



アカウントティングの設定

AAA アカウントティング機能を使用すると、ユーザーがアクセスするサービス、およびユーザーが消費するネットワーク リソース量を追跡できます。AAA アカウントティングをイネーブルにすると、ネットワーク アクセス サーバーから TACACS+ または RADIUS セキュリティ サーバー（実装しているセキュリティ手法によって異なります）に対して、アカウントティング レコードの形式でユーザー アクティビティがレポートされます。各アカウントティング レコードにはアカウントティングの Attribute-Value (AV) ペアが含まれ、レコードはセキュリティ サーバーに格納されます。このデータを分析して、ネットワーク管理、クライアント課金、および監査に利用できます。

- [アカウントティングを設定するための前提条件 \(1 ページ\)](#)
- [アカウントティングの設定の制約事項 \(2 ページ\)](#)
- [アカウントティングの設定に関する情報 \(2 ページ\)](#)
- [AAA アカウントティングの設定方法 \(17 ページ\)](#)
- [AAA アカウントティングの設定例 \(26 ページ\)](#)
- [アカウントティングの設定に関するその他の参考資料 \(30 ページ\)](#)
- [アカウントティングの設定の機能履歴 \(31 ページ\)](#)

アカウントティングを設定するための前提条件

次のタスクを実行してから、名前付き方式リストを使用してアカウントティングを設定します。

- ネットワークアクセスサーバで AAA 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 **aaa new-model** コマンドを使用します。
- RADIUS または TACACS+ 認可が発行されている場合、RADIUS または TACACS+ セキュリティ サーバの特性を定義します。Cisco ネットワーク アクセス サーバを設定して RADIUS セキュリティ サーバと通信する方法の詳細については、「RADIUS の設定」モジュールを参照してください。Cisco ネットワーク アクセス サーバを設定して TACACS+ セキュリティ サーバと通信する方法の詳細については、「TACACS+ の設定」モジュールを参照してください。

アカウントティングの設定の制約事項

- アカウントティング情報は、最大 4 台の AAA サーバにのみ同時送信できます。

アカウントティングの設定に関する情報

アカウントティングの名前付き方式リスト

認証および認可方式リストと同様に、アカウントティングの方式リストには、アカウントティングの実行方法とその方式を実行するシーケンスが定義されています。

アカウントティングの名前付き方式リストには、特定のセキュリティプロトコルを指定し、アカウントティングサービスの特定の行またはインターフェイスに使用できます。唯一の例外は、デフォルトの方式リスト（「default」という名前）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストは、シーケンスで照会されるアカウントティング方式（RADIUS、TACACS+ など）を説明する単なる名前付きリストです。方式リストでは、アカウントティングに1つまたは複数のセキュリティプロトコルを指定できます。そのため、最初の方式が失敗した場合に備えてアカウントティングのバックアップシステムを確保できます。Cisco IOS ソフトウェアでは、リストされている最初の方式を使用して、アカウントティングをサポートします。その方式が応答しない場合、リストされている次のアカウントティング方式が選択されます。このプロセスは、リストのいずれかのアカウントティング方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。



- (注) Cisco IOS ソフトウェアでは、前の方式で応答が得られない場合にのみ、リストされている次のアカウントティング方式でアカウントティングが試行されます。このサイクルの任意の時点でアカウントティングが失敗した場合（つまり、セキュリティサーバーからユーザー アクセスの拒否応答が返される場合）、アカウントティングプロセスは停止し、その他のアカウントティング方式は試行されません。

アカウントティング方式リストは、要求されるアカウントティングの種類によって変わります。AAA は、次の 7 種類のアカウントティングをサポートしています。

- **Network** : パケットやバイトカウントなど、すべての PPP、SLIP、または ARAP セッションに関する情報を提供します。
- **EXEC** : ネットワークアクセスサーバのユーザ EXEC ターミナルセッションに関する情報を提供します。

- **Commands** : ユーザが発行する EXEC モードコマンドに関する情報を提供します。コマンドアカウントティングは、特定の特権レベルに関連付けられた、グローバルコンフィギュレーションコマンドなどのすべての EXEC モードコマンドについて、アカウントティングレコードを生成します。
- **Connection** : Telnet、ローカルエリアトランスポート (LAT)、TN3270、パケットアセンブラ/ディスアセンブラ (PAD)、rlogin などのネットワークアクセスサーバから行われたすべてのアウトバンド接続に関する情報を提供します。
- **System** : システムレベルのイベントに関する情報を提供します。
- **Resource** : ユーザ認証に成功したコールの「開始」および「終了」レコードを提供します。また、認証に失敗したコールの「終了」レコードを提供します。
- **VRRS** : Virtual Router Redundancy Service (VRRS) に関する情報を提供します。



(注) システムアカウントティングは、名前付きアカウントティングリストを使用しません。システムアカウントティングのデフォルトリストだけを定義できます。

方式指定リストが作成されると、指定したアカウントティングタイプのアカウントティング方式のリストが定義されます。

アカウントティング方式リストを特定の回線またはインターフェイスに適用してから、定義済み方式のいずれかを実行する必要があります。唯一の例外は、デフォルトの方式リスト (「default」という名前) です。名前付き方式リストを指定せずに、特定のアカウントティングタイプに対して **aaa accounting** コマンドを発行すると、明示的に名前付き方式リストが定義されている場合を除き、すべてのインターフェイスまたは回線にデフォルトの方式リストが自動的に適用されます (定義した方式リストは、デフォルトの方式リストよりも優先されます)。デフォルトの方式リストが定義されていない場合、アカウントティングは実行されません。

ここでは、次の内容について説明します。

方式リストとサーバグループ

サーバグループは、方式リストに使用する既存の RADIUS または TACACS+ サーバホストをグループ化する方法の 1 つです。次の図に、4 台のセキュリティサーバ (R1 と R2 は RADIUS サーバ、T1 と T2 は TACACS+ サーバ) が設置された一般的な AAA ネットワーク設定を示します。R1 と R2 は RADIUS サーバのグループから構成されます。T1 と T2 は TACACS+ サーバのグループから構成されます。

Cisco IOS ソフトウェアでは、RADIUS および TACACS+ サーバ設定はグローバルです。サーバグループを使用して、設定済みのサーバホストのサブセットを指定できます。このようなサーバグループは、特定のサービスに使用できます。たとえば、サーバグループを使用すると、R1 と R2 を個別のサーバグループ (SG1 と SG2) として定義し、T1 と T2 を個別のサーバグループ (SG3 と SG4) として定義できます。つまり、R1 と T1 (SG1 と SG3) または R2 と T2 (SG2 と SG4) を方式リストに指定することができます。そのため、RADIUS および TACACS+ のリソースを割り当てる場合の柔軟性が高くなります。

サーバグループには、1台のサーバに対して複数のホストエントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IPアドレスとUDPポート番号の組み合わせで構成されます。これにより、RADIUSホストとして定義されているさまざまなポートが、固有のAAAサービスを提供できるようになります。つまり、この固有識別情報を使用して、1台のサーバ上に複数のUDPポートが存在する場合、同じIPアドレスからそれぞれのUDPポートに対してRADIUS要求を送信できます。1台のRADIUSサーバ上にある異なる2つのホストエントリが1つのサービス（アカウントングなど）に設定されている場合、設定されている2番目のホストエントリは最初のホストエントリのフェールオーバーバックアップとして動作します。この例を使用して、最初のホストエントリがアカウントングサービスの提供に失敗した場合、ネットワークアクセスサーバは、同じデバイスに設定されている2番目のホストエントリに対してアカウントングサービスを試行します（RADIUSホストエントリは、設定順に試行されます）。

サーバグループの設定および着信番号識別サービス（DNIS）番号に基づくサーバグループの設定の詳細については、「RADIUSの設定」または「TACACS+の設定」を参照してください。

AAA アカウントング方式

次の2つのアカウントング方式がサポートされます。

- TACACS+：ネットワークアクセスサーバは、アカウントングレコードの形式でTACACS+セキュリティサーバに対してユーザアクティビティを報告します。各アカウントングレコードは、アカウントングAVペアが含まれ、セキュリティサーバ上で保管されます。
- RADIUS：ネットワークアクセスサーバは、アカウントングレコードの形式でRADIUSセキュリティサーバに対してユーザアクティビティを報告します。各アカウントングレコードは、アカウントングAVペアが含まれ、セキュリティサーバ上で保管されます。



(注) パスワードおよびアカウントングログは、TACACS+またはRADIUSセキュリティサーバへ送信される前にマスクされます。マスクされていない情報をTACACS+またはRADIUSセキュリティサーバに送信するには、**aaa accounting commands visible-keys** コマンドを使用します。

アカウントングレコードの種類

最小限のアカウントングの場合、**stop-only** キーワードを使用します。このキーワードによって、要求されたユーザプロセスの終了時に、終了レコードアカウントング通知を送信するように、指定した方式（RADIUSまたはTACACS+）に指示します。詳細なアカウントング情報が必要な場合、**start-stop** キーワードを使用して、要求されたイベントの開始時には開始アカウントング通知、そのイベントの終了時には修理用アカウントング通知を送信します。この回線またはインターフェイスですべてのアカウントングアクティビティを終了するには、**none** キーワードを使用します。

アカウントング方式

次の表に、サポートされるアカウントング方式を示します。

表 1:AAA アカウントティング方式

キーワード	Description
group radius	アカウントティングにすべての RADIUS サーバーのリストを使用します。
group tacacs+	アカウントティングにすべての TACACS+ サーバーのリストを使用します。
group <i>group-name</i>	<i>group-name</i> サーバーグループで定義したように、アカウントティングのための RADIUS サーバーまたは TACACS+ サーバーのサブセットを使用します。

method 引数は、認証アルゴリズムが試行する実際の方式を指します。追加の認証方式は、直前の方式で（失敗した場合ではなく）エラーが返された場合にのみ使用されます。他のすべての方式がエラーを返しても、認証に成功したことを指定するには、コマンドで追加の方式を指定します。たとえば、TACACS+ 認証がエラーを返す場合に認証のバックアップ方式として RADIUS を指定する `acct_tac1` という方式リストを作成するには、次のコマンドを入力します。

```
aaa accounting network acct_tac1 stop-only group tacacs+ group radius
```

名前付きリストが `aaa accounting` コマンドに指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。

たとえば、ログイン時のユーザー認証のデフォルト方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa accounting network default stop-only group radius
```

AAA アカウントティングは、次の方式をサポートします。

- **group tacacs** : ネットワークアクセスサーバーからアカウントティング情報を TACACS+ セキュリティサーバーに送信するには、**group tacacs+ method** キーワードを使用します。
- **group radius** : ネットワークアクセスサーバーからアカウントティング情報を RADIUS セキュリティサーバーに送信するには、**group radius method** キーワードを使用します。



(注) SLIP のアカウントティング方式リストは、関連インターフェイスで PPP に設定されているすべての方式に従います。特定のインターフェイスに定義および適用されるリストがない場合（または PPP 設定が指定されていない場合）、アカウントティングのデフォルト設定が適用されます。

- **group group-name** : RADIUS または TACACS+ サーバーのサブセットを指定して、アカウントティング方式として使用するには、**group group-name** 方式を指定して **aaa accounting** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group loginrad** のメンバを最初に定義します。

```
aaa group server radius loginrad
server 172.16.2.3
server 172.16.2.17
server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバーが **group loginrad** のメンバとして指定されます。

他の方式リストが定義されていない場合、ネットワークアカウントティングの方式として **group loginrad** を指定するには、次のコマンドを入力します。

```
aaa accounting network default start-stop group loginrad
```

アカウントティング方式としてグループ名を使用するには、事前に RADIUS または TACACS+ セキュリティ サーバーとの通信をイネーブルにする必要があります。

AAA アカウンティング タイプ

ネットワーク アカウンティング

ネットワーク アカウンティングは、パケットやバイト カウントなど、すべての PPP、SLIP、または ARAP セッションに関する情報を提供します。

次に、EXEC セッションを介して着信する PPP ユーザの RADIUS ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:44:45 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "0000000D"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 27 04:45:00 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
```

```

Service-Type = Framed
Acct-Session-Id = "0000000E"
Framed-IP-Address = "10.1.1.2"
Framed-Protocol = PPP
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identififier = "172.16.25.15"
Wed Jun 27 04:47:46 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "0000000E"
Framed-IP-Address = "10.1.1.2"
Framed-Protocol = PPP
Acct-Input-Octets = 3075
Acct-Output-Octets = 167
Acct-Input-Packets = 39
Acct-Output-Packets = 9
Acct-Session-Time = 171
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identififier = "172.16.25.15"
Wed Jun 27 04:48:45 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "408"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "0000000D"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identififier = "172.16.25.15"

```

次に、最初にEXECセッションを開始したPPPユーザのTACACS+ネットワークアカウントティングレコードに含まれる情報の例を示します。

```

Wed Jun 27 04:00:35 2001 172.16.25.15 username1 tty4 562/4327528
starttask_id=28 service=shell
Wed Jun 27 04:00:46 2001 172.16.25.15 username1 tty4 562/4327528
starttask_id=30 addr=10.1.1.1 service=ppp
Wed Jun 27 04:00:49 2001 172.16.25.15 username1 tty4 408/4327528
updattask_id=30 addr=10.1.1.1 service=ppp protocol=ip addr=10.1.1.1
Wed Jun 27 04:01:31 2001 172.16.25.15 username1 tty4 562/4327528 stoptask_id=30
addr=10.1.1.1 service=ppp protocol=ip addr=10.1.1.1
bytes_in=2844 bytes_out=1682 paks_in=36
paks_out=24 elapsed_time=51
Wed Jun 27 04:01:32 2001 172.16.25.15 username1 tty4 562/4327528 stoptask_id=28
service=shell elapsed_time=57

```



(注) アカウントティングパケットレコードの正確なフォーマットは、セキュリティサーバデーモンに応じて変わります。

次に、autoselect を介して着信する PPP ユーザの RADIUS ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:30:52 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 3
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "0000000B"
Framed-Protocol = PPP
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 27 04:36:49 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 3
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "0000000B"
Framed-Protocol = PPP
Framed-IP-Address = "10.1.1.1"
Acct-Input-Octets = 8630
Acct-Output-Octets = 5722
Acct-Input-Packets = 94
Acct-Output-Packets = 64
Acct-Session-Time = 357
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
```

次に、autoselect を介して着信する PPP ユーザの TACACS+ ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:02:19 2001 172.16.25.15 username1 Async5 562/4327528
starttask_id=35 service=ppp
Wed Jun 27 04:02:25 2001 172.16.25.15 username1 Async5 562/4327528
updatetask_id=35 service=ppp protocol=ip addr=10.1.1.2
Wed Jun 27 04:05:03 2001 172.16.25.15 username1 Async5 562/4327528 stoptask_id=35
service=ppp protocol=ip addr=10.1.1.2
bytes_in=3366 bytes_out=2149 paks_in=42
paks_out=28 elapsed_time=164
```

EXEC アカウンティング

EXEC アカウンティングは、ネットワーク アクセス サーバ上にあるユーザ EXEC ターミナル セッション（ユーザシェル）に関する情報を提供します。たとえば、ユーザ名、日付、開始時刻と終了時刻、アクセスサーバの IP アドレス、および（ダイヤルインユーザの場合）発信元の電話番号などです。

次に、ダイヤルインユーザの RADIUS EXEC アカウントティング レコードに含まれる情報の例を示します。

```

Wed Jun 27 04:26:23 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 1
  User-Name = "username1"
  Client-Port-DNIS = "4327528"
  Caller-ID = "5622329483"
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS
  Service-Type = Exec-User
  Acct-Session-Id = "00000006"
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"
Wed Jun 27 04:27:25 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 1
  User-Name = "username1"
  Client-Port-DNIS = "4327528"
  Caller-ID = "5622329483"
  Acct-Status-Type = Stop
  Acct-Authentic = RADIUS
  Service-Type = Exec-User
  Acct-Session-Id = "00000006"
  Acct-Session-Time = 62
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"

```

次に、ダイヤルインユーザの TACACS+ EXEC アカウントティング レコードに含まれる情報の例を示します。

```

Wed Jun 27 03:46:21 2001      172.16.25.15      username1      tty3      5622329430/4327528
  start
  task_id=2      service=shell
Wed Jun 27 04:08:55 2001      172.16.25.15      username1      tty3      5622329430/4327528
  stop
  task_id=2      service=shell      elapsed_time=1354

```

次に、Telnet ユーザの RADIUS EXEC アカウントティング レコードに含まれる情報の例を示します。

```

Wed Jun 27 04:48:32 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 26
  User-Name = "username1"
  Caller-ID = "10.68.202.158"
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS
  Service-Type = Exec-User
  Acct-Session-Id = "00000010"
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"
Wed Jun 27 04:48:46 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 26
  User-Name = "username1"

```

```

Caller-ID = "10.68.202.158"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "00000010"
Acct-Session-Time = 14
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

```

次に、Telnet ユーザの TACACS+ EXEC アカウントング レコードに含まれる情報の例を示します。

```

Wed Jun 27 04:06:53 2001      172.16.25.15      username1      tty26      10.68.202.158
starttask_id=41      service=shell
Wed Jun 27 04:07:02 2001      172.16.25.15      username1      tty26      10.68.202.158
stoptask_id=41      service=shell      elapsed_time=9

```

コマンドアカウントング

コマンドアカウントングは、ネットワーク アクセス サーバで実行される各特権レベルの EXEC シェル コマンドに関する情報を提供します。各コマンドアカウントング レコードには、その特権レベルで実行されるコマンド、各コマンドが実行された日時、および実行したユーザのリストが含まれます。

次に、特権レベル 1 の TACACS+ コマンドアカウントング レコードに含まれる情報の例を示します。

```

Wed Jun 27 03:46:47 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=3      service=shell      priv-lvl=1      cmd=show version <cr>
Wed Jun 27 03:46:58 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=4      service=shell      priv-lvl=1      cmd=show interfaces Ethernet
0 <cr>
Wed Jun 27 03:47:03 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=5      service=shell      priv-lvl=1      cmd=show ip route <cr>

```

次に、特権レベル 15 の TACACS+ コマンドアカウントング レコードに含まれる情報の例を示します。

```

Wed Jun 27 03:47:17 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=6      service=shell      priv-lvl=15      cmd=configure terminal <cr>
Wed Jun 27 03:47:21 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=7      service=shell      priv-lvl=15      cmd=interface Serial 0 <cr>
Wed Jun 27 03:47:29 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=8      service=shell      priv-lvl=15      cmd=ip address 10.1.1.1
255.255.255.0 <cr>

```



(注) Cisco の RADIUS 実装は、コマンドアカウントングをサポートしていません。

接続アカウントング

接続アカウントングは、Telnet、LAT、TN3270、PAD、rlogin などのネットワーク アクセス サーバから行われるすべての発信接続に関する情報を提供します。

次に、発信 Telnet 接続の RADIUS 接続アカウントティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:28:00 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "00000008"
Login-Service = Telnet
Login-IP-Host = "10.68.202.158"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identififier = "172.16.25.15"
```

```
Wed Jun 27 04:28:39 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "00000008"
Login-Service = Telnet
Login-IP-Host = "10.68.202.158"
Acct-Input-Octets = 10774
Acct-Output-Octets = 112
Acct-Input-Packets = 91
Acct-Output-Packets = 99
Acct-Session-Time = 39
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identififier = "172.16.25.15"
```

次に、発信 Telnet 接続の TACACS+ 接続アカウントティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:47:43 2001          172.16.25.15      username1  tty3      5622329430/4327528
start      task_id=10      service=connection      protocol=telnet  addr=10.68.202.158
cmd=telnet username1-sun
Wed Jun 27 03:48:38 2001          172.16.25.15      username1  tty3      5622329430/4327528
stop      task_id=10      service=connection      protocol=telnet  addr=10.68.202.158
cmd=telnet username1-sun      bytes_in=4467  bytes_out=96      paks_in=61      paks_out=72
elapsed_time=55
```

次に、発信 rlogin 接続の RADIUS 接続アカウントティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:29:48 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Start
```

```

Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "0000000A"
Login-Service = Rlogin
Login-IP-Host = "10.68.202.158"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:30:09 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "0000000A"
Login-Service = Rlogin
Login-IP-Host = "10.68.202.158"
Acct-Input-Octets = 18686
Acct-Output-Octets = 86
Acct-Input-Packets = 90
Acct-Output-Packets = 68
Acct-Session-Time = 22
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

```

次に、発信 rlogin 接続の TACACS+ 接続アカウント記録に含まれる情報の例を示します。

```

Wed Jun 27 03:48:46 2001      172.16.25.15      username1  tty3      5622329430/4327528
start  task_id=12      service=connection  protocol=rlogin addr=10.68.202.158
cmd=rlogin username1-sun /user username1
Wed Jun 27 03:51:37 2001      172.16.25.15      username1  tty3      5622329430/4327528
stop   task_id=12      service=connection  protocol=rlogin addr=10.68.202.158
cmd=rlogin username1-sun /user username1 bytes_in=659926 bytes_out=138 paks_in=2378
paks_
out=1251      elapsed_time=171

```

次に、発信 LAT 接続の TACACS+ 接続アカウント記録に含まれる情報の例を示します。

```

Wed Jun 27 03:53:06 2001      172.16.25.15      username1  tty3      5622329430/4327528
start  task_id=18      service=connection  protocol=lat   addr=VAX      cmd=lat
VAX
Wed Jun 27 03:54:15 2001      172.16.25.15      username1  tty3      5622329430/4327528
stop   task_id=18      service=connection  protocol=lat   addr=VAX      cmd=lat
VAX bytes_in=0      bytes_out=0      paks_in=0      paks_out=0      elapsed_time=6

```

システム アカウンティング

システム アカウンティングは、すべてのシステムレベル イベント（たとえば、システムのリブート時やアカウント記録のオン/オフ時）に関する情報を提供します。

次のアカウント記録は、AAA アカウンティングがオフになったことを示す一般的な TACACS+ システム アカウンティング記録 サーバを示します。

```
Wed Jun 27 03:55:32 2001      172.16.25.15      unknown unknown unknown start  task_id=25
service=system
event=sys_acct  reason=reconfigure
```



(注) アカウントティングパケットレコードの正確なフォーマットは、TACACS+デーモンに応じて変わります。

次のアカウントティングレコードは、AAAアカウントティングがオンになったことを示すTACACS+システムアカウントティングレコードを示します。

```
Wed Jun 27 03:55:22 2001      172.16.25.15      unknown unknown unknown stop  task_id=23
service=system
event=sys_acct  reason=reconfigure
```

リソース アカウントティング

シスコが採用している AAA アカウントティングでは、ユーザー認証を通過したコールに対する「開始」レコードと「終了」レコードがサポートされます。ユーザー認証の一部として認証に失敗したコールの「終了」レコードを生成する追加機能もサポートされます。このようなレコードは、ネットワークを管理およびモニタするアカウントティングレコードを採用する場合に必要です。

ここでは、次の内容について説明します。

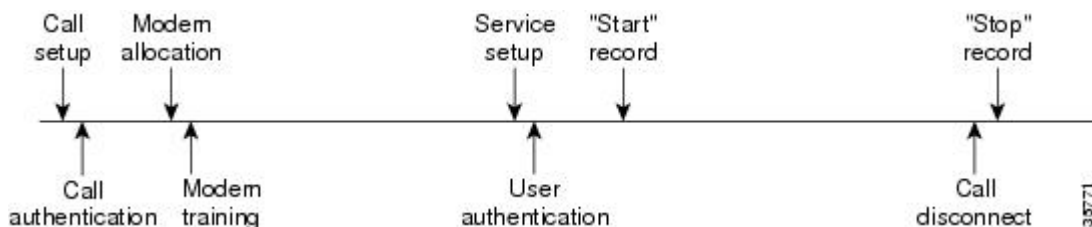
AAA リソース失敗終了アカウントティング

AAA リソース失敗終了アカウントティングの前には、コール設定シーケンスのユーザー認証段階に到達できなかったコールについて、アカウントティングレコードを提供する方式がありませんでした。このようなレコードは、ネットワークおよびその卸売りの顧客を管理およびモニタするアカウントティングレコードを採用する場合に必要です。

この機能によって、ユーザー認証に到達しなかったコールの「終了」アカウントティングレコードが生成されます。「終了」レコードは、コール設定の時点から生成されます。ユーザー認証に成功したすべてのコールは、従来と同様に動作します。つまり、追加のアカウントティングレコードは確認されません。

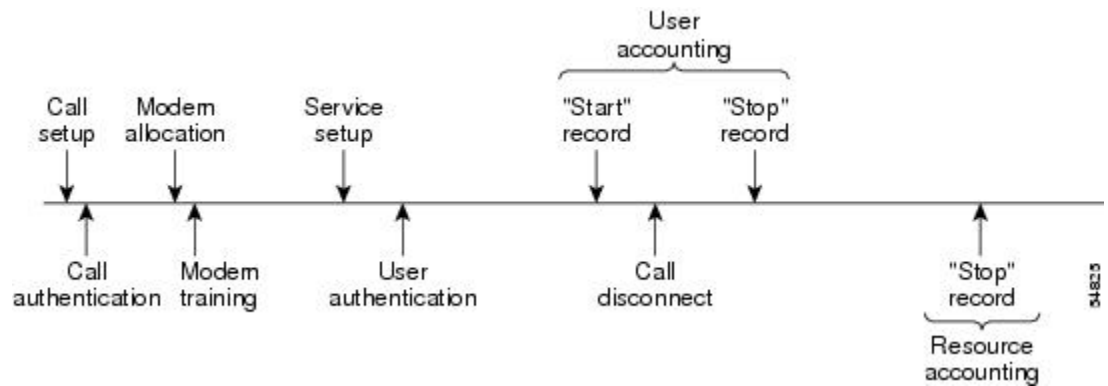
次の図に、通常のコールフローで、AAA リソース失敗終了アカウントティングを有効にしていないコールシーケンスを示します。

図 1: 通常のフローで AAA リソース失敗終了アカウントティングを有効にしていないモデムダイヤルインコール設定シーケンス



次の図に、通常のコールフローで、AAA リソース失敗終了アカウントिंगを有効にしたコールシーケンスを示します。

図 2: 通常のフローで AAA リソース失敗終了アカウントिंगを有効にしたモデムダイヤルインコール設定シーケンス



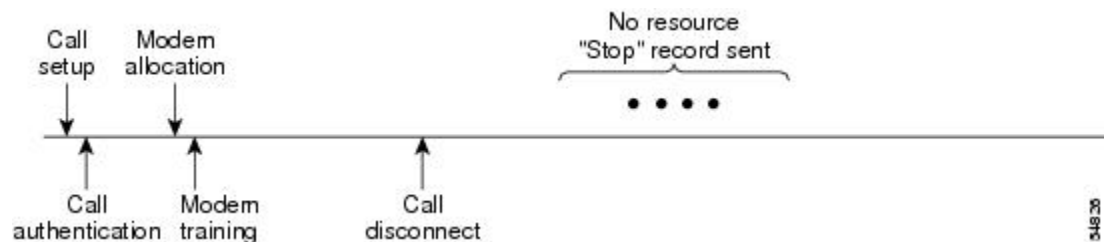
次の図に、ユーザー認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウントिंगを有効にしたコール設定シーケンスを示します。

図 3: ユーザー認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウントिंगを有効にしたモデムダイヤルインコール設定シーケンス



次の図に、ユーザー認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウントिंगを有効にしていないコール設定シーケンスを示します。

図 4: ユーザー認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウントिंगをイネーブルにしていないモデムダイヤルインコール設定シーケンス



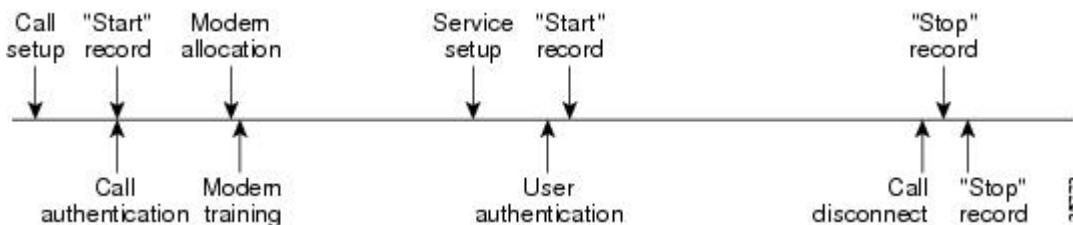
開始 - 終了レコードの AAA リソース アカウントिंग

開始 - 終了レコードの AAA リソース アカウントिंगは、各コール設定時に「開始」レコードを送信し、コールの接続解除時に対応する「終了」レコードを送信する機能をサポートしています。この機能は、アカウントिंगレコードなどを報告するデータの発信元の1つから、卸売りの顧客を管理およびモニターするために使用できます。

この機能を使用すると、コール設定およびコールの接続解除の「開始-終了」アカウントティングレコードは、デバイスに対するリソース接続の進行状況を追跡します。個別のユーザー認証「開始-終了」アカウントティングレコードが、ユーザー管理の進行状況を追跡します。これら2セットのアカウントティングレコードは、そのコールで固有のセッションIDを使用して相互リンクされます。

次の図は、AAA リソース開始-終了アカウントティングを有効にしたコール設定シーケンスを示します。

図 5: リソース開始-終了アカウントティングを有効にしたモデムダイヤルインコール設定シーケンス



AAA アカウントティングの強化

AAA ブロードキャストアカウントティング

AAA ブロードキャストアカウントティングを有効にすると、アカウントティング情報を複数のAAAサーバに同時に送信できます。つまり、アカウントティング情報を1つまたは複数のAAAサーバに同時にブロードキャストすることが可能です。この機能を使用すると、サービスプロバイダーは自社使用のプライベートAAAサーバやエンドユーザのAAAサーバにアカウントティング情報を送信できるようになります。この機能では、音声アプリケーションによる課金情報も提供されます。

ブロードキャストは、RADIUS または TACACS+ サーバのグループに使用できます。また、各サーバグループは、他のグループとは関係なく、フェールオーバーの場合のバックアップサーバを定義できます。

したがって、サービスプロバイダーとそのエンドユーザは、アカウントティングサーバに異なるプロトコル (RADIUS または TACACS+) を使用できます。また、サービスプロバイダーとそのエンドユーザは、それぞれ単独でバックアップサーバを指定することもできます。音声アプリケーションについては、独自のフェールオーバーシーケンスを持つ個別のグループを介して、冗長的なアカウントティング情報を単独で管理できます。

AAA セッション MIB

ユーザがAAAセッションMIB機能を使用すると、簡易ネットワーク管理プロトコル (SNMP) を使用して自身の認証済みクライアント接続をモニタおよび終了できます。そのクライアントのデータが提示されるため、RADIUS または TACACS+ サーバから報告されるAAAアカウントティング情報に直接関連付けることができます。AAAセッションMIBは、次の情報を提供します。

- 各AAA機能の統計情報 (`show radius statistics` コマンドと併用する場合)

- AAA 機能を提供するサーバのステータス
- 外部 AAA サーバの ID
- (アイドル時間などの) リアルタイム情報 (アクティブ コールを終了するかどうかを評価する SNMP ネットワークが使用する追加基準を提供します)

次の表に、認証済みクライアントと AAA セッション MIB 機能との接続をモニタおよび終了するために使用できる SNMP ユーザエンド データ オブジェクトを示します。

表 2: SNMP エンドユーザ データ オブジェクト

SessionId	AAA アカウントング プロトコルに使用されるセッション ID (RADIUS 属性 44 (Acct-Session-ID) から報告される値と同じ)
UserId	ユーザ ログイン ID または (ログインが使用できない場合) 長さがゼロの文字列
IpAddr	セッションの IP アドレスまたは (IP アドレスが適用されない場合、または使用できない場合) 0.0.0.0
IdleTime	セッションがアイドルになってからの経過時間
Disconnect	そのクライアントとの接続を解除するために使用されるセッション終了オブジェクト
CallId	コール トラッカー レコードが保存した、このアカウントング セッションに対応するエントリ インデックス

次の表に、システム別に SNMP を使用する AAA セッション MIB 機能から提供される AAA の概要情報を示します。

表 3: SNMP AAA セッションの概要

ActiveTableEntries	現在アクティブなセッションの数
ActiveTableHighWaterMark	システムが最後に再インストールされてからの同時接続セッションの最大数
TotalSessions	システムが最後に再インストールされてからのセッションの合計数
DisconnectedSessions	システムが最後に再インストールされてから接続解除されたセッションの合計数

アカウントング属性と値のペア

ネットワーク アクセス サーバは、TACACS+ AV のペアまたは RADIUS 属性 (実装しているセキュリティ方式によって異なります) に定義されたアカウントング機能をモニタします。

AAA アカウントティングの設定方法

名前付き方式リストによる AAA アカウントティングの設定

名前付き方式リストを使用して AAA アカウントティングを設定するには、次の手順を実行します。



(注) システム アカウントティングは、名前付き方式リストを使用しません。システム アカウントティングの場合、デフォルトの方式リストだけを定義します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 ・パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： 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	aaa accounting {system network exec connection commands level} {default list-name} {start-stop stop-only none} [method1 [method2...]] 例： Device(config)# aaa accounting system default start-stop	アカウントティング方式リストを作成し、アカウントティングを有効にします。引数 <i>list-name</i> は、作成したリストに名前を付けるときに使用される文字列です。
ステップ 4	次のいずれかを実行します。 ・ line [aux console tty vty] line-number [ending-line-number] ・ interface interface-type interface-number 例： Device(config)# line aux line1	アカウントティング方式リストを適用する回線について、ラインコンフィギュレーション モードを開始します。 または アカウントティング方式リストを適用するインターフェイスについて、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> • accounting {arap commands level connection exec} {default list-name} • ppp accounting {default list-name} <p>例：</p> <pre>Device(config-line)# accounting arap default</pre>	<p>1つの回線または複数回線にアカウントング方式リストを適用します。</p> <p>または</p> <p>1つのインターフェイスまたは複数インターフェイスにアカウントング方式リストを適用します。</p>
ステップ 6	<p>end</p> <p>例：</p> <pre>Device(config-line)# end</pre>	<p>(任意) ライン コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。</p>

ヌルユーザ名セッション時のアカウントングレコード生成の抑制

AAA アカウントングをアクティブにすると、Cisco IOS ソフトウェアは、システム上のすべてのユーザにアカウントングレコードを発行します。このとき、プロトコル変換のためユーザ名文字列がヌルになっているユーザも含まれます。この例では、**aaa authentication login method-list none** コマンドが適用される回線で着信するユーザがそれに該当します。関連付けられているユーザ名がないセッションについて、アカウントングレコードが生成されないようにするには、グローバル コンフィギュレーションモードで次のコマンドを使用します。

コマンド	目的
<pre>Device (config)# aaa accounting suppress null-username</pre>	ユーザ名文字列がヌルのユーザについて、アカウントティングレコードが生成されないようにします。

中間アカウントティング レコードの生成

アカウントティング サーバに定期的な中間アカウントティング レコードを送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 モードで次のコマンドを使用します。

コマンド	目的
<pre>Device (config)# aaa accounting update [newinfo] [periodic] <i>number</i></pre>	アカウントティング サーバに送信される定期的中間アカウントティングレコードをイネーブルにします。

aaa accounting update コマンドをアクティブにすると、Cisco IOS ソフトウェアによってシステム上のすべてのユーザーの中間アカウントティングレコードが発行されます。 **newinfo** キーワードを使用した場合は、レポートする新しいアカウントティング情報が発生するたびに、中間アカウントティングレコードがアカウントティングサーバに送信されます。たとえば、IPCP がリモートピアとの間で IP アドレスのネゴシエーションを完了したときなどです。中間アカウントティングレコードには、リモートピアに使用されるネゴシエート済み IP アドレスが含まれます。

キーワード **periodic** と一緒に使用した場合は、*number* 引数による定義に基づいて、中間アカウントングレコードが定期的送信されます。中間アカウントングレコードには、中間アカウントングレコードが送信される時間までに、そのユーザについて記録されたすべてのアカウントング情報が含まれます。



注意 多数のユーザがネットワークにログインしている場合には、**aaa accounting update periodic** コマンドを使用すると、重度の輻輳が発生する可能性があります。

定期的アカウントングレコードを有効化する代替手段の設定

次の代替手段を使用して、アカウントングサーバーに送信される定期的中間アカウントングレコードをイネーブルにできます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： 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	aaa accounting network default 例： Device(config)# aaa accounting network default	すべてのネットワーク関連のサービス要求のデフォルトのアカウントングを設定し、アカウントング方式リストの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	action-type {none start-stop [periodic {disable interval minutes}] stop-only} 例： Device(cfg-acct-mlist)# action-type start-stop 例： periodic interval 5	アカウントングレコードに対して実行されるアクションのタイプを指定します。 • (任意) periodic キーワードは、定期的なアカウントングアクションを示します。 • interval キーワードは、定期的なアカウントング間隔を指定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>value</i> 引数は、アカウントティング更新レコードの間隔を指定します（分単位）。 • disable キーワードは、定期的なアカウントティングを無効にします。
ステップ 5	end 例： Device(cfg-acct-mlist)# end	アカウントティング方式リスト コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

中間サービス アカウントティング レコードの生成

このタスクを実行して、サブスクリバに対する定期的な間隔での中間サービスアカウントティングレコードの生成をイネーブルにします。

始める前に

ユーザー サービス プロファイルの RADIUS 属性 85 は設定済みの中間の間隔値よりも常に優先されます。RADIUS 属性 85 は、ユーザー サービス プロファイル内にある必要があります。詳細については、RADIUS 属性の概要および RADIUS IETF 属性の機能のドキュメントを参照してください。



- (注) RADIUS 属性 85 がユーザー サービス プロファイル内にない場合、中間アカウントティングレコードの生成で設定された中間の間隔値がサービスの中間アカウントティングレコードに使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： 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。

	コマンドまたはアクション	目的
ステップ 3	subscriber service accounting interim-interval minutes 例： Device(config)# subscriber service accounting interim-interval 10	サブスクリバに対する定期的な間隔での中間サービス アカウントングレコードの生成をイネーブルにします。 <i>minutes</i> 引数は、アカウントング更新レコードを送信する定期的な間隔を1～71582分で示します。
ステップ 4	end 例： Device(config)# end	グローバル コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

失敗したログインまたはセッションに対するアカウントングレコードの生成

AAA アカウントングをアクティブにすると、Cisco IOS XE ソフトウェアは、ログイン認証に失敗したシステム ユーザー、またはログイン認証には成功しても何らかの理由で PPP ネゴシエーションに失敗したユーザーのアカウントングレコードを生成しません。

ログイン時またはセッションネゴシエーション中の認証に失敗したユーザーについて、アカウントング終了レコードを生成するように指定するには、グローバルコンフィギュレーションモードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa accounting send stop-record authentication failure	ログイン時またはセッションネゴシエーション中の認証に失敗したユーザについて、「終了」レコードを生成します。

EXEC-Stop レコードよりも前のアカウントング NETWORK-Stop レコードの指定

EXEC 終了セッションを開始する PPP ユーザーの場合、EXEC-stop レコードの前に、NETWORK レコードを生成するように指定できます。特定のサービスについて顧客に課金する場合など、状況によっては、ネットワークの開始レコードと終了レコードを一緒に保持する方が望ましいことがあります。その際、基本的に、EXEC の開始メッセージと終了メッセージのフレームワーク内に「ネスト」にします。たとえば、PPP を使用するユーザーダイヤルインによって、EXEC-start、NETWORK-start、EXEC-stop、NETWORK-stop というレコードを作成できます。ネットワーク アカウントングレコードをネストにすることで、NETWORK-stop レコードは NETWORK-start メッセージ (EXEC-start、NETWORK-start、NETWORK-stop、EXEC-stop) に従います。

ユーザーセッションのアカウントティングレコードをネストするには、グローバルコンフィギュレーションモードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa accounting nested	ネットワークアカウントティングレコードをネストします。

スイッチオーバー上のシステム アカウントティング レコードの抑制

スイッチオーバー中のシステム アカウントティングオンおよびアカウントティングオフ メッセージを抑制するには、グローバルコンフィギュレーションモードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa accounting redundancy suppress system-records	スイッチオーバー中のシステムアカウントティングレコードを抑制します。

AAA リソース失敗終了アカウントティングの設定

リソース失敗終了アカウントティングを有効にするには、グローバルコンフィギュレーションモードで次のコマンドを使用します。

コマンド	目的
<pre>Device(config)# aaa accounting resource method-list stop-failure group server-group</pre>	<p>ユーザー認証に到達しないコールについて、「終了」レコードを生成します。</p> <p>(注) この機能を設定する前に、アカウントティングを設定するための前提条件 (1 ページ) のセクションに記載されている作業を実行し、ネットワークアクセスサーバー上でSNMPを有効にしてください。</p>

開始 - 終了レコードの AAA リソース アカウントティングの設定

開始 - 終了レコードのフルリソースアカウントティングをイネーブルにするには、グローバルコンフィギュレーションモードで次のコマンドを使用します。

コマンド	目的
<pre>Device(config)# aaa accounting resource method-list start-stop group server-group</pre>	<p>各コール設定時に「開始」レコードを送信し、コールの接続解除時に対応する「終了」レコードを送信する機能をサポートします。</p> <p>(注) この機能を設定する前に、アカウントिंगを設定するための前提条件 (1 ページ) のセクションに記載されている作業を実行し、ネットワークアクセスサーバー上でSNMPを有効にしてください。</p>

AAA ブロードキャスト アカウンティング

AAA ブロードキャスト アカウンティングを有効にすると、アカウントング情報を複数の AAA サーバに同時に送信できます。つまり、アカウントング情報を 1 つまた複数の AAA サーバに同時にブロードキャストすることが可能です。この機能を使用すると、サービスプロバイダーは自社使用のプライベート AAA サーバやエンドユーザの AAA サーバにアカウントング情報を送信できるようになります。この機能では、音声アプリケーションによる課金情報も提供されます。

ブロードキャストは、RADIUS または TACACS+ サーバのグループに使用できます。また、各サーバグループは、他のグループとは関係なく、フェールオーバーの場合のバックアップサーバを定義できます。

したがって、サービスプロバイダーとそのエンドユーザは、アカウントングサーバに異なるプロトコル (RADIUS または TACACS+) を使用できます。また、サービスプロバイダーとそのエンドユーザは、それぞれ単独でバックアップサーバを指定することもできます。音声アプリケーションについては、独自のフェールオーバーシーケンスを持つ個別のグループを介して、冗長的なアカウントング情報を単独で管理できます。

DNIS による AAA ブロードキャスト アカウンティングの設定

AAA ブロードキャストアカウントングを設定するには、グローバルコンフィギュレーションモードで `aaa dnis map accounting network` コマンドを使用します。

コマンド	目的
<pre>Device(config)# aaa dnis map dnis-number accounting network [start-stop stop-only none] [broadcast] <i>method1</i> [<i>method2...</i>]</pre>	<p>DNIS によるアカウントティングの設定を許可します。このコマンドは、グローバルの aaa accounting コマンドよりも優先されます。</p> <p>複数の AAA サーバに対するアカウントティングレコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウントティングレコードを同時に送信します。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップサーバが使用されます。</p>

AAA サーバーが到達不能な場合のデバイスとのセッションの確立

AAA サーバーが到達不能の場合に、デバイスとの間にコンソールセッションを確立するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
<pre>no aaa accounting system guarantee-first</pre>	<p>aaa accounting system guarantee-first コマンドは、システムアカウントを最初のレコードとして保証します。これは、デフォルトの条件です。</p> <p>状況によっては、システムの再ロードが完了するまで（3分よりも長くかかる可能性があります）、ユーザーがコンソールまたは Telnet 接続でセッションを開始できない可能性があります。この問題を解決するには、no aaa accounting system guarantee-first コマンドを使用します。</p>

アカウントティングのモニタリング

RADIUS または TACACS+ アカウントティングの場合、特定の **show** コマンドは存在しません。ログインしているユーザーに関する情報を表示するアカウントティングレコードを取得するには、特権 EXEC モードで次のコマンドを使用します。

コマンドまたはアクション	目的
<pre>show accounting</pre>	<p>ネットワークでアクティブなアカウント可能なイベントの表示を許可し、アカウントティングサーバでデータが損失した場合に情報を収集できます。</p>

アカウントINGのトラブルシューティング

アカウントING情報の問題を解決するには、特権 EXEC モードで次のコマンドを使用します。

コマンドまたはアクション	目的
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。

AAA アカウントINGの設定例

例：名前付き方式リストの設定

次に、RADIUS サーバーから AAA サービスを提供するためにシスコ デバイス（AAA および RADIUS セキュリティサーバーとの通信で有効）を設定する例を示します。RADIUS サーバーが応答に失敗すると、認証情報と認可情報についてローカルデータベースへの照会が行われ、アカウントING サービスは TACACS+ サーバーによって処理されます。

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login admins local
Device(config)# aaa authentication ppp dialins group radius local
Device(config)# aaa authorization network network1 group radius local
Device(config)# aaa accounting network network2 start-stop group radius group tacacs+
Device(config)# username root password ALongPassword
Device(config)# tacacs server server1
Device(config-server-tacacs)# address ipv4 172.31.255.0
Device(config-server-tacacs)# key goaway
Device(config-server-tacacs)# exit
Device(config)# radius server isp
Device(config-sg-radius)# key myRaDiUSpassWoRd
Device(config-sg-radius)# exit
Device(config)# interface group-async 1
Device(config-if)# group-range 1 16
Device(config-if)# encapsulation ppp
Device(config-if)# ppp authentication chap dialins
Device(config-if)# ppp authorization network1
Device(config-if)# ppp accounting network2
Device(config-if)# exit
Device(config)# line 1 16
Device(config-line)# autoselect ppp
Device(config-line)# autoselect during-login
Device(config-line)# login authentication admins
Device(config-line)# modem dialin
Device(config-line)# end
```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。

- **aaa authentication login admins local** コマンドは、ログイン認証に方式リスト「admins」を定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、認証方式リスト「dialins」を定義します。このリストは、最初にRADIUS認証を指定して、次に（RADIUSサーバーが応答しない場合）PPPを使用してシリアル回線上でローカル認証が使用されます。
- **aaa authorization network network1 group radius local** コマンドで、「network1」というネットワーク許可方式リストを定義します。これにより、PPPを使用してシリアル回線上でRADIUS許可を使用するよう指定されます。RADIUSサーバーが応答に失敗すると、ローカルネットワークの認可が実行されます。
- **aaa accounting network network2 start-stop group radius group tacacs+** コマンドで、「network2」というネットワークアカウントティング方式リストを定義します。これにより、PPPを使用してシリアル回線上でRADIUSアカウントティングサービス（この場合、特定のイベントに対する開始レコードと終了レコード）を使用するよう指定されます。RADIUSサーバーが応答に失敗すると、アカウントティングサービスはTACACS+サーバーによって処理されます。
- **username** コマンドはユーザ名とパスワードを定義します。これらの情報は、PPPパスワード認証プロトコル（PAP）の発信元身元確認に使用されます。
- **tacacs server** コマンドはTACACS+サーバーホストの名前を定義します。
- **key** コマンドは、ネットワークアクセスサーバーとTACACS+サーバーホストの間の共有秘密テキスト文字列を定義します。
- **radius server** コマンドはRADIUSサーバーホストの名前を定義します。
- **key** コマンドは、ネットワークアクセスサーバーとRADIUSサーバーホストの間の共有秘密テキスト文字列を定義します。
- **interface group-async** コマンドは、非同期インターフェイスグループを選択して定義します。
- **group-range** コマンドは、インターフェイスグループ内のメンバ非同期インターフェイスを定義します。
- **encapsulation ppp** コマンドは、指定のインターフェイスに使用されるカプセル化方式としてPPPを設定します。
- **ppp authentication chap dialins** コマンドは、PPP認証方式としてチャレンジハンドシェイク認証プロトコル（CHAP）を選択し、指定したインターフェイスに「dialins」方式リストを適用します。
- **ppp authorization network1** コマンドによって、blue1ネットワーク許可方式リストが、指定したインターフェイスに適用されます。
- **ppp accounting network2** コマンドによって、red1ネットワークアカウントティング方式リストが、指定したインターフェイスに適用されます。

- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからライン コンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselect ppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるように Cisco IOS XE ソフトウェアを設定します。
- **autoselect during-login** コマンドを使用すると、Return キーを押さずにユーザ名およびパスワードのプロンプトが表示されます。ユーザがログインすると、autoselect 機能（この場合は PPP）が開始します。
- **login authentication admins** コマンドは、ログイン認証に admins 方式リストを適用します。
- **modem dialin** コマンドは、選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。

show accounting コマンドを使用すると、前述の設定に関する出力が次のように生成されます。

```
Active Accounted actions on tty1, User username2 Priv 1
Task ID 5, Network Accounting record, 00:00:52 Elapsed
task_id=5 service=ppp protocol=ip address=10.0.0.98
```

次の表に、前述の出力に含まれるフィールドについて説明します。

表 4: **show accounting** のフィールドの説明

フィールド	説明
Active Accounted actions on	ユーザがログインに使用する端末回線またはインターフェイス名
User	ユーザの ID。
Priv	ユーザの特権レベル。
Task ID	各アカウントングセッションの固有識別情報
Accounting Record	アカウントングセッションタイプ
Elapsed	このセッションタイプの期間 (hh:mm:ss)
attribute=value	このアカウントングセッションに関連付けられている AV ペア

例：AAA リソース アカウントングの設定

次に、リソース失敗終了アカウントング、および開始 - 終了レコード機能のリソース アカウントングを設定する例を示します。

```
!Enable AAA on your network access server.
Device(config)# aaa new-model
!Enable authentication at login and list the AOL string name to use for login
authentication.
Device(config)# aaa authentication login AOL group radius local
!Enable authentication for ppp and list the default method to use for PPP authentication.
Device(config)# aaa authentication ppp default group radius local
```

```

!Enable authorization for all exec sessions and list the AOL string name to use for
authorization.
Device(config)# aaa authorization exec AOL group radius if-authenticated
!Enable authorization for all network-related service requests and list the default
method
to use for all network-related authorizations.
Device(config)# aaa authorization network default group radius if-authenticated
!Enable accounting for all exec sessions and list the default method to use for all
start-stop
accounting services.
Device(config)# aaa accounting exec default start-stop group radius
!Enable accounting for all network-related service requests and list the default method
to use
for all start-stop accounting services.
Device(config)# aaa accounting network default start-stop group radius
!Enable failure stop accounting.
Device(config)# aaa accounting resource default stop-failure group radius
!Enable resource accounting for start-stop records.
Device(config)# aaa accounting resource default start-stop group radius

```

例：AAA ブロードキャスト アカウントティングの設定

次に、グローバル **aaa accounting** コマンドを使用して、ブロードキャストアカウントティングを有効にする例を示します。

```

Device> enable
Device# configure terminal
Device(config)# aaa group server radius isp
Device(config-sg-radius)# server 10.0.0.1
Device(config-sg-radius)# server 10.0.0.2
Device(config-sg-radius)# exit
Device(config)# aaa group server tacacs+ isp_customer
Device config-sg-tacacs+)# server 172.0.0.1
Device config-sg-tacacs+)# exit
Device(config)# aaa accounting network default start-stop broadcast group isp group
isp_customer
Device(config)# tacacs server server1
Device(config-server-tacacs)# address ipv4 172.0.0.1
Device(config-server-tacacs)# key key2
Device(config-server-tacacs)# end

```

broadcast キーワードによって、ネットワーク接続に関する「開始」および「終了」アカウントティングレコードが、グループ **isp** ではサーバー 10.0.0.1 に、グループ **isp_customer** ではサーバー 172.0.0.1 に同時送信されます。サーバ 10.0.0.1 が使用できなくなると、サーバ 10.0.0.2 へのフェールオーバーが行われます。サーバ 172.0.0.1 が使用できなくなっても、グループ **isp_customer** にはバックアップサーバが設定されていないため、フェールオーバーは行われません。

例：DNIS による AAA ブロードキャスト アカウントティングの設定

次に、グローバル **aaa dnis map accounting network** コマンドを使用して、DNIS ごとのブロードキャストアカウントティングを有効にする例を示します。

```

Device> enable
Device# configure terminal
Device(config)# aaa group server radius isp
Device(config-sg-radius)# server 10.0.0.1

```

例：AAA セッション MIB

```
Device(config-sg-radius)# server 10.0.0.2
Device(config-sg-radius)# exit
Device(config)# aaa group server tacacs+ isp_customer
Device config-sg-tacacs+)# server 172.0.0.1
Device config-sg-tacacs+)# exit
Device(config)# aaa dnis map enable
Device(config)# aaa dnis map 7777 accounting network start-stop broadcast group isp group
isp_customer
Device(config)# tacacs server server1
Device(config-server-tacacs)# address ipv4 172.0.0.1
Device(config-server-tacacs)# key key_2
Device(config-server-tacacs)# end
```

broadcast キーワードによって、DNIS 番号 7777 のネットワーク接続コールに関する「開始」および「終了」アカウントティングレコードが、グループ **isp** ではサーバー 10.0.0.1 に、グループ **isp_customer** ではサーバー 172.0.0.1 に同時送信されます。サーバ 10.0.0.1 が使用できなくなると、サーバ 10.0.0.2 へのフェールオーバーが行われます。サーバ 172.0.0.1 が使用できなくなっても、グループ **isp_customer** にはバックアップサーバが設定されていないため、フェールオーバーは行われません。

例：AAA セッション MIB

次に、AAA セッション MIB 機能を設定して、PPP ユーザの認証済みクライアント接続を解除する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication ppp default group radius
Device(config)# aaa authorization network default group radius
Device(config)# aaa accounting network default start-stop group radius
Device(config)# aaa session-mib disconnect
Device(config)# end
```

アカウントティングの設定に関するその他の参考資料

ここでは、アカウントティングの設定機能に関する関連資料について説明します。

MIB

MIB	MIB のリンク
<ul style="list-style-type: none"> • CISCO-AAA-SESSION-MIB 	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、および機能セットの 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

シスコのテクニカル サポート

説明	リンク
<p>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。</p> <p>お使いの製品のセキュリティ情報や技術情報入手するために、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。</p> <p>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。</p>	<p>http://www.cisco.com/en/US/support/index.html</p>

アカウントティングの設定の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	AAA ブロードキャスト アカウンティング	AAA ブロードキャスト アカウンティングを有効にすると、アカウンティング情報を複数の AAA サーバーに同時に送信できます。つまり、アカウンティング情報を1つまた複数の AAA サーバーに同時にブロードキャストすることが可能です。
Cisco IOS XE Everest 16.5.1a	AAA セッション MIB	ユーザーが AAA セッション MIB 機能を使用すると、SNMP を使用して自身の認証済みクライアント接続をモニターおよび終了できます。
Cisco IOS XE Everest 16.5.1a	接続アカウンティング	接続アカウンティングは、Telnet、ローカルエリアトランスポート、TN3270、Packet Assembler/disassembler (PAD)、rlogin など、ネットワークアクセスサーバーからのアウトバウンド接続すべてに関する情報を提供します。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	AAA 中間アカウントティング	AAA 中間アカウントティングにより、レポートする必要がある新しいアカウントティング情報が発生するたびに、または定期的に、アカウントティングサーバーに中間アカウントティングレコードを送信できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。

翻訳について

このドキュメントは、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。