Cisco Catalyst 스위치에서 MAC Flaps/Loop 문제 해결

목차

소개

이 문서에서는 Cisco Catalyst 스위치에서 MAC Flaps/Loop 문제를 해결하는 방법을 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 기본적인 스위칭 개념에 대한 기본적인 지식과 Cisco Catalyst 스위치의 STP(Spanning Tree Protocol) 및 기능에 대한 이해를 권장합니다.

사용되는 구성 요소

이 문서의 정보는 모든 버전의 Cisco Catalyst 스위치를 기반으로 합니다(이 문서는 특정 소프트웨어 또는 하드웨어 버전으로 제한되지 않음).

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.

배경 정보

이 문서는 Cisco Catalyst 스위치의 MAC 플랩 또는 루프 문제를 해결하는 체계적인 접근 방법을 설명하는 가이드 역할을 합니다. MAC 플랩/루프는 스위치의 MAC 주소 테이블 불일치로 인한 네트워크 중단입니다. 이 문서에서는 이러한 문제를 식별하고 해결하기 위한 단계를 제공할 뿐만 아니라 이해를 돕기 위한 실용적인 예도 제공합니다.

MAC 플래핑이란 무엇입니까?

MAC 플랩은 스위치에서 동일한 MAC 소스 주소가 있지만 처음에 학습한 인터페이스와는 다른 인터페이스의 프레임을 수신할 때 발생합니다. 그러면 스위치가 포트 사이를 플랩하여 MAC 주소 테이블을 새 인터페이스로 업데이트합니다. 이러한 상황은 네트워크의 불안정을 야기하고 성능 문제를 초래할 수 있습니다.

Cisco 스위치에서 MAC 플래핑은 일반적으로 다음과 유사한 메시지로 로깅됩니다.

```
"%SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan x is flapping between port (1) and port (2)"
```

이 예에서 MAC 주소는xxxx.xxxx.xxxx먼저 인터페이스 포트 (1)에서 학습된 다음 인터페이스 포트 (2)에서 확인되어 MAC 플랩이 발생했습니다.

MAC 플래핑의 가장 일반적인 원인은 네트워크에서 레이어 2 루프이며, STP의 잘못된 구성 또는 이중화 링크 문제로 인해 발생하는 경우가 많습니다. 다른 원인으로는 하드웨어 오류, 소프트웨어 버그 또는 MAC 스푸핑과 같은 보안 문제가 있을 수 있습니다.

MAC 플랩 트러블슈팅에는 종종 네트워크의 루프를 식별 및 해결, 디바이스 컨피그레이션 확인 또는 디바이스 펌웨어/소프트웨어 업데이트가 포함됩니다.

일반 문제 해결 지침

- MAC Flapping(MAC 플래핑) 식별: 스위치에서 MAC 플래핑을 나타내는 로그를 확인합니다. 예를 들어 Cisco 스위치에서 로그 메시지는 다음과 같습니다.

```
%SW_MATM-4-MACFLAP_NOTIF: Host [mac_address] in vlan [vlan_id] is flapping between port [port_id_
```

- MAC Address and Interfaces(MAC 주소 및 인터페이스) 참고: 로그 메시지는 플래핑되는 MAC 주소와 플래핑되는 인터페이스를 제공합니다. 조사에 도움이 될 수 있도록 이러한 사항

을 기록해 두십시오.

- Investigate the Affected Interfaces(영향을 받는 인터페이스 조사): 관련된 인터페이스를 조사하려면 스위치의 CLI를 사용합니다. 또는 같은 명령을 사용하여show interfacesshow mac address-table어떤 디바이스가 인터페이스에 연결되었고 MAC 주소가 어디에서 학습되는지 확인할 수 있습니다.

- 플래핑 MAC 주소 추적: MAC은 포트 X와 Y를 통해 학습합니다. 한 포트는 MAC이 연결된 곳으로, 다른 포트는 루프로 연결됩니다. 포트를 선택하고 경로의 각 레이어 2 스위치에서 명령을 사용하여show mac address-table작업을 시작합니다.

- 물리적 루프 확인: 네트워크 토폴로지를 확인하여 물리적 루프가 있는지 확인합니다. 스위치 간에 경로가 여러 개인 경우 이러한 문제가 발생할 수 있습니다. 루프가 발견되면 루프를 제거하려면 네트워크를 다시 구성해야 합니다.

- STP 확인: STP는 특정 경로를 차단하여 네트워크에서 루프를 방지하기 위해 설계되었습니다. STP가 잘못 구성되면 루프를 방지하지 않습니다. STP 컨피그레이션을 확인하기 위해 같은show spanning-tree명령을 사용합니다. 또한 명령을 사용하여 TCN(Topology Change Notifications)을 확인합니다show spanning-tree detail | include ieee|occur|from|is.

- 중복 MAC 주소 확인: 네트워크에 있는 두 디바이스의 MAC 주소가 동일한 경우(대부분 HA(High Availability) 설정과 여러 NIC(Network Interface Controller or Cards)에 표시됨) MAC 플래핑이 발생할 수 있습니다. 네트워크에서show mac address-table중복된 MAC 주소를 검색하려면 이 명령을 사용합니다.

- 결함이 있는 하드웨어 또는 케이블 확인: 결함이 있는 네트워크 케이블 또는 하드웨어로 인해 잘못된 인터페이스로 프레임이 전송되어 MAC 플래핑이 발생할 수 있습니다. 케이블의 물리적 상태를 확인하고 문제가 지속되는지 확인하기 위해 하드웨어를 교체해 보십시오. 인터페이스 플래핑은 스위치에서 MAC 플래핑을 일으킬 수도 있습니다.

- 소프트웨어 버그 확인: 때때로 MAC 플래핑은 네트워크 장치의 소프트웨어에 있는 버그로 인해 발생할 수 있습니다. 버그 검색 툴을 확인합니다.

버그 검색 도구: https://bst.cloudapps.cisco.com/bugsearch

버그 검색 도구 도움말:
https://www.cisco.com/c/en/us/support/web/tools/bst/bsthelp/index.html#search

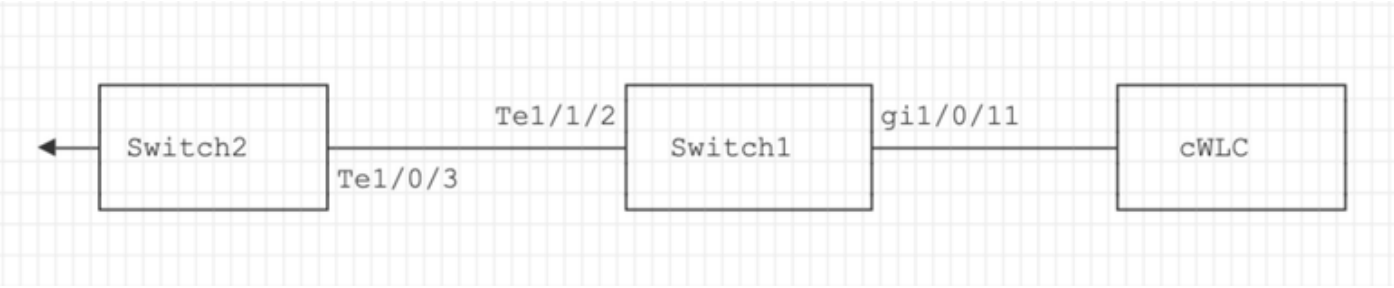
- TAC 지원에 문의: 모든 방법을 시도했지만 문제가 지속되는 경우 Cisco TAC 지원에 문의할 수 있습니다. 추가적인 지원을 제공할 수 있습니다.

사례 연구 1

문제 설명

eWLC 컨트롤러에서 게이트웨이에 대한 연결이 끊어지고 패킷 삭제로 인해 AP가 컨트롤러에 조인할 수 없습니다.

토폴로지



문제 해결 단계

MAC 플래핑은 eWLC에 연결된 스위치(Switch1)에서 확인되었습니다.

```
*Aug  5 05:52:50.750: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:03.327: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:21.466: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
```

MAC 학습:

포트에서show mac address-table address
학습된 MAC 주소를 확인하려면 명령을 입력합니다.

<#root>

```
Switch1#show mac address-table address 0000.5e00.0101

          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.5e00.0101    DYNAMIC     Gi1/0/11


   4    0000.5e00.0101    DYNAMIC     Te1/1/2
```

포트 Gi1/0/11 및 Te1/1/2 구성:

인터페이스 컨피그레이션show running-config interface
을 확인하려면 명령을 입력합니다.

<#root>

```
interface GigabitEthernet1/0/11
```

```
 switchport trunk native vlan 4
 switchport mode trunk
end
```

```
interface TenGigabitEthernet1/1/2
```

```
 switchport mode trunk
end
```

포트 Gi1/0/11 및 Te1/1/2의 CDP 네이버:

연결된 디바이스show cdp neighbors
의 세부 정보를 확인하려면 명령을 입력합니다.

<#root>

```
Switch1#show cdp neighbors gi1/0/11
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
eWLC            Gig 1/0/11        130              R T   C9115AXI- Gig 0 < ----- eWLC Controller
```

```
Switch1#show cdp neighbors gi1/1/2
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Switch2
                Ten 1/1/2         163             R S I  C9500-16X Ten 1/0/3 < ----- Uplink Switch
```

스위치 2의 MAC 학습(업링크 스위치):

포트에서show mac address-table address
학습된 MAC 주소를 확인하려면 명령을 입력합니다.

<#root>

```
Switch2#show mac address-table address 0000.5E00.0101
```

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.5e00.0101    STATIC
```

Vl4 < ----- VRRP MAC of Vlan4

```
   4    0000.5e00.0101    DYNAMIC
```

Te1/0/13 < ----- Learning from Switch1 (eWLC connected Switch)

<#root>

Switch2#show vrrp vlan 4

Vlan4 - Group 1

```
 - Address-Family IPv4
  State is MASTER
  State duration 5 days 4 hours 22 mins
  Virtual IP address is x.x.x.x
```

Virtual MAC address is 0000.5E00.0101 < ------ VRRP MAC of Vlan4

```
  Advertisement interval is 1000 msec
```

근본 원인

스위치 2의 VRRP(Virtual Router Redundancy Protocol) ID와 eWLC가 동일하여 VRRP에서 동일한 가상 MAC을 생성함을 검증하였다.

해결

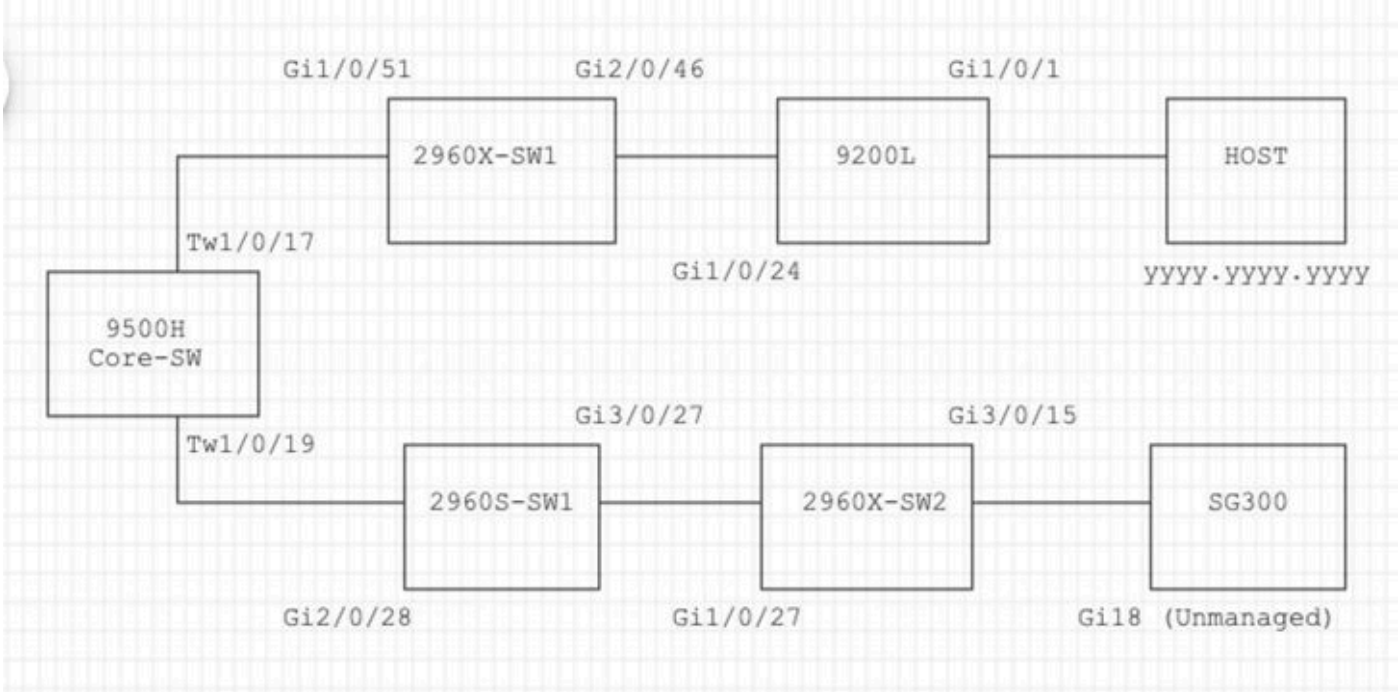
WLC에서 VRRP 인스턴스를 변경한 후 문제가 해결되었습니다. 이 경우 스위치에서 중복 MAC가 발생하여 게이트웨이에 대한 연결이 끊어지고 패킷이 삭제되어 AP가 컨트롤러에 조인할 수 없습니다.

사례 연구 2

문제 설명

일부 서버에 액세스할 수 없거나 심각한 대기 시간/삭제 현상이 발생했습니다.

토폴로지



문제 해결 단계

1. 코어 스위치에서 발생하는 MAC 플래핑을 발견했습니다.

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port Tw
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port Tw
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port Po
```

2. 문제 해결 프로세스yyyy.yyyy.yyyy를 위한 MAC 주소를 선택합니다.

MAC 학습:

포트에서show mac address-table address
학습된 MAC 주소를 확인하려면 명령을 입력합니다.

<#root>

```
Core-SW#show mac address-table address yyyy.yyyy.yyyy

          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy    DYNAMIC     Twe1/0/17
```

TWE 1/0/17 및 Twe 1/0/17 포트의 CDP 네이버:

연결된 디바이스show cdp neighbors
의 세부 정보를 확인하려면 명령을 입력합니다.

<#root>

```
Core-SW#show cdp neighbors Twe 1/0/17


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

2960X-SW1


                 Twe 1/0/17        162              S I   WS-C2960X Gig 1/0/51



Core-SW#show cdp neighbors Twe 1/0/19


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

2960S-SW1


                 Twe 1/0/19        120              S I   WS-C2960S Gig 2/0/28
```

Core-SW Twe1/0/17에 연결된 2960X-SW1의 로그:

MACyyyy.yyyy.yyyy이 포트 Gi1/0/51과 Gi2/0/46(9200L) 사이에서 플래핑합니다.

<#root>

```
2960X-SW1#show mac address-table address yyyy.yyyy.yyyy


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy    DYNAMIC     Gi1/0/51



2960X-SW1#show mac address-table address yyyy.yyyy.yyyy


          Mac Address Table
```

```
----------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi2/0/46
```

2960X-SW1#show run interface gi 1/0/51

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/51
switchport mode trunk
end
```

2960X-SW1#show run interface gi 2/0/46

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet2/0/46
switchport mode trunk
end
```

9200L의 로그:

(이 포트는 이 MAC 주소의 올바른 포트입니다.)

<#root>

9200L#show mac address-table address yyyy.yyyy.yyyy

```
          Mac Address Table
----------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi1/0/1
```

9200L#show run interface gi 1/0/1

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/1
switchport mode access
end
```

Core-SW Twe1/0/19에 연결된 2960S-SW1:

(루프 경로로 보입니다.) 루프를 완화하기 위해 Core-SW의 포트가 종료되었습니다.

그러나 Core-SW에서는 여전히 MAC 플랩(flap)이 관찰되었습니다.

2960S-SW1의 로그:

<#root>

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port G
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port G
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port G
```

2960S-SW1#show run interface gi 3/0/27

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet3/0/27
switchport mode trunk
end
```

2960S-SW1#show cdp neighbor gi 3/0/27

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

2960X-SW2

Gig 3/0/27 176 S I WS-C2960X Gig 1/0/27

2960X-SW2의 로그:

<#root>

2960X-SW2#show run interface gi 3/0/15

```
Building configuration...

Current configuration : 39 bytes
!
interface GigabitEthernet3/0/15
end
```

```
2960X-SW2#show cdp neighbor gi 3/0/15


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

SG300     Gig 3/0/15        157              S I   SG300-28P gi18




2960X-SW2#config terminal


2960X-SW2(config)#interface gi 3/0/15


2960X-SW2(config-if)#shutdown
```

근본 원인

네트워크에 연결된 SG300(비관리형) 스위치 때문에 MAC 플랩이 발생했습니다.

해결

비관리 스위치 SG300에 연결된 포트를 종료하여 MAC 플래핑 문제를 해결했습니다.

예방

STP 포트패스트:

STP PortFast를 사용하면 레이어 2 LAN 포트가 수신 및 학습 상태를 우회하여 전달 상태로 즉시 전환됩니다. STP PortFast는 STP BPDU(Bridge Protocol Data Unit)를 수신하지 않는 포트에서 의미가 없는 STP TCN이 생성되는 것을 방지합니다. STP PortFast는 VLAN을 종료하는 엔드 호스트 장치에 연결되어 있고 포트가 브리징을 지원하도록 구성되지 않은 라우터의 워크스테이션, 서버, 포트 등과 같이 STP BPDU를 수신하지 않아야 하는 포트에서만 구성합니다.

BPDU 가드:

STP BPDU Guard는 STP PortFast의 기능을 보완합니다. STP PortFast 지원 포트에서 STP BPDU Guard는 STP PortFast가 활성화된 경우 STP가 제공할 수 없는 레이어 2 루프를 보호합니다. STP BPDU 가드는 BPDU를 수신하는 포트를 종료합니다.

루트 가드:

루트 가드는 포트가 STP 루트 포트가 되는 것을 방지합니다. STP 루트 가드를 사용하여 부적합한 포트가 STP 루트 포트가 되는 것을 방지합니다. 부적합한 포트의 예는 직접 네트워크 관리 제어 외부에 있는 디바이스에 링크되는 포트입니다.

루프 가드:

Loop Guard는 STP를 위한 Cisco 고유의 최적화 기능입니다. Loop Guard는 포인트-투-포인트 링크(예: 네트워크 인터페이스 오작동 또는 사용 중인 CPU)에서 BPDU의 정상적인 포워딩을 방해하는 경우 발생하는 루프로부터 레이어 2 네트워크를 보호합니다. 루프 가드는 UDLD(Unidirectional Link Detection)에서 제공하는 단방향 링크 장애에 대한 보호를 보완합니다. 루프 가드는 장애를 격리하고 STP가 안정적인 토폴로지로 수렴할 수 있도록 해주며, 장애가 발생한 구성 요소는 STP 토폴로지에서 제외됩니다.

BPDU 필터:

이렇게 하면 STP가 비활성화됩니다. BPDU는 수신 시 전송 또는 처리되지 않습니다. 반드시 엔터프라이즈 네트워크일 필요는 없으며, 통신 사업자에게 흔히 사용됩니다.

UDLD Aggressive:

Cisco 전용 UDLD 프로토콜은 UDLD를 지원하는 디바이스와 포트 간 링크의 물리적 컨피그레이션을 모니터링합니다. UDLD는 단방향 링크의 존재를 탐지합니다. UDLD는 일반 또는 적극적인 모드에서 작동할 수 있습니다. 일반 모드 UDLD는 수신된 UDLD 패킷에 인접 디바이스에 대해 올바른 정보가 포함되어 있지 않은 경우 링크를 단방향으로 분류합니다. 일반 모드 UDLD의 기능 외에, 이전에 동기화된 두 인접 디바이스 간의 관계를 다시 설정할 수 없는 경우 aggressive 모드 UDLD는 포트를 err-disabled 상태로 전환합니다.

스톰 컨트롤:

트래픽 스톰 제어는 하드웨어에서 구현되며 스위치의 전체 성능에 영향을 미치지 않습니다. 일반적으로 PC 및 서버와 같은 엔드 스테이션은 억제할 수 있는 브로드캐스트 트래픽의 소스입니다. 과도한 브로드캐스트 트래픽의 불필요한 처리를 방지하려면 엔드 스테이션에 연결되는 액세스 포트 및 주요 네트워크 노드에 연결되는 포트에서 브로드캐스트 트래픽에 대한 트래픽 스톰 제어를 활성화합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.