「Configuring Accounting」

AAA アカウンティング機能を使用すると、ユーザがアクセスするサービス、およびユーザ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 サーバから TACACS+ または RADIUS セキュリティ サーバ（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、アカウンティング レコードの形式でユーザ アクティビティがレポートされます。各アカウンティング レコードにはアカウンティングの 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。

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、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

アカウン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 **aaanew-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。

アカウンティングの設定の制約事項

- アカウンティング情報は、最大 4 台の AAA サーバにのみ同時送信できます。
- Service Selection Gateway（SSG）システムの場合、**aaa accounting network broadcast** コマンドを実行すると、**start-stop** アカウンティング レコードのみがブロードキャストされます。**ssg accounting interval** コマンドを使用して中間アカウンティング レコードを設定する場合、中間アカウンティング レコードは、設定したデフォルト RADIUS サーバにのみ送信されます。

アカウンティングの設定に関する情報

アカウンティングの方式指定リスト

認証および認可方式リストと同様に、アカウンティングの方式リストには、アカウン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ティング方式でアカウン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ティングが失敗した場合（つまり、セキュリティ サーバからユーザ アクセスの拒否応答が返される場合）、アカウンティング プロセスは停止し、その他のアカウンティング方式は試行されません。

アカウンティング方式リストは、要求されるアカウン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出力します。
- **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 アカウンティングは、名前付きアカウンティング リストを使用しません。システム アカウンティングのデフォルト リストだけを定義できます。

この場合も、名前付き方式リストが作成されると、指定したアカウンティング タイプのアカウンティング方式のリストが定義されます。

アカウン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 LDAP、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 で RADIUS サーバのグループを構成します。T1 と T2 で TACACS+ サーバのグループを構成します。

サーバ グループを使用して、設定したサーバ ホストのサブセットを指定し、特定のサービスに使用します。たとえば、サーバ グループを使用すると、R1 および R2 を 1 つのサーバ グループとして定義し、T1 および T2 を別のサーバ グループとして定義できます。R1 と T1 を方式リストに指定することや、R2 と T2 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、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、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（認可など）に設定されている場合、設定されている 2 番めのホスト 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。この場合、最初のホスト エントリがアカウンティング サービスを提供できなかった場合、ネットワーク アクセス サーバは同じ装置上でアカウンティング サービス用に設定されている 2 番めのホスト エントリを試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

AAA アカウンティング方式

Cisco IOS ソフトウェアはアカウンティングについて次の 2 つの方式をサポートします。

- TACACS+：ネットワーク アクセス サーバは、アカウンティング 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。各アカウンティング レコードは、アカウンティング 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、アカウンティング 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。各アカウンティング レコードは、アカウンティング 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） CSCuc32663 では、パスワードおよびアカウンティング 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。

アカウンティング レコードの種類

最小限のアカウンティングの場合、**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 アカウンティング通知を送信するよう、指定した方式（**RADIUS**または **TACACS+**）に指示します。詳細なアカウンティ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ティング通知、そのイベントの終了時には修理用アカウンティ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ティング 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。

AAA アカウンティング方式

Cisco IOS ソフトウェアはアカウンティングについて次の 2 つの方式をサポートします。

- TACACS+：ネットワーク アクセス サーバは、アカウンティング 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。各アカウンティング レコードは、アカウンティング 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、アカウンティング 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。各アカウンティング レコードは、アカウンティング 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） CSCuc32663 では、パスワードおよびアカウンティング 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。

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-Identifier = "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-Identifier = "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-Identifier = "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     update
   task_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     update
   task_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 04:06:53 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 アカウンティング

コマンド アカウンティングは、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 アカウンティング 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 03:46:47 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 03:47:17 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 アカウンティングをサポートしていません。

接続アカウンティング

接続アカウンティングは、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-Identifier = "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-Identifier = "172.16.25.15"
```

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

```
Wed Jun 27 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 03:48:46 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 03:53:06 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ティングのオン/オフ時）に関する情報を提供します。

次のアカウンティング レコードは、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 レコード 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。

次のアカウンティング レコードは、AAAアカウン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
```

システム リソースを測定する追加のタスクについては、他の Cisco IOS ソフトウェア コンフィギュレーション ガイドを参照してください。たとえば、IP アカウンティング タスクについては、『*Cisco IOS Application Services Configuration Guide*』の「Configuring IP Services」を参照してください。

リソース アカウンティング

シスコが採用しているAAAアカウンティングでは、ユーザ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。

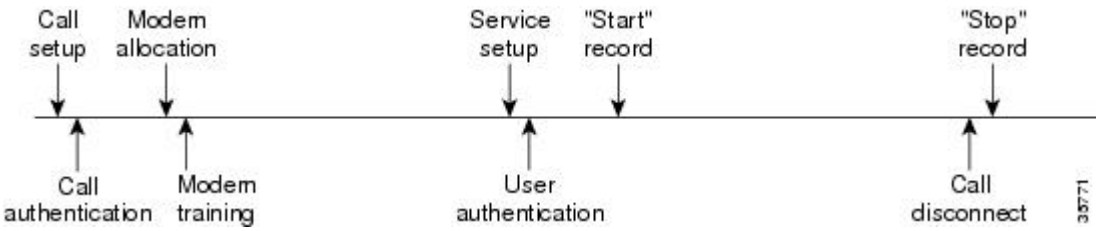
AAA リソース失敗終了アカウンティング

AAA リソース失敗終了アカウンティングの前には、コール設定シーケンスのユーザ認証段階に到達できなかったコールについて、アカウンティング 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、ユーザ認証に到達しなかったコールの「終了」アカウンティング 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。

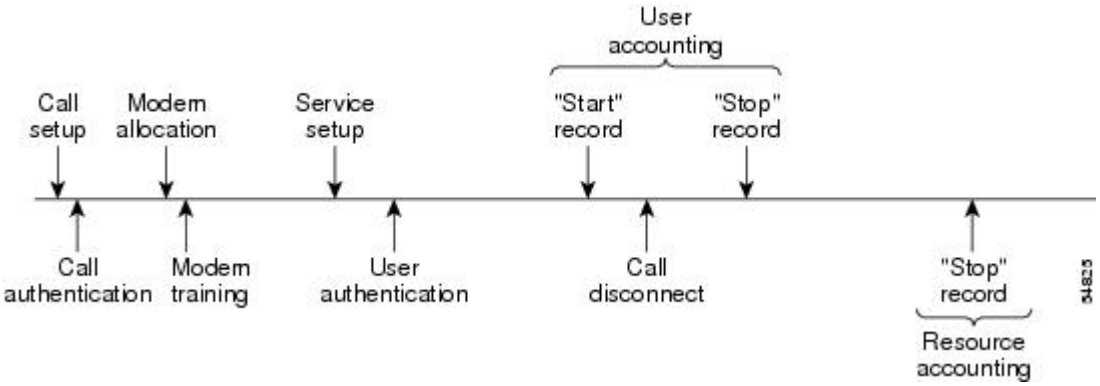
次の図に、通常のコール フローで、AAA リソース失敗終了アカウンティングを有効にしていないコール シーケンスを示します。

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ティング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

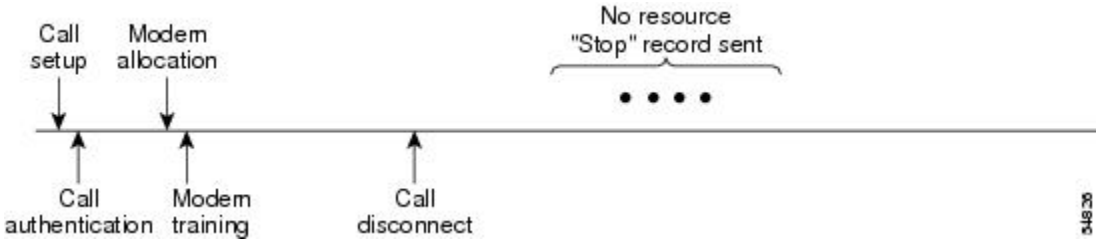


次の図に、ユーザ認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウンティングを有効にしたコール設定シーケンスを示します。

図 *3:* ユーザ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

次の図に、ユーザ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ティング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ティング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



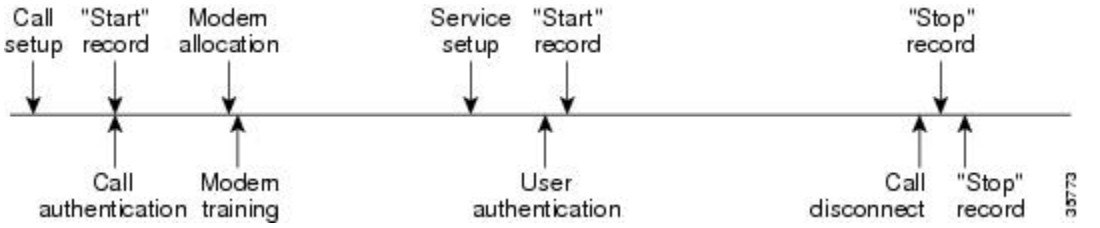
開始 - 終了レコードの AAA リソース アカウンティング

開始 - 終了レコードの AAA リソース アカウンティングは、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、アカウンティング 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。個別のユーザ認証「開始 - 終了」アカウンティング レコードが、ユーザ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



VRRS アカウンティング

Virtual Router Redundancy Service（VRRS）はマルチクライアント情報の抽象化機能を備え、First Hop Redundancy Protocol（FHRP）と登録済みクライアント間に管理サービスを提供しています。VRRS マルチクライアント サービスは、複数の FHRP を抽象化し、FHRP の状態の理想的なビューを提供することで、FHRPプロトコルとの一貫したインターフェイスを提供します。VRRS はデータの更新を管理しています。また、関連するクライアントを 1 か所で登録し、名前付きの FHRP グループまたはすべての登録済み FHRP グループに関する更新を受信できます。

VRRS アカウンティング プラグイン

VRRS アカウンティング プラグインには、VRRS グループの状態が遷移したときに RADIUS サーバに更新情報を提供する、設定可能な AAA 方式リスト メカニズムが用意されています。VRRS アカウンティング プラグインは、既存の AAA システム アカウンティング メッセージの拡張です。VRRS アカウンティング プラグインには、accounting-on および accounting-off メッセージと、RADIUS アカウンティング メッセージで設定済みの VRRS 名を送信する追加のベンダー固有属性（VSA）が用意されています。VRRS 名を設定するには、インターフェイス コンフィギュレーション モードで **vrrp name** コマンドを使用します。

VRRS アカウンティング プラグインには、VRRS グループの状態が遷移したときに RADIUS サーバに更新情報を提供する、設定可能な AAA 方式リスト メカニズムが用意されています。

VRRS アカウンティング プラグインは、既存の AAA システム アカウンティング メッセージの拡張です。VRRS アカウンティング プラグインには、accounting-on および accounting-off メッセージと、RADIUS アカウンティング メッセージで設定済みの VRRS 名を送信する追加のベンダー固有属性（VSA）が用意されています。VRRS 名を設定するには、インターフェイス コンフィギュレーション モードで **vrrp name** コマンドを使用します。VRRS グループがマスター状態に遷移すると、VRRS アカウンティング プラグインは accounting-on メッセージを RADIUS に送信します。また、VRRS グループがマスター状態から遷移すると、accounting-off メッセージを送信します。

次の RADIUS 属性は、デフォルトで VRRS アカウンティング メッセージに含まれます。

- 属性 4（NAS-IP-Address）
- 属性 26（Cisco VSA Type 1、VRRS Name）
- 属性 40（Acct-Status-Type）
- 属性 41（Acct-Delay-Time）
- 属性 44（Acct-Session-Id）

VRRS がマスター状態から遷移した場合のアカウンティング メッセージは、すべての PPPoE アカウンティングがその VRRS の一部であるセッションに関するメッセージを停止した後に送信されます。

AAA アカウンティングの強化

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（**showradiusstatistics** 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）

（注） このコマンドがサポートされるのは、Cisco AS5300 および Cisco AS5800 ユニバーサル アクセス サーバ プラットフォームだけです。

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 *1 : SNMP* エンドユーザ データ オブジェクト

SessionId	AAA アカウンティング 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、このアカウンティング 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 *2 : 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

アカウンティ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ティング機能をモニタします。

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

手順の概要

1. **enable**
2. **configure terminal**
3. **aaaaccounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [*method1* [*method2...*]]
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*
5. 次のいずれかを実行します。
   - **accounting** {**arap** | **commands** *level* | **connection** | **exec**} {**default** | *list-name*}
   - **pppaccounting**{**default** | *list-name*}
6. Device(config-line)# **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**aaaaccounting** {**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`	アカウンティング方式リストを作成し、アカウンティングを有効にします。引数 *list-name* 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*	アカウン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

	コマンドまたはアクション	目的
	例： `Device(config)# line aux line1`	アカウン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。
ステップ 5	次のいずれかを実行します。 • **accounting** {**arap** | **commands** *level* | **connection** | **exec**} {**default** | *list-name*} • **pppaccounting**{**default** | *list-name*} 例： `Device(config-line)# accounting arap default`	1 つの回線または複数回線にアカウンティング方式リストを適用します。 または 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ティング方式リストを適用します。
ステップ 6	Device(config-line)# **end** 例： `Device(config-line)# end`	（任意）ライン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

RADIUS システム アカウンティングの設定

このタスクを実行して、グローバル RADIUS サーバで RADIUS システム アカウンティングを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaanew-model**
4. **radius-serveraccountingsystemhost-config**
5. **aaagroupserverradius***server-name*
6. **server-private** {*host-name* | *ip-address*} **key** {[**0** *server-key* | **7** *server-key*] *server-key*
7. **accountingsystemhost-config**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `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	**configure terminal** 例：	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
	`Device# configure terminal`	
ステップ 3	**aaanew-model** 例： `Device(config)# aaa new-model`	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。
ステップ 4	**radius-serveraccountingsystemhost-config** 例： `Device(config)# radius-server accounting system host-config`	RADIUS サーバの追加および削除のために、デバイスからシステム アカウンティング レコードを送信できるようにします。
ステップ 5	**aaagroupserverradius***server-name* 例： `Device(config)# aaa group server radius radgroup1`	RADIUS サーバを追加し、server-group コンフィギュレーション モードを開始します。 • *server-name* 引数には、RADIUS サーバ グループ名を指定します。
ステップ 6	**server-private** {*host-name* | *ip-address*} **key** {[**0** *server-key* | **7** *server-key*] *server-key* 例： `Device(config-sg-radius)# server-private 172.16.1.11 key cisco`	RADIUS サーのホスト名または IP アドレスと、非表示のサーバ キーを入力します。 • （任意）**0** を伴った *server-key* 引数により、暗号化されていない（クリアテキストの）非表示のサーバ キーが後に続くことを指定します。 • （任意）**7** を伴った *server-key* 引数により、暗号化された非表示のサーバ キーが後に続くことを指定します。 • *server-key* 引数は、非表示のサーバ キーを指定します。*server-key* 引数の前に **0** も **7** も付いていない場合、サーバ キーは暗号化されません。 （注） **server-private** コマンドが設定されると、RADIUS システム アカウンティングが有効になります。
ステップ 7	**accountingsystemhost-config** 例： `Device(config-sg-radius)# accounting system host-config`	プライベート サーバ ホストの追加または削除時に、システム アカウンティング レコードの生成をイネーブルにします。
ステップ 8	**end** 例：	サーバ グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-sg-radius)# end`	

ヌル ユーザ名セッション時のアカウンティング レコード生成の抑制

AAA アカウンティ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ティング 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、**aaaauthenticationlogin** *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、アカウンティング 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
`Device(config)# aaa accounting suppress null-username`	ユーザ名文字列がヌルのユーザについて、アカウンティング レコードが生成されないようにします。

中間アカウンティング レコードの生成

アカウンティング サーバに定期的な中間アカウンティング 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
`Device(config)# aaa accounting update [newinfo] [periodic] number`	アカウンティング サーバに送信される定期的中間アカウンティング レコードをイネーブルにします。

aaaaccountingupdatecommand 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中間アカウンティング レコードを発行します。キーワードとして **newinfo** を使用した場合は、レポートすべき新しいアカウンティング情報が発生するたびに、中間アカウンティング レコードがアカウンティング 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、中間アカウンティング レコードが定期的に送信されます。中間アカウンティング レコードには、中間アカウンティング 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ティ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、**aaaaccountingupdateperiodic** 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。

失敗したログインまたはセッションに対するアカウンティングレコードの生成

AAA アカウンティングをアクティブにすると、Cisco IOS ソフトウェアは、ログイン認証に失敗したシステム ユーザや、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システム ユーザには、アカウンティング 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について、アカウンティ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	目的
`Device(config)# aa 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。
`Device(config)# aaa accounting send stop-record always`	開始レコードが送信済みかどうかに関係なく、認証、許可、アカウンティング（AAA）終了レコードを送信します。

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

PPP ユーザが EXEC ターミナル セッションを開始する場合、EXEC 終了レコードの前に生成する NETWORK レコードを指定できます。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 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。アカウンティング 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 セッションのアカウンティング 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	目的
`Device(config)# aaa accounting nested`	ネットワーク アカウンティング レコードをネストします。

AAA リソース失敗終了アカウンティングの設定

リソース失敗終了アカウン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
`Device(config)# aaa accounting resource` *method-list* **stop-failure group** *server-group*	ユーザ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。 （注） この機能を設定する前に、アカウンティングを設定するための前提条件 （2 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 サーバ上で SNMP を有効にしてください。

開始 - 終了レコードの AAA リソース アカウンティングの設定

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
`Device(config)# aaa accounting resource` *method-list* **start-stop group** *server-group*	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。 （注） この機能を設定する前に、アカウンティングを設定するための前提条件 （2 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 サーバ上で SNMP を有効にしてください。

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 アカウンティ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 accounting** コマンドを使用します。

コマンド	目的
`Device(config)# aaa accounting {system | network | exec | connection | commands` *level*`} {default |` *list-name*`} {start-stop | stop-only | none} [broadcast]` *method1* `[`*method2*`...]`	複数の AAA サーバに対するアカウンティング 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。

DNIS による AAA ブロードキャスト アカウンティングの設定

DNIS による AAA ブロードキャスト アカウンティ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
`Device(config)# aaa dnis map dnis-number accounting network [start-stop | stop-only | none] [broadcast] method1 [method2...]`	DNIS によるアカウン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。 複数の AAA サーバに対するアカウンティング 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。

AAA セッション MIB の設定

次のタスクは、次の AAA セッション MIB 機能の設定よりも前に実行する必要があります。

- SNMP を設定します。
- AAA を設定します。
- RADIUS または TACACS+ サーバの特性を定義します。

（注） SNMP を多用すると、全体のシステム パフォーマンスに影響が出る可能性があります。そのため、この機能を使用するときに、通常のネットワーク管理パフォーマンスを考慮する必要があります。

AAA セッション MIB を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Device (config)# **aaasession-mibdisconnect**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device (config)# **aaasession-mibdisconnect**	SNMP を使用して、認証済みクライアント接続をモニタおよび終了します。

	コマンドまたはアクション	目的
		コールを終了するには、**disconnect** キーワードを使用する必要があります。

VRRS アカウンティングの設定

次のタスクを実行して、AAA アカウンティング メッセージを AAA サーバに送信するように Virtual Router Redundancy Service（VRRS）を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaaaccountingvrrs** {**default** | *list-name*} **start-stop** *method1* [*method2...*]
4. **aaaattributelist** *list-name*
5. **attributetype** *name value* [**service** *service*] [**protocol** *protocol*][**mandatory**][**tag** *tag-value*]
6. **exit**
7. **vrrs** *vrrs-group-name*
8. **accountingdelay** *seconds*
9. **accountingmethod** {**default** | *accounting-method-list*}
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `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	**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	**aaaaccountingvrrs** {**default**	*list-name*} **start-stop** *method1* [*method2...*] 例： `Device(config)# aaa accounting vrrs default start-stop`	VRRS の AAA アカウンティングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**aaaattributelist** *list-name* 例： `Device(config)# aaa attribute list list1`	デバイス上で AAA 属性リストをローカルに定義し、属性リスト コンフィギュレーション モードを開始します。
ステップ 5	**attributetype** *name value* [**service** *service*] [**protocol** *protocol*][**mandatory**][**tag** *tag-value*] 例： `Device(config-attr-list)# attribute type example 1`	属性リストへ追加される属性タイプをデバイス上でローカルに定義します。
ステップ 6	**exit** 例： `Device(config-attr-list)# exit`	属性リスト コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**vrrs** *vrrs-group-name* 例： `Device(config)# vrrs vrrs1`	（任意）VRRS グループを定義し、VRRS グループのパラメータを設定し、VRRS コンフィギュレーション モードを開始します。
ステップ 8	**accountingdelay** *seconds* 例： `Device(config-vrrs)# accounting delay 10`	（任意）accounting-off メッセージを VRRS に送信する際の遅延時間を指定します。
ステップ 9	**accountingmethod** {**default** | *accounting-method-list*} 例： `Device(config-vrrs)# accounting method default`	（任意）VRRS グループの VRRS アカウンティングをイネーブルにします。
ステップ 10	**end** 例： `Device(config-vrrs)# end`	VRRS 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。

AAA サーバが到達不能な場合のデバイスとのセッションの確立

AAA サーバが到達不能の場合に、デバイスとの間にコンソールまたは Telnet 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	目的
`Device(config)# no aaa accounting system guarantee-first`	**aaa accounting system guarantee-first** コマンドは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。 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、**noaaaaccountingsystemguarantee-first** コマンドを使用できます。

（注） **noaaaaccountingsystemguarantee-first** コマンドを入力することがコンソールまたは Telnet セッションを開始できる唯一の条件というわけではありません。たとえば、特権EXECセッションが TACACS+ によって認証され、TACACS+ サーバが到達不能の場合、セッションは開始できません。

アカウンティングのモニタリング

RADIUS または TACACS+ アカウンティングの場合、特定の **show** コマンドは存在しません。現在ログインしているユーザに関する情報を表示するアカウンティング 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	目的
`Device# show accounting`	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。

アカウンティングのトラブルシューティング

アカウンティング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	目的
`Device# 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。

アカウンティングの設定例

名前付き方式リストの設定例

次に、RADIUS サーバから AAA サービスを提供するために Cisco AS5200（AAA および RADIUS セキュリティ サーバとの通信で有効）を設定する例を示します。RADIUS サーバ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、アカウンティング サービスは TACACS+ サーバによって処理されます。

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network blue1 group radius local
aaa accounting network red1 start-stop group radius group tacacs+
username root password ALongPassword
tacacs-server host 172.31.255.0
tacacs-server key goaway
radius-server host 172.16.2.7
radius-server key myRaDiUSpassWoRd
interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication chap dialins
 ppp authorization blue1
 ppp accounting red1
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaanew-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。
- **aaaauthenticationloginadminslocal** コマンドは、ログイン認証に方式リスト「admins」を定義します。
- **aaaauthenticationpppdialinsgroupradiuslocal** コマンドで、最初に RADIUS 認証を示す認証方式リスト「dialins」を定義します。次に、（RADIUS サーバが応答しない場合）PPP を使用するシリアル回線にはローカル認証が使用されます。
- **aaaauthorizationnetworkblue1groupradiuslocal** コマンドで、「blue1」というネットワーク認可方式リストを定義します。これにより、PPP を使用するシリアル回線で RADIUS 認可を使用するよう指定されます。RADIUS サーバ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。
- **aaaaccountingnetworkred1start-stopgroupradiusgrouptacacs+** コマンドで、「red1」というネットワーク アカウンティング方式リストを定義します。これにより、PPP を使用するシリアル回線で RADIUS アカウンティング 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 サーバが応答に失敗すると、アカウンティングサービスは TACACS+ サーバ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）認証での発信元の身元確認に使用されます。
- **tacacs-serverhost** コマンドは TACACS+ サーバ ホストの名前を定義します。
- **tacacs-serverkey** コマンドは、ネットワーク アクセス サーバと TACACS+ サーバ ホストの間の共有秘密テキスト文字列を定義します。
- **radius-serverhost** コマンドは RADIUS サーバ ホストの名前を定義します。
- **radius-serverkey** コマンドは、ネットワーク アクセス サーバと RADIUS サーバ ホストの間の共有秘密テキスト文字列を定義します。
- **interfacegroup-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 グループのメンバの非同期インターフェイスを定義します。
- **encapsulationppp** コマンドは指定のインターフェイスに使用される PPP をカプセル化方式として設定します。
- **pppauthenticationchapdialins** 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、特定のインターフェイスに「dialins」方式リストを適用します。
- **pppauthorizationblue1** コマンドによって、blue1 ネットワーク認可方式リストが、指定したインターフェイスに適用されます。
- **pppaccountingred1** コマンドによって、red1 ネットワーク アカウン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。
- **autoselectppp** 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 ソフトウェアを設定します。
- **autoselectduring-login** コマンドを使用して、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を表示します。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。
- **loginauthenticationadmins** 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。

showaccounting 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 *3 : 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。
タスク ID	各アカウンティング セッションの固有識別情報
Accounting record	アカウンティング 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	このアカウンティング セッションに関連付けられている AV ペア

AAA リソース アカウンティングの設定例

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

```
!Enable AAA on your network access server.
aaa new-model
!Enable authentication at login and list the AOL string name to use for login
authentication.
aaa authentication login AOL group radius local
!Enable authentication for ppp and list the default method to use for PPP authentication.
aaa authentication ppp default group radius local
!Enable authorization for all exec sessions and list the AOL string name to use for
authorization.
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.
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.
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.
aaa accounting network default start-stop group radius
!Enable failure stop accounting.
aaa accounting resource default stop-failure group radius
!Enable resource accounting for start-stop records.
aaa accounting resource default start-stop group radius
```

AAA ブロードキャスト アカウンティングの設定例

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 アカウンティングを有効にする例を示します。

```
aaa group server radius isp
 server 10.0.0.1
 server 10.0.0.2
aaa group server tacacs+ isp_customer
 server 172.0.0.1
aaa accounting network default start-stop broadcast group isp group isp_customer
radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key1
tacacs-server host 172.0.0.1 key key2
```

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」アカウンティング レコードが、グループ isp ではサーバ 10.0.0.1 に、グループ isp_customer ではサーバ 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。

DNIS による AAA ブロードキャスト アカウンティングの設定例

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

```
aaa group server radius isp
 server 10.0.0.1
 server 10.0.0.2
aaa group server tacacs+ isp_customer
 server 172.0.0.1
aaa dnis map enable
aaa dnis map 7777 accounting network start-stop broadcast group isp group isp_customer
radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key_1
tacacs-server host 172.0.0.1 key key_2
```

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」アカウンティング レコードが、グループ isp ではサーバ 10.0.0.1 に、グループ isp_customer ではサーバ 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。

AAA セッション MIB の例

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。

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
aaa session-mib disconnect
```

VRRS アカウンティングの設定例

次に、AAA アカウンティング メッセージを AAA に送信するように VRRS を設定する例を示します。

```
Router# configure terminal
Router(config)# aaa accounting vrrs vrrp-mlist-1 start-stop group radius
Router(config)# aaa attribute list vrrp-1-attr
Router(config-attr-list)# attribute type account-delay 10
Router(config-attr-list)# exit
Router(config)# vrrs vrrp-group-1
Router(config-vrrs)# accounting delay 10
Router(config-vrrs)# accounting method vrrp-mlist-1
Router(config-vrrs)# exit
```

アカウンティングの設定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』
Cisco セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

RFC

RFC	Title
RFC 2903	「*Generic AAA Architecture*」
RFC 2904	「*AAA Authorization Framework*」

RFC	Title
RFC 2906	「*AAA Authorization Requirements*」
RFC 2989	「*Criteria for Evaluating AAA Protocols for Network Access*」

シスコのテクニカル サポート

説明	Link
★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

アカウンティングの設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリース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 *4:* アカウンティングの設定に関する機能情報

機能名	リリース	機能情報
AAA ブロードキャスト アカウンティング	Cisco IOS 15.2(1)E	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 サーバに同時にブロードキャストすることが可能です。

機能名	リリース	機能情報
開始 - 終了レコードの AAA リソース アカウンティング	Cisco IOS 15.2(1)E	開始 - 終了レコードの AAA リソース アカウンティングは、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、アカウンティング 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するために使用できます。
AAA セッション MIB	Cisco IOS 15.2(1)E	ユーザが 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 アカウンティング情報に直接関連付けることができます。
AAA：IPv6 アカウンティングの遅延の強化	Cisco IOS 15.2(1)E	VRRS はマルチクライアント情報の抽象化機能を備え、First Hop Redundancy Protocol（FHRP）と登録済みクライアント間に管理サービスを提供しています。