CHAPTER 12

Cisco Network Assistant による Catalyst 4500 シリーズ スイッチの設定

この章では、ワークステーション上に Network Assistant をインストールして、Catalyst 4500（または Catalyst 4900）シリーズ スイッチが Network Assistant と通信するように設定する方法について説明します （これまでの *Catalyst 4500 シリーズ スイッチ*という用語は、両方のスイッチ タイプを意味するように使用されています）。また、コミュニティおよびクラスタの作成方法についても説明します。Network Assistant は 2 つのテクノロジーを使用して、Catalyst 4500 シリーズ スイッチなどのネットワーク デバイスのグループを管理します。

Network Assistant は、無料のネットワーク管理ツールで、グラフィカル ユーザ インターフェイス（GUI）による Catalyst 4500 シリーズ スイッチの設定および管理を可能にします。Network Assistant は、セキュア環境および非セキュア環境の両方で稼働します。Network Assistant は、スタンドアロン デバイス、デバイス グループ、またはスイッチ グループ（コミュニティまたはクラスタ内）を、ご使用のイントラネットの任意の場所で管理します。Network Assistant を使用すると、コマンドを覚える必要がなく、複数の設定作業を実行できます。

（注） この章のスイッチ コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps5931/prod_installation_guides_list.html

この章の内容は、次のとおりです。

（注） Network Assistant は Cisco.com 上のオンライン ソフトウェア イメージとバンドルされていません。Network Assistant は、次の URL からダウンロードできます。

http://www.cisco.com/en/US/products/ps5931/index.html

（注）　Network Assistant のソフトウェアおよびハードウェア要件、インストール方法、起動方法、およびデバイスへの接続方法の詳細については、次の URL の『*Getting Started with Cisco Network Assistant*』を参照してください。

http://www.cisco.com/en/US/products/ps5931/prod_installation_guides_list.html

Network Assistant の関連機能およびデフォルト設定

表 1 に、Catalyst 4500 シリーズ スイッチの Network Assistant 関連の設定パラメータを示します。

表 1　Catalyst 4500 シリーズ スイッチの Network Assistant 関連の設定

機能	デフォルト値	推奨値
認証	ディセーブル	オプション
IP アドレス	コミュニティまたは検出オプションにより異なります。[1]	ユーザ選択可能
IP HTTP ポート番号	80	オプション[2]
IP HTTPS ポート番号	443	オプション[3]
IP HTTP サーバ	ディセーブル	イネーブル[4]
Cluster run	ディセーブル	イネーブル[5]

1. コミュニティのデバイス検出およびクラスタ コマンダには、スイッチごとに IP アドレスを設定する必要があります。
2. Network Assistant のポート番号と Catalyst 4500 シリーズ スイッチは一致させる必要があります。
3. デバイスのクラスタのこの値だけ、変更できます。Network Assistant のポート番号と Catalyst 4500 シリーズ スイッチは一致させる必要があります。値は、1024 より上の任意の非デフォルト番号に変更できます。
4. Network Assistant がデバイスにアクセスするのに必要です。
5. デバイスのクラスタを管理する場合にだけ、イネーブルです。

CLI コマンドの概要

表 2 に、Network Assistant 関連の CLI コマンドの概要を示します。

表 2　CLI コマンド

コマンド	機能
[no] cluster enable	クラスタに名前を付けます。
[no] cluster run	クラスタリングをイネーブルにします。 （注）　このコマンドは、クラスタリング専用です。
[no] ip http server	スイッチで HTTP を設定します。
[no] ip http port *port_number*	HTTP ポートを設定します。
[no] ip domain-name *domain_name*	スイッチ上でドメインを設定します。

表 2　CLI コマンド（続き）

コマンド	機能
[no] ip http secure-server	スイッチ上で HTTPS を設定して、イネーブルにします。
[no] ip http secure-port *port_number*	HTTPS ポートを設定します。
[no] ip http max-connections *connection_number*	HTTP サーバへの最大同時接続数を設定します。
[no] ip http timeout-policy idle *idle_time* **life** *life_time* **requests** *requests*	HTTPS ポートを設定します。 **idle** 値は 180 秒を推奨します。 **life** 値は 180 秒を推奨します。 許可できる **requests** の最大数は 25 を推奨します。
line vty	CNA が使用する追加の VTY を設定します。
show version	Cisco IOS Release を表示します。
show running-config	スイッチ設定を表示します。
vtp domain	VLAN を管理する VTP ドメインを作成します。
vtp mode	VLAN の VTP 管理に関する動作を設定します。

スイッチでの Network Assistant の設定

ここでは、次の内容について説明します。

- 「CNA から Catalyst 4500 へアクセスするのに必要な最小設定」（P.12-3）
- 「コミュニティを使用する必要がある場合の追加設定」（P.12-4）
- 「クラスタを使用する必要がある場合の追加設定」（P.12-4）

CNA から Catalyst 4500 へアクセスするのに必要な最小設定

デフォルトの設定を使用する場合は、Catalyst 4500 シリーズ スイッチにアクセスして、**ip http server**（HTTP 用）または **ip http secure-server**（HTTPS 用）グローバル コンフィギュレーション コマンドを入力します。

	コマンド	目的
ステップ 1	`Switch# 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 2	`Switch(config)# ip http server`
	or
	`Switch(config)# ip domain-name domain_name`
		（**HTTP の場合だけ**）スイッチ上で HTTP サーバをイネーブルにします。デフォルトでは、HTTP サーバはディセーブルに設定されています。
		スイッチでドメイン名をイネーブルにして、HTTPS を設定します。

ステップ 3	`Switch(config)# ip http secure-server`	スイッチ上で HTTPS サーバをイネーブルにします。デフォルトでは、HTTPS サーバはディセーブルに設定されています。

	コマンド	目的
ステップ 4	`Switch(config)# ip http max-connections connection_number`	HTTP サーバへの最大同時接続数を設定します。 *connection_number* は 16 を推奨します。
ステップ 5	`Switch(config)# ip http timeout-policy idle idle_time life life_time requests requests`	HTTPS ポートを設定します。 **idle** キーワードでは、接続がアイドル状態でいる最大時間数を指定します。**idle** 値は 180 秒を推奨します。 **life** キーワードでは、接続が確立してからオープンでいる最大時間数を指定します。**life** 値は 180 秒を推奨します。 **requests** キーワードでは、接続での最大要求数を指定します。許可できる **requests** の最大数は 25 を推奨します。
ステップ 6	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Switch# show running-config`	設定を確認します。

（注） クラスタリングがイネーブルの場合、コミュニティを設定する前にクラスタリングをディセーブルにします（表 2 を参照）。

コミュニティを使用する必要がある場合の追加設定

コミュニティを使用する場合は、スイッチごとに IP アドレスを定義します。

	コマンド	目的
ステップ 1	`Switch# configuration 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 2	`Switch(config)# interface {vlan vlan_ID | {fastethernet | gigabitethernet} slot/interface | Port-channel number}`	インターフェイスを選択します。
ステップ 3	`Switch(config-if)# ip address ip_address address_mask`	（任意）Catalyst 4500 シリーズに IP アドレスを割り当てます。 **（注）** スイッチがコミュニティの一部またはクラスタ コマンド スイッチの場合、この手順は必須です。スイッチがクラスタ メンバ候補の場合、この手順は任意です。
ステップ 4	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Switch# show running-config`	設定を確認します。

クラスタを使用する必要がある場合の追加設定

クラスタリングを使用する場合、デバイスごとに **cluster run** グローバル コンフィギュレーション コマンドを入力し、クラスタ コマンダで **ip address** インターフェイス コンフィギュレーション コマンドを入力します。

	コマンド	目的
ステップ 1	`Switch# configuration 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 2	`Switch(config)# cluster run`	クラスタリングをイネーブルにします。 （注）　クラスタの一部となる可能性のあるスイッチすべてでクラスタリングをイネーブルにします。
ステップ 3	`Switch(config)# cluster enable`	クラスタに名前を付けます。
ステップ 4	`Switch(config)# interface {vlan vlan_ID | {fastethernet | gigabitethernet} slot/interface | Port-channel number}`	インターフェイスを選択します。
ステップ 5	`Switch(config-if)# ip address ip_address address_mask`	（任意）Catalyst 4500 シリーズ スイッチのクラスタ マスターに IP アドレスを割り当てます。 （注）　スイッチがコミュニティの一部またはクラスタ コマンド スイッチの場合、この手順は必須です。スイッチがクラスタ メンバ候補の場合、この手順は任意です。
ステップ 6	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Switch# show running-config`	設定を確認します。

コミュニティを使用したネットワーク管理

ここでは、Network Assistant アプリケーションによる*デバイス*（Catalyst 4500 シリーズ スイッチ、ルータ、アクセス ポイント、および PIX ファイアウォールを含む）管理におけるコミュニティの使用方法について説明します。

コミュニティを使用してネットワーク内のスイッチを分類する場合、唯一の要件は HTTP サーバおよびスイッチごとの IP アドレスの設定です。

コミュニティ内のデバイスの総数は、20 以下になるようにします（最大 4 つの Catalyst 4500 シリーズ スイッチ（モジュラ式）、16 の Catalyst 2900/3500 または Catalyst 4948/4948-10GE スイッチ（非モジュラ式）、2 つのルータ、および 2 つの PIX ファイアウォールも含む）。

（注）　アクセス ポイントはデバイス制限から除外されました。現在、CNA が管理できるアクセス ポイント数に制限はありません。

（注）　**Add to Community** ダイアログにより、多数のデバイスが表示されますが、20 のデバイスしか選択できません。21 番めのデバイスを追加しようとすると、ダイアログは 21 番めのデバイスを表示して、不要なデバイスの選択が要求されます。

（注）　Network Assistant を使用してスイッチ コミュニティを設定する詳細な手順については、次の URL の『*Getting Started with Cisco Network Assistant*』を参照してください。

http://www.cisco.com/en/US/products/ps5931/prod_installation_guides_list.html

ここでは、コミュニティを作成する前に理解する必要がある注意事項、要件について説明します。ここでは、次の内容について説明します。

候補およびメンバの特性

候補は、IP アドレスを持ちますが、コミュニティには追加されていないネットワーク デバイスです。メンバは、現在コミュニティに含まれるネットワーク デバイスです。

コミュニティに加入するには、候補は次の要件を満たす必要があります。

- IP アドレスが指定されている。
- デバイスを自動検出する場合、Cisco Discovery Protocol（CDP）バージョン 2 がイネーブルに設定されていること（デフォルト）。
- HTTP（または HTTPS）がイネーブルであること。

（注）　クラスタ メンバはコミュニティに追加できますが、その逆はできません。

（注）　クラスタ コマンダがコミュニティに追加されても、クラスタのその他のメンバ デバイスは自動的に追加されません。クラスタ メンバを管理するには、個別にコミュニティに追加する必要があります。

候補およびメンバの自動検出

Network Assistant は、CDP を使用してネットワーク内の利用可能なデバイスのすべてを確認または検出し、コミュニティを形成します。起動デバイスの IP アドレスおよび HTTP（または HTTPS）プロトコルのポート番号から始めて、Network Assistant は CDP を使用して起動デバイスに隣接するコミュニティ候補のリストをコンパイルします。Network Assistant は、有効な IP アドレスを持つかぎり、複数のネットワークおよび VLAN 間で候補デバイスおよびメンバ デバイスを検出できます。

（注）　デフォルトでは、コミュニティ モードの Network Assistant は最大 4 ホップ先まで検出します。

ネットワーク デバイスが検出されるための要件のリストについては、「候補およびメンバの特性」（P.12-6）を参照してください。

（注）　Network Assistant により検出する場合は、候補、メンバ、またはネットワーク デバイスで CDP をディセーブルにしないでください。

（注）　PIX ファイアウォールは CDP をサポートしないため、[Topology] ビューにネイバーとして自動表示されません。[Create Community] または [Modify Community] ウィンドウを使用してコミュニティに追加した場合にだけ表示されます。PIX ファイアウォールと他のコミュニティ メンバとのリンクを確認するには、[Topology] ポップアップ メニューで [ADD Link] を選択して手動でリンクを追加する必要があります。

検出されたデバイスのリストを編集し、必要に応じてコミュニティに追加できます。デバイスがコミュニティに追加されるたびに、そのネイバーが検出され、候補デバイスのリストに追加されます。Network Assistant がデバイスを検出できない場合は、IP 管理アドレスにより手動で追加できます。

コミュニティ名

メンバ デバイスのリストにコミュニティの設定情報を適用すると、Network Assistant によりコミュニティの名前（または IP アドレス）の入力が要求されます。コミュニティを管理するには、まず名前を割り当てる必要があります。Network Assistant は、この名前をご使用の PC に保存します。

コミュニティ名には、0 ～ 9、a ～ z、および A ～ Z の文字と、文字間のスペースを使用できます。

（注）　クラスタには、IP アドレスによってだけ接続できます。名前を選択すると、常にそのコミュニティの名前となります。

ホスト名

起動デバイスまたはコミュニティ メンバには、ホスト名を割り当てる必要はありません。ただし、シスコではホスト名の割り当てを推奨しています。Network Assistant は、デフォルトでは割り当てません。検出されたデバイスにホスト名がある場合、Network Assistant はこのデバイスの情報を識別するために、IP アドレス、通信プロトコル、および指定されたプロトコル ポートとともにホスト名をご使用の PC に保存します。

パスワード

コミュニティ メンバとなるデバイスにはパスワードを割り当てる必要はありませんが、シスコではパスワードの割り当てを推奨しています。

コミュニティ メンバごとに別々のパスワードを割り当てることができます。

通信プロトコル

Network Assistant は、HTTP（または HTTPS）プロトコルを使用してネットワーク デバイスと通信します。候補デバイスの検出に CDP を使用すると、HTTP（または HTTPS）と通信しようとします。

Network Assistant のアクセス モード

Network Assistant がコミュニティまたはクラスタに接続されている場合、パスワードにより読み書きモードおよび読み出し専用モードの 2 つのモードが使用できます。

コミュニティ情報

Network Assistant は、すべてのコミュニティの設定情報および個別のデバイス情報（IP アドレス、ホスト名、通信プロトコルなど）をご使用のローカル PC に保存します。Network Assistant がコミュニティに接続するとき、ローカルに保存されたデータを使用してメンバ デバイスを再検出します。

別の PC を使用して既存のコミュニティを管理しようとすると、メンバ デバイスの情報は使用できません。再度コミュニティを作成し、これと同じメンバ デバイスを追加する必要があります。

デバイスの追加

コミュニティにメンバを追加するには、次の 3 つの方法があります。

1 つめの方法では、Network Assistant 上の [Devices Found] ウィンドウを使用して、検出したデバイスを新しいコミュニティに追加します。

a. [Devices Found] ウィンドウで、追加する候補デバイスを選択します。

複数の候補デバイスを追加するには、Ctrl キーを押して選択をするか、Shift キーを押して範囲の最初と最後のデバイスを選択します。

b. [Add] をクリックします。

2 つめの方法では、[Modify Community] ウィンドウを使用して、既存のコミュニティにデバイスを追加します。

a. [Application] > [Communities] を選択し、[Communities] ウィンドウを開きます。

b. [Communities] ウィンドウで、デバイスを追加するコミュニティ名を選択し、[Modify] をクリックします。

c. 手動で単一のデバイスを追加するには、[Modify Community] ウィンドウで所定のデバイスの IP アドレスを入力し、[Add] をクリックします。

d. 候補デバイスを検出するには、起動デバイスの IP アドレスを入力し、[Discover] をクリックします。

e. リストから候補デバイスを選択し、[Add] をクリックしてから、[OK] をクリックします。

複数の候補デバイスを追加するには、Ctrl キーを押して選択をするか、Shift キーを押して範囲の最初と最後のデバイスを選択します。

デバイスを追加する 3 つめの方法では、[Topology] ビューを使用します。

a. [Topology] ビューが表示されない場合は、機能バーから [View] ウィンドウ > [Topology] を選択します。

b. 候補アイコンを右クリックして、[Add to Community] を選択します。

候補はシアン、メンバはグリーンになります。複数の候補を追加するには、Ctrl キーを押して、追加する候補を左クリックします。

コミュニティに 20 のメンバが所属している場合、そのコミュニティでは [Add to Community] オプションは使用できません。この場合、新しいメンバを追加する前に 1 つのメンバを削除する必要があります。

（注）　コミュニティにログインしていて、他の CNA インスタンスからそのコミュニティを削除する場合、このコミュニティ セッションを終了しないかぎり、セッションを介してすべての設定を実行できます。セッションの終了（つまり、コミュニティの削除）後は、このコミュニティに接続できなくなります。

クラスタのコミュニティへの変換

Cluster Conversion ウィザードにより、クラスタをコミュニティに変換できます。変換が完了するとただちに、デバイス グループをコミュニティとして管理できます。コミュニティ管理の利点は、コミュニティ内のデバイスとの通信がクラスタ内のデバイスとの通信よりもセキュアである（複数のパスワードおよび HTTPS を介するため）ことです。さらに、デバイスのアベイラビリティは高く、メンバにできるデバイスの範囲も広くなります。

（注）　Cluster Conversion ウィザードでは、クラスタ定義は変更されません。そのため、デバイスをクラスタとしても管理できます。

Cluster Conversion ウィザードを開始するには、次の手順を実行します。

ステップ 1　Network Assistant を開始し、コマンダの IP アドレスを介して既存のクラスタに接続します。

ステップ 2　機能バーで、[Configure] > [Cluster] > [Cluster Conversion Wizard] をクリックします。

「Do you want to convert this cluster to a community?」（このクラスタをコミュニティに変換しますか）という質問が表示されます。

ステップ 3　[Yes] を選択して次に進むか、Cluster Conversion ウィザードを手動で立ち上げる場合は [No] を選択します。

[Yes] を選択すると、初期画面が表示され、クラスタ、コミュニティ、およびその利点に関する情報が提供されます。

次に、クラスタ内のデバイスを示す表が IP アドレスおよびサブネット マスクを持たないデバイスから表示されます。コミュニティのメンバとなるには、クラスタ内のすべてのデバイスで IP アドレスおよびサブネット マスクを持つ必要があることに注意してください。

（注）　デバイスに IP アドレスおよびサブネット マスクを持つインターフェイスが複数ある場合は、セルをクリックすると複数のインターフェイスが表示されます。最初に表示されたものとは異なるインターフェイスを選択できます。

ステップ 4　[IP Address] カラムでは、IP アドレスを持たない各デバイスの IP アドレスを入力します。

ステップ 5　[Subnet Mask] カラムでは、サブネット マスクを持たない各デバイスのセルをクリックし、サブネット マスクを選択します。

ステップ 6　コミュニティ名を入力します。

ステップ 7　変換を開始するには、[Finish] をクリックします。

変換が完了すると、Network Assistant が再開し、新しく作成されたコミュニティに自動的に接続します。

（注）　クラスタリングがイネーブルの場合、コミュニティを設定する前にクラスタリングをディセーブルにする必要があります（表 2 を参照）。

クラスタを使用したネットワーク管理

ここでは、クラスタリングを使用して、スタンドアロンの Network Assistant アプリケーションまたはコマンドライン インターフェイス（CLI）を使用する Catalyst 4500 シリーズ スイッチの作成および管理方法について説明します。

ネットワーク内のスイッチを分類するには、クラスタリングを使用できます。管理されるスイッチごとにクラスタ実行コマンドを入力する必要があります。主な利点は、1 つの IP アドレスで 16 のデバイスを管理できることです。

（注）　クラスタリングは、CNA 1.0 で使用される自動検出メカニズムです。

（注）　Network Assistant を使用してスイッチ クラスタを設定する詳細な手順については、次の URL の『*Getting Started with Cisco Network Assistant*』を参照してください。

http://www.cisco.com/en/US/products/ps5931/prod_installation_guides_list.html

ここでは、次の内容について説明します。

- 「スイッチ クラスタの概要」（P.12-10）
- 「CLI によるスイッチ クラスタの管理」（P.12-12）

スイッチ クラスタの概要

ここでは、次の内容について説明します。

- 「クラスタリングの概要」（P.12-10）
- 「クラスタ コマンド スイッチの特性」（P.12-11）
- 「候補スイッチおよびクラスタ メンバ スイッチの特性」（P.12-12）

クラスタリングの概要

*スイッチ クラスタ*は、最大 16 個の接続されたクラスタ対応 Catalyst スイッチで、単一エンティティとして管理されます。1 つの IP アドレスを介して異なる Catalyst 4500 シリーズ スイッチ プラットフォーム グループを設定およびトラブルシューティングできるように、クラスタのスイッチはスイッチ クラスタリング技術を使用します。

スイッチ クラスタを使用すると、スイッチの物理的なロケーションやプラットフォーム ファミリに関係なく、複数のスイッチの管理を簡略にします。

（注）　デフォルトでは、クラスタリング モードの Network Assistant は最大 7 ホップ先まで検出します。

スイッチ クラスタでは、1 つのスイッチは*クラスタ コマンダ スイッチ*になる必要があります。最大 15 個の残りのスイッチは*クラスタ メンバ スイッチ*になります。1 つのクラスタは、16 台以内のスイッチで構成する必要があります。クラスタ コマンド スイッチは、クラスタ メンバ スイッチの設定、管理、およびモニタを実行できる唯一のスイッチです。クラスタ メンバは、一度に 1 つのクラスタにしか所属できません。

（注） 必ずクラスタ コマンド スイッチとして Catalyst 4500 または 4948 シリーズ スイッチを選択してください。

クラスタ コマンド スイッチの特性

クラスタ コマンド スイッチは、次の要件を満たしている必要があります。

- Cisco IOS Release 12.2(20)EWA 以降を使用していること。
- IP アドレスが指定されている。
- Cisco Discovery Protocol（CDP）バージョン 2 がイネーブル（デフォルト）に設定されている。
- クラスタ対応ソフトウェアを使用し、クラスタリングがイネーブルであること。
- IP HTTP（または HTTPS）サーバがイネーブルであること。

（注） Catalyst 4500 シリーズ スイッチでは、HTTP および HTTPS はデフォルトでイネーブルに設定されていません。

- 16 本の VTY 回線があること。

（注） Catalyst 4500 シリーズ スイッチのデフォルトは 4 回線です。スイッチでの値が 16 になるよう設定します。

- 他のクラスタのクラスタ コマンド スイッチまたはクラスタ メンバ スイッチではない。

（注） ご使用のスイッチ クラスタに Catalyst 4500 シリーズ スイッチが含まれている場合、クラスタ コマンド スイッチも Catalyst 4500 シリーズ スイッチにする必要があります。

Network Assistant と VTY

Network Assistant は仮想端末（VTY）回線を使用して、クラスタ コマンド デバイスと通信します。Catalyst 4500 シリーズ スイッチには、デフォルト設定で 5 本の VTY 回線が設定されています。Network Assistant では、その他に 8 本の回線を採用できます。このため、最大数の回線（または最低 8 + 5 = 13）を設定し、Network Assistant がスイッチとやり取りできるようにして、Telnet で必要となる可能性がある VTY 回線を使用しないでください。

line vty コンフィギュレーション コマンドを使用して、適切な VTY 回線数をサポートするよう Catalyst 4500 シリーズ スイッチを設定できます。たとえば、VTY 回線を 9 本含めるようスイッチを設定するには、**line vty 6 15** コマンドを使用します。

（注） 既存の VTY 回線がデフォルト以外の設定の場合、この設定を新しい VTY 回線に適用する必要があります。

候補スイッチおよびクラスタ メンバ スイッチの特性

候補スイッチとは、クラスタに含まれないクラスタ対応スイッチです。クラスタ メンバ スイッチとは、現在スイッチ クラスタに含まれているスイッチです。候補スイッチまたはクラスタ メンバ スイッチには独自の IP アドレスおよびパスワードがありますが、必須ではありません。

（注）　候補のホスト名では、[a-zA-Z0-9]-*n* 形式は禁止されています。*n* は 0 ～ 16 です。これらの名前は予約済みです。

クラスタに加入する候補スイッチは、次の要件を満たしている必要があります。

- クラスタ対応ソフトウェアを実行し、クラスタリングがイネーブルであること。
- CDP バージョン 2 がイネーブルに設定されている。
- HTTP サーバがイネーブルであること。

（注）　コマンダ スイッチ上で HTTP がイネーブルの場合でも、コマンダ スイッチとメンバ スイッチ間の通信は HTTP を通じて行われます。そのため、セキュアではありません。

- 16 本の VTY 回線があること。
- 他のクラスタのクラスタ コマンド スイッチまたはクラスタ メンバ スイッチではない。
- 少なくとも 1 つの共通 VLAN を介して、クラスタ コマンド スイッチに接続されている。

  Catalyst 4500 候補スイッチおよびクラスタ メンバ スイッチを設定する場合は、クラスタ コマンド スイッチとの VLAN 接続上の SVI を使用することを推奨します。

CLI によるスイッチ クラスタの管理

クラスタ コマンド スイッチに最初にログインすると、CLI からクラスタ メンバ スイッチを設定できます。**rcommand** ユーザ EXEC コマンドおよびクラスタ メンバ スイッチ番号を入力して、（コンソールまたは Telnet 接続を経由して）Telnet セッションを開始し、クラスタ メンバ スイッチの CLI にアクセスします。コマンド モードは変更され、Cisco IOS コマンドは通常どおり動作します。クラスタ メンバ スイッチで **exit** 特権 EXEC コマンドを入力すると、コマンド スイッチの CLI に戻ります。

次に、コマンドスイッチ CLI からメンバ スイッチ 3 にログインする例を示します。

```
switch# rcommand 3
```

メンバ スイッチ番号が不明の場合は、クラスタ コマンド スイッチで **show cluster members** 特権 EXEC コマンドを入力します。**rcommand** コマンドおよびその他すべてのクラスタ コマンドの詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』を参照してください。

Telnet セッションは、クラスタ コマンド スイッチと同じ権限レベルでメンバ スイッチの CLI にアクセスします。その後、Cisco IOS コマンドを通常どおりに使用できます。スイッチの Telnet セッションの設定手順については、「Telnet を使用して CLI にアクセスする場合」（P.2-2）を参照してください。

（注）　CISCO-CLUSTER_MIB はサポートされません。

コミュニティ モードまたはクラスタ モードでの Network Assistant の設定

ここでは、コミュニティまたはクラスタで稼働する Network Assistant の設定で使用される CLI の詳細について説明します。Network Assistant は、HTTP（または HTTPS）接続で Cisco IOS コマンドを送信することで、Catalyst 4500 シリーズ スイッチと通信します。

ここでは、次の内容について説明します。

コミュニティ モードのネットワーク スイッチ上での Network Assistant の設定

コミュニティ モードのネットワーク スイッチ上で Network Assistant を設定するには、スイッチで次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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 2	`Switch(config)# enable password` *name*	コンフィギュレーション モードのパスワード保護をイネーブルにします。
ステップ 3	`Switch(config)# vtp domain` *name*	VLAN を管理するために、VTP ドメインを作成します。
ステップ 4	`Switch(config)# vlan` *vlan_id*	VLAN を作成します。
ステップ 5	`Switch(config-vlan)# interface {vlan` *vlan_ID* `| {fastethernet | gigabitethernet} slot/interface | Port-channel` *number*`}`	ご使用の CNA 対応 PC に接続するインターフェイスを選択します。
ステップ 6	`Switch(config-if)# switchport access vlan` *vlan_id*	指定の VLAN で選択されたインターフェイスをイネーブルにします。
ステップ 7	`Switch(config-if)# interface {vlan` *vlan_ID* `| slot/interface | Port-channel` *number*`}`	設定用の VLAN インスタンスを選択します。
ステップ 8	`Switch(config-if)# ip address` *ip_address*	SVI に IP アドレスを割り当てます。
ステップ 9	`Switch(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 10	`Switch(config-if)# ip http server`	Network Assistant がスイッチと対話できるよう HTTP サーバを開始します。
ステップ 11	`Switch(config)# ip domain-name` *domain_name*	スイッチでドメイン名をイネーブルにして、HTTPS を設定します。
ステップ 12	`Switch(config)# ip http secure-server`	スイッチ上で HTTPS サーバをイネーブルにします。デフォルトでは、HTTPS サーバはディセーブルに設定されています。
ステップ 13	`Switch(config)# ip http max-connections` *connection_number*	HTTP サーバへの最大同時接続数を設定します。 *connection_number* は 16 を推奨します。

	コマンド	目的
ステップ 14	`Switch(config)# ip http timeout-policy idle idle_time life life_time requests requests`	HTTPS ポートを設定します。 **idle** キーワードでは、接続がアイドル状態でいる最大時間数を指定します。**idle** 値は 180 秒を推奨します。 **life** キーワードでは、接続が確立してからオープンでいる最大時間数を指定します。**life** 値は 180 秒を推奨します。 **requests** キーワードでは、接続の最大要求数を指定します。**requests** 値は 25 を推奨します。
ステップ 15	`Switch(config-if)# ip http secure-server`	（任意）スイッチが Network Assistant からの HTTPS 接続を受け入れるようにします。
ステップ 16	`Switch(config)# ip route a.b.c`	デフォルト ルータとのルートを確立します。これは通常、ローカル インターネット プロバイダーにより供給されます。 **（注）** この回線だけが、スタンドアロン スイッチとネットワーク スイッチの設定の相違点です。
ステップ 17	`Switch(config)# line con 0`	コンソール ポートを選択して設定を実行します。
ステップ 18	`Switch(config-line)# exec-timeout x y`	端末にキーボード入力または出力が表示されない場合、自動セッション ログアウトを設定します。
ステップ 19	`Switch(config-line)# password password`	コンソール ポートのパスワードを指定します。
ステップ 20	`Switch(config-line)# login`	コンソール ポートへのログインを許可します。
ステップ 21	`Switch(config-line)# line vty x y`	CNA がスイッチにアクセスするための追加の VTY 回線を作成します。
ステップ 22	`Switch(config-line)# password password`	スイッチのパスワードを指定します。
ステップ 23	`Switch(config-line)# login`	スイッチへのログインを許可します。
ステップ 24	`Switch(config-line)# line vty x y`	CNA がスイッチにアクセスするための追加の VTY 回線を作成します。
ステップ 25	`Switch(config-line)# password password`	スイッチのパスワードを指定します。
ステップ 26	`Switch(config-line)# login`	スイッチへのログインを許可します。
ステップ 27	`Switch(config-line)# end`	特権 EXEC モードに戻ります。
ステップ 28	`Switch# show running-config`	設定を確認します。

次に、コミュニティ モードのネットワーク スイッチ上で Network Assistant を設定する例を示します。

```
Switch# configure terminal
Switch(config)# vtp domain cnadoc
Changing VTP domain name from cisco to cnadoc
Switch(config)# vlan 2
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 2/1
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
Switch(config)# interface vlan 2
Switch(config-if)# ip address 123.123.123.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# ip http server
Switch(config)# ip domain-name cisco.com
Switch(config)# ip http secure-server
Switch(config)# ip http max-connections 16
```

```
Switch(config)# ip http timeout-policy idle 180 life 180 requests 25
Switch(config)# ip route 0.0.0.0 0.0.0.0 123.123.123.2
Switch(config)# line con 0
Switch(config-line)# exec-timeout 0 0
Switch(config-line)# password keepout
Switch(config-line)# login
Switch(config-line)# line vty 5 15
Switch(config-line)# password keepout
Switch(config-line)# login
Switch(config-line)# line vty 5 15
Switch(config-line)# end
Switch# show running-config
Building configuration...

Current configuration : 1426 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
enable password cna
!
no aaa new-model
ip subnet-zero
ip domain-name cisco.com
!
vtp domain cnadoc
vtp mode transparent
!
crypto pki trustpoint TP-self-signed-913087
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-913087
 revocation-check none
 rsakeypair TP-self-signed-913087
!!
crypto pki certificate chain TP-self-signed-913087
 certificate self-signed 01
  3082028E 308201F7 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  52312B30 29060355 04031322 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 39313330 38373123 30210609 2A864886 F70D0109 02161456
  61646572 2D343531 302E6369 73636F2E 636F6D30 1E170D30 36303432 30323332
  3435305A 170D3230 30313031 30303030 30305A30 52312B30 29060355 04031322
  494F532D 53656C66 2D536967 6E65642D 43657274 69666963 6174652D 39313330
  38373123 30210609 2A864886 F70D0109 02161456 61646572 2D343531 302E6369
  73636F2E 636F6D30 819F300D 06092A86 4886F70D 01010105 0003818D 00308189
  02818100 F2C86FEA 49C37856 D1FA7CB2 9AFF748C DD443295 F6EC900A E83CDA8E
  FF8F9367 0A1E7A20 C0D3919F 0BAC2113 5EE37525 94CF24CF 7B313C01 BF177A73
  494B1096 B4D24729 E087B39C E44ED9F3 FCCD04BB 4AD3C6BF 66E0902D E234D08F
  E6F6C001 BAC80854 D4668160 9299FC73 C14A33F3 51A17BF5 8C0BEA07 3AC03D84
  889F2661 02030100 01A37430 72300F06 03551D13 0101FF04 05300301 01FF301F
  0603551D 11041830 16821456 61646572 2D343531 302E6369 73636F2E 636F6D30
  1F060355 1D230418 30168014 BB013B0D 00391D79 B628F2B3 74FC62B4 077AD908
  301D0603 551D0E04 160414BB 013B0D00 391D79B6 28F2B374 FC62B407 7AD90830
  0D06092A 864886F7 0D010104 05000381 81002963 26762EFA C52BA4B3 6E641A9D
  742CE404 E45FECB1 B5BD2E74 6F682476 A7C3DAA5 94393AE3 AA103B6E 5974F81B
  09DF16AE 7F9AE67C 5CB3D5B1 B945A5F3 36A8CC8C 8F142364 F849344D 5AE36410
```

```
  51182EB9 24A9330B 3583E1A3 79151470 D304C157 3417E240 52BE2A91 FC7BBEDE
  562BEDAD E6C46D9A F7FF3148 4CE9CEE1 5B17
  quit
!
!
!
power redundancy-mode redundant
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 2
!
interface GigabitEthernet1/1
 switchport access vlan 2
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
!
interface GigabitEthernet1/5
!
interface GigabitEthernet1/6
!
interface GigabitEthernet1/7
!
interface GigabitEthernet1/8
!
interface GigabitEthernet1/9
!
interface GigabitEthernet1/10
!
interface GigabitEthernet1/11
!
interface GigabitEthernet1/12
!
interface GigabitEthernet1/13
!
interface GigabitEthernet1/14
!
interface GigabitEthernet1/15
!
interface GigabitEthernet1/16
!
interface GigabitEthernet1/17
!
interface GigabitEthernet1/18
!
interface GigabitEthernet1/19
!
interface GigabitEthernet1/20
!
interface Vlan1
 no ip address
!
interface Vlan2
 ip address 123.123.123.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 123.123.123.2
ip http server
```

```
ip http secure-server
ip http max-connections 16
ip http timeout-policy idle 180 life 180 requests 25
!
line con 0
 password cna
 login
 stopbits 1
line vty 0 4
 password cna
 login
line vty 5 15
 password cna
 login
!
!
end

Switch#
```

クラスタ モードのネットワーク スイッチ上での Network Assistant の設定

クラスタ モードのネットワーク スイッチ上で Network Assistant を設定するには、スイッチで次の作業を行います。

	コマンド	目的
ステップ 1	Switch# **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 2	Switch(config)# **enable password** *name*	コンフィギュレーション モードのパスワード保護をイネーブルにします。
ステップ 3	Switch(config)# **vtp domain** *name*	VLAN および名前を管理するために、VTP ドメインを作成します。
ステップ 4	Switch(config)# **cluster run**	クラスタ コマンダ上でクラスタを開始します。
ステップ 5	Switch(config)# **cluster enable** *cluster_name*	スイッチをクラスタ コマンダに設定します。
ステップ 6	Switch(config)# **vlan** *vlan_id*	VLAN を作成します。
ステップ 7	Switch(config-vlan)# **interface** {**vlan** *vlan_ID* | {**fastethernet** | **gigabitethernet**} *slot/interface* | **Port-channel** *number*}	ご使用の CNA 対応 PC に接続するインターフェイスを選択します。
ステップ 8	Switch(config-if)# **switchport access vlan** *vlan_id*	指定の VLAN 内の物理ポートをイネーブルにします。
ステップ 9	Switch(config-if)# **interface** {**vlan** *vlan_ID* | *slot/interface* | **Port-channel** *number*}	設定用の VLAN インスタンスを選択します。
ステップ 10	Switch(config-if)# **ip address** *ip_address*	SVI に IP アドレスを割り当てます。
ステップ 11	Switch(config-if)# **no shut**	インターフェイスをイネーブルにします。
ステップ 12	Switch(config-if)# **ip http server**	Network Assistant がスイッチと対話できるよう HTTP サーバを開始します。
ステップ 13	Switch(config)# **ip http secure-server**	（任意）スイッチが Network Assistant からの HTTPS 接続を受け入れるようにします。
ステップ 14	Switch(config)# **ip route** *a.b.c*	デフォルト ルータとのルートを確立します。これは通常、ローカル インターネット プロバイダーにより供給されます。 **（注）** この回線だけが、スタンドアロン スイッチとネットワーク スイッチの設定の相違点です。

	コマンド	目的
ステップ 15	Switch(config)# **line con 0**	コンソール ポートを選択して設定を実行します。
ステップ 16	Switch(config-line)# **exec-timeout** *x y*	端末にキーボード入力または出力が表示されない場合、自動セッション ログアウトを設定します。
ステップ 17	Switch(config-line)# **password** *password*	コンソール ポートのパスワードを指定します。
ステップ 18	Switch(config-line)# **login**	コンソール ポートへのログインを許可します。
ステップ 19	Switch(config-line)# **line vty** *x y*	CNA がスイッチにアクセスするための追加の VTY 回線を作成します。
ステップ 20	Switch(config-line)# **password** *password*	スイッチのパスワードを指定します。
ステップ 21	Switch(config-line)# **login**	スイッチへのログインを許可します。
ステップ 22	Switch(config-line)# **line vty** *x y*	CNA がスイッチにアクセスするための追加の VTY 回線を作成します。
ステップ 23	Switch(config-line)# **password** *password*	スイッチのパスワードを指定します。
ステップ 24	Switch(config-line)# **login**	スイッチへのログインを許可します。
ステップ 25	Switch(config-line)# **end**	特権 EXEC モードに戻ります。
ステップ 26	Switch# **show running-config| include http**	HTTP サーバがイネーブルであることを確認します。

次に、クラスタ モードのネットワーク スイッチ上で Network Assistant を設定する例を示します。

```
Switch# configure terminal
Switch(config)# vtp domain cnadoc
Switch(config)# cluster run
Switch(config)# cluster enable cnadoc
Switch(config)# vlan 10
Switch(config-vlan)# interface GigabitEthernet 2/1
Switch(config-if)# switchport access vlan 10
Switch(config-if)# interface vlan10
Switch(config-if)# ip address aa.bb.cc.dd
Switch(config-if)# no shut
Switch(config-if)# ip http server
Switch(config-if)# ip http secure-server
Switch(config)# ip route 0.0.0.0 0.0.0.0 123.123.123.2
Switch(config)# line con 0
Switch(config-line)# exec-timeout 0 0
Switch(config-line)# password keepout
Switch(config-line)# login
Switch(config-line)# line vty 5 15
Switch(config-line)# password keepout
Switch(config-line)# login
Switch(config-line)# line vty 5 15
Switch(config-line)# end
Switch# show running-config
Building configuration...

Current configuration : 1469 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
!
hostname Switch
```

```
!
boot-start-marker
boot-end-marker
!
enable password cna
!
no aaa new-model
ip subnet-zero
!
vtp domain cnadoc
vtp mode transparent
cluster run
cluster enable cnadoccluster 0
!
!
!
!
!
power redundancy-mode redundant
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 2
!
interface GigabitEthernet1/1
 switchport access vlan 2
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
!
interface GigabitEthernet1/5
!
interface GigabitEthernet1/6
!
interface GigabitEthernet1/7
!
interface GigabitEthernet1/8
!
interface GigabitEthernet1/9
!
interface GigabitEthernet1/10
!
interface GigabitEthernet1/11
!
interface GigabitEthernet1/12
!
interface GigabitEthernet1/13
!
interface GigabitEthernet1/14
!
interface GigabitEthernet1/15
!
interface GigabitEthernet1/16
!
interface GigabitEthernet1/17
!
interface GigabitEthernet1/18
!
```

```
interface GigabitEthernet1/19
!
interface GigabitEthernet1/20
!
interface Vlan1
 no ip address
!
interface Vlan2
 ip address 123.123.123.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 123.123.123.2
ip http server
no ip http secure-server
!
!
!
line con 0

Switch#
```