

# Catalyst 9000 DHCP 릴레이 에이전트의 느린 DHCP 또는 간헐적인 DHCP 문제 해결

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[문제](#)

[시나리오 1: ICMP 리디렉션](#)

[솔루션](#)

[시나리오 2: ICMP 연결 불가](#)

[솔루션](#)

[시나리오 3: ICMP TTL-Exceeded](#)

[솔루션](#)

[관련 정보](#)

## 소개

이 문서에서는 Catalyst 9000 Series 스위치에서 DHCP 릴레이 에이전트로 느린 DHCP(Dynamic Host Configuration Protocol) 주소 할당 또는 간헐적인 DHCP 주소 할당 오류를 해결하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- DHCP 및 DHCP 릴레이 에이전트
- Internet Control Message Protocol (ICMP)
- CoPP(컨트롤 플레인 정책)

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 9000 시리즈 스위치
- Cisco IOS XE® 버전 16.x 및 17.x

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.

## 관련 제품

이 문서는 다음과 같은 하드웨어 및 소프트웨어 버전에서도 사용할 수 있습니다.

- Cisco IOS XE® 16.x를 사용하는 Catalyst 3650/3850 Series 스위치

## 배경 정보

CoPP(Control Plane Policing) 기능은 불필요한 트래픽 및 DoS(Denial of Service) 공격으로부터 CPU를 보호하여 디바이스의 보안을 강화합니다. 또한 우선 순위가 낮은 다른 많은 트래픽으로 인해 발생하는 트래픽 중단으로부터 제어 트래픽과 관리 트래픽을 보호할 수 있습니다.

디바이스는 일반적으로 각각 고유한 목적을 가진 세 가지 운영 평면으로 분할됩니다.

- 데이터 패킷을 전달할 데이터 플레인.
- 컨트롤 플레인으로, 데이터를 올바르게 라우팅합니다.
- 네트워크 요소를 관리하는 관리 플레인입니다.

CoPP를 사용하여 대부분의 CPU 바운드 트래픽을 보호하고 라우팅 안정성, 연결성 및 패킷 전달을 보장할 수 있습니다. 가장 중요한 것은 CoPP를 사용하여 DoS 공격으로부터 CPU를 보호할 수 있다는 것입니다.

CoPP는 이러한 목표를 달성하기 위해 모듈형 QoS MQC(명령줄 인터페이스) 및 CPU 큐를 사용합니다. 서로 다른 유형의 컨트롤 플레인 트래픽은 특정 기준에 따라 그룹화되어 CPU 대기열에 할당됩니다. 하드웨어에서 전용 폴리서의 컨피그레이션을 통해 이러한 CPU 대기열을 관리할 수 있습니다. 예를 들어 특정 CPU 대기열(트래픽 유형)에 대한 폴리서 비율을 수정하거나 특정 트래픽 유형에 대한 폴리서를 비활성화할 수 있습니다.

폴리서가 하드웨어에서 구성되더라도 CoPP는 CPU 성능이나 데이터 플레인의 성능에 영향을 미치지 않습니다. 그러나 CPU로 향하는 패킷의 수를 제한하므로 CPU 로드가 제어됩니다. 즉, 하드웨어에서 패킷을 기다리는 서비스에서 더 제어된 인그레스 패킷 비율(사용자 구성 가능)을 확인할 수 있습니다.

## 문제

Catalyst 9000 스위치는 라우티드 인터페이스 또는 SVI에서 **ip helper-address** 명령이 구성된 경우 DHCP 릴레이 에이전트로 구성됩니다. 헬퍼 주소가 구성된 인터페이스는 일반적으로 다운스트림 클라이언트의 기본 게이트웨이입니다. 스위치에서 클라이언트에 성공적인 DHCP 릴레이 서비스를 제공하려면 인바운드 DHCP Discover 메시지를 처리할 수 있어야 합니다. 이를 위해서는 스위치가 DHCP Discover를 수신하고 처리할 CPU에 이 패킷을 보내야 합니다. DHCP Discover가 수신 및 처리되면 릴레이 에이전트는 DHCP Discover가 수신된 인터페이스에서 소싱되고 IP **헬퍼 주소 컨피그레이션**에 정의된 대로 IP 주소로 향하는 새 유니캐스트 패킷을 생성합니다. 패킷이 생성된 후 하드웨어가 전달되며 DHCP 서버로 전송되어 처리되고 마지막으로 릴레이 에이전트로 다시 전송되므로 클라이언트에 대해 DHCP 프로세스가 계속될 수 있습니다.

일반적인 문제는 릴레이 에이전트의 DHCP 트랜잭션 패킷이 ICMP 리디렉션 또는 ICMP 대상 도달 불가 메시지와 같은 특정 ICMP 시나리오의 영향을 받기 때문에 CPU로 전송되는 트래픽에 의해 도치 않게 영향을 받는 경우입니다. 이 동작은 클라이언트가 DHCP에서 IP 주소를 적시에 가져올 수 없거나 총 DHCP 할당 실패로 나타날 수 있습니다. 일부 시나리오에서는 하루 중 특정 시간에만 이러한 동작이 관찰될 수 있습니다(예: 네트워크에 대한 로드가 완전히 최대화된 피크 업무 시간).

Background(백그라운드) 섹션에서 설명한 것처럼, Catalyst 9000 Series Switch는 디바이스에서 구성 및 활성화된 기본 CoPP 정책과 함께 제공됩니다. 이 CoPP 정책은 전면 패널 포트에서 수신된 트래픽의 경로에 위치하며 디바이스 CPU를 대상으로 하는 QoS(Quality of Service) 정책의 역할을 합니다. 이 속도는 정책에 구성된 트래픽 유형 및 사전 정의된 임계값을 기반으로 트래픽을 제한합니다. 기본적으로 분류되고 속도가 제한되는 트래픽의 예로는 라우팅 제어 패킷(일반적으로 DSCP CS6로 표시됨), 토폴로지 제어 패킷(STP BPDU), BFD(Low Latency Packets)가 있습니다. 이러한 패킷을 안정적으로 처리할 수 있으면 안정적인 네트워크 환경이 조성되므로 이러한 패킷의 우선 순위를 지정해야 합니다.

**show platform hardware fed switch active qos queue stats internal cpu policer 명령을 사용하여 CoPP policer 통계를 확인합니다.**

ICMP 리디렉션 대기열(대기열 6)과 BROADCAST 대기열(대기열 12)은 모두 동일한 PlcIdx 0(폴리서 인덱스)을 공유합니다. 즉, DHCP Discover와 같이 디바이스 CPU에서 처리해야 하는 모든 브로드캐스트 트래픽은 ICMP 리디렉션 대기열에서 디바이스 CPU로 목적지이기도 한 트래픽과 공유됩니다. 이는 ICMP 리디렉션 대기열 트래픽이 BROADCAST 대기열에서 처리해야 하는 트래픽을 제외하기 때문에 DHCP 트랜잭션이 실패하여 합법적인 브로드캐스트 패킷이 삭제되는 앞에서 언급한 문제를 야기할 수 있습니다.

```
9300-Switch#show platform hardware fed switch active qos queue stats internal cpu policer

CPU Queue Statistics
=====
(default) (set) Queue Queue
QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
-----
0 11 DOT1X Auth Yes 1000 1000 0 0
1 1 L2 Control Yes 2000 2000 0 0
2 14 Forus traffic Yes 4000 4000 0 0
3 0 ICMP GEN Yes 600 600 0 0
4 2 Routing Control Yes 5400 5400 0 0
5 14 Forus Address resolution Yes 4000 4000 0 0
6 0 ICMP Redirect Yes 600 600 0 0 <-- Policer
Index 0
7 16 Inter FED Traffic Yes 2000 2000 0 0
8 4 L2 LVX Cont Pack Yes 1000 1000 0 0
9 19 EWLC Control Yes 13000 13000 0 0
10 16 EWLC Data Yes 2000 2000 0 0
11 13 L2 LVX Data Pack Yes 1000 1000 0 0
12 0 BROADCAST Yes 600 600 0 0 <-- Policer
Index 0
13 10 Openflow Yes 200 200 0 0
14 13 Sw forwarding Yes 1000 1000 0 0
15 8 Topology Control Yes 13000 16000 0 0
16 12 Proto Snooping Yes 2000 2000 0 0
17 6 DHCP Snooping Yes 500 500 0 0
18 13 Transit Traffic Yes 1000 1000 0 0
19 10 RPF Failed Yes 250 250 0 0
20 15 MCAST END STATION Yes 2000 2000 0 0
<snip>
```

CoPP 정책에서 기본 600 패킷/초 속도를 초과하는 트래픽은 CPU에 도달하기 전에 삭제됩니다.

```
9300-Switch#show platform hardware fed switch active qos queue stats internal cpu policer

CPU Queue Statistics
=====
(default) (set) Queue Queue
```

```

QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
-----
0 11 DOT1X Auth Yes 1000 1000 0 0
1 1 L2 Control Yes 2000 2000 0 0
2 14 Forus traffic Yes 4000 4000 0 0
3 0 ICMP GEN Yes 600 600 0 0
4 2 Routing Control Yes 5400 5400 0 0
5 14 Forus Address resolution Yes 4000 4000 0 0
6 0 ICMP Redirect Yes 600 600 3063106173577 3925209161
<-- Dropped packets in queue
7 16 Inter FED Traffic Yes 2000 2000 0 0
8 4 L2 LVX Cont Pack Yes 1000 1000 0 0
9 19 EWLC Control Yes 13000 13000 0 0
10 16 EWLC Data Yes 2000 2000 0 0
11 13 L2 LVX Data Pack Yes 1000 1000 0 0
12 0 BROADCAST Yes 600 600 1082560387 3133323
<-- Dropped packets in queue
13 10 Openflow Yes 200 200 0 0
14 13 Sw forwarding Yes 1000 1000 0 0
15 8 Topology Control Yes 13000 16000 0 0
16 12 Proto Snooping Yes 2000 2000 0 0
17 6 DHCP Snooping Yes 500 500 0 0
18 13 Transit Traffic Yes 1000 1000 0 0
19 10 RPF Failed Yes 250 250 0 0
20 15 MCAST END STATION Yes 2000 2000 0 0
<snip>

```

## 시나리오 1: ICMP 리디렉션

첫 번째 시나리오에서는 이 토폴로지를 고려하십시오.



이벤트의 순서는 다음과 같습니다.

1. 10.10.10.100의 사용자가 원격 네트워크인 디바이스 10.100.100에 대한 텔넷 연결을 시작합니다.
2. 대상 IP가 다른 서브넷에 있으므로 패킷이 사용자 기본 게이트웨이 10.10.10.15로 전송됩니다.
3. Catalyst 9300이 이 패킷을 받아 라우팅하면 해당 패킷을 CPU에 전달하여 ICMP 리디렉션을 생성합니다.

ICMP 리디렉션은 9300 스위치의 관점에서 랩톱이 이 패킷을 10.10.10.1의 라우터에 직접 전송하는 것이 더 효율적이므로, Catalyst 9300의 다음 홉이며 사용자가 속한 VLAN과 동일한 VLAN에 있기 때문에 생성됩니다.

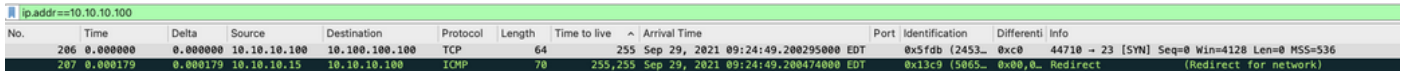
문제는 전체 흐름이 ICMP 리디렉션 기준을 충족하므로 CPU에서 처리된다는 것입니다. 다른 디바이스가 ICMP 리디렉션 시나리오를 충족하는 전송 트래픽인 경우, 동일한 CoPP 폴리서를 공유하므로 BROADCAST 대기열에 영향을 줄 수 있는 이 대기열의 CPU에 더 많은 트래픽이 전달되기 시작합니다.

ICMP 리디렉션 syslog를 보려면 ICMP를 디버깅합니다.

```
9300-Switch#debug ip icmp      <-- enables ICMP debugs
ICMP packet debugging is on
9300-Switch#show logging | inc ICMP
*Sep 29 12:41:33.217: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE,
dscp 0 topoid 0
*Sep 29 12:41:33.218: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE,
dscp 0 topoid 0
*Sep 29 12:41:33.219: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE,
dscp 0 topoid 0
*Sep 29 12:41:33.219: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE,
dscp 0 topoid 0
*Sep 29 12:43:08.127: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:09.517: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:10.017: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1      <-- ICMP Redirect to use 10.10.10.1 as Gateway
*Sep 29 12:50:14.293: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:19.053: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:23.797: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:28.537: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:33.284: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
```

**주의:** 규모에 따라 복잡성이 심하므로 ICMP 디버깅을 활성화하기 전에 콘솔 로깅 및 터미널 모니터링을 비활성화하는 것이 좋습니다.

Catalyst 9300 CPU의 임베디드 패킷 캡처는 CPU의 텔넷 연결에 대한 초기 TCP SYN 및 생성된 ICMP 리디렉션을 보여줍니다.



No.	Time	Delta	Source	Destination	Protocol	Length	Time to live	Arrival Time	Port	Identification	Differenti	Info
206	0.000000	0.000000	10.10.10.100	10.100.100.100	TCP	64	255	Sep 29, 2021 09:24:49.200295000 EDT		0x5fdb (2453)	0xc0	44718 - 23 [SYN] Seq=0 Win=4128 Len=0 MSS=536
207	0.000179	0.000179	10.10.10.15	10.10.10.100	ICMP	70	255,255	Sep 29, 2021 09:24:49.200474000 EDT		0x13c9 (3865)	0x00,0...	Redirect (Redirect for network)

ICMP 리디렉션 패킷은 클라이언트로 향하는 Catalyst 9300 VLAN 10 인터페이스에서 소싱되며 ICMP 리디렉션 패킷이 전송되는 원래 패킷 헤더를 포함합니다.

```

▼ Internet Protocol Version 4, Src: 10.10.10.15, Dst: 10.10.10.100
  0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x13c9 (5065)
  ▶ Flags: 0x0000
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x7f75 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.10.15
    Destination: 10.10.10.100
▼ Internet Control Message Protocol
  Type: 5 (Redirect)
  Code: 0 (Redirect for network)
  Checksum: 0x2bec [correct]
  [Checksum Status: Good]
  Gateway address: 10.10.10.1
▼ Internet Protocol Version 4, Src: 10.10.10.100, Dst: 10.100.100.100
  0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 44
    Identification: 0x5fdb (24539)
  ▶ Flags: 0x0000
    Time to live: 255
    Protocol: TCP (6)
    Header checksum: 0xd7fa [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.10.100
    Destination: 10.100.100.100
  ▶ Transmission Control Protocol, Src Port: 44710, Dst Port: 23

```

## 솔루션

이 시나리오에서는 CPU까지 전달되는 패킷을 방지할 수 있습니다. 그러면 ICMP 리디렉션 패킷의 생성도 중지됩니다.

최신 운영 체제에서는 ICMP 리디렉션 메시지를 사용하지 않으므로 이러한 패킷을 생성하고 전송하고 처리하는 데 필요한 리소스가 네트워크 디바이스에서 CPU 리소스를 효율적으로 사용하지 못합니다.

또는 사용자가 10.10.10.1의 기본 게이트웨이를 사용하도록 지정할 수 있지만, 이러한 컨피그레이션은 이유가 있을 뿐 이 문서의 범위에 속하지 않습니다.

**no ip redirects** CLI를 사용하여 ICMP 리디렉션을 비활성화하기만 하면 됩니다.

```

9300-Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
9300-Switch(config)#interface vlan 10
9300-Switch(config-if)#no ip redirects      <-- disable IP redirects
9300-Switch(config-if)#end

```

인터페이스에서 ICMP 리디렉션이 비활성화되었는지 확인합니다.

```

9300-Switch#show ip interface vlan 10
Vlan10 is up, line protocol is up
Internet address is 10.10.10.15/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.102
Outgoing Common access list is not set
Outgoing access list is not set
Inbound Common access list is not set
Inbound access list is BLOCK-TELNET
Proxy ARP is disabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are never sent          <-- redirects disabled
ICMP unreachable are never sent
ICMP mask replies are never sent
IP fast switching is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF switching turbo vector
<snip>

```

ICMP 리디렉션 및 전송 시기에 대한 자세한 내용은

<https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13714-43.html> 링크를 참조하십시오.

## 시나리오 2: ICMP 연결 불가

10.10.10.100의 사용자가 10.100.100.100에 대한 텔넷 연결을 시작하는 것과 동일한 토폴로지를 고려하십시오. 이번에는 텔넷 연결을 차단하는 VLAN 10 SVI에서 인바운드로 액세스 목록이 구성되었습니다.



```

9300-Switch#show running-config interface vlan 10
Building Configuration..

Current Configuration : 491 bytes
!
interface Vlan10
ip address 10.10.10.15 255.255.255.0
no ip proxy-arp
ip access-group BLOCK-TELNET in          <-- inbound ACL
end
9300-Switch#
9300-Switch#show ip access-list BLOCK-TELNET
Extended IP access list BLOCK-TELNET
10 deny tcp any any eq telnet          <-- block telnet

```

```
20 permit ip any any
9300-Switch#
```

이벤트의 순서는 다음과 같습니다.

1. 10.10.10.100의 사용자가 디바이스 10.100.100.100에 대한 텔넷 연결을 시작합니다.
2. 대상 IP가 다른 서브넷에 있으므로 패킷이 사용자 기본 게이트웨이로 전송됩니다.
3. Catalyst 9300이 이 패킷을 수신하면 인바운드 ACL에 대해 평가되어 차단됩니다.
4. 패킷이 차단되고 IP 연결 불가능 패킷이 인터페이스에서 활성화되므로, 디바이스에서 ICMP 대상 연결 불가능 패킷을 생성할 수 있도록 패킷이 CPU에 펀팅됩니다.

ICMP destination unreachable syslog를 보려면 ICMP를 디버깅합니다.

```
9300-Switch#debug ip icmp          <-- enables ICMP debugs
ICMP packet debugging is on
9300-Switch#show logging | include ICMP
<snip>
*Sep 29 14:01:29.041: ICMP: dst (10.100.100.100) administratively prohibited unreachable sent to
10.10.10.100   <-- packet blocked and ICMP message sent to client
```

주의: 규모에 따라 복잡성이 심하므로 ICMP 디버깅을 활성화하기 전에 콘솔 로깅 및 터미널 모니터링을 비활성화하는 것이 좋습니다.

Catalyst 9300 CPU의 Embedded Packet Capture는 CPU의 텔넷 연결에 대한 초기 TCP SYN과 전송된 ICMP Destination Unreachable을 보여줍니다.

```
106 8:015085 8:015085 10.10.10.100 10.100.100.100 TCP 64 255 Sep 29, 2021 10:01:29.041195000 EDT 0x52ea (2122) 0xc8 28767 - 23 [SYN] Seq=0 Win=4128 Len=0 MSS=536
107 0x000123 0x000123 10.10.10.15 10.10.10.100 ICMP 78 255,255 Sep 29, 2021 10:01:29.043300000 EDT 0x1003 (0220) 0x00,0 Destination unreachable (Communication administratively filtered)
```

ICMP Destination Unreachable 패킷은 클라이언트로 향하는 Catalyst 9300 VLAN 10 인터페이스에서 소싱되며 ICMP 패킷이 전송되는 원래 패킷 헤더를 포함합니다.

```
▶ Internet Protocol Version 4, Src: 10.10.10.15, Dst: 10.10.10.100
▼ Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 13 (Communication administratively filtered)
  Checksum: 0xf3f6 [correct]
  [Checksum Status: Good]
  Unused: 00000000
▼ Internet Protocol Version 4, Src: 10.10.10.100, Dst: 10.100.100.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  Total Length: 44
  Identification: 0x52ea (21226)
  ▶ Flags: 0x0000
  Time to live: 255
  Protocol: TCP (6)
  Header checksum: 0xe4eb [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.10.10.100
  Destination: 10.100.100.100
▶ Transmission Control Protocol, Src Port: 28767, Dst Port: 23
```



## 솔루션

이 시나리오에서는 ICMP Destination Unreachable 메시지를 생성하기 위해 ACL에 의해 차단된 편트된 패킷의 동작을 비활성화합니다.

IP Unreachable 기능은 Catalyst 9000 Series 스위치의 라우티드 인터페이스에서 기본적으로 활성화되어 있습니다.

```
9300-Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
9300-Switch(config)#interface vlan 10
9300-Switch(config-if)#no ip unreachableables <-- disable IP unreachableables
인터페이스에 대해 비활성화되어 있는지 확인합니다.
```

```
9300-Switch#show ip interface vlan 10
Vlan10 is up, line protocol is up
Internet address is 10.10.10.15/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.102
Outgoing Common access list is not set
Outgoing access list is not set
Inbound Common access list is not set
Inbound access list is BLOCK-TELNET
Proxy ARP is disabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are never sent
ICMP unreachableables are never sent <-- IP unreachableables disabled
ICMP mask replies are never sent
IP fast switching is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF switching turbo vector
<snip>
```

### 시나리오 3: ICMP TTL-Exceeded

이전 2가지 시나리오에 사용된 이전 토폴로지를 고려하십시오. 이번에는 10.10.10.100의 사용자가 해제된 이후에 네트워크의 리소스에 도달하려고 시도합니다. 이로 인해 이 네트워크를 호스팅하던 SVI 및 VLAN이 Catalyst 9300에 더 이상 존재하지 않습니다. 그러나 라우터에는 이 네트워크의 다음 홉으로 Catalyst 9300 VLAN 10 인터페이스를 가리키는 고정 경로가 여전히 있습니다.

Catalyst 9300에는 더 이상 이 네트워크가 구성되지 않으므로 직접 연결된 것으로 표시되지 않으며, 9300은 특정 경로가 없는 모든 패킷을 10.10.10.1의 라우터를 가리키는 고정 기본 경로로 라우팅합니다.

이 동작은 사용자가 192.168.10.0/24 주소 공간의 리소스에 연결하려고 시도할 때 네트워크에 라우팅 루프를 도입합니다. 패킷은 TTL이 만료될 때까지 9300과 라우터 간에 루핑됩니다.



1. 사용자가 192.168.10/24 네트워크의 리소스에 연결하려고 합니다.
  2. 패킷은 Catalyst 9300에서 수신되며 다음 홉 10.10.10.1을 사용하여 기본 경로로 라우팅되고 TTL이 1만큼 감소합니다.
  3. 라우터가 이 패킷을 수신하고 라우팅 테이블을 검사하여 다음 홉이 10.10.10.15인 이 네트워크에 대한 경로가 있는지 확인합니다. TTL을 1로 줄이고 패킷을 9300으로 다시 라우팅합니다.
  4. Catalyst 9300은 패킷을 수신하여 다시 10.10.10.1로 라우팅하고 TTL을 1만큼 줄입니다.
- 이 프로세스는 IP TTL이 0에 도달할 때까지 반복됩니다.

Catalyst에서 IP TTL = 1의 패킷을 수신하면 CPU에 패킷을 보내고 ICMP TTL-Exceeded 메시지를 생성합니다.

ICMP 패킷 유형은 11이고 코드는 0입니다(전송 시 TTL이 만료됨). 이 패킷 유형은 CLI 명령을 통해 비활성화할 수 없습니다

DHCP 트래픽의 문제는 이 시나리오에서 나타납니다. 반복되는 패킷은 수신된 인터페이스와 동일한 인터페이스를 제외하므로 ICMP 리디렉션의 영향을 받지 않습니다.

사용자가 보낸 패킷도 ICMP 리디렉션의 대상이 됩니다. 이 시나리오에서 DHCP 트래픽은 BROADCAST 대기열에서 쉽게 제외될 수 있습니다. 이 시나리오는 리디렉션 대기열에서 펀트된 패킷의 수로 인해 규모에 따라 더욱 악화됩니다.

여기서 CoPP 삭제는 1000 ping을 통해 192.168.10.0/24 네트워크에 대해 각 ping 간에 0초의 시간 초과로 데모됩니다. 9300의 CoPP 통계는 지워지며 PING이 전송되기 전에 0바이트에서 삭제됩니다.

```
9300-Switch#clear platform hardware fed switch active qos statistics internal cpu policer
<-- clear CoPP stats
```

```
9300-Switch#show platform hardware fed switch active qos queue stats internal cpu policer | i
Redirect|Drop <-- verify 0 drops
QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
6 0 ICMP Redirect Yes 600 600 0 0 <-- bytes dropped 0
<snip>
```

사용자가 원격 네트워크로 트래픽을 전송합니다.

```
User#ping 192.168.10.10 timeout 0 rep 1000 <-- User sends 1000 pings
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 192.168.10.10, timeout is 0 seconds:
.....
.....
.....
```



덱스를 사용하며 DHCP 트래픽에 영향을 주지 않도록 BROADCAST와 큐를 공유하지 않습니다.

IP 리디렉션 CLI 없이 ICMP 리디렉션을 비활성화하기만 하면 됩니다.

```
9300-Switch#configure terminal
```

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

```
9300-Switch(config)#interface vlan 10
```

```
9300-Switch(config-if)#no ip redirects          <-- disable IP redirects
```

```
9300-Switch(config-if)#end
```

## 관련 정보

- [내장형 패킷 캡처 구성](#)
- [ICMP 리디렉션 이해](#)
- [기술 지원 및 문서 - Cisco Systems](#)

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.