

Network Working Group
Request for Comments: 1723
Aggiorna: RFC 1058
Rende obsoleta: RFC 1388

G. Malkin
Xylogics, Inc.

Novembre 1994

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 per la comunità Internet, e ne chiede discussione e suggerimenti per migliorarlo. Si faccia riferimento alla corrente edizione "Internet Official Protocol Standards" (STD 1) per lo stato di standardizzazione di questo protocollo. La distribuzione di questo memorandum è illimitata.

Astratto

Questo documento specifica un'estensione di Routing Information Protocol (RIP), come definito ai punti uno e due, per aumentare la quantità d'informazione utile trasportata nei pacchetti RIP e per aggiungere una misura di sicurezza. Questo documento rende obsoleto RFC 1388, che specifica un aggiornamento al "Routing Information Protocol" STD 34, RFC 1058.

L'analisi del protocollo RIP-2 è documentata in RFC 1721 (4).

Le dichiarazioni d'applicabilità di RIP-2 è documentata in RFC 1722 (5)

La descrizione di RIP-2 è definita in RFC 1724 (3). Tale memorandum rende obsoleta RFC 1389.

Ringraziamenti

Vorrei ringraziare il Gruppo di Lavoro ripv2 dell'Internet Engineering Task Force (IETF) per il loro aiuto a migliorare il protocollo RIP-2.

Tabella dei Contenuti

1. Giustificazione	2
2. RIP attuale	2
3. Estensioni al Protocollo	2
3.1 Autenticazione	3
3.2 Marcatura delle Rotte (Route Tag)	4
3.3 Machera di Sottorete (Subnet Mask)	4
3.4 Salto successivo (Next Hop)	4
3.5 Trasmissione in modo Multicasting	5
3.5 Richieste	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

5 Considerazioni sulla sicurezza	6
Appendice A	6
Referenze	6
Indirizzo dell'Autore	6

1. Giustificazione.

Con l'avvento di OSPF e IS-IS, ci sono persone 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 riguardo 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 ancora più vero, poiché il guadagno è molto più grande rispetto al costo del cambiamento.

2. RIP attuale.

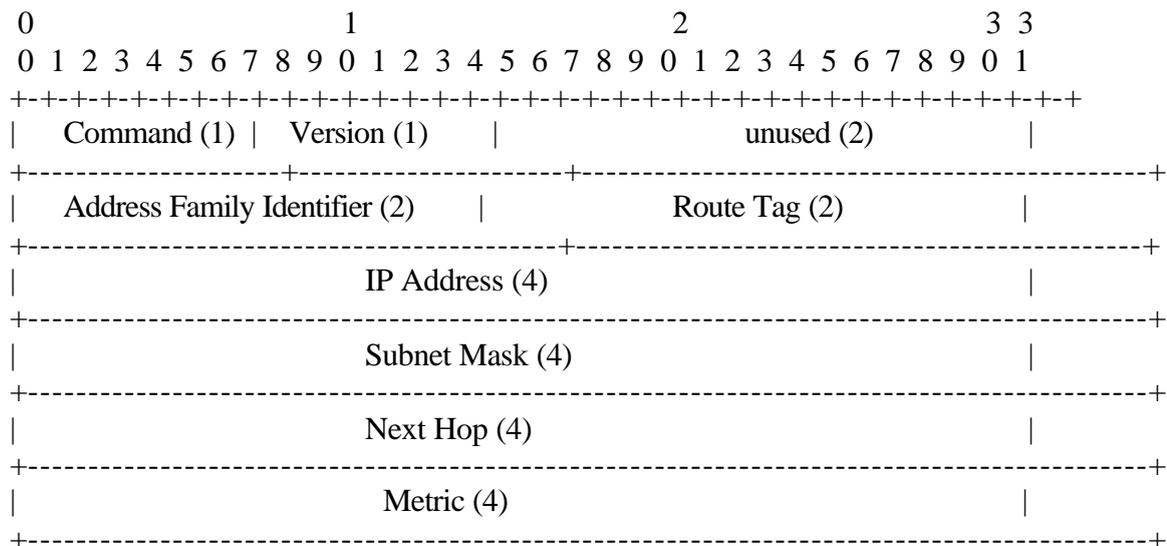
L'attuale pacchetto RIP contiene la quantità minima d'informazione necessaria ai routers per instradare i messaggi attraverso una rete. Contiene anche una gran quantità di spazio inutilizzato, dovuto alle sue origini.

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. Una rotta RIP è una rotta di rete (tutti i bit a zero 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. Ora, 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 messaggi che consente ai routers di condividere importanti informazioni aggiuntive.

Il nuovo formato del protocollo RIP è:

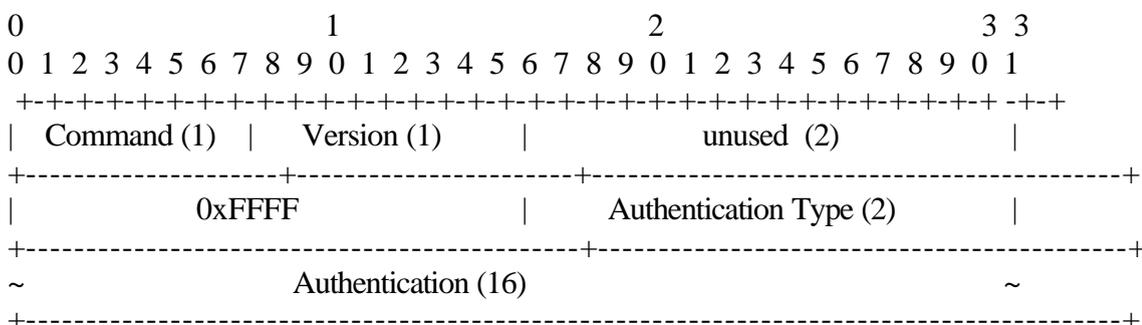


I campi, Address Family Identifier (AFI), IP address, e Metric hanno tutti i significati definiti nel RFC 1058. Il campo Version specificherà il numero di versione due per i datagrammi RIP che usano l'autenticazione o porta informazioni in alcuni dei nuovi campi. Il contenuto del campo *unused* (due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

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

3.1 Autenticazione

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



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

3.2 Marcatura delle Rotte (Route Tag)

Il campo marcatura delle rotte (Route Tag) è un attributo assegnato alla rotta che deve essere preservato e ripubblicata con una rotta. Lo scopo di Route Tag è fornire un metodo per separare le rotte “interne” RIP (rotte per reti interne entro il dominio di routing RIP) dalle rotte “esterne” RIP, che possono essere state importate da un protocollo EGP o un altro IGP.

I routers che supportano protocolli diversi da RIP, dovrebbero essere configurabili per consentire la marcatura delle rotte (Route Tag) per le rotte importate da differenti fonti. Per esempio, le rotte importate dal protocollo EGP o BGP dovrebbero essere in grado di avere il loro Route Tag impostato ad un valore arbitrario, o almeno al numero di Autonomous System dal quale le rotte sono state apprese.

Altri usi di Route Tag sono validi, purchè tutti i routers nel dominio RIP siano d'accordo. Ciò consentirà di realizzare un documento per l'interazione tra i protocolli BGP-RIP, che dovranno descrivere i metodi per sincronizzare l'instradamento in una rete di transito.

3.3 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 regole:

- 1) L'informazione interna ad una rete non deve mai essere pubblicizzata in un'altra rete,
- 2) L'informazione circa una più specifica sottorete può non essere pubblicata dove i router RIP-1 la considerano come una rotta host.
- 3) Rotte superrete (rotte con un netmask meno specifico della naturale maschera di rete) non devono essere pubblicate dove queste possono essere mal interpretate dai routers RIP-1.

3.4 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 quale si compie l'emissione.

Il proposito del campo Next Hop (salto successivo) è eliminare pacchetti in via d'instradamento attraverso nuovi 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 consigliato. Cioè, se l'informazione fornita è ignorata, può essere scelta una possibile rotta non ottimale, ma assolutamente valida.

3.5 Multicasting

Allo scopo di ridurre il carico sui computer che stanno ascoltando messaggi 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 sono 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.

3.6 Richieste (Queries)

Se un router RIP-2 riceve una richiesta RIP-1, esso dovrebbe rispondere con un messaggio RIP-1. Se un router è configurato per emettere solo messaggi RIP-2, non dovrebbe rispondere a richieste RIP-1.

4. Compatibilità

Il documento RFC 1058 ha mostrato considerevole lungimiranza nella sua specifica nella gestione dei numeri di versione. Esso specifica che messaggi RIP di versione zero sono scartati, che messaggi RIP di versione uno saranno scartati se il campo Must Be Zero (MBZ) è diverso da zero, e che i messaggi 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 dovrebbe essere configurabile su base interfaccia.

Il commutatore ha quattro impostazioni: RIP-1, nel quale solo messaggi RIP-1 vengono inviati; compatibilità RIP-1, nel quale messaggio pacchetto RIP-2 vengono inviati come broadcasts, e RIP-2, nel quale messaggi RIP-2 vengono inviati come multicast; e "none" che disabilita l'emissioni di messaggi RIP. Il valore predefinito raccomandato per questo commutatore è la compatibilità con RIP-1.

Per completezza, i routers dovrebbero anche implementare un commutatore di controllo di ricezione che dovrebbe determinare se accettare, solo RIP-1, solo RIP-2, entrambi, o niente. Esso dovrebbe anche essere configurabile su base interfaccia.

4.2 Autenticazione

Si dovrebbe essere usare il seguente algoritmo per autenticare un messaggio RIP. Se il router non è configurato per autenticare messaggi RIP-2, allora saranno accettati messaggi RIP-1 e RIP-2 senza autenticazione; i messaggi RIP-2 autenticati saranno scartati. Se il router è configurato per autenticare messaggi RIP-2, allora messaggi messaggi RIP-1 e RIP-2 che passeranno la prova dell'autenticazione saranno accettati; mentre quelli che la falliranno saranno scartati. Per la

massima sicurezza, bisognerebbe ignorare i messaggi RIP-1 quando è in uso l'autenticazione (vedi la sezione 4.1).

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. Perciò, si noti che l'uso di autenticazione non impedirà a sistemi RIP-1 di vedere messaggi RIP-2. Se desiderato questo può essere effettuato utilizzando emissioni multicasting, come descritto nelle sezioni 3.5 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 ottetto singolo e riutilizzare i tre ottetti più alti, ma ciò interromperebbe qualsiasi implementazione che trattasse la metrica come un'entità a quattro ottetti.

4.4 Collegamenti senza indirizzi.

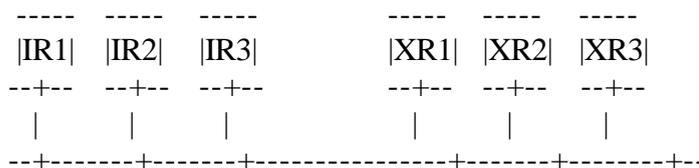
Collegamenti senza indirizzo non saranno supportati da RIP-2, come in RIP-1.

5 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 tra le migliori. Questo meccanismo viene descritto nelle sezioni 3.1 e 4.2.

Appendice A

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



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 diversi protocolli d'instradamento (per es., OSPF). XR1, XR2, e XR3 scambiano informazioni di instradamento tra di loro cosicchè essi sanno che la miglior rotta verso le reti N1 e N2 sia via XR1, verso N3, N4, e N5 sia via XR2, e verso N6 e N7 sia 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 affinché accada l'instradamento senza ulteriori salti via XR1. Senza l'impiego di "Next Hop" (per es., se fosse utilizzato RIP-1) sarebbe necessario per XR2 e XR3 partecipare anche al protocollo RIP-2 per eliminare nuovi salti.

Referenze

[1] Hedrick, C., "Routing Information Protocol", STD 34, RFC 1058, Rutgers University, June 1988.

[2] Malkin, G., "RIP Version 2 - Carrying Additional Information", RFC 1388, Xylogics, Inc., January 1993.

[3] Malkin, G., and F. Baker, "RIP Version 2 MIB Extension", RFC 1724, Xylogics, Inc., Cisco Systems, November 1994.

[4] Malkin, G., "RIP Version 2 Protocol Analysis", RFC 1721, Xylogics, Inc., November 1994.

[5] Malkin, G., "RIP Version 2 Protocol Applicability Statement", RFC 1722, Xylogics, Inc., November 1994.

Indirizzo dell'autore

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