CHAPTER 10

SNMP の設定

この章では、ユーザ、メッセージ暗号化、通知、TCP での認証などを含む SNMP を設定する方法を説明します。

ここでは、次の内容について説明します。

- 「SNMP に関する情報」（P.10-1）
- 「SNMP の前提条件」（P.10-5）
- 「SNMP の前提条件」（P.10-5）
- 「注意事項および制約事項」（P.10-5）
- 「SNMP の設定」（P.10-5）
- 「SNMP の設定確認」（P.10-14）
- 「SNMP の設定例」（P.10-14）
- 「デフォルト設定」（P.10-15）
- 「その他の関連資料」（P.10-15）

SNMP に関する情報

Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）は、SNMP マネージャとエージェント間の通信用メッセージ フォーマットを提供する、アプリケーション レイヤ プロトコルです。SNMP はネットワーク デバイスの監視や管理に使用される、標準化されたフレームワークと共通言語を提供します。

ここでは、次の内容について説明します。

- 「SNMP 機能の概要」（P.10-1）
- 「SNMP 通知」（P.10-2）
- 「SNMPv3」（P.10-2）
- 「ハイ アベイラビリティ」（P.10-5）

SNMP 機能の概要

SNMP フレームワークは、3 つの部分からなります。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスの動作を制御および監視するためのシステム。

- SNMP エージェント：管理デバイス内部のソフトウェア コンポーネントで、デバイスに関するデータを維持し、必要に応じてこれらのデータを管理システムに伝えます。Cisco Nexus 1000V はエージェントと MIB をサポートします。SNMP エージェントをイネーブルにするには、マネージャとエージェント間の関係を定義する必要があります。
- Managed Information Base（MIB; 管理情報ベース）：SNMP エージェント上の管理対象オブジェクトのコレクション。

SNMP は RFC 3411 ～ 3418 で定義されています。

（注）　SNMP セットはサポートされていません。

SNMPv1、SNMPv2c、および SNMPv3 です。SNMPv1 および SNMPv2c の両方により、コミュニティベースのセキュリティ形式の使用がサポートされています。

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を作成できるということです。これらの通知は、SNMP マネージャからの要求送信を必要としません。通知によって、不正なユーザ認証、再起動、接続の終了、ネイバー ルータとの接続切断、またはその他の重要イベントを示すことができます。

SNMP 通知は、トラップまたは応答要求として生成されます。トラップは、エージェントからホスト レシーバー テーブルで指定された SNMP マネージャに送信される、非同期の非確認応答メッセージです。応答要求は、SNMP エージェントから SNMP マネージャに送信される非同期メッセージで、マネージャは受信したという確認応答が必要です。

トラップの信頼性は、応答要求よりも低くなります。これは、SNMP マネージャがトラップを受信するときには、確認応答を送信しないためです。Cisco Nexus 1000V では、トラップを受信したかどうかを判断できません。応答要求を受信した場合、SNMP マネージャは SNMP 応答 Protocol Data Unit（PDU; プロトコル データ ユニット）を使用して、メッセージを確認します。応答がなかった場合、Cisco Nexus 1000V はもう一度、応答要求を送信します。

複数のホスト レシーバーに通知を送信するように、Cisco Nexus 1000V を設定できます。ホスト レシーバーの詳細については、「SNMP 通知レシーバーの設定」（P.10-8）を参照してください。

SNMPv3

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。SNMPv3 が提供するセキュリティ機能は、次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：有効な送信元からのメッセージであることを判別します。
- 暗号化：パケット内容のスクランブルによって、不正な送信元で判読できないようにします。

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方を提供します。セキュリティ モデルは、ユーザおよびユーザに与えられている役割に合わせて設定される認証方式です。セキュリティ レベルは、セキュリティ モデル内で許可されるセキュリティ レベルです。セキュリティ モデルとセキュリティ レベルのコンビネーションによって、SNMP パケットを取り扱うときに使用するセキュリティ メカニズムが決まります。

ここでは、次の内容について説明します。

- 「SNMPv1、v2、v3 のセキュリティ モデルおよびセキュリティ レベル」（P.10-3）

- 「User-Based Security Model」（P.10-3）
- 「CLI および SNMP ユーザの同期」（P.10-4）
- 「グループベースの SNMP アクセス」（P.10-5）

SNMPv1、v2、v3 のセキュリティ モデルおよびセキュリティ レベル

セキュリティ レベルによって、SNMP メッセージを開示から保護する必要があるか、メッセージの認証が必要かどうかが決定されます。セキュリティ モデル内に存在する各種セキュリティ レベルは、次のとおりです。

- noAuthNoPriv：認証も暗号化も行わないセキュリティ レベル
- authNoPriv：認証は行うが暗号化は行わないセキュリティ レベル
- authPriv：認証と暗号化の両方を行うセキュリティ レベル

SNMPv1、SNMPv2c、SNMPv3 の 3 つのセキュリティ モデルが利用できます。セキュリティ レベルと組み合わされたセキュリティ モデルによって、SNMP メッセージの処理時に適用されるセキュリティ メカニズムが決まります。

表 10-1 に、セキュリティ モデルとセキュリティ レベルのコンビネーションが何を意味するかを示します。

表 10-1　SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	動作
v1	noAuthNoPriv	コミュニティ ストリング	なし	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	なし	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	ユーザ名	なし	ユーザ名の照合を使用して認証します。
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	なし	Hash-Based Message Authentication Code（HMAC）Message Digest 5（MD5）アルゴリズムまたは HMAC Secure Hash Algorithm（SHA）に基づいて認証します。
v3	authPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC MD5 または HMAC SHA アルゴリズムに基づいて認証します。Cipher Block Chaining（CBC; 暗号ブロック連鎖）DES（DES-56）規格に基づいた認証に加え、Data Encryption Standard（DES; データ暗号規格）56 ビット暗号化を行います。

User-Based Security Model

SNMPv3 User-Based Security Model（USM）は SNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されず、データ シーケンスが悪意なく起こり得る範囲を超えて変更されていないことを保証します。

- メッセージ起点認証：ユーザのために受信したデータの起点として主張されたアイデンティティが確認されていることを保証します。
- メッセージの機密性：不正な個人、エンティティ、またはプロセスに対して、情報が使用可能になったり開示されたりしていないことを保証します。

SNMPv3 は、設定ユーザによる管理操作だけを許可し、SNMP メッセージを暗号化します。

Cisco Nexus 1000V では、SNMPv3 に対応する 2 種類の認証プロトコルを使用します。

- HMAC-MD5-96 認証プロトコル
- HMAC-SHA-96 認証プロトコル

Cisco Nexus 1000V は、SNMPv3 メッセージ暗号化用プライバシー プロトコルの 1 つとして、Advanced Encryption Standard（AES）を使用し、RFC 3826 に準拠します。

priv オプションで、SNMP セキュリティ暗号化に DES を使用するか、それとも 128 ビット AES 暗号化を使用するかを選択できます。**priv** オプションと **aes-128** トークンを組み合わせた場合は、このプライバシー パスワードが 128 ビットの AES 鍵を作成するためのものであることを意味します。AES priv パスワードは、8 文字以上の長さにできます。パスフレーズをクリア テキストで指定する場合は、大文字と小文字を区別して、最大 64 文字の英数字を指定できます。ローカライズした鍵を使用する場合は、130 文字まで指定できます。

（注） 外部 AAA（認証、認可、アカウンティング）サーバを使用する SNMPv3 動作の場合は、外部 AAA サーバ上のユーザ コンフィギュレーションで、プライバシー プロトコルとして AES を使用する必要があります。

CLI および SNMP ユーザの同期

SNMPv3 のユーザ管理は、Access Authentication and Accounting（AAA）サーバ レベルで集中させることができます。この集中ユーザ管理によって、Cisco Nexus 1000V の SNMP エージェントは AAA サーバのユーザ認証サービスを活用できます。ユーザ認証が確認されると、SNMP PDU がさらに処理されます。また、ユーザ グループ名の保管に AAA サーバも使用されます。SNMP ではグループ名を使用して、スイッチでローカルに使用できるアクセス/ロール ポリシーを適用します。

ユーザ グループ、ロール、またはパスワードの設定を変更すると、SNMP と AAA の両方について、データベースの同期が図られます。

Cisco Nexus 1000V では次のように、ユーザ設定を同期させます。

- **snmp-server user** コマンドで指定された認証パスフレーズが CLI ユーザのパスワードになります
- **username** コマンドで指定されたパスワードが SNMP ユーザの認証およびプライバシーパスフレーズになります。
- SNMP または CLI を使用してユーザを削除すると、SNMP と CLI の両方でユーザが削除されます。
- ユーザとロール（役割）間のマッピング変更は、SNMP と CLI で同期します。
- CLI から行ったロール変更（削除または変更）は、SNMP と同期します。

（注） パスフレーズまたはパスワードをローカライズした鍵または暗号形式で設定した場合、Cisco Nexus 1000V はパスワードを同期させません。

Cisco NX-OS はデフォルトで、同期したユーザ設定を 60 分間維持します。このデフォルト値の変更方法については、「AAA 同期時間の変更」（P.10-14）を参照してください。

グループベースの SNMP アクセス

（注）　*グループ*が業界全体で使用されている標準 SNMP 用語なので、この SNMP の項では、ロールのことをグループと言います。

SNMP のアクセス権は、グループ別に編成されます。SNMP の各グループは、CLI でのロールと同様です。各グループは読み取りアクセス権または読み取りと書き込みアクセス権を指定して定義します。

自分のユーザ名を作成すると、エージェントとの通信を開始し、管理者に自分のロールを設定してもらい、そのロールに自分を追加してもらうことができます。

ハイ アベイラビリティ

SNMP ではステートレス リスタートがサポートされています。リブートまたはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションを適用します。

SNMP の前提条件

SNMP の前提条件は、次のとおりです。

注意事項および制約事項

SNMP に関する設定時の注意事項および制約事項は、次のとおりです。

- 一部の SNMP MIB に対する読み取り専用アクセスがサポートされています。詳細については次の URL にアクセスして、Cisco NX-OS の MIB サポート リストを参照してください。

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

SNMP の設定

ここでは、次の内容について説明します。

- 「SNMP ユーザの設定」（P.10-6）
- 「SNMP メッセージ暗号化の強制」（P.10-7）
- 「複数のロールへの SNMPv3 ユーザの割り当て」（P.10-8）
- 「SNMP コミュニティの作成」（P.10-8）
- 「SNMP 通知レシーバーの設定」（P.10-8）
- 「通知ターゲット ユーザの設定」（P.10-9）
- 「SNMP 通知のイネーブル化」（P.10-10）
- 「インターフェイスに関する linkUp/linkDown 通知のディセーブル化」（P.10-11）
- 「TCP による SNMP のワンタイム認証のイネーブル化」（P.10-12）
- 「SNMP スイッチのコンタクトおよびロケーション情報の指定」（P.10-12）

- 「SNMP のディセーブル化」（P.10-13）
- 「AAA 同期時間の変更」（P.10-14）

（注）　この機能に対応する Cisco NX-OS コマンドは、Cisco IOS で使用されているコマンドと異なる場合があるので注意してください。

SNMP ユーザの設定

この手順を使用して、SNMP のユーザを設定します。

始める前に

- EXEC モードで CLI にログインします。

手順の概要

1. **config t**
2. **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]]
3. **show snmp user**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`switch(config)#`
		グローバル コンフィギュレーション モードに切り替えます。

ステップ 2	**snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]] **例：** `switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh`	認証およびプライバシー パラメータを指定して、SNMP ユーザを設定します。パスフレーズには最大 64 文字の英数字を使用できます。大文字と小文字を区別します。**localizekey** キーワードを使用する場合は、パスフレーズに大文字と小文字を区別した英数字を 130 文字まで使用できます。 engineID の形式は、12 桁のコロンで区切った 10 進数字です。

	コマンド	目的
ステップ 3	**show snmp user** **例：** `switch(config-callhome)# show snmp user`	（任意）1 つ以上の SNMP ユーザに関する情報を表示します。
ステップ 4	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行中のコンフィギュレーションをスタートアップ コンフィギュレーションにコピーし、リブートと再起動を行って、永久的に保存します。

SNMP のコンタクトおよびロケーション情報を設定する例を示します。

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
```

SNMP メッセージ暗号化の強制

着信要求の認証または暗号化を求めるように、SNMP を設定できます。デフォルトでは、SNMP エージェントは認証および暗号化を行わないでも SNMPv3 メッセージを受け付けます。プライバシーを強化する場合、Cisco Nexus 1000V は noAuthoNoPriv または authNoPriv の securityLevel パラメータを使用している SNMPv3 PDU 要求に、authorizationError で応答します。

SNMP メッセージの暗号化をユーザに強制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server user *name* **enforcePriv** **例：** `switch(config)# snmp-server user Admin enforcePriv`	このユーザに SNMP メッセージの暗号化を強制します。

SNMP メッセージの暗号化をすべてのユーザに強制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server globalEnforcePriv **例：** `switch(config)# snmp-server globalEnforcePriv`	すべてのユーザに SNMP メッセージの暗号化を強制します。

複数のロールへの SNMPv3 ユーザの割り当て

SNMP ユーザの設定後、ユーザに複数のロールを割り当てることができます。

（注）　他のユーザにロールを割り当てることができるのは、network-admin ロールに属しているユーザだけです。

SNMP ユーザにロールを割り当てるには、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
snmp-server user *name group* **例：** `switch(config)# snmp-server user Admin superuser`	この SNMP ユーザを設定済みのユーザ ルールに関連付けます。

SNMP コミュニティの作成

SNMPv1 または SNMPv2c に対応する SNMP コミュニティを作成できます。

SNMP コミュニティ ストリングを作成するには、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
snmp-server community *name group* {**ro** | **rw**} **例：** `switch(config)# snmp-server community public ro`	SNMP コミュニティ ストリングを作成します。

SNMP 通知レシーバーの設定

複数のホスト レシーバーに対して SNMP 通知を作成するように、Cisco Nexus 1000V を設定できます。

SNMPv1 トラップのホスト レシーバーを設定するには、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。

コマンド	目的
snmp-server host *ip-address* **traps version 1** *community* [**udp_port** *number*] **例：** `switch(config)# snmp-server host 192.0.2.1 traps version 1 public`	SNMPv1 トラップのホスト レシーバーを設定します。コミュニティには最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。

SNMPv2c トラップまたは応答要求のホスト レシーバーを設定するには、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。

コマンド	目的
snmp-server host *ip-address* {**traps** | **informs**} **version 2c** *community* [**udp_port** *number*] **例：** `switch(config)# snmp-server host 192.0.2.1 informs version 2c public`	SNMPv2c トラップまたは応答要求のホスト レシーバーを設定します。コミュニティには最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。

SNMPv3 トラップまたは応答要求のホスト レシーバーを設定するには、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。

コマンド	目的
snmp-server host *ip-address* {**traps** | **informs**} **version 3** {**auth** | **noauth** | **priv**} *username* [**udp_port** *number*] **例：** `switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS`	SNMPv2c トラップまたは応答要求のホスト レシーバーを設定します。ユーザ名には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。

（注） SNMP マネージャは SNMPv3 メッセージを認証して解読するために、Cisco Nexus 1000V デバイスの SNMP engineID に基づいてユーザ クレデンシャル（authKey/PrivKey）を調べる必要があります。

通知ターゲット ユーザの設定

通知ホスト レシーバーに SNMPv3 応答要求通知を送信するには、デバイス上で通知ターゲット ユーザを設定する必要があります。

Cisco Nexus 1000V は通知ターゲット ユーザのクレデンシャルを使用して、設定された通知ホスト レシーバーへの SNMPv3 応答要求通知メッセージを暗号化します。

（注） 受信した INFORM PDU を認証して解読する場合、Cisco Nexus 1000V で設定されているのと同じ、応答要求を認証して解読するユーザ クレデンシャルが通知ホスト レシーバーに必要です。

通知ターゲット ユーザを設定するには、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。

コマンド	目的
snmp-server user *name* [**auth** {md5 | sha} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] **例：** `switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID 00:00:00:63:00:01:00:10:20:15:10:03`	通知ホスト レシーバーの engineID を指定して、通知ターゲット ユーザを設定します。engineID の形式は、12 桁のコロンで区切った 10 進数字です。

SNMP 通知のイネーブル化

通知をイネーブルまたはディセーブルにできます。通知の名前を指定しなかった場合、Cisco Nexus 1000V はすべての通知をイネーブルにします。

表 10-2 には、Cisco Nexus 1000V MIB に関する通知をイネーブルにする、CLI コマンドを示します。

（注）　**snmp-server enable traps** コマンドを使用すると、設定されている通知ホスト レシーバーに応じて、トラップおよび応答要求の両方がイネーブルになります。

表 10-2　SNMP 通知のイネーブル化

MIB	関連コマンド
すべての通知	**snmp-server enable traps**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa**
ENITY-MIB	**snmp-server enable traps entity**
CISCO-ENTITY-FRU-CONTROL-MIB	**snmp-server enable traps entity fru**
CISCO-LICENSE-MGR-MIB	**snmp-server enable traps license**
IF-MIB	**snmp-server enable traps link**
CISCO-PSM-MIB	**snmp-server enable traps port-security**
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**

ライセンス通知は、デフォルトでイネーブルです。その他の通知はすべて、デフォルトでディセーブルです。

指定した通知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
snmp-server enable traps **例：** `switch(config)# snmp-server enable traps`	すべての SNMP 通知をイネーブルにします。
snmp-server enable traps aaa [**server-state-change**] **例：** `switch(config)# snmp-server enable traps aaa`	AAA SNMP 通知をイネーブルにします。
snmp-server enable traps entity [**fru**] **例：** `switch(config)# snmp-server enable traps entity`	ENTITY-MIB SNMP 通知をイネーブルにします。
snmp-server enable traps license **例：** `switch(config)# snmp-server enable traps license`	ライセンス SNMP 通知をイネーブルにします。
snmp-server enable traps link **例：** `switch(config)# snmp-server enable traps link`	リンク SNMP 通知をイネーブルにします。
snmp-server enable traps port-security **例：** `switch(config)# snmp-server enable traps port-security`	ポート セキュリティ SNMP 通知をイネーブルにします。
snmp-server enable traps snmp [**authentication**] **例：** `switch(config)# snmp-server enable traps snmp`	SNMP エージェント通知をイネーブルにします。

インターフェイスに関する linkUp/linkDown 通知のディセーブル化

個々のインターフェイスに関する linkUp および linkDown 通知をディセーブルにできます。これにより、フラッピング インターフェイス（アップとダウン間の移行を繰り返しているインターフェイス）に関する通知を制限できます。

インターフェイスに関する linkUp/linkDown 通知をディセーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
no snmp trap link-status **例：** `switch(config-if)# no snmp trap link-status`	インターフェイスの SNMP リンクステート トラップをディセーブルにします。このコマンドは、デフォルトでイネーブルにされています。

TCP による SNMP のワンタイム認証のイネーブル化

TCP セッションでの 1 回限りの SNMP 認証をイネーブルにできます。

TCP による SNMP のワンタイム認証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
snmp-server tcp-session [**auth**] **例：** `switch(config)# snmp-server tcp-session`	TCP セッションでの 1 回限りの SNMP 認証をイネーブルにします。デフォルトはディセーブルです。

SNMP スイッチのコンタクトおよびロケーション情報の指定

32 文字までの長さで（スペースを含まない）のスイッチ コンタクト情報を指定できます。さらに、スイッチ ロケーションを指定できます。

始める前に

- EXEC モードで CLI にログインします。

手順の概要

1. **config t**
2. **snmp-server contact** *name*
3. **snmp-server location** *name*
4. **show snmp**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`switch(config)#`
		グローバル コンフィギュレーション モードに切り替えます。

ステップ 2	**snmp-server contact** *name* **例：** `switch(config)# snmp-server contact Admin`	SNMP コンタクト名として sysContact を設定します。
ステップ 3	**snmp-server location** *name* **例：** `switch(config)# snmp-server location Lab-7`	SNMP ロケーションとして sysLocation を設定します。
ステップ 4	**show snmp** **例：** `switch(config)# show snmp`	（任意）1 つ以上の宛先プロファイルに関する情報を表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行中のコンフィギュレーションをスタートアップ コンフィギュレーションにコピーし、リブートと再起動を行って、永久的に保存します。

SNMP のコンタクトおよびロケーション情報を設定する例を示します。

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp contact Admin
switch(config)# snmp location Lab-7
```

SNMP のディセーブル化

デバイス上で SNMP プロトコルをディセーブルにできます。

SNMP プロトコルをディセーブルにするには、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
no snmp-server protocol enable **例：** `switch(config)# no snmp-server protocol enable`	SNMP プロトコルをディセーブルにします。このコマンドは、デフォルトでイネーブルにされています。

AAA 同期時間の変更

同期したユーザ設定を Cisco NX-OS に維持させる時間の長さを変更できます。

AAA 同期時間を変更するには、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
snmp-server aaa-user cache-timeout *seconds* **例：** `switch(config)# snmp-server aaa-user cache-timeout 1200.`	ローカル キャッシュで AAA 同期ユーザ設定を維持する時間を設定します。値の範囲は 1 ～ 86400 秒です。デフォルト値は 3600 です。

SNMP の設定確認

SNMP 設定を表示するには、次のコマンドを使用します。

コマンド	目的
show running-config snmp [**all**]	SNMP の実行コンフィギュレーションを表示します。
show snmp	SNMP ステータスを表示します。
show snmp community	SNMP コミュニティ ストリングを表示します。
show snmp context	SNMP コンテキスト マッピングを表示します。
show snmp engineID	SNMP engineID を表示します。
show snmp group	SNMP ロールを表示します。
show snmp session	SNMP セッションを表示します。
show snmp trap	SNMP 通知がイネーブルなのかディセーブルなのかを表示します。
show snmp user	SNMPv3 ユーザを表示します。

SNMP の設定例

Blue VRF を使用してある通知ホスト レシーバーに Cisco linkUp/linkDown 通知を送信するように設定し、Admin と NMS という 2 つの SNMP ユーザを定義する例を示します。

```
config t
 snmp-server contact Admin@company.com
 snmp-server user Admin auth sha abcd1234 priv abcdefgh
 snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID
00:00:00:63:00:01:00:22:32:15:10:03
 snmp-server host 192.0.2.1 informs version 3 auth NMS
 snmp-server host 192.0.2.1 use-vrf Blue
 snmp-server enable traps link cisco
```

デフォルト設定

表 10-3 に、SNMP パラメータのデフォルト設定をリスト表示します。

表 10-3　デフォルトの SNMP パラメータ

パラメータ	デフォルト
license notifications	イネーブル

その他の関連資料

SNMP の実装に関連する詳細情報については、次の項を参照してください。

- 「標準規格」（P.10-15）
- 「MIB」（P.10-15）

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

MIB

MIB	MIB のリンク
• SNMP-COMMUNITY-MIB • SNMP-FRAMEWORK-MIB • SNMP-NOTIFICATION-MIB • SNMP-TARGET-MIB • SNMPv2-MIB	MIB を見つけてダウンロードするには、次の URL を参照してください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

SNMP 機能の履歴

表 10-4 に、この機能のリリース履歴をリスト表示します。

表 10-4　SNMP 機能の履歴

機能名	リリース	機能情報
SNMP	4.0	初回 Cisco Nexus 1000V 製品リリース