VPDN コンフィギュレーション ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.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、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、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、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

VPDN 技術の概要 3

機能情報の確認 3

VPDN に関する情報 4

VPDN 技術の概要 4

VPDN の用語 5

VPDN のハードウェア デバイス 5

VPDN トンネル 6

VPDN セッション 7

VPDN アーキテクチャ 7

クライアント側開始ダイヤルイン VPDN トンネリング 7

NAS 側開始ダイヤルイン VPDN トンネリング 8

マルチホップ VPDN のトンネリング 8

MMP スタック グループへの VPDN トンネリング 9

トンネル スイッチング VPDN 9

VPDN トンネリング プロトコル 10

L2TP 10

L2TPv3 14

VPDN グループ設定モード 14

次の作業 15

その他の参考資料 15

VPDN 技術の概要に関する機能情報 17

VPDN 用の AAA 設定 19

機能情報の確認 19

VPDN 用の AAA 設定の前提条件 20

VPDN 用の AAA に関する情報 20

VPDN トンネル認証の検索順序 20

ドメイン名に基づく VPDN トンネル ルックアップ 20
DNIS 情報に基づく VPDN トンネル ルックアップ 20
ドメイン名と DNIS 情報の両方に基づく VPDN トンネル ルックアップ 21
マルチホップのホスト名に基づく VPDN トンネル ルックアップ 21
ユーザごとの VPDN AAA 21
誘導要求ユーザの VPDN 認証 22
ドメイン名のプレフィックス、サフィックスの削除 22
VPDN トンネル認証 22
L2TP VPDN の RADIUS トンネル アカウンティング 23
VPDN 固有のリモート RADIUS AAA サーバ設定 23
PPPoE タギング情報の L2TP 転送 24
DSL Sync-Rate VSA 26
LNS アドレス チェック 27
LNS アドレス チェック機能の利点 27
RADIUS サーバを使用した LNS アドレス チェック 27
ドロップされた制御パケットのデバッグ 28
改訂版 LNS のデッド キャッシュ処理 28
VPDN に対する AAA の設定方法 29
NAS とトンネル サーバでの VPDN の有効化 29
VPDN トンネル認証の検索順序の設定 29
NAS でのユーザごとの VPDN 設定 31
前提条件 31
制限事項 31
グローバルでのユーザごとの VPDN 設定 31
VPDN グループのユーザごとの VPDN 設定 32
NAS とトンネル サーバでの AAA の設定 33
VPDN 用のリモート AAA の設定 35
ダイヤルイン VPDN のリモート AAA 用の NAS の設定 36
次の作業 38
L2TP トンネルのリモート RADIUS AAA 用のトンネル終端装置の設定 38
次の作業 40
リモート AAA 設定の確認とトラブルシューティング 41

VPDN トンネルのアップ状態の確認 41
リモート RADIUS AAA サーバ設定の確認 41
NAS でのリモート TACACS+ AAA サーバ設定の確認 42
トンネル サーバでのリモート TACACS+ AAA サーバ設定の確認 46
リモート クライアントでの L2TP トンネルの確立と PPP のネゴシエーションおよび認証の確認 48
VPDN ユーザの誘導要求の認証の設定 50
トンネル サーバでの VPDN ユーザの誘導要求の認証の設定 50
次の作業 51
NAS での VPDN ユーザの誘導要求の認証の設定 52
次の作業 53
ドメイン名のプレフィックス、サフィックスの削除の設定 53
次の作業 56
VPDN トンネル認証の設定 57
前提条件 58
ホスト名を使用した VPDN トンネル認証の設定 58
次の作業 59
ローカル名を使用した VPDN トンネル認証の設定 59
次の作業 60
L2TP トンネル パスワードを使用した VPDN トンネル認証の設定 60
次の作業 62
L2TP トンネル用の VPDN トンネル認証の無効化 62
L2TP VPDN 用の RADIUS トンネル アカウンティングの設定 63
トンネル終端装置のリモート RADIUS AAA サーバでの L2TP トンネルの認証の設定 65
NAS リモート RADIUS AAA サーバのトンネル割り当て設定 66
NAS リモート RADIUS AAA サーバのセキュアなトンネル認証名の設定 68
PPPoE タギング情報の L2TP 転送の設定 69
PPPoE のタギング情報の L2TP 転送設定 69
PPPoE タグ情報の L2TP 転送の上書き 70
circuit-id での nas-port VSA の上書き 71
remote-id での called-station-id VSA の上書き 71

PPPoE タグ情報の L2TP 転送の削除 72
セッション アクティビティ ログの表示 73
PPPoE から受信した転送 rx 速度値と tx 速度値に対する L2TP の上書きの設定 75
RADIUS サーバを使用しない場合での rx 速度値と tx 速度値の設定 75
RADIUS サーバでの rx 速度値と tx 速度値の設定 77
RADIUS サーバでの ANCP からの rx 速度値と tx 速度値の設定 77
RADIUS サーバでの RAM-min からの rx 速度値と tx 速度値の設定 80
LNS アドレス チェックの設定 82
改訂版 LNS のデッド キャッシュ処理の設定 83
デッド キャッシュ状態での LNS の特定 83
デッド キャッシュ状態での LNS のクリア 84
デッド キャッシュ エントリに対する SNMP イベントの生成 85
デッド キャッシュ エントリに対する Syslog イベントの生成 86
VPDN 用の AAA の設定例 88
例：VPDN トンネル認証の検索順序の設定 88
例：NAS でユーザごとの VPDN の設定 88
例：NAS とトンネル サーバでの AAA の設定 89
例：L2TP トンネル終端装置の VPDN 用のリモート AAA の設定 89
例：VPDN ユーザの誘導要求の認証の設定 90
例：ドメイン名のプレフィックス、サフィックス削除の設定 91
例：VPDN トンネル認証の設定 92
例：NAS の RADIUS トンネル アカウンティングの設定 93
例：トンネルサーバの RADIUS トンネル アカウンティングの設定 94
例：NAS RADIUS AAA サーバのトンネル割り当て設定 95
例：rx 速度値と tx 速度値の設定 96
例：セキュアな認証名の設定 96
例：LNS アドレスチェックの設定 97
例：改訂版 LNS のデッド キャッシュ処理の設定 98
次の作業 99
その他の参考資料 99
VPDN 用の AAA の機能情報 101
NAS 側開始ダイヤルイン VPDN トンネリングの設定 105

機能情報の確認 105
NAS 側開始ダイヤルイン VPDN トンネリング設定の前提条件 106
NAS 側開始ダイヤル イン VPDN トンネリング設定の制約事項 106
NAS 側開始ダイヤルイン VPDN トンネリングに関する情報 106
NAS 側開始ダイヤルイン VPDN トンネリング 106
L2TP 発信側ステーション ID の抑制 107
L2TP のフェールオーバー 107
NAS 側開始ダイヤルイン VPDN トンネリングの設定方法 108
ダイヤル イン VPDN トンネル要求のための NAS の設定 108
次の作業 111
ダイヤル イン VPDN トンネル受け入れのためのトンネル サーバの設定 111
次の作業 113
トンネル サーバの仮想テンプレートの設定 113
NAS による VPDN 設定の確認 115
NAS とトンネル サーバ間のトンネル確立の確認とトラブルシューティング 115
クライアントと NAS 間の接続の確認 117
L2TP 発信側ステーション ID の抑制の設定 119
L2TP 発信側ステーション ID の抑制を設定するための前提条件 119
NAS でのグローバル L2TP 発信側ステーション ID の抑制の設定 120
NAS での VPDN グループに対する L2TP 発信側ステーション ID の抑制の設定 121
NAS リモート RADIUS サーバでの L2TP 発信側ステーション ID 抑制の設定 122
NAS によるダイヤルイン VPDN トンネリングの設定例 124
例：ダイヤル イン VPDN への NAS の設定 124
例：ダイヤルイン VPDN のトンネル サーバの設定 124
例：ローカル認証での L2TP 発信側ステーション ID の抑制 125
例：RADIUS 認証での L2TP 発信側ステーション ID の抑制 127
次の作業 128
その他の参考資料 128
NAS 側開始ダイヤルイン VPDN トンネリング設定の機能情報 130
マルチホップ VPDN の設定 133
機能情報の確認 133

マルチホップ VPDN の前提条件 134
マルチホップ VPDN の制約事項 134
マルチホップ VPDN に関する情報 134
マルチホップ VPDN を使用したトンネル スイッチング 134
マルチホップ VPDN の設定方法 135
マルチホップ トンネル スイッチの設定 135
マルチホップ トンネル スイッチ設定の前提条件 136
トンネル スイッチでのマルチホップ VPDN の有効化 136
次の作業 137
着信 VPDN トンネルを終了するためのマルチホップ トンネル スイッチの設定 137
次の作業 138
発信 VPDN トンネル開始のためのマルチホップ トンネル スイッチの設定 139
マルチホップ VPDN の設定例 141
例：マルチホップ VPDN トンネルのスイッチングの設定 141
次の作業 142
その他の参考資料 142
マルチホップ VPDN の機能情報 144
VPDN 追加機能の設定 147
機能情報の確認 147
VPDN 追加機能の設定に関する情報 148
VPDN テンプレート 148
VPDN 送信元 IP アドレス 148
PPP 経由の VPN ルーティング転送（VRF）フレームルート（プール）割り当て 149
VRF 認識型 VPDN トンネル 149
L2TP VPDN トンネルへの MTU 調整 149
IP MTU の調整を使用しての MTU の調整 150
パス MTU ディスカバリを使った MTU 調整 150
TCP MSS アドバタイジングを使用した MTU 調整 151
PPP MRU アドバタイジングを使用した MTU 調整 151
VPDN トンネルへの QoS 152

QoS 分類の保持 153

VPDN トンネル向け IP プレシデンス 153

VPDN トンネルの ToS の分類 153

VPDN グループ選択 153

VPDN グループ選択の利点 153

VPDN 追加機能の設定方法 154

VPDN テンプレートの作成 154

VPDN グループと VPDN テンプレートの関連付け 155

VPDN グループと VPDN テンプレートの関連付け解除 156

VPDN 送信元 IP アドレスの設定 157

グローバル VPDN 送信元 IP アドレスの設定 157

VPDN グループの送信元 IP アドレスの設定 158

VRF 認識型 VPDN トンネリング設定 159

ローカルでの VRF 認識型 VPDN トンネリングの設定 159

リモート RADIUS AAA サーバでの VRF 認識型 VPDN トンネリングの設定 161

L2TP の VPDN に対する MTU 調整の実行 163

VPDN 配置のための IP MTU の手動設定 163

VPDN 配置での IP MTU 自動調整の有効化 164

VPDN に対するパス MTU ディスカバリの有効化 166

アドバタイズされた TCP MSS の手動設定 167

MRU アドバタイジングの設定 168

VPDN グループ選択の設定 171

ホスト名に基づく VPDN グループ選択の設定 171

送信元 IP アドレスに基づく VPDN グループ選択の設定 172

VRF に基づく VPDN グループ選択の設定 174

VPDN グループ選択の表示 175

VPDN に対する QoS パケット分類の設定 176

ToS バイトの QoS 分類の維持の設定 176

VPDN 用の IP プレシデンスの手動設定 177

VPDN セッション用の ToS の手動設定 178

VPDN の追加機能の設定例 180

例：グローバル VPDN テンプレートの設定 180

例：名前付き VPDN テンプレートの設定 180
例：VPDN テンプレートからの VPDN グループの関連付けの解除 180
例：グローバル VPDN 送信元 IPアドレスの設定 180
例：VPDN グループの送信元 IP アドレスの設定 181
例：VRF 認識型 VPDN トンネルのローカル設定 181
例：リモート RADIUS AAA サーバでの VRF 認識型 VPDN トンネルの設定 182
例：VPDN 配置のための IP MTU の手動設定 183
例：VPDN 配置での IP MTU の自動調整の有効化 183
例：アドバタイズされた TCP MSS の手動設定 183
例：MRU のアドバタイズの設定 183
例：ToS バイトの QoS 分類保護の設定 183
例：VPDN 用の IP プレシデンスの手動設定 184
例：VPDN セッションの ToS の手動設定 184
VPDN グループ選択の設定例 184
例：ホスト名に基づく VPDN グループ選択の設定 184
例：IP アドレスに基づく VPDN グループ選択の設定 184
例：VRF に基づく VPDN グループ選択の設定 185
例：ホスト名と IP アドレスに基づく VPDN グループ選択の設定 185
例：ホスト名と VRF に基づいた VPDN グループ選択の設定 185
例：IP アドレスおよび VRF に基づいた VPDN グループ選択の設定 186
例：ホスト名 VRF と IP アドレスに基づく VPDN グループ選択の設定 186
例：VPDN グループ選択の表示 187
例：VPDN グループ選択の概要の表示 188
次の作業 188
その他の参考資料 188
VPDN 追加機能の機能情報 190
VPDN トンネル管理 193
機能情報の確認 193
VPDN トンネル管理の前提条件 194
VPDN トンネル管理の制約事項 194
VPDN トンネル管理に関する情報 194
VPDN トンネルの終了 194

VPDN セッション制限 194
VPDN トンネルに対する制御パケットのパラメータ 195
L2TP 輻輳回避 195
L2TP 輻輳回避の仕組み 195
VPDN イベント ロギング 196
VPDN トンネルの管理方法 196
VPDN トンネルの手動での終了 196
VPDN トンネルのソフト シャットダウンの有効化 197
VPDN トンネルのソフト シャットダウンの確認 199
許容される同時 VPDN セッション数の制限 200
制限事項 201
グローバル VPDN セッション制限の設定 201
VPDN テンプレートの VPDN セッション制限の設定 202
VPDN グループに対するセッション制限の設定 203
VPDN セッション制限の確認 204
VPDN トンネルの L2TP 制御パケット パラメータの設定 205
L2TP 輻輳回避の設定 209
VPDN の障害イベントロギングの設定 211
一般的な VPDN イベント ロギングの有効化 212
VPDN トンネル管理の設定例 213
例：VPDN トンネルの手動終了 213
例：VPDN トンネルのソフト シャットダウンの有効化 214
例：VPDN セッション制限の設定 214
例：VPDN グループに対するセッション制限の確認 215
例：VPDN トンネルの L2TP パケット制御タイマーと再試行カウンタの設定 215
例：L2TP 輻輳回避のデバッグと確認の設定 215
例：VPDN の障害イベントロギングの設定 217
例：一般的な VPDN のイベント ロギングの設定 217
その他の参考資料 218
VPDN トンネル管理の機能情報 219
LAC/LNS 上での L2TP HA セッションの SSO/ISSU の設定 223
機能情報の確認 223

LAC/LNS での L2TP HA セッション SSO/ISSU の前提条件 224
LAC/LNS での L2TP HA Session SSO/ISSU の機能制限 224
LAC/LNS 上での L2TP HA セッションの SSO/ISSU に関する情報 224
ステートフル スイッチオーバー 224
データのチェックポインティング 225
ISSU ソフトウェア スーパーパッケージおよびローリング アップグレードの要件 225
ソフトウェアのアップグレードとダウングレード 226
受信ウィンドウ サイズの調整 226
LAC/LNS 上での L2TP HA セッションの SSO/ISSU の設定方法 226
ルート プロセッサの SSO 設定 227
グローバル L2TP HA SSO モードの設定 228
L2TP HA SSO 用の VPDN グループまたは VPDN テンプレートの設定 229
L2TP HA パケット再同期の制御 231
L2TP HA セッションのチェックポイント ステータスの確認 233
VPDN セッションのチェックポイント ステータスの確認 234
L2TP または VPDN 冗長セッションのトラブルシューティング 235
RADIUS サーバでの L2TP HA SSO/ISSU の設定 236
LAC/LNS での L2TP HA Session SSO/ISSU の設定例 237
例：ルート プロセッサの SSO 設定 237
例：L2TP ハイ アベイラビリティの設定 237
例：L2TP チェックポイント ステータスの表示 237
例：L2TP の冗長性情報の表示 237
例：L2TP の冗長性の詳細情報の表示 237
例：すべての L2TP の冗長性情報の表示 238
例：L2TP の冗長性 ID 情報の表示 238
例：L2TP の冗長性の詳細 ID 情報の表示 238
その他の参考資料 238
LAC/LNS での L2TP HA セッション SSO/ISSU の機能情報 240
L2TP の切断の原因情報 243
機能情報の確認 243
L2TP 切断原因の情報についての制約事項 243

L2TP の切断原因についての情報 244
L2TP 切断原因情報の仕組み 244
L2TP 切断原因情報の利点 244
L2TP 切断原因の情報コード 244
その他の参考資料 246
L2TP の切断原因の情報に関する機能情報 247
管理型 IPv6 レイヤ 2 トンネリング プロトコル ネットワーク サーバの設定 249
機能情報の確認 249
管理型 IPv6 LNS を設定するための前提条件 250
管理型 IPv6 LNS を設定するための情報 250
L2TP ネットワーク サーバ 250
トンネル アカウンティング 251
管理型 LNS の設定方法 252
LNS での VRF の設定 252
仮想テンプレート インターフェイスの設定 255
RADIUS サーバを介した VRF 割り当て 257
L2TP トラフィックを開始および受信するための LNS の設定 259
トンネルごとのセッション数の制限 261
RADIUS 属性の許可、拒否リストの設定 263
名前付き方式リストによる AAA アカウンティングの設定 265
LNS の RADIUS トンネル認証方式リストの設定 267
RADIUS トンネル認証用の LNS の設定 269
LNS の RADIUS トンネル認証方式リストの設定 269
AAA 認証方式の設定 272
管理型 IPv6 レイヤ 2 トンネリング プロトコル ネットワーク サーバの設定例 273
例：管理型 IPv6 LNS の設定 273
例：LNS トンネル アカウンティングの設定 276
例：RADIUS サーバのユーザ プロファイルの確認 278
その他の参考資料 278
管理型 IPv6 レイヤ 2 トンネリング プロトコル ネットワーク サーバの設定に関する機能情報 279
ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポート 281

機能情報の確認 282
ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの前提条件 282
ブロードバンド アグリゲーションの ISDN/ダイヤラ アクセス リンク サポートの制約事項 282
ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートに関する情報 283
ブロードバンドアグリゲーションに関する ISDN/ダイヤラアクセスリンク サポートの導入モデル 283
ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの設定方法 283
L2TP アクセス コンセントレータの設定 284
PRI グループの設定 286
ISDN PRI インターフェイス向けのダイヤラの設定 288
PPP 認証を有効化によるダイヤラ インターフェイスの設定 290
ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの確認 292
トラブルシューティングのヒント 293
ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの設定例 293
例：L2TP アクセス コンセントレータの設定 293
例：PRI グループの設定 294
例：ISDN PRI インターフェイス向けのダイヤラの設定 294
例：PPP 認証を有効にしてのダイヤラ インターフェイスの設定 294
その他の参考資料 294
ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの機能情報 296

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

強力な Cisco IOS XE リリース 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジ ルーティング用）の 2 つのリリースは、コンバージド リリース バージョンとして Cisco IOS XE 16 にマージされました。Cisco IOS XE 16 は、スイッチングおよびルーティング ポートフォリオの幅広いアクセス範囲とエッジ製品を網羅する単一のリリースとなります。

（注） 技術設定ガイドの機能情報の表には、機能が導入された時期が示されています。その他のプラットフォームでその機能がサポートされた時期については示されていない場合があります。特定の機能がご使用のプラットフォームでサポートされているかどうかを特定するには、製品のランディング ページに示されている技術設定ガイドを参照してください。技術設定ガイドが製品のランディングページに表示されている場合は、その機能がプラットフォームでサポートされていることを示します。

第 2 章

VPDN 技術の概要

バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）は、パブリック ネットワークを介してプライベート データを伝送し、インターネットなどの共有インフラストラクチャ上でプライベート ネットワークへのアクセスをリモート ユーザに付与します。VPDN は、コスト効率の高い方法でリモート ユーザと中央ネットワーク間のポイントツーポイント接続を提供しながら、プライベート ネットワークと同じセキュリティ ポリシーと管理を維持します。

- 機能情報の確認，3 ページ
- VPDN に関する情報，4 ページ
- 次の作業，15 ページ
- その他の参考資料，15 ページ
- VPDN 技術の概要に関する機能情報，17 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

VPDN に関する情報

VPDN 技術の概要

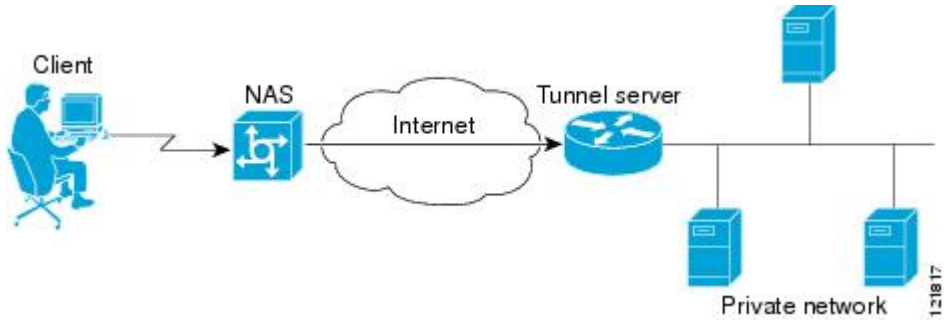
VPDN は、リモート ユーザに対し、プライベート ネットワーク ダイヤルイン サービスを拡大させます。VPDN はレイヤ 2 トンネリング技術を使い、仮想ポイントツーポイント接続をリモート クライアントとプライベート ネットワークとの間で作成します。VPDN は、コスト効率の高い方法でリモート ユーザと中央ネットワーク間のポイントツーポイント接続を提供しながら、プライベート ネットワークと同じセキュリティ ポリシーと管理を維持します。

リモート プライベート ネットワークに直接接続する代わりに、VPDN ユーザは近くのアクセス サーバに接続します。これは、多くの場合インターネット サービス プロバイダー（ISP）のローカル Point Of Presence（POP）内にあります。データはアクセス サーバからプライベート ネットワークへインターネットを介してセキュアに転送され、リモートクライアントとプライベート ネットワーク間でのコスト効率の高い通信方法が実現します。

VPDN の利点は、ネットワークに対する責任を委任する方法にあります。顧客は、情報技術（IT）インフラストラクチャの責任を、リモート ユーザがダイヤル インを行うモデムを保守する ISP やアクセス サーバ、インターネットワーキングの専門技術に委託することができます。そのため、顧客の持つ責任はユーザ認証やプライベート ネットワークの管理に関してのみになります。

次の図は、基本的な VPDN ネットワーク配置について示しています。

図 *1*：基本的な *VPDN* ネットワーク配置



PPP クライアントは、ネットワーク アクセス サーバ（NAS）と呼ばれる ISP アクセス サーバにダイヤルインします。NAS は、プライベート ネットワークであるトンネル サーバに関する窓口として機能するアクセス サーバまたはルータに対して、その PPP セッションを転送するかどうかを決めます。トンネル サーバは、ユーザを認証し、PPP ネゴシエーションを開始します。PPP 設定が完了すると、クライアントとトンネル サーバ間で送られる全てのフレームが NAS を通過します。

VPDN はこれらのトンネリング プロトコルを使い、リンク レベルのフレームをトンネリングできます。

- レイヤ 2 トンネリング プロトコル（L2TP）

- レイヤ 2 トンネリング プロトコル バージョン 3（L2TPv3）
- レイヤ 2 フォワーディング（L2F）
- ポイントツーポイント トンネリング プロトコル（PPTP）

次のプロトコルのいずれかを使用することで、トンネルが NAS やクライアントとトンネル サーバの間で確立され、インタネットなどの共有インフラストラクチャを介したセキュアなデータの転送を可能にします。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでの VPDN はレイヤ 2 トンネリング プロトコル（L2TP）またはレイヤ 2 トンネリング プロトコル バージョン 3（L2TPv3）のみを使用して、リンクレベルのフレームをトンネリングします。

VPDN の用語

VPDN のハードウェア デバイス

一般に、VPDN トンネルには 3 つのデバイスが関わります。これらのデバイスの 2 つは、トンネルのエンドポイントとして機能します。一方のデバイスは VPDN トンネルを開始し、もう一方のデバイスでは、VPDN トンネルを終了します。トンネリング アーキテクチャにより、異なるデバイス タイプがローカルのトンネル エンドポイントとして機能します。

新たなトンネリング プロトコルが VPDN 用に開発されたため、VPDN トンネリングに参加するデバイスをいくつか説明するために、プロトコル固有の用語が作成されました。ただし、これらのデバイスは、使用されるトンネリング プロトコルに関わらず、同じ基本機能を実行します。わかりやすくするために、このドキュメント内で VPDN デバイスに言及する場合は、次の用語を総称的に使用します。

- クライアント：クライアント デバイスは、ダイヤル イン ユーザの PC、またはローカル ネットワークに接続されているルータなどです。クライアントによる VPDN のトンネリング シナリオでは、クライアント デバイスは、トンネル エンドポイントとして機能します。
- NAS：ネットワーク アクセス サーバ（NAS）は、通常、VPDN サービスを顧客へ提供する ISP によって保持されるデバイスです。NAS はクライアント デバイスのローカルの接続先です。NAS とクライアント間で接続を確立することは、ダイヤル イン、ダイヤルアウトのどちらのシナリオを説明しているかにより、コール受信またはコール発信と呼びます。トンネリング アーキテクチャによって、NAS は次のように機能します。
  - NAS 側開始の VPDN トンネリングシナリオと、ダイヤルアウト VPDN トンネリングシナリオの場合、NAS はトンネル エンドポイントとして機能します。NAS はダイヤル イン VPDN トンネルを開始し、ダイヤルアウト VPDN トンネルを終了させます。Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、ダイヤル インのみをサポートします。

- クライアント側開始の VPDN トンネリングシナリオの場合、NAS はトンネル エンドポイントとして機能せず、インターネットの接続のみ提供します。

- トンネル サーバ:トンネル サーバは通常顧客によって維持されており、リモート プライベート ネットワークに対するコンタクト ポイントです。トンネル サーバはダイヤル イン VPDN トンネルを終了させ、ダイヤルアウト VPDN トンネルを開始します。
- トンネル サーバ:トンネル サーバは通常顧客によって維持されており、リモート プライベート ネットワークに対するコンタクト ポイントです。トンネル サーバはダイヤル イン VPDN トンネルを終了させ、ダイヤルアウト VPDN トンネルを開始します。
- トンネル スイッチ：トンネルスイッチは、マルチホップ VPDN トンネリングの実行のために設定されるデバイスです。トンネル スイッチは、NAS とトンネル サーバの両方として機能します。トンネル スイッチは受信する VPDN トンネルを終了させ、発信 VPDN トンネルを開始し、データを次のホップへと伝送します。

トンネルスイッチは、技術的には着信と発信の両方のトンネルに対するトンネルエンドポイントですが、わかりやすくするために、マルチホップ導入でのトンネル エンドポイントは、最初のトンネルを開始するデバイス、およびマルチホップ パスの最後のトンネルを終了するデバイスであるとみなします。

以下の表に、NASとトンネルサーバを説明するために使用される、一般的な用語と対応する技術固有の用語を示します。

表 *1*：*VPDN* ハードウェアの用語

一般的な用語	L2F 用語	L2TP 用語	PPTP 用語
NAS	NAS	L2TP アクセス コンセントレータ（LAC）	PPTP アクセス コンセントレータ（PAC）
トンネル サーバ	ホーム ゲートウェイ	L2TP ネットワーク サーバ（LNS）	PPTP ネットワーク サーバ（PNS）

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、L2TP のみをサポートします。

VPDN トンネル

VPDN トンネルは、2 つのトンネル エンドポイントの間に存在します。トンネルは制御接続と、ゼロ以上のレイヤ 2 のセッションで構成されます。トンネルは、トンネル エンドポイント間で、カプセル化された PPP データグラムと制御メッセージを伝送します。複数の VPDN セッションが同じ VPDN トンネルを使用できます。

VPDN セッション

VPDN セッションは、エンドツーエンドの PPP 接続がクライアントとトンネルサーバ間に確立される時に、トンネル エンドポイント間で作成されます。PPP 接続に関連するデータグラムはトンネルを通じて送信されます。確立されたセッションとそれに関連付けられたコールの間に 1 対 1 の関係があります。複数の VPDN セッションが同じ VPDN トンネルを使用できます。

VPDN アーキテクチャ

クライアント側開始ダイヤルイン VPDN トンネリング

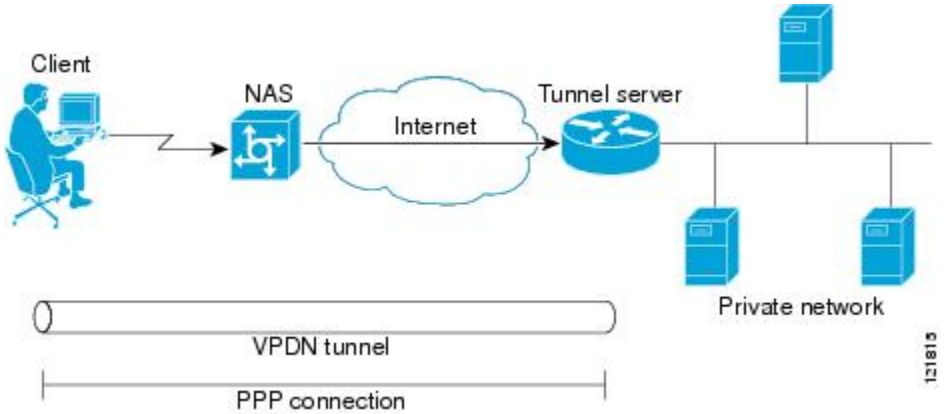
クライアント側開始ダイヤルイン VPDN トンネリングは、自発的トンネリングとも呼ばれます。クライアント側開始ダイヤルイン VPDN トンネリングのシナリオでは、クライアント デバイスがトンネル サーバへのレイヤ 2 トンネルを開始し、NAS はトンネルのネゴシエーションまたは確立に関与しません。このシナリオでは、NAS はトンネルエンドポイントではなく、インターネット接続を提供するだけです。トンネルを開始するように、クライアント デバイスを設定する必要があります。

クライアント側開始 VPDN トンネリングの主な利点は、このトンネリングによってクライアントと ISP NAS 間の接続がセキュリティで保護されることです。ただし、クライアント側開始 VPDN は NAS 側開始 VPDN ほど拡張性はなく、またより複雑です。

クライアント側開始 VPDN トンネリングでは、クライアント デバイスがルータの場合、L2TP プロトコルまたは L2TPv3 プロトコルを使用できます。クライアント デバイスが PC の場合、PPTP プロトコルだけがサポートされます。

次の図は、クライアント側開始 VPDN トンネリングのシナリオを示しています。

図 *2*：クライアント側開始ダイヤルイン *VPDN* のシナリオ



クライアント側開始トンネリングの導入の詳細については、「クライアント側開始ダイヤルイン VPDN トンネリングの設定」モジュールを参照してください。

クライアント側開始ダイヤルイン VPDN トンネリングの導入を設定する前に、「VPDN 用の AAA 設定」モジュールに記載されている必要な各タスクを完了させておく必要があります。

NAS 側開始ダイヤルイン VPDN トンネリング

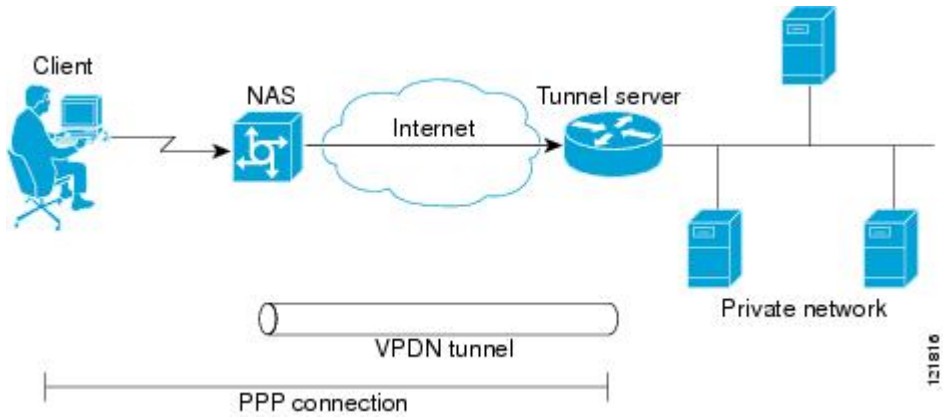
NAS 側開始ダイヤルイン VPDN トンネリングは Compulsory Tunneling とも呼ばれます。NAS 側開始ダイヤルイン VPDN トンネリングのシナリオでは、PPP をサポートするメディアを介してクライアントが NAS へダイヤルインします。デジタル加入者線（DSL）、ISDN、公衆電話交換網（PSTN）などのセキュアと見なされるメディアを介してクライアントからインターネット サービス プロバイダー（ISP）の NAS へ接続する場合、クライアントは追加のセキュリティを提供しないよう選択できます。PPP セッションは、クライアントからの専門知識や操作を必要とせずに、NAS からトンネル サーバにセキュアにトンネリングされます。

NAS 側開始 VPDN トンネリングは L2TP または L2F プロトコルを使って設定できます。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、L2TP のみをサポートします。

次の図は NAS 側開始ダイヤルイントンネリングのシナリオを示します。

図 *3*：*NAS* 側開始ダイヤルイン *VPDN* のシナリオ



NAS 側開始のトンネリング導入に関しての詳細については、「NAS 側開始のダイヤルイン VPDN トンネリング設定」のモジュールを参照してください。

NAS 側開始ダイヤルイン VPDN トンネリングの導入を設定する前に、「VPDN 用の AAA 設定」のモジュールにある必須タスクを完了させる必要があります。

マルチホップ VPDN のトンネリング

マルチホップ VPDN は特殊な VPDN 設定で、複数のトンネルを通過するパケットを許可します。通常、パケットが複数のトンネルを通過することは許可されていません。マルチホップ トンネリングの導入では、VPDN トンネルは各ホップの後に終了し、新たなトンネルが次のホップ先に向けて開始されます。最大 4 つのホップがサポートされます。

マルチホップ VPDN は、このセクションで説明されているシナリオで必要です。

MMP スタック グループへの VPDN トンネリング

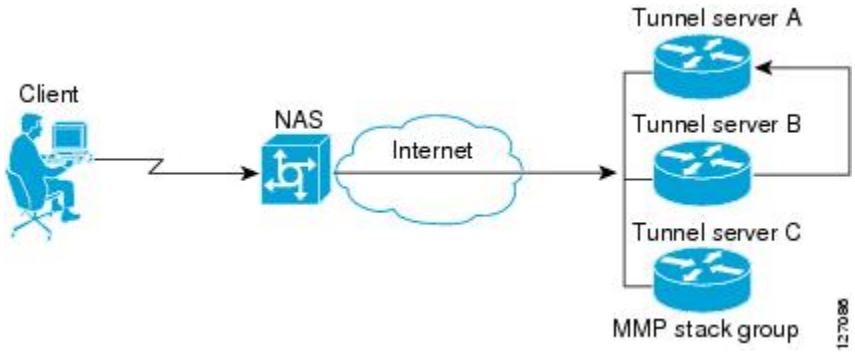
マルチホップ VPDN は、プライベート ネットワークがスタック グループで複数のトンネル サーバを用いてマルチシャーシのマルチリンク PPP（MMP）を使用するときに必要です。スタック グループの設定では、利用するハードウェア デバイスの間でレイヤ 2 トンネルを確立できる必要があります。受信データが VPDN トンネルを介してスタック グループに送られる場合、マルチホップ VPDN がスタック グループを機能させるために必要となります。

MMP を用いたマルチホップ VPDN トンネリングは、L2TP または L2F プロトコルを使って設定します。

（注） Cisco ASR 1000 アグリゲーション サービス ルータは、L2TP のみをサポートします。

次の図は、MMP 導入によるマルチホップ VPDN を使用したネットワーク シナリオを示しています。

図 *4*：マルチホップ *VPDN* を使用した *MMP*



MMP導入に関するマルチホップVPDNの設定についてのさらなる情報は、「マルチホップVPDNの設定」のモジュールを参照してください。

MMP 導入に関するマルチホップ VPDN の設定をする前に、MMP を設定し、「VPDN 用の AAA の設定」モジュールにある必須タスクを完了させる必要があります。

トンネル スイッチング VPDN

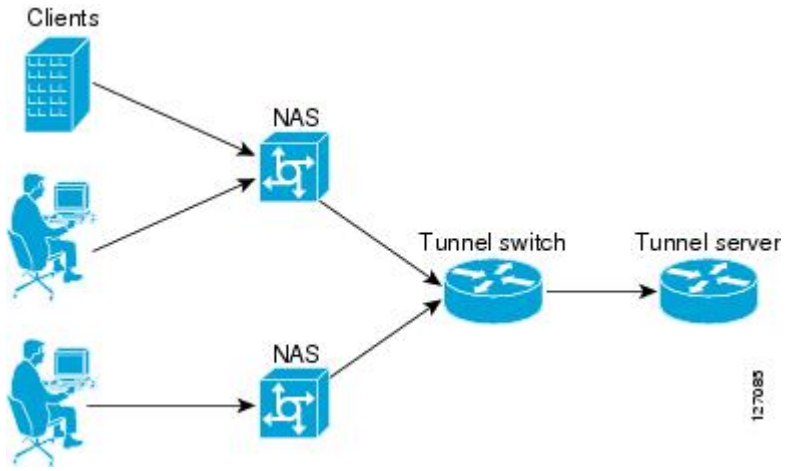
マルチホップVPDNを使用して、トンネル スイッチとしてルータを設定することができます。トンネル スイッチは、NAS とトンネル サーバの両方として設定されるデバイスです。トンネル スイッチは、着信 VPDN トンネルからのパケットを受信し、送信先 VPDN トンネルに送ることができます。トンネル スイッチの設定は、ISP 間でホールセール VPDN サービスを提供するために使われます。

マルチホップ トンネル スイッチングは、L2TP、L2F、PPTP プロトコルを使用して設定できます。

（注） Cisco ASR 1000 アグリゲーション サービス ルータは、L2TP のみをサポートします。

次の図は、トンネルのスイッチング導入を利用したネットワーク シナリオを示しています。

図 *5*：マルチホップ *VPDN* を使用したトンネル スイッチング



マルチホップ トンネル スイッチイング導入に関しての詳細については、「マルチホップ VPDN の設定」のモジュールを参照してください。

マルチホップ トンネル スイッチング導入を設定する前に、「VPDN 用の AAA の設定」のモジュールにある必須タスクを完了させる必要があります。

VPDN トンネリング プロトコル

VPDN はレイヤ 2 プロトコルを使い、上位層プロトコルのリンク層（たとえば、PPP フレームや非同期ハイレベル データ リンク コントロール（HDLC）など）をトンネリングします。ISP は、ユーザからのコールを受信して、それを顧客のトンネル サーバに転送するよう NAS を設定します。

通常、ISP は顧客のトンネル サーバに関する情報だけを保持します。顧客は、ユーザの IP アドレス、ルーティングやその他ユーザ データベース機能を保持します。ISP とトンネル サーバ間の管理は、IP 接続へと減少します。

このセクションでは、Cisco ASR 1000 シリーズ ルータで VPDN トンネリングに対して使用できる唯一のプロトコルである、L2TP と L2TPv3 関する情報が含まれます。

L2TP

L2TP とは、それよりも前から存在する 2 つのトンネリング プロトコルである Cisco L2F と Microsoft PPTP の最良の機能が組み合わされた、Internet Engineering Task Force（IETF）の標準規格です。

L2TP には、L2F と同じ幅広い機能一式が備わっており、さらに追加の機能も提供しています。L2TP 対応トンネル サーバは、既存の L2F NAS と連携して機能すると同時に、L2TP を実行するアップグレードされたコンポーネントもサポートします。トンネル サーバは、個々の NAS が L2F から L2TP にアップグレードされるたびに再設定する必要はありません。次の表では、L2F と L2TP の各機能コンポーネントが比較されています。

表 *2*：*L2F* と *L2TP* の機能の比較

機能	L2F	L2TP
フロー制御	いいえ	はい
属性と値（Attribute-Value: AV）のペアの隠蔽	いいえ	はい
トンネル サーバのロード シェアリング	はい	はい
トンネル サーバのスタック構成/マルチホップのサポート	はい	はい
トンネル サーバのプライマリ バックアップとセカンダリ バックアップ	はい	はい
ドメイン ネーム システム（DNS）名のサポート	はい	はい
ドメイン名の柔軟性	はい	はい
アイドル タイムアウトと絶対タイムアウト	はい	はい
マルチリンク PPP のサポート	はい	はい
マルチシャーシ マルチリンク PPP のサポート	はい	はい

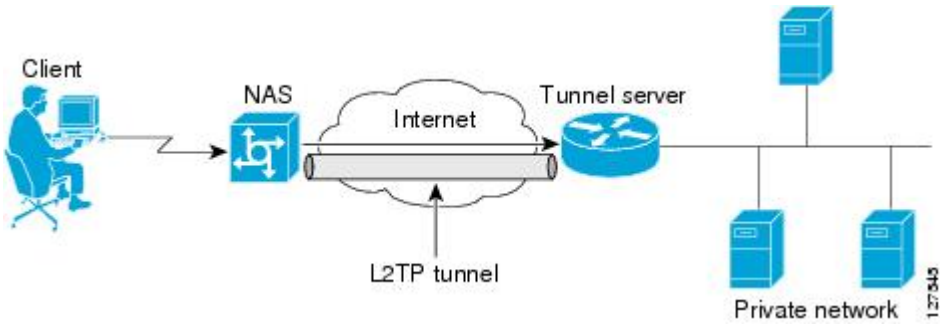
機能	L2F	L2TP

セキュリティ	• 次の複数のユーザ単位の認証オプションを含む、PPPのセキュリティのすべての利点：
	  • チャレンジ ハンドシェイク認証プロトコル（CHAP）
	  • Microsoft CHAP（MS-CHAP）
	  • パスワード認証プロトコル（PAP）
	• トンネル認証は必須
		• 次の複数のユーザ単位の認証オプションを含む、PPPのセキュリティのすべての利点：
		  • CHAP
		  • MS-CHAP
		  • PAP
		• トンネル認証はオプション

従来のダイヤルアップ ネットワーキング サービスでは登録済みの IP アドレスだけがサポートされるため、VPDNを介して実行されるアプリケーションのタイプが限定されます。L2TPでは、複数のプロトコルと、プライベートに管理されている未登録の IP アドレスがサポートされます。これによって、インターネット、モデム、アクセス サーバ、ISDN 端末アダプタ（TA）などの既存のアクセスインフラストラクチャを使用できます。また、お客様は、ダイヤルアウトサポートを外部に委託できるため、ハードウェアのメンテナンスコストとフリーダイヤルの料金の間接費が削減され、自社の各ゲートウェイ リソースを一か所に集めることもできます。

次の図は、通常のダイヤルイン環境における基本的な L2TP アーキテクチャを示しています。

図 *6*：*L2TP* アーキテクチャ

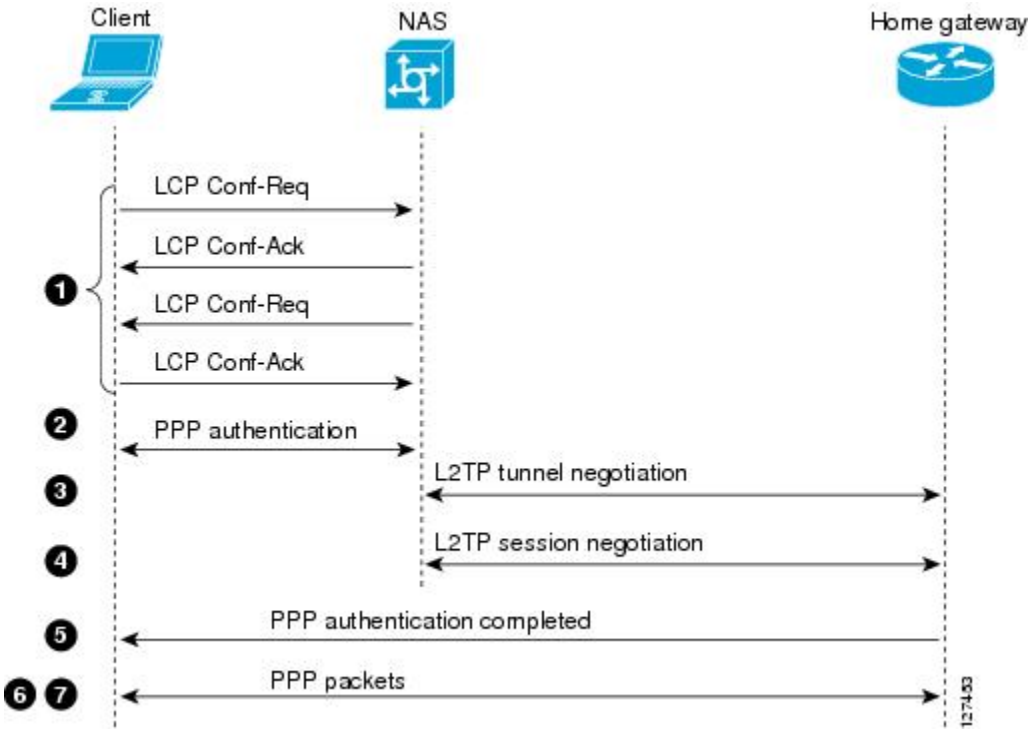


L2TP トンネリングを使用すると、ISP や他のアクセス サービスは、仮想トンネルを作成して、リモート サイトまたはリモート ユーザを企業のホーム ネットワークにリンクさせることができます。ISP の POP にある NAS は、リモート ユーザと PPP メッセージを交換し、L2TP の要求と応答によってプライベート ネットワークのトンネル サーバと通信してトンネルをセットアップします。L2TPでは、ポイントツーポイント接続のエンドポイント間の仮想トンネルを介してプロトコ

ルレベルのパケットを受け渡します。リモート ユーザからのフレームは、ISP の NAS によって受け入れられ、すべてのリンクされたフレーミングまたは透過性バイトから除去され、L2TP でカプセル化され、適切なトンネルを介して転送されます。プライベート ネットワークのトンネル サーバでは、これらの L2TP フレームを受け入れて、L2TP のカプセル化を解除し、適切なインターフェイスのために着信フレームを処理します。

次の図は、NAS 側開始ダイヤルイン L2TP 接続の確立中に発生するイベントを示しています。

図 *7* : *L2TP* プロトコルのネゴシエーションのイベント



次の説明は、この図に示されている一連のイベントの説明で、図の番号に対応しています。

1. リモート ユーザが、アナログ電話システムなどの PPP をサポートするメディアを使用して、ISP の NAS への PPP 接続を開始します。NAS がこの接続を受け入れ、PPP リンクが確立され、Link Control Protocol（LCP）がネゴシエートされます。
2. エンド ユーザと NAS が LCP をネゴシエートした後、NAS が CHAP または PAP を使用してエンド ユーザを部分的に認証します。ユーザ名、ドメイン名、または着信番号情報サービス（Dialed Number Information Service; DNIS）を使用して、ユーザが VPDN クライアントかどうかを判別します。ユーザが VPDN クライアントではない場合、認証は続行され、クライアントはインターネットまたは他の通信先サービスにアクセスします。ユーザ名が VPDN クライアントの場合、マッピングによって、特定のエンドポイント（トンネル サーバ）が指定されます。
3. トンネル エンドポイント、NAS、およびトンネル サーバが、トンネルまたはセッションの確立を試みる前に相互に認証を行います。あるいは、トンネル サーバは NAS のトンネル認証な

しでトンネルの作成を受け入れることもできます。NAS とトンネル サーバが、トンネルの確立をネゴシエートするために制御メッセージを交換します。

4 トンネルが確立されると、L2TP セッションがエンドユーザに対して作成されます。NAS とトンネル サーバが、コール メッセージを交換してセッションの確立をネゴシエートします。

5 NAS がネゴシエートされた LCP オプションと、部分的に認証された CHAP または PAP 情報をトンネル サーバに伝達します。トンネル サーバが、ネゴシエートされたオプションと認証情報を仮想アクセスインターフェイスに直接送り込み、認証を完了できます。仮想テンプレートインターフェイスに設定されたオプションが NAS とネゴシエートされたオプションと一致しない場合、接続は失敗し、切断通知が NAS に送信されます。

6 PPP パケットが、ダイヤルイン クライアントとリモート トンネル サーバ間で、あたかも仲介デバイス（NAS）が関与していないかのように交換されます。

その後の（同じトンネル サーバに指定された）PPP 着信セッションでは、L2TP トンネルがすでに開かれているため、L2TP トンネル ネゴシエーションを繰り返しません。

L2TPv3

L2TPv3 は、レイヤ 2 ペイロードをトンネリングする機能を備えた L2TP の拡張バージョンです。L2TPv3 は、レイヤ 2 バーチャル プライベート ネットワーク（VPN）を使用して、IP コア ネットワークを介して、レイヤ2ペイロードをトンネリングするためのL2TPプロトコルを定義します。

VPDN の導入では、ローカル ルータから擬似回線と呼ばれるエミュレート回線上のユーザのリモート ネットワークにクライアントによるトンネルを確立するために、L2TPv3 を使用できます。L2TPv3 セッションごとに関連付けされた疑似回線が 1 つあります。

L2TPv3 は VPDN グループ設定を使用するのではなく、疑似回線に関連付けされた L2TP クラス設定を使用しています。ローカル デバイスの L2TP クラスと、顧客ネットワークでの accept-dialin VPDN グループを設定することで、L2TPv3 擬似回線を L2TP トンネルの確立のために使用できます。

L2TPv3 プロトコルについての詳細は、「その他の参考資料」セクションを参照してください。

VPDN グループ設定モード

多くの VPDN 設定タスクは、VPDN グループ内で実行されます。VPDN グループは、NAS VPDN グループか、トンネル サーバ VPDN グループのどちらか一方に設定され、両方に設定されることはありません。しかし、個々のルータでは、NAS VPDN グループとトンネル サーバ VPDN グループの両方に設定することができます。

下のテーブルに示すリストのコマンドを 1 つ以上発行することより、VPDN グループを、特定のタイプとして設定できます。

表 3 : VPDN サブグループ設定モード

VPDN グループ タイプ	コマンド	コマンド モード	コマンド モード プロンプト
トンネル サーバ	**accept-dialin**	VPDN の accept-dialin 設定	Router(config-vpdn-acc-in)#
NAS	**request-dialin**	VPDN の request-dialin 設定	Router(config-vpdn-req-in)#

適切に VPDN トンネリングを設定するのに必要なコマンドの多くは、上の表に表示されている VPDN サブグループ設定モードの 1 つで発行されます。VPDN のサブグループ コマンドの設定を削除すると、すべての下位の VPDN サブグループの設定コマンドも同様に使用できなくなります。

次の作業

設定したい VPDN アーキテクチャと使用するトンネリング プロトコルを特定したら、「VPDN 用の AAA の設定」モジュールでの必要なタスクを実行する必要があります。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
VPDN コマンド	『*Cisco IOS VPDN Command Reference*』
L2TP のテクニカル サポートのドキュメンテーション	『Layer 2 Tunnel Protocol（L2TP）』
VPDN のテクニカル サポートのドキュメンテーション	『Virtual Private Dial-Up Network (VPDN)』
L2TPv3 に関する情報	「L2TPv3：レイヤ 2 トンネリング プロトコル バージョン 3」のモジュール

標準

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
• CISCO-VPDN-MGMT-MIB • CISCO-VPDN-MGMT-EXT-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2661	『*Layer Two Tunneling Protocol L2TP*』
RFC 3931	『*Layer Two Tunneling Protocol - Version 3 (L2TPv3)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VPDN 技術の概要に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *4*：*VPDN* 技術の概要に関する機能情報

機能名	リリース	機能情報
レイヤ 2 トンネル プロトコル（L2TP）	Cisco IOS XE リリース 2.1 Cisco IOS XE リリース 3.3S	この機能は、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータで導入されました。 VPDN は、レイヤ 2 プロトコルを使用して、上位層プロトコルのリンク層（たとえば、PPP フレームや非同期 HDLC など）をトンネリングします。L2TP は、Cisco L2F と Microsoft PPTP という 2 つの以前のトンネリング プロトコルの最善の特長を取り入れた IETF 標準規格です。 この機能によって導入または変更されたコマンドはありません。

機能名	リリース	機能情報
バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 VPDNはパブリック ネットワークを介してプライベート データを伝送し、インターネットなどの共有インフラストラクチャ上でプライベート ネットワークへのアクセスをリモートユーザに付与します。VPDNは、コスト効率の高い方法でリモートユーザと中央ネットワーク間のポイントツーポイント接続を提供しながら、プライベートネットワークと同じセキュリティ ポリシーと管理を維持します。 この機能によって導入または変更されたコマンドはありません。

第 3 章

VPDN 用の AAA 設定

このモジュールでは、認証、認可、およびアカウンティング（AAA）をバーチャル プライベート ダイヤルアップ ネットワーク（VPDN）に設定する方法について説明します。

- 機能情報の確認，19 ページ
- VPDN 用の AAA 設定の前提条件，20 ページ
- VPDN 用の AAA に関する情報，20 ページ
- VPDN に対する AAA の設定方法，29 ページ
- VPDN 用の AAA の設定例，88 ページ
- 次の作業，99 ページ
- その他の参考資料，99 ページ
- VPDN 用の AAA の機能情報，101 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

VPDN 用の AAA 設定の前提条件

- VPDN 用の AAA を設定する前に、「*VPDN* 技術の概要」のモジュールの概念をよく理解しておく必要があります。
- 実装する VPDN アーキテクチャを特定する必要があります。
- 使用するトンネリング プロトコルを特定する必要があります。
- リモート AAA を設定しようとする場合、「認証、許可、およびアカウンティング（AAA）」のモジュールと「セキュリティ サーバ プロトコル」のモジュールの概念をよく理解しておく必要があります。
- Point-to-Point Protocol over Ethernet（PPPoE）のタギング情報の レイヤ 2 トンネリング プロトコル（L2TP）転送を設定しようとする場合、この機能を設定する前に、RFC 2516 および DSL Forum TR-101 についてよく理解しておくことをお勧めします。

VPDN 用の AAA に関する情報

VPDN トンネル認証の検索順序

ネットワーク アクセス サーバ（NAS）へのコールがトンネル サーバへトンネリングされる場合、NAS はどのトンネル サーバへコールを転送するか特定する必要があります。ルータはユーザを認証し、ユーザ名のドメイン部分、着信番号識別サービス（DNIS）番号、マルチホップ ホスト名、またはこれら 3 つのパラメータの指定した順序での組み合わせに基づき、発信先トンネルを選択できます。VPDN トンネル認証のデフォルトの検索順序では、最初は DNIS で検索し、次はドメインによって検索します。

これらのセクションは、VPDN トンネル ルックアップ評価基準の情報を含みます。

ドメイン名に基づく VPDN トンネル ルックアップ

NAS がユーザ ドメイン名に基づいて VPDN コールを転送するとき、ユーザは、*username@domain* の形式のユーザ名を使用する必要があります。そうすると、NAS はユーザのドメイン名と検索用に設定されたドメイン名を比較します。NAS は一致を検出すると、ユーザのコールを適切なトンネル サーバへ転送します。

DNIS 情報に基づく VPDN トンネル ルックアップ

NAS がユーザ DNIS 情報に基づいて VPDN コールを転送するように設定されているとき、NAS は ISDN 回線にて提供されるユーザ DNIS 情報を特定し、コールを適切なトンネル サーバに転送します。

DNIS 情報に基づくトンネル選択ができることは、VPDN サービスを提供するネットワーク サービス プロバイダーやサービスを利用する企業に対してさらなる柔軟性を与えます。トンネル選択にドメイン名だけを使用するのではなく、NAS は着信番号情報を使用できます。

この機能により、かつてはドメイン名が1つだけだった企業も複数の特定の電話番号を用意でき、ユーザはこの番号を使ってサービス プロバイダーの Point of Presence（POP）での NAS へのダイヤルインができるようになります。サービスプロバイダーは、着信番号に基づいて、企業ネットワークや適切なサービスに繋ぐトンネルの選択ができます。

ドメイン名と DNIS 情報の両方に基づく VPDN トンネル ルックアップ

サービス プロバイダーが複数の AAA サーバを設定しているとき、ドメイン名に基づいた VPDN トンネル認証の検索は時間がかかり、クライアント セッションがタイムアウトする可能性があります。

より高い柔軟性を提供するために、サービス プロバイダーは NAS に対し、認証検索をドメイン名のみ、DNIS のみ、または指定した順序での2つの組み合わせにより行うよう設定することができます。

マルチホップのホスト名に基づく VPDN トンネル ルックアップ

デバイスがマルチホップ トンネル スイッチとして機能する場合、トンネルの認証検索は、マルチホップのホスト名に基づき実行されます。トンネル スイッチでのマルチホップのホスト名を設定することで、認証検索は、トンネルを開始するピア デバイスの ID に基づき行うことができます。マルチホップのホスト名は、入力トンネルを開始したリモート ピアのホスト名、または入力トンネルに関連付けられたトンネル ID となります。

マルチホップ トンネル スイッチは、認証検索をマルチホップのホスト名のみ、ドメイン名のみ、DNIS のみ、または指定した順序でのそれらの組み合わせにより行うよう設定することができます。

ユーザごとの VPDN AAA

リモート AAA が VPDN に対し使用されている場合、ユーザからコールを受信する NAS は、そのユーザについての情報をリモート AAA サーバへ転送します。基本的な VPDN により、ドメイン名に基づく認証を行うときは NAS はユーザのドメイン名を送信し、DNIS に基づく認証を行うときは、ユーザの発信元電話番号を送信します。

ユーザごとの VPDN を設定すると、ルータが AAA サーバに初めて接続するときに、すべての設定済みユーザ名が AAA RADIUS サーバに送信されます。これにより、共通のドメイン名または DNIS を使用する個々のユーザのトンネル属性をソフトウェアでカスタマイズできるようになります。

ユーザごとの VPDN 設定がないと、ソフトウェアは VPDN トンネル属性情報を判別するためにドメイン名または DNIS のみを送信します。その後、VPDN トンネル属性を返さない場合、ソフトウェアは、全体のユーザ名文字列を送信します。

誘導要求ユーザの VPDN 認証

誘導要求により、NAS にログインしているユーザが認証のために RADIUS サーバを選択できるようになります。誘導要求を有効にすると、「@」記号より前のユーザ名の一部のみが、「@」記号の後に指定されたホストに送信されます。誘導要求を使用すると、認証要求は設定済みサーバのいずれかに誘導でき、指定のサーバにはユーザ名だけが送信されます。

ドメイン名のプレフィックス、サフィックスの削除

AAA 用のリモート サーバを使用するように設定された NAS にユーザが接続すると、NAS ではリモート AAA サーバにそのユーザ名が転送されます。一部の RADIUS サーバまたは TACACS+ サーバでは、ユーザ名が、完全なユーザ名のフォーマットとは異なる場合がある、特別なフォーマットである必要があります。たとえば、リモート AAA サーバで、ユーザ名を user@domain.com というフォーマットにする必要があるのに、完全なユーザ名を prefix/user@domain.com@suffix にできる場合があります。ドメイン名の除去を設定すると、NAS で、完全なユーザ名から互換性のない部分を除去した後で、再フォーマットされたユーザ名をリモート AAA サーバに転送することができます。

NAS は、次のことを実行するように設定できます。

- サフィックスのデリミタ（区切り）文字の @ を使用する完全なユーザ名から汎用のサフィックスを除去する。解析された最初の区切りの後の、完全なユーザ名の部分は除去されます。
- サフィックスのデリミタとして異なる 1 文字または一連の文字を使用する。
- サフィックスおよびプレフィックスの両方を完全なユーザ名から除去する。NAS は、汎用のサフィックス除去を実行する代わりに、指定されたサフィックスだけを除去するように設定することもできます。

VPDN トンネル認証

VPDN トンネル認証を使用すれば、ルータは VPDN トンネルを確立する前に、他のトンネル エンドポイントを認証できます。L2TP トンネルでは、VPDN トンネル認証はオプションです。

クライアントによる VPDN トンネル導入に関する VPDN トンネリングの認証設定についての詳細情報は、「VPDN トンネル認証の設定」のセクションを参照してください。

VPDN トンネルの認証は、次の方法で実行できます。

- NAS とトンネル サーバの両方でのローカル AAA の使用
- NAS でのリモート RADIUS AAA サーバとトンネルサーバでのローカル AAA の使用
- NAS でのリモート TACACS+ AAA サーバとトンネルサーバでのローカル AAA の使用

L2TP トンネルのみ、リモート RADIUS AAA サーバを使い、次のような VPDN トンネル終端装置にて VPDN トンネル認証を実行できます。

- ダイヤルイン VPDN 用のトンネル サーバでリモート RADIUS AAA サーバを使用する
- ダイヤルアウト VPDN 用の NAS でリモート RADIUS AAA サーバを使用する

リモート RADIUS または TACACS+ サーバの設定の詳細情報については、「その他の参考資料」セクションを参照してください。

L2TP VPDN の RADIUS トンネル アカウンティング

VPDN 向け RADIUS トンネル アカウンティングは、6 つの新しい RADIUS アカウンティング タイプを導入している RFC 2867 でサポートされています。RADIUS トンネル アカウンティングのサポートがないと、ネットワーク アカウンティングのある VPDN は、アカウンティング レコード ファイルの全ての属性を報告しません。RADIUS トンネル アカウンティング サポートにより、ユーザは tunnel-link のステータス変更を決定することができます。使用可能なすべての属性を表示できるため、ユーザはアカウンティング レコードをインターネット サービス プロバイダー（ISP）で確認しやすくなっています。

トンネルタイプのアカウンティング レコードを有効にすることで、ルータは RADIUS サーバに、tunnel-link のアカウンティング レコードを送信できます。アカウンティング レコードの 2 つのタイプにより、次の説明のように VPDN トンネリング イベントを識別できるようになります。

Tunnel-Type アカウンティング レコード

AAA は、次のイベントを特定するために、Tunnel-Start、Tunnel-Stop、または Tunnel-Reject のアカウンティング レコードを RADIUS サーバに送信します。

- VPDN トンネルが構築または破壊された。
- VPDN トンネルの作成要求が拒否された。

Tunnel-Link-Type アカウンティング レコード

AAA は、次のイベントを特定するために、Tunnel-Link-Start、Tunnel-Link-Stop、または Tunnel-Link-Reject のアカウンティング レコードを RADIUS サーバに送信します。

- VPDN トンネル内のユーザ セッションが起動または停止された。
- ユーザ セッション作成要求が拒否された。

VPDN 固有のリモート RADIUS AAA サーバ設定

RADIUS 属性は VPDN 設定によって異なります。リモート RADIUS または TACACS+ サーバの設定の詳細情報については、「その他の参考資料」セクションを参照してください。

VPDN 固有の RADIUS 属性は次の機能を提供します。

- トンネル割り当て：トンネル タイプとトンネル エンドポイントが同一のとき、NAS の AAA サーバは、ユーザ単位またはドメイン単位の異なる RADIUS プロファイルからのユーザを同じアクティブ VPDN トンネルにグループ分けするよう設定することができます。
- NAS 側開始のトンネルの認証名：AAA NAS サーバは NAS および NAS AAA サーバのデフォルト名以外の認証名を設定できます。

PPPoE タギング情報の L2TP 転送

PPPoE タグ情報の L2TP 転送機能により、L2TP アクセス コンセントレータ（LAC）から L2TP ネットワーク サーバ（LNS）へ DSL ライン情報を送ることができます。たとえば、LAC は actual-rate-up と actual-rate-down の PPPoE タグ情報を LNS に送信します。LNS は、顧客構内設備（CPE）やデジタル加入者線アクセス マルチプレクサ（DSLAM）によりネゴシエートされた、実際の PPPoE 転送速度を学習します。DSLAM はレートアップとレートダウンに対して、PPPoE タグ値を挿入し、LAC での PPPoE 確立時に情報を送ります。これにより、LNS にこの情報が送られます。

PPPoE タグ情報の L2TP 転送機能を利用することにより、LNS 上で、Circuit-ID と Remote-ID をそれぞれ nas-port-id または、calling-station-id VSA の一方、もしくは両方を上書きすることができます。

dsl-line-info-forwarding コマンドを VPDN グループもしくは VPDN テンプレート コンフィギュレーション モード内において設定するとき、そして LNS が指定した AV ペアの□つを受け取るとき、LNS は一致する VSA を RADIUS サーバに AAA リクエストとして送信します。AAA 関連の属性は次のとおりです。

- AAA_CIRCUIT_ID（RADIUS 属性 87）
- AAA_REMOTE_ID（RADIUS 属性 31）
- DSL Sync Rate VSA

radius-server attribute 87 circuit-id コマンドを入力して、nas-port-id を CIRCUIT_ID VSA で上書きします。**radius-server attribute 31 remote-id** コマンドを入力して、calling-station-id を REMOTE_ID VSA で上書きします。

DSL Forum 2004-71 によると、DSL は回線の識別にベンダー固有のタグを使用します。最初の 2 オクテット（TAG_TYPE）は PPPOE_TAG_VENDSPEC（0x0105）です。次の 2 オクテット（TAG_LENGTH）には、Sub-options、Sub-option-lengths と Tag-values を含む、トータル長が含まれます。TAG_VALUE の最初の 4 オクテットには、ベンダー ID が含まれます。次のオクテットはリモート エージェント ID（0x02）の sub-option が含まれます。次のオクテットはバイト単位での Sub-option-tag のトータル長が含まれます。

Remote-ID タグの最大長は 63 バイトです。Remote-ID タグには、関連 DSL 回線上でユーザを特定する一意のオペレータ管理文字列が含まれます。電話番号、電子メール アドレス、請求先アカウント番号や、サービス プロバイダーがトラッキングに使用できるその他の文字列などが Remote-ID タグになります。

ディスカバリ フレームに sub-option 0x01 がある場合、Circuit-ID タグがあることを示しています。シングル フレームは、Circuit-ID、Remote-ID、またはその両方に対応します。Circuit-ID が同じフレーム内にある場合、Nas-Port-ID 属性により、RADIUS サーバに送信されます。

次の例では、Remote-ID タグおよび DSL-Sync-Rat タグで RADIUS サーバに送信されたアクセス、アカウンティング要求を示しています。

```
01:24:52: RADIUS/ENCODE: Best Local IP-Address 10.0.73.20 for Radius-Server 128.107.164.254
01:24:52: RADIUS(00000011): Send Access-Request to 192.107.164.254:1645 id 1645/3, len 391
01:24:52: RADIUS:  authenticator 3B 49 F5 7D 8A 6F A4 D7 - 57 99 E6 60 A9 D0 C7 B9
01:24:52: RADIUS:  Vendor, Cisco       [26]  41
01:24:52: RADIUS:   Cisco AVpair       [1]   35  "client-mac-address=0090.bf06.c81c"
01:24:52: RADIUS:  Vendor, Cisco       [26]  39
01:24:52: RADIUS:   Cisco AVpair       [1]   33  "actual-data-rate-upstream=20480"
01:24:52: RADIUS:  Vendor, Cisco       [26]  39
01:24:52: RADIUS:   Cisco AVpair       [1]   33  "actual-data-rate-downstream=512"
01:24:52: RADIUS:  Vendor, Cisco       [26]  39
01:24:52: RADIUS:   Cisco AVpair       [1]   33  "minimum-data-rate-upstream=1024"
01:24:52: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
01:24:52: RADIUS:  User-Name           [1]   16  "pshroff-client"
01:24:52: RADIUS:  CHAP-Password       [3]   19  *
01:24:52: RADIUS:  NAS-Port-Type       [61]  6   Ethernet                  [15]
01:24:52: RADIUS:  Vendor, Cisco       [26]  46
01:24:52: RADIUS:   Cisco AVpair       [1]   40  "circuit-id-tag=Ethernet1/0.1:abababababa"
01:24:52: RADIUS:  Vendor, Cisco       [26]  36
01:24:52: RADIUS:   Cisco AVpair       [1]   30  "remote-id-tag=0090.bf06.c81c"
01:24:52: RADIUS:  NAS-Port            [5]   6   268435486
01:24:52: RADIUS:  NAS-Port-Id         [87]  25  "Ethernet1/0.1:abababababa"
01:24:52: RADIUS:  Vendor, Cisco       [26]  41
01:24:52: RADIUS:   Cisco AVpair       [1]   35  "client-mac-address=0090.bf06.c81c"
01:24:52: RADIUS:  Service-Type        [6]   6   Framed                    [2]
01:24:52: RADIUS:  NAS-IP-Address      [4]   6   10.0.73.20
01:24:55: RADIUS(00000011): Send Accounting-Request to 192.107.164.254:1646 id 1646/4, len
 495
01:24:55: RADIUS:  authenticator 22 6F B2 F3 88 B1 03 91 - 4A 70 53 BD 44 A6 A6 0F
01:24:55: RADIUS:  Acct-Session-Id     [44]  19  "1/0/0/30_00000008"
01:24:55: RADIUS:  Vendor, Cisco       [26]  39
01:24:55: RADIUS:   Cisco AVpair       [1]   33  "actual-data-rate-upstream=20480"
01:24:55: RADIUS:  Vendor, Cisco       [26]  39
01:24:55: RADIUS:   Cisco AVpair       [1]   33  "actual-data-rate-downstream=512"
01:24:55: RADIUS:  Vendor, Cisco       [26]  39
01:24:55: RADIUS:   Cisco AVpair       [1]   33  "minimum-data-rate-upstream=1024"
01:24:55: RADIUS:  Vendor, Cisco       [26]  49
01:24:55: RADIUS:   Cisco AVpair      [1]   43  "minimum-data-rate-downstream-low-power=32"
01:24:55: RADIUS:  Vendor, Cisco       [26]  46
01:24:55: RADIUS:   Cisco AVpair       [1]   40  "maximum-interleaving-delay-upstream=64"
01:24:55: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
01:24:55: RADIUS:  User-Name           [1]   16  "pshroff-client"
01:24:55: RADIUS:  Vendor, Cisco       [26]  32
01:24:55: RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
01:24:55: RADIUS:  Acct-Authentic      [45]  6   RADIUS                    [1]
01:24:55: RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
01:24:55: RADIUS:  NAS-Port-Type       [61]  6   Ethernet                  [15]
01:24:55: RADIUS:  Vendor, Cisco       [26]  46
01:24:55: RADIUS:   Cisco AVpair       [1]   40  "circuit-id-tag=Ethernet1/0.1:abababababa"
01:24:55: RADIUS:  Vendor, Cisco       [26]  36
01:24:55: RADIUS:   Cisco AVpair       [1]   30  "remote-id-tag=0090.bf06.c81c"
01:24:55: RADIUS:  NAS-Port            [5]   6   268435486
01:24:55: RADIUS:  NAS-Port-Id         [87]  25  "Ethernet1/0.1:abababababa"
01:24:55: RADIUS:  Vendor, Cisco       [26]  41
01:24:55: RADIUS:   Cisco AVpair       [1]   35  "client-mac-address=0090.bf06.c81c"
01:24:55: RADIUS:  Service-Type        [6]   6   Framed                    [2]
01:24:55: RADIUS:  NAS-IP-Address      [4]   6   10.0.73.20
01:24:55: RADIUS:  Acct-Delay-Time     [41]  6   0
01:24:57: RADIUS: Received from id 1646/4 192.107.164.254:1646, Accounting-response, len
20
```

LAC は DSL 回線 情報を含む、示唆される AV ペアを LNS に送ります。LNS は AAA を通して、RADIUS サーバに送ります。RADIUS サーバは、AAA 要求の処理時に DSL 回線 ID を使用します。

PPPoE タギング情報の L2TP 転送を設定しようとする場合、この機能を設定する前に、RFC 2516 および DSL Forum TR-101 についてよく理解しておくことをお勧めします。

DSL Sync-Rate VSA

DSL では、Sync-Rate タグ情報に、PPPoE ベンダー固有タグを使用します。DSL Sync-Rate は、kbps 単位のレートを表す 32 ビットの 2 進値として符号化されます。タグの長さは 4 バイトです。次の表は、必須の DSL Sync-Rate タグとそれらに関連付けられた RADIUS VSA を示しています。

表 *5*：必須の *DSL Sync-Rate* タグ

DSL 回線情報	RADIUS VSA	説明
DSL 回線の Actual-Data-Rate-Upstream AVP	AAA_AT_ACTUAL_RATE_UP	実際のアップストリーム データ レート（kbps 単位）。
DSL 回線の Actual-Data-Rate-Downstream AVP	AAA_AT_ACTUAL_RATE_DOWN	実際のダウンストリーム データ レート（kbps 単位）。
DSL 回線の Minimum-Data-Rate-Upstream AVP	AAA_AT_MIN_RATE_UP	最小のアップストリーム データ レート（kbps 単位）。
DSL 回線の Minimum-Data-Rate-Downstream AVP	AAA_AT_MIN_RATE_DOWN	最小のダウンストリーム データ レート（kbps 単位）。

PADI/PADR フレームには、オプションの DSL Sync-Rate タグが含まれていることがあります。次の表は、オプションの DSL Sync-Rate タグに関する DSL 回線情報とそれらに関連付けられた RADIUS VSA を示しています。

表 *6*：オプションの *DSL Sync-Rate* タグ

DSL 回線情報	RADIUS VSA	説明
DSL 回線の Attainable-Data-Rate-Upstream AVP	AAA_AT_ATTAINABLE_RATE_UP	達成可能なアップストリーム データ レート（kbps 単位）。
DSL 回線の Attainable-Data-Rate-Downstream AVP	AAA_AT_ATTAINABLE_RATE_DOWN	達成可能なダウンストリーム データ レート（kbps 単位）。
DSL 回線の Maximum-Data-Rate-Upstream AVP	AAA_AT_MAX_RATE_UP	最大のアップストリーム データ レート（kbps 単位）。

DSL 回線情報	RADIUS VSA	説明
DSL 回線の Maximum-Data-Rate-Downstream AVP	AAA_AT_MAX_RATE_DOWN	最大のダウンストリーム データ レート（kbps 単位）。
DSL 回線の Minimum-Data-Rate-Upstream -Low-Power AVP	AAA_AT_MIN_RATE_UP_LOW_POWER	低電力状態での最小のアップストリーム データ レート（kbps 単位）。
DSL 回線の Minimum-Data-Rate-Downstream -Low-Power AVP	AAA_AT_MIN_RATE_DOWN_LOW_POWER	低電力状態での最小のダウンストリーム データ レート（kbps 単位）。
DSL 回線の Maximum-Interleaving-Delay-UpStream AVP	AAA_AT_MAX_INTER_DELAY_UP	最大のアップストリームインターリーブ遅延（ms 単位）。
DSL 回線の Maximum-Interleaving-Delay-DownStream AVP	AAA_AT_MAX_INTER_DELAY_DOWN	最大のダウンストリームインターリーブ遅延（ms 単位）。
DSL 回線の Actual-Interleaving-Delay-Upstream AVP	AAA_AT_ACTUAL_INTER_DELAY_UP	実際のアップストリームインターリーブ遅延（kbps 単位）。
DSL 回線の Actual-Interleaving-Delay-Downstream AVP	AAA_AT_ACTUAL_INTER_DELAY_DOWN	実際のダウンストリームインターリーブ遅延（kbps 単位）。

LNS アドレス チェック

LNS アドレス チェック機能の利点

LNS アドレス チェック機能を使用すれば、LAC が L2TP トンネルのセットアップ時に、その LAC にトラフィックを送信する LNS の IP アドレスをチェックできるため、異なるインターフェイスから到着する、アップリンクとダウンリンクのトラフィックに対するチェック機能が提供されます。

LNS アドレス チェック機能の利点は、トラフィックを代わりのネットワークを通じて送り返すユーザから収入が失われないようにすることです。

RADIUS サーバを使用した LNS アドレス チェック

RADIUS サーバから認証時にダウンロードした Cisco Attribute-Value Pair（AVP）を使用し、LAC での IP アドレス チェックを有効にします。

Cisco AVP は以下のとおりです。

l2tp-security-ip-address-check=yes

次の RADIUS プロファイルの例は、LNS アドレス チェックが有効であることを示しています。

```
example.com Password="example"
Service-Type=Outbound
Cisco-Avpair="vpdn:tunnel-id=tunnel"
Cisco-Avpair="vpdn:tunnel-type=l2tp"
Cisco-Avpair=":ip-address=10.10.10.1"
Cisco-Avpair="vpdn:l2tp-tunnel-password=example"
Cisco-Avpair="vpdn:l2tp-security-ip-address-check=yes"
```

ドロップされた制御パケットのデバッグ

LNS アドレス チェック機能を使用して、ドロップされた制御パケットのトラブルシューティングに役立てます。**debug vpdn l2x-error** コマンドを設定すると、ドロップされた制御パケットごとの情報メッセージが次の形式で表示されます。

```
Tnl <tunnel-ID>
 L2TP: Drop <L2TP-packet-name>
 from y.y.y.y (attempted) x.x.x.x
```

改訂版 LNS のデッド キャッシュ処理

改訂版 LNS のデッド キャッシュ処理の機能により、デッド キャッシュ（ダウン）状態のレイヤ 2 トンネリング プロトコル（L2TP）ネットワーク サーバ（LNS）エントリーを表示またはクリア（再起動）することができます。この機能を使い、LNS がデッドキャッシュ状態になるとき、または終了するときに、Simple Network Management Protocol（SNMP）または、システム メッセージ ログ（syslog）イベントを生成することができます。LNS がデッドキャッシュ状態を終了すると、LNS は新しいセッションを確立できるようになります。

Cisco IOS XE リリース 2.4 以前では、ネットワークは LAC でのロード シェアリング グループ（LSG）の状態を特定することはできませんでした。その結果、LNS が応答していない（デッド キャッシュ状態）ことを知ることができませんでした。LNS がデッド キャッシュ状態の場合、LSG が LAC からのコールを拒否する原因となります。

また、LNS がデッドキャッシュ状態になるとき、またはデッドキャッシュ状態からクリアされるとき、Syslog か SNMP イベントのいずれかを介しても、ネットワークにはロギングの方法がありません。

改訂版 LNS のデッド キャッシュ処理の機能は、デッド キャッシュ（ダウン）状態の 1 つ以上の LNS エントリーを閲覧（特定）またはクリア（再起動）することができ、LNS がデッド キャッシュ状態になる、または終了するときに、syslog や SNMP イベントを生成します。LNS がデッドキャッシュ状態をクリアすると、LNS はアクティブ状態となり、新しいコールセッションを確立することができるようになります。

VPDN に対する AAA の設定方法

NAS とトンネル サーバでの VPDN の有効化

VPDN設定タスクを実行する前にNASとトンネルサーバでVPDNを有効にする必要があります。マルチホップ VPDN トンネル スイッチング アーキテクチャを導入する場合、トンネル スイッチでも VPDN を有効にするする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnenable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnenable** 例： `Router(config)# vpdn enable`	ルータで VPDN をイネーブルにします。

VPDN トンネル認証の検索順序の設定

デフォルトの順序以外を使用するためにVPDNトンネル認証の検索順序を設定するには、NASまたはトンネル スイッチで次の作業を実行します。VPDN トンネル認証のデフォルトの検索順序では、最初は DNIS で検索し、次はドメインによって検索します。

はじめる前に

「NAS とトンネルサーバでの VPDN の設定」セクションの作業を実行する必要があります。

（注） マルチホップ ホスト名に基づいたトンネル認証検索はマルチホップのトンネル スイッチング構成でのみサポートされます。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnsearch-order** {**dnis** [**domain**] [**multihop-hostname**] | **domain** [**dnis**] [**multihop-hostname**] | **multihop-hostname** [**dnis**] [**domain**]}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnsearch-order** {**dnis** [**domain**] [**multihop-hostname**]	**domain** [**dnis**] [**multihop-hostname**]	**multihop-hostname** [**dnis**] [**domain**]} 例： `Router(config)# vpdn search-order domain dnis`	サービス プロバイダー NAS またはトンネル スイッチが VPDN トンネル認証の検索を実行する方法を指定します。 • 少なくとも 1 つ以上の検索パラメータ キーワードを指定する必要があります。検索の実行順序を決めるために複数の検索パラメータ キーワードを任意の順序で指定できます。 （注） **multihop-hostname** キーワードは、トンネル スイッチとして設定されているデバイスでのみ使用します。

NAS でのユーザごとの VPDN 設定

ユーザごとの VPDN はグローバルに、または各 VPDN グループごとに設定できます。VPDN グループの設定がグローバル設定よりも優先されます。

NAS 上で次のいずれかのタスクを実行して、ユーザ単位の VPDN を設定します。

前提条件

NAS リモート RADIUS サーバを AAA 向けに設定する必要があります。「その他の参考資料」セクションを参照してください。

制限事項

- ユーザごとの VPDN 設定は AAA プロトコルとして RADIUS のみをサポートします。
- このタスクは、NAS 側開始ダイヤルイン VPDN のシナリオにのみ互換性があります。

グローバルでのユーザごとの VPDN 設定

NAS にユーザごとの VPDN を設定することで、NAS がはじめて AAA サーバと通信する際に NAS はすべての設定済みユーザ名を RADIUS AAA サーバに送信するようになります。ユーザごとの VPDN はグローバルに、または各 VPDN グループごとに設定できます。ユーザごとの VPDN をグローバルに設定すると、ユーザごとの VPDN は NAS に設定してあるすべての request-dialin VPDN グループに適用されます。

ユーザごとの VPDN をグローバルに設定するには、NAS で次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnauthen-before-forward**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnauthen-before-forward** 例： `Router(config)# vpdn authen-before-forward`	ダイヤルイントンネルで転送を決定する前に完全なユーザ名の認証を要求するよう NAS を設定します。

VPDN グループのユーザごとの VPDN 設定

NAS にユーザごとの VPDN を設定することで、NAS がはじめて AAA サーバと通信する際に NAS はすべての設定済みユーザ名を RADIUS AAA サーバに送信するようになります。ユーザごとの VPDN はグローバルに、または各 VPDN グループごとに設定できます。ユーザごとの VPDN を VPDN グループレベルで設定すると、ユーザごとの VPDN はその特定の VPDN グループに関係する発信のみに適用されます。

特定の VPDN グループ向けのユーザごとの VPDN を設定するには、NAS で次のタスクを実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **request-dialin**
5. **protocoll2tp**
6. **exit**
7. **authen-before-forward**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**request-dialin** 例： `Router(config-vpdn)# request-dialin`	NAS がトンネル サーバへ L2TP トンネルの確立を要求するように設定し、request-dialin VPDN サブグループを作成し、VPDN request-dialin サブグループ設定モードを開始します。
ステップ 5	**protocoll2tp** 例： `Router(config-vpdn-req-in)# protocol l2tp`	VPDN グループが使用するレイヤ 2 トンネリング プロトコルを指定します。
ステップ 6	**exit** 例： `Router(config-vpdn-req-in)# exit`	VPDN グループ コンフィギュレーション モードを終了します。
ステップ 7	**authen-before-forward** 例： `Router(config-vpdn)# authen-before-forward`	VPDN グループに属するダイヤルイン L2TP トンネルで転送を決定する前に完全なユーザ名の認証を要求するよう NAS を設定します。

NAS とトンネル サーバでの AAA の設定

NAS 側開始のダイヤル イン VPDN トンネルと L2TP ダイヤルアウトトンネルの導入では、このタスクを NAS とトンネルサーバで実行します。

クライアントの開始したダイヤル イン VPDN トンネルでは、このタスクをトンネルサーバで実行します。

はじめる前に

- 「NAS とトンネル サーバでの VPDN の有効化, （29 ページ）」に示されているタスクを実行する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. **aaaauthenticationlogin** {**default** | *list-name*} *method1* [*method2...*]
5. **aaaauthenticationppp**{**default** |*list-name*} *method1* [*method2...*]
6. **aaaauthorization**{**network** | **exec** | **commands***level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
7. **vpdnaaaattribute**{**nas-ip-address**{**vpdn-nas** | **vpdn-tunnel-client**} | **nas-port** {**physical-channel-id** | **vpdn-nas**}}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaanew-model** 例： `Router(config)# aaa new model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**aaaauthenticationlogin** {**default** | *list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authentication login default local`	ログイン時の AAA 認証を設定します。

	コマンドまたはアクション	目的
ステップ 5	**aaaauthenticationppp**{**default** |*list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authentication ppp default radius`	PPP を実行しているシリアル インターフェイス上で使用する 1 つ以上の AAA 認証方式を指定します。 （注） VPDNにシェルベースの認証を設定する場合、*method1* 引数用に **if-needed** オプションでこのコマンドを設定する必要があります。これにより、ユーザがログインプロンプトで認証されている場合には、PPP がユーザ認証をバイパスするよう設定されます。
ステップ 6	**aaaauthorization**{**network**	**exec**	**commands***level*	**reverse-access**	**configuration**} {**default**	*list-name*} [*method1* [*method2...*]] 例： `Router(config)# aaa authorization network default radius`	ネットワークへのユーザ アクセスを制限するパラメータを設定します。
ステップ 7	**vpdnaaaattribute**{**nas-ip-address**{**vpdn-nas**	**vpdn-tunnel-client**}	**nas-port** {**physical-channel-id**	**vpdn-nas**}} 例： `Router(config)# vpdn aaa attribute nas-ip-address vpdn-nas`	（オプション）アカウンティング レコードでAAA サーバに報告される VPDN に関連する AAA 属性を有効にします。 （注） NAS でリモート AAA アカウンティングが有効になる場合、トンネル サーバだけにこのコマンドを設定します。

VPDN 用のリモート AAA の設定

トンネル認証には、リモート RADIUS AAA サーバまたはリモート TACACS+ AAA サーバを使用できます。リモート RADIUS サーバまたはリモート TACACS+ サーバの設定の詳細については、「その他の参考資料」セクションを参照してください。

リモート AAA 認証は、次に示すように NAS またはトンネル サーバ上で設定できます。

ダイヤルイン設定

- リモート AAA サーバを使用するように NAS を設定できます。
- トンネル ターミネータとして機能するトンネル サーバを、L2TP トンネル専用のリモート AAA サーバを使用するように設定できます。

ダイヤルアウト設定

- トンネル ターミネータとして機能する NAS を、L2TP トンネル専用のリモート AAA サーバを使用するように設定できます。

次のいずれかのタスクを実行して、VPDN に対してリモート AAA を設定します。

ダイヤルイン VPDN のリモート AAA 用の NAS の設定

リモート RADIUS サーバまたはリモート TACACS+ サーバを使用してトンネル認証するよう NAS を設定するには、次の作業を実行します。この作業は、ダイヤルイン VPDN 設定だけに適用されます。

はじめる前に

手順の概要

1. **enable**
2. **configureterminal**
3. 次のいずれかを実行します。
   - **radius-serverhost** {*hostname* |*ip-address*} [**auth-port***port-number*] [**acct-port***port-number*] [**timeout***seconds*] [**retransmit***retries*] [**key***string*] [**alias** {*hostname* | *ip-address*}]
   - **tacacs-serverhost** {*host-name* | *host-ip-address*} [**key***string*] [**nat**] [**port** [*integer*]] [**single-connection**] [**timeout** [*integer*]]
4. 次のいずれかを実行します。
   - **aaagroupserverradius***group-name*
   - **aaagroupservertacacs+***group-name*
5. 次のいずれかを実行します。
   - **server***ip-address*[**auth-port***port-number*] [**acct-port***port-number*]
   - **server***ip-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかを実行します。
	• **radius-serverhost** {*hostname* |*ip-address*} [**auth-port***port-number*] [**acct-port***port-number*] [**timeout***seconds*] [**retransmit***retries*] [**key***string*] [**alias** {*hostname* | *ip-address*}]
	• **tacacs-serverhost** {*host-name* | *host-ip-address*} [**key***string*] [**nat**] [**port** [*integer*]] [**single-connection**] [**timeout** [*integer*]]
	
	例：
	`Router(config)# radius-server host 10.1.1.1`
	
	例：
	`Router(config)# tacacs-server host 10.2.2.2`
		RADIUS サーバ ホストを指定します。
		または
		TACACS+ ホストを指定します。

ステップ 4	次のいずれかを実行します。
	• **aaagroupserverradius***group-name*
	• **aaagroupservertacacs+***group-name*
	
	例：
	`Router(config)# aaa group server radius group1`
	
	例：
	`Router(config)# aaa group server tacacs+ group7`
		（オプション）異なる RADIUS サーバ ホストを別々のリストと方式にグループ化し、RADIUS server-group コンフィギュレーション モードを開始します。
		または
		（オプション）異なる TACACS+ サーバ ホストを別々のリストと方式にグループ化し、RADIUS server-group コンフィギュレーション モードを開始します。

ステップ 5	次のいずれかを実行します。 • **server***ip-address*[**auth-port***port-number*] [**acct-port***port-number*] • **server***ip-address*	（オプション）グループ サーバ用の RADIUS サーバの IP アドレスを設定します。 または （オプション）グループ サーバ用の TACACS+ サーバの IP アドレスを設定します。

	コマンドまたはアクション	目的

	例：
	`Router(config-sg-radius)# server 10.1.1.1 auth-port 1000 acct-port 1646`
	例：
	`Router(config-sg-radius)# server 10.2.2.2`
		（注） サーバ グループの一部として複数の RADIUS または TACACS+ サーバを設定するには、この手順を複数回実行します。

次の作業

「VPDN トンネル認証の設定」セクションでのプロセスを実行する必要があります。

L2TP トンネルのリモート RADIUS AAA 用のトンネル終端装置の設定

リモート RADIUS AAA を実行するよう、L2TP VPDN トンネルを終端するデバイスを設定できます。この機能がなければ、トンネルの終端装置はローカルの L2TP 認証しかできません。ローカル認証には、トンネル エンドポイントのデータを VPDN グループ内で設定する必要があります。この方法では、VPDN グループに保持される各デバイスの情報を独自に更新する必要が生じ、十分な拡張性をもちません。

リモート RADIUS 認証では、RADIUS サーバで設定を保存でき、この設定情報をローカルで保存しておく必要がなくなります。新しい情報を必要に応じて RADIUS サーバに追加でき、トンネル終端装置のグループは RADIUS サーバの共通データベースをアクセスできます。

トンネル終端装置で L2TP トンネルのリモート RADIUS AAA を設定するには、次の作業を実行します。この作業は、ダイヤルイン VPDN トンネルではトンネル サーバで、ダイヤルアウト VPDN トンネルでは NAS で実行できます。

はじめる前に

- リモート RADIUS AAA サーバを設定する必要があります。リモート RADIUS AAA サーバの設定の詳細については、「その他の参考資料」セクションを参照してください。
- AAA が有効である必要があります。AAA を有効にするには、「NAS とトンネルサーバでの AAA の設定」セクションの作業を実行してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **radius-serverhost** {*hostname* |*ip-address*} [**auth-port***port-number*] [**acct-port***port-number*] [**timeout***seconds*] [**retransmit***retries*] [**key***string*] [**alias** {*hostname* | *ip-address*}]
4. **aaagroupserverradius***group-name*
5. **server***ip-address*[**auth-port***port-number*] [**acct-port***port-number*]
6. **exit**
7. **vpdntunnelauthorizationnetwork** {*list-name* | **default**}
8. **vpdntunnelauthorizationvirtual-template***vtemplate-number*
9. **vpdntunnelauthorizationpassword***password*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-serverhost** {*hostname* |*ip-address*} [**auth-port***port-number*] [**acct-port***port-number*] [**timeout***seconds*] [**retransmit***retries*] [**key***string*] [**alias** {*hostname*	*ip-address*}] 例： `Router(config)# radius-server host 10.1.1.1`	RADIUS サーバ ホストを指定します。
ステップ 4	**aaagroupserverradius***group-name* 例： `Router(config)# aaa group server radius group1`	異なる RADIUS サーバ ホストを別々のリストと方式にグループ化し、RADIUS server-group コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**server***ip-address*[**auth-port***port-number*] [**acct-port***port-number*] 例： `Router(config-sg-radius)# server 10.1.1.1 auth-port 1000 acct-port 1646`	グループ サーバ用の RADIUS サーバの IP アドレスを設定します。 （注） サーバ グループの一部として複数の RADIUS または TACACS+ サーバを設定するには、この手順を複数回実行します。
ステップ 6	**exit** 例： `Router(config-sg-radius)# exit`	RADIUS サーバ グループ コンフィギュレーション モードを終了します。
ステップ 7	**vpdntunnelauthorizationnetwork** {*list-name* | **default**} 例： `Router(config)# vpdn tunnel authorization network default`	リモート ホスト名ベースの認証で使用する AAA 認証方式リストを指定します。 • *list-name* 引数が **aaaauthorization** コマンドで指定された場合、ここでそのリスト名を使用します。 • default キーワードが **aaaauthorization** コマンドで指定された場合、ここでそのキーワードを使用します。
ステップ 8	**vpdntunnelauthorizationvirtual-template***vtemplate-number* 例： `Router(config)# vpdn tunnel authorization virtual-template 3`	（オプション）仮想アクセス インターフェイスの複製元のデフォルトの仮想テンプレートを選択します。
ステップ 9	**vpdntunnelauthorizationpassword***password* 例： `Router(config)# vpdn tunnel authorization password my-secret`	（オプション）リモート トンネルのホスト名に基づいたトンネル設定を取得するための RADIUS 認証要求の「偽」のパスワードを設定します。 （注） このコマンドが有効でない場合、このパスワードは「cisco」になります。

次の作業

「発信 VPDN トンネル開始のためのマルチホップ トンネル スイッチの設定」に示されているタスクを実行する必要があります。

リモート AAA 設定の確認とトラブルシューティング

VPDN トンネルのアップ状態の確認

手順の概要

1. **enable**
2. **showvpdntunnel**

手順の詳細

ステップ 1 **enable**
このコマンドを使用して、特権 EXEC モードを有効にします。プロンプトにパスワードを入力します。

例：

```
Router> enable
```

ステップ 2 **showvpdntunnel**
アクティブなVPDNトンネルに関する情報を表示するには、このコマンドを使用します。少なくとも、トンネルとセッションが 1 つずつ設定されている必要があります。

例：

```
Router# show vpdn tunnel
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote   Name   State  Remote Address  Port  Sessions VPDN Group
4571  61568 csidtw13        est    10.0.195.4      1701  1        ?
LocID RemID TunID Intf          Username               State  Last Chg
4     11    4571  Vi4.1         csidtw9@cisco.com       est    00:02:29
%No active PPPoE tunnels
```

リモート RADIUS AAA サーバ設定の確認

リモート AAA 認証サーバがトンネル エンドポイントに設定され、トンネルのエンドポイントが RADIUS サーバからの属性 90 および 69 を受信できることを確認するには、次の作業を実行します。

この例では、作業の各手順は、トンネルの終端装置としてリモートRADIUSAAAを実行しているトンネル サーバで実行されます。ダイヤル イン VPDN のトンネル イニシエータとして、また、ダイヤルアウト VPDN のトンネル ターミネータとして、リモート RADIUS AAA が NAS で実行されている場合、これらの手順は NAS でも実行できます。

手順の概要

1. **enable**
2. **debugradius**
3. **showlogging**

手順の詳細

ステップ 1 **enable**
このコマンドを使用して、特権 EXEC モードを有効にします。プロンプトにパスワードを入力します。

例：

```
Router> enable
```

ステップ 2 **debugradius**
RADIUS のデバッグ メッセージを表示するには、トンネル サーバで次のコマンドを入力します。

例：

```
Router# debug radius
```

ステップ 3 **showlogging**
このコマンドをトンネル サーバで入力して、標準システム ロギング メッセージ バッファの内容を表示します。以下に太字で示されているように、「access-accept」が出力にあり、属性 90 および 69 が RADIUS 応答に表示されることを確認してください。

例：

```
Router# show logging
00:32:56: RADIUS: Received from id 21645/5 172.19.192.50:1645, Access-Accept
, len 81
00:32:56: RADIUS:  authenticator 73 2B 1B C2 33 71 93 19 - 62 AC 3E BE 0D 13 14 85
00:32:56: RADIUS:  Service-Type        [6]   6   Outbound                  [5]
00:32:56: RADIUS:  Tunnel-Type         [64]  6   00:L2TP                   [3]
00:32:56: RADIUS:  Tunnel-Medium-Type  [65]  6   00:IPv4                   [1]
00:32:56: RADIUS:  Tunnel-Client-Auth-I[90]
  6   00:"csidtw13"
00:32:56: RADIUS:  Tunnel-Password     [69]
 8   *
00:32:56: RADIUS:  Vendor, Cisco       [26]  29
00:32:56: RADIUS:   Cisco AVpair       [1]   23  "vpdn:vpdn-vtemplate=1"
```

NAS でのリモート TACACS+ AAA サーバ設定の確認

リモート TACACS+ AAA サーバが正しく設定されていることを確認するには、NAS で次の作業を実行します。

はじめる前に

この作業を実行する前に、次のデバッグ コマンドを有効にします。

- **debugaaaaccounting**：説明の義務があるイベントが発生したときに、その情報を表示します。
- **debugaaaauthentication**：AAA TACACS+ 認証の情報を表示します。
- **debugaaaauthorization**：AAA TACACS+ 認可に関する情報を表示します。
- **debugtacacs**：TACACS+ に関する情報を表示します。
- **debugvpdnerror**：レイヤ 2 プロトコルに依存しないエラーに関する情報を表示します。
- **debugvpdnevents**：通常のトンネル確立またはシャットダウンの一部であり、レイヤ2プロトコルに依存しないイベントに関する情報を表示します。
- **debugvpdnl2x-errors**：通常の PPP トンネル確立またはシャットダウンの一部である、レイヤ 2 プロトコル固有のエラーに関する情報を表示します。
- **debugvpdnl2x-events**：通常の PPP トンネル確立またはシャットダウンの一部である、レイヤ 2 プロトコル固有のイベントに関する情報を表示します。
- **debugvpdnl2x-packets**：レイヤ 2 プロトコル固有の情報を表示します。
- **debug vtemplate**：仮想アクセスインターフェイスの複製情報を、仮想テンプレートから複製された時点から、通信終了により仮想アクセスインターフェイスがダウンするまで表示します。

手順の概要

1. **enable**
2. **showdebugging**
3. デバッグ出力を調べます。

手順の詳細

ステップ 1 **enable**

このコマンドを使用して、特権 EXEC モードを有効にします。プロンプトにパスワードを入力します。

例：

```
Router> enable
```

ステップ 2 **showdebugging**

ルータで有効になっているデバッグのタイプに関する情報を表示するには、このコマンドを入力します。

例：

```
Router# show debugging
General OS:
```

```
AAA Authentication debugging is on
AAA Authorization debugging is on
AAA Accounting debugging is on
VPN:
L2X protocol events debugging is on
L2X protocol errors debugging is on
VPDN events debugging is on
VPDN errors debugging is on
VTEMPLATE:
Virtual Template debugging is on
!
```

ステップ 3 デバッグ出力を調べます。
次の例は、NAS でリモート TACACS+ AAA 認証を使用して VPDN トンネル確立に成功した NAS からの完全なデバッグ出力を示しています。

例：

```
Jan 30 12:17:09: As1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
20:03:18: %LINK-3-UPDOWN: Interface Async1, changed state to up
Jan 30 12:17:09: As1 VPDN: Looking for tunnel -- rtp.cisco.com --
Jan 30 12:17:09: AAA: parse name=Async1 idb type=10 tty=1
Jan 30 12:17:09: AAA: name=Async1 flags=0x11 type=4 shelf=0 slot=0 adapter=0
port=1 channel=0
Jan 30 12:17:09: AAA/AUTHEN: create_user (0x278B90) user='rtp.cisco.com'
ruser=''
port='Async1' rem_addr='' authen_type=NONE service=LOGIN priv=0
Jan 30 12:17:09: AAA/AUTHOR/VPDN (898425447): Port='Async1' list='default'
service=NET
Jan 30 12:17:09: AAA/AUTHOR/VPDN: (898425447) user='rtp.cisco.com'
Jan 30 12:17:09: AAA/AUTHOR/VPDN: (898425447) send AV service=ppp
Jan 30 12:17:09: AAA/AUTHOR/VPDN: (898425447) send AV protocol=vpdn
Jan 30 12:17:09: AAA/AUTHOR/VPDN (898425447) found list "default"
Jan 30 12:17:09: AAA/AUTHOR/VPDN: (898425447) Method=TACACS+
Jan 30 12:17:09: AAA/AUTHOR/TAC+: (898425447): user=rtp.cisco.com
Jan 30 12:17:09: AAA/AUTHOR/TAC+: (898425447): send AV service=ppp
Jan 30 12:17:09: AAA/AUTHOR/TAC+: (898425447): send AV protocol=vpdn
Jan 30 12:17:09: TAC+: (898425447): received author response status = PASS_ADD
Jan 30 12:17:09: AAA/AUTHOR (898425447): Post authorization status = PASS_ADD
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV service=ppp
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV protocol=vpdn
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV tunnel-id=rtp_tunnel
Jan 30 12:17:09: AAA/AUTHOR/VPDN: Processing AV ip-addresses=10.31.1.56
Jan 30 12:17:09: As1 VPDN: Get tunnel info for rtp.cisco.com with NAS
rtp_tunnel, IP 10.31.1.56
Jan 30 12:17:09: AAA/AUTHEN: free_user (0x278B90) user='rtp.cisco.com' ruser=''
port='Async1' rem_addr='' authen_type=NONE service=LOGIN priv=0
Jan 30 12:17:09: As1 VPDN: Forward to address 10.31.1.56
Jan 30 12:17:09: As1 VPDN: Forwarding...
Jan 30 12:17:09: AAA: parse name=Async1 idb type=10 tty=1
Jan 30 12:17:09: AAA: name=Async1 flags=0x11 type=4 shelf=0 slot=0 adapter=0
port=1 channel=0
Jan 30 12:17:09: AAA/AUTHEN: create_user (0x22CDEC) user='user1@rtp.cisco.com'
ruser='' port='Async1' rem_addr='async' authen_type=CHAP
service=PPP priv=1
Jan 30 12:17:09: As1 VPDN: Bind interface direction=1
Jan 30 12:17:09: Tnl/Cl 74/1 L2TP: Session FS enabled
Jan 30 12:17:09: Tnl/Cl 74/1 L2TP: Session state change from idle to
wait-for-tunnel
Jan 30 12:17:09: As1 74/1 L2TP: Create session
Jan 30 12:17:09: Tnl 74 L2TP: SM State idle
Jan 30 12:17:09: Tnl 74 L2TP: O SCCRQ
Jan 30 12:17:09: Tnl 74 L2TP: Tunnel state change from idle to wait-ctl-reply
Jan 30 12:17:09: Tnl 74 L2TP: SM State wait-ctl-reply
Jan 30 12:17:09: As1 VPDN: user1@rtp.cisco.com is forwarded
Jan 30 12:17:10: Tnl 74 L2TP: I SCCRP from ABCDE
```

```
Jan 30 12:17:10: Tnl 74 L2TP: Got a challenge from remote peer, ABCDE
Jan 30 12:17:10: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:10: AAA/AUTHEN: create_user (0x23232C) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: AAA/AUTHEN/START (1598999635): port='' list='default'
action=SENDAUTH service=PPP
Jan 30 12:17:10: AAA/AUTHEN/START (1598999635): found list default
Jan 30 12:17:10: AAA/AUTHEN (1598999635): status = UNKNOWN
Jan 30 12:17:10: AAA/AUTHEN/START (1598999635): Method=TACACS+
Jan 30 12:17:10: TAC+: send AUTHEN/START packet ver=193 id=1598999635
Jan 30 12:17:10: TAC+: ver=192 id=1598999635 received AUTHEN status = ERROR
Jan 30 12:17:10: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:10: AAA/AUTHEN: create_user (0x232470) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: TAC+: ver=192 id=3400389836 received AUTHEN status = PASS
Jan 30 12:17:10: AAA/AUTHEN: free_user (0x232470) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: AAA/AUTHEN (1598999635): status = PASS
Jan 30 12:17:10: AAA/AUTHEN: free_user (0x23232C) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: Tnl 74 L2TP: Got a response from remote peer, ABCDE
Jan 30 12:17:10: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:10: AAA/AUTHEN: create_user (0x22FBA4) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: AAA/AUTHEN/START (2964849625): port='' list='default'
action=SENDAUTH service=PPP
Jan 30 12:17:10: AAA/AUTHEN/START (2964849625): found list default
Jan 30 12:17:10: AAA/AUTHEN (2964849625): status = UNKNOWN
Jan 30 12:17:10: AAA/AUTHEN/START (2964849625): Method=TACACS+
Jan 30 12:17:10: TAC+: send AUTHEN/START packet ver=193 id=2964849625
20:03:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1,
changed state to up
Jan 30 12:17:11: TAC+: ver=192 id=2964849625 received AUTHEN status = ERROR
Jan 30 12:17:11: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:11: AAA/AUTHEN: create_user (0x22FC8C) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: As1 74/1 L2TP: Discarding data packet because tunnel
is not open
Jan 30 12:17:11: As1 74/1 L2TP: Discarding data packet because tunnel
is not open
Jan 30 12:17:11: TAC+: ver=192 id=1474818051 received AUTHEN status = PASS
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x22FC8C) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN (2964849625): status = PASS
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x22FBA4) user='rtp_tunnel'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: Tnl 74 L2TP: Tunnel Authentication success
Jan 30 12:17:11: Tnl 74 L2TP: Tunnel state change from wait-ctl-reply to
established
Jan 30 12:17:11: Tnl 74 L2TP: O SCCCN to ABCDE tnlid 56
Jan 30 12:17:11: Tnl 74 L2TP: SM State established
Jan 30 12:17:11: As1 74/1 L2TP: O ICRQ to ABCDE 56/0
Jan 30 12:17:11: As1 74/1 L2TP: Session state change from wait-for-tunnel
to wait-reply
Jan 30 12:17:11: Tnl 74 L2TP: Dropping old CM, Ns 0, expected 1
Jan 30 12:17:11: As1 74/1 L2TP: O ICCN to ABCDE 56/1
Jan 30 12:17:11: As1 74/1 L2TP: Session state change from wait-reply to
established
```

トンネル サーバでのリモート TACACS+ AAA サーバ設定の確認

リモート TACACS+ AAA サーバが正しく設定されていることを確認するには、トンネル サーバで次の作業を実行します。

はじめる前に

この作業を実行する前に、次のデバッグ コマンドを有効にします。

- **debugaaaauthentication**：AAA 認証に関する情報を表示します。
- **debugaaaauthorization**：AAA 認証に関する情報を表示します。
- **debugaaaaccounting**：説明の義務があるイベントが発生したときに、その情報を表示します。このコマンドで表示される情報は、アカウンティング情報をサーバに転送するために使用されるアカウンティング プロトコルとは別です。
- **debug tacacs+**：TACACS+ に関連する詳細なデバッグ情報を表示します。
- **debug vtemplate**：仮想アクセスインターフェイスの複製情報を、仮想テンプレートから複製された時点から、通信終了により仮想アクセスインターフェイスがダウンするまで表示します。
- **debugvpdnerror**：トンネル確立の時点から、PPP トンネルの確立を阻害するエラーを表示します。また、確立されたトンネルを閉じてしまうエラーを表示します。
- **debugvpdnevents**：通常の PPP トンネル確立またはシャットダウンの一部であるイベントに関するメッセージを表示します。
- **debugvpdnl2x-errors**：通常の PPP トンネル確立またはシャットダウンの一部であるイベントに関するメッセージを表示します。
- **debugvpdnl2x-events**：レイヤ 2 での通常の PPP トンネル確立またはシャットダウンの一部であるイベントに関するメッセージを表示します。

手順の概要

1. **enable**
2. **showdebugging**
3. デバッグ出力を調べます。

手順の詳細

ステップ 1 **enable**

このコマンドを使用して、特権 EXEC モードを有効にします。プロンプトにパスワードを入力します。

例：

```
Router> enable
```

ステップ 2 **showdebugging**

ルータで有効になっているデバッグのタイプに関する情報を表示するには、このコマンドを入力します。

例：

```
Router# show debugging
General OS:
AAA Authentication debugging is on
AAA Authorization debugging is on
AAA Accounting debugging is on
VPN:
L2X protocol events debugging is on
L2X protocol errors debugging is on
VPDN events debugging is on
VPDN errors debugging is on
VTEMPLATE:
Virtual Template debugging is on
```

ステップ 3 デバッグ出力を調べます。

次の例は、NAS でリモート TACACS+ AAA 認証を使用して VPDN トンネル確立に成功したトンネル サーバからの完全なデバッグ出力を示しています。

例：

```
Jan 30 12:17:09: L2TP: I SCCRQ from rtp_tunnel tnl 74
Jan 30 12:17:09: Tnl 56 L2TP: New tunnel created for remote
rtp_tunnel, address 10.31.1.144
Jan 30 12:17:09: Tnl 56 L2TP: Got a challenge in SCCRQ, rtp_tunnel
Jan 30 12:17:09: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:09: AAA/AUTHEN: create_user (0x21F6D0) user='ABCDE'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:09: AAA/AUTHEN/START (3194595626): port='' list='default'
action=SENDAUTH service=PPP
Jan 30 12:17:09: AAA/AUTHEN/START (3194595626): found list default
Jan 30 12:17:09: AAA/AUTHEN (3194595626): status = UNKNOWN
Jan 30 12:17:09: AAA/AUTHEN/START (3194595626): Method=TACACS+
Jan 30 12:17:09: TAC+: send AUTHEN/START packet ver=193 id=3194595626
Jan 30 12:17:09: TAC+: ver=192 id=3194595626 received AUTHEN status = ERROR
Jan 30 12:17:09: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:09: AAA/AUTHEN: create_user (0x2281AC) user='ABCDE'
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:09: TAC+: ver=192 id=3639011179 received AUTHEN status = PASS
Jan 30 12:17:09: AAA/AUTHEN: free_user (0x2281AC) user='ABCDE' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:09: AAA/AUTHEN (3194595626): status = PASS
Jan 30 12:17:09: AAA/AUTHEN: free_user (0x21F6D0) user='ABCDE' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:09: Tnl 56 L2TP: O SCCRP to rtp_tunnel tnlid 74
Jan 30 12:17:09: Tnl 56 L2TP: Tunnel state change from idle to
wait-ctl-reply
Jan 30 12:17:10: Tnl 56 L2TP: O Resend SCCRP, flg TLF, ver 2, len 152,
tnl 74, cl 0, ns 0, nr 1
Jan 30 12:17:10: Tnl 56 L2TP: I SCCCN from rtp_tunnel tnl 74
Jan 30 12:17:10: Tnl 56 L2TP: Got a Challenge Response in SCCCN from rtp_tunnel
Jan 30 12:17:10: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:10: AAA/AUTHEN: create_user (0x227F3C) user='ABCDE'
```

```
ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:10: AAA/AUTHEN/STARTTranslating "rtp.cisco.com"
(4117701992): port='' list='default' action=SENDAUTH service=PPP
Jan 30 12:17:10: AAA/AUTHEN/START (4117701992): found list default
Jan 30 12:17:10: AAA/AUTHEN (4117701992): status = UNKNOWN
Jan 30 12:17:10: AAA/AUTHEN/START (4117701992): Method=TACACS+
Jan 30 12:17:10: TAC+: send AUTHEN/START packet ver=193 id=4117701992
Jan 30 12:17:11: TAC+: ver=192 id=4117701992 received AUTHEN status = ERROR
Jan 30 12:17:11: AAA: parse name= idb type=-1 tty=-1
Jan 30 12:17:11: AAA/AUTHEN: create_user (0x228E68) user='ABCDE' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: TAC+: ver=192 id=2827432721 received AUTHEN status = PASS
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x228E68) user='ABCDE' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: AAA/AUTHEN (4117701992): status = PASS
Jan 30 12:17:11: AAA/AUTHEN: free_user (0x227F3C) user='ABCDE' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
Jan 30 12:17:11: Tnl 56 L2TP: Tunnel Authentication success
Jan 30 12:17:11: Tnl 56 L2TP: Tunnel state change from wait-ctl-reply
to established
Jan 30 12:17:11: Tnl 56 L2TP: SM State established
Jan 30 12:17:11: Tnl 56 L2TP: I ICRQ from rtp_tunnel tnl 74
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: Session FS enabled
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: Session state change from idle to
wait-for-tunnel
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: New session created
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: O ICRP to rtp_tunnel 74/1
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: Session state change from wait-for-tunnel
to wait-connect
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: I ICCN from rtp_tunnel tnl 74, cl 1
Jan 30 12:17:11: Tnl/Cl 56/1 L2TP: Session state change from wait-connect
to established
Jan 30 12:17:11: Vi1 VTEMPLATE: Reuse Vi1, recycle queue size 0
Jan 30 12:17:11: Vi1 VTEMPLATE: Hardware address 00e0.1e68.942c
Jan 30 12:17:11: Vi1 VPDN: Virtual interface created for user1@rtp.cisco.com
Jan 30 12:17:11: Vi1 VPDN: Set to Async interface
Jan 30 12:17:11: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
Jan 30 12:17:11: Vi1 VTEMPLATE: Has a new cloneblk vtemplate, now it has vtemplate
Jan 30 12:17:11: Vi1 VTEMPLATE: ************ CLONE VACCESS1 *****************
Jan 30 12:17:11: Vi1 VTEMPLATE: Clone from Virtual-Template1
```

リモート クライアントでの L2TP トンネルの確立と PPP のネゴシエーションおよび認証の確認

このタスクは、L2TP トンネルが確立済みであること、およびトンネル サーバがリモート クライアントと PPP ネゴシエーションおよび認証を実行できることを確認する場合に実行します。

次の例の各ステップは、リモート AAA をトンネル ターミネータとして実行するトンネル サーバで実行されています。これらのステップは、リモート AAA がダイヤルイン VPDN 用のトンネル イニシエータ、またはダイヤルアウト VPDN 用のトンネル ターミネータとして NAS で実行中のときは、NAS で実行することもできます。

手順の概要

1. **enable**
2. **debugpppnegotiation**
3. **debugpppauthentication**
4. **showlogging**

手順の詳細

ステップ 1 **enable**
このコマンドを使用して、特権 EXEC モードを有効にします。プロンプトにパスワードを入力します。

例：

```
Router> enable
```

ステップ 2 **debugpppnegotiation**
このコマンドをトンネル サーバで入力して、PPP ネゴシエーションのデバッグ メッセージを表示します。

例：

```
Router# debug ppp negotiation
```

ステップ 3 **debugpppauthentication**
このコマンドをトンネル サーバで入力して、PPP 認証のデバッグ メッセージを表示します。

例：

```
Router# debug ppp authentication
```

ステップ 4 **showlogging**
このコマンドをトンネル サーバで入力して、標準システム ロギング メッセージ バッファの内容を表示します。トンネル サーバが PPP チャレンジ ハンドシェイク認証プロトコル（CHAP）のチャレンジを受信してから、クライアントに PPP CHAP の「SUCCESS」を送信することを確認します。

例：

```
00:38:50: ppp3 PPP: Received LOGIN Response from AAA = PASS
00:38:50: ppp3 PPP: Phase is FORWARDING, Attempting Forward
00:38:50: Vi4.1  Tnl/Sn4571/4 L2TP: Session state change from wait-for-service-selection to
established
00:38:50: Vi4.1 PPP: Phase is AUTHENTICATING, Authenticated User
00:38:50: Vi4.1 CHAP: O SUCCESS id 1 len 4
```

PPP 認証が成功したら、デバッグ出力で PPP ネゴシエーションが開始済みであること、トンネル サーバが Link Control Protocol（LCP）IP Control Protocol（IPCP）パケットを受信済みであること、およびそのネゴシエーションが成功していることを確認します。

例：

```
00:38:50: Vi4.1 IPCP: State is Open
00:38:50: Vi4.1 IPCP: Install route to 10.1.1.4
```

VPDN ユーザの誘導要求の認証の設定

VPDN ユーザの誘導される認可要求を NAS またはトンネル サーバで設定することができます。誘導される要求は、最終的に認証を実行するデバイス上で設定します。誘導される要求は、通常トンネル サーバで設定されます。

次のいずれかのタスクを実行して、VPDN ユーザの誘導される認可要求を有効にします。

トンネル サーバでの VPDN ユーザの誘導要求の認証の設定

トンネルサーバが認証を行っている場合、VPDN ユーザの誘導要求の認証を設定するには、トンネル サーバでこの作業を実行します。

はじめる前に

手順の概要

1. **enable**
2. **configureterminal**
3. **iphost**{*name* | **t***modem-telephone-number*} [*tcp-port-number*] *address1* [*address2...address8*]
4. 次のいずれかを実行します。
   - **radius-serverdirected-request** [**restricted**]
   - **tacacs-serverdirected-request** [**restricted**] [**no-truncate**]
5. **vpdnauthorizedirected-request**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**iphost**{*name* | **t***modem-telephone-number*} [*tcp-port-number*] *address1* [*address2...address8*] 例： `Router(config)# ip host example.com 10.3.3.3`	ネットワーク サーバのホスト名を指定または修正します。 （注） 「VPDN 用のリモート AAA の設定, （35 ページ）」のタスクを実行するときは、**iphost** コマンドに指定した IP アドレスは **radius-serverhost** または **tacacs-serverhost** コマンドに設定した IP アドレスと一致する必要があります。

ステップ 4	次のいずれかを実行します。
	
	• **radius-serverdirected-request** [**restricted**]
	
	• **tacacs-serverdirected-request** [**restricted**] [**no-truncate**]
	
	例：
	
	`Router(config)# radius-server directed-request`
	
	例：
	
	`Router(config)# tacacs-server directed-request`
		NAS にログインしているユーザが認証用の RADIUS サーバを選択できるようにします。
		
		または
		
		NAS にログインしているユーザが認証用の TACACS+ サーバを選択できるようにします。

ステップ 5	**vpdnauthorizedirected-request** 例： `Router(config)# vpdn authorize directed-request`	誘導要求ユーザの VPDN 認証を有効にします。

次の作業

「VPDN トンネル認証の設定」セクションでのプロセスを実行する必要があります。

NAS での VPDN ユーザの誘導要求の認証の設定

NAS が認証を行うときは、VPDN ユーザの誘導認証を設定するには、NAS でこの作業を実行します。

はじめる前に

「VPDN 用のリモート AAA」セクションのタスクを実行する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **iphost**{*name* | **t***modem-telephone-number*} [*tcp-port-number*] *address1* [*address2...address8*]
4. 次のいずれかを実行します。
   - **radius-serverdirected-request** [**restricted**]
   - **tacacs-serverdirected-request** [**restricted**] [**no-truncate**]
5. **vpdnauthorizedirected-request**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**iphost**{*name* | **t***modem-telephone-number*} [*tcp-port-number*] *address1* [*address2...address8*] 例： `Router(config)# ip host example.com 10.3.3.3`	ネットワーク サーバのホスト名を指定または修正します。 （注） 「VPDN 用のリモート AAA の設定, （35 ページ）」のタスクを実行するときは、**iphost** コマンドに指定した IP アドレスは **radius-serverhost** または **tacacs-serverhost** コマンドに設定した IP アドレスと一致する必要があります。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかを実行します。
	• **radius-serverdirected-request** [**restricted**]
	• **tacacs-serverdirected-request** [**restricted**] [**no-truncate**]
	例：
	`Router(config)# radius-server directed-request`
	例：
	`Router(config)# tacacs-server directed-request`
		NAS にログインしているユーザが認証用の RADIUS サーバを選択できるようにします。
		または
		NAS にログインしているユーザが認証用の TACACS+ サーバを選択できるようにします。

ステップ 5	**vpdnauthorizedirected-request** 例： `Router(config)# vpdn authorize directed-request`	誘導要求ユーザの VPDN 認証を有効にします。

次の作業

「VPDN トンネル認証の設定」セクションでのプロセスを実行する必要があります。

ドメイン名のプレフィックス、サフィックスの削除の設定

単一の削除ルールのセットをグローバルに設定できます。各バーチャルプライベートネットワーク（VPN）ルーティングと転送（VRF）インスタンス用に、独立した一連の削除ルールを設定できます。

グローバルの削除のルールはすべてのユーザ名に適用され、VRF ごとのルールは指定した VRF に関連付けられたユーザ名のみに適用されます。VRF ごとのルールが設定されている場合、その VRF と関連付けられたユーザ名については、グローバルのルールより優先されます。

グローバルまたは VRF ごとの一連の削除ルールを設定するには、NAS でこの作業を実行します。

はじめる前に

- AAA を NAS で有効にする必要があります。「NAS とトンネルサーバでの AAA の設定」セクションを参照してください。

- 『VPDN Command Reference』の説明を参照し、**radius-serverdomain-stripping** コマンドの使用方法のガイドラインを理解する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. 次のいずれかを実行します。
   - **radius-serverdomain-stripping**[**right-to-left**] [**prefix-delimiter***character* [*character2...character7*]] [**delimiter***character* [*character2...character7*]] [**vrf***vrf-name*]
   - **tacacs-serverdomain-stripping**[**right-to-left**] [**prefix-delimiter***character* [*character2...character7*]] [**delimiter***character* [*character2...character7*]] [**vrf***vrf-name*]
4. 次のいずれかを実行します。
   - **radius-serverdomain-strippingstrip-suffix***suffix*[**vrf***vrf-name*]
   - **tacacs-serverdomain-strippingstrip-suffix***suffix*[**vrf***vrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを実行します。 • **radius-serverdomain-stripping**[**right-to-left**] [**prefix-delimiter***character* [*character2...character7*]] [**delimiter***character* [*character2...character7*]] [**vrf***vrf-name*] • **tacacs-serverdomain-stripping**[**right-to-left**] [**prefix-delimiter***character* [*character2...character7*]] [**delimiter***character* [*character2...character7*]] [**vrf***vrf-name*]	（オプション）ユーザ名を RADIUS サーバに転送する前にユーザ名からサフィックスまたはプレフィックスとサフィックスの両方を削除するようルータを設定します。 または （オプション）ユーザ名を TACACS+ サーバに転送する前にユーザ名からサフィックスまたはプレフィックスとサフィックスの両方を削除するようルータを設定します。

	コマンドまたはアクション	目的

	例：
	`Router(config)# radius-server domain-stripping prefix-delimiter #%&\\ delimiter @/`
	
	例：
	`Router(config)# tacacs-server domain-stripping prefix-delimiter %\$ vrf myvrf`
		• **right-to-left**：デリミタのユーザ名をデフォルトの左から右ではなく、右から左へと解析するようルータを設定します。プレフィックスまたはサフィックスはルータによって検出された最初の有効なデリミタ文字から削除されます。ルータがユーザ名を解析する方向を変更することで、有効なデリミタが複数あるユーザ名から削除する部位を制御できます。
		
		（注） グローバルまたはVRFごとの一連のルールには、分析方向をひとつだけ設定できます。ルータは、プレフィックスをある方向に解析し、サフィックスを別の方向に解析するようには設定できません。
		
		• **prefix-delimiter***character* [*character2...character7*]：プレフィックスの削除を有効にし、プレフィックス デリミタとして認識される 1 つまたは複数の文字を指定します。*character* 引数の有効な値は @、/、$、%、\、# と - です。スペースを挟むことなく複数の文字を入力できます。プレフィックスデリミタとして7文字までを定義できます。これが有効な文字の最大数です。*character* 引数の最後の文字または唯一の文字として\を入力する場合は、\\ と入力する必要があります。
		
		（注） プレフィックスの削除を有効にすると、デフォルトのサフィックスデリミタである@を使用したサフィックスの削除が自動的に有効になります。ただし、**delimiter***character* キーワード、引数を使用して別のサフィックスデリミタを設定した場合を除きます。
		
		• **delimiter***character* [*character2...character7*]：サフィックスのデリミタとして認識される文字を指定します。*character*引数の有効な値は@、/、$、%、\、# と - です。スペースを挟むことなく複数の文字を入力できます。プレフィックス デリミタとして 7 文字までを定義できます。これが有効な文字の最大数です。*character* 引数の最後の文字または唯一の文字として\を入力する場合は、\\ と入力する必要があります。

	コマンドまたはアクション	目的
		• **vrf***vrf-name*：削除設定を VRF インスタンスに限定します。*vrf-name* 引数には、設定されている VRF の名前を指定します。

ステップ 4	次のいずれかを実行します。
	• **radius-serverdomain-strippingstrip-suffix***suffix*[**vrf***vrf-name*]
	• **tacacs-serverdomain-strippingstrip-suffix***suffix*[**vrf***vrf-name*]
	例：
	`Router(config)# radius-server domain-stripping strip-suffix cisco.com`
	例：
	`Router(config)# tacacs-server domain-stripping strip-suffix cisco.net vrf myvrf`
		（オプション）ユーザ名を RADIUS サーバに転送する前にユーザ名から特定のサフィックスを削除するようルータを設定します。
		または
		（オプション）ユーザ名を TACACS+ サーバに転送する前にユーザ名から特定のサフィックスを削除するようルータを設定します。
		• **strip-suffix***suffix*：サフィックスごとのサフィックス削除を有効にし、削除するために一致を検証する文字列を指定します。
		（注） フルユーザ名からサフィックスが削除されるのは、サフィックスデリミタとサフィックスの両方が一致した場合のみです。別のサフィックス デリミタまたは一連のサフィックスデリミタを指定しない場合は、デフォルトのサフィックスデリミタである @ が使用されます。
		• **vrf***vrf-name*：サフィックスごとの削除設定を VRF インスタンスに限定します。*vrf-name* 引数は、VRF の名前を指定します。
		（注） この手順を複数回実行することで、複数の特定のサフィックスを削除する単一のルールセットを設定できます。

次の作業

「VPDN トンネル認証の設定」セクションでのプロセスを実行する必要があります。

VPDN トンネル認証の設定

VPDN トンネル認証を使用すれば、ルータは VPDN トンネルを確立する前に、他のトンネル エンドポイントを認証できます。VPDN トンネル認証はオプションですが、L2TP、L2TPv3、および PPTP の各トンネルについては強く推奨します。

デフォルトでは、ルータは VPDN トンネル認証のトンネル名としてホスト名を使用します。ローカル名が VPDN グループの下で設定されている場合、ルータはその VPDN グループに属すトンネルに対して認証をネゴシエートする際に、このローカル名を使用します。

NAS 側開始 VPDN 導入の場合、トンネル認証には 1 つの共有秘密が NAS とトンネル サーバの両方で設定される必要があります。L2TP トンネルの場合、パスワードは、ホスト名、ローカル名、または L2TP トンネルのパスワードを使用して設定できます。

クライアント側開始 VPDN トンネリング導入の場合、トンネル認証には、1 つの共有秘密がクライアントとトンネル サーバの両方で設定される必要があります。使用できる認証設定のオプションは、使用されるトンネリング プロトコルによって異なります。

L2TPv3 クライアント側開始 VPDN トンネルの場合、共有秘密は、次のいずれかの方法で、ローカル ピア ルータおよびトンネル サーバ上で設定できます。

- L2TP クラスの設定で。このセクションに記載されているプロセスの代わりに、「クライアント側開始ダイヤルイン VPDN トンネリングの設定」モジュールの「L2TP コントロール チャネルの認証パラメータの設定」タスクを実行します。
- このセクションに記載されているプロセスの説明に従ってルータのホスト名を使用。

L2TP クライアント側開始 VPDN トンネルの場合、共有秘密は、このセクションに記載されているプロセスの説明に従って、ホスト名、ローカル名、または L2TP トンネルのパスワードを使用してトンネル サーバで設定できます。共有秘密は、次のいずれかの方法で、ローカル ピア ルータ上で設定できます。

- L2TP クラスの設定で。このセクションに記載されているプロセスの代わりに、「クライアント側開始ダイヤルイン VPDN トンネリングの設定」モジュールの「L2TP コントロール チャネルの認証パラメータの設定」タスクを実行します。
- このセクションに記載されているプロセスの説明に従ってルータのホスト名を使用。

PPTP クライアント側開始 VPDN トンネルの場合、認証パラメータは、このセクションに記載されているプロセスの説明に従って、ホスト名またはローカル名を使用して設定できます。

VPDN トンネル認証を設定するには、必要に応じて NAS およびトンネル サーバ上で次のいずれかのタスクを実行する必要があります。NASおよびトンネルサーバ上で秘密を設定するために、同じ方法を選択する必要はありません。ただし、設定されるパスワードは両方のデバイスで同じでなければなりません。

L2TP トンネルでは、VPDN トンネル認証はオプションです。VPDN トンネル認証を無効にする場合は、NAS およびトンネル サーバ上で次のタスクを実行します。

前提条件

AAA が有効である必要があります。「NAS とトンネルサーバでの AAA の設定」セクションを参照してください。

ホスト名を使用した VPDN トンネル認証の設定

ホスト名を使って VPDN トンネル認証を設定するには、NAS またはトンネル サーバで次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **hostname***name*
4. **username***name***password***secret*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**hostname***name* 例： `Router(config)# hostname tunnelserver12`	ネットワーク サーバのホスト名を指定または修正します。
ステップ 4	**username***name***password***secret* 例： `Router(config)# username nas4 password mysecret`	ユーザ名をベースとした認証システムを構築します。 • 指定するユーザ名はリモート ルータの名前とします。 • 両方のルータでシークレット パスワードが同じである必要があります。

次の作業

- トンネルのエンドポイントでシークレット パスワードを設定したら、対応するトンネル エンドポイントで同じトンネルの鍵を設定する必要があります。

ローカル名を使用した VPDN トンネル認証の設定

ローカル名を使って VPDN トンネル認証を設定するには、NAS またはトンネル サーバで次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **localname***host-name*
5. **exit**
6. **username***name***password***secret*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group mygroup`	VPDN グループ設定モードに入り、VPDN グループを作成します。

	コマンドまたはアクション	目的
ステップ 4	**localname***host-name* 例： `Router(config-vpdn)# local name tunnelserver2`	トンネルが自身を識別するために使用するローカル ホスト名を指定します。
ステップ 5	**exit** 例： `Router(config-vpdn)# exit`	VPDN グループ コンフィギュレーション モードを終了します。
ステップ 6	**username***name***password***secret* 例： `Router(config)# username nas7 password mysecret`	ユーザ名をベースとした認証システムを構築します。 • 指定するユーザ名はリモート ルータの名前とします。 • 両方のルータでシークレット パスワードが同じである必要があります。

次の作業

- トンネルのエンドポイントでシークレット パスワードを設定したら、対応するトンネル エンドポイントで同じトンネルの鍵を設定する必要があります。

L2TP トンネル パスワードを使用した VPDN トンネル認証の設定

L2TP トンネル パスワードを使って VPDN トンネル認証を設定するには、NAS またはトンネル サーバで次の作業を実行します。この作業は、L2TP トンネルの VPDN トンネル認証でのみ使用できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **l2tptunnelpassword***password*
5. **localname***host-name*
6. **exit**
7. **username***name***password***secret*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group mygroup`	VPDN グループ設定モードに入り、VPDN グループを作成します。
ステップ 4	**l2tptunnelpassword***password* 例： `Router(config-vpdn)# l2tp tunnel password mysecret`	トンネルを認証するためにルータが使用するパスワードを設定します。
ステップ 5	**localname***host-name* 例： `Router(config-vpdn)# local name tunnelserver2`	（オプション）トンネルが自身を識別するために使用するローカル ホスト名を指定します。 • リモート ルータが L2TP トンネル パスワードを使用しない場合、この手順を実行する必要があります。
ステップ 6	**exit** 例： `Router(config-vpdn)# exit`	（オプション）VPDN グループ コンフィギュレーション モードを終了します。 • リモート ルータが VPDN トンネル認証で L2TP トンネル パスワード方式を使用しない場合のみ、この手順を実行する必要があります。
ステップ 7	**username***name***password***secret* 例： `Router(config)# username nas64 password mysecret`	（オプション）ユーザ名をベースとした認証システムを構築します。 • リモート ルータが VPDN トンネル認証で L2TP トンネル パスワード方式を使用しない場合のみ、この手順を実行する必要があります。 • 指定するユーザ名はリモート ルータの名前とします。

	コマンドまたはアクション	目的
		• 両方のルータでパスワードが同じである必要があります。

次の作業

- トンネルのエンドポイントでシークレット パスワードを設定したら、対応するトンネル エンドポイントで同じトンネルの鍵を設定する必要があります。

L2TP トンネル用の VPDN トンネル認証の無効化

L2TP トンネルの VPDN トンネル認証を無効にするには、次の作業を実行します。VPDN トンネル認証を無効にするには、NAS とトンネル サーバの両方でこの作業を実行する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **nol2tptunnelauthentication**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group mygroup`	VPDN グループ設定モードに入り、VPDN グループを作成します。

	コマンドまたはアクション	目的
ステップ 4	**nol2tptunnelauthentication** 例： `Router(config-vpdn)# no l2tp tunnel authentication`	L2TP トンネル認証を無効化します。

L2TP VPDN 用の RADIUS トンネル アカウンティングの設定

新しい RADIUS トンネル アカウンティング タイプは、アカウンティング要求がユーザ サービスの始まり（開始）と終わり（終了）のどちらを表しているかを示す、RADIUS アカウンティング属性の Acct-Status-Type（属性 40）と一緒に使用されます。

このタスクを使用して、トンネル レコードと tunnel-link アカウンティング レコードをリモートの RADIUS サーバに送信するように NAS またはトンネルサーバを設定します。

はじめる前に

- NAS とトンネル サーバでの AAA の設定, （33 ページ）でタスクを実行する必要があります。
- 「VPDN 用のリモート AAA の設定, （35 ページ）」の説明に従って、リモート AAA RADIUS サーバを使用するようにルータを設定する必要があります。
- 「VPDN トンネル認証の設定」セクションにあるタスクを実行する必要があります。

（注） RADIUS トンネルアカウンティングは L2TP トンネル プロトコルを使用する VPDN でのみサポートされています。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaaaccountingnetworkdefault**| *list-name*} {**start-stop** | **stop-only** | **wait-start** | **nonegroup***groupname*
4. **vpdntunnelaccountingnetwork***list-name*
5. **vpdnsessionaccountingnetwork***list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaaaccountingnetworkdefault**| *list-name*} {**start-stop** | **stop-only** | **wait-start** | **nonegroup***groupname* 例： `Router(config)# aaa accounting network list1 start-stop group radius`	ネットワーク アカウンティングを有効にします。 • **default**：デフォルトのネットワーク アカウンティングの方式リストが設定され、インターフェイス上でどの追加のアカウンティング設定も有効になっていない場合は、デフォルトで、ネットワーク アカウンティングが有効になります。**vpdn session accounting network** コマンドまたは **vpdn tunnel accounting network** コマンドが **default** 方式リストにリンクされている場合、すべてのトンネルおよびトンネルリンク アカウンティング レコードが、これらのセッションで有効になります。 • *list-name*：**aaa accounting** コマンドで定義された *list-name* は、VPDN コマンドで定義された *list-name* と同一である必要があります。そうでない場合、アカウンティングは発生しません。
ステップ 4	**vpdntunnelaccountingnetwork***list-name* 例： `Router(config)# vpdn tunnel accounting network list1`	Tunnel-Start、Tunnel-Stop、および Tunnel-Reject アカウンティング レコードを有効にします。 • *list-name*：*list-name* は、**aaa accounting** コマンドで定義された *list-name* と一致している必要があります。そうでない場合、ネットワーク アカウンティングは発生しません。
ステップ 5	**vpdnsessionaccountingnetwork***list-name* 例： `Router(config)# vpdn session accounting network list1`	Tunnel-Link-Start、Tunnel-Link-Stop、および Tunnel-Link-Reject アカウンティング レコードを有効にします。 • *list-name*：*list-name* は、**aaa accounting** コマンドで定義された *list-name* と一致している必要があります。そうでない場合、ネットワーク アカウンティングは発生しません。

トンネル終端装置のリモート RADIUS AAA サーバでの L2TP トンネルの認証の設定

L2TP トンネルの場合、リモート RADIUS AAA を実行するように、VPDN トンネルを終端させるデバイスを設定できます。リモート RADIUS AAA サーバは、トンネル ターミネータで VPDN トンネル認証を実行するために、次のように使用できます。

- ダイヤルイン VPDN 用のトンネル サーバでリモート RADIUS AAA サーバを使用する
- ダイヤルアウト VPDN 用の NAS でリモート RADIUS AAA サーバを使用する

このタスクは、トンネルを終端させるデバイスでVPDNトンネルを認証するように、RADIUSサーバを設定する場合に、リモート RADIUS AAA サーバで実行します。

はじめる前に

- RADIUS サーバは AAA 向けに設定されている必要があります。リモート RADIUS AAA サーバの設定の詳細については、「その他の参考資料」セクションを参照してください。
- トンネル イニシエータの RADIUS ユーザ プロファイル内のサービス タイプは、常に「Outbound」に設定する必要があります。

（注） このタスクは、VPDN トンネルを終端させるデバイスがリモート RADIUS AAA を実行している場合にのみ当てはまります。リモート RADIUS AAA を実行するようにトンネル ターミネータを設定するには、「L2TP トンネルのリモート RADIUS AAA 用のトンネル終端装置の設定」セクションのタスクを実行してください。

手順の概要

1. **servicetype=***Outbound*
2. **tunnel-type=***protocol*
3. **Cisco:Cisco-Avpair=vpdn:dout-dialer=***NAS-dialer-number*
4. **Cisco:Cisco-Avpair=vpdn:vpdn-vtemplate=***vtemplate-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**servicetype=***Outbound* 例： `service type = Outbound`	サービス タイプを指定します。
ステップ 2	**tunnel-type=***protocol* 例： `tunnel-type = l2tp`	トンネリング プロトコルを指定します。 （注） このタスクでは、L2TP が唯一の有効なプロトコルです。
ステップ 3	**Cisco:Cisco-Avpair=vpdn:dout-dialer=***NAS-dialer-number* 例： `Cisco:Cisco-Avpair = vpdn:dout-dialer = 2`	ダイヤルアウト設定用の NAS で使用するダイヤラを指定します。 （注） この手順は、ダイヤルアウト設定についてのみ実行します。
ステップ 4	**Cisco:Cisco-Avpair=vpdn:vpdn-vtemplate=***vtemplate-number* 例： `Cisco:Cisco-Avpair = vpdn:vpdn-vtemplate = 1`	ダイヤルイン設定用のトンネル サーバで使用する仮想テンプレート番号を指定します。 （注） この手順は、ダイヤルイン設定についてのみ実行します。 （注） この設定は、「L2TP トンネルのリモート RADIUS AAA 用のトンネル終端装置の設定，（38 ページ）」のタスクで **vpdntunnelauthorizationvirtual-template** コマンドが使用される場合はオプションです。

NAS リモート RADIUS AAA サーバのトンネル割り当て設定

トンネル割り当てにより、異なるユーザプロファイルのユーザや複数のドメイン RADIUS プロファイルからのユーザを同一のアクティブなトンネルにグループ分けできます。この機能により、トンネル タイプ、トンネル エンドポイントのタイプ、トンネル割り当て ID が同じ場合にトンネルの重複した確立を防止できます。

同一トンネルのグループに分類する各ユーザとドメインについて、NAS リモート RADIUS AAA サーバで次の作業を実行します。

はじめる前に

RADIUS サーバは AAA 向けに設定されている必要があります。

手順の概要

1. 次のいずれかを実行します。
   - *user@domain.com***Password="***secret***"Service-Type=Outbound**
   - *user.domain.com***Password="***secret***"Service-Type=Outbound**
2. **tunnel-type=***protocol*
3. **tunnel-server-endpoint=***ip-address*
4. **tunnel-assignment-id=***name*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	次のいずれかを実行します。
	• *user@domain.com***Password="***secret***"Service-Type=Outbound**
	• *user.domain.com***Password="***secret***"Service-Type=Outbound**
	
	例：
	`user@cisco.com Password = "cisco" Service-Type = Outbound`
	
	例：
	`user.cisco.com Password = "cisco" Service-Type = Outbound`
		ユーザまたはドメイン、トンネルのパスワードとサービス タイプを指定します。

ステップ 2	**tunnel-type=***protocol* 例： `tunnel-type = l2tp`	使用するトンネリング プロトコルを指定します。 • トンネルのタイプは、同一のトンネルに分類するユーザについて同じでなければなりません。
ステップ 3	**tunnel-server-endpoint=***ip-address* 例： `tunnel-server-endpoint = 10.1.1.1`	指定したユーザまたはドメインからの通信をトンネルするトンネル サーバの IP アドレスを指定します。 • トンネル サーバのエンドポイントは、同一のトンネルに分類するユーザについて同じでなければなりません。

	コマンドまたはアクション	目的
ステップ 4	**tunnel-assignment-id=***name* 例： `tunnel-assignment-id = group1`	指定したユーザまたはドメインからの通信に割り当てられるトンネル ID を指定します。 • トンネル割り当て ID は、同一のトンネルにグループ分けされるユーザについて同じでなければなりません。

NAS リモート RADIUS AAA サーバのセキュアなトンネル認証名の設定

NAS AAA サーバには NAS または NAS AAA サーバ向けのデフォルト名以外の認証名を設定できます。それにより、VPDN トンネル確立時により高度なセキュリティが確保できます。

RADIUS トンネル認証名属性により、デフォルト以外の名前をトンネル イニシエータとトンネル ターミネータに指定できます。これらの認証名は RADIUS トンネル属性 90 および 91 を使用して指定します。

リモート RADIUS AAA サーバで次の手順を実行します。この作業は、L2TP または L2F による NAS 始動のトンネルに適用されます。

はじめる前に

- RADIUS サーバは AAA 向けに設定されている必要があります。
- NAS は RADIUS 属性 90 および 91 を認識できる必要があります。
- RADIUS トンネル属性の 90 と 91 を使用するには、RADIUS サーバがタグ付き属性をサポートしている必要があります。タグ付き属性は、RFC 2868 の『*RADIUS Tunnel Authentication Attributes*』で定義されています。

手順の概要

1. 次のいずれかを実行します。
   - *user@example.com***Password="***secret***"Service-Type=Outbound**
   - *user.example.com***Password="***secret***"Service-Type=Outbound**
2. **tunnel-client-auth-id={:1 |:2}:"***NAS-name***"**
3. **tunnel-server-auth-id={:1 |:2}:"***tunnel-server-name***"**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	次のいずれかを実行します。
	• *user@example.com***Password="***secret***"Service-Type=Outbound**
	• *user.example.com***Password="***secret***"Service-Type=Outbound**
	例：
	`user@cisco.com Password = "cisco" Service-Type = Outbound`
	例：
	`user.cisco.com Password = "cisco" Service-Type = Outbound`
		ユーザまたはドメイン、トンネルのパスワードとサービス タイプを指定します。

ステップ 2	**tunnel-client-auth-id=**{**:1** |**:2**}**:"***NAS-name***"** 例： `tunnel-client-auth-id = :2:NAS36`	トンネル サーバでトンネルの設置を認証する際に NAS が使用する名前を指定します。 • **:1**：L2F トンネルを指定します。 • **:2**：L2TP トンネルを指定します。
ステップ 3	**tunnel-server-auth-id=**{**:1** |**:2**}**:"***tunnel-server-name***"** 例： `tunnel-server-auth-id = :2:TS14`	NAS でトンネルの設置を認証する際にトンネル サーバが使用する名前を指定します。 • **:1**：L2F トンネルを指定します。 • **:2**：L2TP トンネルを指定します。

PPPoE タギング情報の L2TP 転送の設定

PPPoE のタギング情報の L2TP 転送設定

LNS の nas-port-id 属性に circuit-id タグを代入し、calling-station-id 属性に remote-id タグを代入するため、PPPoE タギング情報の L2TP 転送を設定するには LAC で次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **dsl-line-info-forwarding**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group pppoe-group`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**dsl-line-info-forwarding** 例： `Router(config-vpdn)# dsl-line-info-forwarding`	PADR パケットで受信した PPPoE Vendor-Specific タグの処理を有効にし、一致した VSA を RADIUS アクセスおよびアカウンティング要求で AAA サーバに送信します。
ステップ 5	**exit** 例： `Router(config-vpdn)# exit`	VPDN グループ コンフィギュレーション モードを終了します。

PPPoE タグ情報の L2TP 転送の上書き

PPPoE タギング情報の L2TP 転送機能の設定をして、次の VSA を上書きすることができます。

circuit-id での nas-port VSA の上書き

LNS の nas-port-id 属性の circuit-id タグの内容を上書きするには、LNS で次の手順を実行してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **radius-serverattribute87circuit-id**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-serverattribute87circuit-id** 例： `Router(config)# radius-server attribute 87 circuit-id`	RADIUS アクセスとアカウンティング要求の Circuit-ID 属性で NAS-Port-Id 属性を上書きします。
ステップ 4	**exit** 例： `Router(config)# exit`	現在のモードを終了します。

remote-id での called-station-id VSA の上書き

LNS の remote-id で calling-station-id VSA を上書きするには、次の手順を実行してください:

手順の概要

1. **enable**
2. **configureterminal**
3. **radius-serverattribute31remote-id**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius-serverattribute31remote-id** 例： `Router(config)# radius-server attribute 31 remote-id`	RADIUS アクセスとアカウンティング要求の Remote-ID 属性で calling-station-id VSA を上書きします。
ステップ 4	**exit** 例： `Router(config)# exit`	現在のモードを終了します。

PPPoE タグ情報の L2TP 転送の削除

発信 PADO および PADS パケットには DSLAM で挿入された Vendor-Specific Line-Id タグが含まれます。また、DSLAM はパケットから Circuit-Id タグを取り除く必要があります。DSLAM でタグを取り除くことができない場合、BRAS はパケットを送信する前にタグを削除する必要があります。この作業は、BBA グループ コンフィギュレーション モードで **vendor-tagremote-idstrip** コマンドを設定して実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **bba-groupppppoe***group-name*
4. **vendor-tagremote-idstrip**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bba-groupppppoe***group-name* 例： `Router(config)# bba-group pppoe pppoe-group`	PPPoE プロファイルを定義し、BBA グループ コンフィギュレーション モードを開始します。
ステップ 4	**vendor-tagremote-idstrip** 例： `Router(config-bba-group)# vendor-tag remote-id strip`	BRAS で発信 PADO および PADS パケットから着信 Vendor-Specific Remote-Id タグを取り除くことができるようにします。

セッション アクティビティ ログの表示

radius-serverattributenas-portformatd グローバル コンフィギュレーション コマンドが BRAS の PPPoE Circuit-Id タグ処理機能に追加されると（例については、「例：VPDN トンネル認証の検索順序の設定，（88 ページ）」を参照してください）、**debugradius** 特権 EXEC コマンドからのレポートに、ディスカバリ フレームを受信する着信アクセスインターフェイスに関する情報と、確立されているセッションに関する情報が PPPoE 拡張 NAS-Port 形式（format d）で含まれます。

手順の概要

1. セッション アクティビティのレポートを表示するには、**debugradius** コマンドを有効にします。ここに示す例では、次を前提とします。

手順の詳細

セッション アクティビティのレポートを表示するには、**debugradius** コマンドを有効にします。ここに示す例では、次を前提とします。

- acct_session_id は、16 進形式の 79 または 4F です。
- メッセージ「*Acct-session-id pre-pended with Nas Port = 0/0/0/200*」で、PPPoE ディスカバリ フレームが到着したインターフェイスは FastEthernet0/0.200 です。0/0/0 は、slot/subslot/port のシスコ形式です。
- Acct-Session-Id の vendor-specific 属性 44 には、入力インターフェイスとセッション ID の組み合わせを表す文字列「*0/0/0/200_0000004F*」が含まれます。

（注） **debugradius** 出力ログの重要な文字列は、例示のみの目的で太字になっています。

例：

```
Router# debug radius
02:10:49: RADIUS(0000003F): Config NAS IP: 0.0.0.0
02:10:49: RADIUS/ENCODE(0000003F): acct_session_id: 79
02:10:49: RADIUS(0000003F): sending
02:10:49: RADIUS/ENCODE: Best Local IP-Address 10.0.58.141 for Radius-Server 172.20.164.143
02:10:49: RADIUS(0000003F): Send Access-Request to 172.20.164.143:1645 id 1645/65, len 98
02:10:49: RADIUS:  authenticator 1C 9E B0 A2 82 51 C1 79 - FE 24 F4 D1 2F 84 F5 79
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                        [1]
02:10:49: RADIUS:  User-Name           [1]   7   "peer1"
02:10:49: RADIUS:  CHAP-Password       [3]   19  *
02:10:49: RADIUS:  NAS-Port-Type       [61]  6 Ethernet                   [15]
02:10:49: RADIUS:  NAS-Port            [5]   6   200
02:10:49: RADIUS:  NAS-Port-Id         [87]  22  "FastEthernet6/0.200:"
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                     [2]
02:10:49: RADIUS:  NAS-IP-Address      [4]   6   10.0.58.141
02:10:49: RADIUS: Received from id 1645/65 172.20.164.143:1645, Access-Accept, len 32 02:10:49:
RADIUS:  authenticator 06 45 84 1B 27 1F A5 C3 - C3 C9 69 6E B9 C0 6F 94
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                     [2]
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                        [1]
02:10:49: RADIUS(0000003F): Received from id 1645/65
02:10:49: [62]PPPoE 65: State LCP_NEGOTIATION    Event PPP_LOCAL
02:10:49: PPPoE 65/SB: Sent vtemplate request on base Vi2
02:10:49: [62]PPPoE 65: State VACCESS_REQUESTED    Event VA_RESP
02:10:49: [62]PPPoE 65: Vi2.1 interface obtained
02:10:49: [62]PPPoE 65: State PTA_BINDING    Event STAT_BIND
02:10:49: [62]PPPoE 65: data path set to Virtual Acess
02:10:49: [62]PPPoE 65: Connected PTA
02:10:49: [62]PPPoE 65: AAA get dynamic attrs
02:10:49: [62]PPPoE 65: AAA get dynamic attrs
02:10:49: RADIUS/ENCODE(0000003F):Orig. component type = PPoE
02:10:49: RADIUS/ENCODE(0000003F): Acct-session-id pre-pended with Nas Port = 0/0/0/200
02:10:49: RADIUS(0000003F): Config NAS IP: 0.0.0.0
02:10:49: RADIUS(0000003F): sending
02:10:49: RADIUS/ENCODE: Best Local IP-Address 10.0.58.141 for Radius-Server 172.20.164.143
02:10:49: RADIUS(0000003F): Send Accounting-Request to 172.20.164.143:1646 id 1 646/42, len 117
02:10:49: RADIUS:  authenticator 57 24 38 1A A3 09 62 42 - 55 2F 41 71 38 E1 CC 24
```

```
02:10:49: RADIUS:  Acct-Session-Id      [44]  20  "0/0/0/200_0000004F"
02:10:49: RADIUS:  Framed-Protocol      [7]   6 PPP                        [1]
02:10:49: RADIUS:  User-Name            [1]   7   "peer1"
02:10:49: RADIUS:  Acct-Authentic       [45]  6 RADIUS                     [1]
02:10:49: RADIUS:  Acct-Status-Type     [40]  6 Start                      [1]
02:10:49: RADIUS:  NAS-Port-Type        [61]  6 Ethernet                   [15]
02:10:49: RADIUS:  NAS-Port             [5]   6   200
02:10:49: RADIUS:  NAS-Port-Id          [87]  22  "FastEthernet6/0.200:"
02:10:49: RADIUS:  Service-Type         [6]   6 Framed                     [2]
02:10:49: RADIUS:  NAS-IP-Address       [4]   6   10.0.58.141
02:10:49: RADIUS:  Acct-Delay-Time      [41]  6   0
02:10:49: RADIUS: Received from id 1646/42 172.20.164.143:1646, Accounting-resp onse, len 20
02:10:49: RADIUS:  authenticator 34 84 7E B2 F4 40 B2 7C - C5 B2 4E 98 78 03 8B C0
```

PPPoE から受信した転送 rx 速度値と tx 速度値に対する L2TP の上書きの設定

L2TP は、デフォルトでは PPPoE から受信速度（receive-speed）（rx-speed）の値および送信速度（transmit-speed）（tx-speed）の値を取得し、それらの値を LNS に送信します。PPPoE から受信した転送 rx 速度値と tx 速度値の L2TP 転送を上書き（オーバーライド）するには、rx 速度値 と tx 速度値を RADIUS サーバで設定するか、あるいは VPDN グループの設定または VPDN テンプレート コンフィギュレーション モードで、**l2tp rx-speed** コマンドと **l2tp tx-speed** コマンドを使用して設定する必要があります。これらの速度の値は、kbps 単位で設定します。

RADIUS サーバを使用しない場合での rx 速度値と tx 速度値の設定

RADIUS サーバを使用しない場合、rx 速度と tx 速度の値は VPDN グループ設定または VPDN テンプレート コンフィギュレーション モードで指定できます。VPDN グループ コンフィギュレーションモードで設定した rx 速度と tx 速度の値は VPDN グループ専用のもので、トンネルの下にあるすべてのセッションに送信されます。

RADIUS サーバを使用しない場合、rx 速度と tx 速度の値を VPDN グループ コンフィギュレーションまたは VPDN テンプレート コンフィギュレーションモードで指定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnenable**
4. 次のいずれかを実行します。
   - **vpdn-group***name*
   - **vpdn-template***name*
5. **l2tprx-speed***value*
6. **l2tptx-speed***value*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnenable** 例： `Router(config)# vpdn enable`	ルータで VPDN をイネーブルにします。

ステップ 4	次のいずれかを実行します。
	• **vpdn-group***name*
	• **vpdn-template***name*
	例：
	`Router(config)# vpdn-group 1`
	例：
	`Router(config)# vpdn-template 1`
		VPDN グループ コンフィギュレーション モードを開始します。
		または
		VPDN テンプレート コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**l2tprx-speed***value* 例： `Router(config-vpdn)# l2tp rx-speed 15000`	LNS に rx 速度値を送信します。 • rx 速度値を指定しないと、L2TP は rx 速度の値を PPPoE から受け取ります。 （注） コマンドは、VPDN コンフィギュレーション モードまたは VPDN テンプレート コンフィギュレーション モードのどちらで入力されても同じです。次の手順では、VPDN グループ コンフィギュレーション モードでのコマンド入力の方法を説明します。
ステップ 6	**l2tptx-speed***value* 例： `Router(config-vpdn)# l2tp tx-speed 15000`	LNS に tx 速度値を送信します。 • tx 速度値を指定しないと、L2TP は tx 速度の値を PPPoE から受け取ります。
ステップ 7	**end** 例： `Router(config-vpdn)# end`	VPDN グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

RADIUS サーバでの rx 速度値と tx 速度値の設定

RADIUS サーバ上で rx 速度値と tx 速度値を指定して、RADIUS サーバで rx 速度値と tx 速度値を設定することができます。

rx 速度値と tx 速度値は、セッション単位で設定します。L2TP では、LAC 上で設定される **vpdn-authen-before-forward** コマンドを使用して、セッションごとに rx 速度値と tx 速度値を格納します。

RADIUS サーバ上でデフォルトの rx 速度値と tx 速度値を設定する手順は、RADIUS サーバを使用しない場合に rx 速度値と tx 速度値を設定する手順と同じです。RADIUS サーバ上での rx 速度値と tx 速度値の設定については、「RADIUS サーバを使用しない場合での rx 速度値と tx 速度値の設定」を参照してください。

RADIUS サーバでの ANCP からの rx 速度値と tx 速度値の設定

ANCP は L2TP にアップストリームとダウンストリームの値を送信します。アップストリームの値は rx 速度値であり、ダウンストリームの値は tx 速度値です。

ANCP で rx 速度と tx 速度値を設定するには、RADIUS サーバで次の作業を実行します。

はじめる前に

- クライアントと LAC 間の PPPoE に Quality of Service（QoS）ポリシーが設定されている必要があります。
- ANCP セッションと ANCP ネイバーセッションを開始しておく必要があります。
- ポリシー マップ クラス コンフィギュレーション モードで **shapeaverage** コマンドを使用し、デフォルトクラスのトラフィック シェーピングの平均レートを設定する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnenable**
4. 次のいずれかを実行します。
   - **vpdn-group***name*
   - **vpdn-template***name*
5. **l2tprx-speedancp** [*value*]
6. **l2tptx-speedancp** [*value*]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnenable** 例： `Router(config)# vpdn enable`	ルータで VPDN をイネーブルにします。
ステップ 4	次のいずれかを実行します。 • **vpdn-group***name*	VPDN グループ コンフィギュレーション モードを開始します。 または

	コマンドまたはアクション	目的

	• **vpdn-template***name*
	
	例：
	`Router(config)# vpdn-group 1`
	
	例：
	`Router(config)# vpdn-template 1`
		VPDN テンプレート コンフィギュレーション モードを開始します。

ステップ 5	**l2tprx-speedancp** [*value*] 例： `Router(config-vpdn)# l2tp rx-speed ancp 15000`	ANCP の rx 速度値が設定されていない場合、rx 速度の値を LNS に送信します。 • ANCP の rx 速度の値が設定されず、コマンドに rx 速度の値を指定しない場合は、L2PT は VPDN グループ設定または VPDN テンプレート コンフィギュレーション モードで設定されている rx 速度の値を送信します。 • rx 速度の値が VPDN グループ設定または VPDN テンプレート コンフィギュレーション モードで設定されていない場合は、L2TP は平均レート トラフィック シェーピング値を LNS へ送信します。 • ATM インターフェイスでは、平均レート トラフィック シェーピング値が設定されていない場合は、L2PT は VC- クラス コンフィギュレーション モードで設定されている rx 速度の値を送信します。rx 速度の値が VC- クラス コンフィギュレーション モードで設定されていない場合は、L2TP は PPPoE で取得した rx 速度値を送信します。 • イーサネット インターフェイスでは、平均レート トラフィック シェーピング値が設定されていない場合は、L2TP は PPPoE で取得した rx 速度値を送信します。
ステップ 6	**l2tptx-speedancp** [*value*] 例： `Router(config-vpdn)# l2tp tx-speed ancp 15000`	ANCP の tx 速度値が設定されていない場合、tx 速度の値を LNS に送信します。 • ANCP の tx 速度の値が設定されず、コマンドに tx 速度を指定しない場合は、L2PT は VPDN グループ コンフィギュレーションまたは VPDN テンプレート コンフィギュレーション モードで設定されている tx 速度の値を送信します。 • tx 速度の値がグループ コンフィギュレーションまたは VPDN テンプレート コンフィギュレーション モードで設定されていない場合は、L2TP は平均レート トラフィック シェーピング値を LNS へ送信します。

	コマンドまたはアクション	目的
		• ATM インターフェイスでは、平均レート トラフィック シェーピング値が設定されていない場合は、L2PT は **vbr-nrt** コマンドを使用して VC- クラス コンフィギュレーション モードに設定されたピーク セル レート（PCR）の値を送信します。tx 速度の値が VC- クラス コンフィギュレーション モードで設定されていない場合は、L2TP は PPPoE で取得した tx 速度値を送信します。 • イーサネット インターフェイスでは、平均レート トラフィック シェーピング値が設定されていない場合は、L2TP は PPPoE で取得した tx 速度値を送信します。
ステップ 7	**end** 例： `Router(config-vpdn)# end`	VPDN グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

RADIUS サーバでの RAM-min からの rx 速度値と tx 速度値の設定

RAM-min で rx 速度と tx 速度値を設定するには、RADIUS サーバで次の作業を実行します。

はじめる前に

- クライアントと LAC 間の PPPoE に Quality of Service（QoS）ポリシーが設定されている必要があります。
- ポリシー マップ クラス コンフィギュレーション モードで **shapeaverage** コマンドを使用し、デフォルトクラスのトラフィック シェーピングの平均レートを設定する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnenable**
4. 次のいずれかを実行します。
   - **vpdn-group***name*
   - **vpdn-template***name*
5. **l2tprx-speedram-min** [*value*]
6. **l2tptx-speedram-min** [*value*]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnenable** 例： `Router(config)# vpdn enable`	ルータで VPDN をイネーブルにします。

ステップ 4	次のいずれかを実行します。
	• **vpdn-group***name*
	• **vpdn-template***name*
	例：
	`Router(config)# vpdn-group 1`
	例：
	`Router(config)# vpdn-template 1`
		VPDN グループ コンフィギュレーション モードを開始します。
		または
		VPDN テンプレート コンフィギュレーション モードを開始します。

ステップ 5	**l2tprx-speedram-min** [*value*] 例： `Router(config-vpdn)# l2tp rx-speed ram-min 15000`	平均レート トラフィック シェーピング値が設定されていない場合、rx 速度の値を LNS に送信します。 • ATM インターフェイスでは、平均レート トラフィック シェーピング値が設定されず、コマンドに rx 速度の値を指定しない場合は、L2PT は VC- クラス コンフィギュレーション モードで設定されている rx 速度の値を送信します。rx 速度の値が VC- クラス コンフィギュレーションモードで設定されていない場合は、L2TP は PPPoE で取得した rx 速度値を送信します。 • イーサネット インターフェイスでは、平均レート トラフィック シェーピング値が設定されず、コマンドに rx 速度の値を指定しない場合は、L2TP は PPPoE で取得した rx 速度値を送信します。

	コマンドまたはアクション	目的
ステップ 6	**l2tptx-speedram-min** [*value*] 例： `Router(config-vpdn)# l2tp tx-speed ram-min 15000`	平均レート トラフィック シェーピング値が設定されていない場合、tx 速度の値を LNS に送信します。 • ATM インターフェイスでは、平均レート トラフィック シェーピング値が設定されず、コマンドに tx 速度の値を指定しない場合は、L2PT は **vbr-nrt** コマンドにより VC- クラス コンフィギュレーション モードに設定されたピーク セル レート（PCR）の値を送信します。tx 速度の値が VC- クラス コンフィギュレーション モードで設定されていない場合は、L2TP は PPPoE で取得した tx 速度値を送信します。 • イーサネット インターフェイスでは、平均レート トラフィック シェーピング値が設定されず、コマンドに tx 速度の値を指定しない場合は、L2TP は PPPoE で取得した tx 速度値を送信します。
ステップ 7	**end** 例： `Router(config-vpdn)# end`	VPDN グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

LNS アドレス チェックの設定

L2TP トンネルのセットアップの際、LAC が LNS が送信したトラフィックの IP アドレスを検証することを許容し、それにより複数のインターフェイスから到着するアップリンク、ダウンリンク トラフィックを検証するには、次の手順に従います。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnenable**
4. **vpdn-group***name*
5. **l2tpsecurityipaddress-check**
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnenable** 例： `Router(config)# vpdn enable`	ルータ上のバーチャル プライベート ダイヤルアップ ネットワーキングを有効にして、ルータにローカル データベースまたはリモート認可サーバ（ホームゲートウェイ、存在する場合）上でトンネル定義を検索するように指示します。
ステップ 4	**vpdn-group***name* 例： `Router(config)# vpdn-group example`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 5	**l2tpsecurityipaddress-check** 例： `Router(config-vpdn)# l2tp security ip address-check`	LNS がインバウンド、アウトバウンドのメッセージに含まれる IP アドレスを比較し、同一であることを確認するよう設定します。IP アドレスが一致しない場合、L2TP トンネルは確立されません。
ステップ 6	**exit** 例： `Router(config-vpdn)# exit`	VPDN グループ コンフィギュレーション モードを終了します。

改訂版 LNS のデッド キャッシュ処理の設定

デッド キャッシュ状態での LNS の特定

LNS のデッド キャッシュ処理の変更機能で、**showvpdndead-cache** コマンドを使用して、LAC の LSG にある LNS の状態を表示し、LNS が応答していない（デッドキャッシュ状態）かどうかを判

定できます。**showvpdndead-cache** コマンドは応答しない LNS の IP アドレスと、LNS がダウンしている時間のエントリを表示します。

この手順では、**showvpdndead-cache** コマンドを使用して LNS の状態を表示し、LNS が応答していない（デッドキャッシュ状態）かどうかを判定する方法を示します。LNS がキャッシュデッド状態のとき、新しいセッションや通話は確立できません。

手順の概要

1. **enable**
2. **showvpdndead-cache**{**group***name* | **all**}
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showvpdndead-cache**{**group***name*	**all**} 例： `Router# show vpdn dead-cache all`	デッドキャッシュ状態の一切の LNS のステータスを表示します。加えて、エントリがどれだけの時間デッドキャッシュ状態にあるかを示します。
ステップ 3	**exit** 例： `Router# exit`	特権 EXEC モードを終了します。

デッド キャッシュ状態での LNS のクリア

改訂版 LNS のデッド キャッシュ処理の機能で、**clearvpdndead-cache** コマンドを使用して、LNS の IP アドレスに基づいて LNS エントリをクリアできます。また、VPDN グループのすべての LNS デッドキャッシュ状態もクリアできるほか、LNS エントリのデッドキャッシュ全部をクリアすることもできます。LNS をその IP アドレスに基づいてクリアし、LNS が複数の VPDN グループに関連付けられていた場合は、LNS はそのすべての関連 VPDN グループでクリアされます。

この手順では、デッドキャッシュ状態の LNS をクリアする方法を示します。デッドキャッシュ状態から一旦エントリをクリアすると、エントリは新しいセッション確立や通話で使用できるようになります。

はじめる前に

この手順を LAC で実行します。

手順の概要

1. **enable**
2. **clearvpdndead-cache**{**group***name* | **ip-address***ip-address* | **all**}
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clearvpdndead-cache**{**group***name* | **ip-address***ip-address* | **all**} 例： `Router# clear vpdn dead-cache ip-address 10.10.10.1`	指定した LNS をデッドキャッシュ状態からクリアします。
ステップ 3	**exit** 例： `Router# exit`	特権 EXEC モードを終了します。

デッド キャッシュ エントリに対する SNMP イベントの生成

マネージャが多数のデバイスを管理する必要があり、各デバイスに多数のオブジェクトがある場合に、すべてのデバイスのすべてのオブジェクトに情報をポーリングまたは要求することは非現実的です。SNMP トラップ誘導通知は、イベントのトラップと呼ばれるメッセージを送信することで自動的に通知を行います。イベントの受信後、イベントを表示し、イベントに基づいて適切なアクションを選択できます。

LNS のデッドキャッシュ状態が変わったときに SNMP イベントを生成するには、次の手順に従います。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-serverenabletrapsvpdndead-cache**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-serverenabletrapsvpdndead-cache** 例： `Router(config)# snmp-server enable traps vpdn dead-cache`	LNS のデッドキャッシュ状態が変わったときの SNMP イベント生成を有効にします。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

デッド キャッシュ エントリに対する Syslog イベントの生成

デッドキャッシュ状態から LNS 追加、削除、またはクリアされた時に syslog イベントを表示するには、**vpdnloggingdead-cache** コマンドを設定します。ネットワークのトラブルシューティングのため、syslog イベントを使用できます。

次の表は、**vpdnloggingdead-cache** コマンドの使用によって生成された syslog メッセージを示します。

表 7：*VPDN* ロギング デッド キャッシュ イベント

syslog メッセージ	説明
MM:DD:hh:mm:ss %VPDN-6-VPDN_DEADCACHE_EVENT: LSG dead cache entry <ip-address> added	Added：LSG テーブルのエントリは DOWN ステータスになり、デッドキャッシュエントリとしてマークされます。
MM:DD:hh:mm:ss %VPDN-6-VPDN_DEADCACHE_EVENT: LSG dead cache entry <ip-address> deleted	Deleted：LSG テーブルのエントリは DOWN ステータスからはずれ、テーブルのデッドキャッシュエントリから削除されます。
MM:DD:hh:mm:ss %VPDN-6-VPDN_DEADCACHE_EVENT: LSG dead cache entry <ip-address> cleared	Cleared：LSG テーブルのエントリは手動でクリアされます。

LNS のデッドキャッシュ状態が変わったときに syslog イベントを生成するには、次の手順に従います。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnloggingdead-cache**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnloggingdead-cache** 例： `Router(config)# vpdn logging dead-cache`	LNS のデッドキャッシュ状態が変わったときの syslog イベント生成を有効にします。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

VPDN 用の AAA の設定例

例：VPDN トンネル認証の検索順序の設定

次の例では、VPDN を有効にし、DNIS 番号、ドメインの順になっているデフォルト検索順序の代わりに使用するトンネル認証の検索順序を設定します。

```
vpdn enable
vpdn search-order domain dnis
```

次の例では、VPDN とマルチホップを有効にし、まずマルチホップのホスト名、次にドメイン、そして DNIS 番号の順に検索するようにトンネル認可の検索順序を設定します。この設定は、トンネル スイッチでのみ使用されます。

```
vpdn enable
vpdn multihop
vpdn search-order multihop-hostname domain dnis
```

例：NAS でユーザごとの VPDN の設定

次の例では、VPDN を有効化して、すべてのダイヤルイン VPDN トンネル用に NAS のユーザごとのグローバル VPDN を設定します。最初にリモート RADIUS AAA サーバに NAS がコンタクトするときには、ドメイン名または DNIS 番号でだけではなく、すべての構造化されたユーザ名が送信されます。

```
vpdn enable
vpdn authen-before-forward
```

次の例では、VPDN を有効化し、cisco1 という名前の VPDN グループに属するダイヤルイン VPDN トンネルに対して、NAS でユーザごとの VPDN を設定します。最初にリモート RADIUS AAA サーバに NAS がコンタクトするときには、ドメイン名または DNIS 番号でだけではなく、すべての構造化されたユーザ名が送信されます。

```
vpdn enable
vpdn-group cisco1
 request-dialin
  protocol l2tp
  exit
 authen-before-forward
```

例：NAS とトンネル サーバでの AAA の設定

次の例では、NAS とトンネルサーバでの VPDN およびローカル認証と許可を有効にします。

```
vpdn enable
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
aaa authorization network default local
```

次の例では、リモート RADIUS AAA 認証が NAS で起きるときに、VPDN を有効にし、ダイヤルイン VPDN トンネル用に NAS とトンネル サーバを設定します。

NAS の設定

```
vpdn enable
!
aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius
aaa authorization network default radius
aaa accounting network default start-stop radius
radius-server host 10.1.1.1 auth-port 1939 acct-port 1443
vpdn aaa untagged
```

トンネル サーバの設定

```
vpdn enable
!
aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius
aaa authorization network default radius
aaa accounting network default start-stop radius
vpdn aaa attribute nas-ip-address vpdn-nas
vpdn aaa untagged
```

「Basic TACACS+ Configuration Example」のドキュメントでは、NAS に対するユーザ ダイヤルアップ認証用の TACACS+ の基本設定について説明しています。

例：L2TP トンネル終端装置の VPDN 用のリモート AAA の設定

次の例では、VPDN を有効にし、トンネルサーバで発生するリモート RADIUS AAA 認証により、ダイヤルイン VPDN トンネル用に NAS およびトンネル サーバを設定します。リモート RADIUS AAA サーバのサンプル RADIUS ユーザ プロファイルも表示されます。

NAS の設定

```
vpdn enable
!
aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius
aaa authorization network default radius
aaa accounting network default start-stop radius
radius-server host 10.1.1.1 auth-port 1939 acct-port 1443
vpdn aaa untagged
```

トンネル サーバの設定

```
vpdn enable
!
aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius
aaa authorization network default mymethodlist group myvpdngroup
radius-server host 10.2.2.2 auth-port 1939 acct-port 1443
aaa group server radius myvpdngroup
 server 10.2.2.2 auth-port 1939 acct-port 1443
!
vpdn tunnel authorization network mymethodlist
vpdn tunnel authorization virtual-template 1
```

RADIUS ユーザ プロファイル

```
csidtw13  Password = "cisco"
        Service-Type = Outbound,
        Tunnel-Type = :0:L2TP,
        Tunnel-Medium-Type = :0:IP,
        Tunnel-Client-Auth-ID = :0:"csidtw13",
        Tunnel-Password = :0:"cisco"
        Cisco:Cisco-Avpair = "vpdn:vpdn-vtemplate=1"
```

例：VPDN ユーザの誘導要求の認証の設定

次の例では、VPDN を有効にし、トンネル サーバ上で誘導要求のユーザの VPDN 認証によりリモート RADIUS AAA を設定します。

```
vpdn enable
!
aaa new-model
aaa authentication login default radius
aaa authentication ppp default radius
aaa authorization network default mymethodlist group myvpdngroup
radius-server host 10.3.3.3 auth-port 1939 acct-port 1443
aaa group server radius myvpdngroup
 server 10.3.3.3 auth-port 1939 acct-port 1443
!
ip host example.com 10.3.3.3
radius-server directed-request
vpdn authorize directed-request
```

次の例では、VPDN を有効にし、NAS 上でユーザごとの VPDN、リモート TACACS+ AAA、および誘導要求のユーザの VPDN の認証を設定します。

```
vpdn enable
vpdn-group 1
 request-dialin
  protocol l2tp
  domain example.com
!
 initiate-to 10.3.3.3
 local name local1
 authen-before-forward
!
aaa new-model
aaa authentication login default tacacs
aaa authentication ppp default tacacs
aaa authorization network default mymethod group mygroup
radius-server host 10.4.4.4 auth-port 1201 acct-port 1450
aaa group server tacacs mygroup
 server 10.3.3.3 auth-port 1201 acct-port 1450
```

```
!
ip host example.com 10.3.3.3
radius-server directed-request
vpdn authorize directed-request
```

例：ドメイン名のプレフィックス、サフィックス削除の設定

次の例では、ルータのユーザ名を右から左へ解析するように設定し、@、\、および $ を有効なサフィックス デリミタ文字として設定します。フルユーザ名が cisco/user@cisco.com$cisco.net であれば、ユーザ名を右から左へ解析するとき、$ の文字が NAS の検出する最初の有効なデリミタであるため、ユーザ名の */user@cisco.com* が RADIUS サーバに転送されます。

```
radius-server domain-stripping right-to-left delimiter @\$
```

次の例は、ルータが、abc と名付けられた VRF インスタンスに関連するユーザのみに対して、ユーザ名からドメイン名を削除する設定を示します。デフォルトのサフィックスデリミタである @ は一般的なサフィックスの削除に使用されます。

```
radius-server domain-stripping vrf abc
```

次の例は、/ をプレフィックスデリミタとして使用して、プレフィックスの削除を有効にします。デフォルトのサフィックスデリミタ文字の @ が一般的なサフィックスの削除に使用されます。フルユーザ名が cisco/user@cisco.com であれば、ユーザ名の *user* が TACACS+ サーバに転送されます。

```
tacacs-server domain-stripping prefix-delimiter /
```

次の例は、プレフィックスの削除を有効にし、/ の文字をプレフィックスデリミタとして設定し、# をサフィックスのデリミタとして設定します。フルユーザ名が cisco/user@cisco.com#cisco.net であれば、ユーザ名の *user@cisco.com* が RADIUS サーバに転送されます。

```
radius-server domain-stripping prefix-delimiter / delimiter #
```

次の例は、プレフィックスの削除を有効にし、/ の文字をプレフィックスデリミタとして設定し、$、@、および # をサフィックスのデリミタとして設定し、cisco.com のサフィックスのサフィックスごとの削除を設定します。フルユーザ名が cisco/user@cisco.com であれば、ユーザ名の *user* が TACACS+ サーバに転送されます。フルユーザ名が cisco/user@cisco.com#cisco.net であればユーザ名の「user@cisco.com」が転送されます。

```
tacacs-server domain-stripping prefix-delimiter / delimiter $@#
tacacs-server domain-stripping strip-suffix cisco.com
```

次の例では、ルータのユーザ名を右から左へ解析するように設定し、cisco.com のサフィックスでユーザ名のサフィックス削除を有効にします。フルユーザ名が cisco/user@cisco.net@cisco.com であれば、ユーザ名の *cisco/user@cisco.net* が RADIUS サーバに転送されます。フルユーザ名が cisco/user@cisco.com@cisco.net であれば、このフルユーザ名が転送されます。

```
radius-server domain-stripping right-to-left
radius-server domain-stripping strip-suffix cisco.com
```

次の例は、@ をデリミタとして使用して cisco.com のサフィックスを削除する一連のグローバルな削除ルールと、myvrf という名前の VRF と関連するユーザ名に対する異なった一連の削除ルールを設定します。

```
radius-server domain-stripping strip-suffix cisco.com
!
```

```
radius-server domain-stripping prefix-delimiter # vrf myvrf
radius-server domain-stripping strip-suffix cisco.net vrf myvrf
```

例：VPDN トンネル認証の設定

次の例では、NAS 上ではホスト名、トンネル サーバ上ではローカルの名前を使用して VPDN トンネル認証を設定します。各デバイスに設定されたシークレット パスワードが一致していることに注意してください。

NAS の設定

```
hostname NAS1
username tunnelserver1 password supersecret
```

トンネル サーバの設定

```
vpdn-group 1
 local name tunnelserver1
 exit
username NAS1 password supersecret
```

次の例では、NAS 上ではローカルの名前、トンネル サーバ上では L2TP トンネル パスワードを使用して、VPDN トンネル認証を設定します。各デバイスに設定されたシークレット パスワードが一致していることに注意してください。

NAS の設定

```
vpdn-group 2
 local name NAS6
!
username tunnelserver12 password verysecret
```

トンネル サーバの設定

```
vpdn-group 4
 l2tp tunnel password verysecret
 local name tunnelserver12
 exit
username NAS6 password verysecret
```

次の例では、NAS とトンネル サーバの両方で L2TP トンネル パスワードを使用して VPDN トンネル認証を設定します。各デバイスに設定されたシークレット パスワードが一致していることに注意してください。

NAS の設定

```
vpdn-group l2tp
 l2tp tunnel password rathersecret
```

トンネル サーバの設定

```
vpdn-group 46
 l2tp tunnel password rathersecret
```

例：NAS の RADIUS トンネル アカウンティングの設定

次の例では、リモート AAA 用に NAS を設定し、ダイヤルイン VPDN 配置を設定し、トンネルと tunnel-link のアカウンティング レコードの RADIUS サーバへの送信を有効にする方法を示しています。

```
aaa new-model
!
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$IDjH$iL7puCja1RMlyOM.JAeuf/
enable password secret
!
username ISP-LAC password 0 tunnelpass
!
resource-pool disable
!
ip subnet-zero
ip cef
no ip domain-lookup
ip host myhost 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
vpdn search-order domain dnis
!
vpdn-group 1
 request-dialin
 protocol l2tp
 domain cisco.com
 initiate-to ip 10.1.26.71
 local name ISP-LAC
!
isdn switch-type primary-5ess
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
controller T1 7/4
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
interface GigabitEthernet0/0/0
 ip address 10.1.27.74 255.255.255.0
 no ip mroute-cache
 duplex half
 speed auto
 no cdp enable
!
interface GigabitEthernet0/1/0
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
interface Serial7/4:23
 ip address 10.0.0.2 255.255.255.0
 encapsulation ppp
 dialer string 2000
 dialer-group 1
 isdn switch-type primary-5ess
```

```
 ppp authentication chap
!
interface Group-Async0
 no ip address
 shutdown
 group-range 1/00 3/107
!
ip default-gateway 10.1.27.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.27.254
no ip http server
ip pim bidir-enable
!
dialer-list 1 protocol ip permit
no cdp run
!
radius-server host 172.19.192.26 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
```

例：トンネルサーバの RADIUS トンネル アカウンティングの設定

次の例は、リモート AAA 用にトンネル サーバを設定し、ダイヤル イン VPDN 配置を設定し、トンネルと tunnel-link のアカウンティング レコードの RADIUS サーバへの送信を有効にする方法を示しています。

```
aaa new-model
!
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$ftf.$wE6Q5Yv6hmQiwL9pizPCg1
!
username ENT_LNS password 0 tunnelpass
username user1@cisco.com password 0 lab
username user2@cisco.com password 0 lab
!
spe 1/0 1/7
 firmware location system:/ucode/mica_port_firmware
!
spe 2/0 2/9
 firmware location system:/ucode/mica_port_firmware
!
resource-pool disable
clock timezone est 2
!
ip subnet-zero
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 10.24.80.28 10.47.0.0
ip host myhost 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
!
vpdn-group 1
accept-dialin
 protocol l2tp
 virtual-template 1
 terminate-from hostname ISP_NAS
 local name ENT_TS
!
isdn switch-type primary-5ess
!
fax interface-type modem
mta receive maximum-recipients 0
!
```

```
interface Loopback0
 ip address 10.0.0.101 255.255.255.0
!
interface Loopback1
 ip address 10.0.0.201 255.255.255.0
!
interface Ethernet0
 ip address 10.1.26.71 255.255.255.0
 no ip mroute-cache
 no cdp enable
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool vpdn-pool1
 ppp authentication chap
!
interface Virtual-Template2
 ip unnumbered Loopback1
 peer default ip address pool vpdn-pool2
 ppp authentication chap
!
interface FastEthernet0
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
speed auto
 no cdp enable
!
ip local pool vpdn-pool1 10.0.0.2 10.0.0.200
ip local pool vpdn-pool2 10.0.0.1 10.0.0.100
ip default-gateway 10.1.26.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.26.254
ip route 10.1.1.2 255.255.255.255 10.1.26.254
no ip http server
ip pim bidir-enable
!
dialer-list 1 protocol ip permit
no cdp run
!
radius-server host 172.16.192.80 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
```

例：NAS RADIUS AAA サーバのトンネル割り当て設定

次の例では、トンネルのセッションをグループ化するように RADIUS サーバを設定します。

ユーザ単位の設定

```
user@cisco.com Password = "cisco" Service-Type = Outbound,
       tunnel-type = :1:L2TP,
       tunnel-server-endpoint = :1:"10.14.10.54",
       tunnel-assignment-Id = :1:"router"
client@cisco.com Password = "cisco" Service-Type = Outbound,
       tunnel-type = :1:L2TP,
       tunnel-server-endpoint = :1:"10.14.10.54",
       tunnel-assignment-Id = :1:"router"
```

ドメインの設定

```
eng.cisco.com Password = "cisco" Service-Type = Outbound,
        tunnel-type = :1:L2TP,
        tunnel-server-endpoint = :1:"10.14.10.54",
```

```
        tunnel-assignment-Id = :1:"router"
sales.cisco.com Password = "cisco" Service-Type = Outbound,
        tunnel-type = :1:L2TP,
        tunnel-server-endpoint = :1:"10.14.10.54",
        tunnel-assignment-Id = :1:"router"
```

例：rx 速度値と tx 速度値の設定

次の例では、ポリシー マップ クラス コンフィギュレーション モードのデフォルトのクラスの値に対する平均レート トラフィック シェーピング値を設定する方法を示しています。

```
interface GigabitEthernet3/1/0.30880387
  encapsulation dot1Q 3088 second-dot1q 20
  ancp neighbor name ancp-neighbor id 0016.fa11.0488 client-ID "12.124.234.132/0.0.0.0 eth
 3/4/1.32"
  pppoe enable group test2
  service-policy output speed:ether:22000:1200:06/0
!
policy-map speed:ether:22000:1200:06/0
     class class-default
    shape average 10281000 !10,281 Mbps is so-called Rate Adaptive Mode (RAM) MIN value!
!
```

次の例では、0, 0 を含む rx 速度と tx 速度値が RADIUS サーバで設定されていない場合に、ATM インターフェイスに対する rx 速度と tx 速度値を設定する方法を示します。平均レート トラフィック シェーピング値はイーサネット インターフェイス用に設定されます。ポリシー マップ クラス コンフィギュレーション モード内でデフォルト クラス用に平均レート トラフィック シェーピング値が設定されていない場合、**l2tprx-speed** および **l2tp tx-speed** コマンド内で指定されている rx、tx 速度は、ATM インターフェイス用に設定されています。

```
Interface ATM 1/0/4.2
vpdn-template 2
l2tp rx-speed ram-min 8000
l2tp tx-speed ram-min 8000
```

次の例では、0, 0 を含む rx 速度値と tx 速度値が RADIUS サーバで設定されていない場合に、イーサネット インターフェイス用に rx 速度と tx 速度値を設定する方法を示します。ANCP 用に設定された rx、tx 速度値は、イーサネット インターフェイス用に設定されます。ANCP 用に rx、tx 速度値が設定されていない場合、**l2tp rx-speed** および **l2tp tx-speed** コマンド内で指定されている rx、tx 速度は、イーサネット インターフェイス用に設定されています。

```
Interface Ethernet 3/0/1.3
vpdn-template 1
l2tp rx-speed ancp 15000
l2tp tx-speed ancp 15000
```

例：セキュアな認証名の設定

RADIUS トンネリング属性の 90 と 91 を含む RADIUS ユーザ プロファイルの例を次に示します。このエントリは 2 つのトンネルをサポートします。1 つは L2F 用、もう 1 つは L2TP 用です。:1 が指定されたタグ エントリは L2F トンネルをサポートし、:2 が指定されたタグ エントリは L2TP トンネルをサポートします。

```
cisco.com Password = "cisco", Service-Type = Outbound
Service-Type = Outbound,
Tunnel-Type = :1:L2F,
```

```
Tunnel-Medium-Type = :1:IP,
Tunnel-Client-Endpoint = :1:"10.0.0.2",
Tunnel-Server-Endpoint = :1:"10.0.0.3",
Tunnel-Client-Auth-Id = :1:"l2f-cli-auth-id",
Tunnel-Server-Auth-Id = :1:"l2f-svr-auth-id",
Tunnel-Assignment-Id = :1:"l2f-assignment-id",
Cisco-Avpair = "vpdn:nas-password=l2f-cli-pass",
Cisco-Avpair = "vpdn:gw-password=l2f-svr-pass",
Tunnel-Preference = :1:1,
Tunnel-Type = :2:L2TP,
Tunnel-Medium-Type = :2:IP,
Tunnel-Client-Endpoint = :2:"10.0.0.2",
Tunnel-Server-Endpoint = :2:"10.0.0.3",
Tunnel-Client-Auth-Id = :2:"l2tp-cli-auth-id",
Tunnel-Server-Auth-Id = :2:"l2tp-svr-auth-id",
Tunnel-Assignment-Id = :2:"l2tp-assignment-id",
Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
Tunnel-Preference = :2:2
```

例：LNS アドレスチェックの設定

次に、クライアント ルータ用の設定例を示します。

```
hostname Client
!
enable password example
!
no aaa new-model
!
vpdn enable
!
bba-group pppoe 1
 virtual-template 1
!
interface <interface toward LAC>
 pppoe enable group 1
!
interface Virtual-Template 1
 ip unnumbered <interface>
 ppp pap sent-username@example.com
!
end
```

次に、LAC 用の設定例を示します。

```
hostname LAC
!
enable password example
!
no aaa new-model
!
vpdn enable
!
vpdn-group 1
 request-dialin
 protocol l2tp
 domain example.com
 initiate-to ip <lns 1 IP address>
 l2tp tunnel password 0 example
!
bba-group pppoe 1
 virtual-template 1
!
interface Virtual-Template 1
 no ip address
 ppp authentication pap
!
interface <interface>
```

```
 pppoe enable group 1
!
end
```

次に、LNS 1 用の設定例を示します。

```
hostname LNS1
!
enable password example
!
aaa authentication ppp default local
!
vpdn enable
!
vpdn-group 1
!Default L2TP VPDN group
 accept-dialin
 protocol l2tp
 virtual-template 1
 l2tp tunnel password 0 example
!
vpdn-group 2
 request-dialin
 protocol l2tp
 domain example.com
 initiate-to ip <lns 2 IP address>
 l2tp tunnel password 0 example
!
interface Virtual-Template 1
 ip unnumbered <interface>
 ppp authentication pap
!
end
```

例：改訂版 LNS のデッド キャッシュ処理の設定

次に、**show vpdn dead-cache all** コマンドからの設定例を示します。

```
Router> enable
Router# show vpdn dead-cache all
vpdn-group     ip address     down time
exampleA     192.168.2.2     00:10:23
exampleB     192.168.4.2     00:10:16
exampleB     192.168.4.3     00:10:15
exampleB     192.168.4.4     00:10:12
```

以下に、IP アドレスに基づいてデッドキャッシュ状態から LNS をクリアする設定例を示します。

```
Router# clear vpdn dead-cache ip-address 192.168.4.4
Router#
*Sept. 30 22:58:32 %VPDN-6-VPDN_DEADCACHE_CHANGE: LSG dead cache entry 192.168.4.4 cleared
LAC# show vpdn dead-cache all
vpdn-group     ip address     down time
exampleA     192.168.2.2     00:10:28
exampleB     192.168.4.2     00:10:21
exampleB     192.168.4.3     00:10:20
```

次に、デッドキャッシュ状態から LNS グループをクリアする設定例を示します。

```
Router# clear vpdn dead-cache group exampleB
Router#
*Sept. 30 22:58:32 %VPDN-6-VPDN_DEADCACHE_CHANGE: LSG dead cache entry 192.168.4.2 cleared
*Sept. 30 22:58:32 %VPDN-6-VPDN_DEADCACHE_CHANGE: LSG dead cache entry 192.168.4.3 cleared
Router# show vpdn dead-cache all
vpdn-group     ip address     down time
exampleA     192.168.2.2     00:10:31
```

次の作業

設定する VPDN 配置の種類により、次のモジュールうちのどれかのタスクを実行する必要があります。

- NAS によるトンネリング導入を設定するには、「NAS 側開始ダイヤルイン VPDN トンネリング設定」のモジュールへ進みます。
- マルチホップ MMP、マルチホップ トンネル スイッチングを設定するには、「マルチホップ VPDN の設定」のモジュールに進みます。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
VPDN 技術の概要	「VPDN 技術の概要」のモジュール
VPDN コマンド：完全なコマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS VPDN Command Reference*』
AAA の設定に関する情報	「認証、許可、およびアカウンティング（AAA）」のモジュール
レイヤ 2 トンネル プロトコル	『レイヤ *2* トンネル プロトコル』
RADIUS および TACACS+ の設定に関する情報	「セキュリティ サーバプロトコル」のモジュール
セキュリティ コマンド：コマンド構文の詳細、コマンドモード、デフォルト、使用上の注意事項、および例	『*Cisco IOS Security Command Reference*』
ダイヤル テクノロジー コマンド：完全なコマンド構文、コマンドモード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS Dial Technologies Command Reference*』

標準

規格	タイトル
DSL Forum 2004-72	--

MIB

MIB	MIB のリンク
• CISCO-VPDN-MGMT-MIB • CISCO-VPDN-MGMT-EXT-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2516	『*A Method for Transmitting PPP Over Ethernet (PPPoE)*』
RFC 2867	『*RADIUS Accounting Modifications for Tunnel Protocol Support*』
RFC 2868	『*RADIUS Tunnel Authentication Attributes*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VPDN 用の AAA の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *8*：*VPDN* 用の *AAA* の機能情報

機能名	リリース	機能情報
RADIUS サーバ向けドメイン名のプレフィックス、サフィックス削除の設定	Cisco IOS XE リリース 2.1	この機能により、フル ユーザ名からプレフィックス、サフィックスまたは両方を削除するよう NAS を設定できます。この処理後、再フォーマットされたユーザ名をリモート AAA サーバに転送します。 この機能によって、次のコマンドが導入または変更されました。 **radius-serverdomain-stripping**。
RADIUS 属性 82：トンネル割り当て ID	Cisco IOS XE リリース 2.1	この機能により、トンネル エンドポイント、トンネル タイプおよびトンネル割り当て ID が同じ場合に、L2TP NAS はユーザ単位またはドメイン単位の異なる RADIUS プロファイルからのユーザを同じアクティブ トンネルにグループ分けできるようにします。 この機能によって導入または変更されたコマンドはありません。

機能名	リリース	機能情報
RADIUS トンネル属性拡張	Cisco IOS XE リリース 2.1	この機能は RADIUS 属性 90 と RADIUS 属性 91 を導入します。この両方の属性は、ユーザに NAS と RADIUS サーバの認証名の指定を許可することによって、VPDN での Compulsory Tunneling のプロビジョニングをサポートします。 この機能によって導入または変更されたコマンドはありません。
RFC-2867 RADIUS トンネル アカウンティング	Cisco IOS XE リリース 2.1	この機能は、6 つの新しい RADIUS アカウンティング タイプを導入しています。これらのタイプは、アカウンティング要求がユーザ サービスの始まり（開始）と終わり（終了）のどちらを表しているかを示す、RADIUS アカウンティング属性の Acct-Status-Type（属性 40）と一緒に使用されます。 この機能により、次のコマンドが導入または変更されました。**aaaaccounting**、**vpdnsessionaccountingnetwork**、**vpdntunnelaccountingnetwork**。

機能名	リリース	機能情報
トンネル ターミネータでの RADIUS経由でのトンネル認証	Cisco IOS XE リリース 2.1	この機能により、L2TP トンネルサーバで、着信L2TPNAS ダイヤルイン接続要求での RADIUS を使用したリモート認証および許可を実行できます。また、この機能により、L2TP NAS で、着信 L2TP トンネル サーバ ダイヤルアウト接続要求での RADIUS を使用したリモート認証および認可を実行できます。 この機能により、次のコマンドが導入されました。**vpdntunnelauthorizationnetwork**、**vpdntunnelauthorizationpassword**、**vpdntunnelauthorizationvirtual-template**。
PPPoE タギング情報の L2TP 転送	Cisco IOS XE リリース 2.4	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。
LNS アドレス チェック	Cisco IOS XE リリース 2.4	この機能は、LNSからデータを受信している LAC が L2TP トンネル確立前に LNS の IP アドレスを確認することを可能とします。 この機能により、次のコマンドが導入されました。**l2tpsecurityipaddress-check**。
改訂版 LNS のデッド キャッシュ処理	Cisco IOS XE リリース 2.4	この機能は、デッドキャッシュ（DOWN）状態のすべてのLNS エントリを表示し、クリア（再起動）します。 この機能により、次のコマンドが導入されました。**clearvpdndead-cache**、**showvpdndead-cache**。 この機能により、次のコマンドが変更されました。**snmp-serverenabletraps**、**vpdnlogging**。

機能名	リリース	機能情報
TACACS+ サーバ向けドメイン名のプレフィックス、サフィックスの削除の設定	Cisco IOS XE リリース 2.5	この機能により、フル ユーザ名からプレフィックス、サフィックスまたは両方を削除するよう NAS を設定できます。この処理後、再フォーマットされたユーザ名をリモート AAA サーバに転送します。 この機能によって、次のコマンドが導入または変更されました。 **tacacs-serverdomain-stripping**。
LNS での ANCP 値設定サポート	Cisco IOS XE リリース 3.2S	この機能により、L2TP は VPDN グループ設定または VPDN テンプレート コンフィギュレーション モードで設定されている rx 速度値、tx 速度値や RADIUS サーバ上で設定されている rx 速度値、tx 速度値を LNS へ送信できます。 この機能によって、次のコマンドが導入されました。 **l2tprx-speed**、**l2tptx-speed**。

第 4 章

NAS 側開始ダイヤルイン VPDN トンネリングの設定

ネットワーク アクセス サーバ（NAS）側開始ダイヤルイン トンネリングでは、特別な知識やクライアントから必要な対話型操作なしで、NASからトンネルサーバへのPPPセッションのセキュアなトンネリングが提供されます。

- 機能情報の確認，105 ページ
- NAS 側開始ダイヤルイン VPDN トンネリング設定の前提条件，106 ページ
- NAS 側開始ダイヤル イン VPDN トンネリング設定の制約事項，106 ページ
- NAS 側開始ダイヤルイン VPDN トンネリングに関する情報，106 ページ
- NAS 側開始ダイヤルイン VPDN トンネリングの設定方法，108 ページ
- NAS によるダイヤルイン VPDN トンネリングの設定例，124 ページ
- 次の作業，128 ページ
- その他の参考資料，128 ページ
- NAS 側開始ダイヤルイン VPDN トンネリング設定の機能情報，130 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

NAS 側開始ダイヤルイン VPDN トンネリング設定の前提条件

- このモジュールで説明されているタスクを実行する前に、「VPDN 用の AAA 設定」のモジュール内の必要なタスクを実行する必要があります。
- NAS は、ISDN、公衆電話交換網（PSTN）、デジタル加入者線（DSL）またはケーブル モデムを使用するクライアントからの着信コールを受信するように設定する必要があります。

NAS 側開始ダイヤル イン VPDN トンネリング設定の制約事項

- Layer 2 Forwarding（L2F）プロトコルは、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータではサポートされません。

NAS 側開始ダイヤルイン VPDN トンネリングに関する情報

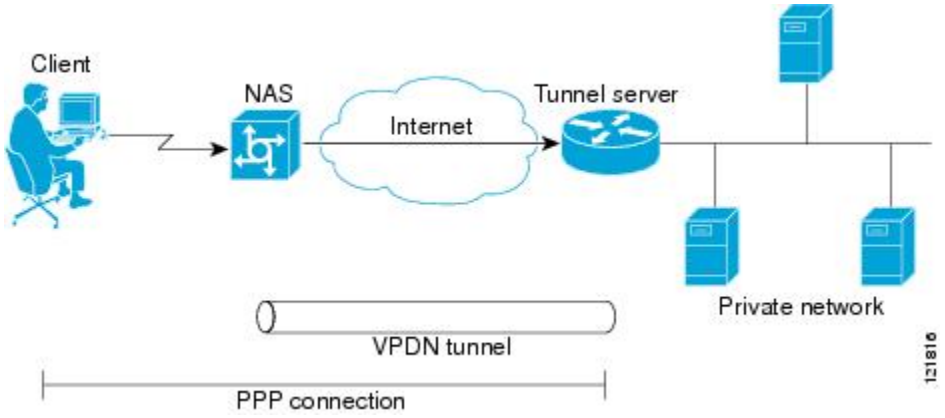
NAS 側開始ダイヤルイン VPDN トンネリング

NAS 側開始ダイヤルイン VPDN トンネリングは Compulsory Tunneling とも呼ばれます。NAS 側開始ダイヤルイン VPDN トンネリングでは、PPP をサポートするメディアを介してクライアントが NAS へダイヤルインします。DSL、ISDN や PSTN などのセキュアと見なされるメディアを介してクライアントからインターネット サービス プロバイダー（ISP）の NAS へ接続する場合、クライアントは追加のセキュリティを提供しないよう選択することがあります。PPP セッションは、クライアントからの専門知識や操作を必要とせずに、NAS からトンネル サーバにセキュアにトンネリングされます。NAS 側開始ダイヤルイン VPDN トンネルはレイヤ 2 トンネリング プロトコル（L2TP）またはレイヤ 2 フォワーディング（L2F）プロトコルのどちらかを使用します。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、L2TP のみをサポートします。

NAS 側開始ダイヤルイントンネリングのシナリオを次の図に示します。

図 *8*：*NAS* 側開始ダイヤルイン *VPDN* のシナリオ



L2TP 発信側ステーション ID の抑制

NAS 側開始ダイヤルイン L2TP トンネリングのシナリオでは、NAS は、トンネル サーバに接続する際に、セッションセットアップ プロセスの一部として、非常に多数の属性と値（Attribute-Value: AV）のペアを送信します。これらの AV ペアの 1 つに、L2TP AV ペア 22 の発信者番号 ID があります。発信番号 ID の AV ペアには、セッションの発信元の発信側ステーション ID が含まれます。この ID は、発信元の電話番号、LAC での接続の確立に使用される論理回線 ID（LLID）、またはネットワークに接続している PC の MAC アドレスのいずれかです。この情報は、NAS とトンネル サーバが異なる事業主体で管理されている場合、機密とみなされる可能性があります。NAS またはエンド ユーザのセキュリティ要件によっては、発信側ステーション ID の一部またはすべてを抑制する（隠す）ことが望ましい場合があります。

発信側ステーション ID の一部はマスクでき、また発信側ステーション ID は完全に除去できます。発信側ステーション ID の抑制は、NAS 上でグローバルに設定することができ、またこの抑制が設定されている場合、NAS またはリモート RADIUS サーバ上で個々の VPDN グループに設定することもできます。

L2TP のフェールオーバー

NAS が L2TP トンネルの確立時にピアへの接続に失敗すると、別の構成済みトンネル サーバへフェールオーバーし、そのデバイスとのトンネルの確立を試行することもできます。

フェールオーバーは、次のようなシナリオで発生する可能性があります。

- ルータが Start Control Connection Request（SCCRQ）を何度も送信し、ピアからの応答がない場合。
- ルータがピアから Stop Control Connection Notification（StopCCN）を受信した場合。
- ルータがピアから Call Disconnect Notify（CDN）メッセージを受信した場合。

StopCNN 制御メッセージと CDN 制御メッセージには両方とも、結果コードの AV ペアが含まれており、それぞれトンネルやセッション終了の理由を示します。この AV ペアには、トンネルやセッション終了の性質を詳しく説明するエラーコードも含まれる場合があります。さまざまな結果コードとエラーコード値が RFC 2661 で標準規格化されています。フェールオーバーは、下の表で定義される結果コードとエラーコード値の組み合わせをピアから受信すると発生します。

表 *9*：*RFC 2661* からの定義済み結果コードとエラーコード

制御メッセージ	結果コード	エラー コード
StopCCN、CDN	2：一般的なエラー、エラーコードを確認してください。	4：この操作を実行するリソースが現在不足しています。 6：一般的なベンダー固有のエラーが発生しました。[1] 7：別の方法を試してください。 9：別の誘導方法を試してください。
CDN	4：リソースが一時的に不足しています。	--

[1] フェールオーバーに関しては、このエラーコードにはエラーメッセージ内のベンダー固有のエラー AVP が伴います。この場合は、シスコ ベンダー コード（SMI_CISCO_ENTERPRISE_CODE）と、シスコ エラー コード（L2TP_VENDOR_ERROR_SLIMIT）が含まれます。

3 つのシナリオのいずれかが発生すると、ルータはデフォルトで 60 秒間ビジー状態としてピアの IP アドレスをマークします。その間は、ピアとトンネルまたはセッションの確立は試行されません。ルータは、設定を行えば代替ピアを選んで接続をするようになります。トンネルが代替ピアにすでに存在している場合、その既存のトンネル内で新しいセッションが始まります。そうでない場合、ルータは代替ピアへのトンネルを確立するためのネゴシエーションを開始します。

NAS 側開始ダイヤルイン VPDN トンネリングの設定方法

ダイヤル イン VPDN トンネル要求のための NAS の設定

NAS がリモート トンネルのサーバにトンネルの確立を要求するには設定が必要です。VPDN リクエスト ダイヤルイン サブグループと VPDN トンネルの他方のエンドポイントとなるトンネルサーバの IP アドレスを設定するには NAS で次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **description***string*
5. **request-dialin**
6. **protocoll2tp**
7. 次のいずれかを実行します。
   - **domain***domain-name*
   - **dnis** {*dnis-number* | *dnis-group-name*}
8. **exit**
9. **initiate-toip***ip-address*[**limit***limit-number*] [**priority***priority-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**description***string* 例： `Router(config-vpdn)# description myvpdngroup`	（オプション）VPDN グループに説明を追記します。

	コマンドまたはアクション	目的
ステップ 5	**request-dialin** 例： `Router(config-vpdn)# request-dialin`	NAS がトンネル サーバへ L2F または L2TP トンネルの確立を要求するように設定し、request-dialin VPDN サブグループを作成し、VPDN request-dialin サブグループ設定モードに入ります。
ステップ 6	**protocoll2tp** 例： `Router(config-vpdn-req-in)# protocol l2tp`	VPDN グループが使用するレイヤ 2 プロトコルを指定します。

ステップ 7	次のいずれかを実行します。
	• **domain***domain-name*
	• **dnis** {*dnis-number* | *dnis-group-name*}
	
	例：
	
	`Router(config-vpdn-req-in)# domain example.com`
	
	例：
	
	`Router(config-vpdn-req-in)# dnis 5687`
		特定のドメイン名からの PPP コールをトンネルするよう要求します。
		または
		特定の着信番号識別サービス（DNIS）番号または DNIS グループからの PPP コールをトンネルするよう要求します。

ステップ 8	**exit** 例： `Router(config-vpdn-req-in)# exit`	VPDN グループ コンフィギュレーション モードを終了します。
ステップ 9	**initiate-toip***ip-address*[**limit***limit-number*] [**priority***priority-number*] 例： `Router(config-vpdn)# initiate-to ip 10.1.1.1 limit 12`	レイヤ 2 トンネリングで使用する IP アドレスを指定します。 • **limit**：この IP アドレスに対して可能な最大の接続数。 • **priority**：この IP アドレスの優先度。 （注） **priority** キーワードは、通常 NAS には設定しません。代わりに、ロードバランシングとフェールオーバーに使用する情報はリモートの AAA サーバに設定されます。「VPDN 用の AAA の設定」モジュールを参照してください。 • initiate-to コマンドを複数設定して、複数トンネルのサーバを NAS に設定できます。

	コマンドまたはアクション	目的

次の作業

「ダイヤル イン VPDN トンネル受け入れのためのトンネル サーバの設定」のセクションのタスクを実行する必要があります。

ダイヤル イン VPDN トンネル受け入れのためのトンネル サーバの設定

リモートNASサーバからのトンネル要求を受け入れるには、トンネルサーバを設定する必要があります。VPDN accept dial-in サブグループを作成し、トンネル サーバが他方のエンドポイントとなる NAS サーバからのトンネル要求を受け入れるように設定するには、トンネル サーバで次の作業を実行します。複数の NAS からのトンネルを受け入れるようにトンネル サーバを設定するには、各 NAS に対してこのタスクを実行する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **description***string*
5. **accept-dialin**
6. **protocoll2tp**
7. **virtual-template***number*
8. **exit**
9. **terminate-fromhostname***host-name*
10. **lcprenegotiation** {**always** | **on-mismatch**}
11. **force-local-chap**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**description***string* 例： `Router(config-vpdn)# description myvpdngroup`	（オプション）VPDN グループに説明を追記します。
ステップ 5	**accept-dialin** 例： `Router(config-vpdn)# accept-dialin`	トンネル サーバが NAS からの L2F、L2TP トンネルの確立、accept-dialin VPDN サブグループの作成の要求を受け入れるよう設定し、ダイヤルインサブグループ設定モードに入ります。
ステップ 6	**protocoll2tp** 例： `Router(config-vpdn-acc-in)# protocol l2tp`	VPDN グループが使用するレイヤ 2 プロトコルを指定します。
ステップ 7	**virtual-template***number* 例： `Router(config-vpdn-acc-in)# virtual-template 1`	仮想アクセス インターフェイスのクローンを作成する際に使用される仮想テンプレートを指定します。
ステップ 8	**exit** 例： `Router(config-vpdn-acc-in)# exit`	VPDN グループ コンフィギュレーション モードを終了します。
ステップ 9	**terminate-fromhostname***host-name* 例： `Router(config-vpdn)# terminate-from hostname NAS12`	VPDN トンネルの受け入れ時に必要なリモート NAS のホスト名を指定します。

	コマンドまたはアクション	目的
ステップ 10	**lcprenegotiation** {**always** | **on-mismatch**} 例： `Router(config-vpdn)# lcp renegotiation always`	（オプション）L2TP または L2F を使ったダイヤルイン通話でトンネル サーバが PPP Link Control Protocol（LCP）を再ネゴシエートするようにします。 • このコマンドは、想定外の LCP オプションのセットを NAS がネゴシエートすることが考えられる、Cisco 以外の NAS へのトンネル接続を行うトンネル サーバで役立ちます。
ステップ 11	**force-local-chap** 例： `Router(config-vpdn)# force-local-chap`	（オプション）トンネル サーバにクライアントの再認証を強制します。 • このコマンドを有効にすると、NAS サーバによるプロキシ認証に加えて、トンネル サーバがクライアントを強制的に再認証します。 （注） このコマンドは、トンネルサーバに設定してある仮想テンプレートで **ppp authentication chap** コマンドを使用して、チャレンジハンドシェイク認証プロトコル（CHAP）認証が PPP で有効となっている場合のみ機能します。

次の作業

「トンネル サーバの仮想テンプレートの設定」のセクションのタスクを実行する必要があります。

トンネル サーバの仮想テンプレートの設定

トンネルの確立の要求がトンネル サーバで受信された際、トンネル サーバは仮想アクセス インターフェイスを作成する必要があります。仮想アクセスインターフェイスは仮想テンプレートインターフェイスから複製され、使用されて、不要となったときに解放されます。仮想テンプレート インターフェイスは、物理インターフェイスに一切結びつきのない論理エンティティです。

基本的な仮想テンプレートを設定するには、トンネル サーバで次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacevirtual-template***number*
4. **ipunnumbered***typenumber*
5. **pppauthentication***protocol1*[*protocol2...*][**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**]
6. **peerdefaultipaddress** {*ip-address*| **dhcp-pool** | **dhcp** | **pool** [*pool-name*]}
7. **encapsulation***encapsulation-type*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfacevirtual-template***number* 例： `Router(config)# interface virtual-template 1`	インターフェイス コンフィギュレーション モードを開始し、仮想アクセス インターフェイスの作成時に動的に設定および適用できる仮想テンプレート インターフェイスを作成します。
ステップ 4	**ipunnumbered***typenumber* 例： `Router(config-if)# ip unnumbered FastEthernet 0/0`	明示的な IP アドレスをインターフェイスに割り当てずにシリアル インターフェイス上で IP 処理を有効にします。 （注） 仮想テンプレート内に **ipaddress** コマンドを設定することは推奨されません。仮想テンプレート内に特定の IP アドレスを設定することで、誤ったルートの確立や IP パケットの損失が発生する可能性があります。
ステップ 5	**pppauthentication***protocol1*[*protocol2...*][**if-needed**] [*list-name*	**default**] [**callin**] [**one-time**] [**optional**] 例： `Router(config-if)# ppp authentication chap`	少なくとも 1 つの PPP 認証プロトコルをイネーブルにして、インターフェイスでプロトコルが選択される順序を指定します。

	コマンドまたはアクション	目的
ステップ 6	**peerdefaultipaddress** {*ip-address*| **dhcp-pool** | **dhcp** | **pool** [*pool-name*]} 例： `Router(config-if)# peer default ip address pool mypool`	このインターフェイスに接続しているリモート ピアに返される、IP アドレス、特定の IP アドレス プールからのアドレス、または Dynamic Host Configuration Protocol（DHCP）メカニズムからのアドレスを指定します。
ステップ 7	**encapsulation***encapsulation-type* 例： `Router(config-if)# encapsulation ppp`	インターフェイスで使用するカプセル化方式を設定します。

NAS による VPDN 設定の確認

NAS とトンネル サーバ間のトンネル確立の確認とトラブルシューティング

このタスクは、NAS とトンネルサーバ間のトンネルが確立済みであることを確認し、またトンネルの確立に関する問題をトラブルシューティングする場合に実行します。

手順の概要

1. **enable**
2. **showvpdntunnelall**
3. **ping***ip-address*
4. **debugvpdnevent**
5. **debugvpdnerrors**

手順の詳細

ステップ 1 **enable**
このコマンドを使用して、特権 EXEC モードを有効にします。プロンプトにパスワードを入力します。

例：

```
Router> enable
```

ステップ 2 **showvpdntunnelall**
このコマンドを入力して、すべてのアクティブな VPDN トンネルに関する詳細を表示します。次の例では、*No active L2TP tunnels* の例が示されています。

例：

```
Router# show vpdn tunnel all
% No active L2TP tunnels
.
.
.
```

NAS でアクティブなトンネルが確立されていない場合、次の手順に進んでこの問題をトラブルシューティングします。

ステップ 3 **ping***ip-address*

このコマンドを入力して、NAS に対して ping を実行します。次の出力では、トンネル サーバから NAS への ping の正常な結果が示されています。

例：

```
Router# ping 172.22.66.25
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 128/132/152 ms
```

トンネル サーバが NAS に対して ping を実行できない場合、デバイス間のルーティング パスに問題があるか、NAS が機能していない可能性があります。

ステップ 4 **debugvpdnevent**

このコマンドを入力して、トンネル確立時に発生する VPDN イベントを表示します。次のトンネル サーバからの出力では、L2TP トンネルの通常の VPDN トンネルの確立が示されています。

例：

```
Router# debug vpdn event
20:19:17: L2TP: I SCCRQ from ts1 tnl 8
20:19:17: L2X: Never heard of ts1
20:19:17: Tnl 7 L2TP: New tunnel created for remote ts1, address 172.21.9.4
20:19:17: Tnl 7 L2TP: Got a challenge in SCCRQ, ts1
20:19:17: Tnl 7 L2TP: Tunnel state change from idle to wait-ctl-reply
20:19:17: Tnl 7 L2TP: Got a Challenge Response in SCCCN from ts1
20:19:17: Tnl 7 L2TP: Tunnel Authentication success
20:19:17: Tnl 7 L2TP: Tunnel state change from wait-ctl-reply to established
20:19:17: Tnl 7 L2TP: SM State established
20:19:17: Tnl/Cl 7/1 L2TP: Session FS enabled
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from idle to wait-for-tunnel
20:19:17: Tnl/Cl 7/1 L2TP: New session created
20:19:17: Tnl/Cl 7/1 L2TP: O ICRP to ts1 8/1
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from wait-for-tunnel to wait-connect
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from wait-connect to established
20:19:17: Vi1 VPDN: Virtual interface created for user1@cisco.com
20:19:17: Vi1 VPDN: Set to Async interface
20:19:17: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
20:19:18: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
20:19:18: Vi1 VPDN: Bind interface direction=2
20:19:18: Vi1 VPDN: PPP LCP accepting rcv CONFACK
20:19:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
```

ステップ 5 **debugvpdnerrors**

このコマンドを入力して、トンネル確立時に生成されるエラー メッセージを表示します。次の NAS からの出力では、トンネル確立時の認証の失敗が示されています。

例：

```
Router# debug vpdn errors
%LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state to down
%LINK-5-CHANGED: Interface Async1, changed state to reset
%LINK-3-UPDOWN: Interface Async1, changed state to down
%LINK-3-UPDOWN: Interface Async1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state to up
VPDN tunnel management packet failed to authenticate
VPDN tunnel management packet failed to authenticate
```

認証の失敗が発生した場合、NAS とトンネル サーバの両方が同じシークレット パスワードで設定されていることを確認します。また、「VPDN に対する AAA の設定」モジュールの説明に従って、L2TP トンネルの確立、リモート クライアントとの PPP ネゴシエーションおよび認証を確認するタスクを実行することもできます。

クライアントと NAS 間の接続の確認

ダイヤル イン クライアントと NAS の間の接続を確認するには、次の作業を実行します。

手順の概要

1. クライアント PC から NAS にダイヤル インします。
2. **enable**
3. **showcalleruser***user*
4. **showinterfacesvirtual-access***number*
5. **showvpdnsession**

手順の詳細

ステップ 1 クライアント PC から NAS にダイヤル インします。
ダイヤル イン接続を確立し、クライアント PC が NAS に接続できることを確認します。NAS に着信すると、NAS の端末画面に LINK-3-UPDOWN メッセージが自動的に表示されます。次の例では、NAS の非同期インターフェイス 14 に着信しています。

例：

```
*Jan  1 21:22:18.410: %LINK-3-UPDOWN: Interface Async14, changed state to up
```

（注） このログメッセージを表示するにあたり、**debug** コマンドは実行されません。このメッセージは、クライアントが最初に架電してから 30 秒以内に表示されます。

NAS でこのメッセージが表示されない場合は、ダイヤルイン設定に問題があります。

ステップ 2 **enable**
このコマンドを使用して、特権 EXEC モードを有効にします。プロンプトにパスワードを入力します。

例：

```
Router> enable
```

ステップ 3 **showcalleruser***user*

クライアントが IP アドレスを受信したことを確認するには、トンネル サーバでこのコマンドを入力します。次の例は、user3 が IP アドレス 10.0.0.1 を使用していることを示しています。

例：

```
Router# show caller user user3@cisco.com
User: user3@cisco.com, line Vi2.502, service PPPoVPDN
Connected for 1d10h
Timeouts: Limit Remaining Timer Type
- - -
PPP: LCP Open, CHAP (<-), IPCP
IP: Local 10.0.0.1, remote 172.16.2.247
Counts: 2052 packets input, 32826 bytes
        2053 packets output, 106742 bytes
```

正しくない IP アドレスが表示される場合や IP アドレスが表示されない場合、IP アドレス割り当ての問題があります。トンネル サーバの仮想テンプレートで **peerdefaultipaddress** コマンドの設定を確認します。

ステップ 4 **showinterfacesvirtual-access***number*

このコマンドを入力して、インターフェイスがアップの状態で、LCP が開いており、エラーが報告されていないことを確認します。次の出力は、インターフェイスが機能していることを示しています。

例：

```
Router# show interfaces virtual-access 2.502
Virtual-Access2.502 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback1001 (60.0.0.1)
  MTU 1454 bytes, BW 2000000 Kbit, DLY 100000 usec,
     reliability 255/255, txload 1/255, rxload 5/255
  Encapsulation PPP, LCP Open
  Open: IPCP
  PPPoVPDN vaccess, cloned from Virtual-Template1
  Vaccess status 0x0
  Protocol l2tp, tunnel id 30485, session id 55909
  Keepalive set (60 sec)
     2056 packets input, 32890 bytes
     2057 packets output, 106950 bytes
  Last clearing of ''show interface'' counters never
```

仮想アクセス インターフェイスは起動しており、回線プロトコルもアップになっており、仮想インターフェイスが正しく確立していることが示されます。

ステップ 5 **showvpdnsession**

アクティブな VPDN セッションがあることを確認するには、トンネル サーバで次のコマンドを入力します。この例では、複数のアクティブなトンネルを持つトンネル サーバの出力を示します。

例：

```
Router# show vpdn session
L2TP Session Information Total tunnels 4000 sessions 15960
LocID      RemID      TunID      Username, Intf/      State  Last Chg Uniq ID
```

```
                                    Vcid, Circuit
43202       40336       22          user@ci..., Vi2.9171 est    1d10h 9184
34090       31996       22          user@ci..., Vi2.1734 est    1d10h 1735
1217        42591       22          user@ci..., Vi2.9312 est    1d10h 9325
6737        22325       22          user@ci..., Vi2.1729 est    1d10h 1730
59420       17035       34          user@ci..., Vi2.9338 est    1d10h 9351
45069       60982       34          user@ci..., Vi2.1645 est    1d10h 1646
27825       44751       34          user@ci..., Vi2.1653 est    1d10h 1654
24600       7627        34          user@ci..., Vi2.9096 est    1d10h 9109
13018       65037       43          user@ci..., Vi2.8166 est    1d10h 8179
43090       34448       43          user@ci..., Vi2.8176 est    1d10h 8189
31798       41505       43          user@c..., Vi2.15752 est    1d10h 15765
56832       64322       43          user@c..., Vi2.15655 est    1d10h 15668
53944       25409       48          user@c..., Vi2.14115 est    1d10h 14128
16215       52915       48          user@c..., Vi2.14134 est    1d10h 14147
17332       14000       48          user@ci..., Vi2.6630 est    1d10h 6643
12466       54817       48          user@ci..., Vi2.6622 est    1d10h 6635
28290       37822       50          user@ci..., Vi2.5094 est    1d10h 15905
44839       30137       50          user@c..., Vi2.15875 est    1d10h 15888
```

クライアントに向けて確立されたセッションがない場合は、「NAS とトンネル サーバ間のトンネル確立の確認とトラブルシューティング, （115 ページ）」のトラブルシューティング手順を実行します。

L2TP 発信側ステーション ID の抑制の設定

発信側ステーション ID の抑制は、NAS 上でグローバルに設定することができ、またこの抑制が設定されている場合、NAS またはリモート RADIUS サーバ上で個々の VPDN グループに設定することもできます。

L2TP の発信側ステーション ID の抑制設定の優先順位は、次のとおりです。

- RADIUS サーバ上の設定が NAS 上のどの設定よりも優先されます。
- VPDN グループの設定が、この VPDN グループに関連付けられているコールに対するグローバル設定よりも優先されます。
- グローバル設定は、他の方法が設定されていない場合に適用されます。

次のタスクを 1 つ以上実行して、L2TP の発信側ステーション ID の抑制を設定します。

L2TP 発信側ステーション ID の抑制を設定するための前提条件

- 「ダイヤル イン VPDN トンネル要求のための NAS の設定」のセクションおよび、「ダイヤルイン VPDN トンネル受け入れのためのトンネルサーバの設定」セクション内でのタスクを実行するとき、NAS およびトンネル サーバを設定して L2TP プロトコルを使用する必要があります。
- 「ダイヤル イン VPDN トンネル要求のための NAS の設定」のセクションでのタスクを実行するときには、NAS を設定して、ドメイン名に基いたコールをトンネリングする必要があります。

- 「VPDN 用の AAA の設定」モジュールの「VPDN トンネル認証の検索順序」セクションでのタスクを実行するときには、ドメイン名を使用するためにVPDN検索順序を設定する必要があります。

NAS でのグローバル L2TP 発信側ステーション ID の抑制の設定

L2TP 発信側ステーション ID の抑制をグローバルに設定した場合は、L2TP AV ペア 22 に含まれる発信側ステーション ID 情報は、ルータに確立されている L2TP セッションごとに削除またはマスキングできます。この設定は、ローカル、リモート認証のいずれとも互換性があります。

グローバルな L2TP 発信側ステーション ID の抑制を設定するには、NAS でこの作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnl2tpattributeclidmask-method** {**right** *mask-character characters* | **remove**} [**match** *match-string*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnl2tpattributeclidmask-method** {**right** *mask-character characters*	**remove**} [**match** *match-string*] 例： `Router(config)# vpdn l2tp attribute clid mask-method right # 6 match %321`	NAS がルータで L2TP 発信側ステーション ID をグローバルに抑制するよう、NAS 自体を設定します。 • **right***mask-charactercharacters*：指定した *mask-character* を使用して発信側ステーション ID を右端からマスクし、*characters* で定義済みの数の文字を置き換えます。*mask-character*（マスク文字）は印刷可能な文字でなければなりません。 • **remove**：発信側ステーション ID のすべてを削除します。 • **match***match-string*：ユーザ名が指定した *match-string*（照合文字列）を含む場合のみ、発信側ステーション ID を削除またはマスクします。

	コマンドまたはアクション	目的

NAS での VPDN グループに対する L2TP 発信側ステーション ID の抑制の設定

特定の VPDN グループに関連した発信について、L2TP AV ペア 22 に含まれる発信側ステーション ID の情報を除去またはマスクできます。この設定はローカル認証の設定と互換性があります。

ローカル認証を使用して、特定の VPDN グループに関連した発信について L2TP 発信側ステーション ID 抑制を設定するには、NAS で次の作業を実行します。

はじめる前に

- 「VPDN 用の AAA の設定」モジュールの「NAS とトンネルサーバでの AAA の設定」セクションで示したタスクの最中では、NAS とトンネルサーバをローカル認証向けに設定する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **l2tpattributeclidmask-method** {**right***mask-charactercharacters*| **remove**} [**match***match-string*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group L2TP`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**l2tpattributeclidmask-method**{**right***mask-charactercharacters*|**remove**} [**match***match-string*] 例： `Router (config-vpdn)# l2tp attribute clid mask-method remove`	NAS が VPDN グループまたは VPDN テンプレートに関連したセッションで L2TP 発信側ステーション ID を抑制するよう、NAS を設定します。 • **right***mask-charactercharacters*：指定した *mask-character* を使用して発信側ステーション ID を右端からマスクし、*characters* で定義済みの数の文字を置き換えます。*mask-character*（マスク文字）は印刷可能な文字でなければなりません。 • **remove**：発信側ステーション ID のすべてを削除します。 • **match***match-string*：ユーザ名が指定した *match-string*（照合文字列）を含む場合のみ、発信側ステーション ID を削除またはマスクします。

NAS リモート RADIUS サーバでの L2TP 発信側ステーション ID 抑制の設定

L2TP 発信側ステーション ID 抑制は直接 NAS に設定するか、または RADIUS のユーザプロファイルに設定できます。L2TP 発信側ステーション ID 抑制を RADIUS のユーザプロファイルに設定すると、複数の NAS に設定を伝達することができ、それぞれ個別に設定する必要がありません。

RADIUS サーバが各 NAS に L2TP 発信側ステーション ID を除去し、またはマスクするよう命令する設定を行うには、次の作業を実行します。

はじめる前に

- NAS はリモート RADIUS AAA 向けに設定されている必要があります。「VPDN 用の AAA の設定」モジュールの説明に従って、NAS とトンネルサーバで AAA を設定するタスクと、VPDN 向けのリモート AAA を設定するタスクを実行します。
- RADIUS サーバは AAA 向けに設定されている必要があります。

手順の概要

1. **Cisco-Avpair=vpdn:l2tp-tunnel-password=***secret*
2. **Cisco-Avpair=vpdn:tunnel-type=l2tp**
3. **Cisco-Avpair=vpdn:tunnel-id=***name*
4. **Cisco-Avpair=vpdn:ip-address=***address*
5. **Cisco-Avpair=vpdn:l2tp-clid-mask-method=**{**right:***character***:***characters* | **remove**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**Cisco-Avpair=vpdn:l2tp-tunnel-password=***secret* 例： `Cisco-Avpair = vpdn:l2tp-tunnel-password=cisco`	RADIUS ユーザ プロファイルで L2TP トンネル パスワードを指定します。
ステップ 2	**Cisco-Avpair=vpdn:tunnel-type=l2tp** 例： `Cisco-Avpair = vpdn:tunnel-type=l2tp`	RADIUS ユーザ プロファイルでトンネリング プロトコルとして L2TP を指定します。
ステップ 3	**Cisco-Avpair=vpdn:tunnel-id=***name* 例： `Cisco-Avpair = vpdn:tunnel-id=test`	RADIUS ユーザ プロファイルでトンネル ID を指定します。
ステップ 4	**Cisco-Avpair=vpdn:ip-address=***address* 例： `Cisco-Avpair = vpdn:ip-address=172.16.9.9`	RADIUS ユーザ プロファイルで NAS IP アドレスを指定します。
ステップ 5	**Cisco-Avpair=vpdn:l2tp-clid-mask-method=**{**right:***character***:***characters*	**remove**} 例： `Cisco-Avpair = vpdn:l2tp-clid-mask-method= right:#:5`	RADIUS ユーザ プロファイルで L2TP 発信側ステーション ID 抑制パラメータを指定します。 • **right**：指定した *mask-character* を使用し、発信側ステーション ID を右からマスクして *characters* で定義済みの数の文字を置き換えます。 • **remove**：発信側ステーション ID のすべてを削除します。

NAS によるダイヤルイン VPDN トンネリングの設定例

例：ダイヤル イン VPDN への NAS の設定

次の例は、ISP-NAS という名前の NAS を L2TP とローカル認証および許可を使用して ENT-TS という名前のトンネル サーバに PPP コールをトンネリングする設定を示します。

```
! Enable AAA authentication and authorization with RADIUS as the default method
aaa new-model
aaa authentication ppp default radius
aaa authorization network default radius
!
! Configure the VPDN tunnel authentication password using the local name
username ISP-NAS password 7 tunnelme
username ENT-TS password 7 tunnelme
!
vpdn enable
!
! Configure VPN to first search on the client domain name and then on the DNIS
vpdn search-order domain dnis
!
! Allow a maximum of 10 simultaneous VPDN sessions
vpdn session-limit 10
!
! Configure the NAS to initiate VPDN dial-in sessions to the tunnel server
vpdn-group 1
 request-dialin
 protocol l2tp
 domain cisco.com
!
 initiate-to ip 172.22.66.25
 local name ISP-NAS
!
! Specifies the RADIUS server IP address, authorization port, and accounting port
radius-server host 172.22.66.16 auth-port 1645 acct-port 1646
!
! Specifies the authentication key to be used with the RADIUS server
radius-server key cisco
!
```

例：ダイヤルイン VPDN のトンネル サーバの設定

次の例は、ローカル認証と許可を使用して、ISP-NAS という名前の NAS から L2TP トンネルを受理するように設定した ENT-TS という名のトンネル サーバを示しています。

```
! Configure AAA to first use the local database and then contact the RADIUS server for
! PPP authentication
aaa new-model
aaa authentication ppp default local radius
!
! Configure AAA network authorization and accounting by using the RADIUS server
aaa authorization network default radius
aaa accounting network default start-stop radius
!
! Configure the VPDN tunnel authentication password using the local name
```

```
username ISP-NAS password 7 tunnelme
username ENT-TS password 7 tunnelme
!
vpdn enable
!
! Configure the tunnel server to accept dial-in sessions from the NAS
vpdn-group 1
 accept-dialin
 protocol l2tp
 virtual-template 1
!
 terminate-from hostname ISP-NAS
 local name ENT-TS
 force-local-chap
!
! Configure the virtual template
interface Virtual-Template1
  gigabitethernet0/0/0
 ppp authentication chap
 peer default ip address pool default
 encapsulation ppp
!
! Specifies the RADIUS server IP address, authorization port, and accounting port
radius-server host 172.22.66.13 auth-port 1645 acct-port 1646
!
! Specifies the authentication key to be used with the RADIUS server
radius-server key cisco
```

例：ローカル認証での L2TP 発信側ステーション ID の抑制

次の例は、仮想 LAN（PPPoEoVLAN）を介したギガビット イーサネット上の PPP 用に NAS を設定します。NAS は、RADIUS を介して LLID NAS ポート前認証から発信側ステーション ID を取得します。発信側ステーション ID は L2TP という VPDN グループに関連付けられたトンネルに対し、ユーザ名に #184 の文字列が含まれている場合、AV ペア 22 から削除されます。

```
hostname LAC
!
enable secret 5 $1$8qtb$MHcYeW2kn8VNYgz932eXl.
enable password lab
!
aaa new-model
!
aaa group server radius LLID-Radius
 server 192.168.1.5 auth-port 1645 acct-port 1646
!
aaa group server radius LAC-Radius
 server 192.168.1.6 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local
aaa authorization network default local
aaa authorization network LLID group LLID-Radius
aaa accounting network default start-stop group LAC-Radius
aaa nas port extended
aaa session-id common
!
ip subnet-zero
ip cef
no ip domain lookup
!
vpdn enable
vpdn search-order domain
!
vpdn-group L2TP
 request-dialin
 protocol l2tp
 domain cisco.com
 domain cisco.com#184
```

```
!
 initiate-to ip 192.168.1.4
 local name test
 l2tp tunnel password 0 cisco
 l2tp attribute clid mask-method remove match #184
!
bba-group ppoe 2
 virtual-template 1
 nas-port format d 2/2/4
!
subscriber access pppoe pre-authorize nas-port-id LLID send username
!
interface Loopback0
 no ip address
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface gigabitethernet0/0/0
 ip address 192.168.1.3 255.255.255.0
 no cdp enable
!
interface gigabitethernet0/0/0.20
 encapsulation dot1Q 1024
 no snmp trap link-status
 ppoe enable group 2
 pppoe max-sessions 200
 no cdp enable
!
interface gigabitethernet1/0/0
 ip address 10.1.1.10 255.255.255.0
 no cdp enable
!
interface Serial2/0/0
no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Virtual-Template1
 ip unnumbered gigabitethernet1/0/0
 ip mroute-cache
 no peer default ip address
 ppp authentication pap
!
ip classless
ip route 0.0.0.0 0.0.0.0 gigabitethernet0/0/0
ip route 10.0.0.0 255.0.0.0 gigabitethernet1/0/0
!
no ip http server
!
radius-server attribute 69 clear
radius-server host 192.168.1.5 auth-port 1645 acct-port 1646
radius-server host 192.168.1.6 auth-port 1645 acct-port 1646
radius-server domain-stripping delimiter #
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password lab
```

例：RADIUS 認証での L2TP 発信側ステーション ID の抑制

次の例は、PPPoEoVLAN 用に NAS を設定します。NAS は、RADIUS を介して LLID NAS ポート前認証から発信側ステーション ID を取得します。RADIUS ユーザ プロファイルは発信側ステーション ID の右側の 6 文字が文字 X でに置き換えられるよう指定します。

NAS の設定

```
hostname LAC
!
enable secret 5 $1$8qtb$MHcYeW2kn8VNYgz932eXl.
enable password lab
!
aaa new-model
!
aaa group server radius LLID-Radius
 server 192.168.1.5 auth-port 1645 acct-port 1646
!
aaa group server radius LAC-Radius
 server 192.168.1.6 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local
aaa authorization network default group LAC-Radius
aaa authorization network LLID group LLID-Radius
aaa accounting network default start-stop group LAC-Radius
aaa nas port extended
aaa session-id common
!
ip subnet-zero
ip cef
no ip domain lookup
!
vpdn enable
vpdn search-order domain
!
bba-group ppoe 2
 virtual-template 1
 nas-port format d 2/2/4
!
subscriber access pppoe pre-authorize nas-port-id LLID send username
!
interface Loopback0
 no ip address
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface gigabitethernet0/0/0
 ip address 192.168.1.3 255.255.255.0
 no cdp enable
!
interface gigabitethernet0/0/0.20
 encapsulation dot1Q 1024
 no snmp trap link-status
 pppoe enable group 2
 pppoe max-sessions 200
 no cdp enable
!
interface gigabitethernet1/0/0
 ip address 10.1.1.10 255.255.255.0
 no cdp enable
!
interface Serial2/0/0
no ip address
 shutdown
 serial restart-delay 0
```

```
!
interface Serial3/0/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Virtual-Template1
 ip unnumbered gigabitethernet1/0/0
 ip mroute-cache
 no peer default ip address
 ppp authentication pap
!
ip classless
ip route 0.0.0.0 0.0.0.0 gigabitethernet0/0/0
ip route 10.0.0.0 255.0.0.0 gigabitethernet1/0/0
!
no ip http server
!
radius-server attribute 69 clear
radius-server host 192.168.1.5 auth-port 1645 acct-port 1646
radius-server host 192.168.1.6 auth-port 1645 acct-port 1646
radius-server domain-stripping delimiter #
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password lab
```

RADIUS ユーザ プロファイルの設定

```
Cisco-Avpair = vpdn:l2tp-tunnel-password=cisco
Cisco-Avpair = vpdn:tunnel-type=l2tp
Cisco-Avpair = vpdn:tunnel-id=test
Cisco-Avpair = vpdn:ip-address=192.168.1.4
Cisco-Avpair = vpdn:l2tp-clid-mask-method=right:X:6
```

次の作業

「VPDN 追加機能の設定」や「VPDN トンネル管理」モジュールでの関連するオプションのタスクをどれでも実行できます。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
VPDN コマンド	『*Cisco IOS VPDN Command Reference*』

関連項目	マニュアル タイトル
VPDN 技術の概要	『*VPDN Technology Overview*』
L2TP のテクニカル サポートのドキュメンテーション	『Layer 2 Tunnel Protocol（L2TP）』
VPDN のテクニカル サポートのドキュメンテーション	『Virtual Private Dial-Up Network (VPDN)』

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
• CISCO-VPDN-MGMT-MIB • CISCO-VPDN-MGMT-EXT-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2661	『レイヤ *2* トンネリング プロトコル（*L2TP*）』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NAS 側開始ダイヤルイン VPDN トンネリング設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *10* : *NAS* 側開始ダイヤルイン *VPDN* トンネリング設定の機能情報

機能名	ソフトウェア リリース	機能情報
L2TP 発信側ステーション ID の抑制	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 この機能は、L2TP AV ペア 22 にある、NAS からの一部またはすべての発信側ステーション ID（発信者番号 ID）を抑制することを可能とします。発信側ステーション ID の抑制はルータ上の個々の VPDN グループ用にルータでグローバルに設定できます。また、設定されている場合、リモート RADIUS サーバでも設定できます。 この機能により、次のコマンドが導入されました。**l2tpattributeclidmask-method**、**vpdnl2tpattributeclidmask-method**。
L2TP 拡張フェールオーバー	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 この機能は、トンネル確立時、ルータがピアから StopCCN メッセージを受信した場合と、セッション確立時、ピアから CDN メッセージを受信した場合にフェールオーバーするよう L2TP フェールオーバーを拡張します。いずれの場合にも、ルータは通信先として別のピアを選択します。 この機能によって導入または変更されたコマンドはありません。

第 5 章

マルチホップ VPDN の設定

マルチホップ バーチャル プライベート ダイヤルアップ ネットワーキング（VPDN）は、パケットが複数のトンネルをパス スルーすることを許可する特殊な VPDN 設定です。通常、パケットが複数のトンネルを通過することは許可されていません。マルチホップを導入すると、VPDN トンネルは各ホップの後に終了し、新たなトンネルが次のホップ先に向けて開始されます。

マルチホップ VPDN 導入は、デバイスをトンネル スイッチとして設定するために使用することもできます。トンネル スイッチは、ネットワーク アクセス サーバ（NAS）とトンネル サーバの両方として機能し、入力 VPDN トンネルからパケットを受信し、それらのパケットを出力 VPDN トンネルから送出できます。トンネル スイッチ構成は、ホールセール VPDN サービスを提供するために、各インターネット サービス プロバイダー（ISP）間で使用できます。

- 機能情報の確認，133 ページ
- マルチホップ VPDN の前提条件，134 ページ
- マルチホップ VPDN の制約事項，134 ページ
- マルチホップ VPDN に関する情報，134 ページ
- マルチホップ VPDN の設定方法，135 ページ
- マルチホップ VPDN の設定例，141 ページ
- 次の作業，142 ページ
- その他の参考資料，142 ページ
- マルチホップ VPDN の機能情報，144 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモ

ジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

マルチホップ VPDN の前提条件

マルチホップ VPDN を設定する前に、VPDN 配置を構成する必要があります。マルチホップ VPDN のシナリオと互換性のある VPDN の導入の詳細については、「マルチホップ トンネル スイッチの設定, （135 ページ）」を参照してください。

マルチホップ VPDN の制約事項

レイヤ 2 トンネリング プロトコル（L2TP）のみが Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでサポートされています。

マルチホップ VPDN に関する情報

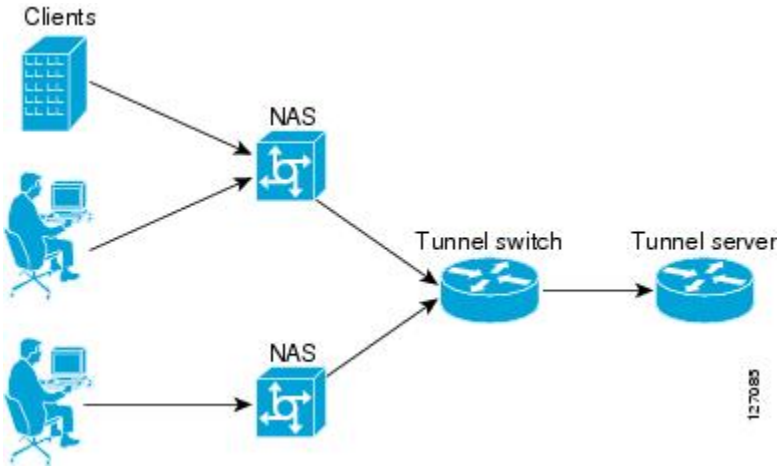
マルチホップ VPDN を使用したトンネル スイッチング

マルチホップ VPDN は、デバイスをトンネル スイッチとして設定するために使用できます。トンネル スイッチは NAS とトンネル サーバの両方として機能し、パケットを着信 VPDN トンネルから受け取り、発信先 VPDN トンネルへと送ります。トンネル スイッチの設定は、ISP 間でホールセール VPDN サービスを提供するために使われます。Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでの VPDN トンネル スイッチは L2TP セッションを転送します。L2F やポイントツーポイント トンネリング プロトコル（PPTP）はサポートされていません。

L2TP トンネルのスイッチング導入では、トンネル エンドポイントは、発信側 NAS と終端側トンネル サーバと見なされます。スイッチ トンネルは、トンネルのエンドポイントとは見なされません。

次の図は、基本的な L2TP トンネルのスイッチング導入を利用したネットワーク シナリオを示します。

図 *9*：マルチホップ *VPDN* を使用したトンネル スイッチング



トンネル スイッチは複数のデバイスから発信される VPDN トンネルを終了するように設定でき、1 つ以上のトンネル サーバに VPDN トンネルの発信を開始するようにも設定できます。

加入者サービス スイッチ（SSS）フレームワークは VPDN トンネル スイッチング用にサポートされています。SSS は、PPP over Ethernet（PPPoE）および Generic Routing Encapsulation（GRE）などの追加のレイヤ 2 プロトコルをサポートしています。VPDN トンネル スイッチングに対する SSS の設定は任意です。SSS プロファイルは、トンネル スイッチング設定の拡張性を、特にマルチプロトコル環境において向上させます。

マルチホップ VPDN の設定方法

マルチホップ トンネル スイッチの設定

マルチホップ VPDN は、デバイスをトンネル スイッチとして設定するために使用できます。トンネル スイッチは、NAS およびトンネル サーバとして機能し、NAS VPDN グループおよびトンネル サーバの VPDN グループの両方を使用して設定する必要があります。

SSS インフラストラクチャを使用したトンネル スイッチングがサポートされます。SSS を使用すると、L2TP、L2F、PPTP、PPPoE、PPPoA、GRE、および General Packet Radio Service（GPRS）の各セッションを、トンネル スイッチを使用した仮想リンクを介して切り替えることができます。SSS 設定は、L2TP、L2F、または PPTP の各トンネルを介してデータをスイッチングするトンネルには必要ありませんが、SSS によってトンネル スイッチング導入の拡張性が向上します。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、L2TP トンネルのみを転送するように、マルチホップ VPDN トンネル スイッチを設定できます。

次の各タスクを実行して、デバイスをマルチホップ VPDN トンネル スイッチとして設定します。

マルチホップ トンネル スイッチ設定の前提条件

- 「NAS 側開始ダイヤルイン VPDN トンネリング設定」のモジュールで説明するように、トンネル エンドポイントは VPDN トンネリング用に設定する必要があります。
- マルチホップのホスト名に基づいて VPDN トンネル認証の検索を実行するには、「VPDN 用の AAA 設定」のモジュールの説明に従って、マルチホップのホスト名を使用する検索を設定する必要があります。

トンネル スイッチでのマルチホップ VPDN の有効化

トンネル スイッチング構成では、パケットが複数のトンネルを通過できる必要があります。機能を実装するには、トンネル スイッチでマルチホップ VPDN を有効にする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnmultihop**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnmultihop** 例： `Router(config)# vpdn multihop`	VPDN マルチホップを有効にします。

次の作業

「着信 VPDN トンネルを終了するためのマルチホップ トンネル スイッチの設定, （137 ページ）」に示されているタスクを実行する必要があります。

着信 VPDN トンネルを終了するためのマルチホップ トンネル スイッチの設定

着信 VPDN トンネルの終端を可能とするには、トンネル スイッチはトンネル サーバとして設定する必要があります。複数のデバイスからのトンネルを終端できるよう、トンネル スイッチを設定できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **description***string*
5. **accept-dialin**
6. **protocoll2tp**
7. **virtual-template***number*
8. **exit**
9. **terminate-fromhostname***host-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**description***string* 例： `Router(config-vpdn)# description myvpdngroup`	（オプション）VPDN グループに説明を追記します。
ステップ 5	**accept-dialin** 例： `Router(config-vpdn)# accept-dialin`	トンネル スイッチが NAS からのトンネルの確立、accept-dialin VPDN サブグループの作成の要求を受け入れるよう設定し、ダイヤルインサブグループ設定モードに入ります。
ステップ 6	**protocoll2tp** 例： `Router(config-vpdn-acc-in)# protocol l2tp`	VPDN グループが使用するレイヤ 2 トンネリング プロトコルを指定します。
ステップ 7	**virtual-template***number* 例： `Router(config-vpdn-acc-in)# virtual-template 1`	（オプション）仮想アクセス インターフェイスのクローンを作成する際に使用される仮想テンプレートを指定します。 ユーザ接続時に仮想アクセスインターフェイスを複製しない場合は、この手順は不要です。
ステップ 8	**exit** 例： `Router(config-vpdn-acc-in)# exit`	VPDN グループ コンフィギュレーション モードを終了します。
ステップ 9	**terminate-fromhostname***host-name* 例： `Router(config-vpdn)# terminate-from hostname NAS12`	VPDN トンネルの受け入れ時に必要なリモート NAS のホスト名を指定します。

次の作業

「発信 VPDN トンネル開始のためのマルチホップ トンネル スイッチの設定」のセクションのタスクを実行する必要があります。

発信 VPDN トンネル開始のためのマルチホップ トンネル スイッチの設定

発信 VPDN トンネルの開始を可能とするには、トンネル スイッチは NAS として設定する必要があります。複数のデバイスへのトンネルを開始できるよう、トンネル スイッチを設定できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **description***string*
5. **request-dialin**
6. **protocoll2tp**
7. 次のいずれかを実行します。
   - **domain***domain-name*
   - **dnis** {*dnis-number* | *dnis-group-name*}
   - **multihop-hostname***ingress-tunnel-name*
8. **exit**
9. **initiate-toip***ip-address*[**limit***limit-number*] [**priority***priority-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**description***string* 例： `Router(config-vpdn)# description myvpdngroup`	（オプション）VPDN グループに説明を追記します。
ステップ 5	**request-dialin** 例： `Router(config-vpdn)# request-dialin`	トンネル スイッチがトンネル サーバへトンネルの確立を要求するように設定し、request-dialin VPDN サブグループを作成し、VPDN request-dialin サブグループ設定モードを開始します。
ステップ 6	**protocoll2tp** 例： `Router(config-vpdn-req-in)# protocol l2tp`	VPDN グループが使用するレイヤ 2 トンネリング プロトコルを指定します。

ステップ 7	次のいずれかを実行します。
	• **domain***domain-name*
	• **dnis** {*dnis-number* | *dnis-group-name*}
	• **multihop-hostname***ingress-tunnel-name*
	
	例：
	`Router(config-vpdn-req-in)# domain company.com`
	
	例：
	`Router(config-vpdn-req-in)# dnis 5687`
	
	例：
	`Router(config-vpdn-req-in)# multihop-hostname nas1`
		特定のドメイン名からの PPP コールをトンネルするよう要求します。
		または
		特定の DNIS 番号または DNIS グループからの PPP コールをトンネルするよう要求します。
		または
		NAS ホスト名または入力トンネル ID に基づいてトンネルを開始できるようトンネル スイッチを有効にします。
		（注） **multihop-hostname** コマンドを使ってトンネル スイッチを設定した場合、**multihop-hostname** キーワードを使って **vpdnsearch-order** コマンドを設定する必要があります。VPDN トンネル認証の検索順序の設定の詳細は、「VPDN 用の AAA の設定」モジュールを参照してください。

ステップ 8	**exit** 例： `Router(config-vpdn-req-in)# exit`	VPDN グループ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 9	**initiate-toip***ip-address*[**limit***limit-number*][**priority***priority-number*] 例： `Router(config-vpdn)# initiate-to ip 10.1.1.1 limit 12`	レイヤ 2 トンネリングで使用する IP アドレスを指定します。 • **limit**：この IP アドレスに対して可能な最大の接続数。 • **priority**：この IP アドレスの優先度。 （注） **priority** キーワードは、通常トンネル スイッチには設定しません。代わりに、ロードバランシングとフェールオーバーに使用する情報はリモートの AAA サーバに設定されます。リモート AAA サーバを使用したロード バランシングとフェールオーバーの優先度の設定の詳細は、「VPDN 用の AAA の設定」モジュールを参照してください。 • **initiate-to** コマンドを複数設定して、複数トンネルのサーバをトンネル スイッチに設定できます。

マルチホップ VPDN の設定例

例：マルチホップ VPDN トンネルのスイッチングの設定

次に、NAS、トンネル スイッチとトンネルサーバを設定し、L2TP を使用してマルチホップ VPDN トンネルを確立する例を示します。

NAS の設定

```
! Configure the NAS to initiate VPDN dial-in sessions to the tunnel switch
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
!
 initiate-to ip 172.22.66.25
 local name ISP-NAS
```

トンネル スイッチの設定

```
!Enable VPDN
vpdn enable
!
```

```
!Enable multihop
vpdn multihop

!

! Configure the tunnel switch to use the multihop hostname in the authentication search.

 vpdn search-order multihop-hostname domain dnis

!

! Configure the tunnel switch to accept dial-in sessions from the NAS
vpdn-group tunnelin
 accept-dialin
  protocol l2tp
  virtual-template 1
!
 terminate-from hostname ISP-NAS
 local name ISP-Sw
!
! Configure the tunnel switch to initiate VPDN dial-in sessions to the tunnel server
vpdn-group tunnelout
 request-dialin
  protocol l2tp
  multihop-hostname ISP-NAS
!
 initiate-to ip 10.2.2.2
 local name ISP-Sw
```

トンネル サーバの設定

```
! Configure the tunnel server to accept dial-in sessions from the NAS
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
!
 terminate-from hostname ISP-Sw
 local name ENT-TS
```

次の作業

「VPDN 追加機能の設定」や「VPDN トンネル管理」モジュールでの関連するオプションのタスクをどれでも実行できます。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
VPDN コマンド	『*Cisco IOS VPDN Command Reference*』
VPDN 技術の概要	『*VPDN Technology Overview*』

関連項目	マニュアル タイトル
ブロードバンド アグリゲーションおよび DSL コマンド	『*Cisco IOS Broadband Access Aggregation and DSL Command Reference*』

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2661	『レイヤ *2* トンネリング プロトコル（*L2TP*）』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

マルチホップ VPDN の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *11*：マルチホップ *VPDN* の機能情報

機能名	ソフトウェア リリース	機能の設定情報
マルチホップ VPDN	Cisco IOS XE リリース 2.2	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 マルチホップ VPDN は特殊な VPDN設定で、複数のトンネルを通過するパケットを許可します。通常、パケットが複数のトンネルを通過することは許可されていません。マルチホップを導入すると、VPDN トンネルは各ホップの後に終了し、新たなトンネルが次のホップ先に向けて開始されます。 この機能によって導入または変更されたコマンドはありません。

機能名	ソフトウェア リリース	機能の設定情報
加入者サービススイッチ（SSS）	Cisco IOS XE リリース 2.2.1	この機能により、多数の加入者が利用可能なサービスに接続する場所や方法、およびそれらのサービスの定義を柔軟に行うことができます。SSS の主な目的は、レイヤ 2 サブスクライバ ポリシーを使用して、PPP をあるポイントから別のポイントへ誘導することです。PPP のトンネリングは、ポリシーに基づいてブリッジングする方法で、ポリシーによって管理されます。 この機能により、次の VPDN コマンドが導入または変更されました。 **multihop-hostname**、**vpdnsearch-order**。

第 6 章

VPDN 追加機能の設定

このモジュールでは、Virtual Private Dialup Network（VPDN）のその他の機能の設定に関連する概念およびタスクについて説明します。次の各オプション機能は、VPDN 導入と組み合わせて使用され、VPDN 導入をまず設定する必要があります。

- VPDN テンプレート
- VPDN 送信元 IP アドレス
- VRF 認識型 VPDN トンネル
- L2TP VPDN トンネルへの MTU 調整
- VPDN トンネルへの QoS
- VPDN グループ選択

このモジュールで説明されているすべてのタスクが、『*Cisco IOS XE VPDN Configuration Guide*』のどこかで説明されている各タスクをまず完了させている必要があります。

- 機能情報の確認，147 ページ
- VPDN 追加機能の設定に関する情報，148 ページ
- VPDN 追加機能の設定方法，154 ページ
- VPDN の追加機能の設定例，180 ページ
- 次の作業，188 ページ
- その他の参考資料，188 ページ
- VPDN 追加機能の機能情報，190 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用の

プラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

VPDN 追加機能の設定に関する情報

VPDN テンプレート

VPDN テンプレートは、システムのデフォルト値を差し替えるグローバルなデフォルト値を設定できます。これらのグローバルデフォルト値は、特定の値が個々の VPDN グループ用に設定されていない限り、すべての VPDN グループに適用されます。

単一グローバル（名前無し）VPDN テンプレートに加え、複数の名前付き VPDN テンプレートを設定できます。VPDN グループは 1 つの VPDN テンプレートにのみ関連付けられます。

グローバル VPDN テンプレートで設定された値は、すべての VPDN グループにデフォルトで適用されます。VPDN グループは、グローバル VPDN テンプレートからの関連付け解除や、名前付き VPDN テンプレートとの関連付けができます。VPDN グループを名前付き VPDN テンプレートと関連付けると、グローバル VPDN テンプレートからの関連付けが解除されます。

VPDN パラメータの VPDN グループへの適用に関するデフォルトの階層は次のようになります。

- 個別の VPDN グループに対する VPDN パラメータ設定は、常にその VPDN グループに適用されます。
- 関連付けされた VPDN テンプレートでの VPDN パラメータ設定は、個別の VPDN グループ設定にて未指定の設定すべてに関して適用されます。
- VPDN パラメータに対するシステムのデフォルト設定は、個別の VPDN グループ設定または、関連付けられた VPDN テンプレートにて未指定の設定すべてに適用されます。

個々の VPDN グループは、関連付けのある VPDN テンプレートから関連付け解除することができ、システムデフォルト設定を、個々の VPDN グループで未設定のパラメータに対して使うことができます。

VPDN 送信元 IP アドレス

トンネル エンドポイントは VPDN トンネルを開くために使用する IP アドレスと異なる送信元 IP アドレスで設定できます。送信元 IP アドレスがトンネルのエンドポイントで設定されると、ルータは、設定した送信元 IP アドレスでラベル付けされた VPDN パケットを生成します。トンネル エンドポイントが異なる企業により管理され、アドレッシングの要件で特定の IP アドレスが使われる必要があるとされる場合、送信元 IP アドレスを設定する必要がある場合があります。

送信元 IP アドレスは、グローバルで、もしくは個別の VPDN グループに対して設定できます。VPDN グループの設定がグローバル設定よりも優先されます。

PPP 経由の VPN ルーティング転送（VRF）フレームルート（プール）割り当て

PPP経由のVPNルーティング転送（VRF）フレームルート（プール）割り当て機能は次のRADIUS属性をVRF認識型にするのをサポートします。対象は属性22（Framed-Route）、属性8フレーム（Framed-IP-Address）と属性9（Framed-IP-Netmask）の組み合わせで、およびCisco VSAルートコマンドです。そのため、スタティック IP ルートは、グローバル ルーティング テーブルではなく特定 VRF ルーティング テーブルに適用できます。

VRF 認識型 VPDN トンネル

Cisco IOS XE リリース 2.2 以前は、VPDN トンネルのエンドポイントにグローバル ルーティング テーブルからの IP アドレスを指定する必要がありました。VRF 認識型 VPDN トンネルは、VRF ルーティングテーブルからのIPアドレスを利用できるようにすることで、バーチャルプライベート ネットワーク（VPN）ルーティングおよび転送（VRF）インスタンスで終了する VPDN トンネルをサポートしています。

VRF 認識型 VPDN トンネルは、マルチプロトコル ラベル スイッチング（MPLS）VPN の外部で VPDN トンネルを開始させ、MPLS VPN 内で終了させ、そして重複する IP アドレスを持たせることにより、VPDN トンネルのサポートを向上させます。たとえば、この機能により、宛先アドレスとして顧客の VRF からの VRF アドレスを利用することができます。

Cisco IOS XE リリース 2.2 以降では、VRF 認識型 VPDN トンネル機能には LNS での L2TP のサポートが追加されます。VRF インスタンス内でのトンネルの開始と終了に関しては、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ上で、LNS とレイヤ 2 アクセス コンセントレータ（LAC）環境の両方でサポートしています。

VRF 認識型 VPDN トンネルはマルチホップおよび VPDN トンネリングのシナリオで利用できます。マルチホップのシナリオでは、この機能は、VRF 認識型 VPDN マルチホップと呼ばれる場合があります。

L2TP VPDN トンネルへの MTU 調整

パケットのフラグメンテーションとリアセンブルはソフトウェア内でプロセス レベルで実行されます。トンネル サーバが大量のセッションとトラフィック フローを集約する際には、プロセス スイッチングでは、パフォーマンスが大幅に低下する可能性があります。そのため、VPDN 配置でのパケット フラグメンテーションとリアセンブルの必要性を減らすかなくし、代わりにクライアント デバイスに必要なパケット リアセンブルの負荷を移動させることがとても理想的です。

パケットサイズよりも少ない最大伝送ユニット（MTU）で出力インターフェイスを通過させようとするときに、パケットはフラグメント化されます。デフォルトでは、ほとんどのインターフェイスのMTUは1500バイトです。このデフォルトMTUサイズにより、TPCセグメントは、デフォ

ルトの 1460 バイトのペイロードで作成され、TCP/IP ヘッダー用に 40 バイトを残します。L2TP のカプセル化で 40 バイトのヘッダー情報を追加するので、MTU 調整が行われていない場合、トンネリングされたパケットはインターフェイスの MTU を超えます。

最終的な宛先に到達するためには、パケットには複数の出力インターフェイスを通過する可能性があります。パス MTU は、パケットが通るインターフェイスすべての最小の MTU として定義されます。

さまざまな方法で、MTU の調整を実行できます。最終的なねらいは、トンネリング用にカプセル化されたあとでのパケットのフラグメンテーションを防ぐことです。これらのメソッドでは、次のセクションで説明されているように、実現するために特別なメカニズムを活用しています。

IP MTU の調整を使用しての MTU の調整

IP MTU の設定は、レイヤ 2 プロトコルでカプセル化されるパケットの許容される最大サイズを制御します。インターフェイスの IP MTU は、パス MTU がわかれば、L2TP ヘッダーのサイズを補うために手動で減らすことができます。

ルータは、L2TP ヘッダーのサイズを補うために、自動的にインターフェイスの IP MTU サイズを調整するように設定することもできます。自動調整は、そのデバイスの出力インターフェイスの MTU に基づいて L2TP ヘッダーのサイズを訂正します。この設定は、そのインターフェイスの MTU がパス MTU と同じときにフラグメンテーションを防止する際にのみ有効です。

パス MTU ディスカバリを使った MTU 調整

NAS とトンネル サーバ間でパス MTU が不明である場合、または変更がある場合は、パス MTU 検出（PMTUD）が MTU 調整のために用いられます。PMTUD は IP ヘッダー内で Don't Fragment（DF）ビットを使用し、ルーティングパスに沿ったすべてのインターフェイスの間で最小の MTU をダイナミックに検出します。

送信元ホストは、まず最初の出力インターフェイスの既知の MTU がパス MTU であるとみなし、IP ヘッダーの DF ビットが設定された状態で、そのパスのすべてのパケットを送信します。もしパケットが大きすぎて、フラグメンテーションなしでパスに沿うデバイスのインターフェイスによる転送ができない場合、そのデバイスはパケットを捨てて、Internet Control Message Protocol（ICMP）接続先到達不能のメッセージを送信元ホストに返します。ICMP 接続先到達不能メッセージにはコード 4 が含まれ、これはフラグメンテーションが必要で、*DF* 設定されていることを示し、またフラグメンテーションなしでのパケット転送ができなかったインターフェイスの IP MTU を示しています。この情報により、送信元ホストは、再送信する前に、インターフェイスを通して適する大きさに、パケットサイズを減らすことができます。

PMTUD を有効化すると、VPDN 配置は、接続のパス MTU を実行不可能なほど低い値に設定するように精巧に作られた ICMP メッセージを使うサービス妨害（DoS）に対しての脆弱性を持つようになります。これは、接続が確立されている状態であっても、スループットが非常に低いため、上位層プロトコルへのタイムアウトを引き起こします。このタイプの攻撃は、スループット低下攻撃に分類されます。L2TP VPDN 配置へのスループット低下の攻撃の詳細については、「その他の参考資料」セクションを参照してください。

スループット低下の攻撃からネットワークを保護するため、パス MTU 用に受け入れ可能な値の範囲を指定することができます。もし設定したサイズ幅を超えてしまうなネクストホップ パス MTU をアドバタイズする ICMP コード 4 のメッセージをデバイスが受信する場合、デバイスはメッセージを無視します。

インターネット経由で実行される場合、一部のルータやファイアウォールがすべての ICMP メッセージをフィルタ処理して除外するように設定されているため、PMTUD は信頼性がなくなり、失敗する場合があります。パケットをフラグメンテーションなしに転送することができないデバイスから送信元ホストが ICMP 接続先到達不能メッセージを受け取らない場合、パケットサイズの縮小は行いません。送信元ホストは同じ大きさのパケットを再送信し続けます。DF ビットが設定されているため、パス MTU を超過していることにより、これらのパケットは継続的に失われます。そして、接続は応答を停止します。

TCP MSS アドバタイジングを使用した MTU 調整

PMTUD が信頼できない可能性があるため、MTU 調整を実行する別の方法が導入されました。MTU 調整のこの方法は、TCP 最大セグメント サイズ（MSS）アドバタイズメントをエンドホストから送られる着信または発信同期（SYN）パケットで活用します。

TCP MSS は単一の TCP/IP データグラムでのホストが受信できるデータの最大量を定義します。MSS 値は、TCP SYN セグメント内でのみ TCP ヘッダー オプションとして送信されます。TCP 接続のそれぞれの側では、もう一方の側に MSS 値をレポートします。送信側ホストは、単一の TCP セグメントのデータ サイズを、受信側ホストで報告された MSS 値以下の値に制限する必要があります。

通常のデフォルト値である 1460 より低い TCP MSS を設定した場合、L2TP ヘッダーによって追加した情報を補うため、TCP セグメントのサイズが減少します。

PPP MRU アドバタイジングを使用した MTU 調整

VPDN L2TP ネットワークのフラグメンテーションを減らすためのもう 1 つのオプションでは、最大受信ユニット（MRU）のネゴシエーションが PPP クライアントによってサポートされている必要があります。MRU ネゴシエーションをサポートする既知のクライアントの 1 つとしては、Windows XP PPP クライアントがあります。残念ながら、ほかに普及している PPP クライアントには、アドバタイズ PPP MRU に適切に準拠していないものもあります。PPP クライアントがアドバタイズされる PPP MRU に正しく応答するかどうかを確認するには、PPP クライアントのドキュメンテーションを参照してください。

PPP MRU は、ピアが最大受信ユニットをアドバタイズするのを可能にします。これは、仮想テンプレート インターフェイスでの MTU 設定から由来するものです。デバイスは、アドバタイズされる MRU より大きなペイロードを含む PPP フレームを処理できません。Cisco PPP の実装は、PPP ネゴシエーションの間に、アドバタイズされた MRU 値としてインターフェイスの MTU を使用します。

仮想テンプレート インターフェイスの MTU は、L2TP ヘッダーのサイズを補うために手動で下げることが可能です。PPP ピアが PPP ネゴシエーションの間にアドバタイズされる MRU を聞き入れる場合、その PPP リンクに対して、MTU（および間接的に IP MTU）を調整します。これは、TCP 接続を開始させるときに、ピアがアドバタイズする TCP MSS を変更することになります。

インターフェイスのデフォルト MTU は 1500 バイトであるため、デフォルトの MRU は 1500 バイトです。インターフェイスの MTU を 1460 に変更すると、アドバタイズされる MRU が 1460 へと変更されます。この設定により、ピアに 40 バイトの L2TP ヘッダー用に容量を残すよう指示します。

仮想テンプレート インターフェイスの MTU を低く設定したときの問題の 1 つに、IP MTU も自動的に低く設定されてしまうことが挙げられます。仮想テンプレート インターフェイスの MTU よりも大きい IP MTU を設定することはできません。アドバタイズされる MRU に基いての MTU の調節の有無が混同するピア デバイスがある場合、問題となります。MRU のアドバタイズメントを受信できず、それに応じて調整のできないクライアントが、ピアへフルサイズのパケットを送信し続けます。低く設定した IP MTU より大きく、通常のデフォルト IP MTU よりも小さいパケットは、フラグメント化を余儀なくされます。たとえば、1490 バイトの L2TP パケットは通常、フラグメント化なしで送信されます。MTU が 1460 バイトに下げられている場合、このパケットには不必要なフラグメント化が起こります。この状況では、より低い MRU を、受信や調整が可能なクライアントに対しアドバタイズし、かつ、調整ができないクライアントに対しフルサイズのパケットを許可するのが最適です。

アドバタイズされた MRU を無視するクライアントでは、「IP MTU の調整を使用しての MTU の調整, （150 ページ）」で説明されている PMTUD の問題が発生する可能性があります。PMTUD は、IP パケット内部の DF ビットをクリアすることでオフにできます。

VPDN トンネルへの QoS

Quality of Service（QoS）パケット分類機能により、ネットワーク トラフィックを複数のプライオリティ レベルまたはサービス クラスに区分することが可能になります。パケット分類はネットワーク内、およびネットワーク間のエンドツーエンドの QoS を調整するために必要な情報を提供します。他の QoS 機能ではパケット分類を使用して、輻輳管理、帯域幅割り当て、および遅延限度などの適切なトラフィック処理ポリシーを各トラフィック クラスに割り当てることができます。

パケットは、IP ヘッダー内のタイプ オブ サービス（ToS）バイトを使用したエンドツーエンドの QoS としてマークすることができます。ToS バイトの先頭 3 ビットは、IP プレシデンス設定に使用されます。残りの 5 ビットのうちの 4 つが ToS を設定するために使用されます。ToS バイトの残りのビットは割り当てられていません。

VPDN 配置では、IP パケットは、顧客のネットワークまたはダウンストリーム クライアントなどの外部ソースにより分類されることがあります。デフォルトでは、トンネル エンドポイントは、レイヤ 2 ヘッダーの ToS バイトをゼロに設定し、通常のサービスを指定します。VPDN 配置により、QoS の分類について、次のいずれかを実施するように VPDN ネットワークを設定できます。

- デフォルト設定のままにすることで、既存の QoS 分類を無視します。
- IP ヘッダーからレイヤ 2 ヘッダーに ToS バイトをコピーするようにトンネル エンドポイントの設定することにより、既存の QoS 分類を維持します。
- ご使用の VPDN ネットワーク固有の QoS の分類を設定します。

以下のセクションで VPDN 配置に関する QoS オプションについての追加情報を説明しています。

QoS 分類の保持

レイヤ 2 パケットを作成すると、ToS バイト値はデフォルトでゼロに設定され、通常のサービスを示します。この設定は、トンネリングされるカプセル化された IP パケットの ToS バイトの値を無視します。トンネル サーバはレイヤ 2 ヘッダーの ToS バイトに内部 IP パケットの ToS フィールドの内容をコピーするように設定できます。IP ヘッダーからレイヤ 2 ヘッダーへ ToS をコピーすると、トンネル パケットのエンドツーエンドの QoS フィールドが保持されます。

VPDN トンネル向け IP プレシデンス

IP プレシデンス設定では、パケットのサービス クラス（CoS）にマークを付けます。IP ヘッダーの ToS フィールドにある 3 つの precedence ビットは、最大 6 つのサービス クラスを定義するために使用できます。レイヤ 2 パケットに特定の IP プレシデンス値を手動で設定した場合、QoS はトンネル全体のエンドツーエンドで維持されません。

VPDN トンネルの ToS の分類

ToS ビットはパケットに対しての ToS の分類をマークします。信頼性、スループット、遅延、コストの 4 つのビットがそれぞれ ToS の特定の性質を制御します。レイヤ 2 パケットに対して、特定の ToS 値を手動で設定する場合、QoS はトンネル全体のエンドツーエンドを保持しません。

VPDN グループ選択

VPDN グループ選択機能により、LAC と LNS 間の複数の VPDN トンネルに対し、異なる VPDN グループの設定ができるようになります。

VPDN グループ選択機能では 2 つの新しいキーを導入したことにより、LNS が同じ LAC から複数の VPDN トンネルに接続できるようになり、カスタマイズした設定に対して、別の VPDN のテンプレートを使用する異なる VPDN グループにバインドできるようになりました。これらのキーは次のとおりです。

- L2TP Start-Control-Connection-Request (SCCRQ) を受信した宛先 IP アドレス
- SCCRQ を受信した Virtual Routing and Forwarding（VRF）インスタンス

VPDN グループ選択機能により、LAC は異なる IP アドレスまたは異なる VRF に VPDN トンネルを構築できます。

VPDN グループ選択の利点

VPDN グループ選択機能を使用すれば、SP は LAC と LNS 間で複数の VPDN グループまたは VPDN トンネルをサポートできます。これは、以前からサポートされているホスト名選択キーに加えて、新しい VPDN グループ選択キーの宛先 IP アドレスまたは VRF ID を使用して実行されます。VPDN グループ選択機能によって、SP は VPDN トンネルごとにカスタマイズした設定を指定できます。

VPDN 追加機能の設定方法

VPDN テンプレートの作成

VPDNテンプレートを作成するには、NASまたはトンネルサーバで次の作業を実行します。名前付きVPDNテンプレートを削除すると、関連付けられていたすべてのVPDNグループは自動的にグローバルVPDNテンプレートに関連付けられます。

（注）
- VPDNテンプレート設定を使用するには、L2TPトンネルが確立している必要があります。トンネルが確立されると、トンネルがダウンし、再確立されるまでVPDNテンプレートの設定の変更はトンネルに影響しません。
- VPDNグループの設定に使用可能なコマンドのすべてがVPDNテンプレートの設定に使用できるとは限りません。VPDN設定モードで使用できるコマンドの一覧は、VPDNテンプレート コンフィギュレーション モードで**?**コマンドを使用して確認します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-template**[*name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ3	**vpdn-template**[*name*] 例： `Router(config)# vpdn-template l2tp`	VPDNテンプレートを作成し、VPDNテンプレート コンフィギュレーション モードを開始します。

VPDN グループと VPDN テンプレートの関連付け

VPDN グループはデフォルトでグローバル VPDN テンプレートに関連付けられています。代わりに、個々の VPDN グループを名前付き VPDN テンプレートに関連付けることもできます。VPDN グループを名前付き VPDN テンプレートに関連付けると、グローバル VPDN テンプレートとの関連は解除されます。

このタスクを NAS またはトンネルサーバで実行し、特定の VPDN グループを名前付き VPDN テンプレートに関連付けます。または、グローバル VPDN テンプレートとの関連が以前に解除された VPDN グループに、再度グローバル VPDN テンプレートとの関連付けを行います。

はじめる前に

- VPDN テンプレートを作成し、有効にします。詳細については、「VPDN テンプレートの作成」のセクションを参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **sourcevpdn-template**[*name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group l2tp`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**sourcevpdn-template**[*name*] 例： `Router(config-vpdn)# source vpdn-template l2tp`	VPDN グループを VPDN テンプレートに関連付けます。 • VPDN グループはデフォルトで無名の VPDN に関連付けられています。 • **nosourcevpdn-template** コマンドを使って VPDN グループの VPDN テンプレートとの関連を解除した場合、**sourcevpdn-template** コマンドを実行して再度の関連付けができます。 • VPDN グループを名前付き VPDN テンプレートに関連付けると、グローバル VPDN テンプレートとの関連は解除されます。

VPDN グループと VPDN テンプレートの関連付け解除

必要に応じて、各 VPDN グループと VPDN テンプレートの関連付けを解除できます。各 VPDN グループに設定されていないパラメータの値にはすべてシステムのデフォルト値が適用されます。

VPDN グループと VPDN テンプレートの関連付けを解除するには、NAS またはトンネル サーバで次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **nosourcevpdn-template**[*name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group l2tp`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**nosourcevpdn-template**[*name*] 例： `Router(config-vpdn)# no source vpdn-template l2tp`	未指定のパラメータすべてについて、VPDNテンプレートの設定ではなく、システムのデフォルトを使用するよう、各 VPDN グループを設定します。 • VPDN グループはデフォルトで無名の VPDN に関連付けられています。VPDN グループと VPDN テンプレートの関連付けを解除するには **nosourcevpdn-template** コマンドを使用します。 • **nosourcevpdn-template** コマンドを使って VPDN グループの VPDN テンプレートとの関連を解除した場合、**sourcevpdn-template** コマンドを実行して再度の関連付けができます。

VPDN 送信元 IP アドレスの設定

NAS またはトンネル サーバ上で送信元 IP アドレスを設定するには、次のいずれかのタスクを実行します。

グローバル VPDN 送信元 IP アドレスの設定

デバイスにグローバルの一意の送信元 IP アドレスを設定できます。送信元 IP アドレスが VPDN グループに設定されている場合は、その VPDN グループに属するトンネルではグローバル送信元 IP アドレスは使用されません。

グローバル発信元 IP アドレスを設定するには、トンネル エンドポイントで次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnsource-ip***ip-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnsource-ip***ip-address* 例： `Router(config)# vpdn source-ip 10.1.1.1`	VPDN トンネルを開くために使用された物理 IP アドレスとは異なるグローバル IP アドレスを指定します。

VPDN グループの送信元 IP アドレスの設定

特定の VPDN グループの送信元の IP アドレスを設定できます。送信元 IP アドレスが VPDN グループに設定されている場合は、その VPDN グループに属するトンネルではグローバル送信元 IP アドレスは使用されません。

特定の VPDN グループに送信元の IP アドレスを設定するには、トンネル エンドポイントで次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **source-ip***ip-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**source-ip***ip-address* 例： `Router(config-vpdn)# source-ip 10.1.1.1`	VPDN グループに属するトンネルについて、VPDN トンネルを開くために使用された物理アドレスとは異なる IP アドレスを指定します。

VRF 認識型 VPDN トンネリング設定

VRF 認識型 VPDN トンネリングは、NAS、トンネル サーバ、またはマルチホップ トンネル スイッチ上でローカルに設定でき、またリモート RADIUS サーバ プロファイル内で設定することもできます。VRF 認識型 VPDN トンネリングを RADIUS サーバ プロファイル内に設定すると、この設定は NAS またはマルチホップ トンネル スイッチにのみ反映されます。VRF 認識型 VPDN トンネルをトンネル サーバに設定するには、そのトンネル サーバをローカルに設定する必要があります。

次のいずれかのタスクを実行して、VRF 認識 VPDN トンネルを設定します。

ローカルでの VRF 認識型 VPDN トンネリングの設定

VRF 認識型 VPDN トンネリングは、NAS、トンネル サーバ、マルチホップ トンネル スイッチ上でローカルに設定することができます。デバイスに VRF 認識型 VPDN トンネリングを設定すると、その VPDN グループに設定されているトンネル エンドポイントの IP アドレスはグローバル

なルーティングテーブルではなく、特定の VRF ルーティングテーブルに属するものと指定したことになります。

VRF に属する VPDN トンネルを設定するには、マルチホップ トンネル スイッチ、NAS またはトンネル サーバで次の作業を実行します。

はじめる前に

- マルチホップ、ダイヤルイン、またはダイヤルアウト VPDN L2TP トンネリングが導入されている必要があります。
- L2TP VPDN グループで設定されている送信元 IP アドレスと宛先 IP アドレスは、指定の VPN 上に存在している必要があります。
- VRF は Cisco Express Forwarding を使用しているため、この作業を実行する前に、Cisco Express Forwarding を設定する必要があります。

（注） L2TP は、VRF 対応の VPDN トンネリングをサポートする唯一のトンネリング プロトコルです。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **vpn** {**vrf***vrf-name* | **id***vpn-id*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group mygroup`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**vpn** {**vrf***vrf-name* | **id***vpn-id*} 例： `Router(config-vpdn)# vpn vrf myvrf`	VPDN グループの送信元および宛先 IP アドレスが、指定した VRF インスタンスに属するように指定します。 • **vrf***vrf-name*：VRF 名により VRF インスタンスを指定します。 • **id***vpn-id*：VPN ID により VRF インスタンスを指定します。

リモート RADIUS AAA サーバでの VRF 認識型 VPDN トンネリングの設定

VRF 認識型 VPDN トンネリングは、リモート RADIUS サーバ プロファイルで設定できます。デバイスに VRF 認識型 VPDN トンネリングを設定すると、その VPDN グループに設定されているトンネル エンドポイントの IP アドレスはグローバルなルーティング テーブルではなく、特定の VRF ルーティングテーブルに属するものと指定したことになります。

VRF 認識型 VPDN トンネリングを RADIUS サーバプロファイル内に設定すると、この設定は NAS またはマルチホップ トンネル スイッチにのみ反映されます。VRF 認識型 VPDN トンネリングをトンネル サーバに設定するには、「VRF 認識型 VPDN トンネルのローカル設定」セクションの作業を実行してトンネル サーバをローカルに設定する必要があります。

リモート RADIUS サーバで次の手順を実行します。RADIUS サーバ プロファイルに設定したトンネル属性は NAS またはマルチホップ トンネル スイッチに伝達されます。

はじめる前に

- マルチホップ、ダイヤルイン、またはダイヤルアウト VPDN L2TP トンネリングが導入されている必要があります。
- L2TP VPDN グループで設定されている送信元 IP アドレスと宛先 IP アドレスは、指定の VPN 上に存在している必要があります。
- VRF は Cisco Express Forwarding を使用しているため、この作業を実行する前に、Cisco Express Forwarding を設定する必要があります。
- NAS またはトンネル スイッチはリモート RADIUS AAA 向けに設定されている必要があります。「VPDN 用の AAA の設定」モジュールの「NAS とトンネルサーバでの AAA の設定」セクションと「VPDN 用のリモート AAA の設定」セクションの作業を実行し、リモート RADIUS AAA 用に NAS を設定します。
- RADIUS サーバは AAA 向けに設定されている必要があります。

（注） L2TP は、VRF 対応の VPDN トンネリングをサポートする唯一のトンネリング プロトコルです。

手順の概要

1. **Cisco-Avpair=vpdn:tunnel-id=***name*
2. **Cisco-Avpair=vpdn:tunnel-type=l2tp**
3. **Cisco-Avpair=vpdn:vpn-vrf=***vrf-name*
4. **Cisco-Avpair=vpdn:l2tp-tunnel-password=***secret*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**Cisco-Avpair=vpdn:tunnel-id=***name* 例： `Cisco-Avpair = vpdn:tunnel-id=test`	RADIUS ユーザ プロファイルでトンネル ID を指定します。
ステップ 2	**Cisco-Avpair=vpdn:tunnel-type=l2tp** 例： `Cisco-Avpair = vpdn:tunnel-type=l2tp`	RADIUS ユーザ プロファイルでトンネリング プロトコルとして L2TP を指定します。

ステップ 3	**Cisco-Avpair=vpdn:vpn-vrf=***vrf-name*
	例：
	`or`
	例：
	Cisco-Avpair = vpdn:vpn-id=*vpn-id*
	例：
	`Cisco-Avpair = vpdn:vpn-vrf=myvrf`
	例：
	`or`
		RADIUS ユーザプロファイルにある VRF 名を使用して VPDN トンネルに関連付けられる VRF インスタンスを指定します。
		または
		RADIUS ユーザプロファイルにある VPN ID を使用して VPDN トンネルに関連付けられる VRF インスタンスを指定します。

	コマンドまたはアクション	目的
	例： `Cisco-Avpair = vpdn:vpn-id=A1:3F6C`	
ステップ 4	**Cisco-Avpair=vpdn:l2tp-tunnel-password=***secret* 例： `Cisco-Avpair = vpdn:l2tp-tunnel-password=cisco`	RADIUS ユーザ プロファイルで L2TP トンネル パスワードを指定します。

L2TP の VPDN に対する MTU 調整の実行

MTU の調整により、VPDN 配置での VPDN パケットのフラグメンテーションや L2TP のリアセンブルを軽減または防止します。トンネル サーバは通常、VPDN 配置で多くのセッションおよびトラフィック フローを集約するデバイスであるため、パケットのフラグメンテーションやリアセンブルに必要なプロセス スイッチングのパフォーマンスの影響は大きく、このデバイス上では望ましくありません。

さまざまな方法で、MTU の調整を実行できます。ねらいは、トンネリング用にカプセル化されたあとでのパケットのフラグメンテーションを防ぐことです。MTU 調整の最も信頼性の高い方法は、アドバタイズされた TCP MSS の手動での設定によるものです。

MTU 調整を実行するには、次のいずれかのタスクを実行します。

VPDN 配置のための IP MTU の手動設定

トンネル パケットのフラグメンテーション量を減らすための 1 つの方法は、完全なレイヤ 2 ヘッダーがパケットに付加される以上、IP MTU を NAS とトンネル サーバ間のパス MTU を超えない最大の IP パケットサイズに手動で設定することです。

IP MTU を手動で下げるには、トンネル サーバで次の作業を実行します。

はじめる前に

- L2TP VPDN を構成する必要があります。
- NAS とトンネル サーバ間のパス MTU を知る必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacevirtual-template***number*
4. **ipmtu***bytes*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfacevirtual-template***number* 例： `Router(config)# interface virtual-template 1`	仮想アクセスインターフェイスの作成でダイナミックに設定して適用できる仮想テンプレート インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipmtu***bytes* 例： `Router(config-if)# ip mtu 1460`	インターフェイスで送信される IP パケットの MTU サイズを設定します。 （注） レイヤ 2 ヘッダーは 40 バイトであるため、*bytes* 引数の推奨値は 1460 です。

VPDN 配置での IP MTU 自動調整の有効化

トンネル サーバは、レイヤ 2 ヘッダーのサイズを補正するため、インターフェイスの IP MTU サイズを自動調整するように設定できます。デバイスの出力インターフェイスの MTU に基づいてレイヤ 2 のヘッダーのサイズの違いを自動的に修正します。この設定は、インターフェイスとパスの MTU が同じ場合のみ、フラグメンテーション防止に役立ちます。

IP MTU の自動調整を有効にするには、トンネル サーバで次の作業を実行します。

はじめる前に

• VPDN 配置を構成する必要があります。

（注）
- IP MTU の自動調整はデフォルトで無効になっています。
- IP MTU は仮想テンプレート インターフェイスに手動で設定された IP MTU がない場合のみ自動調整されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **ipmtuadjust**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**ipmtuadjust** 例： `Router(config-vpdn)# ip mtu adjust`	仮想アクセス インターフェイスの IP MTU の自動調整を有効にします。

VPDN に対するパス MTU ディスカバリの有効化

NAS とトンネル サーバ間のパス MTU が可変または不明であれば、VPDN 用に PMTUD を有効にできます。PMTUD は IP ヘッダーの DF ビットを使い、ルーティング パスに沿ったすべてのインターフェイスの中から、最低の MTU をダイナミックに検出します。

注意 PMTUD を有効にすると、VPDN を使用した構成は偽装した ICMP メッセージを使ってパス MTU を実用不可能なほどに低下させる DoS 攻撃に弱くなります。これは、接続が確立されている状態であっても、スループットが非常に低いため、上位層プロトコルへのタイムアウトを引き起こします。このタイプの攻撃は、スループット低下攻撃に分類されます。スループット低下攻撃と L2TP VPDN 構成における PMTUD 攻撃の検出については「その他の参考資料」セクションを参照してください。

一部のルータやファイアウォールは ICMP メッセージをフィルタリングする設定になっているため、PMTUD をインターネット上で実行した場合、失敗することがあります。パケットをフラグメンテーションなしに転送することができないデバイスから送信元ホストが ICMP 接続先到達不能メッセージを受け取らない場合、パケットサイズの縮小は行いません。送信元ホストは同じ大きさのパケットを再送信し続けます。DF ビットが設定されているため、パス MTU を超えたこれらのパケットはずっとドロップされ、接続の応答は途絶えます。

PMTUD を有効にし、VPDN L2TP 環境をスループット低下、DoS 攻撃から保護するには、トンネル サーバで次の作業を実行します。

はじめる前に

VPDN 配置を構成する必要があります。

（注）
- PMTUD が有効な場合、Cisco ソフトウェアの各リリースはスループット低下を招く DoS 攻撃を受けやすくなります。これらのバージョンのソフトウェアが稼働している場合、DoS 攻撃からの防護を確保するには PMTUD を無効にするしかありません。
- このソフトウェアはスループット低下攻撃に対する保護に有効なパス MTU の調整を行う **vpdnpmtu** コマンドをサポートしていません。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **ippmtu**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**ippmtu** 例： `Router(config-vpdn)# ip pmtu`	レイヤ 2 トラフィックに対しパス MTU のディスカバリを有効にします。
ステップ 5	**exit** 例： `Router(config-vpdn)# exit`	VPDN グループ コンフィギュレーション モードを終了します。

アドバタイズされた TCP MSS の手動設定

アドバタイズ TCP MSS に手動で低い値を設定すると、トランスポート層で TCP が生成する IP パケットが小さくなり、VPDN 構成で発生するパケットのフラグメンテーションが減少または消滅します。

デフォルトのアドバタイズ TCP MSS は 1460 です。これで、40 バイトの TCP/IP ヘッダーのスペースが確保されます。トンネル上でのパケットのフラグメンテーションを防ぐため、TCP MSS をさらに減らし、レイヤ 2 カプセル化ヘッダーのスペースを用意します。

TCP MSS を手動で下げるには、トンネル サーバで次の作業を実行します。

はじめる前に

VPDN 配置を構成する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacevirtual-template***number*
4. **iptcpadjust-mss***bytes*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfacevirtual-template***number* 例： `Router(config)# interface virtual-template 1`	仮想アクセス インターフェイスの作成でダイナミックに設定して適用できる仮想テンプレート インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**iptcpadjust-mss***bytes* 例： `Router(config-if)# ip tcp adjust-mss 1420`	ルータを通過する TCP SYN パケットの MSS 値を調整します。 （注） レイヤ 2 ヘッダーは 40 バイトであるため、*bytes* 引数の推奨値は1420です。

MRU アドバタイジングの設定

レイヤ 2 ヘッダのサイズを補正するため、仮想テンプレートインターフェイスで、低い MTU を手動で設定できます。インターフェイスの MTU は、PPP ピアには MRU としてアドバタイズされます。ピアがこのアドバタイズメントを受信できる PPP クライアントを実行している場合、その PPP リンクについて自己の MTU（および、間接的にその IP MTU）を調整できます。これにより、TCP 接続の開始時にピアがアドバタイズする TCP MSS が変わります。

インターフェイスのデフォルト MTU は 1500 バイトであるため、デフォルトの MRU は 1500 バイトです。インターフェイスの MTU を 1460 に変更すると、アドバタイズされる MRU が 1460 へと

変更されます。この設定により、40 バイトのレイヤ 2 ヘッダ用の余地を残すようにピアに指示できます。

仮想テンプレート インターフェイスの MTU を手動で下げるには、次の作業を実行します。

はじめる前に

VPDN 配置を構成する必要があります。

（注）

- PPP クライアントで MRU ネゴシエーションがサポートされている必要があります。MRU ネゴシエーションをサポートしているクライアントのひとつとして、Windows XP PPP クライアントがあります。ほかに普及している PPP クライアントには、アドバタイズ PPP MRU に適切に準拠していないものもあります。PPP クライアントがアドバタイズされる PPP MRU に正しく応答するかどうかを確認するには、PPP クライアントのドキュメンテーションを参照してください。
- インターフェイスの MTU 値を **mtu** コマンドで変更すると、**ipmtu** コマンドの値に影響することがあります。**ipmtu** コマンドには、**mtu** コマンドに指定する値より大きい値は指定できません。**mtu** コマンドの値を変更し、**ipmtu** 値が新しい **mtu** 値を超えた場合、**ipmtu** の値は自動的に新しく **mtu** コマンドで設定した値に変わります。**ipmtu** コマンドの値を変更しても、**mtu** コマンドの値には影響しません。
- プロキシの Link Control Protocol（LCP）が実行されている場合、MRU オプションが LCP ネゴシエーション中にセットされるため、LCP の再ネゴシエーションを行う必要があります。LCP の再ネゴシエーションを強制するには、VPDN グループの **lcprenegotiation** コマンドを設定します。
- MRU アドバタイジングへの対応、非対応が混在するデバイスと通信するトンネル サーバで MTU を手動で低く設定すると、非対応のデバイスで PMTUD の問題が生じることがあります。この問題についての説明は「VPDN に対するパス MTU ディスカバリの有効化」セクションにあります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacevirtual-template***number*
4. **mtu***bytes*
5. **exit**
6. **vpdn-group***name*
7. **lcprenegotiation** {**always** |**on-mismatch**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfacevirtual-template***number* 例： `Router(config)# interface virtual-template 1`	仮想アクセス インターフェイスの作成でダイナミックに設定して適用できる仮想テンプレート インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**mtu***bytes* 例： `Router(config-if)# mtu 1460`	最大パケット サイズまたは MTU サイズを調整します。 （注） レイヤ 2 ヘッダーは 40 バイトであるため、*bytes* 引数の推奨値は 1460 です。
ステップ 5	**exit** 例： `Router(config-if)# exit`	（オプション）インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	（オプション）VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 7	**lcprenegotiation {always | on-mismatch}** 例： `Router(config-vpdn)# lcp renegotiation always`	（オプション）ダイヤルイン通話でトンネル サーバが PPP LCP を再ネゴシエートするようにします。

VPDN グループ選択の設定

ホスト名に基づく VPDN グループ選択の設定

LNS のステータスを表示し、LNS が有効か確認するには、次の手順を使用します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **accept-dialin**
5. **protocoll2tp**
6. **terminate-fromhostname***hostname*
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**accept-dialin** 例： `Router(config-vpdn)# accept-dialin`	ネットワーク アクセス サーバ（NAS）からの要求を受け付けてダイヤルインのコールをトンネリングようにトンネル サーバを設定する VPDN accept dialin グループを作成し、accept-dialin VPDN サブグループ設定モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**protocoll2tp** 例： `Router(config-vpdn-acc-in)# protocol l2tp`	VPDN サブグループが使用するトンネリング プロトコルを指定します。
ステップ 6	**terminate-fromhostname***hostname* 例： `Router(config-vpdn-acc-in)# terminate-from hostname example`	VPDN トンネルの受け入れ時に必要なリモート LAC または LNS のホスト名を指定します。
ステップ 7	**exit** 例： `Router(config-vpdn-acc-in)# exit`	VPDN accept dialin グループ コンフィギュレーション モードを終了します。

送信元 IP アドレスに基づく VPDN グループ選択の設定

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **accept-dialin**
5. **protocoll2tp**
6. **source-ip***ip-address*
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**accept-dialin** 例： `Router(config-vpdn)# accept dialin`	ネットワーク アクセス サーバ（NAS）からの要求を受け付けてダイヤルインのコールをトンネリングようにトンネル サーバを設定する VPDN accept dialin グループを作成し、accept-dialin VPDN サブグループ設定モードを開始します。
ステップ 5	**protocoll2tp** 例： `Router(config-vpdn-acc-in)# protocol l2tp`	VPDN サブグループが使用するトンネリング プロトコルを指定します。
ステップ 6	**source-ip***ip-address* 例： `Router(config-vpdn-acc-in)# source-ip 10.10.10.1`	加入者トラフィックの宛先 IP アドレスにマップされている送信元 IP アドレスを指定します。
ステップ 7	**exit** 例： `Router(config-vpdn-acc-in)# exit`	VPDN accept dialin グループ コンフィギュレーション モードを終了します。

VRF に基づく VPDN グループ選択の設定

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **accept-dialin**
5. **protocoll2tp**
6. **vpnvrf***vrf-name*
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**accept-dialin** 例： `Router(config-vpdn)# accept dialin`	ネットワーク アクセス サーバ（NAS）からの要求を受け付けてダイヤル インのコールをトンネリングようにトンネル サーバを設定する VPDN accept dialin グループを作成し、accept-dialin VPDN サブグループ設定モードを開始します。
ステップ 5	**protocoll2tp** 例： `Router(config-vpdn-acc-in)# protocol l2tp`	VPDN サブグループが使用するトンネリング プロトコルを指定します。

	コマンドまたはアクション	目的
ステップ 6	**vpnvrf***vrf-name* 例： `Router(config-vpdn-acc-in)# vpn vrf myvrf`	VPDN グループの送信元と宛先の IP アドレスが、指定したバーチャル プライベート ネットワーク（VPN）のルーティングと VRF インスタンスに属するように指定します。 • **vrf***vrf-name*：VRF 名により VRF インスタンスを指定します。
ステップ 7	**exit** 例： `Router(config)# exit`	accept dialin VPDN サブグループモードを終了します。

VPDN グループ選択の表示

手順の概要

1. **enable**
2. **showvpdngroup-select**
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showvpdngroup-select** 例： `Router> show vpdn group-select`	選択した VPDN グループに関する情報を表示します。
ステップ 3	**exit** 例： `Router> exit`	グローバル コンフィギュレーション モードを終了します。

VPDN に対する QoS パケット分類の設定

VPDN 導入によっては、デフォルト設定を使用する代わりに、IP ヘッダーからレイヤ 2 ヘッダーに ToS バイトの内容をコピーして、QoS をエンドツーエンドで維持するように VPDN ネットワークを設定でき、また VPDN ネットワークにカスタムのパケット分類を手動で設定することもできます。

QoS の設定は、通常トンネル サーバ、大量の発信トラフィックを管理して優先順位を付ける必要があるデバイス上でのみ必要になります。

エンドツーエンドの QoS を維持する場合は、次のタスクを実行します。

VPDN 導入にカスタムのパケット分類を手動で設定するには、次の各タスクのいずれかまたは両方を実行します。

ToS バイトの QoS 分類の維持の設定

レイヤ 2 パケットを作成すると、ToS バイト値はデフォルトでゼロに設定され、通常のサービスを示します。この設定は、トンネリングされるカプセル化された IP パケットの ToS バイトの値を無視します。トンネル サーバはレイヤ 2 ヘッダーの ToS バイトに内部 IP パケットの ToS フィールドの内容をコピーするように設定できます。IP ヘッダーからレイヤ 2 ヘッダーへ ToS をコピーすると、トンネル パケットのエンドツーエンドの QoS フィールドが保持されます。

IP パケットの ToS バイトをレイヤ 2 ヘッダにコピーするようにトンネル サーバを設定するには、次の作業を実行します。

はじめる前に

VPDN 配置を構成する必要があります。

（注）

- ToS フィールドを維持するには、トンネリングされたリンクは IP パケットを伝送する必要があります。
- プロキシ PPP ダイヤルインはサポートされていません。
- ToS フィールドを維持するには、トンネリングされたリンクは IP を伝送する必要があります。マルチリンク PPP（MLP）接続のカプセル化されたペイロードは IP ではないため、この作業はトンネルを通過する MLP に影響しません。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **iptosreflect**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**iptosreflect** 例： `Router(config-vpdn)# ip tos reflect`	IP パケットの ToS バイトをレイヤ 2 ヘッダにコピーするように VPDN グループを設定します。

VPDN 用の IP プレシデンスの手動設定

ToS バイトの IP プレシデンス ビットは、レイヤ 2 パケットに CoS をセットするために手動で設定できます。レイヤ 2 パケットの特定の IP プレシデンスの値を手動で設定する場合、QoS はトンネルを通じてエンドツーエンドには保持されません。

レイヤ 2 パケットの CoS を手動で設定するには、トンネル サーバで次の作業を実行します。

はじめる前に

VPDN 配置を構成する必要があります。

（注） マニュアル構築による IP プレシデンスの値は **ip tos reflect** コマンドによって設定された値に優先します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **ipprecedence**[*number* | *name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**ipprecedence**[*number*	*name*] 例： `Router(config-vpdn)# ip precedence 1`	VPDN レイヤ 2 カプセル化ヘッダーに優先順位を設定します。

VPDN セッション用の ToS の手動設定

パケットの ToS をマークするため、ToS ビットを手動で設定できます。レイヤ 2 パケットに対して、特定の ToS 値を手動で設定する場合、QoS はトンネル全体のエンドツーエンドを保持しません。

レイヤ 2 パケットの CoS を手動で設定するには、トンネル サーバで次の作業を実行します。

はじめる前に

VPDN 配置を構成する必要があります。

（注） マニュアル構築による ToS の値は **ip tos reflect** コマンドによって設定された値に優先します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **iptos**{*tos-bit-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**iptos**{*tos-bit-value*	**max-reliability**	**max-throughput**	**min-delay**	**min-monetary-cost**	**normal**} 例： `Router(config-vpdn)# ip tos 9`	VPDN レイヤ 2 カプセル化ヘッダーに ToS ビットを設定します。

VPDN の追加機能の設定例

例：グローバル VPDN テンプレートの設定

次の例では、名前のないグローバル VPDN テンプレートの、2 つの VPDN パラメータを設定します。

```
vpdn-template
 local name host43
 ip tos reflect
```

例：名前付き VPDN テンプレートの設定

次の例では、l2tp という名前の VPDN テンプレートの、2 つの VPDN パラメータを設定します。名前付きの VPDN テンプレートは l2tp_tunnels という名前の VPDN グループと関連付けられます。

```
vpdn-template l2tp
 l2tp tunnel busy timeout 65
 l2tp tunnel password tunnel4me
!
vpdn-group l2tp_tunnels
 source vpdn-template l2tp_tunnels
```

例：VPDN テンプレートからの VPDN グループの関連付けの解除

次の例では、VPDN テンプレートから l2tp という名前の VPDN グループの関連付けを解除します。システムのデフォルト設定は VPDN グループ設定で指定されていないすべての VPDN パラメータに使用されます。

```
vpdn-group l2tp
 no source vpdn-template
```

例：グローバル VPDN 送信元 IPアドレスの設定

次の例では、グローバル送信元 IP アドレスを設定しています。この送信元 IP アドレスは、特定の送信元 IP アドレスが VPDN グループ用に設定されていない限り、ルータで確立されたすべてのトンネルに対し用いられます。

```
vpdn source-ip 10.1.1.1
```

例：VPDN グループの送信元 IP アドレスの設定

以下は、tunneling という名前の VPDN グループに関連付けられたトンネルに対し、送信元 IP アドレスを設定する例を示します。この送信元 IP アドレスは、この VPDN グループに関連付けられたトンネルに対し、任意のグローバル設定された送信元 IP アドレスをオーバーライドします。

```
vpdn-group tunneling
 source-ip 10.1.1.2
```

例：VRF 認識型 VPDN トンネルのローカル設定

次に、NAS が VRF 内のリモート トンネル サーバに接続するようにマルチホップ トンネル スイッチを設定する例を示します。

NAS

```
interface loopback 0
 ip address 172.16.45.6 255.255.255.255
!
vpdn enable
vpdn-group group1
 request-dialin
 protocol l2tp
 domain cisco.com
!
 initiate-to 10.10.104.9
 local name nas32
 source-ip 172.16.45.6
 l2tp tunnel password secret1
```

マルチホップ トンネル スイッチ

```
ip vrf cisco-vrf
 vpn id A1:3F6C
!
interface loopback 0
 ip address 10.10.104.22 255.255.255.255
!
interface loopback 40
 ip vrf forwarding cisco-vrf
 ip address 172.16.40.241 255.255.255.255
!
vpdn enable
vpdn multihop
!
vpdn-group mhopin
 accept-dialin
 protocol l2tp
 virtual-template 4
!
 terminate-from hostname nas32
 source-ip 10.10.104.9
 l2tp tunnel password secret1
!
vpdn-group mhopout
 request-dialin
 protocol l2tp
 domain cisco.com
!
```

```
 vpn vrf cisco-vrf
 initiate-to ip 172.16.45.6
 source-ip 172.16.40.241
 local name multihop-tsw25
 l2tp tunnel password secret2
```

トンネル サーバ

```
interface loopback 0
 ip address 172.16.45.6 255.255.255.255
!
vpdn enable
vpdn-group cisco
 accept-dialin
 protocol l2tp
 virtual-template 1
!
 terminate-from hostname multihop-tsw25
 source-ip 172.16.45.6
 local name ts-12
 l2tp tunnel password secret2
```

例：リモート RADIUS AAA サーバでの VRF 認識型 VPDN トンネルの設定

次の例では、サービス プロバイダー ネットワーク向けの VRF 認識型 VPDN トンネルを設定します。AAA RADIUS サーバのユーザ プロファイルは、VPDN トンネル属性を定義し、これは複数の NAS またはトンネルスイッチに伝播します。

RADIUS ユーザ プロファイル：VRF 名

次の例では、送信元と宛先の IP アドレスが vpn-first という名前の VPN に属するように指定します。

```
cisco.com Password = "secret"
      Service-Type = Outbound-User,
      cisco-avpair = "vpdn:tunnel-id=LAC",
      cisco-avpair = "vpdn:tunnel-type=l2tp",
      cisco-avpair = "vpdn:ip-addresses=10.0.0.1",
      cisco-avpair = "vpdn:source-ip=10.0.0.9",
      cisco-avpair = "vpdn:vpn-vrf=vpn-first"
      cisco-avpair = "vpdn:l2tp-tunnel-password=supersecret"
```

RADIUS ユーザ プロファイル：VRF ID

次の例では、送信元と宛先の IP アドレスが A1:3F6C の ID を持つ VPN に属するように指定します。

```
cisco.com Password = "secret"
      Service-Type = Outbound-User,
      cisco-avpair = "vpdn:tunnel-id=LAC",
      cisco-avpair = "vpdn:tunnel-type=l2tp",
      cisco-avpair = "vpdn:ip-addresses=10.0.0.1",
      cisco-avpair = "vpdn:source-ip=10.0.0.9",
      cisco-avpair = "vpdn:vpn-id=A1:3F6C"
      cisco-avpair = "vpdn:l2tp-tunnel-password=supersecret"
```

例：VPDN 配置のための IP MTU の手動設定

次の例は、1 という名前の virtual-template を使用するすべてのトンネルへ対する 1460 バイトの IP MTU を手動で設定しています。

```
interface virtual-template 1
 ip mtu 1460
```

例：VPDN 配置での IP MTU の自動調整の有効化

次の例では、デバイスの出力インターフェイスの MTU に基づいて自動的に IP MTU を調整するために、tunneler という名前の VPDN グループに関連付けられたトンネルを設定しています。

```
vpdn-group tunneler
 ip mtu adjust
```

例：アドバタイズされた TCP MSS の手動設定

次の例は、2 という名前の virtual-template を使用するすべてのトンネルに対する 1420 バイトの TCP MSS を手動で設定しています。

```
interface virtual-template 2
 ip tcp adjust-mss 1420
```

例：MRU のアドバタイズの設定

次の例では、3 とい名前の仮想テンプレートを使用するすべてのトンネルで 1460 バイトの MTU を手動で設定します。mytunnels という名前の VPDN グループは LCP プロキシを使用するため、LCP の再ネゴシエーションを実行するように設定されます。

```
interface virtual-template 3
 mtu 1460
!
vpdn-group mytunnels
 lcp renegotiation always
```

例：ToS バイトの QoS 分類保護の設定

次の例は、out1 という名前の既存の VPDN グループへの IP ToS フィールドの保護設定を示します。

```
vpdn-group out1
 ip tos reflect
```

例：VPDN 用の IP プレシデンスの手動設定

次の例は、out2 という名前の既存の VPDN グループに対し IP プレシデンス値を手動で設定しています。

```
vpdn-group out2
 ip precedence priority
```

例：VPDN セッションの ToS の手動設定

次の例は、手動で out3 という名前の既存の VPDN グループで ToS の分類を設定しています。

```
vpdn-group out3
 ip tos 9
```

VPDN グループ選択の設定例

例：ホスト名に基づく VPDN グループ選択の設定

次に、LAC-1 が LNS への VPDN トンネルを構築し、LNS が vpdn-group 1 でのセッションを終了する設定の例を示します。

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# terminate-from hostname LAC-1
```

例：IP アドレスに基づく VPDN グループ選択の設定

次の例は、IP アドレス 10.10.10.1 に VPDN トンネルを構築する LAC-1/LAC-2 と、vpdn group 1 のセッションを終了する LNS を示します。LAC-1/LAC-2 が IP アドレス 10.10.10.2 に VPDN トンネルを構築する場合、LNS は vpdn group 2 のセッションを終了します。どの送信元 IP アドレスの一致であっても省略可能です。

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# source-ip 10.10.10.1
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# exit
Router(config)# vpdn-group 2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# source-ip 10.10.10.2
```

例：VRF に基づく VPDN グループ選択の設定

次の例は、service-A で SCCRQ を送信する LAC と vpdn-group 1 のトンネルを終端する LNS の設定例を示します。LAC が service-B で SCCRQ を送信するとき、LNS は vpdn-group 2 のトンネルを終端します。

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-A
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# vpdn-group 2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-B
```

例：ホスト名と IP アドレスに基づく VPDN グループ選択の設定

次の例は、IP アドレス 10.10.10.1 に VPDN トンネルを構築する LAC-1 と、vpdn group 1 でのセッションを終了する LNS を示します。LAC-1 が IP アドレス 10.10.10.2 に VPDN トンネルを構築する場合、LNS は vpdn group 2 でのセッションを終了します。LAC-2 が IP アドレス 10.10.10.1 または 10.10.10.2 に VPDN トンネルを構築する場合、LNS は vpdn group 3 でのセッションを終了します。

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# terminate-from hostname LAC-1
Router(config-vpdn-acc-in)# source-ip 10.10.10.1
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# vpdn-group 2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# terminate-from hostname LAC-1
Router(config-vpdn-acc-in)# source-ip 10.10.10.2
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# vpdn-group 3
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# terminate-from hostname LAC-2
Router(config-vpdn-acc-in)# source-ip 10.10.10.1
Router(config-vpdn-acc-in)# exit
```

例：ホスト名と VRF に基づいた VPDN グループ選択の設定

以下は、任意の宛先 IP アドレスを持つ vrf service-A の SCCRQ を送信する LAC-1 と vpdn group 1 の VPDN トンネルを終端する LNS の設定例を示します。LAC-1 が任意の宛先 IP アドレスを持つ vrf service-B の SCCRQ を送信すると、LNS は vpdn group 2 の VPDN トンネルを終端します。LAC-2

が任意の宛先 IP アドレスを持つ vrf service-B の SCCRQ を送信すると、LNS は vpdn group 3 の VPDN トンネルを終端します。

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-A
Router(config-vpdn-acc-in)# terminate-from hostname LAC-1
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# vpdn-group 2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-B
Router(config-vpdn-acc-in)# terminate-from hostname LAC-1
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# vpdn-group 3
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-B
Router(config-vpdn-acc-in)# terminate-from hostname LAC-2
Router(config-vpdn-acc-in)# exit
```

例：IP アドレスおよび VRF に基づいた VPDN グループ選択の設定

次の設定例は、LAC-1/LAC-2 が vrf service-A 上の SCCRQ を宛先 IP アドレス 10.10.10.1 に送り、LNS は vpdn-group 1 上の VPDN トンネルを終了させます。LAC-1/LAC-2 が vrf service-A 上の SCCRQ を宛先 IP アドレス 10.10.10.2 に送る場合、LNS は vpdn-group 2 上の VPDN トンネルを終了させます。

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-A
Router(config-vpdn-acc-in)# source-ip 10.10.10.1
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# exit
Router(config)# vpdn-group 2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-A
Router(config-vpdn-acc-in)# source-ip 10.10.10.2
Router(config-vpdn-acc-in)# exit
```

例：ホスト名 VRF と IP アドレスに基づく VPDN グループ選択の設定

次の設定例は、LAC-1 が vrf service-A 上の SCCRQ を宛先 IP アドレス 10.10.10.1 に送り、LNS は vpdn-group 1 上の VPDN トンネルを終了させます。LAC-1 が vrf service-B 上の SCCRQ を宛先 IP アドレス 10.10.10.1 に送る場合、LNS は vpdn-group 2 上の VPDN トンネルを終了させます。

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-A
```

```
Router(config-vpdn-acc-in)# terminate-from hostname LAC-1
Router(config-vpdn-acc-in)# source-ip 10.10.10.1
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# exit
Router(config)# vpdn-group 2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# vpn vrf service-B
Router(config-vpdn-acc-in)# terminate-from hostname LAC-1
Router(config-vpdn-acc-in)# source-ip 10.10.10.1
Router(config-vpdn-acc-in)# exit
```

例：VPDN グループ選択の表示

VPDN グループ選択機能により、送信元 IP アドレス、ホスト名、または VFR に基づいて VPDN グループ情報を表示することができます。

例の提示の目的で、次の設定が例の表示用に使用されます。

```
Router> enable
Router# configure terminal
Router(config)# vpdn-group vgdefault
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 20
Router(config-vpdn-acc-in)# local name lns
Router(config-vpdn)# l2tp tunnel password 0 example
Router(config-vpdn)# exit
Router(config)# vpdn-group vg-ip2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# source-ip 10.1.1.2
Router(config-vpdn)# local name lns
Router(config-vpdn)# l2tp tunnel password 0 example
Router(config-vpdn)# exit
Router(config)# vpdn-group vg-ip3
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# source-ip 10.1.1.3
Router(config-vpdn)# local name lns
Router(config-vpdn)# l2tp tunnel password 0
 example

Router(config-vpdn)# exit
Router(config)# vpdn-group vg-lts
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in) # protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# terminate host lts
Router(config-vpdn)# local name lns
Router(config-vpdn)# l2tp tunnel password 0 example
Router(config-vpdn)# exit
Router(config)# vpdn-group vg-lts1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# terminate host lts1
Router(config-vpdn)# local name lns
Router(config-vpdn)# l2tp tunnel password 0 example
Router(config-vpdn)# exit
Router(config)# vpdn-group vg-lts1-ip2
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
```

```
Router(config-vpdn-acc-in)# terminate host lts1
Router(config-vpdn)# source-ip 10.1.1.2
Router(config-vpdn)# local name lns
Router(config-vpdn)# l2tp tunnel password 0 example
Router(config-vpdn)# exit
Router(config)# end
```

例：VPDN グループ選択の概要の表示

次の例では、設定例に対する VPDN グループ選択の情報を示します。

```
Router# show vpdn group-select summary
VPDN Group     Vrf    Remote Name     Source-IP     Protocol     Direction
vg-ip2            10.1.1.2     l2tp     accept-dialin
vg-ip3            10.1.1.3     l2tp     accept-dialin
vg-lts        lts     0.0.0.0     l2tp     accept-dialin
vg-lts1        lts1    0.0.0.0     l2tp     accept-dialin
vg-lts1-ip2     vfr101   lts1     10.1.1.2     l2tp     accept-dialin
vgdefault             0.0.0.0     l2tp     accept-dialin
```

次に、lac-1 という名前で IP アドレスが 10.0.0.1 のホストに対しての **showvpdngroup-selectkeys** コマンドのサンプル出力を示します。

```
Router# show vpdn group-select keys vrf vrf-blue hostname lac-1 source-ip 10.0.0.1
VPDN Group       Vrf        Hostname   Source Ip
vg1              vrf-blue   lac-1      10.0.0.1
```

次に、設定例に対しての **showvpdngroup-selectdefault** コマンドの出力例を示します。

```
Router# show vpdn group-select default
Default VPDN Group       Protocol
vgdefault       l2tp
None       pptp
```

次に、lac-5 という名前で IP アドレスが 10.1.1.0、そして VRF 名が vrf-red であるホストに対しての **showvpdngroup-selectkeys** コマンドのサンプル出力を示します。

```
Router# show vpdn group-select keys vrf vrf-red hostname lac-5 source-ip 10.1.1.0
VPDN Group    Vrf        Hostname    Source Ip
Vg2           vrf-red    lac-5         10.1.1.0
```

次の作業

「VPDN トンネル管理」モジュールでの関連するオプションのタスクを実行できます。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
VPDN 技術の概要	『*VPDN Technology Overview*』

関連項目	マニュアル タイトル
VPDN コマンド：完全なコマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS VPDN Command Reference*』
ダイヤル テクノロジー コマンド：完全なコマンド構文、コマンドモード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS Dial Technologies Command Reference*』
セキュリティ コマンド：コマンド構文の詳細、コマンドモード、デフォルト、使用上の注意事項、および例	『*Cisco IOS Security Command Reference*』
QoS 分類について	「分類の概要」のモジュール
QoS コマンド：完全なコマンド構文、コマンドモード、デフォルト、使用上の注意事項、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
L2TP トンネリング導入の MTU チューニングの情報	『MTU Tuning for L2TP』
IP パケットのフラグメンテーションと PMTUD の情報	『IP Fragmentation and PMTUD』
スループットの低下する DoS 攻撃の情報	『Crafted ICMP Messages Can Cause Denial of Service』

標準

規格	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1191	『*Path MTU Discovery*』
RFC 2661	『レイヤ *2* トンネリング プロトコル（*L2TP*）』
RFC 2923	『*TCP Problems with Path MTU Discovery*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VPDN 追加機能の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *12* : ***VPDN*** 追加機能の設定の機能情報

機能名	ソフトウェア リリース	機能の設定情報
VPDN デフォルト グループ テンプレート	Cisco IOS XE リリース 2.1	この機能により、VPDNテンプレートの VPDN グループ パラメータ用にグローバルなデフォルト値を設定できるようになりました。これらのグローバル デフォルト値は、特定の値が個々の VPDN グループ用に設定されていない限り、すべての VPDN グループに適用されます。 この機能により次のコマンドが導入されました。**sourcevpdn-template**、**vpdn-template**。
VPDN グループ選択	Cisco IOS XE リリース 2.1	この機能は、LAC と LNS 間で異なる VPDN グループ設定をもつ、カスタマイズされた複数の VPDN トンネルを設定します。 この機能により次のコマンドが導入されました。**showvpdngroup-select**、**showvpdngroup-selectkeys**。
PPP 経由の VPN ルーティング転送（VRF）フレームルート（プール）割り当て	Cisco IOS XE リリース 2.1	この機能は次の RADIUS 属性を VRF 認識型にするのをサポートします。対象は属性 22（Framed-Route）、属性 8 フレーム（Framed-IP-Address）と属性 9（Framed-IP-Netmask）の組み合わせで、および Cisco VSA ルートコマンドです。そのため、スタティック IP ルートは、グローバル ルーティング テーブルではなく特定 VRF ルーティング テーブルに適用できます。

機能名	ソフトウェア リリース	機能の設定情報
VRF 認識型 VPDN トンネル	Cisco IOS XE リリース 2.2	この機能は、VPDN トンネルを MPLS VPN 外部で開始し、MPLS VPN の内部で終端することを可能にすることで、VPDN トンネルのサポートを強化します。 この機能により、次のコマンドが導入されました。**vpn**。

第 7 章

VPDN トンネル管理

このモジュールには、バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）トンネルの管理、および VPDN のイベントのモニタリングに関する情報が含まれています。このモジュールで説明されているタスクは VPDN 配置の設定後のみ実行する必要があります。

- 機能情報の確認，193 ページ
- VPDN トンネル管理の前提条件，194 ページ
- VPDN トンネル管理の制約事項，194 ページ
- VPDN トンネル管理に関する情報，194 ページ
- VPDN トンネルの管理方法，196 ページ
- VPDN トンネル管理の設定例，213 ページ
- その他の参考資料，218 ページ
- VPDN トンネル管理の機能情報，219 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

VPDN トンネル管理の前提条件

このモジュールで次のタスクを実行する前に、VPDN の導入を設定する必要があります。VPDN の導入の概要については、「VPDN 技術の概要」のモジュールを参照してください。

VPDN トンネル管理の制約事項

レイヤ2フォワーディング（L2F）プロトコルまたはポイントツーポイントトンネリングプロトコル（PPTP）を使用した VPDN トンネルはサポートされません。

VPDN トンネル管理に関する情報

VPDN トンネルの終了

VPDN トンネルは、手動またはソフト シャットダウンにより終了できます。VPDN トンネルを手動終了すると指定された VPDN トンネルとトンネル内のすべてのセッションの即時のシャットダウンが起き、VPDN サービスが突然中断することになります。ルータのソフト シャットダウンを有効にすると、ルータで終端するすべての VPDN トンネルでの新しい VPDN セッションの確立を防ぐ一方、既存のセッションに影響は与えません。ソフト シャットダウンを有効にして VPDN トンネルを終了すると、VPDN トンネルが手動で終了されたときに発生する確立されたセッションの中断を回避できます。

VPDN セッション制限

ルータで確立される同時 VPDN セッションの数は手動で設定できるため、ネットワーク管理者によるネットワークへのコントロールの幅が広がります。VPDN セッション制限はパフォーマンスを向上させ、大容量で動作するルータの遅延を低減できます。

VPDNセッションの最大数はグローバルに設定でき、VPDNグループのレベルまたは特定のVPDNテンプレートに関連付けられた VPDN グループ全てに設定を行うことができます。

VPDN セッション制限のアプリケーションの階層を次に示します。

- グローバルに設定されたセッションの上限は、VPDN グループに対してまたはVPDNテンプレートで設定されているセッション制限よりも優先されます。ルータでのセッションの合計数は、グローバル セッション制限での設定を超えることはできません。
- VPDNテンプレートに設定されたセッションの上限は、そのVPDNテンプレートに関連付けられたすべての VPDN グループに適用されます。 関連付けられたすべての VPDN グループに対するセッションの合計数は、設定されたVPDNテンプレートのセッション制限を超えることはできません。

- VPDN グループ用に設定されたセッションの制限は、VPDN グループ適用されます。

VPDN トンネルに対する制御パケットのパラメータ

特定の制御パケット タイマー、再試行カウンタ、およびアドバタイズされた制御パケットの受信ウィンドウ サイズを、レイヤ2 トランスポート プロトコル（L2TP）またはレイヤ2 フォワーディング（L2F）の VPDN トンネルに対して設定することができます。これらのパラメータを調整することによって、VPDN 導入の特定のニーズに合わせるために、ルータのパフォーマンスを微調整することが可能になります。

L2TP 輻輳回避

L2TP の輻輳回避には、RFC 2661 で説明されている L2TP 制御メッセージのスロットリングによる、パケットのフロー制御と輻輳回避が備わっています。L2TP の制御メッセージ パケットのスロットリングによって、セッションのドロップが発生する可能性のある、ピアのトンネル エンドポイント上での入力バッファのオーバーフローが防止されます。

L2TP の輻輳回避が導入される前は、ネットワーク アクセス サーバ（NAS）とトンネル サーバ間でのパケットの送信に使用されるウィンドウ サイズが、ピアのエンドポイントからアドバタイズされた値に設定され、変更されることはありませんでした。L2TP の輻輳回避を設定すれば、L2TP のパケット ウィンドウは、スライディング ウィンドウ メカニズムを使用して動的にサイズを変更できます。ウィンドウ サイズは、パケットが正常に配信されている場合は大きくなり、ドロップされたパケットを再送信する必要がある場合は小さくなります。

L2TP の輻輳回避は、いずれかのトンネル エンドポイントから発信されるコールの割合が比較的高いネットワークにおいて役立ちます。L2TP の輻輳回避は、多数の同時セッションに対応する拡張性の高いプラットフォームにも役立ちます。

L2TP 輻輳回避の仕組み

TCP/IP および RFC 2661 では、NAS とトンネル サーバ間の制御メッセージ トラフィックをスロットルするために使用される、スロー スタートと輻輳回避という 2 つのアルゴリズムが定義されています。スロー スタートと輻輳回避は、輻輳を制御するために連携して動作する 2 つの独立したアルゴリズムです。スロースタートと輻輳回避では、スロースタートしきい値（SSTHRESH）サイズと輻輳ウィンドウ（CWND）サイズという 2 つの変数が接続ごとの送信側デバイスによって維持される必要があります。

輻輳ウィンドウでは、送信側がそのピアからの確認応答を待機しなければならない間に送信できるパケット数を定義します。輻輳ウィンドウのサイズは増えたり減ったりしますが、ピア デバイスのアドバタイズされた受信ウィンドウのサイズを超えることはできません。

スロー スタートしきい値では、送信側デバイスがスロー スタート モードから輻輳回避モードに動作を切り替えるタイミングを定義します。輻輳ウィンドウサイズがスロースタートしきい値よりも小さい場合、デバイスはスロー スタート モードで動作します。輻輳ウィンドウ サイズがスロー スタートしきい値と等しい場合、デバイスは輻輳回避モードに切り替わります。

新しい接続が確立されると、送信側デバイスは最初にスロースタートモードで動作します。輻輳ウィンドウ サイズが 1 つのパケットに初期化され、スロー スタートしきい値がピアのトンネル エンドポイント（受信側）からアドバタイズされた受信ウィンドウ サイズに設定されます。

送信側デバイスが1つのパケットを送信して、確認応答されるまで待機することで開始されます。確認応答が受信されると、輻輳ウィンドウ サイズは 1 から 2 に増やされ、2 つのパケットを送信可能になります。これら 2 つのパケットがそれぞれ確認応答されると、輻輳ウィンドウ サイズは 4 に増やされます。輻輳ウィンドウ サイズはラウンド トリップが完了するごとに 2 倍になり、サイズが指数関数的に増加していきます。

輻輳ウィンドウサイズがスロースタートしきい値に達すると、送信側デバイスは輻輳回避モードで動作するように切り替わります。輻輳回避モードでは、輻輳ウィンドウ サイズの増加の割合を低下させます。輻輳回避モードでは、確認応答が受信されるごとに、1 を輻輳ウィンドウ サイズで除算した割合で輻輳ウィンドウサイズを増やします。これによって、輻輳ウィンドウサイズの増加は指数関数的ではなく、線形になります。

ある時点で、ピア デバイスの容量を超えて、パケットがドロップします。これは、送信側デバイスに輻輳ウィンドウ サイズが大きくなりすぎたことを示します。再送信イベントが検出されると、スロースタートしきい値は現在の輻輳ウィンドウサイズの半分にリセットされ、輻輳ウィンドウ サイズは 1 にリセットされ、またデバイスは動作をスロー スタート モードに切り替えます（そのデバイスがこのモードでまだ動作していなかった場合）。

VPDN イベント ロギング

使用可能な VPDN のイベント ロギングには 2 種類あります。VPDN の障害イベント ロギングと、一般的な VPDN のイベントロギングです。VPDN 障害イベント ロギングはデフォルトで有効になっています。一般的な VPDN のイベント ロギングはデフォルトで無効になっているため、一般的なイベント メッセージを参照するには、明示的に有効にする必要があります。

VPDN トンネルの管理方法

VPDN トンネルの手動での終了

VPDN トンネルを手動終了すると指定された VPDN トンネルとトンネル内のすべてのセッションの即時のシャットダウンが起き、VPDN サービスが突然中断することになります。手動で VPDN トンネルを終了する前に、「VPDN トンネルのソフト シャットダウンの有効化, （197 ページ）」のタスクを実行することを検討してください。

手動で終了した VPDN トンネルは、ユーザのログインと共に即時に再開できます。VPDN イベント ロギングを有効にしたまま、手動で VPDN トンネルを終了して再起動することで、VPDN セッション確立に関する有用なトラブルシューティング情報を取得できます。

手動で特定の VPDN トンネルをシャットダウンし、その結果トンネルとそのセッションすべてを終了するには、次の作業を実行します。この作業は、次のデバイスでも実行できます。

- トンネル サーバ
- トンネル エンドポイントとして機能している NAS

（注）
- クライアントが開始した L2TP トンネルでは、この作業はトンネル サーバにだけ実行できます。
- L2F プロトコルと PPTP を使用したトンネルはサポートされません。

手順の概要

1. **enable**
2. **clearvpdntunnel2tp** {**all** | **hostname** *remote-name* [*local-name*] | **id** *local-id* | **ip** *local-ip-address* | **ip** *remote-ip-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clearvpdntunnel2tp** {**all**	**hostname** *remote-name* [*local-name*]	**id** *local-id*	**ip** *local-ip-address*	**ip** *remote-ip-address*} 例： `Router# clear vpdn tunnel l2tp all`	指定されたトンネルとトンネル内のすべてのセッションをシャットダウンします。

VPDN トンネルのソフト シャットダウンの有効化

ルータの VPDN トンネルのソフト シャットダウンを有効にすると、既存のセッションに影響せずに、そのルータで終端するすべての VPDN トンネルで新しい VPDN セッションの確立を防止できます。ソフト シャットダウンを有効にして VPDN トンネルを終了すると、VPDN トンネルが手動で終了されたときに発生する確立されたセッションの中断を回避できます。ルータまたはアクセス サーバのソフト シャットダウンを有効にすると、そのデバイスで終端するすべてのトンネルに影響します。特定のトンネルに限ってソフト シャットダウンを有効にする方法はありません。他のトンネルに影響を与えることなくデバイスの特定のトンネルをシャットダウンするには、この方法に代わり「VPDN トンネルの手動での終了，（196 ページ）」を参照してください。

NASでソフトシャットダウンを実行すると、認証待ちのセッションを単に拒否するのではなく、認証が行われます。認証が行われることで、アカウンティング記録が性格に維持されます。

トンネルサーバでソフト シャットダウンを実行すると、セッション拒否の理由が NAS に戻ります。この情報は、VPDN 障害履歴テーブルに記録されます。

（注） VPDN トンネルのソフト シャットダウンを有効にしても、マルチシャーシ マルチリンク PPP（MMP）トンネルの確立には影響しません。

既存のセッションのサービスを妨げることなく、ルータで終端する VPDN トンネルに新しいセッションが確立することを防止するには、次の作業を実行します。この作業は、次のデバイスでも実行できます。

- トンネル サーバ
- トンネル エンドポイントとして機能している NAS

（注）
- クライアントが開始した L2TP トンネルでは、この作業はトンネル サーバにだけ実行できます。
- VPDN トンネルのソフト シャットダウンを有効にしても、新しい MMP トンネルの確立は回避できません。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnsoftshut**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**vpdnsoftshut** 例： `Router(config)# vpdn softshut`	既存のセッションのサービスを妨げることなく、VPDN トンネルに新しいセッションが確立することを防止します。

VPDN トンネルのソフト シャットダウンの確認

ソフト シャットダウンが正しく動作していることを確認するには、次の作業を実行します。

手順の概要

1. 許可されたユーザ名とパスワードを使用して NAS にダイヤルし、VPDN セッションを確立します。
2. **enable**
3. **configureterminal**
4. **vpdnsoftshut**
5. **exit**
6. **showvpdn**
7. 許可された 2 つ目のユーザ名とパスワードを使用して NAS にダイヤルインし、VPDN セッションの確立を試行します。
8. **showvpdnhistoryfailure**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	許可されたユーザ名とパスワードを使用して NAS にダイヤルし、VPDN セッションを確立します。	
ステップ 2	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 3	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**vpdnsoftshut** 例： `Router(config)# vpdn softshut`	既存のセッションのサービスを妨げることなく、VPDN トンネルに新しいセッションが確立することを防止します。NAS サーバまたはトンネル サーバのいずれでもコマンドを実行することができます。
ステップ 5	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 6	**showvpdn** 例： `Router# show vpdn`	VPDN 内のアクティブな L2TP、L2F トンネルとメッセージ識別子に関する情報を表示します。元のセッションがアクティブになっていることを確認するには、このコマンドを使用します。
ステップ 7	許可された 2 つ目のユーザ名とパスワードを使用して NAS にダイヤル インし、VPDN セッションの確立を試行します。	ソフト シャットダウンが有効になっている場合、ソフトシャットダウンするルータのコンソールにシステム ログ（syslog）メッセージが表示されます。
ステップ 8	**showvpdnhistoryfailure** 例： `Router# show vpdn history failure`	障害履歴テーブルの内容を表示します。

許容される同時 VPDN セッション数の制限

ルータで確立される同時 VPDN セッションの数は手動で設定できるため、ネットワーク管理者によるネットワークへのコントロールの幅が広がります。VPDN セッション制限はパフォーマンスを向上させ、大容量で動作するルータの遅延を低減できます。

VPDN セッションの最大数はグローバルに設定でき、VPDN グループのレベルまたは特定の VPDN テンプレートに関連付けられた VPDN グループ全てに設定を行うことができます。

VPDN セッション制限のアプリケーションの階層を次に示します。

- グローバルに設定されたセッションの上限は、VPDN グループに対してまたは VPDN テンプレートで設定されているセッション制限よりも優先されます。ルータでのセッションの合計数は、グローバル セッション制限での設定を超えることはできません。
- VPDN テンプレートに設定されたセッションの上限は、その VPDN テンプレートに関連付けられたすべての VPDN グループに適用されます。関連付けられたすべての VPDN グループに

対するセッションの合計数は、設定されたVPDNテンプレートのセッション制限を超えることはできません。

- VPDN グループ用に設定されたセッションの制限は、VPDN グループ適用されます。

グローバル、テンプレートレベルでのインタラクションや、グループ レベルのVPDNセッション制限の例については、「例：VPDN セッション制限の設定」を参照してください。

次の任意のタスクのいずれかまたはすべてを実行するため、VPDNセッション制限を設定します。

NAS またはトンネル サーバで次のタスクを実行できます。

制限事項

クライアントの開始した L2TP トンネルについては、トンネルサーバ上でのみこれらのタスクを実行できます。

グローバル VPDN セッション制限の設定

ルータで許可する VPDN セッションの総数を制限するには、この作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnsession-limit***sessions*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnsession-limit***sessions* 例： `Router(config)# vpdn session-limit 6`	ルータでの同時 VPDN セッション数をグローバルに制限します。

VPDN テンプレートの VPDN セッション制限の設定

VPDN テンプレートにセッションの制限を設定するには、次の作業を実行します。VPDN テンプレートに結び付けられているすべての VPDN グループにセッション制限が適用されます。

はじめる前に

- VPDN テンプレートが設定されている必要があります。「VPDN 追加機能の設定」モジュールの「VPDN テンプレートの作成」のセクションを参照してください。
- 名前付き VPDN テンプレートを設定した場合、VPDN テンプレートには目的の VPDN グループを関連付ける必要があります。「VPDN 追加機能の設定」モジュールの「VPDN グループと VPDN テンプレートの関連付け」セクションを参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-template**[*name*]
4. **groupsession-limit***sessions*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-template**[*name*] 例： `Router(config)# vpdn-template l2tp`	VPDN テンプレートを作成し、VPDN テンプレート コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**groupsession-limit***sessions* 例： `Router(config-vpdn-templ)# group session-limit 6`	特定の VPDN テンプレートに関連付けられているすべての VPDN グループ全体で許可される同時セッションの最大数を指定します。

VPDN グループに対するセッション制限の設定

VPDN グループのレベルで VPDN セッションの数を制限するには、この作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **session-limit***number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group 1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**session-limit***number* 例： `Router(config-vpdn)# session-limit 2`	指定された VPDN グループに許可されるセッションの数を制限します。

VPDN セッション制限の確認

VPDN セッションが適切に制限されていることを確認するには、次の作業を実行します。

（注） Telnet セッションを使用して NAS に接続している場合は、EXEC セッションがロギングとデバッグ出力を NAS から確実に受信できるよう、**terminalmonitor** コマンドを有効にします。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnsession-limit***sessions*
4. 許可されたユーザ名とパスワードを使用して NAS にダイヤルし、VPDN セッションを確立します。
5. 許可された 2 つ目のユーザ名とパスワードを使用して NAS にダイヤルインし、VPDN セッションの確立を試行します。
6. **exit**
7. **showvpdnhistoryfailure**

手順の詳細

ステップ 1 **enable**
このコマンドを使用して、特権 EXEC モードを有効にします。プロンプトにパスワードを入力します。

例：

```
Router> enable
```

ステップ 2 **configureterminal**
グローバル コンフィギュレーション モードを開始します。

例：

```
Router# configure terminal
```

ステップ 3 **vpdnsession-limit***sessions*
ルータでの同時 VPDN セッション数を *sessions* 引数に指定した数に制限します。

NAS サーバまたはトンネル サーバのいずれの場合にもこのコマンドを実行します。

例：

```
Router(config)# vpdn session-limit 1
```

ステップ 4 許可されたユーザ名とパスワードを使用して NAS にダイヤルし、VPDN セッションを確立します。

ステップ 5 許可された 2 つ目のユーザ名とパスワードを使用して NAS にダイヤル インし、VPDN セッションの確立を試行します。
VPDN セッションの制限が適切に設定されていれば、このセッションは拒否され、次のような syslog メッセージがルータのコンソールに表示されます。

例：

```
00:11:17:%VPDN-6-MAX_SESS_EXCD:L2F HGW tunnelserver1 has exceeded configured local session-limit
and rejected user user2@cisco.com
```

ステップ 6 **exit**
特権 EXEC モードに戻ります。

ステップ 7 **showvpdnhistoryfailure**
障害履歴テーブルの内容を表示します。

例：

```
Router# show vpdn history failure
User:user2@scisco.com
 NAS:NAS1, IP address = 172.25.52.8, CLID = 2
 Gateway:tunnelserver1, IP address = 172.25.52.7, CLID = 13
 Log time:00:04:21, Error repeat count:1
 Failure type:Exceeded configured VPDN maximum session limit.
!This output shows that the configured session limit is being properly applied.
 Failure reason:
```

VPDN トンネルの L2TP 制御パケット パラメータの設定

L2TP VPDN トンネルの制御パケットタイマー、再試行カウンタ、アドバタイズされた制御パケットウィンドウ サイズを設定できます。これらのパラメータを調整することによって、VPDN 導入の特定のニーズに合わせるために、ルータのパフォーマンスを微調整することが可能になります。

導入されている VPDN の構成が L2TP トンネルを使用している場合に制御パケットのパラメータを設定するには、次のタスクを実行します。各パラメータの設定は省略可能です。パラメータが手動で設定されない限り、デフォルト値が使用されます。

この作業は、次のデバイスでも実行できます。

- トンネル サーバ
- トンネル エンドポイントとして機能している NAS

はじめる前に

l2tptunnelretransmitinitialtimeout コマンドまたは **l2tptunnelretransmitinitialretries** コマンドの設定が機能するには、ロード バランシングが有効になっている必要があります。

（注） クライアントが開始した L2TP トンネルでは、この作業はトンネル サーバにだけ実行できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***name*
4. **l2tptunnelhello***seconds*
5. **l2tptunnelreceivewindow***packets*
6. **l2tptunnelretransmitretries***number*
7. **l2tptunnelretransmittimeout** {**min** | **max**} *seconds*
8. **l2tptunneltimeoutno-session**{*seconds* | **never**}
9. **l2tptunneltimeoutsetup***seconds*
10. **l2tptunnelzlbdelay***seconds*
11. **l2tptunnelretransmitinitialtimeout** {**min** | **max**} *seconds*
12. **l2tptunnelretransmitinitialretries***number*
13. **l2tptunnelbusytimeout***seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***name* 例： `Router(config)# vpdn-group group1`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**l2tptunnelhello***seconds* 例： `Router(config-vpdn)# l2tp tunnel hello 90`	（オプション）L2TP トンネルへの hello キープアライブ パケットの送信間隔を秒数で設定します。 • *seconds*：NAS とトンネル サーバが次の L2TP トンネルキープアライブパケットを送信するまでに待機する時間（秒）。有効値の範囲は 0 ～ 1000 です。デフォルト値は 60 です。
ステップ 5	**l2tptunnelreceivewindow***packets* 例： `Router(config-vpdn)# l2tp tunnel receive window 500`	（オプション）L2TP 制御チャネルのローカル受信ウィンドウに許容されるパケットの数を設定します。 • *packets*：受信ウィンドウ内で許容されるパケットの最大数。有効値の範囲は 1 ～ 5000 です。デフォルト値は、プラットフォームによって異なります。
ステップ 6	**l2tptunnelretransmitretries***number* 例： `Router(config-vpdn)# l2tp tunnel retransmit retries 8`	（オプション）L2TP 制御パケットの再送信の試行回数を設定します。 • *number*：再送信試行回数。有効値の範囲は 5 ～ 1000 です。デフォルト値は 10 です。
ステップ 7	**l2tptunnelretransmittimeout** {**min** | **max**} *seconds* 例： `Router(config-vpdn)# l2tp tunnel retransmit timeout max 4`	（オプション）L2TP 制御パケットを再送信するまでにルータが待機する時間を設定します。 • **min**：制御パケットを再送信するまでにルータが待機する最短の時間を設定します。 • **max**：制御パケットを再送信するまでにルータが待機する最長の時間を設定します。 • *seconds*：制御パケットを再送信するまでにルータが待機するタイムアウトの長さを秒数で指定します。有効な値の範囲は 1 ～ 8 です。デフォルトの最小値は 1 です。デフォルトの最大値は 8 です。
ステップ 8	**l2tptunneltimeoutno-session** {*seconds* | **never**} 例： `Router(config-vpdn)# l2tp tunnel timeout no-session never`	（オプション）L2TP トンネルが空になってから切断するまでにルータが待機する時間を設定します。 • *seconds*：空の L2TP トンネルを切断するまでにルータが待機する時間を秒数で指定します。有効値の範囲は 0 ～ 86400 です。ルータが NAS として設定されている場合、デフォルトは 15 です。ルータがトンネル サーバとして設定されている場合、デフォルトは 10 です。 • **never**：ルータが空の L2TP トンネルを切断しないよう設定します。

	コマンドまたはアクション	目的
ステップ 9	**l2tptunneltimeoutsetup***seconds* 例： `Router(config-vpdn)# l2tp tunnel timeout setup 25`	（オプション）最初の L2TP 制御パケット送出後、ピアを通信中とみなすまでルータが確認メッセージを待機する時間を設定します。 • *seconds*：ルータが確認メッセージを待機する時間を秒数で指定します。有効値の範囲は 60 ～ 6000 です。デフォルト値は 10 です。
ステップ 10	**l2tptunnelzlbdelay***seconds* 例： `Router(config-vpdn)# l2tp tunnel zlb delay 2`	（オプション）Zero Length Bit(ZLB)制御メッセージの確認応答までに許容する遅延を設定します。 • *seconds*：ZLB 制御メッセージの確認応答までのルータの最大の遅延を秒数で指定します。有効値の範囲は 1 ～ 5 です。デフォルト値は 3 です。
ステップ 11	**l2tptunnelretransmitinitialtimeout** {**min** | **max**} *seconds* 例： `Router(config-vpdn)# l2tp tunnel retransmit initial timeout min 2`	（オプション）トンネル確立のために最初に送出するパケットを再送信するまでにルータが待機する時間を秒数で設定します。 • **min**：最初のパケットを再送信するまでにルータが待機する最短の時間を設定します。 • **max**：最初のパケットを再送信するまでにルータが待機する最長の時間を設定します。 • *seconds*：最初のパケットを再送信するまでにルータが待機するタイムアウトの長さを秒数で指定します。有効な値の範囲は 1 ～ 8 です。デフォルトの最小値は 1 です。デフォルトの最大値は 8 です。 （注） **l2tptunnelretransmitinitialtimeout** コマンドで設定する再試行カウンタが機能するには、ロード バランシングが有効になっている必要があります。
ステップ 12	**l2tptunnelretransmitinitialretries***number* 例： `Router(config-vpdn)# l2tp tunnel retransmit initial retries 5`	（オプション：Cisco IOS リリース 12.2(4) T、Cisco IOS リリース 12.2(28) SB と以降のリリース）：相手のルータを通信中とみなすまで、トンネル確立のための最初の制御パケットの送信をルータが試みる回数を設定します。 • *number*：再送信試行回数。有効な値の範囲は、1 ～ 1000 です。デフォルト値は 2 です。 （注） **l2tptunnelretransmitinitialretries** コマンドで設定する再試行カウンタが機能するには、ロード バランシングが有効になっている必要があります。

	コマンドまたはアクション	目的
ステップ 13	**l2tptunnelbusytimeout***seconds* 例： `Router(config-vpdn)# l2tp tunnel busy timeout 90`	（オプション）通信中だったルータと再度の通信を試行するまでにルータが待機する時間を設定します。 • *seconds*：相手のルータが使用可能かの確認を待機する時間を秒数で指定します。有効値の範囲は 60 ～ 6000 です。デフォルト値は 300 です。

L2TP 輻輳回避の設定

トンネルのエンドポイントでの L2TP 輻輳回避を設定し、L2TP 制御パケットのウィンドウ サイズを動的にスロットリングするには、このタスクを実行します。

この作業は、次のデバイスでも実行できます。

- トンネル サーバ
- トンネル エンドポイントとして機能している NAS

このタスクは、送信元デバイスでのみ実行が必要です。

（注）

- このタスクは、L2TP トンネリング プロトコルを使用する VPDN 配置とのみ互換性があります。
- クライアントが開始した L2TP トンネルでは、この作業はトンネル サーバにだけ実行できます。
- 輻輳のウィンドウ サイズは、ピア デバイス上において **l2tptunnelreceive-window** コマンドで設定されたアドバタイズ済み受信ウィンドウ サイズを超えることはできません。リモート ピア デバイスでアドバタイズ済み受信ウィンドウ サイズを設定するには、「VPDN トンネルの L2TP 制御パケット パラメータの設定，（205 ページ）」を参照してください。
- L2TP 輻輳回避は、設定の適用後に確立されたトンネルに対してのみ有効（または無効）になります。**l2tpcongestion-control** コマンド発行時にすでに存在していたトンネルはコマンドの影響を受けません。

手順の概要

1. **enable**
2. **configureterminal**
3. **l2tpcongestion-control**
4. **exit**
5. **showvpdntunnell2tpall**
6. **debugvpdnl2x-events**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**l2tpcongestion-control** 例： `Router(config)# l2tp congestion-control`	L2TP 輻輳回避を有効にします。
ステップ 4	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**showvpdntunnell2tpall** 例： `Router# show vpdn tunnel l2tp all`	有効なすべての L2TP VPDN トンネルの情報を表示します。
ステップ 6	**debugvpdnl2x-events** 例： `Router(config)# debug vpdn l2x-events`	プロトコル固有の VPDN トンネルに関するイベントのトラブルシューティング情報を表示します。

VPDN の障害イベントロギングの設定

履歴テーブルへの障害イベントのロギングは、syslog 機能によるイベント ログによって起動されます。Syslog ファシリティは障害イベントの履歴を保持する障害履歴テーブルを作成します。テーブルはデフォルトで最大 20 までのエントリを保持しまが、設定により 50 エントリまで増加できます。

障害エントリは時間順に履歴テーブルに保持されます。各エントリには、障害イベントの主な情報が記録されます。一意の名前とトンネルクライアントID（CLID）をもつユーザ1人ごとに、最新の障害イベントのみが保持されます。テーブルのエントリの数が設定された最大テーブル サイズに達すると、最も古いレコードが削除され、新しいエントリが追加されます。

VPDN障害履歴テーブルへのVPDN障害イベントのロギングはデフォルトで有効になっています。VPDN 障害イベントロギングは、前に無効に設定された場合のみ、有効に設定する必要があります。VPDN 障害イベントロギングを有効にし、障害履歴テーブルの最大エントリ数を設定し、VPDN 障害履歴テーブルの内容を表示し、クリアするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnhistoryfailure**
4. **vpdnhistoryfailuretable-size***entries*
5. **exit**
6. **showvpdnhistoryfailure**
7. **clearvpdnhistoryfailure**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**vpdnhistoryfailure** 例： `Router(config)# vpdn history failure`	（オプション）VPDN障害履歴テーブルへのVPDN障害イベントのロギングを有効にします。 （注） VPDN 障害ロギングは、デフォルトで有効になっています。以前に **novpdnhistoryfailure** コマンドを使って VPDN 障害履歴ロギングを無効に設定した場合のみ、**vpdnhistoryfailure** コマンドを発行する必要があります。
ステップ 4	**vpdnhistoryfailuretable-size***entries* 例： `Router(config)# vpdn history failure table-size 50`	（オプション）障害履歴テーブルのサイズを設定します。 （注） VPDN 障害履歴テーブルのサイズは、**vpdnhistoryfailure** コマンドを使用して VPDN 障害イベントロギングが有効になっている場合のみ設定できます。
ステップ 5	**exit** 例： `Router# exit`	特権 EXEC モードに戻ります。
ステップ 6	**showvpdnhistoryfailure** 例： `Router# show vpdn history failure`	（オプション）障害履歴テーブルの内容を表示します。
ステップ 7	**clearvpdnhistoryfailure** 例： `Router# clear vpdn history failure`	（オプション）障害履歴テーブルの内容をクリアします。

一般的な VPDN イベント ロギングの有効化

一般的な VPDN イベントとは、エラー、警告、通知、および syslog 機能に記録される情報レポートの組み合わせです。VPDN イベント ロギングがローカルとリモート トンネル エンドポイントで有効になっている場合、イベントの発生に伴って VPDN イベント メッセージがコンソールに出力されます。VPDN イベント メッセージは、認証、認可、およびアカウンティング（AAA）のベンダー固有属性（VSA）でリモート AAA サーバにも報告でき、アカウンティング記録と VPDN 通信成功率の相関比較を可能とします。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnlogging** [**accounting** | **local** | **remote** | **tunnel-drop** | **user**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnlogging** [**accounting**	**local**	**remote**	**tunnel-drop**	**user**] 例： `Router(config)# vpdn logging remote`	（オプション）一般的な VPDN イベントのロギングを有効にします。 • **vpdnlogging** コマンドの複数のインスタンスを発行して、一般的な VPDN イベント ロギングの複数のタイプを必要なだけ設定できます。 （注） AAA サーバへの VPDN イベント ログ メッセージの報告は、他の一切の汎用 VPDN イベント ロギング設定とは別に有効にできます。

VPDN トンネル管理の設定例

例：VPDN トンネルの手動終了

次の例は、ルータで終端するすべての L2TP トンネルを手動で終了します。

```
Router# clear vpdn tunnel l2tp all
```

例：VPDN トンネルのソフト シャットダウンの有効化

次の例では、使用したコマンドが存在するデバイスで終端するすべての VPDN トンネル ソフト シャットダウンを有効化します。

```
Router# configure terminal
Router(config)# vpdn softshut
!The following syslog message will appear on the device whenever an attempt is made to
!establish a new VPDN session after soft shutdown is enabled.
!
00:11:17:%VPDN-6-SOFTSHUT:L2TP HGW tunnelserver1 has turned on softshut and rejected user
user2@cisco.com
```

例：VPDN セッション制限の設定

次の例では、customer7 という名前の VPDN グループを設定し、グループレベルでのセッション数を 25 に制限しています。25 を超えるセッションをこの VPDN グループと関連付けることはできません。

```
Router(config)# vpdn-group customer7
Router(config-vpdn)# session-limit 25
```

それから customer4 という名前の VPDN テンプレートが作成され、8 のセッション制限が、テンプレートのレベルで設定されます。2 つの VPDN グループは VPDN テンプレートと関連付けられ、VPDN グループレベルでのセッション制限は、それぞれ 5 です。

```
Router(config)# vpdn-template customer4
Router(config-vpdn-templ)# group session-limit 8
!
Router(config)# vpdn-group customer4_l2tp
Router(config-vpdn)# source vpdn-template customer4
Router(config-vpdn)# session-limit 5
!
Router(config)# vpdn-group customer4_l2f
Router(config-vpdn)# source vpdn-template customer4
Router(config-vpdn)# session-limit 5
```

この設定では、customer4_l2tp という名前の VPDN グループにアクティブ セッションが 5 つがある場合、customer4_l2f という名前の VPDN グループは 3 つのセッションだけ確立できます。customer7 という名前の VPDN グループは、最大 25 のアクティブ セッションを持つことができます。

16 の VPDN セッションのグローバル制限も設定されている場合は、グローバルの制限は、設定された VPDN グループおよび VPDN テンプレートのセッション制限より優先されます。

```
Router# configure terminal
Router(config)# vpdn session-limit 16
```

3 つの VPDN グループは、それぞれの間で合計 16 のセッションを確立できます。たとえば、customer4_l2tp という名前の VPDN グループが許容されるアクティブなセッションの最大数（5 つのセッション）を持ち、customer4_l2f という名前の VPDN グループが 2 つのアクティブ セッションを持つとき、customer7 という名前の VPDN グループは最大 9 つのセッションのみを確立できます。

例：VPDN グループに対するセッション制限の確認

次の例では、l2tp という名前の VPDN グループを作成し、3 つのセッションに制限します。設定したセッション制限は、**show vpdn group** コマンドが発行されたときに表示されます。

```
Router# configure terminal
Router(config)# vpdn-group l2tp
Router(config-vpdn)# accept dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# terminate-from hostname host1
Router(config-vpdn)# session-limit 3
Router(config-vpdn)# end
Router# show vpdn group l2tp
Tunnel (L2TP)
------
dnis:cg1
dnis:cg2
dnis:jan
cisco.com
Endpoint        Session Limit Priority Active Sessions Status Reserved Sessions
--------        ------------- -------- --------------- ------ -----------------
172.21.9.67     3             1        0               OK     -
--------------- ------------- -------- --------------- ------ -----------------
Total           *                      0                      0
```

例：VPDN トンネルの L2TP パケット制御タイマーと再試行カウンタの設定

次の例では、l2tp という名前の VPDN グループ用に使用可能な L2TP パケット制御パラメータすべてのカスタム値を設定しています。

```
Router# configure terminal

Router(config)# vpdn-group l2tp

Router(config-vpdn)# l2tp tunnel hello 90
Router(config-vpdn)# l2tp tunnel receive window 500
Router(config-vpdn)# l2tp tunnel retransmit retries 8
Router(config-vpdn)# l2tp tunnel retransmit timeout min 2
Router(config-vpdn)# l2tp tunnel timeout no-session 500
Router(config-vpdn)# l2tp tunnel timeout setup 25
Router(config-vpdn)# l2tp tunnel zlb delay 4
Router(config-vpdn)# l2tp tunnel retransmit initial timeout min 2
Router(config-vpdn)# l2tp tunnel retransmit initial retries 5
Router(config-vpdn)# l2tp tunnel busy timeout 90
```

例：L2TP 輻輳回避のデバッグと確認の設定

次の例では、基本的なダイヤル イン L2TP VPDN トンネルを設定し、トンネル サーバ（受信デバイス）でのウィンドウ サイズを 500 に設定し、NAS（送信デバイス）での L2TP 輻輳回避を有効にします。

トンネル サーバの設定

```
Router(config)# vpdn enable
!
Router(config)# vpdn-group 1
Router(config-vpdn)# accept-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 1
!
Router(config-vpdn)# terminate from hostname NAS1
Router(config-vpdn)# l2tp tunnel receive-window 500
```

NAS の設定

```
Router(config)# vpdn enable
!
Router(config)# vpdn-group 1
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol l2tp
Router(config-vpdn-req-in)# domain cisco.com
!
Router(config-vpdn)# initiate-to ip 172.22.66.25
Router(config-vpdn)# local name NAS1
!
Router(config)# l2tp congestion-control
```

次の例では、L2TP の輻輳制御が有効であることを示す情報を含む、L2TP トンネルのアクティビティを示しています。スロースタートのしきい値が、リモートの受信ウィンドウ サイズと同じサイズに設定されていることに注意してください。リモート ピアがアドバタイズするリモートRWS値は、[Remote RWS] フィールドに表示されます。実際の RWS 値がアドバタイズされた値と異なるとき、実際の RWS 値は「*In Use Remote RWS <value>*」のように表示されます。

```
Router# show vpdn tunnel l2tp all
L2TP Tunnel Information Total tunnels 1 sessions 1
Tunnel id 30597 is up, remote id is 45078, 1 active sessions
  Tunnel state is established, time since change 00:08:27
  Tunnel transport is UDP (17)
  Remote tunnel name is LAC1
    Internet Address 172.18.184.230, port 1701
  Local tunnel name is LNS1
    Internet Address 172.18.184.231, port 1701
  Tunnel domain unknown
  VPDN group for tunnel is 1
  L2TP class for tunnel is
  4 packets sent, 3 received
  194 bytes sent, 42 received
  Last clearing of "show vpdn" counters never
  Control Ns 2, Nr 4
  Local RWS 1024 (default), Remote RWS 256
  In Use Remote RWS 15
  Control channel Congestion Control is enabled
    Congestion Window size, Cwnd 3
    Slow Start threshold, Ssthresh 256
    Mode of operation is Slow Start
  Tunnel PMTU checking disabled
  Retransmission time 1, max 2 seconds
  Unsent queuesize 0, max 0
  Resend queuesize 0, max 1
  Total resends 0, ZLB ACKs sent 2
  Current nosession queue check 0 of 5
  Retransmit time distribution: 0 0 0 0 0 0 0 0 0
  Sessions disconnected due to lack of resources 0
  Control message authentication is disabled
```

以下の **debugvpdnl2x-events** コマンドからの出力の一部は、輻輳が発生したことを示します。輻輳のウィンドウ サイズとスロースタートのしきい値は、パケットの再送信イベントによりリセットされています。

```
Router# debug vpdn l2x-events
!
*Jul 15 19:02:57.963:  Tnl 47100 L2TP: Congestion Control event received is retransmission
*Jul 15 19:02:57.963:  Tnl 47100 L2TP: Congestion Window size, Cwnd 1
*Jul 15 19:02:57.963:  Tnl 47100 L2TP: Slow Start threshold, Ssthresh 2
*Jul 15 19:02:57.963:  Tnl 47100 L2TP: Remote Window size, 500
*Jul 15 19:02:57.963:  Tnl 47100 L2TP: Control channel retransmit delay set to 4 seconds
*Jul 15 19:03:01.607:  Tnl 47100 L2TP: Update ns/nr, peer ns/nr 2/5, our ns/nr 5/2
!
```

以下の **debugvpdnl2x-events** コマンドからの出力の一部は、スロースタート モードでの L2TP 輻輳回避を用いてトラフィックが再起動したことを示しています。

```
Router# debug vpdn l2x-events
!
*Jul 15 14:45:16.123:  Tnl 30597 L2TP: Control channel retransmit delay set to 2 seconds
*Jul 15 14:45:16.123:  Tnl 30597 L2TP: Tunnel state change from idle to wait-ctl-reply
*Jul 15 14:45:16.131:  Tnl 30597 L2TP: Congestion Control event received is positive
acknowledgement
*Jul 15 14:45:16.131:  Tnl 30597 L2TP: Congestion Window size, Cwnd 2
*Jul 15 14:45:16.131:  Tnl 30597 L2TP: Slow Start threshold, Ssthresh 500
*Jul 15 14:45:16.131:  Tnl 30597 L2TP: Remote Window size, 500
*Jul 15 14:45:16.131:  Tnl 30597 L2TP: Congestion Ctrl Mode is Slow Start
!
```

例：VPDN の障害イベントロギングの設定

次の例は、最初に VPDN の障害イベントロギング無効にして、再び有効にし、VPDN 障害履歴テーブルのエントリの最大数を 50 に設定します。障害履歴テーブルの内容が表示され、その後クリアされます。

```
Router# configure terminal
Router(config)# no vpdn history failure
Router(config)# vpdn history failure
Router(config)# vpdn history failure table-size 50
Router(config)# end
Router# show vpdn history failure
!
Table size: 50
Number of entries in table: 1
User: user@cisco.com, MID = 1
NAS: isp, IP address = 172.21.9.25, CLID = 1
Gateway: hp-gw, IP address = 172.21.9.15, CLID = 1
Log time: 13:08:02, Error repeat count: 1
Failure type: The remote server closed this session
Failure reason: Administrative intervention
!
Router# clear vpdn history failure
```

例：一般的な VPDN のイベント ロギングの設定

次の例では、ローカルで VPDN ロギングを有効化します。

```
Router# configure terminal
Router(config)# vpdn logging local
```

次の例では、VPDN イベント ロギングをローカルで無効にし、リモート トンネル エンドポイントでの VPDN イベント ロギングを有効にし、VPDN ユーザと VPDN トンネル ドロップ イベントの両方のロギングをリモート ルータに対して有効にします。

```
Router# configure terminal
Router(config)# no vpdn logging local
Router(config)# vpdn logging remote
Router(config)# vpdn logging user
Router(config)# vpdn logging tunnel-drop
```

次の例では、リモート トンネル エンドポイントでの VPDN イベントのロギングを無効にし、VPDN イベント ログ メッセージのロギングを AAA サーバに対して有効にします。

```
Router# configure terminal
Router(config)# no vpdn logging local
Router(config)# no vpdn logging remote
Router(config)# vpdn logging accounting
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
VPDN 技術の概要	「VPDN 技術の概要」のモジュール
VPDN コマンド：完全なコマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS VPDN Command Reference*』
VPDN のテクニカル サポートのドキュメンテーション	仮想私設ダイヤルアップ網（VPDN）
ダイヤル テクノロジー コマンド：完全なコマンド構文、コマンドモード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS Dial Technologies Command Reference*』
VPDN 追加機能の設定に関連する概念およびタスク	「VPDN 追加機能の設定」のモジュール

標準

規格	タイトル
TCP/IP；スロースタートと輻輳回避アルゴリズム	『*TCP/IP Illustrated, Volume 1*』

MIB

MIB	MIB のリンク
• CISCO-VPDN-MGMT-MIB • CISCO-VPDN-MGMT-EXT-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2661	『レイヤ *2* トンネリング プロトコル（*L2TP*）』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VPDN トンネル管理の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *13* : *VPDN* トンネル管理の機能情報

機能名	リリース	機能情報
L2TP 輻輳回避	Cisco IOS XE リリース 2.3	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。RFC 2661 で説明されているようにレイヤ 2 トランスポートプロトコル (L2TP) 制御メッセージをスロットリングすることにより、パケットフロー制御と輻輳回避機能を提供します。 この機能によって、次のコマンドが導入または変更されました。**debugvpdn**、**l2tpcongestion-control**。
VRF ごとのセッション制限	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。共通の VPDN テンプレートに関連付けられているすべての VPDN グループにセッション制限を適用できます。単一の VPN ルーティングおよび転送（VRF）インスタンスに終端する VPDN セッションの数を制限できます。 この機能により次のコマンドが導入され、また変更されました。**groupsession-limit**、**sourcevpdn-template**、**vpdn-template**。

機能名	リリース	機能情報
L2TP 向けタイマーと再試行の機能拡張	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。この機能により、ユーザは調節可能なタイマーとカウンタを L2TP 用に設定できます。 この機能により次のコマンドが導入されました。**l2tptunnelbusytimeout**、**l2tptunnelretransmitinitialretries**、**l2tptunnelretransmitinitialtimeout**。
VPDN グループのセッション制限	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。この機能により、VPDN グループごとに許容する L2TP VPDN セッション数の制限を設定できます。 この機能によって **session-limit** (VPDN) コマンドが導入されました。

第 8 章

LAC/LNS 上での L2TP HA セッションの SSO/ISSU の設定

LAC/LNS 上での L2TP HA セッションの SSO/ISSU 機能では、レイヤ 2 アクセス コンセントレータ（LAC）およびレイヤ 2 ネットワーク サーバ（LNS）上のレイヤ 2 トンネリング プロトコル（L2TP）のための、汎用ステートフル スイッチオーバー/インサービス ソフトウェア アップグレード（SSO/ISSU）メカニズムを提供します。この機能では、SSO スイッチオーバーや、ISSU アップグレードまたはダウングレード中に、完全に確立された PPP および L2TP セッションが保持されます。

- 機能情報の確認，223 ページ
- LAC/LNS での L2TP HA セッション SSO/ISSU の前提条件，224 ページ
- LAC/LNS での L2TP HA Session SSO/ISSU の機能制限，224 ページ
- LAC/LNS 上での L2TP HA セッションの SSO/ISSU に関する情報，224 ページ
- LAC/LNS 上での L2TP HA セッションの SSO/ISSU の設定方法，226 ページ
- LAC/LNS での L2TP HA Session SSO/ISSU の設定例，237 ページ
- その他の参考資料，238 ページ
- LAC/LNS での L2TP HA セッション SSO/ISSU の機能情報，240 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

LAC/LNS での L2TP HA セッション SSO/ISSU の前提条件

- VPDN の導入を設定します。VPDN の導入の概要については、「VPDN 技術の概要」のモジュールを参照してください。
- この実装では、ピア L2TP ノードは HA または冗長性に対応している必要はありません。ピア L2TP ノードは L2TP フェールオーバー RFC を実装する必要はありません。
- ピア L2TP ノードが L2TP RFC 準拠であることを確認します。

LAC/LNS での L2TP HA Session SSO/ISSU の機能制限

- Cisco IOS XE リリース 2.2 は、LAC/LNS での L2TP HA Session SSO/ISSU 機能を Cisco ASR 1000 シリーズ ルータ上でのみサポートします。
- Cisco IOS XE リリース 2.4 は VPDN トンネルとセッション用の VPDN マルチホップ ノードをサポートします。VPDN トンネルとセッションは、デュアル RP ASR セットアップでのルート プロセッサ（RP）フェールオーバー後に保持されます。
- LAC/LNS での L2TP HA Session SSO/ISSU は、次のソフトウェア機能では HA/SSO をサポートせず、これらのセッションは、RP フェールオーバー後に失われます。
  - L2TP ダイヤルアウト
  - L2TP Active Discovery Relay for PPPoE
  - LNS 上のマルチリンク PPP

LAC/LNS 上での L2TP HA セッションの SSO/ISSU に関する情報

ステートフル スイッチオーバー

ステートフル スイッチオーバー（SSO）機能は、Cisco IOS ルータによって構築されるネットワークのアベイラビリティを向上させるために、全体的なプログラムの中で改善を積み重ねることによって発展してきました。

デュアル RP をサポートしている Cisco の特定のネットワーキング デバイスでは、ステートフル スイッチオーバー は RP 冗長性を活用してネットワークのアベイラビリティを向上させます。この機能はRPの一方をアクティブ プロセッサとして設定し、もう一方のRPをスタンバイ プロセッサとして指定したあと、これらのRPの間で重要な状態情報を同期します。2つのプロセッサの初回同期後、SSO はこれらの間の RP ステート情報をダイナミックに維持します。

アクティブRPに障害が発生したとき、アクティブRPがネットワーキング デバイスから削除されたとき、またはメンテナンスのために手動で停止されたときに、アクティブ プロセッサからスタンバイ プロセッサへのスイッチオーバーが発生します。

SSO は特にネットワーク エッジで役立ちます。従来から、コア ルータはルータの冗長化とメッシュ接続を使用して、障害ネットワーク要素を迂回したトラフィック伝送を可能にすることにより、ネットワーク障害からシステムを保護します。SSO は、ネットワーク設計内のシングル ポイント障害であり、障害時には顧客に対するサービス提供が中断する可能性があるネットワーク エッジ デバイスを、デュアル RP によって保護します。

（注） 新しい L2TP セッション要求が、スイッチオーバー後の再同期フェーズにあるトンネルで受診されると、そのリクエストは拒否されます。新しいCiscoベンダー固有の切断原因コード（611）はこのセッション切断の理由を表示します。**showvpdnhistoryfailure** コマンドは障害タイプのフィールドを「Tunnel in HA resync」 として表示します。

データのチェックポインティング

SSO では、HA スイッチオーバー用のリモート RP、および ION 再起動用のローカル RP 上のピア クライアントに転送されるクライアント固有のステート データに対するチェックポインティング、つまり保存および再同期を常に実行しています。有効なチェックポインティング セッションが確立されると、チェックポインティングが実行されたステート データはエラーなしで確定されます。

ISSUソフトウェアスーパーパッケージおよびローリングアップグレードの要件

ここでは、Cisco ASR 1000 シリーズ ルータに対して ISSU スーパーパッケージまたはサブパッケージのソフトウェアのアップグレードまたはダウングレードを実行する際の、L2TP への影響について説明します。ソフトウェアのアップグレードおよびダウングレードの ISSU 操作中に、ISSU の一部のシナリオでは、制御トラフィックの中断が発生し、これが原因で（L2TP サイレント スイッチオーバーを使用した）L2TP の再同期化操作が失敗し、L2TP トンネルまたは L2TP セッションが失われる可能性があります。

通常、ISSU スーパーパッケージまたはサブパッケージのソフトウェアのアップグレードまたはダウングレードを実行中に、データ トラフィックに対する影響はありません。データ トラフィックの中断は、管理および想定される操作セットに含まれています。たとえば、特定の SPA 用のソフトウェアをアップグレードする際、このソフトウェア アップグレードは、その SPA から処理され

るデータ トラフィックにだけ影響を与えます。つまり、残りのネットワークは、引き続き正常に動作します。

ソフトウェアのアップグレードとダウングレード

スーパー パッケージのソフトウェア アップグレードまたはダウングレードを設定するときは、L2TP セッションとトンネルが失われる可能性があります。L2TP トンネルまたはセッションの損失を軽減するために、ローリング アップグレード方式を使用して L2TP トンネルまたはセッションの停止を最小限に抑えます。

（注） IP レイヤによって見られるトンネルまたはセッションの停止に関して、IP ルーティングに対するバックアップ インターフェイスの設定または、L2TP ピアへの入力チャネルの設定によって、最小限に抑えることができます。

Cisco ASR 1000 シリーズ ルータの場合、ISSU の互換性はアップグレードされるソフトウェアのサブパッケージおよびハードウェア構成によって異なる点を認識することが必要です。統合パッケージは、デュアル RP 構成の場合にだけ ISSU との互換性があり、その他にも制限があります。SPA および SIP ソフトウェア サブパッケージは、SPA または SIP 単位でアップグレードする必要があります。

スタンバイのルートプロセッサ（RP）のリロードが必要な Cisco ASR 1000 シリーズ ルータでソフトウェアパッケージをアップグレードする場合、スタンバイの FP、SPA と SIP ソフトウェアを、スイッチオーバーに続くアクティブな RP でプロビジョニングされたソフトウェアと同じバージョンで手動でアップグレードする必要があり、新しいアクティブな RP としてスタンバイの RP が引き継ぐ際のリロードを防ぎます。

受信ウィンドウ サイズの調整

LAC/LNS 上での L2TP HA セッションの SSO/ISSU を設定した場合、Cisco IOS ソフトウェアでは、L2TP 受信ウィンドウ サイズがより小さい値に内部で調整されます。この調整された受信ウィンドウ（receive-window）の値は、**show vpdn tunnel detail** コマンドを使用すると表示されます。必要な場合、**l2tp tunnel resync** コマンドを使用して L2TP 受信ウィンドウのサイズを大きくします。

LAC/LNS 上での L2TP HA セッションの SSO/ISSU の設定方法

l2tpssoenable コマンドを使用すれば、L2TP HA をグローバルに設定できます。VPDN グループ コンフィギュレーション モードで **ssoenable** コマンドを使用すれば、特定の VPDN グループに対して L2TP HA セッションを設定することもできます。グローバルの L2TP HA セッションと VPDN グループの L2TP HA セッションの両方が、デフォルトで有効になります。プロトコルの L2TP が L2TP HA セッション機能を実行するように、VPDN グループに対して **l2tpssoenable** コマンドと **ssoenable** コマンドの両方を設定する必要があります。

グローバルの L2TP HA セッションと VPDN グループ固有の L2TP HA セッションは、**showrunning-config** コマンドの出力に表示されません。これは、これらのセッションがデフォルトで有効になっているためです。**nol2tpssoenable** コマンドを使用した場合、HA コマンドはNVGENとして表示され、**showrunning-config** コマンドの出力に表示されます。

SSO スイッチオーバーの後、L2TP HA セッションでは L2TP ピアで使用されるシーケンス番号を決定します。シーケンス番号の決定には、ピアが多数の確認応答されていないメッセージを送信する場合に時間がかかる可能性があります。**l2tptunnelresync** コマンドを使用すれば、ピアから送信される確認応答されていないメッセージの数を制御できます。パケット数の値を増やすと、多数のセッションがある L2TP HA トンネルのセッション セットアップ レートを向上させることができます。

ルート プロセッサの SSO 設定

Cisco シリーズインターネットルータは、同じバージョンの SSO 認識イメージをデバイスにリロードした後、デフォルトで SSO モードで動作します。

SSO を使用するには、RP で SSO を有効にする必要があります。この作業では、**redundancy** コマンドを使用して RP で SSO を有効にする方法について説明します。この作業により、ピアとの接続での既存のセッションの再生成、再確立で、SSO に続くすべての冗長セッション データが確実に使用されるようになります。

手順の概要

1. **enable**
2. **configureterminal**
3. **redundancy**
4. **modesso**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**redundancy** 例： `Router(config)# redundancy`	冗長コンフィギュレーションモードを開始します。
ステップ 4	**modesso** 例： `Router(config-red)# mode sso`	冗長性モードを指定します。
ステップ 5	**end** 例： `Router(config-red)# end`	特権 EXEC モードに戻ります。

グローバル L2TP HA SSO モードの設定

Cisco シリーズインターネットルータは、同じバージョンの SSO 認識イメージをデバイスにリロードした後、デフォルトで L2TP HA SSO モードで動作します。L2TP HA SSO セッションを使用するのに設定は不要です。

この手順では、HA をグローバルに有効/無効にするための **l2tpssoenable** コマンドの使用方法を示します。**l2tpssoenable** コマンドはデフォルトで有効になっています。

手順の概要

1. **enable**
2. **configureterminal**
3. **l2tpssoenable**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**l2tpssoenable** 例： `Router(config)# l2tp sso enable`	L2TP HA SSO を有効にします。
ステップ 4	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

L2TP HA SSO 用の VPDN グループまたは VPDN テンプレートの設定

L2TP HA SSO に VPDN グループまたは VPDN テンプレートを設定するには、この作業を実行します。この設定例では、使用中の VPDN トンネルの数が多数（たとえば 8000）に上り、各トンネルが少数の VPDN セッションのみをサポートしている場合に推奨されるスケーリング パラメータを提供します。

逆に、VPDN トンネル数が少なく、VPDN トンネルごとの VPDN セッションの数が多い場合は、**l2tptunnelresync** コマンドを使用して再同期の値を増やします。たとえば、VPDN トンネルごとの VPDN セッションの数が数百である場合、**l2tptunnelresync** コマンドを使用して再同期の値を数百に見合った値に増やします。

Cisco IOS XE リリース 2.3 以降では、再送信の再試行とタイムアウトの設定値をデフォルト値に設定できます。

VPDN グループの HA 機能のためには、**l2tpssoenable** と **ssoenable** の両方のコマンドを有効にする必要があります（デフォルト）。どちらかのコマンドが無効になると、VPDN グループで HA 機能は使用できません。

手順の概要

1. **enable**
2. **configureterminal**
3. **l2tpssoenable**
4. **vpdnenable**
5. **vpdn-group***name*
6. **ssoenable**
7. **l2tptunnelresync***packets*
8. **l2tptunnelretransmitretries***number*
9. **l2tptunnelretransmittimeoutmin***seconds*
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**l2tpssoenable** 例： `Router(config)# l2tp sso enable`	L2TP SSO モードを有効にします。
ステップ 4	**vpdnenable** 例： `Router(config)# vpdn enable`	VPDN コンフィギュレーション モードを開始します。
ステップ 5	**vpdn-group***name* 例： `Router(config-vpdn)# vpdn-group example`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**ssoenable** 例： `Router(config-vpdn)# sso enable`	VPDN グループで L2TP SSO を有効にします。
ステップ 7	**l2tptunnelresync***packets* 例： `Router(config-vpdn)# l2tp tunnel resync 4`	確認応答待機前に L2TP HA トンネルが送信する SSO 後のパケット数を設定します。
ステップ 8	**l2tptunnelretransmitretries***number* 例： `Router(config-vpdn)# l2tp tunnel retransmit retries 30`	L2TP 制御パケットの再送信の試行回数を設定します。
ステップ 9	**l2tptunnelretransmittimeoutmin***seconds* 例： `Router(config-vpdn)# l2tp tunnel retransmit timeout min 8`	L2TP 制御パケットを再送信するまでにルータが待機する時間を設定します。
ステップ 10	**exit** 例： `Router(config-vpdn)# exit`	VPDN グループ コンフィギュレーション モードを終了します。

L2TP HA パケット再同期の制御

SSO のスイッチオーバー後、L2TP HA は L2TP ピアが使用するシーケンス番号を決定します。ピアが応答確認のないメッセージを大量に送出すると、シーケンス番号を調べるのに時間がかかることがあります。**l2tptunnelresync** コマンドを使用すれば、ピアから送信される確認応答されていないメッセージの数を制御できます。パケット数の値を増やすと、多数のセッションがある L2TP HA トンネルのセッション セットアップ レートを向上させることができます。

showl2tpredundancy コマンドを使い、ピアの L2TP ノードとの再同期に必要な時間を表示できます。

この手順では、**l2tptunnelresync** コマンドを使い、VPDN グループ設定モードで応答確認待機前に L2TP HA トンネルが送出するパケットの数を制御する方法を示します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnenable**
4. **vpdn-group***name*
5. **l2tptunnelresync***packets*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnenable** 例： `Router(config)# vpdn enable`	VPDN コンフィギュレーション モードを開始します。
ステップ 4	**vpdn-group***name* 例： `Router(config-vpdn)# vpdn-group example`	VPDN グループを作成し、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 5	**l2tptunnelresync***packets* 例： `Router(config-vpdn)# l2tp tunnel resync 250`	SSO 後、確認応答メッセージ送出前に処理するパケットの数を指定します。この例では、確認応答メッセージを送信する前に 250 個のパケットが処理されます。
ステップ 6	**end** 例： `Router(config-vpdn)# end`	特権 EXEC モードに戻ります。

L2TP HA セッションのチェックポイント ステータスの確認

show l2tp redundancy コマンドは L2TP のグローバルな状態と特定の L2TP セッションのチェックポイント状態についての情報を提供します。次の詳細情報が表示できます。

- L2TP HA プロトコルの状態：
  - スタンバイ完了
  - 受信済みメッセージのカウンタ
  - トンネルの数、セッションの数と、HA 対応のトンネルとセッションの数との比較
  - 最後のスイッチオーバー後に L2TP ピアノードで正常に再同期できたトンネルの数と、再同期に失敗した数。
- L2TP 制御チャネル（トンネル）の冗長性情報：
  - トンネルの状態
  - ローカル ID
  - リモート ID
  - リモート名
  - クラスまたはグループ名
  - このトンネルを使用しているセッションの数
- L2TP セッション冗長性情報：
  - ローカル セッション ID
  - リモート セッション ID
  - トンネル ID
  - 論理トンネルと論理セッション ハンドルの割り当てステータス

HA 向けに設定されたトンネル（HA 対応トンネル）の L2TP HA プロトコルの状態の情報と、確立に成功した HA トンネル（HA 確立のトンネル）の情報は、障害が発生していない限り、アクティブ、スタンバイ RP で一致しなければなりません。

スタンバイ RP での **show l2tp redundancy** コマンドの出力は、カウンタの値の合計を表示せず、再同期した L2TP トンネルの値も表示しません。カウンタの値の合計には、HA で保護されていないトンネルとセッションが含まれますが、これらはスタンバイ RP にはありません。

チェックポイント ステータスを持つグローバル L2TP または特定の L2TP セッションを表示するには、次の手順に従います。

手順の概要

1. **enable**
2. **showl2tpredundancy** [**all** | [**detail**] [**id** *local-tunnel-ID* [*local-session-ID*]]]
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showl2tpredundancy** [**all** | [**detail**] [**id** *local-tunnel-ID* [*local-session-ID*]]] 例： `Router# show l2tp redundancy all`	冗長性データを持つL2TPセッションのステータスを表示します。
ステップ 3	**exit** 例： `Router# exit`	特権 EXEC モードを終了します。

VPDN セッションのチェックポイント ステータスの確認

手順の概要

1. **enable**
2. **showvpdnredundancy** [**all** | [**detail**] [**id***local-tunnel-ID* [*local-session-ID*]]]
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showvpdnredundancy** [**all** | [**detail**] [**id***local-tunnel-ID* [*local-session-ID*]]] 例： `Router# show vpdn redundancy all`	チェックポイント データを持つ VPDN セッションのステータスを表示します。
ステップ 3	**exit** 例： `Router# exit`	特権 EXEC モードを終了します。

L2TP または VPDN 冗長セッションのトラブルシューティング

L2TP または VPDN 冗長セッションに対しては、トラブルシューティングは広範囲に渡ります。たとえば、スタンバイ RP が初期化できない場合は、**show l2tp redundancy** コマンドで警告メッセージとトンネルまたはセッションの情報を表示できます。

```
Router# show l2tp redundancy

L2TP HA support: Silent Failover
L2TP HA Status:
  Checkpoint Messaging on: FALSE
  Standby RP is up:        TRUE
  Recv'd Message Count:    0

No HA CC of Session data to display until Standby RP is up.
```

debug l2tp redundancy または **debug vpdn redundancy** コマンドにより、L2TP または VPDN チェックポイントのイベントやエラーのデバッグ情報を表示できます。デバッグ情報には次が含まれます。

- cf：L2TP 冗長性チェックポイント機能イベント（cf- イベント）
- 詳細：L2TP 冗長性の詳細
- エラー：L2TP 冗長性のエラー
- イベント：L2TP 冗長性のイベント
- fsm：L2TP 冗長性 fsm のイベント

- 再同期：L2TP 冗長性の再同期
- rf：L2TP 冗長性機能のイベント（rf- イベント）

冗長性のイベント エラーが発生した L2TP または VPDN セッションをデバッグするには、次の手順に従います。

手順の概要

1. **enable**
2. **debug** {**l2tp** | **vpdn**} **redundancy** {**cf** | **detail** | **error** | **event** | **fsm** | **resync** | **rf**}
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug** {**l2tp**	**vpdn**} **redundancy** {**cf**	**detail**	**error**	**event**	**fsm**	**resync**	**rf**} 例： `Router# debug vpdn redundancy cf`	冗長性データを持つ VPDN セッションのデバッグ情報を表示する。
ステップ 3	**exit** 例： `Router# exit`	特権 EXEC モードを終了します。

RADIUS サーバでの L2TP HA SSO/ISSU の設定

次の RADIUS 属性と値（attribute-value: AV）のペアを使用して、RADIUS サーバで L2TP HA SSO/ISSU を設定することができます。

```
cisco:cisco-avpair="vpdn:l2tp-silent-switchover=1"
```

次の RADIUS AV ペアを使用して、RADIUS サーバで L2TP HA SSO/ISSU の再同期パラメータを設定することができます。

```
cisco:cisco-avpair="vpdn:l2tp-tunnel-resync-packet=<num>"
```

LAC/LNS での L2TP HA Session SSO/ISSU の設定例

例：ルート プロセッサの SSO 設定

次に、ルート プロセッサの SSO を設定する例を示します。

```
Router# configure terminal
Router(config)# redundancy
Router (config-red)# mode sso
Router (config-red)# end
```

例：L2TP ハイ アベイラビリティの設定

次に、L2TP SSO を設定する例を示します。

```
Router# configure terminal
Router(config)# l2tp sso enable
Router (config-red)# end
```

例：L2TP チェックポイント ステータスの表示

例：L2TP の冗長性情報の表示

次では、L2TP 冗長性の情報要求の例を示しています。

```
Router# show l2tp redundancy
L2TP HA support: Silent Failover
L2TP HA Status:
  Checkpoint Messaging on: TRUE
  Standby RP is up:        TRUE
  Recv'd Message Count:    189
  L2TP Tunnels:            2/2/2/0 (total/HA-enabled/HA-est/resync)
  L2TP Sessions:           20/20/20 (total/HA-enabled/HA-est)
  L2TP Resynced Tunnels:   2/0 (success/fail)
  Resync duration 0.63 secs (complete)
```

例：L2TP の冗長性の詳細情報の表示

次の例では、L2TP の冗長性の詳細情報の要求を示しています。

```
Router# show l2tp redundancy detail id 44233 2
 Local session ID        : 2
 Remote session ID        : 2
 Local CC ID        : 44233
 Local UDP port        : 1701
 Remote UDP port        : 1701
 Waiting for VPDN application        : No
 Waiting for L2TP protocol        : No
```

例：すべての L2TP の冗長性情報の表示

次の例では、L2TP 冗長性の全情報の要求を示しています。

```
Router# show l2tp redundancy all

L2TP HA support: Silent Failover
L2TP HA Status:
  Checkpoint Messaging on: FALSE
  Standby RP is up:        TRUE
  Recv'd Message Count:    0
  L2TP Active Tunnels:     1/1/0 (total/HA-enabled/resync)
  L2TP Active Sessions:    1/1 (total/HA-enabled)
 L2TP Resynced Tunnels:  1/0 (success/fail)
L2TP HA CC Check Point Status:
State  LocID RemID Remote Name      Class/Group              Num. Sessions
est    33003 26355 LAC-1            1                        1
L2TP HA Session Status:
LocID      RemID      TunID     Waiting for    Waiting for
                                  VPDN app?     L2TP proto?
28017      10         33003       No             No
```

例：L2TP の冗長性 ID 情報の表示

次の例は、トンネル ID の提供によって表示される情報を制限する方法を示します。

```
Router# show l2tp redundancy id 33003
 L2TP HA Session Status:
LocID  RemID  TunID   Waiting for     Waiting for
       VPDN app?     L2TP proto?
2  2  33003   No     No
```

例：L2TP の冗長性の詳細 ID 情報の表示

次の例は、セッション ID の提供によって表示される情報を制限する方法を示しています。

```
Router# show l2tp redundancy detail id 33003 3
Local session ID        : 3
 Remote session ID        : 3
 Local CC ID        : 33003
 Local UDP port        : 1701
 Remote UDP port        : 1701
 Waiting for VPDN application        : No
 Waiting for L2TP protocol        : No
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
VPDN コマンド	『*Cisco IOS VPDN Command Reference*』

関連項目	マニュアル タイトル
レイヤ 2 トンネル プロトコル	『Layer 2 Tunnel Protocol Technology Brief』
ステートフル スイッチオーバーとハイ アベイラビリティ	「ステートフル スイッチオーバーの設定」のモジュール
Cisco ASR 1000 シリーズ ルータの ISSU	http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/issu.html
VPDN 技術の概要	「VPDN 技術の概要」のモジュール

標準

規格	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2661	『レイヤ *2* トンネリング プロトコル（*L2TP*）』
RFC 4591	『Fail Over for Layer 2 Tunneling Protocol (L2TP)』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

LAC/LNS での L2TP HA セッション SSO/ISSU の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *14* : *LAC/LNS* での *L2TP HA* セッション *SSO/ISSU* の機能情報

機能名	リリース	機能情報
LAC/LNS での L2TP HA セッション SSO/ISSU	Cisco IOS XE リリース 2.2 Cisco IOS XE リリース 2.3 Cisco IOS XE リリース 2.4	LAC および LNS 上のレイヤ 2 トンネリング プロトコル（L2TP）に一般的な SSO/ISSU メカニズムを提供します。 この機能は、Cisco ASR 1000 シリーズ ルータで導入されました。 この機能により、次のコマンドが導入されました。**debugl2tpredundancy**、**debugvpdnredundancy**、**l2tpssoenable**、**l2tptunnelresync**、**showl2tpredundancy**、**showvpdnredundancy**、**ssoenable**。 2.3 では、VPDN グループとテンプレートのパラメータのスケーリングのサポートが追加されました。 2.4 では、VPDN トンネルとセッションのためのマルチホップ VPDN のサポートが追加されました。

第 9 章

L2TP の切断の原因情報

L2TP 切断原因情報機能によって、RFC 3145 で規定されている属性と値（Attribute-Value: AV）のペア 46 を使用した、追加のレイヤ 2 トンネリング プロトコル（L2TP）切断エラー コードのサポートが追加されています。この機能が導入されるまで、L2TP ホストが PPP 切断エラー コードを交換することは不可能でした。

- 機能情報の確認，243 ページ
- L2TP 切断原因の情報についての制約事項，243 ページ
- L2TP の切断原因についての情報，244 ページ
- その他の参考資料，246 ページ
- L2TP の切断原因の情報に関する機能情報，247 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

L2TP 切断原因の情報についての制約事項

- この機能は、RFC 3145 に準拠したエラー コードだけを実装します。

- ルータが AV ペア 46 をサポートされていない切断コードと共に受信した場合、コード 0 にマッピングされ、利用可能な情報が無いことを示します。

L2TP の切断原因についての情報

L2TP 切断原因情報の仕組み

L2TP 切断原因コードによって、L2TP ホストとして機能している各デバイスは、PPP 関連の切断原因情報を交換することができます。L2TP の動作は、通常カプセル化中の PPP セッションの詳細からは分離されています。AV ペア 46 の PPP 切断原因コードが、L2TP ホスト間の PPP 関連の切断原因情報の交換に使用されます。この情報は、認証、認可、およびアカウンティング（AAA）の適切なコードに変換して、リモート RADIUS AAA サーバにリレーすることができます。

L2TP 切断原因情報の利点

L2TP サービスに障害が発生した場合、またはセッションの確立に失敗した場合、PPP 固有の切断情報に、トラブルシューティングまたはアカウンティングのために使用できる非常に役立つ情報が提供されます。この情報がないと、各 L2TP ホストが同じ事業主体や組織によって所有または管理されていない場合は特に問題になります。L2TP 切断原因情報機能によって、サービス プロバイダーは、明確な障害の原因を突き止めることができるため、分析とエラーの修正が容易になります。

L2TP 切断原因の情報コード

以下の表にサポート対象の RFC 3145 からの L2TP の切断原因コードとコードの簡単な説明を示します。

表 *15*：*L2TP* の切断原因コード

コード	説明
グローバル エラー	
0	使用できる情報がありません。 （注） ルータが AV ペア 46 をサポートされていない切断コード（可能性として、他のベンダーや Cisco ソフトウェアの新しいバージョンからのコードなど）と共に受信した場合は、このコードにマッピングされています。

コード	説明
1	管理上の接続解除。
3	通常の接続解除、Link Control Protocol（LCP）の Terminate-Request が送信されました。 有効なディレクション値は次のとおりです。 • 1：ピア デバイスによって送信された LCP Terminate-Request。 • 2：ローカル デバイスによって送信された LCP Terminate-Request。
LCP エラー	
5	有限ステート マシン（FSM）タイムアウト エラー。
6	認識可能な LCP パケットはまだ受信されていません。
8	LCP リンク障害：エコー要求のタイムアウト。
9	ピアが既存のマルチリンク PPP（MLP）バンドルに対して想定外のエンドポイント ディスクリミネータを持っています。
12	PPP ピアで必要とされる強制コールバックが、ピアによって拒否されました。 有効なディレクション値は次のとおりです。 • 1：ローカル デバイスで必須ですが、ピア デバイスにより拒否されました。 • 2：ピア デバイスで必須ですが、ローカル デバイスにより拒否されました。
認証エラー	
13	FSM タイムアウトエラー。

コード	説明
16	PPP 認証が無効なホスト名、パスワード、または秘密鍵により失敗しました。 有効なディレクション値は次のとおりです。 • 1：ローカル システムによるピア ID の認証に失敗しました。 • 2：ピア システムによるローカル ID の認証に失敗しました。
Network Control Protocol（NCP）エラー	
17	FSM タイムアウトエラー。
18	NCP がすべて利用不可（すべて無効または拒否）であるか、または NCP がオープン状態になっています。制御プロトコル番号は、どちらのピアでも NCP を有効にしなかった場合のみゼロにすることができます。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
VPDN L2TP トンネルの設定に関する情報	「VPDN トンネルの管理」のモジュール
VPDN コマンド	『*Cisco IOS VPDN Command Reference*』

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 3145	『L2TP Disconnect Cause Information』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

L2TP の切断原因の情報に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *16* : *L2TP* の切断原因の情報機能に関する機能情報

機能名	リリース	機能情報
L2TP の切断の原因情報	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 L2TP 切断原因情報機能によって、RFC 3145 で規定されている属性と値（Attribute-Value: AV）のペア 46 を使用した、追加のレイヤ 2 トンネリング プロトコル（L2TP）切断エラーコードのサポートが追加されています。この機能が導入されるまで、L2TP ホストが PPP 切断エラー コードを交換することは不可能でした。 この機能によって導入または変更されたコマンドはありません。

第 10 章

管理型 IPv6 レイヤ 2 トンネリング プロトコル ネットワーク サーバの設定

このモジュールでは、管理型 IPv6 レイヤ 2 トンネリング プロトコル ネットワーク サーバ機能を有効にする方法について説明します。

- 機能情報の確認，249 ページ
- 管理型 IPv6 LNS を設定するための前提条件，250 ページ
- 管理型 IPv6 LNS を設定するための情報，250 ページ
- 管理型 LNS の設定方法，252 ページ
- 管理型 IPv6 レイヤ 2 トンネリング プロトコル ネットワーク サーバの設定例，273 ページ
- その他の参考資料，278 ページ
- 管理型 IPv6 レイヤ 2 トンネリング プロトコル ネットワーク サーバの設定に関する機能情報，279 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

管理型 IPv6 LNS を設定するための前提条件

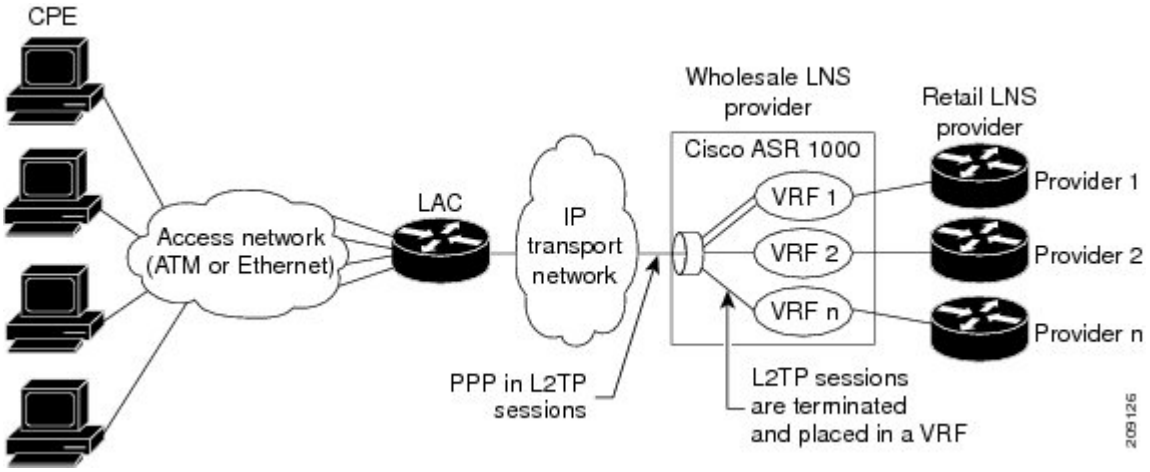
ルータを LNS として機能させるためには、レイヤ 2 トンネル プロトコル ネットワーク サーバ（LNS）とレイヤ 2 アクセス コンセントレータ （LAC）で認証、許可、およびアカウンティング（AAA）を有効にする必要があります。そのために、**aaanew-model** グローバル設定コマンドを入力します。詳細については、『*Cisco IOS XE Security: Securing User Services Configuration Guide* 』内の「Authentication, Authorization, and Accounting」の章を参照してください。

管理型 IPv6 LNS を設定するための情報

L2TP ネットワーク サーバ

ルータは LNS として機能します。LNS は LAC に対するピアで、L2TP トンネルの片側に位置します。LNS は LAC と宛先ネットワークとの間でパケットをルーティングします。ルータが LNS として機能しているときに、PPP セッションを終了し、最終的な宛先に向けてその ISP または社内ネットワークにクライアント IP パケットをルーティングするようにルータを設定できます（下の図を参照）。ルータは管理型 IPv6 LNS 機能を使用して LAC からの L2TP セッションを終了し、仮想テンプレート インターフェイスに適用した VRF、または AAA でユーザに対して取得した VRF に基づいて適切な IPv6 VRF インスタンスに、各セッションを配置することができます。ルータは、宛先ネットワークへ VRF 内の各セッションをルーティングします。

図 *10*：*LAC* からの転送セッションの終了



トンネル アカウンティング

トンネル アカウンティング機能により、RADIUS 情報内のトンネルに関連する統計情報を含む機能を追加することでAAAアカウンティングが強化されています。トンネルの使用状況に関する情報を取得する前に、RADIUS サーバで次の属性を設定する必要があります。

- Acct-Tunnel-Connection：トンネル セッションに割り当てられた識別子を特定します。この属性、および Tunnel-Client-Endpoint 属性と Tunnel-Server-Endpoint 属性により、監査の目的でトンネル セッションを一意に特定する手段が実現します。
- Acct-Tunnel-Packets-Lost：特定のリンク上で失われたパケット数を特定します。

以下のテーブルは、RADIUS サーバのトンネル アカウンティングをサポートする Acct-Status-Type 属性の値を示します。

表 *17*：*RADIUS* トンネル アカウンティングのための *Acct-Status-Type* 値

Acct-Status-Type 値	値	説明
Tunnel-Link-Reject	14	既存のトンネル内の新しいリンクの確立に対する拒否をマークします。
Tunnel-Link-Start	12	複数のリンクを伝送する L2TP トンネル内のトンネル リンクの作成をマークします。
Tunnel-Link-Stop	13	複数のリンクを伝送する L2TP トンネル内のトンネル リンクの廃棄をマークします。
Tunnel-Reject	11	別のデバイスとのトンネルの確立に対する拒否をマークします。
Tunnel-Start	9	別のデバイスとのトンネルの確立をマークします。
Tunnel-Stop	10	別のデバイスから、または別のデバイスへのトンネルの廃棄をマークします。

RADIUS トンネル アカウンティング属性、RADIUS トンネル アカウンティングをサポートする Acct-Status-Type 値に関しての詳細については、RFC 2867「RADIUS Accounting Modifications for Tunnel Protocol Support」を参照してください。

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでサポートされている RADIUS アカウンティング属性に関する情報については、『Cisco IOS XE Security Configuration Guide: Securing User Services』内の「RADIUS Attributes」の章を参照してください。

RADIUS の設定の詳細については、ご使用の RADIUS のユーザ マニュアルを参照してください。

管理型 LNS の設定方法

LNS での VRF の設定

手順の概要

1. **enable**
2. **configureterminal**
3. **vrfdefinition***vrf-name*
4. **rd***route-distinguisher*
5. **address-family** {**ipv4**|**ipv6**}
6. **route-target** {*import*|*export*|*both*} *route-target-ext-community*
7. **exit-address-family**
8. **address-family** {**ipv4**|**ipv6**}
9. **route-target** {*import*|*export*|*both*} *route-target-ext-community*
10. **end**
11. **showipv6routevrf***vrf-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**vrfdefinition***vrf-name* 例： `Router(config)# vrf definition vrf1`	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。 • *vrf-name* 引数は、VRF の名前です。
ステップ 4	**rd***route-distinguisher* 例： `Router(config-vrf)# rd 100:1`	VRF のルーティング テーブルと転送テーブルを作成します。 • *route-distinguisher* 引数によって、8 バイトの値が IPv4 プレフィックスに追加され、VPN IPv4 プレフィックスが作成されます。ルート識別子は、次のいずれかの形式で入力できます。 • 16 ビット ASN：101:3 などの 32 ビット数値 • 32 ビット IP アドレス：192.168.122.15:1 などの 16 ビット数値
ステップ 5	**address-family** {**ipv4**|**ipv6**} 例： `Router(config-vrf) address-family ipv6`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、VRF のアドレス ファミリを指定します。 • **ipv4** キーワードは、VRF の IPv4 アドレス ファミリを指定します。 • **ipv6** キーワードは、VRF の IPv6 アドレス ファミリを指定します。
ステップ 6	**route-target** {*import*|*export*|*both*} *route-target-ext-community* 例： `Router(config-vrf-af) route-target both 100:2`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • **import** キーワードを使用すると、ターゲット VPN 拡張コミュニティからルーティング情報がインポートされます。 • **export** キーワードを使用すると、ルーティング情報がターゲット VPN 拡張コミュニティにエクスポートされます。 • **both** キーワードを使用すると、ルーティング情報のターゲット VPN 拡張コミュニティからのインポート、およびターゲット VPN 拡張コミュニティへのエクスポートの両方が行われます。 • *route-target-ext-community* 引数により、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。

	コマンドまたはアクション	目的
ステップ 7	**exit-address-family** 例： `Router(config-vrf-af)# exit-address-family`	VRF アドレス ファミリ コンフィギュレーション モードを終了し、VRF コンフィギュレーション モードを開始します。
ステップ 8	**address-family** {**ipv4**|**ipv6**} 例： `Router(config-vrf) address-family ipv6`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、VRF のアドレス ファミリを指定します。 • **ipv4** キーワードは、VRF の IPv4 アドレス ファミリを指定します。 • **ipv6** キーワードは、VRF の IPv6 アドレス ファミリを指定します。
ステップ 9	**route-target** {*import*|*export*|*both*} *route-target-ext-community* 例： `Router(config-vrf-af)# route-target both 100:3`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • **import** キーワードを使用すると、ターゲット VPN 拡張コミュニティからルーティング情報がインポートされます。 • **export** キーワードを使用すると、ルーティング情報がターゲット VPN 拡張コミュニティにエクスポートされます。 • **both** キーワードを使用すると、ルーティング情報のターゲット VPN 拡張コミュニティからのインポート、およびターゲット VPN 拡張コミュニティへのエクスポートの両方が行われます。 • *route-target-ext-community* 引数により、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。 • **route-target** コマンドは、各ターゲット コミュニティにつき一度ずつ入力します。
ステップ 10	**end** 例： `Router(config-vrf-af)# end`	VRF アドレス ファミリ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 11	**showipv6routevrf***vrf-name* 例： `Router# show ipv6 route vrf vrf1`	VRF に関連付けられた IPv6 ルーティング テーブルを表示します。

仮想テンプレート インターフェイスの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacevirtual-template***number*
4. **vrfforwarding***name*
5. **pppauthenticationchap**
6. **end**
7. **showinterfacesvirtual-access***number***[configuration]**
8. **debugpppchap**
9. **debugpppnegotiation**
10. **debugpppnegotiationchap**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfacevirtual-template***number* 例： `Router(config)# interface virtual-template 1`	仮想テンプレートインターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**vrfforwarding***name* 例： `Router(config-if)# vrf forwarding vpn-1`	（オプション）仮想テンプレートインターフェイスをVRFルーティングテーブルにマッピングします。 （注） VRF の割り当てを RADIUS サーバを介して受信する場合、この手順は不要です。

	コマンドまたはアクション	目的
ステップ 5	**pppauthenticationchap** 例： `Router(config-if)# ppp authentication chap`	仮想アクセス インターフェイス（VAI）に適用される仮想テンプレートインターフェイスでCHAP認証を有効にします。
ステップ 6	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**showinterfacesvirtual-access***number***[configuration]** 例： `Router# show interfaces virtual-access number [configuration]`	指定の VAI のステータス、トラフィック データ、および設定情報を表示します。
ステップ 8	**debugpppchap** 例： `Router# debug ppp chap`	チャレンジ認証プロトコル（CHAP）パケット交換の認証プロトコル メッセージを表示します。 • このコマンドは、デバイス間の設定の不一致でCHAP認証が失敗した場合に役立ちます。ユーザ名とパスワードの不一致を確認し、修正することで問題が解決します。
ステップ 9	**debugpppnegotiation** 例： `Router# debug ppp negotiation`	PPPを実装するインターネットワークでのトラフィックおよび交換に関する情報を表示します。
ステップ 10	**debugpppnegotiationchap** 例： `Router# debug ppp negotiation chap`	Ciscoのデバイスと Cisco以外のデバイス間の接続の問題による CHAP ネゴシエーションの問題を分析します。

RADIUS サーバを介した VRF 割り当て

手順の概要

1. **enable**
2. **configureterminal**
3. **aaaauthorizationconfiguration***method-name***group***group-name*
4. **ipv6dhcppool***pool-name*
5. **prefix-delegationaaa** [**method-list***method-list*]
6. **dns-server***ipv6-address*
7. **exit**
8. **interfacevirtual-template***number*
9. **ipv6ndprefixframed-ipv6-prefix**
10. **ipv6dhcpserver***pool-name***rapid-commit**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaaauthorizationconfiguration***method-name***group***group-name* 例： `Router(config)# aaa authorization configuration DHCPv6-PD group DHCPv6-PD-RADIUS`	RADIUS を使用して AAA サーバから設定情報をダウンロードします。
ステップ 4	**ipv6dhcppool***pool-name* 例： `Router(config)# ipv6 dhcp pool DHCPv6-PD`	DHCP for IPv6 設定情報プールを設定し、DHCP for IPv6 プール コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**prefix-delegationaaa** [**method-list***method-list*] 例： `Router(config-dhcpv6)# prefix-delegation aaa method-list DHCPv6-PD`	プレフィックスを AAA サーバから取得することを指定します。
ステップ 6	**dns-server***ipv6-address* 例： `Router(config-dhcpv6)# dns-server 2001:0DB8:3000:3000::42`	IPv6 用の DHCP クライアントで使用できるドメイン ネーム システム（DNS）IPv6 サーバを指定します。
ステップ 7	**exit** 例： `Router(config-dhcpv6)# exit`	IPv6 用の DHCP プール コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 8	**interfacevirtual-template***number* 例： `Router(config)# interface virtual-template 1`	VAI の作成で動的に設定して適用できる仮想テンプレーインターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ipv6ndprefixframed-ipv6-prefix** 例： `Router(config-if)# ipv6 nd prefix framed-ipv6-prefix`	受信した RADIUS framed IPv6 prefix 属性のプレフィックスを、インターフェイスのネイバー探索プレフィックス キューに追加します。
ステップ 10	**ipv6dhcpserver***pool-name***rapid-commit** 例： `Router(config-if)# ipv6 dhcp server DHCPv6-PD rapid-commit`	インターフェイスに対して DHCPv6 をイネーブルにします。
ステップ 11	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

L2TP トラフィックを開始および受信するための LNS の設定

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnenable**
4. **vpdn-group***group-name*
5. **accept-dialin**
6. **protocol12tp**
7. **virtual-template***template-number*
8. **exit**
9. **terminate-fromhostname***hostname*
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnenable** 例： `Router(config)# vpdn enable`	ルータ上の VPDN ネットワーキングを有効にして、ローカル データベースおよび存在する場合にはリモート認可サーバ（ホームゲートウェイ）上でトンネル定義を検索するようにルータに指示します。
ステップ 4	**vpdn-group***group-name* 例： `Router(config)# vpdn-group group1`	他の VPDN 変数を割り当てることができるローカル グループ名を定義します。 • VPDN グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**accept-dialin** 例： `Router(config-vpdn)# accept-dialin`	LAC からトンネル化 PPP 接続を受け付ける LNS を設定し、accept-dialin VPDN サブグループを作成します。 • accept-dialin VPDN サブグループ コンフィギュレーション モードを開始します。
ステップ 6	**protocol12tp** 例： `Router(config-vpdn-acc-in)# protocol 12tp`	レイヤ 2 トンネル プロトコルを指定します。
ステップ 7	**virtual-template***template-number* 例： `Router(config-vpdn-acc-in)# virtual-template 1`	VAI のクローンを作成する際に使用される仮想テンプレートを指定します。
ステップ 8	**exit** 例： `Router(config-vpdn-acc-in)# exit`	VPDN グループ コンフィギュレーション モードに戻ります。
ステップ 9	**terminate-fromhostname***hostname* 例： `Router(config-vpdn)# terminate-from hostname lac1-vpn1`	VPDN トンネルの受け入れ時に必要なリモート LAC のホスト名を指定します。
ステップ 10	**end** 例： `Router(config-vpdn)# end`	VPDN コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トンネルごとのセッション数の制限

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdn-group***group-name*
4. **accept-dialin**
5. **protocol12tp**
6. **virtual-template***template-number*
7. **exit**
8. **terminate-fromhostname***host-name*
9. **session-limit***limit-number*
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdn-group***group-name* 例： `Router(config)# vpdn-group group1`	他の VPDN 変数を割り当てることができるローカル グループ名を定義します。 • VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	**accept-dialin** 例： `Router(config-vpdn)# accept-dialin`	LAC からトンネル化 PPP 接続を受け付ける LNS を設定し、accept-dialin VPDN サブグループを作成します。 • accept-dialin VPDN サブグループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**protocol12tp** 例： `Router(config-vpdn-acc-in)# protocol 12tp`	レイヤ 2 トンネル プロトコルを指定します。
ステップ 6	**virtual-template***template-number* 例： `Router(config-vpdn-acc-in)# virtual-template 1`	VAI のクローンを作成する際に使用される仮想テンプレートを指定します。
ステップ 7	**exit** 例： `Router(config-vpdn-acc-in)# exit`	VPDN グループ コンフィギュレーション モードに戻ります。
ステップ 8	**terminate-fromhostname***host-name* 例： `Router(config-vpdn)# terminate-from hostname test_LAC`	VPDN トンネルの受け入れ時に必要なリモート LAC のホスト名を指定します。
ステップ 9	**session-limit***limit-number* 例： `Router(config-vpdn)# session-limit 100`	トンネルごとの最大セッション数を指定します。
ステップ 10	**exit** 例： `Router(config-vpdn)# exit`	VPDN コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

RADIUS 属性の許可、拒否リストの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **aaaauthenticationpppdefaultgroup***group-name*
4. **aaaauthorizationnetworkgroupgroup***group-name*
5. **aaagroupserverradius***group-name*
6. **server-private***ip-address* [**acct-port***port-number*][**timeout***seconds*] [**retransmit***retries*] [**key***string*]
7. **authorization** [**accept**|**reject**] *list-name*
8. **exit**
9. **radius-serverattributelist***listname*
10. **attribute***value1* [*value2* [*value3...*]]
11. **end**
12. **showaccounting**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaaauthenticationpppdefaultgroup***group-name* 例： `Router(config)# aaa authentication ppp default group radius_authen1`	PPP を実行しているシリアル インターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
ステップ 4	**aaaauthorizationnetworkgroupgroup***group-name* 例： `Router(config)# aaa authorization network group group radius_authen1`	ユーザのネットワーク アクセスを制限するパラメータを設定します。

	コマンドまたはアクション	目的
ステップ 5	**aaagroupserverradius***group-name* 例： `Router(config)# aaa group server radius VPDN-Group`	異なる RADIUS サーバ ホストを別々のリストと方式にグループ化し、server group RADIUS コンフィギュレーション モードを開始します。
ステップ 6	**server-private***ip-address* [**acct-port***port-number*][**timeout***seconds*] [**retransmit***retries*] [**key***string*] 例： `Router(config-sg-radius)# server-private 10.1.1.2 acct-port 0 timeout 7 retransmit 3 key cisco1`	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。 • *ip-address* 引数は、プライベート RADIUS サーバ ホストの IP アドレスを指定します。 •（オプション）*port-number* 引数はアカウンティング要求のための UDP 宛先ポートを指定します。 •（オプション）*seconds* 引数はタイムアウト値を秒単位で指定します（1～1000）。 •（オプション）*retries* 引数はサーバが応答しない場合、またはサーバの応答が遅い場合に、RADIUS 要求がサーバに再送信される回数を指定します。 • *string* 引数はルータと RADIUS サーバ間のすべての RADIUS 通信用の認証および暗号キーを指定します。
ステップ 7	**authorization** [**accept**|**reject**] *list-name* 例： `Router(config-sg-radius)# authorization accept vpn1-autho-list`	RADIUS サーバから Access-Accept パケット内で返す属性用のフィルタを指定します。 • **accept** キーワードは、*listname* 引数で指定された属性を除く、すべての属性が拒否されることを意味します。 • **reject** キーワードは、*listname* 引数で指定された属性とすべての標準属性を除く、すべての属性が許可されることを意味します。
ステップ 8	**exit** 例： `Router(config-sg-radius)# exit`	サーバ グループ RADIUS コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	**radius-serverattributelist***listname* 例： `Router(config)# radius-server attribute list vpn1-autho-list`	**attribute** コマンドを使用して定義された属性のセットに付けるリスト名を定義し、RADIUS 属性リスト設定モードに入ります。 • 手順 7 の定義と同様に *listname* 引数を定義します。
ステップ 10	**attribute***value1* [*value2* [*value3...*]] 例： `Router(config-radius-attrl)# attribute 26,200`	設定した許可リストまたは拒否リストに属性を追加します。 • このコマンドは、許可リストまたは拒否リストに属性を追加するために何回も使用できます。
ステップ 11	**end** 例： `Router(config-radius-attrl)# end`	RADIUS 属性リスト設定モードを終了し、特権 EXEC モードに戻ります。
ステップ 12	**showaccounting** 例： `Router# show accounting`	現在ログインしているユーザのアカウンティング レコードが表示されます。 • ネットワーク上でアクティブなアカウント可能イベントを表示して、アカウンティング サーバ上でのデータ消失イベント時の情報収集を支援します。

名前付き方式リストによる AAA アカウンティングの設定

（注） システム アカウンティングは、名前付き方式リストを使用しません。システム アカウンティングの場合、デフォルトの方式リストだけが定義できます。詳細については、『Cisco IOS XE Security Configuration Guide: Securing User Services』の「Configuring Accounting」の章を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaaaccountingnetwork***list-name***start-stopgroupradius**
4. **line** [**aux** | **console**| **vty**] [*line-number*]
5. **accounting** {**arap**|**commands***level*|**connection**|**exec**|**resource**} [**default** | *list-name*]
6. **end**
7. **debugaaaaccounting**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaaaccountingnetwork***list-name***start-stopgroupradius** 例： `Router(config)# aaa accounting network methodlist start-stop group radius`	アカウンティング方式リストを作成し、アカウンティングを有効にします。
ステップ 4	**line** [**aux**	**console**| **vty**] [*line-number*] 例： `Router(config)# line console 0`	アカウンティング方式リストを適用する回線のライン コンフィギュレーション モードを開始します。
ステップ 5	**accounting** {**arap**|**commands***level*|**connection**|**exec**|**resource**} [**default**	*list-name*] 例： `Router(config-line)# accounting commands 15 list1`	1 つの回線または複数回線にアカウンティング方式リストを適用します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Router(config-line)# end`	回線コンフィギュレーションモードを終了します。続いて、特権 EXEC モードに戻ります。
ステップ 7	**debugaaaaccounting** 例： `Router# debug aaa accounting`	説明の義務があるイベントが発生したときに、その情報を表示します。

LNS の RADIUS トンネル認証方式リストの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa authorization network** *list-name method1* [*method2...*]
4. **vpdn tunnel authorization network** *lmethod-ist-name method1* [*method2...*]
5. **vpdn tunnel authorization virtual-template** *vtemplate-number*
6. **vpdn tunnel authorization password** *dummy-password*
7. **debug aaa authorization**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**aaa authorization network** *list-name method1* [*method2...*] 例： `Router(config)# aaa authorization network mymethodlist group VPDN-Group`	ネットワークへのユーザアクセスを制限するパラメータを設定します。 • *list-name* 引数は、ユーザがログインするときに試行される認証方式リストに名前を付けるときに使用する文字列です。 • **group radius**：すべての RADIUS サーバのリストを認証に使用します。 • **group** *group-name*：**aaa group server radius** コマンドで定義されている RADIUS サーバのサブセットを認証に使用します。 • **if-authenticated**：ユーザが正しく認証されると成功します。 • **local**：ローカルユーザ名データベースを認証に使用します。 • **none**：認証を使用しません。 （注） 方式リストはドメインおよび Digital Number Identification Service （DNIS）認証ではなく、VPDN トンネル認証と終了のためのみのものです。したがって方式リストは、トンネル終端デバイス、つまりダイヤルアウトセッションでは LAC 、ダイヤル イン セッションでは LNS のみに適用されます。
ステップ 4	**vpdn tunnel authorization network** *lmethod-ist-name method1* [*method2...*] 例： `Router(config)# vpdn tunnel authorization network mymethodlist`	VPDN リモート トンネル ホスト名ベースの認証で使用する AAA 認証方式リストを指定します。 • **vpdn tunnel authorization network** コマンドを使用して方式リストを指定しない場合（デフォルトの方式リストを含む）、ローカル認証はローカル VPDN グループの設定を使用して行われます。
ステップ 5	**vpdn tunnel authorization virtual-template** *vtemplate-number* 例： `Router(config)# vpdn tunnel authorization virtual-template 10`	VAI を複製するために使用するデフォルトの仮想テンプレート インターフェイスを指定します。 • ローカル VPDN グループ設定またはリモート RADIUS 設定で仮想テンプレートインターフェイスを指定しない場合は、デフォルトの仮想テンプレート インターフェイスが使用されます。
ステップ 6	**vpdn tunnel authorization password** *dummy-password* 例： `Router(config)# vpdn tunnel authorization password mypassword`	リモートトンネルのホスト名に基づいたトンネル設定を取得するための RADIUS 認証要求で使用するパスワードを指定します。

	コマンドまたはアクション	目的
ステップ 7	**debug aaa authorization** 例： `Router# debug aaa authorization`	AAA 認証に関する情報を表示します。

RADIUS トンネル認証用の LNS の設定

RADIUS トンネル認証用に LNS を設定するには、次のタスクを実行します。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、L2TP のトンネル認可がサポートされます。ただし、RADIUS では、l2tp tunnel timeout、l2tp tunnel hello 間隔、l2tp tunnel receive window サイズのようなパラメータ値の属性は提供されていません。Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、パラメータの RADIUS 属性を受信しません。ルータではデフォルト値を使用します。

LNS の RADIUS トンネル認証方式リストの設定

RADIUS トンネル認証用の方式リストを LNS に設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaaauthorizationnetwork***list-namemethod1* [*method2...*]
4. **vpdntunnelauthorizationnetwork***method-list-name*
5. **vpdntunnelauthorizationvirtual-template***vtemplate-number*
6. **vpdntunnelauthorizationpassword***dummy-password*
7. **end**
8. **debugaaaauthorization**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaaauthorizationnetwork***list-namemethod1* [*method2...*] 例： `Router(config)# aaa authorization network mymethodlist group VPDN-Group`	ネットワークへのユーザ アクセスを制限するパラメータを設定します。 • *list-name* 引数は、ユーザがログインするときに試行される認証方式リストに名前を付けるときに使用する文字列です。 • **groupradius**：すべての RADIUS サーバのリストを認証に使用します。 • **group***group-name*：**aaagroupserverradius** コマンドで定義されている RADIUS サーバのサブセットを認証に使用します。 • **if-authenticated**：ユーザが正しく認証されると成功します。 • **local**：ローカル ユーザ名データベースを認証に使用します。 • **none**：認証を使用しません。 （注） 方式リストはドメインおよび Digital Number Identification Service （DNIS）認証ではなく、VPDN トンネル認証と終了のためのみのものです。したがって方式リストは、トンネル終端デバイス、つまりダイヤルアウト セッションでは LAC 、ダイヤル イン セッションでは LNS のみに適用されます。

	コマンドまたはアクション	目的
ステップ 4	**vpdntunnelauthorizationnetwork***method-list-name* 例： `Router(config)# vpdn tunnel authorization network mymethodlist`	VPDN リモート トンネル ホスト名ベースの認証で使用する AAA 認証方式リストを指定します。 • **vpdntunnelauthorizationnetwork** コマンドを使用して方式リストを指定しない場合（デフォルトの方式リストを含む）、ローカル認証はローカル VPDN グループの設定を使用して行われます。
ステップ 5	**vpdntunnelauthorizationvirtual-template***vtemplate-number* 例： `Router(config)# vpdn tunnel authorization virtual-template 10`	VAI を複製するために使用するデフォルトの仮想テンプレート インターフェイスを指定します。 • ローカル VPDN グループ設定またはリモート RADIUS 設定で仮想テンプレート インターフェイスを指定しない場合は、デフォルトの仮想テンプレートインターフェイスが使用されます。 （注） **vpdntunnelauthorizationvirtual-template** コマンドは LNS にのみ適用されます。
ステップ 6	**vpdntunnelauthorizationpassword***dummy-password* 例： `Router(config)# vpdn tunnel authorization password mypassword`	リモート トンネルのホスト名に基づいたトンネル設定を取得するための RADIUS 認証要求で使用するパスワードを指定します。 • デフォルトのパスワードは cisco ですが、ほかのパスワードを設定できます。 （注） **vpdntunnelauthorizationpassword** コマンドは LAC、LNS 両方に適用できます。
ステップ 7	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 8	**debugaaaauthorization** 例： `Router# debug aaa authorization`	AAA 認証に関する情報を表示します。

AAA 認証方式の設定

手順の概要

1. **enable**
2. **configureterminal**
3. **aaanew-model**
4. RADIUS セキュリティ プロトコルのパラメータを設定します。RADIUS の詳細については、『Cisco IOS XE Security Configuration Guide: Securing User Services』の「Configuring RADIUS」の章を参照してください。
5. **aaaauthentication**
6. インターフェイス、単一または複数の回線に認証方法リストを適用します。認証方法リストの詳細については、『Cisco IOS XE Security Configuration Guide: Securing User Services』の「Configuring Authentication」の章を参照してください。
7. **end**

手順の詳細

ステップ 1 **enable**

ステップ 2 **configureterminal**

ステップ 3 **aaanew-model**
グローバル コンフィギュレーション モードでこのコマンドを入力し、AAA を有効にします。

ステップ 4 RADIUS セキュリティ プロトコルのパラメータを設定します。RADIUS の詳細については、『Cisco IOS XE Security Configuration Guide: Securing User Services』の「Configuring RADIUS」の章を参照してください。

ステップ 5 **aaaauthentication**
このコマンドを入力して、認証方式リストを定義します。

ステップ 6 インターフェイス、単一または複数の回線に認証方法リストを適用します。認証方法リストの詳細については、『Cisco IOS XE Security Configuration Guide: Securing User Services』の「Configuring Authentication」の章を参照してください。

ステップ 7 **end**

管理型 IPv6 レイヤ 2 トンネリング プロトコル ネットワーク サーバの設定例

例：管理型 IPv6 LNS の設定

次に、ルータでの管理型 IPv6 LNS の設定方法の例を示します。この例では、ルータは LAC からのトンネルを終了し、インターフェイスおよび仮想テンプレートインターフェイスに VRF を関連付けます。この設定は、RADIUS 属性のスクリーニングと VRF 用の AAA アカウンティングの設定の方法も示します。

```
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition user_vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv6
 exit-address-family
!
logging buffered 10000000
enable password lab
!
aaa new-model
!
!
aaa group server radius radius_authen1
 server-private 10.1.1.2 acct-port 0 timeout 7 retransmit 3 key cisco1
 ip radius source-interface Loopback20000
!
aaa authentication login default none
aaa authentication ppp default group radius_authen1
aaa authorization network default group radius_authen1
aaa authorization configuration DHCPv6-PD group radius_authen1
!
!
!
!
!
aaa session-id common
aaa policy interface-config allow-subinterface
ppp hold-queue 80000
clock timezone EST -5 0
ip source-route
no ip gratuitous-arps
!
!
!
!
!
!
!
no ip domain lookup
```

```
ip host mcp-matrix 10.0.0.2
ip host mcp-sun-2 10.0.0.2
!
!
ipv6 unicast-routing
ipv6 dhcp binding track ppp
ipv6 dhcp pool ipv6_dhcp_pool1
 prefix-delegation aaa method-list DHCPv6-PD
!
!
!
!
multilink bundle-name authenticated
vpdn enable
!
vpdn-group VPDN_LNS1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname test_LAC1
 source-ip 10.0.0.2
 local name test_LNS1
 l2tp tunnel password 0 tunnel1
 l2tp tunnel receive-window 100
 l2tp tunnel timeout no-session 30
 l2tp tunnel retransmit retries 7
 l2tp tunnel retransmit timeout min 2
!
!
no virtual-template snmp
!
!
!
!
!
!
!
!
!
username asifp1@test1 password 0 hello1
!
redundancy
 notification-timer 30000
 mode none
!
!
!
!
!
ip tftp source-interface GigabitEthernet 0
!
!
!
!
!
!
!
!
interface Loopback1
 no ip address
!
interface Loopback20000
 ip address 209.165.202.131 255.255.255.224
!
interface GigabitEthernet1/1/0
 mac-address 8888.8888.8888
 no ip address
 load-interval 30
 negotiation auto
 hold-queue 4096 in
 hold-queue 4096 out
!
interface GigabitEthernet1/1/0.1
```

```
 encapsulation dot1Q 3
 ip address 209.165.202.132 255.255.255.224
!
interface GigabitEthernet1/1/1
 mac-address 4444.4444.4444
 no ip address
 load-interval 30
 no negotiation auto
 hold-queue 4096 in
 hold-queue 4096 out
!
interface GigabitEthernet1/1/1.1
 vrf forwarding user_vrf1
 encapsulation dot1Q 2
 ipv6 address 12::1/72
!
interface GigabitEthernet1/1/2
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/3
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/4
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/5
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/6
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/7
 description Connected to RADIUS
 ip address 209.165.201.1 255.255.255.224
 negotiation auto
!
interface GigabitEthernet1/3/0
 no ip address
 media-type sfp
 negotiation auto
!
interface GigabitEthernet1/3/1
 no ip address
 media-type sfp
 negotiation auto
!
interface GigabitEthernet 0
 vrf forwarding Mgmt-intf
 ip address 209.165.201.1 255.255.255.224
 negotiation auto
!
interface Virtual-Template 1
 no ip address
 no logging event link-status
 ipv6 dhcp server ipv6_dhcp_pool1 rapid-commit
 keepalive 30
 ppp mtu adaptive
 ppp authentication pap
!
ip default-gateway 10.1.0.5
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 209.165.201.1 255.255.255.254 172.16.1.1
ip route vrf Mgmt-intf 209.165.201.29 255.255.255.224 172.16.0.1
!
ip radius source-interface GigabitEthernet1/1/7
```

```
logging esm config
cdp run
ipv6 route vrf user_vrf1 ::/0 12::2
!
ipv6 neighbor 12::2 GigabitEthernet1/1/1.1 2222.2222.2222
!
!
!
control-plane
!
call admission limit 90
!
!
!
alias exec call show caller summ
alias exec caller show caller summ
alias exec palt show plat
alias exec plat show platform
alias exec evsi sho plat hard cpp act feat ess stat
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password password1
!
exception data-corruption buffer truncate
end
```

例：LNS トンネル アカウンティングの設定

次の例は、トンネル アカウンティング レコードを RADIUS サーバに送信する LNS の設定方法を示しています。

```
aaa new-model
!
!
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$ftf.$wE6Q5Yv6hmQiwL9pizPCg1
!
username ENT_LNS password 0 tunnelpass
username user1@example.com password 0 lab
username user2@example.com password 0 lab
spe 1/0 1/7
firmware location system:/ucode/mica_port_firmware
spe 2/0 2/9
firmware location system:/ucode/mica_port_firmware
!
!
resource-pool disable
clock timezone est 2
!
ip subnet-zero
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 10.24.80.28 10.47.0.0
ip host dirt 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
!
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
```

```
terminate-from hostname ISP_LAC
local name ENT_LNS
!
isdn switch-type primary-5ess
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
interface Loopback 0
ip address 172.16.0.101 255.255.255.0
!
interface Loopback 1
ip address 192.168.0.101 255.255.255.0
!
interface Ethernet 0
ip address 10.1.26.71 255.255.255.0
no ip mroute-cache
no cdp enable
!
interface virtual-template 1
ip unnumbered Loopback 0
peer default ip address pool vpdn-pool1
ppp authentication chap
!
interface virtual-template 2
ip unnumbered Loopback1
peer default ip address pool vpdn-pool2
ppp authentication chap
!
interface fastethernet 0
no ip address
no ip mroute-cache
shutdown
duplex auto
speed auto
no cdp enable
!
ip local pool vpdn-pool1 172.16.5.1 172.16.128.100
ip local pool vpdn-pool2 10.0.0.1 10.0.0.100
ip default-gateway 10.1.26.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.26.254
ip route 192.168.1.2 255.255.255.255 10.1.26.254
no ip http server
ip pim bidir-enable
!
!
dialer-list 1 protocol ip permit
no cdp run
!
!
radius-server host 172.16.192.80 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
end
```

（注） アカウンティングのほかの例については、『Cisco IOS XE Security: Secure Services Configuration Guide』の「Configuring Accounting」の章を参照してください。

例：RADIUS サーバのユーザ プロファイルの確認

次は、RADIUS サーバのユーザ プロファイルの例です。Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、RADIUS サーバからユーザ プロファイルの情報を取得します。

```
Radius Profile "user1"
Auth-Type = Local, User-Password = "pwd"
User-Service-Type = Framed-User
Framed-Protocol = PPP
cisco-avpair = "lcp:interface-config=vrf forwarding VRF01"
cisco-avpair = "lcp:interface-config=ipv6 unnumbered loopback1"
Framed-IPv6-Prefix = "2001:DB8:4567:1234::/64"
Delegated-IPv6-Prefix = "2001:DB8:AAAA::/48"
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS XE MPLS コマンド	『*Cisco IOS MPLS* コマンド リファレンス』
認証、許可、アカウンティング	『認証、許可、アカウンティング（AAA）』
RADIUS の設定	『RADIUS の設定』
アカウンティングの設定	『Configuring Accounting』
RADIUS 属性	『*Cisco IOS XE Security Configuration Guide: Securing User Services*』内の「RADIUS Attributes Overview and RADIUS IETF Attributes」のモジュール

標準

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	—

MIB

MIB	MIB のリンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2867	『RADIUS Accounting Modifications for Tunnel Protocol Support』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

管理型 IPv6 レイヤ 2 トンネリング プロトコル ネットワーク サーバの設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *18*：管理型 *IPv6* レイヤ *2* トンネリング プロトコル ネットワーク サーバの機能情報

機能名	リリース	機能情報
管理型 IPv6 レイヤ 2 トンネリング プロトコル ネットワーク サーバ	Cisco IOS XE リリース 3.3S	管理型 IPv6 LNS 機能により、サービス プロバイダーは IPv4、IPv6 の両方のスケーラブルなエンドツーエンド VPN サービスをリモートユーザに提供することが可能になります。この機能は、マルチプロトコル ラベル スイッチング（MPLS）が有効になっているバックボーンにブロードバンド アクセスの機能を統合します。 次のコマンドが導入または変更されました。 atm pppatm passive、radius-server attribute list、radius-server key、radius-server retransmit、radius-server vsa send。
管理型 IPv6 Layer 2 Tunnel Protocol ネットワーク サーバ：VRF-Lite のみ	Cisco IOS XE リリース 3.3S	管理型 IPv6 LNS 機能により、サービス プロバイダーは IPv4、IPv6 の両方のスケーラブルなエンドツーエンド VPN サービスをリモートユーザに提供することが可能になります。この機能は、VRF-Lite が有効になっているバックボーンにブロードバンド アクセスの機能を統合します。
管理型 IPv6 Layer 2 Tunnel Protocol ネットワーク サーバ：MPLS VPN	Cisco IOS XE リリース 3.7S	管理型 IPv6 LNS 機能により、サービス プロバイダーは IPv4、IPv6 の両方のスケーラブルなエンドツーエンド VPN サービスをリモートユーザに提供することが可能になります。この機能は、MPLS が有効になっているバックボーンにブロードバンド アクセスの機能を統合します。

第 11 章

ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポート

ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポート機能では、IPv4 を介した ISDN PRI レイヤ 2 トンネリング プロトコル（L2TP）アクセス コンセントレータ（LAC）セッションを使用した、PPP 接続によるネットワークへのクライアント接続が提供されます。

このモジュールでは、ブロードバンド アグリゲーションに関する ISDN およびダイヤラ アクセスリンク サポートを設定する方法について説明します。

- 機能情報の確認，282 ページ
- ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの前提条件，282 ページ
- ブロードバンド アグリゲーションの ISDN/ダイヤラ アクセス リンク サポートの制約事項，282 ページ
- ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートに関する情報，283 ページ
- ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの設定方法，283 ページ
- ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの確認，292 ページ
- ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの設定例，293 ページ
- その他の参考資料，294 ページ
- ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの機能情報，296 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの前提条件

- ブロードバンドの ISDN サポートを設定する前に、レイヤ 2 トンネリング プロトコル（L2TP）ネットワークサーバ（LNS）を設定し、IPv4 を有効にする必要があります。
- 次回のリロード時に *adventerprise* ライセンスのアクティベーションを有効にして、ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポート機能が正しくインストールされていることを確認してください。

```
enable
 configure terminal
  license boot level adventerprise
end
```

ブロードバンド アグリゲーションの ISDN/ダイヤラ アクセス リンク サポートの制約事項

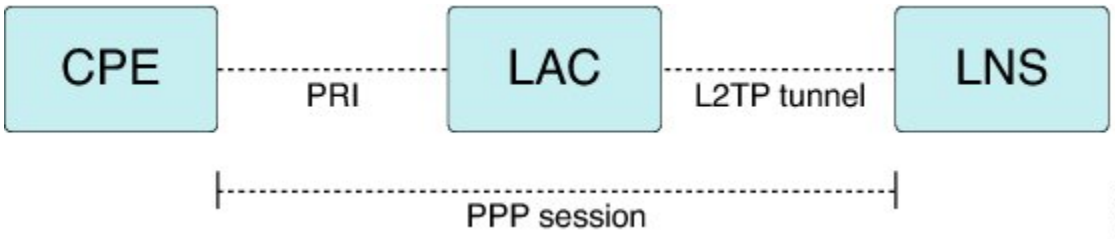
- レイヤ 2 トンネリング プロトコル（L2TP）バージョン 2 のトンネル内の IPv4 PPP セッションのみがサポートされます。
- ダイヤラ インターフェイスまたは d - チャネルインターフェイスでは ISDN 終端はサポートされていません。PPP 終了時の集約（PTA）を実現するには、ルータは L2TP アクセスコンセントレータ（LAC）として動作し、ISDN 着信を L2TP ネットワークサーバ（LNS）に転送する必要があります。

ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートに関する情報

ブロードバンドアグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの導入モデル

ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポート機能には、レイヤ 2 トンネリング プロトコル（L2TP）ネットワーク サーバ（LNS）のブロードバンド PPP IPv4 セッションへの ISDN とダイヤラの PRI アクセス リンクのサポートが提供されています。これらのセッションは、IPv4 を介した ISDN を使用した L2TP アクセス コンセントレータ（LAC）によって PPP を介して搬送されます。これらのセッションは、LAC から LNS に L2TP トンネルを通じて送信されます。LNS は PPP セッションを終了し、クライアントにネットワーク層アドレスを割り当てます。IPv4 パケット内のクライアント データは、次に ISP または企業のネットワークにルーティングされ、最終的な宛先に転送されます。LNS では、PPP セッションに対する認証、認可、およびアカウンティング（AAA）のアクションも実行されます。この導入モデルを次の図に示します。

図 *11*：トポロジ図



ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの設定方法

（注） ISDN スイッチ タイプをインターフェイスに設定するには、事前に **isdn switch-type** グローバル コンフィギュレーション コマンドを使用して、グローバル ISDN スイッチ タイプを設定する必要があります。グローバル コマンドは、インターフェイスレベル コマンドの前に処理されるため、最初にスイッチタイプをグローバルに追加していた場合を除き、コマンドパーサーはインターフェイスに対する **isdn switch-type** コマンドを受け付けません。

L2TP アクセス コンセントレータの設定

このタスクを実行して、バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）、レイヤ 2 トンネリング プロトコル（L2TP）、アクセス コンセントレータ（LAC）および ISDN スイッチ タイプを設定します。

手順の概要

1. **enable**
2. **configureterminal**
3. **vpdnenable**
4. **vpdn search-order domain dnis**
5. **vpdn-group***group-name*
6. **request-dialin**
7. **protocol l2tp**
8. **domain***domain-name*
9. **exit**
10. **initiate-to ip***ip-address*
11. **local name***host-name*
12. **l2tp tunnel password***password*
13. **exit**
14. **isdn switch-type***switch-type*
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vpdnenable** 例： `Device(config)# vpdn enable`	デバイスの VPDN を有効にします。

	コマンドまたはアクション	目的
ステップ 4	**vpdn search-order domain dnis** 例： `Device(config)# vpdn search-order domain dnis`	ネットワーク アクセス サーバ（NAS）またはトンネル スイッチが VPDN トンネル認証の検索を実行する方法を指定します。
ステップ 5	**vpdn-group***group-name* 例： `Device(config)# vpdn-group group1`	VPDN グループを作成し、カスタマーまたは VPDN プロファイルに関連付け、VPDN グループ設定モードを開始します。
ステップ 6	**request-dialin** 例： `Device(config-vpdn)# request-dialin`	ダイヤリング方向を示す request-dialin VPDN サブグループを作成し、トンネルを開始し、VPDN request-dialin グループコンフィギュレーションモードを開始します。
ステップ 7	**protocol l2tp** 例： `Device(config-vpdn-req-in)# protocol l2tp`	L2TP を VPDN サブグループで使用するトンネリング プロトコルとして指定します。
ステップ 8	**domain***domain-name* 例： `Device(config-vpdn-req-in)# domain xyz.com`	VPDN を使い、トンネルサーバへ転送されるユーザのドメイン名を指定します。
ステップ 9	**exit** 例： `Device(config-vpdn-req-in)# exit`	VPDN グループ コンフィギュレーション モードに戻ります。
ステップ 10	**initiate-to ip***ip-address* 例： `Device(config-vpdn)# initiate-to ip 192.0.2.55`	レイヤ 2 トンネリングで使用する IP アドレスを指定します。
ステップ 11	**local name***host-name* 例： `Device(config-vpdn)# local name host1`	トンネルが自己識別で使用するローカル ホスト名を指定します。
ステップ 12	**l2tp tunnel password***password* 例： `Device(config-vpdn)# l2tp tunnel password password1`	レイヤ 2 トンネリング プロトコル（L2TP）トンネルを認証するためにデバイスが使用するパスワードを設定します。

	コマンドまたはアクション	目的
ステップ 13	**exit** 例： `Device(config-vpdn)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	**isdn switch-type***switch-type* 例： `Device(config)# isdn switch-type primary-4ess`	PRI に対応するサービス プロバイダーのスイッチ タイプを選択します。 • この例では、ISDN スイッチ タイプは、primary-4ess です。
ステップ 15	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

PRI グループの設定

このタスクを実行して ISDN スイッチ タイプを指定し、PRI グループを設定します。

手順の概要

1. **enable**
2. **configureterminal**
3. **isdnswitch-type***switch-type*
4. **controller** {**T1** | **E1**} *slot*/*port*
5. **framing esf**
6. **linecode** {**ami** | **b8zs** | **hdb3**}
7. **cablelengthlong***db-gain-valuedb-loss-value*
8. **pri-grouptimeslots***timeslot-range*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**isdnswitch-type***switch-type* 例： `Device(config)# isdn switch-type primary-ni`	PRI に対応するサービス プロバイダーのスイッチ タイプを選択します。
ステップ 4	**controller** {**T1** | **E1**} *slot*/*port* 例： `Device(config)# controller T1 0/1`	コントローラ コンフィギュレーション モードを開始します。
ステップ 5	**framing esf** 例： `Device(config-controller)# framing esf`	T1 データ回線の Extended Super Frame（ESF）タイプを選択します。
ステップ 6	**linecode** {**ami** | **b8zs** | **hdb3**} 例： `Device(config-controller)# linecode b8zs`	T1 または E1 回線のライン コード タイプを選択します。 • Alternate Mark Inversion（AMI）は T1 回線のデフォルトです。 • Binary 8-Zero Substitution（B8ZS）は T1 コントローラのみで有効です。 • High-Density Bipolar 3（hdb3）は E1 回線のデフォルトです。
ステップ 7	**cablelengthlong***db-gain-valuedb-loss-value* 例： `Device(config-controller)# cablelength long gain36 0db`	T1 ケーブルでパルス均等化と線路補償を使い、レシーバで信号のパルスを拡大し、トランスミッタからのパルスを減少します。
ステップ 8	**pri-grouptimeslots***timeslot-range* 例： `Device(config-controller)# pri-group timeslots 1-2`	T1 または E1 コントローラの PRI グループが音声トラフィックを伝送するように設定します。 • 範囲を示すには、ハイフンを使用します。タイムスロットの範囲のグループをカンマ区切りで表記したもの（たとえば、1-4,8-23）も使用できます。 • PRI グループには、使用できるすべてのタイムスロットを含むよう設定できるほか、特定のグループのみを選択しての設定もできます。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-controller)# end`	特権 EXEC モードに戻ります。

ISDN PRI インターフェイス向けのダイヤラの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **interfaceserial***controller-number*:*time-slot*
4. **no ip address**
5. **dialer rotary-group***interface-number*
6. **dialer-group***group-number*
7. **exit**
8. **isdn switch-type***switch-type*
9. **isdn timer***timer milliseconds*
10. **isdn skipsend-idverify**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfaceserial***controller-number*:*time-slot* 例： `Device(config)# interface serial 0/1/7:23`	チャネル化 E1 コントローラまたはチャネル化 T1 コントローラで作成されたシリアル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**no ip address** 例： `Device(config-if)# no ip address`	既存の IP アドレスを削除するか、IP 処理を無効にします。
ステップ 5	**dialer rotary-group***interface-number* 例： `Device(config-if)# dialer rotary-group 100`	ダイヤラ ロータリー グループに指定したインターフェイスを加えます。
ステップ 6	**dialer-group***group-number* 例： `Device(config-if)# dialer-group group1`	特定のダイヤリング グループに属するようインターフェイスを設定して、アクセスを制御します。
ステップ 7	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**isdn switch-type***switch-type* 例： `Device(config)# isdn switch-type primary-4ess`	PRI に対応するサービス プロバイダーのスイッチ タイプを選択します。
ステップ 9	**isdn timer***timer milliseconds* 例： `Device(config)# isdn timer T321 30000`	ISDN タイマーを特定して設定し、ネットワーク、通話接続、切断待機期間のタイマーの値を変更します。
ステップ 10	**isdn skipsend-idverify** 例： `Device(config)# isdn skipsend-idverify`	ユーザ側 PRI インターフェイスからの ID 確認情報の送信を停止します。
ステップ 11	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

PPP 認証を有効化によるダイヤラ インターフェイスの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacedialer***dialer-rotary-group-number*
4. **no ip address**
5. **encapsulation***encapsulation-type*
6. **dialer in-band**
7. **dialer idle-timeout***seconds*
8. **dialer-group***group-number*
9. **no peer default ip address**
10. **ppp authentication***protocol1* [*protocol2...*][**if-needed** | *list-name* | **default** | **callin** | **one-time** | **optional**]
11. **exit**
12. **dialer-list***dialer-group***protocol***protocol-name* {**permit** | **deny** | **list***access-list-number* | **access-group**}
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfacedialer***dialer-rotary-group-number* 例： `Device(config)# interface dialer 100`	ダイヤラ ロータリー グループを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no ip address** 例： `Device(config-if)# no ip address`	既存の IP アドレスを削除するか、IP 処理を無効にします。

	コマンドまたはアクション	目的
ステップ 5	**encapsulation***encapsulation-type* 例： `Device(config-if)# encapsulation ppp`	インターフェイスで使用するカプセル化方式を設定します。
ステップ 6	**dialer in-band** 例： `Device(config-if)# dialer in-band`	ダイヤルオンデマンドルーティング（DDR）をサポートするよう指定します。
ステップ 7	**dialer idle-timeout***seconds* 例： `Device(config-if)# dialer idle-timeout 5000`	通話を切断するまでのアイドル時間を指定します。
ステップ 8	**dialer-group***group-number* 例： `Device(config-if)# dialer-group group1`	特定のダイヤリング グループに属するようインターフェイスを設定して、アクセスを制御します。
ステップ 9	**no peer default ip address** 例： `Device(config-if)# no peer default ip address`	インターフェイスのピア IP アドレス プーリング設定を無効にするか、または現在使用中の設定からデフォルトのアドレスを削除します。
ステップ 10	**ppp authentication***protocol1* [*protocol2...*][**if-needed** | *list-name* | **default** | **callin** | **one-time** | **optional**] 例： `Device(config-if)# ppp authentication chap callin`	少なくとも 1 つの PPP 認証プロトコルをイネーブルにして、インターフェイスでプロトコルが選択される順序を指定します。
ステップ 11	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**dialer-list***dialer-group***protocol***protocol-name* {**permit** | **deny** | **list***access-list-number* | **access-group**} 例： `Device(config)# dialer-list dialergroup1 protocol ip permit`	プロトコルによって、またはプロトコルと以前に定義したアクセス リストの組み合わせによって、ダイヤルするための DDR ダイヤラ リストを定義します。

	コマンドまたはアクション	目的
ステップ 13	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの確認

手順の概要

1. **enable**
2. **show ppp all**
3. **show vpdn**

手順の詳細

ステップ 1 **enable**
特権 EXEC モードをイネーブルにします。

例：

```
Device> enable
```

ステップ 2 **show ppp all**
PPP セッション情報を表示します。

例：

```
Device# show ppp all

Interface/ID OPEN+ Nego* Fail-     Stage    Peer Address    Peer Name
------------ -------------------- -------- --------------- --------------------
Se0/1/0:0    LCP+ CHAP*           Fwded    10.1.1.1         example@example.com
```

ステップ 3 **show vpdn**
すべてのアクティブなバーチャル プライベート ダイヤルアップ ネットワーク（VPDN）トンネルに関する基本情報を表示します。

例：

```
Device# show vpdn
```

```
L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocTunID   RemTunID   Remote Name   State  Remote Address  Sessn L2TP Class/
                                                          Count VPDN Group
46988      29813      o2-lns        est    192.0.2.55        1     1

LocID      RemID      TunID      Username, Intf/         State  Last Chg Uniq ID
                                 Vcid, Circuit
2300       46414      46988      example@e..., Se0/1/0:0  est    00:00:38 3
```

トラブルシューティングのヒント

ブロードバンドアグリゲーションに関する ISDN/ダイヤラ アクセス リンクのサポートのトラブルシューティングには、次のコマンドを使用します。

- **debug dialer**：ダイヤラ インターフェイスで受信したパケットについてのデバッグ情報を表示します。
- **debug isdn q931**：ローカル ルータ（ユーザ側）とネットワークの間でのコール セットアップおよび ISDN ネットワーク接続（レイヤ 3）のティアダウンに関する情報を表示します。
- **debug ppp authentication**：チャレンジ認証プロトコル（CHAP）パケット交換やパスワード認証プロトコル（PAP）交換を含む認証プロトコル メッセージを表示します。
- **debug ppp negotiation**：トラフィックの情報や、PPP の始動時に、PPP オプションをネゴシエートするときに送信された PPP パケットの交換に関する情報を表示します。

ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの設定例

例：L2TP アクセス コンセントレータの設定

次の例は、レイヤ 2 トンネリング プロトコル（L2TP）アクセス コンセントレータ（LAC）を設定する方法を示します。

```
Device(config)# vpdn enable
Device(config)# vpdn search-order domain dnis
Device(config)# vpdn-group group1
Device(config-vpdn)# request-dialin
Device(config-vpdn-req-in)# protocol l2tp
Device(config-vpdn-req-in)# domain xyz.com
Device(config-vpdn-req-in)# exit
Device(config-vpdn)# initiate-to ip 192.0.2.55
Device(config-vpdn)# local name host1
Device(config-vpdn)# l2tp tunnel password password1
```

```
Device(config-vpdn)# exit
Device(config)# isdn switch-type primary-4ess
```

例：PRI グループの設定

次の例は、スロット 0、ポート 1 に対し T1 コントローラー上で ISDN PRI を指定し、タイムスロット 1 から 2 を設定する方法を示しています。

```
Device(config)# isdn switch-type primary-ni
Device(config)# controller T1 0/1
Device(config-controller)# framing esf
Device(config-controller)# linecode b8zs
Device(config-controller)# cablelength long gain36 0db
Device(config-controller)# pri-group timeslots 1-2
```

例：ISDN PRI インターフェイス向けのダイヤラの設定

次の例は、ISDN PRI インターフェイス用にダイヤラ プロファイル設定を指定する方法を示します。

```
Device(config)# interface serial 0/1/7:23
Device(config-if)# no ip address
Device(config-if)# dialer rotary-group 100
Device(config-if)# dialer-group group1
Device(config-if)# exit
Device(config)# isdn switch-type primary-4ess
Device(config)# isdn timer T321 30000
Device(config)# isdn skipsend-idverify
```

例：PPP 認証を有効にしてのダイヤラ インターフェイスの設定

```
Device(config)# interface dialer 100
Device(config-if)# no ip address
Device(config-if)# encapsulation ppp
Device(config-if)# dialer in-band
Device(config-if)# dialer idle-timeout 5000
Device(config-if)# dialer-group group1
Device(config-if)# no peer default ip address
Device(config-if)# ppp authentication chap callin
Device(config-if)# exit
Device(config)# dialer-list dialergroup1 protocol ip permit
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
ブロードバンドと DSL のコマンド	『Cisco IOS Broadband Access Aggregation and DSL Command Reference』
ダイヤル コマンド	『Cisco IOS Dial Technologies Command Reference』
VPDN コマンド	『Cisco IOS VPDN Command Reference』
ブロードバンドと DSL の設定	『*Broadband Access Aggregation and DSL Configuration Guide*』
L2TP のテクニカル サポートのドキュメンテーション	『*Layer 2 Tunnel Protocol（L2TP）*』
PPP のテクニカル サポートのドキュメンテーション	『*Point-to-Point Protocol (PPP)*』

標準および RFC

標準/RFC	タイトル
RFC 1661	『*Point-to-Point Protocol (PPP)*』
RFC 2661	『レイヤ 2 トンネリング プロトコル（*L2TP*）』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ブロードバンド アグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *19*：ブロードバンド アグリゲーションに関する *ISDN*/ダイヤラ アクセス リンク サポートの機能情報

機能名	リリース	機能情報
ブロードバンドアグリゲーションに関する ISDN/ダイヤラ アクセス リンク サポート	Cisco IOS XE リリース 3.8S	ブロードバンド アグリゲーション機能に関する ISDN/ダイヤラ アクセス リンクのサポートは、IPv4 を介する ISDN PRI LAC セッションを使用して、PPP によるネットワークへのクライアントの接続を可能とします。