URWBモードの産業用ワイヤレスアクセスポイントでのSNMPの設定

内容

はじめに

このドキュメントでは、URWBモードで動作するSNMP産業用ワイヤレスアクセスポイント(AP)の設定およびトラブルシューティングについて説明します。

SNMPの基本

簡易ネットワーク管理プロトコル(SNMP)は、IPネットワーク上のデバイスを管理および監視するために広く使用されているプロトコルです。ネットワーク管理者は、デバイスに関する情報を収集して、円滑な運用を確保できます。SNMPは、ネットワーク監視を監視するSNMPマネージャと、管理対象デバイス上に存在するSNMPエージェントとの間でメッセージを交換することによって動作します。このプロトコルでは、Management Information Base（MIB；管理情報ベース）という変数の階層データベースを使用して、アクセスや変更が可能な情報を定義して保存します。GET（情報を取得）、SET（構成を変更）、TRAP（アラートを受信）などのさまざまなSNMP操作を通じて、管理者はネットワークの健全性の監視、パフォーマンスの追跡、障害の検出、およびデバイスの設定をリモートで行うことができます。

簡易ネットワーク管理プロトコル(SNMP)プロトコルは、ネットワーク管理機能のためにURWBソフトウェアで使用されます。

SNMPクライアント（任意のモニタリングアプリケーション）は、CURWB無線で実行されているSNMPエージェントに要求を送信します。SNMPエージェントはサブエージェントに要求を渡します。サブエージェントがSNMPエージェントに応答します。SNMPエージェントは、SNMP応答パケットを作成し、要求を開始するリモートネットワーク管理アプリケーションに送信します。

SNMPのバージョン

SNMPは複数のバージョンを経て進化し、各バージョンでセキュリティと機能が強化されています。元のバージョンであるSNMPv1は、基本的なモニタリング機能を提供しますが、アクセス制御に単純なコミュニティストリングを使用するなど、強力なセキュリティは備えていません。SNMPv2cではパフォーマンスが向上し、新しい操作が追加されましたが、SNMPv1と同じ制限付きセキュリティモデルが維持されました。最新バージョンのSNMPv3では、認証や暗号化などの堅牢なセキュリティ機能が導入されており、セキュアなネットワーク管理に最適な選択肢となっています。SNMPv1とSNMPv2cはレガシーシステムでも広く使用されていますが、セキュリティとデータ保護機能が強化されているため、ほとんどのネットワークにSNMPv3を推奨します。

コンフィギュレーション

V2の設定

次のCLIコマンドを使用してSNMPを有効にします。

```
Device#configure snmp enable
```

SNMPプロトコルバージョンを指定するには、次のCLIコマンドを使用します。

```
Device#configure snmp version v2c
```

SNMP v2cコミュニティID番号（SNMP v2cのみ）を指定するには、次のCLIコマンドを使用します。

```
Device#configure snmp v2c community-id
```

以下に例を挙げます。

Device#configure snmp v2c community-id MytestPa$$word!

V3の設定

SNMP v3では、認証と暗号化を設定する必要があります。

次のCLIコマンドを使用してSNMPを有効にします。

```
Device#configure snmp enable
```

SNMPプロトコルバージョンを指定するには、次のCLIコマンドを使用します。

```
Device#configure snmp version v3
```

SNMP v3ユーザ名（SNMP v3のみ）を指定するには、次のCLIコマンドを使用します。

```
Device#configure snmp v3 username
```

SNMP v3ユーザパスワード（SNMP v3のみ）を指定するには、次のCLIコマンドを使用します。

```
Device#configure snmp v3 password
```

SNMP v3認証プロトコル（SNMP v3のみ）を指定するには、次のCLIコマンドを使用します。

```
Device#configure snmp auth-method
```

SNMP v3暗号化プロトコル（SNMP v3のみ）を指定するには、次のCLIコマンドを使用します。

```
Device#configure snmp encryption {des | aes | none}
```

トラップの有効化

SNMPトラップは、SNMPエージェント（この場合はIW無線）からSNMPマネージャ（任意の監視アプリケーション）に送信される非同期通知で、エラー、リブート、パフォーマンスしきい値の超過など、デバイスのステータスの重要なイベントや変更をアラートで通知します。通常のポーリングとは異なり、トラップではデバイスが問題の発生時に自動的にレポートを作成できるため、ネットワークの問題を迅速に検出して解決できます。

SNMPイベントトラップを有効または無効にするには、次のCLIコマンドを使用します。

```
Device#configure snmp event-trap {enable | disable}
```

アプリケーションが実行されているネットワーク監視サーバのホスト名またはIPアドレスを指定するには、次のCLIコマンドを使用します。

```
Device#configure snmp nms-hostname {hostname |Ip Address}
```

SNMP定期トラップの設定を指定するには、次のCLIコマンドを使用します。

```
Device#configure snmp periodic-trap {enable | disable}
```

定期的なSNMPトラップの通知トラップ期間を指定するには、次のCLIコマンドを使用します。

```
Device#configure snmp trap-period <1-2147483647>
```

サポートされたMIB

IW9167Eでサポートされ ているMIBを次に示します

- UCD-SNMP-MIB（.1.3.6.14.1.2021部分的にサポート）
- IF-MIB（.1.3.6.1.2.1.2部分的にサポート）
- CISCO-URWB-MIB(1.3.6.1.4.1.9.9.1056)

SNMPサービスの検証

コマンド「show system status snmpd」を使用すると、デバイスのSNMPエージェントが実行されているかどうかを確認できます（バージョン17.9.x）

SNMPv2が有効な場合：

MP_TRK_Backhaul#show snmp

SNMP：有効

バージョン：v2c

コミュニティID: mytest123!

Periodic Trap：無効

イベントトラップ：無効

SNMPv3が有効な場合：

MP_TRK_Backhaul#show snmp

SNMP：有効

バージョン：v3

ユーザ名：snmpadmin

パスワード：Mytest12349!

認証方式：MD5

暗号化：AES

暗号化パスフレーズ：Mytest12349!

エンジンID: 0x800000090368790989fa94

Periodic Trap：無効

イベントトラップ：無効

設定は、show runコマンドを使用して確認することもできます。このコマンドのSNMP設定は、Advanced Configセクションの下にあります。

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。