アカウンティングの設定

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。

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 **aaa new-model** コマンドを使用します。
- RADIUS または TACACS+ 許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。

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名前付き方式リスト

認証および許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。

アカウンティングの方式リストは、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。

アカウンティングの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、この固有の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。同じ RADIUS サーバ上の異なる 2 つのホストエントリに同じサービス（たとえば許可）を設定した場合、2 番目に設定したホストエントリは、最初に設定した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 番目のホスト 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） 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 タイプ

この項では、さまざまな AAA アカウンティングタイプについて説明します。

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
updatetask_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
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
```

リソース アカウンティング

Cisco IOS 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。

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 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（**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 *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

	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：	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	**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* 例： `Device(config)# line aux line1`	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 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*} • **ppp accounting**{**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	**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、特権 EXEC 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

	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 new-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-server accounting system host-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	**aaa group server radius** *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** と *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** と *server-key* 引数により、暗号化されている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

	コマンドまたはアクション	目的
		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**	**accounting system host-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： `Device(config-sg-radius)# end`	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。

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、**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な中間アカウンティング 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の中間アカウン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、**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。

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)# 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。
`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、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。

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。

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*...]	

コマンド	目的
	複数の **A** サバに対するアカウンティングレコードの送信をイネブルにします。各グループの最初のサバ

コマンド	目的
	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セカンダリサーバが

コマンド	目的
	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

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

	コマンドまたはアクション	目的
ステップ 1	Device (config)# **aaa session-mib disconnect**	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

	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 vrrs** {**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。
ステップ 4	**aaa attribute list** *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	**attribute type** *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	**accounting delay** *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。

	コマンドまたはアクション	目的
ステップ 9	**accounting method** {**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`	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ために、**no aaa accounting system guarantee-first** コマンドを使用できます。

（注） **no aaa accounting system guarantee-first** コマンドの入力は、コンソールセッションまたは Telnet セッションを起動可能にするための唯一の条件ではありません。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

例：名前付き方式リストの設定

次に、RADIUS サーバから AAA サービスを提供するためにデバイス（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、認証情報と許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。

```
Device> enable
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 blue1 group radius local
Device(config)# aaa accounting network red1 start-stop group radius group tacacs+
Device(config)# username root password ALongPassword
Device(config)# tacacs-server host 172.31.255.0
Device(config)# tacacs-server key goaway
Device(config)# radius-server host 172.16.2.7
Device(config)# radius-server key myRaDiUSpassWoRd
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 blue1
Device(config-if)# ppp accounting red1
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 blue1 group radius local** コマンドで、「blue1」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サーバが応答に失敗すると、ローカル ネットワークの許可が実行されます。
- **aaa accounting network red1 start-stop group radius group tacacs+** 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 を使用してシリアル回線上で 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）の発信元身元確認に使用されます。
- **tacacs-server host** コマンドは TACACS+ サーバ ホストの名前を定義します。
- **tacacs-server key** 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-server host** コマンドは RADIUS サーバ ホストの名前を定義します。
- **radius-server key** 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。
- **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、特定のインターフェイスに「dialins」方式リストを適用します。
- **ppp authorization blue1** 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 red1** 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。
- **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 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。

```
Device# show accounting

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
Task 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

例：AAA リソース アカウンティングの設定

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
```

例：AAA ブロードキャスト アカウンティングの設定

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)# radius-server host 10.0.0.1
Device(config)# radius-server host 10.0.0.2
Device(config)# radius-server key key1
Device(config)# tacacs-server host 172.0.0.1 key key2
Device(config)# 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。

例：DNIS による AAA ブロードキャスト アカウンティングの設定

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

```
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-radius)# server 172.0.0.1
Device(config-sg-radius)# 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)# radius-server host 10.0.0.1
Device(config)# radius-server host 10.0.0.2
Device(config)# radius-server key key_1
Device(config)# tacacs-server host 172.0.0.1 key key_2
Device(config)# 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。

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
```

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。

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

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
この章で使用するコマンドの完全な構文および使用方法の詳細。	Consolidated Platform Command Reference, Cisco IOS Release 15.2(7)Ex (Catalyst 1000 Switches)

RFC

RFC	タイトル
RFC 2903	「*Generic AAA Architecture*」
RFC 2904	「*AAA Authorization Framework*」
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	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

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 リリース 15.2(7)E1	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 リリース 15.2(7)E1	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。

機能名	リリース	機能情報
AAA セッション MIB	Cisco IOS リリース 15.2(7)E1	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 リリース 15.2(7)E1	VRRS はマルチクライアント情報の抽象化機能を備え、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。