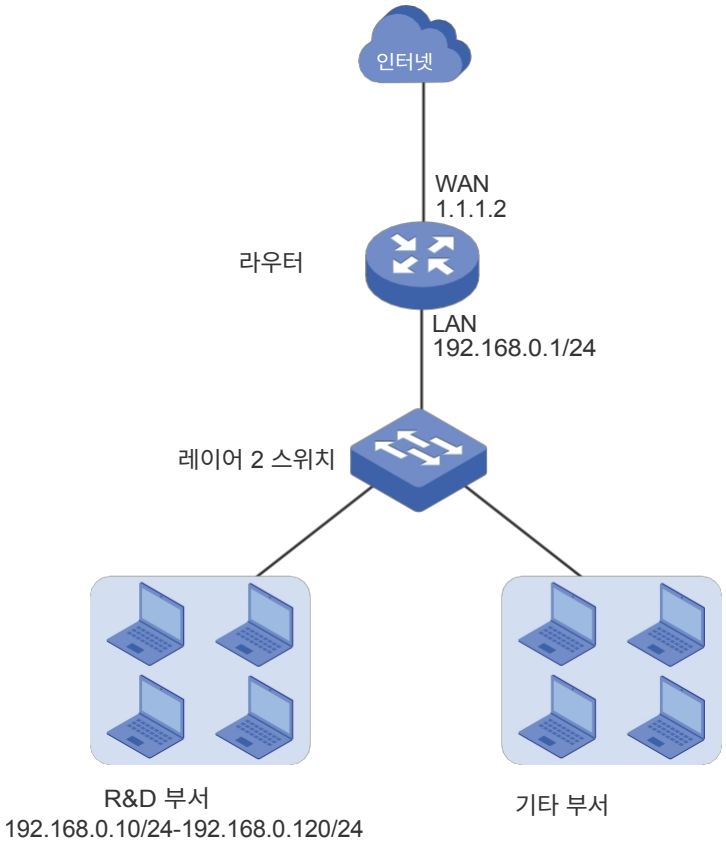
그림 3-5 ARP 스푸핑 방지 구성하기

3.2 액세스 제어 예제

3.2.1 네트워크 요구 사항

아래 다이어그램에서 R&D 부서와 일부 다른 부서는 레이어 2 스위치에 연결되어 있으며 라우터를 통해 인터넷에 접속합니다. 외부 사서함으로 이메일을 보내는 등 R&D 부서 사용자의 행위를 제한하기 위해 R&D 부서 사용자는 언제든지 인터넷에서 HTTP를 통해 웹 사이트만 방문할 수 있도록 해야 합니다. 다른 부서의 경우 제한이 없습니다.

그림 3-1 네트워크 토폴로지



3.2.2 구성 체계

이러한 요구 사항을 충족하기 위해 라우터에 액세스 제어 규칙을 구성하여 R&D 부서에서 특정 유형의 패킷을 필터링할 수 있습니다. 즉, HTTP 및 HTTPs 패킷만 인터넷으로 전송할 수 있고 다른 유형의 패킷은 허용되지 않습니다. 구성 개요는 다음과 같습니다:

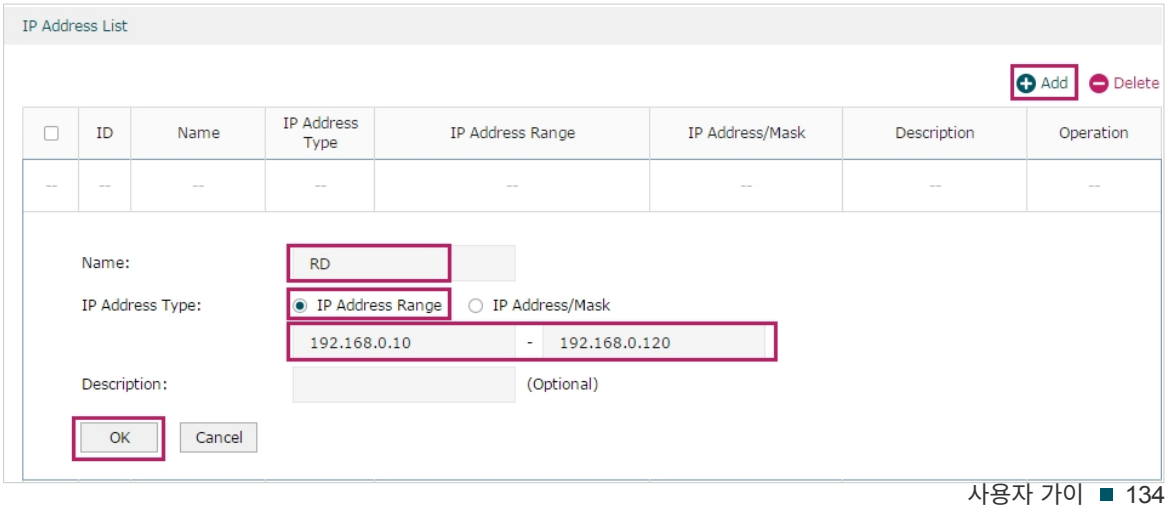
1) **환경설정** 모듈에서 R&D 부서에 대한 IP 그룹을 추가합니다.
2) 기본적으로 HTTP 서비스 유형은 이미 존재하며, **환경설정** 모듈의 서비스 유형 목록에 HTTP를 추가해야 합니다.
3) R&D 부서의 HTTP 및 HTTPs 패킷이 WAN으로 전송되도록 허용하는 두 가지 규칙을 만듭니다.
4) 인터넷을 방문하려면 DNS 서비스가 필요하므로 DNS 패킷이 WAN으로 전송되도록 허용하는 규칙을 추가하세요. DNS 서비스는 기본적으로 서비스 유형 목록에 이미 있습니다.
5) R&D 부서에서 WAN으로 전송되는 모든 패킷을 차단하는 규칙을 만듭니다. 이 규칙은 모든 규칙 중에서 우선순위가 가장 낮아야 합니다.

3.2.3 구성 절차

아래 단계에 따라 구성을 완료하세요:

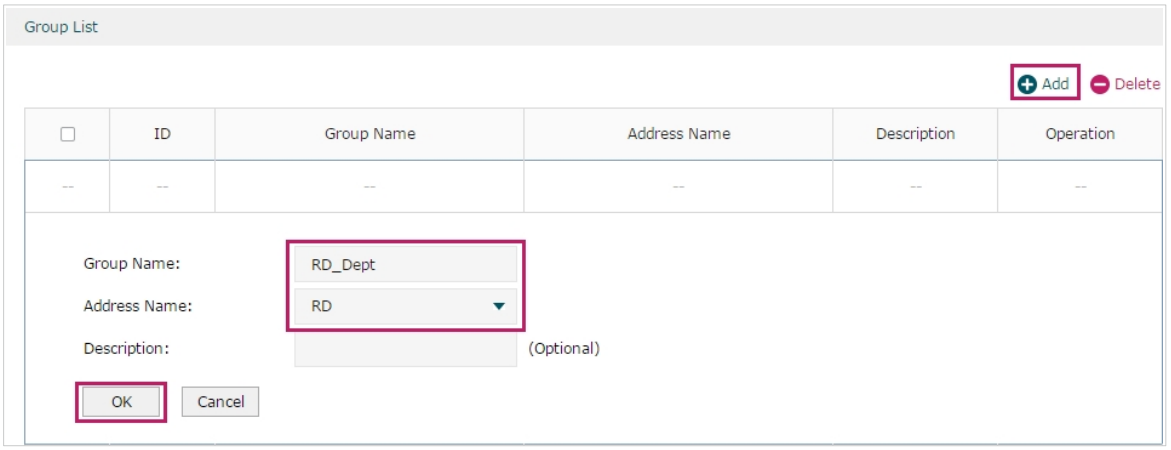
1) **환경설정 > IP 그룹 > IP 주소** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다. RD라는 이름을 지정하고 **IP 주소 범위를** 선택한 다음 R&D 부서의 IP 주소 범위를 입력합니다. **확인을** 클릭합니다.

그림 3-2 IP 주소 범위 구성



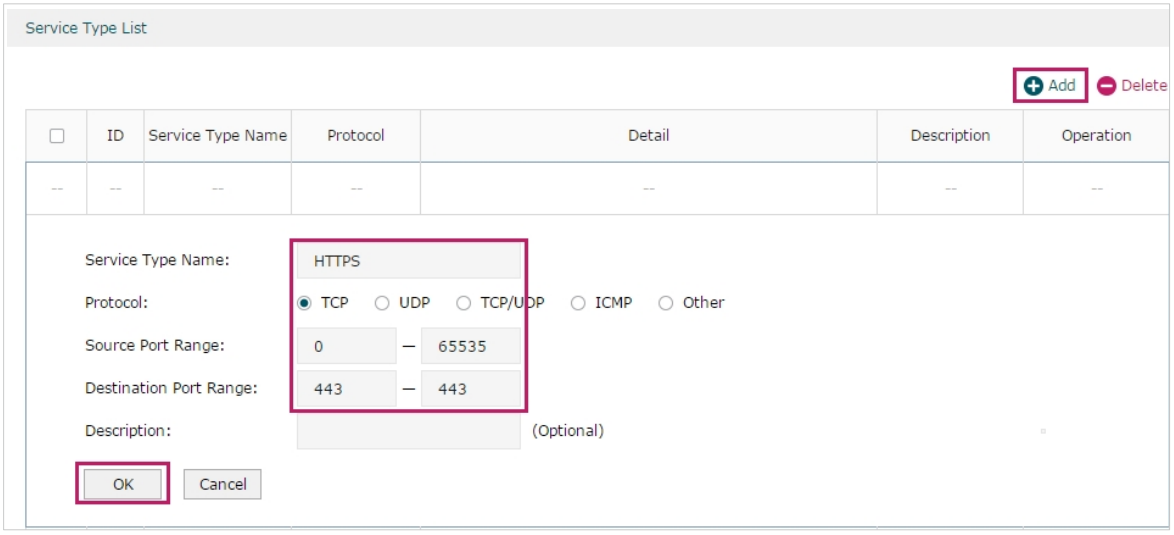
2) **환경설정 > IP 그룹 > IP 그룹** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다. 그룹 이름 "RD_Dept"를 지정하고 미리 설정된 주소 범위 **"**RD"를 선택한 후 **확인을** 클릭합니다.

그림 3-3 IP 그룹 구성



3) **환경설정 > 서비스 유형 > 서비스 유형** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다. 서비스 유형 이름을 "HTTPS"로 지정하고 프로토콜을 "TCP"로 선택한 다음 소스 포트 범위를 "0-65535"로, 대상 포트 범위를 "443-443"으로 지정한 후 **확인을** 클릭합니다.

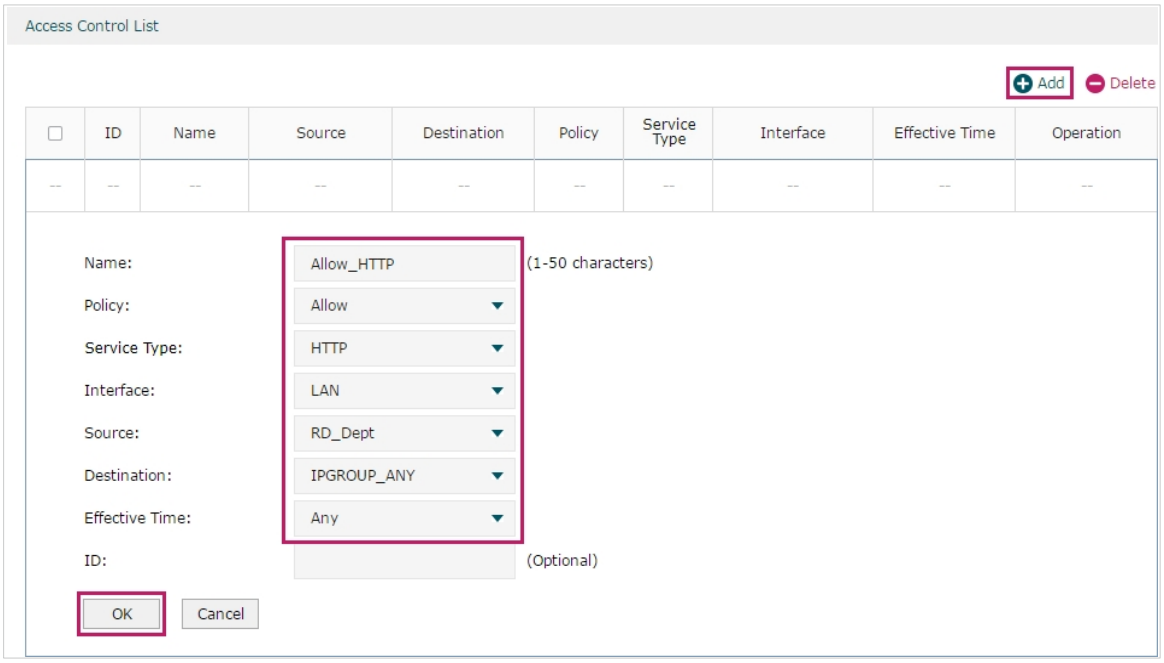
그림 3-4 HTTPS 서비스 유형 구성



4) **방화벽 > 액세스 제어 > 액세스 제어** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다. 이 규칙의 이름을 지정합니다. 규칙 정책으로 "허용"을, 서비스 유형으로 "HTTP"를, 유효 트래픽 방향으로 "LAN -> WAN"을, 소스 IP 그룹으로 "RD_ Dept"를, 대상 IP 그룹으로 "IPGROUP_ANY"를, 유효 시간으로 "임의"를 선택합니다. **확인을** 클릭합니다.

이 규칙은 R&D 부서의 모든 HTTP 패킷이 언제든지 LAN에서 인터넷으로 전송될 수 있음을 의미합니다.

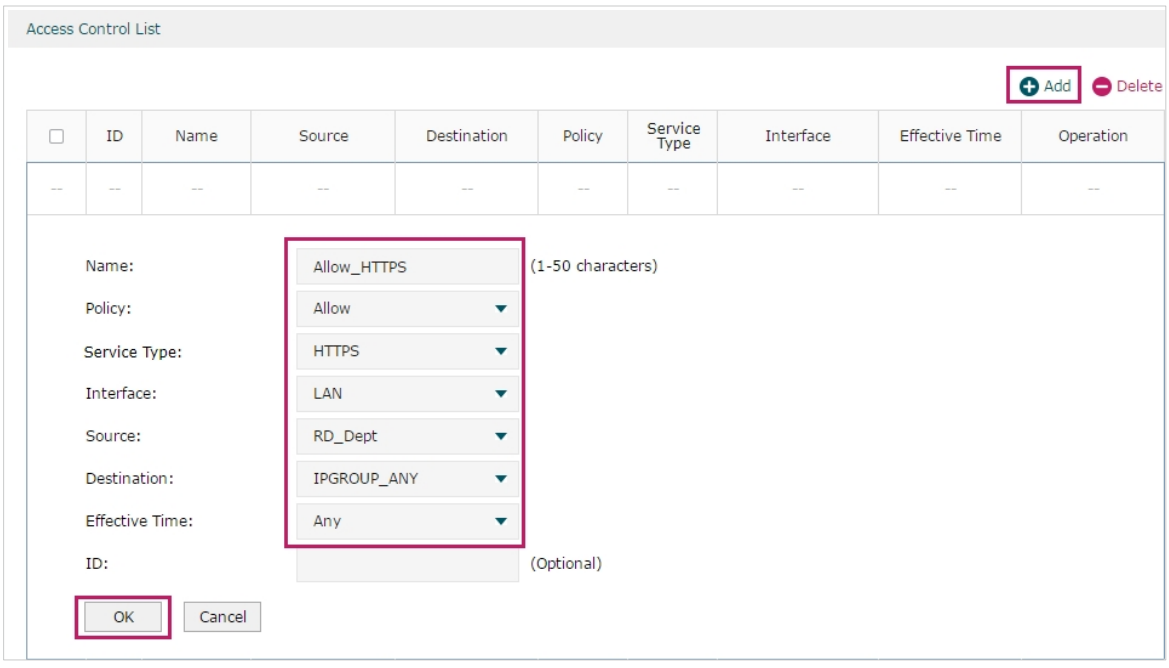
그림 3-5 HTTP 서비스에 대한 허용 규칙 구성



5) **방화벽 > 액세스 제어 > 액세스 제어** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다. 이 규칙의 이름을 지정합니다. 규칙 정책으로 "허용"을, 서비스 유형으로 "HTTPS"를, 유효 트래픽 방향으로 "LAN -> WAN"을, 소스 IP 그룹으로 "RD_ Dept"를, 대상 IP 그룹으로 "IPGROUP_ANY"를, 유효 시간으로 "임의"를 선택합니다. **확인을** 클릭합니다.

이 규칙은 R&D 부서의 모든 HTTPS 패킷을 언제든지 LAN에서 인터넷으로 전송할 수 있도록 허용한다는 의미입니다.

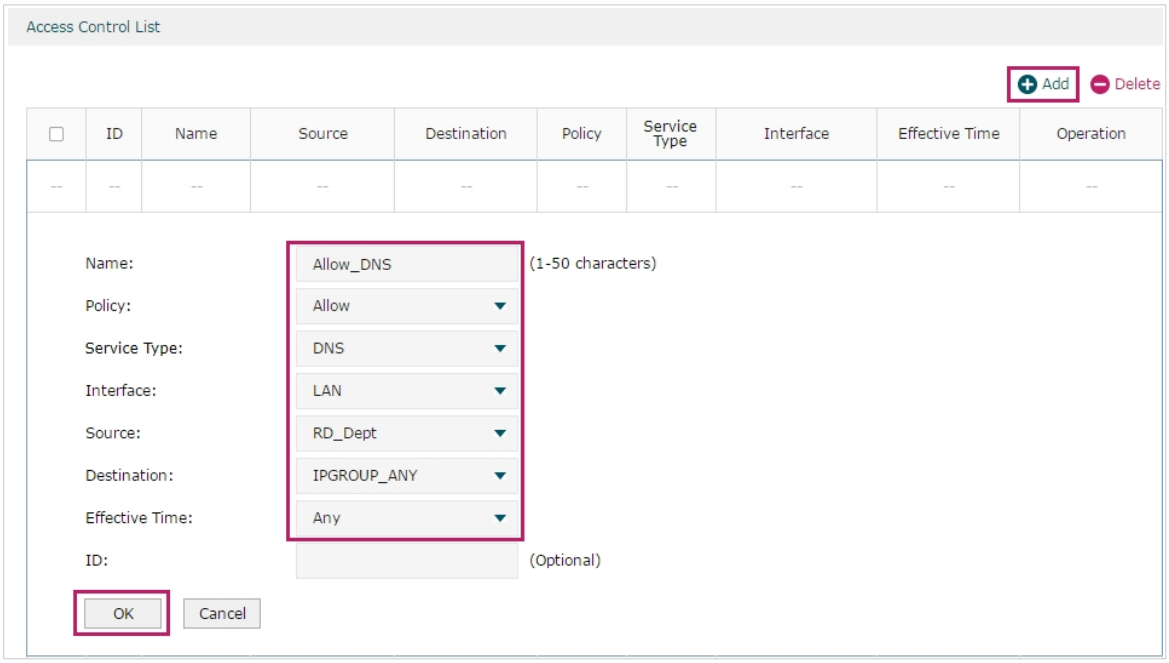
그림 3-6 HTTPS 서비스에 대한 허용 규칙 구성



6) **방화벽 > 액세스 제어 > 액세스 제어** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다. 이 규칙의 이름을 지정합니다. 규칙 정책으로 "허용"을 선택하고, 서비스 유형으로 "DNS"를 선택하고, 유효 트래픽 방향으로 "LAN -> WAN"을 선택하고, RD_.

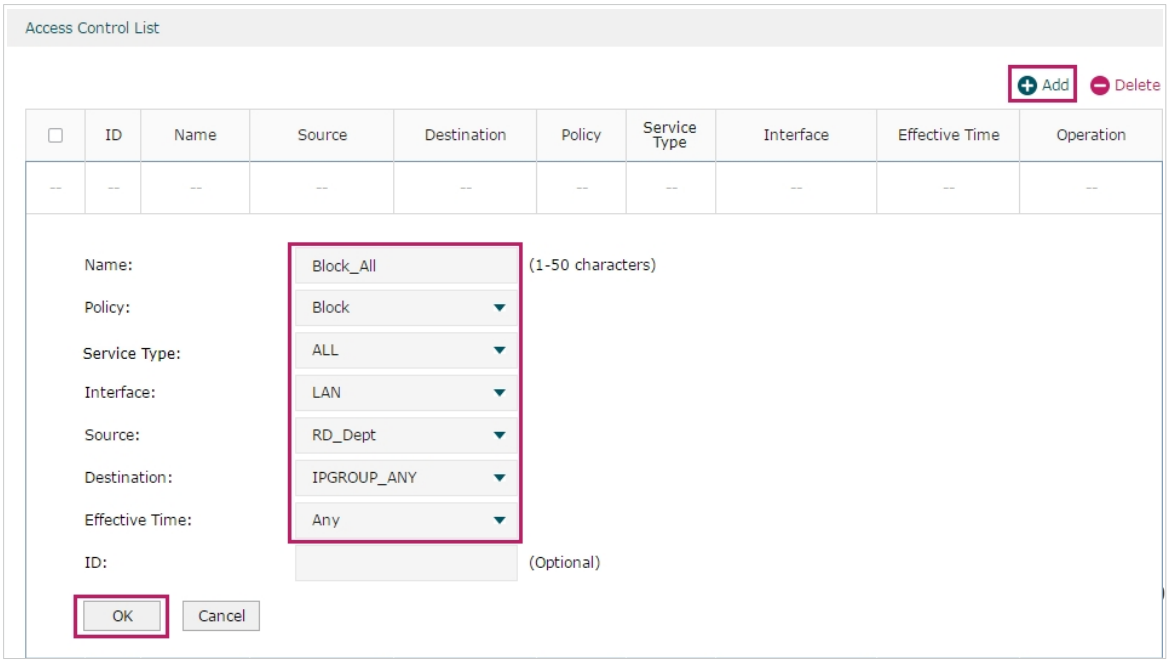
Dept"를 소스 IP 그룹으로, "IPGROUP_ANY"를 대상 IP 그룹으로, "Any"를 적용 시간으로 입력합니다. **확인을** 클릭합니다.

이 규칙은 R&D 부서의 모든 DNS 패킷을 언제든지 LAN에서 인터넷으로 전송할 수 있음을 의미합니다.

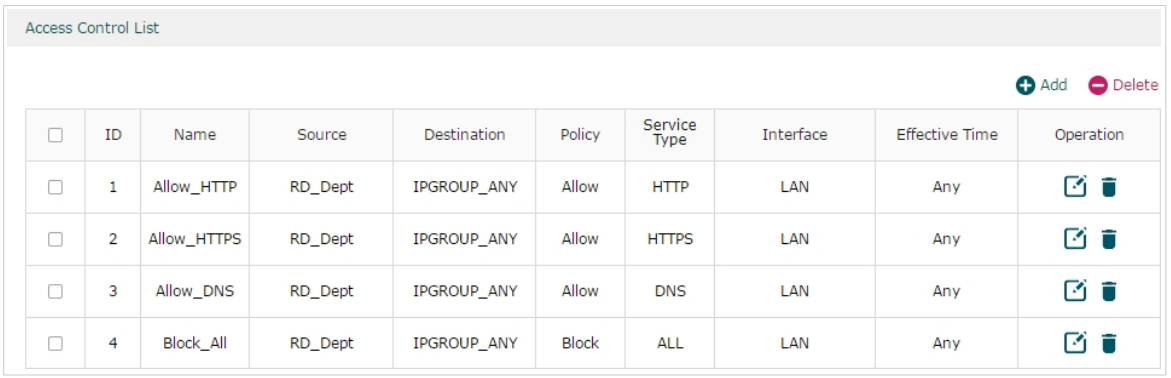


7) **방화벽 > 액세스 제어 > 액세스 제어** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다. 이 규칙의 이름을 지정합니다. 규칙 정책으로 "차단"을, 서비스 유형으로 "ALL"을, 유효 트래픽 방향으로 "LAN -> WAN"을, 소스 IP 그룹으로 "RD_ Dept"를, 대상 IP 그룹으로 "IPGROUP_ANY"를, 유효 시간으로 "Any"를 선택합니다. **확인을** 클릭합니다.

이 규칙은 R&D 부서의 모든 패킷이 LAN에서 인터넷으로 전송되는 것을 항상 차단한다는 의미입니다.



8) 구성 결과를 확인합니다. 액세스 제어 목록에서 ID가 작은 규칙이 더 높은 우선순위를 갖습니다. 라우터는 우선순위가 가장 높은 규칙부터 일치시키므로 세 개의 허용 규칙이 차단 규칙에 비해 ID 번호가 더 작은지 확인하세요. 이렇게 하면 라우터는 수신된 패킷이 3개의 허용 규칙과 일치하는지 먼저 확인하고 허용 규칙 중 하나라도 일치하지 않는 패킷만 차단합니다.



	ID	Name	Source	Destination	Policy	Service Type	Interface	Effective Time	Operation
☐	1	Allow_HTTP	RD_Dept	IPGROUP_ANY	Allow	HTTP	LAN	Any	
☐	2	Allow_HTTPS	RD_Dept	IPGROUP_ANY	Allow	HTTPS	LAN	Any	
☐	3	Allow_DNS	RD_Dept	IPGROUP_ANY	Allow	DNS	LAN	Any	
☐	4	Block_All	RD_Dept	IPGROUP_ANY	Block	ALL	LAN	Any	

파트 8

행동 제어 구성

챕터

1 행동 제어

1.1 개요

행동 제어 기능을 사용하면 로컬 호스트의 온라인 행동을 제어할 수 있습니다. URL 또는 키워드를 사용하여 특정 호스트가 특정 웹사이트에 액세스하는 것을 차단하고, HTTP 게시물을 차단하고, 인터넷에서 특정 유형의 파일을 다운로드하지 못하도록 할 수 있습니다.

1.2 지원되는 기능

행동 제어 모듈은 두 가지 기능을 지원합니다: 웹 필터링과 웹 보안입니다.

웹 필터링

웹 필터링은 특정 웹사이트를 필터링하는 데 사용됩니다. 라우터는 웹사이트를 필터링하는 두 가지 방법을 제공합니다: 웹 그룹 필터링과 URL 필터링입니다.

- 웹 그룹 필터링: 여러 웹사이트를 웹 그룹으로 구성하고 그룹에 대한 필터링 규칙을 설정할 수 있습니다. 둘 이상의 그룹을 만들 수 있으며 여러 그룹이 동일한 필터링 규칙을 공유할 수 있습니다.

- URL 필터링: 특정 전체 URL 또는 키워드에 대한 필터링 규칙을 직접 설정할 수 있습니다.

웹 보안

웹 보안은 로컬 사용자의 특정 온라인 동작을 제어하는 데 사용됩니다. 이 기능을 구성하여 HTTP 게시를 차단하면 로컬 사용자는 로그인, 댓글 제출 또는 HTTP 게시가 필요한 기타 작업을 수행할 수 없습니다. 또한 로컬 사용자가 인터넷에서 특정 유형의 파일을 다운로드하지 못하도록 금지할 수도 있습니다.

2 행동 제어 구성

행동 제어 모듈에서는 다음 기능을 구성할 수 있습니다:

- 웹 필터링
- 웹 보안

2.1 웹 필터링 구성

웹사이트를 필터링하는 방법에는 두 가지가 있습니다: 웹 그룹 필터링과 URL 필터링입니다.

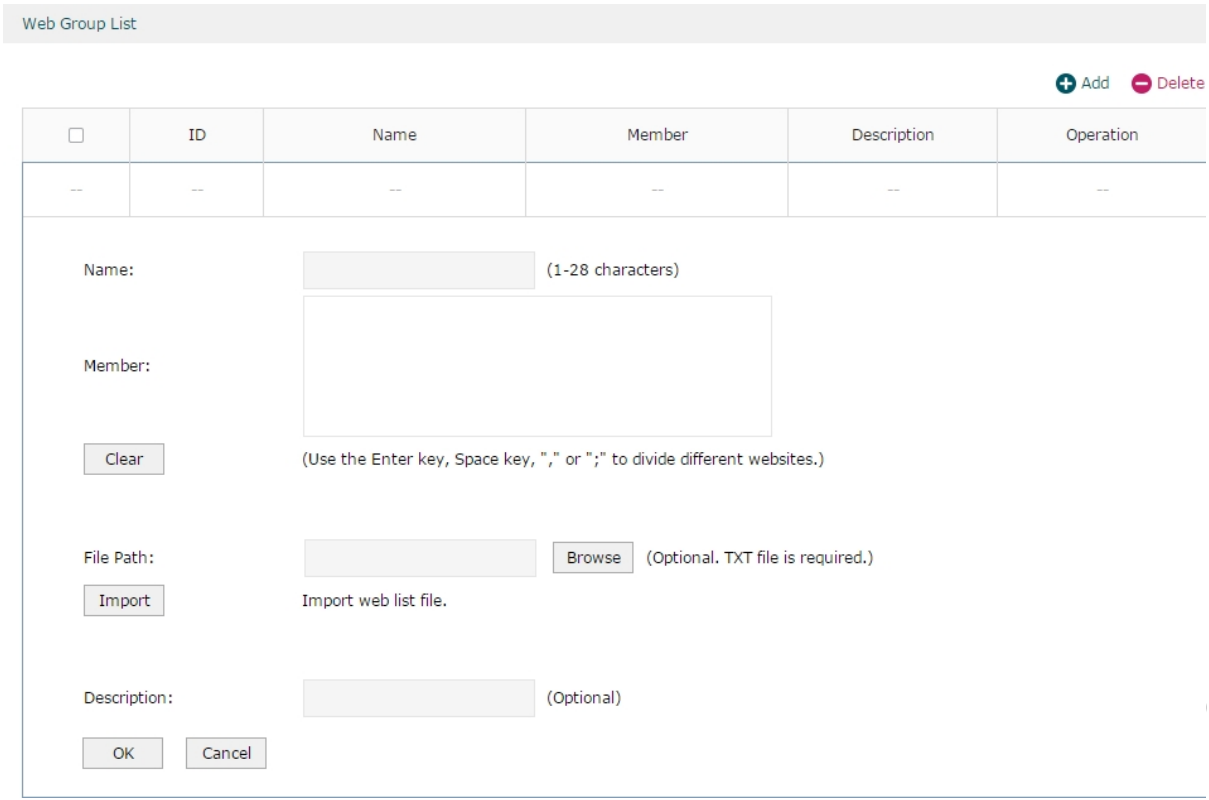
2.1.1 웹 그룹 필터링 구성

웹 그룹 필터링을 구성하려면 먼저 하나 이상의 웹 그룹을 추가한 다음 생성된 그룹을 사용하여 웹 그룹 필터링 항목을 추가합니다.

웹 그룹 추가

행동 제어 > 웹 필터링 > 웹 그룹 메뉴를 선택하고 **추가를** 클릭하여 다음 페이지를 로드합니다.

그림 2-1 웹 그룹 페이지



행동 제어 구성

다음 매개변수를 구성하고 **확인을** 클릭합니다.

이름	그룹의 이름을 지정합니다. 각 그룹의 이름은 반복할 수 없습니다.
회원	그룹에 웹사이트 회원을 한 명 이상 추가합니다. 웹사이트 멤버의 형식은 "www.tp-link.com" 또는 "*.tp-link.com"이며, 여기서 "*"는 와일드카드입니다. Enter 키, 스페이스 키, "," 또는 ";"를 사용하여 여러 웹사이트를 구분합니다.
파일 경로	호스트에서 TXT 파일로 회원 목록을 가져옵니다. 형식은 "www.tp-link. com" 또는 "*.tp-link.com"이며, 여기서 "*"는 와일드카드입니다. Enter 키, 스페이스 키, "," 또는 ";"을 사용하여 여러 웹사이트를 구분합니다.
설명	그룹에 대한 간단한 설명을 입력합니다.

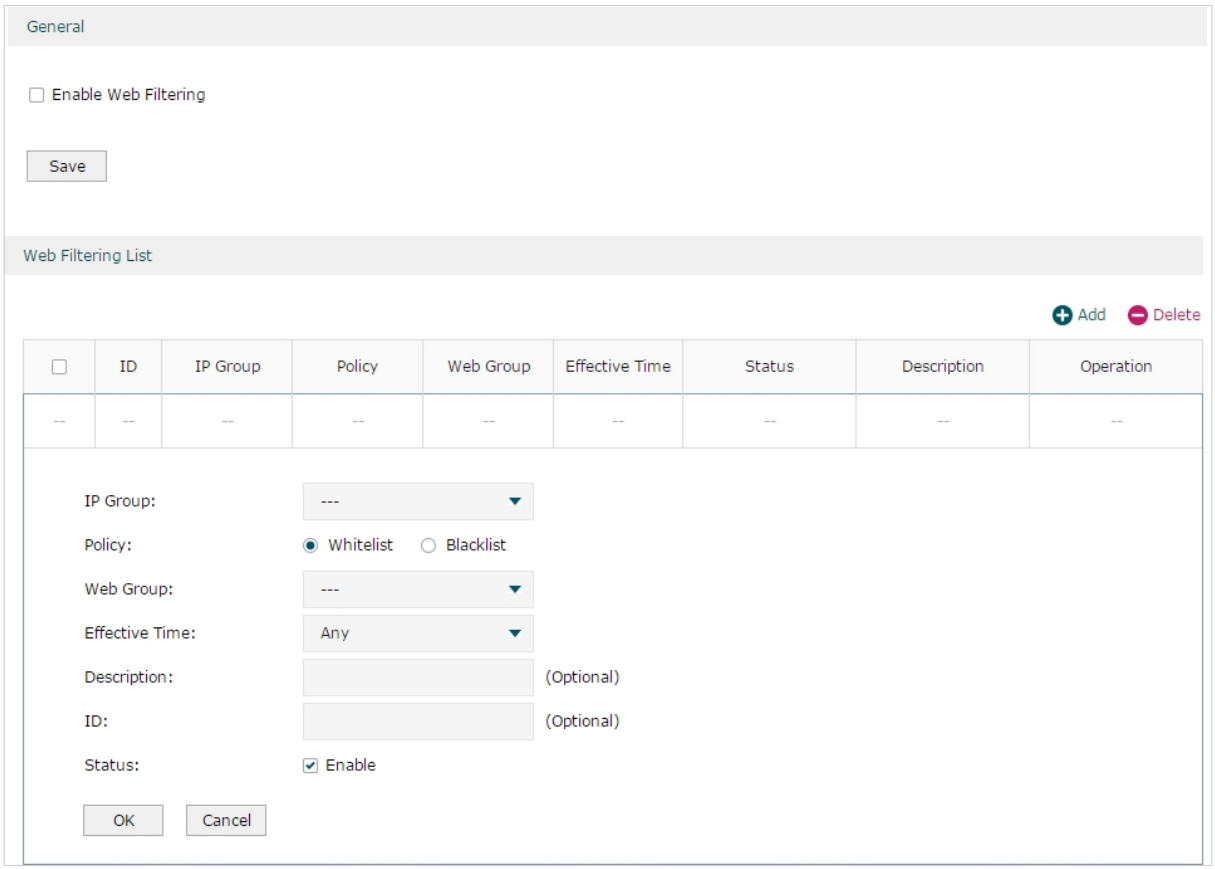
웹 그룹 필터링 항목 추가

웹 그룹 항목을 구성하기 전에 **환경설정** 모듈로 이동하여 필요에 따라 IP 그룹 및 유효 시간을 구성하세요.

행동 제어 > 웹 필터링 > 웹 그룹 필터링 메뉴를 선택하고 **추가를** 클릭합니다.

를 클릭하면 다음 페이지가 로드됩니다.

그림 2-2 웹 그룹 필터링 페이지



웹 그룹 필터링 항목을 추가하려면 아래 단계를 따르세요:

1) **웹 필터링 목록** 섹션에서 필요한 매개변수를 구성하고 **확인을** 클릭합니다.

IP 그룹	규칙의 IP 그룹을 선택합니다. 여기서 참조하는 IP 그룹은 **환경설정 > IP 그룹** 페이지에서 만들 수 있습니다.

정책	선택한 웹 그룹에 있는 웹사이트를 허용하거나 거부하도록 선택합니다.
웹 그룹	하나 이상의 웹 그룹을 선택합니다. 여기서 참조하는 웹 그룹은 **행동 제어 > 웹 필터링 > 웹 그룹** 페이지에서 만들 수 있습니다.
유효 시간	유효 시간을 선택합니다. 여기서 참조하는 유효 시간은 **환경설정 > 시간 범위** 페이지에서 만들 수 있습니다.
설명	그룹에 대한 간단한 설명을 입력합니다.
ID	규칙 ID를 지정합니다. ID가 작을수록 우선 순위가 높습니다. 이 값은 선택 사항입니다. 이 필드를 비워 둔 상태에서 새로 추가된 규칙은 모든 규칙 중에서 가장 큰 ID를 갖게 되며, 이는 새로 추가된 규칙의 우선 순위가 가장 낮다는 의미입니다.
상태	규칙을 활성화하려면 확인란을 선택합니다.

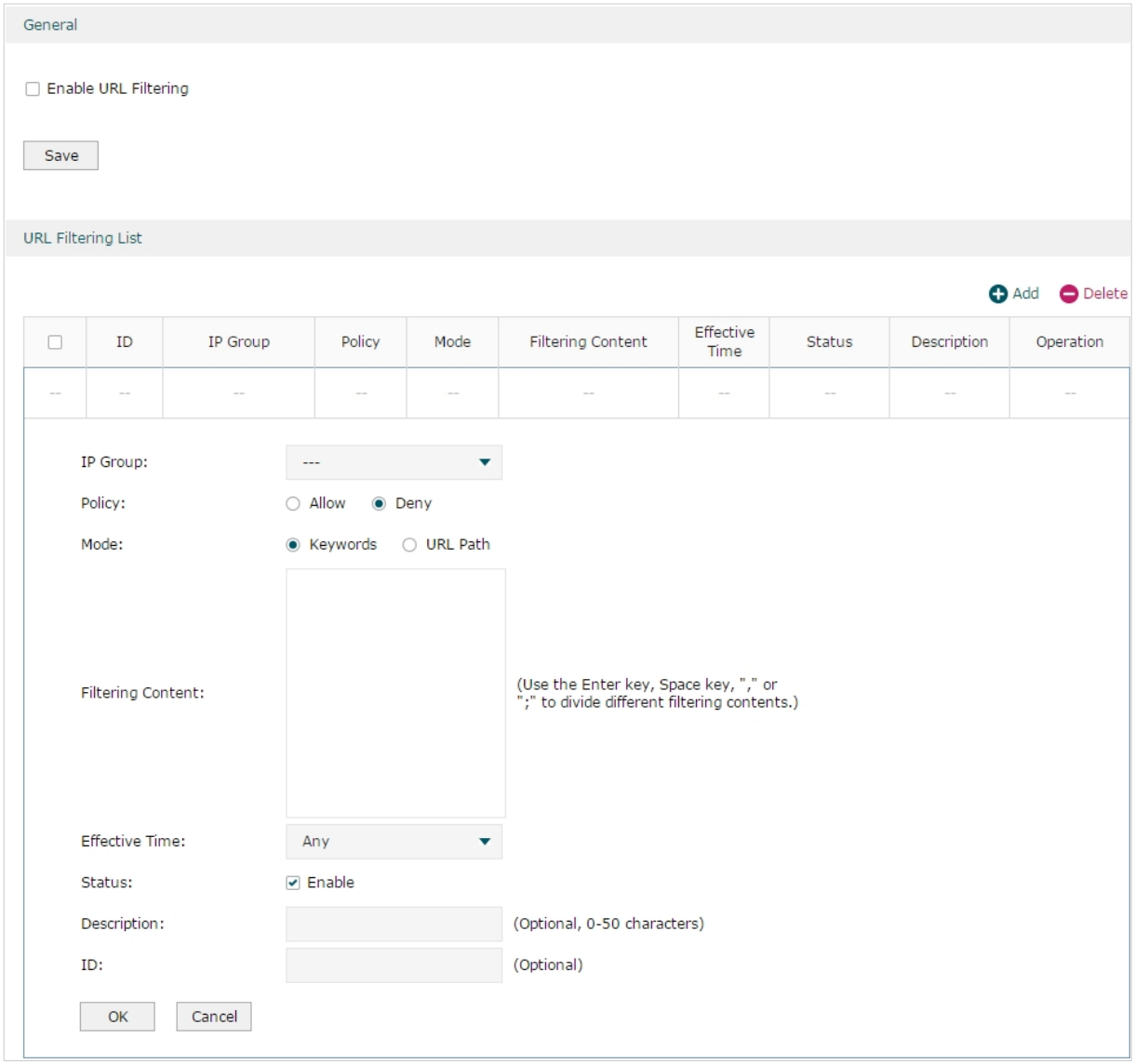
2) **일반** 섹션에서 웹 필터링을 사용 설정합니다. **저장을** 클릭합니다.

2.1.2 URL 필터링 구성

URL 필터링을 구성하기 전에 **환경설정** 모듈로 이동하여 필요에 따라 IP 그룹 및 유효 시간을 구성하세요.

행동 제어 > 웹 필터링 > URL 필터링 메뉴를 선택하고 **추가를** 클릭하여 다음 페이지를 로드합니다.

그림 2-3 URL 필터링 페이지



URL 필터링을 구성하려면 아래 단계를 따르세요:

1) URL 필터링 목록 섹션에서 **추가를** 클릭하고 필요한 매개변수를 구성합니다. 클릭 **OK.**

IP 그룹	규칙의 IP 그룹을 선택합니다. 여기서 참조하는 IP 그룹은 **환경설정 > IP 그룹** 페이지에서 만들 수 있습니다.

정책	필터링 콘텐츠와 일치하는 웹사이트를 허용하거나 거부하도록 선택합니다.

모드	필터링 모드를 선택합니다. **키워드**: 웹사이트 주소에 키워드가 포함되어 있는 경우 해당 웹사이트에 정책이 적용됩니다. **URL 경로**: 웹사이트 주소가 전체 URL 중 어느 것과도 동일한 경우 이 웹사이트에 정책이 적용됩니다.
콘텐츠 필터링	필터링 콘텐츠를 추가합니다. Enter 키, 스페이스 키, "," 또는 ";"을 사용하여 서로 다른 필터링 콘텐츠를 구분합니다. "."는 이 규칙이 모든 웹사이트에 적용됨을 의미합니다. 예를 들어 웹사이트 A는 허용하고 다른 웹사이트는 거부하려는 경우 필터링 콘텐츠가 "A"인 허용 규칙을 추가하고 필터링 콘텐츠가 "."인 거부 규칙을 추가하면 됩니다. "." 규칙은 ID 번호가 가장 커야 하며, 이는 우선순위가 가장 낮다는 것을 의미합니다.
유효 시간	유효 시간을 선택합니다. 여기서 참조하는 유효 시간은 **환경설정 > 시간 범위** 페이지에서 만들 수 있습니다.
상태	확인란을 선택하여 규칙을 활성화합니다.
설명	그룹에 대한 간단한 설명을 입력합니다.
ID	규칙 ID를 지정합니다. ID가 작을수록 우선 순위가 높습니다. 이 값은 선택 사항입니다. 이 값을 구성하지 않고 새로 추가된 규칙은 모든 규칙 중에서 가장 큰 ID를 가지며, 이는 새로 추가된 규칙의 우선 순위가 가장 낮다는 것을 의미합니다.

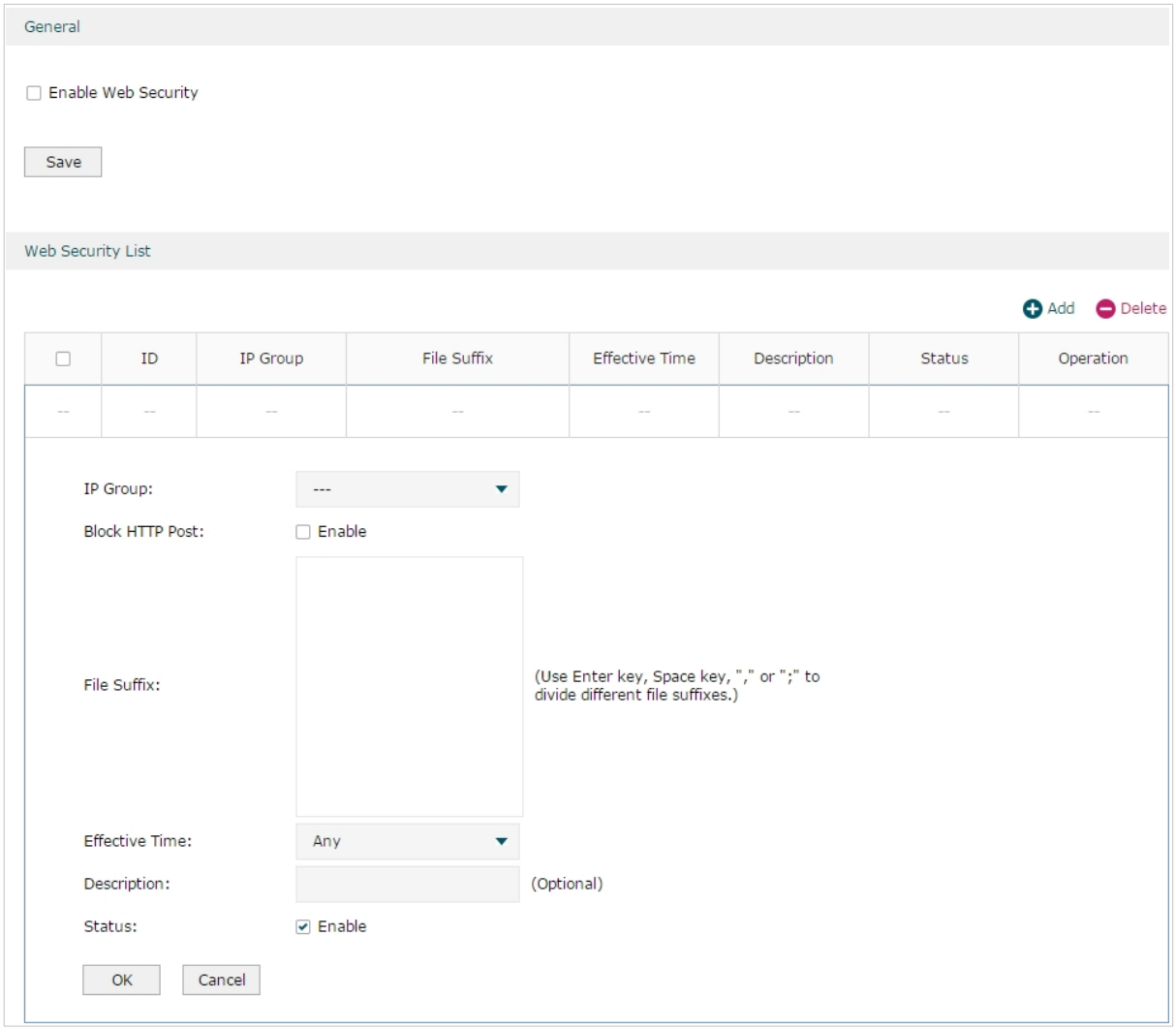
2) **일반** 섹션에서 URL 필터링을 사용 설정합니다. **저장을** 클릭합니다.

2.2 웹 보안 구성

웹 보안을 구성하기 전에 **환경설정** 모듈로 이동하여 필요에 따라 IP 그룹 및 유효 시간을 구성하세요.

행동 제어 > 웹 보안 > 웹 보안 메뉴를 선택하고 **추가를** 클릭하여 다음 페이지를 로드합니다.

그림 2-4 웹 보안 페이지



아래 단계에 따라 웹 보안을 구성합니다.

1) **웹 보안 목록** 섹션에서 다음 매개변수를 구성하고 **확인을** 클릭하여 웹 보안 규칙을 추가합니다.

IP 그룹	규칙의 IP 그룹을 선택합니다. 여기서 참조하는 IP 그룹은 **환경설정 > IP 그룹** 페이지에서 만들 수 있습니다.
HTTP 글 차단	이 옵션을 활성화하면 HTTP 글이 차단됩니다. 선택한 IP 그룹의 호스트는 로그인, 댓글 제출 또는 HTTP 게시물을 사용하여 어떤 작업도 할 수 없습니다.

행동 제어 구성

파일 접미사파일 접미사를 입력하여 파일 형식을 지정합니다. Enter 키, 스페이스 키, "," 또는 ";"을 사용하여 서로 다른 파일 접미사를 구분할 수 있습니다. 선택한 IP 그룹의 호스트는 인터넷에서 이러한 유형의 파일을 다운로드할 수 없습니다.	
유효 시간	유효 시간을 선택합니다. 여기서 참조하는 유효 시간은 **환경설정 > 시간 범위** 페이지에서 만들 수 있습니다.
설명	그룹에 대한 간단한 설명을 입력합니다.
상태	확인란을 선택하여 규칙을 활성화합니다.

2) **일반** 섹션에서 웹 보안을 사용 설정하고 **저장을** 클릭합니다.

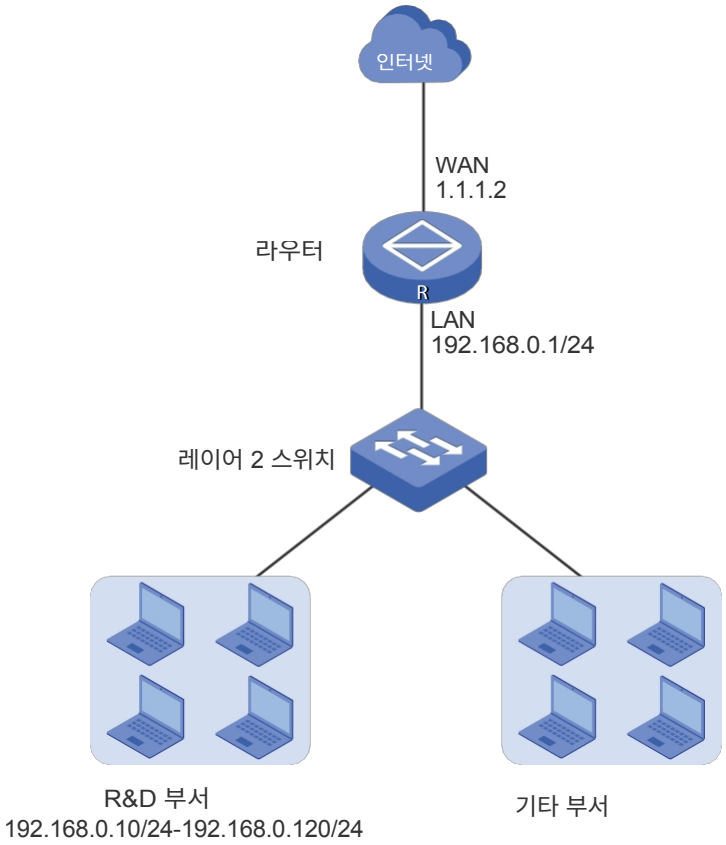
3 구성 예시

3.1 액세스 제어 예제

3.1.1 네트워크 요구 사항

아래 다이어그램에서 R&D 부서와 일부 다른 부서는 레이어 2 스위치에 연결되어 있으며 라우터를 통해 인터넷에 액세스합니다. 데이터 보안을 위해 R&D 부서 사용자는 회사의 공식 웹사이트(예: https://www.tp-link.com)만 방문할 수 있습니다. 다른 부서의 경우 웹사이트 접속에 제한이 없습니다.

그림 3-1 네트워크 토폴로지



3.1.2 구성 체계

웹 필터링을 구성하여 특정 호스트의 웹사이트 액세스를 제한할 수 있습니다. 웹 그룹 필터링과

URL 필터링 모두 이를 수행할 수 있습니다. 이 예에서 웹 그룹 필터링과 URL 필터링의 구성 차이는 다음과 같습니다:

- 웹 그룹 필터링에서 필터링 규칙을 구성하기 전에 웹 그룹에 공식 웹사이트 주소를 추가해야 합니다.

- URL 필터링에서는 필터링 규칙에 공식 웹사이트 주소를 직접 지정할 수 있습니다.

여기서는 웹 그룹 필터링을 예로 들어 보겠습니다. 구성 개요는 다음과 같습니다:

1) **환경설정** 모듈에서 R&D 부서에 대한 IP 그룹을 추가합니다.

2) 그룹 구성원 www.tp-link.com 으로 웹 그룹을 만듭니다.

3) R&D 부서 사용자가 www.tp-link.com 에 액세스할 수 있도록 화이트리스트 규칙을 추가합니다.

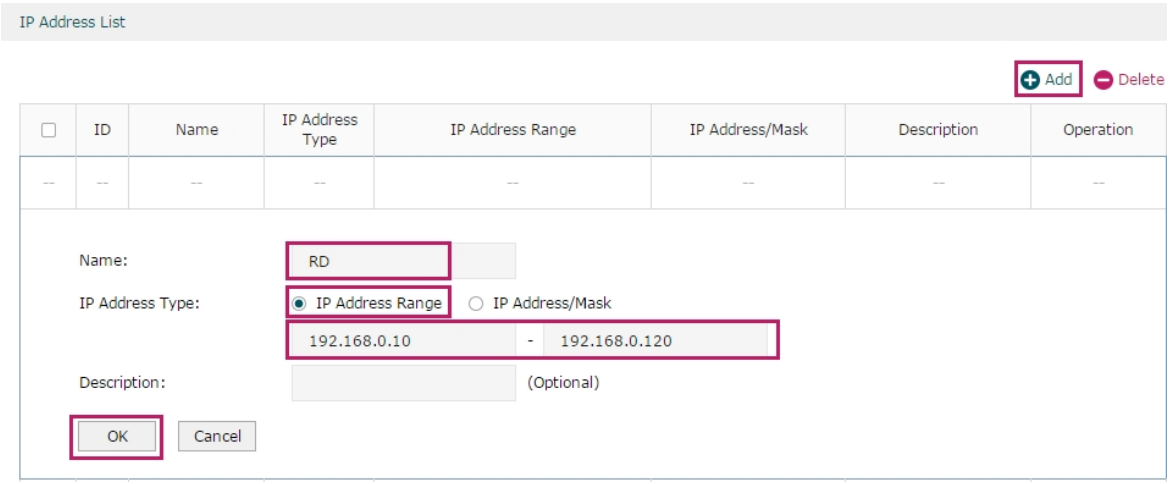
4) R&D 부서 사용자가 모든 웹사이트에 액세스하는 것을 금지하는 블랙리스트 규칙을 추가합니다. 이 규칙의 우선순위는 화이트리스트 규칙보다 낮아야 한다는 점에 유의하세요.

3.1.3 구성 절차

아래 단계에 따라 구성을 완료하세요:

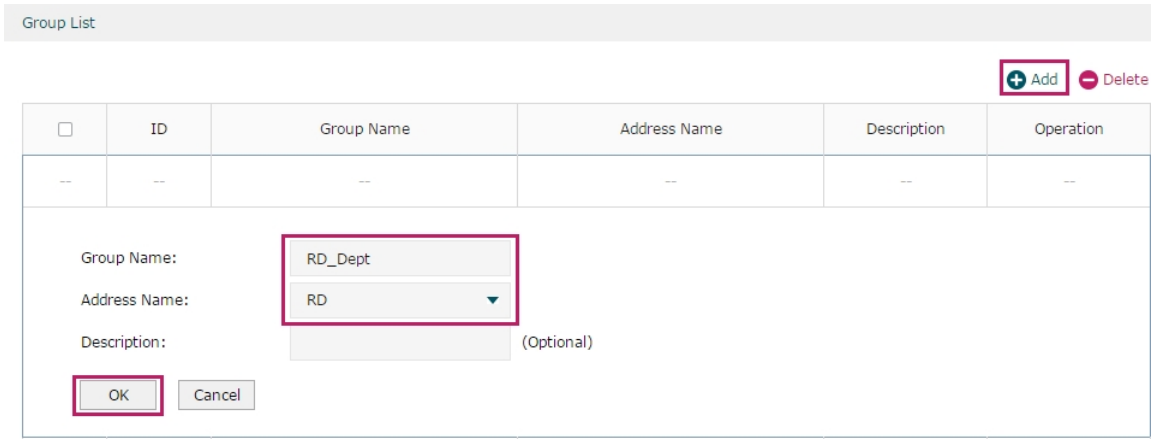
1) **환경설정 > IP 그룹 > IP 주소** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다. 이름을 "RD"로 지정하고 **IP 주소 범위를** 선택한 다음 R&D 부서의 IP 주소 범위를 입력합니다. **확인을** 클릭합니다.

그림 3-2 IP 주소 범위 구성



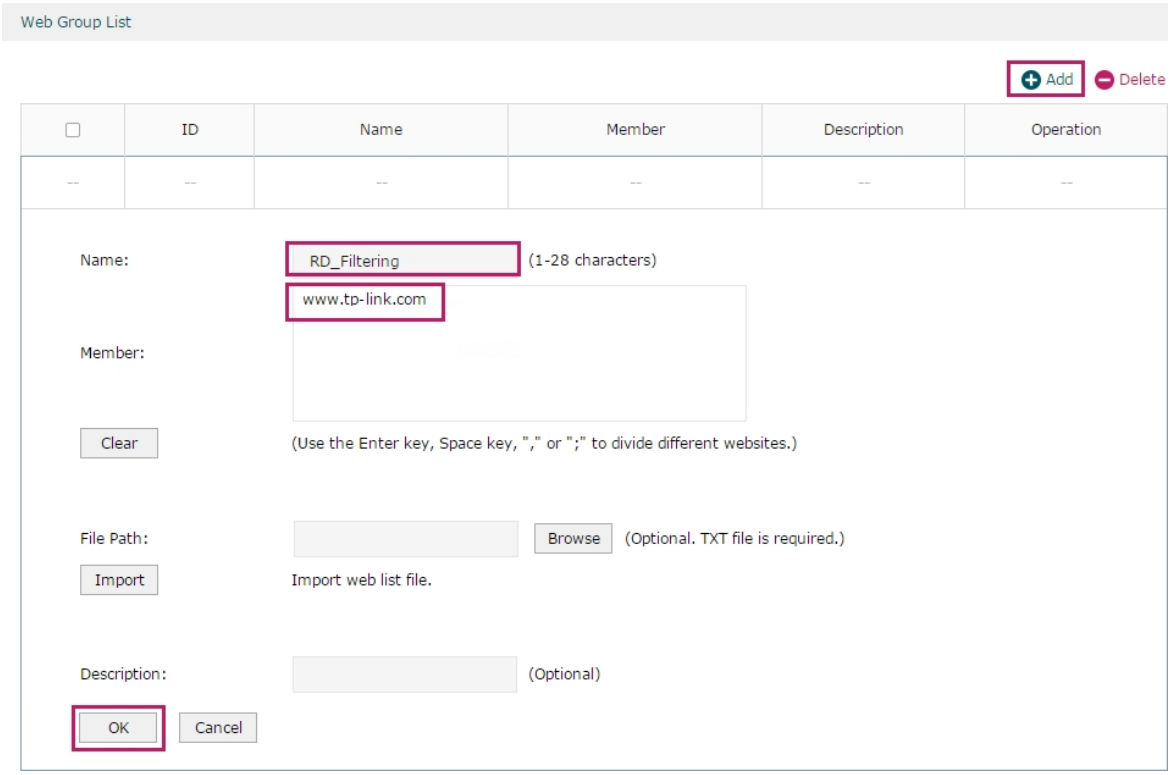
2) **환경설정 > IP 그룹 > IP 그룹** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다. 그룹 이름 "RD_Dept"를 지정하고 미리 설정된 주소 범위 "RD"를 선택한 후 **확인을** 클릭합니다.

그림 3-3 IP 그룹 구성


Group List
Add
Delete
ID
Group Name
Address Name
Description
Operation
Group Name:
RD_Dept
Address Name:
RD
Description:
(Optional)
OK
Cancel

3) **동작 제어 > 웹 필터링 > 웹 그룹** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다. 이 웹 그룹의 이름을 "RD_Filtering"으로 지정하고 멤버 "www.tp-link.com"를 추가합니다. **확인을** 클릭합니다.

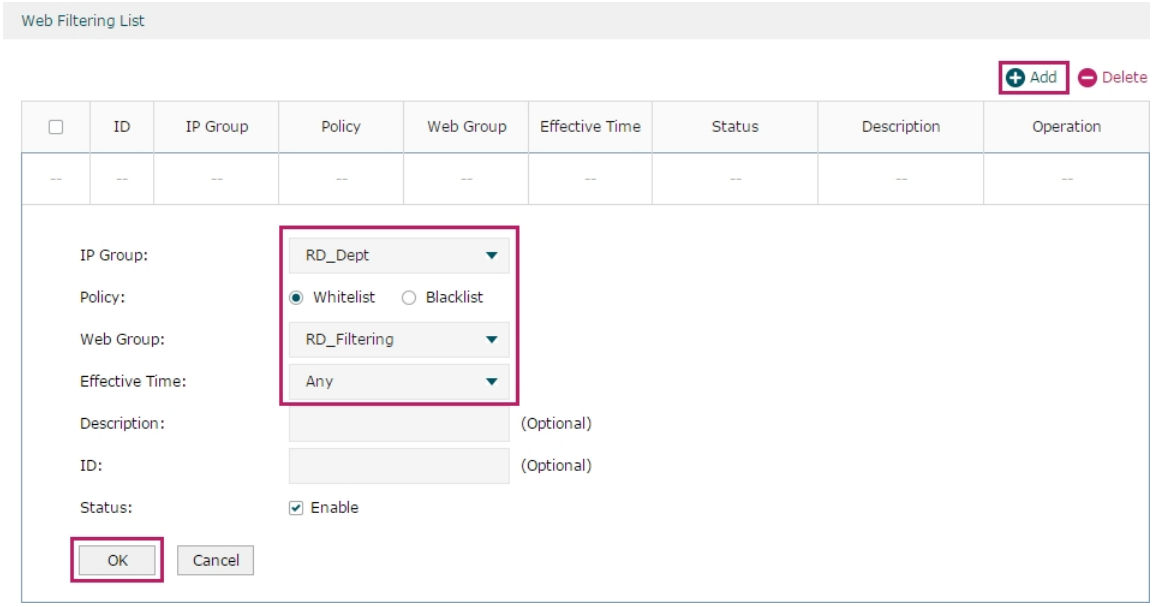
그림 3-4 웹 그룹 구성



4) **행동 제어 > 웹 필터링 > 웹 그룹 필터링** 메뉴를 선택하여 구성 페이지를 로드하고 **추가를** 클릭합니다. **IP 그룹으로** 'RD_Dept', **정책으로** '화이트리스트', **웹 그룹으로** 'RD_필터링', **유효 시간으로** '모두'를 선택합니다. **확인을** 클릭합니다.

이 규칙에 따라 R&D 부서의 호스트는 언제든지 www.tp-link.com 웹사이트에 액세스할 수 있습니다.

그림 3-5 화이트리스트 규칙 구성하기

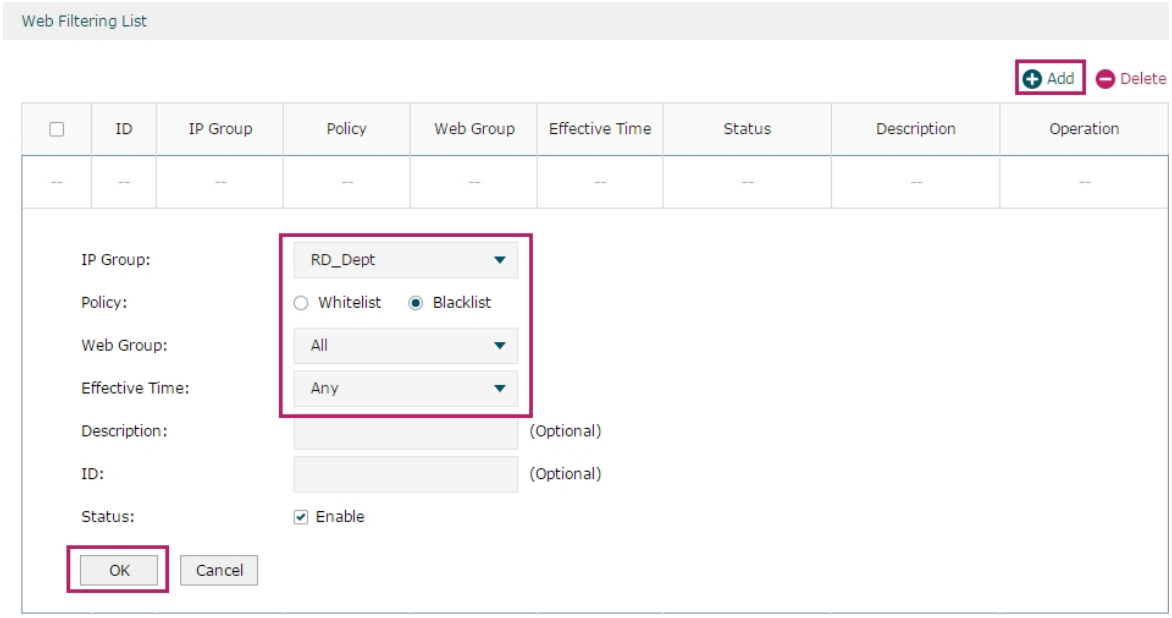

Web Filtering List
Add
Delete
ID
IP Group
Policy
Web Group
Effective Time
Status
Description
Operation
IP Group:
RD_Dept
Policy:
Whitelist
Blacklist
Web Group:
RD_Filtering
Effective Time:
Any
Description:
(Optional)
ID:
(Optional)
Status:
Enable
OK
Cancel

5) 같은 페이지에서 **추가를** 클릭합니다. **IP** 그룹으로 "RD_Dept"를 선택하고, 블랙리스트로 "블랙리스트"를 선택합니다.

정책, **웹 그룹은** '모두'로, **적용 시간은** '모두'로 선택합니다. **확인을** 클릭합니다.

이 규칙에 따라 R&D 부서의 호스트는 항상 모든 웹사이트에 대한 액세스가 거부됩니다.

그림 3-6 블랙리스트 규칙 구성

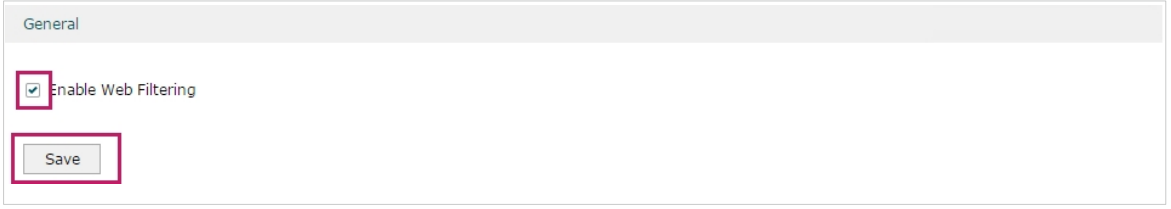


6) 같은 페이지에서 구성을 확인합니다. 웹 필터링 목록에서 ID가 작은 규칙의 우선순위가 더 높습니다. 라우터는 우선순위가 가장 높은 규칙부터 일치시키므로 화이트리스트 규칙의 ID 번호가 더 작은지 확인하세요. 이러한 방식으로 라우터는 호스트가 화이트리스트 웹사이트에 액세스하는 것은 허용하고 다른 웹사이트에 액세스하는 것은 거부합니다.

그림 3-7 구성 결과 확인

7) 같은 페이지의 **일반** 섹션에서 웹 필터링을 전역으로 사용 설정하고 **저장을** 클릭합니다.

그림 3-8 웹 필터링 활성화

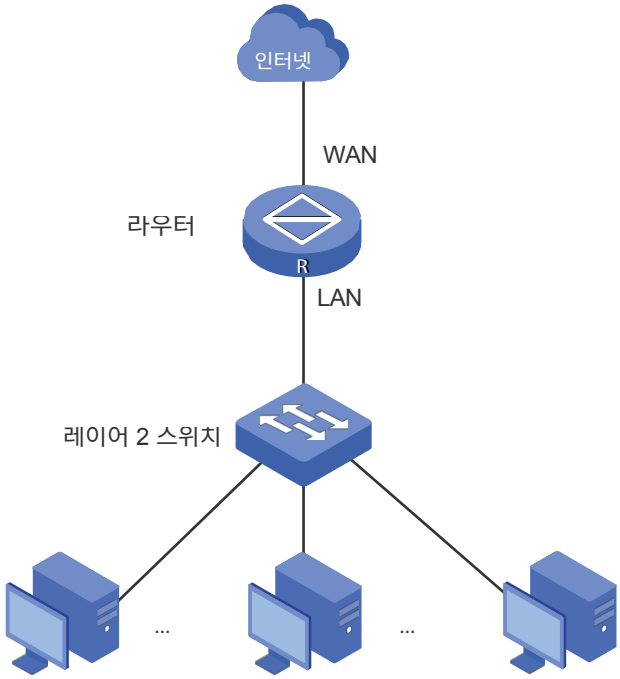


3.2 웹 보안의 예

3.2.1 네트워크 요구 사항

아래 다이어그램에서 회사의 호스트는 레이어 2 스위치에 연결되어 있으며 라우터를 통해 인터넷에 액세스합니다. 보안상의 이유로 LAN에 있는 사용자는 인터넷에서 로그인, 댓글 제출 또는 rar 파일 다운로드가 불가능합니다.

그림 3-9 네트워크 토폴로지



3.2.2 구성 체계

이러한 요구 사항을 충족하도록 웹 보안을 구성할 수 있습니다. 로그인 및 댓글 제출과 같은 동작을 차단하려면 HTTP 게시물을 차단하도록 라우터를 구성하고, rar 파일의 다운로드를 차단하려면 파일 접미사 열에 접미사 'rar'를 지정하면 됩니다.

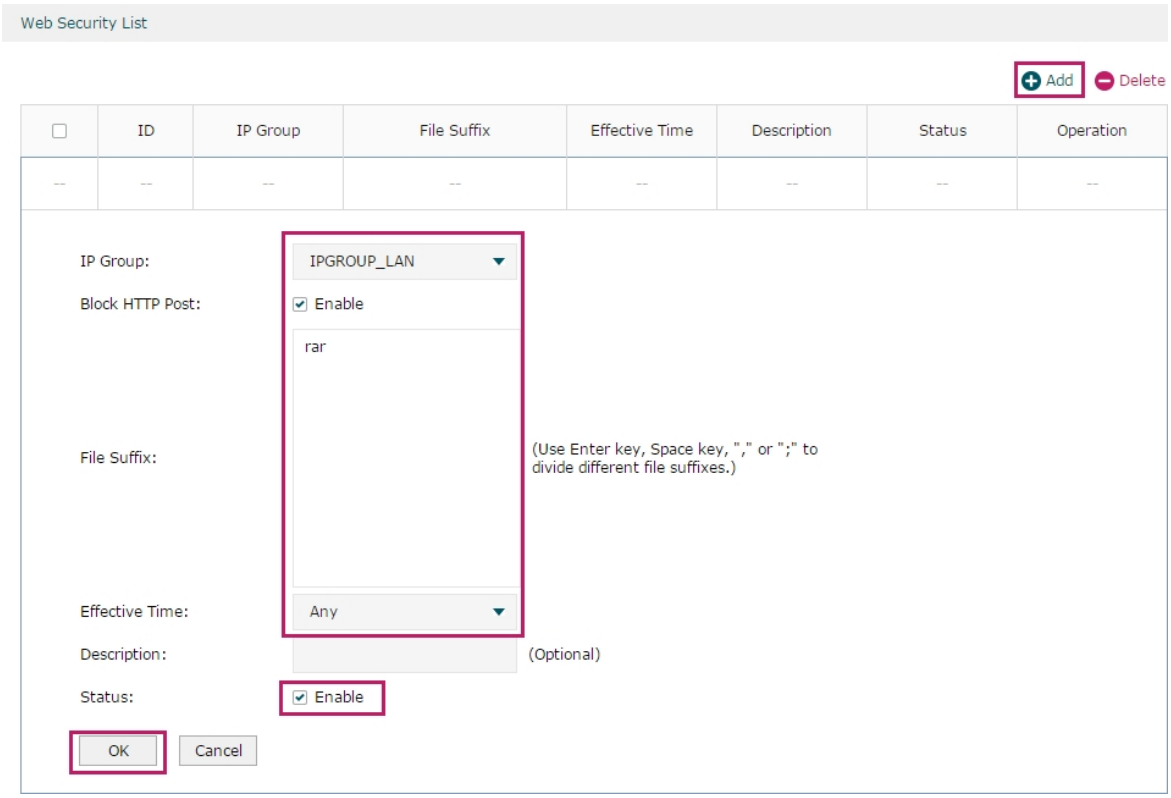
3.2.3 구성 절차

아래 단계에 따라 구성을 완료하세요:

1) **행동 제어 > 웹 보안 > 웹 보안** 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다. **IP 그룹으로** "IPGROUP_LAN"을 선택하고, **HTTP 게시물 차단을** 활성화하고, **파일 접미사에** "rar"

을 입력하고, **유효 시간으로** "모두"를 선택하고, **상태를** "사용"으로 유지합니다. **확인을** 클릭합니다.

그림 3-10 웹 보안 항목 구성



2) 같은 페이지의 **일반** 섹션에서 **웹 보안을** 활성화하고 **저장을** 클릭합니다.

그림 3-11 웹 보안 사용

파트 9

VPN 구성

챕터

7. 와이어가드 VPN 구성

8. 사용자 구성

1 VPN

1.1 개요

VPN(가상 사설망)은 인터넷과 같은 공용 WAN(광역 네트워크)을 통해 원격 컴퓨터 간에 안전하게 통신할 수 있는 수단을 제공합니다. 가상은 VPN 연결이 물리적 종단 간 연결이 아닌 논리적 종단 간 연결을 기반으로 함을 나타냅니다. 비공개는 사용자가 자신의 요구 사항에 따라 VPN 연결을 설정할 수 있으며 특정 사용자만 VPN 연결을 사용할 수 있음을 나타냅니다.

VPN의 핵심은 터널링 프로토콜을 통해 데이터 캡슐화, 데이터 전송 및 데이터 압축 해제 작업을 수행하는 터널 통신을 실현하는 것입니다. 일반적인 터널링 프로토콜은 레이어 2 터널링 프로토콜과 레이어 3 터널링 프로토콜입니다.

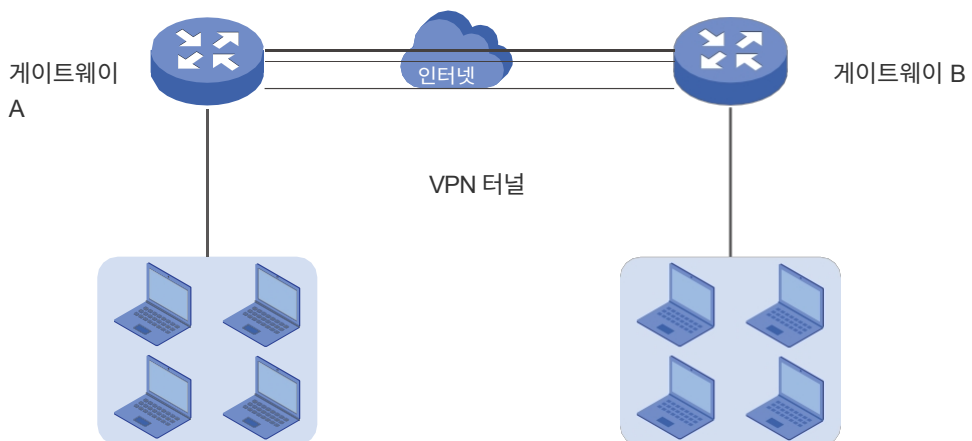
네트워크 토폴로지에 따라 두 가지 기본 애플리케이션 시나리오가 있습니다: LAN 간 VPN과 클라이언트 간 VPN입니다.

네트워크 토폴로지에 따라 두 가지 기본 애플리케이션 시나리오가 있습니다: LAN-to-LAN VPN과 클라이언트-to-LAN VPN입니다.

- LAN-to-LAN VPN

이 시나리오에서는 서로 다른 사설 네트워크가 인터넷을 통해 서로 연결됩니다. 예를 들어, 한 회사의 지사와 본사의 사설 네트워크는 서로 다른 곳에 위치해 있습니다. LAN-to-LAN VPN은 이러한 사설 네트워크의 호스트가 서로 통신하는 데 필요한 수요를 충족할 수 있습니다. 다음 그림은 이 시나리오의 일반적인 네트워크 토폴로지를 보여줍니다.

그림 1-1 LAN-to-LAN VPN

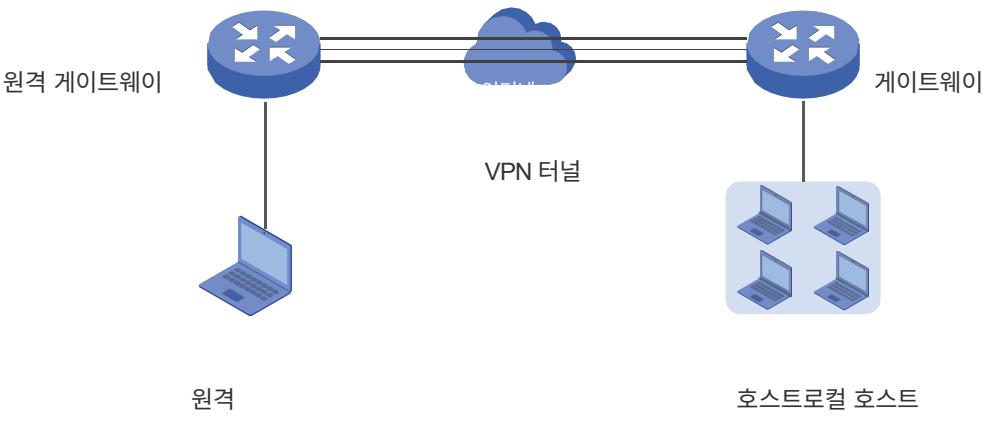


지사본사

■ 클라이언트-랜 간 VPN

이 시나리오에서는 원격 호스트에 로컬 호스트에 대한 보안 액세스가 제공됩니다. 예를 들어, 출장 중인 직원은 회사의 사설 네트워크에 안전하게 접속할 수 있습니다. 클라이언트-랜 간 VPN은 이러한 요구를 충족할 수 있습니다. 다음 그림은 이 시나리오의 일반적인 네트워크 토폴로지를 보여줍니다.

그림 1-2 클라이언트-랜 간 VPN



1.2 지원되는 기능

이 라우터는 IPSec, L2TP, PPTP 및 OpenVPN을 지원합니다.

IPsec

IPsec(IP 보안)은 IP 계층에서 데이터 기밀성, 데이터 무결성 및 데이터 출처 인증과 같은 보안 서비스를 제공할 수 있습니다. IPsec은 IKEv1(인터넷 키 교환 버전 1) 및 IKEv2(인터넷 키 교환 버전 2)를 사용하여 사용자가 지정한 정책에 따라 프로토콜 및 알고리즘의 협상을 처리하고 IPsec에서 사용할 암호화 및 인증키를 생성합니다. IKEv1/IKEv2 협상에는 IKEv1/IKEv2 1단계와 2단계의 두 가지 단계가 포함됩니다. IPsec의 기본 개념은 다음과 같습니다:

■ 제안서

제안은 IPsec IKEv1 협상에서 적용하기 위해 수동으로 구성한 보안 제품군입니다. 구체적으로 말하면, IKEv1 1단계에 적용되는 해시 알고리즘, 대칭 암호화 알고리즘, 비대칭 암호화 알고리즘과 2단계에 적용되는 보안 프로토콜, 해시 알고리즘, 대칭 암호화 알고리즘을 말합니다.

■ 협상 모드

IKEv1 1단계 협상에 대해 구성된 협상 모드에 따라 협상 과정에서 VPN 라우터가 수행하는 역할이 결정됩니다. 협상 모드를 응답자 모드 또는 개시자 모드로 지정할 수 있습니다.

응답자 모드: 응답자 모드에서 VPN 라우터는 IKEv1 협상 요청에 응답하고 VPN 서버 또는 응답자 역할을 합니다.

초기자 모드: 초기자 모드에서 VPN 라우터는 IKEv1 협상 요청을 전송하고 VPN 클라이언트 또는 초기자 역할을 합니다.

■ 교환 모드

교환 모드는 IKEv1 1단계에서 VPN 라우터가 협상하는 방식을 결정합니다. 교환 모드를 기본 모드 또는 공격 모드로 지정할 수 있습니다.

메인 모드: 기본 모드에서는 인증을 위한 식별 정보가 암호화되어 보안이 강화됩니다.

공격적 모드: 공격적 모드에서는 교환되는 패킷이 줄어들어 속도가 향상됩니다.

■ 인증 ID 유형

인증 ID 유형은 IKEv1 1단계에서 적용되는 인증 식별자의 유형을 결정합니다. 여기에는 로컬 ID 유형과 원격 ID 유형이 포함됩니다. 로컬 ID는 상대방에게 전송되는 인증 식별자를 나타내며, 원격 ID는 상대방이 예상하는 인증 식별자를 나타냅니다. 인증 ID 유형은 IP 주소 또는 이름으로 지정할 수 있습니다.

IP 주소: 라우터는 인증에 IP 주소를 사용합니다.

이름: 라우터는 인증에 FQDN(정규화된 도메인 이름)을 사용합니다.

■ 캡슐화 모드

캡슐화 모드는 VPN 터널에서 전송되는 패킷이 캡슐화되는 방식을 결정합니다. 캡슐화 모드로 터널 모드 또는 전송 모드를 선택할 수 있습니다. 대부분의 사용자에게는 터널 모드를 사용하는 것이 좋습니다.

■ PFS

PFS(완전 전달 비밀)는 IKEv1 2단계에서 생성된 키가 IKEv1 1단계에서 생성된 키와 관련이 있는지 여부를 결정합니다. PFS를 none, dh1, dh2 또는 dh5로 지정할 수 있습니다. 없음은 PFS가 구성되지 않았음을 나타내며 IKEv1 2단계에서 생성된 키가 IKEv1 1단계의 키와 관련이 있는 반면, dh1, dh2 또는 dh5는 서로 다른 키 교환 그룹을 의미하므로 IKEv1 2단계에서 생성된 키가 IKEv1 1단계의 키와 관련이 없는 것입니다.

GRE

GRE VPN은 일부 네트워크 계층 프로토콜의 데이터 패킷을 캡슐화하여 다른 네트워크 프로토콜로 전송할 수 있도록 합니다. 하지만 GRE는 패킷을 암호화할 수 없기 때문에 보통 IPsec과 함께 사용됩니다.

L2TP

L2TP(계층 2 터널링 프로토콜)는 전화 접속 사용자가 VPN 서버에 가상 PPP(지점 간 프로토콜)를 연결할 수 있는 방법을 제공합니다. 기밀성이 부족하기 때문에

프로토콜에 내재되어 있으며, 종종 IPsec과 함께 구현됩니다. L2TP의 기본 개념은 다음과 같습니다:

- IPsec 암호화

IPsec 암호화는 터널의 트래픽이 IPsec으로 암호화되는지 여부를 결정합니다. IPsec 암호화로 암호화 또는 암호화 안 함을 선택할 수 있습니다. 암호화를 선택하면 미리 공유한 키를 입력해야 하며, 그러면 L2TP 트래픽이 기본 IPsec 구성으로 암호화됩니다. 암호화되지 않음을 선택하면 VPN 터널 트래픽이 암호화되지 않습니다.

- 인증

L2TP는 VPN 서버에서 인증을 위해 계정 이름과 비밀번호를 사용합니다. 합법적인 클라이언트만 서버와 터널을 설정할 수 있으므로 네트워크 보안이 강화됩니다.

PPTP

PPTP(지점 간 터널링 프로토콜)는 TCP/IP 기반 데이터 네트워크에서 VPN을 생성하여 원격 클라이언트에서 프라이빗 기업 서버로 데이터를 안전하게 전송할 수 있는 네트워크 프로토콜입니다. PPTP는 인터넷과 같은 공용 네트워크를 통해 온디맨드, 다중 프로토콜, 가상 사설망을 지원합니다. PPTP의 기본 개념은 다음과 같습니다:

- MPPE 암호화

MPPE(Microsoft 지점 간 암호화) 체계는 RFC 3078에 정의된 암호화된 형식으로 PPP 패킷을 표현하는 수단입니다. MPPE 암호화로 암호화 또는 비암호화를 선택할 수 있습니다. 암호화를 선택하면, 데이터 기밀성을 보장하기 위해 VPN 터널 트래픽이 RSA RC4 알고리즘으로 암호화됩니다. 암호화되지 않음을 선택하면 VPN 터널 트래픽이 암호화되지 않습니다.

- 인증

PPTP는 VPN 서버에서 인증을 위해 계정 이름과 비밀번호를 사용합니다. 합법적인 클라이언트만 서버와 터널을 설정할 수 있으므로 네트워크 보안이 강화됩니다.

OpenVPN

OpenVPN은 트래픽 전송을 위한 UDP 및 TCP 암호화를 위해 OpenSSL(개방형 보안 소켓 계

층)을 사용합니다. OpenVPN은 클라이언트-서버 연결을 사용하여 인터넷을 통해 서버와 원격 클라이언트 간의 보안 통신을 제공합니다.

WireGuard VPN

Wireguard VPN은 안전하고 빠르며 현대적인 VPN 프로토콜입니다. UDP 프로토콜을 기반으로 하며 최신 암호화 알고리즘을 사용하여 업무 효율성을 향상시킵니다.

사용자 계정 목록

이 기능을 사용하면 원격 장치에서 VPN 서버에 연결하기 위한 VPN 연결 계정을 생성할 수 있습니다. 라우터가 L2TP/PPTP 클라이언트 역할을 하는 경우, 이 페이지에서 L2TP/ PPTP 사용자 계정을 구성할 필요가 없습니다.

2 IPSec VPN 구성

IPSec VPN 구성을 완료하려면 다음 단계를 따르세요:

1) IPSec 정책을 구성합니다.

2) IPSec VPN 터널의 연결을 확인합니다.

구성 가이드라인

- VPN 터널의 양쪽 끝에서 사전 공유 키, 제안서, 교환 모드, 캡슐화 모드가 동일해야 합니다.

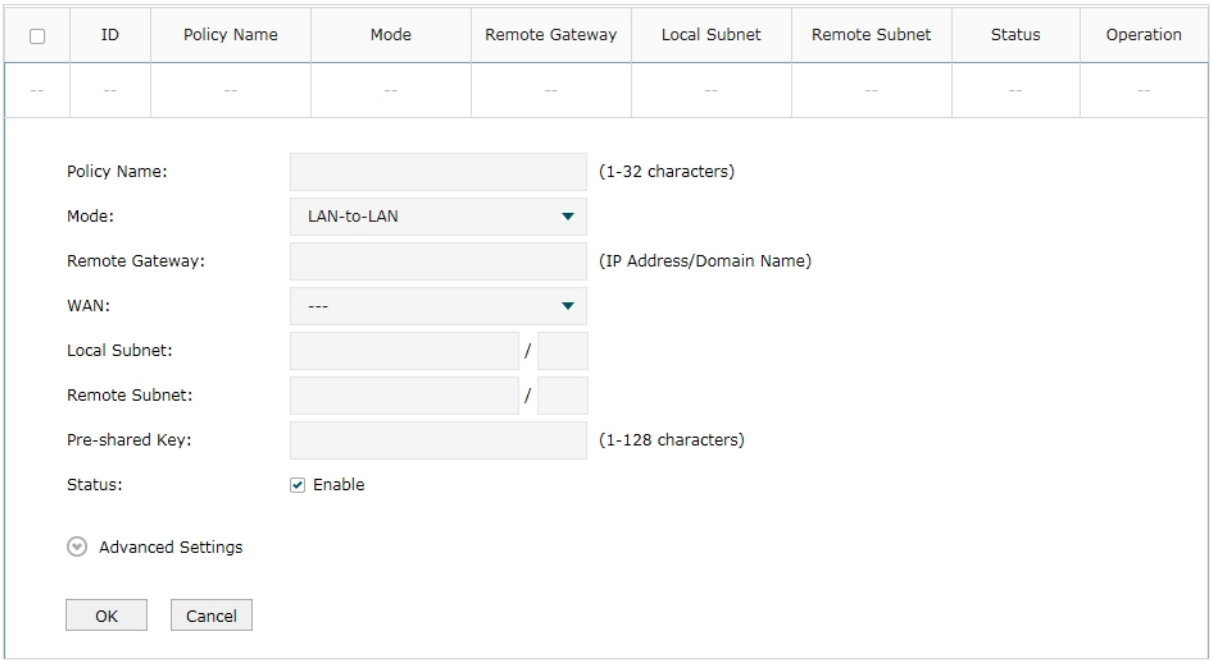
- VPN 터널의 양쪽 끝에서 원격 게이트웨이, 로컬/원격 서브넷, 로컬/원격 ID 유형이 일치해야 합니다.

2.1 IPSec 정책 구성

2.1.1 기본 매개변수 구성하기

VPN > IPSec > IPSec 정책 메뉴를 선택하고 추가를 클릭하여 다음 페이지를 로드합니다.

그림 2-1 기본 매개변수 구성하기

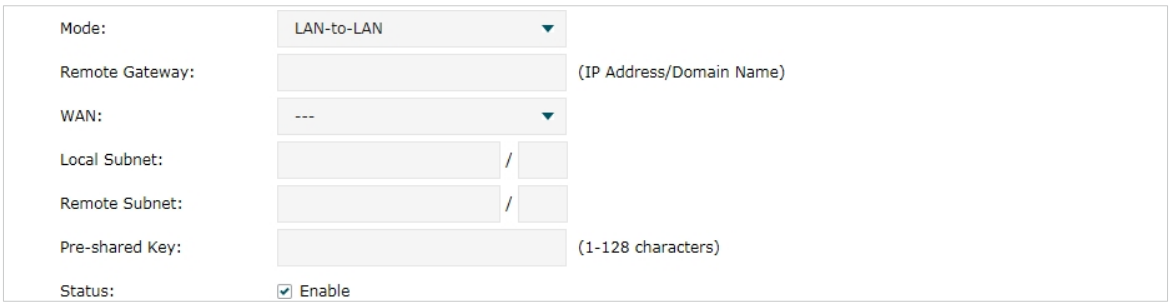


기본 매개변수를 구성하려면 다음 단계를 따르세요:

1) IPSec 정책의 이름을 지정합니다.

2) 네트워크 모드를 구성합니다. 네트워크가 다른 네트워크에 연결되어 있는 경우 **LAN-to-LAN을** 선택합니다. 호스트가 네트워크에 연결되어 있는 경우 클라이언트-대-랜을 선택합니다.

LAN-to-LAN 모드를 선택하면 다음 섹션이 표시됩니다.

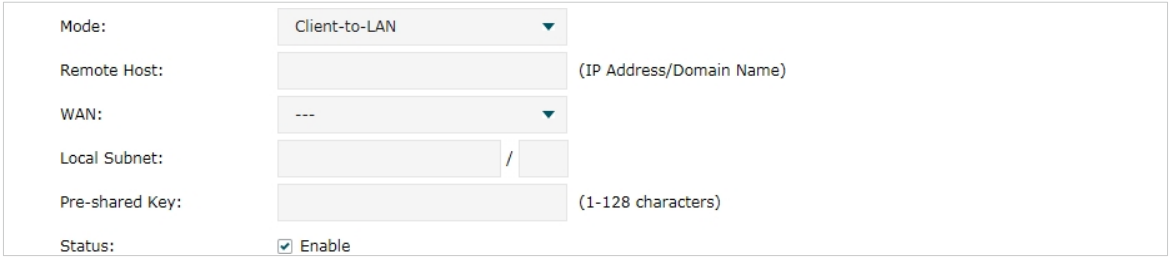


원격 게이트웨이	원격 게이트웨이로 IP 주소 또는 도메인 이름(1~255자)을 입력합니다. 0.0.0.0은 모든 IP 주소를 나타냅니다. 협상 모드가 응답자 모드로 설정된 경우에만 0.0.0.0을 입력할 수 있습니다.
WAN	IPSec 터널이 설정되는 WAN 포트를 지정합니다.
로컬 서브넷	로컬 네트워크를 지정합니다. (항상 VPN 터널의 로컬 측에 있는 LAN의 IP 주소 범위입니다). IP 주소와 서브넷 마스크로 구성됩니다.
원격 서브넷	원격 네트워크를 지정합니다. (항상 VPN 터널의 원격 피어에 있는 LAN의 IP 주소 범위입니다). IP 주소와 서브넷 마스크로 구성됩니다.
사전 공유 키	두 피어의 인증을 위한 고유한 사전 공유 키를 지정합니다. 상태
	IPSec 정책을 사용하도록 선택합니다.

참고:

VPN 모드로 LAN-to-LAN을 선택할 때 로컬 서브넷과 원격 서브넷이 동일한 네트워크 세그먼트에 있지 않아야 합니다.

클라이언트-랜 모드를 선택하면 다음 섹션이 나타납니다.



원격 호스트원격 호스트의 IP 주소를 입력합니다.	0.0.0.0은 모든 IP 주소를 나타냅니다. WAN IPSec 터널이 설정되는 WAN 포트를 지정합니다.
로컬 서브넷	로컬 네트워크를 지정합니다. (VPN 터널의 로컬 측에 있는 LAN의 IP 주소 범위입니다). IP 주소와 서브넷 마스크로 구성됩니다.
사전 공유 키	두 피어의 인증을 위해 미리 공유한 고유 키를 지정합니다.

상태	IPSec 정책을 사용하도록 선택합니다.

3) **확인을** 클릭합니다.

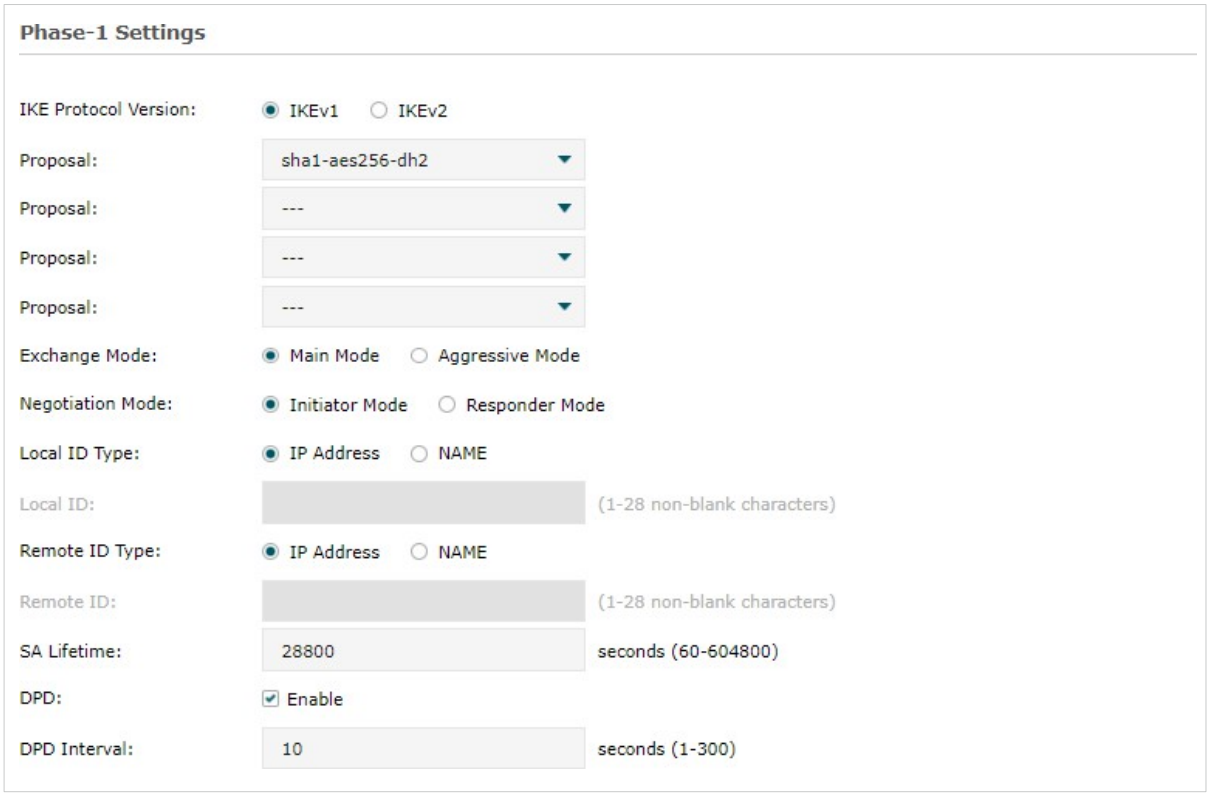
2.1.2 고급 매개변수 구성하기

고급 설정에는 IKEv1/IKEv2 1단계 설정 및 IKEv1/IKEv2 2단계 설정이 포함됩니다. 1단계는 통신의 양쪽을 인증하고 IKE SA를 설정하는 데 사용됩니다. 2단계는 키 및 보안 관련 매개변수에 대해 협상한 후 IPSec SA를 설정하는 데 사용됩니다. 기본 고급 설정을 유지하는 것이 좋습니다. 실제 필요에 따라 구성을 완료할 수 있습니다.

■ IKE 1단계 매개변수 구성

VPN > IPSec > IPSec 정책 메뉴를 선택하고 **고급 설정을** 클릭하면 다음 페이지가 로드됩니다.

그림 2-2 IKE 1단계 매개변수 구성하기



1단계 설정 섹션에서 IKE 1단계 매개변수를 구성하고 **확인을** 클릭합니다.

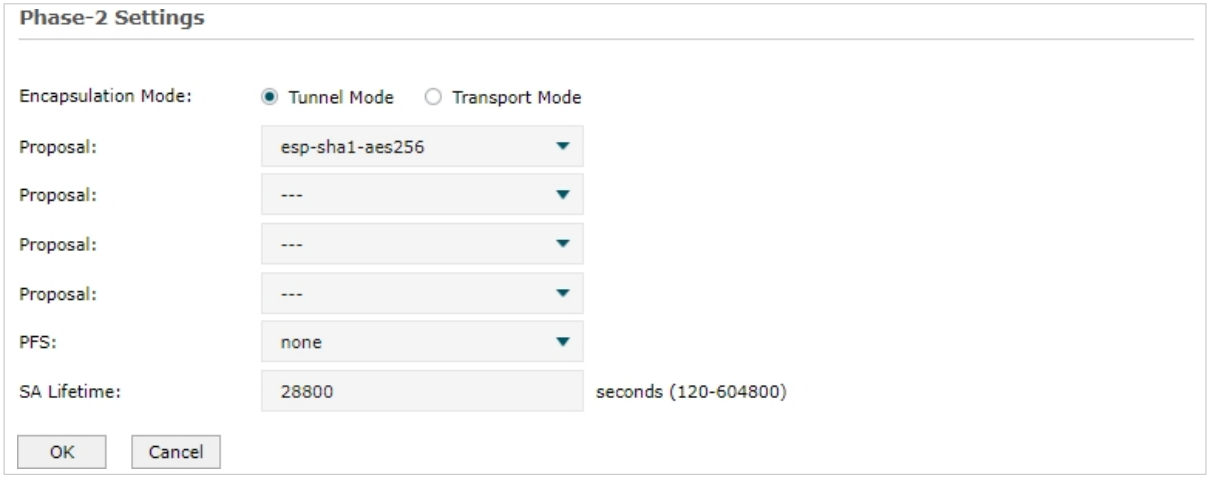
제안	IKE 협상 1단계에 대한 제안을 선택하여 암호화 알고리즘, 인증 알고리즘 및 DH 그룹을 지정합니다. 최대 4개의 제안을 선택할 수 있습니다.

교환 모드	IKE 교환 모드를 기본 모드 또는 공격 모드로 지정합니다. 기본값은 기본 모드입니다. **기본 모드:** 주 모드는 신원 보호 기능을 제공하고 더 많은 정보를 교환하며, 신원 보호에 대한 요구 사항이 더 높은 시나리오에 적용됩니다. **적극적 모드:** 공격적 모드는 더 빠른 연결을 설정하지만 보안은 더 낮으며, 신원 보호에 대한 요구 사항이 낮은 시나리오에 적용됩니다.
협상 모드	IKE 협상 모드를 개시자 모드 또는 응답자 모드로 지정합니다. **초기자 모드**: 로컬 장치가 피어에 대한 연결을 시작합니다. **초기자 모드**: 로컬 장치가 피어에 대한 연결을 시작합니다.
로컬 ID 유형	IKE 협상을 위한 로컬 ID 유형을 지정합니다. **IP 주소**: IKE 협상에서 IP 주소를 ID로 사용합니다. 기본 유형입니다. **이름**: 이름을 IKE 협상에서 ID로 사용합니다. FQDN(정규화된 도메인 이름)을 나타냅니다.
로컬 ID	로컬 ID 유형이 이름으로 구성된 경우, 로컬 장치의 이름을 IKE 협상에서 ID로 입력합니다.
원격 ID 유형	IKE 협상을 위한 원격 ID 유형을 지정합니다. **IP 주소**: IKE 협상에서 IP 주소를 ID로 사용합니다. 기본 유형입니다. **이름**: 이름을 IKE 협상에서 ID로 사용합니다. FQDN(정규화된 도메인 이름)을 나타냅니다.
원격 ID원격 ID 유형이 이름으로 구성된 경우	원격 피어의 이름을 IKE 협상에서 ID로 입력합니다.
SA 수명IKE 협상에서 ISAKMP SA(보안 협회) 수명을 지정합니다.	SA 수명이 만료되면 관련 ISAKMP SA가 삭제됩니다.
DPD	이 확인란을 선택하여 DPD(데드 피어 감지) 기능을 사용하거나 사용하지 않도록 설정합니다. 이 기능을 사용하도록 설정하면 IKE 엔드포인트가 피어에 DPD 요청을 전송하여 IKE 피어가 살아 있는지 검사할 수 있습니다.
DPD 간격	DPD가 트리거되는 경우 DPD 요청을 보내는 간격을 지정합니다. 이 간격 동안 IKE 엔드포인트가 피어로부터 응답을 받으면 피어가 살아 있는 것으로 간주합니다. 이 간격 동안 IKE 엔드포인트가 응답을 받지 못하면 피어가 죽은 것으로 간주하고 SA를 삭제합니다.

■ IKE 2단계 매개변수 구성

VPN > IPSec > IPSec 정책 메뉴를 선택하고 **고급 설정을** 클릭하면 다음 페이지가 로드됩니다.

그림 2-3 IKE 2단계 매개변수 구성하기



2단계 설정 섹션에서 IKE 2단계 매개변수를 구성하고 **확인을** 클릭합니다.

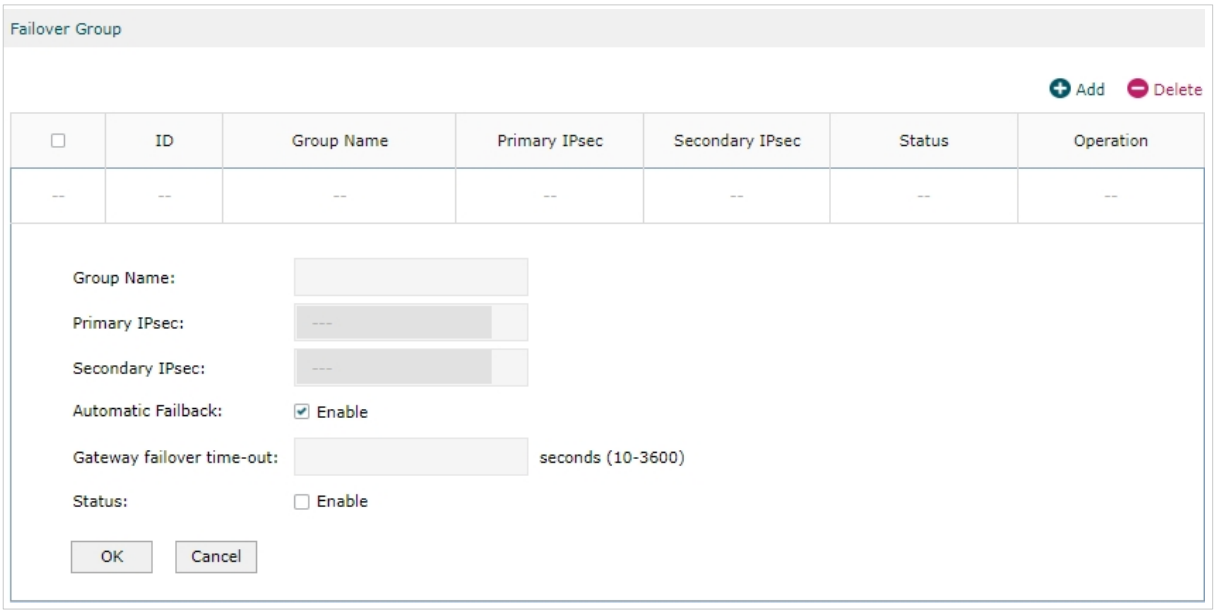
캡슐화 모드	캡슐화 모드를 터널 모드 또는 전송 모드로 지정합니다. 터널의 양쪽 끝이 호스트인 경우 두 모드 중 하나를 선택할 수 있습니다. 터널의 엔드포인트 중 하나 이상이 보안 게이트웨이인 경우 안전을 위해 터널 모드를 사용하는 것이 좋습니다.
제안	암호화 알고리즘, 인증 알고리즘 및 프로토콜을 지정하려면 IKE 협상 2단계에 대한 제안을 선택합니다. 최대 4개의 제안을 선택할 수 있습니다.
PFS	DH 그룹을 선택하여 IKE 모드에 PFS(Perfect Forward Security)를 사용하도록 설정하면 2단계에서 생성된 키가 1단계의 키와 무관하게 되어 네트워크 보안이 강화됩니다. 없음을 선택하면 PFS가 비활성화되고 1단계의 키를 기반으로 2단계의 키가 생성됩니다.
SA 수명	IKE 협상에서 IPSec SA(보안 협회) 수명을 지정합니다. SA 수명이 만료되면 관련 IPSec SA가 삭제됩니다.

2.1.3 장애 조치 그룹 구성

장애 조치 그룹에 두 개의 IPsec 연결을 사용할 수 있습니다. 기본 연결이 실패하면 그룹의 보조 연결이 자동으로 이어받습니다.

VPN > IPSec > IPSec 정책 메뉴를 선택하고, **IPsec 정책 목록** 섹션에서 여러 연결을 추가한 다음, **장애 조치 그룹** 섹션에서 **추가를** 클릭하여 다음 페이지를 로드합니다.

그림 2-4 장애 조치 그룹 구성하기



다음 단계에 따라 매개변수를 구성한 다음 **확인을** 클릭합니다:

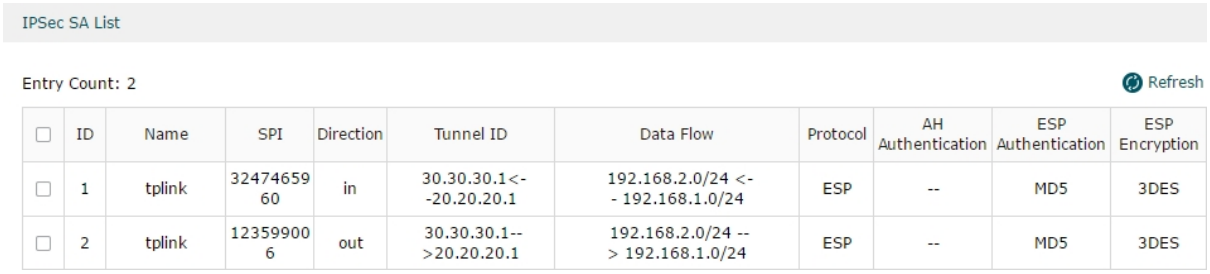
그룹 이름:	그룹을 식별할 수 있는 이름을 입력합니다.
기본 IPsec	IP초 연결을 기본 IPsec 연결로 선택합니다.
보조 IPsec	기본 IPsec 연결로 IP sec 연결을 선택합니다.
자동 페일백	이 기능을 활성화하면 기본 IPsec 연결이 복원될 때 재사용됩니다,
게이트웨이 장애 조치 시간 초과:	라우터가 기본 IPSec 연결 상태를 쿼리하기 위해 요청을 보낼 시간 간격을 설정합니다.
상태:	그룹을 활성화하려면 확인란을 선택합니다.

참고: 두 개의 IPsec 연결은 동일한 원격 IP에 설정되며, 관련 매개변수는 동일해야 합니다.

2.2 IPSec VPN 터널의 연결성 확인

VPN > IPSec > IPSec SA 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 2-5 IPSec SA 목록


IPSec SA List

Entry Count: 2 Refresh

	ID	Name	SPI	Direction	Tunnel ID	Data Flow	Protocol	AH Authentication	ESP Authentication	ESP Encryption
☐	1	tplink	3247465960	in	30.30.30.1<--20.20.20.1	192.168.2.0/24 <--192.168.1.0/24	ESP	--	MD5	3DES
☐	2	tplink	123599006	out	30.30.30.1-->20.20.20.1	192.168.2.0/24 -->192.168.1.0/24	ESP	--	MD5	3DES

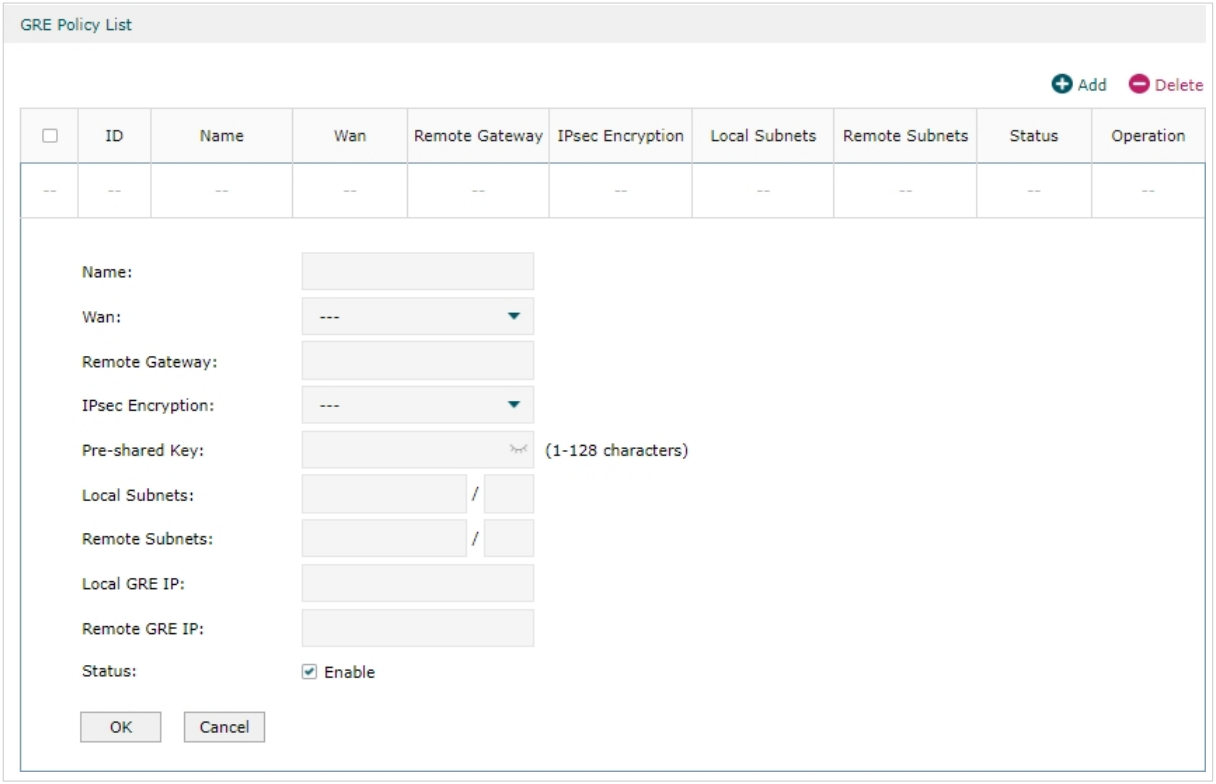
IPSec SA 목록에는 설정된 IPSec VPN 터널의 정보가 표시됩니다.

이름	SA와 연결된 IPSec 정책의 이름을 표시합니다.
SPI	나가는 SPI 및 들어오는 SPI를 포함하여 SA의 SPI(보안 매개변수 인덱스)를 표시합니다. 각 SA의 SPI는 고유합니다.
방향	SA의 방향(인: 수신/아웃: 발신)을 표시합니다. 터널 ID 로컬
및 원격 피어의 IP 주소를 표시합니다.	
데이터 흐름	SA가 적용되는 로컬 서브넷 및 원격 서브넷/호스트를 표시합니다. 프로토콜
	SA에서 사용하는 인증 프로토콜 및 암호화 프로토콜을 표시합니다.
AH 인증	SA에서 사용하는 AH 인증 알고리즘을 표시합니다.
ESP 인증	SA에서 사용하는 ESP 인증 알고리즘을 표시합니다.
ESP 암호화	SA에서 사용하는 ESP 암호화 알고리즘을 표시합니다.

3 GRE VPN 구성

GRE VPN 구성을 완료하려면, IPsec VPN을 구성했는지 확인하세요. **VPN > GRE** 메뉴를 선택하여 다음 페이지를 로드합니다. 추가를 클릭하여 GRE 정책을 추가합니다.

그림 3-1 GRE 정책 구성



이름	GRE VPN을 식별할 이름을 입력하세요.
WAN	GRE 터널이 설정되는 WAN 포트를 지정합니다.
원격 게이트웨이	원격 게이트웨이로 IP 주소를 입력합니다.
IPsec 암호화	터널에 암호화를 사용할지 여부를 지정합니다. 활성화하면 GRE 터널이 IPsec(GRE over IPsec)으로 암호화됩니다.
미리 공유한 키	IPsec 암호화가 암호화됨으로 구성된 경우, IKE 인증을 위한 미리 공유한 키를 지정합니다.
로컬 서브넷	로컬 네트워크를 지정합니다. 항상 VPN 터널의 로컬 측에 있는 LAN의 IP 주소 범위입니다. IP 주소와 서브넷 마스크로 구성됩니다. VPN 터널이 설정되면 피어는 로컬 서브넷에 액세

스할 수 있습니다.

원격 서브넷 원격 네트워크를 지정합니다. 항상 VPN 터널의 원격 피어에 있는 LAN의 IP 주소 범위입니다. IP 주소와 서브넷 마스크로 구성됩니다. 원격 서브넷에 대한 트래픽만 VPN 터널을 통해 전달됩니다.

로컬 GRE IP	GRE VPN의 로컬 가상 IP 주소를 지정합니다. 이 IP는 원격 게이트웨이 IP와 동일해서는 안 되며, 로컬 서브넷 또는 원격 서브넷에 있어서는 안 됩니다.
원격 GRE	IP그리 VPN의 원격 가상 IP 주소를 지정합니다. 이 IP는 원격 게이트웨이 IP와 동일해서는 안 되며, 로컬 서브넷 또는 원격 서브넷에 있어서는 안 됩니다.
상태	확인란을 선택하면 GRE VPN이 활성화됩니다.

4 L2TP 구성

L2TP 구성을 완료하려면 다음 단계를 따르세요:

1) VPN IP 풀을 구성합니다.
2) L2TP를 전역으로 구성합니다.
3) L2TP 서버/클라이언트를 구성합니다.
4) (선택 사항) L2TP 사용자를 구성합니다.
5) L2TP VPN 터널의 연결을 확인합니다.

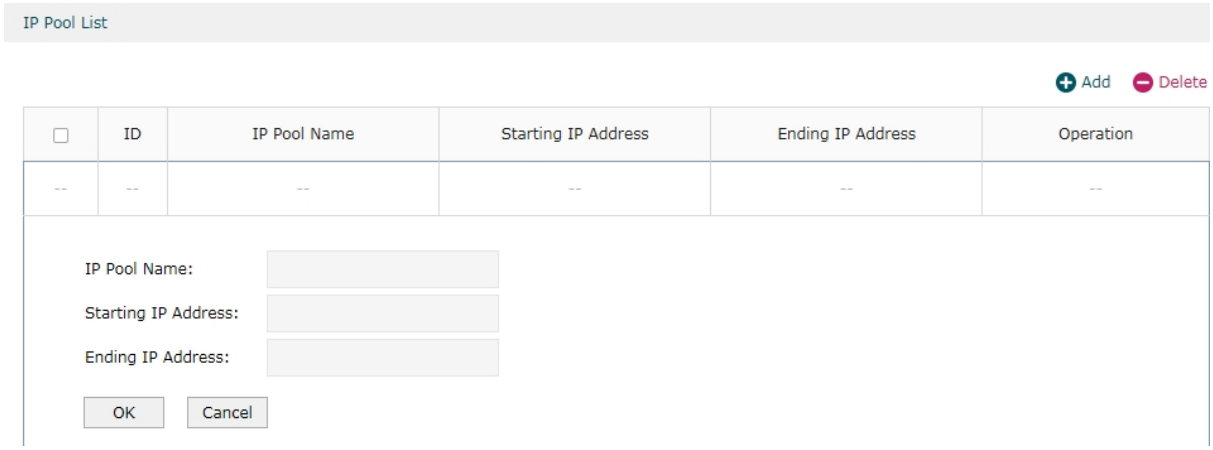
구성 가이드라인

- 네트워크 모드가 Client-to-LAN으로 구성되고 라우터가 L2TP 서버 역할을 하는 경우 라우터에서 L2TP 클라이언트를 구성할 필요가 없습니다.
- 네트워크 모드가 LAN-to-LAN으로 구성되고 라우터가 L2TP 클라이언트 게이트웨이 역할을 하는 경우 라우터에서 L2TP 사용자를 구성할 필요가 없습니다.

4.1 VPN IP 풀 구성

환경설정 > VPN IP 풀 > VPN IP 풀 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 4-1 VPN IP 풀 구성



VPN IP 풀을 구성하려면 다음 단계를 따르세요:

1) IP 풀의 이름을 지정합니다.

2) IP 풀의 시작 IP 주소와 종료 IP 주소를 지정합니다.

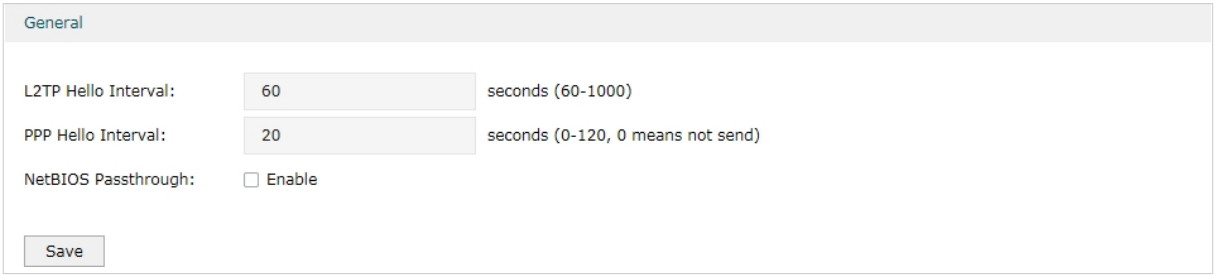
참고:

- 시작 IP 주소는 종료 IP 주소보다 크지 않아야 합니다.
- IP 풀의 범위는 겹칠 수 없습니다.

4.2 전역적으로 L2TP 구성하기

VPN > L2TP > 글로벌 구성 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 4-2 전역적으로 L2TP 구성하기



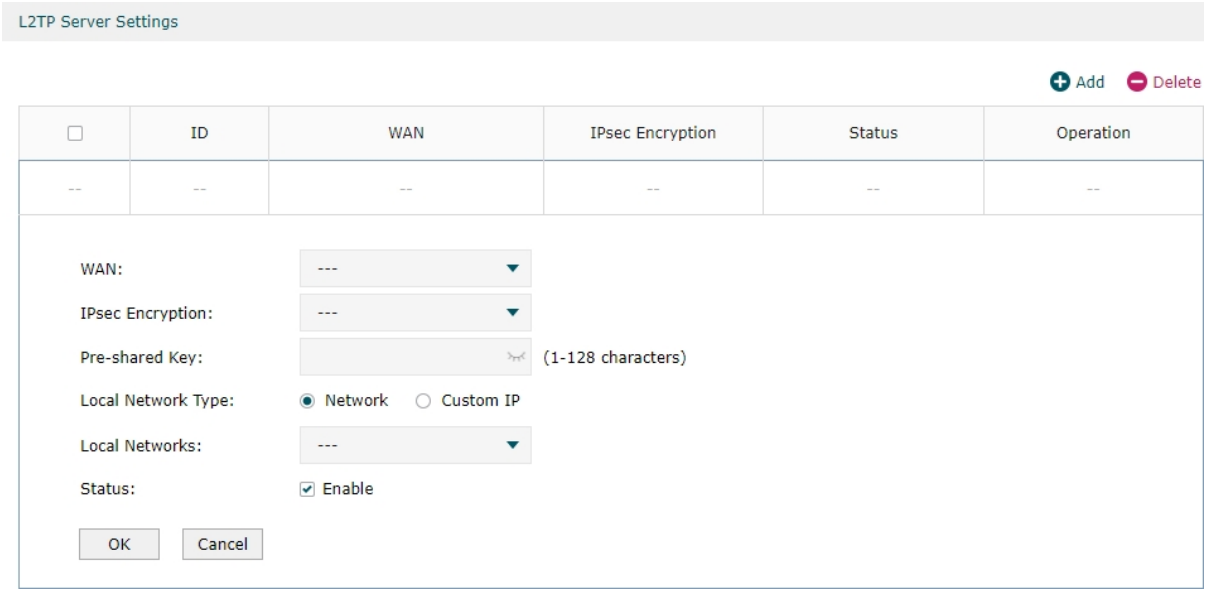
일반 섹션에서 L2TP 매개변수를 전역적으로 구성하고 **저장을** 클릭합니다.

L2TP 헬로우 간격	L2TP 피어 감지 패킷을 전송하는 시간 간격을 지정합니다.
PPP 헬로우 간격	PPP 피어 감지 패킷을 전송하는 시간 간격을 지정합니다.
NetBIOS 패스스루	NetBIOS 패킷이 VPN 터널을 통해 브로드캐스트되도록 허용하려면 NetBIOS 패스스루 기능을 사용하도록 설정합니다.

4.3 L2TP 서버 구성

VPN > L2TP > L2TP 서버 메뉴를 선택하고 추가를 클릭하면 다음 페이지가 로드됩니다.

그림 4-3 L2TP 서버 구성하기



L2TP 서버를 구성하려면 다음 단계를 따르세요:

1) L2TP 터널에 사용되는 WAN 포트를 지정합니다.

2) 터널에 대한 암호화 사용 여부를 지정합니다.

IPSec 암호화	터널에 암호화를 사용할지 여부를 지정합니다. 사용하도록 설정하면 L2TP 터널이 IPSec(L2TP over IPSec)에 의해 암호화됩니다. 자동을 선택하면 L2TP 서버가 클라이언트의 암호화 설정에 따라 터널을 암호화할지 여부를 결정합니다.

3) IKE 인증을 위한 사전 공유 키를 지정합니다.

4) 특정 로컬 네트워크 또는 IP 주소에 VPN 정책을 적용할지 여부를 지정합니다.

네트워크	VPN 터널의 로컬 네트워크를 지정합니다. VPN 정책은 선택한 로컬 네트워크에만 적용됩니다.
사용자 지정	VPN 터널의 IP 주소를 지정합니다. VPN 정책은 지정된 IP 주소에만 적용됩니다.

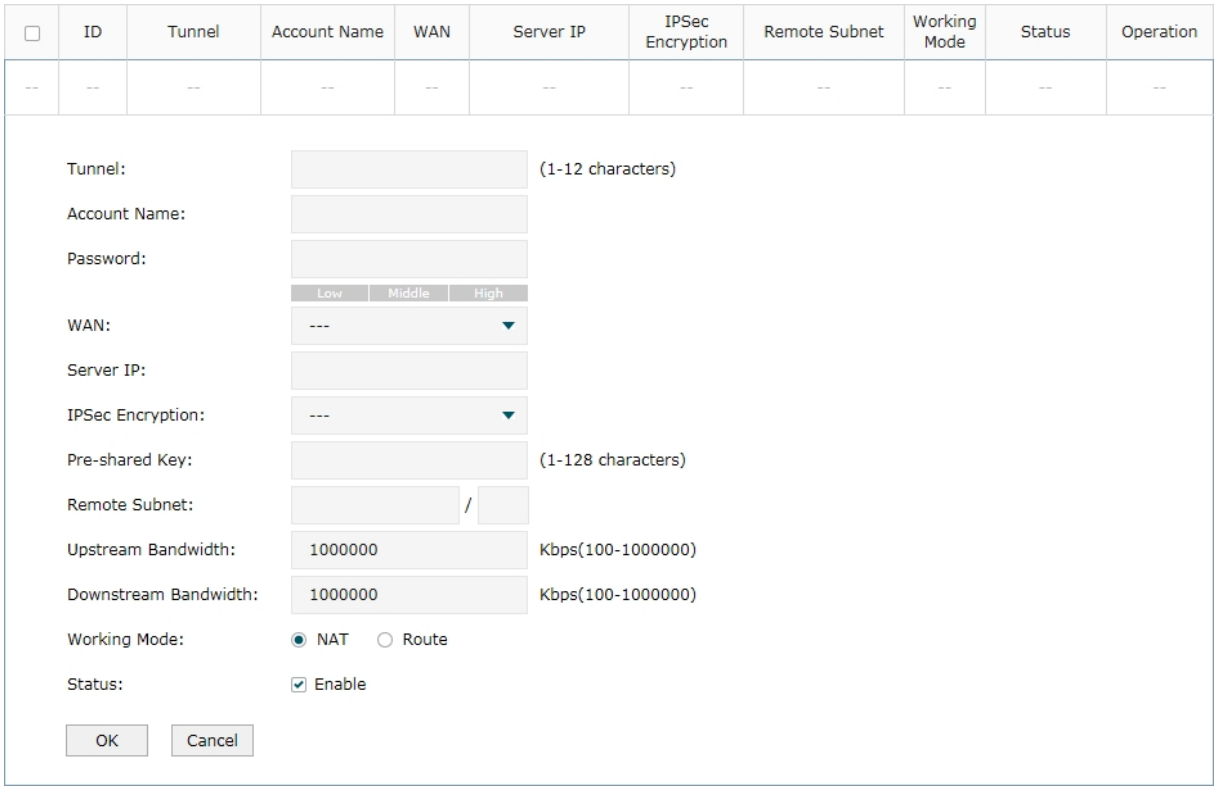
6) L2TP 터널을 활성화합니다.

7) **확인을** 클릭합니다.

4.4 L2TP 클라이언트 구성

VPN > L2TP > L2TP 클라이언트 메뉴를 선택한 후 추가를 클릭하면 다음 페이지가 로드됩니다.

그림 4-4 L2TP 클라이언트 구성하기



L2TP 클라이언트를 구성하려면 다음 단계를 따르세요:

1) L2TP 터널의 이름을 지정하고 실제 네트워크 환경에 따라 L2TP 클라이언트의 기타 관련 매

개변수를 구성합니다.

터널	L2TP 터널의 이름을 지정합니다.
계정 이름	L2TP 터널의 계정 이름을 지정합니다. 서버와 클라이언트에서 동일하게 구성해야 합니다.
비밀번호	L2TP 터널의 비밀번호를 지정합니다. 서버와 클라이언트에서 동일하게 구성해야 합니다.
WAN	L2TP 터널에 사용되는 WAN 포트를 지정합니다.
서버 IP	L2TP 서버의 IP 주소 또는 도메인 이름을 지정합니다.
IPSec 암호	화

터널에 암호화를	사용할지 여부를 지정합니다. 활성화하면 L2TP 터널이 IPSec(L2TP over IPSec)에 의해 암호화됩니다.
미리 공유한 키	IKE 인증을 위한 미리 공유한 키를 지정합니다.
원격 서브넷원격	네트워크를 지정합니다. (항상 VPN 터널의 원격 피어에 있는 LAN의 IP 주소 범위입니다). IP 주소와 서브넷 마스크의 조합입니다.

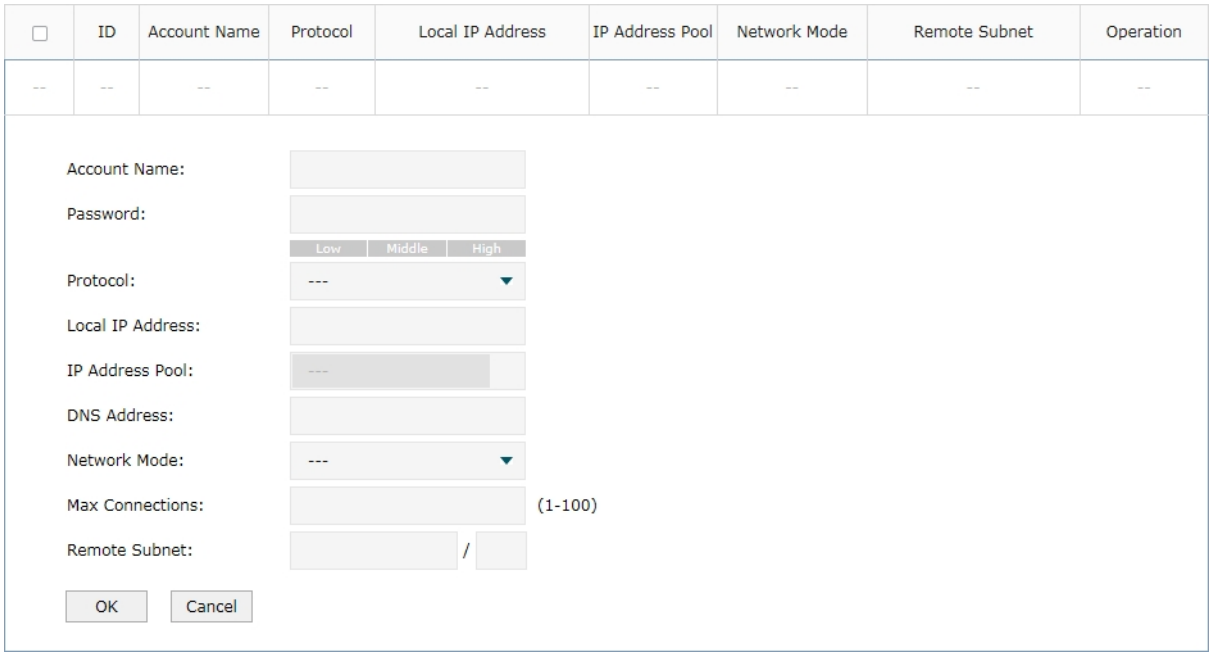
업스트림 대역폭	L2TP 터널의 업스트림 제한 속도를 Kbps 단위로 지정합니다.
다운스트림 대역폭	L2TP 터널의 다운스트림 제한 속도를 Kbps 단위로 지정합니다.
작업 모드	작업 모드를 NAT 또는 라우팅으로 지정합니다. **NAT**: NAT(네트워크 주소 변환) 모드를 사용하면 라우터가 L2TP 패킷을 전달할 때 L2TP 패킷의 소스 IP 주소를 WAN IP로 변환할 수 있습니다. **경로**: 라우트 모드에서는 라우터에서 라우팅 프로토콜을 통해 L2TP 패킷을 전달할 수 있습니다.
상태	L2TP 터널을 사용하려면 확인란을 선택합니다.

2) **확인을** 클릭합니다.

4.5 (선택 사항) L2TP 사용자 구성하기

VPN > 사용자 > 사용자 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 4-5 L2TP 사용자 구성하기



L2TP 사용자를 구성하려면 다음 단계를 따르세요:

1) L2TP 사용자의 계정 이름과 비밀번호를 지정합니다.

계정 이름	VPN 터널에 사용되는 계정 이름을 지정합니다. 이 매개변수는 L2TP 클라이언트의 매개변수와 동일해야 합니다.
비밀번호	사용자의 비밀번호를 지정합니다. 이 매개변수는 L2TP 클라이언트의 비밀번호와 동일해야 합니다.

2) 프로토콜을 L2TP로 지정하고 기타 관련 매개변수 cc를 구성합니다.

프로토콜	VPN 터널의 프로토콜을 지정합니다. 두 가지 유형이 있습니다: L2TP와 PPTP.
로컬 IP 주소	터널의 로컬 IP 주소를 지정합니다. 로컬 장치의 LAN IP를 입력할 수 있습니다.
IP 주소 풀	VPN 클라이언트에 IP 주소를 할당할 IP 주소 풀을 지정합니다. 여기서 참조하는 IP 풀은 **환경설정 > VPN IP 풀** 페이지에서 생성할 수 있습니다.
DNS 주소	VPN 클라이언트에 할당할 DNS 주소를 지정합니다(예: 8.8.8.8).
네트워크 모드	네트워크 모드를 지정합니다. 두 가지 모드가 있습니다: **클라이언트-랜** 간: L2TP/PPTP 클라이언트가 단일 호스트인 경우 이 옵션을 선택합니다. **LAN-to-LAN**: L2TP/PPTP 클라이언트가 VPN 게이트웨이인 경우 이 옵션을 선택합니다. 터널링 요청은 항상 장치에서 시작됩니다.
최대 연결 수	터널이 지원할 수 있는 최대 연결 수를 지정합니다.
원격 서브넷	원격 네트워크를 지정합니다. (L2TP/PPTP 터널의 원격 피어에 있는 LAN의 IP 주소 범위입니다). IP 주소와 서브넷 마스크의 조합입니다.

3) **확인을** 클릭합니다.

4.6 L2TP VPN 터널의 연결 확인

VPN > L2TP > 터널 목록 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 4-6 L2TP VPN 터널 목록

터널 목록에는 설정된 L2TP VPN 터널의 정보가 표시됩니다.

계정 이름	L2TP 터널의 계정 이름을 표시합니다. 모드 장치가 서버인지 클라이언트인지 표시합니다.
터널	라우터가 L2TP 클라이언트인 경우 터널의 이름을 표시합니다. 로컬 IP

	터널의 로컬 IP 주소를 표시합니다.
원격 IP	터널의 원격 실제 IP 주소를 표시합니다.

원격 로컬 IP	터널의 원격 로컬 IP 주소를 표시합니다.
DNS	터널의 DNS 주소를 표시합니다.

5 PPTP 구성

PPTP 구성을 완료하려면 다음 단계를 따르세요:

1) VPN IP 풀을 구성합니다.
2) PPTP를 전역적으로 구성합니다.
3) PPTP 서버/클라이언트를 구성합니다.
4) (선택 사항) PPTP 사용자를 구성합니다.
5) PPTP VPN 터널의 연결을 확인합니다.

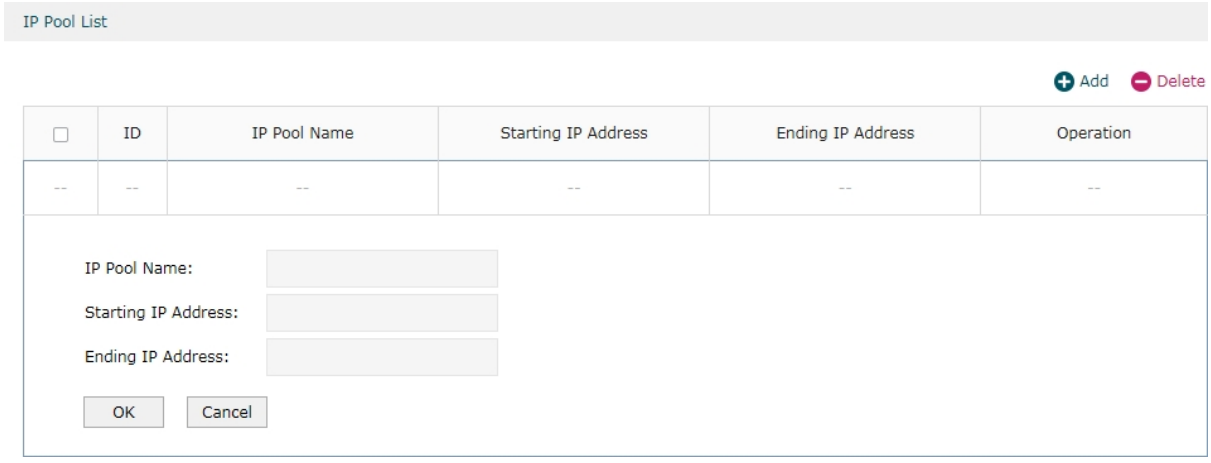
구성 가이드라인

- 네트워크 모드가 클라이언트-대-랜으로 구성되고 라우터가 PPTP 서버 역할을 하는 경우, 라우터에서 PPTP 클라이언트를 구성할 필요가 없습니다.
- 네트워크 모드가 LAN-to-LAN으로 구성되어 있고 라우터가 PPTP 클라이언트 게이트웨이 역할을 하는 경우, 라우터에서 PPTP 사용자를 구성할 필요가 없습니다.

5.1 VPN IP 풀 구성

환경설정 > VPN IP 풀 > VPN IP 풀 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 5-1 VPN IP 풀 구성



VPN IP 풀을 구성하려면 다음 단계를 따르세요:

1) IP 풀의 이름을 지정합니다.

2) IP 풀의 시작 IP 주소와 종료 IP 주소를 지정합니다.

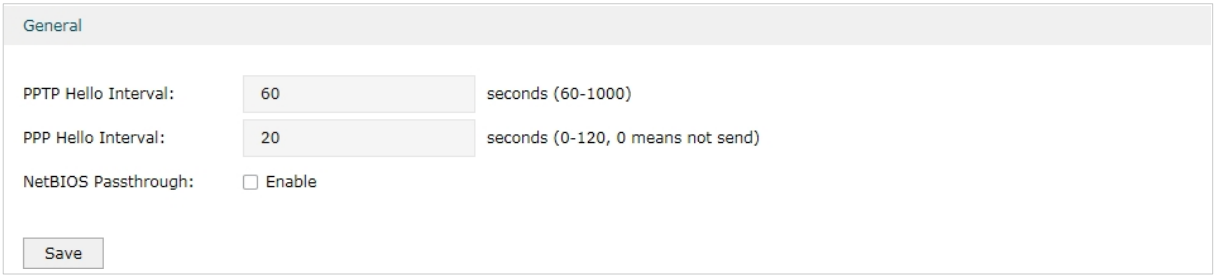
참고:

- 시작 IP 주소는 종료 IP 주소보다 크지 않아야 합니다.
- IP 풀의 범위는 겹칠 수 없습니다.

5.2 PPTP를 전역으로 구성하기

VPN > PPTP > 글로벌 구성 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 5-2 전역적으로 PPTP 구성하기



일반 섹션에서 PPTP 매개변수를 전역적으로 구성하고 **저장을** 클릭합니다.

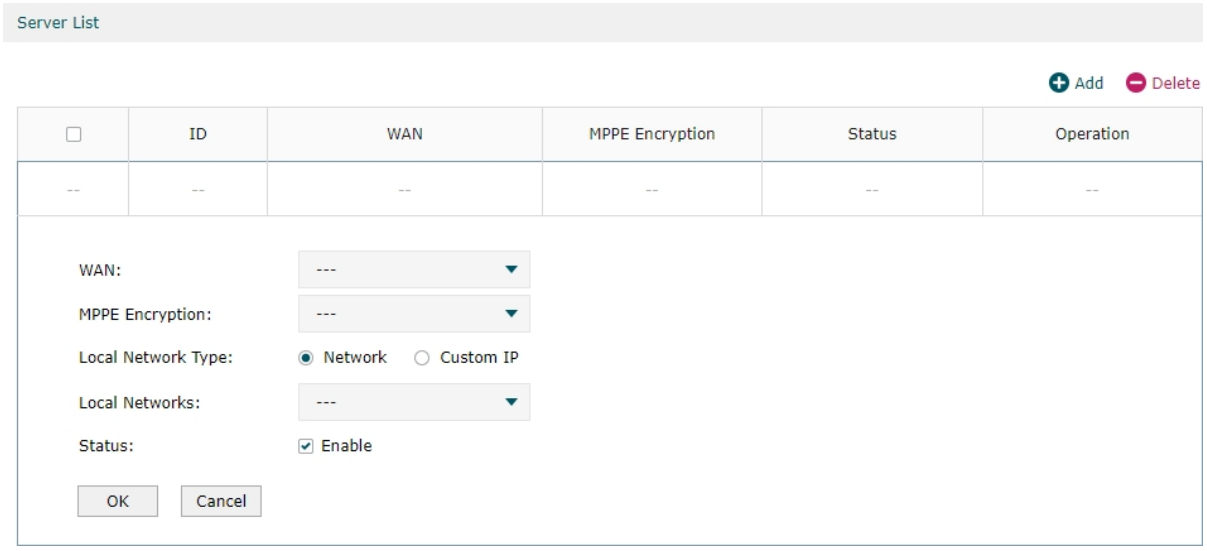
PPTP 헬로우 간격	PPTP 피어 감지 패킷을 전송하는 시간 간격을 지정합니다.
PPP 헬로우 간격	PPP 피어 감지 패킷을 전송하는 시간 간격을 지정합니다.

NetBIOS 패스스루	NetBIOS 패킷이 VPN 터널을 통해 브로드캐스트되도록 허용하려면 NetBIOS 패스스루 기능을 사용하도록 설정합니다.

5.3 PPTP 서버 구성

VPN > PPTP > PPTP 서버 메뉴를 선택하고 추가를 클릭하면 다음 페이지가 로드됩니다.

그림 5-3 PPTP 서버 구성하기



PPTP 서버를 구성하려면 다음 단계를 따르세요:

1) PPTP 터널에 사용되는 WAN 포트를 지정합니다.

2) PPTP 터널에 대해 MPPE 암호화를 사용할지 여부를 지정합니다.

3) 특정 로컬 네트워크 또는 IP 주소에 VPN 정책을 적용할지 여부를 지정합니다.

네트워크	VPN 터널의 로컬 네트워크를 지정합니다. VPN 정책은 선택한 로컬 네트워크에만 적용됩니다.
사용자 지정	VPN 터널의 IP 주소를 지정합니다. VPN 정책은 지정된 IP 주소에만 적용됩니다.

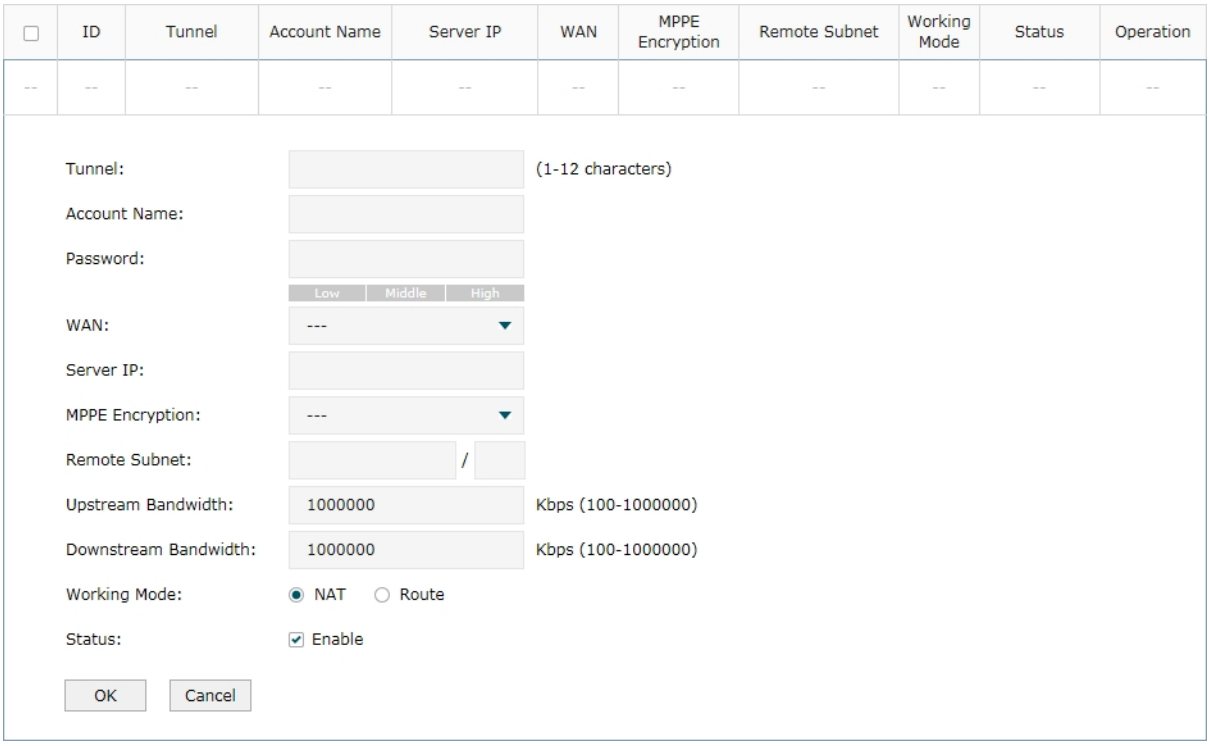
4) PPTP 터널을 활성화합니다.

5) **확인을** 클릭합니다.

5.4 PPTP 클라이언트 구성

VPN > PPTP > PPTP 클라이언트 메뉴를 선택하고 추가를 클릭하면 다음 페이지가 로드됩니다.

그림 5-4 PPTP 클라이언트 구성하기



PPTP 클라이언트를 구성하려면 다음 단계를 따르세요:

1) PPTP 터널의 이름을 지정하고 실제 네트워크 환경에 따라 PPTP 클라이언트의 기타 관련 매개변수를 구성합니다.

터널	PPTP 터널의 이름을 지정합니다.
계정 이름	PPTP 터널의 계정 이름을 지정합니다. 서버와 클라이언트에서 동일하게 구성해야 합니다.
비밀번호	PPTP 터널의 비밀번호를 지정합니다. 서버와 클라이언트에서 동일하게 설정해야 합니다.
WAN	PPTP 터널에 사용되는 WAN 포트를 지정합니다.
서버 IP	PPTP 서버의 IP 주소 또는 도메인 이름을 지정합니다.
MPPE 암호화	터널에 암호화를 사용할지 여부를 지정합니다. 활성화하면 PPTP 터널이 MPPE에 의해 암

호화됩니다.

원격 서브넷원격	네트워크를 지정합니다. (항상 VPN 터널의 원격 피어에 있는 LAN의 IP 주소 범위입니다). IP 주소와 서브넷 마스크의 조합입니다.
업스트림 대역폭	PPTP 터널의 업스트림 제한 속도를 Kbps 단위로 지정합니다.

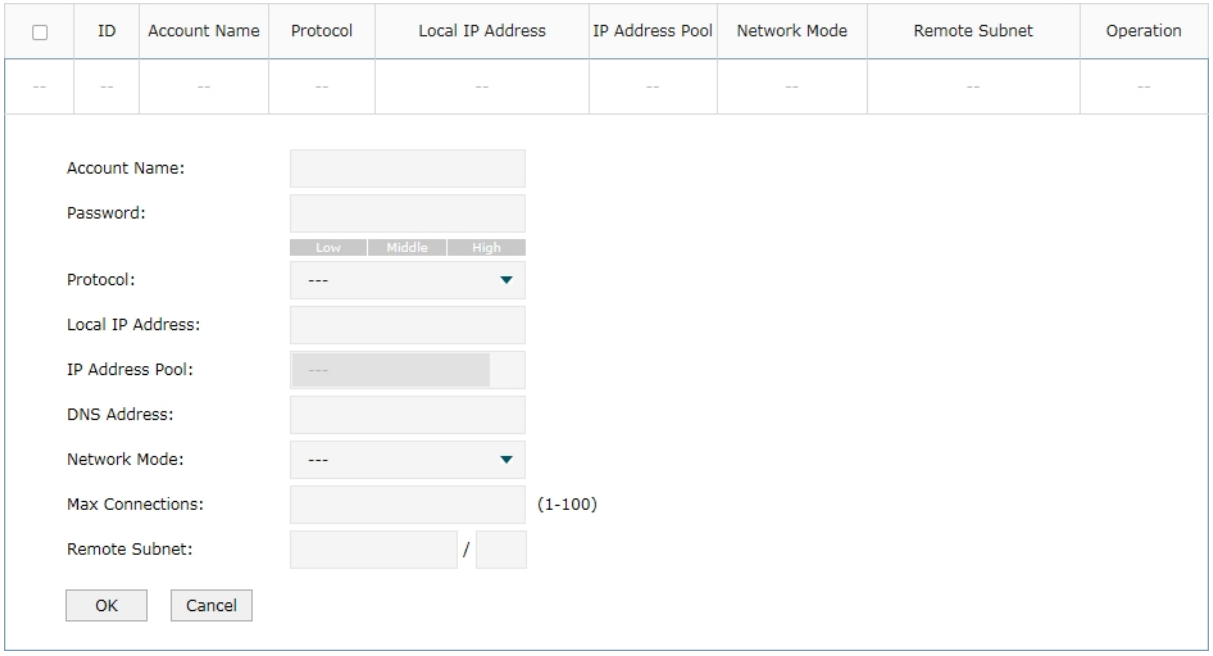
다운스트림 대역폭	PPTP 터널의 다운스트림 제한 속도를 Kbps 단위로 지정합니다.
작업 모드	작업 모드를 NAT 또는 라우팅으로 지정합니다. **NAT**: NAT(네트워크 주소 변환) 모드를 사용하면 라우터가 PPTP 패킷을 전달할 때 PPTP 패킷의 소스 IP 주소를 WAN IP로 변환할 수 있습니다. **경로**: 라우트 모드에서는 라우터에서 라우팅 프로토콜을 통해 PPTP 패킷을 전달할 수 있습니다.
상태	확인란을 선택하면 PPTP 터널이 활성화됩니다.

2) **확인을** 클릭합니다.

5.5 (선택 사항) PPTP 사용자 구성

VPN > 사용자 > 사용자 메뉴를 선택하고 추가를 클릭하면 다음 페이지가 로드됩니다.

그림 5-5 PPTP 사용자 구성하기



PPTP 사용자를 구성하려면 다음 단계를 따르세요:

1) PPTP 사용자의 계정 이름과 비밀번호를 지정합니다.

계정 이름	VPN 터널에 사용되는 계정 이름을 지정합니다. 이 매개변수는 PPTP 클라이언트의 매개변수와 동일해야 합니다.

비밀번호	사용자의 비밀번호를 지정합니다. 이 매개변수는 PPTP 클라이언트의 비밀번호와 동일해야 합니다.

2) 프로토콜을 PPTP로 지정하고 실제 네트워크 환경에 따라 기타 관련 매개변수를 구성합니다.

프로토콜	VPN 터널의 프로토콜을 지정합니다. 두 가지 유형이 있습니다: L2TP와 PPTP.
로컬 IP 주소	터널의 로컬 IP 주소를 지정합니다. 로컬 장치의 LAN IP를 입력할 수 있습니다.
IP 주소 풀	VPN 클라이언트에 IP 주소를 할당할 IP 주소 풀을 지정합니다. 여기서 참조하는 IP 풀은 **환경설정 > VPN IP 풀** 페이지에서 생성할 수 있습니다.
DNS 주소	VPN 클라이언트에 할당할 DNS 주소를 지정합니다(예: 8.8.8.8).
네트워크 모드	네트워크 모드를 지정합니다. 두 가지 모드가 있습니다: **클라이언트-랜 간**: PPTP/PPTP 클라이언트가 단일 호스트인 경우 이 옵션을 선택합니다. **LAN-to-LAN**: PPTP/PPTP 클라이언트가 VPN 게이트웨이인 경우 이 옵션을 선택합니다. 터널링 요청은 항상 장치에서 시작됩니다.
최대 연결 수	터널이 지원할 수 있는 최대 연결 수를 지정합니다.
원격 서브넷	원격 네트워크를 지정합니다. (PPTP/PPTP 터널의 원격 피어에 있는 LAN의 IP 주소 범위입니다). IP 주소와 서브넷 마스크의 조합입니다.

3) **확인을** 클릭합니다.

5.6 PPTP VPN 터널의 연결성 확인

VPN > PPTP > 터널 목록 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 5-6 PPTP VPN 터널 목록

터널 목록에는 설정된 PPTP VPN 터널의 정보가 표시됩니다.

계정	PPTP 터널의 계정 이름을 표시합니다.
모드	장치가 서버인지 클라이언트인지 표시합니다.
터널	라우터가 PPTP 클라이언트인 경우 터널의 이름을 표시합니다.
로컬 IP	

	터널의 로컬 IP 주소를 표시합니다.
원격 IP	터널의 원격 실제 IP 주소를 표시합니다.

원격 로컬 IP	터널의 원격 로컬 IP 주소를 표시합니다.
DNS	터널의 DNS 주소를 표시합니다.

6 운영 enVPN 구성

OpenVPN 구성을 완료하려면 다음 단계를 따르세요:

1) OpenVPN 서버/클라이언트를 구성합니다.

2) 터널 목록을 확인하여 OpenVPN 터널의 연결을 확인하세요.

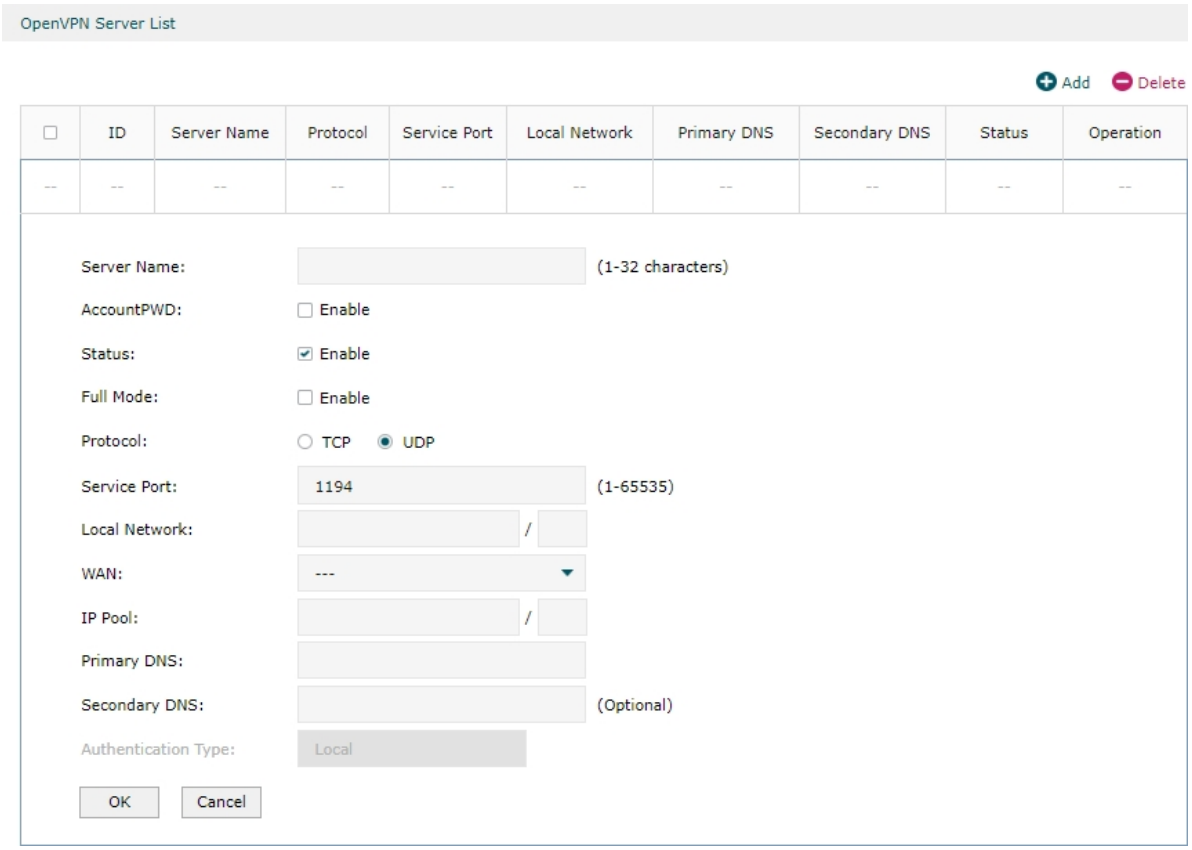
구성 가이드라인

- 라우터를 OpenVPN 서버로만 사용하는 경우, OpenVPN 클라이언트를 구성할 필요가 없습니다.

6.1 OpenVPN 서버 구성

VPN > OpenVPN > OpenVPN 서버 메뉴를 선택하고 **추가를** 클릭하여 다음 페이지를 로드하세요.

그림 6-1 OpenVPN 서버 구성하기



OpenVPN 서버의 이름을 지정하고 실제 네트워크 환경에 따라 기타 관련 파라미터를 구성한 후 **확인을** 클릭합니다.

서버 이름	VPN 서버를 식별할 이름을 입력합니다.
AccountPWD	활성화하면 OpenVPN은 사용자 이름/비밀번호를 사용하여 사용자를 인증합니다. 상
태	OpenVPN 서버를 활성화하려면 이 확인란을 선택합니다.
전체 모드	모든 클라이언트 트래픽이 터널을 통과하도록 허용하려면 이 옵션을 선택합니다.
프로토콜	OpenVPN 서버로 작동하는 게이트웨이의 통신 프로토콜을 선택합니다. 두 가지 통신 프로토콜을 사용할 수 있습니다: TCP와 UDP.
서비스 포트	VPN 장치가 연결되는 VPN 서비스 포트를 입력합니다. 기본 포트는 1194입니다.
로컬 네트워크	VPN 터널의 로컬 측 네트워크를 선택합니다. VPN 정책은 선택한 로컬 네트워크에만 적용됩니다.
WAN	VPN 터널이 설정될 WAN 포트를 선택합니다. 게이트웨이가 OpenVPN 서버로 작동하는 경우 각 WAN 포트는 하나의 OpenVPN 터널만 지원합니다.
IP 풀	IP 주소와 서브넷 마스크를 입력하여 VPN IP 풀의 범위를 결정합니다. 터널이 설정되면 VPN 서버가 원격 호스트에 IP 주소를 할당합니다. 로컬 피어 라우터에 있는 LAN의 IP 주소와 겹치지 않는 합리적인 IP 주소를 지정할 수 있습니다.
기본 DNS	클라이언트에 푸시되는 기본 DNS 서버를 지정합니다.
보조 DNS	클라이언트에 푸시되는 보조 DNS 서버를 지정합니다.
인증 유형	OpenVPN 서버에서 사용하는 인증 방법을 지정합니다. 로컬: 터널이 생성될 때 내장된 인증 서버를 사용하여 인증합니다. 추가 외부 서버가 없는 경우 로컬 인증을 선택할 수 있습니다. LDAP: 터널이 생성될 때 외부 LDAP 서버를 사용하여 인증합니다.

참고:

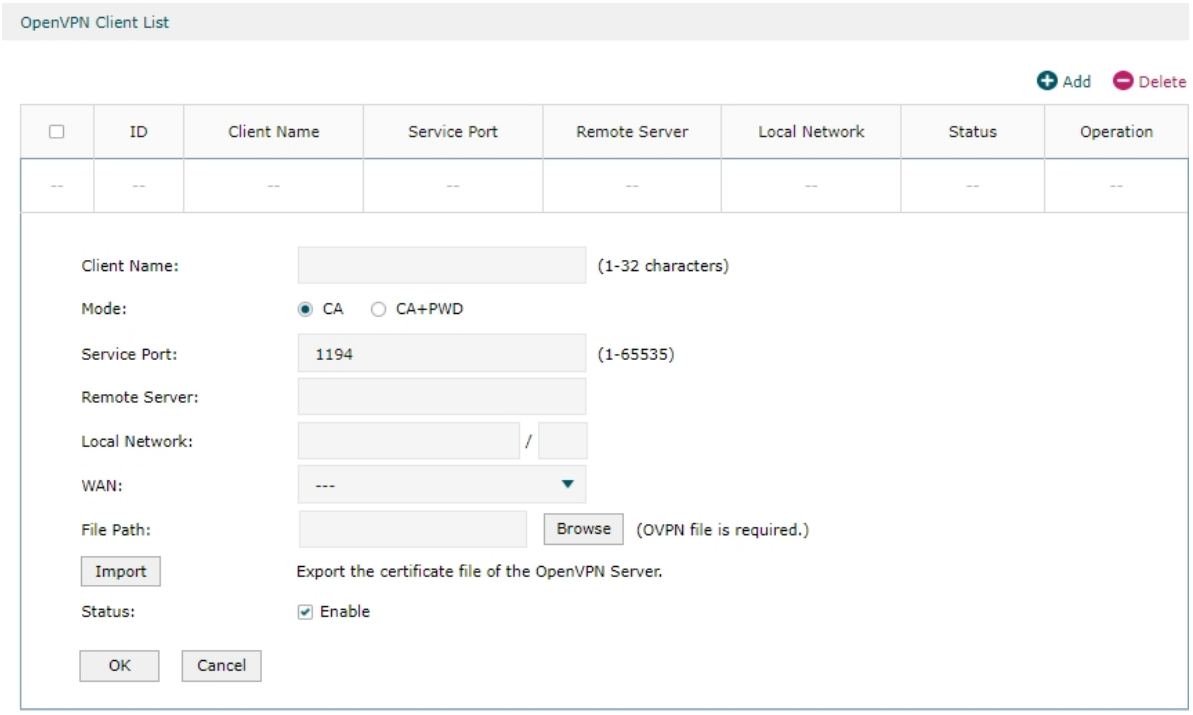
- 설정을 저장한 후, 원격 클라이언트에서 사용할 .ovpn으로 끝나는 OpenVPN 파일을 내보냅니다.

내보낸 OpenVPN 파일에는 인증서 및 구성 정보가 포함됩니다. 인증서를 내보내는 데 약 2분이 소요될 수 있습니다.

6.2 OpenVPN 클라이언트 구성

VPN > OpenVPN > OpenVPN 클라이언트 메뉴를 선택한 후 추가를 클릭하여 다음 페이지를 로드하세요. 라우터는 원격 서버와 VPN 터널을 설정하기 위해 OpenVPN 클라이언트 역할을 합니다.

그림 6-2 OpenVPN 클라이언트 구성하기



OpenVPN 클라이언트의 이름을 지정하고 실제 네트워크 환경에 따라 기타 관련 파라미터를 구성한 후 **확인을** 클릭합니다.

클라이언트 이름	OpenVPN 클라이언트의 이름을 지정합니다.
모드	클라이언트에서 사용할 인증 방법을 선택합니다. ca 모드에서는 인증서 파일만 필요합니다. ca+pwd 모드에서는 추가 사용자 이름과 비밀번호가 필요합니다. 사용자 이름 - 클라이언트 인증에 필요한 사용자 이름을 입력합니다. 비밀번호 - 클라이언트 인증에 필요한 비밀번호를 입력합니다.
서비스 포트	VPN 장치가 연결되는 VPN 서비스 포트를 입력합니다. 기본 포트는 1194입니다.
원격 서버	OpenVPN 서버의 IP 주소 또는 도메인 이름을 입력합니다.

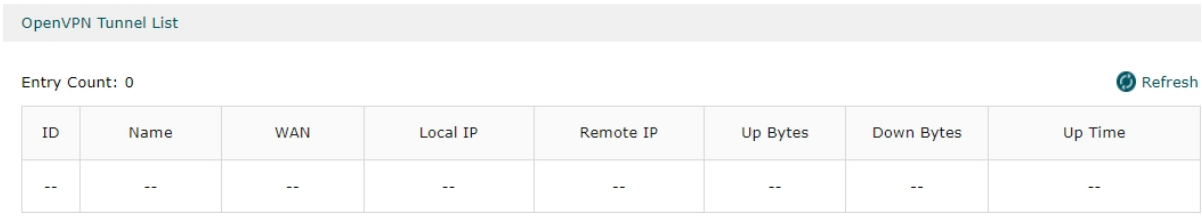
로컬 네트워크	VPN 터널의 로컬 측 네트워크를 선택합니다. VPN 정책은 선택한 로컬 네트워크에만 적용됩니다.
WAN	VPN 터널이 설정되는 WAN 포트를 선택합니다.

파일 경로	파일을 검색하여 OpenVPN 서버에서 생성한 .ovpn으로 끝나는 OpenVPN 파일을 찾습니다.
가져오기	이 버튼을 클릭하면 OpenVPN 서버에서 생성한 .ovpn으로 끝나는 OpenVPN 파일을 가져올 수 있습니다. 하나의 파일만 가져올 수 있습니다. 인증서 파일과 구성 파일이 OpenVPN 서버에 의해 단독으로 생성된 경우, 두 파일을 결합하여 전체 파일을 가져옵니다.
상태	이 확인란을 선택하면 OpenVPN 클라이언트가 활성화됩니다.

6.3 OpenVPN 터널 보기

VPN > OpenVPN > OpenVPN 터널 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 6-3 OpenVPN 터널 보기



최신 정보를 보려면 **새로** 고침을 클릭합니다.

이름	OpenVPN 서버/클라이언트의 계정 이름을 표시합니다.
WAN	VPN 터널이 설정되는 WAN 포트를 표시합니다. 로컬 IP 터널에 할
당된 가상 로컬 IP 주소를 표시합니다.	
원격 IP터널에 할당된 가상 로컬 IP 주소를 표시합니다.	업스트림 바이트 업스트
림 처리량을 표시합니다.	
다운 바이트	다운스트림 처리량을 표시합니다.
가동 시간	터널이 켜져 있는 시간을 표시합니다.

7 Wir eGuard VPN 구성

WireGuard VPN 구성을 완료하려면 다음 단계를 따르세요:

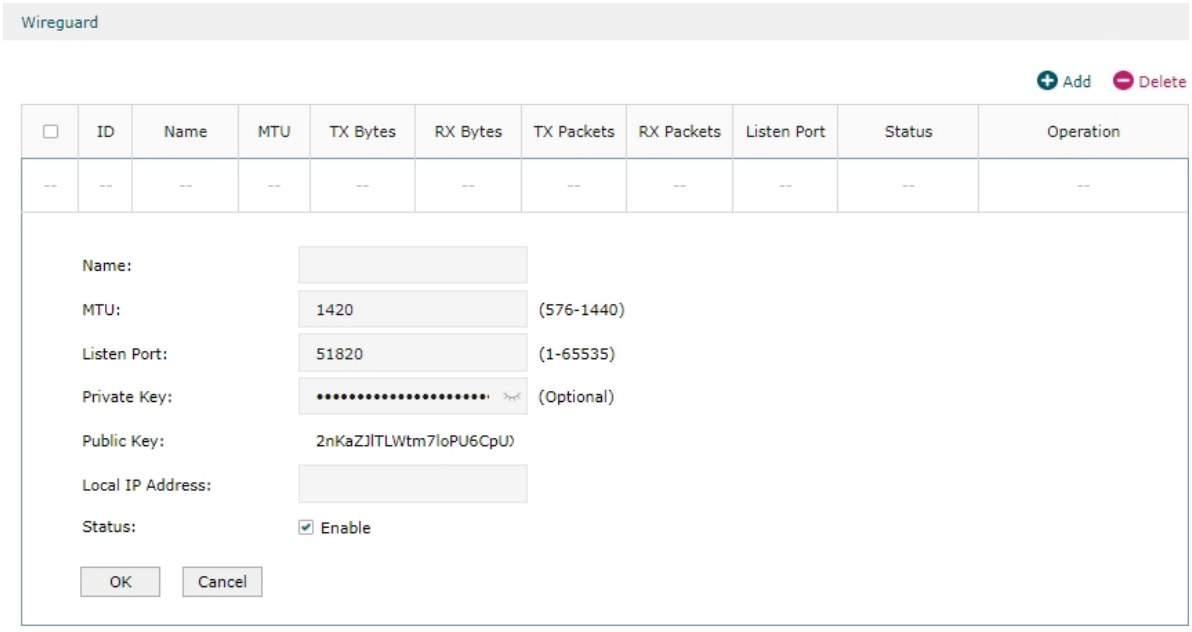
1) WireGuard 서버를 구성합니다.

2) 피어 설정을 구성합니다.

7.1 WireGuard VPN 서버 구성

VPN > WireGard > WireGard 메뉴를 선택하고 추가를 클릭하면 다음 페이지가 로드됩니다.

그림 7-1 와이어가드 VPN 서버 구성하기



WireGuard VPN 서버의 이름을 지정하고 실제 네트워크 환경에 따라 기타 관련 매개변수를 구성한 후 **확인을** 클릭합니다.

이름	와이어가드 인터페이스를 식별하는 이름을 지정합니다.
MTU	Wireguard 인터페이스의 MTU 값을 지정합니다. 기본값 1420을 사용하는 것이 좋습니다.
수신 포트	Wireguard 인터페이스가 수신 대기하는 포트 번호를 지정합니다.

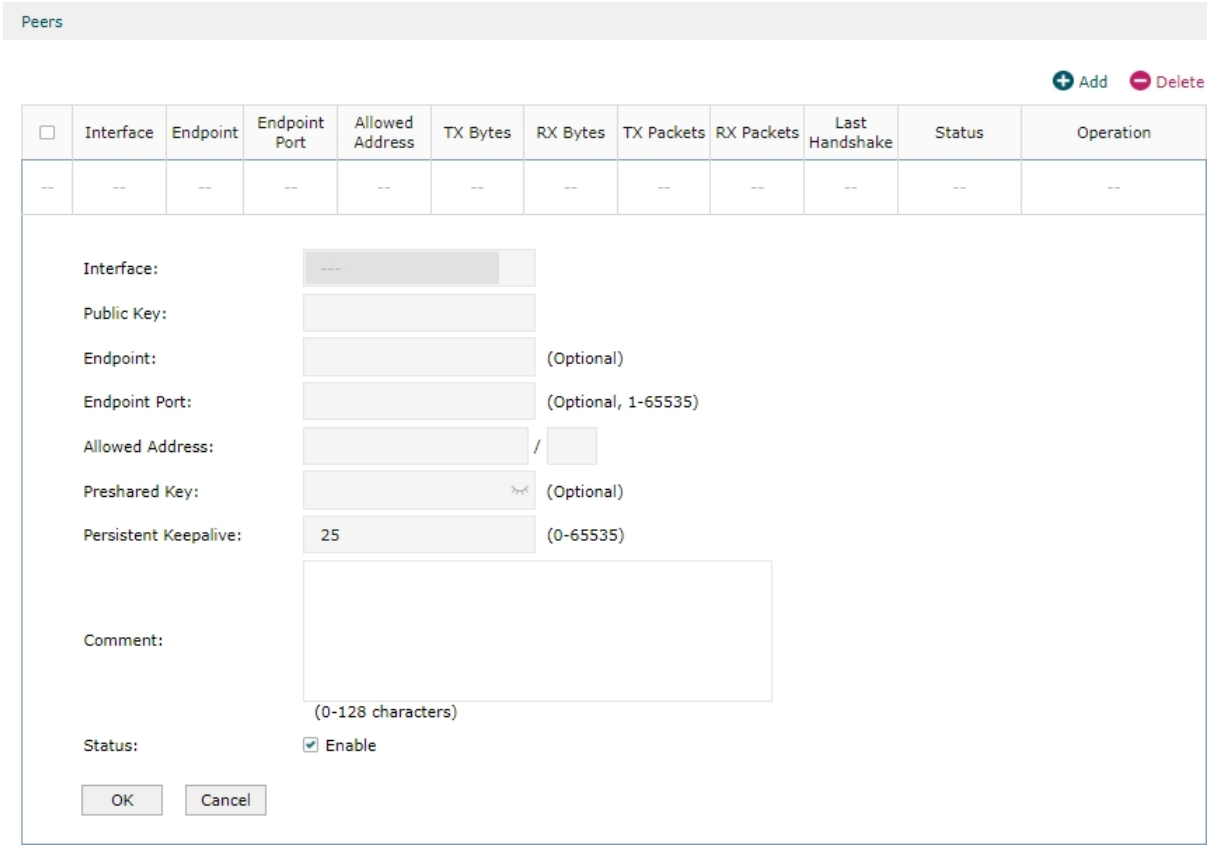
서비스 포트	VPN 장치가 연결되는 VPN 서비스 포트를 입력합니다. 기본 포트는 1194입니다.
개인 키	Wireguard 인터페이스의 개인 키를 지정합니다. 이 값은 장치에서 자동으로 생성되며 수동으로 수정할 수도 있습니다.

공개 키	Wireguard 인터페이스의 공개 키를 지정합니다. 이 필드는 개인 키를 기반으로 자동으로 생성됩니다.
로컬 IP 주소	WireGuard 인터페이스의 IP 주소를 지정합니다. IP 충돌을 피하려면 예약 주소를 선택하세요.
상태	와이어가드 인터페이스 활성화 여부를 지정합니다.

7.2 피어 설정 구성하기

VPN > WireGuard > 피어 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 7-2 피어 구성하기



하나 이상의 피어 라우터에 대해 엔드포인트와 엔드포인트 포트를 구성해야 합니다.

인터페이스	피어가 속한 와이어가드 인터페이스를 지정합니다. 공개 키
	피어의 공개 키를 지정합니다.

엔드포인트	피어의 IP 주소를 지정합니다.
엔드포인트 포트	피어의 포트 번호를 지정합니다.

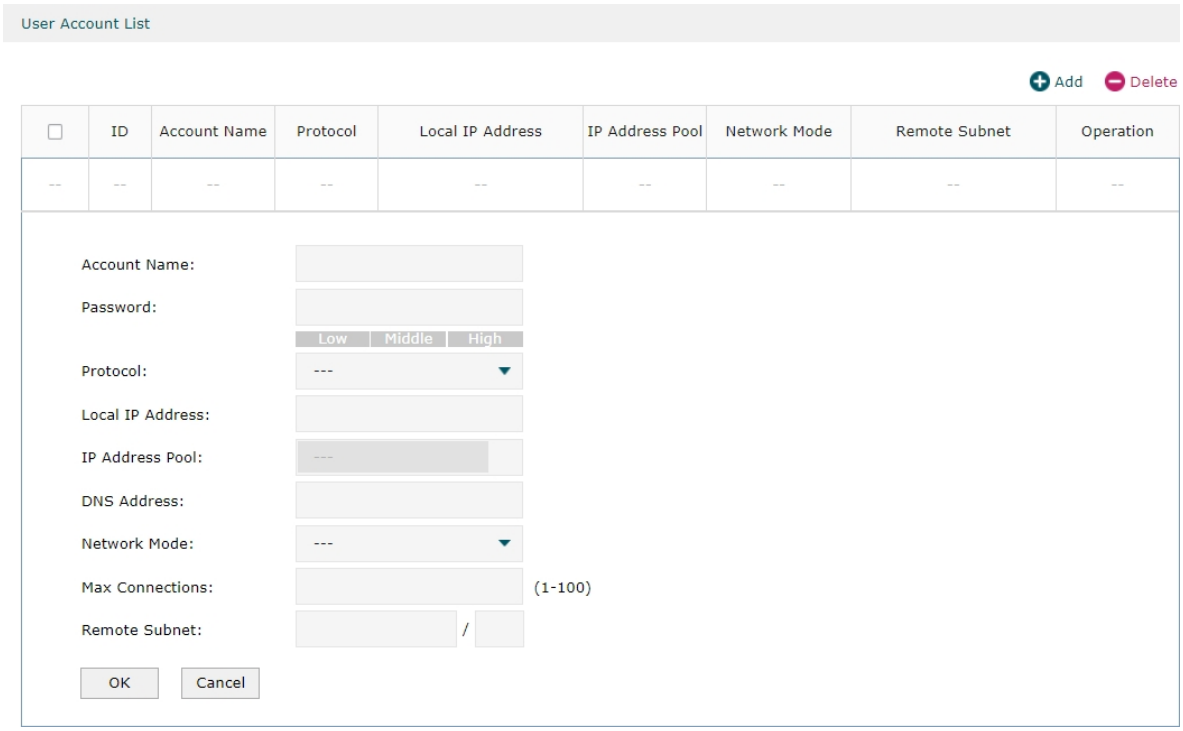
허용된 주소	트래픽이 통과할 수 있는 주소 세그먼트를 지정합니다. 일반적으로 피어의 서브넷 주소를 입력하면 됩니다.
영구 킵얼라이브	터널 킵얼라이브 패킷 간격을 지정합니다.
댓글	피어의 설명을 입력합니다.
상태	피어를 활성화할지 여부를 지정합니다.

8 미국 ers 구성

사용자의 계정을 구성하려면 **VPN > 사용자 > 사용자** 메뉴를 선택하고 **추가를** 클릭합니다.

를 클릭하면 다음 페이지가 로드됩니다.

그림 8-1 사용자 계정 구성하기



계정 이름과 비밀번호를 입력하고 실제 네트워크 환경에 따라 기타 관련 매개변수를 구성한 후 **확인을** 클릭합니다.

계정 이름	VPN 터널에 사용되는 계정 이름을 지정합니다.
비밀번호	VPN 터널에 사용되는 계정 비밀번호를 지정합니다. VPN 클라이언트는 이 계정 이름과 비밀번호를 인증에 사용합니다.
프로토콜	VPN 터널의 프로토콜을 지정합니다. 두 가지 유형이 있습니다: L2TP와 PPTP.
로컬 IP 주소	VPN 서버의 로컬 가상 IP 주소를 지정합니다. IP 충돌을 일으킬 수 있는 DHCP 범위의 IP 주소를 사용하지 마시고, 라우터의 LAN IP를 입력하세요. DHCP 범위를 확인하려면 네트워크 > LAN > 네트워크 목록으로 이동하여 원하는 네트워크의 정보를 확인하세요.
IP 주소 풀	VPN 클라이언트에 IP 주소를 할당할 IP 주소 풀을 지정합니다. 여기서 참조하는 IP 풀은 환경설정 > VPN IP 풀 페이지에서 생성할 수 있습니다.

DNS 주소	VPN 클라이언트에 할당할 DNS 주소(예: 8.8.8.8)를 지정하고, 라우터의 LAN IP를 입력할 수 있습니다.

네트워크 모드	네트워크 모드를 지정합니다. 두 가지 모드가 있습니다: **클라이언트-랜 간**: L2TP/PPTP 클라이언트가 단일 호스트인 경우 이 옵션을 선택합니다. 일반적으로 외부에서 내부 서비스에 액세스하는 데 사용됩니다. **LAN-to-LAN**: L2TP/PPTP 클라이언트가 VPN 게이트웨이인 경우 이 옵션을 선택합니다. 터널링 요청은 항상 장치에서 시작됩니다. 일반적으로 두 사무실 간의 액세스에 사용됩니다.
최대 연결 수	터널이 지원할 수 있는 최대 연결 수를 지정합니다. 클라이언트-랜 네트워크 모드가 활성화된 경우 동시에 연결되는 장치 수를 제한하는 데 사용할 수 있습니다.
원격 서브넷	원격 네트워크를 지정합니다. (L2TP/PPTP 터널의 원격 피어에 있는 LAN의 IP 주소 범위입니다). IP 주소와 서브넷 마스크의 조합입니다. LAN-to-LAN 네트워크 모드가 활성화된 경우에 적용됩니다.

참고:

- 원격 장치에서 VPN 서버에 연결할 수 있는 VPN 연결 계정을 만듭니다.
- 라우터가 L2TP/PPTP 클라이언트 역할을 하는 경우, 이 페이지에서 L2TP/ PPTP 사용자 계정을 구성할 필요가 없습니다.

파트 10

SSL VPN 구성

챕터

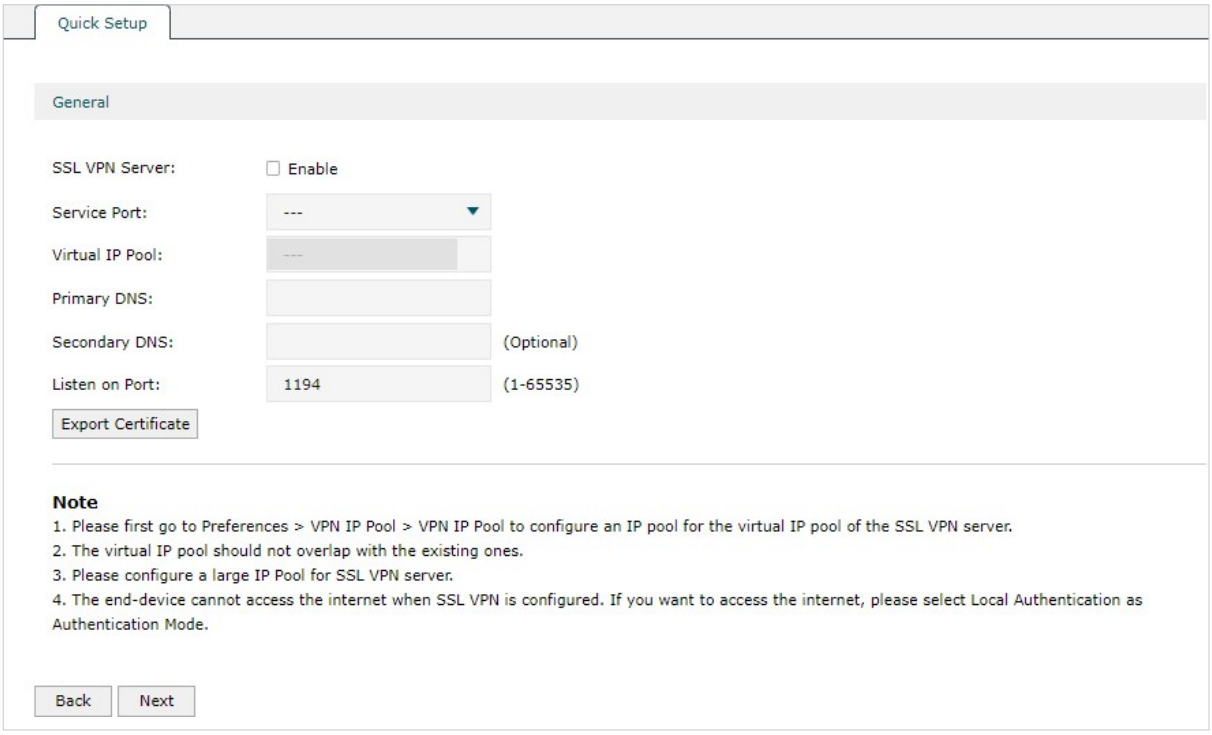
1 Ov erview

SSL VPN은 원격 사용자가 인터넷의 어느 곳에서나 기업 네트워크에 액세스할 수 있도록 합니다. 원격 액세스는 보안 소켓 계층(SSL) VPN 게이트웨이를 통해 활성화됩니다.

2 빠른 설정

빠른 설정은 기본 네트워크 매개변수를 구성하는 방법을 알려줍니다. 빠른 설정을 시작하려면 **SSL VPN > 빠른 설정 > 빠른 설정** 메뉴를 선택하고 시작을 클릭하면 다음 페이지가 로드됩니다.

그림 2-1 빠른 설정



빠른 설정에 따라 SSL VPN을 구성하세요.

3 S 상태 구성

이 기능을 사용하면 SSL VPN에 연결된 모든 클라이언트의 정보를 볼 수 있습니다. 필요에 따라 특정 클라이언트를 차단하거나 연결 해제할 수도 있습니다. 또한 현재 잠긴 사용자를 확인하고 항목을 추가, 삭제 또는 편집할 수 있습니다.

3.1 상태 정보 보기

SSL VPN > 상태 > 연결 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 3-1 상태 정보 보기

온라인 사용자 섹션에서 SSL VPN에 연결된 모든 클라이언트의 정보를 볼 수 있습니다. 필요에 따라 특정 클라이언트를 차단하거나 연결을 해제할 수도 있습니다.

사용자 이름	클라이언트가 로그인에 사용한 사용자명을 표시합
니다. 로그인 IP클라이언트의	IP 주소를 표시합니다.
가상 IPSSL VPN 서버에서 클라이언트에 할당된 가상 IP 주소를 표시합니다.	로그인 시간클라이언트
가 로그인한	시간을 표시합니다.
업로드	클라이언트의 총 업로드 트래픽을 표시합니다.
다운로드	클라이언트의 총 다운로드 트래픽을 표시합니
다. 동작	클라이언트를 차단하거나 연결을 끊습니다.

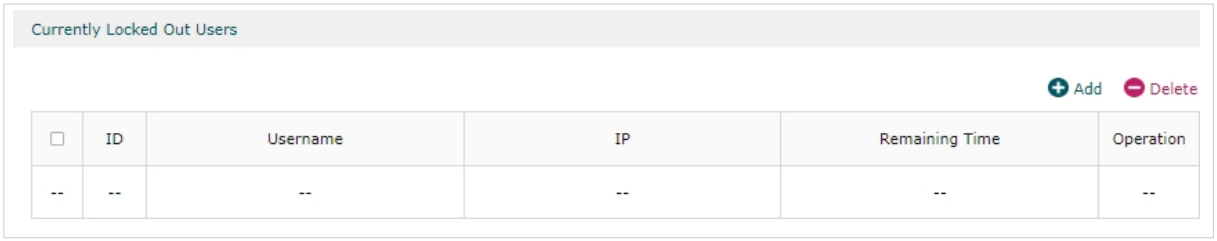
차단: 클라이언트 연결을 끊고 해당 클라이언트를 차단된 사용자 목록에 추가합니다. A 잠긴 사용자는 다시 로그인할 수 없습니다. 사용자 이름 잠금 또는 IP 잠금을 사용 설정하려면 **SSL VPN > SSL VPN 서버 > 고급으로** 이동하세요.

연결 해제: 한 번만 클라이언트의 연결을 끊습니다.

3.2 잠긴 사용자 보기

SSL VPN > 상태 > 잠긴 **사용자** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 3-2 잠긴 사용자 보기



현재 차단된 사용자 섹션에서는 현재 차단된 사용자를 볼 수 있으며, 사용자를 추가하고 차단 **기간을** 설정하거나 항목을 삭제 또는 수정할 수 있습니다.

유형	잠긴 유형을 표시합니다.
사용자 이름	잠긴 사용자의 사용자 아이디를 표시합니다. IP
	잠긴 사용자의 IP 주소를 표시합니다.
남은 시간	잠긴 항목의 남은 유효 시간을 표시합니다.

참고:

- SSL VPN을 구성하기 전에 환경설정 **> VPN IP 풀 > VPN IP 풀로** 이동하여 SSL VPN 서버에 대한 가상 IP 풀을 설정하세요.
- SSL VPN은 구성이 완료된 후 적용됩니다.

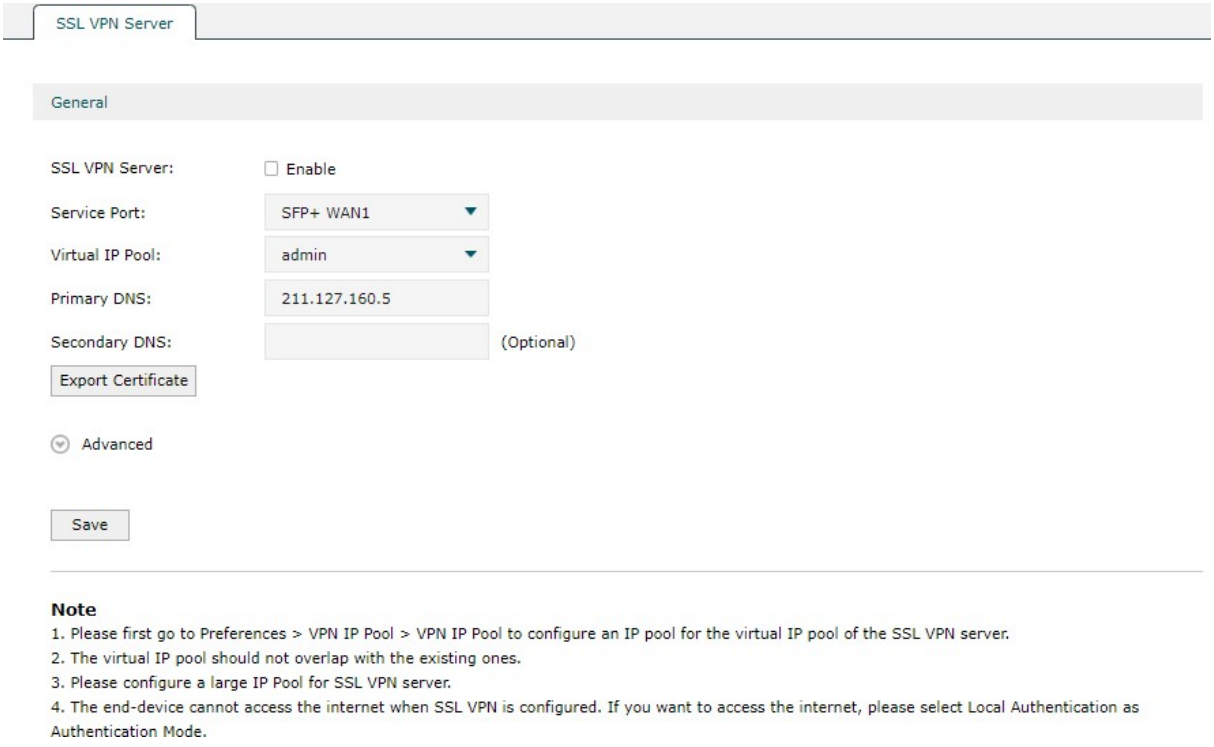
4 S SL VPN 서버 구성

SSL VPN 서버에서 기능을 활성화하고 SSL VPN 설정을 구성할 수 있습니다.

4. 1 SSL VPN 서버 구성하기

SSL VPN > SSL VPN 서버 > SSL VPN 서버 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 4-1 SSL VPN 서버 구성



확인란을 선택하여 기능을 활성화한 다음 해당 매개변수를 구성합니다.

서비스 포트	SSL VPN 서버가 수신 대기할 포트를 선택하면 해당 포트에서 VPN 터널이 적용됩니다.
가상 IP 풀	가상 IP 풀을 선택하면 SSL VPN 서버가 풀 내의 연결된 클라이언트에 IP 주소를 할당합니다. IP 풀을 만들려면 **환경설정 > VPN IP 풀 > VPN IP 풀로** 이동합니다. IP 풀의 IP 주소 수는 4개 이상이어야 합니다.
기본 DNS	DNS 서버의 IP 주소를 지정합니다. SSLVPN DNS 서버에 LAN IP를 할당하세요.

보조 DNS	DNS 서버의 IP 주소를 지정합니다. SSLVPN DNS 서버에 LAN IP를 할당하세요.
포트 수신 대기	SSL VPN 서버가 수신 대기할 포트를 지정합니다. 기본값은 1194입니다.
인증 유형	클라이언트에 대한 인증을 선택합니다. RADIUS 인증의 경우, **SSL VPN > 인증으로** 이동하여 구성합니다.
사용자 이름 잠금	특정 로그인 사용자 아이디를 가진 클라이언트를 차단합니다. **Max. 로그인 시도 횟수:** 사용자 아이디에 대한 최대 로그인 실패 횟수를 지정합니다. 최대 시도에 도달하면 사용자 아이디가 잠깁니다. **잠금 기간:** 사용자 아이디를 잠글 기간을 지정합니다.
IP 차단	특정 로그인 IP의 클라이언트를 차단합니다. **Max. 로그인 시도 횟수:** 사용자 아이디에 대한 최대 로그인 실패 횟수를 지정합니다. 최대 시도에 도달하면 사용자 아이디가 잠깁니다. **잠금 기간:** 사용자 아이디를 잠글 기간을 지정합니다.
유휴 시간 제한	이 기능을 활성화하면 지정된 시간 동안 트래픽이 없는 경우 VPN 터널이 자동으로 닫힙니다.
전체 모드	이 기능을 활성화하면 모든 트래픽이 SSL VPN 터널을 통과합니다. 이 기능을 비활성화하면 리소스 관련 트래픽만 터널을 통과합니다.

참고:

- 먼저 환경설정 **> VPN IP 풀 > VPN IP 풀로** 이동하여 SSL VPN 서버의 가상 IP 풀에 대한 IP 풀을 구성하세요.
- 가상 IP 풀은 기존 IP 풀과 겹치지 않아야 합니다.
- SSL VPN 서버용 대형 IP 풀을 구성하세요.
- SSL VPN이 구성된 경우 최종 기기는 인터넷에 액세스할 수 없습니다. 인터넷에 액세스하려면 인증 모드로 로컬 인증을 선택하세요.

5 리소스 관리

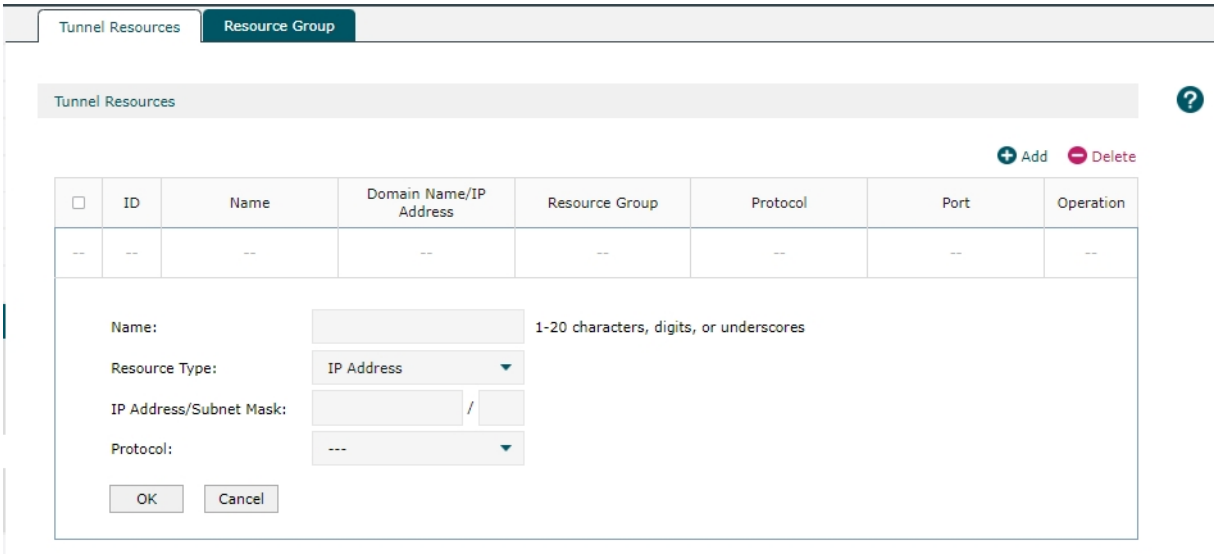
이 기능을 사용하면 클라이언트가 VPN 터널을 통해 액세스할 수 있는 리소스(IP 범위 및 도메인 이름 포함)를 구성하거나 여러 터널 리소스를 그룹에 추가하여 보다 효율적으로 관리할 수 있습니다.

5.1 리소스 구성

SSL VPN > 리소스 관리 > 터널 리소스 메뉴를 선택하고 **추가를** 클릭합니다.

를 클릭하면 다음 페이지가 로드됩니다.

그림 5-1 리소스 구성하기



항목의 이름을 지정하고 다른 매개변수를 구성한 후 **확인을** 클릭합니다.

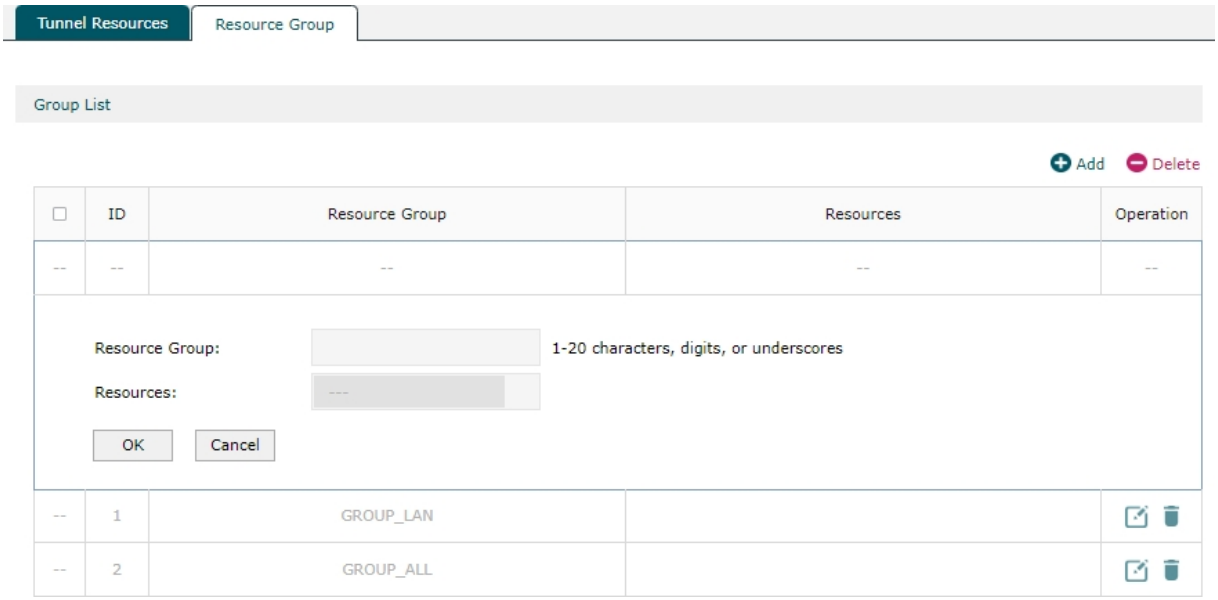
리소스 유형	리소스의 유형을 선택합니다. **IP 주소:** 클라이언트가 액세스할 수 있는 IP 범위와 클라이언트가 액세스할 때 사용할 수 있는 프로토콜을 지정합니다. **도메인 이름:** 클라이언트가 액세스할 수 있는 도메인 이름을 지정합니다.

5.2 터널 리소스 그룹화

SSL VPN > 리소스 관리 > 터널 리소스 메뉴를 선택하고 **추가를** 클릭합니다.

를 클릭하면 다음 페이지가 로드됩니다.

그림 5-2 터널 리소스 그룹화



리소스 그룹의 이름을 지정하고 그룹의 리소스를 선택한 다음 **확인을** 클릭합니다.

참고:

- 리소스 항목은 여러 리소스 그룹에 추가할 수 있으며, 리소스 그룹에 추가된 후에는 항목을 삭제할 수 없습니다. 리소스 항목을 삭제하려면 먼저 리소스 그룹에서 해당 항목을 제거하세요.
- GROUP_LAN은 LAN 세그먼트의 리소스를 나타냅니다.
- GROUP_ALL은 모든 네트워크 세그먼트의 리소스를 나타냅니다.

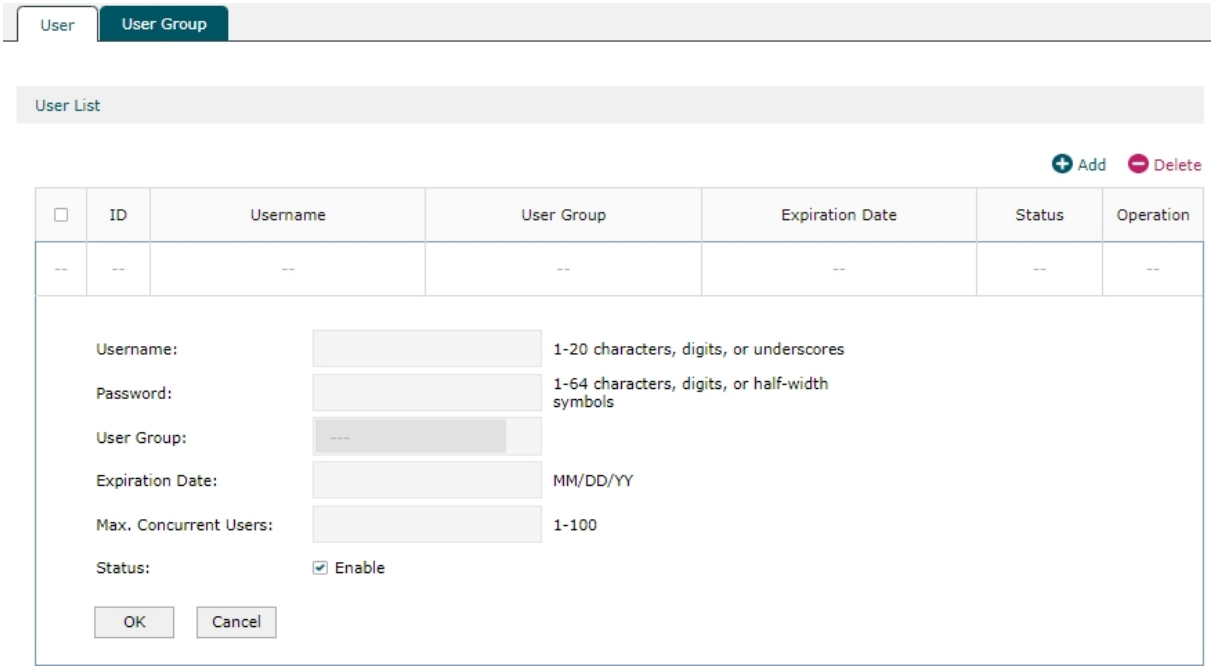
6 사용자 관리

이 기능을 사용하면 SSL VPN의 모든 사용자 설정을 확인 및 구성하거나 여러 사용자를 그룹에 추가하여 보다 효율적으로 관리할 수 있습니다.

6.1 사용자 목록 추가하기

SSL VPN > 사용자 관리 > 사용자 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 6-1 사용자 목록 추가하기



관련 매개변수를 구성하고 **확인을** 클릭합니다.

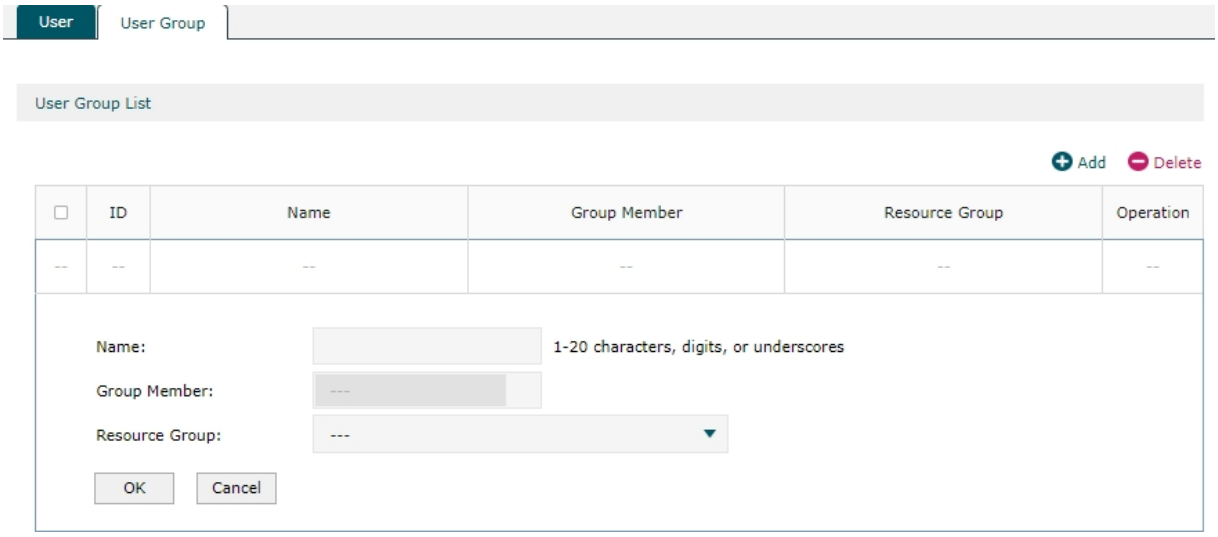
사용자 이름	클라이언트가 로그인에 사용할 사용자 아이디
를 지정합니다. 비밀번호	클라이언트가 로그인에 사용하는 비밀번
호를 지정합니다.	
사용자 그룹	사용자가 속할 그룹을 선택합니다. 사용자는 하나의 사용자 그룹에만 추가할 수 있습니다.
만료 날짜	사용자가 만료되는 시점을 지정합니다.
Max. 동시 사용자	

로그인		에 사용자 아이디를 동시에 사용할 수 있는 최대 클라이언트 수를 지정합니다. 최대 수에 도달하면 새로운 로그인 시도가 거부됩니다.
	상태	사용자 항목의 상태를 표시합니다.

6.2 사용자 그룹화

SSL VPN > 사용자 관리 > 사용자 그룹 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 6-2 사용자 그룹화



사용자 그룹의 이름을 지정하고 그룹의 리소스를 선택한 다음 **확인을** 클릭합니다.

이름	사용자 그룹의 이름을 지정합니다.
그룹 구성원	그룹에 추가할 사용자를 선택합니다. 그룹의 모든 사용자는 동일한 리소스를 공유합니다.
리소스 그룹	사용자 그룹의 리소스 그룹을 선택합니다.

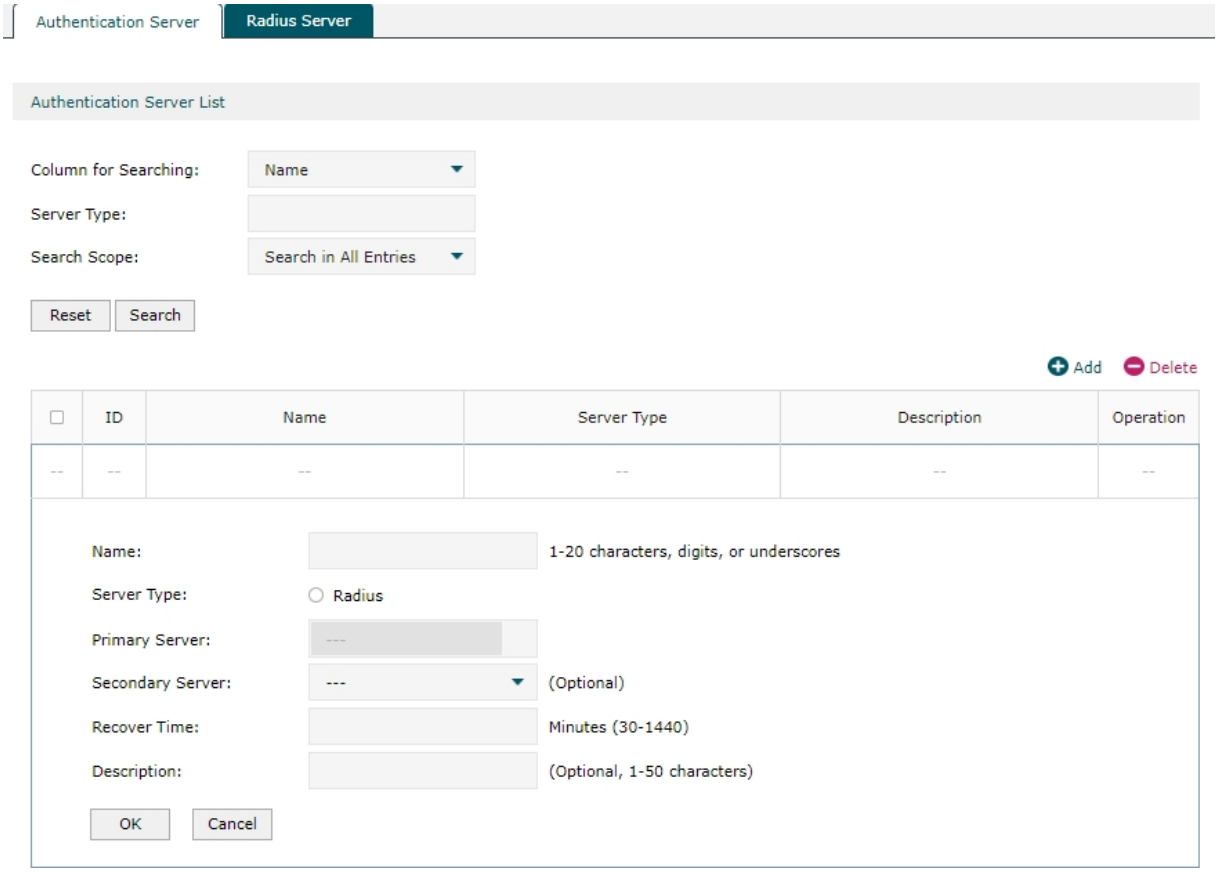
7 인증

이 기능을 사용하면 인증 서버를 확인 및 추가하거나 RADIUS 서버 설정을 확인 및 구성할 수 있습니다.

7.1 인증 서버 목록 추가

SSL VPN > 인증 > 인증 서버 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 7-1 인증 서버 목록 추가하기



인증 서버의 이름을 지정하고 관련 매개변수를 구성한 후 **확인을** 클릭합니다.

서버 유형	인증 서버의 유형을 선택합니다. 현재는 RADIUS 서버만 지원됩니다.
기본 서버	인증을 위한 기본 서버를 지정합니다.
보조 서버	인증을 위한 보조 서버를 지정합니다. 기본 서버가 다운되면 보조 서버가 사용됩니다.
복구 시간	기본 서버가 다운되었을 때 기본 서버를 다시 연결할 간격을 지정합니다.

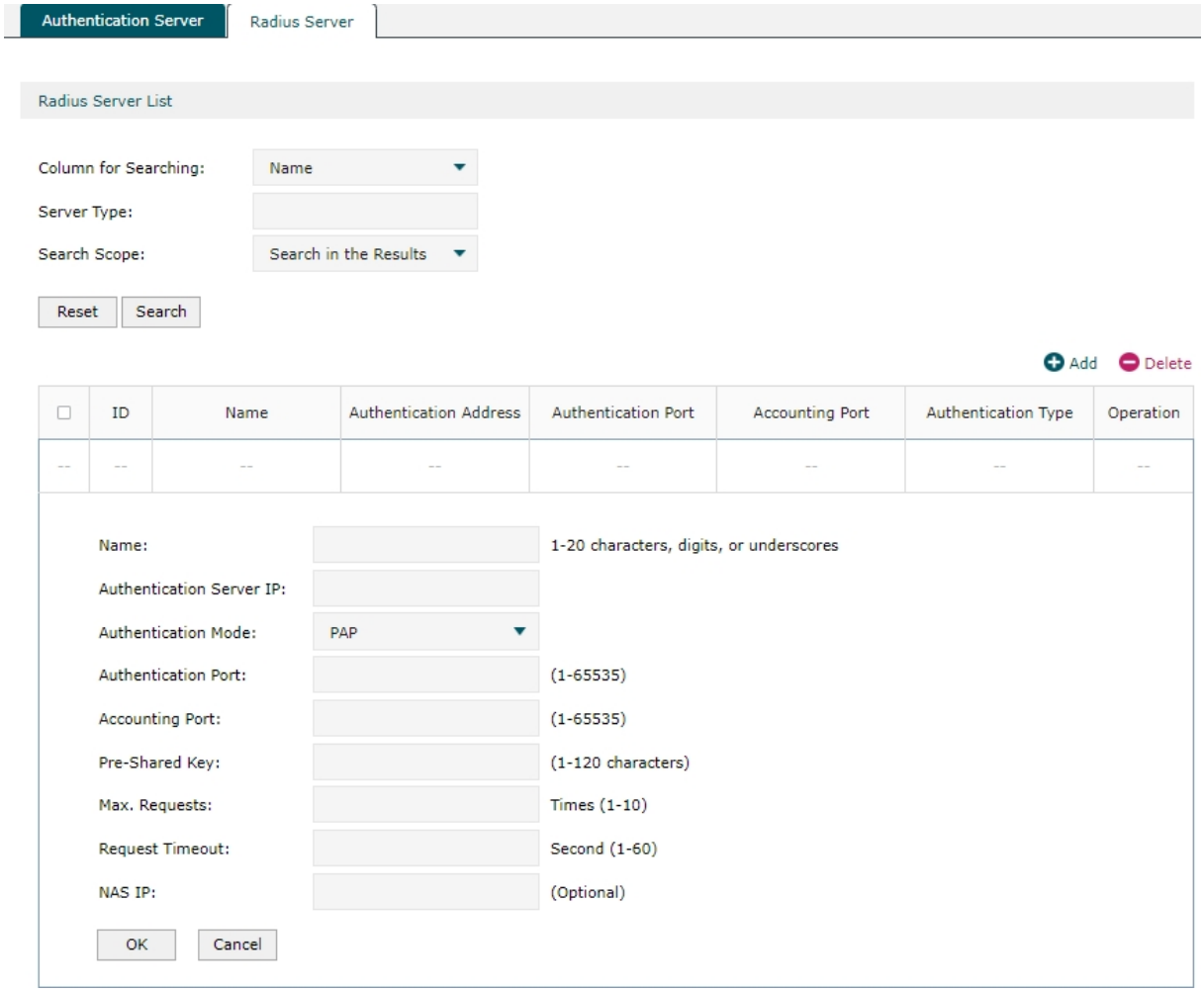
설명	서버에 대한 설명을 입력합니다.

상태	사용자 항목의 상태를 표시합니다.

7.2 래디우스 서버 구성

SSL VPN > 인증 > 래디우스 서버 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

그림 7-2 래디우스 서버 구성



RADIUS 서버의 이름을 지정하고 관련 매개변수를 구성한 후 **확인을** 클릭합니다.

인증 서버 IP	RADIUS 서버의 IP 주소를 지정합니다.
인증 모드	RADIUS 서버의 인증 프로토콜을 선택합니다. 두 가지 인증 프로토콜을 사용할 수 있습니다: PAP와 CHAP.
인증 포트	인증 요청에 대한 인증 서버의 UDP 대상 포트를 지정합니다. 권장 포트는 1812입니다.

회계 포트	계정 요청에 대한 RADIUS 서버의 UDP 대상 포트를 지정합니다. 권장 포트는 1813입니다.
사전 공유 키	라우터와 RADIUS 인증 서버 간의 통신을 확인하는 데 사용할 비밀번호를 지정합니다.
Max. 요청	응답이 수신되지 않을 때 전송되는 최대 요청 수를 지정합니다.
요청 시간 초과	요청 타임아웃의 최대 간격을 지정합니다. 시간 초과 후 요청이 다시 전송됩니다.
NAS IP	라우터가 RADIUS 서버와 통신할 수 있는 IP 주소를 지정합니다.

Part 11

인증 구성

챕터

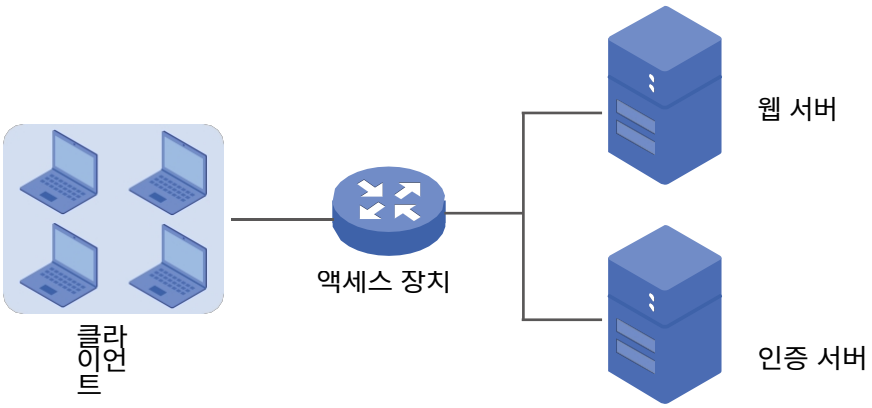
1 Ov erview

웹 인증이라고도 하는 포털 인증은 일반적으로 호텔이나 커피숍과 같은 게스트 액세스 네트워크에서 클라이언트의 인터넷 액세스를 제어하기 위해 배포됩니다. 포털 인증에서는 클라이언트의 모든 HTTP 요청이 먼저 인증 페이지로 리디렉션됩니다. 클라이언트는 인증 페이지에 계정 정보를 입력하여 인증을 받아야 하며, 인증에 성공한 후 인터넷을 방문할 수 있습니다.

1.1 일반적인 토폴로지

포털 인증의 일반적인 토폴로지는 아래와 같습니다:

그림 1-1 포털 인증의 토폴로지



- 클라이언트

인터넷 액세스를 허용하기 전에 인증해야 하는 최종 장치입니다.

- 액세스 장치

포털 인증을 지원하는 장치입니다. 이 사용자 가이드에서는 라우터를 의미합니다. 액세스 디바이스는 인증 전에 모든 HTTP 요청을 웹 서버로 리디렉션하고, 인증 프로세스 중에 인증 서버와 상호작용하여 클라이언트를 인증하고, 인증에 성공한 후 사용자가 인터넷에 액세스할 수 있도록 허용하는 등의 기능을 수행합니다.

- 웹 서버

웹 서버는 클라이언트의 HTTP 요청에 응답하고 인증 로그인 페이지를 반환합니다.

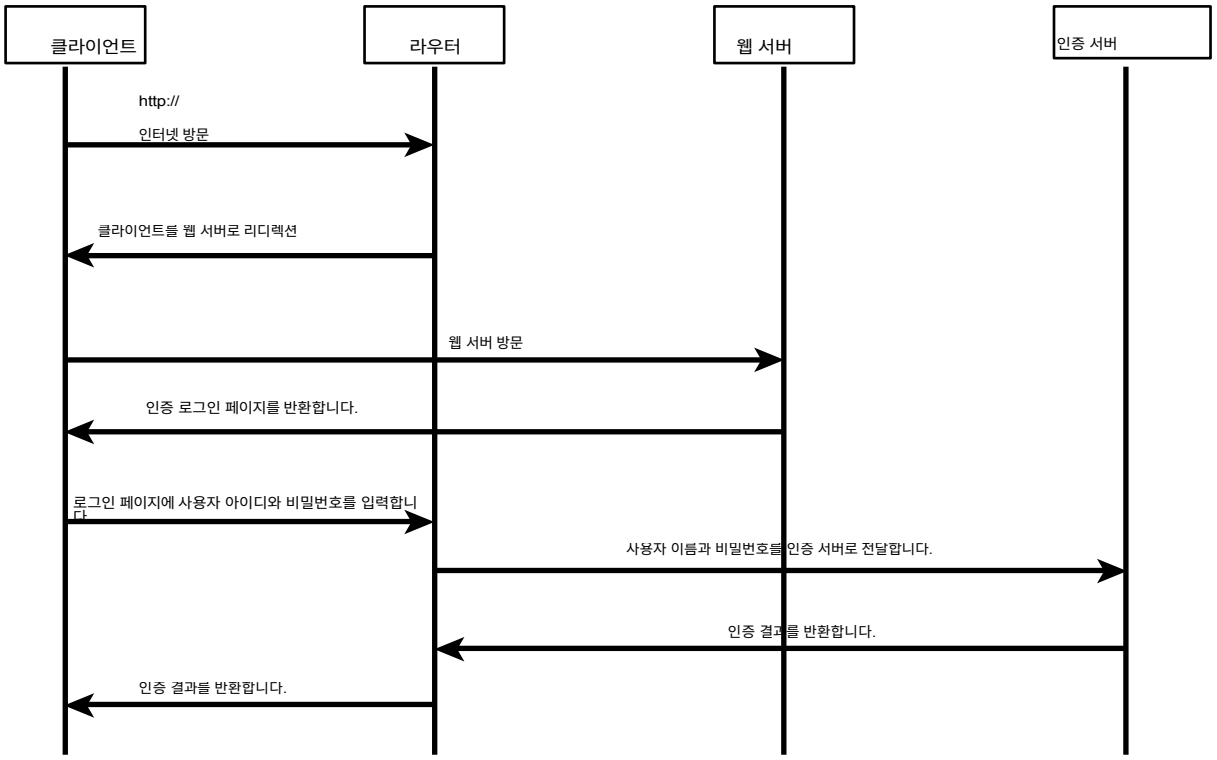
■ 인증 서버

인증 서버는 사용자 계정의 정보를 기록하고 액세스 장치와 상호 작용하여 클라이언트를 인증합니다.

1.2 포털 인증 프로세스

포털 인증 프로세스는 다음과 같습니다:

그림 1-2 포털 인증 프로세스



1) 클라이언트가 라우터에 연결되었지만 인증되지 않은 상태에서 HTTP를 통해 인터넷을 방문하기 시작합니다;
2) 라우터는 클라이언트의 HTTP 요청을 웹 서버로 리디렉션합니다;
3) 클라이언트가 웹 서버를 방문합니다;
4) 웹 서버는 인증 로그인 페이지를 클라이언트에 반환합니다;
5) 클라이언트는 인증 로그인 페이지에서 사용자 이름과 비밀번호를 입력합니다;
6) 라우터는 사용자 이름과 비밀번호를 인증 서버로 전달합니다;
7) 인증 서버는 인증 결과를 라우터로 반환합니다;
8) 라우터가 인증 결과를 클라이언트에 회신합니다;
9) 클라이언트가 인증에 성공한 후 인터넷을 방문합니다.

1.3 지원되는 기능

포털 인증을 구성하려면 웹 서버와 인증 서버를 모두 구성해야 합니다. 웹 서버는 로그인을 위한 인증 페이지를 제공하고, 인증 서버는 계정 정보를 기록하고 클라이언트를 인증합니다.

1.3.1 지원되는 웹 서버

라우터에는 웹 서버가 내장되어 있으며 외부 웹 서버도 지원합니다. 내장 서버 또는 외부 서버를 사용하여 인증 페이지를 구성할 수 있습니다.

사용자 지정 페이지

기본 제공 웹 서버를 사용하고 라우터에서 인증 페이지를 사용자 지정할 수 있습니다.

외부 링크

외부 웹 서버를 지정하고 외부 웹 서버에서 인증 페이지를 구성할 수 있습니다.

1.3.2 지원되는 인증 서버

라우터는 세 가지 유형의 포털 인증을 제공합니다:

반경 인증

래디우스 인증에서는 외부 래디우스 서버를 인증 서버로 지정할 수 있습니다. 사용자의 계정 정보는 Radius 서버에 기록됩니다.

로컬 인증

추가 Radius 서버가 없는 경우 로컬 인증을 선택할 수 있습니다. 로컬 인증에서는 라우터가 내장된 인증 서버를 사용하여 인증합니다. 내장 인증 서버는 최대 500개의 로컬 사용자 계정을 기록할 수 있으며, 각 계정은 최대 1024개의 클라이언트를 인증하는 데 사용할 수 있습니다.

원키 온라인

원키 온라인 인증에서는 사용자가 계정 정보를 입력하지 않고도 네트워크에 액세스할 수 있습니다.

1.3.3 게스트 리소스

게스트 리소스는 포털 인증을 통과하기 전에 사용자에게 무료 리소스를 제공하는 데 사용됩니다.

2 인증 구성

로컬 인증을 구성하려면 다음 단계를 따르세요:

1) 인증 페이지를 구성합니다.

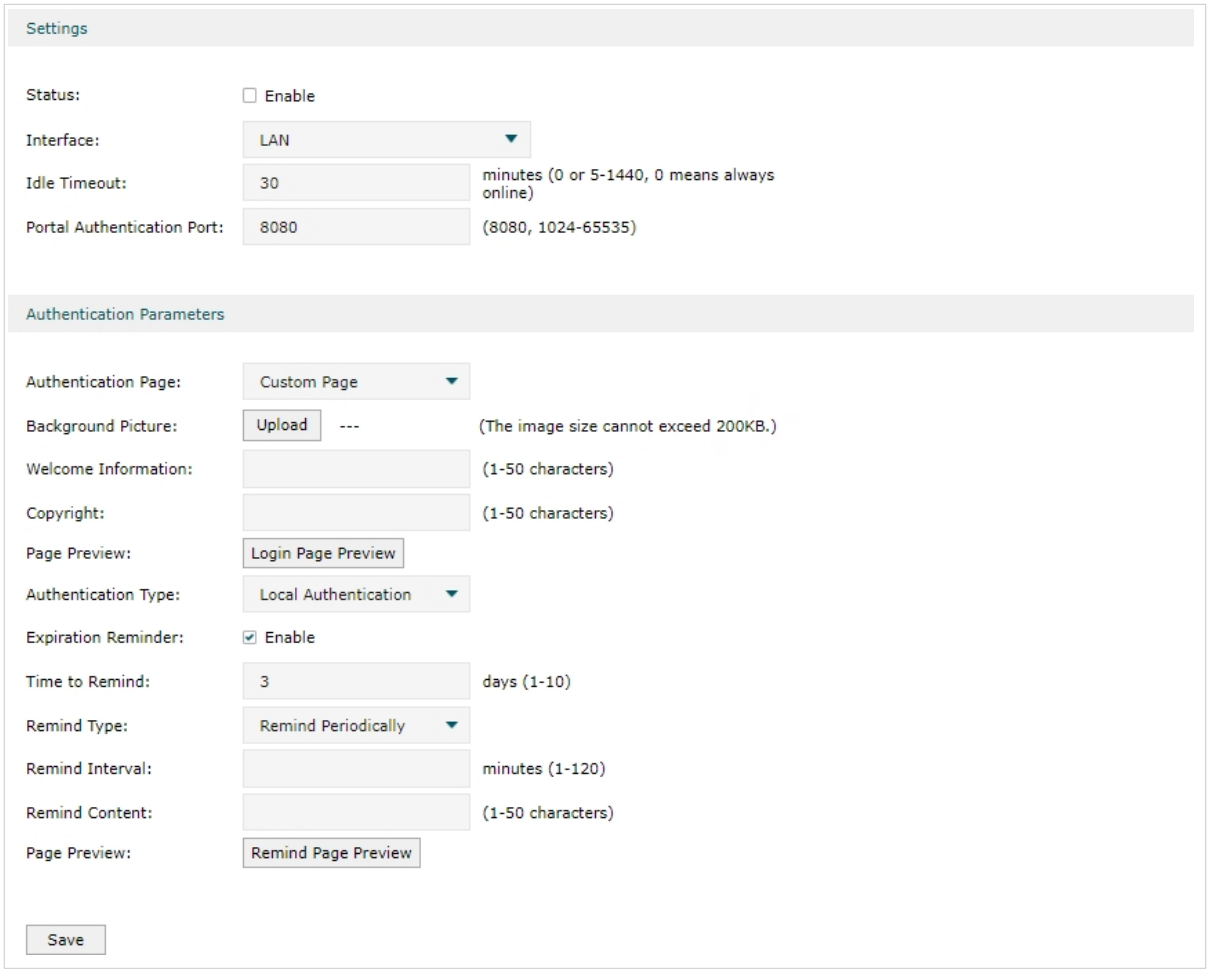
2) 로컬 사용자 계정을 구성합니다.

2.1 인증 페이지 구성하기

클라이언트가 인터넷에 액세스하려고 하면 브라우저는 인증 페이지로 리디렉션됩니다. 인증 페이지에서 사용자는 로그인하기 위해 사용자 이름과 비밀번호를 입력해야 합니다. 인증에 성공하면 사용자는 인터넷에 액세스할 수 있습니다.

인증 > **인증 설정** > **웹 인증** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 2-1 인증 페이지 구성하기



인증 페이지를 구성하려면 다음 단계를 따르세요:

1) **설정** 섹션에서 인증 상태를 활성화하고 유휴 시간 제한 및 포털 인증 포트를 구성합니다.

상태	포털 인증을 사용하려면 확인란을 선택합니다.
인터페이스	효과적인 인터페이스를 지정합니다.
유휴 시간 제한	유휴 시간 제한을 지정합니다. 지정된 기간(유휴 시간 제한) 동안 비활성 상태가 지속되면 클라이언트의 연결이 끊어지고 다시 인증받아야 합니다. 값 0은 클라이언트가 비활성 상태이더라도 임대된 인증 타임아웃까지 클라이언트가 항상 온라인 상태를 유지함을 의미합니다.
포털 인증 포트	포털 인증을 위한 서비스 포트를 입력합니다. 기본 설정은 8080입니다.

2) **인증 매개변수** 섹션에서 인증 페이지의 매개변수를 구성합니다.

인증 페이지	인증 페이지 유형을 선택합니다. **사용자 지정**: 기본 제공 웹 서버를 사용하여 배경 사진, 환영 정보 및 저작권 정보를 지정하여 인증 페이지를 사용자 지정할 수 있습니다. **외부 링크**: 외부 웹 서버의 URL을 입력하여 인증 페이지를 제공할 외부 웹 서버를 지정할 수 있습니다.
배경 그림	**업로드** 버튼을 클릭하여 사용자 지정 인증 페이지의 배경 사진으로 로컬 이미지를 선택합니다.
환영 정보	사용자 지정 인증 페이지에 표시할 환영 정보를 지정합니다.
저작권	사용자 지정 인증 페이지에 표시할 저작권 정보를 지정합니다.
페이지 미리보기	**로그인 페이지 미리 보기** 버튼을 클릭하면 사용자 지정한 인증 페이지를 미리 볼 수 있습니다.
인증 URL	인증 페이지를 '외부 링크'로 선택한 경우 인증 페이지의 URL을 지정합니다. 클라이언트가 인증을 시작할 때 브라우저가 이 URL로 리디렉션됩니다.
성공 리디렉션 URL	인증 페이지를 '외부 링크'로 선택한 경우 성공 리디렉션 URL을 지정합니다. 인증이 성공하면 브라우저가 이 URL로 리디렉션됩니다.
리디렉션 실패	URL인증 페이지를 '외부 링크'로 선택한 경우 리디렉션 실패 URL을 지정합니다. 인증에 실패하면 브라우저가 이 URL로 리디렉션됩니다.

참고:

웹 서버가 LAN에 배포되지 않은 경우 인증에 성공하기 전에 클라이언트가 외부 웹 서버에 액세스할 수 있도록 게스트 리소스 항목을 만들어야 합니다. 게스트 리소스를 구성하려면 게스트 리소스 구성으로 이동합니다.

3) 인증 유형을 선택하고 만료 알림을 구성한 다음 **저장을** 클릭합니다.

인증 유형	인증 유형을 로컬 인증으로 선택합니다.
만료 알림	만료 알림을 사용하려면 확인란을 선택합니다. 온라인 시간이 곧 만료될 때 사용자에게 알려주는 알림 페이지가 표시됩니다.
알림 시간	사용자에게 알림을 보낼 만료일 전 일수를 지정합니다. 알림 유형 알림 유형을 지정합니다. **한 번 알림**: 인증이 성공한 후 사용자에게 한 번만 알림을 보냅니다. **주기적으로 미리 알림**: 미리 알림 기간 동안 지정된 간격으로 사용자에게 미리 알림을 보냅니다.
알림 간격	알림 유형을 "주기적으로 알림"으로 지정한 경우 라우터가 사용자에게 알림을 보내는 간격을 지정합니다.
미리 알림 콘텐츠 미리 알림 콘텐츠를 지정합니다.	콘텐츠가 미리 알림 페이지에 표시됩니다. 페이지 미리
보기	미리 알림 페이지를 보려면 버튼을 클릭합니다.

2.2 로컬 사용자 계정 구성

로컬 인증에서 라우터는 내장된 인증 서버를 사용하여 사용자를 인증합니다. 로컬 사용자에 대한 인증 계정을 구성해야 합니다.

라우터는 두 가지 유형의 로컬 사용자를 지원합니다:

정식 사용자: 사용자에게 장기간(일 단위) 네트워크 서비스를 제공하려는 경우 해당 사용자에 대한 정식 사용자 계정을 만들 수 있습니다.

무료 사용자: 사용자에게 단기간(분 단위) 네트워크 서비스를 제공하려는 경우 해당 사용자에게 무료 사용자 계정을 만들 수 있습니다.

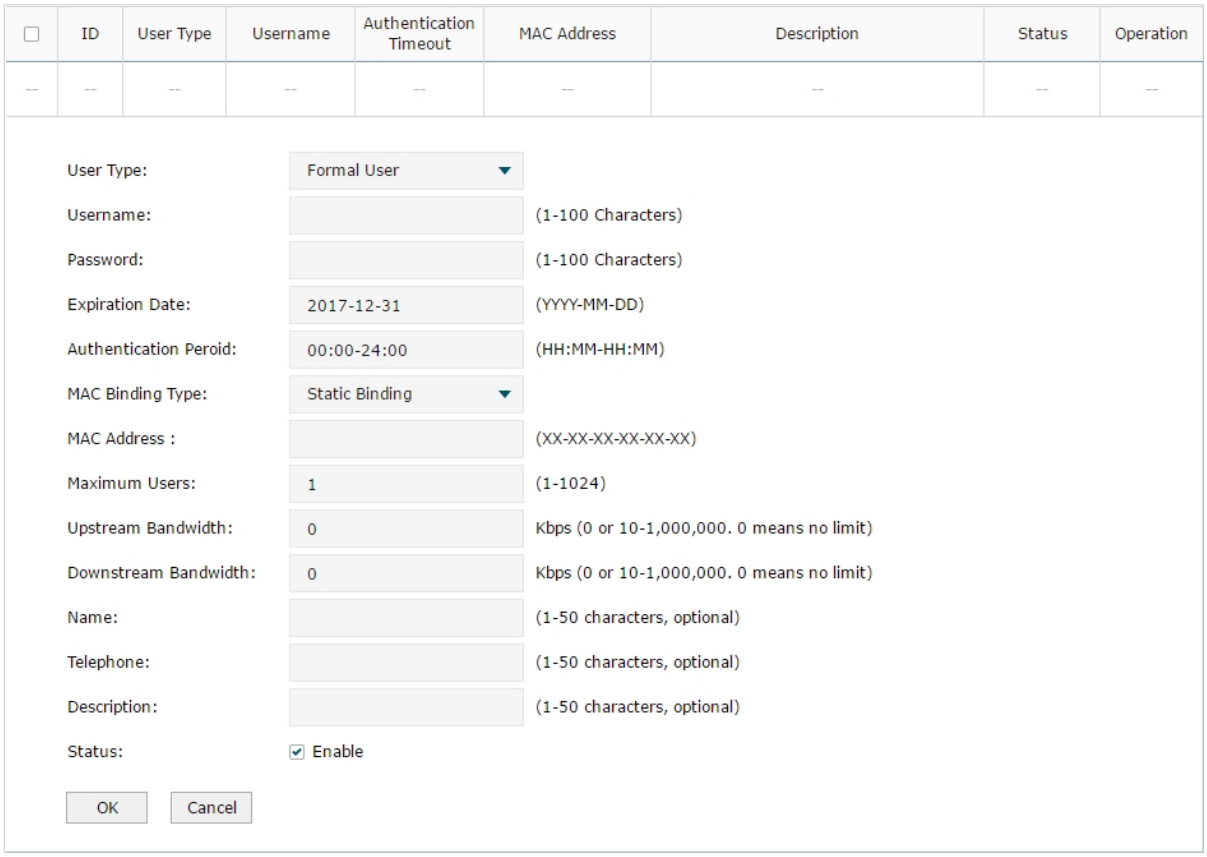
2.2.1 로컬 사용자 계정 구성

■ 공식 사용자 계정 구성하기

인증 > **사용자 관리** > **사용자 관리** 메뉴를 선택하고 **추가를** 클릭합니다.

를 클릭하면 다음 페이지가 로드됩니다.

그림 2-2 공식 사용자 계정 구성하기



사용자 유형을 지정하고, 공식 사용자 계정의 사용자 이름과 비밀번호를 구성하고, 기타 해당 매개변수를 구성합니다. 그런 다음 **확인을** 클릭합니다.

사용자 유형	사용자 유형을 공식 사용자로 지정합니다.
사용자 이름/ 비밀번호	계정의 사용자 아이디와 비밀번호를 지정합니다. 사용자 아이디는 기존 아이디와 동일할 수 없습니다.
만료 날짜	계정의 만료일을 지정합니다. 정식 사용자는 이 날짜 이전에 이 계정을 사용하여 인증할 수 있습니다.
인증 페로이드	클라이언트의 인증이 허용되는 기간을 지정합니다.
MAC 바인딩 유형	MAC 바인딩 유형을 지정합니다. MAC 바인딩에는 세 가지 유형이 있습니다: 바인딩 없음, 정적 바인딩, 동적 바인딩입니다. **바인딩 없음**: 클라이언트의 MAC 주소가 바인딩되지 않습니다. **정적 바인딩**: 바인딩할 클라이언트의 MAC 주소를 수동으로 입력합니다. 바인딩된 클라이언트만 사용자 이름과 비밀번호를 사용하여 인증할 수 있습니다.

동적 바인딩: 인증을 통과	한 첫 번째 클라이언트의 MAC 주소가 바인딩됩니다. 이후에는 바인딩된 클라이언트만 사용자 이름과 비밀번호를 사용하여 인증할 수 있습니다.
MAC 주소	MAC 바인딩 유형을 "정적 바인딩"으로 선택한 경우 바인딩할 클라이언트의 MAC 주소를 입력합니다.

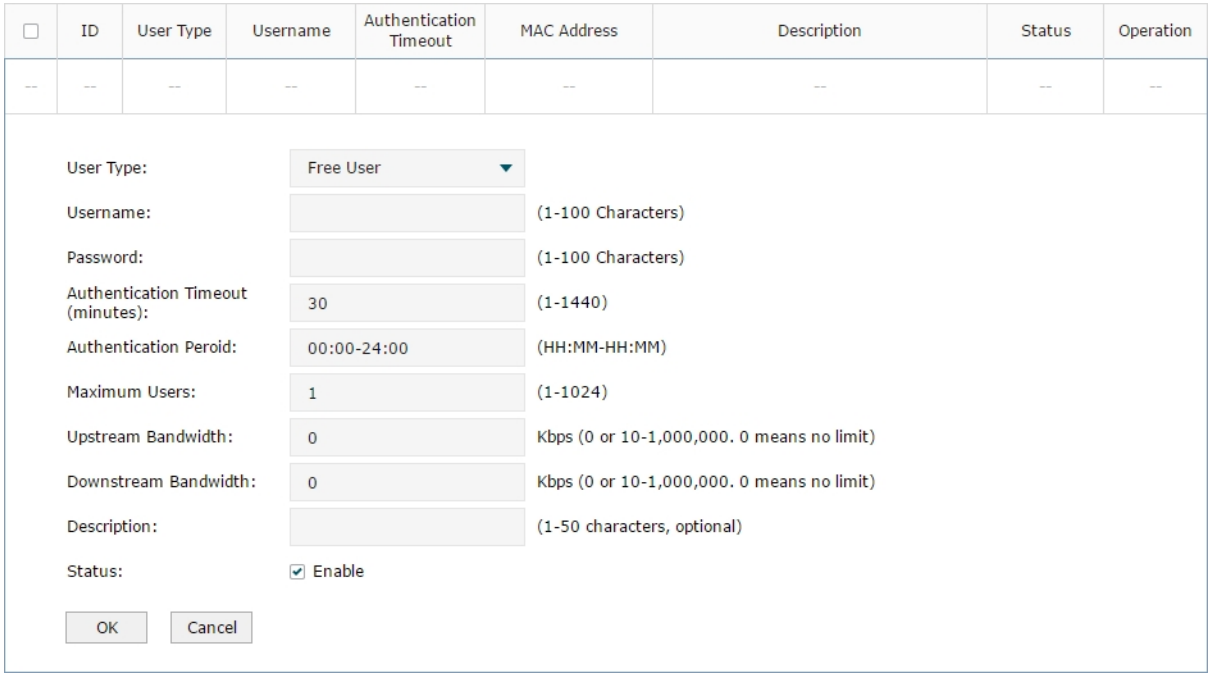
최대 사용자 수	이 계정을 사용하여 인증할 수 있는 최대 사용자 수를 지정합니다. 참고: MAC 바인딩 유형이 정적 바인딩 또는 동적 바인딩인 경우, 최대 사용자 수 값이 1명보다 크도록 구성되어 있어도 바인딩된 클라이언트, 즉 한 클라이언트만 이 사용자 이름과 비밀번호를 사용하여 인증할 수 있습니다.
업스트림 대역폭/다운스트림 대역폭	(선택 사항) 사용자의 업스트림/다운스트림 대역폭을 지정합니다. 0은 제한이 없음을 의미합니다.
이름	(선택 사항) 사용자의 이름을 기록합니다.
전화번호	(선택 사항) 사용자의 전화번호를 기록합니다. 설명
	(선택 사항) 사용자에 대한 간단한 설명을 입력합
니다. 상태	이 계정을 활성화하려면 확인란을 선택합니다.

■ 무료 사용자 계정 구성하기

인증 > 사용자 관리 > 사용자 관리 메뉴를 선택하고 **추가를** 클릭합니다.

를 클릭하면 다음 페이지가 로드됩니다.

그림 2-3 무료 사용자 계정 구성하기



사용자 유형을 지정하고, 무료 사용자 계정의 사용자 이름과 비밀번호를 구성하고, 기타 해당 매개변수를 구성합니다. 그런 다음 **확인을** 클릭합니다.

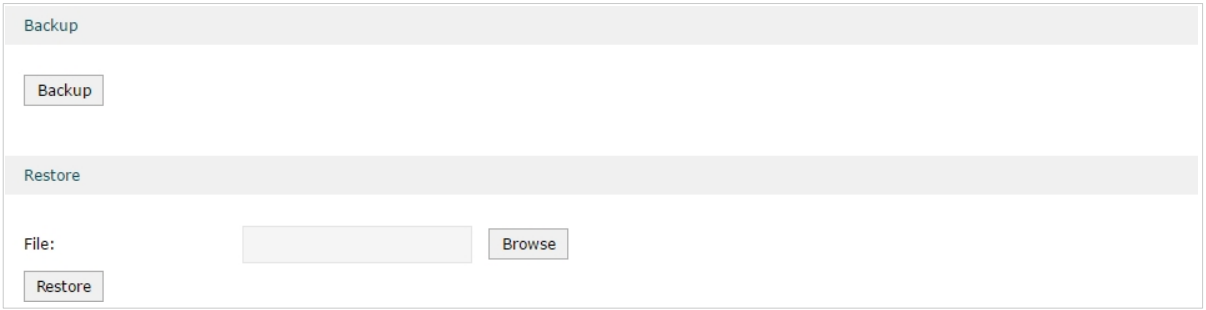
사용자 유형	사용자 유형을 무료 사용자로 지정합니다.

사용자 이름/비밀번호	사용자 계정의 사용자 아이디와 비밀번호를 지정합니다. 사용자 아이디는 기존 아이디와 동일할 수 없습니다.
인증 시간 초과	계정의 무료 기간을 지정합니다. 기본값은 30분입니다.
최대 사용자 수	이 사용자 아이디와 비밀번호를 사용하여 인증할 수 있는 최대 사용자 수를 지정합니다.
업스트림 대역폭/다운스트림 대역폭	(선택 사항) 사용자의 업스트림/다운스트림 대역폭을 지정합니다. 0은 제한이 없음을 의미합니다.
상태	이 계정을 활성화하려면 확인란을 선택합니다.

2.2.2 (선택 사항) 로컬 사용자 백업 구성하기

인증 > **사용자 관리** > **구성 백업** 메뉴를 선택하면 다음 페이지가 로 드 됩 니 다 .

그림 2-4 공식 사용자 구성하기



■ 로컬 사용자의 계정을 백업하려면 다음과 같이 하세요.

백업 버튼을 클릭하면 모든 로컬 사용자 계정을 ANSI 코딩 형식의 CSV 파일로 백업할 수 있습니다.

■ 로컬 사용자의 계정을 복원하려면 다음과 같이 하세요.

백업이 있는 경우 라우터로 계정을 가져올 수 있습니다. **찾아보기를** 클릭하여 파일 경로(백업은 CSV 파일이어야 함)를 선택한 다음 **복원을** 클릭하여 계정을 복원합니다.

한 번에 여러 로컬 사용자 계정을 수동으로 추가할 수도 있습니다:

1) Excel 파일을 만들고 로컬 사용자 계정을 추가한 다음, 이 Excel 파일을 ANSI 코딩 형식의 CSV 파일로 저장합니다. **백업을** 클릭하여 올바른 형식의 CSV 파일을 가져올 수 있습니다.

2) 찾아보기를 클릭하여 파일 경로를 선택한 다음 **복원을** 클릭하여 파일을 복원합니다.

참고:

Excel을 사용하여 CSV 파일을 열면 일부 숫자 형식이 변경되어 숫자가 잘못 표시될 수 있습니다. Excel을 사용하여 CSV 파일을 편집하는 경우 셀 형식을 텍스트로 설정하세요.

3 반경 인증 구성

반경 인증을 구성하려면 다음 단계를 따르세요:

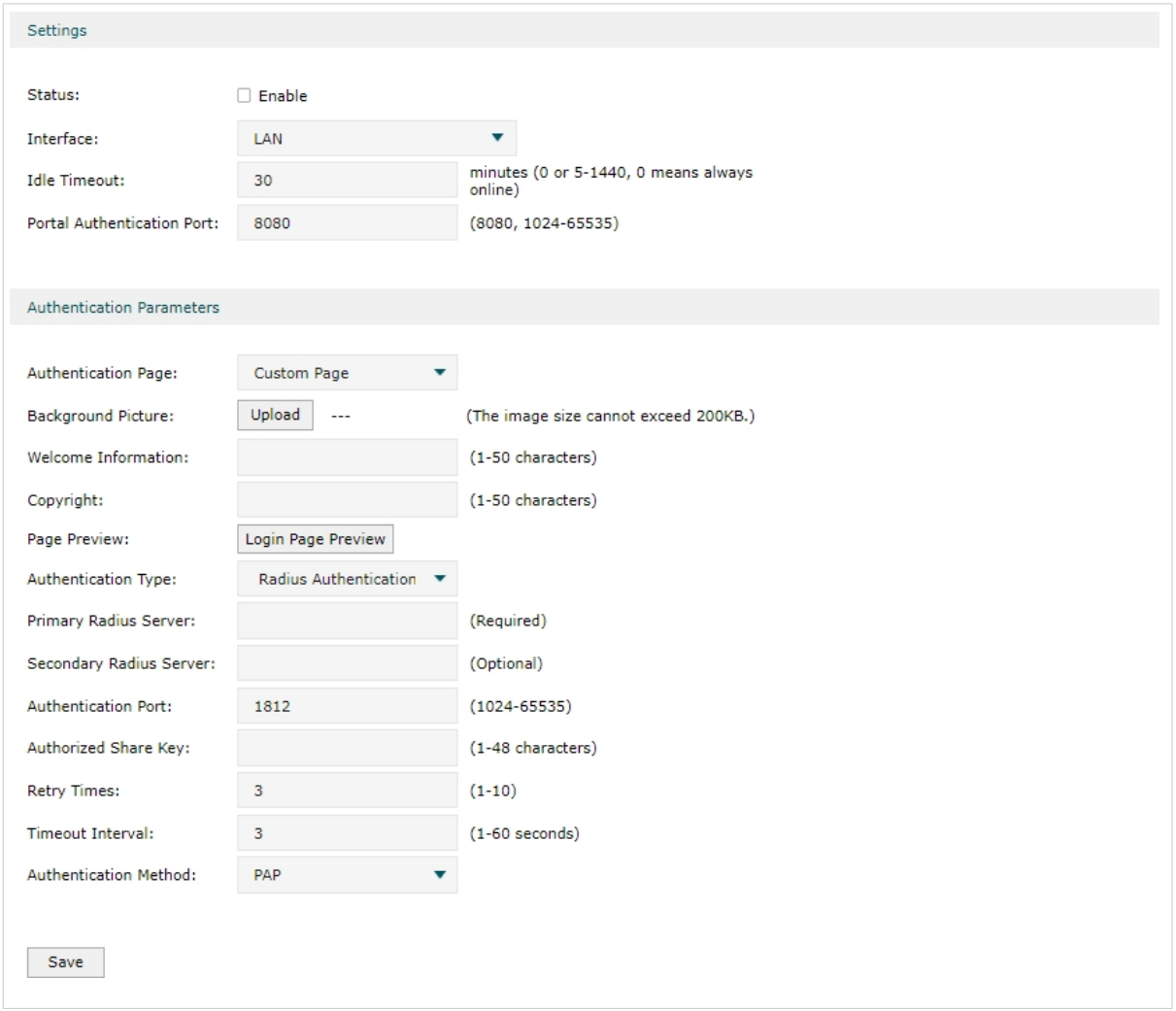
1) 인증 페이지를 구성합니다.

2) 외부 Radius 서버를 지정하고 해당 매개변수를 구성합니다.

3.1 반경 인증 구성

인증 > **인증 설정** > **웹 인증** 메뉴를 **선택하면** 다음 페이지가 로드됩니다.

그림 3-1 반경 인증 구성하기



반경 인증을 구성하려면 다음 단계를 따르세요:

1) **설정** 섹션에서 인증 상태를 활성화하고 유휴 시간 제한 및 포털 인증 포트를 구성합니다.

상태	포털 인증을 사용하려면 확인란을 선택합니다.
인터페이스	효과적인 인터페이스를 지정합니다.
유휴 시간 제한	유휴 시간 제한을 지정합니다. 지정된 기간(유휴 시간 제한) 동안 비활성 상태가 지속되면 클라이언트의 연결이 끊어지고 다시 인증받아야 합니다. 값 0은 클라이언트가 비활성 상태이더라도 임대된 인증 타임아웃까지 클라이언트가 항상 온라인 상태를 유지함을 의미합니다.
포털 인증 포트	포털 인증을 위한 서비스 포트를 입력합니다. 기본 설정은 8080입니다.

2) **인증 매개변수** 섹션에서 인증 페이지의 매개변수를 구성합니다.

인증 페이지	인증 페이지 유형을 선택합니다. **사용자 지정**: 기본 제공 웹 서버를 사용하여 배경 사진, 환영 정보 및 저작권 정보를 지정하여 인증 페이지를 사용자 지정할 수 있습니다. **외부 링크**: 외부 링크를 인증 페이지로 지정하여 외부 페이지를 사용할 수 있습니다.
배경 그림	**업로드** 버튼을 클릭하여 사용자 지정 인증 페이지의 배경 사진으로 로컬 이미지를 선택합니다.
환영 정보	사용자 지정 인증 페이지에 표시할 환영 정보를 지정합니다.
저작권	사용자 지정 인증 페이지에 표시할 저작권 정보를 지정합니다.
페이지 미리보기	**로그인 페이지 미리 보기** 버튼을 클릭하면 사용자 지정한 인증 페이지를 미리 볼 수 있습니다.
인증 URL	인증 페이지를 '외부 링크'로 선택한 경우 인증 페이지의 URL을 지정합니다. 클라이언트가 인증을 시작할 때 브라우저가 이 URL로 리디렉션됩니다.
성공 리디렉션 URL	인증 페이지를 '외부 링크'로 선택한 경우 성공 리디렉션 URL을 지정합니다. 인증이 성공하면 브라우저가 이 URL로 리디렉션됩니다.
리디렉션 실패	URL인증 페이지를 '외부 링크'로 선택한 경우 리디렉션 실패 URL을 지정합니다. 인증에 실패하면 브라우저가 이 URL로 리디렉션됩니다.

참고:

웹 서버가 LAN에 배포되지 않은 경우 인증에 성공하기 전에 클라이언트가 외부 웹 서버에 액세스할 수 있도록 게스트 리소스 항목을 만들어야 합니다. 게스트 리소스를 구성하려면 게스트 리소스 구성으로 이동합니다.

3) 외부 Radius 서버를 지정하고 해당 매개변수를 구성한 다음 **저장을** 클릭합니다.

인증 유형	인증 유형을 반경 인증으로 선택합니다.
기본 반경 서버	기본 Radius 서버의 IP 주소를 입력합니다.
보조 반경 서버	(선택 사항) 보조 Radius 서버의 IP 주소를 입력합니다. 기본 서버가 다운되면 보조 서버가 작동합니다.
인증 포트	Radius 인증을 위한 서비스 포트를 입력합니다. 기본값은 1812입니다.
인증된 공유 키	인증된 공유 키를 지정합니다. 이 키는 Radius 서버에 구성된 것과 동일해야 합니다.
재시도 횟수	인증에 실패한 후 라우터가 인증 요청 전송을 다시 시도할 횟수를 지정합니다.
시간 초과 간격	반경 서버가 응답하기 전까지 클라이언트가 대기할 수 있는 시간 초과 간격을 지정합니다.
인증 방법	인증 프로토콜을 PAP 또는 CHAP로 지정합니다.

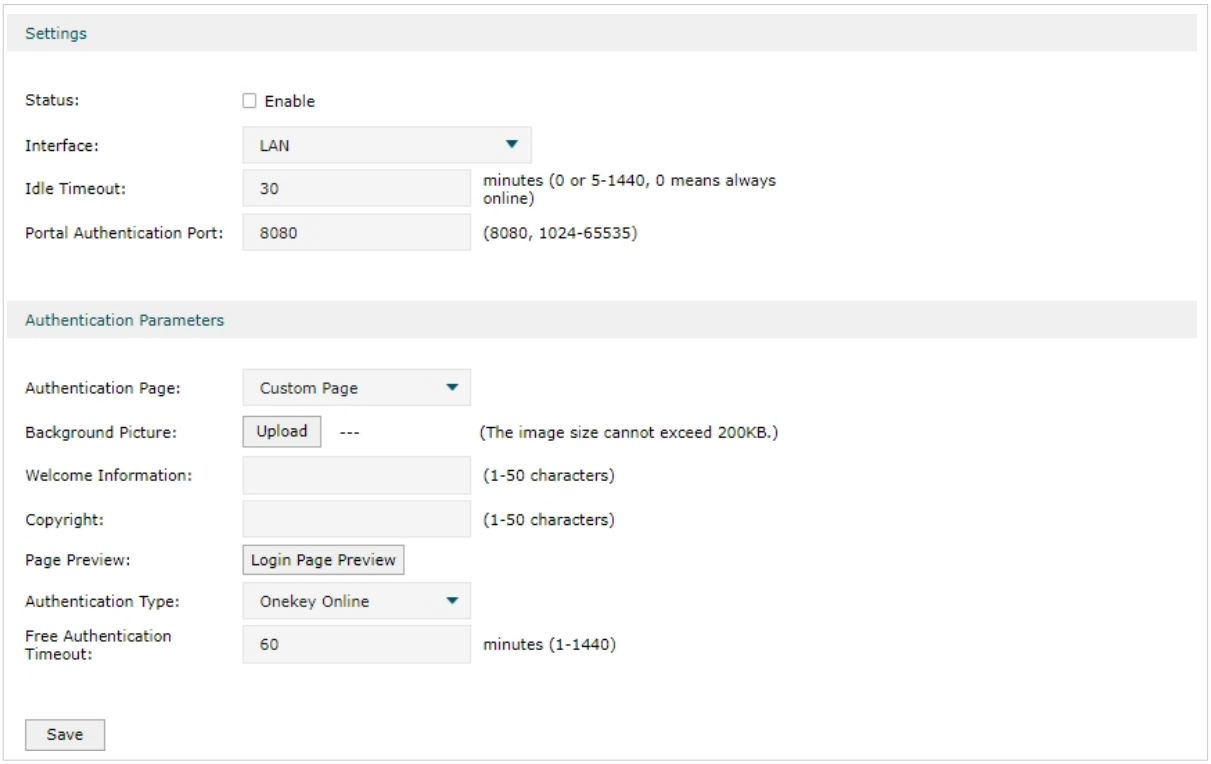
4 원키 온라인 구성

원키 온라인 인증에서 사용자는 인증 페이지에서 "원키 온라인" 버튼을 클릭하기만 하면 인터넷에 액세스할 수 있습니다. 사용자 이름과 비밀번호는 필요하지 않습니다.

4.1 인증 페이지 구성하기

인증 > **인증 설정** > **웹 인증** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 4-1 웹 인증 구성하기



원키 온라인 인증을 구성하려면 다음 단계를 따르세요:

1) **설정** 섹션에서 인증 상태를 활성화하고 유휴 시간 제한 및 포털 인증 포트를 구성합니다.

상태	포털 인증을 사용하려면 확인란을 선택합니다.
인터페이스	효과적인 인터페이스를 지정합니다.
유휴 시간 제한	유휴 시간 제한을 지정합니다. 지정된 기간(유휴 시간 제한) 동안 비활성 상태가 지속되면 클라이언트의 연결이 끊어지고 다시 인증받아야 합니다. 값 0은 클라이언트가 비활성 상태이더라도 임대된 인증 타임아웃까지 클라이언트가 항상 온라인 상태를 유

지함을 의미합니다.

포털 인증 포트	포털 인증을 위한 서비스 포트를 입력합니다. 기본 설정은 8080입니다.

2) **인증 매개변수** 섹션에서 인증 페이지의 매개변수를 구성하고 인증 유형을 선택한 다음 **저장을** 클릭합니다.

인증 페이지	인증 페이지 유형을 사용자 지정 페이지로 선택합니다. 참고: 원키 온라인에서는 외부 링크를 사용할 수 없습니다.
배경 그림	**업로드** 버튼을 클릭하여 사용자 지정 인증 페이지의 배경 사진으로 로컬 이미지를 선택합니다.
환영 정보	사용자 지정 인증 페이지에 표시할 환영 정보를 지정합니다.
저작권	사용자 지정 인증 페이지에 표시할 저작권 정보를 지정합니다.
페이지 미리보기	**로그인 페이지 미리 보기** 버튼을 클릭하면 사용자 지정한 인증 페이지를 미리 볼 수 있습니다.
인증 유형	인증 유형을 원키 온라인으로 선택합니다.
무료 인증 시간 초과	원키 온라인의 무료 기간을 지정합니다. 무료 기간이 만료되면 사용자는 인증 페이지에서 "원키 온라인" 버튼을 클릭하여 인터넷에 계속 접속할 수 있습니다.

5 게스트 리소스 구성

게스트 리소스는 포털 인증을 통과하기 전에 사용자에게 제공되는 제한된 네트워크 리소스입니다.

게스트 리소스는 두 가지 방법으로 구성할 수 있습니다:

- 5개의 튜플 유형

IP 주소, MAC 주소, VLAN ID, 서비스 포트 및 프로토콜의 설정에 따라 클라이언트와 클라이언트가 방문할 수 있는 네트워크 리소스를 지정합니다. 사용 가능한 네트워크 리소스의 IP 주소와 서비스 포트를 이미 알고 있는 경우 5개 튜플 유형을 선택하는 것이 좋습니다.

- URL 유형

URL, IP 주소, MAC 주소 및 서비스 포트의 설정에 따라 클라이언트와 클라이언트가 방문할 수 있는 네트워크 리소스를 지정합니다. 무료 네트워크 리소스의 URL을 이미 알고 있는 경우 URL 유형을 선택하는 것이 좋습니다.

참고:

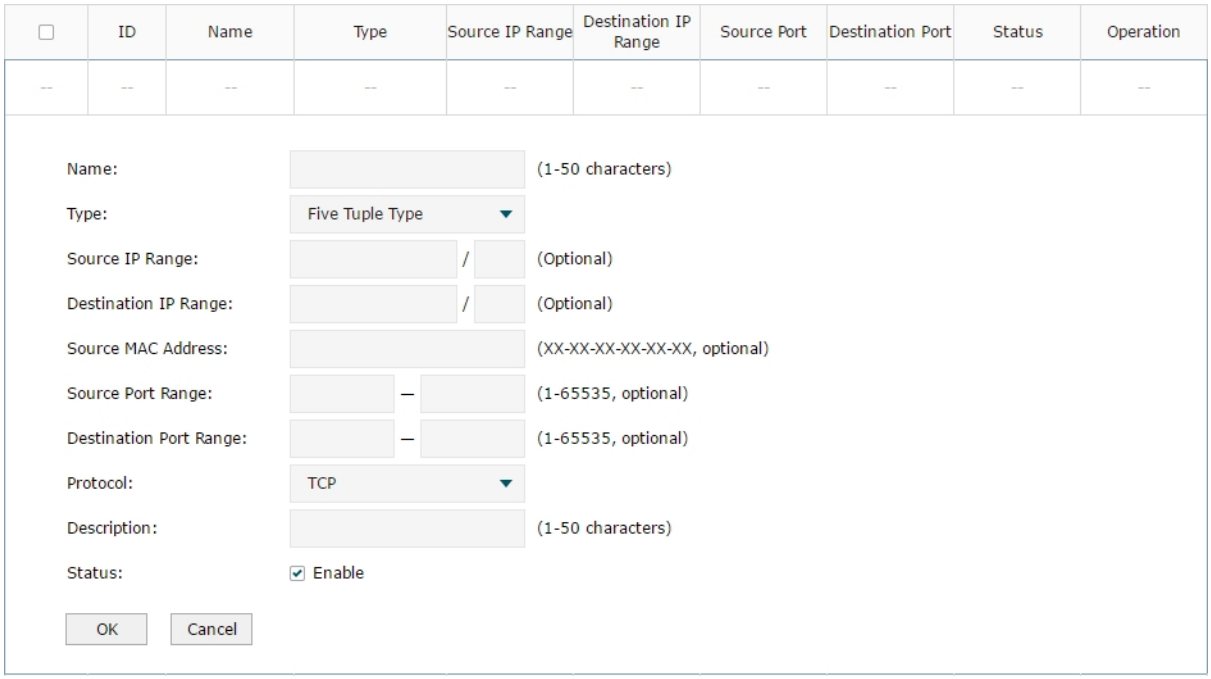
기본적으로 게스트 리소스 테이블은 비어 있으며, 이는 모든 클라이언트가 포털 인증을 통과하기 전에는 네트워크 리소스를 방문할 수 없음을 의미합니다.

5.1 5가지 튜플 유형 구성

인증 > **인증 설정** > **게스트 리소스** 메뉴를 선택하고 다음을 클릭합니다.

추가를 클릭하면 다음 페이지가 로드됩니다.

그림 5-1 5개의 튜플 유형 구성하기



IP 주소, MAC 주소 및 서비스 포트를 구성하여 클라이언트와 클라이언트가 방문할 수 있는 네트워크 리소스를 지정한 다음 **확인을** 클릭합니다.

이름	게스트 리소스 항목의 이름을 입력합니다.
유형	게스트 리소스 유형을 5개의 튜플 유형으로 선택합니다.
소스 IP 범위	네트워크 주소와 서브넷 마스크 비트를 입력하여 클라이언트의 IP 범위를 지정합니다. 지정된 클라이언트만 게스트 리소스를 방문할 수 있습니다.
대상 IP 범위	네트워크 주소와 서브넷 마스크 비트를 입력하여 게스트 리소스를 제공하는 서버의 IP 범위를 지정합니다.
소스 MAC 주소	클라이언트의 MAC 주소를 입력합니다.
소스 포트 범위	소스 서비스 포트 범위를 입력합니다.
목적지 포트 범위	대상 서비스 포트 범위를 입력합니다.
설명	게스트 리소스 항목에 대한 간단한 설명을 입력하여 검색 및 관리를 쉽게 할 수 있도록 합니다.
프로토콜	게스트 리소스에 대한 프로토콜을 TCP 또는 UDP로 지정합니다.

상태	게스트 리소스 항목을 활성화하려면 확인란을 선택합니다.

참고:

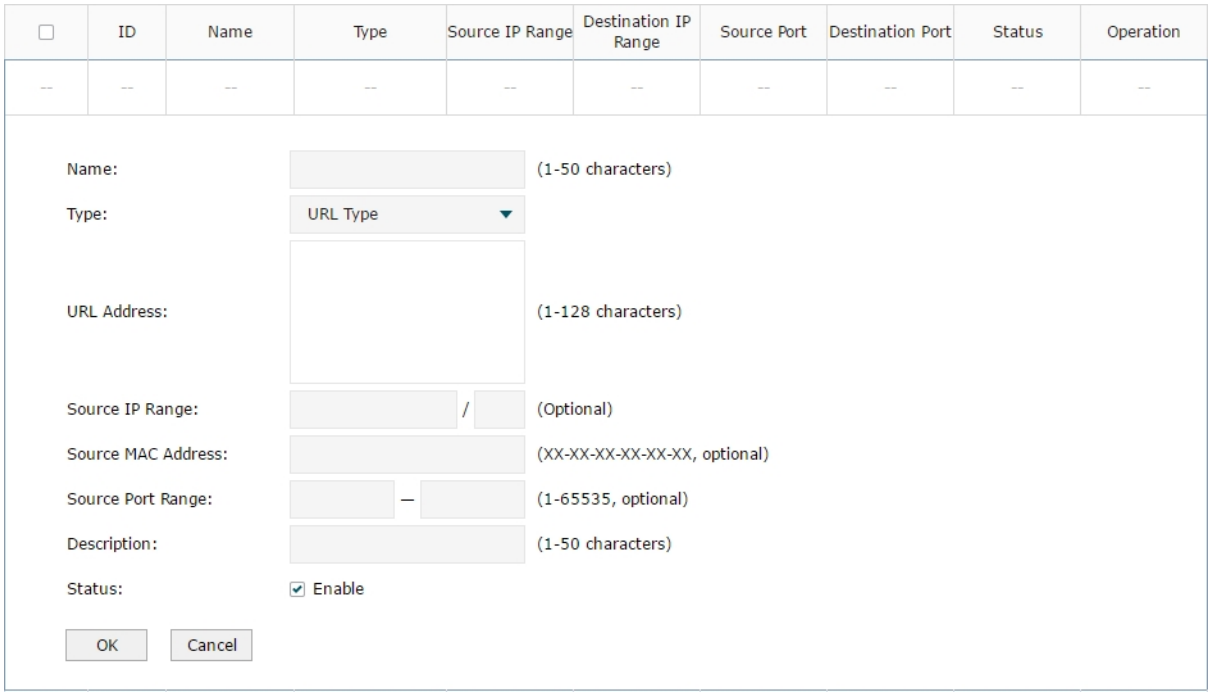
게스트 리소스 항목에서 일부 매개변수가 비어 있으면 라우터가 해당 매개변수를 제한하지 않는다는 의미입니다. 예를 들어, 소스 IP 범위가 비어 있으면 모든 클라이언트가 지정된 게스트 리소스를 방문할 수 있다는 뜻입니다.

5.2 URL 유형 구성

인증 > **인증 설정** > **게스트 리소스** 메뉴를 선택하고 다음을 클릭합니다.

추가를 클릭하면 다음 페이지가 로드됩니다.

그림 5-1 URL 구성하기



네트워크 리소스의 URL과 클라이언트의 매개변수를 구성하여 클라이언트와 클라이언트가 방문할 수 있는 네트워크 리소스를 지정한 다음 **확인을** 클릭합니다.

이름	게스트 리소스 항목의 이름을 입력합니다.
유형	게스트 리소스 유형을 URL 유형으로 선택합니다.
URL 주소	무료로 방문할 수 있는 네트워크 리소스의 URL 주소 또는 IP 주소를 입력합니다.
소스 IP 범위	네트워크 주소와 서브넷 마스크 비트를 입력하여 클라이언트의 IP 범위를 구성합니다.

소스 MAC 주소	클라이언트의 MAC 주소를 입력합니다.
소스 포트 범위	소스 서비스 포트 범위를 입력합니다.

설명	게스트 리소스 항목에 대한 간단한 설명을 입력하여 검색 및 관리를 쉽게 할 수 있도록 합니다.
상태	게스트 리소스 항목을 활성화하려면 확인란을 선택합니다.

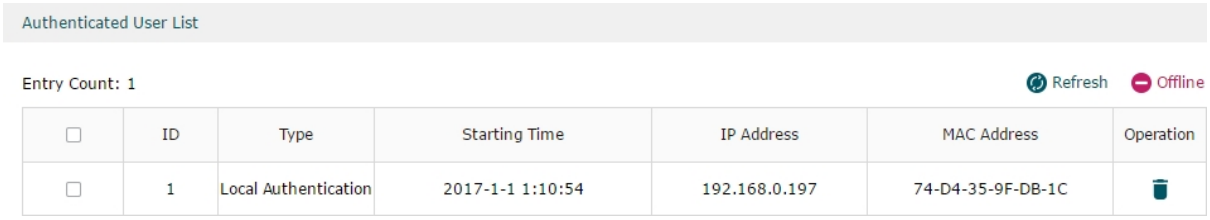
참고:

게스트 리소스 항목에서 일부 매개변수가 비어 있으면 라우터가 해당 매개변수를 제한하지 않는다는 의미입니다. 예를 들어, 소스 IP 범위가 비어 있으면 모든 클라이언트가 지정된 게스트 리소스를 방문할 수 있다는 뜻입니다.

6 Vie 인증 상태 확인

인증 > 인증 상태 > 인증 상태 메뉴를 **선 택 하 면** 다음 페이지가 로드됩니다.

그림 6-1 인증 상태 보기



여기에서 포털 인증을 통과한 클라이언트를 볼 수 있습니다.

유형	클라이언트의 인증 유형을 표시합니다. 시작 시간
	인증 시작 시간을 표시합니다. IP 주소 클라
이언트의 IP 주소를 표시합니다.	
MAC 주소	클라이언트의 MAC 주소를 표시합니다.

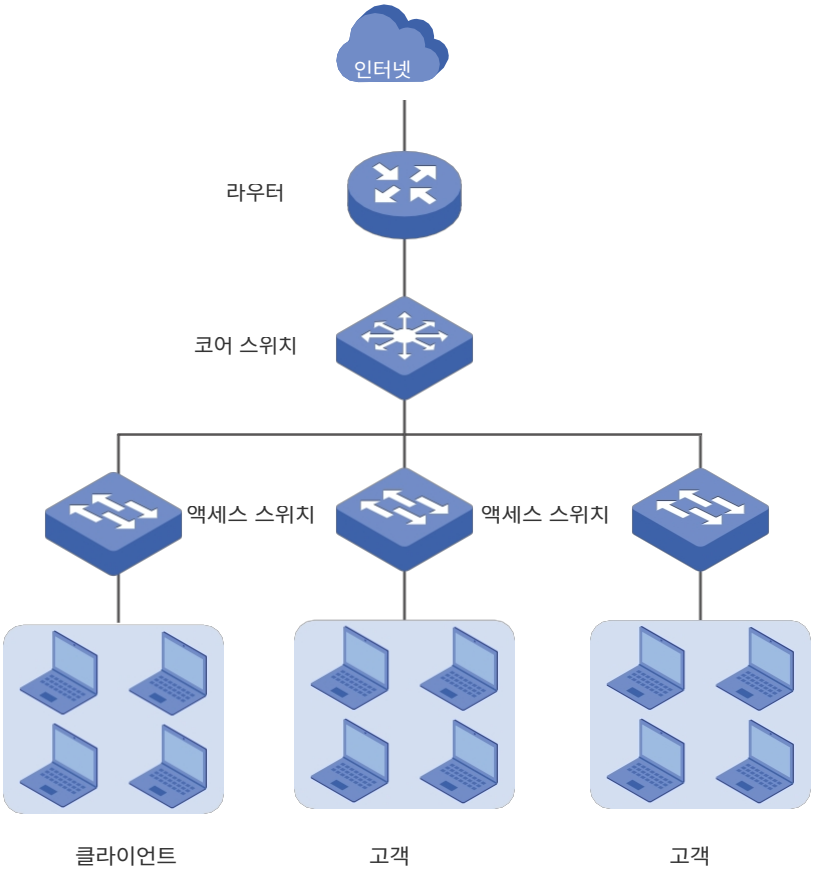
7 구성 예시

여기서는 로컬 인증의 적용을 예로 들어 보겠습니다.

7.1 네트워크 요구 사항

호텔은 투숙객에게 인터넷 서비스를 제공하고 호텔 광고를 푸시해야 합니다. 네트워크 보안을 위해 승인된 게스트만 인터넷에 액세스할 수 있습니다.

그림 7-1 네트워크 토폴로지



7.2 구성 체계

호텔에 외부 웹 서버나 인증 서버가 없는 경우, 이 요건을 충족하기 위해 로컬 인증을 선택하는 것이 좋습니다.

- 게스트의 인터넷 액세스를 제어하려면 게스트에 대한 로컬 사용자 계정을 만들면 됩니다. 게

스트는 자신에게 할당된 계정을 사용하여 인증을 받은 후 인터넷을 사용할 수 있습니다. 다른 사람들은 인증 계정이 없으면 호텔 네트워크를 통해 인터넷에 접속할 수 없습니다.

- 호텔 광고를 푸시하려면 배경 사진과 환영 정보를 설정하여 인증 페이지를 사용자 지정하기만 하면 됩니다.

7.3 구성 절차

1) 포털 인증을 사용하도록 설정하고 인증 유형을 로컬 인증으로 선택한 다음 인증 페이지를 사용자 지정합니다.

2) 게스트의 인증 계정을 만듭니다.

7.3.1 인증 페이지 구성하기

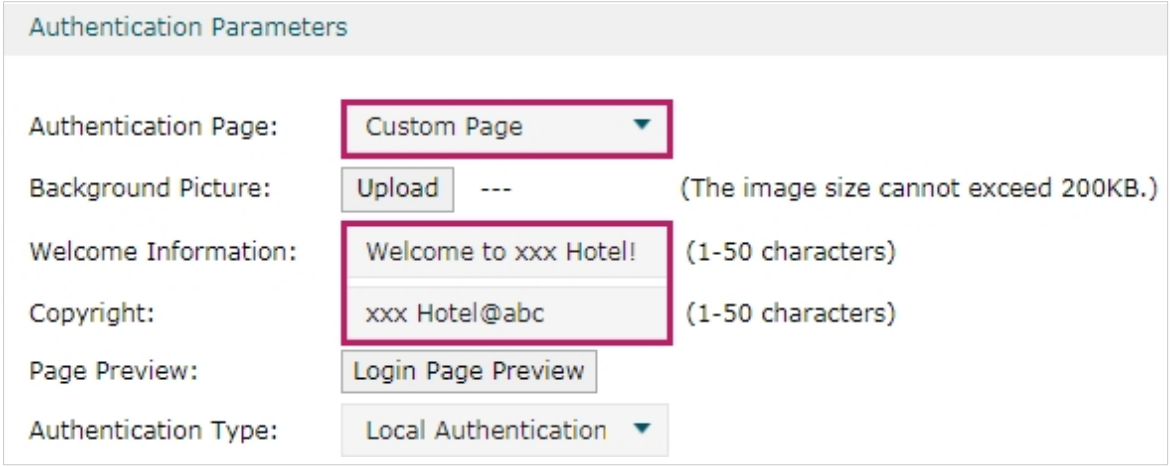
인증 > 인증 설정 > 웹 인증 메뉴를 **선택하면** 다음 페이지가 로드됩니다.

1) 포털 인증을 사용하도록 설정하고 유휴 시간 초과 및 포털 인증 포트를 기본 설정으로 유지합니다.

그림 7-2 포털 인증 활성화

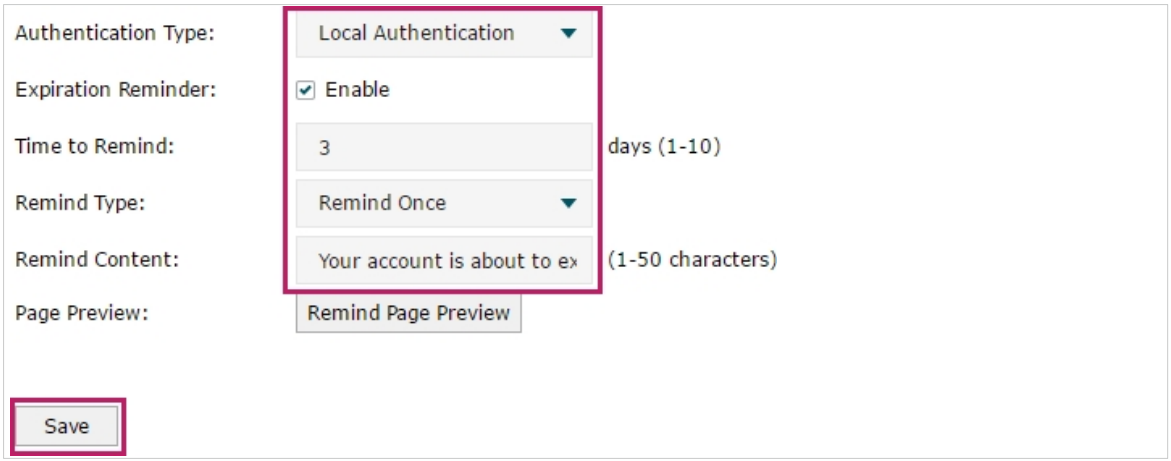
2) 인증 페이지를 사용자 지정 페이지로 선택하고 인증 페이지의 배경 사진으로 호텔 사진을 선택한 다음 환영 정보 및 저작권을 지정합니다.

그림 7-3 인증 페이지 사용자 지정



3) 인증 유형을 로컬 인증으로 선택하고 만료 알림의 매개변수를 구성합니다. 그런 다음 **저장을** 클릭합니다.

그림 7-4 인증 유형 및 만료 알림 구성하기

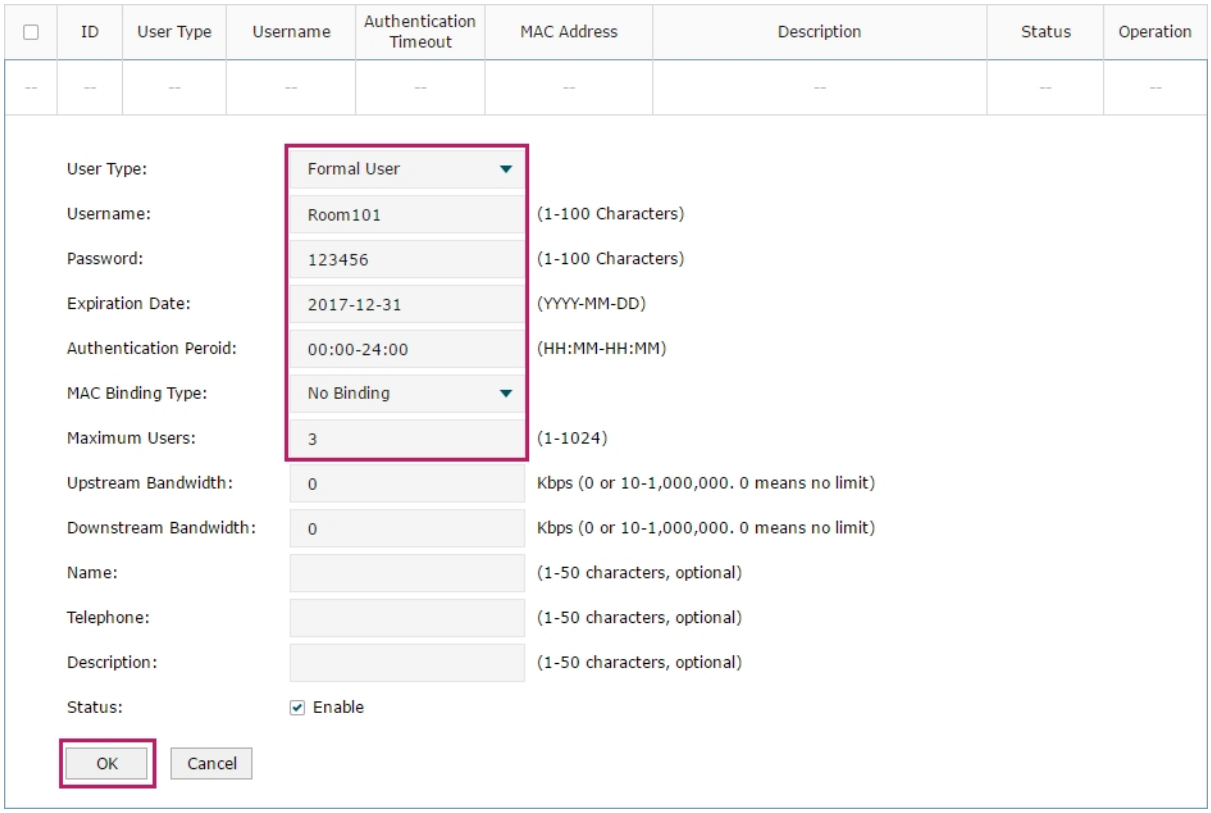


7.3.2 게스트의 인증 계정 구성하기

인증 > 사용자 관리 > 사용자 관리 메뉴를 선택하면 다음 페이지가 로드됩니다.

여기서는 공식 사용자 계정의 구성을 예로 들어 보겠습니다. 101호 객실의 게스트를 위한 계정을 만듭니다. 사용자 이름은 Room101, 비밀번호는 123456이며, 최대 세 명의 게스트가 이 계정을 사용하여 인증할 수 있습니다. 그런 다음 **확인을** 클릭합니다.

그림 7-5 게스트용 계정 구성하기



모든 구성이 완료되면 게스트는 인증에 성공한 후 해당 계정을 사용하여 인증하고 인터넷에 액세

스할 수 있습니다.

파트 12

서비스 관리

챕터

7. DNS 프록시DNS 프록시

1 Ser vices

1.1 개요

서비스 모듈은 편리한 네트워크 서비스를 제공하기 위해 DDNS(동적 DNS)와 UPnP(범용 플러그 앤 플레이)의 두 가지 기능을 통합합니다.

1.2 지원 기능

동적 DNS

오늘날 ISP는 사용자에게 공인 IP 주소를 할당하기 위해 PPPoE 및 DHCP와 같은 네트워크 프로토콜을 널리 사용하고 있습니다. 이러한 프로토콜을 사용하면 사용자의 공인 IP 주소가 동적으로 변경될 수 있습니다. DDNS는 고정 도메인 이름을 사용하여 다양한 공인 IP 주소를 가진 네트워크에 액세스할 수 있도록 하는 인터넷 서비스입니다. 즉, 인터넷 호스트가 사용자의 네트워크에 더 쉽게 액세스할 수 있습니다.

UPnP

네트워킹과 고급 컴퓨팅 기술의 발달로 네트워크에 더 많은 수의 장치가 등장했습니다. UPnP는 이러한 네트워크 장치 간의 통신 문제를 해결하기 위해 고안되었습니다. UPnP 기능을 사용하면 추가 구성 없이도 장치가 서로를 동적으로 검색하고 통신할 수 있습니다. 예를 들어, 포트를 열지 않고도 P2P 소프트웨어를 다운로드할 수 있습니다.

mDNS

mDNS(멀티캐스트 DNS) 리피터는 mDNS 요청/응답 패킷이 여러 네트워크 세그먼트에 분산되도록 도와줍니다. 이 기능을 사용하면 mDNS 프로토콜을 사용하여 게시된 서비스를 여러 네트워크 세그먼트에서 검색할 수 있습니다.

재부팅 일정

재부팅 일정에서는 필요에 따라 연결된 장치를 주기적으로 재부팅하도록 일정을 설정할 수 있습

니다. 여러 항목을 생성하여 재부팅 일정을 유연하게 구성할 수 있습니다.

DNS 프록시

DNS 프록시는 LAN 측 클라이언트에 DNS 쿼리 서비스를 제공합니다. LAN 측 클라이언트의 DNS 요청을 선택한 업스트림 DNS 서버로 전달하고 그에 따라 DNS 응답을 전달합니다.

2 D ynamic DNS 구성

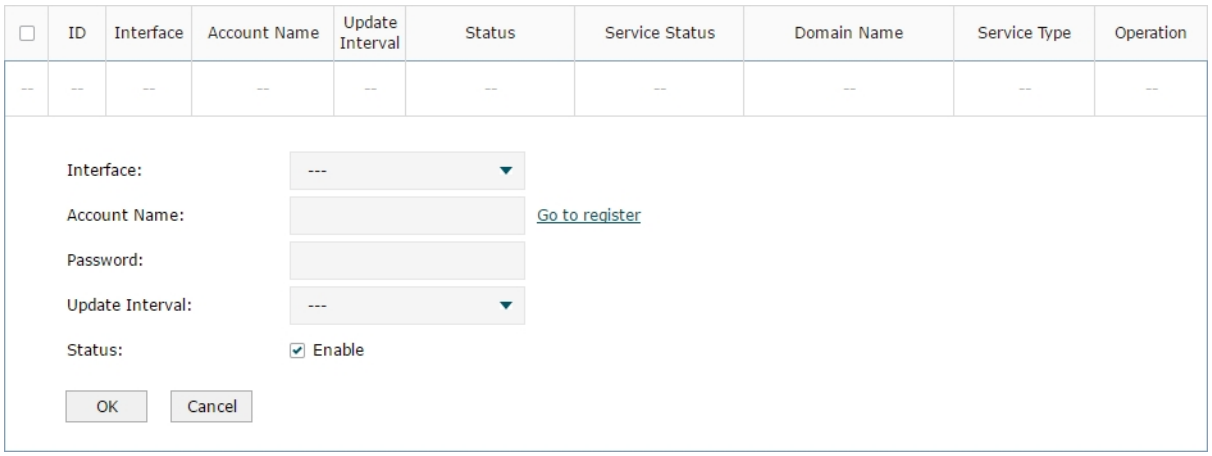
동적 DNS 구성을 사용하면 가능합니다:

- Peanuthull DDNS 구성 및 보기
- Comexe DDNS 구성 및 보기
- DynDNS 구성 및 보기
- NO-IP DDNS 구성 및 보기
- 사용자 지정 DDNS

2.1 Peanuthull DDNS 구성 및 보기

서비스 > **동적 DNS** > **Peanuthull** 메뉴를 선택하고 **추가를** 클릭하여 다음 페이지를 로드합니다.

그림 2-1 Peanuthull DDNS 구성하기



다음 단계에 따라 Peanuthull DDNS를 구성합니다.

1) **등록하려면** 이동을 클릭하여 Peanuthull의 공식 웹사이트를 방문하고 계정과 도메인 이름을 등록합니다.

2) 다음 매개변수를 구성하고 **확인을** 클릭합니다.

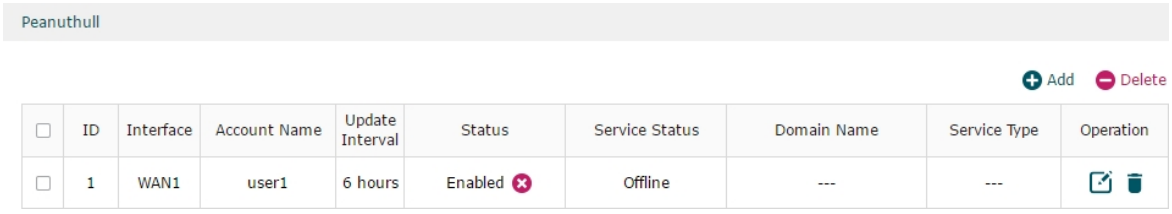
인터페이스	DDNS 서비스의 인터페이스를 선택합니다.
계정 이름DDNS 계정의 계정 이름을 입력합니다.	**등록하러 가기 버튼을** 클릭하여 Peanuthull 공식 웹사이트로 이동하여 계정을 등록할 수 있습니다.

비밀번호	DDNS 계정의 비밀번호를 입력합니다.
업데이트 간격	장치가 등록된 도메인 이름에 대해 IP 주소를 동적으로 업데이트하는 업데이트 간격을 지정합니다.

상태	DDNS 서비스를 사용하려면 확인란을 선택합니다.

3) DDNS 상태를 확인합니다.

그림 2-2 Peanuthull DDNS 상태 보기

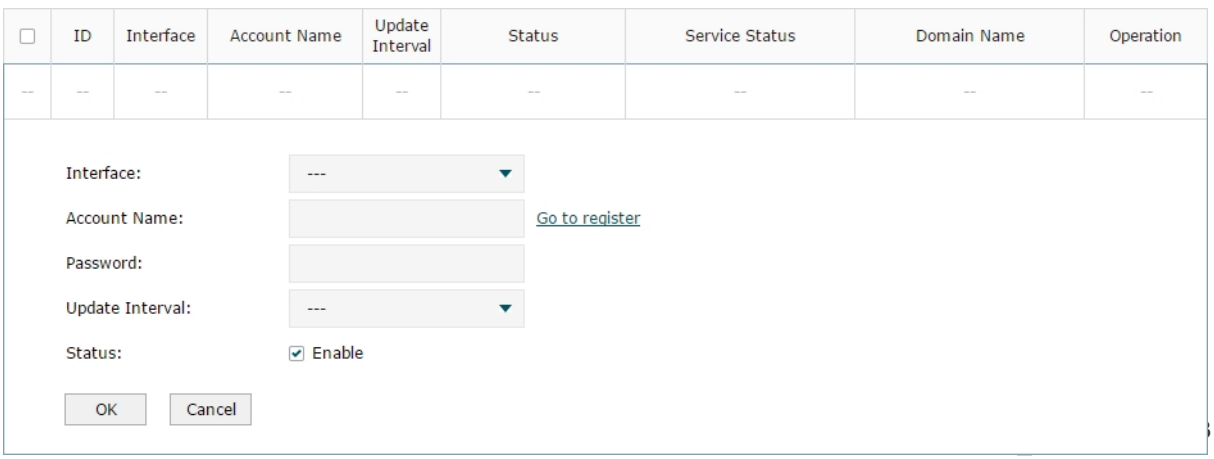


상태	해당 DDNS 서비스가 활성화되어 있는지 여부를 표시합니다. 서비스 상태
	DDNS 서비스의 현재 상태를 표시합니다. **오프라인:** DDNS 서비스가 오프라인 상태입니다. **연결 중입니다:** DDNS 클라이언트가 서버에 연결 중입니다. **온라인:** DDNS가 정상적으로 작동합니다. **잘못된 계정 이름 또는 비밀번호:** 계정 이름 또는 비밀번호가 올바르지 않습니다.
도메인 이름	DDNS 서버에서 가져온 도메인 이름을 표시합니다.
서비스 유형	프로페셔널 서비스 및 스탠다드 서비스를 포함한 DDNS 서비스 유형을 표시합니다.

2.2 Comexe DDNS 구성 및 보기

서비스 > **동적 DNS** > **Comexe** 메뉴를 선택하고 **추가를** 클릭하여 다음 페이지를 로드합니다.

그림 2-3 Comexe DDNS 구성



다음 단계에 따라 Comexe DDNS를 구성합니다.

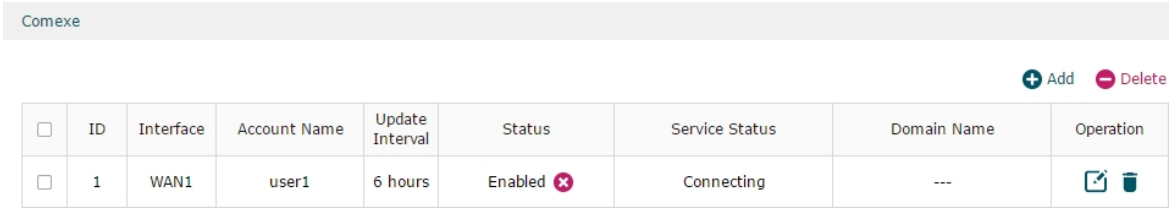
1) **등록하려면 이동을** 클릭하여 Comexe의 공식 웹사이트를 방문하고 계정과 도메인 이름을 등록합니다.

2) 다음 매개변수를 구성하고 **확인을** 클릭합니다.

인터페이스	DDNS 서비스의 인터페이스를 선택합니다.
계정 이름	DDNS 계정의 계정 이름을 입력합니다. **등록하러 가기** 버튼을 클릭하여 Comexe의 공식 웹사이트로 이동하여 계정을 등록할 수 있습니다.
비밀번호	DDNS 계정의 비밀번호를 입력합니다.
업데이트 간격	장치가 등록된 도메인 이름에 대한 IP 주소를 동적으로 업데이트하는 업데이트 간격을 지정합니다.
상태	DDNS 서비스를 사용하려면 확인란을 선택합니다.

3) DDNS 상태를 확인합니다.

그림 2-4 Comexe DDNS 상태 보기

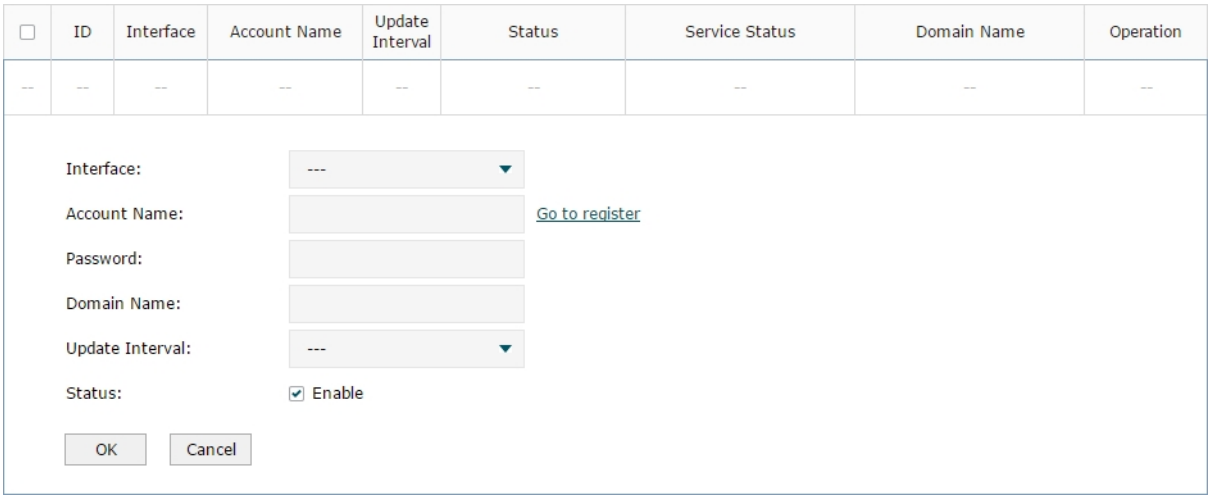


상태	해당 DDNS 서비스가 활성화되어 있는지 여부를 표시합니다. 서비
스 상태	DDNS 서비스의 현재 상태를 표시합니다. **오프라인:** DDNS 서비스가 오프라인 상태입니다. **연결 중입니다:** DDNS 클라이언트가 서버에 연결 중입니다. **온라인:** DDNS가 정상적으로 작동합니다. **잘못된 계정 이름 또는 비밀번호:** 계정 이름 또는 비밀번호가 올바르지 않습니다.
도메인 이름	DDNS 서버에서 가져온 도메인 이름을 표시합니다.

2.3 DynDNS 구성 및 보기

서비스 > **동적 DNS** > **DynDNS** 메뉴를 선택하고 **추가를** 클릭하여 다음 페이지를 로드합니다.

그림 2-5 DynDNS 구성



다음 단계에 따라 DynDNS를 구성합니다.

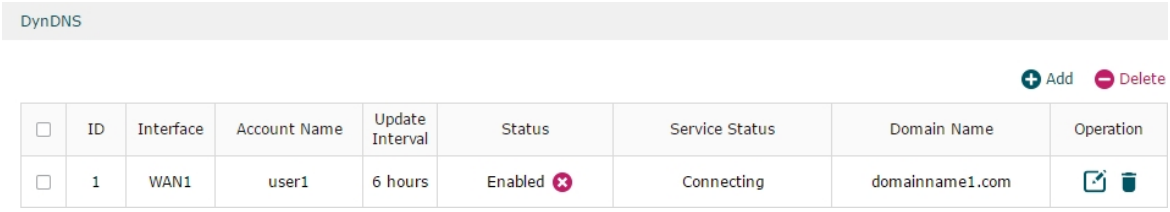
1) 등록을 클릭하여 DynDNS의 공식 웹사이트를 방문하고 계정과 도메인 이름을 등록합니다.

2) 다음 매개변수를 구성하고 **확인을** 클릭합니다.

인터페이스	DDNS 서비스의 인터페이스를 선택합니다.
계정 이름	DDNS 계정의 계정 이름을 입력합니다. **등록하러 가기** 버튼을 클릭하여 DynDNS 공식 웹사이트로 이동하여 계정을 등록할 수 있습니다.
비밀번호	DDNS 계정의 비밀번호를 입력합니다.
도메인 이름	DDNS 서비스 제공업체에 등록한 도메인 이름을 지정합니다.
업데이트 간격	장치가 등록된 도메인 이름에 대한 IP 주소를 동적으로 업데이트하는 업데이트 간격을 지정합니다.
상태	DDNS 서비스를 사용하려면 확인란을 선택합니다.

3) DDNS 상태를 확인합니다.

그림 2-6 DynDNS 상태 보기



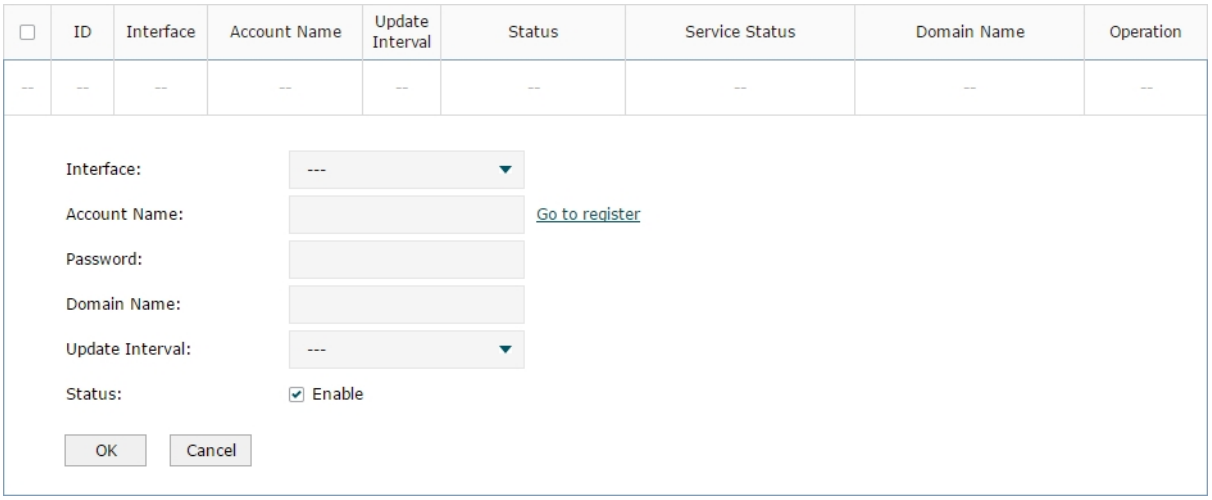
상태	해당 DDNS 서비스가 활성화되어 있는지 여부를 표시합니다.

서비스 상태	DDNS 서비스의 현재 상태를 표시합니다. **오프라인:** DDNS 서비스가 오프라인 상태입니다. **연결 중입니다:** DDNS 클라이언트가 서버에 연결 중입니다. **온라인:** DDNS가 정상적으로 작동합니다. **잘못된 계정 이름 또는 비밀번호:** 계정 이름 또는 비밀번호가 올바르지 않습니다. **잘못된 도메인 이름:** 도메인 이름이 올바르지 않습니다.
도메인 이름	DDNS 서버에서 가져온 도메인 이름을 표시합니다.

2.4 NO-IP DDNS 구성 및 보기

서비스 > **동적 DNS** > **NO-IP** 메뉴를 선택하고 추가를 클릭하여 다음 페이지를 로드합니다.

그림 2-7 NO-IP DDNS 보기



다음 단계에 따라 NO-IP DDNS를 구성합니다.

1) 등록하기를 클릭하여 NO-IP의 공식 웹사이트를 방문하여 계정과 도메인 이름을 등록합니다.

2) 다음 매개변수를 구성하고 **확인을** 클릭합니다.

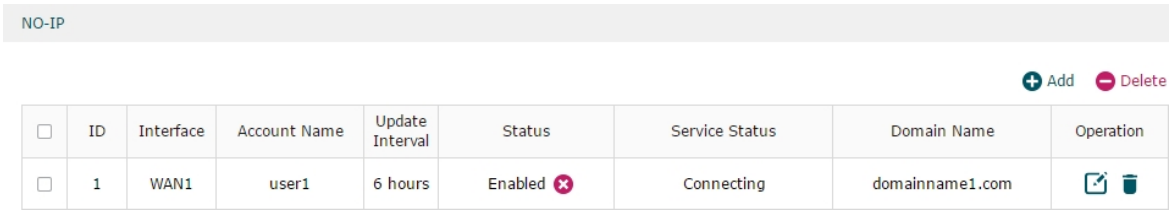
인터페이스	DDNS 서비스의 인터페이스를 선택합니다.
계정 이름	DDNS 계정의 계정 이름을 입력합니다. **등록하러 가기** 버튼을 클릭하여 NO-IP 공식 웹사이트로 이동하여 계정을 등록할 수 있습니다.

비밀번호	DDNS 계정의 비밀번호를 입력합니다.
도메인 이름	DDNS 서비스 제공업체에 등록한 도메인 이름을 지정합니다.

업데이트 간격	장치가 등록된 도메인 이름에 대한 IP 주소를 동적으로 업데이트하는 업데이트 간격을 지정합니다.
상태	DDNS 서비스를 사용하려면 확인란을 선택합니다.

3) DDNS 상태를 확인합니다.

그림 2-8 NO-IP DDNS 상태 보기



상태	해당 DDNS 서비스가 활성화되어 있는지 여부를 표시합니다. 서비스 상태
	DDNS 서비스의 현재 상태를 표시합니다. **오프라인:** DDNS 서비스가 오프라인 상태입니다. **연결 중입니다:** DDNS 클라이언트가 서버에 연결 중입니다. **온라인:** DDNS가 정상적으로 작동합니다. **잘못된 계정 이름 또는 비밀번호:** 계정 이름 또는 비밀번호가 올바르지 않습니다. **잘못된 도메인 이름:** 도메인 이름이 올바르지 않습니다.
도메인 이름	DDNS 서버에서 가져온 도메인 이름을 표시합니다.

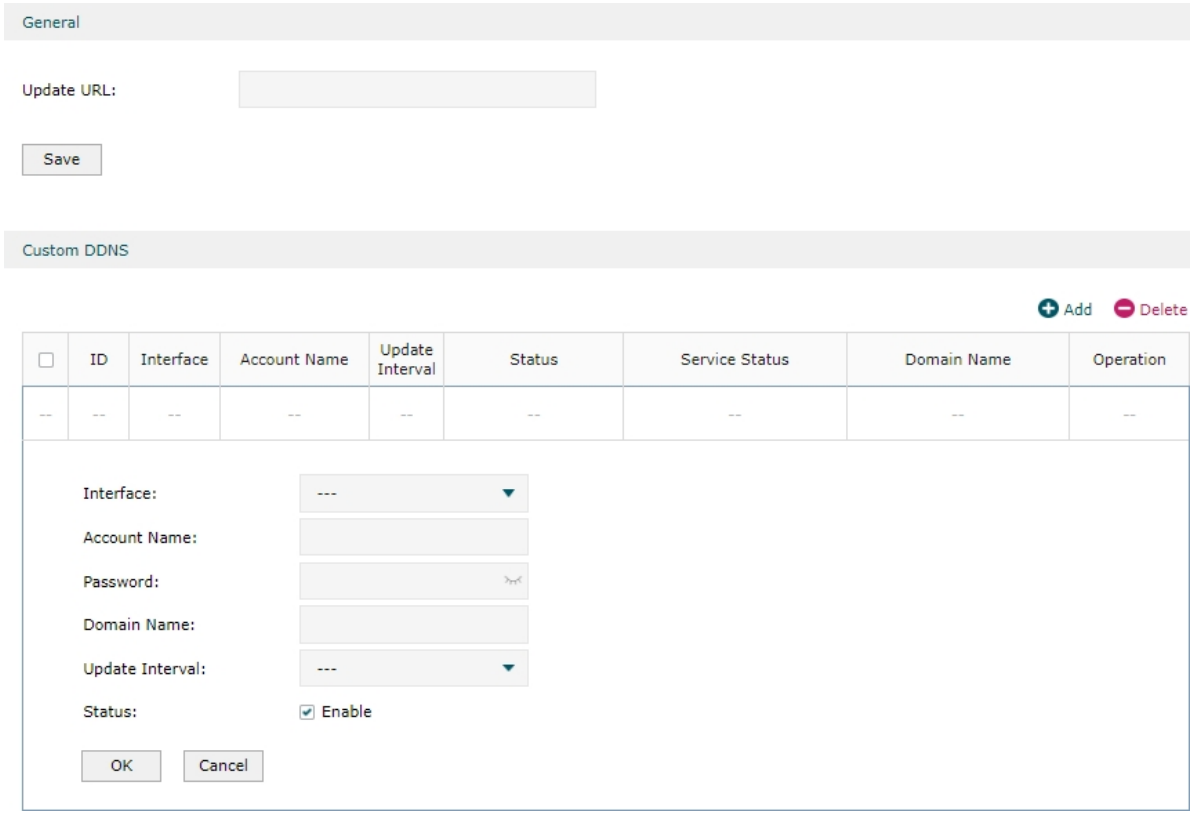
2.5 사용자 지정 DDNS

라우터에는 일반적인 DDNS 서비스 제공업체가 나열됩니다. 등록한 서비스 공급업체가 목록에 없는 경우 사용자 지정 DDNS 항목을 추가할 수 있습니다.

1) 서비스 제공업체에 등록하고 사용자 아이디, 비밀번호, 도메인 이름을 받습니다.

2) **서비스 > 동적 DNS > 사용자 지정 DDNS** 메뉴를 선택하고 추가를 클릭하여 다음 페이지를 로드합니다.

그림 2-9 사용자 지정 DDNS



3) 다음 매개변수를 구성하고 **확인을** 클릭합니다.

업데이트	URLDDNS 서비스 제공업체에서 제공한 URL을 http://[USERNAME]:[PASSWORD]@api.cp.easydns.com/dyn/tomato.php?hostname=[DOMAIN]&myip=[IP] 형식으로 입력합니다. 라우터가 자동으로 사용자 정보를 서비스 제공업체에 업데이트합니다.
인터페이스	DDNS 항목이 적용되는 WAN 포트를 선택합니다. 계정 이
름	서비스 공급업체의 계정 이름을 입력합니다.
비밀번호	서비스 제공업체의 비밀번호를 입력합니다.
도메인 이름	서비스 제공업체에서 제공한 도메인 이름을 입력합니다. 원격 사용자는 이 도메인 이름을 사용하여 WAN 포트를 통해 로컬 네트워크에 액세스할 수 있습니다.
업데이트 간격	DDNS 서비스의 WAN IP 주소 변경을 보고할 업데이트 간격을 지정합니다.

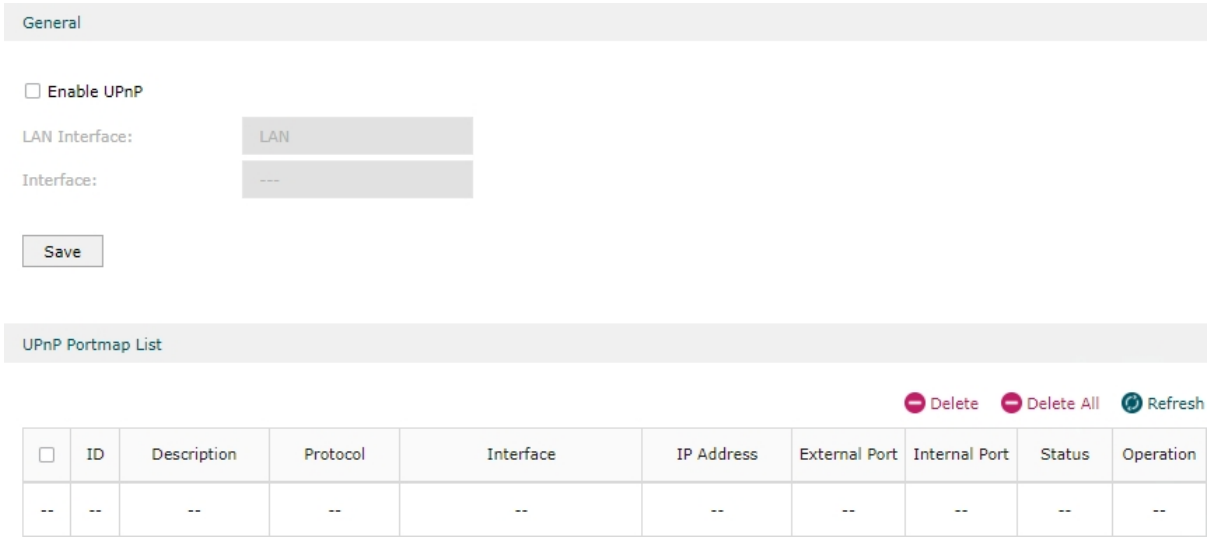
상태	항목을 활성화하려면 확인란을 클릭합니다.

3 UP nP 구성

UPnP(범용 플러그 앤 플레이)는 장치가 서로를 검색한 다음 통신을 위한 연결을 설정할 수 있는 네트워킹 프로토콜입니다. UPnP의 도움으로 장치 간, 특히 WAN에서 LAN으로의 원활한 연결을 실현하는 것이 편리합니다.

서비스 > **UPnP** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 3-1 UPnP 구성



다음 단계에 따라 UPnP를 구성합니다.

1) 확인란을 선택하면 **UPnP** 기능이 활성화됩니다.

2) 유효한 인터페이스를 지정합니다. 그런 다음 **저장을** 클릭합니다.

3) (선택 사항) **UPnP 포트맵 목록** 섹션에서 포트맵 목록을 확인합니다.

설명	UPnP 프로토콜을 사용하는 애플리케이션에 대한 설명을 표시합니
다. 프로토콜	UPnP 프로세스에 사용된 프로토콜 유형을 표시합니다. 인터페이스
	UPnP 프로세스에 사용된 인터페이스를 표시합니다.
IP 주소	로컬 호스트의 IP 주소를 표시합니다.
외부 포트	라우터에 의해 애플리케이션을 위해 열린 외부 포트를 표시합니다. 내부 포트 로

컬 호스트가 애플리케이션을 위해 열어둔 내부 포트를 표시합니다. 상태해당 UPnP 항목의 상태를 표

시합니다.

활성화됨: 매핑이 활성화됩니다.

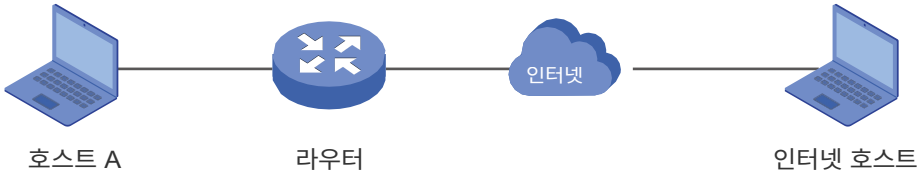
비활성화됨: 매핑이 비활성 상태입니다.

4 동적 DNS의 구성 예제

4.1 네트워크 요구 사항

호스트 A는 PPPoE 다이얼업 연결을 통해 ISP(인터넷 서비스 제공업체)로부터 인터넷 서비스를 받습니다. 사용자가 인터넷의 다른 호스트를 사용하여 라우터의 웹 관리 인터페이스를 방문하려고 합니다.

그림 4-1 네트워크 토폴로지



4.2 구성 체계

보안 관리를 위해 라우터를 관리하려는 인터넷 호스트는 라우터에서 허용해야 합니다. 원격 관리는 이러한 호스트의 IP 주소를 관리하는 데 사용됩니다.

사용자가 PPPoE를 사용하여 네트워크에 액세스하기 때문에 전화 접속 연결이 설정될 때마다 라우터의 공인 IP 주소가 변경될 수 있습니다. 라우터의 공인 IP 주소가 변경되면 DDNS 서비스는 DNS 서버가 현재 도메인 이름을 새 IP 주소에 다시 바인딩하도록 합니다. 즉, 사용자는 공용 IP 주소가 변경된 경우에도 항상 동일한 도메인 이름을 사용하여 라우터에 연결할 수 있습니다.

4.3 구성 절차

4.3.1 호스트의 IP 주소 지정

DDNS를 구성하기 전에 원격 관리를 위한 인터넷 호스트의 IP 주소를 지정해야 합니다. 자세한 내용은 **시스템 도구 > 관리자 설정 > 원격 관리** 페이지로 이동하세요.

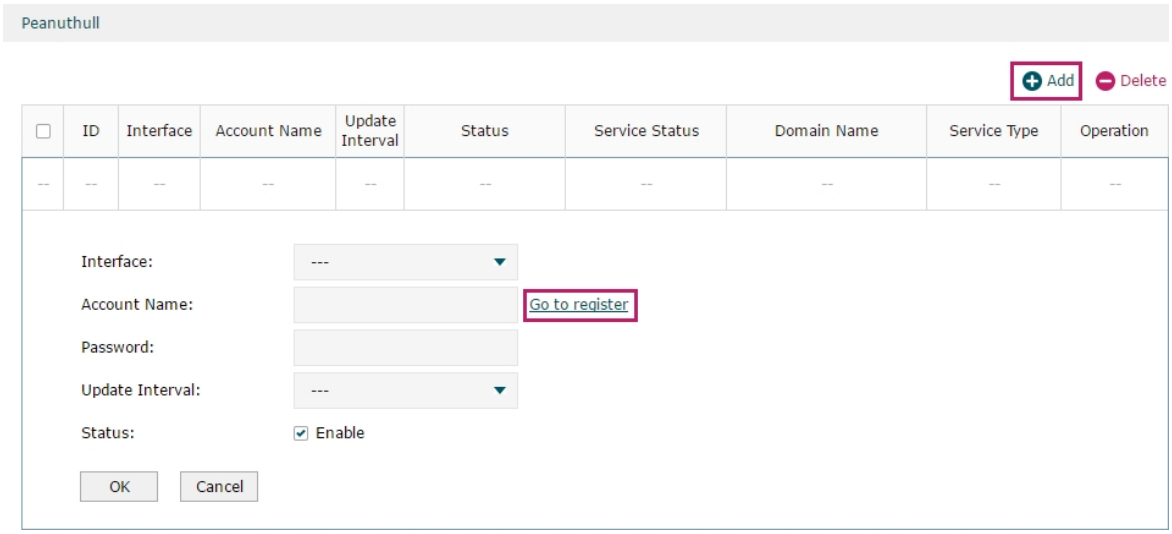
4.3.2 DDNS 기능 구성

라우터에서 지원하는 DDNS 서버는 4개이며, 여기서는 Peanuthull DNS를 예로 들어 설명합니다.

1) **서비스 > 동적 DNS > Peanuthull** 메뉴를 선택하고 **추가를** 클릭하면 다음 페이지가 로드됩니다.

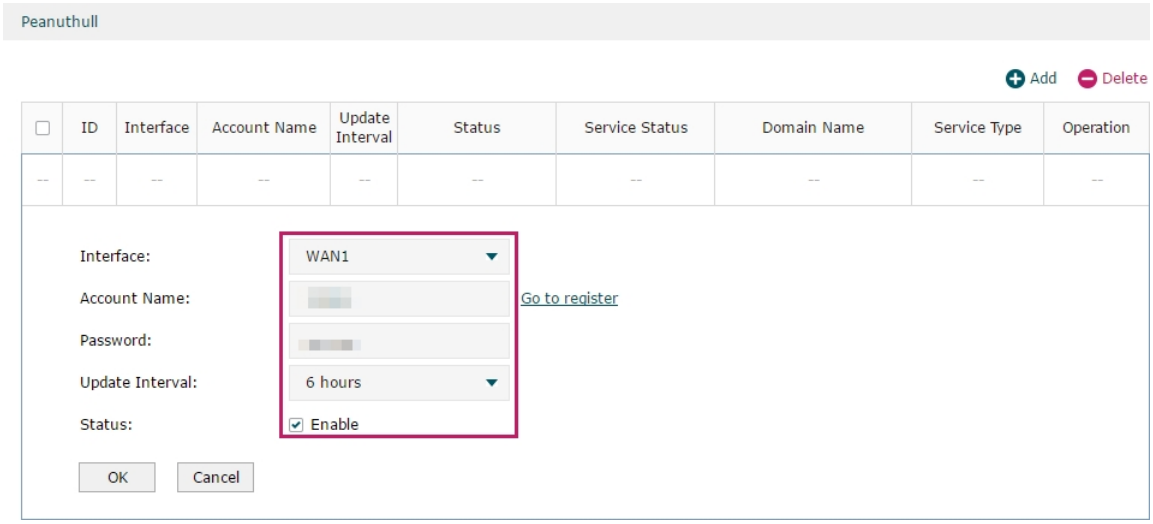
등록을 클릭하여 Peanuthull의 공식 웹사이트에 도메인 네임을 등록합니다.

그림 4-2 도메인 이름 등록하기



2) 인터페이스를 WAN1으로 설정하고 업데이트 간격을 6시간으로 설정한 다음 이전에 등록한 계정 이름과 비밀번호를 입력합니다. **확인을** 클릭합니다.

그림 4-3 Peanuthull DDNS 매개변수 지정하기

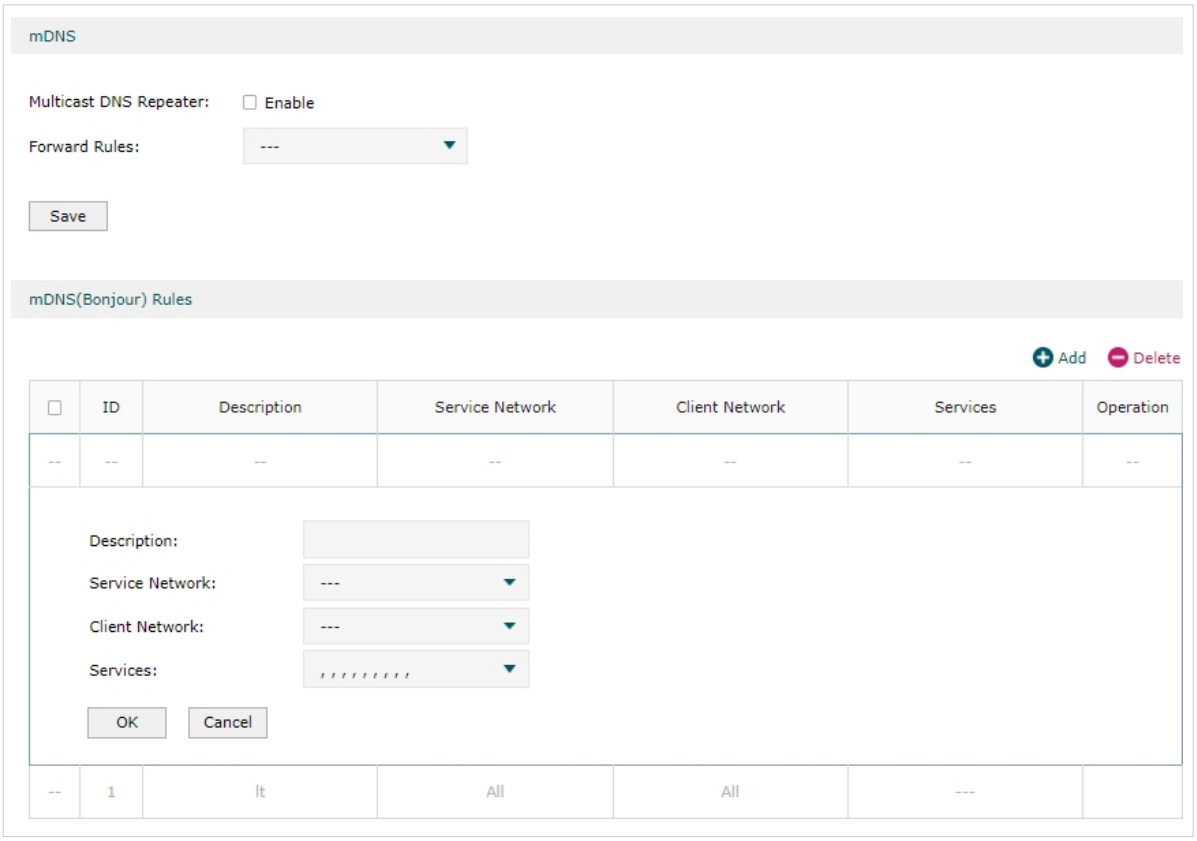


5 mDNS 구성

멀티캐스트 DNS 리피터를 활성화하고 정방향 규칙을 지정하여 mDNS 요청/응답 패킷이 통과할 수 있는 네트워크 세그먼트, 즉 네트워크 세그먼트에서 찾을 수 있는 서비스 범위를 결정합니다. 봉쥬르는 mDNS 프로토콜을 기반으로 하는 Apple의 개방형 제로 구성 네트워크 표준으로, IP 네트워크에서 컴퓨터, 장치 및 서비스를 자동으로 검색할 수 있습니다.

서비스 > **mDNS** 메뉴를 선택하고 **추가를** 클릭하여 다음 페이지를 로드합니다.

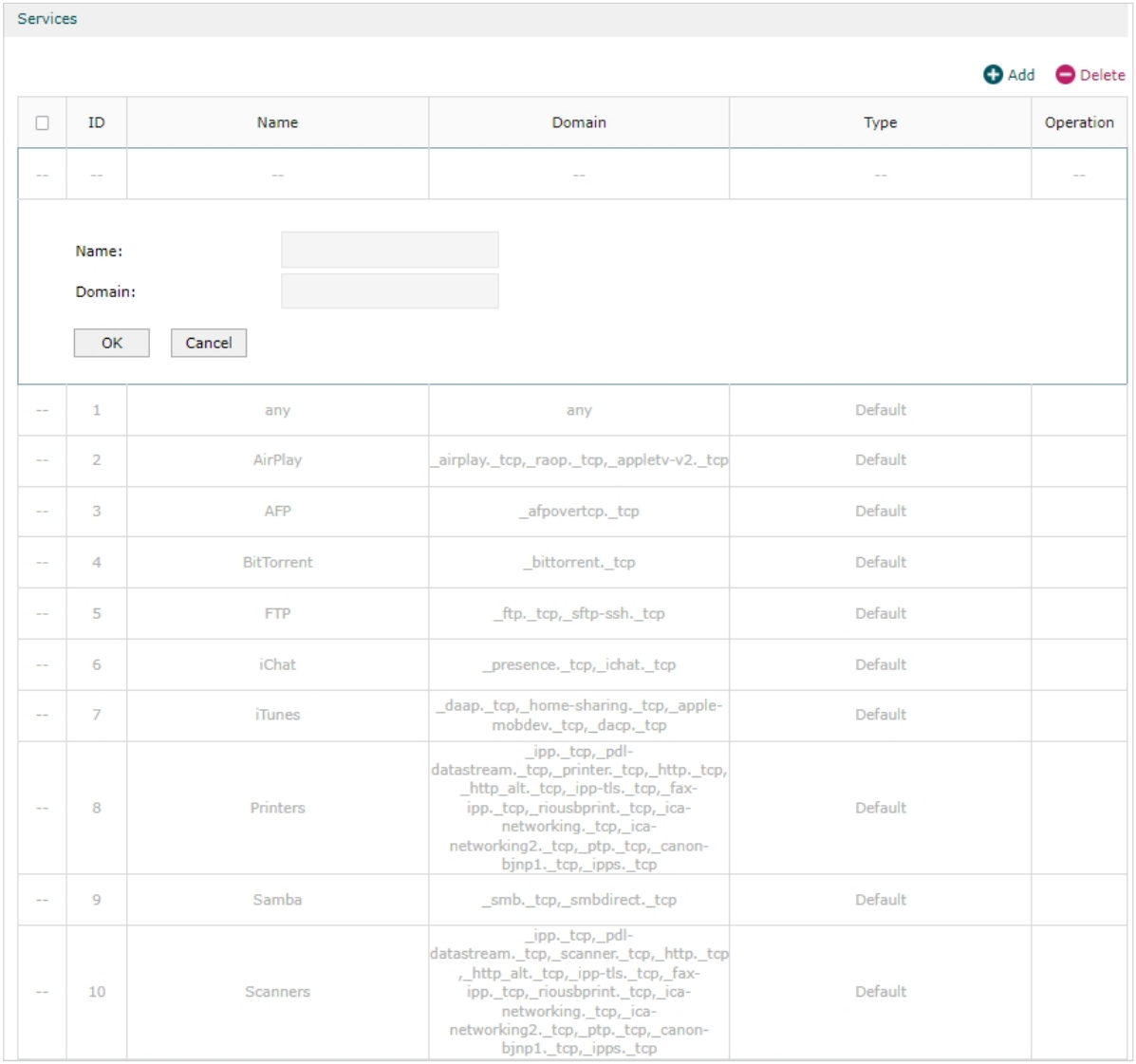
그림 5-1 mDNS 기능 구성



멀티캐스트 DNS 리피터	기능을 활성화하려면 확인란을 선택합니다.
포워드 규칙	mDNS 요청/응답 패킷을 전달하기 위해 하나 또는 여러 개의 mDNS(봉쥬르) 규칙을 선택합니다.
설명	규칙에 이름을 지정합니다.
서비스 네트워크	네트워크를 선택하면 게이트웨이에서 해당 mDNS 응답 패킷을 전달합니다. 클라이언트
네트워크	네트워크를 선택하면 게이트웨이에서 해당 네트워크의 mDNS 요청 패킷을 전달합니다.

서비스	서비스 유형을 선택하면 해당 서비스의 트래픽을 게이트웨이에서 전달할 수 있습니다.

서비스 섹션에서 mDNS가 지원하는 서비스 유형 **추가** 및 관리를 클릭합니다.



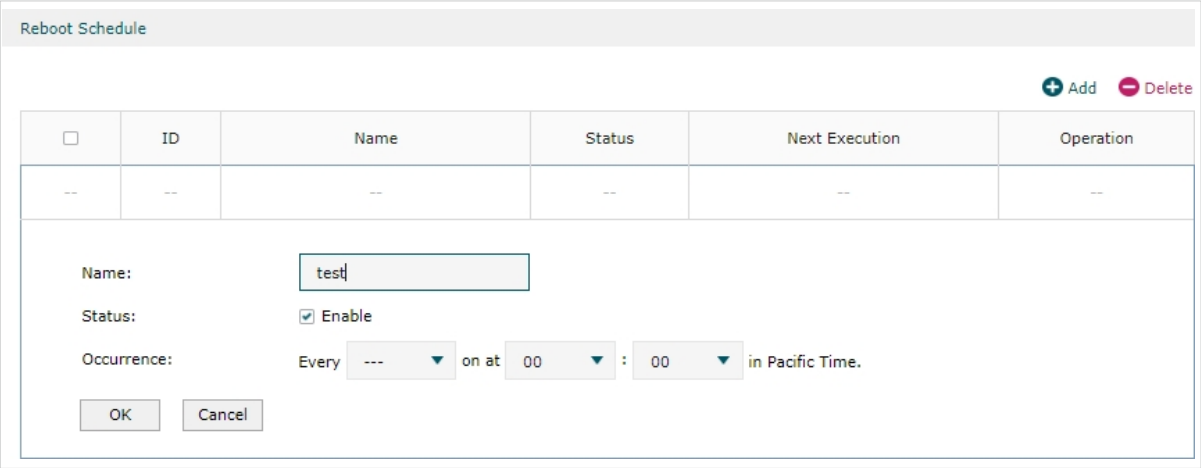
이름	서비스를 식별할 이름을 입력합니다.
상태	서비스의 도메인을 입력합니다.

6 R 전자 부팅 일정

재부팅 일정에서는 필요에 따라 연결된 장치를 주기적으로 재부팅하도록 일정을 설정할 수 있습니다. 여러 항목을 생성하여 재부팅 일정을 유연하게 구성할 수 있습니다.

서비스 > **재부팅 일정** 메뉴를 선택하고 **추가를** 클릭하여 다음 페이지를 로드합니다.

그림 6-1 재부팅 일정 구성하기



이름	재부팅 일정 항목을 식별할 이름을 입력합니다.
상태	재부팅 일정 항목을 활성화하려면 확인란을 클릭합니다. 발
생	장치를 재부팅할 날짜와 시간을 지정합니다.

7 DNS 프록시

DNS 프록시는 LAN 측 클라이언트에 DNS 쿼리 서비스를 제공합니다. LAN 측 클라이언트의 DNS 요청을 선택한 업스트림 DNS 서버로 전달하고 그에 따라 DNS 응답을 전달합니다.

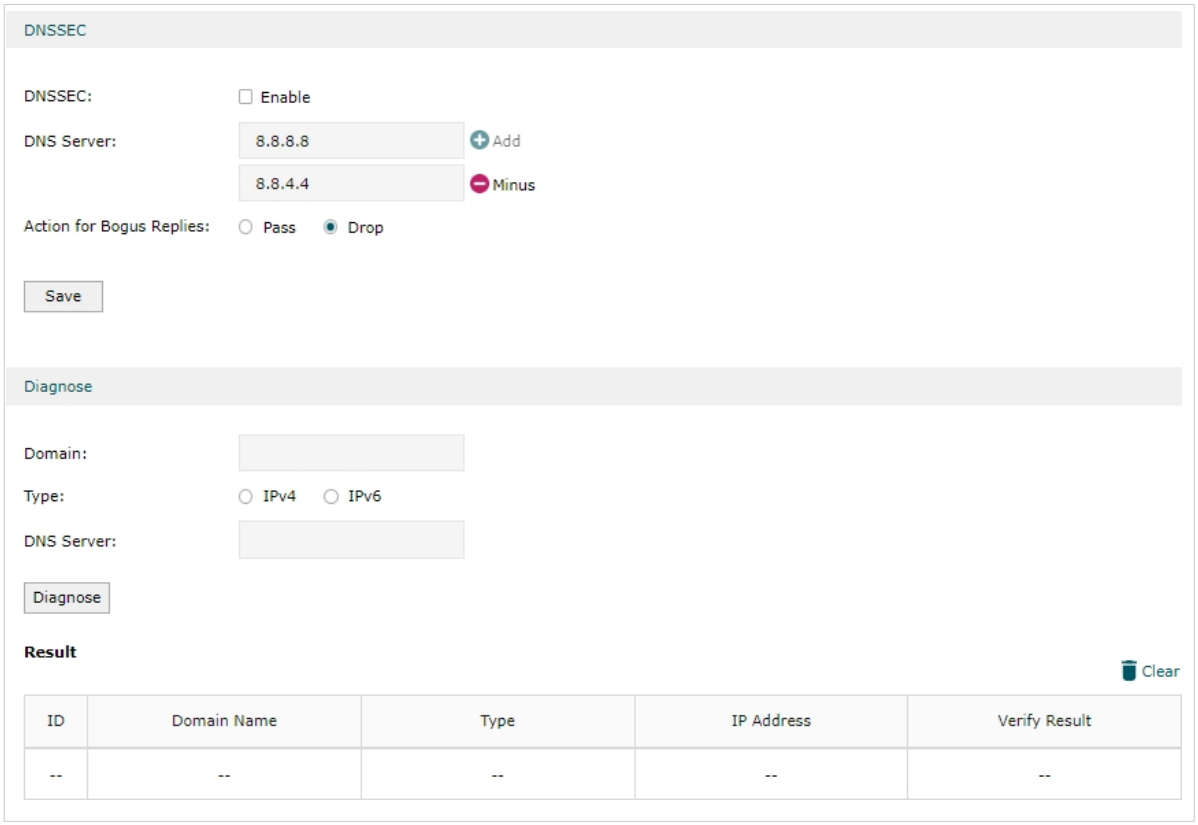
DNS 프록시를 위한 세 가지 보안 옵션은 DNSSEC(DNS 보안 확장), DoT(TLS를 통한 DNS), DoH(Https를 통한 DNS)입니다. DNSSEC는 DNS 레코드의 무결성을 확인하며, DoT/DoH는 쿼리를 암호화합니다.

세 가지 옵션 모두 이를 지원하는 업스트림 DNS 서버가 필요합니다.

7.1 DNSSEC

서비스 > **DNS 프록시** > **DNSSEC** 메뉴를 선택하여 다음 페이지를 로드합니다.

그림 7-1 DNSSEC 구성



DNSSEC에서 다음 파라미터를 구성합니다.

DNSSEC	확인란을 선택하여 기능을 활성화합니다.

DNS 서버	DNSSEC 서버의 IP 주소를 지정합니다. 최대 2개의 IP 주소를 구성할 수 있습니다.
가짜 답글에 대한 조치	서명 확인에 실패한 DNS 응답 패킷을 처리하는 작업을 지정합니다.

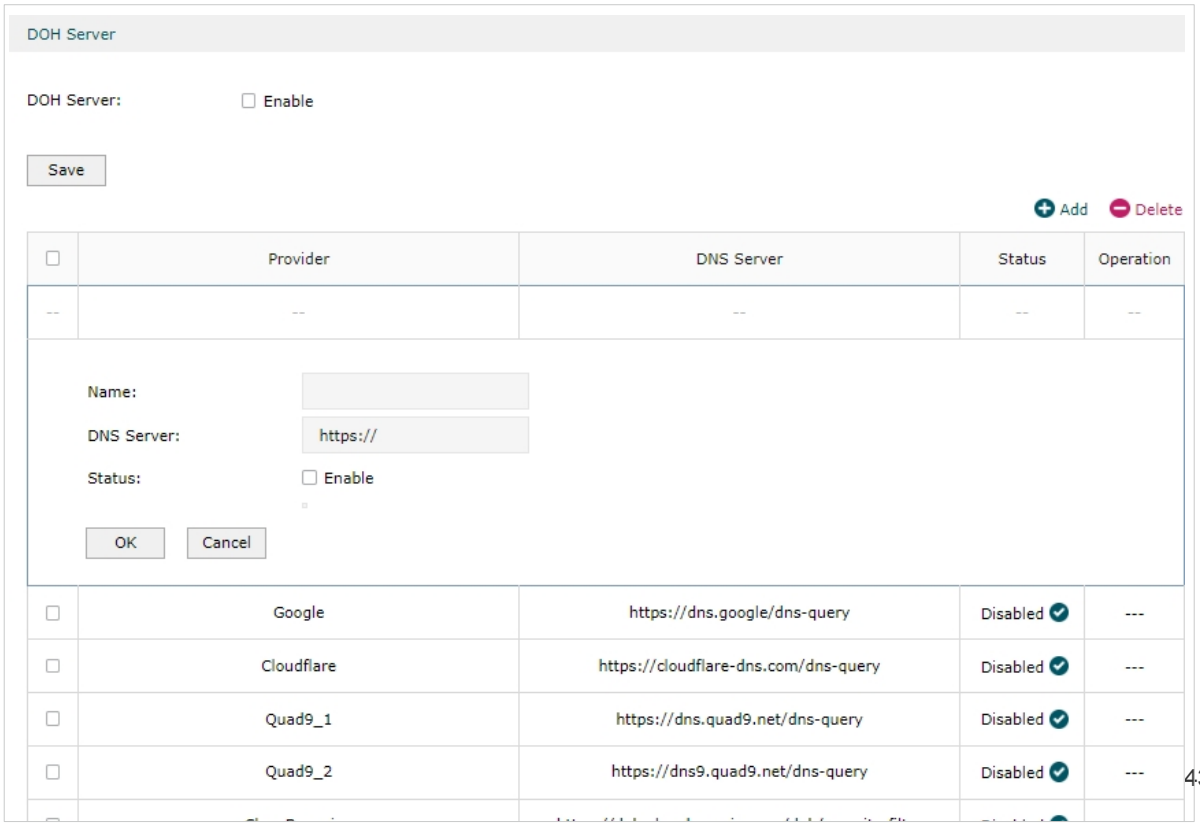
진단 섹션에서 다음 매개변수를 구성합니다.

도메인	쿼리하려는 도메인 이름을 지정합니다.
유형	도메인 이름에 해당하는 IPv4/IPv6 주소를 쿼리합니다. DNS 서버 사용되는 업스트림 DNS 서버를 지정합니다.
진단	도메인 네임을 진단하고 결과를 확인하려면 클릭합니다. 진단 결과는 세 가지가 있을 수 있습니다: 보안: 쿼리한 도메인 이름이 DNSSEC 서명 확인을 통과했습니다. Bogus: 쿼리한 도메인 이름이 DNSSEC 서명 확인을 통과하지 못했습니다. 도메인 이름 인증에 실패했습니다. 안전하지 않습니다: 장치가 쿼리된 도메인 이름의 DNSSEC 서명을 확인할 수 없습니다.

7.2 DOH

서비스 > **DNS 프록시** > **DOH** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 7-2 DOH 구성



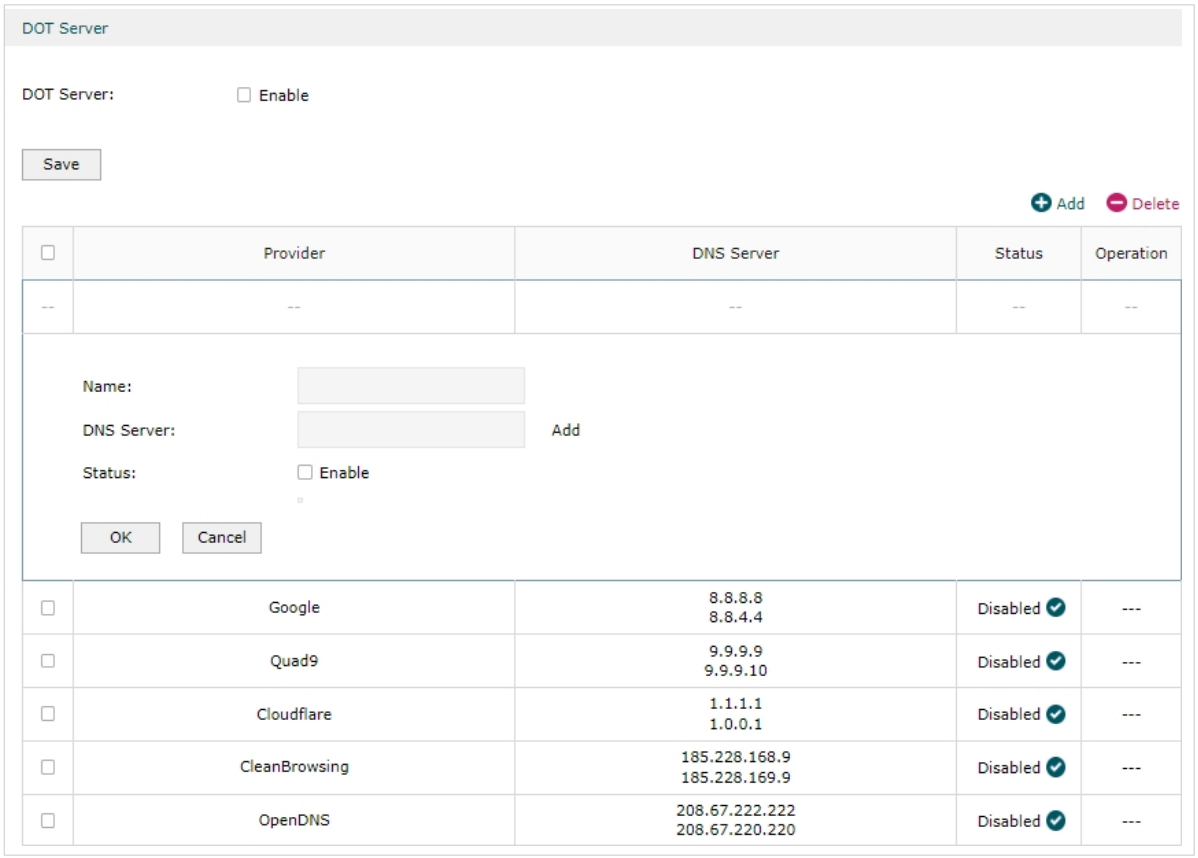
기능을 활성화하고 추가를 클릭하여 새 서버 항목을 만듭니다.

DOH 서버	이 확인란을 선택하면 DoH(DNS over Https) 서버를 활성화합니다.
이름	서버의 이름을 지정합니다.
DNS 서버	DNS 서버의 도메인 이름을 지정합니다. 서버는 하나만 추가할 수 있습니다.
상태	이 서버 항목을 활성화할지 여부를 지정합니다. 동시에 최대 두 개의 서버 항목을 활성화할 수 있습니다.

7.3 DOT

서비스 > **DNS 프록시** > **DOT** 메뉴를 선택하여 다음 페이지를 로드합니다.

그림 7-3 DOT 구성



기능을 활성화하고 추가를 클릭하여 새 서버 항목을 만듭니다.

DOT 서버	이 확인란을 선택하면 DoT(DNS over TLS) 서버를 사용하도록 설정할 수 있습니다.
이름	서버의 이름을 지정합니다.
DNS 서버	DNS 서버의 IP 주소를 지정합니다. 최대 2개의 서버를 추가할 수 있습니다.

상태	이 서버 항목을 활성화할지 여부를 지정합니다. 동시에 최대 두 개의 서버 항목을 활성화할 수 있습니다.

파트 13

시스템 도구

챕터

7. 시간 설정

8. 시스템 로그

1 S 시스템 도구

1.1 개요

시스템 도구 모듈은 사용자가 라우터를 관리할 수 있는 여러 가지 시스템 관리 도구를 제공합니다
.

1.2 지원 기능

관리자 설정

관리자 설정은 사용자 로그인에 대한 매개변수를 구성하는 데 사용됩니다. 이 기능을 사용하면 로그인 계정을 수정하고, 원격 액세스를 위한 IP 서브넷과 마스크를 지정하고, HTTP 및 HTTPS 서버 포트를 지정할 수 있습니다.

관리

관리 섹션은 라우터의 펌웨어 및 구성 파일을 관리하는 데 사용됩니다. 이 기능을 통해 라우터를 재설정하고, 구성 파일을 백업 및 복원하고, 라우터를 재부팅하고, 펌웨어를 업그레이드할 수 있습니다.

SNMP

SNMP(단순 네트워크 관리 프로토콜)는 표준 네트워크 관리 프로토콜입니다. 네트워크 관리자가 네트워크 장치를 구성하고 모니터링하는 데 도움이 됩니다. 네트워크 관리자는 SNMP를 사용하여 네트워크 장치 정보를 보고 수정하고, 네트워크 오류를 감지 및 분석하는 등의 작업을 수행할 수 있습니다. 이 라우터는 SNMPv1 및 SNMPv2c를 지원합니다.

진단

진단은 네트워크 오류 및 장비 오류를 감지하는 데 사용됩니다. 이 기능을 사용하면 핑 또는 추적 라우팅 명령으로 네트워크 연결을 테스트하고 기술자의 도움을 받아 라우터를 검사할 수 있습니다.

시간 설정

시간 설정은 시스템 시간 및 서머타임을 구성하는 데 사용됩니다.

시스템 로그

시스템 로그는 라우터의 시스템 로그를 보는 데 사용됩니다. 로그를 서버로 보내도록 라우터를 구성할 수도 있습니다.

2 A dmin 설정

관리자 설정 모듈에서 다음 기능을 구성할 수 있습니다:

- 관리자 설정
- 원격 관리
- 시스템 설정

2.1 관리자 설정

시스템 도구 > **관리자 설정** > **관리자 설정** 메뉴를 선택하여 다음 페이지를 로드합니다.

그림 2-1 관리자 계정 수정하기

계정 섹션에서 다음 매개변수를 구성하고 **저장을** 클릭하여 관리자 계정을 수정합니다.

이전 사용자 아이디이전 사용자 아이디를 입력합

니다. 이전 비밀번호이전 비밀번호를 입력합니다.

새 사용자 아이디새 사용

자 아이디를 입력합니다. 새 비밀번호새 비

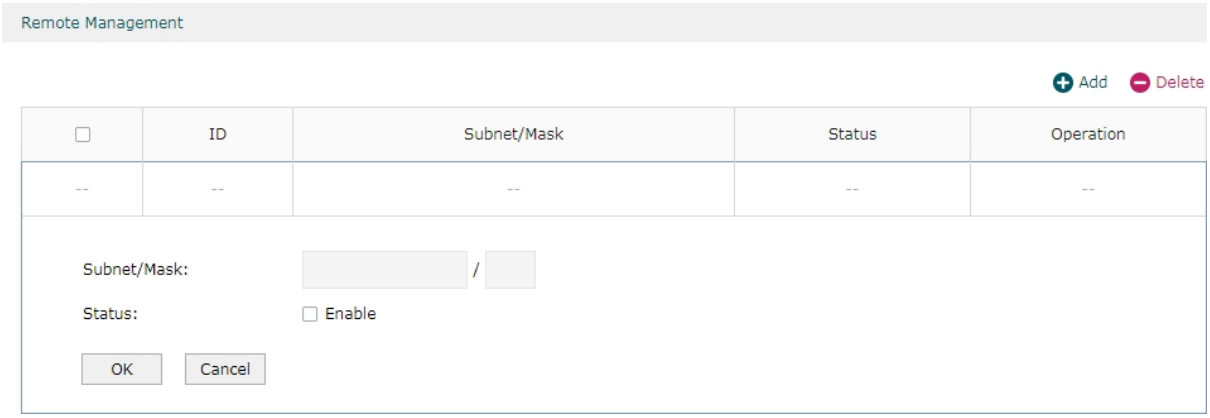
밀번호를 입력합니다.

새 비밀번호	확인을 위해 새 비밀번호를 다시 입력합니다.
확인	

2.2 원격 관리

시스템 도구 > **관리자 설정** > **원격 관리** 메뉴를 선택하고 **추가를** 클릭하여 다음 페이지를 로드합니다.

그림 2-2 원격 관리 구성



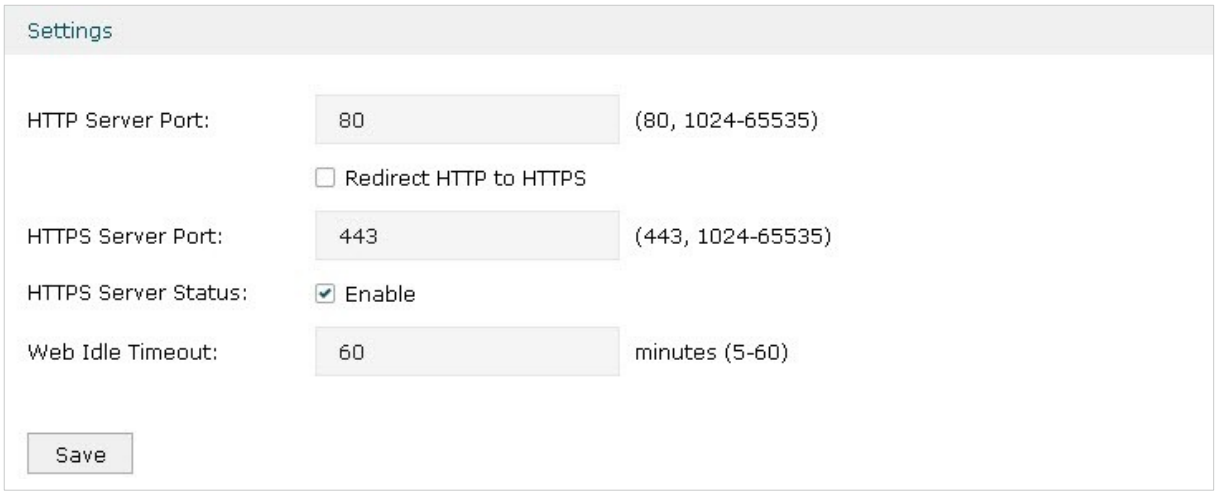
원격 관리 섹션에서 다음 매개변수를 구성하고 **확인을** 클릭하여 원격 관리를 위한 IP 서브넷과 마스크를 지정합니다.

서브넷/마스크	원격 호스트의 IP 서브넷과 마스크를 입력합니다.
상태	이 확인란을 선택하면 원격 호스트에 대한 원격 관리 기능이 활성화됩니다.

2.3 시스템 설정

시스템 도구 > **관리자 설정** > **시스템 설정** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 2-3 시스템 설정 구성하기



설정 섹션에서 다음 매개변수를 구성하고 **저장을** 클릭합니다.

HTTP 서버 포트	웹 관리를 위한 http 서버 포트를 입력합니다. 포트 번호는 다른 서버의 포트 번호와 달라야 합니다. 기본 설정은 80입니다. http 서버 포트를 변경한 후 192.168.0.1:1600 형식의 IP 주소와 포트 번호를 사용하여 인터페이스에 액세스해야 합니다.
HTTP를 HTTPS로 리디렉션	이 확인란을 선택하여 기능을 활성화하면 HTTP 프로토콜 대신 HTTPS 프로토콜로 웹 관리 인터페이스에 액세스하게 됩니다.
HTTPS 서버 포트	웹 관리를 위한 https 서버 포트를 입력합니다. 포트 번호는 다른 서버의 포트 번호와 달라야 합니다. 기본 설정은 443입니다. https 서버 포트를 변경한 후에는 https://192.168.0.1:1800 형식의 IP 주소와 포트 번호를 사용하여 인터페이스에 액세스해야 합니다.
HTTPS 서버 상태	확인란을 선택하면 HTTPS 서버가 활성화됩니다.
웹 유휴 시간 초과	장치의 세션 시간 제한 시간을 입력합니다. 세션 제한 시간 내에 작업이 없는 경우 보안을 위해 웹 세션이 로그아웃됩니다.

3 컨트롤러 설정

컨트롤러가 라우터를 채택하도록 하려면 컨트롤러에서 라우터를 검색할 수 있는지 확인하세요. 컨트롤러 설정에서 다음 시나리오 중 하나에서 라우터를 검색할 수 있도록 설정합니다.

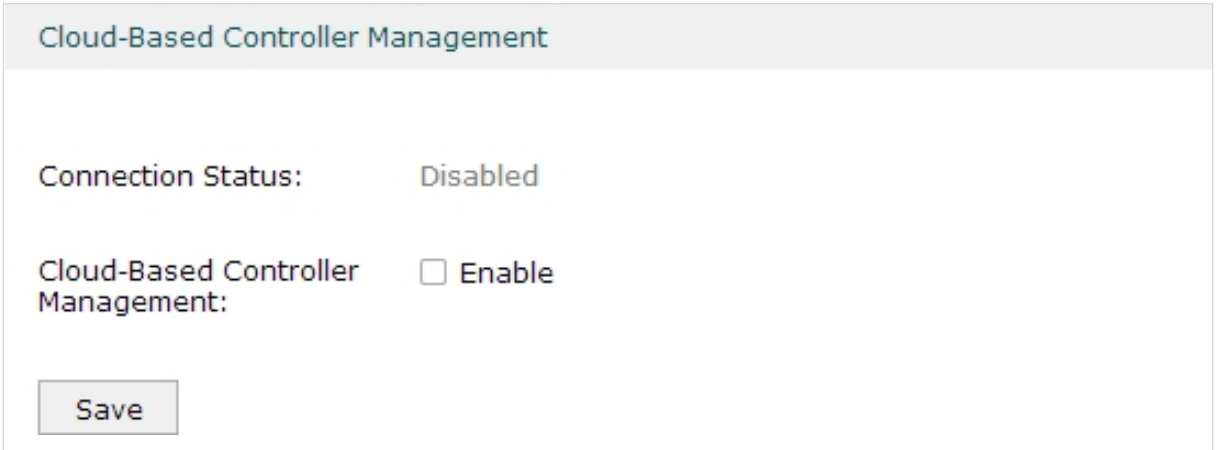
- Omada 클라우드 기반 컨트롤러를 사용하는 경우 클라우드 기반 컨트롤러 관리를 사용 설정합니다.
- 라우터와 컨트롤러가 동일한 네트워크, LAN 및 VLAN에 있는 경우 컨트롤러는 컨트롤러 설정 없이도 라우터를 검색하여 채택할 수 있습니다. 그렇지 않은 경우 컨트롤러의 URL/IP 주소를 라우터에 알려야 하며, 한 가지 가능한 방법은 컨트롤러 알리기 URL 구성을 사용하는 것입니다.

전체 절차에 대한 자세한 내용은 Omada Pro SDN 컨트롤러의 사용자 가이드를 참조하세요. 이 가이드는 공식 웹사이트의 다운로드 센터(https:// www.tp-link.com/support/download/)에서 확인할 수 있습니다.

3.1 클라우드 기반 컨트롤러 관리 사용

시스템 도구 > **컨트롤러 설정** 페이지 메뉴를 선택합니다. 클라우드 기반 컨트롤러 관리 섹션에서 클라우드 기반 컨트롤러 관리를 사용 설정하고 **저장을** 클릭합니다. 이 페이지에서 연결 상태를 확인할 수 있습니다.

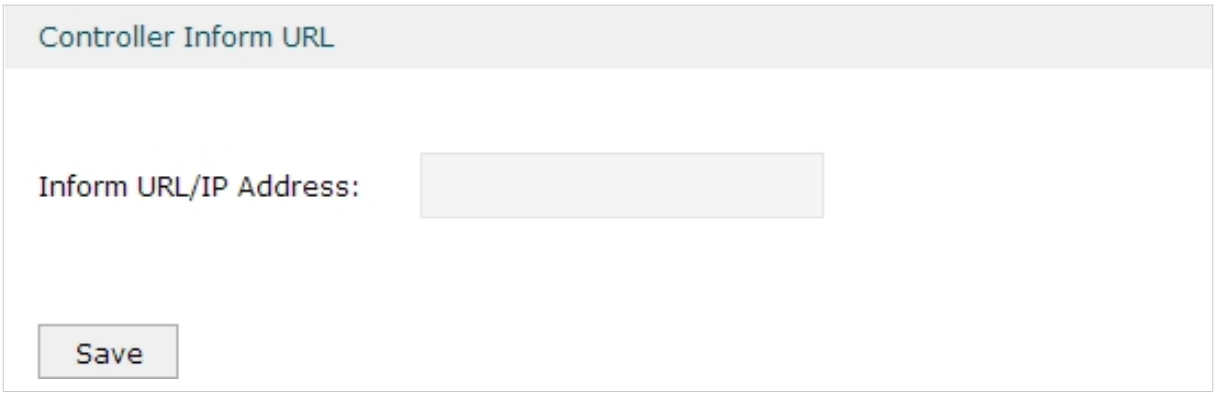
그림 3-1 클라우드 기반 컨트롤러 관리



3.2 컨트롤러 정보 URL 구성

시스템 도구 > **컨트롤러 설정** 페이지 메뉴를 선택합니다. 컨트롤러에 URL 알리기 섹션에서 라우터에 컨트롤러의 URL/IP 주소를 알려주고 **저장을** 클릭합니다. 그러면 라우터가 컨트롤러와 연결하여 컨트롤러가 라우터를 검색할 수 있습니다.

그림 3-2 클라우드 기반 컨트롤러 관리



4 관리

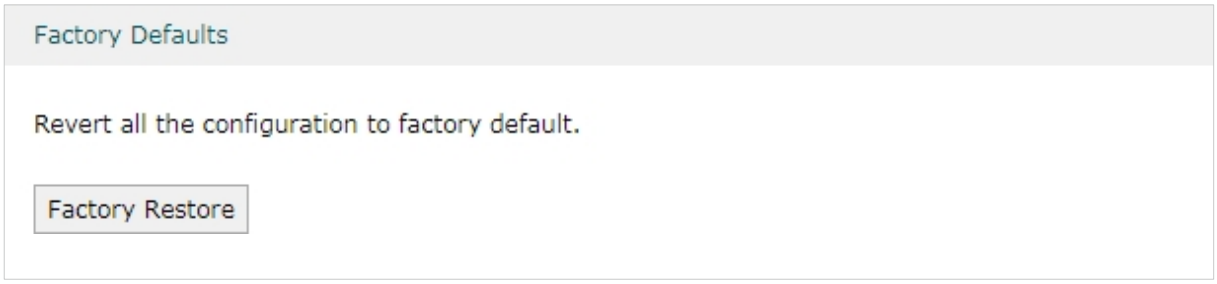
관리 모듈에서는 다음 기능을 구성할 수 있습니다:

- 공장 기본값 복원
- 백업 및 복원
- 재부팅
- 펌웨어 업그레이드

4.1 공장 기본값 복원

시스템 도구 > **관리** > **공장** 기본값 **복원** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 4-1 장치 재설정하기

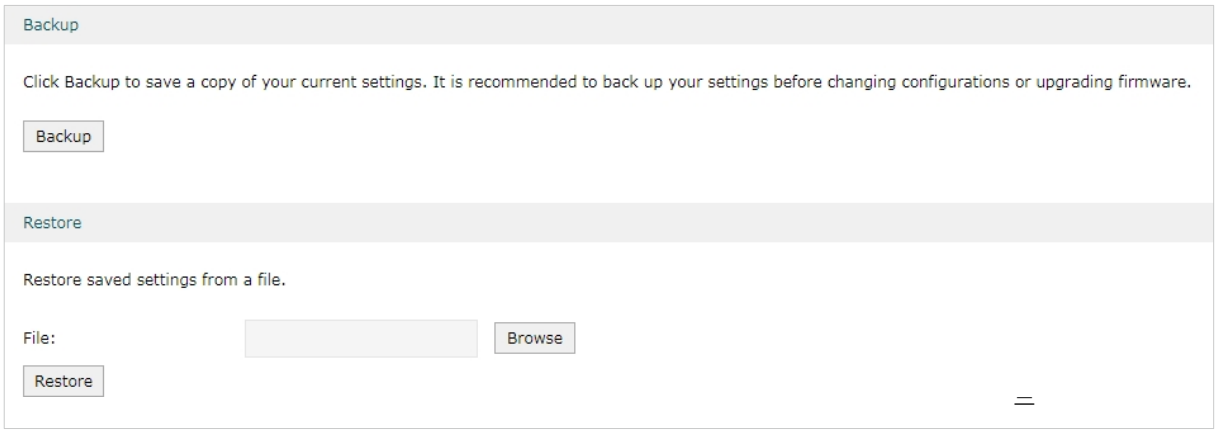


공장 초기화를 클릭하여 장치를 재설정합니다.

4.2 백업 및 복원

시스템 도구 > **관리** > **백업 및 복원** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 4-2 백업 및 복원 페이지



필요에 따라 해당 작업을 선택합니다:

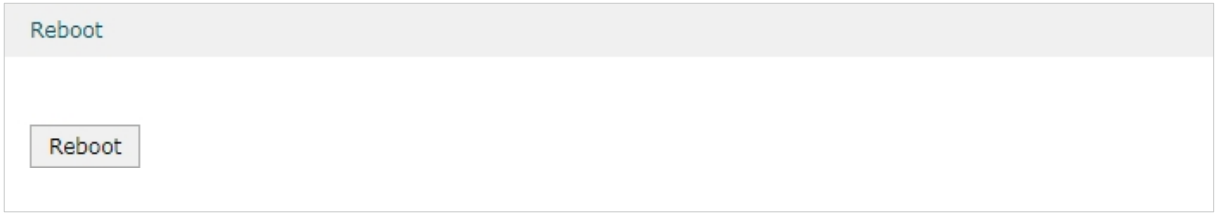
1) **백업** 섹션에서 **백업을** 클릭하여 현재 구성을 구성 파일로 저장하고 파일을 호스트로 내보냅니다.

2) **복원** 섹션에서 호스트에 저장된 구성 파일 하나를 선택하고 **복원을** 클릭합니다.
를 클릭하여 저장된 구성을 라우터로 가져옵니다.

4.3 재부팅

시스템 도구 > **관리** > **재부팅** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 4-3 장치 재부팅하기



재부팅을 클릭하여 장치를 재부팅합니다.

4.4 펌웨어 업그레이드

시스템 도구 > **관리** > **펌웨어 업그레이드** 메뉴를 선택하면 다음 페이지가 로드됩니다.

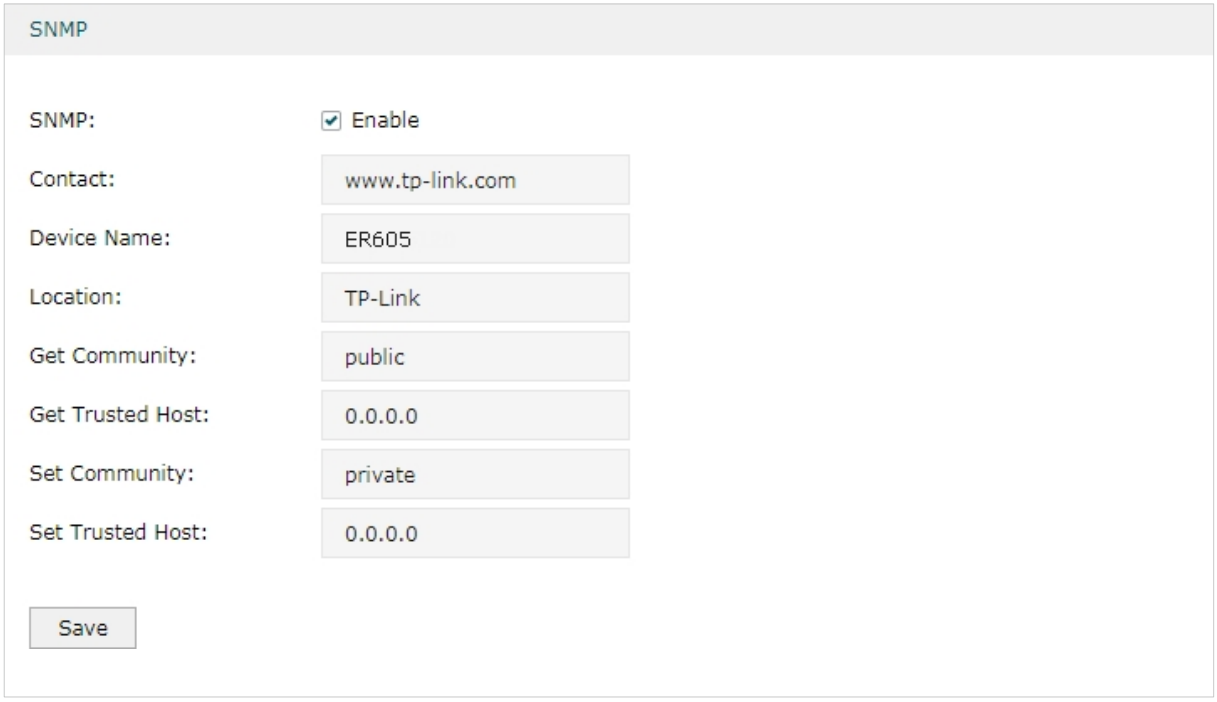
그림 4-4 시스템 설정 구성

하나의 펌웨어 파일을 선택하고 **업그레이드를** 클릭하여 장치의 펌웨어를 업그레이드합니다.

5 SNMP

시스템 도구 > **SNMP** > **SNMP** 메뉴를 선택하여 다음 페이지를 로드합니다.

그림 5-1 SNMP 구성



SNMP 기능을 구성하려면 다음 단계를 따르세요:

1) SNMP 기능을 사용하려면 확인란을 선택합니다.

2) 다음 매개변수를 구성하고 **저장을** 클릭합니다.

연락처	연락처 또는 이메일 주소와 같이 이 기기에 대한 담당자의 텍스트 식별 정 보 를 입력합니다.
장치 이름	디바이스의 이름을 입력합니다.
위치	디바이스의 위치를 입력합니다. 예를 들어 이름은 건물, 층수, 방 위치로 구성할 수 있습니다.
커뮤니티 가져오기	디바이스의 SNMP 정보에 대한 읽기 전용 액세스 권한이 있는 커뮤니티를 지정합니다.
신뢰할 수 있는 호스트 확보	

이 디바이스의	SNMP 정보를 읽을 수 있는 커뮤니티 가져오기 역할을 할 수 있는 IP 주소를 입력합니다.
커뮤니티 설정	디바이스의 SNMP 정보에 대한 읽기 및 쓰기 권한이 있는 커뮤니티를 지정합니다.
신뢰할 수 있는 호스트 설정	이 디바이스의 SNMP 정보를 읽고 쓸 수 있도록 커뮤니티 설정 역할을 할 수 있는 IP 주소를 입력합니다.

6 진단

진단 모듈에서는 다음 기능을 구성할 수 있습니다:

- 진단
- 원격 지원

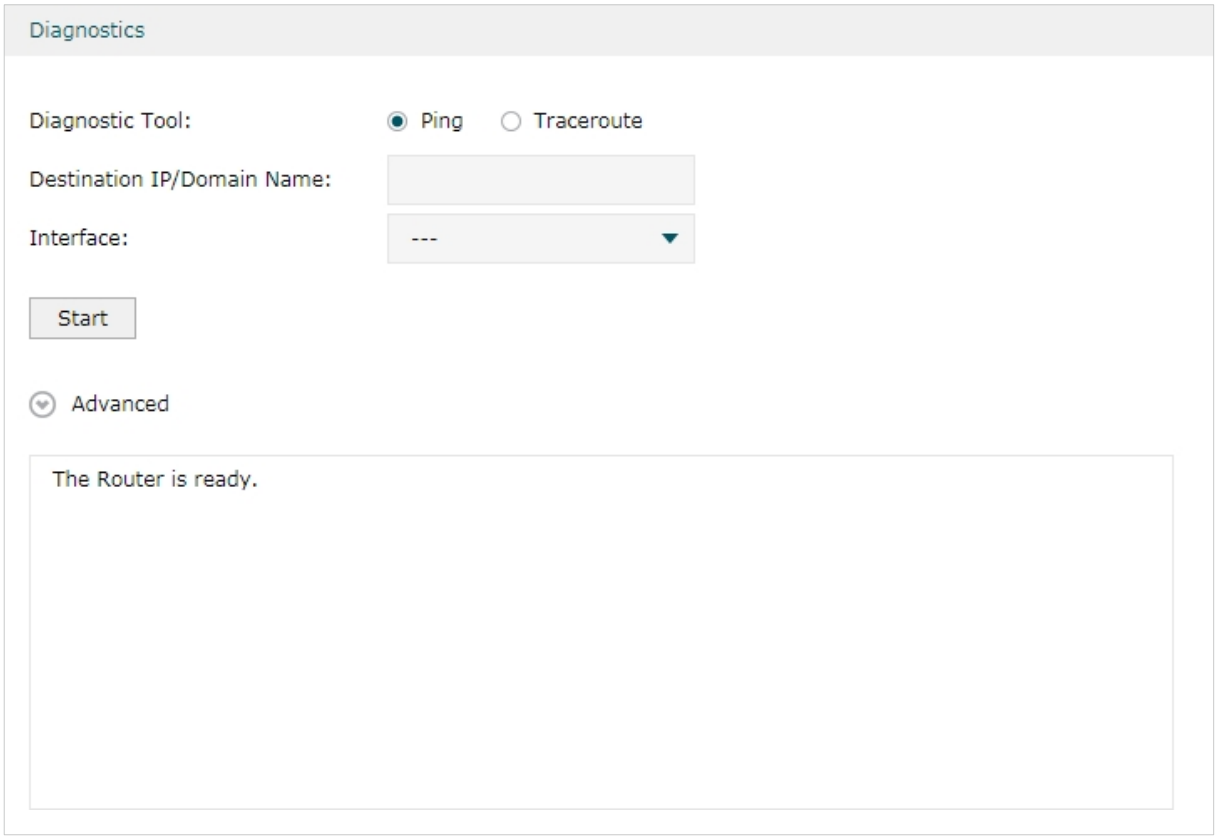
6.1 진단

핑과 추적 경로는 모두 네트워크에서 두 장치 간의 연결을 테스트하는 데 사용됩니다. 또한 핑은 두 디바이스 간의 왕복 시간을 직접 표시할 수 있고, 추적 경로는 경로 경로에 있는 라우터의 IP 주소를 표시할 수 있습니다.

6.1.1 Ping 구성

시스템 도구 > **진단** > **진단** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 6-1 진단 구성하기



진단을 구성하려면 다음 단계를 따르세요:

1) **진단** 섹션에서 Ping을 선택하고 다음 매개변수를 구성합니다.

진단 도구	Ping을 선택하여 라우터와 원하는 디바이스 간의 연결을 테스트합니다.

대상 IP/도메인 이름	핑 또는 추적할 IP 주소 또는 도메인 이름을 입력합니다.
인터페이스	탐지 패킷을 전송하는 인터페이스를 선택합니다.

2) (선택 사항) 고급을 클릭하면 다음 섹션이 나타납니다.

그림 6-2 핑 방법의 고급 매개 변수

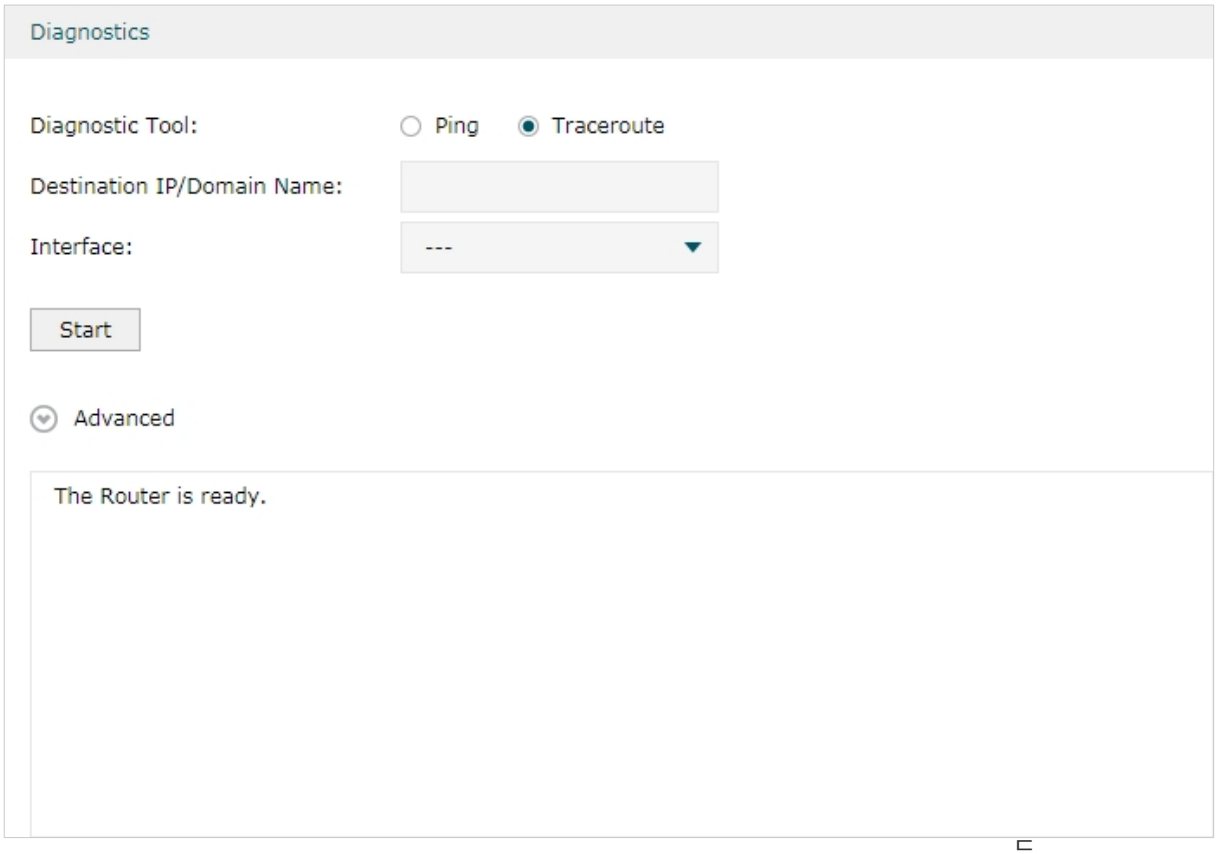
핑 횟수	핑 프로세스 중에 전송할 테스트 패킷의 수를 지정합니다. 핑 패킷 크기
	핑 프로세스 중에 전송할 테스트 패킷의 크기를 지정합니다.

3) **시작을** 클릭합니다.

6.1.2 추적 경로 구성

시스템 도구 > **진단** > **진단** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 6-3 진단 구성하기



드

진단을 구성하려면 다음 단계를 따르세요:

1) **진단** 섹션에서 **추적** 경로를 선택하고 다음 매개변수를 구성합니다.

진단 도구	라우터와 원하는 디바이스 간의 연결을 테스트하려면 **경로 추적을** 선택합니다.
대상 IP/도메인 이름	핑 또는 추적할 IP 주소 또는 도메인 이름을 입력합니다.
인터페이스	탐지 패킷을 전송하는 인터페이스를 선택합니다.

2) (선택 사항) 고급을 클릭하면 다음 섹션이 나타납니다.

그림 6-4 추적 경로 메서드의 고급 매개 변수

최대 TTL 추적 경로	추적 라우팅 프로세스 중 추적 라우팅 최대 TTL(Time To Live)을 지정합니다. 테스트 패킷이 통과할 수 있는 경로 홉의 최대 개수입니다.

3) **시작을** 클릭합니다.

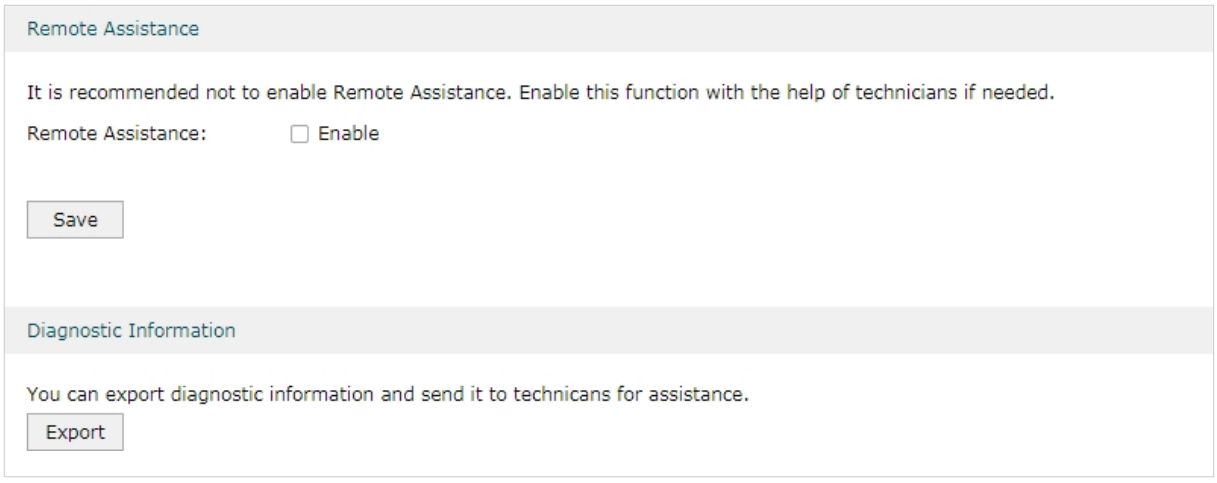
6.2 원격 지원

참고:

이 기능을 사용하기 전에 기술자에게 문의해 주세요.

시스템 도구 > **진단** > **원격 지원** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 6-5 원격 지원 페이지



1) **원격 지원** 섹션에서 확인란을 선택하고 **저장을** 클릭하여 원격 지원 기능을 활성화하면 기술자가 라우터에 액세스하여 SSH를 통해 문제 해결을 도울 수 있습니다.
2) **진단 정보** 섹션에서 **내보내기를** 클릭하여 유용한 정보가 포함된 바이너리(.bin) 파일을 다운로드한 다음 기술자에게 보내 도움을 요청합니다.

7 시간 설정

시간 설정 모듈에서는 다음과 같은 기능을 구성할 수 있습니다:

- 시스템 시간
- 일광 절약 시간제

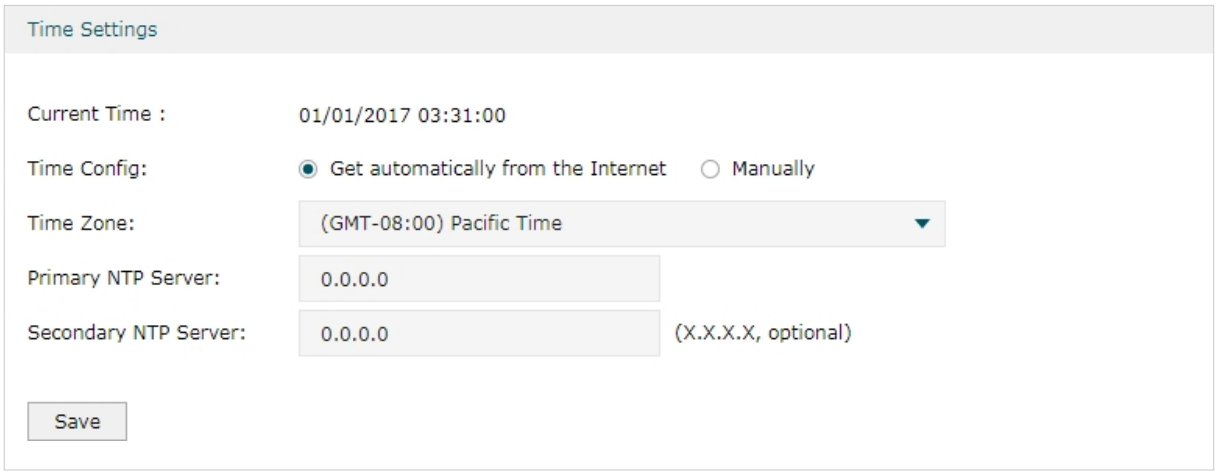
7.1 시스템 시간 설정

시스템 시간을 설정하는 방법 중 하나를 선택합니다.

7.1.1 인터넷에서 자동으로 시간 얻기

시스템 도구 > **시간 설정** > **시간 설정** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 7-1 인터넷에서 자동으로 가져오기



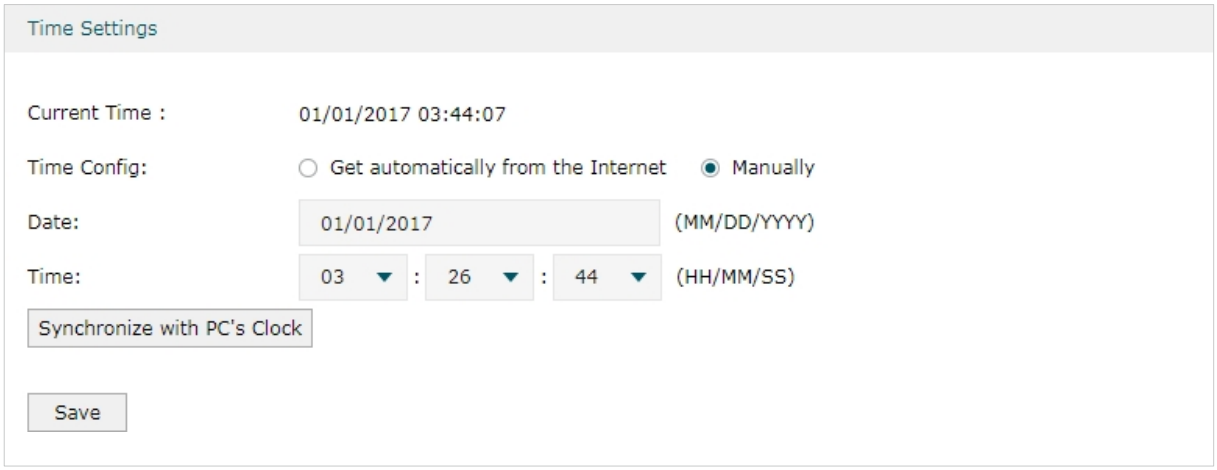
시간 설정 섹션에서 다음 매개변수를 구성하고 **저장을** 클릭합니다.

현재 시간	현재 시스템 시간을 표시합니다.
시간 **구성인터넷에서 자동으로** 가져오기를 선택하여 NTP 서버에서 시스템 시간을 가져옵니다.	
시간대	기기가 위치한 표준 시간대를 선택합니다.
기본 NTP 서버	기본 NTP 서버의 IP 주소를 입력합니다.
보조 NTP 서버	보조 NTP 서버의 IP 주소를 입력합니다.

7.1.2 시스템 시간 수동 설정

시스템 도구 > **시간 설정** > **시간 설정** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 7-2 시스템 시간 수동 설정하기



시간 설정 섹션에서 다음 매개변수를 구성하고 **저장을** 클릭합니다.

현재 시간	현재 시스템 시간을 표시합니다.
시간 구성시스템 시간을 수동으로 설정하려면 **수동을** 선택합니다. 날짜	
	시스템 날짜를 지정합니다.
시간	시스템의 시간을 지정합니다.
PC의 시계와 동기화	라우터의 시스템 시간을 PC의 시계와 동기화합니다.

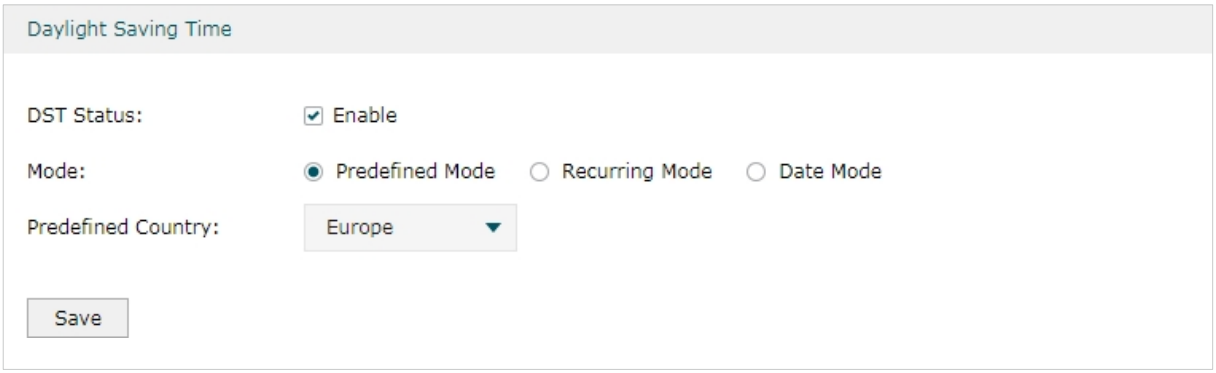
7.2 일광 절약 시간제 설정하기

서머타임을 설정하는 방법 중 하나를 선택합니다.

7.2.1 사전 정의 모드

시스템 도구 > **시간 설정** > **시간 설정** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 7-3 사전 정의 모드 페이지



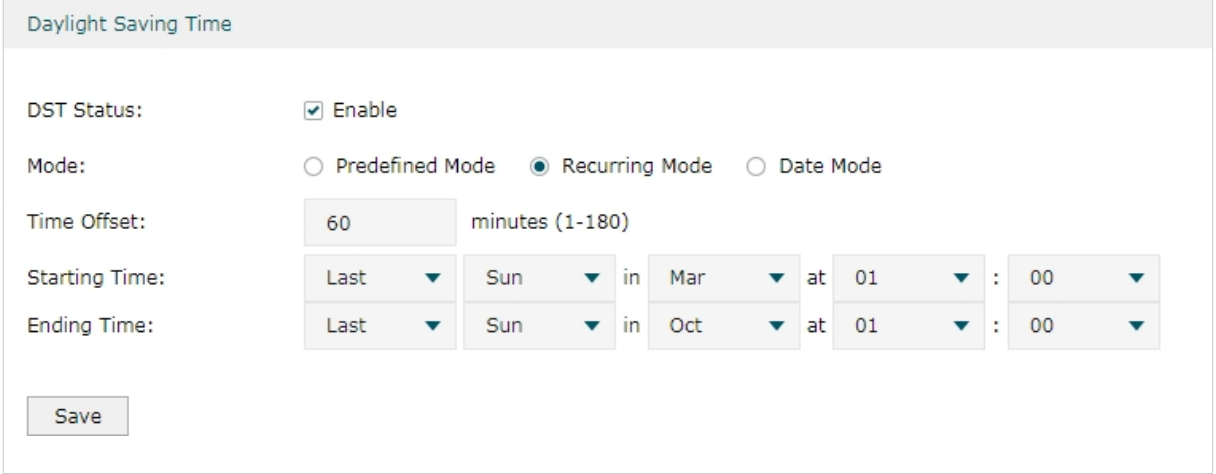
일광 절약 시간제 섹션에서 미리 정의된 DST 일정을 하나 선택하고 **저장을** 클릭합니다.

DST 상태	확인란을 선택하면 DST 기능이 활성화됩니다.
모드	미리 정의된 일광 절약 시간을 선택하려면 미리 **정의된 모드를** 선택합니다.
미국	미국의 일광 절약 시간을 선택합니다. 3월 둘째 주 일요일 오전 2시부터 11월 첫째 주 일요일 오전 2시까지입니다.
유럽	유럽의 일광 절약 시간을 선택합니다. 3월 마지막 일요일 오전 1시부터 10월 마지막 일요일 오전 1시까지입니다.
호주	호주의 일광 절약 시간을 선택합니다. 10월 첫째 주 일요일 오전 2시부터 4월 첫째 주 일요일 오전 3시까지입니다.
뉴질랜드	뉴질랜드의 일광 절약 시간을 선택합니다. 9월 마지막 일요일 오전 2시부터 4월 첫 일요일 오전 3시까지입니다.

7.2.2 반복 모드

시스템 도구 > **시간 설정** > **시간 설정** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 7-4 반복 모드 페이지



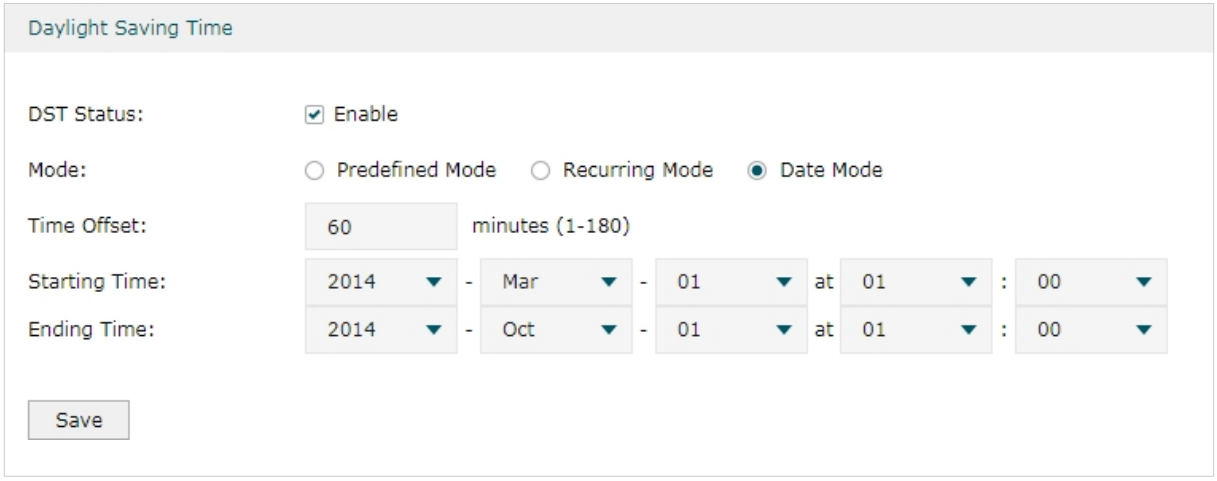
일광 절약 **시간제** 섹션에서 다음 매개 변수를 구성하고 **저장을** 클릭합니다.

DST 상태	확인란을 선택하면 DST 기능이 활성화됩니다.
모드	서머타임의 주기 시간 범위를 지정하려면 **반복 모드를** 선택합니다. 이 구성은 매년 적용됩니다.
시간 오프셋	서머타임이 적용될 때 추가되는 시간을 분 단위로 지정합니다.
시작 시간	일광 절약 시간제의 시작 시간을 지정합니다. 시작 시간은 표준 시간을 기준으로 합니다.
종료 시간서머타임의 종료 시간을 지정합니다.	종료 시간은 서머타임을 기준으로 합니다.

7.2.3 날짜 모드

시스템 도구 > **시간 설정** > **시간 설정** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 7-5 날짜 모드 페이지



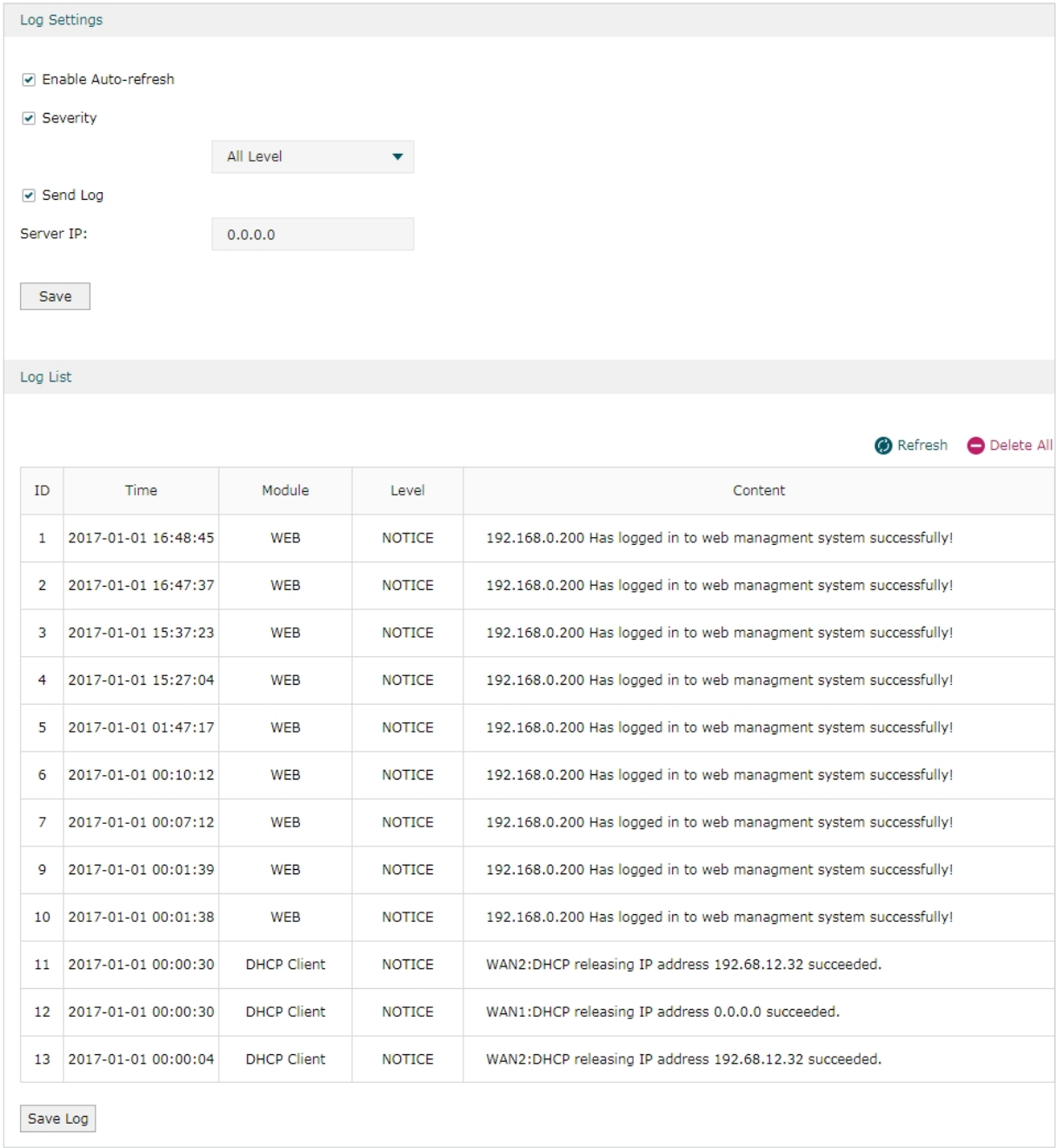
일광 절약 시간제 섹션에서 미리 정의된 DST 일정을 하나 선택하고 **저장을** 클릭합니다.

DST 상태	확인란을 선택하면 DST 기능이 활성화됩니다.
모드	날짜 모드를 선택하면 서머타임의 절대 시간 범위를 지정할 수 있습니다. 시간 오프
셋	일광 절약 시간제가 적용될 때 추가되는 시간을 분 단위로 지정합니다.
시작 시간	일광 절약 시간제의 시작 시간을 지정합니다. 시작 시간은 표준 시간을 기준으로 합니다.
종료 시간서머타임의 종료 시간을 지정합니다.	종료 시간은 서머타임을 기준으로 합니다.

8 S 시스템 로그

시스템 도구 > **시스템 로그** > **시스템 로그** 메뉴를 선택하면 다음 페이지가 로드됩니다.

그림 8-1 시스템 로그 페이지



ID	Time	Module	Level	Content
1	2017-01-01 16:48:45	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
2	2017-01-01 16:47:37	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
3	2017-01-01 15:37:23	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
4	2017-01-01 15:27:04	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
5	2017-01-01 01:47:17	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
6	2017-01-01 00:10:12	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
7	2017-01-01 00:07:12	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
9	2017-01-01 00:01:39	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
10	2017-01-01 00:01:38	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!
11	2017-01-01 00:00:30	DHCP Client	NOTICE	WAN2:DHCP releasing IP address 192.68.12.32 succeeded.
12	2017-01-01 00:00:30	DHCP Client	NOTICE	WAN1:DHCP releasing IP address 0.0.0.0 succeeded.
13	2017-01-01 00:00:04	DHCP Client	NOTICE	WAN2:DHCP releasing IP address 192.68.12.32 succeeded.

시스템 로그를 보려면 다음 단계를 따르세요:

1) **로그 설정** 섹션에서 다음 매개변수를 구성하고 **저장을** 클릭합니다.

자동 새로 고침 사용	이 기능을 활성화하려면 확인란을 선택하면 10초마다 페이지가 자동으로 새로고침됩니다.

심각도	심각도를 사용 설정하고 로그 목록에서 보려는 로그의 중요도를 지정합니다. **모든 레벨**: 모든 레벨의 로그입니다. **긴급**: 하드웨어 오류와 같이 라우터를 사용할 수 없게 만드는 오류입니다. **경고**: 플래시 쓰기 오류와 같이 즉시 해결해야 하는 오류입니다. **CRITICAL**: 메모리 해제 실 패와 같이 시스템을 위험에 빠뜨릴 수 있는 오류입니다. **오류**: 일반 오류입니다. **경고**: WinNuke 공격 경고와 같은 경고 메시지. **알림**: IKE 정책 불일치 등 의 중요 알림. **INFO**: 정보 메시지. **DEBUG**: 라우터가 DNS 패킷을 수신할 때와 같은 디버그 수준의 알림입니다.
로그 보내기	로그 보내기 기능을 활성화하면 새로 생성된 로그가 지정된 서버로 전송됩니다.
서버 IP	로그를 전송할 서버의 IP 주소를 지정합니다.

2) (선택 사항) **로그** 저장을 클릭하여 현재 로그를 호스트에 저장합니다.