

# StarOS의 합법적 차단 컨텍스트에서 "버퍼" 컨피그레이션 문제 해결

## 목차

- [소개](#)
- [사전 요구 사항](#)
- [요구 사항](#)
- [사용되는 구성 요소](#)
- [약어](#)
- [문제](#)
- [합법적 감청\(Lawful Intercept\)](#)
- [문제 해결](#)
- [해결](#)
- [설정](#)

## 소개

이 문서에서는 StarOS의 합법적 차단 컨텍스트에서 "버퍼" 컨피그레이션의 문제를 해결하는 방법을 설명합니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 StarOS에 대한 지식이 있는 것을 권장합니다.

### 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.

## 약어

리	합법적 감청(Lawful Intercept)
레아	사법 당국
AF	접근 기능
MF	중재 함수
DF	전달 함수
CF	제어 기능
이리	인터셉트 관련 정보
참조	커뮤니케이션 내용

AF는 모든 StarOS 노드가 될 수 있습니다. CF는 LEA 프리미엄 또는 관리 도메인에 있습니다.

## 문제

적법한 차단 모듈에서 버퍼링 옵션을 구성할 때, 이벤트/콘텐츠 기반 버퍼링 옵션 관련 파라미터를 CLI 컨피그레이션 리스트에서 사용할 수 없었음이 관찰된다.

이 옵션은 NI 컨텍스트당 기본 5000개의 IRI 레코드 및 1000개의 CC 레코드의 버퍼 값을 정의하는데 도움이 됩니다.

컨피그레이션 목록에서 사용할 수 있는 유일한 옵션은 "dest-addr"이었습니다.

```
[li-context]<hostname>(config-ctx)# lawful-intercept tcp event-delivery
dest-addr - Destination IP address where the intercepted information needs to be forwarded.
```

앞서 언급한 옵션 목록에서 "dest-addr" 옵션과 함께 "buffer" 키워드를 표시하는 것이 좋습니다.

## 합법적 감청(Lawful Intercept)

**참고:** Lawful Intercept는 라이선스 지원 기능입니다. Basic Lawful Intercept 라이선스는 활성 가입자를 위한 CC(Call Content) 가로채기를 위한 전송 프로토콜로서 UDP를 지원합니다. IRI(Event Interception) 가로채기와 전송을 위한 전송 프로토콜인 TCP는 Basic 라이선스에서 지원되지 않습니다. Enhanced Lawful Intercept 라이선스는 모든 기본 NI 라이선스 기능과 함께 IRI(Event Interception) 및 가로채기 패킷 전달을 위한 전송 프로토콜인 TCP를 지원합니다.

Lawful Intercept 기능은 네트워크 운영자에게 대상 모바일 사용자의 제어 및 데이터 메시지를 가로챌 수 있는 기능을 제공합니다. 이러한 지원을 호출하기 위해, LEA는 네트워크 운영자에게 특정 모바일 사용자의 인터셉션을 시작하도록 요청할 것이다. 이 요청은 법원의 명령이나 영장에 의해 뒷받침될 것이다. 국가마다 합법적 감청 기준이 다릅니다.

일반적인 합법적 감청 프로세스에는 다음과 같은 일련의 이벤트가 포함됩니다.

1. LEA는 특정 개인의 세션을 가로채기 시작할 것을 TSP에 요청합니다. 이는 일반적으로 법원 명령 또는 영장에 의해 지원되어야 합니다. 개인을 식별할 수 있는 정보(전화 번호 또는 이름/주소 등)가 제공됩니다.
2. 통신사업자(TSP) 관리자가 대상 가입자의 제어/데이터 이벤트 가로채기를 시작할 수 있도록 TSP 액세스 기능/전달 기능을 구성합니다. 가입자 세션이 이미 진행 중이면 인터셉션이 즉시 발생합니다. 그렇지 않으면 액세스 함수는 가입자 세션이 연결될 때까지 기다려야 합니다.
3. 액세스 기능은 가로챈 세션에 대한 제어/데이터 이벤트의 복사본을 전달 기능으로 보냅니다.
4. 전달 기능은 가로챈 정보를 LEA의 관리 영역에 있는 하나 이상의 수집 기능으로 전송합니다. 수집 기능은 가로챈 정보를 분석하고 저장합니다.
5. LEA가 가로채기 중지를 요청할 때, TSP 관리자는 특정 가입자 세션에 대한 가로채기를 중지하도록

록 액세스 기능 및 전달 기능을 구성한다.

SSH 세션을 통한 CLI(Command Line Interface)는 대상 ID의 NI 프로비저닝 및 디프로비저닝과 NI 통계 모니터링에 DF에서 사용됩니다.

NI 이벤트와 콘텐츠를 DF에 전달하기 위해 StarOS에서 이러한 프로토콜/모드(IPv4 및 IPv6)가 지원됩니다.

- UDP(Un-ack) 모드: DF2 및 DF3의 주소는 UDP 미승인 모드에 대한 프로비저닝 시 제공됩니다.
- TCP 모드: TCP 모드의 경우 컨피그레이션은 피어 주소만 제공합니다. 모든 가로채기된 이벤트 전달(IRI)은 DF2로 전송되고 모든 가로채기된 데이터(CC) 전달은 DF3로 전송됩니다.

## 문제 해결

StarOS 컨피그레이션에는 이 기능에 적합한 라이선스가 있어야 합니다.

```
[local]<hostname># show license information | grep -i lawful
Monday December 10 01:54:13 UTC 2018
Lawful Intercept [ ASR5K-XX-CSXZZLI ]
+ Enhanced Lawful Intercept [ ASR5K-XX-CS0ZZELI / ASR5K-00-CS00XZI ]
Persistent Lawful Intercept [ ASR5K-XX-CS1ZZPLI ]
Segregating Lawful Intercept Context based on Count [ ASR5K-XX-PWXZZICS ]
```

또한 StarOS에는 "분리된 li-configuration"이 있어야 합니다.

이 기능을 사용하면 "li-administrator"만 전용 li 컨텍스트에서 NI 인터페이스 통합 세부사항을 보고 편집할 수 있습니다.

NI 관리자 사용자는 컨피그레이션에서 li-administration에 매핑해야 합니다.

```
administrator liadmin encrypted password *** ftp li-administration
```

그러나 여전히 StarOS는 합법적 가로채기 컨피그레이션 모듈에서 "buffer" 옵션을 정의하는 것을 허용하지 않는 것으로 나타났습니다.

```
[local]<hostname># context li
[li]<hostname># config
[li]<hostname>(config-ctx)# lawful-intercept tcp event-delivery
dest-addr - Destination IP address where the intercepted information needs to be forwarded.
====> customer do see only this option
```

```
[li]<hostname>(config-ctx)# lawful-intercept tcp event-delivery buff
Unknown command - "buff", unrecognized keyword
```

버퍼 컨피그레이션에 대해 이와 같은 CLI를 완료하려면 "buffer" 키워드가 포함된 옵션을 보는 것이 좋습니다.

```
configure
context
lawful-intercept tcp event-delivery buffer max-limit <1000 ... 50000>
end
```

## 해결

모든 StarOS 사용자에게 대한 li-admin 권한을 얻으려면 관리자 권한이 있는 li 컨텍스트에서 해당 사용자를 정의해야 합니다. 이 "버퍼" 옵션을 활성화하려면 외부 서버(LEA)에서 로그인해야 하는 li-admin 사용자입니다. 로컬 컨텍스트 아래의 노드에 로그인을 시도하는 다른 관리자 사용자는 이 "버퍼" 옵션을 정의할 수 없습니다.

다음은 LI 모듈에서 StarOS의 "버퍼" 옵션을 가져오는 데 필요한 단계입니다.

1. 로컬 관리자 사용자로 노드에 로그인합니다.
  2. li 컨텍스트를 작성합니다(전용 li 컨텍스트가 없으므로).
  3. 로컬 컨텍스트에서 li-admin 권한이 있는 li 사용자를 생성합니다.
  4. li 컨텍스트에서 li-admin 권한이 있는 li 사용자를 생성합니다.
- <<로컬 컨텍스트에서 li-admin을 제거하여 전용 li를 추가했습니다. 이렇게 하면 로컬 컨텍스트에서 li 컨텍스트를 분리할 수 있습니다.>>
5. 로컬 컨텍스트에서 li-admin 권한이 있는 li 사용자를 제거합니다.
  6. li 구성을 분리할 수 있도록 전용 li 컨텍스트를 생성합니다.
  7. li 컨텍스트 아래에서 액세스 목록을 정의합니다.
  8. 노드에서 로그아웃합니다.
  9. li-admin 권한이 있는 "li" 사용자로 노드에 다시 로그인합니다.
  10. 필요한 버퍼 옵션을 구성합니다. 이 옵션을 사용하면 구성할 수 있습니다.

## 설정

```
[local]<hostname>(config)# context local
[local]<hostname>(config-ctx)# administrator li-admin password *** li-administration ftp
[local]<hostname>(config-ctx)# end
```

```
[local]<hostname>(config)# context li
[li]<hostname>(config-ctx)# administrator li-admin password *** ftp li-administration
```

<we removed li-admin from local context to add dedicated li which will help us to enable the segregate the li context from local context >

```
[local]<hostname>(config-ctx)# no administrator li-admin
[local]<hostname>(config-ctx)# exit
```

```
[local]<hostname>(config)# dedicated-li context li
Warning: Creating a dedicated LI context is a permanent configuration setting
Info: Context li is dedicated to Lawful-Intercept configuration
Info: Undefined ACLs will be set to deny-all within this context
[li]<hostname>(config-ctx)#
[li]<hostname>(config-ctx)# access-list undefined permit-all
[li]<hostname>(config-ctx)# end
```

예를 들어, li-admin 사용자를 사용하여 로그인한 다음 필요한 모든 옵션을 볼 수 있습니다.

```
<local-node><hostname>$ ssh li-admin@li@
```

```
li-admin@li@aa.bb.cc.dd's password:  
Last login: Wed Jan 23 17:32:31 -0500 2019 on pts/2 from 10.xx.yy.zz.  
Cisco Systems QvPC-SI  
Lawful Intercept Interface
```

```
No entry for terminal type "xterm-256color";  
using dumb terminal settings.
```

```
[li] # configure
```

```
Warning: One or more other administrators may be configuring this system
```

```
[li]
```

**buffer** - This is used to configure the LI buffering >>>>>> **We can see the buffer option now.**  
**dest-addr** - Destination IP address where the intercepted information needs to be forwarded.

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.