CISCO SYSTEMS

Cisco Broadband Access Center for Cable アドミニストレータ ガイド

Release 2.7

Text Part Number: OL-4409-01-J

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。見当たらない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）パブリック ドメイン バージョンとして、UCB が開発したプログラムを最適化したものです。All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCSP、Cisco Square Bridge のロゴ、Follow Me Browsing、および StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn および iQuick Study は、Cisco Systems, Inc. のサービスマークです。Access Registrar、Aironet、ASIST、BPX、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Cisco Unity、Empowering the Internet Generation、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、FormShare、GigaDrive、GigaStack、HomeLink、Internet Quotient、IOS、IP/TV、iQ Expertise、iQ のロゴ、iQ Net Readiness Scorecard、LightStream、Linksys、MeetingPlace、MGX、Networkers のロゴ、Networking Academy、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、ProConnect、RateMUX、ScriptShare、SlideCast、SMARTnet、StrataView Plus、SwitchProbe、TeleRouter、The Fastest Way to Increase Your Internet Quotient、TransPath、および VCO は、米国および一部の国における Cisco Systems, Inc. とその関連会社の登録商標です。

このマニュアルおよび Web サイトで言及されているその他の商標はすべて、それぞれの所有者のものです。「パートナー」という語の使用は、シスコと他社の提携関係を意味するものではありません。（0501R）

Cisco Broadband Access Center for Cable アドミニストレータ ガイド
Copyright © 2002 - 2005 Cisco Systems, Inc.
All rights reserved.

CONTENTS

このマニュアルについて xv

- **対象読者** xv
- **マニュアルの構成** xvi
- **表記法** xvii
- **関連資料** xviii
- **技術情報の入手方法** xix
  - Cisco.com xix
  - Product Documentation DVD（英語版） xix
  - **マニュアルの発注方法（英語版）** xx
  - **シスコシステムズマニュアルセンター** xx
- **シスコ製品のセキュリティの概要** xxi
  - **シスコ製品のセキュリティ問題の報告** xxi
- **テクニカル サポート** xxii
  - Cisco Technical Support & Documentation Web **サイト** xxii
  - Japan TAC Web **サイト** xxii
  - **サービス リクエストの発行** xxiii
  - **サービス リクエストのシビラティの定義** xxiii
- **その他の資料および情報の入手方法** xxiv

CHAPTER 1 **Broadband Access Center for Cable の概要** 1-1

- **機能と利点** 1-1
- **サポート対象の技術** 1-2
  - DOCSIS **高速データ通信** 1-2
  - PacketCable **音声サービス** 1-2
  - **ノンセキュア** PacketCable **音声サービス** 1-2
  - Euro-PacketCable **音声サービス** 1-2
  - **ノンセキュア** CableHome **プロビジョニング** 1-3

CHAPTER 2 **Broadband Access Center for Cable システム アーキテクチャ** 2-1

- **アーキテクチャ** 2-2
- **登録モード** 2-3

標準モード 2-3
無差別モード 2-3
ローミング モード 2-3
混在モード 2-3
Regional Distribution Unit 2-4
デバイス構成の生成 2-4
サービス レベル選択 2-5
Regional Distribution Unit のフェールオーバー 2-5
Device Provisioning Engine 2-6
Device Provisioning Engine の種類 2-6
ハードウェア Device Provisioning Engine 2-6
Solaris Device Provisioning Engine 2-7
DPE ライセンス キー 2-7
TACACS+ および DPE 認証 2-7
TACACS+ 特権レベル 2-8
TACACS+ クライアント設定 2-8
DPE サーバの割り当て 2-8
TFTP サーバ 2-9
DOCSIS 共有秘密情報 2-9
DOCSIS 共有秘密情報のリセット 2-10
プロビジョニング グループ 2-11
Cisco Network Registrar 2-12
ダイナミック ホスト コンフィギュレーション プロトコル 2-12
ドメイン ネーム システム 2-12
リース予約 2-13
鍵発行局 2-14
デフォルトの KDC のプロパティ 2-14
Euro-PacketCable のサポート 2-15
KDC 証明書 2-16
KDC ライセンス 2-16
複数領域のサポート 2-17
BACC MIB 2-18
BACC エージェント 2-19
SNMP エージェント 2-19
MIB のサポート 2-19
BACC エージェント 2-20
監視対象プロセス 2-20
BACC エージェント コマンドライン 2-20

ロギング 2-22
Regional Distribution Unit のログ 2-22
Device Provisioning Engine のログ 2-22
ログのレベルおよび構造 2-22
ログ レベルの設定 2-23
dpe.log ファイルの表示 2-24
管理者のユーザ インターフェイス 2-24
サンプル ユーザ インターフェイス 2-24

CHAPTER 3 設定のワークフローとチェックリスト 3-1
コンポーネントのワークフロー 3-2
RDU チェックリスト 3-2
ハードウェア DPE のチェックリスト 3-3
Solaris DPE のチェックリスト 3-4
Network Registrar チェックリスト 3-6
技術のワークフロー 3-7
DOCSIS チェックリスト 3-7
PacketCable チェックリスト 3-8
PacketCable 3-8
ノンセキュア PacketCable 3-10
Euro-PacketCable 3-12
ノンセキュア CableHome プロビジョニング チェックリスト 3-14

CHAPTER 4 DOCSIS 設定 4-1
DOCSIS ワークフロー 4-1
ダイナミック DOCSIS テンプレートによる MIB の使用方法 4-3
DOCSIS 設定のための BACC 機能 4-4
動的設定 TLV 4-4
DPE TFTP IP 検証 4-4
DOCSIS 1.0、1.1、2.0 のサポート 4-5
DOCSIS バージョンに基づいた DOCSIS 設定ファイル 4-5
DOCSIS ネットワークのトラブルシューティング 4-5
ネットワーク層以上の設定 4-6
DHCP 状態の確立 4-6
ToD 状態の確立 4-7
セキュリティ アソシエーション状態 4-7
設定ファイル状態 4-8
登録状態 4-8
プライバシー状態の確立 4-8

動作状態 4-9
ケーブル モデムの状態のトラブルシューティング 4-10
オンライン状態 4-10
オフライン状態 4-11
レンジング プロセス：init(r1)、init(r2)、および init(rc) 状態 4-16
DHCP：init(d) 状態 4-18
DHCP：init(i) 状態 4-20
TOD 交換：init(t) 状態 4-23
オプション ファイル転送開始：init(o) 状態 4-25
online、online(d)、online(pk)、online(pt) 状態 4-26
reject(pk) および reject(pt) 状態 4-29
登録：reject (m) 状態 4-31
登録：reject (c) 状態 4-32

CHAPTER 5 PacketCable 音声設定 5-1
PacketCable EMTA のセキュア プロビジョニング 5-2
BACC PacketCable のセキュアなプロビジョニングのフロー 5-2
PacketCable EMTA の BASIC プロビジョニング 5-5
PacketCable の TLV 38 と MIB のサポート 5-6
SNMP v2C 通知 5-6
Euro-PacketCable 5-6
Euro-PacketCable の MIB 5-6
Euro-PacketCable の MIB の設定 5-7
eMTA プロビジョニングのトラブルシューティング 5-8
コンポーネント 5-8
組み込み型メディア ターミナル アダプタ 5-8
DHCP サーバ 5-9
DNS サーバ 5-9
鍵発行局 5-9
PacketCable プロビジョニング サーバ 5-9
Call Management Server 5-10
基本変数 5-10
証明書 5-10
スコープ選択タグ 5-11
MTA 設定ファイル 5-11
トラブルシューティングのツール 5-12
ログ 5-12
Ethereal、SnifferPro、およびその他のパケット キャプチャ ツール 5-12
トラブルシューティングのシナリオ 5-13

証明書信頼階層 5-17
証明書の検証 5-18
MTA デバイス証明書階層 5-19
MTA ルート証明書 5-19
MTA 製造業者証明書 5-20
MTA デバイス証明書 5-21
MTA 製造業者コード検証証明書 5-21
CableLabs サービス プロバイダー証明書階層 5-22
CableLabs サービス プロバイダー ルート証明書 5-22
サービス プロバイダー CA 証明書 5-23
ローカル システム CA 証明書 5-24
運用上の補助証明書 5-25
証明書失効 5-28
コード検証証明書階層 5-28
CVC の全般的要件 5-28
CableLabs コード検証ルート CA 証明書 5-29
CableLabs コード検証 CA 証明書 5-29
製造業者コード検証証明書 5-30
サービス プロバイダー コード検証証明書 5-31
CVC の証明書失効リスト 5-31

CHAPTER 6 CableHome の設定 6-1
ノンセキュア CableHome プロビジョニングのフロー 6-2
CableHome の設定 6-3
Network Registrar の設定 6-3
RDU の設定 6-3
CableHome WAN-Man の設定 6-3
CableHome WAN-Data の設定 6-4
Device Provisioning Engine の設定 6-4

CHAPTER 7 データベース管理 7-1
障害復元力について 7-1
データベース ファイル 7-2
データベース ストレージ ファイル 7-2
データベースのトランザクション ログ ファイル 7-2
自動ログ管理 7-3
各種データベース ファイル 7-3
ディスク容量の要件 7-4
ディスク容量不足の対処方法 7-4

バックアップと回復 7-5
データベースのバックアップ 7-5
データベースの回復 7-6
データベースの復元 7-7
データベースの場所の変更 7-8
RDU データベースの移行 7-8

CHAPTER 8 管理者のユーザ インターフェイスについて 8-1
BACC 管理者のグラフィカル ユーザ インターフェイスへのアクセス 8-2
ログイン 8-2
ログアウト 8-4
管理者のユーザ インターフェイス 8-5
ナビゲーション バー項目の選択 8-5
Main Menu 8-6
Configuration 8-6
Devices 8-6
Servers 8-6
Nodes 8-7
Users 8-7
管理者 8-7
読み取り / 書き込みユーザ 8-7
読み取り専用ユーザ 8-7
前後へのスクロール 8-8

CHAPTER 9 Broadband Access Center for Cable 管理者のユーザ インターフェイスの使用方法 9-1
ユーザ管理 9-2
新規ユーザの追加 9-2
ユーザの修正 9-3
ユーザの削除 9-4
デバイス管理 9-5
Manage Devices ページ 9-5
デバイス管理コントロール 9-6
デバイスの検索 9-8
検索タイプ 9-8
デバイスの詳細の表示 9-9
デバイスの管理 9-14
デバイスの追加 9-14
デバイスの修正 9-15

デバイスの削除 9-15
デバイス構成の再生成 9-16
デバイスの関連付けと関連付け解除 9-16
デバイスのリセット 9-17
デバイスの登録解除 9-17
ノード管理 9-18
ノード タイプの管理 9-18
ノード タイプの追加 9-18
ノード タイプの修正 9-19
ノード タイプの削除 9-19
ノードの管理 9-19
新規ノードの追加 9-19
ノードの修正 9-20
ノードの削除 9-20
ノードに対するノード タイプの関連付けと関連付け解除 9-20
ノードの詳細の表示 9-20
サーバの表示 9-21
Device Provisioning Engine のリスト 9-21
Network Registrar 拡張ポイントのリスト 9-24
プロビジョニング グループのリスト 9-26
Regional Distribution Unit の詳細の表示 9-27

CHAPTER 10 Broadband Access Center for Cable の設定 10-1
サービス クラスの設定 10-2
サービス クラスの追加 10-3
サービス クラスの修正 10-4
サービス クラスの削除 10-5
カスタム プロパティの設定 10-7
デフォルトの設定 10-8
設定オプションの選択 10-8
ATA 186 Defaults 10-8
ATA 188 Defaults 10-10
CableHome WAN Defaults 10-10
CableHome WAN Data Defaults 10-11
CableHome WAN-Man Defaults 10-12
Computer Defaults 10-13
DOCSIS Defaults 10-14
Network Registrar Defaults 10-16
PacketCable Defaults 10-18

RDU Defaults 10-20
System Defaults 10-22
Gateway（xGCP）Control Protocol Defaults 10-24
DHCP 基準の設定 10-25
DHCP 基準の追加 10-25
DHCP 基準の修正 10-26
DHCP 基準の削除 10-26
外部ファイルの管理 10-27
外部ファイルの追加 10-28
外部ファイルの表示 10-29
外部ファイルの置換 10-30
外部ファイルのエクスポート 10-31
外部ファイルの削除 10-31
ライセンス キーの管理 10-32
ライセンスの追加と修正 10-33
Regional Distribution Unit 拡張の管理 10-34
新しいクラスの作成 10-34
RDU カスタム拡張ポイントのインストール 10-34
RDU 拡張の表示 10-35
プロビジョニング データのパブリッシング 10-36
データストアの変更のパブリッシング 10-36
パブリッシング プラグイン設定の修正 10-37
Network Registrar DNS サーバでの SRV レコードの設定 10-38
PacketCable MTA との通信を安全に行うための、RDU および DPE 上での SNMPV3 クローン作成の設定 10-39
キー関連情報の作成およびキーの生成 10-39
FQDN の自動生成 10-40
自動生成される FQDN の形式 10-40
自動生成される FQDN のプロパティ 10-40
FQDN の検証 10-41
FQDN の自動生成の例 10-41

CHAPTER 11 サンプル ユーザ インターフェイスの設定および使用方法 11-1
サンプル ユーザ インターフェイスについて 11-2
サンプル ユーザ インターフェイスの開始および停止 11-2
サンプル ユーザ インターフェイスの設定オプション 11-3
サービス クラス 11-3
無差別モード 11-3
インターネット サービス プロバイダーの選択 11-3

技術者ログインの使用方法 11-3
管理者アクセス レベル 11-4
加入者プロビジョニングの例 11-5
標準の顧客宅内機器登録 11-5
新しいケーブル モデムおよび新しいコンピュータのプロビジョニング 11-5
新しいコンピュータおよび既存のケーブル モデムのプロビジョニング 11-6
既存のコンピュータの ISP の変更 11-6
無差別モードの顧客宅内機器登録 11-6
新しいケーブル モデムおよび新しいコンピュータのプロビジョニング 11-7
既存のケーブル モデムおよび新しいコンピュータのプロビジョニング 11-7
管理者プロビジョニングの例 11-8
アカウントの検索 11-8
アカウント番号による検索 11-8
IP アドレスによる検索 11-8
MAC アドレスによる検索 11-8
アカウントの保守 11-9
新しいアカウントの登録 11-9
サービス クラスの管理 11-9
ケーブル モデムの管理 11-10
コンピュータの管理 11-10
アカウントの削除 11-11
サンプルの sampleui.properties ファイル 11-12

CHAPTER 12 Broadband Access Center for Cable がサポートするツールと高度な概念 12-1
テンプレート ファイルの作成 12-2
テンプレートの文法 12-2
コメント 12-3
インクルード 12-3
オプション 12-4
インスタンス修飾子 12-5
SNMP Varbind 12-6
DOCSIS MIB 12-6
PacketCable MIB 12-7
CableHome MIB 12-7
マクロ変数 12-7
定義済みオプションの符号化タイプ 12-9

BITS 値の構文 12-11
OCTETSTRING の構文 12-11
MIB を使用しない SNMP TLV の追加 12-11
DOCSIS オプションのサポート 12-12
PacketCable オプションのサポート 12-23
ノンセキュア CableHome オプションのサポート 12-23
設定ファイル ユーティリティの使用方法 12-25
設定ファイル ユーティリティの実行 12-25
設定ファイル ユーティリティの使用方法 12-27
バイナリ ファイルのテンプレート ファイルへの変換 12-27
ローカル テンプレート ファイルの解析 12-28
外部テンプレート ファイルの解析 12-29
テンプレート ファイルの解析とユーザ指定の共有秘密情報の追加 12-31
コマンドラインでのマクロ変数の指定 12-32
マクロ変数のデバイスの指定 12-33
バイナリ ファイルへの出力の指定 12-35
ローカル バイナリ ファイルの表示 12-36
外部バイナリ ファイルの表示 12-37
PacketCable BASIC フローの有効化 12-38
RDU ログ レベル ツール 12-39
RDU ログ レベル ツールの使用方法 12-39
RDU ログ レベルの設定 12-40
RDU の現在のログ レベルの表示 12-41
KDC 証明書を管理するための PKCert.sh ツールの使用方法 12-42
PKCert ツールの実行 12-42
KDC 証明書の作成 12-43
KDC 証明書の検証 12-44
changeNRProperties.sh ツールの使用 12-45
Keygen ツールの使用方法 12-47
snmpAgentCfgUtil.sh コマンドの使用方法 12-49
ホストの追加 12-49
ホストの削除 12-50
SNMP エージェント コミュニティの追加 12-50
SNMP エージェント コミュニティの削除 12-51
SNMP エージェントの開始 12-51
SNMP エージェントの停止 12-51
SNMP エージェント リスニング ポートの設定 12-52
SNMP エージェントの場所の変更 12-52

SNMP の連絡先の設定 12-52
SNMP エージェントの設定のリスト 12-53
SNMP 通知タイプの指定 12-53
利用可能なディスク領域を監視するための disk_monitor.sh ツールの使用方法 12-54
MAC アドレスによるデバイスのトラブルシューティング 12-55

APPENDIX A アラートとエラー メッセージ A-1
アラート メッセージ A-1
メッセージ形式 A-1
RDU のアラート A-2
Solaris DPE のアラート A-3
エージェントのアラート A-4
Network Registrar 拡張ポイントのアラート A-5
CCM による RDU エラーメッセージ A-6
[OBJECT_EXISTS] A-6
[RemoveReservation: NOT_FOUND] A-7
[AddReservation: INVALID_PARENT] A-7
[AddReservation: INVALID_SECOND_PARENT] A-7
[AddReservation: FORWARD_FAILED] A-7
事例 1： A-7
事例 2： A-8
[AddReservation: AX_ETIME] A-8
[AddReservation: INVALID_OBJECT] A-8
Selection-criteria exclusion tags will be ignored A-8
[AX_EIO] A-9
[AX_EPIPE] A-9

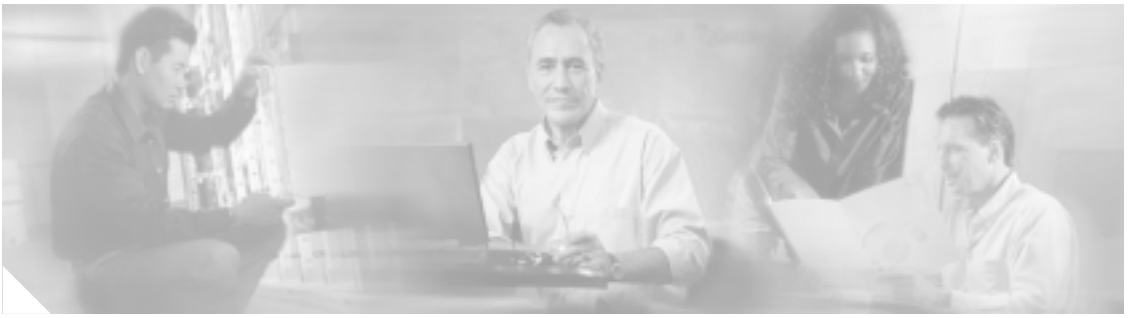
APPENDIX B PacketCable DHCP オプションと BACC プロパティのマッピング B-1
オプション 122 と BACC プロパティの比較 B-2
オプション 177 と BACC プロパティの比較 B-3

APPENDIX C Broadband Access Center for Cable のアプリケーション プログラミング インターフェイスの使用例 C-1
使用例 C-2
固定標準モードでのセルフプロビジョニングされたモデムとコンピュータ C-3
固定標準モードでの新しいコンピュータの追加 C-6
加入者のディセーブル化 C-8

モデムおよびセルフプロビジョニングされたコンピュータの事前プロビジョニング C-10
既存のモデムの修正 C-12
加入者のデバイスの登録解除と削除 C-13
無差別モードでの最初のアクティベーションのセルフプロビジョニング C-16
無差別モードでの 100 個のモデムの一括プロビジョニング C-19
無差別モードでの最初のアクティベーションの事前プロビジョニング C-21
既存のモデムの交換 C-24
無差別モードでの 2 台目のコンピュータの追加 C-25
NAT を使用した最初のアクティベーションのセルフプロビジョニング C-26
NAT を持つモデムの背後への新しいコンピュータの追加 C-29
別の DHCP スコープへのデバイスの移動 C-30
イベントを使用したデバイス削除のロギング C-31
イベントを使用した RDU 接続の監視 C-32
イベントを使用したバッチ完了のロギング C-33
デバイスの詳細情報の取得 C-34
デフォルトのサービス クラスを使用した検索 C-35
ベンダープレフィックスに一致するデバイスの取得 C-37
PacketCable eMTA の事前プロビジョニング C-39
PacketCable eMTA 上での SNMP クローン作成 C-41
PacketCable eMTA の差分プロビジョニング C-43
動的設定ファイルを使用した DOCSIS モデムの事前プロビジョニング C-45
オプティミスティック ロッキング C-46
加入者の帯域幅の一時的なスロットリング C-48
CableHome WAN-Man の事前プロビジョニング C-49
ファイアウォール設定を持つ CableHome C-51
CableHome WAN-Man のデバイス機能の取得 C-53
CableHome WAN-Man のセルフプロビジョニング C-55
リース予約の使用例 C-58
- リース予約機能の影響を受ける API コール C-58
- サービス プロバイダーの IP アドレスを使用したデバイスのオンライン化 C-58
- 予約の削除と再作成 C-60
- 新しいデバイスに対する古いデバイスの IP アドレスの割り当て C-61
- 予約の削除と新しい IP アドレスの割り当て C-62
- 同一の IP アドレスを使用したデバイスのリブート C-63
- BACC からのデバイスの削除 C-64
- BACC が CCM を使用するときに送信済みバッチが失敗する C-65
- BACC が CCM を使用しないときに送信済みバッチが失敗する C-65

GLOSSARY 用語集

INDEX 索引



このマニュアルについて

『*Cisco Broadband Access Center for Cable アドミニストレータ ガイド*』をご利用いただきありがとうございます。ここでは、このマニュアルの後続の章について概要を示し、このマニュアルで使用されているスタイルと表記法を説明します。

(注) このマニュアルは、P.xviii の「関連資料」に挙げられているマニュアルと併せてご利用ください。

この項では、次のトピックについて取り上げます。

- 対象読者（P.xv）
- マニュアルの構成（P.xvi）
- 表記法（P.xvii）
- 関連資料（P.xviii）
- 技術情報の入手方法（P.xix）
- シスコ製品のセキュリティの概要（P.xxi）
- テクニカル サポート（P.xxii）
- その他の資料および情報の入手方法（P.xxiv）

対象読者

『*Cisco Broadband Access Center for Cable アドミニストレータ ガイド*』は、ブロードバンド アクセスにおいて大規模なプロビジョニングを自動化するシステム管理者を対象としています。ネットワーク管理者は、次の項目について熟知している必要があります。

- 基本的なネットワークの概念および専門用語
- ネットワーク管理
- ケーブル ネットワーク

マニュアルの構成

このマニュアルでは、Broadband Access Center for Cable（BACC）の管理方法とメンテナンス方法について説明します。

表 1　各章の概要

第 1 章「Broadband Access Center for Cable の概要」	BACC の機能と特長、および BACC アーキテクチャの詳細を説明します。
第 2 章「Broadband Access Center for Cable システム アーキテクチャ」	Broadband Access Center for Cable 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。
第 3 章「設定のワークフローとチェックリスト」	BACC を設定する際のチェックリストを提供します。
第 4 章「DOCSIS 設定」	BACC DOCSIS の配備を運用に移すためにチェックまたは設定する必要のある機能、および使用可能なツールについて説明します。
第 5 章「PacketCable 音声設定」	PacketCable 音声を配備してサービスを提供するために必要となる、すべての作業について説明します。
第 6 章「CableHome の設定」	ノンセキュア（DHCP）なバージョンの CableHome テクノロジーに関して、適切な CableHome 配備を実現するために必要となる作業について説明します。
第 7 章「データベース管理」	RDU データベースの管理とメンテナンスに関する情報について説明します。他のデータベースと同様に、管理者がデータベースのバックアップ手順と復元手順を理解し、熟知していることが必要です。
第 8 章「管理者のユーザ インターフェイスについて」	BACC へのアクセス方法と、各種のユーザ インターフェイス コンポーネントについて説明します。
第 9 章「Broadband Access Center for Cable 管理者のユーザ インターフェイスの使用方法」	デバイス情報の検索、表示などの管理アクティビティについて説明します。
第 10 章「Broadband Access Center for Cable の設定」	BACC 管理アプリケーションを使用して実行される設定アクティビティについて説明します。
第 11 章「サンプル ユーザ インターフェイスの設定および使用方法」	サンプル ワークフロー ユーザ インターフェイスの概念、使用方法、およびアプリケーションについて説明します。
第 12 章「Broadband Access Center for Cable がサポートするツールと高度な概念」	BACC の設定、メンテナンス、インストールの効率化、配備、使用に役立つツールについて説明します。
付録 A「アラートとエラー メッセージ」	すべての BACC アラート メッセージを挙げ、それぞれについて説明します。
付録 B「PacketCable DHCP オプションと BACC プロパティのマッピング」	PacketCable プロビジョニングで使用される、BACC プロパティと PacketCable DHCP オプションのマッピングを挙げます。
付録 C「Broadband Access Center for Cable のアプリケーション プログラミング インターフェイスの使用例」	プロビジョニング API の最も一般的な使用例を列挙します。この使用例には、サービス プロバイダーの一般的なワークフローをモデル化するときに使用できる擬似コード セグメントなどがあります。
Glossary	このマニュアルで使用されている用語と、説明されている技術に一般的に使用される用語を定義します。

表記法

このマニュアルは、次の表記法を使用しています。

項目	表記法
コマンドおよびキーワード	太字
ユーザが値を指定する変数	イタリック体
セッション情報およびシステム情報の表示出力	`screen` フォント
ユーザが入力する情報	太字の **`screen`** フォント
ユーザが入力する変数	イタリック体の *`screen`* フォント
メニュー項目およびボタン名	太字
本文中のメニュー項目の選択	**Option > Network Preferences**
表中のメニュー項目の選択	Option > Network Preferences

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

関連資料

（注） 初版発行後、印刷物または電子マニュアルのアップデートを行う場合があります。マニュアルのアップデートについては、Cisco.com で確認してください。

BACC 2.7 には次のマニュアルがあります。

- *Release Notes for Cisco Broadband Access for Cable 2.7*
- *Cisco Broadband Access for Cable Installation Guide*
- *Cisco Broadband Access for Cable Administrator's Guide*
- *Cisco Broadband Access for Cable CLI Reference Guide*

DPE-590 をサポートする場合は、次のマニュアルを参照してください。

- *Device Provisioning Engine 590 Recovery CD-ROM Release Notes*
- *Cisco Content Engine 500 Series Hardware Installation Guide*

DPE-2115 をサポートする場合は、次のマニュアルを参照してください。

- *Device Provisioning Engine 2115 Recovery CD-ROM Release Notes*
- Installation and Setup Guide for the Cisco 1102 VLAN Policy Server

注意 このマニュアルは、ポートおよびコネクタの識別と、ハードウェアのインストールにのみ使用してください。このマニュアルにある設定手順は、絶対に行わないでください。

- *Cisco Network Registrar User's Guide*
- *Cisco Network Registrar CLI Reference*

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

次の URL から、シスコ製品の最新資料を入手することができます。

http://www.cisco.com/techsupport

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

シスコの Web サイトの各国語版には、次の URL からアクセスしてください。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

Product Documentation DVD（英語版）

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Product Documentation DVD パッケージでご利用いただけます。Product Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納した、包括的なライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関する複数のバージョンのマニュアルにアクセスし、技術情報を HTML で参照できます。また、この DVD を使用すると、シスコの Web サイトで参照できるのと同じマニュアルに、インターネットに接続せずにアクセスできます。一部の製品については、PDF 版のマニュアルもご利用いただけます。

Product Documentation DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザ（Cisco Direct Customers）の場合、Ordering ツールまたは Cisco Marketplace から Product Documentation DVD（Product Number DOC-DOCDVD=）を発注できます。

Cisco Ordering ツール：

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace：

http://www.cisco.com/go/marketplace/

マニュアルの発注方法（英語版）

2005 年 6 月 30 日以降、Cisco.com 登録ユーザの場合、Cisco Marketplace の Product Documentation Store からシスコ製品の英文マニュアルを発注できるようになっています。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/

Ordering ツールを使用したマニュアル発注も引き続きご利用いただけます。

- Cisco.com（Cisco Direct Customers）に登録されている場合、Ordering ツールから英文マニュアルを発注できます。次の URL にアクセスしてください。

  http://www.cisco.com/en/US/partner/ordering/
- Ordering ツールを使用した英文マニュアル発注の手順については、次の URL を参照してください。

  http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm
- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル（英文のみ）を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告および注意事項の最新のリストには、次の URL からアクセスできます。

http://www.cisco.com/go/psirt

勧告および注意事項がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）フィードにアクセスしてください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合：security-alert@cisco.com（英語のみ）

  緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと見なされます。
- 緊急でない場合：psirt@cisco.com（英語のみ）

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302（英語のみ）
- 1 408 525-6532（英語のみ）

ヒント シスコに機密情報をお送りいただく際には、PGP（Pretty Good Privacy）または互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.*x* から 8.*x* と互換性のある暗号化情報に対応しています。

無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/techsupport

Cisco Technical Support & Documentation Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

(注) Web または電話でサービス リクエストを発行する前に、Cisco Product Identification（CPI）ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support & Documentation Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/contacts

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンラインサービスへのリンクの内容が含まれます。『Packet』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『Packet』は、米国版『Packet』と日本版のオリジナル記事で構成されています。日本語版『Packet』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet/

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『iQ Magazine』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/iqmagazine

  デジタル版には、次の URL からアクセスできます。

  http://ciscoiq.texterity.com/ciscoiq/sample/

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『Internet Protocol Journal』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコシステムズが提供するネットワーキング製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共有できます。次の URL にアクセスしてディスカッションに参加してください。

  http://www.cisco.com/discuss/networking

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Broadband Access Center for Cable の概要

Broadband Access Center for Cable（BACC）は、ブロードバンド サービス プロバイダーがサポートするネットワーク デバイスの設定とプロビジョニングを自動化します。実質的にどのような規模のネットワークにも適合するように拡大、縮小することができる柔軟性があります。BACC は、サービス プロバイダーの急成長に対応できるように設計されています。この製品の対象となるユーザは、ハイブリッド ファイバ ネットワークおよび同軸ケーブルネットワーク上に IP データ、音声、映像を配置する必要があるブロードバンド サービス プロバイダー（マルチプル サービス オペレータを含む）、インターネット サービス プロバイダー、および音声サービス プロバイダーです。BACC は冗長性やフェールオーバーの保護などの重要な機能も提供します。BACC の動作方法を制御できるプロビジョニング アプリケーション プログラミング インターフェイス（API）を利用することにより、新しい環境または既存の環境に BACC を統合することができます。プロビジョニング API により、BACC はデバイスとデバイス構成を登録して、BACC プロビジョニング システム全体を設定することが可能になります。

機能と利点

BACC により、マルチプル サービス オペレータ（MSO）は急速に変化するケーブル データ通信サービスの需要に対応できます。BACC を利用して、そのアーキテクチャに関する次の特徴と利点を実現することができます。

- スケーラビリティの向上
- 分散アーキテクチャ
- 冗長性
- 拡張性

サポート対象の技術

最新バージョンの BACC は以下の技術をサポートします。

- DOCSIS 高速データ通信
- PacketCable 音声サービス
- ノンセキュア PacketCable 音声サービス
- Euro-PacketCable 音声サービス
- ノンセキュア CableHome プロビジョニング

DOCSIS 高速データ通信

Data Over Cable Service Interface Specification は、ケーブルテレビ システム ネットワーク上での高速データの配信に必要なケーブル モデムの機能性を定義します。この機能により、MSO はインターネット常時接続を介してさまざまなサービスを提供することが可能になります。たとえば、ブロードバンド インターネット接続、電話、リアルタイムの対話型ゲーム、ビデオ会議などのサービスを提供できます。

(注)　Broadband Access Center for Cable は DOCSIS 1.0、1.1 および 2.0 のデバイスをサポートします。

PacketCable 音声サービス

PacketCable 音声技術は、双方向ケーブル ネットワーク上での先進的なリアルタイムのマルチメディア サービスの配信を可能にします。PacketCable は、ケーブル モデムがサポートするインフラ上に構築され、IP 電話、マルチメディア会議、対話型ゲーム、全般的なマルチメディア アプリケーションなどさまざまなマルチメディア サービスを可能にします。

PacketCable 音声技術により、ブロードバンド ケーブル アクセス ネットワーク上で基本電話サービスや拡張電話サービスなどの付加的なサービスを効率的かつ経済的な方法で提供することが可能になります。

(注)　最新バージョンの BACC では、PacketCable 仕様のバージョン 1.0 と 1.1 をサポートします。

ノンセキュア PacketCable 音声サービス

ノンセキュア PacketCable 音声サービスは、ノンセキュア バリアントにおいてセキュリティが保持されないという点を除き、標準 PacketCable 音声サービスと同じです。

Euro-PacketCable 音声サービス

Euro-PacketCable サービスは、北米の PacketCable 規格の欧州版に相当します。両者の唯一の大きな違いは、Euro-PacketCable　では異なる　MIB　を使用する点です。詳細については、P.5-7　の「Euro-PacketCable の MIB の設定」を参照してください。

ノンセキュア CableHome プロビジョニング

ノンセキュア CableHome 1.0 プロビジョニング（以下、ホーム ネットワーキング技術と呼ぶ）は、既存の DOCSIS 規格上に構築され、住宅用ブロードバンド サービスの家庭内接続向け「プラグアンドプレイ」環境をサポートします。このような形態のホーム ネットワーキング技術には、CableHome 機能をサポートする DOCSIS 家庭内アクセス デバイスが含まれます。このデバイスはポータル サービスと呼ばれ、家庭のエントリ ポイントとみなされます。

■　サポート対象の技術

CHAPTER 2

Broadband Access Center for Cable システム アーキテクチャ

この章では、この Broadband Access Center for Cable（BACC）リリースで実装されるシステム アーキテクチャについて説明します。この章に示すアーキテクチャは、あくまでも説明のためであり、BACC 製品を使用する場合のバックグラウンドとして示すものです。

アーキテクチャ

ここでは、以下のコンポーネントから成る BACC 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。
  - BACC システムの権限あるデータ格納
  - API の要求を処理するためのサポート
  - デバイス検出エンジン、デバイス構成エンジン、デバイス中断エンジン。デバイスの種類の決定、構成の生成、特定のデバイス中断のサポートのために、インストールされているさまざまな拡張機能を呼び出します。

  詳細については、P.2-4 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。
  - TFTP プロトコル サーバ
  - 構成のキャッシュ
  - 冗長性
  - 時刻サーバ
  - PacketCable プロビジョニング サービス

  詳細については、P.2-6 の「Device Provisioning Engine」を参照してください。
- プロビジョニング グループ

  詳細については、P.2-11 の「プロビジョニング グループ」を参照してください。
- Cisco Network Registrar サーバ。次の機能を提供します。
  - ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）
  - ドメイン ネーム システム（DNS）

  詳細については、P.2-12 の「Cisco Network Registrar」を参照してください。
- Kerberos サーバ。PacketCable MTA を認証します。詳細については、P.2-14 の「鍵発行局」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。
  - SNMP バージョン v2c のサポート
  - SNMP 通知のサポート

  詳細については、P.2-19 の「SNMP エージェント」を参照してください。
- BACC エージェント。次の機能を提供します。
  - すべての重要な BACC プロセスに対する管理モニタリング
  - プロセス自動再開機能
  - BACC 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.2-20 の「BACC エージェント」を参照してください。

登録モード

登録モードによって、サービス プロバイダーは加入者との対話数を制御することができます。登録されたすべてのデバイスを対象に、サービス プロバイダーはデバイスに対する変更があれば処理するように準備する必要があります。そのため、背後に登録解除されたコンピュータのあるケーブル モデムを 100 台登録する作業と、背後に登録済みのコンピュータが大量に存在する可能性のあるケーブル モデムを 100 台登録する作業には、大きな違いがあります。この理由により、サービス プロバイダーは登録モードを標準モード、無差別モード、およびローミング モードから慎重に選択する必要があります。

標準モード

標準モード（固定モードとも呼ぶ）で動作しているときに、コンピュータを別のケーブル モデムの背後に移すと、そのコンピュータにはプロビジョニング解除されたアクセス権が与えられます。

無差別モード

デバイスだけが登録されます。DHCP サーバは別のデバイスの背後で動作するデバイスのリース情報を維持します。登録されたデバイスの背後にあるすべてのデバイスは、ネットワーク アクセスを受け付けます。

ローミング モード

ローミング モードでは、登録されたデバイスが他のすべての登録済みデバイスの背後にあるサービス クラスを受け付けることができます。これによって、たとえば、場所を移動しながらラップトップを使用し、複数のケーブル モデムからサービスを入手することができます。

混在モード

無差別モードとローミング モードを混在させて、2 つの別個のモードとして使用し、同時に共存させることもできます。

Regional Distribution Unit

RDU は BACC プロビジョニング システムの主要サーバです。RDU は以下の機能も提供します。

- デバイス構成生成の管理
- BACC システムの権限あるデータ格納
- デバイス中断
- すべてのアプリケーション プログラミング インターフェイス（API）の要求が通過する情報センター機能
- BACC 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。また、RDU は以下のこともサポートします。

- API によるデータ アクセスと操作
- スケーラビリティのための DPE への構成の分配
- 外部クライアント、オペレーション サポート システム（OSS）、API によるその他のプロビジョニング関連の機能性

RDU の概念については、次のセクションで説明します。

- デバイス構成の生成（P.2-4）
- サービス レベル選択（P.2-5）
- Regional Distribution Unit のフェールオーバー（P.2-5）

（注） RDU は、DPE および Network Registrar 拡張の名前を、それらが RDU に接続するインターフェイスによって判別します。つまり、DPE または Network Registrar 拡張の名前は、RDU マシンが判断した名前になります。このため、RDU でその名前を解決（両方向）できる必要があります。

デバイス構成の生成

デバイスはブート時に BACC 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。デバイス構成には、DHCP IP アドレスの選択、帯域幅、データ レート、フロー制御、通信速度、サービス レベルなど、顧客が必要とするプロビジョニング情報を含めることができます。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がインストールされ、ブート操作が実行されると、適切な技術のデフォルト設定が BACC から入手され、DHCP または TFTP によってデバイスに送信されます。サポートされる技術ごとに、デフォルトの設定を変更することができます。

サービス レベル選択

サービス レベル選択拡張ポイントは、RDU が使用する基準を決定し、デバイス構成の生成時に使用される基準を RDU に通知します。RDU は各デバイスについてこの情報を RDU データベースに保存します。デバイスは 1 つの基準セットを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、選択された基準を検索して使用します。したがって、RDU 自動再生成は 2 つ目の基準セットが使用されることを認識するので、その基準に何らかの変更が発生した場合にはデバイス構成が再生成されます。

サービス レベル選択拡張ポイントは、さまざまなテクノロジー デフォルト ページで入力されます（詳細については、P.10-8 の「デフォルトの設定」を参照）。これらは拡張のカンマ区切りリストとして入力され、その特定の拡張ポイント向けの拡張として使用できるオブジェクトの作成をインスタンス化します。これらのプロパティにはデフォルトで、ゼロまたは組み込み拡張の 1 つが入力されます。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、これらの拡張は修正しないでください。

Regional Distribution Unit のフェールオーバー

最新バージョンの Broadband Access Center for Cable では、1 回のインストールにつき 1 つの RDU をサポートします。フェールオーバーに対応するには、お持ちのハードウェアの冗長システムをご利用になるか、ホットスワップ機能を持つ同様のシステムをご用意ください。

Device Provisioning Engine

Cisco Device Provisioning Engine（DPE）は RDU と通信して、デバイスに構成を割り当てます。各 DPE は最大 100 万個のデバイスの情報をキャッシュします。冗長性とスケーラビリティを確保するために複数の DPE を利用することができます。

DPE は、デバイスの設定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 Cisco 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 が単一の DHCP サーバと通信することができます。

DPE は以下のアクティビティを管理します。

- 最終段階のデバイス構成の生成（DOCSIS タイムスタンプなど）
- 組み込み TFTP サーバを介した設定ファイルのやり取り
- Cisco Network Registrar との統合
- 時刻プロトコル サーバ
- 音声技術プロビジョニング サービス

Device Provisioning Engine の種類

最新バージョンの BACC では、従来のハードウェア デバイス（DPE-590 または DPE-2115 のいずれか）と、ソフトウェア限定の Solaris DPE の 2 種類の DPE がサポートされます。詳細については、P.2-6 の「ハードウェア Device Provisioning Engine」および P.2-7 の「Solaris Device Provisioning Engine」を参照してください。

ここでは、さまざまな種類の DPE の他、以下の主要な DPE コンポーネントについて説明します。

- DPE ライセンス キー（P.2-7）
- TACACS+ および DPE 認証（P.2-7）
- DPE サーバの割り当て（P.2-8）
- TFTP サーバ（P.2-9）
- プロビジョニング グループ（P.2-11）

ハードウェア Device Provisioning Engine

最新バージョンの BACC では、DPE-590 および DPE-2115 ハードウェア Device Provisioning Engine をサポートします。デバイス自体、ポート、コネクタ、および背面パネルのコンポーネントの詳細については、次のマニュアルを参照してください。

- DPE-590 の場合は、『*Cisco Content Engine 500 Series Hardware Installation Guide*』を参照してください。次の URL からアクセスできます。

  www.cisco.com/en/US/products/hw/contnetw/ps761/products_installation_guide_book09186a00800801e0.html

- DPE-2115 の場合は、『*Installation and Setup Guide for the Cisco 1102 VLAN Policy Server*』を参照してください。次の URL からアクセスできます。

  www.cisco.com/en/US/products/sw/secursw/ps2136/products_installation_and_configuration_guide_book09186a00801f0d02.html

（注） DPE-2115 と Catalyst スイッチとの間のインターフェイス リンクが中断されるときは、データ トラフィックが流れる前にデフォルトの 30 秒遅延が発生しています。

Solaris Device Provisioning Engine

Solaris DPE は、Solaris 8 または Solaris 9 オペレーティング システムで動作するコンピュータに BACC 製品の当該部分がインストールされているという点を除き、ハードウェア DPE と同じように機能します。ごく少数の例外を除き、ハードウェアでも Solaris DPE でも、同じコマンドライン インターフェイス CLI が使用されます。各 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 for Cable Command Line Interface Reference*』を参照してください。

DPE ライセンス キー

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、そのような新しい DPE は登録されず、拒否されます。一方、既存の有効な DPE はオンラインのままとなり、任意で RDU に再登録されます。

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

RDU に登録する DPE のライセンス数には、バージョン番号または種類に関係なく、ハードウェアと Solaris DPE が含まれます。BACC ラボ インストールの一部として利用されるものも含まれます。詳細については、『*Broadband Access Center for Cable Installation Guide*』を参照してください。

ライセンスの追加、評価ライセンスの拡張、評価ライセンスの満了のいずれかによってライセンスを変更するときは必ず、その変更がすぐに有効になります。

RDU データベースから DPE を削除すると、ライセンスは解放されます。

削除された DPE は、対応するすべてのプロビジョニング グループから除外され、DPE が利用不可能となったことが Network Registrar のすべての拡張部分に通知されます。そのため、過去に削除された DPE が再登録されると、再びライセンスが与えられたとみなされ、RDU から再び削除されるまで、あるいはライセンスが満了するときまでその状態が続きます。

RDU を介してライセンスが与えられていない DPE は管理者のユーザ インターフェイスには表示されません。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（dpe.log と rdu.log）を調べる必要があります。

BPR 2.0.x または BACC 2.5 のいずれかを実行する削除済みもしくはライセンスなしのハードウェア DPE は、常に RDU への登録を試みます。これは、上記のバージョンのソフトウェアを実行するデバイスにとって正常な動作であり、拒否された登録はすべて RDU ログ、およびこの状況を識別する SYSLOG アラートの生成に記録されます。

TACACS+ および DPE 認証

Terminal Access Controller Access Control System plus（TACACS+）は TCP ベースのプロトコルで、多数のネットワーク デバイスを対象とする中央集中型のアクセス コントロールと、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することができます。各ユーザ名とログインおよびイネーブル 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 2-1 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 2-1　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 Command Line Interface（CLI; コマンドライン インターフェイス）を使用して設定される多数のプロパティを使用します。これらの TACACS+ 関連の CLI コマンドについては、『*Cisco Broadband Access Center for Cable Command Line Reference*』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 FQDN を、デフォルト値以外を使用して指定する必要があります。

管理者は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することができます。

- 各 TACACS+ サーバの共有秘密キー。このキーは DPE と TACACS+ サーバとの間のデータ暗号化に使用されます。特定の TACACS+ サーバの共有秘密情報を省略するように選択した場合、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。これは、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です。
- TACACS+ サーバのリトライ回数。これは、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みる回数を示します。

(注) これらのコマンドは、ハードウェア DPE と Solaris DPE の両方で使用できます。ハードウェア DPE ではコンソール モードだけが使用できます。

DPE サーバの割り当て

BACC は複数の DPE をサポートします。それらの DPE はデバイス、DHCP フェールオーバー構成、および RDU と通信します。インストール中に、以下のように DPE の割り当てを行う必要があります。

- 1 つ以上のデバイス論理グループまたはプロビジョニング グループに責任を負うように DPE を割り当てる。
- RDU の IP アドレスとポート番号

DPE の主な目的は、顧客のデバイスの電源投入またはリブートのたびに、そのデバイスに構成を送信することです。これを迅速に実行するために、DPE は各デバイスの構成のコピーをローカル キャッシュ データベースに保存します。

(注) DPE は単一のプロビジョニング グループに割り当てる必要があります。

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要求元から DOCSIS 設定ファイルを含むファイル要求を受信します。その後、このサーバは要求元にファイルを送信します。

TFTP サーバは、ローカル ファイル システム アクセスに利用されるホーム ディレクトリに配置されます。ローカル ファイルは BACC_DATA/dpe/tftp ディレクトリに格納されます。

デフォルトでは、TFTP サーバは TFTP 読み取り用のキャッシュだけに表示されます。ただし、tftp allow-read-access コマンドが実行された場合は、TFTP サーバはキャッシュを確認する前にまずローカル ファイル システムを確認します。ファイルがローカル ファイル システムにある場合は、そこから読み取られます。そうでない場合は、TFTP サーバはキャッシュを確認します。そこにファイルがあれば、サーバはそれを利用します。そこにファイルがない場合は、サーバはファイル要求を RDU に送信します。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。

BACC はローカル ファイル システムへの書き込みだけを許可します。DPE キャッシュへの書き込みは一切許可しません。tftp allow-write-access DPE CLI コマンドを実行すると、BACC は TFTP ホーム ディレクトリへの書き込みを許可します。デフォルトでは、ディレクトリまたは上書きファイルの作成は許可されません。これを変更するには、tftp allow-create-dirs コマンドまたは tftp allow-override コマンドを実行します。

DOCSIS 共有秘密情報

動的 DOCSIS 設定ファイルについてのみ、BACC を使用して、複数の異なる DOCSIS Shared Secret（DSS; DOCSIS 共有秘密情報）を異なる CMTS に属するデバイス上で定義することができます。このように、信頼のおけない共有秘密情報により、信頼のおけない CMTS の数は限られたものとなり、配置全体のすべての CMTS が対象となることはありません。

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、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する必要があります。

注意　単一のプロビジョニング グループ内で複数の DSS を設定すると、場合によっては CMTS のパフォーマンスが低下する可能性があります。これは、実質的に BACC には何の影響もありません。

共有秘密情報は、クリア テキストまたは IOS 暗号化形式で入力できます。

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、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。

対応する CLI 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 から設定す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、または管理目的で共有秘密情報を変更する場合には、CLI コマンドの show running config を実行し、表示された設定から DOCSIS 共有秘密情報の行を DPE 設定にコピー アンド ペーストして戻すことができます。このようにして、Cisco CMTS での入力内容を DPE CLI にコピーすることができます。詳細については、『*Cisco Broadband Access Center for Cable Command Line Reference*』を参照してください。

（注） 上で説明したように共有秘密情報を変更するには、CMTS が V 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 を変更する必要があるときは、次の作業を行う必要があります。

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 および 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 上で信頼のおけない DSS をセカンダリ DSS に変更します。これにより、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 モデムで登録を続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、CMTS の信頼のおけないセカンダリ共有秘密情報を CMTS 設定から削除します。

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、2 つ以上の DPE と DHCP サーバのフェールオーバー ペアから成る地域別のサーバのグループ化を目的として設計されています。この設計により、最高 100 万個のデバイスのプロビジョニングの必要性に対処することができます。デバイスの数が 100 万個を上回る場合は、追加のプロビジョニング グループを配置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される必要はありません。中央の NOC に簡単に配置することができます。

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 グループは任意の数の DPE に対応できます。DHCP サーバから要求が入ってくると、その要求はプロビジョニング グループの 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 が安定した状態にある間、このアフィニティは保たれます。特定のデバイスは通常同一の DPE に割り当てられるため、負荷がかかる Kerberos チケット再発行処理を行わずに済みます。

Cisco Network Registrar

Network Registrar には、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）およびドメイン ネーム システム（DNS）の機能があります。完全な管理ユーザ インターフェイスがあり、カスタマイズされた BACC 設定画面と組み合せれば、大規模な企業管理システム内で利用できます。

(注)　Network Registrar の詳細については、『*Network Registrar User's Guide*』、『*Network Registrar CLI Reference*』、および『*Network Registrar Installation Guide*』を参照してください。

ダイナミック ホスト コンフィギュレーション プロトコル

DHCP サーバは、TCP/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遂行する機能の多くを実行します。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可動性が高まり、管理しやすくなります。

DHCP フェールオーバーを使用すると、DHCP サーバ ペアの一方が機能を停止した場合に他方が処理を引き継げるようにサーバが機能します。サーバのペアをプライマリ サーバとバックアップ サーバと呼びます。通常の状況では、プライマリ サーバがすべての DHCP 機能を実行します。プライマリ サーバが使用できなくなった場合、バックアップ サーバが処理を引き継ぎます。このようにして DHCP フェールオーバーは、プライマリ サーバの障害時に DHCP サービスの利用停止を防ぎます。

ドメイン ネーム システム

ドメイン ネーム システム（DNS）サーバは、IP アドレス、ホスト名、ルーティング情報など、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との変換のためにその情報を利用します。このように 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。

DNS ディレクトリ サービスには次のものが含まれます。

- DNS データ
- DNS サーバ
- サーバからデータを呼び出すためのインターネット プロトコル
- 音声プロビジョニングのためのダイナミック DNS

リース予約

BACC リース予約は、Network Registrar の Central Configuration Management（CCM）と連動して、プロビジョニング時にデバイスに固定 IP アドレスを割り当てます。

新しいデバイスのプロビジョニング時に、BACC は IP アドレスが指定されているかどうかを判別し、アドレスが有効な IP アドレスであることを確認する Network Registrar サーバを判別します。確認後に、リース予約機能により、Network Registrar CCM を使用してデバイスの予約が作成されます。

リース予約は BACC でサポートされるすべてのテクノロジーで動作します。次の機能があります。

- BACC グラフィカル ユーザ インターフェイスを使用した IP アドレス予約の追加および削除が可能になります。詳細については、P.9-14 の「デバイスの管理」を参照してください。
- すでに使用されている IP アドレスを予約しようとして発生したすべてのエラー、または予約が CCM サーバから削除されているかどうかについて報告します。

（注） リース予約が適切に動作するためには、ライセンスを取得した CCM サーバが存在する CNS Network Registrar バージョン 6.1.2.3 をネットワークにインストールしておく必要があります。

BACC にリース予約を実装する前に、CCM アドレス、ポート、ユーザ名、およびパスワードを設定する必要があります。これらのパラメータは RDU Defaults ページから設定します。変更は動的に行われ、入力後すぐ有効になります（これらの構成パラメータについては、P.10-20 の「RDU Defaults」を参照）。

（注） リース予約機能はデフォルトでは無効に設定され、所定の時間 CCM にアクセスできないときはタイムアウトになります。

鍵発行局

Key Distribution Center（KDC; 鍵発行局）は、MTA を認証してセキュリティ チケットを与えるのに利用される認証サーバです。

(注)　KDC はマルチプロセッサ コンピュータでサポートされます。

デフォルトの KDC のプロパティ

KDC には、BACC のインストール中に <BACC_HOME>/kdc/solaris/kdc.ini プロパティ ファイルに読み込まれるデフォルトのプロパティがいくつかあります。このファイルを編集し、操作要求に応じて値を変更することができます。変更を行った後、プロパティ ファイル、キー、または証明書の変更を有効にするには KDC を再起動する必要があります。デフォルトでは、プロパティは以下のように設定されています。

- interface address：Kerberos 着信メッセージのために KDC に監視させる必要があるローカル イーサネット インターフェイスの IP アドレスです。次に例を示します。

  ```
  interface address = 10.10.10.1
  ```

- FQDN：KDC がインストールされている Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を識別します。次に例を示します。

  ```
  FQDN = kdc.cisco.com
  ```

(注)　インストール中に、KDC Realm Name 画面から interface address と FQDN を入力します。詳細については、『*Broadband Access Center for Cable Installation Guide*』を参照してください。

- maximum log file size：KDC が一連のログファイルを生成します。このプロパティはログファイルの最大サイズ（キロバイト）を指定します。そのため、最新ファイルがこの最大サイズに達したときに限り、KDC は新しいログファイルを作成します。次に例を示します。

  ```
  maximum log file size = 1000
  ```

- *n* saved log files：KDC が保存する古いログファイルの数を定義します。デフォルト値は 7 ですが、必要に応じた数を指定することができます。次に例を示します。

  ```
  n saved log files = 10
  ```

- log debug level：ログファイルのロギング レベルを指定します。

  ```
  log debug level = 5
  ```

- minimum (maximum) ps backoff：BACC が FQDN-REQUEST に応答するまでの KDC の最短（または最長）待ち時間を 0.1 秒単位で指定します。次に例を示します。

  ```
  minimum ps backoff = 150
  ```

上記の例の値を使用すると、例に挙げた INI ファイルに含まれるデータは例 2-1 と同じになります。

例 2-1　サンプル KDC INI 設定ファイル

```
interface address =  10.10.10.1
FQDN = kdc.cisco.com
maximum log file size = 1000
n saved log files = 10
log debug level = 5
minimum ps backoff = 150
maximum ps backoff = 300
```

最短および最長のチケット継続時間を設定すると、配置中に発生する可能性がある過剰な数のチケット要求を効果的に取り除くことができます。大半の配置が従来の勤務時間中に行われ、過度の負荷がパフォーマンスに悪影響を及ぼす場合があることを考えると、これは有益なことです。

(注) チケット継続時間を短くすると、MTA は頻繁に KDC を認証しなければならなくなります。この方法により電話エンドポイントの認証に対する管理が強まる一方、KDC に対するメッセージの負荷がはるかに重くなり、ネットワークのトラフィックも増加します。たいていの場合、デフォルトの設定は適切であり、変更は必要ありません。

- maximum ticket duration：KDC が生成するチケットの最長継続期間を定義します。デフォルトの単位は「時間」ですが、**m** または **d** を追加すると、それぞれ単位が「分」、「日」に変更されます。

  デフォルトの値は 168（7 日間）です。これは PacketCable のセキュリティの仕様を満たすのに必要な継続時間であるため、この値を変更しないことをお勧めします。次に例を示します。

  ```
  maximum ticket duration = 168
  ```

- minimum ticket duration：KDC が生成するチケットの最短継続期間を定義します。デフォルトの単位は「時間」ですが、**m** または **d** を追加すると、それぞれ単位が「分」、「日」に変更されます。

  デフォルトの値は 144（6 日間）です。この値を変更しないことをお勧めします。次に例を示します。

  ```
  minimum ticket duration = 144
  ```

Euro-PacketCable のサポート

Key Distribution Center（KDC; 鍵発行局）コンポーネントは、Euro-PacketCable（tComLabs）証明書チェーンをサポートします。例 2-2 に Euro-PacketCable 対応の KDC 設定ファイルの例を示します。

例 2-2　Euro-PacketCable 対応の KDC 設定ファイルの例

```
[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
```

KDC 証明書

KDC の認証に使用される証明書は BACC に同梱されていません。Cable Television Laboratories Inc.（CableLabs）から必要な証明書を入手する必要があります。その証明書の内容は MTA にインストールされているものと一致しなければなりません。詳細については、P.12-42 の「KDC 証明書を管理するための 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ないと、KDC は機能しません。

KDC ライセンス

シスコの代理店から KDC ライセンスをご入手のうえ、適切なディレクトリにインストールしてください。

KDC ライセンス ファイルをインストールするには、以下の手順を実行します。

ステップ 1　ライセンス ファイルを入手します。

ステップ 2　ライセンス ファイルを <BACC_HOME>/kdc ディレクトリにコピーします。

注意　ASCII ファイルとしてコピーしないように注意してください。このファイルには、ASCII 転送中に不要な変更が行われやすいバイナリ データが含まれています。

ステップ 3　KDC ライセンス ファイルの名前が **bacckdc.license** ではない場合、ファイル名を **bacckdc.license** に変更します。

ステップ 4　/etc/init.d ディレクトリから **bprAgent restart kdc** コマンドを実行して、KDC サーバを再起動し、変更を有効にします。

（注）　KDC ライセンス ファイルは転送プロセスにより損傷を受ける可能性があるため、異なるオペレーティング システム間でコピーすることはできません。

複数領域のサポート

BACC KDC は複数領域の管理をサポートします。

追加領域を設定するには、次の手順に従います。

ステップ 1　KDC 証明書が格納されているディレクトリを見つけます。

ステップ 2　そのディレクトリに、目的の領域名と一致する名前のサブディレクトリを作成します。このサブディレクトリは大文字だけを使用して作成する必要があります。

ステップ 3　このディレクトリに、領域の KDC 証明書および秘密鍵を配置します。

ステップ 4　新しい領域が KDC 証明書と同じサービス プロバイダーにチェーン化されていない場合は、証明書ディレクトリ内の証明書とは異なる、より高いレベルの追加証明書をすべて含めます。ただし、すべての領域は同じ証明書チェーンをルートとする必要があるため、KDC のインストールごとに 1 つのロケール（PacketCable、Euro-PacketCable）だけがサポートされます。

（注）　指定された任意の DPE は単一の領域にサービスを提供するように制限されます。

BACC MIB

Broadband Access Center for Cable はさまざまな MIB をサポートします。次の MIB があります。

- CISCO-BACC-DPE-MIB：P.2-19 の「MIB のサポート」を参照してください。
- CISCO-APPLIANCE-MIB：P.2-19 の「MIB のサポート」を参照してください。
- CISCO-BACC-RDU-MIB：P.2-19 の「SNMP エージェント」を参照してください。
- CISCO-BACC-SERVER-MIB：すべての BACC サーバに共通する管理対象オブジェクトを定義します。この MIB は、同一のデバイスにインストールされている複数の BACC サーバのモニタリングをサポートします。サーバの状態が変化するたびに `ciscoBaccServerStateChanged` 通知が生成されます。

表 2-2 に、インストールのタイプに応じた BACC MIB のサポートをまとめます。各インストール タイプの説明については、『*Cisco Broadband Access Center for Cable Installation Guide*』を参照してください。

表 2-2　BACC でサポートされる MIB

インストールのタイプ	サポート対象の MIB
Solaris DPE	CISCO-BACC-SERVER-MIB
	CISCO-BACC-DPE-MIB
ハードウェア DPE	RFC1213 - MIB II
	CISCO-APPLIANCE-MIB
	CISCO-BACC-SERVER-MIB
	CISCO-BACC-DPE-MIB
RDU	CISCO-BACC-SERVER-MIB
	CISCO-BACC-RDU-MIB

BACC エージェント

この項では、BACC エージェントの機能とエージェントが重要な理由について説明します。続いて、エージェントの使用および理解に必要なすべての詳細情報について説明します。対象のエージェントは次のとおりです。

- SNMP エージェント（P.2-19）
- BACC エージェント（P.2-20）

SNMP エージェント

BACC では、DPE サーバおよび RDU サーバについて基本的な SNMP v2 ベースのモニタリングがサポートされます。BACC SNMP エージェントでは SNMP 通知と SNMP トラップの両方がサポートされます。snmp-server CLI コマンドを使用して DPE に SNMP エージェントを設定し、SNMP 設定 CLI コマンドを使用して RDU に SNMP エージェントを設定できます。

SNMP 設定コマンドライン ツールの詳細については P.12-49 の「snmpAgentCfgUtil.sh コマンドの使用方法」、DPE CLI の詳細については『*Cisco Broadband Access Center for Cable Command Line Reference*』を参照してください。

MIB のサポート

RFC 1213（MIB-II）の他、SNMP エージェントは CISCO-CW-APPLIANCE-MIB もサポートします。この MIB はハードウェア DPE にインストールされたソフトウェア コンポーネントの管理対象オブジェクトを定義します。MIB は CPU、メモリ、およびディスクの使用率を監視し、使用率が特定のしきい値を上回ると通知を生成します。通知は、イネーブルとディセーブルを選択して設定できます。リソースの使用率は定期的にポーリングされ、連続する 2 つのデータ ポイントの平均がしきい値を上回ると、通知が生成されます。

SNMP エージェントは CISCO-BACC-DPE-MIB もサポートします。この MIB は Solaris DPE にインストールされたソフトウェア コンポーネントの管理対象オブジェクトを定義します。DPE は、すべてのサポート対象デバイスで使用されるデバイス構成および設定ファイルのローカル キャッシュを管理します。この MIB によって、TFTP サーバおよび ToD サーバのエントリなど、いくつかの基本 DPE 設定および統計情報が提供されます。

SNMP エージェントでは、Cisco NMS アプリケーションの状態の通知と関連オブジェクトを定義する CISCO-NMS-APPL-HEALTH-MIB がサポートされます。そのような通知は、NMS アプリケーションの状態を知らせるために OSS/NMS に送信されます。たとえば、開始、中止、機能不全、使用中、またはアプリケーションの何らかの異常終了などの状態を通知します。デフォルトの MIB として MIB-II が使用されます。

SNMP エージェントでは、RDU サーバの起動、シャットダウン、障害、または終了状態の変化を知らせるために cnaHealthNotif トラップが生成されます。

SNMP エージェントでは、RDU の管理対象オブジェクトを定義する CISCO-BACC-RDU-MIB がサポートされます。この MIB には、RDU と DPE 間、および RDU と Network Registrar 間の統計情報を定義する管理対象オブジェクトも含まれます。

（注）　これらの MIB は <BACC_HOME>/rdu/mibs ディレクトリにあります。

BACC エージェント

BACC エージェントは、すべての BACC 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。

BACC エージェントは、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

監視対象のアプリケーションが機能しなくなると、自動的に再開されます。何らかの理由で再開プロセスも機能しない場合は、BACC エージェント サーバは所定の時間待機してから再び再開を試みます。

(注) Network Registrar の拡張を監視するには、BACC エージェントおよび SNMP エージェントを利用する必要はありません。

再開を試みる間隔は 5 分に達するまで指数関数的に長くなります。その後、プロセスの再開が成功するまで 5 分間隔で試みられます。再開の成功の 5 分後に、期間は再び自動的に 1 秒にリセットされます。

次に例を示します。

- プロセス A が失敗します。
- BACC エージェント サーバはプロセスの再開を試み、1 回目の再開が失敗します。
- BACC エージェント サーバは 2 秒間待機してからプロセスの再開を試み、2 回目の再開が失敗します。
- BACC エージェント サーバは 4 秒間待機してからプロセスの再開を試み、3 回目の再開が失敗します。
- BACC エージェント サーバは 16 秒間待機してからプロセスの再開を試み、4 回目の再開が失敗します。

BACC エージェント コマンドライン

BACC エージェントは、システムのブートアップのたびに自動的に起動します。そのため、このエージェントは、制御対象として設定されている BACC システム コンポーネントも起動します。BACC エージェントは単純なコマンド ライン インターフェイスからも制御できます。このためには、/etc/init.d ディレクトリから bprAgent コマンドを実行します。

表 2-3 は、BACC エージェントに利用できる CLI コマンドを示します。CLI は etc/init.d ディレクトリから実行できます。

表 2-3　BACC コマンドライン インターフェイス

コマンド	説明
bprAgent start	すべての監視対象プロセスを含む BACC エージェントを開始します。
bprAgent stop	すべての監視対象プロセスを含む BACC エージェントを中止します。

表 2-3　BACC コマンドライン インターフェイス （続き）

コマンド	説明
bprAgent restart	すべての監視対象プロセスを含む BACC エージェントを再起動します。
bprAgent status	すべての監視対象プロセスを含む BACC エージェントの状態を入手します。
bprAgent start <*process-name*>	特定の 1 つの監視対象プロセスを開始します。<*process-name*> 値がそのプロセスを識別します。
bprAgent stop <*process-name*>	特定の 1 つの監視対象プロセスを中止します。<*process-name*> 値がそのプロセスを識別します。
bprAgent restart <*process-name*>	特定の 1 つの監視対象プロセスを再開します。<*process-name*> 値がそのプロセスを識別します。
bprAgent status <*process-name*>	特定の 1 つの監視対象プロセスの状態を入手します。<*process-name*> 値がそのプロセスを識別します。

（注）　表 2-3 の中の <*process-name*> は、rdu プロセス、kdc プロセス、dpe プロセス、SnmpAgent プロセス、jrun プロセス（管理者およびサンプル ユーザ インターフェイスを実行する）のいずれかになります。CLI プロセスは Lab および DPE のインストール時にも監視されます。

（注）　RDU は Solaris 環境で動作します。Solaris **reboot** コマンドが利用されるたびに正常にシャットダウンしないことがあります。システムを終了するための優先コマンドは、**shutdown** です。

ロギング

イベントのロギングは DPE と RDU の両方で実行されます。まれに 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 ディレクトリに配置され、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 TAC 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。

Regional Distribution Unit のログ

RDU には次の 2 つのログがあり、BACC_DATA/rdu/logs ディレクトリで保持されます。

- rdu.log：設定されたデフォルト レベルを持つ RDU イベントがすべて記録されます。デフォルトのログ レベルの設定方法については、P.12-40 の「RDU ログ レベルの設定」を参照してください。
- audit.log：BACC の設定または機能に対して行われた高いレベルの変更がすべて記録されます。このような変更を行ったユーザも記録されます。

Device Provisioning Engine のログ

DPE では dpe.log ファイルが BACC_DATA/dpe/logs ディレクトリで保持されます。このファイルには、設定されたデフォルト レベルを持つすべてのイベントも記録されます。システム障害が連続して起こるなど、DPE で破局的な障害が発生した場合、破局的なエラーは rdu.log ファイルにも記録されます。

DPE サーバで PacketCable がイネーブルになっている場合、DPE では詳細なデバッグ情報を提供するために SNMPService.logyyy.log ログ ファイルが使用されます。ファイルの内容を表示するには、DPE の CLI コマンドである **show packetcable snmp log** を使用します。このファイルも BACC_DATA/dpe/logs ディレクトリにあります。PacketCable コマンドの使用方法については、『*Cisco Broadband Access Center for Cable Command Line Reference*』を参照してください。

(注) PacketCable ログ メッセージは dpe.log ファイルに送信され、詳細な SNMP デバッグは SNMPService.logyyy.log ファイルに送信されます。

ログのレベルおよび構造

ログ ファイルの構造は、ここで説明するとともに、例 2-3 で例示しています。ログ ファイルの構造に含まれる情報は次のとおりです。

- Domain Name：ログ ファイルが生成されたコンピュータの名前。
- Date and Time：メッセージがログに記録された日時。ここには、該当するシステムの時間帯も示されます。
- Facility：システムを識別します（この場合は BACC）。
- SubFacility：BACC のサブシステムまたはコンポーネント。
- Severity Number：ログの問題を処理するときの緊急性を識別するために使用される重大度。ログ システムでは、7 段階のログ レベルが定義されます。次のログ レベルの設定方法については、P.2-23 の「ログ レベルの設定」を参照してください。
  - 0：緊急。システムが不安定な状態です。
  - 1：アラート。すぐに対応が必要です。
  - 2：クリティカル。クリティカルな状態が存在します。

— 3：エラー。エラー状態が存在します。
— 4：警告。警告状態が存在します。
— 5：通知。通常ですが、重大な状態が存在します。
— 6：情報。情報メッセージのみです。

(注)　デバッグとして知られるもう 1 つのレベルは、シスコでデバッグの目的にのみ使用されます。Cisco TAC で指示された場合を除き、このレベルは使用しないようにしてください。

- Message ID：メッセージ テキストの固有な識別子。
- Message：実際のログ メッセージ。

(注)　ロギングの詳細については、P.12-39 の「RDU ログ レベル ツール」を参照してください。

ログ レベルの設定

RDU と DPE のログ レベルは、いずれも特定の要件に合せて設定できます。たとえば、RDU のログ レベルを「警告」、DPE のログ レベルを「アラート」に設定できます。

ログ メッセージは、特定のイベントの発生に基づいて記述されます。イベントが発生するたびに、該当するログ メッセージとログ レベルが割り当てられます。ログ レベルが設定したレベル以下であれば、メッセージがログに書き込まれます。レベルが設定した値より高い場合、メッセージはログに書き込まれません。

たとえば、ログ レベルが 4（警告）に設定されているとします。ログ ファイルには、ログ レベルが 4 以下に設定されているイベントの生成するメッセージがすべて書き込まれます。ログ レベルが 6（情報）に設定されている場合、ログ ファイルにはすべてのメッセージが書き込まれます。したがって、ログ レベルを高く設定するほど、ログ ファイルのサイズは大きくなります。

例 2-3　ログ ファイルのサンプル

Domain Name	Data and Time	Facility	Sub-facility	Security Level	Msg ID	Message
BACC1:	2005 3 16 03:06:11 EST:	BPR-	RDU-		0236:	BPR Regional Distribution Unit starting up
BACC1:	2005 3 16 03:06:15 EST:	BPR-	RDU-	5	0566:	Initialized API defaults
BACC1:	2005 3 16 03:06:15 EST:	BPR-	RDU-	5	0567:	Initialized CNR defaults
BACC1:	2005 3 16 03:06:15 EST:	BPR-	RDU-	5	0568:	Initialized server defaults
BACC1:	2005 3 16 03:06:18 EST:	BPR-	RDU-	5	0570:	Initialized DOCSIS defaults
BACC1:	2005 3 16 03:06:18 EST:	BPR-	RDU-	5	0571:	Initialized computer defaults
BACC1:	2005 3 16 03:06:19 EST:	BPR-	RDU-	5	0573:	Initialized CableHome defaults
BACC1:	2005 3 16 03:06:19 EST:	BPR-	RDU-	5	0572:	Initialized PacketCable defaults
BACC1:	2005 3 16 03:06:19 EST:	BPR-	RDU-	5	0569:	Created default admin user
BACC1:	2005 3 16 03:06:19 EST:	BPR-	RDU-	5	0574:	Loaded 6 license keys
BACC1:	2005 3 16 03:06:20 EST:	BPR-	RDU-	5	0575:	Database initialization completed in 471 msec
BACC1:	2005 3 16 03:06:25 EST:	BPR-	RDU-	3	0015:	Unable to locate manifest file
BACC1:	2005 3 16 03:06:28 EST:	BPR-	RDU-	3	0280:	Command error

(注)　このログ ファイルでは KDC は考慮されていません。

dpe.log ファイルの表示

ログ ファイルの内容を表示するには、DPE の CLI から **show log** コマンドを使用します。詳細については、『*Cisco Broadband Access Center for Cable Command Line Reference*』を参照してください。

BACC では、DHCP サーバの拡張から拡張のトレース レベル設定に基づいてログ メッセージが生成されます。拡張のトレース レベルは、管理者のユーザ インターフェイスを使用して変更することができます。

変更するには、次の手順に従います。

ステップ 1　DHCP Server を選択して、拡張設定を展開します。

ステップ 2　変更を有効にするため、DHCP サーバをリロードします。

管理者のユーザ インターフェイス

BACC 管理者のユーザ インターフェイスは、HTML ベースのアプリケーションで、システムに登録されたユーザとデバイスを設定および管理することができます。このユーザ 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 8 章「管理者のユーザ インターフェイスについて」では、BACC 管理ユーザ インターフェイスへのアクセス方法と、各種のインターフェイス コンポーネントについて説明します。
- 第 9 章「Broadband Access Center for Cable 管理者のユーザ インターフェイスの使用方法」では、各種 BACC コンポーネントのモニタリングなど、管理作業を行う方法について説明します。
- 第 10 章「Broadband Access Center for Cable の設定」では、BACC を設定するために実行する作業について説明します。

サンプル ユーザ インターフェイス

BACC 製品には Sample User Interface（SUI; サンプル ユーザ インターフェイス）アプリケーションも付属しています。SUI の説明は、第 11 章「サンプル ユーザ インターフェイスの設定および使用方法」にあります。これは、ラボ テストのシナリオで BACC を使用して、セルフプロビジョニングと事前プロビジョニング、およびその他の BACC 基本機能を実行する場合のデモを行うために使用します。BACC のフル配備では、課金、OSS、およびワークフローの各アプリケーションのいずれかまたはすべてが SUI 機能を備えることになります。

注意　SUI を実稼動環境で使用することは想定されていません。デモでの使用のみを目的としています。

CHAPTER 3

設定のワークフローとチェックリスト

この章は大きな 2 つの項で構成されており、さまざまなテクノロジーをサポートするように BACC コンポーネントを設定する際のプロセスを定義します。次の項で構成されています。

- コンポーネントのワークフロー（P.3-2）
- 技術のワークフロー（P.3-7）

コンポーネントのワークフロー

この項では、BACC でサポートされるテクノロジーに合せて各 BACC コンポーネントを設定する際に必要なワークフローについて説明します。これらの設定作業を行ってから、特定のテクノロジーをサポートするように BACC を設定します。ラボ インストールまたはコンポーネント インストールの場合にだけ該当する手順もあります。このような場合は、適切な指示が行われます。

この項で説明するコンポーネントのワークフローはチェックリストの形式で用意されており、次のものがあります。

- RDU チェックリスト
- DPE チェックリスト（次のチェックリストが含まれます）
  - ハードウェア DPE のチェックリスト
  - Solaris DPE のチェックリスト
- Network Registrar チェックリスト

(注) アスタリスク（*）が付いている項目は、必須の作業または手順です。

RDU チェックリスト

表 3-1 は、RDU 設定時のワークフローを示します。

表 3-1　RDU ワークフロー チェックリスト

No.	手順	参照先	インストールのタイプ
1.	BACC に利用されるシステム syslog サービスを設定する。	『*Cisco Broadband Access Center for Cable Installation Guide*』	両方
2.	BACC 管理ユーザ インターフェイスにアクセスする。	BACC 管理者のグラフィカル ユーザ インターフェイスへのアクセス（P.8-2）	両方
3.	管理者のパスワードを変更する。	BACC 管理者のグラフィカル ユーザ インターフェイスへのアクセス（P.8-2）	両方
4.	適切なライセンス キーを追加する。	ライセンス キーの管理（P.10-32）	両方
5.	RDU データベース バックアップ手順を設定する。	バックアップと回復（P.7-5）	コンポーネントのみ
6.	RDU SNMP エージェントを設定する。	snmpAgentCfgUtil.sh コマンドの使用方法（P.12-49）	コンポーネントのみ

ハードウェア DPE のチェックリスト

表 3-2 に示されている操作は、表 3-1、RDU ワークフロー チェックリストに示されている操作の後で実行する必要があります。

(注)　アスタリスク（*）が付いている項目は、必須の作業または手順です。

表 3-2　ハードウェア DPE 設定チェックリスト

No.	手順	参照先	インストールのタイプ
1.	パスワードを変更する。	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「password」コマンド	コンポーネントのみ
2.	BACC に利用されるシステム syslog サービスを設定する。	『*Cisco Broadband Access Center for Cable Installation Guide*』	両方
3.	IP アドレスを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「interface ethernet 0..1 ip address」コマンド	コンポーネントのみ
4.	プロビジョニング インターフェイスを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「interface <0..1> provisioning enabled」コマンド	コンポーネントのみ
5.	デフォルトのハードウェア ゲートウェイを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「ip default-gateway」コマンド	コンポーネントのみ
6.	プロビジョニング FQDN を設定する。	FQDN の自動生成のイネーブル化と設定に関する詳細については、P.10-40 の「FQDN の自動生成」を参照。	コンポーネントのみ
7.	BACC の共有秘密情報を設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「dpe shared-secret」コマンド	コンポーネントのみ
8.	目的の RDU に接続するために DPE を設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「dpe rdu-server (IP)」コマンド	コンポーネントのみ
9.	ネットワーク タイム プロトコル（NTP）を設定する。	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「ntp server (IP)」コマンド	コンポーネントのみ
10.	プライマリ プロビジョニング グループを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「dpe provisioning-group primary」コマンド	コンポーネントのみ
11.	ホスト名を設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「hostname」コマンド	コンポーネントのみ

表 3-2　ハードウェア DPE 設定チェックリスト （続き）

No.	手順	参照先	インストールのタイプ
12.	ドメイン名を設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「ip domain-name」コマンド	コンポーネントのみ
13.	1 つ以上のネーム サーバを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「ip name-server」コマンド	コンポーネントのみ
14.	ネットワークのデバイスおよびその他の BACC コンポーネントへの必要なルートを設定する。	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「ip route」コマンド	コンポーネントのみ
15.	DPE SNMP エージェントを設定する。	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』の「SNMP Agent Commands」の項	コンポーネントのみ
16.	RDU に接続されていることを確認する。	サーバの表示（P.9-21）	コンポーネントのみ

Solaris DPE のチェックリスト

表 3-3 に示されている操作は、表 3-1、RDU ワークフロー チェックリストに示されている操作の後で実行する必要があります。

(注)　このチェックリストは Solaris DPE のコンポーネント インストールに適用されます。ラボ インストールでは、必要なパラメータの入力が要求され、選択された技術が自動的に設定されます。ラボ インストールでは、DPE と RDU の両方を監視するために単一の SNMP エージェントも使用されます。これは、DPE の CLI または snmpAgentCfgUtil.sh ツールを使用して設定することができます。詳細については、P.12-49 の「snmpAgentCfgUtil.sh コマンドの使用方法」を参照してください。

(注)　アスタリスク（*）が付いている項目は、必須の作業または手順です。

表 3-3　Solaris DPE 設定チェックリスト

No.	手順	参照先	インストールのタイプ
1.	BACC に利用されるシステム syslog サービスを設定する。	『*Cisco Broadband Access Center for Cable Installation Guide*』	両方
2.	パスワードを変更する。	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「password」コマンド	両方
3.	プロビジョニング インターフェイスを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「interface ethernet [intf0|intf1]」コマンド	コンポーネントのみ

表 3-3　Solaris DPE 設定チェックリスト （続き）

No.	手順	参照先	インストールのタイプ
4.	プロビジョニング FQDN を設定する。	FQDN の自動生成のイネーブル化と設定に関する詳細については、P.10-40 の「FQDN の自動生成」を参照。	コンポーネントのみ
5.	BACC の共有秘密情報を設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「dpe shared-secret」コマンド	コンポーネントのみ
6.	目的の RDU に接続するために DPE を設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「dpe rdu-server (IP)」コマンド	コンポーネントのみ
7.	ネットワーク タイム プロトコル（NTP）を設定する。	設定については、Solaris のマニュアルを参照。	コンポーネントのみ
8.	プライマリ プロビジョニング グループを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「dpe provisioning-group primary」コマンド	コンポーネントのみ
9.	ネットワークのデバイスおよびその他の BACC コンポーネントへの必要なルートを設定する。	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』に示されている「ip route」コマンド	コンポーネントのみ
10.	DPE SNMP エージェントを設定する。	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』の「SNMP Agent Commands」の項	コンポーネントのみ
11.	RDU に接続されていることを確認する。	サーバの表示（P.9-21）	両方

Network Registrar チェックリスト

表 3-4 に示されている操作は、表 3-2、ハードウェア DPE 設定チェックリスト、または表 3-3、Solaris DPE 設定チェックリストに示された操作の後で実行する必要があります。

注意　BACC DHCP のオプション設定は必ず、Network Registrar 内で設定された DHCP のオプション値より優先されます。

(注)　アスタリスク（*）が付いている項目は、必須の作業または手順です。

表 3-4　Network Registrar ワークフロー チェックリスト

No.	手順	参照先	インストールのタイプ
1.	Network Registrar の拡張を確認する。	妥当な拡張の設定については、『*Broadband Access Center for Cable Installation Guide*』を参照。	両方
2.	BACC に利用されるシステム syslog サービスを設定する。	BACC のシステム syslog サービスの設定に関する詳細については、『*Broadband Access Center for Cable Installation Guide*』を参照。	両方
3.	RDU で定義されたものと一致する client-classes/scope-selection-tags を設定する。*	client-classes および scope-selection-tags の設定の詳細については、『*Network Registrar User's Guide*』を参照。	両方
4.	スコープを設定する。*	スコープの設定に関する詳細については、『*Network Registrar User's Guide*』を参照。	両方
5.	ポリシーを設定する。*	ポリシーの設定に関する詳細については、『*Network Registrar User's Guide*』を参照。	両方
6.	Network Registrar データベースのバックアップ手順を設定する。	Network Registrar データベースのバックアップに関する詳細については、『*Network Registrar User's Guide*』を参照。	コンポーネントのみ
7.	正しい RDU に接続されていることを確認する。	サーバの表示（P.9-21）	両方

技術のワークフロー

この項では、特定のテクノロジーをサポートするように BACC を設定する際に必要な作業について説明します。これらの設定作業は、BACC コンポーネントの設定後に実行します。ラボ インストールまたはコンポーネント インストールの場合にだけ該当する場合もあります。このような場合は、適切な指示が行われます。

この項で説明する技術のワークフローはチェックリストの形式で用意されており、次のものがあります。

- DOCSIS チェックリスト（P.3-7）
- PacketCable チェックリスト（次のチェックリストが含まれます）
  - PacketCable（P.3-8）
  - ノンセキュア PacketCable（P.3-10）
  - Euro-PacketCable（P.3-12）
- ノンセキュア CableHome プロビジョニング チェックリスト（P.3-14）

(注)　アスタリスク（*）が付いている項目は、必須の作業または手順です。

DOCSIS チェックリスト

DOCSIS の操作のための BACC の設定を成功させるには、表 3-5 に示されている操作の他に、P.3-2 の「コンポーネントのワークフロー」に示されている操作を実行する必要があります。

このチェックリスト中の操作は、指定された順序で実行してください。

表 3-5　DOCSIS チェックリスト

ステップ	操作	参照先
RDU を設定する		
1.	プロビジョニングされる DHCP 基準をすべて設定する。	詳細については、P.10-25 の「DHCP 基準の設定」を参照。
2.	プロビジョニングされるサービス クラスを設定する。 プロビジョニングされる DOCSIS モデムが利用する可能性があるすべてのサービス クラスを追加します。	サービス クラスの設定（P.10-2）
3.	無差別モードの操作を設定する。	System Defaults（P.10-22）
Network Registrar を設定する		
1.	プロビジョニングされる DOCSIS モデムの DHCP 基準で追加されるものと一致するクライアントクラス選択タグ / スコープ選択タグを設定する。	クライアントクラス選択タグおよびスコープ選択タグの設定の詳細については、『*Network Registrar User's Guide*』を参照。

PacketCable チェックリスト

BACC では、3 つの異なる PacketCable がサポートされます。この項では、次のそれぞれについて、必要な操作を示します。

- PacketCable（P.3-8）
- ノンセキュア PacketCable（P.3-10）
- Euro-PacketCable（P.3-12）

(注)　この項で示すチェックリストでは、適切な PacketCable 設定ファイルと正しい MIB が読み込まれていることを前提にしています。

PacketCable

表 3-6 に示されている PacketCable 関連の操作は、P.3-2 の「コンポーネントのワークフロー」に示されている操作の後で実行する必要があります。PacketCable チェックリストには、ほぼすべての BACC コンポーネントと協調することが含まれます。

このチェックリスト中の操作は、指定された順序で実行してください。

(注)　KDC と DPE の間のデフォルトの最長クロック スキューは 5 分です。

(注)　アスタリスク（*）が付いている項目は、必須の作業または手順です。

表 3-6　PacketCable チェックリスト

ステップ	操作	参照先
RDU を設定する		
1.	MTA FQDN の自動生成をイネーブルにする。	FQDN の自動生成のイネーブル化と設定に関する詳細については、P.10-40 の「FQDN の自動生成」を参照。
2.	プロビジョニングされる DHCP 基準をすべて設定する。	詳細については、P.10-25 の「DHCP 基準の設定」を参照。
3.	プロビジョニングされるサービス クラスをすべて設定する。	詳細については、P.10-2 の「サービス クラスの設定」を参照。
4.	SNMPv3 クローニング キーを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「packetcable snmp key-material」コマンド (注)　このコマンドは、コンソール モードから実行する必要があります。

表 3-6　PacketCable チェックリスト （続き）

ステップ	操作	参照先
DPE を設定する		
1.	KDC サービス キーを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「packetcable registration kdc-service-key」コマンド
2.	プライバシー ポリシーを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「packetcable registration policy-privacy」コマンド
3.	SNMPv3 クローニング キーを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「packetcable snmp key-material」コマンド **（注）** このコマンドは、コンソール モードから実行する必要があります。
4.	PacketCable をイネーブルにする。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「packetcable enable」コマンド
5.	任意の MTA ファイルの暗号化を設定する。	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「packetcable registration encryption」コマンド
KDC を設定する		
1.	シスコ代理店から KDC ライセンスを入手して、そのファイルを <BACC_HOME>/kdc ディレクトリにコピーする。	KDC ライセンス（P.2-16）
2.	証明書チェーンを設定する。	KDC 証明書を管理するための PKCert.sh ツールの使用方法（P.12-42）
3.	各 DPE のプロビジョニング FQDN のサービス キー ペアを設定する。	Keygen ツールの使用方法（P.12-47）
4.	チケット認可チケット（TGT）のサービス キーを設定する。	Keygen ツールの使用方法（P.12-47）
5.	Call Management Server のサービス キーを設定する。	Keygen ツールの使用方法（P.12-47）
6.	ネットワーク タイム プロトコル（NTP）を設定する。	Solaris の NTP の設定に関する詳細については、Solaris のマニュアルを参照。

表 3-6　PacketCable チェックリスト （続き）

ステップ	操作	参照先
DHCP を設定する		
1.	必要な PacketCable 音声技術のプロパティをすべて設定する。	changeNRProperties.sh ツールの使用（P.12-45）
2.	MTA スコープのダイナミック DNS を設定する。	ダイナミック DNS の設定に関する詳細については、『*Network Registrar User's Guide*』を参照。
3.	RDU で定義されたものと一致する client-classes/scope-selection-tags を設定する。*	client-classes および scope-selection-tags の設定の詳細については、『*Network Registrar User's Guide*』を参照。
DNS を設定する		
1.	各 DHCP サーバの ダイナミック DNS を設定する。	ダイナミック DNS の設定に関する詳細については、『*Network Registrar User's Guide*』を参照。
2.	KDC 領域のゾーンを設定する。	ゾーンの設定に関する詳細については、『*Network Registrar User's Guide*』を参照。
3.	KDC の SRV レコードを設定する。	SRV レコードの設定に関する詳細については、P.10-38 の「Network Registrar DNS サーバでの SRV レコードの設定」および『*Network Registrar User's Guide*』を参照。
4.	KDC および DPE プロビジョニング インターフェイス名のレコードを設定する。	レコードの設定に関する詳細については、『*Network Registrar User's Guide*』を参照。

（注） DNS サーバの IP アドレスのリバース ゾーンを設定する際は、DNS 手順を利用することをお勧めします。nslookup など一部の DNS クライアントは、DNS サーバの IP アドレスを FQDN に変換しようとします。この場合、リバース ゾーンがあり、それが適切に設定されていない限り、DNS からレコードを検索できない可能性があります。

ノンセキュア PacketCable

表 3-7 に示されている PacketCable 関連の操作は、P.3-2 の「コンポーネントのワークフロー」に示されている操作の後で実行する必要があります。ノンセキュア PacketCable チェックリストには、ほぼすべての BACC コンポーネントと協調することが含まれます。

このチェックリスト中の操作は、指定された順序で実行してください。

（注） KDC と DPE の間のデフォルトの最長クロック スキューは 5 分です。

（注） アスタリスク（*）が付いている項目は、必須の作業または手順です。

表 3-7　ノンセキュア PacketCable チェックリスト

ステップ	操作	参照先
DPE を設定する		
1.	KDC サービス キーを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「packetcable registration kdc-service-key」コマンド
2.	プライバシー ポリシーを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「ipacketcable registration policy-privacy」コマンド
3.	SNMPv3 クローニング キーを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「packetcable snmp key-material」コマンド **(注)** このコマンドは、コンソール モードから実行する必要があります。
4.	PacketCable をイネーブルにする。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「packetcable enable」コマンド
DHCP を設定する		
1.	必要なノンセキュア PacketCable 音声技術のプロパティをすべて設定する。	changeNRProperties.sh ツールの使用（P.12-45）
2.	MTA スコープのダイナミック DNS を設定する。	ダイナミック DNS の設定に関する詳細については、『*Network Registrar User's Guide*』を参照。
3.	RDU で定義されたものと一致する client-classes/scope-selection-tags を設定する。*	client-classes および scope-selection-tags の設定の詳細については、『*Network Registrar User's Guide*』を参照。
DNS を設定する		
1.	各 DHCP サーバの ダイナミック DNS を設定する。	ダイナミック DNS の設定に関する詳細については、『*Network Registrar User's Guide*』を参照。

(注) DNS サーバの IP アドレスのリバース ゾーンを設定する際は、DNS 手順を利用することをお勧めします。nslookup など一部の DNS クライアントは、DNS サーバの IP アドレスを FQDN に変換しようとします。この場合、リバース ゾーンがあり、それが適切に設定されていない限り、DNS からレコードを検索できない可能性があります。

Euro-PacketCable

表 3-8 に示されている Euro-PacketCable 関連の操作は、P.3-2 の「コンポーネントのワークフロー」に示されている操作の後で実行する必要があります。Euro-PacketCable チェックリストには、ほぼすべての BACC コンポーネントと協調することが含まれます。

このチェックリスト中の操作は、指定された順序で実行してください。

(注)　アスタリスク（*）が付いている項目は、必須の作業または手順です。

表 3-8　Euro-PacketCable チェックリスト

ステップ	操作	参照先
RDU を設定する		
1.	MTA FQDN の自動生成をイネーブルにする。	FQDN の自動生成のイネーブル化と設定に関する詳細については、P.10-40 の「FQDN の自動生成」を参照。
2.	プロビジョニングされる DHCP 基準をすべて設定する。	詳細については、P.10-25 の「DHCP 基準の設定」を参照。
3.	プロビジョニングされるサービス クラスをすべて設定する。	詳細については、P.10-2 の「サービス クラスの設定」を参照。
4.	SNMPv3 クローニング キーを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「packetcable snmp key-material」コマンド (注)　このコマンドは、コンソール モードから実行する必要があります。
DPE を設定する		
1.	KDC サービス キーを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「packetcable registration kdc-service-key」コマンド
2.	プライバシー ポリシーを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「ipacketcable registration policy-privacy」コマンド

表 3-8　Euro-PacketCable チェックリスト （続き）

ステップ	操作	参照先
3.	SNMPv3 クローニング キーを設定する。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「packetcable snmp key-material」コマンド (注) このコマンドは、コンソール モードから実行する必要があります。
4.	PacketCable をイネーブルにする。*	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「packetcable enable」コマンド
5.	任意の MTA ファイルの暗号化を設定する。	『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』および『*Cisco Broadband Access Center for Cable Installation Guide*』に示されている「packetcable registration encryption」コマンド
KDC を設定する		
1.	シスコ代理店から KDC ライセンスを入手して、そのファイルを <BACC_HOME>/kdc ディレクトリにコピーする。	KDC ライセンス（P.2-16）
2.	PKCert.sh ツールで -e スイッチを使用して証明書チェーンを設定する。	KDC 証明書を管理するための PKCert.sh ツールの使用方法（P.12-42）
3.	各 DPE のプロビジョニング FQDN のサービス キー ペアを設定する。	Keygen ツールの使用方法（P.12-47）
4.	チケット認可チケット（TGT）のサービス キーを設定する。	Keygen ツールの使用方法（P.12-47）
5.	Call Management Server のサービス キーを設定する。	Keygen ツールの使用方法（P.12-47）
6.	ネットワーク タイム プロトコル（NTP）を設定する。	Solaris の NTP の設定に関する詳細については、Solaris のマニュアルを参照。
DHCP を設定する		
1.	必要な PacketCable 音声技術のプロパティをすべて設定する。	changeNRProperties.sh ツールの使用（P.12-45）
2.	MTA スコープのダイナミック DNS を設定する。	ダイナミック DNS の設定に関する詳細については、『*Network Registrar User's Guide*』を参照。
3.	RDU で定義されたものと一致する client-classes/scope-selection-tags を設定する。*	client-classes および scope-selection-tags の設定の詳細については、『*Network Registrar User's Guide*』を参照。
DNS を設定する		
1.	各 DHCP サーバの ダイナミック DNS を設定する。	ダイナミック DNS の設定に関する詳細については、『*Network Registrar User's Guide*』を参照。
2.	KDC 領域のゾーンを設定する。	ゾーンの設定に関する詳細については、『*Network Registrar User's Guide*』を参照。

表 3-8　Euro-PacketCable チェックリスト （続き）

ステップ	操作	参照先
3.	KDC の SRV レコードを設定する。	SRV レコードの設定に関する詳細については、P.10-38 の「Network Registrar DNS サーバでの SRV レコードの設定」および『*Network Registrar User's Guide*』を参照。
4.	KDC および DPE プロビジョニング インターフェイス名のレコードを設定する。	レコードの設定に関する詳細については、『*Network Registrar User's Guide*』を参照。

(注)　DNS サーバの IP アドレスのリバース ゾーンを設定する際は、DNS 手順を利用することをお勧めします。nslookup など一部の DNS クライアントは、DNS サーバの IP アドレスを FQDN に変換しようとします。この場合、リバース ゾーンがあり、それが適切に設定されていない限り、DNS からレコードを検索できない可能性があります。

ノンセキュア CableHome プロビジョニング チェックリスト

ノンセキュア CableHome プロビジョニング作業のための BACC の設定を成功させるには、表 3-9 に示されている操作の他に、P.3-2 の「コンポーネントのワークフロー」に示されている操作を実行する必要があります。

このチェックリスト中の操作は、指定された順序で実行してください。

表 3-9　ノンセキュア CableHome プロビジョニング チェックリスト

ステップ	操作	参照先
RDU を設定する		
1.	プロビジョニングされる DHCP 基準を設定する。 プロビジョニングされるノンセキュア CableHome デバイスが利用する可能性がある DHCP 基準をすべて追加します。	DHCP 基準の設定（P.10-25）
2.	プロビジョニングされるサービス クラスを設定する。 プロビジョニングされるノンセキュア CableHome デバイスが利用する可能性があるサービス クラスをすべて追加します。	サービス クラスの設定（P.10-2）
3.	無差別モードの操作を設定する。	System Defaults（P.10-22）
Network Registrar を設定する		
1.	プロビジョニングされるノンセキュア CableHome の DHCP 基準で追加されるものと一致する client-classes/scope-selection-tags を設定する。	client-classes および scope-selection-tags の設定の詳細については、『*Network Registrar User's Guide*』を参照。

DOCSIS 設定

この章では、BACC DOCSIS の配備を運用に移すためにチェックまたは設定する必要のある機能を示します。また、設定に先立って必要な情報を説明し、使用可能なツールについて説明します。

- DOCSIS ワークフロー（P.4-1）
- ダイナミック DOCSIS テンプレートによる MIB の使用方法（P.4-3）
- DOCSIS 設定のための BACC 機能（P.4-4）
- DOCSIS ネットワークのトラブルシューティング（P.4-5）
- ネットワーク層以上の設定（P.4-6）
- ケーブル モデムの状態のトラブルシューティング（P.4-10）

(注) この BACC リリースでサポートされる DOCSIS オプションについては、P.12-12 の「DOCSIS オプションのサポート」を参照してください。

DOCSIS ワークフロー

DOCSIS プロビジョニングの仕様に含まれるプロビジョニング（ワークフロー）手順を図 4-1 に示します。

図 4-1　DOCSIS プロビジョニング フロー

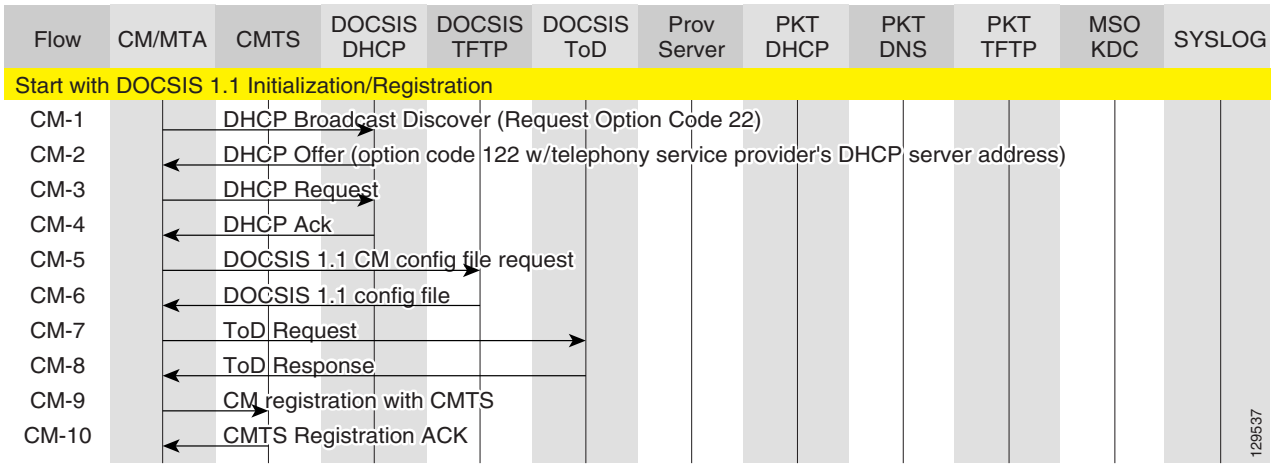


表 4-1 は、図 4-1 に示されるさまざまな DOCSIS プロビジョニング手順で発生する可能性がある問題について説明します。

表 4-1　DOCSIS ワークフローの説明

ステップ	DOCSIS ワークフロー手順	潜在的な問題
CM-1	DHCP 検出	• init(d) 状態。 • 使用可能なアドレスがない。 • BACC 共有秘密情報が正しいことを確認する。 • サービス クラスが誤って設定される。 • DOCSIS テンプレートの解析エラー（無効なオプション、インクルード ファイルが見つからないなど）。 **CNR DHCP** • CNR DHCP 設定に誤りがある。 • DHCP サーバがプロビジョニング グループ内にあることを確認する。 **BACC CNR 拡張** • BACC CNR 拡張が DPE に接続できない。 • BACC CNR 拡張がプロビジョニング グループ内の DPE を検出できない。 • 拡張が RDU に接続されていることを確認する。 • BACC CNR 拡張が DPE キャッシュ ミスを取得し、要求を RDU に送信する。 **RDU** • 適切なスコープが定義されていない（または BACC RDU 設定と一致しない）。 • RDU の IP アドレスが正しいことを確認する。 • RDU ポートが正しいことを確認する（デフォルトは 49187）。 • DPE から RDU に PING を実行できることを確認する。 • RDU で構成の生成に失敗している。 • RDU ライセンス数が超過したため、設定されない。 • RDU でデバイスの検出に失敗している。 **DPE** • DPE がプロビジョニング グループに割り当てられていることを確認する。 • DHCP サーバから DPE に PING を実行できることを確認する。 • DPE インターフェイスでプロビジョニングがイネーブルになっていることを確認する。
CM-2	DHCP オファー	DHCP と CMTS 間のルーティングの問題。
CM-3	DHCP 要求	init(i) 状態。 DHCP サーバからすべての必須パラメータが提供されなかった。
CM-4	DHCP 確認応答	

表 4-1　DOCSIS ワークフローの説明（続き）

ステップ	DOCSIS ワークフロー手順	潜在的な問題
CM-5	TFTP 要求	• init(o) 状態。 • CMTS と DPE 間のルーティングの問題。 • TFTP サーバ（DPE）からモデムへのルートがない。 • DPE キャッシュ ミス（静的ファイル、RDU がダウンしているかファイルがない）。 • TFTP サーバ（DPE）でファイルが見つからない。 • DPE キャッシュ ミス（動的ファイル）。 • DPE IP 検証エラー（たとえば、デバイスの IP アドレスが予期したアドレスではない、Dynamic Shared Secret が CMTS でイネーブルになっている、DOCSIS モデムとしてハッカーがスプーフィングしている）。
CM-6	TFTP 応答	DPE と CMTS 間のルーティングの問題。
CM-7	ToD 要求	init(t) 状態：タイム サーバ（DPE）からモデムへのルートがない。
CM-8	ToD 応答	
CM-9	CMTS への CM の登録	• reject(m)：* CMTS 共有秘密情報が BACC または DPE DSS 共有秘密情報と一致しない。 • reject(c)：* 誤った DOCSIS 設定ファイルが配送された（1.1 ファイルを 1.0 CM へ配送）。
CM-10	CMTS 登録確認応答	許容できる状態： • online • online(d) • online(pk) • online(pt)

ダイナミック DOCSIS テンプレートによる MIB の使用方法

BACC に付属する MIB の完全なリストについては、P.12-6 の「SNMP Varbind」を参照してください。

RDU にロードされる DOCSIS MIB には、2 つのバージョンがあります。

- DOCS-CABLE-DEVICE-MIB-OBSOLETE（実験的ブランチ）
- DOCS-CABLE-DEVICE-MIB（mib2 ブランチ）

これらの使用方法については、P.12-6 の「DOCSIS MIB」を参照してください。

API の呼び出しを使用するか、rdu.properties を修正することにより、MIB を追加することができます。詳細については、P.5-7 の「Euro-PacketCable の MIB の設定」を参照してください。

使用可能な MIB がないときに SNMP TLV をテンプレートに追加することができます。詳細については、P.12-11 の「MIB を使用しない SNMP TLV の追加」を参照してください。

DOCSIS 設定のための BACC 機能

この項では、DOCSIS テクノロジーと関連する BACC の付加価値機能について説明します。

動的設定 TLV

これらの TLV は、動的 DOCSIS 設定の TFTP 要求が受け取られるたびに、DPE によって追加されます。

- TLV 19（TFTP Server Timestamp。オプション）：Configure DOCSIS Defaults ページに TFTP Time Stamp オプションとして表示されます。詳細については、P.10-15 の「表 10-5」を参照してください。この TLV では CMTS および DPE における NTP の同期が必要です。
- TLV 20（TFTP Server Provisioned Modem Address。オプション）：Configure DOCSIS Defaults ページに TFTP Modem Address Option として表示されます。詳細については、P.10-15 の「表 10-5」を参照してください。
- TLV 6（CM MIC Configuration Setting。必須）
- TLV 7（CMTS MIC Configuration Setting。必須）：Configure DOCSIS Defaults ページに CMTS Shared Secret として表示されます。詳細については、P.10-15 の「表 10-5」を参照してください。

(注) CMTS MIC を設定するときは、次の CMTS IOS リリースの依存関係に注意してください。

- TLV 39 または TLV 40 を含める場合、DOCSIS 2.0 CMTS MIC には CMTS IOS 12.3BC が必要です。
- 次の CMTS IOS コマンドが BACC によって設定されているものとします。
  - ip dhcp relay information option
  - no ip dhcp relay information check
  - cable helper-address <x.x.x.x>
  - cable dhcp-giaddr primary

DPE TFTP IP 検証

DPE TFTP サーバは動的設定ファイルを対象に、TFTP クライアントの IP アドレスが DOCSIS ケーブル モデムの予期した IP アドレスに一致することを確認します。一致しない場合、要求は破棄されます。この機能に Cisco CMTS DMIC 機能との互換性はありません。

TFTP の動的構成要求における要求者の IP アドレスの検証をディセーブルにするには、次の no tftp verify-ip コマンドを使用します。

```
dpe# no tftp verify-ip
%OK
```

DOCSIS 1.0、1.1、2.0 のサポート

BACC 2.7 では DOCSIS 1.0、1.1、および 2.0 がサポートされます。BACC によって各 DOCSIS バージョンでサポートされる TLV およびオプションの詳細については、第 12 章「Broadband Access Center for Cable がサポートするツールと高度な概念」を参照してください。

DOCSIS バージョンの動的選択

BACC では、ケーブル モデムの DOCSIS バージョンを着信 DHCP 要求から検出することができます。また、GIADDR から DOCSIS バージョン番号へのマッピングを行う任意の顧客提供ソースから CMTS DOCSIS バージョンを検出することもできます。

DOCSIS バージョンは設定ファイル ユーティリティに指定できます。詳細については、P.12-25 の「設定ファイル ユーティリティの使用方法」を参照してください。

DOCSIS バージョンに基づいた DOCSIS 設定ファイル

デフォルトの DOCSIS コード生成の拡張では、モデムをプロビジョニングするための DOCSIS バージョンを使用して、モデムに送信する DOCSIS 設定ファイルのファイル名を決定します。

DOCSIS バージョン依存のサービス クラス プロパティ

次の新しいサービス クラス プロパティが、管理者のユーザ インターフェイスおよび BACC API でサポートされます。

```
/cos/docsis/file/1.0
/cos/docsis/file/1.1
/cos/docsis/file/2.0
```

DOCSIS 設定ファイル名を特定の DOCSIS バージョンと関連付けるために、これらのプロパティをオプションで DOCSIS サービス クラスに追加することができます。これらの各プロパティ（設定した場合）により、既存の DOCSIS 設定ファイル名プロパティで行われるように、サービス クラスとプロパティ値で指定されたファイルとの間に RDU によってデータベース関係を確立できます。

DOCSIS ネットワークのトラブルシューティング

共有 HFC ネットワーク全体にトール品質音声、データ サービス、およびマルチメディア アプリケーションを提供するために必要な帯域幅および遅延が DOCSIS によって保証されます。下位互換性があるように設計されているため、DOCSIS 1.0、1.1、および 2.0 モデムは同一ネットワークの同一スペクトラムで動作することができます。

(注) この項の大部分は、BACC および Cisco uBR7246 CMTS に関する DOCSIS テクノロジーの説明です。例は Cisco uBR7246 CMTS のものですが、その内容は他の CMTS ベンダーがサポートしなければならない DOCSIS 規格に関連しています。

ネットワーク層以上の設定

レンジングが正常に行われた後、動作するサポート サーバからケーブル モデムに追加の設定を行う必要があります。サーバから提供および設定されるサービスの集まりを Operational Support Services（OSS; オペレーション サポート サービス）と呼びます。

（注） この時点でモデムは機能しています。モデムは、ブリッジのように動作してかなり高速な伝送デバイスとなることもありますが、管理者の設定、診断、サービス クラス、セキュリティ、プライバシー、またはリモート ソフトウェア アップグレードの機能がないため、DOCSIS には準拠しません。

DHCP 状態の確立

```
MAC State --->>> 'establish_dhcp_state'
cmWriteFlashFile("CM_MACCONFIG", 0x8313db6, 0x12e) by TID 0x82eb0f8 (tConfigNV)
usrEraseSysFlash(1, 0x1e0400, 0x12e) by TID 0x82eb0f8 (tConfigNV)
.........cmWriteFlashFile("CM_DHCPLEASE", 0x810ebe4, 0x24) by TID 0x82d825c (tLease-0)
usrEraseSysFlash(1, 0x1e0200, 0x24) by TID 0x82d825c (tLease-0)
```

OSS の設定における最初のタスクは、DHCP によるネットワーク設定の取得です。ブロードキャスト DHCP DISCOVER メッセージがモデムによって発行されます。通常、ブロードキャスト メッセージはルータによって転送されませんが、UDP プロトコルの集合（このうちの 1 つが DHCP）に対しては、転送されるようにルータを設定することができます。DHCP サーバが DISCOVER に対して OFFER で応答すると、モデムはオファーされた設定の REQUEST を送信するように選択できます。

DHCP サーバは ACK（確認応答）または NAK（否定応答）で応答します。互換性のない IP アドレスとゲートウェイ アドレスの結果として NAK が返される場合があります。これは、モデムがあるダウンストリーム チャネルから別のサブネット上のダウンストリーム チャネルにホップした場合に発生する可能性があります。モデムがリースの更新を求めると、DHCP REQUEST メッセージの IP アドレスおよびゲートウェイ アドレスではネットワーク番号が異なり、DHCP サーバは REQUEST を NAK で拒否します。このような事態はまれで、モデムはリースを解放し DHCP DISCOVER メッセージからやり直します。

establish_dhcp_state マニフェストでは NAK でなくタイムアウトでエラーとなることがよくあります。効率的にトラブルシューティングするには、次の手順に従います。

- 下位層から開始して上位に進む。
- ローカルで開始してリモートで可能性のある部分へと進む。
- DHCP ログから DHCP サーバを診断する前に、モデムを調査する。

また、上記のレンジングでログ マスク 0xffff00bf を使用すると、モデムの始動時に発生する可能性があるほぼすべての問題をトラブルシューティングするのに役立ちます。これは、始動時エラーのトラブルシューティングを開始するのに最適です。DHCP メッセージの順序は、DISCOVER、OFFER、REQUEST、ACK でなければなりません。DHCP サーバから OFFER 応答がない状態でモデムが DISCOVER を送信している場合は、次のコマンドを使用して、uBR の UDP デバッグをオンにしてください。

uBR# **debug ip udp**

（注） telnet セッションか、コンソール セッション以外のセッションを介してルータに接続している場合にデバッグ メッセージを表示するには、**terminal monitor** コマンド（省略形は **term mon**）が必要です。**term mon** をオフにするには、**term no mon** コマンドを使用するか、ログアウトします。

注意　数台以上のモデムを備えた uBR7246 上でデバッグ コマンドを実行すると、デバッグに対応するため uBR7246 によってシステムが停止する可能性があります。この場合には、すべてのモデムで同期が失われるおそれがあり、デバッグの意味がなくなります。

デバッグ メッセージの中にパケットが現れない場合、このモデムの接続先であるケーブル インターフェイスで ip helper-address 文の設定をチェックします。この文が正しく設定されていて、DHCP サーバのサブネットのパケット トレースでもモデムから DHCP パケットが送信されていないことが判明したら、モデムのケーブル インターフェイスの出力エラーを確認するか、または uBR のケーブル インターフェイスの入力エラーを確認します。減衰を高めてトランスミッタの電力を少し上げることも得策です。

パケットが DHCP サーバのサブネットに送信されている場合には、パラメータの要求エラーや割り当てエラーがないかどうかをモデムのデバッグ メッセージで再度チェックします。この段階のトラブルシューティングでは、モデムと DHCP サーバ間のルーティングを調査する必要があります。また、DHCP サーバの設定を再度チェックすることもお勧めします。

ToD 状態の確立

```
MAC State --->>> 'establish_tod_state'
```

モデムは、ネットワーク パラメータを取得した後に、Time Of Day（TOD; 時刻）サーバの時刻を要求する必要があります。TOD は UTC タイムスタンプ（1970 年 1 月 1 日からの秒数）を使用します。DHCP からのタイム オフセット オプション値を組み合せると、現在時刻を計算できます。時刻は、syslog とイベント ログのタイムスタンプに使用されます。

時刻のエラーは、ほとんどの場合、DHCP の設定に誤りがあることを示しています。TOD エラーにつながる設定の誤りには、IP アドレスやゲートウェイ アドレスの誤設定、間違った TOD サーバ アドレスがあります。モデムが保存した DHCP パラメータを次のコマンドを使用して調べ、再度トラブルシューティングをローカルで開始します。

```
-> cmShowDhcpParameters
```

または

```
-> cmAddLogValues ("SEV_ALL FAC_DHCP")
```

後者のコマンドによって、DHCP アクションおよびタスクのデバッグ出力が示されます。

vxWorks **routeShow** コマンドを使用してモデムのルーティング テーブルも確認します。

セキュリティ アソシエーション状態

```
MAC State --->>> 'security_association_state'
```

これは、まだ定義されていない状態のためのプレースホルダーです。セキュリティ サーバとのセキュリティ アソシエーションによってモデムに IPsec のようなセキュリティが提供されることを想定しています。その設計および実装はまだ検討中です。その間、DOCSIS 1.0 ではこの状態について、セキュリティ サーバ用の DHCP オプションを含む将来の定義をモデムでサポートするように求めています。この状態が DOCSIS で定義されてモデムに実装されるまで、この状態に関する問題がモデムで発生することはまずありません。

設定ファイル状態

CM に対する設定および管理の主要インターフェイスは、プロビジョニング サーバからダウンロードした設定ファイルです。この設定ファイルには、ダウンストリーム チャネルとアップストリーム チャネルの識別情報および特性に加え、サービス クラス設定、ベースライン プライバシー設定、全般的な運用設定、ネットワーク管理情報、ソフトウェア アップグレード フィールド、フィルタ、およびベンダー固有の設定が含まれます。

この状態で起こる障害の一般的な理由としては、ファイルの欠落、ファイル アクセス権の誤り、TFTP サーバにアクセスできない、ファイル形式の誤り、ファイルに必須オプションがない、必須オプションの誤設定、オプションの誤りなどがあります。たとえば、不明な TLV または無効な TLV などです。

設定ファイルのトランザクションおよび解析を行うデバッグ コマンドを次に示します。

```
-> cmAddLogValues ("SEV_ALL FAC_CONFIGFILE")
```

登録状態

```
MAC State --->>> 'registration_state'
```

設定後に、モデムは必要な設定のサブセットと共に登録要求（REG-REQ）を送信し、CM と CMTS の Message Integrity Check（MIC; メッセージの完全性チェック）も送信します。CM の MIC は設定ファイルの設定をハッシュ計算した結果であり、設定ファイルが中継時に改ざんされなかったことをモデムが確認する手段を提供します。CMTS の MIC も類似していますが、共有秘密情報の認証文字列用の設定も含まれます。この共有秘密情報は CMTS およびプロビジョニング サーバによって認識され、認証されたプロビジョニング サーバによって設定されたモデムだけが CMTS への登録を許可されることを保証します。

登録状態に関する問題は、ほとんどの場合、設定ファイルにエラーがあることを示しています。モデムと CMTS の両方で設定ファイルの設定がサポートされていることを確認してください。CMTS でサービス クラス プロファイルの作成が許可されていることを確認するか、または CMTS によって作成されたプロファイルを使用します。CMTS のケーブル インターフェイス設定および設定ファイルで、認証文字列を確認してください。

プライバシー状態の確立

```
MAC State --->>> 'establish_privacy_state'
```

次のすべての条件を満たす場合、モデムは Baseline Privacy Key Management プロトコルを介して CMTS とのベースライン プライバシーのネゴシエーションを行う必要があります。

- モデム ソフトウェアがベースライン プライバシーをサポートしている。
- サービス クラスが、プライバシーの有効なプロファイルである。
- ベースライン プライバシー設定が設定ファイルに存在する。

この状態で発生するエラーの原因として考えられるのは、設定ファイルの誤りです。CM と CMTS の両方でベースライン プライバシーがサポートされていることと、CMTS のインターフェイス設定および CM の設定ファイルでベースライン プライバシーが有効になっていることを確認してください。

暗号化のエクスポート制限によるエラーが発生する可能性もあります。一部のベンダーのモデムでは uBR7246 のインターフェイス設定で次のコマンドが必要になることがあります。

```
uBR(config-if)# cable privacy 40-bit-des
```

動作状態

```
MAC State --->>> 'operational_state' cmWriteFlashFile("CM_BOOT", 0x8109180, 0x13e) by
TID 0x83049b8 (tMACCtrl)
usrEraseSysFlash(1, 0x1e0900, 0x13e) by TID 0x83049b8 (tMACCtrl)
```

登録およびベースライン プライバシー ネゴシエーション（必要な場合）が正常に行われると、モデムは動作状態となり、トラフィックを受け渡す準備ができます。

モデムは動作可能になりますが、動作状態を維持しない場合があります。これは、同期の損失や DHCP リース更新の障害などによって発生する可能性があります。

ケーブル モデムの状態のトラブルシューティング

この項では、次のケーブル モデムの状態について取り上げます。

- オンライン状態（P.4-10）
- オフライン状態（P.4-11）
- レンジング プロセス：init(r1)、init(r2)、および init(rc) 状態（P.4-16）
- DHCP：init(d) 状態（P.4-18）
- DHCP：init(i) 状態（P.4-20）
- TOD 交換：init(t) 状態（P.4-23）
- オプション ファイル転送開始：init(o) 状態（P.4-25）
- online、online(d)、online(pk)、online(pt) 状態（P.4-26）
- reject(pk) および reject(pt) 状態（P.4-29）
- 登録：reject (m) 状態（P.4-31）
- 登録：reject (c) 状態（P.4-32）

オンライン状態

この項では、ケーブル モデムの *オンライン状態* について説明し、この状態で示される Radio Frequency（RF; 無線周波数）問題などをトラブルシューティングする方法について説明します。

(注) ここで扱う問題の多くは、すべてではありませんが RF に関連する問題です。Cisco uBR7246VXR とそのドメインにある CM との問題をトラブルシューティングする一般的な方法を理解するには、この項を参照してください。

Cisco uBR7246VXR で最初に使用する最も便利なコマンドは **show cable modem** です。

```
#show cable modem

Interface Prim Online       Timing  Rec     QoS  CPE  IP address   MAC address
Sid            State        Offset  Power
Cable2/0/U0 5  online(pt)   2290     -0.25  5    0    10.1.1.25    0050.7366.2223
Cable2/0/U0 6  offline      2287    -0.25   2    0    10.1.1.26    0050.7366.2221
```

Online State フィールドは状態を表します。状態は、表 4-2 のいずれかになります。

表 4-2　状態値

状態値	説明
offline	ケーブル モデムがオフラインと見なされた。
init (r1)	ケーブル モデムが初期レンジングを送信した。
init (r2)	ケーブル モデムがレンジング中である。
init (rc)	ケーブル モデムのレンジングが完了した。
init (d)	DHCP 要求を受信した。
init (i)	DHCP 応答を受信した。IP アドレスが割り当てられた。
init (t)	TOD 交換が開始された。
init (o)	オプション ファイル転送が開始された。

表 4-2　状態値（続き）

状態値	説明
online	ケーブル モデムは登録され、データの送受信が可能になった。
online(d)	ケーブル モデムは登録されたが、ケーブル モデムのネットワーク アクセスは無効になっている。
online(pk)	ケーブル モデムは登録され、BPI が有効になり、KEK が割り当てられた。
online(pt)	ケーブル モデムは登録され、BPI が有効になり、TEK が割り当てられた。
reject (pk)	KEK モデム キーの割り当てが拒否された。
reject (pt)	TEK モデム キーの割り当てが拒否された。
reject (m)	ケーブル モデムが登録を試行したが、不正な MIC（メッセージの完全性チェック）により、登録は拒否された。
reject (c)	ケーブル モデムが登録を試行したが、不正な Class of Service（COS; サービス クラス）により、登録は拒否された。

次の項では、各*状態*の値、考えられる原因、正しい状態（オンライン）にするための手順について説明します。

オフライン状態

場合によっては、ケーブル モデムが他の状態を循環してから、オフラインに戻ることがあります。ケーブル モデムで Quadrature Amplitude Modulation（QAM; 直交振幅変調）ロックが失敗する最も一般的な理由を次に示します。

- キャリア信号が弱い（ノイズが多すぎる）。
- ダウンストリーム中心周波数が正しくない。
- DOCSIS ファイルで指定されている周波数が正しくない。
- ダウンストリームのデジタル QAM 変調信号が存在しない。
- Cisco uBR7246VXR の **cable modem change-frequency** で指定されている周波数が正しくない。

次に示すのは、モデムで入力された **show controllers cable-modem 0** の出力結果の一部です。

```
#sh cont c 0

BCM Cable interface 0:
CM unit 0, idb 0x8086C88C, ds 0x8086E460, regaddr = 0x2700000, reset_mask 0x80
station address 0030.96f9.65d9  default station address 0030.96f9.65d9
PLD VERSION: 1
Concatenation: ON Max bytes Q0: 2000 Q1: 2000 Q2: 2000 Q3: 2000

MAC State is ds_channel_scanning_state, Prev States = 3
MAC mcfilter 01E02F00  data mcfilter 00000000

MAC extended header ON
DS: BCM 3300 Receiver: Chip id = BCM3300
US: BCM 3300 Transmitter: Chip id = 3300

Tuner: status=0x00
Rx: tuner_freq 529776400, symbol_rate 5361000, local_freq 11520000
    snr_estimate 166(TenthdB), ber_estimate 0, lock_threshold 26000
    QAM not in lock, FEC not in lock, qam_mode QAM_64    (Annex B)
Tx: tx_freq 27984000, symbol rate 8 (1280000 sym/sec)
    power_level: 6.0 dBmV (commanded)
        7  (gain in US AMP units)
        63  (BCM3300 attenuation in .4 dB units)
...[Rest of the displayed output is omitted]
```

上の出力例で Signal to Noise ratio（SNR; 信号対雑音比）の推定値は 16.6 dB です。CM が 64 QAM で正常に動作するための適切な値は 30 dB 以上です。DOCSIS のダウンストリームおよびアップストリームの信号については、RF 仕様を参照してください。場合によっては、良好な SNR（34 dB など）が得られているのに、インパルス ノイズなどのノイズが存在することがあります。これは、ゼロスパン モードで動作するスペクトル アナライザを使用しないと検出できません。インパルス ノイズを示すものとして、修正できないエラーがあります。このエラーは、次に示すように **show interfaces cable 2/0 upstream 0** の出力結果に出現します。

```
#show interfaces cable 2/0 upstream 0

    Cable2/0: Upstream 0 is up
    Received 46942 broadcasts, 0 multicasts, 205903 unicasts
    0 discards, 12874 errors, 0 unknown protocol
```

（注） 値が 10,000 分の 1 を超えていれば、インパルス ノイズが存在すると考えられます。

```
    252845 packets input, 1 uncorrectable
    12871 noise, 0 microreflections Total Modems On This Upstream Channel : 3 (3
    active)
    Default MAC scheduler
    Queue[Rng Polls]  0/64, fifo queueing, 0 drops
    Queue[Cont Mslots]  0/104, fifo queueing, 0 drops
    Queue[CIR Grants]  0/64, fair queueing, 0 drops
    Queue[BE Grants]  0/64, fair queueing, 0 drops
    Queue[Grant Shpr]   0/64, calendar queueing, 0 drops
    Reserved slot table currently has 0 CBR entries
    Req IEs 77057520, Req/Data IEs 0
    Init Mtn IEs 1194343, Stn Mtn IEs 117174
    Long Grant IEs 46953, Short Grant IEs 70448
    Avg upstream channel utilization : 1%
    Avg percent contention slots : 96%
    Avg percent initial ranging slots : 4%
    Avg percent minislots lost on late MAPs : 0%
    Total channel bw reserved 0 bps
    CIR admission control not enforced
    Current minislot count   : 7192093    Flag: 0
    Scheduled minislot count : 7192182    Flag: 0
```

CM での最適な入力電力レベルは 0 dBmV であり、レシーバの範囲は -15 dBmv ～ +15 dBmV です。この値はスペクトル アナライザで測定できます。電力レベルが低すぎる場合は、『*Cisco uBR 7246 Hardware Installation Guide*』の指示に従って、アップコンバータを設定しなければならないことがあります。信号レベルが強すぎる場合は、高周波ポート接続でさらに減衰を加えることが必要な場合もあります。特定の周波数でノイズが多すぎる場合は、スペクトラム内で別の周波数の選択が必要になることがあります。

CM で QAM ロックが失敗しているかどうかを確認するには、**debug cable-modem mac log verbose** をオンにします。次のような出力結果が表示されます。

```
2d18h:    239198.516        CMAC_LOG_LINK_DOWN
2d18h:    239198.516    CMAC_LOG_LINK_UP
2d18h:    239198.516    CMAC_LOG_STATE_CHANGE                    ds_channel_scanning_
                                                                 state
2d18h:    239198.520    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   99/805790200/99770
2d18h:    239198.520    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   98/601780000/79970
2d18h:    239198.520    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   97/403770100/59570
2d18h:    239198.524    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   96/73753600/115750
2d18h:    239198.524    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   95/217760800/39770
2d18h:    239198.528    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   94/121756000/16970
2d18h:    239198.528    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   93/175758700/21170
2d18h:    239198.528    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   92/79753900/857540
2d18h:    239198.532    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   91/55752700/677530
2d18h:    239198.532    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   90/177000000/21300
2d18h:    239198.532    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   89/219000000/22500
2d18h:    239198.536    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   88/141000000/17100
2d18h:    239198.536    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   87/135012500/13500
2d18h:    239198.540    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   86/123012500/12900
2d18h:    239198.540    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   85/405000000/44700
2d18h:    239198.540    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   84/339012500/39900
2d18h:    239198.544    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   83/333025000/33300
2d18h:    239198.544    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   82/231012500/32700
2d18h:    239198.544    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   81/111025000/11700
2d18h:    239198.548    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   80/93000000/105000
2d18h:    239198.548    CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND   79/453000000/85500
NOTE—unable to lock on:
2d18h:    239198.552    CMAC_LOG_WILL_SEARCH_SAVED_DS_FREQUENCY  453000000
2d18h:    239199.672    CMAC_LOG_DS_NO_QAM_FEC_LOCK              453000000
2d18h:    239200.788    CMAC_LOG_DS_NO_QAM_FEC_LOCK              453000000
2d18h:    239201.904    CMAC_LOG_DS_NO_QAM_FEC_LOCK              453000000
2d18h:    239203.020    CMAC_LOG_DS_NO_QAM_FEC_LOCK              459000000
```

CM で QAM ロックが失敗する別の理由として、アップコンバータで設定されたダウンストリーム中心周波数が正しくない場合があります。たとえば、北米の標準 6 MHz チャネル帯域に対応した National Television Systems Committee（NTSC）周波数マップによれば、中心周波数が 651 MHz のチャネル 100-100 は 648.0 ～ 654.0 を使用しています。しかし、ビデオ キャリア周波数で動作するように設計されたアップコンバータを使用している場合（たとえば、中心周波数よりも 1.75 MHz 低い周波数を使用する GI C6U など）、チャネル 100-100 では周波数を 649.25 MHz に設定する必要があります。

よくある別の誤りとして、Cisco Broadband Configurator（cisco.com からのダウンロードで入手可能）の Radio Frequency Info の下にある *Downstream Frequency* フィールドで正しくない周波数を指定することがあります。通常、このオプションで周波数値を指定する必要はありません。ただし、必要な場合（特定のモデムを異なる周波数でロックしなければならないときなど）には、前述のように適切な周波数値を選択する必要があります。次のデバッグ出力は、この場合を示しています。ここで、CM は初期状態で 453 MHz にロックされ、その後 DOCSIS 設定ファイルで指定された 535.25 MHz にロックされます。これによってケーブル モデムはリセットされ、このプロセスが無限に繰り返されます。

4d00h:	345773.916	CMAC_LOG_WILL_SEARCH_SAVED_DS_FREQUENCY	453000000
4d00h:	345774.956	CMAC_LOG_UCD_MSG_RCVD	
4d00h:	**345775.788**	**CMAC_LOG_DS_64QAM_LOCK_ACQUIRED**	**453000000**
4d00h:	345775.792	CMAC_LOG_DS_CHANNEL_SCAN_COMPLETED	
4d00h:	345775.794	CMAC_LOG_STATE_CHANGE	wait_ucd_state
4d00h:	345776.946	CMAC_LOG_UCD_MSG_RCVD	1
4d00h:	345778.960	CMAC_LOG_UCD_MSG_RCVD	1
4d00h:	345778.962	CMAC_LOG_ALL_UCDS_FOUND	
4d00h:	345778.966	CMAC_LOG_STATE_CHANGE	wait_map_state
4d00h:	345778.968	CMAC_LOG_FOUND_US_CHANNEL	1
4d00h:	345780.996	CMAC_LOG_UCD_MSG_RCVD	1
4d00h:	345781.000	CMAC_LOG_UCD_NEW_US_FREQUENCY	27984000
4d00h:	345781.004	CMAC_LOG_SLOT_SIZE_CHANGED	8
4d00h:	345781.084	CMAC_LOG_UCD_UPDATED	
4d00h:	345781.210	CMAC_LOG_MAP_MSG_RCVD	
4d00h:	345781.212	CMAC_LOG_INITIAL_RANGING_MINISLOTS	40
4d00h:	345781.216	CMAC_LOG_STATE_CHANGE	ranging_1_state
4d00h:	345781.220	CMAC_LOG_RANGING_OFFSET_SET_TO	9610
4d00h:	345781.222	CMAC_LOG_POWER_LEVEL_IS	22.0 dBmV (comma)
4d00h:	345781.226	CMAC_LOG_STARTING_RANGING	
4d00h:	345781.228	CMAC_LOG_RANGING_BACKOFF_SET	0
4d00h:	345781.232	CMAC_LOG_RNG_REQ_QUEUED	0
4d00h:	345781.272	CMAC_LOG_RNG_REQ_TRANSMITTED	
4d00h:	345781.280	CMAC_LOG_RNG_RSP_MSG_RCVD	
4d00h:	345781.282	CMAC_LOG_RNG_RSP_SID_ASSIGNED	3
4d00h:	345781.284	CMAC_LOG_ADJUST_RANGING_OFFSET	2288
4d00h:	345781.288	CMAC_LOG_RANGING_OFFSET_SET_TO	11898
4d00h:	345781.292	CMAC_LOG_ADJUST_TX_POWER	7
4d00h:	345781.294	CMAC_LOG_POWER_LEVEL_IS	24.0 dBmV (comma)
4d00h:	345781.298	CMAC_LOG_STATE_CHANGE	ranging_2_state
4d00h:	345781.302	CMAC_LOG_RNG_REQ_QUEUED	3
4d00h:	345782.298	CMAC_LOG_RNG_REQ_TRANSMITTED	
4d00h:	345782.300	CMAC_LOG_RNG_RSP_MSG_RCVD	
4d00h:	345782.304	CMAC_LOG_RANGING_SUCCESS	
4d00h:	345782.316	CMAC_LOG_STATE_CHANGE	dhcp_state
4d00h:	345782.450	CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS	10.1.1.25
4d00h:	345782.452	CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS	10.10.20.1
4d00h:	345782.456	CMAC_LOG_DHCP_TOD_SERVER_ADDRESS	10.10.20.2
4d00h:	345782.460	CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS	
4d00h:	345782.464	CMAC_LOG_DHCP_TZ_OFFSET	0
4d00h:	345782.466	CMAC_LOG_DHCP_CONFIG_FILE_NAME	frequency.cm
4d00h:	345782.470	CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR	
4d00h:	345782.474	CMAC_LOG_DHCP_COMPLETE	
4d00h:	345782.598	CMAC_LOG_STATE_CHANGE	establish_tod_state
4d00h:	345782.606	CMAC_LOG_TOD_REQUEST_SENT	
4d00h:	345782.620	CMAC_LOG_TOD_REPLY_RECEIVED	3178880491

```
4d00h:    345782.628    CMAC_LOG_TOD_COMPLETE
4d00h:    345782.630    CMAC_LOG_STATE_CHANGE                    security_associate_
                                                                 state
4d00h:    345782.634    CMAC_LOG_SECURITY_BYPASSED
4d00h:    345782.636    CMAC_LOG_STATE_CHANGE                    configuration_file
4d00h:    345782.640    CMAC_LOG_LOADING_CONFIG_FILE             frequency.cm
4d00h: %LINEPROTO-5-UPDOWN:  Line protocol on Interface cable-modem0,changed state to
up
4d00h:    345783.678    CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
NOTE—frequency override:
4d00h:    345783.682    CMAC_LOG_DS_FREQ_OVERRIDE                535250000
4d00h:    345783.686    CMAC_LOG_STATE_CHANGE                    reset_hardware_state
4d00h:    345784.048    CMAC_LOG_STATE_CHANGE                    wait_for_link_up_state
4d00h:    345784.052    CMAC_LOG_DRIVER_INIT_IDB_RESET           0x082A5226
4d00h:    345784.054    CMAC_LOG_LINK_DOWN
4d00h:    345784.056    CMAC_LOG_LINK_UP
4d00h:    345784.062    CMAC_LOG_STATE_CHANGE                    ds_channel_scanning_
                                                                 state
4d00h:    345785.198    CMAC_LOG_DS_NO_QAM_FEC_LOCK              535250000
4d00h:    345785.212    CMAC_LOG_DS_TUNER_KEEPALIVE
4d00h:    345787.018    CMAC_LOG_UCD_MSG_RCVD                    1
4d00h:    345787.022    CMAC_LOG_DS_64QAM_LOCK_ACQUIRED          453000000
```

Cisco uBR7246VXR 上の **cable modem change-frequency** で指定された周波数が正しくない場合にも、CM で周波数の切り替えが発生します。ルータで設定された周波数が正しく選択されていなければ、上記と同様の結果になります。Cisco uBR7246VXR の **cable modem change-frequency** コマンドはオプションで、通常はデフォルトで省略されます。

ダウンストリーム チャネルの取得および遅延の計算が完了すると、次のタスクとして適切なアップストリーム チャネルの特定が行われます。ケーブル モデムは、アップストリーム チャネルの物理的なプロパティが含まれる Upstream Channel Descriptor（UCD; アップストリーム チャネル ディスクリプタ）を受信します。プロパティには、バースト ディスクリプタに定義されている周波数、変調、チャネル幅、およびその他のパラメータなどがあります。

ケーブル モデムが使用可能な UCD を見つけられない場合、そのモデムはアップストリーム サービスの提供されていないダウンストリーム チャネル上にある可能性があります。これは、ルータの設定に誤りがあるものと考えられます。この場合は、**show controller cable** *x* コマンドを使用して確認できます。ケーブル モデムが使用可能な UCD を見つけられない別の理由としては、そのハードウェアまたは MAC がバースト ディスクリプタ内のパラメータをサポートしていないことが考えられます。これは、Cisco uBR7246VXR の設定に誤りがあるか、CM が DOCSIS に準拠していない可能性があります。

使用可能な UCD が見つかると、ケーブル モデムは MAP（帯域幅割り当てマップ）メッセージの受信を開始します。MAP にはアップストリームの帯域幅割り当て時間マップが含まれています。時間のセクションが各ミニスロットにマッピングされ、個々のモデムに割り当てられます。MAP には、ブロードキャスト、コンテンションベースの初期メンテナンス（またはブロードキャスト）レンジング用の領域もあります。ケーブル モデムは、Cisco uBR7246VXR がレンジング応答（RNG-RSP）で応答するまで、MAP のこれらの領域にモデム自体の初期レンジング要求を送信する必要があります。

T2 タイマーが切れる前に CM が初期メンテナンス領域を見つけられない場合は、Cisco uBR7246VXR の設定に誤りがないかどうかを確認してください。また、ルータのケーブル インターフェイスの **insertion-interval** も確認する必要があります。

レンジング プロセス：init(r1)、init(r2)、および init(rc) 状態

この段階では、CM はレンジング プロセスを開始し、適切な入力電力レベルで Cisco uBR7246VXR に到達するために必要な伝送電力レベルを計算します。通常良好とされる伝送電力は、およそ 40 ～ 50 dBmV です（uBR7246 入力電力が 0 dBmV である場合に基づく）。この値は、ハードウェアによっては異なる場合もあります。ダウンストリーム チャネルと同様に、アップストリーム チャネル内のキャリアも、Cisco uBR7246VXR レシーバがシンボルを識別できてビット誤り率が増加するほど高くない十分な強さを持つ必要があります。

CM はレンジング要求（RNG-REQ）メッセージを Cisco uBR7246VXR に送り、レンジング応答（RNG-RSP）メッセージが送り返されてくるか、または T3 タイマーが切れるのを待ちます。T3 のタイムアウトが発生した場合は、リトライ回数が増します。リトライ回数がリトライ最大回数よりも少なければ、ケーブル モデムはより高い電力レベルで別の RNG-REQ を送信します。レンジング プロセスは MAP の初期メンテナンス領域またはブロードキャスト領域で発生します。これは、Cisco uBR7246VXR が、MAP 内のユニキャスト送信に使用する Service Identifier（SID; サービス ID）をまだモデムに割り当てていないためです。このため、ブロードキャスト レンジングはコンテンション ベースとなり、コリジョンの影響を受けます。これを補正するため、ケーブル モデムは RNG-REQ 送信の間のランダムなバックオフ時間を計算するためのレンジング バックオフ アルゴリズムを備えています。このアルゴリズムは、**cable upstream range-backoff** コマンドを使用して設定できます。伝送電力が Cisco uBR7246VXR に対して十分なレベルに達すると、Cisco uBR7246VXR は一時的な SID を含む RNG-RSP で RNG-REQ に応答します。この SID は、ユニキャスト レンジングで使用される MAP 内のユニキャスト送信領域の識別に使用されます。

次の出力は、init(r1) 状態にある CM が初期レンジング段階を完了できないことを示しています。

```
r#show cable modem

Interface Prim    Online      Timing    Rec      QoS   CPE   IP address   MAC address
Sid               State       Offset    Power
Cable2/0/U0 6     init(r1)    2813       12.00   2     0     10.1.1.22    0050.7366.1e01
```

次のデバッグは、CM がレンジング プロセスの完了に失敗して T3 タイマー切れとなり、リセットされる状況を示しています。Cisco uBR7246VXR が CMAC_LOG**_ADJUST_TX_POWER** メッセージを送信し、CM に対して電力を調整するよう指示を出していることがわかります。

```
1w3d:     871160.618    CMAC_LOG_STATE_CHANGE                  ranging_1_state
1w3d:     871160.618    CMAC_LOG_RANGING_OFFSET_SET_TO         9610
1w3d:     871160.622    CMAC_LOG_POWER_LEVEL_IS                19.0  dBmV (comman)
1w3d:     871160.622    CMAC_LOG_STARTING_RANGING
1w3d:     871160.622    CMAC_LOG_RANGING_BACKOFF_SET           0
1w3d:     871160.622    CMAC_LOG_RNG_REQ_QUEUED                0
1w3d:     871160.678    CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d:     871160.682    CMAC_LOG_RNG_RSP_MSG_RCVD
1w3d:     871160.682    CMAC_LOG_RNG_RSP_SID_ASSIGNED          6
1w3d:     871160.682    CMAC_LOG_ADJUST_RANGING_OFFSET         2813
1w3d:     871160.682    CMAC_LOG_RANGING_OFFSET_SET_TO         12423
1w3d:     871160.686    CMAC_LOG_ADJUST_TX_POWER               48
1w3d:     871160.686    CMAC_LOG_STATE_CHANGE                  ranging_2_state
1w3d:     871160.686    CMAC_LOG_RNG_REQ_QUEUED                6
1w3d:     871161.690    CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d:     871161.690    CMAC_LOG_RNG_RSP_MSG_RCVD
```

```
1w3d:     871161.694     CMAC_LOG_ADJUST_TX_POWER                    -36
1w3d:     871161.694     CMAC_LOG_RANGING_CONTINUE
1w3d:     871162.698     CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d:     871162.898     CMAC_LOG_T3_TIMER
1w3d:     871163.734     CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d:     871163.934     CMAC_LOG_T3_TIMER
1w3d:     871164.766     CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d:     871164.966     CMAC_LOG_T3_TIMER
131.CABLEMODEM.CISCO: 1w3d: %UBR900-3-RESET_T3_RETRIES_EXHAUSTED: R03.0 Ranging
1w3d:     871164.966     CMAC_LOG_RESET_T3_RETRIES_EXHAUSTED
1w3d:     871164.966     CMAC_LOG_STATE_CHANGE                    reset_interface_state
1w3d:     871164.966     CMAC_LOG_STATE_CHANGE                    reset_hardware_state
Note: init(r1) is ranging_1_state and init(r2) is ranging_2_state
```

次のコマンドにより、CM での伝送電力の状況を確認できます。

```
#sh cont cable-modem 0
BCM Cable interface 0:
CM unit 0, idb 0x2010AC, ds 0x86213E0, regaddr = 0x800000, reset_mask 0x80
station address 0050.7366.2223  default station address 0050.7366.2223
PLD VERSION: 32

MAC State is wait_for_link_up_state, Prev States = 2
MAC mcfilter 00000000  data mcfilter 00000000

MAC extended header ON
DS: BCM 3116 Receiver: Chip id = 2
US: BCM 3037 Transmitter: Chip id = 30AC

Tuner: status=0x00
Rx: tuner_freq 0, symbol_rate 5055932, local_freq 11520000
    snr_estimate 30640, ber_estimate 0, lock_threshold 26000
    QAM not in lock, FEC not in lock, qam_mode QAM_64
Tx: tx_freq 27984000, power_level 0x20 (8.0 dBmV), symbol_rate 8 (1280000 sym/s)
```

ケーブル モデムがレンジング状態から先に進めない場合は、伝送電力レベルが十分でないことが原因と考えられます。低周波ポートで減衰を調整することにより伝送電力を調整できます。減衰を増やすと、結果的に伝送電力レベルが上昇します。20 ～ 30 dBmV の減衰から始めることをお勧めします。

初期レンジング init(r1) の後、ケーブル モデムは init(r2) に進みます。init(r2) では、ケーブル モデムからの送信が正しいタイミングで受信され、その送信が Cisco uBR7246VXR レシーバでの入力電力レベルの許容範囲に収まるようにするため、ケーブル モデムは送信のタイミング オフセットと電力レベルを設定する必要があります。この設定はユニキャストの RNG-REQ および RNG-RSP メッセージのやり取りを通じて実行されます。RNG-RSP メッセージには、ケーブル モデムで実行しなければならない電力およびタイミング オフセットの訂正値が含まれています。

ケーブル モデムは、RNG-RSP メッセージでレンジングの成功が示されるか、または init(rc) 状態への到達によってレンジングが完了するまで RNG-REQ を送信し続け、RNG-RSP ごとに調整を実行します。ケーブル モデムが init (r2) から先に進めない場合は、伝送電力を調整する必要があります。

init(r2) 状態の CM の出力表示を次に示します。Rec Power 列の隣にあるアスタリスク（*）記号は、ノイズ電力調整機構がこのモデムでアクティブになっていることを示しています。感嘆符（!）が表示された場合は、ケーブル モデムが最大伝送電力に達したことを意味します。

```
#show cable modem

Interface Prim    Online      Timing    Rec     QoS   CPE   IP address   MAC address
Sid               State       Offset    Power
Cable2/0/U0 5     init(r2)    2289      *4.00   2     0     10.1.1.25     0050.7366.2223
```

DHCP：init(d) 状態

レンジングが成功すると、次の段階として DHCP によるネットワーク設定の取得が行われます。

次の **show cable modem** の出力表示は、ケーブル モデムが init(d) 状態にあること、つまり DHCP 要求を CM から受信したことを示しています。

```
#show cable modem

Interface Prim    Online      Timing    Rec     QoS   CPE   IP address   MAC address
Sid               State       Offset    Power
Cable2/0/U0 7     init(d)     2811       0.25   2     0     10.1.1.20     0030.96f9.65d9
```

CM は init(r1) から init(d) までの状態を無限に循環することに注意してください。考えられる原因を次に示します。

- Cisco uBR7246VXR から DHCP サーバへの IP 接続性に関する問題。
- DHCP サーバのダウン。
- 間違ったデフォルト ゲートウェイが DHCP サーバで設定されている。
- CM での伝送電力が低い。

(注) Cisco uBR7246VXR から DHCP サーバに PING を実行することはできますが、DHCP に正しくないゲートウェイが設定されるという問題は起こる可能性があります。これは、DHCP は Cisco uBR7246VXR ケーブル インターフェイスのプライマリ IP アドレスに応答できますが、DHCP ディスカバリ フェーズでソース IP アドレスとして使用されるセカンダリ IP アドレスには応答できないためです。

DHCP 状態のマニフェストでエラーが NAK ではなくタイムアウトとして現れることがよくあります。DHCP メッセージの順序は、DISCOVER、OFFER、REQUEST、ACK でなければなりません。DHCP サーバから OFFER 応答がない状態でケーブル モデムが DISCOVER を送信している場合は、次のコマンドを使用して、Cisco uBR7246VXR の UDP デバッグをオンにしてください。

```
# debug ip udp

4d01h:     UDP:       rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
4d01h:     BOOTP:     opcode 1 from host 0.0.0.0 on Cable2/0, 0 secs, 0 hops
4d01h:     UDP:       forwarded broadcast 67 from 10.1.1.10 to 10.20.20.9 on Ethernet0
4d01h:     UDP:       rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
4d01h:     BOOTP:     opcode 1 from host 0.0.0.0 on Cable2/0, 0 secs, 0 hops
4d01h:     UDP:       forwarded broadcast 67 from 10.1.1.10 to 10.20.20.9 on Ethernet0
4d01h:     UDP:       rcvd src=172.17.110.136(67), dst=10.1.1.10(67), length=314
4d01h:     BOOTP:     opcode 2 from host 10.20.20.9 on Ethernet1/0, 0 secs, 0 hops
```

```
4d01h:     BOOTP:     Broadcasting response 10.20.20.9 -> 10.1.1.20 (Cable2/0)
4d01h:     UDP:       forwarded broadcast 68 from 10.20.20.9 to 255.255.255.255 on Ca0
4d01h:     UDP:       rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
4d01h:     BOOTP:     opcode 1 from host 0.0.0.0 on Cable2/0, 0 secs, 0 hops
4d01h:     UDP:       forwarded broadcast 67 from 10.1.1.10 to 110.20.20.9 on Ethernet0
4d01h:     UDP:       rcvd src=10.20.20.9(67), dst=10.1.1.10(67), length=314
4d01h:     BOOTP:     opcode 2 from host 10.20.20.9 on Ethernet1/0, 0 secs, 0 hops
4d01h:     BOOTP:     Broadcasting response 10.20.20.9 -> 10.1.1.20 (Cable2/0)
4d01h:     UDP:       forwarded broadcunast 68 from 10.20.20.9 to 255.255.255.255 on 1
All possible debugging has been turned off
```

注意　数台以上のモデムを備えた uBR7246（ユニバーサル ブロードバンド ルータ）上でデバッグ コマンドを実行すると、デバッグに対応するため Cisco uBR7246VXR によってシステムが停止する可能性があります。この場合には、すべてのケーブル モデムで同期が失われるおそれがあり、デバッグの意味がなくなります。

デバッグ メッセージの中にパケットが現れない場合、このモデムの接続先であるケーブル インターフェイスで **cable helper-address** 文の設定をチェックします。この文が正しく設定されていて、DHCP サーバのサブネットのパケット トレースでもケーブル モデムから DHCP パケットが送信されていないことが判明したら、モデムのケーブル インターフェイスの出力エラーを確認するか、または Cisco uBR7246VXR のケーブル インターフェイスの入力エラーを確認します。減衰を高めて CM のトランスミッタの電力を少し上げることも得策です。

DHCP サーバのサブネットに送信されているパケットがあれば、パラメータの要求エラーや割り当てエラーがないかどうかをモデムのデバッグ メッセージでチェックします。この段階のトラブルシューティングでは、CM と DHCP サーバ間のルーティングを調査する必要があります。また、DHCP サーバの設定や DHCP のログについても再度チェックします。

CM で **debug cable-modem mac log verbose** コマンドを実行して得られたデバッグ例を次に示します。

```
1w3d:     865015.920     CMAC_LOG_RANGING_SUCCESS
1w3d:     865015.920     CMAC_LOG_STATE_CHANGE                    dhcp_state
1w3d:     865053.580     CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d:     865053.584     CMAC_LOG_RNG_RSP_MSG_RCVD
1w3d:     865055.924     CMAC_LOG_WATCHDOG_TIMER
131.CABLEMODEM.CISCO: 1w3d: %UBR900-3-RESET_DHCP_WATCHDOG_EXPIRED:
Cable Interface Reset due to DHCP watchdog timer expiration
1w3d:     865055.924     CMAC_LOG_RESET_DHCP_WATCHDOG_EXPIRED
1w3d:     865055.924     CMAC_LOG_STATE_CHANGE                    reset_interface_state
1w3d:     865055.924     cMAC_LOG_DHCP_PROCESS_KILLED
1w3d:     865055.924     CMAC_LOG_STATE_CHANGE                    reset_hardware_state
```

上の例では、DHCP プロセスが失敗し、ケーブル モデムがリセットされたことがわかります。

DHCP：init(i) 状態

DHCP 要求への応答を受信して IP アドレスがケーブル モデムに割り当てられると、次の **show cable modem** コマンドで出力される状態は init(i) になります。

#show cable modem

```
Interface Prim    Online      Timing    Rec     QoS   CPE   IP address   MAC address
Sid               State       Offset    Power
Cable2/0/U0 7     init(i)     2815      -0.25   2     0     10.1.1.20    0030.96f9.65d9
```

上の結果では、CM が init(i) 状態から先に進んでいません。**show cable modem** を繰り返し実行すると、一般にケーブル モデムは init(r1)、init(r2)、init(rc)、init(d) および init(i) の間を無限に循環します。

ケーブル モデムが init(i) から先に進まない理由として、よくある原因を次に示します。

- DHCP サーバで指定されている DOCSIS ファイルが正しくないか、または無効である。
- TFTP サーバの問題。IP アドレスが正しくない、TFTP サーバが到達不能であるなど。
- TOD またはタイミング オフセットの取得に関する問題。
- DHCP 設定内の Router の設定が正しくない。

ケーブル モデムは init(i) までは到達しているので、IP アドレスの取得までは完了していることがわかります。このことは、次に示すケーブルモデムでの **debug cable-modem mac log verbose** コマンドの出力表示からわかります。

```
3d20h:    334402.548    CMAC_LOG_RANGING_SUCCESS
3d20h:    334402.548    CMAC_LOG_STATE_CHANGE dhcp_state
NOTE—IP address Assigned to CM:
3d20h:    334415.492    CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS          10.1.1.20
3d20h:    334415.492    CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS          10.20.20.9
3d20h:    334415.492    CMAC_LOG_DHCP_TOD_SERVER_ADDRESS           10.20.20.9
3d20h:    334415.492    CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
3d20h:    334415.492    CMAC_LOG_DHCP_TZ_OFFSET                    0
NOTE—DOCSIS file CM is trying to load:
3d20h:    334415.496    CMAC_LOG_DHCP_CONFIG_FILE_NAME             nofile
3d20h:    334415.496    CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
3d20h:    334415.496    CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRESS
3d20h:    334415.496    CMAC_LOG_DHCP_COMPLETE
3d20h:    334415.508    CMAC_LOG_STATE_CHANGE                      establish_tod_state
3d20h:    334415.512    CMAC_LOG_TOD_REQUEST_SENT                  10.20.20.9
3d20h:    334415.524    CMAC_LOG_TOD_REPLY_RECEIVED                3178343318
3d20h:    334415.524    CMAC_LOG_TOD_COMPLETE
3d20h:    334415.528    CMAC_LOG_STATE_CHANGE                      security_association
                                                                   _state
3d20h:    334415.528    CMAC_LOG_SECURITY_BYPASSED
3d20h:    334415.528    CMAC_LOG_STATE_CHANGE                      configuration_file
NOTE—DOCSIS file name:
3d20h:    334415.528    CMAC_LOG_LOADING_CONFIG_FILE               nofile
133.CABLEMODEM.CISCO: 3d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface cap
3d20h:    334416.544    CMAC_LOG_CONFIG_FILE_TFTP_FAILED           -1
3d20h:    334416.548    CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
3d20h:    334416.548    CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
```

同様に、TFTP サーバに関する問題でも同じようなエラーが見られ、結果としてケーブル モデムがリセットされて同じプロセスを無限に循環することになります。

```
3d21h:    336136.520    CMAC_LOG_STATE_CHANGE                    dhcp_state
3d21h:    336149.404    CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS         10.1.1.20
NOTE—TFTP Server address
3d21h:    336149.404    CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS        10.1.1.10
3d21h:    336149.404    CMAC_LOG_DHCP_TOD_SERVER_ADDRESS         10.1.1.20
3d21h:    336149.404    CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
3d21h:    336149.404    CMAC_LOG_DHCP_TZ_OFFSET                  0
3d21h:    336149.408    CMAC_LOG_DHCP_CONFIG_FILE_NAME           platinum.cm
3d21h:    336149.408    CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
3d21h:    336149.408    CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRES
3d21h:    336149.408    CMAC_LOG_DHCP_COMPLETE
3d21h:    336149.420    CMAC_LOG_STATE_CHANGE                    establish_tod_state
3d21h:    336149.424    CMAC_LOG_TOD_REQUEST_SENT                10.1.1.20
3d21h:    336149.436    CMAC_LOG_TOD_REPLY_RECEIVED              3178345052
3d21h:    336149.436    CMAC_LOG_TOD_COMPLETE
3d21h:    336149.440    CMAC_LOG_STATE_CHANGE                    security_association_
                                                                 state
3d21h:    336149.440    CMAC_LOG_SECURITY_BYPASSED
3d21h:    336149.440    CMAC_LOG_STATE_CHANGE                    configuration_file
3d21h:    336149.440    CMAC_LOG_LOADING_CONFIG_FILE             platinum.cm
133.CABLEMODEM.CISCO: 3d21h: %LINEPROTO-5-UPDOWN: Line protocol on Interface cap
3d21h:    336163.252    CMAC_LOG_RNG_REQ_TRANSMITTED
3d21h:    336163.252    CMAC_LOG_RNG_RSP_MSG_RCVD
NOTE—TFTP process failing:
3d21h:    336165.448    CMAC_LOG_CONFIG_FILE_TFTP_FAILED         -1
3d21h:    336165.448    CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
3d21h:    336165.452    CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
3d21h:    336165.452    CMAC_LOG_STATE_CHANGE                    reset_interface_state
```

Time of Day（TOD; 時刻）またはタイミング オフセットの取得に関する問題がある場合も、ケーブル モデムはオンライン ステータスに達しません。

```
3d21h:    338322.500   CMAC_LOG_STATE_CHANGE                    dhcp_state
3d21h:    338334.260   CMAC_LOG_RNG_REQ_TRANSMITTED
3d21h:    338334.260   CMAC_LOG_RNG_RSP_MSG_RCVD
3d21h:    338335.424   CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS         10.1.1.20
3d21h:    338335.424   CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS        10.10.10.1
3d21h:    338335.424   CMAC_LOG_DHCP_ERROR_ACQUIRING_TOD_ADDRESS
3d21h:    338335.424   CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
3d21h:    338335.424   CMAC_LOG_DHCP_ERROR_ACQUIRING_TZ_OFFSET
3d21h:    338335.424   CMAC_LOG_DHCP_CONFIG_FILE_NAME            platinum.cm
3d21h:    338335.428   CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
3d21h:    338335.428   CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRESS
3d21h:    338335.428   CMAC_LOG_DHCP_COMPLETE
```

```
3d21h:    338335.428    CMAC_LOG_RESET_DHCP_FAILED
3d21h:    338335.432    CMAC_LOG_STATE_CHANGE                    reset_interface_state
3d21h:    338335.432    CMAC_LOG_STATE_CHANGE                    reset_hardware_state
3d21h:    338336.016    CMAC_LOG_STATE_CHANGE                    wait_for_link_up_state
```

(注)　Cisco IOS バージョン 12.1(1) よりも前のバージョンでは、ケーブル モデムをオンラインにするために、TOD を DHCP サーバで指定する必要がありました。しかし、Cisco IOS バージョン 12.1(1) 以降では TOD は必要ありません。ただし、ケーブル モデムでは、次に示すように引き続きタイミング オフセットを取得する必要があります。

```
344374.528     CMAC_LOG_STATE_CHANGE                        dhcp_state
344377.292     CMAC_LOG_RNG_REQ_TRANSMITTED
344377.292     CMAC_LOG_RNG_RSP_MSG_RCVD
344387.412     CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS             10.1.1.20
344387.412     CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS            10.10.10.1
NOTE— TOD server IP address obtained:
344387.412     CMAC_LOG_DHCP_TOD_SERVER_ADDRESS             10.10.10.1
344387.412     CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
NOTE— Timing offset not specified in DHCP server:
344387.412     CMAC_LOG_DHCP_ERROR_ACQUIRING_TZ_OFFSET
344387.412     CMAC_LOG_DHCP_CONFIG_FILE_NAME               platinum.cm
344387.412     CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
344387.412     CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRESS
344387.412     CMAC_LOG_DHCP_COMPLETE
344387.412     CMAC_LOG_RESET_DHCP_FAILED
NOTE—Modem resetting:
344387.412     CMAC_LOG_STATE_CHANGE                        reset_interface_state
```

次のデバッグではタイム サーバを指定していませんが、DHCP サーバでタイミング オフセットを設定しているので、ケーブル モデムはオンラインになります。

```
3d23h:    345297.516    CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS          10.1.1.20
3d23h:    345297.516    CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS          172.17.110.136
3d23h:    345297.516    CMAC_LOG_DHCP_ERROR_ACQUIRING_TOD_ADDRESS
3d23h:    345297.516    CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
3d23h:    345297.516    CMAC_LOG_DHCP_TZ_OFFSET                    0
3d23h:    345297.516    CMAC_LOG_DHCP_CONFIG_FILE_NAME             platinum.cm
3d23h:    345297.520    CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
3d23h:    345297.520    CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRESS
3d23h:    345297.520    CMAC_LOG_DHCP_COMPLETE
3d23h:    345297.532    CMAC_LOG_STATE_CHANGE                      establish_tod_state
3d23h:    345297.532    CMAC_LOG_TOD_NOT_REQUESTED_NO_TIME_ADDR
3d23h:    345297.532    CMAC_LOG_STATE_CHANGE                      security_association_
                                                                    state
```

```
3d23h:    345297.536    CMAC_LOG_SECURITY_BYPASSED
3d23h:    345297.536    CMAC_LOG_STATE_CHANGE                    configuration_file
3d23h:    345297.536    CMAC_LOG_LOADING_CONFIG_FILE             platinum.cm
3d23h:    345297.568    CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
3d23h:    345297.568    CMAC_LOG_STATE_CHANGE                    registration_state
3d23h:    345297.592    CMAC_LOG_REG_RSP_MSG_RCVD
3d23h:    345297.592    CMAC_LOG_COS_ASSIGNED_SID                1/7
3d23h:    345297.596    CMAC_LOG_RNG_REQ_QUEUED                  7
3d23h:    345297.596    CMAC_LOG_REGISTRATION_OK
3d23h:    345297.596    CMAC_LOG_STATE_CHANGE                    establish_privacy_sta
                                                                 te
3d23h:    345297.596    CMAC_LOG_PRIVACY_NOT_CONFIGURED
3d23h:    345297.596    CMAC_LOG_STATE_CHANGE                    maintenance_state
133.CABLEMODEM.CISCO: 3d23h: %LINEPROTO-5-UPDOWN: Line protocol on Interface changed
state to up
```

DHCP サーバで Router オプション設定を含めなかったり、Router オプション フィールドで無効な IP アドレスを指定したりした場合にも、ケーブル モデムが init(i) 状態から先に進まなくなります。これを次の **debug cable-modem mac log verbose** の出力結果に示します。

```
1d16h:    146585.940    CMAC_LOG_CONFIG_FILE_TFTP_FAILED         -1
1d16h:    146585.940    CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
1d16h:    146585.944    CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
1d16h:    146585.944    CMAC_LOG_STATE_CHANGE                    reset_interface_state
1d16h:    146585.944    CMAC_LOG_STATE_CHANGE                    reset_hardware_state
```

TOD 交換：init(t) 状態

モデムは、ネットワーク パラメータを取得した後に、Time Of Day（TOD; 時刻）サーバの時刻を要求する必要があります。TOD は UTC タイムスタンプ（1970 年 1 月 1 日からの秒数）を使用します。DHCP からのタイム オフセット オプション値を組み合せると、現在時刻を計算できます。時刻は、syslog とイベント ログのタイムスタンプに使用されます。

次の例では、SID 1 および 2 のモデムが init(t) 状態にあります。Cisco IOS バージョン 12.1(1) よりも後の IOS では、TOD 交換に失敗した場合でもケーブル モデムがオンラインになります。次の **show cable modem** コマンドの出力結果を参照してください。

#show cable modem

```
Interface Prim      Online      Timing    Rec     QoS    CPE   IP address   MAC address
Sid                 State       Offset    Power
Cable2/0/U0 1       init(t)     2808      0.00    2      0     10.1.1.20     0030.96f9.65d9
Cable2/0/U0 2       init(t)     2809      0.25    2      0     10.1.1.21     0030.96f9.6605
Cable2/0/U0 3       init(i)     2810      -0.25   2      0     10.1.1.22     0050.7366.1e01
```

```
2d01h:    177933.712    CMAC_LOG_STATE_CHANGE                     dhcp_state
2d01h:    177933.716    CMAC_LOG_RNG_REQ_TRANSMITTED
2d01h:    177933.716    CMAC_LOG_RNG_RSP_MSG_RCVD
```

```
2d01h:    177946.596    CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS          10.1.1.20
2d01h:    177946.596    CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS          10.20.20.1
2d01h:    177946.596    CMAC_LOG_DHCP_TOD_SERVER_ADDRESS           10.30.30.1
2d01h:    177946.596    CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
2d01h:    177946.596    CMAC_LOG_DHCP_TZ_OFFSET                    0
2d01h:    177946.600    CMAC_LOG_DHCP_CONFIG_FILE_NAME             platinum.cm
2d01h:    177946.600    CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
2d01h:    177946.600    CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRESS
2d01h:    177946.600    CMAC_LOG_DHCP_COMPLETE
2d01h:    177946.612    CMAC_LOG_STATE_CHANGE                      establish_tod_state
2d01h:    177946.716    CMAC_LOG_RNG_REQ_TRANSMITTED
2d01h:    177946.716    CMAC_LOG_RNG_RSP_MSG_RCVD
133.CABLEMODEM.CISCO: 2d01h: %LINEPROTO-5-UPDOWN: Line protocol on Interface cap
2d01h:    177947.716    CMAC_LOG_RNG_REQ_TRANSMITTED
2d01h:    177947.716    CMAC_LOG_RNG_RSP_MSG_RCVD
2d01h:    177948.616    CMAC_LOG_TOD_REQUEST_SENT                  10.30.30.1
2d01h:    177948.716    CMAC_LOG_RNG_REQ_TRANSMITTED
2d01h:    177954.616    CMAC_LOG_TOD_REQUEST_SENT                  10.30.30.1
2d01h:    177954.716    CMAC_LOG_RNG_REQ_TRANSMITTED
2d01h:    177954.716    CMAC_LOG_RNG_RSP_MSG_RCVD
2d01h:    177960.616    CMAC_LOG_TOD_REQUEST_SENT                  10.30.30.1
2d01h:    177960.712    CMAC_LOG_RNG_REQ_TRANSMITTED
2d01h:    177960.716    CMAC_LOG_RNG_RSP_MSG_RCVD
2d01h:    177961.716    CMAC_LOG_RNG_REQ_TRANSMITTED
131.CABLEMODEM.CISCO: 2d01h: %UBR900-3-TOD_FAILED_TIMER_EXPIRED:TOD failed, but Cable
Interface proceeding to operational state
2d01h:    177986.616    CMAC_LOG_TOD_WATCHDOG_EXPIRED
2d01h:    177986.616    CMAC_LOG_STATE_CHANGE                      security_association_
                                                                   state
2d01h:    177986.616    CMAC_LOG_SECURITY_BYPASSED
2d01h:    177986.616    CMAC_LOG_STATE_CHANGE                      configuration_file
2d01h:    177986.620    CMAC_LOG_LOADING_CONFIG_FILE               platinum.cm
2d01h:    177986.644    CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
2d01h:    177986.644    CMAC_LOG_STATE_CHANGE                      registration_state
2d01h:    177986.644    CMAC_LOG_REG_REQ_MSG_QUEUED
2d01h:    177986.648    CMAC_LOG_REG_REQ_TRANSMITTED
2d01h:    177986.652    CMAC_LOG_REG_RSP_MSG_RCVD
2d01h:    177986.652    CMAC_LOG_COS_ASSIGNED_SID                  1/1
2d01h:    177986.656    CMAC_LOG_RNG_REQ_QUEUED                    1
NOTE— Modem online:
2d01h:    177986.656    CMAC_LOG_REGISTRATION_OK
2d01h:    177986.656    CMAC_LOG_STATE_CHANGE                      establish_privacy_
                                                                   statee
2d01h:    177986.656    CMAC_LOG_PRIVACY_NOT_CONFIGURED
2d01h:    177986.656    CMAC_LOG_STATE_CHANGE                      maintenance_state
2d01h:    177988.716    CMAC_LOG_RNG_REQ_TRANSMITTED
```

時刻のエラーは、ほとんどの場合、DHCP の設定に誤りがあることを示しています。TOD エラーにつながる設定の誤りには、次のものがあります。

- ゲートウェイ アドレスの誤設定
- 間違った TOD サーバ アドレス

タイム サーバへの PING を実行して、IP 接続性の問題がないこと、およびタイム サーバが使用可能であることを確認してください。

オプション ファイル転送開始：init(o) 状態

ケーブル モデムに対する設定および管理の主要インターフェイスは、プロビジョニング サーバからダウンロードした設定ファイルです。この設定ファイルには、ダウンストリーム チャネルとアップストリーム チャネルの識別情報および特性に加え、サービス クラス設定、ベースライン プライバシー設定、全般的な運用設定、ネットワーク管理情報、ソフトウェア アップグレード フィールド、フィルタ、およびベンダー固有の設定が含まれます。

ケーブル モデムが nit(o) 状態から先に進まない場合、通常は、ケーブル モデムが設定ファイルのダウンロードを開始したか、ダウンロードの準備ができているものの、ダウンロードが成功しなかったことを示しています。これには次の理由が考えられます。

- DOCSIS 設定ファイルが正しくない、壊れている、または見つからない。
- TFTP サーバが使用できないか IP 接続性がないため、TFTP サーバに到達できない。
- DOCSIS ファイル内の構成パラメータが無効であるか、または見つからない。
- TFTP サーバのファイル アクセス権が間違っている。

状態として必ずしも init(o) が示されるとは限らず、init(i) の後に init(r1) から init(i) までが循環することもあるので注意してください。より正確な状態を判断するには、**show controller cable-modem 0 mac state** の出力を表示します。

この表示の一部を次に示します。

```
#show controller cable-modem 0 mac state

MAC State:                 configuration_file_state
Ranging SID:               4
Registered:                FALSE
Privacy Established:       FALSE
```

show cable modem の出力に init(o) が表示されるときに **debug cable-modem mac log verbose** を実行しても、設定ファイルが壊れているのか、または TFTP サーバの障害が原因なのかはわかりません。このデバッグはこれらの両方を指摘しています。

Cisco Broadband Configurator（cisco.com からのダウンロードで入手可能）における無効な構成パラメータの例として、ベンダー ID やベンダー固有情報が無効または見つからないことが挙げられます。この場合、次の出力表示と類似した結果になります。

```
w3d:       880748.992   CMAC_LOG_STATE_CHANGE                    dhcp_state
1w3d:      880751.652   CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d:      880751.656   CMAC_LOG_RNG_RSP_MSG_RCVD
1w3d:      880761.876   CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS        10.1.1.20
1w3d:      880761.876   CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS        10.10.10.1
1w3d:      880761.876   CMAC_LOG_DHCP_TOD_SERVER_ADDRESS         10.10.10.1
```

```
1w3d:      880761.876   CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
1w3d:      880761.876   CMAC_LOG_DHCP_TZ_OFFSET                    0
NOTE—Corrupt configuration file:
1w3d:      880761.880   CMAC_LOG_DHCP_CONFIG_FILE_NAME             data.cm
1w3d:      880761.880   CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
1w3d:      880761.880   CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRESS
1w3d:      880761.880   CMAC_LOG_DHCP_COMPLETE
1w3d:      880761.892   CMAC_LOG_STATE_CHANGE                      establish_tod_state
1w3d:      880761.896   CMAC_LOG_TOD_REQUEST_SENT                  10.10.10.1
1w3d:      880761.904   CMAC_LOG_TOD_REPLY_RECEIVED                3180091733
1w3d:      880761.908   CMAC_LOG_TOD_COMPLETE
1w3d:      880761.908   CMAC_LOG_STATE_CHANGE                      security_association
                                                                   _state
1w3d:      880761.908   CMAC_LOG_SECURITY_BYPASSED
1w3d:      880761.912   CMAC_LOG_STATE_CHANGE                      configuration_file_
                                                                   state
1w3d:      880761.912   CMAC_LOG_LOADING_CONFIG_FILE               data.cm
1w3d:      880762.652   CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d:      880762.652   CMAC_LOG_RNG_RSP_MSG_RCVD
133.CABLEMODEM.CISCO: 00:13:07: %LINEPROTO-5-UPDOWN: Line protocol on Interface
cable-modem0, changed state to up
00:13:08:  788.004      CMAC_LOG_CONFIG_FILE_CISCO_BAD_TYPE        155
00:13:08:  788.004      CMAC_LOG_CONFIG_FILE_CISCO_BAD_TYPE        115
00:13:08:  788.004      CMAC_LOG_CONFIG_FILE_CISCO_BAD_TYPE        116
00:13:08:  788.004      CMAC_LOG_CONFIG_FILE_CISCO_BAD_ATTR_MAX_   128
                        LENG
00:13:08:  788.008      CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
00:13:08:  788.008      CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
```

online、online(d)、online(pk)、online(pt) 状態

次の状態は、ケーブル モデムがオンライン ステータスに達して、データの送受信が可能になったことを示します。

- online
- online(pk)
- online(pt)

一方、online(d) は、ケーブル モデムがオンラインになったものの、ネットワーク アクセスが拒否されたことを示します。

#show cable modem

```
Interface Prim    Online       Timing   Rec     QoS   CPE   IP address   MAC address
Sid               State        Offset   Power
Cable2/0/U0 4     online       2810     -0.75   6     0     10.1.1.20    0030.96f9.65d9
Cable2/0/U0 5     online(pt)   2290     0.25    5     0     10.1.1.25    0050.7366.2223
Cable2/0/U0 6     online(d)    2815     0.00    6     0     10.1.1.27    0001.9659.4461
```

online(d) になる原因は、通常、Cisco Broadband Configurator（cisco.com からのダウンロードで入手可能）の Radio Frequency info の下にある Network Access オプションが無効になっているためです。Network Access はデフォルトでは**有効**になっています。このことは、上の **show cable modem** の出力と、次の **debug cable-modem mac log verbose** の出力で確認できます。

```
04:11:34:   15094.700   CMAC_LOG_STATE_CHANGE                       dhcp_state
04:11:46:   15106.392   CMAC_LOG_RNG_REQ_TRANSMITTED
04:11:46:   15106.396   CMAC_LOG_RNG_RSP_MSG_RCVD
04:11:47:   15107.620   CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS           10.1.1.20
04:11:47:   15107.620   CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS           172.17.110.136
04:11:47:   15107.620   CMAC_LOG_DHCP_TOD_SERVER_ADDRESS            172.17.110.136
04:11:47:   15107.620   CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
04:11:47:   15107.620   CMAC_LOG_DHCP_TZ_OFFSET                     0
NOTE—Network Access disabled:
04:11:47:   15107.624   CMAC_LOG_DHCP_CONFIG_FILE_NAME              noaccess.cm
04:11:47:   15107.624   CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
04:11:47:   15107.624   CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRES
04:11:47:   15107.624   CMAC_LOG_DHCP_COMPLETE
04:11:47:   15107.636   CMAC_LOG_STATE_CHANGE                       establish_tod_state
04:11:47:   15107.640   CMAC_LOG_TOD_REQUEST_SENT                   172.17.110.136
04:11:47:   15107.648   CMAC_LOG_TOD_REPLY_RECEIVED                 3179226080
04:11:47:   15107.652   CMAC_LOG_TOD_COMPLETE
04:11:47:   15107.652   CMAC_LOG_STATE_CHANGE                       security_associatio
                                                                     n_state
04:11:47:   15107.652   CMAC_LOG_SECURITY_BYPASSED
04:11:47:   15107.652   CMAC_LOG_STATE_CHANGE                       configuration_file_
                                                                     state
04:11:47:   15107.652   CMAC_LOG_LOADING_CONFIG_FILE                noaccess.cm
133.CABLEMODEM.CISCO: 04:11:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface
cable-modem0, changed state to up
04:11:48:   15108.672   CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
04:11:48:   15108.672   CMAC_LOG_STATE_CHANGE                       registration_state
04:11:48:   15108.672   CMAC_LOG_REG_REQ_MSG_QUEUED
04:11:48:   15108.676   CMAC_LOG_REG_REQ_TRANSMITTED
04:11:48:   15108.680   CMAC_LOG_REG_RSP_MSG_RCVD
04:11:48:   15108.680   CMAC_LOG_COS_ASSIGNED_SID                   1/4
04:11:48:   15108.684   CMAC_LOG_RNG_REQ_QUEUED                     4
04:11:48:   15108.684   CMAC_LOG_NETWORK_ACCESS_DENIED
04:11:48:   15108.684   CMAC_LOG_REGISTRATION_OK
04:11:48:   15108.684   CMAC_LOG_STATE_CHANGE                       establish_privacy_
                                                                     state
04:11:48:   15108.684   CMAC_LOG_PRIVACY_NOT_CONFIGURED
04:11:48:   15108.684   CMAC_LOG_STATE_CHANGE                       maintenance_state
04:11:49:   15109.392   CMAC_LOG_RNG_REQ_TRANSMITTED
```

また、ケーブル モデムで **show controllers cable-modem 0 mac state** の出力を調べて確認することもできます。

(注)　この例は説明用であり、一部省略されています。

```
Config File:
    Network Access: FALSE <<<<<<<<<<<<<<<<<<<<< network access denied
Maximum CPEs:                    3
Baseline Privacy:
    Auth. Wait Timeout:          10
    Reauth. Wait Timeout:        10
    Auth. Grace Time:            600
    Op. Wait Timeout:            1
    Retry Wait Timeout:          1
    TEK Grace Time:              600
    Auth. Reject Wait Time:      60
COS  1:
    Assigned SId:                4
    Max Downstream Rate:         10000000
    Max Upstream Rate:           1024000
    Upstream Priority:           7
    Min Upstream Rate:           0
    Max Upstream Burst:          0
    Privacy Enable:              FALSE
```

online とは、ケーブル モデムがオンラインになり、Cisco uBR7246VXR と通信できるようになったことを意味します。Baseline Privacy Interface（BPI; ベースライン プライバシー インターフェイス）が有効でない場合、ケーブル モデムの初期化は成功したとみなし、オンライン ステータスはデフォルト状態となります。BPI が設定されている場合には、ステータス online(pk) が表示されてから、そのすぐ後に online(pt) が表示されます。次のデバッグ出力表示は、ケーブル モデム側で **debug cable-modem mac log verbose** コマンドを使用して得られた出力のうち、登録に関する部分だけを示しています。

```
5d03h:      445197.804   CMAC_LOG_STATE_CHANGE                 registration_state
5d03h:      445197.804   CMAC_LOG_REG_REQ_MSG_QUEUED
5d03h:      445197.812   CMAC_LOG_REG_REQ_TRANSMITTED
5d03h:      445197.816   CMAC_LOG_REG_RSP_MSG_RCVD
5d03h:      445197.816   CMAC_LOG_COS_ASSIGNED_SID             1/4
5d03h:      445197.816   CMAC_LOG_RNG_REQ_QUEUED               4
5d03h:      445197.816   CMAC_LOG_REGISTRATION_OK
5d03h:      445197.816   CMAC_LOG_STATE_CHANGE                 establish_privacy_state
5d03h:      445197.820   CMAC_LOG_PRIVACY_FSM_STATE_CHANGE
machine: KEK, event/state: EVENT_1_PROVISIONED/STATE_A_START, new state:
STATE_B_AUTH_WAIT
5d03h:      445197.828   CMAC_LOG_BPKM_REQ_TRANSMITTED
```

```
5d03h:      445197.848   CMAC_LOG_BPKM_RSP_MSG_RCVD
5d03h:      445197.848   CMAC_LOG_PRIVACY_FSM_STATE_CHANGE
machine: KEK, event/state: EVENT_3_AUTH_REPLY/STATE_B_AUTH_WAIT, new state:
STATE_C_AUTHORIZED
5d03h:      445198.524   CMAC_LOG_PRIVACY_FSM_STATE_CHANGE
machine: TEK, event/state: EVENT_2_AUTHORIZED/STATE_A_START, new state: STATE_B_OP_WAIT
5d03h:      445198.536   CMAC_LOG_RNG_REQ_TRANSMITTED
5d03h:      445198.536   CMAC_LOG_RNG_RSP_MSG_RCVD
5d03h:      445198.536   CMAC_LOG_BPKM_REQ_TRANSMITTED
5d03h:      445198.536   CMAC_LOG_BPKM_RSP_MSG_RCVD
5d03h:      445198.540   CMAC_LOG_PRIVACY_FSM_STATE_CHANGE
machine: TEK, event/state: EVENT_8_KEY_REPLY/STATE_B_OP_WAIT, new state:
STATE_D_OPERATIONAL
5d03h:      445198.548   CMAC_LOG_PRIVACY_INSTALLED_KEY_FOR_SID 4
5d03h:      445198.548   CMAC_LOG_PRIVACY_ESTABLISHED
5d03h:      445198.552   CMAC_LOG_STATE_CHANGE                    maintenance_state
5d03h:      445201.484   CMAC_LOG_RNG_REQ_TRANSMITTED
5d03h:      445201.484   CMAC_LOG_RNG_RSP_MSG_RCVD
```

一般に、BPI に問題がある場合は、鍵認証の段階を通過できなかったことを示す reject(pk) が表示されます。この状態については、reject(pk) および reject (pt) の項で取り上げています。

BPI を正常に機能させるため、必ず Cisco uBR7246VXR とケーブル モデムの両方で BPI 対応イメージを実行してください。BPI 対応イメージ名には記号 **K1** が含まれています。

また、Cisco Broadband Configurator（cisco.com からのダウンロードで入手可能）の Class of Service オプションの下で、必ず **Baseline Privacy Enable** フィールドに 1 を設定してください。Cisco uBR7246VXR では BPI 対応イメージを実行していて、ケーブル モデムでは実行していない場合、Cisco Broadband Configurator で BPI を有効にすると、ケーブル モデムが online と offline の間を循環します。

reject(pk) および reject(pt) 状態

次に示す Cisco uBR7246VXR での **show cable modem** の出力は、reject(pk) 状態を示しています。

#show cable modem

```
Interface Prim    Online       Timing    Rec     QoS    CPE   IP address   MAC address
Sid               State        Offset    Power
Cable2/0/U0 2     reject(pk)   2812      0.00    6      0     10.1.1.20    0030.96f9.65d9
```

```
01:58:51: %UBR7200-5-UNAUTHSIDTIMEOUT: CMTS deleted BPI unauthorized Cable Modem
0030.96f9.65d9
```

BPI の設定に問題があると、多くの場合、reject(pk) 状態が表示されます。一般に、この状態は次の原因によって起こります。

- 認証要求に含まれる CM の公開鍵が壊れている。イベントの正しい順序については、サンプルの debug cable privacy を参照してください。
- cable privacy authenticate-modem 設定コマンドが CMTS ルータには存在するが、RADIUS サーバには存在しない。
- RADIUS サーバの設定が適切でない。

Reject(pt) は、通常、無効な Traffic Encryption Key（TEK; トラフィック暗号化鍵）が原因となって起こります。Cisco uBR7246VXR の **debug cable privacy** を使用した出力表示を次に示します。

```
02:32:08: CMTS Received AUTH REQ.
02:32:08: Created a new CM key for 0030.96f9.65d9.
02:32:08: CMTS generated AUTH_KEY.
02:32:08: Input : 70D158F106B0B75
02:32:08: Public Key:
02:32:08: 0x0000: 30 68 02 61 00 DA BA 93 3C E5 41 7C 20 2C D1 87
02:32:08: 0x0010: 3B 93 56 E1 35 7A FC 5E B7 E1 72 BA E6 A7 71 91
02:32:08: 0x0020: F4 68 CB 86 A8 18 FB A9 B4 DD 5F 21 B3 6A BE CE
02:32:08: 0x0030: 6A BE E1 32 A8 67 9A 34 E2 33 4A A4 0F 8C DB BD
02:32:08: 0x0040: D0 BB DE 54 39 05 B0 E0 F7 19 29 20 8C F9 3A 69
02:32:08: 0x0050: E4 51 C6 89 FB 8A 8E C6 01 22 02 34 C5 1F 87 F6
02:32:08: 0x0060: A3 1C 7E 67 9B 02 03 01 00 01
02:32:08: RSA public Key subject:
02:32:08: 0x0000: 30 7C 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05
02:32:08: 0x0010: 00 03 6B 00 30 68 02 61 00 DA BA 93 3C E5 41 7C
02:32:08: 0x0020: 20 2C D1 87 3B 93 56 E1 35 7A FC 5E B7 E1 72 BA
02:32:08: 0x0030: E6 A7 71 91 F4 68 CB 86 A8 18 FB A9 B4 DD 5F 21
02:32:08: 0x0040: B3 6A BE CE 6A BE E1 32 A8 67 9A 34 E2 33 4A A4
02:32:08: 0x0050: 0F 8C DB BD D0 BB DE 54 39 05 B0 E0 F7 19 29 20
02:32:08: 0x0060: 8C F9 3A 69 E4 51 C6 89 FB 8A 8E C6 01 22 02 34
02:32:08: 0x0070: C5 1F 87 F6 A3 1C 7E 67 9B 02 03 01 00 01
02:32:08: RSA encryption result = 0
02:32:08: RSA encrypted output:
02:32:08: 0x0000: B6 CA 09 93 BF 2C 05 66 9D C5 AF 67 0F 64 2E 31
02:32:08: 0x0010: 67 E4 2A EA 82 3E F7 63 8F 01 73 10 14 4A 24 ED
02:32:08: 0x0020: 65 8F 59 D8 23 BC F3 A8 48 7D 1A 08 09 BF A3 A8
02:32:08: 0x0030: D6 D2 5B C4 A7 36 C4 A9 28 F0 6C 5D A1 3B 92 A2
02:32:08: 0x0040: BC 99 CC 1F C9 74 F9 FA 76 83 ED D5 26 B4 92 EE
02:32:08: 0x0050: DD EA 50 81 C6 29 43 4F 73 DA 56 C2 29 AF 05 53
02:32:08: CMTS sent AUTH response.
02:32:08: CMTS Received TEK REQ.
02:32:08: Created a new key for SID 2.
02:32:08: CMTS sent KEY response.
```

認証が失敗したときのケーブル モデムでのデバッグ出力例を次に示します。

```
6d02h:      527617.480   CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
6d02h:      527617.480   CMAC_LOG_STATE_CHANGE                  registration_state
6d02h:      527617.484   CMAC_LOG_REG_REQ_MSG_QUEUED
6d02h:      527617.488   CMAC_LOG_REG_REQ_TRANSMITTED
6d02h:      527617.492   CMAC_LOG_REG_RSP_MSG_RCVD
6d02h:      527617.492   CMAC_LOG_COS_ASSIGNED_SID              1/2
6d02h:      527617.492   CMAC_LOG_RNG_REQ_QUEUED                2
6d02h:      527617.492   CMAC_LOG_REGISTRATION_OK
6d02h:      527617.496   CMAC_LOG_STATE_CHANGE                  establish_privacy_state
6d02h:      527617.496   CMAC_LOG_PRIVACY_FSM_STATE_CHANGE
machine: KEK, event/state: EVENT_1_PROVISIONED/STATE_A_START, new state:
STATE_B_AUTH_WAIT
6d02h:      527617.504   CMAC_LOG_BPKM_REQ_TRANSMITTED
6d02h:      527617.504   CMAC_LOG_BPKM_RSP_MSG_RCVD
6d02h:      527617.508   CMAC_LOG_PRIVACY_FSM_STATE_CHANGE
machine: KEK, event/state: EVENT_2_AUTH_REJECT/STATE_B_AUTH_WAIT, new state:
STATE_E_AUTH_REJ_WAIT
129.CABLEMODEM.CISCO: 6d02h: %CMBPKM-1-AUTHREJECT: Authorization request rejected by
CMTS: Unauthorized CM
6d02h:      527618.588   CMAC_LOG_RNG_REQ_TRANSMITTED
6d02h:      527618.592   CMAC_LOG_RNG_RSP_MSG_RCVD
```

同様に、Cisco uBR7246VXR での **debug cable privacy** は次のエラーを示します。

```
02:47:00: CMTS Received AUTH REQ.
02:47:00: Sending KEK REJECT.
02:47:05: %UBR7200-5-UNAUTHSIDTIMEOUT: CMTS deleted BPI unauthorized Cable Modem
0030.96f9.65d9
```

(注) ケーブル モデムは reject(pk) から init(r1) までを無限に循環し続けます。

これ以外に発生する可能性があるエラーとしては、暗号化のエクスポート制限によるものがあり、一部のベンダーのモデムでは Cisco uBR7246VXR のインターフェイス設定で次のコマンドが必要になることがあります。

```
(config-if)#cable privacy 40-bit-des
```

登録：reject (m) 状態

設定後に、ケーブル モデムは必要な設定のサブセットと共に登録要求（REG-REQ）を送信し、ケーブル モデムと uBR7246 の Message Integrity Check（MIC; メッセージの完全性チェック）も送信します。ケーブル モデムの MIC は設定ファイルの設定をハッシュ計算した結果であり、設定ファイルが中継時に改ざんされなかったことをケーブル モデムが確認する手段を提供します。Cisco uBR7246VXR の MIC も類似していますが、cable shared-secret 認証文字列用の設定も含まれる点で異なります。この共有秘密情報は Cisco uBR7246VXR およびプロビジョニング サーバによって認識され、プロビジョニング サーバによって認証されたケーブル モデムだけがルータへの登録を許可されることを保証します。

reject(m) 状態となるケーブル モデムには、不正な MIC があります。これは、通常、次の理由によって発生します。

- ケーブル インターフェイスのもとで設定された cable shared-secret と、Cisco Broadband Configurator（cisco.com からダウンロード可能）の Miscellaneous オプションの下にある CMTS Authentication 値が一致しない。
- 設定ファイル（DOCSIS ファイル）が壊れている。

問題を修正するには、設定ファイルが有効であることを確認し、**CMTS Authentication** の値と、ケーブル インターフェイスの **cable shared-secret <line>** で設定されている値が同一であることを確認してください。また、Cisco uBR7246VXR でサービス クラス プロファイルの作成が許可されていることを確認するか、あるいは Cisco uBR7246VXR によって作成されたプロファイルを使用します。

登録：reject (c) 状態

ケーブル モデムは、不正な Class of Service（COS; サービス クラス）が原因で登録に失敗すると、reject(c) 状態になります。通常は次の原因で起こります。

- uBR7246 が要求された特定の COS を与えることができない、または与えようとしない。
- Cisco Broadband Configurator（cisco.com からのダウンロードで入手可能）の Class of Service オプションにあるパラメータの設定が間違っている。たとえば、同じ ID を持つサービス クラスが 2 つあるなど。

ケーブル モデム側で得られた次の **debug cable-modem mac log verbose** の出力結果は、不正な COS が原因で登録に失敗したことを示しています。

```
w3d:      885643.820    CMAC_LOG_STATE_CHANGE                 registration_state
1w3d:     885643.820    CMAC_LOG_REG_REQ_MSG_QUEUED
1w3d:     885643.824    CMAC_LOG_REG_REQ_TRANSMITTED
1w3d:     885643.828    CMAC_LOG_REG_RSP_MSG_RCVD
1w3d:     885643.828    CMAC_LOG_SERVICE_NOT_AVAILABLE        0x01,0x01,0x01
1w3d:     885643.828    CMAC_LOG_RESET_SERVICE_NOT_AVAILABLE
1w3d:     885643.828    CMAC_LOG_STATE_CHANGE                 reset_interface_state
1w3d:     885643.832    CMAC_LOG_STATE_CHANGE                 reset_hardware_state
1w3d:     885644.416    CMAC_LOG_STATE_CHANGE                 wait_for_link_up_state
1w3d:     885644.420    CMAC_LOG_DRIVER_INIT_IDB_RESET        0x8039E23C
1w3d:     885644.420    CMAC_LOG_LINK_DOWN
1w3d:     885644.420    CMAC_LOG_LINK_UP
1w3d:     885644.420    CMAC_LOG_STATE_CHANGE                 ds_channel_scanning_state
133.CABLEMODEM.CISCO:
1w3d:     %LINEPROTO-5-UPDOWN: Line protocol on Interface cable-modem0, changed state
          to down
1w3d:     885645.528    CMAC_LOG_UCD_MSG_RCVD                 1
1w3d:     885646.828    CMAC_LOG_DS_64QAM_LOCK_ACQUIRED       453000000
```

同様に、Cisco uBR7246VXR での **debug cable registration** は次の内容を出力します。

```
sniper#debug cable registration
CMTS registration debugging is on
sniper#
1d04h: %UBR7200-5-CLASSFAIL: Registration failed for Cable Modem 0001.9659.4461 on
interface Cable2/0/U0:
Bad/Missing Class of Service Config in REG-REQ
```

最終的にケーブル モデムはリセットされ、最初から動作をやり直します。

CHAPTER 5

PacketCable 音声設定

この章では、PacketCable 音声を配備してサービスを提供するために必要となる、すべての作業について説明します。この章は、PacketCable の次の使用形態に関する情報を含んでいます。

- PacketCable EMTA のセキュア プロビジョニング（P.5-2）
- PacketCable EMTA の BASIC プロビジョニング（P.5-5）
- Euro-PacketCable（P.5-6）

また、PacketCable 音声技術の配備を妨げるおそれのある問題を解決するための情報も示します。

- eMTA プロビジョニングのトラブルシューティング（P.5-8）
- トラブルシューティングのツール（P.5-12）
- トラブルシューティングのシナリオ（P.5-13）
- 証明書信頼階層（P.5-17）

この章は、PacketCable MTA Device Provisioning Specification（PKT-SPPROV1.5-I01-050128）の内容を熟知している読者を対象としています。詳細については、www.packetcable.com を参照してください。

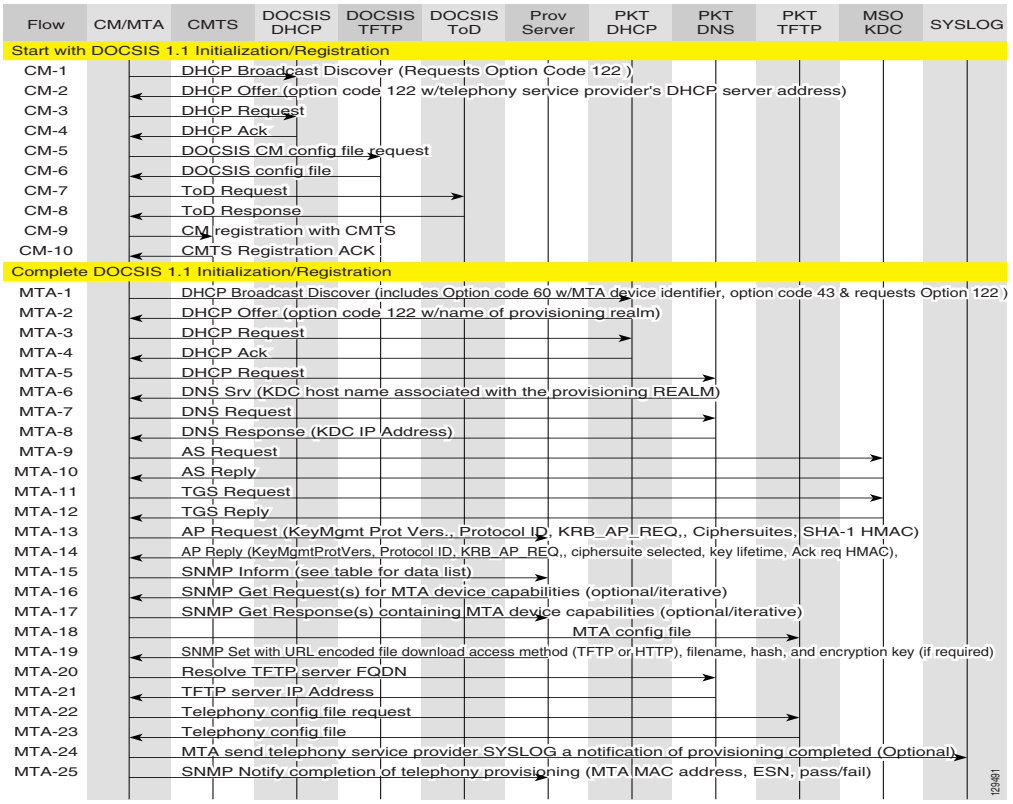
PacketCable EMTA のセキュア プロビジョニング

この項では、主にセキュアな PacketCable 音声プロビジョニングについて取り上げます。PacketCable Secure は、テレフォニー サービスの盗用や、悪意のあるサービス中断などが発生する可能性を最小限に抑えるように設計されています。PacketCable Secure では、Kerberos インフラストラクチャを利用して、MTA とプロビジョニング システムを相互に認証します。MTA とプロビジョニング システム間の対話をセキュリティで保護するために、SNMPv3 も使用されます。

BACC PacketCable のセキュアなプロビジョニングのフロー

PacketCable のプロビジョニングのすべてのフローは、一連のステップとして定義されます。EMTA プロビジョニングの問題点を診断するときは、ここで示すフロー説明を参考にすると、PacketCable プロビジョニング フローのどのステップが失敗しているかを特定できます。図 5-1 に、PacketCable 組み込み型 MTA のセキュアなプロビジョニングのフローを示します。

図 5-1　組み込み型 MTA のセキュアなプロビジョニングのフロー



(注)　データ パケットをキャプチャできるプロトコル アナライザ（プロトコル スニッファ）を使用して、どのステップが失敗しているかを正確に把握することを強くお勧めします。

また、KDC の障害の根本的な原因を把握するには、KDC ログ ファイルの内容が重要です。

1. CM-1 ～ 10：これは通常の DOCSIS CM ブート フローで、PacketCable DHCP サーバのリストを MTA に提供するための DHCP オプション 122 が付加されます。MTA は、これらの DHCP サーバから DHCP OFFER を受け付けられるようになります。
2. MTA-1 ～ 4：DHCP を使用して、MTA が自身を PacketCable MTA としてアナウンスし、どの機能およびプロビジョニング フロー（SECURE、BASIC など）をサポートしているかについて情報を提供します。MTA は、アドレス解決情報と DHCP オプション 122 も取得します。DHCP オプション 122 は、PacketCable ProvServ のアドレスとセキュリティ領域名を含んでいます。

   この情報は、MTA が KDC および ProvServer にアクセス可能になるために必要なものです。基本的なトラブルシューティングのヒントを次に示します。

   - CMTS 上で DHCP リレー エージェントが正しく設定されていることを確認する。CMTS が正しい 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 間のルーティングが正しいことを確認する。
   - セカンダリ サブネットが CMTS 上で正しく設定されていることを確認する。
   - Network Registrar の DHCP 設定が正しいことを確認する。スコープが設定され、IP アドレスが利用可能であり、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ます。
   - BACC の設定を確認する。cnr_ep.properties ファイルを確認して、必要な PacketCable CNR 拡張のプロパティが設定されていることを確認します。この properties ファイルの詳細については、付録 B「PacketCable DHCP オプションと BACC プロパティのマッピング」を参照してください。

     MTA がフロー ステップの MTA-1 ～ 2 を循環していることをパケット トレースで発見した場合は、DHCP オプション 122（領域名またはプロビジョニング サーバ FQDN のサブオプション）、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）の設定に問題がある可能性があります。これらのオプションは、すべて MTA にとって必須となる DHCP コンテンツです。
3. MTA-5 ～ 8：MTA が（DHCP オプション 122 で提供される）セキュリティ領域名を使用して、KDC サービスに対して DNS SRV ルックアップを実行し、KDC の IP アドレスを解決します。基本的なトラブルシューティングのヒントを次に示します。

   - パケット スニッファを使用して、Network Registrar DNS に送信される、送信先や形式が不正な DNS パケットを検出する。
   - Network Registrar DNS のログ レベルをパケット詳細トレースに設定して、Network Registrar DNS にどのようなパケットが到達するかを確認する。
   - DNS の設定を確認する。cnr_ep.properties に指定されている DNS サーバは、KDC の領域ゾーン、SRV レコード、および DNS「A」レコードを保持している必要があります。
4. MTA-9：AS_REQ 要求メッセージが KDC によって使用され、MTA が認証されます。基本的なトラブルシューティングのヒントを次に示します。

   - KDC のログ ファイルを確認して、AS_REQ が到達しているかどうかを特定し、エラーや警告がないことを確認する。
   - KDC が、正しい MTA_Root 証明書を使用して設定されていることを確認する。MTA が AS_REQ メッセージに添付して送信する製造業者証明書およびデバイス証明書は、KDC にインストールされている MTA_Root 証明書とチェーンを構成する必要があります。

5. FQDN_REQ および FQDN_REP（フローには示していません）：KDC が MTA の MAC アドレスを MTA 証明書から抽出して、検証のために ProvServ に送信します。ProvServ がこの MAC アドレスの FQDN を保持している場合は、FQDN が KDC に返されます。KDC は、MTA から受信した FQDN を FQDN_REP 応答メッセージで受信した FQDN と比較します。

   基本的なトラブルシューティングのヒントを次に示します。

   - パケット スニッファを使用して、送信先や形式が不正な DNS パケットを検出する。MTA は、（MTA が DHCP オプション 122 で受信した）ProvServ の FQDN を AS_REP メッセージ内で KDC に渡します。KDC は、この FQDN を使用して ProvServ 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する。DPE 内の KDC サービス キーは、KDC にあるサービス キーと一致している必要があります。KDC にあるサービス キー ファイルの名前は、非常に重要です。

6. MTA-10（AS_REP）：KDC がプロビジョニング サービス チケットを MTA に付与し、サービス プロバイダー証明書、ローカル システム プロバイダー証明書（オプション）、および KDC 証明書を MTA に送信します。MTA は、KDC によって送信された証明書が、MTA に格納されているサービス プロバイダー ルート証明書とチェーンを構成していることを確認します。これらの証明書がチェーンを構成していない場合、MTA はプロビジョニング フローのステップ MTA-1 に処理を戻します。KDC.cer ファイルの詳細については、P.12-42 の「KDC 証明書を管理するための PKCert.sh ツールの使用方法」を参照してください。基本的なトラブルシューティングのヒントを次に示します。

   - KDC のログ ファイルを表示して、AS_REP メッセージがデバイスに送信されたことを確認する。MTA がステップ MTA-1 ～ MTA-10 を循環していることをパケット トレースで発見した場合は、サービス プロバイダー証明書チェーンに問題があります。

7. MTA-13（AP_REQ）：MTA が、（MTA-10 で受信した）チケットを DHCP オプション 122 で指定されている ProvServ に提示します。

8. MTA-14（AP_REP）：ProvServ が KDC 共有秘密情報を使用して AP_REQ を復号化し、MTA の提示した ProvServ チケットを検証して、AP_REP を SNMPv3 キーを使用して送信します。以後の SNMPv3 は認証済みになり、必要な場合は暗号化されます。

9. MTA-15（SnmpV3 Inform）：MTA が、プロビジョニング情報を受信可能なことを ProvServ に通知します。

10. MTA-19（SNMPv3 SET）：ProvServ が、MTA 設定ファイルの URL、このファイルの暗号キー、およびこのファイルのハッシュ値を含んだ SNMPv3 SET を MTA に対して実行します。

11. MTA-22 ～ 23：MTA が、指定された TFTP サーバから VoIP 設定ファイルをダウンロードする処理を進めます。BACC によって、TFTP サーバが DPE コンポーネントに統合されていることに注意してください。

12. MTA-25（SnmpV3 Inform）：MTA が、新しい設定を受け付け可能かどうかを ProvServ に通知します。

PacketCable EMTA の BASIC プロビジョニング

BACC では、PacketCable BASIC もサポートしています。BASIC は、簡潔で DOCSIS に似た、ノンセキュアなプロビジョニング フローを提供します。

ここでは、BASIC.1 のフローについて説明します。

1. MTA-1：セキュアなフローと同様に実行されます。
2. MTA-2：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、プロビジョニング システムは、オプション 122 のサブオプション 6 を含んだ DHCP OFFER を返します。このサブオプションには、特殊な予約済み領域名「BASIC.1」が含まれています。この予約済み領域名は、MTA に対して BASIC.1 プロビジョニング フローを使用するように指示するものです。また、この OFFER はプロビジョニング システムの IP アドレスをオプション 122.3 に保持しており、file フィールドと siaddr フィールドに MTA 設定ファイルの位置が入力されています。
3. MTA-3、4：MTA DHCP 交換の残りの部分が実行されます（REQUEST および ACK が交換されます）。
4. MTA は、ステップ MTA-22 まで直接スキップします。file および siaddr の情報を使用して、MTA は設定ファイルをプロビジョニング システムから TFTP で取得します。

(注) MTA および ProvServ の認証や、暗号化は一切発生しません。

BASIC.2 フローは BASIC.1 と同一ですが、次の点が異なります。

- MTA の DHCP オプション 122 のサブオプション 6 に、「BASIC.2」が入力される。
- フローの最後となる MTA-25 で、MTA がプロビジョニング ステータス SNMPv2c INFORM を発行する（INFORM ターゲットは、DHCP オプション 122 のサブオプション 3 で指定されたもの）。

BASIC PacketCable フローは DOCSIS フローと似ていますが、次の点が異なります。

- MTA と プロビジョニング システムの間で ToD 交換が発生しない。
- MTA 設定ファイルの中に、完全性ハッシュが含まれている必要がある。具体的には、設定ファイルの内容全体の SHA1 ハッシュが pktcMtadevConfigFileHash SNMP varbind に入力され、End of File TLV の直前の TLV 11 内に配置されている必要があります。
- BASIC.2 フローは、MTA が設定ファイルを受信して処理した後に、プロビジョニング ステータス SNMPv2c INFORM を発行する。この INFORM は、MTA のプロビジョニングが正常に完了したかどうか、つまりプロビジョニングに問題がなかったかどうかを BACC に通知するものです。問題がある場合は、エラーが生成されて、イベントが DPE から RDU に送信され、次に BACC クライアントに送信されることがあります。この INFORM は、設定ファイルの問題点をデバッグする場合に特に役立ちます。

DOCSIS フローの詳細については、第 4 章「DOCSIS 設定」を参照してください。

(注) PacketCable BASIC プロビジョニング フローを使用する場合は、PacketCable BASIC 対応の eMTA を使用していることを事前に確認してください。eMTA は、BASIC に対応していることを DHCP DISCOVER のオプション 60、TLV 5.18（サポートされているフロー）で報告する必要があります。

PacketCable の TLV 38 と MIB のサポート

BACC は、一連の PacketCable 1.5 MIB を完全にサポートしています。

BACC 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 を使用して、複数の SNMP 通知ターゲットを設定できます。この TLV を設定すると、すべての通知が TLV 38 で設定したターゲットにも発行されます。

SNMP v2C 通知

BACC では、PacketCable MTA からの SNMP v2C TRAP 通知と SNMP v2C INFORM 通知の両方をサポートしています。

Euro-PacketCable

Euro-PacketCable サービスは、基本的には North American PacketCable サービスのヨーロッパ版にあたりますが、次の点が異なります。

- Euro-PacketCable では、使用する MIB が異なる。
- Euro-PacketCable では、使用するデバイス証明書（MTA_Root.cer）とサービス プロバイダー証明書（サービス プロバイダー ルート）のセットが異なる。

  Euro-PacketCable の証明書の場合は、kdc.ini に「euro-packetcable = true」プロパティが記述されている必要があります。詳細については、P.2-15 の「Euro-PacketCable のサポート」を参照してください。

  Euro-PacketCable を使用する場合は、PacketCable のプロパティ /pktcbl/prov/locale の値を必ず EURO に設定してください（デフォルトは NA（North America）です）。ロケールは、設定ファイル ユーティリティで指定することができます。詳細については、P.12-25 の「設定ファイル ユーティリティの使用方法」を参照してください。

Euro-PacketCable の MIB

Euro-PacketCable の MIB は、基本的にはドラフト IETF MIB のスナップショットです。MTA の設定ファイルは、MIB を参照する SNMPVarBind が基本的な構成要素です。PacketCable の MIB と Euro の MIB は大きく異なるため、PacketCable と Euro-PacketCable の設定ファイルには互換性がありません。インストール時に、PacketCable のサンプル ファイル（cw29_config.tmpl）と Euro-PacketCable のサンプル ファイル（ecw15_mta_config.tmpl）が <BACC_HOME>/rdu/samples ディレクトリにコピーされます。

BACC には、次の Euro-PacketCable MIB が付属しています。

- DOCS-IETF-BPI2-MIB
- INTEGRATED-SERVICES-MIB
- DIFFSERV-DSCP-TC
- DIFFSERV-MIB
- TCOMLABS-MIB
- PKTC-TCOMLABS-MTA-MIB
- PKTC-TCOMLABS-SIG-MIB

Euro-PacketCable の MIB の設定

Euro-PacketCable の MIB を使用するように BACC を設定するには、ロードされる MIB を指定している BACC 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、このプロパティは PacketCable の MIB を含んでいます。

この操作は、次のいずれかの方法で実行できます。

- rdu.properties を修正して、RDU を再起動する。
- 管理者のユーザ インターフェイスを使用する。Configuration > Defaults > System Defaults に移動して、MIB リストを下に示したリストに置き換えます。RDU を再起動する必要はありあません。
- Prov API の changeSystemDefaults() コールを使用する。RDU を再起動する必要はありあません。

プロパティの名前は、/snmp/mibs/mibList（properties ファイル）、または SNMPPropertyKeys.MIB_LIST（Prov API の定数の名前）です。プロパティの値はカンマ区切り形式（CSV）で、下に示す必要な MIB 名で構成されています。

```
/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-CABL
E-SPECTRUM-MIB,CISCO-DOCS-EXT-MIB,SNMP-FRAMEWORK-MIB,DOCS-CABLE-DEVICE-MIB,DOCS-CABLE-
DEVICE-MIB-OBSOLETE,DOCS-QOS-MIB,CISCO-CABLE-MODEM-MIB,DOCS-IETF-BPI2-MIB,INTEGRATED-S
ERVICES-MIB,DIFFSERV-DSCP-TC,DIFFSERV-MIB,TCOMLABS-MIB,PKTC-TCOMLABS-MTA-MIB,PKTC-TCOM
LABS-SIG-MIB
```

eMTA プロビジョニングのトラブルシューティング

PacketCable 組み込み型メディア ターミナル アダプタ（eMTA）のプロビジョニングは、比較的複雑なプロセスです。ただし、適切なツールと方法を使用することで、ごく簡単に eMTA を運用可能にすることができます。

この章では、Network Registrar と BACC の両方を使用していることを前提としています。ただし、情報の多くはこれ以外の配備状態にも適用されます。また、Network Registrar の基礎知識（スコープ、ポリシー、基本的な DNS ゾーン設定、およびレコード エントリ）と BACC の基礎知識（サービス クラス、DHCP 基準、外部ファイル、および BACC ディレクトリ構造）があることを前提としています。

PacketCable eMTA のプロビジョニング プロセスは、セキュアなフローの場合は 25 ステップで構成されます。BASIC フローでは、ステップの数はかなり少なくなります。eMTA をトラブルシューティングするには、PacketCable プロビジョニング仕様に基づいたこれらの 25 ステップに関する知識が不可欠です。

この項では、次のトピックについて取り上げます。

- コンポーネント（P.5-8）
- 基本変数（P.5-10）

コンポーネント

eMTA をトラブルシューティングする前に、以降の項で説明する次のシステム コンポーネントについて理解する必要があります。

- 組み込み型メディア ターミナル アダプタ
- DHCP サーバ
- DNS サーバ
- 鍵発行局
- PacketCable プロビジョニング サーバ
- Call Management Server

組み込み型メディア ターミナル アダプタ

eMTA は、ケーブル モデム（CM）とメディア ターミナル アダプタ（MTA）を、よく利用されるソフトウェア イメージとともに 1 つのボックスに組み込んだものです。CM と MTA はいずれも固有の MAC アドレスを持っており、それぞれが DHCP を実行して固有の IP アドレスを取得します。eMTA は、少なくとも 3 つの証明書を保持しています。証明書の 1 つは、一意の MTA 証明書です。2 番目の証明書は、MTA の製造業者を識別するものです。デバイス証明書と製造業者証明書は、デバイスや製造業者を認証するために、いずれも MTA によって鍵発行局（KDC）に送信されます。3 番目の証明書は、KDC から MTA に送信される証明書を検証するためのテレフォニー ルート証明書です。KDC の証明書は、テレフォニー ルートを起点としてチェーンを構成するため、KDC 証明書の信頼性を検証するには、テレフォニー ルートが MTA 上に存在している必要があります。MTA 部分は、MTA を制御するコール エージェントを識別するための固有の設定ファイルを受信します。

DHCP サーバ

DOCSIS 仕様では、ケーブル モデムが自身の IP アドレスをダイナミック ホスト コンフィギュレーション プロトコル（DHCP）を使用してネゴシエートするように規定されています。MTA は、DOCSIS ネットワーク上のほとんどの CPE と同様に、DHCP を使用して自身の IP アドレスおよびその他の必須情報（DNS サーバ、Kerberos 領域名のための PacketCable オプション 122、プロビジョニング サーバの FQDN）を取得する必要があります。

（注） ケーブル モデム部分は、通常の必須 DHCP オプションに加えて、オプション 122 のサブオプション 1 も要求して取得する必要があります。このサブオプションは、オファーの送信元となる適切な DHCP サーバの IP アドレスとして、ケーブル モデム部分が MTA 部分に渡します。

PacketCable をサポートする BACC を使用すると、正しく設定した BACC は、オプション 122 フィールドに加えて、ToD サーバ、DNS サーバ、TFTP サーバのフィールドにも自動的に値を入力します。これらについて、Network Registrar ポリシーで明示的に設定する必要はありません。

DNS サーバ

ドメイン ネーム システム（DNS）サーバは、PacketCable のプロビジョニングに不可欠です。BACC アーキテクチャにおけるデバイス プロビジョニング エンジン（DPE）である PacketCable プロビジョニング サーバは、適切なゾーン内にアドレス（A）レコードを持っている必要があります。これは、このサーバの完全修飾ドメイン名（FQDN）が DHCP サーバによって MTA にオプション 122 で提供されるためです。KDC 領域は、Kerberos サーバの FQDN を記述したサーバ（SRV）レコードを含んでいる領域名と同じ名前でゾーンを持っている必要があります。

SRV レコードで指定される Kerberos サーバは、適切なゾーン内に自身の A レコードを持っている必要があります。MTA 設定ファイルで指定される Call Management Server（CMS）も、適切なゾーン内に A レコードを持っている必要があります。最後に、MTA 自体も適切なゾーン内に A レコードを持っている必要があります。これは、CMS は MTA の FQDN を解決することによって MTA に到達するためです。MTA の A レコードを作成する方法としては、ダイナミック DNS（DDNS）をお勧めします。DDNS の設定およびトラブルシューティングについては、Cisco Network Registrar のマニュアルを参照してください。

鍵発行局

KDC は、MTA の認証を担当します。このため、KDC は MTA の証明書を検証するとともに、MTA が KDC を認証できるように KDC 自身の証明書を提供する必要があります。また、KDC は DPE（プロビジョニング サーバ）と通信して、MTA がネットワーク上でプロビジョニングされていることを検証します。

PacketCable プロビジョニング サーバ

PacketCable プロビジョニング サーバは、SNMP を使用して MTA 設定ファイルの位置を MTA に伝達し、MTA のパラメータをプロビジョニングします。MTA とプロビジョニング サーバ間のすべての通信で、SNMPv3 が使用されます。SNMPv3 通信の開始に使用されるキーは、MTA によって、KDC との認証フェーズ中に取得されます。プロビジョニング サーバの機能は、BACC アーキテクチャにおける DPE によって提供されます。

Call Management Server

Call Management Server（CMS）は、基本的にはソフト スイッチ（コール エージェント）です。ケーブル ネットワーク上の QoS を制御するための追加の PacketCable 機能を備えています。PacketCable プロビジョニングが成功すると、MTA はネットワーク コール シグナリング（NCS）の Restart in Progress（RSIP）メッセージを CMS に送信します。

基本変数

この項では、eMTA の適切なプロビジョニングに必要となる基本変数について説明します。

- 証明書（P.5-10）
- スコープ選択タグ（P.5-11）
- MTA 設定ファイル（P.5-11）

証明書

MTA_Root.cer ファイルには、MTA ルート証明書（正式な PacketCable MTA ルートがルートになっている証明書）が含まれています。MTA_Root.cer は、通常は重大な問題を引き起こすことはありません。

プロビジョニングの対象となる MTA でどのテレフォニー ルート証明書が必要になるかについて、あらかじめ把握しておく必要があります。実稼働ネットワークへの配備では、実在の PacketCable ルートがルートになっているテレフォニー証明書を使用します。ルートには、ラボ環境およびテスト環境で使用される PacketCable テスト ルートもあります。KDC が自身を MTA に認証させるために使用する KDC 証明書は、MTA に格納されているものと同じテレフォニー ルート（PacketCable の実在ルートまたはテスト ルート）がルートになっている必要があります。MTA 製造業者のほとんどは、Telnet ログイン機能と HTTP ログイン機能の一方または両方を備えたテスト イメージをサポートしているため、どのテレフォニー ルートがイネーブルになっているかを特定して、使用されるルートを変更することができます（ほとんどの場合、選択できるのは PacketCable 実在ルートとテスト ルートのいずれかのみです）。

最も一般的なシナリオでは、次の証明書を（$BACC_HOME/kdc/solaris/packetcable/certificates ディレクトリから）ロードした KDC を使用します。

- CableLabs_Service_Provider_Root.cer
- Service_Provider.cer
- Local_System.cer
- KDC.cer
- MTA_Root.cer

最初の 4 つの証明書は、テレフォニー証明書チェーンを構成します。MTA_Root.cer ファイルは、MTA の送信する証明書を検証するために KDC が使用する MTA ルートを保持しています。

(注)　KDC 証明書のインストールおよび管理については、P.12-42 の「KDC 証明書を管理するための PKCert.sh ツールの使用方法」を参照してください。

PacketCable テスト ルートを現在使用しているかどうかを特定するには、CableLabs_Service_Provider_Root.cer ファイルを Windows で開いて、Subject OrgName エントリが **O = CableLabs** であることを確認するか、サブジェクト代替名が **CN=CABLELABS GENERATED TEST ROOT FOR EQUIPMENT TEST PURPOSES ONLY** と記述されていることを確認します。

KDC 証明書（KDC.cer）は、使用する領域名を保持しています。BACC（および対応する DNS ゾーン）で使用するように設定されている領域名は、この領域名と一致している必要があります。また、MTA 設定ファイルの領域オリジナル名が、テレフォニー ルート内にある組織名と一致している必要があります。

KDC 証明書は、対応する秘密鍵を持っています。この秘密鍵は、$BACC_HOME/kdc/solaris ディレクトリにインストールされている必要があります。秘密鍵の名前は、通常は KDC_private_key.pkcs8 または KDC_private_key_proprietary です。証明書を変更するときは、秘密鍵も変更する必要があります。

スコープ選択タグ

ほとんどのシナリオでは、BACC は、BACC 管理ユーザ インターフェイスの DHCP 基準ページで指定されている選択基準に一致しているスコープ選択タグを使用して、スコープからのすべての DHCP 要求の処理に関係します。クライアント クラスもスコープを BACC 処理に関連付けるために使用できます。この関連付けは、デバイスをプロビジョニングする前に実行する必要があります。

MTA 設定ファイル

MTA 設定ファイルは、CMS の位置を保持しています。また、領域名のエントリを保持している必要があります。この値は、使用中の証明書チェーンの値と一致している必要があります。

MTA 設定ファイル内の特定のテーブル エントリは、MTA にオプション 122 で配送された領域名に基づいてインデックス付けされます。MTA 設定ファイル内のこの領域名エントリは、オプション 122 で配送されたものと一致する必要があります。たとえば、オプション 122 で配送された領域名が **DEF.COM** であった場合、MTA 設定ファイルの pktcMtaDevRealm テーブルのエントリは、この領域名の ASCII 符号化文字値（Cisco Broadband Configurator を使用している場合はドット区切り 10 進形式）、68.69.70.46.67.79.77 で構成されるサフィックスを使用してインデックス付けされます。Web には、この変換を容易にする無料の ASCII 変換ページが多数存在しています。

トラブルシューティングのツール

PacketCable MTA Device Provisioning Specification に記述されている 25 の eMTA セキュア プロビジョニングのステップについては、図 5-1 に示しています。

この項では、次のトピックについて取り上げます。

- ログ（P.5-12）
- Ethereal、SnifferPro、およびその他のパケット キャプチャ ツール（P.5-12）

ログ

次に示すログ ファイルを使用して、次の情報が管理されています。

- Network Registrar の 2 つのログ（name_dhcp_1_log と name_dns_1_log）。Network Registrar の直近のいくつかのログ エントリを保持しています。DHCP または DNS に関する問題については、これらのファイルを調べてください。
- $BACC_HOME/kdc/logs/kdc.log ファイル。KDC と MTA とのインタラクション、および KDC と DPE とのインタラクションのすべてを記録しています。
- $BACC_DATA/dpe/logs/dpe.log ファイル。MTA との SNMPv3 インタラクションに関連する主なステップを記録しています。ハードウェア DPE に対して作業している場合は、**show log** CLI コマンドも使用できます。

（注） コマンドライン インターフェイスを使用して、SNMP、登録サーバ、および登録サーバの詳細メッセージのトレースを有効にしておくと、PacketCable に潜在的な問題があった場合のトラブルシューティングに役立ちます。適切なトラブルシューティング コマンドについては、『*Cisco Broadband Access Center for Cable Command Line Interface Reference*』を参照してください。

Ethereal、SnifferPro、およびその他のパケット キャプチャ ツール

eMTA のトラブルシューティングには、パケット キャプチャ ツールが不可欠です。CableLabs がパッケージ化している Ethereal バージョンには、PacketCable 固有の数多くのパケット デコーダが含まれています。これらには、Kerberos の AS パケットおよび AP パケットが含まれます。

- 特定の障害が DHCP に関係していると考えられる場合は、CMTS ケーブル インターフェイスの IP アドレスと DHCP サーバの IP アドレスを送信元または宛先とするパケットをフィルタリングしながら、パケットをキャプチャします。
- 特定の障害が、DHCP の後に発生する 25 ステップのいずれかに関係していると考えられる場合は、eMTA の IP アドレスを送信元または宛先とするパケットをすべてフィルタリングします。この方法では、図 5-1 に示したプロビジョニング ステップ 5 ～ 25 を単純な手順で容易にトレースできます。

トラブルシューティングのシナリオ

組み込み型 MTA に関して発生するおそれのある障害のシナリオを、表 5-1 に示します。

表 5-1　トラブルシューティングのシナリオ

発生する問題	考えられる原因	対処の方法
KDC が起動しない。	KDC 証明書が秘密鍵と対応していません。	互いに対応する証明書と秘密鍵があることを確認します。
	KDC ライセンスが有効期限切れであるか、見つかりません。	KDC ライセンスを $BACC_HOME/kdc ディレクトリに復元します。
MTA デバイスが BACC の Devices ページに表示されない。	不正なケーブル ヘルパー アドレスが設定されている可能性があります。	ヘルパー アドレスを修正します。
	スコープ選択タグが、BACC ユーザ インターフェイスで選択されている DHCPCriteria と一致しません。	MTA スコープ選択タグが、関係する MTA について BACC で作成した PacketCable DHCP 基準のスコープ選択タグと一致していることを確認します。
	Network Registrar 拡張ポイントが正しくインストールされていません。	Network Registrar 拡張ポイントを再インストールします。正しい手順については、『*Cisco Broadband Access Center for Cable Installation Guide*』を参照してください。
	ケーブル モデム部分がオプション 122 を受信しませんでした。	ケーブル モデム部分のスコープのタグが、BACC に設定されている DOCSIS DHCP 基準と一致していることを確認します。
MTA が DHCP オファーを受け付けず、DHCP フローを循環し続ける。	無効な DHCP オプションが設定されています。	スコープ ポリシーに DNS サーバ オプションが含まれていること、または cnr_ep.properties ファイルにプライマリ DNS サーバとセカンダリ DNS サーバのエントリが含まれていることを確認します。
	DHCP オファーが、ケーブル モデム部分のオプション 122 のサブオプション 1 で指定されているものとは別の DHCP サーバから送信された可能性があります。	cnr_ep.properties ファイルを確認して、プライマリとセカンダリの DHCP サーバが正しく設定されていることを確認します。
KDC.log ファイルと ethereal　トレースの両方が、MTA が KDC にアクセスしないことを示している。	cnr_ep.properties ファイルと MTA スコープ ポリシーの一方または両方で、不正な DNS サーバが指定されています。	cnr_ep.properties の DNS サーバを確認し、修正します。
	Kerberos 領域のゾーンが見つからないか、正しく設定されていません。	領域と同じ名前のゾーンが作成されていること、およびゾーンが「SRV」レコードを「_kerberos._udp 0 0 88 <KDC FQDN>」形式で保持していることを確認します。
	KDC の「A」レコード エントリが見つからないか、正しくありません。	Kerberos ゾーンの「SRV」レコードに含まれている FQDN について、「A」レコードが存在していることを確認します。
	DPE の FQDN を解決できません。	dpe.properties の provFQDNs エントリに、DPE の正しい FQDN と IP が記述されていることを確認します。

表 5-1　トラブルシューティングのシナリオ（続き）

発生する問題	考えられる原因	対処の方法
Kerberos の AS-Request 中に、KDC が障害を報告する。	MTA 証明書が、KDC によって使用されている MTA ルートと一致しません。	MTA_Root.cer を現用システムで使用されているものと比較して、MTA_Root.cer が適切なことを確認します。 適切なものである場合は、MTA 自体で証明書に関する問題が発生している可能性があります。この状況は非常にまれであり、該当する場合は MTA 製造業者に連絡してください。
	プロビジョニング サーバに対する KDC からの FQDN ルックアップが失敗しました。デバイスが、まだ BACC でプロビジョニングされていない可能性があります。	デバイスが表示されることを確認します。サービス クラスと DHCP 基準が与えられている必要があります。
	クロック スキュー エラー。詳細については、P.3-8 の「PacketCable チェックリスト」を参照してください。	すべての BACC ネットワーク要素が NTP を介してクロック同期していることを確認します。詳細については、『*Broadband Access Center for Cable Command Line Interface Reference*』を参照してください。
	KDC と DPE の間にミスマッチが存在している可能性があります。 **（注）** 他のデバイスが正しくプロビジョニングされている場合、これは問題の原因ではありません。	次の 3 つのエントリが、$BACC_HOME/kdc/solaris/keys ディレクトリに存在していることを確認します。 • mtafqdnmap,dpe.abc.com@DEF.COM • mtaprovsrvr,dpe.abc.com@DEF.COM • krbtgt,DEF.COM@DEF.COM システムに、この例と異なる DPE FQDN と領域名が保持されています。これらのエントリの内容は、dpe.properties の「KDCServiceKey」エントリ、または keygen ユーティリティを使用して生成されるキーに含まれているエントリと一致している必要があります。
KDC は AS-Request と AS-Reply（図 5-1 のステップ 9 とステップ 10）が成功したことを報告するが、MTA はステップ 9 より後に進まず、このステップまでを再プロビジョニングし続ける。	MTA でロードされているかイネーブルになっているテレフォニー ルートと、KDC でロードされているテレフォニー ルートとの間で、証明書のミスマッチが存在しています。	MTA と KDC の証明書を確認します。
	非常にまれですが、テレフォニー証明書チェーンが破損している可能性があります。 **（注）** 他のデバイスが正しくプロビジョニングされている場合、これは問題の原因ではありません。	MTA で正しい証明書がロードされているか、イネーブルになっていることを確認します。正常にプロビジョニングできているデバイスがまったくない場合は、KDC 上で別の証明書を試してみます。

表 5-1　トラブルシューティングのシナリオ（続き）

発生する問題	考えられる原因	対処の方法
AP Request と AP Reply（図 5-1 のステップ 14）が失敗する。	クロック スキュー エラー。詳細については、P.3-8 の「PacketCable チェックリスト」を参照してください。	すべての BACC ネットワーク要素が NTP を介してクロック同期していることを確認します。詳細については、『*Broadband Access Center for Cable Command Line Interface Reference*』を参照してください。
	プロビジョニング サーバの FQDN を解決できません。	プロビジョニング サーバ（DPE）の DNS エントリが正しいことを確認します。dpe.properties の provFQDNs エントリに、プロビジョニング サーバ（DPE）の正しい FQDN と IP が保持されていることを確認します。
	MTA から DPE に到達するルートが存在していません。	ルーティングの問題を解決します。
MTA が設定ファイルの TFTP 要求を発行しない。	DPE 上で実行されている TFTP サーバに到達するためのルートが存在していません。	ルーティングの問題を解決します。
MTA が TFTP 設定ファイルを受信しない。	設定ファイルが DPE でキャッシュされていません。	次のプロビジョニング試行でファイルがキャッシュされるまで、待機します。この方法で失敗する場合には、MTA をリセットします。
	Network Registrar の MTA スコープ ポリシーに、矛盾する TFTP サーバ オプションが含まれています。	TFTP サーバの DPE アドレスは BACC が挿入するため、このオプションはポリシーから削除しても問題ありません。
MTA は設定ファイルを受信するが、dpe.log ファイルを参照すると、DPE が SNMP Inform（図 5-1 のステップ 25）の受信に失敗している。	次のいずれかが発生しています。 • 設定ファイル内部での矛盾 • テレフォニー証明書チェーンの領域オリジナル名との矛盾 • オプション 122 で提供されている領域名との矛盾	MTA 設定ファイルに一貫性があることを確認します。
RSIP が送信されていないにもかかわらず、MTA が成功を報告する（図 5-1 のステップ 25）。	MTA が、MTA 設定ファイルで指定されている CMS FQDN の IP アドレスを解決できません。	CMS の DNS エントリが存在していることを確認します。
	MTA が CMS の IP アドレスに到達できません。これは、ルートが設定されていないことを示しています。	ルーティングの問題をすべて解決します。
CMS サービスのために KDC に再度アクセスしようとしているにもかかわらず、MTA が成功を報告する（図 5-1 のステップ 25）。	MTA 設定ファイルが誤ったケーブル モデムをポイントしています。	設定ファイルを修正するか、設定ファイルにリストされている FQDN を使用するように Cisco BTS 10200 を再設定します。
	MTA 設定ファイルの pktcMtaDevCmsIPsecCtrl 値が見つからないか、1 に設定されています。これは、MTA がセキュア NCS コール シグナリングを実行すること、または CMS FQDN の ASCII サフィックスと一致しない ASCII サフィックスを使用することを意味します。	設定ファイルを修正します。セキュア シグナリングを実行する場合は、必要な手順に従って、セキュア シグナリングをサポートするように KDC と BTS を設定します。

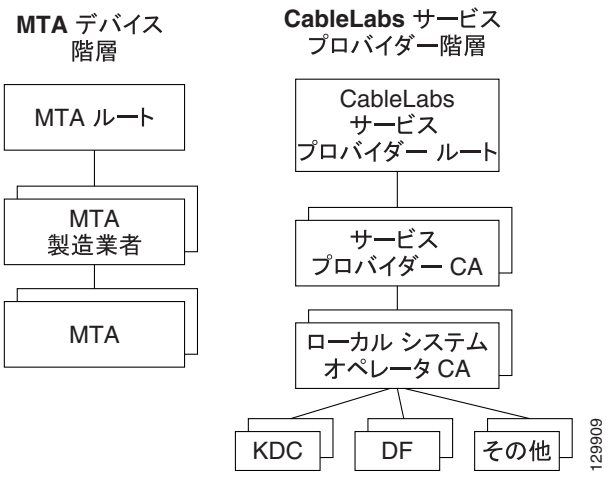
表 5-1　トラブルシューティングのシナリオ（続き）

発生する問題	考えられる原因	対処の方法
MTA が成功を報告して（図 5-1 のステップ 25）、RSIP を送信するが、ソフト スイッチからの応答がないか、応答としてエラーを受信する。	MTA が Cisco BTS 10200 上でプロビジョニングされていないか、不正にプロビジョニングされています。	MTA を Cisco BTS 10200 上でプロビジョニングします。
	eMTA の DNS エントリが存在していません。	適切な DNS ゾーンに eMTA のエントリを配置します。ダイナミック DNS を使用することをお勧めします。DDNS のイネーブル化については、Cisco Network Registrar のマニュアルを参照してください。

証明書信頼階層

BACC PacketCable には、図 5-2 に示すように、MTA デバイス証明書階層と CableLabs サービス プロバイダー証明書階層の 2 つの証明書階層があります。

図 5-2　PacketCable の証明書階層



BACC PacketCable の実装作業を行う前に、次の技術ドキュメントの内容を完全に理解しておく必要があります。

- *RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile*
- *DOCSIS Baseline Privacy Plus Interface Specification*（*SP-BPI+-I11-040407*、*2004 年 4 月 7 日*）

(注)

Euro-PacketCable は PacketCable のセキュリティ仕様（PKT-SP-SEC-I08-030415）を使用していますが、Euro-PacketCable 環境で使用されるデジタル証明書に関しては、変更の必要な部分があります。Euro-PacketCable と PacketCable を可能な限り類似したものにするため、Euro-PacketCable では、セキュリティ仕様の新しいリビジョン（PKTSP-SEC-I08-030415）を含めて、PacketCable のすべてのセキュリティ技術を使用しています。

Euro-PacketCable 証明書の要素で PacketCable 証明書と異なっているものについては、以降の表で示します。

Euro-PacketCable では、Euro-PacketCable 証明書が有効となる唯一の証明書です。
PKT-SP-SEC-I08-030415 で述べられている、PacketCable 証明書について言及している PacketCable のすべての要件は、対応する Euro-PacketCable 証明書の要件に変更されます。

Euro-PacketCable 対応の組み込み型 MTA では、DOCSIS CVC CA の公開鍵の代わりに、Euro-DOCSIS ルート CVC CA の公開鍵が CM の不揮発性メモリに格納されている必要があります。
Euro-PacketCable 対応の独立型 MTA では、不揮発性メモリに tComLabs CVC ルート証明書と tComLabs CVC CA 証明書が格納されている必要があります。製造業者の CVC は、証明書チェーンを検証することで検証されます。

証明書の検証

PacketCable 証明書の検証では、通常は証明書のチェーン全体が検証されます。たとえば、プロビジョニング サーバが MTA デバイス証明書を検証するときは、次の証明書チェーンが検証されます。

MTA ルート証明書 + MTA 製造業者証明書 + MTA デバイス証明書

MTA 製造業者証明書の署名は MTA ルート証明書を使用して検証され、MTA デバイス証明書の署名は MTA 製造業者証明書を使用して検証されます。MTA ルート証明書は自己署名されていて、プロビジョニング サーバにとって既知のものです。MTA ルート証明書に存在する公開鍵は、この証明書自体の署名を検証するために使用されます。

チェーンの最初の証明書は、ケーブル経由で送信される証明書チェーンに通常は明示的に含まれていません。最初の証明書が明示的に含まれている場合、最初の証明書は、検証する側にとって既知のものである必要があり、変更が一切加えられていない必要があります。ただし例外として、証明書シリアル番号、有効期間、署名の値は変更されてもかまいません。ケーブル経由で渡された CableLabs サービス プロバイダー ルート証明書に、既知の CableLabs サービス プロバイダー ルート証明書と比較してこれら以外の変更点が存在している場合、比較を実行するデバイスは証明書の検証に失敗する必要があります。

証明書チェーンの検証のためのルール自体が、RFC 2459 に完全に準拠している必要があります。この RFC では、証明書パスの検証として言及されています。通常、X.509 証明書では、証明書の発行者名がもう一方の証明書のサブジェクト名と一致している場合、一連の緩やかな判定ルールがサポートされます。ルールが緩やかであるため、2 つの名前フィールドのバイナリ比較が一致していない場合でも、2 つの名前フィールドは一致していると宣言されることがあります。RFC 2459 では、実装が単純なバイナリ比較を使用して一致またはミスマッチを宣言できるように、認証局が名前フィールドの符号化を制限することを勧めています。

PacketCable のセキュリティは、この推奨事項に従っています。したがって、PacketCable 証明書の DER 符号化された tbsCertificate.issuer フィールドが、発行者の証明書の DER 符号化された tbsCertificate.subject フィールドと完全に一致している必要があります。実装は、DER 符号化された tbsCertificate.issuer フィールドと tbsCertificate.subject フィールドのバイナリ比較を実行することによって、発行者名をサブジェクト名と比較できます。

以降の項では、必要な証明書チェーンが指定されています。この証明書チェーンを使用して、図 5-2 に示している PacketCable 証明書信頼階層のリーフ ノード（最下層）に該当する各証明書を検証する必要があります。

入れ子化されている有効期間は検証されず、強制されません。このため、証明書の有効期間は、その証明書を発行した証明書の有効期間内に収まっている必要はありません。

MTA デバイス証明書階層

デバイス証明書階層は、DOCSIS1.1/BPI+ 階層のデバイス証明書階層をそのまま写したものです。一連の製造業者証明書の発行元証明書として使用される、CableLabs 発行の PacketCable MTA ルート証明書がルートになっています。製造業者証明書は、個々のデバイス証明書に署名するために使用されます。

以降の表に含まれている情報は、RFC 2459 に従った必須フィールドで使用する PacketCable 固有の値を示しています。これらの PacketCable 固有の値は、表 5-2 に従って指定する必要がありますが、Validity Period は各表で示されているとおりにする必要があります。必須フィールドの PacketCable での値が特に示されていない場合は、RFC 2459 のガイドラインに従う必要があります。

MTA ルート証明書

この証明書は、MTA ルート証明書、MTA 製造業者証明書、および MTA デバイス証明書で構成される証明書チェーンの一環として検証する必要があります。

表 5-2　MTA ルート証明書

MTA ルート証明書		
Subject Name Form	**PacketCable** C=US O=CableLabs OU=PacketCable CN=PacketCable Root Device Certificate Authority	**Euro-PacketCable** C=BE O=tComLabs OU=Euro-PacketCable CN=Euro-PacketCable Root Device Certificate Authority
Intended Usage	この証明書は、MTA 製造業者証明書に署名するために KDC によって使用されます。この証明書は MTA によって使用されることがないため、MTA MIB には表示されません。	
Signed By	自己署名	
Validity Period	20 年以上。この証明書を再発行する必要のない、十分な長さの有効期間であると想定されます。	
Modulus Length	2048	
Extensions	keyUsage[c,m](keyCertSign, cRLSign) subjectKeyIdentifier[n,m] basicConstraints[c,m](cA=true, pathLenConstraint=1)	

MTA 製造業者証明書

この証明書は、MTA ルート証明書、MTA 製造業者証明書、および MTA デバイス証明書で構成される証明書チェーンの一環として検証する必要があります。state/province、city、および製造業者のファシリティは、オプションのアトリビュートです。製造業者は、製造業者証明書を複数保有していることがあり、証明書が製造業者ごとに 1 つまたはそれ以上存在することがあります。同じ製造業者のすべての証明書が、製造時または現地でのアップデート中に各 MTA に提供される可能性があります。MTA は、MTA デバイス証明書の発行者名を MTA 製造業者証明書のサブジェクト名と比較して、使用する適切な証明書を選択する必要があります。デバイス証明書の authorityKeyIdentifier は、存在する場合、RFC 2459 に記述されているとおり、製造業者証明書の subjectKeyIdentifier と一致している必要があります。O と CN にある <CompanyName> フィールドは、2 つのインスタンス間で異なる場合があります。

表 5-3　MTA 製造業者証明書

MTA 製造業者証明書		
Subject Name Form	**PacketCable** C=US O=CableLabs OU=PacketCable CN=PacketCable Root Device Certificate Authority	**Euro-PacketCable** C = <Country of Manufacturer> O = <Company Name> [stateOrProviceName = <state/province>] [localityName = <City>] OU = Euro-PacketCable [organizationalUnitName = <Manufacturing Location>] CN = <Company Name> Euro-PacketCable CA
Intended Usage	この証明書は各 MTA 製造業者に発行され、PacketCable Security Specification で規定されているとおり、（製造時または現地でのアップデート中に）セキュア コード ダウンロードの一環として各 MTA に提供されることがあります。この証明書は、読み取り専用パラメータとして MTA MIB に表示されます。この証明書は、KDC による認証中に、MTA デバイスのアイデンティティ（MAC アドレス）を認証するために MTA デバイス証明書とともに使用されます。	
Signed By	MTA ルート証明書の CA	
Validity Period	20 年	
Modulus Length	2048	
Extensions	keyUsage[c,m](keyCertSign, cRLSign)、subjectKeyIdentifier[n,m]、authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA certificate>)、basicConstraints[c,m](cA=true, pathLenConstraint=0)	

MTA デバイス証明書

この証明書は、MTA ルート証明書、MTA 製造業者証明書、および MTA デバイス証明書で構成される証明書チェーンの一環として検証する必要があります。state/province、city、および製造業者のファシリティは、オプションのアトリビュートです。MAC アドレスは、6 組のコロン区切り 16 進数（「00:60:21:A5:0A:23」など）で記述されている必要があります。16 進数のアルファベット文字（A ～ F）は、大文字で記述されている必要があります。MTA デバイス証明書は、置換および更新しないでください。

表 5-4　MTA デバイス証明書

MTA デバイス証明書		
Subject Name Form	**PacketCable** C=<country> O = <Company Name> [ST=<state/province>] [L=<city>], OU=PacketCable [OU=<Product Name>] [OU=<Manufacturer's Facility>] CN=<MAC Address>	**Euro-PacketCable** C = <Country of Manufacturer> O = <Company Name> [ST=<state/province>] [L = <City>] OU = Euro-PacketCable [OU=<Product Name>] [OU = <Manufacturing Location>] CN=<MAC Address>
Intended Usage	この証明書は MTA 製造業者によって発行され、製造時にインストールされています。プロビジョニング サーバはこの証明書をアップデートできません。この証明書は、読み取り専用パラメータとして MTA MIB に表示されます。この証明書は、プロビジョニング中に MTA デバイスのアイデンティティ（MAC アドレス）を認証するために使用されます。	
Signed By	MTA 製造業者証明書の CA	
Validity Period	20 年以上	
Modulus Length	1024、1536、または 2048	
Extensions	keyUsage[c,o](digitalSignature, keyEncipherment) authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA certificate>)	

MTA 製造業者コード検証証明書

組み込み型 MTA のコード検証証明書（CVC）の仕様は、DOCSIS 仕様 SP-BPI+-I11-040407 で指定されている DOCSIS 1.1 CVC と同一である必要があります。

CableLabs サービス プロバイダー証明書階層

サービス プロバイダー証明書階層は、CableLabs 発行の CableLabs サービス プロバイダー ルート証明書がルートになっています。この証明書は、一連のサービス プロバイダー証明書の発行元証明書として使用されます。サービス プロバイダー証明書は、オプションのローカル システム証明書に署名するために使用されます。ローカル システム証明書が存在する場合は、ローカル システム証明書を使用して補助装置証明書が署名されます。存在しない場合には、補助証明書はサービス プロバイダーの CA によって署名されます。

表 5-5 に含まれている情報は、RFC 2459 に従った必須フィールドで使用する固有の値を示しています。これらの固有値に従って指定する必要があります。必須フィールドの値が特に示されていない場合は、RFC 2459 のガイドラインを遵守する必要があります。

CableLabs サービス プロバイダー ルート証明書

Kerberos キー管理を行うには、Kerberos プロトコルの PKINIT 拡張を使用して、事前に MTA と KDC の相互認証を実行しておく必要があります。MTA は、KDC 証明書チェーンを含んだ PKINIT Reply メッセージを受信した後に KDC を認証します。KDC の認証で、MTA は KDC 証明書チェーンを検証します。このチェーンは、CableLabs サービス プロバイダー ルート CA が署名した KDC のサービス プロバイダー証明書を含んでいます。

表 5-5　CableLabs サービス プロバイダー ルート証明書

CableLabs サービス プロバイダー ルート証明書		
Subject Name Form	**PacketCable** C=US O=CableLabs CN=CableLabs Service Provider Root CA	**Euro-PacketCable** C=BE O=tComLabs CN=tComLabs Service Provider Root CA
Intended Usage	この証明書は、サービス プロバイダー CA 証明書に署名するために使用されます。この証明書は、各 MTA に製造時にインストールされるか、または PacketCable Security Specification で規定されているとおり、セキュア コード ダウンロードでインストールされます。プロビジョニング サーバでアップデートすることはできません。このルート証明書および対応する公開鍵は、MTA MIB に表示されません。	
Signed By	自己署名	
Validity Period	20 年以上。この証明書を再発行する必要のない、十分な長さの有効期間であると想定されます。	
Modulus Length	2048	
Extensions	keyUsage[c,m](keyCertSign, cRLSign) subjectKeyIdentifier[n,m] basicConstraints[c,m](cA=true)	

サービス プロバイダー CA 証明書

これはサービス プロバイダーが保有する証明書で、CableLabs サービス プロバイダー ルート CA によって署名されます。CableLabs サービス プロバイダー ルート証明書、テレフォニー サービス プロバイダー証明書、オプションのローカル システム証明書、およびエンドエンティティ サーバ証明書で構成される証明書チェーンの一環として検証されます。認証する側のエンティティは、通常はすでに CableLabs サービス プロバイダー ルート証明書を所有しており、この証明書は、証明書チェーンの残りの部分とともに転送されることはありません。

サービス プロバイダー CA 証明書が常に明示的に証明書チェーンに含まれているため、サービス プロバイダーは、自身の証明書を柔軟に変更できます。変更時に、この証明書チェーンを検証する各エンティティ（たとえば、MTA は PKINIT Reply を検証します）を再設定する必要はありません。サービス プロバイダー CA 証明書を変更したら、そのたびに署名を CableLabs サービス プロバイダー ルート証明書を使用して検証する必要があります。ただし、同じサービス プロバイダーの新しい証明書では、SubjectName の OrganizationName アトリビュートが以前と同じ値に保たれている必要があります。O と CN にある <Company> フィールドは、2 つのインスタンス間で異なる場合があります。

表 5-6　CableLabs サービス プロバイダー CA 証明書

CableLabs サービス プロバイダー ルート証明書		
Subject Name Form	**PacketCable** C=<Country> O=<Company> CN=<Company> CableLabs Service Provider CA	**Euro-PacketCable** C=<Country> O=<Company> CN=<Company> tComLabs Service Provider CA
Intended Usage	この証明書は、サービス プロバイダー CA 証明書に署名するために使用されます。この証明書は、各 MTA に製造時にインストールされるか、または PacketCable Security Specification で規定されているとおり、セキュア コード ダウンロードでインストールされます。プロビジョニング サーバでアップデートすることはできません。このルート証明書および対応する公開鍵は、MTA MIB に表示されません。	
Signed By	自己署名	
Validity Period	20 年以上。この証明書を再発行する必要のない、十分な長さの有効期間であると想定されます。	
Modulus Length	2048	
Extensions	keyUsage[c,m](keyCertSign cRLSign), subjectKeyIdentifier[n,m] basicConstraints[c,m](cA=true)	

ローカル システム CA 証明書

サービス プロバイダー CA は、ローカル システム CA（対応するローカル システム証明書を持つ）と呼ばれる地域別の認証局に証明書の発行を委任することがあります。ネットワーク サーバは、同じサービス プロバイダーの地域別の認証局の間を自由に移動できます。したがって、MTA MIB には、ローカル システム証明書に関する情報は含まれません（ローカル システム証明書では、MTA が特定地域内の KDC に制限される場合があるためです）。

表 5-7　ローカル システム CA 証明書

ローカル システム CA 証明書		
Subject Name Form	**PacketCable** C=<Country> O=<Company> OU=<Local System Name> CN=<Company> CableLabs Local System CA	**Euro-PacketCable** C=<Country> O=<Company> OU=<Local System Name> CN = <Company> tComLabs Local System CA
Intended Usage	サービス プロバイダー CA は、ローカル システム CA（対応するローカル システム証明書を持つ）と呼ばれる地域別の認証局に証明書の発行を委任することがあります。ネットワーク サーバは、同じサービス プロバイダーの地域別の認証局の間を自由に移動できます。したがって、MTA MIB には、ローカル システム証明書に関する情報は含まれません（ローカル システム証明書では、MTA が特定地域内の KDC に制限される場合があるためです）。	
Signed By	サービス プロバイダー CA 証明書	
Validity Period	20 年	
Modulus Length	1024, 1536, 2048	
Extensions	keyUsage[c,m](keyCertSign, cRLSign)、subjectKeyIdentifier[n,m]、authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA certificate>)、basicConstraints[c,m](cA=true, pathLenConstraint=0)	

運用上の補助証明書

ここで説明する証明書は、すべてローカル システム CA またはサービス プロバイダー CA のいずれかによって署名されます。他の補助証明書がこの標準に将来追加されることがあります。

鍵発行局証明書

この証明書は、CableLabs サービス プロバイダー ルート証明書、サービス プロバイダー CA 証明書、および補助デバイス証明書で構成される証明書チェーンの一環として検証する必要があります。PKINIT 仕様では、KDC 証明書に subjectAltName v.3 証明書拡張が含まれていることを要件としています。この拡張の値は、KDC の Kerberos プリンシパル名である必要があります。

表 5-8　鍵発行局証明書

鍵発行局証明書		
Subject Name Form	**PacketCable** C=<Country> O=<Company>, [OU=<Local System Name>] OU= CableLabs Key Distribution Center CN=<DNS Name>	**Euro-PacketCable** C=<Country> O=<Company> [OU = <Local System Name>] OU = tComLabs Key Distribution Center CN=<DNS Name>
Intended Usage	KDC サーバのアイデンティティを PKINIT 交換中に MTA に対して認証すること。この証明書は PKINIT 応答の中で MTA に渡されるため、MTA MIB には含まれておらず、プロビジョニング サーバがアップデートおよびクエリーすることはできません。	
Signed By	サービス プロバイダー CA 証明書またはローカル システム証明書	
Validity Period	20 年	
Modulus Length	1024、1536、または 2048	
Extensions	keyUsage[c,o](digitalSignature)authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA certificate>)subjectAltName[n,m]	

配送機能（DF）

この証明書は、CableLabs サービス プロバイダー ルート証明書、サービス プロバイダー CA 証明書、および補助デバイス証明書で構成される証明書チェーンの一環として検証する必要があります。この証明書は、（電子サーベイランスで使用される）DF 間でのフェーズ 1 IKE ドメイン間交換に署名するために使用されます。Local System Name はオプションですが、ローカル システム CA がこの証明書に署名する場合は必須です。IP アドレスは、245.120.75.22 などの標準的なドット付き 4 数字列表記で指定する必要があります。

表 5-9　DF 証明書

DF 証明書		
Subject Name Form	**PacketCable** C=<Country> O=<Company> [OU = <Local System Name>] OU=PacketCable Electronic Surveillance CN=<IP address>	**Euro-PacketCable** C=<Country> O=<Company> [OU = <Local System Name>] OU = Euro-PacketCable Electronic Surveillance CNe = <IP address>
Intended Usage	IKE キー管理を認証するために、1 組の DF 間で IPsec セキュリティ アソシエーションを確立するのに使用されます。これらのセキュリティ アソシエーションは、合法的に傍聴されているサブジェクトが、新しい傍聴サーバ（DF）に転送される必要のあるコール情報を含んだコール メッセージとイベント メッセージを転送するときに使用されます。	
Signed By	サービス プロバイダー CA 証明書またはローカル システム CA 証明書	
Validity Period	20 年	
Modulus Length	2048	
Extensions	keyUsage[c,o](digitalSignature) authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA certificate>) subjectAltName[n,m] (dNSName=<DNSName>)	

PacketCable サーバ証明書

これらの証明書は、CableLabs サービス プロバイダー ルート証明書、サービス プロバイダー証明書、ローカル システム オペレータ証明書（使用されている場合）、および補助デバイス証明書で構成される証明書チェーンの一環として検証する必要があります。これらの証明書は、PacketCable システムの各種サーバを識別するために使用されます。たとえば、フェーズ 1 IKE 交換に署名するため、または PKINIT 交換を認証するために使用される場合があります。Local System Name はオプションですが、ローカル システム CA がこの証明書に署名する場合は必須です。IP アドレスの値は、245.120.75.22 などの標準的なドット区切り 10 進表記で指定する必要があります。DNS Name の値は、device.packetcable.com などの完全修飾ドメイン名（FQDN）で指定する必要があります。

表 5-10　PacketCable サーバ証明書

PacketCable サーバ証明書		
Subject Name Form	**PacketCable**	**Euro-PacketCable**
	C=<Country>	C=<Country>
	O=<Company>	O=<Company>
	OU=PacketCable	OU = Euro-PacketCable
	OU=[<Local System Name>]	[OU = <Local System Name>]
	OU=<Sub-System Name>	OU = <Sub-system Name>
	CN=<Server Identifier[:<Element ID>]>	CN=<Server Identifier[:<Element ID>]>
	<Server Identifier> の値は、サーバの FQDN または IP アドレスにする必要があります。オプションで、値の後にコロン（:）に続けて Element ID を記述できます（コロンの前後は空白なし）。 <Element ID> は、課金イベント メッセージに表示される ID です。イベント メッセージを生成できるすべてのサーバの証明書に含まれている必要があります。このようなサーバとしては、CMS、CMTS、および MGC があります。Element ID は 5 オクテットの右揃え ASCII 符号化数値文字列として定義し、余白には空白文字を埋め込みます。Element ID を証明書で使用するために変換するときは、空白文字を ASCII の 0（0x48）に変換する必要があります。 たとえば、CMTS の Element ID が「311」で IP アドレスが 123.210.234.12 である場合、CMTS の通常名は「123.210.234.12:00311」になります。 <Sub-System Name> の値は、次のいずれかにする必要があります。 • ボーダー プロキシの場合：bp • ケーブル モデム ターミネーション システムの場合：cmts • Call Management Server の場合：cms • メディア ゲートウェイの場合：mg • メディア ゲートウェイ コントローラの場合：mgc • メディア プレーヤーの場合：mp • メディア プレーヤー コントローラの場合：mpc • プロビジョニング サーバの場合：ps • レコード記録サーバの場合：rks • シグナリング ゲートウェイの場合：sg	commonName の仕様の詳細については、PKT-SP-SEC-IO8-030415 を参照してください。
Intended Usage	これらの証明書は、PacketCable システムの各種サーバを識別するために使用されます。たとえば、フェーズ 1 IKE 交換に署名するため、または PKINIT 交換でデバイスを認証するために使用される場合があります。	
Signed By	テレフォニー サービス プロバイダー証明書またはローカル システム証明書	
Validity Period	MSO ポリシーにより設定	

表 5-10　PacketCable サーバ証明書（続き）

PacketCable サーバ証明書	
Modulus Length	2048
Extensions	keyUsage[c,o](digitalSignaturekeyEncipherment) authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA cert>) subjectAltName[n,m](dNSName=<DNSName> | iPAddress=<IP AddressName>) keyUsage タグはオプションです。使用する場合は、このタグをクリティカルとしてマークする必要があります。以降で特に説明のない限り、subjectAltName 拡張には、対応する名前値が、サブジェクトの CN フィールドで指定されているとおりに含まれている必要があります。

CMS 証明書の CN アトリビュート値は、Element ID にする必要があります。subjectAltName 拡張には、CMS の IP アドレスまたは FQDN のいずれかが含まれている必要があります。CMTS 証明書の CN アトリビュート値は、Element ID にする必要があります。subjectAltName 拡張には、CMTS の IP アドレスまたは FQDN のいずれかが含まれている必要があります。

MGC 証明書の CN アトリビュート値は、Element ID にする必要があります。subjectAltName 拡張には、MGC の IP アドレスまたは FQDN のいずれか含まれている必要があります。

証明書失効

現時点では、PacketCable の仕様範囲外です。

コード検証証明書階層

CableLabs コード検証証明書（CVC）PKI は汎用的な性質を持っており、CVC を必要とするすべての CableLabs プロジェクトに適用できます。つまり、基本インフラストラクチャをあらゆる CableLabs プロジェクトで再利用することができます。必要となるエンドエンティティ証明書は、プロジェクトごとに異なる場合がありますが、エンドエンティティ証明書が重複している場合は、1 つのエンドエンティティ証明書を使用してその重複に対応できる可能性があります。

CableLabs CVC 階層は、eMTA には適用されません。

CVC の全般的要件

すべてのコード検証証明書に対して、次の要件が適用されます。

- 証明書は、DER 符号化されている必要がある。
- 証明書は、バージョン 3 である必要がある。
- 証明書は、以降の各表で指定する拡張を含んでいる必要があり、その他の拡張を含んでいてはならない。
- 公開指数は、F4（10 進数の 65537）にする必要がある。

CableLabs コード検証ルート CA 証明書

この証明書は、CableLabs コード検証ルート CA 証明書、CableLabs コード検証 CA 証明書、およびコード検証証明書で構成される証明書チェーンの一環として検証する必要があります。証明書の検証方法の詳細については、P.5-18 の「証明書の検証」を参照してください。

表 5-11　CableLabs コード検証ルート CA 証明書

CableLabs コード検証ルート CA 証明書		
Subject Name Form	**PacketCable** C=US O=CableLabs CN=CableLabs CVC Root CA	**Euro-PacketCable** C = BE O = tComLabs CN = tComLabs CVC Root CA
Intended Usage	この証明書は、コード検証 CA 証明書に署名するために使用されます。この証明書は、製造時に S-MTA 不揮発性メモリに含める必要があります。	
Signed By	自己署名	
Validity Period	20 年以上	
Modulus Length	2048	
Extensions	KeyUsage [c,m] (keyCertSign, cRL Sign) subjectkeyidentifier [n,m] basicConstraints[c,m](cA=true)	

CableLabs コード検証 CA 証明書

CableLabs コード検証 CA 証明書は、CableLabs コード検証ルート CA 証明書、CableLabs コード検証 CA 証明書、およびコード検証証明書で構成される証明書チェーンの一環として検証する必要があります。証明書の検証方法の詳細については、P.5-18 の「証明書の検証」を参照してください。CableLabs コード検証 CA は、複数存在する場合があります。S-MTA は、一度に 1 つずつ CableLabs CVC CA をサポートする必要があります。

表 5-12　CableLabs コード検証 CA 証明書

CableLabs コード検証 CA 証明書		
Subject Name Form	**PacketCable** C=US O=CableLabs CN=CableLabs CVC CA	**Euro-PacketCable** C = BE O = tComLabs CN = tComLabs CVC CA
Intended Usage	この証明書は、CableLabs コード検証ルート CA によって CableLabs に発行されます。この証明書がコード検証証明書を発行します。この証明書は、製造時に S-MTA 不揮発性メモリに含める必要があります。	
Signed By	CableLabs コード検証ルート CA	
Validity Period	CableLabs ポリシーにより設定	
Modulus Length	2048	
Extensions	KeyUsage [c,m] (keyCertSign, cRL Sign) subjectKeyIdentifier[n,m] authorityKeyIdentifier [n,m] basicConstraints [c,m](cA=true, pathLenConstraint=0)	

製造業者コード検証証明書

CableLabs コード検証 CA は、認可された各製造業者に対して、この証明書を発行します。この証明書は、セキュアなソフトウェア ダウンロードのために CATV 事業者により設定されたポリシーで使用されます。

表 5-13　製造業者コード検証証明書

製造業者コード検証証明書		
Subject Name Form	**PacketCable** C=<country> O = <Company Name> [ST=<state/province>] [L=<city>] CN=<Company Name> Mfg CVC	**Euro-PacketCable** C=<Country> O = <Company Name> [ST=<state/province>] [L = <City>] CN=<Company Name> Mfg CVC
Intended Usage	CableLabs コード検証 CA は、認可された各製造業者に対して、この証明書を発行します。この証明書は、セキュアなソフトウェア ダウンロードのために CATV 事業者により設定されたポリシーで使用されます。	
Signed By	CableLabs コード検証 CA	tComLabs コード検証 CA 証明書
Validity Period	CableLabs ポリシーにより設定	
Modulus Length	1024, 1536, 2048	
Extensions	extendedKeyUsage [c,m] (id-kp-codeSigning) authorityKeyIdentifier [n,m]	

Organization の Company Name と Common Name の Company Name は、異なる場合があります。

サービス プロバイダー コード検証証明書

サービス プロバイダー コード検証証明書は、CableLabs コード検証ルート CA 証明書、CableLabs コード検証 CA 証明書、およびサービス プロバイダー コード検証証明書で構成される証明書チェーンの一環として検証する必要があります。証明書の検証方法の詳細については、P.5-18 の「証明書の検証」を参照してください。

表 5-14　サービス プロバイダー コード検証証明書

サービス プロバイダー コード検証証明書		
Subject Name Form	C=<country> O = <Company Name> [ST=<state/province>] [L=<city>] CN=<Company Name> Service Provider CVC	C=<Country> O = <Company Name> [ST=<state/province>] [L = <City>] CN=<Company Name> Service Provider CVC
Intended Usage	CableLabs コード検証 CA は、認可された各サービス プロバイダーに対して、この証明書を発行します。この証明書は、セキュアなソフトウェア ダウンロードのために CATV 事業者により設定されたポリシーで使用されます。	
Signed By	CableLabs コード検証 CA	tComLabs コード検証 CA 証明書
Validity Period	CableLabs ポリシーにより設定	
Modulus Length	1024, 1536, 2048	
Extensions	extendedKeyUsage [c,m] (id-kp-codeSigning) authorityKeyIdentifier [n,m]	

Organization の Company Name と Common Name の Company Name は、異なる場合があります。

CVC の証明書失効リスト

S-MTA は、CVC の証明書失効リスト（CRL）をサポートしている必要はありません。

CHAPTER 6

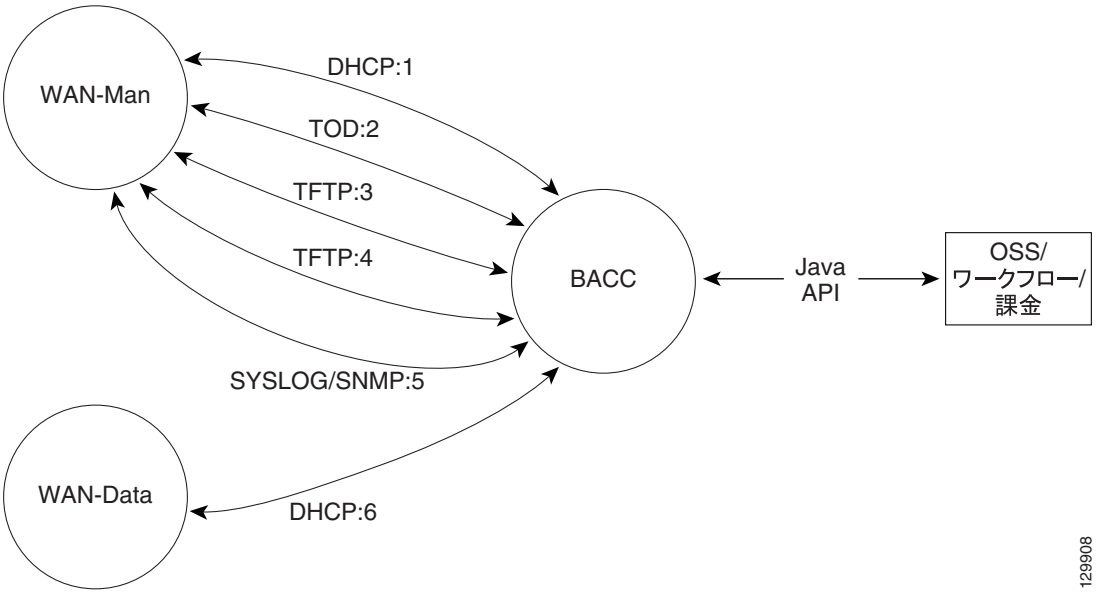
CableHome の設定

この章では、適切な CableHome 配備を実現するために必要となる作業について説明します。CableHome テクノロジーには、セキュア（SNMP）とノンセキュア（DHCP）の 2 つのバージョンがあります。この章では、主にノンセキュアなバージョンについて取り上げます。

ノンセキュア CableHome プロビジョニングのフロー

ノンセキュア CableHome プロビジョニングのフローでどのステップが失敗したかを特定して、それから他の詳細事項を診断するようにすると、非常に便利です。重要なプロビジョニング フローの要約を図 6-1 に示し、それらのフローについて以降の手順で説明します。

図 6-1　ノンセキュア CableHome のフロー



1. DHCP:1：WAN-Man が、自身の IP リースをこのステップで取得します。この IP リースでは、ポータル サービスが DHCP（ノンセキュア）モードでプロビジョニングされること、TFTP サーバ、および設定ファイルも指定されます。
2. TOD:2：ポータル サービスが、MSO のネットワークにある時刻サーバとのタイム同期を実行します。
3. TFTP:3：ポータル サービスが、ステップ 1 の説明と似た方法で設定ファイルを取得します。
4. TFTP:4：ステップ 3 で取得した設定ファイルにファイアウォールの情報が含まれている場合、ポータル サービスはファイアウォール設定ファイルも取得します。
5. SYSLOG/SNMP:5：設定が正常に終了した後に実行されます。ポータル サービスが SYSLOG メッセージまたは SNMP PDU を送信して、正常に設定されたことを BACC に通知します。
6. DHCP:6：ステップ 3 で取得したポータル サービス設定ファイルに、WAN-Data の IP アドレス数を 1 またはそれ以上に設定する MIB 設定が含まれている場合、ポータル サービス WAN-Data は要求された数の IP アドレスを取得します。

CableHome の設定

この項では、Network Registrar および CMTS を設定する方法について説明します。

Network Registrar の設定

ステップ 1　プロビジョニングされる WAN-Man とプロビジョニングされない WAN-Man の選択タグを作成し、プロビジョニングされる WAN-Data の選択タグも作成します。

ステップ 2　ケーブル モデムについて、プロビジョニングされないクライアント クラスとプロビジョニングされるクライアント クラス、およびスコープを『*Network Registrar User's Guide*』で指定されているとおりに設定します。

ステップ 3　WAN-Man について、プロビジョニングされないクライアント クラスとプロビジョニングされるクライアント クラス、およびスコープを設定します。

ステップ 4　WAN-Data について、プロビジョニングされるクライアント クラス、およびスコープを設定します。

ステップ 5　すべてのサブネットに到達するためのルートを追加します。

RDU の設定

RDU に対する CableHome サポートを設定するには、次の設定を行います。

- CableHome WAN-Man の設定（P.6-3）
- CableHome WAN-Data の設定（P.6-4）

CableHome WAN-Man の設定

ステップ 1　プロビジョニングされる WAN-Man の DHCPCriteria を作成します。作成するには、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。

ステップ 2　プロビジョニングされる WAN-Man のサービス クラスを作成します。

- /cos/chWanMan/file を、このサービス クラス用の適切な CableHome 設定ファイルに設定します。
- /chWanMan/firewall/file を、目的のファイアウォール設定ファイルに設定します。

CableHome WAN-Data の設定

ポータル サービスで WAN-Data の IP アドレスを取得するときは、そのたびに次の WAN-Data パラメータを設定します。

ステップ 1　WAN-Data の DHCPCriteria を作成します。

ステップ 2　WAN-Data の ClassOfService を作成します。

Device Provisioning Engine の設定

CableHome テクノロジーをサポートするように DPE を設定するには、次の手順に従います。

ステップ 1　CableHome デバイス プロビジョニング WAN-Man 設定ファイルを開いて、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。一部の製造業者は、独自の MIB オブジェクトを使用して、単純なケーブル モデム、CableHome 以外のルータ、または CableHome ルータとして動作するようにデバイスに指示していることがあります。デバイスの DHCP パケットの DHCP オプション 60 に CableHome1.0 または CableHome1.1 が含まれていない場合、デバイスは必ずコンピュータとして表示されます。

ステップ 2　ポータル サービスで WAN-Data の IP アドレスを取得する場合は、次の手順に従います。

- WAN-Man 設定ファイルに含まれている TLV 28 で、cabhCdpWanDataIpAddrCount が 0 を超える値に設定されていることを確認します。
- ケーブル モデム設定ファイルで、CPE の最大数を、WAN-Data の IP アドレス数を収容できる数に設定します。

ステップ 3　CableHome デバイスのブート時にセルフプロビジョニングをイネーブルにするには、次の手順に従います。

- unprov-wan-man.cfg ポータル サービス設定ファイルで、ポータル サービスをパススルー モードで設定します。
- ケーブル モデム設定ファイルで、CPE の最大数を 2 以上に設定して、WAN-Man とコンピュータをプロビジョニングできるようにします。このコンピュータは、サインアップ Web ページに直接アクセスしてセルフプロビジョニングできます。

ステップ 4　CableHome 設定ファイルを閉じて保存します。

CHAPTER 7

データベース管理

この章では、RDU データベースの管理および保守について説明します。RDU データベースは、Broadband Access Center for Cable（BACC）の中央データベースです。他のデータベースと同様に、管理者がデータベースのバックアップ手順と回復手順を理解し、熟知していることが必要です。

障害復元力について

RDU データベースでは、アプリケーション障害、システム障害、停電のような予測できない問題などが原因で発生するデータベースの破損を防止するために、*先行書き込みロギング*と呼ばれる手法を使用しています。

先行書き込みロギングでは、データベース ファイルに変更を書き込む前に、すべてのデータベース変更の記述をログ ファイルに書き込みます。これによって、システム障害の原因になった可能性がある不適切なデータベース書き込みを修復できます。

RDU サーバでは、起動されるたびに自動回復が実行されます。この回復処理時に、データとデータベース ファイルとの同期をとるために、ログ ファイルが使用されます。ログには書き込まれたものの、データベースには書き込まれていなかったデータベース変更は、この自動回復の処理中にデータベースに書き込まれます。

このようにして、先行書き込みロギングによって、RDU サーバの再起動時にデータベースが自動的に修復されるので、RDU サーバの障害時にデータベースが破損しないことが実質的に保証されます。

先行書き込みロギングが正しく機能するには、次の条件が必要です。

- ファイル システムおよび物理ストレージが、要求時にデータを確実に物理ストレージ内にフラッシュするように設定されている必要があります。たとえば、書き込みキャッシュが RAM だけで構成されたストレージ システムは、システム障害中にデータが失われるので、適切ではありません。ただし、ディスクアレイの書き込みキャッシュがバッテリー バックアップされていて、システム障害時にもデータが失われないことが保証されている場合は正しく機能します。
- ファイル システムは、RDU データベースのブロック サイズに合せて、ブロック サイズが 8192 バイトに設定されている必要があります。Solaris では、通常、明示的に調整しないかぎり、このブロック サイズがデフォルトで設定されます。

データベース ファイル

RDU データベースでは、ファイルが格納されたパーティションをマウントしたファイル システムを使用して、データがバイナリ ファイルに保存されます。システム障害発生後の回復時間が長くならないようにファイル システムを選択し、設定することがきわめて重要です。

データベース ファイルは RDU の動作にとってきわめて重要です。したがって、誤って削除するなどの手作業による操作が行われないように、データベース ファイルを保護するための特別な予防措置を講じる必要があります。これらの重要ファイルを保護するための標準的なシステム管理方法に従ってください。たとえば、これらのファイルには、root ユーザだけがアクセス可能なアクセス権を与える必要があります。また、運用中のシステムには root ユーザではなく、root ユーザよりも権限の低いユーザとしてログインし、sudo コマンドを使用して root 特権が必要なタスクを実行することも、有効な方法です。

(注) バックアップ、復元、および回復の各ツールを使用して、それぞれの作業をデータベースで行います。Broadband Provisioning Registrar（BPR）の旧リリースでは、特定のツールを使用しないでこれらの作業の一部を直接行うことが可能でした。ツールを使用しないでこれらの作業を行うことは避けてください。これらのツールの詳細については、P.7-5 の「バックアップと回復」を参照してください。

データベース ストレージ ファイル

RDU サーバは、データベース ディレクトリにある bpr.db というファイルに自身のデータベースを格納します。このディレクトリは <BACC_DATA>/rdu/db ディレクトリにあり、コンポーネントのインストール時に BACC_DATA パラメータを指定することで設定します。データベースの移動の詳細については、P.7-8 の「データベースの場所の変更」を参照してください。

(注) 通常、データベース　ファイルはランダムにアクセスされます。したがって、最高のデータベース パフォーマンスを得るためには、シーク時間が最も速く、回転アクセス レイテンシが最も小さいディスクを選択する必要があります。

データベースのトランザクション ログ ファイル

RDU サーバでは、データベースのトランザクション ログは 10 MB のファイルに保存され、そのファイルはデータベースのログ ディレクトリに保存されます。このディレクトリは、BACC_DBLOG パラメータを指定することでインストール時に設定します。ログ ディレクトリは、<BACC_DBLOG>/rdu/dblog ディレクトリにあります。トランザクション ログの新しいディレクトリへの移動の詳細については、P.7-8 の「データベースの場所の変更」を参照してください。

データベースのログ ファイルの名前には、最初に log.00000001、次に log.00000002 というように連番が付けられます。

(注) トランザクション ログが保存されるディスクは、通常、シーケンシャルにアクセスされるので、データはログ ファイルの最後に追加されます。最高のデータベース パフォーマンスを達成するには、このアクセス パターンを効率的に処理できるディスクを選択する必要があります。

自動ログ管理

データベースのトランザクション ログ ファイルは、トランザクション データのデータベースへの書き込みが完了するまで、そのデータを保存しておくために使用されます。その後、トランザクション ログ データは冗長になりますが、RDU サーバのデータベースはトランザクション ログ ファイルを自動的に管理するので、ファイルが自動的にシステムから削除されます。通常の状況では、データベースのトランザクション ログ ディレクトリ内にあるログ ファイルの数は数個以内にする必要があります。時間の経過とともに古いトランザクション ログはなくなり、新しいトランザクション ログが作成されます。

(注) データベースのトランザクション　ログは、データベースにとって不可欠です。トランザクション ログ ファイルを手動で削除すると、データベースが破損することがあります。

各種データベース ファイル

データベース ディレクトリには、他にもデータベースの動作に不可欠なファイルが保存されています。これらのファイルは、bpr.db ファイルとともに <BACC_DATA>/rdu/db ディレクトリにあり、データベース バックアップの一環としてコピーされます。

- DB_VERSION：データベースの物理的および論理的なバージョンを識別するためのもので、RDU によって内部で使用されます。
- history.log：ログ ファイルの自動的な削除、バックアップ、回復、復元処理などの不可欠なデータベース管理タスクに関するロギング動作のために使用されます。このログ ファイルは、管理者に有用な履歴情報を提供するだけでなく、RDU のデータベース処理にとっても非常に重要です。

ディスク容量の要件

完全に実装されたデータベースのサイズは、多くの要素で決まります。重要な要素は、RDU によって管理されるデバイス オブジェクトの数と、各オブジェクト上に保存されているカスタム プロパティの数です。各パーティション上で必要なディスク容量の概算値は、次のとおりです。

- BACC_DATA（デバイス オブジェクトごとに約 3 ～ 5 KB）
- BACC_DBLOG（500 MB 以上）

注意　これらの数値は、単なる指針として示したものなので、通常のシステム監視の必要がなくなるわけではありません。

disk_monitor.sh コマンドを使用すると、使用可能なディスク容量を監視したり、管理者に警告したりできます。詳細については、P.12-54 の「利用可能なディスク領域を監視するための disk_monitor.sh ツールの使用方法」を参照してください。

ディスク容量不足の対処方法

RDU サーバでディスク容量が不足すると、syslog ファシリティを通じて syslog アラートが生成され、RDU ログが記録されます。その後、RDU サーバは自動的に再起動を試みます。RDU サーバが再起動を試みたときにディスク容量不足のエラーが再び発生し、もう一度再起動が試みられる場合があります。

RDU サーバは、空きディスク容量が使用可能になるまで、繰り返し再起動しようとします。空き容量がなくなっているディスク上である程度のディスク領域を解放すると、次の再起動で RDU が正常に起動します。

データベースのサイズが増大して現在のディスク パーティションの容量を超えた場合、そのデータベースを新しいディスクまたはパーティションに移動する必要があります。この操作を行う方法については、P.7-8 の「データベースの場所の変更」を参照してください。

（注）　ディスク容量の使用率を監視して障害を防止するのが望ましい方法です。詳細については、P.12-54 の「利用可能なディスク領域を監視するための disk_monitor.sh ツールの使用方法」を参照してください。

バックアップと回復

RDU サーバは、サーバを停止したり、サーバの活動を一時停止したりしなくても実行できる、効率性の高いバックアップ処理をサポートしています。データベースのバックアップおよび回復は、次の手順から構成されます。

- バックアップ：稼働中のサーバから RDU データベースのスナップショットをとります。
- 回復：データベース スナップショットを再利用するための準備をします。
- 復元：回復したデータベース スナップショットを RDU サーバにコピーします。

これらの手順のそれぞれに自動ツールが用意されています。これらのツールは対話モードまたはサイレント モードで使用できますが、これらのツールを使用するには root 特権が必要です。

データベースのバックアップ

バックアップとは、データベース ファイルをバックアップ ディレクトリにコピーする処理です。そのときに、これらのファイルを圧縮し、テープやその他のアーカイブに保存することができます。

RDU データベースのバックアップは、サーバのアクティビティを中断しないでファイルをコピーするだけなので、非常に効率的です。ただし、RDU データベース ディスクにアクセスするため、バックアップを行うと RDU のパフォーマンスが低下する場合があります。その逆の場合もあります。バックアップ中に発生した RDU のアクティビティにより、バックアップのパフォーマンスが低下します。そのため、バックアップは、RDU の使用率の低い時間帯に行う必要があります。

バックアップのパフォーマンスは、同時に実行されているシステム アクティビティ以外に、基礎となっているディスクおよびファイル システムのパフォーマンスからも影響を受けます。基本的にバックアップ速度は、データベース ファイルをコピー元からコピー先へコピーする速度と同じです。

<BACC_DATA>/rdu/bin ディレクトリにある **backupDb.sh** コマンドを使用して、データベースのバックアップを行います。

- このコマンドを使用するには、バックアップ ファイルを保存するバックアップ先ディレクトリを指定する必要があります。このディレクトリは、現在のデータベース ファイル サイズの 120% に相当する使用可能ディスク容量があるディスクまたはパーティション上に存在する必要があります。
- 次の例で説明するように、このコマンドは、ユーザが指定したディレクトリの下に、タイムスタンプ付きのサブディレクトリを自動的に作成し、そこにバックアップを保存します。

例

backupDb.sh コマンドの使用例を次に示します。

```
backupDb.sh /var/backup
```

入力する内容は次のとおりです。

- */var/backup*：データベースのバックアップ ディレクトリを指定します。

この例では、バックアップするすべてのデータベース　ファイルは　/var/backup/rdu-backup-09252002-130345 というディレクトリにストアされます。最下位のサブディレクトリ（rdu-backup-09252002-130345）は自動的に作成され、現在のタイムスタンプが付けられます。

(注) タイムスタンプ付きのサブディレクトリの形式は、rdu-backup-MMddyyyy-HHmmss　が使用されます。この例では、サブディレクトリは rdu-backup-04272003-175430 になります。これは、そのディレクトリに 2003 年 4 月 27 日午後 5 時 54 分 30 秒に開始したバックアップが保存されていることを意味しています。

また、backupDb.sh コマンドは、自動的に経過を画面にレポートし、その動作を履歴ログに記録します。

(注)　backupDb.sh コマンドを使用するときに、**–help** オプションを使用すると、使用状況情報を取得できます。また、必要であれば、**-nosubdir** という別のオプション フラグを使用して、サブディレクトリの自動作成をディセーブルにできます。

データベースの回復

データベースの回復とは、データベースを一貫性のある状態に戻す処理です。バックアップは稼働中の RDU 上で行われるので、データベースはコピー中に変更される場合があります。ただし、データベースのログ ファイルによって、データベースを一貫性のある状態に戻せることが保証されています。

回復は、データベースのスナップショットに対して行われます。つまり、このタスクは、稼働中の RDU サーバ上のデータベースには作用しません。回復タスクは、バックアップの直後か、または、データベースを RDU サーバに復元する前に実行できます。

(注)　シスコでは、バックアップを行うたびに、その直後に回復を行うことを推奨しています。この方法をとると、緊急時にバックアップしたデータベースをより速やかに復元できます。

データベースの回復に要する時間は、バックアップの一環としてコピーするデータベースのログ ファイルの数によって決まり、したがって、バックアップの実行時の RDU のアクティビティ レベルによって決まります。バックアップの実行時に RDU が同時に実行している活動の数が多いほど、バックアップの一環としてコピーする必要があるトランザクション ログ ファイルの数が多くなり、回復に要する時間が長くなります。一般に、データベースの回復の所要時間は、トランザクション ログ ファイル当たり 10 ～ 60 秒です。

<BACC_DATA>/rdu/bin ディレクトリにある **recoverDb.sh** コマンドを使用して、データベースのスナップショットの回復を行います。このコマンドを使用するときは、バックアップの場所を指定する必要があります。このディレクトリでは、回復も行われます。

例　recoverDb.sh コマンドの使用例を次に示します。

```
# recoverDb.sh /var/backup/rdu-backup-04272003-130345
```

この例では、/var/backup/rdu-backup-04272003-130345 ディレクトリにあるスナップショットを一貫性のある状態に回復します。回復処理の経過は画面に表示され、そのアクティビティはスナップショット ディレクトリにある history.log ファイルに記録されます。

(注)　recoverDb.sh コマンドを使用するときに、**–help** オプションを使用して、使用状況情報を取得できます。

データベースの復元

データベースの復元とは、あらかじめ回復したデータベースのスナップショットを、RDU サーバによって使用されるデータベース上の場所にコピーする処理です。復元できるのは、あらかじめ回復しておいたデータベースだけです。

データベースの復元とは現行の RDU データベースの交換を意味するので、最初に古いデータベースを適切に削除し、アーカイブすることが非常に重要になります。

(注) 置換中にデータベースの削除を絶対に行わないでください。古いデータベースのコピーを残しておくと、将来のシステム診断が簡単になる場合があります。

<BACC_DATA>/rdu/bin ディレクトリにある **restoreDb.sh** コマンドを使用して、現行の RDU データベースを別のデータベースと置換します。このコマンドを使用するときは、入力ディレクトリを指定する必要があります。このディレクトリには、RDU サーバに復元するデータベースの、回復したバックアップ スナップショットが含まれている必要があります。

(注) restoreDb.sh ユーティリティを実行する前に、RDU サーバを停止する必要があります。

例

restoreDb.sh ユーティリティの実行例を次に示します。

```
# restoreDb.sh /var/backup/rdu-backup-04272003-130345
```

この例では、/var/backup/rdu-backup-042752003-130345 ディレクトリにあるデータベースが RDU サーバに復元されます。

(注) restoreDb.sh コマンドを使用するときに、**–help** オプションを使用すると、使用状況情報を取得できます。

復元処理の完了後は、RDU を再起動する必要があります。RDU ログ ファイルには、起動が成功したことを示すメッセージが書き込まれます。

このコマンドを実行すると、経過が画面に表示され、その動作が history.log ファイルに記録されます。

データベースの場所の変更

あるパーティションまたはディスクから、同じシステム上の別のパーティションまたはディスクにデータベースを移動することができます。管理上の理由で、この処理が必要になる場合があります。この処理を行うには、RDU サーバおよび BPR エージェントを停止する必要があります。

データベースの場所を変更する処理では、1 つまたは 2 つのシステム パラメータを変更し、該当のファイルを新しい場所にコピーします。次のパラメータの一方または両方を調整できます。

- BACC_DATA：このパラメータは、インストール時に最初に設定され、データベース、およびログや設定ファイルなどその他多くの重要なファイルが保存されるディレクトリを示しています。
- BACC_DBLOG：このパラメータは、インストール時に最初に設定され、データベースのトランザクション ログ ファイルが保存されるディレクトリを示しています。

上記のパラメータの値は、<BACC_DATA>/bpr_definitions.sh というファイルに記録されます。このファイルを変更した場合、システム上で実行されているすべての BACC コンポーネントを再起動する必要があります。

データベースおよびトランザクション ファイルの場所を変更するには、次の手順に従います。

ステップ 1　**/etc/init.d/bprAgent stop** コマンドを実行して BACC エージェントを停止します。

ステップ 2　<BACC_DATA>/bpr_definitions.sh ファイルのバックアップ コピーを作成します。

ステップ 3　このファイルを編集して、BACC_DATA パラメータおよび BACC_DBLOG パラメータの一方または両方を新しいディレクトリに変更します。

ステップ 4　このファイルを保存します。

ステップ 5　BACC_DATA ディレクトリと BACC_DBLOG ディレクトリの一方または両方の元のディレクトリ構造および内容を、新しい場所にコピーまたは移動します。コピーを行う場合は、すべてのファイルおよびディレクトリのアクセス権が維持されるようにしてください。

ステップ 6　**/etc/init.d/bprAgent start** コマンドを実行して、BACC エージェントおよびすべての BACC コンポーネントを起動します。

ステップ 7　該当のログ ファイルを監視して、すべてのコンポーネントが正常に起動したことを確認します。

RDU データベースの移行

RDU データベースの移行に関する情報は、すべて『Cisco Broadband Access Center for Cable Installation Guide』に記載されています。

CHAPTER 8

管理者のユーザ インターフェイスについて

この章では、Broadband Access Center for Cable（BACC）管理ユーザ インターフェイスへのアクセス方法と、その重要な点について説明します。

第 9 章「Broadband Access Center for Cable 管理者のユーザ インターフェイスの使用方法」では、BACC 管理者のユーザ インターフェイスを使用して管理作業を実行する方法を説明します。また、Device Provisioning Engine（DPE）デバイスに対するアクセス、監視、および制御で使用する CLI コマンドについては、『Cisco Broadband Access Center for Cable Command Line Interface Reference』に説明があります。

BACC 管理者のグラフィカル ユーザ インターフェイスへのアクセス

BACC のユーザ インターフェイスには、BACC アプリケーションの URL にアクセスできる任意のコンピュータからアクセスできます。

ログイン

BACC のユーザ インターフェイスには、管理ユーザ、読み取り / 書き込みユーザ、または読み取り専用ユーザとしてログインできます。P.8-7 の「Users」で説明するとおり、実行可能な機能は各ユーザ タイプで異なりますが、ユーザ インターフェイスには同じ方法でアクセスします。

BACC 管理者のユーザ インターフェイスにアクセスするには、次の手順に従います。

ステップ 1　Web ブラウザを起動します。この BACC リリースでサポートされるブラウザのリストを表 8-1 に示します。

表 8-1　ブラウザのプラットフォーム サポート

プラットフォーム	サポートするブラウザ
Windows 2000（Service Pack 2）	Internet Explorer 6.0 以降 Netscape 4.7 以降
Red Hat Linux（7.1）	Netscape 4.7 以降
Solaris（2.9）	Netscape 4.7 以降

ステップ 2　次の構文を使用して、管理者の場所を入力します。

```
http://<machine_name>:8100/adminui/
```

入力する内容は次のとおりです。

- *<machine_name>*：Regional Distribution Unit（RDU）を実行しているコンピュータを示します。
- *8100*：サーバ側の管理アプリケーションを実行しているコンピュータ ポートを示します。このポート番号は、8100 で固定です。

ステップ 3　メイン ログイン ページ（図 8-1）が表示されます。

図 8-1　ログイン ページ

ステップ 4　デフォルトのユーザ名（**admin**）とパスワード（**changeme**）を入力します。

ログインした RDU サーバの FQDN が User Login 領域に表示されます。

ステップ 5　初めてログインする場合は、次の手順に従います。

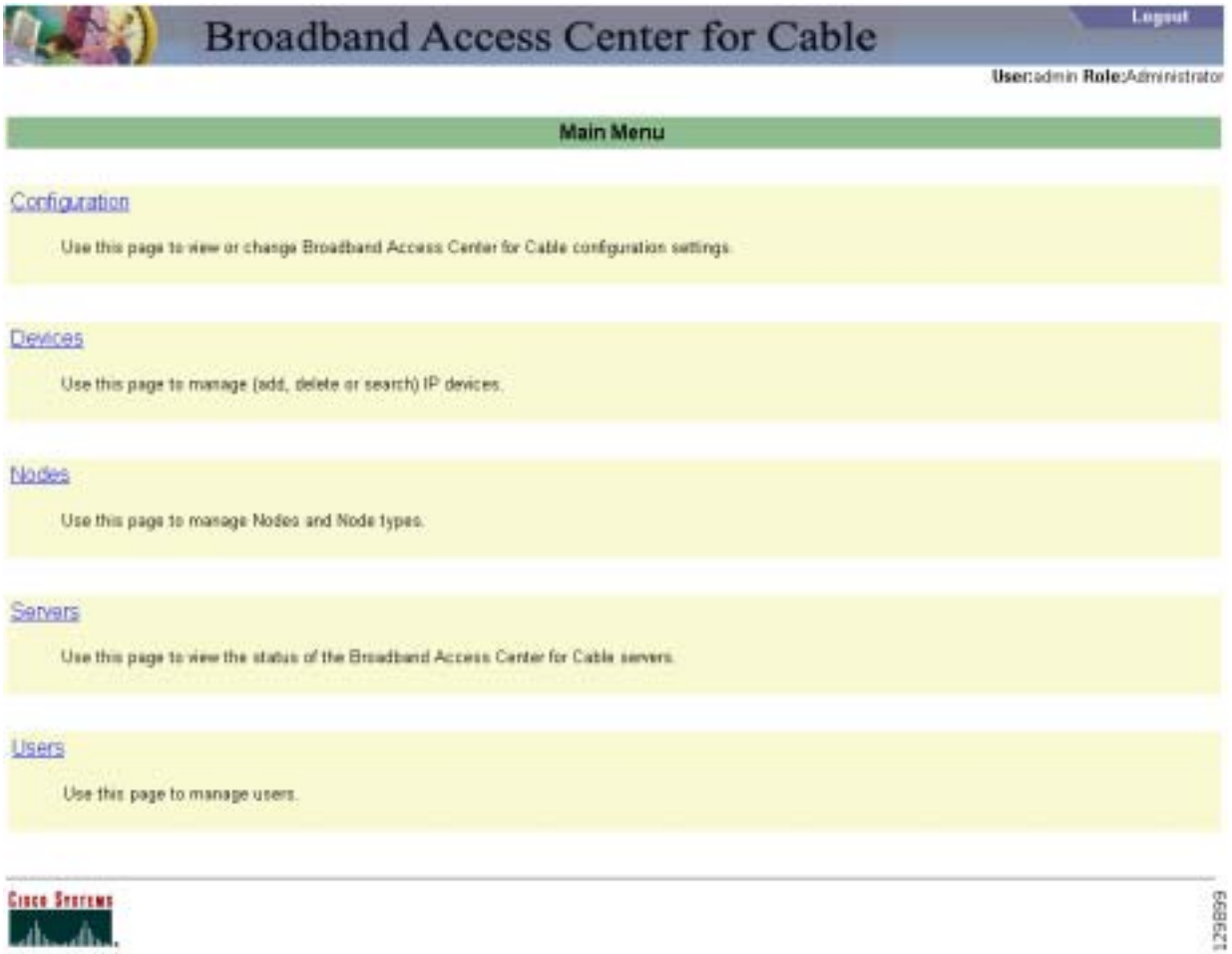
a. デフォルト パスワードの変更を要求するプロンプトが表示されます。新しいパスワードを入力して、**OK** をクリックします。

b. Add License Keys ページへのリンクを備えたプロンプトが表示されます。このページでは、使用許諾を得たテクノロジー ライセンスを入力できます。

（注）　ライセンス キーの入力の詳細については、第 10 章「Broadband Access Center for Cable の設定」を参照してください。

ステップ 6　**Login** をクリックすると、Main Menu ページ（図 8-2）が表示されます。

図 8-2　Main Menu ページ



ログアウト

BACC からログアウトするには、次の手順に従います。

ステップ 1　すべての管理者ページの右上にある **Logout** をクリックします。確認ダイアログが表示されます。

ステップ 2　**OK** をクリックします。User Login ページ（図 8-1）に戻ります。

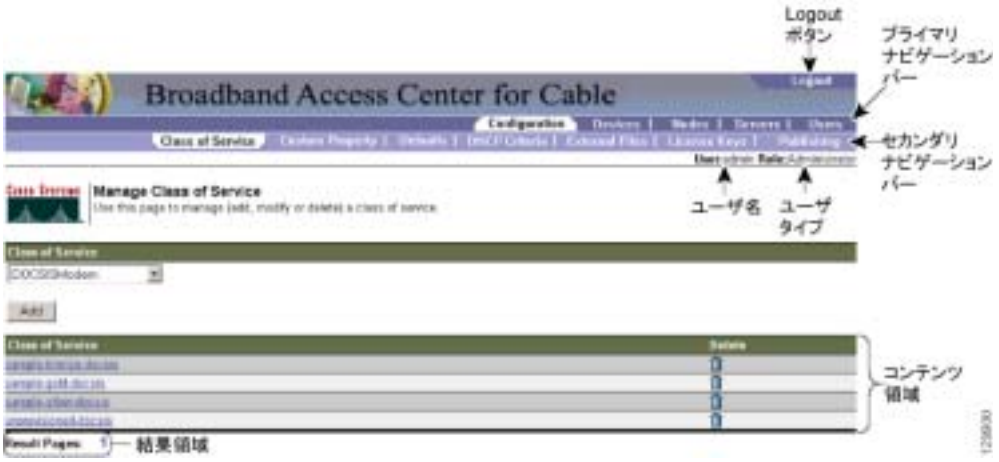
管理者のユーザ インターフェイス

BACC 管理者のユーザ インターフェイス（図 8-3）は、次の 3 領域に分かれています。

- バナー領域：**Logout** ボタン、プライマリ ナビゲーション バー、セカンダリ ナビゲーション バーなど、すべてのメニュー オプションが含まれます。
- コンテンツ領域：プライマリおよびセカンダリ ナビゲーション バーで実行した機能の結果であるすべての BACC データが含まれます。
- 結果領域：利用可能な情報ページ数が表示されます。これは、検索結果を検討するときに、特に役立ちます。

BACC 管理者ページには、View、Delete、Submit、または Reset の各コントロールが含まれているページもあります。

図 8-3　管理者のユーザ インターフェイス



ナビゲーション バー項目の選択

ナビゲーション バー項目を選択するには、目的のプライマリ ナビゲーション バー項目をクリックしてから、該当するセカンダリ ナビゲーション バー項目をクリックします（図 8-3 を参照してください）。Users オプションには、セカンダリ オプションがありません。

Main Menu

Main Menu で選択できるオプションは、次のとおりです。

- Configuration
- Devices
- Servers
- Nodes
- Users

これらのオプションのいずれかを選択した後、プライマリ ナビゲーション バーで目的のメニュー項目をクリックして、さらにメニューを選択できます。また、各プライマリ ナビゲーション バー メニュー項目に固有のオプションがセカンダリ ナビゲーション バーに表示されます。

Configuration

Configuration メニューを使用して、システム全体のさまざまな設定を表示および修正します。設定する項目は次のとおりです。

- サービス クラス
- カスタム プロパティ
- デフォルト（テクノロジー デフォルトを含む）
- DHCP 基準
- 外部ファイル
- ライセンス キー
- 発行

Devices

Devices メニューを使用して、デバイスを管理および保守します。また、次の検索形式で任意のデバイスを検索します。

- サービス クラス
- DHCP 基準
- 完全修飾ドメイン名（FQDN）
- IP アドレス
- MAC アドレス
- オーナー ID

Servers

Servers メニューを使用して、次の項目または選択したコンポーネントの現在の状態を表示します。

- DPE：Device Provisioning Engine
- NR：Network Registrar サーバ
- プロビジョニング グループ
- RDU：Regional Distribution Unit

Nodes

Nodes メニューでは、デバイスを特定のカテゴリにグループ化して、ログ エントリを使用して検索およびドキュメント化できるようにします。このカテゴリは、作成された非常に詳細なログ エントリに基づいて検索できます。BACC では、デバイスのグループ化に使用できる事前定義済みのノードをサポートしています。必要に応じて、独自のノードを作成することもできます。

Users

ユーザ タイプによっては、このメニューを使用して、ユーザを追加、修正、および削除できます。このメニューには、BACC を使用するように設定されているユーザがすべて表示され、それらのユーザのユーザ タイプも示されます。

BACC ユーザには、管理者、読み取り / 書き込みユーザ、読み取り専用ユーザという 3 つのタイプがあります。各ユーザ タイプはアクセス レベルが異なり、一意のアクセス権を付与されているため、アクセスを確実に制御してプロビジョニング データの一貫性を保つことができます。

割り当てられているユーザ タイプは、各管理ユーザ インターフェイス画面の右上近くに表示されます。

管理者

BACC が認識する管理者は 1 名のみです。このユーザは、デバイス データを表示、追加、変更、削除したり、他のユーザを作成したりできます。管理者は、他のユーザのアクセス権を読み取り / 書き込みから読み取り専用に変更することや、読み取り専用から読み取り / 書き込みに変更することもできます。また、他の任意のユーザ タイプのパスワードを変更することもできます。

読み取り / 書き込みユーザ

読み取り / 書き込みユーザは管理者と同じ機能を実行できますが、他のユーザを作成することや、他のユーザのユーザ タイプおよびパスワードを変更することはできません。読み取り / 書き込みユーザは、自分のパスワードを変更できます。

読み取り専用ユーザ

読み取り専用ユーザは、自分のパスワードの変更や、デバイス データの表示などの基本的なアクセスを実行できますが、デバイス データを変更することはできません。デバイスの動作を中断させるような操作は、一切実行できません。たとえば、構成のリセットや再生成は実行できません。

(注) 移行可能な旧リリースから BACC 2.7 に移行するときは、移行されるすべてのユーザに読み取り / 書き込み特権が割り当てられます。

前後へのスクロール

BACC 管理者の機能には、1 ページで表示できない長い情報リストを生成するものもあります。これらのページは、各ページの左下にあるコントロールのグループを使用して、1 ページずつ表示できます。複数の情報ページを利用できる場合は、ページ数も表示されます。特定のページにアクセスするには、そのページ番号をクリックします。左右の矢印コントロールをクリックすると、表示されたページ数の中でそれぞれ前後に移動します。

CHAPTER 9

Broadband Access Center for Cable 管理者のユーザ インターフェイスの使用方法

この章では、Broadband Access Center for Cable（BACC）管理者のユーザ インターフェイスを使用して実行する管理作業について説明します。管理作業には主に、次のような BACC コンポーネントのアクションの監視があります。

- ユーザ管理（P.9-2）
- デバイス管理（P.9-5）
- ノード管理（P.9-18）
- サーバの表示（P.9-21）

(注) この章で説明した手順は、チュートリアルの形式で示されています。可能な限り、各手順の結果を表す例を示すようにしてあります。

ユーザ管理

ユーザの管理には、BACC を管理するユーザの追加、修正、削除があります。この項では、BACC ユーザ管理の次の手順について説明します。

- 新規ユーザの追加
- ユーザの修正
- ユーザの削除

（注） ユーザを追加または削除できるのは、管理者としてログインしている場合のみです。ユーザ　タイプの詳細については、P.8-7 の「Users」を参照してください。

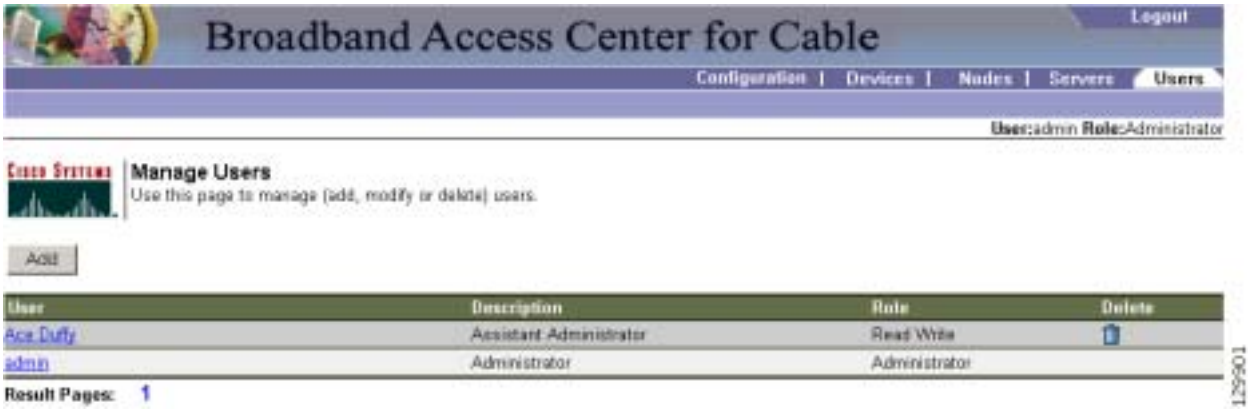
新規ユーザの追加

新規ユーザの追加は、ユーザ名を入力し、パスワードを作成する単純な手順です。ただし、新規ユーザを作成するときは、ユーザを読み取り / 書き込みユーザと読み取り専用ユーザのどちらのタイプにするかを決定する必要があります。BACC には、1 つの管理者ユーザがあらかじめ作成されています。管理者を新規ユーザとして作成することはできません。

新規ユーザを追加するには、次の手順に従います。

ステップ 1　Main Menu またはプライマリ ナビゲーション バーから **Users** をクリックします。Manage Users ページが表示されます（図 9-1 を参照してください）。

図 9-1　Manage Users ページの例



ステップ 2　**Add** をクリックして Add User ページを表示します。

ステップ 3　新規ユーザのユーザ名とパスワードを入力します。

ステップ 4　新規ユーザのパスワードを確認のためにもう一度入力し、新規ユーザのロールを読み取り専用または読み取り / 書き込みのどちらにするかを選択します。各ユーザ タイプの詳細については、P.8-7 の「Users」を参照してください。

ステップ 5　新規ユーザの簡単な説明を入力します。

ヒント　説明フィールドを使用して、ユーザの仕事または役職がわかるようにしたり、新規ユーザを区別したりします。

ステップ 6　入力後、**Submit** をクリックします。新規ユーザが追加された状態で Manage Users ページが表示されます。

（注）　新規ユーザのパスワードは、記録して安全な場所に保管する必要があります。これは、パスワードの紛失または盗用、および不正な侵入を防ぐために役立ちます。

ユーザの修正

どのユーザ タイプでも自分のパスワードとユーザ説明は修正できますが、他のユーザの情報を修正できるのは管理者のみです。管理者は、パスワード、ユーザ タイプ、および説明を修正できます。

（注）　作成された管理者以外のユーザは、admin ユーザの修正または削除に使用できません。

ユーザ プロパティを修正するには、次の手順に従います。

ステップ 1　Main Menu またはプライマリ ナビゲーション バーから **Users** をクリックします。Manage User ページが表示されます。

ステップ 2　目的のユーザ名をクリックして対象ユーザの Modify User ページを表示します。

ステップ 3　パスワード、ユーザ タイプ（管理者としてログインしている場合）、およびユーザ説明に対して必要な変更を行います。

ステップ 4　**Submit** をクリックします。ユーザ情報が適切に修正された状態で Manage Users ページが表示されます。

ユーザの削除

Manage Users ページに表示される管理者以外のユーザは、管理者のみが削除できます。ユーザを削除するには、次の手順に従います。

ステップ 1　Main Menu またはプライマリ ナビゲーション バーから **Users** をクリックします。Manage User ページが表示されます。

（注）　デフォルト ユーザである **admin** は削除できません。

ステップ 2　削除するユーザに対応する **Delete** アイコンをクリックします。Delete User ダイアログボックスが表示されます。

ステップ 3　**OK** をクリックして、選択したユーザを削除します。削除したユーザが含まれていない状態で Manage Users ページが表示されます。

デバイス管理

各種のデバイスをプロビジョニングおよび管理するには、Devices メニューを使用します。次の操作を実行できます。

- 指定した基準を共有している、特定のデバイスまたはデバイス グループを検索する。P.9-8 の「デバイスの検索」を参照してください。
- RDU データベースを対象として、デバイスを追加、修正、または削除する。次の項を参照してください。
  - デバイスの追加（P.9-14）
  - デバイスの修正（P.9-15）
  - デバイスの削除（P.9-15）
- デバイス構成を再生成する。P.9-16 の「デバイス構成の再生成」を参照してください。
- 任意のデバイスを、特定のノードを対象として関連付けまたは関連付け解除する。P.9-16 の「デバイスの関連付けと関連付け解除」を参照してください。
- 選択した任意のデバイスをリセットまたはリブートする。P.9-17 の「デバイスのリセット」を参照してください。
- デバイスをリブートしないまま、デバイス構成をデフォルト状態に戻す。P.9-17 の「デバイスの登録解除」を参照してください。

Manage Devices ページ

Manage Devices ページは、Main Menu またはプライマリ メニュー バーの **Devices** をクリックすると表示されます。このページ（図 9-2）には、すべてのデバイス管理機能の実行に必要なフィールドとコントロールが含まれています。

図 9-2　Manage Devices ページ

Manage Devices ページでは、互いに関連する 2 つの独立領域を利用して、検索結果を生成します。この結果を使用して、多くのデバイス管理機能を実行できます。領域は、実行する検索を定義する Search Type ドロップダウン リストと、その検索タイプの内容を指定する検索値フィールドです。次の検索を実行できます。

- サービス クラスの検索
- DHCP 基準の検索
- FQDN の検索
- IP アドレスの検索
- MAC アドレスの検索
- ノードの検索
- オーナー ID の検索

実行可能な検索の中には、ワイルドカード文字（*）を使用して検索機能を拡張できるものがあります。たとえば FQDN の場合、ワイルドカード文字を使用して検索するときは、次の形式を使用します。

- modem10.cisco.com
- *.cisco.com
- *.com
- *

(注) 大量のデバイスをサポートするシステムで、最後のワイルドカード検索（*）を使用することはお勧めしません。数千もの検索結果が返されて、大量のシステム リソースを消費してパフォーマンスに悪影響を与えるおそれがあります。

また、Page Size ドロップダウン リストを使用すると、1 ページあたりの検索結果表示件数を制限できます。結果表示件数は、25、50、または 75 から選択できます。返される検索結果の件数が選択した件数を超えている場合は、管理者のユーザ インターフェイスの左下に画面プロンプトが表示され、結果ページ間を移動することができます。

デバイス管理コントロール

ここで説明するボタンは、検索機能フィールドのすぐ下に配置されており、通常は検索機能と連携して使用します。たとえば、特定のデバイス グループに属するデバイスを検索して、何らかの管理機能を実行することができます。次のボタンを使用できますが、使用する検索タイプによっては、それぞれの管理機能を利用できない場合があります。

Add

Add 機能を使用して、新しいデバイスを RDU データベースに追加できます。適切な手順については、P.9-14 の「デバイスの追加」を参照してください。

Delete

Delete ボタンを使用して、選択したデバイスを RDU データベースから削除できます。適切な手順については、P.9-15 の「デバイスの削除」を参照してください。

Regenerate

Regenerate 機能を使用して、古い構成をアップデートします。デバイス構成は、サービス クラス パラメータまたは DHCP 基準パラメータを変更すると古くなることがあります。サービス クラス プロパティまたは DHCP プロパティを変更するか、新しい基準を指定すると、デバイス構成はそのたびに自動的に再生成されます。また、外部ファイルを置換したときにも再生成が発生します。ただし、自動的に再生成できない構成があります。これらは、generationConfiguration() メソッドまたは管理者のユーザ インターフェイスを使用して手動で再生成する必要があります。

Relate

Relate 機能を使用して、デバイスを（MAC アドレスを使用して）特定のノードと関連付けることができます。

Reset

Reset ボタンは、選択したデバイスを自動的にリブートします。

Unrelate

この機能は、選択したデバイスと、そのデバイスが現在関連付けられているノードとの関連付けを解除します。

Unregister

Unregister 機能を使用して、ネットワークでブートした直後のデフォルトにデバイスをリセットできます。

Identifier

検索基準と一致するすべてのデバイスを示します。表示される各 ID には、そのデバイスを修正できる別ページへのリンクが設定されます。

Device Type

利用可能なデバイス タイプを示すドロップダウン リストが表示されます。画面に表示される選択肢には次のものがあります。

- ATA186
- ATA188
- CableHomeManData
- CableHomeManWan
- DOCSISmodem
- Computer
- PacketCableMTA

Status

デバイスがプロビジョニングされたかどうかを示します。プロビジョニングされたデバイスとは、アプリケーション プログラミング インターフェイス（API）または管理ユーザ インターフェイスを使用して登録され、ネットワーク上でブートされたデバイスです。

Details

選択したデバイスに関する利用可能なすべての詳細情報が表示されます。詳細については、P.9-9 の「デバイスの詳細の表示」を参照してください。

デバイスの検索

BACC を使用して、さまざまな方法でデバイス情報を検索できます。生成された各検索結果には、View Details 機能が付属します。表示される詳細は、使用した検索方式にかかわらず同一です。

デバイス タイプを検索するには、Manage Devices ページから **Search Type** ボタンをクリックして、ドロップダウン リストを表示します。後続の検索ページには、選択した検索タイプに固有の画面コンポーネントが含まれます。

検索結果の数が選択したページ サイズよりも大きい場合は、ページ コントロールがページの左下に表示されます。これらのコントロールを使用して、1 ページずつ前後にスクロールしたり、特定のページを選択できます。詳細については、P.8-8 の「前後へのスクロール」を参照してください。

(注) 任意のクエリーから返される結果の最大数は 1000 で、1 ページに表示される結果の最大数は 75 です。デフォルトの最大数を変更するには、<BACC_HOME>/rdu/conf/adminui.properties ファイルの /adminui/maxReturned プロパティを修正し、**bprAgent restart jrun** コマンド（/etc/init.d/ ディレクトリにあります）を実行して、BACC JRun コンポーネントを再起動します。

検索タイプ

次の機能を使用して、特定のデバイスを検索できます。

- 登録されているサービス クラス検索：デバイスにプロビジョニングされているサービス クラスを使用して検索します。
- 選択されているサービス クラス検索：RDU によって選択されたサービス クラスを使用して、登録されているサービス クラスを何らかの理由で保持できないデバイスを検索します。
- 関連付けられているサービス クラス検索：登録されているサービス クラスと選択されているサービス クラスの両方を使用して検索します。
- 登録されている DHCP 基準検索：特定の DHCP 基準に属しているデバイスを検索します。
- 選択されている DHCP 基準検索：RDU によって選択された DHCP 基準を使用して、登録されている DHCP 基準を何らかの理由で保持できないデバイスを検索します。
- 関連付けられている DHCP 基準検索：登録されている DHCP 基準と選択されている DHCP 基準の両方を使用して検索します。

(注) 通常の状況では、関連付けられているサービス クラスと選択されているサービス クラス、関連付けられている DHCP 基準と選択されている DHCP 基準は同一になる必要があります。同一でない場合は、原因を調査して、選択されているサービス クラスまたは DHCP 基準を修正し、関連付けられているサービス クラスまたは DHCP 基準に一致させる必要があります。

- Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）検索：Fully Qualified Domain Name（FQDN）検索は、特にデバイス MAC アドレスが不明で、DNS サーバで割り当てられた FQDN で識別されるデバイスを検索する場合に便利です。

  たとえば、**www.cisco.com** は完全修飾ドメイン名です。ここでは、**www** がホスト、**cisco** が第 2 レベル ドメイン、**.com** が第 1 レベル ドメインを示しています。
- IP アドレス検索：IP アドレス検索では、現在、特定の IP アドレスが DHCP リースされているネットワーク上のすべてのデバイスが返されます。

- MAC アドレス検索：MAC アドレス検索機能は、特定のモデムの正確な MAC アドレスがわかっている場合、または特定のベンダープレフィックスを持つすべてのデバイスで明確に装置ベンダーが識別される場合に、最も適した方式です。そのため、MAC アドレス検索を実行すると、MAC アドレスによってデバイスのメーカーとタイプを識別できます。この検索基準の効果的な使用方法については、P.12-55 の「MAC アドレスによるデバイスのトラブルシューティング」を参照してください。

（注） ベンダープレフィックスは、MAC アドレスの先頭 3 オクテットです。たとえば、MAC アドレスが 1,6,aa:bb:cc:dd:ee:ff の場合、ベンダープレフィックスは「aa:bb:cc」です。

- ノード検索：ノード検索機能は、作成済みのノードおよびノード タイプを検索するために使用します。
- オーナー ID 検索：オーナー ID でデバイスを識別でき、サービス登録者のアカウント番号、またはそのデバイスを一意に示すすべてのものを識別できます。ワイルドカード検索は、この検索機能ではサポートされていません。

デバイスの詳細の表示

検索結果で示された任意のデバイスの詳細を表示できます。任意のデバイスの詳細を表示するには、表示するデバイスの Details アイコンをクリックして View Device Details ページを表示します。図 9-3 に、View Device Details ページの例を示します。

View Device Details ページに表示される情報は、選択したデバイスのタイプによって異なります。ただし、ほとんどのデバイスで表示される標準的な詳細情報は、図 9-3 に示されています。

図 9-3　View Device Details ページ

図 9-3 のフィールドを表 9-1 に示します。

表 9-1　View Device Details ページ

フィールドまたはボタン	説明
Device Details	
Device Type	利用可能なデバイス タイプを示すドロップダウン リストが表示されます。
MAC Address	デバイスの MAC アドレスを示します。
FQDN	選択したデバイスの完全修飾ドメイン名を示します。たとえば、ACME.COM は完全修飾ドメイン名です。
Host Name	ホストを示します。たとえば、上記の FQDN の場合は ACME がホスト名です。
Domain Name	ホストが存在するドメインを示します。たとえば、上記の FQDN の場合は .COM がドメイン名です。
Behind Device	このデバイスの背後のデバイスを示します。
Provisioning Group	デバイスが割り当てられているプロビジョニング グループを示します。
DHCP Criteria	使用する DHCP 基準を示します。これはアクティブ リンクで、クリックすると、対応する Modify DHCP Criteria ページが表示されます。
CPE DHCP Criteria	無差別モードの場合に、顧客が用意した装置に使用する DHCP 基準を示します。
Device Properties	このデバイスに設定できる、このページに表示されていないプロパティを示します。これらはカスタム プロパティです。
Device Provisioned State	デバイスがプロビジョニングされたかどうかを示します。デバイスは、登録されてネットワーク上でブートされた場合にのみプロビジョニングされます。
Device Registered State	デバイスが登録されたかどうかを示します。
Relay Agent Circuit Identifier	デバイスのリレー エージェント回路 ID を示します。DHCP オプション 82、サブ オプション 1 と等価です。
Relay Agent Remote Identifier	デバイスのリレー エージェント リモート ID を示します。DHCP オプション 82、サブ オプション 2 と等価です。
Client Identifier	DHCP メッセージでデバイスが使用するクライアント ID を示します。
Client Request Host Name	DHCP メッセージでクライアントが要求したホスト名を示します。
Class of Service	このデバイスに割り当てられたサービス クラスを示します。
Owner Identifier	デバイスを示します。ユーザ ID およびアカウント番号になるか、空白のままになります。
Detected Properties	デバイス構成が生成されたときに、RDU デバイス検出拡張が返したプロパティを示します。
Selected Properties	デバイス構成が生成されたときに、検出されたデバイス タイプについて RDU サービス レベル選択拡張が返したプロパティを示します。

表 9-1　View Device Details ページ （続き）

フィールドまたはボタン	説明
Is Behind Required Device	必要なリレー エージェント デバイスを IPDeviceKeys.MUST_BE_BEHIND_DEVICE プロパティを使用して確立した場合、このデバイスが必要なリレー エージェントの背後でブートしなかったことをサービス レベル選択拡張が特定すると、ここに「偽」が返されます。
Is In Required Provisioning Group	必要なプロビジョニング グループを IPDeviceKeys.MUST_BE_IN_PROV_GROUP プロパティを使用して確立した場合、このデバイスが必要なプロビジョニング グループでブートしなかったことをサービス レベル選択拡張が特定すると、ここに「偽」が返されます。
Selected Access	サービス レベル選択拡張によってデバイスに付与されているアクセスを示します。 • REGISTERD：デバイスが登録され、アクセス要件をすべて満たしたことを示します。 • PROMISCUOUS：デバイスのプロビジョニングが、デバイスのリレー エージェントに割り当てられているポリシーに基づいて実行されることを示します。 • DEFAULT：デバイスが、このデバイス タイプのデフォルト アクセスをプロビジョニングされることを示します。 • OTHER：BACC に組み込まれているデフォルト拡張では使用されません。カスタム拡張で使用するために提供されています。
Selected Class of Service	デバイス構成の生成に使用されたサービス クラスの名前を示します。
Selected DHCP Criteria	デバイス構成の生成に使用された DHCP 基準の名前を示します。
Selected Explanation	サービス レベル選択拡張が、デバイスに付与したアクセスを選択した理由の説明です。 たとえば、デバイスは、必要なプロビジョニング グループでブートしなかったためにデフォルト アクセスを付与されていることがあります。

表 9-1　View Device Details ページ （続き）

フィールドまたはボタン	説明
Selected Reason	サービス レベル選択拡張が、デバイスに付与したアクセスを選択した理由について、列挙型コードで示します。表示される値は、次のいずれかです。 • NOT_BEHIND_REQUIRED_DEVICE • NOT_IN_REQUIRED_PROV_GROUP • NOT_REGISTERED • OTHER • PROMISCUOUS_ACCESS_ENABLED • REGISTERED • RELAY_NOT_IN_REQUIRED_PROV_GROUP • RELAY_NOT_REGISTERED これらのほとんどは、登録済みアクセスまたは無差別モード アクセスを付与する要件に違反しているために、デフォルト アクセスが付与されていることを示します。
Related Node Type	このデバイスが関連付けられているノード タイプを示します。詳細については、P.9-18 の「ノード管理」を参照してください。
DHCP Information	
DHCP Inform Dictionary	構成の生成を要求するときに、Network Registrar 拡張が RDU に送信した追加情報を示します。これは BACC の内部でのみ使用します。
DHCP Request Dictionary	構成の生成を要求するときに、Network Registrar 拡張が RDU に送信した DHCPDISCOVER または DHCPREQUEST パケット詳細を示します。
DHCP Response Dictionary	このフィールドは BACC の内部でのみ使用するもので、常に空です。
DHCP Environment Dictionary	このフィールドは BACC の内部でのみ使用するもので、常に空です。
Lease Information	
IP Address	デバイスの IP アドレスを示します。
DHCP Lease Properties	リース プロパティを示します。常に空です。
Technology Specific Information	
(注) テクノロジー固有情報は、使用ライセンスを取得しているテクノロジーに関係があるデータのみを示します。	
XGCP Ports	ゲートウェイ コントロール プロトコルがアクティブなポートを示します。
DOCSIS Version	現在使用中の DOCSIS バージョンを示します。

デバイスの管理

この章のこれまでの項で説明したとおり、Devices メニューを使用すると、RDU データベース内にデバイスを作成したり、デバイスの保守方法を管理したりできます。デバイスの管理には、デバイスの追加、削除、修正に加えて、構成の再生成、選択したデバイスの関連付けと登録解除が含まれます。

この項では、新しいデバイスまたは既存のデバイスに対して、各種のデバイス管理機能を実行する方法について説明します。いくつかの情報フィールドは、すべてのデバイス管理ページで常に表示されます。このようなフィールドには、次のものがあります。

- Devices Type：デバイスを追加するときに、BACC に作成できる利用可能なデバイス タイプを示すドロップダウン リストです。画面に表示される選択肢には次のものがあります。
  - ATA186
  - ATA188
  - CableHomeManData
  - CableHomeManWan
  - DOCSISmodem
  - Computer
  - PacketCableMTA

  デバイスを修正するときに、デバイス タイプを編集または変更することはできません。
- MAC Address：追加するデバイスの MAC アドレスです。

  追加するデバイスの MAC アドレスをこのフィールドに入力します。入力するときは、カンマとコロンが正しい位置に入力されていることを確認してください。次に例を示します。

  ```
  1,6,00:00:00:00:00:AE
  ```

- Host Name：デバイスのホストを示します。たとえば、FQDN が node.cisco.com の場合は、node がホスト名です。
- Domain Name：ホストが存在するドメインを示します。たとえば、FQDN が node.cisco.com の場合は、cisco.com がドメイン名です。
- Owner Identifier：ホスト名以外を使用してデバイスを示します。ユーザ ID またはアカウント番号を入力するか、あるいは空白のままにします。
- Class of Service：プロビジョニングするデバイスのサービス クラスを指定します。
- DHCP Criteria：プロビジョニングするデバイスの DHCP 基準を指定します。

表示したページによっては、追加の情報が表示される場合があります。この追加情報が存在する場合は、以降の手順で示しています。

デバイスの追加

デバイスを追加するには、次の手順に従います。

ステップ 1　Manage Devices ページから **Add** をクリックします。Add Device ページが表示されます。

ステップ 2　デバイス タイプとサービス クラスを選択し、このページのその他のフィールドに入力します。この項のここまでで説明したフィールドに加えて、既存のプロパティ名と値のペアに新しい値を追加することもできます。

- Property Name：カスタムまたは組み込みデバイス プロパティの名前を示します。
- Property Value：プロパティの値を示します。

ステップ 3　**Submit** をクリックしてデバイスを追加するか、**Reset** をクリックしてすべてのフィールドをクリアします。

(注)　無差別モード コンピュータで使用するために DOCSIS モデムの CPE DHCP 基準を指定するには、プロパティ（/provisioning/cpeDhcpCriteria）を指定する必要があります。値は、有効な DHCP 基準にする必要があります。

デバイスの修正

デバイスを修正するには、次の手順に従います。

ステップ 1　Manage Devices ページから、目的のデバイスに対応する **Identifier** リンクをクリックします。Modify Device ページが表示されます。

ステップ 2　適切なドロップダウン リストから目的のパラメータを選択するか、適切なフィールドにデータを入力します。**Add** をクリックして既存の任意のプロパティ名と値のペアを修正するか、**Delete** をクリックして任意のペアを削除します。

ステップ 3　**Submit** をクリックしてこのデバイスに対する変更を保存するか、**Reset** をクリックしてすべてのフィールドをクリアします。

デバイスの削除

デバイスの削除は単純な手順ですが、慎重に使用する必要があります。削除を取り消すには、以前バックアップしたデータベースを復元するか、そのデバイスを再度追加する必要があります。

(注)　バックアップしたデータベースの復元が必要になった場合は、P.7-7 の「データベースの復元」を参照してください。

デバイスを削除するには、次の手順に従います。

ステップ 1　Devices ページで、削除するデバイスを検索します。そのためには、いずれかの検索タイプを使用します。

ステップ 2　目的のデバイスの左のチェックボックスをクリックします。

ステップ 3　**Delete** をクリックします。RDU データベースにストアされているデバイス レコードが削除されます。

デバイス構成の再生成

多くの異なるサービス クラスまたは DHCP 基準パラメータの変更が必要になることがあります。この場合、既存のデバイス構成は古くなり、構成の再生成が必要になります。各構成を手動で再生成する必要性をなくし、エラーの発生を減らすために、BACC には自動的にすべてのデバイス構成を再生成する Configuration Regeneration Service（CRS; 構成再生成サービス）が用意されています。

デバイス構成は、次の場合に自動的に再生成されます。

- サービス クラス プロパティが変更されたとき。
- DHCP 基準プロパティが変更されたとき。
- 外部ファイルが置換されたとき。これは、ダイナミック DOCSIS テンプレートのファイル、およびサービス クラスに直接関連付けられたファイルに適用されます。
- 新しいデフォルト サービス クラスまたは DHCP 基準が指定されたとき。

自動的に再生成できない構成があります。これらは、generationConfiguration() メソッドまたは管理者のユーザ インターフェイスを使用して手動で再生成する必要があります。手動で構成を再生成する必要があるのは、次の場合です。

- テクノロジー デフォルトが変更されたとき。
- システム デフォルトが変更されたとき。
- 別の DOCSIS テンプレートに含まれるファイルが変更されたとき。

(注) 構成の再生成方法に関係なく、デバイスをリブートするまで構成はデバイスに伝搬されません。

デバイスの関連付けと関連付け解除

デバイスの関連付けという概念は、サービス クラスや DHCP 基準の概念に似ている部分があります。これは、デバイスが特定のサービス クラスまたは特定の DHCP 基準に関連付けられるためです。大きな違いは、サービス クラスと DHCP 基準は事前定義ノードだと考えられること、定義した任意のグループにデバイスをグループ化する場合は、ノードを使用することです。

この意味では、関連付け機能を使用すると、デバイスを MAC アドレスを使用して特定のノードに関連付けることができ、ノードは特定のノード タイプに関連付けられます。

デバイスを特定のノードに関連付けると、そのデバイスについて膨大な量の情報が記録されます。この情報を使用して、発生した問題をトラブルシューティングすることができます。表 9-2 に、関連付け機能と関連付け解除機能を使用した場合に可能となるワークフローを示します。

表 9-2　関連付けおよび関連付け解除の手順の例

ステップ	操作
1.	問題が存在しているかどうかを調査して、どのデバイスが影響を受けているかを特定します。
2.	デバイスをノードに関連付けます。
3.	数分間待機してデバイスのトラフィックを確実に通過させるか、デバイスのハード ブートを実行します。
4.	rdu.log ファイルをワード プロセッサ アプリケーションで開いて、当該デバイスの MAC アドレスのエントリを見つけます。
5.	問題を特定して修正し、テストして検証します。
6.	デバイスとノードとの関連付けを解除します。

デバイスのリセット

Reset ボタンを使用して、選択した任意のデバイスをリブートできます。

デバイスの登録解除

登録解除機能を使用して、ネットワークでブートした直後のデフォルトにデバイスをリセットできます。

(注) デバイスがネットワーク上でブートされていない場合は、削除されます。

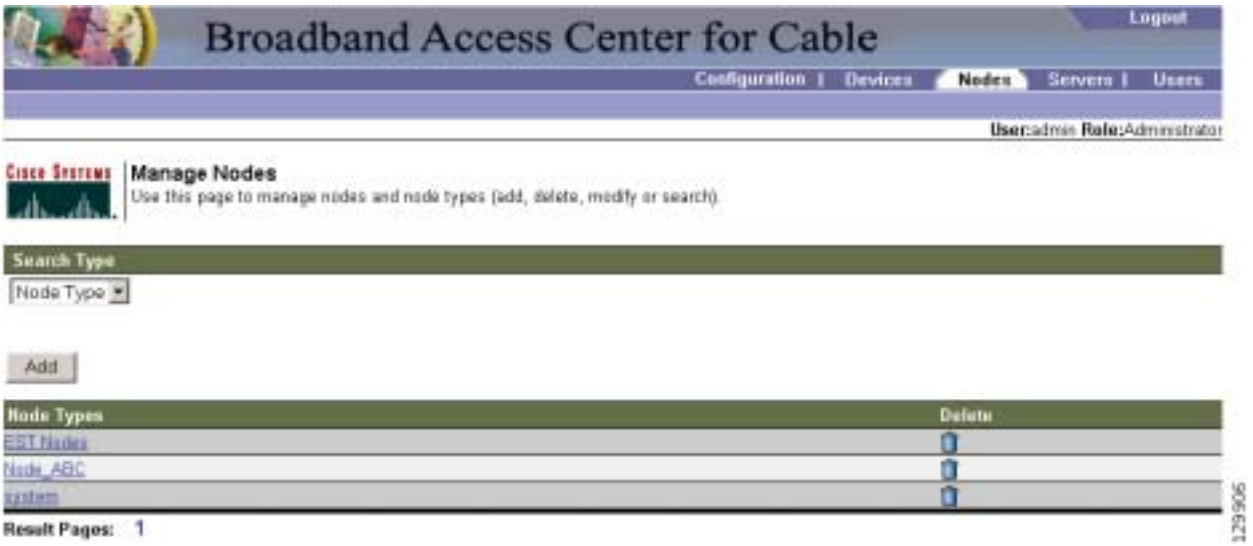
ノード管理

ノードの管理では、ノードとノード タイプの作成、修正、削除を実行できます。BACC においては、ノード タイプはノードのグループと考えることができ、ノード自体がノード タイプを構成します。

ノード タイプの管理

Main Menu またはプライマリ メニュー バーから Nodes を選択して、Manage Nodes ページ（図 9-4）にアクセスします。このページを表示すると、デフォルト設定では Node Type が選択されています。

図 9-4　Manage Nodes ページ



ノード タイプの追加

新しいノード タイプを追加するには、次の手順に従います。

ステップ 1　**Add** をクリックして Add Node Type ページを表示します。

ステップ 2　新しいノード タイプの名前を入力します。

ステップ 3　ドロップダウン リストから適切な Property Name を選択し、必要な Property Value を入力します。

ステップ 4　**Add** をクリックして新しいノード タイプを表示します。必要に応じて、プロパティを引き続きいくつでも追加することができます。

ステップ 5　選択後、**Submit** をクリックします。新しいノード タイプが RDU に記録され、新しいノード タイプが追加された状態で Manage Node Types ページが表示されます。

ノード タイプの修正

ノード タイプのプロパティを修正するには、次の手順に従います。

ステップ 1　目的のノード タイプをクリックして Modify Node Type ページを表示します。

ステップ 2　Property Name と Property Value のペアに対して必要な修正を行います。特定のペアを削除する必要がある場合は、目的のペアの隣にある **Delete** をクリックします。

ステップ 3　**Submit** をクリックします。Manage Node ページが表示され、修正内容が適切に反映されます。

ノード タイプの削除

ノード タイプを削除するには、次の手順に従います。

ステップ 1　Manage Nodes ページで、目的のノード タイプに対応する **Delete** アイコンをクリックします。

ステップ 2　Delete Node Type ダイアログボックスで、**OK** をクリックして選択したノード タイプを削除します。または、**Cancel** をクリックして前のページに戻ります。

削除したノード タイプが消えた状態で Manage Nodes ページが表示されます。

ノードの管理

ノードを作成および修正し、不要なノードを削除できます。

新規ノードの追加

新規ノードを追加するには、次の手順に従います。

ステップ 1　Manage Nodes ページのドロップダウン リストから **Nodes** を選択します。

ステップ 2　**Add** をクリックして Add Node ページを表示します。

ステップ 3　新規ノードの名前を入力して、このノードに使用する適切な Node Type を選択します。

完了後、**Submit** をクリックすると、新規ノードが追加された状態で Manage Nodes ページが表示されます。

ステップ 4　ドロップダウン リストから適切な Property Name を選択し、必要な Property Value を入力します。

ステップ 5　**Add** をクリックして、該当する Property Name と Property Value のペアの数を増やします。

ステップ 6　選択後、**Submit** をクリックします。新しいノードが RDU に記録され、新しいノードが追加された状態で Manage Nodes ページが表示されます。

ノードの修正

ノード プロパティを修正するには、次の手順に従います。

ステップ 1　目的のノードをクリックして Modify Nodes ページを表示します。

ステップ 2　Property Name と Property Value のペアに対して必要な修正を行います。特定のペアを削除する必要がある場合は、目的のペアの隣にある **Delete** をクリックします。

ステップ 3　**Submit** をクリックします。Manage Node ページが表示され、修正内容が適切に反映されます。

ノードの削除

Manage Nodes ページに表示されるノードを削除するには、削除するノードに対応するチェックボックスをオンにして、**Delete** をクリックします。ノードはただちに削除されます。

ノードに対するノード タイプの関連付けと関連付け解除

関連付け機能と関連付け解除機能は、特定のノード タイプとノードの間に関連性を確立するために使用します。この関連性を確立または解除するには、次の手順に従います。

ステップ 1　選択したノードについて、目的に応じて **Relate** または **Unrelate** をクリックします。Relate Nodes ページまたは Unrelate Node ページが表示されます。

ステップ 2　適切な **Node Type** をドロップダウン リストから選択し、ノードの関連付けまたは関連付け解除の対象となるグループを選択します。

ステップ 3　**Submit** をクリックして Manage Nodes ページを表示します。

ノードの詳細の表示

特定のノードを検索するには、**Devices** アイコンを使用します。このアイコンを使用すると、Manage Devices ページにノード検索機能が表示されます。このページから適切な Node Type を選択し、ノード名を入力します。ワイルドカード文字を使用して、名前の類似するノードをまとめて検索することもできます。検索機能の詳細については、P.9-8 の「デバイスの検索」を参照してください。

サーバの表示

この項では、BACC 管理者のサーバ表示ページについて説明します。

- Device Provisioning Engine のリスト（P.9-21）
- Network Registrar 拡張ポイントのリスト（P.9-24）
- プロビジョニング グループのリスト（P.9-26）
- Regional Distribution Unit の詳細の表示（P.9-27）

Device Provisioning Engine のリスト

List Device Provisioning Engines ページで、現在 BACC データベースに登録されているすべての DPE のリストを監視できます。このページに表示される各 DPE 名は、その DPE の詳細を表示する別ページへのリンクになっています。詳細ページ（例：図 9-5）を表示するには、このリンクをクリックします。

(注)　RDU は、CNR 拡張と DPE が RDU への接続に使用しているインターフェイスに基づいて、CNR 拡張と DPE の名前を特定します。つまり、DPE または CNR 拡張の名前は、RDU マシンが判断した名前です。

図 9-5　View Device Provisioning Engines Details ページ

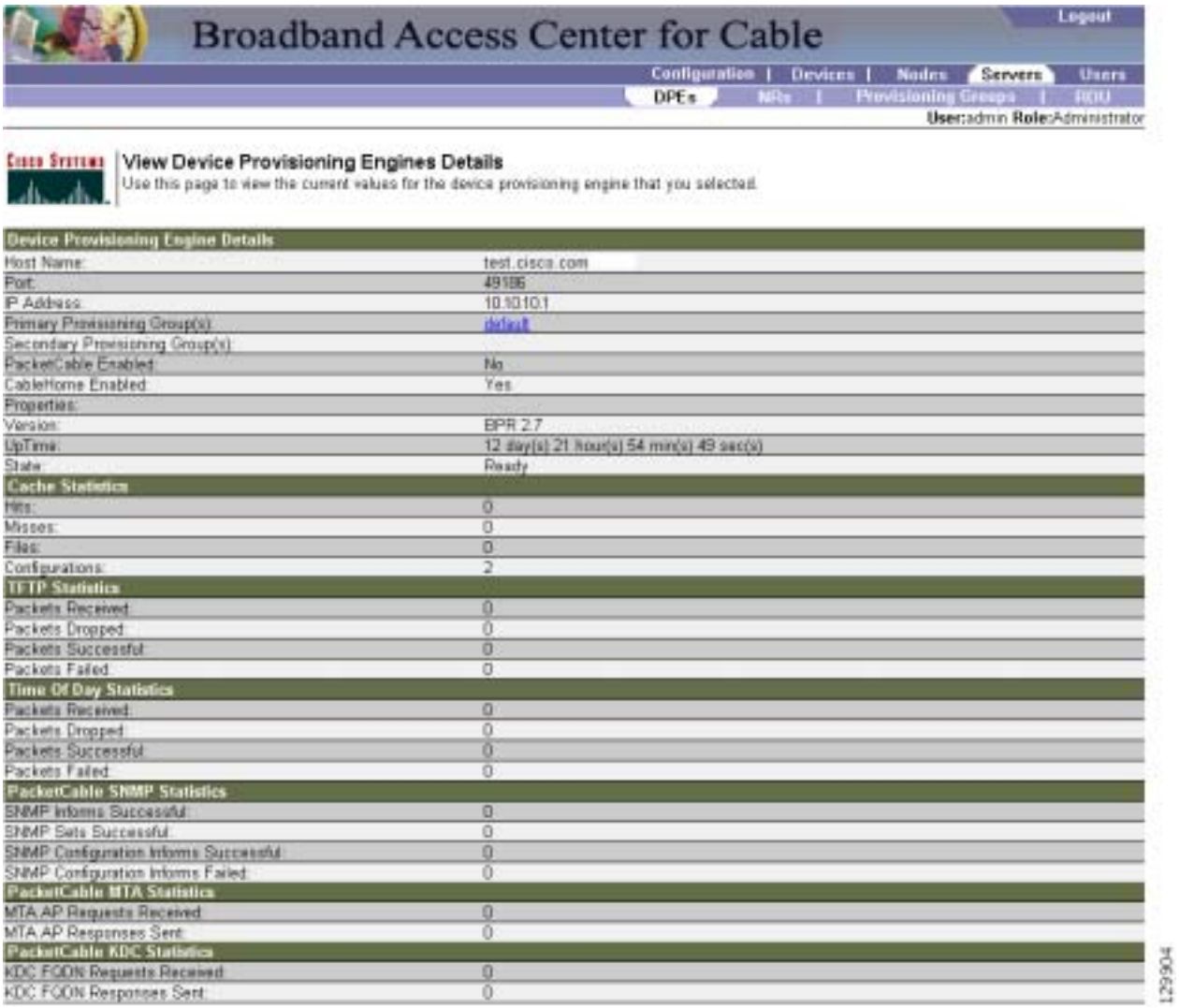


図 9-5 のフィールドとボタンを表 9-3 に示します。

(注)　表示される DPE 詳細の種類は、ハードウェアと Solaris DPE で同じです。

表 9-3　View Device Provisioning Engines Details ページ

フィールドまたはボタン	説明
Device Provisioning Engine Details	
Host Name	DPE ホスト名を示します。
Port	DPE ポート番号を示します。
IP Address	DPE の IP アドレスを示します。
Primary Provisioning Group(s)	選択した DPE が属するプライマリ プロビジョニング グループを示します。これはアクティブ リンクで、クリックすると、そのプロビジョニング グループの Provisioning Group Details ページが表示されます。

表 9-3　View Device Provisioning Engines Details ページ（続き）

フィールドまたはボタン	説明
Secondary Provisioning Group(s)	選択した DPE が属するセカンダリ プロビジョニング グループを示します（この DPE がセカンダリ プロビジョニング グループに属する場合）。
PacketCable Enabled	この DPE で PacketCable 音声技術がイネーブルかどうかを示します。
CableHome Enabled	この DPE でホーム ネットワーキング技術がイネーブルかどうかを示します。
Properties	この DPE に割り当てられているプロパティを示します。
Version	現在使用中の DPE ソフトウェアのバージョンを示します。
Up Time (in seconds)	DPE が最後にダウンしてから、運用が継続している合計時間を示します。
State	DPE が動作可能かどうかを示します。 (注)　このフィールドが Offline の場合、up time およびそれ以下のすべてのフィールドが表示されません。
Cache Statistics	
Hits	DPE が最後に起動されてから発生したキャッシュ ヒット数を示します。
Misses	DPE が最後に起動されてから発生したキャッシュ ミス数を示します。
Files	DPE に現在ストアされているキャッシュ ファイル数を示します。
Configurations	キャッシュに保存されているデバイス設定ファイル数を示します。
TFTP Statistics	
Packets Received	選択した DPE が受信した TFTP パケット数を示します。
Packets Dropped	DPE の過負荷が原因で破棄された TFTP パケット数を示します。
Packets Successful	正常に転送された TFTP パケット数を示します。
Packets Failed	転送中に失敗した TFTP パケット数を示します。
Time of Day Statistics	
Packets Received	選択した DPE が受信した Time of Day パケット数を示します。
Packets Successful	正常に転送された Time of Day パケット数を示します。
Packets Failed	転送中に失敗した Time of Day パケット数を示します。
PacketCable SNMP Statistics	
SNMP Informs Successful	正常に送信された通知要求数を示します。
SNMP Sets Successful	正常な SNMP セット数を示します。
Configuration Informs Successful	正常にプロビジョニングされたことを示す PacketCable MTA から受信した SNMP 通知数を示します。
Configuration Informs Failed	プロビジョニングに失敗したことを示す PacketCable MTA から受信した SNMP 通知数を示します。

Network Registrar 拡張ポイントのリスト

List Network Registrar Extension Points ページには、RDU に登録され、BACC で使用するように構成されたすべての Network Registrar サーバの拡張ポイントのリストが表示されます。Network Registrar サーバは、起動したときに自動的に RDU に登録されます。

このページに表示される各 Network Registrar 拡張ポイントは、その拡張ポイントの詳細を表示する 2 番目のページへのリンクになっています。詳細ページ（例：図 9-6）を表示するには、このリンクをクリックします。

図 9-6　View Network Registrar Extension Point Details ページ

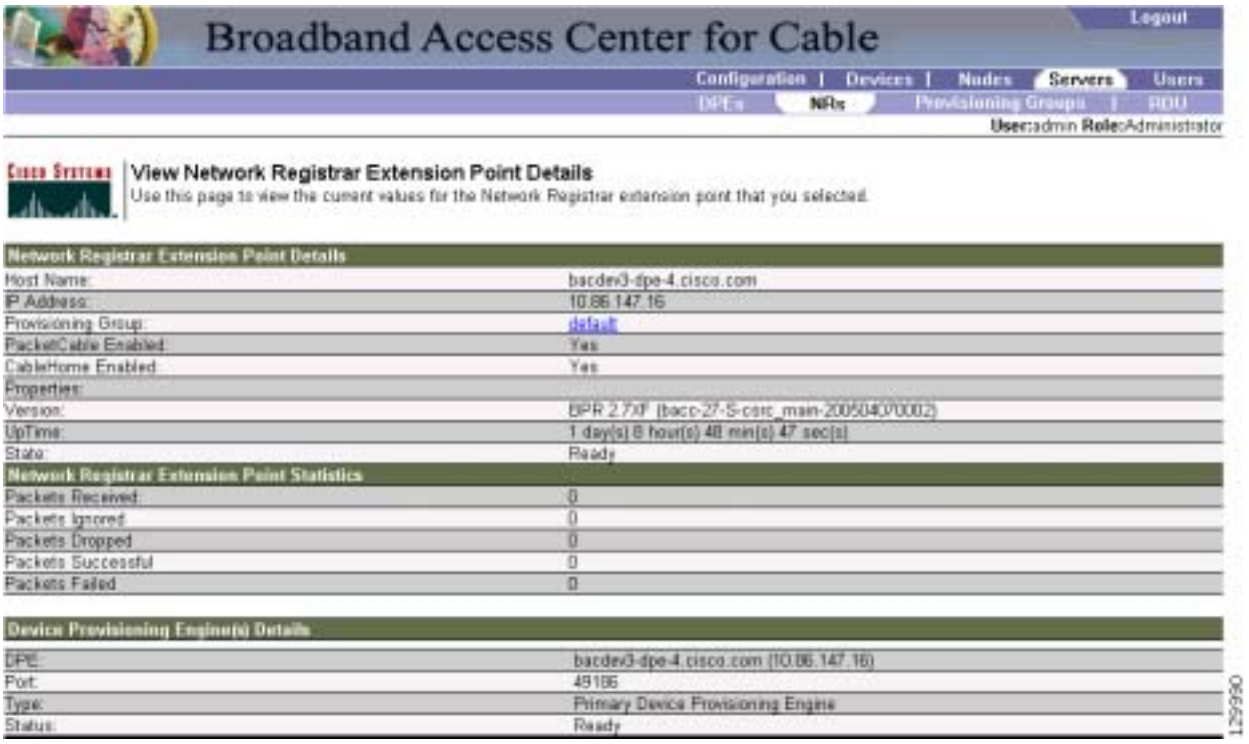


図 9-6 のフィールドとボタンを表 9-4 に示します。

表 9-4　View Network Registrar Extension Point Details ページ

フィールドまたはボタン	説明
Network Registrar Extension Point Details	
Host Name	Network Registrar を実行しているシステムのホスト名が表示されます。
IP Address	Network Registrar の IP アドレスを示します。
Provisioning Group	この Network Registrar サーバのプロビジョニング グループを示します。これはアクティブ リンクで、クリックすると、そのプロビジョニング グループの Provisioning Group Details ページが表示されます。
PacketCable Enabled	PacketCable 音声技術がイネーブルかどうかを示します。
Properties	選択した Network Registrar に適用されているプロパティを示します。
Version	現在使用中の拡張ポイント バージョンを示します。

表 9-4　View Network Registrar Extension Point Details ページ （続き）

フィールドまたはボタン	説明
Up Time	Network Registrar 拡張ポイントの運用が継続している時間を示します。時、分、秒で示されます。
State	DPE が動作可能かどうかを示します。 (注) このフィールドが Offline の場合、up time およびそれ以下のすべてのフィールドが表示されません。
Network Registrar Extension Point Statistics	
Packets Received	受信したパケット数を示します。
Packets Ignored	無視したパケット数を示します。
Packets Dropped	破棄したパケット数を示します。
Packets Successful	正常に転送されたパケット数を示します。
Packets Failed	転送に失敗したパケット数を示します。
Device Provisioning Engine(s) Details	
DPE	Device Provisioning Engine の IP アドレスを示します。
Port	DPE ポート番号を示します。
Type	この DPE がプライマリ DPE かセカンダリ DPE かを示します。
Status	DPE が動作可能かどうかを示します。

プロビジョニング グループのリスト

List Provisioning Groups ページを使用して、現在のプロビジョニング グループをすべて監視できます。このリストに表示される各プロビジョニング グループは、そのグループの詳細ページへのリンクになっています。詳細ページ（例：図 9-7）を表示するには、このリンクをクリックします。

図 9-7　View Provisioning Group Details ページ

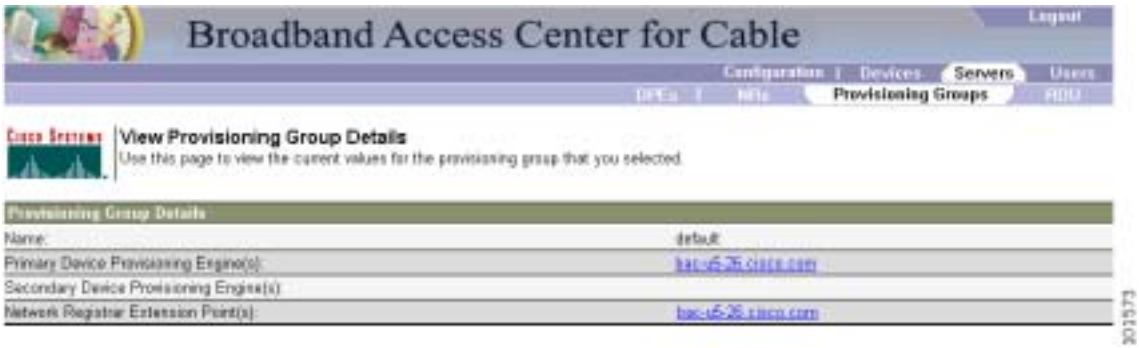


図 9-7 のフィールドとボタンを表 9-5 に示します。表 9-5 で説明するフィールドには、アクティブリンクが含まれていることがあります。クリックすると、対応する詳細ページが表示されます。

表 9-5　View Provisioning Group Details ページ

フィールドまたはボタン	説明
Name	List Provisioning Groups ページで選択したプロビジョニング グループ名を示します。
Primary Device Provisioning Engine(s)	このプロビジョニング グループのプライマリ DPE のホスト名を示します。
Secondary Device Provisioning Engine(s)	このプロビジョニング グループのセカンダリ DPE のホスト名を示します。
Network Registrar Extension Points	このプロビジョニング　グループに割り当てられた Network Registrar サーバのホスト名を示します。

Regional Distribution Unit の詳細の表示

Servers メニューの RDU オプションを使用すると、現在使用中の RDU の詳細が表示されます。RDU 詳細ページの例を図 9-8 に示します。

図 9-8　View Regional Distribution Unit Details ページ

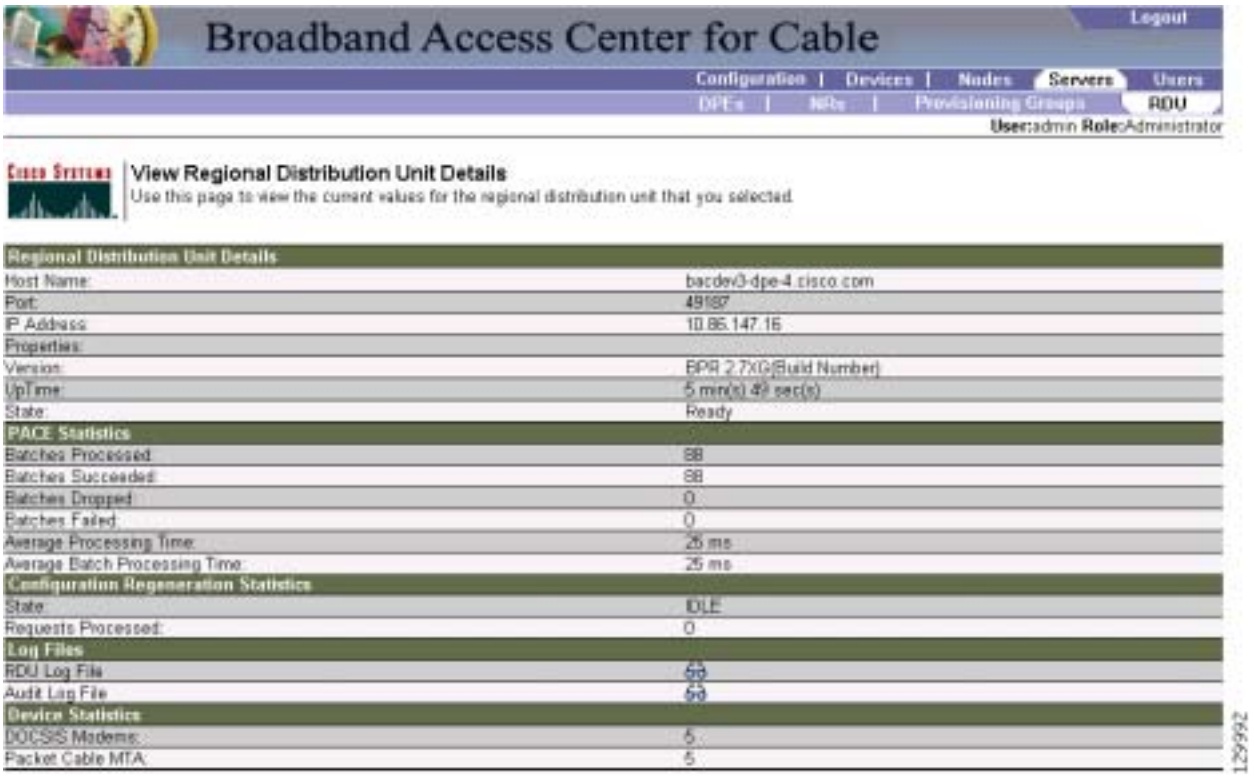


図 9-8 のフィールドとボタンを表 9-6 に示します。

表 9-6　View Regional Distribution Unit Details ページ

フィールドまたはボタン	説明
Regional Distribution Unit Details	
Host Name	Regional Distribution Unit を実行しているシステムのホスト名を示します。
Port	RDU リスニング ポート番号を示します。デフォルトのポート番号は 49187 ですが、このフィールドに表示されるポート番号は、インストール時に Regional Distribution Unit Host/Port 画面で入力した番号と同じです。
IP Address	RDU に割り当てられている IP アドレスを示します。
Properties	サーバの構成および制御に使用する RDU プロパティを示します。
Version	現在使用中の RDU ソフトウェアのバージョンを示します。
Up Time	RDU が最後にダウンしてから、運用が継続している合計時間を示します。
State	RDU が要求に応答するかどうかを示します。

表 9-6　View Regional Distribution Unit Details ページ（続き）

フィールドまたはボタン	説明
PACE Statistics	
Batches Processed	PACE エンジンの運用中に処理された、独立したバッチの数を示します。
Batches Succeeded	PACE エンジンの運用中に正常に処理された、独立したバッチの数を示します。
Batches Dropped	PACE エンジンの運用中に破棄されたバッチの数を示します。
Batches Failed	PACE エンジンの運用中に処理が失敗したバッチの数を示します。
Average Processing Time	RDU がビジーでキューに留まっていた時間を除いて、バッチの処理にかかった平均時間をミリ秒単位で示します。
Average Batch Processing Time	RDU がビジーでキューに留まっていた時間を含めて、バッチの処理にかかった平均時間をミリ秒単位で示します。
Configuration Regeneration Statistics	
State	構成再生成サービスが要求に応答するかどうかを示します。
Requests Processed	処理された構成再生成要求の数を示します。
Device Statistics	
この領域に表示される情報は、ライセンスを取得し、設定したテクノロジーに依存します。テクノロジーごとに表示される値は、RDU データベースで識別されるデバイスの数を表します。次のデバイスが含まれます。 • DOCSIS モデム • コンピュータ • ATA 186 および 188 デバイス • PacketCable MTA • CableHome WAN DATA/WAN MAN デバイス **（注）** Device Statistics セクションが表示されるのは、該当するデバイスが存在する場合のみです。外部 Jar ファイルがインストールされている場合は、詳細情報が Device Statistics セクションの直後に表示されます。	

（注） パフォーマンス上の理由により、デバイス レコードが更新されても、RDU は更新されたデータベース統計情報をディスクに書き込みません。表 9-6 に示すデバイス オブジェクト カウンタなどのデータベース統計情報は、メモリに保存され、定期的にデータベースに書き込まれます。そのため、このページに表示されるデバイス統計情報は概算値で、データベースの実際のデバイス数とは異なることがあります。

CHAPTER 10

Broadband Access Center for Cable の設定

この章では、次に示す Configuration メニュー オプションを使用して行う、Broadband Access Center for Cable（BACC）の設定作業について説明します。

- サービス クラスの設定（P.10-2）
- カスタム プロパティの設定（P.10-7）
- デフォルトの設定（P.10-8）
- DHCP 基準の設定（P.10-25）
- 外部ファイルの管理（P.10-27）
- ライセンス キーの管理（P.10-32）
- Regional Distribution Unit 拡張の管理（P.10-34）
- プロビジョニング データのパブリッシング（P.10-36）

サービス クラスの設定

BACC 管理アプリケーションを使用して、お客様に提供するサービス クラスを設定できます。たとえば、DOCSIS オプションを様々な DOCSIS サービス クラスと関連付けることができます。BACC 管理者のユーザ インターフェイスを使用して、選択したサービス クラスを追加、修正、表示、または削除します。図 10-1 に示されるような Manage Class of Service ページで作業を開始します。

図 10-1　Manage Class of Service ページ

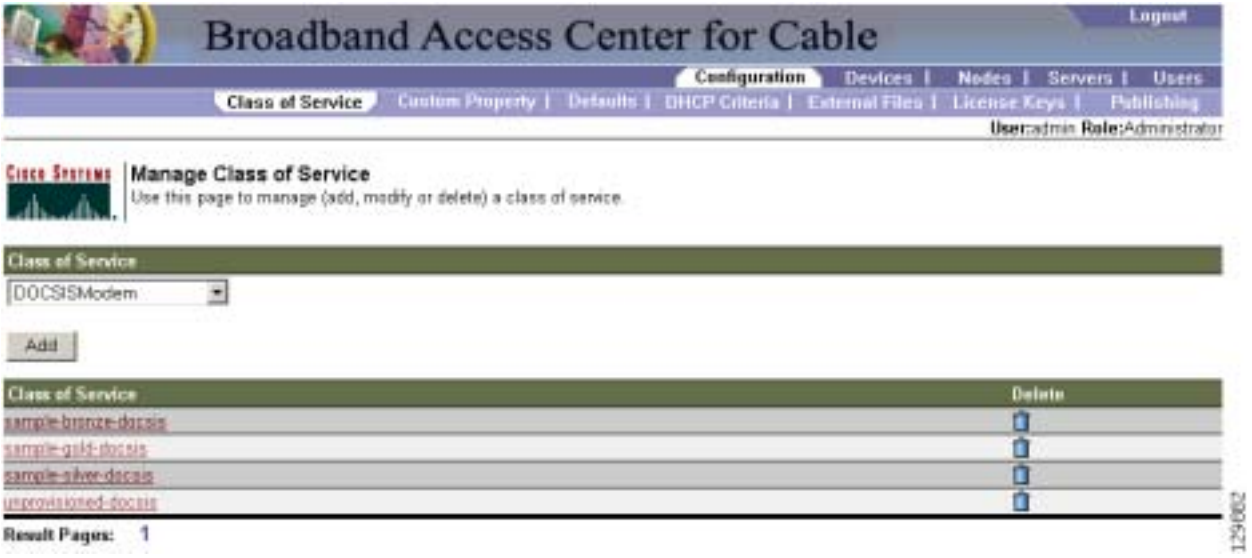


図 10-1 のフィールドとボタンを表 10-1 に示します。

表 10-1　Manage Class of Service ページ

フィールドまたはボタン	説明
Class of Service	検索できるテクノロジー サービス クラスを示すドロップダウン リストです。画面に表示される選択肢には次のものがあります。 • ATA 186 • ATA 188 • CableHomeManData • CableHomeManWan • DOCSISmodem • Computer • PacketCableMTA (注)　これらのテクノロジー分野の詳細については、P.10-8 の「デフォルトの設定」を参照してください。
Add	新しいサービス クラスを追加します。
Class of Service リスト	選択されたサービス クラスの属性が表示されます。
Delete	選択されたサービス クラスを削除します。

サービス クラスの追加

特定のサービス クラスを追加するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Class of Service** を選択します。

ステップ 3　**Add** をクリックします。Add Class of Service ページが表示されます。このページでは、選択したサービス クラスの各種の設定を指定します。

ステップ 4　新しいサービス クラスの名前を入力します。

ステップ 5　**Class of Service Type** を選択します。

ステップ 6　**Property Name** フィールドと **Property Value** フィールドに、それぞれプロパティ名とプロパティ値を入力します。

例：

DOCSIS モデムに対して Gold-Classic という名前の新しいサービス クラスを作成する場合を考えます。次のような手順になります。

a. Class of Service Name フィールドに、サービス クラス名 **Gold-Classic** を入力します。

b. サービス タイプのドロップダウン リストで **DOCSIS** を選択します。

c. プロパティ ファイル名 /cos/docsis/file を選択します。

d. Property Value フィールドに **Gold-Classic.cm** と入力してから、この手順の残りを続行します。

ステップ 7　**Add** をクリックして、定義するサービス クラスにそのプロパティを追加します。

ステップ 8　**Submit** をクリックして、この手順を完了させるか、または、**Reset** をクリックして、すべてのフィールドを元の設定に戻します。サービス クラスを決定した後、Manage Class of Service ページが表示されて、その特定のデバイス タイプに対して新規に追加されたサービス クラスが表示されます。

(注)　このページには、プロパティ名とプロパティ値のペアが複数表示される場合があります。サービス クラスから不要なペアを削除するには、**Delete** ボタンを使用します。

注意

DOCSISModem サービス クラスを追加する場合は、あらかじめ追加した外部ファイルの名前が値として含まれている /cos/docsis/file プロパティを指定する必要があります。このファイルは、このサービス クラスを持つ DOCSIS デバイスをプロビジョニングするときに使用されます。

PacketCable サービス クラスを追加する場合は、あらかじめ追加した外部ファイルの名前が値として含まれている /cos/packetCableMTA/file プロパティを指定する必要があります。このファイルは、このサービス クラスを持つ Packetcable デバイスをプロビジョニングするときに使用されます。

CableHomeWanMan サービス クラスを追加する場合は、あらかじめ追加した外部ファイルの名前が値として含まれている /cos/cableHomeWanMan/file プロパティを指定する必要があります。このファイルは、このサービス クラスを持つ CableHomeWanMan デバイスをプロビジョニングするときに使用されます。

表 10-2 に、Add Class of Service ページに表示されるフィールドとボタンを示します。

表 10-2　Add Class of Service ページ

フィールドまたはボタン	説明
Class of Service Name and Type	
Class of Service Name	新しいサービス クラスの名前を入力します。
Class of Service Type	選択できるサービス クラスのタイプが表示されるドロップダウン リストです。
Property Name/Value	
Property Name	適切なプロパティを指定します。ドロップダウン リストから目的のプロパティを選択できます。
Property Value	選択したプロパティ名に対する値を指定します。
Add	Property Name と Property Value の新しいペアを追加して、新しいサービス クラスを作成します。
Submit	行った変更を有効化または実装します。
Reset	すべての設定を元の設定に戻します。

サービス クラスの修正

サービス クラスを修正するには、種々のプロパティを選択し、適切なプロパティ値を割り当てます。サービス クラスを初めて作成する場合は、必須のプロパティをすべて選択し、値を割り当てる必要があります。入力内容に誤りがあった場合や、特定のサービス クラスを修正することが必要になった場合は、以前の修正を確定する前にプロパティ値を修正するか、または Property Name と Property Value のペアをまとめて削除します。

(注)

これ以後のデバイス構成には、ここで行う修正が加えられます。既存の構成はすべて再生成されますが、ネットワーク上のデバイスは、リブートされるまで新しい構成を取得しません。

サービス クラスのプロパティを追加、削除、または修正するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Class of Service** を選択します。

ステップ 3　修正するサービス クラスを選択します。

ステップ 4　目的のサービス クラスに対応するリンクをクリックします。Modify Class of Service ページが表示されます。ページの説明の下に、選択したサービス クラスの名前およびタイプが表示されます。

- 選択したサービス クラスに新しいプロパティを追加するには、次の手順に従います。
  - Property Name ドロップダウンから、選択したサービス クラスに割り当てる最初のプロパティを選択し、そのプロパティの適切な値を入力してから、**Add** をクリックします。
  - 選択したサービス クラスに割り当てる他のすべてのプロパティについて、この手順を繰り返します。
- 選択したサービス クラスのプロパティを削除するには、次の手順に従います。
  - Property Name ドロップダウンのすぐ上にあるリストで、不要なプロパティを見つけます。
  - **Delete** をクリックします。
- プロパティに現在割り当てられている値を修正するには、次の手順に従います。
  - 上記と同じ方法で、該当するプロパティを削除します。
  - 同じプロパティをサービス クラスに再度追加し、Property Value に新しい値を入力します。

(注)　必須のプロパティを削除した場合は、修正を確定する前に、そのプロパティを再度追加し、適切な値を選択する必要があります。

ステップ 5　**Submit** をクリックして、サービス クラスに対する修正を実行します。**Submit** をクリックすると、サービス クラスに追加された各プロパティが表示されます。次に、選択したサービス クラスでデバイスの構成を再生成するための確認ページが表示されます。

ステップ 6　**OK** をクリックすると、修正したサービス クラスが Manage Class of Service ページで使用できるようになります。

サービス クラスの削除

既存のサービス クラスはすべて削除できます。ただし、削除する前に、そのサービス クラスに関連付けられたデバイスが存在しないことを確認する必要があります。

ヒント　削除するサービス クラスに関連付けられたデバイスが多数存在する場合は、BACC アプリケーション プログラミング インターフェイス（API）を使用して、これらすべてのデバイスに別のサービス クラスを再割り当てするプログラムを記述します。

デバイスが関連付けられているサービス クラスを削除しようとすると、次のエラー メッセージが表示されます。

```
The following error(s) occurred while processing your request.
Error: Class Of Service [sample-COS] has devices associated with it, unable to delete

Please correct the error(s) and resubmit your request.
```

エラー メッセージでは、特定のサービス クラスが指定されます。この例では、*sample-COS* と指定されています。

サービス クラスを削除するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Class of Service** を選択します。

ステップ 3　目的のサービス クラスに対応する **Delete** をクリックすると、確認ダイアログボックスが表示されます。

(注)　デフォルトの「unprovisioned-docsis」サービス クラスは削除できません。

ステップ 4　**OK** をクリックしてファイルを削除するか、または、**Cancel** をクリックして Manage Class of Service ページに戻ります（図 10-1 を参照してください）。

(注)　サービス クラスにデバイスが関連付けられている場合、または、デフォルトのサービス クラスとして指定されている場合、そのサービス クラスは削除できません。

カスタム プロパティの設定

カスタム プロパティを使用すると、RDU データベースに保存される追加のカスタマイズ可能なデバイス情報を指定できます。Custom Property 設定ページが Configuration メニューの下にあります。このページを使用して、カスタム プロパティを追加または削除します。

注意　カスタム プロパティは使用中でも削除できますが、削除すると、そのプロパティを使用している他の領域に深刻な障害が起こる原因になります。

カスタム プロパティを設定するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Custom Property** を選択します。Configure Custom Properties ページが表示されます。

- カスタム プロパティを追加するには、次の手順に従います。
  - Configure Custom Properties ページで **Add** をクリックします。Add Custom Property ページが表示されます。
  - 新しいカスタム プロパティの名前を入力します。
  - ドロップダウン リストからカスタム プロパティ タイプを選択します。
  - 選択後、**Submit** をクリックします。プロパティが管理データベースに追加されると、Configure Custom Properties ページが表示されます。
- カスタム プロパティを削除するには、次の手順に従います。
  - Configure Custom Properties ページから削除するカスタム プロパティを指定します。
  - 目的のカスタム プロパティに対応する **Delete** アイコンをクリックします。カスタム プロパティ削除ダイアログボックスが表示されます。
  - **OK** をクリックして、そのカスタム プロパティを削除します。

ステップ 3　**Submit** または **OK** をクリックして、カスタム プロパティが追加または削除されると、Configure Custom Properties ページが表示されます。

デフォルトの設定

Configuration オプションから選択した Defaults ページを使用すると、Reagional Distribution Unit（RDU）、Network Registration 拡張、およびサポートされているその他すべての技術を含む、システム全体のデフォルト設定にアクセスできます。

設定オプションの選択

特定のデフォルト タイプを設定する手順は、すべて共通です。この手順に従って目的のデフォルト ページを表示してから、この章の該当する項で、ページの各部分の説明を参照してください。

ステップ 1　プライマリ ナビゲーション バーまたは Main Menu ページで、**Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Defaults** を選択します。Configure Defaults ページが表示されます。

ステップ 3　画面の左側にあるリストから、目的のデフォルト タイプを選択します。対応するデフォルト ページが表示されます。

ATA 186 Defaults

Cisco ATA 186 は、受話器とイーサネット間に接続するアダプタで、従来の電話をイーサネット IP 電話に変換します。このデバイスに既存のアナログ電話を接続することで、IP テレフォニーの多くのアプリケーションが利用できるようになります。

ATA 186 Defaults の Configure Defaults ページ（図 10-2）には、ATA 186 をサポートするために現在使用できるデフォルト値のリストが表示されます。

図 10-2　ATA 186 Defaults の Configure Defaults ページ

図 10-2 のフィールドとボタンを表 10-3 に示します。多くの場合、このページに表示されるパラメータは他のデフォルト ページにも表示されます。

表 10-3　ATA 186 Defaults の Configure Defaults ページ

フィールドまたはボタン	説明
Extension Point	このテクノロジーのデバイスに対する構成を生成するときに実行する拡張ポイントを指定します。
Disruption Extension Point	このテクノロジーのデバイスを中断するために実行する拡張ポイントを指定します。
Service Level Selection Extension Point	デバイスに必要な DHCP 基準およびサービス クラスを判別するために使用される拡張ポイントを指定します。
Default Class of Service	特定のデバイス テクノロジー（この例では、ATA186）に対する現行のデフォルト サービス クラスを指定します。そのテクノロジー タイプの、まだ認識されていない新規のデバイスは、このサービス クラスに割り当てられます。ドロップダウン リストを使用して、新しいデフォルト値を選択します。
Default DHCP Criteria	特定のデバイス テクノロジー（この例では、ATA186）に対する現行のデフォルト DHCP 基準を指定します。そのテクノロジー タイプの、まだ認識されていない新規のデバイスは、このデフォルト DHCP 基準に割り当てられます。ドロップダウン リストを使用して、新しいデフォルト値を選択します。

表 10-3　ATA 186 Defaults の Configure Defaults ページ （続き）

フィールドまたはボタン	説明（続き）
Automatic FQDN Generation	デバイスに対するホスト名およびドメイン名を自動的に生成します。次の 2 つのオプションを選択できます。 • Enabled：FQDN の自動生成をイネーブルにします。 • Disabled：FQDN の自動生成をディセーブルにします。 （注）　詳細については、P.10-40 の「FQDN の自動生成」を参照してください。
Submit	行った変更を有効にします。管理データベースが更新されると、行った変更が Configure Defaults ページに反映されます。
Reset	すべての設定を元の設定に戻します。

ATA 188 Defaults

Cisco ATA 188 は、通常の電話機と IP ベースのイーサネット テレフォニー ネットワークとをつなぎます。ATA 188 は、企業、小規模オフィス、および先端の VoIP 管理音声サービスやローカル サービス市場などのニーズに対応した、真の次世代 VoIP の終端を提供します。

ATA 188 Default の Configure Defaults ページには、ATA 188 をサポートするために現在使用できるデフォルト値のリストが表示されます。ATA 188 に対して表示されるデフォルト パラメータは、ATA 186 に対して表示されるものと同じですが、選択する値が異なる場合があります。

CableHome WAN Defaults

CableHome WAN のデフォルト画面には、WAN-Data デバイス用と WAN-Man デバイス用の 2 つの異なる画面があります。

対応する WAN-Man デバイスに完全に依存している WAN-Data デバイスは、ケーブル モデムと比較すると、無差別モードで動作するコンピュータに似ています。WAN-Data デバイスは、MAC アドレスと IP アドレスだけです。

どちらの場合も、表示されるリストから目的のデフォルトを選択して、対応するページを表示します。WAN の各デフォルト ページには、表 10-4 に示すフィールドとボタンが含まれています。

表 10-4　WAN MAN または WAN Data Defaults の Configure Defaults ページ

フィールドまたはボタン	説明
Extension Point	WAN デバイスに対する構成を生成するときに実行する拡張ポイントを指定します。
Disruption Extension Point	WAN デバイスを中断するために実行する拡張ポイントを指定します。
Service Level Selection Extension Point	デバイスに必要な DHCP 基準およびサービス クラスを判別するために使用される拡張ポイントを指定します。
Default Class of Service	WAN-Data に対する現行のデフォルト サービス クラスを指定します。まだ認識されていない新規の WAN デバイスは、このサービス クラスに割り当てられます。ドロップダウン リストを使用して、新しいデフォルト値を選択します。

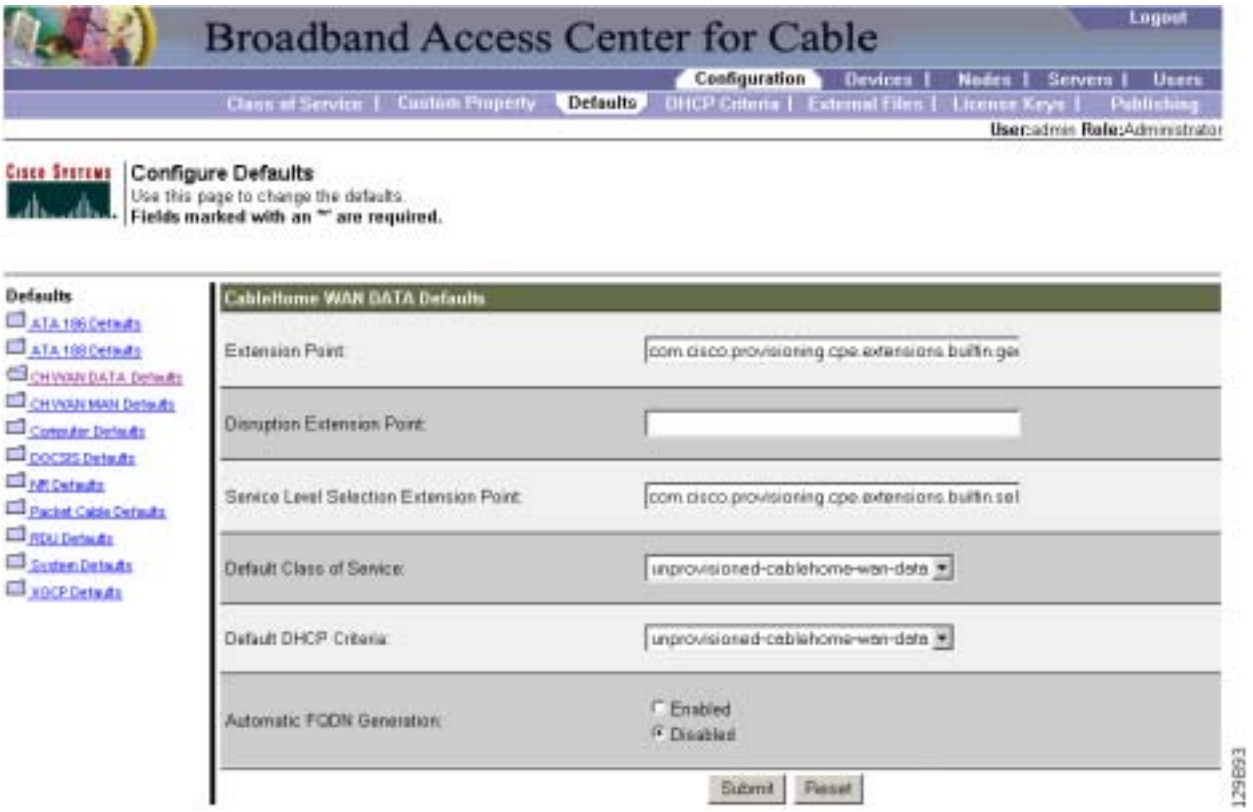
表 10-4　WAN MAN または WAN Data Defaults の Configure Defaults ページ（続き）

フィールドまたはボタン	説明
Default DHCP Criteria	特定のデバイス テクノロジーに対する現行のデフォルト DHCP 基準を指定します。まだ認識されていない新規の WAN デバイスは、このデフォルト DHCP 基準に割り当てられます。ドロップダウン リストを使用して、新しいデフォルト値を選択します。
Automatic FQDN Generation	デバイスに対するホスト名およびドメイン名を自動的に生成します。次の 2 つのオプションを選択できます。 • Enabled：FQDN の自動生成をイネーブルにします。 • Disabled：FQDN の自動生成をディセーブルにします。 (注)　詳細については、P.10-40 の「FQDN の自動生成」を参照してください。

CableHome WAN Data Defaults

CableHome Wide Area Network（WAN）DATA Defaults リンクを選択すると、CableHome WAN DATA Defaults の Configure Defaults ページ（図 10-3 を参照）が表示されます。このページを使用して、WAN-Data デバイス タイプを設定します。

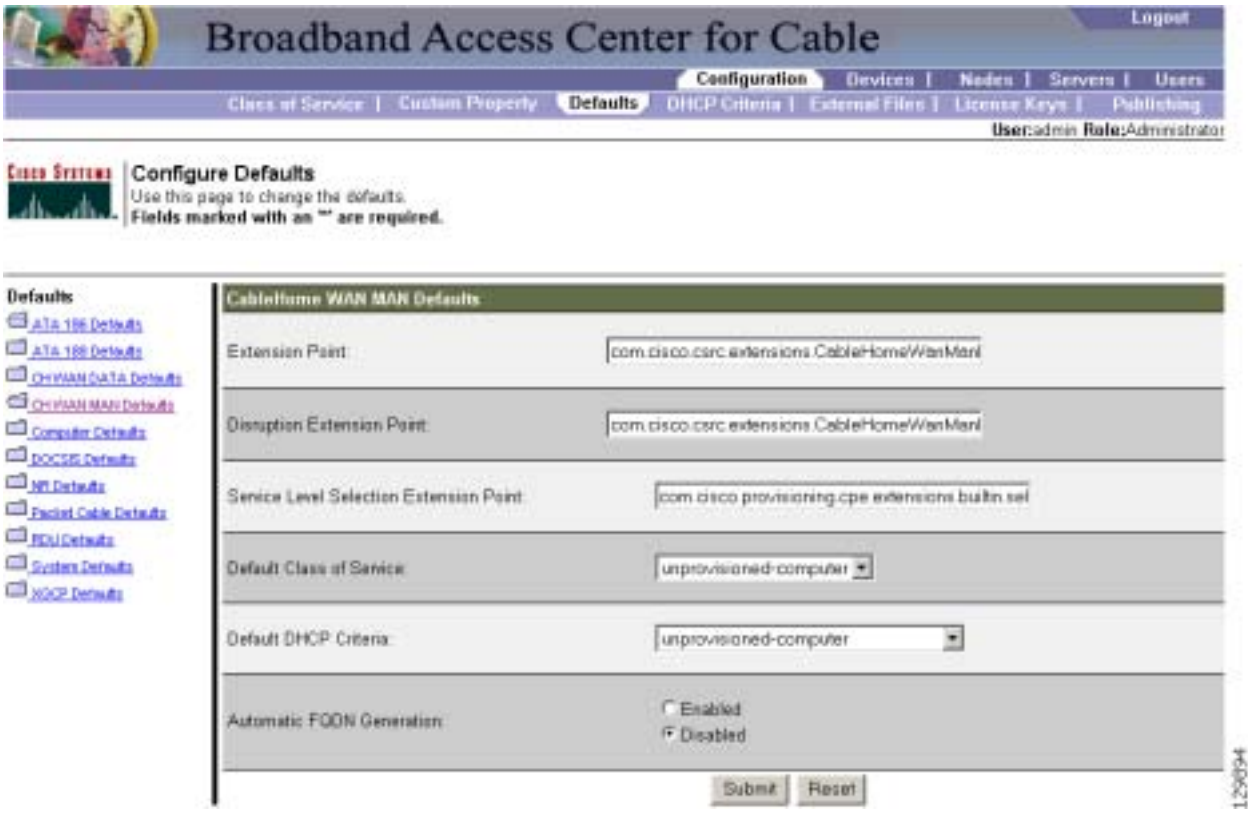
図 10-3　CableHome WAN-Data Defaults の Configure Defaults ページ



CableHome WAN-Man Defaults

CableHome WAN-Man Defaults リンクを選択すると、CableHome WAN-Man Defaults の Configure Defaults ページ（図 10-4 を参照）が表示されます。このページを使用して、WAN-Man デバイス タイプを設定します。

図 10-4　CableHome WAN-Man Defaults の Configure Defaults ページ



Computer Defaults

Computer Defaults ページ（図 10-5）には、BACC によってサポートされるコンピュータに現在適用されているデフォルト値のリストが表示されます。

図 10-5　Computer Defaults の Configure Defaults ページ

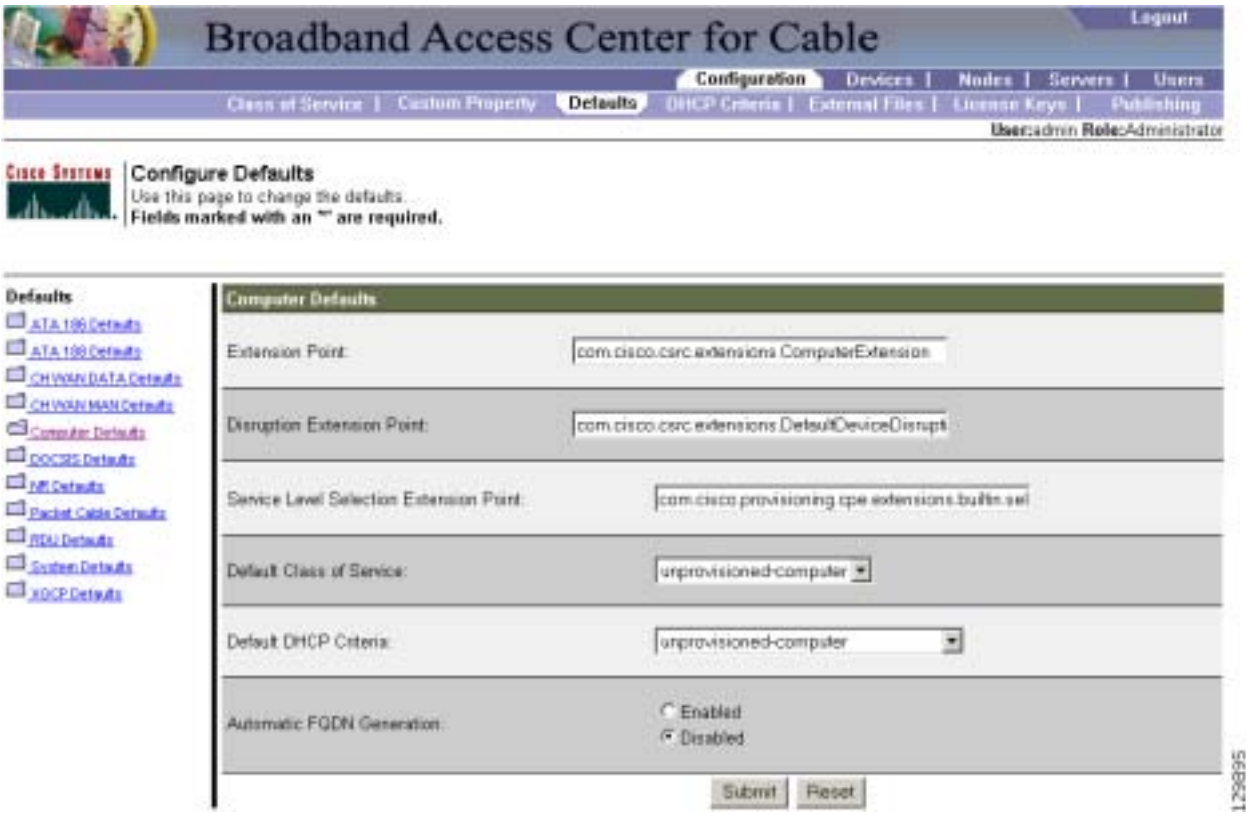


図 10-5 に示すすべてのフィールドとボタンの説明については、表 10-3 を参照してください。

(注)　デフォルト サービス クラスとデフォルト DHCP 基準を変更すると、再生成が実行されます。このページにそれ以外の変更を行っても、現行のデバイスに影響を与えません。

DOCSIS Defaults

DOCSIS Defaults オプションを選択すると、DOCSIS Defaults ページが表示されます。このページ（図 10-6）には、BACC によってサポートされるケーブル モデムに現在適用されているデフォルト DOCSIS 値のリストが表示されます。

図 10-6　DOCSIS Defaults の Configure Defaults ページ

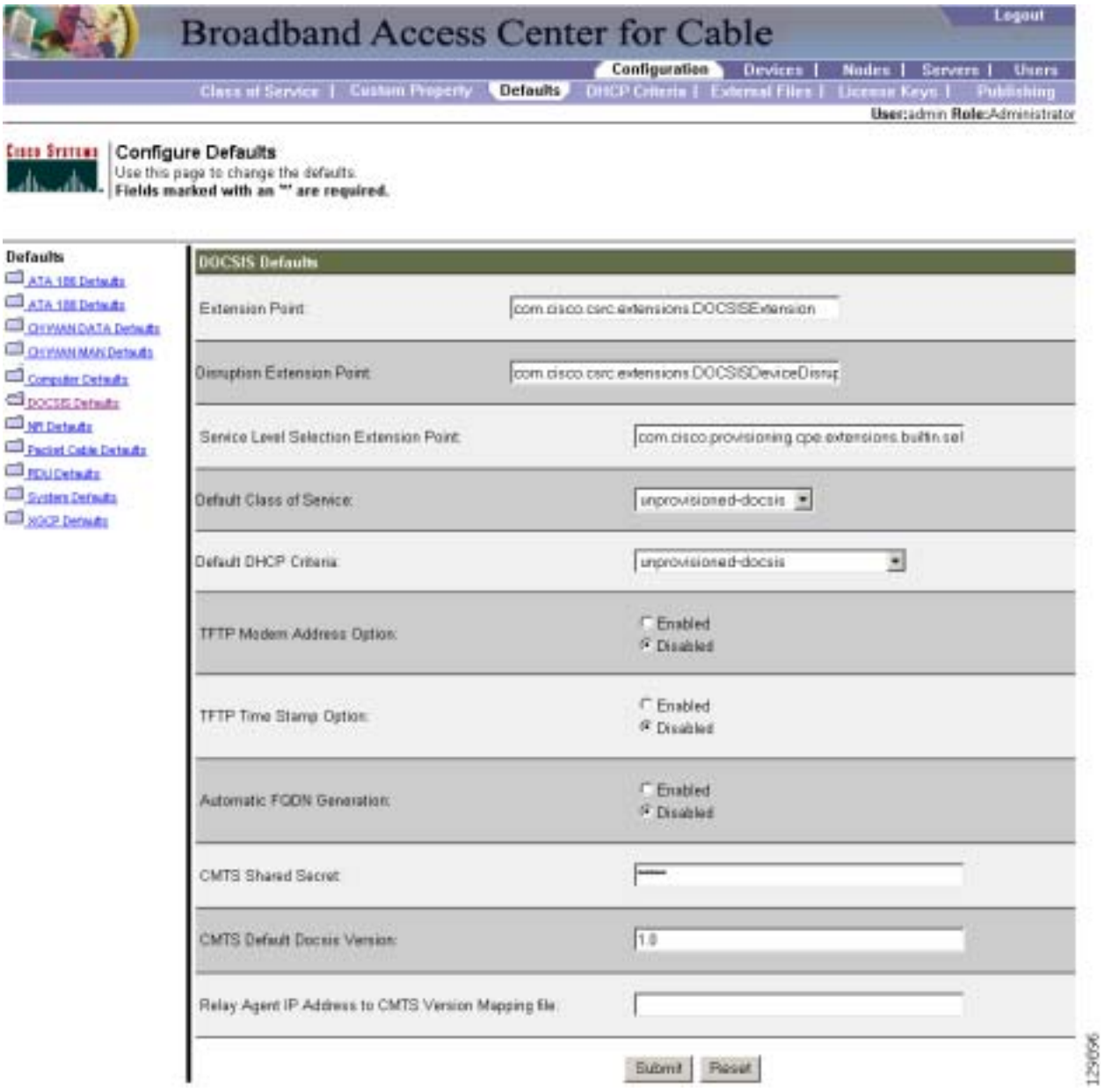


図 10-6 に示すすべてのフィールドとボタンの説明については、表 10-5 を参照してください。

（注）　デフォルト サービス クラスとデフォルト DHCP 基準を変更すると、再生成が実行されます。いずれかの TFTP オプションを変更すると、次回の TFTP 転送から有効になります。

このデフォルト ページに固有のフィールドとボタンを表 10-5 に示します。

表 10-5　DOCSIS Defaults の Configure Defaults ページ

フィールドまたはボタン	説明
Extension Point	DOCSIS デバイスに対する構成を生成するときに実行する拡張ポイントを指定します。
Disruption Extension Point	DOCSIS デバイスを中断するために実行する拡張ポイントを指定します。
Service Level Selection Extension Point	デバイスに必要な DHCP 基準およびサービス クラスを判別するために使用される拡張ポイントを指定します。
Default Class of Service	デバイスに対する現行のデフォルト サービス クラスを指定します。まだ認識されていない新規のデバイスは、このサービス クラスに割り当てられます。ドロップダウン リストを使用して、新しいデフォルト値を選択します。
Default DHCP Criteria	特定のデバイス テクノロジーに対する現行のデフォルト DHCP 基準を指定します。まだ認識されていない新規のデバイスは、このデフォルト DHCP 基準に割り当てられます。ドロップダウン リストを使用して、新しいデフォルト値を選択します。
TFTP Modem Address Option	TFTP モデム アドレス オプションをイネーブルにするかどうかを指定します。
TFTP Time Stamp	TFTP サーバがタイム スタンプを発行するかどうかを指定します。
Automatic FQDN Generation	デバイスに対するホスト名およびドメイン名を自動的に生成します。次の 2 つのオプションを選択できます。 • Enabled：FQDN の自動生成をイネーブルにします。 • Disabled：FQDN の自動生成をディセーブルにします。 **(注)** 詳細については、P.10-40 の「FQDN の自動生成」を参照してください。
CMTS Shared Secret	BACC が設定ファイルの CMTS MIC の計算に使用する文字列を指定します。CMTS はこの文字列を使用して、ケーブル モデムが許可を得るために CMTS に送信する設定ファイルを認証します。
CMTS Default Docsis Version	すべての CMTS で使用されるデフォルトの DOCSIS バージョンを指定します。このフィールドに DOCSIS バージョンを入力しない場合は、デフォルトでバージョン 1.0 が指定されます。
Relay Agent IP Address to CMTS Version Mapping file	CMTS で使用されるマッピング ファイルを指定します。このファイルは、CMTS が使用する DOCSIS バージョンを指定します。

(注) このページの TFTP オプションの一方または両方をイネーブルにした場合、それに対応する TFTP 情報は、DOCSIS ケーブル モデムに送信される前に、TFTP ファイルに書き込まれます。

Network Registrar Defaults

BACC は、Network Registrar（NR）拡張ポイントを提供します。これらの拡張ポイントによって、BACC は、着信 DHCP パケットから、デバイスのテクノロジーを検出するための情報を引き出すことができます。また、これらの拡張ポイントによって、BACC は、DPE に保存されている設定に対応するオプションが指定されたデバイス DHCP 要求に応答することができます。

NR Defaults オプションを選択すると、NR Defaults ページ（図 10-7 を参照）が表示されます。

図 10-7　Network Registrar Defaults の Configure Default ページ

図 10-7 に示すすべてのフィールドとボタンの説明については、表 10-6 を参照してください。

表 10-6　Network Registrar Defaults の Configure Default ページ

フィールドまたはボタン	説明
NR Attributes from Request Dictionary (for 2.0 Extensions)	現行デバイスの構成を生成する要求を RDU に送信するときに、Network Registrar 要求辞書から文字列として引き出される属性を、カンマ区切りリストで指定します。 **（注）** このプロパティは、BPR 2.0 Network Registrar 拡張のみに適用されます。
NR Attributes from Request Dictionary as Bytes (for 2.5 Extensions)	現行デバイスの構成を生成する要求を RDU に送信するときに、Network Registrar 要求辞書からバイトとして引き出される属性を、カンマ区切りリストで指定します。 **（注）** このプロパティは、BACC 2.5（または、それ以降）の Network Registrar 拡張のみに適用されます。

表 10-6　Network Registrar Defaults の Configure Default ページ （続き）

フィールドまたはボタン	説明
NR Attributes from Request Directory as Strings (for 2.5 Extensions)	現行デバイスの構成を生成する要求を RDU に送信するときに、Network Registrar 要求辞書から文字列として引き出される属性を、カンマ区切りリストで指定します。 （注）　このプロパティは、BACC 2.5（または、それ以降）の Network Registrar 拡張のみに適用されます。
NR Attributes from Environment Directory	現行デバイスの構成を生成する要求を RDU に送信するときに、Network Registrar 環境辞書から文字列として引き出される属性を、カンマ区切りリストで指定します。 （注）　このプロパティは、BPR 2.0 および BACC 2.5（または、それ以降）の Network Registrar 拡張のみに適用されます。
Submit	行った変更を有効化または実装します。管理データベースが更新されて、行った変更が反映されると、修正した内容が Configure Defaults ページに表示されます。
Reset	すべての設定を元の設定に戻します。

（注）　このページに対して行った変更は、Network Registrar 拡張がリロードされるまで有効になりません。

PacketCable Defaults

PacketCable Defaults ページでは、PacketCable 音声技術をサポートするために必要なデフォルトを設定します。選択すると、PacketCable Defaults ページ（図 10-8 を参照）が表示されます。

図 10-8　PacketCable（音声技術）Defaults の Configure Defaults ページ

このデフォルト ページに固有のフィールドとボタンを表 10-7 に示します。

表 10-7　PacketCable（音声技術）Defaults の Configure Defaults ページ

フィールドまたはボタン	説明
Extension Point	このテクノロジーのデバイスに対する構成を生成するときに実行する拡張ポイントを指定します。
Disruption Extension Point	このテクノロジーのデバイスを中断するために実行する拡張ポイントを指定します。
Service Level Selection Extension Point	デバイスに必要な DHCP 基準およびサービス クラスを判別するために使用される拡張ポイントを指定します。
Default Class of Service	デバイスに対する現行のデフォルト サービス クラスを指定します。まだ認識されていない新規のデバイスは、このサービス クラスに割り当てられます。ドロップダウン リストを使用して、新しいデフォルト値を選択します。

表 10-7　PacketCable（音声技術）Defaults の Configure Defaults ページ （続き）

フィールドまたはボタン	説明
Default DHCP Criteria	特定のデバイス テクノロジーに対する現行のデフォルト DHCP 基準を指定します。まだ認識されていない新規のデバイスは、このデフォルト DHCP 基準に割り当てられます。ドロップダウン リストを使用して、新しいデフォルト値を選択します。
SNMP Set Timeout	SNMP の設定タイムアウトを秒単位で指定します。
MTA Provisioning Notification	MTA イベントが発生したことを知らせる通知です。MTA がプロビジョニング完了情報を送信するとき、選択されたオプションに基づいたイベントが発生します。次のオプションを選択できます。 • On Failure • On Success • During Provisioning • Always • Never
Automatic FQDN Generation	Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を生成するかどうかを指定します。

RDU Defaults

RDU Defaults リンクを選択すると、RDU Defaults ページ（図 10-9 を参照）が表示されます。このページを使用して、RDU が Network Registrar と通信するように設定します。詳細については、『*Cisco CNS Network Registrar User's Guide*』を参照してください。

図 10-9　RDU Defaults の Configure Defaults ページ

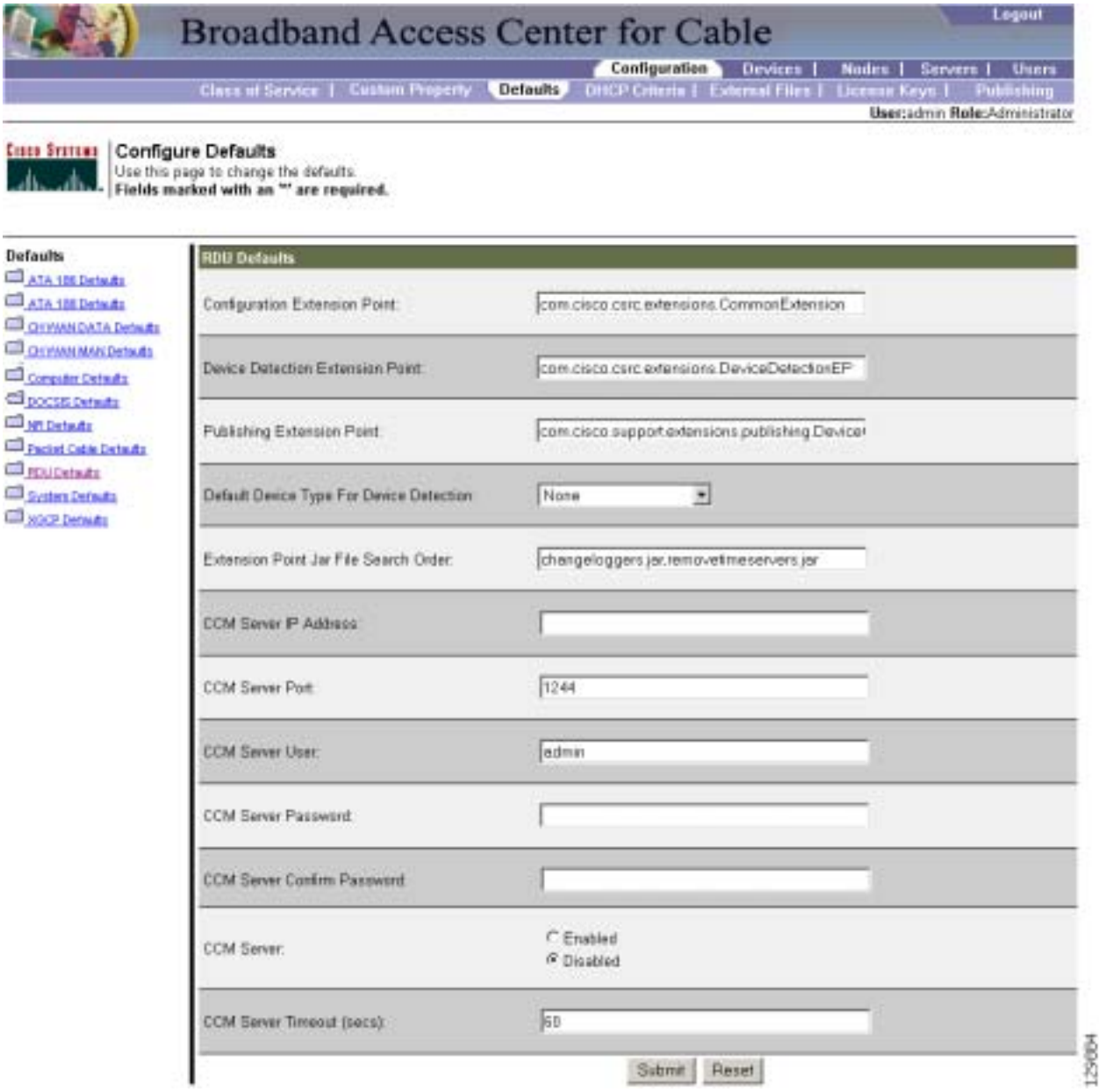


図 10-9 に示すすべてのフィールドとボタンを表 10-8 に示します。

表 10-8　RDU Defaults の Configure Defaults ページ

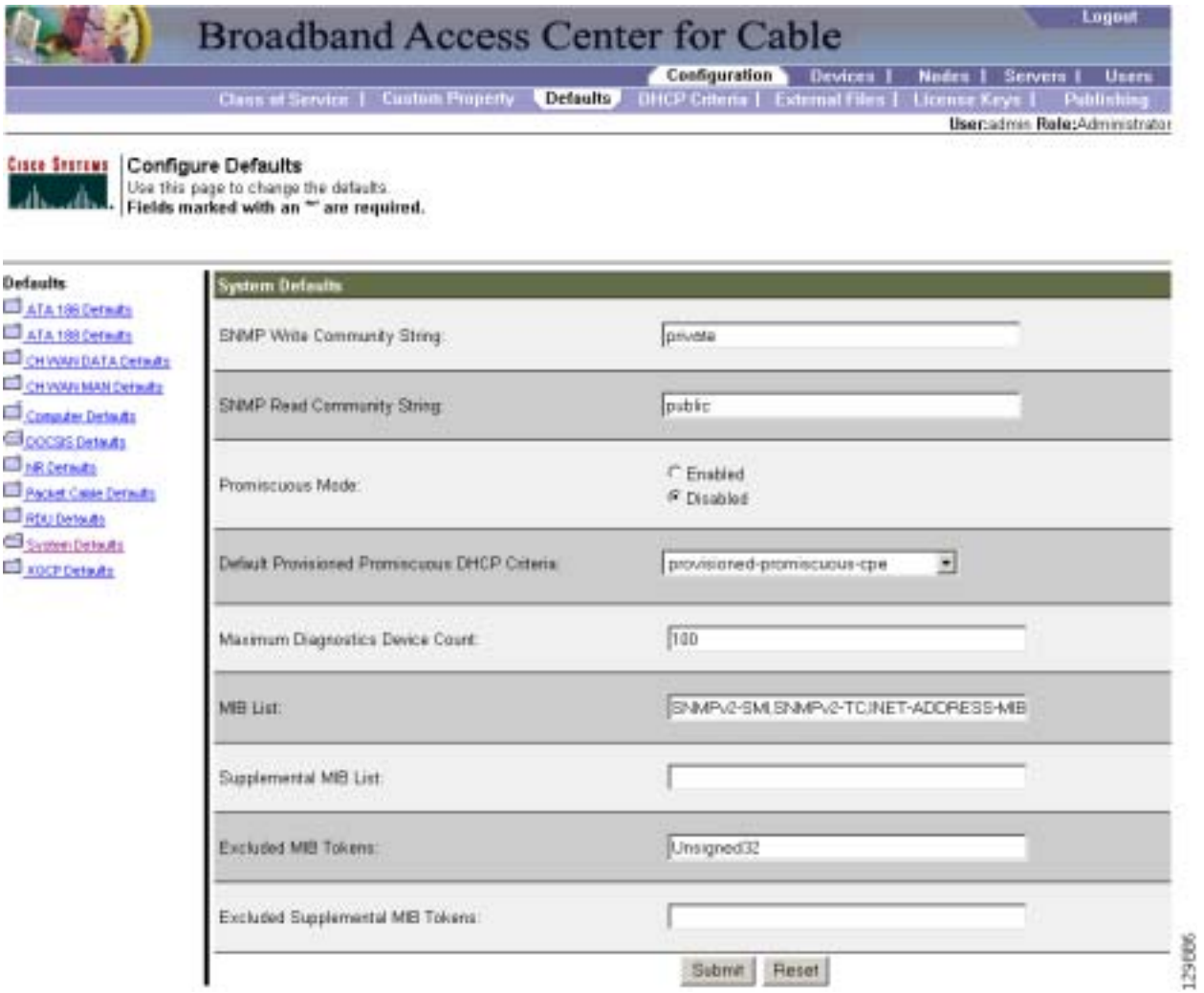
フィールドまたはボタン	説明
Configuration Extension Point	他のテクノロジー拡張ポイントが実行される前に実行する共通拡張ポイントを指定します。
Device Detection Extension Point	デバイスの DHCP DISCOVER 要求から引き出された情報に基づいてデバイス タイプ（DOCSIS やコンピュータなど）を判別するために使用される拡張ポイントを指定します。
Publishing Extension Point	RDU パブリッシング プラグインに使用される拡張ポイントを指定します。これは、RDU データを別のデータベースにパブリッシングするときに役立ちます。
Extension Point Jar File Search Order	上記の 4 つのフィールドにリストされている Jar ファイルでクラスを検索するときの順序を指定します。
CCM Server IP Address	CCM サーバの IP アドレスを指定します。
CCM Server Port	BACC が通信する CCM サーバのポートを指定します。
CCM Server User	CCM サーバのユーザ名を指定します。このユーザ名は、パスワード フィールドと組み合せて使用されます。
CCM Server Password	CCM サーバのユーザ認証に使用されるパスワードを指定します。
CCM Server Confirm Password	CCM サーバのパスワードを認証します。
CCM Server	CCM サーバに対する BACC インターフェイスをイネーブルにするかどうかを指定します。
CCM Server Timeout (ms)	BACC が接続ダウンを宣言する前に CCM サーバとの接続を試行する期間を指定します。

（注） RDU 拡張ポイントの詳細については、P.10-34 の「Regional Distribution Unit 拡張の管理」を参照してください。

System Defaults

Systems Defaults リンクを選択すると、System Defaults ページ（図 10-10 を参照）が表示されます。

図 10-10　System Defaults の Configure Defaults ページ



(注)　BACC のアプリケーション プログラム インターフェイスを使用して、デフォルト値を設定できます。

図 10-10 に示すすべてのフィールドとボタンを表 10-9 に示します。

表 10-9　System Defaults の Configure Defaults ページ

フィールドまたはボタン	説明
SNMP Write Community String	SNMP 情報を必要とする可能性があるデバイスに対するデフォルトのライト（write）コミュニティ ストリングを指定します。デフォルトのライト（write）コミュニティ ストリングは、**private** です。
SNMP Read Community String	SNMP MIB に対する読み取りまたはアクセスが可能なデバイスに対するデフォルトのリード（read）コミュニティ ストリングを指定します。デフォルトのリード（read）コミュニティ ストリングは、**public** です。
Promiscuous Mode	無差別モードをイネーブルにするかどうかを指定します。次の 2 つのオプションを選択できます。 • Enable：BACC の内部で無差別モードをイネーブルにします。 • Disable：BACC　の内部で無差別モードをディセーブルにします。
Default Provisioned Promiscuous DHCP Criteria	CPE が背後にあるデバイスが CPE DHCP 基準を指定されていない場合に、CPE を無差別モードでプロビジョニングするために使用されるデフォルトの DHCP 基準を指定します。
Maximum Diagnostic Device Count	一度にトラブルシューティングを行うことができる MAC アドレス（デバイス）の最大数を指定します。
MIB List	RDU の再起動を必要としない、RDU で使用される MIB のリストを指定します。
Supplemental MIB List	RDU で使用される MIB の拡張リストを指定します。
Excluded MIB Tokens	MIB で再定義できないキーワード（トークン）を定義します。
Excluded Supplemental MIB Tokens	MIB で再定義できず、Excluded MIB Tokens リストに表示されない追加のキーワード（トークン）を定義します。

Gateway（xGCP）Control Protocol Defaults

XGCP は、外部のコール エージェントが VoIP 環境でゲートウェイを制御できるゲートウェイ コントロール プロトコルです。XGCP Defaults の Configure Defaults ページ（図 10-11）には、BACC によってサポートされる xGCP ゲートウェイ デバイスに現在適用されているデフォルト値のリストが表示されます。

図 10-11　XGCP Defaults の Configure Defaults ページ

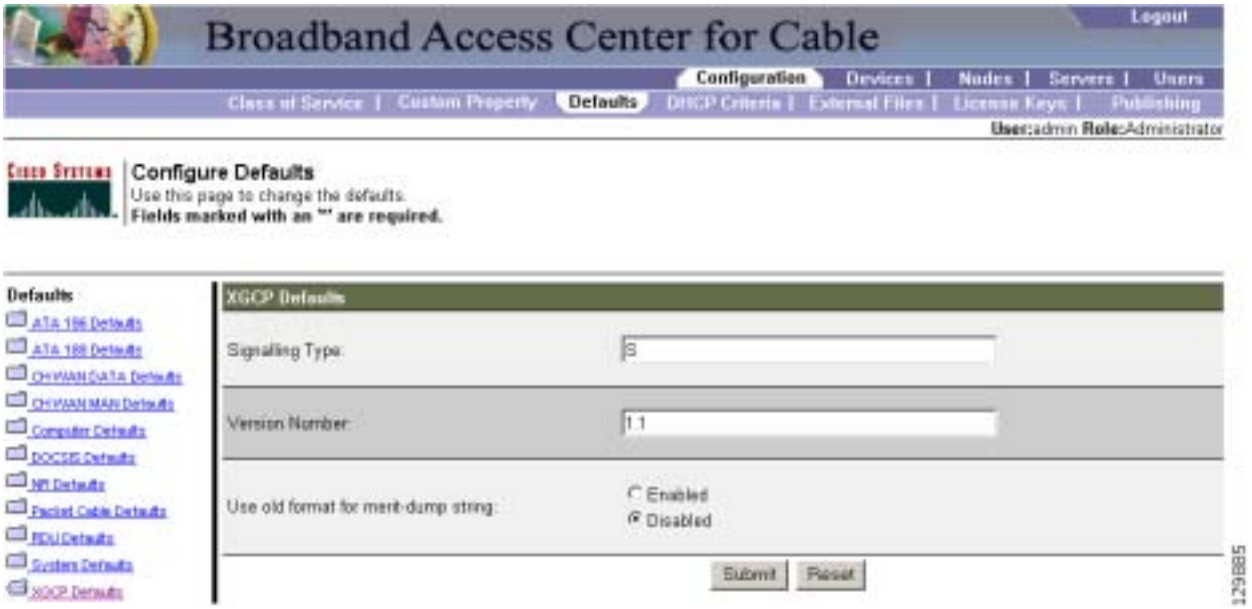


図 10-11 に示すすべてのフィールドとボタンを表 10-10 に示します。

表 10-10　XGCP Defaults の Configure Defaults ページ

フィールドまたはボタン	説明
Signalling Type	S、M などの xGCP シグナリング タイプを指定します。
Version Number	使用している xGCP のバージョン番号を指定します。
Use old format for merit-dump string	このバージョン番号には含まれていない、古い文字列形式の使用をイネーブルまたはディセーブルにします。

（注）　これ以後のデバイス構成には、ここで行う修正が加えられます。ただし、既存のすべての構成が変更されるわけではありません。既存の構成に変更を加えるには、アプリケーション プログラミング インターフェイス（API）を使用して構成を再生成する必要があります。

DHCP 基準の設定

BACC では、Network Registrar 内のスコープを選択するときのデバイスに対する特定の基準が、DHCP 基準に記述されています。たとえば、**provisioned-docsis** という DHCP 基準には、**tagProvisioned** という包含選択タグが含まれています。DHCP 基準は、DOCSIS モデムと関連付けられています。このモデムが Network Registrar からの IP アドレスを要求すると、Network Registrar は、スコープ選択タグ **tagProvisioned** に関連付けられたスコープを検索します。

DHCP Criteria ページを表示するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **DHCP Criteria** を選択します。Manage DHCP Criteria ページが表示されます。

DHCP 基準の追加

DHCP 基準を追加するには、次の手順に従います。

ステップ 1　DHCP Criteria ページで **Add** をクリックします。Add DHCP Criteria ページが表示されます。

ステップ 2　作成する DHCP 基準の名前を入力します。

ステップ 3　DHCP 基準クライアントクラス名を入力します。

ステップ 4　包含選択タグと除外選択タグを入力します。

（注）　新規の DHCP 基準を作成するとき、入力するクライアントクラス、包含選択タグ、および除外選択タグの名前は、Network Registrar 内から取得した正確な名前にする必要があります。クライアントクラスおよび選択タグの詳細については、『*Network Registrar User's Guide*』および『*Network Registrar CLI Reference*』を参照してください。新規の DHCP 基準を作成するときは、クライアントクラス名、包含選択タグ名、または除外選択タグ名のいずれかを指定する必要があります。

ステップ 5　DHCP 基準に追加するプロパティを追加または修正できます。Property Name でプロパティ名を入力または選択するか、あるいは既存の名前を選択し、該当の Property Value を入力または修正します。

ステップ 6　プロパティ名とプロパティ値のペアを変更または作成してから、**Add** をクリックします。

ステップ 7　**Submit** をクリックします。RDU データベースに DHCP 基準が正常に追加されると、Manage DHCP Criteria ページにその基準が表示されます。

DHCP 基準の修正

既存の DHCP 基準を修正するには、次の手順に従います。

ステップ 1　Manage DHCP Criteria ページで、修正する DHCP 基準のリンクをクリックします。Modify DHCP Criteria ページが表示されます。

ステップ 2　クライアントクラス、包含選択タグ、除外選択タグ、およびプロパティ値の設定に対して必要な変更を行います。

ステップ 3　**Submit** をクリックします。RDU データベース内の DHCP 基準が正常に修正された後、Manage DHCP Criteria ページが表示されます。

(注)　これ以後のデバイス構成には、ここで行う修正が加えられます。既存の構成はすべて再生成されますが、ネットワーク上のデバイスは、リブートされるまで新しい構成を取得しません。

DHCP 基準の削除

管理アプリケーションを使用して DHCP 基準を削除しても、実際の DHCP サーバ構成は DHCP サーバから削除されません。DHCP サーバ構成は手動で削除する必要があります。既存の基準を削除するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **DHCP Criteria** を選択します。Manage DHCP Criteria ページが表示されます。

ステップ 3　削除する基準に対応する **Delete** アイコンをクリックします。削除ダイアログボックスが表示されます。

ステップ 4　**OK** をクリックして基準を削除するか、または、**Cancel** をクリックして操作を中断します。Manage DHCP Criteria ページが表示されます。

(注)　DHCP 基準を削除できるのは、その基準に関連付けられているデバイスがなく、かつ、その基準がデフォルト DHCP 基準として指定されていない場合に限られます。DHCP 基準にデバイスが関連付けられている場合、その基準を削除する前に、別の DHCP 基準を関連付ける必要があります。

外部ファイルの管理

BACC 管理ユーザ インターフェイスを使用して、DOCSIS、PacketCable MTA、および WAN-Man ファイル、またはデバイスのソフトウェア イメージを動的生成するための TFTP サーバ ファイルまたはテンプレート ファイルを管理できます（図 10-12 を参照してください）。次に示すいずれかのファイル タイプを追加、削除、置換、またはエクスポートできます。

- テンプレート ファイル：このファイルは、DOCSIS オプション、PacketCable オプション、または CableHome オプションのいずれかが記述されたテキスト ファイルであり、特定のサービス クラスと組み合せて使用する場合には、動的ファイル生成を行うための値も記述されています。

(注) テンプレート ファイルは、任意のテキスト エディタで作成できますが、tmpl ファイル拡張子を付ける必要があります。テンプレートの詳細については、P.12-2 の「テンプレート ファイルの作成」を参照してください。

- 静的設定ファイル：このファイルは、デバイス用の設定ファイルとして使用されます。たとえば、gold.cm という静的設定ファイルは、gold DOCSIS サービス クラスを識別表します。BACC は、このファイル タイプをその他のバイナリ ファイルと同様に扱います。
- IOS イメージ：シスコのデバイス用のファームウェアが格納されたイメージです。シスコのデバイスは、このイメージをアップロードすることによって機能をアップグレードできます。BACC は、このファイル タイプをその他のバイナリ ファイルと同様に扱います。

(注) 図 10-12 は、Manage External Files ページで Search ボタンをクリックすると表示されます。

図 10-12　Manage External Files ページ

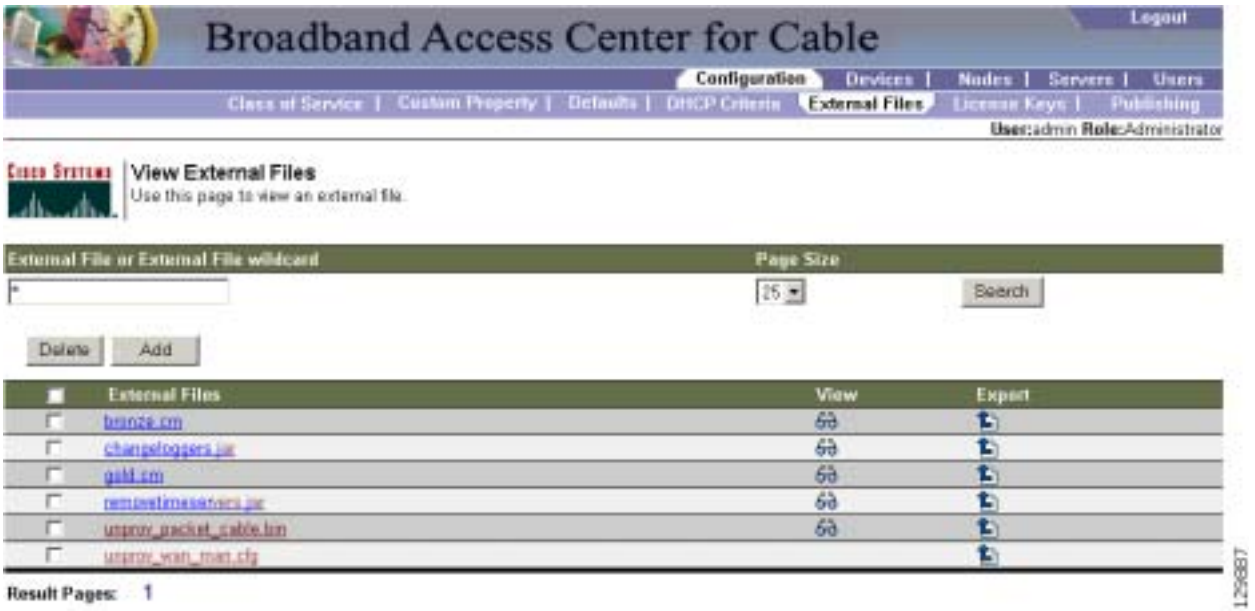


図 10-12 のフィールドとボタンを表 10-11 に示します。

表 10-11　Manage External Files ページ

フィールドまたはボタン	説明
External Files	ファイル名を指定します。アスタリスク（*）をワイルドカードとして使用して、ファイル名の一部で検索できます。たとえば、***.cm** と入力して、末尾に .cm 拡張子が付いた外部ファイルをすべて一覧表示できます。無効なワイルドカードの例は、bronze* です。
Page Size	表示するページの長さを指定します。
Search	External Files フィールドに入力したファイル名と一致する外部ファイルの検索を開始します。
Delete	選択した外部ファイルをデータベースから削除します。
Add	新しいファイルを追加します。
External Files list	検索基準と一致した外部ファイルのリストが表示されます。 **（注）** このリストで選択した項目を削除するには、その項目のすぐ左にあるチェックボックスをチェックする必要があります。
View	選択したバイナリ ファイルの詳細情報が表示されます。
Export	選択したファイルをクライアントのコンピュータにエクスポートします。

外部ファイルの追加

既存の外部ファイルを追加するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **External Files** を選択します。Manage External Files ページが表示されます。

ステップ 3　**Add** をクリックして Add External Files ページを表示します。

ステップ 4　**Source filename** にソース ファイル名、**External filename** に外部ファイル名を入力します。

（注） ソースファイルの正確な名前が分からない場合は、**Browse** 機能を使用して目的のディレクトリまで移動し、そのファイルを選択します。デフォルトでは、最大 12 MB のファイル サイズがサポートされています。

ステップ 5　**Submit** をクリックします。Manage External Files ページが表示され、追加されたファイルが示されます。

外部ファイルの表示

DOCSIS または PacketCable 音声技術の外部ファイルの内容を表示するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **External Files** を選択します。Manage External Files ページが表示されます。

ステップ 3　検索フィールドと適切なワイルドカード文字を使用して、必要なファイルを検索します。

ステップ 4　DOCSIS、CableHome WAN-Man、および PacketCable MTA バイナリ設定ファイルに対応する **Details** アイコンをクリックします。View Binary File Contents ページが表示されます。図 10-13 にバイナリ ファイルの内容の例を、図 10-14 に Jar ファイルの内容の例を示します。

図 10-13　バイナリ ファイルの内容の例

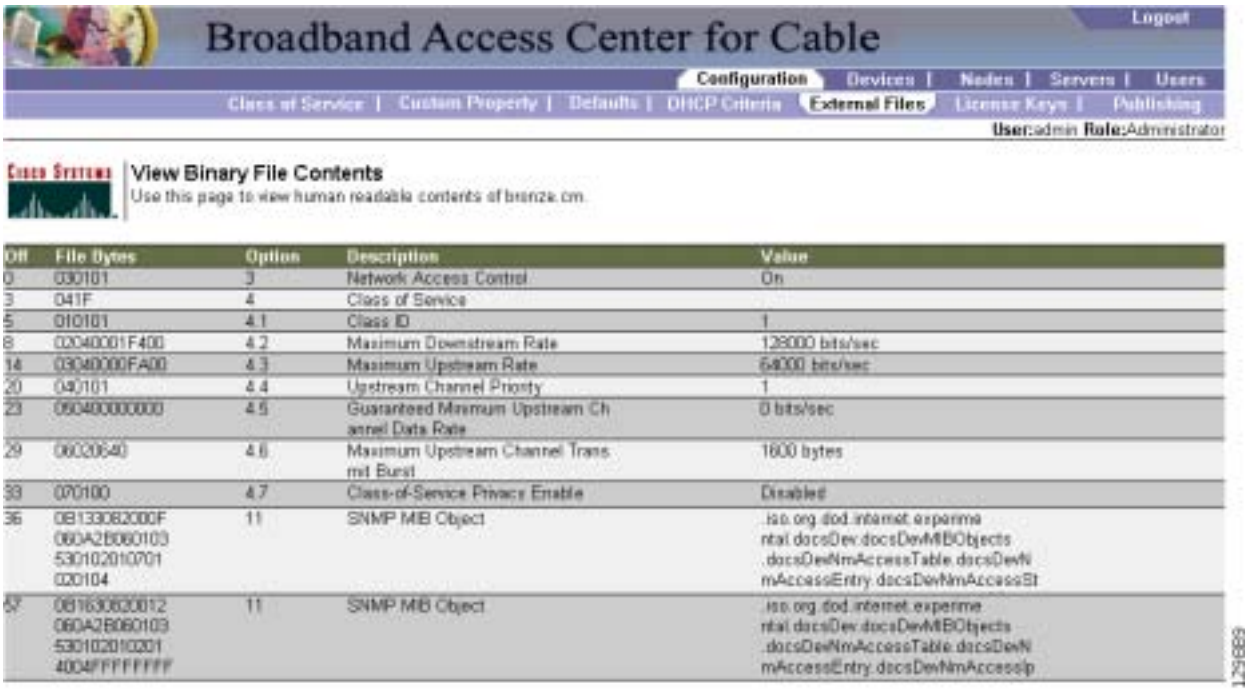
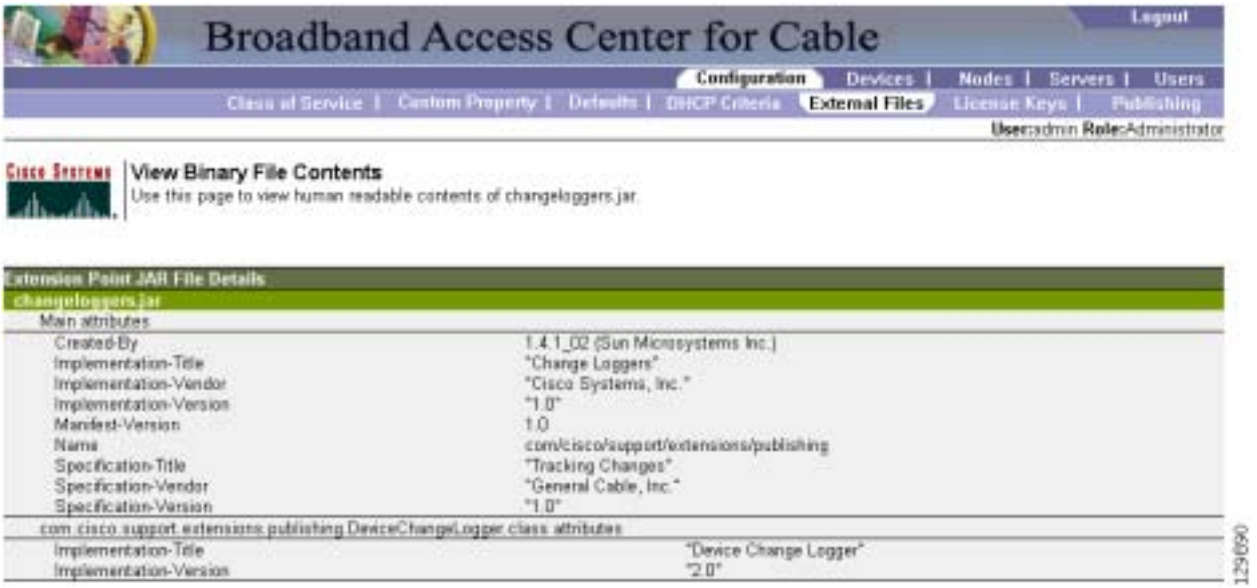


図 10-14　Jar ファイルの内容の例



外部ファイルの置換

既存の外部ファイルを置換するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **External Files** を選択します。

ステップ 3　検索出力リストから、置換するファイルに対応するリンクを選択します。Replace External Files ページが表示されます。選択したファイル名がすでにこのページに表示されています。

ステップ 4　ファイル名が表示されている外部ファイルと置換する、ソース ファイルのパスおよびファイル名を入力します。

（注）　ソースファイルの正確な名前や場所が分からない場合は、**Browse**　機能を使用して目的のディレクトリまで移動し、そのファイルを選択します。

ステップ 5　**Submit**　をクリックします。置換ファイルを決定した後に確認ページが表示されて、置換後、影響を受けるデバイスの構成が BACC によって再生成されることが示されます。

ステップ 6　**OK** をクリックします。Manage External Files ページが表示されます。

（注）　置換が終了すると、サービス クラスを通してこのファイルを使用するすべてのデバイスが再生成されます。

外部ファイルのエクスポート

エクスポート機能を使用して、外部ファイルを自分のローカル ハード ドライブにコピーできます。

(注) 次に示す手順は、Internet Explorer を使用している場合のものです。Netscape Navigator を使用している場合は、手順が異なります。

ファイルをエクスポートするには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **External Files** を選択します。

ステップ 3　エクスポートする外部ファイルを指定します。

ステップ 4　**Export** アイコンをクリックします。ファイルを開くか、または保存するよう求めるメッセージが表示されます。

ステップ 5　BACC のユーザ インターフェイスに戻ります。

外部ファイルの削除

既存の外部ファイルを削除するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **External Files** を選択します。

ステップ 3　**External Files** フィールドに、修正する外部ファイルのファイル名を入力します。

ステップ 4　**Search** をクリックします。該当のファイルが External Files リストに表示されます。

ステップ 5　該当の 1 つまたは複数のファイルを選択します。

ステップ 6　**Delete** をクリックします。

注意　サービス　クラスに直接リンクされていないが、サービス　クラスにリンクされている他のテンプレート ファイルによって参照されるテンプレート ファイルを削除すると、構成の再生成サービスが失敗する原因になります。

(注) サービス　クラスが関連付けられているファイルは削除できません。操作を続ける前に、サービス クラスの関連付けを削除する必要があります。詳細については、P.10-2 の「サービス クラスの設定」を参照してください。

ライセンス キーの管理

ソフトウェア ライセンスは、特定の機能を有効にするか、または自分の環境の機能を高めるために使用します。それぞれのライセンスは、永久ライセンスまたは評価ライセンスとして入手できます。

- Permanent：永久ライセンスは、自分のネットワーク環境で使用するために購入するライセンスで、それに対応する特定の機能が有効になります。
- Evaluation：評価ライセンスは、インストール後の所定の期間、機能が有効になります。新しい永久ライセンス番号を入力することによって、評価ライセンスを永久ライセンスにアップグレードできます。

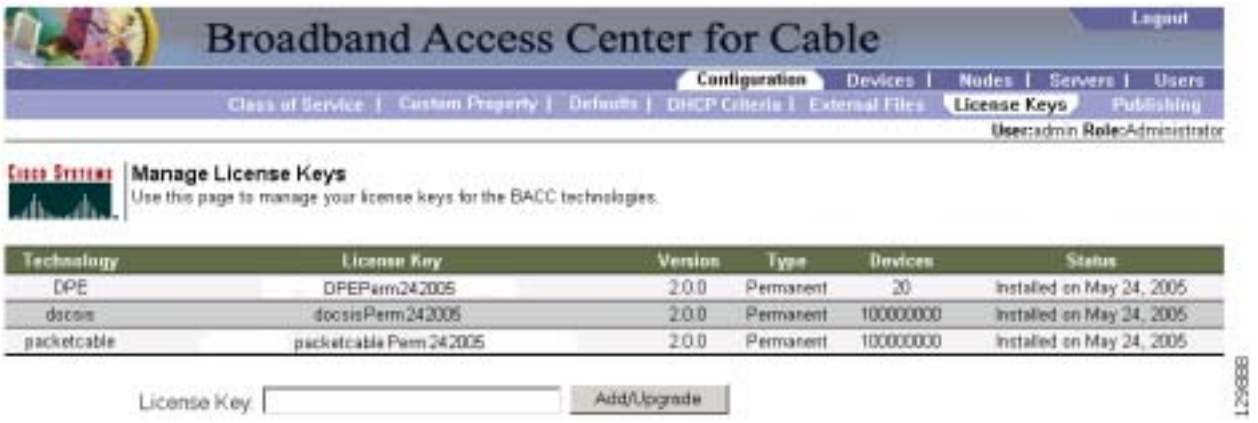
注意　評価ライセンス キーがインストールされた状態で、完全運用のネットワークへの展開を行わないようにしてください。評価ライセンスを使用して行ったプロビジョニングは、その評価ライセンスの期限が満了した時点で無効になります。

評価ライセンスから永久ライセンスにアップグレードするときに、ソフトウェアを再インストールする必要はありません。BACC 管理者のユーザ インターフェイスから直接アップグレードを実行することができます。インストール処理全体を繰り返す必要はありません。

Manage License Keys ページ（図 10-15）に、自分の実装用に入力したライセンスのリストが表示されます。この BACC リリースでは、高速データ（DOCSIS ケーブル モデム）、PacketCable MTA、ATA、DPE、CableHome WAN-Man/WAN-Data デバイス、およびコンピュータに対する評価ライセンスと永久ライセンスの両方がサポートされています。また、使用可能な各ライセンスのステータスが有効、期限満了、または未インストールのいずれかで表示されるか、あるいは期限満了日が表示されます。

（注）　評価ライセンスをアップグレードして永久ライセンスにすることができます。また、永久ライセンスをアップグレードして、ライセンスされるデバイスの数を増やすこともできます。ライセンスされたデバイスの数が上限に達すると、新しいデバイスをプロビジョニングできませんが、すでにプロビジョニングされた既存のデバイスは引き続きサービスを受けられます。

図 10-15　Manage License Keys ページ



ライセンスの追加と修正

ライセンスを追加、修正、またはアップグレードするには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Licenses** を選択します。

ステップ 3　米国シスコシステムズ社の代理店または Cisco Technical Assistance Center（TAC）のウェブサイトから新しいライセンス キーを取得します。TAC の連絡先については、このガイドの「はじめに」を参照してください。

ステップ 4　License Key フィールドに新しいライセンス キーを入力します。

ステップ 5　**Add/Upgrade** をクリックして新しいライセンス キーをインストールします。永久ライセンス キーを入力すると、対応する評価ライセンス キー（そのキーがインストールされていた場合）が無効になります。新しいテクノロジーに対するライセンス キー（永久または評価）を入力すると、テクノロジー リストにそのテクノロジーが表示されます。

Regional Distribution Unit 拡張の管理

カスタム拡張ポイントの作成は、基本的には、プログラミング作業です。この作業では、BACC 管理者のユーザ インターフェイスを併用することで、サポートされるデバイス タイプとテクノロジーの数を増やすことができます。

拡張の管理には、次の作業があります。

- 新しいクラスの作成（P.10-34）
- RDU カスタム拡張ポイントのインストール（P.10-34）
- RDU 拡張の表示（P.10-35）

（注） 拡張ポイントが連続的に実行されるようにすることによって、複数の拡張ポイントを指定できます。これを行うには、カンマ区切りリスト形式で拡張ポイントを指定します。

新しいクラスの作成

次の手順は、カスタム拡張の作成プロセス全体をより明確に説明するためのものです。さまざまなタイプの拡張を作成できます。次の手順では、新しいパブリッシング拡張ポイントを使用します。

新しいクラスを作成するには、次の手順に従います。

ステップ 1　カスタム パブリッシング拡張に関する Java ソース ファイルを作成します。

ステップ 2　拡張クラスを記述する Jar ファイルの明示的ファイルを作成します。

ステップ 3　カスタム拡張ポイントに関する Jar ファイルを作成します。jar ファイルには任意の名前を割り当てることができますが、特性を説明するような名前にする必要があります。また、他の既存の Jar ファイルと同じ名前にすることはできません。

RDU カスタム拡張ポイントのインストール

Jar ファイルを作成したら、管理者のユーザ インターフェイスを使用してファイルをインストールします。

ステップ 1　P.10-28 の「外部ファイルの追加」の手順に従って、新しい Jar ファイルを追加します。

（注） Browse 機能を使用して、P.10-34 の「新しいクラスの作成」の手順で作成した Jar ファイルを見つけ、このファイルをソース ファイルとして選択します。External File Name を空白のままにすると、ソース ファイルと外部ファイルの両方に同じファイル名が割り当てられます。外部ファイル名は、管理者のユーザ インターフェイスに表示される名前です。

ステップ 2　**Submit** をクリックします。

(注)　クラス名が jar ファイル内に存在しない場合や、BACC が他のエラーを検出した場合は、エラー メッセージが生成されます。

ステップ 3　RDU Defaults の Configure Defaults ページに戻り、新しく追加された Jar ファイルが Extension Point Jar File Search Order フィールドに表示されることを確認します。

ステップ 4　Publishing Extension Point フィールドに拡張クラス名を入力します。

ステップ 5　**Submit** をクリックして、変更を RDU データベースにコミットします。

ステップ 6　RDU 拡張を表示し、正しい拡張がロードされることを確認します。

RDU 拡張の表示

すべての RDU 拡張の属性は、View Regional Distribution Unit Details ページに直接表示できます。このページには、インストールされている拡張 Jar ファイルとロードされた拡張クラス ファイルに関する詳細が表示されます。P.9-27 の「Regional Distribution Unit の詳細の表示」を参照してください。

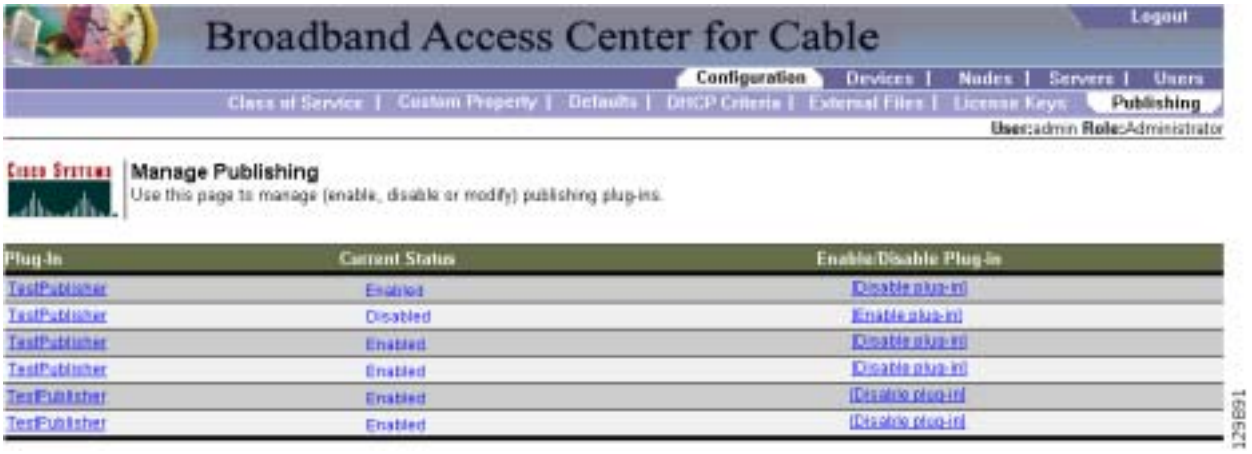
プロビジョニング データのパブリッシング

BACC には、追跡したプロビジョニング データを外部データストアにリアルタイムにパブリッシングする機能があります。そのためには、目的のデータストアにデータを書き込むパブリッシング プラグインを開発する必要があります。Manage Publishing ページ（図 10-16 を参照）には、プラグインの名前、その現在のステータス（イネーブルかどうか）、およびイネーブルまたはディセーブルにするためのスイッチが表示されます。

実装に必要なプラグインはすべてイネーブルにすることができますが、パブリッシング プラグインを使用するとシステム パフォーマンスが低下することがあるため、注意が必要です。

(注)　BACC にはパブリッシング プラグインが付属していません。ユーザは独自のプラグインを作成し、それらのプラグインをこのページから管理する必要があります。図 10-16 に示すプラグインは、説明のためにのみ作成されたものです。

図 10-16　Manage Publishing ページ



データストアの変更のパブリッシング

外部データストアへの変更をパブリッシングするには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Publishing** を選択します。Manage Publishing ページが図 10-16 のように表示されます。このページには、使用可能なデータベースのすべてのプラグインのリストが表示され、それぞれのプラグインの現在のステータスが示されます。

ステップ 3　目的のプラグインをイネーブルまたはディセーブルにするには、対応するステータス インジケータをクリックします。ステータスをクリックすることで、イネーブルとディセーブルが切り替わります（図 10-16 を参照してください）。

パブリッシング プラグイン設定の修正

これらの設定は、プラグインの作成者が各自のデータストアの RDU にプラグイン設定を保存するための便利な手段です。パブリッシング プラグイン設定を修正するには、次の手順に従います。

ステップ 1　プライマリ ナビゲーション バーの **Configuration** を選択します。

ステップ 2　セカンダリ ナビゲーション バーの **Publishing** を選択します。Manage Publishing ページが表示されます。

ステップ 3　修正するプラグインに対応するリンクをクリックします。Modify Publishing Plug-Ins ページが表示されます。

Modify Publishing Plug-Ins ページに表示されるフィールドを表 10-12 に示します。

表 10-12　Modify Publishing Plug-ins ページ

フィールドまたはボタン	説明
Plug-In	パブリッシング プラグインの名前が表示されます。
Server	データストアがあるサーバの名前を指定します。
Port	データストアがあるポートの番号を指定します。
IP Address	データストアがあるサーバの IP アドレスを指定します。通常、この IP アドレスは、サーバ名を使用しない場合に指定します。
User	データストアにアクセスするためのユーザ名を指定します。
Password	データストアにアクセスするためのユーザのパスワードを指定します。
Confirm Password	確認のため、上のフィールドに入力したパスワードをこのフィールドにも入力します。

ステップ 4　Server、Port、IP Address、User、Password、および Confirm Password の各フィールドに必要な値を入力します。これらはすべて必須フィールドなので、これらの情報を入力しなければ、次の操作へ進むことができません。

ステップ 5　**Submit** をクリックして、選択したプラグインへの変更を実行するか、または、**Reset** をクリックして、このページのすべてのフィールドをクリアします。

Network Registrar DNS サーバでの SRV レコードの設定

Network Registrar DNS サーバが KDC とともに動作するように設定する必要があります。この設定を行うには、Network Registrar のマニュアルおよび次の説明を参照してください。

(注) 目的の領域名と一致するゾーン名を作成すること、および、この特殊なゾーン内にある DNS レコード（ゾーンを維持するために DNS サーバが必要とするレコード以外）のみをその領域に対する 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 領域が voice.acme.com であり、他のすべての KDC、Network Registrar、DPE の各設定がすでに行われているとします。また、KDC の FQDN が kdc.acme.com と仮定します。

ステップ 1　**nrcmd** CLI（通常は、/opt/nwreg2/local/usrbin にあります）を起動し、自分のユーザ名とパスワードを入力します。

ステップ 2　次のコマンドを入力して、Kerberos 領域に対するゾーンを作成します。

```
nrcmd> zone voice.acme.com create primary <address of nameserver> hostmaster
```

ステップ 3　次のコマンドを入力して、SRV レコードを新しいゾーンに追加します。

```
nrcmd> zone voice.acme.com. addRR _kerberos._udp. srv 0 0 88 <address of KDC>
```

ステップ 4　次のコマンドを入力して、DNS サーバの保存とリロードを行います。

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

PacketCable MTA との通信を安全に行うための、RDU および DPE 上での SNMPV3 クローン作成の設定

BACC では、SNMPV3 が MTA デバイスにアクセスするための外部ネットワーク マネージャーをイネーブルにできます。さらに、RDU は、特定の MTA で SNMPV3 処理を実行できます。

この機能を有効にするには、DPE および RDU でセキュリティ キー関連情報を設定します。キー関連情報が設定されると、クローン化 SNMPV3 エントリを作成するために使用される BACC API コールがイネーブルになります。

(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を与えます。

キー関連情報の作成およびキーの生成

キー関連情報の作成は、2 段階の手順で行います。最初に、RDU 上でスクリプト コマンドを実行し、次に、DPE 上で CLI コマンドを実行します。

(注) この共有秘密情報は、CMTS または BACC 共有秘密情報と同じものではありません。

キー関連情報を作成するには、次の手順に従います。

ステップ 1　<BACC_HOME>/rdu/bin ディレクトリから、次のスクリプトを RDU 上で実行します。

```
generateSharedSecret.sh <password>
```

<password> は、自分が作成した 6 ～ 20 文字のパスワードです。このパスワードは、46 バイトのキーを生成するために使用されます。このキーは、<BACC_HOME>/rdu/conf ディレクトリにある keymaterial.txt というファイルに保存されます。

ステップ 2　ステップ 1 で当該キーの生成のために使用した <password> を使用して、この音声技術が有効になっているすべての DPE 上で **packetcable snmp key-material** DPE CLI コマンドを実行します。

このコマンドの実行によって、DPE 上で同じ 46 バイトのキーが生成され、RDU と 1 つまたは複数の DPE が同期し、MTA との通信が安全に行えるようになります。

FQDN の自動生成

PacketCable 音声技術を設定する場合、KDC がそれぞれの音声デバイスに対する Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を登録サーバに照会するときに、その FQDN が BACC データベースに存在している必要があります。BACC の FQDN 自動生成機能は、ある 1 つの音声技術だけが使用できるのではなく、あらゆる BACC 技術で使用できます。

自動生成される FQDN の形式

BACC で自動生成される FQDN は、次の形式に従います。

```
prefix<htype>-<hlen>-aa-bb-cc-dd-ee-ffsuffix.domain
```

入力する内容は次のとおりです。

- prefix、suffix、および domain：BACC 管理者のユーザ インターフェイスまたはプロビジョニング API を使用して設定された情報です。

(注)　ここで使用している FQDN の例では、*prefix1,6,aa-bb-cc-dd-ee-ffsuffix* が生成されたホスト名、*domain* がドメイン名です。

- 1,6,aa-bb-cc-dd-ee-ff：デバイスの MAC アドレスです。

プレフィックスおよびサフィックス プロパティの項目はオプションです。これらのプロパティを指定せず、かつ、PacketCable MTA のプロビジョニング時にホスト名を指定しない場合、および、プレフィックス プロパティとサフィックス プロパティのいずれも BACC プロパティ階層内に定義されていない場合は、デバイスの MAC アドレスの後にドメイン名を付けたものが、生成された FQDN として使用されます。

例：

MAC アドレスが **1,6,aa:bb:cc:dd:ee:ff** のデバイスには、次の FQDN が生成されます。

```
aa-bb-cc-dd-ee-ff.domain
```

また、PacketCable およびその他多くの技術に対する設定を行うときには、ドメイン名プロパティも設定する必要があります。PacketCable MTA のプロビジョニング時にドメイン名を指定しない場合、BACC プロパティ階層が検索され、見つからなければ、MTA はプロビジョニングされません。ただし、MTA のプロビジョニング時にドメイン名を指定する場合、そのドメイン名が使用されるので、BACC プロパティ階層内のどのドメイン名プロパティが指定されているかは関係ありません。

自動生成される FQDN のプロパティ

プロパティは、BACC プロパティ階層内の任意の許容ポイントで定義できます。System Defaults、Technology Defaults、DHCP Criteria、または Class of Service を使用してこのプロパティを定義できますが、デバイス レベルでも定義できます。

FQDN の検証

FQDN を生成するために使用される情報を入力するときに、考慮すべき点がいくつかあります。次の点を考慮します。

- 生成される FQDN には有効な英数字のみを使用する。
- 各レベル（生成される FQDN 内のドットとドットの間にある文字）の長さは 62 文字以下にする。
- 生成される FQDN の全体の長さが 254 文字以内にする。

（注） FQDN は、RFC1035 のホスト名およびドメイン名をサポートします。

FQDN の自動生成の例

この項では、自動生成 FQDN の作成の例を示します。

ステップ 1　該当のサービス クラスを選択し、/fqdn/domain プロパティの値として、このサービス クラスを使用するすべてのデバイスの DNS ドメインを設定します。この例では、使用されるドメインは **pctest.com** であり、PacketCable デバイスのセットをそのドメイン内にプロビジョニングすることを前提にしています。

（注） ドメインを指定しない場合、そのサービス クラス内のデバイスは、BACC から DHCP 構成を受け取りません。

ステップ 2　**Submit** をクリックします。

この例では、MAC アドレスが 1,6,aa:bb:cc:dd:ee:ff のデバイスは、1-6-aa-bb-cc-dd-ee-ff.pctest.com という自動生成 FQDN を生成します。また、デバイスのデフォルト設定で Automatic FQDN Generation フィールドをイネーブルにしておく必要があります。

CHAPTER 11

サンプル ユーザ インターフェイスの設定および使用方法

Broadband Access Center for Cable（BACC）の Sample User Interface（SUI; サンプル ユーザ インターフェイス）は、セルフプロビジョニングおよび事前プロビジョニングのためのサンプル ユーザ インターフェイスを提供します。SUI は、ラボ テストのシナリオで BACC の基本機能のデモを行うことができます。BACC のフル配備では、課金、OSS、およびワークフローの各アプリケーションのいずれかまたはすべてが SUI 機能を備えることになります。

注意 SUI は、配備には使用できません。デモのみに使用できます。

サンプル ユーザ インターフェイスについて

BACC には、ネットワーク上のデバイスの自動プロビジョニングを管理するワークフロー アプリケーションと、BACC で保守されるアカウントの管理担当者に基本的な機能を提供する管理者インターフェイスが備えられています。

SUI では、データはネットワーク上のデバイスの登録と、それらの登録によって生じる結果のアカウンティングという、2 つの異なる方法で管理されます。たとえば、クレジット カード情報を使用して新しいケーブル モデムの完全なセルフプロビジョニングを実行できるページでは、デバイスのトラッキングとともに、サービスの自動課金を処理できる必要があります。SUI では、アカウンティング情報のトラッキングは行われませんが、各デバイスをオーナー識別情報（オーナー ID）に関連付けることはできます。たとえば、オーナー ID に関連付けることで、BACC に保存されているオブジェクトを、課金アカウント システムのような外部オブジェクトと関連付けることができます。このサンプル ワークフローでは、オーナー ID はアカウント番号として使用されますが、実際には外部データに関連付けられていません。BACC 内のデバイス オブジェクトで関連付けられたオーナー ID は、デバイスのグループ化に使用する任意の外部文字列にできます。

SUI では、ショートカットの使用によって、アカウンティングなどの機能をサポートするインターフェイスが提供されるので、外部アカウンティング エンティティを実際には必要としません。アカウンティング情報は、カスタム プロパティとしてモデム オブジェクト上に保存されます。アカウントを表示すると、オーナー ID を使用してモデムを検索できるので、そのアカウント データをモデムから取得できます。

BACC では、標準モードと無差別モードという 2 つの異なるデバイス管理方法がサポートされています。

- 標準モードでは、モデムとコンピュータは個別にトラッキングされます。
- 無差別モードでは、モデムの相手側にコンピュータが何台存在しているかに関係なく、モデムだけがトラッキングされます。無差別モードがイネーブルになっている場合、プロビジョニングされたモデムの背後にあるコンピュータは、アクセスのみを受け付けます。

サンプル ユーザ インターフェイスの開始および停止

SUI には、加入者インターフェイスと管理者インターフェイスがあります。事前プロビジョニング、セルフプロビジョニング、コンピュータのトラッキング、およびアクセスを許可されたデバイスのトラッキングがサポートされるように、加入者インターフェイス フローを変更することができます。SUI を使用する前に、sampleui.properties ファイルの内容を確認する必要があります。このファイルには、インターフェイスの動作を指定する各種のコントロールが含まれています。デフォルトの sampleui.properties ファイルの内容については、P.11-12 の「サンプルの sampleui.properties ファイル」を参照してください。

テキスト エディタを使用してこのファイルを開き、必要な機能を実行するようにその内容を変更できます。変更を完了して保存し、その SUI を再起動すると、すべての変更が有効になります。

次のコマンドを実行して SUI を起動します。

```
startSampleUI.sh
```

次のコマンドを実行して SUI を停止します。

```
stopSampleUI.sh
```

(注)　これらのコマンドは両方とも <BACC_HOME>/rdu/sampleUI/bin ディレクトリにあります。

サンプル ユーザ インターフェイスの設定オプション

この項で説明するオプションを使用して、SUI を設定できます。これらのオプションを変更すると、SUI は異なるフローで動作するようになります。この項では、必要なことの大部分を説明します。これらのオプションは、BACC 内にある設定によって制御されるか、または、sampleui.properties ファイル内で定義されます。詳細については、P.11-12 の「サンプルの sampleui.properties ファイル」を参照してください。

サービス クラス

サービス クラスは、インターフェイス設定ファイル内で定義され、また、BACC 内の通常のサービス定義の中でも定義されます。SUI 内部のサービス クラスは、デバイスに対して使用される所定の DHCP 基準も参照し、また、インターフェイス内での表現形式についての記述もあります。たとえば、Blue というサービス クラスを選択した場合、SUI はそれを Gold という BACC サービス クラス、および residential-provisioned という DHCP 基準に変換することがあります。SUI は、起動されると、参照されているサービス クラスがすでに定義されていることを確認しようとします。

無差別モード

無差別モードは、コンピュータをトラッキングする方法に関する動作として定義されます。無差別モードがイネーブルな場合、プロビジョニングされたケーブル モデムの背後に接続されているコンピュータは、プロビジョニングされた設定を自動的に受信します。

無差別モードをイネーブルにすると、コンピュータに登録情報を問い合せません。しかし、このモードをディセーブルにすると（標準モードという状態になる）、SUI はユーザにコンピュータの登録を求めます。この登録には、各コンピュータに対する Internet Service Provider（ISP; インターネット サービス プロバイダー）のオプション選択も含まれます。この登録は BACC 内部で保守され、管理者のユーザ インターフェイス内の RDU Defaults ページからアクセスできます。

（注） 無差別モードを変更した後、SUI を再起動する必要があります。

インターネット サービス プロバイダーの選択

標準モードの PC 登録モード（無差別モード以外）が使用されている場合は、アカウントに登録されている各コンピュータに対して、インターネット サービス プロバイダー（ISP）を個別に選択できます。ISP の選択は、コンピュータに割り当てる DHCP 基準の選択と同じ効力があります。この設定値は、インターフェイスの設定ファイル内に設定されます。ISP が 1 つしかない場合、加入インターフェイス内を移動するときに、ISP 選択コントロールはバイパスされます。

技術者ログインの使用方法

技術者ログインを使用して、技術者がケーブル モデムを顧客宅内に搬入してプラグインするプロビジョニング フローのデモを行うことができます。Technician Login ページは、ネットワーク上でケーブル モデムのプロビジョニングを進める前に、システム内で技術者を認証するために表示されます。

認証がディセーブルになっているが、技術者プロビジョニングがイネーブルになっている場合、このデモはセルフプロビジョニングの一部として実行されます。

管理者アクセス レベル

SUI 管理インターフェイスにアクセスできる管理者は、インターフェイス設定ファイル内で設定されます。SUI 内では 4 種類の管理者を使用できます。

- full：このタイプでは、インターフェイス内でアカウントの作成と削除、およびデバイスの管理を行う完全なアクセスが可能です。
- createonly：このタイプでは、インターフェイスを使用してアカウントを新規作成するアクセスのみが可能です。
- readonly：このタイプでは、システム内に作成されたアカウントを表示するアクセスのみが可能です。
- tech：このタイプでは、技術者インターフェイスを通してログインするアクセスのみが可能です。顧客宅内からデバイスを自動プロビジョニングするために使用されます。

加入者プロビジョニングの例

この項では、SUI の使用時に提供される各種のワークフローを説明します。無差別モードをイネーブルまたはディセーブルにすると、SUI の動作が大きく影響を受けます。そのため、この項では、それぞれの場合のフローを個別に説明します。

標準の顧客宅内機器登録

この項では、システムが無差別モードではなく標準モードで動作しているときのプロビジョニング動作について説明します。次の項で、これらのプロビジョニング動作について説明します。

- 新しいケーブル モデムおよび新しいコンピュータのプロビジョニング（P.11-5）
- 新しいコンピュータおよび既存のケーブル モデムのプロビジョニング（P.11-6）
- 既存のコンピュータの ISP の変更（P.11-6）

新しいケーブル モデムおよび新しいコンピュータのプロビジョニング

新しいモデムと新しいコンピュータをネットワークに接続し、ユーザが Web ブラウザをオンラインにすると、ユーザはプロビジョニング インターフェイスにリダイレクトされます。

ステップ 1　SUI は sampleui.properties ファイルをチェックして、技術者プロビジョニングがイネーブルになっているかどうかを判断します。

- この機能がイネーブルになっていると、SUI は次の手順に進みます。
- この機能がディセーブルになっている場合、エラー ページが表示されて、モデムが登録されていないことと、顧客が MSO に連絡してケーブル モデムをシステムに登録する必要があることが通知されます。

ステップ 2　SUI は sampleui.properties ファイルをチェックして、技術者認証が必要であるかどうかを判断します。

- この機能が必要ではない場合、システムに登録するアカウント詳細情報を入力するためのモデム登録画面が表示されます。
- この機能が必要である場合、システムに登録する技術者ユーザ名とパスワード、およびアカウント詳細情報を入力するためのモデム登録画面が表示されます。

ステップ 3　コンピュータ登録ページが表示されます。このページを使用して、モデムの登録と同時にコンピュータの登録ができます。このページには、モデム登録が成功したことも表示されます。

ステップ 4　SUI は sampleui.properties ファイルをチェックして、オプションの ISP 選択がイネーブルになっているかどうかを判断します。

- イネーブルになっている場合、使用可能な ISP のドロップダウン リストが表示され、該当の ISP オプションを選択できます。
- ディセーブルになっている場合、ISP 選択は表示されません。

ステップ 5　**Register This Computer** をクリックすると、コンピュータがネットワークに正常に登録されたことを通知するメッセージが表示されます。

新しいコンピュータおよび既存のケーブル モデムのプロビジョニング

既存のモデムと新しいコンピュータをネットワークに接続し、ユーザが Web ブラウザをオンラインにすると、ユーザはプロビジョニング インターフェイスにリダイレクトされます。

ステップ 1　SUI にコンピュータ登録ページが表示されます。このページから、ネットワーク上のコンピュータを登録できます。

ステップ 2　SUI は sampleui.properties ファイルをチェックして、オプションの ISP 選択がイネーブルになっているかどうかを判断します。

- イネーブルになっている場合、使用可能な ISP のドロップダウン リストが表示され、該当の ISP オプションを選択できます。
- ディセーブルになっている場合、ISP 選択は表示されません。

ステップ 3　**Register This Computer** をクリックすると、コンピュータがネットワークに正常に登録されたことを通知するメッセージが表示されます。

既存のコンピュータの ISP の変更

既存のモデムと既存のコンピュータをネットワークに接続し、ユーザが Web ブラウザをオンラインにすると、ユーザはそのネットワークをブラウズできます。その後、ユーザはブラウザをプロビジョニング インターフェイスに接続します。

ステップ 1　SUI は、オプションの ISP 選択機能がイネーブルになっているかどうかを判断します。

- イネーブルになっている場合、使用可能な ISP のドロップダウン リストが表示され、該当の ISP オプションを選択できます。
- ディセーブルになっている場合、ISP 選択は表示されず、このコンピュータがすでにシステムに登録されていることを通知するメッセージが表示されます。

ステップ 2　**Register This Computer** をクリックすると、コンピュータがネットワークに正常に登録されたことを通知するメッセージが表示されます。

無差別モードの顧客宅内機器登録

この項では、SUI を使用した機器登録について説明します。次の項で、これらのプロビジョニング動作について説明します。

- 新しいケーブル モデムおよび新しいコンピュータのプロビジョニング（P.11-7）
- 既存のケーブル モデムおよび新しいコンピュータのプロビジョニング（P.11-7）

新しいケーブル モデムおよび新しいコンピュータのプロビジョニング

新しいモデムと新しいコンピュータをネットワークに接続し、ユーザが Web ブラウザをオンラインにすると、ユーザはプロビジョニング インターフェイスにリダイレクトされます。

ステップ 1　SUI は sampleui.properties ファイルをチェックして、技術者プロビジョニングがイネーブルになっているかどうかを判断します。

- この機能がイネーブルになっていると、SUI は次の手順に進みます。
- この機能がディセーブルになっている場合、エラー ページが表示されて、モデムが登録されていないことと、顧客が MSO に連絡してケーブル モデムをシステムに登録する必要があることが通知されます。

ステップ 2　SUI は sampleui.properties ファイルをチェックして、技術者認証が必要であるかどうかを判断します。

- この機能が必要ではない場合、システムに登録するアカウント詳細情報を入力するためのモデム登録画面が表示されます。
- この機能が必要である場合、システムに登録する技術者ユーザ名とパスワード、およびアカウント詳細情報を入力するためのモデム登録画面が表示されます。

ステップ 3　モデムおよびコンピュータがネットワークに正常に登録されたことを通知するメッセージが表示されます。

既存のケーブル モデムおよび新しいコンピュータのプロビジョニング

既存のモデムと新しいコンピュータをネットワークに接続し、ユーザが Web ブラウザをオンラインにすると、ユーザはそのネットワークをブラウズできます。ネットワークをブラウズできるようになると、ユーザはブラウザをプロビジョニング インターフェイスに接続する必要があります。接続後、ケーブル モデムとコンピュータがシステムに登録されたことを通知するメッセージが表示されます。

管理者プロビジョニングの例

この項では、SUI を使用してアカウントの保守およびアカウントの検索を行う例をいくつか示します。各 SUI ページで、所定のアクセス権が割り当てられている場合にのみ表示されるコンポーネントは、コンポーネント名の最後に付けられた *if applicable* の注記によって識別されます。

アカウントの検索

この項では、SUI を使用してアカウントの検索を実行する方法を説明します。次の検索動作について説明します。

- アカウント番号による検索（P.11-8）
- IP アドレスによる検索（P.11-8）
- MAC アドレスによる検索（P.11-8）

アカウント番号による検索

ログイン後に、アカウント番号を使用してアカウントを検索できます。検索するアカウントの番号を指定し、そのアカウントが見つかれば、アカウントの詳細情報が表示されます。アカウントが見つからない場合は、そのアカウント番号がシステム内に存在しないことを通知するエラー メッセージが表示されます。

IP アドレスによる検索

ログイン後に、IP アドレスを使用してアカウントを検索できます。BACC によって現在プロビジョニングされているコンピュータまたはモデムの IP アドレスを指定します。それが見つかった場合は、その所有者がチェックされて、どのアカウントを表示するかが決定されます。

有効なアカウントが見つかった場合、そのデバイスのアカウント詳細情報がすべて表示されます。有効なデバイスは見つかったが、有効なアカウントが見つからない場合は、そのデバイスの 現在の MAC アドレスおよび IP アドレスが検索ページの最下部に表示されます。

デバイスが見つからない場合、一致するデバイスが検索されなかったことを示すエラーが表示されます。

MAC アドレスによる検索

ログイン後に、MAC アドレスを使用してアカウントを検索できます。BACC によって現在プロビジョニングされているコンピュータまたはモデムの MAC アドレスを指定します。それが見つかった場合は、その所有者がチェックされて、どのアカウントを表示するかが決定されます。

有効なアカウントが見つかった場合、そのデバイスのアカウント詳細情報がすべて表示されます。有効なデバイスが見つかったが、有効なアカウントは見つからない場合は、そのデバイスの現在の MAC アドレスおよび IP アドレスが検索ページの最下部に表示されます。

デバイスが見つからない場合、一致するデバイスが検索されなかったことを示すエラーが表示されます。

アカウントの保守

この項では、SUI を使用してアカウントの保守を実行する方法を説明します。次の項で、これらの保守作業について説明します。

- 新しいアカウントの登録（P.11-9）
- サービス クラスの管理（P.11-9）
- ケーブル モデムの管理（P.11-10）
- コンピュータの管理（P.11-10）

新しいアカウントの登録

このワークフローを使用して、新しいアカウント、およびモデムを SUI で登録できます。システムにログインし、次の手順に従う必要があります。

ステップ 1　SUI には、（該当する場合に）検索オプションが選択肢として表示されます。このページには、**Create a new Account** ボタンも表示されます。

ステップ 2　**Create a new Account** をクリックします。

ステップ 3　SUI には、アカウント番号、ケーブル モデムの MAC アドレス、およびそのアカウントに適用できるサービス クラスを入力するページが表示されます。

ステップ 4　必要な情報を入力し、確定すると、アカウントが作成されます。

ステップ 5　アカウントが作成されると、アカウントの新規作成ページが表示されます。このページを使用して、複数のアカウントをすばやくシステムに入力できます。

サービス クラスの管理

このワークフローを使用して、アカウントに対するサービス クラスを変更したり、ケーブル モデムをディセーブルにできます。システムにログインし、次の手順に従う必要があります。

ステップ 1　SUI　には、（該当する場合に）検索オプションが選択肢として表示されます。検索基準として、アカウント番号、IP アドレス、または MAC アドレスを使用してアカウントを検索できます。

ステップ 2　SUI には、現在選択されているサービス クラス、ケーブル モデムがイネーブルかどうか、アカウント所有者情報、登録されているコンピュータのリストなど、そのアカウントに関するすべての情報を示すページが表示されます。

ステップ 3　ドロップダウン メニューから該当のサービス クラスを選択します。

ステップ 4　**Update** をクリックします。

ステップ 5　SUI には、すべてのアカウント情報を示す同じページが再表示されます。ただし、このページでは、サービス クラスが変更されています。

ケーブル モデムの管理

このワークフローを使用して、現在アカウントに関連付けられているモデムを変更できます。このワークフローに従って、ユーザ名などのアカウント詳細情報も更新できます。システムにログインし、次の手順に従う必要があります。

ステップ 1　SUI には、（該当する場合に）検索オプションが選択肢として表示されます。検索基準として、アカウント番号、IP アドレス、または MAC アドレスを使用してアカウントを検索できます。

ステップ 2　SUI には、現在選択されているサービス クラス、ケーブル モデムがイネーブルかどうか、アカウント所有者情報、登録されているコンピュータのリストなど、そのアカウントに関するすべての情報を示すページが表示されます。

ステップ 3　そのアカウントのケーブル モデムの新しい MAC アドレスを入力します。

ステップ 4　**Update** をクリックします。

ステップ 5　SUI には、すべてのアカウント情報を示す同じページが再表示されます。ただし、このページでは、MAC アドレスが変更されています。

コンピュータの管理

このワークフローを使用すると、SUI の Subscriber 部分を使用して以前登録したコンピュータを登録解除できます。このワークフローは、標準モードの PC 登録が使用されている場合にのみ適用できます。システムにログインし、次の手順に従う必要があります。

ステップ 1　SUI には、（該当する場合に）検索オプションが選択肢として表示されます。検索基準として、アカウント番号、IP アドレス、または MAC アドレスを使用してアカウントを検索できます。

ステップ 2　SUI には、現在選択されているサービス クラス、ケーブル モデムがイネーブルかどうか、アカウント所有者情報、登録されているコンピュータのリストなど、そのアカウントに関するすべての情報を示すページが表示されます。

ステップ 3　登録解除するコンピュータを決定し、該当の **Delete** ボタンをクリックします。

ステップ 4　SUI には、すべてのアカウント情報を示す同じページが再表示されますが、そのコンピュータはリストから削除されています。

アカウントの削除

このワークフローを使用すると、USI を使用して登録したアカウントを削除できます。システムにログインし、次の手順に従う必要があります。

ステップ 1　SUI には、（該当する場合に）検索オプションが選択肢として表示されます。検索基準として、アカウント番号、IP アドレス、または MAC アドレスを使用してアカウントを検索できます。

ステップ 2　SUI には、現在選択されているサービス クラス、ケーブル モデムがイネーブルかどうか、アカウント所有者情報、登録されているコンピュータのリストなど、そのアカウントに関するすべての情報を示すページが表示されます。

ステップ 3　システム プロンプトの Delete acount フィールドで **X** をクリックします。

ステップ 4　SUI には、すべてのアカウント情報を示す同じページが表示されます。Delete ボタンのすぐ横に、次の手順に進む前の確認のプロンプトが表示されます。

ステップ 5　アカウントの削除をもう一度確認するために、システム プロンプトの Delete acount フィールドで **X** をクリックします。

ステップ 6　SUI に、アカウントが削除されたことを示す最初の検索ページが表示されます。

サンプルの sampleui.properties ファイル

この項では、サンプルの sampleui.properties ファイルの内容を示します。このプロパティ ファイルは、<BACC_HOME>/rdu/conf ディレクトリにあります。

```
#  (C) Copyright 2001-2003 by Cisco Systems, Inc.
#  This program contains proprietary and confidential information.
#  All rights reserved. This software shall not be used by an party
#  except by prior written consent of Cisco Systems.
#
#  DO NOT CHANGE.  This is the version of the properties file which
#  is used during execution and for system updates.
#
version=1.2
######################################################################
#  System connection information.
######################################################################
#
#  BPR RDU connection information
#
adminuser=admin
adminpass=admin
host=localhost
port=49187
######################################################################
#  Provisioning configuration parameters
######################################################################
#
#  Administrator access credentials
#
#  3 levels of access: full, createonly, and readonly
#  full -- can create and read accounts
#  createonly -- can only create new accounts
#  readonly -- can only read accounts
#  tech -- technician access for auto-provisioning modems
#  (The default access level is 'full')
#
#  The user.number must equal the number of user accounts
#  being tracked.  If the number is 4, there must exist
#  entries for users 1-4.
#
user.number=4
user.1.name=admin
user.1.password=changeme
user.1.access=full
user.2.name=config
user.2.password=changeme
```

```
user.2.access=createonly
user.3.name=monitor
user.3.password=changeme
user.3.access=readonly
user.4.name=tech
user.4.password=changeme
user.4.access=tech
#
#  Indicates if promiscuous-mode is enabled
#
#  promiscuous-mode is a special mode of BPR in which computers are not
#  tracked by the provisioning system. (true/false)
#
#  This is controled by setting the RDU Defaults option:
#    ModemKeys.PROMISCUOUS_MODE_ENABLED
#
#  Indicates if technician auto-provisioning is enabled
#
#  This mode allows a technician to provision a new account in the field
#  without requiring the MAC address to be pre-registered.
#
techprovisioning.enabled=true
#
#  Indicates if technician username/password is required for modem
#  registration
#
#  If technician username/password is not required, then this
#  demo can be used to simulate modem self-registration
#
techprovisioning.authentication=false
#
#  Unprovisioned configuration (for disabled modems)
#
#  The client class should match the unprovisioned client class configured
#  in CNR.  The service must be unique (i.e. NOT have the same name of
#  any of the services specified below).
#
#  These values are controlled by setting the DOCSIS Defaults options, use:
#      TechnologyDefaultsKeys.DOCSIS_DEFAULT_CLASS_OF_SERVICE
#      TechnologyDefaultsKeys.DOCSIS_DEFAULT_DHCP_CRITERIA
#      TechnologyDefaultsKeys.COMPUTER_DEFAULT_DHCP_CRITERIA
#
#  Classes of Service for Modems
#
#  The DHCP criterias specified here must match valid
#  DHCP criterias specified in the RDU.  If promiscuous
#  mode is enabled, you must specify CPE DHCP criterias.
```

■ サンプルの sampleui.properties ファイル

```
#
#  The service.number must equal the number of services
#  being tracked.  If the number is 3, there must exist
#  entries for services 1-3.
#
service.number=3
service.1.name=gold
service.1.title=1.5Mb/s Lightning Fast!
service.1.dhcpcriteria=ccProvisionedDOCSISModem
service.1.cpedhcpcriteria=provcpetagProvisionedPromiscuousCpe
service.2.name=silver
service.2.title=512Kb/s Power User
service.2.dhcpcriteria=ccProvisionedDOCSISModem
service.2.cpedhcpcriteria=provcpetagProvisionedPromiscuousCpe
service.3.name=bronze
service.3.title=64kb/s Economy Service
service.3.dhcpcriteria=ccProvisionedDOCSISModem
service.3.cpedhcpcriteria=provcpetagProvisionedPromiscuousCpe
#
#  ISPs for Computers
#
#  The computerisp.number must equal the number of ISPs
#  available.  If the number is 1, there must exist
#  entries for ISPs 1-1.
#
computerisp.number=1
computerisp.1.name=msonet
computerisp.1.title=MSO.net Services
computerisp.1.dhcpcriteria=ccProvisionedComputer
#
#  Default COS, DHCPCriteria and CPE DHCPCriteria
#  that modem and computers are placed in when modem's
#  access is disabled through administrator UI
#
#  Appropriate DOCSISClassOfService and DHCPCriteria objects have
#  to be pre-created in the RDU
#
#  disabled.modem.cpedhcpcriteria=disabled-computer -- defined a
#  DHCPCriteria which computer's behind the modem get when modem's
#  access is disabled
#
disabled.modem.cos=disabled
disabled.modem.dhcpcriteria=disabled-modem
disabled.modem.cpedhcpcriteria=disabled-computer
```

CHAPTER 12

Broadband Access Center for Cable がサポートするツールと高度な概念

この章では、Broadband Access Center for Cable（BACC）の保守、および製品のインストール、配備、使用の高速化と改善に役立つツールとその使用方法について説明します。

この章では、次のトピックについて取り上げます。

- テンプレート ファイルの作成（P.12-2）
- 設定ファイル ユーティリティの使用方法（P.12-25）
- RDU ログ レベル ツール（P.12-39）
- KDC 証明書を管理するための PKCert.sh ツールの使用方法（P.12-42）
- changeNRProperties.sh ツールの使用（P.12-45）
- Keygen ツールの使用方法（P.12-47）
- snmpAgentCfgUtil.sh コマンドの使用方法（P.12-49）
- 利用可能なディスク領域を監視するための disk_monitor.sh ツールの使用方法（P.12-54）
- MAC アドレスによるデバイスのトラブルシューティング（P.12-55）

(注) この項では、ツールの使用方法について、多くの例を示します。多くの場合、ツールのファイル名には <BACC_HOME> と指定されたパスが含まれます。これは、デフォルトのディレクトリ位置を示しています。

テンプレート ファイルの作成

BACC が使用するテンプレートは、管理者がダイナミック PacketCable、DOCSIS、および CableHome ファイルを配備するときに役立ちます。テンプレートを使用して、読みやすい形式のテンプレート ファイルを作成し、迅速かつ簡単に編集することができます。テンプレートは、有効な PacketCable、DOCSIS、または CableHome ファイルを生成するときに使用する PacketCable、DOCSIS、または CableHome のオプションおよび値を表す ASCII テキスト ファイルです。BACC は、.tmpl ファイル拡張子を使用してテンプレート ファイルを識別します。サービス クラスでテンプレート ファイルを参照する前に、管理者のユーザ インターフェイスまたは API を使用して、外部ファイルとしてそのファイルを RDU に追加する必要があります。

BACC RDU コンポーネントをインストールするときに、いくつかのサンプル テンプレート ファイルが <BACC_HOME>/rdu/samples ディレクトリにコピーされます。

テンプレートを作成または編集するために必要なツールは単純なテキスト エディタだけですが、独自のテンプレート ファイルを作成する前に、次の点を十分に理解する必要があります。

- BACC プロビジョニングのフロー
- DOCSIS 1.0、1.1、および 2.0 RFI の仕様
- PacketCable 1.0 および 1.1 の仕様
- MTA デバイス プロビジョニングの仕様
- CableHome 1.0 の仕様
- ケーブル デバイス用の SNMP MIB（DOCS-CABLE-DEVICE-MIB など）

テンプレートの文法

テンプレートは、4 種類の異なる文で構成されます。

- コメント（P.12-3）
- インクルード（P.12-3）
- オプション（P.12-4）
- インスタンス修飾子（P.12-5）

コメントで、テンプレートに注釈を付けることができます。Include 文で、他のテンプレートで使用するビルディング ブロック テンプレートを作成できます。オプションで、PacketCable、DOCSIS、または CableHome の TLV（type length value）を説明的に指定できます。表 12-1 に、利用可能なテンプレートの文法オプションを示します。

表 12-1　テンプレートの文法

オプション	説明
<comment>	::= #[ascii-string]
<include>	::= include “<filename.tmpl>”
<option-description>	::= option <option-num> [instance <instance-num>] <option-value>
<option-num>	::= <unsigned-byte>[.<unsigned-byte>]*
<option-value>	::= <well-defined-value> | <custom-value>
<well-defined-value>	::= <option-value-string>[,<option-value-string>]*
<custom-value>	::= <ascii-value> | <hex-value> | <ip-value> | <snmp-value>
<ascii-value>	::= ascii <ascii-string>
<hex-value>	::= hex <hex-string>
<ip-value>	::= ip <ip-string>

表 12-1　テンプレートの文法（続き）

オプション	説明
<instance-num>	::= <unsigned integer>
<template>	::= <template-statement>*
<template-statement>	::= <comment> | <include> | <option-description>
<snmp-value>	::= snmp <snmpvar-oid>,<snmpvar-type>,<snmpvar-value>

コメント

コメントは情報のみを提供し、常にシャープ記号（#）から行末までの間に配置されます。例 12-1 に、コメントの使用方法の例を示します。

例 12-1　コメントの使用方法の例

```
#
# Template for gold service
#

option 3 1 # enabling network access
```

インクルード

インクルード ファイルを使用すると、似ているが少し異なるテンプレートの階層を構築できます。多くのサービス クラスで共通のオプションを定義する場合に、複数のテンプレートでオプションを重複させる必要がなくなり、便利です。

単一のテンプレートで複数の include 文を使用できますが、テンプレート中での include 文の場所は重要です。インクルード ファイルの内容は、テンプレート中で include 文が見つかった場所で読み込まれます。インクルードするテンプレートは、使用する前に、外部ファイルとして RDU に追加する必要があります。テンプレートは RDU データベースにパス情報なしにストアされるため、インクルードするファイルには ../.. などの位置修飾子を含めることができません。例 12-2 と 12-3 は、それぞれ、インクルード オプションの正しい使用方法と誤った使用方法を示しています。

例 12-2　include 文の正しい使用方法

```
# Valid, including common options
include "common_options.tmpl"
```

例 12-3　include 文の誤った使用方法

```
# Invalid, using location modifier
include "../common_options.tmpl"

# Invalid, using incorrect file suffix
include "common_options.common"

# Invalid, not using double quotes
include common_options.tmpl
```

オプション

PacketCable、DOCSIS、および CableHome の設定ファイルは、適切に符号化されたオプション ID と値のペアで構成されます。サポートされるオプションの形式には、定義済みとカスタムの 2 種類があります。

- オプションを正しく定義するには、オプション番号と値が必要です。値は、オプション番号の符号化タイプに基づいて符号化されます。
- カスタム オプションには、オプション番号、明示的な値の符号化タイプ、値が必要です。

option 43 などの複合オプションを使用するときは、インスタンス修飾子を使用して、TLV グループを指定できます。詳細については、P.12-5 の「インスタンス修飾子」を参照してください。

テンプレートで定義済みオプションのいずれかを指定するときは、値の値符号化を指定する必要はありません。定義済み符号化タイプの詳細については、P.12-9 の「定義済みオプションの符号化タイプ」および P.12-12 の「DOCSIS オプションのサポート」を参照してください。

カスタム オプション（option 43 など）を指定するときは、オプションの符号化タイプを指定する必要があります。利用可能な符号化タイプは、次のとおりです。

- ASCII：ASCII タイプは、指定された任意の値を NULL ターミネータなしの ASCII 文字列として符号化します。値にスペースを含める場合は、二重引用符で囲む必要があります。
- hex：値は有効な 16 進数で、各オクテットに正確に 2 文字入るようにする必要があります。値として 01 を指定した場合は、符号化で正確に 1 オクテットが使用されます。値として 0001 を指定した場合は、符号化で正確に 2 オクテットが使用されます。
- IP アドレス：IP アドレス タイプでは、指定された任意の値が 4 オクテットに符号化されます。たとえば、IP アドレス 10.10.10.1 は 0A0A0A01 に符号化されます。

1 行に複数の値があるオプションでは、カンマを使用して値を区切ります。このように値が扱われるので、場合によっては値の 1 つを二重引用符で囲む必要がありますが、他の値を囲む必要はありません。複数の値を持つオプションの例として、option 11（SNMP Varbind）があります。詳細については、P.12-6 の「SNMP Varbind」を参照してください。

複合オプションを指定するときは、トップ レベル オプション（option 4.1 を指定するときの option 4 など）を指定する必要がありません。例 12-4 と 12-5 は、それぞれ、option 文の正しい使用方法と誤った使用方法を示しています。

例 12-4　option 文の正しい使用方法

```
# Valid, specifying the number for well known option 3
option 3 1

# Valid, specifying the number for option 4 sub-option 1
option 4.1 1

# Valid, specifying a vendor option as hex
option 43.200 hex 00000C

# Valid, specifying a vendor option as ascii
option 43.201 ascii "enable log"

# Valid, specifying a vendor option as IP
option 43.202 ip 10.4.2.1
```

例 12-5　option 文の誤った使用方法

```
# Invalid, using hex with incorrect hex separator
option 43.200 hex 00.00.0C

# Invalid, not using double quotes when needed
option 43.201 ascii enable log

# Invalid, not specifying IP address correctly
option 43.202 ip 10-10-10-1

# Invalid, specifying the description for option "Network Access Control"
option "Network Access Control" 1

# Invalid, specifying top level option
option 4
```

インスタンス修飾子

インスタンス修飾子は、複合オプションを特定の個別 Tag-Length-Value（TLV）にグループ化するために使用します。例 12-6 と 12-7 は、それぞれ、個別の TLV を作成する正しい方式と誤った方式を示しています。IOS コマンドを 2 つの個別のコマンドに解釈するために、IOS DOCSIS モデムをイネーブルにする必要があります。

例 12-6　正しい IOS コマンドライン入力

```
# Valid, each IOS command gets its own TLV
option 43.8 instance 1 00-00-0C
option 43.131 instance 1 ascii "login"
option 43.8 instance 2 00-00-0C
option 43.131 instance 2 ascii "password cable"
```

例 12-7　誤った IOS コマンドライン入力

```
# Invalid, IOS commands are grouped into one TLV
option 43.8 00-00-0C
option 43.131 ascii "login"
option 43.131 ascii "password cable"

# Invalid, using instance on non-compound options
option 3 instance 1 1
```

（注） option 43.8 の符号化タイプは Organizationally Unique Identifier（OUI）です。例 12-4 とは異なり、00-00-0C 形式のみが可能です。

SNMP Varbind

DOCSIS option 11、PacketCable option 64、または CableHome option 28 を指定するときは、Object Identifier（OID; オブジェクト識別子）を使用する必要があります。OID を含む MIB は、RDU がロードする次の MIB のいずれかに存在する必要があります。オブジェクトを一意に識別するために必要な数の OID を指定する必要があります。OID の名前または番号を使用できます。RDU は、次の MIB を自動的にロードします。

- SNMPv2-SMI
- SNMPv2-TC
- CISCO-SMI
- CISCO-TC
- SNMPv2-MIB
- RFC1213-MIB
- IANAifType-MIB
- IF-MIB

DOCSIS MIB

次の DOCSIS MIB が RDU にロードされます。

- DOCS-IF-MIB
- DOCS-BPI-MIB
- CISCO-CABLE-SPECTRUM-MIB
- CISCO-DOCS-EXT-MIB
- SNMP-FRAMEWORK-MIB
- DOCS-CABLE-DEVICE-MIB
- DOCS-CABLE-DEVICE-MIB-OBSOLETE
- CISCO-CABLE-MODEM-MIB

RDU にロードされる DOCS-CABLE-DEVICE MIB には、2 つのバージョンがあります。

- DOCS-CABLE-DEVICE-MIB-OBSOLETE（実験的ブランチ）
- DOCS-CABLE-DEVICE-MIB（mib2 ブランチ）

完全修飾された MIB OID（.experimental...）は常に、MIB OID を一意に識別します。

DOCS-CABLE-DEVICE-MIB のうち、完全修飾されていない MIB OID を使用する場合、MIB OID は常に、デフォルトで DOCS-CABLE-DEVICE-MIB に設定されます（DOCS-CABLE-DEVICE-MIB-OBSOLETE には設定されません）。

例 12-8 と 12-9 は、それぞれ、完全修飾された MIB OID と完全修飾されていない MIB OID の使用方法を示しています。

例 12-8　完全修飾された MIB OID

```
# Valid, uniquely identifying an OID
option 11 .experimental.docsDev.docsDevMIBObjects.docsDevNmAccessTable.docsDevNmAccess
Entry.docsDevNmAccessStatus.1, Integer, 4
```

例 12-9　完全修飾されていない MIB OID（デフォルトで DOCS-CABLE-DEVICE-MIB に設定される）

```
# Valid, Non-Fully Qualified MIB OID.
option 11 .docsDevNmAccessStatus.1, Integer, 4
```

配備中の DOCSIS CM が DOCS-CABLE-DEVICE-MIB-OBSOLETE を要求しない場合は、常に短縮形の MIB OID を使用することができます。

PacketCable MIB

次の PacketCable（North American）MIB が RDU にロードされます。

- CLAB-DEF-MIB
- PKTC-MTA-MIB
- PKTC-SIG-MIB
- PKTC-EVENT-MIB

CableHome MIB

次の CableHome MIB が RDU にロードされます。

- CABH-CAP-MIB
- CABH-CDP-MIB
- CABH-CTP-MIB
- CABH-PS-DEV-MIB
- CABH-QOS-MIB
- CABH-SEC-MIB

次の追加 MIB が必要ですが、BACC 製品の一部ではありません。

- CABH-CTP-MIB には RMON2-MIB、TOKEN-RING-RMON-MIB が必要です。
- CABH-SEC-MIB には DOCS-BPI2-MIB が必要です。

マクロ変数

マクロ変数はテンプレートで値として指定され、これを使用してデバイス固有のオプション値を指定できます。マクロ変数がテンプレートにあると、プロパティ階層でマクロ変数名が検索され、変数の値が代入されます。変数名はカスタム プロパティで、事前に RDU に定義します。スペースは使用できません。

（注） マクロ変数のカスタム プロパティを使用する場合は、DataType.STRING を使用する必要があります。

カスタム プロパティを定義すると、次の階層で使用できるようになります。

- システム デフォルト
- テクノロジー デフォルト（PacketCable、DOCSIS、CableHome など）
- DHCP 基準プロパティ
- サービス クラス プロパティ
- デバイス プロパティ

テンプレート パーサーは、階層の下から上にプロパティを検索し（最初はデバイス、次にサービス クラス）、テンプレート オプション構文に変換します。マクロ変数をサポートする構文は次のとおりです。

- ${var-name}：この構文は、単純な代入です。変数が見つからない場合は、エラーが生成されます。
- ${var-name, ignore}：この構文では、変数値がプロパティ階層で見つからなかった場合に、このオプションが無視されます。
- ${var-name, default-value}：この構文では、変数がプロパティ階層で見つからなかった場合に、デフォルト値が使用されます。

例 12-10 と 12-11 は、それぞれ、option 11 の正しい使用方法と誤った使用方法を示しています。

例 12-10　マクロ変数の正しい使用方法

```
# Valid, using macro variable for max CPE's, straight substitution
option 18 ${MAX_CPES}

# Valid, using macro variable for max CPE's, ignore option if variable not found
# option 18 will not be defined in the DOCSIS configuration file if MAX_CPES
# is not found in the properties hierarchy
option 18 ${MAX_CPES, ignore}

# Valid, using macro variable for max CPE's with a default value
option 18 ${MAX_CPES, 1}


# Valid, using macro variable for vendor option
option 43.200 hex ${MACRO_VAR_HEX}

# Valid, using macro variable for vendor option
option 43.201 ascii ${MACRO_VAR_ASCII}

# Valid, using macro variable for vendor option
option 43.202 ip ${MACRO_VAR_IP}

# Valid, using macro variable in double quotes
option 18 "${MAX_CPES}"

# Valid, using macro variable within a value
option 43.131 ascii "hostname ${HOSTNAME}"

# Valid, using macro variables in multi-valued options
option 11 ${ACCESS_CONTROL_MIB,
.mib-2.docsDev.docsDevMIBObjects.docsDevNmAccessTable.docsDevNmAccessEntry.docsDevNmAc
cessControl.1}, Integer, ${ACCESS_CONTROL_VAL, 3}

# Valid, using macro variable in an include statement
include "${EXTRA_TEMPLATE}"

# Valid, using macro variable in an include statement with a default value
include "${EXTRA_TEMPLATE, modem_reset.tmpl}"

# Valid, using macro variable in an include statement with a default value
include "${EXTRA_TEMPLATE, modem_reset}.tmpl"

# Valid, using macro variable in an include statement with an ignore clause
include "${MY_TEMPLATE, ignore}"
```

例 12-11　マクロ変数の誤った使用方法

```
# Invalid, using macro variable as the option number
option ${MAX_CPES} 1

# Invalid, using macro variable with space in name
option 18 ${MAX CPES}
```

定義済みオプションの符号化タイプ

表 12-2 に、定義済み符号化タイプを持つオプションを示します。

表 12-2　定義済みオプション符号化タイプ

符号化	入力	例
ブール値	0 が false、1 が true です。	`0`
バイト	連続した 16 進オクテットです。各オクテットの長さは、正確に 2 文字です。	`000102030405060708`
IP アドレス	ドット（.）で区切られた 4 つの 8 ビット符号なし整数です。	`10.10.10.1`
複数の IP アドレス	カンマで区切られた IP アドレスのリストです。	`10.11.12.13,10.11.12.14`

MAC アドレス	コロン（:）またはダッシュ（-）で区切られた 6 つの 16 進オクテットです。各オクテットの長さは、正確に 2 文字です。コロンとダッシュを混在させることはできません。	`00:01:02:03:04:05`
		または
		`00-01-02-03-04-05`

MAC アドレスとマスク	コロン（:）またはダッシュ（-）で区切られた 12 オクテットです。各オクテットの長さは、正確に 2 文字です。コロンとダッシュを混在させることはできません。先頭の 6 オクテットが MAC アドレスを表し、末尾の 6 オクテットが MAC アドレスのマスクを表します。	`00:01:02:03:04:05:06:07:08:09:0A:0B`
		または
		`00-01-02-03-04-05-06-07-08-09-0A-0B`

NVTASCII	ASCII 文字列です。符号化された文字列に NULL ターミネータは含まれません。	`This is an ASCII string`
OID	SNMP OID 文字列です。	`sysinfo.0`
OIDCF	SNMP OID 文字列と、カンマで区切られた符号なし整数（0 または 1）です。	`sysinfo.0,1`
OUI	コロン（:）またはダッシュ（-）で区切られた 3 つの 16 進オクテットです。各オクテットの長さは、正確に 2 文字です。	`00-00-0C`

表 12-2　定義済みオプション符号化タイプ（続き）

符号化	入力	例
SNMPVarBind	SNMP OID 文字列、タイプ、および値です。それぞれがカンマで区切られます。有効なタイプは次のとおりです。 • BITS • Counter • Counter32 • Counter64 • Gauge • Gauge32 • INTEGER • Integer32 • IpAddress • OCTETSTRING • OBJECTIDENTIFIER • Opaque • TimeTicks • Unsigned32 **（注）** OCTETSTRING は、末尾に NULL を含まない 16 進表記に変換される文字列（オクテット文字列など）または一重引用符で囲まれた 16 進表記（'aa:bb:cc' など）です。	`.experimental.docsDev.docsDevMIBObjects.docsDevNmAccessTable.docsDevNmAccessEntry.docsDevNmAccessStatus.1, INTEGER, 4`

サブタイプ	カンマで区切られた、1 つまたは 2 つの 8 ビット符号なし整数です。	`12`
		または
		`12,14`

8 ビット符号なし整数	0 ～ 255。	`14`
16 ビット符号なし整数	0 ～ 65535。	`1244`
32 ビット符号なし整数	0 ～ 4294967295。	`3455335`
8 ビット符号なし整数および 16 ビット符号なし整数	カンマで区切られた、1 つの 8 ビット符号なし整数と 1 つの 16 ビット符号なし整数です。	`3,12324`
8 ビット符号なし整数のペア	カンマで区切られた 2 つの 8 ビット符号なし整数です。	`1,3`
3 ビット バイトの 8 ビット符号なし整数	カンマで区切られた 3 つの 8 ビット符号なし整数です。	`1,2,3`
ZTASCII	ASCII 文字列です。符号化された文字列に NULL ターミネータが含まれます。	`This is an ASCII string`

BITS 値の構文

BITS 型を使用する場合は、ラベル（「interval1 interval2 interval3」）または数値によるビット位置（「0 1 2」）を指定する必要があります。ラベル値は 1 ベースで、ビット値は 0 ベースであることに注意してください。

ビット番号を使用する構文の例を示します。

```
option 11 .pktcSigDevR0Cadence.0,STRING,"0 1 2 3 4 5 6 7 8 9 10 11 12 13 14"
```

ラベルを使用するカスタマー オクテット文字列（FFFE000000000000）の構文を示します。

```
option 11 .pktcSigDevR0Cadence.0,STRING,"interval1 interval2 interval3
interval4 interval5 interval6 interval7 interval8 interval9 interval10
interval11 interval12 interval13 interval14 interval15"
```

OCTETSTRING の構文

OCTETSTRING は、末尾に NULL を含まない 16 進表記に変換される文字列（オクテット文字列など）または一重引用符で囲まれた 16 進表記（'aa:bb:cc' など）です。

MIB を使用しない SNMP TLV の追加

RDU で MIB をロードしなくても、SNMP TLV を動的設定ファイル（DOCSIS、PacketCable、CableHome）に追加できます。次の方法を使用すると、RDU 設定の拡張から、DOCSISOptionFactory インターフェイスを使用して機能にアクセスできます。

```
public OptionValue createOptionValue(OptionSyntax syntax, String optionNumStr,
String[] optionValueList)
```

上記の方法では、public OptionSyntax.SNMP 列挙値を、OID, Type, Value という値のセットを含む optionValueList と組み合せて使用できます。

RDU 動的設定テンプレートから、次の構文を使用して、RDU MIB に対して検証されていない SNMP TLV を指定します。

```
option <option-number> snmp <OID>, <Type>, <Value>
```

例：

```
# DOCS-CABLE-DEVICE-MIB:
option 11 snmp .docsDevNmAccessIp.1,IPADDRESS,192.168.1.1

# Arris vendor specific SNMP TLV (OID numbers only, mix names/numbers)
option 11 snmp .1.3.6.1.4.1.4115.1.3.1.1.2.3.2.0, INTEGER, 6
option 11 snmp .enterprises.4115.1.3.1.1.2.3.2.0, INTEGER, 6


# NOTE: trailing colon required for single octet
option 11 snmp .1.3.6.1.2.1.69.1.2.1.6.3, STRING, 'c0:'
```

利用可能な SNMP 変数タイプの名前は、次のとおりです。

IETF 標準の SMI データ タイプ	SNMP API の名前
Integer32	INTEGER
Integer（Enumerated）	INTEGER
Unsigned32	UNSIGNED32

IETF 標準の SMI データ タイプ	SNMP API の名前
Gauge32	GAUGE
Counter32	COUNTER
Counter64	COUNTER64
Timeticks	TIMETICKS
OCTET STRING	STRING
OBJECT IDENTIFIER	OBJID
IpAddress	IPADDRESS
BITS	STRING

たとえば、SMI Integer32 タイプを指定する場合は、Integer32 および INTEGER タイプが利用可能です（大文字と小文字は区別されません）。

OCTET STRING タイプの場合は、OCTET STRING、OCTETSTRING、または STRING タイプがすべて利用可能です。

カスタム SNMP TLV テンプレート オプションを使用して、任意の SNMP TLV（RDU MIB に存在するものを含む）を指定することができます。カスタム SNMP TLV エラー チェックはあまり厳しくないため、誤ったスカラ / 列の参照は検出されません（たとえば、OID 名における .0 と .n の区別）。

DOCSIS オプションのサポート

表 12-3 では、DOCSIS のオプションと各オプションに固有のバージョンのサポートについて説明します。

表 12-3　DOCSIS のオプションとバージョンのサポート

オプション番号	説明	符号化	検証	多値	DOCSIS のバージョン		
					1.0	1.1	2.0
0	PAD	長さ、値ともになし	N/A	True	✓	✓	✓
1	ダウンストリーム周波数	32 ビット符号なし整数	62500 の倍数	False	✓	✓	✓
2	アップストリーム チャネル ID	8 ビット符号なし整数	なし	False	✓	✓	✓
3	ネットワーク アクセス制御	ブール	なし	False	✓	✓	✓
4	サービス クラス	複合	なし	False	✓	✓	✓
4.1	クラス ID	8 ビット符号なし整数	1 以上 16 以下	False	✓	✓	✓
4.2	最大ダウンストリーム レート	32 ビット符号なし整数	なし	False	✓	✓	✓
4.3	最大アップストリーム レート	32 ビット符号なし整数	なし	False	✓	✓	✓
4.4	アップストリーム チャネル プライオリティ	8 ビット符号なし整数	8 未満	False	✓	✓	✓
4.5	アップストリーム チャネル データの保証最低速度	32 ビット符号なし整数	なし	False	✓	✓	✓

表 12-3　DOCSIS のオプションとバージョンのサポート （続き）

オプション番号	説明	符号化	検証	多値	DOCSIS のバージョン		
					1.0	1.1	2.0
4.6	アップストリーム チャネル伝送の最大バースト	16 ビット符号なし整数	なし	False	✓	✓	✓
4.7	CoS プライバシー イネーブル	ブール	なし	False	✓	✓	✓
6	CM MIC コンフィギュレーション設定	16 バイト	なし	False	✓	✓	✓
7	CMTS MIC コンフィギュレーション設定	16 バイト	なし	False	✓	✓	✓
9	ソフトウェア　アップグレードのファイル名	NVTASCII	なし	True	✓	✓	✓
10	SNMP の書き込みアクセス制御	OIDCF	なし	True	✓	✓	✓
11	SNMP の MIB オブジェクト	SNMPVarBind	なし	True	✓	✓	✓
14	CPE のイーサネット MAC アドレス	MAC アドレス	なし	True	✓	✓	✓
15	テレフォニーの設定オプション	NVTASCII	なし	False	✓	✓	✓
15.2	サービス プロバイダーの名前	NVTASCII	なし	False	✓	✓	✓
15.3	電話番号（1）	NVTASCII	なし	False	✓	✓	✓
15.4	電話番号（2）	NVTASCII	なし	False	✓	✓	✓
15.5	電話番号（3）	NVTASCII	なし	False	✓	✓	✓
15.6	接続のしきい値	8 ビット符号なし整数	なし	False	✓	✓	✓
15.7	ログインのユーザ名	NVTASCII	なし	False	✓	✓	✓
15.8	ログインのパスワード	NVTASCII	なし	False	✓	✓	✓
15.9	DHCP 認証	ブール	なし	False	✓	✓	✓
15.10	DHCP サーバ	IP アドレス	なし	False	✓	✓	✓
15.11	RADIUS 領域	NVTASCII	なし	False	✓	✓	✓
15.12	PPP 認証	8 ビット符号なし整数	なし	False	✓	✓	✓
15.13	デマンド ダイヤルの非アクティビティ タイマーのしきい値	8 ビット符号なし整数	なし	False	✓	✓	✓
16	SNMP の IP アドレス（不用になったもの）	IP アドレス	なし	False	✓	✓	✓
17	ベースライン プライバシーのコンフィギュレーション設定	複合	なし	False	✓	✓	✓

表 12-3　DOCSIS のオプションとバージョンのサポート （続き）

オプション番号	説明	符号化	検証	多値	DOCSIS のバージョン		
					1.0	1.1	2.0
17.1	待機タイムアウトの許可	32 ビット符号なし整数	1 以上 30 以下	False	✓	✓	✓
17.2	待機タイムアウトの再許可	32 ビット符号なし整数	1 以上 30 以下	False	✓	✓	✓
17.3	猶予時間の許可	32 ビット符号なし整数	1 以上 1800 以下	False	✓		
17.3	猶予時間の許可	32 ビット符号なし整数	1 以上 6047999 以下	False		✓	✓
17.4	待機タイムアウトの運用	32 ビット符号なし整数	1 以上 10 以下	False	✓	✓	✓
17.5	待機タイムアウトのキーの再生成	32 ビット符号なし整数	1 以上 10 以下	False	✓	✓	✓
17.6	TEK の猶予時間	32 ビット符号なし整数	1 以上 1800 以下	False	✓		
17.6	TEK の猶予時間	32 ビット符号なし整数	1 以上 302399 以下	False		✓	✓
17.7	待機タイムアウト拒否の許可	32 ビット符号なし整数	1 以上 600 以下	False	✓	✓	✓
17.8	SA マップの待機タイムアウト	32 ビット符号なし整数	1 以上 18006 以下	False		✓	✓
17.9	最大クロック ドリフト	32 ビット符号なし整数	1 以上 10 以下	False		✓	✓
18	CPE の最大数	32 ビット符号なし整数	1 以上	False	✓	✓	✓
19	TFTP サーバのタイムスタンプ	32 ビット符号なし整数	なし	False	✓	✓	✓
20	TFTP サーバのプロビジョニング済みモデムのアドレス	IP アドレス	なし	False	✓	✓	✓
21	ソフトウェア　アップグレードの TFTP サーバ	IP アドレス N	なし	False	✓	✓	✓
22	アップストリーム パケットの分類の符号化	複合	なし	True		✓	✓
22.1	分類子の参照	8 ビット符号なし整数	1 以上 255 以下	False		✓	✓
22.2	分類子の識別子	16 ビット符号なし整数	1 以上 65535 以下	False		✓	✓
22.3	サービス フローの参照	16 ビット符号なし整数	1 以上 65535 以下	False		✓	✓
22.4	サービス フローの識別子	32 ビット符号なし整数	1 以上	False		✓	✓
22.5	規則の優先順位	8 ビット符号なし整数	なし	False		✓	✓

表 12-3　DOCSIS のオプションとバージョンのサポート （続き）

オプション番号	説明	符号化	検証	多値	DOCSIS のバージョン		
					1.0	1.1	2.0
22.6	分類子のアクティベーション状態	ブール	なし	False		✓	✓
22.7	ダイナミック サービスの変更アクション	8 ビット符号なし整数	3 未満	False		✓	✓
22.8	分類子エラーの符号化	複合	なし	False		✓	✓
22.8.1	エラー パラメータ	サブ タイプ	なし	False		✓	✓
22.8.2	エラー コード	8 ビット符号なし整数	26 未満	False		✓	✓
22.8.3	エラー メッセージ	ZTAASCII	なし	False		✓	✓
22.9	IP パケットの分類の符号化	複合	なし	False		✓	✓
22.9.1	サービス範囲とマスクの IP タイプ	3 ビット バイトの 8 ビット符号なし整数	なし	False		✓	✓
22.9.2	IP プロトコル	16 ビット符号なし整数	258 未満	False		✓	✓
22.9.3	IP 発信元アドレス	IP アドレス	なし	False		✓	✓
22.9.4	IP 発信元マスク	IP アドレス	なし	False		✓	✓
22.9.5	IP 宛先アドレス	IP アドレス	なし	False		✓	✓
22.9.6	IP 宛先マスク	IP アドレス	なし	False		✓	✓
22.9.7	TCP/UDP 発信元ポートの開始	16 ビット符号なし整数	なし	False		✓	✓
22.9.8	TCP/UDP 発信元ポートの終了	16 ビット符号なし整数	なし	False		✓	✓
22.9.9	TCP/UDP 宛先ポートの開始	16 ビット符号なし整数	なし	False		✓	✓
22.9.10	TCP/UDP 宛先ポートの終了	16 ビット符号なし整数	なし	False		✓	✓
22.10	イーサネット LLC パケットの分類の符号化	複合	なし	False		✓	✓
22.10.1	宛先 MAC アドレス	MAC アドレスとマスク	なし	False		✓	✓
22.10.2	発信元 MAC アドレス	MAC アドレス	なし	False		✓	✓
22.10.3	Ethertype/DSAP/MacType	8 ビット符号なし整数および 16 ビット符号なし整数	なし	False		✓	✓
22.11	IEEE 802.1P/Q パケットの分類の符号化	複合	なし	False		✓	✓
22.11.1	IEEE 802.1P User_Priority	8 ビット符号なし整数のペア	8 未満	False		✓	✓
22.11.2	IEEE 802.1Q VLAN_ID	16 ビット符号なし整数	なし	False		✓	✓
22.43	ベンダー固有の分類子パラメータ	複合	なし	False		✓	✓

表 12-3　DOCSIS のオプションとバージョンのサポート （続き）

オプション番号	説明	符号化	検証	多値	DOCSIS のバージョン		
					1.0	1.1	2.0
22.43.8	ベンダー ID	OUI	なし	False		✓	✓
23	ダウンストリーム パケットの分類の符号化	複合	なし	True		✓	✓
23.1	分類子の参照	8 ビット符号なし整数	1 以上 255 以下	False		✓	✓
23.2	分類子の識別子	16 ビット符号なし整数		False		✓	✓
23.3	サービス フローの参照	16 ビット符号なし整数	1 ～ 65535	False		✓	✓
23.4	サービス フローの識別子	32 ビット符号なし整数	1 ～ 65535	False		✓	✓
23.5	規則の優先順位	8 ビット符号なし整数	1 以上	False		✓	✓
23.6	分類子のアクティベーション	ブール	なし	False		✓	✓
23.7	ダイナミック サービスの変更アクション	8 ビット符号なし整数	3 未満	False		✓	✓
23.8	分類子エラーの符号化	複合	なし	False		✓	✓
23.8.1	エラー パラメータ	サブ タイプ	なし	False		✓	✓
23.8.2	エラー コード	8 ビット符号なし整数	26 未満			✓	✓
23.8.3	エラー メッセージ	ZTASCII	なし	False		✓	✓
23.9	IP 分類の符号化	複合	なし	False		✓	✓
23.9.1	サービス範囲とマスクの IP タイプ	8 ビット符号なし整数	なし	False		✓	✓
23.9.2	IP プロトコル	16 ビット符号なし整数	258 未満	False		✓	✓
23.9.3	IP 発信元アドレス	IP アドレス	なし	False		✓	✓
23.9.4	IP 発信元マスク	IP アドレス	なし	False		✓	✓
23.9.5	IP 宛先アドレス	IP アドレス	なし	False		✓	✓
23.9.6	IP 宛先マスク	IP アドレス	なし	False		✓	✓
23.9.7	TCP/UDP 発信元ポートの開始	16 ビット符号なし整数	なし	False		✓	✓
23.9.8	TCP/UDP 発信元ポートの終了	16 ビット符号なし整数	なし	False		✓	✓
23.9.9	TCP/UDP 宛先ポートの開始	16 ビット符号なし整数	なし	False		✓	✓
23.9.10	TCP/UDP 宛先ポートの終了	16 ビット符号なし整数	なし	False		✓	✓
23.10	イーサネット LLC パケットの分類の符号化	複合					✓
23.10.1	宛先 MAC アドレス	MAC アドレスとマスク	なし	False		✓	✓

表 12-3　DOCSIS のオプションとバージョンのサポート （続き）

オプション番号	説明	符号化	検証	多値	DOCSIS のバージョン		
					1.0	1.1	2.0
23.10.2	発信元 MAC アドレス	MAC アドレス	なし	False		✓	✓
23.10.3	Ethertype/DSAP/MacType	8 ビット符号なし整数および 16 ビット符号なし整数	なし	False		✓	✓
23.11	IEEE 802.1P/Q パケットの分類の符号化	複合	なし	False		✓	✓
23.11.1	IEEE 802.1P User_Priority	8 ビット符号なし整数のペア	8 未満	False		✓	✓
23.11.2	IEEE 802.1Q VLAN_ID	16 ビット符号なし整数	なし	False		✓	✓
23.43	ベンダー固有の分類子パラメータ	複合	なし	False		✓	✓
23.43.8	ベンダー ID	OUI	なし	False		✓	✓
24	アップストリーム サービス フローのスケジューリング	複合	なし	True		✓	✓
24.1	サービス フローの参照	16 ビット符号なし整数	1 以上	False		✓	✓
24.3	サービスの識別子	16 ビット符号なし整数	なし	False		✓	✓
24.4	サービス クラスの名前	ZTASCII	なし	False		✓	✓
24.5	サービス フロー エラーの符号化	複合	なし	True		✓	✓
24.5.1	エラー パラメータ	8 ビット符号なし整数	なし	False		✓	✓
24.5.2	エラー コード	8 ビット符号なし整数	26 未満	False		✓	✓
24.5.3	エラー メッセージ	ZTASCII	なし	False		✓	✓
24.6	QOS パラメータのセットタイプ	8 ビット符号なし整数	8 未満	False		✓	✓
24.7	トラフィックの優先順位	8 ビット符号なし整数	8 未満	False		✓	✓
24.8	アップストリーム平均トラフィック レートの最大値	32 ビット符号なし整数	なし	False		✓	✓
24.9	最大トラフィック バースト	32 ビット符号なし整数	なし	False		✓	✓
24.10	最小の予約済みトラフィック レート	32 ビット符号なし整数	なし	False		✓	✓
24.11	予約済みレートのパケットサイズの最小値（仮定）	16 ビット符号なし整数	なし	False		✓	✓
24.12	アクティブな QOS パラメータのタイムアウト	16 ビット符号なし整数	なし	False		✓	✓
24.13	公認の QOS パラメータのタイムアウト	16 ビット符号なし整数	なし	False		✓	✓
24.14	最大連結バースト	16 ビット符号なし整数	なし	False		✓	✓

表 12-3　DOCSIS のオプションとバージョンのサポート （続き）

オプション番号	説明	符号化	検証	多値	DOCSIS のバージョン		
					1.0	1.1	2.0
24.15	サービス フローのスケジューリングのタイプ	8 ビット符号なし整数	1 以上 6 以下	False		✓	✓
24.16	要求 / 伝送のポリシー	32 ビット符号なし整数	512 未満	False		✓	✓
24.17	公称のポーリング間隔	32 ビット符号なし整数	なし	False		✓	✓
24.18	ポールの許容ジッタ	32 ビット符号なし整数	なし	False		✓	✓
24.19	任意の許可サイズ	16 ビット符号なし整数	なし	False		✓	✓
24.20	公称の許可間隔	32 ビット符号なし整数	なし	False		✓	✓
24.21	許可の許容ジッタ	32 ビット符号なし整数	なし	False		✓	✓
24.22	間隔単位の許可	8 ビット符号なし整数	128 未満	False		✓	✓
24.23	サービス オーバーライトの IP タイプ	8 ビット符号なし整数のペア	なし	False		✓	✓
24.24	任意の許可タイミング基準	32 ビット符号なし整数	なし	False		✓	✓
24.43	ベンダー固有の PHS パラメータ	複合	なし	False		✓	✓
24.43.8	ベンダー ID	OUI	なし	False		✓	✓
25	ダウンストリーム サービス フローのスケジューリング	複合	なし	True		✓	✓
25.1	サービス フローの参照	16 ビット符号なし整数	1 以上	False		✓	✓
25.3	サービスの識別子	16 ビット符号なし整数	なし	False		✓	✓
25.4	サービス クラスの名前	ZTASCII	なし	False		✓	✓
25.5	サービス フロー エラーの符号化	複合	なし	True		✓	✓
25.5.1	エラー パラメータ	8 ビット符号なし整数	なし	False		✓	✓
25.5.2	エラー コード	8 ビット符号なし整数	26 未満	False		✓	✓
25.5.3	エラー メッセージ	ZTASCII	なし	False		✓	✓
25.6	QOS パラメータのセットタイプ	8 ビット符号なし整数	8 未満	False		✓	✓
25.7	トラフィックの優先順位	8 ビット符号なし整数	8 未満	False		✓	✓
25.8	ダウンストリーム平均トラフィック レートの最大値	32 ビット符号なし整数	なし	False		✓	✓
25.9	最大トラフィック バースト	32 ビット符号なし整数	なし	False		✓	✓
25.10	最小の予約済みトラフィック レート	32 ビット符号なし整数	なし	False		✓	✓
25.11	予約済みレートのパケットサイズの最小値（仮定）	16 ビット符号なし整数	なし	False		✓	✓

表 12-3　DOCSIS のオプションとバージョンのサポート （続き）

オプション番号	説明	符号化	検証	多値	DOCSIS のバージョン		
					1.0	1.1	2.0
25.12	アクティブな QOS パラメータのタイムアウト	16 ビット符号なし整数	なし	False		✓	✓
25.13	公認の QOS パラメータのタイムアウト	16 ビット符号なし整数	なし	False		✓	✓
25.14	最大ダウンストリーム遅延	32 ビット符号なし整数	なし	False		✓	✓
25.43	ベンダー固有の PHS パラメータ	複合	なし	False		✓	✓
25.43.8	ベンダー ID	OUI	なし	False		✓	✓
26	ペイロード ヘッダー抑制	複合	なし	True		✓	✓
26.1	分類子の参照	8 ビット符号なし整数	1 以上	False		✓	✓
26.2	分類子の識別子	16 ビット符号なし整数	1 以上	False		✓	✓
26.3	サービス フローの参照	16 ビット符号なし整数	1 以上	False		✓	✓
26.4	サービス フローの識別子	32 ビット符号なし整数	1 以上	False		✓	✓
26.5	ダイナミック サービスの変更アクション	8 ビット符号なし整数	4 未満	False		✓	✓
26.6	ペイロード ヘッダー抑制エラーの符号化	複合	なし	False		✓	✓
26.6.1	エラー パラメータ	8 ビット符号なし整数	なし	False		✓	✓
26.6.2	エラー コード	8 ビット符号なし整数	26 未満	False		✓	✓
26.6.3	エラー メッセージ	ZTASCII	なし	False		✓	✓
26.7	ペイロード ヘッダー抑制フィールド（PHSF）	バイト配列	なし	False		✓	✓
26.8	ペイロード ヘッダー抑制インデックス（PHSI）	8 ビット符号なし整数	1 以上	False		✓	✓
26.9	ペイロード ヘッダー抑制マスク（PHSM）	バイト配列	なし	False		✓	✓
26.10	ペイロード ヘッダー抑制サイズ（PHSS）	8 ビット符号なし整数	なし	False		✓	✓
26.11	ペイロード ヘッダー抑制確認（PHSV）	ブール	なし	False		✓	✓
26.43	ベンダー固有の PHS パラメータ	複合	なし	False		✓	✓
26.43.8	ベンダー ID	OUI	なし	False		✓	✓
28	分類子の最大数	16 ビット符号なし整数	なし	False		✓	✓
29	プライバシー イネーブル	ブール	なし	False		✓	✓
32	製造業者の CVC	バイト配列	なし	False		✓	✓
33	保証人の CVC	バイト配列	なし	False		✓	✓

表 12-3　DOCSIS のオプションとバージョンのサポート （続き）

オプション番号	説明	符号化	検証	多値	DOCSIS のバージョン		
					1.0	1.1	2.0
34	SnmpV3 Kickstart の値	複合	なし	False		✓	✓
34.1	SnmpV3 Kickstart のセキュリティ名	NVTASCII	なし	False		✓	✓
34.2	SnmpV3 Kickstart のマネージャ パブリック番号	バイト配列	なし	False		✓	✓
35	加入者管理のコントロール	バイト配列	なし	False		✓	✓
36	加入者管理の CPE IP テーブル	複数の IP アドレス	なし	False		✓	✓
37	加入者管理のフィルタ グループ	バイト配列	なし	False		✓	✓
38	設定ファイルの要素（docsisV3 通知受信者）	複合	なし	False		✓	✓
38.1	トラップ レシーバの IP アドレス	IP アドレス	なし	False		✓	✓
38.2	トラップ レシーバの UDP ポート番号	16 ビット符号なし整数	なし	False		✓	✓
38.3	PS による送信トラップのタイプ	8 ビット符号なし整数	なし	False		✓	✓
38.4	タイムアウト	32 ビット符号なし整数	なし	False		✓	✓
38.5	最初に情報を送信した後で情報を送信するときのリトライ回数	8 ビット符号なし整数	なし	False		✓	✓
38.6	通知フィルタリング パラメータ	OID	なし	False		✓	✓
38.7	SNMP V3 通知の送信時に使用するセキュリティ名	NVTASCII	なし	False		✓	✓
39	Enable 2.0 モード	Enable/Disable	なし	False			✓
40	Enable Test モード	SubOptions	なし	True			✓
41	ダウンストリーム チャネル リスト	SubOptions	なし	True			✓
41.1	単一ダウンストリーム チャネル	SubOptions	なし	True			✓
41.1.1	単一ダウンストリーム チャネルのタイムアウト	16 ビット符号なし整数	なし	False			✓
41.1.2	単一ダウンストリーム チャネル周波数	32 ビット符号なし整数	なし	False			✓
41.2	ダウンストリーム周波数範囲	SubOptions		True			✓
41.2.1	ダウンストリーム周波数範囲のタイムアウト	16 ビット符号なし整数	なし	False			✓

表 12-3　DOCSIS のオプションとバージョンのサポート （続き）

オプション番号	説明	符号化	検証	多値	DOCSIS のバージョン		
					1.0	1.1	2.0
41.2.2	ダウンストリーム周波数範囲の開始点	32 ビット符号なし整数	62500 の倍数	False			✓
41.2.3	ダウンストリーム周波数範囲の終了点	32 ビット符号なし整数	62500 の倍数	False			✓
41.2.4	ダウンストリーム周波数範囲のステップ サイズ	32 ビット符号なし整数	なし	False			✓
41.3	デフォルト スキャン	32 ビット符号なし整数	なし	True			✓
42	マルチキャスト MAC アドレス	MAC アドレス	なし	True			✓
43	ベンダー固有の情報	複合	なし	True	✓	✓	✓
43.1	スタティック ダウンストリーム周波数	32 ビット符号なし整数	なし	False	✓	✓	✓
43.2	同期損失のタイムアウト	32 ビット符号なし整数	なし	False	✓	✓	✓
43.3	ブート モニタ イメージのアップデート	NVTASCII	なし	False	✓	✓	✓
43.4	電力のバックオフ	16 ビット符号なし整数	なし	False	✓	✓	✓
43.8	ベンダー ID	OUI	なし	False	✓	✓	✓
43.9	工場出荷時のシステム イメージのアップデート	ブール	なし	False	✓	✓	✓
43.10	電話回線	8 ビット符号なし整数	なし	False	✓	✓	✓
43.11	IP 優先順位の設定	複合	なし	True	✓	✓	✓
43.11.1	IP 優先順位の値	8 ビット符号なし整数	なし	False	✓	✓	✓
43.11.2	速度制限	32 ビット符号なし整数	なし	False	✓	✓	✓
43.128	IOS 設定ファイルの名前	NVTASCII	なし	False	✓	✓	✓
43.129	コンソールがディセーブルになっていない場合の IOS 設定ファイル	NVTASCII	なし	False	✓	✓	✓
43.131	IOS CLI コマンド	NVTASCII	なし	True	✓	✓	✓
43.132	1.0 Plus のフローの符号化	複合	なし	False	✓	✓	✓
43.132.1	1.0 Plus のフロー ID	8 ビット符号なし整数	なし	False	✓	✓	✓
43.132.2	クラス ID	8 ビット符号なし整数	なし	False	✓	✓	✓
43.132.3	任意の許可サイズ	16 ビット符号なし整数	1 以上 65535 以下	False	✓	✓	✓
43.132.4	公称の許可間隔	32 ビット符号なし整数	1 以上 65535 以下	False	✓	✓	✓
43.132.5	間隔単位の許可	8 ビット符号なし整数	0 以上 127 以下	False	✓	✓	✓

表 12-3　DOCSIS のオプションとバージョンのサポート （続き）

オプション番号	説明	符号化	検証	多値	DOCSIS のバージョン		
					1.0	1.1	2.0
43.132.6	埋め込み音声コール	8 ビット符号なし整数	0 以上 127 以下	False	✓	✓	✓
43.132.7	保留キューの長さ	16 ビット符号なし整数	0 以上 4096 以下	False	✓	✓	✓
43.132.8	均等化キュー	複合	なし	False	✓	✓	✓
43.132.8.1	輻輳廃棄のしきい	16 ビット符号なし整数	1 以上 4096 以下	False	✓	✓	✓
43.132.8.2	ダイナミックな会話のキュー数	16 ビット符号なし整数	16 以上 4096 以下	False	✓	✓	✓
43.132.8.3	予約可能な会話のキュー数	16 ビット符号なし整数	0 以上 1000 以下	False	✓	✓	✓
43.132.9	カスタム キュー リストの長さ	8 ビット符号なし整数	1 以上 16 以下	False	✓	✓	✓
43.132.10	ランダム検出	ブール	なし	False	✓	✓	✓
43.132.11	プライオリティ グループ	8 ビット符号なし整数	1 以上 16 以下	False	✓	✓	✓
43.132.12	サービス ポリシー ファイル	NVTASCII	なし	False	✓	✓	✓
43.132.13	非アクティビティ タイマー	16 ビット符号なし整数	1 以上 10080 以下	False	✓	✓	✓
43.132.14	COS タグ	NVTASCII	なし	False	✓	✓	✓
43.133	ダウンストリーム サブチャネル ID	8 ビット符号なし整数	0 以上 15 以下	False	✓	✓	✓
43.134	SU タグ	NVTASCII	なし	False	✓	✓	✓
255	データ終了（EOD）マーカー	長さ、値ともになし	N/A	False	✓	✓	✓

PacketCable オプションのサポート

表 12-4 は、BACC でサポートされている PacketCable 1.0 MTA のオプションを示します。

表 12-4　PacketCable MTA 1.0 のオプション

番号	説明	符号化	検証	多値	PacketCable のバージョン	
					1.0	1.1
11	SNMP の MIB オブジェクト	1 バイト長の SNMPVarBind	なし	True	✓	✓
38	SNMPv3 通知受信者	SubOptions	なし	True	✓	✓
38.1	SNMPv3 通知受信者の IP アドレス	IP アドレス	なし	False	✓	✓
38.2	SNMPv3 通知受信者の UDP ポート番号	16 ビット符号なし整数	なし	False	✓	✓
38.3	SNMPv3 通知受信者のトラップ タイプ	SNMPTrapType	1 ～ 5	False	✓	✓
38.4	SNMPv3 通知受信者のタイムアウト	16 ビット符号なし整数	なし	False	✓	✓
38.5	SNMPv3 通知受信者のリトライ	16 ビット符号なし整数	0 ～ 255	False	✓	✓
38.6	通知受信者のフィルタリング パラメータ	OID	なし	False	✓	✓
38.7	通知受信者のセキュリティ名	NVTASCII	なし	False	✓	✓
43	ベンダー固有の情報	SubOptions	なし	True	✓	✓
43.8	ベンダー ID	OUI	なし	False	✓	✓
64	SNMP の MIB オブジェクト	2 バイト長の SNMPVarBind	なし	True	✓	✓
254	テレフォニー設定ファイルの開始 / 終了	8 ビット符号なし整数	1 または 255	False	✓	✓

ノンセキュア CableHome オプションのサポート

表 12-5 は、BACC でサポートされているノンセキュア CableHome のオプションを示しています。

表 12-5　ノンセキュア CableHome のオプションとバージョン サポート

オプション番号	説明	符号化	検証	多値	CableHome のバージョン
					1.0
0	PAD	長さ、値ともになし	なし	True	✓
9	ソフトウェア アップグレードのファイル名	NVTASCII	なし	False	✓
10	SNMP の書き込みアクセス制御	OIDCF	なし	True	✓

表 12-5　ノンセキュア CableHome のオプションとバージョン サポート （続き）

オプション番号	説明	符号化	検証	多値	CableHome のバージョン 1.0
12	モデムの IP アドレス	IP アドレス	なし	False	✓
14	CPE のイーサネット MAC アドレス	MAC アドレス	なし	True	✓
21	ソフトウェア アップグレードの TFTP サーバ	IP アドレス	なし	False	✓
28	SNMP の MIB オブジェクト	SNMPVarBind	なし	True	✓
32	製造業者の CVC	バイト配列	なし	False	✓
33	保証人の CVC	バイト配列	なし	True	✓
34	SnmpV3 Kickstart の値	SubOptions	なし	False	✓
34.1	SnmpV3 Kickstart のセキュリティ名	NVTASCII	なし	False	✓
38	SNMPv3 通知受信者	SubOptions	なし	True	✓
38.1	SNMPv3 通知受信者の IP アドレス	IP アドレス	なし	False	✓
38.2	SNMPv3 通知受信者の UDP ポート番号	16 ビット符号なし整数	なし	False	✓
38.3	SNMPv3　通知受信者のトラップ タイプ	SNMPTrapType	1 ～ 5	False	✓
38.4	SNMPv3 通知受信者のタイムアウト	16 ビット符号なし整数	なし	False	✓
38.5	SNMPv3 通知受信者のリトライ	16 ビット符号なし整数	なし	False	✓
38.6	通知受信者のフィルタリング パラメータ	OID	なし	False	✓
38.7	通知受信者のセキュリティ名	NVTASCII	なし	False	✓
43	ベンダー固有の情報	SubOptions	なし	True	✓
43.1	ベンダー ID	OUI	なし	False	✓
53	PS MIC。PS 設定ファイルの 20 オクテット SHA-1 ハッシュ。	バイト配列	なし	False	✓
255	データ終了（EOD）マーカー	長さ、値ともになし	なし	False	✓

設定ファイル ユーティリティの使用方法

設定ファイル ユーティリティを使用して、PacketCable 1.0、DOCSIS 1.0/1.1/2.0、および CableHome のテンプレート ファイルと設定ファイルをテスト、検証、および表示できます。これらの作業は、独自の設定ファイルを正常に展開するために重要です。テンプレートの詳細については、P.12-2 の「テンプレート ファイルの作成」を参照してください。

設定ファイル ユーティリティは、RDU をインストールし、ユーティリティを <BACC_HOME>/rdu/bin ディレクトリにインストールしたときにのみ利用可能です。

符号化するテンプレート ファイルとデコードするバイナリ ファイルの両方が、設定ファイル ユーティリティを起動するディレクトリに存在する必要があります。

この項のすべての例では、RDU が運用中で、次の条件が適用されていることを前提にしています。

- BACC アプリケーションは、ホームディレクトリ（/opt/CSCObpr）にインストールされています。
- RDU ログイン名は admin です。
- RDU ログイン パスワードは changeme です。

(注)　この項の例では、一部が出力例にとって重要でない場合に、その部分を省略して切り詰めていることがあります。その場合は、例中のサマリーの直前に連続したピリオド（...）で示してあります。

この項では、次のトピックについて取り上げます。

- ローカル テンプレート ファイルの解析（P.12-28）
- 外部テンプレート ファイルの解析（P.12-29）
- コマンドラインでのマクロ変数の指定（P.12-32）
- マクロ変数のデバイスの指定（P.12-33）
- バイナリ ファイルへの出力の指定（P.12-35）
- ローカル バイナリ ファイルの表示（P.12-36）
- 外部バイナリ ファイルの表示（P.12-37）

設定ファイル ユーティリティの実行

次の手順と例で、「設定ファイル ユーティリティを実行する」というフレーズは、指定されたディレクトリから **runCfgUtil.sh** コマンドを入力することを意味します。設定ファイル ユーティリティを実行するには、ホーム ディレクトリから次のコマンドを実行します。

```
runCfgUtil.sh (options)
```

利用可能な *(options)* は、次のとおりです。

- -c <secret>：DOCSIS テンプレート ファイルを解析するときの CMTS 共有秘密情報を指定します。デフォルトの共有秘密情報を指定するには、**-c cisco** と入力します。
- -cablehome：入力ファイルが CableHome ポータル サービス設定ファイルであることを示します。-docsis または -pkt オプションと同時に使用することはできません。
- -d：バイナリ入力ファイルをデコードします。-e オプションと同時に使用することはできません。
- -docsis：入力ファイルが DOCSIS 設定ファイルであると指定します。このデフォルトを -pkt オプションと同時に使用することはできません。

- -e：テンプレート入力ファイルを符号化します。このデフォルトを -d オプションと同時に使用することはできません。
- -g：docsis、packetcable、または cablehome バイナリ ファイルからテンプレート ファイルを生成します。
- -h<host:port>：ホストとポート番号を指定します。デフォルトのポート番号は 49187 です。
- -i <device id>：マクロ変数を解析するときに使用するデバイスを指定します。たとえば、デバイス ID が 1,6,00:00:00:00:00:00:01 の場合は、**-i 1,6,00:00:00:00:00:01** と入力します。このオプションを使用するときは、-u および -p オプションを使用して、それぞれユーザ名とパスワードを指定する必要もあります。-m オプションと同時に使用することはできません。
- -l <filename>：入力ファイルがローカル ファイル システムにあることを示します。たとえば、入力ファイルの名前が any_file の場合は、-l **any_file** と入力します。-r オプションと同時に使用することはできません。
- -loc：PacketCable のロケールを na（北アメリカ）または euro（ヨーロッパ）に指定します。デフォルトは na です。MTA が euro-MTA の場合は、ロケールを euro に設定する必要があります。
- -m <*macros*>：マクロ変数のキーと値のペアを指定します。形式は key=value です。複数のマクロ変数が必要な場合は、key_1=value_1,,key_2=value_2 のように、キーと値のペアを 2 つのカンマで区切ります。-i オプションと同時に使用することはできません。
- -p <password>：RDU に接続するときに使用するパスワードを指定します。たとえば、パスワードが 123456 の場合は、**-p 123456** と入力します。
- -o <filename>：解析したテンプレート ファイルをバイナリ ファイルとして保存します。たとえば、出力をファイル op_file に保存するには、**-o op_file** と入力します。
- -pkt：入力ファイルが PacketCable MTA 設定ファイルであることを示します。-docsis オプションと同時に使用することはできません。
- -r <filename>：入力ファイルが RDU に追加した外部ファイルであることを示します。たとえば、ファイル名が file25 の場合は、**-r file25** と入力します。このオプションを使用するときは、-u および -p オプションを使用して、それぞれユーザ名とパスワードを指定する必要もあります。-l オプションと同時に使用することはできません。
- -s：解析されたテンプレートまたはバイナリ ファイルの内容を人間が読める形式で表示します。
- -t：PacketCable の符号化タイプを secure または basic に指定します（デフォルトは secure）。
- -u <username>：RDU に接続するときに使用するユーザ名を指定します。たとえば、ユーザ名が admin の場合は、**-u admin** と入力します。
- -v <version>：使用している DOCSIS のバージョンを指定します。たとえば、DOCSIS 1.1 を使用している場合は、**-v 1.1** と入力します。バージョン番号を指定しない場合、コマンドはデフォルトで DOCSIS 2.0 を使用します。

（注） 設定ファイル ユーティリティでは、テンプレート ファイルに option 19（TFTP サーバ タイムスタンプ）と option 20（TFTP サーバのプロビジョニングされたモデム アドレス）は含まれません。ただし、BACC TFTP 混在では含まれます。また、option 6（CM MIC）および 7（CMTS MIC）は両方とも、符号化されたテンプレート ファイルに自動的に挿入されます。したがって、これらの Message Integrity Check（MIC; メッセージ完全性チェック）を指定する必要はありません。

設定ファイル ユーティリティの使用方法

設定ファイル ユーティリティを使用して、BACC テンプレートをテストするには、次の手順に従います。

ステップ 1　P.12-2 の「テンプレート ファイルの作成」の説明に従い、テンプレートを作成します。

ステップ 2　ローカル ファイル システムで設定ファイル ユーティリティを実行します。テンプレートにマクロ変数が含まれている場合は、次の操作を順に実行します。

a.　コマンドライン代入でテストします。

b.　RDU に追加したデバイスでテストします。

ステップ 3　テンプレート（および、そのテンプレートにインクルードするテンプレート）を RDU に追加します。

ステップ 4　外部ファイルとして設定ファイル ユーティリティを実行します。テンプレートにマクロ変数が含まれている場合は、次の操作を順に実行します。

a.　コマンドライン代入でテストします。

b.　RDU に追加したデバイスでテストします。

ステップ 5　テンプレートを使用するサービス クラスを構成します。

バイナリ ファイルのテンプレート ファイルへの変換

使用上のガイドライン

runCfgUtil.sh コマンドを使用して、バイナリ設定メモリ ファイルをテンプレート ファイルに変換します。BACC の動的構成生成は、作成されるテンプレートに基づきます。既存のテスト済みバイナリ ファイルをテンプレート ファイルに自動的に変換すると、プロセスの速度が向上し、エラーの発生する可能性が低下します。

シンタックスの説明

runCfgUtil.sh コマンドを使用して既存のバイナリ ファイルをテンプレート ファイルに変換するときは、次の構文を使用する必要があります。

```
runCfgUtil.sh -g -l <binary_file> -o <template_file>
```

入力する内容は次のとおりです。

- -g：入力バイナリ ファイルからテンプレート ファイルを生成することを指定します。
- -l <binary_file>：ローカル入力ファイル（パス名を含む）を指定します。いかなる場合も、入力バイナリ ファイルの名前には *.cm ファイル拡張子が割り当てられます（たとえば、bronze.cm）。
- -o <template_file>：出力テンプレート ファイル（パス名を含む）を指定します。いかなる場合も、出力テンプレート ファイルの名前には *.tmpl ファイル拡張子が割り当てられます（たとえば、test.tmpl）。

ローカル テンプレート ファイルの解析

使用上のガイドライン　**runCfgUtil.sh** コマンドを使用して、外部テンプレート ファイルを解析します。

シンタックスの説明　**runCfgUtil.sh** コマンドを使用してローカル テンプレート ファイルを解析するときは、次の構文を使用する必要があります。

```
runCfgUtil.sh -pkt -l <file>
```

入力する内容は次のとおりです。

- -pkt：入力ファイルが packetcable MTA ファイルであることを示します。
- -l：入力ファイルがローカル ファイル システムにあることを指定します。
- <file>：解析する入力テンプレート ファイルを示します。

ファイルの解析

ローカル ファイル システムにあるテンプレート ファイルを解析するには、次の手順に従います。

ステップ 1　/opt/CSCObpr/rdu/samples/packet_cable にディレクトリを変更します。

ステップ 2　使用するテンプレート ファイルを選択します。

（注）　この例では、unprov_packet_cable.tmpl という既存のテンプレート ファイルを使用します。PacketCable MTA テンプレートなので、-pkt オプションを使用します。

ステップ 3　次のコマンドを使用して、設定ファイル ユーティリティを実行します。

```
runCfgUtil.sh -pkt -l unprov_packet_cable.tmpl
```

入力する内容は次のとおりです。

- -pkt：入力ファイルが packetcable MTA ファイルであることを示します。
- -l：入力ファイルがローカル ファイル システムにあることを指定します。
- unprov_packet_cable.tmpl：解析する入力テンプレート ファイルを示します。

ユーティリティを実行すると、次のような結果が表示されます。

```
Off    File Bytes      Option    Description           Value
0      FE0101          254       Telephony Config File 1
                                 Start/End
3      0B153013060E    11        SNMP MIB Object       .iso.org.dod.internet.private.ent
       2B06010401A30B                                  erprises.cableLabs.clabProject.cl
       0202010101                                      abProjPacketCable.pktcMtaMib.pktc
       0700020102                                      MtaMibObjects .pktcMtaDevBase.
                                                       pktcMtaDevEnable d.0,INTEGER,
                                                       false(2)

.....................................

0 error(s), 0 warning(s) detected. Parsing of unprov_packet_cable.tmpl was successful.
The file unprov_packet_cable.tmpl was parsed successfully in 434 ms.
The parser initialization time was 92 ms.
The parser parse time was 342 ms.
```

外部テンプレート ファイルの解析

使用上のガイドライン　**runCfgUtil.sh** コマンドを使用して、外部テンプレート ファイルを解析します。

シンタックスの説明　**runCfgUtil.sh** コマンドを使用して外部テンプレート ファイルを解析するときは、次の構文を使用する必要があります。

```
runCfgUtil.sh -r <file> -u <username> -p <password>
```

入力する内容は次のとおりです。

- -r <file>：入力ファイルが RDU に追加した外部ファイルであることを示します。
- -u <username>：RDU に接続するときに使用するユーザ名を指定します。
- -p <password>：RDU に接続するときに使用するパスワードを指定します。

ファイルの解析

RDU に追加したテンプレート ファイルを解析するには、次の手順に従います。

ステップ 1　/opt/CSCObpr/rdu/samples/docsis にディレクトリを変更します。

ステップ 2　使用するテンプレート ファイルを選択します。

（注）　この例では、unprov.tmpl という既存のテンプレート ファイルを使用します。DOCSIS テンプレートが使用されているので、-docsis オプションを使用します。

ステップ 3　次のコマンドを使用して、設定ファイル ユーティリティを実行します。

```
runCfgUtil.sh -r <unprov.tmpl> -u <admin> -p <changeme> -docsis
```

入力する内容は次のとおりです。

- unprov.tmpl：入力ファイルを示します。
- admin：ユーザ名を示します。
- changeme：パスワードを示します。
- -docsis：ファイルが DOCSIS テンプレートであることを示します。

ユーティリティを実行すると、次のような結果が表示されます。

(注)　ここで示す結果は説明用であり、短く切り詰めてあります。

```
Off     File Bytes       Option      Description                    Value
0       030101           3           Network Access Control         On
3       041F             4           Class of Service
5       010101           4.1         Class ID                       1
8       02040000FA00     4.2         Maximum Downstream Rate        128000 bits/sec
14      03040000FA00     4.3         Maximum Upstream Rate          64000 bits/sec
20      040101           4.4         Upstream Channel Priority      1
. . . . . .
. . . . . .
252     06108506547F     6           CM MIC Configuration Setting   8506547FC9152B44
        C9152B44DB95                                                DB955420843EF6FE
        5420843EF6FE
270     0710644B675B     7           CMTS MIC Configuration Setting 644B675B70B7BD3E
        70B7BD3E09AC                                                09AC210F794A1E8F
        210F794A1E8F
288     FF               255         End-of-Data Marker
289     00               0           PAD
290     00               0           PAD
291     00               0           PAD
0 error(s), 0 warning(s) detected. Parsing of unprov.tmpl was successful.
The file unprov.tmpl was parsed successfully in 375 ms.
The parser initialization time was 63 ms.
The parser parse time was 312 ms.
```

テンプレート ファイルの解析とユーザ指定の共有秘密情報の追加

使用上のガイドライン　**runCfgUtil.sh** コマンドを使用して、テンプレート ファイルを解析し、指定した共有秘密情報を追加します。

シンタックスの説明　**runCfgUtil.sh** コマンドを使用してテンプレート ファイルを解析し、共有秘密を追加するときは、次の構文を使用する必要があります。

```
runCfgUtil.sh -e -docsis -l <file> -c <secret>
```

入力する内容は次のとおりです。

- -e：符号化オプションを示します。
- -docsis：入力ファイルが DOCSIS テンプレート ファイルであることを示します。
- -l：入力ファイルがローカル ファイル システムにあることを指定します。
- <file>：解析する入力テンプレート ファイルを示します。
- -c <secret>：DOCSIS テンプレート ファイルを解析するときの CMTS 共有秘密情報を指定します。デフォルトの共有秘密情報は、**-c cisco** です。

ファイルの解析

ローカルに保存されたテンプレート ファイルを解析し、ユーザ指定の共有秘密情報を設定するには、次の手順に従います。

ステップ 1　/opt/CSCObpr/rdu/samples/docsis にディレクトリを変更します。

ステップ 2　解析するテンプレート ファイルを選択します。

(注)　この例では、unprov.tmpl という既存のテンプレート ファイルを使用します。DOCSIS テンプレートなので、-docsis オプションを使用します。

ステップ 3　次のコマンドを使用して、設定ファイル ユーティリティを実行します。

```
runCfgUtil.sh -e -docsis -l unprov.tmpl -c shared
```

入力する内容は次のとおりです。

- -e：符号化オプションを示します。
- -docsis：入力ファイルが DOCSIS テンプレート ファイルであることを示します。
- -l：入力ファイルがローカル ファイル システムにあることを指定します。この例で使用するローカルに保存されたファイルは、unprov.tmp です。
- -c：共有秘密情報を設定することを示します。shared は、その新しい共有秘密情報を示します。

ユーティリティを実行すると、次のような結果が表示されます。

```
Off     File Bytes      Option    Description                    Value
0       030100          3         Network Access Control         Off
3       041F            4         Class of Service
5       010101          4.1       Class ID                       1
8       02040001F400    4.2       Maximum Downstream Rate        128000 bits/sec
14      03040000FA00    4.3       Maximum Upstream Rate          64000 bits/sec
20      040101          4.4       Upstream Channel Priority      1
. . . . . .
. . . . . .
252     06108506547F    6         CM MIC Configuration Setting    8506547FC9152B44
        C9152B44DB95                                             DB955420843EF6FE
        5420843EF6FE
270     0710644B675B    7         CMTS MIC Configuration Setting 644B675B70B7BD3E
        70B7BD3E09AC                                             09AC210F794A1E8F
        210F794A1E8F
288     FF              255       End-of-Data Marker
289     00              0         PAD
290     00              0         PAD
291     00              0         PAD
0 error(s), 0 warning(s) detected. Parsing of unprov.tmpl was successful.
The file unprov.tmpl was parsed successfully in 375 ms.
The parser initialization time was 63 ms.
The parser parse time was 312 ms.
```

コマンドラインでのマクロ変数の指定

使用上のガイドライン　**runCfgUtil.sh** コマンドを使用して、マクロ変数を指定します。

シンタックスの説明　**runCfgUtil.sh** コマンドを使用してコマンドラインでマクロ変数を指定するときは、次の構文を使用する必要があります。

```
runCfgUtil.sh -e -l <file> -m <“macros”>
```

入力する内容は次のとおりです。

- -e：符号化オプションを示します。
- -l：入力ファイルがローカル ファイル システムにあることを指定します。
- <file>：解析する入力テンプレート ファイルを示します。
- -m：テンプレートを解析するときに代入するマクロ変数を指定します。
- <“macros”>：目的のマクロを示します。複数のマクロ変数が必要な場合は、各マクロの間に 2 つのカンマを挿入します。

コマンドラインでマクロ変数の値を指定するには、次の手順に従います。

ステップ 1　/opt/CSCObpr/rdu/samples/templates にディレクトリを変更します。

ステップ 2　使用するテンプレート ファイルを選択します。

ステップ 3　テンプレートのマクロ変数を調べます。この例のマクロ変数は、macro1（option 3）と macro11（option 4.2）です。

ステップ 4　マクロ変数の値を調べます。macro1 の値を 1 に設定し、macro11 の値を 64000 に設定します。

ステップ 5　次のコマンドを使用して、設定ファイル ユーティリティを実行します。

```
runCfgUtil.sh -e -l macro.tmpl -m "macro1=1,,macro11=64000"
```

入力する内容は次のとおりです。

- -e：符号化オプションを示します。
- -unprov.tmpl：入力ファイルを示します。
- macro1=1,,macro11=64000：マクロ変数のキーと値のペアを示します。複数のマクロ変数が必要なので、キーと値のペアの間に 2 つのカンマを挿入して区切ります。

ユーティリティを実行すると、次のような結果が表示されます。

```
Off     File Bytes       Option      Description                    Value
 0       030101           3          Network Access Control          On
 3       041F             4          Class of Service
 5       010101           4.1        Class ID                        1
 8       02040000FA00    4.2        Maximum Downstream Rate         64000 bits/sec
 14      03040000FA00    4.3        Maximum Upstream Rate           64000 bits/sec
 20      040101           4.4       Upstream Channel Priority       1
.....................................

0 error(s), 0 warning(s) detected. Parsing of macro.tmpl was successful.
The file macro.tmpl was parsed successfully in 854 ms.
The parser initialization time was 76 ms.
The parser parse time was 778 ms.
```

マクロ変数のデバイスの指定

使用上のガイドライン　**runCfgUtil.sh** コマンドを使用して、マクロ変数用のデバイスを指定します。

シンタックスの説明　**runCfgUtil.sh** コマンドを使用してマクロ変数用のデバイスを指定するときは、次の構文を使用する必要があります。

```
runCfgUtil.sh -e -l <file> -i <MAC> -u <username> -p <password>
```

入力する内容は次のとおりです。

- -e：符号化オプションを示します。
- -l：入力ファイルがローカル ファイル システムにあることを指定します。
- <file>：解析する入力テンプレート ファイルを示します。
- -i：マクロ変数を解析するときに使用するデバイスを指定します。
- <MAC>：デバイスの MAC アドレスを示します。
- -u <username>：RDU に接続するときに使用するユーザ名を指定します。

- -p <password>：RDU に接続するときに使用するパスワードを指定します。

マクロ変数代入に使用するデバイスを指定するには、次の手順に従います。

ステップ 1　/opt/CSCObpr/rdu/samples/templates にディレクトリを変更します。

ステップ 2　使用するテンプレート　　ファイルを選択します。この例では、既存のテンプレート　　ファイル macro.tmpl を使用します。

ステップ 3　テンプレートのマクロ変数を調べます。この例のマクロ変数は、macro1（option 3）と macro11（option 4.2）です。

ステップ 4　使用するデバイスを調べます。この例では、デバイスが RDU に存在し、マクロ変数がプロパティとして設定されているものとします。macro1 の値を 1 に設定し、macro11 の値を 64000 に設定します。

ステップ 5　次のコマンドを使用して、設定ファイル ユーティリティを実行します。

```
runCfgUtil.sh -l macro.tmpl -i "1,6,00:01:02:03:04:05" -u admin -p changeme
```

入力する内容は次のとおりです。

- macro.tmpl：入力ファイルを示します。
- 1,6,00:01:02:03:04:05：デバイスの MAC アドレスを示します。この MAC アドレスは、例として示す目的でのみ使用しています。
- admin：この例で使用するデフォルトのユーザ名を示します。
- changeme：この例で使用するデフォルトのパスワードを示します。

ユーティリティを実行すると、次のような結果が表示されます。

```
Off     File Bytes       Option      Description                    Value
0        030101           3         Network Access Control          On
3        041F             4         Class of Service
5        010101           4.1       Class ID                        1
8        02040000FA00     4.2       Maximum Downstream Rate         64000 bits/sec
14       03040000FA00     4.3       Maximum Upstream Rate           64000 bits/sec
20       040101           4.4       Upstream Channel Priority       1
.....................................

0 error(s), 0 warning(s) detected. Parsing of macro.tmpl was successful.
The file macro.tmpl was parsed successfully in 823 ms.
The parser initialization time was 102 ms.
The parser parse time was 803 ms.
```

バイナリ ファイルへの出力の指定

使用上のガイドライン　**runCfgUtil.sh** コマンドを使用して、マクロ変数用のデバイスを指定します。

シンタックスの説明　**runCfgUtil.sh** コマンドを使用してバイナリ ファイルへの出力を指定するときは、次の構文を使用する必要があります。

```
runCfgUtil.sh -l <input_file> -o <output_file>
```

入力する内容は次のとおりです。

- -l：入力ファイルがローカル ファイル システムにあることを指定します。
- <input_file>：解析する入力テンプレート ファイルを示します。
- -o：解析するテンプレート ファイルのバイナリ コンテンツをストアするファイル名を指定します。
- <output_file>：使用する出力ファイル名を指定します。

テンプレートを解析してバイナリ ファイルに出力するように指定するには、次の手順に従います。

ステップ 1　/opt/CSCObpr/rdu/samples/templates にディレクトリを変更します。

ステップ 2　使用するテンプレート ファイルを選択します。

ステップ 3　出力ファイル名を調べます。この例では、unprov.cm を使用します。

ステップ 4　次のコマンドを使用して、設定ファイル ユーティリティを実行します。

```
runCfgUtil.sh -l unprov.tmpl -o unprov.cm
```

入力する内容は次のとおりです。

- unprov.tmpl：バイナリ ファイルに解析する、既存のテンプレート ファイルを示します。
- unprov.cm：使用する出力ファイル名を指定します。

ユーティリティを実行すると、次のような結果が表示されます。

```
# /opt/CSCObpr/rdu/bin/runCfgUtil.sh -l unprov.tmpl -o unprov.cm
Broadband Provisioning Registrar Configuration Utility
Version: 2.7

0 error(s), 0 warning(s) detected. Parsing of unprov.tmpl was successful.
The file unprov.tmpl was parsed successfully in 595 ms.
The parser initialization time was 262 ms.
The parser parse time was 333 ms.
```

ローカル バイナリ ファイルの表示

使用上のガイドライン　**runCfgUtil.sh** コマンドを使用して、ローカル バイナリ ファイルを表示します。

シンタックスの説明　**runCfgUtil.sh** コマンドを使用してローカル バイナリ ファイルを表示するときは、次の構文を使用する必要があります。

```
runCfgUtil.sh -d -l <file>
```

入力する内容は次のとおりです。

- -d：このコマンドでバイナリ入力ファイルを表示することを指定します。
- -l：入力ファイルがローカル ファイル システムにあることを示します。
- <file>：表示する既存のバイナリ入力ファイルを示します。

ローカル ファイル システムにあるバイナリ ファイルを表示するには、次の手順に従います。

ステップ 1　/opt/CSCObpr/rdu/samples/packet_cable にディレクトリを変更します。

ステップ 2　表示するバイナリ ファイルを選択します。

ステップ 3　次のコマンドを使用して、設定ファイル ユーティリティを実行します。

```
runCfgUtil.sh  -d -l unprov_packet_cable.bin
```

入力する内容は次のとおりです。

- unprov_packet_cable.bin：表示する既存のバイナリ入力ファイルを示します。

ユーティリティを実行すると、次のような結果が表示されます。

```
Off    File Bytes      Option    Description                    Value
0       FE0101          254     Telephony Config File Start/End  1
       0B153013060E    11        SNMP MIB Object                .iso.org.dod.internet.
3      2B06010401A30                                            private.enterprises.ca
       B020201010107                                            bleLabs.clabProject.
       00020102                                                 clabProjPacketCa
                                                                ble.pktcMtaMib.pktcMta
                                                                MibObjects
                                                                .pktcMtaDevBase.
                                                                pktcMtaDevEnable
                                                                d.0,INTEGER,fals e(2)
. . . . . . . . . . . . . . . . . .
```

外部バイナリ ファイルの表示

使用上のガイドライン　**runCfgUtil.sh** コマンドを使用して、外部バイナリ ファイルを表示します。

シンタックスの説明　**runCfgUtil.sh** コマンドを使用して外部バイナリ ファイルを表示するときは、次の構文を使用する必要があります。

```
runCfgUtil.sh -d -r <file> -u <username> -p <password>
```

入力する内容は次のとおりです。

- -d：このコマンドでバイナリ入力ファイルを表示することを指定します。
- -r：入力ファイルが RDU に追加した外部ファイルであることを示します。
- <file>：RDU に存在する外部バイナリ ファイルを示します。
- -u <username>：RDU に接続するときに使用するユーザ名を指定します。
- -p <password>：RDU に接続するときに使用するパスワードを指定します。

RDU に追加したバイナリ ファイルを表示するには、次の手順に従います。

(注)　この例では、RDU が localhost:49187 だとします。

ステップ 1　表示するバイナリ ファイルを選択します。この例では、既存のバイナリ ファイル unprov.cm を使用します。

ステップ 2　次のコマンドを使用して、設定ファイル ユーティリティを実行します。

```
runCfgUtil.sh -d -r unprov.cm -u admin -p changeme
```

入力する内容は次のとおりです。

- unprov.cm：RDU に存在する外部バイナリ ファイルを示します。
- admin：この例で使用するユーザ名を示します。
- changeme：この例で使用するパスワードを示します。

ユーティリティを実行すると、次のような結果が表示されます。

```
Off     File Bytes       Option      Description                  Value
0       030100           3          Network Access Control        Off
3       041F             4          Class of Service
5       010101           4.1        Class ID                      1
8       02040001F400     4.2        Maximum Downstream Rate       128000 bits/sec
14      03040000FA00     4.3        Maximum Upstream Rate         64000 bits/sec
20      040101           4.4        Upstream Channel Priority     1
. . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . .
252     06108506547F     6          CM MIC Configuration Setting  8506547FC9152B44
        C9152B44DB95                                              DB955420843EF6FE
        5420843EF6FE
```

```
270     0710644B675B     7          CMTS MIC Configuration Setting    644B675B70B7BD3E
        70B7BD3E09AC                                                  09AC210F794A1E8F
        210F794A1E8F
288     FF               255        End-of-Data Marker
289     00               0          PAD
290     00               0          PAD
291     00               0          PAD
0 error(s), 0 warning(s) detected. Parsing of unprov.tmpl was successful.
The file unprov.tmpl was parsed successfully in 375 ms.
The parser initialization time was 63 ms.
The parser parse time was 312 ms.
```

PacketCable BASIC フローの有効化

使用上のガイドライン

runCfgUtil.sh コマンドを使用して、PacketCable BASIC フローの完全性ハッシュを生成し、BASIC フローの静的設定ファイルに挿入することをサポートします。

シンタックスの説明

runCfgUtil.sh コマンドを使用して PacketCable BASIC フローをサポートするときは、次の構文を使用する必要があります。

```
runCfgUtil.sh -t <basic/secure>
```

入力する内容は次のとおりです。

- -basic：このオプションは、PacketCable BASIC フローの完全性ハッシュを計算し、MTA 静的設定ファイルに挿入します。
- -secure：このオプションは、PacketCable BASIC フローの完全性ハッシュを MTA 静的設定ファイルに挿入しません。これがデフォルト設定です。

RDU ログ レベル ツール

RDU ログ レベル ツールを使用して、コマンドラインから（ローカル コンピュータの）RDU の現在のログ レベルを変更します。このツールは RDU 環境でのみ利用可能ですが、<BACC_HOME>/rdu/bin ディレクトリにあります。表 12-6 に、利用可能なログ レベルと、イネーブルにした場合にログ ファイルに書き込まれるメッセージの種類を示します。

表 12-6　ログ レベル

ログ レベル	説明
緊急	システムが不安定です。
アラート	すぐに対応が必要です。
クリティカル	クリティカルな状態が存在します。
エラー	エラー状態が存在します。
警告	警告状態が存在します。
通知	正常ですが重要な状態です。
情報	情報メッセージのみに使用されます。

安定した動作状態を維持するためには、RDU ロギング レベルを警告レベルのままにすることをお勧めします。デバッグ動作中に安定した状態パフォーマンスを維持する必要がある場合は、情報レベルをお勧めします。ただし、情報レベルに設定して実行すると大量のログ エントリが作成され、このことがパフォーマンスに悪影響を与える可能性があるため、注意が必要です。

RDU ログ レベル ツールの使用方法

すべての例では、RDU のユーザ名は admin、RDU のパスワードは changeme とし、RDU が実行中であることを前提にしています。

次のコマンドを入力して、RDU ログ レベル ツールを実行します。

```
setLogLevel.sh [0..6] [-help] [-show] [-default] [-debug]
```

入力する内容は次のとおりです。

- -[*0..6*]：使用するログ レベルを示します。利用可能なレベルは、次のとおりです。
  - 0：緊急レベルです。すべての緊急メッセージを保存するように、ロギング機能を設定します。
  - 1：アラート　レベルです。すぐに対応が必要なすべてのアクティビティ、およびさらに深刻な活動を保存するように、ロギング機能を設定します。
  - 2：クリティカル　レベルです。すべての異常な状態、およびさらに深刻な状態を保存するように、ロギング機能を設定します。
  - 3：エラー レベルです。すべてのエラー メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。
  - 4：警告レベルです。すべての緊急メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。
  - 5：通知レベルです。すべての通知レベル　メッセージ、およびさらに深刻なメッセージを保存するように、ロギング機能を設定します。
  - 6：情報レベルです。利用可能なすべてのロギング　メッセージを保存するように、ロギング機能を設定します。
- *-help*：ツールのヘルプを表示します。
- *-show*：RDU サーバの現在のログ レベル設定を表示します。

- *-default*：RDU をインストール デフォルト レベルの 5（通知）に設定します。
- *-debug*：RDU サーバのカテゴリのトレースをイネーブルまたはディセーブルにするように、対話モードを設定します。

（注） シスコのサポート　スタッフの指示があった場合にのみ、デバッグ設定をイネーブルにしてください。

このツールを使用して、次の機能も実行できます。

- RDU ログ レベルの設定（P.12-40）
- RDU の現在のログ レベルの表示（P.12-41）

RDU ログ レベルの設定

このツールを使用して、ロギング レベルをある値から別の値に変更できます。次の例では、RDU ロギング レベルを警告レベル（**setLogLevel.sh** コマンドでは数値 4 で示されるレベル）に設定する方法を示します。実際のログ レベル設定は手順にとって重要ではないので、必要に応じて読み替えてください。

RDU ロギング レベルを設定するには、次の手順に従います。

ステップ 1　<BACC_HOME>/rdu/bin にディレクトリを変更します。

ステップ 2　次のコマンドを使用して、RDU ログ レベル ツールを実行します。

```
setLogLevel.sh 4
```

次のプロンプトが表示されます。

```
Please type RDU username:
```

ステップ 3　プロンプトに対して、RDU ユーザ名を入力します。この例では、デフォルト ユーザ名（admin）を使用します。

```
Please type RDU username: admin
```

次のプロンプトが表示されます。

```
Please type RDU password:
```

ステップ 4　プロンプトに対して、RDU　のパスワードを入力します。この例では、デフォルト　パスワード（changeme）を使用します。

```
Please type RDU password: changeme
```

次のメッセージが表示され、ログ レベルが変更されたことが通知されます。この例では、レベル 5（通知）から 4（警告）に変更されました。

```
RDU Log level was changed from 5 (notification) to 4 (warning).
```

RDU の現在のログ レベルの表示

このツールを使用して、ロギング レベルの値を変更する前に、RDU ログを表示し、設定されている値を判別できます。この手順では、ツールを使用して RDU の現在のロギング レベルを表示する方法を示します。ここでは、コンピュータが RDU にすでに接続されていることを前提としています。

RDU の現在のロギング レベルを表示するには、次の手順に従います。

ステップ 1　<BACC_HOME>/rdu/bin にディレクトリを変更します。

ステップ 2　次のコマンドを実行します。

```
setLogLevel.sh -show
```

次のプロンプトが表示されます。

```
Please type RDU username:
```

ステップ 3　RDU ユーザ名（admin）を入力し、**Enter** キーを押します。

```
Please type RDU username: admin
```

次のプロンプトが表示されます。

```
Please type RDU password:
```

ステップ 4　RDU パスワード（changeme）を入力し、**Enter** キーを押します。

```
Please type RDU password: changeme
```

次のメッセージが表示されます。

```
The logging is currently set at level: 4 (warning)
All tracing is currently disabled.
```

KDC 証明書を管理するための PKCert.sh ツールの使用方法

PKCert ツールを使用して、KDC のオペレーションに必要な KDC 証明書をインストールし、管理できます。このツールは、獲得した CableLabs サービス プロバイダー証明書を取得し、KDC のオペレーションに必要な次のような一連の証明書ファイルに変換します。

- Cablelabs_Service_Provider_Root.cer
- Service_Provider.cer
- Local_System.cer
- KDC.cer

このツールで、証明書チェーンの検証や、KDC が要求する名前へのコピーおよび名前の変更もできます。

(注)　このツールは、KDC コンポーネントをインストールした場合にのみ利用可能です。

PKCert ツールの実行

次のコマンドを実行して、デフォルト位置の <BACC__HOME>/kdc ディレクトリで PKCert ツールを実行します。

```
PKCert.sh [function] [option]
```

入力する内容は次のとおりです。

- *[function]*：実行する機能を示します。たとえば、適切な機能を選択する次のスイッチのいずれかを入力します。
  - -c：KDC 証明書を作成します。詳細については、P.12-43 の「KDC 証明書の作成」を参照してください。
  - -v：PacketCable 証明書セットを検証し、標準化します。詳細については、P.12-44 の「KDC 証明書の検証」を参照してください。

(注)　これらのオプションの使用方法がわからない場合は、-? オプションを指定すると、利用可能なすべてのヘルプ情報がコンピュータの画面に表示されます。

- *[option]*：上で選択した機能に依存するオプション機能を実装します。

PKCert コマンドを実行すると、要求された動作の実行中に発生したすべてのエラーのリストが出力されます。このプリントアウトを使用して、発生した可能性があるすべての問題をトラブルシューティングできます。

KDC 証明書の作成

/opt/CSCObpr/kdc ディレクトリから次のコマンドを入力して、KDC 証明書を作成します。

`PKCert.sh` -s <*dir*> *-d <dir> -c <cert> -e -r <realm> -a <name> -k <keyFile> [-n <serial>] [-o]*

入力する内容は次のとおりです。

- -a <name>：KDC の DNS 名を指定します。
- -c <Cert File>：サービス プロバイダー証明書を使用します（DER 符号化）。
- -d <directory>：作成先ディレクトリを指定します。
- -e：証明書が Euro-PacketCable 証明書であることを示します。
- -k <Key File>：サービス プロバイダー秘密鍵を使用します（DER 符号化）。
- -n <Serial#>：証明書のシリアル番号を設定します。
- -o：既存のファイルを上書きします。
- -r <Realm>：KDC 証明書の Kerberos 領域を指定します。
- -s <directory>：作成元ディレクトリを指定します。

新しい証明書を作成してインストールするとき、新しい証明書は、subject alternate name フィールドで領域を識別します。新しい証明書は現在の環境に対して、次の項目において一意です。

- KDC 領域。
- MTA が使用する、この KDC に関連付けられた DNS 名。

  次に例を示します。

```
PKCert.sh  -c "-s . \
-d /opt/CSCObpr/kdc/solaris/packetcable/certificates \
-k CLCerts/Test_LSCA_privkey.der \
-c CLCerts/Test_LSCA.cer \
-r PCTEST.CISCO.COM \
-n 100 \
-a kdc.pctest.cisco.com \
-o"
```

このコマンドを使用して、ファイル /opt/CSCObpr/kdc/solaris/packetcable/certificates/KDC.cer と /opt/CSCObpr/kdc/solaris/packetcable/certificates/KDC_private_key.pkcs8 を作成します。この KDC 証明書では、realm は PCTEST.CISCO.COM、シリアル番号は 100、KDC サーバの FQDN は kdc.pctest.cisco.com に設定されます。

(注) 正常にコマンドが終了すると、ファイル /opt/CSCObpr/kdc/solaris/packetcable/certificates/KDC_private_key.pkcs8 を /opt/CSCObpr/kdc/solaris/KDC_private_key.pkcs8 にコピーする必要があることを示すコンソール メッセージが表示されます。コマンドライン オプション **-o** を使用すると、ユーティリティは既存のファイルを上書きします。

KDC 証明書の検証

このコマンドで、指定した作成元ディレクトリのすべてのファイルを検査し、X.509 証明書として識別します。正規の X.509 証明書が見つかった場合、ファイルは適切な名前に変更され、宛先ディレクトリにコピーされます。特定の目的（サービス プロバイダーまたはデバイス）で、正規の証明書チェーンが複数確認された場合は、エラーが生成されます。この場合は、余分な証明書を作成元ディレクトリから削除し、コマンドを再度実行する必要があります。

(注)　**PKCert.sh -v -?** コマンドを入力すると、PKCert の使用方法が画面に表示されます。

/opt/CSCObpr/kdc ディレクトリから次のコマンドを入力して、KDC 証明書を検証します。

```
PKCert.sh -v -s <dir> -d <dir> -o -r <dir>
```

入力する内容は次のとおりです。

- -s <directory>：作成元ディレクトリを指定します。
- -d <directory>：作成先ディレクトリを指定します。
- -o：既存のファイルを上書きします。
- -r <directory>：参照証明書ディレクトリを指定します。

検証は、このパッケージに組み込まれた参照証明書を対象に実行されます。'-d' オプションを指定すると、名前が正規化されて、証明書がターゲット ディレクトリにインストールされます。

次に例を示します。

```
PKCert.sh  -v \
"-s . \
-d /opt/CSCObpr/kdc/solaris/packetcable/certificates \
-o"
```

changeNRProperties.sh ツールの使用

BACC インストール プログラムは、Network Registrar DHCP サーバに組み込まれる BACC 拡張で使用する設定プロパティの値を設定します。キー設定プロパティを変更するには、<BACC_HOME>/cnr_ep/bin ディレクトリにある **changeNRProperties.sh** コマンドを使用します。

パラメータを付けずにスクリプトを起動すると、設定できるプロパティのリストを示すヘルプ メッセージが表示されます。

コマンドを実行するには、次の手順に従います。

ステップ 1　<BACC_HOME>/cnr_ep/bin にディレクトリを変更します。

ステップ 2　changeNRProperties.sh コマンドを実行します。

```
changeNRProperties.sh <options>
```

<*options*> には、次のものを指定できます。

- -help：このヘルプ メッセージを表示します。-help オプションは、排他的に使用する必要があります。その他のオプションと同時に使用することはできません。
- -e <enabled|disabled>：PacketCable enable プロパティを設定します。プロパティをイネーブルにするには **-e enabled** を入力し、ディセーブルにするには **-e disabled** を入力します。
- -d：現在のプロパティを表示します。-d オプションは、排他的に使用する必要があります。その他のオプションと同時に使用することはできません。
- -s <secret>：BACC 共有秘密情報を示します。たとえば、共有秘密情報が単語 *secret* の場合は、**-s secret** と入力します。
- -f <fqdn>：RDU の FQDN を示します。たとえば、完全修飾ドメイン名として rdu.cisco.com を使用する場合は、**-f rdu.cisco.com** と入力します。
- -p <port>：使用する RDU ポートを示します。たとえば、ポート番号 49187 を使用する場合は、**-p 49187** と入力します。
- -r <realm>：PacketCable 領域を示します。たとえば、PacketCable realm が CISCO.COM の場合は、**-r CISCO.COM** と入力します。

(注)　領域は大文字で入力する必要があります。

- -g <prov group>：プロビジョニング グループを示します。たとえば、プロビジョニング グループが group1 の場合は、**-g group1** と入力します。
- -t <00|01>：PacketCable TGT をオフまたはオンに設定することを示します。たとえば、オフに設定する場合は **-t 00** と入力し、オンに設定する場合は **-t 01** と入力します。
- -a <ip>：PacketCable のプライマリ DHCP サーバ アドレスを示します。たとえば、プライマリ DHCP サーバの IP アドレスが 10.10.10.2 の場合は、**-a 10.10.10.2** と入力します。
- -b <ip>：PacketCable のセカンダリ DHCP サーバ アドレスを示します。たとえば、セカンダリ DHCP サーバの IP アドレスが 10.10.10.4 の場合は、**-b 10.10.10.4** と入力します。必要な場合は、**-b null** と入力して、ヌル値を設定することもできます。
- -y <ip>：PacketCable のプライマリ DNS サーバ アドレスを示します。たとえば、PacketCable プライマリ DNS サーバの IP アドレスが 10.10.10.6 の場合は、**-y 10.10.10.6** と入力します。
- -z <ip>：PacketCable のセカンダリ DNS サーバ アドレスを示します。たとえば、セカンダリ DNS サーバの IP アドレスが 10.10.10.8 の場合は、**-z 10.10.10.8** と入力します。必要な場合は、**-z null** と入力して、ヌル値を設定することもできます。

ステップ 3　DHCP サーバを再起動します。

例

Network Registrar 拡張を NR Extensions Properties ツールで変更する例を示します。

```
# /opt/CSCObpr/cnr_ep_bin/changeNRProperties.sh -g primary1
Current NR Properties:
RDU Port: 49187
RDU FQDN: rdu.acme.com
Provisioning Group: primary1
Shared Secret: fggTaLg0XwKRs
PacketCable Enable: enabled
PacketCable TGT: 01
PacketCable Realm: ACME.COM
PacketCable Primary DHCP Server: 192.168.1.2
PacketCable Secondary DHCP Server: NOT SET
PacketCable Primary DNS Server: 192.168.1.2
PacketCable Secondary DNS Server: NOT SET
```

(注)　変更を有効にするには、NR DHCP サーバを再起動する必要があります。

現在のプロパティの表示例です。

```
# /opt/CSCObpr/cnr_ep_bin/changeNRProperties.sh -d
Current NR Properties:
RDU Port: 49187
RDU FQDN: rdu.acme.com
Provisioning Group: primary1
Shared Secret: fggTaLg0XwKRs
PacketCable Enable: enabled
PacketCable TGT: 01
PacketCable Realm: ACME.COM
PacketCable Primary DHCP Server: 192.168.1.2
PacketCable Secondary DHCP Server: NOT SET
PacketCable Primary DNS Server: 192.168.1.2
PacketCable Secondary DNS Server: NOT SET
```

Keygen ツールの使用方法

keygen ツールを使用して、PacketCable サービス キーを生成します。サービス キーは、KDC 通信に必要な共通鍵暗号方式による 3 ビット バイト データ暗号規格（3 ビット バイト DES または 3DES）キー（共有秘密情報）です。KDC サーバでは、DPE のプロビジョニング FQDN ごとにサービス キーが必要です。

KDC サーバは、起動時にサービス キーを読み取ります。サービス キーを修正した場合は、KDC サーバを再起動する必要があります。DPE CLI で DPE プロビジョニング FQDN を変更する場合は、対応する KDC サービス キー ファイル名も変更する必要があります。これは、KDC サービス キーが DPE プロビジョニング FQDN をファイル名の一部として使用するためです。

このツールは、<BACC_HOME>/kdc ディレクトリにあり、コマンドライン引数として DPE プロビジョニング FQDN、領域名、パスワードをとり、サービス キー ファイルを生成します。

シンタックスの説明

Keygen ツールを使用するときは、次の構文を使用します。

keygen *[options]* <fqdn> <realm> <password>

options には、次のものがあります。

- -?：この使用方法メッセージを表示し、コマンドを終了します。
- -v、-version：このツールのバージョンを表示し、コマンドを終了します。
- -q、-quiet：出力を作成しないクワイエット モードを実装します。
- -c、-cms：CMS システムのサービス キーを作成します。
- <*fqdn*>：DPE の完全修飾ドメイン名を示します。これは必須エントリです。
- <*realm*>：Kerberos 領域を示します。これは必須エントリです。
- <*password*>：使用するパスワードを指定します。これも必須フィールドです。パスワードの長さは、6 文字から 20 文字までにする必要があります。次に例を示します。

次のファイル名構文によって、3 つのサービス キー ファイルが KDC キー ディレクトリに書き込まれます。

```
mtafqdnmap,<fqdn>@<REALM>
mtaprovsrvr,<fqdn>@<REALM>
krbtgt,<REALM>@<REALM>
```

サービス キー ファイルには、常に、バージョン フィールド 0x0000 が含まれます。

例

次の例では、KDC が DPE 通信を行うときに使用するサービス キーを生成する方法を示します。次のコマンドを入力します。

```
bash-2.05b$ keygen dpe.cisco.com CISCO.COM changeme
```

このコマンドを実装すると、次の KDC サービス キーが <BACC_HOME>/kdc/solaris/keys ディレクトリに書き込まれます。

```
mtafqdnmap,dpe.cisco.com@CISCO.COM
mtaprovsrvr,dpe.cisco.com@CISCO.COM
krbtgt,CISCO.COM@CISCO.COM
```

（注） 新しいキーを認識するには、KDC を再起動する必要があります。

次の BPR エージェント コマンドを使用して、KDC を再起動します。

```
/etc/init.d/bprAgent restart kdc
```

次の例では、CMS サービス キーの生成を示します。次のコマンドを入力します。

```
bash-2.05b$ keygen -c cms-fqdn.com CMS-REALM-NAME changeme
```

このコマンドを実装すると、次の CMS サービス キーが <BACC_HOME>/kdc/solaris/keys ディレクトリに書き込まれます。

```
cms,cms-fqdn.com@CMS-REALM-NAME
```

(注)　このツールを実行するときは、PacketCable registration kdc-service-key コマンドと同じパスワードを入力します。詳細については、『*Cisco Broadband Access Center for Cable Command Line Reference*』を参照してください。

snmpAgentCfgUtil.sh コマンドの使用方法

snmpAgentCfgUtil.sh コマンドを使用すると、Solaris コンピュータにインストールされている SNMP エージェントを管理できます。このコマンドは <BACC_HOME>/snmp/bin ディレクトリにあり、これを使用して、SNMP 通知を受信する他のホストのリストにホストを追加（またはリストから削除）したり、SNMP エージェント プロセスを起動および中止できます。このコマンドは、ローカル ディレクトリから実行する必要があります。

（注） Solaris コンピュータ上で動作する SNMP エージェントのデフォルト ポート番号は 8001 です。

RDU SNMP エージェントを使用して、次のことができます。

- ホストの追加（P.12-49）
- ホストの削除（P.12-50）
- SNMP エージェント コミュニティの追加（P.12-50）
- SNMP エージェント コミュニティの削除（P.12-51）
- SNMP エージェントの開始（P.12-51）
- SNMP エージェントの停止（P.12-51）
- SNMP エージェントの場所の変更（P.12-52）
- SNMP の連絡先の設定（P.12-52）
- SNMP エージェントの設定のリスト（P.12-53）

ホストの追加

次のコマンドは、SNMP エージェントから SNMP 通知を受信するホストのリストにホスト アドレスを追加します。

シンタックスの説明

ホストを追加するには、次のコマンドを入力します。

```
> snmpAgentCfgUtil.sh add host <host-addr> community  <community> [udp-port <port>]
```

入力する内容は次のとおりです。

- *<host-addr>*：ホストのリストに追加するホストの IP アドレスまたは FQDN を指定します。
- *<community>*：SNMP　通知を送信するときに使用するコミュニティ（リードまたはライト）を指定します。
- *<port>*：SNMP 通知の送信に使用する UDP ポートを示します。

例

次の例で、**snmpAgentCfgUtil.sh** コマンドを使用してホストを追加する方法を示します。

```
> snmpAgentCfgUtil.sh add host test.cisco.com community trapCommunity udp-port 162
OK
Please restart [stop and start] SNMP agent.
```

ホストの削除

SNMP エージェントから SNMP 通知を受信するホストのリストからホストを削除できます。

シンタックスの説明　ホストを削除するには、次のコマンドを入力します。

snmpAgentCfgUtil.sh delete host <*host-addr*>

入力する内容は次のとおりです。

- <*host-addr*>：ホストのリストから削除するホストの IP アドレスを指定します。

例　次の例で、**snmpAgentCfgUtil.sh** コマンドを使用してホストを削除する方法を示します。

```
> ./snmpAgentCfgUtil.sh delete host test.cisco.com
OK
Please restart [stop and start] SNMP agent.
```

SNMP エージェント コミュニティの追加

SNMP コミュニティ ストリングを追加して、SNMP エージェントへのアクセスを許可できます。

シンタックスの説明　コミュニティ ストリングを追加するには、次のコマンドを入力します。

snmpAgentCfgUtil.sh add community *string* ***[ro | rw]***

入力する内容は次のとおりです。

- <*string*>：SNMP コミュニティを示します。
- <*ro*>：読み取り専用（ro）のコミュニティ ストリングを割り当てます。実行できるのは *get* 要求（クエリー）だけです。ro コミュニティ ストリングは、*get* 要求を許可しますが、*set* オペレーションは許可しません。NMS と管理対象デバイスは、同じコミュニティ ストリングを参照する必要があります。
- <*rw*>：読み取りと書き込み（rw）コミュニティ ストリングを割り当てます。SNMP アプリケーションでは、*set* オペレーションに rw アクセスが必要です。rw コミュニティ ストリングを使用すると、OID 値への書き込みアクセスが可能になります。

（注）　デフォルトの ro および rw コミュニティ ストリングは、それぞれ bprread と bprwrite です。BACC を配備する前に、これらの値を変更することをお勧めします。

例　次の例で、SNMP エージェント コミュニティ ストリングを追加する方法を示します。

```
> snmpAgentCfgUtil.sh add community fsda54 ro
OK
Please restart [stop and start] SNMP agent.
```

SNMP エージェント コミュニティの削除

SNMP コミュニティ ストリングを削除して、SNMP エージェントへのアクセスを禁止できます。

シンタックスの説明　コミュニティ ストリングを削除するには、次のコマンドを入力します。

```
snmpAgentCfgUtil.sh delete community string [ro | rw]
```

入力する内容は次のとおりです。

- <*string*>：SNMP コミュニティを示します。
- <*ro*>：読み取り専用（ro）コミュニティ ストリングを割り当てます。
- <*rw*>：読み取りと書き込み（rw）コミュニティ ストリングを割り当てます。

（注）　ro および rw コミュニティ ストリングの詳細については、P.12-50 の「SNMP エージェント コミュニティの追加」を参照してください。

例　次の例で、SNMP エージェント コミュニティ ストリングを削除する方法を示します。

```
> snmpAgentCfgUtil.sh delete community fsda54 ro
OK
Please restart [stop and start] SNMP agent.
```

SNMP エージェントの開始

次のコマンドは、BACC がすでにインストールされている Solaris コンピュータで SNMP エージェント プロセスを開始します。

シンタックスの説明　SNMP エージェント プロセスを開始するには、次のコマンドを入力します。

```
snmpAgentCfgUtil.sh start
```

SNMP エージェントの停止

次のコマンドは、BACC がすでにインストールされている Solaris コンピュータで SNMP エージェント プロセスを停止します。

シンタックスの説明　SNMP エージェント プロセスを停止するには、次のコマンドを入力します。

```
snmpAgentCfgUtil.sh stop
```

SNMP エージェント リスニング ポートの設定

次のコマンドは、SNMP エージェントがリッスンするポート番号を指定します。RDU SNMP エージェントが使用するデフォルト ポート番号は 8001 です。

シンタックスの説明　SNMP エージェントがリッスンするポートを確立するには、次のコマンドを入力します。

snmpAgentCfgUtil.sh udp-port *<port>*

<*port*> は、SNMP エージェントがリッスンするポート番号を示します。

SNMP エージェントの場所の変更

次のコマンドを使用すると、SNMP エージェントを実行するデバイスの場所を示す際に使用できるテキスト文字列を入力できます。たとえば、このコマンドを使用してデバイスの物理的な場所を示すことができます。場所として、最大 254 文字の任意の文字列を入力できます。

シンタックスの説明　SNMP エージェントの場所を入力するには、次のコマンドを入力します。

snmpAgentCfgUtil.sh location *<location>*

<*location*> は、エージェントの場所を示す文字列です。

例　次の例では、SNMP エージェントの物理的な場所は、rack 5D と示された装置ラックです。

```
snmpAgentCfgUtil.sh location "equipment rack 5D"
```

SNMP の連絡先の設定

次のコマンドを使用すると、SNMP エージェントの連絡担当者と、この担当者への連絡方法を示す際に使用できるテキスト文字列を入力できます。たとえば、このコマンドを使用して、特定の担当者（電話番号を含む）を示すことができます。最大 255 文字の任意の文字列を入力できます。

シンタックスの説明　次の構文を使用して、特定の SNMP エージェントの連絡先情報を入力します。

snmpAgentCfgUtil.sh contact *<contact-info>*

<*contact-info*> は、SNMP エージェントに関する連絡担当者を示す文字列です。

例　次の例では、連絡担当者の名前は Ace Duffy で、内線番号は 1234 です。

```
snmpAgentCfgUtil.sh contact "Ace Duffy - ext 1234"
```

SNMP エージェントの設定のリスト

使用上のガイドライン　このコマンドでは、現在の SNMP 設定をすべて表示できます。

シンタックスの説明　現在の SNMP 設定をすべて表示するには、次のコマンドを入力します。

```
snmpAgentCfgUtil.sh show
```

例　このコマンドを実行すると、次のようなサンプル出力が表示されます。

```
# ./snmpAgentCfgUtil.sh show
Location : Washington_1
Contact : John
Port Number : 8001
Notification Type : trap
Notification Recipient Table :
[ Host IP address, Community, UDP Port ]
[ 10.10.10.1, public , 162 ]
Access Control Table :
Read Only Communities
baccread
Read Write Communities
baccwrite
```

SNMP 通知タイプの指定

使用上のガイドライン　次のコマンドを使用すると、SNMP エージェントから送信される通知のタイプ（トラップまたは通知）を指定できます。デフォルトではトラップが送信されますが、SNMP 通知を送信するように設定することもできます。

シンタックスの説明　このコマンドを入力するときは、次の構文を使用する必要があります。

```
snmpAgentCfgUtil.sh inform [retries timeout] |trap
```

パラメータは、リトライ間のバックオフ タイムアウトです。

利用可能なディスク領域を監視するための disk_monitor.sh ツールの使用方法

利用可能なディスク領域を監視することは、重要なシステム管理作業です。多数のカスタム スクリプトまたは市販のツールを使用して、この作業を実行できます。

disk_monitor.sh コマンドは <BACC_HOME>/rdu/sample/tools ディレクトリにあり、1 つ以上のファイル システムのしきい値を設定します。これらのしきい値を超えると、追加のディスク領域が利用可能になるまで、60 秒ごとに Solaris の syslog 機能によってアラートが生成されます。

(注) 少なくとも、disk_monitor.sh スクリプトを使用して <BACC_DATA> および <BACC_DBLOG> ディレクトリを監視することをお勧めします。

利用可能なディスク領域を監視するには、次のコマンドを実行します。

```
# ./disk_monitor.sh (file system-directory) (x)
```

入力する内容は次のとおりです。

- *(file system-directory)*：監視するファイル システムのディレクトリを示します。
- *(x)*：指定したファイル システムに適用するしきい値をパーセントで示します。

例

データベース ログが保存されるファイル システム（ここでは /var/CSCObpr）の利用率が 80% に達したときに、通知するものとします。次の構文を使用して、コマンドを入力します。

```
# ./disk_monitor.sh /var/CSCObpr 80
```

データベース ログのディスク領域の利用率が 80% に達すると、次のようなアラートが syslog ファイルに送信されます。

```
Dec 7 8:16:03 perf-u80-1 BPR: [ID 702911 local6.warning] File system /var/bpr usage is
81% (threshold is 80%)
```

MAC アドレスによるデバイスのトラブルシューティング

ノード管理を使用して、特定のデバイスまたはデバイス グループのトラブルシューティングを行うことができます。この場合、ロギングをオンにしたり、デバイス固有またはグループ固有の情報についてのログ ファイルを検索したりする必要はありません。

BACC は、問題のトラブルシューティングに関する詳細なデバイス情報を含むデバイス リストを、MAC アドレスに基づいて保守します。トラブルシューティング情報は、RDU で一元的に保管され、デバイス単位で保守されます。DPE も Network Registrar 拡張も、このデータを保管しません。反対に、DPE または Network Registrar 拡張は、この情報を RDU に転送します。RDU は、情報を受信すると、適切なデバイス ログ ファイルに書き込みます。DPE または Network Registrar 拡張から RDU への接続が失われた場合、この情報は、その接続が復元されるまで廃棄されます。

(注) 新しいデバイスまたはグループの追加など、このリストに加える変更は即時に有効になります。デバイスをリブートする必要はありません。

DPE は、すべてのデバイスの MAC アドレスを、そのデバイスの IP アドレス マッピングにマップします。また、Network Registrar 拡張は、デバイスのトラブルシューティングがイネーブルになっていると判断するたびに、IP アップデートを DPE に送信します。

デバイス トラッキング リストを管理するには、管理者の GUI を使用して、任意の時点でトラッキング可能なデバイスの数を設定します。デフォルト値は 100 デバイスです。トラッキング機能は、デバイスがリスト表示されるまで、オフとみなされます。詳細については、P.9-5 の「デバイス管理」を参照してください。

注意 この機能を使用する場合は、追加のメモリおよびディスク領域が必要になります。トラッキング対象のデバイス数が増えると、作成されたログの数をサポートするのに必要なメモリおよびディスク領域の容量も増えます。

アラートとエラー メッセージ

この付録では、Broadband Access Center for Cable（BACC）で生成されるすべてのアラート メッセージとエラー メッセージについて説明します。

アラート メッセージ

BACC のアラートは、UNIX の syslog サービスを通して生成されます。syslog は、UNIX 上で情報のロギングを管理するためのクライアント / サーバ プロトコルです。BACC の syslog アラートは、ロギング サービスではありません。問題が発生した場合には通知されますが、問題の原因がいつも特定されるとは限りません。この情報が該当する BACC ログ ファイルに書き込まれる場合もあります。

メッセージ形式

BACC によって生成されるアラート メッセージの形式は次のとおりです。

XXX-#-####: <Message>

内容は次のとおりです。

- *XXX*：ファシリティ コードを表します。次のようなコードがあります。
  - RDU（Regional Distribution Unit）
  - DPE（Device Provisioning Engine）
  - AGENT（rduSnmpAgent または dpeSnmpAgent）
  - NR_EP（Network Registrar 拡張ポイント）
  - KDC
- #：使用されている重大度のレベルを表します。アラートは、1（アラート）、3（エラー）、6（情報メッセージ）という 3 つのレベルがあります。
- ###：数字のエラー コードを表します。詳細については、次の項を参照してください。
- <*Message*>：アラートのテキスト（メッセージ）を表します。

RDU のアラート

RDU の syslog アラートが送信されるたびに、追加の詳細が <BACC_DATA>/rdu/logs/rdu.log というログ ファイルに書き込まれます（追加の詳細がある場合）。表 A-1 は、RDU のアラートを示します。

表 A-1　RDU のアラート

アラート	説明
RDU-1-101: RDU ran out of disk space	このアラートは、RDU サーバが使用するハード ドライブのパーティションに、空き領域が不足していることを示します。必要に応じて、ログ ファイルを削除または圧縮してください。 ディスクのアップグレードの詳細については、第 12 章「Broadband Access Center for Cable がサポートするツールと高度な概念」を参照してください。
RDU-1-103: RDU ran out of memory	このアラートは、RDU のメモリが不足していることを示します。
RDU-1-111: Evaluation key for technology *[<technology_name>]* expired	このアラートは、指定したテクノロジーの評価キーの期限が満了していることを示します。シスコの営業担当または TAC にお問い合せのうえ、新しいライセンス キーを入手してください。
RDU-1-115: You have used *[<percent>]*% of available *[<technology_name>]* licenses.	このアラートは、ライセンスの総許容数のうち使用されているライセンスの数をパーセントで示します。このアラートは、ライセンスの総許容量の 80% に達したときに初めて生成されます。
BPR-RDU-4-1140: DNS took [X] seconds for lookup of address [10.0.0.1/test.com]; Check DNS configuration and health of servers	このアラートは BACC のパフォーマンスが低下していることを示します。このアラートは、IP アドレスのループ アップが 60 秒を上回るたびに生成されます。

Solaris DPE のアラート

DPE の syslog アラートが送信されるたびに、追加の詳細が DPE ログに書き込まれます。

DPE ログにアクセスするには、**show log** コマンドを使用します。詳細については、『*Cisco Broadband Access Center for Cable Command Line Reference*』を参照してください。

DPE エラーの中には、RDU サーバのログ ファイルに伝播されるものもあります。これらのエラーは、<BACC_DATA>/rdu/logs/rdu.log ファイルで確認できます。表 A-2 は、Solaris DPE のアラートを示します。

表 A-2　DPE のアラート

アラート	説明
DPE-1-102: DPE ran out of disk space	このアラートは、DPE のハード ドライブに空き領域がないことを示します。次の 3 段階の解決方法があります。 **a.** ディスクに常駐する過剰のサポート バンドルをクリアします。そうするには、不要なサポート バンドルを別のコンピュータへ移動した後、DPE の CLI から **clear bundles** コマンドを実行します。 **b.** DPE の CLI から **clear logs** コマンドを実行して、さらにディスク領域をクリアします。 **c.** 最後の手段として、DPE CLI の **clear cache** コマンドを実行します。この結果、すべてのキャッシュ ファイルが削除され、DPE では RDU サーバとの再同期化が必要となります。
DPE-1-104: DPE ran out of memory	このアラートは、DPE プロセスのメモリが不足していることを示します。 DPE に存在するデバイス構成の数を確認します。デバイス構成が多いほど、使用されるメモリは多くなります。デバイス構成の数を減らすには、DPE がサービスするプロビジョニング グループ（プライマリまたはセカンダリ）の数を制限します。
DPE-1-109: Failed to connect to RDU	このアラートは、RDU に接続できないことを示します。次の作業を行う必要があります。 **a.** DPE ネットワークが正しく構成および接続されていることを確認します。 **b.** **dpe rdu-server** コマンドを使用して、DPE が正しい RDU に接続するよう構成されていること、および接続ポートが正しく構成されていることを確認します。 **c.** RDU プロセスが正しいサーバで実行され、正しいポートで受信されていることを確認します。RDU への接続が確立されるまで、数秒ごとに DPE から RDU プロセスへの再接続が試行されます。

エージェントのアラート

ウォッチドッグ エージェントのプロセスによって syslog アラートが送信されるたびに、エラーの詳細が <BACC_DATA>/agent/logs/ agent_console.log ファイルに書き込まれます（エラーの詳細がある場合）。また、アラートで言及されている特定のコンポーネントに対応したログ ファイルにも出力されます。たとえば、*The [rdu] unexpectedly terminated* のようなアラートを予期せず受信した場合は、RDU サーバのログ ファイル（<BACC_DATA>/rdu/logs/rdu.log）で追加の情報を確認します。表 A-3 はエージェントのアラートを示します。

表 A-3　エージェントのアラート

アラート	説明
AGENT-3-9001: Failed to start the *[<component>]*	このアラートは、プロセスが指定したコンポーネントの開始に失敗したことを示します。
AGENT-3-9002: The *[<component>]* unexpectedly terminated	このアラートは、エージェント プロセスで監視されていた特定のコンポーネントが、不意に失敗したことを示します。
AGENT-3-9003: Failed to stop the *[<component>]*	このアラートは、エージェントが通常終了しようとしたコンポーネントが停止しなかったことを示します。
AGENT-6-9004: The *[<component>]* has started	このアラートは、エージェントによってコンポーネントが正常に開始されるたびに生成されます。
AGENT-6-9005: The *[<component>]* has stopped	このアラートは、ウォッチドッグ エージェントを通してコンポーネントが正常に終了するたびに生成されます。このメッセージは情報の提供のみを目的としています。

表 A-3 でエージェントのアラート リストに示された *[<component>]* 変数は、次のコンポーネント値のいずれかを表します。

- rdu
- dpe
- jrun
- rduSnmpAgent
- dpeSnmpAgent
- kdc

Network Registrar 拡張ポイントのアラート

BAC の Network Registrar 拡張ポイントの syslog アラートが送信されるたびに、追加の詳細が Network Registrar のログ ファイルに書き込まれます。

表 A-4　Network Registrar 拡張ポイントのアラート

アラート	説明
NR_EP-1-106: Failed to connect to RDU	このアラートは、Network Registrar サーバから RDU に接続できないことを示します。RDU プロセスが実行されているかどうかを確認し、まだ実行されていない場合は RDU を開始します。 RDU が実行されている場合は、Network Registrar コンピュータを使用して RDU の PING を実行します。RDU の PING を実行できない場合は、2 つのデバイス間のルーティング テーブルや他の通信パラメータを修正します。 このアラートが頻繁に繰り返される場合は、2 つのホスト間の接続が不安定になっている可能性があります。一般に認められたネットワークのトラブルシューティング テクニックを使用して、2 つのホスト間の接続性を改善してください。
NR_EP-1-107: Failed to connect to any DPEs	このアラートは、Network Registrar 拡張から DPE に接続できないことを示します。 プロビジョニング グループの DPE が Network Registrar 拡張ごとに存在するかどうかを確認します。DPE がプロビジョニング　グループに存在しない場合は、Network Registrar のプロビジョニング グループを DPE が利用可能なものに変更します。DPE がプロビジョニング グループに存在する場合は、Network Registrar 拡張が RDU に登録されていることを確認します。登録されていない場合、DPE は認識されません。 チェックが完了した後もアラートが継続する場合は、プロビジョニング グループの Network Registrar 拡張と DPE との間でネットワークの接続性を確認します。 このアラートが頻繁に繰り返される場合は、2 つのホスト間の接続が不安定になっている可能性があります。一般に認められたネットワークのトラブルシューティング テクニックを使用して、2 つのホスト間の接続性を改善してください。
NR_EP-6-108: The BACC NR extensions have started	このアラートは、Network Registrar 拡張が起動したことを示します。
NR_EP-6-109: The BACC NR extensions have stopped	このアラートは、Network Registrar 拡張が停止したことを示します。
NR_EP-6-110: Registered with RDU *[address and port]*	このアラートは、Network Registrar 拡張が RDU に登録されたことを示します。*[address and port]*　は、Network Registrar 拡張が登録された RDU のアドレスを表します。

CCM による RDU エラーメッセージ

この項で説明する RDU エラー メッセージには、示された問題を是正するために行う対応策があります。これらのエラー メッセージは rdu.log ファイルにあり、リース予約機能による直接の結果です。そのため、Network Registrar の地域別 CCM 機能を使用していない場合、これらのエラー メッセージは表示されません。

BACC 2.7 では、リース予約に関連する次のような 3 種類のエラー メッセージが生成されます。

- 予約要求を追加できなかったことによる失敗。これらのメッセージの前に、次の情報が表示されます。この情報によって、エラーに関するいくつかの要素が特定されます。

  ```
  rdu.cisco.com: 2005 02 09 13:25:11 EST: %BPR-RDU-3-1146: PACE-13: Failed to add
  reservation [10.10.10.1] for [1,6,03:03:14:00:00:21] using client-class
  [unprovisioned-docsis] and selection-tag [NULL]; [AddReservation: FORWARD_FAILED]
  ```

- 予約要求を削除できなかったことによる失敗。これらのメッセージの前に、次の情報が表示されます。この情報によって、エラーに関するいくつかの要素が特定されます。

  ```
  rdu.cisco.com: 2005 02 09 13:25:11 EST: %BPR-RDU-3-1147: Failed to remove
  reservation [10.10.10.1] for [1,6,03:03:14:00:00:21];
  ```

- 選択基準の除外タグ エラー。これらのメッセージの前に、次の情報が表示されます。この情報によって、エラーに関するいくつかの要素が特定されます。

  ```
  rdu.cisco.com: 2005 02 09 13:25:11 EST: %BPR-RDU-4-1145: The use of
  selection-criteria exclusion tags [black] is not allowed when adding a lease
  reservation. They will be ignored.
  ```

上記の例で、表示される内容は次のとおりです。

- rdu.cisco.com：RDU FQDN を表します。
- 2005 02 09 13:25:11 EST：エラーが発生した日時を表します。
- %BPR-RDU-#-####：RDU のエラー番号（#）とエラー メッセージ ID（####）を表します。
- [10.10.10.1]：予約する IP アドレスを表します。
- [1,6,03:03:14:00:00:21]：IP アドレスの予約を試みている MAC アドレスを表します。2 番目の例は、BACC が可変長の MAC アドレスをサポートすることを示しています。

これらの各例には、エラーの一般的な説明の他、Network Registrar から返される追加のエラー メッセージが含まれます。

次の項では、BACC によって生成されるエラー メッセージについて説明します。

[OBJECT_EXISTS]

ユーザが MAC アドレス [1,6,03:03:14:00:00:21] で [11.100.14.21] を予約しようとしていますが、重複する IP を使用したため予約要求が失敗しました（IP はデータベース内の別のデバイスによってすでに予約されている）。

対応策：

別の IP アドレスを使用するか、または目的の IP アドレスを解放します。

[RemoveReservation: NOT_FOUND]

ユーザが MAC デバイス [1,1,35] で予約 [11.100.0.103] を削除しようとしていますが、CCM データベースに予約がないため要求は失敗しました。つまり、CCM はデータベースでこの予約を検出できません。

対応策：

予約が CCM データベースに存在することを確認します。

[AddReservation: INVALID_PARENT]

CCM が予約の IP アドレスに対応するスコープを検出しなかったことを意味します。ローカル CCM では、予約が含まれる可能性のあるスコープを検出する必要があります。予約された IP がスコープの範囲外にある場合、CCM によってこのエラー メッセージが表示されます。存在しないサブネットまたはスコープに予約を追加しようとすると、このエラー メッセージが表示されます。

対応策：

DHCP サーバ構成（スコープ、サブネットなど）を再確認します。

[AddReservation: INVALID_SECOND_PARENT]

このメッセージを返すのは、ローカル CCM だけです。予約が含まれる可能性のあるスコープは、設定に存在しないという意味です。DHCP サーバ構成（スコープ、サブネットなど）を再確認します。

地域別のクラスタに存在するサブネットに予約を追加しようとして、そのようなスコープまたはサブネットがローカル クラスタに存在しない場合、このエラーが表示されます。

または、予約された IP アドレスと、一致するクライアントクラス / 選択タグ基準の両方が含まれるスコープを CCM で検出できません。

対応策：

DHCP サーバ構成（スコープ、サブネット、クライアントクラス、選択タグなど）を再確認します。

[AddReservation: FORWARD_FAILED]

地域別の CCM が予約要求をローカル CCM に転送できませんでした。これは、予約された IP アドレスと、一致するクライアントクラス / 選択タグ基準の両方が含まれるスコープを CCM で検出できないときに発生します。

次の 2 つの使用例で、このエラーの潜在的な原因に対するソリューションを説明します。

事例 1：

3 つのスコープ A、B、C があり、スコープ A は赤色と灰色、スコープ B は青色と赤色、スコープ C は青色と緑色、というアトリビュートおよびタグを持つものとします。AddReservation API コールで赤色および灰色タグの包含を指定しても、要求された IP アドレスを含むスコープはスコープ B になります。

このような状況になると、予約要求が失敗し、このエラーが rdu.log ファイルに記録されます。

対応策：

同じセットアップまたは設定を使用しますが、AddReservation API コールが上で説明した赤色および灰色タグではなく、赤色タグのみの包含を指定するように修正します。この処理は正常に行われて、IP アドレスを含むスコープのうち、すべての選択タグと一致するスコープが使用されます。

(注)　この例でデバイスは、スコープ B から予約を取得することになります。

事例 2：

3 つのスコープ A、B、C があり、スコープ A は赤色、スコープ B は青色、スコープ C は緑色、というアトリビュートおよびタグを持つものとします。また、AddReservation API コールはクライアントクラス test1 を指定し、Network Registrar は緑色の選択基準を持つ test1 を定義し、要求される IP はスコープ B に含まれるものとします。

このような状況になると、予約要求が失敗し、このエラーが rdu.log ファイルに記録されます。

対応策：

同じセットアップまたは設定を使用しますが、test1 クライアントクラスを青色の選択基準で Network Registrar に設定し直します。これによって、IP アドレスを含むスコープのうち、すべての選択タグと一致するスコープが使用されるように、問題が是正されます。

[AddReservation: AX_ETIME]

予約要求のタイムアウトが発生したことを示します。これは CCM が過負荷状態、またはタスクと要求でビジー状態になっていて、予約要求を処理できなかったことにより、発生した可能性があります。

対応策：

管理者のユーザ インターフェイスを使用して、より長いタイムアウト値を設定します。予約要求の発行については、P.10-20 の「RDU Defaults」を参照してください。

[AddReservation: INVALID_OBJECT]

MAC アドレスが無効、IP アドレスが見つからない、無効なクライアントクラス名か選択タグが指定されたなどの理由で、予約自体が無効でした。

対応策：

予約要求の MAC アドレス、IP アドレス、クライアントクラス、選択タグなどを確認します。

Selection-criteria exclusion tags will be ignored

リース予約の追加時に、選択基準の除外タグ [black] は使用できません。除外タグは無視されます。

対応策：

選択基準の除外タグは使用できないため、DHCP 基準に選択基準の除外タグを設定しないでください。

[AX_EIO]

これは、RDU と CCM 間の接続またはセッションが切断されていることを示します。

対応策：

このエラーが発生した場合、ユーザが対応する必要はありません。RDU によって自動的に CCM への別の接続が確立されます。

[AX_EPIPE]

これは、RDU と CCM 間の接続またはセッションが切断されていることを示します。

対応策：

このエラーが発生した場合、ユーザが対応する必要はありません。RDU によって自動的に CCM への別の接続が確立されます。

APPENDIX B

PacketCable DHCP オプションと BACC プロパティのマッピング

この付録では、PacketCable のプロビジョニングで使用される PacketCable DHCP オプションと BACC プロパティのマッピングについて示します。

これらのプロパティの必要最小限のセットは、インストール中に <BACC_HOME>/cnr_ep/conf/cnr_ep.properties ファイルに設定されます。このファイルは Network Registrar のホスト上にあります。cnr_ep.properties で定義されたプロパティのセットは、プロビジョニング グループ内のすべての PacketCable 音声技術デバイスに適用されます。他の BACC プロパティと同じように、これらのプロパティもデバイスや CoS（サービス クラス）に設定できます。管理者のユーザ インターフェイスか API のいずれかを使用して、プロパティを RDU に設定すると、cnr_ep.properties ファイルの対応する設定値が上書きされます。

(注) これらのキー設定プロパティの変更については、P.12-45 の「changeNRProperties.sh ツールの使用」を参照してください。

BACC では PacketCable DHCP オプション 122（RFC 3495 および 3594 で規定）と推奨されない PacketCable DHCP オプション 177 をどちらもサポートします。BACC は、オプション 122 および 177 の一方または両方のコンテンツを読み込めなくても、DHCP 要求を無視しません。オプション 122 および 177 のコンテンツが使用可能であれば読み込み、オプションを無視するかどうかの判断は eMTA に委ねられます。

オプション 122 と 177 の両方を要求する DHCP 要求を BACC が受信したときは、オプション 177 の要求を無視し、オプション 122 のコンテンツだけを読み込みます。

注意 <BACC_HOME>/cnr_ep/conf/cnr_ep.properties のプロパティには、それぞれインスタンスが 1 つずつしかありません。

オプション 122 と BACC プロパティの比較

表 B-1 は RFC-3495 および RFC-3594 のオプション 122 の定義に適用される BACC プロパティを示します。

表 B-1　DHCP オプション 122 と BACC プロパティの比較

DHCP オプション	タイプ	BACC プロパティ名
6	IP addr	/ccc/dns/primary
6	IP addr	/ccc/dns/secondary
122.1	IP addr	/ccc/dhcp/primary
122.2	IP addr	/ccc/dhcp/secondary
122.3	FQDN	/ccc/prov/fqdn **（注）** オプション 122.3 は、BACC によって自動的に設定されるので、このプロパティは手動では設定しないでください。
122.4	Integer	/ccc/kerb/auth/backoff/nomTimeout /ccc/kerb/auth/backoff/maxTimeout /ccc/kerb/auth/backoff/maxRetries
122.5	Integer	/ccc/kerb/app/backoff/nomTimeout /ccc/kerb/app/backoff/maxTimeout /ccc/kerb/app/backoff/maxRetries
122.6	String	/ccc/kerb/realm
122.7	Boolean	/ccc/tgt
122.8	Integer	/ccc/prov/timer
122.9	Integer	/ccc/security/ticket/invalidation

注意　/ccc/kerb/auth/backoff/nomTimeout、/ccc/kerb/auth/backoff/maxTimeout、または /ccc/kerb/auth/backoff/maxRetries が 1 つでも定義されている場合、この 3 つがすべて定義される必要があります。同様に、/ccc/kerb/app/backoff/nomTimeout、/ccc/kerb/app/backoff/maxTimeout、または /ccc/kerb/app/backoff/maxRetries が 1 つでも定義されている場合は、この 3 つすべてが定義される必要があります。

オプション 177 と BACC プロパティの比較

PacketCable Compliance Wave 26 では、オプション 177 は推奨されておらず、オプション 122 が優先する MTA プロビジョニング オプションになっています。現在も オプション 177 をサポートしている従来のデバイスのために、オプション 177 の定義に適用される BACC プロパティを表 B-2 に示します。

表 B-2　DHCP オプション 177 と BACC プロパティの比較

オプション 177	タイプ	BACC プロパティ名
177.1	ip addr	/pktcbl/dhcp/primary
177.2	ip addr	/pktcbl/dhcp/secondary
177.3	fqdn	/pktcbl/snmp/entity/fqdn
177.4	ip addr	/pktcbl/dns/primary
177.5	ip addr	/pktcbl/dns/secondary
177.6	string	/pktcbl/snmp/realm
177.7	boolean	/pktcbl/snmp/tgt
177.8	integer	/pktcbl/provisioning/timer
177.10	integer	/pktcbl/kerberos/authentication/backoff/nomTimeout /pktcbl/kerberos/authentication/backoff/maxTimeout /pktcbl/kerberos/authentication/backoff/maxRetries
177.11	integer	/pktcbl/kerberos/application/backoff/nomTimeout /pktcbl/kerberos/application/backoff/maxTimeout /pktcbl/kerberos/application/backoff/maxRetries
177.12	integer	/pktcbl/snmp/kerberos/ticket/invalidation

オプション 177 と BACC プロパティの比較

APPENDIX C

Broadband Access Center for Cable のアプリケーション プログラミング インターフェイスの使用例

この付録では、プロビジョニング API の最も一般的な使用例を列挙します。この使用例には、サービス プロバイダーの一般的なワークフローをモデル化するときに使用できる擬似コード セグメントなどがあります。使用例で使われている擬似コードは java に似ていますが、直接コンパイルできるようにはなっていません。詳細や、個々の API コールと機能を説明するサンプルの Java コード セグメントについては、BACC 2.7 API Javadoc を参照してください。

次の使用例は、デバイス（およびサービス）のプロビジョニングに直接関連しています。サービス クラス、DHCP 基準、およびライセンスの管理など、多くの管理操作についてはここでは取り上げません。関連する API コールの詳細については、API javadoc を参照することを強くお勧めします。また、管理者のユーザ インターフェイスを使用して、これらのアクティビティのほとんどを実行することもできます。

使用例

この付録には、次の使用例が含まれています。

- 固定標準モードでのセルフプロビジョニングされたモデムとコンピュータ（P.C-3）
- 固定標準モードでの新しいコンピュータの追加（P.C-6）
- 加入者のディセーブル化（P.C-8）
- モデムおよびセルフプロビジョニングされたコンピュータの事前プロビジョニング（P.C-10）
- 既存のモデムの修正（P.C-12）
- 加入者のデバイスの登録解除と削除（P.C-13）
- 無差別モードでの最初のアクティベーションのセルフプロビジョニング（P.C-16）
- 無差別モードでの 100 個のモデムの一括プロビジョニング（P.C-19）
- 無差別モードでの最初のアクティベーションの事前プロビジョニング（P.C-21）
- 既存のモデムの交換（P.C-24）
- 無差別モードでの 2 台目のコンピュータの追加（P.C-25）
- NAT を使用した最初のアクティベーションのセルフプロビジョニング（P.C-26）
- NAT を持つモデムの背後への新しいコンピュータの追加（P.C-29）
- 別の DHCP スコープへのデバイスの移動（P.C-30）
- イベントを使用したデバイス削除のロギング（P.C-31）
- イベントを使用した RDU 接続の監視（P.C-32）
- イベントを使用したバッチ完了のロギング（P.C-33）
- デバイスの詳細情報の取得（P.C-34）
- デフォルトのサービス クラスを使用した検索（P.C-35）
- ベンダープレフィックスに一致するデバイスの取得（P.C-37）
- PacketCable eMTA の事前プロビジョニング（P.C-39）
- PacketCable eMTA 上での SNMP クローン作成（P.C-41）
- PacketCable eMTA の差分プロビジョニング（P.C-43）
- 動的設定ファイルを使用した DOCSIS モデムの事前プロビジョニング（P.C-45）
- オプティミスティック ロッキング（P.C-46）
- 加入者の帯域幅の一時的なスロットリング（P.C-48）
- CableHome WAN-Man の事前プロビジョニング（P.C-49）
- ファイアウォール設定を持つ CableHome（P.C-51）
- CableHome WAN-Man のデバイス機能の取得（P.C-53）
- CableHome WAN-Man のセルフプロビジョニング（P.C-55）
- リース予約の使用例（P.C-58）

固定標準モードでのセルフプロビジョニングされたモデムとコンピュータ

加入者は、建物内にコンピュータを設置し、DOCSIS ケーブル モデムを購入しています。コンピュータには Web ブラウザがインストールされています。

求める結果

次のワークフローを使用して、プロビジョニングされていない新しい DOCSIS ケーブル モデムとコンピュータをオンラインにし、適切なレベルのサービスを受けられるようにします。

ステップ 1　加入者が DOCSIS ケーブル モデムを購入して建物内に設置し、コンピュータをケーブル モデムに接続します。

ステップ 2　加入者がモデムとコンピュータの電源をオンにし、BACC が制限付きアクセス権をモデムに与えます。コンピュータとモデムには、制限付きアクセス プールから IP アドレスが割り当てられます。

ステップ 3　加入者が Web ブラウザを起動します。スプーフィング DNS サーバにより、Web ブラウザがサービス プロバイダーの登録サーバ（OSS ユーザ インターフェイスやメディエータなど）にアクセスします。

ステップ 4　加入者がサービス プロバイダーのユーザ インターフェイスを使用して、サービス クラスの選択など、登録に必要な手順を完了します。

ステップ 5　サービス プロバイダーのユーザ インターフェイスが、加入者の情報（選択されたサービス クラスやコンピュータの IP アドレスなど）を BACC に渡します。次に、BACC が加入者のモデムとコンピュータを登録します。

```
// First we query the computer's information to find the modem's
// MAC address. We use the computers IP address (the web browser
// received this when the subscriber opened the service providers
// web interface)

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// NO_ACTIVATION is the activation mode because this is a query
// NO_CONFIRMATION is the confirmation mode because we are not
// attempting to reset the device

LeaseResults computerLease =

        getAllForIPAddress("10.0.14.38");
        // ipAddress: restricted access.


// Derive the modem MAC address from the computer's network
// information. The 1,6, is a standard prefix for an Ethernet
// device. The fully qualified MAC address is required by BACC

String modemMACAddress = "1,6," +
        computerLease.getSingleLease().get(RELAY_AGENT_REMOTE_ID);
```

```
// Now let's provision the modem and the computer in the same
// batch. This can be done because the activation mode of this
// batch is NO_ACTIVATION. More than one device can be operated
// on in a batch if the activation mode does not lead to more
// than one device being reset. NO_ACTIVATION will generate a
// configuration for the devices. However it will not attempt
// to reset the devices. The configuration can be generated
// because the devices have booted. NO_CONFIRMATION is the
// confirmation mode because we are not attempting to reset
// the modem. We do not want to reset the modem here because
// we want to notify the user to reset their computer. If we
// reset the modem in this batch, we will not be able to notify
// the user of anything until the modem has come back online.
// To add a DOCSIS modem:

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

add(
        DeviceType: DOCSIS,
                // deviceType: DOCSIS
        modemMACaddress,
                // macAddress: derived from computer lease
        null,
                // hostName: not used in this example
        null,
                // domainName: not used in this example
        "0123-45-6789",
                // ownerID: here, account number from billing system
        "Silver",
                // ClassOfService
        "provisionedCM",
                // DHCP Criteria: Network Registrar uses this to
                // select a modem lease granting provisioned IP address
        null
                // properties: not used
        );
                // properties: not used
String computerMACAddress = computerLease.
        getSingleLease().get(DeviceDetailsKeys.MAC_ADDRESS);

// Create a Map for the computer's properties

Map properties;

// Setting the property IPDeviceKeys.MUST_BE_BEHIND_DEVICE
// on the computer ensures that when the computer boots it
// will only receive its provisioned access when it is behind
// the given device. If it is not behind the given device,
// it will receive default access (unprovisioned). This makes
// the computer "fixed" behind the specified modem.

properties.put(IPDeviceKeys.MUST_BE_BEHIND_DEVICE,
                modemMACaddress);

add(
        DeviceType.COMPUTER,
                // deviceType: COMPUTER
```

```
        computerMACAddress,
                // macAddress: derived from computer lease
        null,
                // hostName: not used in this example
        null,
                // domainName: not used in this example
        "0123-45-6789",
                // ownerID: here, account number from billing system
        null,
                // classOfService : get the default COS
        "provisionedCPE",
                // DHCP Criteria: Network Registrar uses this to
                // select a modem lease granting provisioned IP address
        properties
                // properties:
        );
```

ステップ 6　ユーザ インターフェイスにより、加入者はコンピュータをリブートするように求められます。

ステップ 7　プロビジョニング　クライアントが　*performOperation(DeviceOperation.RESET,　modemMACaddress, null)* を呼び出してモデムをリブートし、プロビジョニングされたアクセス権をモデムに与えます。

```
get-new-batch(AUTOMATIC, NO_CONFIRMATION);

// AUTOMATIC is the activation mode because we are attempting
// to reset the modem so that it receives its new class of service.
// NO_CONFIRMATION is the confirmation mode because we don't
// want the batch to fail if we can't reset the modem. The user
// may have power cycled the modem when they rebooted their computer.
// Send a batch to reset the modem now that the user has been
// notified to reboot their computer.

performOperation(
        DeviceOperation.RESET,
                //deviceOperation: Reset operation
        modemMACaddress,
                // macAddress:Modem's MAC address
        null
                // properties: not used
        );
```

ステップ 8　リブート後、コンピュータが新しい IP アドレスを受信します。これで、ケーブル　モデムとコンピュータの両方が、プロビジョニングされたデバイスとなります。コンピュータは、サービス プロバイダーのネットワークを介してインターネットにアクセスできます。

固定標準モードでの新しいコンピュータの追加

Multiple Service Operator（MSO; マルチプル サービス オペレータ）が、加入者に対し、ケーブル モデムの背後に 2 台のコンピュータを接続することを許可しています。加入者は 1 台のコンピュータをすでに登録しています。今回は、職場からラップトップ コンピュータを持ち帰ってアクセスします。加入者がハブを設置し、ラップトップをハブに接続します。

求める結果

次のワークフローを使用して、プロビジョニングされていない新しいコンピュータを、すでにプロビジョニングされているケーブル モデムでオンラインにし、新しいコンピュータが適切なレベルのサービスを受けられるようにします。

ステップ 1　加入者が新しいコンピュータの電源をオンにし、BACC が制限付きアクセス権をコンピュータに与えます。

ステップ 2　加入者が新しいコンピュータの Web ブラウザを起動します。スプーフィング DNS サーバにより、Web ブラウザがサービス プロバイダーの登録サーバ（OSS ユーザ インターフェイスやメディエータなど）にアクセスします。

ステップ 3　加入者がサービス プロバイダーのユーザ インターフェイスを使用して、新しいコンピュータの追加に必要な手順を完了します。

ステップ 4　サービス プロバイダーのユーザ インターフェイスが、加入者の情報（選択されたサービス クラスやコンピュータの IP アドレスなど）を BACC に渡します。次に、BACC が加入者のモデムとコンピュータを登録します。

```
// First we query the computer's lease information to its
// MAC address. We use the computers IP address (the web browser
// received this when the subscriber opened the service providers
// web interface)

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

/ NO_ACTIVATION is the activation mode because this is a query
// NO_CONFIRMATION is the confirmation mode because we are not
// attempting to reset the device.

LeaseResults computerLease =
       getAllForIPAddress("10.0.14.39");
       // ipAddress: restricted access.

String computerMACAddress = computerLease.
       getSingleLease().get(DeviceDetailsKeys.MAC_ADDRESS);
```

```
// We have the MAC address now. Let's add the computer to BACC.

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// NO_ACTIVATION will generate a configuration for the computer.
// However it will not attempt to reset the computer (this
// can not be done). The configuration can be generated because
// the device has booted. NO_CONFIRMATION is the confirmation
// mode because we are not attempting to reset the modem.

Map properties; // Map containing the properties for the computer

// Setting the property IPDeviceKeys.MUST_BE_BEHIND_DEVICE on
// the computer ensures that when the computer boots, it will
// only receive its provisioned access when it is behind the
// given device. If it is not behind the given device, it
// will receive default access (unprovisioned) and hence the
// fixed mode.

properties.put(IPDeviceKeys.MUST_BE_BEHIND_DEVICE, modemMACaddress);

// The IPDeviceKeys.MUST_BE_IN_PROV_GROUP property ensures that
// the computer will receive its provisioned access only when
// it's brought up in the specified provisioning group. This prevents
// the computer (and/or the modem) from moving from one locality to
// to another locality.

properties.put(IPDeviceKeys.MUST_BE_IN_PROV_GROUP, "bostonProvGroup");

add(
        DeviceType.COMPUTER,
                // deviceType: COMPUTER
        computerMACAddress,
                // macAddress: derived from computer lease
        null,
                // hostName: not used in this example
        null,
                // domainName: not used in this example
        "0123-45-6789",
                // ownerID: here, account number from billing system
        null,
                // classOfService: get the default COS
        "provisionedCPE",
                // DHCP Criteria: Network Registrar uses this to
                // select a modem lease granting provisioned IP address
        properties
                // properties:
        );
```

ステップ 5　ユーザ　インターフェイスにより、加入者は新しいコンピュータをリブートするように求められます。リブートすると、BACC が登録済みのサービス レベルをコンピュータに与えます。

ステップ 6　これで、コンピュータはプロビジョニングされたデバイスとなり、適切なレベルのサービスにアクセスできます。

加入者のディセーブル化

加入者が滞納を繰り返したという理由により、サービス プロバイダーが加入者のインターネット アクセスをディセーブルにします。

求める結果

次のワークフローを使用して、動作中のケーブル モデムとコンピュータをディセーブルにします。この結果、デバイスがユーザのインターネット アクセスを一時的に制限します。また、この使用例では、ユーザのブラウザを特別なページにリダイレクトして、次のようなメッセージを通知することも可能です。

```
You haven't paid your bill so your Internet access has been disabled.
```

ステップ 1　サービス プロバイダーのアプリケーションが、プロビジョニング クライアント プログラムを使用して、加入者のデバイスすべてのリストを BACC に要求します。次に、サービス プロバイダーのアプリケーションが、プロビジョニング クライアントを使用して、加入者のデバイスを個別にディセーブルにするか、または制限します。

```
// The service provider's application uses a provisioning client
// to get a list of all of the subscriber's devices.

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// NO_ACTIVATION is the activation mode because this is a query.
// NO_CONFIRMATION is the confirmation mode because we are not
// attempting to reset the devices.

getAllForOwnerID(

"0123-45-6789"); // Query all the devices for this account number
// For each device in the retrieved list:


// We are only interested in the modems. If we disable network
// access of the modems, we disable network access for all the

// subscriber's devices. If we are using roaming standard mode,
// we may also change the computer's network access (DHCPCriteria)
// because the subscriber may still be able to access the network
// from a different modem.

DeviceLoop:
{
        if (Device.deviceType == DOCSIS_MODEM)
        {
                get-new-batch(AUTOMATIC, NO_CONFIRMATION)

                // AUTOMATIC is the activation mode because we are
                // attempting to reset the modem so that becomes
                // disabled. NO_CONFIRMATION is the confirmation mode
                // because we do not want the batch to fail if we cannot
                // reset the modem. If the modem is off, it will
                // be disabled when it is turned back on.

                // Let's change the COS of the device so that it will restrict
                // the bandwidth usage of the modem.

                changeClassOfService(

                        Device.MAC_ADDRESS,

                                // macAddress: unique identifier for this modem
```

```
        "DisabledCOS");
                // newClassOfService: restricts bandwidth usage

// Let's change the DHCP Crtieria so that the modem will get an IP
// address from a disabled CNR scope. This scope also points to
// a spoofing DNS server so that the subscriber gets a restricted
// access page.

changeDHCPCriteria(
        Device.MAC_ADDRESS,
                // macAddress: unique identifier for this modem
        "DisabledDHCPCriteria");
                // newDHCPCriteria: disables Internet access
        }
}
// end DeviceLoop
```

(注) DisabledCOS の特性を定義し、モデムをリセットするときは、モデムの背後の CPE に及ぼす影響の考慮が必要となる場合があります。このことは、モデムの背後に音声エンドポイントが接続されている場合に特に重要です。これは、ケーブル モデムの動作を中断すると、その時点で進行中の電話会話に影響を及ぼす可能性があるためです。

これで、加入者がディセーブルになります。

モデムおよびセルフプロビジョニングされたコンピュータの事前プロビジョニング

新しい加入者がサービス プロバイダーに連絡し、サービスを要求します。加入者は、建物内にコンピュータを設置しています。サービス プロバイダーが、すべてのケーブル モデムをまとめて事前プロビジョニングします。

求める結果

次のワークフローを使用して、事前プロビジョニングされたケーブル モデムとプロビジョニングされいないコンピュータを、ローミング標準モードでオンラインにします。この作業は、両方のデバイスが適切なレベルのサービスを受けられ、登録されるようにするために必要です。

ステップ 1　サービス プロバイダーが、課金システムで使用する加入者のユーザ名とパスワードを選択します。

ステップ 2　サービス プロバイダーが、加入者にアクセスを許可するサービスを選択します。

ステップ 3　サービス プロバイダーの現場技術者が、新しい加入者の建物内に物理ケーブルを敷設し、事前プロビジョニングされたデバイスを設置して、加入者のコンピュータに接続します。

ステップ 4　技術者がモデムの電源をオンにし、BACC がプロビジョニングされた IP アドレスをモデムに与えます。

ステップ 5　技術者がコンピュータの電源をオンにし、BACC がプライベート IP アドレスをコンピュータに与えます。

ステップ 6　技術者がコンピュータのブラウザ アプリケーションを起動し、ブラウザがサービス プロバイダーのユーザ インターフェイスにアクセスします。

ステップ 7　技術者がサービス プロバイダーのユーザ インターフェイスにアクセスし、プロビジョニングされたケーブル モデムの背後にあるコンピュータの登録に必要な手順を完了します。

```
// To provision a computer:
// First we query the computer's lease information to its
// MAC address. We use the computers IP address (the web browser
// received this when the subscriber opened the service provider's
// web interface)

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// NO_ACTIVATION is the activation mode because this is a query
// NO_CONFIRMATION is the confirmation mode because we are not
// attempting to reset the device

LeaseResults computerLease =
       getAllForIPAddress("10.0.14.38");
       // ipAddress:
String computerMACAddress = computerLease.
       getSingleLease().get(DeviceDetailsKeys.MAC_ADDRESS);
```

```
// MSO admin UI calls the provisioning API to provision a computer.

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// NO_ACTIVATION will generate a new configuration for the computer
// however it will not attempt to reset it.
// NO_CONFIRMATION is the confirmation mode because we are not
// attempting to reset the computer because this cannot be done.

add(
        DeviceType.COMPUTER,
                // deviceType: Computer
        computerMACAddress,
                // macAddress: derived from computer lease
        null,
                // hostName: not used in this example
        null,
                // domainName: not used in this example
        "0123-45-6789",
                // ownerID: here, account number from billing system
        null,
                // ClassOfService : get the default COS
        "provisionedCPE",
                // DHCP Criteria: Network Registrar uses this to
                // select a modem lease granting provisioned IP address
        null
                // properties: not used
);
```

(注) IPDeviceKeys.MUST_BE_BEHIND_DEVICE プロパティはコンピュータに設定されませんが、このプロパティを使用すると、ケーブル モデムの背後から別のケーブル モデムへのローミングが可能になります。

ステップ 8　技術者がコンピュータを再起動し、コンピュータがプロビジョニングされた新しい IP アドレスを受信します。これで、ケーブル モデムとコンピュータはいずれもプロビジョニングされたデバイスとなります。コンピュータは、サービス プロバイダーのネットワークを介してインターネットにアクセスできます。

既存のモデムの修正

サービス プロバイダーの加入者が、現在 **Silver** というレベルのサービスを受けていますが、**Gold** サービスにアップグレードすることにしました。加入者は、建物内にコンピュータを設置しています。

(注) この使用例は、デバイスの修正方法を示すことを目的としています。この例は、ローミング標準以外のモードでプロビジョニングされたデバイスに適用可能です。

求める結果

次のワークフローを使用して、既存のモデムのサービス クラスを修正し、そのサービスの変更をサービス プロバイダーの外部システムに渡します。

ステップ 1　加入者がサービス プロバイダーに電話をかけて、サービスのアップグレードを依頼します。サービス プロバイダーはユーザ インターフェイスを使用して、サービス クラスを **Silver** から **Gold** に変更します。

ステップ 2　サービス プロバイダーのアプリケーションが、BACC で次の API コールを行います。

```
get-new-batch(AUTOMATIC, NO_CONFIRMATION)

// AUTOMATIC will generate a configuration for the device
// and will attempt to reset the device
// The configuration will be able to be generated because
// the device has booted. NO_CONFIRMATION is the confirmation
// mode because we don't want the batch to fail if the reset failed.
// This use case is a perfect example of the different
// confirmation modes that could be used instead of
// NO_CONFIRMATION. These confirmation modes give you
// a method to test whether a configuration was taken by
// a device. Also, these modes will take more time because
// the batch has to wait for the modem to reset.

changeClassOfService(
        "1,6,00:11:22:33:44:55",
                // macAddress: unique identifier for this modem
        "Gold"
                // newClassOfService
);
```

ステップ 3　これで、加入者がサービス プロバイダーのネットワークにアクセスし、*Gold* サービスを受けられるようになります。

加入者のデバイスの登録解除と削除

サービス プロバイダーが、サービスの利用を中止した加入者を削除します。

求める結果

次のワークフローを使用して、加入者のデバイスすべてをサービス プロバイダーのネットワークから完全に削除します。

ステップ 1　サービス プロバイダーのユーザ インターフェイスが、加入者へのサービスを停止します。

ステップ 2　サービス プロバイダーのアプリケーションが、プロビジョニング クライアント プログラムを使用して、加入者のデバイスすべてのリストを BACC に要求します。次に、各デバイスを登録解除してリセットします。その結果、各デバイスがデフォルトの（プロビジョニングされていない）サービス レベルに低下します。

(注)　「unregister」API へのパラメータに指定されたデバイスがすでに登録解除された状態にある場合は、API コールからのステータス コードが CommandStatusCodes .CMD_ERROR_DEVICE_UNREGISTER_UNREGISTERED_ERROR に設定されます。これは、通常および所定の動作です。

```
// MSO admin UI calls the provisioning API to get a list of
// all the subscriber's devices.

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// NO_ACTIVATION is the activation mode because this is a query.
// NO_CONFIRMATION is the confirmation mode because we are
// not attempting to reset the devices.

getAllForOwnerID(
        "0123-45-6789");
        // query all the devices for this account number

// We need to unregister all the devices behind each modem(s) or else the
// unregister call for that modem will fail.

// for each computer in the retrieved list:
DeviceLoop:
{

        if (Device.deviceType == COMPUTER)
        {
                get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

                // NO_ACTIVATION is the activation mode because we can't
                // to reset Computers.
                // NO_CONFIRMATION is the confirmation mode because
                // the unregister call will not reset the devices.

                unregister(
                        Device.MAC_ADDRESS,
                        // macAddress: unique identifier for this device
                );

        }
```

```
}

// for each modem in the retrieved list:
DeviceLoop:
{

        if (Device.deviceType == DOCSIS_MODEM)
        {
                get-new-batch(AUTOMATIC, NO_CONFIRMATION)

                // AUTOMATIC is the activation mode because we want
                // to reset as we unregister the device.

                unregister(
                        Device.MAC_ADDRESS,
                        // macAddress: unique identifier for this device
                );
        }
}

// end DeviceLoop.
```

(注) サービス プロバイダーによっては、故障の場合を除いてケーブル モデムをデータベースに残す場合があるため、次のステップはオプションです。次のステップが必要になるのは、デバイスをデータベースから削除する場合のみです。

ステップ 3　サービス プロバイダーのアプリケーションが、プロビジョニング クライアント プログラムを使用して、加入者の残りのデバイスをデータベースから個別に削除します。

```
// MSO admin UI calls the provisioning API to get a list of
// all the subscriber's devices.

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// NO_ACTIVATION is the activation mode because this is a query.
// NO_CONFIRMATION is the confirmation mode because we are
// not attempting to reset the devices.

getAllForOwnerID(
        "0123-45-6789");
        // query all the devices for this account number
// for each device in the retrieved list:

DeviceLoop:
{
        // get a new batch for each modem being deleted

        if (Device.deviceType == DOCSIS_MODEM)
        {
                get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

                // NO_ACTIVATION is the activation mode because we don't want
                // to reset as we are deleting the device.
                // NO_CONFIRMATION is the confirmation mode because
                // the delete call will not reset the devices.

                delete(
                        Device.MAC_ADDRESS,
                        // macAddress: unique identifier for this device
                        true
                        // deleteDevicesBehind: deletes CPEs behind this modem.
                );

        }
}
//end DeviceLoop.
```

無差別モードでの最初のアクティベーションのセルフプロビジョニング

加入者が、建物内にコンピュータ（ブラウザ アプリケーションを持つ）を設置し、DOCSIS ケーブル モデムを購入しています。

求める結果

次のワークフローを使用して、プロビジョニングされていない新しい DOCSIS ケーブル モデムとコンピュータをオンラインにし、適切なレベルのサービスを受けられるようにします。

ステップ 1　加入者が DOCSIS ケーブル モデムを購入し、建物内に設置します。

ステップ 2　加入者がモデムの電源をオンにし、BACC が制限付きアクセス権をモデムに与えます。

ステップ 3　加入者がコンピュータのブラウザ アプリケーションを起動します。スプーフィング DNS サーバにより、ブラウザがサービス プロバイダーの登録サーバ（OSS ユーザ インターフェイスやメディエータなど）にアクセスします。

ステップ 4　加入者がサービス プロバイダーのユーザ インターフェイスを使用して、サービス クラスの選択など、登録に必要な手順を完了します。

サービス プロバイダーのユーザ インターフェイスが、加入者の情報（選択されたサービス クラスやコンピュータの IP アドレスなど）を BACC に渡します。次に、加入者のケーブル モデムとコンピュータが BACC に登録されます。

```
get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// NO_ACTIVATION is the activation mode because this is a
// query. NO_CONFIRMATION is the confirmation mode because
// we are not attempting to reset the device.
// First we query the computer's information to find the
// modems MAC address.
// We use the computer’s IP address (the web browser
// received this when the subscriber opened the service
// provider’s web interface). We also assume that “bostonProvGroup”
// is the provisioning group  used in that locality.

List provGroupList;
provGroupList = provGroupList.add(“bostonProvGroup”);
Map computerLease = getAllForIPAddress(
        "10.0.14.38",
        // ipAddress: restricted access computer lease
        provGroupList
        // provGroups: List containing provgroup)

// Derive the modem MAC address from the computer's network

// information.The 1,6, is a standard prefix for an Ethernet

// device.The fully qualified MAC address is required by BACC


String modemMACAddress = "1,6," +
        computerLease.GetSingleLease().get(RELAY_AGENT_REMOTE_ID);
```

```
get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// Now let's provision the modem
// NO_ACTIVATION will generate a configuration for the
// modem, however it will not attempt to reset it
// The configuration will be able to be generated because
// the modem has booted.
// NO_CONFIRMATION is the confirmation mode because we
// are not attempting to reset the modem
// Create a Map for the properties of the modem

Map properties;
// Set the property ModemKeys.PROMISCUOUS_MODE_ENABLED
// to enable promiscuous mode on modem

properties.put(ModemKeys.PROMISCUOUS_MODE_ENABLED, "enabled");

properties.put(ModemKeys.CPE_DHCP_CRITERIA, "provisionedCPE");

add(
        DeviceType.DOCSIS,
                // deviceType: DOCSIS
        modemMACaddress,
                // macAddress: derived from computer lease
        null,
                // hostName: not used in this example
        null,
                // domainName: not used in this example
        "0123-45-6789",
                // ownerID: here, account number from billing system
        "Silver",
                // ClassOfService
        "provisionedCM",
                // DHCP Criteria: Network Registrar uses this to
                // select a modem lease granting provisioned IP address
        properties
                // properties:
);
```

ステップ 5　ユーザ インターフェイスにより、加入者はコンピュータをリブートするように求められます。

ステップ 6　プロビジョニング クライアントが *performOperation(…)* を呼び出してモデムをリブートし、プロビジョニングされたアクセス権をモデムに与えます。

```
get-new-batch(AUTOMATIC, NO_CONFIRMATION)

// AUTOMATIC is the activation mode because we are attempting
// to reset the modem so that it receives the new class of service.
// NO_CONFIRMATION is the confirmation mode because we don't want
// the batch to fail if we can't reset the modem. The user might
// have power cycled the modem when they rebooted their computer

// send a batch to reset the modem now that the user has been
// notified to reboot their computer

performOperation(
        DeviceOperation.RESET,
                //deviceOperation: Reset operation
        modemMACaddress,
                // macAddress:Modem's MAC address
        null
                // properties : not used
        );
```

ステップ 7　コンピュータをリブートすると、コンピュータが新しい IP アドレスを受信します。これで、ケーブル モデムがプロビジョニングされたデバイスとなります。コンピュータは BACC に登録されていませんが、サービス プロバイダーのネットワークを介してインターネットにアクセスできます。無差別モードのモデムの背後でオンラインになっているコンピュータは、引き続き、プロビジョニング API を使用して利用することができます。

無差別モードでの 100 個のモデムの一括プロビジョニング

サービス プロバイダーにおいて、サービスセンターのカスタマー サービス担当者が、配送する 100 個のケーブル モデムを事前プロビジョニングします。

求める結果

次のワークフローを使用して、すべてのモデムのモデム データを新しい加入者に割り当てます。カスタマー サービス担当者は、割り当て可能なモデムのリストを持っています。

ステップ 1　サービス プロバイダーの発送センターで、新しいケーブル モデムまたは再利用するケーブル モデムの MAC アドレス データがリストにまとめられます。

ステップ 2　特定のサービスセンターに割り当てられたモデムが BACC に一括ロードされ、そのサービスセンターの識別名が付けられます。

ステップ 3　サービスセンターでモデムを新しい加入者に割り当てる際、カスタマー　サービス担当者が新しいサービス パラメータを入力し、モデムの Owner ID フィールドを新しい加入者のアカウント番号に合せて変更します。

```
// get a single batch for bulk load or 100 modems

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)
// The activation mode for this batch should be NO_ACTIVATION.
// NO_ACTIVATION should be used in this situation because no
// network information exists for the devices because they
// have not booted yet. A configuration can't be generated if no
// network information is present. And because the devices
// have not booted, they are not online and therefore cannot
// be reset. NO_CONFIRMATION is the confirmation mode because
// we are not attempting to reset the devices.
// Create a Map for the properties of the modem


Map properties;

// Set the property ModemKeys.PROMISCUOUS_MODE_ENABLED to
// enable promiscuous mode on modem.
// This could be done at a system level if promiscuous mode
// is your default provisioning mode.
properties.put(ModemKeys.PROMISCUOUS_MODE_ENABLED, "enabled")

// The ModemKeys.CPE_DHCP_CRITERIA is used to specify the DHCP
// Criteria to be used while selecting IP address scopes for
// CPEs behind this modem in the promiscuous mode.

properties.put(ModemKeys.CPE_DHCP_CRITERIA, "provisionedCPE");

// for each modem MAC-address in list:

ModemLoop:
{
        add(
                DeviceType.DOCSIS,
                        // deviceType: DOCSIS
                modemMACaddress,
                        // macAddress: derived from computer lease
                null,
                        // hostName: not used in this example
                 null,
                        // domainName: not used in this example
                "0123-45-6789",
                        // ownerID: here, account number from billing system
                 "Silver",
                        // ClassOfService
                "provisionedCM",
                        // DHCP Criteria: Network Registrar uses this to
                        // select a modem lease granting provisioned IP address
                 properties
                         // properties:
        );
)
//end ModemLoop.
```

無差別モードでの最初のアクティベーションの事前プロビジョニング

新しい加入者がサービス プロバイダーに連絡し、サービスを要求します。加入者は、建物内にコンピュータを設置しています。

求める結果

次のワークフローを使用して、プロビジョニングされていない新しいケーブル モデムとコンピュータをオンラインにし、適切なレベルのサービスを受けられるようにします。

ステップ 1　サービス プロバイダーが、課金システムで使用する加入者のユーザ名とパスワードを選択します。

ステップ 2　サービス プロバイダーが、加入者にアクセスを許可するサービスを選択します。

ステップ 3　サービス プロバイダーが、独自のユーザ インターフェイスを使用して、デバイスを登録します。

ステップ 4　サービス プロバイダーのユーザ インターフェイスが、モデムの MAC アドレスやサービス クラスなどの情報を BACC に渡します。また、モデムが CPE DHCP 基準設定を取得します。この基準設定により、Network Registrar はモデムの背後に接続するコンピュータに対して、プロビジョニングされたアドレスを選択できます。次に、新しいモデムが BACC に登録されます。

ステップ 5　サービス プロバイダーの現場技術者が、新しい加入者の建物内に物理ケーブルを敷設し、事前プロビジョニングされたデバイスを設置して、加入者のコンピュータに接続します。

// MSO admin UI calls the provisioning API to pre-provision

// an HSD modem.

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// The activation mode for this batch should be NO_ACTIVATION.

// NO_ACTIVATION should be used in this situation because no

// network information exists for the modem because it has not

// booted.A configuration cannot be generated if no network

// information is present.And because the modem has not booted,

// it is not online and therefore cannot be reset.

// NO_CONFIRMATION is the confirmation mode because we are not

// attempting to reset the modem.

```
// Create a map for the properties of the modem.
Map properties;
// Set the property ModemKeys.PROMISCUOUS_MODE_ENABLED to enable
```

// promiscuous mode on modem

properties.put(ModemKeys.PROMISCUOUS_MODE_ENABLED, "enabled")

properties.put(ModemKeys.CPE_DHCP_CRITERIA, "provisionedCPE");

```
add(
        DeviceType.DOCSIS,
                // deviceType: DOCSIS
        "1,6,00:11:22:33:44:55",
                // macAddress: derived from computer lease
        null,
                // hostName: not used in this example
        null,
                // domainName: not used in this example
        "0123-45-6789",
                // ownerID: here, account number from billing system
        "Silver",
                // ClassOfService
        "provisionedCM",
```

```
                // DHCP Criteria: Network Registrar uses this to
                // select a modem lease granting provisioned IP address
        properties
                // properties:
);
```

ステップ 6　技術者がケーブル モデムの電源をオンにし、BACC がプロビジョニングされたアクセス権をケーブル モデムに与えます。

ステップ 7　技術者がコンピュータの電源をオンにし、BACC　がプロビジョニングされたアクセス権をコンピュータに与えます。これで、ケーブル モデムとコンピュータはいずれもプロビジョニングされたデバイスとなります。コンピュータは、サービス プロバイダーのネットワークを介してインターネットにアクセスできます。

既存のモデムの交換

サービス プロバイダーが、故障したモデムを交換します。

(注) モデムから別のモデムへのローミングを制限するオプションがコンピュータに設定されている場合、モデムを交換したときは、コンピュータに設定されているモデムの MAC アドレスも変更する必要があります。

求める結果

次のワークフローを使用して、加入者に提供するサービスのレベルを変更することなく、既存のケーブル モデムを新しいモデムに物理的に交換します。

ステップ 1　サービス プロバイダーが、既存のモデムの MAC アドレスを新しいモデムの MAC アドレスに変更します。

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

```
// NO_ ACTIVATION is the activation mode because we will
// not be able to reset as the new modem has not booted
// on the network.
// NO_CONFIRMATION is the confirmation mode because we are
// not trying to reset the modem
// To change the MAC address of a DOCSIS modem:

changeMACAddress (
        "1,6,00:11:22:33:44:55"
                // old macAddress: unique identifier for the old modem
        "1,6,11:22:33:44:55:66"
                //// new macAddress: unique identifier for the new modem
);
```

ステップ 2　サービス プロバイダーが、ケーブル モデムを交換し、その電源をオンにします。コンピュータの電源もオンにする必要があります。

ステップ 3　これで、ケーブル モデムが完全にプロビジョニングされたデバイスとなり、適切なレベルのサービスを受けられるようになります。ケーブル モデムの背後にあるコンピュータも同様です。

無差別モードでの 2 台目のコンピュータの追加

加入者が、設置されているケーブル モデムの背後に 2 台目のコンピュータを接続します。

求める結果

次のワークフローを使用して、加入者の選択したサービスが複数の CPE の接続を許可すること、および接続された両方のコンピュータから加入者がネットワークにアクセスできることを保証します。

(注) この事例では、プロビジョニング API の呼び出しは必要ありません。

ステップ 1　加入者が、ケーブル モデムの背後に 2 台目のコンピュータを接続します。

ステップ 2　加入者がコンピュータの電源を入れます。

ステップ 3　加入者の選択したサービスが複数の CPE の接続を許可すると、BACC がインターネットへのアクセス権を 2 台目のコンピュータに与えます。

NAT を使用した最初のアクティベーションのセルフプロビジョニング

大学が、Network Address Translation（NAT; ネットワーク アドレス変換）および DHCP 機能を持つ DOCSIS ケーブル モデムを購入しました。建物の利用者 5 人がそれぞれ、コンピュータにブラウザ アプリケーションをインストールしています。

求める結果

次のワークフローを使用して、プロビジョニングされていない新しいケーブル モデム（NAT を持つ）と、モデムの背後にあるコンピュータをオンラインにし、適切なレベルのサービスを受けられるようにします。

ステップ 1　加入者が、NAT および DHCP 機能を持つケーブル モデムを購入し、集合建物内に設置します。

ステップ 2　加入者がモデムの電源をオンにし、BACC が制限付きアクセス権をモデムに与えます。

ステップ 3　加入者がラップトップ コンピュータをケーブル モデムに接続し、モデム内の DHCP サーバが IP アドレスをラップトップに与えます。

ステップ 4　加入者がコンピュータのブラウザ アプリケーションを起動します。スプーフィング DNS サーバにより、ブラウザがサービス プロバイダーの登録サーバ（OSS ユーザ インターフェイスやメディエータなど）にアクセスします。

ステップ 5　加入者がサービス プロバイダーのユーザ インターフェイスを使用して、ケーブル モデムの登録に必要な手順を完了します。登録用のユーザ インターフェイスが、モデムで NAT が使用されていることを検出し、モデムを登録して、モデムが NAT 互換のサービス クラスを受けられることを確認します。

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

```
// NO_ACTIVATION is the activation mode because this is a query.
// NO_CONFIRMATION is the confirmation mode because we are not
// attempting to reset the device.
// First we query the computer's information to find the modems
// MAC address.
// With NAT, the computer is never seen by the Network Registrar
// DHCP server. Instead, the modem has translated the IP address
// it assigned to the computer, so the web browser sees the
// modem's IP address. When the lease data is examined, the MAC
// address for the device and the relay-agent-remote-id are the
// same, indicating that this is an unprovisioned modem device,
// which is therefore presumed to be performing NAT.

LeaseResults modemLease =
        getAllForIPAddress("10.0.14.38");
        // ipAddress: restricted access.

String modemMACAddress = modemLease.
        getSingleLease().get(DeviceDetailsKeys.MAC_ADDRESS);
```

// MSO client registration program then calls the provisioning

```
// API to provision the NAT modem (with an appropriate class of
// service for NAT).

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// NO_ACTIVATION will generate a configuration for the modem
// however it will not attempt to reset it.
// The configuration will be able to be generated because the
// modem has booted. NO_CONFIRMATION is the confirmation mode
// because we are not attempting to reset the modem

add(
        DeviceType.DOCSIS,
                // deviceType: DOCSIS
        modemMACAddress,
                // macAddress: derived from its lease
        null,
                // hostName: not used in this example
        null,
                // domainName: not used in this example
        "0123-45-6789",
                // ownerID: here, account number from billing system
        "Silver",
                // ClassOfService
        "provisionedCM",
                // DHCP Criteria: Network Registrar uses this to
                // select a modem lease granting provisioned IP address
        null
                // properties: not used
);
```

ステップ 6　ユーザ インターフェイスにより、加入者はコンピュータをリブートするように求められます。

ステップ 7　プロビジョニング クライアントが *performOperation(…)* を呼び出してモデムをリブートし、プロビジョニングされたアクセス権をモデムに与えます。

```
get-new-batch(AUTOMATIC, NO_CONFIRMATION)

// AUTOMATIC is the activation mode because we are attempting
// to reset the modem so that it receives its new class of service.
// NO_CONFIRMATION is the confirmation mode because we don't want
// the batch to fail if we can't reset the modem.The user might
// have power cycled the modem when they rebooted their computer
// send a batch to reset the modem now that the user has been
// notified to reboot their computer


performOperation(
        DeviceOperation.RESET,
                //deviceOperation: Reset operation
        "1,6,00:11:22:33:44:55",
                // macAddress:Modem's MAC address
        null
                // properties : not used
        );
```

ステップ 8　これで、ケーブル モデムが完全にプロビジョニングされ、モデムの背後にあるコンピュータがサービス プロバイダーのネットワークにフル アクセスできるようになります。

(注)　NAT を持つ特定のケーブル モデムでは、新しいサービス クラス設定を取得するためにコンピュータをリブートするように求められる場合があります。ケーブル モデムと NAT デバイスが別々のデバイスになっている場合は、NAT デバイスもコンピュータの登録と同じように登録する必要があります。

NAT を持つモデムの背後への新しいコンピュータの追加

アパートの大家が 4 人の借家人に対し、モデムの共有と、サービス プロバイダーのネットワークへのアクセスを提供しています。この大家が新しい借家人に対し、建物のモデムを共有したインターネット アクセスを提供します。モデムには NAT および DHCP 機能が含まれています。新しい借家人が、モデムにコンピュータを接続します。

求める結果

次のワークフローを使用して、プロビジョニングされていない新しいコンピュータを、すでにプロビジョニングされているケーブル モデムでオンラインにし、新しいコンピュータが適切なレベルのサービスを受けられるようにします。

（注） この事例では、プロビジョニング API の呼び出しは必要ありません。

ステップ 1　加入者がコンピュータの電源を入れます。

ステップ 2　これで、コンピュータはプロビジョニングされたデバイスとなり、適切なレベルのサービスにアクセスできます。

（注） プロビジョニングされた NAT モデムは、モデムの背後にあるコンピュータをネットワークから見えなくします。

別の DHCP スコープへのデバイスの移動

サービス プロバイダーが、ネットワークに番号を再割り当てします。これに伴い、登録済みケーブル モデムには、別の Network Registrar スコープの IP アドレスが必要になります。

求める結果

プロビジョニング クライアントが DHCP 基準を変更し、ケーブル モデムが対応する DHCP スコープから IP アドレスを受信します。

ステップ 1　DOCSIS モデムの DHCP 基準を「newmodemCriteria」に変更します。

```
get-new-batch(AUTOMATIC, NO_CONFIRMATION);
// AUTOMATIC is the Activation mode because we are attempting
// to reset the modem so that a phone line is disabled
// NO_CONFIRMATION is the Confirmation mode because we don't
// want the batch to fail if we can't reset the modem.

// This use case assumes that the DOCSIS modem has been
// previously added to the database

changeDHCPCriteria(
        "1,6,ff:00:ee:11:dd:22"
                // Modem's MAC address or FQDN
                "newmodemCriteria"
        );
```

ステップ 2　モデムが、「newmodemCriteria」によって対象とされたスコープから IP アドレスを取得します。

イベントを使用したデバイス削除のロギング

サービス プロバイダーが、複数のプロビジョニング クライアントを保有しており、デバイス削除をログに記録します。

求める結果

どのプロビジョニング クライアントがデバイスを削除しても、プロビジョニング クライアントはイベントを 1 か所のログに記録します。

ステップ 1　デバイス削除イベントのリスナーを作成します。このクラスは、*DeviceAdapter* 抽象クラスを拡張するか、または *DeviceListener* インターフェイスを実装する必要があります。さらに、このクラスは、イベントをログに記録するために *deletedDevice(DeviceEvent ev)* メソッドを無効にする必要もあります。

```
public DeviceDeletionLogger
                extends DeviceAdapter
                //Extend the DeviceAdapter class.
{
         public void deletedDevice(DeviceEvent ev)
                        //Override deletedDevice.
        {
                logDeviceDeletion(ev.getDeviceID());
                        //Log the deletion.
        }
}
```

ステップ 2　*PACEConnection* インターフェイスを使用して、イベントのリスナーと修飾子を登録します。

```
DeviceDeletionLogger deviceDeletionLogger =
        new DeviceDeletionLogger();
                // Modem's MAC address or FQDN
                "newmodemCriteria"
qualifier = new DeviceEventQualifier();
// We are interested only in device deletion.
qualifier.setDeletedDevice ();
// Add device listener using PACEConnection
connection.addDeviceListener(deviceDeletionLogger, qualifier
);
```

ステップ 3　システムからデバイスが削除されると、イベントが生成され、リスナーに通知されます。

イベントを使用した RDU 接続の監視

サービス プロバイダーが、1 つのプロビジョニング クライアントを実行しており、プロビジョニング クライアントと RDU 間の接続が切断された場合に通知されるようにします。

求める結果

次のワークフローを使用して、接続が切断された場合にイベント インターフェイスからサービス プロバイダーに通知されるように設定します。

ステップ 1　メッセージ イベントのリスナーを作成します。このクラスは、MessagingAdapter 抽象クラスを拡張するか、または MessagingListener インターフェイスを実装する必要があります。さらに、このクラスは *connectionStopped(MessagingEvent ev)* メソッドを無効にする必要もあります。

```
// Extend the service provider's Java program using the
// provisioning client to receive Messaging events.
public MessagingNotifier
        extends MessagingAdapter
        //Extend the MessagingAdapter class.
{
        public void connectionStopped(MessagingEvent ev)
                //Override connectionStopped.
        {
                doNotification(ev.getAddress(), ev.getPort());
                        //Do the notification.
        }
}
```

ステップ 2　*PACEConnection* インターフェイスを使用して、イベントのリスナーと修飾子を登録します。

```
MessagingQualifier qualifier =
        new MessagingQualifier();
qualifier.setAllPersistentConnectionsDown();
MessagingNotifier messagingNotifier = new MessagingNotifier();
connnection.addMessagingListener(messagingNotifier, qualifier
);
```

ステップ 3　接続が切断されると、イベントが生成され、リスナーに通知されます。

イベントを使用したバッチ完了のロギング

サービス プロバイダーが、複数のプロビジョニング クライアントを保有しており、バッチ完了をログに記録します。

求める結果

どのプロビジョニング クライアントがバッチを完了しても、イベントが 1 か所のログに記録されます。

ステップ 1　イベントのリスナーを作成します。このクラスは、*BatchAdapter* 抽象クラスを拡張するか、または *BatchListener* インターフェイスを実装する必要があります。さらに、このクラスは、イベントをログに記録するために *completion(BatchEvent ev)* メソッドを無効にする必要もあります。

```
public BatchCompletionLogger
        extends BatchAdapter
        //Extend the BatchAdapterclass.
{
        public void completion(BatchEvent ev)
                              //Override completion.
        {
                logBatchCompletion(ev.BatchStatus().getBatchID());
                                      //Log the completion.
        }
}
```

ステップ 2　PACEConnection インターフェイスを使用して、イベントのリスナーと修飾子を登録します。

```
BatchCompletionLogger batchCompletionLogger =
        new BatchCompletionLogger();
Qualify All qualifier = new Qualify All();
connection.addBatchListener(batchCompletionLogger , qualifier
);
```

ステップ 3　バッチが完了すると、イベントが生成され、リスナーに通知されます。

デバイスの詳細情報の取得

サービス プロバイダーが管理者に対し、特定のデバイスの詳細情報を表示することを許可します。

求める結果

サービス プロバイダーの管理アプリケーションが、特定のデバイスに関する既知の詳細をすべて表示します。この詳細には、MAC アドレス、リース情報、デバイスのプロビジョニング ステータス、およびデバイス タイプ（既知の場合）などがあります。

ステップ 1　管理者が、サービス プロバイダーの管理ユーザ インターフェイスに、クエリーするデバイスの MAC アドレスを入力します。

ステップ 2　BACC が、デバイスの詳細を組み込みデータベースにクエリーします。

```
get-new-batch(AUTOMATIC, NO_CONFIRMATION);

// MSO admin UI calls the provisioning API to query the details
// for the requested device. Query may be performed based on MAC
// address or IP address, depending on what is known about the
// device.
Map deviceDetails =
        getDetails(
                "1,6,00:11:22:33:44:55",
                        // macORFqdn: unique identifier for the device
                true
                        // needLeaseInfo: yes we need it
                };
```

ステップ 3　サービス プロバイダーのアプリケーションが、デバイス データの詳細に関するページを表示します。このページには、要求されたデバイスに関する既知の情報をすべて表示できます。デバイスがサービス プロバイダーのネットワークに接続された場合、このデータにはリース情報（IP アドレスやリレー エージェントの ID など）が含まれます。データは、デバイスがプロビジョニングされたかどうかを示します。プロビジョニングされた場合、データにはデバイス タイプも含まれます。

```
// extract device detail data from the map
String deviceType = (String)deviceDetails.get(DEVICE_TYPE);
String macAddress = (String)deviceDetails.get(MAC_ADDRESS);
String ipAddress = (String)deviceDetails.get(IP_ADDRESS);
String relayAgentID = (String)deviceDetails.get(RELAY_AGENT_ID);
Boolean isProvisioned = (Boolean)deviceDetails.get(IS_PROVISIONED);
// The admin UI now formats and prints the detail data to a view page
```

デフォルトのサービス クラスを使用した検索

サービス プロバイダーが管理者に対し、DOCSIS デバイス タイプの *default* サービス クラスを持つすべてのモデムのデータを表示することを許可します。

求める結果

サービス プロバイダーの管理アプリケーションが、デフォルトのサービス クラスを持つ DOCSIS デバイスのリストを返します。

ステップ 1　管理者が、サービス プロバイダーの管理ユーザ インターフェイスで、検索オプションを選択します。

ステップ 2　BACC が、要求されたデフォルトのサービス クラスに一致するデバイスの MAC アドレスすべてのリストを、組み込みデータベースにクエリーします。

```
get-new-batch(AUTOMATIC, NO_CONFIRMATION);

// Create a MACAddressSearchType to indicate search by
// default class of service.

MACAddressSearchType mst =
        new MACAddressSearchType.getByDefaultClassOfService(
                                        DeviceType.DOCSIS);
// Create a MACAddressSearchFilter to get 20 devices
// at a time. This indicates that we have a page size of 20.

MACAddressSearchFilter mySearchFilter =
        new MACAddressSearchFilter(
                mst,
                        // type: MAC address search type
                false,
                        // isInclusive:
                20
                        // maximumReturned:
                );
// MAC address to start the search from.
String startMac = null;

// A list containing the MAC addresses returned from
// search.
List deviceList = null;

// If the size of deviceList is equal to 20 then
// there may be devices matching the search criteria.
        while ((deviceList == null) ||
                        (deviceList.size() == 20))
        {
```

```
                // Use the provisioning API call to search BACC
                // database. The search starts from the MAC address
                // "startMac". If "startMac" is null then the search
                // starts from the very begining of the index.

                deviceList = search (mySearchFilter, startMac);

                // See Step 3 for the definition of processMACAddressList

                startMac = processMACAddressList(deviceList);
}
```

ステップ 3　サービス プロバイダーのアプリケーションが、これらのデバイスの詳細を BACC から要求し、デバイス データのページを表示します。デバイスごとに、デバイス タイプ、MAC アドレス、クライアント クラス、およびデバイスのプロビジョニング ステータスがコード表示されます。デバイスは 1 行ずつ表示されます。

```
processMACAddressList (List deviceList)
{
        Iterator iter = deviceList.iterator();

        String startMac = null;

        while (iter.hasNext())
        {
                startMac = (String) iter.next();
                // Get details for this device
                Map detailMap = getDetails (
                        startMac,
                                // MAC of current device
                        true
                                // yes, we need lease info
                        );
                // extract device detail data from each map
                // this can be used for displaying in UI
                String deviceType = (String)detailMap.get(DEVICE_TYPE);
                String macAddress = (String)detailMap.get(MAC_ADDRESS);
                String clientClass = (String)detailMap.get(CLIENT_CLASS);
                Boolean isProvisioned = (Boolean)detailMap.get(IS_PROVISIONED);
                // format and print above data in output line
        }

        // We return the last MAc address in the list
        // so that the next search can be started from here

        return startMAC;
}
```

ベンダープレフィックスに一致するデバイスの取得

サービス プロバイダーが管理者に対し、特定のベンダープレフィックスに一致するすべてのデバイスのデータを表示することを許可します。

求める結果

サービス プロバイダーの管理アプリケーションが、要求されたベンダープレフィックスに一致するデバイスのリストを返します。

ステップ 1　管理者が、サービス プロバイダーの管理ユーザ インターフェイスに、目的のベンダープレフィックスに一致する部分文字列を入力します。

ステップ 2　BACC が、要求されたベンダープレフィックスに一致するデバイスの MAC アドレスすべてのリストを、組み込みデータベースにクエリーします。

```
// Create a MACAddressPattern corresponding to the requested
// vendor prefix

MACAddressPattern pattern =

         new MACAddressPattern(

                "1,6,ff:00:ee:*",

                        // macAddressPattern: the requested vendor prefix

                );

// Create a MACAddressSearchType to indicate search by
// MAC address pattern

MACAddressSearchType mst =

        new MACAddressSearchType.getDevices(pattern);

// Create a MACAddressSearchFilter to get 20 devices
// at a time. This indicates that we have a page size of 20.

MACAddressSearchFilter mySearchFilter =

        new MACAddressSearchFilter(

                mst,

                        // type: MAC address search type

                false,

                        // isInclusive:

                20

                         // maximumReturned:

                );

// MAC address to start the search from.
String startMac = null;

// A list containing the MAC addresses returned from
// search.
List deviceList = null;

// If the size of deviceList is equal to 20 then
// there may be devices matching the search criteria.

while ((deviceList == null) ||

        (deviceList.size() == 20))

{
```

```
        // Use the provisioning API call to search BACC
        // database. The search starts from the MAC address
        // "startMac". If "startMac" is null then the search
        // starts from the very begining of the index.

        deviceList = search (mySearchFilter, startMac);

        // See Step 3 for the definition of processMACAddressList

        startMac = processMACAddressList(deviceList);
}
```

ステップ 3　サービス プロバイダーのアプリケーションが、これらのデバイスの詳細を BACC から要求し、デバイス データのページを表示します。デバイスごとに、デバイス タイプ、MAC アドレス、クライアント クラス、およびデバイスのプロビジョニング ステータスがコード表示されます。デバイスは 1 行ずつ表示されます。

```
processMACAddressList (List deviceList)
{
        Iterator iter = deviceList.iterator();

        String startMac = null;

        while (iter.hasNext())
        {
                startMac = (String) iter.next();
                // Get details for this device
                Map detailMap = getDetails (
                        startMac,
                                // MAC of current device
                        true
                                // yes, we need lease info
                        ) ;

                // extract device detail data from each map
                // this can be used for displaying in UI
                String deviceType = (String)detailMap.get(DEVICE_TYPE);
                String macAddress = (String)detailMap.get(MAC_ADDRESS);
                String clientClass = (String)detailMap.get(CLIENT_CLASS);
                Boolean isProvisioned = (Boolean)detailMap.get(IS_PROVISIONED);
                // format and print above data in output line
                }
        // We return the last MAc address in the list
        // so that the next search can be started from here

        return startMac;
}
```

PacketCable eMTA の事前プロビジョニング

新しい顧客が、サービス プロバイダーに連絡して PacketCable 音声サービスを注文します。顧客は、プロビジョニングされた組み込み型 MTA を受け取ります。

求める結果

次のワークフローを使用して、組み込み型 MTA を事前プロビジョニングし、モデムの MTA コンポーネントがオンラインになったときに適切なレベルのサービスを受けられるようにします。

(注) 次の使用例では、eMTA から電話をかけるのに必要なコール エージェントのプロビジョニングを省略しています。

ステップ 1　サービス プロバイダーが、課金システムで使用する加入者のユーザ名とパスワードを選択します。

ステップ 2　サービス プロバイダーが、モデム コンポーネントに適切なサービス クラスと DHCP 基準を選択し、コンポーネントを BACC に追加します。

```
get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// Let's provision the modem and the MTA component in the same
// batch. This can be done because the activation mode of this
// batch is NO_ACTIVATION. More than one device can be operated
// on in a batch if the activation mode does not lead to more
// than one device being reset.
// To add a DOCSIS modem:

add(
        DeviceType.DOCSIS,
                // deviceType: DOCSIS
        "1,6,01:02:03:04:05:06",
                // macAddress: scanned from the label
        null
                // hostName: not used in this example
        null
                // domainName: not used in this example
        "0123-45-6789",
                // ownerID: here, account number from billing system
        "Silver",
                // classOfService
        "provisionedCM",
                // DHCP Criteria: Network Registrar uses this to
                // select a modem lease granting provisioned IP address
        null
                // properties: not used
);
```

ステップ 3　サービス プロバイダーが、MTA コンポーネントに適切なサービス クラスと DHCP 基準を選択し、コンポーネントを BACC に追加します。

```
// Continuation of the batch in Step2
// To add the MTA component:

add(
        DeviceType.PACKET_CABLE_MTA,
                // deviceType: PACKET_CABLE_MTA
        "1,6,01:02:03:04:05:07",
                // macAddress: scanned from the label
        null,
                // hostName: not used in this example, will be auto generated
        null,
                // domainName: not used in this example, will be auto generated.
                // The FqdnKeys.AUTO_FQDN_DOMAIN property must be set somewhere in the
                // property hierarchy.
        "0123-45-6789",
                // ownerID: here, account number from billing system
        "Silver",
                // ClassOfService
        "provisionedMTA",
                // DHCP Criteria: Network Registrar uses this to
                // select an MTA lease granting provisioned IP address
        null
                // properties: not used
);
```

ステップ 4　組み込み型 MTA が顧客に出荷されます。

ステップ 5　顧客が、組み込み型 MTA をオンラインにして、電話をかけます。

PacketCable eMTA 上での SNMP クローン作成

顧客が SNMP Element Manager を所有しており、これを使用して PacketCable eMTA にアクセスします。

求める結果

外部の Element Manager に、PacketCable eMTA へのセキュアな SNMPv3 アクセス権が与えられます。

(注) RW MIB 変数に加えた変更は永続的なものではなく、BACC の eMTA に関する設定において更新されることはありません。eMTA MIB に書き込まれた情報は、次回 MTA を電源オフにするか、またはリセットしたときに失われます。

ステップ 1　プロビジョニング API メソッドである performOperation() を呼び出します。その際は、MTA の MAC アドレスと、MTA 上に作成する新しいユーザのユーザ名を渡します。このユーザ名は、後で Element Manager が SNMP コールを行うときに使用されます。

```
get-new-batch(NO_ACTIVATION, NO_CONFIRMATION);

// NO_ACTIVATION is the activation mode because we don't want to
// reset the device.
// NO_CONFIRMATION is the confirmation mode because we are
// not attempting to reset the device.

// The goal here is to create a new user on the MTA indicated
// by the MAC address. The other parameter needed here is the new
// user name, which is passed in the Map.
// Create a map that contains one element - the name of
// the new user to be created on the MTA
HashMap map = new HashMap();
map.put( SNMPPropertyKeys.CLONING_USERNAME, "newUser" );
// The first param is the actual device operation to perform.
performOperation(
        DeviceOperation.ENABLE_SNMPV3_ACCESS,
                // deviceOperation : ENABLE_SNMPV3_ACCESS
        "1,6,00:00:00:00:00:99",
                // macORFqdn : MAC Address of the modem
        map
                // parameters: operation specific parameters
);
```

ステップ 2　プロビジョニング API が、ステップ 1 で渡された新しいユーザに対応するエントリを MTA 上に作成するため、SNMPv3 クローン作成操作の実行を試みます。新しいユーザのエントリ行で使用されるキーは、BACC 内で定義された 2 つのパスワードの関数です。これらのパスワードは、顧客が利用できるようになります。また、RDU コマンドが、これらのパスワード（auth および priv パスワード）をキー ローカリゼーション アルゴリズムに渡して、auth および priv キーを作成します。これらのキーは、新しいユーザとセットで、eMTA のユーザ テーブルに格納されます。

（注） このステップに記載されている auth および priv パスワードを変更するには、rdu.properties 設定ファイル内の SNMPPropertyKeys.CLONING_AUTH_PASSWORD（/snmp/cloning/auth/password）および SNMPPropertyKeys.CLONING_PRIV_PASSWORD（/snmp/cloning/priv/password）プロパティをそれぞれ設定変更します。

ステップ 3　顧客が、上で指定されたユーザ名、パスワード、および キー ローカリゼーション アルゴリズムを使用して SNMPv3 要求を発行し、MTA とのセキュアな通信を可能にします。

PacketCable eMTA の差分プロビジョニング

顧客が、PacketCable eMTA を使用しており、その 1 つ目の回線（エンドポイント）をイネーブルにしています。この顧客が、eMTA 上の 2 つ目の電話回線（エンドポイント）をイネーブルにし、その回線に電話を接続します。

求める結果

顧客が eMTA 上の 2 つ目の回線（エンドポイント）に電話を接続し、どのサービスも中断することなく正常に電話をかけられるようになる必要があります。

（注） eMTA 上で 2 つ目の回線を使用するには、コール エージェントを適切に設定する必要があります。コール エージェントのプロビジョニングについては、この使用例では取り上げません。

ステップ 1　サービス プロバイダーのアプリケーションが、BACC API を起動して、eMTA のサービス クラスを変更します。新しいサービス クラスは、eMTA 上の 2 つのエンドポイントをサポートします。このサービス クラスの変更は、eMTA をリセットして初めて有効になります。eMTA を中断することは好ましくありません。そのため、差分プロビジョニングが次のステップで行われます。

```
get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// NO_ACTIVATION is the activation mode because we don't want to
// reset the device.
// NO_CONFIRMATION is the Confirmation mode because we are not
// disrupting the device.

changeClassOfService(
        "1,6,ff:00:ee:11:dd:22" // eMTA's MAC address or FQDN
,"twoLineEnabledCOS" // This COS supports two lines.
);
```

ステップ 2　サービス プロバイダーのアプリケーションが、BACC 差分更新機能を使用して、eMTA に SNMP オブジェクトを設定します。そのため、eMTA を中断することなく、サービスがイネーブルになります。

```
// The goal here is to enable a second phone line, assuming one
// phone line is currently enabled.  We will be adding a new
// row to the pktcNcsEndPntConfigTable.

get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// NO_ACTIVATION is the activation mode because we don't want to
// reset the device.
// NO_CONFIRMATION is the confirmation mode because we are
// not attempting to reset the device.
```

```
// Create a map containing one element - the list of SNMP
// variables to set on the MTA
HashMap map = new HashMap();

// Create an SnmpVarList to hold SNMP varbinds
SnmpVarList list = new SnmpVarList();

// An SnmpVariable represents an oid/value/type triple.

// pktcNcsEndPntConfigTable is indexed by the IfNumber, which in this
// case we will assume is interface number 12 (this is the last
// number in each of the oids below.

// The first variable represents the creation of a new row in
// pktcNcsEndPntConfigTable  we are setting the RowStatus
// column (column number 26).  The value of 4 indicates that
// a new row is to be created in the active state.
SnmpVariable variable = new SnmpVariable(
        ".1.3.6.1.4.1.4491.2.2.2.1.2.1.1.26.12",
        "4",
        SnmpType.INTEGER );
list.add( variable );

// The next variable represents the call agent id for this new
// interface, which we'll assume is 'test.com'
SnmpVariable variable = new SnmpVariable(
        ".1.3.6.1.4.1.4491.2.2.2.1.2.1.1.1.12",
        "test.com",
        SnmpType.STRING );
list.add( variable );

// The final variable represents the call agent port
SnmpVariable variable = new SnmpVariable(
        ".1.3.6.1.4.1.4491.2.2.2.1.2.1.1.2.12",
        "2728",
        SnmpType.INTEGER );
list.add( variable );

// Add the SNMP variable list to the Map to use in the API call
map.put( SNMPPropertyKeys.SNMPVAR_LIST, list );

// Invoke the BACC API to do incremental update on the eMTA.
performOperation( DeviceOperation.INCREMENTAL_UPDATE  // device operation
        ,"1,6,00:00:00:00:00:99" // MAC Address
        , map   // Parameters for the operation
        );
```

ステップ 3　eMTA で 2 つ目の電話回線を使用できるようになります。eMTA は、ステップ 1 でサービス クラスが変更された後（リセット後）から、継続的に同じサービスを受けられるようになります。

動的設定ファイルを使用した DOCSIS モデムの事前プロビジョニング

新しい顧客が、サービス プロバイダーに連絡して、DOCSIS モデムと、モデムの背後に接続された 2 つの CPE を対象とする高速な *Gold* データ サービスを注文します。

求める結果

次のワークフローを使用して、DOCSIS テンプレートを使用するサービス クラスで DOCSIS モデムを事前プロビジョニングします。テンプレートから生成される動的設定ファイルは、モデムがオンラインになるときに使用されます。

ステップ 1　サービス プロバイダーが、課金システムで使用する加入者のユーザ名とパスワードを選択します。

ステップ 2　サービス プロバイダーが、Gold サービス クラスと適切な DHCP 基準を選択し、ケーブル モデムを BACC に追加します。

```
get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)


Map properties;

// Set the property ModemKeys.PROMISCUOUS_MODE_ENABLED to enable
// promiscuous mode on modem

properties.put(ModemKeys.PROMISCUOUS_MODE_ENABLED, "enabled")

// No CPE DHCP Criteria is specified.
// The CPEs behind the modem will use the default provisioned
// promiscuous CPE DHCP criteria specified in the system defaults.

// This custom property corresponds to a macro variable in the
// DOCSIS template for “gold” class of service indicating the
// maximum number of CPEs allowed behind this modem. We set it
// to two CPEs from this customer.

properties.put(“docsis-max-cpes”, "2");

// To add a DOCSIS modem:

add(
        DeviceType.DOCSIS,
                // deviceType: DOCSIS
        “1,6,01:02:03:04:05:06”,
                // macAddress: scanned from the label
        null,
                // hostName: not used in this example
        null,
                // domainName: not used in this example
        "0123-45-6789",
                // ownerID: here, account number from billing system
        "gold",
                // classOfService:
        "provisionedCM",
                        // DHCP Criteria: Network Registrar uses this to
                // select a modem lease granting provisioned IP address
        properties
                // properties:
        );
```

ステップ 3　ケーブル モデムが顧客に出荷されます。

ステップ 4　顧客がケーブル モデムをオンラインにし、モデムの背後にコンピュータを接続します。

オプティミスティック ロッキング

サービス プロバイダー アプリケーションのインスタンスが、同じアプリケーションの別のインスタンスによって行われた変更を上書きしないことを保証します。

求める結果

次のワークフローを使用して、BACC API が提供するオプティミスティック ロッキング機能のデモを行います。

(注)　オブジェクトのロッキングは、マルチユーザ　システムで変更の完全性を維持するために実行されます。その結果、ユーザの変更が、別のユーザによって不用意に上書きされなくなります。オプティミスティック ロッキングを使用してプログラム記述する場合、コミットしようとするオブジェクトの少なくとも 1 つが、処理の開始後に別のユーザによって変更されていたときは、コミットが失敗する可能性があります。

ステップ 1　サービス担当者が、サービス プロバイダーのユーザ インターフェイスで検索オプションを選択し、ケーブル モデムの MAC アドレスを入力します。

ステップ 2　BACC が、組み込みデータベースにクエリーし、デバイスの詳細を取得します。次に、その情報が MSO ユーザ インターフェイスに表示されます。

```
// MSO admin UI calls the provisioning API to query the details
// for the requested device.
Map deviceDetails =
        getDetails(
                "1,6,00:11:22:33:44:55",
                        // macORFqdn: unique identifier for the device
                true
                        // needLeaseInfo: yes we need it
                };
// extract device detail data from the map
String deviceType = (String)deviceDetails.get(DEVICE_TYPE);
String macAddress = (String)deviceDetails.get(MAC_ADDRESS);
String ipAddress = (String)deviceDetails.get(IP_ADDRESS);
String relayAgentID = (String)deviceDetails.get(RELAY_AGENT_ID);

Boolean isProvisioned = (Boolean)deviceDetails.get(IS_PROVISIONED);
// service provider admin UI displays this information.

// Let's save the OID_REVISION_NUMBER property so that we can se in
// step 3.
String oidRevisionNumber = (String)deviceDetails.get(OID_REVISION_NUMBER);
```

ステップ 3　サービス担当者が、ユーザ インターフェイスを使用して、モデムのサービス クラスと DHCP 基準を変更します。その結果、BACC API が起動します。

```
// We need a reference to Batch instance so that ensureConsistency()
// method can be invoked on it.
Batch batch = conn.newBatch() ;

List oidList = new ArrayList();
// Add the oid-rev number saved from step 2 to the list
oidList.add(oidRevisionNumber);

// Sends a list of OID revision numbers to validate before processing the
// batch.  This ensures that the objects specified have not been modified
// since they were last retrieved.
batch.ensureConsistency(oidList);
        batch.changeClassOfService (
                "1,6,00:11:22:33:44:55",
                // macORFqdn: unique identifier for the device.
        "gold"
                // newCOSName : Class of service name.
                )
batch.changeDHCPCriteria (
        "1,6,00:11:22:33:44:55",
                // macORFqdn: unique identifier for the device.
        "specialDHCPCriteria"
                // newDHCPCriteria : New DHCP Criteria.
                )
// This batch fails with BatchStatusCodes.BATCH_NOT_CONSISTENT,
// in case if the device is updated by another client in the mean time.
// If there is a conflict occurs, then the service provider client
// is responsible for resolving the conflict by querying the database
// again and then applying changes appropriately.
```

ステップ 4　これで、ユーザが Gold サービス クラスと適切な DHCP 基準を受けられるようになります。

加入者の帯域幅の一時的なスロットリング

MSO が、加入者に許可するダウンロードのデータ量を 1 か月あたり 10 MB に制限するサービスを提供します。その限度に達すると、加入者のダウンストリーム帯域幅が 1 MB から 56 KB に制限されます。月が替わると 1 MB に戻ります。

(注) ピアツーピア ユーザや Web サイトを運営するユーザはアップロード帯域幅の使用率が非常に高くなる傾向があるため、アップストリーム帯域幅の変更も考慮することが必要になる場合があります。

求める結果

次のワークフローを使用して、加入者の帯域幅をその契約条件に従って増減させます。

ステップ 1　MSO が、*NetFlow* などのレート追跡システムを使用します。このシステムは、MAC アドレスに基づいて各顧客の使用率を追跡します。最初に、顧客は、1 MB のダウンストリームを持つ *Gold* サービス クラスのレベルでプロビジョニングされます。

ステップ 2　レート追跡ソフトウェアが、加入者が 10 MB の限度に達したことを特定すると、OSS に通知します。次に、OSS が BACC API を呼び出して、加入者のサービス クラスを *Gold* から *Gold-throttled* に変更します。

```
get-new-batch(AUTOMATIC, NO_CONFIRMATION)

// AUTOMATIC is the activation mode because we are
// attempting  to reset the modem so that it
// receives low bandwidth service.
// NO_CONFIRMATION is the confirmation mode
// because we do not want the batch to fail if we cannot
// reset the modem. If the modem is off, when it will
// be disabled when it is turned back on.

// Let's change the COS of the device so that it restricts
// bandwidth usage of the modem.
        changeClassOfService(
                Device.MAC_ADDRESS,
                        // macAddress: unique identifier for this modem
                "Gold-throttled");
                        // newClassOfService: restricts bandwidth usage to 56k
```

ステップ 3　支払い請求周期の期末になると、OSS が BACC API を呼び出して、加入者のサービス クラスを *Gold* に戻します。

CableHome WAN-Man の事前プロビジョニング

新しい顧客が、サービス プロバイダーに連絡してホーム ネットワーキング サービスを注文します。顧客には、プロビジョニングされた CableHome デバイスが出荷されます。

求める結果

次のワークフローを使用して、CableHome デバイスを事前プロビジョニングし、ケーブル モデムとその WAN-Man コンポーネントがオンラインになったときに適切なレベルのサービスを受けられるようにします。

ステップ 1　サービス プロバイダーが、課金システムで使用する加入者のユーザ名とパスワードを選択します。

ステップ 2　サービス プロバイダーが、モデム コンポーネントに適切なサービス クラスと DHCP 基準を選択し、コンポーネントを BACC に追加します。

```
get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// Let's provision the modem and the WAN-Man component in the same
// batch.
// To add a DOCSIS modem:

add(
        DeviceType.DOCSIS,
                // deviceType: DOCSIS
        "1,6,01:02:03:04:05:06",
                // macAddress: scanned from the label
        null,
                // hostName: not used in this example
        null,
                // domainName: not used in this example
        "0123-45-6789",
                // ownerID: here, account number from billing system
        "Silver",
                // classOfService
        "provisionedCM",
                // DHCP Criteria: Network Registrar uses this to
                // select a modem lease granting provisioned IP address
        null
                // properties: not used
);
```

ステップ 3　サービス プロバイダーが、WAN-Man コンポーネントに適切なサービス クラスと DHCP 基準を選択し、コンポーネントを BACC に追加します。

```
// Continuation of the batch in Step2
        // To add the WAN-Man component:
add(
        DeviceType.CABLEHOME_WAN_MAN,
                // deviceType: CABLEHOME_WAN_MAN
        "1,6,01:02:03:04:05:07",
                // macAddress: scanned from the label
        null,
                // hostName: not used in this example.
        null,
                // domainName: not used in this example.
        "0123-45-6789",
                // ownerID: here, account number from billing system
        "silverWanMan",
                // ClassOfService
        "provisionedWanMan",
                // DHCP Criteria: Network Registrar uses this to
                // select an MTA lease granting provisioned IP address
        null
                // properties: not used
        );
```

ステップ 4　CableHome デバイスが顧客に出荷されます。

ステップ 5　顧客が CableHome デバイスをオンラインにします。

ファイアウォール設定を持つ CableHome

顧客が、サービス プロバイダーに連絡して、ファイアウォール機能がイネーブルになったホーム ネットワーキング サービスを注文します。顧客は、プロビジョニングされた CableHome デバイスを受け取ります。

求める結果

次のワークフローを使用して、CableHome デバイスを事前プロビジョニングし、ケーブル モデムとその WAN-Man コンポーネントがオンラインになったときに適切なレベルのサービスを受けられるようにします。

ステップ 1　サービス プロバイダーが、課金システムで使用する加入者のユーザ名とパスワードを選択します。

ステップ 2　サービス プロバイダーが、ケーブル モデム コンポーネントに適切なサービス クラスと DHCP 基準を選択し、コンポーネントを BACC に追加します。

```
get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// Let's provision the modem and the WAN-Man component in the same
// batch.
// To add a DOCSIS modem:

add(
        DeviceType.DOCSIS,
                // deviceType: DOCSIS
        "1,6,01:02:03:04:05:06",
                // macAddress: scanned from the label
        null,
                // hostName: not used in this example
        null,
                // domainName: not used in this example
        "0123-45-6789",
                // ownerID: here, account number from billing system
        "Silver",
                // classOfService
        "provisionedCM",
                        // DHCP Criteria: Network Registrar uses this to
                // select a modem lease granting provisioned IP address
        null
                // properties: not used
        );
```

ステップ 3　サービス プロバイダーが、WAN-Man コンポーネントに適切なサービス クラスと DHCP 基準を選択し、コンポーネントを BACC に追加します。

```
// Continuation of the batch in Step2
// To add the WAN-Man component:

// Create a Map to contain WanMan's properties

Map properties;

// The fire wall configuration for the Wan Man component is specified
// using the CableHomeKeys.CABLEHOME_WAN_MAN_FIREWALL_FILE property.
// This use case assumes that the firewall configuration file named
// "firewall_file.cfg" is already present in the RDU database and the
// firewall configuration is enabled in the Wan Man configuration file
// specified with the corresponding class of service.

properties.put(CableHomeKeys.CABLEHOME_WAN_MAN_FIREWALL_FILE,
"firewall_file.cfg");

add(
        DeviceType.CABLEHOME_WAN_MAN,
                // deviceType: CABLEHOME_WAN_MAN
        "1,6,01:02:03:04:05:07",
                // macAddress: scanned from the label
        null,
                // hostName: not used in this example.
        null,
                // domainName: not used in this example.
        "0123-45-6789",
                // ownerID: here, account number from billing system
        "silverWanMan",
                // ClassOfService
        "provisionedWanMan",
                // DHCP Criteria: Network Registrar uses this to
                // select an MTA lease granting provisioned IP address
        properties
                // properties: contains the firewall config file
        );
```

ステップ 4　CableHome デバイスが顧客に出荷されます。

ステップ 5　顧客が CableHome デバイスをオンラインにします。次に、ケーブル モデムと WAN-Man コンポーネントが、プロビジョニングされた IP アドレスと正しい設定ファイルを取得します。

CableHome WAN-Man のデバイス機能の取得

サービス プロバイダーが管理者に対し、CableHome WAN-Man デバイスの機能の情報を表示することを許可します。

求める結果

サービス プロバイダーの管理アプリケーションが、特定の CableHome WAN-Man コンポーネントに関する既知の詳細をすべて表示します。この詳細には、MAC アドレス、リース情報、プロビジョニング ステータス、およびデバイス機能の情報などがあります。

ステップ 1　管理者が、サービス プロバイダーのユーザ インターフェイスに、クエリーする WAN-Man の MAC アドレスを入力します。

ステップ 2　BACC が、入力された MAC アドレスを使用して特定したデバイスの詳細を、組み込みデータベースにクエリーします。

```
get-new-batch(NO_ACTIVATION, NO_CONFIRMATION);

// MSO admin UI calls the provisioning API to query the details
// for the requested device.

Map deviceDetails =
        getDetails(
                1,6,00:11:22:33:44:55","
                        // macORFqdn: unique identifier for the device
                true
                        // needLeaseInfo: yes we need it
                };
```

ステップ 3　サービス プロバイダーのアプリケーションが、デバイス データの詳細に関するページを表示します。このページには、要求されたデバイスに関する既知の情報をすべて表示できます。デバイスがサービス プロバイダーのネットワークに接続された場合、このデータにはリース情報（IP アドレスやリレー エージェントの ID など）が含まれます。このデータは、デバイスがプロビジョニングされているかどうかを示します。プロビジョニングされている場合、データにはデバイス タイプとデバイス機能の情報も含まれます。

```
// extract device details information from the map
String deviceType      = (String)   deviceDetails.get(DeviceDetailsKeys.DEVICE_TYPE);
String macAddress      = (String)   deviceDetails.get(DeviceDetailsKeys.MAC_ADDRESS);
String ipAddress       = (String)   deviceDetails.get(DeviceDetailsKeys.IP_ADDRESS);
String relayAgentID    = (String)   deviceDetails.get(
                                            DeviceDetailsKeys.RELAY_AGENT_ID);
Boolean isProvisioned  = (Boolean)  deviceDetails.get(
                                            DeviceDetailsKeys.IS_PROVISIONED);
String formation       = (String)    deviceDetails.get(
                                            IPDeviceCapabilities.FORMATION);
String deviceList      = (String)    deviceDetails.get(
                                            IPDeviceCapabilities.DEVICE_LIST);
String serNum          = (String)   deviceDetails.get(
                                            IPDeviceCapabilities.SERIAL_NUMBER);
String hwVer           = (String)   deviceDetails.get(
                                            IPDeviceCapabilities.HARDWARE_VERSION);
String swVer           = (String)   deviceDetails.get(
                                            IPDeviceCapabilities.SOFTWARE_VERSION);
String brVer           = (String)   deviceDetails.get(
                                            IPDeviceCapabilities.BOOT_ROM_VERSION);
String vendorOui       = (String)   deviceDetails.get(
                                            IPDeviceCapabilities.VENDOR_OUI);
String modelNum        = (String)   deviceDetails.get(
                                            IPDeviceCapabilities.MODEL_NUMBER);
String vendorNum       = (String)   deviceDetails.get(
                                            IPDeviceCapabilities. VENDOR_NAME)
String sysDesc         = (String)    deviceDetails.get(
                                            IPDeviceCapabilities.SYSTEM_DESCRIPTION);
String fwVer           = (String)   deviceDetails.get(
                                            IPDeviceCapabilities.FIRMWARE_VERSION);
String fwVer           = (String)   deviceDetails.get(
                                            IPDeviceCapabilities.FIREWALL_VERSION);
// The admin UI now formats and prints the detail data to a view page
```

CableHome WAN-Man のセルフプロビジョニング

加入者が、建物内にブラウザ アプリケーションを持つコンピュータを設置し、組み込み CableHome デバイスを購入しています。

求める結果

次のワークフローを使用して、プロビジョニングされていない新しい組み込み CableHome デバイスをオンラインにし、適切なレベルのサービスを受けられるようにします。さらに、組み込み CableHome デバイスに接続されたコンピュータから加入者がインターネットにアクセスできるようにします。

ステップ 1　加入者が、組み込み CableHome デバイスを購入し、建物内に設置します。

ステップ 2　加入者が、組み込み CableHome デバイスの電源をオンにします。BACC が、制限付きのアクセス権を組み込みケーブル モデムに与えます。つまり、アクセス権が 2 つの CPE（CableHome WAN-Man とコンピュータ）に制限されます。

(注)　この使用例は、プロビジョニングされていない DOCSIS モデムの背後に 2 つの CPE を接続できることを前提としています。特に設定しない限り、BACC では、プロビジョニングされていない DOCSIS モデムの背後に接続できるデバイスは 1 台のみです。この動作を変更するには、2 つの CPE をサポートする適切なサービス クラスを定義してから、そのサービス クラスを DOCSIS デバイスのデフォルト サービス クラスとして使用します。

ステップ 3　BACC が CableHome WAN-Man を設定します。この設定には、IP 接続や、デフォルトの CableHome ブート ファイルのダウンロードなどがあります。デフォルトの CableHome ブート ファイルは、CableHome デバイスをパススルー モードに設定します。まだ、CableHome デバイスはプロビジョニングされません。

ステップ 4　加入者が、コンピュータを CableHome デバイスに接続します。コンピュータが、プロビジョニングされていない（制限された）IP アドレスを取得します。加入者がコンピュータ上でブラウザ アプリケーションを起動します。スプーフィング DNS サーバにより、Web ブラウザがサービス プロバイダーの登録サーバ（OSS ユーザ インターフェイスやメディエータなど）にアクセスします。

ステップ 5　加入者がサービス プロバイダーのユーザ インターフェイスを使用して、ケーブル モデムの登録に必要な手順（サービス クラスの選択など）を完了します。また、加入者は CableHome のサービス クラスも選択します。

ステップ 6　サービス プロバイダーのユーザ インターフェイスが、加入者の情報（ケーブル モデムと CableHome に対して選択されたサービス クラスやコンピュータの IP アドレスなど）を BACC に渡します。次に、加入者が BACC に登録されます。

```
get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// NO_ACTIVATION is the activation mode because this is a
// query. NO_CONFIRMATION is the confirmation mode because
// we are not attempting to reset the device.
// First we query the computer's information to find the
// modems MAC address.
// We use the computers IP address (the web browser
// received this when the subscriber opened the service
// providers web interface). We also assume that "bostonProvGroup"
// is the provisioning group  used in that locality.

List provGroupList;
provGroupList = provGroupList.add("bostonProvGroup");
Map computerLease = getAllForIPAddress(

            "10.0.14.38",
        // ipAddress: restricted access computer lease

                provGroupList

        // provGroups: List containing provgroup)

// Derive the modem MAC address from the computer's network
// information. The 1,6, is a standard prefix for an Ethernet
// device. The fully qualified MAC address is required by BPR

String modemMACAddress = "1,6," +


        computerLease.getSingleLease().get(RELAY_AGENT_REMOTE_ID);


get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

// Now let's provision the modem
// NO_ACTIVATION will generate a configuration for the
// modem however it will not attempt to reset it
// The configuration will be able to be generated because
// the modem has booted.
// NO_CONFIRMATION is the confirmation mode because we
// are not attempting to reset the modem
// Create a Map for the properties of the modem

Map properties;
// Set the property ModemKeys.PROMISCUOUS_MODE_ENABLED
// to enable promiscuous mode on modem

properties.put(ModemKeys.PROMISCUOUS_MODE_ENABLED, "enabled");

properties.put(ModemKeys.CPE_DHCP_CRITERIA, "provisionedCPE");

add(
        DeviceType.DOCSIS,
                // deviceType: DOCSIS
        modemMACaddress,
                // macAddress: derived from computer lease
        null,
                // hostName: not used in this example
        null,
                // domainName: not used in this example
        "0123-45-6789",
                // ownerID: here, account number from billing system
        "Silver",
                // ClassOfService
```

```
        "provisionedCM",
                // DHCP Criteria: Network Registrar uses this to
                // select a modem lease granting provisioned IP address
        properties
                // properties:
);
```

ステップ 7　ユーザ インターフェイスにより、加入者はコンピュータをリブートするように求められます。

ステップ 8　プロビジョニング クライアントが performOperation(…) を呼び出してモデムをリブートし、プロビジョニングされたアクセス権をモデムに与えます。

```
get-new-batch(AUTOMATIC, NO_CONFIRMATION)

// AUTOMATIC is the activation mode because we are attempting
// to reset the modem so that is receives its new class of service
// NO_CONFIRMATION is the confirmation mode because we don't want
// the batch to fail if we can't reset the modem. The user might
// have power cycled the modem when they rebooted their computer
// send a batch to reset the modem now that the user has been
// notified to reboot their computer

performOperation(
        DeviceOperation.RESET,
                //deviceOperation: Reset operation
        modemMACaddress,
                // macAddress:Modem's MAC address
        null
                // properties : not used
        );
```

ステップ 9　コンピュータをリブートすると、コンピュータが CableHome デバイスの DHCP サーバから新しい IP アドレスを受信します。これで、ケーブル モデムと CableHome デバイスはいずれもプロビジョニングされます。この結果、加入者は CableHome デバイスのイーサネット ポートに多数のコンピュータを接続し、インターネットにアクセスすることができます。

(注)　WAN-Man コンポーネントに提供された設定ファイルによってボックスの WAN-Data コンポーネントがイネーブルになる場合、コンポーネントは無差別モードでプロビジョニングされます。無差別モードは DeviceType.CABLEHOME_WAN_DATA デバイス タイプのテクノロジー デフォルト レベルでイネーブルになることが前提となっています。

リース予約の使用例

この項では、リース予約機能の使用を主とした使用例について説明します。サービス クラス、DHCP 基準、およびライセンスの管理など、標準的な管理操作についてはここでは取り上げません。リース予約の使用例には、次のものがあります。

- サービス プロバイダーの IP アドレスを使用したデバイスのオンライン化（P.C-58）
- 予約の削除と再作成（P.C-60）
- 新しいデバイスに対する古いデバイスの IP アドレスの割り当て（P.C-61）
- 予約の削除と新しい IP アドレスの割り当て（P.C-62）
- 同一の IP アドレスを使用したデバイスのリブート（P.C-63）
- BACC からのデバイスの削除（P.C-64）
- BACC が CCM を使用するときに送信済みバッチが失敗する（P.C-65）
- BACC が CCM を使用しないときに送信済みバッチが失敗する（P.C-65）

リース予約機能の影響を受ける API コール

次の API コールの実装が、リース予約機能をサポートします。

- IPDevice.add(DeviceType DeviceType, String macAddress, String hostName, String domainName, String ownerID, String cosName, String dhcpCriteria, Map Properties)
- IPDevice.changeProperties(String macORFqdn, Map newPropToAdd, List propToDelete)
- IPDevice.changeMACAddress(String macORFqdn, String newMAC)
- IPDevice.delete(String macORFqdn, Boolean deleteDevicesBehind)

サービス プロバイダーの IP アドレスを使用したデバイスのオンライン化

デバイスを BACC システムのデータベースに追加するときに、サービス プロバイダーが BACC プロパティ（IPDeviceKeys.IP_RESERVATION）を使用して、そのデバイスにデバイス固有の IP アドレスを設定します。

求める結果

サービス プロバイダーによってプロパティに設定されたとおりの IP アドレスで、デバイスをオンラインにします。付与された IP アドレスが、そのデバイスに対して予約されます（リース予約）。

ステップ 1　サービス プロバイダーが、BACC システムに新しいデバイスを追加します。サービス プロバイダーは、新しいデバイスに固有の IP アドレス 10.10.10.1 を設定します。

ステップ 2　サービス プロバイダーのユーザ インターフェイスが、デバイス情報（MAC アドレス、FQDN、およびサービス クラスなど）を BACC に渡します。BACC プロパティ（IPDeviceKeys.IP_RESERVATION）が使用され、そのデバイスに対して固有の IP アドレス（10.10.10.1）が予約されます。

```
Map properties;

        // Set the property IPDeviceKeys.IP_RESERVATION to a specific
        // IP address

        properties.put( IPDeviceKeys.IP_RESERVATION, "10.10.10.1");

        // To add a DOCSIS modem:

        get-new-batch(NO_ACTIVATION, NO_CONFIRMATION)

        add(
                 DeviceType.DOCSIS,
                        // deviceType: DOCSIS
                "1,6,01:02:03:04:05:06",
                        // macAddress: scanned from the label
                null,
                        // hostName: not used in this example
                null,
                        // domainName: not used in this example
                "0123-45-6789",
                        // ownerID: here, account number from billing system
                "gold",
                        // classOfService:
                "provisionedCM",
                         // DHCP Criteria: Network Registrar uses this to
                        // select a modem lease granting provisioned IP address
                properties
                        // properties:
                );
```

ステップ 3　新しいデバイスが BACC に登録されます。また、BACC/Network Registrar システムで、MAC アドレス「01:02:03:04:05:06」に対する 10.10.10.1 の予約も作成されます。

ステップ 4　デバイスをリブートすると、デバイスが、サービス プロバイダーによってプロパティに設定されたとおりの IP アドレス（10.10.10.1）を受信します。

API コマンドの処理中にエラーが発生した場合、または変更が RDU データベースにコミットできなかった場合は、必要に応じてロールバックが実行されます。MAC アドレス「01:02:03:04:05:06」に対応する 10.10.10.1 のリース予約がコマンド処理中に作成されていた場合は、コマンド実装によりその予約が BACC/Network Registrar から削除されます。

予約の削除と再作成

予約済みの IP アドレスでデバイスを BACC システムに登録した後で、サービス プロバイダーが、BACC プロパティ（IPDeviceKeys.IP_RESERVATION）を使用して、デバイスに別の IP アドレスを再割り当てします。

求める結果

デバイスが、サービス プロバイダーによってプロパティに設定されたとおりの IP アドレスでリブートされます。予約が削除され、再作成されます。そのデバイスに対して以前割り当てられた IP アドレスは予約解除され、新しい IP アドレスがそのデバイスに与えられ、予約されます（リース予約）。

ステップ 1　デバイスは、予約済みの IP アドレス 10.10.10.1 で BACC に登録されます。

ステップ 2　サービス プロバイダーのアプリケーションが、BACC で次の API コールを行い、予約済みの IP を 10.10.10.5 に変更します。

```
get-new-batch(AUTOMATIC, NO_CONFIRMATION);
// AUTOMATIC is the Activation mode because we are attempting
// to reset the device
// NO_CONFIRMATION is the Confirmation mode because we don't
// want the batch to fail if we can't reset the modem.

// This use case assumes that the DOCSIS modem has been
// previously added to the database

        Map properties;
                // Set the property IPDeviceKeys.IP_RESERVATION to a specific
                // IP address

                properties.put( IPDeviceKeys.IP_RESERVATION, "10.10.10.5");
                // To reassign a different IP to:


                    changeProperties(

                        "1,6,01:02:03:04:05:06",
                        // macAdd
                        properties, null


                     );
```

ステップ 3　MAC アドレス「01:02:03:04:05:06」に対する 10.10.10.1 の予約が、BACC/Network Registrar システムから削除されます。MAC アドレス「01:02:03:04:05:06」に対する 10.10.10.5 の予約が、BACC/Network Registrar システムで作成されます。

ステップ 4　PACE　ディスラプタによるデバイス中断の結果としてデバイスがリブートされた場合（アクティベーション モードには AUTOMATIC を使用）、デバイスは、サービス プロバイダーによってプロパティに設定されたとおりの IP アドレス（10.10.10.5）を受信します。

API コマンドの処理中にエラーが発生した場合、または変更が RDU データベースにコミットできなかった場合は、必要に応じてロールバックが実行されます。コマンドの実装により、デバイスに対して以前の動作設定へのロールバックが試行されます。このとき、MAC アドレス「01:02:03:04:05:06」に対する 10.10.10.1 の予約が削除されていた場合は、その予約が BACC/Network

Registrar システムに再度追加されます。一方、MAC アドレス「01:02:03:04:05:06」に対する 10.10.10.5 の予約がコマンド処理中に作成されていた場合は、その予約が BACC/Network Registrar システムから削除されます。

新しいデバイスに対する古いデバイスの IP アドレスの割り当て

予約済みの IP アドレスでデバイスを BACC システムに登録した後で、サービス プロバイダーが、故障したデバイスを新しい MAC アドレスを持つデバイスに交換します。

求める結果

新しいデバイスが、故障した古いデバイスに与えられたものと同じ IP アドレスでブートされます。デバイスの IP アドレスが変更された場合と同様に、予約が削除され、再作成されます。

ステップ 1　デバイスは、予約済みの IP アドレス 10.10.10.5 で BACC に登録されます。

ステップ 2　サービス プロバイダーが、BACC システムで、既存のデバイスの MAC アドレス（「01:02:03:04:05:06」）を新しいデバイスの MAC アドレス（「01:02:03:04:05:07」）に変更します。

```
get-new-batch(AUTOMATIC, NO_CONFIRMATION);
// NO_ ACTIVATION is the activation mode because we will
// not be able to reset as the new device has not booted
// on the network.
// NO_CONFIRMATION is the confirmation mode because we are
// not trying to reset the device

        // To change the MAC address of a device:

        changeMACAddress (
                "1,6,01:02:03:04:05:06",
                        // old macAddress: unique identifier for the old device
                 "1,6,01:02:03:04:05:07"
                        //// new macAddress: unique identifier for the new device
                 );
```

ステップ 3　MAC アドレス「01:02:03:04:05:06」に対する 10.10.10.5 の予約が、BACC/Network Registrar システムから削除されます。MAC アドレス「01:02:03:04:05:07」に対する 10.10.10.5 の予約が、BACC/Network Registrar システムで作成されます。

ステップ 4　MAC アドレス「01:02:03:04:05:07」を持つデバイスの電源がオンになると、デバイスは、故障した古いデバイスに与えられたものと同じ IP アドレス（10.10.10.5）を受信します。

API コマンドの処理中にエラーが発生した場合、または変更が RDU データベースにコミットできなかった場合は、必要に応じてロールバックが実行されます。コマンドの実装により、デバイスに対して以前の動作設定へのロールバックが試行されます。このとき、MAC アドレス「01:02:03:04:05:06」に対する 10.10.10.5 の予約が削除されていた場合は、その予約が BACC/Network Registrar システムに再度追加されます。一方、MAC アドレス「01:02:03:04:05:07」に対する 10.10.10.5 の予約がコマンド処理中に作成されていた場合は、その予約が BACC/Network Registrar システムから削除されます。

予約の削除と新しい IP アドレスの割り当て

予約済みの IP アドレスでデバイスを BACC システムに登録した後で、デバイスに対する予約済み IP の割り当てが不要になったため、サービス プロバイダーが、固有の IP アドレスの予約を削除します。

求める結果

予約がシステムから削除されます。次に、Network Registrar/BACC が、選択された DHCP 基準に基づいて、適切な IP プールで次に利用可能な IP アドレスを選択し、デバイスに割り当てます。

ステップ 1　デバイスは、予約済みの IP アドレス 10.10.10.5 で BACC に登録されます。

ステップ 2　サービス プロバイダーのアプリケーションが、BACC で次の API コールを行い、予約を削除します。

```
 get-new-batch(AUTOMATIC, NO_CONFIRMATION);
// AUTOMATIC is the Activation mode because we are attempting
// to reset the device
// NO_CONFIRMATION is the Confirmation mode because we don't
// want the batch to fail if we can't reset the modem.


// Add the property IPDeviceKeys.IP_RESERVATION the list to be removed

list.add( IPDeviceKeys.IP_RESERVATION);

// To reassign a different IP to:

changeProperties(
        "1,6,01:02:03:04:05:07",
        // macAdd
        null, list
);
```

ステップ 3　MAC アドレス「1,6,01:02:03:04:05:07」に対する 10.10.10.5 の予約がシステムから削除されます。

ステップ 4　デバイス中断の結果としてデバイスがリブートされた場合は（アクティベーション モードには AUTOMATIC を使用）、動的アドレス割り当てが発生します。Network Registrar/BACC が、デバイスに対して選択および設定された DHCP 基準に基づいて、適切な IP アドレス プールで次に利用可能な IP アドレスを選択し、デバイスに与えます。

API コマンドの処理中にエラーが発生した場合、または変更が RDU データベースにコミットできなかった場合は、必要に応じてロールバックが実行されます。コマンドの実装により、デバイスに対して以前の動作設定へのロールバックが試行されます。このとき、MAC アドレス「01:02:03:04:05:07」に対応する 10.10.10.5 の予約がコマンド処理中に削除されていた場合は、その予約が BACC/Network Registrar システムに再度追加されます。

同一の IP アドレスを使用したデバイスのリブート

BACC/Network Registrar によって与えられたプロビジョニング済みの IP アドレス（動的 IP 割り当てであって予約済み IP ではない）でデバイスを BACC システムに登録した後で、サービス プロバイダーが、BACC プロパティ（IPDeviceKeys.IP_RESERVATION）を使用して、デバイスに別の IP アドレスを再割り当てします。

求める結果

デバイスが、サービス プロバイダーによってプロパティ（IPDeviceKeys.IP_RESERVATION）に設定されたとおりの IP アドレスでリブートされます。その結果、付与された新しい IP アドレスが、そのデバイスに対して予約されます（リース予約）。

ステップ 1　動的 IP アドレスでデバイスが BACC に登録されます。この IP アドレスは、Network Registrar/BACC が、デバイスに対して選択された DHCP 基準に基づいて、適切な IP プールで選択し、デバイスに与えたものです。

ステップ 2　サービス プロバイダーのアプリケーションが、BACC で次の API コールを行い、IP アドレスを再割り当てします。

```
get-new-batch(AUTOMATIC, NO_CONFIRMATION);
// AUTOMATIC is the Activation mode because we are attempting
// to reset the device
// NO_CONFIRMATION is the Confirmation mode because we don't
// want the batch to fail if we can't reset the modem.

Map properties;

// Set the property IPDeviceKeys.IP_RESERVATION to a specific
// IP address

properties.put( IPDeviceKeys.IP_RESERVATION, "10.10.10.1");

// To reassign a different IP to:

changeProperties(

        "1,6,01:02:03:04:05:08",
                // macAdd
                properties, null

        ):
```

ステップ 3　MAC アドレス「01:02:03:04:05:08」に対する 10.10.10.1 の予約が BACC/Network Registrar で作成されます。

ステップ 4　デバイス中断の結果としてデバイスがリブートされた場合（アクティベーション モードには AUTOMATIC を使用）、デバイスは、サービス プロバイダーによってプロパティに設定されたとおりの IP アドレス（10.10.10.1）を受信します。

API コマンドの処理中にエラーが発生した場合、または変更が RDU データベースにコミットできなかった場合は、必要に応じてロールバックが実行されます。コマンドの実装により、デバイスに対して以前の動作設定へのロールバックが試行されます。MAC アドレス「01:02:03:04:05:08」に対する 10.10.10.1 の予約がコマンド処理中に追加されていた場合は、その予約が BACC/Network Registrar システムから削除されます。デバイスをリブートすると、BACC/Network Registrar が、選択された DHCP 基準に基づいて、適切な IP プールで次に利用可能な IP アドレスを選択し、デバイスに与えます。

BACC からのデバイスの削除

サービス プロバイダーが、予約済みの IP を持つ加入者のデバイスを BACC システムから削除します。

求める結果

加入者のデバイスを BACC システムから完全に削除します。付与された IP アドレスが、そのデバイスに対して予約解除されます。

ステップ 1　デバイスは、予約済みの IP アドレス 10.10.10.5 で BACC に登録されます。

ステップ 2　サービス プロバイダーが独自のユーザ インターフェイスを使用して、デバイスを BACC システムから削除します。サービス プロバイダーのユーザ インターフェイスは、BACC クライアントとして機能し、情報を BACC に渡します。BACC がデバイス情報を更新し、デバイスを削除します。

```
delete(
        "1,6,01:02:03:04:05:07",
        // macAdd
        // deleteDevicesBehind ress: unique identifier for this device
        true: deletes CPEs behind this modem.
):
```

ステップ 3　MAC アドレス「01:02:03:04:05:07」に対する 10.10.10.5 の予約も、BACC/Network Registrar システムから削除されます。

API コマンドの処理中にエラーが発生した場合、または変更が RDU データベースにコミットできなかった場合は、必要に応じてロールバックが実行されます。コマンドの実装により、デバイスに対して以前の動作設定へのロールバックが試行されます。MAC アドレス「01:02:03:04:05:07」に対する 10.10.10.5 の予約がコマンド処理中に削除されていた場合は、その予約が BACC/Network Registrar システムに再度追加されます。

BACC が CCM を使用するときに送信済みバッチが失敗する

BACC が、CCM を使用するように設定されています。OSS が、予約を追加または削除するために API 要求を送信しますが、CCM が利用不能になっています（接続ダウン、CCM の設定ミス、CCM ライセンスの問題など）。

求める結果

送信バッチが失敗した場合は、BACC/Network Registrar で予約の追加または削除が行われず、定義済みかつ周知のエラー コードが正常に返されます。

ステップ 1　OSS が、予約を追加または削除するために、P.C-58 の「リース予約機能の影響を受ける API コール」にリストされている API コールを含むバッチを作成し、送信します。

ステップ 2　RDU がバッチを受信し、それを処理します。RDU は処理中に、リース予約関連のタスクに関する外部 CCM コールを行います（P.C-58 の「リース予約機能の影響を受ける API コール」にリストされている API コマンドを使用）。

ステップ 3　CCM が利用不能であるため、エラーが発生します。API コールからの戻りステータス コードが、CommandStatusCodes .CMD_ERROR_CCM_UNREACHABLE に設定されます。

BACC が CCM を使用しないときに送信済みバッチが失敗する

BACC は、CCM を使用するように設定されて**いません**。OSS が、予約を追加または削除するために API 要求を送信します。

求める結果

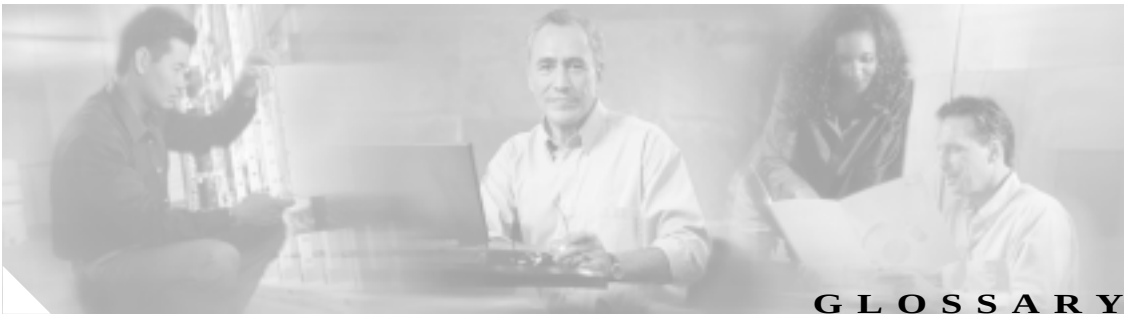
送信済みバッチが失敗します。BACC/Network Registrar システムで予約の追加または削除が行われず、定義済みかつ周知のエラー コードが正常に返されます。

ステップ 1　OSS が、予約を追加または削除するために、P.C-58 の「リース予約機能の影響を受ける API コール」にリストされている API コールを含むバッチを作成し、送信します。

ステップ 2　RDU がバッチを受信し、それを処理します。RDU は処理中に、CCM がリース予約機能について設定されていないことを検出します（P.C-58 の「リース予約機能の影響を受ける API コール」にリストされている API コマンドを使用）。

ステップ 3　エラーが発生します。API コールからの戻りステータス コードが、CommandStatusCodes .CMD_ERROR_CCM_NOT_CONFIGURED に設定されます。

■ リース予約の使用例



GLOSSARY

A

API アプリケーション プログラミング インターフェイス（Application programming interface）。サービスへのインターフェイスを定義する関数呼び出し規定の仕様です。

B

BACC ブロードバンド モデムの構成と管理を行う有線サービス プロバイダーの統合ソリューションで、加入者の自動登録とアクティベーションを可能にし、これを管理します。BACC は大量のデバイスをサポートできるスケーラブルな製品です。

Broadband Access Center for Cable 「BACC」を参照。

C

CMTS ケーブル モデム ターミネーション システム（Cable modem termination system）。CMTS は、デジタル信号をケーブル ネットワーク上のケーブル モデムと交換するコンポーネントです。CMTS は、通常、プロバイダーのローカル オフィスにあります。

CMTS 共有秘密情報 「共有秘密情報」を参照。

CPE 顧客宅内装置（Customer premises equipment）。電話、コンピュータ、モデムなど、顧客側で用意され、インストールされる着信側機器です。

D

Device Provisioning Engine 「DPE」を参照。

DOCSIS 共有秘密情報 BACC 配備の中で、DOCSIS デバイス間の通信に使用される共有秘密情報。

Data Over Cable Service Interface Specification 「DOCSIS」を参照。

DOCSIS Data over cable service interface specification。DOCSIS は、ケーブルテレビ システム ネットワーク上での高速データの配信に必要なケーブル モデムの機能性を定義します。

DPE Device provisioning engine。DPE は、BACC のスケーラビリティを保証し、デバイスへの設定ファイルのダウンロードなどの構成要求を処理するために、デバイス情報をキャッシュします。

DSTB デジタル セットトップ ボックス（Digital set-top box）。テレビをインターネットへのユーザ インターフェイスにして、デジタル テレビ信号の受信とデコードを行うデバイスです。

F

FQDN 完全修飾ドメイン名（Fully qualified domain name）。FQDN は、ホスト名以外も含む、システムの完全名です。たとえば、cisco がホスト名で、www.cisco.com が FQDN です。

I

IP アドレス IP アドレスは、インターネットにパケットで送信される情報の送信者または受信者を識別する 32 ビットの数値です。

K

KDC 限定された Kerberos 機能を実装する鍵発行局。PacketCable MTA のプロビジョニングに使用します。

M

MAC アドレス LAN に接続するすべてのポートまたはデバイスに必要な、標準化されたデータリンク層アドレス。ネットワークのその他のデバイスは、これらのアドレスを使用して、ネットワークで特定のポートを検索し、ルーティング テーブルとデータ構造を作成および更新します。MAC アドレスの長さは 6 バイトで、IEEE が管理します。ハードウェア アドレス、MAC レイヤ層アドレス、物理アドレスとも言います。ネットワーク アドレスと比較してください。

MSO マルチプル サービス オペレータ（Multiple service operator）。複数のケーブル TV またはブロードバンド システムを運営する企業のことです。

MTA ブロードバンド（PacketCable）ネットワークの顧客側の終端装置。

N

NAT ネットワーク アドレス変換。グローバルに一意な IP アドレスを使用する必要性を減らすメカニズムです。NAT を使用すると、グローバルに一意でないアドレスをグローバルにルーティング可能なアドレス空間に変換することによって、このようなアドレスを持つ組織をインターネットに接続できます。Network Address Translation とも言います。

NR Cisco Network Registrar。ネットワーク ポリシーおよびサービス ポリシーに基づき、IP アドレス、構成パラメータ、DNS 名を DOCSIS ケーブル モデムおよび PC に提供するソフトウェア製品です。

NTP ネットワーク タイム プロトコル（Network Time Protocol）。NTP は、ネットワークを通じてサーバ クロックを同期させるためのプロトコルです。

R

RDU Regional distribution unit。RDU は、BACC プロビジョニング システムのプライマリ サーバです。デバイス構成の生成を管理し、すべての API 要求を処理し、BACC システムを管理します。

T

TFTP Trivial File Transfer Protocol。あるコンピュータから別のコンピュータにネットワーク経由でファイルを転送するファイル転送プロトコル（FTP）の簡素化したバージョン。

TLV Type-Length-Value。DOCSIS または PacketCable 設定ファイル内のタプルです。

Trivial File Transfer Protocol 「TFTP」を参照。

Type Length Value 「TLV」を参照。

U

uBr ユニバーサル ブロードバンド ルータ（Universal Broadband Router）。Cisco 7246、7223 などがあります。DOCSIS CMTS の Cisco ルータ実装です。

V

Voice over IP 「VoIP」を参照。

VoIP Voice over IP。VoIP は、IP ベースのデータ ネットワークによる通話呼および FAX 送信を可能にし、最適な QoS と優れた費用対効果を発揮します。

X

XGCP ネットワーク間でデータを受け渡すために使用するゲートウェイ コントロール プロトコル（Gateway Control Protocol）。M（メディア）GCP と S（シンプル）GCP が含まれています。

あ

アクティブ ログ これらのデータベース ログ ファイルには、まだデータベースに書き込まれていないデータが含まれています。冗長になるまで、アクティブ ログ ファイルは保存しておく必要があります。「冗長ログ」と「削除可能」ログも参照。

アラート ネットワークの問題をオペレータまたは管理者に通知する syslog または SNMP メッセージ。

え

エージェント ウォッチドッグ エージェントは、RDU、JRun、SNMP の各エージェントなどの BAC コンポーネント プロセスを監視、中止、開始、再開するデーモン プロセスです。

か

鍵発行局 「KDC」を参照。

監査ログ RDU データベースの大きな変更の概要が含まれているログ ファイル。システム デフォルト、テクノロジー デフォルト、DHCP 基準、サービス クラスの変更が含まれます。

完全修飾ドメイン名 「FQDN」を参照。

き

キャッシング 前のトランザクションで学習した情報を後のトランザクションで処理するために使用する複製の形式。

共有秘密情報 2 台のサーバまたはデバイス間で安全な通信を行うために使用する文字列。

く

クライアントクラス 共通ネットワークに接続されたユーザに、固有のサービスを提供する Network Registrar の機能。クライアントクラスは、デバイスに固有の DHCP サービスを提供するために、BACC DHCP 基準で使用されます。

け

ケーブル モデム ターミネーション システム 「CMTS」を参照。

こ

構成の生成 DHCP、TFTP、または SNMP を使用してデバイスに配送される属性のセットを組み合せるプロセス。

顧客宅内装置 「CPE」を参照。

さ

削除可能ログ データベースのログ ファイルは、バックアップされるか、このログ ファイルのデータを含むデータベース全体がバックアップされると、削除可能になります。「アクティブ ログ」と「冗長ログ」も参照。

し

冗長性 インターネットワーキングでの、デバイス、サービス、接続などの複製。障害が発生した場合は、障害が発生したデバイス、サービス、接続の代わりに、冗長なデバイス、サービス、接続が機能を実行します。

冗長ログ データベースのログ ファイルは、データがデータベースに書き込まれると、冗長になります。「アクティブ ログ」と「削除可能ログ」も参照。

せ

静的設定ファイル デバイスの設定ファイルとして使用します。たとえば、gold.cm という静的設定ファイルは、gold DOCSIS サービス クラスを設定します。BACC は、このファイル タイプをその他のバイナリ ファイルと同様に扱います。

設定ファイル プロビジョニングするデバイスの構成パラメータが含まれているファイル。

選択タグ Network Registrar スコープに関連付けられた選択タグ。スコープに関連付けられたクライアントおよびクライアントクラスを定義します。

た

帯域幅 ネットワーク信号で利用可能な最高周波数と最低周波数の差。あるネットワーク メディアまたはプロトコルの定格スループット キャパシティを表すこともあります。

タプル プログラミング言語では、順序付けされた値のセット。データ型としてのタプルは、一般的に、あるプログラムから別のプログラムにパラメータ文字列を渡したり、リレーショナル データベースの値属性のセットを表すために使用されます。

て

テンプレート ファイル DOCSIS または PacketCable MTA オプションおよび値を含むテキスト ファイル。DOCSIS または PacketCable MTA サービス クラスと組み合せて使用して、動的ファイル生成を行います。

と

動的設定ファイル テンプレート ファイルを使用して、動的に作成される設定ファイル。プロビジョニング プロセスでの、柔軟性とセキュリティを高めます。

ね

ネットワーク アドレス変換 「NAT」を参照。

ネットワーク オペレータ 日常的にネットワークを監視および制御し、アラームの確認と対応、スループットの監視、新しい回線の構成、問題の解決などの作業を実行する人。「ネットワーク管理者」も参照。

ネットワーク管理者 ネットワークの運用、メンテナンス、および管理を担当する人。「ネットワーク オペレータ」も参照。

ネットワーク タイム プロトコル 「NTP」を参照。

は

パブリッシング プロビジョニング情報を外部データストアにリアルタイムで発行すること。データをデータストアに書き込むために、パブリッシング プラグインを開発する必要があります。

ふ

ブロードバンド 複数の独立した信号を 1 本のケーブルに多重化する転送システム。テレコミュニケーションの用語では、音声レベルのチャネル（4 kHz）を超える帯域幅のチャネルのことです。LAN の用語では、アナログ シグナリングを使用する同軸ケーブルのことです。

プロビジョニング API オペレーティング システムにさまざまな機能を実行させるために、プログラムで使用できる一連の BACC 関数。

プロビジョニング グループ ネットワーク トポロジまたは地理的条件に基づいて DPE サーバと DHCP サーバをグループ化すること。

ま

マルチプル サービス オペレータ 「MSO」を参照。

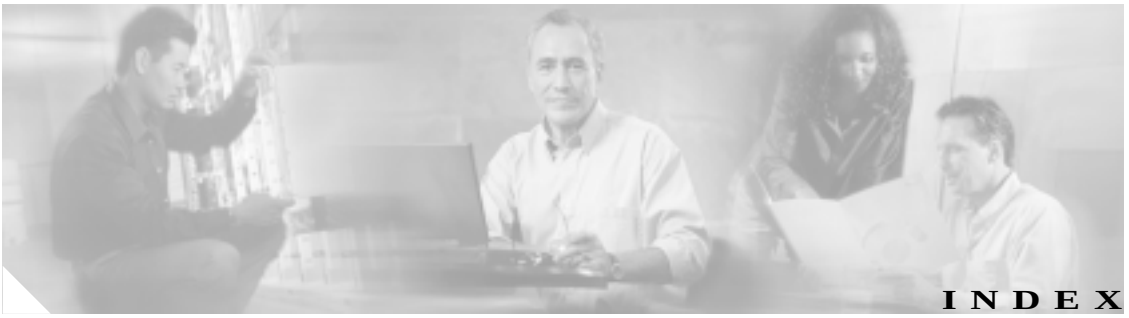
め

メディア ターミナル アダプタ 「MTA」を参照。

り

領域 単一の Kerberos データベースと鍵発行局のセットによる論理ネットワーク。

領域名 慣習的に、領域名はすべて大文字を使用して、領域とインターネット ドメインを区別します。「領域」を参照。



A

ATA 186 のデフォルト、設定　10-8
ATA 188 のデフォルト、設定　10-10

B

BACC（BAC)、定義　1
BACC の機能、概要　1-1
BACC の使用方法　9-1 – 9-28
　サーバ、表示　9-21 – 9-28
　　DPE、リスト　9-21
　　Network Registrar 拡張ポイントのリスト　9-24
　　RDU の詳細　9-27
　　プロビジョニング グループ、リスト　9-26
　デバイス、管理　9-5 – 9-17
　　Manage Devices ページ　9-5
　　コントロール　9-6
　　削除、デバイス　9-15
　　説明　9-14
　　デバイス構成、再生成　9-16
　　デバイスの関連付けと関連付け解除　9-16
　　デバイスの検索　9-8
　　デバイスの修正　9-15
　　デバイスの詳細、表示　9-9
　　デバイスの追加　9-14
　　デバイスの登録解除　9-17
　　デバイスのリセット　9-17
　ノード、管理　9-18 – 9-20
　　削除　9-20
　　修正　9-20
　　詳細、表示　9-20
　　追加　9-19
　　ノードに対するノード タイプの関連付けと関連付け解除　9-20
　ノード タイプ、管理　9-18
　　削除、ノード タイプ　9-19
　　修正、ノード タイプ　9-19
　　追加、ノード タイプ　9-18
　　ノードに対するノード タイプの関連付けと関連付け解除　9-20
　ユーザの管理　9-2 – 9-4
　　削除、ユーザ　9-4
　　修正、ユーザ　9-3
　　新規ユーザの追加　9-2
BACC の設定　10-1 – 10-41
　DHCP 基準　10-25 – 10-26
　　基準の削除　10-26
　　基準の修正　10-26
　　基準の追加　10-25
　FQDN、自動生成　10-40 – 10-41
　　形式　10-40
　　検証　10-41
　　プロパティ　10-40
　　例　10-41
　RDU および DPE 上での SNMPV3 クローン作成　10-39
　　キー関連情報　10-39
　　キーの生成　10-39
　RDU 拡張、管理　10-34 – 10-35
　　新しいクラス、作成　10-34
　　カスタム拡張ポイント、インストール　10-34
　　表示　10-35
　SRV レコード、Network Registrar DNS サーバの　10-38
　外部ファイル、管理　10-27 – 10-31
　　ファイルのエクスポート　10-31
　　ファイルの削除　10-31
　　ファイルの置換　10-30
　　ファイルの追加　10-28
　　ファイルの表示　10-29
　カスタム プロパティ　10-7
　サービス クラス　10-2 – 10-6
　　クラスの追加　10-3
　　削除　10-5

修正　10-4
デフォルト　10-8 – 10-24
ATA 186 のデフォルト　10-8
ATA 188 のデフォルト　10-10
CableHome WAN Defaults　10-10
Computer Defaults　10-13
DOCSIS Defaults　10-14
Network Registrar Defaults　10-16
PacketCable Defaults　10-18
設定オプション、選択　10-8
プロビジョニング データ、パブリッシング　10-36 – 10-37
データストアの変更　10-36
プラグイン設定、変更　10-37
ライセンス キー、管理　10-32 – 10-33
ライセンスの修正　10-33
ライセンスの追加　10-33

C

CableHome
WAN Defaults、設定　10-10
WAN-Man Defaults、設定　10-12
設定　6-1 – 6-4
Device Provisioning Engine　6-4
Network Registrar　6-3
RDU　6-3
ノンセキュア プロビジョニング フロー　6-2
プロビジョニング
サポート　1-3
チェックリスト（ノンセキュア）　3-14
CableHome の設定　6-1 – 6-4
DPE　6-4
Network Registrar　6-3
RDU　6-3
CableLabs サービス プロバイダー証明書信頼階層　5-22
運用上の補助証明書　5-25
PacketCable サーバ証明書　5-26
鍵発行局（KDC）証明書　5-25
配送機能（DF）証明書　5-26
サービス プロバイダー CA 証明書　5-23
ルート証明書　5-22
CMTS（ケーブル モデム ターミネーション システム）
共有秘密情報、定義　4
定義　1
Configuration メニューについて　8-6

D

Devices メニューについて　8-6
DHCP
Network Registrar、および～　2-12
基準のデフォルト、設定　10-25 – 10-26
基準の削除　10-26
基準の修正　10-26
基準の追加　10-25
状態、および DOCSIS 設定　4-6
disk_monitor.sh ツール　12-54
DNS（ドメイン ネーム システム）、Network Registrar、および～　2-12
DOCSIS（Data Over Cable Service Interface Specification）
DOCSIS ネットワークのトラブルシューティング　4-5
機能　4-4 – 4-5
DOCSIS 1.0、1.1、2.0 のサポート　4-5
動的設定 TLV　4-4
共有秘密情報、定義　4
高速データのサポート　1-2
設定　4-1 – 4-32
ネットワーク層以上　4-6 – 4-9
ワークフロー、完全な　4-1 – 4-3
ワークフロー、チェックリスト　3-7
定義　1
DOCSIS の設定
ネットワーク層以上
DHCP 状態　4-6
ToD 状態　4-7
セキュリティ アソシエーション状態　4-7
設定ファイル状態　4-8
動作状態　4-9
登録状態　4-8
プライバシー状態の確立　4-8
ワークフロー
完全な　4-1 – 4-3
チェックリスト　3-7
DPE（Device Provisioning Engine）
BACC のアーキテクチャ、および～
dpe.log ファイル、表示　2-24
ログ　2-22
dpe.log ファイル、表示　2-24
DSS、および～　2-9

DSS のリセット 2-10
SNMPV3 クローン作成、設定 10-39
キー関連情報 10-39
キーの生成 10-39
Solaris DPE のアラート A-3
DPE-1-102 A-3
DPE-1-104 A-3
DPE-1-109 A-3
Solaris DPE のチェックリスト 3-4 - 3-5
TACACS+、および DPE 認証 2-7
クライアント設定 2-8
特権レベル 2-8
TFTP サーバ、および～ 2-9
サーバの割り当て 2-8
種類 2-6
Solaris DPE 2-7
ハードウェア DPE（Device Provisioning Engine） 2-6
設定 6-4
説明 2-6
定義 1
ハードウェア DPE のチェックリスト 3-3 - 3-4
ライセンス キー 2-7
リスト
現在登録されている DPE 9-21
サーバ 8-6
DSS（DOCSIS 共有秘密情報）、および DPE
DSS のリセット 2-10
説明 2-9
DSTB、定義 2

E

Ethereal、パケット キャプチャ ツール 5-12
Euro-PacketCable
音声サービスのサポート 1-2
サポート、および KDC 2-15
設定 5-6

F

FQDN（完全修飾ドメイン名）
自動生成 10-40 - 10-41
形式 10-40
検証 10-41
プロパティ 10-40
例 10-41
定義 2

G

GUI（「管理者のユーザ インターフェイス」を参照）

I

IP アドレス、定義 2
ISP、選択 11-3

K

KDC（鍵発行局）
BACC のアーキテクチャ、および～ 2-14 - 2-17
Euro-PacketCable のサポート 2-15
証明書 2-16
デフォルトの KDC のプロパティ 2-14
複数領域のサポート 2-17
ライセンス 2-16
証明書、管理 12-42 - 12-44
PKCert ツールの実行 12-42
検証 12-44
作成 12-43
定義 2
Keygen ツール 12-47 - 12-48

M

MAC アドレス、定義 2
MIB
BACC のアーキテクチャ、および～ 2-18
CableHome、および SNMP Varbind 12-7
DOCSIS、および SNMP Varbind 12-6
DPE SNMP エージェント、および MIB サポート 2-19
Euro-PacketCable と PacketCable の音声設定 5-7
PacketCable、および SNMP Varbind 12-7
TLV 38 と MIB のサポート 5-6
MSO、定義 2
MTA（メディア ターミナル アダプタ）
製造業者 CVC、および DOCSIS 5-21
定義 2

N

NAT（ネットワーク アドレス変換）、定義　2
Network Registrar
　DHCP、および～　2-12
　DNS、および～　2-12
　DNS サーバの SRV レコード、設定　10-38
　SRV レコード、DNS サーバの、設定　10-38
　アーキテクチャ　2-12 - 2-13
　拡張ポイントのアラート　A-5
　　NR_EP-1-106　A-5
　　NR_EP-1-107　A-5
　　NR_EP-6-108　A-5
　　NR_EP-6-109　A-5
　　NR_EP-6-110　A-5
　拡張ポイントのリスト　9-24
　サーバ、リスト　8-6
　設定　6-3
　説明　2-12 - 2-13
　　DHCP、および～　2-12
　　DNS、および～　2-12
　　リース予約　2-13
　デフォルト、設定　10-16
　リース予約　2-13
　ワークフロー チェックリスト　3-6
Network Registrar の設定　6-3
　SRV レコード、DNS サーバの　10-38
　デフォルト　10-16
　ワークフロー チェックリスト　3-6
NR、定義　2
NRProperties.sh ツール　12-45 - 12-46
NTP、定義　2

P

PacketCable
　BACC プロパティ、DHCP オプションへのマッピング　B-1 - B-3
　　オプション 122 と BACC プロパティの比較　B-2
　　オプション 177 と BACC プロパティの比較　B-3
　MTA、SNMPV3 クローン作成、および～　10-39
　　キー関連情報　10-39
　　キーの生成　10-39
　音声サービスのサポート
　　Euro-PacketCable　1-2
　　ノンセキュア　1-2
　　標準　1-2
　デフォルト、設定　10-18
　　RDU Defaults　10-20
　　xGCP Gateway Control Protocol Defaults　10-24
　　システム デフォルト　10-22
　ワークフロー チェックリスト　3-8 - 3-14
　　Euro-PacketCable　3-12
　　PacketCable　3-8
　　ノンセキュア PacketCable　3-10
PacketCable 音声設定　5-1 - 5-31
　eMTA プロビジョニング、トラブルシューティング　5-8 - 5-11
　　基本変数　5-10
　　コンポーネント　5-8
　Euro-PacketCable の MIB　5-7
　Euro-PacketCable　5-6
　PacketCable BASIC　5-5 - 5-6
　　SNMP v2C 通知　5-6
　　TLV 38 と MIB のサポート　5-6
　PacketCable のセキュアな　5-2 - 5-4
　　PacketCable のフロー　5-2
　証明書信頼階層　5-17 - 5-31
　　CableLabs サービス プロバイダー　5-22
　　MTA デバイス証明書　5-21
　　MTA デバイス証明書階層　5-19
　　検証　5-18
　　コード検証　5-28
　　失効　5-28
　トラブルシューティングのシナリオ　5-13 - 5-16
　トラブルシューティングのツール　5-12
　　Ethereal、SnifferPro など　5-12
　　ログ　5-12
PacketCable の eMTA プロビジョニング、トラブルシューティング　5-8 - 5-11
　基本変数　5-10
　　MTA 設定ファイル　5-11
　　証明書　5-10
　　スコープ選択タグ　5-11
　コンポーネント　5-8
　　Call Management Server　5-10
　　DHCP サーバ　5-9
　　DNS サーバ　5-9
　　PacketCable プロビジョニング サーバ　5-9
　　鍵発行局　5-9
　　組み込み型 MTA　5-8
PacketCable の証明書信頼階層　5-17 - 5-31

MTA デバイス証明書 5-21
MTA デバイス証明書階層 5-19
MTA 製造業者証明書 5-20
MTA ルート証明書 5-19
検証 5-18
PacketCable の設定 5-1 - 5-31
Euro-PacketCable 5-6
PacketCable BASIC 5-5
SNMP v2C 通知 5-6
TLV 38 と MIB のサポート 5-6
PacketCable のセキュアな 5-2
証明書信頼階層 5-17 - 5-31
CableLabs サービス プロバイダー証明書階層 5-22
MTA 階層 5-19
MTA デバイス証明書 5-21
コード検証証明書階層 5-28
証明書失効 5-28
証明書の検証 5-18
トラブルシューティング、eMTA プロビジョニング 5-8, 5-11
基本変数 5-10
コンポーネント 5-8
トラブルシューティングのシナリオ 5-13 - 5-16
トラブルシューティングのツール 5-12
Ethereal、SnifferPro など 5-12
ログ 5-12
PKCert.sh ツール 12-42 - 12-44
KDC 証明書、検証 12-44
KDC 証明書、作成 12-43
実行 12-42

R

RDU（Regional Distribution Unit）
SNMPV3 クローン作成、設定 10-39
キー関連情報 10-39
キーの生成 10-39
アラート A-2
BPR-RDU-4-1140 A-2
RDU-1-101 A-2
RDU-1-103 A-2
RDU-1-111 A-2
RDU-1-115 A-2
エラー メッセージ A-6 - A-9
AddReservation: AX_ETIME A-8
AddReservation:FORWARD_FAILED A-7
AddReservation: INVALID_OBJECT A-8
AddReservation: INVALID_PARENT A-7
AddReservation: INVALID_SECOND_PARENT A-7
AX_EIO A-9
AX_EPIPE A-9
OBJECT_EXISTS A-6
RemoveReservation: NOT_FOUND A-7
Selection-criteria exclusion tags ignored A-8
拡張、管理 10-34 - 10-35
新しいクラス、作成 10-34
カスタム拡張ポイント、インストール 10-34
表示 10-35
詳細、表示 9-27
設定、および CableHome 6-3
WAN-Data 6-4
WAN-Man 6-3
説明 2-4 - 2-5
構成の生成 2-4
サービス レベル選択 2-5
フェールオーバー 2-5
定義 3
データベースの移行 7-8
リスト 8-6
ログ 2-22
ログ レベル ツール 12-39 - 12-41
現在のログ レベル、表示 12-41
使用方法 12-39
設定 12-40
ワークフロー チェックリスト 3-2

S

Servers メニューについて 8-6
SnifferPro、パケット キャプチャ ツール 5-12
SNMP
PacketCable eMTA 上でのクローン作成（使用例） C-41
SNMP エージェント
開始 12-51
コミュニティ、削除 12-51
コミュニティ、追加 12-50
設定、リスト 12-53
停止 12-51
場所、変更 12-52

snmpAgentCfgUtil.sh コマンド　12-49
SNMP 通知タイプ、指定　12-53
SNMP の連絡先、新規設定　12-52
SNMP リスニング ポート、指定　12-52
ホスト、削除　12-50
ホスト、追加　12-49
SNMPV3 クローン作成、RDU および DPE 上での設定　10-39
キー関連情報　10-39
キーの生成　10-39
SRV レコード、Network Registrar DNS サーバの、設定　10-38
SUI（サンプル ユーザ インターフェイス）
BACC のアーキテクチャ、および～　2-24
サンプルの sampleui.properties ファイル　11-12 - 11-14
設定　11-1 - 11-14
ISP、選択　11-3
開始および停止　11-2
管理者アクセス レベル　11-4
技術者ログイン、使用方法　11-3
サービス クラス　11-3
サンプルの設定オプション　11-3 - 11-4
無差別モード　11-3
説明　11-2
SUI の設定　11-1 - 11-14
加入者プロビジョニングの例　11-5 - 11-7
標準の顧客宅内機器登録　11-5
無差別モードの顧客宅内機器登録　11-6
管理者プロビジョニングの例　11-8 - 11-11
アカウントの検索　11-8
アカウントの保守　11-9
サンプルの sampleui.properties ファイル　11-12 - 11-14
サンプルの設定オプション　11-3 - 11-4
ISP、選択　11-3
管理者アクセス レベル　11-4
技術者ログイン、使用方法　11-3
サービス クラス　11-3
無差別モード　11-3

T

TFTP、定義　3
TLV、定義　3
ToD 状態、DOCSIS 設定のための確立　4-7
Trivial File Transfer Protocol、定義　3
Type Length Value、定義　3

U

uBr、定義　3
uBR7246 デバイスとデバッグ コマンドに関する注意　4-7, 4-19
Users メニューについて　8-7
管理者　8-7
読み取り / 書き込みユーザ　8-7
読み取り専用ユーザ　8-7

V

VoIP、定義　3

X

XGCP、定義　3

あ

アーキテクチャ　2-1 - 2-24
DPE　2-6
DSS、および～　2-9
TACACS+、および DPE 認証　2-7
TFTP サーバ、および～　2-9
サーバの割り当て　2-8
種類　2-6
ライセンス キー　2-7
KDC　2-14 - 2-17
Euro-PacketCable のサポート　2-15
証明書　2-16
デフォルトの KDC のプロパティ　2-14
複数領域のサポート　2-17
ライセンス　2-16
MIB　2-18
Network Registrar　2-12 - 2-13
DHCP、および～　2-12
DNS、および～　2-12
リース予約　2-13
RDU　2-4 - 2-5
構成の生成　2-4
サービス レベル選択　2-5
フェールオーバー　2-5

エージェント　2-19 - 2-21
BACC エージェント　2-20
SNMP エージェント　2-19
管理者のインターフェイス　2-24
サンプル ユーザ インターフェイス　2-24
説明　2-2
登録モード　2-3
混在モード　2-3
標準モード　2-3
無差別モード　2-3
ローミング モード　2-3
プロビジョニング グループ　2-11
ロギング　2-22 - 2-24
DPE のログ　2-22
dpe.log ファイル、表示　2-24
アラート メッセージ　A-1 - A-5
Network Registrar 拡張ポイントのアラート　A-5
NR_EP-1-106　A-5
NR_EP-1-107　A-5
NR_EP-6-108　A-5
NR_EP-6-109　A-5
NR_EP-6-110　A-5
RDU のアラート　A-2
BPR-RDU-4-1140　A-2
RDU-1-101　A-2
RDU-1-103　A-2
RDU-1-111　A-2
RDU-1-115　A-2
Solaris DPE のアラート　A-3
DPE-1-102　A-3
DPE-1-104　A-3
DPE-1-109　A-3
アラート、定義　3
エージェントのアラート　A-4
AGENT-3-9001　A-4
AGENT-3-9002　A-4
AGENT-3-9003　A-4
AGENT-6-9004　A-4
AGENT-6-9005　A-4
メッセージ形式　A-1

え

エージェント、BACC アーキテクチャ
エージェント、定義　3
エージェント、BACC のアーキテクチャおよび～ 2-19 - 2-21
BACC エージェント　2-20
監視対象プロセス　2-20
コマンドライン　2-20
DPE SNMP エージェント
MIB サポート　2-19
SNMP エージェント　2-19
エージェントのアラート（「エージェントのアラート」を参照）
エラー メッセージ、RDU　A-6 - A-9
AddReservation: AX_ETIME　A-8
AddReservation:FORWARD_FAILED　A-7
AddReservation: INVALID_OBJECT　A-8
AddReservation: INVALID_PARENT　A-7
AddReservation: INVALID_SECOND_PARENT　A-7
AX_EIO　A-9
AX_EPIPE　A-9
OBJECT_EXISTS　A-6
RemoveReservation: NOT_FOUND　A-7
Selection-criteria exclusion tags ignored　A-8

お

音声サービスのサポート　1-2
Euro-PacketCable　1-2
PacketCable　1-2
PacketCable、ノンセキュア　1-2
オンライン状態
online、online(d)、online(pk)、online(pt) 状態　4-26
トラブルシューティング　4-10

か

外部ファイル、管理　10-27 - 10-31
エクスポート　10-31
削除　10-31
置換　10-30
追加　10-28
表示　10-29
概要
BACC　1-1 - 1-3
機能と利点　1-1
サポート対象の技術　1-2
加入者プロビジョニングの例　11-5 - 11-7

標準の顧客宅内機器登録　11-5
新しいケーブル モデムと新しいコンピュータ　11-5
既存のケーブル モデムと新しいコンピュータ　11-6
既存のコンピュータの ISP、変更　11-6
無差別モードの顧客宅内機器登録　11-6
新しいケーブル モデムと新しいコンピュータ　11-7
既存のケーブル モデムと新しいコンピュータ　11-7
監査ログ、定義　4
管理者のユーザ インターフェイス　8-1 - 8-8
BACC のアーキテクチャ、および～　2-24
アクセス　8-2
スクロール　8-8
ナビゲート　8-5
Configuration メニュー　8-6
Devices メニュー　8-6
Main Menu　8-6
Nodes メニュー　8-7
Servers メニュー　8-6
Users メニュー　8-7
メニュー バー　8-5
ログアウト　8-4
ログイン　8-2
管理者プロビジョニングの例　11-8 - 11-11
アカウントの検索　11-8
IP アドレスによる　11-8
MAC アドレスによる　11-8
アカウント番号による　11-8
アカウントの保守　11-9
アカウントの削除　11-11
新しいアカウント、登録　11-9
ケーブル モデム、管理　11-10
コンピュータ、管理　11-10
サービス クラス、管理　11-9

き

共有秘密情報
DSS（DOCSIS 共有秘密情報）
DHCP、および～　2-9
説明　2-9
リセット　2-10
設定ファイル ユーティリティ、および　12-31
定義　4

く

クライアントクラス、定義　4

け

ケーブル モデムの状態、トラブルシューティング　4-10 - 4-32
DHCP
init(d)　4-18
init(i)　4-20
reject(pk) と reject(pt)　4-29
TOD 交換
init(t)　4-23
オプション ファイル転送開始
init(o)　4-25
オフライン　4-11
オンライン　4-10
登録
reject (c)　4-32
reject (m)　4-31
レンジング プロセス
init(r1)、init(r2)、および init(rc)　4-16

こ

構成の生成、定義　4
高度な概念（「ツールと高度な概念」を参照）
コード検証証明書階層　5-28
CableLabs コード検証 CA 証明書　5-29
CableLabs コード検証ルート CA 証明書　5-29
CVC の全般的要件　5-28
サービス プロバイダー コード検証証明書　5-31
証明書失効リスト、CVC の　5-31
製造業者コード検証証明書　5-30
顧客宅内装置、定義　4

さ

サーバ、表示　9-21 - 9-28
DPE、リスト　9-21
RDU の詳細　9-27
プロビジョニング グループ、リスト　9-26
サービス クラス
SUI の設定サンプル　11-3
管理、管理者プロビジョニングの例　11-9

設定　10-2 - 10-6
クラスの削除　10-5
クラスの修正　10-4
クラスの追加　10-3
サービス クラス（「サービス クラス」を参照）
削除可能ログ、定義　4

し

冗長性、定義　4
冗長ログ、定義　4
証明書失効　5-28
使用例
PacketCable eMTA 上での SNMP クローン作成　C-41
PacketCable eMTA の差分プロビジョニング　C-43
イベントを使用した RDU 接続の監視　C-32
オプティミスティック ロッキング　C-46
加入者の帯域幅、一時的なスロットリング　C-48
加入者のディセーブル化　C-8
加入者のデバイスの登録解除と削除　C-13
既存のモデムの交換　C-24
既存のモデムの修正　C-12
事前プロビジョニング
CableHome Wan-Man　C-49
PacketCable eMTA　C-39
動的設定ファイルを使用した DOCSIS モデム　C-45
無差別モードでの最初のアクティベーション　C-21
モデムおよびセルフプロビジョニングされたコンピュータ　C-10
取得
CableHome Wan-Man のデバイス機能　C-53
ベンダープレフィックスに一致するデバイス　C-37
使用例について　C-1 - C-2
セルフプロビジョニング
CableHome Wan-Man　C-55
NAT を使用した最初のアクティベーション　C-26
固定標準モードでのモデムとコンピュータ　C-3
無差別モードでの最初のアクティベーション　C-16
追加
NAT を持つモデムの背後への新しいコンピュータ　C-29
固定標準モードでの新しいコンピュータ　C-6
無差別モードでの 2 台目のコンピュータ　C-25
デバイスの詳細情報の取得　C-34
デフォルトのサービス クラスを使用した検索　C-35
ファイアウォール設定を持つ CableHome　C-51
別の DHCP スコープへのデバイスの移動　C-30
無差別モードでの 100 個のモデムの一括プロビジョニング　C-19
リース予約の使用例　C-58
BACC が CCM を使用しないときに送信済みバッチが失敗する　C-65
BACC が CCM を使用するときに送信済みバッチが失敗する　C-65
BACC からのデバイスの削除　C-64
新しいデバイスに対する古いデバイスの IP アドレスの割り当て　C-61
サービス プロバイダーの IP アドレスを使用したデバイスのオンライン化　C-58
同一の IP アドレスを使用したデバイスのリブート　C-63
予約の削除と新しい IP アドレスの割り当て　C-62
予約の削除と再作成　C-60
リース予約の影響を受ける API コール　C-58
ロギング
イベントを使用したデバイス削除　C-31
イベントを使用したバッチ完了　C-33

せ

静的設定ファイル、定義　5
セキュリティ アソシエーション状態、および DOCSIS 設定　4-7
設定のワークフローとチェックリスト　3-1 - 3-14
技術のワークフロー　3-7 - 3-14
CableHome プロビジョニング（ノンセキュア）　3-14
DOCSIS のチェックリスト　3-7
PacketCable のチェックリスト　3-8 - 3-14
コンポーネントのワークフロー　3-2 - 3-6
DPE のチェックリスト　3-3 - 3-4
Network Registrar のチェックリスト　3-6

RDU のチェックリスト　3-2
Solaris DPE のチェックリスト　3-4 - 3-5
設定ファイル、定義　5
設定ファイル ユーティリティ、使用方法　12-25 - 12-38
PacketCable BASIC フロー、有効化　12-38
外部テンプレート ファイルの解析　12-29
実行　12-25
使用方法　12-27
テンプレート ファイルの解析と共有秘密情報の追加　12-31
バイナリ ファイル、外部、表示　12-37
バイナリ ファイル、テンプレート ファイルへの変換　12-27
バイナリ ファイル、ローカル、表示　12-36
バイナリ ファイルの出力、指定　12-35
マクロ変数、CLI での指定　12-32
マクロ変数、デバイスの指定　12-33
ローカル テンプレート ファイルの解析　12-28
設定ファイル状態、および DOCSIS 設定　4-8
選択タグ、定義　5

た

対象読者、このマニュアルの　xv
タプル、定義　5

ち

注意
意味　xvii
項目
BACC DHCP のオプション設定　3-6
BACC_HOME/kdc ディレクトリ　2-16
cnr_ep.properties ファイル　B-1
DOCSISModem サービス クラス、追加　10-4
DSS、複数、単一のプロビジョニング グループ内　2-9
KDC 証明書、欠落　2-16
kerb auth nomTimeout、maxTimeout、および maxRetries　B-2
MAC アドレスによるデバイスのトラブルシューティング　12-55
uBR7246 デバイスとデバッグ コマンド　4-7, 4-19
カスタム プロパティ、削除　10-7
サンプル ユーザ インターフェイス　2-24, 11-1
ディスク容量の要件の数値　7-4
テンプレート ファイル、削除　10-31
評価ライセンス キーを使用したネットワーク展開　10-32

つ

ツールと高度な概念　12-1 - 12-55
disk_monitor.sh ツール　12-54
Keygen tool　12-47 - 12-48
MAC アドレスによるデバイスのトラブルシューティング　12-55
NRProperties.sh ツール　12-45 - 12-46
PKCert.sh ツール　12-42 - 12-44
KDC 証明書、検証　12-44
KDC 証明書、作成　12-43
実行　12-42
RDU ログ レベル ツール　12-39 - 12-41
現在のログ レベル、表示　12-41
使用方法　12-39
設定　12-40
snmpAgentCfgUtil.sh コマンド　12-49
SNMP エージェント、開始　12-51
SNMP エージェント コミュニティ、削除　12-51
SNMP エージェント コミュニティ、追加　12-50
SNMP エージェント、停止　12-51
SNMP エージェントの設定、リスト　12-53
SNMP エージェントの場所、変更　12-52
SNMP 通知タイプ、指定　12-53
SNMP の連絡先、新規設定　12-52
SNMP リスニング ポート、指定　12-52
ホスト、削除　12-50
ホスト、追加　12-49
設定ファイル ユーティリティ　12-25 - 12-38
PacketCable BASIC フロー、有効化　12-38
外部テンプレート ファイルの解析　12-29
実行　12-25
使用方法　12-27
バイナリ ファイル、外部、表示　12-37
バイナリ ファイル､テンプレート ファイルへの変換　12-27
バイナリ ファイル、ローカル、表示　12-36
バイナリ ファイルの出力、指定　12-35

マクロ変数、CLI での指定 12-32
マクロ変数、デバイスの指定 12-33
ローカル テンプレート ファイルの解析 12-28
テンプレート ファイル、作成 12-2 - 12-23
DOCSIS オプションのサポート 12-12
PacketCable オプションのサポート 12-23
SNMP Varbind 12-6
定義済みオプションの符号化タイプ 12-9
文法 12-2
マクロ変数 12-7
ノンセキュア CableHome オプションのサポート 12-23 - 12-24

て

ディスク領域、監視 12-54
データベースの管理 7-1 - 7-8
RDU データベースの移行 7-8
障害復元力について 7-1
ディスク容量の要件 7-4
対処方法 7-4
～に関する注意 7-4
場所、変更 7-8
バックアップと回復 7-5 - 7-7
回復 7-6
バックアップ 7-5
復元 7-7
ファイル 7-2 - 7-3
DB_VERSION 7-3
自動ログ管理 7-3
ストレージ 7-2
トランザクション ログ 7-2
履歴ログ 7-3
デバイス管理 9-5 - 9-17
Manage Devices ページ 9-5
コントロール 9-6
削除、デバイス 9-15
説明 9-14
デバイス構成、再生成 9-16
デバイスの関連付けと関連付け解除 9-16
デバイスの検索 9-8
デバイスの修正 9-15
デバイスの詳細、表示 9-9
デバイスの追加 9-14
デバイスの登録解除 9-17
デバイスのリセット 9-17
テンプレート ファイル、作成 12-2 - 12-23
DOCSIS オプションのサポート 12-12
PacketCable オプションのサポート 12-23
SNMP Varbind 12-6
CableHome MIB 12-7
DOCSIS MIB 12-6
PacketCable MIB 12-7
定義済みオプションの符号化タイプ 12-9
BITS 値の構文 12-11
OCTETSTRING の構文 12-11
テンプレート ファイルの定義 5
文法 12-2
インクルード ファイル 12-3
インスタンスの修飾子 12-5
オプション 12-4
コメント 12-3
マクロ変数 12-7

と

動作状態、および DOCSIS 設定 4-9
動的設定ファイル、定義 5
登録状態、および DOCSIS 設定 4-8
トラブルシューティング
DOCSIS ネットワーク 4-5
PacketCable 音声設定のシナリオ 5-13 - 5-16
PacketCable 音声設定のツール 5-12
Ethereal、SnifferPro など 5-12
ログ 5-12
PacketCable の eMTA プロビジョニング 5-8 - 5-11
基本変数 5-10
コンポーネント 5-8
アラート メッセージ A-1 - A-5
RDU のアラート A-2
Solaris DPE のアラート A-3
エージェントのアラート A-4
メッセージ形式 A-1
ケーブル モデムの状態 4-10 - 4-32
DHCP
init(d) 4-18
init(i) 4-20
reject(pk) と reject(pt) 4-29
TOD 交換
init(t) 4-23

オプション ファイル転送開始
init(o) 4-25
オフライン 4-11
オンライン 4-10
登録
reject (c) 4-32
reject (m) 4-31
レンジング プロセス
init(r1)、init(r2)、および init(rc) 4-16
デバイス、MAC アドレスによる 12-55

ね

ネットワーク オペレータ、定義 5
ネットワーク タイム プロトコル、定義 5
ネットワーク管理者、定義 5

の

ノード、管理 9-18 - 9-20
Nodes メニューについて 8-7
削除 9-20
修正 9-20
詳細の表示 9-20
説明 9-19
追加 9-19
ノード タイプ 9-18
削除 9-19
修正 9-19
追加 9-18
ノードに対するノード タイプの関連付けと関連付け解除 9-20

は

バックアップと回復、データベース 7-5 - 7-7
パブリッシング、定義 5

ひ

表記法、このマニュアルの xvii

ふ

プライバシー状態の確立、および DOCSIS 設定 4-8
プロビジョニング API、定義 6
プロビジョニング グループ
説明 2-11
定義 6
リスト 8-6
プロビジョニング データ、パブリッシング 10-36 - 10-37
データストアの変更 10-36
プラグイン設定、変更 10-37

ま

マニュアル xviii
この製品に関連する～ xviii
構成 xvi
対象読者 xv
使用されている表記法 xvii
マルチプル サービス オペレータ、定義 6

ゆ

ユーザ、管理 9-2 - 9-4
削除 9-4
修正 9-3
追加 9-2

ら

ライセンス キー、管理 10-32 - 10-33
ライセンスの修正 10-33
ライセンスの追加 10-33

り

領域、定義 6
領域名、定義 6

ろ

ロギング
BACC のアーキテクチャ、および～ 2-22 - 2-24
DPE のログ 2-22
dpe.log ファイル、表示 2-24
RDU のログ 2-22
ログ レベル、設定 2-23

ログのレベルおよび構造　2-22
アクティブ ログ、定義　3
削除可能ログ、定義　4
冗長ログ、定義　4
ログイン、BACC への　8-2