スイッチの用語集

目的

この記事では、Cisco Small Businessスイッチのセットアップ、設定、およびトラブルシューティングに使用される用語のリストを示します。

適用可能なデバイス

- Sx200シリーズ
- Sx250シリーズ
- Sx300シリーズ
- Sx350 シリーズ
- SG300Xシリーズ
- Sx500 シリーズ
- Sx550X シリーズ

用語の一覧

- 802.1Xサプリカント：サプリカントは、802.1X IEEE標準の3つのロールの1つです。802.1Xは、OSIモデルのレイヤ2にセキュリティを提供するために開発されました。サプリカント、オーセンティケータ、認証サーバの各コンポーネントで構成されます。サプリカントとは、ネットワーク上のリソースにアクセスできるようにネットワークに接続するクライアントまたはソフトウェアです。IPアドレスを取得し、その特定のネットワークの一部となるには、クレデンシャルまたは証明書を提供する必要があります。サプリカントは、認証されるまでネットワークのリソースにアクセスできません。
- ACL：アクセスコントロールリスト(ACL)は、セキュリティを向上させるために使用されるネットワークトラフィックフィルタと相関アクションのリストです。特定のリソースへのアクセスをブロックまたは許可するACLには、ネットワークデバイスへのアクセスを許可または拒否するホストが含まれます。ルータやスイッチは各パケットを検査し、アクセスリスト内の指定された基準に基づいて、パケットを転送するか廃棄するかを決定します。アクセスリストの基準には、トラフィックの送信元アドレス、トラフィックの宛先アドレス、上位層プロトコル、またはその他の情報を指定できます。

- IGMPスヌーピング：Internet Group Management Protocol(IGMP)は、スイッチ上で動作するプロトコルで、スイッチはマルチキャストトラフィックについて動的に学習できます。IGMPスヌーピングは、ネットワークスイッチがホストとルータ間のIGMP通信をリッスンできるようにする機能です。IGMPスヌーピングは、グループのマルチキャストトラフィックを、グループに加入しているポートだけに転送するために、ルータで有効になっているフィルタリングメカニズムを実行します。したがって、IGMPスヌーピングを使用すると、ネットワーク上のトラフィックが減少し、ルータの背後にあるホストのパフォーマンスが向上します。マルチキャストは、それらを必要としないリンクからフィルタリングできます。

- IPv4:IPv4は、ネットワーク内のデバイスを識別するために使用される32ビットアドレッシングシステムです。これは、インターネットを含むほとんどのコンピュータネットワークで使用されるアドレッシングシステムです。

- IPv6:IPv6は128ビットのアドレッシングシステムで、ネットワーク内のデバイスを識別するために使用されます。IPv4の後継であり、コンピュータネットワークで使用される最新バージョンのアドレッシングシステムです。IPv6は現在、世界中に展開されています。IPv6アドレスは、16ビットを含む16進数の8つのフィールドで表されます。IPv6アドレスは2つの部分に分割され、各部分は64ビットで構成されます。最初の部分はネットワークアドレスで、2番目の部分はホストアドレスです。

- リンクフラップ：リンクフラップは、スイッチの物理インターフェイスが連続してアップとダウンを繰り返す状況で、少なくとも10秒間が1秒間に3回以上発生します。一般的な原因は、通常、不良、サポートされていない、または非標準のケーブルやSmall Form-Factor Pluggable(SFP)に関連しているか、その他のリンク同期の問題に関連しています。リンクフラッピングの原因は、断続的または永続的な場合があります。

- MACベースのACL：メディアアクセスコントロール(MAC)ベースのアクセスコントロールリスト(ACL)は、送信元MACアドレスのリストです。パケットがワイヤレスアクセスポイント(AP)からローカルエリアネットワーク(LAN)ポートへ、またはその逆に着信する場合、このデバイスはパケットの送信元MACアドレスがこのリスト内のエントリに一致するかどうかをチェックし、フレームの内容と照合してACLルールをチェックします。次に、一致した結果を使用して、このパケットを許可または拒否します。ただし、LANからLANポートへのパケットはチェックされません。

- MLDスヌーピング：マルチキャストは、あるホストからグループ内の選択されたホストにデータパケットを送信するネットワーク層の技術です。下位レイヤでは、スイッチは、1つのホストだけが受信したい場合でも、すべてのポートでマルチキャストトラフィックをブロードキャストします。マルチキャストリスナー検出(MLD)スヌーピングは、IPv6マルチキャストトラフィックを目的のホストにのみ転送するために使用されます。スイッチでMLDスヌーピングが有効になっている場合、IPv6ルータとインターフェイスに接続されているマルチキャストホストの間で交換されるMLDメッセージを検出します。次に、IPv6マルチキャストトラフィックを制限するテーブルを維持し、トラフィックを受信するポートにトラフィックを動的に転送します。

- MSTP:Multiple Spanning Tree Protocol(MSTP)は、単一の物理ネットワーク上の各仮想LAN(VLAN)に対して複数のスパニングツリー（インスタンス）を作成するプロトコルです。これにより、各VLANに設定済みのルートブリッジと転送トポロジを設定できます。これ

により、ネットワーク全体のブリッジプロトコルデータユニット(BPDU)の数が減り、ネットワークデバイスの中央処理装置(CPU)への負荷が軽減されます。

- ポート/VLANミラーリング：ミラーリングは、ネットワークトラフィックの監視に使用される方法です。ポートまたはVLANミラーリングを使用すると、ネットワークデバイスのポート（送信元ポート）での着信パケットと発信パケットのコピーが、パケットが調査される別のポート（ターゲットポート）に転送されます。これは、ネットワーク管理者によって診断ツールとして使用されます。

- ポートセキュリティ：ポートセキュリティの設定は、ネットワークセキュリティを強化する1つの方法です。特定のポートまたはLink Aggregation Group（LAG；リンクアグリゲーショングループ）に設定できます。LAGは、個々のインターフェイスを1つの論理リンクに結合し、最大8つの物理リンクの集約帯域幅を提供します。特定のポート/LAG上の異なるユーザへのアクセスを制限または許可できます。ポートセキュリティは、動的に学習されたスタティックMACアドレスで使用して、ポートの入力トラフィックを制限することもできます。

- プロトコルベースのVLAN：プロトコルベースのグループを定義してポートにバインドできるため、プロトコルグループから発信されるすべてのパケットは、ページ上の設定済みVLANに割り当てられます。プロトコルベースVLANは、必要なプロトコルごとに物理ネットワークを論理VLANグループに分割します。着信パケットでは、フレームがチェックされ、プロトコルタイプに基づいてVLANメンバーシップを決定できます。Protocol-Based Groups to VLANマッピングは、プロトコルグループを単一のポートにマッピングするのに役立ちます。

- QoS:Quality of Service(QoS)により、さまざまなアプリケーション、ユーザ、またはデータフローのトラフィックに優先順位を付けることができます。また、特定のレベルまでパフォーマンスを保証するために使用することもできるため、クライアントのサービス品質に影響を与えます。QoSは一般に、ジッタ、遅延、パケット損失などの要因の影響を受けます。

- RADIUSサーバ：Remote Authentication Dial-In User Service(RADIUS)は、デバイスがネットワークサービスに接続して使用するための認証メカニズムです。これは、中央集中型の認証、認可、アカウンティングの目的で使用されます。RADIUSサーバは、入力されたログインクレデンシャルによってユーザのIDを確認することで、ネットワークへのアクセスを規制します。たとえば、公共のWi-Fiネットワークが大学のキャンパスに設置されているとします。パスワードを持つ受講者だけが、これらのネットワークにアクセスできます。RADIUSサーバは、ユーザが入力したパスワードをチェックし、必要に応じてアクセスを許可または拒否します。

- RSTP：ラピッドスパニングツリープロトコル(RSTP)はSTPの拡張機能です。RSTPは、トポロジ変更後のスパニングツリーコンバージェンスを高速化します。STPがトポロジの変更に応答するのに30 ~ 50秒かかり、RSTPが設定されたhelloタイムの3倍以内に応答する場合があります。RSTPはSTPと下位互換性があります。

- SNMP：簡易ネットワーク管理プロトコル(SNMP)は、ネットワークデバイスに関する情報を保存および共有するためのネットワーク標準です。SNMPは、ネットワーク管理、トラブルシューティング、およびメンテナンスを容易にします。

- スパニングツリー：スパニングツリープロトコル(STP)は、ローカルエリアネットワーク(LAN)で使用されるネットワークプロトコルです。STPの目的は、LANのループフリートポロジを保証することです。STPは、2つのネットワークデバイス間にアクティブパスが1つしかないことを保証するアルゴリズムを使用して、ループを除去します。STPは、トラフィックがネットワーク内で可能な限り最短のパスを通ることを保証します。また、STPは、アクティブなパスに障害が発生した場合に、冗長パスをバックアップパスとして自動的に再び有効にすることもできます。

- SSLサーバ：セキュアソケットレイヤ(SSL)は、主にインターネットでのセキュリティ管理に使用されるプロトコルです。HTTP層とTCP層の間にあるプログラム層を使用する。認証のために、SSLはデジタル署名され、公開キーにバインドされた証明書を使用して、秘密キーの所有者を識別します。この認証は、接続時に役立ちます。SSLを使用して、認証プロセス中にITU-T標準X.509で説明されている形式のブロックで証明書が交換されます。次に、外部機関である証明機関によって、デジタル署名されたX.509証明書が発行されます。

- Syslog集約：Syslogサービスはメッセージを受け入れ、単純な設定ファイルに従ってファイルに保存するか、印刷するだけです。Syslog Aggregationは、インスタンスが発生するたびに同じタイプの複数のsyslogメッセージが画面に表示されないことを意味します。ロギング集約を有効にすると、特定の期間に受信するシステムメッセージをフィルタリングできます。同じタイプのsyslogメッセージをいくつか収集するため、発生時には表示されず、指定された間隔で表示されます。

- TACACS+:Terminal Access Controller Access Control System(TACACS+)はCisco独自のプロトコルで、ユーザ名とパスワードによる認証と許可を提供することでセキュリティを強化するために使用されます。TACACS+サーバを設定するには、ユーザは特権15アクセス権を持つ必要があります。これにより、ユーザはスイッチのすべての設定機能にアクセスできます。一部のスイッチはTACACS+クライアントとして機能し、接続されているすべてのユーザを、適切に設定されたTACACS+サーバを介してネットワーク内で認証および認可できます。TACACS+はIPv4のみをサポートします。

- TFTPサーバ：トリビアルファイル転送プロトコル(TFTP)サーバは、LAN上のデバイス間で設定ファイルとブートファイルを自動的に転送するために使用されるサーバです。このプロトコルはシンプルであるため、メモリの使用量が少なくなりますが、このシンプルさによってプロトコルが容易に危険にさらされることにもなります。このため、TFTPがインターネットで使用されることはほとんどありません。

- VLAN：仮想ローカルエリアネットワーク(VLAN)は、ユーザの物理的な場所に関係なく、機能、エリア、またはアプリケーションによって論理的にセグメント化されたスイッチドネットワークです。VLANは、ネットワーク内の任意の場所に配置でき、同じ物理セグメント上にあるかのように通信するホストまたはポートのグループです。VLANを使用すると、物理接続を変更せずにデバイスを新しいVLANに移動できるため、ネットワーク管理が簡素化されます。

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。