

UDLD 프로토콜 기능 구성

목차

- [소개](#)
 - [사전 요구 사항](#)
 - [요구 사항](#)
 - [사용되는 구성 요소](#)
 - [표기 규칙](#)
 - [문제 정의](#)
 - [단방향 링크 감지 프로토콜의 작동 방식](#)
 - [UDLD 작동 모드](#)
 - [사용 가능성](#)
 - [구성 및 모니터링](#)
 - [관련 정보](#)
-

소개

이 문서에서는 UDLD(Unidirectional Link Detection) 프로토콜이 스위치 네트워크에서 루프 및 트래픽 변칙을 방지하는 데 어떻게 도움이 되는지 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

표기 규칙

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

문제 정의

STP(Spanning-Tree Protocol)는 이중화된 물리적 토폴로지를 루프 프리(loop-free) 트리와 같은 포워드 토폴로지로 변환합니다.

이를 위해 하나 이상의 포트를 차단합니다. 하나 이상의 포트가 차단된 상태에서 전달 토폴로지에는 루프가 없습니다. STP는 BPDU(Bridge Protocol Data Unit)의 수신 및 전송에 대한 작업을 사용합니다. 차단 상태의 포트가 있는 스위치에서 실행되는 STP 프로세스가 업스트림(지정된) 스위치에서 BPDU를 수신하지 않는 경우, STP는 결국 포트에 대한 STP 정보를 에이징 아웃하고 전달 상태로 전환합니다.

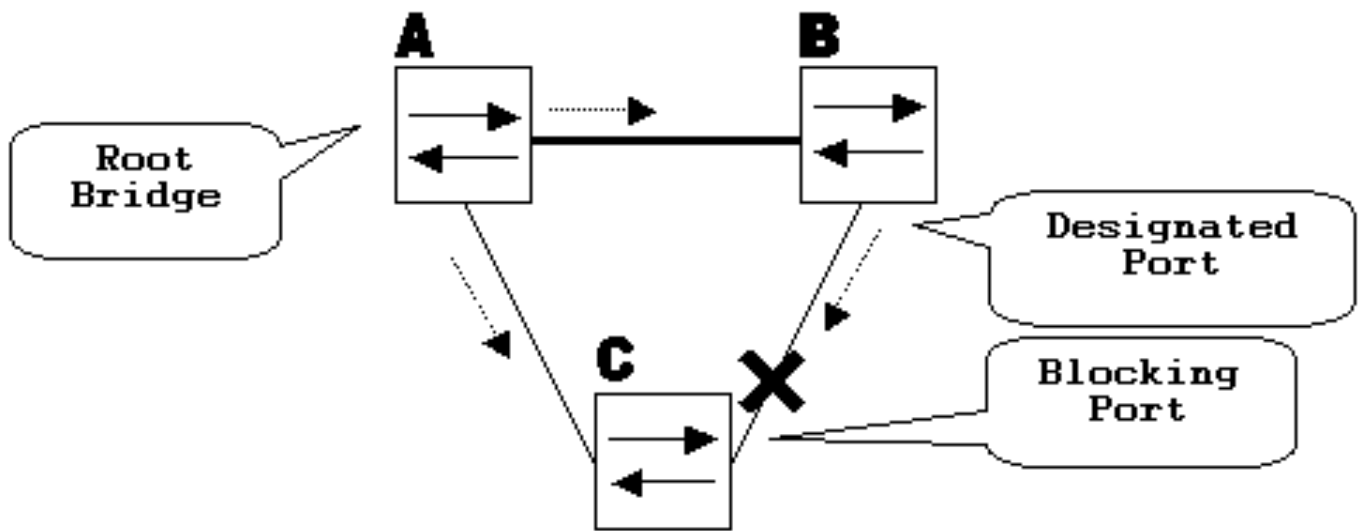
이렇게 하면 패킷이 반복 경로를 따라 무한 순환하기 시작하고 더 많은 대역폭과 리소스를 소비하는 STP 루프를 생성할 수 있습니다. 이로 인해 네트워크 중단이 발생할 수 있습니다.

포트가 작동하는 동안 스위치에서 BPDU를 수신하지 못하는 방법은 무엇입니까? 그 이유는 단방향 링크입니다.

이러한 경우 링크는 단방향으로 간주됩니다.

- 링크가 연결의 양쪽에 있습니다.
- 로컬측은 원격측이 전송한 패킷을 수신하지 않는 반면 원격측은 로컬측이 전송한 패킷을 수신한다.

이 시나리오를 고려해 보십시오. 화살표는 STP BPDU의 흐름을 나타냅니다.



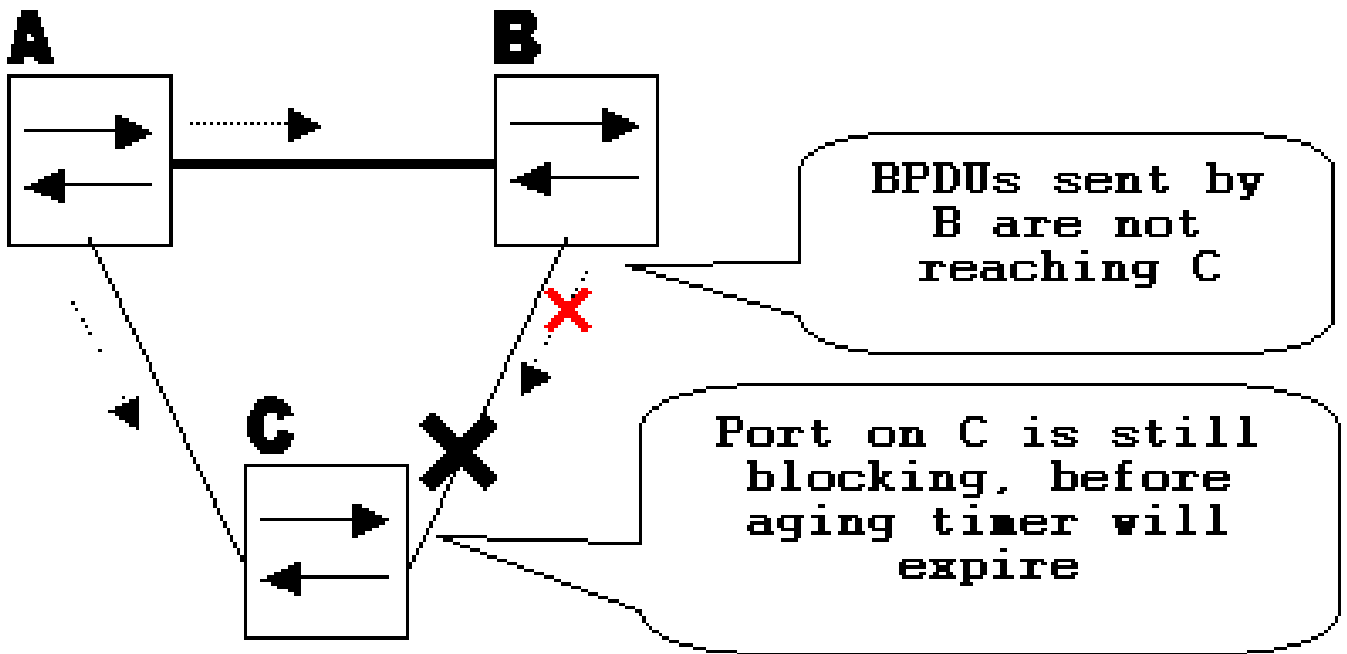
정상 작동 중에 브리지 B는 링크 B-C에서 지정된 포트입니다. 브리지 B는 BPDU를 포트를 차단하는 C로 전송합니다. C가 해당 링크의 B에서 BPDU를 확인하는 동안 포트가 차단됩니다.

이제 링크 B-C가 C 방향으로 실패하면 어떻게 되는지 생각해 보십시오. C가 B에서 트래픽을 수신하지 않지만 B는 여전히 C에서 트래픽을 수신합니다.

위로

C는 링크 B-C에서 BPDU를 수신하지 않으며, 마지막 BPDU로 수신한 정보를 에이징합니다. 최대 20초가 걸리며 이는 maxAge STP 타이머에 따라 달라집니다. 포트에서 STP 정보가 에이징 아웃되면 해당 포트는 차단 상태에서 듣기, 학습 및 전달 STP 상태로 전환됩니다. 이렇게 하면 삼각형 A-B-C에 차단된 포트가 없으므로 루프가 생성됩니다. 패킷이 경로를 따라 순환하며(B는 C에서 패킷을 수신함), 링크가 완전히 채워질 때까지 추가 대역폭을 소비합니다.

이 시나리오에서는 네트워크가 중단될 수 있습니다. 단방향 링크로 인해 발생할 수 있는 또 다른 문제는 트래픽 블랙홀입니다.



단방향 링크 감지 프로토콜의 작동 방식

UDLD는 레이어 1(L1) 메커니즘과 함께 작동하여 링크의 물리적 상태를 결정하는 레이어 2(L2) 프로토콜입니다. 레이어 1에서 자동 협상은 물리적 신호 처리와 결함 탐지를 처리합니다. UDLD는 자동 협상이 수행할 수 없는 작업(예: 네이버 ID 탐지 및 잘못 연결된 포트 종료)을 수행합니다. 자동 협상과 UDLD를 모두 활성화하면 레이어 1 및 레이어 2 탐지가 함께 작동하여 물리적/논리적 단방향 연결과 다른 프로토콜의 오작동을 방지합니다.

UDLD는 인접 디바이스 간의 프로토콜 패킷 교환을 통해 작동합니다. UDLD가 작동하려면 링크의 두 디바이스 모두 UDLD를 지원하고 해당 포트에서 활성화해야 합니다.

UDLD에 대해 구성된 각 스위치 포트는 포트 디바이스/포트 ID 및 해당 포트에서 UDLD에 표시된 인접 디바이스/포트 ID를 포함하는 UDLD 프로토콜 패킷을 전송합니다. 인접한 포트는 다른 쪽에서 받은 패킷에서 자체 디바이스/포트 ID(에코)를 볼 수 있습니다. 특정 시간 동안 들어오는 UDLD 패킷에서 포트에 자체 디바이스/포트 ID가 없으면 링크가 단방향으로 간주됩니다.

이 에코 알고리즘에서는 다음 문제를 탐지할 수 있습니다.

- 링크가 양쪽에서 모두 작동하지만 패킷은 한쪽에서만 수신됩니다.
- 피이버를 받을 때와 보낼 때의 연결(전선) 실수가 원격측의 동일한 포트에 연결되지 않는다.

UDLD에서 단방향 링크가 탐지되면 해당 포트가 비활성화되고 이 메시지가 콘솔에 출력됩니다.

```
UDLD-3-DISABLE: Unidirectional link detected on port 1/2. Port disabled
```

UDLD에 의한 포트 종료는 수동으로 활성화되거나 tilerdisabletimeout이 만료될 때까지 비활성화됩니다(구성된 경우).

UDLD 작동 모드

UDLD는 일반과 적극적인 두 가지 모드로 작동할 수 있습니다.

- 일반 모드에서 포트의 링크 상태가 양방향이라고 판단되고 UDLD 정보가 시간 초과되면 UDLD는 아무런 조치도 취하지 않습니다. UDLD의 포트 상태가 undetermined(미결정)로 표시됩니다. 포트는 STP 상태에 따라 작동합니다.
- Aggressive 모드에서 포트의 링크 상태가 양방향임을 확인하고 포트의 링크가 계속 작동 중인 동안 UDLD 정보가 시간 초과되면 UDLD는 포트의 상태를 다시 설정하려고 시도합니다. 성공하지 못하면 포트는 errdisable 상태가 됩니다.

UDLD 정보 시간 초과는 UDLD를 실행하는 포트가 보류 시간 동안 인접 포트에서 UDLD 패킷을 수신하지 못할 때 발생합니다. 포트의 보류 시간은 원격 포트에 의해 지정되며 원격 측의 메시지 간격에 따라 달라집니다. 메시지 간격이 짧을수록 대기 시간이 짧아지고 탐지 속도가 빨라집니다. UDLD의 최근 구현은 메시지 간격의 컨피그레이션을 허용합니다. 일부 물리적 문제 또는 이중 불일치로 인한 포트의 높은 오류율로 인해 UDLD 정보가 오래될 수 있습니다. 이러한 패킷 삭제는 링크가 단방향임을 의미하지 않으며 일반 모드의 UDLD는 그러한 링크를 비활성화하지 않습니다.

적절한 탐지 시간을 보장하려면 적절한 메시지 간격을 선택할 수 있어야 합니다. 전달 루프가 생성되기 전에 단방향 링크를 탐지할 수 있을 만큼 메시지 간격이 빨라야 하지만 스위치 CPU를 과부하해서는 안 됩니다. 기본 메시지 간격은 15초이며, 기본 STP 타이머를 사용하여 정방향 루프가 생성되기 전에 단방향 링크를 탐지할 수 있을 만큼 빠릅니다. 탐지 시간은 메시지 간격의 약 3배와 같습니다.

예: $T_{\text{detection}} \sim \text{message_interval} \times 3$

기본 메시지 간격 15초의 경우 45초입니다.

단방향 링크 장애가 발생할 경우 STP가 다시 통합되려면 $T_{\text{reconvergence}} = \text{max_age} + 2 \times \text{forward_delay}$ 가 필요합니다. 기본 타이머의 경우 $20 + 2 \times 15 = 50$ 초가 소요됩니다.

$T_{\text{detection}} < T_{\text{reconvergence}}$ 를 유지하고 적절한 메시지 간격을 선택하는 것이 좋습니다.

Aggressive 모드에서 정보가 에이징되면 UDLD는 링크 상태를 다시 설정하고 8초 동안 1초마다 패킷을 전송합니다. 링크 상태가 여전히 확인되지 않으면 링크가 비활성화됩니다.

Aggressivemode는 다음과 같은 상황에 대한 추가 탐지를 추가합니다.

- 포트가 고정됩니다(한쪽 면에는 포트가 전송 또는 수신하지 않지만 링크는 양쪽 모두 작동).
- 링크는 한 면에 위쪽에 있고 다른 면에 아래쪽으로 있습니다. 이 문제는 파이버 포트에서 전송 파이버가 로컬 포트에서 플러그를 뽑았을 때 링크가 로컬 쪽에서 가동 상태로 남아 있는 것을 볼 수 있습니다. 그러나 원격에서 </tt> 다운됩니다.

가장 최근에 파이버 FastEthernet 하드웨어 구현에는 이러한 상황에서 양쪽의 링크를 아래로 보내기 위해 FEFI(Far End Fault Indication) 기능이 있습니다. GigabitEthernet에서도 링크 협상을 통해 유

사한 기능을 제공합니다. 구리 포트는 이더넷 링크 펄스를 사용하여 링크를 모니터링하므로 일반적으로 이러한 유형의 문제에 취약하지 않습니다. 두 경우 모두 포트 간에 연결이 없기 때문에 정방향 루프가 발생하지 않는다는 점을 언급해야 합니다. 그러나 링크가 한 쪽에 있는 경우 다른 쪽에 있는 경우 트래픽 블랙홀이 발생할 수 있습니다. 이를 방지하기 위해 Aggressive UDLD를 설계하였다.

사용 가능성

UDLD는 Cisco IOS® Software Release 12 이상에서 일반 모드와 적극적인 모드로 사용할 수 있습니다.

구성 및 모니터링

show uddl 명령을 실행하여 인터페이스에서 UDLD가 활성화되어 있는지 확인합니다.

```
<#root>
```

```
Switch#
```

```
show uddl
```

```
Interface Gi1/0/1
```

```
---
```

```
Port enable administrative configuration setting: Disabled
```

```
Port enable operational state: Disabled
```

```
Current bidirectional state: Unknown
```

```
Interface Gi1/0/2
```

```
---
```

```
Port enable administrative configuration setting: Disabled
```

```
Port enable operational state: Disabled
```

```
Current bidirectional state: Unknown
```

```
Interface Gi1/0/3
```

```
---
```

```
Port enable administrative configuration setting: Disabled
```

```
Port enable operational state: Disabled
```

```
Current bidirectional state: Unknown
```

Aggressive UDLD는 `uddl port aggressive` 명령을 사용합니다:

```
<#root>
```

```
Switch#
```

```
configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)#
```

```
interface gigabitEthernet1/0/1
```

```
Switch(config-if)#
udld port aggressive
```

```
Switch(config-if)#
end
```

```
Switch#
```

명령 `show udld`

및 `show udld neighbors` 명령어로 포트에서 UDLD가 활성화되었는지 또는 비활성화되었는지, 그리고 링크 및 인접 디바이스 상태가 무엇인지 확인할 수 있습니다.

```
<#root>
```

```
Switch#
```

```
show udld GigabitEthernet1/0/1
```

```
Interface Gi1/0/1
```

```
---
```

```
Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state:
```

```
Enabled / in aggressive mode
```

```
Current bidirectional state:
```

```
Bidirectional
```

```
Current operational state: Advertisement - Single neighbor detected
```

```
Message interval: 15000 ms
```

```
Time out interval: 5000 ms
```

```
Port fast-hello configuration setting: Disabled
```

```
Port fast-hello interval: 0 ms
```

```
Port fast-hello operational state: Disabled
```

```
Neighbor fast-hello configuration setting: Disabled
```

```
Neighbor fast-hello interval: Unknown
```

```
Entry 1
```

```
---
```

```
Expiration time: 31600 ms
```

```
Cache Device index: 1
```

```
Current neighbor state:
```

```
Bidirectional
```

```
Device ID: 346288238580
```

```
Port ID: Gi4/0/1
```

```
Neighbor echo 1 device: 70B4F35F080
```

```
Neighbor echo 1 port: Gi1/0/1
TLV Message interval: 15 sec
No TLV fast-hello interval
TLV Time out interval: 5
TLV CDP Device name: MXC.TAC.M.02-3850-01
```

<#root>

Switch#

```
show udd neighbors
```

Port	Device Name	Device ID	Port ID	Neighbor State
Gi1/0/1	346288238580	1	Gi4/0/1	Bidirectional

Total number of bidirectional entries displayed: 1

이 `udld message time` 메시지 간격을 변경하는 명령:

<#root>

Switch(config)#

```
udld message time 10
```

UDLD message interval set to 10 seconds

간격은 1~90초이며 기본값은 15초입니다.

관련 정보

- [Cisco 기술 지원 및 다운로드](#)
- Catalyst 3560 스위치의 경우 UDLD [구성을 참조하십시오](#).
- Cisco IOS를 실행하는 Catalyst 4500/4000의 경우 UDLD [구성을 참조하십시오](#).
- Catalyst 9300 스위치의 경우 UDLD [구성 방법을 참조하십시오](#)
- Catalyst 9500 스위치의 경우 UDLD [구성 방법을 참조하십시오](#)

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.