

Table of Contents

<u>Understanding Service Access Point Access Control Lists</u>	1
<u>Document ID: 12403</u>	1
<u>Introduction</u>	1
<u>Before You Begin</u>	1
<u>Conventions</u>	1
<u>Prerequisites</u>	1
<u>Components Used</u>	1
<u>Filtering Systems Network Architecture</u>	1
<u>Filtering NetBIOS</u>	3
<u>Filtering IPX</u>	3
<u>Permit or Deny All Traffic</u>	3
<u>Related Information</u>	3

Understanding Service Access Point Access Control Lists

Document ID: 12403

Introduction

Before You Begin

Conventions

Prerequisites

Components Used

Filtering Systems Network Architecture

Filtering NetBIOS

Filtering IPX

Permit or Deny All Traffic

Related Information

Introduction

This document explains how to read and create Service Access Point (SAP) Access Control Lists (ACLs) in Cisco routers. Although there are several types of ACLs, this document focuses on the ones that filter based on SAP values. The numerical range for this type of ACL is 200 to 299. These ACLs can be applied to Token Ring interfaces to filter Source Route Bridge (SRB) traffic, to Ethernet interfaces to filter Transparent Bridge (TB) traffic, or to Data Link Switching (DLSw) peer routers.

The main challenge with SAP ACLs is to know exactly what SAPs are being permitted or denied by a particular ACL entry. We'll analyze four different scenarios where a particular protocol is being filtered.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Filtering Systems Network Architecture

IBM's Systems Network Architecture (SNA) traffic uses SAPs ranging from 0x00 to 0xFF. Virtual Telecommunications Access Method (VTAM) V3R4 and later support a SAP value range of 4 to 252 (or 0x04 to 0xFC in hexadecimal representation), where 0xF0 is reserved for NetBIOS traffic. SAPs must be multiples of 0x04, beginning with 0x04. The following ACL permits the most common SNA SAPs, and denies the rest (considering there is an implicit **deny all** at the end of each ACL):

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

Hexadecimal	Binary
0x0000	DSAP SSAP Wildcard Mask for DSAP and SSAP respectively
0x0D0D	----- ----- ----- -----
	0000 0000 0000 0000 0000 1101 0000 1101

Use the bits in the wildcard mask to determine which SAPs are allowed by this particular ACL entry. Use the following rules when interpreting the wildcard mask bits:

- 0 = Exact match required. This means that the allowed SAP must have the same value as the SAP configured in the ACL. Refer to the table below for more details.
- 1 = The allowed SAP can have either a 0 or 1 at this bit position, the "do not care" position.

Allowed Saps by ACL, Where X=0 or X=1	Wildcard Mask	SAP Configured in ACL
0	0	0
0	0	0
0	0	0
0	0	0
X	1	0
X	1	0
0	0	0
X	1	0

Using the results in the previous table, the list of SAPs that meet the above pattern is shown below.

Allowed Saps (Binary)								Allowed Saps (Hexadecimal)
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

As you can see from the above table, not all possible SNA SAPs are included in this ACL. These SAPs, however, cover the most common cases.

Another point to consider when designing the ACL is that SAP values change depending on if they are commands or responses. The Source Service Access Point (SSAP) includes the Command/Response (C/R) bit

to differentiate between them. The C/R is set to 0 for commands and to 1 for responses. Therefore, the ACL must allow or block commands as well as responses. For example, SAP 0x05 (used for responses) is SAP 0x04 with the C/R set to 1. The same applies to SAP 0x09 (SAP 0x08 with C/R set to 1), 0x0D, and 0x01.

Filtering NetBIOS

NetBIOS traffic uses SAP values 0xF0 (for commands) and 0xF1 (for responses). Typically, network administrators use these SAP values to filter this protocol. The access list entry shown below permits NetBIOS traffic and denies everything else (remember the implicit **deny all** at the end of each ACL):

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

Using the same procedure shown in the previous section, you can determine that the above ACL permits SAPs 0xF0 and 0xF1.

On the contrary, if the requirement is to block NetBIOS and allow the rest of the traffic, use the following ACL:

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

Filtering IPX

By default, Cisco routers bridge IPX traffic. To change this behavior, you must issue the **ipx routing** command on the router. IPX, using 802.2 encapsulation, uses SAP 0xE0 as the Destination Service Access Point (DSAP) and SSAP. Therefore, if a Cisco router is bridging IPX and the requirement is to permit only this type of traffic, use the following ACL:

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

On the contrary, the following ACL blocks IPX and allows the rest of the traffic:

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

Permit or Deny All Traffic

Every ACL includes an implicit **deny all**. You must be aware of this entry when analyzing the behavior of a configured ACL. The last ACL entry shown below denies all traffic.

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

Remember when reading the wildcard mask (in binary), 1 is considered a "do not care" bit position. An all 1s wildcard mask in binary representation translates to 0xFFFF in hexadecimal representation.

Related Information

- [DLSw Support Page](#)
- [Access Control Lists: Overview and Guidelines](#)
- [DLSw+ SAP/MAC Filtering Techniques](#)

- **List of Common SAPs**
 - **Technical Support – Cisco Systems**
-

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Mar 14, 2006

Document ID: 12403
