

Keep-it-alived :

Étude de la sécurité du protocole VRRP

Geoffrey SAUVAGEOT-BERLAND ~ @archidote



Présentation disponible ici :



ou ici <https://urlr.me/FbBCpZ>

Sommaire

01

Introduction

02

Menaces de sécurité

03

Au-delà du tie-break

04

Take aways &
Recommandations



01

Introduction



Qu'est-ce VRRP ? (Virtual Router Redundancy Protocol)

- > Protocole réseau (couche 3* du modèle OSI)
- > Open-standard
- > Utilisé pour garantir la haute disponibilité des équipements réseau



*Couche réseau

Pourquoi l'utiliser ?

- > Facile à configurer
- > Permet une bascule transparente entre les nœuds (automatic failover)
- > Interopérabilité (contrairement à ses homologues HSRP, GLBP : propriétaire Cisco)



Où utilise-t-on ce protocole ?

- > Organismes publics
- > Fournisseurs d'accès à Internet (FAI)
- > Data centers d'entreprises utilisant des équipements de différents éditeurs



Comment celui-ci fonctionne-t-il ?

- > Création d'une VIP (Virtual IP address)
- > Partagée entre un groupe de nœuds identifiés par un VRID
- > Un seul nœud élu **Master**, les autres en état de « **Backup** »
- > En cas de crash, un Backup prend le relais automatiquement
- > Valeurs de priorité (0-255) utilisées pour l'élection du Master
- > Le master envoie des annonces 1/s (avertissements)

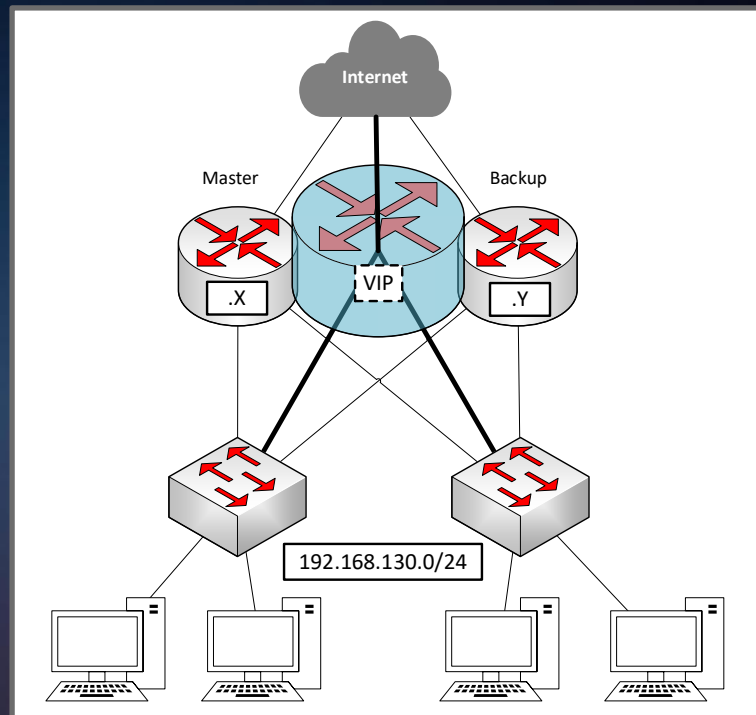


schéma retravaillé - source original : fingerinthenet.com



Comment celui-ci fonctionne ?

- > ~~Ports~~: Ø port TCP/UDP n'est utilisé, car VRRP fonctionne au niveau de la couche réseau IP.
- > Mode de diffusion : Multicast par défaut et unicast
- > **Attention** : High Availability (Failover, Load balancer)



VRRPv2 vs VRRPv3

	VRRPv2	VRRPv3																																																																																				
Type d'authentification	<ul style="list-style-type: none">- Pas d'authentification- « Plain-text password »- IP AH (HMAC-MD5-96)	<ul style="list-style-type: none">- Pas de mécanisme d'authentification																																																																																				
Spécification	<ul style="list-style-type: none">- RFC 2338 (1998), puis 3768 (2004)- IPv4	<ul style="list-style-type: none">- RFC 5798 (2010), puis 9568 (2024)- IPv4 et IPv6																																																																																				
Format du paquet	<table><tr><td>0</td><td>3</td><td>4</td><td>7</td><td>15</td><td>23</td><td>31</td></tr><tr><td>Version</td><td>Type</td><td>Virtual Rtr ID</td><td>Priority</td><td>Count IP Addr</td><td colspan="2"></td></tr><tr><td colspan="2">Auth Type</td><td>Adver Int</td><td colspan="4">Checksum</td></tr><tr><td colspan="7">IP Address (1)</td></tr><tr><td colspan="7">⋮</td></tr><tr><td colspan="7">IP Address (n)</td></tr><tr><td colspan="7">Authentication Data (1)</td></tr><tr><td colspan="7">Authentication Data (2)</td></tr></table>	0	3	4	7	15	23	31	Version	Type	Virtual Rtr ID	Priority	Count IP Addr			Auth Type		Adver Int	Checksum				IP Address (1)							⋮							IP Address (n)							Authentication Data (1)							Authentication Data (2)							<table><tr><td>0</td><td>3</td><td>4</td><td>7</td><td>15</td><td>23</td><td>31</td></tr><tr><td>Version</td><td>Type</td><td>Virtual Rtr ID</td><td>Priority</td><td>Count IP Addr</td><td colspan="2"></td></tr><tr><td colspan="7">Checksum</td></tr><tr><td colspan="7">IPvX Address (es)</td></tr></table>	0	3	4	7	15	23	31	Version	Type	Virtual Rtr ID	Priority	Count IP Addr			Checksum							IPvX Address (es)						
0	3	4	7	15	23	31																																																																																
Version	Type	Virtual Rtr ID	Priority	Count IP Addr																																																																																		
Auth Type		Adver Int	Checksum																																																																																			
IP Address (1)																																																																																						
⋮																																																																																						
IP Address (n)																																																																																						
Authentication Data (1)																																																																																						
Authentication Data (2)																																																																																						
0	3	4	7	15	23	31																																																																																
Version	Type	Virtual Rtr ID	Priority	Count IP Addr																																																																																		
Checksum																																																																																						
IPvX Address (es)																																																																																						



02

Menaces de sécurité



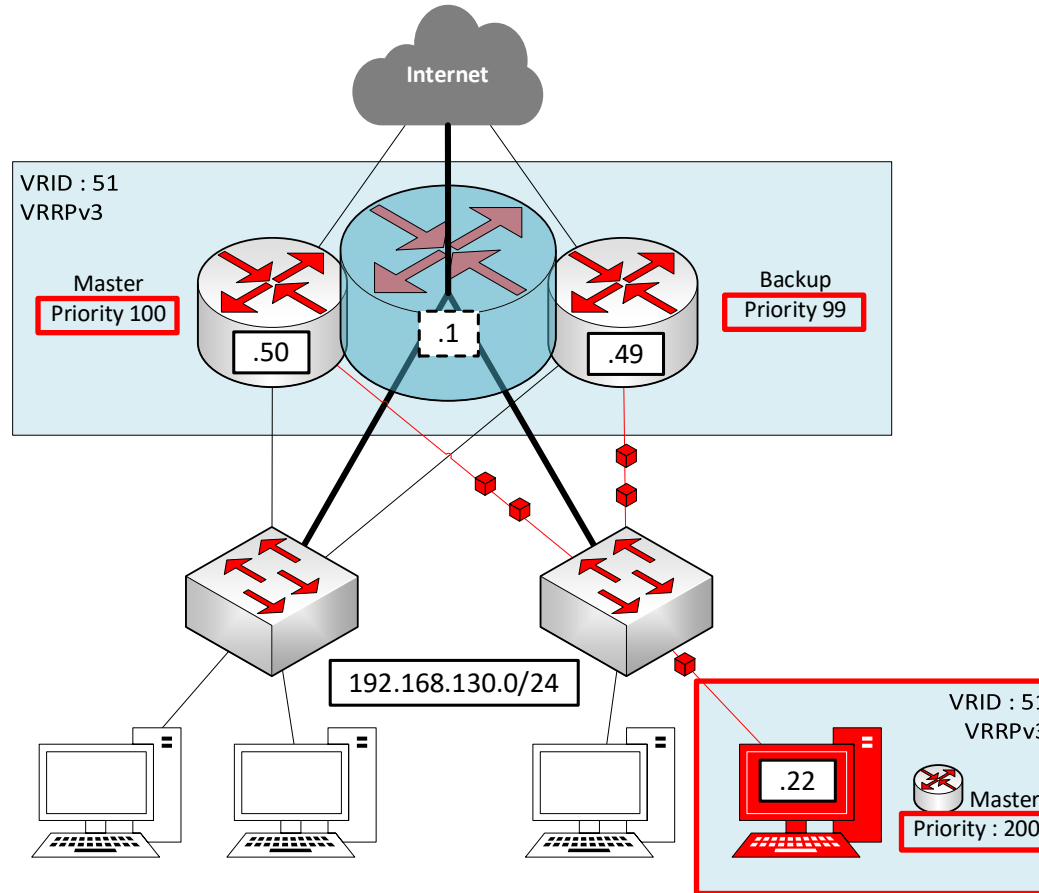
Menaces de sécurité

Prérequis : être dans le même sous-réseau que les nœuds VRRP

- > Priorités mal configurées permettant la prise de contrôle du groupe VRRP par un attaquant.
- > Rejeu de mot de passe (uniquement pour VRRPv2 – Plain-text password)
- > Atteinte à la disponibilité en inondant le réseau de paquets VRRP « mal formés » (DoS logique)

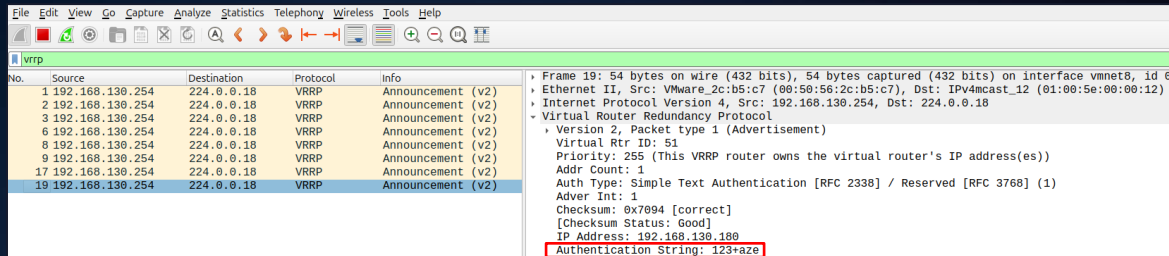


Menaces / Défaut de priorité



Menaces / Rejeu de mot de passe

> VRRPv2 – Plain-text password Auth



Wireshark packet capture showing VRRPv2 announcements. The packet list on the left shows multiple VRRPv2 announcement packets from source 192.168.130.254 to destination 224.0.0.18. The packet details on the right show the structure of the VRRPv2 packet, including the Virtual Router ID (51), Priority (255), and Authentication String (123*aze).

No.	Source	Destination	Protocol	Info
1	192.168.130.254	224.0.0.18	VRRP	Announcement (v2)
2	192.168.130.254	224.0.0.18	VRRP	Announcement (v2)
3	192.168.130.254	224.0.0.18	VRRP	Announcement (v2)
6	192.168.130.254	224.0.0.18	VRRP	Announcement (v2)
8	192.168.130.254	224.0.0.18	VRRP	Announcement (v2)
9	192.168.130.254	224.0.0.18	VRRP	Announcement (v2)
17	192.168.130.254	224.0.0.18	VRRP	Announcement (v2)
19	192.168.130.254	224.0.0.18	VRRP	Announcement (v2)

Frame 19: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface vmmnet8, id 0
Ethernet II, Src: VMware_2c:b5:c7 (00:50:56:2c:b5:c7), Dst: IPv4mcast_12 (01:00:5e:00:00:12)
Internet Protocol Version 4, Src: 192.168.130.254, Dst: 224.0.0.18
Virtual Router Redundancy Protocol
Version 2, Packet type 1 (Advertisement)
Virtual Rtr ID: 51
Priority: 255 (This VRRP router owns the virtual router's IP address(es))
Addr Count: 1
Auth Type: Simple Text Authentication [RFC 2338] / Reserved [RFC 3768] (1)
Adver Int: 1
Checksum: 0x7994 [correct]
[Checksum Status: Good]
IP Address: 192.168.130.180
Authentication String: 123*aze



Powering Business Worldwide

Onduleur

- Propriétés de l'onduleur
- Contrôle de l'onduleur
- Programmation M/A
- Paramètres d'arrêt

Historiques et Notification

- Mesures
- Evénements onduleur
- Evénements système

Contrôle de l'onduleur

Eaton SP 650

Output

Etat

Master

Alimentée

Aucun

Executer



HP LaserJet 400 M401dn

HP LaserJet 400 M401dn

Accueil

Système

Imprimer

Mise en réseau

Services Web HP

HP Smart Install

Résumé réseau

Configuration

Configuration IPv4

Configuration IPv6

Identification réseau

Avancés

Sécurité

Réglages

Certificats

Réglages

Paramètres réseau

Nom de fonction/service

Valeur actuelle

Autorisation

Mot de passe administrateur

Certificat de l'imprimante

Certificat CA

Désactivé

Installé

Non installé(e)

Storage Management Utility

System Status

System Time

System Events

Configuration View

SRVPR

View

Provisioning

Help

Host Overview

Details about a specific host

Host Overview

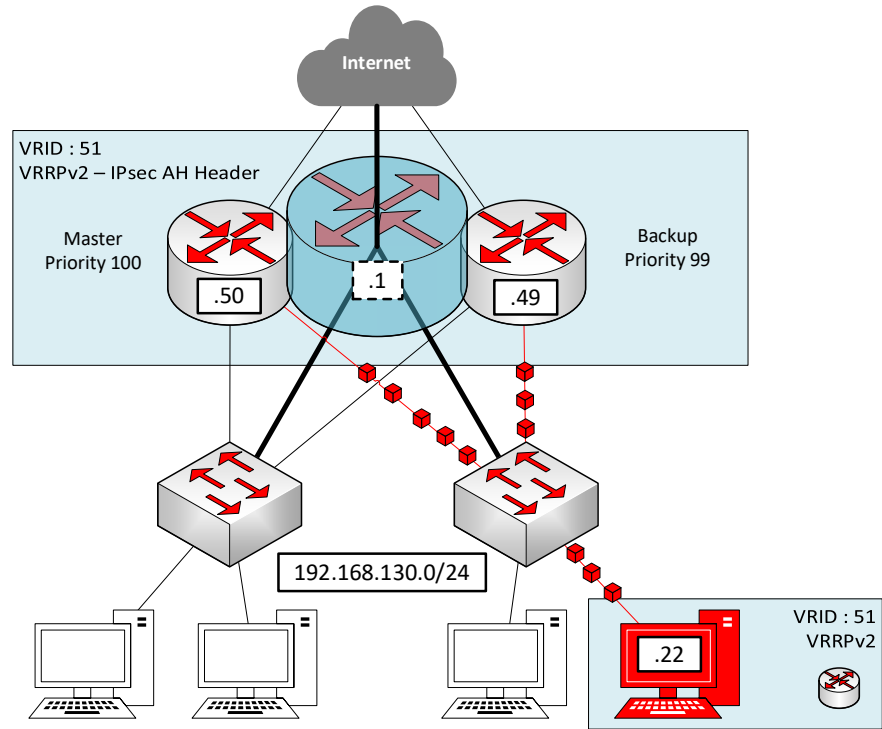
Menaces / Flooding de paquets VRRP

> Envoie d'une grande quantité de paquets VRRP mal formés (DoS logique)

```

> Authentication Header
> Virtual Router Redundancy Protocol
> Version 2, Packet type 1 (Advertisement)
  Virtual Rtr ID: 51
  Priority: 255 (This VRRP router owns the virtual router's IP address(es))
  Addr Count: 1
  Auth Type: IP Authentication Header [RFC 2338] / Reserved [RFC 3768] (2)
  Adver Int: 1
  Checksum: 0x9a6c [correct]
  [Checksum Status: Good]
  IP Address: 192.168.130.180

```



Etude : Panorama des mauvaises configurations VRRP trouvées en ligne

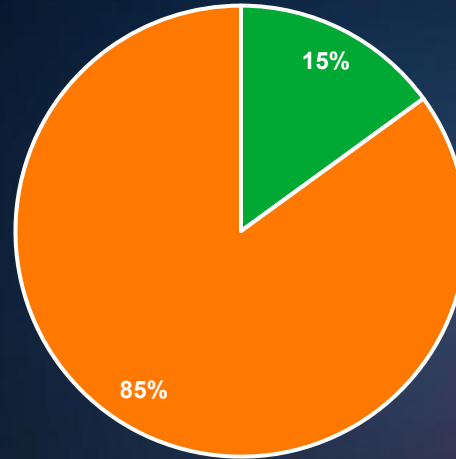


[Lien de l'étude complète \(anonymisé\)](#)



Menaces / Synthèse de l'étude

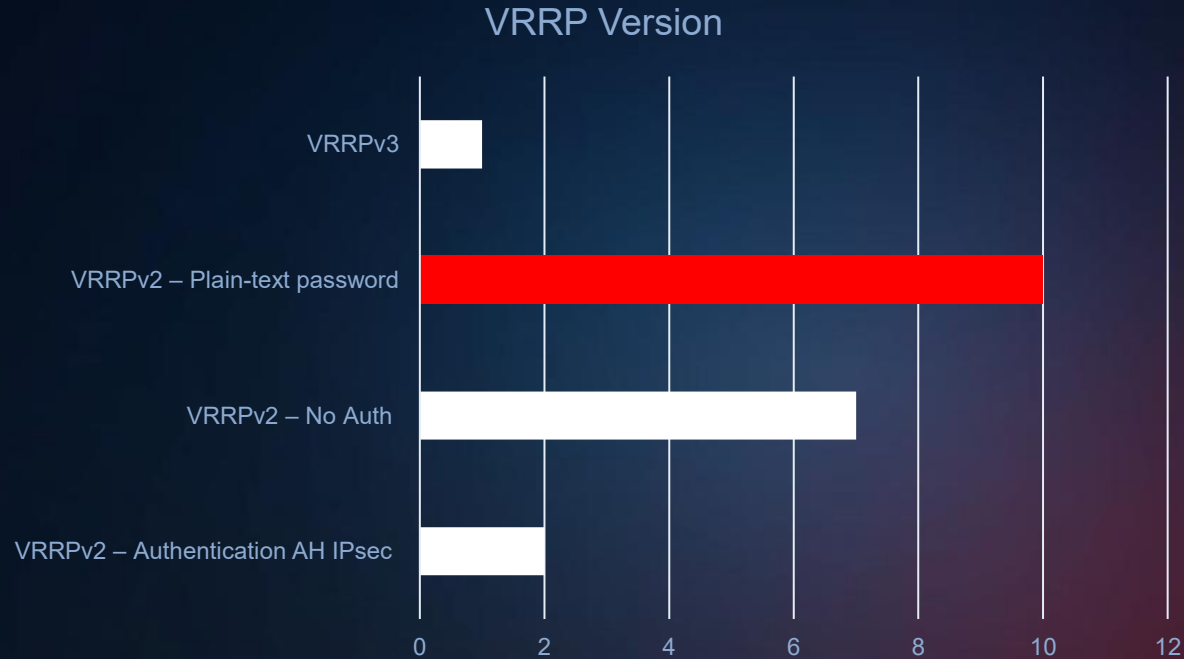
Master's Priority (equal to 255)



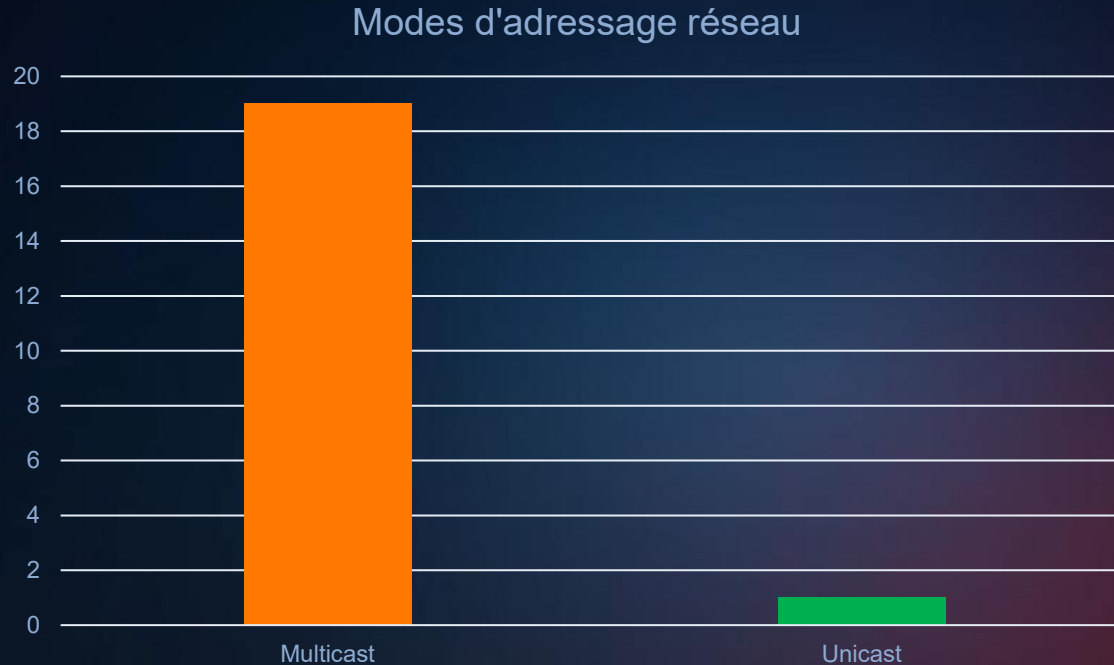
yes no



Menaces / Synthèse de l'étude



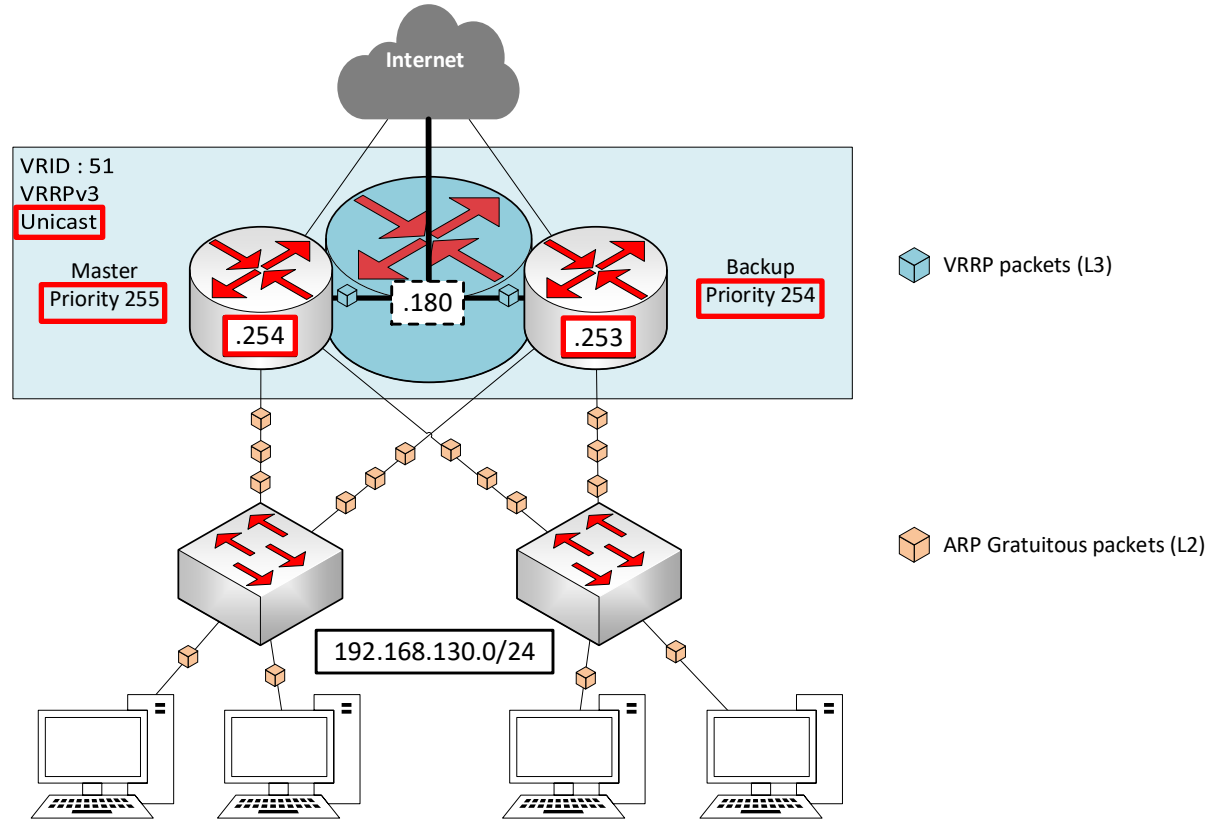
Menaces / Synthèse de l'étude



***À quoi correspond une configuration
VRRP « propre » ?***



Configuration « SOTA* »



Comment départager deux nœuds qui ont la même priorité VRRP (ex : 255) ?



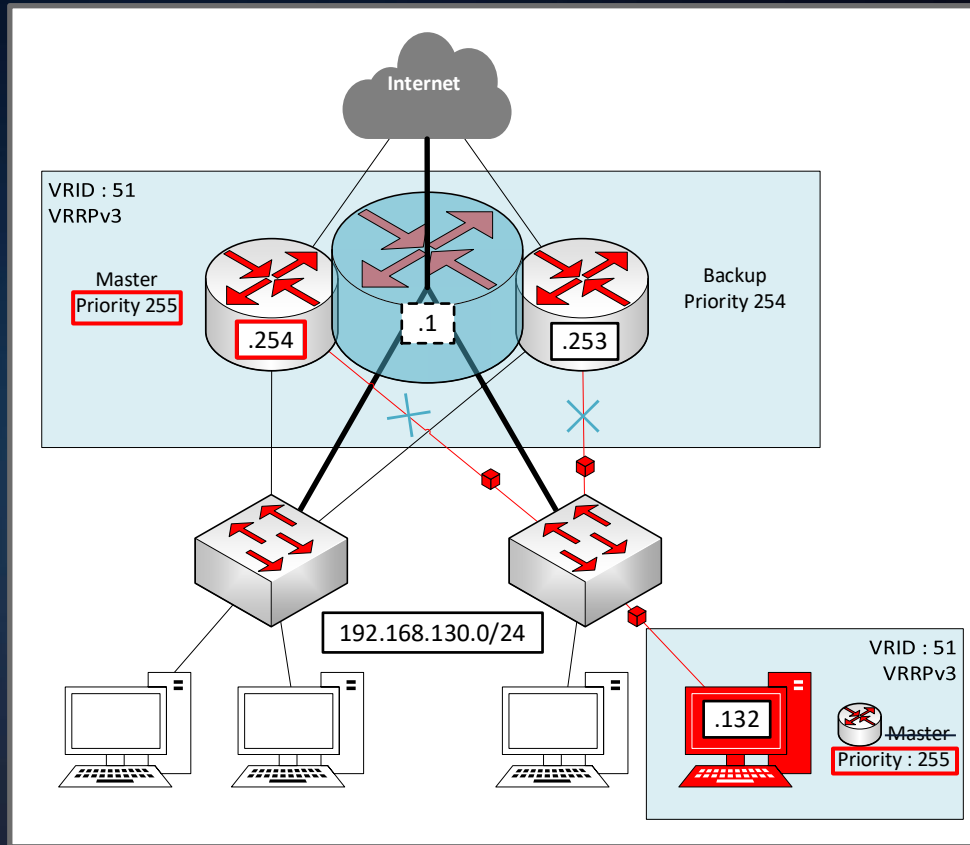
03

Au-delà du tie-break



La théorie

- > Si priorités identique → comparaison des IP
- > Le Nœud avec « l'IP la plus haute* » → Master

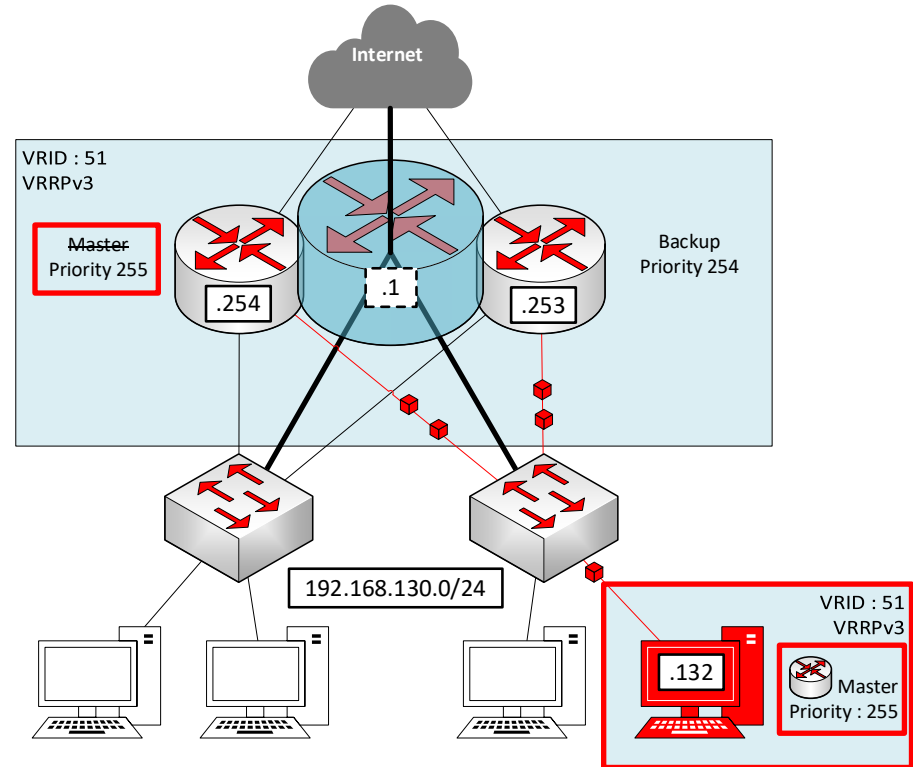


*Sur le dernier octet

En pratique

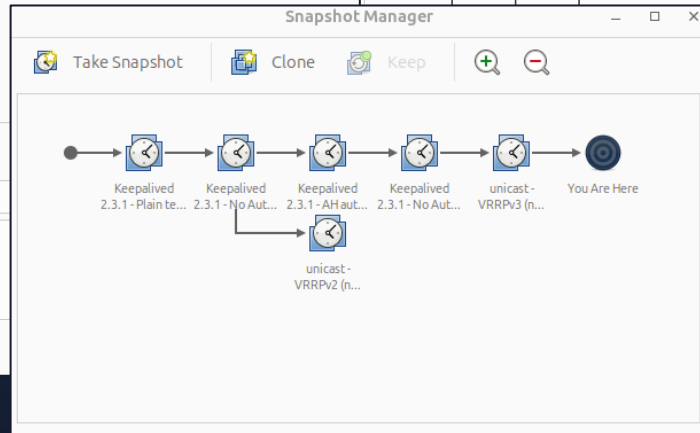
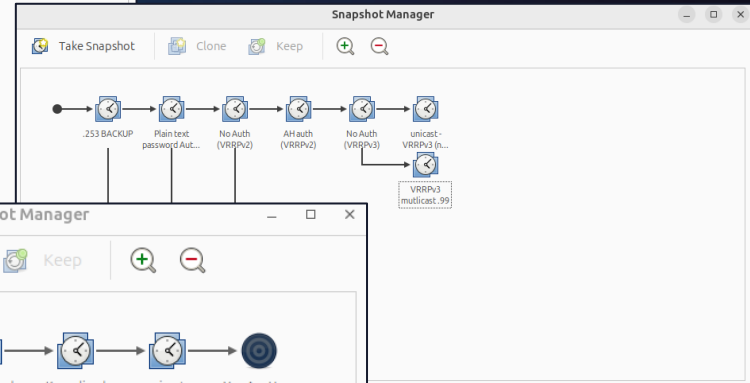
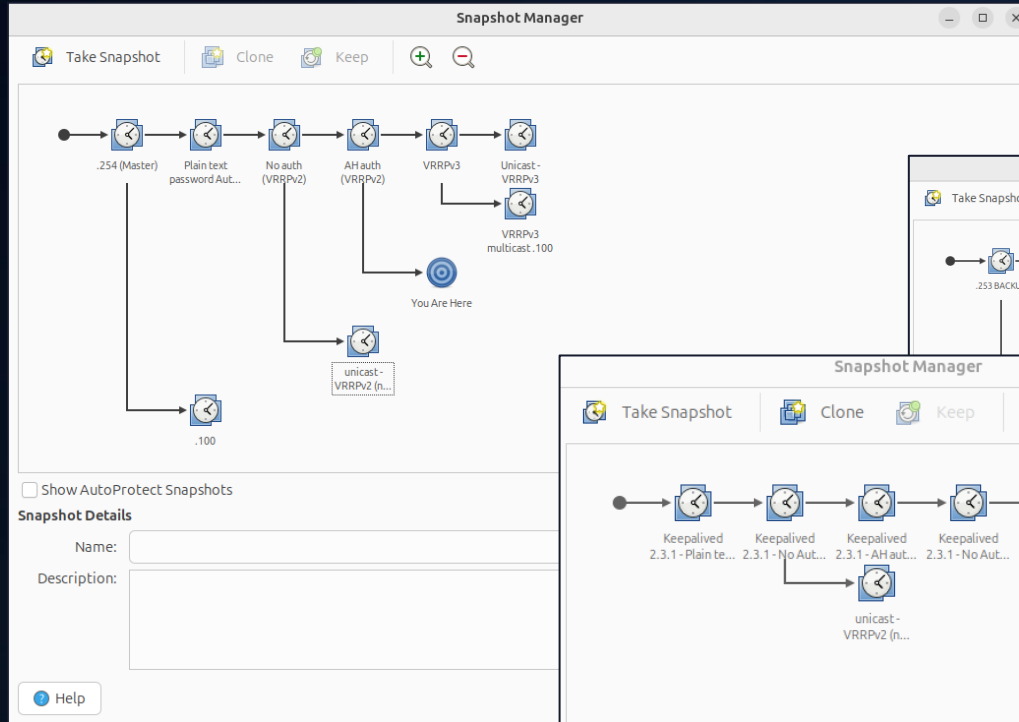
Time	Source	Destination	Protocol
0.000000000	192.168.130.254	224.0.0.18	VRRP
1.000842596	192.168.130.254	224.0.0.18	VRRP
2.001542242	192.168.130.254	224.0.0.18	VRRP
3.002588182	192.168.130.254	224.0.0.18	VRRP
4.003553864	192.168.130.254	224.0.0.18	VRRP
5.004465329	192.168.130.254	224.0.0.18	VRRP
6.005107748	192.168.130.254	224.0.0.18	VRRP
7.005660781	192.168.130.254	224.0.0.18	VRRP
8.006168162	192.168.130.254	224.0.0.18	VRRP
9.006924695	192.168.130.254	224.0.0.18	VRRP
10.008327784	192.168.130.254	224.0.0.18	VRRP
11.008792729	192.168.130.254	224.0.0.18	VRRP
12.009561696	192.168.130.254	224.0.0.18	VRRP
12.134268401	192.168.130.132	224.0.0.18	VRRP
13.135030066	192.168.130.132	224.0.0.18	VRRP
14.136016145	192.168.130.132	224.0.0.18	VRRP
15.136539738	192.168.130.132	224.0.0.18	VRRP
16.137009814	192.168.130.132	224.0.0.18	VRRP
17.137358428	192.168.130.132	224.0.0.18	VRRP
18.138092732	192.168.130.132	224.0.0.18	VRRP
19.138802673	192.168.130.132	224.0.0.18	VRRP
20.139799419	192.168.130.132	224.0.0.18	VRRP

```
> Frame 158: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface vmmnet8, id 0
> Ethernet II, Src: VMware_7b:82:1e (00:0c:29:7b:82:1e), Dst: IPv4mcast_12 (01:00:5e:00:00:12)
> Internet Protocol Version 4, Src: 192.168.130.132, Dst: 224.0.0.18
> Virtual Router Redundancy Protocol
  > Version 3, Packet type 1 (Advertisement)
    Virtual Rtr ID: 51
    Priority: 255 (This VRRP router owns the virtual router's IP address(es))
    Addr Count: 1
    0000 .... = Reserved: 0
    .... 0000 0110 0100 = Adver Int: 100
    Checksum: 0x684d [correct]
    [Checksum Status: Good]
    IP Address: 192.168.130.180
```





Jeux de tests – (projet keepalived)



Jeux de tests – (projet keepalived)

	VRRPv2	VRRPv3
Type d'auth	<p>Pas d'authentification</p> <p>Simple Text Password (<i>Sniffer le réseau et essayer de casser le secret au préalable</i>)</p> <p>IP AH (<i>Sniffer le réseau et essayer de casser le secret au préalable</i>)</p>	<p>Pas d'authentification</p>
Mode de diffusion	<p>Multicast & Unicast (<i>attaque possible mais en pratique purement hypothétique dans un cas réel</i>)</p>	<p>Multicast & Unicast (...)</p>

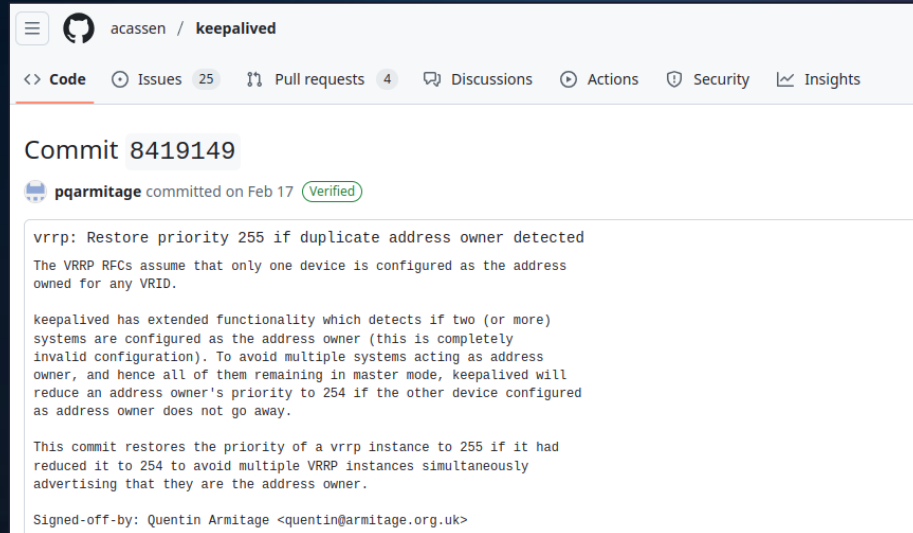


Shhhhh ! I'm the master now



CVE ?

- > Tests avec deux implémentations : Keepalived et Cisco
- > Seul Keepalived est vulnérable
- > Keepalived fait un patch mais remet en cause la RFC 9568



```
acassen / keepalived
<> Code Issues 25 Pull requests 4 Discussions Actions Security Insights

Commit 8419149
pqarmitage committed on Feb 17 Verified

vrrp: Restore priority 255 if duplicate address owner detected

The VRRP RFCs assume that only one device is configured as the address
owned for any VRID.

keepalived has extended functionality which detects if two (or more)
systems are configured as the address owner (this is completely
invalid configuration). To avoid multiple systems acting as address
owner, and hence all of them remaining in master mode, keepalived will
reduce an address owner's priority to 254 if the other device configured
as address owner does not go away.

This commit restores the priority of a vrrp instance to 255 if it had
reduced it to 254 to avoid multiple VRRP instances simultaneously
advertising that they are the address owner.

Signed-off-by: Quentin Armitage <quentin@armitage.org.uk>
```



~~CVE~~?



> Keepalived suivait à la lettre la RFC 9568

- > Le problème provenait de la RFC 9568
- > Les paquets VRRP avec priorité 255 étaient « *ignorés avant traitement* » (discard) [RFC 9568]
- > Cela *bloquait le déclenchement* du mécanisme d'IP-tie breaking
- > **Conséquence** : conflits non détectés entrainant la rétrogradation de la priorité du Master (légitime)
- > Si on stoppe l'attaque :

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
Current filter: vrrp					
Time	Source	Destination	Protocol	Info	
11.735285573	192.168.130.132	224.0.0.18	VRRP	Announcement (v3)	Frame 15953: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface vmnet8, id
12.735627466	192.168.130.132	224.0.0.18	VRRP	Announcement (v3)	Ethernet II, Src: VMware_2c:b5:c7 (00:50:56:2c:b5:c7), Dst: IPv4mcast_12 (01:00:5e:00:00:12)
13.737730633	192.168.130.132	224.0.0.18	VRRP	Announcement (v3)	Internet Protocol Version 4, Src: 192.168.130.254, Dst: 224.0.0.18
14.724236196	192.168.130.132	224.0.0.18	VRRP	Announcement (v3)	Virtual Router Redundancy Protocol
15.692442768	192.168.130.132	224.0.0.18	VRRP	Announcement (v3)	Version 3, Packet type 1 (Advertisement)
16.434528946	192.168.130.132	224.0.0.18	VRRP	Announcement (v3)	Virtual Rtr ID: 51
16.442997203	192.168.130.254	224.0.0.18	VRRP	Announcement (v3)	Priority: 254 (Non-default backup priority)
16.444568561	192.168.130.254	224.0.0.18	VRRP	Announcement (v3)	Addr Count: 1
17.445590190	192.168.130.254	224.0.0.18	VRRP	Announcement (v3)	0000 = Reserved: 0
18.445806554	192.168.130.254	224.0.0.18	VRRP	Announcement (v3) 0000 0110 0100 = Adver Int: 100
19.446225627	192.168.130.254	224.0.0.18	VRRP	Announcement (v3)	Checksum: 0x68d3 [correct]
					[Checksum Status: Good]
					IP Address: 192.168.130.132

Création d'un erratum (8298) sur la RFC avec l'équipe de keepalived

> Autorise un nœud avec une *prio* 255 à traiter « normalement » les paquets VRRP en cas de priorité égale.

Errata ID: 8298
Status: Verified
Type: Technical
Publication Format(s) : TEXT, PDF, HTML
Reported By: Quentin Armitage
Date Reported: 2025-02-17
Verifier Name: Jim Guichard
Date Verified: 2025-03-06

Section 7.1 says:

It MUST verify that the VRID is configured on the receiving interface and the local router is not the IPvX address owner (Priority = 255 (decimal)).

If any one of the above checks fails, the receiver MUST discard the packet, SHOULD log the event (subject to rate-limiting), and MAY indicate via network management that an error occurred.

It should say:

It MUST verify that the VRID is configured on the receiving interface.

If any one of the above checks fails, the receiver MUST discard the packet, SHOULD log the event (subject to rate-limiting), and MAY indicate via network management that an error occurred.

It SHOULD verify that the local router is not the IPvX address owner (Priority = 255 (decimal)) and log the event (subject to rate-limiting) and MAY indicate via network management that a misconfiguration was detected.



Conséquences

- > Les éditeurs doivent MAJ leurs implémentations VRRP pour refléter ce changement conceptuel
- > Le tie-break basé sur l'adresse IP peut désormais s'appliquer
- > Cisco n'était pas vulnérable → conforme à l'ancienne RFC* (qui gérait correctement ce mécanisme)



04

Recommendations & Take aways



Qu'avez-vous besoin pour reproduire ces tests ?

- > Manuellement : Wireshark + Une instance VRRP keepalived* (Dans une VM ou via un conteneur)
- > Semi-automatiquement : Utilisez [VRRP hijacker.py](#)

**Keepalived ne doit être utilisé que dans un cadre éducatif ou pour des tests encadrés. Toute utilisation en dehors de ce contexte relève de la seule responsabilité de l'utilisateur.*



Recos'

> Si vous utilisez VRRPv2 :

Utilisez le mode unicast pour restreindre le domaine de diffusion.

Utilisez l'authentification IPSec AH si les appareils le prennent en charge.

Respectez un adressage rigoureux et l'ordre des priorités VRRP.

Segmentation du réseau.

> Si vous utilisez VRRPv3 :

Utilisez le mode unicast pour restreindre la propagation du trafic.

Respectez un adressage rigoureux et l'ordre des priorités VRRP.

Segmentation du réseau.



Take aways

- > Protocole établi, mais sa sécurité est souvent négligée.
- > Ce n'était pas une CVE sur keepalived, mais un problème dans la RFC.
- > Une configuration durcit reste indispensable pour VRRP.



Ressources

- > [RFC 5798](#), [RFC 9568](#)
- > [Projet keepalived](#)
- > Article dans le magazine [MISC](#) (N°140) «La sécurité du protocole VRRP»



Remerciements

- > Claire Vacherot (@non_curat_lex)
- > Laurent Levron
- > Théo Lorette-Froidevaux (@tolfsh)
- > Keepalived team (keepalived.org)
- > Orange Cyberdefense (@OrangeCyberFR)
- > Mes proches



Keep-it-alived :

Étude de la sécurité du protocole VRRP

Q&A

