

Traduzione di Pizzichetti Lino Centesperimat Treviso settembre 1997 spvgw1@cente.glt.org

RIP Versione 2 **Trasportare più informazioni**

Stato di questo Memorandum

Questo documento indica la strada per un protocollo standard IAB per la comunità Internet, e ne chiede discussione e suggerimenti per migliorarlo. Si faccia riferimento alla corrente edizione "IAB Official Protocol Standards" per lo stato di standardizzazione di questo protocollo. La distribuzione di questo memorandum è illimitata.

Astratto

Questo documento specifica una estensione di Routing Information Protocol (RIP), come definito al punto 1, per aumentare la quantità di informazione utile trasportata nei pacchetti RIP e per aggiungere una misura di sicurezza. Un documento allegato definirà gli oggetti SNMP MIB per il RIP-2.

Ringraziamenti

Vorrei ringraziare le seguenti persone per il loro contributo alla stesura di questo documento:
Fred Baker, Noel Chiappa and Vince Fuller.

Questo memorandum è un prodotto del Gruppo di Lavoro RIP-2 dell'Internet Engineering Task Force (IETF).

Tabella dei Contenuti

1. Giustificazione	2
2. RIP attuale	2
3. Estensioni al Protocollo	2
3.1 Autenticazione	3
3.2 Dominio di instradamento (Routing Domain)	4
3.3 Marcatura delle Rotte (Route Tag)	4
3.4 Machera di Sottorete (Subnet Mask)	4
3.5 Salto successivo (Next Hop)	4
3.6 Trasmissione in modo Multicasting	5
4. Compatibilità	5
4.1 Commutatore di Compatibilità (Compatibility Switch)	5
4.2 Autenticazione	5
4.3 Infinito più grande	5
4.4 Collegamenti senza Indirizzo (Addressless Links)	6
Appendice A	6
Referenze	6
Considerazioni sulla Sicurezza	6

1. Giustificazione.

Con l'avvento di OSPF e IS-IS, ci sono quelli che credono che RIP sia obsoleto. Mentre è vero che i nuovi protocolli di instradamento interni (IGP) sono molto superiori al RIP, questo mantiene alcuni vantaggi. Primo, in piccole reti, RIP pesa poco in termini di larghezza di banda utilizzata e tempo di configurazione e gestione. RIP è anche molto semplice da implementare, specialmente in relazione ai più nuovi protocolli interni.

Inoltre ci sono molte più implementazioni RIP sul campo rispetto a OSPF e IS-IS messe assieme ed è probabile che rimanga così per alcuni anni ancora.

Dato che RIP sarà utile in molti ambienti per certi periodi, è ragionevole aumentarne l'utilità. Ciò è vero, poiché il guadagno è molto più grande rispetto al costo del cambiamento.

2. RIP attuale.

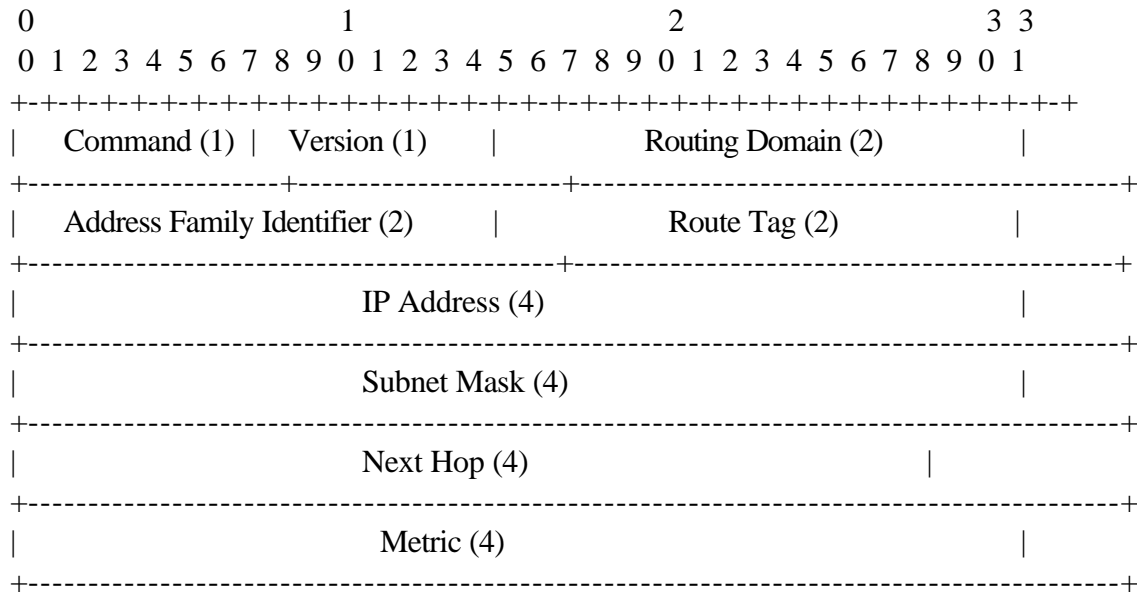
L'attuale pacchetto RIP contiene la quantità minima d'informazioni necessaria ai routers per instradare i pacchetti attraverso una rete. Contiene anche una gran quantità di spazio inutilizzato, dovuto alle sue origini.

L'attuale protocollo RIP non considera i sistemi autonomi e le interazioni con altri protocolli d'instradamento interni o esterni (IGP/EGP), sottoreti, e autenticazione poiché le implementazioni di questi sono successive al RIP. La mancanza di maschere di sottorete è un problema particolarmente serio per i routers poiché essi necessitano di una maschera di sottorete per sapere come determinare una rotta. Se una rotta RIP è una rotta di rete (tutti i bit a 0 nella parte host dell'indirizzo IP), la maschera di sottorete equivale alla maschera di rete. Comunque, se alcuni dei bits sono impostati nella parte host, il router non può determinare se la rotta IP è di tipo sottorete o host. Attualmente, alcuni routers scelgono semplicemente la maschera di sottorete dell'interfaccia sulla quale la rotta è stata acquisita e determina il tipo di rotta da quella.

3. Estensioni al protocollo

Questo documento non cambia il protocollo RIP in se. Piuttosto, esso fornisce estensioni al formato dei datagrammi che consente ai routers di condividere importanti informazioni aggiuntive.

Il nuovo formato del protocollo RIP è:

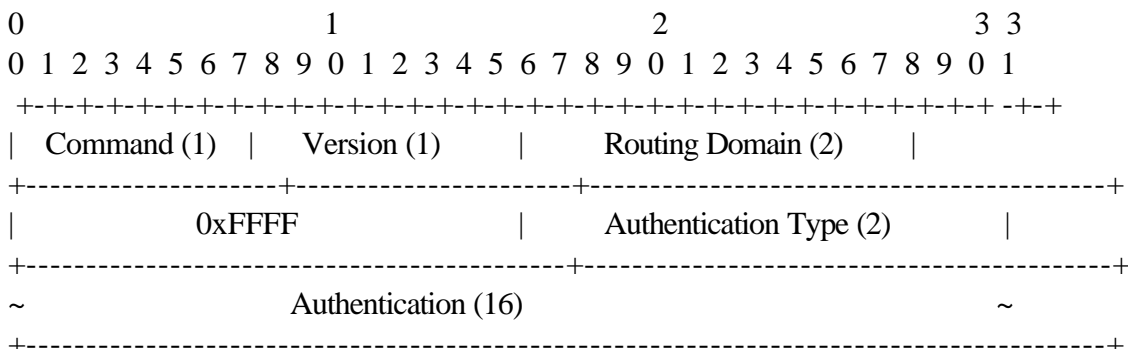


I campi, Address Family Identifier (AFI), IP address, e Metric hanno tutti i significati definiti nel RFC 1058. Il campo Version specificherà il numero di versione 2 per i datagrammi RIP che usano l'autenticazione o porta informazioni in alcuni dei nuovi campi.

Tutti i campi sono codificati nell'ordine di byte rete IP (big-endian).

3.1 Autenticazione

Poiché l'autenticazione è una funzione per pacchetto, poiché c'è un solo campo di due byte disponibile nella testata del pacchetto, e siccome qualsiasi schema ragionevole di autenticazione richiederebbe più di due byte, lo schema di autenticazione per la versione 2 del RIP userà lo spazio di una intera voce RIP. Se l'Identificatore della Famiglia d'Indirizzo della prima (e solo il primo) voce nel pacchetto è 0xFFFF, allora il resto della voce contiene l'autenticazione. Questo significa che ci possono essere, almeno 24 elementi RIP nel resto del pacchetto. Se l'autenticazione non è in uso, allora nessuna voce nel pacchetto dovrebbe avere un Identificatore della Famiglia d'Indirizzi posto a 0xFFFF. Un pacchetto RIP che contiene una voce d'autenticazione, avrà il seguente formato:



Attualmente, l'unico tipo di autenticazione, è la semplice password ed è tipo 2. I rimanenti sedici bytes contengono la parola chiave in chiaro. Se la parola chiave è inferiore a sedici bytes, essa deve essere giustificata a sinistra e riempita verso destra con caratteri nulli (0x00).

3.2 Domini di instradamento (Routing domain).

Il valore di Routing Domain è il numero di processo d'instradamento al quale quest'aggiornamento appartiene. Il campo è utilizzato per associare l'aggiornamento ad un processo di routing specifico sul router che sta ricevendo. Il Routing Domain è necessario per consentire "nuvole" multiple, indipendenti di RIP affinché coesistano sulla stessa rete fisica. Questo da agli amministratori la capacità di avviare istanze multiple, possibilmente parallele, di RIP allo scopo di implementare una semplicemente politica. Ciò significa che un router che opera all'interno di un dominio d'instradamento, o un insieme di domini d'instradamento, dovrebbe ignorare i pacchetti RIP che appartengono ad una altro dominio di routing. Il dominio zero è il valore predefinito di routing domain.

3.3 Marcatura delle Rotte (Route Tag)

Il campo marcatura delle rotte (Route Tag) esiste come supporto per i protocolli esterni (EGP). I contenuti e l'uso di questo campo vanno al di fuori dello scopo di questo protocollo. In ogni modo, ci si aspetta che il campo sarà utilizzato per trasportare i numeri di sistema autonomo (AS) per protocolli esterni EGP e BGP. Qualsiasi sistema RIP che riceva una voce che contenga un valore di RT (Route Tag) diverso da zero, deve ripubblicare quel valore. Quei routers che non hanno un valore di RT, devono pubblicare un valore di RT a zero.

3.4 Maschera di Sottorete (Subnet mask)

Questo campo contiene la maschera di sottorete che è applicata all'indirizzo IP per produrre la porzione non host dell'indirizzo. Se questo campo è zero, allora nessuna maschera di sottorete è stata inclusa per questa voce.

Su un'interfaccia dove un router RIP-1 può ascoltare e operare sull'informazione nella voce d'instradamento RIP-2 si applicano le seguenti due regole:

- 1) L'informazione interna ad una rete non deve mai essere pubblicizzata in un'altra, e
- 2) L'informazione circa una più specifica sottorete può non essere pubblicata dove i router RIP-1 la considerano come una rotta host.

3.5 Salto Successivo (Next Hop)

Esso rappresenta il salto immediatamente successivo dell'indirizzo IP al quale dovrebbero essere inoltrati i pacchetti per la destinazione specificata da questa voce rotta. Specificando un valore di 0.0.0.0. in questo campo indica che l'instradamento dovrebbe avvenire attraverso l'originatore delle emissioni RIP. Un

indirizzo specificato come salto successivo deve, per forza, essere raggiungibile direttamente sulla sottorete logica sulla qual è stata eseguita l'emissione.

Il proposito del campo Next Hop (salto successivo) è eliminare pacchetti in via d'instradamento attraverso altri salti sul sistema. È particolarmente utile quando RIP non è attivo su tutti i routers sulla rete. Un esempio semplice è mostrato nell'appendice A. Da notare che il campo Next Hop è consigliabile. Cioè, se l'informazione fornita è ignorata, può essere scelta una possibile rotta non ottimale, ma assolutamente valida.

3.7 Multicasting

Allo scopo di ridurre il carico sui computer che stanno ascoltando pacchetti RIP-2, sarà utilizzato un indirizzo IP multicast per un'emissione periodica broadcast. Vale a dire 224.0.0.9. Da notare che il protocollo IGMP non è necessario essendo questi messaggi tra router che non vengono inoltrati.

Allo scopo di mantenere la compatibilità all'indietro, l'utilizzo dell'indirizzo multicast sarà configurabile, come descritto nella sezione 4.1. Se fosse utilizzato multicast, dovrebbe essere utilizzato su tutte le interfacce che lo supportano.

4. Compatibilità

Il documento RFC 1058 ha mostrato considerevole lungimiranza nella sua specifica nella gestione dei numeri di versione. Esso specifica che pacchetti RIP di versione zero sono scartati, che pacchetti RIP di versione uno saranno scartati se il campo Must Be Zero (MBZ) è diverso da zero, e che i pacchetti RIP di qualsiasi versione più grande di uno non dovrebbero essere scartati semplicemente perché il campo MBZ contiene un valore diverso da zero. Ciò significa che la nuova versione di RIP è totalmente compatibile indietro con le esistenti implementazioni RIP che aderiscono a questa parte della specifica.

4.1 Commutatore di compatibilità (Compatibility Switch)

Un commutatore di compatibilità diventa necessario per due ragioni. Primo, ci sono implementazioni di RIP-1 sul campo che non seguono le indicazioni del documento RFC 1058, come descritto qui sopra. Secondo, l'uso d'emissioni multicasting impedirebbe ai sistemi con RIP-1 di ricevere aggiornamenti RIP-2 (che può essere una caratteristica desiderabile in alcuni casi).

Il commutatore ha tre impostazioni: RIP-1, nel quale solo pacchetti RIP-1 vengono inviati; compatibilità RIP-1, nel quale pacchetto RIP-2 vengono inviati come broadcasts; e RIP-2, nel quale pacchetti RIP-2 vengono inviati come multicast. Il valore predefinito raccomandato per questo commutatore è la compatibilità con RIP-1.

4.2 Autenticazione

Poiché una voce autenticazione è marcata con un identificatore di famiglia d'indirizzi con valore di 0xFFFF, un sistema RIP-1 ignorerebbe questa voce poiché essa apparterebbe ad una famiglia d'indirizzi diversa da IP. Da notare, perciò, che l'uso d'autenticazione non impedisce a sistemi RIP-1 di vedere pacchetti RIP-2. Se desiderato questo può essere effettuato utilizzando emissioni multicasting, come descritto nelle sezioni 3.6 e 4.1.

4.3 Valore d'infinito più grande

Sul tema della compatibilità, c'è un elemento che la gente ha richiesto: incremento del valore infinito. Ciò non si può realizzare per la ragione che sarebbe una violazione di compatibilità all'indietro. Un valore d'infinito più grande confonderebbe ovviamente le più vecchie versioni di RIP. Nel caso migliore, esse ignorerebbero la rotta perchè ignorerebbero una metrica di sedici. C'è stata anche una proposta per rendere la metrica un byte singolo e riutilizzare i tre bytes più alti, ma ciò interromperrebbe qualsiasi implementazione che tratta la metrica come una lunghezza.

4.4 Collegamenti senza indirizzi.

I collegamenti senza indirizzo non saranno supportati da RIP-2, come già accade in RIP-1.

Appendice A

Questo che segue è un esempio dell'uso del campo Next Hop in un pacchetto RIP.

```
-----
|IR1| |IR2| |IR3|           |XR1| |XR2| |XR3|
-+-+ -+-+ -+-+           -+-+ -+-+ -+-+
|      |      |           |      |      |
+-----+-----+-----+-----+-----+
<-----RIP-2----->
```

Si assuma che IR1, IR2, e IR3 siano tutti routers "interni". Essi sono sotto un'amministrazione, (per es. un campus) che ha scelto di utilizzare RIP-2 come suo protocollo interno (IGP). XR1, XR2, e XR3, dall'altra parte, sono sotto separata amministrazione (per esempio, una rete regionale, della quale il campus è un membro) e stanno utilizzando alcuni protocolli d'instradamento diversi (per es., OSPF). XR1, XR2, e XR3 scambiano informazioni di instradamento tra di loro cosicchè essi sanno che la miglior rotta alla rete N1 e N2 sia via XR1, verso N3, N4, e N5 sono via XR2, e verso N6 e N7 sono via XR3. Impostando il campo Next Hop correttamente (verso XR2 per N3/N4/N5, verso XR3 per N6/N7), solo XR1 necessita di scambiare rotte RIP-2 con IR1/IR2/IR3 per instradare affinché accada senza ulteriori salti via XR1. Senza l'impiego del "salto successivo" (per es., se fosse utilizzato RIP-1) sarebbe necessario per XR2 e XR3 partecipare anche al protocollo RIP-2 per eliminare salti ulteriori.

Referenze

- [1] Hedrick, C., "Routing Information Protocol", RFC 1058, Rutgers University, June 1988.
- [2] Malkin, G., and F. Baker, "RIP Version 2 MIB Extension", RFC 1389, Xylogics, Inc., Advanced Computer Communications, January 1993.
- [3] Malkin, G., "RIP Version 2 Protocol Analysis", RFC 1387, Xylogics, Inc., January 1993

Considerazioni sulla sicurezza

RIP base non è un protocollo sicuro. Per portare RIP-2 in linea con i protocolli d'instradamento più moderni, un meccanismo d'estensione dell'autenticazione è stato incorporato nelle migliorie del protocollo. Questo meccanismo viene descritto nella sezione 3.1 e 4.2.

Indirizzo dell'autore

Gary Scott Malkin Xylogics, Inc. 53 Third Avenue Burlington, MA 01803 Phone: (617) 272-8140 EMail: gmalkin@Xylogics.COM