IGRP 介绍

Contents

[Introduction](#)
[IGRP 的目标](#)
[路由问题](#)
[IGRP 概述](#)
[与 RIP 的比较](#)
[详细说明](#)
[总体概述](#)
[稳定性功能](#)
[禁用抑制](#)
[更新过程的详细信息](#)
[数据包路由](#)
[接收路由更新](#)
[定期处理](#)
[生成更新消息](#)
[计算度量信息](#)
[IP 实施的详细信息](#)
[请求](#)
[更新](#)
[度量计算](#)
[Related Information](#)

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 协议可供许多网关用来协调路由。其目标如下：

- 即使在非常大或复杂的网络中也能实现稳定的路由。不应该形成任何路由环路，哪怕是暂时出现。
- 快速响应网络拓扑的变化。
- 开销低，即 IGRP 本身使用的带宽不应超过其任务实际所需的带宽。
- 当多个并行路由的可取性大致相当时，在这些路由之间分割流量。
- 将错误率和不同路径上的流量水平纳入考虑范围。

目前实施的 IGRP 只为 TCP/IP 处理路由。不过，其基本设计宗旨是能够处理多种协议。

没有哪一种工具能够解决所有路由问题。按照惯例，路由问题可分为几个部分。如 IGRP 这样的协议称为“内部网关协议”(IGP)。这些协议旨在用于一组网络内部，这些网络要么接受单一管理，要么处于密切协调的管理下。这样的一组网络间通过“外部网关协议”(EGP) 连接。IGP 旨在跟踪大量有关网络拓扑的详细信息。设计 IGP 时，优先考虑生成最佳路由和快速响应变化。EGP 旨在保护一个网络系统免受其他系统的错误或故意失实陈述的影响，BGP 就是此类外部网关协议的一个例子。设计 EGP 时，优先考虑稳定性和管理控制。通常，生成合适的路由对 EGP 来说已经够用，不需要生成最佳路由。

IGRP 与 Xerox 的路由信息协议、Berkeley 的 RIP 和 Dave Mills 的 Hello 等比较早的协议有一些相似之处。它与这些协议的不同之处主要在于它是为更大更复杂的网络设计的。请参阅与 RIP 的比较部分，了解它与使用最广泛的老一代协议 RIP 的详细比较结果。

IGRP 与这些比较早的协议一样，是一种距离矢量协议。在此类协议中，网关仅与相邻的网关交换路由信息。此路由信息包含有关网络其余部分的信息摘要。此信息可采用数学方式显示，将所有网关集中起来，通过相当于分布式算法的方法解决优化问题。每个网关只需要解决一部分问题，而且也只需要接收总数据的其中一部分。

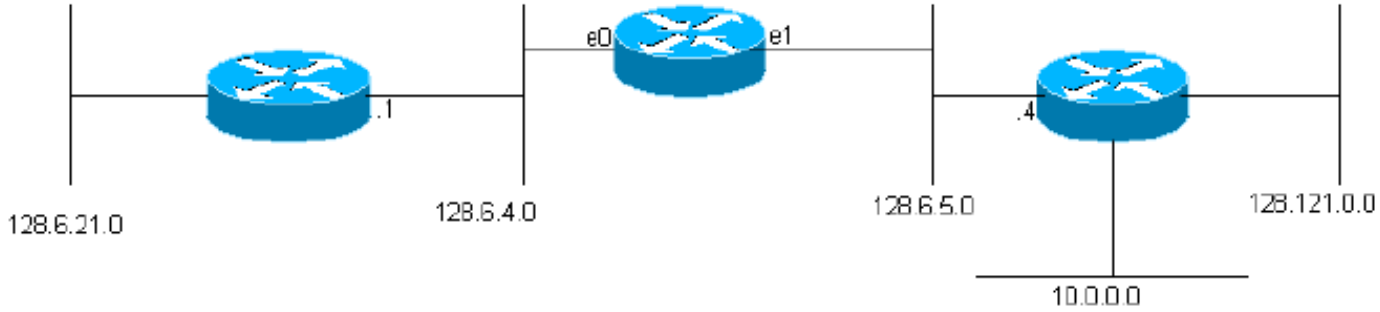
IGRP 的主要替代选择是增强型 IGRP (EIGRP) 和一类称为 SPF（最短路径优先）的算法。OSPF 使用的就是这个概念。要了解有关 OSPF 的详细信息，请参阅 OSPF 设计指南。OSPF 这类协议基于泛洪技术，每个网关会随时了解有关其他各个网关上各接口最新状态的信息。每个网关从自己的角度使用数据独立解决整个网络的优化问题。每种方法各有优势。在某些情况下，SPF 或许能够更快地响应变化。为了防止路由环路，IGRP 必须在发生某些特定变化后的几分钟内忽略新数据。而由于 SPF 拥有直接来自每个网关的信息，自然能够避免此类路由环路。因此，它可以立即按照新信息采取行动。但是，无论是在内部数据结构还是网关之间的消息方面，SPF 要处理的数据都远远多于 IGRP。

路由问题

IGRP 旨在供连接多个网络的网关使用。我们假设这些网络使用基于数据包的技术。实际上，这些网关发挥着数据包交换机的作用。当连接到一个网络的系统要向不同网络中的系统发送数据包时，它会将数据包发往网关。如果目的地位于该网关所连接的其中一个网络中，网关会将数据包转发到目的地。如果目的地更远，网关则会将数据包转发到距离目的地更近的另一个网关。网关使用路由表来帮助确定如何处理数据包。以下是路由表的一个简单例子。（示例中使用的地址是属于美国罗格斯大学的 IP 地址。请注意，其他协议的基本路由问题也与此类似，但此说明假设 IGRP 被用于路由 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
```



（正如我们将看到的，实际的 IGRP 路由表还包含每个网关的其他信息。）此网关连接到名为 0 和 1 的两个以太网。它们已得到 IP 网络号（实际上是子网号）128.6.4 和 128.6.5。因此，只需使用相应的以太网接口，即可将发往这些特定网络的数据包直接发送到目的地。附近有两个网关，128.6.4.1 和 128.6.5.4。发往 128.6.4 和 128.6.5 以外网络的数据包将转发到这两个网关其中之一，非此即彼。路由表指出了哪个网络应该使用哪个网关。例如，发往网络 10 中主机的数据包应转发到网关 128.6.5.4。我们希望此网关距离网络 10 更近，即通往网络 10 的最佳路径经过此网关。IGRP 的主要目的是让网关创建并维护这样的路由表。

IGRP 概述

如前所述，IGRP 是让网关能够通过与其他网关交换信息来创建其路由表的协议。网关从所有与其直接连接的网络的条目着手。它通过与相邻网关交换路由更新来获取有关其他网络的信息。在最简单的情况下，网关会找到一条代表通往每个网络最佳途径的路径。该路径具有以下特征：数据包应发送到的下一跳网关、应该使用的网络接口，以及度量信息。度量信息是描述路径良好程度的一组数字。网关可以通过此信息来比较它从不同网关处获知的路径，并决定到底使用哪一条路径。有时可能有必要在两条或多条路径之间分割流量，这种情况时有发生。但凡两条或多条路径同样良好，IGRP 就会进行此分割。用户也可以将其配置为在路径几乎同样良好时分割流量。在此情况下，更多流量将沿着度量值更优的路径发送。其目的是在 9600 BPS 线路和 19200 BPS 线路之间分割流量，而 19200 BPS 线路上的流量约为 9600 BPS 线路上流量的两倍。

IGRP 使用的度量包括：

- 拓扑延迟时间
- 路径上带宽最低一段的带宽
- 路径的信道占用率
- 路径的可靠性

拓扑延迟时间是沿着该路径到达目的地所需的时间（假设网络无负载）。当然，当网络有负载时，则会产生额外延迟。不过，负载是使用信道占用率的数值得出的，不会尝试测量实际延迟。路径带宽就是路径中最慢链路的带宽，以每秒位数为单位。信道占用率表示该带宽当前正在使用的部分有多少。这是测量得出的数据，并将随负载而变化。可靠性表示当前的错误率。它是完好无损到达目的地的数据包比率，经过测量得出。

还有两项信息尽管未用作度量的一部分，但也随度量信息一起传输：跳数和最大传输单位 (MTU)。跳数就是数据包到达目的地所必须经过的网关数。MTU 是可以沿着整条路径不分片发送的最大数据包大小。（换言之，它是该路径中涉及的所有网络的最小 MTU。）

根据度量信息，为路径计算一个“复合度量”。复合度量将度量的各个组成部分的影响合并为一个表示路径“良好程度”的数字。实际用于确定最佳路径的正是复合度量。

每个网关会定期向所有相邻网关广播其整个路由表（因水平分割规则而要经过一些删改）。当网关从其他网关收到此广播时，它会将该表与其现有的路由表进行比较。任何新的目的地和路径都会添加到网关的路由表中。网关还会将广播中的路径与现有路径进行比较。如果新路径更好，则会取代

现有路径。广播中的信息还会用于更新信道占用率和有关现有路径的其他信息。这一通用程序与所有距离矢量协议使用的程序类似。在数学文献中，它被称为贝尔曼-福特 (Bellman-Ford) 算法。请参阅 RFC 1058， 了解该基本程序的详细发展过程（介绍了较早的距离矢量协议 RIP）。

IGRP 在三个重要方面对通用的贝尔曼-福特算法进行了修改。首先，IGRP 没有使用简单度量，而是使用度量矢量来描述路径的特征。其次，IGRP 不是选取一条度量值最小的路径，而是在度量值属于指定范围内的多条路径之间分割流量。第三，IGRP 引入了多项功能，即便在拓扑发生变化的情况下也能提供稳定性。

最佳路径的选择基于复合度量：

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

其中，K1、K2 = 常量，Be = 无负载的路径带宽 x（1 - 信道占用率），Dc = 拓扑延迟，r = 可靠性。

复合度量最小的路径是最佳路径。有多条路径通往同一目的地的情况下，网关可以通过多条路径路由数据包。这一点是按照每条数据路径的复合度量来完成的。例如，如果一条路径的复合度量为 1 而另一条路径的复合度量为 3，则会通过复合度量为 1 的数据路径发送三倍的数据包。

使用度量矢量信息有两个优势。第一个优势是能够从同一组数据支持多种服务类型。第二个优势是准确性提高。使用单一度量时，通常会将其视同延迟。路径中的每条链路都被添加到总度量中。如果存在低带宽链路，通常以高延迟来表示。但是，带宽限制并不能真正按照延迟的累积方式累计。将带宽视为一个单独的要素才是正确的处理方式。同样，负载也可以通过一个单独的信道占用率数字来处理。

IGRP 为计算机网络的互联提供了一种系统，可以平稳地处理包括环路的常规图形拓扑。该系统维护完整的路径度量信息，即它知道通往任何网关连接到的所有其他网络的路径参数。流量可以分布于并行路径上，并且可以同时计算整个网络上的多条路径参数。

与 RIP 的比较

此部分将对 IGRP 与 RIP 进行比较。因为 RIP 广泛用于与 IGRP 类似的目的，所以这种比较颇具实用价值。但是，这样做并不完全公平。RIP 的本意并非是为了实现与 IGRP 相同的所有目标，而是旨在用于一些具有比较统一的技术的小型网络。在这种应用场合中，RIP 通常就足以胜任。

IGRP 与 RIP 之间最基本的区别在于度量结构。遗憾的是，这种变化并不是对 RIP 进行简单的改进就能实现的。它需要新的算法和 IGRP 中采用的数据结构。

RIP 使用简单的“跳数”度量来描述网络。与通过延迟、带宽等来描述每条路径的 IGRP 不同，RIP 使用从 1 到 15 的数字来描述路径。通常，此数字用于表示该路径在到达目的地之前会经过多少网关。这意味着，网速缓慢的串行线路和以太网之间并无区别。在某些 RIP 实施中，系统管理员可以指定应该多次计算给定的一跳。慢速网络可以用比较大的跳数来表示。但是，由于最大值是 15，此数值的计算次数不能过多。例如，如果用 1 表示以太网，用 3 表示 56Kb 线路，则一条路径最多只能有 5 条 56Kb 线路，否则就会超过最大值 15。要想全面地表示各种可用网络速度并支持用于大型网络，思科进行的研究表明，需要使用 24 位度量。如果最大度量太小，系统管理员就面临着一个令人不快的选择：要么无法区分快速和慢速路由，要么就不能将整个网络都纳入限制范围之内。事实上，有许多全国性网络现在已经太大，即使每一跳只计算一次，RIP 也无法处理。RIP 根本不能用于此类网络。

对这一问题的直接反应是修改 RIP 使其支持更大的度量。遗憾的是，这种办法行不通。与所有距离矢量协议一样，RIP 也有“计数到无穷大”的问题。RFC 1058 中对此进行了详细说明。当拓扑发生变

化时，会引入虚假路由。与这些虚假路由相关的度量缓慢增加，直至达到 15，届时这些路由将被删除。15 是足够小的最大值，假设使用触发更新的话，此过程的收敛速度会相当快。如果将 RIP 改为允许使用 24 位度量，环路会保留足够长的时间，让度量可以累计到 2**24。这是无法容忍的。IGRP 具有一些用于防止引入虚假路由的功能。下文第 5.2 部分将介绍这些功能。如果不对 SPF 等协议引入此类功能或做出更改，想要处理复杂的网络是不切实际的。

IGRP 并不仅仅是增加允许的度量范围。它对度量进行了重组，以便描述延迟、带宽、可靠性和负载。在 RIP 等单一度量中也可以表示此类考虑因素，但是 IGRP 采用的方法可能更准确。例如，使用单一度量时，多条连续的快速链路看起来与一条慢速链路有同样的效果。以延迟为首要关注点的交互式流量就是这种情况。但在进行批量数据传输时，最关心的是带宽，那么将各项度量加起来就不是适合这种情况的正确方法。IGRP 对延迟和带宽分开处理，累计延迟，但是取最低带宽。了解如何将可靠性和负载的影响纳入单一要素的度量中并非易事。

在我看来，IGRP 的一大优势就是易于配置。它可以直接表示具有物理意义的数量。这意味着可以根据接口类型、线速等自动对其进行设置。使用单一要素的度量，更有可能必须“修改”度量来纳入多项不同因素的影响。

其他创新更多的是在算法和数据结构方面而非在路由协议上。例如，IGRP 指定了支持在几条路由之间分割流量的算法和数据结构。要设计一种 RIP 实施来做到这一点肯定也可以。但是，一旦要重新实施路由，就没有理由坚持使用 RIP 了。

到目前为止，本文一直在介绍“通用 IGRP”，这项技术可以支持任何网络协议的路由。但是，在此部分，更值得一提的是特定的 TCP/IP 实施。这是要与 RIP 进行比较的实施。

RIP 更新消息只包含路由表的快照。换言之，其中包含许多目的地和度量值，除此之外几乎没有其他信息。而 IGRP 的 IP 实施则有更多结构。首先，更新消息以“自治系统编号”标识。此术语来自 Arpanet 的传统，并有着特定含义。但是对大多数网络而言，这个词的意思是指可以在同一个网络中运行多种不同的路由系统。这对来自多个组织的网络的收敛位置非常有用。每个组织都可以维护自己的路由。由于每次更新都会进行标记，因此可将网关配置为仅关注合适的更新。将特定网关配置为接收来自多个自治系统的更新。它们以可控方式在系统之间传送信息。请注意，这不是路由安全问题的完整解决方案。任何网关都可以配置为侦听来自任何自治系统的更新。但是，在实施路由策略时（在这种情况下，网络管理员之间的信任程度尚可），这仍然不失为一种非常有用的工具。

有关 IGRP 更新消息的第二项结构上的功能会影响 IGRP 处理默认路由的方式。大多数路由协议都有默认路由的概念。路由更新要列出世界上每个网络往往是不切实际的。通常，一组网关需要详细列出组织内部网络的路由信息。发往组织外部目的地的所有流量均可发送到几个边界网关之一。这些边界网关可能有着更完整的信息。通往最佳边界网关的路由就是“默认路由”。我们使用它来到达内部路由更新中未明确列出的任何目的地，从这个意义上来说，它是默认路由。RIP 和一些其他路由协议如同对待真实网络一样传播有关默认路由的信息。IGRP 却采用不同的方法。IGRP 允许将真实网络标记为默认路由的候选，而不是用一个虚假条目作为默认路由。它通过将有关这些网络的信息放到更新消息的特殊外部部分中来实现这一点。但也可将其视为打开一个与这些网络相关联的位。IGRP 定期扫描所有候选的默认路由，并选择度量最小的路由作为实际默认路由。

这种默认路由方法有可能比大多数 RIP 实施所采用的方法更加灵活一点。RIP 网关通常可以设置为生成具有某个指定度量的默认路由。其目的是让此操作在边界网关上完成。

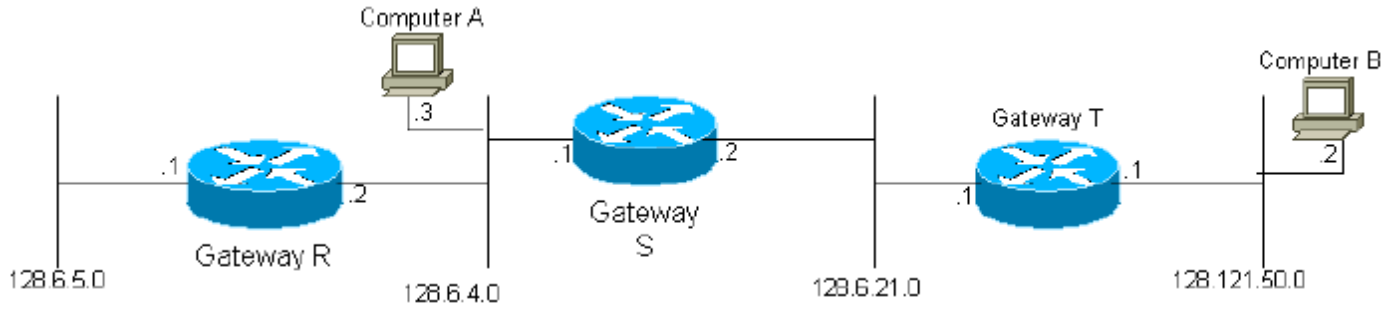
详细说明

此部分提供对 IGRP 的详细说明。

总体概述

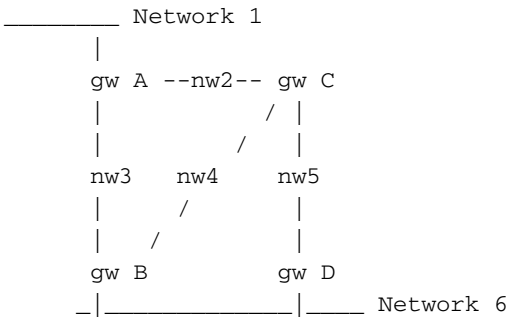
首次打开网关时，其路由表将进行初始化。此操作可以由操作人员从控制台终端完成，也可以通过从配置文件读取信息来完成。提供连接到网关的每个网络的说明，包括沿链路的拓扑延迟（例如，一个位穿过这条链路需要的时间）和链路的带宽。

图 2



以上图为例，网关 S 会获知其可以通过相应接口连接到网络 2 和网络 3。因此，最初网关 2 只知道其可以访问网络 2 和网络 3 中的任何目的计算机。所有网关都已编程为定期向邻居网关传输其初始化的信息，以及从其他网关收集的信息。因此，网关 S 会收到网关 R 和网关 T 的更新，并获知其可以通过网关 R 访问网络 1 中的计算机，可以通过网关 T 访问网络 4 中的计算机。由于网关 S 发送的是整个路由表，在下一个周期中，网关 T 将获知其可以通过网关 S 访问网络 1。不难看出，有关系统中每个网络的信息最终将传遍系统中的每个网关，只要这些网络完全连接。

图 3



每个网关通过计算复合度量来确定通往目的计算机的数据路径的可取性。以上图为例，若目的地在网络 6 中，网关 A (gw A) 会计算通过网关 B 和网关 C 的两条路径的度量函数。请注意，路径只以下一跳来定义。实际上，从 A 到网络 6 有三条可能的路由：

- 直接到 B
- 先到 C 再到 B
- 先到 C 再到 D

但是，网关 A 不需要在涉及 C 的两条路由之间进行选择。A 中的路由表只有一个条目代表通往 C 的路径。其度量表示该路径是从 C 前往最终目的地的最佳途径。如果 A 向 C 发送数据包，则使用 B 还是 D 将由 C 来决定。

等式 1

为每条数据路径计算的复合度量函数如下所示：

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

其中，r = 可靠信比率（下一跳成功收到的传输数据包的百分比），Dc = 复合延迟，Be = 有效带宽

：无负载的带宽 x（1 - 信道占用率），K1 和 K2 = 常量。

等式 2

求复合延迟 (Dc) 的方法大体上如下所示：

```
Dc = Ds + Dcir + Dt
```

其中，Ds = 交换延迟，Dcir = 电路延迟（1 个位的传播延迟），DT = 传输延迟（1500 个位的消息的无负载延迟）。

不过，实际上我们是对每种类型的网络技术使用一个标准延迟数值。例如，对以太网和任何一种特定比特率的串行线路分别有一个标准延迟数值。

以下为上图网络 6 的情况下网关 A 的路由表示例。（请注意，为简单起见，未显示度量矢量的各个组成部分。）

路由表示例：

网络	接口	下一跳网关	度量
1	NW 1	无	直连
2	NW 2	无	直连
3	NW 3	无	直连
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

贝尔曼-福特算法描述了通过与邻居交换信息来创建路由表的基本过程。该算法用于一些比较早的协议中，例如 RIP (RFC 1058)。为了处理更复杂的网络，IGRP 对基本贝尔曼-福特算法增加了三项功能：

1. 不使用简单度量，而是使用度量矢量来描述路径的特征。可以根据此矢量按照前文等式 1 计算出一个复合度量。矢量的使用可以让网关使用等式 1 中的多个不同系数来适应不同服务类型。而且，它还能比单一度量更准确地表示网络特征。
2. 不是选取一条度量值最小的路径，而是在度量值属于指定范围内的多条路径之间分割流量。这样就能并行使用多条路由，提供比任何单一路由都更高效的带宽。网络管理员指定差量 V。保留复合度量为最小值 M 的所有路径。此外，度量小于 V x M 的所有路径也保留。流量分布在与这些复合度量成反比的多条路径之间。
3. 此差量概念存在一些问题。想要提出使用差量值大于 1 但又不会导致数据包循环的策略非常困难。思科 8.2 版中未实现差量功能。（不确定哪个版本中删除了该功能。）其结果是将差量永久设置为 1。
4. 引入了多项功能，即便在拓扑发生变化的情况下也能提供稳定性。这些功能旨在防止路由环路和“计数到无穷大”，这是以前尝试将福特类型算法用于此类应用场合时的特征。主要的稳定性功能包括“抑制”、“触发更新”、“水平分割”和“毒化”。下文将更加详细地介绍这些功能。

流量分割（第 2 点）引发了一种相当微妙的危险。差量 V 旨在让网关能够使用速度不同的并行路径。例如，为了实现冗余，可能存在 9600 BPS 线路与 19200 BPS 线路并行运行的情况。如果差量

V 为 1，则只会使用最佳路径。因此，如果 19200 BPS 线路的可靠性尚可，则不会使用 9600 BPS 线路。（但是，如果多条路径相同，则会在其之间分摊负载。）通过提出差量，我们就可以在最佳路由与几乎同样良好的其他路由之间分割流量。如果差量足够大，就会在两条线路之间分割流量。危险在于当差量足够大时，允许使用的路径不仅速度变慢，而且实际上是“错误的方向”。因此，还应该用一条规则来防止流量被发送到“上游”：如果路径的远程复合度量（在下一跳计算的复合度量）大于在网关处计算的复合度量，则不沿该路径发送流量。一般建议系统管理员不要设置大于 1 的差量，除非是在需要使用并行路径的特定情况下。在此情况下，应仔细设置差量，以期达到“正确”的结果。

IGRP 旨在处理多种“服务类型”和多个协议。服务类型是数据包中用于修改路径评估方式的规范。例如，TCP/IP 协议允许数据包指定高带宽、低延迟或高可靠性的相对重要性。通常，交互式应用会指定低延迟，而批量传输应用则会指定高带宽。这些要求决定了适合用于等式中的 K1 和 K2 的相对值。1.要支持的数据包中的每种规范组合称为“服务类型”。对于每种服务类型，必须选择一组参数 K1 和 K2。每种服务类型保留一份路由表。之所以如此，是因为路径是根据等式所定义的复合度量来选择和排序的。1.每种服务类型的复合度量都有所不同。来自所有这些路由表中的信息合并起来，就生成了由网关交换的路由更新消息，如图 7 所示。

稳定性功能

此部分介绍抑制、触发更新、水平分割和毒化等功能。这些功能旨在防止网关选择错误路由。如 RF 1058C 中所述，当路由因网关或网络出现故障而不可用时，就会发生这种情况。一般而言，相邻的网关会检测到故障。然后，它们会发送路由更新，显示旧路由不可用。但是，更新有可能根本不会到达网络的某些部分，或延迟到达某些网关。仍然认为旧路由状况良好的网关会继续传播该路由的信息，从而让故障路由重新进入系统中。最终，此信息将通过网络传播，并传回到重新添加该信息的网关。其结果就是造成循环路由。

实际上，这些对策中存在一些冗余。大体上来说，抑制和触发更新原本应该足以防止错误路由。但实际上各种各样的通信故障可能会导致这两种对策力有不逮。水平分割和路由毒化旨在防止任何情况下出现路由环路。

通常，新的路由表会定期发送到邻居网关（默认情况下每隔 90 秒发送一次，但系统管理员可对此进行调整）。触发更新是响应一些变化而立即发送新路由表。最重要的变化是删除路由。发生这种情况可能是因为超时周期结束（可能邻居网关或线路已关闭），也可能是因为来自路径中下一跳网关的更新消息显示路径不再可用。当网关 G 检测到某条路由不再可用时，会立即触发更新。此更新将显示该路由不可用。可以考虑一下当此更新到达邻居网关时会发生什么情况。如果邻居的路由指向 G，则邻居必须删除该路由。这会导致邻居触发更新，依次类推。因此，一次故障会触发一波更新消息。这一波更新将传遍途经故障网关或网络的路由所经过的网络部分。

如果我们可以保证这一波更新能立即到达每个恰当的网关，则触发更新就够用了。但是，存在两个问题。第一个问题，包含更新消息的数据包可能会被网络中的某些链路丢弃或损坏。第二个问题，触发更新不会即刻发生。尚未收到触发更新的网关有可能在错误的时间发出定期更新，导致错误的路由被重新添加至已收到触发更新的邻居中。抑制就是为应对这些问题而设计的。抑制规则规定，删除一条路由时，在一段时间内不接受同一目的地的新路由。这让触发更新有时间到达所有其他网关，从而确定我们获得的新路由不会是一些网关重新添加的旧路由。抑制期的时长必须足以让一波触发更新传遍整个网络。此外，这个时长还应包括几个定期广播周期，以便处理丢弃的数据包。考虑一下如果其中一个触发更新被丢弃或损坏会发生什么情况。发出该更新的网关将在下一次定期更新时发出另一次更新。这将在错过最初一波更新的邻居那里重新启动一波触发更新。

触发更新与抑制相结合，应该足以摆脱过期路由并防止其重新添加。不过，还有一些其他预防措施仍然值得一做。这些措施考虑到损耗非常大的网络和分区的网络。IGRP 需要的其他预防措施包括水平分割和路由毒化。水平分割起因于以下观察结果：将路由沿来途方向发送回去毫无意义。请考虑以下情况：

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

网关 A 告诉网关 B 它有一条通往网络 1 的路由。那么当 B 向 A 发送更新时，它就没有任何理由提及网络 1。由于 A 离 1 更近，因此它也没有理由考虑途经 B。水平分割规则规定，应该为每个邻居（实际上是每个相邻网络）生成单独的更新消息。特定邻居的更新应忽略指向该邻居的路由。此规则可防止相邻网关之间形成环路。例如，假设 A 与网络 1 连接的接口发生故障。如果没有水平分割规则，B 就会告诉 A 它可以连接到 1。因为 A 不再有实际路由，所以它可能会选取该路由。在此情况下，A 和 B 都会有通往 1 的路由。但是，A 会指向 B 而 B 会指向 A。当然，触发更新和抑制应该能够防止这种情况发生。不过，因为没有理由将信息发送回其来处，所以仍然值得进行水平分割。除了防止环路的作用外，水平分割还能控制更新消息的大小。

水平分割应防止相邻网关之间形成环路。路由毒化则旨在中断较大的环路。该规则规定，当更新显示现有路由的度量增加足够多时，则表示存在环路。应删除并抑制该路由。当前，该规则规定，如果复合度量增加倍数超过 1.1，则删除路由。如果复合度量出现任何增加就触发删除路由并不安全，因为信道占用率或可靠性的变化可能会导致度量的细微变化。所以，1.1 的倍数只是一个试探性的数值。确切的值并不重要。我们预计此规则只需要中断非常大的环路，因为触发更新和抑制会防止小环路。

禁用抑制

自 8.2 版起，思科代码提供禁用抑制的选项。抑制的缺点在于当旧路由发生故障时，它们会延迟采用新路由。如果使用默认参数，路由器在发生变化后采用新路由可能需要几分钟。但是，出于上述原因，仅仅删除抑制并不安全。其结果是计数到无穷大，如 RFC 1058 中所述。我们推测（但不能证明），如果使用加强版的路由毒化，则不再需要通过抑制来阻止计数到无穷大。因此，禁用抑制能够实现这种加强型路由毒化。请注意，水平分割和触发更新仍然有效。

加强型路由毒化基于跳数。如果路径的跳数增加，则删除该路由。这种做法无疑会删除仍然有效的路由。例如，如果网络中其他地方发生某些变化，导致路径现在要多经过一个网关，跳数就会增加。在此情况下，该路由仍然有效。但是，没有完全安全的方法来区分这种情况与路由环路（计数到无穷大）。因此，最安全的方法就是只要跳数增加就删除路由。如果路由仍然合法，则会在下一次更新重新添加该路由，继而导致触发更新，在系统中的其他位置重新添加该路由。

通常，距离矢量算法比较容易采用新路由。从系统中完全清除旧路由才是问题。因此，过于激进地删除可疑路由的规则应该是安全的。

更新过程的详细信息

图 4 到图 8 中介绍的一系列过程旨在处理单个网络协议，例如 TCP/IP、DECnet 或 ISO/OSI 协议。不过，只提供了 TCP/IP 协议的详细信息。一个网关可能会处理遵守多种协议的数据。因为每种协议的编址结构和数据包格式不同，所以每种协议用于实施图 4 到图 8 的计算机代码通常也不同。正如图 4 的详细说明中所述，图 4 中介绍的过程差异最大。图 5 到图 8 中介绍的过程采用相同的一般结构。不同协议之间的主要区别是路由更新数据包的格式，该格式必须设计为与具体协议兼容。

请注意，目的地的定义因不同协议而异。此处介绍的方法可用于通往单个主机的路由、通往网络的路由，或用于更复杂的分层地址方案。使用哪种类型的路由取决于协议的编址结构。当前的 TCP/IP 实施仅支持通往 IP 网络的路由。因此，“目的地”实际上表示 IP 网络或子网编号。只保留相连网络的子网信息。

图 4 到图 7 显示了网关使用的路由过程各部分的伪代码。开始编程时，输入可接受的协议和描述每个接口的参数。

网关只会处理列出的特定协议。如果系统使用的协议不在列表中，则来自该系统的任何通信都将被忽略。数据输入如下：

- 网关连接到的网络。
- 每个网络的无负载带宽。
- 每个网络的拓扑延迟。
- 每个网络的可靠性。
- 每个网络的信道占用率。
- 每个网络的 MTU。

然后，按照等式 1 计算每条数据路径的度量函数。请注意，前三项在相当大的程度上是固定不变的。它们是底层网络技术的函数，并不取决于负载。可以通过配置文件对其进行设置，也可以由操作人员直接输入。请注意，IGRP 不使用测量得出的延迟。理论和经验都表明，使用测量得出的延迟的协议非常难以保持稳定的路由。测量得出的参数有两个：可靠性和信道占用率。可靠性基于网络接口硬件或固件报告的错误率。

除了这些输入外，路由算法还需要若干路由参数的值。其中包括计时器值、差量，以及是否启用了抑制。这些值通常会通过配置文件或操作人员输入来指定。（自思科 8.2 版起，将差量永久设置为 1。）

输入初始信息后，网关中的操作将由事件（数据包到达某一个网络接口或计时器到期）触发。图 4 到图 7 中介绍的过程如下触发：

- 当数据包到达时，根据图 4 对其进行处理。这会导致将数据包从另一个接口发送出去、丢弃数据包或接受数据包进行进一步处理。
- 当网关接受数据包进行进一步处理时，将以此规范中未介绍的协议特定方式对数据包进行分析。如果数据包是路由更新，则根据图 5 对其进行处理。
- 图 6 所示为计时器触发的事件。计时器设置为每秒生成一次中断。当中断发生时，执行图 6 中显示的过程。
- 图 7 所示为路由更新子例程。图 5 和图 6 中显示了对此子例程的调用。
- 此外，图 8 还显示了图 5 和图 7 中引用的度量计算的详细信息。

有四个重要的时间常量控制着路由的传播和过期。这些时间常量可由系统管理员设置，但也有默认值。这些时间常量包括：

- 广播时间 - 所有网关按照此频率在所有连接的接口上广播更新。默认值为每 90 秒一次。
- 无效时间 - 如果没有在此时间内收到给定路径的更新，则认为该路径已超时。此时间应为广播时间的数倍，以便虑及网络可能丢弃包含更新的数据包的可能性。默认值为广播时间的 3 倍。
- 保持时间 - 当某个目的地已无法访问（或度量的增加足以导致毒化）时，该目的地会进入“抑制”状态。在此状态下，这段时间内不会接受同一目的地的新路径。保持时间表示此状态应持续多长时间。此时间应为广播时间的数倍。默认值为广播时间的 3 倍加上 10 秒。（如禁用抑制部分所述，可以禁用抑制功能。）
- 刷新时间 - 如果在此时间内未收到给定目的地的更新，则从路由表中删除该路径的条目。请注意无效时间与刷新时间之间的区别：超过无效时间后，路径将超时并被删除。如果没有其余路径通往目的地，则现在无法访问目的地。但是，目的地的数据库条目保留不变。仍然必须执行抑制。而超过刷新时间后，将从表中删除数据库条目。此时间应比无效时间加上抑制时间之和稍长。默认值为广播时间的 7 倍。

这些数值以下列主要数据结构为先决条件。为网关支持的每种协议保留单独的一组此类数据结构。在每种协议中，为要支持的每种服务类型保留单独的一组数据结构。

对于系统知道的每个目的地，有一个（可能是 null 值）通往目的地的路径的列表、一个抑制到期时间和一个上次更新时间。上次更新时间表示上一次此目的地的任何路径包含于来自其他网关的更新

中的时间。请注意，还保留了每条路径的更新时间。当通往目的地的最后一条路径被删除时，除非抑制功能已禁用（有关详细信息，请参阅禁用抑制部分），否则目的地将进入抑制状态。抑制到期时间表示抑制到期的时间。此值非零的事实表明目的地处于抑制状态。为了节约计算时间，为每个目的地保留一个“最佳度量”也不失为一个好主意。这就是通往目的地的所有路径的最小复合度量值。

对于通往目的地的每条路径，有路径中下一跳的地址、要使用的接口、描述路径特征的度量矢量（包括拓扑延迟、带宽、可靠性和信道占用率）。其他信息也与每条路径相关联，其中包括跳数、MTU、信息源、远程复合度量，以及使用这些数字按照等式 1 计算出的复合度量。还有上次更新时间。信息源表示该路径的最新更新来自何处。实际上，这与下一跳的地址相同。上次更新时间就是此路径的最近一次更新到达的时间。它用于让超时路径过期。

请注意，IGRP 更新消息有三个部分：内部、系统（表示“此自治系统”而非内部）和外部。内部部分包括通往子网的路由，但并不包括所有子网信息，而是只包括一个网络的子网。这是与更新要发送到的地址相关联的网络。因为通常会在每个接口上广播更新，所以这就是在其中发送广播的网络。（对 IGRP 请求的响应和点对点 IGRP 会出现其他情况。）主要网络（例如，非子网）除非明确标记为外部，否则会放入更新消息的系统部分。

如果某个网络是从其他网关获知的并且该信息包含在更新消息的外部部分到达，则将该网络标记为外部。思科的实施还允许系统管理员将特定网络声明为外部。外部路由也称为“candidate default”（候选默认路由）。这些路由可以到达或经过被视为适合作为默认路由的网关，用于没有通往目的地的明确路由的情况。例如在美国罗格斯大学，我们将连接到罗格斯大学的网关配置为地区网络，因此它将通往 NSFnet 主干的路由标记为外部。思科的实施通过选取度量最小的外部路由来选择默认路由。

以下各部分旨在为图 4 到图 8 等特定部分提供说明。

数据包路由

图 4 描述了输入数据包的总体处理。这只是用于阐明术语。显而易见，这不是对 IP 网关作用的完整说明。

此过程使用初始化网关时输入的受支持协议的列表和有关接口的信息。数据包处理的细节取决于数据包使用的协议。这一点通过步骤 A 来确定。步骤 A 是图 4 中所有协议都相同的唯一部分。知道协议类型后，即可使用适合协议类型的相应图 4 实施。协议的规范描述了数据包内容的详细信息。协议的规范包括用于确定数据包目的地的程序、用于将目的地与网关自己的地址进行比较以确定网关本身是不是目的地的程序、用于确定数据包是不是广播的程序，以及用于确定目的地是否属于指定网络的程序。图 4 的步骤 B 和步骤 C 中使用了这些程序。步骤 D 中的测试需要搜索路由表中列出的目的地。如果路由表中有目的地的条目，并且目的地至少有一条与其关联的可用路径，则测试结果理想。请注意，这一步和下一步中使用的目的地和路径数据是针对支持的每种服务类型分别维护的。因此，这一步首先确定数据包指定的服务类型，并选择相应的一组数据结构用于这一步和下一步。

如果路径的远程复合度量小于其复合度量，则可用于步骤 D 和步骤 E 的用途。如果路径的远程复合度量大于其复合度量，则该路径的下一跳离目的地“更远”，如度量所测量的那样。这种路径称为“上游路径”。通常，人们期望度量的使用能够阻止选择上游路径。不难看出，上游路径绝不可能是最佳路径。但是，如果允许使用较大的差量，则可以使用除最佳路径以外的路径。这其中就有可能包括上游路径。

步骤 E 计算要使用的路径。远程复合度量不小于其复合度量的路径不予考虑。如果有多条可接受的路径，以循环交替的加权形式使用这些路径。路径的使用频率与其复合度量成反比。

接收路由更新

图 5 描述从邻居网关收到的路由更新的处理。此类更新包括一个条目列表，其中的每个条目提供一个目的地的信息。为了适应多种服务类型的需要，一次路由更新中可能会出现同一目的地有多个条目的情况。如图 5 中所述，每个条目单独处理。如果条目属于更新的外部部分，则会为相应的目的地设置外部标记（如果此过程的结果是添加该目的地）。

对网关支持的每种服务类型，必须使用一组与该服务类型相关联的目的地/路径信息，重复一次图 5 中所述的整个过程。图 5 最外层一圈显示了这一点。必须为每种服务类型处理一次整个路由更新。（请注意，IGRP 的当前实施不支持多种服务类型，因此最外层一圈实际上并未实施。）

步骤 A 中对路径进行了基本可接受性测试。这应该包括对目的地的合理性测试。不可能（“Martian”）的网络号应该拒绝。（请参阅 RFC 1009 和 R FC 1122 了解详细信息。）如果它们所指的目的地处于抑制状态，即抑制到期时间非零且晚于当前时间，更新也会被拒绝。

步骤 B 通过搜索路由表来确定此条目描述的路径是否已知。路由表中的路径由其关联的目的地、作为该路径一部分列出的下一跳、要用于该路径的输出接口和信息源（发送更新的地址 - 实际上通常与下一跳相同）来定义。更新数据包中的条目描述了如下路径：其目的地在条目中列出，其输出接口是更新传入时的接口，其下一跳和信息源是发送更新的网关的地址（“源”S）。

在步骤 H 和步骤 T 中，对图 7 中所述的更新过程进行了安排。实际上，此过程将在图 5 中所述的整个过程完成后运行。也就是说，即使在图 5 中所述的处理过程期间多次触发，图 7 中所述的更新过程也只会发生一次。此外，如果网络变化速度很快，必须采取预防措施来防止过于频繁地发出更新。

如果路由表中已存在更新数据包中当前条目所述的目的地，则需要完成步骤 K。步骤 K 将根据更新数据包中的数据计算的新复合度量与目的地的最佳复合度量进行比较。请注意，最佳复合度量并非此时重新计算的，因此，如果考虑的路径已在路由表中，此测试可能会比较同一条路径的新旧度量。

对不如现有最佳复合度量的路径执行步骤 L。这包括不如现有路径的新路径和复合度量有所增加的现有路径。步骤 L 测试新路径是否可接受。请注意，此测试执行了新路径是否良好到足以保留和路由毒化这两项测试。要达到可接受的程度，延迟值不能是表示目的地无法访问的特殊值（对当前的 IP 实施而言，是 24 位字段中全为 1），且复合度量（按图 8 中指定的程序计算）必须可接受。要确定复合度量是否可接受，请将其与通往目的地的所有其他路径的复合度量进行比较。以 M 为这些度量的最小值。如果它 < V X M（其中，V 是初始化网关时设置的差量），则新路径可接受。如果 V = 1（自思科 8.2 版起总是如此），则任何不如现有度量的度量都不可接受。这一条有一种例外情况：如果该路径已经存在且是通往目的地的唯一路径，则当度量的增加未超过 10%（或在禁用抑制的情况下跳数未增加）时将保留该路径。

当路径的新信息表明复合度量将减少时，需要完成步骤 V。比较通往目的地 D 的所有路径的复合度量。在此比较中，使用 P 而非出现在路由表中的路径的新复合度量。计算最小复合度量 M。然后，再次检查通往 D 的所有路径。如果任何路径的复合度量 > M x V，则删除该路径。V 是初始化网关时输入的差量。（自思科 8.2 版起，将差量永久设置为 1。）

定期处理

图 6 中所述的过程每秒触发一次。该过程检查路由表中的各种计时器是否有任何已过期。前文已介绍过这些计时器。

步骤 U 将激活图 7 中所述的过程。

步骤 R 和步骤 S 很有必要，因为路由表中存储的复合度量取决于根据测量得出的信道占用率，它会随着时间推移而变化。使用测得的流经接口的流量的移动平均值定期重新计算信道占用率。如果新计算的值与现有值不同，则必须调整涉及该接口的所有复合度量。检查路由表中显示的每条路径。对下一跳使用接口“I”的任何路径重新计算复合度量。此复合度量按照等式 1 进行计算，使用路由表中作为该路径度量的一部分存储的信道占用率最大值和新计算的接口信道占用率。

生成更新消息

图 7 介绍网关如何生成要向其他网关发送的更新消息。为连接到网关的每个网络接口生成单独的消息。然后，将该消息发送到可通过该接口访问的所有其他网关（步骤 J）。为了完成此操作，通常会将该消息作为广播发送。但是，如果网络技术或协议不允许使用广播，则可能需要分别向每个网关发送该消息。

一般情况下，步骤 G.会在路由表中为每个目的地添加一个条目，以此创建该消息。请注意，必须使用与每种服务类型相关联的目的地/路径数据。最糟糕的情况是，为每种服务类型向每个目的地的更新中添加了新条目。但是，在步骤 G 向更新消息中添加条目之前，已经对已添加的条目进行了扫描。如果新条目已存在于更新消息中，则不会再次添加该条目。当目的地和下一跳网关相同时，新条目将复制现有条目。

为简单起见，伪代码将省略一件事 - IGRP 更新消息分为三个部分：内部、系统和外部，这意味着实际上目的地之上有三个圈。第一圈只包括要向其发送更新的网络的子网。第二圈包括未标记为外部的所有主要网络（例如，非子网）。第三圈包含标记为外部的所有主要网络。

步骤 E 执行水平分割测试。在正常情况下，如果路由的最佳路径来自向外发送更新的同一接口，此测试将失败。但是，如果更新是发送到特定目的地（例如，响应来自其他网关的 IGRP 请求，或作为“点对点 IGRP”的一部分），则只有当最佳路径最初来自该目的地（其“信息源”与目的地相同）且其输出接口与传入请求的接口相同时，水平分割才会失败。

计算度量信息

图 8 介绍如何根据网关收到的更新消息处理度量信息，以及如何为网关发送的更新消息生成度量信息。请注意，条目基于通往目的地的一条特定路径。如果有多条通往目的地的路径，则选择复合度量最小的路径。如果有多条路径的复合度量最小，则采用任意平局决胜规则。（对大多数协议而言，这根据下一跳网关的地址而定。）

图 4 - 处理传入数据包

```
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 - 处理传入路由更新

```
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
```

图 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
```

图 8 - 度量计算的详细信息

此部分介绍根据到达的路由更新计算度量和跳数的程序。此函数的输入是路由更新数据包中具体目的地的条目。其输出是可用于计算复合度量的度量矢量和跳数。如果此路径被添加到路由表中，则在表中输入整个度量矢量。以下定义中使用的接口参数是初始化网关时设置的参数，对于路由更新所到达的接口，不同之处在于信道占用率和可靠性基于测得的流经接口的流量的移动平均值。

- 延迟 = 数据包中的延迟 + 接口拓扑延迟
- 带宽 = 最大值（数据包中的带宽、接口带宽）
- 可靠性 = 最小值（数据包中的可靠性、接口可靠性）
- 信道占用率 = 最大值（数据包中的信道占用率、接口的信道占用率）（带宽使用最大值，因为带宽度量是以相反形式存储的。从概念上说，我们需要的是最低带宽。）请注意，必须保存数据包中的原始信道占用率，因为每当接口的信道占用率发生变化时，重新计算有效的信道占用率需要使用此值。

以下不是度量矢量的一部分，但也作为路径的特征保留在路由表中：

- 跳数 = 数据包中的跳数。
- MTU = 最小值（数据包中的 MTU、接口 MTU）。
- 远程复合度量 = 使用数据包中的度量值按照等式 1 计算得出。也就是说，度量的各组成部分来自数据包中的数值，不会如上所示更新。显然，必须在进行上面显示的调整之前计算此值。
- 复合度量 = 使用按此部分所述计算的度量值按照等式 1 计算得出。

此部分的剩余部分介绍用于为要发送的路由更新计算度量和跳数的程序。

此函数确定要放入传出更新数据包中的度量信息和跳数。如果有任何可用的路径，则此函数根据通往目的地的具体路径计算。如果没有路径或所有路径均为上游路径，则称该目的地“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 实施的详细信息

此部分简要介绍思科 IGRP 使用的数据包格式。IGRP 通过 IP 协议 9 (IGP) 使用 IP 数据报发送。数据包以报头开始。它紧跟在 IP 报头之后。

```
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，路由信息紧跟在报头之后。

版本号当前为 1。其他版本号的数据包将被忽略。

操作码可为 1 = 更新或 2 = 请求。

这表示消息的类型。下文将介绍两种消息类型的格式。

Edition 是序列号，每当路由表中发生变化时就会增加。（这种变化发生在上述伪代码触发路由更新的情况下。）版本号可以让网关避免处理包含已知信息的更新。（这一点当前未实现。换言之，版本号能够正确生成，但在输入时会被忽略。因为数据包有可能被丢弃，所以不清楚版本号是否足以避免重复处理。需要确保与该版本相关联的所有数据包都已得到处理。）

Asystem 是自治系统编号。在思科实施中，网关可以加入多个自治系统。每个此类系统都会运行自己的 IGRP 协议。从概念上说，每个自治系统有完全独立的路由表。从一个自治系统通过 IGRP 到达的路由仅在该自治系统的更新中发送。网关可以通过此字段选择要使用哪一组路由表处理此消息。如果网关收到未配置的自治系统的 IGRP 消息，会忽略该消息。实际上，思科实施允许从一个自治系统向另一个自治系统“泄漏”信息。但是，我将之视为管理工具而不是协议的一部分。

Ninterior、*nsystem* 和 *nexterior* 分别表示更新消息的三个部分中每部分的条目数。前文已介绍过这三个部分。各部分之间没有任何其他分界线。首先的 ninterior 条目为内部部分，其次的 nsystem 条目为系统部分，最后的 nexterior 条目为外部部分。

校验和是 IP 校验和，使用与 UDP 校验和相同的校验和算法进行计算。校验和根据 IGRP 报头和跟在其后的任何路由信息计算得出。在计算校验和时，校验和字段设置为零。校验和不包括 IP 报头，也不包括任何如 UDP 和 TCP 中那样的虚拟报头。

请求

IGRP 请求要求接收方发送其路由表。请求消息只包含报头。仅使用版本、操作码和 asystem 字段。所有其他字段均为零。接收方应向请求方发送正常的 IGRP 更新消息。

更新

IGRP 更新消息包含报头，后面紧跟路由条目。包含的路由条目多多益善，以 1500 字节的数据报（包括 IP 报头）为容纳上限。按当前的结构声明，最多可包含 104 个条目。如果需要的条目更多，则发送多个更新消息。由于更新消息就是简单地逐个条目进行处理，使用单个分片的消息较之多个独立的消息并无任何优势。

以下是路由条目的结构：

```
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 */
```

这些字段定义了 uchar [2] 和 uchar[3] 只是正常 IP 网络顺序的 16 位和 24 位二进制整数。

编号用于定义所描述的目的地。它是一个 IP 地址。为节省空间，除内部部分之外，其余部分只提供了 IP 地址的前 3 个字节。内部部分中则提供了后 3 个字节。系统和外部路由不可能是子网，因此低位字节始终为零。内部路由始终是已知网络的子网，因此会提供该网络号的第一个字节。

延迟的单位为 10 微秒。这可提供 10 微秒到 168 秒的取值范围，似乎足够了。全部为 1 的延迟表示网络无法访问。

带宽是相反形式的带宽，以每秒位数为单位，以 1.0e10 的系数为调节比例。范围是从 1200 BPS 线路到 10 Gbps。（也就是说，如果带宽为 N Kbps，则使用的数字为 10000000/N。）

MTU 以字节为单位。

可靠性以 255 的分数形式给出。换言之，255 为 100%。

负载以 255 的分数形式给出。

跳数是简单的计数。

由于带宽和延迟所用的单位有点异乎寻常，似乎应提供一些示例才妥当。所以，以下是用于几种常见介质的默认值。

	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

以下是对思科 8.0(3) 版中复合度量的实际计算方法的说明。

```
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