了解ICMP重定向消息

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[背景信息](#)
[ICMP重定向消息](#)
[通过以太网络的次优路径](#)
[静态路由](#)
[基于策略的路由](#)
[点对点链路上的ICMP重定向](#)
[Nexus平台注意事项](#)
[监控和诊断流量的工具](#)
[show ip traffic](#)
[Ethanalyzer](#)
[禁用 ICMP 重定向](#)
[摘要](#)

简介

本文档介绍互联网控制消息协议(ICMP)数据包重定向功能。

先决条件

要求

Cisco 建议您了解以下主题：

- Nexus 7000平台架构
- Cisco NX-OS软件配置
- Internet控制消息协议，如请求注解(RFC)792中所述

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Nexus 7000
- Cisco NX-OS软件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档讨论互联网控制消息协议(ICMP)提供的数据包重定向功能。 本文档说明了网络中通常存在ICMP重定向消息的情况，以及可以采取什么措施来最大限度地减少与导致ICMP重定向消息生成的网络条件相关的负面影响。

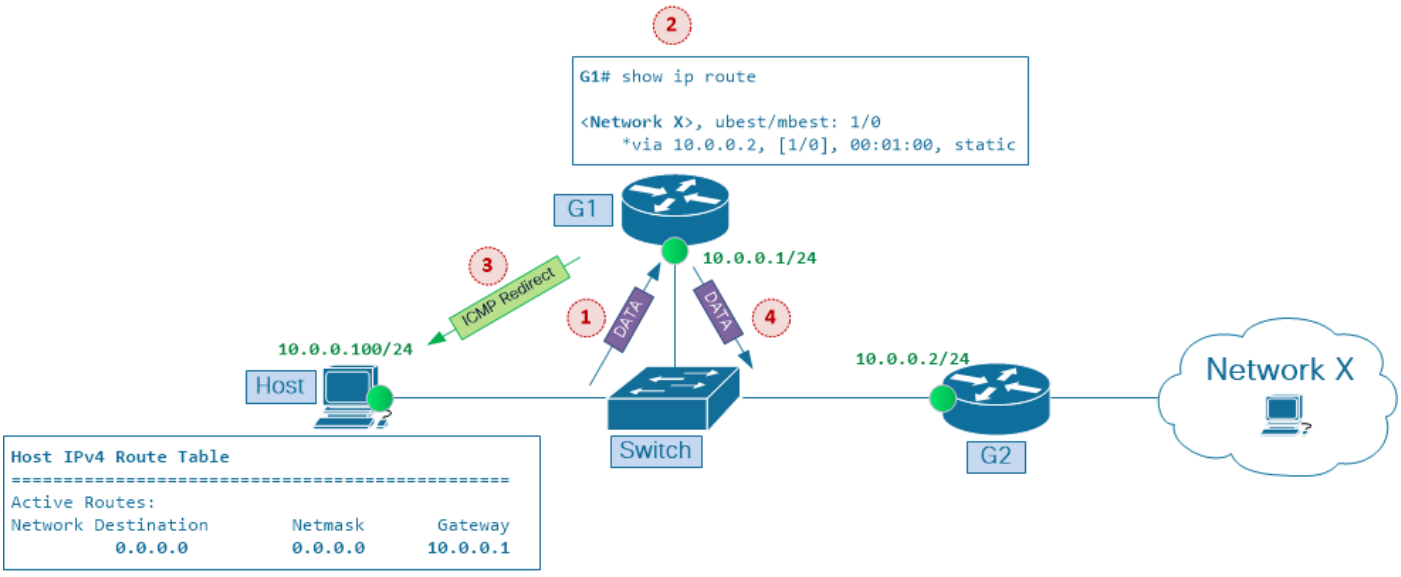
ICMP重定向消息

ICMP重定向功能在RFC 792 Internet Control Message Protocol中进行了说明，该示例包括：

> 在这种情况下，网关会向主机发送重定向消息。
>
> 网关G1从网关所连接的网络中的主机接收Internet数据报。网关G1检查其路由表并获取通往数据报Internet目的网络X的路由中下一个网关G2的地址
>
> 如果G2和数据报的Internet源地址所标识的主机位于同一网络中，则会向主机发送重定向消息。重定向消息建议主机将网络X的流量直接发送到网关G2，因为这是通向目的地的较短路径。
>
> 网关将原始数据报数据转发到其Internet目标。

此场景如图1所示。*主机和两台路由器(G1和*G2)连接到共享以太网网段，并在同一网络10.0.0.0/24中具有IP地址

图1多点以太网中的ICMP重定向



多点以太网中的ICMP重定向

主机的IP地址为10.0.0.100。主机路由表有一个默认路由条目，该条目指向路由器G1的IP地址10.0.0.1作为默认网关。路由器G1在将流量转发到目的网络X时，使用路由器G2的IP地址10.0.0.2作为下一跳。

这就是当主机向目的网络X发送数据包时发生的情况：

1. IP地址为10.0.0.1的网关G1从主机10.0.0.100接收数据包，该主机位于与它连接的网络上。

2.网关G1检查其路由表并获取通往数据包目的网络X的路由上的下一个网关G2的IP地址10.0.0.2。

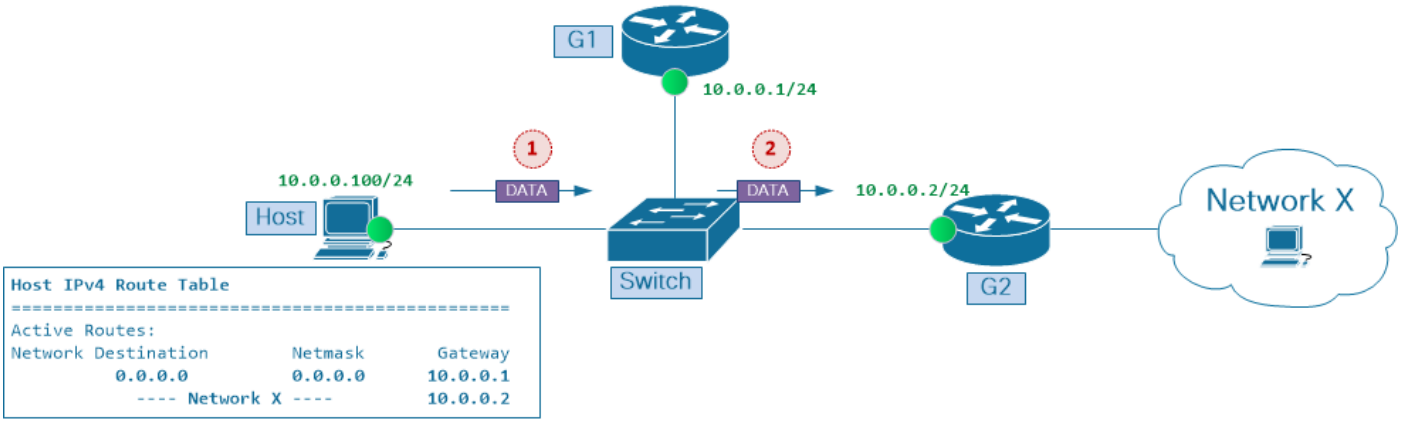
3.如果G2和IP数据包的源地址所标识的主机位于同一网络中，则会向主机发送ICMP重定向消息。ICMP重定向消息建议主机将网络X的流量直接发送到网关G2，因为这是通往目标的较短路径。

4. 网关G1将原始数据包转发到目的地。

根据主机配置，它可以选择忽略G1向其发送的ICMP重定向消息。但是，如果主机使用ICMP重定向消息调整其路由缓存并开始将后续数据包直接发送到G2，则在此场景中可获得这些优势

- 优化通过网络的数据转发路径；流量更快地到达目的地
- 降低网络资源利用率，例如带宽和路由器CPU负载

图2安装在主机路由缓存中的下一跳G2



安装在主机路由缓存中的下一跳G2

如图2所示，在主机为网络X创建路由缓存条目，并将G2作为下一跳之后，网络中即可看到以下优势：

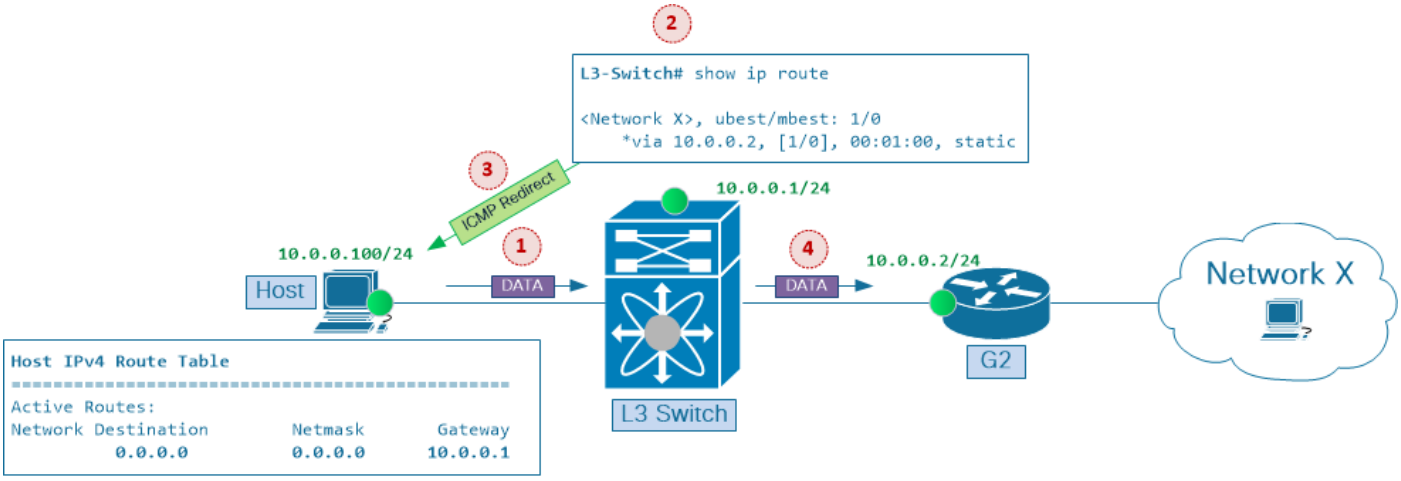
- 交换机和路由器G1之间链路的带宽利用率在两个方向上都有所下降。
- 路由器G1上的CPU使用率降低，因为从主机到网络X的流量不再流经此节点。
- 主机与网络X之间的端到端网络延迟得到改善。

要了解ICMP重定向机制的重要性，请记住，早期的互联网路由器实施主要依赖于CPU资源来处理数据流量。因此，希望减少任何单个路由器必须处理的流量，并最小化特定流量在到达目的地的过程中必须经过的路由器跳数。同时，第2层转发（也称为交换）主要在定制的专用集成电路(ASIC)中实现，从转发性能的角度来说，与第3层转发（也称为路由）相比，相对“便宜”，同样是在通用处理器中完成的。

较新的ASIC代可以同时执行第2层和第3层数据包转发。在硬件中执行的第3层表查找有助于降低与路由器处理数据包相关的性能成本。此外，当将第3层转发功能集成到第2层交换机（现在称为第3层交换机）时，数据包转发操作更加高效，这消除了单臂路由器(也称为单臂路由**器)设计选项的需要，并避免了与这些网络配置相关的限**制。

图3基于图1中的场景。现在，最初由两个独立节点（交换机和路由器G1）提供的第2层和第3层功能整合到单个第3层交换机中，例如Nexus 7000系列平台。

图3第3层交换机取代“单臂路由器”配置



第3层交换机取代“单臂路由器”配置

这就是当主机向目的网络X发送数据包时会发生的情况：

1. IP地址为10.0.0.1的网关L3交换机从其所连接网络上的主机10.0.0.100接收数据包。

2.网关L3交换机检查其路由表并获取下一网关G2在通往数据包目的网络X的路由上的地址10.0.0.2。

3.如果G2和IP数据包的源地址所标识的主机位于同一网络中，则会向主机发送ICMP重定向消息。ICMP重定向消息建议主机将网络X的流量直接发送到网关G2，因为这是通往目标的较短路径。

4. 网关将原始数据包转发到目的地。

由于第3层交换机现在能够在ASIC级别同时执行第2层和第3层数据包转发，可以得出结论，ICMP重定向功能的优势、(a)通过网络改善延迟和(b)降低网络资源利用率都得以实现，并且无需再过多关注多点以太网网段中的路径优化技术。

但是，由于第3层接口上启用了ICMP重定向功能，通过多点以太网网段的次优转发会继续存在潜在的性能瓶颈，即使出于不同原因，如本文档后面的Nexus平台注意事项部分所述。

> **注意**：默认情况下，ICMP重定向在Cisco IOS和Cisco NX-OS软件的第3层接口上启用。

> **注意**：生成ICMP重定向消息时的条件摘要：如果数据包要从接收此数据包的第3层接口转发出去，第3层交换机将生成ICMP重定向消息返回数据包源。

通过以太网络的次优路径

内部网关协议(IGP)(例如开放最短路径优先(OSFP)和思科增强型内部网关路由协议(EIGRP))旨在同步路由器之间的路由信息，并在所有支持此类信息的网络节点上提供一致且可预测的数据包转发行为。例如，对于多点以太网络，如果网段中的所有第3层节点使用相同的路由信息并同意到达目的地的同一出口点，则很少会出现通过此类网络进行次优转发的情况。

要了解导致次优转发路径的原因，请记住，第3层节点会做出彼此独立的数据包转发决策。也就是说，路由器B作出的数据包转发决策并不依赖于路由器A作出的数据包转发决策。这是排除通过IP网络转发数据包故障时需要记住的关键原则之一，也是研究多点以太网络中的次优转发路径时要记住的重要原则。

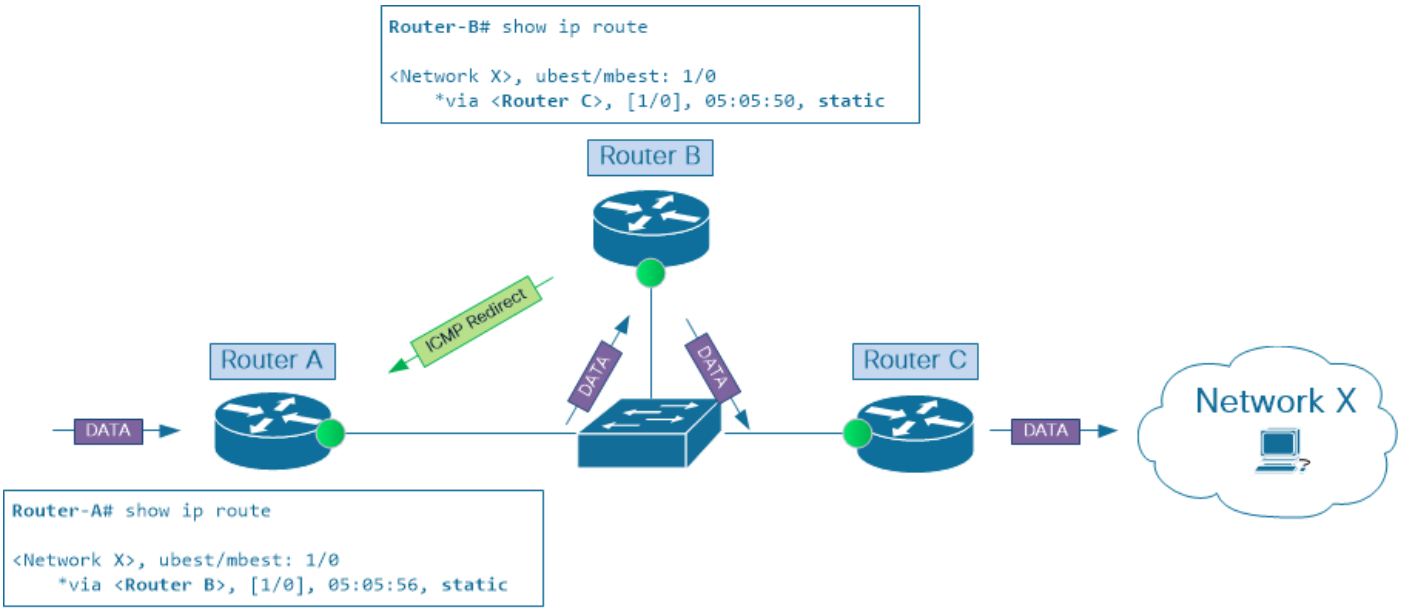
如前所述，在网络中，所有路由器都依靠单个动态路由协议在端点之间传输流量，因此不能通过多点以太网网段进行次优转发。然而，在现实的网络中，经常会发现各种数据包路由和转发机制的组合，例如各种IGP、静态路由和基于策略的路由。这些功能通常共同用于实现所需的流量在网络上转发。

虽然结合使用这些机制有助于微调流量并满足特定网络设计的需求，但它们忽视了这些工具一起使用在多点以太网络中可能导致的负面影响，即整体网络性能不佳。

静态路由

为了说明这一点，请考虑图4中的场景。路由器A具有到网络X的静态路由，路由器B是其下一跳。同时，路由器B使用路由器C作为到网络X的静态路由的下一跳。

图4使用静态路由的次优路径



静态路由次优路径

当流量在路由器A进入此网络，离开它通过路由器C并最终被传送到目的网络X时，数据包在到达目的地的途中，必须通过此IP网络两次。这不能有效利用网络资源。相反，将数据包从路由器A直接发送到路由器C将获得相同的结果，同时消耗较少的网络资源。

> **注意：**尽管在此方案中，路由器A和路由器C用作此IP网段的入口和出口第3层节点，但如果后者的路由配置导致相同的数据包转发行为，则两个节点都可以替换为网络设备（如负载均衡器或防火墙）。

基于策略的路由

策略型路由(PBR)是另一种机制，它可能导致通过以太网的路径不理想。但是，与静态或动态路由不同，PBR不在路由表级别运行。相反，它直接在交换机硬件中编程流量重定向访问控制列表(ACL)。因此，对于选定的流量流，入口线卡上的数据包转发查找会绕过通过静态或动态路由获取的路由信息。

在图4中，路由器A和路由器B使用其中一个动态路由协议交换有关目的网络X的路由信息。两者都同意，路由器B是通向此网络的最佳下一跳。

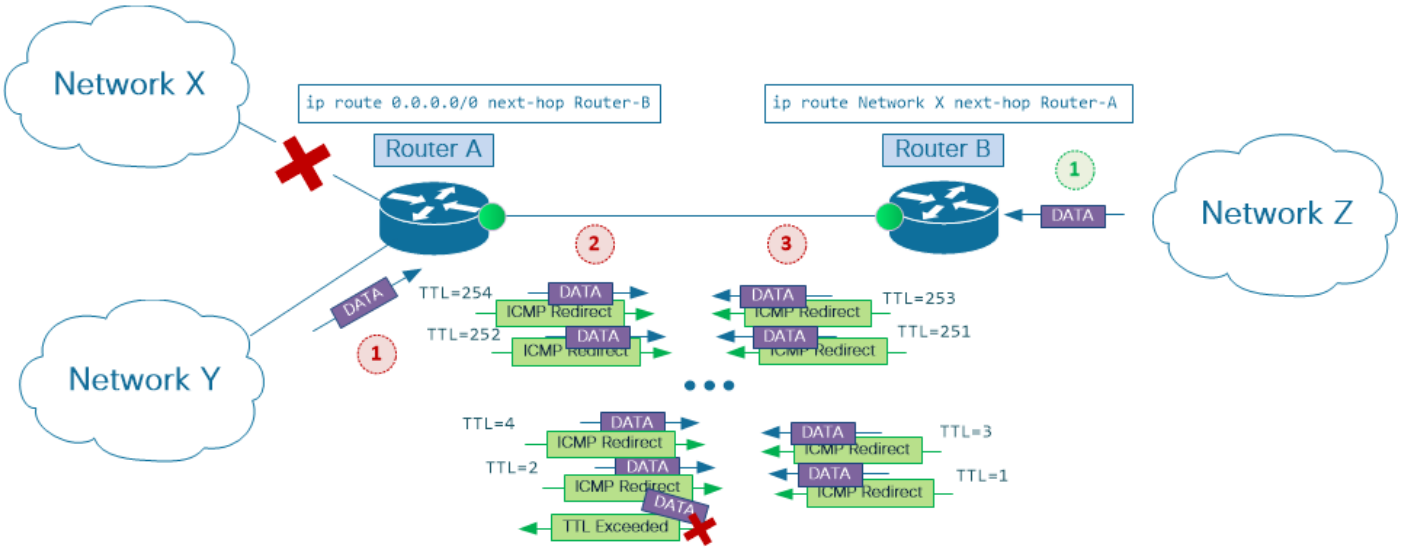
但是，路由器B上的PBR配置会覆盖从路由协议接收的路由信息，并将路由器C设置为通向网络X的下一跳，因此满足触发ICMP重定向功能的条件，并将数据包发送到路由器B的CPU进行进一步处理。

点对点链路上的ICMP重定向

迄今为止，本文档介绍连接了三个（或多个）第3层节点的以太网网络，因此称为多点以太网网络。但请注意，ICMP重定向消息也可在点对点以太网链路上生成。

考虑图5中的场景。路由器A使用静态默认路由向路由器B发送流量，而路由器B具有指向路由器A的网络X静态路由。

图5点对点链路上的ICMP重定向



静态路由次优路径

当您将小型用户环境连接到服务提供商网络时，这种设计选项（也称为单宿主连接）是常用选择。这里，路由器B是提供商边缘(PE)设备，而路由器A是用户边缘(CE)设备。

注意，典型的CE配置包括到指向Null0接口的用户IP地址块的聚合静态路由。此配置是具有静态路由的单宿主CE-PE连接选项的建议最佳实践。但是，在本示例中，假设不存在此类配置。

假设路由器A失去了与网络X的连接，如图所示。当来自用户网络Y或远程网络Z的数据包尝试到达网络X时，路由器A和B会相互之间退回流量，并减小每个数据包中的IP生存时间字段，直到其值达到1，此时无法进一步路由数据包。

当流向网络X的流量在PE和CE路由器之间来回反弹时，CE-PE链路带宽使用率会显着（且不必要地）增加，如果在点对点PE-CE连接的一端或两端启用ICMP重定向则问题会更严重。在这种情况下，流向网络X的流中的每个数据包都会在每个路由器的CPU中多次处理，以帮助生成ICMP重定向消息。

Nexus平台注意事项

在第3层接口上启用ICMP重定向且传入的数据包使用此接口进出第3层交换机时，将生成ICMP重定向消息。在Cisco Nexus 7000平台上的硬件中执行第3层数据包转发时，交换机CPU仍负责构建ICMP重定向消息。为此，Nexus 7000 Supervisor模块上的CPU需要获取流的IP地址信息，该流可

通过网段进行路径优化。这是入口线卡向Supervisor模块发送数据包背后的原因。

如果ICMP重定向消息的收件人忽略该消息并继续将数据流量转发到启用ICMP重定向的Nexus交换机的第3层接口，则会为每个数据包触发ICMP重定向生成过程。

在线卡级别上，进程以硬件转发异常的形式启动。当线卡模块无法成功完成数据包转发操作时，在ASIC上引发异常。在这种情况下，需要将数据数据包发送到Supervisor模块以进行正确的数据包处理。

> **注意**：Supervisor模块上的CPU不仅生成ICMP重定向消息，还处理许多其他数据包转发异常，例如生存时间(TTL)值设置为1的IP数据包，或需要在发送到下一跳之前分段的IP数据包。

当Supervisor模块上的CPU向源发送ICMP重定向消息后，它将通过出口线卡模块将数据数据包转发到下一跳来完成异常处理。

虽然Nexus 7000 Supervisor模块使用功能强大的CPU处理器来处理大量流量，但该平台的设计可在线卡级别处理大多数数据流量，而无需在数据包转发过程中使用Supervisor CPU处理器。这使CPU能够专注于其核心任务，并将数据包转发操作留给线卡上的专用硬件引擎。

在稳定的网络中，如果发生数据包转发异常，预计将以相当低的速率发生。使用此假设，它们可以由Supervisor CPU处理而不会对其性能产生重大影响。另一方面，CPU处理以极高速率出现的数据包转发异常会对整体系统稳定性和响应性产生负面影响。

Nexus 7000平台设计提供多种机制来保护交换机CPU免受大量流量的影响。这些机制在系统的不同点实施。在线卡级别，有硬件速率限制器和控制平面 Policing (CoPP)功能。两者都设置了流量速率阈值，有效控制从每个线卡模块转发到Supervisor的流量。

这些保护机制优先处理对网络稳定性和交换机可管理性至关重要的各种控制协议（如OSPF、BGP或SSH）的流量，同时它们积极过滤对控制交换机的平面功能不重要的流量类型。如果由于数据包转发异常而转发到CPU，则大多数数据流量会受到此类机制的严格管制。

硬件速率限制器和CoPP policing 这些机制提供了交换机的控制平面的稳定性，强烈建议始终启用，它们可能是导致整个网络中数据包丢弃、传输延迟和整体应用性能不佳的主要原因之一。因此，必须了解流量流经网络的路径以及使用工具监控能够和/或预期使用ICMP重定向功能的网络设备。

监控和诊断流量的工具

show ip traffic

Cisco IOS和Cisco NX-OS软件均提供检查由CPU处理的流量的统计信息的方法。这是通过 **show ip traffic** 命令。此命令可用于检查第3层交换机或路由器接收和/或生成ICMP重定向消息。

```
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 命令并检查ICMP重定向计数器是否增加。

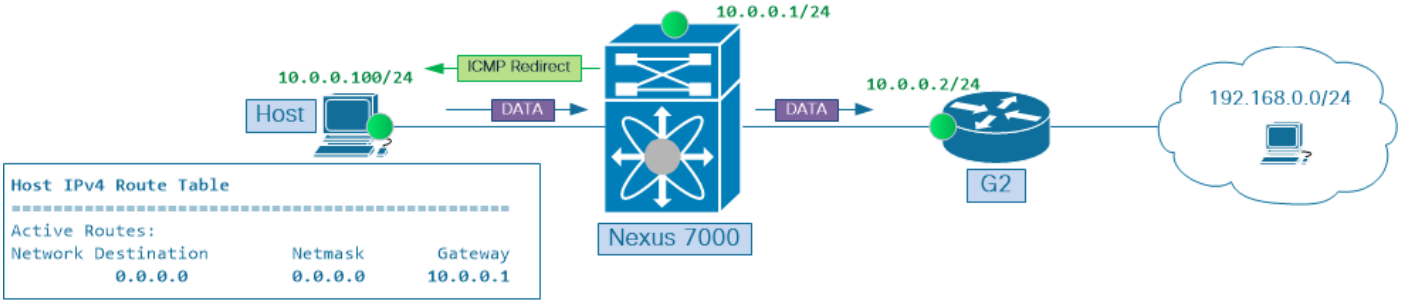
Ethanalyzer

Cisco NX-OS软件具有捕获流量的内置工具 flowing 交换机CPU（称为Ethanalyzer）之间的连接。

> **注意**：有关Ethanalyzer的详细信息，请参阅Nexus 7000上的Ethanalyzer故障排除指南。

图6显示的场景与图3中的场景类似。此处网络X由192.168.0.0/24网络取代。

图6运行Ethanalyzer捕获



运行Ethanalyzer捕获

主机10.0.0.100向目标IP地址192.168.0.1发送一条ICMP回应请求连续流。该主机使用Nexus 7000交换机的交换机虚拟接口(SVI)10作为其到远程网络192.168.0.0/24的下一跳。出于演示目的，主机配置为忽略ICMP重定向消息。

使用以下下一命令捕获Nexus 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

...
```

上一个输出中的时间戳表明此示例中突出显示的三个数据包同时被捕获，即2018-09-15 23:45:40.128。接下来是此数据包组的每个数据包的细分

- 第一个数据包是入口数据包，在本例中是ICMP回应请求。
  2018-09-15 23:45:40.128348 10.0.0.100 -> 192.168.0.1 ICMP响应(ping)请求
- 第二个数据包是由网关生成的ICMP重定向数据包。此数据包将发送回主机。
  2018-09-15 23:45:40.128611 10.0.0.1 -> 10.0.0.100 ICMP重定向（主机重定向）
- 第三个数据包是CPU路由后在出口方向捕获的数据包。尽管之前未显示，此数据包的IP TTL会递减并重新计算校验和。
  2018-09-15 23:45:40.128659 10.0.0.100 -> 192.168.0.1 ICMP响应(ping)请求

当您浏览包含许多不同类型和流量的数据包的大型Ethanalyzer捕获时，很难将ICMP重定向消息与相应的数据流量相关联。

在这些情况下，请重点关注ICMP重定向消息以检索有关未优化转发流量的信息。ICMP重定向消息包括Internet报头以及原始数据报数据的前64位。数据报的源使用此数据将消息与相应的进程进行匹配。

使用带有**detail**关键字的Ethanalyzer数据包捕获工具显示ICMP重定向消息的内容并查找未优化转发的数据流的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

如果网络设计要求流量从进入交换机或路由器的同一第3层接口路由，则当您禁用对应的第3层接口上的ICMP重定向功能时，可以阻止流量通过CPU路由。

事实上，对于大多数网络，最好在所有第3层接口上主动禁用ICMP重定向，包括物理接口（如以太网接口）和虚拟接口（如端口通道和SVI接口）。请使用 no ip redirects Cisco NX-OS接口级命令可禁用第3层接口上的ICMP重定向。要验证ICMP重定向功能是否已禁用，请执行以下操作：

- 确保**no ip redirects**命令已添加到接口配置中。

```
Nexus7000#show run interface vlan 10

interface Vlan10
no shutdown no ip redirects
  ip address 10.0.0.1/24
```

- 确保接口上的ICMP重定向的状态显示为“disabled”。

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

- 确保Cisco NX-OS软件组件将ICMP重定向启用/禁用标志设置为**0**，该组件将接口配置从交换机Supervisor推送到多个线卡之一。

```
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
```

- 确保一个或多个线卡上特定第3层接口的ICMP重定向启用/禁用标志设置为**0**。

```
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
```

摘要

如RFC 792中所述，ICMP重定向机制旨在优化通过多点网段的转发路径。在Internet刚开始时，此类优化有助于保护昂贵的网络资源，如链路带宽和路由器的CPU周期。随着网络带宽变得更加经济实惠，相对较慢的基于CPU的数据包路由演变为专用硬件ASIC中更快的第3层数据包转发，通过多点网段传输最佳数据的重要性降低了。默认情况下，ICMP重定向功能在每个第3层接口上启用。但

是，它尝试向多点以太网网段上的网络节点通知最佳转发路径的尝试并不总是被网络人员理解和执行。在结合使用各种转发机制（如静态路由、动态路由和基于策略的路由）的网络中，如果保留ICMP重定向功能启用并且未正确监控，则可能导致不必要地使用中转节点CPU来处理生产流量。这反过来又会对生产流量和网络基础设施的控制平面稳定性造成重大影响。

对于大多数网络，最好在网络基础设施中的所有第3层接口上主动禁用ICMP重定向功能。这有助于防止在存在通过多点网段的更好转发路径时，在第3层交换机和路由器的CPU中处理生产数据流量的场景。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。