プライム ケーブル プロビジョニング テクノロジーの設定

この章では、特定のテクノロジーをサポートするプライム ケーブル プロビジョニングを設定するとき、実行する必要があるタスクを説明しています。

DOCSIS の設定

このセクションでは、DOCSIS テクノロジーをサポートするプライム ケーブル プロビジョニングを設定するとき、実行する必要があるタスクを説明しています。

（注） プライム ケーブル プロビジョニング リリースでサポートされている DOCSIS オプションの詳細については、テクノロジー オプション サポート を参照してください。

DOCSIS Workflow

プライム ケーブル プロビジョニングは、これらの DOCSIS 仕様のバージョンをサポートしています：1.0、1.1、2.0、3.0、3.1 および。

DOCSIS 操作のためプライム ケーブル プロビジョニングを適切に設定するには、このセクションで説明されている事項に加えて、プライム ケーブル プロビジョニング コンポーネントの設定 で説明されているようにコンポーネントを設定する必要があります。

次の表では、DOCSIS をサポートするプライム ケーブル プロビジョニングを設定するときに、準拠するワークフローを特定します。

表 *1 : DOCSIS* ワークフロー

	タスク	参照先
ステップ 1	RDU の設定	
	a. プロビジョニングされたすべての DHCP 条件を設定します。	DHCP 条件の設定
	b. プロビジョニングされたサービス クラスを設定します。	サービス クラスの設定
	c.操作の無差別モードを設定します。	システムのデフォルト
ステップ 2	DPE の設定	
	a. TFTP サービスを有効にします。	**service tftp** *1..1* **ipv4 | ipv6 enabled true** コマンドは Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド で説明されています。
	b. 必要に応じて ToD サービスを有効にします。	**service tod** *1..1* **ipv4 | ipv6 enabled true** コマンドは Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド で説明されています。
ステップ 3	Cisco プライム ネットワーク レジスタの設定	
	プロビジョニングされた DOCSIS モデム DHCP 条件に追加されたものと一致するクライアント クラス/選択タグを設定します。	Cisco プライム ネットワーク レジスタ エンドユーザー ガイド

DOCSIS 共有秘密鍵

プライム ケーブル プロビジョニングにより、各ケーブル モデム終端システム（CMTS）に異なる DOCSIS 共有秘密鍵（DSS）を定義します。この方法で、侵害された共有秘密鍵は展開のあらゆる CMTS の代わりに、CMTS の制限数のみに影響を与えます。

各 DPE の DSS を設定できますが、プロビジョニング グループ単位で設定する必要があります。また、そのプロビジョニング グループで CMTS に設定されているものと一致することを確認します。

注意 一部の状況でプロビジョニング グループ内の複数の DSS を設定することで、CMTS パフォーマンスの低下につながります。ただし、この要素はプライム ケーブル プロビジョニングにほとんど影響しません。

クリア テキスト文字列または IOS で暗号化された文字列として共有秘密鍵を入力できます。クリア テキストで入力すると、IOS バージョン 12.2BC に合わせて DSS が暗号化されます。

Admin UI または API を使用して、RDU から DSS も設定できます。この状況では、DSS が入力され、RDU に保存され、クリア テキストですべての DPEに送信されます。したがって、この方法で DSS を入力する前に DPE で保存され、暗号化されます。

CLI から **dpe docsis shared-secret** コマンドを使用して DPE で直接 DSS を設定する場合、この DSS は RDU からの手順を踏襲します。

DOCSIS 共有秘密鍵のリセット

DSS のセキュリティが侵害される場合 DSS をリセットするか、管理目的で共有秘密鍵を簡単に変更できます。

DSS をリセットするには、CMTS CLI から **show running-config** コマンドを実行し、DPE 設定に表示される設定から DOCSIS 共有秘密鍵をコピーして貼り付けます。この方法では、Cisco CMTS に入力した設定を DPE CLI にコピーすることができます。

（注） 説明のように共有秘密鍵を変更するには、CMTS はバージョン 12.2BC 以外のソフトウェア バージョンを実行する必要があります。

（注） 上記のコマンドの詳細と、これらのコマンドを実行する特定のセキュリティ権限については、Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド を参照してください。

DSS を変更するには。

ステップ 1 DOCSIS 共有秘密鍵をリセットする必要があるプロビジョニング グループを識別します。

ステップ 2 DPE およびプロビジョニング グループに関連付けられている CMTS のリストを調べます。

ステップ 3 CMTS でプライマリ DSS を変更します。

ステップ 4 CMTS で侵害された DSS をセカンダリ DSS に変更します。この変更は、新しい DSS を使用する DOCSIS 設定ファイルのすべてが正常に変更されるまで、ケーブル モデムが引き続き登録可能である必要があります。

ステップ 5 どの DPE が影響を受けたか判断し、それに従ってそれぞれで DSS を変更します。

ステップ 6 DOCSIS 設定ファイルが新しい DSS を使用していることを確認し、CMTS 設定から侵害されたセカンダリ共有秘密鍵を削除します。

拡張 CMTS MIC 共有秘密鍵

プライム ケーブル プロビジョニングにより、EMIC 計算の各ケーブル モデム終端システム（CMTS）に対して、異なる拡張 CMTS MIC（EMIC）共有秘密鍵を定義します。

CMTS では、事前 3.0 DOCSIS CMTS MIC 計算の共有秘密鍵とは異なる EMIC 計算の共有秘密鍵の設定をサポートする必要があります。このような設定がない場合は、CMTS は事前 3.0 DOCSIS CMTS MIC ダイジェスト計算として、拡張 CMTS MIC ダイジェスト計算に同じ共有秘密鍵を使用します。

この方法で、侵害された共有秘密鍵は展開のあらゆるCMTSの代わりに、CMTSの制限数のみに影響を与えます。

DSS と同様に、EMIC DOCSIS 共有秘密鍵を各 DPE に設定可能で、プロビジョニング グループ単位で設定する必要があります。また、そのプロビジョニング グループで CMTS に設定されているものと一致することを確認します。

注意 一部の状況でプロビジョニング グループ内の複数の EMIC DOCSIS 共有秘密鍵を設定することで、CMTS パフォーマンスの低下につながります。ただし、この要素はプライム ケーブル プロビジョニングにほとんど影響しません。

クリア テキスト文字列または IOS で暗号化された文字列として共有秘密鍵を入力できます。クリア テキストで入力すると、IOS バージョン 12.2BC に合わせて EMIC 共有秘密鍵が暗号化されます。

Admin UI または API を使用して、RDU から EMIC 共有秘密鍵も設定できます。この状況では、EMIC 共有秘密鍵が入力され、RDU に保存され、クリア テキストですべての DPEに送信されます。したがって、この方法で拡張 MIC 共有秘密鍵を入力する前に DPE で保存され、暗号化されます。

CLI から **dpe docsis emic shared-secret** コマンドを使用して DPE で直接 MIC 共有秘密鍵を設定する場合、この拡張 MIC 秘密鍵は RDU からの手順を踏襲します。

共有秘密鍵のリセット

EMIC 共有秘密鍵のセキュリティが侵害される場合 拡張 MIC 共有秘密鍵をリセットするか、管理目的で共有秘密鍵を簡単に変更できます。

DSS をリセットするには、CMTS CLI から **show running-config** コマンドを実行し、DPE 設定に表示される設定から EMIC 共有秘密鍵をコピーして貼り付けます。この方法では、Cisco CMTS に入力した設定を DPE CLI にコピーすることができます。

（注） 説明のように共有秘密鍵を変更するには、CMTS はバージョン 12.2(11)CX 以外のソフトウェア バージョンを実行する必要があります。

（注） 上記のコマンドの詳細と、これらのコマンドを実行する特定のセキュリティ権限については、Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド を参照してください。

拡張 MIC 共有秘密を変更するには。

ステップ 1 EMIC 共有秘密鍵をリセットする必要があるプロビジョニング グループを識別します。

ステップ 2 DPE およびプロビジョニング グループに関連付けられている CMTS のリストを調べます。

ステップ 3 CMTS でプライマリ EMIC 共有秘密を変更します。

ステップ 4 CMTS の侵害された EMIC 共有秘密鍵をセカンダリ EMIC 共有秘密に変更します。この変更は、新しい DSS を使用する DOCSIS 設定ファイルのすべてが正常に変更されるまで、ケーブル モデムが引き続き登録可能である必要があります。

ステップ 5 どの DPE が影響を受けたか判断し、それに従ってそれぞれで EMIC 共有秘密鍵を変更します。

ステップ 6 DOCSIS 設定ファイルが新しい EMIC 共有秘密鍵を使用していることを確認し、CMTS 設定から侵害されたセカンダリ共有秘密鍵を削除します。

PacketCable の設定

このセクションでは、プライム ケーブル プロビジョニングの設定を説明し、Packetcable テクノロジをサポートし、サービスに PacketCable 音声を導入します。

PacketCable 2.0 では、音声、ビデオ、データ、およびモビリティ テクノロジーのコンバージェンスをサポートしています。Session Initiation Protocol（SIP）および IP マルチ メディア システム（IM）に基づき、Non-Embedded User Equipment（UE）および Embedded User Equipment（E-UE）の管理をサポートしています。

プライム ケーブル プロビジョニング DOCSIS ケーブル モデムに埋め込まれ、E UE または組み込みデジタル音声アダプタ（E DVA）と呼ばれる UE のみをサポートしています。E DVA は RST （住宅 SIP テレフォニーをサポートします。

プライム ケーブル プロビジョニング PacketCable Basic およびセキュア モードの両方の IPv4 モードで E-DVA プロビジョニングをサポートし、PacketCable Basic モードでのみ IPv6 モードの E-DVA プロビジョニングをサポートします。

このセクションには、PacketCable のこれらのバリエーションに関する情報が含まれています。

- PacketCable 基本の設定 （8 ページ）
- PacketCable Secure の設定 （13 ページ）

PacketCable 音声テクノロジ導入の問題を解決するのに役立つ情報については、Troubleshooting PacketCable Provisioning を参照してください。

この章では、PacketCable マルチ メディア ターミナル アダプタ（MTA）デバイス プロビジョニング仕様、PKT-SP-PROV1.5-I03-070412 の内容に精通していることを前提としています。詳細については、PacketCable web サイトを参照してください。

PacketCable ワークフロー

プライム ケーブル プロビジョニングは、これらの PacketCable 仕様のバージョンをサポートしています：1.0、1.5 および 2.0。

プライム ケーブル プロビジョニングは、PacketCable 音声サービスの 2 つのバリアントをサポートしています。デフォルトのセキュア モードと非セキュアの基本的なモードです。PacketCable Basic は、非セキュア バリアントで検出されたセキュリティの脆弱性を除き、標準的な PacketCable と同じです。

このセクションでは、バリアントごとに実行する必要があるタスクを示します。

- PacketCable 基本 （6 ページ）
- PacketCable セキュリティ保護 （10 ページ）

（注） このセクションのワークフローでは、適切な PacketCable 設定ファイルと正しい MIB がロードされていることを前提としています。

PacketCable 基本

プライム ケーブル プロビジョニング コンポーネントの設定 で説明されている手順を完了した後にのみ、このセクションに記載されている PacketCable に関連するタスクを実行します。

次の表では、プライム ケーブル プロビジョニングで PacketCable Basic を設定するときに、準拠するワークフローを特定します。

（注） アスタリスク（*）が付いている質問には必ず回答してください。

表 *2 : PacketCable Basic* ワークフロー

	タスク	参照先
ステップ 1	DPE の設定	
	a. KDC サービス キー.* を設定します。	Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド で説明されている **service packetcable** *1..1* **registration kdc-service-key** コマンド。

	タスク	参照先
	b. PacketCable が有効にします。*。	Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド で説明されている **service packetcable** *1..1* **enable** コマンド。
ステップ 2	DHCP を設定します	
	a. MTA 範囲の動的 DNS を設定します。	Cisco プライム ネットワーク レジスタ エンドユーザー ガイド
	b. プロビジョニングされた PacketCable MTA DHCP 条件の追加と一致するクライアント クラス/範囲選択タグを設定します。*。	Cisco プライム ネットワーク レジスタ エンドユーザー ガイド
ステップ 3	DNS の設定	
	動的 DNS を各 DHCP サーバに設定します。	Cisco プライム ネットワーク レジスタ エンドユーザー ガイド
ステップ 4	サービス クラスを設定し、次のプロパティを含むようにします。	
	a. */pktcbl/prov/flow/mode* このプロパティは、MTA を使用する特定のフローをコマンドします。このプロパティをいずれかに設定します。 • BASIC.1—BASIC.1 フローを実行します。 • BASIC.2—BASIC.2 フローを実行します。 （注） デバイス プロパティ階層でこのプロパティをどこでも設定できます。	サービス クラスの設定

	タスク	参照先
	b. */cos/packetCableMTA/file* このプロパティには、MTA に表示される設定ファイルの名前が含まれています。設定ファイルは、プライム ケーブル プロビジョニングのファイルとして保存されます。 Basic MTA に対して提示される設定ファイルには、Basic 整合性ハッシュを含める必要があります。動的設定テンプレートを使用する場合、テンプレートの処理中に、ハッシュが透過的に挿入されます。Secure および Basic モードの両方でプロビジョニングするため、動的テンプレートを使用できます。 ただし、ファイルが Secure スタティック設定ファイルの場合は、Secure および Basic スタティック設定ファイルが相互運用可能ではないため、Basic スタティック設定ファイルにこのファイルを変換する必要があります。この変換を実行する方法の詳細については、PacketCable Basic フローのアクティブ化 を参照してください。	サービス クラスの設定

PacketCable 基本の設定

プライム ケーブル プロビジョニングは PacketCable Basic もサポートしており、シンプルかつ DOCSIS のような非セキュア プロビジョニング フローを提供します。次の表に、図 1 : 組み込み MTA セキュア電源オン プロビジョニング フロー （15 ページ） のプロビジョニング ワークフローを使用して、BASIC.1 フローを説明します。

表 *3 : PacketCable Basic eMTA* プロビジョニング

ステップ	ワークフロー	説明
MTA-1	DHCP ブロードキャスト検出	セキュア フローとして実行します。
MTA-2	DHCP Offer	プロビジョニング システムが BASIC.1 モードで MTA をプロビジョニングするように設定されている場合、特別な予約済みレルム名「」BASIC.1を含むプロビジョニング システムはオプション 122 サブオプション 6 を含む DHCP オファーを返します。この予約済みレルム名は、MTA に BASIC.1 プロビジョニング フローを使用するようにコマンドします。このオファーにはオプション 122.3 のプロビジョニング システム IP アドレスも含まれており、ファイルと siaddr フィールドには MTA の設定ファイル場所が入力されています。
MTA-3	DHCP REQUEST	MTA DHCP 交換のリマインダが実行されます（要求と交換された Ack）。
MTA-4	DHCP Ack	
MTA-22	テレフォニー設定ファイルの要求	MTA は手順 MTA-22 に直接スキップします。ファイルと siaddr 情報を使用して、MTA は TFTP 経由でプロビジョニング システムからその設定ファイルをコピーします。プライム ケーブル プロビジョニングが DPE コンポーネントに TFTP サーバを統合することに注意してください。 （注） MTA/プロビジョニング サーバまたは暗号化の認証は行われません。
MTA-23	テレフォニー設定ファイル	

BASIC.2 フローは、次の例外を除いて BASIC.1 と同じです。

- 「BASIC.2」が MTA の DHCP オプション 122 サブオプション 6 に入力されます。
- MTA はフローの一番最後の MTA-25 のプロビジョニング ステータス SNMP2c INFORM を発行します（DHCP オプション 122 サブオプション 3 はインフォーム ターゲットを指定します）。

PacketCable Basic フローは、DOCSIS フローと同様ですが次の違いがあります。

- MTA およびプロビジョニング システム間で ToD 交換はありません。
- MTA 設定ファイルには、整合性ハッシュが含まれています。具体的には、設定ファイルのコンテンツ全体の [SHA1] ハッシュは、pktcMtadevConfigFileHash SNMP VarBind に入力され、ファイル TLV の終了直前に TLV 11 内に配置します。
- BASIC.2 フローは、MTA が設定ファイルを受信し処理した後に、プロビジョニング ステータスを SNMPv2c 通知を発行します。MTA のプロビジョニングが正常に完了した場合に、このインフォームはプライム ケーブル プロビジョニングを通知します。問題がある場合、エラーが生成され、イベントが DPE から RDU に送信され、プライム ケーブル プロビジョニング クライアントに配置されます。このインフォームは、設定ファイル問題のデバッグ中に便利です。

DOCSIS フローに関する詳細については、DOCSIS の設定 （1 ページ） を参照してください。

（注） PacketCable Basic プロビジョニング フローを使用する前に、PacketCable Basic 対応 eMTA を使用していることを確認します。eMTA は、DHCP 検出オプション 60、TLV 5.18（サポートされるフロー）で Basic 対応であることを報告する必要があります。

PacketCable TLV 38 および MIB サポート

プライム ケーブル プロビジョニング は、PacketCable 1.5 MIB の完全なセットをサポートしています。

プライム ケーブル プロビジョニングは、PacketCable 設定テンプレートで TLV 38 をサポートしています。この TLV では、複数の SNMP 通知ターゲットを設定することができます。この TLV の設定は、すべての通知が TLV 38 で設定されているターゲットにも発行されたことを意味します。

SNMP 通知

プライム ケーブル プロビジョニングは、PacketCable MTA から SNMP v2C TRAP および INFORM 通知の両方をサポートしています。

PacketCable セキュリティ保護

プライム ケーブル プロビジョニングは、PacketCable Secure の 2 つのバリアントをサポートします。

- 北米仕様 PacketCable
- 欧州仕様 PacketCable

欧州仕様の PacketCable サービスは、北米 PacketCable 標準と同等のヨーロッパ仕様です。2 つの仕様の中で唯一の大きな違いは、欧州仕様の PacketCable では異なる MIB を使用していることです。詳細については、欧州仕様 PacketCable （32 ページ）を参照してください。

プライム ケーブル プロビジョニング コンポーネントの設定 で説明されているコンポーネントの設定を完了した後にのみ、このセクションに記載されている PacketCable に関連するタスクを実行します。

（注） PacketCable に準拠した操作については、MTA、KDC、および DPE 間の最大許容クロック スキューは 300 秒（5 分）です。この値は、デフォルト設定です。

次の表では、PacketCable Secure をサポートするプライム ケーブル プロビジョニングを設定するときに、準拠するワークフローを特定します。

（注） アスタリスク（*）が付いている質問には必ず回答してください。

表 *4 : PacketCable Secure* ワークフロー

	タスク	参照先
ステップ 1	RDU の設定	
	a. マルチメディア ターミナル アダプタ（MTA）FQDN の自動生成を有効にします。	自動 FQDN 生成
	b. すべてのプロビジョニングされた DHCP 条件を設定します。	DHCP 条件の設定
	c. すべてプロビジョニングされたサービス クラスを設定します。	サービス クラスの設定
	d. SNMPv3 クローニング キーを設定します。*。	PacketCable MTA との通信のためのセキュリティ保護用 RDU および DPE のSNMPv3 クローニング設定 （31 ページ）

	タスク	参照先
	e. 欧州仕様 PacketCable を使用している場合は、欧州仕様 PacketCable MIB を使用する RDU を設定します。	欧州仕様 PacketCable （32 ページ）
ステップ 2	DPE の設定	
	a. KDC サービス キーを設定します。*。	Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド で説明されている **service packetcable** *1..1* **registration kdc-service-key** コマンド。
	b. プライバシー ポリシーを設定します。*。	Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド で説明されている **service packetcable** *1..1* **registration policy-privacy** コマンド。
	c. SNMPv3 クローニング キーを設定します。*。	Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド で説明されている **service packetcable** *1..1* **snmp key-material** コマンド。
	d. PacketCable を有効にします。*。	Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド で説明されている **service packetcable** *1..1* **enable** コマンド。
	e. 必要に応じて MTA ファイル暗号化を設定します。	Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド で説明されている **service packetcable** *1..1* **registration encryption enable** コマンド。
ステップ 3	KDC を設定します	
	a. Cisco 担当者からライセンス ファイルを取得します。	KDC 証明書

	タスク	参照先
	b. PKCert.sh ツールを使用して証明書チェーンを設定します。欧州仕様 PacketCable については、**-e** オプションを使用します。	PKCert.sh の使用
	c. 各 DPE のプロビジョニング FQDN のサービス キー ペアを設定します。	KeyGen ツールの使用
	d. ticket-granting-ticket（TGT）のサービスのキーを設定します。	KeyGen ツールの使用
	e. NTP 同期を設定します。	NTP の設定に関する Linux のマニュアル
ステップ 4	DHCP を設定します	
	a. すべての必要な PacketCable プロパティを設定します。	changeNRProperties.sh の使用
	b. MTA 範囲の動的 DNS を設定します。	http://www.cisco.com/en/us/products/ps11808/products_user_guide_list.html
	c. プロビジョニングされた PacketCable MTA DHCP 条件の追加と一致するクライアント クラス/範囲選択タグを設定します。*****。	http://www.cisco.com/en/us/products/ps11808/products_user_guide_list.html
ステップ 5	DNS の設定	
	a. 各 DHCP サーバの動的 DNS を設定します。	http://www.cisco.com/en/us/products/ps11808/products_user_guide_list.html
	b. KDC レルムのゾーンを設定します。	http://www.cisco.com/en/us/products/ps11808/products_user_guide_list.html

PacketCable Secure の設定

このセクションでは、セキュリティ保護された PacketCable 音声プロビジョニングについて特に詳細に説明しています。PacketCable Secure はテレフォニ サービスの盗難、サービスの悪意のある中断などの可能性を最小限にするように設計されています。PacketCable Secure は Kerberos

インフラストラクチャに依存して、MTA およびプロビジョニング システムを相互に認証します。プライム ケーブル プロビジョニングでは、キー発行局 (KDC) は Kerberos サーバとして機能します。SNMPv3 は MTA およびプロビジョニング システム間の通信をセキュリティ保護するために使用されます。

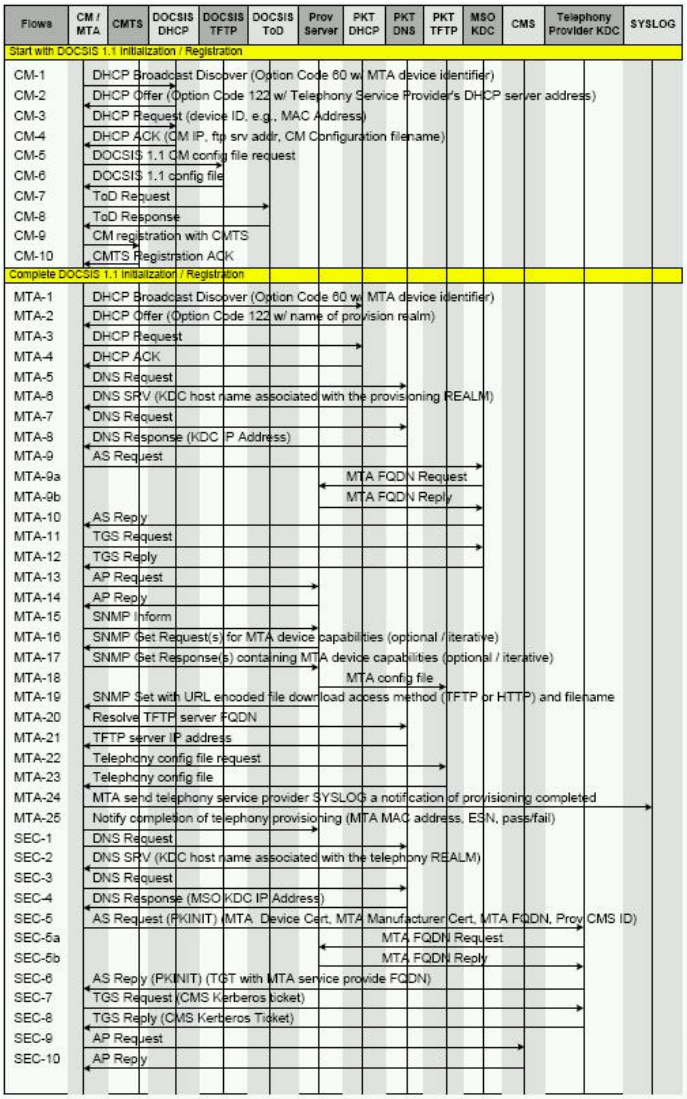
（注） IPv6 のデバイスでは、PacketCable セキュリティ保護されたプロビジョニングはサポートされていません。

プライム ケーブル プロビジョニング *PacketCable* セキュリティ保護プロビジョニング フロー

すべての PacketCable プロビジョニング フローは、一連の手順として定義されます。

次の図は、PacketCable eMTA のセキュア プロビジョニング フローを説明しています。

図 ***1*** *:* 組み込み ***MTA*** セキュア電源オン プロビジョニング フロー



（注） 障害が発生している手順を正確に理解するため、データ パケットをキャプチャする機能を持つ、プロトコル アナライザ（プロトコル スニファ）を使用することを強く推奨します。

さらに、KDC ログファイルの内容は、KDC の障害の根本的な原因を理解する上で重要です。

組み込みマルチメディア終端アダプタ（eMTA）のプロビジョニングで問題を診断するとき、次の表のフロー説明が PacketCable プロビジョニング フローのどの手順に障害が発生しているか特定するのに役立ちます。

表 ***5 : PacketCable Secure eMTA*** プロビジョニング

ステップ	ワークフロー	説明
CM-1	DHCP ブロードキャスト検出	これは、DHCP オプションが追加されている DHCPv4 または DHCPv6 の DOCISI ケーブルモデム（CM）起動フローと同様で、DHCP のオファーを承認可能な MTA から PacketCable DHCP サーバのリストとともにMTAを提供します。
CM-2	DHCP Offer	
CM-3	DHCP REQUEST	
CM-4	DHCP Ack	
CM-5	DOCSIS 1.1 CM 設定ファイル要求	
CM-6	DOCSIS 1.1 設定ファイル	
CM-7	ToD 要求	
CM-8	ToD 応答	
CM-9	CMTS（ケーブル モデム終端システム）による CM 登録	
CM-10	CMTS 登録 Ack	

ステップ	ワークフロー	説明
MTA-1	DHCP ブロードキャスト検出	
MTA-2	DHCP Offer	
MTA-3	DHCP REQUEST	
MTA-4	DHCP Ack	

ステップ	ワークフロー	説明
		DHCP を使用して、MTA は PacketCable MTA として公開し、サポートする機能とプロビジョニング フローで情報を提供します（Secure、Basic など）。また、MTA はアドレッシング情報と DHCP オプション 122 を取得します。DHCP オプション 122 には、PacketCable プロビジョニング サーバ アドレスおよびセキュリティ レルム名が含まれています。この情報は、MTA が KDC とプロビジョニング サーバに接続できるようにするため使用されます。 いくつかの重要なトラブルシューティングのヒントは次のとおりです。 • 適切な設定について CMTS の DHCP リレー エージェントをチェックします。CMTS が適切な DHCP サーバをポイントしていることを確認します。 • MTA、CMTS、DHCP サーバ、DPE 間で正しいルーティングが行われていることを確認します。 • CMTS でセカンダリのサブネットが正しく設定されていることを確認します。 • Prime Network RegistrarDHCP 設定を確認します。範囲が設定され、IP アドレスが使用可能であり、すべてのセカンダリ サブネットが設定されていることを確認し

ステップ	ワークフロー	説明
		ます。 • プライム ケーブル プロビジョニング設定を確認します。*Cnr_ep.properties* ファイルを確認し、必要な PacketCable Network Registrar 拡張プロパティが設定されていることを確認します。詳細については、PacketCable DHCP オプションをプライム ケーブル プロビジョニング プロパティにマッピングするを参照してください。 パケット トレースにより MTA-1 および MTA-2 間でサイクルされていることが明らかになった場合、DHCP オプション 122（レルム名またはプロビジョニング サーバ FDQN サブオプション）、DHCP オプション 12（ホスト名）、または DHCP オプション 15（ドメイン名）に問題がある可能性があります。

ステップ	ワークフロー	説明
MTA-5	DNS 要求	MTA はセキュリティ レルム名（DHCP オプション 122 内で配信）を使用し、KDC サービス DNS SRV 検索を実行し、KDC IP アドレスを解決します。 いくつかの重要なトラブルシューティングのヒントは次のとおりです。 • Network Registrar DNS に送信された誤った宛先または不正な形式の DNS パケットを視聴するには、パケット スニファを使用します。 • Network Registrar DNS ログ レベルを詳細なパケット トレーシングに設定し、到着内容を確認します。 • DNS 設定のチェック：*cnr_ep.properties* で指定された DNS サーバには、KDC のレルム ゾーン、SRV レコード、DNS「A」レコードを含める必要があります。
MTA-6	DNS SRV	
MTA-7	DNS リクエスト	
MTA-8	DNS レスポンス（DNS Response）	

ステップ	ワークフロー	説明
MTA-9	AS 要求	AS-REQ 要求メッセージは、KDC で MTA の認証に使用されます。 いくつかの重要なトラブルシューティングのヒントは次のとおりです。 • AS-REQが到着しており、エラーまたは警告が存在するかKDC ログファイルを確認します。 • KDC が正しい MTA_Root 証明書に設定されていることを確認します。AS^REQ メッセージ内で MTA から送信された製造元とデバイスの証明書を、KDC にインストールされている MTA_Root 証明書をチェーンにする必要があります。

ステップ	ワークフロー	説明
MTA-9a	MTA FQDN 要求	KDC は MTA 証明書から MTA MAC アドレスを抽出し、検証のためプロビジョニング サーバに送信します。プロビジョニング サーバがその MAC アドレスの FQDN を有する場合、KDC に返されます。KDC は MTA からの FQDN を、FQDN REP 応答メッセージで受信した FQDN-REP 返信メッセージと比較します。 いくつかの重要なトラブルシューティングのヒントは次のとおりです。 • 誤った宛先または不正な形式の DNS パケットを視聴するには、パケット スニファを使用します。MTA は AS-REP メッセージ内のプロビジョニング サーバ FQDN（DHCP オプション 122 で受信した MTA）を KDC に送信します。KDC はこの FQDN を使用して、プロビジョニング サーバの IP アドレスを解決します。 • KDC キー ファイルのファイル名と内容を確認します。DPE の KDC サービス キーは、KDC のサービス キーと一致する必要があります。KDC のサービス キー ファイル名は重要です。
MTA 9b	MTA FQDN 応答	

ステップ	ワークフロー	説明
MTA-10	AS 応答（AS REP）	KDC は MTA にプロビジョニング サービス チケットを付与し、MTA にサービス プロバイダ、ローカル システム プロバイダ（オプション）、KDC 証明書を送信します。MTA は、証明書が KDC チェーンにより MTA に保存されているサービス プロバイダのルート証明書に送信されているか確認します。これらの証明書チェーン設定されていない場合、MTA はプロビジョニングのフローの手順 MTA-1 にループ バックします。*KDC.cer* ファイルの詳細については、PKCert.sh の使用 を参照してください。 重要なトラブルシューティングのヒント：KDC ログ ファイルにより、AS-REP メッセージがデバイスに送信されたことを示しているか確認します。パケット トレースにより手順 MTA-1 と MTA-10 間で MTA がサイクルしていることが明らかになった場合、サービス プロバイダ証明書チェーンに問題があります。
MTA-11	TGS 要求	手順 MTA-10 に従い、MTA がサービス チケットまたは ticket-granting-ticket（TGT）のいずれかを受信します。MTA が手順 MTA-10 のサービス チケットではなく TGT を取得した場合、ticket-granting-server（KDC）に接続してサービス チケットを取得します。
MTA-12	TGS 応答	KDC は MTA に TGS 返信のサービス チケットを送信します。

ステップ	ワークフロー	説明
MTA-13	AS 要求（AP-REQ）	MTA は、DHCP オプション 122 で指定されたプロビジョニング サーバにチケット（手順 MTA-10 で受信）を提示します。
MTA-14	AP 返信（AP-REP）	プロビジョニング サーバは KDC 共有秘密鍵を使用して AP-REQ を復号化して、MTA によって提示されたプロビジョニング サーバ チケットを検証し、SNMPv3 キーを使用して AP-REP を送信します。SNMPv3 はここで認証され、（オプション）暗号化されます。
MTA-15	snmp 情報	プロビジョニング情報を受信可能なプロビジョニング サーバに MTA 信号を送信します。
MTA-16	SNMP Get 要求	SNMPv3：プロビジョニング サーバ（DPE）が追加のデバイス機能を要求する場合、MTA 機能で必要な情報を取得するため、MTA は 1 個以上の SNMPv3 GEt 要求を送信します。プロビジョニング サーバ（DPE）は GetBulk 要求を使用して、単一メッセージの一括情報を要求できます。
MTA-17	SNMP Get 応答	SNMPv3：MTA はプロビジョニング サーバ（DPE）に、手順 MTA-16 で要求された MTA 機能の情報を含む各 GetRequest の応答を送信します。
MTA-18	MTA 設定ファイル	手順 MTA-16 および MTA-17 で使用可能な情報により、プロビジョニング サーバ（DPE）は MTA 設定データ ファイルの内容を決定します。

ステップ	ワークフロー	説明
MTA-19	SNMP Set	SNMPv3：プロビジョニング サーバは、MTA 設定ファイル、ファイルの暗号化キー、ファイル ハッシュ値を含む MTA に、SNMPv3 を実行します。
MTA-20	TFTP サーバ FQDN の解決	DNS 要求：IPv4 アドレスの代わりに URL エンコードアクセス方法が FQDN を含む場合、MTA はサービス プロバイダ ネットワークの DNS サーバを使用して、FQDN を TFTP サーバまたは HTTP サーバの IPv4 アドレスに解決します。
MTA-21	TFTP Server IP Address	DNS 応答：手順 MTA-20 の手順で要求されたように、DNS サーバはサービス プロバイダ ネットワークの IPv4 IP アドレスを返します。
MTA-22	テレフォニー設定ファイルの要求	MTA は指定された TFTP サーバから VoIP 設定ファイルのダウンロードを続行します。プライム ケーブル プロビジョニングが DPE コンポーネントに TFTP サーバを統合することに注意してください。
MTA-23	テレフォニー設定ファイル	
MTA-24	MTA の送信	MTA オプションで syslog 通知を、プロビジョニングが完了したサービス プロバイダに送信します。
MTA-25	テレフォニー プロビジョニングの完了通知	新しい設定が許容可能な場合、プロビジョニング サーバへ MTA 信号を送信します。
SEC-1 ～ SEC-10	次の手順は post-MTA プロビジョニング セキュリティ フローであり、プライム ケーブル プロビジョニングのプロビジョニングには適用されません。このフローには、MTA が通信する各 CMS に関連付けられた、Kerberos チケットの取得が含まれます。詳細については、PacketCable セキュリティ仕様を参照してください。	

プライム ネットワーク レジスタ *DNS* サーバの *SRV* レコードの設定

KDC で動作するように、Prime Network Registrar の DNS サーバを設定する必要があります。この設定を行うには、Prime Network Registrar のマニュアルと次の手順を参照してください。

（注） 適切なレルム名と一致するゾーン名を作成して、この特別ゾーンの DNS レコードのみ（DNS サーバにより必要とされるレコード以外）をレルムの SRV レコードにすることをお勧めします。この例では、目的の Kerberos レルムが voice.example.com であり、その他すべての KDC、Network Registrar、および DPE 設定が実行されていると仮定します。KDC の FQDN は、kdc.example.com と見なされます。

ステップ 1 **nrcmd** コマンド ライン ツールを開始します（デフォルトで */opt/nwreg2/local/usrbin* ディレクトリに存在しています）。

ステップ 2 ユーザ名とパスワードを入力します。

ステップ 3 Kerberos レルムのゾーンを作成するには、次のコマンドを入力します。

```
nrcmd> zone voice.example.com create primary address_of_nameserver hostmaster
```

name-server がネーム サーバの IP アドレスを指定します。

ステップ 4 新しいゾーンに SRV レコードを追加するには、次を入力してください。

```
nrcmd> zone voice.example.com. addRR _kerberos._udp. srv 0 0 88 KDC_FQDN
```

KDC_FQDN が KDC の FQDN を指定します。

ステップ 5 DNS サーバを保存しリロードするには、次のコマンドを入力します。

```
nrcmd> save
nrcmd> dns reload
```

DHCPv6 サーバ選択の設定

プライム ケーブル プロビジョニング PacketCable 2.0 デバイスのプロビジョニングのため、RFC 3925 で指定されたオプション 125 のサブオプション 123 と、RDC 3315 で指定されたオプション 17 のサブオプション 2171 をサポートします。DHCPv6 でサーバ ID を提供するため、プライム ケーブル プロビジョニング は CableLabs 固有の DHCP サーバの選択 ID を使用します。DHCPv4 オプション CL_V4OPTION_CCCV6（123）または DHCPv6 オプション CL_OPTION_CCCV6（2171）内で、eCM はサブオプション 1 および 2 を経由してプライマリおよびセカンダリ DHCP サーバ選択 ID とともに提供されます。

DHCP サーバ選択 ID の設定値では、デバイスがプロビジョニング可能か定義します。パケット ケーブルが無効の場合、デフォルトでこの値は ff:ff:ff:ff に設定されます。CPNR-EP コンポーネントまたは changeNRProperties.sh の使用 のインストール時に、この値を設定できます。

たとえば、eCM CL_V4OPTION_CCCV6 または CL_OPTION_CCCV6 のサブ オプション 1 の値 ff:ff:ff:ffを取得した場合、ためを有効な DHCPv6 アドバタイズのサーバの DHCP サーバの選択識別子に関係なく、すべてのサーバからを受け入れるには無料であります。同様に、00:00:00:00 の値は eUE をプロビジョニングしないことを示します。

オプション 17.2171 および 125.123 の詳細については、オプション 17.2171 または 125.123 と プライム ケーブル プロビジョニングプロパティの比較 を参照してください。

DSS_ID および IP 優先順位の DHCP オプションは、プロビジョニング グループ **IPv6 - PacketCable 2.0** が有効になっている場合にのみ、応答に追加されます。（ProvGroupCapabilitiesKeys. PACKET_CABLE_V6).

PG 機能 **IPv6 - PacketCable 2.0** が無効になっているときに DHCP 手順を生成する場合、下のオプションは無視されます。

- CL_V4OPTION_CCCV6 (123)
- CL_V4OPTION_IP_PREF (124)
- CL_OPTION_CCCV6 (2171)
- CL_OPTION_IP_PREF(39)

（注） 上記のオプションは、 **IPv6 - PacketCable 2.0** 機能が有効になっているときに DHCP 手順に追加できます。ただし、これらのオプションの含有/無視は、次のプロパティで制御されます。

1. **/pktcbl/ipPreference**
2. **/pktcbl/dssid/processing/enable**

プロパティ **/pktcbl/dssid/processing/enable** (PacketCableDefaultKeys。PKTCBL_OPTION_DSS_ID_PROCESSING_ENABLE）は、DHCP 手順を生成中に DSS_ID オプションの含有を制御できます。このブール値プロパティが無効になっている場合、DHCP 手順の生成中に下のオプションは無視（またはフィルタ）されます。

- CL_V4OPTION_CCCV6 (123)
- CL_OPTION_CCCV6(2171)

Admin UI で DSS_ID 処理オプションは、プロパティ **/pktcbl/dssid/processing/enable** を使用して RDU でデバイス、サービス クラス、DOCSIS デフォルト、PacketCable デフォルト、DHCP 条件レベルで設定できます。デフォルトでは、DSS_ID 処理オプションは無効になります。

IP 設定オプションの設定

プライムケーブルプロビジョニングは、DHCP IP 設定オプション CL_V4OPTION_IP_PREF（125.124）および CL_OPTION_IP_PREF（17.39）をサポートします。ネットワークでプロビジョニングされるときに、IP 設定オプションが DOCSIS モデム（eCM:EDVA）によって必要です。これらのオプションは、ほとんどの操作に対して、単一のスタック モードまたはデュアル

モードで eUE を操作する必要があるか示します（たとえば、メディア、SIP シグナリング）。RDU は、単一のスタックまたはデュアル スタック機能に基づいて、PacketCable デバイスに IP 設定値を割り当てます。これらの DHCP IP 設定オプションでは、IPv4 または IPv6 アドレスが eUE プロビジョニングに使用される場合示します。

Admin UI で、プロパティ*/pcktcbl/ipPreference*を使用して RDU の IP 設定を、デバイス、サービス クラス、DOCSIS デフォルト、DHCP 条件レベルに設定できます。これは、デバイス、プロビジョニング グループ、サービス クラス、DHCP 条件、テクノロジー デフォルトなど、プロパティ階層の承認可能な時点で、RDU API から設定できます。デフォルトでは、RDU の IP 設定値は 0 に設定されます。

次の表では、RDU および対応するプロビジョニング フローで設定可能な IP 設定値をすべて説明します。

表 *6:* 設定可能な *RDU* の *IP* 設定値

IP 設定値	Description
0	null として解釈されますeUE はデフォルト プロビジョニング フロー IP モードに基づきプロビジョニングされます（IPv4 または IPv6）。
1	eUE は IPv4アドレスのみを取得し、IPv4 アドレスはプロビジョニング フローを含む操作すべてに使用されます。
2	eUE は IPv6アドレスのみを取得し、IPv6 アドレスはプロビジョニング フローを含む操作すべてに使用されます。
5	eUE は操作のために IPv4 および IPv6 アドレス両方を取得しますが、IPv4 アドレスのみがプロビジョニング フローに使用されます。
6	eUE は操作のために IPv4 および IPv6 アドレス両方を取得しますが、IPv6 アドレスのみがプロビジョニング フローに使用されます。

次の表では、デバイスから送信される IP 設定値すべてと、対応する値の RDU の解釈を説明します。

表 *7:* デバイスからの *IP* 設定値

IP 設定値	Description
null	デバイスがデュアル スタックではないことを示します。
7(b' 111)	デバイスがデュアル スタック モードでプロビジョニング可能であることを示します。

デバイスがデュアル スタック モードをサポートしておらず、RDU の IP 設定値がデュアル スタック モード値（5 または 6）である場合、応答 DHCP パケットの IP 設定値はデバイス機能に調整されます。

たとえば、デバイスが IP 設定の値を送信せず、RDU の IP 設定値が 5 または 6 である場合、DHCP ack で送信された IP 設定値と返信パケットは、対応する単一スタック モード値に個別に設定されます（例：1 または 2）。

IP設定はRDUで設定されておらず、デバイスがIP設定値を送信していない場合、RDUはeUEのIP設定DHCPオプションの生成を無視します。

次の表は、RDUで設定されたデバイスおよび値から送信されるIP設定値に基づき、DHCP ackまたは返信パケットで送信されたIP設定値を説明します。

表 *8 : IP* 設定決定マトリクス

Packetcable DQOS 有効				PacketCable デュアル スタック無効			
IP 設定のデバイス信号	RDU プロパティ値	Decision		IP 設定のデバイス信号	RDU プロパティ値	Decision	
		eCM の DHCP 検出 IPv4 フロー	eCM の DHCP 検出 IPv6 フロー			eCM の DHCP 検出 IPv4 フロー	eCM の DHCP 検出 IPv6 フロー
null	0	IPv4 および IPv6 モードそれぞれのオプション 125.124 および 17.39 の DHCP 指示生成を無視します。		null	0	IPv4 および IPv6 モードそれぞれのオプション 125.124 および 17.39 の DHCP 指示生成を無視します。	
null	1	1		null	1	1	
null	2	2		null	2	2	
null	5	5		null	5	1	
null	6	6		null	6	2	
7	1	1	1	7	1	1	1
7	2	2	2	7	2	2	2
7	5	5	5	7	5	1	1
7	6	6	6	7	6	2	2
7	[0]	5	6	7	0	1	2

PacketCable 2.0 Groovy ダイヤル プランの追加

ダイヤル プランはUEでプロビジョニングされ、ダイヤルした番号の解釈方法についてUEに通知します。ダイヤルプランは、正規表現に一致する場合にUEによって実行されるアクションを示す、一部の特別トークンと組み合わせた正規表現の番号付きのセットです。

ダイヤルプランは、一連のルールに編成されます。UEは順番にダイヤルプランのルールを適用する必要があり、タイマーを含むパターンに一致する場合に、UEは指定されたアクションまたはアクション実行する必要があります。

ダイヤルプランを作成するには、EFC 4234で定義されたAugmented Backus-Naur Form（ABNF）の表記と内容を熟知する必要があります。次0はを参照用として使用できるサンプル ダイヤルプランです。

（注） デバイス機能を決定する際に問題が発生した場合、プライム ケーブル プロビジョニングは [Secure（セキュア）] モードにデフォルトになります。ダイヤル プランを追加するときに、groovy スクリプトまたはバイナリ ファイルのいずれかを使用できますが、テンプレートは使用しません。

ダイヤル プランを作成するサンプルの groovy ファイル

```
def dialPlan = '''
            TIMER S=4.000000
            TIMER Z=2.000000

            domain = "@ims.packetcable.com"
            dialString = ";user=dialstring"
            dialPhone = ";user=phone"

            homeEmergencyNumber = "911"
            localEmergencyNumber = "911"

            MAP MainTable =
            "0S" : MAKE-CALL
            "0#" : MAKE-CALL
            "00" : MAKE-CALL
            "(=Emergency)" : EMERGENCY-CALL("sip:" "911" =domain =dialPhone)
            "(=N11)" : MAKE-CALL("sip:" #1v =domain =dialString)
            "(=SpeedDial)" : MAKE-CALL("sip:" #1v =domain =dialString)
            "(=PhoneNumber)" : MAKE-CALL("sip:" #1v =domain =dialPhone)
            "(=ImmediateVSCs)" : RETURN
            "(=DelayedVSCs)" : RETURN
            "(x{1-20})S" : MAKE-CALL("sip:" #1 =domain =dialPhone)
            "(x{1-20})#" : MAKE-CALL("sip:" #1 =domain =dialPhone)
'''
* PKTC-IETF-MTA-MIB pktcMtaDevEnabled (1.3.6.1.2.1.140.1.1.6.0)
*/
configFile.add(TLV_SNMP("1.3.6.1.2.1.140.1.1.6.0", "Integer", "1"))
/*
* Device Level Configuration (Secure flow only):
* Include required Secure-flow realm TLVs
*/
if (isSecureProvFlowMode)
{
   // PKTC-IETF-MTA-MIB pktcMtaDevRealmName.1 (1.3.6.1.2.1.140.1.3.6.1.2.1)
   configFile.add(
       TLV_SNMP("1.3.6.1.2.1.140.1.3.6.1.2.1", "STRING", realmName))
   // PKTC-IETF-MTA-MIB pktcMtaDevRealmOrgName.1 (1.3.6.1.2.1.140.1.3.6.1.5.1)
       configFile.add(
       TLV_SNMP("1.3.6.1.2.1.140.1.3.6.1.5.1", "STRING", realmOrgName))
}

configFile.add(option.createOptionValue(OptionSyntax.SNMP,"64",[".pktcEUERSTDMValue.1","STRING",dialPlan]));
```

（注） サンプル PacketCable 2.0 groovy スクリプト（example_edva.groovy）は、PacketCable Secure モード SNMP TLVs の数字 OID を使用します（pktcMtaDevRealmName、pktcMtaDevRealmOrgName）。

オプション 64 の TLV 長が 4500 を超える場合、/opt/CSCObac/api/conf/api.properties and in /opt/CSCObac/rdu/conf/rdu.properties のプロパティ/default/asnParser/bufferLength=20000 に更新する必要があります。

PacketCable MTA との通信のための セキュリティ保護用 RDU および DPE のSNMPv3 クローニング設定

プライム ケーブル プロビジョニングにより、MTA デバイスへの SNMPv3 アクセスに対して、外部ネットワーク マネージャを有効にすることができます。さらに、RDU は特定の MTA で SNMPv3 操作を実行できます。

この機能を有効にするには、DPE および RDU セキュリティ キー素材を設定します。キー素材を設定すると、複製された SNMPv3 エントリを作成するために使用されるプライム ケーブル プロビジョニング アプリケーション プログラミング インターフェイス（API）コールが有効になります。

（注） この機能を有効にすると、プロビジョニングのパフォーマンスに影響します。

キー素材の作成とキーの生成

キー素材の作成には 2 段階あります。

1. RDU でスクリプト コマンドを実行します。
2. DPE で CLI コマンドを実行します。

（注） この共有秘密鍵は、CMTS またはプライム ケーブル プロビジョニングと同じ共有秘密鍵ではありません。

キー素材を作成するには。

ステップ 1 *BPR_HOME/rdu/bin* ディレクトリから、RDU でこのスクリプトを実行します。

```
# generateSharedSecret.sh password
```

password は、6 ～ 20 文字で作成した任意のパスワードです。このパスワードは、46 バイト キーを生成するために使用されます。このキーは *keymaterial.txt* と呼ばれるファイルに保存され、*BPR_HOME/rdu/conf* ディレクトリに存在します。

ステップ 2 **service packetcable** *1..1* **snmp key-material** DPE CLI コマンドを手順 1 で使用された *password* で実行し、この音声テクノロジーが有効になっているすべての DPE でキーを生成します。 このコマンドは、DPE で同じ 46 バイト キーを生成し、RDU および DPE が同期され、MTA と安全に通信できることを保証します。コマンドの詳細と、これらのコマンドを実行する特定のセキュリティ権限については、Cisco プライム ケーブル プロビジョニング 6.1.2 リファレンス ガイド を参照してください。

欧州仕様 PacketCable

欧州 PacketCable サービスは、基本的に北米 PacketCable サービスと同等のヨーロッパ仕様であり、次の違いがあります。

- 欧州 PacketCable は、さまざまな MIB を使用します。
- 欧州 PacketCable は、異なるデバイス証明書（*MTA_Root.cer*）とサービス プロバイダ証明書（サービス プロバイダ ルート）の異なる設定を使用します。

  欧州 PacketCable 証明書については、 *kdc.ini* ファイルの *euro-packetcable* プロパティを true に設定する必要があります。KDC は欧州 PacketCable（tComLabs）証明書チェーンをサポートしています。サンプルの欧州 PacketCable 対応 KDC 設定ファイルを次に示します。

```
[general]
interface address = 10.10.10.1
FQDN = servername.cisco.com
maximum log file size = 10000
n saved log files = 100
log debug level = 5 minimum
ps backoff = 150 maximum
ps backoff = 300
euro-packetcable = true
```

  欧州 PacketCable を使用する場合、PacketCable プロパティ */pktcbl/prov/locale* の値が EURO に設定されていることを確認します。デフォルトでは、NA（北米）です。設定ファイル ユーティリティのロケールを指定できます。詳細については、テンプレートの設定ファイル ユーティリティの使用を参照してください。

欧州 PacketCable MIB

欧州 PacketCable MIB は、本質的な draft-IETF MIB のスナップショットです。MTA 設定ファイルは、MIB を参照する SNMP VarBinds で構成されています。北米 PacketCable と欧州 PacketCable MIB には重要な違いがあります。したがって、北米 PacketCable および欧州 PacketCable 設定ファイルには互換性がありません。インストール中に、北米 PacketCable（*cw29_config.tmpl*）および欧州 PacketCable（*ecw15_mta_config.tmpl*）のサンプル ファイルが *BPR_HOME/rdu/*サンプル ディレクトリにコピーされます。

次の欧州 PacketCable MIB がプライム ケーブル プロビジョニングに同梱しています。

- DOCS-IETF-BPI2
- INTEGRATED-SERVICES-MIB

- DIFFSERV-DSCP-TC
- DIFFSERV-MIB
- TCOMLABS-MIB
- PKTC TCOMLABS MTA MIB
- PKTC-TCOMLABS-SIG-MIB

欧州 PacketCable MIB の設定

欧州 PacketCable MIB を使用するプライム ケーブル プロビジョニングを設定するには、ロードする MIB を指定するプライム ケーブル プロビジョニング RDU プロパティを変更する必要があります。デフォルトでは、このプロパティには PacketCable MIB を含みます。

次のいずれかの方法でプロパティを変更できます。

- *Rdu.properties* を変更し、RDU を再起動します。
- Admin UI で **[Configuration（設定）] > [Defaults（デフォルト）] > [System Defaults（システム デフォルト）]** に移動し、次に示されるリストに MIB を置換します。RDU を再起動する必要はありません。
- Prov API *changeSystemDefaults()* コールを使用します。RDU を再起動する必要はありません。

プロパティ名は */snmp/mibs/mibList*（プロパティ ファイル）または SNMPPropertyKeys.MIB_LIST（prov API 定数名）です。プロパティ値は、次に示すように必要な MIB 名で構成されるカンマ区切り値（CSV）です。

/snmp/mibs/mibList=SNMPv2-SMI,SNMPv2-TC,INET-ADDRESS-MIB,CISCO-SMI,CISCO-TC,SNMPv2-MIB、RFC1213 MIB、IANAifType-MIB,IF-MIB,DOCS-IF-MIB,DOCS-IF-EXT-MIB,DOCS-BPI-MIB,CISCO-CABLE-SPECTRUM-MIB,CISCO-DOCS-EXT-MIB,SNMP-FRAMEWORK-MIB、ドキュメント -CABLE-DEVICE-MIB,DOCS-QOS-MIB,CISCO-CABLE-MODEM-MIB,DOCS-IETF-BPI2-MIB,INTEGRATED-SERVICES-MIB,DIFFSERV-DSCP-TC,DIFFSERV - MIB、TCOMLABS MIB、PKTC-TCOMLABS-MTA-MIB,PKTC TCOMLABS-SIG-MIB

DPoE の設定

Ethernet Passive Optical Network（DPoE）1.0 の DOCSIS プロビジョニングは、既存の DOCSIS プロビジョニング フローを使用して EPON アクセス テクノロジーをプロビジョニングするための標準です。DPoE ネットワークは、DPoE ネットワークが DOCSIS CMTS のように動作する場合、DOCSIS ネットワークと同様の IP 高速データ サービスを提供します。DPoE システムと DPoE 光ネットワーク ユニットは、仮想 CM（vCM）とも呼ばれる DOCSIS CM 同様に動作するように表示されます。プライム ケーブル プロビジョニングは、DPoE vCM デバイスの既存の DOCSIS デバイス タイプを使用します。DPoE 設定ファイルには、DOCSIS と DPoE 固有 TLV の両方が含まれています。

5.3 リリースから、プライム ケーブル プロビジョニングは DPoE 2.0 もサポートします。DPoE 2.0 仕様では、追加のサービス機能と対応するプロビジョニングおよびネットワーク管理機能の要件を提供する DPoE 1.0 仕様を強化ています。これは、複雑なネットワーク全体のサービスのプロビジョニングを簡素します。

DPoE vCM を特定するために、[Device Details（デバイスの詳細）] ページの表示される要求ディクショナリでキャプチャされた DHCP 検出データを参照します。次の例のような詳細が表示され、ページに太字のテキストが表示されたら、 DPoE vCM です。

例：

```
v-i-vendor-opts = enterprise-id 4491, (oro 1 2)
chaddr = 00:00:00:00:0d:12
relay-agent-info = (circuit-id 1 80:01:03:ef), (remote-id 2 00:00:00:00:0d:12), (v-i-vendor
-opts 9 enterprise-id 4491, (cmts-capabilities 1 (docsis-version 1 03:00
), (dpoe-system-version 1 01:00), (dpoe-system-pbb 4 10248294639d, 1a9eb
ee4971b, 26d07cd85ab2, 33800cf1abbb, 3b87c25dffbb, 47bd40a08f95, 4fc50b5
3a070, 5768bd554059, 591cf857aea1, 638c2d178f8f, 6d932a665ec9, 74efc6fc0
60b, 7a602d489587)))
relay-agent-circuit-id = 01:04:80:01:03:ef
client-id-created-from-mac-address = 0
dhcp-class-identifier = AIC Echo,docsis3.0:
hlen = 06
giaddr = 4.0.0.1
vendor-encapsulated-options = (device-serial-number 4 000000000d12),
(hardware-version-number 5 v3.2.1
), (software-version-number 6 v1.0.2), (boot-rom-version 7 BOOT1.0), (ve
ndor-oui 8 000000), (vendor-name 10 XEROX CORPORATION), (dpoe-embedded-c
omponents-list 55 ECM)
dhcp-parameter-request-list = {1,3,6,7,12,15,51,54,4,2,67,66}
client-id = ff:00:00:00:00:00:03:00:01:00:00:00:00:0d:12
```

サンプル DPoE 設定ファイル

サンプル DPoE 設定ファイルは、次の場所にインストールされたパッケージで使用できます。

- スタティック ファイル：dpoe_vcm.cm--/opt/CSCObac/rdu/samples/docsis
- Groovy ファイル：example_dpoe_vcm.groovy--/opt/CSCObac/rdu/samples/groovy
- テンプレート ファイル：dpoe_vcm.tmpl--/opt/CSCObac/rdu/templates

（注） プライム ケーブル プロビジョニングは、IPv4 と IPv6 モードで DPoE vCMs のプロビジョニングをサポートします。また、DPoE vCMs からコンピュータ デバイスのダウン ストリームのみがサポートされます。

DPoE TLVs については、DPoE オプション サポートOption Suppor を参照してください。

DPoE と DOCSIS プロビジョニングの違い

DPoE vCM のプロビジョニングは、DOCSIS CM のプロビジョニングとほぼ同じです。これにより、既存の DOCSIS ベース バックオフィス システム（プロビジョニング サーバなど）で、

変更を最小限に抑えながら DPoE vCM プロビジョニングをサポートします。ただし、DPoE vCM と DOCSIS CM プロビジョニングには少し違いがあります。

- DPoE 仕様は、PacketCable 音声サービスをサポートしていません。IP（HSD）および MEF サービスのみがサポートされます。
- DPoE システム（CMTS）には、追加のリレー エージェント DHCP オプションが用意されています。DHCPv4 リレー エージェント CMTS 機能オプションには、追加のサブオプションが含まれます（サブオプション 2：DPoE システム バージョンおよびサブオプション 4：DHCPv4 PBB サービス オプション）。
- DPoE vCM は ToD を要求しません。DPoE システム（CMTS）は、vCM に直接時間の参照を提供します。
- DPoE vCM は、DOCSIS 3.0 CM（例：docsis3.0）として同じ DHCPv4 オプション 60 を使用します。単独では、DHCPv4 オプション 60 値は DPoE vCM としてデバイスを識別するために十分ではありません。
- DPoE vCM は、eCM の背後にある eSAFE デバイスのリストを指定するために、新しい eSAFE DHCP オプション 43 サブオプション 55 を使用します。
- DPoE vCM は、DOCSIS 3.0 MULPI によりサポートされていない新しい設定ファイル TLVs をサポートしています（例：TLVs [22/23].14、[22/23].14.1、[22/23].14.2、[22/23].14.5、[22/23].14.6、[22/23].15、[22/23].15.1、[22/23].15.2）。
- DPoE vCM は、DOCSIS 3.0 MULPI で必要なすべての設定ファイル TLVs をサポートする必要はありません。DPoE システムはサポートされていない TLV を検出すると、DPoE システムは TLV を無視し、DPoE ONU を正常に登録できます。

DPoE ワークフロー

DPoE ワークフローは、DOCSIS ワークフローと同じです。詳細については、『DOCSIS Workflow』を参照してください。

CableHome の設定

このセクションでは、十分な CableHome 展開を実行する必要があるアクティビティについて説明します。CableHome テクノロジーには 2 つのバージョンがあります・セキュア（SNMP）と非セキュア（DHCP）です。このセクションでは、非セキュアバージョンのみを取り扱います。

このセクションでは、CableHome Specification CH-SP-CH1.0-I05-030801 の内容に精通していることを前提としています。

CableHome Workflow

非セキュア CableHome テクノロジーを使用するプロビジョニングに、プライム ケーブル プロビジョニングを正常に設定するには、この セクションでの説明事項に加えて、プライム ケー

ブル プロビジョニング コンポーネントの設定 に説明されているタスクを実行する必要があります。

次の表では、CableHome をサポートするためにプライム ケーブル プロビジョニングで実行する必要があるタスクを説明します。

表 *9 : CableHome* ワークフロー

	タスク	参照先
ステップ 1	RDU の設定	
	a. プロビジョニングされた DHCP 条件を設定します。 プロビジョニングする非セキュア CableHome デバイスで使用される、すべての DHCP 条件を追加します。	DHCP 条件の設定
	b. プロビジョニングされたサービス クラスを設定します。 非セキュア CableHome デバイスをプロビジョニングすることで、使用可能なサービス クラスを追加します。	サービス クラスの設定
	c.操作の無差別モードを設定します。	システムのデフォルト
ステップ 2	DPE の設定	
ステップ 3	Network Registrar の設定	
	クライアント クラス/範囲選択タグを設定して、プロビジョニングされた非セキュア CableHome DHCP 条件に追加されたものと一致させます。	Cisco プライム ネットワーク レジスタ エンドユーザー ガイド

Prime Network Registrar の設定

このセクションでは、Prime Network Registrar、ケーブル モデムの設定システム（CMTS）を設定する方法について説明します。

ステップ 1 プロビジョニング済みおよび未プロビジョニング WAN MAN およびプロビジョニング済み WAN データの選択タグを作成します。

『Cisco Prime Network Registrar End-User Guides』で指定されている新規およびプロビジョニング済みクライアント クラスと、ケーブル モデムの範囲を設定します。

ステップ 2 未プロビジョニングおよびプロビジョニング済みクライアント クラスと WAN MAN の範囲を設定します。

ステップ 3 プロビジョニング済みクライアント クラスと WAN データの範囲を設定します。

ステップ 4 すべてのサブネットへのルートを追加します。

RDU の設定

RDU で CableHome サポートを設定するには、次の設定を実行します。

CableHome WAN MAN の設定

1. プロビジョニングされた WAN MAN の DHCP 条件を作成します。これを行うには、クライアント クラスを Network Registrar CableHome WAN-MAN で設定されているクライアント クラス名に設定します。
2. プロビジョニングされた WAN MAN のサービス クラスを作成します。
   - サービス クラスに適切な CableHome 設定ファイルに */cos/chWanMan/file* を設定します。
   - 適切なファイアウォール設定ファイルに */chWanMan/firewall/file* を設定します。

CableHome WAN データの設定

ポータルのサービスにより WAN データの IP アドレスを取得する場合、これらの WAN データ パラメータを設定します。

1. WAN データの DHCP 条件を作成します。
2. WAN データのサービス クラスを作成します。

DPE の設定

CableHome テクノロジーをサポートする DPE を設定するには？

ステップ 1 CableHome デバイス プロビジョニング WAN MAN 設定ファイルを開き、DHCP オプション 60 が CableHome1.0 または CableHome1.1 のいずれかに設定されていることを確認します。一部の製造元は純粋なケーブル モデム、非 CableHome ルータ、CableHome ルータとして動作するように、デバイスを指示する独自の MIB

オブジェクトを使用します。デバイス DHCP パケットに DHCP オプション 60 の CableHome1.0 または CableHome1.1 を含まない場合、デバイスはコンピュータとして表示されます。

ステップ 2 ポータル サービスにより WAN データの IP アドレスを取得する場合：

- WAN MAN 設定ファイルには、0 よりも大きい値に cabhCdpWanDataIpAddrCount を設定する TLV 28 が含まれていることを確認します。
- ケーブル モデムの設定ファイルでは、WAN データ IP アドレスの番号を含むデバイスの最大数を設定します。

ステップ 3 CableHome デバイスを起動する場合自己プロビジョニングを有効にするには？

- *Unprov wan man.cfg* ポータル サービスでは、パススルー モードでポータル サービスを設定します。
- ケーブル モデム設定ファイルでは、デバイスの最大数を最低でも 2 に設定し、WAN-MAN およびコンピュータのプロビジョニングを許可します。コンピュータは、自己プロビジョニングするサインアップの web ページに直接アクセスできます。