# 200/220/300シリーズスイッチでの802.1Xホスト およびセッション認証の設定

#### 目的

802.1Xは、ポートに接続されているデバイスに認証方式を提供する、ポートベースのネットワークアクセス制御(PNAC)のIEEE標準です。スイッチの管理GUIの[Host and Session Authentication]ページを使用して、ポート単位で使用する認証タイプを定義します。ポート単位の認証は、ネットワーク管理者が必要な認証タイプに基づいてスイッチポートを分割できるようにする機能です。[Authenticated Hosts]ページには、認証されたホストに関する情報が表示されます。

この記事では、ポート単位でホスト認証とセッション認証を設定する方法、および 200/220/300シリーズマネージドスイッチの802.1Xセキュリティ設定で認証済みホストを表 示する方法について説明します。

# 該当するデバイス

- Sx200シリーズ
- •Sx220シリーズ
- Sx300シリーズ

### [Software Version]

- 1.4.5.02 Sx200シリーズ、Sx300シリーズ
- 1.1.0.14 Sx220シリーズ

# ホストおよびセッションの認証

ステップ 1:Webベースのユーティリティにログインし、[Security] > [802.1X] > [Host and Session Authentication] を選択します。

注:次のイメージは、SG220-26Pスマートスイッチから取得したものです。

<ul> <li>IP Configuration</li> </ul>						
- S	ecurity					
	TACACS+					
	RADIUS					
	Management Access Method					
	Password Strength					
	Management Access Authentication					
	TCP/UDP Services					
	Storm Control					
	Port Security					
•	802.1X					
	Properties					
	Port Authentication					
	Host and Session Authentication					
	Authenticated Hosts					
	Denial of Service					

#### ステップ2:編集するポートのオプションボタンをクリックします。

Host and Session Authentication									
Hos	Host and Session Authentication Table								
	Entry No. Port Host Authen		Host Authentication	Single Host					
				Action on Violation	Traps	Trap Frequency	Number of Violation		
0	1	GE1	Multiple Host						
•	2	GE2	Multiple Host						
0	3	GE3	Multiple Host						
0	4	GE4	Multiple Host						
0	5	GE5	Multiple Host						
0	6	GE6	Multiple Host						
0	7	GE7	Multiple Host						

**注:この**例では、ポートGE2が選択されています。

ステップ 3 : Editをクリックして、指定したポートのホストおよびセッションの認証を編集 します。

Copy Settings	Edit
---------------	------

ステップ 4: [Edit Port Authentication]ウィンドウがポップアップ表示されます。 [Interface]ドロップダウンリストから、指定したポートが手順2で選択したポートであること を確認します。それ以外の場合は、ドロップダウン矢印をクリックして右ポートを選択しま す。

Interface:	Port GE2 🔻
Host Authentication:	<ul> <li>Single Host</li> <li>Multiple Host</li> <li>Multiple Sessions</li> </ul>

**注**:200または300シリーズを使用している場合は、[Edit Host and Session Authentication]ウィンドウが表示されます。

ステップ 5 : [Host Authentication] フィールドで、目的の認証モードに対応するオプション ボタンをクリックします。次のオプションがあります。

- Single Host:スイッチは、ポートへの単一の認可ホストアクセスのみを許可します。
- ・複数のホスト(802.1X):複数のホストが単一のポートにアクセスできます。これはデフォルトモードです。スイッチは最初のホストだけを認証する必要があり、その後、ポートに接続されている他のすべてのクライアントはネットワークにアクセスできます。認証に失敗すると、最初のホストと接続されているすべてのクライアントがネットワークへのアクセスを拒否されます。
- Multiple Sessions:複数のホストが1つのポートにアクセスできますが、各ホストは認証を受ける必要があります。

**注:この**例では、[Single host]が選択されています。



**注**: [Multiple Host]または[Multiple Sessions]を選択した場合は、<u>ステップ9</u>に進みます。

手順 6: [Host Violation Settings]領域で、目的の[Action on Violation]に対応するオプション ボタンをクリックします。元のサプリカントのMACアドレスと一致しないMACアドレスを 持つホストからパケットが到着すると、違反が発生します。これが発生すると、元のサプリ カントと見なされていないホストから着信するパケットに対する処理が決定されます。次の オプションがあります。

- Protect(Discard):パケットをドロップします。これはデフォルトのアクションです。
- Restrict(Forward):アクセスを許可し、パケットを転送します。
- Shutdown:パケットをブロックし、ポートをシャットダウンします。ポートは、再アクティ ブ化されるか、スイッチがリブートされるまでダウンしたままになります。

**注**:この例では、[Restrict (Forward)]が選択されています。

Single Host Violation Settings:

Action on Violation: Protect (Discard) Restrict (Forward) Shutdown

ステップ7:(オプション)[Traps] フィールドの[Enable] をオンにして、トラップを有効に します。トラップは、システムイベントの報告に使用される簡易ネットワーク管理プロトコ ル(SNMP)メッセージを生成します。違反が発生すると、スイッチのSNMPマネージャにト ラップが送信されます。

Single Host Violation Settings:

Action on Violation:	Protect (Discard)			
	Restrict (Forward)			
	Shutdown			
Traps:	🕑 Enable			

ステップ 8 : [Trap Frequency] フィールドに、送信したトラップの間隔を秒単位で入力します。トラップの送信頻度を定義します。

注:この例では、30秒が使用されています。

Single Host Violation	Single Host Violation Settings:						
Action on Violation:	•	Protect (Discard) Restrict (Forward) Shutdown					
Traps:	•	Enable					
🌣 Trap Frequency:	30			sec (Range: 1 - 1000000, Default: 10)			
Apply Close							

<u>ステップ 9 : [</u>Apply] をクリックします。

これで、スイッチでホスト認証とセッション認証が設定されました。

# 認証されたホストの表示

ステップ1:Webベースのユーティリティにログインし、[Security] > [802.1X] > [Authenticated Host] を選択します。

IP Configuration					
• S	ecurity				
	TACACS+				
	RADIUS				
	Management Access Method				
	Password Strength				
	Management Access Authent				
	TCP/UDP Services				
	Storm Control				
	Port Security				
	802.1X				
	Properties				
	Port Authentication				
	Host and Session Authentic				
	Authenticated Hosts				
	Denial of Service				

「認証されたホスト」テーブルには、認証されたホストに関する次の情報が表示されます。

Authenticated Hosts								
Authenticated Host Table								
User Name	Port	Session Time (DD:HH:MM:SS)	Authentication Method	MAC Address	VLAN ID			
0 results found.								

- [User Name]:ポートで認証されたサプリカント名を指定します。
- Port:サプリカントが接続されるポート番号を指定します。
- Session Time:サプリカントがポートに接続された全時間を指定します。形式は DD:HH:MM:SS(日:時:分:秒)です。
- [Authentication Method]:認証に使用する方式を指定します。可能な値は次のとおりです。
- None:サプリカントが認証されなかったことを指定します。

- Radius:サプリカントがRADIUSサーバによって認証されたことを指定します。
- •[MAC Address]:サプリカントのMACアドレスを指定します。
- VLAN ID : ホストが属するVLANを指定します。[VLAN ID]列は、220シリーズSmart Plusスイッチでのみ使用できます。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。