Catalyst 9000 DHCPリレーエージェントでのDHCPの低速または断続的な問題のトラブルシューティング

内容

概要

このドキュメントでは、DHCPリレーエージェントとしてのCatalyst 9000シリーズスイッチでのDynamic Host Configuration Protocol(DHCP)アドレス割り当ての速度低下やDHCPアドレス割り当ての断続的な失敗のトラブルシューティング方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- DHCPおよびDHCPリレーエージェント
- Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）
- コントロール プレーン ポリシング（CoPP）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Catalyst 9000 シリーズ スイッチ
- Cisco IOS XE®バージョン16.xおよび17.x

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- Cisco IOS XE® 16.xを搭載したCatalyst 3650/3850シリーズスイッチ

背景説明

コントロールプレーンポリシング(CoPP)機能は、不要なトラフィックやサービス拒否(DoS)攻撃からCPUを保護することで、デバイスのセキュリティを向上させます。また、大量の他の低優先度トラフィックによって引き起こされるトラフィックドロップから制御トラフィックと管理トラフィックを保護することもできます。

通常、デバイスは3つの操作面にセグメント化され、それぞれが独自の目的を持ちます。

- データパケットを転送するためのデータプレーン。
- コントロールプレーンを使用して、データを正しくルーティングします。
- ネットワーク要素を管理するための管理プレーン。

CoPPを使用すると、CPUに送られるトラフィックのほとんどを保護し、ルーティングの安定性、到達可能性、およびパケット配信を確保できます。最も重要なことは、CoPPを使用してCPUをDoS攻撃から保護できることです。

CoPPは、モジュラQoSコマンドラインインターフェイス(MQC)とCPUキューを使用して、これらの目的を達成します。さまざまなタイプのコントロールプレーントラフィックが特定の基準に基づいてグループ化され、CPUキューに割り当てられます。これらのCPUキューは、ハードウェア内の専用ポリサーを設定することによって管理できます。たとえば、特定のCPUキュー（トラフィックタイプ）のポリサーレートを変更したり、特定のタイプのトラフィックのポリサーを無効にすることができます。

ポリサーはハードウェアで設定されますが、CoPPはCPUパフォーマンスやデータプレーンのパフォーマンスには影響しません。ただし、CPUに向かうパケットの数が制限されるため、CPUの負荷は制御されます。つまり、ハードウェアからのパケットを待つサービスは、より制御された入力パケットのレートを参照できます（レートはユーザが設定できます）。

問題

Catalyst 9000スイッチは、ルーテッドインターフェイスまたはSVIで**ip helper-address**コマンドが設定されている場合、DHCPリレーエージェントとして設定されます。ヘルパーアドレスが設定されているインターフェイスは、通常、ダウンストリームクライアントのデフォルトゲートウェイです。スイッチがクライアントに正常なDHCPリレーサービスを提供するには、スイッチが着信DHCP Discoverメッセージを処理できる必要があります。これには、スイッチがDHCP Discoverを受信し、このパケットをCPUにパントして処理する必要があります。DHCP Discoverを受信して処理すると、リレーエージェントは、DHCP Discoverを受信したインターフェイスを送信元とし、**ip helper-address**設定で定義されたIPアドレスを宛先とする新しいユニキャストパケットを作成します。パケットが作成されると、パケットはハードウェアで転送され、DHCPサーバに送信されます。ここでパケットは処理され、最終的にリレーエージェントに返さ

れます。これにより、クライアントに対してDHCPプロセスを続行できます。

よくある問題は、リレーエージェントのDHCPトランザクションパケットが、ICMPリダイレクトやICMP宛先到達不能メッセージなどの特定のICMPシナリオの対象となるため、CPUに送信されるトラフィックの影響を受けないことです。この動作は、クライアントがDHCPからIPアドレスをタイムリーに取得できない、またはDHCP割り当ての失敗の合計として現れる可能性があります。ネットワークの負荷が完全に最大になるピーク業務時間など、特定の時間帯にのみ動作が観察されるシナリオもあります。

「背景説明」の項で説明したように、Catalyst 9000シリーズスイッチには、デバイスで設定および有効化されたデフォルトCoPPポリシーが付属しています。このCoPPポリシーは、フロントパネルポートで受信され、デバイスのCPUを宛先とするトラフィックのパスに配置されるQuality of Service(QoS)ポリシーとして機能します。トラフィックタイプと、ポリシーで設定された定義済みのしきい値に基づいて、トラフィックをレート制限します。デフォルトで分類され、レートが制限されるトラフィックの例としては、ルーティング制御パケット（通常はDSCP CS6でマーキングされる）、トポロジ制御パケット(STP BPDU)、低遅延パケット(BFD)などがあります。これらのパケットを確実に処理する機能によって安定したネットワーク環境が実現するため、これらのパケットには優先順位を付ける必要があります。

show platform hardware fed switch active qos queue stats internal cpu policerコマンドを使用して、CoPPポリサーの統計情報を表示します。

ICMPリダイレクトキュー（キュー6）とBROADCASTキュー（キュー12）は、どちらも同じPlcIdx 0（ポリサーインデックス）を共有します。つまり、デバイスCPUで処理する必要があるブロードキャストトラフィック（DHCP Discoverなど）は、ICMPリダイレクトキュー内のデバイスCPUを宛先とするトラフィックと共有されます。これにより、前述した問題が発生する可能性があります。ICMPリダイレクトキュートラフィックがブロードキャストキューによる処理を必要とするトラフィックを使い果たし、正当なブロードキャストパケットが廃棄されるために、DHCPトランザクションが失敗します。

```
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>
```

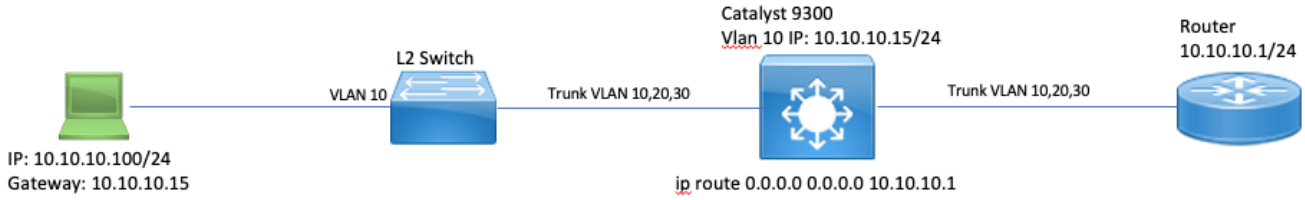
CoPPポリシーでデフォルトの600パケット/秒レートを超えるトラフィックは、CPUに到達する前にドロップされます。

```
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>
```

シナリオ1:ICMPリダイレクト

最初のシナリオでは、次のトポロジを検討します。



イベントのシーケンスは次のとおりです。

1. 10.10.10.100のユーザが、リモートネットワークであるデバイス10.100.100.100へのTelnet接続を開始します。

2.宛先IPは異なるサブネットにあるため、パケットはユーザのデフォルトゲートウェイ

10.10.10.15に送信されます。

3. Catalyst 9300は、このパケットを受信してルーティングを行うと、ICMPリダイレクトを生成するためにCPUにパケットをパントします。

ICMPリダイレクトが生成される理由は、9300スイッチから見ると、このパケットを10.10.10.1のルータに直接送信する方がノートPCにとって効率的であるためです。これは、いずれにせよこれはCatalyst 9300のネクストホップであり、ユーザが属するVLANと同じであるためです。

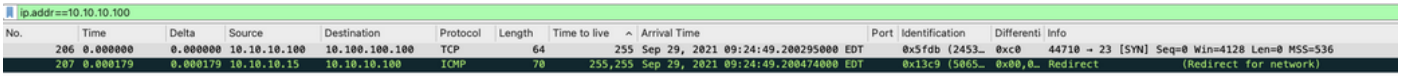
問題は、ICMPリダイレクト基準を満たしているため、フロー全体がCPUで処理されることです。ICMPリダイレクトシナリオを満たす送信トラフィックが他のデバイスにある場合は、さらに多くのトラフィックがこのキュー内のCPUにパントされ始めます。これらのデバイスは同じCoPPポリサーを共有しているため、ブロードキャストキューに影響を与える可能性があります。

ICMPリダイレクトsyslogを表示するには、ICMPをデバッグします。

```
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
```

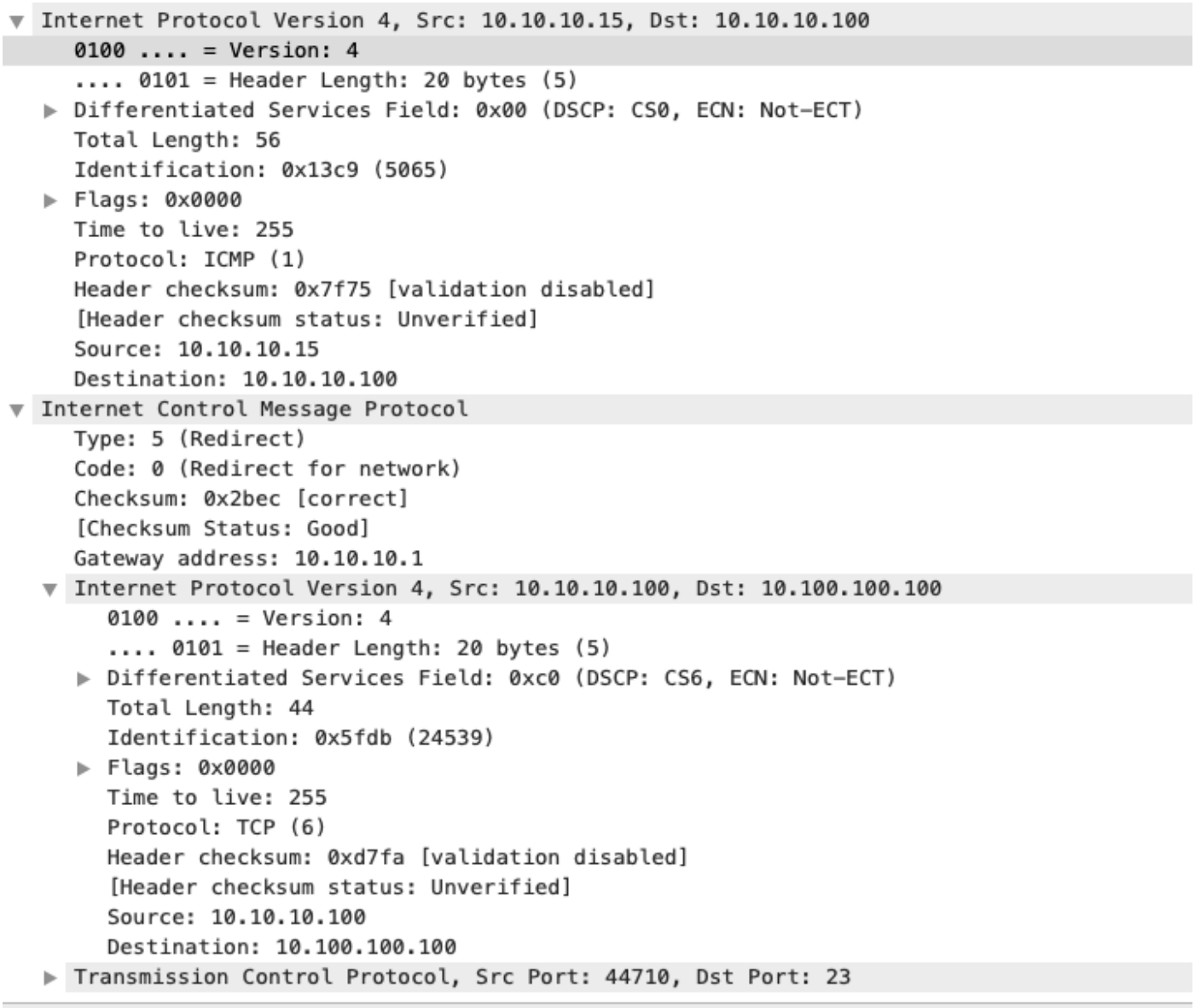
> **注意**：大規模な冗長性があるため、ICMPデバッグを有効にする前に、コンソールロギングと端末モニタリングを無効にすることをお勧めします。

Catalyst 9300 CPUでの組み込みパケットキャプチャ(EPC)は、CPUでのTelnet接続の初期TCP SYNと、生成されるICMPリダイレクトを示します。



ICMPリダイレクトパケットの送信元は、Catalyst 9300 VLAN 10インターフェイスのクライアントを宛先とし、ICMPリダイレクトパケットの送信先となる元のパケットヘッダーが含まれていま

す。



解決方法

このシナリオでは、CPUにパントされるパケットを防止できるため、ICMPリダイレクトパケットの生成も停止します。

最近のオペレーティングシステムではICMPリダイレクトメッセージの使用が採用されていないため、これらのパケットの生成と送信および処理に必要なリソースは、ネットワークデバイス上のCPUリソースの効率的な使用にはなりません。

または、デフォルトゲートウェイ10.10.10.1を使用するようにユーザに指示します。ただし、このような設定は理由により適切であり、このドキュメントの範囲外です。

no ip redirects CLIを使用してICMPリダイレクトを無効にするだけです。

```
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
```

ICMPリダイレクトがインターフェイスで無効になっていることを確認します。

```
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 unreachables 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リダイレクトおよびICMPリダイレクトがいつ送信されるかについては、次のリンクを参照してください。https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13714-43.html

シナリオ2:ICMP到達不能

10.10.10.100のユーザが10.100.100.100へのTelnet接続を開始する同じトポロジについて考えます。今回は、Telnet接続をブロックするVLAN 10 SVIのインバウンドにアクセスリストが設定されました。


```
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#
```

イベントのシーケンスは次のとおりです。

1. 10.10.10.100のユーザがデバイス10.100.100.100へのTelnet接続を開始します。

2.宛先IPは異なるサブネットにあるため、パケットはユーザのデフォルトゲートウェイに送信されます。

3. Catalyst 9300がこのパケットを受信すると、着信ACLに対して評価され、ブロックされます。

4.パケットがブロックされ、IP到達不能がインターフェイスで有効になるため、パケットはCPUにパントされ、デバイスはICMP宛先到達不能パケットを生成できます。

ICMP宛先到達不能syslogを表示するには、ICMPをデバッグします。

```
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
```

> **注意**：大規模な冗長性があるため、ICMPデバッグを有効にする前に、コンソールロギングと端末モニタリングを無効にすることをお勧めします。

Catalyst 9300 CPUでの組み込みパケットキャプチャ(EPC)は、CPUでのTelnet接続の初期TCP SYNと、送信されるICMP宛先到達不能を示します。

ICMP Destination Unreachableパケットの送信元は、クライアントを宛先とするCatalyst 9300 VLAN 10インターフェイスで、ICMPパケットの送信先となる元のパケットヘッダーが含まれています。

```
▶ 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
```

解決方法

このシナリオでは、ICMP Destination Unreachableメッセージを生成するために、ACLによってブロックされるパントされたパケットの動作を無効にします。

IP到達不能機能は、Catalyst 9000シリーズスイッチのルーテッドインターフェイスではデフォルトで有効になっています。

```
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 unreachables      <-- disable IP unreachables
```

インターフェイスで無効になっていることを確認します。

```
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 unreachables are never sent      <-- IP unreachables 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>
```

シナリオ3:ICMP TTL超過

前の2つのシナリオで使用した以前のトポロジを検討します。今度は、10.10.10.100のユーザが、その後に使用停止になったネットワーク内のリソースに到達しようとします。このため、このネットワークをホストするために使用されたSVIおよびVLANは、Catalyst 9300上に存在しなくなります。ただし、ルータには、このネットワークのネクストホップとしてCatalyst 9300 VLAN 10インターフェイスを指し示すスタティックルートがあります。

Catalyst 9300ではこのネットワークが設定されていないため、直接接続されていると表示されず、9300は10.10.10.1のルータを指すスタティックデフォルトルートに、特定のルートを持たないパケットをルーティングします。

この動作により、ユーザが192.168.10.0/24アドレス空間のリソースに接続しようとすると、ネットワークにルーティングループが発生します。パケットは、TTLの期限が切れるまで、9300とルータの間でループされます。

1. ユーザが192.168.10/24ネットワーク内のリソースに接続を試みる

2. Catalyst 9300でパケットが受信され、ネクストホップが10.10.10.1のデフォルトルートにルーティングされ、TTLが1ずつ減らされます。

3.ルータはこのパケットを受信し、ルーティングテーブルをチェックして、ネクストホップが10.10.10.15であるこのネットワークへのルートを見つけます。TTLを1減らし、パケットを9300に戻します。

4. Catalyst 9300はパケットを受信し、10.10.10.1に再ルーティングし、TTLを1ずつ減らします。

このプロセスは、IP TTLがゼロに達するまで繰り返されます。

Catalystは、IP TTL = 1のパケットを受信すると、そのパケットをCPUにパントし、ICMP TTL-Exceededメッセージを生成します。

ICMPパケットタイプは11で、コードは0（転送中にTTLが期限切れ）です。このパケットタイプは、CLIコマンドでは無効にできません

このシナリオでは、DHCPトラフィックに関する問題が発生します。これは、ループしているパケットは、受信されたインターフェイスと同じインターフェイスを送出されないため、ICMPリダイレクションの影響を受けるためです。

ユーザから送信されるパケットもICMPリダイレクションの対象になります。このシナリオでは、

DHCPトラフィックはBROADCASTキューから簡単に枯渇する可能性があります。このシナリオは、リダイレクトキューにパントされたパケットの数が多いため、規模の点ではさらに悪くなります。

ここでは、192.168.10.0/24ネットワークに対する1000回のpingを実行し、各ping間のタイムアウトを0秒としてCoPPドロップを示します。9300のCoPP統計情報はクリアされ、pingが送信される前に0バイトで廃棄されます。

```
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>
```

ユーザはリモートネットワークにトラフィックを送信します。

```
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:
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................
Success rate is 0 percent (0/1000)
```

ICMPデバッグには、ルーティングループが原因のリダイレクトおよびTTL超過syslogが表示されます。

```
9300-Switch#debug ip icmp
ICMP packet deubgging is on
*Sep 29 16:33:22.676: ICMP: redirect sent to 10.10.10.100 for dest 192.168.10.10, use gw
10.10.10.1    <-- redirect sent
*Sep 29 16:33:22.678: ICMP: time exceeded (time to live) sent to 10.10.10.100 (dest was
192.168.10.10), topology BASE, dscp 0 topoid 0    <-- TTL exceeded observed
*Sep 29 16:33:22.678: ICMP: time exceeded (time to live) sent to 10.10.10.100 (dest was
192.168.10.10), topology BASE, dscp 0 topoid 0
*Sep 29 16:33:22.678: ICMP: time exceeded (time to live) sent to 10.10.10.100 (dest was
192.168.10.10), topology BASE, dscp 0 topoid 0
<snip>
```

> **注意**：大規模な冗長性があるため、ICMPデバッグを有効にする前に、コンソールロギングと端末モニタリングを無効にすることをお勧めします。

CoPPドロップは、リダイレクションのためにCPUにパントされたトラフィックの量が原因で発

生します。これは単一のクライアントに対してだけであることに注意してください。

```
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      15407990     126295    <--
drops in redirect queue
7 16 Inter FED Traffic Yes 2000 2000 0 0
8 4 L2 LVX Cont Pack Yes 1000 1000 0 0
<snip>
```

解決方法

このシナリオの解決策は、シナリオ1と同様に、ICMPリダイレクトを無効にすることです。ルーティングループも問題ですが、パケットがリダイレクション用にパントされるため、強度が悪化します。

ICMPのTTL超過パケットは、TTLが1の場合にもパントされますが、これらのパケットは異なるCoPPポリサーインデックスを使用し、BROADCASTとキューを共有しないため、DHCPトラフィックには影響しません。

no ip redirects CLIを使用してICMPリダイレクトを無効にするだけです。

```
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
```

関連情報

- 組み込みパケットキャプチャの設定
- ICMPリダイレクトについて
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。