CHAPTER 15

フィルタの設定

この章では、Web ブラウザ インターフェイスを使用して、アクセス ポイント / ブリッジに media access control（MAC; メディア アクセス制御）アドレス、IP、および Ethertype フィルタを設定し、管理する方法について説明します。この章の内容は、次のとおりです。

フィルタの概要

プロトコル フィルタ（IP プロトコル、IP ポート、および Ethertype）は、アクセス ポイント / ブリッジのイーサネット ポートや無線ポートを通じた、特定プロトコルの使用を許可または禁止するために使用します。プロトコル フィルタは個別に、または複数をまとめて設定することができます。無線クライアント デバイス、または有線 LAN 上のユーザ、あるいはその両方について、プロトコルをフィルタできます。たとえば、アクセス ポイント / ブリッジの無線ポートに SNMP フィルタを設定すると、無線クライアントはアクセス ポイント / ブリッジで SNMP を使用できなくなります。しかし、有線 LAN からの SNMP アクセスは排除されません。

IP アドレス フィルタや MAC アドレス フィルタによって、特定の MAC アドレスに対して送受信されるユニキャストおよびマルチキャスト パケットの転送が許可または禁止されます。指定以外のすべてのアドレスにトラフィックを転送するフィルタを作成することも、指定以外のすべてのアドレスへのトラフィックを排除するフィルタを作成することもできます。

フィルタの設定には、Web ブラウザ インターフェイスを使用するか、または command-line interface（CLI; コマンドライン インターフェイス）にコマンドを入力します。

ヒント　アクセス ポイント / ブリッジの QoS（Quality Of Service）ポリシーにフィルタを追加することもできます。QoS ポリシーの設定手順の詳細は、第 14 章「QoS（Quality Of Service）の設定」を参照してください。

CLI を使用したフィルタの設定

IOS コマンドを使用してフィルタを設定するには、Access Control List（ACL; アクセス コントロール リスト）とアクセス ポイント / ブリッジ グループを使用します。これらの概念に関する説明や実装手順については、以下の資料を参照してください。

- 『Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2』。次のリンクをクリックすると、「Configuring Transparent Bridging」の章を参照できます。
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcfpart1/bcftb.htm
- 『Catalyst 4908G-L3 Cisco IOS Release 12.0(10)W5(18e) Software Feature and Configuration Guide』。次のリンクをクリックすると、「Command Reference」の章を参照できます。
  http://www.cisco.com/univercd/cc/td/doc/product/l3sw/4908g_l3/ios_12/10w518e/config/cmd_ref.htm

Web ブラウザ インターフェイスを使ったフィルタの設定

この項では、Web ブラウザ インターフェイスを使用してフィルタを設定し、有効化する方法について説明します。フィルタを設定し有効化する手順は、次の 2 つに分かれます。

1. フィルタの設定ページを使用して、フィルタに名前をつけ、設定します。
2. Apply Filters ページを使用して、フィルタを有効化します。

次の項では、3 種類のフィルタの設定および有効化について説明します。

- MAC アドレス フィルタの設定と有効化（P. 15-3）
- IP フィルタの設定と有効化（P. 15-8）
- Ethertype フィルタの設定と有効化（P. 15-12）

MAC アドレス フィルタの設定と有効化

MAC アドレス フィルタによって、特定の MAC アドレスに対して送受信されるユニキャストおよびマルチキャスト パケットの転送が許可または禁止されます。指定以外のすべての MAC アドレスにトラフィックを転送するフィルタを作成することも、指定以外のすべての MAC アドレスへのトラフィックを排除するフィルタを作成することもできます。作成したフィルタはイーサネット ポートと無線ポートのどちらか、またはこの両方に適用できます。また、受信パケットか送信パケット、またはこの両方に適用することも可能です。

（注）　CLI を使用した場合、フィルタに設定できる MAC アドレスは最大 2,048 個です。Web ブラウザ インターフェイスを使用した場合、フィルタに設定できる MAC アドレスは最大 43 個です。

（注）　MAC アドレス フィルタは強力なので、フィルタの設定を間違えると、自分自身をアクセス ポイント / ブリッジからロックアウトしてしまう可能性があります。誤ってアクセス ポイント / ブリッジから自分自身をロックアウトしてしまった場合は、CLI を使用してフィルタを無効にするか、アクセス ポイント / ブリッジ パワー インジェクタの Mode ボタンを使用してアクセス ポイント / ブリッジをデフォルトにリセットします。

MAC Address Filters ページを使用して、アクセス ポイント / ブリッジの MAC アドレス フィルタを作成します。図 15-1 は、MAC Address Filters ページを示しています。

図 15-1　MAC Address Filters ページ

次のリンク パスに従って、MAC Address Filters ページを表示します。

1. 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 **MAC Address Filters** タブをクリックします。

MAC アドレス フィルタの作成

MAC アドレス フィルタを作成する手順は、次のとおりです。

ステップ 1　リンク パスに従って、MAC Address Filters ページを表示します。

ステップ 2　新規 MAC アドレス フィルタを作成する場合、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。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。

ステップ 3　Filter Index フィールドに、700 ～ 799 までの数字を使ってフィルタ名を入力します。ここで指定した数字により、この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。

ステップ 4　Add MAC Address フィールドに MAC アドレスを入力します。アドレスは、たとえば 0005.9a39.3456 のように、ピリオドを使って、4 つの英数字からなる 3 つのグループに分けて入力します。

（注）　フィルタが確実に正しく動作するようにするには、MAC アドレスで使用する文字をすべて小文字で入力してください。

ステップ 5　Mask 入力フィールドには、フィルタが MAC アドレスに対して左から右にチェックするビット数を入力します。たとえば、MAC アドレスと正確に一致させる（すべてのビットをチェックする）には、**0000.0000.0000** を入力します。先頭 4 バイトだけをチェックするには、**0.0.FFFF** と入力します。

ステップ 6　Action メニューから **Forward** または **Block** を選択します。

ステップ 7　**Add** をクリックします。追加した MAC アドレスが Filters Classes フィールドに表示されます。Filters Classes リストから MAC アドレスを削除するには、そのアドレスを選択して **Delete Class** をクリックします。

ステップ 8　このフィルタにさらにアドレスを追加するには、ステップ 4 から ステップ 7 を繰り返します。

ステップ 9　Default Action メニューから **Forward All** または **Block All** を選択します。このフィルタのデフォルト アクションは、フィルタに含まれる少なくとも 1 つのアドレスのアクションの逆である必要があります。たとえば、複数のアドレスを入力したときに、これらのアドレスすべてに対するアクションとして **Block** を選択した場合、フィルタのデフォルト アクションには **Forward All** を選択する必要があります。

ヒント　許可された MAC アドレスのリストは、ネットワーク上の認証サーバに作成できます。MAC ベースの認証の使用方法については、第 10 章「認証タイプの設定」を参照してください。

ステップ 10　**Apply** をクリックします。このフィルタはアクセス ポイント / ブリッジに保存されますが、Apply Filters ページで適用するまで有効化されません。

ステップ 11　**Apply Filters** タブをクリックして、Apply Filters ページに戻ります。図 15-2 は、Apply Filters ページを示しています。

図 15-2　Apply Filters ページ

ステップ 12　MAC 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どちらか、またはこの両方に適用できます。また、受信パケットか送信パケット、またはこの両方に適用することも可能です。

ステップ 13　**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。

クライアントがただちにフィルタされない場合は、System Configuration ページの **Reload** をクリックして、アクセス ポイント / ブリッジを再起動します。System Configuration ページを表示するには、タスク メニューの **System Software** をクリックしてから、**System Configuration** をクリックします。

MAC アドレス ACL を使用した、アクセス ポイントへのクライアント アソシエーションの許可と禁止

MAC アドレス ACL を使用して、アクセス ポイントへのクライアント アソシエーションを許可または禁止できます。インターフェイスを通過するトラフィックをフィルタする代わりに、ACL を使用して、アクセス ポイントの無線とのアソシエーションをフィルタします。

ACL を使用してアクセス ポイントの無線へのアソシエーションをフィルタする手順は、次のとおりです。

ステップ 1　「MAC アドレス フィルタの作成」の項（P. 15-4）のステップ 1 ～ 10 に従って、ACL を作成します。アソシエートを許可する MAC アドレスについては、Action メニューから **Forward** を選択します。アソシエートを禁止するアドレスについては、**Block** を選択します。Default Action メニューから **Block All** を選択します。

ステップ 2　**Security** をクリックして、Security Summary ページを表示します。図 15-3 は、Security Summary ページを示しています。

図 15-3　Security Summary ページ

ステップ 3　**Advanced Security** をクリックして、Advanced Security: MAC Address Authentication ページを表示します。図 15-4 は、MAC Address Authentication ページを示しています。

図 15-4　Advanced Security: MAC Address Authentication ページ

ステップ 4　**Association Access List** タブをクリックして、Association Access List ページを表示します。図 15-5 は、Association Access List ページを示しています。

図 15-5　Association Access List ページ

ステップ 5　ドロップダウン メニューから、必要な MAC アドレス ACL を選択します。

ステップ 6　**Apply** をクリックします。

次に、「MAC アドレス ACL を使用した、アクセス ポイントへのクライアント アソシエーションの許可と禁止」の項（P. 15-6）に記載された手順と同じ働きをする CLI コマンドの例を示します。

```
ap# configure terminal
ap(config)# dot11 association access-list 777
ap(config)# end
```

この例では、アクセス リスト 777 にリストされている MAC アドレスを持つクライアント デバイスだけが、アクセス ポイントへのアソシエートを許可されます。その他の MAC アドレスはすべて、アソシエーションがブロックされます。

この例で使用されているコマンドの詳細は、『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges』を参照してください。

IP フィルタの設定と有効化

IP フィルタ（IP アドレス、IP プロトコル、および IP ポート）は、アクセス ポイント / ブリッジのイーサネット ポートや無線ポートを通じた、特定のプロトコルの使用を許可または禁止するために使用します。また、IP アドレス フィルタを使用して、特定の IP アドレスとの間で送受信されるユニキャスト パケットやマルチキャスト パケットの転送を許可または禁止できます。指定以外のすべてのアドレスにトラフィックを転送するフィルタを作成することも、指定以外のすべてのアドレスへのトラフィックを排除するフィルタを作成することもできます。IP フィルタ方法の 1 つ、2 つ、または 3 つすべての要素を含むフィルタを作成できます。作成したフィルタはイーサネット ポートと無線ポートのどちらか、またはこの両方に適用できます。また、受信パケットか送信パケット、またはこの両方に適用することも可能です。

IP Filters ページを使用して、アクセス ポイント / ブリッジの IP フィルタを作成します。図 15-6 は、IP Filters ページを示しています。

図 15-6　IP Filters ページ

IP Filters ページは、次のリンク パスに従って表示します。

1. 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 **IP Filters** タブをクリックします。

IP フィルタの作成

IP フィルタを作成する手順は、次のとおりです。

ステップ 1　リンク パスに従って、IP Filters ページを表示します。

ステップ 2　新規フィルタを作成する場合、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名を選択します。

ステップ 3　Filter Name フィールドに、新しいフィルタにつける、わかりやすい名前を入力します。

ステップ 4　フィルタのデフォルト アクションとして、Default Action メニューから **Forward All** または **Block All** を選択します。このフィルタのデフォルト アクションは、フィルタに含まれる少なくとも 1 つのアドレスのアクションの逆である必要があります。たとえば、IP アドレス、IP プロトコル、IP ポートに適用されるフィルタを作成し、これらすべてに対するアクションとして **Block** を選択した場合、フィルタのデフォルト アクションには **Forward All** を選択する必要があります。

ステップ 5　IP アドレスをフィルタするには、IP Address フィールドにアドレスを入力します。

（注）　許可された IP アドレスを除き、すべての IP アドレスへのトラフィックを禁止する場合は、許可された IP アドレスのリストに自分の PC のアドレスを入力し、アクセス ポイント / ブリッジへの接続が失われないようにします。

ステップ 6　Mask フィールドに、この IP アドレスで使用するマスクを入力します。このマスクは、たとえば、112.334.556.778 のように、ピリオドを使って、文字のグループに分けて入力します。マスクに 255.255.255.255 を指定した場合、このアクセス ポイント / ブリッジはすべての IP アドレスを受け付けるようになります。0.0.0.0 を指定した場合、IP Address フィールドに入力した IP アドレスと完全に一致するアドレスがアクセス ポイント / ブリッジによって検索されます。このフィールドに入力したマスクは、CLI に入力したマスクと同様の動作をします。

ステップ 7　Action メニューから **Forward** または **Block** を選択します。

ステップ 8　**Add** をクリックします。追加したアドレスが Filters Classes フィールドに表示されます。Filters Classes リストからアドレスを削除するには、そのアドレスを選択して **Delete Class** をクリックします。このフィルタにさらにアドレスを追加するには、ステップ 5 から ステップ 8 を繰り返します。

フィルタに IP プロトコルや IP ポート要素を追加する必要がない場合は、ステップ 15 にスキップして、アクセス ポイント / ブリッジにフィルタを保存します。

ステップ 9　IP プロトコルをフィルタするには、IP Protocol ドロップダウン メニューから共通プロトコルの 1 つを選択するか、**Custom** ラジオ ボタンを選択して、既存の ACL 番号を Custom フィールドに入力します。ACL 番号を 0 ～ 255 の範囲で入力します。IP プロトコルと対応する識別番号の一覧については、付録 B「プロトコル フィルタ」を参照してください。

ステップ 10　Action メニューから **Forward** または **Block** を選択します。

ステップ 11　**Add** をクリックします。追加したプロトコルが Filters Classes フィールドに表示されます。Filters Classes リストからプロトコルを削除するには、そのプロトコルを選択して **Delete Class** をクリックします。このフィルタにさらにプロトコルを追加するには、ステップ 9 から ステップ 11 を繰り返します。

フィルタに IP ポート要素を追加する必要がない場合は、ステップ 15 にスキップして、アクセス ポイント / ブリッジにフィルタを保存します。

ステップ 12　Transmission Control Protocol（TCP）または User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート プロトコルをフィルタするには、TCP Port または UDP Port ドロップダウン メニューから共通ポート プロトコルの 1 つを選択するか、**Custom** ラジオ ボタンを選択して、既存のプロトコル番号を Custom フィールドの 1 つに入力します。プロトコル番号を 0 ～ 65535 の範囲で入力します。IP ポート プロトコルと対応する識別番号の一覧については、付録 B「プロトコル フィルタ」を参照してください。

ステップ 13　Action メニューから **Forward** または **Block** を選択します。

ステップ 14　**Add** をクリックします。追加したプロトコルが Filters Classes フィールドに表示されます。Filters Classes リストからプロトコルを削除するには、そのプロトコルを選択して **Delete Class** をクリックします。このフィルタにさらにプロトコルを追加するには、ステップ 12 から ステップ 14 を繰り返します。

ステップ 15　フィルタが完成したら、**Apply** をクリックします。このフィルタはアクセス ポイント / ブリッジに保存されますが、Apply Filters ページで適用するまで有効化されません。

ステップ 16　**Apply Filters** タブをクリックして、Apply Filters ページに戻ります。図 15-7 は、Apply Filters ページを示しています。

図 15-7　Apply Filters ページ

ステップ 17　IP ドロップダウン メニューの 1 つから、フィルタ名を選択します。フィルタはイーサネット ポートと無線ポートのどちらか、またはこの両方に適用できます。また、受信パケットか送信パケット、またはこの両方に適用することも可能です。

ステップ 18　**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。

Ethertype フィルタの設定と有効化

Ethertype フィルタは、アクセス ポイント / ブリッジのイーサネット ポートと無線ポートを経由した、特定のプロトコルの使用を許可または禁止するために使用します。作成したフィルタはイーサネット ポートと無線ポートのどちらか、またはこの両方に適用できます。また、受信パケットか送信パケット、またはこの両方に適用することも可能です。

Ethertype Filters ページを使用して、アクセス ポイント / ブリッジの Ethertype フィルタを作成します。図 15-8 は、Ethertype Filters ページを示しています。

図 15-8　Ethertype Filters ページ

次のリンク パスに従って、Ethertype Filters ページを表示します。

1. 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。

Ethertype フィルタの作成

Ethertype フィルタを作成する手順は、次のとおりです。

ステップ 1　リンク パスに従って、Ethertype Filters ページを表示します。

ステップ 2　新規フィルタを作成する場合、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。

ステップ 3　Filter Index フィールドに、200 ～ 299 までの数字を使ってフィルタ名を入力します。ここで指定した数字により、この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。

ステップ 4　Add Ethertype フィールドに Ethertype 番号を入力します。プロトコルと対応する識別番号の一覧については、付録 B「プロトコル フィルタ」を参照してください。

ステップ 5　Mask フィールドに、この Ethertype で使用するマスクを入力します。

ステップ 6　Action メニューから **Forward** または **Block** を選択します。

ステップ 7　**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。Filters Classes リストから Ethertype を削除するには、そのアドレスを選択して **Delete Class** をクリックします。このフィルタにさらに Ethertype を追加するには、ステップ 4 から ステップ 7 を繰り返します。

ステップ 8　Default Action メニューから **Forward All** または **Block All** を選択します。このフィルタのデフォルト アクションは、フィルタに含まれる少なくとも 1 つの Ethertype のアクションの逆である必要があります。たとえば、複数の Ethertype を入力したときに、これらの Ethertype すべてに対するアクションとして **Block** を選択した場合、フィルタのデフォルト アクションには **Forward All** を選択する必要があります。

ステップ 9　**Apply** をクリックします。このフィルタはアクセス ポイント / ブリッジに保存されますが、Apply Filters ページで適用するまで有効化されません。

ステップ 10　**Apply Filters** タブをクリックして、Apply Filters ページに戻ります。図 15-9 は、Apply Filters ページを示しています。

図 15-9　Apply Filters ページ

ステップ 11　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どちらか、またはこの両方に適用できます。また、受信パケットか送信パケット、またはこの両方に適用することも可能です。

ステップ 12　**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。