De betekenis van Service Access Point-toegangscontrolelijsten

Inhoud

Inleiding

Dit document legt uit hoe u Service Access Point (SAP) toegangscontrolelijsten (ACL's) in Cisco-routers kunt lezen en maken. Hoewel er verschillende typen ACL's zijn, richt dit document zich op de soorten die op basis van SAP-waarden filteren. Het numerieke bereik voor dit type ACL is 200 tot 299. Deze ACL's kunnen worden toegepast op Token Ring-interfaces op verkeer van routebrug (SRB) van filter, op Ethernet-interfaces op filter Transparent Bridge (TB)-verkeer, of op Data Link Switching (DLSw) peer-routers.

De belangrijkste uitdaging met SAP ACL's is te weten welke SAP's door een bepaalde ACL-ingang worden toegestaan of geweigerd. We analyseren vier verschillende scenario's waarbij een bepaald protocol wordt gefilterd.

Voordat u begint

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Voorwaarden

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Netwerkarchitectuur voor filtering systemen

IBM's Systems Network Architecture (SNA) maakt gebruik van SAP's variërend van 0x00 tot 0xFF. Virtual Telecommunications Access Methode (VTAM) V3R4 en ondersteunen later een SAP-waarde van 4 tot 252 (of 0x04 tot 0xFC in hexadecimale weergave), waarbij 0xF0 is gereserveerd voor NetISO-verkeer. SAP's moeten meerdere exemplaren van 0x04 zijn, te beginnen met 0x04. De volgende ACL's staat de meest gebruikelijke SNA SAP's toe en ontkent de rest (gezien dat **alle** tekens aan het einde van elke ACL impliciet **worden ontkend**):

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

hexadecimaal	Binair
0x0000 x0D	DSAP SSAP Wildcard Mask for DSAP and SSAP respectively |-------| |-------| |-------| |-------| 0000 0000 0000 0000 0000 1101 0000 1101

Gebruik de bits in het jokermasker om te bepalen welke SAP's zijn toegestaan door deze specifieke ACL-ingang. Gebruik de volgende regels bij het interpreteren van de jokermaskers:

- 0 = Exacte overeenkomst vereist. Dit betekent dat de toegestane SAP dezelfde waarde moet hebben als de SAP die in de ACL is ingesteld. Raadpleeg de onderstaande tabel voor meer informatie.
- 1 = De toegestane SAP kan 0 of 1 hebben op deze bit positie, de "not care" positie.

Toegestaan aps door ACL, waarbij X=0 of X=1	Wildcard-masker	SAP ingesteld 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

Aan de hand van de resultaten in de vorige tabel wordt de lijst met SAP's die aan het bovenstaande patroon voldoen, hieronder weergegeven.

Toegestane splitsingen (binair)								Toegestaan kranen (hexadecimaal)
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

Zoals u in de bovenstaande tabel kunt zien, zijn niet alle mogelijke SNA SAP's in deze ACL's opgenomen. Deze strategiedocumenten bestrijken echter de meest voorkomende gevallen.

Een ander punt om bij het ontwerpen van ACL rekening te houden is dat de waarden van SAP afhankelijk van of zij bevelen of reacties zijn veranderen. Het Source Service Access Point (SSAP) bevat het commando/Response (C/R) bit om het verschil tussen beide te bepalen. De C/R is ingesteld op 0 voor opdrachten en op 1 voor antwoorden. Daarom moet ACL zowel opdrachten als reacties toestaan of blokkeren. Bijvoorbeeld, SAP 0x05 (gebruikt voor antwoorden) is SAP 0x04 met de C/R ingesteld op 1. Hetzelfde geldt voor SAP 0x09 (SAP 0x08 met C/R ingesteld op 1), 0x0D en 0x01.

NetVOS filteren

Netoverheid gebruikt SAP-waarden 0xF0 (voor opdrachten) en 0xF1 (voor antwoorden). Netwerkbeheerders gebruiken deze SAP-waarden doorgaans om dit protocol te filteren. De toegangslijst die hieronder wordt getoond, maakt NetConfiguration-verkeer mogelijk en ontkent al het andere (vergeet de impliciete **ontkenning aan** het einde van elke ACL):

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

Met behulp van de zelfde procedure die in de vorige sectie wordt getoond, kunt u bepalen dat bovenstaande ACL's SAP's 0xF0 en 0xF1 toestaat.

Integendeel, als de eis is om Netopgemerkt te blokkeren en de rest van het verkeer toe te staan, gebruikt u de volgende ACL:

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

IPX filteren

Standaard overbruggen Cisco-routers IPX-verkeer. Om dit gedrag te veranderen moet u het **ipx Routing** commando op de router uitgeven. IPX, met gebruik van 802.2 insluiting, gebruikt SAP 0xE0 als access point (DSAP) en SSAP. Daarom, als een router van Cisco IPX overbruggt en de vereiste is om alleen dit type verkeer toe te staan, gebruik de volgende ACL:

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

In tegendeel, de volgende ACL blokkeert IPX en staat de rest van het verkeer toe:

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

Alle verkeer toestaan of weigeren

Elke ACL bevat een impliciet **ontkennen alles**. U moet zich van deze ingang bewust zijn wanneer u het gedrag van een geconfigureerde ACL analyseert. De laatste ACL-ingang die hieronder wordt weergegeven, ontkent al verkeer.

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

Onthoud wanneer je het masker leest (in binair), wordt 1 gezien als een positie van het "niet schelen" bit. Een all 1s wild-kaartmasker in binaire weergave vertaalt zich naar 0xFFFF in hexadecimale weergave.

Gerelateerde informatie

- DLSw-ondersteuningspagina
- Toegangscontrolelijsten: Overzicht en richtsnoeren
- DLSw+ SAP/MAC-filtering
- Technische ondersteuning - Cisco-systemen