orange Cyberdefense

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

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)

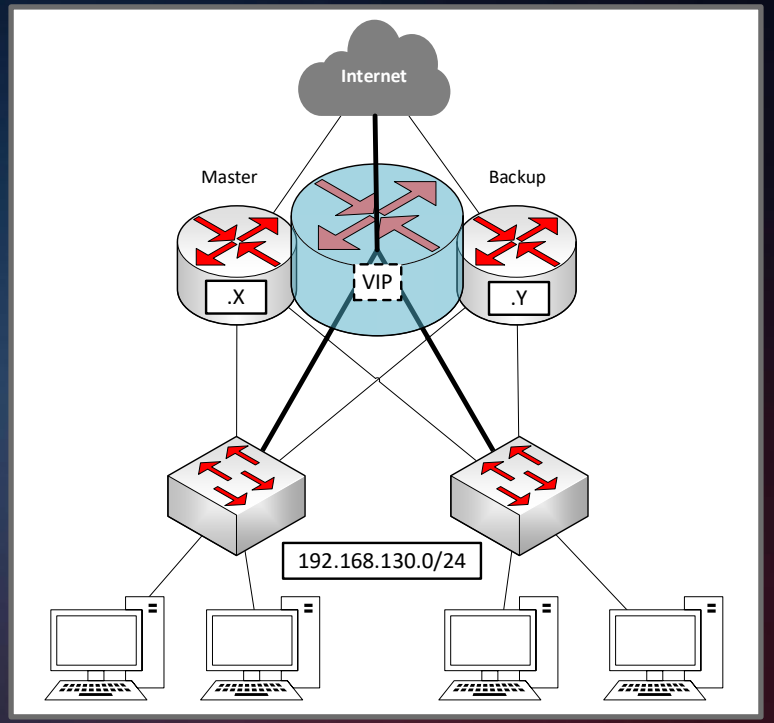


schéma retravaillé– source original : fingerinthenet.com

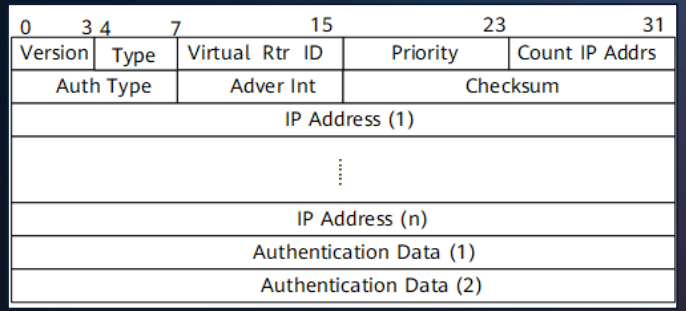
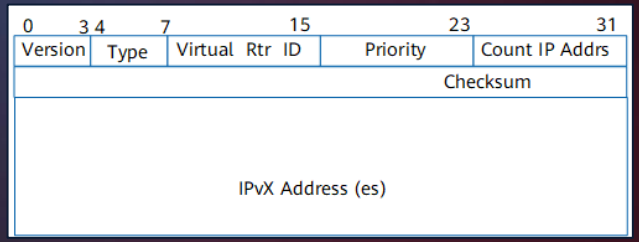
Comment celui-ci fonctionne ?

> ~~**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	- Pas d'authentification - « Plain-text password » - IP AH (HMAC-MD5-96)	- Pas de mécanisme d'authentification
Spécification	- RFC 2338 (1998), puis 3768 (2004) - IPv4	- RFC 5798 (2010), puis 9568 (2024) - IPv4 et IPv6
Format du paquet		

02

Menaces de sécurité

Menaces de sécurité

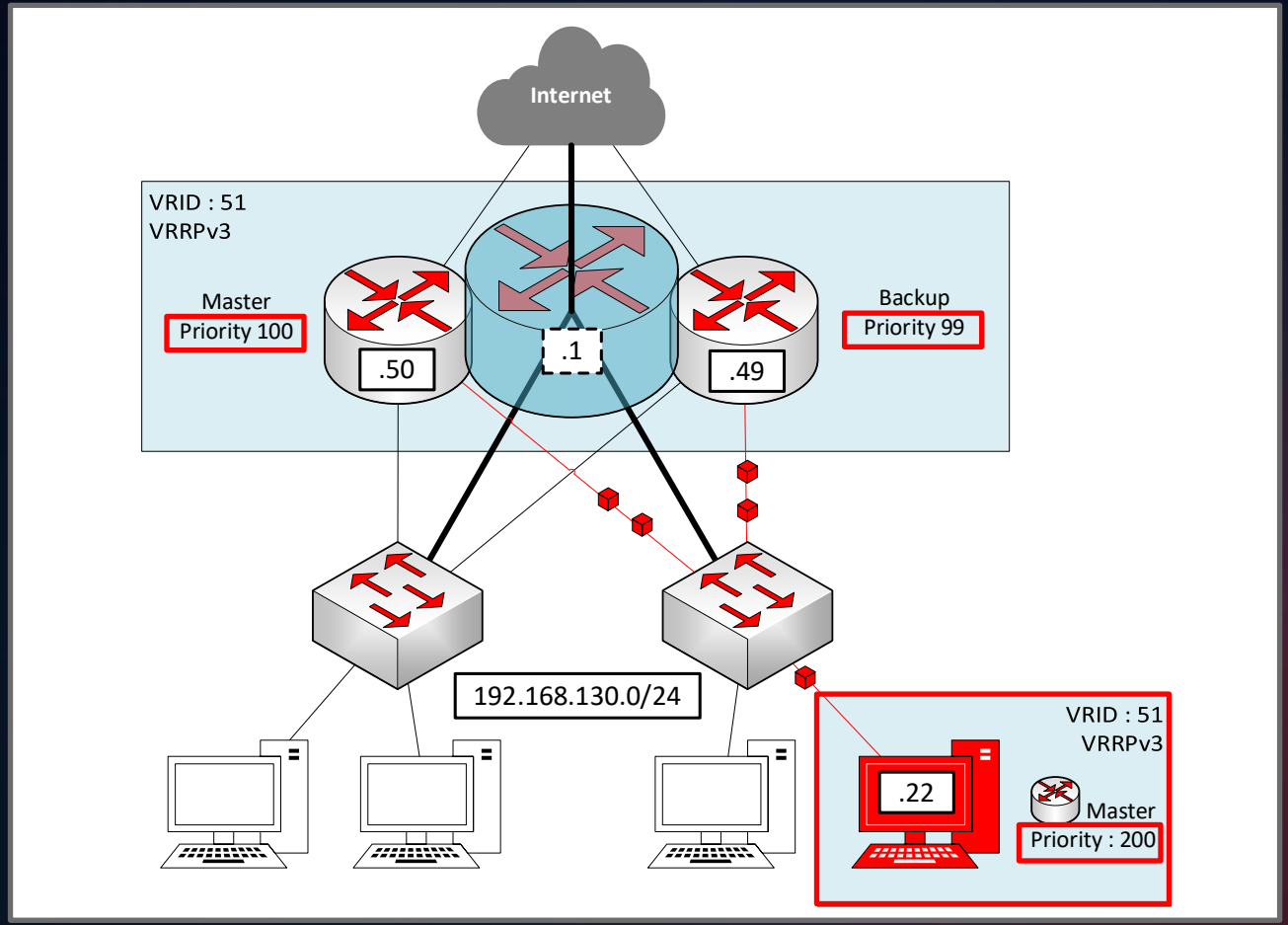
Prérequis *: être dans le même sous-réseau que les nœuds VRRP*

> 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)

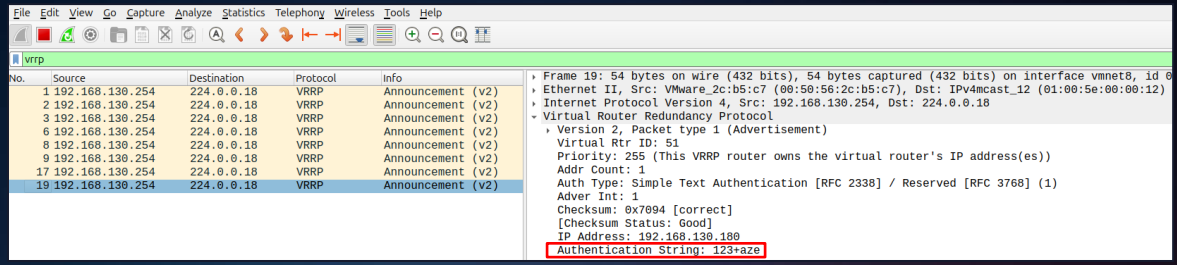
> Atteinte à la disponibilité en inondant le réseau de paquets VRRP « mal formés » (DoS logique)

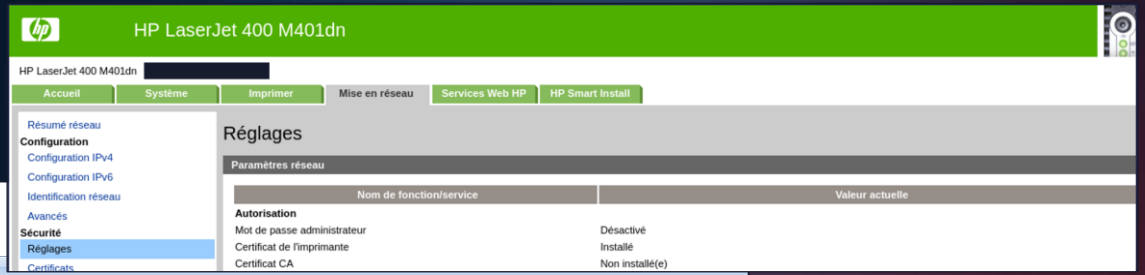
Menaces / Défaut de priorité

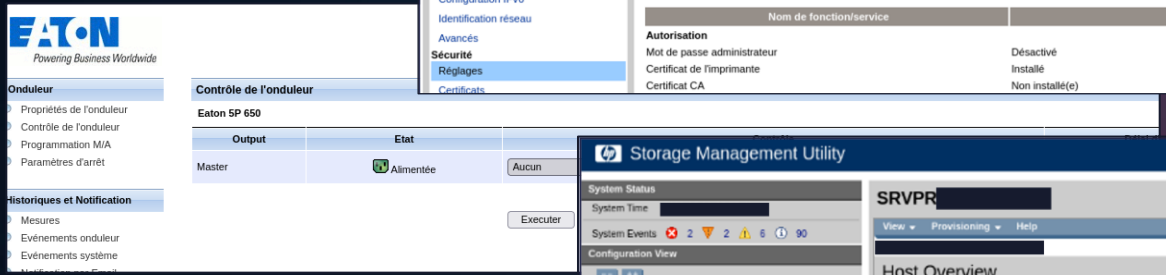


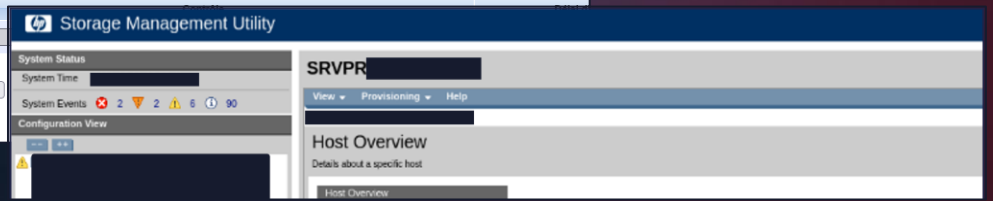
Menaces / Rejeu de mot de passe

> **VRRPv2** – Plain-text password Auth





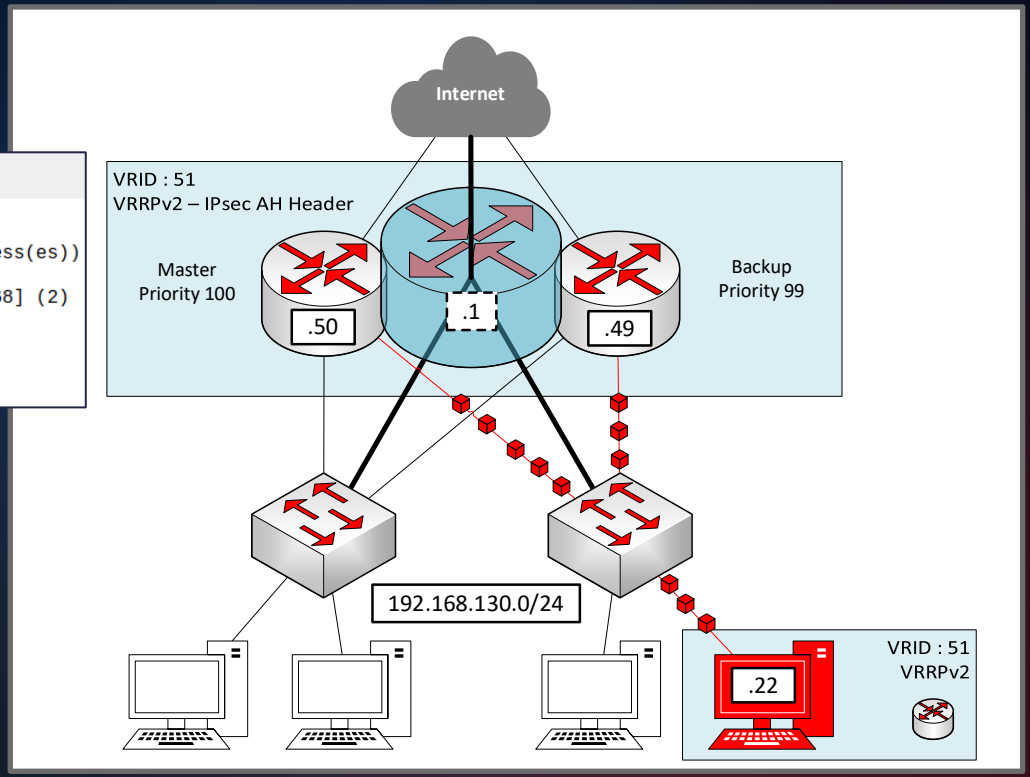




Menaces / Flooding de paquets VRRP

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

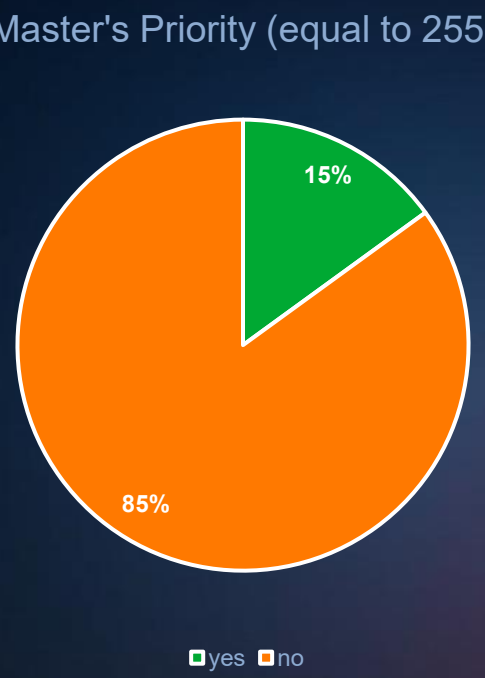
```
▸ Authentication Header
▾ Virtual Router Redundancy Protocol
  ▸ Version 2, Packet type 1 (Advertisement)
    Virtual Rtr ID: 51
    Priority: 255 (This VRRP router owns the virtual router's IP address(es))
    Addr Count: 1
    Auth Type: IP Authentication Header [RFC 2338] / Reserved [RFC 3768]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



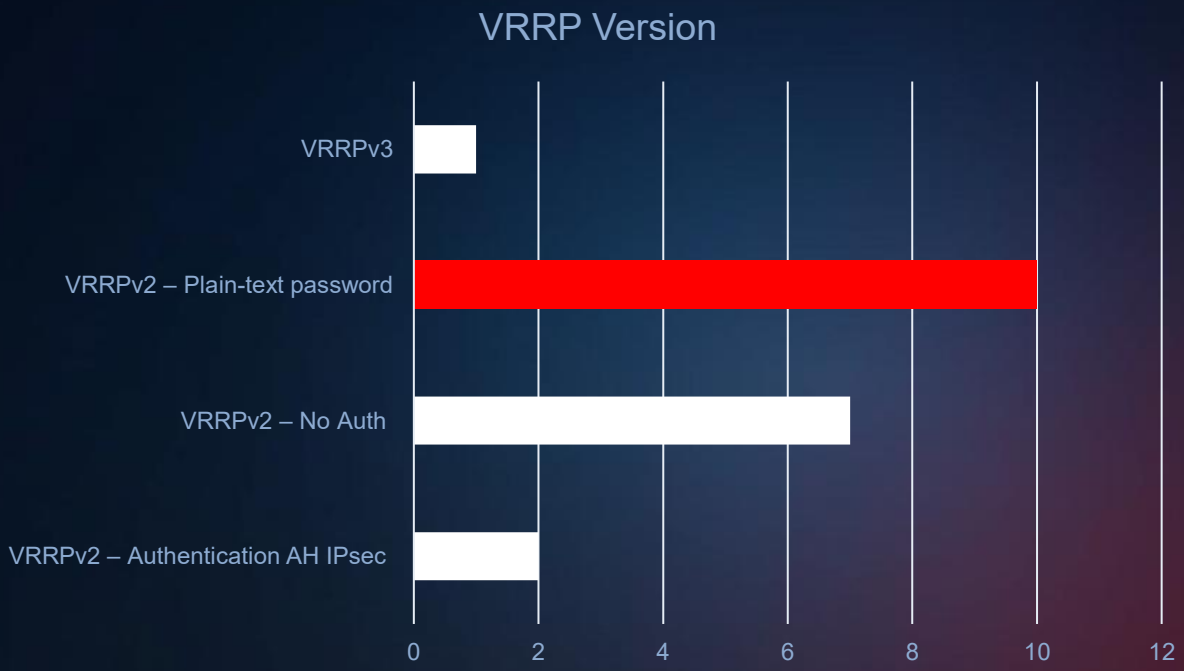
Etude : Panorama des mauvaises configurations VRRP trouvées en ligne

Lien de l'étude complète (anonymisé)

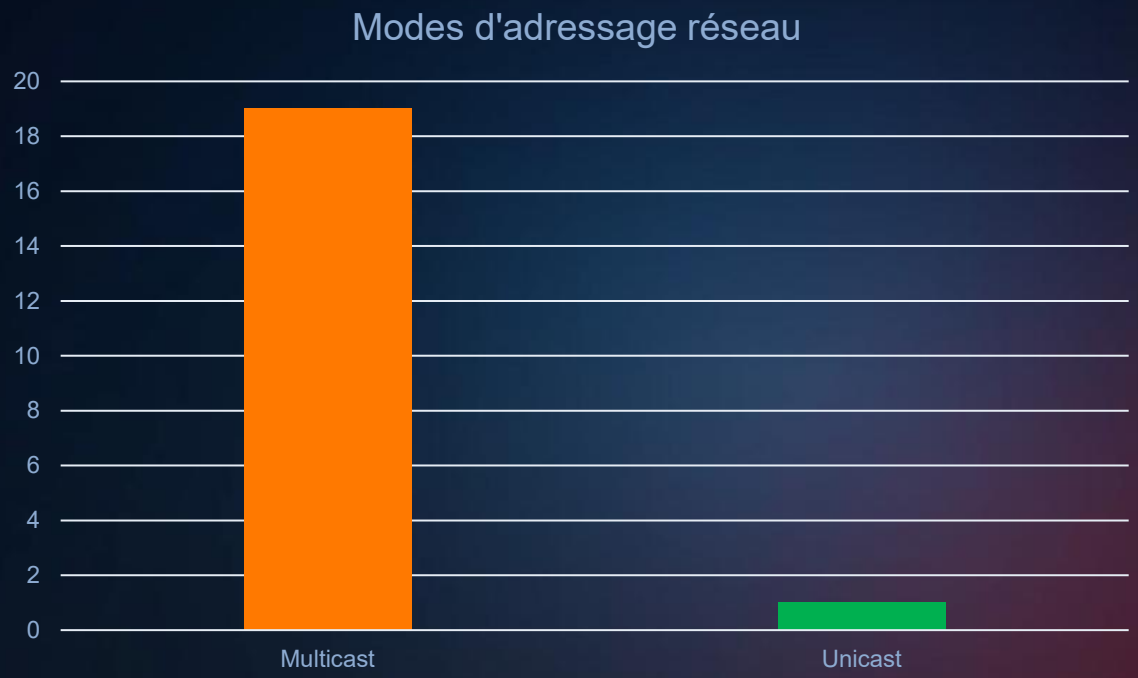
Menaces / Synthèse de l'étude



Menaces / Synthèse de l'étude

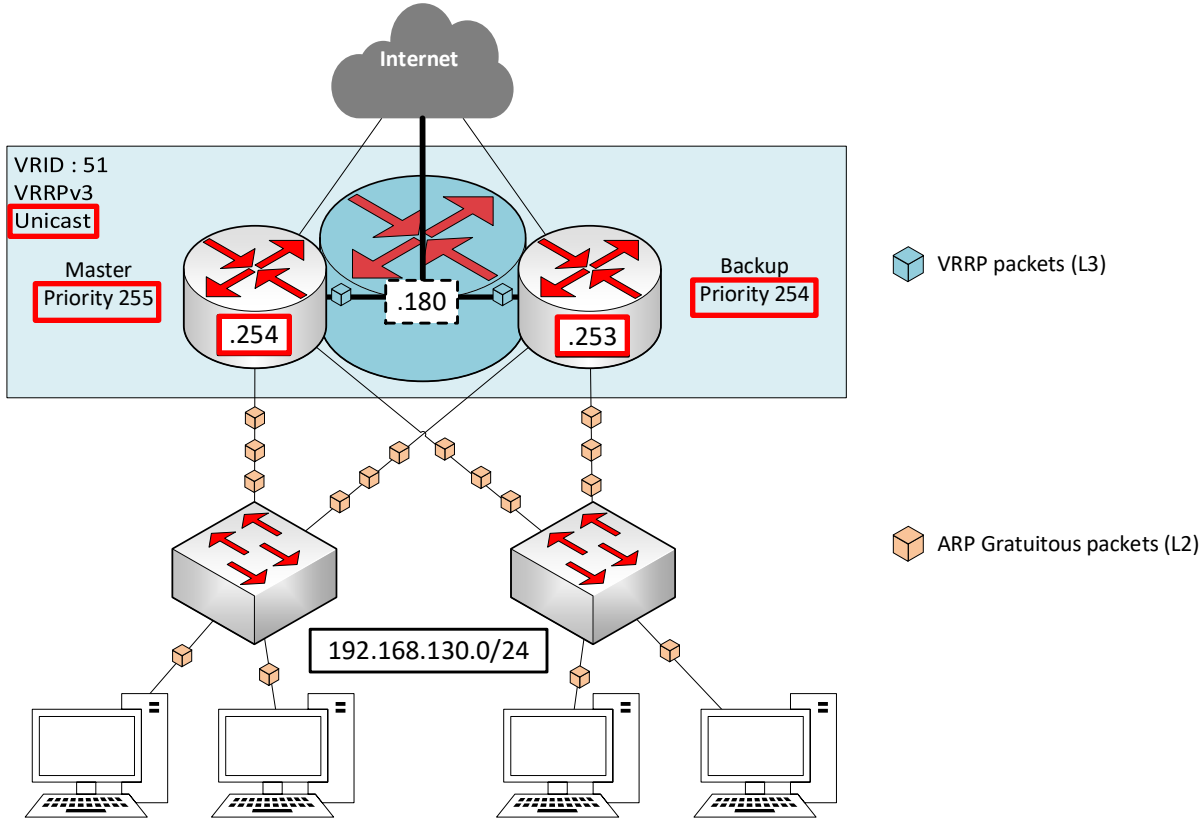


Menaces / Synthèse de l'étude



À quoi correspond une configuration VRRP « propre » ?

Configuration « SOTA*»



*State of the art

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

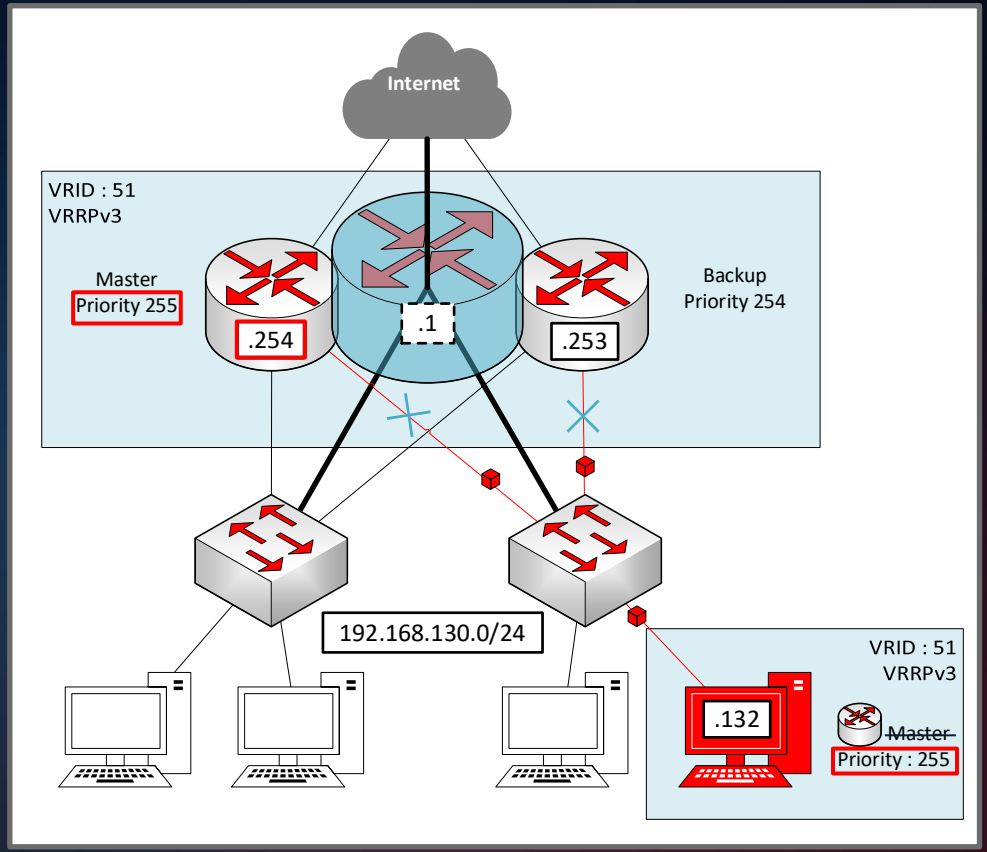
03

Au-delà du tie-break

La théorie

> Si priorités identique ➜ comparaison des IP

> Le Nœud avec « *l'IP la plus haute** » ➜ Master



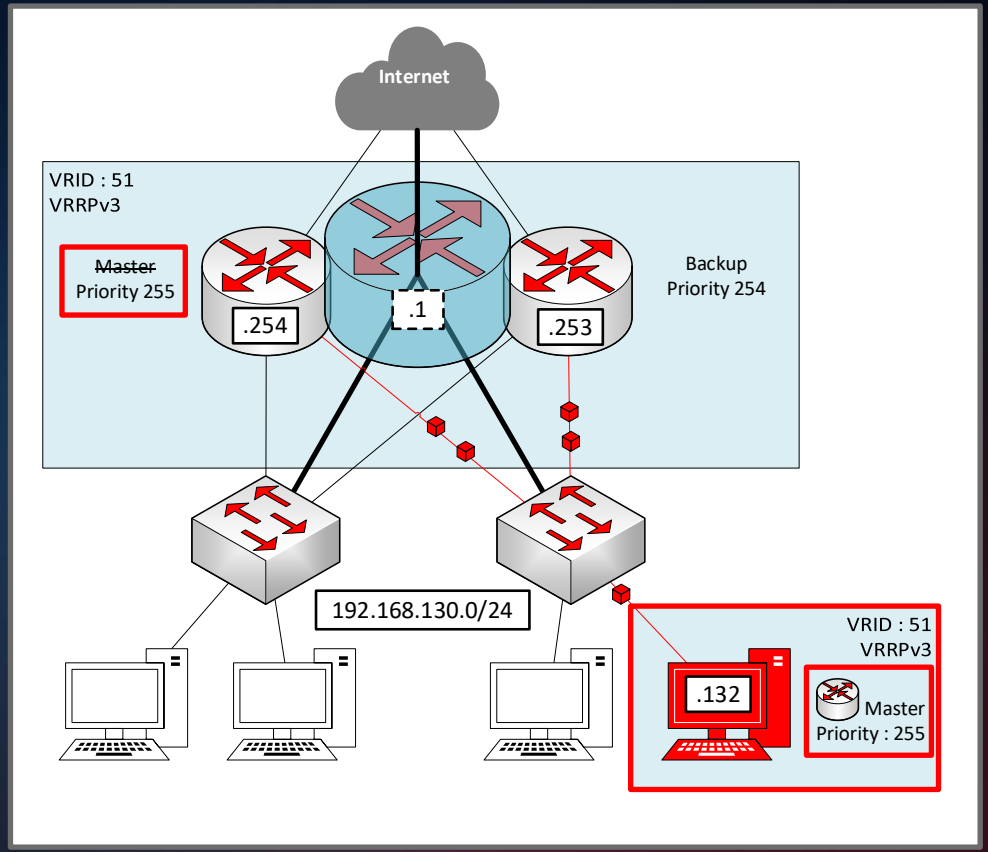
**Sur le dernier octet*

En pratique

vrrp

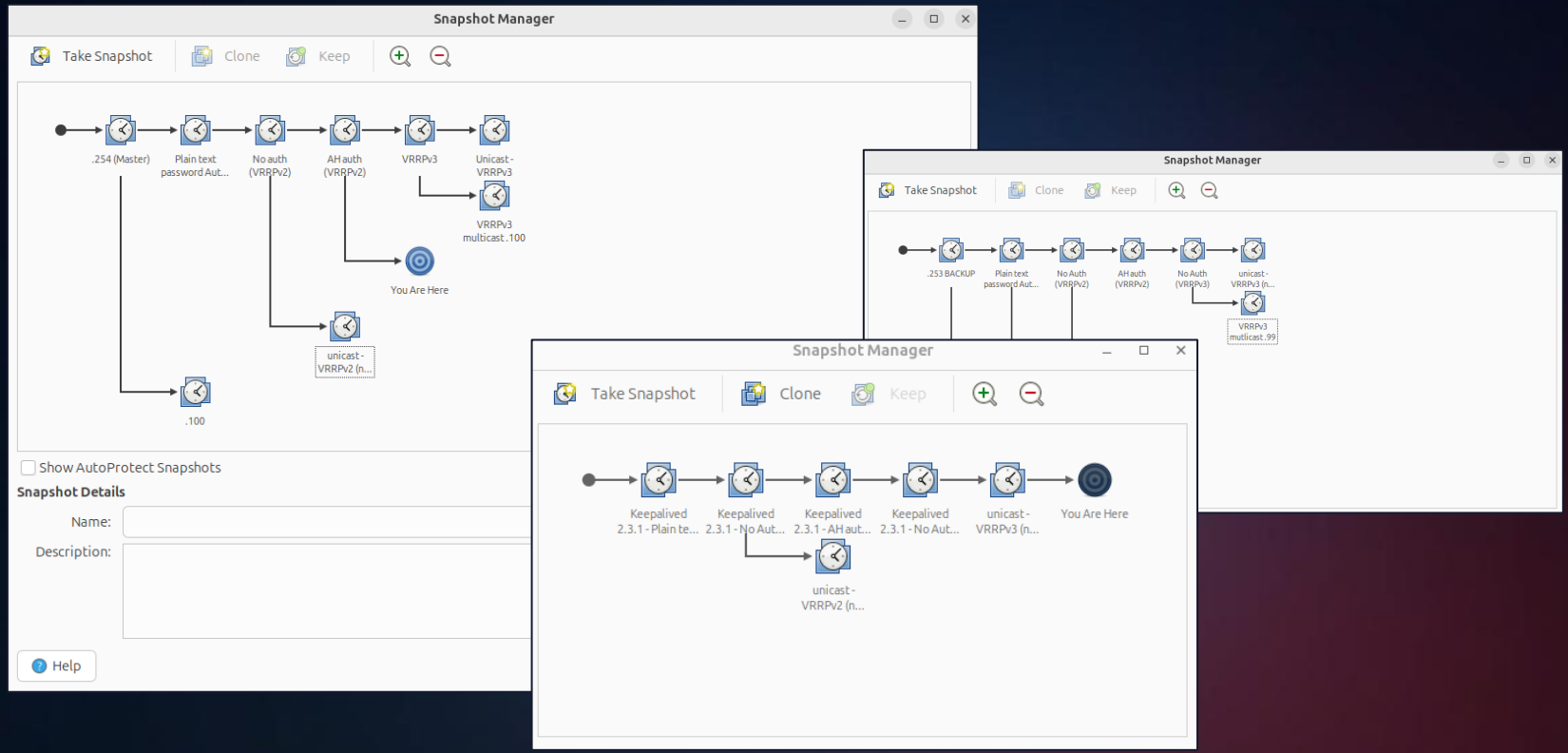
Time	Source	Destination	Protocol
0.000000000	192.168.130.254	224.0.0.18	VRRP
1.000842596	192.168.130.254	224.0.0.18	VRRP
2.001542242	192.168.130.254	224.0.0.18	VRRP
3.002588182	192.168.130.254	224.0.0.18	VRRP
4.003553864	192.168.130.254	224.0.0.18	VRRP
5.004465329	192.168.130.254	224.0.0.18	VRRP
6.005107748	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 vmnet8, 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
```




HUM...
imgflip.com

Jeux de tests – (projet keepalived)



Jeux de tests – (projet keepalived)

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

Shhhh ! 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**

~~CVE ?~~

> Keepalived suivait à la lettre la RFC 9568

~~CVE~~ ?

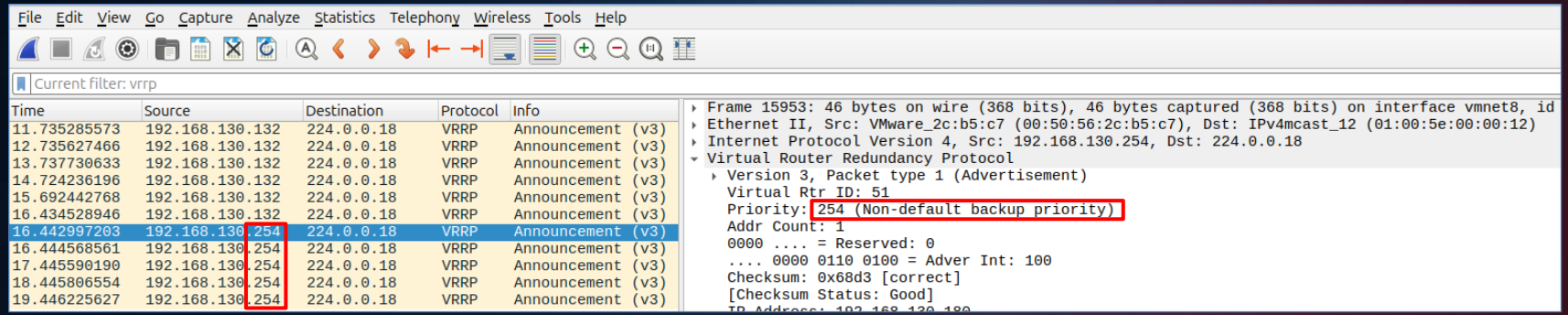
> Le problème provenait de la RFC 9568

> 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 :



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)

*RFC 5798

04

Recommandations & 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

orange Cyberdefense

Keep-it-alived :

Étude de la sécurité du protocole VRRP

Q&A