# IGRP简介

## Contents



## Introduction

本技术文档简要介绍了内部网关路由选择协议（IGRP）。本文档有两个目的。第一个目的是向那些对使用、评估、实施IGRP技术的读者提供该技术概要。第二个目的是更广泛地探讨IGRP中所蕴含的一些有趣的想法。请参考“配置 IGRP”、“Cisco IGRP 实施”和“IGRP 命令”以了解有关如何配置 IGRP 的信息。

## IGRP的目标

IGRP协议允许一定数量的网关协调他们的路由。其目标下列：

- 稳定的路由甚而在非常大或复杂网络。路由循环不应该出现，既使临时。
- 对变化的快速的回应在网络拓扑上。
- 低开销。即IGRP不应该使用更多带宽比什么为其任务实际上是需要的。
- 在几并行路由中的分割数据流，当他们是大致相等的中意。
- 考虑到数据流的错误率和级别在不同的路径的。

IGRP的当前实施处理TCP/IP的路由。然而，基本设计打算能处理各种各样的协议。

工具不解决所有路由问题。按常规路由问题分成几个部分。协议例如IGRP称为“内部网关协议”(IGP)。他们供在一套网络内的使用使用，在单个管理或严密被协调的管理下。这样套网络由“外部网关协议”连接(EGP)。IGP设计记录关于网络拓扑的很多详细资料。在设计IGP的优先级在快速生产最佳路由和回应被设定更改。EGP打算保护一个网络系统以防止错误或由其他系统的故意误传，BGP是一这样外部网关规约。在设计EGP的优先级在稳定性和管理控制。通常生产一个合理的路由，而不是最佳路由EGP是满足的。

IGRP有一些相似性对更旧的协议例如Xerox的路由信息协议，伯克利的RIP和Dave磨房的Hello。它与这些协议有所不同主要在更大和更多复杂网络的设计。请参阅与RIP的比较部分关于一个更加详细的与RIP的比较，是最用途广泛协议的更旧的生成。

类似这些更旧的协议， IGRP是距离矢量协议。在这样协议，网关仅交换路由信息与邻接网关。此路由信息包含信息汇总关于网络的其余的。可以数学上显示同时地采取的所有网关由对一种分布式算法的什么总数解决一个优化问题。每个网关只需要解决一部分的问题，并且必须只接受总数据的部分。

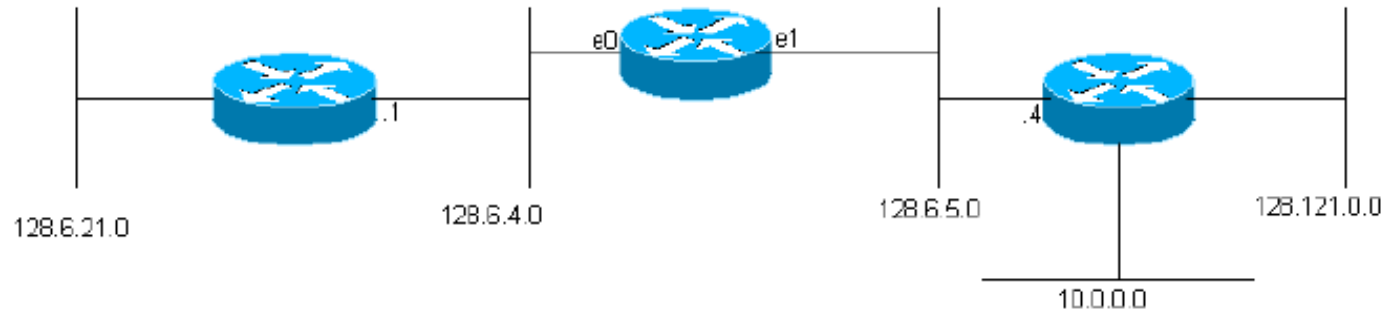
对IGRP的专业选择是改进的IGRP (EIGRP)和指SPF算法组(最短路径优先)。OSPF使用此概念。要得知更多OSPF请参见OSPF设计指南。OSPF这些是根据泛滥技术，每个网关保持最新状态关于每个接口的状况在其他网关的。使用数据为整个网络，每个网关独立地解决优化问题从其观点。有优点对每方法。在某些情况下SPF可能能回应对迅速更改。为了防止路由循环， IGRP必须在某些种类更改以后几分钟忽略新的数据。由于SPF有信息直接地从每个网关，能避免这些路由循环。因而它在最新信息能立即操作。然而， SPF比IGRP必须处理充分地更多数据，在内部数据结构和在网关之间的消息。

## 路由问题

IGRP供在连接几网络的网关的使用使用。我们假设，网络使用基于信息包的技术。实际上网关作为分组交换机。当系统被连接到一网络要发送信息包到在不同的网络时的一个系统，寄信息包到网关。如果目的地在其中一网络被连接到网关，网关将转发信息包到目的地。如果目的地是更加遥远的，网关将转发信息包到是离目的地较近的另一个网关。网关帮助他们的使用路由表决定如何处理信息包。这是简单的示例路由表。(用于示例的地址是从路特葛斯大学采取的IP地址。注意基本的路由问题为其他协议是类似的，但是此说明假设， IGRP使用路由IP。)

**图 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
```



(实际IGRP路由表有每个网关的其他信息，因为我们将看到。)此网关被连接到两个以太网，被呼叫0和1。产生了他们IP网络号(实际上子网编号) 128.6.4和128.6.5。通过使用适当的以太网接口，因而为这些特定网络寻址的信息包可以被发送直接地到目的地，完全。有两附近的网关、128.6.4.1和128.6.5.4。网络的信息包除128.6.4和128.6.5之外将转发到之一或那些网关其他。路由表指示应该用于哪个网关网络。例如，应该转发信息包被寄到在网络10的一台主机到网关128.6.5.4。一个人希望此网关是离网络的10最佳路径通过此网关的网络10较近，即。IGRP的主要目的是允许网关构件和维护象这样的路由表。

## IGRP小结

如上所述， IGRP是允许网关通过交换信息加强他们的路由表与其他网关的协议。网关从直接地被连接到它的所有的条目出发网络。它通过交换路由更新获得关于其他网络的信息与邻接网关。最简单的情况，网关将查找表示最佳方法达到每网络的一条路径。路径描绘的是为信息包应该发送的下个网关，应该使用的网络接口和度量信息。度量信息是分析的一组数字多么好路径是。这允许网关比较从多种网关听到了的路径和决定哪个使用。经常有有意义分裂两个或多个路径之间的数据流的案件。IGRP将执行此，每当两个或多个路径是同样好的。当路径是几乎同样好的时，用户能也配置它分裂数据流。在这种情况下更多数据流沿有更好的权值的路径将被发送。目的是数据流可以被分裂在一条9600 bps线路和19200 BPS线路之间，并且第19200行将大致两倍获得同等数量数据流象9600 BPS线路。

IGRP使用的权值包括以下：

- 拓扑延迟时间
- 路径的最缩小的带宽分段的带宽
- 路径的信道占用
- 路径的可靠性

拓扑延迟时间是它将采取有沿该路径的目的地的时间，假设转存的网络。当然，当网络被装载时，有另外的延迟。然而，通过使用信道占用形象，负荷占，不通过尝试测量实际延迟。路径带宽是低速连接的以每秒位计的带宽在路径的。信道占用指示多少该带宽正在使用中。它被测量和随负荷改变。可靠性指示当前错误率。它是到达未损坏的目的地信息包的部分。它被测量。

作为权值一部分，虽然他们没有使用，两个添加信息通过与它：跳次计数和MTU。跳次计数是信息包将必须经历达到目的地网关的数量。MTU是可以沿整个路径被发送，不用分段的最大信息包大小。(即它是所有网络MTU的最小数量在路径涉及的。)

凭度量信息，单个“综合度量值”为路径被计算。综合度量值结合多种度量构成的效果到单数表示“善良”该路径。它是实际上使用决定最佳路径的综合度量值。

周期地每个网关对所有邻接网关播放其整个路由表(当一些检察由于水平分割规则)。当网关从另一个网关时获得此广播，表与其现有的表比较。所有新的目的地和路径被添加到网关的路由表。在广播的路径与现有路径比较。如果一条新的路径是更好的，可能替换现有的一个。在广播的信息也用于更新信道占用率和其他信息关于现有路径。此常规手续类似于所有距离矢量协议使用的那。它在数学文件指Bellman-Ford算法。参考 基本过程的详细的发展的RFC 1058，描述RIP，一个更旧的距离矢量协议。

在IGRP中，一般Bellman-Ford算法在三个重要方面被修改。首先，而不是简单的权值，度量矢量用于分析路径。其次，而不是选择有最小的权值的单个路径，数据流在几条路径中被分裂，权值落入指定的范围。第三，介绍几个功能提供在拓扑更改的情况的稳定性。

最佳路径根据一个综合度量值选择：

```
[(K1 / Be) + (K2 * Dc)] r
```
那里K1， K2 =常数， =转存的路径带宽x (1 -信道占用)， Dc =拓扑延迟和r =可靠性。

有的路径最小的综合度量值将是最佳路径。那里有多条路径对同一个目的地，网关能路由在超过一条路径的信息包。这执行符合每数据路径的综合度量值。例如，如果一条路径有一个综合度量值1，并且另一条路径有一个综合度量值3，三次许多个信息包在有的数据路径将被发送综合度量值1。

有两个优点对使用度量矢量信息。第一是提供能力支持从同一个数据集的多样的服务类型。第二个优点是被改进的准确性。当使用时单个度量，通常对待，好象它延迟。在路径的每条链路被添加到总度量值。如果有与低带宽的一条链路，由大延迟通常表示。然而，带宽限制确实不累积延迟的方式。通过带宽把单独的组件看作，它可以正确地被处理。同样地，负荷可以由单独的信道占用率编号处理。

IGRP为互联能稳定处理一一般图形拓扑包括循环的计算机网络提供一个系统。系统维护完整路径度量信息，即，称作路径参数对所有网关被连接的所以其他网络。数据流可以在并行路径被分发，并且多条路径参数可以在整个网络同时被计算。

## 与RIP的比较

此部分IGRP与RIP比较。因为RIP广泛使用目的类似于IGRP，此比较是有用的。然而，执行此不是完全公平的。RIP未打算达到所有目标和IGRP一样。RIP供在小的网络的使用使用与相当一致的技术。在这样应用程序它是通常适当的。

IGRP和RIP之间的多数基本区别是他们的权值结构。不幸地这不是可能被更新到RIP的更改。它要求新的算法和数据结构当前在IGRP。

RIP使用简单的“跳次计数”权值描述网络。不同于IGRP，每条路径是由延迟、带宽等等描述的，在RIP它由从1的一个编号描述到15。通常此编号用于表示多少个网关路径在达到经历目的地前。这意味着差异没有被做在慢速串行线路和以太网之间。在RIP的一些实施，指定系统管理员是可能的应该不止一次计数一次特定跳跃。低速网络可以由一个大跳次计数表示。但是，因为最大数量是15，这不可能执行。即，如果以太网由1和由3的一条56Kb线路表示，可以有至多在路径的5条56Kb线路，或者最多15被超出。为了表示全方位可用的网络速度和允许一个大型网络， Cisco完成的研究建议24位权值是需要的。如果最大度量是太小的，系统管理员看到一个令人不快的选择：或者他不能区分之间快速和慢的路由，或者他不能适合他的整个网络到限制。实际上RIP不能处理他们的一定数量的全国性网络当前足够大，即使每次跳跃只一次计数。RIP不可能用于这样网络。

明显的回应是修改RIP允许更大的权值。不幸地，这不会工作。类似所有距离矢量协议， RIP有“计数的问题对无限”。这在RFC 1058较详细地描述 。当，寄生路由将引入拓扑更改。与这些寄生路由产生关联的权值缓慢增加，直到他们到达15，到时去除路由。15此进程相当迅速将聚合的一足够小最大，假设，使用触发更新。如果修改RIP允许24位权值，循环将仍然存在太久为了权值能将计数至2**24。这不是能忍受的。IGRP有设计的功能防止寄生路由介绍。这些在第5.2部分如下讨论。它不是实用的处理复杂网络不介绍这样功能或变成一个协议例如SPF。

IGRP执行有点更多比增加允许的权值的范围。它调整权值描述延迟、带宽、可靠性和负荷。表示在一单个度量的这样考虑例如裂口， IGRP采取的方法是潜在更加准确的然而是可能的。例如，与单个度量，几条连续的快速的链路将看来是等同的与单个减慢一。这可能是交互式数据流的论点，延迟是最关心。然而，对于批量数据传输，最关心是带宽，并且添加权值一起不在正确的方法那里。IGRP分开处理延迟和带宽，累积延迟，但是采取带宽的最小数量。发现如何合并可靠性和负荷的作用到单组件权值里是不容易的。

以我所见，其中一个IGRP的大优点是配置方便。它能直接地表示有实际含义的数量。这意味着可以根据接口类型自动地设置，线路速度等等。使用单组件权值，权值是可能必须“被烹调”合并几件不同的事的作用。

其他创新是更多算法和数据结构问题比路由协议。例如， IGRP指定支持在几个路由中的分割数据流的算法和数据结构。设计执行此RIP的实施是确实可能的。然而，一旦路由再实施的，没有理由停留与RIP。

到目前为止我描述了“通用的IGRP”，可能支持所有网络协议的路由的技术。然而，在此部分它值得提及有点更多关于特定TCP/IP实施。那是与RIP比较的实施。

RIP更新消息包含路由表的快照。即他们有一定数量的目的地和度量值和少许。IGRP的IP实施有另外的结构。首先，更新消息是由“自控系统号确定的”。此术语从Arpanet传统出来，并且有特定意味着那里。然而，对于多数网络什么意味着是您能运行在同一网络的几个不同的路由系统。这为从几组织的网络会聚的地方是有用的。每个组织能维护其自己的路由。由于每次更新被标记，可以配置网关注意仅正确一个。配置某些网关从几自控系统接收更新。他们以受控方式通过信息在系统之间。注意这不是完整的解决方案对路由安全性的问题。可以配置所有网关听从任何自控系统的更新。然而，它仍然是在实现一个合理的程度在网络管理员之间的信任的路由策略的非常有用的工具。

关于IGRP更新消息的第二个结构上的功能影响默认路由由IGRP处理的方式。多数路由协议有默认路由的概念。它经常不是实用的为了路由更新能列出每网络在世界上。典型地一套网关需要选派了网络的路由信息在他们的组织内。目的地的所有数据流他们的组织的外部可以被发送到一些边界网关之一。那些边界网关可能有完全信息。路由到最佳的边界网关是“默认路由”。它是默认值，也就是说用于达到在内部路由更新不特别地列出的所有目的地。RIP和一些其他路由协议，流通关于默认路由的信息，好象它一个真实的网络。IGRP采取一不同的方法。而不是默认路由的单个假条目，IGRP允许真实的网络被标记作为为是的候选默认值。这通过安置关于那些网络的信息实现在更新消息的一个特殊外部部分。然而，不妨被重视如启用有点产生关联与那些网络。周期地IGRP扫描所有候选默认路由并且选择那个与最低权值作为实际默认路由。

潜在地对默认值的此方法比多数RIP实施采取的方法稍微灵活。可以最典型设置RIP网关生成与有些指定的权值的默认路由。目的是这将执行在边界网关。

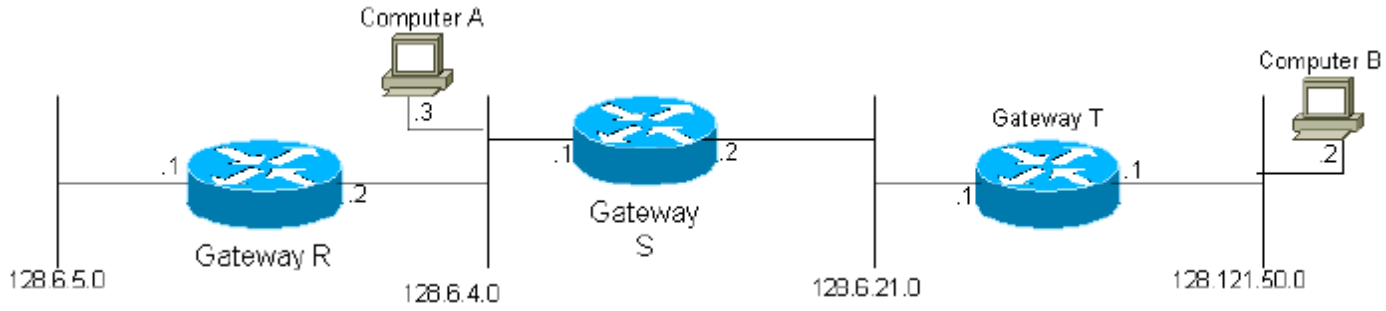
# 详细规格说明

此部分提供IGRP的一个详细规格说明。

## 整体说明

当网关首先启动时，其路由表初始化。这可能完成由从控制台终端的运算符，或者由读的信息从配置文件。每网络的说明被连接到网关提供，包括沿链路的拓扑延迟(例如，多长时间需要一位对横向链路)和链路的带宽。

**图 2**




例如，在以上图表，网关S被通知被连接到网络2和3通过对应接口。因此，最初，网关2仅知道能到达在网络2和3.的所有目的地计算机。所有网关被编程周期地传达给他们的相邻网关从其他网关收集的信息他们初始化了与，以及信息。因此，网关S从网关R和T将接收更新并且获悉能通过网关T.到达在网络1通过网关R的在网络4的计算机和计算机。因为网关S发送其整个路由表，在下个循环网关T获悉能达到网络1通过网关S。发现是容易的关于每网络的信息在系统最终将到达在系统的每个网关，提供只网络完全连接。

**图 3**

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

每个网关计算一个综合度量值确定数据路径的中意到目的地计算机。例如，在以上图表，在网络6的一个目的地的，网关A (千兆瓦A)通过网关B和C将计算两条路径的度量功能。注意路径是由下一跳定义的。实际上有三个可能的路由从A到网络6 ：

- 处理对B
- 对C然后对B
- 对C然后对D

然而，网关A不需要选择在介入C的两个路由之间。在A的路由表有代表路径的单个条目对C。其权值表示最佳方法有从C最终目的地。如果A发送一个信息包到C，是否的是至C要决定使用B或D。

**式1**

为每数据路径计算的综合度量值功能是如下所示：

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

那里r =小部分可靠性(成功接受在下一跳)发射的%， Dc =复合延迟，是=有效带宽：卸载带宽x (1 -信道占用)和K1和K2 =常数。

**式2**

原则上复合延迟， Dc，能确定如下所示：

```
Dc = Ds + Dcir + Dt
```
那里Ds =交换的延迟、Dcir =电路延迟(1位的传播延迟)和DT =传输延迟(一个1500位消息的无载延迟)。

然而，一个标准延迟数实践上使用每种网络类型技术。例如，将有一个标准延迟数以太网的和串行线路的以任何特定的比特率。

这是示例网关A的路由表如何也许查找一旦网络6以上图表。(请注意度量矢量的独立组件没有显示，简而言之。)

**路由表示例：**

| 网络 | 接口 | 下个网关 | 量度 |
|---|---|---|---|
| 1 | NW 1 | 无 | 直接地连接 |
| 2 | NW 2 | 无 | 直接地连接 |
| 3 | NW 3 | 无 | 直接地连接 |
| 4 | NW 2 | C | 1270 |
| | NW 3 | B | 1180 |
| 5 | NW 2 | C | 1270 |
| | NW 3 | B | 2130 |
| 6 | NW 2 | C | 2040 |
| | NW 3 | B | 1180 |

加强一张路由表基本流程通过交换信息与相邻是由Bellman-Ford算法描述的。算法用于更早的协议例如RIP (RFC 1058)。为了处理更多复杂网络， IGRP添加三个功能到基本的Bellman-Ford算法：

1. 而不是简单的权值，度量矢量用于分析路径。单个综合度量值可以从此向量被计算根据式1，上述。使用向量允许网关适应不同的服务类型，通过使用在式1.的几个不同的系数。它比单个度量也允许网络的特性的更多准确表示。
2. 而不是选择有最小的权值的单个路径，数据流在有落入指定的范围的权值的几条路径中被分裂。比所有单个路由允许几个路由平行使用这，提供更加巨大的有效带宽。差异v由网络管理员指定。有最小的综合度量值的M所有路径保持。另外，权值是较少的所有路径比V x M保持。数据流在相反比例的多条路径中被分发对综合度量值。
3. 有差异的此概念的一些问题。产生利用极大差异值比1的策略是难的和也不导致信息包循环。在Cisco版本8.2，差异功能不是被实施的。(我不是肯定的在什么版本去除了功能。)此的效果是永久性设置差异到1。
4. 介绍几个功能提供在拓扑更改的情况的稳定性。这些功能打算防止路由循环和“计数对无限”，分析了早先尝试使用Ford型算法此种应用程序。主要的稳定性功能是“抑制”， “触发更新”，“分裂了展望期”，和“毒害”。这些如下较详细地讨论。

数据流分裂(点2)提高相当细微的危险。差异v设计允许网关使用不同的速度并行路径。例如，也许有运行与19200 BPS线路平行的9600 BPS线路，冗余的。如果差异v是1，只有将使用最佳路径。不会因此9600 BPS线路，如果19200 BPS线路有一种合理的可靠性，将使用。(然而，如果几条路径是相同的，负荷在他们将被共享。)通过提高差异，我们能允许数据流被分裂在最佳路由和其他路由之间是接近如好。以足够大差异，数据流将被分裂在两条线路之间。危险是那足够大差异，不是仅更慢的路径变得准许，但是实际上“在错误方向”。因而应该有防止数据流的额外的规则被发送“上行”：数据流没有沿远程合成度量值的路径被发送(综合度量值被计算在下一跳)比综合度量值极大被计算在网关。在一般系统管理员鼓励不设置在1上的差异除了在特定的情况下需要使用的地方并行路径。在这种情况下，仔细设置差异提供“权利”结果。

IGRP打算处理多样的“服务类型”，和多个协议。服务类型是在修改方式路径将被评估的数据包的一个规格。例如， TCP/IP协议允许信息包指定高带宽、低延迟或者高可靠性相对重要性。通常，交互式应用程序将指定低延迟，而批量转发应用程序将指定高带宽。这些需求确定是适当的用于Eq的相对值K1和K2。1.规格的每个组合在将支持的信息包的指" type of service "。对于每种服务类型，必须选择一套参数K1和K2。路由表为每种服务类型保持。因为路径根据Eq，定义的综合度量值选择并且被定购这执行。1.这为每种服务类型是不同的。从所有的信息这些路由表被结合生成网关交换的路由更新消息，正如Figure7所描述。

## 稳定性功能

此部分描述抑制、触发更新、分开的展望期和毒化。这些功能设计防止网关拾起错误的路由。正如RFC 1058所描述 ，当路由变得不可用，由于网关或网络时的故障这能发生。原则上，邻接网关发现故障。他们然后发送显示旧路由如不可用的路由更新。然而，根本不到达网络的一些部分，或者被延迟更新是可能的在到达某些网关。仍然相信的网关旧路由是好能持续传播该信息，因而重新输入失败的路由到系统。最终此信息通过网络将传播并且来到再注入它的网关。结果是循环路由。

实际上有在对抗措施中的若干冗余。原则上，抑制和触发更新应该是满足防止错误的路由首先。然而，实践上，多种种类的通信故障能造成他们是不足的。无论如何分开的展望期和路由毒抑打算防止路由循环。

通常，新的路由表经常被发送到相邻网关(默认情况下每90秒，虽然这可以由系统管理员调整)。触发更新是立即发送的一张新的路由表，以回应若干更改。最重要的更改是路由的删除。这能发生，因为超时到期了(很可能一条相邻网关或线路断开了)，或者，因为从下个网关的一个更新消息在路径表示，路径不再是可用的。当网关G发现时路由不再是可用的，立即触发更新。此更新将显示该路由如不可用。请考虑发生了什么，当此更新到达相邻网关。如果邻居的路由指向了回到G，相邻必须去除路由。这造成相邻触发更新等等。因而故障将触发一系列的更新消息。此通知将传播在路由通过失败的网关或网络网络中的该部分。

触发更新是满足的，如果我们可能保证更新通知立即到达了每个适当的网关。然而，有两个问题。首先，包含更新消息的信息包可以由在网络的某条链路丢弃或毁损。其次，触发更新不瞬间地发生。很可能，未得到触发更新的网关在已经得到了触发更新的相邻在错误时间将发布一次定期更新，造成坏路由被再插入。抑制设计避过这些问题。抑制规则说，当去除时路由，新的路由不会为某段时期的同一个目的地接受。这提供触发更新时刻达到其他网关，因此我们可以肯定我们获得的任何新的路由不是再插入老一个的仅一些网关。抑制周期必须是足够长期允许触发更新通知去在网络中。另外，它应该包括两三个正常广播循环，处理丢弃的数据包。请考虑发生了什么，如果其中一次触发更新被丢弃或毁损。发布该更新的网关将发布另一次更新在下次定期更新。这将重新启动触发更新通知在错过最初的通知的相邻。

触发更新和抑制的组合应该是满足摆脱过期路由和防止他们被再插入。然而，一些另外的预防措施值得无论如何执行。他们允许非常损耗变得分成的网络和网络。要求由IGRP另外的预防措施是分开的展望期和路由毒抑。分开的展望期从在方向从未有道理送回路由来自的观察出现。考虑以下情况：

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

网关A将告诉B有一个路由对网络1。当B发送更新到A时，从未有它的所有原因提及网络1。因为A是离1较近，没有理由它考虑去通过B。水平分割规则说应该为每相邻(实际上每相邻的网络)生成一个分开的更新消息。为特定相邻的更新应该省略指向该相邻的路由。此规则防止在邻接网关之间的循环。即请假设对网络1的A的接口发生故障。没有水平分割规则， B是告诉A能达到1。因为它不再有一个实际路由， A也许拾起该路由。在这种情况下， A和B两个将有路由到1。当然，但是A将指向B和B将指向A.触发更新，并且抑制应该防止其发生。但是，因为没有理由送回信息到地方它来自

，分开的展望期值得无论如何执行。除其在防止循环的作用之外，分开的展望期控制更新消息的大小。

分开的展望期应该防止在邻接网关之间的循环。路由毒抑打算中断更大的循环。规则是，当更新显示现有的路由的权值能充分时地增加了，有循环。应该去除路由和放到抑制。目前规则是去除路由，如果综合度量值比要素增加更多1.1。因为小的量度的更改能发生由于在信道占用或可靠性上的变化触发路由的删除在综合度量值的所有增量是不安全的。因此要素1.1是启发式的。确切值不是重要。因为小那些将由触发更新和抑制，防止我们盼望此规则只必要中断非常大循环。

## 功能失效抑制

自版本8.2，思科的代码提供一个选项禁用抑制。抑制的缺点是他们延迟一个新的路由的采用，当旧路由发生故障时。使用默认参数，在路由器在更改以后前，采用一个新的路由它能花费几分钟。然而，由于如上所述的原因，去除抑制是不安全的。结果是计数到无穷大，正如RFC 1058所描述。我们臆想，但是不能证明，与路由毒抑的一个更加严格的版本，抑制不再必要终止计数到无穷大。因而禁用抑制enable (event)路由毒抑的此更加严格的表。注意已分解展望期和触发更新实际上仍然是。

路由毒抑的更加严格的表根据跳次计数。如果路径的跳次计数增加，去除路由。这将明显地去除是有效的路由。如果在别处某事在网络更改，以便路径当前还通过一个网关，跳次计数将增加。在这种情况下，路由是有效的。然而，没有十分安全的方式与路由循环(计数到无穷大区分此案件)。因而最安全的方法将去除路由，每当跳次计数增加。如果路由合法，将由下一次更新重新安装，并且那将导致在系统在别处将重新安装路由的一次触发更新。

一般来说，距离矢量algorithms1容易采用新的路由。问题从系统完全地净化老那些。因而是非常激进的关于去除可疑路由的规则应该是安全的。

## 更新进程的详细资料

在图描述的一组流程4到8打算处理单个网络协议，例如， TCP/IP、DECNet或者ISO/OSI协议。然而，协议详细资料为TCP/IP将仅被给予。单个网关可能处理跟随超过一个协议的数据。由于每个协议有不同的寻址结构和信息包格式，用于的计算机编码实现图4到8通常为每个协议将是不同的。在图描述的进程4将变化多数，正如图4.的详细的附注所描述。在图描述的进程5到8将有同一个一般结构。主要的区别从协议到协议将是路由更新信息包的格式，必须设计是与一个特定协议兼容。

注意目的地的定义可能从协议变化到协议。被描述的方法这里可以用于路由对单个主机，对网络，或者更加复杂的分层的地址方案的。使用路由的哪种类型将取决于协议的寻址结构。当前TCP/IP实施支持只路由对IP网络。因而“目的地”确实意味着IP网络或子网号码。子网信息为连接的网络只被保存。

图4到7显示网关使用的路由进程的多种部分的伪代码。在程序的开始，可接受的描述每个接口的协议和参数被输入。

网关只将处理是列出的某些协议。从一个系统的所有通信使用一个协议不关于列表将被忽略。数据输入下列：

- 网关被连接的网络。
- 卸载带宽每网络。
- 每网络拓扑延迟。
- 每网络的可靠性。
- 每网络信道占用。

- 每网络MTU。

每数据路径的度量功能根据式1.然后被计算。注意前三个项目是相当持久的。他们是基础网络技术的功能和不取决于负荷。他们能设置从配置文件或由直接操作员输入。注意IGRP不使用可测量的延迟。理论和经验建议为使用可测量的延迟维护稳定的路由的协议是非常困难的。有两个被测量的参数：可靠性和信道占用。可靠性根据网络接口硬件或固件报告的错误率。

另外这些输入，路由算法为几个路由参数要求值。这包括计时器值，差异，并且抑制是否是启用的。这将由配置文件或操作员输入通常指定。(自Cisco版本8.2，差异永久设置到1.)

一旦初始信息输入，在网关的操作由计时器的事件—数据包的到达一致网络接口或者到期触发。在图描述的进程4到7被触发如下：

- 当信息包到达时，根据图4.被处理。这导致为进一步处理被派出另一个接口，丢弃或者接受的信息包。
- 当信息包由进一步处理的时网关接受，在此规格没描述的一个协议特殊化方式被分析。如果信息包是路由更新，根据图5.被处理。
- 图6显示计时器触发的事件。设置计时器产生一个中断一次每秒。当中断发生时，在图显示的进程6上被执行。
- Figure7显示路由更新子例行程序。对此子例行程序的呼叫在表5和6.显示。
- 另外，图8在表5和7.显示是指的度量计算详细资料。

有控制路由传播和到期的四个重要时间常数。这些时间常数可能由系统管理员设置。然而，有默认值。这些时间常数是：

- 广播定期的更新经常是广播由在所有连接的接口的所有网关这。默认值一次是每90秒。
- 无效定期，如果更新未为在此时间内的一条特定路径接收，考虑计时了。应该是几时间广播时间，为了允许可能性包含更新的信息包可能通过网络丢弃。默认值是3倍广播时间。
- 对负定期，当目的地成为不可得到时(或权值增加足够导致毒化)，目的地进入“抑制”。在此状态期间，新的路径不会为此时间的同一个目的地被接受。保持时间指示多久此状态应该持续。应该是几时间广播时间。DEFAULT值是3倍广播时间加上10秒。(正如Disable Holddowns部分所描述，禁用抑制。)是可能的
- 冲洗定期，如果更新未为在此时间内的一个指定的目的地接收，它的条目从路由表被去除。注意在无效的时间和通过时间之间的区别：在无效的时间之后路径被计时并且被删除。如果没有剩余的路径对目的地，目的地当前是不可得到的。然而，目的地的数据库条目依然存在。它必须保持强制执行抑制。在通过时间之后，数据库条目从表被去除。它比无效的时间应该有些长加上抑制计时。默认值是7倍广播时间。

这些图预料以下主要数据结构。另二套这些数据结构为网关支持的每个协议保持。在每个协议内，另二套数据结构保持为了能将支持的每种服务类型。

每个目的地为系统所知，有路径a (可能空)列表对目的地、抑制到期时间和一个更新时间。更新时间指示上次所有路径的此目的地在从另一个网关的一次更新包括了。注意也有保持的更新时间每条路径的。当向目的地删除时最后路径，目的地被放到抑制，除非抑制是失效的(请参阅Disable Holddowns部分欲知更多信息)。抑制到期时间指示抑制到期的时间。事实是非零表明目的地在抑制。为了保存计算，它也是一个好想法保持“最好权值”每个目的地的。这是综合度量值的最小数量所有路径的对目的地。

对于每条路径向目的地，有下一跳的地址在路径、接口将使用的，分析路径，包括拓扑延迟、带宽、可靠性和信道占用的度量矢量的。其他信息与每条路径也产生关联，包括跳次计数、MTU、信息源、远程合成度量值和从这些编号计算的一个综合度量值根据式1。也有一个最后更新时间。信息源指示该路径的多数最新更新何处来自。实际上这是相同的象下一跳的地址。更新时间是多数最新更新为此路径到达的时间。它用于到期超时路径。

注意IGRP更新消息有三个部分：内部、系统(含义“此自控系统”，但是不内部)和外部。内部部分是为路由对子网。不是所有的子网信息是包括的。一网络仅子网是包括的。这是与更新被发送的地址产生关联的网络。通常更新是在每个接口的广播，因此这是广播被发送的网络。(其他案件为对IGRP请求和点对点IGRP的回应来了。)主要网络(例如，非子网)被放到更新消息的系统部分，除非他们特别地被标记作为外部。

网络将被标记作为外部，如果从另一个网关是获知，并且信息在更新消息的外部部分到达。思科的实施也允许系统管理员宣称特定网络作为外部。外部路由也指“候选默认值”。他们是请通过或认为适当的作为默认值，将使用的网关的路由，当没有显式路由对目的地时。例如在Rutgers我们配置连接Rutgers到我们的区域网的网关，以便标记路由到NSFnet骨干网作为外部。思科的实施通过选择选择默认路由与最小的权值的外部路由。

以下部分打算澄清图4到8.的某些部分。

## 信息包路由

图4描述整体处理输入信息包。这用于澄清术语。明显地这不是IP网关完整说明。

此进程使用支持的协议列表，并且关于接口的信息进入了，当网关初始化时。信息包处理的详细资料取决于信息包使用的协议。这在步骤A. Step A确定是由所有协议共享图4的唯一的部分。一旦协议类型知道，适当对协议类型使用图4的实施。信息包内容的详细资料由协议的规格描述。协议的规格包括确定信息包的目的地方法，目的地方法与网关的自己的地址比较确定网关是否是目的地、方法确定信息包是否是广播和方法确定目的地是否是指定的网络的一部分。这些程序用于步骤B和C图4。在步骤D的测试要求在路由表里列出的目的地的搜索。测试是满足的，如果有一个条目在目的地的路由表里，并且该目的地连结与它至少一可用路径。注意目的地和路径用于在这中和下一步为支持的每种服务类型分开被维护。因而此步骤通过确定信息包指定的服务类型和选择对应的数据集结构使用开始此和下一步。

路径是可用的为步骤D和E，如果其远程合成度量值比其综合度量值是较少。远程合成度量值比其综合度量值下一跳从目的地是“去的”的路径极大的一条路径，如测量由权值。这指“上行路径”。通常一预计使用权值将防止上行路径被选择。发现是容易的上行路径不可以是最佳一个。然而，如果大差异允许，可以使用除最佳一个之外的路径。一些那些能上行。

步骤E算出路径使用。远程合成度量值比他们的综合度量值不是较少的路径没有考虑。如果超过一条路径是可接受的，这样路径用于循环叠更的一种被衡量的形式。一起使用路径的频率与是反比例的对其综合度量值。

## 路由更新的接收

图5描述从一个相邻网关接收的处理路由更新。这样更新包括条目列表，其中每一提供单个目的地信息。超过同一个目的地的一个条目在单个路由更新能发生，适应多样的服务类型。这些条目中的每一个单个被处理，正如图5.所描述。如果条目在更新的外部部分，外部标志位为目的地将设置由于此进程，如果被添加。

必须为网关支持的每种服务类型一次重复在图描述的整个过程5，使用套的位置/与那种服务产生关联的路径信息。这在最外层的环路在表5.显示。必须为每种服务类型一次处理整个路由更新。(请注意IGRP的当前实施不支持多样的服务类型，因此最外层的环路实际上不是被实施的。)

在步骤A，基本的可接受性测试在路径进行。这应该包括目的地的合理测试。应该拒绝不可能的(“火星”)网络号。(请参见RFC 1009 和RFC 1122 欲知更多信息。)更新也被拒绝，如果他们是指的目的地在抑制，即抑制到期时间晚于当前时间是非零和。

在步骤B路由表被搜索发现此条目是否描述已经知道的一条路径。一条路径在路由表里是由是关联的目的地，下一跳列出作为路径一部分，将用于路径输出接口和信息源(的地址更新来—通常实践上定义的同下一跳一样)。从更新信息包的条目描述目的地在条目列出，输出接口是接口的一条路径更新进来，并且下一跳和信息源是网关的地址发送更新(“来源” S)。

在步骤H和步骤T，安排在Figure7描述的更新进程。此进程实际上将追捕在图描述的整个过程5完成。即在Figure7描述的更新进程一次只将发生，即使在图描述中的处理被触发几次5。此外，如果网络迅速，更改必须采取预防措施保持从太经常发出的更新。

如果当前条目描述的目的地在更新信息包在路由表里，已经存在步骤K被实行。K从在更新信息包的数据计算的新的综合度量值与目的地的佳合成度量值比较。注意佳合成度量值没有此时重新计算，如此，如果考虑的路径已经在路由表里，此测试可能比较同一条路径的新和老权值。

步骤L为比现有的佳合成度量值坏的路径被执行。这包括比现有的那些坏的新的路径和综合度量值增加了的现有路径。步骤L测试新的路径是否是可接受的。注意这试验实施两个测试为一条新的路径是否是足够好保持和路由毒抑。为了是可接受的，延迟值不能是指示一个不可得到的目的地的特殊值(当前IP实施，所有部分在一个24个位域)和综合度量值(被计算在图上指定8)一定是可接受的。要确定综合度量值是否是可接受的，它与其他路径比较综合度量值与目的地。让M是这些的最小数量。新的路径是可接受的，如果是< V x M，其中V是差异SET，当网关初始化了。IF总是TRUE自CISCO版本8.2)的V = 1 (则量度的ANY BAD比现有的一个不是可接受的。有一例外对此：IF PATH已经存在并且是唯一的PATH对目的地， PATH将是保留的IF量度的HAS没增加由超过10% (或抑制是失效的地方， IF没增加的跳次计数HAS)。

第v步被实行，当路径最新信息表明时综合度量值将被减少。所有路径综合度量值向目的地D比较。和此比较起来， P的新的综合度量值使用，而不是那个出现在路由表里。最小的合成公尺M被计算。然后所有路径向D再被检查。如果，该路径取消任何path>的M x v综合度量值。当网关初始化了，v是差异，被输入。(自Cisco版本8.2，差异永久设置到1.)

## 定期处理

在图描述的进程6一次被触发一秒钟。它在路由表里检查多种计时器，发现其中任一是否到期了。这些计时器如上所述。

在步骤U，启动在Figure7描述的进程。

步骤R和步骤S根据评定是必要的，因为在路由表里存储的综合度量值取决于信道占用，随着时间的推移更改。使用一个被测数据流移动平均数通过接口，周期地信道占用被重估。如果新计算的值与现有的一个有所不同，必须调整介入该接口的所有综合度量值。在路由表里显示的每条路径被检查。下一跳使用接口“我”的所有路径有其被重估的综合度量值。这执行符合式1，作为路径的度量一部分，使用作为信道占用值的最大数量在路由表和接口的最近被计算的信道占用存储了。

## 生成更新消息

Figure7描述网关如何生成将被发送的更新消息到其他网关。一个分开的消息为每个网络接口生成附加网关。该信息然后传送到通过接口的其他网关(步骤J)是可及的。通常这由传送信息完成作为广播。然而，如果网络技术或协议不允许广播，单个传送信息到每个网关可能是必要的。

一般来说，消息通过添加每个目的地的一个条目加强在路由表里，在步骤G。注意必须使用与每种服务类型产生关联的目的地/路径数据。在最坏的情况下，一个新的条目被添加到为每个目的地的更新每种服务类型的。然而，在添加条目前到在步骤G的更新消息，已经被添加的条目被扫描。如果新的条目已经是存在更新消息，再没有被添加。当目的地和下一跳网关是相同的时，一个新的条目复制一现有的一个。

简单说来，伪代码省略一件事— IGRP更新消息有三部分：内部、系统和外部，因此意味着实际上有在目的地的三个循环。第一包括更新被发送网络仅的子网。第二包括没有被标记作为外部的所有主要网络(例如，非子网)。第三包括被标记作为外部的所有主要网络。

步骤E实现已分解展望期测试。正常情况，此测试为最佳路径出去同一个接口的路由失败更新被派出。然而，如果更新被发送到一个特定目的地(例如，以回应自另一个网关的一个IGRP请求，或者作为“点对点IGRP一部分”)，分开的展望期发生故障，只有当最佳路径最初来自该目的地(其“信息源”是相同的象目的地)，并且其输出接口是作为那个请求进来自的相同的。

## 估计度量信息

图8描述度量信息如何从网关收到的更新消息被处理，并且如何为网关被发送的更新消息生成。注意条目根据一个特定路径向目的地。如果有超过一条路径对目的地，综合度量值最低的路径被选择。如果超过一条路径有最小的合成公尺，使用一个任意线断阻规则。(对于多数协议，这根据下一跳网关的地址。)

**图4 —处理流入信息包**

```
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.
```

**图5 —处理流入路由更新**

```
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
```

**图6 —定期处理**

```
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
```

**Figure7 —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
```

**图8 —度量计算详细资料**

此部分描述计算度量值和跳次计数程序从到达的路由更新。对此功能的输入是一个特定目的地的条目在路由更新信息包。输出是可以用于计算综合度量值的度量矢量和跳次计数。如果此路径被添加到路由表，整个度量矢量在表里被输入。用于以下定义的接口参数是那些集，当网关初始化了的接口的路由更新到达，除了信道占用和可靠性根据一个被测数据流移动平均数通过接口。

- 从信息包+接口拓扑延迟的延迟=延迟
- 带宽=最大(从信息包，接口带宽的带宽)
- 可靠性=分钟(从信息包，接口可靠性的可靠性)
- 信道占用=最大(从信息包，接口信道占用的信道占用)(最大使用带宽，因为带宽度量存储以相反形式。概念上，我们想要最小带宽。)注意必须保存从信息包的原始信道占用，因为将是需要的重新计算有效信道占用，每当接口信道占用更改。

下列不作为度量矢量的部分，然而也被保留在路由表作为路径的特性：

- 跳跃count=从信息包的跳次计数。
- MTU =分钟(从信息包的MTU，接口MTU)。
- 远程合成度量值=计算从式1使用从信息包的度量值。即度量构成是那些从信息包和没有更新如上所述。明显地这，在显示的调节如上完成前，必须计算。
- 综合度量值=计算从式1使用度量值被计算正如此部分所描述。

此部分此剩下的事描述计算度量值程序和能将被发送的路由更新的跳次计数。

此功能确定将被放的度量信息和跳次计数到一个流出的更新信息包。如果有任何可用的路径，它根据一条特定路径向目的地。如果没有路径，或者路径是全部上行，目的地被称为“不可访问”。

```
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实施的详细资料

此部分briefle由Cisco IGRP描述信息包格式的。IGRP被发送使用与IP协议9 (IGP)的IP数据包。信息包从报头开始。它在IP头之后开始。

```
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 */
```

对于更新消息，路由信息在报头之后跟随。

版本号是1.有的信息包其他版本号当前被忽略。

操作码可以是1 =更新或2 =请求。

这指示消息类型。如下将产生两种消息类型的格式。

*版本*是被增加的序列号，每当有在路由表上的一个变化。(这在以上的伪代码说触发路由更新。)的那些情况执行版本号允许网关避免处理包含他们已经看见的信息的更新。(这当前没有实现。即版本号正确地生成，但是在输入被忽略。由于丢弃信息包是可能的，不很清楚版本号是满足避免复制处理。确信是必要的，与版本产生关联的所有信息包被处理了。)

*Asystem*是自控系统号。在Cisco实施，网关能参加超过一个自控系统。每个这样系统运行其自己的IGRP协议。概念上，有完全每个自控系统的分开的路由表。通过从一个自控系统的IGRP到达的路由在为该AS的更新仅被发送。此字段允许设置路由表使用处理此消息的网关选择。如果网关接受一个IGRP信息AS的没有被配置为，被忽略。实际上， Cisco实施允许信息“从一个泄漏”至于别的。然而，我看待作为而不是管理工具一部分的协议。

*Ninterior*、*nsystem*和*nexterior*指示条目的数量在更新消息的三个部分中的每一个的。这些部分如上所述。没有在部分之间的其他分界。第一个ninterior条目被采取是内部，下个nsystem条目作为是系统和最终nexterior作为外部。

校验和是IP校验和，被计算使用校验和算法和UDP校验和一样。校验和在IGRP报头和跟随它的所有路由信息被计算。当计算校验和时，检查和字段调整到零。校验和不包括IP头，亦没有所有虚拟报头正如在UDP和TCP。

## 请求

IGRP请求要求接收人发送其路由表。Request信息有仅一个报头。使用版本、操作码和仅asystem字段。其他字段是零。接收人预计传送一个正常IGRP更新消息到请求方。

## 更新

IGRP更新消息包含一个报头，立即跟随由路由条目。许多个路由条目包括和将适合到1500字节数据包(包括IP头)。使用当前结构说明，这允许104个条目。如果更多条目是需要的，传送几个更新消息。因为更新消息是被处理的条目由条目，没有优点对使用单个被分段的消息而不是几独立部分。

这是路由条目的结构：

```
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 */
```

字段定义了uchar[2]和uchar[3]是完全16个和24个位二进制整数，按正常IP网络顺序。

编号定义了被描述的目的地。它是IP地址。要节省空间， IP地址的仅前3个字节产生，除了在内部部分。在内部部分，产生前3个字节。对于系统和外部路由，子网不是可能的，因此低位字节总是零。内部路由总是一个已知网络的子网，该网络号第一个字节如此被供应。

延迟在10微秒单元。这给予10微秒到168秒的范围，似乎满足。所有部分的延迟表明网络是不可得到的。

带宽是在1.0e10要素每秒扩展的位的相反带宽。范围是从1200 BPS线路到10 Gbps。(即，如果带宽是N Kbps，使用的编号是10000000/N.)

MTU在字节。

可靠性产生作为一小部分255。即255是100%。

负荷提供作为一小部分255。

跳次计数是简单的计数。

由于用于带宽和延迟的有些奇怪的单元，一些示例按顺序似乎。这些是用于几个普通的媒体的默认值。

| | 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 |

## 度量计算

这是综合度量值在Cisco版8.0(3)实际上被计算方式的说明。

```
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
```

# Related Information

- IP 路由支持页
- IGRP支持页面
- Technical Support - Cisco Systems