Einführung in IGRP

Inhalt

Einführung

In diesem Dokument wird das Interior Gateway Routing Protocol (IGRP) vorgestellt. Es hat zwei Ziele. Eine davon ist die Einführung der IGRP-Technologie für diejenigen, die daran interessiert sind, diese zu nutzen, zu evaluieren und möglicherweise zu implementieren. Die andere besteht darin, einige interessante Ideen und Konzepte, die im IGRP enthalten sind, näher zu beleuchten. Informationen zur Konfiguration des IGRP finden Sie unter Konfigurieren von IGRP, Cisco IGRP-Implementierung und IGRP-Befehlen.

Ziele für IGRP

Das IGRP-Protokoll ermöglicht es einer Reihe von Gateways, ihr Routing zu koordinieren. Ihre Ziele sind:

- Stabiles Routing auch in sehr großen oder komplexen Netzwerken. Es sollten keine Routing-Schleifen auftreten, selbst wenn es sich um transiente Meldungen handelt.
- Schnelle Reaktion auf Änderungen in der Netzwerktopologie.

- Geringer Overhead. Das heißt, IGRP selbst sollte nicht mehr Bandbreite nutzen, als tatsächlich für seine Aufgabe benötigt wird.
- Aufteilung des Datenverkehrs auf mehrere parallele Routen, wenn diese von ungefähr gleicher Erwünschtheit sind.
- Unter Berücksichtigung der Fehlerquoten und des Datenverkehrsniveaus auf verschiedenen Pfaden.

Die aktuelle IGRP-Implementierung übernimmt das Routing für TCP/IP. Das grundlegende Design soll jedoch eine Vielzahl von Protokollen verarbeiten können.

Keines der Tools wird alle Routing-Probleme lösen. Üblicherweise ist das Routing-Problem in mehrere Teile unterteilt. Protokolle wie IGRP werden als "interne Gateway-Protokolle" (IGPs) bezeichnet. Sie sind für den Einsatz in einem einzigen Netzwerk bestimmt, entweder unter einem einzigen Management oder in einem eng koordinierten Management. Derartige Netzwerke werden über "externe Gateway-Protokolle" (EGPs) verbunden. Ein IGP ist so konzipiert, dass eine Fülle von Details zur Netzwerktopologie erfasst wird. Die Priorität beim Design eines IGP besteht darin, optimale Routen zu erstellen und schnell auf Änderungen zu reagieren. Ein EGP soll ein System von Netzwerken vor Fehlern oder vorsätzlicher Falschdarstellung durch andere Systeme schützen. BGP ist ein solches Protokoll für das externe Gateway. Bei der Konzeption eines EGP geht es vorrangig um Stabilität und Verwaltungskontrollen. Oft reicht es aus, dass ein EGP eine vernünftige Route und nicht die optimale Route schafft.

IGRP weist einige Ähnlichkeiten mit älteren Protokollen auf, z. B. das Routing Information Protocol von Xerox, das RIP in Berkeley und Dave Mills' Hello. Sie unterscheidet sich von diesen Protokollen vor allem dadurch, dass sie für größere und komplexere Netzwerke entwickelt wurden. Im Abschnitt Vergleich mit RIP finden Sie einen ausführlicheren Vergleich mit RIP, der am häufigsten von älteren Protokollgenerationen verwendet wird.

Wie bei diesen älteren Protokollen ist IGRP ein Distanzvektor-Protokoll. In einem solchen Protokoll tauschen Gateways Routing-Informationen nur mit benachbarten Gateways aus. Diese Routing-Informationen enthalten eine Zusammenfassung der Informationen zum Rest des Netzwerks. Es kann mathematisch gezeigt werden, dass alle Gateways zusammen ein Optimierungsproblem lösen, indem sie einen verteilten Algorithmus verwenden. Jedes Gateway muss nur einen Teil des Problems lösen, und es muss nur ein Teil der Gesamtdaten empfangen werden.

Die wichtigste Alternative zu IGRP ist Enhanced IGRP (EIGRP) und eine Algorithmusklasse, die als SPF bezeichnet wird (Shortest Path First). OSPF verwendet dieses Konzept. Weitere Informationen zu OSPF finden Sie im OSPF-Designleitfaden. OSPF Diese Dienste basieren auf einer Überflutungstechnik, bei der jedes Gateway über den Status jeder Schnittstelle auf jedem anderen Gateway auf dem Laufenden gehalten wird. Jedes Gateway löst das Optimierungsproblem aus seiner Sicht unabhängig mithilfe von Daten für das gesamte Netzwerk. Jeder Ansatz bietet Vorteile. In einigen Fällen kann SPF schneller auf Änderungen reagieren. Um Routingschleifen zu vermeiden, muss IGRP nach bestimmten Änderungen einige Minuten lang neue Daten ignorieren. Da SPF Informationen direkt von jedem Gateway hat, können diese Routing-Schleifen vermieden werden. Auf diese Weise kann sie sofort auf neue Informationen reagieren. SPF muss jedoch wesentlich mehr Daten als IGRP verarbeiten, sowohl in internen Datenstrukturen als auch in Nachrichten zwischen Gateways.

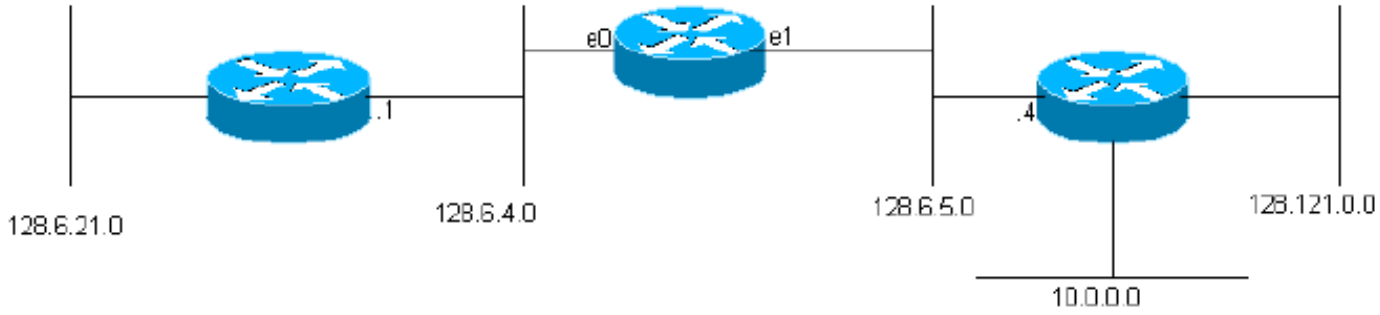
Das Routing-Problem

IGRP ist für die Verwendung in Gateways vorgesehen, die mehrere Netzwerke miteinander

verbinden. Wir gehen davon aus, dass die Netzwerke paketbasierte Technologien verwenden. Die Gateways fungieren im Prinzip als Paket-Switches. Wenn ein mit einem Netzwerk verbundenes System ein Paket an ein System in einem anderen Netzwerk senden möchte, wird es an ein Gateway adressiert. Wenn sich das Ziel in einem der Netzwerke befindet, die mit dem Gateway verbunden sind, leitet das Gateway das Paket an das Ziel weiter. Wenn das Ziel weiter entfernt ist, leitet das Gateway das Paket an ein anderes Gateway weiter, das näher am Ziel ist. Gateways verwenden Routing-Tabellen, um sie bei der Entscheidung über die Paketverwendung zu unterstützen. Nachfolgend finden Sie ein einfaches Beispiel für eine Routing-Tabelle. (Die in den Beispielen verwendeten Adressen sind IP-Adressen der Rutgers University. Beachten Sie, dass das grundlegende Routing-Problem auch für andere Protokolle ähnlich ist. Bei dieser Beschreibung wird jedoch davon ausgegangen, dass IGRP für das Routing von IP verwendet wird.)

Abbildung 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
```



(Die tatsächlichen IGRP-Routing-Tabellen enthalten zusätzliche Informationen für jedes Gateway.) Dieses Gateway ist mit zwei Ethernet-Netzwerken namens 0 und 1 verbunden. Ihnen wurden IP-Netzwerknummern (tatsächlich Subnetznummern) 128.6.4 und 128.6.5 zugewiesen. So können Pakete, die für diese spezifischen Netzwerke adressiert sind, einfach über die entsprechende Ethernet-Schnittstelle direkt an das Ziel gesendet werden. Es gibt zwei nahegelegene Gateways 128.6.4.1 und 128.6.5.4. Pakete für andere Netzwerke als 128.6.4 und 128.6.5 werden an das eine oder andere dieser Gateways weitergeleitet. Die Routing-Tabelle gibt an, welches Gateway für welches Netzwerk verwendet werden soll. Beispielsweise sollten Pakete, die an einen Host im Netzwerk 10 adressiert sind, an Gateway 128.6.5.4 weitergeleitet werden. Es ist zu hoffen, dass dieses Gateway näher an Netzwerk 10 ist, d. h. dass der beste Pfad zum Netzwerk 10 über dieses Gateway verläuft. Der Hauptzweck von IGRP besteht darin, den Gateways die Erstellung und Verwaltung von Routing-Tabellen wie diesen zu ermöglichen.

Zusammenfassung des IGRP

Wie oben erwähnt, ist IGRP ein Protokoll, das es Gateways ermöglicht, ihre Routing-Tabelle durch den Austausch von Informationen mit anderen Gateways aufzubauen. Ein Gateway beginnt mit Einträgen für alle Netzwerke, die direkt mit ihm verbunden sind. Sie erhält Informationen zu anderen Netzwerken, indem sie Routing-Updates mit benachbarten Gateways austauscht. Im einfachsten Fall findet das Gateway einen Pfad, der den besten Weg zum jeweiligen Netzwerk

darstellt. Ein Pfad zeichnet sich durch das nächste Gateway aus, an das Pakete gesendet werden sollen, die zu verwendende Netzwerkschnittstelle und metrische Informationen. Metrische Informationen sind eine Reihe von Zahlen, die angeben, wie gut der Pfad ist. So kann das Gateway Pfade vergleichen, die es von verschiedenen Gateways gehört hat, und entscheiden, welche es verwenden soll. In manchen Fällen ist es sinnvoll, den Datenverkehr auf zwei oder mehr Pfade aufzuteilen. IGRP macht dies, wenn mindestens zwei Pfade gleich gut sind. Der Benutzer kann auch so konfigurieren, dass Datenverkehr geteilt wird, wenn Pfade fast gleich gut sind. In diesem Fall wird mehr Datenverkehr über den Pfad mit der besseren Metrik gesendet. Der Datenverkehr soll auf eine 9600-Bit-Leitung und eine 19200-BPS-Leitung aufgeteilt werden können. Die 19200-Leitung erhält ungefähr doppelt so viel Datenverkehr wie die 9600-BPS-Leitung.

IGRP verwendet die folgenden Kennzahlen:

- Topologische Verzögerungszeit
- Bandbreite des engsten Bandbreitensegments des Pfades
- Kanalbelegung des Pfades
- Zuverlässigkeit des Pfads

Die topologische Verzögerungszeit ist die Zeit, die erforderlich ist, um das Ziel über diesen Pfad zu erreichen, vorausgesetzt, ein entladenes Netzwerk wird entladen. Natürlich kommt es auch zu weiteren Verzögerungen, wenn das Netzwerk geladen wird. Die Auslastung wird jedoch mithilfe der Kanalbelegung berücksichtigt, nicht durch den Versuch, tatsächliche Verzögerungen zu messen. Die Pfadbandbreite ist einfach die Bandbreite in Bit pro Sekunde der langsamsten Verbindung im Pfad. Die Kanalbelegung gibt an, wie viel dieser Bandbreite derzeit genutzt wird. Es wird gemessen und ändert sich mit der Last. Zuverlässigkeit gibt die aktuelle Fehlerrate an. Dies ist der Anteil der Pakete, die unbeschädigt am Ziel ankommen. Es wird gemessen.

Obwohl sie nicht als Teil der Kennzahl verwendet werden, werden zwei zusätzliche Informationen übergeben: Hop Count und MTU Die Hop-Anzahl ist einfach die Anzahl der Gateways, die ein Paket durchlaufen muss, um zum Ziel zu gelangen. MTU ist die maximale Paketgröße, die über den gesamten Pfad ohne Fragmentierung gesendet werden kann. (Dies ist das Minimum der MTUs aller Netzwerke, die am Pfad beteiligt sind.)

Basierend auf den metrischen Informationen wird für den Pfad eine einzige "zusammengesetzte Metrik" berechnet. Die Composite-Metrik kombiniert die Wirkung der verschiedenen metrischen Komponenten in einer einzigen Zahl, die die "Güte" dieses Pfads darstellt. Es ist die zusammengesetzte Metrik, die tatsächlich verwendet wird, um den besten Pfad zu bestimmen.

Jedes Gateway sendet in regelmäßigen Abständen seine gesamte Routing-Tabelle (wobei aufgrund der Split-Horizon-Regel etwas Zensur gilt) an alle benachbarten Gateways. Wenn ein Gateway diese Übertragung von einem anderen Gateway abruft, vergleicht es die Tabelle mit der vorhandenen Tabelle. Alle neuen Ziele und Pfade werden der Routing-Tabelle des Gateways hinzugefügt. Die Pfade im Broadcast werden mit vorhandenen Pfaden verglichen. Wenn ein neuer Pfad besser ist, kann er den vorhandenen ersetzen. Informationen im Broadcast werden auch verwendet, um die Kanalbelegung und andere Informationen über vorhandene Pfade zu aktualisieren. Dieses allgemeine Verfahren ähnelt dem aller Distanzvektor-Protokolle. Sie wird in der mathematischen Literatur als Bellman-Ford-Algorithmus bezeichnet. Unter RFC 1058 finden Sie eine detaillierte Entwicklung des Grundverfahrens, in dem RIP, ein älteres Distanzvektor-Protokoll, beschrieben wird.

Beim IGRP wird der allgemeine Bellman-Ford-Algorithmus in drei kritische Aspekte geändert. Erstens wird anstelle einer einfachen Metrik ein Metrikvektor verwendet, um Pfade zu

charakterisieren. Zweitens wird der Datenverkehr nicht auf einen einzelnen Pfad mit der kleinsten Kennzahl aufgeteilt, sondern auf mehrere Pfade, deren Kennzahlen in einen bestimmten Bereich fallen. Drittens werden mehrere Funktionen eingeführt, um Stabilität in Situationen zu gewährleisten, in denen sich die Topologie ändert.

Der beste Pfad wird anhand einer zusammengesetzten Metrik ausgewählt:

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

wobei K1, K2 = Konstanten, Be = entladene Pfadbandbreite x (1 - Kanalbelegung), Dc = topologische Verzögerung und r = Zuverlässigkeit.

Der Pfad mit der kleinsten Composite-Metrik ist der beste Pfad. Wenn mehrere Pfade zum gleichen Ziel vorhanden sind, kann das Gateway die Pakete über mehr als einen Pfad weiterleiten. Dies erfolgt entsprechend der Composite-Metrik für jeden Datenpfad. Wenn beispielsweise ein Pfad eine zusammengesetzte Metrik von 1 und ein anderer Pfad eine zusammengesetzte Metrik von 3 aufweist, werden dreimal so viele Pakete über den Datenpfad mit der zusammengesetzten Metrik von 1 gesendet.

Die Verwendung eines Vektors metrischer Informationen bietet zwei Vorteile. Zum einen können mehrere Arten von Diensten aus demselben Datensatz unterstützt werden. Der zweite Vorteil ist eine höhere Genauigkeit. Wenn eine einzige Kennzahl verwendet wird, wird sie in der Regel wie eine Verzögerung behandelt. Jeder Link im Pfad wird zur Gesamtmetrik hinzugefügt. Wenn eine Verbindung mit niedriger Bandbreite vorhanden ist, wird sie normalerweise durch eine große Verzögerung dargestellt. Bandbreitenbeschränkungen kumulieren jedoch nicht die Art und Weise, wie Verzögerungen auftreten. Wenn Bandbreite als separate Komponente behandelt wird, kann sie korrekt verarbeitet werden. Ebenso kann die Last über eine separate Kanalbelegungsnummer bewältigt werden.

IGRP bietet ein System zur Verbindung von Computernetzwerken, das stabil eine allgemeine Graphtopologie einschließlich Schleifen handhaben kann. Das System verwaltet vollständige Pfadmetrik-Informationen, d. h., es kennt die Pfadparameter zu allen anderen Netzwerken, mit denen ein Gateway verbunden ist. Der Datenverkehr kann über parallele Pfade verteilt werden, und es können mehrere Pfade-Parameter gleichzeitig über das gesamte Netzwerk berechnet werden.

Vergleich mit RIP

In diesem Abschnitt wird IGRP mit RIP verglichen. Dieser Vergleich ist nützlich, da RIP in großem Umfang für ähnliche Zwecke wie IGRP verwendet wird. Dies zu tun ist jedoch nicht ganz fair. RIP war nicht dazu gedacht, alle Ziele des IGRP zu erfüllen. RIP war für den Einsatz in kleinen Netzwerken mit relativ einheitlicher Technologie vorgesehen. Bei solchen Anwendungen ist sie im Allgemeinen ausreichend.

Der grundlegende Unterschied zwischen IGRP und RIP besteht in der Struktur der Kennzahlen. Leider ist dies keine Änderung, die einfach in RIP nachgerüstet werden kann. Sie erfordert die neuen Algorithmen und Datenstrukturen, die im IGRP vorhanden sind.

RIP verwendet zur Beschreibung des Netzwerks eine einfache Hop Count-Metrik. Im Gegensatz zu IGRP, bei dem jeder Pfad durch eine Verzögerung, Bandbreite usw. beschrieben wird, wird er im RIP durch eine Zahl zwischen 1 und 15 beschrieben. Normalerweise wird diese Nummer verwendet, um die Anzahl der Gateways anzugeben, die der Pfad durchläuft, bevor er zum Ziel

gelangt. Das bedeutet, dass keine Unterscheidung zwischen einer langsamen seriellen Leitung und einem Ethernet getroffen wird. In einigen Implementierungen von RIP kann der Systemadministrator angeben, dass ein Hop mehr als einmal gezählt werden soll. Langsame Netzwerke können durch eine hohe Hop-Anzahl dargestellt werden. Aber da das Maximum 15 ist, kann das nicht viel gemacht werden. Beispiel: Wenn ein Ethernet durch eine 1- und eine 56-KB-Leitung durch 3 dargestellt wird, können maximal 5 56-KB-Leitungen in einem Pfad vorhanden sein, oder die maximal 15-KB-Leitung wird überschritten. Um die gesamte Bandbreite der verfügbaren Netzwerkgeschwindigkeiten darzustellen und ein großes Netzwerk zu ermöglichen, legen Studien von Cisco nahe, dass eine 24-Bit-Metrik erforderlich ist. Wenn die maximale Metrik zu klein ist, hat der Systemadministrator die Wahl: Entweder kann er nicht zwischen schnellen und langsamen Routen unterscheiden, oder er kann sein gesamtes Netzwerk nicht an seine Grenzen anpassen. Tatsächlich sind inzwischen mehrere nationale Netzwerke groß genug, dass RIP sie nicht mehr bewältigen kann, selbst wenn jeder Hop nur einmal gezählt wird. RIP kann einfach nicht für solche Netzwerke verwendet werden.

Die naheliegendste Antwort wäre, RIP zu ändern, um eine größere Kennzahl zuzulassen. Leider wird das nicht funktionieren. Wie alle Distanzvektorprotokolle hat auch RIP das Problem, "bis unendlich zu zählen". Dies wird ausführlicher in RFC 1058 beschrieben. Wenn sich die Topologie ändert, werden gefälschte Routen eingeführt. Die Kennzahlen für diese falschen Routen nehmen langsam zu, bis sie 15 erreichen. An diesem Punkt werden die Routen entfernt. 15 ist ein kleines Maximum, dass dieser Prozess relativ schnell konvergiert, vorausgesetzt, dass getriggerte Updates verwendet werden. Wenn RIP so geändert wurde, dass eine 24-Bit-Metrik verwendet werden kann, bleiben Schleifen lange genug bestehen, bis die Metrik bis zu 2**24 gezählt wird. Das ist nicht hinnehmbar. Das IGRP verfügt über Funktionen, die die Einführung falscher Routen verhindern. Diese werden nachfolgend in Abschnitt 5.2 erläutert. Komplexe Netzwerke lassen sich ohne die Einführung solcher Funktionen oder das Ändern eines Protokolls wie SPF nicht handhaben.

IGRP bietet mehr als nur eine Erhöhung der zulässigen Kennzahlen. Die Kennzahlen werden neu strukturiert, um Verzögerungen, Bandbreite, Zuverlässigkeit und Last zu beschreiben. Derartige Überlegungen können in einer einzigen Metrik wie RIPs dargestellt werden. Allerdings ist der Ansatz des IGRP möglicherweise präziser. Bei einer einzigen Metrik werden beispielsweise mehrere aufeinander folgende schnelle Verbindungen einer einzelnen langsamen entsprechen. Dies kann bei interaktivem Datenverkehr der Fall sein, bei dem Verzögerungen das Hauptanliegen sind. Bei der Übertragung großer Datenmengen geht es jedoch in erster Linie um die Bandbreite, und das Hinzufügen von Metriken ist hier nicht der richtige Ansatz. IGRP verarbeitet Verzögerungen und Bandbreite separat, wodurch Verzögerungen kumuliert werden, wobei jedoch die Bandbreite auf ein Minimum reduziert wird. Es ist nicht einfach zu erkennen, wie die Auswirkungen von Zuverlässigkeit und Last in eine Einzelkomponentenmetrik integriert werden können.

Meiner Meinung nach ist eine der Hauptvorteile von IGRP die einfache Konfiguration. Es kann direkt Mengen darstellen, die eine physische Bedeutung haben. Dies bedeutet, dass sie automatisch eingerichtet werden kann, basierend auf Schnittstellentyp, Leitungsgeschwindigkeit usw. Bei einer Einzelkomponentenmetrik ist es wahrscheinlicher, dass die Metrik "gekocht" werden muss, um Effekte von mehreren verschiedenen Dingen einzubeziehen.

Andere Innovationen sind eher eine Frage von Algorithmen und Datenstrukturen als des Routing-Protokolls. IGRP gibt beispielsweise Algorithmen und Datenstrukturen an, die die Aufteilung des Datenverkehrs auf mehrere Routen unterstützen. Es ist sicherlich möglich, eine Implementierung von RIP zu entwerfen, die dies tut. Nach der Reimplementierung des Routings gibt es jedoch keinen Grund, an RIP festzuhalten.

Bisher habe ich das "generische IGRP" beschrieben, eine Technologie, die das Routing für jedes Netzwerkprotokoll unterstützen kann. In diesem Abschnitt sollte jedoch etwas mehr über die spezifische TCP/IP-Implementierung erwähnt werden. Dies ist die Implementierung, die mit RIP verglichen werden wird.

RIP-Aktualisierungsmeldungen enthalten lediglich Snapshots der Routing-Tabelle. Das heißt, sie haben eine Reihe von Zielen und metrischen Werten, und wenig mehr. Die IP-Implementierung des IGRP weist eine zusätzliche Struktur auf. Zuerst wird die Aktualisierungsmeldung durch eine "autonome Systemnummer" identifiziert. Diese Terminologie entstammt der Tradition von Arpanet und hat dort eine besondere Bedeutung. Für die meisten Netzwerke bedeutet dies jedoch, dass Sie mehrere verschiedene Routing-Systeme im selben Netzwerk ausführen können. Dies ist für Orte nützlich, an denen Netzwerke aus verschiedenen Organisationen konvergieren. Jedes Unternehmen kann sein eigenes Routing beibehalten. Da jede Aktualisierung mit einem Label versehen ist, können Gateways so konfiguriert werden, dass nur die richtige Technologie berücksichtigt wird. Bestimmte Gateways sind so konfiguriert, dass sie Updates von mehreren autonomen Systemen empfangen. Sie geben Informationen auf kontrollierte Weise zwischen den Systemen weiter. Beachten Sie, dass dies keine vollständige Lösung für Probleme bei der Routing-Sicherheit ist. Jedes Gateway kann so konfiguriert werden, dass es Aktualisierungen von jedem autonomen System abhört. Es ist jedoch weiterhin ein sehr nützliches Tool für die Implementierung von Routing-Richtlinien, bei denen ein angemessenes Maß an Vertrauen zwischen den Netzwerkadministratoren besteht.

Die zweite strukturelle Funktion von IGRP-Aktualisierungsmeldungen beeinflusst die Art und Weise, wie IGRP Standardrouten behandelt. Die meisten Routing-Protokolle haben ein Standardrouten-Konzept. Routing-Updates sind häufig nicht in der Lage, jedes Netzwerk weltweit aufzulisten. In der Regel benötigen eine Reihe von Gateways detaillierte Routing-Informationen für die Netzwerke in ihrem Unternehmen. Der gesamte Datenverkehr für Ziele außerhalb der Organisation kann an eines der wenigen Grenz-Gateways gesendet werden. Diese Grenz-Gateways können umfassendere Informationen haben. Die Route zum besten Begrenzungs-Gateway ist eine "Standardroute". Es ist ein Standard, der verwendet wird, um zu einem Ziel zu gelangen, das nicht speziell in den internen Routing-Updates aufgeführt ist. RIP und einige andere Routing-Protokolle geben Informationen über die Standardroute so weiter, als handele es sich um ein echtes Netzwerk. IGRP verfolgt einen anderen Ansatz. IGRP ermöglicht es, echte Netzwerke als Standard zu kennzeichnen, anstatt nur einen falschen Eintrag für die Standardroute zu verwenden. Dies wird implementiert, indem Informationen zu diesen Netzwerken in einem speziellen externen Abschnitt der Aktualisierungsmeldung platziert werden. Es kann jedoch auch davon ausgegangen werden, dass es sich um ein mit diesen Netzwerken verbundenes Stück handelt. Regelmäßiges IGRP scannt alle Standardrouten der Kandidaten und wählt die Route mit der niedrigsten Metrik als tatsächliche Standardroute aus.

Potenziell ist dieser Ansatz für Standardwerte etwas flexibler als der Ansatz der meisten RIP-Implementierungen. In der Regel können RIP-Gateways so konfiguriert werden, dass sie eine Standardroute mit einer bestimmten Metrik generieren. Dies soll auf Grenzgateways geschehen.

Detaillierte Beschreibung

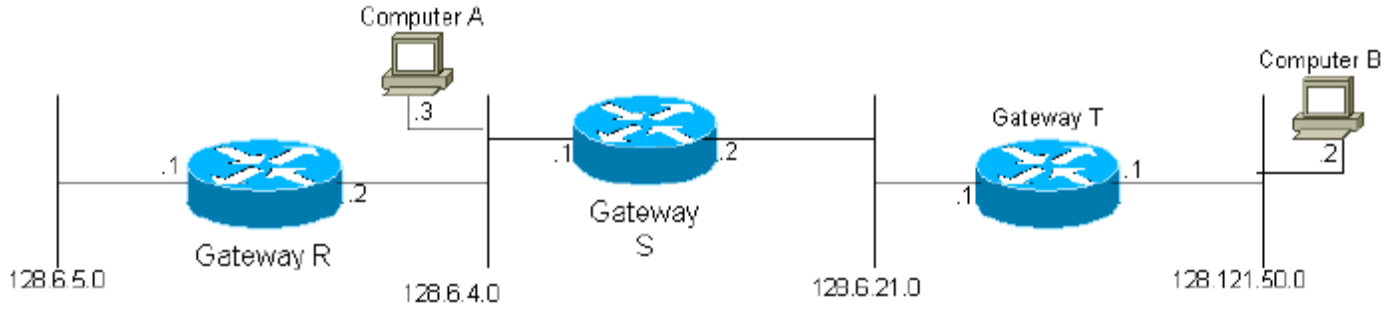
Dieser Abschnitt enthält eine detaillierte Beschreibung des IGRP.

Allgemeine Beschreibung

Wenn ein Gateway zum ersten Mal eingeschaltet wird, wird seine Routing-Tabelle initialisiert. Dies

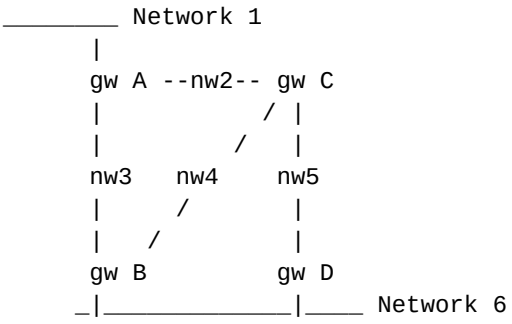
kann von einem Operator über ein Konsolenterminal oder durch Lesen von Informationen aus Konfigurationsdateien erfolgen. Es wird eine Beschreibung jedes mit dem Gateway verbundenen Netzwerks bereitgestellt, einschließlich der topologischen Verzögerung entlang der Verbindung (z. B. die Dauer der Übertragung über ein einzelnes Bit) und der Bandbreite der Verbindung.

Abbildung 2



Im obigen Diagramm wird beispielsweise Gateway S angewiesen, über die entsprechenden Schnittstellen mit den Netzwerken 2 und 3 verbunden zu sein. Daher weiß Gateway 2 zunächst nur, dass es in den Netzwerken 2 und 3 jeden Zielcomputer erreichen kann. Alle Gateways sind so programmiert, dass sie die Informationen, mit denen sie initialisiert wurden, sowie die Informationen, die von anderen Gateways gesammelt wurden, regelmäßig an ihre benachbarten Gateways übermitteln. Gateway S erhält daher Updates von den Gateways R und T und lernt, dass er Computer in Netzwerk 1 über Gateway R und Computer in Netzwerk 4 über Gateway T erreichen kann. Da Gateway S seine gesamte Routing-Tabelle sendet, wird Gateway T im nächsten Zyklus erfahren, dass das Gateway 1 über Gateway S erreichen kann. Es ist leicht zu erkennen, dass Informationen über jedes Netzwerk im System letztendlich alle Gateways im System erreichen, vorausgesetzt, das Netzwerk ist vollständig verbunden.

Abbildung 3



Jedes Gateway berechnet eine zusammengesetzte Metrik, um die Zweckmäßigkeit der Datenpfade zu den Zielcomputern zu bestimmen. Im obigen Diagramm würde beispielsweise Gateway A (gw A) für ein Ziel in Netzwerk 6 metrische Funktionen für zwei Pfade über Gateways B und C berechnen. Beachten Sie, dass Pfade einfach durch den nächsten Hop definiert werden. Es gibt tatsächlich drei mögliche Routen von A nach Netzwerk 6:

- Direkt an B
- An C und dann an B
- An C und dann an D

Gateway A muss jedoch nicht zwischen den beiden Routen wählen, die C beinhalten. Die Routing-Tabelle in A hat einen einzigen Eintrag, der den Pfad zu C darstellt. Die Metrik stellt die

beste Möglichkeit dar, von C zum endgültigen Ziel zu gelangen. Wenn A ein Paket an C sendet, muss C entscheiden, ob B oder D verwendet werden soll.

Gleichung 1

Die für die einzelnen Datenpfade berechnete zusammengesetzte metrische Funktion ist wie folgt:

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

wobei r = fraktionale Zuverlässigkeit (% der Übertragungen, die am nächsten Hop erfolgreich empfangen wurden), Dc = Composite-Verzögerung, Be = effektive Bandbreite: entladene Bandbreite x (1 Kanalbelegung) und K1 und K2 = Konstanten.

Gleichung 2

Grundsätzlich könnte die Composite-Verzögerung, Dc, wie folgt bestimmt werden:

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

Ds = Switching-Verzögerung, Dcir = Schaltungsverzögerung (Übertragungsverzögerung von 1 Bit) und DT = Übertragungsverzögerung (Verzögerung ohne Last für eine 1500-Bit-Nachricht).

In der Praxis wird jedoch für jeden Netzwerktechnologietyp eine standardmäßige Verzögerungszahl verwendet. Beispielsweise wird eine standardmäßige Verzögerungszahl für Ethernet und für serielle Leitungen mit einer bestimmten Bitrate angegeben.

Im Beispiel unten sehen Sie die Routing-Tabelle von Gateway A im obigen Diagramm für Netzwerk 6. (Beachten Sie, dass einzelne Komponenten des metrischen Vektors aus Gründen der Einfachheit nicht angezeigt werden.)

Beispiel für eine Routing-Tabelle:

Netzwerk	Schnittstelle	Nächstes Gateway	Kennzahl
1	NW 1	Keine	Direkt verbunden
2	NW 2	Keine	Direkt verbunden
1	NW 3	Keine	Direkt verbunden
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

Der grundlegende Prozess zum Erstellen einer Routing-Tabelle durch den Austausch von Informationen mit Nachbarn wird durch den Bellman-Ford-Algorithmus beschrieben. Der Algorithmus wurde in früheren Protokollen wie RIP (RFC 1058) verwendet. Für komplexere

Netzwerke fügt IGRP dem Bellman-Ford-Basisalgorithmus drei Funktionen hinzu:

1. Anstelle einer einfachen Metrik wird ein Metrikvektor verwendet, um Pfade zu charakterisieren. Aus diesem Vektor kann eine einzelne zusammengesetzte Metrik gemäß Gleichung 1, oben, berechnet werden. Durch die Verwendung eines Vektors kann das Gateway verschiedene Arten von Diensten aufnehmen, indem verschiedene Koeffizienten in Gleichung 1 verwendet werden. Außerdem können die Netzwerkmerkmale genauer dargestellt werden als eine einzelne Metrik.
2. Anstatt einen einzelnen Pfad mit der kleinsten Kennzahl auszuwählen, wird der Datenverkehr auf mehrere Pfade aufgeteilt, deren Kennzahlen in einen bestimmten Bereich fallen. Dies ermöglicht die parallele Verwendung mehrerer Routen, wodurch eine größere effektive Bandbreite als bei jeder einzelnen Route entsteht. Eine Variante V wird vom Netzwerkadministrator angegeben. Alle Pfade mit minimalen zusammengesetzten Metriken M werden beibehalten. Darüber hinaus werden alle Pfade, deren Metrik weniger als V x M ist, beibehalten. Der Datenverkehr wird im umgekehrten Verhältnis zu den zusammengesetzten Metriken auf mehrere Pfade verteilt.
3. Mit diesem Varianzkonzept gibt es einige Probleme. Strategien, bei denen Varianzwerte größer als 1 verwendet werden und die nicht auch zu Paketschleifen führen, sind schwierig zu finden. In Cisco Version 8.2 ist die Varianzfunktion nicht implementiert. (Ich bin mir nicht sicher, in welcher Version die Funktion entfernt wurde.) Dadurch wird die Varianz dauerhaft auf 1 festgelegt.
4. Es werden mehrere Funktionen eingeführt, um Stabilität in Situationen zu gewährleisten, in denen sich die Topologie ändert. Diese Funktionen sollen Routing-Schleifen und "Zählen bis Unendlichkeit" verhindern, die frühere Versuche zur Verwendung von Ford-Algorithmen für diese Art von Anwendung charakterisiert haben. Die wichtigsten Stabilitätsfunktionen sind "Holddowns", "Triggered Updates", "Split Horizon" und "Poisoning". Diese werden nachfolgend ausführlicher behandelt.

Die Aufteilung des Datenverkehrs (Nummer 2) stellt eine relativ geringe Gefahr dar. Die Variante V ist so konzipiert, dass Gateways parallele Pfade unterschiedlicher Geschwindigkeiten verwenden können. Aus Redundanzgründen kann es beispielsweise vorkommen, dass eine 9600-BPS-Leitung parallel zu einer 19200-BPS-Leitung ausgeführt wird. Wenn die Variante V 1 ist, wird nur der beste Pfad verwendet. Die BPS-Leitung 9600 wird also nicht verwendet, wenn die BPS-Leitung des 19200 über eine angemessene Zuverlässigkeit verfügt. (Wenn jedoch mehrere Pfade identisch sind, wird die Last von ihnen gemeinsam genutzt.) Durch die Erhöhung der Varianz kann der Datenverkehr zwischen der besten Route und anderen, fast ebenso guten Routen aufgeteilt werden. Bei ausreichender Abweichung wird der Datenverkehr auf die beiden Leitungen aufgeteilt. Die Gefahr besteht darin, dass mit einer ausreichenden Varianz Pfade zugelassen werden, die nicht nur langsamer sind, sondern tatsächlich "in die falsche Richtung" führen. Daher sollte eine zusätzliche Regel vorhanden sein, um zu verhindern, dass Datenverkehr "Upstream" gesendet wird: Es wird kein Datenverkehr über Pfade gesendet, deren Metrik für Remote-Composite (die zusammengesetzte Metrik, berechnet am nächsten Hop) größer ist als die am Gateway berechnete Metrik für Composite. Im Allgemeinen wird Systemadministratoren empfohlen, die Varianz nicht über 1 zu setzen, außer in bestimmten Situationen, in denen parallele Pfade verwendet werden müssen. In diesem Fall wird die Varianz sorgfältig eingestellt, um die "richtigen" Ergebnisse zu liefern.

IGRP ist für die Verarbeitung mehrerer "Service-Typen" und mehrerer Protokolle vorgesehen. Type of Service ist eine Spezifikation in einem Datenpaket, die die Art und Weise ändert, wie Pfade ausgewertet werden. Das TCP/IP-Protokoll ermöglicht es dem Paket beispielsweise, die relative Wichtigkeit hoher Bandbreite, niedriger Verzögerung oder hoher Zuverlässigkeit

anzugeben. Im Allgemeinen werden interaktive Anwendungen eine geringe Verzögerung angeben, während Anwendungen für Massenübertragungen eine hohe Bandbreite angeben. Diese Anforderungen bestimmen die relativen Werte von K1 und K2, die für die Verwendung in Eq geeignet sind. 1. Jede Kombination von Spezifikationen im zu unterstützenden Paket wird als "Servicetyp" bezeichnet. Für jeden Servicetyp müssen die Parameter K1 und K2 ausgewählt werden. Für jeden Servicetyp wird eine Routing-Tabelle gespeichert. Dies geschieht, weil Pfade ausgewählt und entsprechend der durch Eq. definierten zusammengesetzten Metrik sortiert werden. 1. Dies ist für jeden Servicetyp unterschiedlich. Die Informationen aus allen Routing-Tabellen werden so kombiniert, dass die Routing-Update-Meldungen, die von den Gateways ausgetauscht werden, wie in Abbildung 7 beschrieben, erstellt werden.

Stabilitätsmerkmale

In diesem Abschnitt werden Holddowns, ausgelöste Updates, Split Horizon und Vergiftung beschrieben. Diese Funktionen sollen verhindern, dass Gateways fehlerhafte Routen annehmen. Wie in RFC 1058 beschrieben, kann dies passieren, wenn eine Route aufgrund eines Ausfalls eines Gateways oder eines Netzwerks nicht mehr verwendbar ist. Grundsätzlich erkennen die benachbarten Gateways Ausfälle. Anschließend senden sie Routing-Updates, die die alte Route als nicht verwendbar anzeigen. Updates können jedoch nicht in bestimmte Teile des Netzwerks gelangen oder sich bei der Erreichbarkeit bestimmter Gateways verzögern. Ein Gateway, der immer noch der Meinung ist, dass die alte Route gut ist, kann diese Informationen weiter verbreiten und so die ausgefallene Route wieder in das System eingeben. Nach einiger Zeit werden diese Informationen über das Netzwerk weitergeleitet und an das Gateway zurückgesendet, von dem sie erneut eingespeist werden. Das Ergebnis ist eine zirkuläre Route.

Tatsächlich gibt es bei den Gegenmaßnahmen eine gewisse Redundanz. Im Prinzip sollten Holddowns und ausgelöste Updates ausreichen, um fehlerhafte Routen überhaupt zu verhindern. In der Praxis können jedoch Kommunikationsfehler unterschiedlicher Art dazu führen, dass sie nicht ausreichen. Split Horizon und Routenvergiftung sollen Routing-Schleifen in jedem Fall verhindern.

Normalerweise werden neue Routing-Tabellen regelmäßig (standardmäßig alle 90 Sekunden, jedoch vom Systemadministrator angepasst) an benachbarte Gateways gesendet. Ein getriggertes Update ist eine neue Routing-Tabelle, die als Reaktion auf eine Änderung sofort gesendet wird. Die wichtigste Änderung ist das Entfernen einer Route. Dies kann auftreten, weil ein Timeout abgelaufen ist (wahrscheinlich ist ein benachbartes Gateway oder eine Leitung nicht verfügbar) oder eine Aktualisierungsmeldung vom nächsten Gateway im Pfad zeigt, dass der Pfad nicht mehr verwendbar ist. Wenn ein Gateway G erkennt, dass eine Route nicht mehr verwendbar ist, löst es sofort ein Update aus. Dieses Update zeigt an, dass diese Route nicht verwendbar ist. Überlegen Sie, was geschieht, wenn dieses Update die benachbarten Gateways erreicht. Wenn die Route des Nachbarn zurück zu G zeigt, muss der Nachbar die Route entfernen. Dies bewirkt, dass der Nachbar ein Update auslöst usw. Ein Fehler löst eine Welle von Aktualisierungsmeldungen aus. Diese Welle breitet sich über den Teil des Netzwerks aus, in dem Routen durch das ausgefallene Gateway oder Netzwerk verlaufen.

Getriggerte Updates wären ausreichend, wenn wir garantieren könnten, dass die Flut an Updates sofort jedes geeignete Gateway erreicht. Es gibt jedoch zwei Probleme. Zuerst können Pakete, die die Aktualisierungsmeldung enthalten, verworfen oder durch eine Verbindung im Netzwerk beschädigt werden. Zweitens erfolgen die angestoßenen Updates nicht sofort. Es ist möglich, dass ein Gateway, das das getriggerte Update noch nicht erhalten hat, gerade zur falschen Zeit ein regelmäßiges Update ausgibt, wodurch die fehlerhafte Route in einen Nachbarn zurückgesetzt wird, der das getriggerte Update bereits erhalten hat. Holddowns wurden entwickelt, um diese

Probleme zu umgehen. Die Holddown-Regel besagt, dass beim Entfernen einer Route für dieselbe Route für einen bestimmten Zeitraum keine neue Route akzeptiert wird. Dadurch haben Sie genügend Zeit, um alle anderen Gateways zu erreichen, sodass wir sicher sein können, dass alle neuen Routen nicht nur ein Gateway zum Einsetzen des alten Gateways sind. Die Ausfallzeit muss so lang sein, dass die Welle ausgelöster Updates im gesamten Netzwerk stattfinden kann. Darüber hinaus sollte es einige regelmäßige Broadcast-Zyklen umfassen, um verlorene Pakete zu behandeln. Stellen Sie sich vor, was passiert, wenn eines der getriggerten Updates verworfen oder beschädigt wird. Das Gateway, das dieses Update herausgegeben hat, wird beim nächsten regulären Update erneut aktualisiert. Dadurch wird die Welle ausgelöster Updates bei Nachbarn neu gestartet, die die anfängliche Welle verpasst haben.

Die Kombination aus ausgelösten Updates und Holddowns sollte ausreichen, um abgelaufene Routen zu entfernen und zu verhindern, dass diese wieder eingesetzt werden. Einige zusätzliche Vorsichtsmaßnahmen sind jedoch dennoch sinnvoll. Sie ermöglichen sehr verlustbehaftete Netzwerke und Netzwerke, die inzwischen partitioniert sind. Die vom IGRP geforderten zusätzlichen Vorsichtsmaßnahmen sind Split Horizon und Route Poisoning. Split Horizont ergibt sich aus der Beobachtung, dass es nie sinnvoll ist, eine Route zurück in die Richtung zu senden, aus der sie kam. Betrachten Sie folgende Situation:

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

Gateway A weist B darauf hin, dass es eine Route zu Netzwerk 1 hat. Wenn B Updates an A sendet, gibt es keinen Grund, Netzwerk 1 zu erwähnen. Da A näher an 1 ist, gibt es keinen Grund, die Umstellung über B in Erwägung zu ziehen. Die Split Horizon-Regel besagt, dass für jeden Nachbarn (eigentlich jedes Nachbarnetzwerk) eine separate Aktualisierungsmeldung generiert werden sollte. Das Update für einen bestimmten Nachbarn sollte Routen auslassen, die auf diesen Nachbarn zeigen. Diese Regel verhindert Schleifen zwischen benachbarten Gateways. Beispiel: Die Schnittstelle von A zu Netzwerk 1 schlägt fehl. Ohne die Split Horizon-Regel würde B A sagen, dass es zu 1 kommen kann. Da es keine echte Route mehr gibt, könnte A diese Route nehmen. In diesem Fall hätten A und B beide Routen zu 1. Aber A verweist auf B und B auf A. Natürlich sollten ausgelöste Updates und Ausfälle verhindern, dass dies geschieht. Aber da es keinen Grund gibt, Informationen an den Ort zurückzuschicken, von dem sie stammen, lohnt sich Split Horizon trotzdem. Zusätzlich zu seiner Rolle bei der Verhinderung von Schleifen hält Split Horizon die Größe der Aktualisierungsnachrichten niedrig.

Split Horizon sollte Schleifen zwischen benachbarten Gateways verhindern. Die Vergiftung der Route dient dazu, größere Schleifen zu brechen. Die Regel ist, dass eine Schleife vorhanden ist, wenn ein Update die Metrik für eine vorhandene Route anzeigt, um ausreichend erhöht zu sein. Die Route sollte entfernt und in Holddown gesetzt werden. Derzeit besteht die Regel darin, dass eine Route entfernt wird, wenn die zusammengesetzte Metrik größer als der Faktor 1,1 ist. Es ist nicht sicher, dass nur eine Erhöhung der Verbundmetrik das Entfernen der Route auslöst, da kleine metrische Änderungen aufgrund von Änderungen bei der Kanalbelegung oder der Zuverlässigkeit auftreten können. Der Faktor 1,1 ist also nur heuristisch. Der genaue Wert ist nicht entscheidend. Wir gehen davon aus, dass diese Regel nur benötigt wird, um sehr große Schleifen zu brechen, da kleine Loops durch ausgelöste Updates und Holddowns verhindert werden.

Holddowns deaktivieren

Ab Version 8.2 bietet der Code von Cisco die Möglichkeit, Holddowns zu deaktivieren. Der Nachteil von Holddowns besteht darin, dass sie die Einführung einer neuen Route verzögern, wenn eine alte Route ausfällt. Bei Standardparametern kann es einige Minuten dauern, bis ein

Router nach einer Änderung eine neue Route einführt. Aus den oben genannten Gründen ist es jedoch nicht sicher, einfach Holddowns zu entfernen. Wie in RFC 1058 beschrieben, würde das Ergebnis auf Unendlichkeit zählen. Wir vermuten, aber können nicht beweisen, dass mit einer stärkeren Version der Routenvergiftung Holddowns nicht mehr nötig sind, um die Zahl bis zur Unendlichkeit aufzuhalten. Die Deaktivierung von Holddowns ermöglicht eine stärkere Form der Routenvergiftung. Beachten Sie, dass Split Horizon und getriggerte Updates noch in Kraft sind.

Die stärkere Form der Routenvergiftung beruht auf einer Hopfenanzahl. Wenn die Hop-Anzahl für einen Pfad steigt, wird die Route entfernt. Dadurch werden natürlich noch gültige Routen entfernt. Wenn sich an einem anderen Ort im Netzwerk etwas ändert, sodass der Pfad nun über ein weiteres Gateway verläuft, erhöht sich die Hop-Anzahl. In diesem Fall ist die Route noch gültig. Es gibt jedoch keine sichere Möglichkeit, diesen Fall von Routing-Schleifen (Anzahl bis Unendlichkeit) zu unterscheiden. Der sicherste Ansatz besteht daher darin, die Route bei einer Erhöhung der Hop-Anzahl zu entfernen. Wenn die Route immer noch legitim ist, wird sie bei der nächsten Aktualisierung neu installiert, was zu einem ausgelösten Update führt, das die Route an anderer Stelle im System neu installiert.

Im Allgemeinen nehmen Distanzvektor-Algorithmen1 ganz einfach neue Routen an. Das Problem besteht darin, alte vollständig aus dem System zu entfernen. Daher sollte eine Regel, die zu aggressiv ist, um verdächtige Routen zu entfernen, sicher sein.

Details des Aktualisierungsprozesses

Die in den Abbildungen 4 bis 8 beschriebenen Prozesse sollen ein einzelnes Netzwerkprotokoll behandeln, z. B. TCP/IP, DECnet oder das ISO/OSI-Protokoll. Die Protokolldetails werden jedoch nur für TCP/IP angegeben. Ein einzelnes Gateway kann Daten verarbeiten, die mehr als einem Protokoll folgen. Da jedes Protokoll unterschiedliche Adressierungsstrukturen und Paketformate hat, wird der Computercode für die Implementierung der Abbildungen 4 bis 8 für jedes Protokoll im Allgemeinen unterschiedlich sein. Der in Abbildung 4 beschriebene Prozess variiert am häufigsten, wie in den detaillierten Hinweisen zu Abbildung 4 beschrieben. Die in den Abbildung 5 bis 8 beschriebenen Prozesse weisen dieselbe allgemeine Struktur auf. Der Hauptunterschied zwischen Protokoll und Protokoll besteht im Format des Routing-Update-Pakets, das so ausgelegt sein muss, dass es mit einem bestimmten Protokoll kompatibel ist.

Beachten Sie, dass die Definition eines Ziels von Protokoll zu Protokoll variieren kann. Die hier beschriebene Methode kann für das Routing zu einzelnen Hosts, zu Netzwerken oder für komplexere hierarchische Adressschemata verwendet werden. Welche Art von Routing verwendet wird, hängt von der Adressierungsstruktur des Protokolls ab. Die aktuelle TCP/IP-Implementierung unterstützt nur das Routing zu IP-Netzwerken. "Ziel" bedeutet also tatsächlich IP-Netzwerk- oder Subnetznummer. Subnetzinformationen werden nur für verbundene Netzwerke gespeichert.

Die Abbildungen 4 bis 7 zeigen den Pseudocode für verschiedene Teile des Routing-Prozesses, die von den Gateways verwendet werden. Zu Beginn des Programms werden akzeptable Protokolle und Parameter eingegeben, die jede Schnittstelle beschreiben.

Das Gateway verarbeitet nur bestimmte Protokolle, die aufgelistet sind. Jede Kommunikation von einem System, das ein Protokoll verwendet, das nicht in der Liste enthalten ist, wird ignoriert. Die Dateneingaben sind wie folgt:

- Netzwerke, mit denen das Gateway verbunden ist.
- Entladene Bandbreite jedes Netzwerks
- Topologische Verzögerung jedes Netzwerks

- Zuverlässigkeit der einzelnen Netzwerke.
- Kanalbelegung in jedem Netzwerk.
- MTU der einzelnen Netzwerke

Die metrische Funktion für jeden Datenpfad wird dann gemäß Gleichung 1 berechnet. Beachten Sie, dass die ersten drei Posten relativ dauerhaft sind. Sie sind eine Funktion der zugrunde liegenden Netzwerktechnologie und sind nicht von der Last abhängig. Sie können aus einer Konfigurationsdatei oder durch direkte Operatoreingabe festgelegt werden. Beachten Sie, dass IGRP keine gemessene Verzögerung verwendet. Sowohl Theorie als auch Erfahrung deuten darauf hin, dass es für Protokolle, die eine gemessene Verzögerung verwenden, sehr schwierig ist, ein stabiles Routing aufrechtzuerhalten. Es gibt zwei Messwerte: Zuverlässigkeit und Kanalbelegung. Die Zuverlässigkeit basiert auf Fehlerquoten, die von der Hardware oder Firmware der Netzwerkschnittstelle gemeldet wurden.

Darüber hinaus erfordert der Routing-Algorithmus einen Wert für mehrere Routing-Parameter. Dazu gehören Timer-Werte, Varianz und ob Holddowns aktiviert sind. Dies wird normalerweise durch eine Konfigurationsdatei oder eine Operatoreingabe angegeben. (Ab Cisco Version 8.2 ist die Abweichung dauerhaft auf 1 festgelegt.)

Sobald die ersten Informationen eingegeben wurden, werden Vorgänge im Gateway durch Ereignisse ausgelöst - entweder durch das Eintreffen eines Datenpakets an einer der Netzwerkschnittstellen oder durch den Ablauf eines Timers. Die in den Abbildungen 4 bis 7 beschriebenen Prozesse werden wie folgt ausgelöst:

- Wenn ein Paket eingeht, wird es gemäß Abbildung 4 verarbeitet. Dadurch wird das Paket an eine andere Schnittstelle gesendet, verworfen oder zur weiteren Verarbeitung akzeptiert.
- Wenn ein Paket vom Gateway zur weiteren Verarbeitung akzeptiert wird, wird es auf protokollspezifische Weise analysiert, die in dieser Spezifikation nicht beschrieben ist. Wenn es sich bei dem Paket um ein Routing-Update handelt, wird es gemäß Abbildung 5 verarbeitet.
- Abbildung 6 zeigt Ereignisse, die von einem Zeitgeber ausgelöst wurden. Der Timer ist so eingestellt, dass einmal pro Sekunde eine Unterbrechung generiert wird. Wenn das Interrupt auftritt, wird der in Abbildung 6 dargestellte Prozess ausgeführt.
- Abbildung 7 zeigt eine Unterroutine für Routing-Updates. Anrufe an diese Unterroutine sind in den Abbildungen 5 und 6 dargestellt.
- Abbildung 8 zeigt außerdem Einzelheiten der in den Abbildungen 5 und 7 genannten metrischen Berechnungen.

Es gibt vier kritische Zeitkonstanten, die die Weiterleitung und den Ablauf von Routen steuern. Diese Zeitkonstanten können vom Systemadministrator festgelegt werden. Es gibt jedoch Standardwerte. Diese Zeitkonstanten sind:

- Broadcast Time (Sendezeit): Updates werden in dieser Zeit von allen Gateways an allen verbundenen Schnittstellen übertragen. Der Standardwert ist einmal alle 90 Sekunden.
- Ungültige Zeit - Wenn für einen bestimmten Pfad innerhalb dieser Zeit keine Aktualisierung empfangen wurde, gilt dies als Zeitüberschreitung. Die Sendezeit sollte mehrmals betragen, damit Pakete, die ein Update enthalten, vom Netzwerk verworfen werden können. Der Standardwert ist das Dreifache der Sendezeit.
- Haltezeit - Wenn ein Ziel nicht erreichbar ist (oder die Metrik so stark angestiegen ist, dass es vergiftet wird), geht das Ziel in "Holddown". Während dieses Zustands wird für dasselbe Ziel für diesen Zeitraum kein neuer Pfad akzeptiert. Die Haltezeit gibt an, wie lange dieser Zustand andauern soll. Die Sendezeit sollte mehrere Male betragen. Der Standardwert ist das

Dreifache der Sendezeit plus 10 Sekunden. (Wie im Abschnitt Deaktivierung von Haltepunkten beschrieben, können Holddowns deaktiviert werden.)

- Pleasedauer - Wenn innerhalb dieser Zeit für ein bestimmtes Ziel keine Aktualisierung empfangen wurde, wird der Eintrag für dieses Ziel aus der Routing-Tabelle entfernt. Beachten Sie den Unterschied zwischen ungültiger Zeit und Leerlaufzeit: Nach der ungültigen Zeit wird ein Pfad nach dem Timeout beendet und entfernt. Wenn keine weiteren Pfade zu einem Ziel vorhanden sind, ist das Ziel jetzt nicht erreichbar. Der Datenbankeintrag für das Ziel bleibt jedoch erhalten. Es muss bleiben, den Holddown durchzusetzen. Nach der Leerlaufzeit wird der Datenbankeintrag aus der Tabelle entfernt. Er sollte etwas länger sein als die ungültige Zeit plus die Ausfallzeit. Der Standardwert ist das 7-fache der Sendezeit.

Diese Zahlen setzen die folgenden wichtigen Datenstrukturen voraus. Für jedes vom Gateway unterstützte Protokoll wird ein separater Satz dieser Datenstrukturen aufbewahrt. Innerhalb jedes Protokolls wird ein separater Satz von Datenstrukturen für jeden unterstützten Diensttyp beibehalten.

Für jedes dem System bekannte Ziel gibt es eine (möglicherweise NULL-)Liste von Pfaden zum Ziel, eine Haltefrist und eine letzte Aktualisierungszeit. Die letzte Aktualisierungszeit gibt an, wann ein Pfad für dieses Ziel zum letzten Mal von einem anderen Gateway aktualisiert wurde. Beachten Sie, dass für jeden Pfad auch Aktualisierungszeiten gespeichert werden. Wenn der letzte Pfad zu einem Ziel entfernt wird, wird das Ziel in Holddown gesetzt, es sei denn, Holddowns sind deaktiviert (weitere Informationen finden Sie im Abschnitt Deaktivierung von Haltepunkten). Die Haltedauer gibt an, zu welchem Zeitpunkt das Holddown abläuft. Die Tatsache, dass sie nicht 0 ist, zeigt an, dass sich das Ziel im Holddown befindet. Um die Berechnungszeit zu sparen, empfiehlt es sich auch, für jedes Ziel eine "beste Kennzahl" zu verwenden. Dies ist einfach die Mindestanzahl der zusammengesetzten Metriken für alle Pfade zum Ziel.

Für jeden Pfad zu einem Ziel gibt es die Adresse des nächsten Hop im Pfad, die zu verwendende Schnittstelle, einen Messvektor, der den Pfad charakterisiert, einschließlich topologischer Verzögerung, Bandbreite, Zuverlässigkeit und Kanalbelegung. Weitere Informationen sind auch mit jedem Pfad verknüpft, einschließlich Hop Count, MTU, Informationsquelle, der Remote-Composite-Metrik und einer zusammengesetzten Metrik, die aus diesen Zahlen nach Gleichung 1 berechnet wird. Es gibt auch eine letzte Aktualisierung. Die Informationsquelle gibt an, woher das letzte Update für diesen Pfad stammte. In der Praxis entspricht dies der Adresse des nächsten Hop. Die letzte Aktualisierungszeit ist einfach der Zeitpunkt, zu dem das letzte Update für diesen Pfad angekommen ist. Sie wird verwendet, um Pfade mit abgelaufenem Ablaufdatum zu erstellen.

Beachten Sie, dass eine IGRP-Aktualisierungsnachricht aus drei Teilen besteht: Intern, System (bedeutet "dieses autonome System", aber nicht Innen) und Außen. Der interne Abschnitt dient der Weiterleitung zu Subnetzen. Nicht alle Subnetzinformationen sind enthalten. Es sind nur Subnetze eines Netzwerks enthalten. Dies ist das Netzwerk, dem die Adresse zugeordnet ist, an die das Update gesendet wird. In der Regel werden Updates auf jeder Schnittstelle gesendet. Dies ist also einfach das Netzwerk, auf dem der Broadcast gesendet wird. (Andere Fälle können bei Antworten auf IGRP-Anfragen und IGRP-Point-to-Point-Anfragen auftreten.) Größere Netzwerke (z. B. Nicht-Subnetze) werden in den Systemteil der Aktualisierungsnachricht eingefügt, es sei denn, sie werden ausdrücklich als "extern" gekennzeichnet.

Ein Netzwerk wird als extern markiert, wenn es von einem anderen Gateway gelernt wurde und die Informationen im äußeren Teil der Aktualisierungsnachricht eintreffen. Dank der Implementierung von Cisco kann der Systemadministrator bestimmte Netzwerke auch als Außenbereiche deklarieren. Exteriore Routen werden auch als "Kandidat default" bezeichnet. Es handelt sich um Routen, die zu oder über Gateways gehen, die als Standard gelten und bei denen keine explizite Route zu einem Ziel verwendet wird. Bei Rutgers konfigurieren wir beispielsweise

das Gateway, das Rutgers mit unserem regionalen Netzwerk verbindet, sodass es die Route zum NSFnet-Backbone als außen markiert. Die Implementierung von Cisco wählt eine Standardroute aus, indem sie diese externe Route mit der kleinsten Kennzahl auswählt.

In den folgenden Abschnitten werden bestimmte Teile der Abbildungen 4 bis 8 erläutert.

Paketrouting

Abbildung 4 beschreibt die Gesamtverarbeitung von Eingabepaketen. Dies dient lediglich der Klärung der Terminologie. Dies ist offensichtlich keine vollständige Beschreibung dessen, was ein IP-Gateway tut.

Bei diesem Prozess werden die Liste der unterstützten Protokolle und die bei der Initialisierung des Gateways eingegebenen Schnittstelleninformationen verwendet. Die Details der Paketverarbeitung hängen vom vom vom Paket verwendeten Protokoll ab. Dies wird in Schritt A bestimmt. Schritt A ist der einzige Teil von Abbildung 4, der von allen Protokollen gemeinsam genutzt wird. Sobald der Protokolltyp bekannt ist, wird die für den Protokolltyp geeignete Abbildung 4 implementiert. Details zum Paketinhalt sind in den Spezifikationen des Protokolls beschrieben. Zu den Spezifikationen eines Protokolls gehören ein Verfahren zur Bestimmung des Ziels eines Pakets, ein Verfahren zum Vergleich des Ziels mit den eigenen Adressen des Kabelmodems, um festzustellen, ob das Gateway selbst das Ziel ist, ein Verfahren zur Bestimmung, ob es sich bei einem Paket um eine Broadcast-Verbindung handelt, und ein Verfahren zur Bestimmung, ob das Ziel Teil eines bestimmten Netzwerks ist. Diese Verfahren werden in den Schritten B und C in Abbildung 4 verwendet. Der Test in Schritt D erfordert eine Suche nach den in der Routing-Tabelle aufgeführten Zielen. Der Test ist zufrieden, wenn in der Routing-Tabelle ein Eintrag für das Ziel vorhanden ist und dieses Ziel mindestens einem verwendbaren Pfad zugeordnet wurde. Beachten Sie, dass die in diesem und im nächsten Schritt verwendeten Ziel- und Pfaddaten für jeden unterstützten Diensttyp separat verwaltet werden. In diesem Schritt wird zunächst der vom Paket angegebene Servicetyp bestimmt und der entsprechende Satz von Datenstrukturen für diesen und den nächsten Schritt ausgewählt.

Ein Pfad kann für die Zwecke der Schritte D und E verwendet werden, wenn seine Metrik für Remote-Composite-Elemente kleiner ist als ihre Composite-Metrik. Ein Pfad, dessen Remote-Composite-Metrik größer ist als seine Composite-Metrik, ist ein Pfad, dessen nächster Hop, gemessen anhand der Metrik, "weiter entfernt" vom Ziel ist. Dies wird als "Upstream-Pfad" bezeichnet. Normalerweise würde man erwarten, dass die Verwendung von Metriken die Auswahl von Upstream-Pfaden verhindern würde. Es ist leicht zu erkennen, dass ein Upstream-Pfad niemals der beste sein kann. Wenn jedoch eine große Abweichung erlaubt ist, können andere Pfade als die beste verwendet werden. Einige davon könnten Upstream sein.

Schritt E berechnet den zu verwendenden Pfad. Pfade, deren Remote-Composite-Metrik nicht kleiner als ihre Composite-Metriken ist, werden nicht berücksichtigt. Wenn mehr als ein Pfad zulässig ist, werden diese Pfade in einer gewichteten Form des Round-Robin-Wechsels verwendet. Die Frequenz, mit der ein Pfad verwendet wird, ist umgekehrt proportional zu seiner zusammengesetzten Metrik.

Empfang von Routing-Updates

Abbildung 5 beschreibt die Verarbeitung eines Routing-Updates, der von einem benachbarten Gateway empfangen wurde. Solche Aktualisierungen bestehen aus einer Liste von Einträgen, die jeweils Informationen für ein einzelnes Ziel enthalten. Bei einem Routing-Update können mehrere Einträge für dasselbe Ziel eingegeben werden, um mehrere Arten von Services zu unterstützen.

Jeder dieser Einträge wird individuell verarbeitet, wie in Abbildung 5 beschrieben. Befindet sich ein Eintrag im äußeren Bereich der Aktualisierung, wird das äußere Flag für das Ziel festgelegt, wenn es als Ergebnis dieses Prozesses hinzugefügt wird.

Der gesamte in Abbildung 5 beschriebene Prozess muss einmal für jeden vom Gateway unterstützten Servicetyp wiederholt werden, wobei die Zielinformationen bzw. Pfadinformationen zu diesem Servicetyp zu verwenden sind. Dies wird in der äußersten Schleife in Abbildung 5 gezeigt. Das gesamte Routing-Update muss für jeden Servicetyp einmal verarbeitet werden. (Beachten Sie, dass die aktuelle IGRP-Implementierung nicht mehrere Arten von Diensten unterstützt, sodass die äußerste Schleife nicht tatsächlich implementiert ist.)

In Schritt A werden grundlegende Akzeptanztests auf dem Pfad durchgeführt. Dies sollte auch Plausibilitätstests für das Ziel umfassen. Unmögliche ("Martian") Netzwerknummern sollten abgelehnt werden. (Weitere Informationen finden Sie in RFC 1009 und RFC 1122 .) Aktualisierungen werden auch dann abgelehnt, wenn sich das Ziel, auf das sie sich beziehen, im Holddown-Menü befindet, d. h. die Haltedauer nicht 0 und später als die aktuelle Zeit ist.

In Schritt B wird die Routing-Tabelle durchsucht, um festzustellen, ob dieser Eintrag einen bereits bekannten Pfad beschreibt. Ein Pfad in der Routing-Tabelle wird definiert durch das Ziel, mit dem er verknüpft ist, den nächsten Hop, der als Teil des Pfads aufgeführt ist, die für den Pfad zu verwendende Ausgabeschnittstelle und die Informationsquelle (die Adresse, von der das Update stammt - in der Praxis entspricht dies in der Regel dem nächsten Hop). Der Eintrag aus dem Aktualisierungspaket beschreibt einen Pfad, dessen Ziel im Eintrag aufgeführt ist, dessen Ausgabeschnittstelle die Schnittstelle ist, in der das Update einging, und dessen nächster Hop und Informationsquelle die Adresse des Gateways sind, das das Update gesendet hat (der "Quell"-S).

In Schritt H und Schritt T ist der in Abbildung 7 beschriebene Aktualisierungsvorgang geplant. Dieser Prozess wird tatsächlich ausgeführt, nachdem der gesamte in Abbildung 5 beschriebene Prozess abgeschlossen ist. Das heißt, der in Abbildung 7 beschriebene Aktualisierungsvorgang findet nur einmal statt, auch wenn er bei der Verarbeitung, wie in Abbildung 5 beschrieben, mehrmals ausgelöst wird. Darüber hinaus müssen Vorkehrungen getroffen werden, um zu verhindern, dass Updates zu häufig durchgeführt werden, wenn sich das Netzwerk schnell ändert.

Schritt K wird durchgeführt, wenn das durch den aktuellen Eintrag im Aktualisierungspaket beschriebene Ziel bereits in der Routing-Tabelle vorhanden ist. K vergleicht die neue zusammengesetzte Metrik, die aus Daten im Aktualisierungspaket berechnet wurde, mit der besten zusammengesetzten Metrik für das Ziel. Beachten Sie, dass die beste zusammengesetzte Metrik zu diesem Zeitpunkt nicht neu berechnet wird. Wenn sich der zu prüfende Pfad also bereits in der Routing-Tabelle befindet, kann dieser Test neue und alte Metriken für denselben Pfad vergleichen.

Schritt L wird für die Pfade ausgeführt, die schlechter sind als die vorhandene beste Composite-Metrik. Dies schließt sowohl neue Pfade ein, die schlechter sind als bestehende, als auch vorhandene Pfade, deren zusammengesetzte Metrik gestiegen ist. Schritt L prüft, ob der neue Pfad zulässig ist. Beachten Sie, dass dieser Test sowohl den Test auf die Frage implementiert, ob ein neuer Pfad gut genug ist, um zu behalten, als auch die Weiterleitung von Vergiftungen. Um akzeptabel zu sein, darf der Verzögerungswert nicht der Sonderwert sein, der auf ein nicht erreichbares Ziel hinweist (bei der aktuellen IP-Implementierung alle Werte in einem 24-Bit-Feld), und die zusammengesetzte Metrik (berechnet wie in Abbildung 8 angegeben) muss akzeptabel sein. Um festzustellen, ob die zusammengesetzte Metrik zulässig ist, vergleichen Sie sie mit den zusammengesetzten Metriken aller anderen Pfade zum Ziel. Lassen Sie mich das Mindeste davon sein. Der neue Pfad ist akzeptabel, wenn er < V X M ist, wobei V DER VARIANZ-SATZ IST, WENN DAS GATEWAY INITIALISIERT WURDE. WENN V = 1 (DAS IST IMMER BEI CISCO

VERSION 8.2 GÜLTIG), IST EIN METRIKT, DER SCHLIESSLICH IST ALS DER VORHANDENE, NICHT AKZEPTABEL. AUSGENOMMEN: WENN DER PFAD BEREITS VORHANDEN IST UND DER EINZIGE PFAD ZUM ZIEL IST, WIRD DER PFAD ERHALTEN, WENN DER METRIKT NICHT UM MEHR ALS 10 % ERHÖHT WURDE (ODER WENN DIE ANZAHL DER HOP NICHT ERHÖHT WURDE).

Schritt V wird ausgeführt, wenn die neuen Informationen für einen Pfad darauf hinweisen, dass die zusammengesetzte Metrik verringert wird. Die zusammengesetzten Metriken aller Pfade zum Ziel D werden verglichen. In diesem Vergleich wird die neue zusammengesetzte Metrik für P verwendet, nicht die in der Routing-Tabelle. Die minimale zusammengesetzte Metrik M wird berechnet. Dann werden alle Pfade zu D erneut untersucht. Wenn die zusammengesetzte Metrik für einen Pfad > M x V ist, wird dieser Pfad entfernt. V ist die Variable, die bei Initialisierung des Gateways eingegeben wurde. (Ab Cisco Version 8.2 ist die Abweichung dauerhaft auf 1 festgelegt.)

Regelmäßige Verarbeitung

Der in Abbildung 6 beschriebene Prozess wird einmal pro Sekunde ausgelöst. Dabei werden verschiedene Timer in der Routing-Tabelle geprüft, um festzustellen, ob ein Timer abgelaufen ist. Diese Timer werden oben beschrieben.

In Schritt U wird der in Abbildung 7 beschriebene Prozess aktiviert.

Schritt R und Schritt S sind erforderlich, da die in der Routing-Tabelle gespeicherten zusammengesetzten Metriken von der Kanalbelegung abhängen, die sich je nach Messung im Laufe der Zeit ändert. Die Kanalbelegung wird regelmäßig neu berechnet, wobei der gemessene Datenverkehr durch die Schnittstelle fließt. Wenn sich der neu berechnete Wert von dem vorhandenen unterscheidet, müssen alle zusammengesetzten Metriken für diese Schnittstelle angepasst werden. Jeder in der Routing-Tabelle angezeigte Pfad wird geprüft. Bei jedem Pfad, dessen nächster Hop die Schnittstelle "I" verwendet, wird die Composite-Metrik neu berechnet. Dies erfolgt gemäß Gleichung 1, wobei als Kanalbelegung der maximal in der Routing-Tabelle gespeicherte Wert als Teil der Pfadmetrik und die neu berechnete Kanalbelegung der Schnittstelle verwendet werden.

Nachrichten erstellen

Abbildung 7 beschreibt, wie das Gateway Aktualisierungsmeldungen generiert, die an andere Gateways gesendet werden. Für jede Netzwerkschnittstelle, die an das Gateway angeschlossen ist, wird eine separate Nachricht generiert. Diese Nachricht wird dann an alle anderen Gateways gesendet, die über die Schnittstelle erreichbar sind (Schritt J). Im Allgemeinen geschieht dies durch Senden der Nachricht als Broadcast. Wenn jedoch die Netzwerktechnologie oder das Netzwerkprotokoll keine Broadcasts zulässt, kann es erforderlich sein, die Nachricht einzeln an jedes Gateway zu senden.

Im Allgemeinen wird die Nachricht durch Hinzufügen eines Eintrags für jedes Ziel in der Routing-Tabelle in Schritt G erstellt. Beachten Sie, dass die Ziel-/Pfaddaten, die den einzelnen Servicetypen zugeordnet sind, verwendet werden müssen. Im schlimmsten Fall wird dem Update für jedes Ziel für jeden Diensttyp ein neuer Eintrag hinzugefügt. Bevor Sie jedoch in Schritt G der Aktualisierungsmeldung einen Eintrag hinzufügen, werden die bereits hinzugefügten Einträge gescannt. Wenn der neue Eintrag bereits in der Aktualisierungsmeldung vorhanden ist, wird er nicht erneut hinzugefügt. Ein neuer Eintrag dupliziert einen vorhandenen Eintrag, wenn die Ziele und die nächsten Hop-Gateways identisch sind.

Aus Gründen der Einfachheit lässt der Pseudocode eines außen vor: IGRP-Aktualisierungsnachrichten bestehen aus drei Teilen: Innen-, System- und Außenbereiche, d. h. es gibt drei Schleifen über Ziele. Das erste umfasst nur Subnetze des Netzwerks, an das das Update gesendet wird. Das zweite umfasst alle großen Netzwerke (z. B. Nicht-Subnetze), die nicht als Außenbereiche gekennzeichnet sind. Die dritte Kategorie umfasst alle großen Netzwerke, die als Außenbereiche gekennzeichnet sind.

Schritt E implementiert den Split Horizon-Test. Im normalen Fall schlägt dieser Test bei Routen fehl, deren bestmöglicher Pfad dieselbe Schnittstelle verlässt, die auch die Aktualisierung aussendet. Wenn das Update jedoch an ein bestimmtes Ziel gesendet wird (z. B. als Reaktion auf eine IGRP-Anfrage von einem anderen Gateway oder als Teil von "Point-to-Point IGRP"), schlägt Split Horizon nur fehl, wenn der beste ursprünglich von diesem Ziel stammende Pfad stammt (seine "Informationsquelle" ist dieselbe wie das Ziel) und seine Ausgabeschnittstelle dieselbe ist wie die, von der die Anforderung stammt.

Computing-Metrik-Informationen

Abbildung 8 beschreibt, wie die metrischen Informationen aus Aktualisierungsmeldungen verarbeitet werden, die vom Gateway empfangen wurden, und wie diese Informationen für Aktualisierungsmeldungen generiert werden, die vom Gateway gesendet werden. Beachten Sie, dass der Eintrag auf einem bestimmten Pfad zum Ziel basiert. Wenn es mehr als einen Pfad zum Ziel gibt, wird ein Pfad ausgewählt, dessen zusammengesetzte Metrik mindestens ist. Wenn mehr als ein Pfad über die minimale zusammengesetzte Metrik verfügt, wird eine beliebige zeitkritische Regel verwendet. (Bei den meisten Protokollen basiert dies auf der Adresse des nächsten Hop-Gateways.)

Abbildung 4: Verarbeiten eingehender Pakete

```
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.
```

Abbildung 5: Verarbeiten eingehender Routing-Updates

```
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
```

Abbildung 6: Periodische Verarbeitung

```
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
```

Abbildung 7: Aktualisieren generieren

```
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
```

Abbildung 8: Details der metrischen Berechnungen

In diesem Abschnitt wird die Vorgehensweise für die Berechnung von Metriken und Hop-Zählungen bei einem eingehenden Routing-Update beschrieben. Die Eingabe für diese Funktion ist der Eintrag für ein bestimmtes Ziel in einem Routing-Update-Paket. Die Ausgabe ist ein Vektor von Metriken, die zur Berechnung der zusammengesetzten Metrik verwendet werden können, und eine Hop-Zählung. Wenn dieser Pfad der Routing-Tabelle hinzugefügt wird, wird der gesamte Metrikvektor in die Tabelle eingegeben. Die in den folgenden Definitionen verwendeten Schnittstellenparameter sind die Parameter, die bei der Initialisierung des Gateways für die Schnittstelle festgelegt wurden, auf der die Routing-Aktualisierung angekommen ist. Die Kanalbelegung und -zuverlässigkeit basieren jedoch auf einem gleitenden Durchschnitt des gemessenen Datenverkehrs durch die Schnittstelle.

- Verzögerung = Verzögerung bei der topologischen Verzögerung von Paket + Schnittstelle
- Bandbreite = max. (Bandbreite vom Paket, Schnittstellenbandbreite)

- Zuverlässigkeit = min (Zuverlässigkeit von Paket, Schnittstellenzuverlässigkeit)
- Kanalbelegung = max (Kanalbelegung aus Paket, Schnittstellenkanal-Belegung)(Max wird für Bandbreite verwendet, da die Bandbreitenmetrik in umgekehrter Form gespeichert wird. Grundsätzlich wollen wir die Mindestbandbreite.) Beachten Sie, dass die ursprüngliche Kanalbelegung aus dem Paket gespeichert werden muss, da diese benötigt wird, um die effektive Kanalbelegung bei jeder Änderung der Kanalbelegung neu zu berechnen.

Die folgenden Elemente sind nicht Teil des metrischen Vektors, sondern werden auch in der Routing-Tabelle als Merkmale des Pfads beibehalten:

- Hop count = Hop Count von Paket.
- MTU = min (MTU von Paket, Interface MTU).
- Remote-Composite-Metrik = berechnet aus Gleichung 1 unter Verwendung der metrischen Werte aus dem Paket. Das heißt, die metrischen Komponenten stammen aus dem Paket und werden nicht wie oben gezeigt aktualisiert. Dies muss natürlich vor den oben beschriebenen Anpassungen berechnet werden.
- Mischmetrik = berechnet aus Gleichung 1 unter Verwendung der gemäß diesem Abschnitt berechneten metrischen Werte.

Im verbleibenden Teil dieses Abschnitts werden die Verfahren für die Computing-Kennzahlen und die Hop-Anzahl für das Senden von Routing-Updates beschrieben.

Diese Funktion legt die metrischen Informationen und die Hop-Anzahl fest, die in ein ausgehendes Aktualisierungspaket eingegeben werden sollen. Es basiert auf einem bestimmten Pfad zu einem Ziel, wenn es irgendwelche verwendbaren Pfade gibt. Wenn keine Pfade vorhanden sind oder die Pfade alle Upstream-Pfade sind, wird das Ziel als "unzugänglich" bezeichnet.

```
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.
```

Details zur IP-Implementierung

In diesem Abschnitt werden die vom Cisco IGRP verwendeten Paketformate beschrieben. IGRP wird mithilfe von IP-Datagrammen mit IP Protocol 9 (IGP) gesendet. Das Paket beginnt mit einem Header. Er beginnt unmittelbar nach dem IP-Header.

```
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 */
```

Bei Aktualisierungsmeldungen folgen die Routing-Informationen unmittelbar nach dem Header.

Die Versionsnummer ist derzeit 1. Pakete mit anderen Versionsnummern werden ignoriert.

Der Opcode kann 1 = update oder 2 = request sein.

Zeigt den Meldungstyp an. Das Format der beiden Meldungstypen wird nachfolgend angegeben.

Edition ist eine Seriennummer, die bei jeder Änderung der Routing-Tabelle erhöht wird. (Dies geschieht unter den Bedingungen, unter denen im obigen Pseudocode angegeben wird, dass ein Routing-Update ausgelöst wird.) Mit der Editionsnummer können Gateways Updates mit bereits bekannten Informationen nicht verarbeiten. (Dies ist derzeit nicht implementiert. Das heißt, die Editionsnummer wird korrekt generiert, aber sie wird bei der Eingabe ignoriert. Da Pakete verworfen werden können, ist nicht klar, ob die Edition-Nummer ausreicht, um eine doppelte Verarbeitung zu vermeiden. Es muss sichergestellt werden, dass alle der Edition zugeordneten Pakete verarbeitet wurden.)

Ein System ist die autonome Systemnummer. Bei der Cisco Implementierung kann ein Gateway an mehr als einem autonomen System teilnehmen. Jedes dieser Systeme führt ein eigenes IGRP-Protokoll aus. Konzeptionell gibt es für jedes autonome System völlig separate Routing-Tabellen. Routen, die über IGRP von einem autonomen System eintreffen, werden nur in Aktualisierungen für dieses AS gesendet. In diesem Feld kann das Kabelmodem festlegen, welche Routingtabellen für die Verarbeitung dieser Nachricht verwendet werden sollen. Wenn das Gateway eine IGRP-Nachricht für ein AS empfängt, für das es nicht konfiguriert ist, wird diese ignoriert. Bei der Implementierung von Cisco können Informationen von einem AS in ein anderes übertragen werden. Ich halte das jedoch für ein Verwaltungstool und nicht für einen Teil des Protokolls.

Intern, *systemintern* und *nebenbei* geben die Anzahl der Einträge in jedem der drei Abschnitte der Aktualisierungsmeldungen an. Diese Abschnitte wurden oben beschrieben. Es gibt keine andere Abgrenzung zwischen den Abschnitten. Die ersten Inneneinträge gelten als Innenräume, die nächsten Systemeinträge als System und die letzte als Außenbereich.

Prüfsumme ist eine IP-Prüfsumme, die mit demselben Prüfsummenalgorithmus wie eine UDP-Prüfsumme berechnet wird. Die Prüfsumme wird auf dem IGRP-Header und allen zugehörigen Routing-Informationen berechnet. Das Prüfsummenfeld wird bei der Berechnung der Prüfsumme auf Null gesetzt. Die Prüfsumme enthält weder den IP-Header noch einen virtuellen Header wie in UDP und TCP.

Anfragen

Bei einer IGRP-Anfrage wird der Empfänger aufgefordert, seine Routing-Tabelle zu senden. Die Anforderungsnachricht hat nur einen Header. Es werden nur die Felder Version, Opcode und System verwendet. Alle anderen Felder sind 0. Es wird erwartet, dass der Empfänger eine normale IGRP-Aktualisierungsmeldung an den Antragsteller sendet.

Aktualisierungen

Eine IGRP-Aktualisierungsnachricht enthält einen Header, gefolgt von Routingeinträgen. Es sind so viele Routingeinträge enthalten, dass sie in ein 1500-Byte-Datagramm passen (einschließlich IP-Header). Bei aktuellen Strukturdeklarationen sind damit bis zu 104 Einträge möglich. Wenn mehr Einträge benötigt werden, werden mehrere Aktualisierungsmeldungen gesendet. Da Aktualisierungsnachrichten einfach nur für die Eingabe verarbeitet werden, gibt es keinen Vorteil,

eine einzelne fragmentierte Nachricht anstelle mehrerer unabhängiger Nachrichten zu verwenden.

Die Struktur eines Routing-Eintrags ist wie folgt:

```
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 */
```

Bei den Feldern uchar[2] und uchar[3] handelt es sich einfach um 16- und 24-Bit-Binärzahlen in normaler IP-Netzwerkreihenfolge.

Nummer definiert das zu beschreibende Ziel. Es ist eine IP-Adresse. Um Platz zu sparen, werden nur die ersten 3 Byte der IP-Adresse angegeben, außer im inneren Abschnitt. Im inneren Bereich werden die letzten 3 Bytes angegeben. Für System- und Außenrouten sind keine Subnetze möglich, daher ist das Byte in niedriger Reihenfolge immer 0. Interne Routen sind immer Subnetze eines bekannten Netzwerks, sodass das erste Byte dieser Netzwerknummer angegeben wird.

Die Verzögerung liegt in Einheiten von 10 Mikrosekunden. Das ergibt einen Bereich von 10 bis 168 Sekunden, was ausreichend erscheint. Eine Verzögerung aller weist darauf hin, dass das Netzwerk nicht erreichbar ist.

Die Bandbreite wird in Bits pro Sekunde umgekehrt, die um den Faktor 1,0e10 skaliert werden. Der Bereich reicht von 1200 BPS bis zu 10 Gbit/s. (Wenn die Bandbreite N Kbit/s beträgt, wird 1000000/N verwendet.)

MTU ist in Byte angegeben.

Die Zuverlässigkeit wird als Bruchteil von 255 angegeben. Das heißt, 255 sind 100 %.

Die Last wird als Bruchteil von 255 angegeben.

Hop Count ist eine einfache Zählung.

Aufgrund der etwas seltsamen Einheiten, die für Bandbreite und Verzögerung verwendet werden, scheinen einige Beispiele in Ordnung zu sein. Dies sind die Standardwerte, die für mehrere gängige Medien verwendet werden.

	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

Metrische Berechnungen

Im Folgenden wird beschrieben, wie die zusammengesetzte Metrik in Cisco Version 8.0(3) tatsächlich berechnet wird.

```
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
```

Zugehörige Informationen

- Support-Seite für IP-Routing
- IGRP-Support-Seite
- Technischer Support - Cisco Systems