# Übersicht über die Zugriffskontrolllisten für Service Access Points

## Inhalt



## Einführung

In diesem Dokument wird erläutert, wie Sie Access Point (SAP) Access Control Lists (ACLs) in Cisco Routern lesen und erstellen. Obwohl es mehrere Typen von ACLs gibt, konzentriert sich dieses Dokument auf diejenigen, die auf Basis von SAP-Werten filtern. Der numerische Bereich für diesen ACL-Typ liegt zwischen 200 und 299. Diese ACLs können auf Token Ring-Schnittstellen angewendet werden, um den Source Route Bridge-Datenverkehr (SRB) zu filtern, auf Ethernet-Schnittstellen zum Filtern von Transparent Bridge (TB)-Datenverkehr oder auf Data Link Switching (DLSw) Peer-Router zu filtern.

Die größte Herausforderung bei SAP-ACLs besteht darin, genau zu wissen, welche SAPs von einem bestimmten ACL-Eintrag zugelassen oder abgelehnt werden. Wir analysieren vier verschiedene Szenarien, in denen ein bestimmtes Protokoll gefiltert wird.

## Bevor Sie beginnen

### Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

### Voraussetzungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

## Filtersysteme Netzwerkarchitektur

Der SNA-Datenverkehr (Systems Network Architecture) von IBM nutzt SAPs von 0 x 00 bis 0 x FF. Virtual Telecommunications Access Method (VTAM) V3R4 und höher unterstützt einen SAP-Wertebereich von 4 bis 252 (oder 0x04 bis 0xFC in hexadezimaler Darstellung), wobei 0xF0 für NetBIOS-Datenverkehr reserviert ist. Bei SAPs muss es sich um ein Vielfaches von 0 x 04 handeln, beginnend mit 0 x 04. Die folgende ACL erlaubt die gängigsten SNA-SAPs und verweigert den Rest (wenn am Ende jeder ACL ein implizites **Ablehnen aller** Pakete vorliegt):

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

| Hexadezimal | Binär |
|---|---|
| 0x0000 0x0D0D | DSAP SSAP Wildcard Mask for DSAP and SSAP respectively<br>\|-------\| \|-------\| \|-------\| \|-------\|<br>0000 0000 0000 0000 0000 1101 0000 1101 |

Bestimmen Sie mithilfe der Bits in der Platzhaltermaske, welche SAPs von diesem bestimmten ACL-Eintrag zugelassen sind. Verwenden Sie bei der Interpretation der Platzhalterbits die folgenden Regeln:

- 0 = Genaue Übereinstimmung erforderlich. Das bedeutet, dass der zulässige SAP-Wert mit dem in der ACL konfigurierten SAP-Wert übereinstimmen muss. Weitere Informationen finden Sie in der Tabelle unten.
- 1 = Der zulässige SAP-Code kann an dieser Bitposition entweder eine 0 oder 1 haben, die "Keine Sorge"-Position.

| Zugelassene Saps nach ACL, wobei X=0 oder X=1 ist | Platzhaltermaske | In ACL konfiguriertes 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 |

Anhand der Ergebnisse aus der vorherigen Tabelle wird nachfolgend die Liste der SAPs angezeigt, die dem oben beschriebenen Muster entsprechen.

| Zugelassene Saps (Binär) | Zugelassene Saps |
|---|---|

| | | | | | | | | (hexadezimal) |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 x 00 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 x 01 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 x 04 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 x 05 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 x 08 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 x 09 |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0x0C |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0x0D |

Wie aus der obigen Tabelle ersichtlich, sind in dieser ACL nicht alle möglichen SNA-SAPs enthalten. Diese SAPs decken jedoch die gängigsten Fälle ab.

Ein weiterer zu berücksichtigender Punkt beim Entwerfen der ACL ist, dass sich die SAP-Werte abhängig davon ändern, ob es sich um Befehle oder Antworten handelt. Der Source Service Access Point (SSAP) enthält das Command/Response (C/R)-Bit, um zwischen ihnen zu unterscheiden. Für Befehle ist der Wert für "C/R" auf "0" und für Antworten auf "1" festgelegt. Aus diesem Grund muss die ACL Befehle sowie Antworten zulassen oder blockieren. Beispielsweise ist SAP 0x05 (für Antworten verwendet) SAP 0x04, wobei C/R auf 1 festgelegt ist. Gleiches gilt für SAP 0x09 (SAP 0x08 mit C/R auf 1), 0x0D und 0x01.

## Filtern von NetBIOS

Der NetBIOS-Datenverkehr verwendet die SAP-Werte 0xF0 (für Befehle) und 0xF1 (für Antworten). In der Regel verwenden Netzwerkadministratoren diese SAP-Werte, um dieses Protokoll zu filtern. Der unten angezeigte Zugriffslisteneintrag erlaubt NetBIOS-Datenverkehr und verweigert alles andere (denken Sie daran, dass **alle** am Ende jeder ACL **blockiert werden**):

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

Mit dem gleichen Verfahren wie im vorherigen Abschnitt können Sie feststellen, dass die oben aufgeführte ACL den SAPs 0xF0 und 0xF1 zulässt.

Im Gegenteil: Wenn NetBIOS blockiert und der restliche Datenverkehr zugelassen werden soll, verwenden Sie die folgende ACL:

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

## IPX filtern

Standardmäßig überbrücken Cisco Router den IPX-Datenverkehr. Um dieses Verhalten zu ändern, müssen Sie den Befehl **ipx routing** auf dem Router ausführen. IPX verwendet mit 802.2-Kapselung SAP 0xE0 als Ziel Service Access Point (DSAP) und SSAP. Wenn ein Cisco Router IPX überbrückt und nur diese Art von Datenverkehr zulassen muss, verwenden Sie daher die

folgende ACL:

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

Im Gegenteil: Die folgende ACL blockiert IPX und erlaubt den Rest des Datenverkehrs:

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

## Zulassen oder Verweigern des gesamten Datenverkehrs

Jede ACL enthält eine implizite **Ablehnungsklausel**. Dieser Eintrag muss bei der Analyse des Verhaltens einer konfigurierten ACL berücksichtigt werden. Der letzte unten dargestellte ACL-Eintrag verweigert den gesamten Datenverkehr.

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

Denken Sie daran, beim Lesen der Platzhaltermaske (binär), 1 wird als "nicht kümmern"-Bitposition betrachtet. Eine alle 1s Platzhaltermaske in binärer Darstellung entspricht 0xFFFF in hexadezimaler Darstellung.

## Zugehörige Informationen

- DLSw-Support-Seite
- Zugriffskontrolllisten: Übersicht und Richtlinien
- DLSw+ SAP/MAC-Filtertechniken
- Technischer Support - Cisco Systems