技術的な詳細

ネットワーク プロトコル

Cisco IP Conference Phone 8832 では、音声通信に必要な複数の業界標準およびシスコのネットワーク プロトコルがサポートされています。次の表に、電話機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 *1 : Cisco IP* 会議用電話サポートのネットワーク 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、電話機などのネットワーク デバイスを有効化し、IP アドレスなどの確かなスタートアップ情報を見つけます。	—
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。	電話機は CDP を使用して、ポートの電源管理ごとの Auxiliary VLAN ID などの情報と Cisco Catalyst スイッチの Quality of Service（QoS）設定情報を通信します。

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
Dynamic Host Configuration Protocol（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、デフォルトでは有効になっています。無効にした場合は、個々の電話機がある場所で、IP アドレス、サブネットマスク、ゲートウェイ、および TFTP サーバを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 150 を使用することを推奨します。この方式では、TFTP サーバの IP アドレスをオプション値として設定しています。サポートされている DHCP 設定を追加するには、お使いの Cisco Unified Communications Manager のリリースにあるドキュメンテーションを確認してください。 （注） オプション 150 を使用できない場合は、DHCP オプション 66 を使用します。
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。	電話機は、XML サービス、プロビジョニング、アップグレード、トラブルシューティングの目的で 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 の両方をサポートしている Web アプリケーションでは、2 つの URL が設定されています。HTTPS をサポートする電話機では、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。

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
IEEE 802.1X	IEEE 802.1X 標準規格では、クライアントサーバベースのアクセス制御と、認証されていないクライアントがパブリックにアクセスできるポートからLANに接続するのを規制する認証プロトコルを定義します。 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。	電話機は、認証方式EAP-FASTおよびEAP-TLS をサポートする IEEE 802.1X 標準規格を実装します。 電話機で 802.1X 認証が有効である場合は、ボイスVLANを無効にします。
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。 Dynamic Host Configuration Protocol（DHCP）を使用できる電話機を使用している場合、IPアドレス、サブネット、ゲートウェイ ID 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。 電話機は、IPv6アドレスをサポートしています。詳細については、該当するCisco Unified Communications Managerリリースのマニュアルを参照してください。
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。	電話機は PC ポートの LLDP をサポートしています。

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
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。	電話機は、SW ポートでLLDP-MED をサポートし、次のような情報を通信します。 • 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。 [illegible]
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。	電話機はRTPプロトコルを使用して、他の電話機およびゲートウェイとの間で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、デフォルトでは有効になっています。
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 Cisco Unified Communications Manager 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	使用方法に関する特記事項
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する機能です。
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。	電話機は、メディア暗号化のために SRTP を使用します。
Transmission Control Protocol（TCP）	TCP は、接続型の転送プロトコルです。	電話機は TCP を使用して Cisco Unified Communications Manager に接続し、XML サービスにアクセスします。
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ている場合、Cisco Unified Communications Manager でセキュアな登録をするときに、電話機は TLS プロトコルを使用します。詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。
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。 電話機で TFTP を使用すると、電話機のタイプ固有の設定ファイルを入手できます。	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。DHCP サーバが指定する以外の TFTP サーバを電話機で使用する場合は、電話機の [ネットワークのセットアップ（Network Setup）] メニューを使用して、TFTP サーバの IP アドレスを手動で割り当てる必要があります。 詳細については、該当する Cisco Unified Communications Manager リリースのマニュアルを参照してください。

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
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。

ネットワーク輻輳時の電話機の挙動

ネットワークパフォーマンスの低下の原因となるものは、電話の音声に影響を及ぼすため、場合によっては、通話が中断される可能性があります。 ネットワーク パフォーマンスの低下は、次のような原因が考えられます。

- 内部ポート スキャンやセキュリティ スキャンなどの管理タスク。
- サービス拒否攻撃など、ネットワーク上で発生した攻撃。

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トランス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

```
as1bsoft     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 （8 ページ）とSIP プロキシ フォールバック（9 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 トランスポートが**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、サーバ一覧のステータスを更新します。 利用不可能なサーバ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)**タグで**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。 T2-T1 > = 60の場合、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。

（注） MPP 電話機は、UDP 接続でのみデュアル登録をサポートします。

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。

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
```

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）
- 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 ポリシーの確定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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。