瞭解ICMP重新導向訊息

目錄

簡介

本檔案介紹網際網路控制訊息通訊協定(ICMP)封包重新導向功能。

必要條件

需求

思科建議您瞭解以下主題：

- Nexus 7000平台架構
- Cisco NX-OS軟體配置
- 網際網路控制訊息通訊協定，記錄於要求建議(RFC)792中

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Nexus 7000
- Cisco NX-OS軟體

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本檔案將討論網際網路控制訊息通訊協定(ICMP)提供的封包重新導向功能。 本檔案將說明網路中存在ICMP重新導向訊息通常表示什麼，以及可以做些什麼來儘量減少與導致ICMP重新導向訊息產生的網路條件相關的負面影響。

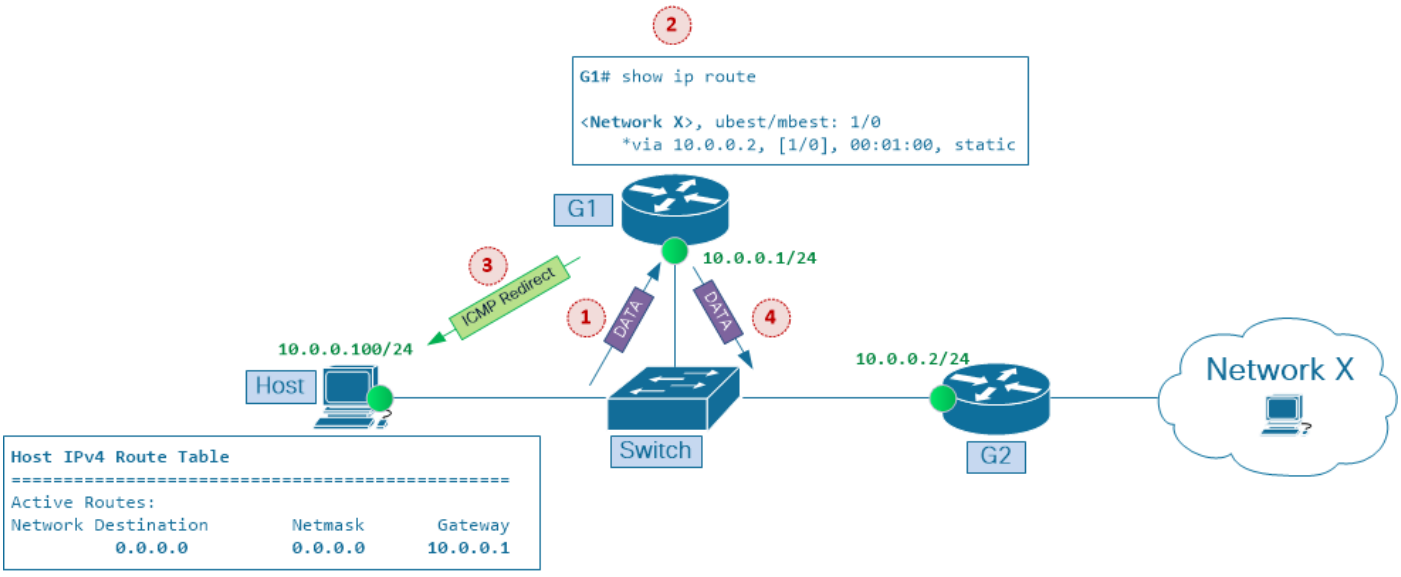
ICMP重定向消息

RFC 792網際網路控制訊息通訊協定中詳述ICMP重新導向功能，並提供以下範例：

> 在這種情況下，閘道會向主機傳送重新導向訊息。
>
> 網關G1從網關所連線的網路中的主機接收網際網路資料包。網關G1檢查其路由表並獲取通往資料包網際網路目的網路X的路由上的下一個網關G2的地址
>
> 如果G2和由資料包的Internet源地址標識的主機位於同一網路中，則會向主機傳送重定向消息。重定向消息建議主機將網路X的流量直接傳送到網關G2，因為這是通往目的地的較短路徑。
>
> 網關將原始資料包資料轉發到其Internet目標。

此場景如圖1所示。主機和兩個路由器（G1和G2）連線到共用乙太網網段，並在同一網路10.0.0.0/24中具有IP地址

圖1多點乙太網中的ICMP重定向



多點乙太網路中的ICMP重新導向

主機的IP地址為10.0.0.100。主機路由表有一個預設路由條目，該條目指向路由器G1的IP地址10.0.0.1作為預設網關。路由器G1在將流量轉發到目的網路X時，使用路由器G2的IP地址10.0.0.2作為下一跳。

這就是主機將封包傳送到目的地網路X時發生的情況：

1. IP地址為10.0.0.1的網關G1從它連線的網路中的主機10.0.0.100接收資料包。

2.網關G1檢查其路由表並獲取下一個網關G2的IP地址10.0.0.2，該路由到資料包目的網路X。

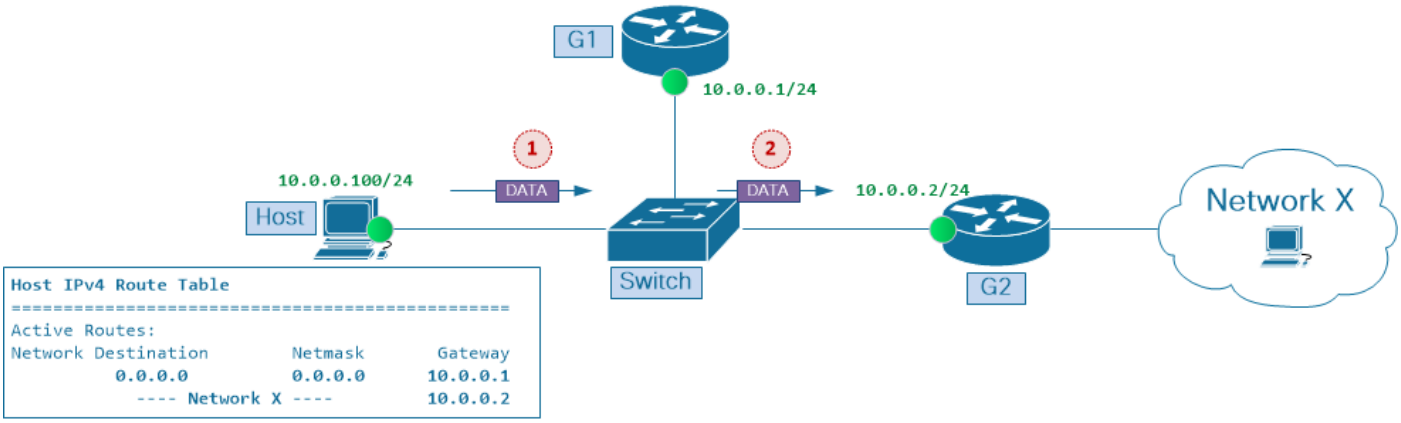
3.如果G2和IP資料包的源地址所標識的主機位於同一網路中，則會向主機傳送ICMP重定向消息。ICMP重定向消息建議主機將網路X的流量直接傳送到網關G2，因為這是通往目標的較短路徑。

4. 網關G1將原始資料包轉發到其目的地。

根據主機配置，它可以選擇忽略G1向其傳送的ICMP重定向消息。但是，如果主機使用ICMP重定向消息來調整其路由快取並開始將後續資料包直接傳送到G2，則在此場景中可實現這些優勢

- 最佳化通過網路的資料轉發路徑；流量更快地到達目的地
- 降低網路資源利用率，例如頻寬和路由器CPU負載

圖2安裝在主機路由快取中的下一跳G2



在主機路由快取中安裝下一跳G2

如圖2所示，在主機為G2作為其下一跳的網路X建立路由快取條目後，網路中可以看到以下優點：

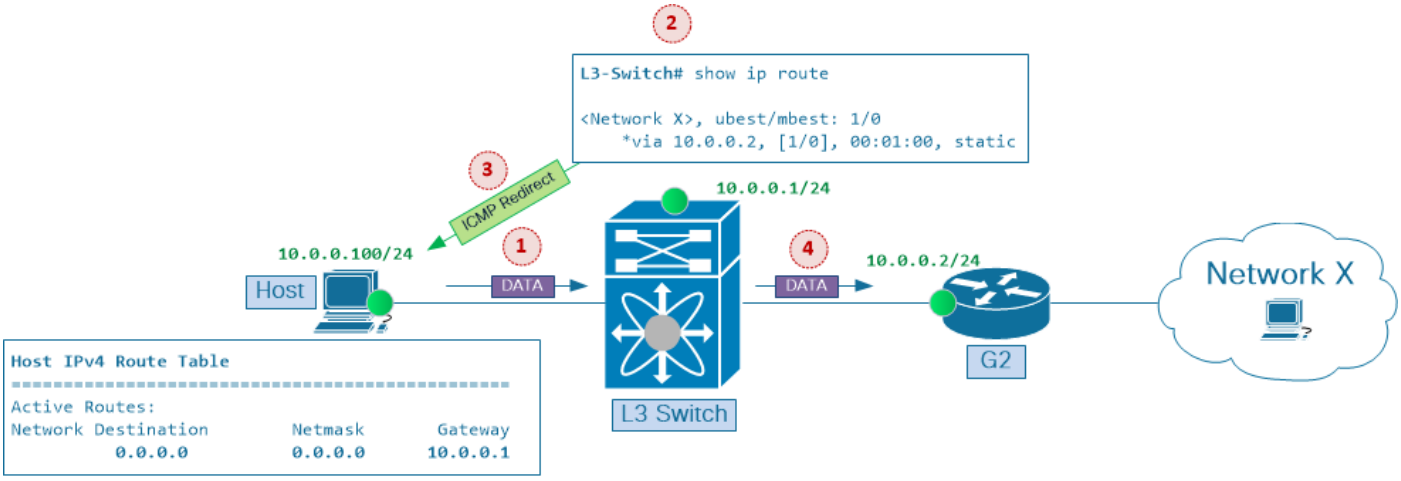
- 交換機和路由器G1之間鏈路的頻寬利用率在兩個方向上都有所下降。
- 路由器G1上的CPU使用率降低，因為從主機到網路X的流量不再流經此節點。
- 主機與網路X之間的端到端網路延遲得到改善。

要瞭解ICMP重定向機制的重要性，請記住，早期的網際網路路由器實施主要依賴於CPU資源來處理資料流量。因此，希望減少必須由任何單個路由器處理的流量，並最小化特定流量在到達目的地的途中必須經過的路由器跳數。同時，第2層轉送（也稱為交換）主要在定製的專用積體電路(ASIC)中實現，並且從轉送效能的角度來說，相對於第3層轉送（也稱為路由）相對「便宜」，同樣是在通用處理器中完成的。

較新的一代ASIC可以同時執行第2層和第3層資料包轉發。在硬體中執行的第3層表查詢有助於降低與路由器處理資料包相關的效能成本。此**外，當將第3層轉發功能整合到第2層交換機（現在稱為第3層交換機）時，資料包轉發操作更加高效，這消除了單臂路由器(也稱為單臂路由器)設計選項的需要，並避免了與此類網路配置相關的限**制。

圖3基於圖1中的場景。現在，最初由兩個獨立節點（交換機和路由器G1）提供的第2層和第3層功能整合到單個第3層交換機中，如Nexus 7000系列平台。

圖3第3層交換機取代「單臂路由器」配置



第3層交換機取代「單臂路由器」配置

這就是當主機將資料包傳送到目的網路X時發生的情況：

1. IP地址為10.0.0.1的網關L3交換機從其所連線的網路中的主機10.0.0.100接收資料包。

2.網關L3交換機檢查其路由表，獲取下一網關G2在通往資料包目的網路X的路由上的地址10.0.0.2。

3.如果G2和IP資料包的源地址所標識的主機位於同一網路中，則會向主機傳送ICMP重定向消息。ICMP重定向消息建議主機將網路X的流量直接傳送到網關G2，因為這是通往目標的較短路徑。

4. 網關將原始資料包轉發到其目的地。

由於第3層交換器現在能夠在ASIC層執行第2層和第3層封包轉送，因此可以得出結論，ICMP重新導向功能可同時實現以下兩個優點：(a)改善透過網路的延遲；(b)降低網路資源利用率，且無需再過多關注多點乙太網路區段中的路徑最佳化技術。

但是，由於第3層介面上啟用了ICMP重定向功能，通過多點乙太網網段的次優轉發仍會存在潛在的效能瓶頸，即使出於不同原因，如本文檔後面的Nexus平台注意事項部分所述。

> **附註**：Cisco IOS和Cisco NX-OS軟體的第3層介面預設啟用ICMP重定向。

> **附註**：產生ICMP重新導向訊息時的條件摘要：如果資料包要從接收此資料包的第3層介面轉發出去，第3層交換機將生成ICMP重定向消息返回資料包的來源。

通過乙太網路的次最佳路徑

內部閘道通訊協定(IGP)(例如開放最短路徑優先(OSFP)和思科增強型內部閘道路由通訊協定(EIGRP))是專為同步路由器之間的路由資訊而設計，並在所有接受此類資訊的網路節點上提供一致且可預測的封包轉送行為。例如，對於多點乙太網路，如果網段中的所有第3層節點使用相同的路由資訊並在到達目的地的相同出口點上達成一致，則很少會存在通過此類網路進行次優轉發的情況。

要瞭解導致非最佳轉發路徑的原因，請記住第3層節點會做出彼此獨立的資料包轉發決策。即，路由器B做出的資料包轉發決定並不依賴於路由器A做出的資料包轉發決定。當您對通過IP網路的資料包轉發進行故障排除時，這是需要牢記的關鍵原則之一；當您調查多點乙太網中的次優轉發路徑時，請牢記這一點。

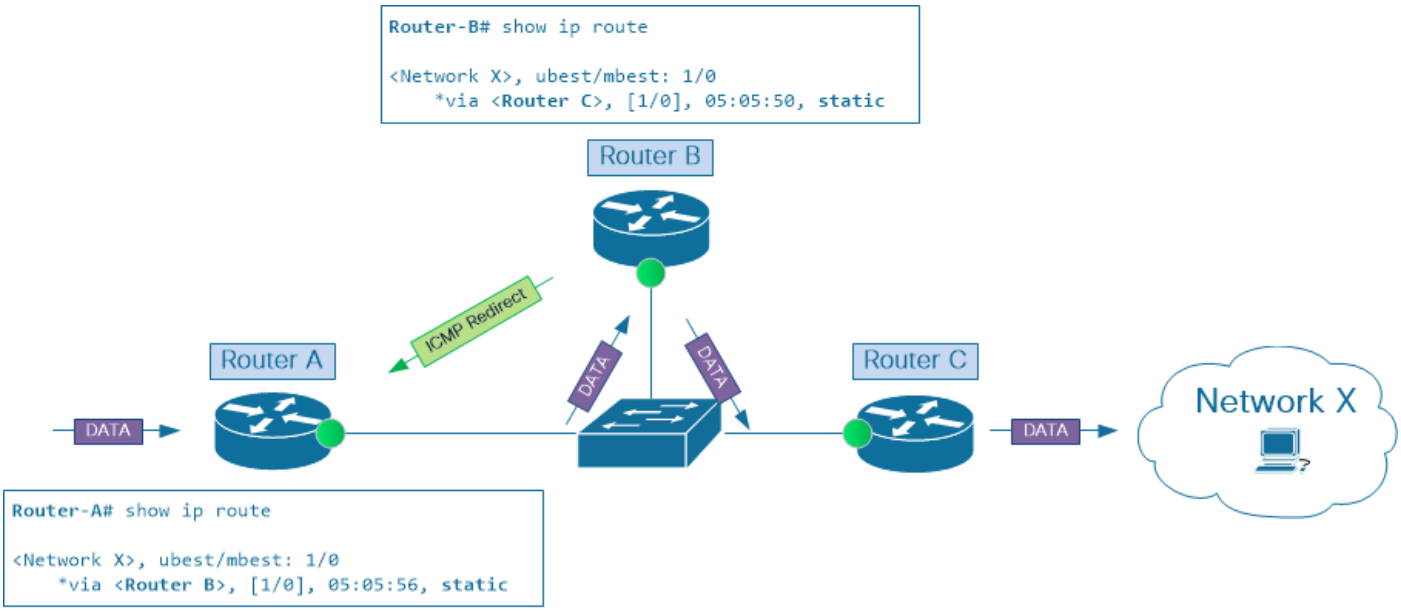
如前所述，在所有路由器都依靠單個動態路由協定在端點之間傳送流量的網路中，不得通過多點乙太網段進行次優轉發。然而，在現實的網路中，經常會發現各種資料包路由和轉發機制的組合，例如各種IGP、靜態路由和基於策略的路由。這些功能通常一起用於實現通過網路轉發所需的流量。

雖然結合使用這些機制有助於微調流量並滿足特定網路設計的需求，但它們忽視了這些工具共同使用在多點乙太網中可能導致的整體網路效能不佳的副作用。

靜態路由

為了說明此情況，請考慮圖4中的場景。路由器A具有到網路X的靜態路由，路由器B是其下一跳。同時，路由器B將路由器C用作通往網路X的靜態路由的下一跳。

圖4使用靜態路由的次優路徑



靜態路由次優路徑

當流量在路由器A進入此網路、通過路由器C離開後，最終被傳送到目的網路X時，資料包在到達目的地的途中，必須經過此IP網路兩次。這不能有效利用網路資源。相反，將資料包從路由器A直接傳送到路由器C將獲得相同的結果，同時消耗的網路資源較少。

> **附註**：即使在此案例中，路由器A和路由器C用作此IP網段的入口和出口第3層節點，但如果後者的路由配置導致相同的資料包轉發行為，則兩個節點都可以替換為網路裝置（如負載平衡器或防火牆）。

原則型路由

原則型路由(PBR)是另一種可能會造成乙太網路中的次佳路徑的機制。但是，與靜態或動態路由不同，PBR不在路由表級別運行。相反，它直接在交換機硬體中程式設計流量重定向訪問控制清單(ACL)。因此，對於選定的流量流，入口線卡上的資料包轉發查詢會繞過通過靜態或動態路由獲得的路由資訊。

在圖4中，路由器A和B使用其中一個動態路由協定交換有關目的網路X的路由資訊。雙方都同意，路由器B是通往此網路的最佳下一跳。

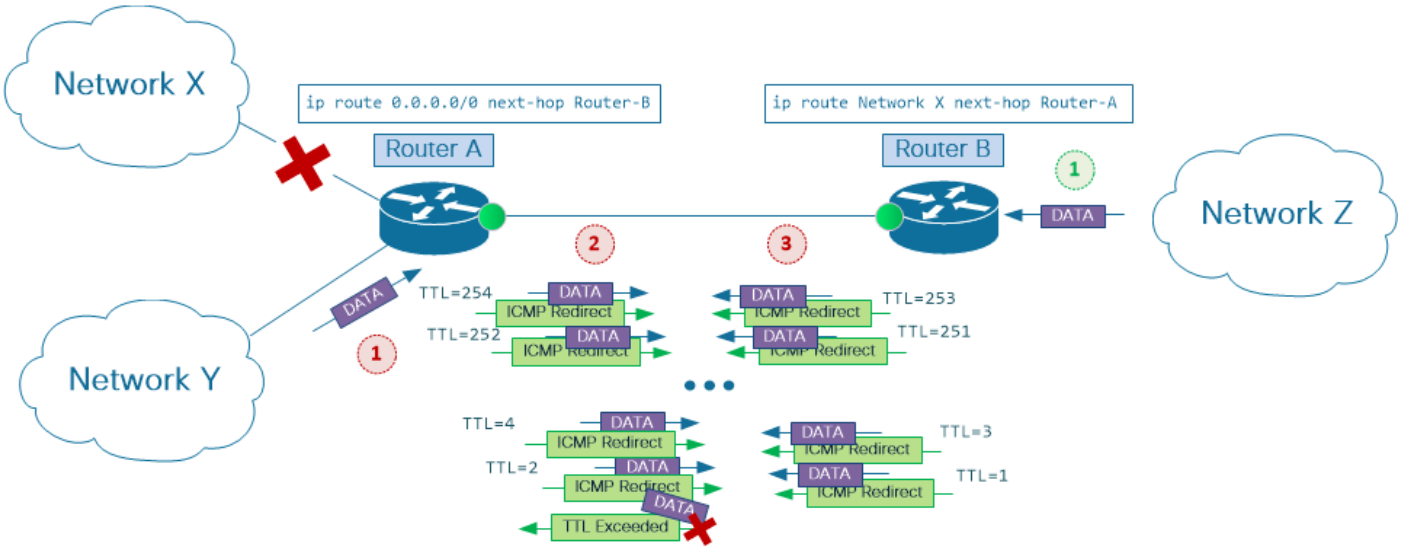
但是，路由器B上的PBR配置會覆蓋從路由協定接收的路由資訊，並將路由器C設定為通向網路X的下一跳，因此滿足觸發ICMP重定向功能的條件，並將資料包傳送到路由器B的CPU進行進一步處理。

點對點連結上的ICMP重新導向

到目前為止，本文檔所指的乙太網連線了三個（或更多個）第3層節點，因此稱為多點乙太網路。但是請注意，ICMP重新導向訊息也可能會在點對點乙太網路連結上產生。

考慮圖5中的場景。路由器A使用靜態預設路由將流量傳送到路由器B，而路由器B具有指向路由器A的網路X靜態路由。

圖5點對點連結上的ICMP重新導向



靜態路由次優路徑

將小型使用者環境連線到服務提供商網路時，此設計選項（也稱為單宿主連線）是常用的選擇。這裡，路由器B是提供商邊緣(PE)裝置，而路由器A是使用者邊緣(CE)裝置。

請注意，典型的CE配置包括到指向Null0介面的使用者IP地址塊的聚合靜態路由。對於具有靜態路由的單宿主CE-PE連線選項，建議採用此配置。但是在本範例中，假設沒有此類組態。

假設路由器A斷開與網路X的連線，如圖所示。當來自使用者網路Y或遠端網路Z的資料包嘗試到達網路X時，路由器A和B會相互之間退回流量，並減小每個資料包中的IP生存時間欄位，直到其值達到1，此時無法進一步路由資料包。

儘管到Network X的流量在PE和CE路由器之間來回反彈，但CE-PE鏈路頻寬利用率卻顯著增加（而且不必要地），如果在點對點PE-CE連線的一端或兩端啟用ICMP重定向則問題會變得更糟。在此案例中，導向網路X的流量中的每個封包會在每個路由器的CPU中處理多次，以協助產生ICMP重新導向訊息。

Nexus平台注意事項

在第3層介面上啟用ICMP重新導向且傳入資料封包使用此介面來輸入和輸出第3層交換器時，會產生ICMP重新導向訊息。雖然第3層封包轉送在Cisco Nexus 7000平台上的硬體中完成，但交換器CPU仍負責建立ICMP重新導向訊息。若要執行此操作，Nexus 7000監督器模組上的CPU需要取得

其透過網段的路徑可最佳化的流量的IP位址資訊。這是入口線卡向Supervisor模組傳送資料封包之後發生的原因。

如果ICMP重定向消息的收件人忽略該消息並繼續將資料流量轉發到已啟用ICMP重定向的Nexus交換機的第3層介面，則會為每個資料包觸發ICMP重定向生成過程。

線上卡級別，進程以硬體轉發異常的形式啟動。當線卡模組無法成功完成資料包轉發操作時，在ASIC上引發異常。在這種情況下，資料包需要傳送到Supervisor模組以進行正確的資料包處理。

> **附註**：Supervisor模組上的CPU不僅生成ICMP重定向消息，還處理許多其他資料包轉發異常，例如生存時間(TTL)值設定為1的IP資料包，或需要在傳送到下一跳之前分段的IP資料包。

Supervisor模組上的CPU向源傳送ICMP重定向消息後，通過出口線卡模組將資料包轉發到下一跳來完成異常處理。

雖然Nexus 7000 Supervisor模組使用功能強大的CPU處理器來處理大量流量，但該平台的設計可線上卡級別處理大部分資料流量，而無需在資料包轉發過程中使用Supervisor CPU處理器。這允許CPU集中處理其核心任務，並將資料包轉發操作保留給線卡上的專用硬體引擎。

在穩定的網路中，資料包轉發異常（如果發生）預計將以相當低的速率發生。使用此假設，它們可以由Supervisor CPU處理，而不會對其效能產生重大影響。另一方面，對於處理以非常高速率發生的資料包轉發異常的CPU，可能會對整體系統穩定性和響應性產生負面影響。

Nexus 7000平台設計提供多種機制來保護交換機CPU免受大量流量的影響。這些機制在系統的不同點實施。線上卡級別，有硬體速率限制器和控制平面 Policing (CoPP)功能。二者都設定了流量速率閾值，有效控制從每個線卡模組轉發到Supervisor的流量。

這些保護機制優先使用對網路穩定性和交換機可管理性至關重要的各種控制協定（例如OSPF、BGP或SSH）的流量，同時它們積極過濾對控制交換機的平面功能不重要的流量型別。如果由於資料包轉發異常而轉發到CPU，則大部分資料流量會受到此類機制的嚴格監管。

硬體速率限制器和CoPP policing 這些機制提供了交換機的控制平面的穩定性，強烈建議始終啟用，它們可能是導致整個網路中資料包丟棄、傳輸延遲和整體應用程式效能不佳的主要原因之一。這就是為什麼必須瞭解流量流經網路的路徑，以及使用工具監控能夠和/或預期使用ICMP重定向功能的網路裝置。

監控和診斷流量的工具

show ip traffic

Cisco IOS和Cisco NX-OS軟體均提供檢查CPU處理流量的統計資訊的方法。這是通過 **show ip traffic** 指令。此命令可用於檢查第3層交換機或路由器收到和/或生成ICMP重定向消息的情況。

```
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#
```

運行 show ip traffic 命令並檢查ICMP重定向計數器是否增加。

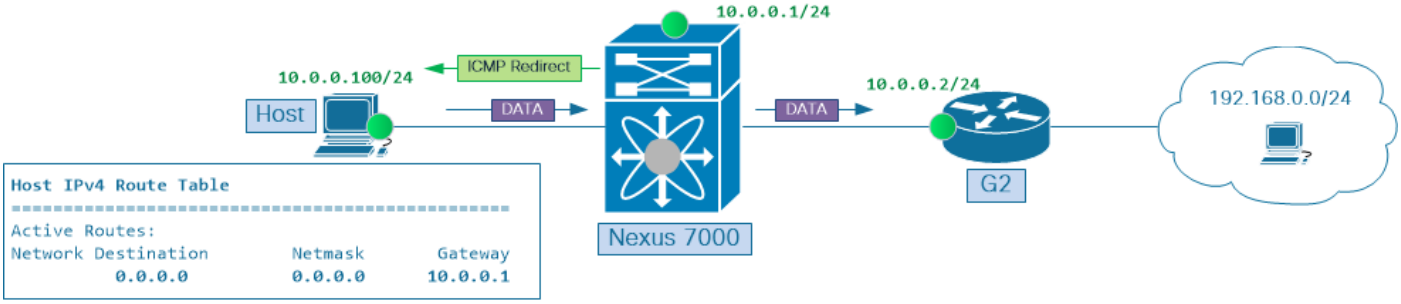
Ethanalyzer

Cisco NX-OS軟體具有捕獲流量的內建工具 flowing 交換機CPU之間的連線，稱為Ethanalyzer。

> **附註**：有關Ethanalyzer的詳細資訊，請參閱Nexus 7000上的Ethanalyzer故障排除指南。

圖6顯示的場景與圖3中的場景類似。此處網路X由192.168.0.0/24網路替換。

圖6運行Ethanalyzer捕獲



運行Ethanalyzer捕獲

主機10.0.0.100向目標IP地址192.168.0.1傳送連續ICMP回應請求流。該主機使用Nexus 7000交換機的交換機虛擬介面(SVI)10作為其到遠端網路192.168.0.0/24的下一跳。為了進行演示，該主機配置為忽略ICMP重定向消息。

使用以下命令捕獲Nexus 7000 CPU接收和傳送的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

...
```

前面輸出中的時間戳表明此示例中突出顯示的三個資料包是同時捕獲的，即2018-09-15 23:45:40.128。接下來是此資料包組的每個資料包細分

- 第一個封包是輸入資料封包，在本範例中為ICMP回應請求。
  2018-09-15 23:45:40.128348 10.0.0.100 -> 192.168.0.1 ICMP回應(ping)請求
- 第二個資料包是由網關生成的ICMP重定向資料包。此封包會傳送回主機。
  2018-09-15 23:45:40.128611 10.0.0.1 -> 10.0.0.100 ICMP重新導向（主機重新導向）
- 第三個資料包是CPU路由後在出口方向捕獲的資料包。雖然之前未顯示，此封包的IP TTL會遞減並重新計算總和檢查碼。
  2018-09-15 23:45:40.128659 10.0.0.100 -> 192.168.0.1 ICMP回應(ping)請求

當您瀏覽包含許多不同型別和流量的資料包的大型Ethanalyzer捕獲時，很難將ICMP重定向消息與相應的資料流量相關聯。

在這些情況下，請聚焦ICMP重定向消息以檢索有關未以最佳狀態轉發的流量的資訊。ICMP重定向消息包括Internet報頭加上原始資料包資料的前64位。資料包的源使用此資料將消息與相應進程匹配。

使用帶有**detail**關鍵字的Ethanalyzer封包擷取工具以顯示ICMP重新導向訊息的內容，並尋找未以最佳方式轉送的資料流的IP位址資訊

```
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

如果網路設計要求流量從進入交換器或路由器的同一第3層介面路由出去，則如果在對應的第3層介面上停用ICMP重新導向功能，便可防止流量通過CPU路由。

事實上，對於大多數網路，最好在所有第3層介面上主動禁用ICMP重定向，物理介面（如乙太網介面）和虛擬介面（如埠通道和SVI介面）。使用 no ip redirects Cisco NX-OS介面級命令禁用第3層介面上的ICMP重定向。驗證ICMP重新導向功能是否已停用：

- 確保**no ip redirects**命令被新增到介面配置。

```
Nexus7000#show run interface vlan 10

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

- 確保介面上的ICMP重新導向狀態顯示為「disabled」。

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

- 確保Cisco NX-OS軟體元件將ICMP重定向啟用/禁用標誌設定為**0**，該元件將介面配置從交換機Supervisor推送到多個線卡之一。

```
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
```

- 確保一個或多個線卡上將特定第3層介面的ICMP重定向啟用/禁用標誌設定為**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

RFC 792中所述的ICMP重新導向機制旨在最佳化通過多點網段的轉送路徑。在Internet剛開始時，此類最佳化有助於保護昂貴的網路資源，如鏈路頻寬和路由器的CPU週期。隨著網路頻寬變得更加經濟實惠，並且相對較慢的基於CPU的資料包路由演變為專用硬體ASIC中更快速的第3層資料包轉發，通過多點網段傳輸最佳資料的重要性降低了。預設情況下，ICMP重定向功能在每個第3層介

面上啟用。但是，它試圖通知多點乙太網段上的網路節點最佳轉發路徑的嘗試並不總是由網路人員理解和執行。在結合使用各種轉發機制（如靜態路由、動態路由和基於策略的路由）的網路中，如果您保留ICMP重定向功能並且未正確監控，則可能導致不必要地使用傳輸節點CPU來處理生產流量。這反過來又會對網路基礎設施的生產流量流和控制平面穩定性造成重大影響。

對於大多數網路，主動停用網路基礎架構中所有第3層介面的ICMP重新導向功能是很好的作法。這有助於防止在存在通過多點網段的更佳轉發路徑時，在第3層交換機和路由器的CPU中處理生產資料流量的情況。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。