# 了解ICMP重定向消息

## Contents



## Introduction

本文讨论数据包互联网控制消息协议(ICMP)提供的重定向功能。本文解释ICMP在网络的重定向消息什么出现通常指示，并且什么可以执行最小化负副作用关联以导致ICMP重定向消息的生成的网络状况。

## Prerequisites

### Requirements

Cisco 建议您了解以下主题：

- 连结7000平台体系结构
- NX-OS软件配置
- 互联网控制消息协议如提供在请求注释(RFC) 792上

### Components Used

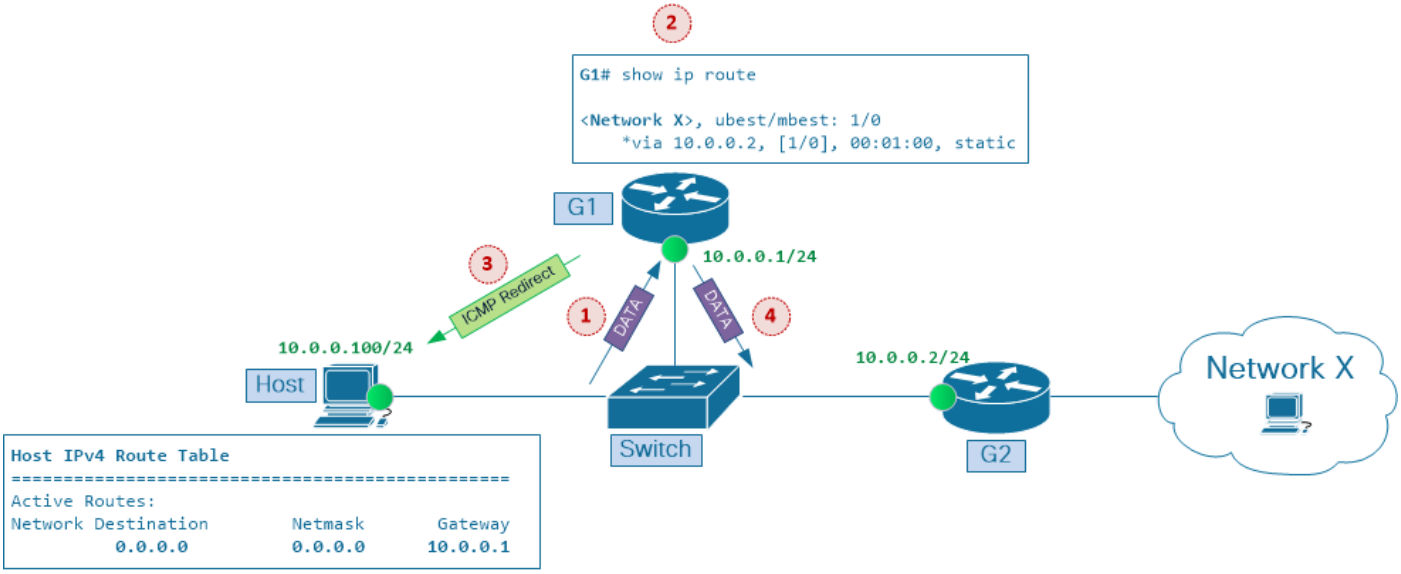
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

## ICMP重定向消息

ICMP重定向功能在RFC 792解释"互联网控制消息协议"与以下示例

> *网关传送重定向信息到在以下情况的一台主机。*
>
> *网关， G1，接收从一台主机的一互联网数据包在网关附加的网络。网关， G1，检查其路由表并且得到下个网关的地址， G2，在路由对数据包的互联网目的地网络， X。*
>
> *如果G2和数据包的互联网源地址识别的主机在同一网络，重定向信息传送到主机。因为这是一个更短的路径对目的地，重定向消息建议主机发送其网络的x流量直接地到网关G2。*
>
> *网关转递原始数据包的数据对其互联网目的地。*

此方案在*图片1.*主机和两路由器显示， G1和G2，连接对共享以太网分段并且有IP地址在同一网络10.0.0.0/24




Picture 1. ICMP Redirects in multi-point Ethernet networks

主机有IP地址10.0.0.100。主机的路由表有指向路由器G1的一个默认路由条目IP地址10.0.0.1作为默认网关。当转发流量对目的地网络X.时，路由器G1使用路由器G2 IP地址10.0.0.2作为其下一跳。

当主机发送数据包对目的地网络x时，下列发生

1. 网关G1用从主机10.0.0.100的IP地址10.0.0.1接收数据包在附加的网络。

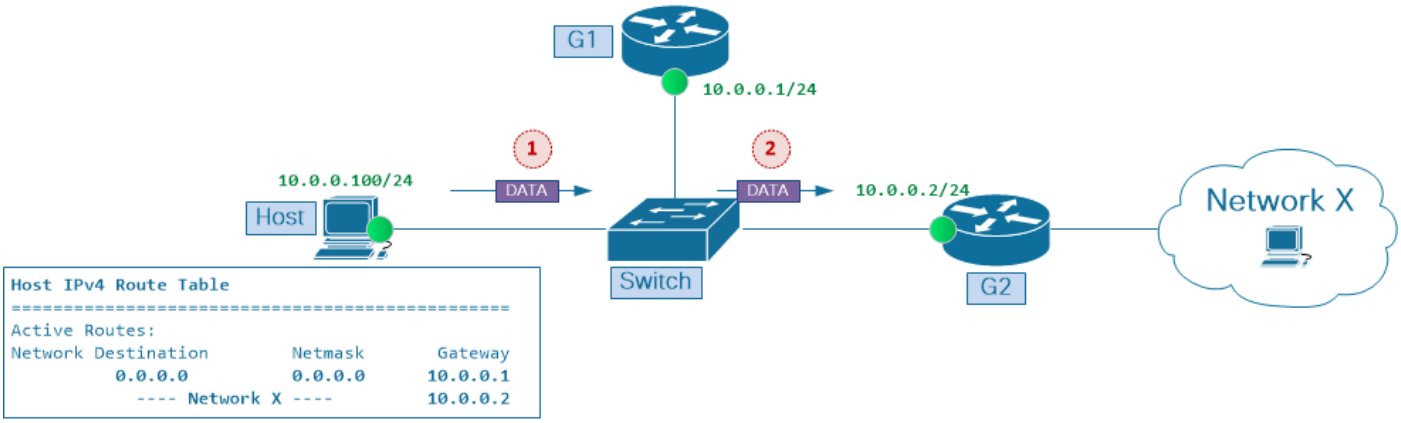
2. 网关， G1，检查其路由表并且得到IP地址10.0.0.2下个网关， G2，在路由对数据包的目的地网络， X。

3. 如果G2和IP数据包源地址识别的主机在同一网络， ICMP重定向信息传送到主机。 因为这是一个更短的路径对目的地， ICMP重定向消息建议主机发送其网络的x流量直接地到网关G2。

4. 网关G1转发原始信息包对其目的地。

根据主机配置，它可以选择忽略ICMP G1传送对它的重定向信息。然而，如果主机使用ICMP重定向消息调节其路由缓存并且开始发送随后数据数据包直接地对G2，以下好处在此方案达到

- 数据转发路径的最优化穿过网络;流量到达更加快速其的目的地
- 网络资源利用率的减少，例如带宽和路由器CPU负载




Picture 2. Next Hop G2 installed in Host routing cache

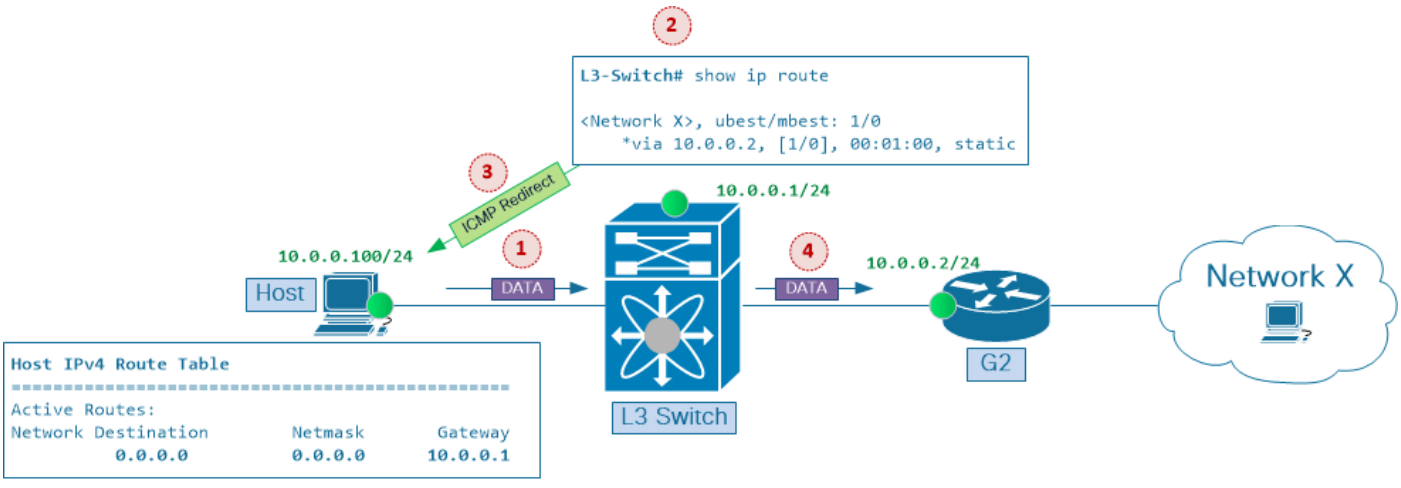
如在主机创建的路由缓存条目以后的*图片2所显示*，与G2的网络的x作为其下一跳，这些好处在网络被看到：

- 在链路的带宽利用率交换机和路由器G1之间在两个方向减小
- 因为通信流从主机到网络x不再，横断此节点在路由器G1的CPU利用率减少
- 主机和网络x之间的端到端网络延迟改善。

要了解ICMP重定向机制的重要性，请记住早期的Internet路由器设备依靠主要CPU资源处理数据流。因此，减少必须通过所有单个路由器和最小化路由器跳数量处理特定的流量运输流量在其途中必须横断到目的地的流量是非常理想。同时， Layer2转发(亦称*交换*)在定制的专用集成电路(ASIC)在通用处理器主要实现和从转发性能方面相对是'便宜的'与第3层转发比较(也呼叫*路由*)，那，再做。

更新的ASIC生成能执行Layer2和第3层信息包转发。有在硬件帮助执行的第3层表查找请降低性能开销关联与数据包处理由路由器。此外，集成第3层转发功能到里当前呼叫*第三层交换机*)的第二层交换机(做信息包转发操作更有效的，排除对"独臂路由器" (亦称"单臂路由器")设计选项的需要和避免限制关联与这样网络配置。

在方案的*图片3*修造在*图片1*。 现在Layer2和第3层功能，最初提供由两不同节点，交换机和路由器G1，在一单层3统一交换，例如连结7000系列平台。




Picture 3. Layer3 Switch replaces "one-armed router" configuration

当主机发送数据包对目的地网络x时，下列在网络发生

1. 网关L3交换机用从一台主机10.0.0.100的IP地址10.0.0.1接收数据包在附加的网络。

2. 网关， L3交换机，检查其路由表并且得到下个网关的地址10.0.0.2， G2，在路由对数据包的目的地网络， X。

3. 如果G2和IP数据包源地址识别的主机在同一网络， ICMP重定向信息传送到主机。 因为这是一个更短的路径对目的地， ICMP重定向消息建议主机发送其网络的x流量直接地到网关G2。

4. 网关转发原始信息包对其目的地。

使用当前的第三层交换机能执行Layer2和第3层信息包转发在ASIC级别，可以推断ICMP的两个好处通过网络重定向功能， (a)延迟的网络资源利用率的改进和(b)减少，达到，并且那儿不无需要有对路径优化技术的注意在多点以太网段。

然而，当ICMP重定向功能启用在第3层通过多点以太网段建立接口，不理想的转发继续提交潜在的性能瓶颈，即使为一个不同的原因，和在*连结平台Considerations部分*解释后在本文。

**Note**: 默认情况下ICMP重定向在第3层接口在IOS和NX-OS软件方面启用

**Note**:情况摘要，当ICMP重定向消息生成：第3层交换机生成ICMP重定向消息回到数据源数据包，如果数据包将转发此数据包接收的第3层接口。

# 次优路径到以太网

内部网关协议(IGP)，例如开放最短路径(OSFP)和首先思科增强的内部网关路由选择协议(EIGRP)，是在路由器之间的设计的同步路由信息和提供一致和可预测的信息包转发行为在尊敬这样信息的所有网络节点。采取多点以太网为例，如果在分段的所有第3层节点使用同一路由信息并且对对目的地的同一出口点达成协议，在间这样网络的不理想的转发很少是实际情形。

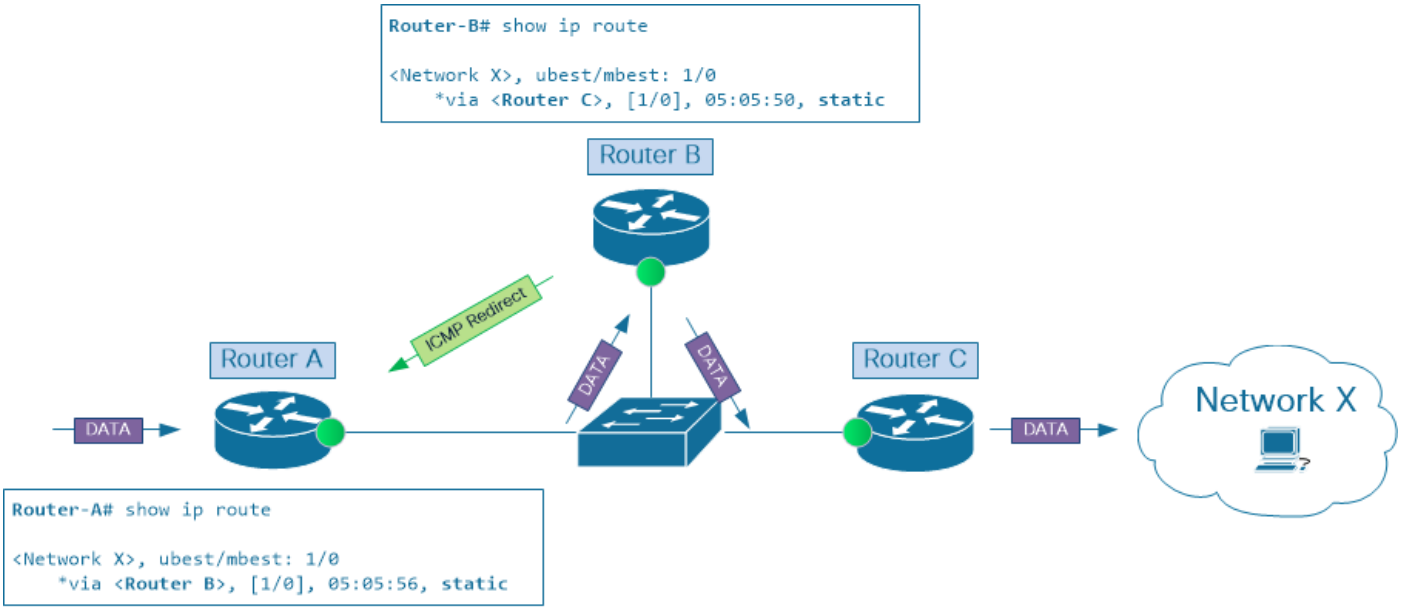
要了解什么导致不理想的转发路径，请记住第3层节点做出信息包转发决定对立于彼此。即路由器做的信息包转发决定B不取决于由路由器A做的信息包转发决定。这是记住的其中一个关键原理，当排除故障信息包转发通过IP网络时，并且是要记住的一重要一个，当调查多点以太网的时不理想的转发路径。

如前面提到，在所有路由器在单个动态路由协议取决于提供端点之间的流量的网络，不理想的转发通过多点以太网段不应该发生。然而，在实际全球网络它是非常普通查找多种信息包路由和转发机制的组合。 示例的这样机制是多种IGP、静态路由和策略基于路由。这些功能典型地并用通过网络达到所需流量转发。

当复合使用这些机制可帮助优化通信流和符合特定网络设计的要求时，这些工具能的多点以太网一起引起的俯视的副作用可能导致恶劣的总体网络性能。

## 静态路由

要说明此，请考虑在*图片4.*路由器A的方案有静态路由对网络x用路由器B作为其下一跳。同时路由器B使用路由器C作为其next-hop in静态路由对网络X。




Picture 4. Sub-optimal path with static routing

当流量进入此网络在路由器A时，通过路由器C留下它和最终被传送到目的地网络x，数据包必须两次交叉此IP网络在他们的途中到目的地。这不是effiencient使用网络资源。反而，发送从路由器A的数据包直接地对路由器C将取得同样结果，当浪费较少网络资源时。

> **Note**: 即使在此方案路由器A和路由器C使用作为入口和出口第3层节点此IP网络分段，两节点可以用网络设施替换(例如负载平衡器或防火墙)，如果后者有导致同一种信息包转发行为的路由配置。

### 基于策略的路由

基于策略的路由(PBR)是能导致次优路径到以太网的另一机制。然而，不同于静态或动态路由，PBR不运行在路由表级别。 反而，它直接地在交换机硬件方面编程流量重定向访问控制表(ACL)。 结果，对于挑选通信流，在进入线路卡的信息包转发查找绕过通过静态或动态路由得到的路由信息。

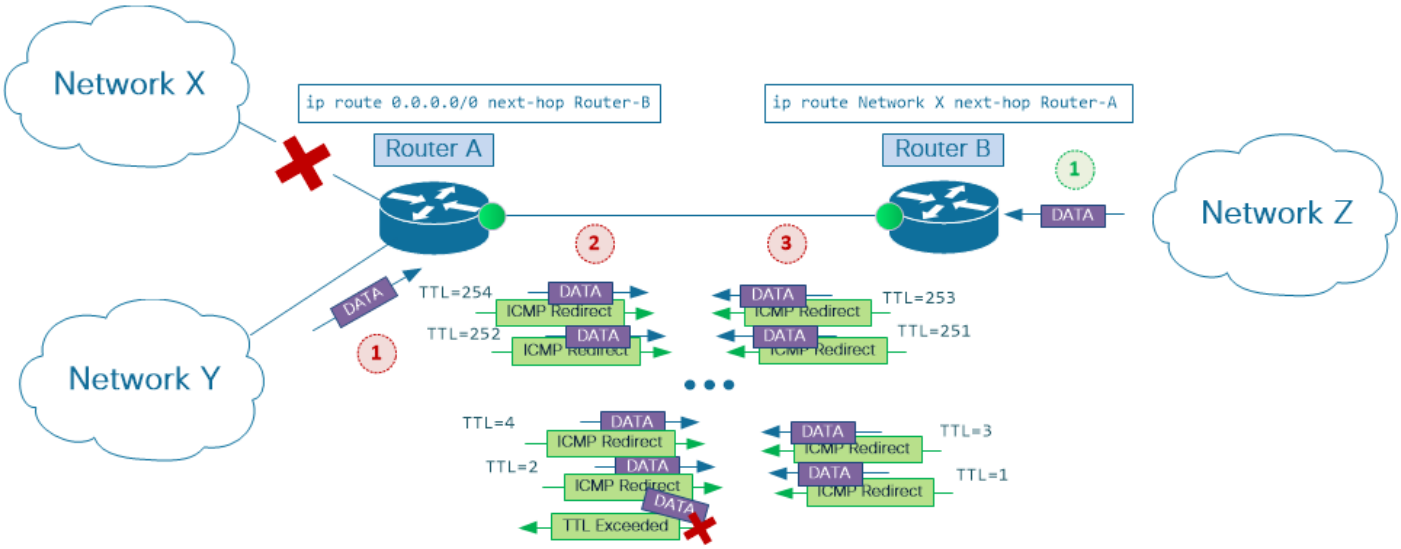
使用其中一个动态路由协议，在*图片5*，路由器A和B交换关于目的地网络x的路由信息。 两个对是的路由器B达成协议最好的下一跳此网络。

然而，与在改写从路由协议接收的路由信息并且设置路由器C作为下一跳为网络x的路由器B的PBR配置，条件触发ICMP重定向功能满足和数据包获得发送对路由器B CPU进一步处理的。

## 在点对点链路的ICMP重定向

到目前为止本文是指有附加的三的以太网(或更多)第3层节点，因此命名*多点*以太网。然而请注意ICMP重定向消息在点到点以太网链路可以生成。

而路由器B有静态路由对网络指向路由器A.的x考虑在*图片6.*路由器A用途静态默认路由的方案发送流量到路由器B。




Picture 6. ICMP Redirects on point-to-point links

当连接小用户环境对服务提供商网络时，此设计选项，亦称单址的连接，是一普遍的选择。在这里路由器B服务商边缘设备，并且路由器A是用户边缘(CE)设备。

注意典型的CE配置包括聚集静态路由到客户指向Null0接口的IP地址块。此配置是单址的CE-PE连接选项的一建议的最佳实践与静态路由。然而，为此示例假设这样配置不存在。

假设如图片所显示，路由器A丢失连接对网络x。当从客户网络Y或远程网络Z的数据包设法到达网络x，路由器A和B将重新启动流量在彼此之间，减少IP每数据包的Time-to-live字段，直到其值到达1，到时数据包的进一步路由不是可能的。

现在，而对网络x的流量反复重新启动在PE和CE路由器之间，大量地(和不必要地)增加CE-PE链路带宽利用率，问题变更坏，如果ICMP重定向在点到点PE-CE连接一个或两边启用。在这种情况下在流的每数据包被注定对网络x在对应的路由器多个时间CPU将处理帮助生成ICMP重定向消息。

# 连结平台考虑事项

当ICMP重定向在第3层接口时启用，并且流入的数据数据包使用此接口到入口和出口第3层交换机，ICMP重定向消息生成。 当第3层信息包转发在思科连结7000平台时的硬件方面完成，仍然是交换机的CPU的责任修建ICMP重定向消息。 要执行此，在连结7000 Supervisor模块的CPU需要得到路径穿过网段可以优化流的IP地址信息。这是原因在进入线路卡发送的数据包背后对Supervisor模块。

如果ICMP重定向消息的收件人忽略它并且继续数据流量对的连结交换机第3层接口ICMP重定向启用，ICMP重定向生成过程为每个数据包被触发。

以硬件转发例外的形式，在线路卡级别进程开始。当信息包转发操作不可能由线路卡模块时，顺利地完成例外在ASIC被上升。在这种情况下，数据包需要发送到正确数据包处理的Supervisor模块。

> **Note**:其他然后生成的ICMP重定向消息，在Supervisor模块的CPU处理许多其他信息包转发例外，例如处理IP信息包存活时间(TTL)值设置对1或者需要在发送被分段对下一跳前的IP信息包。

在Supervisor模块的CPU传送了ICMP重定向信息对来源后，由转发数据数据包完成异常处理对下一跳通过出口线路卡模块。

当连结7000个Supervisor模块使用能够处理大数据流的强大的CPU处理器时，平台设计处理大多数数据流在线路卡级，无需从事Supervisor的CPU处理器在信息包转发进程。这允许CPU着重其核心任务，留下信息包转发操作对在线路卡的专用硬件引擎。

在稳定网络中，信息包转发例外，应该他们发生，预计发生以一合理低速率。 使用此假定，他们可以由Supervisor CPU处理，不用在其性能的重大影响。另一方面，有CPU交易有发生以非常高速率的信息包转发例外能有对整个系统稳定性和responsivness的一个负面影响。

连结7000平台设计提供一定数量的机制保护从被淹没的交换机CPU由重大数额流量。这些机制实现在系统的不同的点。在线路卡级别，有硬件速率防幅器和控制平面策略(CoPP)功能。两集合流量速率阈值，将转发的有效控制的流量总量对从每个线路卡模块的Supervisor。

这些防护机制提供首选对为网络稳定性是关键并且交换可管理性，例如OSPF、BGP或者SSH，当积极地过滤流量类型时不对交换机的控制层面功能至关重要多种控制协议的流量。大多数数据流，如果转发对CPU由于信息包转发例外，由这样机制大量地管辖。

当硬件修正机制的速率防幅器和CoPP提供交换机的控制层面的稳定性和严格推荐总是启用时，他们可以是其中一个数据包丢包、传输延迟和整体恶劣的应用程序性能主要原因在间网络。这就是为什么了解通信流通过网络采取的路径和有工具对能并且/或者预计使用的监控网络设备ICMP重定向功能是重要。

# 监听和诊断工具

## show ip traffic

两Cisco IOS和NX-OS软件提供一个方式检查由CPU处理流量的统计信息。这实行同**show ip traffic命令**。此命令可以由第三层交换机或路由器用于检查ICMP重定向消息的收据和生成

```
Nexus7000# show ip traffic | begin ICMP

ICMP Software Processed Traffic Statistics
-----------------------------------------
Transmission:
 Redirect: 1000, unreachable: 0, echo request: 0, echo reply: 0,

<output omitted for brevity>

ICMP originate Req: 0, Redirects Originate Req: 1000
Originate deny - Resource fail: 0, short ip: 0, icmp: 0, others: 0
Reception:
Redirect: 0, unreachable: 0, echo request: 0, echo reply: 0,

<output omitted for brevity>

Nexus7000#
```

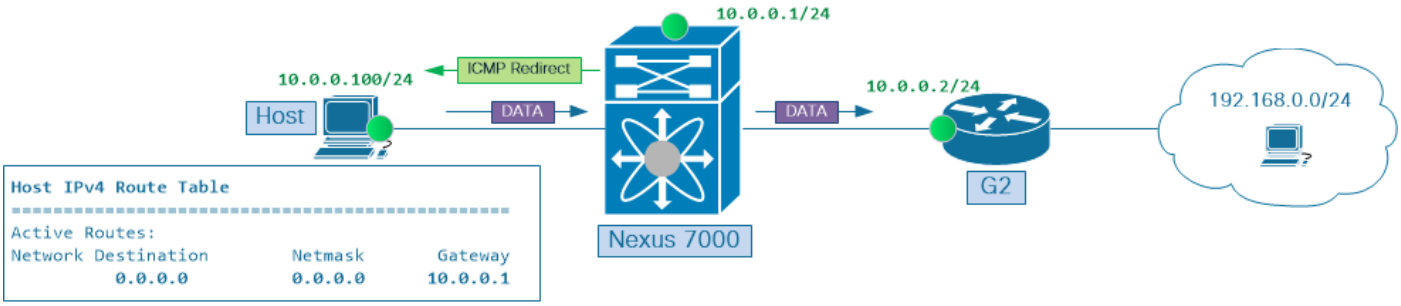
运行**show ip traffic命令**几次和检查ICMP重定向计数器是否增加。

## Ethanalyzer

Cisco NX-OS软件有捕获一个内置的工具到/从交换机的CPU的数据流，叫作Ethanalyzer。

**Note**: 关于Ethanalyzer的更多信息，参考在连结7000故障排除指南的Ethanalyzer

*图片7*显示方案类似于那个在*图片3*。此处网络x通过192.168.0.0/24网络替换。




Picture 7. Running Ethanalyzer capture

主机10.0.0.100发送ICMP echo请求连续流对目的IP地址192.168.0.1。主机用途Switch Virtual Interface (SVI)连结7000交换机10作为其对远程网络192.168.0.0/24的下一跳。演示目的，主机cofigured忽略ICMP重定向消息。

请使用以下命令捕获连结7000 CPU接收和发送的ICMP流量

```
Nexus7000# ethanalyzer local interface inband capture-filter icmp limit-captured-frames 1000

Capturing on inband
2018-09-15 23:45:40.124077   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.124477     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.124533   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.126344   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.126607     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.126655   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
    2018-09-15 23:45:40.128348   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
 2018-09-15 23:45:40.128611 10.0.0.1 -> 10.0.0.100 ICMP Redirect (Redirect for host) 2018-09-15
23:45:40.128659 10.0.0.100 -> 192.168.0.1 ICMP Echo (ping) request
2018-09-15 23:45:40.130362   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.130621     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.130669   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.132392   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.132652     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.132700   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.134347   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.134612     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.134660   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.136347   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.136598     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.136645   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.138351   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.138607     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.138656   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
```

...

时间戳上面输出建议在本例中突出显示的三数据包同时捕获， 2018-09-15 23:45:40.128。下面此数据包组每个信息包细分

- 第一数据包是入口数据包，在本例中是一ICMP echo请求。

  **2018-09-15 23:45:40.128348 10.0.0.100 - > 192.168.0.1 ICMP回音(ping)请求**

- 第二数据包是ICMP重定向数据包，生成由网关。此数据包被退还的到主机。

  **2018-09-15 23:45:40.128611 10.0.0.1 - > 10.0.0.100 ICMP重定向(主机的重定向)**

- 在CPU后，路由第三数据包是在输出方向捕获的数据包。虽则没显示以上，此数据包有其被重估的IP TTL减少的和校验和。

  **2018-09-15 23:45:40.128659 10.0.0.100 - > 192.168.0.1 ICMP回音(ping)请求**

当导航通过有许多数据包不同的类型和流时的大Ethanalyzer捕获，关联ICMP重定向消息与数据流量可能不是容易的。

在这些情况下，在ICMP获取关于不最理想转发的通信流的信息的重定向消息的重点。ICMP重定向消息包括互联网报头加上原始数据包的数据的前64个位。 此数据由数据包的来源用于匹配消息到适当的进程。

以***详细信息***关键字使用Ethanalyzer数据包捕获工具显示ICMP重定向消息内容和找到不最理想转发数据流的IP地址信息

```
Nexus7000# ethanalyzer local interface inband capture-filter icmp limit-captured-frames 1000
detail

...
Frame 2 (70 bytes on wire, 70 bytes captured)
Arrival Time: Sep 15, 2018 23:54:04.388577000
[Time delta from previous captured frame: 0.000426000 seconds]
[Time delta from previous displayed frame: 0.000426000 seconds]
[Time since reference or first frame: 0.000426000 seconds]
Frame Number: 2
Frame Length: 70 bytes
Capture Length: 70 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:icmp:ip:icmp:data]
Ethernet II, Src: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf), Dst: 00:0a:00:0a:00:0a
(00:0a:00:0a:00:0a)
Destination: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
Address: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
Source: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf)
Address: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.100 (10.0.0.100)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 56
Identification: 0xf986 (63878)
Flags: 0x00
0.. = Reserved bit: Not Set
.0. = Don't fragment: Not Set
```

```
..0 = More fragments: Not Set
Fragment offset: 0
Time to live: 255
Protocol: ICMP (0x01)
Header checksum: 0xadd9 [correct]
[Good: True]
[Bad : False]
Source: 10.0.0.1 (10.0.0.1)
Destination: 10.0.0.100 (10.0.0.100)
Internet Control Message Protocol
 Type: 5 (Redirect)
 Code: 1 (Redirect for host)
Checksum: 0xb8e5 [correct]
Gateway address: 10.0.0.2 (10.0.0.2)
Internet Protocol, Src: 10.0.0.100 (10.0.0.100), Dst: 192.168.0.1 (192.168.0.1)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 84
Identification: 0xf986 (63878)
Flags: 0x00
0.. = Reserved bit: Not Set
.0. = Don't fragment: Not Set
..0 = More fragments: Not Set
Fragment offset: 0
Time to live: 254
Protocol: ICMP (0x01)
Header checksum: 0xa8ae [correct]
[Good: True]
[Bad : False]
Source: 10.0.0.100 (10.0.0.100)
Destination: 192.168.0.1 (192.168.0.1)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0 ()
Checksum: 0x02f9 [incorrect, should be 0xcae1]
Identifier: 0xa01d
Sequence number: 36096 (0x8d00)

...
```

# 禁用 ICMP 重定向

如果网络设计要求将路由的通信流在进入交换机或路由器的同一个第3层接口外面，防止流路由通过CPU由在对应的层3接口的明确地禁用的ICMP重定向功能是可能的。

实际上，为了多数网络它是良好的做法主动地禁用在所有第3层接口的ICMP重定向，物理，类似以太网接口，和虚拟，类似Port-Channel和SVI接口。请使用interface-level命令**no ip redirects**的NX-OS禁用在第3层接口的ICMP重定向。遵从这些步骤验证ICMP重定向功能禁用

- 保证**no ip redirects**命令被添加到接口配置

```
Nexus7000# show run interface vlan 10

interface Vlan10
```

```
no shutdown  no ip redirects
  ip address 10.0.0.1/24

Nexus7000#
```

- 保证ICMP重定向状况在接口的显示“*禁用*”

```
Nexus7000# show ip interface vlan 10 | include redirects
IP icmp redirects: disabled
Nexus7000#
```

- 保证ICMP重定向启用/禁用标志设置到“*0*”由推送从交换机的Supervisor的接口配置到更多线路卡之一的NX-OS软件组件

```
Nexus7000# show system internal eltm info interface vlan 10 | i icmp_redirect
  per_pkt_ls_en = 0, icmp_redirect = 0, v4_same_if_check = 0
Nexus7000#
```

- 保证ICMP重定向启用/禁用一个特定的第3层接口的标志设置到“*0*”在一个或更多线路卡

```
Nexus7000# attach module 7
Attaching to module 7 ...
To exit type 'exit', to abort type '$.'
Last login: Wed Sep 15 23:56:25 UTC 2018 from 127.1.1.1 on pts/0
module-7#

<optionally, jump to non-admin Virtual Device Context (VDC) if verification needs to be done in
one of the custom VDCs>
module-7# vdc 6

module-7# show system internal iftmc info interface vlan 10 | include icmp_redirect
icmp_redirect : 0x0 ipv6_redirect : 0x1
module-7#
```

# 摘要

ICMP重定向机制，正如RFC 792所描述，设计通过多点网段优化转发路径。 在早期互联网帮助的这样最优化节约昂贵网络资源，类似链路带宽和路由器CPU周期。

当网络带宽变为更加价格合理和相对更加缓慢的基于CPU的信息包路由转变了成在专用硬件ASIC的更加快速的第3层信息包转发，最佳的数据传输的重要性通过减小的多点网段和不得到同样多网络设计者今天的关心象使用了。

默认情况下， ICMP重定向功能在每个第3层接口启用。然而，其尝试通知在多点以太网段的网络节点关于最佳的转发路径没有由网络人员总是了解并且操作。

在与复合使用的网络中多种转发机制，例如静态路由，动态路由和基于策略的路由，离开ICMP重定向功能启用，不用适当的监听可能导致不理想的使用转接点CPU处理生产数据流。这，反过来，可能导致重大影响在生产数据流运输流量和在网络基础设施的控制层面稳定性。

对于多数网络认为良好的做法主动地禁用ICMP在所有第3层接口的重定向功能在网络基础设施。当有更加好的转发路径通过mutli点网段时，这帮助防止制作数据流方案在第三层交换机和路由器CPU被处理的。