サービス アクセス ポイントのアクセス コントロール リストについて

内容

概要

このドキュメントでは、Cisco ルータのサービス アクセスポイント（SAP）アクセス コントロール リスト（ACL）の読み取りおよび作成方法について説明します。ACL には数種類ありますが、SAP 値に基づいたフィルタリングを行うものにに注目します。このタイプのACLの数値範囲は、200 ~ 299です。これらのACLは、トークンリングインターフェイスに適用してSource Route Bridge(SRB)トラフィックをフィルタし、イーサネットインターフェイスに適用してTransparent Bridge(TB)トラフィックをフィルタしますピアルータ。

SAP ACL での主な身元証明要求は、特定の ACL エントリで許可または拒 否されている SAP を正確に認識することです。特定のプロトコルをフィルタ リングする異なる 4 つのシナリオについて分析します。

はじめに

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。

前提条件

このドキュメントに関しては個別の前提条件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるもの

ではありません。

システム ネットワーク アーキテクチャ（SNA）のフィルタリング

IBM の SNA トラフィックは 0x00 ~ 0xFF の範囲をとる SAP を使用し ます。Virtual Telecommunications Access Method（VTAM）V3R4 以降のバー ジョンでは、SAP 値の範囲 4 ~ 252（16 進数表示の 0x04 ~ 0xFC）をサポ ートします。ここで、0xF0 は NetBIOS トラフィックに予約されます。SAPは0x04の倍数である必要があり、0x04で始まります。次のACLは、最も一般的なSNA SAPを許可し、それ以外を拒否します(各ACLの最後に暗黙的**deny allが存在することを考慮**)。

```
access-list 200 permit 0x0000 0x0D0D
```

16 進数	バイナリ
0x0000 0x0D0D	DSAP SSAP Wildcard Mask for DSAP and SSAP respectively |-------| |-------| |-------| |-------| 0000 0000 0000 0000 0000 1101 0000 1101

ワイルドカード マスクのビットを使用して、この特定の ACL エントリ が許可する SAP を判別します。ワイルドカード マスクのビットを変換する 場合は、次のルールを使用します。

- 0：完全一致が必要。これは、許可された SAP に ACL で 設定された SAP と同じ値を持つ必要があることを意味します。詳細について は、次の表を参照してください。
- 1：許可された SAP は、このビット位置、つまり「無指定」位置が 0 または 1 のいずれかになる。

ACL で設定された SAP	ワイル ドカード マスク	ACL で許可 された SAP、X=0 または X=1
0	0	0
0	0	0
0	0	0
0	0	0
X	1	0
X	1	0
0	0	0
X	1	0

前述の表の結果を使用して、ここで上記のパターンに一致する SAP のリストを 示します。

許可された SAP（2 進数）								許可された SAP（16 進 数）
0	0	0	0	0	0	0	0	0x00

0	0	0	0	0	0	0	1	0x01
0	0	0	0	0	1	0	0	0x04
0	0	0	0	0	1	0	1	0x05
0	0	0	0	1	0	0	0	0x08
0	0	0	0	1	0	0	1	0x09
0	0	0	0	1	1	0	0	0x0C
0	0	0	0	1	1	0	1	0x0D

上記の表でわかるように、予想されるすべての SNA SAP がこの ACL に含まれるわけではありません。ただし、これらの SAP は最も一 般的な場合を対象にしています。

ACL の設定時に考慮する別の点は、SAP 値がコマンドか、レスポンス かによって変わることです。SSAP には、それらを区別するコマンド/レスポンス (C/R) ビットがあります。C/R は、コマンドの場合は 0、レスポンスの場合は 1 に設定さ れます。このため、ACL はレスポンスと同様にコマンドを許可またはブロックす る必要があります。たとえば、SAP 0x05 (応答に使用) は SAP 0x04で、C/Rは1に設定されます。SAP 0x09 (C/Rが1に設定されたSAP 0x08)、0x0D、および0x01にも適用されます。

NetBIOS のフィルタリング

NetBIOS トラフィックでは SAP 値 0xF0 (コマンド用) と 0xF1 (応答用) が使用されます。 通常、ネットワーク管理者は、これらの SAP 値 を使用してこのプロトコルをフィルタリングします。次のアクセス リストの エントリは、NetBIOS トラフィックを許可し、他をすべて拒否します (各 AC L の最後には暗黙の "deny all" があります)。

```
access-list 200 permit 0xF0F0 0x0101
```

前のセクションの説明と同じ手順を使用して、上記の ACL が次の SAP を許可することを決定でできます。

その一方で、NetBIOS をブロックしてトラフィックの残りを許可したい 場合は、次の ACL を使用します。

```
access-list 200 deny 0xF0F0 0x0101
access-list 200 permit 0x0000 0xFFFF
```

IPX のフィルタリング

デフォルトでは、Cisco ルータが IPX トラフィックをブリッジしま す。この動作を変更するには、ルータで ipx routing を設定する必 要があります。802.2 カプセル化を使用する IPX は、DSAP および SSAP と して SAP 0xE0 を使用します。このため、Cisco ルータが IPX をブリッジし ていて、要件がこのタイプのトラフィックを許可することである場合には、 この ACL を使用します。

```
access-list 200 permit 0xE0E0 0x0101
```

一方、次の ACL は IPX をブロックして、残りのトラフィックを許可しま す。

```
access-list 200 deny 0xE0E0 0x0101
access-list 200 permit 0x0000 0xFFFF
```

すべてのトラフィックの許可または拒否

すべての ACL には、暗黙の "deny all" があります。設定された ACL の 動作を分析する際は、このエントリに注意する必要があります。次に示す最 後の ACL エントリは、すべてのトラフィックを拒否します。

```
access-list 200 permit ....
access-list 200 permit ....
access-list 200 deny 0x0000 0xFFFF
```

ワイルドカード マスク（2 進数）の読み取りの際は、1 が「無指定」ビ ット位置になります。また、2 進数で表されたすべてのワイルドカード マ スクはそれぞれ 16 進数の 0xFFFF に換わります。

関連情報

- DLSw に関するサポート ページ
- アクセス コントロール リスト:概要とガイドライン
- DLSw+ SAP/MAC フィルタリング技術
- テクニカルサポート - Cisco Systems