目次

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する固有の要件はありません。

使用するコンポーネント

この資料は Cisco Aironet に VxWorks か Cisco IOS® ソフトウェアを実行するアクセス ポイントを加えます。

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、クリアな（デフォルト）設定で作業を開始しています。 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 ポイントに接続して下さい

Webブラウザまたはターミナル エミュレータのアクセス ポイント シリアルポートを通してアクセス ポイントの管理 システムを開くことができます。 方法の方向のためのウェブブラウザインターフェイスを使用して VxWorks、か 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のにウェブブラウザインターフェイスを使用することを実行するアクセス ポイントに接続するアクセス ポイントに接続する方法と不慣れ参照すればなら。

設定

VxWorks を実行するアクセス ポイント

アクセス ポイントにブラウザ接続を確立したら、フィルタを IPXトラフィックをブロックするために設定および適用するようにこれらのステップを実行して下さい。

フィルタを作成して下さい

次の手順を実行します。

1. Setup メニューの下で、『Ethertype Filters』 を選択 して下さい。
2. Set Name フィールドでは、フィルタ名前を (たとえば、「BlockIPX」) 入力し、『Add New』 をクリック して下さい。
3. Next ページで、デフォルト 開封を見ます。 2 つのオプションは *前方*および *ブロック*です。 ドロップダウン メニューから『forward』 を選択 して下さい。
4. Special Cases フィールドでは、**0x8137 を**入力し、『Add New』 をクリック して下さい。
5. New ウィンドウはこれらのオプションと表示する:開封Priorityユニキャスト 存続可能時間マルチキャスト 存続可能時間アラート開封に関しては、『Block』 を選択 して下さい。 デフォルト設定でその他のオプションを残して下さい。 [OK] をクリックします。Ethertype Filter Set 画面に戻ります。 ステップ 4 およびステップ 5 を繰り返し、型 **0x8138**、**0x00ff** および **0x00e0 を**追加して下さい。

フィルタを適用して下さい

フィルタが作成されれば実施されるために、インターフェイスに適用する必要があります。

1. セットアップページに戻って下さい。 行によってマークされるイーサネットの Network Ports セクションの下で、『Filters』 をクリック して下さい。
2. レシーブおよび前方設定との EtherType を見ます。 各ドロップダウン メニューから、作成のステップ 2 でフィルタ プロシージャを作成した選択し、『OK』 をクリック して下さいフィルタを。 このステップは作成したフィルタをアクティブにします。

Cisco IOSソフトウェアを実行するアクセス ポイント

フィルタを作成して下さい

次の手順を実行します。

1. ページ ナビゲーション バーで『Services』 をクリック して下さい。
2. Services ページ リストで、『Filters』 をクリック して下さい。

3. Apply Filters ページで、ページの上で **Ethertype Filters タブを**クリックして下さい。
4. （デフォルト）Create/Edit Filter Index メニューで選択されることを**新しいことを**確かめて下さい。 既存のフィルタを編集したい場合 Create/Edit Filter Index メニューからフィルタ番号を選択して下さい。
5. [Filter Index] フィールドで、200 ~ 299 の範囲の番号でフィルタ名を設定します。 割り当てる数はフィルタのための Access Control List（ACL）を作成します。
6. Add Ethertype フィールドで **0x8137 を**入力して下さい。
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 して下さい。
9. [Add] をクリックします。 Ethertype は Filters Classes フィールドに現われます。
10. Ethertype を Filters Classes リストから取除くために、それを選択し、『Delete Class』 をクリック して下さい。 ステップ 6 からステップ 9 を繰り返し、フィルタに型 **0x8138**、**0x00ff** および **0x00e0 を**追加して下さい。
11. Default Action メニューから『Forward All』 を選択 して下さい。 このフィルタのすべての IPX パケットをブロックするので、他のすべてのパケットに適用するデフォルト アクションを持たなければなりません。
12. [Apply] をクリックします。

フィルタを適用して下さい

フィルタはアクセス ポイントで、この時点で、保存されましたが、Apply Filters ページでそれを加えるまで有効に なりません。

1. Apply Filters ページに戻るために **Apply Filters タブを**クリックして下さい。
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て下さい。 どちらかまたはイーサネットおよび無線ポート両方とどちらかまたは着信およびアウトゴーイングパケットにフィルタを適用できます。
3. [Apply] をクリックします。 フィルタは選択されたポートで有効に なります。

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

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