CHAPTER 8

FC-SP および DHCHAP の設定

Fibre Channel Security Protocol（FC-SP）機能は、スイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。Diffie-Hellman（DH）Challenge Handshake Authentication Protocol（DHCHAP）は、Cisco MDS 9000 ファミリ スイッチとその他のデバイス間で認証を行う FC-SP プロトコルです。DHCHAP は、CHAP プロトコルと DH 交換を組み合わせたものです。

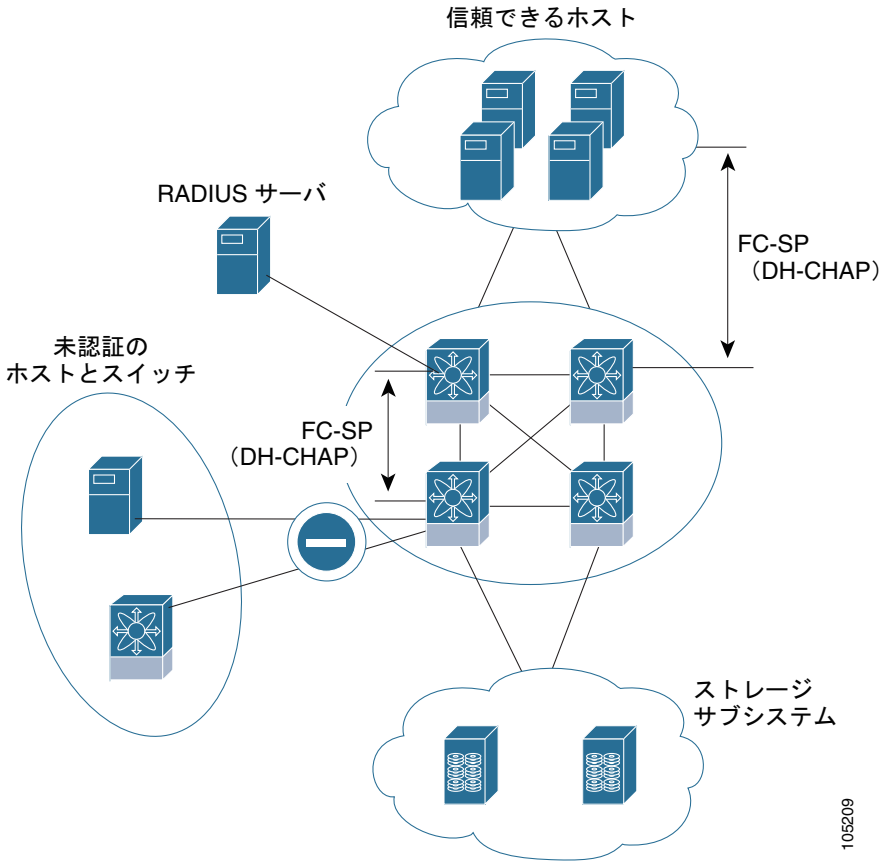
この章の内容は、次のとおりです。

ファブリック認証の概要

Cisco MDS 9000 ファミリのスイッチはすべて、スイッチ間またはスイッチとホスト間の認証をファブリック全体で実行できます。これらのスイッチおよびホスト認証は、各ファブリックでローカルに実行することも、リモートで実行することもできます。ストレージ アイランドを企業全体のファブリックに統合して、移行すると、新しいセキュリティ問題が発生します。ストレージ アイランドを保護する方法が、企業全体のファブリックで必ずしも保証されなくなります。

たとえば、スイッチが地理的に分散しているキャンパス環境では、他のユーザが故意に、またはユーザ自身が偶然に、互換性のないスイッチを相互接続することにより、Inter-Switch Link（ISL; スイッチ間リンク）分離やリンク切断が発生することがあります。Cisco MDS 9000 ファミリ スイッチでは、物理セキュリティに対するこのようなニーズに対応しています（図 8-1 を参照）。

図 8-1　スイッチおよびホストの認証



DHCHAP

DHCHAP は、スイッチに接続されたデバイスを認証する認証プロトコルです。ファイバ チャネル認証を使用すると、信頼できるデバイスだけをファブリックに追加できるので、不正なデバイスのスイッチへのアクセスを防止できます。

（注）　この章では、FC-SP および DHCHAP という用語を共通の意味で使用しています。

DHCHAP は、スイッチ間およびホストとスイッチ間の認証をサポートする、必須のパスワードベースのキーエクスチェンジ認証プロトコルです。DHCHAP は、ハッシュ アルゴリズムおよび DH グループとネゴシエートしてから、認証を実行します。また、Message Digest 5（MD5）および Secure Hash Algorithm（SHA-1）アルゴリズムベース認証をサポートします。

DHCHAP 機能の設定には、ENTERPRISE_PKG ライセンスが必要です（『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照）。

ローカル パスワード データベースを使用して DHCHAP 認証を設定する手順は、次のとおりです。

ステップ 1　DHCHAP をイネーブルにします。

ステップ 2　DHCHAP 認証モードを識別して設定します。

ステップ 3　ハッシュ アルゴリズムおよび DH グループを設定します。

ステップ 4　ローカル スイッチおよびファブリック上の他のスイッチの DHCHAP パスワードを設定します。

ステップ 5　再認証用の DHCHAP タイムアウト値を設定します。

ステップ 6　DHCHAP 設定を確認します。

ここで説明する内容は、次のとおりです。

既存の Cisco MDS 機能との DHCHAP の互換性

ここでは、DHCHAP 機能および既存の Cisco MDS 機能の設定の影響について説明します。

- ポートチャネル インターフェイス：ポートチャネルに属しているポートに対して DHCHAP がイネーブルの場合、DHCHAP 認証はポートチャネル レベルでなく、物理インターフェイス レベルで実行されます。
- Fibre Channel over IP（FCIP）インターフェイス：DHCHAP プロトコルは、物理インターフェイスの場合と同様に、FCIP インターフェイスと連携します。
- ポート セキュリティまたはファブリック バインディング：ファブリック バインディング ポリシーは、DHCHAP によって認証される ID に基づいて実行されます。
- Virtual Storage Area Network（VSAN; 仮想ストレージ エリア ネットワーク）：DHCHAP 認証は VSAN 単位では実行されません。

- High Availability（HA; ハイ アベイラビリティ）：DHCHAP 認証は既存の HA 機能とトランスペアレントに連携します。

DHCHAP イネーブル化の概要

デフォルトでは、Cisco MDS 9000 ファミリの全スイッチで DHCHAP 機能はディセーブルに設定されています。

ファブリック認証用の設定コマンドおよび確認コマンドにアクセスするには、DHCHAP 機能をイネーブルにする必要があります。この機能をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

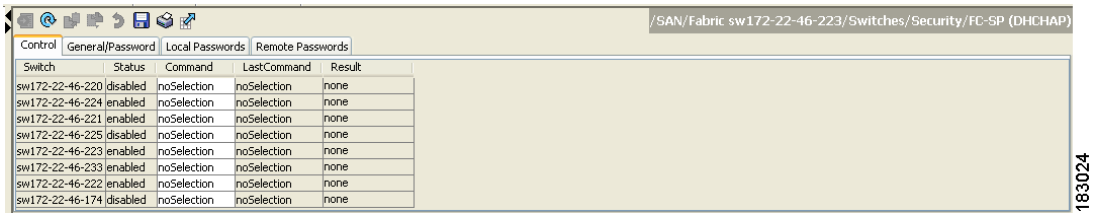
DHCHAP のイネーブル化

Fabric Manager を使用して Cisco MDS スイッチの DHCHAP をイネーブルにする手順は、次のとおりです。

ステップ 1　[Switches]、[Security] の順に展開し、[FC-SP] を選択します。

[Information] ペインに FC-SP（DHCHAP）の設定が表示されます（図 8-2 を参照）。

図 8-2　FC-SP の設定



[Control] タブがデフォルトです。ファブリック内の全スイッチの FC-SP イネーブル ステートが表示されます。

ステップ 2　FC-SP をイネーブルにするすべてのスイッチについて、[Command] ドロップダウン メニューを [enable] に設定します。

ステップ 3　[Apply Changes] アイコンをクリックし、選択したスイッチ上で FC-SP および DHCHAP をイネーブルにします。

DHCHAP 認証モードの概要

各インターフェイスの DHCHAP 認証ステータスは、設定された DHCHAP ポート モードによって異なります。

スイッチ内で DHCHAP 機能がイネーブルの場合には、各ファイバ チャネル インターフェイスまたは FCIP インターフェイスを 4 つの DHCHAP ポート モードのいずれかに設定できます。

- on：接続元デバイスが DHCHAP 認証をサポートしている場合、スイッチの初期化中に認証シーケンスが実行されます。接続元デバイスが DHCHAP 認証をサポートしていない場合には、リンクが分離状態になります。

- auto-active：接続元デバイスが DHCHAP 認証をサポートしている場合、スイッチの初期化中に認証シーケンスが実行されます。接続元デバイスが DHCHAP 認証をサポートしていない場合には、認証シーケンスの残りが継続されます。
- auto-passive（デフォルト）：スイッチは DHCHAP 認証を開始しませんが、接続元デバイスが DHCHAP 認証を開始した場合には、DHCHAP 認証に参加します。
- off：スイッチは DHCHAP 認証をサポートしません。このようなポートに認証メッセージが送信された場合、開始元スイッチにエラー メッセージが戻されます。

（注）　DHCHAP ポート モードを Off モード以外のモードに変更すると、再認証が実行されます。

表 8-1 に、さまざまなモードに設定した 2 台の Cisco MDS スイッチ間での認証動作について説明します。

表 8-1　2 台の MDS スイッチ間の DHCHAP 認証ステータス

スイッチ N DHCHAP モード	スイッチ 1 DHCHAP モード			
	on	**auto-active**	**auto-passive**	**off**
on	FC-SP 認証が実行されます。	FC-SP 認証が実行されます。	FC-SP 認証が実行されます。	リンクがダウンになります。
auto-active				FC-SP 認証は*実行されません。*
auto-passive			FC-SP 認証は*実行されません。*	
off	リンクがダウンになります。	FC-SP 認証は*実行されません。*		

DHCHAP モードの設定

Fabric Manager を使用して特定のインターフェイスに DHCHAP モードを設定する手順は、次のとおりです。

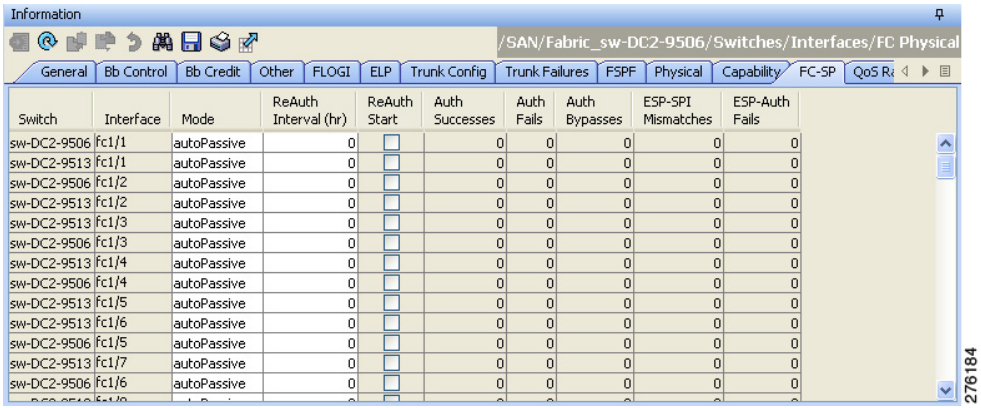
ステップ 1　[Switches]、[Interfaces] の順に展開し、[FC Physical] を選択します。

[Information] ペインにインターフェイス設定が表示されます。

ステップ 2　[FC-SP] タブをクリックします。

[Information] ペインに FC-SP（DHCHAP）の設定が表示されます（図 8-3 を参照）。

図 8-3　FC-SP（DHCHAP）インターフェイス モード



ステップ 3　[Mode] ドロップダウン メニューで、インターフェイスに設定する DHCHAP 認証モードを設定します。

ステップ 4　[Apply Changes] アイコンをクリックして、DHCHAP ポート モードの設定を保存します。

DHCHAP ハッシュ アルゴリズムの概要

Cisco MDS スイッチは、DHCHAP 認証用のデフォルト ハッシュ アルゴリズム プライオリティ リスト（MD5 のあとに SHA-1）をサポートしています。

ヒント　ハッシュ アルゴリズムの設定を変更する場合には、ファブリック内のすべてのスイッチに対してグローバルに変更します。

注意　Remote Access Dial-In User Service（RADIUS）および Terminal Access Controller Access Control System Plus（TACACS+）プロトコルは CHAP 認証に必ず MD5 を使用します。ハッシュ アルゴリズムとして SHA-1 を使用すると、これらの Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）プロトコルが DHCHAP 認証に対してイネーブルに設定されていても、RADIUS および TACACS+ を使用できないことがあります。

DHCHAP ハッシュ アルゴリズムの設定

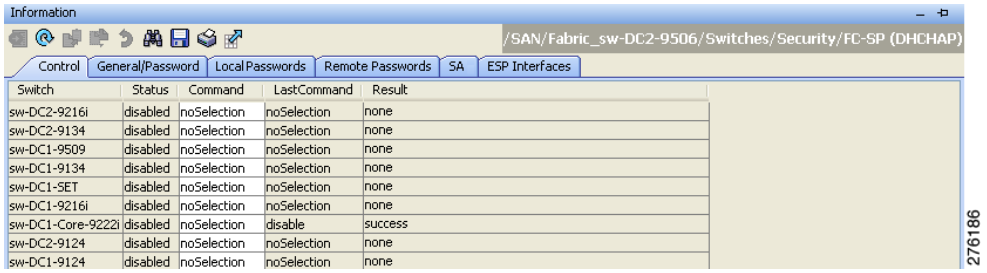
Fabric Manager を使用してハッシュ アルゴリズムを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を選択し、[FC-SP] を選択します。

ステップ 2　[General/Password] タブをクリックします。

各スイッチの DHCHAP 一般設定モードが表示されます（図 8-4 を参照）。

図 8-4　[General/Password] タブ



ステップ 3　ファブリック内の各スイッチの DHCHAP HashList を変更します。

ステップ 4　[Apply Changes] アイコンをクリックして、更新したハッシュ アルゴリズム プライオリティ リストを保存します。

DHCHAP グループ設定の概要

すべての Cisco MDS ファミリ スイッチは、標準で指定されたすべての DHCHAP グループをサポートします。これらのグループは、0（Diffie-Hellman 交換を実行しないヌル DH グループ）、1、2、3、または 4 です。

ヒント　DH グループの設定を変更する場合には、ファブリック上の全スイッチに対してグローバルに変更してください。

DHCHAP グループの設定

Fabric Manager を使用して DH グループ設定を変更する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[FC-SP] を選択します。

ステップ 2　[General/Password] タブをクリックします。

ステップ 3　ファブリック内の各スイッチの DHCHAP GroupList を変更します。

ステップ 4　[Apply Changes] アイコンをクリックして、更新したハッシュ アルゴリズム プライオリティ リストを保存します。

DHCHAP パスワードの概要

DHCHAP 認証を方向ごとに実行するには、接続されたデバイス間の共有シークレット パスワードが必要です。このパスワードを使用するには、DHCHAP に参加するファブリック上のすべてのスイッチで、次の 3 つの方法のいずれかを使用してパスワードを管理します。

- 方法 1：ファブリック上のすべてのスイッチに同じパスワードを使用します。これは最も簡単な方法です。新しいスイッチを追加する場合、このファブリック上では同じパスワードを使用してそのスイッチを認証することになります。したがって、ファブリック内のいずれかのスイッチに外部から不正アクセスを試みる場合、これは最も脆弱な方法です。
- 方法 2：ファブリック上のスイッチごとに異なるパスワードを使用して、このパスワード リストを維持します。新しいスイッチを追加する場合には、新規パスワード リストを作成して、この新規リストを使用してすべてのスイッチを更新します。いずれかのスイッチにアクセスすると、このファブリック上のすべてのスイッチに関するパスワード リストが生成されます。
- 方法 3：ファブリック上のスイッチごとに異なるパスワードを使用します。新規スイッチを追加する場合は、ファブリック上の各スイッチに対応する複数の新規パスワードを生成して、各スイッチに設定する必要があります。いずれかのスイッチが被害にあっても、他のスイッチのパスワードは引き続き保護されます。この方法では、ユーザ側で大量のパスワード メンテナンス作業が必要になります。

（注） すべてのパスワードは 64 個の英数字に制限され、変更可能ですが、削除はできません。

ヒント 6 台以上のスイッチを含むファブリックでは、RADIUS または TACACS+ の使用を推奨します。ローカル パスワード データベースを使用する必要がある場合には、方法 3 を使用し、Cisco MDS 9000 ファミリ Fabric Manager を使用して、パスワード データベースを管理します。

ローカル スイッチの DHCHAP パスワードの設定

Fabric Manager を使用してローカル スイッチに DHCHAP パスワードを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[FC-SP] を選択します。

[Information] ペインに、FC-SP の設定が表示されます。

ステップ 2　[Local Passwords] タブをクリックします。

ステップ 3　[Create Row] アイコンをクリックして、新しいローカル パスワードを作成します。

[Create Local Passwords] ダイアログボックスが表示されます。

ステップ 4　（任意）同じローカル パスワードを設定するスイッチをチェックします。

ステップ 5　スイッチ World Wide Name（WWN）を選択し、[Password] フィールドにパスワードを入力します。

ステップ 6　[Create] ボタンをクリックして、更新したパスワードを保存します。

リモート デバイスのパスワード設定の概要

ファブリック上の他のデバイスのパスワードを、ローカル認証データベースに設定できます。他のデバイスは、スイッチ WWN またはデバイス WWN と呼ばれるデバイス名によって識別されます。パスワードは 64 文字に制限され、クリア テキスト（0）または暗号化テキスト（7）で指定できます。

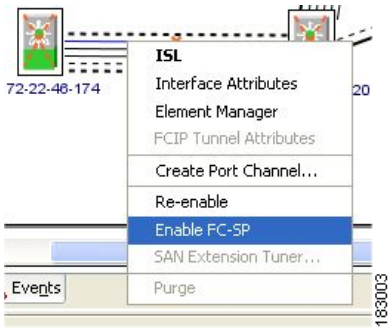
（注）　スイッチ WWN は物理スイッチを識別します。スイッチ WWN はスイッチを認証する場合に使用され、VSAN ノードの WWN とは異なります。

リモート デバイスの DHCHAP パスワードの設定

Fabric Manager を使用して、ファブリック内の別のスイッチのリモート DHCHAP パスワードをローカルで設定する手順は、次のとおりです。

ステップ 1　ISL を右クリックし、ドロップダウン リストから [Enable FC-SP] を選択します（図 8-5 を参照）。

図 8-5　[Enable FC-SP]



[Enable FC-SP] ダイアログボックスが表示されます。

図 8-6　[Enable FC-SP] ダイアログボックス

ステップ 2　[Apply] ボタンをクリックして、更新したパスワードを保存します。

DHCHAP タイムアウト値の概要

DHCHAP プロトコルの交換中に、MDS スイッチが待機中の DHCHAP メッセージを指定インターバル内に受信しなかった場合、認証は失敗したと見なされます。このインターバルは 20（認証が実行されない）～ 1000 秒です。デフォルトは 30 秒です。

タイムアウト値を変更する場合には、次の要因について考慮してください。

- 既存の RADIUS および TACACS+ タイムアウト値。
- ファブリック上の全スイッチに同じ値を設定する必要があります。

DHCHAP タイムアウト値の設定

Fabric Manager を使用して DHCHAP タイムアウト値を設定する手順は、次のとおりです。

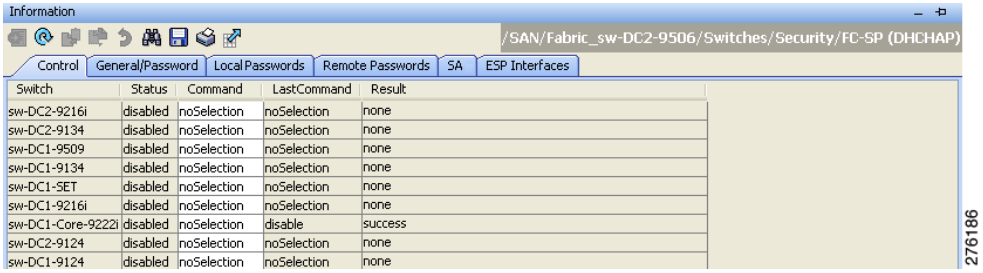
ステップ 1　[Switches] > [Security] を展開し、[FC-SP] を選択します。

[Information] ペインに、FC-SP の設定が表示されます。

ステップ 2　[General/Password] タブをクリックします。

各スイッチの DHCHAP 一般設定モードが表示されます（図 8-7 を参照）。

図 8-7　[General/Password] タブ



ステップ 3　ファブリック内の各スイッチの DHCHAP タイムアウト値を変更します。

ステップ 4　[Apply Changes] アイコンをクリックして、更新情報を保存します。

DHCHAP AAA 認証の設定

認証オプションは個別に設定できます。認証を設定しない場合、デフォルトでローカル認証が使用されます。

AAA 認証の設定については、第 4 章「RADIUS および TACACS+ の設定」を参照してください。

ISL 上での FC-SP のイネーブル化

Fabric Manager には、ISL のどちらかの側のスイッチ上で FC-SP をイネーブルにする、[Enable FC-SP] と呼ばれる ISL のポップアップ メニューがあります。FC-SP 一般パスワードを入力し、関連ポートの FC-SP インターフェイス モードを ON に設定します。この機能を設定するには、ISL を右クリックして、[Enable FC-SP] ポップアップ メニューをクリックします。

デフォルト設定値

表 8-2 に、スイッチのすべてのファブリック セキュリティ機能のデフォルト設定を示します。

表 8-2　ファブリック セキュリティのデフォルト設定

パラメータ	デフォルト
DHCHAP 機能	ディセーブル
DHCHAP ハッシュ アルゴリズム	最初に MD5、次に SHA-1 のプライオリティ リストで DHCHAP 認証を実行
DHCHAP 認証モード	auto-passive
DHCHAP グループのデフォルトの交換プライオリティ	0、4、1、2、3 の順
DHCHAP タイムアウト値	30 秒