



アカウントティングの設定

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、アカウント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)
- [アカウントティングの設定方法](#) (13 ページ)
- [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。

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 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。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トティング 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トティング 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 アカウントティング方式

Cisco IOS ソフトウェアはアカウント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、アカウント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。各アカウントティングレコードは、アカウントティング 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、アカウント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。各アカウントティングレコードは、アカウントティング 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トティングログは、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。

アカウントティング レコードの種類

最小限のアカウントティングの場合、**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ト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。詳細なアカウント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トティング通知、そのイベントの終了時には修理用アカウント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ト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 アカウントティング タイプ

この項では、さまざまな AAA アカウント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-Identifer = "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-Identifer = "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-Identifer = "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 04:00:35 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) アカウントング 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 04:30:52 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-Identififier = "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-Identififier = "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-Identififier = "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 アカウントING 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ING 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ING

コマンドアカウントING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ING 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ING 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、コマンドアカウントティングをサポートしていません。

接続アカウントティング

接続アカウントティングは、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-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+ 接続アカウント記録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 接続アカウント記録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トティングのオン/オフ時）に関する情報を提供します。

次のアカウントティング 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。

次のアカウントティング 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 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、このアカウント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

アカウント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トティング機能をモニタします。

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	<p>enable</p> <p>例 :</p> <pre>Device> enable</pre>	<p>特権 EXEC モードを有効にします。</p> <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	<p>configure terminal</p> <p>例 :</p> <pre>Device# configure terminal</pre>	<p>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。</p>
ステップ 3	<p>aaa accounting {system network exec connection commands level} {default list-name} {start-stop stop-only none} [method1 [method2...]]</p> <p>例 :</p> <pre>Device(config)# aaa accounting system default start-stop</pre>	<p>アカウントング方式リストを作成し、アカウント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。</p>
ステップ 4	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> line [aux console tty vty] line-number [ending-line-number] interface interface-type interface-number <p>例 :</p> <pre>Device(config)# line aux line1</pre>	<p>アカウント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。</p> <p>または</p> <p>アカウント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。</p>
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>

RADIUS システム アカウントティングの設定

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 アカウント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。 <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。
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トティング 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。 <ul style="list-style-type: none"> <i>server-name</i> 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 サーバのホスト名または IP アドレスと、非表示のサーバ キーを入力します。 <ul style="list-style-type: none"> (任意) 0 と <i>server-key</i> 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 <i>server-key</i> 引数により、暗号化されている非表示のサーバ

	コマンドまたはアクション	目的
		<p>バキーが後に続くことを指定します。</p> <ul style="list-style-type: none"> • <i>server-key</i> 引数は、非表示のサーバキーを指定します。<i>server-key</i> 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。 <p>(注) server-private コマンドが設定されると、RADIUS システムアカウントングが有効になります。</p>
ステップ 7	<p>accounting system host-config</p> <p>例 :</p> <pre>Device(config-sg-radius)# accounting system host-config</pre>	<p>プライベートサーバホストの追加または削除時に、システムアカウントングレコードの生成をイネーブルにします。</p>
ステップ 8	<p>end</p> <p>例 :</p> <pre>Device(config-sg-radius)# end</pre>	<p>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。</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に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>	<p>ユーザ名文字列がヌルのユーザについて、アカウントングレコードが生成されないようにします。</p>

中間アカウントングレコードの生成

アカウントングサーバに定期的な中間アカウント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] <i>number</i>	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ション済み 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。中間アカウントティングレコードには、中間アカウント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ト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トティングレコードの生成

AAA アカウント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、アカウント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、アカウント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トING 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と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。アカウントING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トING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 アカウントINGレコードをネストします。

AAA リソース失敗終了アカウントINGの設定

リソース失敗終了アカウントING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 <i>method-list stop-failure group</i> <i>server-group</i>	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 アカウントINGの設定

開始 - 終了レコードのフル リソース アカウントING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>

AAA ブロードキャスト アカウントティングの設定

AAA ブロードキャスト アカウント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
<pre>Device(config)# aaa accounting {system network exec connection commands <i>level</i>} {default <i>list-name</i>} {start-stop stop-only none} [broadcast] <i>method1</i> [<i>method2...</i>]</pre>	

コマンド	目的
	複数の A サバに対してするアカウント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
	に対しアカウントINGグレ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エラーメッセージが

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 アカウントティングの設定

AAA ブロードキャストアカウント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
<pre>Device(config)# aaa dnis map dnis-number accounting network [start-stop stop-only none] [broadcast] method1 [method2...]</pre>	<p>DNIS によるアカウント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 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。

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	<p>最初のレコードとしてシステムアカウントティングを保証します（これが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。</p>



- (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。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	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。

アカウントティングのトラブルシューティング

アカウント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。

アカウントिंग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、アカウントングサービスは 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 server1
Device(config-tacacs-server)# address IPv4 172.31.255.0
Device(config-tacacs-server)# key goaway
Device(config-tacacs-server)# exit
Device(config)# radius server server2
Device(config-radius-server)# address IPv4 172.16.2.7
Device(config-radius-server)# key myRaDiUSpassWoRd
Device(config-radius-server)# 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 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、アカウント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** コマンドは TACACS+ サーバホスト名を定義し、**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** コマンドは RADIUS サーバホスト名を定義し、**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ー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.
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)# radius server server
Device(config-radius-server)# address IPv4 10.0.0.1
Device(config-radius-server)# key key_1
Device(config-radius-server)# exit
Device(config)# radius server server
Device(config-radius-server)# address IPv4 10.0.0.2
Device(config-radius-server)# key key_1
Device(config-radius-server)# exit
Device(config)# tacacs server server1
Device(config-tacacs-server)# address IPv4 172.0.0.1
Device(config-tacacs-server)# key key2
Device(config-tacacs-server)# 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 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 単位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
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
```

例：AAA セッション MIB

```
Device(config)# radius server server
Device(config-radius-server)# address IPv4 10.0.0.1
Device(config-radius-server)# key key_1
Device(config-radius-server)# exit
Device(config)# radius server server
Device(config-radius-server)# address IPv4 10.0.0.2
Device(config-radius-server)# key key_1
Device(config-radius-server)# exit
Device(config)# tacacs server server
Device(config-tacacs-server)# address IPv4 172.0.0.1
Device(config-tacacs-server)# key key_2
Device(config-tacacs-server)# end
s
```

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
```

アカウント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。	<i>Consolidated Platform Command Reference, Cisco IOS Release 15.2(7)Ex (Catalyst Micro Switches)</i>

RFC

RFC	タイトル
<i>RFC 2903</i>	「 <i>Generic AAA Architecture</i> 」
<i>RFC 2904</i>	「 <i>AAA Authorization Framework</i> 」

RFC	タイトル
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
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 Release 15.2(7)E3k	アカウントティング (Accounting)	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。

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。

