技術的な詳細

- 物理環境および動作環境に関する仕様 （1 ページ）
- ケーブル仕様 （3 ページ）
- ネットワーク ポートとコンピュータ ポートのピン割り当て （3 ページ）
- 電話機の所要電力 （4 ページ）
- ネットワーク プロトコル （7 ページ）
- VLAN の連携 （11 ページ）
- 外部デバイス （12 ページ）
- SIP と NAT の設定 （13 ページ）
- Cisco 検出プロトコル （17 ページ）
- LLDP-MED （17 ページ）
- 最終的なネットワーク ポリシーの解決と QoS （23 ページ）

物理環境および動作環境に関する仕様

次の表に、マルチプラットフォーム対応のファームウェアを備えた Cisco IP 電話 7800 シリーズの物理仕様と動作環境仕様を示します。

表 *1*：物理仕様および動作環境仕様

仕様	値または範囲
動作温度	0 ～ 40 °C（32 ～ 104 °F）
動作相対湿度	10 ～ 90%（結露しないこと）
保管温度	–10 ～ 60 °C（14 ～ 140 °F）
高さ(T)：	207 mm（8.14 インチ）

技術的な詳細

仕様	値または範囲
幅(W)：	• Cisco IP 電話 7811：195 mm（7.67 インチ） • Cisco IP 電話 7821：206 mm（8.11 インチ） • Cisco IP 電話 7841：206 mm（8.11 インチ） • Cisco IP 電話 7861：264.91 mm（10.42 インチ）
深さ	28 mm（1.1 インチ）
重み	• Cisco IP 電話 7811：0.84 kg • Cisco IP 電話 7821：0.867 kg • Cisco IP 電話 7841：0.868 kg • Cisco IP 電話 7861：1.053 kg
電力	• AC アダプタ使用時：100 ～ 240 VAC、50 ～ 60 Hz、0.5 A • ネットワーク ケーブル経由のインライン電源使用時：48 VDC、0.2 A
ケーブル	Cisco IP 電話 7811、7821、7841、および 7861 • 10 Mbps ケーブルの場合はカテゴリ 3/5/5e/6 の 4 ペア • 100 Mbps ケーブルの場合はカテゴリ 5/5e/6 の 4 ペア Cisco IP 電話 7841：1000 Mbps ケーブルの場合はカテゴリ 5/5e/6 を 4 ペア （注） ケーブルは、合計 8 本のコンダクタに対して 4 ペアのワイヤで構成されています。
距離要件	イーサネット仕様でサポートされているとおり、各 Cisco IP 電話 とスイッチ間のケーブル長は最大 100 メートル（330 フィート）とします。

詳細については、『*Cisco IP* 電話 *7800 Series Data Sheet*』を参照してください。
https://www.cisco.com/c/en/us/products/collaboration-endpoints/ip-phone-7800-series-multiplatform-firmware/datasheet-listing.html

ケーブル仕様

- ハンドセットおよびヘッドセット接続用の RJ-9 ジャック（4 コンダクタ）。

（注） Cisco IP 電話 7811 にはヘッドセット ジャックが含まれていません。

- LAN 10/100BaseT 接続用（Cisco IP 電話 7811、7821、および 7861）および LAN 1000BaseT 接続用（Cisco IP 電話 7841）の RJ-45 ジャック。
- 2 番目の 10/100BaseT 準拠接続用（Cisco IP 電話 7811、7821、および 7861）および LAN 1000BaseT 接続用（Cisco IP 電話 7841）の RJ-45 ジャック。
- 48 ボルト電源コネクタ。

ネットワークポートとコンピュータポートのピン割り当て

ネットワーク ポートとコンピュータ（アクセス）ポートはいずれもネットワーク接続に使用されますが、それぞれ異なる目的で使用され、ポートのピン割り当ても異なっています。

- ネットワーク ポートは、10/100 SW ポートです。Cisco IP 電話 7841 には 10/100/1000 SW ネットワーク ポートがあります。
- コンピュータ（アクセス）ポートは 10/100 PC ポートです。Cisco IP 電話 7841 には 10/100/1000 PC コンピュータ ポートがあります。

ネットワーク ポート コネクタ

次の表に、ネットワーク ポート コネクタのピン割り当てを示します。

表 *2:* ネットワーク ポート コネクタのピン割り当て

ピン番号	機能
1	BI_DA+
2	BI_DA-

ピン番号	機能
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
（注） BI は双方向を表し、DA、DB、DC、DD はそれぞれデータ A、データ B、データ C、データ D を表します。	

コンピュータ ポート コネクタ

次の表に、コンピュータ ポート コネクタのピン割り当てを示します。

表 *3:* コンピュータ（アクセス）ポート コネクタのピン割り当て

ピン番号	機能
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
（注） BI は双方向を表し、DA、DB、DC、DD はそれぞれデータ A、データ B、データ C、データ D を表します。	

電話機の所要電力

Cisco IP 電話は、外部電源または Power over Ethernet（PoE）で電力を供給できます。外部電源は個別の電源装置によって提供されます。スイッチは電話機のイーサネット ケーブル経由で PoE を供給できます。

（注） 外部電源を使用する場合、イーサネット ケーブルを電話機に接続する前に、電源装置を電話機に接続する必要があります。外部電源から電力が供給されている電話機を取り外す場合は、電源装置を取り外す前に、イーサネット ケーブルを電話機から取り外してください。

表 *4 : Cisco IP* 電話の電源に関するガイドライン

電源の種類	ガイドライン
外部電源：CP-PWR-CUBE-3=外部電源を通じて電力を供給	Cisco IP 電話シリーズでは、CP-PWR-CUBE-3 電源を使用します。
外部電源：Cisco IP 電話パワー インジェクタを通じて電力を供給	Cisco IP 電話パワー インジェクタは、ほとんどの Cisco IP 電話で使用できます。電話機のデータシートで、電話機がパワー インジェクタを使用できるかどうかを特定できます。 インジェクタは、ミッドスパン デバイスとして機能し、接続されている電話機にインライン パワーを供給します。Cisco IP 電話パワー インジェクタは、スイッチ ポートと IP 電話間に接続されます。また、通電していないスイッチと IP 電話 間で最大 100 m のケーブル長をサポートします。
PoE 電源：イーサネット ケーブルを介して電話機に接続されているスイッチを通じて電力を供給。	電話機を無停電で運用するには、スイッチがバックアップ電源を備えている必要があります。 スイッチ上で実行されている CatOS または IOS のバージョンが、目的とする電話機配置をサポートしていることを確認します。オペレーティング システムのバージョンに関する情報については、スイッチのマニュアルを参照してください。

次の表にあるドキュメントは、次のトピックに関する詳細情報を提供します。

- Cisco IP 電話と連携する Cisco スイッチ
- 双方向電力ネゴシエーションをサポートしている Cisco IOS リリース
- 電力に関するその他の要件および制限事項

ドキュメントのトピック	URL
PoE ソリューション	http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html
Cisco Catalyst スイッチ	http://www.cisco.com/c/en/us/products/switches/index.html
サービス統合型ルータ	http://www.cisco.com/c/en/us/products/routers/index.html
Cisco IOS ソフトウェア	http://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html

停電

電話機を経由して緊急サービスにアクセスするには、その電話機が電力を受信する必要があります。停電が発生した場合、電源が復旧するまでは、電話サービスおよび緊急コールサービスダイヤルが機能しません。電源の異常および障害が発生した場合は、装置をリセットまたは再設定してから、電話サービスおよび緊急コールサービスダイヤルを利用する必要があります。

電力削減

省電力モードを使用すると、Cisco IP 電話の消費電力量を削減できます。

省電力（Power Save）

Power Save モードでは、電話機が使用されていないときにはスクリーンのバックライトが消灯します。電話機は、ユーザがハンドセットを持ち上げるか任意のボタンを押すまで、省電力モードのままです。省電力設定は、電話機ごとに有効または無効にセットアップします。

（注） Cisco IP 電話 7811 は、電話画面にバックライトがないため省電力をサポートしていません。

LLDP での電力ネゴシエーション

電話機とスイッチは、電話機が消費する電力のネゴシエーションを行います。Cisco IP 電話は複数の電力設定で動作し、これにより、使用する電力が少ないときの電力消費を削減します。

電話機のリブートの後、スイッチは電力ネゴシエーションの 1 つのプロトコル（CDP または LLDP）にロックされます。スイッチは、電話機が送信した最初のプロトコル（電力の[しきい値限度値 [TLV]（Threshold Limit Value [TLV]）] を含む）にロックされます。システム管理者

が電話機でそのプロトコルを無効にすると、スイッチがもう一方のプロトコルでの電力要求に応答しないため、電話機はアクセサリの電源を投入できなくなります。

電力ネゴシエーションをサポートするスイッチに接続する場合は、常に電力ネゴシエーションを有効（デフォルト）にすることをお勧めします。

電力ネゴシエーションを無効にすると、スイッチは電話機の電源を切断する場合があります。スイッチが電力ネゴシエーションをサポートしていない場合は、アクセサリの電源を PoE+ で投入する前に、電力ネゴシエーション機能を無効にしてください。電力ネゴシエーション機能を無効にすると、電話機は IEEE 802.3af-2003 規格で許容される最大値まで、アクセサリに電力を供給できます。

（注）
- CDP と電力ネゴシエーションを無効にすると、電話機は最大 15.4 W までアクセサリに電力を供給できます。

ネットワーク プロトコル

Cisco IP 電話は、音声通信に必須の複数の業界標準ネットワーク プロトコルとシスコ ネットワーク プロトコルをサポートしています。次の表に、Phone でサポートされるネットワーク プロトコルの概要を示します。

表 *5 : Cisco IP* 電話でサポートされているネットワーク プロトコル

ネットワーク プロトコル	目的	使用方法に関する特記事項
ブートストラップ プロトコル（BootP）	BootP は、特定の起動情報（IP アドレスなど）を Cisco IP 電話などのネットワーク デバイスが検出できるようにするものです。	—
Cisco Discovery Protocol（CDP）	CDP は、シスコの製造するすべての装置で動作するデバイス検出プロトコルです。 デバイスは、CDP を使用して自身の存在をネットワーク内の他のデバイスにアドバタイズし、ネットワーク内の他のデバイスの情報を受信できます。	Cisco IP Phone では、補助 VLAN ID、ポートごとの電源管理の詳細情報、Quality of Service（QoS）設定情報などの情報を、CDP を使用して Cisco Catalyst スイッチとやり取りしています。
Domain Name Server (DNS)	DNS はドメイン名を IP アドレスに変換します。	Cisco IP 電話は、ドメイン名を IP アドレスに変換する DNS クライアントを備えています。

技術的な詳細

ネットワーク プロトコル	目的	使用方法に関する特記事項
ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）	DHCP は、IP アドレスを動的に確保して、ネットワーク デバイスに割り当てるものです。 DHCP を使用すると、IP 電話をネットワークに接続すれば、その電話機が機能するようになります。IP アドレスを手動で割り当てたり、ネットワーク パラメータを別途設定したりする必要はありません。	DHCP は、デフォルトで有効になっています。無効になっている場合は、IP アドレス、サブネット マスク、およびゲートウェイを電話機ごとに手動で設定する必要があります。 DHCP のカスタム オプション 160 および 159 を使用することを推奨します。
Hypertext Transfer Protocol（HTTP）	HTTP は、インターネットや Web 経由で情報を転送し、ドキュメントを移送するための標準プロトコルです。	Cisco IP 電話では、XML サービス、プロビジョニング、アップグレード、およびトラブルシューティングに HTTP を使用します。
Hypertext Transfer Protocol Secure （HTTPS）	Hypertext Transfer Protocol Secure（HTTPS）は、サーバの暗号化とセキュアな ID を確保できるように、ハイパーテキスト転送プロトコルと SSL/TLS プロトコルを組み合わせたものです。	HTTP と HTTPS の両方をサポートする Web アプリケーションには 2 つの URL が設定されています。HTTPS をサポートする Cisco IP 電話は、HTTPS URL を選択します。 サービスへの接続が HTTPS 経由である場合、鍵のアイコンがユーザに表示されます。

技術的な詳細

ネットワーク プロトコル	目的	使用方法に関する特記事項
インターネット プロトコル（IP）	IP は、パケットの宛先アドレスを指定し、ネットワーク経由で送信するメッセージング プロトコルです。	IP を使用して通信するには、ネットワーク デバイスに対して、IP アドレス、サブネット、およびゲートウェイが割り当てられている必要があります。 IP アドレス、サブネット、およびゲートウェイの識別情報は、Dynamic Host Configuration Protocol（DHCP）を通じて Cisco IP Phone を使用する場合は、自動的に割り当てられます。DHCP を使用しない場合は、個々の電話機がある場所で、これらのプロパティを手動で割り当てる必要があります。
リンク層検出プロトコル（LLDP）	LLDP は、CDP と同様の標準化されたネットワーク検出プロトコルで、一部のシスコ デバイスとサードパーティ製デバイスでサポートされています。	Cisco IP 電話は、PC ポートで LLDP をサポートします。
Link Layer Discovery Protocol-Media Endpoint Devices（LLDP-MED）	LLDP-MED は、音声製品用に開発された、LLDP 標準の拡張です。	Cisco IP Phone は、次のような情報をやり取りするために、SW ポートで LLDP-MED をサポートします。 • ボイス VLAN の設定 • デバイスの検出 • 電源管理 • インベントリ管理 LLDP-MED サポートの詳細については、次の URL にある『*LLDP-MED and Cisco Discovery Protocol*』ホワイト ペーパーを参照してください。 http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper

技術的な詳細

ネットワーク プロトコル	目的	使用方法に関する特記事項
Network Transport Protocol（NTP）	NTP は、遅延変動のあるパケット交換データ ネットワークでコンピュータ システムのクロックを同期するためのネットワーキング プロトコルです。	Cisco IP 電話は、ソフトウェアに統合された NTP クライアントを備えています。
Real-Time Transport Protocol（RTP）	RTP は、インタラクティブな音声やビデオなどのリアルタイム データをデータ ネットワーク経由で転送するための標準プロトコルです。	Cisco IP 電話は、RTP プロトコルを使用して、他の電話機やゲートウェイとリアルタイム音声トラフィックを送受信します。
Real-Time Control Protocol (RTCP)	RTCP は RTP と連動して、RTP ストリーム上で QoS データ（ジッター、遅延、ラウンドトリップ遅延など）を伝送します。	RTCP はデフォルトでは無効になっています。
Session Description Protocol（SDP）	SDP は SIP プロトコルの一部であり、2 つのエンドポイント間で接続が確立されている間に、どのパラメータを使用できるかを決定します。会議は、会議に参加するすべてのエンドポイントがサポートする SDP 機能だけを使用して確立されます。	コーデック タイプ、DTMF 検出、コンフォート ノイズなどの SDP 機能は、通常は運用中のサードパーティ コール制御システムまたはメディア ゲートウェイでグローバルに設定されています。SIP エンドポイントの中には、これらのパラメータをエンドポイント上で設定できるものがあります。
Session Initiation Protocol（SIP）	SIP は、IP を介したマルチメディア会議のためのインターネット技術特別調査委員会（IETF）標準です。SIP は、アプリケーション層の ASCII ベースの制御プロトコルであり（RFC 3261 で規定）、2 つ以上のエンドポイント間でコールを確立、維持、および終了するために使用できます。	他の Voice over IP（VoIP）プロトコルと同様に、SIP はパケット テレフォニー ネットワークにおけるシグナリングとセッション管理の機能に対応するよう設計されています。シグナリングは、ネットワーク境界を越えてコール情報を伝送する機能です。セッション管理は、エンドツーエンド コールの属性を制御する機能です。

ネットワーク プロトコル	目的	使用方法に関する特記事項
Secure Real-Time Transfer protocol (SRTP)	SRTP は、Real-Time Protocol（RTP）Audio/Video Profile の拡張で、RTP パケットと Real-Time Control Protocol（RTCP）パケットの整合性を保証して、2つのエンドポイント間のメディア パケットの認証、整合性、および暗号化を実現します。	Cisco IP 電話は、メディア暗号化に SRTP を使用します。
Transmission Control Protocol（TCP）	TCP は、コネクション型の転送プロトコルです。	—
Transport Layer Security（TLS）	TLS は、通信のセキュリティ保護と認証に使用される標準プロトコルです。	セキュリティを実装すると、Cisco IP 電話は TLS プロトコルを使用して、サードパーティ コール制御システムへの登録をセキュアに実行します。
Trivial File Transfer Protocol（TFTP）	TFTP を使用すると、ファイルをネットワーク経由で転送できます。 Cisco IP Phone で TFTP を使用すると、電話機タイプに固有の設定ファイルを取得できます。	TFTP では、ネットワーク内に TFTP サーバが必要です。このサーバは、DHCP サーバで自動的に識別できます。
User Datagram Protocol（UDP）	UDP は、データ パケットを配信するためのコネクションレス型メッセージング プロトコルです。	UDP は RTP ストリームにのみ使用されます。SIP は、UDP、TCP、および TLS を使用します。

関連トピック

ネットワーク セットアップの確認
電話機起動の確認

VLAN の連携

Cisco IP 電話は内蔵イーサネット スイッチを備えているため、電話機や、電話機の背面にあるコンピュータ（アクセス）ポートおよびネットワーク ポートにパケットを転送できます。

コンピュータ（アクセス）ポートにコンピュータを接続した場合、コンピュータと電話機は、スイッチへの同じ物理リンクとスイッチ上の同じポートを共有します。このように物理リンクが共有されるため、ネットワークのVLAN設定について、次のような考慮事項が存在します。

- 現在の VLAN を IP サブネット ベースで設定することは可能です。ただし、追加の IP アドレスを取得して、同じポートに接続されている他のデバイスと同じサブネットに電話機を割り当てることはできません。
- VLAN をサポートしている電話機上に存在するデータ トラフィックによって、VoIP トラフィックの品質が低下することがあります。
- ネットワーク セキュリティを確保するために、VLAN 音声トラフィックと VLAN データ トラフィックの分離が必要になることがあります。

これらの問題は、音声トラフィックを別の VLAN 上に分離することで解決できます。電話機の接続先となるスイッチ ポートには、伝送用に、それぞれ別個の VLAN を設定します。

- IP 電話で送受信される音声トラフィック（Cisco Catalyst 6000 上などの補助 VLAN）
- IP 電話のコンピュータ（アクセス）ポート経由でスイッチに接続されている PC で送受信されるデータ トラフィック（ネイティブ VLAN）

複数の電話機を別々の補助 VLAN に分離すると、音声トラフィックの品質が向上するとともに、各電話機に割り当てる IP アドレスが十分にない既存ネットワークに対しても、多数の電話機を追加できます。

詳細については、Cisco スイッチに添付されているマニュアルを参照してください。スイッチに関する情報には、次の URL からもアクセスできます。

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

外部デバイス

不要な無線周波数（RF）信号および可聴周波数（AF）信号を遮断する高品質の外部デバイスを使用することをお勧めします。外部デバイスには、ヘッドセット、ケーブル、コネクタが含まれます。

これらのデバイスの品質や、携帯電話および双方向ラジオなど他のデバイスとの間隔によっては、雑音が入ることもあります。その場合は、次の方法で対処することをお勧めします。

- RF または AF の信号源から外部デバイスを離す。
- RF または AF の信号源から外部デバイスのケーブルの経路を離す。
- 外部デバイス用にシールドされたケーブルを使用するか、高品質なシールドおよびコネクタを備えたケーブルを使用する。
- 外部デバイスのケーブルを短くする。
- 外部デバイスのケーブルに、フェライトまたは同様のデバイスを適用する。

シスコでは、外部デバイス、ケーブル、およびコネクタのパフォーマンスを保証できません。

⚠

注意 欧州連合諸国では、EMC Directive [89/336/EC] に完全に準拠した外部スピーカ、マイクロフォン、ヘッドセットだけを使用してください。

SIP と NAT の設定

SIP と Cisco IP 電話

Cisco IP 電話は Session Initiation Protocol（SIP）を使用します。このプロトコルは、SIP をサポートしているすべての IT サービス プロバイダーとの相互運用を可能にします。SIP は、IP ネットワーク上の音声通信セッションを制御する IETF 定義のシグナリング プロトコルです。

SIP は、パケットテレフォニーネットワーク内のシグナリングおよびセッション管理を処理します。シグナリングは、ネットワーク境界を越えてコール情報を伝送する機能です。セッション管理は、エンドツーエンド コールの属性を制御します。

一般的な商用 IP テレフォニー導入では、すべてのコールが SIP プロキシサーバを通過します。受信側の電話機は SIP ユーザ エージェント サーバ（UAS）と呼ばれており、要求側の電話機はユーザ エージェント クライアント（UAC）と呼ばれています。

SIP メッセージのルーティングは動的に行われます。ある SIP プロキシが UAS から接続要求を受信したが、UAC を特定できなかった場合は、プロキシがそのメッセージをネットワーク内の別の SIP プロキシに転送します。UAC が特定された場合は、応答が UAS に返され、2 つの UA がダイレクト ピアツーピア セッションを使用して接続します。音声トラフィックは、リアルタイム プロトコル（RTP）を使用して、動的に割り当てられたポートを経由して UA 間で送信されます。

RTP は、音声やビデオなどのリアルタイム データを送信しますが、データのリアルタイム配信は保証しません。RTP は、送信側と受信側のアプリケーションがストリーミング データをサポートするためのメカニズムです。通常、RTP は UDP 上で動作します。

SIP Over TCP

状態指向の通信を保証するために、Cisco IP 電話は SIP 用のトランスポート プロトコルとして TCP を使用することができます。TCP、では配信の保証が実現されているため、失われたパケットが再送されます。また、TCP は SIP パッケージが送信された順序で受信されることも保証します。

TCP は、会社のファイアウォールによる UDP ポート ブロッキングの問題を解決します。TCP を使用すると、新しいポートを開いたり、パケットをドロップしたりする必要がありません。これは、TCP がすでにインターネット閲覧や e-コマースなどの基本的な活動に使用されているためです。

SIP プロキシ冗長性

平均的なSIPプロキシサーバは、数万人の加入者を処理できます。バックアップサーバによって、アクティブサーバは一時的にメンテナンス用に切り替えることができます。シスコの電話機はバックアップSIPプロキシサーバの使用をサポートしており、サービス中断を最小化または排除しています。

プロキシ サーバのスタティック リストは常に十分であるとは限りません。たとえば、ユーザ エージェントが複数の異なるドメインにサービスを提供している場合は、各ドメインのプロキシ サーバから各 Cisco IP 電話 へのスタティック リストを設定しないでください。

プロキシの冗長性をサポートする簡単な方法は、Cisco IP 電話の設定プロファイルで SIP プロキシ サーバを設定することです。DNS SRV レコードは、SIP メッセージで指定されたドメインの SIP プロキシ サーバと通信するように電話機に指示します。電話機は DNS サーバに問い合わせます。設定されている場合は、DNS サーバが SRV レコードを返します。これには、そのドメインの SIP プロキシ サーバのリストが、ホスト名、優先順位、リスニング ポートなどとともに含まれています。Cisco IP 電話は優先度の順序でホストへの接続を試みます。

Cisco IP電話 が現在、優先順位の低いプロキシサーバを使用している場合、電話機は優先順位の高いプロキシを定期的に調べ、使用可能になったら優先順位の高いプロキシに切り替えます。

デュアル登録

電話機は、必ず、プライマリ（またはプライマリ アウトバウンド）プロキシと代替（または代替アウトバウンド）プロキシの両方に登録します。登録後は、電話機が最初にプライマリ プロキシを介して Invite SIP メッセージと Non-Invite SIP メッセージを送信します。プライマリ プロキシからの新しい INVITE に対する応答がなかった場合は、タイムアウト後に、電話機が代替プロキシとの接続を試みます。電話機がプライマリ プロキシへの登録に失敗した場合は、プライマリ プロキシを試すことなく、INVITE を代替プロキシに送信します。

デュアル登録は回線単位でサポートされます。追加された以下の 3 つのパラメータは、Web ユーザ インターフェイスとリモート プロビジョニングを介して設定できます。

- [代替プロキシ（Alternate Proxy）]：デフォルトは空です。
- [代替アウトバウンドプロキシ（Alternate Outbound Proxy）]：デフォルトは空です。
- [デュアル登録（Dual Registration）]：デフォルトは[いいえ（NO）]（オフに設定）です。

パラメータを設定したら、機能を有効にするために電話機を再起動します。

（注） 機能が正しく動作するように、プライマリ プロキシ（またはプライマリ アウトバウンド プロキシ）と代替プロキシ（または代替アウトバウンド プロキシ）の値を指定します。

デュアル登録と DNS SRV の制限

- デュアル登録を有効にする場合、DNS SRV プロキシのフォールバックまたはリカバリを無効にする必要があります。
- 他のフォールバックまたはリカバリ メカニズムとともにデュアル登録を使用しないでください。たとえば、BroadSoft メカニズムがあります。
- 機能要求のリカバリ メカニズムはありません。ただし、管理者は、プライマリおよび代替プロキシの登録状態のプロンプト更新に対する登録時間を調整できます。

デュアル登録と代替プロキシ

デュアル登録パラメータが [いいえ（No）] に設定されている場合、代替プロキシは無視されます。

フェールオーバーとリカバリ登録

- フェールオーバー：電話機は、トランスポートのタイムアウト/障害または TCP 接続失敗時にフェールオーバーを実行します。[バックアップRSCの試行（Try Backup RSC）] または [登録RSCの再試行（Retry Reg RSC）] 値にデータが入力されます。
- リカバリ：電話機は、セカンダリ プロキシに登録完了後または接続中にプライマリ プロキシに登録しようとします。

  [フェールオーバー時に自動登録（Auto Register When Failover）] パラメータは、エラーが発生したときのフェールオーバー動作を制御します。このパラメータが [はい（Yes）] に設定されている場合、電話機はフェールオーバーまたはリカバリ時に再登録されます。

フォールバック動作

フォールバックは、現在の登録が期限切れになった場合、または [プロキシのフォールバック間隔（Proxy Fallback Intvl）] が開始されると発生します。

[プロキシのフォールバック間隔（Proxy Fallback Intvl）] を超えると、すべての新しい SIP メッセージがプライマリ プロキシに送信されます。

たとえば、[登録期限切れ（Register Expires）] の値が 3600 秒で、[プロキシのフォールバック間隔（Proxy Fallback Intvl）] が 600 秒の場合、フォールバックは 600 秒後にトリガーされます。

[登録期限切れ（Register Expires）] の値が 800 秒で、[プロキシのフォールバック間隔（Proxy Fallback Intvl）] が 1000 秒の場合、フォールバックは 800 秒でトリガーされます。

元のプライマリ サーバへの登録が正常に行われると、すべての SIP メッセージはプライマリ サーバに送信されます。

RFC3311

Cisco IP 電話は、RFC-3311 の SIP UPDATE メソッドをサポートします。

SIP NOTIFY XML サービス

Cisco IP 電話は、SIP NOTIFY XML サービス イベントをサポートします。電話機は、XML サービス イベントを含む SIP NOTIFY メッセージを受信すると、メッセージに正しいクレデンシャルが含まれていない場合、401 応答で NOTIFY をチャレンジします。クライアントは、IP フォンの対応する回線の SIP アカウント パスワードと MD5 ダイジェストを使用して正しいクレデンシャルを提供する必要があります。

メッセージの本文には XML イベント メッセージを含めることができます。例：

```
<CiscoIPPhoneExecute>
  <ExecuteItem Priority="0" URL="http://xmlserver.com/event.xml"/>
</CiscoIPPhoneExecute>
```

認証：

```
challenge  = MD5( MD5(A1) ":" nonce ":" nc-value ":" cnonce ":" qop-value
":" MD5(A2) )
where A1 = username ":" realm ":" passwd
and A2 = Method ":" digest-uri
```

電話機を使用した NAT トランスバーサル

ネットワーク アドレス変換（NAT）を使用すると、複数のデバイスでルーティング可能な単一のパブリック IP アドレスを共有して、インターネット経由で接続を確立することができます。NAT は、パブリックおよびプライベート IP アドレスを変換するために多くのブロードバンド アクセス デバイスに備えられています。VoIP が NAT と共存するには、NAT トラバーサルが必要です。

すべてのサービス プロバイダーが NAT トラバーサルを提供しているわけではありません。サービス プロバイダーが NAT トラバーサルを提供していない場合、次のようなオプションがあります。

- **セッションボーダーコントローラを使用した NAT マッピング**：セッション ボーダー コントローラを介して NAT マッピングをサポートするサービスプロバイダーを選択することをお勧めします。サービス プロバイダーが提供する NAT マッピングを使用すると、ルータの選択肢が増えます。
- **SIP-ALGルーターを使用したNATマッピング**NAT マッピングは、SIP アプリケーション レイヤゲートウェイ（ALG）を備えたルータを使用して実現できます。SIP-ALG ルータを使用すると、サービス プロバイダーの選択肢が増えます。
- **静的 IP アドレスを使用した NATマッピング**:外部（パブリック）静的IPアドレスを使用したNATマッピングによって、サービスプロバイダーとの相互運用性を確実にすることを実現できます。ルータで使用される NAT メカニズムは対称である必要があります。詳細については、対称または非対称 NAT の決定を参照してください。

  NAT マッピングは、サービス プロバイダー ネットワークがセッション ボーダー コントローラ機能を提供しない場合にのみ使用します。静的 IP を使用した NAT マッピングを設

定する方法の詳細については、静的 IP アドレスを使用した NAT マッピングを設定するを参照してください。

- **STUNを使用したNATマッピング**：サービス プロバイダー ネットワークがセッション ボーダー コントローラ機能を提供しない場合、および他の要件が満たされている場合、NAT（STUN）用のセッション トラバーサル ユーティリティを使用して NAT マッピングを検出することができます。STUN を使用した NAT マッピングの設定方法の詳細については、STUN を使用した NAT マッピングの設定を参照してください。

セッション ボーダー コントローラを使用した NAT マッピング

セッション ボーダー コントローラを介して NAT マッピングをサポートするサービス プロバイダーを選択することをお勧めします。サービス プロバイダーが提供する NAT マッピングを使用すると、ルータの選択肢が増えます。

SIP-ALG ルータを使用した NAT マッピング

NAT マッピングは、SIP アプリケーション層ゲートウェイ（ALG）を備えたルータを使用して実現できます。SIP-ALG ルータを使用すると、サービス プロバイダーの選択肢が増えます。

Cisco 検出プロトコル

Cisco Discovery Protocol（CDP）はネゴシエーション ベースであり、Cisco IP 電話 が存在する仮想 LAN（VLAN）を特定します。Cisco スイッチを使用している場合、Cisco Discovery Protocol（CDP）が利用可能であり、デフォルトで有効にされます。CDP には、次の属性があります。

- ネイバー デバイスのプロトコル アドレスを取得し、各デバイスのプラットフォームを検出します。
- ルータが使用しているインターフェイスに関する情報を表示します。
- メディアおよびプロトコルに依存しません。

CDP なしで VLAN を使用している場合、Cisco IP 電話の VLAN ID を入力する必要があります。

LLDP-MED

Cisco IP 電話は、レイヤ 2 自動ディスカバリ メカニズムを使用するシスコまたは他のサードパーティ ネットワーク接続デバイスでの導入のために Link Layer Discovery Protocol for Media Endpoint Devices（LLDP-MED）をサポートしています。LLDP-MED の実装は、2005 年 5 月の IEEE 802.1AB（LLDP）仕様と 2006 年 4 月の ANSI TIA-1057 に従って実行されます。

Cisco IP 電話は、メディア エンドポイント ディスカバリ参照モデルと定義（ANSI TIA-1057 セクション 6）に従って、ネットワーク接続機器への LLDP-MED 直接リンクを備えた LLDP-MED メディア エンドポイント クラス III デバイスとして動作します。

技術的な詳細

Cisco IP 電話は、LLDP-MED メディア エンド ポイント デバイス クラス III として、次の限定された一連のタイプ/長さ/値のみをサポートします。

- シャーシ ID TLV
- ポート ID TLV
- パケット存続時間（TTL）TLV
- ポート記述 TLV
- システム名 TLV
- システム機能 TLV
- IEEE 802.3 MAC/PHY コンフィギュレーション/ステータス TLV（有線ネットワークの場合のみ）
- LLDP-MED 機能 TLV
- LLDP-MED ネットワーク ポリシー TLV（アプリケーション タイプが音声の場合のみ）
- LLDP-MED 拡張 Power-Via-MDI TLV（有線ネットワークの場合のみ）
- LLDP-MED ファームウェア リビジョン TLV
- LLDPDU TLV の最後

発信 LLDPDU には、上記の TLV がすべて（該当する場合）含まれます。着信 LLDPDU の場合、次の TLV のいずれかがない場合、LLDPDU は破棄されます。他のすべての TLV は検証されず、無視されます。

- シャーシ ID TLV
- ポート ID TLV
- パケット存続時間（TTL）TLV
- LLDP-MED 機能 TLV
- LLDP-MED ネットワーク ポリシー TLV（アプリケーション タイプが音声の場合のみ）
- LLDPDU TLV の最後

Cisco IP 電話は、該当する場合 LLDPDU を送信します。LLDPDU のフレームには、次の TLV が含まれます。

- シャーシ ID TLV
- ポート ID TLV
- パケット存続時間（TTL）TLV
- LLDPDU TLV の最後

Cisco IP 電話の LLDP-MED の実装にはいくつかの制限があります。

- ネイバー情報の格納と検索はサポートされていません。
- SNMP および対応する MIB はサポートされていません。
- 統計情報カウンタの記録と検索はサポートされていません。
- すべて TLV の完全な検証は行われません。電話機に適用されない TLV は無視されます。
- 標準規格に示されるプロトコル ステート マシンは、参照目的でのみ使用されます。

シャーシ ID TLV

発信 LLDPDU の場合、TLV は subtype=5（ネットワーク アドレス）をサポートします。IP アドレスがわかっている場合、シャーシ ID の値は INAN アドレス ファミリ番号のオクテットに、音声通信に使用される IPv4 アドレスのオクテット文字列が続きます。IP アドレスが不明な場合、シャーシ ID の値は `0.0.0.0` です。サポートされている唯一の INAN アドレス ファミリは IPv4 です。現在、シャーシ ID に対して IPv6 アドレスはサポートされていません。

着信 LLDPDU では、シャーシ ID は MSAP 識別子を形成する不透明な値として扱われます。値はそのサブタイプに照らして検証されません。

シャーシ ID TLV は最初の TLV として必須です。発信および着信 LLDPDU に対して 1 つのシャーシ ID TLV のみ許可されます。

ポート ID TLV

発信 LLDPDU では、TLV は subtype=3（MAC アドレス）をサポートします。イーサネット ポート用の 6 オクテットの MAC アドレスは、ポート ID の値に使用されます。

着信 LLDPDU の場合、ポート ID TLV は MSAP 識別子を形成する不透明な値として扱われます。値はそのサブタイプに照らして検証されません。

ポート ID TLV は 2 番目の TLV として必須です。発信および着信 LLDPDU に対して 1 つのポート ID TLV のみ許可されます。

パケット存続時間（TTL）TLV

発信 LLDPDU では、パケット存続時間（TTL）値は 180 秒です。これは、標準規格で推奨される 120 秒値とは異なります。シャット ダウン LLDPDU の場合、TTL 値は常に 0 です。

パケット存続時間 TLV は、3 番目の TLV として必須です。発信および着信 LLDPDU ポートに対して 1 つのパケット存続時間（TLV）のみ許可されます。

LLDPDU TLV の最後

値は 2 オクテットで、すべてゼロです。この TLV は必須で、発信および着信 LLDPDU に対して 1 つだけ許可されます。

ポート記述 TLV

発信 LLDPDU では、ポート記述 TLV のポート記述の値は CDP の「ポート ID TLV」と同じになります。着信 LLDPDU の場合、ポート記述 TLV は無視され、検証されません。発信および着信 LLDPDU に対して 1 つのポート記述 TLV のみ許可されます。

システム名 TLV

Cisco IP 電話の値は SEP+MAC アドレスです。

例：SEPAC44F211B1D0

着信LLDPDUの場合、システム名TLVは無視され、検証されません。発信および着信LLDPDUポートに対して 1 つのシステム名 TLV のみ許可されます。

システム機能 TLV

発信 LLDPDU では、システム機能 TLV で、2 オクテット システム機能フィールドのビット値を、PC ポートを備えた電話機の場合はビット 2（ブリッジ）とビット 5（電話機）に設定する必要があります。電話機に PC ポートがない場合、ビット 5 のみを設定する必要があります。同じシステム機能値を、有効な機能フィールドに設定する必要があります。

着信 LLDPDUでは、システム機能 TLV は無視されます。TLV は MED デバイス タイプに対して意味的な検証は行われません。

システム機能 TLV は発信 LLDPDU で必須です。1 つのシステム機能 TLV のみ許可されます。

管理アドレス TLV

TLVは、ローカルLLDPエージェント（上位層のエンティティに到達するために使用される）に関連付けられているアドレスを識別して、ネットワーク管理によるディスカバリを補助します。TLV によって、この管理アドレスに関連付けられているシステム インターフェイス番号とオブジェクト識別子（OID）（いずれかまたは両方が判明している場合）を両方含めることができます。

- [TLV情報文字列長（TLV information string length）]：このフィールドには、TLV 情報文字列内のすべてのフィールドの長さ（オクテット単位）が含まれます。
- [管理アドレス文字列長（Management address string length）]：このフィールドには、管理アドレス サブタイプと管理アドレスのフィールドの長さ（オクテット）が含まれます。

システム記述 TLV

この TLV を使用して、ネットワーク管理でシステム記述をアドバタイズできます。

- [TLV情報文字列長（TLV information string length）]：このフィールドは、システム記述の正確な長さ（オクテット単位）を示します。

- [システム説明（System Description）]：このフィールドには、ネットワーク エンティティのテキスト記述である英数字文字列が含まれます。システム記述には、システムのハードウェア タイプ、ソフトウェア オペレーティング システム、ネットワーク ソフトウェアの完全な名前とバージョン識別番号が含まれます。実装で IETF RFC 3418 がサポートされる場合、このフィールドに sysDescr オブジェクトを使用する必要があります。

IEEE 802.3 MAC/PHY コンフィギュレーション/ステータス TLV

TLVは、自動ネゴシエーション用ではなく、トラブルシューティング目的で使用されます。着信 LLDPDU の場合、TLV は無視され、検証されません。発信 LLDPDU の場合、TLV に対して、オクテット値の自動ネゴシエーションのサポート/ステータスは次のようになります。

- ビット 0：自動ネゴシエーションのサポート機能がサポートされていることを示す 1 に設定します。
- ビット 1：自動ネゴシエーションの状態が有効であることを示す 1 に設定します。
- ビット 2 ～ 7：0 に設定します。

2 オクテットの PMD 自動ネゴシエーション アドバタイズ機能フィールドのビット値は次のように設定する必要があります。

- ビット 13：10BASE-T 半二重モード
- ビット 14：10BASE-T 全二重モード
- ビット 11：100BASE-TX 半二重モード
- ビット 10：100BASE-TX 全二重モード
- ビット 15：不明

ビット 10、11、13、14 を設定する必要があります。

2 オクテットの運用 MAU タイプの値は、実際の運用 MAU タイプを反映するように設定する必要があります。

- 16：100BASE-TX 全二重
- 15：100BASE-TX 半二重
- 11：10BASE-T 全二重
- 10：10BASE-T 半二重

たとえば、通常、電話機は 100BASE-TX 全二重に設定されます。つまり、値 16 を設定する必要があります。TLV は有線ネットワークではオプションで、ワイヤレス ネットワークには適用できません。電話機は、この TLV を有線モード時のみ送信します。電話機が自動ネゴシエーション用に設定されておらず、発信 LLDPDU TLV 用に特定の速度/デュプレックスが設定されている場合、オクテット値の自動ネゴシエーションのサポート/ステータスのビット 1 をクリアして（0）、自動ネゴシエーションが無効であることを示す必要があります2 オクテットの

PMD 自動ネゴシエーション アドバタイズ機能フィールドは、不明を示す 0x8000 に設定する必要があります。

LLDP-MED 機能 TLV

発信 LLDPDU では、TLV は 2 オクテットの機能フィールドに次のビットが設定されているデバイス タイプ 3（エンド ポイント クラス III）を TLV に設定する必要があります。

ビット位置	機能
0	LLDP-MED 機能
1	ネットワーク ポリシー
4	MDI-PD 経由の拡張電源
5	インベントリ

着信 TLV では、LLDP-MED TLV が存在しない場合、LLDPDU は破棄されます。LLDP-MED 機能の TLV は必須で、発信および着信 LLDPDU に対して 1 つだけ許可されます。他の LLDP-MED TLV は、LLDP-MED 機能の前に存在している場合、無視されます。

ネットワーク ポリシー TLV

発信 LLDPDU の TLV では、VLAN または DSCP が決定される前に、不明ポリシー フラグ（U）が 1 に設定されます。VLAN 設定または DSCP が判明している場合、値は 0 に設定されます。ポリシーが不明な場合、他のすべての値が 0 に設定されます。VLAN が決定または使用される前に、タグ付きフラグ（T）は 0 に設定されます。電話機にタグ付き VLAN（VLAN ID > 1）が使用されている場合、タグ付きフラグ（T）は 1 に設定されます。予約済み（X）は常に 0 に設定されます。VLAN が使用されている場合、対応する VLAN ID と L2 優先順位が必要に応じて設定されます。VLAN ID の有効な値は 1 ～ 4094 です。ただし、VLAN ID = 1 は使用されません（制限）。DSCP が使用される場合、必要に応じて値は 0 ～ 63 になります。

着信 LLDPDU の TLV では、さまざまなアプリケーション タイプに対応する複数のネットワーク ポリシー が許可されます。

LLDP-MED 拡張 Power-Via-MDI TLV

発信 LLDPDU の TLV では、電源タイプの 2 進値が「0 1」に設定され、電話機の電源タイプが PD デバイスであることを示します。電話機の電源は、2 進値「1 1」の「PSE とローカル」に設定されます。電力優先順位はバイナリ「0 0 0 0」に設定されて優先順位は不明であることが示されますが、電力値は最大電力値に設定されます。Cisco IP 電話の電力値は 12900 mW です。

着信 LLDPDU の場合、TLV は無視され、検証されません。発信および受信の LLDPDU で許可されるのは、1 つの TLV のみです。電話機は、有線ネットワークの場合のみ TLV を送信します。

LLDP-MED 標準規格は、イーサネットのコンテキストで草稿されました。ワイヤレス ネットワークの LLDP-MED について議論が進行中です。ANSI-TIA 1057、付録 C、「C.3 Applicable TLV for VoWLAN」の表 24 を参照してください。TLV はワイヤレス ネットワークのコンテキストでは適用しないことをお勧めします。この TLV は、PoE とイーサネットのコンテキストでの使用を対象にしています。TLV を追加しても、スイッチのネットワーク管理または電源ポリシーの調整では値が提供されません。

LLDP-MED インベントリ管理 TLV

この TLV は、デバイス クラス III のオプションです。発信 LLDPDU の場合は、ファームウェア リビジョン TLV のみをサポートします。ファームウェア リビジョンの値は、電話機のファームウェアのバージョンです。着信 LLDPDU の場合、TLV は無視され、検証されません。発信および受信の LLDPDU で許可されるのは、1 つのファームウェア リビジョン TLV のみです。

最終的なネットワーク ポリシーの解決と QoS

特別な VLAN

VLAN=0、VLAN=1、および VLAN=4095 は、タグなしの VLAN と同じように扱われます。VLAN にタグがないため、サービス クラス（CoS）は適用されません。

SIP モードのデフォルトの QoS

CDP または LLDP-MED からのネットワーク ポリシーが存在しない場合、デフォルトのネットワーク ポリシーが使用されます。CoS は、特定の内線番号の設定に基づいています。これは、手動 VLAN が有効で、手動 VLAN ID が 0、1、または 4095 と等しくない場合にのみ適用されます。タイプ オブ サービス（ToS）は、特定の内線番号の設定に基づいています。

CDP の QoS 解決

CDP からの有効なネットワーク ポリシーが存在する場合：

- VLANが0、1、または4095の場合、VLANは設定されないか、タグなしになります。CoSは適用されませんが、DSCP は適用されます。ToS は、前述のようにデフォルトに基づいています。
- 1 より大きく、4095 より小さい VLAN は適宜設定されます。CoS と ToS は、前述のようにデフォルトに基づいています。DSCP が適用されます。
- 電話機は再起動し、ファスト スタート シーケンスが再開します。

LLDP-MED の QoS 解決

CoS が適用可能で、CoS = 0 の場合、前述のように、デフォルトが特定の内線番号に使用されます。ただし、発信 LLDPDU の TLV の L2 優先順位に表示される値は、内線番号 1 に使用される値に基づきます。CoS が適用可能で、CoS != 0 の場合、CoS はすべての内線番号に使用されます。

DSCP（ToS にマップされた）が適用可能で、DSCP = 0 の場合、前述のように、デフォルトが特定の内線番号に使用されます。ただし、発信 LLDPDU の TLV の DSCP に表示される値は、内線番号 1 に使用される値に基づきます。DSCP が適用可能で、DSCP != 0 の場合、DSCP はすべての内線番号に使用されます。

1 より大きく、4095 より小さい VLAN は適宜設定されます。CoS と ToS は、前述のようにデフォルトに基づいています。DSCP が適用されます。

LLDP-MED PDU からの音声アプリケーションに有効なネットワーク ポリシーがある場合、およびタグ付きフラグが設定されている場合、VLAN、L2 優先順位（CoS）、および DSCP（ToS にマップされた）がすべて適用できます。

LLDP-MED PDU からの音声アプリケーションに有効なネットワーク ポリシーがある場合、およびタグ付きフラグが設定されていない場合、DSCP（ToS にマップされた）のみ適用できます。

Cisco IP 電話は再起動し、ファスト スタート シーケンスが再開します。

CDP との共存

CDP と LLDP-MED の両方が有効になっている場合は、VLAN のネットワーク ポリシーにより、ディスカバリ モードのいずれかで設定または変更される最後のポリシーが決定されます。LLDP-MED と CDP の両方が有効になっている場合は、起動中に電話機が CDP PDU と LLDP-MED PDU を送信します。

CDP モードと LLDP-MED モードに関するネットワーク接続デバイスの設定と動作が一貫していない場合は、異なる VLAN に切り替えられることになり、電話機の再起動動作が変動する可能性があります。

VLAN が CDP と LLDP-MED によって設定されなかった場合は、手動で設定された VLAN ID が使用されます。VLAN ID が手動で設定されなかった場合は、どの VLAN もサポートされません。必要に応じて DSCP が使用され、ネットワーク ポリシーによって LLDP-MED が決定されます。

LLDP-MED と複数のネットワーク デバイス

ネットワーク ポリシーに対して同じアプリケーション タイプを使用できます。ただし、電話機は、複数のネットワーク接続デバイスから異なるレイヤ 2 またはレイヤ 3 QoS ネットワーク ポリシーを受信します。このような場合は、最後の有効なネットワーク ポリシーが受け入れられます。

LLDP-MED と IEEE 802.X

Cisco IP 電話はIEEE 802.X をサポートせず、802.1 X 有線環境では機能しません。ただし、ネットワーク デバイス上の IEEE 802.1 X またはスパニング ツリー プロトコルによって、ファストスタートの応答が遅延する可能性があります。