アクセス ポイントで Ethertype フィルタを使用して IPX トラフィックをブロックする方法

目次

概要
前提条件
要件
使用するコンポーネント
表記法
アクセスポイントへの接続
設定
VxWorks が稼働するアクセスポイント
Cisco IOS ソフトウェアが稼働するアクセス ポイント
確認
トラブルシューティング
関連情報

概要

このドキュメントでは、Ethertype フィルタを使用して、Cisco Aironet アクセス ポイントの Internetwork Packet Exchange (IPX) トラフィックをブロックする方法について説明します。 これが役立つ一般的な状況は、大規模な企業ネットワークで時々発生する、IPX サーバのブロードキャストがワイヤレス リンクを抑制する場合です。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントは、VxWorks または Cisco IOS® ソフトウェアを実行する Cisco Aironet アクセス ポイントに適用されます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、コマンドを使用する前にその潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

アクセスポイントへの接続

Web ブラウザまたはターミナル エミュレータを持つアクセスポイントのシリアル ポートを介してアクセスポイントの管理システムを開くことができます。 アクセス ポイントに接続する方法に慣れていない場合は、『Web ブラウザ インターフェイスを使用する』で VxWorks を実行するアクセス ポイントに接続する方法を参照するか、『Web ブラウザ インターフェイスを使用する』で Cisco IOS ソフトウェアを実行するアクセス ポイントに接続する方法を参照します。

設定

VxWorks が稼働するアクセスポイント

アクセス ポイントへのブラウザ接続を確立できたら、次の手順を実行し、IPX トラフィックをブロックするフィルタを設定し適用します。

フィルタの作成

次の手順を実行します。

1. [Setup] メニューで、[Ethertype Filters] を選択します。
2. [Set Name] フィールドで、フィルタ名 (たとえば「BlockIPX」) を入力し、[Add New] をクリックします。
3. 次のページで、デフォルトの処理が表示されます。 選択できるオプションは、*forward* と *block* のいずれかです。 ドロップダウン メニューから [forward] を選択します。
4. [Special Cases] フィールドで **0x8137** と入力し、[Add New] をクリックします。
5. 新しいウィンドウが表示され、次のオプションが示されます。評価Priorityユニキャスト存続時間マルチキャスト存続時間アラート処理には、[Block] を選択します。 その他のオプションは、そのデフォルト設定のままにします。 [OK] をクリックします。[Ethertype Filter Set] 画面に戻ります。 ステップ 4 とステップ 5 を繰り返し、**0x8138**、**0x00ff**、および **0x00e0** のタイプを追加します。

フィルタの適用

フィルタが作成された後、有効にするにはインターフェイスに適用する必要があります。

1. [Setup] ページに戻ります。 [Network Ports] セクションの [Ethernet] という行で、[Filters] をクリックします。
2. [EtherType] に [Receive] と [Forward] が設定されています。 各ドロップダウン メニューから、[Create a Filter] のステップ 2 で作成したフィルタを選択し、[OK] をクリックします。 この手順により、作成したフィルタが有効になります。

Cisco IOS ソフトウェアが稼働するアクセス ポイント

フィルタの作成

次の手順を実行します。

1. ページ ナビゲーション バーの [Services] をクリックします。
2. [Services] ページ リストで [Filters] をクリックします。
3. [Apply Filters] ページで、ページの最上部にある [Ethertype Filters] タブをクリックします。
4. [Create/Edit Filter Index] メニューで [NEW]（デフォルト）が選択されていることを確認します。 既存のフィルタを編集するには、[Create/Edit Filter Index] メニューからフィルタ番号を選択します。
5. [Filter Index] フィールドで、フィルタに 200 ~ 299 の範囲で番号を付けます。 割り当てた番号で、フィルタのアクセス コントロール リスト（ACL）が作成されます。
6. [Add Ethertype] フィールドに **0x8137** と入力します。
7. [Mask] フィールドの Ethertype のマスクは、デフォルト値のままにします。
8. [Action] メニューから、[Block] を選択します。
9. [Add] をクリックします。 追加した Ethertype が [Filters Classes] フィールドに表示されます。
10. [Filters Classes] リストから Ethertype を削除するには、その Ethertype を選択して [Delete Class] をクリックします。 ステップ 6 からステップ 9 を繰り返し、**0x8138**、**0x00ff**、および **0x00e0** のタイプをフィルタに追加します。
11. [Default Action] メニューから [Forward All] を選択します。 このフィルタを使用してすべての IPX パケットをブロックするので、すべての他のパケットに適用されるデフォルトのアクションが必要です。
12. [Apply] をクリックします。

フィルタの適用

この時点でこのフィルタはアクセス ポイントに保存されていますが、[Apply Filters] ページで適用するまで有効化されません。

1. [Apply Filters] タブをクリックして [Apply Filters] ページに戻ります。
2. [Ethertype] ドロップダウン メニューの 1 つから、フィルタ番号を選択します。 フィルタはイーサネット ポートと無線ポートのいずれか、または両方に適用できます。また、受信パケットか送信パケット、または両方に適用することも可能です。
3. [Apply] をクリックします。 選択したポートで、このフィルタが有効化されます。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- ワイヤレス LAN 製品に関するサポート
- ワイヤレス LAN テクノロジーに関するサポート

- ワイヤレス LAN ソフトウェア
- テクニカル サポートとドキュメント – Cisco Systems