IGRP簡介

目錄

簡介

本檔案介紹內部閘道路由通訊協定(IGRP)。 它有兩個目的。其中之一是為有興趣使用、評估並可能實施該技術的使用者介紹該技術。另一種是更廣泛地介紹一些在IGRP中體現的有趣的想法和概念。有關如何配置IGRP的資訊，請參閱配置IGRP、Cisco IGRP實施和IGRP命令。

IGRP的目標

IGRP協定允許許多網關協調其路由。其目標如下：

- 即使是在非常大型或複雜的網路中，路由也是穩定的。即使瞬時，也不會發生路由回圈。
- 快速響應網路拓撲的變化。
- 低開銷。也就是說，IGRP本身使用的頻寬不應超過其任務實際需要的頻寬。
- 當多條並行路由的期望值大致相等時將其流量分開。
- 考慮不同路徑上的錯誤率和流量級別。

IGRP的當前實施可處理TCP/IP的路由。但是，基本設計旨在能夠處理各種協定。

沒有一種工具可以解決所有路由問題。傳統上，路由問題被分解成多個部分。IGRP等協定稱為「內部網關協定」(IGP)。 它們可以用在一組單一的網路中，用一種管理系統或者一些能夠密切配合的管理系統來管理。此類網路組通過「外部網關協定」(EGP)連線。 IGP旨在跟蹤有關網路拓撲的大量詳細資訊。設計IGP的首要任務是生成最佳路由並快速響應變化。EGP旨在保護一個網路系統免受其他系統的錯誤或故意誤報的影響，BGP就是這樣一個外部網關協定。設計EGP的重點是穩定性和行政控制。通常EGP產生合理的路徑是足夠的，而不是最優路徑。

IGRP與Xerox的路由資訊協定、Berkeley的RIP和Dave Mills的Hello等舊協定有一些相似之處。它不同於這些協定，主要是為更大型和更複雜的網路而設計。請參見與RIP的比較一節，以獲取與RIP（老一代協定中最廣泛使用的協定）的更詳細比較。

與這些舊協定一樣，IGRP也是距離向量協定。在這種協定中，網關只與相鄰網關交換路由資訊。此路由資訊包含有關網路其餘部分的資訊摘要。從數學上可以看出，所有網關一起解決的是一個最佳化問題，相當於一個分散式演算法。每個網關只需要解決部分問題，並且只需要接收總資料的一部分。

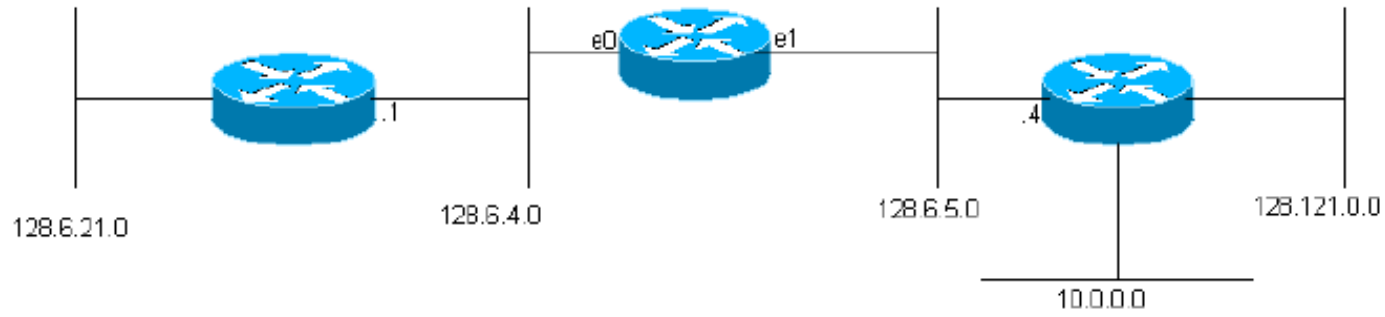
IGRP的主要替代方案是增強型IGRP(EIGRP)和一類稱為SPF（最短路徑優先）的演算法。OSPF使用此概念。要瞭解有關OSPF的詳細資訊，請參閱OSPF設計手冊。OSPF這些路由基於泛洪技術，其中每個網關都保持有關其他每個網關上每個介面狀態的最新資訊。每個網關使用整個網路的資料從自己的角度獨立解決最佳化問題。每種方法都有優勢。在一些情況下，SPF可以非常快地對變動做出響應。為了防止路由環路，IGRP必須在某些型別的更改之後將新資料忽略幾分鐘。因為SPF直接擁有來自每個網關的資訊，所以它能夠避免這些路由環路。因此，它可以立即對新資訊採取行動。然而，無論在內部資料結構還是在網關之間的消息中，SPF都必須處理比IGRP多得多的資料。

路由問題

IGRP旨在用於連線多個網路的網關。我們假設網路使用基於資料包的技術。實際上，網關充當資料包交換機。當連線到一個網路的系統想要將資料包傳送到不同網路上的系統時，它會將該資料包地址到網關。如果目的地位於連線到閘道的其中一個網路上，則閘道會將封包轉送到目的地。如果目的地更遠，則網關會將資料包轉發到更靠近目的地的另一個網關。網關使用路由表幫助他們決定如何處理資料包。以下是簡單的路由表示例。(示例中使用的地址是從羅格斯大學獲取的IP地址。請注意，其它協定的基本路由問題也類似，但此說明假設IGRP用於路由IP。)

圖1

```
network      gateway     interface
  -------      -------     ---------
  128.6.4      none        ethernet 0
  128.6.5      none        ethernet 1
  128.6.21     128.6.4.1   ethernet 0
  128.121      128.6.5.4   ethernet 1
  10           128.6.5.4   ethernet 1
```



（如我們將看到的，實際IGRP路由表包含每個網關的附加資訊。）此網關連線到兩個名為0和1的乙太網。它們的IP網路號（實際子網號）為128.6.4和128.6.5。因此，只需使用適當的乙太網介面，就可以直接將針對這些特定網路定址的資料包傳送到目的地。有兩個臨近的網關：128.6.4.1和128.6.5.4。用於128.6.4和128.6.5以外網路的資料包將轉發到這兩個網關中的一個或另一個。路由表指示哪個網關應該用於哪個網路。例如，發往網路10上主機的資料包應轉發到網關128.6.5.4。希望此網關更靠近網路10，即到達網路10的最佳路徑通過此網關。IGRP的主要目的是允許網關構建和維護這樣的路由表。

IGRP摘要

如上所述，IGRP是一種協定，允許網關通過與其他網關交換資訊來建立路由表。網關以直接連線到它的所有網路的條目開頭。它通過與相鄰網關交換路由更新來獲取有關其他網路的資訊。在最簡單的情況下，網關會找到一條代表到達每個網路的最佳方式的路徑。路徑的特徵是應該將資料包傳送到下一個網關、應該使用的網路介面和度量資訊。度量資訊是一組表示路徑效能好壞的數字。這允許網關比較它從各種網關中聽到的路徑，並決定使用哪個路徑。通常情況下，在兩個或多個路徑之間分割流量是合理的。每當兩條或多條路徑同等好時，IGRP都會執行此任務。使用者也可以將其設定為幾乎同等良好路徑時分割流量。在這種情況下，將有更多流量沿著具有更好指標的路徑傳送。其用意是流量可以在9600 bps線路和19200 BPS線路之間分隔，而19200線路得到的流量大約是9600 BPS線路的兩倍。

IGRP使用的度量包括：

- 拓撲延遲時間
- 路徑的最窄頻寬段的頻寬
- 路徑的通道佔用率
- 路徑的可靠性

拓撲延遲時間是沿該路徑到達目的地所花費的時間（假定網路已解除安裝）。當然，載入網路時會有額外的延遲。然而，負載是使用通道佔用率數位計算的，而不是嘗試測量實際延遲。路徑頻寬只是路徑中最慢鏈路的頻寬（以位/秒為單位）。通道佔用率表示該頻寬的當前使用量。它是測量的，並且會隨負載而變化。可靠性表示當前錯誤率。它是未損壞地到達目的地的資料包的分數。它是測量的。

雖然它們不用作度量的一部分，但會隨度量傳遞兩個附加資訊：跳數和MTU。跳數只是資料包到達目的地所需經過的網關數量。MTU是整個路徑中可傳送而不進行分段的最大封包大小。（也就是說，這是路徑中涉及的所有網路的MTU的最小值。）

根據度量資訊，為路徑計算單個「複合度量」。複合度量將各種度量分量的效果合併為一個表示該路徑的「優度」的數字。它是實際用於確定最佳路徑的複合度量。

每個網關定期向所有相鄰網關廣播其整個路由表（由於水準分割規則而進行了一些審查）。當網關從另一個網關收到此廣播時，它會將該表與其現有表進行比較。任何新的目的地和路徑都將新增到網關的路由表中。廣播中的路徑會與現有路徑進行比較。如果新路徑更好，它可能會取代現有路徑。廣播中的資訊還用於更新通道佔用情況和有關現有路徑的其他資訊。此常規過程類似於所有距離向量協定使用的過程。數學文獻中稱其為貝爾曼 — 福特演算法。請參閱RFC 1058，詳細瞭解基本程式的開發過程，其中描述較舊的距離向量協定RIP。

在IGRP中，對通用的Bellman-Ford演算法進行了三個關鍵方面的改進。首先，不是使用簡單的度量，而是使用度量向量來描述路徑。其次，不是選取度量最小的單個路徑，而是將流量分割到多個路徑中，這些路徑的度量落在指定的範圍內。第三，引入了幾個功能，以便在拓撲發生變化的情況下提供穩定性。

根據複合度量選擇最佳路徑：

```
[(K1 / Be) + (K2 * Dc)] r
```

其中K1、K2 =常數、Be =解除安裝路徑頻寬x（1 — 通道佔用率）、Dc =拓撲延遲、r =可靠性。

具有最小複合度量的路徑將是最佳路徑。當有多個路徑到達同一目的地時，網關可以通過多條路徑路由資料包。這是根據每個資料路徑的複合度量完成的。例如，如果一條路徑的複合度量為1，而另一條路徑的複合度量為3，則將通過複合度量為1的資料路徑傳送三倍於此的資料包。

使用度量資訊向量有兩個優點。首先，它提供了從同一組資料中支援多種型別的服務的能力。第二個優點是提高了精度。當使用單個度量時，通常將其視為延遲。路徑中的每個鏈路都新增到總度量中。如果鏈路的頻寬較低，則通常代表較大的延遲。但是，頻寬限制不會像延遲那樣真正累積。通過將頻寬視為獨立的元件，可以正確處理頻寬。同樣，負載可以由單獨的通道佔用數來處理。

IGRP提供了一種用於互連電腦網路的系統，其可以穩定地處理包括環的一般圖形拓撲。系統維護完整的路徑度量資訊，即它知道連線到任何網關的所有其他網路的路徑引數。流量可以分佈於並行路徑上，並且可以在整個網路中同時計算多個路徑引數。

與RIP的比較

本節將IGRP與RIP進行比較。這種比較很有用，因為RIP被廣泛用於類似於IGRP的目的。然而，這樣做並不完全公平。RIP並非旨在實現與IGRP相同的所有目標。RIP旨在用於具有合理統一技術的小型網路。在這種應用中，它通常是適當的。

IGRP和RIP之間最基本的區別在於其度量結構。遺憾的是，這種更改不能簡單地更新為RIP。它需要新的演算法和IGRP中的資料結構。

RIP使用簡單的「跳數」度量來描述網路。與IGRP不同，在RIP中，每條路徑都用延遲、頻寬等來描述，而在RIP中，則用1到15之間的數字來描述。通常，這個數字用於表示路徑到達目的地之前經過多少個網關。這表示慢速串列線路和乙太網之間沒有區別。在RIP的一些實現中，系統管理員可以指定對給定跳數進行多次計數。慢速網路可能代表較大的跳數。但是由於最大值為15，所以這很難做到。例如，如果乙太網由1表示，56Kb線路由3表示，則一條路徑中最多可以有5條56Kb線路，或者超出最大值15。為了表示所有可用網路速度，並適應大型網路，Cisco的研究建議需要24位度量。如果最大度量太小，系統管理員將面臨一個令人不快的選擇：他要麼無法區分快和慢路由，要麼無法讓整個網路達到極限。事實上，現在許多全國性網路已足夠大，即使每跳只計數一次，RIP也無法處理它們。RIP根本不能用於此類網路。

顯而易見的反應是修改RIP以允許更大的度量。不幸的是，這行不通。與所有距離向量協定一樣，RIP也存在「計數到無窮大」的問題。 RFC 1058 中將對此進行更詳細的說明。當拓撲發生變化時，會引入虛假路由。與這些虛假路由相關的度量會緩慢增加，直到達到15時才刪除路由。15是一個足夠小的最大值，因此假定使用觸發更新，此過程會較快收斂。如果將RIP修改為允許使用24位度量，環路將持續足夠長的時間，該度量將被計數到2**24。這是不可容忍的。IGRP具有旨在防止引入虛假路由的功能。這些將在下面的5.2節中討論。不引入這些功能或更改SPF等協定就無法處理複雜的網路。

IGRP的作用遠不止簡單地增加允許度量的範圍。它重組度量以描述延遲、頻寬、可靠性和負載。可以在單個度量（如RIP）中表示這些注意事項。但是，IGRP採用的方法可能更準確。例如，對於單個度量，多個連續的快速連結將等效於單個慢速連結。對於以延遲為主要問題的互動式流量來說可能也是如此。但是，對於批次資料傳輸，主要關注的是頻寬，而將度量加在一起並不是正確的方法。IGRP單獨處理延遲和頻寬，累計延遲，但頻寬最小。我們並不容易看到如何將可靠性和負載的影響結合到單元件度量中。

在我看來，IGRP的一大優勢是易於配置。它可以直接表示具有物理意義的數量。這意味著它可以根據介面型別、線路速度等自動設定。若使用單分量度量，則更有可能必須「熟化」該度量以包含多種不同因素的影響。

其他創新更多的是演算法和資料結構，而不是路由協定。例如，IGRP指定了支援將流量劃分為多個路由的演算法和資料結構。RIP的實現完全可以做到這一點。但是，一旦重新實施路由，就沒有理由繼續使用RIP。

到目前為止，我已經描述了「通用IGRP」，這是一種可以支援任何網路協定路由的技術。但是，在本節中，值得進一步介紹特定的TCP/IP實施。這就是要與RIP進行比較的實現。

RIP更新消息只包含路由表的快照。也就是說，它們具有許多目標和度量值，除此之外幾乎沒有其他值。IGRP的IP實現具有附加的結構。首先，更新消息用「自治系統編號」標識。 這一術語來自Arpanet傳統，並且有具體的含義。但是，對於大多數網路而言，這意味著您可以在同一網路上運行多個不同的路由系統。對於來自多個組織的網路進行融合的地方，這很有用。每個組織可以維護自己的工藝路線。由於每個更新都帶有標籤，因此可以將網關配置為只關注正確的更新。某些網關配置為從多個自治系統接收更新。它們以受控的方式在系統之間傳遞資訊。請注意，這不是路由安全問題的完整解決方案。可以將任何網關配置為偵聽來自任何自治系統的更新。但是，如果網路管理員之間存在合理程度的信任，它仍是一個非常有用的路由策略實施工具。

有關IGRP更新消息的第二個結構功能影響IGRP處理預設路由的方式。大多數路由協定都有預設路由的概念。路由更新列出世界上每個網路通常是不切實際的。通常，一組網關需要其組織內網路的詳細路由資訊。發往組織外部目的地的所有流量可以傳送到幾個邊界網關之一。這些邊界網關可能具有更完整的資訊。到最佳邊界網關的路由是「預設路由」。 這是一種預設方式，用於到達內部路由更新中未明確列出的任何目的地。RIP和其它一些路由協定將預設路由的資訊當作真實網路來傳播。IGRP採取了一種不同的做法。IGRP允許將實際網路標籤為預設路由的候選路由，而不是預設路由的一個虛假條目。這可以通過在更新消息的特殊外部部分放置有關這些網路的資訊來實現。但是，也可以認為它開啟了與這些網路相關的部分連線。IGRP定期掃描所有候選預設路由，並選擇度量最低的路由作為實際預設路由。

與大多數RIP實施相比，這種預設方法可能更為靈活。通常，可以將RIP網關設定為使用特定的指定度量生成預設路由。其意圖是在邊界網關處完成此操作。

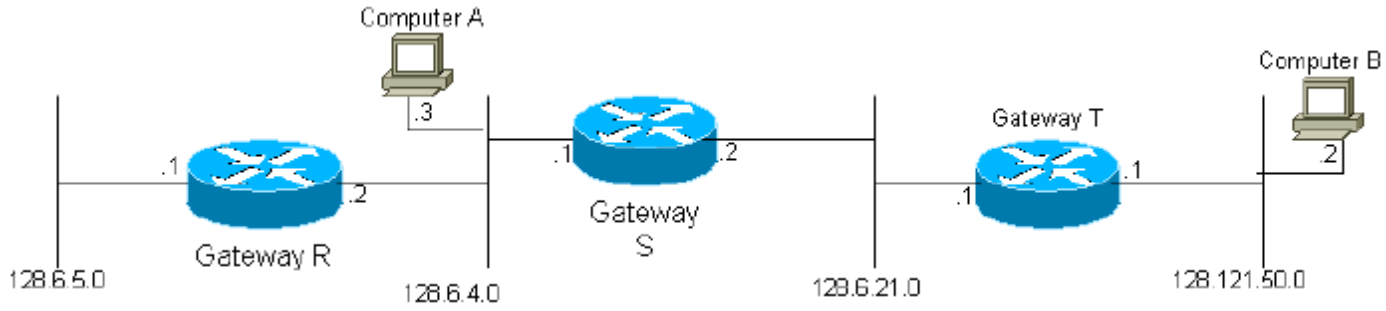
詳細說明

本節詳細介紹了IGRP。

總體說明

當網關首次開啟時，其路由表將被初始化。這可以由操作員從控制檯終端完成，也可以通過從配置檔案讀取資訊完成。提供了與網關連線的每個網路的描述，包括鏈路的拓撲延遲（例如，橫跨鏈路的單個位需要多長時間）和鏈路的頻寬。

圖2



例如，在上圖中，網關S會被告知它通過相應的介面連線到網路2和網路3。因此，最初，網關2隻知道它可以到達網路2和3中的任何目的電腦。所有網關都經過程式設計以定期向它們的相鄰網關傳輸它們已經初始化的資訊，以及從其它網關收集的資訊。因此，網關S將從網關R和T接收更新，並獲知它可以通過網關R到達網路1中的電腦，並通過網關T到達網路4中的電腦。由於網關S傳送其整個路由表，在下一個週期中，網關T將獲知它可以通過網關S到達網路1。很容易看出，系統中每個網路的資訊最終會到達系統中的每個網關，只要網路完全連線。

圖3

```
________ Network 1
       |
       gw A --nw2-- gw C
       |            / |
       |          /   |
       nw3    nw4     nw5
       |      /        |
       |    /          |
       gw B            gw D
      _|_______________|____ Network 6
```

每個網關計算複合度量，以確定到目標電腦的資料路徑是否可取。例如，在上圖中，對於網路6中的目的地，閘道A(gw A)會透過閘道B和C計算兩個路徑的度量函式。請注意，路徑是簡單地由下一個躍點定義的。實際上有三種可能從A路由到網路6:

- 直接到B
- 到C，然後到B
- 到C，然後到D

但是，網關A不需要在涉及C的兩個路由之間進行選擇。A中的路由表有一個條目代表通往C的路徑。它的度量代表從C到達最終目的地的最佳方式。如果A傳送一個資料包到C，則由C來決定是否使用B或D。

等式1

為每個資料路徑計算的複合度量函式如下所示：

```
[(K1 / Be) + (K2 * Dc)] r
```

其中r =分數可靠性（在下一跳成功接收的傳輸的%），Dc =複合延遲，Be =有效頻寬：解除安裝頻寬x（1 — 通道佔用），K1和K2 =常數。

等式2

原則上複合延遲Dc可如下確定：

```
Dc = Ds + Dcir + Dt
```
其中Ds =切換延遲，Dcir =電路延遲（1位的傳播延遲），DT =傳輸延遲（1500位消息的無負載延遲）。

但是，在實踐中，每種網路技術都使用標準的延遲數字。例如，對於乙太網，以及任何特定位元率的串列線路，都有一個標準的延遲數字。

以下範例顯示閘道A的路由表在上面網路6圖的情況下的樣子。（請注意，為簡單起見，度量向量的各個分量未顯示。）

路由表示例：

網路	介面	下一個網關	指標
1	NW 1	無	直接連線
2	NW 2	無	直接連線
3	西北3	無	直接連線
4	NW 2	思	1270
	西北3	B	1180
5	NW 2	思	1270
	西北3	B	2130
6	NW 2	思	2040
	西北3	B	1180

Bellman-Ford演算法描述了通過與鄰居交換資訊來建立路由表的基本過程。此演演算法已用於早期的通訊協定，例如RIP(RFC 1058)。 為了處理更複雜的網路，IGRP在基本的Bellman-Ford演算法中增加了三個功能：

1. 不是簡單的度量，而是使用度量向量來表徵路徑。根據上面的Equation 1，可以從此向量計算單個複合度量。通過使用向量，通過使用等式1中的幾個不同係數，網關可以容納不同型別的服務。與單個度量相比，向量還允許更準確地表示網路的特徵。
2. 流量不是選擇具有最小度量的單個路徑，而是被分割為多個度量落入指定範圍的路徑。這樣可以並行使用多條路由，從而提供比任何單條路由更高的有效頻寬。超差V由網路管理員指定。保留具有最小複合度量M的所有路徑。此外，還會保留度量小於V x M的所有路徑。流量按與複合度量成反比的方式分佈在多個路徑中。
3. 這種方差概念存在一些問題。很難提出使用大於1的方差值的策略，並且不會導致資料包循環。在Cisco 8.2版中，並未實作差異功能。（我不知道該功能是在哪個版本中移除的。）這樣做的效果是將差異永久設定為1。
4. 引入了幾個功能，以便在拓撲發生變化時提供穩定性。這些功能旨在防止路由環路和「計數至無窮大」，這些功能是以前嘗試使用Ford類演算法用於此類應用的典型特徵。主要的穩定性功能是「抑制」、「觸發更新」、「水準分割」和「中毒」。 下文將更詳細地討論這些問題。

流量分割（第2點）帶來相當微妙的危險。方差V設計為允許網關使用不同速度的並行路徑。例如，可能有一條9600 BPS線路與19200 BPS線路並行運行，以實現冗餘。如果方差V為1，則僅使用最佳路徑。因此，如果19200 BPS線路具有合理的可靠性，則不會使用9600 BPS線路。（但是，如果多個路徑相同，則負載將在這些路徑之間共用。）通過增加差異，我們可以允許流量在最佳路由和幾乎同樣好的其他路由之間分配。如果方差足夠大，流量將在兩條線路之間分配。危險在於，如果偏差足夠大，允許路徑不僅速度較慢，而且實際上是「朝著錯誤的方向」。 因此，應該有額外的規則來防止流量被傳送「上游」：不會沿其遠端複合度量（在下一跳計算的複合度量）大於在網關上計算的複合度量的路徑傳送流量。一般情況下，建議系統管理員不要將變數設定為大於1，除非是

在需要使用並行路徑的特定情況下。在這種情況下，將仔細設定差異以提供「正確」的結果。

IGRP旨在處理多個「服務型別」和多個協定。服務型別是資料包中修改路徑評估方式的規範。例如，TCP/IP協定允許資料包指定高頻寬、低延遲或高可靠性的相對重要性。通常，互動式應用程式會指定低延遲，而批次傳輸應用程式會指定高頻寬。這些要求確定適合在Eq中使用的K1和K2的相對值。1.資料包中要支援的每個規範組合都稱為「服務型別」。 對於每種型別的服務，必須選擇一組引數K1和K2。每種服務都保留一個路由表。這是因為路徑是根據均衡器定義的複合度量進行選擇和排序的。1.每種服務型別不同。將來自所有這些路由表的資訊組合起來，生成由網關交換的路由更新消息，如圖7所示。

穩定性功能

本節介紹抑制、觸發更新、水準分割和中毒。這些功能旨在防止網關發現錯誤的路由。如RFC 1058中所述，當由於網關或網路故障導致路由不可用時，可能會發生這種情況。一般來說，相鄰網關檢測故障。然後，它們會傳送路由更新，顯示舊路由不可用。但是，更新可能根本無法到達網路的某些部分，或者到達某些網關時延遲。仍然相信舊路由良好的網關可以繼續傳播該資訊，從而將故障路由重新進入系統。最終，此資訊將通過網路傳播，並返回到重新注入它的網關。結果是循環路由。

事實上，這些對策之間存在著一些冗餘。原則上，抑制和觸發更新應足以首先防止錯誤的路由。然而，在實踐中，各種通訊故障都可能導致其不足。水準分割和路由毒化旨在在任何情況下防止路由環路。

通常，會定期向相鄰網關傳送新的路由表（預設情況下每90秒傳送一次，不過系統管理員可以調整此值）。觸發更新是新的路由表，它會立即傳送以響應某些更改。最重要的更改是刪除路由。發生這種情況的原因是：超時已過期（可能是相鄰網關或線路已關閉），或者路徑中下一個網關的更新消息顯示路徑不再可用。當網關G檢測到路由不再可用時，它會立即觸發更新。此更新將顯示該路由不可用。請考慮此更新到達相鄰網關時發生的情況。如果鄰居的路由指向G，則該鄰居必須刪除該路由。這會導致鄰居觸發更新等。因此，故障將觸發更新消息浪潮。此波將在路由經過故障網關或網路的整個網路中傳播。

如果我們能夠保證立即到達每個適當的網關，觸發更新就足夠了。但是有兩個問題。首先，包含更新消息的資料包可能會被網路中的某些鏈路丟棄或損壞。其次，觸發更新不會立即發生。尚未獲得觸發更新的網關可能將在錯誤的時間發佈常規更新，從而導致錯誤的路由重新插入已經獲得觸發更新的鄰居。抑制旨在避開這些問題。抑制規則表示，當刪除某個路由時，在一段時間內，不會接受同一目標的新路由。這樣，觸發更新就有時間到達所有其他網關，因此我們可以確保獲得的任何新路由不只是某個網關重新插入舊路由。抑制期必須足夠長，以便觸發更新波在網路中傳播。此外，它應該包括幾個常規的廣播週期，以處理丟棄的資料包。考慮當其中一個觸發更新丟失或損壞時會發生的情況。發出該更新的網關將在下一次定期更新時發出另一個更新。這將重新啟動錯過初始波次的鄰居的觸發更新。

觸發更新和抑制的組合應足以消除過期路由並防止它們重新插入。不過，還是應該採取一些額外的防範措施。它們允許非常損耗的網路和已分割槽的網路。IGRP要求的額外預防措施包括水準分割和路由中毒。水準分割的起因是，人們發現將一條路由發回其發源方向從來都是不合理的。請考慮以下情況：

```
network 1        network 2
  -------------X-----------------X
           gateway A          gateway B
```

網關A會告知B它擁有通往網路1的路由。當B向A傳送更新時，它根本沒有理由提及網路1。因為A更接近1，所以沒有理由考慮通過B。水準分割規則表示應該為每個鄰居（實際上每個相鄰網路）生成單獨的更新消息。 指定鄰居的更新應省略指向該鄰居的路由。此規則可防止相鄰網關之間的環路。

例如，假設A到網路1的介面發生故障。如果沒有水準分割規則，B會告訴A它可以到達1。由於它不再具有實際路線，A可能會選擇這條路線。在這種情況下，A和B都有指向1的路由。但A會指向B，B會指向A。當然，觸發的更新和抑制應能防止發生這種情況。但是，既然我們沒有理由把資訊傳回原來的地方，那麼不管怎樣，水準分割都是值得的。水準分割除了具有防止環路的作用外，還降低了更新消息的大小。

水準分割應可防止相鄰網關之間的環路。路由毒化旨在打破較大的環路。規則是，當更新顯示現有路由已充分增加的度量時，就會出現環路。應刪除路由並將其置於抑制狀態。目前的規則是，如果複合度量的增加超過1.1倍，則路由將被刪除。僅增加複合度量的任何增加觸發路由刪除並不安全，因為可能會由於通道佔用率或可靠性的變化而發生較小的度量更改。因此，1.1的係數只是一個啟發式。精確值並不重要。我們預計只需使用此規則即可中斷非常大的環路，因為觸發更新和抑制會阻止較小的環路。

禁用抑制

自版本8.2起，思科的代碼提供禁用抑制的選項。抑制的缺點是，當舊路由發生故障時，它們會延遲採用新路由。使用預設引數時，路由器在更改後採用新路由可能需要幾分鐘時間。然而，出於上述原因，僅僅消除抑制是不安全的。如RFC 1058所述，結果將計數至無窮大。我們猜想（但無法證明）隨著路由毒化的更強版本，不再需要抑制來阻止計數至無窮大。因此，禁用抑制會啟用這種更強大的路由中毒形式。請注意，水準分割和觸發更新仍然有效。

路由中毒的較強形式是基於跳數。如果路徑的跳數增加，則刪除該路由。這顯然會刪除仍然有效的路由。如果網路中的其他部分發生更改，導致路徑現在經過另一個網關，則跳數將會增加。在這種情況下，路由仍然有效。但是，要將這種情況與路由回圈（計數到無窮大）區分開來，沒有完全安全的方法。 因此，最安全的方法是在跳數增加時刪除路由。如果路由仍然合法，它將在下一次更新時重新安裝，這將導致觸發更新，在系統中的其他位置重新安裝路由。

一般來說，距離向量演算法1很容易採用新的路由。問題在於從系統中徹底清除舊裝置。因此，對於刪除可疑路由過於激進的規則應該是安全的。

更新過程的詳細資訊

圖4至圖8中描述的一組過程旨在處理單個網路協定，例如TCP/IP、DECnet或ISO/OSI協定。但是，協定詳細資訊將僅針對TCP/IP提供。單個網關可以處理遵循多個協定的資料。由於每種協定具有不同的編址結構和資料包格式，因此用於實現圖4至圖8的電腦代碼對於每種協定通常都是不同的。圖4中描述的流程變化最大，如圖4的詳細說明中所述。圖5到圖8中描述的流程具有相同的常規結構。協定與協定的主要區別在於路由更新資料包的格式，此格式必須設計為與特定協定相容。

請注意，目的地的定義可能因協定而異。此處介紹的方法可用於路由到單個主機、網路或更複雜的分層地址方案。使用的路由型別取決於協定的地址結構。當前的TCP/IP實施僅支援到IP網路的路由。因此，「destination」實際上指的是IP網路或子網號。子網資訊只保留給連線的網路。

圖4至圖7顯示了網關使用的路由過程各部分的虛擬碼。程式開始時，輸入描述每個介面的可接受協定和引數。

網關將只處理列出的某些協定。來自使用不在清單上的協定的系統的任何通訊將被忽略。資料輸入如下：

- 網關連線的網路。
- 每個網路的已解除安裝頻寬。
- 每個網路的拓撲延遲。

- 每個網路的可靠性。
- 每個網路的通道佔用率。
- 每個網路的MTU。

然後根據等式1計算每個資料路徑的度量函式。請注意，前三項是相當永久的。它們是底層網路技術的函式，不依賴於負載。可以從配置檔案或通過直接操作員輸入來設定。請注意，IGRP不使用測量的延遲。理論和經驗都表明，使用測量延遲來保持路由穩定的協定非常困難。有兩個測量的引數：可靠性和通道佔用率。可靠性取決於網路介面硬體或韌體報告的錯誤率。

除了這些輸入外，路由演算法還需要幾個路由引數的值。這包括計時器值、差異以及是否啟用抑制。這通常由配置檔案或操作員輸入指定。（自思科8.2版起，差異永久設定為1。）

輸入初始資訊後，網關中的操作由事件觸發 — 資料包到達其中一個網路介面或計時器過期。圖4至圖7中描述的流程觸發如下：

- 資料包到達時，會根據圖4進行處理。這導致資料包從另一個介面發出、被丟棄或被接受以進行進一步處理。
- 當網關接受資料包進行進一步處理時，將採用本規範中未描述的特定協定方式對其進行分析。如果資料包是路由更新，則根據圖5進行處理。
- 圖6顯示由計時器觸發的事件。計時器設定為每秒生成一次中斷。當中斷發生時，圖6中所示的進程被執行。
- 圖7顯示了路由更新子常式。對此子常式的呼叫在圖5和圖6中顯示。
- 此外，圖8顯示了度量值計算的詳細過程，請參見圖5和圖7。

有四個控制路由傳播和到期的關鍵時間常數。這些時間常數可以由系統管理員設定。但是有預設值。這些時間常數為：

- 廣播時間 — 所有連線的介面上的所有網關經常廣播更新。預設設定為每90秒一次。
- 無效時間 — 如果在此時間內未收到給定路徑的更新，則認為已超時。它應為廣播時間的數倍，以便允許網路丟棄包含更新的資料包。預設值為廣播時間的3倍。
- 保持時間 — 當目的地變得不可達（或度量增長到足以導致中毒）時，目的地將進入「抑制狀態」。 在此狀態期間，在這段時間內不會接受同一目標的任何新路徑。保持時間指示此狀態應持續的時間。它應為廣播時間的幾倍。預設值為廣播時間的3倍加上10秒。(如禁用抑制部分所述，可以禁用抑制。)
- 刷新時間 — 如果在此時間內未收到給定目標的更新，則將從路由表中刪除其條目。請注意無效時間和清除時間之間的差異：在無效時間後，路徑將超時並刪除。如果沒有剩餘前往目的地的路徑，現在無法訪問目的地。但是，目標資料庫條目保持不變。它必須保持克制。刷新時間過後，資料庫條目將從表中刪除。它應該比無效時間加上抑制時間長一些。預設值為廣播時間的7倍。

這些數字以以下主要資料結構為前提。為網關支援的每個協定保留一組單獨的資料結構。在每個協定中，為要支援的每種服務型別保留一組單獨的資料結構。

對於系統已知的每個目標，都有一個（可能為空）指向目標的路徑清單、抑制過期時間和上次更新時間。上次更新時間表示此目標的任何路徑上次包括在來自另一個網關的更新中的時間。請注意，每個路徑也會保留更新時間。刪除通往目標的最後一條路徑時，除非禁用抑制，否則目標將被抑制(有關詳細資訊，請參閱禁用抑制部分)。 抑制到期時間表示抑制到期的時間。非零值表示目的地處於抑制狀態。為了節省計算時間，最好為每個目標保留「最佳度量」。這只是到達目的地的所有路徑的合成度量的最小值。

對於到達目的地的每條路徑，都有路徑中下一跳的地址、要使用的介面、表徵路徑的度量向量，包括拓撲延遲、頻寬、可靠性和通道佔用率。其他資訊還與每條路徑相關聯，包括跳數、MTU、資訊源、遠端複合度量，以及根據等式1根據這些數位計算的複合度量。還有最後一次更新時間。資訊源

指出該路徑的最新更新來自何處。實際上，此地址與下一跳的地址相同。上次更新時間只是此路徑的最新更新到達的時間。用於使超時路徑過期。

請注意，IGRP更新消息包含三個部分：內部、系統（意為「這個自治系統」，但不指內部）和外部。內部部分用於通往子網的路由。並非所有子網資訊都包括在內。僅包括一個網路的子網。這是與將更新傳送到的地址關聯的網路。通常，更新會在每個介面上廣播，因此這只是傳送廣播的網路。（對IGRP請求作出響應並指向點IGRP會出現其他情況。）主要網路（例如，非子網）被置於更新消息的系統部分，除非它們被特別標籤為外部。

如果網路是從另一個網關獲知的，並且資訊到達更新消息的外部部分，則網路將被標籤為外部。思科的實施還允許系統管理員將特定網路宣告為外部網路。外部路由也稱為「候選預設路由」。 它們是到達或經過被視作合適的預設網關的路由，當沒有到達目的地的明確路由時使用。例如，在Rutgers，我們配置將Rutgers連線到我們區域網路的網關，以便它將到NSFnet主幹網路的路由標籤為外部。思科的實施方案通過選取具有最小度量的外部路由來選擇預設路由。

以下各節旨在說明圖4至圖8的某些部分。

封包路由

圖4描述了輸入資料包的整體處理。這僅用於說明術語。顯然，這不是對IP網關功能的完整描述。

此過程使用支援的協定清單以及初始化網關時輸入的介面資訊。封包處理的詳細資訊取決於封包使用的通訊協定。這一點在步驟A中確定。步驟A是圖4中由所有協定共用的唯一部分。一旦協定型別已知，則使用圖4中與協定型別相應的實現。資料包內容的詳細資訊由協定規範描述。協定規範包括：確定資料包的目的地的程式；將目的地與網關自身的地址進行比較以確定網關本身是否為目的地的程式；確定資料包是否為廣播的程式；以及確定目的地是否為指定網路的一部分的程式。這些步驟用於圖4的步驟B和C。步驟D中的測試需要搜尋路由表中列出的目標。如果路由表中存在與目的地相關的條目，並且目的地與它至少關聯了一條可用路徑，則會滿足測試要求。請注意，對於支援的每種服務型別，在此步驟和下一步中使用的目標和路徑資料將分別進行維護。因此，此步驟首先確定資料包指定的服務型別，並選擇用於此步驟和下一步驟的相應資料結構集。

如果路徑的遠端複合度量小於其複合度量，則路徑可用於步驟D和E。遠端複合度量大於其複合度量的路徑是指下一跳距離目標「更遠」的路徑，如度量所度量。這稱為「上游路徑」。 通常，人們會認為使用度量會阻止選擇上游路徑。不難看出，上游路徑永遠不是最好的路徑。但是，如果允許較大的差異，則可以使用最佳路徑以外的路徑。其中一些可能是上游。

步驟E計算要使用的路徑。不考慮其遠端複合度量不小於其複合度量的路徑。如果可以接受多個路徑，則這些路徑將採用循環交替的加權形式。使用路徑的頻率與其複合度量成反比。

接收路由更新

圖5描述了從相鄰網關接收的路由更新的處理。此類更新包含條目清單，每個條目提供單個目的地的資訊。同一目標的多個條目可在單個路由更新中發生，以適應多種型別的服務。這些條目中的每一個都單獨處理，如圖5所示。如果條目在更新的外部部分，則如果作為此過程的結果新增該條目，則將為目標設定外部標誌。

對於網關支援的每種型別的服務，必須使用與該服務型別關聯的一組目標/路徑資訊，重複圖5中描述的整個過程。如圖5最外部環路所示。每種服務必須處理一次整個路由更新。（請注意，當前的IGRP實施不支援多種型別的服務，因此實際上並未實施最外部的環路。）

在步驟A中，對路徑進行基本可接受性測試。這應該包括對目的地的合理性測試。應該拒絕不可能的(「Martian」)網路號。(如需詳細資訊，請參閱RFC 1009 和RFC 1122 。) 如果所引用的目標處

於抑制狀態（即抑制過期時間不為零且晚於當前時間），則也會拒絕更新。

在步驟B中，將搜尋路由表，看此條目是否描述了已知路徑。路由表中的路徑由與其關聯的目標、作為路徑一部分列出的下一跳、用於該路徑的輸出介面以及資訊源（更新來自的地址，實際上通常與下一跳相同）定義。 更新資料包中的條目描述其目標列在條目中的路徑，其輸出介面是更新傳入的介面，其下一跳和資訊源是傳送更新的網關（「源」）的地址。

在步驟H和步驟T中，計畫了圖7中描述的更新過程。該過程將在圖5中描述的整個過程完成後實際運行。也就是說，圖7中描述的更新過程只會發生一次，即使它在圖5中描述的處理過程中被觸發多次。此外，如果網路變化迅速，還必須採取預防措施來防止更新發佈過於頻繁。

如果更新資料包中當前條目所描述的目標已經存在於路由表中，則完成步驟K。K將從更新資料包中的資料計算的新複合度量與目標的最佳複合度量進行比較。請注意，此時不會重新計算最佳複合度量，因此，如果考慮的路徑已經在路由表中，則此測試可能會比較同一路徑的新度量與舊度量。

對於低於現有最佳複合度量的路徑，執行步驟L。這既包括比現有路徑更差的新路徑，也包括複合度量已增加的現有路徑。步驟L測試新路徑是否可接受。請注意，此測試會同時執行新路徑是否足以保留以及路由毒化的測試。為了可以接受，延遲值不能是表示無法到達目標的特殊值（對於當前IP實現，24位欄位中的所有值），並且複合度量（如圖8中所指定計算）必須是可以接受的。要確定複合度量是否可接受，請將其與到達目標的所有其他路徑的複合度量進行比較。讓我做最起碼的事。如果新路徑是< V X M ，則此路徑是可接受的，其中V是初始化網關時設定的差異。如果V = 1（自思科版本8.2起始終為真），則不能接受比現有度量更差的度量。有一個例外：如果路徑已經存在，並且是到達目標的唯一路徑，則如果度量增加不超過10%（或者如果跳數沒有增加，抑制被禁用），該路徑將被保留。

當路徑的新資訊指示複合度量將減少時，執行步驟V。比較到達目的地D的所有路徑的複合度量。在本比較中，使用了新的P複合度量，而不是路由表中顯示的度量。計算最小複合度量M。然後再次檢查到D的所有路徑。如果任何路徑的複合度量> M x V，則該路徑將被刪除。V是初始化網關時輸入的差異。（自思科8.2版起，差異永久設定為1。）

定期處理

圖6中所述的過程每秒觸發一次。它會檢查路由表中的各種計時器，檢視是否有任何計時器已過期。這些計時器如上所述。

在步驟U中，啟用圖7中所述的過程。

步驟R和步驟S是必需的，因為路由表中儲存的複合度量取決於通道佔用率，基於測量值，通道佔用率會隨時間而變化。週期性地使用通過介面的測量流量的移動平均值重新計算通道佔用。如果新計算的值與現有值不同，則必須調整涉及該介面的所有複合度量。檢查路由表中顯示的每條路徑。下一跳使用介面「I」的任何路徑都會重新計算其複合度量。這是根據等式1完成的，使用儲存在路由表中的最大值作為路徑度量的一部分，以及新計算的介面通道佔用率，作為通道佔用率。

生成更新消息

圖7描述了網關如何生成要傳送到其他網關的更新消息。為連線到網關的每個網路介面生成單獨的消息。然後，該消息將傳送到可通過介面到達的所有其他網關（步驟J）。 通常，這是通過以廣播形式傳送消息來實現的。但是，如果網路技術或協定不允許廣播，則可能需要單獨將消息傳送到每個網關。

通常，在步驟G中，通過在路由表中為每個目標新增條目來構建消息。請注意，必須使用與每種服務型別關聯的目標/路徑資料。最壞的情況是，針對每種型別的服務，在更新中都會新增一個新條目

。但是，在步驟G中將條目新增到更新消息之前，將掃描已新增的條目。如果更新消息中已存在新條目，則不會再次新增該條目。當目的地和下一跳網關相同時，新條目將複製現有的條目。

為簡單起見，虛擬碼忽略了一件事 — IGRP更新消息包含三個部分：內部、系統和外部，這意味著實際上有三個環路。第一個子網只包含要向其傳送更新的網路的子網。第二個包括未標籤為外部的所有主要網路（例如，非子網）。第三個網路包括標籤為外部的所有主要網路。

步驟E實施水準分割測試。在正常情況下，此測試對於最佳路徑通過傳送更新的同一介面的路由失敗。但是，如果更新被傳送到特定目標（例如，響應來自另一網關的IGRP請求，或作為「點對點IGRP」的一部分），水準分割只有在最佳路徑最初來自該目標（其「資訊源」與目標相同），並且其輸出介面與請求來自的介面相同時才會失敗。

計算度量資訊

圖8描述了如何從網關接收的更新消息處理度量資訊，以及如何為網關傳送的更新消息生成度量資訊。請注意，該條目基於到達目的地的一條特定路徑。如果有多條路徑通往目的地，則會選擇其複合度量最小的路徑。如果多個路徑的複合度量最小，則使用任意連線斷開規則。（對於大多數協定，這基於下一跳網關的地址。）

圖4 — 處理傳入資料包

```
Data packet arrives using interface I

A   Determine protocol used by packet

    If protocol is not supported
      then discard packet

B   If destination address matches any of gateway's addresses
    or the broadcast address
      then process packet in protocol-specific way

C   If destination is on a directly-connected network
      then send packet direct to the destination, using
      the encapsulation appropriate to the protocol and link type

D   If there are no paths to the destination in the routing
    table, or all paths are upstream
      then send protocol-specific error message and discard the packet

E   Choose the next path to use. If there are more than
    one, alternate round-robin with frequency proportional
    to inverse of composite metric.

    Get next hop from path chosen in previous step.

    Send packet to next hop, using encapsulation appropriate
    to protocol and data link type.
```

圖5 — 處理傳入路由更新

```
Routing update arrives from source S

    For each type of service supported by gateway
      Use routing data associated with this type of service

      For each destination D shown in update
```

```
A       If D is unacceptable or in holddown
          then ignore this entry and continue loop with next destination D

B       Compute metrics for path P to D via S (see Fig 8)

        If destination D is not already in the routing table
        then Begin

          Add path P to the routing table, setting last
          update times for P and D to current time.

H         Trigger an update

          Set composite metric for D and P to new composite
          metric computed in step B.

          End

        Else begin (dest. D is already in routing table)

K         Compare the new composite metric for P with best
          existing metric for D.

           New > old:

L            If D is shown as unreachable in the update,
             or holddowns are enabled and
              the new composite metric >
                (the existing metric for D) * V
                [use 1.1 instead of V if V = 1,
                as it is as of Cisco release 8.2]
O            or holddowns are disabled and
             P has a new hop count > old hop count
             then Begin

              Remove P from routing table if present

              If P was the last route to D
                then Unless holddowns are disabled
                    Set holddown time for D to
                     current time + holddown time
T                  and Trigger an update

              End

             else Begin

              Compute new best composite metric for D

              Put the new metric information into the
              entry for P in the routing table

              Add path P to the routing table if it
              was not present.

              Set last update times for P and D to
              current time.

              End

           New <= OLD:

V            Set composite metric for D and P to new
```

```
              composite metric computed in step B.

              If any other paths to D are now outside the
              variance, remove them.

              Put the new metric information into the
              entry for P in the routing table

              Set last update times for P and D to
              current time.

            End

          End of for

        End of for
```

圖6 — 定期處理

```
Process is activated by regular clock, e.g. once per second

    For each path P in the routing table (except directly
    connected interfaces)

      If current time < P'S LAST UPDATE TIME + INVALID TIME
        THEN CONTINUE WITH THE NEXT PATH P

      Remove P from routing table

      If P was the last route to D
        then Set metric for D to inaccessible
          Unless holddowns are disabled,
            Start holddown timer for D and
          Trigger an update

        else Recompute the best metric for D

      End of for

    For each destination D in the routing table

      If D's metric is inaccessible
        then Begin

        Clear all paths to D

        If current time >= D's last update time + flush time
          then Remove entry for D

        End

      End of for

    For each network interface I attached to the gateway

R     Recompute channel occupancy and error rate

S     If channel occupancy or error rate has changed,
        then recompute metrics

      End of for

    At intervals of broadcast time
```

```
U     Trigger update
```

圖7 — 生成更新

```
Process is caused by "trigger update"

    For each network interface I attached to the gateway

      Create empty update message

      For each type of service S supported

        Use path/destination data for S

        For each destination D

E         If any paths to D have a next hop reached through I
            then continue with the next destination

          If any paths to D with minimal composite metric are
          already in the update message
            then continue with the next destination

G         Create an entry for D in the update message, using
          metric information from a path with minimal
          composite metric (see Fig. 8)

          End of for

        End of for

J     If there are any entries in the update message
       then send it out interface I

      End of for
```

圖8 — 度量計算的詳細資訊

本節介紹從到達路由更新計算度量和跳數的過程。此函式的輸入是路由更新資料包中特定目標的條目。輸出是可用於計算合成度量的度量向量以及跳數。如果將此路徑新增到路由表中，則在表中輸入整個度量向量。下列定義中使用的介面引數是當網關初始化時為路由更新到達的介面設定的引數，但通道佔用率和可靠性基於經過介面的測量流量的移動平均值。

- 延遲=來自資料包的延遲+介面拓撲延遲
- 頻寬=最大（來自資料包的頻寬、介面頻寬）
- 可靠性=最小（資料包可靠性、介面可靠性）
- 通道佔用率=最大值（資料包的通道佔用率、介面通道佔用率）(Max用於頻寬，因為頻寬度量是以逆形式儲存的。從概念上講，我們需要最低頻寬。) 請注意，必須儲存來自資料包的原始通道佔用率，因為每當介面通道佔用率發生變化時，將需要重新計算有效的通道佔用率。

以下內容不是度量向量的一部分，而是作為路徑的特徵保留在路由表中：

- 跳數=來自資料包的跳數。
- MTU = min（來自資料包的MTU，介面MTU）。
- 遠端複合度量=使用資料包的度量值根據公式1計算。也就是說，度量元件是來自資料包的元件，不會按如上所示進行更新。顯然，必須在進行上述調整之前計算此值。
- 複合度量=使用本節所述的度量值由等式1計算。

本節的其餘部分介紹了計算要傳送的路由更新的度量和跳數的過程。

此函式確定要放入傳出更新資料包的度量資訊和跳數。如果存在任何可用路徑，則它基於到目的地的特定路徑。如果沒有路徑，或者路徑都是上游路徑，則目標稱為「不可訪問」。

```
If destination is inaccessible, this is indicated by using a specific
        value in the delay field. This value is chosen to be larger
        than the largest valid delay. For the IP implementation this is
        all ones in a 24-bit field.

   If destination is directly reachable through one of the interfaces, use
        the delay, bandwidth, reliability, and channel occupancy of the
        interface. Set hop count to 0.

   Otherwise, use the vector of metrics associated with the path in the
        routing table. Add one to the hop count from the path in the
        routing table.
```

IP實施的詳細資訊

本節簡要介紹Cisco IGRP使用的資料包格式。使用IP資料包和IP協定9(IGP)傳送IGRP。 封包以標頭開頭。它會在IP報頭之後立即啟動。

```
unsigned version: 4;  /* protocol version number */
    unsigned opcode: 4;   /* opcode */
    uchar edition;        /* edition number */
    ushort asystem;       /* autonomous system number */
    ushort ninterior;     /* number of subnets in local net */
    ushort nsystem;       /* number of networks in AS */
    ushort nexterior;     /* number of networks outside AS */
    ushort checksum;      /* checksum of IGRP header and data */
```

對於更新消息，路由資訊緊跟在標題之後。

版本號當前為1。具有其他版本號的資料包將被忽略。

操作碼可以是1 =更新或2 =請求。

這表示消息的型別。這兩種報文型別的格式如下。

*版*本是一個序列號，當路由表發生更改時，該序列號會遞增。（在以上虛擬碼指示觸發路由更新的情況下執行此操作。）版本號使網關能夠避免處理包含它們已經看到的資訊的更新。(目前尚未執行。也就是說，版本號生成正確，但在輸入時忽略它。由於可能會丟棄資料包，因此版本號是否足以避免重複處理並不明確。有必要確保已處理與該版本關聯的所有資料包。)

*系統*是自治系統編號。在思科實施中，一個網關可以參與多個自治系統。每個此類系統運行自己的IGRP協定。從概念上講，每個自治系統都有完全獨立的路由表。從一個自治系統通過IGRP到達的路由僅在該AS的更新中傳送。此欄位允許網關選擇用於處理此消息的路由表集。如果網關收到未為其配置的AS的IGRP消息，則會忽略該消息。實際上，思科實施允許資訊從一個AS「洩露」到另一個AS。但是，我認為這是一種管理工具，而不是議定書的一部分。

Ninterior、*nsystem*和*nexterior*指示更新消息三個部分中每個部分的條目數。以上已對這些部分進行了說明。各節之間沒有其他分界。第一個內部條目被當作內部，下一個系統條目被當作系統，而最後一個外部條目作為外部。

校驗和是IP校驗和，使用與UDP校驗和相同的校驗和演算法計算。校驗和在IGRP報頭及其後的任何路由資訊上計算。計算校驗和時，校驗和欄位設定為零。校驗和不包括IP報頭，也沒有任何如

UDP和TCP中的虛擬報頭。

要求

IGRP請求要求收件人傳送其路由表。請求消息只有一個標題。僅使用version、opcode和system欄位。所有其他欄位為零。接收方應該向請求方傳送正常的IGRP更新消息。

更新

IGRP更新消息包含一個報頭，後面緊跟路由條目。1500位元組資料包（包括IP標頭）中包含的路由專案數與包含的數量相若。 使用當前結構宣告時，最多允許104個條目。如果需要更多條目，將傳送多個更新消息。由於更新消息只是逐條處理條目，因此使用單個分段消息而不是幾個獨立的消息沒有好處。

以下是路由條目的結構：

```
uchar number[3];       /* 3 significant octets of IP address */
    uchar delay[3];        /* delay, in tens of microseconds */
    uchar bandwidth[3];    /* bandwidth, in units of 1 Kbit/sec */
    uchar mtu[2];          /* MTU, in octets */
    uchar reliability;     /* percent packets successfully tx/rx */
    uchar load;            /* percent of channel occupied */
    uchar hopcount;        /* hop count */
```

uchar[2]和uchar[3]定義的欄位只是普通IP網路順序中的16位和24位二進位制整數。

數字定義所描述的目標。它是IP地址。為了節省空間，只給出IP地址的前3個位元組，內部部分除外。在interior部分中給出了最後3個位元組。對於系統和外部路由，不可能存在子網，因此低位位元組始終為零。內部路由始終是已知網路的子網，因此提供該網路編號的第一個位元組。

延遲單位為10微秒。這給出10微秒到168秒的範圍，似乎已足夠。所有延遲都表示網路無法連線。

頻寬是以1.0e10的倍數為單位的每秒位數的反向頻寬。範圍從1200 BPS線路到10 Gbps。(即，如果頻寬為N Kbps，則使用的數字為10000000 / N。)

MTU以位元組為單位。

可靠性為255的分數，即255為100%。

負載以255的分數給出。

跳數是一個簡單的計數。

由於用於頻寬和延遲的單元有些奇怪，因此有些示例看起來很正常。這些是幾種常用介質的預設值。

	Delay	Bandwidth
Satellite	200,000 (2 sec)	20 (500 Mbit)
Ethernet	100 (1 ms)	1,000
1.544 Mbit	2000 (20 ms)	6,476
64 Kbit	2000	156,250
56 Kbit	2000	178,571

```
      10 Kbit            2000              1,000,000
      1 Kbit             2000             10,000,000
```

度量計算

以下說明在Cisco 8.0(3)版中實際計算複合指標的方式。

```
metric = [K1*bandwidth + (K2*bandwidth)/(256 - load) + K3*delay] *
                        [K5/(reliability + K4)]

    If K5 == 0, the reliability term is not included.

    The default version of IGRP has K1 == K3 == 1, K2 == K4 == K5 == 0
```

相關資訊

- IP 路由支援頁面
- IGRP支援頁
- 技術支援 - Cisco Systems