FC-SP および DHCHAP の設定

この章の内容は、次のとおりです。

FC-SP および DHCHAP の設定

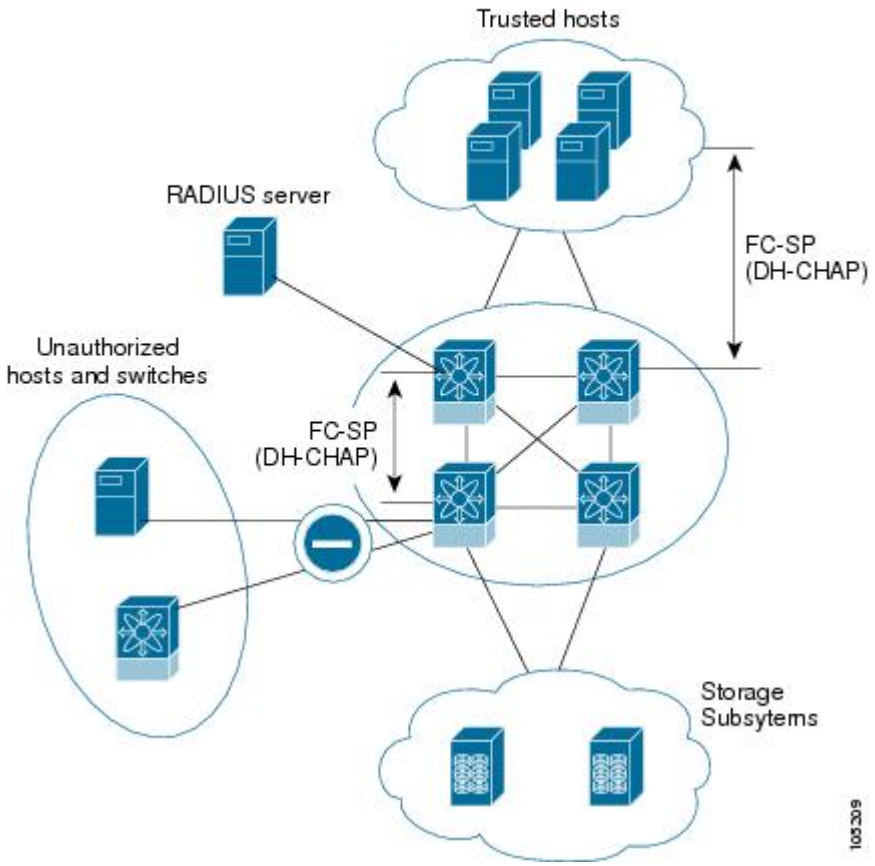
Fibre Channel Security Protocol（FC-SP）機能は、スイッチとスイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。Diffie-Hellman チャレンジ ハンドシェイク認証プロトコル（DHCHAP）は、Cisco SAN スイッチとその他のデバイス間で認証を行う FC-SP プロトコルです。 DHCHAP は、CHAP プロトコルと Diffie-Hellman 交換を組み合わせて構成されています。

ファブリック認証に関する情報

Cisco SAN の全スイッチで、1 台のスイッチから他のスイッチへ、またはスイッチからホストへ、ファブリック規模の認証を実行できます。 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またはリモートで実行できます。 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誤って、互換性のないスイッチに故意に相互接続すると、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 SAN スイッチでは、物理的なセキュリティに対処する認証機能がサポートされます（次の図を参照）。

図 *1*：スイッチおよびホストの認証



（注） ホスト スイッチ認証には、適切なファームウェアおよびドライバを備えたファイバ チャネル Host Bus Adapter（HBA）が必要です。

DHCHAP

DHCHAP は、スイッチに接続している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、必須のパスワードに基づくキー交換による認証プロトコルであり、スイッチ間およびホスト スイッチ間の認証をサポートします。 DHCHAP はハッシュ アルゴリズムおよび DH グループをネゴシエートしてから、認証を実行します。 また、MD5 および SHA-1 アルゴリズムベース認証をサポートします。

ローカル パスワード データベースを使用する DHCHAP 認証の設定手順は、次のとおりです。

手順の概要

1. DHCHAP をイネーブルにします。
2. DHCHAP 認証モードを識別して設定します。
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。
4. ローカル スイッチおよびファブリックの他のスイッチの DHCHAP パスワードを設定します。
5. 再認証の DHCHAP タイムアウト値を設定します。
6. DHCHAP の設定を確認します。

手順の詳細

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 再認証の DHCHAP タイムアウト値を設定します。
ステップ 6 DHCHAP の設定を確認します。

ファイバ チャネル機能と DHCHAP の互換性

ここでは、DHCHAP 機能を既存の Cisco NX-OS 機能と一緒に設定した場合の影響について説明します。

- SAN ポートチャネル インターフェイス：SAN 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 レベルではなく、物理インターフェイス レベルで実行されます。
- 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。
- VSAN：DHCHAP 認証は、VSAN 単位では実行されません。

DHCHAP イネーブル化の概要

デフォルトでは、DHCHAP 機能はすべての Cisco SAN スイッチでディセーブルです。

ファブリック認証用のコンフィギュレーション 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

Cisco Nexus 5000 シリーズ スイッチ用の DHCHAP をイネーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcsp enable**
3. switch(config)# **no fcsp enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcsp enable**	このスイッチ上でDHCHAP をイネーブルにします。
ステップ 3	switch(config)# **no fcsp enable**	このスイッチ上でDHCHAP をディセーブル（デフォルト）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、DHCHAP ポート モードの設定によって変化します。

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次の 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、ソフトウェアにより、初期化シーケンスの残りが実行されます。

- 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 認証を開始すれば、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。 このモードで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。

次の表で、さまざまなモードに設定した 2 台のシスコ スイッチ間での認証について説明します。

表 *1*：*2* 台の *SAN* スイッチ間の *DHCHAP* 認証ステータス

スイッチ N の DHCHAP モード	スイッチ 1 の 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

特定のインターフェイスの DHCHAP モードを設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **interface fc** *slot*/*port* - *slot*/*port*
3. switch(config-if)# **fcsp on**
4. switch(config-if)# **no fcsp on**
5. switch(config-if)# **fcsp auto-active 0**
6. switch(config-if)# **fcsp auto-active** *timeout-period*
7. switch(config-if)# **fcsp auto-active**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **interface fc** *slot*/*port* - *slot*/*port*	インターフェイスの範囲を選択し、インターフェイス コンフィギュレーション モードに入ります。
ステップ 3	switch(config-if)# **fcsp on**	選択したインターフェイスの DHCHAP モードを on ステートに設定します。
ステップ 4	switch(config-if)# **no fcsp on**	これら 3 つのインターフェイスを出荷時デフォルトの auto-passive に戻します。
ステップ 5	switch(config-if)# **fcsp auto-active 0**	選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。 0 は、ポートが再認証を実行しないことを表します。 （注） 再許可インターバル設定は、デフォルトの動作と同じです。
ステップ 6	switch(config-if)# **fcsp auto-active** *timeout-period*	選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。タイムアウト期間の値（分）では、最初の認証後の再認証の頻度を設定します。
ステップ 7	switch(config-if)# **fcsp auto-active**	選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。 再認証はディセーブルになります（デフォルト）。 （注） 再許可インターバル設定は、0 に設定した場合と同じです。

DHCHAP ハッシュ アルゴリズムの概要

Cisco SAN スイッチは、DHCHAP 認証のためのデフォルトのハッシュ アルゴリズムのプライオリティ リストとして、最初に MD5、次に SHA-1 をサポートします。

ハッシュ アルゴリズムの設定を変更する場合は、ファブリック上の全スイッチに対して設定をグローバルに変更してください。

注意 RADIUS および TACACS+ プロトコルは、CHAP 認証で常に MD5 を使用します。 SHA-1 をハッシュ アルゴリズムとして使用すると、DHCHAP 認証用に RADIUS および TACACS+ がイネーブルになっていても、これらの AAA プロトコルが使用できなくなる可能性があります。

DHCHAP ハッシュ アルゴリズムの設定

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。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcsp dhchap hash** [**md5**] [**sha1**]
3. switch(config)# **no fcsp dhchap hash sha1**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcsp dhchap hash** [**md5**] [**sha1**]	MD5 または SHA-1 ハッシュ アルゴリズムを使用するように設定します。
ステップ 3	switch(config)# **no fcsp dhchap hash sha1**	出荷時デフォルトのハッシュ アルゴリズム プライオリティ リスト（最初に MD5、次に SHA-1）に戻します。

DHCHAP グループ設定の概要

すべての Cisco SAN スイッチは、規格 0（Diffie-Hellman 交換を実行しないヌルの DH グループ）、1、2、3、または 4 で指定されたすべての DHCHAP グループをサポートします。

DH グループの設定を変更する場合は、ファブリック内のすべてのスイッチの設定をグローバルに変更してください。

DHCHAP グループの設定

DH グループの設定を変更する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcsp dhchap dhgroup** [**0** | **1** | **2** | **3** | **4**]
3. switch(config)# **no fcsp dhchap dhgroup** [**0** | **1** | **2**| **3** | **4**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcsp dhchap dhgroup** [**0** | **1** | **2** | **3** | **4**]	DH グループを設定された順序で使用するようにプライオリティ リスト化します。
ステップ 3	switch(config)# **no fcsp dhchap dhgroup** [**0** | **1** | **2**| **3** | **4**]	DHCHAP の出荷時デフォルトの順序（0、4、1、2、3）に戻します。

DHCHAP パスワードの概要

DHCHAP 認証を実行する方向ごとに、接続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ために、次の 3 つの設定例のいずれかを使用して DHCHAP に参加するファブリック内のすべてのスイッチのパスワードを管理します。

- 設定例 1：ファブリック内の全スイッチに同じパスワードを使用します。 これは最も単純な設定例です。 新しいスイッチを追加する場合、このファブリック内では同じパスワードを使用してそのスイッチを認証します。 したがってこれは、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が試みられた場合に最も脆弱な設定例です。
- 設定例 2：スイッチごとに異なるパスワードを使用して、ファブリック内のスイッチごとにパスワード リストを保持します。 新しいスイッチを追加する場合は、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。
- 設定例 3：ファブリック内のスイッチごとに、異なるパスワードを使用します。 新しいスイッチを追加する場合は、ファブリック内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。 この設定例では、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） パスワードはすべて 64 文字以内の英数字に制限されます。パスワードは変更できますが、削除はできません。

スイッチが 6 台以上のファブリックでは、RADIUS または TACACS+ の使用をお勧めします。 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、パスワード データベースを管理するために、設定 3 および Cisco MDS 9000 ファミリ Fabric Manager を引き続き使用できます。

ローカル スイッチの DHCHAP パスワードの設定

ローカル スイッチの DHCHAP パスワードを設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcsp dhchap password** [**0** | **7**] *password* [**wwn** *wwn-id*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcsp dhchap password** [**0** | **7**] *password* [**wwn** *wwn-id*]	ローカル スイッチのクリアテキスト パスワードを設定します。

リモート デバイスのパスワード設定の概要

ファブリック内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 やデバイス WWN といったデバイス名で表されます。 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。 この WWN はスイッチの認証に使用されます。また、VSAN ノード 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

ファブリック内の他のスイッチのリモート DHCHAP パスワードをローカル側で設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcsp dhchap devicename** *switch-wwn* **password** *password*
3. switch(config)# **no fcsp dhchap devicename** *switch-wwn* **password** *password*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcsp dhchap devicename** *switch-wwn* **password** *password*	スイッチWWNデバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。
ステップ 3	switch(config)# **no fcsp dhchap devicename** *switch-wwn* **password** *password*	ローカル認証データベースから、このスイッチのパスワード エントリを削除します。

DHCHAP タイムアウト値の概要

DHCHAP プロトコル交換を実行するとき、スイッチが指定時間内に予期した DHCHAP メッセージを受信しない場合、認証は失敗したと見なされます。 この（認証が失敗したと見なされるまでの）時間は、20 ～ 1000 秒の範囲で設定できます。 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。
- ファブリック内のすべてのスイッチに同じ値を設定する必要もあります。

DHCHAP タイムアウト値の設定

DHCHAP タイムアウト値を設定する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **fcsp timeout** *timeout*
3. switch(config)# **no fcsp timeout** *timeout*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **fcsp timeout** *timeout*	再認証タイムアウトを指定された値に設定します。単位は秒です。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **no fcsp timeout** *timeout*	出荷時デフォルトの 30 秒に戻します。

DHCHAP AAA 認証の設定

AAA 認証で RADIUS または TACACS+ サーバ グループを使用するように設定できます。 AAA 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。

プロトコル セキュリティ情報の表示

ローカル データベースの設定を表示するには、**show fcsp** コマンドを使用します。

次に、指定されたインターフェイスに関する DHCHAP 設定を表示する例を示します。

```
switch# show fcsp interface fc2/4
fc2/4:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
```

次に、指定されたインターフェイスに関する DHCHAP 統計情報を表示する例を示します。

```
switch# show fcsp interface fc2/4 statistics
```

次に、指定されたインターフェイスに接続されたデバイスの FC-SP WWN を表示する例を示します。

```
switch# show fcsp interface fc2/1 wwn
```

次に、スイッチに設定済みのハッシュ アルゴリズムおよび DHCHAP グループを表示する例を示します。

```
switch# show fcsp dhchap
```

次に、DHCHAP ローカル パスワード データベースを表示する例を示します。

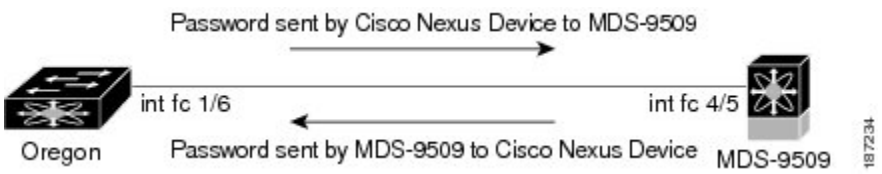
```
switch# show fcsp dhchap database
```

RADIUS サーバおよび TACACS+ サーバにスイッチ情報を設定する場合、デバイス WWN の ASCII 表記を使用してください。

設定例

ここでは、次の図に示した例を設定するための手順について説明します。

図 *2*：*DHCHAP* 認証の例



認証を設定するには、次の作業を行います。

手順の概要

1. ファブリックの Cisco SAN スイッチのデバイス名を取得します。 ファブリックの Cisco SAN スイッチは、スイッチ WWN によって識別されます。
2. このスイッチで DHCHAP を明示的にイネーブルにします。
3. このスイッチのクリア テキスト パスワードを設定します。 このパスワードは、接続先デバイスで使用されます。
4. スイッチWWNデバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。
5. 必要なインターフェイスの DHCHAP モードをイネーブルにします。
6. DHCHAP ローカル パスワード データベースを表示して、このスイッチに設定されたプロトコル セキュリティ情報を確認します。
7. インターフェイスの DHCHAP 設定を表示します。
8. 接続スイッチでこれらの手順を繰り返します。

手順の詳細

ステップ 1 ファブリックの Cisco SAN スイッチのデバイス名を取得します。 ファブリックの Cisco SAN スイッチは、スイッチ WWN によって識別されます。

例：
```
switch# show wwn switch
Switch WWN is 20:00:00:05:30:00:54:de
```

ステップ 2 このスイッチで DHCHAP を明示的にイネーブルにします。

（注） DHCHAP 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。

例：
```
switch(config)# fcsp enable
```

ステップ 3 このスイッチのクリア テキスト パスワードを設定します。 このパスワードは、接続先デバイスで使用されます。

例：
```
switch(config)# fcsp dhchap password rtp9216
```

ステップ 4 スイッチ WWN デバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。

例：
```
switch(config)# fcsp dhchap devicename 20:00:00:05:30:00:38:5e password rtp9509
```

ステップ 5 必要なインターフェイスの DHCHAP モードをイネーブルにします。

（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。

例：
```
switch(config)# interface fc2/4
switch(config-if)# fcsp on
```

ステップ 6 DHCHAP ローカル パスワード データベースを表示して、このスイッチに設定されたプロトコル セキュリティ情報を確認します。

例：
```
switch# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:*******
Other Devices' Passwords:
        Password for device with WWN:20:00:00:05:30:00:38:5e is *******
```

ステップ 7 インターフェイスの DHCHAP 設定を表示します。

例：
```
switch# show fcsp interface fc2/4
fc2/4
        fcsp authentication mode:SEC_MODE_ON
        Status:Successfully authenticated
```

ステップ 8 接続スイッチでこれらの手順を繰り返します。

例：
```
MDS-9509# show wwn switch
Switch WWN is 20:00:00:05:30:00:38:5e
MDS-9509(config)# fcsp enable
MDS-9509(config)# fcsp dhchap password rtp9509
MDS-9509(config)# fcsp dhchap devicename 20:00:00:05:30:00:54:de password rtp9216
MDS-9509(config)# interface fc 4/5
MDS-9509(config-if)# fcsp on
MDS-9509# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:*******
Other Devices' Passwords:
        Password for device with WWN:20:00:00:05:30:00:54:de is *******
MDS-9509# show fcsp interface fc2/4
Fc2/4
        fcsp authentication mode:SEC_MODE_ON
        Status:Successfully authenticated
```

これで、設定例用の DHCHAP 認証が設定およびイネーブルにされました。

デフォルトのファブリック セキュリティ設定値

次の表に、任意のスイッチにおける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 *2*：デフォルトのファブリック セキュリティ設定値

パラメータ	デフォルト
DHCHAP 機能	ディセーブル

パラメータ	デフォルト
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