



技術的な詳細

- [ネットワーク プロトコル \(1 ページ\)](#)
- [VLAN の連携 \(5 ページ\)](#)
- [USB ポート情報 \(6 ページ\)](#)
- [SIP と NAT の設定 \(8 ページ\)](#)
- [Cisco Discovery Protocol, on page 14](#)
- [LLDP-MED, on page 15](#)
- [最終的なネットワーク ポリシーの解決と QoS \(20 ページ\)](#)

ネットワーク プロトコル

Cisco IP 電話 8800 シリーズは、音声通信に必要な業界標準ネットワーク プロトコルおよびシスコネットワーク プロトコルを複数サポートしています。次の表に、電話でサポート対象ネットワーク プロトコルの概要を示します。

表 1: Cisco IP 電話 8800 シリーズでサポート対象ネットワーク プロトコル

ネットワーク プロトコル	目的	使用上の注意
Bluetooth	Bluetooth は、短距離におけるデバイスの通信方法を指定する Wireless Personal Area Network (WPAN) プロトコルです。	Cisco IP 電話s 8845、8865、および 8851 は Bluetooth 4.1 をサポートしています。 Cisco IP 電話 8861 は Bluetooth 4.0 をサポートしています。 Cisco IP 電話 8811 および 8841 では Bluetooth をサポートしていません。
Bootstrap Protocol (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。	—

ネットワーク プロトコル	目的	使用上の注意
Cisco Discovery Protocol (CDP)	<p>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。</p> <p>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、他のデバイスの情報を受信することができます。</p>	<p>Cisco IP 電話では、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。</p>
Dynamic Host Configuration Protocol (DHCP)	<p>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。</p> <p>DHCPを使用すると、IP電話機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。</p>	<p>DHCPは、デフォルトでは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。</p> <p>(注) [使用するDHCPオプション (DHCP Option To Use)] パラメータのデフォルト値は、66、160、159、150、60、43、125です。この値は、電話機が DHCP サーバによって指定された IP アドレスを使用する順序を示します。</p>
Hypertext Transfer Protocol (HTTP)	<p>HTTPは、インターネットやWeb経路で情報を転送し、ドキュメントを移送するための標準的な手段です。</p>	<p>Cisco IP 電話は、XML サービス、電話機のプロビジョニング、電話機のアップグレード、およびトラブルシューティングに HTTP プロトコルを使用します。</p>
Hypertext Transfer Protocol Secure (HTTPS)	<p>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。</p>	<p>一部の Web アプリケーションは、HTTP プロトコルと HTTPS プロトコルの両方をサポートします。HTTPS をサポートする Cisco IP 電話は、HTTPS URL を使用します。</p>

ネットワーク プロトコル	目的	使用上の注意
IEEE 802.1X	<p>IEEE 802.1X 標準は、クライアント/サーバベースのアクセスコントロールと認証プロトコルを定義します。これにより、未承認のクライアントが一般にアクセス可能なポートから LAN に接続するのを制限します。</p> <p>802.1X アクセス コントロールでは、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN (EAPOL) トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。</p>	<p>Cisco IP 電話では、EAP-FAST および EAP-TLS 認証方式をサポートすることによって、IEEE 802.1X 標準が実装されています。</p> <p>電話機で 802.1X 認証が有効になっている場合、PC ポートとボイス VLAN を無効にする必要があります。</p>
IEEE 802.11n/802.11ac	<p>IEEE 802.11 標準は、ワイヤレス ローカルエリア ネットワーク (WLAN) におけるデバイスの通信方法を指定します。</p> <p>802.11n は 2.4 GHz 帯域と 5 GHz 帯域で動作し、802.11ac は 5 GHz 帯域で動作します。</p>	<p>802.11 インターフェイスは、イーサネットのケーブル接続が利用できないか望ましくない場合の展開オプションです。</p> <p>Cisco IP 電話 8861 および 8865 のみ WLAN をサポートします。</p>
インターネット プロトコル (IP)	<p>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。</p>	<p>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。</p> <p>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。</p>
リンク層検出プロトコル (LLDP)	<p>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。</p>	<p>Cisco IP 電話は、PC ポートで LLDP をサポートします。</p>

ネットワーク プロトコル	目的	使用上の注意
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MEDは、音声製品用LLDP標準の拡張です。	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>LLDP-MED サポートの詳細については、LLDP-MED および『Cisco Discovery Protocol』ホワイトペーパーを参照してください。</p> <p>http://www.cisco.com/US/65370techmgw/pt00ac8046.html</p>
Real-Time Transport Protocol (RTP)	RTPは、インタラクティブな音声のよう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、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。

ネットワーク プロトコル	目的	使用上の注意
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 VoIP プロトコルと同様に、SIP はシグナリングとセッション管理の機能をパケットテレフォニーネットワークの内部で処理します。シグナリングによって、ネットワーク境界を越えて通話情報を伝送することが可能になります。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。 Cisco IP 電話は、電話機が IPv6 のみ、IPv4 のみ、または IPv4 と IPv6 の両方で動作している場合に SIP プロトコルをサポートします。
Transmission Control Protocol (TCP)	TCP は、接続型の転送プロトコルです。	Cisco IP 電話は、サードパーティコール制御システムへの接続、および XML サービスへのアクセスに TCP を使用します。
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。	セキュリティが実装されると、Cisco IP 電話は、サードパーティコール制御システムへの登録を安全に行う際に TLS プロトコルを使用します。
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 は DHCP サーバが自動的に識別する TFTP サーバがネットワーク内に必要です。
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。電話機の SIP シグナリングは UDP をサポートしていません。

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 アドレスが十分で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 からアクセスできます。

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

USB ポート情報

Cisco IP 電話 8851、8861、および 8865 は各 USB ポートに接続する最大で 5 つのデバイスをサポートします。電話機に接続された各デバイスは、最大デバイス数に含まれます。たとえば、ご使用の電話機は側面ポートで 5 台の USB デバイス、背面ポートでさらに 5 台の標準 USB デバイスをサポートできます。多くのサードパーティ製 USB 製品は複数の USB デバイスとしてカウントされます。たとえば、USB ハブとヘッドセットを含むデバイスは、2 台の USB デバイスとしてカウントできます。詳細については、USB デバイスのマニュアルを参照してください。



- (注)
- 通電していないハブはサポートされません。また、電力供給されていても 5 個以上のポートを備えたハブはサポートされません。
 - USB ハブを経由して電話機に接続している USB ヘッドセットはサポートされません。

電話機に接続された各キー拡張モジュールは、USB デバイスとしてカウントされます。3 台のキー拡張モジュールが電話機に接続されている場合、これらは 3 台の USB デバイスとしてカウントされます。

USB ポートを無効にする

ユーザーが特定の目的で1つまたはすべての USB ポートを使用できないようにする場合は、電話機の背面または側面、または両方の USB ポートを無効にできます。無効にされた USB ポートは機能しません。たとえば、無効にされた USB ポートは、USB ヘッドセットとキー拡張モジュール (KEM) を認識しません。また、接続されているデバイスも充電しません。

Cisco IP Phone 8851 には、1つの USB ポート (側面 USB ポート) だけが含まれています。Cisco IP Phone 8861 および 8865 には、2つの USB ポート (1つの側面 USB ポートと1つの背面 USB ポート) が含まれています。

始める前に

電話管理の Web ページにアクセスします。 [電話機 ウェブインターフェイスへのアクセス](#) を参照してください。

手順

ステップ 1 [音声 (Voice)] > [システム (System)] を選択します。

ステップ 2 [電源設定 (Power Settings)] セクションで、パラメータ [背面 USB ポートを無効にする (Disable Back USB Port)] を [はい (Yes)] に設定して背面 USB ポートを無効にします。

次の形式で文字列を入力することによって、設定ファイル (cfg.xml) でこのパラメータを設定することができます。

```
<Disable_Back_USB_Port ua="na">No</Disable_Back_USB_Port>
```

オプション: [はい (Yes)] と [いいえ (No)]

デフォルト: [いいえ (No)]

ステップ 3 [電源設定 (Power Settings)] セクションで、パラメータ [側面 USB ポートを無効にする (Disable Side USB Port)] を [はい (Yes)] に設定して側面 USB ポートを無効にします。

次の形式で文字列を入力することによって、設定ファイル (cfg.xml) でこのパラメータを設定することができます。

```
<Disable_Side_USB_Port ua="na">No</Disable_Side_USB_Port>
```

オプション: [はい (Yes)] と [いいえ (No)]

デフォルト: [いいえ (No)]

ステップ 4 [すべての変更の送信 (Submit All Changes)] をクリックします。

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通話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。電話機はバックアップ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。

プロキシの冗長性をサポートする簡単な方法は、電話機の設定プロファイルで SIP プロキシサーバを指定することです。電話機は DNS サーバに DNS NAPTR または SRV クエリを送信し

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。電話機は優先度の順序でサーバへの接続を試みます。番号が小さいサーバは、より高い優先順位を持ちます。クエリでは最大 6 個の NAPTR レコードと 12 個の SRV レコードがサポートされています。

電話機がプライマリサーバとの通信に失敗すると、電話機は優先順位の低いサーバにフェールオーバーできるようになります。設定されている場合、電話機はプライマリに接続を復元できます。フェールオーバーとフェールバックのサポートは、異なる SIP トラnsポートプロトコルを使用しているサーバ間で切り替わります。電話機は、通話が終了しフェールバック条件が満たされるまで、アクティブコール中のプライマリサーバへのフェールバックを実行しません。

DNS サーバからのリソースレコードの例

```
aslbsoft      3600      IN NAPTR 50 50 "s" "SIPS+D2T" "" _sips._tcp.tlstest
              3600      IN NAPTR 90 50 "s" "SIP+D2T" "" _sip._tcp.tcptest
              3600      IN NAPTR 100 50 "s" "SIP+D2U" "" _sip._udp.udptest

_sips._tcp.tlstest  SRV 1 10 5061 srv1.sipurash.com.
                    SRV 2 10 5060 srv2.sipurash.com.
_sip._tcp.tcptest  SRV 1 10 5061 srv3.sipurash.com.
                    SRV 2 10 5060 srv4.sipurash.com.
_sip._udp.udptest  SRV 1 10 5061 srv5.sipurash.com.
                    SRV 2 10 5060 srv6.sipurash.com.

srv1      3600      IN      A      1.1.1.1
srv2      3600      IN      A      2.2.2.2
srv3      3600      IN      A      3.3.3.3
srv4      3600      IN      A      4.4.4.4
srv5      3600      IN      A      5.5.5.5
srv6      3600      IN      A      6.6.6.6
```

次の例は、電話機の視点から見たサーバの優先順位を示しています。

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	UP
2nd	2.2.2.2	TLS	UP
3rd	3.3.3.3	TCP	UP
4th	4.4.4.4	TCP	UP
5th	5.5.5.5	UDP	UP
6th	6.6.6.6	UDP	UP

電話機は、常に、最優先順位を持つ使用可能なアドレスに SIP メッセージを送信し、リスト内のステータスを取得します。この例では、電話機はすべての SIP メッセージをアドレス 1.1.1.1 に送信します。リストの 1.1.1.1 アドレスがステータスを DOWN としてマークされている場合、電話機は代わりに 2.2.2.2 と通信します。電話機は、指定されたフェールバック条件が満たされた場合に、接続を 1.1.1.1 に復元できます。フェールオーバーとフェールバックの詳細については、[SIP プロキシフェールオーバー \(9 ページ\)](#) と [SIP プロキシフェールバック \(11 ページ\)](#) を参照してください。

SIP プロキシ フェールオーバー

電話機は、次のいずれかの場合にフェールオーバーを実行します。

- 電話機は SIP メッセージを送信し、サーバからの応答を受信しません。
- サーバは、**バックアップ RSC を試す**で指定されたコードと一致するコードを使用して応答します。
- 電話機は TCP 切断リクエストを取得します。

SIP トラnsポートが自動に設定されている場合は、フェールオーバー時に自動登録を[はい(Yes)]に設定することを強く推奨します。

内線固有パラメータは、設定ファイル(cfg.xml)でも設定できます。

```
<SIP_Transport_n_ua="na">Auto</SIP_Transport_n_>
<Auto_Register_When_Failover_n_ua="na">Yes</Auto_Register_When_Failover_n_>
```

*n*は内線番号です。

電話機のフェールオーバー動作

電話機は、現在接続されているサーバとの通信に失敗すると、サーバー一覧のステータスを更新します。利用不可能なサーバー一覧のステータスがDOWNとしてマークされています。電話機は、リストにステータスを設定して、上位優先順位のサーバに接続しようとしています。

次の例では、アドレス 1.1.1.1 と 2.2.2.2 は使用できません。電話機は 3.3.3.3 に SIP メッセージを送信します。これは、ステータスがあるサーバの中で最上位の優先順位を持っています。

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	DOWN
2nd	2.2.2.2	TLS	DOWN
3rd	3.3.3.3	TCP	UP
4th	4.4.4.4	TCP	UP
5th	5.5.5.5	UDP	UP
6th	6.6.6.6	UDP	UP

次の例では、DNS NAPTR 応答に 2 つの SRV レコードがあります。各 SRV レコードには、3 つの A レコード (IP アドレス) があります。

Priority	IP Address	SIP Protocol	Server	Status
1st	1.1.1.1	UDP	SRV1	DOWN
2nd	1.1.1.2	UDP	SRV1	UP
3rd	1.1.1.3	UDP	SRV1	UP
4th	2.2.2.1	TLS	SRV2	UP
5th	2.2.2.2	TLS	SRV2	UP
6th	2.2.2.3	TLS	SRV2	UP

電話機は 1.1.1.1 に接続できなかったものとし、次に 1.1.1.2 に登録するとしましょう。1.1.1.2 がダウンすると、電話機の動作は **プロキシフォールバック Intvl** の設定によって異なります。

- プロキシフォールバック **Intvl** が **0** に設定されている場合、電話機は次の順序でアドレスを使用します。1.1.1.1、1.1.1.3、2.2.2.1、2.2.2.2、2.2.2.3。
- **Proxy Fallback Intvl** が 0 以外の値に設定されている場合、電話機は次の順序でアドレスを使用します。1.1.1.3、2.2.2.1、2.2.2.2、2.2.2.3。

SIP プロキシ フォールバック

プロキシフォールバック **Intvl** では、電話機の Web インターフェイスの **内線 (n)** タブで、0 以外の値が指定されている必要があります。このフィールドを 0 に設定すると、SIP プロキシフェールバック機能は無効になります。内線固有パラメータは、次の形式で設定ファイル(cfg.xml)も設定できます。

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
```

n は内線番号です。

電話機がフェールバックをトリガーする時間は、電話機の設定と使用している SIP トランスポートプロトコルによって異なります。

電話機が異なる SIP トランスポートプロトコル間でフェールバックを実行できるようにするには、電話機の Web インターフェイスの **内線 (n)** タブで **SIP トランスポート** を **自動** に設定します。次の XML 文字列を使用して、設定ファイルでこの内線固有のパラメータを設定することもできます。

```
<SIP_Transport_n_ ua="na">Auto</SIP_Transport_n_>
```

n は内線番号です。

UDP 接続からのフェールバック

UDP 接続からのフェールバックは、SIP メッセージによってトリガーされます。次の例では、サーバからの応答がないため、電話機が時間 T1 で 1.1.1.1 (TLS) の登録に最初に失敗しました。SIP Timer F の期限が切れると、電話機は時間 T2 (T2 = T1 + SIP タイマー F) で 2.2.2.2 (UDP) に登録されます。現在の接続は、UDP 経由で 2.2.2.2 上です。

Priority	IP Address	SIP Protocol	Status	
1st	1.1.1.1	TLS	DOWN	T1 (Down time)
2nd	2.2.2.2	UDP	UP	
3rd	3.3.3.3	TCP	UP	

電話機の設定は次のとおりです。

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
<Register_Expires_n_ ua="na">3600</Register_Expires_n_>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
```

n は内線番号です。

電話機は、T2 (T2=(3600-16)*78%) の時点で登録を更新します。電話機は、IP アドレスとダウンタイムを使用して、アドレス一覧を確認します。条件 T2-T1 >= 60、障害が発生したサーバ 1.1.1.1 が復旧し、一覧が次のように更新されます。電話機は、1.1.1.1 に SIP メッセージを送信します。

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	UP
2nd	2.2.2.2	UDP	UP
3rd	3.3.3.3	TCP	UP

TCP または TLS の接続からのフェールバック

TCP または TLS のいずれかの接続からのフェールバックは、パラメータ **プロキシのフォールバック Intvl** によってトリガーされます。次の例では、電話機は T1 で 1.1.1.1 (UDP) の時点で登録できなかったため、2.2.2.2 (TCP) に登録されませんでした。現在の接続は、TCP 経由で 2.2.2.2 上です。

Priority	IP Address	SIP Protocol	Status	
1st	1.1.1.1	UDP	DOWN	T1 (Down time)
2nd	2.2.2.2	TCP	UP	
3rd	3.3.3.3	TLS	UP	

電話機の設定は次のとおりです。

```
<Proxy_Fallback_Intvl_n_ua="na">60</Proxy_Fallback_Intvl_n_>
<Register_Expires_n_ua="na">3600</Register_Expires_n_>
<SIP_Timer_F_ua="na">16</SIP_Timer_F_>
```

n は内線番号です。

プロキシフォールバック間隔 (60 秒) が T1 からカウントダウンします。電話機は、T1 + 60 の時点でプロキシフェールバックをトリガーします。この例では、プロキシのフォールバック間隔を 0 に設定すると、電話機は 2.2.2.2 に接続を維持します。

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 ユーザー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。



Note 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。次に例を示します。

```
<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
```

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 Discovery Protocol

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、デフォルトでは有効になっています。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。

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)

- LLDPPDU TLV の最後

Cisco IP 電話は、該当する場合 LLDPPDU を送信します。LLDPPDU 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
- LLDPPDU 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 LLDPPDU 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 LLDPPDU 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 LLDPPDU 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 LLDPPDU 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 LLDPPDU 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 LLDPPDU 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 LLDPPDU の場合、TLV は無視され、検証されません。発信 LLDPPDU 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「01」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「11」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「0000」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、

手動の VLAN が有効であり、手動の 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 ポリシーに同じアプリケーションタイプが使用されていても、電話機が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 ポリシーを受信する場合、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。ネットワーク ポリシーの確実性と一貫性を確保するために、複数のネットワーク接続デバイスでは同じアプリケーションタイプに対して競合するネットワーク ポリシーを送信すべきではありません。

LLDP-MED と IEEE 802.X

Cisco IP 電話は IEEE 802.X をサポートせず、802.1X 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 802.1X またはスパンニング 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。