



## 기술 세부사항

- 물리적 및 운영 환경 사양, 1 페이지
- 케이블 사양, 2 페이지
- 전화기 전원 요구 사항, 4 페이지
- 네트워크 프로토콜, 6 페이지
- VLAN 상호 작용, 10 페이지
- Cisco Unified Communications Manager 상호 작용, 10 페이지
- Cisco Unified Communications Manager Express 상호 작용, 11 페이지
- 음성 메시징 시스템 상호 작용, 12 페이지
- 전화기 시작 개요, 12 페이지
- 외부 장치, 14 페이지
- USB 포트 정보, 14 페이지
- 전화기 구성 파일, 15 페이지
- 네트워크 혼잡 시 전화기 동작, 15 페이지
- 두 개의 네트워크 라우터가 있는 네트워크에서 네트워크 동작, 16 페이지
- 애플리케이션 프로그래밍 인터페이스, 16 페이지

## 물리적 및 운영 환경 사양

다음 표에는 Cisco IP 전화기 8800 시리즈의 물리적 및 운영 환경 명세가 정리되어 있습니다.

표 1: 물리적 운영 사양

사양	값 또는 범위
동작 온도	0°~40°C(32°~104°F)
작동 상대 습도	작동: 10% ~ 90%(비응축) 비작동: 10% ~ 95%(비응축)
보관 온도	-10°~60°C(14°~140°F)

사양	값 또는 범위
높이	9.02in(229.1mm)
폭	10.13in(257.34mm)
깊이	1.57in(40mm)
무게	2.62lb(1.19kg)
전원	AC 어댑터 사용 시 100-240VAC, 50-60Hz, 0.5A 네트워크 케이블을 통한 인라인 전력 사용 시 48VDC, 0.2A
케이블	Category 3/5/5e/6 10Mbps 케이블, 4쌍 Category 5/5e/6 100Mbps 케이블, 4쌍 Category 5e/6 1000Mbps 케이블, 4쌍 참고 케이블에는 총 8개의 전도체를 위한 4쌍의 선이 있습니다.
거리 요구 사항	이더넷 사양에서 지원하는 대로, 각 Cisco IP 전화기와 스위치 사이의 최대 길이는 330피트(100미터)로 가정합니다.

## 케이블 사양

다음 정보는 케이블 사양을 나열합니다.

- 핸드셋 및 헤드셋 연결을 위한 RJ-9 잭(4-conductor)
- LAN 10/100/1000BaseT 연결을 위한 RJ-45 잭(전화기의 10/100/1000 네트워크 포트)
- 두 번째 10/100/1000BaseT 준수 연결을 위한 RJ-45 잭(전화기의 10/100/1000 컴퓨터 포트)
- 스피커 연결용 3.5mm 잭(Cisco IP 전화기 8861만 해당)
- 48볼트 전원 커넥터
- USB 포트/커넥터: Cisco IP 전화기 8851용 USB 포트 1개 및 Cisco IP 전화기 8861용 USB 포트 2개
- Cisco IP 전화기 8851 및 8861용 USB 커넥터로 간주되는 키 확장 모듈 커넥터 3개

## 네트워크 및 컴퓨터 포트 핀 배치도

비록 네트워크 연결에 네트워크 및 컴퓨터(액세스) 포트가 모두 사용될지라도, 이들은 각기 다른 용도를 지원하고 포트 핀 배치도가 서로 다릅니다.

- 네트워크 포트는 Cisco IP 전화기의 10/100/1000 SW 포트입니다.
- 컴퓨터(액세스) 포트는 Cisco IP 전화기의 10/100/1000 PC 포트입니다.

## 네트워크 포트 커넥터

다음 표에서는 네트워크 포트 커넥터 핀 배치도에 대해 설명합니다.

표 2: 네트워크 포트 커넥터 핀 배치도

핀 번호	기능
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
참고	BI는 양방향을 의미하고 DA, DB, DC 및 DD는 각각 데이터 A, 데이터 B, 데이터 C 및 데이터 D를 의미합니다.

## 컴퓨터 포트 커넥터

다음 표에서는 컴퓨터 포트 커넥터 핀 배치도에 대해 설명합니다.

표 3: 컴퓨터 (액세스) 포트 커넥터 핀 배치도

핀 번호	기능
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
참고	BI는 양방향을 의미하고 DA, DB, DC 및 DD는 각각 데이터 A, 데이터 B, 데이터 C 및 데이터 D를 의미합니다.

## 전화기 전원 요구 사항

Cisco IP 전화기는 외부 전원이나 PoE(Power over Ethernet)로 켤 수 없습니다. 별도의 전원 공급장치에서 외부 전원을 공급합니다. 스위치는 전화기 이더넷 케이블을 통해 PoE를 제공할 수 있습니다.

Cisco IP 전화기 8861 및 8865는 PoE 클래스 4 장치이며 추가 기능을 지원하는 클래스 4 기능이 있는 스위치 또는 회선 카드가 필요합니다.

전화기 전원 요구 사항에 대한 자세한 내용은 전화기의 데이터 시트를 참조하십시오.

외부 전원에서 전원이 공급되는 전화기를 설치할 때는 이더넷 케이블을 전화기에 연결하기 전에 전원 공급장치를 연결합니다. 외부 전원에서 전원이 공급되는 전화기를 삭제할 때는 전원 공급장치를 분리하기 전에 전화기와 이더넷 케이블의 연결을 해제합니다.

표 4: Cisco IP 전화기 전원 지침

전원 유형	지침
외부 전원: CP-PWR-CUBE-4= 외부 전원 공급장치를 통해 공급됩니다.	Cisco IP 전화기는 CP-PWR-CUBE-4 전원 공급장치를 사용합니다.
PoE 전원—전화기에 연결된 이더넷 케이블을 통해 스위치에서 공급됩니다.	Cisco IP 전화기 8851, 8851NR, 8861, 8865 및 8865NR은 액세스리용으로 802.3af를 지원합니다. 자세한 내용은 전화기의 데이터 시트를 참조하십시오. 스위치를 사용하려면 전화기의 무중단 작동을 위해 백업 전원 공급 장치가 필요합니다. 스위치에서 실행되는 CatOS 또는 IOS 버전이 원하는 전화기 배포를 지원하는지 확인하십시오. 운영 체제 버전용 스위치에 관한 정보는 설명서를 참조하십시오.
UPoE(Universal Power Over Ethernet)	Cisco IP 전화기 8865 및 8865NR을 UPoE를 지원합니다.

다음 표의 문서는 다음 항목에 대한 추가 정보를 제공합니다.

- Cisco IP 전화기와 함께 작동하는 Cisco 스위치
- 양방향 전원공급 협상을 지원하는 Cisco IOS 릴리스
- 전원 요구 사항에 대한 기타 요구 사항 및 제한 사항

표 5: 추가 정보

문서 항목	URL
PoE 솔루션	<a href="http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html">http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html</a>
UPoE	<a href="http://www.cisco.com/c/en/us/solutions/enterprise-networks/upoe">http://www.cisco.com/c/en/us/solutions/enterprise-networks/upoe</a>
Cisco Catalyst 스위치	<a href="http://www.cisco.com/c/en/us/products/switches/index.html">http://www.cisco.com/c/en/us/products/switches/index.html</a>

문서 항목	URL
통합 서비스 라우터	<a href="http://www.cisco.com/c/en/us/products/routers/index.html">http://www.cisco.com/c/en/us/products/routers/index.html</a>
Cisco IOS 소프트웨어	<a href="http://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html">http://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html</a>

## 정전

전화를 통해 긴급 서비스에 액세스하려면 전화에 전원이 공급되어야 합니다. 정전이 발생할 경우 전력이 복원될 때까지 서비스 또는 긴급 통화 서비스 전화 걸기 기능이 작동하지 않습니다. 전원 공급이 안되거나 중단되는 경우 서비스 또는 긴급 통화 서비스 전화 걸기 기능을 사용하려면 장비를 재설정하거나 재구성해야 할 수 있습니다.

## 전력 소비 감소

절전 또는 EnergyWise(절전 플러스) 모드를 사용하면 Cisco IP 전화기에서 소비하는 에너지량을 줄일 수 있습니다.

### 절전

절전 모드에서 화면의 백라이트는 전화기가 사용 중이 아니면 켜지지 않습니다. 전화기는 예약된 기간 동안 또는 사용자가 송수화기를 들어올리거나 임의의 버튼을 누를 때까지 절전 모드에 남아 있습니다.

### 절전 플러스(EnergyWise)

Cisco IP 전화기는 Cisco EnergyWise(절전 플러스) 모드를 지원합니다. 네트워크에 EW(EnergyWise) 컨트롤러가 포함되어 있다면(예: EnergyWise 기능이 있는 Cisco 스위치가 활성화됨), 이 전화기는 전력 소비량을 더욱 줄이도록 일정에 맞춰 대기(절전) 및 활성화(작동)로 구성할 수 있습니다.

각 전화기에 [EnergyWise] 설정을 활성화 또는 비활성화하도록 설정합니다. [EnergyWise]가 활성화되어 있으면 대기(절전) 및 활성화(작동) 시간과 기타 매개 변수를 구성합니다. 이러한 매개 변수는 전화기 구성 XML 파일 항목으로 전화기에 전송됩니다.

## LLDP에 대한 전원공급 협상

전화기와 스위치는 전화기가 소비하는 전원을 협상합니다. Cisco IP 전화기는 다중 전원 설정에서 작동하여, 사용할 수 있는 전원이 적을 때 전력 소비를 낮춥니다.

전화기가 재부팅한 후, 스위치는 전원공급 협상을 위해 한 프로토콜(CDP 또는 LLDP)에 잠깁니다. 스위치는 전화기가 전송하는 첫 번째 프로토콜(전원 TLV[Threshold Limit Value]를 포함함)에 잠깁니다. 시스템 관리자가 전화기에서 해당 프로토콜을 비활성화하면 스위치가 기타 프로토콜의 전원 요청에는 응답하지 않으므로, 전화기는 액세서리에 전원을 공급할 수 없습니다.

Cisco는 전원공급 협상을 지원하는 스위치에 연결할 때는 항상 전원공급 협상을 활성화(디폴트)할 것을 권장합니다.

전원공급 협상이 비활성화되면 스위치가 전화기의 전원을 중단할 수 있습니다. 스위치가 전원공급 협상을 지원하지 않으면 PoE를 통해 액세서리에 전원을 공급하기 전에 전원공급 협상 기능을 비활성화하십시오. 전원공급 협상 기능이 비활성화될 때 전화기는 IEEE 802.3af-2003 표준이 허용하는 최대 값까지 액세서리에 전원을 공급할 수 있습니다.



참고 • CDP 및 전원공급 협상이 비활성화될 때 전화기는 최대 15.4W까지 액세서리에 전원을 공급할 수 있습니다.

## 네트워크 프로토콜

Cisco IP 전화기 8800 시리즈는 음성 통신에 필요한 몇 개의 업계 표준과 Cisco 네트워크 프로토콜을 지원합니다. 다음 표에는 전화기에서 지원하는 네트워크 프로토콜에 대한 개요가 나와 있습니다.

표 6: Cisco IP Phone 8800 시리즈에서 지원하는 네트워크 프로토콜

네트워크 프로토콜	목적	사용 참고 사항
블루투스	블루투스는 짧은 거리에서 장치가 통신하는 방식을 지정하는 무선 개인 영역 네트워크(WPAN) 프로토콜입니다.	Cisco IP 전화기 8845, 8865 및 8851은 블루투스 4.1을 지원합니다.  Cisco IP 전화기 8861은 블루투스 4.0을 지원합니다.  Cisco IP 전화기 8811, 8841, 8851NR 및 8865NR은 블루투스를 지원하지 않습니다.
BootP(Bootstrap Protocol)	BootP는 Cisco IP 전화기와 같은 네트워크 장치를 활성화하여 IP 주소와 같은 특정 시작 정보를 확인합니다.	—
CAST(Cisco Audio Session Tunnel)	CAST 프로토콜을 통해 전화기와 관련 애플리케이션은 시그널링 구성 요소를 변경하지 않고 원격 IP 전화기와 통신할 수 있습니다.	Cisco IP 전화기는 SIP 프록시로 Cisco IP 전화기를 사용해 Cisco Unified Communications Manager와 CUVA 간의 인터페이스로 CAST를 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.	Cisco IP Phone은 CDP를 사용해 Cisco Catalyst 스위치와 보조 VLAN ID, 포트별 전원 관리 세부 정보 및 QoS(Quality of Service) 구성 정보 같은 정보를 주고 받을 수 있습니다.

네트워크 프로토콜	목적	사용 참고 사항
<p>CPPDP(Cisco Peer-to-Peer Distribution Protocol)</p>	<p>CPPDP는 장치의 피어 투 피어 계층 구조를 형성하는 데 사용되는 Cisco의 독점적 프로토콜입니다. 이 계층 구조는 피어 장치에서 주변 장치로 펌웨어 파일을 배포하는 데 사용됩니다.</p>	<p>CPPDP는 피어 펌웨어 공유 기능에 사용됩니다.</p>
<p>DHCP(Dynamic Host Configuration Protocol)</p>	<p>DHCP는 네트워크 장치에 IP 주소를 역동적으로 할당합니다.</p> <p>DHCP를 사용하면 네트워크 IP 전화기를 연결하고, 수동으로 IP 주소를 할당하거나 추가 네트워크 매개 변수를 구성하지 않고도 전화기를 작동시킬 수 있습니다.</p>	<p>DHCP는 디폴트로 활성화됩니다. 비활성화된 경우에는 로컬에서 각 전화기에 IP 주소, 서브넷 마스크, 게이트웨이 및 TFTP 서버를 수동으로 구성해야 합니다.</p> <p>DHCP 사용자 정의 옵션 150을 사용할 것을 권합니다. 이런 방식으로 TFTP 서버 IP 주소를 옵션 값으로 구성합니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p> <p>참고        옵션 150을 사용할 수 없다면, DHCP 옵션 66을 사용해 볼 수 있습니다.</p>
<p>HTTP(Hypertext Transfer Protocol)</p>	<p>HTTP는 인터넷 및 웹 상에서 정보 교환 및 문서 이동을 위해 사용하는 표준 경로입니다.</p>	<p>Cisco IP Phone은 XML 서비스 및 문제 해결을 위해 HTTP를 사용합니다.</p>
<p>HTTPS(Hypertext Transfer Protocol Secure)</p>	<p>HTTPS(Hypertext Transfer Protocol Secure)는 HTTP(Hypertext Transfer Protocol)와 SSL/TLS 프로토콜의 조합으로 서버에 암호화 및 보안 식별 기능을 제공합니다.</p>	<p>HTTP와 HTTPS가 모두 지원되는 웹 애플리케이션에는 2개의 URL이 구성됩니다. HTTPS를 지원하는 Cisco IP 전화기는 HTTPS URL을 선택합니다.</p>
<p>IEEE 802.1X</p>	<p>IEEE 802.1X 표준은 클라이언트 서버 기반 액세스 제어 및 개방형 액세스 포트를 통한 LAN 연결에서 인증받지 못한 클라이언트를 제한하는 인증 프로토콜을 정의합니다.</p> <p>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.</p>	<p>Cisco IP 전화기는 EAP-FAST 및 EAP-TLS라는 인증 방식에 대한 지원을 제공하여 IEEE 802.1X 표준을 시행합니다.</p> <p>전화기에서 802.1X 인증이 활성화되면, PC 포트와 음성 VLAN을 비활성화해야 합니다.</p>
<p>IEEE 802.11n/802.11ac</p>	<p>IEEE 802.11 표준은 무선 근거리망(WLAN) 상에서 장치의 통신 방법을 지정합니다.</p> <p>802.11n은 2,4 GHz 및 5GHz 대역에서 작동하고 802.11ac는 5GHz 대역에서 작동합니다.</p>	<p>802.11 인터페이스는 이더넷 케이블 연결을 사용할 수 없거나 원하지 않는 경우의 배포 옵션입니다.</p> <p>Cisco IP 전화기 8861 및 8865만 WLAN을 지원합니다.</p>

네트워크 프로토콜	목적	사용 참고 사항
IP(Internet Protocol)	IP는 네트워크를 통해 패킷을 처리하고 전송하는 메시징 프로토콜입니다.	<p>IP를 사용하여 통신하기 위해서는 네트워크 장치에 IP 주소, 서브넷 및 게이트웨이가 있어야 합니다.</p> <p>IP 주소, 서브넷 및 게이트웨이 ID는 Cisco IP 전화기에서 DHCP(Dynamic Host Configuration Protocol)를 사용하고 있는 경우 자동으로 할당됩니다. DHCP를 사용하지 않는다면 로컬에서 각 전화기에 수동으로 이러한 속성을 할당해야 합니다.</p> <p>Cisco IP 전화기는 IPv6 주소를 지원합니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.</p>
LLDP(Link Layer Discovery Protocol)	LLDP는 일부 Cisco 및 타사 장치에서 지원되는 표준화된 네트워크 검색 프로토콜(CDP와 유사)입니다.	Cisco IP 전화기는 PC 포트에서 LLDP를 지원합니다.
LLDP-MED(Link Layer Discovery Protocol-Media Endpoint Devices)	LLDP-MED는 음성 제품을 위한 LLDP 확장 표준입니다.	<p>Cisco IP 전화기는 다음과 같은 정보를 주고받기 위해 SW 포트에서 LLDP-MED를 지원합니다.</p> <ul style="list-style-type: none"> <li>• 음성 VLAN 구성</li> <li>• 장치 검색</li> <li>• 전력 관리</li> <li>• 재고 관리</li> </ul>
RTP(Real-Time Transport Protocol)	RTP는 데이터 네트워크상에서 대화형 음성과 같은 실시간 데이터를 전송하기 위한 표준 프로토콜입니다.	Cisco IP 전화기는 RTP 프로토콜을 사용해 기타 전화기 및 게이트웨이에서 실시간 음성 트래픽을 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.
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.



네트워크 프로토콜	목적	사용 참고 사항
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 제어를 제공합니다.  전화기가 IPv4 전용, IPv6 전용 및 IPv4와 IPv6 둘 모두에서 작동하면 Cisco IP 전화기는 SIP 프로토콜을 지원합니다.
TCP(Transmission Control Protocol)	TCP는 연결 지향형 전송 프로토콜입니다.	Cisco IP 전화기는 TCP를 사용해 Cisco Unified Communications Manager에 연결하고, XML 서비스에 액세스합니다.
TLS(Transport Layer Security)	TLS는 통신 보안 및 인증을 위한 표준 프로토콜입니다.	보안 구현 시, Cisco IP 전화기는 Cisco Unified Communications Manager에 안전하게 등록된 경우 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.	UDP는 RTP 스트림에만 사용됩니다. 전화기에서 SIP 시그널링은 UDP를 지원하지 않습니다.

LLDP-MED 지원에 대한 자세한 내용은 LLDP-MED 및 Cisco Discovery Protocol 백서를 참조하십시오.

[http://www.cisco.com/en/US/tech/tk652/tk701/technologies\\_white\\_paper0900aecd804cd46d.shtml](http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml)

관련 항목

[802.1X 인증](#)

[네트워크 설정 구성](#)

[전화기 시작 확인](#)

[VLAN 상호 작용, 10 페이지](#)

[Cisco Unified Communications Manager 상호 작용, 10 페이지](#)

[Cisco Unified Communications Manager Express 상호 작용, 11 페이지](#)

[오디오 및 비디오 포트 범위 설정](#)

## Cisco Unified Communications Manager 설명서

## VLAN 상호 작용

Cisco IP 전화기에는 내부 이더넷 스위치가 들어 있어 전화기, 컴퓨터 (액세스) 포트, 그리고 전화기 후면의 네트워크 포트에 패킷을 착신 전환할 수 있습니다.

컴퓨터가 컴퓨터 (액세스) 포트에 연결되면, 컴퓨터와 전화기는 스위치에 대해 같은 물리적 링크를 공유하고 스위치에서 같은 포트를 공유합니다. 이렇게 공유된 링크는 네트워크상의 VLAN 구성에 다음과 같은 영향을 미칩니다.

- 현재 VLAN은 IP 서브넷 기반으로 구성되어 있을 수 있습니다. 그러나 동일한 포트에 연결된 다른 장치로 동일한 서브넷에 전화기를 할당하기 위해 추가 IP 주소가 제공되지 않을 수 있습니다.
- VLAN 지원 전화기의 데이터 트래픽으로 인해 VoIP 트래픽 품질이 떨어질 수 있습니다.
- 네트워크 보안상 VLAN 데이터 트래픽에서 VLAN 음성 트래픽을 격리해야 할 필요가 생길 수도 있습니다.

음성 트래픽을 별도의 VLAN으로 격리시키면 이러한 문제를 해결할 수 있습니다. 전화기가 연결된 스위치 포트는 다음을 처리하도록 별도의 VLAN에 구성됩니다.

- IP 전화기와 주고받는 음성 트래픽(예: Cisco Catalyst 6000 시리즈의 보조 VLAN)
- IP 전화기의 컴퓨터 (액세스) 포트를 통해 스위치와 연결된 PC와 주고받는 데이터 트래픽(기본 VLAN)

별도의 보조 VLAN에 전화기를 격리하면 음성 트래픽의 품질이 향상되고, 각 전화기를 위한 IP 주소가 충분하지 않은 기존 네트워크에 다수의 전화기를 추가할 수 있습니다.

자세한 내용은 Cisco 스위치에 포함된 문서를 참조하십시오. 스위치 정보는 다음 URL에서도 확인할 수 있습니다.

<http://cisco.com/en/US/products/hw/switches/index.html>

## 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 Unified Communications Manager Administration의 [전화 유형] 드롭다운 목록에 나타나지 않으면 Cisco.com에서 보유 중인 Cisco Unified Communications Manager 버전에 맞는 최신 장치 패키지를 설치하십시오.

관련 항목

[Cisco Unified Communications Manager 설명서](#)

## Cisco Unified Communications Manager Express 상호 작용

전화기에서 Cisco Unified Communications Manager Express(Unified CME)를 사용하면 전화기는 CME 모드로 바뀌어야 합니다.

사용자가 전화회의 기능을 시작하면, 태그를 통해 전화기는 로컬 또는 네트워크 하드웨어 컨퍼런스 브리지를 사용할 수 있습니다.

전화기에서는 다음과 같은 작업을 지원하지 않습니다.

- 호전환 - 연결된 통화 호전환 시나리오에서만 지원됩니다.
- 전화회의 - 연결된 통화 호전환 시나리오에서만 지원됩니다.
- 통화참가 - [전화회의] 버튼이나 후플래시 액세스를 통해서만 지원됩니다.
- 보류 - [보류] 버튼을 사용하여 지원됩니다.
- 참여 및 병합 - 지원되지 않습니다.
- 호연결 - 지원되지 않습니다.
- 선택 - 지원되지 않습니다.

사용자는 다른 회선에서는 전화회의와 호전환 통화를 실행할 수 없습니다.

Unified CME는 귓속말 페이지링이라고도 하는 인터콤 전화를 지원합니다. 하지만 통화 중 전화기에 의해 페이지가 거부됩니다.

CME 모드에서는 세션 라인 모드와 고급 라인 모드가 모두 지원됩니다.

## 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.

Cisco Unified Communications Manager를 사용하여 Cisco IP 전화기에 [메시지] 버튼을 구성했는지 확인하십시오.

- 음성 메시징 시스템에 액세스하기 위한 초기 암호.

모든 사용자에게 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.

## 전화기 시작 개요

VoIP 네트워크에 연결할 때 Cisco IP 전화기는 표준 시작 프로세스를 통과합니다. 특정 네트워크 구성에 따라, 이러한 단계 중 일부만 Cisco IP 전화기에서 발생할 수 있습니다.

1. 스위치에서 전원을 연습니다. 전화기가 외부 전원을 사용하고 있지 않으면 스위치는 전화기에 연결된 이더넷 케이블을 통해 인라인 전원을 제공합니다.
2. (무선 LAN의 Cisco IP 전화기 8861 및 8865 전용) 액세스 지점을 검색합니다. Cisco IP 전화기 8861 및 8865의 경우 무선 통신으로 RF 적용 범위를 검색합니다. 전화기는 네트워크 프로파일을 검색하고 일치하는 SSID 및 인증 유형을 포함하는 액세스 지점을 검색합니다. 전화기는 네트워크 프로파일과 일치하는 최고 RSSI를 사용하여 액세스 지점과 연결됩니다.
3. (무선 LAN의 Cisco IP 전화기 8861 및 8865 전용) 액세스 지점에서 인증합니다. Cisco IP 전화기가 인증 프로세스를 시작합니다. 다음 표에서는 인증 프로세스에 대해 설명합니다.

인증 유형	키 관리 옵션	설명
열기	없음	아무 장치나 액세스 지점에 인증할 수 있습니다. 보안 강화를 위해 정적 WEP 암호화가 선택적으로 사용될 수 있습니다.

인증 유형	키 관리 옵션	설명
공유 키	없음	전화기는 WEP 키를 사용하여 도전 텍스트를 암호화하고 액세스 지점은 네트워크 액세스를 사용하려면 도전 텍스트를 암호화하는 데 사용된 WEP 키를 확인해야 합니다.
PEAP 또는 EAP-FAST	없음	네트워크 액세스를 사용할 수 있으려면 RADIUS 서버가 사용자 이름 및 암호를 인증해야 합니다.

4. 저장된 전화기 이미지를 로드합니다. 시작 시, 전화기는 플래시 메모리에 저장되는 전화기 펌웨어 이미지를 로드하는 부트스트랩 로더를 실행합니다. 이 이미지를 사용하는 경우 전화기는 소프트웨어와 하드웨어를 초기화합니다.
5. VLAN을 구성합니다. Cisco IP 전화기가 Cisco Catalyst 스위치에 연결된 경우 스위치에 정의된 음성 VLAN에 대해 전화기에 알립니다. IP 주소에 대한 DHCP(Dynamic Host Configuration Protocol) 요청으로 진행하려면 전화기에서 VLAN 구성원 자격을 알고 있어야 합니다.
6. IP 주소를 얻습니다. Cisco IP 전화기가 DHCP를 사용하여 IP 주소를 얻으려면 전화기에서 DHCP 서버를 조회하여 IP 주소를 얻습니다. 네트워크에서 DHCP를 사용하지 않는다면 로컬에서 각 전화기에 로컬로 정적 IP 주소를 할당해야 합니다.
7. CTL 파일을 요청합니다. TFTP 서버는 CTL 파일을 저장합니다. 이 파일은 전화기와 Cisco Unified Communications Manager 간에 보안 연결을 설정하는 데 필요한 인증서를 포함합니다.  
자세한 내용은 특정 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오.
8. ITL 파일을 요청합니다. 전화기는 CTL 파일을 요청한 후 ITL 파일을 요청합니다. ITL 파일은 전화기가 신뢰할 수 있는 엔티티의 인증서를 포함합니다. 인증서는 서버와 보안 연결을 인증하거나 서버에서 서명한 디지털 서명을 인증하는 데 사용됩니다. Cisco Unified Communications Manager 8.5 이상은 ITL 파일을 지원합니다.
9. TFTP 서버에 액세스합니다. IP 주소를 할당할 뿐만 아니라, DHCP 서버는 Cisco IP 전화기를 TFTP 서버에 연결합니다. 전화기가 통계적으로 정의된 IP 주소를 가질 경우, 전화기에 로컬로 TFTP 서버를 구성해야 합니다. 그런 다음 전화기는 TFTP 서버에 직접 연결합니다.



참고 또한 DHCP가 할당하는 서버 대신 사용할 대체 TFTP 서버를 할당할 수 있습니다.

10. 구성 파일을 요청합니다. TFTP 서버에는 Cisco Unified Communications Manager에 연결하기 위한 매개 변수와 전화기용 기타 정보를 정의하는 구성 파일이 있습니다.
11. Cisco Unified Communications Manager에 연결합니다. 구성 파일은 Cisco IP 전화기가 Cisco Unified Communications Manager와 통신하고 전화기에 로드 ID를 제공하는 방법을 정의합니다. 전화기는 TFTP 서버에서 파일을 얻은 후, 목록에서 가장 우선 순위가 높은 Cisco Unified Communications Manager에 연결을 시도합니다.

보안 시그널링(암호화되거나 인증됨)을 위해 전화기의 보안 프로파일이 구성되고 Cisco Unified Communications Manager가 보안 모드로 설정된 경우 전화기는 TLS 연결을 설정합니다. 그렇지 않으면, 전화기는 비보안 TCP 연결을 설정합니다.

전화기가 수동으로 데이터베이스에 추가되었으면 Cisco Unified Communications Manager가 전화를 식별합니다. 전화기가 수동으로 데이터베이스에 추가되지 않았고 자동 등록이 Cisco Unified Communications Manager에서 활성화된 경우 전화기가 Cisco Unified Communications Manager 데이터베이스에서 자동 등록을 시도합니다.



참고 CTL 클라이언트를 구성할 때 자동 등록은 비활성화됩니다. 이 경우, 전화를 수동으로 Cisco Unified Communications Manager 데이터베이스에 추가해야 합니다.

관련 항목

[Cisco Unified Communications Manager 설명서](#)

## 외부 장치

잘못된 RF(무선 주파수) 및 AF(오디오 주파수) 신호를 차단하는 우수한 품질의 외부 장치를 사용하는 것이 좋습니다. 외부 장치로는 헤드셋, 케이블 및 커넥터가 있습니다.

이러한 장치의 품질과 휴대 전화 또는 양방향 무선 장치 등과 같은 기타 장치와의 근접 정도에 따라 약간의 오디오 잡음이 계속 발생할 수도 있습니다. 이러한 경우 다음 중 한 가지 이상의 작업을 수행하는 것이 좋습니다.

- 외부 장치를 RF 또는 AF 신호 발생지로부터 멀리 옮기십시오.
- 외부 장치 케이블의 경로를 RF 또는 AF 신호 발생지로부터 멀리 지정하십시오.
- 외부 장치에 차폐된 케이블을 사용하거나 보호성이 좋은 케이블과 커넥터를 사용하십시오.
- 외부 장치 케이블의 길이를 줄이십시오.
- 외부 장치용 케이블에 페라이트 또는 이와 유사한 기타 물질을 바르십시오.

Cisco에서는 기존 장치, 케이블 및 커넥터의 성능을 보장할 수 없습니다.



주의 EU(유럽 연합) 국가에서는 EMC 규정 [89/336/EC]를 엄격히 준수하는 외부 스피커, 마이크 및 헤드셋만 사용하십시오.

## USB 포트 정보

Cisco IP 전화기 8851, 8851NR, 8861, 8865 및 8865NR은 각 USB 포트에 연결하는 장치를 최대 5개까지 지원합니다. 전화기에 연결하는 각 장치는 최대 장치 수에 포함됩니다. 예를 들어 전화기에서 측

면 포트에 있는 5개 USB 장치를 지원하고 후면 포트에서 5개 이상의 표준 USB 장치를 지원할 수 있습니다. 다양한 타사 USB 제품은 다수의 USB 장치로 간주합니다. 예를 들면 USB 허브 및 헤드셋을 포함하는 장치는 두 개의 USB 장치로 계산될 수 있습니다. 자세한 내용은 USB 장치 설명서를 참조하십시오.



- 참고
- 전원이 공급되지 않은 허브는 지원되지 않고, 전원이 공급되지만 5개 이상의 포트가 있는 허브는 지원되지 않습니다.
  - USB 허브를 통해 전화기에 연결하는 USB 헤드셋은 지원되지 않습니다.

전화기에 연결된 각 키 확장 모듈은 USB 장치로 계산됩니다. 3개의 키 확장 모듈이 전화기에 연결된 경우 이들은 3개의 USB 장치로 계산됩니다.

## 전화기 구성 파일

전화기에 대한 구성 파일은 TFTP 서버에 저장되고 Cisco Unified Communications Manager에 연결하기 위한 매개 변수를 정의합니다. 일반적으로 전화기를 재설정해야 하는 변경 사항을 Cisco Unified Communications Manager에서 작성할 때 자동으로 전화기 구성 파일에 변경 사항이 작성됩니다.

또한 구성 파일은 전화기를 로드하는 이미지가 실행 중이어야 하는 정보를 포함합니다. 이 이미지가 로드된 현재 전화기에 로드된 이미지와 다를 경우 전화기는 TFTP 서버에 연결하여 필수 로드 파일을 요청합니다.

Cisco 통합 커뮤니케이션 매니저 관리에서 보안 관련 설정을 구성할 경우 전화기 구성 파일은 중요 정보를 포함합니다. 구성 파일의 프라이버시를 보장하려면 암호화에 대한 설정을 구성해야 합니다. 자세한 내용은 해당 Cisco Unified Communications Manager 릴리스용 문서를 참조하십시오. 전화기는 재설정되고 Cisco Unified Communications Manager에 등록할 때마다 구성 파일을 요청합니다.

다음 조건이 있을 때 전화기는 TFTP 서버에서 XmlDefault.cnf.xml이라는 기본 구성 파일에 액세스합니다.

- 에서 자동 등록을 활성화했습니다. Cisco Unified Communications Manager
- 전화기가 Cisco Unified Communications Manager 데이터베이스에 추가되지 않았습니다.
- 전화기가 처음 등록되는 중입니다.

관련 항목

[Cisco Unified Communications Manager 설명서](#)

## 네트워크 혼잡 시 전화기 동작

네트워크 성능을 저하시키는 것이라면 무엇이든 전화기 오디오 및 비디오 품질에 영향을 미칠 수 있고, 어떤 경우에는 통화가 끊어지게 만들 수도 있습니다. 네트워크 저하의 근원에는 다음과 같은 활동이 포함되며 이에 국한되는 것은 아닙니다.

- 관리자 작업(예: 내부 포트 스캔 또는 보안 스캔)
- 네트워크에 발생한 공격(예: DoS(서비스 거부) 공격 등)

## 두 개의 네트워크 라우터가 있는 네트워크에서 네트워크 동작

Cisco IP 전화기 8800 시리즈는 방화벽을 사용하여 중간자 공격과 같은 사이버 침투에 대한 보호를 제공합니다. 이 방화벽은 비활성화할 수 없습니다. 그러나 동일한 서브넷의 두 네트워크 라우터 2개 및 IP 재전송으로 네트워크를 구성하는 경우에는 전화기의 트래픽을 중지할 수 있습니다.

이 네트워크 설정은 중간자 공격과 유사하므로 전화기 방화벽이 트래픽을 중지합니다. 전화기는 전화기의 다른 서브넷에서 다른 대상 IP에 대한 재전송 패킷을 수신합니다. 전화기는 두 개 이상의 라우터가 있는 네트워크에 있고 기본 라우터는 트래픽을 두 번째 라우터로 보냅니다.

방화벽이 트래픽을 중지하는 것으로 의심되는 경우 전화기 로그를 살펴보십시오. 연결 설정을 시도할 때 운영 체제에서 오류 코드 1 알람을 살펴봅니다. 서명 중 하나는 다음과 같습니다.

```
sip_tcp_create_connection: socket connect failed cpr_errno: 1.
```

동일한 서브넷에 두 개의 네트워크 라우터가 있고 IP 재전송 기능이 있는 네트워크는 일반 구성이 아닙니다. 이 네트워크 설정을 사용하는 경우 서브넷의 한 라우터만 사용할 것을 고려하십시오. 그러나 동일한 서브넷에 두 개의 네트워크 라우터가 필요한 경우 라우터의 IP 재전송을 비활성화하고 전화기를 재부팅하십시오.

## 애플리케이션 프로그래밍 인터페이스

Cisco는 타사 애플리케이션 개발자가 Cisco를 통해 테스트하고 인증한 타사 애플리케이션의 전화 API 활용을 지원합니다. 인증되지 않은 애플리케이션 상호 작용과 관련된 전화기 문제는 제3자가 해결해야 하며 Cisco는 이를 해결하지 않습니다.

Cisco 인증 타사 애플리케이션/솔루션의 지원 모델은 [Cisco Solution Partner Program](#) 웹 사이트를 참조하십시오.



## 번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.