서비스 액세스 포인트 액세스 제어 목록 이해

목차

소개

이 문서에서는 Cisco 라우터에서 SAP(Service Access Point) ACL(Access Control List)을 읽고 생성하는 방법에 대해 설명합니다.ACL에는 여러 유형이 있지만 이 문서에서는 SAP 값을 기반으로 필터링하는 ACL에 초점을 맞춥니다.이 유형의 ACL에 대한 숫자 범위는 200~299입니다. 이러한 ACL은 토큰 링 인터페이스에 적용하여 SRB(Source Route Bridge) 트래픽을 필터링하거나 이더넷 인터페이스에 적용되어 TB(Transparent Bridge) 트래픽을 필터링하거나 DLS(Data Link Switching) 피어 라우터에 적용할 수 있습니다.

SAP ACL의 주요 과제는 특정 ACL 항목에 의해 허용되거나 거부되는 SAP를 정확하게 파악하는 것입니다.특정 프로토콜이 필터링되는 네 가지 시나리오를 분석합니다.

시작하기 전에

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

사전 요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

시스템 네트워크 아키텍처 필터링

IBM의 SNA(Systems Network Architecture) 트래픽은 0x00~0xFF 범위의 SAP를 사용합니다 .VTAM(Virtual Telecommunications Access Method) V3R4 이상에서는 4~252(또는 16진수 표현에서 0x04~0xFC)의 SAP 값 범위를 지원합니다. 여기서 0xF0은 NetBIOS 트래픽용으로 예약됩니다 .SAP는 0x04로 시작하는 0x04의 배수여야 합니다. 다음 ACL은 가장 일반적인 SNA SAP를 허용하고 나머지는 거부합니다(각 ACL의 끝에 암시적 **거부**가 있다는 점을 고려함).

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

16진수	이진
0x0000 0x0D0D	DSAP SSAP Wildcard Mask for DSAP and SSAP respectively |-------| |-------| |-------| |-------| 0000 0000 0000 0000 0000 1101 0000 1101

이 특정 ACL 항목에서 허용할 SAP를 결정하려면 와일드카드 마스크의 비트를 사용합니다.와일드카드 마스크 비트를 해석할 때 다음 규칙을 사용합니다.

- 0 = 정확히 일치해야 합니다.즉, 허용된 SAP는 ACL에 구성된 SAP와 동일한 값을 가져야 합니다.자세한 내용은 아래 표를 참조하십시오.
- 1 = 허용되는 SAP는 이 비트 위치인 "관심 없음" 위치를 0 또는 1로 가질 수 있습니다.

ACL로 허용되는 SAPS(X=0 또는 X=1)	와일드카드 마스크	ACL에 구성된 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

이전 표의 결과를 사용하여 위의 패턴을 충족하는 SAP 목록이 아래에 표시됩니다.

허용되는 SAPS(이진)								허용되는 SAPS(16진수)
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

위 표에서 볼 수 있듯이, 모든 가능한 SNA SAP가 이 ACL에 포함되는 것은 아닙니다.그러나 이러한 SAP는 가장 일반적인 사례를 다룹니다.

ACL을 설계할 때 고려해야 할 또 다른 점은 SAP 값이 명령 또는 응답인지 여부에 따라 변경된다는 것입니다.SSAP(Source Service Access Point)에는 C/R(Command/Response) 비트가 포함되어 있으며 이를 구별합니다.C/R은 명령에 대해 0으로, 응답에 대해서는 1로 설정됩니다.따라서 ACL은 응답뿐 아니라 명령도 허용하거나 차단해야 합니다.예를 들어, 응답에 사용되는 SAP 0x05는 C/R이 1로 설정된 SAP 0x04입니다. SAP 0x09(C/R이 1로 설정된 SAP 0x08), 0x0D 및 0x01에도 동일하게 적용됩니다.

NetBIOS 필터링

NetBIOS 트래픽은 SAP 값 0xF0(명령의 경우) 및 0xF1(응답의 경우)을 사용합니다. 일반적으로 네트워크 관리자는 이러한 SAP 값을 사용하여 이 프로토콜을 필터링합니다.아래 표시된 액세스 목록 항목은 NetBIOS 트래픽을 허용하고 다른 모든 것을 거부합니다(각 ACL의 끝에서 암시적 **모두 거부**를 기억하십시오).

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

이전 섹션에 나와 있는 동일한 절차를 사용하여 위 ACL에서 SAP 0xF0 및 0xF1을 허용하는지 확인할 수 있습니다.

반대로, NetBIOS를 차단하고 나머지 트래픽을 허용해야 하는 경우 다음 ACL을 사용합니다.

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

IPX 필터링

기본적으로 Cisco 라우터는 IPX 트래픽을 연결합니다.이 동작을 변경하려면 라우터에서 **ipx routing** 명령을 실행해야 합니다.802.2 캡슐화를 사용하는 IPX는 SAP 0xE0을 DSAP(Destination Service Access Point) 및 SSAP로 사용합니다.따라서 Cisco 라우터가 IPX를 브리징하고 있고 이 유형의 트래픽만 허용해야 하는 경우 다음 ACL을 사용합니다.

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

반대로 다음 ACL은 IPX를 차단하고 나머지 트래픽을 허용합니다.

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

모든 트래픽 허용 또는 거부

모든 ACL에는 암시적 **모두 거부**가 포함됩니다.구성된 ACL의 동작을 분석할 때 이 항목을 알아야 합니다.아래에 표시된 마지막 ACL 항목은 모든 트래픽을 거부합니다.

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

와일드카드 마스크(이진 형식)를 읽을 때 1은 "관심 없음" 비트 위치로 간주됩니다.이진 표현에서 모든 1s 와일드카드 마스크는 16진수 표현에서 0xFFFF로 변환됩니다.

관련 정보

- DLSw 지원 페이지
- 액세스 제어 목록:개요 및 지침
- DLSw+ SAP/MAC 필터링 기술
- Technical Support - Cisco Systems