

Réseau - Protocole RIP



Difficulté : Confirmé

Notions : Protocoles réseaux, routage, routage dynamique.

I. Introduction

Le protocole RIP pour **R**outing **I**nformation **P**rotocol est un protocole permettant aux routeurs d'échanger automatiquement leurs tables de routage. Il fait partie des protocoles IGP (**I**nterior **G**ateway **P**rotocol) qui sont utilisés à l'intérieur d'un même réseau ou organisation.

C'est un protocole de ***couche 3***.

Cela facilite la gestion du parc, permettant notamment de mettre à jour automatiquement les tables de routages en cas d'ajout ou suppression d'un réseau, rendant celui-ci facilement scalable et simple à administrer.

II. Principes de base

2.1 Fonctionnement

Le principe du RIP est assez simple :

Chaque routeur génère une table de routage composée de ses réseaux connus directement accessibles via ses interfaces. Il y ajoute les routes connues ainsi que leur distance en nombre de saut.

Puis, régulièrement (par défaut 30 secondes), il envoie cette table à ses partenaires de réplication. Dans la première version du protocole, cela se fait par broadcast. Puis cela a été changé pour du multicast dans les versions suivantes du protocole (224.0.0.9 pour RIPv2 en IPv4, puis dans le RIPv6 pour IPv6 : FF02::9)

Chaque routeur met ainsi ses tables à jour et peut les propager aux autres. Les doublons sont éliminés et les routes avec un minimum de saut sont conservées afin d'optimiser la performance.

Si une route n'a pas eu d'update dans un délai de 180 secondes, elle est marquée comme invalide. Passé 240 secondes, elle est supprimée.

Ces délais permettent ainsi d'ajouter une purge des routes inutiles en plus des ajouts, permettant de conserver des tables de routage précises.

2.2 Mécanismes internes

Le RIP utilise plusieurs mécanismes internes pour éviter des boucles dans la topologie.

- **Split Horizon** : un routeur n'annonce pas une route sur l'interface par laquelle il l'a apprise.
- **Route Poisoning** : Une route devenue invalide est supprimée.
- **Hold-down Timer** : Empêche une acceptation trop rapide d'une route potentiellement incorrecte

Voici une liste plus détaillée des timers clés :

Timer	Valeur	Rôle
Update	30 s	Envoi périodique des tables
Invalid	180 s	Route considérée invalide

Timer	Valeur	Rôle
Hold-down	180 s	Stabilisation
Flush	240 s	Suppression de la route

2.2 Limitations

Le RIP repose essentiellement sur le *hop count*. Ce compteur de saut est limité à 15 sauts.

Cela le rends inefficace pour de larges topologies et limite donc son usage à des réseaux de petite tailles ou de tailles moyennes.

De plus en terme de priorité de traitement, les requêtes RIP sont les moins prioritaires.

Protocoler	Distance administrative
RIP	120
OSPF	110
EIGRP	90
statique	1
connectée	0

III. Versions de RIP

Il existe 3 versions du protocole RIP :

Feature	RIPv1 (1988)	RIPv2 (1993)	RIPng (1997) for IPv6
Méthode de mise à jour	Broadcast (255.255.255.255)	Multicast (224.0.0.9)	Multicast (FF02::9)
Adressage	Classful (pas d'info de sous réseau)	Classless (inclus le masque)	Classless (IPv6)
Authentification	Pas de support	plain text, MD5	plain text, MD5

Feature	RIPv1 (1988)	RIPv2 (1993)	RIPng (1997) for IPv6
Version IP supportées	IPv4	IPv4	IPv6
Protocole / port	UDP 520	UDP 520	UDP 521

IV. Considérations de sécurité

Attention : Le protocole RIP est considéré aujourd'hui comme obsolète. Il est en effet remplacé par d'autres protocoles plus modernes et sécurisés.

Le principal risque du protocole RIP reste l'empoisonnement des routes par un tiers ou un équipement malveillant.

Il est donc primordial de respecter à minima les deux conditions suivante lors de la mise en place :

- Utiliser à minima la version 2 du protocole qui permet une authentification
- Utiliser une authentification MD5 et pas une authentification plainText.

Il est à noter que le RIP n'utilise pas directement MD5 pour hasher un mot de passe, mais comme fonction de hashage dans un mécanisme d'authentification HMAC-Like.

Aussi, il ne s'agit pas de hasher un mot de passe, mais le paquet RIP complet. Lors de l'échange, les routeurs disposant tous de la même clé, ils vont recalculer localement le hash de la trame reçue afin de certifier qu'elle est bien originaire d'un routeur connu.

V. Conclusion

Même si son usage est déprécié, Il reste intéressant à voir à des fins pédagogiques car il permet d'introduire les principes de routage dynamique avec un protocole simple dans son fonctionnement.

De plus, sur les équipements plus anciens, il s'agit souvent de la seule alternative disponible.

Revision #2

Created 2026-07-17 20:31:39 UTC by Olivier

Updated 2026-07-17 20:39:22 UTC by Olivier