

RV320 VPN 라우터, WAP321 Wireless-N Access Point 및 SX300 Series 스위치에서 다중 무선 네트워크 활성화

목표

끊임없이 변화하는 비즈니스 환경에서 소규모 비즈니스 네트워크는 강력하고 유연하며 액세스 가능하며 안정성이 뛰어나야 합니다. 특히 성장을 우선시하는 경우 더욱 그렇습니다. 무선 장치의 인기는 기하급수적으로 증가했지만 놀라운 일은 아닙니다. 무선 네트워크는 비용 효율적이고 구축이 용이하며 유연하고 확장 가능하며 모바일이므로 네트워크 리소스를 원활하게 제공합니다. 인증은 네트워크 장치가 사용자의 합법성을 확인하고 보장하는 동시에 무단 사용자로부터 네트워크를 보호할 수 있도록 허용합니다. 안전하고 관리가 용이한 무선 네트워크 인프라를 구축하는 것이 중요합니다.

Cisco RV320 Dual Gigabit WAN VPN Router는 귀사와 귀사의 직원들에게 안정적이고 매우 안전한 액세스 연결을 제공합니다. Cisco WAP321 Wireless-N Selectable-Band Access Point with Single Point Setup은 기가비트 이더넷으로 고속 연결을 지원합니다. 브리지는 LAN을 무선으로 연결하여 소규모 비즈니스가 네트워크를 더 쉽게 확장할 수 있도록 합니다.

이 문서에서는 라우터, 스위치 및 액세스 포인트의 VLAN(Inter-Virtual Local Area Network) 라우팅, 여러 SSID(Service Set Identifier) 및 무선 보안 설정을 비롯하여 Cisco 중소기업 네트워크에서 무선 액세스를 활성화하는 데 필요한 구성에 대한 단계별 지침을 제공합니다.

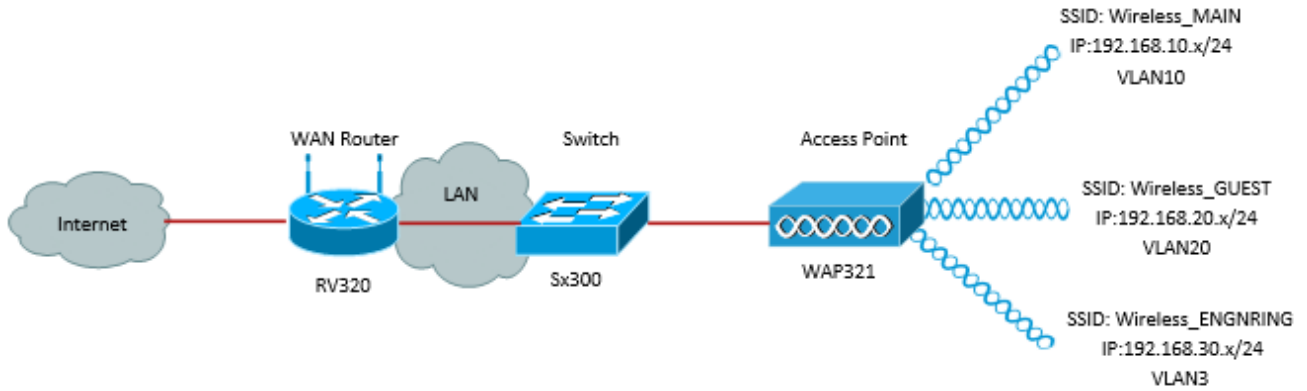
적용 가능한 디바이스

- RV320 VPN Router
- WAP321 Wireless-N Access Point
- SX300 Series 스위치

소프트웨어 버전

- 1.1.0.09(RV320)
- 1.0.4.2(WAP321)
- 1.3.5.58(SX300)

네트워크 토폴로지



위의 이미지는 Cisco Small Business WAP, 스위치 및 라우터를 사용하는 여러 SSID를 사용하는 무선 액세스를 위한 샘플 구현을 보여줍니다. WAP는 스위치에 연결되고 트렁크 인터페이스를 사용하여 여러 VLAN 패킷을 전송합니다. 스위치는 트렁크 인터페이스를 통해 WAN 라우터에 연결되며 WAN 라우터는 VLAN 간 라우팅을 수행합니다. WAN 라우터는 인터넷에 연결됩니다. 모든 무선 장치가 WAP에 연결됩니다.

주요 기능

Cisco RV 라우터에서 제공하는 VLAN 간 라우팅 기능과 소규모 비즈니스 액세스 포인트에서 제공하는 무선 SSID 격리 기능을 결합하면 기존의 모든 Cisco 소규모 비즈니스 네트워크에서 무선 액세스를 위한 간단하고 안전한 솔루션을 제공합니다.

VLAN 간 라우팅

서로 다른 VLAN의 네트워크 디바이스는 VLAN 간에 트래픽을 라우팅하기 위해 라우터가 없으면 서로 통신할 수 없습니다. 소규모 비즈니스 네트워크에서 라우터는 유무선 네트워크 모두에 대해 VLAN 간 라우팅을 수행합니다. 특정 VLAN에 대해 VLAN 간 라우팅이 비활성화되면 해당 VLAN의 호스트는 다른 VLAN의 호스트 또는 디바이스와 통신할 수 없습니다.

무선 SSID 격리

무선 SSID 격리는 두 가지 유형이 있습니다. 무선 격리(SSID 내)가 활성화되면 동일한 SSID의 호스트가 서로를 볼 수 없게 됩니다. 무선 격리(SSID 간)가 활성화된 경우 한 SSID의 트래픽이 다른 SSID로 전달되지 않습니다.

IEEE 802.1x

IEEE 802.1x 표준은 이더넷 네트워크에 대한 인증된 네트워크 액세스를 제공하는 데 사용되는 포트 기반 네트워크 액세스 제어를 구현하는 데 사용되는 방법을 지정합니다. 포트 기반 인증은 포트에 연결된 사용자가 인증될 때까지 자격 증명 교환만 네트워크를 통과하도록 허용하는 프로세스입니다. 자격 증명이 교환되는 동안 포트가 제어되지 않는 포트라고 합니다. 인증이 완료된 후 포트를 제어 포트라고 합니다. 이는 단일 물리적 포트 내에 존재하는 2개의 가상 포트를 기반으로 합니다.

이렇게 하면 스위치 LAN 인프라의 물리적 특성을 사용하여 LAN 포트에 연결된 디바이스를 인증합니다. 인증 프로세스가 실패할 경우 포트에 대한 액세스를 거부할 수 있습니다. 이 표준은 원래 유선 이더넷 네트워크용으로 설계되었지만 802.11 무선 LAN에서 사용하도록 수정되었습니다.

RV320 구성

이 시나리오에서는 RV320이 네트워크의 DHCP 서버 역할을 수행하도록 해야 하므로 이를 설정하고 디바이스에서 별도의 VLAN을 구성해야 합니다. 시작하려면 이더넷 포트 중 하나에 연결하고 192.168.1.1으로 이동하여 라우터에 로그인합니다(라우터의 IP 주소를 아직 변경하지 않은 경우).

1단계. 웹 구성 유틸리티에 로그인하고 Port Management(포트 관리) > **VLAN Membership(VLAN 멤버십)**을 선택합니다. 새 페이지가 열립니다. 각기 다른 대상 고객을 나타내기 위해 3개의 개별 VLAN을 생성합니다. Add(추가)를 클릭하여 새 행을 추가하고 VLAN ID 및 설명을 편집합니다. 또한 VLAN이 이동해야 할 모든 인터페이스에서 *Tagged*로 설정되었는지 확인해야 합니다.

VLAN ID	Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4
<input type="checkbox"/> 1	Default	Disabled	Enabled	Untagged	Untagged	Untagged	Untagged
<input type="checkbox"/> 25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged
<input type="checkbox"/> 100	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged
<input type="text" value="10"/>	<input type="text" value="Wireless_MAIN"/>	Disabled	Enabled	Tagged	Tagged	Tagged	Tagged
<input type="text" value="20"/>	<input type="text" value="Wireless_GUEST"/>	Disabled	Enabled	Tagged	Tagged	Tagged	Tagged
<input type="text" value="30"/>	<input type="text" value="Wireless_ENGNRING"/>	Disabled	Enabled	Tagged	Tagged	Tagged	Tagged

2단계. 웹 구성 유틸리티에 로그인하고 DHCP 메뉴 > **DHCP Setup**을 선택합니다. DHCP Setup 페이지가 열립니다.

- VLAN ID 드롭다운 상자에서 주소 풀을 설정할 VLAN을 선택합니다(이 예에서는 VLAN 10, 20, 30).
- 이 VLAN에 대한 디바이스 IP 주소를 구성하고 IP 주소 범위를 설정합니다. 원하는 경우 여기에서 DNS 프록시를 활성화하거나 비활성화할 수 있으며 이는 네트워크에 따라 달라집니다. 이 예에서는 DNS 프록시가 DNS 요청을 전달하도록 작동합니다.
- Save(저장)를 클릭하고 각 VLAN에 대해 이 단계를 반복합니다.

DHCP Setup

IPv4 IPv6

VLAN Option 82

VLAN ID: 10

Device IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

DHCP Mode: Disable DHCP Server DHCP Relay

Remote DHCP Server: 0.0.0.0

Client Lease Time: 1440 min (Range: 5 - 43200, Default: 1440)

Range Start: 192.168.10.100

Range End: 192.168.10.149

DNS Server: Use DNS Proxy

Static DNS 1: 0.0.0.0

Static DNS 2: 0.0.0.0

WINS Server: 0.0.0.0

TFTP Server and Configuration Filename (Option 66/150 & 67):

TFTP Server Host Name:

TFTP Server IP: 0.0.0.0

Configuration Filename:

Save Cancel

3단계. 탐색 창에서 **Port Management(포트 관리) > 802.1x Configuration(802.1x 컨피그레이션)**을 선택합니다. 802.1X 구성 페이지가 열립니다.

- 포트 기반 인증을 활성화하고 서버의 IP 주소를 구성합니다.
- RADIUS Secret은 서버와 통신하는 데 사용되는 인증 키입니다.
- 이 인증을 사용할 포트를 선택하고 Save(저장)를 클릭합니다.

802.1X Configuration

Configuration

Port-Based Authentication

RADIUS IP:

RADIUS UDP Port:

RADIUS Secret:

Port Table

Port	Administrative State	Port State
1	Force Authorized	Link Down
2	Force Authorized	Link Down
3	Force Authorized	Link Down
4	Force Authorized	Authorized

Save Cancel

SX300 구성

SG300-10MP 스위치는 실제 네트워크 환경을 시뮬레이션하기 위해 라우터와 WAP321 간의 중간 역할을 합니다. 스위치의 구성은 다음과 같습니다.

1단계. 웹 컨피그레이션 유틸리티에 로그인하고 **VLAN Management(VLAN 관리) > Create VLAN(VLAN 생성)**을 선택합니다. 새 페이지가 열립니다.

2단계. **추가**를 클릭합니다. 새 창이 나타납니다. VLAN ID와 VLAN 이름을 입력합니다(섹션 1의 설명과 동일하게 사용). Apply(적용)를 클릭한 다음 VLAN 20 및 30에 대해 이 단계를 반복합니다.

VLAN

VLAN ID: (Range: 2 - 4094)

VLAN Name: (13/32 Characters Used)

Range

* VLAN Range: - (Range: 2 - 4094)

Apply Close

3단계. 탐색 창에서 **VLAN Management > Port to VLAN**을 선택합니다. 새 페이지가 열립니다.

- 페이지 상단에서 추가 중인 VLAN에 "VLAN ID equals to(VLAN ID equals to)"를 설정한 다음 (이 경우 VLAN 10) 오른쪽에서 **Go(이동)**를 클릭합니다. 그러면 해당 VLAN에 대한 설정으로 페이지가 업데이트됩니다.
- VLAN 10이 "Excluded(제외)" 대신 "Tagged(태그 지정)"가 되도록 각 포트의 설정을 변경합니다. VLAN 20 및 30에 대해 이 단계를 반복합니다.

Port to VLAN

Filter: VLAN ID equals to AND Interface Type equals to

Interface	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10
Access	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trunk	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
General	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Customer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Excluded	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tagged	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Untagged	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multicast TV VLAN	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PVID	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4단계. 탐색 창에서 **Security > Radius**를 선택합니다. RADIUS 페이지가 열립니다.

- RADIUS 서버에서 사용할 액세스 제어 방법(관리 액세스 제어 또는 포트 기반 인증)을 선택합니다. Port Based Access Control(포트 기반 액세스 제어)을 선택하고 Apply(적용)를 클릭합니다.
- 인증할 새 서버를 추가하려면 페이지 하단에 **Add**를 클릭합니다.

RADIUS

RADIUS Accounting for Management Access can only be enabled when TACACS+ Accounti

RADIUS Accounting: Port Based Access Control (802.1X, MAC Based)
 Management Access
 Both Port Based Access Control and Management Access
 None

5단계. 표시되는 창에서 서버의 IP 주소를 구성합니다(이 경우 192.168.1.32). 서버에 대한 우선순위를 설정해야 하지만 이 예에서는 우선 순위를 인증할 서버가 하나만 있으므로 중요하지 않습니다. 선택할 RADIUS 서버가 여러 개 있는 경우 이는 중요합니다. 인증 키를 구성하고 나머지 설정은 기본값으로 둘 수 있습니다.

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface:

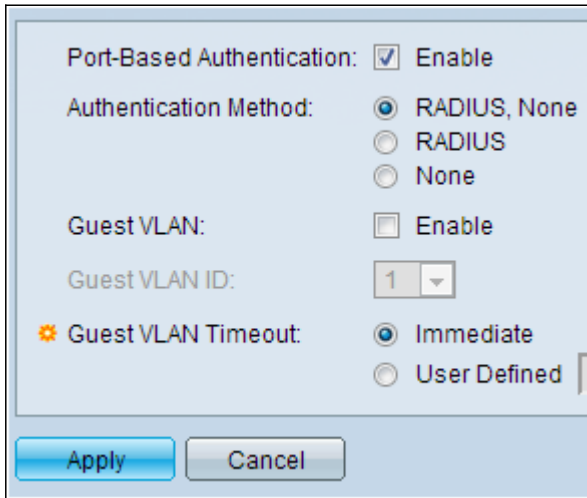
✳ Server IP Address/Name:

✳ Priority: (Range: 0 - 65535)

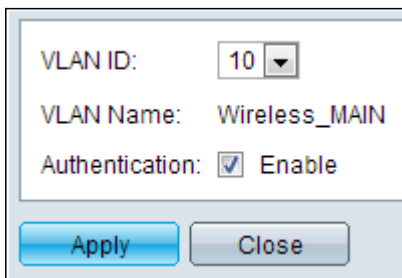
Key String: Use Default
 User Defined (Encrypted)
 User Defined (Plaintext)

6단계. 탐색 창에서 **Security > 802.1X > Properties**를 선택합니다. 새 페이지가 열립니다.

- 802.1x 인증을 켜고 인증 방법을 선택하려면 Enable(활성화)을 선택합니다. 이 경우 RADIUS 서버를 사용하고 있으므로 첫 번째 또는 두 번째 옵션을 선택합니다.
- Apply를 클릭합니다.



7단계. VLAN 중 하나를 선택하고 Edit(수정)를 클릭합니다. 새 창이 나타납니다. Enable(활성화)을 선택하여 해당 VLAN에 대한 인증을 허용하고 Apply(적용)를 클릭합니다. 각 VLAN에 대해 반복합니다.



WAP321 구성

VAP(Virtual Access Point)는 무선 LAN을 이더넷 VLAN과 동일한 무선 기능인 여러 브로드캐스트 도메인으로 분할합니다. VAP는 하나의 물리적 WAP 디바이스에서 여러 액세스 포인트를 시뮬레이션합니다. WAP121에서는 최대 4개의 VAP가 지원되며 WAP321에서는 최대 8개의 VAP가 지원됩니다.

각 VAP는 VAP0을 제외하고 독립적으로 활성화하거나 비활성화할 수 있습니다. VAP0은 물리적 라디오 인터페이스이며 라디오가 활성화된 한 계속 활성화됩니다. VAP0의 작업을 비활성화하려면 라디오 자체를 비활성화해야 합니다.

각 VAP는 사용자가 구성한 SSID(Service Set Identifier)로 식별됩니다. 여러 VAP는 동일한 SSID 이름을 가질 수 없습니다. SSID 브로드캐스트는 각 VAP에서 독립적으로 활성화하거나 비활성화할 수 있습니다. SSID 브로드캐스트는 기본적으로 활성화되어 있습니다.

1단계. 웹 구성 유틸리티에 로그인하고 **무선 > 라디오**를 선택합니다. *라디오* 페이지가 열립니다.

- 무선 라디오를 활성화하려면 Enable 확인란을 클릭합니다.
- 저장을 클릭합니다. 그러면 라디오가 켜집니다.

Radio

Global Settings

TSPEC Violation Interval:

Basic Settings

Radio: Enable

MAC Address: CC:EF:48:87:49:78

Mode:

Channel Bandwidth:

Primary Channel:

Channel:

2단계. 탐색 창에서 **Wireless > Networks**를 선택합니다. 네트워크 페이지가 열립니다.

Networks

Virtual Access Points (SSIDs)

VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="Cisco1"/>	<input checked="" type="checkbox"/>	<input type="text" value="WPA Personal"/>	<input type="text" value="Disabled"/>	<input type="checkbox"/>
Show Details							
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="2"/>	<input type="text" value="Cisco2"/>	<input checked="" type="checkbox"/>	<input type="text" value="WPA Personal"/>	<input type="text" value="Disabled"/>	<input type="checkbox"/>
Show Details							
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="3"/>	<input type="text" value="Cisco3"/>	<input checked="" type="checkbox"/>	<input type="text" value="WPA Personal"/>	<input type="text" value="Disabled"/>	<input type="checkbox"/>
Show Details							

참고: VAP0의 기본 SSID는 ciscosb입니다. 생성된 모든 추가 VAP에는 빈 SSID 이름이 있습니다. 모든 VAP의 SSID는 다른 값으로 구성할 수 있습니다.

3단계. 각 VAP는 VLAN과 연결되며, VLAN ID(VID)로 식별됩니다. VID는 1에서 4094 사이의 값일 수 있습니다(포함). WAP121은 5개의 활성 VLAN을 지원합니다(WLAN의 경우 4개, 관리 VLAN 1개). WAP321은 9개의 활성 VLAN을 지원합니다(WLAN의 경우 8개 + 관리 VLAN 1개).

기본적으로 WAP 디바이스의 컨피그레이션 유틸리티에 할당된 VID는 1이며, 이는 태그가 지정되지 않은 기본 VID이기도 합니다. 관리 VID가 VAP에 할당된 VID와 동일한 경우 이 특정 VAP와 연결된 WLAN 클라이언트가 WAP 디바이스를 관리할 수 있습니다. 필요한 경우 WLAN 클라이언트에서 관리를 비활성화하기 위해 ACL(Access Control List)을 생성할 수 있습니다.

이 화면에서 다음 단계를 수행해야 합니다.

- SSID를 수정하려면 왼쪽에 있는 확인 표시 버튼을 클릭합니다.
- VLAN ID 상자에 VLAN ID에 필요한 값을 입력합니다.
- SSID를 입력한 후 Save(저장) 버튼을 클릭합니다.

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	10	Wireless_MAIN	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	Show Details	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	20	Wireless_GUEST	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	Show Details	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	30	Wireless_ENGNRING	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	Show Details	

4단계. 탐색 창에서 **System Security > 802.1X Supplicant**를 선택합니다. 802.1X 신청자 페이지가 열립니다.

- Administrative Mode 필드에서 Enable(활성화)을 선택하여 디바이스가 802.1X 인증에서 신청자로 작동하도록 합니다.
- EAP Method 필드의 드롭다운 목록에서 적절한 유형의 EAP(Extensible Authentication Protocol) 방법을 선택합니다.
- 액세스 포인트가 802.1X 인증자로부터 인증을 얻기 위해 사용하는 사용자 이름과 비밀번호를 Username and Password 필드에 입력합니다. 사용자 이름과 비밀번호의 길이는 1자~64자의 영숫자 및 기호 문자여야 합니다. 인증 서버에 이미 구성되어 있어야 합니다.
- Save(저장)를 클릭하여 설정을 저장합니다.

802.1X Supplicant

Supplicant Configuration

Administrative Mode: Enable

EAP Method: MD5

Username: example-username (Range: 1 - 64 Characters)

Password: ***** (Range: 1 - 64 Characters)

Certificate File Status

Certificate File Present: Yes

Certificate Expiration Date: Dec 26 18:43:36 2019 GMT

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP TFTP

Filename: No file chosen

참고: Certificate File Status(인증서 파일 상태) 영역에는 인증서 파일이 있는지 여부가 표시됨

니다. SSL 인증서는 웹 브라우저가 웹 서버와 안전하게 통신할 수 있도록 하는 인증 기관에서 디지털 서명 인증서입니다. SSL 인증서를 관리 및 구성하려면 [WAP121 및 WAP321 액세스 포인트의 SSL\(Secure Socket Layer\) 인증서 관리](#) 문서를 참조하십시오.

5단계. 탐색 창에서 **Security > RADIUS Server**를 선택합니다. RADIUS Server 페이지가 열립니다. 매개변수를 입력하고 Radius Server 매개변수를 입력한 후 **Save(저장)** 버튼을 클릭합니다.

RADIUS Server

Server IP Address Type: IPv4
 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)

Server IP Address-2: (xxx.xxx.xxx.xxx)

Server IP Address-3: (xxx.xxx.xxx.xxx)

Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)

Key-2: (Range: 1 - 64 Characters)

Key-3: (Range: 1 - 64 Characters)

Key-4: (Range: 1 - 64 Characters)

RADIUS Accounting: Enable