CHAPTER 2

Broadband Access Center のアーキテクチャ

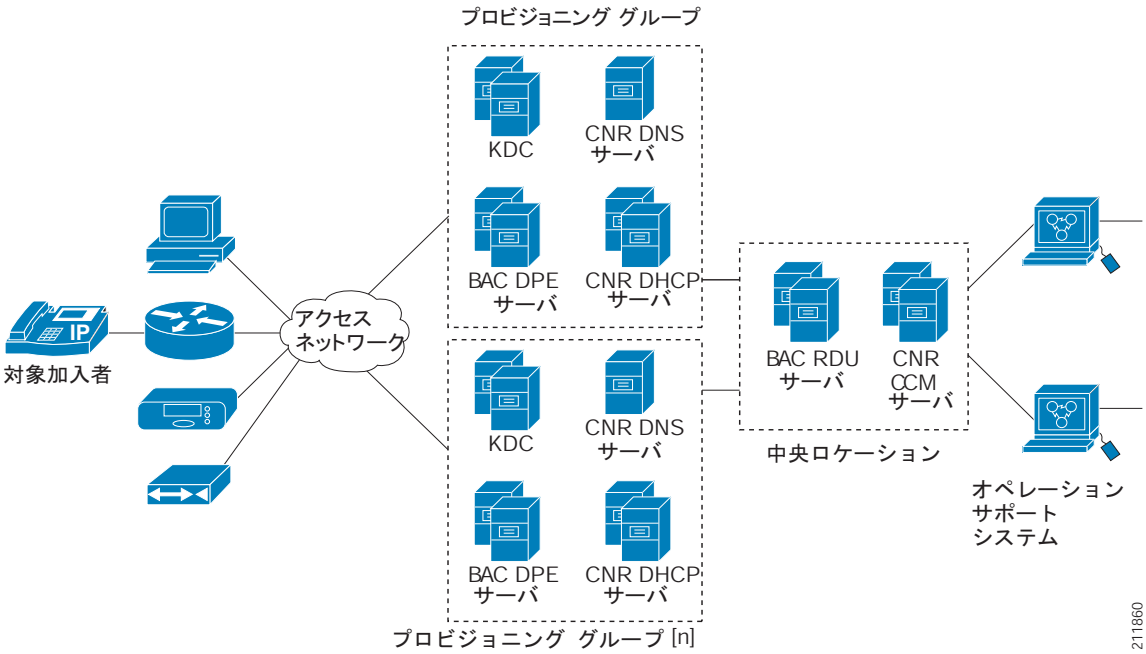
この章では、この Cisco Broadband Access Center（BAC）リリースに実装されているシステム アーキテクチャについて説明します。

この章は、次の項で構成されています。

配備

図 2-1 は、BAC ネットワークにおける一般的な完全冗長の配備を示しています。

図 2-1　BAC を使用した配備



アーキテクチャ

ここでは、次に示すコンポーネントから成る BAC の基本アーキテクチャについて説明します。

- Regional Distribution Unit（RDU）。次の機能を提供します。
  - BAC システムの権限あるデータ格納
  - Application Programming Interface（API; アプリケーション プログラミング インターフェイス）の要求を処理するためのサポート
  - システム全体のステータスおよび状態の監視

  詳細については、P.2-3 の「Regional Distribution Unit」を参照してください。
- Device Provisioning Engine（DPE）。次の機能を提供します。
  - 顧客宅内装置（CPE）とのインターフェイス
  - 構成キャッシュ
  - RDU および他の DPE から独立した操作
  - PacketCable プロビジョニング サービス
  - 構成用の IOS ライクなコマンドライン インターフェイス（CLI）

  詳細については、P.2-6 の「Device Provisioning Engine」を参照してください。
- クライアントからシステムの機能をすべて制御できるようにする BAC API。
- Cisco Network Registrar サーバ。次の機能を提供します。
  - Dynamic Host Configuration Protocol（DHCP）
  - Domain Name System（DNS; ドメイン ネーム システム）

  詳細については、P.2-13 の「Network Registrar」を参照してください。
- プロビジョニング グループ。次の機能を提供します。
  - 冗長クラスタ内の Network Registrar サーバおよび DPE の論理的なグループ化
  - 冗長性とスケーラビリティ

  詳細については、P.2-16 の「プロビジョニング グループ」を参照してください。
- Kerberos サーバ。PacketCable Multimedia Terminal Adapter（MTA; マルチメディア ターミナル アダプタ）を認証します。詳細については、P.2-14 の「Key Distribution Center」を参照してください。
- BAC プロセス ウォッチドッグ。次の機能を提供します。
  - すべての重要な BAC プロセスに対する管理のための監視
  - プロセス自動再開機能
  - BAC コンポーネント プロセスを開始および中止する機能

  詳細については、P.9-2 の「BAC プロセス ウォッチドッグ」を参照してください。
- SNMP エージェント。次の機能を提供します。
  - サードパーティの管理システム
  - SNMP バージョン v2
  - SNMP 通知

  詳細については、P.9-5 の「SNMP エージェント」を参照してください。
- 管理者のユーザ インターフェイス。次の機能をサポートします。
  - デバイスの追加、削除、修正、および検索
  - グローバル デフォルトの設定およびカスタム プロパティの定義

  詳細については、P.2-15 の「管理者のユーザ インターフェイス」を参照してください。

Regional Distribution Unit

RDU は BAC プロビジョニング システムの主要サーバです。RDU は Solaris オペレーティング システムを実行しているサーバにインストールする必要があります。

RDU には次の機能があります。

- デバイス構成生成の管理
- デバイス構成の生成、およびキャッシングのための DPE への配信
- デバイス構成を最新の状態に保つための DPE との同期
- すべての BAC 機能に対する API 要求の処理
- BAC システムの管理

RDU は、拡張性のあるアーキテクチャにより新しい技術とサービスの追加をサポートします。

現行の BAC では、1 回のインストールで 1 つの RDU がサポートされます。フェールオーバーをサポートする場合は、Veritas または Sun のクラスタリング ソフトウェアを使用することをお勧めします。フェールオーバーのセットアップでは、RAID（冗長ディスクアレイ）の共有ストレージを使用することをお勧めします。

以降の項では、次の RDU の概念について説明します。

- デバイス構成の生成（P.2-3）
- サービス レベル選択（P.2-4）

デバイス構成の生成

デバイスはブート時に、BAC に構成を要求します。この構成がデバイスのサービス レベルを決定します。この処理中、DHCP サーバは RDU にデバイスの構成を作成するように要求します。RDU は構成を生成して、そのデバイスが属するプロビジョニング グループにサービスを提供するすべての DPE に転送します。これで、DPE は RDU にアクセスしなくてもデバイスに構成を提供できるようになります。

デバイス構成には、ユーザが必要とする次のプロビジョニング情報を含めることができます。

- DHCP IP アドレス選択
- 帯域幅
- データ レート
- フロー制御
- 通信速度
- サービス レベル

構成には、任意のデバイスの DHCP 構成と TFTP ファイルを含めることができます。プロビジョニングされていないデバイスをインストールしてブートすると、デフォルトのテクノロジー固有の構成が割り当てられます。BAC がサポートするテクノロジーごとにデフォルト構成を変更できます。

RDU は、次の場合にデバイスの構成を再生成します。

- デバイスのサービス クラス変更など、特定のプロビジョニング API コールが実行された場合。
- 構成の検証が失敗した場合。デバイスから送信された DHCP 要求の特定のパラメータが最初の要求パラメータと異なる場合などに発生します。
- DPE がキャッシュへの再読み込みを行った場合。

RDU がデバイスの構成を再生成するたびに、更新された構成が該当する DPE に転送されます。

サービス レベル選択

サービス レベル選択の拡張ポイントは、RDU がデバイスの構成を生成するときに使用する DHCP 基準とサービス クラスを決定します。RDU は、この情報をデバイスごとにデータベースに保存します。

RDU がデバイス構成の生成に使用する DHCP 基準とサービス クラスは、デバイスに付与されているアクセス権のタイプに基づきます。デバイスのアクセス権には次の 3 つのタイプがあります。

- デフォルト：デフォルト アクセス権を付与されているデバイスの場合、BAC はデバイス タイプに割り当てられているデフォルトのサービス クラスと DHCP 基準を使用します。
- 無差別：無差別アクセス権を付与されているデバイスの場合、BAC はそのデバイスが背後にあるリレー エージェントからサービス クラスと DHCP 基準を取得します。
- 登録済み：登録済みアクセス権を付与されているデバイスの場合、BAC は RDU データベース内にある、デバイスの登録済みサービス クラスと DHCP 基準を使用します。

デバイス タイプごとに必ず 1 つのデフォルト拡張が存在している必要があります。

Configuration > Defaults のデフォルト ページを使用して特定のテクノロジーのサービス レベル選択の拡張ポイントを入力できます。詳細については、P.13-7 の「デフォルトの設定」を参照してください。デフォルトでは、これらのプロパティにゼロまたは組み込み拡張の 1 つが入力されます。

注意　独自のカスタム拡張をインストールしている場合を除き、これらの拡張を修正しないでください。

デバイスは、DHCP 基準とサービス クラスのセットを 1 つ受け付けるように登録されていても、実際には 2 つ目のセットを選択する場合があります。構成生成の拡張は、選択された DHCP 基準とサービス クラスを検索して使用します。

サービス レベル選択拡張は、デバイスに対して指定された特定のルールに基づいて 2 つ目のサービス クラスと DHCP 基準を選択します。たとえば、特定のプロビジョニング グループ内のデバイスについて、特定のサービス クラスと DHCP 基準を割り当てるには、そのデバイスをブートするように指定する場合があります。

拡張は、DHCP 基準とサービス クラスの特定のセットがデバイスのプロビジョニングに選択される理由となる情報を返します。これらの理由は、View Device Details ページの管理者のユーザ インターフェイスで確認できます。

表 2-1 に、これらの理由とその場合に付与されるアクセス権のタイプを示します。

表 2-1　サービス レベル選択拡張がデバイスのアクセス権を決定した理由

理由コード	説明	付与されるデバイス アクセス権のタイプ		
		デフォルト	無差別	登録済み
NOT_BEHIND_REQUIRED_DEVICE	必要なリレー エージェントの背後にデバイスがありません。	✓		
NOT_IN_REQUIRED_PROV_GROUP	必要なプロビジョニング グループにデバイスが含まれていません。	✓		
NOT_REGISTERED	デバイスが登録されていません。	✓		
PROMISCUOUS_ACCESS_ENABLED	リレー エージェントに対して無差別モードのアクセス権がイネーブルになっています。		✓	
REGISTERED	デバイスが登録されています。			✓
RELAY_NOT_IN_REQUIRED_PROV_GROUP	必要なプロビジョニング グループにリレー エージェントが含まれていません。	✓		
RELAY_NOT_REGISTERED	リレー エージェントが登録されていません。	✓		

（注） これらの理由のほとんどは、登録済みまたは無差別のアクセス権を付与するための要件違反を示しており、結果としてデフォルト アクセス権が付与されています。

Device Provisioning Engine

Device Provisioning Engine（DPE）は、CPE と通信してプロビジョニング機能および管理機能を実行します。

RDU は、DHCP 命令とデバイス構成ファイルを生成し、それらを関連する DPE サーバに配信します。DPE は DHCP 命令とデバイス構成ファイルをキャッシュします。次に、DHCP 命令は Network Registrar 拡張とのインタラクションで使用され、構成ファイルは TFTP サーバを介してデバイスに配信されます。

BAC は複数の DPE をサポートします。複数の DPE を使用して、冗長性とスケーラビリティを確保できます。

DPE は、デバイスへの構成ファイルの提供を含む、すべての構成要求を処理します。DPE は Network Registrar DHCP サーバと統合され、各デバイスの IP アドレスの割り当てを制御します。複数の DPE が 1 つの DHCP サーバと通信できます。

DPE は次に示すアクティビティを管理します。

- 最新の構成を取得してキャッシュするために RDU と同期する。
- 最終段階のデバイス構成を生成する（DOCSIS タイムスタンプなど）。
- DHCP サーバに DHCP メッセージ交換を制御する命令を提供する。
- TFTP を介して構成ファイルを配信する。
- Network Registrar と統合する。
- 音声テクノロジー サービスをプロビジョニングする。

DPE を Solaris オペレーティング・システムを実行するサーバにインストールする必要があります。CLI から DPE の設定と管理を行います。CLI には、ローカルで、または Telnet を介してリモートでアクセスできます。DPE がサポートする CLI コマンドの詳細については、『*Cisco Broadband Access Center DPE CLI Reference 4.0*』を参照してください。

（注）　インストール中に、各 DPE に対して次の項目を設定する必要があります。

- DPE が属するプロビジョニング グループの名前。この名前によって、DPE がサービスを提供するデバイスの論理グループが決まります。
- RDU の IP アドレスとポート番号。

DPE に関する重要な情報については、次の項を参照してください。

- DPE のライセンシング（P.2-7）
- TACACS+ および DPE 認証（P.2-7）
- DPE と RDU 間の同期（P.2-8）
- TFTP サーバ（P.2-10）
- ToD サーバ（P.2-11）

また、P.2-16 の「プロビジョニングの概念」の情報も十分に理解しておいてください。

DPE のライセンシング

ライセンシングにより、ご使用になれる DPE（ノード）の数が管理されます。お持ちのライセンスより多くの DPE をインストールしようとすると、新しい DPE は RDU に登録されず、拒否されます。ライセンスされている既存の DPE は、オンラインのままになります。

（注）　ライセンシングの目的上、登録済みの DPE は 1 つのノードと見なされます。

ライセンスの追加または評価ライセンスの延長を行った場合、または評価ライセンスが満了した場合、その変更はただちに有効になります。

RDU データベースから登録済みの DPE を削除すると、ライセンスは解放されます。DPE は RDU に自動的に登録されるため、ライセンスを開放する場合は DPE をオフラインにする必要があります。次に、管理者のユーザ インターフェイスまたは API を介して、DPE を RDU データベースから削除します。

削除した DPE は、属するすべてのプロビジョニング グループから削除されます。すべての Network Registrar 拡張に、その DPE が使用できなくなったことが通知されます。そのため、以前に削除された DPE が再度登録されると、再度ライセンスされたと見なされ、RDU から再度削除されるかライセンスが満了するまで、その状態が続きます。

RDU を使用してライセンスされていない DPE は、管理者のユーザ インターフェイスに表示されません。ライセンスの状態を判断するには、DPE と RDU のログファイルを調べる必要があります（*dpe.log* と *rdu.log*）。

（注）　特定のライセンスを介してイネーブルにした機能は、対応するライセンスがシステムから削除されても、引き続き動作します。

ライセンシングの詳細については、P.13-23 の「ライセンスの管理」を参照してください。

TACACS+ および DPE 認証

TACACS+ は TCP ベースのプロトコルで、多くのネットワーク デバイスを対象とする中央集中型のアクセスと DPE CLI のユーザ認証をサポートします。

TACACS+ を使用して、DPE は複数のユーザをサポートできます。各ユーザ名とログイン パスワードおよびイネーブル パスワードは、TACACS+ サーバで設定されます。TACACS+ は、TACACS+ クライアント / サーバ プロトコルを実装するために使用されます（ASCII ログインのみ）。

TACACS+ 特権レベル

TACACS+ サーバは、TACACS+ プロトコルを使用して DPE にログインするユーザを認証します。TACACS+ クライアントは、そのユーザに設定される特定のサービス レベルを指定します。

表 2-2 は、DPE ユーザのアクセスを許可するために使用される 2 つのサービス レベルを示します。

表 2-2　TACACS+ サービス レベル

モード	説明
ログイン	*router>* プロンプトでのユーザレベル コマンド
イネーブル	*router#* プロンプトでのイネーブルレベル コマンド

TACACS+ クライアント設定

TACACS+ は、CLI を使用して設定される複数のプロパティを使用します。TACACS+ に関するコマンドの詳細については、『*Cisco Broadband Access Center DPE CLI Reference 4.0*』を参照してください。

TACACS+ をイネーブルにする場合、管理者はすべての TACACS+ サーバの IP アドレスまたは Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を、デフォルト値以外に指定する必要があります。

次の設定についても、該当する場合はデフォルト値を使用して指定できます。

- 各 TACACS+ サーバの共有秘密鍵。この鍵を使用して、DPE と TACACS+ サーバの間のデータを暗号化できます。特定の TACACS+ サーバの共有秘密情報を省略することを選択した場合、TACACS+ メッセージ暗号化は使用されません。
- TACACS+ サーバのタイムアウト値。この値を使用して、TACACS+ サーバがプロトコル要求に応答するのを TACACS+ クライアントが待機する最長時間を指定できます。
- TACACS+ サーバのリトライ回数。この値を使用して、TACACS+ クライアントが TACACS+ サーバとの有効なプロトコル交換を試行する回数を指定できます。

DPE と RDU 間の同期

DPE と RDU 間の同期とは、RDU との整合を取るために、DPE キャッシュを自動的に更新するプロセスです。DPE キャッシュは、デバイスの構成を含む構成キャッシュと、デバイスに必要なファイルを含むファイル キャッシュから構成されます。

通常、RDU は、構成の更新が含まれるイベントを生成し、関係するすべての DPE に送信して DPE を最新の状態に保ちます。同期が必要になるのは、接続の切断によって DPE 側でいくつかのイベントが欠落した場合です。切断の原因としては、ネットワークの問題、管理目的での DPE サーバのダウン、または障害などが考えられます。

また、同期は、RDU データベースをバックアップから復元するという特殊なケースでも使用されます。このケースでは、RDU との整合を取るために、DPE キャッシュのデータベースを古い状態に戻す必要があります。

RDU と DPE 間の同期プロセスは自動的に実行されるため、管理操作は必要ありません。同期プロセスの実行中でも、DPE は CPE に対してプロビジョニング操作や管理操作をすべて実行できます。

同期プロセス

DPE は RDU との接続を確立するたびに同期プロセスをトリガーします。

DPE は最初に起動したときに、RDU への接続を確立し、RDU に登録して構成変更の更新を受信します。次に、DPE と RDU が、ハートビート メッセージの交換を使用して、接続を監視します。DPE は、RDU への接続が切断されたと判断すると、接続の再確立を自動的に試みます。この試行は、成功するまでバックオフのリトライ間隔で続行されます。

RDU も、接続の切断を検出すると、DPE へのイベントの送信を停止します。接続の切断によって RDU からの更新イベントが DPE 側で欠落する場合があるため、DPE は、RDU との接続を確立するたびに同期を実行します。

一般的な DPE の状態

同期プロセス中、DPE は次の状態になります。

1. Registering : RDU との接続を確立して登録するプロセスの間、DPE は *Registering* 状態になっています。
2. Synchronizing : DPE は、必要な構成のグループを RDU に要求します。このプロセスの間、DPE は、ストレージ内の構成のうち、整合の取れていない（バージョン番号が間違っている）もの、欠落しているもの、および削除するものを判別し、必要であればキャッシュ内の構成を更新します。また、DPE は TFTP サーバに配信可能なキャッシュ内のファイルを同期します。DPE では、RDU が構成要求によって過負荷にならないようにするため、一度に 1 つのバッチだけを中央サーバに送信します。
3. Ready : DPE は最新の状態であり、RDU と完全に同期が取れています。通常 DPE はこの状態にあります。

表 2-3 に、DPE に発生し得るその他の状態を示します。

表 2-3　関連する DPE の状態

状態	説明
Initializing	起動中です。
Shutting Down	停止処理中です。
Down	Network Registrar 拡張ポイントからのクエリーに応答しません。
Ready Overloaded	DPE が実行されているシステムに過大な負荷がかかっている点を除き、*Ready* と同様です。

（注）　DPE の状態に関係なく、デバイス構成要求、TFTP 要求、および ToD 要求に引き続きサービスが提供されます。

DPE 状態は次の方法で表示できます。

- 管理者のユーザ インターフェイスから表示します。P.12-23 の「Device Provisioning Engine の表示」を参照してください。
- **show dpe** コマンドを使用して DPE CLI から表示します。『*Cisco Broadband Access Center DPE CLI Reference 4.0*』を参照してください。

TFTP サーバ

統合された TFTP サーバは、デバイスおよびデバイス以外のエンティティから、DOCSIS 構成ファイルを含む、ファイル要求を受信します。その後、このサーバはファイルを要求元のエンティティに送信します。

TFTP サーバは、ローカル ファイルシステム アクセスに使用されるホーム ディレクトリにあります。ローカル ファイルは、*BPR_DATA/dpe/tftp* ディレクトリに格納されています。このリリースでは、すべての配信可能な TFTP ファイルは、事前に DPE にキャッシュされます。つまり、DPE は常にシステム内のすべてのファイルが使用された最新の状態になっています。

（注）　DPE での TFTP サービスには、要件に合せてサービスを設定できる機能があります。

デフォルトでは、TFTP サーバは TFTP 読み取りに対してキャッシュしか検索しません。ただし、DPE コマンドラインから **service tftp** *1..1* **allow-read-access** コマンドを実行すると、TFTP サーバはキャッシュの前にローカル ファイル システムを検索します。ファイルがローカル ファイル システムにある場合は、そこからファイルを読み取ります。ファイルがない場合、TFTP サーバはキャッシュを検索します。ファイルがキャッシュにある場合、サーバはそのファイルを使用し、キャッシュにない場合はエラーを返します。

ローカル ファイル システムからの読み取りアクセスをイネーブルにできる場合、ディレクトリ構造読み取り要求は、ローカル ファイル システムからだけ許可されます。

（注）　すべての TFTP ファイルに一意の名前を指定します。ファイルを大文字と小文字を使用して区別しないようにしてください。DPE は、ローカル ディレクトリまたはキャッシュでファイルを検索するとき、すべてのファイル名を小文字に変換するため、ファイル名の文字は重要です。

IPv4 または IPv6 を使用する TFTP 転送を指定するには、DPE コマンドラインから **service tftp** *1..1* **ipv4 | ipv6 enabled true** コマンドを使用します。また、転送のブロックサイズを指定するには、***service tftp*** *1..1* ***ipv4*** **|** ***ipv6 blocksize*** コマンドを使用します。blocksize オプションには、データ オクテットの数を指定します。これにより、クライアントとサーバが、ネットワーク メディアにより適したブロック サイズをネゴシエートできます。blocksize をイネーブルにすると、TFTP サービスは、要求されたブロック サイズが指定された上限と下限の間に収まっていれば、転送に使用します。詳細については、『*Cisco Broadband Access Center DPE CLI Reference 4.0*』を参照してください。

TFTP サービスは、TFTPv4 と TFTPv6 について、処理された TFTP パケット数の統計情報を保持しています。これらの統計情報は、Device Details ページの管理者のユーザ インターフェイスで表示できます。詳細については、P.12-10 の「デバイスの詳細の表示」を参照してください。

ToD サーバ

BAC の統合された Time of Day（ToD）サーバは、RFC 868 の高性能 UDP を実装します。

（注）　DPE での ToD サービスには、要件に合せてサービスを設定できる機能があります。

ToD サービスをイネーブルにして IPv4 または IPv6 をサポートするには、DPE コマンドラインから **service tod** *1..1* **enabled true** コマンドを使用します。デフォルトでは、ToD サービスは DPE でディセーブルになっています。

このプロトコルを DPE に設定するときには、プロビジョニング用に設定したインターフェイスにだけ ToD サービスはバインドされることに注意してください。ToD サービスの設定の詳細については、『*Cisco Broadband Access Center DPE CLI Reference 4.0*』を参照してください。

ToD サービスは、ToDv4 と ToDv6 について、処理された ToD パケット数の統計情報を保持しています。これらの統計情報は、Device Details ページの管理者のユーザ インターフェイスで表示できます。詳細については、P.12-10 の「デバイスの詳細の表示」を参照してください。

DOCSIS 共有秘密情報

BAC では、Cable Modem Termination System（CMTS; ケーブル モデム ターミネーション システム）ごとに異なる DOCSIS Shared Secret（DSS; DOCSIS 共有秘密情報）を定義できます。このように定義すると、共有秘密情報が侵害されても影響を受ける CMTS の数が限られ、配備におけるすべての CMTS が対象となりません。

DSS は DPE ごとに設定できますが、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 に設定されている内容と一致させる必要があります。

注意　1 つのプロビジョニング グループ内に複数の DSS を設定すると、場合によって CMTS のパフォーマンスが低下する可能性があります。ただし、実質的に BAC には影響がありません。

共有秘密情報はクリア テキスト文字列または IOS 暗号化文字列で入力できます。クリア テキストで入力する場合、DSS は IOS バージョン 12.2BC に適合するように暗号化されます。

また、管理者のユーザ インターフェイスまたは API を使用して、RDU から DSS を設定することもできます。この場合、DSS はクリア テキストで入力され、RDU に格納されて、すべての DPE に渡されます。そのため、このように入力された DSS は、DPE に保存される前に暗号化されます。

CLI から ***dpe docsis shared-secret*** コマンドを使用して直接 DSS を DPE で設定する場合、この設定は RDU から設定される内容よりも優先されます。

DOCSIS 共有秘密情報のリセット

DSS のセキュリティが侵害された場合、または単に管理目的で共有秘密情報を変更する場合は DSS をリセットできます。

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、表示された設定から DOCSIS 共有秘密情報を DPE 設定にコピー アンド ペーストします。この方法で、Cisco CMTS に入力した設定を DPE CLI にコピーできます。

（注）　上記で説明されたように共有秘密情報を変更するには、CMTS は 12.2BC より新しいソフトウェア バージョンで実行されている必要があります。

DSS を変更するには、次の手順に従います。

ステップ 1　リセットする DOCSIS 共有秘密情報を持つプロビジョニング グループを確認します。

ステップ 2　そのプロビジョニング グループに関連付けられた DPE と CMTS のリストを調べます。

ステップ 3　CMTS 上でプライマリ DSS を変更します。

ステップ 4　CMTS 上で侵害された DSS をセカンダリ DSS に変更します。すべての DOCSIS 設定ファイルが新しい DSS を使用するように正しく変更されるまで、ケーブル モデムで登録を実行できるようにする必要があります。

ステップ 5　影響を受けた DPE を判別し、それぞれ 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てから、侵害されたセカンダリ共有秘密情報を CMTS 設定から削除します。

Network Registrar

Network Registrar は、BAC で DHCP および DNS 機能を提供します。Network Registrar の DHCP 拡張ポイントは、BAC を Network Registrar と統合します。これらの拡張を使用して、BAC は DHCP 要求の内容を調べてデバイス タイプを検出し、その構成に従って内容を操作し、プロビジョニングするデバイスのカスタマイズされた構成を配信します。

Network Registrar の詳細については、『*User Guide for Cisco Network Registrar 7.0*』、*/docs* ディレクトリの *CLIFrame.html*、および『*Installation Guide for Cisco Network Registrar, 7.0*』を参照してください。

DHCP

DHCP サーバは、IP ネットワーク上で IP アドレスを設定するプロセスを自動化します。このプロトコルは、デバイスをネットワークに接続するときにシステム管理者が行う多くの機能を実行します。DHCP はネットワーク ポリシーの決定を自動的に管理するため、手動の設定が不要になります。これにより、ネットワーク デバイスの設定の柔軟性とモビリティが高まり、管理が容易になります。

このリリースの BAC は、IPv6 用の DHCP（DHCPv6 とも呼ばれる）をサポートします。DHCPv6 を使用すると、DHCP サーバは、拡張を介して設定パラメータを IPv6 ホストに配信できるようになります。IPv6 ホストは、デフォルトでステートレス自動設定を使用します。これは、IPv6 ホストがローカル IPv6 ルータを使用して独自のアドレスを設定できるようにするものです。DHCPv6 とは、このステートフル自動設定オプションのことで、サーバがホストに設定情報を設定する技術の 1 つです。

DHCPv6 には次の利点があります。

- IPv6 アドレスによるアドレッシング機能の拡張
- ステートフル自動設定プロトコルを使用した容易なネットワーク管理
- オプションと拡張のサポート向上
- リレー エージェント機能
- 1 つのインターフェイスへの複数アドレスの割り当て

DHCPv4 と DHCPv6 の比較

DHCPv6 は、DHCPv4 と同様にクライアント / サーバ モデルを使用します。DHCP サーバと DHCP クライアントは、IP アドレスの要求、オファー、およびリースを行うために一連のメッセージを交わします。DHCPv4 とは異なり、DHCPv6 は、一括して会話を行う場合、ブロードキャスト メッセージではなく、ユニキャスト メッセージとマルチキャスト メッセージの組み合せを使用します。

この他にも DHCPv4 と DHCPv6 には次のような違いがあります。

- DHCPv4 とは異なり、DHCPv6 の IPv6 アドレス割り当てはメッセージ オプションを使用して処理されます。
- DHCP 検出や DHCP オファーなど、DHCPv4 でサポートされていたメッセージ タイプが DHCPv6 では削除されています。代わりに、DHCPv6 サーバはクライアントの送信要求メッセージとその後に続くサーバのアドバタイズ メッセージによって検索されます。
- DHCPv4 クライアントとは異なり、DHCPv6 クライアントは複数の IPv6 アドレスを要求できます。

DHCPv4 フェールオーバーによって、DHCP サーバのペアは、片方が機能を停止したらもう一方が引き継ぐという方法で機能します。このサーバのペアは、メイン サーバおよびバックアップ サーバと呼ばれます。通常の状況では、メイン サーバがすべての DHCP 機能を実行します。メイン サーバが使用不能になると、バックアップ サーバが引き継ぎます。このように、DHCP フェールオーバーでは、メイン サーバに障害が発生しても DHCP サービスへのアクセスが失われないようにします。

DNS

DNS サーバは、IP アドレス、ホスト名など、ネットワーク全体のホストに関する情報を格納します。DNS は主に IP アドレスとドメイン名を変換するためにこの情報を利用します。www.cisco.com などの名前を IP アドレスに変換することで、インターネットベースのアプリケーションへのアクセスが簡素化されます。

リース クエリー

リース クエリー機能を使用すると、プロビジョニング グループ内の Network Registrar DHCP サーバに、現在の IP アドレス情報を直接要求できます。デバイスの IP アドレスを見つけるために、RDU は DHCP リース クエリー メッセージを、デバイスのプロビジョニング グループ内の DHCP サーバだけに送信し、ネットワーク上のすべての DHCP サーバにクエリーが送信されないようにします。すべての応答の中で、デバイスと最後に通信したサーバからの応答が信頼できる応答と見なされます。

以前のバージョンの BAC では、リース クエリー機能は、リース クエリー要求を送信するための送信元インターフェイスと送信元ポートの選択をオペレーティング システムに依存していました。このリリースでは、特定のインターフェイスと送信元ポートを使用するように RDU を設定できます。

このリリースの BAC でのリース クエリー サポートの詳細については、P.6-19 の「リース クエリー」を参照してください。

Key Distribution Center

Key Distribution Center（KDC; 鍵発行局）は、PacketCable MTA を認証し、サービス チケットを MTA に与えます。そのため、MTA の証明書を検査するとともに、KDC 自体の証明書を提示して MTA が KDC を認証できるようにする必要があります。また、DPE（プロビジョニング サーバ）と通信して、MTA がネットワークでプロビジョニングされていることを検証します。

KDC は Solaris オペレーティング・システムを実行するサーバにインストールする必要があります。

KDC の認証に使用される証明書は BAC には同梱されていません。必要な証明書を Cable Television Laboratories, Inc.（CableLabs）から入手する必要があります。また、これらの証明書の内容は、MTA にインストールされているものと一致する必要があります。詳細については、P.14-3 の「PKCert.sh ツールの使用方法」を参照してください。

注意　証明書がインストールされていないと、KDC は機能しません。

KDC では、ライセンスが機能している必要があります。シスコ代理店から KDC ライセンスを入手し、正しいディレクトリにインストールしてください。ライセンスのインストール方法については、P.7-9 の「KDC ライセンス」を参照してください。

KDC には、BAC インストール中に *BPR_HOME/kdc/solaris/kdc.ini* プロパティ ファイルに入力される、いくつかのデフォルト プロパティがあります。このファイルを編集して、操作要件で指示された値に変更することができます。詳細については、P.7-7 の「KDC のデフォルト プロパティ」を参照してください。

また、KDC は複数のレルムの管理をサポートします。追加のレルム設定の詳細については、P.7-10 の「複数レルムのサポート」を参照してください。

BAC プロセス ウォッチドッグ

BAC プロセス ウォッチドッグは、すべての BAC プロセスのランタイム状況を監視する管理エージェントです。このウォッチドッグ プロセスにより、プロセスが予想外に停止した場合に自動的に再開されるようになります。BAC コンポーネントを実行する各システム上で、BAC プロセス ウォッチドッグのインスタンスが 1 つ実行されます。

BAC プロセス ウォッチドッグは、監視対象プロセスの状態を開始、停止、再開、決定するコマンドライン ツールとして利用できます。

監視対象プロセスの管理方法の詳細については、P.9-2 の「BAC プロセス ウォッチドッグ」を参照してください。

SNMP エージェント

BAC では、RDU サーバおよび DPE サーバについて基本的な SNMP v2 ベースの監視がサポートされます。BAC SNMP エージェントでは SNMP 通知と SNMP トラップがサポートされます。それらをまとめて「通知」と呼びます。

SNMP エージェントは、次の方法で設定できます。

- RDU で、SNMP 設定コマンドライン ツール（P.10-10 の「SNMP の使用によるサーバの監視」を参照）または API を介して設定する。
- DPE で、**snmp-server** CLI コマンドを使用して設定する。『*Cisco Broadband Access Center DPE CLI Reference 4.0*』を参照してください。

管理者のユーザ インターフェイス

BAC 管理者のユーザ インターフェイスは、BAC システムを集中管理するための Web ベースのアプリケーションです。このシステムを使用して、次の作業を行うことができます。

- グローバル デフォルトの設定
- カスタム プロパティの定義
- サービス クラスの追加、修正、および削除
- DHCP 基準の追加、修正、および削除
- デバイスの追加、修正、および削除
- デバイスのグループ化
- サーバの状態とサーバ ログの表示
- ユーザの管理

このインターフェイスの使用方法については、それぞれ次の章を参照してください。

- 第 11 章「管理者のユーザ インターフェイスについて」：BAC 管理者のユーザ インターフェイスにアクセスする方法や設定方法について説明します。
- 第 12 章「管理者のユーザ インターフェイスの使用方法」：各種 BAC コンポーネントの監視など、管理作業を行う方法について説明します。
- 第 13 章「Broadband Access Center の設定」：BAC を設定するために実行する作業について説明します。

プロビジョニングの概念

この項では、プロビジョニングの重要な概念について説明します。次の項目を取り上げます。

プロビジョニング グループ

プロビジョニング グループは、通常 1 つ以上の DPE と DHCP サーバのフェールオーバー ペアで構成されるサーバを、論理的に（通常は地理的に）グループ化したものになるように設計されています。特定のプロビジョニング グループ内の各 DPE では、RDU からの同一の構成セットがキャッシュされます。その結果、冗長性とロード バランシングが可能になります。デバイスの数が増えたら、追加のプロビジョニング グループを配備に加えることができます。

（注）　プロビジョニング　グループのサーバは、各地域に設置する必要はありません。中央のネットワーク オペレーション センターに簡単に配備できます。

プロビジョニング グループでは、BAC 配備のスケーラビリティを拡張する手段として、各プロビジョニング グループをデバイスのサブセットだけに関連付けます。このようなデバイスのパーティション化では、デバイスを地域的にグループ化することや、サービス プロバイダーによって定義されたポリシー別にグループ化することができます。

サービス プロバイダーで配備を拡大するには、次の作業を行います。

- 既存の DPE サーバのハードウェアをアップグレードする。
- プロビジョニング グループに DPE サーバを追加する。
- プロビジョニング グループを追加する。

冗長性とロード シェアリングをサポートするために、各プロビジョニング サポートは任意の数の DPE に対応できます。DHCP サーバから要求が届くと、その要求はプロビジョニング グループ内の DPE 間に分配され、デバイスと特定の DPE の間にアフィニティが確立されます。プロビジョニング グループ内の DPE 状態が安定している限り、このアフィニティは保たれます。

静的プロビジョニングと動的プロビジョニングの比較

BAC は、デバイス構成を使用してネットワークにデバイスをプロビジョニングします。デバイス構成とは、テクノロジー タイプに基づいた特定のデバイスのプロビジョニング データです。BAC を使用したデバイスのプロビジョニング方法には、静的プロビジョニングと動的プロビジョニングの 2 つがあります。

静的プロビジョニング時には、BAC システムに静的設定ファイルを入力します。この設定ファイルは、構成を生成するために TFTP を介して特定のデバイスに配信されます。BAC は、静的設定ファイルをその他のバイナリ ファイルと同様に扱います。

動的プロビジョニング時にはテンプレートを使用します。テンプレートは、DOCSIS、PacketCable、または CableHome オプションと、特定のサービス クラスで使用されると動的にファイルを生成する値が含まれるテキスト ファイルです。動的設定ファイルを使用すると、プロビジョニング プロセス中の柔軟性とセキュリティが強化されます。

表 2-4 に、それぞれのファイルを使用した静的プロビジョニングと動的プロビジョニングの影響を示します。

表 2-4　静的プロビジョニングと動的プロビジョニングの比較

静的ファイルを使用した静的プロビジョニング	テンプレート ファイルを使用した動的プロビジョニング
使用可能なサービス オファリングの数が少ない場合に使用する	使用可能なサービス オファリングの数が多い場合に使用する
限定的な柔軟性	より高い柔軟性（特にデバイスに固有の構成が必要な場合）
相対的に低い安全性	より高い安全性
高いパフォーマンス	低いパフォーマンス。これは、デバイスに割り当てられているテンプレートが更新されるたびに、そのテンプレートに関連付けられているすべてのデバイスの構成が更新されるためです。
簡単な使用方法	より複雑な使用方法

プロビジョニング グループの機能

配備にデバイスのサブセットをプロビジョニングするには、プロビジョニング グループによるそれらのデバイスのプロビジョニングが可能であり、かつイネーブルになっている必要があります。たとえば、DPE がこの機能をサポートするように設定されていない場合、プロビジョニング グループは PacketCable MTA を Secure モードでプロビジョニングできません。

以前のリリースの BAC では、プロビジョニング グループ内の各 DPE がサポートできる機能を起動時に RDU に登録していました。この情報が、プロビジョニング グループに含まれる他の DPE の情報と結合されて、グループがサポートできるデバイス タイプを決定していました。サーバは、その下位機能を登録し、またそれらの機能をイネーブルまたはディセーブルに登録しました。サーバの登録後、プロビジョニング グループは自動的にイネーブルになり、サポート可能なデバイス タイプをサポートしていました。一方、このリリースの BAC では、次のように手動でデバイス サポートをイネーブルにする必要があります。

- Provisioning Group Details ページの管理者のユーザ インターフェイスを使用します。P.12-29 の「プロビジョニング グループの表示」を参照してください。
- API で *ProvGroupCapabilitiesKeys* 定数を使用します。詳細については、API Javadoc を参照してください。

イベントのロギング

イベントのロギングは RDU と DPE で実行されます。まれに、視認性向上のために、DPE イベントが RDU に記録されることもあります。ログ ファイルはそれぞれのログ ディレクトリに保存され、任意のテキスト エディタを使用して調べることができます。ログ ファイルを圧縮すると、トラブルシューティングや障害の解決のために Cisco Technical Assistance Center またはシステム インテグレータに電子メールで送信しやすくなります。また、RDU と DPE のログには、管理者のユーザ インターフェイスからアクセスすることもできます。

ログのレベルと構造、およびログ ファイルの番号付けと循環の詳細については、P.10-2 の「ログのレベルおよび構造」を参照してください。