Introduzione alla tecnologia IGRP

Sommario

Introduzione

Questo documento introduce il protocollo IGRP (Interior Gateway Routing Protocol). Ha due scopi. Uno è quello di formare un'introduzione alla tecnologia IGRP, per coloro che sono interessati a utilizzare, valutare e possibilmente implementare. L'altro è quello di dare una più ampia esposizione ad alcune idee e concetti interessanti che si concretizzano nell'IGRP. Per informazioni su come configurare il protocollo IGRP, consultare il documento sulla configurazione del protocollo IGRP, l'implementazione di Cisco IGRP e i comandi IGRP.

Obiettivi per IGRP

Il protocollo IGRP permette a diversi gateway di coordinare il proprio routing. I suoi obiettivi sono i seguenti:

- Routing stabile anche su reti molto grandi o complesse. Non devono verificarsi loop di routing, neanche come eventi temporanei.
- Risposta rapida alle modifiche della topologia di rete.

- Sovraccarico ridotto. In altre parole, lo stesso IGRP non dovrebbe utilizzare una larghezza di banda maggiore di quella effettivamente necessaria per il proprio compito.
- Frazionamento del traffico tra più percorsi paralleli quando sono più o meno ugualmente desiderabili.
- Tenendo conto dei tassi di errore e del livello di traffico su percorsi diversi.

L'implementazione corrente di IGRP gestisce il routing per TCP/IP. Tuttavia, il progetto di base è progettato per essere in grado di gestire una varietà di protocolli.

Nessuno strumento risolverà tutti i problemi di instradamento. In genere, il problema di routing è suddiviso in più parti. Protocolli quali IGRP sono chiamati "protocolli gateway interni" (IGP). Sono destinati all'utilizzo in un unico insieme di reti, sotto una gestione unica o in una gestione strettamente coordinata. Tali gruppi di reti sono connessi da "protocolli gateway esterni" (EGP). Un IGP è progettato per tenere traccia di una buona quantità di dettagli sulla topologia di rete. La priorità nella progettazione di un IGP è data alla produzione di percorsi ottimali e alla risposta rapida ai cambiamenti. Un EGP ha lo scopo di proteggere un sistema di reti da errori o false dichiarazioni intenzionali da parte di altri sistemi; BGP è uno di questi protocolli gateway esterni. Nella progettazione di un EGP la priorità è data ai controlli amministrativi e di stabilità. Spesso è sufficiente che un EGP produca una via ragionevole, piuttosto che la via ottimale.

IGRP presenta alcune analogie con protocolli precedenti, quali Routing Information Protocol di Xerox, RIP di Berkeley e Hello di Dave Mills. Differisce da questi protocolli principalmente perché è progettato per reti più grandi e complesse. Per un confronto più dettagliato con RIP, il più utilizzato tra i protocolli della generazione precedente, vedere la sezione Confronto con RIP.

Analogamente ai protocolli precedenti, il protocollo IGRP è un protocollo vettoriale di distanza. In questo tipo di protocollo, i gateway scambiano le informazioni di routing solo con i gateway adiacenti. Queste informazioni di instradamento contengono un riepilogo delle informazioni relative al resto della rete. È matematicamente possibile dimostrare che tutti i gateway utilizzati insieme risolvono un problema di ottimizzazione in base a ciò che equivale a un algoritmo distribuito. Ogni gateway deve solo risolvere parte del problema e ricevere solo una parte dei dati totali.

L'alternativa principale all'IGRP è l'Enhanced IGRP (EIGRP) e una classe di algoritmi chiamata SPF (short-path first). OSPF utilizza questo concetto. Per ulteriori informazioni su OSPF, consultare la guida alla progettazione OSPF. OSPF Queste interfacce sono basate su una tecnica di flooding, in cui ogni gateway è tenuto aggiornato sullo stato di ogni interfaccia di ogni altro gateway. Ciascun gateway risolve il problema di ottimizzazione in modo indipendente dal proprio punto di vista, utilizzando i dati per l'intera rete. Ogni approccio presenta dei vantaggi. In alcune circostanze SPF può essere in grado di rispondere alle modifiche più rapidamente. Per evitare loop di routing, il protocollo IGRP deve ignorare i nuovi dati per alcuni minuti dopo alcuni tipi di modifiche. Poiché SPF dispone di informazioni direttamente da ciascun gateway, è in grado di evitare questi loop di routing. In questo modo può intervenire immediatamente sulle nuove informazioni. Tuttavia, SPF deve gestire una quantità di dati notevolmente superiore rispetto all'IGRP, sia nelle strutture di dati interne che nei messaggi tra gateway.

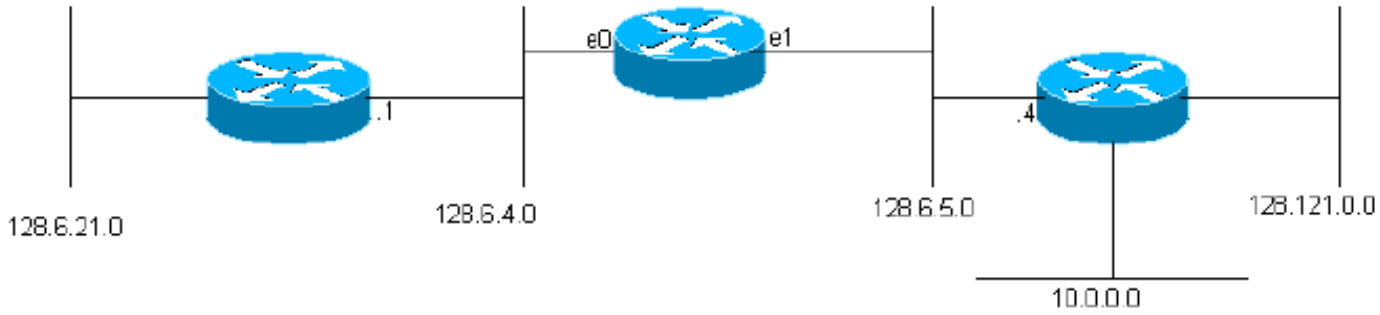
Il problema di routing

Il protocollo IGRP è destinato all'uso nei gateway che connettono diverse reti. Si presume che le reti utilizzino la tecnologia basata su pacchetti. In effetti, i gateway funzionano come switch di pacchetti. Quando un sistema connesso a una rete desidera inviare un pacchetto a un sistema su un'altra rete, il pacchetto viene indirizzato a un gateway. Se la destinazione si trova su una delle

reti connesse al gateway, quest'ultimo inoltrerà il pacchetto alla destinazione. Se la destinazione è più distante, il gateway inoltra il pacchetto a un altro gateway più vicino alla destinazione. I gateway utilizzano le tabelle di routing per decidere cosa fare con i pacchetti. Di seguito è riportato un semplice esempio di tabella di routing. (Gli indirizzi utilizzati negli esempi sono indirizzi IP della Rutgers University. Il problema di routing di base è simile anche per altri protocolli, ma questa descrizione presupporrà che per il routing IP venga utilizzato il protocollo IGRP.)

Figura 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
```



Come vedremo, le tabelle di routing IGRP effettive contengono informazioni aggiuntive per ciascun gateway. Questo gateway è connesso a due reti Ethernet, chiamate 0 e 1. Ad esse sono stati assegnati i numeri di rete IP (numeri di subnet) 128.6.4 e 128.6.5. Pertanto, i pacchetti indirizzati per queste reti specifiche possono essere inviati direttamente alla destinazione, semplicemente utilizzando l'interfaccia Ethernet appropriata. I gateway situati nelle vicinanze sono due: 128.6.4.1 e 128.6.5.4. I pacchetti per reti diverse da 128.6.4 e 128.6.5 verranno inoltrati a uno dei due gateway. La tabella di routing indica il gateway da utilizzare per la rete. Ad esempio, i pacchetti indirizzati a un host sulla rete 10 devono essere inoltrati al gateway 128.6.5.4. Si spera che questo gateway sia più vicino alla rete 10, ossia che il miglior percorso alla rete 10 passi attraverso questo gateway. Lo scopo principale del protocollo IGRP è consentire ai gateway di creare e gestire tabelle di routing di questo tipo.

Riepilogo del protocollo IGRP

Come accennato in precedenza, il protocollo IGRP consente ai gateway di creare la tabella di routing scambiando informazioni con altri gateway. Un gateway inizia con le voci per tutte le reti a esso direttamente connesse. Ottiene informazioni su altre reti scambiando aggiornamenti di routing con gateway adiacenti. Nel caso più semplice, il gateway troverà un percorso che rappresenta il modo migliore per raggiungere ciascuna rete. Un percorso è caratterizzato dal gateway successivo a cui devono essere inviati i pacchetti, dall'interfaccia di rete da utilizzare e dalle informazioni sulla metrica. Le informazioni della metrica sono un insieme di numeri che caratterizzano la validità del percorso. In questo modo il gateway può confrontare i percorsi che ha ascoltato da diversi gateway e decidere quale utilizzare. In alcuni casi è preferibile dividere il traffico su due o più percorsi. Il protocollo IGRP esegue questa operazione quando due o più percorsi sono ugualmente validi. L'utente può anche configurarlo per dividere il traffico quando i percorsi sono quasi ugualmente validi. In questo caso, verrà inviato un volume di traffico maggiore

lungo il percorso con una metrica migliore. L'obiettivo è che il traffico possa essere suddiviso tra una linea a 9600 bps e una linea a 19200 BPS, e la linea a 19200 otterrà circa il doppio del traffico della linea a 9600 BPS.

Le metriche utilizzate da IGRP includono:

- Ritardo topologico
- Larghezza di banda del segmento della larghezza di banda più stretta del percorso
- Occupazione del canale del percorso
- Affidabilità del percorso

Il tempo di ritardo topologico è il tempo necessario per raggiungere la destinazione lungo il percorso, presupponendo che la rete sia scarica. Naturalmente si verifica un ulteriore ritardo quando la rete viene caricata. Tuttavia, il carico viene calcolato utilizzando il valore di occupazione del canale e non cercando di misurare i ritardi effettivi. La larghezza di banda del percorso è semplicemente la larghezza di banda in bit al secondo del collegamento più lento nel percorso. L'occupazione del canale indica la quantità di larghezza di banda attualmente in uso. Viene misurato e cambia con il carico. Affidabilità indica la frequenza di errore corrente. È la frazione di pacchetti che arriva alla destinazione senza danni. Viene misurato.

Sebbene non vengano utilizzate come parte della metrica, vengono passate con essa due ulteriori informazioni: numero di hop e MTU. Il numero di hop è semplicemente il numero di gateway attraverso cui deve passare un pacchetto per raggiungere la destinazione. L'MTU è la dimensione massima del pacchetto che può essere inviato lungo l'intero percorso senza frammentazione. (ossia, è il valore minimo delle MTU di tutte le reti coinvolte nel percorso).

In base alle informazioni della metrica, viene calcolata una singola "metrica composita" per il percorso. La metrica composita combina l'effetto dei vari componenti metrici in un unico numero che rappresenta la "bontà" del percorso. È la metrica composita che viene effettivamente utilizzata per decidere il percorso migliore.

Periodicamente, ciascun gateway trasmette la propria intera tabella di routing (con alcune operazioni di censura dovute alla regola della divisione degli orizzonti) a tutti i gateway adiacenti. Quando un gateway ottiene la trasmissione da un altro gateway, confronta la tabella con la relativa tabella esistente. Le nuove destinazioni e i nuovi percorsi vengono aggiunti alla tabella di routing del gateway. I percorsi nella trasmissione vengono confrontati con i percorsi esistenti. Se un nuovo tracciato è migliore, potrebbe sostituire quello esistente. Le informazioni nella trasmissione vengono inoltre utilizzate per aggiornare l'occupazione dei canali e altre informazioni sui percorsi esistenti. Questa procedura generale è simile a quella utilizzata da tutti i protocolli dei vettori di distanza. Nella letteratura matematica si fa riferimento ad esso come all'algoritmo Bellman-Ford. Per uno sviluppo dettagliato della procedura di base, in cui viene descritto RIP, un protocollo vettore di distanza precedente, consultare la RFC 1058 .

In IGRP, l'algoritmo generale Bellman-Ford è modificato in tre aspetti critici. In primo luogo, invece di una semplice metrica, viene utilizzato un vettore di metrica per caratterizzare i percorsi. In secondo luogo, invece di scegliere un singolo percorso con la metrica più piccola, il traffico viene suddiviso tra più percorsi, le cui metriche rientrano in un intervallo specificato. In terzo luogo, vengono introdotte diverse funzionalità per garantire la stabilità in situazioni in cui la topologia sta cambiando.

Il percorso migliore viene selezionato in base a una metrica composita:

```
[(K1 / Be) + (K2 * Dc)] r
```
Dove K1, K2 = costanti, Be = larghezza di banda del percorso scaricato x (1 - occupazione canale), Dc = ritardo topologico e r = affidabilità.

Il percorso con la metrica composita più piccola sarà il percorso migliore. Se vi sono più percorsi alla stessa destinazione, il gateway può indirizzare i pacchetti su più percorsi. Questa operazione viene eseguita in base alla metrica composita per ogni percorso dati. Ad esempio, se un percorso ha una metrica composita di 1 e un altro percorso ha una metrica composita di 3, sul percorso dati verrà inviato il triplo dei pacchetti con la metrica composita di 1.

L'utilizzo di un vettore di informazioni metriche presenta due vantaggi. La prima è che consente di supportare più tipi di servizio dallo stesso insieme di dati. Il secondo vantaggio è una maggiore precisione. Quando si utilizza una singola metrica, questa viene in genere considerata come un ritardo. Ogni collegamento nel percorso viene aggiunto alla metrica dei totali. Se esiste un collegamento con larghezza di banda ridotta, in genere è rappresentato da un ritardo elevato. Tuttavia, le limitazioni della larghezza di banda non si traducono in un accumulo di ritardi. Trattando la larghezza di banda come un componente separato, può essere gestita correttamente. Analogamente, il carico può essere gestito da un numero di occupazione del canale separato.

IGRP fornisce un sistema per l'interconnessione di reti di computer in grado di gestire in modo stabile una topologia di grafico generale, compresi i loop. Il sistema conserva le informazioni sulla metrica del percorso completo, ossia conosce i parametri del percorso di tutte le altre reti a cui è connesso qualsiasi gateway. Il traffico può essere distribuito su percorsi paralleli e più parametri di percorso possono essere calcolati contemporaneamente sull'intera rete.

Confronto con il PIR

In questa sezione viene confrontato il protocollo IGRP con RIP. Questo confronto è utile perché RIP è ampiamente utilizzato per scopi simili a IGRP. Tuttavia, non è del tutto giusto farlo. RIP non è stato progettato per raggiungere tutti gli stessi obiettivi di IGRP. RIP era destinato all'uso in reti di piccole dimensioni con tecnologia ragionevolmente uniforme. In tali applicazioni esso è generalmente adeguato.

La differenza principale tra IGRP e RIP è la struttura delle metriche. Purtroppo non si tratta di una modifica che può essere semplicemente modificata in RIP. Richiede i nuovi algoritmi e le nuove strutture di dati presenti nell'IGRP.

RIP utilizza una semplice metrica di "conteggio hop" per descrivere la rete. A differenza di IGRP, in cui ogni percorso è descritto da un ritardo, una larghezza di banda e così via, in RIP è descritto da un numero compreso tra 1 e 15. In genere questo numero viene utilizzato per rappresentare quanti gateway deve passare il percorso prima di raggiungere la destinazione. Ciò significa che non viene fatta distinzione tra una linea seriale lenta e una rete Ethernet. In alcune implementazioni di RIP, è possibile per l'amministratore di sistema specificare che un determinato hop deve essere conteggiato più di una volta. Le reti lente possono essere rappresentate da un numero elevato di hop. Ma dato che il massimo è 15, non si può fare molto. Ad esempio, se un'interfaccia Ethernet è rappresentata da 1 e una linea da 56 Kb da 3, un percorso può contenere al massimo 5 linee da 56 Kb o superare il valore massimo di 15. Per rappresentare l'intera gamma di velocità di rete disponibili e consentire l'uso di una rete di grandi dimensioni, gli studi condotti da Cisco suggeriscono che è necessaria una metrica a 24 bit. Se la metrica massima è troppo piccola, all'amministratore di sistema viene offerta una scelta sgradevole: o non riesce a distinguere tra percorsi veloci e lenti, o non riesce a inserire tutta la sua rete nel limite. In effetti, un certo numero di reti nazionali sono ora abbastanza grandi da non poter essere gestite da RIP

anche se ogni hop è contato una sola volta. RIP non può essere utilizzato per reti di questo tipo.

La risposta ovvia sarebbe modificare RIP per consentire una metrica più grande. Sfortunatamente, questo non funzionerà. Come tutti i protocolli dei vettori di distanza, RIP ha il problema di "contare all'infinito". Questa condizione viene descritta in dettaglio nella RFC 1058 . Quando la topologia viene modificata, vengono introdotte route non corrette. Le metriche associate a queste route spurie aumentano lentamente fino a raggiungere 15, nel qual caso le route vengono rimosse. 15 è un valore massimo abbastanza piccolo da consentire una convergenza abbastanza rapida di questo processo, presupponendo che vengano utilizzati aggiornamenti attivati. Se RIP venisse modificato per consentire una metrica a 24 bit, i loop persisterebbero per un tempo sufficiente a consentire il conteggio della metrica fino a 2**24. Ciò non è tollerabile. L'IGRP è dotato di funzionalità progettate per impedire l'introduzione di rotte spurie. Tali funzioni sono descritte di seguito nella sezione 5.2. Non è pratico gestire reti complesse senza introdurre tali funzioni o passare a un protocollo come SPF.

Il protocollo IGRP non si limita ad aumentare l'intervallo delle metriche consentite. La metrica viene ristrutturata per descrivere il ritardo, la larghezza di banda, l'affidabilità e il carico. È possibile rappresentare tali considerazioni in un'unica metrica, come i RIP. Tuttavia, l'approccio adottato dall'IGRP è potenzialmente più accurato. Ad esempio, con una singola metrica, diversi collegamenti rapidi successivi risulteranno equivalenti a un singolo collegamento lento. Ciò può avvenire nel caso del traffico interattivo, per il quale il ritardo è la preoccupazione principale. Tuttavia, per il trasferimento di grandi quantità di dati, la preoccupazione principale è la larghezza di banda, e l'aggiunta di metriche insieme non è l'approccio corretto. Il protocollo IGRP gestisce il ritardo e la larghezza di banda separatamente, accumulando i ritardi ma riducendo al minimo le larghezze di banda. Non è facile comprendere come incorporare gli effetti dell'affidabilità e del carico in una metrica a componente singolo.

A mio avviso, uno dei grandi vantaggi dell'IGRP è la facilità di configurazione. Può rappresentare direttamente quantità che hanno un significato fisico. Questo significa che può essere impostato automaticamente, in base al tipo di interfaccia, alla velocità della linea, ecc. Con una metrica a componente singolo, è più probabile che debba essere "cotta" per incorporare gli effetti di diverse cose.

Altre innovazioni sono più una questione di algoritmi e strutture di dati che di protocollo di routing. Ad esempio, IGRP specifica algoritmi e strutture di dati che supportano la divisione del traffico tra più route. È certamente possibile progettare un'implementazione del RIP che faccia questo. Tuttavia, una volta reimplementato il routing, non vi è motivo di attenersi al RIP.

Finora ho descritto "IGRP generico", una tecnologia che potrebbe supportare il routing per qualsiasi protocollo di rete. Tuttavia, in questa sezione vale la pena menzionare qualcosa in più sull'implementazione TCP/IP specifica. Questa è l'attuazione che sarà confrontata con il RIP.

I messaggi di aggiornamento RIP contengono semplicemente snapshot della tabella di routing. Cioè, hanno un numero di destinazioni e valori metrici, e poco altro. L'attuazione del programma IGRP nel quadro della politica industriale ha una struttura supplementare. In primo luogo, il messaggio di aggiornamento è identificato da un "numero di sistema autonomo". Questa terminologia viene fuori dalla tradizione arpanet, e ha un significato specifico lì. Tuttavia, per la maggior parte delle reti questo significa che è possibile eseguire diversi sistemi di routing sulla stessa rete. Questa funzione è utile quando convergono reti di diverse organizzazioni. Ogni organizzazione può gestire il proprio ciclo. Poiché ogni aggiornamento è etichettato, è possibile configurare i gateway in modo che prestino attenzione solo a quello corretto. Alcuni gateway sono configurati per ricevere aggiornamenti da diversi sistemi autonomi. Essi passano informazioni tra i sistemi in modo controllato. Questa non è una soluzione completa ai problemi di sicurezza

dell'instradamento. È possibile configurare qualsiasi gateway per l'ascolto degli aggiornamenti da qualsiasi sistema autonomo. Tuttavia, si tratta ancora di uno strumento molto utile per implementare i criteri di routing quando tra gli amministratori di rete esiste un livello di fiducia ragionevole.

La seconda caratteristica strutturale dei messaggi di aggiornamento IGRP influisce sulla modalità di gestione delle route predefinite da parte di IGRP. La maggior parte dei protocolli di routing ha un concetto di route predefinita. Spesso non è possibile elencare tutte le reti del mondo per gli aggiornamenti di routing. In genere, un set di gateway richiede informazioni di routing dettagliate per le reti all'interno dell'organizzazione. Tutto il traffico per le destinazioni esterne alla loro organizzazione può essere inviato a uno dei pochi gateway di confine. Tali gateway di confine possono avere informazioni più complete. Il percorso al miglior gateway di confine è un "percorso predefinito". Si tratta di un valore predefinito, nel senso che viene utilizzato per raggiungere qualsiasi destinazione non elencata specificamente negli aggiornamenti del routing interno. RIP e alcuni altri protocolli di routing fanno circolare informazioni sulla route predefinita come se si trattasse di una rete reale. L'approccio del protocollo IGRP è diverso. Anziché una singola voce falsa per il percorso predefinito, il protocollo IGRP consente di contrassegnare le reti reali come candidate per l'impostazione predefinita. A tale scopo, le informazioni relative a tali reti vengono inserite in una sezione esterna speciale del messaggio di aggiornamento. Tuttavia, si potrebbe anche pensare che accenda un bit associato a quelle reti. La funzione IGRP esegue periodicamente la scansione di tutte le route predefinite candidate e sceglie quella con la metrica più bassa come route predefinita effettiva.

Potenzialmente questo approccio ai valori predefiniti è un po' più flessibile rispetto a quello adottato dalla maggior parte delle implementazioni RIP. Nella maggior parte dei casi, i gateway RIP possono essere impostati in modo da generare una route predefinita con una determinata metrica specificata. L'intenzione è che ciò avvenga nei gateway di confine.

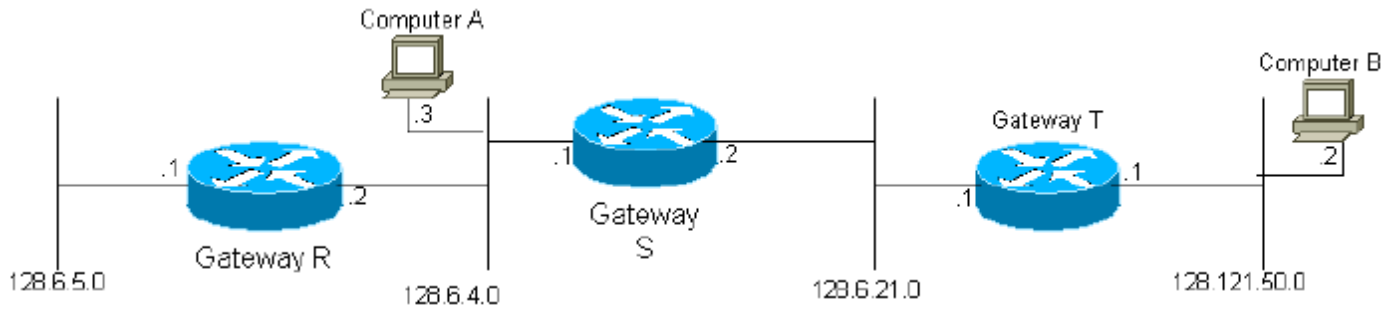
Descrizione dettagliata

In questa sezione viene fornita una descrizione dettagliata del protocollo IGRP.

Descrizione generale

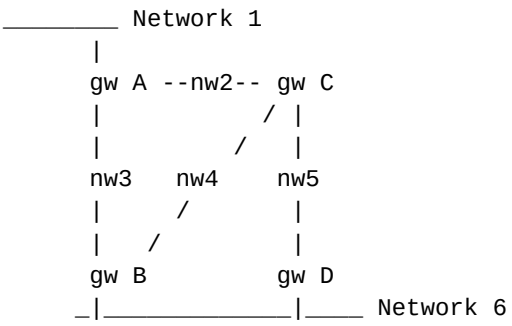
Quando un gateway viene attivato per la prima volta, viene inizializzata la relativa tabella di routing. Questa operazione può essere eseguita da un operatore da un terminale della console o leggendo le informazioni dai file di configurazione. Viene fornita una descrizione di ciascuna rete connessa al gateway, incluso il ritardo topologico lungo il collegamento (ad esempio, quanto tempo impiega un singolo bit per attraversare il collegamento) e la larghezza di banda del collegamento.

Figura 2



Ad esempio, nel diagramma di cui sopra, al gateway S viene detto che è connesso alle reti 2 e 3 tramite le interfacce corrispondenti. Pertanto, inizialmente il gateway 2 è in grado di raggiungere qualsiasi computer di destinazione nelle reti 2 e 3. Tutti i gateway sono programmati per trasmettere periodicamente ai gateway adiacenti le informazioni con cui sono stati inizializzati, nonché le informazioni raccolte da altri gateway. Pertanto, il gateway S riceverà gli aggiornamenti dai gateway R e T e apprenderà che può raggiungere i computer nella rete 1 tramite il gateway R e i computer nella rete 4 tramite il gateway T. Poiché il gateway S invia l'intera tabella di routing, nel ciclo successivo il gateway T apprenderà che può raggiungere la rete 1 tramite il gateway S. È facile vedere che le informazioni su ogni rete nel sistema raggiungeranno alla fine ogni gateway nel sistema, a condizione solo che la rete sia completamente connessa.

Figura 3



Ogni gateway calcola una metrica composita per determinare l'opportunità dei percorsi dati per i computer di destinazione. Ad esempio, nel diagramma precedente, per una destinazione nella rete 6, il gateway A (gw A) calcola le funzioni metriche per due percorsi, tramite i gateway B e C. I percorsi vengono definiti semplicemente dall'hop successivo. Esistono in realtà tre percorsi possibili da A alla rete 6:

- Diretto a B
- A C e quindi a B
- A C e quindi a D

Tuttavia, il gateway A non ha bisogno di scegliere tra le due route che coinvolgono C. La tabella di routing in A ha una singola voce che rappresenta il percorso a C. La sua metrica rappresenta il modo migliore per andare da C alla destinazione finale. Se A invia un pacchetto a C, spetta a C decidere se usare B o D.

Equazione 1

La funzione metrica composita calcolata per ciascun percorso dati è la seguente:

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

Dove r = affidabilità frazionaria (% di trasmissioni ricevute correttamente all'hop successivo), Dc = ritardo composito, Be = larghezza di banda effettiva: larghezza di banda scaricata x (1 - occupazione canali) e K1 e K2 = costanti.

Equazione 2

In linea di massima il ritardo composito, Dc, può essere determinato come indicato di seguito:

```
Dc = Ds + Dcir + Dt
```
Dove Ds = ritardo di commutazione, Dcir = ritardo di circuito (ritardo di propagazione di 1 bit) e DT = ritardo di trasmissione (ritardo a vuoto per un messaggio a 1500 bit).

Tuttavia, in pratica, per ciascun tipo di tecnologia di rete viene utilizzato un valore di ritardo standard. Ad esempio, ci sarà una cifra di ritardo standard per Ethernet e per le linee seriali a qualsiasi bit rate particolare.

Di seguito è riportato un esempio di come potrebbe apparire la tabella di routing del gateway A nel caso del diagramma Network 6 riportato sopra. Per semplicità, i singoli componenti del vettore metrico non vengono visualizzati.

Esempio di tabella di routing:

Rete	Interfaccia	Gateway successivo	Metrica
1	NUOVO 1	Nessuna	Connessione diretta
2	NUOVO 2	Nessuna	Connessione diretta
3	N. 3	Nessuna	Connessione diretta
4	NUOVO 2	C	1270
	N. 3	B	1180
5	NUOVO 2	C	1270
	N. 3	B	2130
6	NUOVO 2	C	2040
	N. 3	B	1180

Il processo di base per la creazione di una tabella di routing tramite lo scambio di informazioni con i vicini è descritto dall'algoritmo Bellman-Ford. L'algoritmo è stato utilizzato in protocolli precedenti, ad esempio RIP (RFC 1058). Per gestire reti più complesse, IGRP aggiunge tre caratteristiche all'algoritmo di base Bellman-Ford:

1. Anziché una semplice metrica, viene utilizzato un vettore di metrica per caratterizzare i percorsi. Da questo vettore è possibile calcolare un'unica metrica composita in base all'equazione 1 riportata sopra. L'uso di un vettore consente al gateway di adattarsi a diversi tipi di servizio, utilizzando diversi coefficienti differenti in Equation 1. Consente inoltre una rappresentazione più accurata delle caratteristiche della rete rispetto a una singola metrica.
2. Anziché scegliere un singolo percorso con la metrica più piccola, il traffico viene suddiviso su più percorsi con metriche che rientrano in un intervallo specificato. Ciò consente l'utilizzo parallelo di diversi percorsi, offrendo una larghezza di banda più efficace rispetto a qualsiasi percorso singolo. Una soluzione temporanea V è specificata dall'amministratore di rete. Vengono mantenuti tutti i percorsi con una metrica composita minima M. Vengono inoltre mantenuti tutti i percorsi con metrica inferiore a V x M. Il traffico viene distribuito tra più percorsi in proporzione inversa rispetto alle metriche composite.
3. Ci sono alcuni problemi con questo concetto di varianza. È difficile trovare strategie che utilizzino valori di varianza maggiori di 1 e che non conducano a cicli dei pacchetti. In Cisco release 8.2, la funzione di soluzione temporanea non è implementata. (Non so in quale

versione la funzione è stata rimossa). L'effetto è quello di impostare la varianza permanentemente su 1.

4. Sono state introdotte diverse funzionalità per garantire la stabilità in situazioni in cui la topologia sta cambiando. Queste funzioni hanno lo scopo di prevenire loop di routing e il "conteggio all'infinito", che hanno caratterizzato i precedenti tentativi di utilizzare algoritmi Ford per questo tipo di applicazioni. Le caratteristiche principali di stabilità sono "blocchi", "aggiornamenti attivati", "split-horizon" e "avvelenamento". Tali aspetti saranno discussi più dettagliatamente in appresso.

La suddivisione del traffico (punto 2) costituisce un pericolo piuttosto sottile. La soluzione temporanea V è progettata per consentire ai gateway di utilizzare percorsi paralleli di velocità diverse. Ad esempio, potrebbe essere presente una linea da 9600 BPS in esecuzione in parallelo con una linea da 19200 BPS, per la ridondanza. Se la varianza V è 1, verrà utilizzato solo il percorso migliore. Quindi la linea 9600 BPS non verrà utilizzata se la linea 19200 BPS ha una ragionevole affidabilità. Se tuttavia più percorsi sono uguali, il carico verrà condiviso tra di essi. Aumentando la varianza, possiamo permettere che il traffico venga diviso tra la rotta migliore e altre rotte che sono quasi altrettanto buone. Con una varianza sufficiente, il traffico verrà suddiviso tra le due linee. Il pericolo è che con un'ampia varianza, vengano permessi percorsi che non sono solo più lenti, ma che in realtà sono "nella direzione sbagliata". Pertanto, dovrebbe essere prevista una regola aggiuntiva per impedire l'invio del traffico "a monte": Non viene inviato alcun traffico lungo percorsi la cui metrica composita remota (la metrica composita calcolata all'hop successivo) è maggiore della metrica composita calcolata al gateway. In generale, si consiglia agli amministratori di sistema di non impostare la varianza su un valore superiore a 1, tranne in situazioni specifiche in cui è necessario utilizzare percorsi paralleli. In questo caso, la soluzione temporanea è impostata in modo da fornire i risultati "corretti".

Il protocollo IGRP è progettato per gestire più "tipi di servizi" e più protocolli. Il tipo di servizio è una specifica di un pacchetto di dati che modifica il modo in cui i percorsi devono essere valutati. Ad esempio, il protocollo TCP/IP consente al pacchetto di specificare l'importanza relativa di un'elevata larghezza di banda, di un basso ritardo o di un'alta affidabilità. In genere, le applicazioni interattive specificano un ritardo basso, mentre le applicazioni di trasferimento di massa specificano una larghezza di banda elevata. Questi requisiti determinano i valori relativi di K1 e K2 appropriati per l'uso in eq. 1. Ogni combinazione di specifiche nel pacchetto da supportare è definita come "tipo di servizio". Per ciascun tipo di servizio, è necessario scegliere una serie di parametri K1 e K2. Per ogni tipo di servizio viene mantenuta una tabella di routing. Questa operazione viene eseguita perché i percorsi vengono selezionati e ordinati in base alla metrica composita definita da Eq. 1. La situazione varia a seconda del tipo di servizio. Le informazioni provenienti da tutte queste tabelle di routing vengono combinate per produrre i messaggi di aggiornamento del routing scambiati dai gateway, come descritto nella Figura 7.

Caratteristiche di stabilità

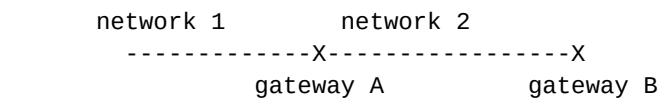
Questa sezione descrive blocchi, aggiornamenti attivati, split-horizon e intossicazione. Queste funzionalità sono progettate per evitare che i gateway rilevino percorsi errati. Come descritto nella RFC 1058 , questa condizione può verificarsi quando un percorso diventa inutilizzabile a causa di un errore di un gateway o di una rete. In linea di principio, i gateway adiacenti rilevano gli errori. Quindi inviano aggiornamenti del routing che mostrano il vecchio percorso come inutilizzabile. È tuttavia possibile che gli aggiornamenti non raggiungano affatto alcune parti della rete o che subiscano ritardi nel raggiungimento di determinati gateway. Un gateway che ritiene ancora valida la vecchia route può continuare a diffondere le informazioni, reinserendo in tal modo la route non riuscita nel sistema. Alla fine queste informazioni si propagheranno attraverso la rete e torneranno al gateway che le ha reinserite. Il risultato è un percorso circolare.

In effetti, vi è una certa ridondanza tra le contromisure. In linea di principio, le sospensioni e gli aggiornamenti attivati dovrebbero essere sufficienti per evitare innanzitutto percorsi errati. Tuttavia, in pratica, i guasti di comunicazione di vario tipo possono essere causa insufficiente. La suddivisione dell'orizzonte e l'avvelenamento del percorso hanno lo scopo di evitare loop di routing in ogni caso.

Normalmente, le nuove tabelle di routing vengono inviate ai gateway adiacenti regolarmente (per impostazione predefinita, ogni 90 secondi, anche se questa impostazione può essere modificata dall'amministratore di sistema). Un aggiornamento attivato è una nuova tabella di routing inviata immediatamente in risposta a una modifica. La modifica più importante è la rimozione di un percorso. Il problema può essere dovuto a un timeout (probabilmente una linea o un gateway adiacente è diventato inattivo) o a un messaggio di aggiornamento inviato dal gateway successivo nel percorso che indica che il percorso non è più utilizzabile. Quando un gateway G rileva che una route non è più utilizzabile, attiva immediatamente un aggiornamento. Questo aggiornamento mostrerà che la route è inutilizzabile. Considera cosa succede quando questo aggiornamento raggiunge i gateway adiacenti. Se il percorso del vicino indicava G, il vicino deve rimuovere il percorso. In questo modo il router adiacente attiva un aggiornamento, ecc. In caso di errore, verrà attivata un'ondata di messaggi di aggiornamento. L'ondata si propagherà in tutta la parte della rete in cui le route hanno attraversato il gateway o la rete con errori.

Gli aggiornamenti attivati sono sufficienti se è possibile garantire che l'ondata di aggiornamenti raggiunga immediatamente ogni gateway appropriato. Tuttavia, ci sono due problemi. In primo luogo, i pacchetti contenenti il messaggio di aggiornamento possono essere scartati o danneggiati da un collegamento nella rete. In secondo luogo, gli aggiornamenti attivati non si verificano immediatamente. È possibile che un gateway che non ha ancora ricevuto l'aggiornamento attivato esegua un aggiornamento regolare al momento sbagliato, causando il reinserimento del percorso non corretto in un router adiacente che aveva già ricevuto l'aggiornamento attivato. I blocchi sono progettati per risolvere questi problemi. La regola di controllo prevede che quando si rimuove una route, per un determinato periodo di tempo non verrà accettata alcuna nuova route per la stessa destinazione. In questo modo gli aggiornamenti attivati avranno il tempo di raggiungere tutti gli altri gateway, in modo da poter essere certi che le nuove route ottenute non siano solo gateway che reinseriscono quella precedente. Il periodo di attesa deve essere sufficientemente lungo da consentire l'esecuzione dell'ondata di aggiornamenti attivati in tutta la rete. Inoltre, deve includere due cicli di trasmissione regolari, per gestire i pacchetti ignorati. Considerare le conseguenze dell'eliminazione o del danneggiamento di uno degli aggiornamenti attivati. Il gateway che ha rilasciato l'aggiornamento eseguirà un altro aggiornamento al successivo aggiornamento regolare. In questo modo verrà riavviata l'ondata di aggiornamenti attivati nei router adiacenti che non hanno rilevato l'ondata iniziale.

La combinazione di aggiornamenti attivati e blocchi deve essere sufficiente per eliminare le route scadute e impedire che vengano reinserite. Tuttavia, vale comunque la pena adottare alcune precauzioni aggiuntive. Consentono reti molto lente e reti che sono state suddivise. Le precauzioni supplementari richieste dall'IGRP sono la separazione dell'orizzonte e l'avvelenamento del percorso. L'orizzonte diviso deriva dall'osservazione che non ha mai senso mandare una strada indietro nella direzione da cui è venuto. Considerare la situazione seguente:



Il gateway A indicherà a B di avere un percorso verso la rete 1. Quando B invia gli aggiornamenti a A, non c'è alcun motivo per menzionare la rete 1. Poiché A è più vicino a 1, non c'è alcun motivo per prendere in considerazione di passare attraverso B. La regola dell'orizzonte di divisione indica

che deve essere generato un messaggio di aggiornamento separato per ogni router adiacente (in realtà ogni rete adiacente). L'aggiornamento per un determinato router adiacente deve omettere le route che puntano a tale router adiacente. Questa regola impedisce i loop tra gateway adiacenti. Si supponga, ad esempio, che l'interfaccia di A sulla rete 1 abbia esito negativo. Senza la regola dell'orizzonte diviso, B direbbe a A che può arrivare a 1. Poiché non ha più un percorso reale, A potrebbe prendere quel percorso. In questo caso, A e B avrebbero entrambi percorsi verso 1. Ma A punterebbe a B e B punterebbe a A. Naturalmente attivati aggiornamenti e blocchi dovrebbero impedire che ciò accada. Ma siccome non c'è motivo di rimandare le informazioni al luogo da cui provengono, vale la pena di fare lo split-horizon. Oltre al ruolo di prevenzione dei loop, split horizon mantiene ridotte le dimensioni dei messaggi di aggiornamento.

La divisione dell'orizzonte deve impedire loop tra gateway adiacenti. L'avvelenamento da route ha lo scopo di rompere loop più grandi. La regola è che quando un aggiornamento indica che la metrica di una route esistente è aumentata in modo sufficiente, si verifica un loop. La via deve essere rimossa e messa in attesa. Attualmente la regola prevede che una route venga rimossa se la metrica composta aumenta di oltre un fattore di 1,1. Non è sicuro che un qualsiasi aumento della metrica composita attivi la rimozione della route, poiché è possibile che vengano apportate piccole modifiche alla metrica a causa di cambiamenti nell'occupazione o nell'affidabilità del canale. Il fattore 1,1 è euristico. Il valore esatto non è critico. Prevediamo che questa regola sia necessaria solo per interrompere loop molto grandi, poiché quelli piccoli verranno impediti da aggiornamenti e blocchi attivati.

Disabilita blocchi

A partire dalla release 8.2, il codice Cisco offre un'opzione per disabilitare le sospensioni. Lo svantaggio delle sospensioni è che ritardano l'adozione di una nuova rotta quando una vecchia rotta fallisce. Con i parametri predefiniti, possono trascorrere diversi minuti prima che un router adotti un nuovo percorso dopo una modifica. Tuttavia, per le ragioni sopra spiegate, non è sicuro semplicemente rimuovere le partecipazioni. Il risultato sarà conteggiato fino all'infinito, come descritto nella RFC 1058. Prevediamo, ma non possiamo provare, che con una versione più forte dell'avvelenamento da itinerari, le sospensioni non sono più necessarie per fermare il conto all'infinito. In questo modo, la disattivazione delle sospensioni consente una forma più forte di avvelenamento da percorso. Notare che gli aggiornamenti a divisione orizzonte e attivati sono ancora attivi.

La forma più forte di avvelenamento da route si basa sul conteggio degli hop. Se il numero di hop per un percorso aumenta, la route viene rimossa. In questo modo verranno ovviamente rimosse le route ancora valide. Se in un altro punto della rete viene modificato in modo che il percorso passi attraverso un altro gateway, il numero di hop aumenta. In questo caso, il percorso è ancora valido. Tuttavia, non esiste un modo completamente sicuro per distinguere questo caso dai loop di routing (conteggio fino all'infinito). Pertanto, l'approccio più sicuro è rimuovere il percorso ogni volta che il numero di hop aumenta. Se la route è ancora valida, verrà reinstallata dal successivo aggiornamento e verrà attivato un aggiornamento che reinstallerà la route in un'altra posizione nel sistema.

In generale, gli algoritmi dei vettori di distanza1 adottano facilmente nuove route. Il problema è eliminare completamente quelli vecchi dal sistema. Pertanto, una regola eccessivamente aggressiva sull'eliminazione delle route sospette dovrebbe essere sicura.

Dettagli del processo di aggiornamento

L'insieme di processi descritti nelle figure da 4 a 8 ha lo scopo di gestire un singolo protocollo di

rete, ad esempio TCP/IP, DECnet o il protocollo ISO/OSI. Tuttavia, i dettagli del protocollo verranno forniti solo per TCP/IP. Un singolo gateway può elaborare dati che seguono più di un protocollo. Poiché ogni protocollo ha strutture di indirizzamento e formati di pacchetto diversi, il codice informatico usato per implementare le figure da 4 a 8 sarà in genere diverso per ogni protocollo. Il processo descritto nella Figura 4 è il più variabile, come descritto nelle note dettagliate della Figura 4. I processi descritti nelle Figure da 5 a 8 hanno la stessa struttura generale. La differenza principale tra i protocolli consiste nel formato del pacchetto di aggiornamento del routing, che deve essere progettato in modo da essere compatibile con un protocollo specifico.

La definizione di una destinazione può variare da protocollo a protocollo. Il metodo qui descritto può essere utilizzato per il routing a singoli host, a reti o per schemi di indirizzi gerarchici più complessi. Il tipo di routing da utilizzare dipende dalla struttura di indirizzamento del protocollo. L'implementazione TCP/IP corrente supporta solo il routing alle reti IP. Pertanto, "destinazione" significa in realtà un numero di rete o di subnet IP. Le informazioni sulla subnet vengono mantenute solo per le reti connesse.

Nelle figure da 4 a 7 viene mostrato lo pseudo-codice di diverse fasi del processo di routing utilizzato dai gateway. All'inizio del programma, vengono immessi i protocolli e i parametri accettabili che descrivono ciascuna interfaccia.

Il gateway gestirà solo alcuni protocolli elencati. Qualsiasi comunicazione da un sistema che utilizza un protocollo non presente nell'elenco verrà ignorata. I dati immessi sono i seguenti:

- Reti a cui è connesso il gateway.
- Larghezza di banda scaricata di ogni rete.
- Ritardo topologico di ogni rete.
- Affidabilità di ogni rete.
- Occupazione dei canali di ciascuna rete.
- MTU di ciascuna rete.

La funzione metrica per ogni percorso dati viene quindi calcolata in base all'equazione 1. Si noti che i primi tre elementi sono ragionevolmente permanenti. Sono una funzione della tecnologia di rete sottostante e non dipendono dal carico. Possono essere impostati da un file di configurazione o mediante l'input diretto dell'operatore. Il protocollo IGRP non utilizza il ritardo misurato. Sia la teoria che l'esperienza suggeriscono che è molto difficile per i protocolli che usano un ritardo misurato mantenere un routing stabile. Esistono due parametri misurati: affidabilità e occupazione dei canali. L'affidabilità si basa sulle percentuali di errore riportate dall'hardware o dal firmware dell'interfaccia di rete.

Inoltre, l'algoritmo di routing richiede un valore per diversi parametri di routing. Sono inclusi i valori del timer, la varianza e l'attivazione dei blocchi. Questo valore viene in genere specificato da un file di configurazione o da un input dell'operatore. (a partire dalla versione 8.2 di Cisco, la soluzione temporanea è permanentemente impostata su 1).

Una volta immesse le informazioni iniziali, le operazioni nel gateway vengono attivate dagli eventi, sia con l'arrivo di un pacchetto dati in una delle interfacce di rete, sia con la scadenza di un timer. I processi descritti nelle figure da 4 a 7 sono attivati come segue:

- Quando arriva un pacchetto, viene elaborato in base alla Figura 4. Di conseguenza, il pacchetto viene inviato a un'altra interfaccia, scartato o accettato per un'ulteriore elaborazione.
- Quando un pacchetto viene accettato dal gateway per un'ulteriore elaborazione, viene

analizzato in un modo specifico del protocollo non descritto in questa specifica. Se il pacchetto è un aggiornamento del routing, viene elaborato in base alla Figura 5.
- La Figura 6 mostra gli eventi attivati da un timer. Il timer è impostato per generare un interrupt una volta al secondo. Quando si verifica l'interrupt, viene eseguito il processo mostrato nella Figura 6.
- La Figura 7 mostra una subroutine di aggiornamento del routing. Le chiamate a questa subroutine sono mostrate nelle figure 5 e 6.
- Inoltre, la figura 8 mostra i dettagli dei calcoli metrici di cui alle figure 5 e 7.

La propagazione e la scadenza della route sono controllate da quattro costanti di tempo critiche. Queste costanti temporali possono essere impostate dall'amministratore di sistema. Sono tuttavia disponibili valori predefiniti. Queste costanti temporali sono:

- Tempo di trasmissione: gli aggiornamenti vengono trasmessi da tutti i gateway su tutte le interfacce connesse con questa frequenza. L'impostazione predefinita è una volta ogni 90 secondi.
- Ora non valida: se non è stato ricevuto alcun aggiornamento per un determinato percorso entro questo periodo di tempo, si considera che sia scaduto. Dovrebbe durare più volte il tempo di trasmissione, in modo da consentire che i pacchetti contenenti un aggiornamento possano essere scartati dalla rete. L'impostazione predefinita è 3 volte la durata della trasmissione.
- Tempo di attesa - Quando una destinazione è diventata irraggiungibile (o la metrica è aumentata abbastanza da causare avvelenamento), la destinazione viene messa in stato di "attesa". Durante questo stato, per questo periodo di tempo non verrà accettato alcun nuovo percorso per la stessa destinazione. Il tempo di attesa indica la durata dello stato. Dovrebbe essere più volte la durata della trasmissione. Il valore predefinito è 3 volte il tempo di trasmissione più 10 secondi. Come descritto nella sezione Disabilita blocchi, è possibile disabilitare i blocchi.
- Tempo di scaricamento: se non è stato ricevuto alcun aggiornamento per una determinata destinazione entro questo periodo di tempo, la voce corrispondente viene rimossa dalla tabella di routing. Notare la differenza tra tempo non valido e tempo di scaricamento: Dopo il periodo di tempo non valido, un percorso è scaduto e rimosso. Se non ci sono percorsi rimanenti verso una destinazione, questa non è più raggiungibile. Tuttavia, la voce del database relativa alla destinazione rimane. Deve rimanere in vigore per far rispettare la sospensione. Dopo il tempo di scaricamento, la voce del database viene rimossa dalla tabella. Deve essere un po' più lungo del tempo non valido più il tempo di attesa. L'impostazione predefinita è 7 volte la durata della trasmissione.

Queste cifre presuppongono le seguenti grandi strutture di dati. Per ogni protocollo supportato dal gateway viene conservato un insieme separato di queste strutture di dati. All'interno di ogni protocollo, viene conservato un set separato di strutture di dati per ogni tipo di servizio da supportare.

Per ogni destinazione nota al sistema, esiste un elenco (probabilmente nullo) di percorsi alla destinazione, un'ora di scadenza del controllo e un'ora di ultimo aggiornamento. L'ora dell'ultimo aggiornamento indica l'ora in cui un percorso per questa destinazione è stato incluso in un aggiornamento da un altro gateway. Si noti che per ogni percorso vengono mantenuti anche gli orari di aggiornamento. Quando viene rimosso l'ultimo percorso verso una destinazione, questa viene messa in attesa, a meno che le sospensioni non siano disabilitate (per ulteriori informazioni, vedere la sezione Disabilita sospensioni). La scadenza della sospensione indica l'ora in cui la sospensione scade. Il fatto che sia diverso da zero indica che la destinazione è bloccata. Per

ridurre i tempi di calcolo, è consigliabile mantenere una metrica ottimale per ogni destinazione. Si tratta semplicemente del valore minimo delle metriche composite per tutti i percorsi alla destinazione.

Per ogni percorso verso una destinazione, c'è l'indirizzo dell'hop successivo nel percorso, l'interfaccia da usare, un vettore di metriche che caratterizzano il percorso, tra cui il ritardo topologico, la larghezza di banda, l'affidabilità e l'occupazione del canale. A ciascun percorso sono associate anche altre informazioni, tra cui il numero di hop, l'MTU, l'origine delle informazioni, la metrica composita remota e una metrica composita calcolata da questi numeri in base all'equazione 1. Esiste anche l'ora dell'ultimo aggiornamento. L'origine delle informazioni indica l'origine dell'aggiornamento più recente per il percorso. In pratica, questo è lo stesso indirizzo dell'hop successivo. L'ora dell'ultimo aggiornamento è semplicemente l'ora in cui è arrivato l'ultimo aggiornamento per questo percorso. Viene utilizzato per impostare la scadenza dei percorsi con timeout.

Un messaggio di aggiornamento IGRP è suddiviso in tre parti: interno, sistema (che significa "questo sistema autonomo" ma non interno) ed esterno. La sezione interna è destinata ai percorsi verso le subnet. Non sono incluse tutte le informazioni sulla subnet. Sono incluse solo le subnet di una rete. Rete associata all'indirizzo a cui viene inviato l'aggiornamento. Normalmente gli aggiornamenti vengono trasmessi su ogni interfaccia, quindi questa è semplicemente la rete su cui viene inviata la trasmissione. (Altri casi si verificano per le risposte a una richiesta IGRP e per i punti IGRP). Le reti principali (ad esempio, non subnet) vengono inserite nella parte di sistema del messaggio di aggiornamento a meno che non siano contrassegnate come esterne.

Una rete verrà contrassegnata come esterna se è stata appresa da un altro gateway e le informazioni sono arrivate nella parte esterna del messaggio di aggiornamento. L'implementazione di Cisco consente anche all'amministratore di sistema di dichiarare reti specifiche come esterne. Le route esterne vengono anche definite "candidate default". Si tratta di route che vanno a o attraverso i gateway considerati appropriati come predefiniti, da utilizzare in assenza di route esplicite verso una destinazione. Ad esempio, in Rutgers viene configurato il gateway che connette Rutgers alla rete regionale in modo che contrassegni il percorso alla backbone NSFnet come esterno. L'implementazione di Cisco sceglie un percorso predefinito scegliendo il percorso esterno con il valore metrico più basso.

Le sezioni che seguono intendono chiarire alcune parti delle figure da 4 a 8.

Packet Routing

La Figura 4 descrive l'elaborazione complessiva dei pacchetti di input. Questo serve semplicemente a chiarire la terminologia. Ovviamente questa non è una descrizione completa di ciò che fa un gateway IP.

Questo processo utilizza l'elenco dei protocolli supportati e le informazioni sulle interfacce immesse quando il gateway viene inizializzato. I dettagli dell'elaborazione del pacchetto dipendono dal protocollo usato dal pacchetto. Questa condizione viene determinata nel passo A. Il passo A è l'unica parte della Figura 4 condivisa da tutti i protocolli. Una volta noto il tipo di protocollo, viene utilizzata l'implementazione della Figura 4 appropriata per il tipo di protocollo. I dettagli dei contenuti del pacchetto sono descritti dalle specifiche del protocollo. Le specifiche di un protocollo includono una procedura per determinare la destinazione di un pacchetto, una procedura per confrontare la destinazione con gli indirizzi del gateway per determinare se il gateway è la destinazione, una procedura per determinare se un pacchetto è una trasmissione e una procedura per determinare se la destinazione fa parte di una rete specificata. Queste

procedure sono utilizzate nelle fasi B e C della figura 4. La prova della fase D richiede una ricerca delle destinazioni elencate nella tabella di routing. Il test è soddisfatto se esiste una voce nella tabella di routing per la destinazione e tale destinazione ha associato ad essa almeno un percorso utilizzabile. Si noti che i dati di destinazione e percorso utilizzati in questo passaggio e in quello successivo vengono gestiti separatamente per ogni tipo di servizio supportato. Questo passaggio inizia quindi con la determinazione del tipo di servizio specificato dal pacchetto e la selezione del set di strutture di dati corrispondente da utilizzare per questo passaggio e per quello successivo.

Un percorso è utilizzabile ai fini dei passi D ed E se la relativa metrica composita remota è minore della relativa metrica composita. Un percorso la cui metrica composita remota è maggiore della relativa metrica composita è un percorso il cui hop successivo è "più lontano" dalla destinazione, come misurato dalla metrica. Tale percorso viene definito "percorso a monte". Normalmente ci si aspetta che l'uso delle metriche impedisca la scelta dei percorsi a monte. È facile capire che un percorso a monte non può mai essere il migliore. Tuttavia, se è consentita una grande varianza, è possibile utilizzare percorsi diversi da quello migliore. Alcuni potrebbero essere a monte.

Il passo E calcola il percorso da utilizzare. I percorsi la cui metrica composita remota non è inferiore alle relative metriche composite non vengono considerati. Se sono accettabili più percorsi, questi vengono utilizzati in una forma ponderata di alternanza round robin. La frequenza con cui viene utilizzato un percorso è inversamente proporzionale alla relativa metrica composita.

Ricezione degli aggiornamenti di routing

Nella Figura 5 viene descritta l'elaborazione di un aggiornamento di routing ricevuto da un gateway adiacente. Tali aggiornamenti consistono in un elenco di voci, ciascuna delle quali fornisce informazioni per una singola destinazione. In un singolo aggiornamento del routing possono essere presenti più voci per la stessa destinazione, in modo da supportare più tipi di servizio. Ciascuna di queste voci viene elaborata singolarmente, come descritto nella Figura 5. Se una voce si trova nella sezione esterna dell'aggiornamento, il flag esterno sarà impostato per la destinazione se viene aggiunto come risultato di questa procedura.

L'intero processo descritto nella Figura 5 deve essere ripetuto una volta per ogni tipo di servizio supportato dal gateway, utilizzando l'insieme di informazioni di destinazione / percorso associate a quel tipo di servizio. Come mostrato nel loop più esterno nella Figura 5. L'intero aggiornamento del routing deve essere elaborato una volta per ogni tipo di servizio. (Si noti che l'implementazione corrente di IGRP non supporta più tipi di servizio, quindi il loop più esterno non è effettivamente implementato.)

Nel passo A vengono eseguiti test di accettabilità di base sul percorso. Ciò dovrebbe comprendere test di ragionevolezza per la destinazione. I numeri di rete impossibili ("Marziani") dovrebbero essere rifiutati. Per ulteriori informazioni, fare riferimento alla RFC 1009 e alla RFC 1122 . Gli aggiornamenti vengono rifiutati anche se la destinazione a cui fanno riferimento è bloccata, ovvero se la scadenza del blocco è diversa da zero e successiva all'ora corrente.

Nel passo B viene eseguita una ricerca nella tabella di routing per verificare se questa voce descrive un percorso già noto. Un percorso nella tabella di routing viene definito dalla destinazione a cui è associato, dall'hop successivo elencato come parte del percorso, dall'interfaccia di output da utilizzare per il percorso e dall'origine delle informazioni (l'indirizzo da cui proviene l'aggiornamento, in pratica lo stesso dell'hop successivo). La voce del pacchetto di aggiornamento descrive un percorso la cui destinazione è elencata nella voce, la cui interfaccia di output è l'interfaccia a cui è stato inviato l'aggiornamento e il cui hop successivo e la cui origine informazioni sono l'indirizzo del gateway che ha inviato l'aggiornamento (l'"origine").

Nei passi H e T, è pianificato il processo di aggiornamento descritto nella Figura 7. Questo processo verrà eseguito al termine dell'intero processo descritto nella Figura 5. In altri termini, il processo di aggiornamento descritto nella Figura 7 si verificherà una sola volta, anche se viene attivato più volte durante l'elaborazione descritta nella Figura 5. Inoltre, è necessario prendere precauzioni per evitare che gli aggiornamenti vengano eseguiti troppo spesso, se la rete cambia rapidamente.

Il passo K viene eseguito se la destinazione descritta dalla voce corrente nel pacchetto di aggiornamento esiste già nella tabella di routing. K confronta la nuova metrica composta calcolata dai dati nel pacchetto di aggiornamento con la metrica composta migliore per la destinazione. Tenere presente che la metrica composita migliore non viene ricalcolata in questo momento, quindi, se il percorso da considerare è già presente nella tabella di routing, questo test può confrontare le metriche nuove e vecchie per lo stesso percorso.

Il passo L viene eseguito per i percorsi peggiori della migliore metrica composta esistente. Sono inclusi sia i nuovi percorsi peggiori di quelli esistenti sia i percorsi esistenti la cui metrica composita è aumentata. Il passo L verifica se il nuovo percorso è accettabile. Si noti che questo test implementa sia il test per verificare se un nuovo percorso è sufficiente per mantenere sia il test per instradare l'avvelenamento. Per essere accettabile, il valore del ritardo non deve essere il valore speciale che indica una destinazione irraggiungibile (per l'implementazione IP corrente, tutte le destinazioni in un campo a 24 bit) e la metrica composita (calcolata come specificato nella Figura 8) deve essere accettabile. Per determinare se la metrica composta è accettabile, confrontarla con le metriche composte di tutti gli altri percorsi alla destinazione. Lasciate che M sia il minimo di questi. Il nuovo percorso è accettabile se è < V X M, DOVE V È LA VARIANZA IMPOSTATA AL MOMENTO DELL'INIZIALIZZAZIONE DEL GATEWAY. SE V = 1 (CHE È SEMPRE VERO COME IN CISCO RELEASE 8.2), UNA METRICA QUALSIASI PEGGIORE DI QUELLA ESISTENTE NON È ACCETTABILE. VI È UN'ECCEZIONE: SE IL PERCORSO ESISTE GIÀ ED È L'UNICO PERCORSO VERSO LA DESTINAZIONE, VERRÀ MANTENUTO SE LA METRICA NON È AUMENTATA DI OLTRE IL 10% (O SE I BLOCCHI SONO DISABILITATI, SE IL NUMERO DI HOP NON È AUMENTATO).

Il passo V viene eseguito quando le nuove informazioni per un percorso indicano che la metrica composita verrà ridotta. Vengono confrontate le metriche composite di tutti i percorsi alla destinazione D. In questo confronto viene utilizzata la nuova metrica composita per P anziché quella visualizzata nella tabella di routing. Viene calcolata la metrica composita minima M. Quindi tutti i percorsi a D vengono esaminati di nuovo. Se la metrica composita per un percorso > M x V, tale percorso viene rimosso. V è la soluzione temporanea immessa quando è stato inizializzato il gateway. (a partire dalla versione 8.2 di Cisco, la soluzione temporanea è permanentemente impostata su 1).

Elaborazione periodica

Il processo descritto nella Figura 6 viene attivato una volta al secondo. Esamina i vari timer nella tabella di routing per verificare se sono scaduti. Questi timer sono descritti in precedenza.

Nel passo U, viene attivato il processo descritto nella Figura 7.

Le fasi R e S sono necessarie perché le metriche composite memorizzate nella tabella di routing dipendono dall'occupazione del canale, che varia nel tempo in base alle misurazioni. L'occupazione dei canali viene ricalcolata periodicamente, utilizzando una media mobile del traffico misurato attraverso l'interfaccia. Se il nuovo valore calcolato differisce da quello esistente, tutte le metriche composite che interessano l'interfaccia devono essere modificate. Vengono

esaminati tutti i percorsi mostrati nella tabella di routing. La metrica composita di qualsiasi percorso il cui hop successivo utilizzi l'interfaccia "I" viene ricalcolata. Questa operazione viene eseguita in base all'equazione 1, utilizzando come occupazione del canale il valore massimo del valore memorizzato nella tabella di routing come parte della metrica del percorso e l'occupazione del canale appena calcolata dell'interfaccia.

Genera messaggi di aggiornamento

Nella figura 7 viene descritto come il gateway genera messaggi di aggiornamento da inviare ad altri gateway. Per ogni interfaccia di rete collegata al gateway viene generato un messaggio separato. Il messaggio viene quindi inviato a tutti gli altri gateway raggiungibili tramite l'interfaccia (passaggio J). In genere, questa operazione viene eseguita inviando il messaggio come trasmissione. Tuttavia, se la tecnologia di rete o il protocollo non consente le trasmissioni, potrebbe essere necessario inviare il messaggio individualmente a ciascun gateway.

In generale, il messaggio viene generato aggiungendo una voce per ciascuna destinazione nella tabella di routing, nel passo G. Si noti che è necessario utilizzare i dati di destinazione/percorso associati a ciascun tipo di servizio. Nel caso peggiore, viene aggiunta una nuova voce all'aggiornamento per ogni destinazione per ogni tipo di servizio. Tuttavia, prima di aggiungere una voce al messaggio di aggiornamento nel passo G, vengono analizzate le voci già aggiunte. Se la nuova voce è già presente nel messaggio di aggiornamento, non verrà aggiunta di nuovo. Una nuova voce duplica una voce esistente quando le destinazioni e i gateway dell'hop successivo sono gli stessi.

Per semplicità, lo pseudocodice omette una cosa: i messaggi di aggiornamento IGRP sono composti da tre parti: interno, sistema ed esterno, il che significa che ci sono in realtà tre loop sulle destinazioni. La prima include solo le subnet della rete a cui viene inviato l'aggiornamento. La seconda include tutte le reti principali, ad esempio non subnet, che non sono contrassegnate come esterne. La terza include tutte le reti principali contrassegnate come esterne.

Il passo E implementa il test dell'orizzonte di divisione. In caso normale, questo test non riesce per le route il cui percorso migliore esce dalla stessa interfaccia a cui viene inviato l'aggiornamento. Tuttavia, se l'aggiornamento viene inviato a una destinazione specifica (ad esempio, in risposta a una richiesta IGRP da un altro gateway o come parte di "IGRP point to point"), la divisione dell'orizzonte ha esito negativo solo se il miglior percorso proviene originariamente da tale destinazione (la sua "origine informazioni" è la stessa della destinazione) e la relativa interfaccia di output è la stessa di quella da cui è arrivata la richiesta.

Calcola informazioni metriche

La Figura 8 descrive come le informazioni della metrica vengono elaborate dai messaggi di aggiornamento ricevuti dal gateway e come vengono generate per i messaggi di aggiornamento inviati dal gateway. Si noti che la voce si basa su un percorso specifico verso la destinazione. Se esistono più percorsi alla destinazione, viene scelto un percorso la cui metrica composta è il minimo. Se più percorsi hanno la metrica composita minima, viene utilizzata una regola di interruzione della connessione arbitraria. Per la maggior parte dei protocolli, questo valore è basato sull'indirizzo del gateway dell'hop successivo.

Figura 4 - Elaborazione dei pacchetti in arrivo

```
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.
```

Figura 5 - Elaborazione degli aggiornamenti del routing in ingresso

```
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
```

Figura 6 - Elaborazione periodica

```
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
```

Figura 7 - Genera aggiornamento

```
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
```

Figura 8 - Dettagli dei calcoli delle metriche

In questa sezione viene descritta la procedura per calcolare le metriche e i conteggi degli hop da un aggiornamento del routing in arrivo. L'input per questa funzione è la voce per una destinazione specifica in un pacchetto di aggiornamento del routing. L'output è un vettore di metriche che possono essere utilizzate per calcolare la metrica composita e un conteggio hop. Se questo percorso viene aggiunto alla tabella di routing, nella tabella viene immesso l'intero vettore della metrica. I parametri di interfaccia utilizzati nelle definizioni seguenti sono quelli impostati quando il gateway è stato inizializzato per l'interfaccia a cui è arrivato l'aggiornamento del routing, con la differenza che l'occupazione e l'affidabilità del canale sono basate su una media mobile del traffico misurato attraverso l'interfaccia.

- Ritardo = ritardo da pacchetto + ritardo topologico interfaccia
- Larghezza di banda = max (larghezza di banda da pacchetto, larghezza di banda interfaccia)
- Affidabilità = min (affidabilità dal pacchetto, affidabilità dell'interfaccia)
- Occupazione canale = max (occupazione canale da pacchetto, occupazione canale interfaccia)Il valore Max viene utilizzato per la larghezza di banda perché la metrica della larghezza di banda è memorizzata in forma inversa. Dal punto di vista concettuale, è necessaria la larghezza di banda minima). Notare che l'occupazione del canale originale del pacchetto deve essere salvata, poiché sarà necessaria per ricalcolare l'occupazione del canale effettiva ogni volta che cambia l'occupazione del canale interfaccia.

Gli elementi riportati di seguito non fanno parte del vettore metrico, ma vengono mantenuti nella tabella di routing come caratteristiche del percorso.

- Conteggio hop = conteggio hop dal pacchetto.
- MTU = min (MTU dal pacchetto, MTU dell'interfaccia).
- Metrica composita remota = calcolata a partire dall'equazione 1 utilizzando i valori delle metriche del pacchetto. In altre parole, i componenti metrici sono quelli del pacchetto e non vengono aggiornati come mostrato in precedenza. Ovviamente, questo valore deve essere calcolato prima di effettuare le regolazioni sopra indicate.
- Metrica composita = calcolata a partire dall'equazione 1 utilizzando i valori delle metriche calcolati come descritto in questa sezione.

Nella parte restante di questa sezione viene descritta la procedura per calcolare le metriche e il numero di hop per l'invio degli aggiornamenti del routing.

Questa funzione determina le informazioni metriche e il numero di hop da inserire in un pacchetto di aggiornamento in uscita. Si basa su un percorso specifico verso una destinazione, se esistono percorsi utilizzabili. Se non ci sono percorsi o se i percorsi sono tutti a monte, la destinazione è chiamata "inaccessibile".

```
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.
```

Dettagli sull'implementazione IP

In questa sezione vengono descritti i formati di pacchetto utilizzati da Cisco IGRP. Il protocollo IGRP viene inviato utilizzando datagrammi IP con protocollo IP 9 (IGP). Il pacchetto inizia con un'intestazione. Inizia subito dopo l'intestazione IP.

```
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 */
```

Per i messaggi di aggiornamento, le informazioni di instradamento seguono immediatamente dopo l'intestazione.

Il numero di versione è attualmente 1. I pacchetti con altri numeri di versione vengono ignorati.

Il codice operativo può essere 1 = aggiornamento o 2 = richiesta.

Indica il tipo di messaggio. Il formato dei due tipi di messaggi sarà specificato di seguito.

Edition è un numero di serie che viene incrementato ogni volta che viene apportata una modifica alla tabella di routing. Questa operazione viene eseguita nelle condizioni in cui lo pseudocodice indicato in precedenza attiva un aggiornamento del routing. Il numero di edizione consente ai gateway di evitare l'elaborazione di aggiornamenti contenenti informazioni già visualizzate. (Attualmente non implementato. In altre parole, il numero di edizione viene generato correttamente, ma viene ignorato durante l'input. Poiché è possibile che i pacchetti vengano ignorati, non è chiaro se il numero di edizione sia sufficiente per evitare l'elaborazione di duplicati. È necessario verificare che tutti i pacchetti associati all'edizione siano stati elaborati.)

Sistema è il numero del sistema autonomo. Nell'implementazione di Cisco, un gateway può partecipare a più di un sistema autonomo. Ciascun sistema esegue il proprio protocollo IGRP. Dal punto di vista concettuale, esistono tabelle di routing completamente separate per ogni sistema autonomo. Le route che arrivano tramite IGRP da un sistema autonomo vengono inviate solo negli aggiornamenti per tale appliance ASA. Questo campo consente al gateway di selezionare il set di tabelle di routing da utilizzare per l'elaborazione del messaggio. Se il gateway riceve un messaggio IGRP per un'appliance ASA per cui non è configurato, viene ignorato. Infatti, l'implementazione Cisco consente la "fuoriuscita" di informazioni da un SA all'altro. Tuttavia, lo considero uno strumento amministrativo e non parte del protocollo.

Ninterior, *nsystem* ed *exterior* indicano il numero di voci in ciascuna delle tre sezioni dei messaggi di aggiornamento. Queste sezioni sono state descritte in precedenza. Non c'è altra delimitazione tra le sezioni. Le prime voci interne sono quelle interne, le voci di sistema successive sono quelle

esterne e l'esterno finale è quello esterno.

Checksum è un checksum IP calcolato utilizzando lo stesso algoritmo di checksum di un checksum UDP. Il checksum viene calcolato sull'intestazione IGRP e sulle eventuali informazioni di routing successive. Il campo checksum è impostato su zero durante il calcolo del checksum. Il checksum non include l'intestazione IP, né un'intestazione virtuale come in UDP e TCP.

Richieste

Una richiesta IGRP chiede al destinatario di inviare la relativa tabella di routing. Il messaggio di richiesta ha solo un'intestazione. Vengono utilizzati solo i campi versione, codice operativo e sistema. Tutti gli altri campi sono zero. Il destinatario deve inviare un normale messaggio di aggiornamento IGRP al richiedente.

Aggiornamenti

Un messaggio di aggiornamento IGRP contiene un'intestazione, seguita immediatamente dalle voci di routing. Vengono incluse tutte le voci di routing adatte a un datagramma di 1500 byte (inclusa l'intestazione IP). Con le dichiarazioni di struttura correnti, questo consente fino a 104 voci. Se sono necessarie più voci, vengono inviati diversi messaggi di aggiornamento. Poiché i messaggi di aggiornamento vengono semplicemente elaborati immissione per voce, non vi è alcun vantaggio nell'utilizzare un singolo messaggio frammentato anziché più messaggi indipendenti.

Di seguito è riportata la struttura di una voce di instradamento:

```
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 */
```

I campi definiti uchar[2] e uchar[3] sono semplicemente numeri interi binari a 16 e 24 bit, nell'ordine normale della rete IP.

Num definisce la destinazione da descrivere. È un indirizzo IP. Per risparmiare spazio, vengono forniti solo i primi 3 byte dell'indirizzo IP, ad eccezione della sezione internal. Nella sezione internal, vengono forniti gli ultimi 3 byte. Per le route di sistema e esterne, non è possibile utilizzare subnet, pertanto il byte di ordine inferiore è sempre zero. Le route interne sono sempre subnet di una rete nota, pertanto viene fornito il primo byte di tale numero di rete.

Il ritardo è espresso in unità di 10 microsecondi. Questo dà un intervallo da 10 microsecondi a 168 secondi, che sembra sufficiente. Il ritardo di tutti indica che la rete non è raggiungibile.

La larghezza di banda è inversa in bit al secondo e viene scalata di un fattore di 1,0e10. L'intervallo va da una linea a 1200 BPS a 10 Gbps. (ovvero, se la larghezza di banda è N Kbps, il numero utilizzato è 10000000 / N.)

L'MTU è espressa in byte.

L'affidabilità è espressa come frazione di 255, ovvero 255 equivale al 100%.

Il carico viene espresso come frazione di 255.

Il conteggio hop è un conteggio semplice.

A causa delle strane unità utilizzate per la larghezza di banda e il ritardo, alcuni esempi sembrano in ordine. Si tratta dei valori predefiniti utilizzati per diversi supporti comuni.

	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

Calcoli delle metriche

Di seguito è riportata una descrizione del modo in cui la metrica composita viene effettivamente calcolata in Cisco versione 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
```

Informazioni correlate

- Pagina di supporto per il routing IP
- Pagina di supporto del protocollo IGRP
- Supporto tecnico – Cisco Systems