瞭解服務接入點訪問控制清單

目錄

簡介

本檔案將說明如何在思科路由器中讀取和建立服務存取點(SAP)存取控制清單(ACL)。雖然有幾種型別的ACL，但本文檔重點介紹根據SAP值過濾的ACL。此類ACL的數值範圍為200到299。這些ACL可應用於令牌環介面以過濾源路由網橋(SRB)流量，應用於乙太網介面以過濾透明網橋(TB)流量，或應用於資料鏈路交換(DLSw)對等路由器。

SAP ACL的主要難題是確切瞭解特定ACL條目允許或拒絕哪些SAP。我們將分析四個不同的場景，其中正在過濾特定協定。

開始之前

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

必要條件

本文件沒有特定先決條件。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

過濾系統網路架構

IBM的系統網路架構(SNA)流量使用範圍從0x00到0xFF的SAP。虛擬電信接入方法(VTAM)V3R4及

更高版本支援4到252的SAP值範圍（或十六進位制表示為0x04到0xFC），其中0xF0保留用於NetBIOS流量。SAP必須是0x04的倍數，從0x04開始。以下ACL允許最常見的SNA SAP，並拒絕其餘的(考慮到每個ACL末尾都有一個隱含的**deny all**):

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

十六進位制	二進位
0x0000 0x0D0D	DSAP SSAP Wildcard Mask for DSAP and SSAP respectively |-------| |-------| |-------| |-------| 0000 0000 0000 0000 0000 1101 0000 1101

使用萬用字元掩碼中的位確定此特定ACL條目允許哪些SAP。解釋萬用字元掩碼位時，請使用以下規則：

- 0 =需要完全匹配。這表示允許的SAP必須具有與ACL中配置的SAP相同的值。有關詳細資訊，請參閱下表。
- 1 =允許的SAP在此位位置可為0或1，即「不比對」位置。

按ACL允許的Sap，其中X=0或X=1	萬用字元掩碼	在ACL中配置的SAP
0	0	0
0	0	0
0	0	0
0	0	0
X	1	0
X	1	0
0	0	0
X	1	0

使用上表中的結果，符合上述模式的SAP清單如下所示。

允許的Sap（二進位）								允許的Sap（十六進位制）
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

如上表所示，此ACL中並未包含所有可能的SNA SAP。但是，這些SAP涵蓋了最常見的情況。

設計ACL時需要考慮的另外一點是， SAP值會根據是命令還是響應而變化。源服務接入點(SSAP)包括命令/響應(C/R)位以區分它們。命令的C/R設定為0，響應的設定為1。因此，ACL必須允許或阻止命令以及響應。例如，SAP 0x05（用於響應）是SAP 0x04,C/R設定為1。這同樣適用於SAP 0x09（SAP 0x08,C/R設定為1）、0x0D和0x01。

過濾NetBIOS

NetBIOS流量使用SAP值0xF0（用於命令）和0xF1（用於響應）。 通常，網路管理員使用這些SAP值來過濾此協定。下面顯示的訪問清單條目允許NetBIOS流量並拒絕所有其他流量(請記住每個ACL結尾的隱含**deny all**):

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

使用上一節中顯示的相同步驟，可以確定上述ACL允許SAP 0xF0和0xF1。

相反，如果要求阻止NetBIOS並允許其餘流量，請使用以下ACL:

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

過濾IPX

預設情況下，Cisco路由器橋接IPX流量。要更改此行為，必須在路由器上發出**ipx routing**命令。IPX使用802.2封裝，使用SAP 0xE0作為目的地服務接入點(DSAP)和SSAP。因此，如果Cisco路由器正在橋接IPX，並且要求僅允許此類流量，請使用以下ACL:

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

相反，以下ACL會阻止IPX並允許其餘流量：

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

允許或拒絕所有流量

每個ACL都包含隱含的**deny all**。分析已設定ACL的行為時，必須注意此專案。下面顯示的最後一個ACL條目拒絕所有流量。

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

請記得，在讀取萬用字元掩碼（二進位制）時，1被視為「不比對」位位置。二進位制表示中的全1萬用字元掩碼轉換為十六進位制表示中的0xFFFF。

相關資訊

- DLSw支援頁面
- 存取控制清單：概述和准則
- DLSw+ SAP/MAC過濾技術
- 技術支援 - Cisco Systems