VoIP 네트워크

네트워크 요구 사항

전화기가 네트워크에서 엔드포인트로 올바르게 작동하려면, 네트워크가 다음과 같은 요구 사항을 충족해야 합니다.

- VoIP 네트워크
  - VoIP는 Cisco 라우터와 게이트웨이에 구성됩니다.
  - Cisco Unified Communications Manager가 네트워크에 설치되어 있으며 통화를 처리하도록 구성되어 있습니다.
- DHCP 또는 IP 주소, 게이트웨이 및 서브넷 마스크 수동 할당을 지원하는 IP 네트워크

참고 전화기가 Cisco Unified Communications Manager의 날짜와 시간을 표시합니다. 사용자가 설정 애플리케이션에서 자동 날짜 및 시간을 끈 경우 시간이 서버 시간과 동기화되지 않을 수 있습니다.

네트워크 프로토콜

Cisco 무선 IP 전화기 8821 및 8821-EX는 음성 통신에 필요한 여러 업계 표준 및 Cisco 네트워크 프로토콜을 지원합니다. 다음 표에는 전화기에서 지원하는 네트워크 프로토콜에 대한 개요가 나와 있습니다.

표 *1:* 지원되는 네트워크 프로토콜

네트워크 프로토콜	목적	사용 참고 사항
블루투스	블루투스는 짧은 거리에서 장치가 통신하는 방식을 지정하는 무선 개인 영역 네트워크(WPAN) 프로토콜입니다.	전화기는 블루투스 4.0을 지원합니다.
BootP(Bootstrap Protocol)	BootP는 Cisco IP 전화기와 같은 네트워크 장치를 활성화하여 IP 주소와 같은 특정 시작 정보를 확인합니다.	없음
CAST(Cisco Audio Session Tunnel)	CAST 프로토콜을 통해 Cisco IP 전화기와 전화기의 관련 애플리케이션은 Cisco Unified Communications Manager(CM)와 게이트웨이 같은 일반적인 시그널링 구성 요소를 변경하지 않고 원격 IP 전화기를 찾아 통신할 수 있습니다.	전화기는 Cisco IP 전화기를 SIP 프록시로 사용하며 CAST를 CUVA 및 Cisco Unified Communications Manager 간의 인터페이스로 사용합니다.
CDP (Cisco 탐색 프로토콜)	CDP는 모든 Cisco 제조 장비에서 실행되는 장치 검색 프로토콜입니다. 장치는 CDP를 사용하여 해당 장치의 존재 여부를 다른 장치에 알리고 네트워크에 있는 다른 장치에 대한 정보를 수신할 수 있습니다.	전화기는 CDP를 사용하여 보조 VLAN ID, 포트별 전원 관리 세부 정보 및 QoS(Quality of Service) 구성 정보 같은 정보를 Cisco Catalyst 스위치와 주고받을 수 있습니다.
CPPDP(Cisco Peer-to-Peer Distribution Protocol)	CPPDP는 장치의 피어 투 피어 계층 구조를 형성하는 데 사용되는 Cisco의 독점적 프로토콜입니다. 이 계층 구조는 피어 장치에서 주변 장치로 펌에어 파일을 배포하는 데 사용됩니다.	CPPDP는 피어 펌웨어 공유 기능에 사용됩니다.
DHCP(Dynamic Host Configuration Protocol)	DHCP는 네트워크 장치에 IP 주소를 역동적으로 할당합니다. DHCP를 사용하면 네트워크 IP 전화기를 연결하고, 수동으로 IP 주소를 할당하거나 추가 네트워크 매개 변수를 구성하지 않고도 전화기를 작동시킬 수 있습니다.	DHCP는 기본값으로 활성화됩니다. 비활성화된 경우에는 로컬에서 각 전화기에 IP 주소, 서브넷 마스크, 게이트웨이 및 TFTP 서버를 수동으로 구성해야 합니다. DHCP 사용자 정의 옵션 150을 사용하는 것이 좋습니다. 이 방법을 사용하여 TFTP 서버 IP 주소를 옵션 값으로 구성합니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오. 참고 옵션 150을 사용할 수 없다면, DHCP 옵션 66을 사용해 볼 수 있습니다.

네트워크 프로토콜	목적	사용 참고 사항
HTTP(Hypertext Transfer Protocol)	HTTP는 인터넷 및 웹 상에서 정보 교환 및 문서 이동을 위해 사용하는 표준 경로입니다.	전화기는 XML 서비스와 문제 해결을 위해 HTTP를 사용합니다.
HTTPS(Hypertext Transfer Protocol Secure)	HTTPS(Hypertext Transfer Protocol Secure)는 HTTP(Hypertext Transfer Protocol)와 SSL/TLS 프로토콜의 조합으로 서버에 암호화 및 보안 식별 기능을 제공합니다.	HTTP와 HTTPS가 모두 지원되는 웹 애플리케이션에는 2개의 URL이 구성됩니다. HTTPS를 지원하는 전화기는 HTTPS URL을 선택합니다.
IEEE 802.1X	IEEE 802.1X 표준은 클라이언트 서버 기반 액세스 제어 및 개방형 액세스 포트를 통한 LAN 연결에서 인증받지 못한 클라이언트를 제한하는 인증 프로토콜을 정의합니다. 클라이언트가 인증될 때까지, 802.1X 액세스 제어는 클라이언트가 연결된 포트를 통해 오직 EAPOL(Extensible Authentication Protocol over LAN) 트래픽만 허용합니다. 인증에 성공하면 정상적인 트래픽은 포트를 통과할 수 있습니다.	전화기는 다음 인증 방식을 지원하여 IEEE 802.1X 표준을 구현합니다. • EAP-FAST • EAP-TLS • PEAP-GTC • PEAP-MSCHAPV2
IEEE 802.11n/802.11ac	IEEE 802.11 표준은 무선 근거리망(WLAN) 상에서 장치의 통신 방법을 지정합니다.	802.11n은 2.4GHz 및 5GHz 대역에서 작동합니다. 802.11ac는 5GHz 대역에서 작동합니다.
IP(Internet Protocol)	IP는 네트워크를 통해 패킷을 처리하고 전송하는 메시징 프로토콜입니다.	IP를 사용하여 통신하기 위해서는 네트워크 장치에 IP 주소, 서브넷 및 게이트웨이가 있어야 합니다. IP 주소, 서브넷 및 게이트웨이 ID는 전화기에서 DHCP(Dynamic Host Configuration Protocol)를 사용하고 있는 경우 자동으로 할당됩니다. DHCP를 사용하지 않는다면 로컬에서 각 전화기에 수동으로 이러한 속성을 할당해야 합니다. 전화기에서 IPv6을 지원하지 않습니다.
RTP(Real-Time Transport Protocol)	RTP는 데이터 네트워크상에서 대화형 음성과 같은 실시간 데이터를 전송하기 위한 표준 프로토콜입니다.	전화기는 RTP 프로토콜을 사용하여 다른 전화기 및 게이트웨이와 실시간 음성 통신을 주고받습니다.
RTCP(Real-Time Control Protocol)	RTCP는 RTP와 함께 작동하여 RTP 스트림에 대한 QoS 데이터(예: 지터, 대기 시간 및 왕복 지연)를 제공합니다.	RTCP는 기본적으로 활성화됩니다.

네트워크 프로토콜	목적	사용 참고 사항
SDP(Session Description Protocol)	SDP는 두 엔드포인트 간 연결 중 사용할 수 있는 매개 변수를 판별하는 SIP 프로토콜의 부분입니다. 전화회의는 전화회의의 모든 엔드포인트가 지원하는 SDP 기능만을 사용하여 설정됩니다.	코덱 유형, DTMF 탐지 및 통신 소음과 같은 SDP 기능은 일반적으로 작동 중인 Cisco Unified Communications Manager 또는 Media Gateway에 의해 전역으로 구성됩니다. 일부 SIP 엔드포인트에서는 엔드포인트 자체에 이러한 매개 변수의 구성을 허용할 수 있습니다.
SIP(Session Initiation Protocol)	SIP는 IP를 통해 멀티미디어 전화 회의를 진행할 때 사용하는 인터넷 IETF(Engineering Task Force) 표준입니다. SIP는 2개 이상의 엔드포인트 간에 통화를 연결, 유지, 종료할 때 사용할 수 있는 ASCII 기반의 애플리케이션 레이어 프로토콜(RFC 3261 정의 내용)입니다.	다른 VoIP 프로토콜처럼 SIP는 패킷 텔레포니 네트워크 내에서 시그널링 및 세션 관리 기능을 처리합니다. 시그널링을 사용하여 네트워크 경계를 넘어서 통화 정보를 전송할 수 있습니다. 세션 관리는 엔드 투 엔드 통화 속성 제어 기능을 제공합니다.
TCP(Transmission Control Protocol)	TCP는 연결 지향형 전송 프로토콜입니다.	전화기는 TCP를 사용하여 Cisco Unified Communications Manager에 연결하고 XML 서비스에 액세스합니다.
TLS(Transport Layer Security)	TLS는 통신 보안 및 인증을 위한 표준 프로토콜입니다.	보안이 적용 중일 때, 전화기는 Cisco Unified Communications Manager에 안전하게 등록한 후 TLS 프로토콜을 사용합니다.
TFTP(Trivial File Transfer Protocol)	TFTP를 사용하면 네트워크상에서 파일을 전송할 수 있습니다. Cisco IP 전화기에서 TFTP는 전화기 유형에 맞는 구성 파일을 확보할 수 있게 해줍니다.	TFTP의 경우 DHCP 서버가 자동으로 식별할 수 있는 TFTP 서버가 네트워크에 필요합니다. 전화기에서 DHCP 서버가 지정한 것이 아닌 다른 TFTP 서버를 사용하려면, 전화기의 네트워크 구성 메뉴를 사용해 해당 TFTP 서버의 IP 주소를 수동으로 할당해야 합니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
사용자 데이터그램 프로토콜	UDP는 데이터 패킷 전달을 위한 연결 메시징 프로토콜입니다.	전화기는 신호 처리를 위해 UDP를 사용합니다.

관련 항목

설정 메뉴에서 전화기 네트워크를 수동으로 설정
Cisco Unified Communications Manager 상호 작용, 15 페이지
WLAN 통신을 위한 802.11 표준, 9 페이지
시작 순서

Cisco 무선 IP 전화기 882x 구축 설명서

Cisco 무선 *IP* 전화기 *882x* 구축 설명서에는 Wi-Fi 환경의 무선 전화기에 대한 유용한 정보가 포함되어 있습니다. 구축 설명서 위치:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

무선랜

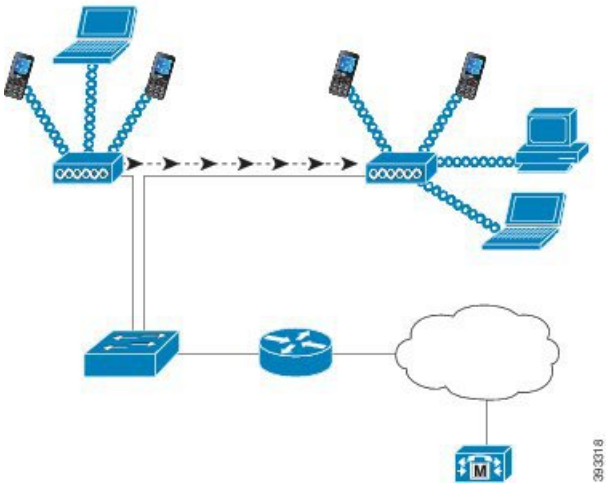
참고 Cisco 무선 IP 전화기 8821 및 8821-EX 배포 및 구성에 대한 자세한 지침은 *Cisco* 무선 *IP* 전화기 *8821 Series* 구축 설명서를 참조하십시오.

무선 기능이 있는 장치는 회사 WLAN 내에서 음성 통신을 제공할 수 있습니다. 장치는 무선 AP(액세스 포인트) 및 Cisco Unified Communications Manager Administration을 비롯한 주요 Cisco IP 전화 통신 구성 요소를 사용하고 상호 작용하며 무선 음성 통신을 제공합니다.

무선 전화기는 802.11a, 802.11b, 802.11g 및 802.11n Wi-Fi를 사용할 수 있는 Wi-Fi 기능을 갖추고 있습니다.

다음 그림에서는 무선 IP 전화 통신용 음성 무선 전송이 가능한 일반적인 WLAN 토폴로지를 보여줍니다.

그림 *1:* 일반적인 ***WLAN*** 토폴로지



전화기는 전원이 켜지면 장치 무선 액세스가 켜짐으로 설정된 경우 우선 AP를 찾고 연결합니다. 기억된 네트워크 범위 내에 없는 경우 브로드캐스트된 네트워크를 선택하거나 수동으로 네트워크를 추가할 수 있습니다.

AP는 유선 네트워크 연결을 사용하여 스위치 및 라우터와 데이터 및 음성 패킷을 송수신합니다. 음성 신호는 통화 처리 및 라우팅을 위해 통화 제어 서버로 전송됩니다.

AP는 네트워크에 대한 무선 링크 또는 핫스폿을 제공하므로 WLAN에서 가장 중요한 구성 요소입니다. 일부 WLAN에서는 각 AP가 LAN 상에 구성된 Cisco Catalyst 3750과 같은 이더넷 스위치로 유선 연결됩니다. 스위치는 게이트웨이에 대한 액세스와 무선 IP 전화 통신을 지원하기 위한 통화 제어 서버에 대한 액세스를 제공합니다.

일부 네트워크에는 무선 구성 요소를 지원하는 유선 구성 요소가 포함됩니다. 유선 구성 요소는 스위치, 라우터, 무선 기능을 활성화하는 특수 모듈을 장착한 브리지로 구성될 수 있습니다.

Cisco Unified 무선 네트워크에 대한 자세한 내용은 https://www.cisco.com/c/en/us/products/wireless/index.html를 참조하십시오.

Wi-Fi 네트워크 컴포넌트

전화기가 정상적으로 전화를 걸고 받으려면 WLAN 상의 여러 네트워크 컴포넌트와 상호작용해야 합니다.

AP 채널 및 도메인 관계

AP(액세스 포인트)는 2.4GHz 또는 5GHz 주파수 대역 내의 채널을 통해 RF 신호 송수신합니다. 안정적인 무선 환경을 제공하고 채널 간섭을 줄이려면 각 AP에 겹치지 않는 채널을 지정해야 합니다.

AP 채널 및 도메인 관계에 대한 자세한 정보는 *Cisco* 무선 *IP* 전화기 *8821 Series* 구축 설명서에서 "음성을 위한 무선 LAN 설계" 섹션을 참조하십시오.

AP 상호 작용

무선 전화기는 무선 데이터 장치와 동일한 AP를 사용합니다. 그러나 WLAN 통한 음성 통신에는 데이터 통신 전용의 WLAN과는 다른 장비 구성과 레이아웃이 필요합니다. 데이터 전송은 음성 전송보다 높은 수준의 RF 노이즈, 패킷 손실 및 채널 경합을 허용할 수 있습니다. 음성 전송 중에 패킷이 손실되면 오디오 잡음이나 손상이 발생하여 통화가 들리지 않을 수 있습니다. 패킷 오류 또한 영상 끊어짐이나 품질 저하의 원인입니다.

무선 전화기 사용자는 통화 중에 캠퍼스나 건물의 층 사이를 이동하는 경우가 많습니다. 이와 대조적으로, 데이터 사용자는 한 곳에 있거나 가끔씩 다른 곳으로 이동합니다. 통화를 유지하면서 로밍하는 기능은 무선 음성 통신의 장점이므로 RF 적용 범위가 계단, 엘리베이터, 회의실 구석, 복도 등을 모두 포함할 수 있어야 합니다.

좋은 음성 품질과 최적의 RF 신호 적용 범위를 보장하려면 현장 조사를 해야 합니다. 현장 조사로 무선 음성에 적절한 설정을 확인하고 AP 배치, 파워 수준, 채널 할당 등, WLAN 설계와 레이아웃에 도움이 되는 정보를 얻을 수 있습니다.

무선 음성을 배포하고 사용을 시작한 후에도 설치 후 현장 조사를 계속해야 합니다. 새 사용자 그룹 추가, 더 많은 장치 설치 또는 대량의 재고 추가와 같은 작업도 무선 환경을 변경합니다. 설치 후 현장 조사는 AP 적용 범위가 최적의 음성 통신에 적합한지 확인합니다.

참고 로밍 중에는 패킷 손실이 발생하지만, 손실되는 패킷의 수는 보안 모드와 고속 로밍의 존재 여부에 따라 결정됩니다. 고속 로밍을 활성화하기 위해 CCKM(Cisco Centralized Key Management)을 구현하는 것이 좋습니다.

음성 QoS에 대한 자세한 내용은 *Cisco* 무선 *IP* 전화기 *8821 Series* 구축 설명서의 내용을 참조하십시오.

액세스 포인트 연결

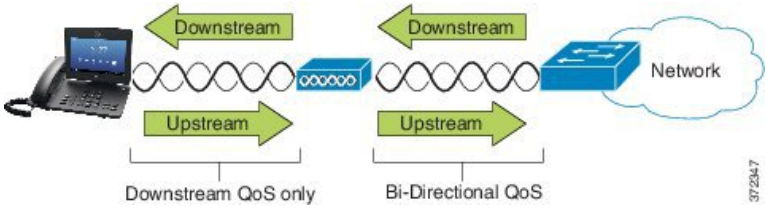
전화기는 시작할 때 SSID와 암호화 유형을 인식하는 AP를 검색합니다. 전화기는 해당하는 AP의 목록을 작성 및 유지 관리하고 현재 구성을 바탕으로 최적의 AP를 선택합니다.

무선 네트워크 상의 **QoS**

무선 LAN 상의 음성 및 비디오 통신은 지연, 지터 및 패킷 손실에 취약합니다. 이러한 문제는 데이터 사용자에게는 영향을 주지 않지만, 음성이나 영상 통화에 심각한 영향을 줄 수 있습니다. 음성과 비디오 통신을 시기 적절하게 전송하고 지연과 지터를 줄이려면 QoS(Quality of Service)를 사용해야 합니다.

장치를 음성 VLAN으로 분리하고 음성 패킷을 높은 QoS로 표시하면 음성 트래픽에 데이터 트래픽보다 높은 우선 순위를 부여하여 패킷 지연과 손실을 줄일 수 있습니다.

전용 대역폭이 있는 유선 네트워크와 달리, 무선 LAN은 QoS를 구현할 때 트래픽 방향을 고려해야 합니다. 트래픽은 다음 그림에 나오는 AP를 기준으로 업스트림 또는 다운스트림으로 분류됩니다.



QoS의 EDCF(Enhanced Distributed Coordination Function) 유형은 다운스트림용(802.11b/g 클라이언트 방향)으로 8개의 대기열 QoS를 가집니다. 다음의 옵션에 따라 대기열을 할당할 수 있습니다.

- 패킷에 대한 QoS 또는 DSCP(Differentiated Services Code Point) 설정
- 레이어 2 또는 레이어 3 액세스 목록
- 특정 트래픽용 VLAN
- 장치의 동적 등록

AP에서 최대 8개의 대기열을 설정할 수 있지만, QoS에서 최상의 결과를 얻으려면 음성, 영상 및 트래픽 신호에 대해 3개의 대기열만 사용해야 합니다. 음성은 음성 대기열(UP6), 영상은 영상 대기열(UP5), 신호(SIP) 트래픽은 영상 대기열(UP4), 그리고 데이터 트래픽은 최선 노력 대기열(UP0)에 배치합니

다. 802.11b/g EDCF가 음성 트래픽을 데이터 트래픽으로부터 완전하게 보호하지는 못하지만 이 대기열 모델을 사용하면 통계적으로 최적의 결과를 얻을 수 있습니다.

대기열은 다음과 같습니다.

- 최선 노력(BE) - 0, 3
- 배경(BK) - 1, 2
- 영상(VI) - 4, 5
- 음성(VO) - 6, 7

참고 장치는 SIP 신호 패킷을 DSCP 값 24(CS3)로 표시하고 RTP 패킷을 DSCP 값 46(EF)으로 표시합니다.

참고 통화 제어(SIP는) UP4(VI)로 전송됩니다. 영상은 영상에 대한 ACM(Admission Control Mandatory)이 비활성화된 경우(트래픽 사양[TSpec] 비활성화) UP5(VI)로 전송됩니다. 음성은 음성에 대한 ACM이 비활성화된 경우(TSpec 비활성화) UP6(VO)로 전송됩니다.

다음 표에 나오는 QoS 프로파일은 AP에서 음성, 영상 및 통화 제어(SIP) 트래픽에 우선 순위를 둡니다.

표 ***2: QoS*** 프로파일과 인터페이스 설정

트래픽 유형	**DSCP**	**802.1p**	**WMM UP**	포트 범위
음성	EF (46)	5	6	UDP 16384-32767
대화식 영상	AF41 (34)	4	5	UDP 16384-32767
통화 제어	CS3 (24)	3	4	TCP 5060-5061

일관적이지 않은 환경에서 음성 전송의 신뢰성을 개선하기 위해, 장치는 IEEE 802.11e 업계 표준과 WMM(Wi-Fi Multimedia)을 지원합니다. WMM은 음성, 영상, 최선 노력 데이터 및 기타 트래픽에 대해 차별화된 서비스를 가능하게 합니다. 이러한 차별화된 서비스가 음성 패킷을 위해 충분한 QoS를 제공할 수 있도록, 동시에 일정한 양의 음성 대역폭에 대해서만 서비스하거나 한 채널에서 허용할 수 있습니다. 네트워크가 예약된 대역폭으로 "N"개의 음성 통화를 처리할 수 있고 음성 트래픽의 양이 이 제한을 초과하는 경우(N+1 통화) 모든 통화의 품질이 저하됩니다.

통화 품질 문제를 해결하려면 초기 CAC(Call Admission Control) 체계가 필요합니다. WLAN에서 SIP CAC를 활성화하면, AP에 구성된 한계를 초과하지 않도록 활성 음성 통화의 수를 제한하는 네트워크 과부하 시나리오가 QoS를 유지 관리합니다. 네트워크 정체 중에는 시스템이 작은 대역폭을 예약하여 AP가 "전용량"으로 사용되더라도 무선 장치 클라이언트가 인접한 AP로 로밍할 수 있도록 합니다. 음성 대역폭 한도에 도달하면 해당 채널의 기존 통화 품질에 영향을 미치지 않도록 다음 통화가 인접한 AP로 로드 밸런싱됩니다.

전화기는 SIP 통신을 위해 TCP를 사용하며 AP가 전용량으로 작동 중이면 통화 제어 시스템 등록이 손실될 수 있습니다. CAC를 통해 "인증"하지 않은 클라이언트가 전송 또는 수신하는 프레임이 삭제되어 통화 제어 시스템 등록이 해제될 수 있습니다. 따라서 SIP CAC는 비활성화하는 것이 좋습니다.

유연한 DSCP 설정

프로시저

단계 1 Cisco 통합 커뮤니케이션 매니저 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 2 클러스터 파라미터(시스템 - 위치 및 지역)에서 몰입형 영상 통화용 비디오 대역폭 풀 사용을 거짓으로 설정합니다.

단계 3 클러스터 파라미터(통화 허용 제어)에서 영상 통화 QoS 표시 정책을 몰입형으로 승격으로 설정합니다.

단계 4 변경 내용을 저장합니다.

WLAN 통신을 위한 802.11 표준

무선 LAN은 모든 이더넷 기반 무선 트래픽을 제어하는 IEEE(Institute of Electrical and Electronics Engineers) 802.11 표준을 따라야 합니다. 무선 전화기는 다음 표준을 지원합니다.

- 802.11a: 더 많은 채널을 제공하며 OFDM 기술을 사용해 데이터 속도를 개선하는 5GHz 대역을 사용합니다. DFS(Dynamic Frequency Selection) 및 TPC(Transmit Power Control)는 이 표준을 지원합니다.
- 802.11b: 낮은 데이터 속도(1, 2, 5.5, 11Mbps)로 데이터를 송수신하기 위한 2.4GHz 무선 주파수(RF)를 지정합니다.
- 802.11d: 액세스 포인트가 현재 지원하는 무선 채널과 전송 파워 수준을 알릴 수 있게 합니다. 802.11d 지원 클라이언트는 해당 정보를 바탕으로 사용할 채널과 파워를 결정할 수 있습니다. 전화기가 해당 국가에서 허용되는 채널을 확인하려면 국제 모드(802.11d)가 필요합니다. 지원되는 채널에 대해서는 다음 표를 참조하십시오. Cisco IOS 액세스 포인트 또는 Cisco Unified 무선 LAN 컨트롤러에서 802.11d가 올바르게 구성되었는지 확인합니다.
- 802.11e: 무선 LAN 애플리케이션에 대한 QoS(Quality of Service) 향상의 품질 집합을 정의합니다.
- 802.11g: 802.11b와 동일하게 비인가 2.4GHz 대역을 사용하지만 OFDM(Orthogonal Frequency Division Multiplexing) 기술을 사용하여 데이터 속도를 높여줍니다. OFDM은 무선 주파수를 사용하여 신호를 전송하기 위한 물리 레이어 인코딩 기술입니다.
- 802.11h: 5GHz 스펙트럼과 전송 파워 관리를 지원합니다. 802.11a MAC(Media Access Control)으로 DFS 및 TPC를 제공합니다.
- 802.11i: 무선 네트워크를 위한 보안 메커니즘을 지정합니다.

- 802.11n: 최고 150Mpbs 속도의 데이터 송수신을 위해 2.4GHz 또는 5GHz 무선 주파수를 사용하며 MIMO(multiple input, multiple output), 채널 본딩, 페이로드 최적화를 활용하여 데이터 전송 속도를 향상합니다.

참고 무선 전화기에는 하나의 안테나가 있으며 MCS 0 ~ MCS 7 데이터 속도만(20MHz 채널에서 72Mbps 및 40MHz 채널에서 150Mbps) 지원하는 SISO(Single Input Single Output) 시스템을 사용합니다. 선택적으로, 802.11n 클라이언트가 높은 데이터 속도를 활용할 수 있는 MIMO 기술을 사용하는 경우 MCS 8 ~ MCS 15를 활성화할 수 있습니다.

- 802.11r: 빠른 보안 로밍을 위한 요구 사항을 지정합니다.
- 802.11ac: 5GHz 무선 주파수를 사용하여 최고 433Mbps 속도로 데이터를 송수신합니다.

표 ***3:*** 지원되는 채널

대역폭	사용 가능한 채널	채널 세트	채널 폭
2.412 - 2.472GHz	13	1 - 13	20 MHz
5.180 - 5.240GHz	4	36, 40, 44, 48	20, 40, 80MHz
5.260 - 5.320GHz	4	52, 56, 60, 64	20, 40, 80MHz
5. 500 - 5.700GHz	11	100 - 140	20, 40, 80MHz
5.745 - 5.825GHz	5	149, 153, 157, 161, 165	20, 40, 80MHz

참고 채널 120 124, 128은 미주, 유럽, 일본에서 지원되지 않지만 세계 다른 지역에서는 지원될 수 있습니다.

WLAN에서 지원되는 데이터 속도, 전송 파워, 수신 감도 등에 대해서는 *Cisco* 무선 *IP* 전화기 *8821 Series* 구축 설명서를 참조하십시오.

국제 모드(802.11d)

무선 전화기는 802.11d를 통해 사용할 채널과 송신 파워 수준을 결정합니다. 전화기는 연결된 AP에서 클라이언트 구성을 가져옵니다. 전화기를 국제 모드로 사용하려면 AP에서 국제 모드(802.11d)를 활성화합니다.

참고 주파수가 2.4GHz이며 현재 액세스 포인트가 1-11 채널로 송신하고 있다면 국제 모드(802.11d)를 활성화할 필요가 없을 수 있습니다.

이러한 주파수는 모든 국가에서 지원하므로 국제 모드(802.11d) 지원에 관계없이 이러한 채널을 검색할 수 있습니다.

국제 모드 활성화 및 2.4GHz 지원에 대한 자세한 내용은 *Cisco* 무선 *IP* 전화기 *8821 Series* 구축 설명서를 참조하십시오.

액세스 포인트가 위치한 해당 국가에 대해 국제 모드(802.11d)를 활성화합니다. Cisco Unified 무선 LAN 컨트롤러에서는 국제 모드가 자동으로 활성화됩니다.

무선 주파수 범위

WLAN 통신은 다음과 같은 RF(무선 주파수) 범위를 사용합니다.

- 2.4GHz—2.4GHz를 사용하는 많은 장치가 802.11b/g 연결을 방해할 가능성이 있습니다. 이러한 방해 때문에 802.11 전송이 실패하는 DoS(서비스 거부) 시나리오가 발생할 수 있습니다.
- 5GHz —이 범위는 UNII(Unlicensed National Information Infrastructure) 대역이라고 하는 여러 섹션으로 나뉘며, 각 대역에 4개의 채널이 있습니다. 2.4GHz가 제공하는 것보다 겹치지 않는 채널을 더 많이 제공하기 위해 20MHz 간격으로 채널이 배치됩니다.

WLAN에서 통신 보안

범위 내에 있는 모든 WLAN 장치는 다른 모든 WLAN 트래픽을 수신할 수 있으므로, WLAN에서는 음성 통신의 보안이 매우 중요합니다. 침입자가 음성 트래픽을 조작하거나 가로챌 수 없게 하기 위해 Cisco SAFE 보안 아키텍처는 무선 전화기 및 Cisco Aironet AP를 지원합니다. 네트워크의 보안에 대한 자세한 내용은 https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html을 참조하십시오.

인증 방법

Cisco Wireless IP 전화 통신 솔루션은 무선 전화기가 지원하는 다음 인증 방법을 사용하여 인증되지 않은 로그인 및 통신 저하를 방지하는 무선 네트워크 보안을 제공합니다.

- WLAN 인증
  - WPA(802.1x 인증 + TKIP 또는 AES 암호화)
  - WPA2(802.1x 인증 + AES 또는 TKIP 암호화)
  - WPA-PSK(사전 공유 키 + TKIP 암호화)
  - WPA2-PSK(사전 공유 키 + AES 암호화)

- EAP-FAST(Extensible Authentication Protocol − Flexible Authentication via Secure Tunneling)
- EAP-TLS(Extensible Authentication Protocol − Transport Layer Security)
- PEAP(Protected Extensible Authentication Protocol) MS-CHAPv2 및 GTC
- CCKM(Cisco Centralized Key Management)
- 공개(없음)

- WLAN 암호화
  - AES(Advanced Encryption Scheme)
  - TKIP / MIC(Temporal Key Integrity Protocol / Message Integrity Check)
  - WEP(Wired Equivalent Protocol) 40/64 및 104/128비트

참고 802.1x 인증 및 공유 키 인증을 사용하는 동적 WEP는 지원되지 않습니다.

인증 방법에 대한 자세한 내용은 *Cisco* 무선 *IP* 전화기 *8821 Series* 구축 설명서의 "무선 보안" 섹션을 참조하십시오.

인증된 키 관리

다음 인증 체계는 RADIUS 서버를 사용하여 인증 키를 관리합니다.

- WPA/WPA2: RADIUS 서버 정보를 사용하여 인증을 위한 고유 키를 생성합니다. 이러한 키는 중앙 집중식 RADIUS 서버에서 생성되므로, WPA/WPA2는 AP 및 장치에 저장된 WAP 사전 공유 키보다 더 강화된 보안을 제공합니다.
- CCKM(Cisco Centralized Key Management): RADIUS 서버와 무선 도메인 서버(WDS) 정보를 사용하여 키를 관리하고 인증합니다. WDS는 빠르고 안전한 재인증을 위해 CCKM 사용 가능 클라이언트 장치에 대한 보안 자격 증명 캐시를 만듭니다.

WPA/WPA2 및 CCKM을 사용할 때, 암호화 키는 장치에 입력되지 않고 AP와 장치 간에 자동으로 파생됩니다. 그러나 인증을 위해 사용되는 EAP 사용자 이름과 암호는 각 장치에 입력해야 합니다.

암호화 방법

음성 트래픽의 보안을 위해 무선 전화기는 암호화를 위한 WEP, TKIP 및 AES(Advanced Encryption Standard)를 지원합니다. 이러한 암호화 메커니즘을 사용하면 AP와 장치 간에 음성 RTP(Real-Time Protocol) 패킷이 암호화됩니다.

WEP

WEP가 무선 네트워크에서 사용되는 경우, 개방형 또는 공유 키 인증을 사용하여 AP에서 인증이 수행됩니다. 전화기에 설정된 WEP 키가 AP에 구성된 WEP 키와 일치해야 정상적으로 연결됩니

다. 전화기는 40비트 암호화 또는 128비트 암호화를 지원하며 장치와 AP에서 정적 상태로 유지됩니다.

TKIP

WPA 및 CCKM은 WEP보다 많이 향상된 TKIP 암호화를 사용합니다. TKIP는 암호화를 강화하는 패킷당 키 암호화 또는 더 긴 초기화 벡터(IV)를 제공합니다. 뿐만 아니라, MIC(Message Integrity Check)가 암호화된 패킷이 변경되지 않도록 합니다. TKIP는 침입자가 WEP 키를 해독하는 데 도움을 주는 WEP의 예측 가능성을 제거합니다.

AES

WPA2 인증을 위해 사용되는 암호화 방법입니다. 이 암호화 국가 표준은 암호화 및 암호 해독에 동일한 키를 가지는 대칭 알고리즘을 사용합니다.

암호화에 대한 자세한 내용은 *Cisco* 무선 *IP* 전화기 *8821 Series* 구축 설명서의 "무선 보안" 섹션을 참조하십시오.

AP 인증 및 암호화 옵션

인증 및 암호화 체계는 무선 LAN 내에서 설정됩니다. VLAN은 네트워크 및 AP에서 구성되고 다른 인증과 암호화의 조합을 지정합니다. SSID는 VLAN과 특정 인증 및 암호화 체계와 연결됩니다. 무선 전화기가 성공적으로 인증하기 위해서는 AP 및 전화기에서 해당 인증 및 암호화 체계를 포함하는 동일한 SSID를 구성해야 합니다.

참고

- WPA 사전 공유 키 또는 WPA2 사전 공유 키를 사용할 때 사전 공유 키가 정적으로 전화기에 설정되어야 합니다. 이러한 키는 AP에 있는 키와 일치해야 합니다.
- 무선 전화기는 자동 EAP 협상을 지원하지 않습니다. EAP-FAST 모드를 사용하려면 이 기능을 지정해야 합니다.

다음 표에서는 전화기가 지원하는 Cisco Aironet AP에 구성되는 인증 및 암호화 체계의 목록을 제공합니다. 표에서는 AP 구성에 상응하는 장치의 네트워크 구성 옵션을 보여줍니다.

표 *4:* 인증 및 암호화 체계

Cisco WLAN 구성			전화기 구성
인증	키 관리	일반 암호화	인증
열기	없음	없음	없음
정적 WEP	없음	WEP	WEP
EAP-FAST	WPA 또는 WPA2(선택적 CCKM 사용)	TKIP 또는 AES	802.1x EAP > EAP-FAST
PEAP-MSCHAPv2	WPA 또는 WPA2(선택적 CCKM 사용)	TKIP 또는 AES	802.1x EAP > PEAP > MSCHAPV2

Cisco WLAN 구성			전화기 구성
PEAP-GTC	WPA 또는 WPA2(선택적 CCKM 사용)	TKIP 또는 AES	802.1x EAP > PEAP > GTC
EAP-TLS	WPA 또는 WPA2(선택적 CCKM 사용)	TKIP 또는 AES	802.1x EAP > TLS
WPA/WPA2-PSK	WPA-PSK 또는 WPA2-PSK	TKIP 또는 AES	WPA/WPA2 PSK

자세한 내용은 *Cisco* 무선 *IP* 전화기 *8821 Series* 구축 설명서를 참조하십시오.

인증서

전화기는 다음 인증서를 지원합니다.

- EAP-TLS용 또는 WLAN 인증을 위해 PEAP + 서버 검증을 활성화하기 위한 X.509 디지털 인증서
- 인증 등록 및 자동 갱신을 위한 SCEP(Simple Certificate Enrollment Protocol)
- 1024, 2048, 4096비트 키
- SHA-1 및 SHA-256 서명 유형
- DER 및 Base-64(PEM) 인코딩 유형
- 개인 키를 포함하는 PKCS #12 형식(.p12 또는 .pfx 확장자)의 사용자 설치 인증서.
- .crt 또는 .cer 확장자를 가지는 서버(루트 CA) 인증서

다음 방법 중 하나로 전화기에 인증서를 설치합니다.

- 관리 웹 페이지를 사용합니다. 자세한 내용은 Cisco IP 전화기 관리 페이지의 내용을 참조하십시오.
- SCEP 서버를 사용하여 인증서를 관리하고 설치합니다. 자세한 정보는 다음을 참조하십시오. SCEP 설정

사용자가 자신의 전화기를 직접 설정하고 각 전화기에 인증서가 필요한 경우 사용자들에게 기타 구성 설정을 제공할 때 인증서 유형을 제공해야 합니다. 인증서 설치를 위해 SCEP를 사용하지 않으면 직접 인증서를 설치해야 합니다.

WLAN 및 로밍

무선 전화기는 WDS(무선 도메인 서버) 상의 세션 자격 증명의 캐시를 제공하는 중앙 집중식 키 관리 프로토콜인 CCKM(Cisco Centralized Key Management)을 지원합니다.

CCKM에 대한 자세한 내용은 다음 위치에서 *Cisco* 고속 보안 로밍 애플리케이션 참고를 참조하십시오.

http://www.cisco.com/en/US/products/hw/wireless/ps4570/prod_technical_reference09186a00801c5223.html

또한 802.11r도 지원합니다. 자세한 내용은 *Cisco* 무선 *IP* 전화기 *8821 Series* 구축 설명서를 참조하십시오.

Cisco Unified Communications Manager 상호 작용

Cisco Unified Communications Manager는 개방형의 업계 표준 통화 처리 시스템입니다. Cisco Unified Communications Manager 소프트웨어는 여러 전화기 사이에서 통화를 설정하고 분류하며, 기존 PBX 기능과 회사 IP 네트워크를 통합합니다. Cisco Unified Communications Manager는 전화기와 같은 텔레포니 시스템 구성 요소와 액세스 게이트웨이, 그리고 전화회의 및 경로 플랜 같은 기능에 필요한 리소스를 관리합니다. Cisco Unified Communications Manager는 다음과 같은 내용도 제공합니다.

- 전화기용 펌웨어
- TFTP 및 HTTP 서비스를 사용하는 CTL(Certificate Trust List) 및 ITL(Identity Trust List) 파일
- 전화기 등록
- 통화 보호, 기본 Communications Manager와 전화기 사이에 시그널링이 사라져도 미디어 세션을 유지할 수 있음

이 장에서 설명한 대로 전화기와 작동하도록 Cisco Unified Communications Manager를 구성하는 것에 관한 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.

참고 구성하려는 전화기 모델이 Cisco 통합 커뮤니케이션 매니저 관리의 [전화 유형] 드롭다운 목록에 나타나지 않으면 Cisco.com에서 보유 중인 Cisco Unified Communications Manager 버전에 맞는 최신 장치 패키지를 설치하십시오.

음성 메시징 시스템 상호 작용

Cisco Unified Communications Manager를 사용하면 Cisco Unity Connection 음성 메시징 시스템을 포함하여 다른 음성 메시징 시스템과 통합할 수 있습니다. 다양한 시스템과 통합할 수 있으므로, 특정 시스템을 사용하는 방법에 대한 정보를 사용자에게 제공해야 합니다.

사용자가 음성 메일로 전환하는 기능을 사용하려면 *xxxxx 전화 걸기 패턴을 설정하고 음성 메일로 모두 착신 전환으로 구성합니다. 자세한 내용은 Cisco Unified Communications Manager 문서를 참조하십시오.

각 사용자에게 다음 정보를 제공합니다.

- 음성 메시징 시스템 계정에 액세스하는 방법.

- 음성 메시징 시스템에 액세스하기 위한 초기 암호.

  모든 사용자에 대한 기본 음성 메시징 시스템 암호를 구성합니다.

- 전화기가 음성 메시지를 대기 중임을 나타내는 방법.

  Cisco Unified Communications Manager를 사용하여 MWI(Message Waiting Indicator) 방법을 설정합니다.