RADIUS 属性の構成ガイド

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。

目 次

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

現行の Cisco IOS XE リリース 3.7.0E（Catalyst スイッチ用）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、1 つのバージョンの統合されたリリース（Cisco IOS XE 16）へと発展しています。これにより、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範囲のアクセスおよびエッジ製品に 1 つのリリースで対応できます。

（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

『RADIUS Attributes Overview and RADIUS IETF Attributes』

Remote Authentication Dial-In User Service（RADIUS）属性は、RADIUS プログラムに保存されたユーザ プロファイル内の特定の認証、認可、およびアカウンティング（AAA）要素を定義するために使用されます。この章では、サポートされる RADIUS 属性を示します。

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。

RADIUS 属性の概要

IETF 属性と VSA の比較

RADIUS インターネット技術特別調査委員会（IETF）属性は、255 個の標準属性で構成されるオリジナルのセットで、クライアントとサーバ間での AAA 情報の伝達に使用されます。IETF 属性は標準であり、属性のデータは事前に定義されています。IETF 属性を使用して AAA 情報を交換するクライアントとサーバは、属性の正確な意味や各属性値の一般的な範囲など、属性データについて合意する必要があります。

RADIUS ベンダー固有属性（VSA）は、ベンダー固有 IETF 属性（属性 26）に由来しています。属性 26 を使用して、ベンダーは 255 種の属性を追加作成できます。つまり、ベンダーは、IETF 属性のデータとは異なる属性を作成して、属性26の背後でカプセル化することができます。新しく作成された属性は、ユーザが属性 26 を受け入れる場合に受信されます。

VSA の詳細については、「RADIUS ベンダー固有属性および RADIUS Disconnect-Cause 属性値」の章を参照してください。

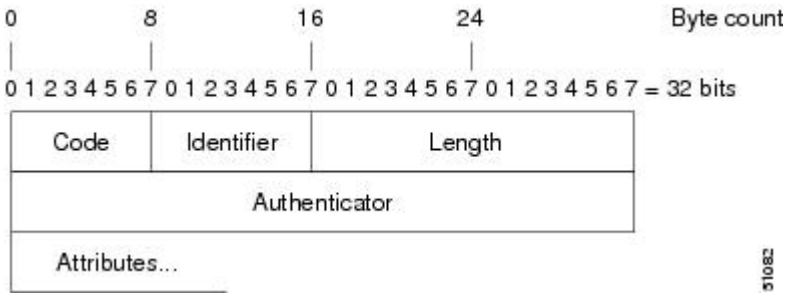
RADIUS パケットのフォーマット

RADIUS サーバと RADIUS クライアント間のデータは、RADIUS パケットで交換されます。データ フィールドは左から右に転送されます。

次の図に、RADIUS パケット内のフィールドを示します。

（注） VSA の図については、「RADIUS ベンダー固有属性および RADIUS Disconnect-Cause 属性値」の章の図 1 を参照してください。

図 *1*：*RADIUS* パケット図



各 RADIUS パケットには、次の情報が含まれています。

- コード：コードフィールドは1オクテットです。次のRADIUSパケットのタイプを識別します。
  - Access-Request（1）
  - Access-Accept（2）
  - Access-Reject（3）
  - Accounting-Request（4）
  - Accounting-Response（5）
- 識別子：識別子フィールドは 1 オクテットです。RADIUS サーバの要求と応答の照合を支援し、重複した要求を検出します。
- 長さ：長さフィールドは 2 オクテットです。パケット全体の長さを示します。
- オーセンティケータ：オーセンティケータフィールドは16オクテットです。最上位オクテットが最初に転送されます。RADIUS サーバからの応答の認証に使用されます。オーセンティケータには次の 2 つのタイプがあります。
  - Request-Authentication：Access-Request パケットと Accounting-Request パケットで使用できます。
  - Response-Authenticator：Access-Accept、Access-Reject、Access-Challenge、および Accounting-Response パケットで使用できます。

RADIUS パケット タイプ

次のリストは、属性情報を含むさまざまなタイプの RADIUS パケットをまとめたものです。

Access-Request：クライアントからRADIUSサーバに送信されます。このパケットには、ユーザにアクセスを許可している特定のネットワークアクセスサーバ（NAS）へのアクセスを許可するかどうかを RADIUS サーバが判断するための情報が含まれています。認証を実行しているユーザは、Access-Request パケットを提出する必要があります。RADIUS サーバは、Access-Request パケットを受信した後、応答を返す必要があります。

Access-Accept：RADIUS サーバは、Access-Request パケットを受信した後、Access-Request パケット内のすべての属性値が受け入れ可能な場合に、Access-Accept パケットを送信する必要があります。Access-Accept パケットには、クライアントからユーザにサービスを提供するために必要な設定情報が含まれています。

Access-Reject：RADIUS サーバは、Access-Request パケットを受信した後、どの属性値も受け入れ可能でなかった場合に、Access-Reject パケットを送信する必要があります。

Access-Challenge：RADIUS サーバは、Access-Accept パケットの受信後、応答が必要な Access-Challengeパケットをクライアントに送信できます。クライアントで応答の仕方がわからない場合、または、パケットが無効な場合は、 RADIUS サーバがそのパケットを破棄します。クライアントがパケットに応答する場合は、オリジナルの Access-Request パケットと一緒に新しい Access-Request パケットを送信する必要があります。

Accounting-Request：クライアントから RADIUS アカウンティング サーバに送信され、アカウンティング情報を提供します。RADIUS サーバが正常に Accounting-Request パケットを記録したら、Accounting-Response パケットを提出する必要があります。

Accounting-Response：RADIUS アカウンティング サーバからクライアントに送信され、Accounting-Request が正常に受信および記録されたことが伝えられます。

RADIUS ファイル

クライアントからサーバに AAA 情報を伝送するためには、RADIUS で使用されるファイルのタイプを理解しておくことが重要です。各ファイルには、ユーザの認証や認可のレベルが定義されています。ディレクトリ ファイルには、ユーザの NAS が実装できる属性が定義され、クライアント ファイルには、RADIUS サーバに要求を行えるユーザが定義され、ユーザ ファイルには、セキュリティおよび構成データに基づいて RADIUS サーバが認証するユーザ要求が定義されます。

ディレクトリ ファイル

ディレクトリ ファイルには、NAS でサポートされている属性に依存する属性のリストが格納されています。ただし、独自の属性のセットをカスタム ソリューション用のディレクトリに追加できます。このファイルでは属性値が定義されるため、構文解析要求などの属性出力を解釈できます。ディレクトリ ファイルには次の情報が含まれています。

- 名前：User-Name などの属性の ASCII 文字列「名」
- ID：属性の数値「名」。たとえば、User-Name 属性は属性 1 です。
- 値型：属性は次の値型のいずれかとして指定できます。
  - abinary：0 ～ 254 オクテット
  - date：ビッグエンディアン順の 32 ビット値。たとえば、1970 年 1 月 1 日 00:00:00 GMT 以降の秒数。
  - ipaddr：ネットワーク バイト順の 4 オクテット
  - integer：ビッグエンディアン順による 32 ビット値（上位バイトが先頭）
  - string：0 ～ 253 オクテット

特定の属性のデータ型が整数の場合は、オプションで、整数を拡張して何らかの文字列と一致させることができます。次のサンプル辞書には、整数ベースの属性と対応する値が含まれています。

```
# dictionary sample of integer entry
#
ATTRIBUTE       Service-Type            6                   integer
VALUE           Service-Type            Login                  1
VALUE           Service-Type            Framed                 2
VALUE           Service-Type            Callback-Login         3
VALUE           Service-Type            Callback-Framed        4
VALUE           Service-Type            Outbound               5
VALUE           Service-Type            Administrative         6
VALUE           Service-Type            NAS-Prompt             7
```

```
VALUE           Service-Type            Authenticate-Only       8
VALUE           Service-Type            Callback-NAS-Prompt     9
VALUE           Service-Type            Call-Check              10
VALUE           Service-Type            Callback-Administrative 11
```

クライアント ファイル

クライアント ファイルには、RADIUS サーバへの認証要求とアカウンティング要求の送信を許可された RADIUS クライアントのリストが含まれています。認証を受けるには、クライアントからサーバに送信された名前と認証キーがクライアント ファイル内のデータと完全一致する必要があります。

クライアント ファイルの例を次に示します。この例に示すキーは、**radius-serverkey***SomeSecret* コマンドと同じにする必要があります。

```
#Client Name        Key
#----------------  ---------------
10.1.2.3:256        test
nas01               bananas
nas02               MoNkEys
nas07.foo.com       SomeSecret
```

ユーザ ファイル

RADIUS ユーザ ファイルには、RADIUS サーバが認証するユーザごとのエントリが含まれています。ユーザ プロファイルとも呼ばれるエントリごとに、そのユーザがアクセス可能な属性が設定されます。

ユーザプロファイルの最初の行は、常に、「ユーザアクセス」行です。つまり、サーバはユーザにアクセス許可を出す前に、最初の行の属性をチェックする必要があります。最初の行にはユーザの名前が含まれています。この名前は、最大 252 文字にすることができ、後ろにユーザのパスワードなどの認証情報が続きます。

ユーザ アクセス行に関連付けられたその他の行は、要求元のクライアントまたはサーバに送信される属性応答を表します。応答内で送信される属性は、ディレクトリ ファイルで定義する必要があります。ユーザ ファイルを調べるときは、等号（=）文字の左側のデータがディレクトリ ファイルで定義された属性で、等号文字の右側のデータが構成データであることに注意してください。

（注） 空白行はユーザ プロファイルのどの場所にも挿入できません。

RADIUS ユーザ プロファイル（Merit Daemon フォーマット）の例を次に示します。この例では、ユーザ名が company.com、パスワードが user1 で、ユーザは 5 つのトンネル属性にアクセスできます。

```
# This user profile includes RADIUS tunneling attributes
company.com  Password="user1" Service-Type=Outbound
     Tunnel-Type = :1:L2TP
     Tunnel-Medium-Type = :1:IP
     Tunnel-Server-Endpoint = :1:10.0.0.1
     Tunnel-Password = :1:"welcome"
     Tunnel-Assignment-ID = :1:"nas"
```

RADIUS IETF 属性

（注） RADIUS トンネル属性では、L2TP に 32 個のタグ付きトンネル セットがサポートされます。

サポートされている RADIUS IETF 属性

表 1 に、シスコがサポートしている IETF RADIUS 属性とそれらが実装されている Cisco IOS リリースを示します。属性がセキュリティ サーバ固有の形式の場合は、この形式が指定されます。

リスト内の属性の説明については、表 2 を参照してください。

（注） 特別な（AA）リリースまたは初期開発（T）リリースで実装された属性が次のメインライン イメージに追加されています。

表 *1*：サポートされている *RADIUS IETF* 属性

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
1	User-Name	yes	yes	yes	yes	yes	yes	yes	yes
2	User-Password	yes	yes	yes	yes	yes	yes	yes	yes
3	CHAP-Password	yes	yes	yes	yes	yes	yes	yes	yes
4	NAS-IP Address	yes	yes	yes	yes	yes	yes	yes	yes
5	NAS-Port	yes	yes	yes	yes	yes	yes	yes	yes
6	Service-Type	yes	yes	yes	yes	yes	yes	yes	yes
7	Framed-Protocol	yes	yes	yes	yes	yes	yes	yes	yes
8	Framed-IP-Address	yes	yes	yes	yes	yes	yes	yes	yes
9	Framed-IP-Netmask	yes	yes	yes	yes	yes	yes	yes	yes
10	Framed-Routing	yes	yes	yes	yes	yes	yes	yes	yes
11	Filter-Id	yes	yes	yes	yes	yes	yes	yes	yes
12	Framed-MTU	yes	yes	yes	yes	yes	yes	yes	yes

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
13	Framed-Compression	yes	yes	yes	yes	yes	yes	yes	yes
14	Login-IP-Host	yes	yes	yes	yes	yes	yes	yes	yes
15	Login-Service	yes	yes	yes	yes	yes	yes	yes	yes
16	Login-TCP-Port	yes	yes	yes	yes	yes	yes	yes	yes
18	Reply-Message	yes	yes	yes	yes	yes	yes	yes	yes
19	Callback-Number	no	no	no	no	no	no	yes	yes
20	Callback-ID	no	no	no	no	no	no	no	no
22	Framed-Route	yes	yes	yes	yes	yes	yes	yes	yes
23	Framed-IPX-Network	no	no	no	no	no	no	no	no
24	State	yes	yes	yes	yes	yes	yes	yes	yes
25	Class	yes	yes	yes	yes	yes	yes	yes	yes
26	Vendor-Specific	yes	yes	yes	yes	yes	yes	yes	yes
27	Session-Timeout	yes	yes	yes	yes	yes	yes	yes	yes
28	Idle-Timeout	yes	yes	yes	yes	yes	yes	yes	yes
29	Termination-Action	no	no	no	no	no	no	no	no
30	Called-Station-Id	yes	yes	yes	yes	yes	yes	yes	yes
31	Calling-Station-Id	yes	yes	yes	yes	yes	yes	yes	yes
32	NAS-Identifier	no	no	no	no	no	no	no	yes
33	Proxy-State	no	no	no	no	no	no	no	no
34	Login-LAT-Service	yes	yes	yes	yes	yes	yes	yes	yes
35	Login-LAT-Node	no	no	no	no	no	no	no	yes
36	Login-LAT-Group	no	no	no	no	no	no	no	no
37	Framed-AppleTalk-Link	no	no	no	no	no	no	no	no
38	Framed-AppleTalk-Network	no	no	no	no	no	no	no	no

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
39	Framed-AppleTalk-Zone	no	no	no	no	no	no	no	no
40	Acct-Status-Type	yes	yes	yes	yes	yes	yes	yes	yes
41	Acct-Delay-Time	yes	yes	yes	yes	yes	yes	yes	yes
42	Acct-Input-Octets	yes	yes	yes	yes	yes	yes	yes	yes
43	Acct-Output-Octets	yes	yes	yes	yes	yes	yes	yes	yes
44	Acct-Session-Id	yes	yes	yes	yes	yes	yes	yes	yes
45	Acct-Authentic	yes	yes	yes	yes	yes	yes	yes	yes
46	Acct-Session-Time	yes	yes	yes	yes	yes	yes	yes	yes
47	Acct-Input-Packets	yes	yes	yes	yes	yes	yes	yes	yes
48	Acct-Output-Packets	yes	yes	yes	yes	yes	yes	yes	yes
49	Acct-Terminate-Cause	no	no	no	yes	yes	yes	yes	yes
50	Acct-Multi-Session-Id	no	yes	yes	yes	yes	yes	yes	yes
51	Acct-Link-Count	no	yes	yes	yes	yes	yes	yes	yes
52	Acct-Input-Gigawords	no	no	no	no	no	no	no	no
53	Acct-Output-Gigawords	no	no	no	no	no	no	no	no
55	Event-Timestamp	no	no	no	no	no	no	no	yes
60	CHAP-Challenge	yes	yes	yes	yes	yes	yes	yes	yes
61	NAS-Port-Type	yes	yes	yes	yes	yes	yes	yes	yes
62	Port-Limit	yes	yes	yes	yes	yes	yes	yes	yes
63	Login-LAT-Port	no	no	no	no	no	no	no	no
64	Tunnel-Type[1]	no	no	no	no	no	no	yes	yes
65	Tunnel-Medium-Type 1	no	no	no	no	no	no	yes	yes
66	Tunnel-Client-Endpoint	no	no	no	no	no	no	yes	yes

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
67	Tunnel-Server-Endpoint 1	no	no	no	no	no	no	yes	yes
68	Acct-Tunnel-Connection-ID	no	no	no	no	no	no	yes	yes
69	Tunnel-Password 1	no	no	no	no	no	no	yes	yes
70	ARAP-Password	no	no	no	no	no	no	no	no
71	ARAP-Features	no	no	no	no	no	no	no	no
72	ARAP-Zone-Access	no	no	no	no	no	no	no	no
73	ARAP-Security	no	no	no	no	no	no	no	no
74	ARAP-Security-Data	no	no	no	no	no	no	no	no
75	Password-Retry	no	no	no	no	no	no	no	no
76	Prompt	no	no	no	no	no	no	yes	yes
77	Connect-Info	no	no	no	no	no	no	no	yes
78	Configuration-Token	no	no	no	no	no	no	no	no
79	EAP-Message	no	no	no	no	no	no	no	no
80	Message-Authenticator	no	no	no	no	no	no	no	no
81	Tunnel-Private-Group-ID	no	no	no	no	no	no	no	no
82	Tunnel-Assignment-ID 1	no	no	no	no	no	no	yes	yes
83	Tunnel-Preference	no	no	no	no	no	no	no	yes
84	ARAP-Challenge-Response	no	no	no	no	no	no	no	no
85	Acct-Interim-Interval	no	no	no	no	no	no	yes	yes
86	Acct-Tunnel-Packets-Lost	no	no	no	no	no	no	no	no
87	NAS-Port-ID	no	no	no	no	no	no	no	no
88	Framed-Pool	no	no	no	no	no	no	no	no

番号	IETF 属性	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
90	Tunnel-Client-Auth-ID [2]	no	no	no	no	no	no	no	yes
91	Tunnel-Server-Auth-ID	no	no	no	no	no	no	no	yes
200	IETF-Token-Immediate	no	no	no	no	no	no	no	no

[1] この RADIUS 属性は、2 つのドラフト IETF 文書、RFC 2868『RADIUS Attributes for Tunnel Protocol Support』と RFC 2867『RADIUS Accounting Modifications for Tunnel Protocol Support』に基づきます。
[2] この RADIUS 属性は、RFC 2865 および RFC 2868 に基づきます。

RADIUS 属性解説の包括的リスト

次の表に、IETF RADIUS 属性とその説明を示します。属性がセキュリティ サーバ固有の形式の場合は、この形式が指定されます。

表 *2*：*RADIUS IETF* 属性

番号	IETF 属性	説明
1	User-Name	RADIUS サーバで認証されるユーザの名前を示します。
2	User-Password	Access-Challenge の後に続くユーザのパスワードとユーザ入力を示します。16 文字を超えるパスワードは、RFC 2865 の仕様により暗号化されます。
3	CHAP-Password	Access-Challenge に対する応答で PPP Challenge Handshake Authentication Protocol（CHAP）ユーザが入力した応答値を示します。
4	NAS-IP Address	認証を要求しているネットワーク アクセス サーバの IP アドレスを示します。デフォルト値は 0.0.0.0/0 です。

番号	IETF 属性	説明
5	NAS-Port	ユーザを認証しているネットワーク アクセス サーバの物理ポート番号を示します。NAS-Port 値（32 ビット）は、1 つまたは 2 つの 16 ビット値（**radius-serverextended-portnames** コマンドの設定に依存）で構成されます。各 16 ビットの数値は、次のように、解釈用の 5 桁の 10 進整数として表示されるはずです。 非同期端末回線、非同期ネットワーク インターフェイス、および仮想非同期インターフェイスの場合、この値は **00ttt** です。ここで、**ttt** は回線番号または非同期インターフェイス ユニット番号です。 • 通常の同期ネットワーク インターフェイスの場合、この値は **10xxx** です。 • プライマリ レート ISDN インターフェイス上のチャネルの場合、この値は **2ppcc** です。 • 基本レート ISDN インターフェイス上のチャネルの場合、この値は **3bb0c** です。 • その他のタイプのインターフェイスの場合、この値は **6nnss** です。

番号	IETF 属性	説明
6	Service-Type	要求されたサービスのタイプまたは指定されたサービスのタイプを示します。 • 要求内： 既知の PPP または Serial Line Internet Protocol（SLIP）接続の場合にフレーム化。**enable** コマンドの場合は Administrative-user。 • 応答内： Login：接続を確立します。Framed：SLIP または PPP を開始します。Administrative User：EXEC または **enableok** を開始します。 Exec User：EXEC セッションを開始します。 サービス タイプは、次のような特定の数値で示されます。 • 1：Login • 2：Framed • 3：Callback-Login • 4：Callback-Framed • 5：Outbound • 6：Administrative • 7：NAS-Prompt • 8：Authenticate Only • 9：Callback-NAS-Prompt

番号	IETF 属性	説明
7	Framed-Protocol	フレーム化アクセスに使用されるフレーム構成を示します。他のフレーム構成は許可されません。 フレーム構成は次のように数値で指定されます。 • 1：PPP • 2：SLIP • 3：ARA • 4：Gandalf独自のシングルリンク/マルチリンク プロトコル • 5：Xylogics 独自の IPX/SLIP
8	Framed-IP-Address	access-request 内でユーザの IP アドレスを RADIUS サーバに送信することによって、ユーザに対して設定する IP アドレスを示します。このコマンドを有効にするには、グローバル コンフィギュレーション モードで **radius-serverattribute8include-in-access-req** コマンドを使用します。
9	Framed-IP-Netmask	ユーザがネットワーク上でデバイスを使用している場合に、ユーザに対して設定する IP ネットマスクを示します。この属性値によって、指定されたマスクを使用して Framed-IP-Address にスタティック ルートが追加されることになります。

番号	IETF 属性	説明
10	Framed-Routing	ユーザがネットワーク上でデバイスを使用している場合に、ユーザに対するルーティング方式を示します。この属性に対してサポートされている値は、「None」と「Send and Listen」だけです。 ルーティング方式は次のように数値で指定されます。 • 0：なし • 1：ルーティング パケットの送信 • 2：ルーティング パケットのリッスン • 3：ルーティング パケットの送信とリッスン
11	Filter-Id	ユーザのフィルタ リストの名前を示し、%d、%d.in、または %d.out としてフォーマットされます。この属性は、最近のサービス タイプ コマンドに関連付けられます。ログインと EXEC の場合は、0 ～ 199 の回線アクセス リスト値として %d または %d.out を使用します。フレーム化サービスの場合は、インターフェイス出力アクセス リストとして %d または %d.out を使用し、入力アクセス リストとして %d.in を使用します。この番号は、参照しているプロトコルに対する自己符号化です。
12	Framed-MTU	最大伝送ユニット（MTU）が PPP でネゴシエートされない場合に、ユーザに対して設定可能な MTU を示します。

番号	IETF 属性	説明
13	Framed-Compression	リンクに使用される圧縮プロトコルを示します。この属性により、EXEC 認可時に生成される PPP または SLIP オートコマンドに「/compress」が追加されます。これは EXEC 認可以外には実装されていません。 圧縮プロトコルは次のように数値で指定されます。 • 0：なし • 1：VJ-TCP/IP ヘッダー圧縮 • 2：IPX ヘッダー圧縮
14	Login-IP-Host	Login-Service 属性が含まれている場合に、ユーザが接続するホストを示しますこの動作はログイン直後に開始されます。
15	Login-Service	ユーザをログイン ホストに接続するために使用すべきサービスを示します。 サービスは次のように数値で指定されます。 • 0：Telnet • 1：Rlogin • 2：TCP-Clear • 3：PortMaster • 4：LAT
16	Login-TCP-Port	Login-Service 属性も存在する場合に、ユーザを接続すべき TCP ポートを定義します。
18	Reply-Message	RADIUS サーバを使用してユーザに表示される可能性のあるテキストを示します。この属性はユーザ ファイルに含めることができますが、プロファイル当たりの Reply-Message エントリ数を 16 以下にする必要があります。

番号	IETF 属性	説明
19	Callback-Number	コールバックに使用するダイヤリング文字列を定義します。
20	Callback-ID	呼び出される場所の名前、つまり、ネットワーク アクセス サーバによって解釈される場所の名前（1つ以上のオクテットからなる）を定義します。
22	Framed-Route	このネットワーク アクセス サーバ上のユーザに対して設定するルーティング情報を指定します。RADIUS RFC 形式（net/bits [router [metric]]）と従来のドット区切りのマスク（net mask [router [metric]]）がサポートされています。デバイス フィールドを省略するか、0 にした場合は、ピア IP アドレスが使用されます。現在、メトリックは無視されます。この属性は access-request パケットです。
23	Framed-IPX-Network	ユーザに対して設定される IPX ネットワーク番号を定義します。
24	State	ネットワーク アクセス サーバと RADIUS サーバ間で状態情報の保持を可能にします。この属性は CHAP チャレンジにしか適用できません。
25	Class	（アカウンティング）RADIUS サーバで入力された場合に、このユーザに関するすべてのアカウンティング パケットにネットワーク アクセス サーバで追加される任意の値

番号	IETF 属性	説明

26	Vendor-Specific	ベンダーに一般使用に適さない独自の拡張属性の使用を許可します。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダータイプ 1（名前は「cisco-avpair」）です。値は、次の形式のストリングです。
		
		`protocol : attribute sep value`
		「protocol」は、特定の認可タイプに使用するシスコの「protocol」属性の値です。「attribute」および「value」は、シスコの TACACS+ 仕様で定義されている適切な AV ペアです。「sep」は、必須の属性の場合は「=」、任意指定の属性の場合は「*」です。これにより、TACACS+認可で使用できるすべての機能を RADIUS にも使用できるようになります。次に例を示します。
		
		`cisco-avpair= ”ip:addr-pool=first“`
		`cisco-avpair= ”shell:priv-lvl=15“`
		1 つめの例は、IP 認可の際（PPP の IPCP アドレスの割り当て中）にシスコの「Multiple Named ip address Pools」機能を有効化します。2つめの例は、ネットワーク アクセス サーバからのユーザ ログイン直後に EXEC コマンドにアクセスできるようにします。
		
		表 1 に、サポートされているベンダー固有 RADIUS 属性（IETF 属性 26）を示します。

27	Session-Timeout	セッションを終了する前に、ユーザにサービスを提供する最大秒数を設定します。この属性値は、ユーザ単位の絶対タイムアウトになります。
28	Idle-Timeout	セッションが終了する前にユーザに許可されるアイドル接続の最大秒数を設定します。この属性値は、ユーザ単位のセッションタイムアウトになります。

番号	IETF 属性	説明
29	Termination-Action	終了は次のように数値で指定されます。 • 0：デフォルト • 1：RADIUS 要求
30	Called-Station-Id	（アカウンティング）ネットワーク アクセス サーバから、ユーザが Access-Request パケットの一部として呼び出した電話番号を送信できるようにします（着信番号識別サービス（DNIS）または同様の技術を使用）。この属性は、ISDN と、PRI と一緒に使用された場合の Cisco AS5200 上のモデム コールに対してのみサポートされます。
31	Calling-Station-Id	（アカウンティング）ネットワーク アクセス サーバから、コールが Access-Request パケットの一部として発信された電話番号を送信できるようにします（自動番号識別または同様の技術を使用）。この属性の値は、TACACS+ の「remote-addr」の値と同じです。この属性は、ISDN と、PRI と一緒に使用された場合の Cisco AS5200 上のモデム コールに対してのみサポートされます。
32	NAS-Identifier	Access-Request を送信したネットワーク アクセス サーバを識別する文字列。**radius-serverattribute32include-in-access-req** 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、Access-Request または Accounting-Request 内で RADIUS 属性 32 を送信します。フォーマットが指定されなかった場合は、デフォルトで、完全修飾ドメイン名（FQDN）が属性内で送信されます。

番号	IETF 属性	説明
33	Proxy-State	Access-Request の転送時にプロキシ サーバから別のサーバに送信可能な属性。この属性は、Access-Accept、Access-Reject、または Access-Challenge 内でそのまま返され、ネットワーク アクセス サーバに応答が送信される前にプロキシ サーバで削除される必要があります。
34	Login-LAT-Service	ユーザをローカルエリア トランスポート（LAT）で接続すべきシステムを示します。この属性は、EXEC モードでのみ使用できます。
35	Login-LAT-Node	ユーザが LAT で自動的に接続されるノードを示します。
36	Login-LAT-Group	ユーザに使用が認可されている LAT グループ コードを識別します。
37	Framed-AppleTalk-Link	AppleTalk デバイスであるシリアル リンクに使用すべき別の AppleTalk のネットワーク番号を示します。
38	Framed-AppleTalk- Network	ユーザに AppleTalk ノードを割り当てるためにネットワーク アクセス サーバで使用される AppleTalk ネットワーク番号を示します。
39	Framed-AppleTalk-Zone	ユーザに使用すべき AppleTalk デフォルト ゾーンを示します。
40	Acct-Status-Type	（アカウンティング）この Accounting-Request がユーザ サービスの始まり（開始）または終わり（終了）をマークするかどうかを示します。
41	Acct-Delay-Time	（アカウンティング）クライアントが特定のレコードの送信を試みる秒数を示します。
42	Acct-Input-Octets	（アカウンティング）このサービスの提供中にポートから受信されたオクテット数を示します。

番号	IETF 属性	説明
43	Acct-Output-Octets	（アカウンティング）このサービスの配信中にポートに送信されたオクテット数を示します。
44	Acct-Session-Id	（アカウンティング）ログ ファイル内の開始レコードと終了レコードのマッチングを容易にする一意のアカウンティング識別子。Acct-Session ID の番号は、デバイスの電源を入れ直したり、ソフトウェアをリロードしたりするたびに、1 から再開します。この属性を access-request パケット内で送信するには、グローバル コンフィギュレーション モードで **radius-serverattribute44include-in-access-req** コマンドを使用します。
45	Acct-Authentic	（アカウンティング）ユーザがどのように認証されたか、RADIUS、ネットワーク アクセス サーバ自体、およびその他のリモート認証プロトコルのどれで認証されたかを示します。この属性は、RADIUS で認証されたユーザの場合は「radius」に、TACACS+ と Kerberos の場合は「remote」に、local、enable、line、および if-needed 方式の場合は「local」に設定されます。その他のすべての方式の場合は、この属性が省略されます。
46	Acct-Session-Time	（アカウンティング）ユーザがサービスを受信していた時間（秒数）を示します。
47	Acct-Input-Packets	（アカウンティング）このサービスのフレーム化ユーザへの提供中にポートから受信されたパケット数を示します。
48	Acct-Output-Packets	（アカウンティング）このサービスのフレーム化ユーザへの配信中にポートに送信されたパケット数を示します。

番号	IETF 属性	説明
49	Acct-Terminate-Cause	（アカウンティング）接続が終了した理由の詳細を報告します。終了の理由は次のように数値で指定されます。 **1** ユーザ要求 **2** キャリアの消失 **3** サービスの消失 **4** アイドル タイムアウト **5** セッション タイムアウト **6** 管理リセット **7** 管理リブート **8** ポート エラー **9** NAS エラー **10** NAS 要求 **11** NAS リブート **12** ポートの不要化 **13** ポートの横取り **14** ポートの保留 **15** 使用できないサービス **16** コールバック **17** ユーザ エラー **18** ホスト要求 （注） 属性 49 に関して、シスコは 1 ～ 6、8、9、12、および 15 ～ 18 の値をサポートしています。

番号	IETF 属性	説明
50	Acct-Multi-Session-Id	（アカウンティング）ログ ファイル内の複数の関連セッションをリンクするために使用される一意のアカウンティング識別子。 マルチリンク セッション内でリンクされたセッションごとに、一意の Acct-Session-Id 値が割り当てられますが、Acct-Multi-Session-Id は共有されます。
51	Acct-Link-Count	（アカウンティング）アカウンティング レコードが生成された時点で特定のマルチリンク セッション内で認識されていたリンク数を示します。ネットワーク アクセス サーバは、複数のリンクが含まれる任意のアカウンティング要求内にこの属性を追加できます。
52	Acct-Input-Gigawords	サービスの提供中に Acct-Input-Octets カウンタが一周（2 の 32 乗）した回数を示します。
53	Acct-Output-Gigawords	サービスの配信中に Acct-Output-Octets カウンタが一周（2 の 32 乗）した回数を示します。

番号	IETF 属性	説明
55	Event-Timestamp	NAS 上でイベントが発生した時刻を記録します。属性 55 内で送信されるタイムスタンプは、1970 年 1 月 1 日 00:00 UTC 以降の秒数です。アカウンティング パケット内で RADIUS 属性 55 を送信するには、**radius-serverattribute55include-in-acct-req** コマンドを使用します。 （注） アカウンティングパケット内で Event-Timestamp 属性を送信するには、ネットワークデバイスのクロックを設定する必要があります（ネットワークデバイスのクロックの設定方法については、ネットワーク管理の設定ガイドの「基本システム管理」の章の「基本システム管理の実行」を参照してください）。ネットワークデバイスがリロードされるたびにネットワークデバイスのクロックを設定するのを避けるには、**clockcalendar-valid** コマンドを有効にします（このコマンドの詳細については、ネットワーク管理の設定ガイドの「基本システム管理」の章の「時刻およびカレンダーサービスの設定」を参照してください）。
60	CHAP-Challenge	ネットワーク アクセス サーバから PPP CHAP ユーザに送信されたチャレンジ ハンドシェーク認証プロトコル チャレンジが保存されます。

番号	IETF 属性	説明
61	NAS-Port-Type	ユーザを認証するためにネットワーク アクセス サーバで使用されている物理ポートのタイプを示します。物理ポートは、次のように数値で示されます。 • 0：非同期 • 1：同期 • 2：ISDN 同期 • 3：ISDN 非同期（V.120） • 4：ISDN 非同期（V.110） • 5：仮想
62	Port-Limit	NAS からユーザに提供される最大ポート数を設定します。
63	Login-LAT-Port	ユーザを LAT で接続すべきポートを定義します。
64	Tunnel-Type[3]	使用されているトンネリング プロトコルを示します。シスコのソフトウェアでは、この属性の値として L2TP がサポートされます。
65	Tunnel-Medium-Type1	トンネルの作成に使用される転送メディア タイプを示します。この属性には、このリリースで使用可能な値（IP）が 1つしかありません。この属性に値を設定しなかった場合は、デフォルトとして IP が使用されます。

番号	IETF 属性	説明
66	Tunnel-Client-Endpoint	トンネルの開始側端のアドレスが含まれています。Access-Request と Access-Accept の両方のパケットに含めて、新しいトンネルを開始するアドレスを示すこともできます。 Tunnel-Client-Endpoint 属性が Access-Request パケットに含まれている場合、RADIUS サーバはその値を指示として取得する必要があります。この属性は、Accounting-Request パケットに含める必要があります。このパケットには、トンネルが開始されたアドレスを示す場合に Start と Stop のどちらかの値を伴う Acct-Status-Type 属性が含まれています。この属性は、Tunnel-Server-Endpoint 属性や Acct-Tunnel-Connection-ID 属性と一緒に使用して、アカウンティングと監査の目的でトンネルを特定する、グローバルで一意の手段を提供できます。 次のように、この属性の 127.0.0.X の値を受け入れるためにネットワーク アクセス サーバの機能が拡張されています。 127.0.0.0 は loopback0 の IP アドレスを使用する必要があることを示し、127.0.0.1 は loopback1 の IP アドレスを使用する必要があることを示します。127.0.0.X は、実際のトンネル クライアント エンドポイントの IP アドレスに loopbackX の IP アドレスを使用する必要があることを示します。この機能拡張によって、複数のネットワーク アクセス サーバ全体のスケーラビリティが向上します。

番号	IETF 属性	説明
67	Tunnel-Server-Endpoint1	トンネルのサーバ端のアドレスを示します。この属性のフォーマットは、Tunnel-Medium-Type の値によって異なります。リリースによっては、トンネル メディア タイプとして IP のみがサポートされ、IP アドレスまたは LNS のホスト名がこの属性に使用できる場合があります。
68	Acct-Tunnel-Connection-ID	トンネル セッションに割り当てられた識別子を示します。この属性は、Start、Stop、または上記のいずれかを値として持つ Acct-Status-Type 属性と一緒に Accounting-Request パケットに含める必要があります。この属性は、Tunnel-Client-Endpoint 属性や Tunnel-Server-Endpoint 属性と一緒に使用して、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を提供できます。
69	Tunnel-Password1	リモート サーバの認証に使用されるパスワードを定義します。この属性は、Tunnel-Type の値（AAA_ATTR_l2tp_tunnel_pw (L2TP)、AAA_ATTR_nas_password (L2F)、および AAA_ATTR_gw_password (L2F)）に基づいて、さまざまな AAA 属性に変換されます。 デフォルトで、受信されたすべてのパスワードが暗号化されます。そのため、NAS が暗号化されていないパスワードを復号化しようとすると、認可エラーが発生する可能性があります。属性 69 を有効にして、暗号化されていないパスワードを受信できるようにするには、グローバル コンフィギュレーション モードで、**radius-serverattribute69clear** コマンドを使用します。
70	ARAP-Password	AppleTalk Remote Access Control（ARAP）の Framed-Protocol を含む Access-Request パケットを識別します。

番号	IETF 属性	説明
71	ARAP-Features	ARAP feature flags パケットで NAS からユーザに送信する必要のあるパスワード情報が含まれています。
72	ARAP-Zone-Access	ユーザの ARAP ゾーン リストの使用方法を示します。
73	ARAP-Security	Access-Challenge パケット内で使用すべき ARAP セキュリティ モジュールを示します。
74	ARAP-Security-Data	Access-Challenge および Access-Request パケットに実際のセキュリティモジュールのチャレンジまたは応答が含まれています。
75	Password-Retry	ユーザが切断されるまでに認証を試みることができる回数を示します。
76	Prompt	ユーザの応答をエコーすべきか否かを NAS に指示します（0 = エコーなし、1 = エコーあり）。
77	Connect-Info	モデム コールに関する追加情報を提供します。この属性は start と stop のアカウンティング レコード内で生成されます。
78	Configuration-Token	使用するユーザ プロファイルのタイプを示します。この属性は、プロキシに基づく大規模な分散認証ネットワークで使用する必要があります。 Access-Accept 内で RADIUS プロキシ サーバから RADIUS プロキシ クライアントに送信されます。NAS には送信しないでください。
79	EAP-Message	Extended Access Protocol（EAP）プロトコルを理解していなくても、NAS で EAP を使用してダイヤルイン ユーザを認証できるように EAP パケットをカプセル化します。

番号	IETF 属性	説明
80	Message-Authenticator	CHAP、ARAP、またはEAP認証方式を使用して Access-Requests のスプーフィングを阻止します。
81	Tunnel-Private-Group-ID	特定のトンネル化されたセッションのグループ ID を示します。
82	Tunnel-Assignment-ID1	セッションが割り当てられた特定のトンネル イニシエータを示します。
83	Tunnel-Preference	各トンネルに割り当てられた相対プリファレンスを示します。この属性は、RADIUS サーバからトンネル イニシエータに複数のトンネリング属性のセットが返される場合に含める必要があります。
84	ARAP-Challenge-Response	ダイヤルイン クライアントのチャレンジに対する応答が含まれています。
85	Acct-Interim-Interval	この特定のセッションの一時更新間隔を秒数で示します。この値は、Access-Accept メッセージにのみ含めることができます。
86	Acct-Tunnel-Packets-Lost	特定のリンク上で失われたパケット数を示します。この属性は、Tunnel-Link-Stop の値を持つ Acct-Status-Type 属性と一緒に Accounting-Requestパケットに含める必要があります。
87	NAS-Port-ID	ユーザを認証しているNASのポートを識別するテキスト文字列が含まれています。
88	Framed-Pool	ユーザにアドレスを割り当てるために使用すべき、割り当て済みのアドレス プールの名前が含まれています。NAS が複数のアドレス プールをサポートしていない場合は、この属性を無視する必要があります。

番号	IETF 属性	説明
90	Tunnel-Client-Auth-ID	トンネルセットアップをトンネルターミネータで認証するときに、トンネルイニシエータ（NAS とも呼ばれる）で使用される名前を示します。L2F プロトコルと L2TP プロトコルをサポートします。
91	Tunnel-Server-Auth-ID	トンネルセットアップをトンネルイニシエータで認証するときに、トンネルターミネータ（ホーム ゲートウェイとも呼ばれる）で使用される名前を示します。L2F プロトコルと L2TP プロトコルをサポートします。
200	IETF-Token-Immediate	ファイル エントリがハンドヘルド セキュリティ カード サーバを示しているログイン ユーザから受け取ったパスワードを RADIUS でどのように処理するかを決定します。 この属性の値は次のように数値で指定されます。 • 0：No - パスワードは無視されます。 • 1：Yes - パスワードが認証に使用されます。

[3] この RADIUS 属性は、2 つのドラフト IETF 文書、RFC 2868『RADIUS Attributes for Tunnel Protocol Support』と RFC 2867『RADIUS Accounting Modifications for Tunnel Protocol Support』に基づきます。

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	『Master Commands List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

RFC

RFC	タイトル
RFC 2865	『Remote Authentication Dial In User Service (RADIUS)』
RFC 2866	『RADIUS Accounting』
RFC 2867	『RADIUS Accounting Modifications for Tunnel Protocol Support』
RFC 2868	『RADIUS Attributes for Tunnel Protocol Support』
RFC 2869	『RADIUS Extensions』

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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

RADIUS 属性の概要と RADIUS IETF 属性の機能情報

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*：*RADIUS* 属性の概要と *RADIUS IETF* 属性の機能情報

機能名	リリース	機能情報
RADIUS IETF 属性	Cisco IOS Release 11.1	この機能は、Cisco IOS Release 11.1 で導入されました。

第 3 章

RADIUS ベンダー固有属性

IETF ドラフト標準には、RADIUS でのネットワーク アクセス サーバと RADIUS サーバ間でベンダー固有情報を通信する方式が規定されています。ただし、ベンダーには固有のアプリケーション向けに拡張した RADIUS 属性セットを持つものがあります。このマニュアルでは、これらベンダー固有 RADIUS 属性の Cisco IOS XE でのサポート情報について記載します。

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。

サポートされるベンダー固有 RADIUS 属性

次の表に、シスコがサポートしているベンダー固有 RADIUS 属性およびこれらを実装している Cisco IOS XE リリースを示します。属性がセキュリティ サーバ固有の形式の場合は、この形式が指定されます。それぞれの説明については、ベンダー固有 RADIUS 属性の表を参照してください。

表 *4* : サポートされるベンダー固有 *RADIUS* 属性

番号	ベンダー固有属性	IOS XE 2.1
17	Change-Password	yes
21	Password-Expiration	yes
68	Tunnel-ID	yes
108	My-Endpoint-Disc-Alias	no
109	My-Name-Alias	no
110	Remote-FW	no
111	Multicast-GLeave-Delay	no
112	CBCP-Enable	no
113	CBCP-Mode	no
114	CBCP-Delay	no
115	CBCP-Trunk-Group	no
116	Appletalk-Route	no
117	Appletalk-Peer-Mode	no
118	Route-Appletalk	no
119	FCP-Parameter	no
120	Modem-PortNo	no
121	Modem-SlotNo	no
122	Modem-ShelfNo	no
123	Call-Attempt-Limit	no
124	Call-Block-Duration	no
125	Maximum-Call-Duration	no
126	Router-Preference	no
127	Tunneling-Protocol	no
128	Shared-Profile-Enable	no

番号	ベンダー固有属性	IOS XE 2.1
129	Primary-Home-Agent	no
130	Secondary-Home-Agent	no
131	Dialout-Allowed	no
133	BACP-Enable	no
134	DHCP-Maximum-Leases	no
135	Primary-DNS-Server	yes
136	Secondary-DNS-Server	yes
137	Ascend-Client-Assign-DNS	no
138	User-Acct-Type	no
139	User-Acct-Host	no
140	User-Acct-Port	no
141	User-Acct-Key	no
142	User-Acct-Base	no
143	User-Acct-Time	no
144	Assign-IP-Client	no
145	Assign-IP-Server	no
146	Assign-IP-Global-Pool	no
147	DHCP-Reply	no
148	DHCP-Pool-Number	no
149	Expect-Callback	no
150	Event-Type	no
151	Ascend-Session-Svr-Key	yes
152	Ascend-Multicast-Rate-Limit	yes
153	IF-Netmask	no

番号	ベンダー固有属性	IOS XE 2.1
154	h323-Remote-Address	no
155	Ascend-Multicast-Client	yes
156	FR-Circuit-Name	no
157	FR-LinkUp	no
158	FR-Nailed-Grp	no
159	FR-Type	no
160	FR-Link-Mgt	no
161	FR-N391	no
162	FR-DCE-N392	no
163	FR-DTE-N392	no
164	FR-DCE-N393	no
165	FR-DTE-N393	no
166	FR-T391	no
167	FR-T392	no
168	Bridge-Address	no
169	TS-Idle-Limit	no
170	TS-Idle-Mode	no
171	DBA-Monitor	no
172	Base-Channel-Count	no
173	Minimum-Channels	no
174	IPX-Route	no
175	FT1-Caller	no
176	Ipsec-Backup-Gateway	yes
177	rm-Call-Type	yes

番号	ベンダー固有属性	IOS XE 2.1
178	Group	no
179	FR-DLCI	no
180	FR-Profile-Name	no
181	Ara-PW	no
182	IPX-Node-Addr	no
183	Home-Agent-IP-Addr	no
184	Home-Agent-Password	no
185	Home-Network-Name	no
186	Home-Agent-UDP-Port	no
187	Multilink-ID	yes
188	Ascend-Num-In-Multilink	yes
189	First-Dest	no
190	Pre-Bytes-In	yes
191	Pre-Bytes-Out	yes
192	Pre-Paks-In	yes
193	Pre-Paks-Out	yes
194	Maximum-Time	yes
195	Disconnect-Cause	yes
196	Connect-Progress	yes
197	Data-Rate	yes
198	PreSession-Time	yes
199	Token-Idle	no
201	Require-Auth	no
202	Number-Sessions	no

番号	ベンダー固有属性	IOS XE 2.1
203	Authen-Alias	no
204	Token-Expiry	no
205	Menu-Selector	no
206	Menu-Item	no
207	PW-Warntime	no
208	PW-Lifetime	yes
209	IP-Direct	yes
210	PPP-VJ-Slot-Compression	yes
211	PPP-VJ-1172	no
212	PPP-Async-Map	no
213	Third-Prompt	no
214	Send-Secret	yes
215	Receive-Secret	no
216	IPX-Peer-Mode	no
217	IP-Pool	yes
218	Static-Addr-Pool	yes
219	FR-Direct	no
220	FR-Direct-Profile	no
221	FR-Direct-DLCI	no
222	Handle-IPX	no
223	Netware-Timeout	no
224	IPX-Alias	no
225	Metric	no
226	PRI-Number-Type	no

番号	ベンダー固有属性	IOS XE 2.1
227	Dial-Number	yes
228	Route-IP	yes
229	Route-IPX	no
230	Bridge	no
231	Send-Auth	yes
232	Send-Passwd	no
233	Link-Compression	yes
234	Target-Util	yes
235	Maximum-Channels	yes
236	Inc-Channel-Count	no
237	Dec-Channel-Count	no
238	Seconds-of-History	no
239	History-Weigh-Type	no
240	Add-Seconds	no
241	Remove-Seconds	no
242	Data-Filter	yes
243	Call-Filter	no
244	Idle-Limit	yes
245	Preempt-Limit	no
246	Callback	no
247	Data-Service	yes
248	Force-56	yes
249	Billing Number	no
250	Call-By-Call	no

番号	ベンダー固有属性	IOS XE 2.1
251	Transit-Number	no
252	Host-Info	no
253	PPP-Address	no
254	MPP-Idle-Percent	no
255	Xmit-Rate	yes

ベンダー固有 RADIUS 属性の説明に関する包括的なリスト

次の表に、既知のベンダー固有 RADIUS 属性の一覧と説明を示します。

表 *5*：ベンダー固有 *RADIUS* 属性

番号	ベンダー固有属性	説明
17	Change-Password	ユーザのパスワード変更要求を指定します。
21	Password-Expiration	ユーザのファイル エントリのユーザ パスワードの有効期限を指定します。
68	Tunnel-ID	（Ascend 5）CLID または DNIS トンネリングを使用する各セッションで、RADIUS により割り当てられるストリングを指定します。アカウンティングが実装されている場合、この値はアカウンティングに使用されます。
108	My-Endpoint-Disc-Alias	（Ascend 5）説明はありません。
109	My-Name-Alias	（Ascend 5）説明はありません。
110	Remote-FW	（Ascend 5）説明はありません。

番号	ベンダー固有属性	説明
111	Multicast-GLeave-Delay	（Ascend 5）説明はありません。
112	CBCP-Enable	（Ascend 5）説明はありません。
113	CBCP-Mode	（Ascend 5）説明はありません。
114	CBCP-Delay	（Ascend 5）説明はありません。
115	CBCP-Trunk-Group	（Ascend 5）説明はありません。
116	Appletalk-Route	（Ascend 5）説明はありません。
117	Appletalk-Peer-Mode	（Ascend 5）説明はありません。
118	Route-Appletalk	（Ascend 5）説明はありません。
119	FCP-Parameter	（Ascend 5）説明はありません。
120	Modem-PortNo	（Ascend 5）説明はありません。
121	Modem-SlotNo	（Ascend 5）説明はありません。
122	Modem-ShelfNo	（Ascend 5）説明はありません。
123	Call-Attempt-Limit	（Ascend 5）説明はありません。
124	Call-Block-Duration	（Ascend 5）説明はありません。
125	Maximum-Call-Duration	（Ascend 5）説明はありません。

番号	ベンダー固有属性	説明
126	Router-Preference	（Ascend 5）説明はありません。
127	Tunneling-Protocol	（Ascend 5）説明はありません。
128	Shared-Profile-Enable	（Ascend 5）説明はありません。
129	Primary-Home-Agent	（Ascend 5）説明はありません。
130	Secondary-Home-Agent	（Ascend 5）説明はありません。
131	Dialout-Allowed	（Ascend 5）説明はありません。
133	BACP-Enable	（Ascend 5）説明はありません。
134	DHCP-Maximum-Leases	（Ascend 5）説明はありません。
135	Primary-DNS-Server	Microsoft PPP クライアントにより IPCP ネゴシエーション中にネットワーク アクセス サーバから要求される可能性がある、プライマリ DNS サーバを特定します。
136	Secondary-DNS-Server	Microsoft PPP クライアントにより IPCP ネゴシエーション中にネットワーク アクセス サーバから要求される可能性がある、セカンダリ DNS サーバを特定します。
137	Client-Assign-DNS	説明はありません。
138	User-Acct-Type	説明はありません。
139	User-Acct-Host	説明はありません。

番号	ベンダー固有属性	説明
140	User-Acct-Port	説明はありません。
141	User-Acct-Key	説明はありません。
142	User-Acct-Base	説明はありません。
143	User-Acct-Time	説明はありません。
144	Assign-IP-Client	説明はありません。
145	Assign-IP-Server	説明はありません。
146	Assign-IP-Global-Pool	説明はありません。
147	DHCP-Reply	説明はありません。
148	DHCP-Pool-Number	説明はありません。
149	Expect-Callback	説明はありません。
150	Event-Type	説明はありません。
151	Session-Svr-Key	説明はありません。
152	Multicast-Rate-Limit	説明はありません。
153	IF-Netmask	説明はありません。
154	Remote-Addr	説明はありません。
155	Multicast-Client	説明はありません。
156	FR-Circuit-Name	説明はありません。
157	FR-LinkUp	説明はありません。
158	FR-Nailed-Grp	説明はありません。
159	FR-Type	説明はありません。
160	FR-Link-Mgt	説明はありません。
161	FR-N391	説明はありません。
162	FR-DCE-N392	説明はありません。

番号	ベンダー固有属性	説明
163	FR-DTE-N392	説明はありません。
164	FR-DCE-N393	説明はありません。
165	FR-DTE-N393	説明はありません。
166	FR-T391	説明はありません。
167	FR-T392	説明はありません。
168	Bridge-Address	説明はありません。
169	TS-Idle-Limit	説明はありません。
170	TS-Idle-Mode	説明はありません。
171	DBA-Monitor	説明はありません。
172	Base-Channel-Count	説明はありません。
173	Minimum-Channels	説明はありません。
174	IPX-Route	説明はありません。
175	FT1-Caller	説明はありません。
176	Backup	説明はありません。
177	Call-Type	説明はありません。
178	Group	説明はありません。
179	FR-DLCI	説明はありません。
180	FR-Profile-Name	説明はありません。
181	Ara-PW	説明はありません。
182	IPX-Node-Addr	説明はありません。
183	Home-Agent-IP-Addr	Ascend Tunnel Management Protocol（ATMP）を使用する際に、ホーム エージェントの IP アドレスをドット付き 10 進表記で示します。

番号	ベンダー固有属性	説明
184	Home-Agent-Password	ATMP で、外部のエージェントが自身の認証に使用するパスワードを指定します。
185	Home-Network-Name	ATMP で、ホーム エージェントがすべてのパケットを送信する接続プロファイルの名前を示します。
186	Home-Agent-UDP-Port	外部のエージェントが ATMP メッセージをホーム エージェントに送信する際に使用する UDP ポート番号を示します。
187	Multilink-ID	セッションが終了した時のマルチリンク バンドルの ID 番号をレポートします。この属性は、マルチリンク バンドルの一部のセッションに適用されます。Multilink-ID 属性は、認証応答パケットに送信されます。
188	Num-In-Multilink	アカウンティング終了パケットでレポートされたセッションが終了したときにマルチリンク バンドルに残っているセッション数をレポートします。この属性は、マルチリンク バンドルの一部のセッションに適用されます。Num-In-Multilink 属性は、認証応答パケットと一部のアカウンティング要求パケットで送信されます。
189	First-Dest	認証後最初に受信したパケットの宛先 IP アドレスを記録します。
190	Pre-Bytes-In	認証前の入力バイト数を記録します。Pre-Bytes-In 属性は、アカウンティング終了記録で送信されます。

番号	ベンダー固有属性	説明
191	Pre-Bytes-Out	認証前の出力バイト数を記録します。Pre-Bytes-Out 属性は、アカウンティング終了記録で送信されます。
192	Pre-Paks-In	認証前の入力パケット数を記録します。Pre-Paks-In 属性は、アカウンティング終了記録で送信されます。
193	Pre-Paks-Out	認証前の出力パケット数を記録します。Pre-Paks-Out 属性は、アカウンティング終了記録で送信されます。
194	Maximum-Time	任意のセッションで許可される最大時間長を秒で指定します。セッションがこの制限した時間に達すると、接続がドロップします。
195	Disconnect-Cause	接続がオフラインになった理由を特定します。Disconnect-Cause 属性は、アカウンティング終了記録で送信されます。また、この属性で、認証が実行される前に接続が切断された場合、最初に開始レコードを生成せずに終了レコードが生成されます。意味の詳細については、ベンダー固有属性（VSA）および RADIUS Disconnect-Cause 属性値の説明を参照してください。
196	Connect-Progress	接続が切断される前の接続状態を示します。
197	Data-Rate	接続のライフタイムでの平均ビット/秒値を指定します。Data-Rate 属性は、アカウンティング終了記録で送信されます。

番号	ベンダー固有属性	説明
198	PreSession-Time	コールが最初に接続された時から認証が完了した時までの時間長を秒で指定します。 PreSession-Time 属性は、アカウンティング終了記録で送信されます。
199	Token-Idle	キャッシュされたトークンが認証間での接続を持続できる最長時間を分で示します。
201	Require-Auth	CLID 認証が行われたクラスで、追加認証が必要かどうかを定義します。
202	Number-Sessions	RADIUS アカウンティング サーバにレポートするクラスごとのアクティブ セッション数を指定します。
203	Authen-Alias	PPP 認証中の RADIUS サーバのログイン名を定義します。
204	Token-Expiry	キャッシュされたトークンのライフタイムを定義します。
205	Menu-Selector	ユーザにデータの入力を指示するために使用するストリングを定義します。
206	Menu-Item	ユーザプロファイルの単一メニュー項目を指定します。プロファイルごとに最大 20 のメニュー項目を割り当てられます。
207	PW-Warntime	（Ascend 5）説明はありません。
208	PW-Lifetime	ユーザ単位ベースで、パスワードの有効日数を指定できます。

番号	ベンダー固有属性	説明
209	IP-Direct	この属性をユーザのファイル エントリに含めると、フレーム ルートがルーティングおよびブリッジング テーブルにインストールされます。 （注） パケット ルーティングは、この新しくインストールしたエントリだけではなくテーブル全体に依存しています。この属性を含めても、すべてのパケットが指定の IP アドレスに送信されるとは限りません。したがって、この属性は、完全にサポートされていません。このような属性の制限は、Cisco ルータが内部ルーティングやブリッジング テーブルを一部しかバイパスできず、指定した IP アドレスにパケットを送信できないために起こります。
210	PPP-VJ-Slot-Comp	VJ 圧縮パケットを PPP リンク経由で送信する際に、Cisco ルータでスロット圧縮しないように指示します。
211	PPP-VJ-1172	PPP で、VJ 圧縮に 0x0037 値を使用するように指示します。

番号	ベンダー固有属性	説明
212	PPP-Async-Map	Cisco ルータに、PPP セッション用の非同期制御文字マップを提供します。指定した制御文字は、PPP リンク経由でデータとして渡され、リンク上で起動しているアプリケーションで使用されます。
213	Third-Prompt	ユーザ名とパスワードの次の、ユーザが追加で入力する 3 番めのプロンプトを定義します。
214	Send-Secret	アウトダイヤル パスワードの通常のパスワードの代わりに暗号化パスワードを使用できるようにします。
215	Receive-Secret	暗号化パスワードを RADIUS サーバで検証できるようにします。
216	IPX-Peer-Mode	（Ascend 5）説明はありません。
217	IP-Pool-Definition	アドレスのプールを X a.b.c Z の形式で定義します。ここで、X はプールインデックス番号、a.b.c はプールの開始 IP アドレス、Z はプールの IP アドレス数です。たとえば、3 10.0.0.1 5 は、10.0.0.1 から 10.0.0.5 までをダイナミック割り当てに割り当てます。
218	Assign-IP-Pool	ルータに、ユーザおよび IP アドレスを IP プールから割り当てるよう指示します。
219	FR-Direct	フレーム リレー リダイレクト モードで接続プロファイルを処理するかどうかを定義します。

番号	ベンダー固有属性	説明
220	FR-Direct-Profile	この接続をフレーム リレー スイッチまで伝送するフレーム リレー プロファイルの名前を定義します。
221	FR-Direct-DLCI	この接続をフレーム リレー スイッチまで伝送する DLCI を示します。
222	Handle-IPX	NCP のウォッチドッグ要求の処理方法を示します。
223	Netware-Timeout	RADIUS サーバが NCP ウォッチドッグ パケットに応答する時間を分で定義します。
224	IPX-Alias	番号が付いたインターフェイスが必要な IPX ルータでエイリアスを定義できます。
225	Metric	説明はありません。
226	PRI-Number-Type	説明はありません。
227	Dial-Number	ダイヤルする番号を定義します。
228	Route-IP	IP ルーティングがユーザのファイル エントリで許可されているかどうかを示します。
229	Route-IPX	IPX ルーティングをイネーブルにできます。
230	Bridge	説明はありません。
231	Send-Auth	CLID 認証に続く、username-password 認証で使用するプロトコル（PAP または CHAP）を定義します。

番号	ベンダー固有属性	説明
232	Send-Passwd	RADIUS サーバで、発信コールの接続のリモート エンドに送信するパスワードを指定できます。
233	Link-Compression	PPP リンクで「stac」圧縮をオンまたはオフのどちらにするかを定義します。 リンク圧縮は、次のように、数値で定義します。 • 0：なし • 1：Stac • 2：Stac-Draft-9 • 3：MS-Stac
234	Target-Util	PPP マルチリンクが定義されている場合に、追加チャネルを立ち上げる負荷しきい値を割合で指定します。
235	Maximum-Channels	割り当て済み/割り当て可能な最大チャネル数を指定します。
236	Inc-Channel-Count	説明はありません。
237	Dec-Channel-Count	説明はありません。
238	Seconds-of-History	説明はありません。
239	History-Weigh-Type	説明はありません。
240	Add-Seconds	説明はありません。
241	Remove-Seconds	説明はありません。

番号	ベンダー固有属性	説明
242	Data-Filter	ユーザごとの IP データ フィルタを定義します。これらのフィルタは、コールが RADIUS 発信プロファイルを使用して発信された場合か、RADIUS 着信プロファイルを使用して応答した場合にのみ取得されます。最初に一致したフィルタのエントリが適用されます。したがって、フィルタのエントリの入力順が重要です。
243	Call-Filter	ユーザごとの IP データ フィルタを定義します。Cisco ルータでは、この属性は Data-Filter 属性と同一です。
244	Idle-Limit	セッションがアイドル状態を持続できる最大時間を秒で指定します。セッションがこのアイドル時間に達すると、接続がドロップします。
245	Preempt-Limit	説明はありません。
246	Callback	コールバックをイネーブルまたはディセーブルにできます。
247	Data-Svc	説明はありません。
248	Force-56	チャネルの 64 K すべてが使用可能に見える場合でも、ネットワーク アクセス サーバが 56 K の部分のみを使用するかどうかを指定します。
249	Billing Number	説明はありません。
250	Call-By-Call	説明はありません。
251	Transit-Number	説明はありません。
252	Host-Info	説明はありません。

番号	ベンダー固有属性	説明
253	PPP-Address	PPP IPCP ネゴシエーション中に発信ユニットにレポートされた IP アドレスを示します。
254	MPP-Idle-Percent	説明はありません。
255	Xmit-Rate	（Ascend 5）説明はありません。

ベンダー固有 RADIUS 属性の詳細については、「RADIUS の設定」機能モジュールを参照してください。

RADIUS ベンダー固有属性の機能情報

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 *6* : ***RADIUS*** ベンダー固有属性の機能情報

機能名	リリース	機能情報
RADIUS ベンダー固有属性	Cisco IOS XE Release 2.1	IETF ドラフト標準には、RADIUS でのネットワーク アクセス サーバと RADIUS サーバ間でベンダー固有情報を通信する方式が規定されています。ただし、ベンダーには固有のアプリケーション向けに拡張した RADIUS 属性セットを持つものがあります。このマニュアルでは、これらベンダー固有 RADIUS 属性の Cisco IOS XE でのサポート情報について記載します。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

第 4 章

RADIUS ベンダー固有属性および RADIUS Disconnect-Cause 属性値

インターネット技術特別調査委員会（IETF）ドラフト標準には、ネットワーク アクセス サーバと RADIUS サーバの間でベンダー固有属性（属性 26）を使用してベンダー固有の情報を伝達する方法が規定されています。属性 26 はベンダー固有属性をカプセル化します。このため、ベンダーは一般的な用途に適さない独自の拡張属性をサポートできます。

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。

RADIUSベンダー固有属性およびRADIUSDisconnect-Cause属性値に関する情報

シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダータイプ 1（名前は「cisco-avpair」）です。値は、次の形式のストリングです。

```
protocol : attribute sep value *
```

「Protocol」は、特定の認可タイプを表すシスコの「protocol」属性です。使用可能なプロトコルには、IP、IPX、VPDN、VOIP、SHELL、RSVP、SIP、AIRNET、OUTBOUND があります。「attribute」および「value」は、シスコの TACACS+ 仕様で定義されている適切な属性値（AV）ペアです。「sep」は、必須の属性の場合は「=」、任意指定の属性の場合は「*」です。これにより、TACACS+ 認可で使用できるすべての機能を RADIUS にも使用できるようになります。

たとえば、次の AV ペアは IP 許可の際（PPP の IPCP アドレス割り当ての際）、シスコの「multiple named ip address pools」機能を起動します。

```
cisco-avpair= ″ip:addr-pool=first″
```

「*」を挿入すると、AV ペア「ip:addr-pool=first」は任意指定になります。AV ペアはオプションにできることに注意してください。

```
cisco-avpair= ″ip:addr-pool*first″
```

次に、ネットワーク アクセス サーバからユーザがログインしたときに、すぐに EXEC コマンドを実行する方法の例を示します。

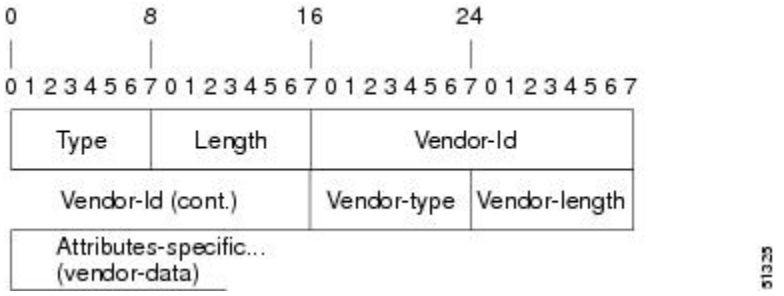
```
cisco-avpair= ″shell:priv-lvl=15″
```

属性 26 には、次の 3 つの要素が含まれています。

- タイプ
- 長さ
- ストリング（またはデータ）
    - Vendor-Id
    - Vendor-Type
    - Vendor-Length
    - Vendor-Data

次の図は、属性 26 の「背後で」カプセル化される VSA のパケットのフォーマットを示します。

図 *2*：属性 *26* の背後でカプセル化される *VSA*



（注） VSA の形式はベンダーが指定します。Attribute-Specific フィールド（Vendor-Data とも呼ばれる）は、ベンダーによるその属性の定義によって異なります。

次の表で、ベンダー固有 RADIUS IETF 属性の表（次の 2 番目の表。サポートされるベンダー固有 RADIUS 属性（IETF 属性 26）を記載）に記載されている重要なフィールドについて説明します。

表 *7*：ベンダー固有属性表のフィールドの説明

フィールド	説明
番号	次の表に示されるすべての属性は、IETF 属性 26 の拡張です。
Vendor-Specific Command Codes	特定のベンダーの識別に使用する定義されたコード。コード 9 は Cisco VSA、311 は Microsoft VSA、529 は Ascend VSA を定義します。
Sub-Type Number	属性 ID 番号。この番号は、属性 26 の背後でカプセル化される「2 番目のレイヤ」の ID 番号である以外は、IETF 属性の ID 番号に似ています。
属性	属性の ASCII ストリング名。
説明	属性の説明。

表 *8*：ベンダー固有 *RADIUS IETF* 属性

番号	ベンダー固有企業コード	Sub-Type Number	属性	説明
MS-CHAP 属性				

番号	ベンダー固有企業コード	Sub-Type Number	属性	説明
26	311	1	MSCHAP-Response	PPP MS-CHAP ユーザがチャレンジに対する応答で提供するレスポンス値が含まれます。Access-Request パケットでしか使用されません。この属性は、PPP CHAP ID と同じです（RFC 2548）。
26	311	11	MSCHAP-Challenge	ネットワークアクセスサーバが MS-CHAP ユーザに送信するチャレンジが含まれます。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。（RFC 2548）。
VPDN 属性				
26	9	1	l2tp-busy-disconnect	LNS の vpdn-group で、事前にコピーするよう設定された仮想テンプレートを使用している場合、この属性は、接続先の事前にコピーされたインターフェイスが検索されない、新しい L2TP セッションのディスポジションを制御します。属性が true（デフォルト）の場合、セッションが LNS により切断されます。そうでない場合は、新しいインターフェイスが仮想テンプレートからコピーされます。

番号	ベンダー固有企業コード	Sub-Type Number	属性	説明
26	9	1	l2tp-cm-local-window-size	L2TP 制御メッセージの最大受信ウィンドウサイズを指定します。この値は、トンネルの確立中にピアにアドバタイズされます。
26	9	1	l2tp-drop-out-of-order	正しくない順序で受信したデータパケットをドロップして、シーケンス番号を順守します。これは受信した場合の処理方法であって、データパケット上でシーケンス番号が送信されるわけではありません。
26	9	1	l2tp-hello-interval	hello キープアライブインターバルの秒数を指定します。ここで指定した秒数、トンネルでデータが送信されないと、hello パケットが送信されます。
26	9	1	l2tp-hidden-avp	イネーブルにすると、L2TP 制御メッセージで、大文字小文字を区別する AVP にスクランブルがかけられるか、または非表示になります。
26	9	1	l2tp-nosession-timeout	タイムアウトおよびシャットダウンまでに、セッションなしでトンネルがアクティブのままになる秒数を指定します。

番号	ベンダー固有企業コード	Sub-Type Number	属性	説明
26	9	1	tunnel-tos-reflect	LNS でトンネルに入るパケットに対して、IP ToS フィールドを各ペイロード パケットの IP ヘッダーからトンネル パケットの IP ヘッダーにコピーします。
26	9	1	l2tp-tunnel-authen	この属性を設定すると、L2TP トンネル認証が実行されます。
26	9	1	l2tp-tunnel-password	L2TP トンネル認証および AVP 隠蔽に使用される共有秘密。
26	9	1	l2tp-udp-checksum	これは認可属性で、L2TP がデータ パケットに対して UDP チェックサムを実行する必要があるかどうかを定義します。有効な値は「yes」および「no」です。デフォルトは no です。
H323 属性				
26	9	23	Remote-Gateway-ID（h323-remote-address）	リモート ゲートウェイの IP アドレスを示します。
26	9	24	Connection-ID（h323-conf-id）	会議 ID を識別します。
26	9	25	Setup-Time（h323-setup-time）	以前、グリニッジ標準時（GMT）およびズールタイムと呼ばれていた協定世界時（UTC）でのこの接続のセットアップ時間を示します。

番号	ベンダー固有企業コード	Sub-Type Number	属性	説明
26	9	26	Call-Origin（h323-call-origin）	ゲートウェイに対するコールの発行元を示します。有効値は、originating および terminating です（回答）。
26	9	27	Call-Type（h323-call-type）	コールのレグタイプを示します。有効値は、**telephony** および **VoIP** です。
26	9	28	Connect-Time（h323-connect-time）	このコール レッグの UTC での接続時間を示します。
26	9	29	Disconnect-Time（h323-disconnect-time）	このコール レッグが UTC で接続解除された時間を示します。
26	9	30	Disconnect-Cause（h323-disconnect-cause）	Q.931 仕様によって、接続がオフラインにされた理由を示します。
26	9	31	Voice-Quality（h323-voice-quality）	コールの音声品質に影響する Impairment Factor（ICPIF）を指定します。
26	9	33	Gateway-ID（h323-gw-id）	下位のゲートウェイの名前を示します。
大規模のダイヤルアウト属性				
26	9	1	callback-dialstring	コールバックに使用するダイヤリング文字列を定義します。
26	9	1	data-service	説明はありません。
26	9	1	dial-number	ダイヤルする番号を定義します。

番号	ベンダー固有企業コード	Sub-Type Number	属性	説明
26	9	1	force-56	チャネルの 64 K すべてが使用可能に見える場合でも、ネットワーク アクセス サーバが 56K の部分のみを使用するかどうかを指定します。
26	9	1	map-class	ユーザ プロファイルに、ダイヤルアウトするネットワーク アクセス サーバ上で同じ名前のマップ クラスで設定される情報の参照を許可します。
26	9	1	send-auth	CLID 認証に続く、username-password 認証で使用するプロトコル（PAP または CHAP）を定義します。
その他の属性				

番号	ベンダー固有企業コード	Sub-Type Number	属性	説明
26	9	2	Cisco-NAS-Port	NAS-Portアカウンティングに追加的なベンダー固有属性（VSA）を指定します。属性値ペア（AVPair）ストリングの形式で追加的なNAS-Port情報を指定するには、radius-server vsa send グローバル コンフィギュレーション コマンドを使用します。 （注） この VSA は、通常アカウンティングで使用されますが認証（Access-Request）パケットで使用される場合もあります。
26	9	1	min-links	MLP に対するリンクの最小数を設定します。
26	9	1	proxyacl#<n>	ダウンロード可能なユーザ プロファイル（ダイナミック ACL）を、認証プロキシを使用して設定でき、これにより設定されたインターフェイスのトラフィックの通過を許可するよう、認証を設定できます。

番号	ベンダー固有企業コード	Sub-Type Number	属性	説明
26	9	1	spi	登録中にホーム エージェントがモバイル ノードの認証で必要とする認証情報を伝送します。コンフィギュレーション コマンド **ipmobilesecurehost<addr>** と同じ構文の情報です。基本的に、この文字列に続く残りのコンフィギュレーションコマンドはそのまま含まれます。これにはセキュリティパラメータインデックス（SPI）、キー、認証アルゴリズム、認証モード、およびリプレイ保護タイムスタンプ範囲が含まれています。
26	9	1	client-mac-address	PPPoE クライアントの MAC アドレスが含まれます。 （注） この属性は、PPP over Ethernet（PPPoE）または PPP over ATM（PPPoA）にのみ適用できます。

NAS を設定して VSA を認識し使用する方法については、「RADIUS の設定」機能モジュールの「ベンダー固有 RADIUS 属性を使用するためのルータの設定」セクションを参照してください。

RADIUS Disconnect-Cause 属性値

Disconnect-cause 属性値は、接続がオフラインにされた理由を指定します。属性値は、Accounting 要求パケットで送信されます。セッションの認証が失敗しても、これらの値は、セッションの終了時に送信されます。セッションが認証されないと、属性が開始レコードを生成せずに終了レコードを発生させる可能性があります。

次の表に、Disconnect-Cause（195）属性の原因コード、値、および説明を示します。

（注） Disconnect-Cause は、RADIUS AVPairs で使用されるごとに 1000 ずつ増分されます。たとえば、disc-cause 4 は 1004 になります。

表 *9* : ***Disconnect-Cause*** 属性値

原因コード	値	説明
2	不明（Unknown）	理由は不明。
4	CLID-Authentication-Failure	calling-party 数の認証の失敗。
10	No-Carrier	キャリアが検出されない。 （注） 最初のモデム接続中に接続解除があると、コード 10、11、および 12 が送信される場合があります。
11	Lost-Carrier	キャリアの喪失。
12	No-Detected-Result-Codes	モデム結果コード検出の失敗。
20	User-Ends-Session	ユーザがセッションを終了した。 （注） コード 20、22、23、24、25、26、27、および 28 は、EXEC セッションに適用されます。
21	Idle-Timeout	ユーザ入力待機中のタイムアウト。 コード 21、100、101、102、および 120 は、すべてのセッションタイプに適用されます。
22	Exit-Telnet-Session	既存の Telnet セッションによる接続解除。

原因コード	値	説明
23	No-Remote-IP-Addr	SLIP/PPP への切り替え不能。リモートエンドに IP アドレスがない。
24	Exit-Raw-TCP	既存の raw TCP による接続解除。
25	Password-Fail	間違ったパスワード。
26	Raw-TCP-Disabled	Raw TCP がディセーブルにされた。
27	Control-C-Detected	Control-C が検出された。
28	EXEC-Process-Destroyed	EXEC プロセスが破棄された。
40	Timeout-PPP-LCP	PPP LCP ネゴシエーションがタイムアウトした。 （注） コード 40、41、42、43、44、45、および 46 は、PPP セッションに適用されます。
41	Failed-PPP-LCP-Negotiation	PPP LCP ネゴシエーションが失敗した。
42	Failed-PPP-PAP-Auth-Fail	PPP PAP 認証が失敗した。
43	Failed-PPP-CHAP-Auth	PPP CHAP 認証が失敗した。
44	Failed-PPP-Remote-Auth	PPP リモート認証が失敗した。
45	PPP-Remote-Terminate	PPP がリモート エンドから Terminate Request を受信した。
46	PPP-Closed-Event	上位層がセッションの終了を要求した。
63	PPP-Echo-Replies	TCP 接続が終了した。
100	Session-Timeout	セッションがタイムアウトした。
101	Session-Failed-Security	セキュリティ上の理由から、セッションが失敗した。
102	Session-End-Callback	コールバックにより、セッションが終了した。

原因コード	値	説明
120	Invalid-Protocol	検出されたプロトコルがディセーブルにされていたため、コールが拒否された。
600	VPN-User-Disconnect	クライアントによってコールが接続解除された（PPP 経由）。 LNS がクライアントから PPP terminate request を受信するとコードが送信されます。
601	VPN-Carrier-Loss	キャリアの喪失。これは回線が物理的に普通になった結果である場合があります。 クライアントがダイヤラを使用してダイヤルアウトできない場合、コードが送信されます。
602	VPN-No-Resources	コールの処理に使用できるリソースがない。 クライアントがメモリを割り当てることができない場合、コードが送信されます（メモリの不足）。
603	VPN-Bad-Control-Packet	L2TP または L2F 制御パケットが間違っている。 このコードは、必須の属性値ペア（AVP）が欠落しているなど、ピアから受信した制御パケットが無効な場合に送信されます。L2TP を使用すると、コードは 6 回の再送信後に送信されます。L2F を使用すると、再送信の回数はユーザ設定が可能です。 （注） トンネルにアクティブなセッションがある場合は、VPN-Tunnel-Shut が送信されます。

原因コード	値	説明
604	VPN-Admin-Disconnect	管理上の接続解除。これは、VPN ソフトシャットダウンの結果である場合があります。これは、クライアントが最大セッション制限に達するか、最大ホップカウントを超過した場合に発生します。 トンネルが、**clearvpdntunnel** コマンドの発行によってダウンした場合に、コードが送信されます。
605	VPN-Tunnel-Shut	トンネルのティアダウン、またはトンネルのセットアップが失敗した。 トンネルにアクティブなセッションがあり、トンネルがダウンした場合にコードが送信されます。 （注） このコードはトンネルの認証が失敗した場合は、送信されません。
606	VPN-Local-Disconnect	LNS PPP モジュールによって、コールが接続解除された。 LNS がクライアントに PPP terminate request を送信するとコードが送信されます。これは通常の PPP 接続解除が LNS によって開始されたことを示します。
607	VPN-Session-Limit	VPN ソフト シャットダウンがイネーブルになった。 前述したソフトシャットダウンの制約事項のいずれかによってコールが拒否されると、コードが送信されます。
611	VPDN-Tunnel-In-Resync	VPDN トンネルは HA 再同期中です。

その他の参考資料

ここでは、RADIUS ベンダー固有属性（VSA）および RADIUS Disconnect-Cause 属性値に関する関連資料について説明します。

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』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
セキュリティ機能	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』
セキュリティ サーバ プロトコル	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「セキュリティ サーバ プロトコル」の項
RADIUS Configuration	「RADIUS の設定」機能モジュール。

標準

規格	タイトル
インターネット技術特別調査委員会（IETF）インターネット ドラフト：Network Access Servers Requirements	「Network Access Servers Requirements: Extended RADIUS Practices」

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 2865	『Remote Authentication Dial In User Service (RADIUS)』

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 Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

RADIUSベンダー固有属性およびRADIUSDisconnect-Cause属性値の機能情報

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 *10*：*RADIUS* ベンダー固有属性（*VSA*）および *RADIUS Disconnect-Cause* 属性値の機能情報

機能名	リリース	機能情報
VPDN Disconnect Cause のアカウンティング	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。

機能名	リリース	機能情報
ベンダー固有の RADIUS 属性	Cisco IOS XE Release 2.1	このマニュアルは、ネットワーク アクセス サーバと RADIUS サーバの間でベンダー固有属性（属性26）を使用してベンダー固有の情報を伝達する方法を規定するインターネット技術特別調査委員会（IETF）ドラフト標準を扱います。属性 26 はベンダー固有属性をカプセル化します。このため、ベンダーは一般的な用途に適さない独自の拡張属性をサポートできます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

第 5 章

Connect-Info RADIUS 属性 77

Connect-Info RADIUS 属性 77 機能を使用すれば、ネットワーク アクセス サーバ（NAS）から、RADIUS クライアント（ダイヤルイン モデム）に送信される RADIUS アカウンティング「start」および「stop」レコード内で Connect-Info（属性 77）を報告できます。これらのレコードを使用すれば、送受信の接続速度、変調、および圧縮を比較することによって、接続端（ネゴシエーション後）での速度がさまざまなダイヤルイン モデム上のユーザ セッションを分析できます。

ネットワーク アクセス サーバ（NAS）からアカウンティング「start」および「stop」レコード内で属性 77 を送信したときの接続レートをプラットフォーム上で測定できます。「送信」速度（NAS モデムが情報を送信する速度）と「受信」速度（NAS が情報を受信する速度）を記録することによって、ユーザ モデム接続でセッションの開始直後に速度を落とすようにネゴシエーションをやり直すかどうかを判断できます。送信速度と受信速度が異なる場合は、属性 77 が両方の速度を報告します。これによって、顧客ごとにセッションからモデム接続速度を取得できます。

属性 77 は、PPPoX などのブロードバンド接続用のクラス文字列、ダイヤル アクセス用の物理接続速度、および **ipvrfforwarding** コマンドで定義されたルータ インターフェイス上のセッションに関する VRF 文字列の送信にも使用されます。

（注） この機能は設定が不要です。

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。

Connect-Info RADIUS 属性 77 の前提条件

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、Connect-Info RADIUS 属性 77 の機能情報, （81 ページ）を参照してください。

NAS からアカウンティング「start」および「stop」レコード内で属性 77 を送信できるようにするには、次の作業を実行する必要があります。

- NAS を認証、認可、およびアカウンティング（AAA）用に設定し、着信モデム コールを受け入れるように設定します。
- グローバル コンフィギュレーション モードで **aaa accounting network default start-stop group radius** コマンドを使用して、AAA アカウンティングを有効にします。
- グローバル コンフィギュレーション モードで **modem link-info poll time** コマンドを使用して、モデム ポーリング タイマーを変更します。

（注） モデム ポーリング タイマーの変更は、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ上で必要です。

Connect-Info RADIUS 属性 77 に関する情報

設定可能な Connect-Info 属性機能により、RADIUS 属性 77（Connect-Info）のサポートが導入されました。これにより、RADIUS アカウンティング「start」および「stop」レコードを使用して、モデム ダイヤルイン接続の接続速度、変調、圧縮に関する情報が提供されます。

イーサネット接続での属性 77 のカスタマイズ

イーサネット接続での属性 77 をカスタマイズするには、イーサネット サブインターフェイスに適用されるサービス ポリシーの名前として接続情報を入力します。ルータはそのポリシー名を取得して、属性 77 にコピーします。

たとえば、次の設定で、speed:eth:25100:5100:19/0 という名前のアウトバウンド サービス ポリシーが、QinQ ギガビット イーサネット サブインターフェイス 1/0/0.2696 に適用されます。ルータはそのポリシー名を属性 77 にコピーし、これを Access-Request、Accounting-Start、または Accounting-Stop メッセージで RADIUS サーバに送信します。

```
interface GigabitEthernet1/0/0.2696
encapsulation dot1q 2696 second-dot1q 256
pppoe enable group global
no snmp trap link-status
service-policy input set_precedence_to_0
service-policy output speed:eth:25100:5100:19/0
```

ATM 接続での属性 77 のカスタマイズ

ATM 接続の属性 77 をカスタマイズするには、次のコンフィギュレーション モードで **aaa connect-info** *string* コマンドを設定します。

- PVC（特定の PVC の場合）
- PVC 範囲（一定範囲の PVC の場合）
- PVC-in-range（一定範囲の PVC の特定 PVC の場合）
- VC クラス（特定の **class-vc** コマンドの指定による）

ルータは、 **class-vc** コマンドで指定した VC クラスの名前、または **aaa connect-info** *string* コマンドで指定した文字列を取得して、属性 77 にコピーします。

たとえば、次の設定では、ATM PVC 10/42 と 10/43 の両方で **class-vc** コマンドが設定され、PVC 10/42 で **aaa connect-info** コマンドが設定されます。

```
interface ATM1/0/0.1 multipoint
description TDSL clients - default TDSL 1024 no ip mroute-cache
class-int speed:ubr:1184:160:10
range pvc 10/41 10/160
!
pvc-in-range 10/42
class-vc speed:ubr:2303:224:10
aaa connect-info speed:ubr:2303:224:10:isp-specific-descr
!
pvc-in-range 10/43
class-vc speed:ubr:2303:224:10
```

PVC 10/42 の場合、ルータは、**aaa connect-info** コマンドで指定された文字列（speed:ubr:2303:224:10:isp-specific-descr）を取得し、属性 77 にコピーします。サブインターフェイスで **aaa connect-info** コマンドが設定されない場合、ルータは **class-vc** コマンドで指定されたクラス名（speed:ubr:2303:224:10）を取得し、属性 77 にコピーします。

PVC 10/43 の場合、ルータは **class-vc** コマンドで指定されたクラス名（speed:ubr:2303:224:10）を取得し、属性 77 にコピーします。

Connect-Info RADIUS 属性 77 の確認方法

Connect-Info RADIUS 属性 77 の確認

アカウンティング「start」および「stop」レコード内の属性 77 を確認するには、特権 EXEC モードで **debugradius** コマンドを使用します。

手順の概要

1. イネーブル化
2. **debugradius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**debugradius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。

例

次の例は、Connect-Info [77] アカウンティング属性を示しています。

```
Router# debug radius
Sep 8 21:53:05.242: RADIUS/ENCODE(00007D34):Orig. component type = PPPoE
Sep 8 21:53:05.242: RADIUS: AAA Unsupported Attr: interface [208] 10
Sep 8 21:53:05.242: RADIUS: 30 2F 31 2F 30 2F 39 2E [ 0/1/0/9.]
Sep 8 21:53:05.242: RADIUS: AAA Unsupported Attr: client-mac-address[45] 14
Sep 8 21:53:05.242: RADIUS: 30 30 30 30 2E 63 30 30 31 2E 30 31 [ 0000.c001.01]
Sep 8 21:53:05.242: RADIUS(00007D34): Config NAS IP: 0.0.0.0
Sep 8 21:53:05.242: RADIUS/ENCODE(00007D34): acct_session_id: 32042
Sep 8 21:53:05.242: RADIUS(00007D34): sending
Sep 8 21:53:05.242: RADIUS/ENCODE: Best Local IP-Address 10.3.8.2 for Radius-Server 10.3.1.107

Sep 8 21:53:05.242: RADIUS(00007D34): Send Access-Request to 10.3.1.107:1645 id 1645/1, len
 116
```

```
Sep 8 21:53:05.242: RADIUS: authenticator FC 82 50 DB 65 8F 21 A9 - F3 0A A8 09 29 E5 56
65
Sep 8 21:53:05.242: RADIUS: Framed-Protocol [7] 6 PPP [1]
Sep 8 21:53:05.242: RADIUS: User-Name [1] 8 ''user1''
Sep 8 21:53:05.242: RADIUS: User-Password [2] 18 *
Sep 8 21:53:05.242: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
Sep 8 21:53:05.242: RADIUS: NAS-Port [5] 6 0
Sep 8 21:53:05.242: RADIUS: NAS-Port-Id [87] 12 ''0/1/0/9.32''
Sep 8 21:53:05.242: RADIUS: Connect-Info [77] 28 ''speed:ubr:3456:448:10/0000''
Sep 8 21:53:05.242: RADIUS: Service-Type [6] 6 Framed [2]
Sep 8 21:53:05.242: RADIUS: NAS-IP-Address [4] 6 10.3.8.2
Sep 8 21:53:05.242: RADIUS(00007D34): Started 5 sec timeout
Sep 8 21:53:05.244: RADIUS: Received from id 1645/1 10.3.1.107:1645, Access-Accept, len 32

Sep 8 21:53:05.244: RADIUS: authenticator 9A F1 29 01 66 53 17 CB - 73 FB 1B CE 7D 80 04
F2
Sep 8 21:53:05.244: RADIUS: Service-Type [6] 6 Framed [2]
Sep 8 21:53:05.244: RADIUS: Framed-Protocol [7] 6 PPP [1]
Sep 8 21:53:05.244: RADIUS(00007D34): Received from id 1645/1
Sep 8 21:53:05.248: RADIUS/ENCODE(00007D34):Orig. component type = PPPoE
Sep 8 21:53:05.248: RADIUS(00007D34): Config NAS IP: 0.0.0.0
Sep 8 21:53:05.248: RADIUS(00007D34): sending
Sep 8 21:53:05.248: RADIUS/ENCODE: Best Local IP-Address 10.3.8.2 for Radius-Server 5.3.1.107

Sep 8 21:53:05.248: RADIUS(00007D34): Send Accounting-Request to 10.3.1.107:1646 id 1646/3,
 len 126
Sep 8 21:53:05.248: RADIUS: authenticator 71 6E 73 9B FD 7E 82 81 - 10 2A CD 83 A8 BD D2
F0
Sep 8 21:53:05.248: RADIUS: Acct-Session-Id [44] 10 ''00007D2A''
Sep 8 21:53:05.248: RADIUS: Framed-Protocol [7] 6 PPP [1]
Sep 8 21:53:05.248: RADIUS: User-Name [1] 8 ''user1''
Sep 8 21:53:05.248: RADIUS: Acct-Authentic [45] 6 RADIUS [1]
Sep 8 21:53:05.248: RADIUS: Acct-Status-Type [40] 6 Start [1]
Sep 8 21:53:05.248: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
Sep 8 21:53:05.248: RADIUS: NAS-Port [5] 6 0
Sep 8 21:53:05.248: RADIUS: NAS-Port-Id [87] 12 ''0/1/0/9.32''
Sep 8 21:53:05.248: RADIUS: Connect-Info [77] 28 ''speed:ubr:3456:448:10/0000
```

Connect-Info RADIUS 属性 77 の設定例

AAA と着信モデム コール用の NAS の設定例

次の例は、AAA と着信モデム コール用の NAS 設定のサンプルです。

```
interface Serial0:15
  no ip address
  isdn switch-type primary-net5
  isdn incoming-voice modem
!
interface Async1
  ip address 192.0.2.2 255.255.255.0
  encapsulation ppp
  async default routing
  async mode interactive
  no peer default ip address
  ppp authentication chap
!
line 1
  modem InOu
  transport preferred none
  transport input all
  autoselect ppp
!
```

その他の参考資料

次の項で、Connect-Info RADIUS 属性 77 機能に関連する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
IOS ダイヤル テクノロジー	『Cisco IOS XE Dial Technologies Configuration Guide, Release 2』
	『*Cisco IOS Dial Technologies Command Reference*』
セキュリティ コマンド	『*Cisco IOS Security 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 IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、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 2869	『RADIUS Extensions』

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 Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

Connect-Info RADIUS 属性 77 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 *11*：*Connect-Info RADIUS* 属性 *77* の機能情報

機能名	リリース	機能情報
Connect-Info RADIUS 属性 77	Cisco IOS XE Release 2.1	Connect-Info RADIUS 属性 77 機能を使用すれば、ネットワーク アクセス サーバ（NAS）から、RADIUS クライアント（ダイヤルイン モデム）に送信される RADIUS アカウンティング「start」および「stop」レコード内で Connect-Info（属性 77）を報告できます。これらの「start」および「stop」レコードを使用すれば、送受信の接続速度、変調、および圧縮を比較することによって、接続端（ネゴシエーション後）での速度がさまざまなダイヤルイン モデム上のユーザ セッションを分析できます。 この機能は、Cisco IOS XE リリース 2.1 で、Cisco ASR 1000 シリーズ ルータに導入されました。

第 6 章

暗号化されたベンダー固有属性

暗号化されたベンダー固有属性の機能により、ユーザは RADIUS サーバでフィルタを一元的に管理することができます。また、この機能は次の種類の文字列のベンダー固有属性（VSA）をサポートしています。

- タグ付きの文字列 VSA, （84 ページ） （この新しい VSA がタグ付きであることを除き、Cisco VSA Type 1（Cisco:AVPair (1)）に類似）
- 暗号化された文字列 VSA, （85 ページ） （この新しい VSA が暗号化されていることを除き、Cisco VSA Type 1 に類似）
- タグ付きおよび暗号化された文字列 VSA, （85 ページ） （この新しい VSA がタグ付きで、暗号化されていることを除き、Cisco VSA Type 1 に類似）

Cisco:AVPairs では、属性と値のペア（AVP）の文字列の形式で追加の認証情報および認可情報を指定します。Internet Engineering Task Force（IETF）の RADIUS 属性 26（Vendor-Specific）が、ベンダー ID 番号「9」およびベンダータイプ値「1」で転送された場合（Cisco AVPair であることを意味します）、Cisco AVPair の RADIUS ユーザ プロファイルは「Cisco:AVPair = "protocol:attribute=value"」というような形式になります。

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。

暗号化されたベンダー固有属性の前提条件

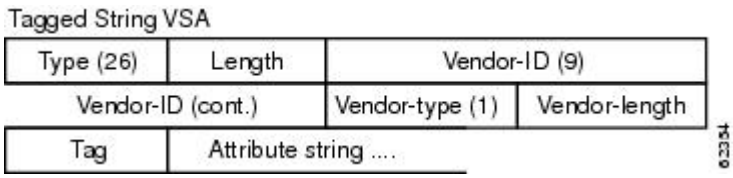
タグ付きで暗号化された VSA を RADIUS サーバが受け付けるようにするためには、AAA 認証および AAA 認可用にサーバを設定し、PPP コールを受け付けるように設定する必要があります。これらの作業方法については、暗号化されたベンダー固有属性の前提条件, （84 ページ）を参照してください。

暗号化されたベンダー固有属性に関する情報

タグ付きの文字列 VSA

次の図は、タグ付きの文字列 VSA のパケット形式を示します。

図 *3*：タグ付きの文字列 *VSA* の形式

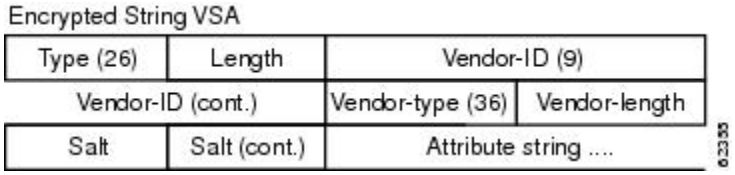


正しい値を取り出すために、Tag フィールドが正しく解析される必要があります。このフィールドの値の範囲はわずか 0x01 ～ 0x1F です。値が指定範囲内にない場合、RADIUS サーバはその値を無視し、Tag フィールドが Attribute String フィールドの一部であると見なします。

暗号化された文字列 VSA

次の図は、暗号化された文字列 VSA のパケット形式を示します。

図 *4*：暗号化された文字列 *VSA* の形式



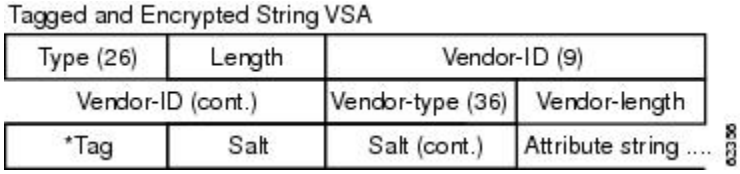
Salt フィールドは、VSA の各インスタンスの暗号化に使用される暗号キーの一意性を保証します。Salt フィールドの先頭の最上位ビットは 1 に設定する必要があります。

（注） Vendor-type (36) は、属性が暗号化された文字列 VSA であることを示しています。

タグ付きおよび暗号化された文字列 VSA

次の図は、新しくサポートされた各 VSA のパケットの形式を示しています。

図 *5*：タグ付きおよび暗号化された文字列 *VSA* の形式



この VSA は、Tag フィールドが追加されていることを除き、暗号化された文字列 VSA とほぼ同じです。Tag フィールドは、値が有効な範囲内（0x01 ～ 0x1F）にない場合、Salt フィールドの一部と見なされます。

暗号化されたベンダー固有属性の確認方法

暗号化されたベンダー固有属性の機能では、設定は必要ありません。RADIUS のタグ付きおよび暗号化 VSA が RADIUS サーバから送信されていることを検証するために、次のコマンドを特権 EXEC モードで実行します。

コマンド	目的
`Router#` **debug radius**	RADIUS 関連の情報を表示します。このコマンドの出力は、タグ付きおよび暗号化 VSA が RADIUS サーバから送信されているかどうかを示しています。

暗号化されたベンダー固有属性の設定例

NAS の設定例

次の例は、タグ付きおよび暗号化 VSA を使用して、基本的な設定のネットワーク アクセス サーバ（NAS）を設定する方法を示しています（この例では、PPP コールの確立に必要な設定がすでにイネーブルになっていると想定されています）。

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
!
radius-server host 10.2.2.2 auth-port 1645 acct-port 1646
radius-server key cisco
```

タグ付きおよび暗号化 VSA がある RADIUS ユーザ プロファイルの例

次の例は、タグ付きおよび暗号化された文字列 VSA をサポートする RADIUS サーバのユーザ プロファイルの例です。

```
mascot   Password = "password1"
         Service-Type = NAS-Prompt,
         Framed-Protocol = PPP,
         Cisco:Cisco-Enc = "ip:route=10.0.0.0 255.0.0.0"
         Cisco.attr Cisco-Enc 36 tag-encstr(*,*)
```

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*』
RADIUS 属性	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』
メディア独立型 PPP およびマルチリンク PPP	「メディア独立型 PPP およびマルチリンク PPP の設定」機能モジュール
認証	「認証の設定」機能モジュール
許可	「認可の設定」機能モジュール

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 2865	『*Remote Authentication Dial In User Service (RADIUS)*』
RFC 2868	『*RADIUS Attributes for Tunnel Protocol Support*』

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 Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

暗号化されたベンダー固有属性の機能情報

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 *12*：暗号化されたベンダー固有属性の機能情報

機能名	リリース	機能情報
暗号化されたベンダー固有属性	Cisco IOS XE Release 2.3	暗号化されたベンダー固有属性の機能により、ユーザは RADIUS サーバでフィルタを一元的に管理できます。また、この機能はタグ付き、暗号化、タグ付きおよび暗号化の各文字列ベンダー固有属性（VSA）をサポートしています。 Cisco IOS XE Release 2.3 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

第 7 章

アクセス要求内の RADIUS 属性 8 Framed-IP-Address

アクセス要求内の RADIUS 属性 8（Framed-IP-Address）機能は、ネットワーク アクセス サーバ（NAS）から RADIUS サーバに、ユーザ認証に先立って、ユーザ IP アドレスのヒントを提供できるようにします。RADIUS サーバ上で動作するアプリケーションは、このヒントを使用して、ユーザ名と アドレスのテーブル（マップ）を作成できます。マッピング情報を使用して、サービス アプリケーションは、正常なユーザ認証に使用するユーザのログイン情報の準備を開始できます。

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。

アクセス要求内の RADIUS 属性 8 Framed-IP-Address の前提条件

RADIUS アクセス要求内で RADIUS 属性 8 を送信する場合は、NAS サーバから IP アドレスを要求するようにログイン ホストを設定しておく必要があります。また、NAS からの IP アドレスを受け入れるようにログイン ホストを設定しておく必要もあります。

NASは、ログインホストをサポートしているインターフェイス上のネットワーク アドレスのプールを使用して設定する必要があります。

アクセス要求内の RADIUS 属性 8 Framed-IP-Address に関する情報

この機能の動作内容

ネットワーク デバイスが RADIUS 認証用に設定された NAS にダイヤルインすると、NAS がユーザ認証に備えて、RADIUS サーバとの通信プロセスを開始します。通常は、ユーザ認証が成功するまで、ダイヤルイン ホストの IP アドレスが RADIUS サーバに通知されません。RADIUS アクセス要求内でサーバにデバイス IP アドレスを通知すれば、他のアプリケーションがその情報を利用できるようになります。

NASがRADIUSサーバと通信するようにセットアップされている場合は、NASが特定のインターフェイス上で設定された IP アドレスのプールからダイヤルイン ホストに IP アドレスを割り当てます。NASは、ダイヤルインホストのIPアドレスを属性8としてRADIUSサーバに送信します。そのとき、NAS は、ユーザ名などの他のユーザ情報も RADIUS サーバに送信します。

RADIUS が NAS からユーザ情報を受信した場合は、次の 2 つの選択肢があります。

- RADIUS サーバ上のユーザ プロファイルにすでに属性 8 が含まれていた場合は、RADIUS が NAS から受け取った IP アドレスをユーザ プロファイル内で属性 8 として定義された IP アドレスに置き換えます。ユーザ プロファイル内で定義されたアドレスが NAS に返されます。
- ユーザプロファイルに属性8が含まれていない場合は、RADIUSサーバが、NASからの属性 8 を受け入れて、そのアドレスを NAS に返すことができます。

RADIUS サーバから返されたアドレスは、セッションが終わるまで、NAS 上のメモリに保存されます。NAS が RADIUS アカウンティング用に設定されている場合は、RADIUS サーバに送信されるアカウンティング開始パケットに属性 8 内のものと同じ IP アドレスが含まれています。以降のすべてのアカウンティング パケット、更新（設定されている場合）、および終了パケットにも、属性 8 で指定されたものと同じ IP アドレスが含まれています。

ただし、RADIUS 属性 8（Framed-IP-Address）は、次の 2 つの状況ではアカウンティング開始パケットに含まれません。

- ユーザがデュアルスタック（IPv4 または IPv6）サブスクライバである場合。
- IP アドレスがローカル プールからであり、RADIUS サーバからではない場合。

これらの状況では、**aaaaccountingdelay-startextended-time***delay-value* コマンドを使用し、設定した遅延値でインターネット プロトコル制御プロトコル バージョン 6（IPCPv6）アドレス ネゴシエーションを遅延させます。遅延している間は、IPCPv4 アドレスが使用され、フレーム化された IPv4 アドレスがアカウンティング開始パケットに追加されます。

利点

アクセス要求機能の RADIUS 属性 8（Framed-IP-Address）を使用すると、ユーザと IP アドレスのマッピング テーブルを構築する RADIUS サーバで、アプリケーションを実行することができます。この機能により、サーバは、RADIUS サーバでの正常なユーザ認証の前に、カスタマイズしたユーザ ログイン ページの準備といった他のアプリケーションで、マッピング テーブルの情報を使用することができます。

アクセス要求内の RADIUS 属性 8 Framed-IP-Address の設定方法

アクセス要求での RADIUS 属性 8 の設定

アクセス要求内で RADIUS 属性 8 を送信するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **radius-serverattribute8include-in-access-req**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**radius-serverattribute8include-in-access-req** 例： `Router(config)# radius-server attribute 8 include-in-access-req`	access-request パケット内で RADIUS 属性 8 を送信します。

アクセス要求内の RADIUS 属性 8 の確認

RADIUS 属性 8 がアクセス要求内で送信されていることを確認するには、次の手順を実行します。属性 8 は、すべての PPP アクセス要求内に存在するはずです。

手順の概要

1. イネーブル化
2. **moresystem:running-config**
3. **debugradius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**moresystem:running-config** 例： `Router# more system:running-config`	現在実行されているコンフィギュレーション ファイルの内容を表示します（**show running-config** コマンドが **more system:running-config** コマンドに置き換えられていることに注意してください）。

	コマンドまたはアクション	目的
ステップ 3	**debugradius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。このコマンドの出力は、属性 8 がアクセス要求内で送信されているかどうかを示しています。

アクセス要求内の RADIUS 属性 8 Framed-IP-Address の設定例

ダイヤルイン ホストの IP アドレスを送信する NAS の設定例

次の例は、ダイヤルイン ホストの IP アドレスを RADIUS アクセス要求内で RADIUS サーバに送信する NAS 設定を示しています。NAS は、RADIUS 認証、許可、アカウンティング（AAA）用に設定されています。IP アドレスのプール（async1-pool）が設定され、インターフェイス virtual-template1 に適用されています。

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
ip address-pool local
!
interface virtual-template1
 peer default ip address pool async1-pool
!
ip local pool async1-pool 209.165.200.225 209.165.200.229
!
radius-server host 172.31.71.146 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 8 include-in-access-req
radius-server key radhost<xxx>: Example
```

その他の参考資料

次の項で、アクセス要求内の RADIUS 属性 8（Framed-IP-Address）に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
認証の設定および RADIUS の設定	『*Cisco IOS XE Security Configuration Guide: Configuring User Services*, Release 2』の「認証の設定」および「RADIUS の設定」の章。
セキュリティ コマンド	『*Cisco IOS Security 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 IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、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 2138	『Remote Authentication Dial In User Service (RADIUS)』

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 Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

アクセス要求内の RADIUS 属性 8 Framed-IP-Address 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 *13*：アクセス要求内の *RADIUS* 属性 *8*（*Framed-IP-Address*）の機能情報

機能名	リリース	機能情報
アクセス要求内の RADIUS 属性 8（Framed-IP-Address） （スティッキー IP とも呼ばれます）	Cisco IOS XE Release 2.1	アクセス要求内の RADIUS 属性 8（Framed-IP-Address）機能は、ネットワーク アクセス サーバ（NAS）から RADIUS サーバに、ユーザ認証に先立って、ユーザ IP アドレスのヒントを提供できるようにします。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 **radius-server attribute 8 include-in-access-req** コマンドが導入または変更されました。

第 8 章

RADIUS 属性 82 トンネル割り当て ID

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。

RADIUS 属性 82 トンネル割り当て ID の前提条件

この機能を使用するには、VPDN をサポートするシスコ プラットフォームを使用している必要があります。

RADIUS 属性 82 トンネル割り当て ID の制約事項

この機能は、VPDN ダイヤルイン アプリケーション専用に設計されています。VPDN ダイヤルアウトはサポートしていません。

RADIUS 属性 82 トンネル割り当て ID に関する情報

RADIUS 属性 82：トンネル割り当て ID 機能を使用すれば、レイヤ 2 トランスポート プロトコル アクセス コンセントレータ（LAC）で複数のユーザ単位またはドメイン 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することができます。RADIUS 属性 82：トンネル割り当て ID 機能は、選択されたエンドポイント、トンネル タイプ、および Tunnel-Assignment-ID が同じ場合に、LAC で複数の RADIUS プロファイルからのユーザを同じトンネルにグループ分けできるようにする新しい avpair の Tunnel-Assignment-ID を定義します。この機能により、新しいソフトウェア機能が導入されました。この機能のために導入されたコマンドはありません。

RADIUS 属性 82 が LAC で使用されているかどうかの確認方法

RADIUS 属性 82：トンネル割り当て ID 機能に関する設定手順はありません。このタスクは、トンネル認可中に LAC で使用される RADIUS 属性 82 を確認します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. Router# **debug radius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	Router# **debug radius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。このコマンドの出力は、属性 82 がアクセス要求内で送信されているかどうかを示します。

RADIUS 属性 82 トンネル割り当て ID の設定例

LAC の設定例

次の例は、VPDN グループがルータで定義されている場合の LAC の設定を示しています。

```
aaa new-model
aaa authentication ppp default local
aaa authorization network default local
!
bba-group pppoe bba_group1
virtual-template 1
!
interface Loopback1
no ip address
vpdn-group VPDN_LAC1
request-dialin
protocol l2tp
local name tb162_LAC1
domain isp1.com
initiate-to ip 10.0.0.2
source-ip 10.0.0.1
l2tp tunnel receive-window 100
l2tp tunnel nosession-timeout 30
l2tp tunnel retransmit retries 5
l2tp tunnel retransmit timeout min 2
l2tp tunnel retransmit timeout max 8
l2tp tunnel hello 60
l2tp tunnel password tunnel1
!
!
interface virtual-template 1
no snmp trap link-status
no keepalive
ip unnumbered loopback1
ppp mtu adaptive
ppp authentication pap
no logging event link-status
!
```

次の例は、VPDN グループが RADIUS で定義されている場合の LAC の設定を示しています。

```
aaa authentication ppp default group radius
aaa authorization network default radius
!
bba-group pppoe bba_group1
virtual-template 1
!
interface Loopback1
no ip address
interface virtual-template 1
no snmp trap link-status
no keepalive
ip unnumbered loopback1
ppp mtu adaptive
ppp authentication pap
no logging event link-status
```

LNS の設定例

次の例は、LNS 上で VPDN を設定します。

```
hostname lns
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
vpdn enable
vpdn-group VPDN_LNS1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname tb162_LAC1
 local name LNS1
 l2tp tunnel hello 90
 l2tp tunnel password 0 hello1
interface Loopback0
 ip address 10.1.1.3 255.255.255.0
interface Virtual-Template1
 ip unnumbered Loopback0
 no keepalive
 peer default ip address pool mypool
 ppp authentication chap
ip local pool mypool 10.1.1.10 10.1.1.50
radius-server host lns-radiusd  auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
```

RADIUS の設定例

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@router.com Password = "cisco" Service-Type = Outbound,
       Tunnel-Type = :1:L2TP,
       Tunnel-Server-Endpoint = :1:"10.14.10.54",
       Tunnel-Assignment-Id = :1:"router"
client@router.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.router.com Password = "cisco" Service-Type = Outbound,
        Tunnel-Type = :1:L2TP,
        Tunnel-Server-Endpoint = :1:"10.14.10.54",
        Tunnel-Assignment-Id = :1:"router"
sales.router.com Password = "cisco" Service-Type = Outbound,
        Tunnel-Type = :1:L2TP,
        Tunnel-Server-Endpoint = :1:"10.14.10.54",
        Tunnel-Assignment-Id = :1:"router"
```

その他の参考資料

次の項で、RADIUS トンネル属性拡張に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
認証	「認証の設定」モジュール。
RADIUS 属性	「RADIUS 属性の概要および RADIUS IETF 属性」モジュール。
VPDN	『*Cisco IOS VPDN Configuration Guide*, Release 15.0』。

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 IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、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 2868	『RADIUS Attributes for Tunnel Protocol Support』

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 Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS 属性 82 トンネル割り当て ID 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 *14* : *RADIUS* 属性 *82* : トンネル割り当て *ID* の機能情報

機能名	リリース	機能情報
RADIUS 属性 82：トンネル割り当て ID	Cisco IOS XE Release 2.1	RADIUS 属性 82：トンネル割り当て ID 機能を使用すれば、レイヤ 2 トランスポート プロトコル アクセス コンセントレータ（LAC）で複数のユーザ単位またはドメイン 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することができます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータのサポートが追加されました。

第 9 章

RADIUS トンネル属性拡張

RADIUS トンネル属性拡張機能は、RADIUS 属性 90（Tunnel-Client-Auth-ID）と RADIUS 属性 91（Tunnel-Server-Auth-ID）を導入しています。この両方の属性は、ユーザにネットワーク アクセス サーバ（NAS）と RADIUS サーバの認証名の指定を許可することによって、バーチャル プライベート ネットワーク（VPN）での強制的トンネリングのプロビジョニングを支援します。

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。

前提条件

RADIUS 属性の 90 と 91 を使用するには、次のタスクを完了する必要があります。

- AAA をサポートするように NAS を設定する。
- RADIUS をサポートするように NAS を設定する。
- VPN をサポートするように NAS を設定する。

制約事項

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。

RADIUS トンネル属性拡張に関する情報

RADIUS トンネル属性拡張の利点

RADIUS トンネル属性拡張の機能により、トンネル イニシエータとトンネル ターミネータの名前が（デフォルト以外で）指定できます。これにより、VPN トンネリングのセットアップ時に、より高度なセキュリティを確立できます。

RADIUS トンネル属性拡張の説明

NAS と RADIUS サーバ間の通信がセットアップされたら、トンネリング プロトコルを有効にできます。トンネリング プロトコルのアプリケーションの一部は自発的ですが、その他は強制的トンネリングを伴います。つまり、ユーザが何らかの処置や選択をしなくてもトンネルが作成されます。このような場合は、NAS から RADIUS サーバにトンネリング情報を伝送して認証を確立するための新しい RADIUS 属性が必要です。この新しい RADIUS 属性を次の表に示します。

（注） 強制的トンネリングでは、配備中のセキュリティ対策がトンネル エンドポイント間のトラフィックにのみ適用されます。トンネル化されたトラフィックの暗号化または完全性保護をエンドツーエンド セキュリティの代替手段と見なさないでください。

表 *15* : *RADIUS* トンネル属性

番号	IETF RADIUS トンネル属性	同等の TACACS+ 属性	サポートされているプロトコル	説明
90	Tunnel-Client-Auth-ID	tunnel-id	レイヤ 2 トンネリングプロトコル（L2TP）	トンネルターミネータを使用してトンネルセットアップを認証する際に、トンネルイニシエータ（NAS とも呼ばれます[4]）によって使用される名前を指定します。
91	Tunnel-Server-Auth-ID	gw-name	レイヤ 2 トンネリングプロトコル（L2TP）	トンネルイニシエータを使用してトンネルセットアップを認証する際に、トンネルターミネータ（ホームゲートウェイとも呼ばれます[5]）によって使用される名前を指定します。

4 L2TP が使用される場合、NAS は L2TP アクセス コンセントレータ（LAC）とも呼ばれます。
5 L2TP が使用される場合、ホーム ゲートウェイは L2TP ネットワーク サーバ（LNS）とも呼ばれます。

RADIUS 属性 90 と RADIUS 属性 91 は次のような状況で追加されます。

- RADIUS サーバが要求を受け入れ、必要な認証名がデフォルトと異なる場合
- アカウンティング要求に値が start と stop のどちらかの Acct-Status-Type 属性が含まれ、トンネル化されたセッションが関係している場合

RADIUS トンネル属性拡張の設定方法

この機能に関連する設定作業はありません。

RADIUS 属性 90 および RADIUS 属性 91 の確認

RADIUS 属性 90 と RADIUS 属性 91 がアクセス受け入れとアカウンティング要求内で送信されていることを確認するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router#` **debug radius**	RADIUS 関連の情報を表示します。このコマンドの出力は、属性 90 と 属性 91 のどちらがアクセス受け入れとアカウンティング要求内で送信されているかを示します。

RADIUS トンネル属性拡張の設定例

L2TP ネットワーク サーバ設定の例

次の例は、RADIUS トンネリング属性の 90 と 91 を使用した基本的な L2F と L2TP の設定を含む LNS の設定方法を示しています。

```
aaa new-model
aaa authentication login default none
aaa authentication login console none
aaa authentication ppp default local group radius
aaa authorization network default group radius if-authenticated
!
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface loopback0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface Virtual-Template1
ip unnumbered loopback0
ppp authentication pap
!
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
radius-server key <deleted>
!
```

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

L2TP トンネル用の 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。

```
cisco.com Password = "cisco", Service-Type = Outbound
Service-Type = Outbound,
Tunnel-Type = :1:L2TP,
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:"l2tp-cli-auth-id",
Tunnel-Server-Auth-Id = :1:"l2tp-svr-auth-id",
Tunnel-Assignment-Id = :1:"l2tp-assignment-id",
Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
Tunnel-Preference = :1:1
```

その他の参考資料

次の項で、RADIUS トンネル属性拡張の機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
認証設定	『*Cisco IOS XE Security Configuration Guide: Configuring User Services*, Release 2』の「認証の設定」
RADIUS の設定	『*Cisco IOS XE Security Configuration Guide: Configuring User Services*, Release 2』の「RADIUS の設定」
RADIUS 属性の概要	『*Cisco IOS XE Security Configuration Guide: Configuring User Services*, Release 2』の「RADIUS 属性の概要および RADIUS IETF 属性」。
セキュリティ コマンド	『*Cisco IOS Security 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 IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、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 2868	『*RADIUS Attributes for Tunnel Protocol Support*』

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 Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS トンネル属性拡張の機能情報

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 *16*：*RADIUS* トンネル属性拡張の機能情報

機能名	リリース	機能情報
RADIUS トンネル属性拡張	Cisco IOS XE Release 2.1	RADIUS トンネル属性拡張機能は、RADIUS 属性 90（Tunnel-Client-Auth-ID）と RADIUS 属性 91（Tunnel-Server-Auth-ID）を導入しています。この両方の属性は、ユーザにネットワーク アクセス サーバ（NAS）と RADIUS サーバの認証名の指定を許可することによって、バーチャル プライベート ネットワーク（VPN）での強制的トンネリングのプロビジョニングを支援します。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

用語集

Layer2TunnelProtocol（L2TP）：ISP などのアクセス サービスで仮想トンネルを作成し、顧客のリモート サイトやリモート 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可能な Layer 2 Tunneling Protocol。具体的には、ISP アクセス ポイント（POP）にあるネットワーク アクセス サーバ（NAS）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

L2TPアクセスコンセントレータ（LAC）：クライアントが直接接続し、PPP フレームが L2TP ネットワーク サーバ（LNS）にトンネリングされるネットワーク アクセス サーバ（NAS）です。LAC は、L2TP が 1 つまたは複数の LNS にトラフィックを渡すために操作するメディアのみを実装します。LAC は PPP 内で伝送されるすべてのプロトコルをトンネルすることができます。また、LAC は着信コールを開始して、発信コールを受け取ります。LAC は L2F ネットワーク アクセス サーバに似ています。

L2TPネットワークサーバ（LNS）：L2TP トンネルの終端点であり、PPP フレームが処理され、上位層プロトコルに渡されるアクセス ポイント。LNS は PPP を終端させる任意のプラットフォーム上で動作できます。LNS はサーバ側の L2TP プロトコルを処理します。L2TP は、L2TP のトンネルが到達する 1 つのメディアにのみ依存します。LNS は発信コールを開始して、着信コールを受け取ります。LNS は L2F テクノロジーのホーム ゲートウェイに似ています。

ネットワークアクセスサーバ（NAS）：パケットの世界（インターネットなど）と回線交換の世界（PSTN など）をインターフェイスする、シスコ プラットフォームまたは AccessPath システムなどのプラットフォームの集合。

トンネル：L2TP アクセス コンセントレータ（LAC）と L2TP ネットワーク サーバ（LNS）間で複数の PPP セッションを伝送可能な仮想パイプ。

バーチャル プライベート ネットワーク（VPN）：リモートでダイヤルイン ネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシステム。VPN は、L2TP と L2F を使用して、L2TP アクセス コンセントレータ（LAC）の代わりに、L2TP ネットワーク サーバ（LNS）でネットワーク接続のレイヤ 2 と上位層を終端させます。

第 10 章

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張

RADIUS 属性 66（Tunnel-Client-Endpoint）拡張機能を使用すれば、ネットワーク アクセス サーバ（NAS）の IP アドレスではなく、NAS のホスト名を RADIUS 属性 66（Tunnel-Client-Endpoint）に指定できます。この機能は、ユーザが数字の IP アドレスよりも覚えやすいホスト名を使用できるようにするとともに、NAS の IP アドレス の隠ぺいを支援します。

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。

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張の前提条件

VPDN をサポートするシスコ プラットフォームが必要です。VPDN の詳細については、用語集,（119 ページ）を参照してください。

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張の制約事項

シスコデバイスでは、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）をサポートするシスコのソフトウェア イメージを実行する必要があります。

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張に関する情報

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張の使用方法

バーチャル プライベート ネットワーク（VPN）は、レイヤ 2 フォワーディング（L2F）または Layer 2 Tunnel Protocol（L2TP）トンネルを使用して、上位層プロトコルのリンク レイヤ（たとえば、PPP、非同期ハイレベル データ リンク コントロール（HDLC）など）をトンネルします。インターネット サービス プロバイダー（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 はトンネル サーバ（トンネル エンドポイント）に関する情報だけを保持します。顧客では、トンネル サーバ ユーザの IP アドレス、ルーティング、その他のユーザ データベース機能が保持されます。RADIUS 属性 66 は、顧客が NAS の IP アドレスの代わりにホスト名を指定できるようにします。

（注） L2F 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。

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張の設定方法

RADIUS 属性 66（Tunnel-Client-Endpoint）拡張のサポートに関連する設定作業はありません。

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張の設定例

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張用の RADIUS プロファイルの設定

次の例は、RADIUS プロファイルの RADIUS 属性 66 （Tunnel-Client-Endpoint）を使用して、ユーザが NAS のホスト名を指定できるようにするための設定方法を示しています。

```
cisco-avpair = vpdn:l2tp-cm-local-window-size=1024
cisco-avpair = vpdn:l2tp-nosession-timeout=30
cisco-avpair = vpdn:l2tp-cm-retransmit-retries=10
cisco-avpair = vpdn:l2tp-cm-min-timeout=2
cisco-avpair = vpdn:l2tp-hello-interval=60
Service-Type = outbound
Tunnel-Assignment-Id_tag1 = ISP1
Tunnel-Client-Auth-Id_tag1 = LAC1
Tunnel-Client-Endpoint_tag1 = 10.0.0.2
Tunnel-Medium-Type_tag1 = IPv4
Tunnel-Password_tag1 = tunnel1
Tunnel-Server-Auth-Id_tag1 = LNS1
Tunnel-Server-Endpoint_tag1 = 10.0.0.1
Tunnel-Type_tag1 = l2tp
```

その他の参考資料

次の項で、RADIUS 属性 66（Tunnel-Client-Endpoint）拡張の機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
RADIUS 属性 66	『*Cisco IOS XE Security Configuration Guide: Configuring User Services*, Release 2』
セキュリティ コマンド	『*Cisco IOS Security 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 IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、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
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

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 Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS 属性 66 Tunnel-Client-Endpoint 拡張の機能情報

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 *17*：*RADIUS* 属性 *66*（*Tunnel-Client-Endpoint*）拡張の機能情報

機能名	リリース	機能情報
RADIUS 属性 66（Tunnel-Client-Endpoint）拡張	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.9S	RADIUS 属性 66（Tunnel-Client-Endpoint）拡張機能を使用すれば、ネットワーク アクセス サーバ（NAS）の IP アドレスではなく、NAS のホスト名を RADIUS 属性 66（Tunnel-Client-Endpoint）に指定できます。この機能は、ユーザが数字の IP アドレスよりも覚えやすいホスト名を使用できるようにするとともに、NAS の IP アドレス の隠ぺいを支援します。 Cisco IOS XE Release 2.3 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

用語集

L2F：レイヤ 2 フォワーディング プロトコル。インターネットでの安全なバーチャル プライベート ダイヤルアップ ネットワークの作成をサポートするプロトコルです。

L2TP：Layer 2 Tunnel Protocol。ダイヤル アクセス領域におけるバーチャル プライベート ネットワークの主要な構成要素の 1 つであり、シスコおよびその他のインターネットワーキング業界のリーダーにより支持されているプロトコルです。このプロトコルは、シスコの L2F プロトコルと Microsoft 社のポイントツーポイント トンネリング プロトコル（PPTP）のいいところを組み合わせたものです。

レイヤ 2 フォワーディング プロトコル：L2F を参照。

Layer 2 Tunnel Protocol：L2TP を参照。

ポイントツーポイント プロトコル：PPP を参照。

PPP：ポイントツーポイント プロトコル。同期回線と非同期回線上でルータ間接続とホスト/ネットワーク間接続を提供する SLIP の代替プロトコル。SLIP は IP と連動するように設計されているのに対して、PPP は IP、IPX、ARA などの複数のネットワーク層プロトコルと連動するように設計されています。PPP には、CHAP および PAP などの組み込みのセキュリティ メカニズムもあります。PPP は LCP と NCP の 2 つのプロトコルに依存します。

RADIUS：Remote Authentication Dial-In User Service。モデムおよび ISDN 接続の認証、および接続のトラッキングのためのデータベースです。

Remote Authentication Dial-In User Service：RADIUS を参照。

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 を参照。

VPDN：バーチャル プライベート ダイヤルアップ ネットワーク。リモートでダイヤルイン ネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシステム。VPDN は、L2TP と L2F を使用して、L2TP アクセス コンセントレータ（LAC）ではなく、L2TP ネットワーク サーバ（LNS）で、レイヤ 2 と上位のネットワーク接続部分を終端します。

第 11 章

RADIUS 属性値スクリーニング

RADIUS 属性値スクリーニング機能を使用すれば、認可やアカウンティングなどの目的で、ネットワーク アクセス サーバ（NAS）上の「許可」または「拒否」RADIUS 属性のリストを設定できます。

NAS が Access-Accept パケットで受信したすべての RADIUS 属性を受け入れて処理する場合は、不必要な属性を処理する可能性があり、顧客の認証、認可、およびアカウンティング（AAA）サーバを制御しないホールセール プロバイダーの場合に問題が発生します。たとえば、顧客が加入していないサービスを指定する属性が存在したり、他のホールセール ダイヤル ユーザ向けのサービスを低下させる属性が存在したりする場合です。そのため、特定の属性の使用を制限するように NAS を設定できることが、多くのユーザの要件になります。

RADIUS 属性値スクリーニング機能を実装するには、次の方法のいずれかを使用する必要があります。

- NAS が、特定の目的で、設定された拒否リストに登録されたものを除く、すべての標準 RADIUS 属性を受け入れて、処理できるようにする
- NAS が、特定の目的で、設定された許可リストに登録されたものを除く、すべての標準 RADIUS 属性を拒否（除外）できるようにする

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。

RADIUS 属性値スクリーニングの前提条件

RADIUS の許可リストおよび拒否リストを設定する前に、AAA を有効にする必要があります。

RADIUS 属性値スクリーニングの制約事項

NAS の要件

この機能を有効にするには、RADIUS グループを使用して認可するように NAS を設定する必要があります。

許可リストまたは拒否リストの制約事項

許可リストまたは拒否リストの設定に使用される 2 つのフィルタは相互排他的です。そのため、ユーザはサーバ グループの目的ごとに、1 つのアクセス リストか、1 つの拒否リストしか設定できません。

ベンダー固有属性

この機能は、ベンダー固有属性（VSA）スクリーニングをサポートしていません。ただし、ユーザは、すべての VSA を許可または拒否する許可リストまたは拒否リスト内で属性 26（Vendor-Specific）を指定できます。

必須属性スクリーニングの推奨事項

次の必須属性は、拒否しないことを推奨します。

- 認可用：
  - 6（Service-Type）
  - 7（Framed-Protocol）

- アカウンティング用：
  - 4（NAS-IP-Address）
  - 40（Acct-Status-Type）
  - 41（Acct-Delay-Time）
  - 44（Acct-Session-ID）

属性が必須の場合は、拒否が無視され、属性のパススルーが許可されます。

（注） 必須属性の拒否リストを設定してもエラーにはなりません。これは、リストでは目的（認可またはアカウンティング）が指定されないためです。サーバが、属性の使用目的を認識したときに、その属性が必須かどうかを判断します。

RADIUS 属性値スクリーニングに関する情報

RADIUS 属性値スクリーニング機能は、次のようなメリットを提供します。

- ユーザは、NAS 上で特定の目的の属性を選択して許可リストまたは拒否リストを設定できるため、不必要な属性が受け入れられ、処理されることがなくなります。
- 関連するアカウンティング属性だけの許可リストを設定することによって、不必要なトラフィックを削減し、アカウンティングデータのカスタマイズを可能にすることができます。

RADIUS 属性のスクリーン方法

RADIUS 属性値スクリーニングの設定

RADIUS 属性の許可リストまたは拒否リストを認可またはアカウンティング用に設定するには、次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. Router(config)# **aaaauthenticationpppdefault**
4. Router(config)# **aaaauthorizationnetworkdefaultgroup***group-name*
5. Router(config)# **aaagroupserverradius***group-name*
6. Router(config-sg-radius)# **server***ip-address*
7. Router(config-sg-radius)# **authorization** [**accept** | **reject**] *listname*
8. Router(config-sg-radius)# **exit**
9. Router(config)# **radius-serverhost** {*hostname* | *ip-address*} [**key***string*
10. Router(config)# **radius-serverattributelist***listname*
11. Router(config-sg-radius)# **attribute***value1* [*value2* [*value3...*]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	Router(config)# **aaaauthenticationpppdefault** 例： **group** *group-name*	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	Router(config)# **aaaauthorizationnetworkdefaultgroup***group-name*	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。
ステップ 5	Router(config)# **aaagroupserverradius***group-name*	複数の RADIUS サーバ ホストを別々のリストと別々の方式にグループ分けします。
ステップ 6	Router(config-sg-radius)# **server***ip-address*	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。

	コマンドまたはアクション	目的
ステップ 7	Router(config-sg-radius)# **authorization** [**accept** | **reject**] *listname* 例： `and/or` 例： `Router(config-sg-radius)#` **accounting** [**accept** | **reject**] *listname*	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。 および/または アカウンティング要求内で RADIUS サーバに送信すべき属性用のフィルタを指定します。 （注） **accept** キーワードは、*listname* 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* 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	Router(config-sg-radius)# **exit**	server-group 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	Router(config)# **radius-serverhost** {*hostname* | *ip-address*} [**key***string*	RADIUS サーバ ホストを指定します。
ステップ 10	Router(config)# **radius-serverattributelist***listname*	**attribute** コマンドで定義された一連の属性に指定されたリスト名を定義します。 （注） *listname* はステップ 5 で定義した *listname* と同じにする必要があります。
ステップ 11	Router(config-sg-radius)# **attribute***value1* [*value2* [*value3...*]]	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。 （注） 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。

RADIUS 属性値スクリーニングの確認

許可リストまたは拒否リストを確認するには、特権 EXEC モードで次のコマンドのいずれかを使用します。

コマンド	目的
`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。
`Router#` **debug aaa authentication**	AAA 認証に関する情報を表示します。
`Router#` **show radius statistics**	アカウンティングパケットと認証パケットについての RADIUS 統計情報を示します。

RADIUS 属性値スクリーニングの設定例

認可許可の例

次の例は、属性 6（Service-Type）と属性 7（Framed-Protocol）用の許可リストの設定方法を示しています。他のすべての属性（VSA を含む）は RADIUS 認可に対して拒否されます。

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
authorization accept min-author
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list min-author
attribute 6-7
```

アカウンティング拒否の例

次の例は、属性 66（Tunnel-Client-Endpoint）と属性 67（Tunnel-Server-Endpoint）用の拒否リストの設定方法を示しています。他のすべての属性（VSA を含む）は RADIUS アカウンティングに対して受け入れられます。

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
accounting reject tnl-x-endpoint
!
radius-server host 10.1.1.1 key mykey1
```

```
radius-server attribute list tnl-x-endpoint
attribute 66-67
```

認可拒否とアカウンティング許可の例

次の例は、RADIUS 認可用の拒否リストと RADIUS アカウンティング用の許可リストの設定方法を示しています。認可またはアカウンティングのサーバ グループごとに複数の許可リストまたは拒否リストを設定できませんが、サーバ グループごとに認可用のリストとアカウンティング用のリストを 1 つずつ設定できます。

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
authorization reject bad-author
accounting accept usage-only
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list usage-only
attribute 1,40,42-43,46
!
radius-server attribute list bad-author
attribute 22,27-28,56-59
```

必須属性の拒否の例

次の例は、**debug aaa accounting** コマンドのデバッグ出力を示しています。この例では、必須属性の 44、40、および 41 が拒否リストの「standard」に追加されています。

```
Router# debug aaa authorization
AAA/ACCT(6): Accounting method=radius-sg (radius)
RADIUS: attribute 44 cannot be rejected
RADIUS: attribute 61 rejected
RADIUS: attribute 31 rejected
RADIUS: attribute 40 cannot be rejected
RADIUS: attribute 41 cannot be rejected
```

その他の参考資料

次の項で、RADIUS 属性値スクリーニング機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
RADIUS	「RADIUS の設定」機能モジュール。
その他のセキュリティ機能	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』
セキュリティ コマンド	『*Cisco IOS Security 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
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
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

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 Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

RADIUS 属性値スクリーニングの機能情報

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 *18* : *RADIUS* 属性値スクリーニングの機能情報

機能名	リリース	機能情報
RADIUS 属性値スクリーニング	Cisco IOS XE Release 2.1	RADIUS 属性値スクリーニング機能を使用すれば、認可やアカウンティングなどの目的で、ネットワーク アクセス サーバ（NAS）上の「許可」または「拒否」RADIUS 属性のリストを設定できます。 この機能は、Cisco IOS XE リリース 2.1 で Cisco ASR 1000 シリーズ アグリゲーション サービスルータに導入されました。 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。**accounting**（**server-group**）、**authorization**（**server-group**）、**attribute**（**server-group**）、**radius-serverattributelist**

第 12 章

RADIUS 属性 55 Event-Timestamp

RADIUS 属性 55 Event-Timestamp 機能により、ネットワーク アクセス サーバ（NAS）は、Network Time Protocol（NTP）同期が行われているまたは行われていない RADIUS サーバに送信されるアカウンティングおよび認証パケットに、イベント タイムスタンプ属性を挿入できます。

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。

RADIUS 属性 55 Event-Timestamp の前提条件

アカウンティングおよび認証要求パケット内でEvent-Timestamp属性を送信するには、ネットワークデバイスのクロックを設定する必要があります。ネットワークデバイスのクロックの設定方法については、ネットワーク管理の設定ガイドの「基本システム管理」の章の「基本システム管理の実行」を参照してください。

ネットワークデバイスがリロードされるたびにネットワークデバイスのクロックを設定するのを避けるには、**clockcalendar-valid** コマンドを有効にします。このコマンドの詳細については、ネットワーク管理の設定ガイドの「基本システム管理」の章の「時刻およびカレンダー サービスの設定」を参照してください。

RADIUS 属性 55 Event-Timestamp に関する情報

ネットワーク デバイスが RADIUS 認証用に設定されたネットワーク アクセス サーバ（NAS）にダイヤルインすると、NAS がユーザ認証に備えて、RADIUS サーバとの通信プロセスを開始します。通常、RADIUS 属性 55（Event-Timestamp）は、Network Time Protocol（NTP）の同期が正常に完了するまで、RADIUS サーバに送信されません。この機能により、NTP が同期していない場合でも、NAS はアカウンティングおよび認証要求パケットに Event-Timestamp 属性を挿入できます。

Event-Timestamp 属性は、NAS で発生したイベントの発生時刻を記録します。このタイムスタンプは RADIUS 属性 55 内で、1970 年 1 月 1 日 00:00 UTC 以降の秒数で送信されます。

Event-Timestamp 属性は、セッションが終わるまで NAS 上のメモリに保存されます。RADIUS アカウンティングおよび認証開始パケットと、それに続くすべてのアカウンティングおよび認証パケット、更新（設定されている場合）、停止パケットもまた、最初のパケットが送信された時刻を表す同じ RADIUS 属性 55 Event-Timestamp を含んでいます。

RADIUS 属性 55 Event-Timestamp の設定方法

RADIUS 属性 55 Event-Timestamp の設定

アカウンティングおよび認証要求内でRADIUS属性55を送信するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **aaanew-model**
4. **aaaauthenticationpppdefaultgroupradius**
5. **aaaaccountingnetworkdefaultstart-stopgroupradius**
6. **radius-serverhost***ip-address*
7. **radius-serverattribute55include-in-acct-req**
8. **radius-serverattribute55access-reqinclude**
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	イネーブル化 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	**aaanew-model** 例： `Device(config)# aaa new-model`	認証、許可、アカウンティング（AAA）をイネーブルにします。
ステップ 4	**aaaauthenticationpppdefaultgroupradius** 例： `Device(config)# aaa authentication ppp default group radius`	認証用のすべてのRADIUSサーバのリストを利用して PPP を実行するシリアル インターフェイスで使用する、1つ以上のAAA方式を指定します。
ステップ 5	**aaaaccountingnetworkdefaultstart-stopgroupradius** 例： `Device(config)# aaa accounting network default start-stop group radius`	ネットワーク アカウンティングを有効にして、RADIUSアカウンティングの方式リスト用の開始アカウンティングおよび停止アカウンティングの通知を RADIUS サーバに送信します。

	コマンドまたはアクション	目的
ステップ 6	**radius-serverhost***ip-address* 例： `Device(config)# radius-server host 192.0.2.3`	RADIUS サーバ ホストの IP アドレスを指定します。
ステップ 7	**radius-serverattribute55include-in-acct-req** 例： `Device(config)# radius-server attribute 55 include-in-acct-req`	account-request パケット内で RADIUS 属性 55 を送信します。
ステップ 8	**radius-serverattribute55access-reqinclude** 例： `Device(config)# radius-server attribute 55 access-req include`	access-request パケット内で RADIUS 属性 55 を送信します。
ステップ 9	**exit** 例： `Device(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。

RADIUS 属性 55 Event-Timestamp の確認

アカウンティングおよび認証パケット内で RADIUS 属性 55 が送信され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. イネーブル化
2. **showrunning-config**
3. **debugradius**

手順の詳細

ステップ 1　イネーブル化

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）。

例：

```
Device> enable
```

ステップ 2 **showrunning-config**

現在実行されているコンフィギュレーション ファイルの内容を表示します

例：

```
Device# show running-config

.
.
.
aaa group server radius sample
aaa accounting network default start-stop group radius group sample
aaa server radius dynamic-author
radius-server attribute 55 include-in-acct-req
radius-server attribute 55 access-request include
radius-server dead-criteria time 10 tries 3
radius-server host 192.0.2.3
radius-server retry method reorder
radius-server retransmit 2
radius-server deadtime 1
radius-server key rad123
radius server host
.
.
.
radius-server attribute 55 include-in-acct-req
radius-server attribute 55 access-request include
```

ステップ 3 **debugradius**

RADIUS 関連の情報を表示します。このコマンドの出力は、アカウンティングおよび認証要求で属性 55 が送信されているかどうかを示しています。

例：

```
Device# debug radius

AAA/BIND(0000000D): Bind i/f Virtual-Template1
AAA/AUTHEN/PPP (0000000D): Pick method list 'default'
RADIUS/ENCODE(0000000D):Orig. component type = PPPoE
RADIUS: DSL line rate attributes successfully added
RADIUS(0000000D): Config NAS IP: 0.0.0.0
RADIUS(0000000D): Config NAS IPv6: ::
RADIUS/ENCODE(0000000D): acct_session_id: 2
RADIUS(0000000D): sending
RADIUS/ENCODE: Best Local IP-Address 192.0.2.3 for Radius-Server 192.0.2.1
RADIUS(0000000D): Sending a IPv4 Radius Packet
RADIUS(0000000D): Send Access-Request to 192.0.2.1:1645 id 1645/1,len 130
RADIUS:  authenticator 66 D8 24 42 BC 45 5B 3D - 0E DC 74 D7 E9 3D 81 85
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  User-Name           [1]   6   "test"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
RADIUS:  Vendor, Cisco       [26]  41
RADIUS:   Cisco AVpair       [1]   35  "client-mac-address=aabb.cc00.6500"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
```

```
RADIUS:  NAS-IP-Address      [4]   6   1.1.1.2
RADIUS:  Event-Timestamp     [55]  6   1362041578
RADIUS(0000000D): Started 5 sec timeout
RADIUS: Received from id 1645/192.0.2.1:1645, Access-Accept, len 20
.
.
.
RADIUS:  authenticator 2A 2B 24 47 06 44 23 8A - CB CC 8C 96 8D 21 76 DD
RADIUS(0000000D): Received from id 1645/1
AAA/BIND(0000000D): Bind i/f Virtual-Access2.1
RADIUS/ENCODE(0000000D):Orig. component type = PPPoE
.
.
.
RADIUS(0000000D): Config NAS IP: 0.0.0.0
RADIUS(0000000D): Config NAS IPv6: ::
RADIUS(0000000D): sending
RADIUS/ENCODE: Best Local IP-Address 192.0.2.3 for Radius-Server 192.0.2.1
RADIUS(0000000D): Sending a IPv4 Radius Packet
RADIUS(0000000D): Send Accounting-Request to 192.0.2.1:1646 id 1646/1,len 182
RADIUS:  authenticator C6 81 D0 D7 EA BA 9A A9 - 19 4B 1B 90 B8 D1 66 BF
RADIUS:  Acct-Session-Id     [44]  10  "00000002"
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  User-Name           [1]   6   "test"
RADIUS:  Vendor, Cisco       [26]  32
RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
RADIUS:  Acct-Authentic      [45]  6   RADIUS                    [1]
RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
RADIUS:  Vendor, Cisco       [26]  41
RADIUS:   Cisco AVpair       [1]   35  "client-mac-address=aabb.cc00.6500"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   1.1.1.2
RADIUS:  home-hl-prefix      [151] 10  "163BD6D4"
RADIUS:  Event-Timestamp     [55]  6   1362041588
RADIUS:  Acct-Delay-Time     [41]  6   0
RADIUS(0000000D): Started 5 sec timeout
.
.
.
RADIUS: Received from id 1646/1 1.1.1.1:1646, Accounting-response, len 20
RADIUS:  authenticator 79 F1 6A 38 07 C3 C8 F9 - 96 66 BE EF 5C FA 91 E6
```

RADIUS 属性 55 Event-Timestamp の設定例

例：アカウンティングおよび認証パケットの RADIUS 属性 55

次の例は、アカウンティングおよび認証パケットで RADIUS 属性 55 を送信する設定を示しています。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication ppp default group radius
Device(config)# aaa accounting network default start-stop group radius
Device(config)# radius-server host 192.0.2.3
Device(config)# radius-server attribute 55 include-in-acct-req
```

```
Device(config)# radius-server attribute 55 access-req include
Device(config)# exit
```

RADIUS 属性 55 Event-Timestamp に関するその他の参考資料

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』
セキュリティ コマンド	• Security Command Reference: Commands A to C』 • Security Command Reference: Commands D to L』 • Security Command Reference: Commands M to R』 • Security Command Reference: Commands S to Z』
「Configuring Authentication」	『*Authentication, Authorization, and Accounting Configuration Guide*』の「認証の設定」の章
RADIUS の設定	『*RADIUS Configuration Guide*』の「RADIUS の設定」の章

標準および RFC

標準/RFC	タイトル
RFC 2138	『*Remote Authentication Dial In User Service (RADIUS)*』

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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

RADIUS 属性 55 Event-Timestamp 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 *19*：***RADIUS*** 属性 ***55 Event-Timestamp*** の機能情報

機能名	リリース	機能情報
RADIUS 属性 55 Event-Timestamp	Cisco IOS XE Release 3.9S	RADIUS 属性 55 Event-Timestamp 機能により、ネットワーク アクセス サーバ（NAS）は、Network Time Protocol（NTP）同期が行われているまたは行われていない RADIUS サーバに送信されるアカウンティングおよび認証パケットに、イベント タイムスタンプ属性が挿入できます。 次のコマンドが導入または変更されました。**radius-server attribute 55 access-req include** および **radius-server attribute 55 include-in-acct-req**。

第 13 章

RADIUS 属性 104

RADIUS 属性 104 機能を使用すれば、RADIUS 認可プロファイル内でプライベート ルート（属性 104）を指定できます。プライベート ルートは、個々のインターフェイス上で受信されたパケットにのみ影響します。ルートはグローバル ルーティング テーブルとは別に保存され、ルーティング プロトコルに埋め込まれて再配布されることはありません。

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。

RADIUS 属性 104 の前提条件

- シスコ RADIUS サーバを使用している必要があります。
- RADIUS の設定に精通している必要があります。
- ポリシーベース ルーティング（PBR）とプライベート ルートに精通している必要があります。
- アクセス コントロール リスト（ACL）に精通している必要があります。
- RADIUS 属性 104 機能を使用する前に、RADIUS AAA 認可と RADIUS ルート ダウンロードを設定する必要があります。
- F:\tips-migration には以下のメモリ バイトが必要です。
  - 1 つのルート マップ：50 バイト
  - 1 つの match-set 句：600 バイト
  - 1 つの拡張 ACL：366 バイト
  - 属性 104 の数 N のメモリ要件は、ユーザ当たり (600+366)*N+50 □1000*N です。

RADIUS 属性 104 の制約事項

- インターフェイス上ですでに PBR がローカル（静的）に設定されている状態で、属性 104 を指定した場合は、ローカルに設定された PBR が無効になります。
- 疑似ネクストホップ アドレスを使用する場合は、ネクストホップ アドレスのルーティング テーブル内に、使用可能なルートが存在する必要があります。どのルートも使用できない場合は、パケットがポリシー ルーティングされません。
- ポリシー ルーティングは match-set 句を順序付けせず、最初の一致を優先するため、一致させたい順序で属性を指定する必要があります。
- メトリック番号は属性内で使用できません。

RADIUS 属性 104 に関する情報

ポリシーベース ルーティングの背景

PBR は、定義済みのポリシーに基づいて、データ パケットを転送またはルーティングするためのメカニズムを提供します。ポリシーは、宛先アドレスではなく、サービス タイプ、送信元アドレス、優先順位、ポート番号、プロトコル タイプなどの他の要因に依存します。

ポリシーベースルーティングは着信パケットに適用されます。ポリシーベースルーティングが有効になっているインターフェイス上で受信されたパケットはすべて、ポリシーベース ルーティングと見なされます。ルータは、ルートマップと呼ばれる拡張パケットフィルタにそれらのパケットを通過させます。ルート マップ内で定義された基準に基づいて、パケットが適切なネクストホップに転送されます。

ルート マップ文のエントリごとに、match 句と set 句の組み合わせまたはコマンドが 1 つずつ含まれています。match 句は、該当するパケットが特定のポリシーを満たしているかどうか（つまり、条件が満たされているかどうか）に関する基準を定義します。set 句は、一致基準を満たしたパケットをどのようにルーティングするかに関する指示を提供します。match 句は、対応する set 句を適用するためにパケットが一致しなければならないフィルタのセットを指定します。

属性 104 とポリシーベース ルート マップ

この項では、属性 104 機能と、そのポリシーベース ルート マップとの連携について説明します。

RADIUS 属性 104 の概要

RADIUS 属性 104 機能を使用すれば、RADIUS 認可プロファイル内でプライベート ルートを指定できます。指定したプライベート ルートは、個々のインターフェイス上で受信されたパケットにのみ影響します。ルートはグローバル ルーティング テーブルとは別に保存され、ルーティング プロトコルに埋め込まれて再配布されることはありません。

許可ルート マップ

ルートマップ ステートメントは、「許可」または「拒否」にマークすることができます。ステートメントが「許可」にマークされると、一致基準を満たすパケットに set 句が適用されます。属性 104 の場合は、ルート マップの設定中に、次のようにルート マップを「許可」としてマークする必要があります。ルートマップの設定に関する情報については、関連資料, （147ページ）を参照してください。

デフォルト プライベート ルート

ポリシー ルーティング プロセスは、一致するものが見つかるまで、ルート マップに沿って進行します。ルート マップ内で一致するものが見つからなかった場合は、グローバル ルーティング テーブルが参照されます。ユーザ プロファイル内でデフォルト ルートを指定した場合は、事実上、デフォルト ルートを越えるルートが無視されます。

ルート マップの順序

ルート マップはサーバ上で適用したい順番に指定する必要があります。

RADIUS 属性 104 の適用方法

RADIUS 属性 104 のユーザ プロファイルへの適用

次の内容を RADIUS サーバ データベースに追加することによって、RADIUS 属性 104 をユーザ プロファイルに適用できます。

手順の概要

1. RADIUS 属性 104 をユーザ プロファイルに適用します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	RADIUS 属性 104 をユーザ プロファイルに適用します。	`Ascend-Private-Route="dest_addr/netmask next_hop"` ルータの宛先ネットワーク アドレスは「dest_addr/netmask」で、ネクストホップ ルータのアドレスは「next_hop」です。

例

発信者に関連付けられた 3 つのプライベート ルートを作成するユーザ プロファイルのサンプルを次に示します。

```
username Password="ascend"; User-Service=Framed-User
   Framed-Protocol=PPP,
   Framed-Address=10.1.1.1,
   Framed-Netmask=255.0.0.0,
   Ascend-Private-Route="172.16.1.1/16 10.10.10.1"
   Ascend-Private-Route="192.168.1.1/32 10.10.10.2"
   Ascend-Private-Route="10.20.0.0/1 10.10.10.3"
   Ascend-Private-Route="10.0.0.0/0 10.10.10.4"
```

上のプロファイルを使用すれば、接続用のプライベート ルーティング テーブルに、デフォルト ルートのほかに次のルートが追加されます。

```
Destination/Mask     Gateway
172.16.1.1/16         10.10.10.1
192.168.1.1/32         10.10.10.2
10.20.20.20/1       10.10.10.3
10.0.0.0/0            10.10.10.4
```

ルート マップの確認

次の **show** コマンドを使用して、設定済みのルート マップを確認します。

手順の概要

1. イネーブル化
2. **showippolicy**
3. **showroute-map**[*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**showippolicy** 例： `Router# show ip policy`	ポリシー ルーティングに使用されるルート マップを表示します。
ステップ 3	**showroute-map**[*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**] 例： `Router# show route-map`	設定済みのすべてのルート マップを表示するか、指定した 1 つのルート マップだけを表示します。

RADIUS プロファイルのトラブルシューティング

プライベート ルート設定が正常に動作しない場合は、「ポリシーベース ルーティングの背景, （142ページ）」セクションを再度読んでみてください。このセクションは、パケットに何が発生しているかを判定するのに役立つことがあります。また、RADIUS プロファイルのトラブルシュートには、次の **debug** コマンドが使用できます。

手順の概要

1. イネーブル化
2. **debugradius**
3. **debugaaaper-user**
4. debug ip policy

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**debugradius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。
ステップ 3	**debugaaaper-user** 例： `Router# debug aaa per-user`	ユーザ認証として各ユーザに適用される属性を表示します。
ステップ 4	debug ip policy 例： `Router# debug ip policy`	IP ルーティング パケットのアクティビティを表示します。

RADIUS 属性 104 の設定例

属性 104 が適用された Route-Map 設定の例

次の出力は、属性 104 が適用された一般的な route-map 設定です。

```
Router# show route-map dynamic
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 0, identifier 1639994476
  Match clauses:
    ip address (access-lists): PBR#1 PBR#2
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 1, identifier 1640264784
  Match clauses:
    ip address (access-lists): PBR#3 PBR#4
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 2, identifier 1645563704
  Match clauses:
    ip address (access-lists): PBR#5 PBR#6
    length 10 100
  Set clauses:
```

```
    ip next-hop 10.1.1.1
    ip gateway10.1.1.1
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```

その他の参考資料

次の項で、RADIUS NAS-IP-Address 属性設定可能性に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
AAA の設定	『*Cisco IOS Security Configuration Guide: Securing User Services*』の「認証、認可、およびアカウンティング（AAA）」の項
RADIUS の設定	「RADIUS の設定」モジュール
RADIUS コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	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 IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、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
なし	--

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 Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS 属性 104 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 *20* : *RADIUS* 属性 *104* の機能情報

機能名	リリース	機能情報
RADIUS 属性 104	Cisco IOS XE Release 3.9S	RADIUS 属性 104 機能を使用すれば、RADIUS 認可プロファイル内でプライベートルート（属性 104）を指定できます。プライベート ルートは、個々のインターフェイス上で受信されたパケットにのみ影響します。ルートはグローバル ルーティング テーブルとは別に保存され、ルーティング プロトコルに埋め込まれて再配布されることはありません。 **showippolicy**、**showroute-map** コマンドが導入または変更されました。

第 14 章

RADIUS NAS-IP-Address 属性設定可能性

RADIUS NAS-IP-Address 属性設定可能性機能を使用すれば、RADIUS パケットの IP ヘッダー内の発信元 IP アドレスを変更せずに、任意の IP アドレスを設定して RADIUS 属性 4（NAS-IP-Address）として使用できます。この機能は、サービス プロバイダーが、スケーラビリティを向上させるために、小規模なネットワーク アクセス サーバ（NAS）のクラスタを使用して大規模な NAS をシミュレートしている場合にも使用できます。この機能を使用すれば、NAS を RADIUS サーバから見て、単一の RADIUS クライアントとして機能させることができます。

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。

RADIUS NAS-IP-Address 属性設定可能性の前提条件

この機能を設定する前に、次の要件を満たす必要があります。

- IP セキュリティ（IPSec）の使用経験と、RADIUS サーバと認証、許可、アカウンティング（AAA）の両方の設定経験が必要です。
- RADIUS サーバと AAA リストを設定する必要があります。

RADIUS NAS-IP-Address 属性設定可能性の制約事項

スケーラビリティを向上させるために、RADIUS クライアントのクラスタを単一の RADIUS クライアントのシミュレーションに使用している場合に、次の制約事項が適用されます。制約事項に対する解決策または次善策についても説明します。

- RADIUS 属性 44（Acct-Session-Id）は、複数の NAS からのセッション間で重複する可能性があります。

2 つの解決策があります。NAS ルータ上で **radius-server attribute 44 extend-with-addr** コマンドと **radius-server unique-ident** コマンドのどちらかを使用して、NAS ルータごとに異なる先頭の番号を指定できます。

- RADIUS サーバベースの IP アドレス プールを NAS ごとに管理する必要があります。

この解決策は、RADIUS サーバ上で NAS ごとに異なる IP アドレス プール プロファイルを設定することです。NAS ごとに異なるプール ユーザ名を使用してそれらを取得します。

- セッション内の RADIUS 要求メッセージは NAS ごとに識別される必要があります。

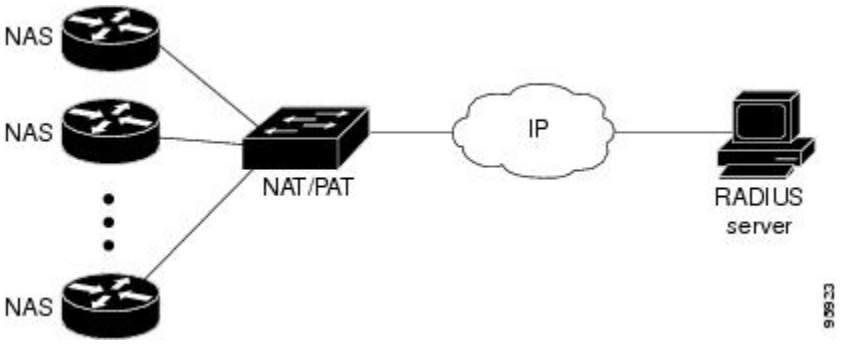
この解決策の 1 つは、NAS 上で **radius-server attribute 32 include-in-access-req** コマンドを使用して、NAS ごとに異なる RADIUS 属性 32（NAS-Identifier）用の形式文字列を設定することです。

RADIUS NAS-IP-Address 属性設定可能性に関する情報

RADIUS NAS-IP-Address 属性設定可能性に関する情報 に示すように、小規模な NAS RADIUS クライアントを使用して大規模な NAS RADIUS クライアントをシミュレートする場合は、ネットワーク アドレス変換（NAT）デバイスまたはポート アドレス変換（PAT）デバイスがネットワークに挿入されます。このデバイスは、NAS のクライアントと、RADIUS サーバに接続された IP クラウドの間に配置されます。複数の NAS からの RADIUS トラフィックが NAT または PAT デバイスを通過するときに、RADIUS パケットの発信元 IP アドレスが単一の IP アドレスに変換されます。ほとんどの場合、この IP アドレスは、NAT または PAT デバイスのループバック インターフェイス上の IP アドレスです。NAS ごとに異なるユーザ データグラム プロトコル（UDP）発信元プールが RADIUS パケットに割り当てられます。サーバから RADIUS 応答が返されると、NAT

または PAT デバイスがそれを受信して、宛先 UDP ポートを使用して宛先 IP アドレスを NAS の IP アドレスに変換し、対応する NAS に転送します。

次の図は、複数の NAS の送信元 IP アドレスが、IP クラウドへの途中で NAT または PAT デバイスを通過するときに、どのように単一の IP アドレスに変換されるかを示しています。



通常は、RADIUS サーバが RADIUS パケットの IP ヘッダー内の発信元 IP アドレスをチェックして、RADIUS 要求の発信元を追跡し、セキュリティを確保します。NAT または PAT による解決策は、RADIUS パケットが複数の NAS ルータから送られてきても単一の発信元 IP アドレスが使用されるため、これらの要件を満たします。

ただし、RADIUS データベースからアカウンティング レコードを取得するときに、課金システムによっては、アカウンティング レコード内で RADIUS 属性 4（NAS-IP-Address）が使用される場合があります。この属性の値は、独自の IP アドレスとして NAS ルータ上に記録されます。NAS ルータは、RADIUS サーバとの間で動作している NAT または PAT を認識しません。そのため、NAS ルータごとに異なる RADIUS 属性 4 アドレスがユーザのアカウンティング レコードに記録されます。最終的に、これらのアドレスは、複数の NAS ルータを RADIUS サーバと対応する課金システムに公開することになります。

RADIUS NAS-IP-Address 属性設定可能性機能の使用方法

RADIUS NAS-IP-Address 属性設定可能性機能を使用すれば、任意の IP アドレスを RADIUS NAS-IP-Address（RADIUS 属性 4）として設定できます。すべてのルータに対して同じ IP アドレス（ほとんどの場合、NAT または PAT デバイスのループバック インターフェイス上の IP アドレス）を手動で設定することによって、NAS ルータのクラスタを NAT または PAT デバイスの後ろに隠して、RADIUS から見えないようにすることができます。

RADIUS NAS-IP-Address 属性設定可能性の設定方法

RADIUS NAS-IP-Address 属性設定可能性の設定

RADIUS NAS-IP-Address 属性設定可能性機能を設定する前に、RADIUS サーバまたはサーバ グループと AAA 方式リストを設定しておく必要があります。

RADIUS NAS-IP-Address 属性設定可能性機能を設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **radius-serverattribute4***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	イネーブル化 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-serverattribute4***ip-address* 例： `Router (config)# radius-server attribute 4 10.2.1.1`	RADIUS NAS-IP-Address（属性 4）として使用する IP アドレスを設定します。

RADIUSNAS-IP-Address属性設定可能性のモニタリングとメンテナンス

RADIUS パケット内で使用されている RADIUS 属性 4 アドレスをモニタするには、**debugradius** コマンドを使用します。

手順の概要

1. イネーブル化
2. **debugradius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**debugradius** 例： `Router# debug radius`	RADIUS 関連の情報を表示します。

例

次のサンプル出力は、**debugradius** コマンドの出力です。

```
Router# debug radius
RADIUS/ENCODE(0000001C): acct_session_id: 29
RADIUS(0000001C): sending
RADIUS(0000001C): Send Access-Request to 10.0.0.10:1645 id 21645/17, len 81
RADIUS:  authenticator D0 27 34 C0 F0 C4 1C 1B - 3C 47 08 A2 7E E1 63 2F
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  User-Name           [1]   18  "shashi@pepsi.com"
RADIUS:  CHAP-Password       [3]   19  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.0.0.21
UDP: sent src=10.1.1.1(21645), dst=10.0.0.10(1645), length=109
UDP: rcvd src=10.0.0.10(1645), dst=10.1.1.1(21645), length=40
RADIUS: Received from id 21645/17 10.0.0.10:1645, Access-Accept, len 32
RADIUS:  authenticator C6 99 EC 1A 47 0A 5F F2 - B8 30 4A 4C FF 4B 1D F0
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS(0000001C): Received from id 21645/17
```

RADIUS NAS-IP-Address 属性設定可能性の設定例

RADIUS NAS-IP-Address 属性設定可能性の設定例

次の例は、IP アドレス 10.0.0.21 が RADIUS NAS-IP-Address 属性として設定されていることを示しています。

```
radius-server attribute 4 10.0.0.21
radius-server host 10.0.0.10 auth-port 1645 acct-port 1646 key cisco
```

その他の参考資料

次の項で、RADIUS NAS-IP-Address 属性設定可能性に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
AAA の設定	『*Cisco IOS Security Configuration Guide: Securing User Services*』の「認証、認可、およびアカウンティング（AAA）」の項
RADIUS の設定	「RADIUS の設定」モジュール
RADIUS コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	--

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。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、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
この機能でサポートが追加または変更された RFC はありません。	--

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 Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS NAS-IP-Address 属性設定可能性の機能情報

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 *21*：***RADIUS NAS-IP-Address*** 属性設定可能性の機能情報

機能名	リリース	機能情報
RADIUS NAS-IP-Address 属性設定可能性	Cisco IOS XE Release 3.9S	この機能を使用すれば、RADIUS パケットの IP ヘッダー内の発信元 IP アドレスを変更せずに、任意の IP アドレスを設定して RADIUS 属性 4（NAS-IP-Address）として使用できます。 **radius-serverattribute4** コマンドがこの機能で導入されました。

第 15 章

サーバ単位グループ レベルで指定された RADIUS 属性 5 NAS-Port フォーマット

サーバ単位グループ レベルで指定された RADIUS 属性 5（NAS-Port）フォーマット機能を使用すれば、RADIUS サーバ グループごとに設定をカスタマイズできます。この柔軟性によって、グローバル フォーマットの代わりに、カスタマイズされたネットワーク アクセス サーバ（NAS）ポート フォーマットを使用できます。

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。

サーバ単位グループ レベルで指定された RADIUS 属性 5 NAS-Port フォーマットの前提条件

- 認証、認可、およびアカウンティング（AAA）コンポーネントを含む Cisco IOS イメージを実行する必要があります。

サーバ単位グループ レベルで指定された RADIUS 属性 5 NAS-Port フォーマットに関する情報

RADIUS 属性 5 フォーマットのカスタマイズ

Cisco IOS リリース 12.3(14)T よりも前の Cisco IOS ソフトウェアでは、アクセス要求またはアカウンティング要求で送信された RADIUS 属性をグローバルにカスタマイズすることが可能でした。設定可能な各属性では、RADIUS サーバとの通信時の動作がカスタマイズできました。サーバ グループの実装により、グローバル属性設定の柔軟性が制限され、ルータと相互に通信する可能性のあるさまざまな RADIUS サーバをサポートするのに必要な、種々のカスタマイズに対処できなくなりました。たとえば、**global radius-server attribute nas-port format command** オプションを設定すると、RADIUS サーバと相互に通信するルータのすべてのサービスが同じ設定で使用されていました。

Cisco IOS リリース 12.3(14)T では、ルータを設定して、サーバ単位のグループを柔軟に上書きできるようになりました。RADIUS サーバ上のさまざまなサービス タイプに固有の名前付け方式を使用するようサービスを設定できます。サービスタイプは、独自のサービス グループを使用するように設定できます。この柔軟性により、NAS-port フォーマットをカスタマイズして、グローバル フォーマットの代わりに使用できるようになりました。

サーバ単位グループ レベルで指定された RADIUS 属性 5 NAS-Port フォーマットの設定方法

サーバ単位グループ レベルの RADIUS 属性 5 フォーマットの設定

サーバ単位グループ レベルの RADIUS 属性 5 フォーマットをサポートするようにルータを設定するには、次の手順を実行します。

（注） サーバ単位グループの機能を使用するには、名前付け方式リストをサービス内で積極的に使用する必要があります。1 つのクライアントを特定の名前付き方式を使用するように設定して、他のクライアントをデフォルト フォーマットを使用するように設定できます。

はじめる前に

次の手順を実行する前に、まずAAAの方式リストを設定して、お客様の状況に適用できるようにする必要があります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **aaagroupserverradius***group-name*
4. **server***ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
5. **attributenas-portformat***format-type*[*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	イネーブル化 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	**aaagroupserverradius***group-name* 例： `Router (config)# aaa group server radius radius1`	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 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	**server***ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] 例： `Router (server-group)# server 172.101.159.172 auth-port 1645 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。
ステップ 5	**attributenas-portformat***format-type*[*string*] 例： `Router (server-group)# attribute nas-port format d`	サービスの種類ごとに固有の名前付け方式を使用するようにサービスを設定します。 • サービス タイプは、独自のサーバ グループを使用するように設定できます。

サーバ単位グループ レベルの RADIUS 属性 5 フォーマットのモニタリングとメンテナンス

サーバ単位グループ レベルの RADIUS 属性 5 フォーマットをモニタおよびメンテナンスするには、次の手順を実行します（**debug** コマンドは個別に使用される場合があります）。

手順の概要

1. イネーブル化
2. **debugaaasg-serverselection**
3. **debugradius**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**debugaaasg-serverselection** 例： `Router# debug aaa sg-server selection`	ルータ内の RADIUS および TACACS+ サーバ グループ システムが特定のサーバを選択している理由に関する情報を表示します。
ステップ 3	**debugradius** 例： `Router# debug radius`	サーバ グループが特定の要求に対して選択されたことを示す情報を表示します。

サーバ単位グループ レベルで指定された RADIUS 属性 5 NAS-Port フォーマットの設定例

サーバ単位グループ レベルで指定された RADIUS 属性 5 フォーマットの例

次の設定例は、デフォルトが形式 F:\tips-migration を使用する一方、RADIUS 属性 5 を送信しないよう選択された専用線 PPP クライアントを示します。

```
interface Serial2/0
 no ip address
 encapsulation ppp
 ppp accounting SerialAccounting
 ppp authentication pap
aaa accounting network default start-stop group radius
aaa accounting network SerialAccounting start-stop group group1
aaa group server radius group1
 server 10.101.159.172 auth-port 1645 acct-port 1646
 attribute nas-port none
radius-server host 10.101.159.172 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
```

その他の参考資料

ここでは、RADIUS ベンダー固有属性（VSA）および RADIUS Disconnect-Cause 属性値に関する関連資料について説明します。

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』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
セキュリティ機能	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』
セキュリティ サーバ プロトコル	『*Cisco IOS XE Security Configuration Guide: Securing User Services*, Release 2』の「セキュリティ サーバ プロトコル」の項
RADIUS Configuration	「RADIUS の設定」機能モジュール。

標準

規格	タイトル
インターネット技術特別調査委員会（IETF）インターネット ドラフト：Network Access Servers Requirements	「Network Access Servers Requirements: Extended RADIUS Practices」

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 2865	『Remote Authentication Dial In User Service (RADIUS)』

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 Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

サーバ単位グループ レベルで指定された RADIUS 属性 5 NAS-Port フォーマットの機能情報

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 *22*：サーバ単位グループ レベルで指定された *RADIUS* 属性 *5*（*NAS-Port*）フォーマットの機能情報

機能名	リリース	機能情報
サーバ単位グループ レベルで指定された RADIUS 属性 5（NAS-Port）フォーマット	Cisco IOS XE Release 3.9S	サーバ単位グループ レベルで指定された RADIUS 属性 5（NAS-Port）フォーマット機能を使用すれば、RADIUS サーバグループごとに設定をカスタマイズできます。この柔軟性によって、グローバルフォーマットの代わりに、カスタマイズされたネットワーク アクセス サーバ（NAS）ポート フォーマットを使用できます。 **attributenas-portformat** コマンドが導入または変更されました。