Access Node Control Protocol コンフィギュレーション ガイド、Cisco IOS XE Release 3S（ASR 1000）

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。

目 次

第 1 章

Access Node Control Protocol

Access Node Control Protocol（ANCP）機能は、デジタル加入者線アクセス マルチプレクサ（DSLAM）とブロードバンド リモート アクセス サーバ（BRAS）間の通信を強化し、マルチプレクサ側とサーバ側の間でのイベント、アクション、および情報要求の交換をイネーブルにします。 これにより、どちらの側でも適切なアクションを実装できます。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

Access Node Control Protocol の前提条件

伝送制御プロトコル（TCP）で ANCP を実行するには、ブロードバンド リモート アクセス サーバ（BRAS）で IP をイネーブルにする必要があります。 RADIUS から BRAS への相互作用は ANCP には必要なく、RADIUS サーバに依存します。

リリースおよびプラットフォーム サポートの詳細については、Access Node Control Protocol の機能情報, （16 ページ）を参照してください。

Access Node Control Protocol の制約事項

Cisco IOS XE Release 2.4 はブロードバンド リモート アクセス サーバ（BRAS）からの RADIUS サーバとの相互作用をサポートします。 RADIUS から BRAS への相互作用は ANCP には必要なく、RADIUS サーバに依存します。

Access Node Control Protocol の詳細

ANCP は、複数の加入者からのトラフィックを集約し、アプリケーションから独立した状態を保ちながら、任意のアプリケーションへの情報を渡します。 ANCP は、現在、デジタル加入者線（DSL）のブロードバンド環境の、DSLAM とブロードバンド リモート アクセス サーバ間のアプリケーションで使用されます。

ANCP 機能により、DSL Aggregation Multiplexer（DSLAM）とネットワーク エッジ デバイス間での閉じた通信が可能になります。 DSLAM と BRAS 間で ANCP を使用すると、イベント、アクション、および情報要求の交換が可能になり、その結果、適切なアクションが DSLAM および BRAS で行われるようになります。

ANCP のアーキテクチャは、ANCP の次の使用をサポートします。

レート アダプティブ モード

レート アダプティブ モードは、特定の回線の回線ビット レートの最大化を支援します。このレートは回線で達成される信号の質に依存します。 レート アダプティブ モードは、DSLAM からブロードバンド リモート アクセス サーバに DSL モデム回線レートを伝送します。

ANCP を実行している BRAS は ANCP ネイバー（DSLAM）からの TCP 要求をリッスンします。

- TCP セッションの確立後：ANCP は BRAS とそのネイバー間の隣接を確立するために、メッセージの交換を開始します。
- 隣接の確立後：ANCP イベント メッセージを DSLAM から BRAS へ送信できます。

レート アダプティブ DSL は回線速度を調整するために信号品質を使用します。 BRAS は、通常、サブスクライバ インターフェイスをサービス ライセンス契約（SLA）で同意した最大帯域幅に設定します。

顧客宅内機器（CPE）が、回線速度よりも遅いデータ レートに同期されると、セルまたはパケット損失が DSLAM で発生します。 これを防ぐために、DSLAM は新しく調整された回線レートの BRAS を通知するために ANCP を使用できます。

カスタマー側のポートの状態に応じて、次のようになります。

- アクティブ：DSLAM は、BRAS に Port Up メッセージを送信します。 適切な Quality Of Service（QoS）は、ANCP によって渡される情報に応じて有効になります。
- 非アクティブ：DSLAM は、BRAS に Port Down メッセージを送信します。 ANCP は、DSLAM から送信された DSL の状態を報告します。これは、通常、サイレントまたはアイドルです。ブロードバンド リモート アクセス サーバが別の Port Up メッセージを受信すると、加入者セッションはタイムアウトになるか、新しいシェーピング レートで更新されます。インターフェイスのシェーピング レートは、ルータが新しい Port Up メッセージを受信するまで変更されません。

RADIUS 相互作用

ブロードバンド リモート アクセス サーバと RADIUS サーバ間の相互作用は、ルータから RADIUS に向けられます。

BRAS は RADIUS サーバに次の属性および属性値ペア（AVP）を送信します。

ANCP ライン レート	アップストリーム データ レート	ダウンストリーム データ レート	出力ポリシー名
VSA 39	属性 197（Ascend-Data-Rate）	属性 255（Ascend-Xmit-Rate）	属性 77（Connect-Speed-Info）
	属性タイプ 38（Rx 接続速度 AVP）	属性タイプ 24（Tx 接続速度 AVP）	

BRAS は、認証、許可、アカウンティング（AAA）モジュールとのやり取りに、ポイントツーポイント プロトコル（PPPoE）を使用します。 RADIUS は情報を処理し、適切なアクションを実行します。

ポート マッピング

ポート マッピングは、BRAS の VLAN サブインターフェイスと DSLAM の顧客宅内機器（CPE）のクライアントを関連付けます。 VLAN には 802.1Q または queue-in-queue（Q-in-Q）階層型 VLAN が含まれます。 ポート マッピングは、特定の DSLAM ネイバーで CPE クライアント ID をグループ化して、BRAS でグローバル コンフィギュレーション モードで設定されます。

ポートをマッピングするために使用するための 2 つの方法があります。すべての VLAN サブインターフェイスを最初に設定し、ANCP ネイバー マッピングを次に設定する方法と、インターフェイスでマッピングを直接設定する方法があります。

たとえば、次のコマンドは、Q-in-Q VLAN サブインターフェイスのポート マッピングを設定します。

```
ancp neighbor name
dslam-name
id
dslam-id
dot1q

outer-vlanid
 second-dot1q

inner-vlanid
 [interface

type number
] client-id
 "
client-id
"
```

または

```
ancp neighbor name
dslam-name
id
 dslam-id
dot1q

outer-vlanid
 client-id
 "
client-id
"
```

client-id は、DSLAM が各ポートのために BRAS に送信する一意の access-loop-circuit-id です。 DSLAM は、ANCP Port Up イベント メッセージのこの ID を送信します。 access-loop-circuit-id は、次に示すように、アクセス ノード識別子およびデジタル加入者線（DSL）の情報から構成される定義された形式を使用します。

ATM/DSL

" *access-node-identifier* **atm** *slot/module/port* **.** *subinterface* **:** *vpi* **.** *vci* **"**

イーサネット/DSL

" *access-node-identifier* **ethernet** *slot* **/** *module* **/** *port* **.** *subinterface* [**:** *vlan-id*]**"**

BRAS は、DSLAM が Port Up メッセージを送るまで、ルータのすべてのポートのデフォルト ステートを Down に設定します。

非インタラクティブな運用、管理、および保守

ANCP は、ブロードバンド リモート アクセス サーバから運用、管理、および保守（OAM）の非インタラクティブ操作を実行するように、アウトオブバンド制御チャネルを提供します。 このチャネルにより、特定の DSLAM ポートの ANCP ポートの状態をルータ オペレータが確認できるようになります。 ANCP ポート ステート情報は、BRAS の ANCP ダイナミック データベースに保存されます。

インタラクティブ OAM

インタラクティブ OAM およびスケーリング強化機能は、運用とトラブルシューティングのために ANCP にオンデマンド ping 機能を追加します。

（注） この機能はデフォルトでイネーブルになり、設定は必要ありません。

General Switch Management Protocol および ANCP

ANCP は、General Switch Management Protocol（GSMP）を拡張したものです。 GSMP はマスター スレーブ ネイバー関係を定義します。ここで、マスターはスレーブへの接続を開始します。 ANCP では、このマスター スレーブ関係が反転します。BRAS（マスター）はDSLAM（スレーブ）からの着信 ANCP 接続をリッスンして受け入れます。 DSLAM はイベント メッセージを使用して、トポロジの変更や、ポート ダウン イベントまたはポート アップ イベントなどの BRAS への非同期イベントでの通信を行います。

BRAS と DSLAM 間の GSMP 接続は TCP/IP（RFC 3293）経由で発生します。 DSLAM はルータへの接続を開始し、ルータは、適切なインターフェイスで ANCP がイネーブルな場合は接続を受け入れます。

GSMP 隣接プロトコルは GSMP のネイバー関係を確立します。

1. 隣接を構築中に、次のように行われます。
    1. DSLAM およびルータが機能をネゴシエートし、2 つの端の同期状態が決まります。
    2. GSMP は、転送障害の場合にルータおよび DSLAM がローカルの情報データベースの状態を保持したかどうかや、両方のデバイスで状態更新が必要かどうかを検出します。
    3. 隣接を再同期化する必要があることが GSMP で判断された場合、隣接の同期プロセスが再開されます。これには、次の場所から入手可能な、ANCP 拡張ドラフトで定義されている機能ネゴシエーションが含まれます。

http://tools.ietf.org/id/draft-wadhwa-gsmp-l2control-configuration-02.txt

1. ANCP では、ネイバー（neighbor1）にそのネイバー（neighbor2）でサポートされていない機能が含まれている場合、neighbor1 はその機能をオフにして、neighbor2 と同じ機能セットで neighbor2 へのパケットを再通信します。
2. 両方のネイバーが同じ機能セットで同意すると、隣接関係が確立されます。

Access Node Control Protocol の設定方法

ANCP を設定するには、次のグローバルまたはインターフェイス コンフィギュレーション タスクを実行します。

イーサネット インターフェイスでの ANCP のイネーブル化

イーサネット インターフェイスで ANCP をイネーブルにするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ancp adjacency timer** *interval*
4. **interface** *type number*
5. **ip address** *address mask*
6. **ancp enable**
7. **interface** *type number* **.** *subinterface*
8. **encapsulation dot1q** *vlanid* [**second-dot1q** *second-vlanid*]
9. **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	**configure terminal** 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	**ancp adjacency timer** *interval* 例： `Router(config)# ancp adjacency timer 100`	ANCP 隣接タイマー間隔を設定します。これは、ANCP hello パケットを DSLAM に送信するまで待機する時間を示します。
ステップ 4	**interface** *type number* 例： `Router(config)# interface FastEthernet1/0/0`	インターフェイス コンフィギュレーション モードを開始してインターフェイスを定義します。

	コマンドまたはアクション	目的
ステップ 5	**ip address** *address mask* 例： `Router(config-if)# ip address 10.16.1.2 255.255.0.0`	IP アドレスとサブネットマスクをインターフェイスに割り当てます。
ステップ 6	**ancp enable** 例： `Router(config-if)# ancp enable`	IP が設定されているインターフェイスで ANCP をイネーブルにします。
ステップ 7	**interface** *type number . subinterface* 例： `Router(config-if)# interface FastEthernet1/0/0.1`	サブインターフェイスを定義するために、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**encapsulation dot1q** *vlanid* [**second-dot1q** *second-vlanid*] 例： `Router(config-subif)# encapsulation dot1q 100 second-dot1q 200`	単一キュー 802.1Q または Q-in-Q VLAN 階層型 VLAN のサブインターフェイスで dot1q VLAN カプセル化をイネーブルにします。
ステップ 9	**exit** 例： `Router(config-subif)# exit`	サブインターフェイス コンフィギュレーション モードを終了します。

ATM インターフェイスでの ANCP のイネーブル化

ancp enable コマンドは、DSLAM から ANCP メッセージを送信する制御 VC に対してのみ設定する必要があります。 ATM インターフェイス上で ANCP をイネーブルにするには、次の作業を行います。

手順の概要

1. **enable**
2. **configure terminal**
3. **ancp adjacency timer** *interval*
4. **interface atm** *slot* / *subslot* / *port* . *subinterface*
5. **ip address** *ip-address mask*
6. **pvc** *vpi* / *vci*
7. **ancp enable**
8. **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	**configure terminal** 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	**ancp adjacency timer** *interval* 例： `Router(config)# ancp adjacency timer 100`	ANCP 隣接タイマー間隔を設定します。これは、ANCP hello パケットを DSLAM に送信するまで待機する時間を示します。
ステップ 4	**interface atm** *slot* / *subslot* / *port* . *subinterface* 例： `Router(config)# interface atm 2/0/1.1`	サブインターフェイスを定義するために、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip address** *ip-address mask* 例： `Router(config-subif)# ip address 10.16.1.2 255.255.0.0`	IP アドレスおよびサブネットマスクをサブインターフェイスに割り当てます。

	コマンドまたはアクション	目的
ステップ 6	**pvc** *vpi* / *vci* 例： `Router(config-subif)# pvc 2/100`	ATM PVC を介した ANCP 接続をイネーブルにするために、ATM 仮想回線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	**ancp enable** 例： `Router(config-if-atm-vc)# ancp enable`	IP が設定されているインターフェイスで ANCP をイネーブルにします。
ステップ 8	**exit** 例： `Router(config-if-atm-vc)# exit`	ATM 仮想回線コンフィギュレーション モードを終了します。

ブロードバンド リモート アクセス サーバの VLAN インターフェイスへの DSLAM ポートのマッピング

BRAS の VLAN インターフェイスに DSLAM ポートをマッピングするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ancp atm shaper percent-factor** *factor*
4. **interface** *type number.subinterface*
5. **encapsulation dot1q** *vlan-id*
6. **ancp neighbor name** *dslam-name* [**id** *dslam-id*] **client-id** *client-id*
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	**configure terminal** 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	**ancp atm shaper percent-factor** *factor* 例： `Router(config)# ancp shaper percent-factor 95`	ATM U インターフェイス接続のために ANCP セルタックス アカウンティングをイネーブルにします。
ステップ 4	**interface** *type number.subinterface* 例： `Router(config)# interface FastEthernet0/0.1`	特定のサブインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**encapsulation dot1q** *vlan-id* 例： `Router(config-subif)# encapsulation dot1q 411`	指定された VLAN で、トラフィックの IEEE 802.1Q カプセル化をイネーブルにします。
ステップ 6	**ancp neighbor name** *dslam-name* [**id** *dslam-id*] **client-id** *client-id* 例： `Router(config-subif)# ancp neighbor name dslam1 id 1.2.3.4 client-id "1.2.3.4. eth 0/0.1"`	ANCP が、VLAN サブインターフェイスがマッピングされる DSLAM にアクセスするように指定します。
ステップ 7	**exit** 例： `Router(config-subif)# exit`	サブインターフェイス コンフィギュレーション モードを終了します。

ブロードバンド リモート アクセス サーバの PVC インターフェイスへの DSLAM ポートのマッピング

ancp neighbor name コマンドは、**pvc** および **pvc-in-range** コマンド モードで使用可能です。 このコマンドは、PVC と DSLAM ポート間の 1 対 1 マッピングを作成します。 BRAS の PVC インターフェイスに DSLAM ポートをマッピングするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ancp atm shaper percent-factor** *factor*
4. **interface atm** *slot* / *subslot* / *port* . *subinterface*
5. 次のいずれかを実行します。
   - **pvc** *vpi* / *vci*
   -
   - **range pvc** *start-vpi* / *start-vci* *end-vpi* / *end-vci*
6. **pvc-in-range** *vpi* / *vci*
7. **ancp neighbor name** *dslam-name* [**id** *dslam-id*] **client-id** *client-id*
8. **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	**configure terminal** 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	**ancp atm shaper percent-factor** *factor* 例： `Router(config)# ancp shaper percent-factor 95`	ATM U インターフェイス接続のために ANCP セル タックス アカウンティングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**interface atm** *slot* / *subslot* / *port* . *subinterface* 例： `Router(config)# interface atm 2/0/1.1`	指定した ATM サブインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 5	次のいずれかを実行します。
	• **pvc** *vpi* / *vci*
	•
	• **range pvc** *start-vpi* / *start-vci* *end-vpi* / *end-vci*
	
	例：
	`Router(config-subif)# pvc 1/101`
	
	例：
	
	例：
	`Router(config-subif)# range pvc 9/100 9/102`
		PVC と DSLAM ポートの間の 1 対 1 マッピングを作成し、ATM 仮想回線コンフィギュレーション モードを開始します。
		または
		ATM PVC の範囲を定義し、PVC 範囲コンフィギュレーション モードを開始します。
		• ATM PVC の範囲を定義した後は、個々の PVC を設定するために **pvc-in-range** コマンドを使用します。

ステップ 6	**pvc-in-range** *vpi* / *vci* 例： `Router(config-if-atm-range-pvc)# pvc-in-range 9/100`	（任意）PVC 範囲コンフィギュレーション モードで範囲内の個々の PVC を設定します。
ステップ 7	**ancp neighbor name** *dslam-name* [**id** *dslam-id*] **client-id** *client-id* 例： `Router(config-if-atm-range-pvc)# ancp neighbor name dslam1 id 1.2.3.4 client-id "1.2.3.4. atm0/0.1"`	ANCP が、PVC サブインターフェイスがマッピングされる DSLAM にアクセスするように指定します。 • このコマンドは、PVC 範囲コンフィギュレーション モードおよび ATM 仮想回線コンフィギュレーション モードで使用できます。
ステップ 8	**end** 例： `Router(config-if-atm-range-pvc)# end`	PVC 範囲コンフィギュレーション モードを終了します。

Access Node Control Protocol の設定例

イーサネット インターフェイスでの Access Node Control Protocol のイネーブル化の例

次に、イーサネット サブインターフェイス 2/0/1 で ANCP をイネーブルにする例を示します。

```
interface GigabitEthernet 2/0/1
 ip address 192.168.64.16 255.255.255.0
 ancp enable
!
interface GigabitEthernet 2/0/1.1
 encapsulation dot1q 100 second-dot1q 200
!
ancp adjacency timer 100
```

ATM インターフェイスでの Access Node Control Protocol のイネーブル化の例

次に、ATM サブインターフェイス 2/0/1.1 で ANCP をイネーブルにする例を示します。

```
interface ATM2/0/0.1 point-to-point
 description ANCP Link to one DSLAM
 no ip mroute-cache
 ip address 192.168.0.2 255.255.255.252
 pvc 254/32
   protocol ip 192.168.0.1
   ancp enable
   no snmp trap link-status
```

BRAS の VLAN インターフェイスへの DSLAM ポートのマッピング例

次に、DSLAM の CPE クライアント ポートを BRAS の Q-in-Q VLAN サブインターフェイスにマッピングする例を示します。 例では、192.68.10.5 の IP アドレスの dslam1 という名前の DSLAM ネイバーに、イーサネット インターフェイス 1/0/0.2 に設定された Q-in-Q VLAN 100 および 200 にマッピングされた CPE クライアント ポートがあります。 別の CPE クライアント ポートは、イーサネット インターフェイス 1/0/0.1 に設定された Q-in-Q VLAN 100 および 100 にマッピングされています。

```
interface GigabitEthernet1/0/0.1
 encapsulation dot1q 100 second-dot1q 100
 ancp neighbor name dslam1 id 192.168.10.5 client-id "192.168.10.5 ethernet1/0/0.2"
!
interface GigabitEthernet1/0/0.2
 encapsulation dot1q 100 second-dot1q 200
```

```
 ancp neighbor name dslam1 id 192.168.10.5 client-id "192.168.10.5 ethernet1/0/0.1"
!
ancp atm shaper percent-factor 95
!
```

上の例は、サブインターフェイス レベルでポートを直接マッピングします。また、次の例に示すように、すべての VLAN サブインターフェイスを最初に設定して、次に ANCP ネイバーでマッピングを実行します。

```
interface GigabitEthernet1/0/0.1
 encapsulation dot1q 100 second-dot1q 100
!
interface GigabitEthernet1/0/0.2
 encapsulation dot1q 100 second-dot1q 200
!
ancp atm shaper percent-factor 95
!
ancp neighbor name dslam1 id 192.168.10.5
 dot1q 100 second-dot1q 100 interface GigabitEthernet1/0/0.1 client-id "192.168.10.5
ethernet1/0/0.2"
!
ancp neighbor name dslam1 id 192.168.10.5
 dot1q 100 second-dot1q 200 interface GigabitEthernet1/0/0.2 client-id "192.168.10.5
ethernet1/0/0.2"
```

BRAS の PVC インターフェイスへの DSLAM ポートのマッピング例

ancp neighbor name コマンドは、DSLAM の CPE クライアント ポートを BRAS の PVC インターフェイスにマッピングします。 このコマンドは、グローバルに設定することも、または PVC/PVC-in-Range モードで設定することもできます。

PVC または PVC-in-Range コンフィギュレーション モード

この例で、ルータは、2 つのポートまたはクライアントを持つ 1 つの DSLAM と接続されます。

```
interface ATM2/0/0.1 point-to-point
  description ANCP Link to one DSLAM
  no ip mroute-cache
  ip address 192.168.0.2 255.255.255.252
  pvc 254/32
     protocol ip 192.168.0.1 255.255.255.252
     ancp neighbor name dslam1 id 192.168.10.5 client-id "dslam-port-x-identifier"
        no snmp trap link-status
      !
interface ATM1/0/0.1 multipoint
  description TDSL clients - default TDSL 1024
  class-int speed:ubr:1184:160:10
  range pvc 10/41 10/160
    service-policy input SET-PRECEDENCE-0
    service-policy output premium-plus:l2c:25088
    pvc-in-range 10/103
      description TDSL client 16 Mbps with ANCP
      class-vc speed:ubr:17696:1184:05
      ancp neighbor name dslam1 id 192.168.10.5 client-id "dslam-port-x-identifier"
       !
  range pvc 11/41 11/160
    service-policy input SET-PRECEDENCE-0
    service-policy output premium-plus:l2c:25088
    pvc-in-range 11/108
      description TDSL client 16 Mbps with ANCP
      class-vc speed:ubr:17696:1184:05
      ancp neighbor name dslam1 id 192.168.10.5 client-id "dslam-port-y-identifier"
        !
```

グローバル コンフィギュレーション モード

ancp neighbor コマンドがグローバルに設定される場合、次の例のように、ATM インターフェイスの PVC 情報も指定する必要があります。

```
interface ATM1/0/0.1 multipoint
 description TDSL clients - default TDSL 1024
 class-int speed:ubr:1184:160:10
 range pvc 10/41 10/160
   service-policy input SET-PRECEDENCE-0
   service-policy output premium-plus:l2c:25088
   pvc-in-range 10/103
     description TDSL client 16 Mbps with ANCP
     class-vc speed:ubr:17696:1184:05
!
 range pvc 11/41 11/160
   service-policy input SET-PRECEDENCE-0
   service-policy output premium-plus:l2c:25088
   pvc-in-range 11/108
     description TDSL client 16 Mbps with ANCP
     class-vc speed:ubr:17696:1184:05
!
ancp neighbor name dslam1 id 192.168.10.5
 atm 10/103 interface ATM1/0/0.1 client-id "dslam-port-x-identifier"
 atm 11/108 interface ATM1/0/0.1 client-id "dslam-port-y-identifier"
```

その他の関連資料

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』
ANCP コマンド	『*Cisco IOS Access Node Control Protocol Command Reference*』
IEEE 802.1Q VLAN	『Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation』
Queue-in-Queue VLAN タグ	『IEEE 802.1Q-in-Q VLAN Tag Termination』

RFC

RFC	タイトル
ANCP 拡張ドラフト	http://tools.ietf.org/id/draft-wadhwa-gsmp-l2control-configuration-02.txt 『GSMP Extensions for Access Node Control Mechanism』（インターネット ドラフト）

RFC	タイトル
RFC 3292	『*General Switch Management Protocol (GSMP) V3*』
RFC 3293	『General Switch Management Protocol (GSMP), Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP)』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 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

Access Node Control Protocol 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 リリースだけを示しています。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 *1*：***Access Node Control Protocol*** の機能情報

機能名	リリース	機能情報
Access Node Control Protocol	Cisco IOS XE Release 2.4	Cisco IOS XE Release 2.4 では、この機能が Cisco ASR 1000 に導入されました。 次のコマンドが導入されました。**ancp vdsl ethernet shaper**。
インタラクティブ OAM およびスケーリング強化	Cisco IOS XE Release 2.4	インタラクティブ OAM およびスケーリング強化機能は、運用とトラブルシューティングのために ANCP にオンデマンド ping 機能を追加します。 Cisco IOS XE Release 2.4 では、この機能が Cisco ASR 1000 に導入されました。 次のコマンドが導入または変更されました。**ping ancp**、**show ancp neighbor port**、**show ancp port**、**show ancp session**、**show ancp session adjacency**、**show ancp session event**、および **show ancp statistics**。

第 2 章

Access-Acceptメッセージでのマルチサービスのアクティブ化

Access-Accept メッセージでのマルチサービスのアクティブ化機能は、Access Node Control Protocol（ANCP）の一部であり、単一の RADIUS Access-Accept メッセージに複数のサービスを含めることが可能です。この機能は、認可変更（CoA）メッセージでのマルチサービスのアクティブ化および非アクティブ化機能に似ていますが、この場合、要求されたすべてのサービス アクティブ化は自動的に処理されます。 サービスのアクティブ化が失敗した場合、以降のサービスのアクティブ化は処理されず、Access-Accept メッセージによってすでにアクティブ化されたすべてのサービスは、非アクティブ化されます。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

Access-Acceptメッセージでのマルチサービスのアクティブ化の制約事項

- サービスのアクティブ化の 1 つが失敗した場合、Access-Accept メッセージからのすべての処理されていないサービスは無視され、アクティブ化された Access-Accept メッセージのすべてのサービスが非アクティブ化されます。
- Access-Accept メッセージのサービスによって Quality of Service（QoS）ポリシーを適用する場合、2 段階の適用プロセスがあります。 最初の段階では、ポリシーを解析し、データプレーンにポリシー値を送信します。 第 2 段階では、データプレーンへの QoS ポリシーの適用を行います。 第 1 段階が正常に完了し、第 2 段階が失敗したインスタンスでは、関連するサービスで、アクティベーションが成功したことを示す場合があります。

Access-Acceptメッセージでのマルチサービスのアクティブ化に関する情報

Access-Accept メッセージでのマルチサービスのアクティブ化の概要

Access-Request メッセージが RADIUS クライアントによって RADIUS サーバに送信され、メッセージに含まれるユーザまたは加入者のプロファイルが認証されます。 ユーザまたは加入者のプロファイルは、次のようになります。

- 受け入れ可能：RADIUS サーバが Access-Accept メッセージを返す可能性があります。
- 受け入れ不可：RADIUS サーバが Access-Reject メッセージを返す可能性があります。

マルチサービスのアクティブ化をイネーブルにするには、Access-Accept メッセージに、アクティブ化するサービス名を指定した、複数の Cisco generic VSA 250（SSG_ACCOUNT_INFO）エントリが含まれることがあります。

RSIM フォーマット

```
vsa cisco generic 250 string "Aservice-name1"
vsa cisco generic 250 string "Aservice-name2"
vsa cisco generic 250 string "Aservice-name3"
```

RADIUS フォーマット

```
07:06:23.234: RADIUS: Received from id 1645/36 11.12.13.2:1645, Access-Accept, len 112
07:06:23.238: RADIUS:  authenticator 92 C5 A2 F2 24 56 37 1E - 74 F4 C6 92 B0 E8 92 4C
07:06:23.238: RADIUS:  Vendor, Cisco       [26]  23
07:06:23.238: RADIUS:   ssg-account-info   [250] 17  "Aservice-name-1"
07:06:23.238: RADIUS:  Vendor, Cisco       [26]  23
07:06:23.238: RADIUS:   ssg-account-info   [250] 17  "Aservice-name-2"
07:06:23.238: RADIUS:  Vendor, Cisco       [26]  23
07:06:23.238: RADIUS:   ssg-account-info   [250] 17  "Aservice-name-3"
```

Access-Accept メッセージを受信すると、指定したサービスが取得され、各サービスは継続的にアクティブ化されます。 サービスのアクティブ化に失敗すると、Access-Accept メッセージからのすべての処理されていないサービスは無視され、アクティブ化された Access-Accept メッセージ内のサービスは非アクティブ化されます。

（注） QoS サービスに対する Access-Accept の複数サービス要求の RSIM 形式は、CoA メッセージの複数のサービスのアクティブ化または非アクティブ化要求には適用できません。 CoA メッセージの形式は VSA 252 です。 詳細については、「CoA メッセージでのマルチサービスのアクティブ化および非アクティブ化」のモジュールを参照してください。

VSA 250 の QoS ポリシー

セッションを確立している間、RADIUS Access-Accept メッセージで VSA 250 の連結 QoS 構文を使用できます。 この構文は、VSA 連結文字列を解析し、QoS と Intelligent Services Gateway（ISG）ポリシーをアクティブ化します。

（注） ISG は、1 つの Access-Accept メッセージで複数の QoS サービスを管理し、スタティックでパラメータ化された QoS をアクティブ化するためにメッセージを適用します。

Access-Acceptメッセージでのマルチサービスのアクティブ化の設定方法

Access-Accept を使用したセッション サービスのアクティブ化

Access-Accept を使用してセッション サービスを動的にアクティブ化するために、RADIUS のサービス プロファイルの Cisco VSA 250 を設定します。 RADIUS は次の構文で Access-Accept メッセージの VSA 250 を使用します。

RSIM フォーマット

```
vsa cisco generic 250 string
"Aservice-name-1"
```

Access-Accept メッセージのマルチサービスの設定例

VSA 250 を使用した QoS サービスのアクティブ化の例

QoS サービスをアクティブ化するには、RADIUS Access-Accept メッセージで *qos:vc-qos-policy-out* 構文を使用します。 連結文字列は解析され、QoS と ISG ポリシーがアクティブ化されます。

次の例は、VSA 250 連結文字列の解析と、ISG サービスおよび QoS ポリシーのアクティブ化を定義します。

qos:<qos-attribute-name>=<attribute value>[;qos:<qos-attribute-name>=<attribute value>...]

qos-attribute-name	QoS 属性名を表示します。 この特別な連結形式で QoS 属性名として受け入れられる属性は次のとおりです。 vc-qos-policy-in vc-qos-policy-out vc-weight vc-watermark-min vc-watermark-max
attribute value	QoS 属性に割り当てる値を表示します。 受け入れられる値の範囲はプラットフォームによって決まります。

ターゲット セッションが ATM VC の場合、vc-weight、vc-watermark-min、および vc-watermark-max の属性が解釈されます。

次に、VSA 250 の連結 QoS 構文の例を示します。

vsa cisco generic 250 string "Aqos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in"

その他の関連資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
ANCP コマンド	『Cisco IOS Access Node Control Protocol Command Reference』
IEEE 802.1Q VLAN	Cisco IOS IEEE 802.1Q サポート フィーチャ モジュール
Access-Node 制御プロトコル	『Metro Ethernet WAN Services and Architectures』（ホワイト ペーパー）、Access Node Control Protocol
Queue-in-Queue VLAN タグ	『IEEE 802.1Q-in-Q VLAN Tag Termination』

RFC

RFC	タイトル
ANCP 拡張ドラフト	『GSMP Extensions for Access Node Control Mechanism』（インターネット ドラフト）
RFC 3292	『*General Switch Management Protocol (GSMP) V3*』
RFC 3293	『*General Switch Management Protocol (GSMP), Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP)*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 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

Access-Acceptメッセージでのマルチサービスのアクティブ化の機能情報

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 リリースだけを示しています。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 *2* : ***Access-Accept*** メッセージでのマルチサービスのアクティブ化の機能情報

機能名	リリース	機能情報
Access-Accept メッセージでのマルチサービスのアクティブ化	Cisco IOS XE Release 2.4	Access-Accept メッセージでのマルチサービスのアクティブ化機能は、RADIUS Access-Accept メッセージを使用した複数サービスの動的なアクティブ化をサポートします。 この機能は、Cisco IOS XE 2.4 で、Cisco ASR 1000 シリーズルータに導入されました。 次のコマンドが、この機能によって変更されました。**subscriber service multiple-accept**。

第 3 章

CoA メッセージでのマルチサービスのアクティブ化および非アクティブ化

この機能では、ポリシーサーバから送信される単一の認可変更（CoA）メッセージによって、複数のサービスをアクティブ化または非アクティブ化することができます。 この機能は、Access Accept メッセージでのマルチサービスのアクティブ化機能に似ていますが、この場合は、ユーザセッションがすでにアクティブであると見なされています。

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。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

CoA メッセージでのマルチサービスのアクティブ化および非アクティブ化の制約事項

- マルチサービスのアクティブ化または非アクティブ化メッセージに含まれるすべてのサービス名は、Intelligent Services Gateway（ISG）対応である必要があります。 たとえば、これらは、class-map タイプのサービス「service1」である必要があります。
- サービスのアクティブ化または非アクティブ化メッセージのうちの 1 つが失敗した場合、ブロードバンド リモート アクセス サーバ（BRAS）は、前回正常にアクティブ化または非アクティブ化されたサービスと、同じマルチサービスのアクティブ化または非アクティブ化CoA メッセージに含まれるサービスのみをロールバックします。
- ただし、現在の ISG 実装には、以前にアクティブ化または非アクティブ化されたサービスの状態を再確立するプロセスに制限があります。 たとえば、重複が可能な機能が同じセッションでイネーブルの場合、正常にアクティブ化または非アクティブ化された新しい機能パラメータは、そのセッションですでにアクティブ化されていた同じ機能の古いパラメータを削除します。 その機能の古いパラメータを再確立しようとする試みは失敗します。
- 有効な CLI で設定された ISG サービスが CoA によって新しいセッションに転送されて失敗すると（ISG サービスがアカウンティング リストを検索できない）、次のようになります。
  - BRAS は、ハードウェアのプロビジョニングを待機しません。
  - ACK メッセージがリレーされます。
  - ISG サービスは適用されません。
  - トレースバックが見られます。

CoA メッセージでのマルチサービスのアクティブ化および非アクティブ化に関する情報

CoA メッセージでのマルチサービスのアクティブ化および非アクティブ化の概要

CoA マルチサービスのアクティブ化または非アクティブ化メッセージには、サービスのリストが含まれます。 複数のサービスが、VSA 252 の複数行の形式で一覧されます。

1 つの CoA メッセージでマルチサービスを非アクティブ化する場合、RADIUS サーバは、1 つの CoA マルチサービス非アクティブ化メッセージで、複数のサービスを非アクティブ化する要求を送信します。マルチサービス非アクティブ化メッセージに表示される各サービスについて、BRAS がサービスを非アクティブ化します。 サービスが正常に非アクティブ化されると、アカウンティング終了メッセージが続きます。

サービスを正常に非アクティブ化できない場合、BRAS はマルチサービス アクティブ化メッセージに含まれるすべての後続サービスの非アクティブ化を中断します。 失敗したサービスがアクティブ化される前に、BRAS では、同じマルチサービス アクティブ化メッセージ内の、正常に非アクティブ化されたすべてのサービスをアクティブ化します。

1 つのマルチサービスのアクティブ化または非アクティブ化 CoA メッセージを形成するために、既存の VSA 252 が使用されます。 1 つのマルチサービスのアクティブ化または非アクティブ化 CoA メッセージを形成するために、メッセージに複数行の VSA 252 が含められます。 次に、1 つの CoA メッセージにマルチサービスのアクティブ化または非アクティブ化が混在する例を示します。

RADIUS フォーマット

```
ISG#
00:41:15: RADIUS: CoA  received from id 76 10.168.1.6:1700, CoA Request, len 67
00:41:15: CoA: 10.168.1.6 request queued
00:41:15: RADIUS:  authenticator C4 AC 5D 50 6A BE D7 00 - F9 1D FA 38 15 32 25 3A
00:41:15: RADIUS:  Vendor, Cisco       [26]  18
00:41:15: RADIUS:   ssg-account-info   [250] 12  "S151.1.1.2"
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0B 70 6F 6C 69 63 65 31           [Service-Log-On service1]
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0B 70 6F 6C 69 63 65 32           [Service-Log-On service2]
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0C 73 65 72 76 69 63 65 33        [Service-Log-Off service3]
00:41:15: RADIUS:  Vendor, Cisco       [26]  17
00:41:15: RADIUS:   ssg-command-code   [252] 11
00:41:15: RADIUS:   0B 70 6F 6C 69 63 65 34           [Service-Log-On service4]
```

VSA 252 の QoS ポリシー

RADIUS CoA メッセージに VSA 252 連結 Quality of Service（QoS）構文を使用できます。 この構文は、VSA 252 連結文字列を解析して、ISG サービスおよび QoS ポリシーをアクティブ化または非アクティブ化するために使用されます。

（注） ISG は、1 つの CoA メッセージで複数の QoS サービスを管理し、スタティックでパラメータ化された QoS をアクティブ化するためにメッセージを適用します。

CoA メッセージでのマルチサービスのアクティブ化および非アクティブ化の設定方法

CoA を使用したセッション サービスのアクティブ化

CoA を使用してセッション サービスを動的にアクティブ化するために、RADIUS のサービス プロファイルの Cisco VSA 252 を設定します。 RADIUS は次の構文で CoA メッセージの VSA 252 を使用します。

```
vsa cisco generic 252 binary 0b suffix
"qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in;;"
```

この例の CoA コマンドでは、次のアクションが実行されます。

- ISG サービス「qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in;;」を開始します。
- 仮想テンプレート IPOne_out のデフォルト QoS 出力子ポリシーを置き換え、仮想テンプレートにデフォルトの出力子ポリシーがない場合は、IPOne_out ポリシーをインストールします。
- 仮想テンプレート IPOne_in のデフォルト QoS 入力子ポリシーを置き換え、仮想テンプレートに設定されているデフォルトの入力子ポリシーがない場合は、IPOne_in ポリシーをインストールします。

CoA を使用したセッション サービスの非アクティブ化

CoA を使用してセッションを動的にアクティブ化し、仮想テンプレートの QoS ポリシーをデフォルト設定するには、RADIUS サービス プロファイルの Cisco VSA 252 を設定します。 RADIUS は次の構文で CoA メッセージの VSA 252 を使用します。

```
vsa cisco generic 252 binary 0c suffix
"qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in;;"
```

この例の CoA コマンドでは、次のアクションが実行されます。

- ISG サービス「qos:vc-qos-policy-out=IPOne_out;qos:vc-qos-policy-in=IPOne_in」を終了します。
- QoS 出力子ポリシー IPOne_out を、適切な仮想テンプレート インターフェイスに設定されたデフォルトの子ポリシーと置き換えます。
- QoS 入力子ポリシー IPOne_in を、適切な仮想テンプレート インターフェイスに設定されたデフォルトの子ポリシーと置き換えます。

CoA メッセージでのマルチサービスのアクティブ化および非アクティブ化の設定例

VSA 252 を使用した QoS サービスのアクティブ化および非アクティブ化の例

QoS サービスをアクティブ化するために、RADIUS は 1 つの VSA 252 文字列の親と子ポリシーに 1 つ以上の複数 QoS クラスを追加し、次の構文をリレーします。

```
CoA VSA 252 0b <new service>
```

既存のサービスに加えて、新しいサービスをインストールし、現在のサービスとクラスが重複しないようにする必要があります。

次に、QoS アクティブ化を定義し、パラメータ化された QoS サービスの RADIUS フォームで QoS クラスを追加する例を示します。

```
VSA252 0b q-p-out=IPOne1-isg-acct_service(1)((c-d,voip)1(200000,9216,0,1,0,0)10(9));q-p-in=
 ((c-d,voip)1(200000,9216,0,1,0,0)10(9))
```

2 つ目のサービスを非アクティブ化するために、RADIUS はサービスのアクティブ化に使用されたのと同じ VSA 252 文字列を「0b」を「0c」に置き換えてリレーします。

次に、QoS 非アクティブ化を定義し、パラメータ化された QoS サービスの RADIUS フォームで QoS クラスを削除する例を示します。

```
VSA252 0c q-p-out=IPOne1-isg-acct_service(1)((c-d,voip)1(200000,9216,0,1,0,0)10(9));q-p-in=
 ((c-d,voip)1(200000,9216,0,1,0,0)10(9))
```

その他の関連資料

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』
ANCP コマンド	『*Cisco IOS Access Node Control Protocol Command Reference*』
IEEE 802.1Q VLAN	『Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation』
Queue-in-Queue VLAN タグ	『IEEE 802.1Q-in-Q VLAN Tag Termination』

RFC

RFC	タイトル
ANCP 拡張ドラフト	『GSMP Extensions for Access Node Control Mechanism』（インターネット ドラフト）
RFC 3292	『*General Switch Management Protocol (GSMP) V3*』
RFC 3293	『*General Switch Management Protocol (GSMP), Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP)*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 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

CoA メッセージでのマルチサービスのアクティブ化および非アクティブ化の機能情報

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 リリースだけを示しています。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 *3* : ***CoA*** メッセージでのマルチサービスのアクティブ化および非アクティブ化の機能情報

機能名	リリース	機能情報
CoA メッセージでのマルチサービスのアクティブ化および非アクティブ化	Cisco IOS XE Release 2.4	CoA メッセージでのマルチサービスのアクティブ化および非アクティブ化機能は、RADIUS CoA メッセージを使用した複数のサービスの動的なアクティブ化および非アクティブ化をサポートします。 この機能は、Cisco IOS XE 2.4 で、Cisco ASR 1000 シリーズ ルータに導入されました。