Catalyst 9000 Series 스위치에 SSDP 모범 사례 구현

목차

소개

이 문서에서는 Catalyst 9000 Series 스위치에서 SSDP(Simple Service Discovery Protocol) 패킷을 삭제 또는 제한하도록 설계된 모범 사례 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- PIM(Protocol Independent Multicast) 작업
- SSDP가 환경에 특정한 방식으로 사용되는 방법

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Catalyst 9200
- Cisco Catalyst 9300
- Cisco Catalyst 9400
- Cisco Catalyst 9500
- Cisco Catalyst 9600

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

엔터프라이즈 환경의 SSDP 위험 파악

일반적으로 랩톱 및 휴대폰과 같은 최종 사용자 디바이스는 SSDP 프로토콜을 사용하는

UPnP(Universal Plug-and-Play) 기능을 자동으로 광고합니다. 클라이언트는 IP 주소 239.255.255.250에 멀티캐스트 광고 패킷을 전송합니다. 이러한 광고는 TTL(Time to Live)이 1인 경우 전송되며 멀티캐스트 패킷을 생성한 호스트의 로컬 서브넷을 초과하지 않습니다. 네트워크에 있는 다른 디바이스의 광고를 수신하려면 엔드포인트는 239.255.255.250 주소로 IGMP 멤버십 보고서를 전송하여 다른 멀티캐스트 소스에서 이 IP 주소로 전송된 멀티캐스트 트래픽도 이 클라이언트로 전달해야 함을 네트워크에 알립니다.

수백 또는 수천 개의 엔드포인트가 모두 소스 역할을 하며 이 그룹의 관심 있는 수신자가 포함된 엔터프라이즈 환경에서 이 클라이언트 활동은 점검 안 되면 네트워크 장치를 쉽게 마비시킬 수 있으며 네트워크 리소스가 모두 소진되면 중단이 발생할 수 있습니다.

이러한 탈진은 주로 두 가지 방법 중 하나로 이루어집니다.

1. 보조 프로토콜 장애를 트리거하는 하드웨어 리소스 소모
2. DDoS(Distributed Denial of Service) 공격으로 사용되는 SSDP의 인터페이스 및 플랫폼 대역폭 소모

이 문서에서는 자세히 설명하지 않지만, SSDP의 개방적인 특성 때문에 공격자가 이 서비스가 활성화된 클라이언트 그룹으로 작성된 패킷을 전송하여 하나 또는 대상 호스트 그룹으로 큰 응답을 보낼 수 있다는 점에 유의해야 합니다. 또한 생성되는 많은 양의 발신 인터페이스 상태는 스위치가 ASIC(Application Specific Integrated Circuit) 내에서 각 발신 인터페이스에 대해 하나의 사본을 만들어야 하기 때문에 적은 양의 멀티캐스트 트래픽에서 스위치 성능 용량이 크게 강조될 수 있음을 의미합니다. 발신 인터페이스에는 20개 이상의 인터페이스에서 용량 문제 및 패킷 손실의 위험이 더 높은 것으로 표시됩니다.

하드웨어 리소스 소모 증상

Catalyst 9000 Series 스위치는 리소스가 다 소모되었을 때 "fman_fp_image" 또는 "FMFP"가 포함된 syslog를 인쇄합니다. 스위치에 리소스가 고갈되어 더 자세히 조사해야 하는 경우 이러한 오류의 일부 또는 전부를 인쇄할 수 있습니다.

이러한 오류는 리소스 소모 중에 나타나는 일반적인 오류 중 일부이지만 포괄적인 목록은 아닙니다 .

그림 1: 스위치에서 리소스 소모가 발생했음을 나타내는 가장 일반적인 오류의 샘플

```
%FMFP-3-OBJ_DWNLD_TO_DP_STUCK: R0/0: fman_fp_image: AOM download to Data Plane is stuck for more
than 1800 seconds for <object details>
%FMFP-3-OBJ_DWNLD_TO_DP_RESUME: R0/0: fman_fp_image: AOM download of objects to Data Plane is
back to normal
%FMFP_QOS-6-QOS_STATS_STALLED: R0/0: fman_fp_image: statistics stalled
%FMFP-3-OBJ_DWNLD_TO_DP_FAILED: R0/0: fman_fp_image: adj <hex>, Flags None download to DP failed
%FMFP-3-OBJ_DWNLD_TO_DP_FAILED: R0/0: fman_fp_image: adj <hex>, Flags Midchain download to DP
failed
%FED_L3M_ERRMSG-3-RSRC_ERR: Switch <num> R0/0: fed: Failed to allocate hardware resource for
group <address> - rc:<number or error>
%FED_L3_ERRMSG-3-RSRC_ERR: Chassis <num> R0/0: fed: Failed to allocate hardware resource for adj
entry due to hardware resource exhaustion - rc:<number or error>
```

SSDP로 인해 하드웨어 리소스 소모 확인

모든 Catalyst 9000 Series 스위치는 특수 ASIC를 활용하여 높은 처리량으로 대부분의 패킷 라우팅

을 수행합니다. 이러한 ASIC는 용량이 한정된 서로 다른 테이블과 내부 리소스를 활용합니다. SSDP 클라이언트는 공통 멀티캐스트 그룹의 소스와 수신자 역할을 하므로, 하드웨어는 이러한 제한된 리소스를 사용하여 패킷이 따라야 할 하드웨어에서 경로를 프로그래밍해야 합니다. 이러한 패킷이 다른 이유로 오거나 삭제되지 않더라도(TTL 1). 하드웨어 리소스가 모두 소진되면 SSDP와 관련된 모든 그룹에 대해 새로운 업데이트나 추가 기능을 설치할 수 없습니다. 설치되지 않은 SSDP 업데이트(상태 변동)가 많이 소프트웨어에 대기열에 포함될 수 있으며, 이로 인해 비 멀티캐스트 트래픽에 대한 하드웨어 업데이트가 중단되거나 실패할 수 있으며, 이로 인해 사용자 트래픽에 영향을 미치고 네트워크 중단이 발생할 수 있습니다.

이 문서는 네트워크가 PIM으로 구성되어 있고 잘 알려진 SSDP 그룹 주소에 대한 레이어 3 멀티캐스트 상태가 있는 경우에만 관련됩니다. 이 기준을 확인하려면 명령을 실행합니다 "**show ip mroute 239.255.255.250**" (필요한 경우 vrf 문을 추가합니다.) 그룹 239.255.255.250은 SSDP 프로토콜에 한정됩니다.

명령 출력에 많은 발신 인터페이스가 포함되어 있거나 이 특정 그룹에 고유한 소스가 많은 경우, 이는 시스템과 네트워크가 SSDP로 인한 중단에 취약함을 나타냅니다. 발신 인터페이스 및 고유 소스 수가 많을수록 서비스에 영향을 미칠 가능성이 높습니다.

그림 2: 샘플 출력 "show ip mroute 239.255.255.250" 명령을 실행할 수 있습니다.

```
Switch#show ip mroute 239.255.255.250
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.255.255.250), 00:08:35/stopped, RP 10.0.0.1, flags: SJC
  Incoming interface: GigabitEthernet0/0/1.40, RPF nbr 10.0.0.1
  Outgoing interface list:
    GigabitEthernet0/0/1.101, Forward/Sparse, 00:08:35/00:02:40
    GigabitEthernet0/0/1.102, Forward/Sparse, 00:08:35/00:02:38
    GigabitEthernet0/0/1.100, Forward/Sparse, 00:08:35/00:02:39

(10.1.1.2, 239.255.255.250), 00:01:40/00:01:19, flags: T
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/0/1.40, Forward/Sparse, 00:01:40/00:01:40, A
    GigabitEthernet0/0/1.100, Forward/Sparse, 00:01:40/00:02:39
    GigabitEthernet0/0/1.102, Forward/Sparse, 00:01:40/00:02:38
    GigabitEthernet0/0/1.101, Forward/Sparse, 00:01:40/00:02:40

(10.1.1.3, 239.255.255.250), 00:02:03/00:00:56, flags: JT
  Incoming interface: GigabitEthernet0/0/1.40, RPF nbr 10.1.1.1
  Outgoing interface list:
    GigabitEthernet0/0/1.100, Forward/Sparse, 00:02:03/00:02:39
```

```
    GigabitEthernet0/0/1.102, Forward/Sparse, 00:02:03/00:02:38
    GigabitEthernet0/0/1.101, Forward/Sparse, 00:02:03/00:02:40

(10.1.1.4, 239.255.255.250), 00:08:35/00:02:32, flags: T
  Incoming interface: GigabitEthernet0/0/1.40, RPF nbr 10.1.1.1
  Outgoing interface list:
    GigabitEthernet0/0/1.100, Forward/Sparse, 00:08:35/00:02:39
    GigabitEthernet0/0/1.102, Forward/Sparse, 00:08:35/00:02:38
    GigabitEthernet0/0/1.101, Forward/Sparse, 00:08:35/00:02:40, A
```

SSDP를 특정 용도로 사용하지 않는 한 이 출력은 비어 있거나, 발신 인터페이스 수가 적거나, 리소스 소모 및 서비스 영향을 방지하기 위해 고유한 소스 수가 낮습니다.

많은 멀티캐스트 그룹이 확인되면 "**show platform software object-manager fp active statistics**" 또는 "**show platform software object-manager fp switch active statistics**" 명령을 사용하여 하드웨어 리소스가 소진되었는지 확인할 수 있습니다.

> **참고:** 이 명령은 멀티캐스트 트래픽에 의해 트리거된 리소스 소진에만 한정되지 않으며, 다른 문제로 인해 이러한 값이 0이 아닐 수 있습니다.

그림 3: 출력 **"show platform software object-manager fp active statistics"**문제 상태

```
Switch#show platform software object-manager fp active statistics
Forwarding Manager Asynchronous Object Manager Statistics
Object update: Pending-issue: 109058, Pending-acknowledgement: 76928   <-- Pending-issue is very
high, this
Batch begin:   Pending-issue: 0, Pending-acknowledgement: 0                  is not expected.
Batch end:     Pending-issue: 0, Pending-acknowledgement: 0
Command:       Pending-acknowledgement: 0
Total-objects: 304085
Stale-objects: 0
Resolve-objects: 0
Childless-delete-objects: 530
Error-objects: 1098

Paused-types: 127
```

그림 3의 출력은 리소스 소모가 있는 스위치의 증상을 보여줍니다. 정상 작업 중에는 예상되지 않는 여러 명령 출력 행이 있습니다.

- 보류 중인 문제: 이 값은 0이거나 거의 0입니다. 이 값이 명령의 여러 번 반복에 비해 0이 아닌 큰 값으로 유지되면 이는 리소스 소모를 나타냅니다
- 승인 보류 중: 이 값은 0이거나 거의 0입니다. 이 값이 명령의 여러 번 반복에 비해 0이 아닌 큰 값으로 유지되면 이는 리소스 소모를 나타냅니다
- 자식-삭제 개체: 0이 될 것으로 예상되며 이에 가깝습니다. 10 이상의 값은 필요하지 않습니다.
- 오류 개체: 0이 될 것으로 예상되며 이에 가깝습니다. 10 이상의 값은 필요하지 않습니다.

"pending-issue" 또는 "pending-acknowledgement" 카운터가 많은 상태에서는 하드웨어가 잘못 프로그래밍될 위험이 커집니다. 잘못 프로그래밍된 하드웨어는 유니캐스트 및 멀티캐스트 트래픽에 대한 중단의 일반적인 원인입니다.

명령 "**show platform hardware fed switch active fwd-asic resource utilization**" or in some models "**show platform hardware fed active fwd-asic resource utilization**" ASIC에서 사용 중인 일부 한정된 리소스를 살펴보고 내부 리소스가 소진되었는지 확인하는 데 사용할 수 있습니다.

그림 4: 샘플 출력"show platform hardware fed active fwd-asic resource utilization"리소스가 거의 소진되지 않습니다.

```
Switch#show platform hardware fed active fwd-asic resource utilization
Resource Info for ASIC Instance: 0
Resource Name           Allocated Free
----------------------------------------
RSC_DI                    3822       38076
RSC_FAST_DI                  0         192
RSC_RIET_0                   1        1024
RSC_RIET_1                   0         512
RSC_RIET_2                   0         512
RSC_RIET_3                   0         512
RSC_RIET_4                   0         512
RSC_RIET_5                   0         512
RSC_RIET_6                   0         256
RSC_RIET_7                   0         255
RSC_VLAN_LE                116        3976
RSC_L3IF_LE                116        3907
RIM_RSC_DGT                  1         255
RSC_VPN_PREFIX_ID            1       32768
RSC_LABEL_STACK_ID           1       65536
RSC_RI                    7358       82730
RSC_LI_RI                    0         129
RSC_PORT_LE_RI               0        2048
RSC_PORT_LE                  0        1827
RSC_RI_REP                10635      120437
RSC_SI                    11842      119072
RSC_SI_IND                   1         255
RSC_SI_STATS              3550       45602
RSC_RCP1_FID                 1        1023
RSC_RCP2_FID                 1        1023
RSC_RCP3_FID                 1        1023
RSC_RCP4_FID                 1        1023
RSC_LV1_ECR                  1          63
RSC_LV2_ECR                  3         253
RSC_ENH_ECR                  1           0
RSC_RPF_MATCH               12        1012
RSC_PLC                      1        2047
RSC_PLC_PF                   1         255
RSC_MTU_INDEX                6         250
RSC_EGR_REDIRECT_INDEX       2        2046
RSC_RIL_INDEX 131065 7 <-- Free entries extremely low, this is not expected.
RSC_SIF                      1        1023
RSC_GROUP_LE                 1        1023
RSC_RI_REP_LOCAL             1           0
RSC_EXT_SI                 512       65024
```

그림 4에서 "RSC_RIL_INDEX"의 값은 131065개의 항목이 사용 중이며 7개만 사용 가능합니다. 이 리소스는 많은 고유 SSDP 그룹에서 사용됩니다. SSDP에 한정되지 않지만, 사용 가능한 항목 수가 적고 할당된 항목 수가 많은 리소스는 스위치가 용량 문제에 근접하고 있음을 나타내므로 반드시 조사해야 합니다.

명령 "**show platform hardware fed switch active fwd-asic resource tcam utilization**" or on some models "**show platform**

hardware fed active fwd-asic resource tcam utilization" ASIC별 리소스 사용률 분석을 확인하는 데 사용할 수 있습니다. SSDP 소진에서 가능한 또 다른 시그니처는 "L3 멀티캐스트 항목"이 "Max Values"에 근접하거나 "L3 Multicast entries"에 사용되는 "Used Values" 열입니다.

그림 5: 샘플 출력"show platform hardware fed active fwd-asic resource tcam utilization"정상 작동

```
Switch#show platform hardware fed active fwd-asic resource tcam utilization
CAM Utilization for ASIC  [0]
 Table                                              Max Values          Used Values
 ------------------------------------------------------------------------------------
 Unicast MAC addresses                               32768/768         6160/21
 L3 Multicast entries                                32768/768         3544/8        <-- Normal
Utilization, not near Max Values
 L2 Multicast entries                                 2304              181          <-- Normal
Utilization, not near Max Values
 Directly or indirectly connected routes            212992/1536       11903/39
 Input Ipv4 QoS Access Control Entries                5632              17
 Input Non Ipv4 QoS Access Control Entries            2560              36
 Output Ipv4 QoS Access Control Entries               6144              13
 Output Non Ipv4 QoS Access Control Entries           2048              27
 Input Ipv4 Security Access Control Entries           7168              12
 Input Non Ipv4 Security Access Control Entries       5120              76
 Output Ipv4 Security Access Control Entries          7168              11
 Output Non Ipv4 Security Access Control Entries      8192              27
 Ingress Netflow ACEs                                 1024               8
 Policy Based Routing ACEs                            3072              20
 Egress Netflow ACEs                                  1024               8
 Flow SPAN ACEs                                        512               5
 Flow Egress SPAN ACEs                                 512               8
 Control Plane Entries                                1024             235
 Tunnels                                              2816              26
 Lisp Instance Mapping Entries                         512               3
 Input Security Associations                           512               4
 SGT_DGT                                             32768/768           0/1
 CLIENT_LE                                            8192/512           0/0
 INPUT_GROUP_LE                                       1024               0
 OUTPUT_GROUP_LE                                      1024               0
 Macsec SPD                                            256               2
```

SSDP로 인한 리소스 소모 방지

리소스 소모를 중지하려면 첫 번째 L3 홉과 멀티캐스트 상태 생성 전에 SSDP 트래픽을 중지해야 합니다. 가장 빠른 솔루션은 인그레스(ingress)에 적용된 IPv4 ACL(Access Control List)을 이 트래픽을 확인하는 PIM으로 구성된 모든 L3 인터페이스에 사용하는 것입니다. "**show ip mroute 239.255.255.250**" 명령을 사용하여 확인하고 각 그룹에 대해 "Incoming Interface"를 확인합니다. 이는 트래픽의 소스가 되는 L3 인터페이스를 나타내며 둘 이상의 고유한 소스 인터페이스가 있을 수 있음을 나타냅니다. 이 컨피그레이션 예에서는 SSDP가 레이어 2에서 작동하고 L2 인접 호스트가 PNP 서비스를 검색할 수 있도록 허용하지만, 클라이언트 광고가 L3 경계를 통해 전달되지 않도록 하고, 멀티캐스트 라우터 또는 스위치에서 L3 멀티캐스트 상태 생성을 방지합니다.

확장 ACL을 구성합니다.

```
ip access-list extended BLOCK_SSDP remark Block SSDP deny ip any host 239.255.255.250  <-- Deny SSDP
permit ip any any    <-- Permit any other group
```

각 L3 인터페이스에서 ACL을 인그레스 방향으로 적용합니다.

```
Switch#configure terminal
Switch(config)#interface vlan100
Switch(config-if)#ip access-group BLOCK_SSDP in
Switch(config-if)#end
```