

# Een Inleiding tot IGRP

## Inhoud

[Inleiding](#)

[Doelstellingen voor IGRP](#)

[Het routingprobleem](#)

[Samenvatting van IGRP](#)

[Vergelijking met RIP](#)

[Gedetailleerde beschrijving](#)

[Algemene beschrijving](#)

[Stabiliteitskenmerken](#)

[Holddowns uitschakelen](#)

[Bijzonderheden van het actualiseringsproces](#)

[Packet-routing](#)

[Ontvang van routingupdates](#)

[Periodieke verwerking](#)

[Update berichten genereren](#)

[Metrische informatie berekenen](#)

[Details van de IP-implementatie](#)

[Verzoeken](#)

[updates](#)

[Metrische berekeningen](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document introduceert Interior Gateway Routing Protocol (IGRP). Het heeft twee doelen. De eerste is het vormgeven van een introductie aan de IGRP-technologie, voor degenen die geïnteresseerd zijn in het gebruik, evalueren en mogelijk uitvoeren ervan. De andere is om een bredere bekendheid te geven aan een aantal interessante ideeën en concepten die in de IGRP zijn opgenomen. Raadpleeg [het configureren IGRP, de IGRP Implementatie](#) en [IGRP Opdrachten](#) voor informatie over hoe u IGRP kunt configureren.

## Doelstellingen voor IGRP

Het IGRP protocol staat een aantal gateways toe om hun routing te coördineren. De doelstellingen zijn:

- Stabiele routing zelfs in zeer grote of complexe netwerken. Geen routinglijnen zouden moeten voorkomen, zelfs als transities.
- Snelle respons op veranderingen in netwerktopologie.

- Lage overhead. Dat wil zeggen, IGRP zelf zou niet meer bandbreedte moeten gebruiken dan wat echt nodig is voor zijn taak.
- Splitsen van het verkeer over verschillende parallelle routes wanneer deze ruwweg even wenselijk zijn.
- Rekening houden met foutenpercentages en het verkeersniveau op verschillende paden.

De huidige implementatie van IGRP behandelt routing voor TCP/IP. Het basisontwerp is echter bedoeld om verschillende protocollen te kunnen behandelen.

Geen enkel gereedschap zal alle routingproblemen oplossen. conventioneel is het routingprobleem in verschillende stukken gebroken. Protocols zoals IGRP worden "interne gateway protocols" (IGP's) genoemd. Ze zijn bedoeld voor gebruik binnen één reeks netwerken, hetzij onder één beheer, hetzij onder nauw gecoördineerd beheer. Zulke groepen netwerken worden aangesloten door "externe gateway Protocols" (EGP's). Een IGP wordt ontworpen om bij te houden van veel details over netwerktopologie. Bij het ontwerpen van een IGP wordt voorrang gegeven aan het produceren van optimale routes en snel reageren op veranderingen. Een EGP is bedoeld om één systeem van netwerken te beschermen tegen fouten of opzettelijke verkeerde voorstelling door andere systemen. BGP is zo'n Buitengewoon toegangprotocol. Bij het ontwerpen van een EGP is voorrang gegeven aan stabiliteit en administratieve controles. Vaak is het voldoende voor een EGP om een redelijke route te produceren in plaats van de optimale route.

IGRP heeft enige gelijkenissen met oudere protocollen zoals Xerox's Routing Information Protocol, Berkeley's RIP en Dave Mills' Hello. Het verschilt voornamelijk van deze protocollen door ontworpen te zijn voor grotere en complexere netwerken. Zie de sectie [Vergelijking met RIP](#) voor een meer gedetailleerde vergelijking met RIP, de meest gebruikte van de oudere generatie protocollen.

Zoals deze oudere protocollen is IGRP een afstandsvectorprotocol. In zo een protocol wisselen gateways routeinformatie uit slechts met aangrenzende gateways. Deze routeinformatie bevat een samenvatting van informatie over de rest van het netwerk. Het kan wiskundig worden aangetoond dat alle gateways samen een optimalisatieprobleem oplossen door wat op een gedistribueerd algoritme neerkomt. Elke gateway hoeft slechts een deel van het probleem op te lossen, en hoeft alleen een deel van de totale gegevens te ontvangen.

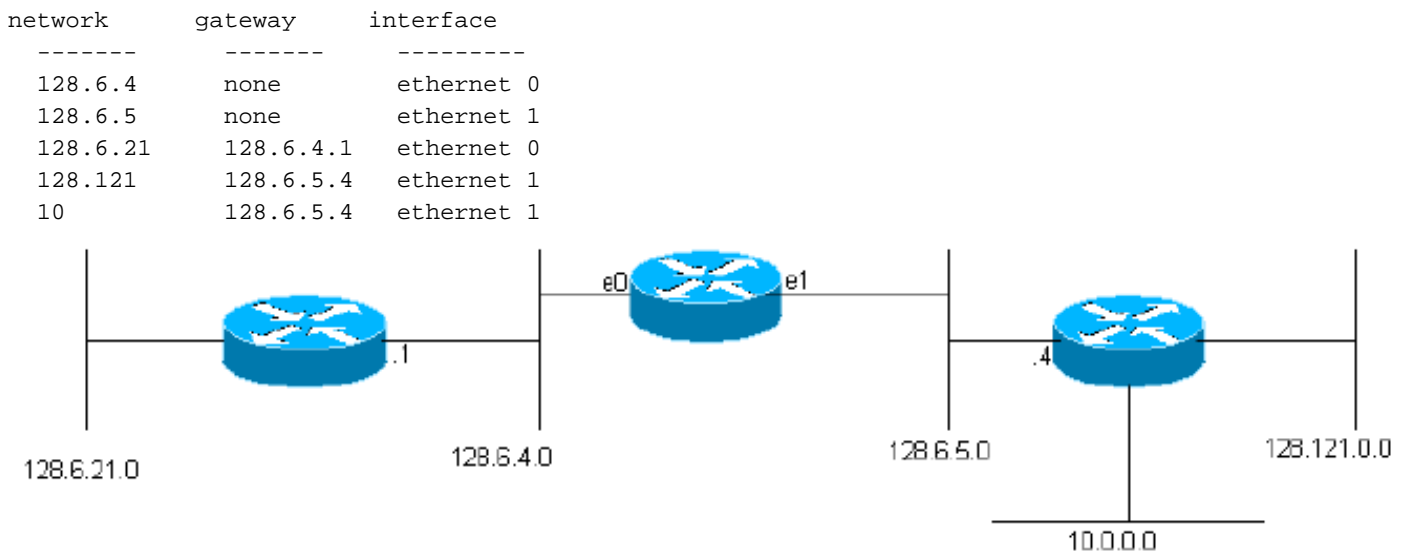
Het belangrijkste alternatief voor IGRP is [Enhanced IGRP \(DHCP\)](#) en een klasse van algoritmen die als SPF (kortst pad eerst) worden aangeduid. OSPF gebruikt dit concept. Om meer over OSPF te weten te komen verwijst naar [OSPF Design Guide](#). OSPF Deze zijn gebaseerd op een overstrometechniek, waar elke gateway op de hoogte wordt gehouden van de status van elke interface op elke andere poort. Elke gateway lost het optimalisatieprobleem onafhankelijk op vanuit zijn standpunt met behulp van gegevens voor het gehele netwerk. Elke benadering heeft voordelen. In sommige gevallen kan SPF sneller reageren op veranderingen. Om het verzenden van loops te verhinderen, moet IGRP nieuwe gegevens voor een paar minuten na bepaalde soorten veranderingen negeren. Omdat SPF informatie direct van elke gateway heeft, kan het deze routinglijnen vermijden. Zij kan dus onmiddellijk op nieuwe informatie reageren. SPF moet echter veel meer gegevens verwerken dan IGRP, zowel in interne gegevensstructuren als in berichten tussen gateways.

## [Het routingprobleem](#)

IGRP is bedoeld voor gebruik in gateways die verschillende netwerken verbinden. We gaan ervan uit dat de netwerken pakketgebaseerde technologie gebruiken. In feite doen de gateways dienst als pakketswitches. Wanneer een systeem dat is aangesloten op een netwerk een pakket naar

een systeem op een ander netwerk wil verzenden, richt het het pakket naar een gateway. Als de bestemming op een van de netwerken is aangesloten die op de gateway worden aangesloten, zal de gateway het pakket naar de bestemming doorsturen. Als de bestemming verder weg is, zal de gateway het pakket naar een andere gateway doorsturen die dichterbij de bestemming is. gateways gebruiken routingtabellen om hen te helpen beslissen wat ze met pakketten doen. Hier is een eenvoudig voorbeeld dat tabel routeert. (De adressen die in de voorbeelden worden gebruikt zijn IP adressen van de Universiteit van Rutgers. Merk op dat het basisroutingprobleem ook voor andere protocollen vergelijkbaar is, maar deze beschrijving zal ervan uitgaan dat IGRP gebruikt wordt voor het routeren van IP.)

**Figuur 1**



(Feitelijke IGRP-routingtabellen hebben aanvullende informatie voor elke gateway, zoals we zullen zien.) Deze gateway is aangesloten op twee Ethernet, genaamd 0 en 1. Ze hebben IP-netwerkgetallen (eigenlijk subnetnummers) 128.6.4 en 128.6.5 gekregen. Dus kunnen pakketten die voor deze specifieke netwerken zijn bedoeld rechtstreeks naar de bestemming worden verzonden, eenvoudig door gebruik te maken van de juiste Ethernet-interface. Er zijn twee nabijgelegen gateways, 128.6.4.1 en 128.6.5.4. Packets voor netwerken anders dan 128.6.4 en 128.6.5 zullen naar een of de andere van die gateways worden doorgestuurd. De routingtabel geeft aan welke gateway moet worden gebruikt voor welk netwerk. Zo moeten pakketten die op een host op netwerk 10 zijn gericht, naar gateway 128.6.5.4 worden doorgestuurd. Je hoopt dat deze gateway dichterbij netwerk 10 ligt, d.w.z. dat de beste route naar netwerk 10 door deze gateway gaat. Het primaire doel van IGRP is toe te staan de gateways om routingstabellen zoals deze te bouwen en onderhouden.

## Samenvatting van IGRP

Zoals hierboven vermeld is IGRP een protocol dat gateways toestaat om hun routingtabel op te bouwen door informatie met andere gateways uit te wisselen. Een gateway begint met ingangen voor alle netwerken die er direct op zijn aangesloten. Het krijgt informatie over andere netwerken door het uitwisselen van routingupdates met aangrenzende gateways. In het eenvoudigste geval, zal de gateway één pad vinden dat de beste manier om aan elk netwerk te krijgen vertegenwoordigt. Een pad wordt gekarakteriseerd door de volgende gateway naar welke pakketten worden verzonden, de netwerkinterface die zou moeten worden gebruikt en metrische informatie. Metrische informatie is een verzameling getallen die weergeven hoe goed het pad is.

Dit laat de gateway toe om wegen te vergelijken die het van verschillende gateways heeft gehoord en beslist welke te gebruiken. Er zijn vaak gevallen waar het zin heeft om verkeer tussen twee of meer paden te splitsen. IGRP zal dit doen wanneer twee of meer paden even goed zijn. De gebruiker kan de modus ook configureren om verkeer te splitsen wanneer paden bijna even goed zijn. In dit geval zal meer verkeer langs het pad met de betere metriek worden verzonden. De bedoeling is dat het verkeer kan worden gesplitst tussen een 9600 bps lijn en een 19200 BPS lijn, en de 19200 lijn zal ruwweg twee keer zoveel verkeer krijgen als de 9600 BPS lijn.

De door IGRP gebruikte metriek omvat het volgende:

- Topologische vertragingstijd
- Bandbreedte van het kleinste bandbreedte-segment van het pad
- Kanaalbezetting van het pad
- Betrouwbaarheid van het pad

Topologische vertragingstijd is de hoeveelheid tijd die het zou kosten om naar de bestemming langs dat pad te gaan, uitgaande van een ongeladen netwerk. Er is natuurlijk extra vertraging wanneer het netwerk wordt geladen. De belasting wordt echter verantwoord met behulp van het bezettingsgetal van het kanaal, niet door te proberen de werkelijke vertraging te meten. De padbandbreedte is eenvoudig de bandbreedte in bits per seconde van de traagste link in het pad. De bezettingsgraad van het kanaal wijst op hoeveel van die bandbreedte momenteel in gebruik is. Het wordt gemeten en zal met de lading veranderen. Betrouwbaarheid geeft het huidige foutenpercentage aan. Het is het deel van de pakketten dat onbeschadigd op de bestemming aankomt. Het wordt gemeten.

Hoewel ze niet als onderdeel van de metriek worden gebruikt, worden er twee toegevoegde stukken informatie bij doorgegeven: hoptelling en MTU. De hoptelling is simpelweg het aantal gateways dat een pakje door zal moeten gaan om aan de bestemming te krijgen. MTU is de maximale pakketgrootte die langs het gehele pad zonder fragmentatie kan worden verzonden. (Dit is het minimum van de MTU's van alle bij het pad betrokken netwerken.)

Op basis van de metrische informatie wordt één enkele "samengestelde metriek" berekend voor het pad. De samengestelde metriek combineert het effect van de verschillende metrische componenten in één enkel getal dat de "goedheid" van dat pad representeert. Het is de samengestelde metriek die eigenlijk wordt gebruikt om te beslissen over het beste pad.

Regelmatig zendt elke gateway zijn gehele routingtabel uit (met wat censuur vanwege de gesplitste horizon regel) naar alle aangrenzende gateways. Wanneer een gateway deze uitzending van een andere gateway krijgt, vergelijkt hij de tabel met zijn bestaande tabel. Alle nieuwe bestemmingen en paden worden toegevoegd aan de routingtabel van de gateway. Paden in de uitzending worden vergeleken met bestaande paden. Als een nieuw pad beter is, kan het het bestaande worden vervangen. Informatie in de uitzending wordt ook gebruikt om kanaalbezetting en andere informatie over bestaande paden bij te werken. Deze algemene procedure is vergelijkbaar met de procedure die wordt gebruikt door alle afstandsvectorprotocollen. In de wiskundige literatuur wordt het Bellman-Ford algoritme genoemd. Raadpleeg [RFC 1058](#) voor een gedetailleerde ontwikkeling van de basisprocedure, die RIP, een ouder vectorprotocol op afstand beschrijft.

In IGRP wordt het algemeen Bellman-Ford-algoritme in drie cruciale aspecten gewijzigd. Eerst wordt in plaats van een eenvoudige metriek een vector van metriek gebruikt om paden te karakteriseren. Ten tweede, in plaats van één enkel pad met de kleinste metrische, wordt het verkeer verdeeld tussen verschillende paden, waarvan de metriek in een gespecificeerd bereik valt. In de derde plaats worden verschillende eigenschappen geïntroduceerd om stabiliteit te

bieden in situaties waar de topologie aan het veranderen is.

Het beste pad wordt geselecteerd op basis van een samengestelde metriek:

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

waarbij K1, K2 = constanten, be = ongeladen padbandbreedte x (1 - kanaalbezetting), Dc = topologische vertraging, en r = betrouwbaarheid.

Het pad met de kleinste samengestelde metriek is het beste pad. Waar er meerdere paden naar dezelfde bestemming zijn, kan de gateway de pakketten over meer dan één pad routeren. Dit gebeurt volgens de samengestelde metriek voor elk gegevenspad. Bijvoorbeeld, als één pad een samengestelde metrische 1 heeft en een ander pad een samengestelde metrisch van 3 heeft, drie keer zo veel pakketten over het gegevenspad worden verzonden met samengestelde metriek van 1.

Er zijn twee voordelen aan het gebruik van een vector van metrische informatie. Het eerste is dat het de mogelijkheid biedt om meerdere servicetypen van dezelfde set gegevens te ondersteunen. Het tweede voordeel is een betere nauwkeurigheid. Wanneer één enkele metriek wordt gebruikt, wordt deze normaal behandeld alsof het een vertraging is. Elke link in het pad wordt toegevoegd aan de totale metriek. Als er een link is met een lage bandbreedte, wordt deze normaal weergegeven door een grote vertraging. Maar bandbreedtebeperkingen cumuleren niet echt de manier waarop vertragingen doen. Door bandbreedte als een afzonderlijk onderdeel te behandelen, kan het correct worden verwerkt. Op dezelfde manier kan de lading worden verwerkt door een afzonderlijk kanaalbezettingstal.

IGRP biedt een systeem voor het onderling verbinden van computernetwerken die op stabiele wijze een algemene topologie van de grafiek met inbegrip van lijnen kunnen verwerken. Het systeem behoudt volledige pad-metrische informatie, d.w.z. het kent de padparameters van alle andere netwerken waarmee een poort is verbonden. Het verkeer kan over parallelle paden worden verdeeld en meerdere pad parameters kunnen tegelijkertijd over het gehele netwerk worden berekend.

## Vergelijking met RIP

In deze sectie worden IGRP en RIP vergeleken. Deze vergelijking is nuttig omdat RIP op grote schaal wordt gebruikt voor soortgelijke doeleinden als IGRP. Dit is echter niet helemaal eerlijk. Het RIP was niet bedoeld om alle doelstellingen van het IGRP te bereiken. RIP was bedoeld voor gebruik in kleine netwerken met een redelijk uniforme technologie. In dergelijke toepassingen is het over het algemeen toereikend.

Het meest fundamentele verschil tussen IGRP en RIP is de structuur van hun metriek. Helaas is dit geen verandering die eenvoudigweg kan worden aangepast aan RIP. Het vereist de nieuwe algoritmen en gegevensstructuren die aanwezig zijn in IGRP.

RIP gebruikt een eenvoudige "hoptelling" metriek om het netwerk te beschrijven. In tegenstelling tot IGRP, waar elke weg door een vertraging, bandbreedte enz. wordt beschreven in RIP wordt het beschreven door een aantal van 1 tot 15. Normaal wordt dit aantal gebruikt om te vertegenwoordigen hoeveel gateways het pad door gaat vóór het bereiken naar de bestemming. Dit betekent dat er geen onderscheid wordt gemaakt tussen een langzaam serielijn en een Ethernet. Bij sommige implementaties van het RIP is het voor de systeembeheerder mogelijk om te specificeren dat een bepaalde hop meer dan eens moet worden geteld. Langzame netwerken

kunnen worden vertegenwoordigd door een grote hoptelling. Maar omdat het maximum 15 is, kan dit niet veel gedaan worden. Als bijvoorbeeld een Ethernet wordt weergegeven door 1 en een 56Kb lijn door 3, kunnen er maximaal 56 Kb lijnen in een pad zijn, of het maximum van 15 wordt overschreden. Om het volledige bereik van beschikbare netwerksnelheden te vertegenwoordigen, en voor een groot netwerk toe te staan, suggereren studies door Cisco dat een metriek van 24 bit nodig is. Als de maximale metriek te klein is, heeft de systeembeheerder een onaangename keuze: of hij kan geen onderscheid maken tussen snelle en langzame routes, of hij kan zijn hele netwerk niet in de limiet passen. In feite zijn een aantal nationale netwerken nu groot genoeg zodat RIP ze niet meer kan verwerken, zelfs niet als elke hop maar één keer wordt geteld. RIP kan eenvoudigweg niet voor dergelijke netwerken worden gebruikt.

De voor de hand liggende reactie zou zijn om RIP te wijzigen om een grotere metriek toe te staan. Helaas zal dit niet werken. Zoals alle afstand vectorprotocollen heeft RIP het probleem van "tellen tot oneindig". Dit wordt in detail beschreven in [RFC 1058](#). Wanneer topologie verandert, zullen de woekerroutes worden geïntroduceerd. De metriek die aan deze onduidelijke routes is gekoppeld, neemt langzaam toe tot ze 15 bereiken, op welk punt de routes worden verwijderd. 15 is een klein genoeg maximum dat dit proces vrij snel zal samenvallen, ervan uitgaande dat de veroorzaakte updates worden gebruikt. Als RIP werd gewijzigd om een metriek met 24 bits toe te staan, zouden loops lang genoeg aanhouden zodat de metriek tot  $2^{24}$  zou worden geteld. Dit is niet te tolereren. IGRP heeft functies die zijn ontworpen om te voorkomen dat onduidelijke routes worden geïntroduceerd. Deze worden hieronder in punt 5.2 besproken. Het is niet praktisch om complexe netwerken aan te pakken zonder dergelijke voorzieningen in te voeren of over te stappen op een protocol zoals het SFP.

IGRP doet een beetje meer dan het bereik van de toegestane parameters vergroten. Het reorganiseert de metriek om vertraging, bandbreedte, betrouwbaarheid, en lading te beschrijven. Het is mogelijk dergelijke overwegingen in één enkele statistiek, zoals RIP's, te weergeven. De door IGRP gevolgde benadering is echter potentieel nauwkeuriger. Met één enkele statistiek lijken meerdere opeenvolgende snelle verbindingen bijvoorbeeld gelijk te zijn aan één enkele trage. Dit kan het geval zijn voor interactief verkeer, waar vertraging de belangrijkste zorg is. Voor bulkgegevensoverdracht is het primaire probleem echter bandbreedte en het samenvoegen van metriek samen is niet de juiste benadering. IGRP behandelt vertraging en bandbreedte afzonderlijk, cumulerend vertragingen, maar het minimum van de bandbreedte nemen. Het is niet makkelijk om te zien hoe de effecten van betrouwbaarheid en lading in één component metrisch moeten worden geïntegreerd.

In mijn ogen is een van de grote voordelen van IGRP het gemak van configuratie. Het kan rechtstreeks betrekking hebben op hoeveelheden met een fysieke betekenis. Dit betekent dat het automatisch kan worden ingesteld, op basis van het interfacetype, de lijnsnelheid, enz. Met een enkele component metriek is het waarschijnlijker dat de metriek 'gekookt' moet worden om effecten van verschillende dingen op te nemen.

Andere innovaties zijn meer een kwestie van algoritmen en gegevensstructuren dan van het routeringsprotocol. IGRP specificeert bijvoorbeeld algoritmen en gegevensstructuren die het splitsen van verkeer tussen verschillende routes ondersteunen. Het is zeker mogelijk om een implementatie van RIP te ontwerpen die dit doet. Zodra de routing echter opnieuw wordt geïmplementeerd, is er geen reden om met RIP te blijven doorgaan.

Tot nu toe heb ik "generieke IGRP" beschreven, een technologie die routing voor elk netwerkprotocol kan ondersteunen. In deze sectie is het echter de moeite waard om wat meer te zeggen over de specifieke TCP/IP-implementatie. Dat is de implementatie die vergeleken zal worden met RIP.

De update berichten van RIP bevatten eenvoudig snapshots van de routingstabel. Ze hebben een aantal bestemmingen en metrische waarden, en weinig anders. De IP-implementatie van IGRP heeft een aanvullende structuur. Ten eerste wordt het update bericht geïdentificeerd door een "autonoom systeemnummer." Deze terminologie komt voort uit de Arpanet-traditie en heeft daar een specifieke betekenis. Voor de meeste netwerken betekent het echter dat je verschillende routingsystemen op hetzelfde netwerk kunt uitvoeren. Dit is handig voor plaatsen waar netwerken van verschillende organisaties samenkomen. Elke organisatie kan haar eigen routing onderhouden. Omdat elke update wordt geëtiketteerd, kunnen gateways worden gevormd om aandacht slechts aan de rechterte besteden. Bepaalde gateways zijn ingesteld om updates van verschillende autonome systemen te ontvangen. Ze geven informatie over tussen de systemen op een gecontroleerde manier door. Merk op dat dit geen volledige oplossing voor problemen van het verzenden van veiligheid is. Elke poort kan worden ingesteld om naar updates van elk autonoom systeem te luisteren. Het is echter nog steeds een zeer nuttig instrument bij het uitvoeren van routingbeleid, waarbij een redelijke mate van vertrouwen tussen de netwerkbeheerders bestaat.

De tweede structurele eigenschap van IGRP update berichten beïnvloedt de manier waarop de standaardroutes door IGRP worden behandeld. De meeste routingprotocollen hebben een concept van standaardroute. Het is vaak niet praktisch voor het routeren van updates om elk netwerk in de wereld van een lijst te maken. Meestal heeft een verzameling gateways gedetailleerde routeinformatie nodig voor netwerken binnen hun organisatie. Al het verkeer naar bestemmingen buiten hun organisatie kan naar één van een paar grenspoorten worden verstuurd. Deze grensgateways kunnen vollediger informatie bevatten. De route naar de beste grenspoort is een "standaardroute". Het is een standaard in de zin dat het gebruikt wordt om naar een bestemming te gaan die niet specifiek vermeld is in de interne routingupdates. RIP, en sommige andere routingprotocollen, verspreiden informatie over de standaardroute alsof het een echt netwerk was. IGRP volgt een andere aanpak. In plaats van één enkele valse ingang voor de standaardroute, staat IGRP echte netwerken toe om als kandidaten voor een standaard te worden gemarkeerd. Dit wordt uitgevoerd door informatie over deze netwerken te plaatsen in een speciaal extern gedeelte van het update bericht. Maar het zou net zo goed kunnen worden gezien als een beetje aanzetten geassocieerd met die netwerken. Periodiek IGRP scant alle kandidaat standaardroutes en kiest degene met de laagste metrische als werkelijke standaardroute.

Mogelijk is deze benadering van wanbetalingen iets flexibeler dan de benadering die door de meeste implementaties van het RIP wordt gevolgd. Meestal kunnen de gateways van RIP worden ingesteld om een standaardroute met een bepaalde gespecificeerde metriek te genereren. Het is de bedoeling dat dit gebeurt bij grenspoorten.

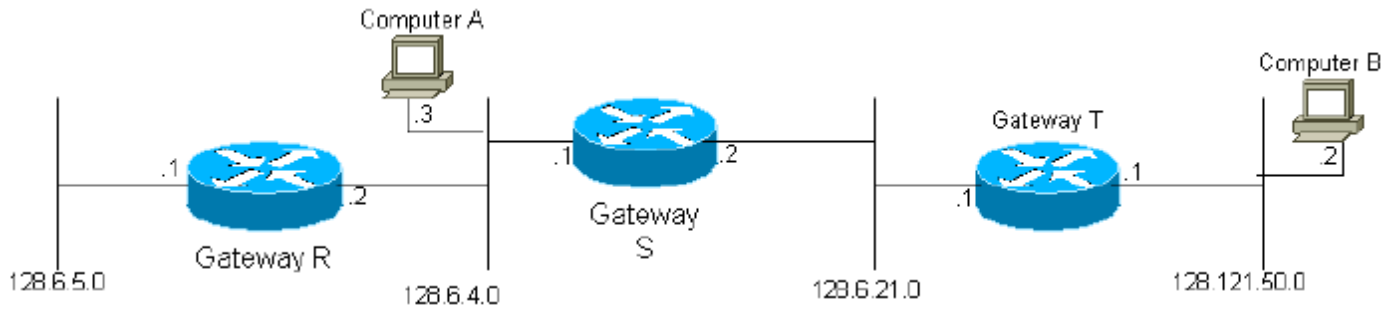
## [Gedetailleerde beschrijving](#)

Deze paragraaf bevat een gedetailleerde beschrijving van IGRP.

### [Algemene beschrijving](#)

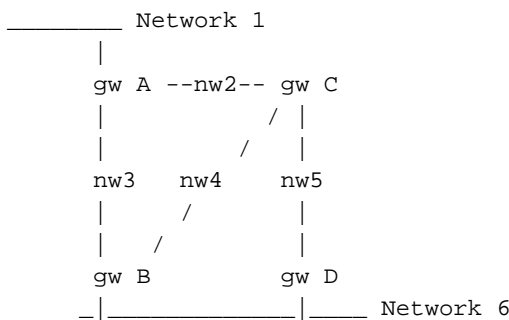
Wanneer een gateway eerst wordt ingeschakeld, wordt zijn routingtabel geïntialiseerd. Dit kan worden gedaan door een operator vanaf een console-terminal, of door informatie te lezen uit configuratiebestanden. Een beschrijving van elk netwerk dat op de gateway wordt aangesloten wordt verstrekt, met inbegrip van de topologische vertraging langs de verbinding (bijvoorbeeld, hoe lang het één enkel beetje duurt om de verbinding te oversteken) en de bandbreedte van de verbinding.

### **Figuur 2**



In het bovenstaande schema wordt bijvoorbeeld aan poort S gemeld dat deze via de corresponderende interfaces is verbonden met netwerken 2 en 3. In eerste instantie weet gateway 2 alleen dat zij elke doelcomputer in netwerken 2 en 3 kan bereiken. Alle gateways zijn geprogrammeerd om periodiek aan hun aangrenzende gateways de informatie door te geven waarmee zij zijn geparafeerd, evenals informatie die van andere gateways is verzameld. Gateway S zou dan updates van gateways R en T ontvangen en leren dat het computers in netwerk 1 kan bereiken via gateway R en computers in netwerk 4 via gateway T. Aangezien poort S zijn gehele routingtabel verstuurt, zal de volgende cyclus-gateway T leren dat het naar netwerk 1 kan gaan via gateway S. Het is gemakkelijk om te zien dat informatie over elk netwerk in het systeem uiteindelijk elke gateway in het systeem zal bereiken, op voorwaarde dat het netwerk volledig is aangesloten.

**Figuur 3**



Elke gateway berekent een samengestelde metriek om de wenselijkheid van de gegevenspaden naar doelcomputers te bepalen. Bijvoorbeeld, in het bovenstaande diagram, voor een bestemming in Netwerk 6, zou gateway A (gw A) metrische functies voor twee paden berekenen, via gateways B en C. Merk op dat paden eenvoudig door de volgende hop worden bepaald. Er zijn eigenlijk drie mogelijke routes van A naar Network 6:

- Direct naar B
- Naar C en vervolgens naar B
- Naar C en dan naar D

Echter, gateway A hoeft niet te kiezen tussen de twee routes met C. De routingtabel in A heeft één enkele ingang die het pad naar C vertegenwoordigt. Zijn metriek vertegenwoordigt de beste manier om van C naar de eindbestemming te krijgen. Als A een pakje naar C stuurt, is het aan C om te beslissen of B of D gebruikt wordt.

**Vergelijking 1**

De samengestelde metrische functie berekend voor elk gegevenspad is zoals hieronder wordt getoond:



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

Waar  $r$  = fractionele betrouwbaarheid (% van de transmissie die met succes ontvangen worden bij de volgende hop),  $Dc$  = samengestelde vertraging,  $be$  = effectieve bandbreedte: ongeladen bandbreedte x (1 - kanaalbezettingsgraad), en  $K1$  en  $K2$  = constanten.

## Vergelijking 2

In principe kan de samengestelde vertraging,  $Dc$ , worden bepaald zoals hieronder wordt aangegeven:

$$Dc = Ds + Dcir + Dt$$

Waar  $Ds$  = switching vertraging,  $Dcir$  = circuitvertraging (propagatievertraging van 1 bit) en  $DT$  = transmissievertraging (geen-lading vertraging voor een 1500 bit bericht).

In de praktijk wordt echter voor elk type netwerktechnologie een standaardvertragingcijfer gebruikt. Bijvoorbeeld, er zal een standaard vertragingcijfer voor Ethernet, en voor serielijnen bij om het even welk bepaald beetje tarief zijn.

Hier is een voorbeeld van hoe de gateway A's routingtabel in het geval van het hierboven aangegeven netwerk 6 zou kunnen kijken. (Merk op dat afzonderlijke onderdelen van de metrische vector niet worden getoond, voor eenvoud.)

### Routing Tabel Voorbeeld:

Netwerknw	Interface	Volgende gateway	metrisch
1	NW 1	None	Direct verbonden
2	NW 2	None	Direct verbonden
3	3 NW	None	Direct verbonden
4	NW 2	C	1270
	3 NW	B	1180
5	NW 2	C	1270
	3 NW	B	2130
6	NW 2	C	2040
	3 NW	B	1180

Het basisproces van het opbouwen van een routingtabel door informatie uit te wisselen met burens wordt beschreven door het Bellman-Ford algoritme. Het algoritme is gebruikt in vroegere protocollen zoals RIP (RFC 1058). Om met complexere netwerken om te gaan, voegt IGRP drie eigenschappen toe aan het basisalgoritme Bellman-Ford:

1. In plaats van een eenvoudige metriek, wordt een vector van metriek gebruikt om paden te karakteriseren. Een enkele samengestelde metriek kan van deze vector worden berekend volgens vergelijking 1, hierboven. Met behulp van een vector kan de poort verschillende soorten diensten verwerken, door gebruik te maken van verschillende coëfficiënten in

vergelijking 1. Het biedt ook een nauwkeuriger weergave van de kenmerken van het netwerk dan één enkele meting.

2. In plaats van één pad te kiezen met de kleinste maatstaf, wordt het verkeer verdeeld onder verschillende paden waarbij de metriek valt in een gespecificeerde range. Dit maakt het mogelijk om verschillende routes parallel te gebruiken, wat een grotere effectieve bandbreedte dan om het even welke route oplevert. Een variantie  $V$  wordt gespecificeerd door de netwerkbeheerder. Alle paden met minimale metrische  $M$  worden bewaard. Daarnaast worden alle paden waarvan de metrische waarde minder is dan  $V \times M$  bewaard. Het verkeer wordt over meerdere paden verdeeld in omgekeerde verhouding tot de samengestelde metriek.
3. Er zijn enkele problemen met dit begrip van variantie. Het is moeilijk om strategieën te bedenken die gebruik maken van variantiewaarden groter dan 1 en niet ook leiden tot looping van pakketten. In Cisco release 8.2 wordt de variantie optie niet geïmplementeerd. (Ik weet niet zeker in welke release de functie is verwijderd.) Dit heeft tot gevolg dat de variantie permanent op 1 wordt ingesteld.
4. Verschillende eigenschappen worden geïntroduceerd om stabiliteit in situaties te voorzien waar de topologie verandert. Deze functies zijn bedoeld om routekaarten en 'tellen naar oneindig' te voorkomen. Deze functies hebben vorige pogingen gekarakteriseerd om Ford-type algoritmen voor dit type toepassing te gebruiken. De primaire stabiliteitskenmerken zijn "holddowns", "getriggerde updates", "gesplitste horizon" en "vergiftiging". Hieronder zal nader worden ingegaan.

Verkeersplitsing (punt 2) brengt een vrij subtiel gevaar met zich mee. De variantie  $V$  is ontworpen om gateways parallelle paden van verschillende snelheden te laten gebruiken. Er kan bijvoorbeeld een 9600 BPS-lijn lopen parallel met een 19200 BPS-lijn, voor redundantie. Als variantie  $V$  1 is, wordt alleen het beste pad gebruikt. De 9600 BPS-lijn zal dus niet worden gebruikt als de BPS-lijn van 19200 een redelijke betrouwbaarheid heeft. (Als echter meerdere paden dezelfde zijn, wordt de lading onder deze paden verdeeld.) Door de variantie te verhogen, kunnen we toestaan dat het verkeer wordt opgesplitst tussen de beste route en andere routes die bijna even goed zijn. Met een voldoende grote variantie zal het verkeer tussen de twee regels worden verdeeld. Het gevaar is dat met een grote genoeg variantie, paden worden toegestaan die niet alleen langzamer zijn, maar zich in de verkeerde richting bevinden. Er moet dus een extra regel komen om te voorkomen dat het verkeer "stroomopwaarts" wordt verstuurd: Er wordt geen verkeer verzonden langs paden waarvan de afstandssamengestelde metriek (de samengestelde metriek berekend bij de volgende hop) groter is dan de samengestelde metriek berekend bij de gateway. In het algemeen worden systeembeheerders aangemoedigd de variantie boven 1 niet in te stellen, behalve in specifieke situaties waarin parallelle paden moeten worden gebruikt. In dat geval wordt de variantie zorgvuldig ingesteld om de "juiste" resultaten te geven.

IGRP is bedoeld voor meerdere 'soorten service' en meerdere protocollen. Het type service is een specificatie in een datapakket waarmee de manier waarop paden moeten worden geëvalueerd, wordt gewijzigd. Bijvoorbeeld, staat het TCP/IP protocol het pakket toe om het relatieve belang van hoge bandbreedte, lage vertraging, of hoge betrouwbaarheid te specificeren. Over het algemeen zullen interactieve toepassingen lage vertraging specificeren, terwijl de bulkoverdrachtstoepassingen hoge bandbreedte zullen specificeren. Deze eisen bepalen de relatieve waarden van  $K1$  en  $K2$  die geschikt zijn voor gebruik in Eq. 1. Elke combinatie van specificaties in het te ondersteunen pakket wordt aangeduid als een "type service". Voor elk type dienst moet een reeks parameters  $K1$  en  $K2$  worden gekozen. Een routingtabel wordt bewaard voor elk type service. Dit gebeurt omdat paden worden geselecteerd en geordend volgens de samengestelde metriek die door Eq wordt gedefinieerd. 1. Dit is verschillend voor elk type service. Informatie van al deze routingtabellen wordt gecombineerd om de routingupdate berichten te

produceren die door de gateways worden uitgewisseld, zoals beschreven in afbeelding 7.

## Stabiliteitskenmerken

In dit gedeelte worden de bewaarinstellingen, de getriggerde updates, de gesplitste horizon en de vergiftiging beschreven. Deze kenmerken zijn ontworpen om te voorkomen dat gateways verkeerde routes oppakken. Zoals beschreven in [RFC 1058](#), kan dit gebeuren wanneer een route onbruikbaar wordt, door het falen van een gateway of een netwerk. In beginsel detecteren de aangrenzende gateways defecten. Ze sturen dan routingupdates die de oude route als onbruikbaar tonen. Het is echter mogelijk dat updates bepaalde delen van het netwerk helemaal niet bereiken of dat ze vertraging oplopen bij het bereiken van bepaalde gateways. Een poort die nog steeds gelooft dat de oude route goed is kan die informatie blijven verspreiden en op die manier de mislukte route in het systeem opnieuw betreden. Uiteindelijk zal deze informatie door het netwerk verspreiden en terugkeren naar de gateway die het opnieuw injecteerde. Het gevolg is een circulaire route.

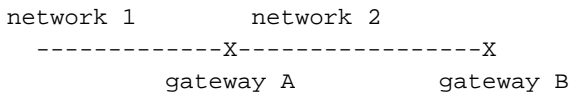
De tegenmaatregelen zijn eigenlijk overbodig. In beginsel zouden houdstermijnen en uitgezette aanpassingen moeten volstaan om verkeerde routes in de eerste plaats te voorkomen. In de praktijk kunnen communicatiestoornissen van verschillende aard er echter toe leiden dat ze ontoereikend zijn. Splitst horizon en routevergiftiging zijn bedoeld om in elk geval routinglijnen te voorkomen.

Normaal gesproken worden er nieuwe routingtabellen naar naburige gateways verzonden (standaard elke 90 seconden, hoewel deze kunnen worden aangepast door de systeembeheerder). Een geactiveerd update is een nieuwe routingtabel die onmiddellijk wordt verzonden, in antwoord op een of andere verandering. De belangrijkste verandering is het verwijderen van een route. Dit kan voorkomen omdat een timeout is verlopen (waarschijnlijk is er een naburige poort of lijn afgevallen) of omdat een update bericht van de volgende poort in het pad aantoont dat het pad niet langer bruikbaar is. Wanneer een gateway G ontdekt dat een route niet meer bruikbaar is, brengt het onmiddellijk een update in. Deze update zal die route als onbruikbaar tonen. Bedenk wat er gebeurt wanneer deze update de aangrenzende gateways bereikt. Als de route van de buur terug naar G wijst, moet de buur de route verwijderen. Dit zorgt ervoor dat de buurman een update teweegbrengt, enz. Zo zal een mislukking leiden tot een golf van update berichten. Deze golf zal zich door dat gedeelte van het netwerk voortplanten waarin de routes door de mislukte gateway of het netwerk gingen.

Gevorderde updates zouden volstaan als we konden garanderen dat de golf van updates onmiddellijk elke passende poort bereikte. Er zijn echter twee problemen. Eerst kunnen pakketten met het update bericht worden verwijderd of beschadigd door een of andere link in het netwerk. Ten tweede, de uitgebrachte updates gebeuren niet onmiddellijk. Het is mogelijk dat een gateway die de getriggerde update nog niet heeft gekregen een regelmatige update op precies het verkeerde tijdstip zal uitgeven, wat ervoor zorgt dat de slechte route opnieuw wordt opgenomen in een buurman die reeds de getriggerde update had gekregen. Holddowns zijn ontworpen om deze problemen te overwinnen. De 'holddown' regel zegt dat wanneer een route wordt verwijderd, er gedurende enige tijd geen nieuwe route voor dezelfde bestemming zal worden geaccepteerd. Dit geeft de getriggerde updates tijd om naar alle andere gateways te gaan, zodat we er zeker van kunnen zijn dat alle nieuwe routes die we krijgen, niet slechts een poort zijn die het oude opnieuw bevestigt. De duur van de vertraging moet lang genoeg zijn om de golf van geactiveerd updates door het netwerk te laten gaan. Daarnaast dient deze een aantal reguliere uitzendcycli te omvatten, zodat u pakjes kunt behandelen die vallen. Bedenk wat er gebeurt als een van de geactiveerd updates wordt ingetrokken of beschadigd. De gateway die deze update heeft verstrekt zal een andere update uitgeven bij de volgende regelmatige update. Dit zal de golf van

geactiveerd updates bij burens die de eerste golf gemist hebben opnieuw opstarten.

De combinatie van uitgestelde updates en holddowns zou moeten volstaan om te voorkomen dat verlopen routes opnieuw worden opgenomen. Maar toch zijn er een paar extra voorzorgsmaatregelen nodig. Ze maken zeer lossy netwerken mogelijk, en netwerken die zijn gepartitioneerd. De door IGRP gevraagde aanvullende voorzorgsmaatregelen zijn gesplitste horizon en routevergiftiging. Split horizon vloeit voort uit de waarneming dat het nooit zinvol is om een route terug te sturen in de richting waarvan zij is gekomen. Bekijk de volgende situatie:



Gateway A zal B vertellen dat het een route naar netwerk 1 heeft. Wanneer B updates naar A stuurt, is er nooit een reden voor om dat netwerk 1 te noemen. Aangezien A dichterbij 1 ligt, is er geen reden voor om via B te gaan. De gesplitste horizon regel zegt dat een afzonderlijk update bericht moet worden gegenereerd voor elke buur (in feite elk naburig netwerk). In de actualisering voor een bepaalde buurstaat moeten de routes naar die buurman worden weggelaten. Deze regel voorkomt lusvorming tussen aangrenzende gateways. Stel bijvoorbeeld dat de interface van A naar netwerk 1 mislukt. Zonder de gesplitste horizon-regel zou B A zeggen dat het 1 kan worden. Aangezien het geen echte route meer heeft, zou A die route kunnen aangrijpen. In dit geval zouden A en B beide routes naar 1 hebben. Maar A zou wijzen naar B en B op A. Natuurlijk zijn er updates en holddowns die dit moeten voorkomen. Maar omdat er geen reden is om informatie terug te sturen naar de plaats waar ze vandaan kwam, is gesplitste horizon toch de moeite waard om te doen. Naast zijn rol bij het voorkomen van mazen in de wet, houdt gesplitste horizon de omvang van bijgewerkte berichten in de gaten.

Split horizon moet loops tussen aangrenzende gateways voorkomen. Vergiftiging van de route is bedoeld om grotere loops te doorbreken. De regel is dat wanneer een update de metriek voor een bestaande route toont voldoende gestegen te hebben, er een lus is. De route moet worden verwijderd en in een holddown toestand worden geplaatst. Momenteel is de regel dat een route wordt verwijderd als de samengestelde metriek meer dan een factor van 1.1 stijgt. Het is niet veilig voor enkel een toename in samengestelde metriek om verwijdering van de route te veroorzaken, omdat kleine metrische veranderingen kunnen optreden door veranderingen in kanaalbezettingsgraad of betrouwbaarheid. Dus de factor 1.1 is slechts een heuristisch. De exacte waarde is niet cruciaal. We verwachten dat deze regel alleen nodig zal zijn om zeer grote mazen in de regelgeving te doorbreken, omdat kleine regels voorkomen zullen worden door uitgestelde updates en holddowns.

## Holddowns uitschakelen

Vanaf release 8.2 biedt de Cisco-code een optie om bewaarinstellingen uit te schakelen. Het nadeel van een 'holddowns' is dat ze de aanname van een nieuwe route vertragen wanneer een oude route faalt. Met standaardparameters kan het meerdere minuten duren voordat een router een nieuwe route na een verandering vaststelt. Om de hierboven uiteengezette redenen is het echter niet veilig om alleen de ingehouden bedragen te verwijderen. Het resultaat zou tot oneindig worden geteld, zoals beschreven in RFC 1058. We veronderstellen, maar kunnen niet bewijzen, dat met een sterkere versie van routevergiftiging, holddowns niet langer nodig zijn om te stoppen met tellen tot oneindig. Aldus maakt het uitschakelen van houdingen deze sterkere vorm van routevergiftiging mogelijk. Merk op dat gesplitste horizon en geactiveerd updates nog steeds van kracht zijn.

De sterkere vorm van routevergiftiging is gebaseerd op een hoptelling. Als de hoptelling voor een

pad stijgt, wordt de route verwijderd. Dit zal natuurlijk routes verwijderen die nog geldig zijn. Als iets anders in het netwerk verandert zodat het pad nu door één poort gaat, zal de hoptelling stijgen. In dit geval is de route nog steeds geldig. Er is echter geen volledig veilige manier om deze case te onderscheiden van het routeren van lijnen (tel tot oneindig). De veiligste aanpak is dus het verwijderen van de route wanneer de hoptelling toeneemt. Als de route nog steeds legitiem is, zal deze door de volgende update opnieuw geïnstalleerd worden, en dat zal een teweeggebrachte update veroorzaken die de route elders in het systeem opnieuw zal installeren.

In het algemeen nemen vectoralgoritmen op afstand1 gemakkelijk nieuwe routes aan. Het probleem is het volledig uit het systeem verwijderen van oude. Dus een regel die overmatig agressief is over het verwijderen van verdachte routes moet veilig zijn.

## Bijzonderheden van het actualiseringsproces

De reeks processen die in de figuren 4 tot en met 8 worden beschreven, zijn bedoeld om één netwerkprotocol te behandelen, bijvoorbeeld TCP/IP, DECnet of het ISO/OSI-protocol. Maar de protocoldetails worden alleen gegeven voor TCP/IP. Eén poort kan gegevens verwerken die meerdere protocollen volgen. Omdat elk protocol verschillende adresstructuren en pakketformaten heeft, zal de computercode die wordt gebruikt om de figuren 4 tot 8 uit te voeren over het algemeen verschillend zijn voor elk protocol. Het in afbeelding 4 beschreven proces zal het meest variëren, zoals beschreven in de gedetailleerde opmerkingen voor figuur 4. De in afbeelding 5 tot en met 8 beschreven processen hebben dezelfde algemene structuur. Het primaire verschil van protocol aan protocol zal het formaat van het routing update pakket zijn, dat moet worden ontworpen om compatibel met een specifiek protocol te zijn.

Merk op dat de definitie van een bestemming van protocol tot protocol kan verschillen. De hier beschreven methode kan worden gebruikt voor het routeren naar individuele hosts, naar netwerken of voor complexere hiërarchische adresschema's. Welk type routing wordt gebruikt, hangt af van de adresstructuur van het protocol. De huidige TCP/IP-implementatie ondersteunt alleen het routeren naar IP-netwerken. Dus "bestemming" betekent in feite IP-netwerk of subnetnummer. Subnetinformatie wordt alleen bewaard voor aangesloten netwerken.

De figuren 4 tot en met 7 tonen pseudo-code voor verschillende stukken van het routingproces dat door de gateways wordt gebruikt. Aan het begin van het programma worden aanvaardbare protocollen en parameters ingevoerd die elke interface beschrijven.

De poort zal alleen bepaalde protocollen verwerken die zijn opgesomd. Elke communicatie vanuit een systeem met een protocol dat niet in de lijst staat, wordt genegeerd. De gegevensinvoer is als volgt:

- Netwerken waaraan de gateway is verbonden.
- Ongeladen bandbreedte van elk netwerk.
- Topologische vertraging van elk netwerk.
- Betrouwbaarheid van elk netwerk.
- Kanaalbezetting van elk netwerk.
- MTU van elk netwerk.

De metrische functie voor elk gegevenspad wordt dan berekend volgens vergelijking 1. Merk op dat de eerste drie posten redelijk permanent zijn. Ze zijn een functie van de onderliggende netwerktechnologie en zijn niet afhankelijk van de lading. Ze kunnen worden ingesteld vanuit een configuratiebestand of door directe invoer van de operator. Merk op dat IGRP geen gemeten vertraging gebruikt. Zowel theorie als ervaring suggereren dat het zeer moeilijk is voor protocollen die gemeten vertraging gebruiken om stabiele routing te onderhouden. Er zijn twee gemeten

parameters: betrouwbaarheid en kanaalbezetting. De betrouwbaarheid is gebaseerd op foutenpercentages die door de hardware of firmware van de netwerkinterface worden gerapporteerd.

Daarnaast vereist het routingalgoritme een waarde voor verschillende routingparameters. Dit omvat timer waarden, variantie en of de instellingen zijn ingeschakeld. Dit wordt normaal gesproken gespecificeerd door een configuratiebestand of een beheerder die wordt ingevoerd. (Vanaf Cisco release 8.2 is de variantie permanent ingesteld op 1.)

Zodra de eerste informatie is ingevoerd, worden de operaties in de gateway geactiveerd door gebeurtenissen—of de aankomst van een gegevenspakket op een van de netwerkinterfaces, of het verlopen van een timer. De in de figuren 4 tot en met 7 beschreven processen worden als volgt geactiveerd:

- Wanneer een pakket arriveert, wordt het verwerkt overeenkomstig afbeelding 4. Dit resulteert in het verzenden van het pakket naar een andere interface, wordt weggegooid of wordt geaccepteerd voor verdere verwerking.
- Wanneer een pakje door de poort wordt geaccepteerd voor verdere verwerking, wordt het geanalyseerd op een protocol-specifieke manier die niet in deze specificatie is beschreven. Als het pakket een routing update is, wordt het verwerkt volgens afbeelding 5.
- Afbeelding 6 toont gebeurtenissen die door een timer zijn geactiveerd. De timer is ingesteld om een keer per seconde te onderbreken. Wanneer de onderbreking optreedt, wordt het proces dat in afbeelding 6 wordt getoond, uitgevoerd.
- Afbeelding 7 toont een routingupdate subroutine. De oproepen naar deze subroutine worden weergegeven in de figuren 5 en 6.
- Afbeelding 8 bevat ook gegevens over de in de figuren 5 en 7 bedoelde metrische berekeningen.

Er zijn vier cruciale tijdconstanten die routepropagatie en -expiratie controleren. Deze tijdconstanten kunnen door de systeembeheerder worden ingesteld. Er zijn echter standaardwaarden. Deze tijdconstanten zijn:

- De tijd-updates van de uitzending worden door alle gateways op alle aangesloten interfaces dit vaak uitgezonden. De standaardinstelling is eens per 90 seconden.
- Ongeldige tijd-als geen update voor een bepaald pad binnen deze tijd is ontvangen, wordt het geacht tijd-out te hebben gehad. Het zou meerdere keren de uitzending tijd moeten zijn, om de mogelijkheid te hebben dat pakketten die een update bevatten door het netwerk kunnen worden ingetrokken. De standaardinstelling is 3 keer de uitzendtijd.
- Houd tijd-wanneer een bestemming onbereikbaar is geworden (of de metriek genoeg gestegen is om vergiftiging te veroorzaken), gaat de bestemming in "holddown". Gedurende deze status wordt er geen nieuw pad voor dezelfde bestemming geaccepteerd voor dezelfde tijd. De opslagtijd geeft aan hoe lang deze toestand moet duren. Het moet verschillende keren de uitzending zijn. De standaardwaarde is 3 keer de uitzendtijd plus 10 seconden. (Zoals beschreven in het gedeelte [Holddowns uitschakelen](#), is het mogelijk houdingen uit te schakelen.)
- Spoeltijd—Als geen update voor een bepaalde bestemming binnen deze tijd is ontvangen, wordt de ingang voor het doel verwijderd uit de routingtabel. Let op het verschil tussen ongeldige tijd en spoeltijd: Nadat de ongeldige tijd is verstreken, wordt een pad uitgezet en verwijderd. Als er geen resterende paden naar een bestemming zijn, is de bestemming nu onbereikbaar. De gegevensbank voor de bestemming blijft echter behouden. Het moet blijven

om de 'holddown' te handhaven. Na de spoeltijd wordt de gegevensbank uit de tabel verwijderd. Het moet iets langer zijn dan de ongeldige tijd plus de vertragingstijd. De standaardinstelling is 7 keer de uitzendtijd.

Deze cijfers veronderstellen de volgende grote gegevensstructuren. Een aparte reeks van deze gegevensstructuren wordt bewaard voor elk protocol dat door de gateway wordt ondersteund. Binnen elk protocol wordt een aparte reeks gegevensstructuren bewaard voor elk type service dat wordt ondersteund.

Voor elke bestemming die aan het systeem bekend is, is er een (mogelijk nul) lijst van paden naar de bestemming, een onthoudingstijd en een laatste update tijd. De laatste update tijd geeft de laatste keer aan dat elk pad voor deze bestemming in een update van een andere gateway was opgenomen. Merk op dat er ook update tijden zijn die voor elk pad worden gehouden. Wanneer het laatste pad naar een bestemming wordt verwijderd, wordt de bestemming in het vak holddown gezet, tenzij bewaarinstellingen worden uitgeschakeld (Zie de sectie [Holddowns](#) van [uitzetten](#) voor meer informatie). De sluitingstijd geeft het tijdstip aan waarop de vertraging afloopt. Het feit dat het niet-nul is geeft aan dat de bestemming in een houdbare positie is. Om calculatietijd op te slaan is het ook een goed idee om een "beste metriek" voor elke bestemming te bewaren. Dit is simpelweg het minimum van de samengestelde metriek voor alle paden naar de bestemming.

Voor elk pad naar een bestemming, is er het adres van de volgende hop in het pad, de te gebruiken interface, een vector van metriek die het pad karakteriseert, inclusief topologische vertraging, bandbreedte, betrouwbaarheid, en kanaalbezetting. Andere informatie wordt ook geassocieerd met elk pad, waaronder hoptelling, MTU, bron van informatie, de samengestelde metriek op afstand en een samengestelde metriek berekend uit deze getallen volgens vergelijking 1. Er is ook een laatste update tijd. De bron van de informatie geeft aan waar de meest recente update voor dat pad vandaan kwam. In de praktijk is dit hetzelfde als het adres van de volgende hop. De laatste update is simpelweg het tijdstip waarop de meest recente update voor dit pad is aangekomen. Het wordt gebruikt om getimed paden te verlopen.

Merk op dat een IGRP-update bericht drie delen heeft: interieur, systeem (d.w.z. "dit autonome systeem", maar niet de binnenkant) en buitenkant. Het binnenste gedeelte is voor routes naar subnetten. Niet alle subnetinformatie is inbegrepen. Slechts subnetten van één netwerk zijn inbegrepen. Dit is het netwerk verbonden aan het adres waaraan de update wordt verzonden. Normaal worden updates op elke interface uitgezonden, dus dit is eenvoudigweg het netwerk waarop de uitzending wordt verzonden. (Andere gevallen doen zich voor voor reacties op een IGRP-verzoek en wijzen naar punt IGRP.) Grote netwerken (bijvoorbeeld niet-subnetwerken) worden in het systeemgedeelte van het update bericht gezet, tenzij ze specifiek als buitenkant worden gemarkeerd.

Een netwerk zal als extern worden gemarkeerd als het van een andere gateway werd geleerd en de informatie in het externe gedeelte van het update bericht was gearriveerd. De implementatie van Cisco stelt de systeembeheerder ook in staat om specifieke netwerken als extern te verklaren. Ook de buitenroutes worden aangeduid als "kandidaat default". Het zijn routes die naar of door gateways gaan die als standaard geschikt worden beschouwd, te gebruiken wanneer er geen expliciete route naar een bestemming is. Bijvoorbeeld bij Rutgers vormen we de poort die Rutgers verbindt met ons regionale netwerk zodat het de route naar de NSFnet backbone als buitenkant markeert. De implementatie van Cisco verkiest een standaardroute door die buitenroute met de kleinste metriek te kiezen.

De volgende rubrieken dienen ter verduidelijking van bepaalde gedeelten van de figuren 4 tot en met 8.

## Packet-routing

Afbeelding 4 beschrijft de algehele verwerking van ingangspakketten. Dit wordt alleen gebruikt om de terminologie te verduidelijken. Duidelijk is dit geen volledige beschrijving van wat een IP gateway doet.

Dit proces gebruikt de lijst van ondersteunde protocollen en de informatie over de ingevoerde interfaces wanneer de gateway wordt geïnitieerd. Details van de pakketverwerking zijn afhankelijk van het protocol dat door het pakket wordt gebruikt. Dit wordt bepaald in Stap A. Stap A is het enige gedeelte van afbeelding 4 dat door alle protocollen wordt gedeeld. Zodra het protocoltype bekend is, wordt de implementatie van figuur 4 voor het protocoltype gebruikt. Details van de pakketinhoud worden beschreven in de specificaties van het protocol. De specificaties van een protocol omvatten een procedure om de bestemming van een pakket te bepalen, een procedure om de bestemming met de eigen adressen van de gateway te vergelijken om te bepalen of de gateway zelf de bestemming is, een procedure om te bepalen of een pakket een uitzending is, en een procedure om te bepalen of de bestemming deel uitmaakt van een bepaald netwerk. Deze procedures worden gebruikt in de stappen B en C van afbeelding 4. De test in stap D vereist een onderzoek van de bestemmingen die in de routingtabel zijn vermeld. De test wordt tevreden als er een ingang in de routingtabel voor de bestemming is, en die bestemming heeft met het minstens één bruikbaar pad geassocieerd. Merk op dat de bestemmings- en padgegevens die in deze en de volgende stap worden gebruikt, afzonderlijk worden gehandhaafd voor elk type service dat wordt ondersteund. Deze stap begint dus met het bepalen van het type service dat door het pakket is gespecificeerd en het selecteren van de corresponderende verzameling gegevensstructuren die voor dit en de volgende stap moet worden gebruikt.

Een pad is bruikbaar voor de toepassing van stap D en E als de afstandssamengestelde metriek minder is dan de samengestelde metriek. Een pad waarvan de afstandssamengestelde metriek groter is dan zijn samengestelde metriek is een pad waarvan de volgende hop "verder weg" van de bestemming is, zoals gemeten door metrisch. Dit wordt een "stroomopwaarts pad" genoemd. Normaal gezien zou je verwachten dat het gebruik van metriek ervoor zorgt dat er geen paden voor de bovenloop worden gekozen. Het is gemakkelijk om te zien dat een stroomopwaarts pad nooit de beste kan zijn. Als echter een grote variantie is toegestaan, kunnen andere paden dan de beste worden gebruikt. Sommige daarvan zouden stroomopwaarts kunnen zijn gericht.

Stap E berekent het te gebruiken pad. Paden waarvan de afstandssamengestelde metriek niet kleiner is dan hun samengestelde metriek worden niet in aanmerking genomen. Als meer dan één pad acceptabel is, worden zulke paden gebruikt in een gewogen vorm van round robin alternatie. De frequentie waarmee een pad wordt gebruikt is omgekeerd evenredig aan de samengestelde metriek.

## Ontvang van routingupdates

Afbeelding 5 beschrijft de verwerking van een routingupdate die van een naburige gateway wordt ontvangen. Deze actualiseringen bestaan uit een lijst van posten, die elk informatie voor één bestemming verstrekken. Meer dan één ingang voor de zelfde bestemming kan in één enkele Routing update voorkomen, om meerdere servicetypen aan te passen. Elk van deze items wordt afzonderlijk verwerkt, zoals in afbeelding 5 is beschreven. Als een vermelding in het buitengedeelte van de bijwerking voorkomt, wordt de buitenste vlag ingesteld voor de bestemming als deze als gevolg van dit proces wordt toegevoegd.

Het gehele proces dat in afbeelding 5 wordt beschreven, moet één keer worden herhaald voor elk type service dat door de gateway wordt ondersteund, met behulp van de reeks bestemming / pad



informatie die met dat type service is verbonden. Dit wordt getoond in de ultraperifere lijn in Afbeelding 5. De volledige routingupdate moet één keer voor elk type service worden verwerkt. (Merk op dat de huidige implementatie van IGRP geen ondersteuning biedt voor meerdere soorten diensten, zodat het ultraperifere netwerk niet daadwerkelijk wordt geïmplementeerd.)

In stap A worden op het pad fundamentele aanvaardbaarheidstests uitgevoerd. Dit moet reëel testen van de bestemming omvatten. Onmogelijke ("Martiaans") netwerknummers moeten worden afgewezen. (Raadpleeg [RFC 1009](#) en [RFC 1122](#) voor meer informatie.) Bijwerkingen worden ook verworpen indien de bestemming waarop zij betrekking hebben, in een holddown staat, d.w.z. de uitbetalingstermijn is niet-nul en later dan de huidige tijd.

In Stap B wordt de routingtabel doorzocht om te zien of deze ingang een pad beschrijft dat al bekend is. Een pad in de routingtabel wordt gedefinieerd door de bestemming waarmee de volgende hop is geassocieerd, de volgende hop die als deel van het pad wordt vermeld, de uitvoerinterface die voor het pad wordt gebruikt en de informatiebron (het adres waar de update kwam—in praktijk kwam gewoonlijk het zelfde als de volgende hop). De ingang van het update pakket beschrijft een pad waarvan de bestemming in de ingang is vermeld, wiens uitvoerinterface de interface is die de update binnenkwam, en waarvan de volgende hop en informatiebron het adres van de gateway zijn die de update (de "bron" S) verstuurd.

In Stap H en Stap T is het in afbeelding 7 beschreven uploadproces. Dit proces wordt daadwerkelijk uitgevoerd nadat het gehele proces dat in afbeelding 5 is beschreven, is voltooid. Dat wil zeggen dat het in figuur 7 beschreven actualiseringsproces slechts eenmaal zal plaatsvinden, zelfs indien het meerdere keren wordt geactiveerd tijdens de in afbeelding 5 beschreven verwerking. Bovendien moeten voorzorgsmaatregelen worden genomen om te voorkomen dat er te vaak bijwerkingen worden verstrekt, indien het netwerk snel verandert.

Stap K wordt gedaan als de bestemming die door de huidige ingang in het update pakket wordt beschreven reeds in de routingtabel bestaat. K vergelijkt de nieuwe samengestelde metriek berekend uit gegevens in het update pakket met de beste samengestelde metriek voor de bestemming. Merk op dat de beste samengestelde metriek op dit moment niet opnieuw berekend wordt, dus als het pad dat overwogen wordt al in de routingtabel is, kan deze test nieuwe en oude metriek voor hetzelfde pad vergelijken.

Stap L wordt uitgevoerd voor de paden die erger zijn dan de bestaande beste samengestelde metriek. Dit omvat zowel nieuwe paden die erger zijn dan bestaande paden en bestaande paden waarvan de samengestelde metriek is toegenomen. Stap L test of het nieuwe pad aanvaardbaar is. Merk op dat deze test zowel de test om na te gaan of een nieuw pad goed genoeg is om te bewaren, als de route vergiftiging implementeert. Om acceptabel te zijn, moet de vertragswaarde niet de speciale waarde zijn die een onbereikbare bestemming aangeeft (voor de huidige IP-implementatie, alle waarden in een 24-bits veld) en de samengestelde metriek (berekend zoals gespecificeerd in afbeelding 8) moet aanvaardbaar zijn. Om te bepalen of samengestelde metriek aanvaardbaar is, vergelijk het met de samengestelde metriek van alle andere paden aan de bestemming. Laat mij het minimum zijn. Het nieuwe pad is acceptabel als  $V < X \cdot M$  is, WAAR V DE VARIANTIE IS DIE IS INGESTELD TOEN DE GATEWAY IS GEÏNITIALISEERD. ALS  $V = 1$  (DAT ALTIJD GELDIG IS VANAF CISCO RELEASE 8.2), IS EEN METRISCHE ERGER DAN DE BESTAANDE NIET AANVAARDBAAR. EEN UITZONDERING IS DAT : ALS HET PAD AL BESTAAT EN HET ENIGE PAD IS VOOR DE BESTEMMING, BLIJFT HET PAD BEHOUDEN ALS DE METRIEK NIET MET MEER DAN 10% IS VERHOOGD (OF WANNEER DE BEDRIJVEN WORDEN UITGESCHAKELD, INDIEN HET HOP-AANTAL NIET IS VERHOOGD).

Stap V wordt uitgevoerd wanneer de nieuwe informatie voor een pad aangeeft dat de

samengestelde metriek wordt verlaagd. De samengestelde metriek van alle paden naar bestemming D wordt vergeleken. In deze vergelijking, wordt de nieuwe samengestelde metriek voor P gebruikt, eerder dan die in het routing tabel verschijnen. De minimum samengestelde metrische M wordt berekend. Dan worden alle paden naar D opnieuw onderzocht. Als de samengestelde metriek voor een pad  $> M \times V$  is, wordt dat pad verwijderd. V is de variantie, die is ingevoerd toen de gateway werd gearafaerd. (Vanaf Cisco release 8.2 is de variantie permanent ingesteld op 1.)

## Periodieke verwerking

Het in afbeelding 6 beschreven proces wordt eenmaal per seconde geactiveerd. Het onderzoekt verschillende timers in de routingtabel, om te zien of er een verlopen is. Deze timers worden hierboven beschreven.

In Stap U wordt het in afbeelding 7 beschreven proces geactiveerd.

Stap R en Stap S zijn noodzakelijk omdat de samengestelde metriek die in de routingtabel is opgeslagen, afhankelijk is van de kanaalbezetting, die in de tijd verandert, op basis van metingen. Regelmatig wordt de kanaalbezettingsgraad herberekend met behulp van een bewegend gemiddelde van gemeten verkeer door de interface. Als de nieuw berekende waarde verschilt van de bestaande, moeten alle samengestelde parameters met betrekking tot die interface worden aangepast. Elk pad dat in de routingtabel wordt getoond wordt onderzocht. Elk pad waarvan de volgende hop interface "I" gebruikt heeft zijn samengestelde metrische herberekend. Dit wordt gedaan in overeenstemming met Vergelijking 1, gebruikt als kanaalbezette het maximum van de waarde die in de routingtabel is opgeslagen als deel van de metriek van het pad, en de nieuw berekende kanaalbezetting van de interface.

## Update berichten genereren

Afbeelding 7 beschrijft hoe de gateway bijgewerkte berichten genereert die naar andere gateways moeten worden verstuurd. Er wordt een afzonderlijk bericht gegenereerd voor elke netwerkinterface die aan de poort is gekoppeld. Dat bericht wordt vervolgens naar alle andere gateways verzonden die via de interface bereikbaar zijn (Stap J). Over het algemeen wordt dit gedaan door het bericht als een uitzending te verzenden. Als de netwerktechnologie of het protocol echter geen uitzendingen toestaat, kan het nodig zijn het bericht afzonderlijk naar elke gateway te versturen.

In het algemeen wordt het bericht opgebouwd door een ingang voor elke bestemming in de routingtabel, in Stap G. Merk op dat de bestemming/pad gegevens die bij elk type service horen gebruikt moeten worden. In het slechtste geval wordt voor elk type service een nieuwe vermelding toegevoegd aan de update. Voordat u echter een ingang aan het update bericht in Stap G toevoegt, worden de reeds toegevoegde waarden gescand. Als de nieuwe vermelding al in het update bericht staat, wordt deze niet meer toegevoegd. Een nieuwe vermelding dupliceert een bestaande wanneer de bestemmingen en volgende hoppoorten hetzelfde zijn.

Omwille van de eenvoud laat de pseudocode één ding weg—IGRP update berichten hebben drie delen: binnen-, systeem- en buitenkant, wat betekent dat er eigenlijk drie loops zijn ten opzichte van bestemmingen. De eerste omvat slechts subnetten van het netwerk waarnaar de update wordt verzonden. Het tweede omvat alle grote netwerken (bijvoorbeeld niet-subnetten) die niet als buitenkant zijn gemarkeerd. Het derde omvat alle grote netwerken die als buitenkant worden gemarkeerd.

Stap E voert de test van de gesplitste horizon uit. In het normale geval faalt deze test voor routes waarvan de beste weg uit de zelfde interface gaat die de update wordt verzonden. Als de update echter naar een specifieke bestemming wordt verzonden (bijvoorbeeld in antwoord op een IGRP-verzoek van een andere gateway, of als onderdeel van "point to point IGRP"), faalt de gesplitste horizon alleen indien de beste route afkomstig was van die bestemming (de "informatiebron" is dezelfde als de bestemming) en de uitvoerinterface dezelfde is als de verbinding waarvan het verzoek afkomstig was.

## Metrische informatie berekenen

Afbeelding 8 beschrijft hoe de metrische informatie wordt verwerkt van update berichten die door de gateway worden ontvangen, en hoe het wordt gegenereerd voor update berichten die door de gateway worden verzonden. Merk op dat de ingang op één bepaald pad naar de bestemming is gebaseerd. Als er meer dan één pad naar de bestemming is, wordt een pad gekozen waarvan de samengestelde metriek minimaal is. Als meer dan één pad de minimum samengestelde metriek heeft, wordt een willekeurige band-breekregel gebruikt. (Voor de meeste protocollen is dit gebaseerd op het adres van de volgende hopgateway.)

### **Afbeelding 4-Verwerking van inkomende pakketten**

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.

### **Afbeelding 5-Verwerking inkomende routingupdates**

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

## Afbeelding 6. Periodieke verwerking

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

## Afbeelding 7 — Actualisering genereren

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

## Afbeelding 8 — Details van de metrieke berekening

In dit gedeelte wordt de procedure beschreven voor het berekenen van metriek en hoptellingen van een aankomende routingupdate. De invoer van deze functie is de ingang voor een specifieke bestemming in een routingupdate pakket. De output is een vector van metriek die kan worden gebruikt om de samengestelde metriek te berekenen, en een hoptelling. Als dit pad aan de routingtabel wordt toegevoegd, wordt de gehele vector van de parameters in de tabel ingevoerd. De interfaceparameters die in de volgende definities worden gebruikt zijn die die zijn ingesteld toen de gateway werd geparafeerd, voor de interface waarop de routingupdate is gearriveerd, behalve dat de kanaalbezettingsgraad en betrouwbaarheid zijn gebaseerd op een bewegend gemiddelde van gemeten verkeer door de interface.

- Vertraging = vertraging van pakket + interface topologische vertraging
- Bandbreedte = max (bandbreedte van pakket, interfacebandbreedte)
- Betrouwbaarheid = min (betrouwbaarheid van het pakket, betrouwbaarheid van de interface)
- Kanaalbezettingsgraad = max (kanaalbezetting vanaf pakje, inbezetting van interfacekanalen)(Max wordt gebruikt voor bandbreedte omdat de metrieke bandbreedte in omgekeerde vorm is opgeslagen. Conceptueel willen we de minimale bandbreedte.) Merk op dat de oorspronkelijke kanaalbezetting van het pakket moet worden opgeslagen, omdat het nodig zal zijn om de effectieve kanaalbezetting opnieuw te berekenen wanneer de bezigheid van het interfacekanaal verandert.

Het volgende maakt geen deel uit van de metrische vector, maar wordt ook in de routingtabel

gehouden als kenmerken van het pad:

- Hop teller = hoptelling uit pakje.
- MTU = min (MTU van pakket, interface MTU).
- Afstandsmetriek = berekend van Vergelijking 1 met behulp van de metrische waarden uit het pakje. Dat wil zeggen, de metrische componenten zijn die van het pakje, en worden niet bijgewerkt zoals hierboven wordt getoond. Dit moet natuurlijk worden berekend voordat de hierboven vermelde aanpassingen worden uitgevoerd.
- Composietmetriek = berekend op basis van vergelijking 1 met behulp van de in deze paragraaf beschreven metrische waarden.

In deze rest van deze paragraaf wordt de procedure beschreven voor het berekenen van metriek en hoptellen voor het routeren van updates die moeten worden verstuurd.

Deze functie bepaalt de metrische informatie en hoptelling om in een uitgaand update pakket te worden gezet. Het is gebaseerd op een specifiek pad naar een bestemming, als er bruikbare paden zijn. Als er geen paden zijn, of de paden allemaal in de bovenloop zijn, wordt de bestemming "ontoegankelijk" genoemd.

```
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 van de IP-implementatie](#)

Deze sectie briefle beschrijft de pakketformaten die door Cisco IGRP worden gebruikt. IGRP wordt verzonden met IP-datagrammen met IP protocol 9 (IGP). Het pakket begint met een header. Het begint onmiddellijk na de 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 */
```

Voor update berichten, volgt de routinginformatie onmiddellijk na de kopbal.

Het versienummer is momenteel 1. Packets met andere versienummers worden genegeerd.

De code kan 1 = update of 2 = verzoek zijn.

Dit geeft het type bericht aan. De twee soorten berichten worden hieronder weergegeven.

*Edition* is een serienummer dat toeneemt wanneer er een wijziging in de routingtabel optreedt. (Dit gebeurt in die omstandigheden waarin de pseudocode hierboven zegt om een routingupdate teweeg te brengen.) Het nummer van de editie staat gateways toe om verwerking van updates met informatie die zij al gezien hebben te vermijden. (Dit wordt momenteel niet ten uitvoer gelegd. Dat wil zeggen, het nummer van de editie wordt correct gegenereerd, maar bij invoer wordt het genegeerd. Omdat het mogelijk is om pakketten te laten vallen, is het niet duidelijk dat het nummer van de editie voldoende is om dubbele verwerking te voorkomen. Zorg ervoor dat alle pakketten die met de editie zijn gekoppeld, zijn verwerkt.)

*Een systeem* is het autonome systeemnummer. In de implementatie van Cisco, kan een gateway aan meer dan één autonoom systeem deelnemen. Elk dergelijk systeem werkt zijn eigen IGRP-protocol. Conceptueel, zijn er volledig afzonderlijke routingtabellen voor elk autonoom systeem. Routes die via IGRP van één autonoom systeem komen worden alleen in updates voor dat AS verzonden. Dit veld biedt de poort om te selecteren welke set routingtabellen u wilt gebruiken voor het verwerken van dit bericht. Als de gateway een IGRP bericht voor een AS ontvangt dat het niet wordt ingesteld, wordt het genegeerd. In feite staat de implementatie van Cisco toe dat de informatie van het ene AS aan het andere wordt "uitgelekt". Ik beschouw dit echter als een administratief instrument en niet als een onderdeel van het protocol.

*Binnenzijde, systeem* en *binnenzijde* geven het aantal items aan in elk van de drie delen van de update berichten. Deze delen zijn hierboven beschreven. Er is geen andere afbakening tussen de delen. De eerste inwendige ingangen worden naar binnen genomen als inwendig, de volgende insysteemingenangen als systeem en de laatste buitenkant als buitenkant.

Checksum is een IP-checksum, berekend met behulp van hetzelfde algoritme als een UDP-checksum. De checksum wordt berekend op de IGRP-header en elke routinginformatie die erop volgt. Het veld checksum is op nul gezet bij het berekenen van de checksum. De checksum bevat niet de IP-header en er is ook geen virtuele header zoals in UDP en TCP.

## Verzoeken

Een IGRP-verzoek vraagt de ontvanger om zijn routingtabel te verzenden. Het aanvraagbericht heeft alleen een header. Alleen de versie-, opcode- en systeemvelden worden gebruikt. Alle andere velden zijn nul. De ontvanger wordt geacht een normaal IGRP-update-bericht naar de aanvrager te sturen.

## updates

Een IGRP update bericht bevat een header, gevolgd door routing items. Zoals veel routing items zijn opgenomen zoals deze in een 1500-byte datagram (inclusief IP-header) passen. Met de huidige structuraangiften maakt dit 104 boekingen mogelijk. Als er meer inzendingen nodig zijn, worden er verschillende update berichten verzonden. Aangezien de update berichten eenvoudig door invoer worden verwerkt, is er geen voordeel in het gebruik van één enkel gefragmenteerd bericht in plaats van meerdere onafhankelijke berichten.

Hier is de structuur van een routeinslag:

```
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 */

```

De velden gedefinieerd als uchar[2] en uchar[3] zijn simpelweg 16 en 24-bits binaire integers, in normale IP-netwerkvolgorde.

Nummer definieert de bestemming die wordt beschreven. Het is een IP-adres. Om ruimte op te slaan, worden alleen de eerste 3 bytes van het IP-adres gegeven, behalve in het gedeelte Interior. In het interieurgedeelte worden de laatste 3 bytes gegeven. Voor systeem- en buitenroutes zijn er geen subnetten mogelijk, dus is de byte met lage orde altijd nul. Binnenlandse routes zijn altijd subnetten van een bekend netwerk, dus de eerste byte van dat netwerknummer wordt geleverd.

De vertraging is in eenheden van 10 microseconden. Dit geeft een bereik van 10 microseconden tot 168 seconden, wat voldoende lijkt. Een vertraging van alle signalen duidt erop dat het netwerk onbereikbaar is.

Bandbreedte is omgekeerde bandbreedte in bits per sec geschaald met een factor van 1.0e10. Het bereik loopt van een 1200 BPS lijn tot 10 Gbps. (Als de bandbreedte N Kbps is, is het gebruikte aantal 1000000/N.)

MTU is in bytes.

Betrouwbaarheid wordt gegeven als een fractie van 255. Dat wil zeggen, 255 is 100%.

De lading wordt gegeven als een fractie van 255.

Hop-tellen is een simpele telling.

Vanwege de ietwat vreemde eenheden die gebruikt worden voor bandbreedte en vertraging, lijken sommige voorbeelden op volgorde. Dit zijn de standaardwaarden die gebruikt worden voor meerdere gewone media.

	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 berekeningen](#)

Hier is een beschrijving van de manier waarop de samengestelde metriek feitelijk wordt berekend in Cisco versie 8.0(3).

```

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

## [Gerelateerde informatie](#)

- [Ondersteuningspagina voor IP-routing](#)
- [IGRP-ondersteuningspagina](#)
- [Technische ondersteuning - Cisco-systemen](#)