ワイヤレスアクセスポイント用語一覧

目的

この記事では、Cisco Wireless Access Points(WAP)の設定、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。

該当するデバイス

- ワイヤレスアクセスポイント

一般条項のリスト

- 802.1QベースのVLAN:IEEE 802.1Q仕様は、イーサネットフレームにVLANメンバーシップ情報をタグ付けする標準的な方法を確立し、ブリッジされたLANインフラストラクチャ内のVLANトポロジの定義、操作、および管理をできるVLANを定義します。802.1Q標準は、ブロードキャストおよびマルチキャストトラフィックが必要以上の帯域幅を使用しないように、大規模なネットワークを小さな部分に分割する方法の問題に対処することを目的としています。また、内部ネットワークのセグメント間のセキュリティのレベルを高めることも可能です。
- 802.1Xサプリカント：サプリカントは、802.1X IEEE標準の3つの役割の1つです。802.1Xは、OSIモデルのレイヤ2のセキュリティを提供するために開発されました。次のコンポーネントで構成されています。サプリカント、オーセンティケータ、および認証サーバ。サプリカントは、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、セキュリティの向上に使用されるネットワークトラフィックフィルタと関連付けられたアクションのリストです。ユーザが特定のリソースにアクセスするの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ています。ACLは、次の2つの方法のいずれかで定義できます。IPv4アドレスまたはIPv6アドレスによって実行されます。
- バンドステア：高度なロードバランシング（バンドステアリングとも呼ばれます）は、5 GHz帯域で伝送できるデバイスを検出する機能です。2.4 GHz帯域は頻繁に輻輳しており、Bluetoothや電子レンジなどのさまざまなデバイスからの干渉を受けています。この機能により、アクセスポイントはデバイスをより最適な無線周波数に誘導および誘導できるため、ネットワークパフォーマンスが向上します。
- 帯域幅使用率：帯域幅使用率を使用すると、通信パスを介した正常な平均データ転送にしきい値を設定できます。これを改善するために使用される技術の一部は、帯域幅シェーピング、管理、キャッピング、および割り当てです。
- Bonjour:Bonjourでは、マルチキャストDNSを使用してアクセスポイントとそのサービスを検出できます。ネットワークにサービスをアドバタイズし、サポートするサービスタイプのクエリに応答するため、小規模企業の環境でのネットワーク設定が簡素化されます。Bonjourがサポートされ ているWAPデバイスで有効になっている場合、どのBonjourクライアントも、事前の設定なしでWebベースのユーティリティを検出してアクセスできます。BonjourはIPv4ネットワークとIPv6ネットワークの両方で動作します。
- キャプティブポータル：キャプティブポータル方式では、ネットワーク上のLANユーザまたはホストがパブリックネットワークに正常にアクセスする前に、特別なWebページを強制的に表示します。キャプティブポータルは、Webブラウザを認証デバイスにします。Webペー

ジでは、アクセスがネットワークの使用を許可される前に、ユーザの操作または認証が必要です。

- チャネル分離：チャネル管理が有効になっているデバイスは、クラスタ内の他のWAPデバイスにワイヤレス無線チャネルを自動的に割り当てます。チャネルの自動割り当てにより、クラスタ外の他のアクセスポイントとの干渉が軽減され、Wi-Fi帯域幅が最大化され、ワイヤレスネットワーク上の通信の効率が維持されます。
- クライアントQoS：クライアントQuality of Service(QoS)アソシエーションは、ワイヤレスクライアントのQoSをカスタマイズするための追加オプションを提供するセクションです。これらのオプションには、送信、受信、または保証が可能な帯域幅が含まれます。クライアントのQoSアソシエーションは、アクセスコントロールリスト(ACL)を使用してさらに操作できます。
- イベントロギング：システムイベントは、システムをスムーズに実行し、障害を防止するために注意と必要なアクションを必要とするシステム内のアクティビティです。これらのイベントはログとして記録されます。システムログを使用すると、管理者はデバイスで発生した特定のイベントを追跡できます。イベントログは、ネットワークのトラブルシューティング、パケットフローのデバッグ、イベントの監視に役立ちます。
- 高速ローミング：ワイヤレスアクセスポイント間の高速ローミングにより、高速で安全で中断のないワイヤレス接続が可能になり、FaceTime、Skype、Cisco Jabberなどのリアルタイムアプリケーションでシームレスなモバイルエクスペリエンスが実現します。
- HTTPS:Hyper Text Transfer Protocol Secure(HTTPS)は、HTTPよりも安全な転送プロトコルです。アクセスポイントは、HTTP/HTTPSサーバの設定時に、HTTP接続とHTTPS接続の両方を介して管理できます。WebブラウザによってはHTTPを使用するものもあれば、HTTPSを使用するものもあります。HTTPSサービスを使用するには、アクセスポイントに有効なSecure Socket Layer(SSL)証明書が必要です。
- 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、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128ビットのアドレッシングシステムです。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アドレス指定システムの最新バージョンです。IPv6は現在、世界中で展開されています。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、2番目の部分はホストアドレスです。
- LLDP:Link Layer Discovery Protocol(LLDP)は、IEEE 802.1AB標準で定義されている検出プロトコルです。LLDPを使用すると、ネットワークデバイスは自身に関する情報をネットワーク上の他のデバイスにアドバタイズできます。LLDPは、論理リンク制御(LLC)サービスを使用して、他のLLDPエージェントとの間で情報を送受信します。LLCは、LLDPへのアクセスにリンクサービスアクセスポイント(LSAP)を提供します。各LLDPフレームは、単一のMACサービス要求として送信されます。各着信LLDPフレームは、MACサービス指標としてLLCエンティティによってMACサービスアクセスポイント(MSAP)で受信されます。
- ロードバランシング：ロードバランシングは、ワークロードを複数のコンピュータ、ネットワークリンク、およびその他のさまざまなリソースに分散して、適切なリソース使用率、スループットの最大化、応答時間の最大化、および主に過負荷を回避するために使用されるネットワーク用語です。
- MAC ACL：アクセスコントロールリスト(ACL)に基づくメディアアクセスコントロール(MAC)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からLANポートへ、またはその逆の場合、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と一致するかどうかを確認し、ACLルールとフレームの内容を照合しま

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。

- 複数のSSID：アクセスポイントで複数のService Set Identifier(SSID)または仮想アクセスポイント(VAP)を設定し、各SSIDに異なる設定値を割り当てることができます。すべてのSSIDが同時にアクティブになっている可能性があります。クライアントデバイスは、任意のSSIDを使用してアクセスポイントに関連付けることができます。
- 動作モード：WAPデバイスは、単一のポイントツーポイントモードアクセスポイント、ポイントツーマルチポイントブリッジ、リピータとして機能できます。ポイントツーポイントモードでは、単一のWAPデバイスがネットワーク内のクライアントやその他のデバイスからの接続を受け入れます。ポイントツーマルチポイントブリッジモードでは、単一のWAPデバイスは多数のアクセスポイント間の共通リンクとして動作します。WAPデバイスは、互いに遠いアクセスポイント間の接続を確立できるリピータとしても機能します。ワイヤレスクライアントはこのリピータに接続できます。Wireless Distribution System(WDS)の役割システムは、リピータの役割と同様に比較できます。
- パケットキャプチャ：パケットキャプチャは、デバイスで送受信されるパケットをキャプチャおよび保存できるネットワークデバイスの機能です。キャプチャされたパケットは、ネットワークプロトコルアナライザで分析して、トラブルシューティングやパフォーマンスの最適化を行うことができます。キャプチャされたパケットファイルは、HTTP/HTTPSまたはTFTPサーバからダウンロードできます。ネットワーク内のパケットフローを理解するために、共有し、さらに分析することができます。[Packet Capture]ページを使用して、リモートパケットキャプチャまたはローカルパケットキャプチャを設定したり、パケットキャプチャファイルをダウンロードしたり、現在のキャプチャステータスを表示したりできます。
- 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、特定のレベルにパフォーマンスを保証するために使用できるため、クライアントのサービス品質に影響を与えます。QoSは、一般に次の要因によって影響を受けます。ジッタ、遅延、およびパケット損失。
- RADIUSサーバ：リモート認証ダイヤルインユーザサービス(RADIUS)は、デバイスが接続してネットワークサービスを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を使用してユーザのIDを確認することにより、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ネットワークは大学のキャンパスに設置されます。これらのネットワークにアクセスできるのは、パスワードを持つ受講者だけです。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。
- リモート管理：リモート管理は、リモートの場所からネットワークデバイスの設定を操作しています。これは通常、コンピュータ、スイッチ、ルータなど、IPアドレスを持つ多くのデバイスで行われます。ネットワーク管理者は、物理的にオンサイトにいる必要がないため、要求や課題に迅速に対応できます。リモート管理のデバイスへのアクセスは、デバイスのローカルIPアドレスを使用してデバイスにローカルにアクセスする点と、デバイスのWAN IPをリモートデバイスで実行する場合に使用される点を除いて、ほとんどローカルと同じです。
- 不正AP検出：不正アクセスポイント(AP)は、システム管理者から明示的な許可を受けずにネットワークにインストールされたアクセスポイントです。不正なアクセスポイントは、エリアへのアクセス権を持つユーザが知らないうちに、または知らないうちにネットワークに不正なユーザがアクセスできるワイヤレスアクセスポイントを設置できるため、セキュリティ上の脅威となります。アクセスポイントの不正AP検出機能を使用すると、範囲内にある不正アクセスポイントを確認でき、その情報がWebベースのユーティリティに表示されます。[Trusted AP List]に権限のあるアクセスポイントを追加できます。
- RSTP:Rapid Spanning Tree Protocol(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。

- スケジューラ：ワイヤレススケジューラは、仮想アクセスポイント(VAP)または無線が動作する時間間隔をスケジュールするのに役立ち、電力の節約とセキュリティの向上に役立ちます。最大16のプロファイルを異なるVAPまたは無線インターフェイスに関連付けることができますが、各インターフェイスで許可されるプロファイルは1つだけです。各プロファイルには、関連するVAPまたはWLANの稼働時間を制御する一定の時間ルールを設定できます。
- シングルポイントセットアップ：シングルポイントセットアップは、機能をサポートするアクセスポイントグループを導入および管理できる、シンプルなマルチデバイス管理テクノロジーです。アクセスポイントを個別に設定する代わりに、アクセスポイントのグループを単一のポイントから設定する利便性を提供します。また、アクセスポイントをローカルまたはリモートで管理することもできます。
- SNMP:Simple Network Management Protocol(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、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確実にすることです。STPは、2つのネットワークデバイス間にアクティブなパスが1つだけであることを保証するアルゴリズムを通じ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。STPは、アクティブパスに障害が発生すると、バックアップパスとして冗長パスを自動的に再び有効にすることもできます。
- SSID:Service Set Identifier(SSID)は、無線クライアントが無線ネットワーク内のすべてのデバイスに接続または共有できる一意の識別子です。大文字と小文字を区別し、32文字以下の英数字を使用してください。これは、ワイヤレスネットワーク名とも呼ばれます。
- SSIDブロードキャスト：ワイヤレスデバイスが接続できるワイヤレスネットワークをエリアで検索すると、その範囲内のワイヤレスネットワークがネットワーク名またはSSIDを通じて検出されます。SSIDのブロードキャストはデフォルトで有効になっています。ただし、無効にすることもできます。
- TSPEC：トラフィック仕様(TSPEC)は、QoS対応のワイヤレスクライアントからWAPデバイスに送信されるトラフィック仕様で、それが表すトラフィックストリーム(TS)に対して一定量のネットワークアクセスを要求します。
- 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でき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。
- WDS:Wireless Distribution System(WDS)は、ネットワーク内のアクセスポイントのワイヤレス相互接続を可能にする機能です。これにより、ユーザは複数のアクセスポイントをワイヤレスでネットワークを拡張できます。また、WDSは、アクセスポイント間のリンク間でクライアントフレームのMACアドレスを保持します。この機能は、クライアントのローミングにシームレスなエクスペリエンスを提供し、複数のワイヤレスネットワークの管理を可能にするため、重要です。
- WMM:Wi-Fi Multimedia(WMM)は、異なる種類のトラフィックに異なるプロセス優先順位を割り当てる機能です。WMMは、次の4つのカテゴリに基づいてワイヤレスデータパケットの優先順位を設定することによって、ワイヤレスネットワークのパフォーマンスを向上させるQoS機能でもあります。音声、ビデオ、ベストエフォート、バックグラウンド。デフォルト

では、WMMは有効になっています。アプリケーションにWMMが必要ない場合は、ビデオや音声よりも低い優先順位が与えられます。
- [Wireless Isolation]：異なるSSIDに接続されているコンピュータ間の通信とファイル転送を防止します。1つのSSID上のトラフィックは、他のSSIDには転送されません。
- WPA/WPA2:Wi-Fi Protected Access（WPAおよびWPA2）は、ワイヤレスネットワーク上で送信されるデータを暗号化してプライバシーを保護するために、ワイヤレスネットワークで使用されるセキュリティプロトコルです。WPAとWPA2は、どちらもIEEE 802.11eおよび802.11iと上位互換性があります。WPAおよびWPA2では、Wired Equivalent Privacy(WEP)セキュリティプロトコルと比較して、認証および暗号化機能が向上しています。

メッシュネットワークの用語リスト

- **アクセスポイント(AP)**:ユーザがネットワークにワイヤレスで接続するために使用されるネットワーク内のデバイス。この機能に応じて、特定のラベルを追加できます。プライマリ、リモート、ルート、下位など
- **ワイヤレスメッシュネットワーク**：無線アクセスポイントが相互に接続してリレー情報を提供するトポロジのタイプ。これらのネットワークは、ニーズを調整し、すべてのユーザの接続を維持するために動的に動作します。
- **プライマリAP**:プライマリAPは、ワイヤレスネットワークとトポロジの管理と制御を行います。これは、インターネットサービスプロバイダー(ISP)を使用する外部ネットワーク（通常はインターネット）の残りの部分へのブリッジです。 プライマリAPは、WAN ISPインターフェイスにトラフィックをルーティングする宅内ルータに直接リンクします。プライマリAPは、メッシュネットワーク内でワイヤレスサービスを提供するすべてのノードのオーケストレータです。ネットワーク上のノードからの情報、各クライアント接続品質、およびネイバー情報を管理して、モバイルクライアントへの最適化されたワイヤレスサービスの最適ルートを決定します。
- **プライマリ**：WLANの管理を担当する現在のAP。
- **優先プライマリ**：特定のプライマリ対応APが優先としてリストされる設定。プライマリAPに障害が発生すると、優先プライマリAPが引き継ぎます。優先APがバックアップされると、自動的にスイッチオーバーされません。優先プライマリを指定していません。
- **プライマリ対応AP**:ネットワークに戻る物理的な有線接続を持つAP。このAPはイーサネットに接続する必要があり、プライマリAPに障害が発生するとプライマリAPになる可能性があります。
- **メッシュエクステンダ**：有線ネットワークに接続されていないネットワーク内のリモートの下位AP。
- **下位AP**:プライマリとして設定されていないメッシュAPに適用できる一般的な用語。
- **親AP**:親APは、プライマリAPへの最適なルートを提供するAPです。
- **子AP**:子APは、親APをプライマリAPへの最適ルートとして選択するメッシュエクステンダです。
- **アップストリームAP**:アップストリームAPは、クライアントからサーバに向かう際にAPを通過する方向を指す一般的な用語です。
- **ダウンストリームAP**:ダウンストリームAPは、インターネットからクライアントにデータを伝送します。
- **共存AP**:バックホールチャネルのブロードキャスト範囲内にあるメッシュエクステンダ。
- **ノード**：この記事では、APをノードと呼びます。一般に、ノードは、ネットワーク内で接続や対話を行うデバイス、または情報の送信、受信、保存、インターネットとの通信、およびIPアドレスを持つデバイスを記述します。メッシュネットワークでは、すべてのノードで最適化された無線パラメータによって最大の無線カバレッジが保証され、ノード間の無線干渉が軽減され、優れたデータ速度とスループットが提供されます。

- **バックホール:**ワイヤレスメッシュネットワークでは、インターネットに到達するために、ローカルエリアネットワーク(LAN)の情報を有線アクセスポイントに到達する必要があります。バックホールは、その情報を有線アクセスポイントに戻すプロセスです。