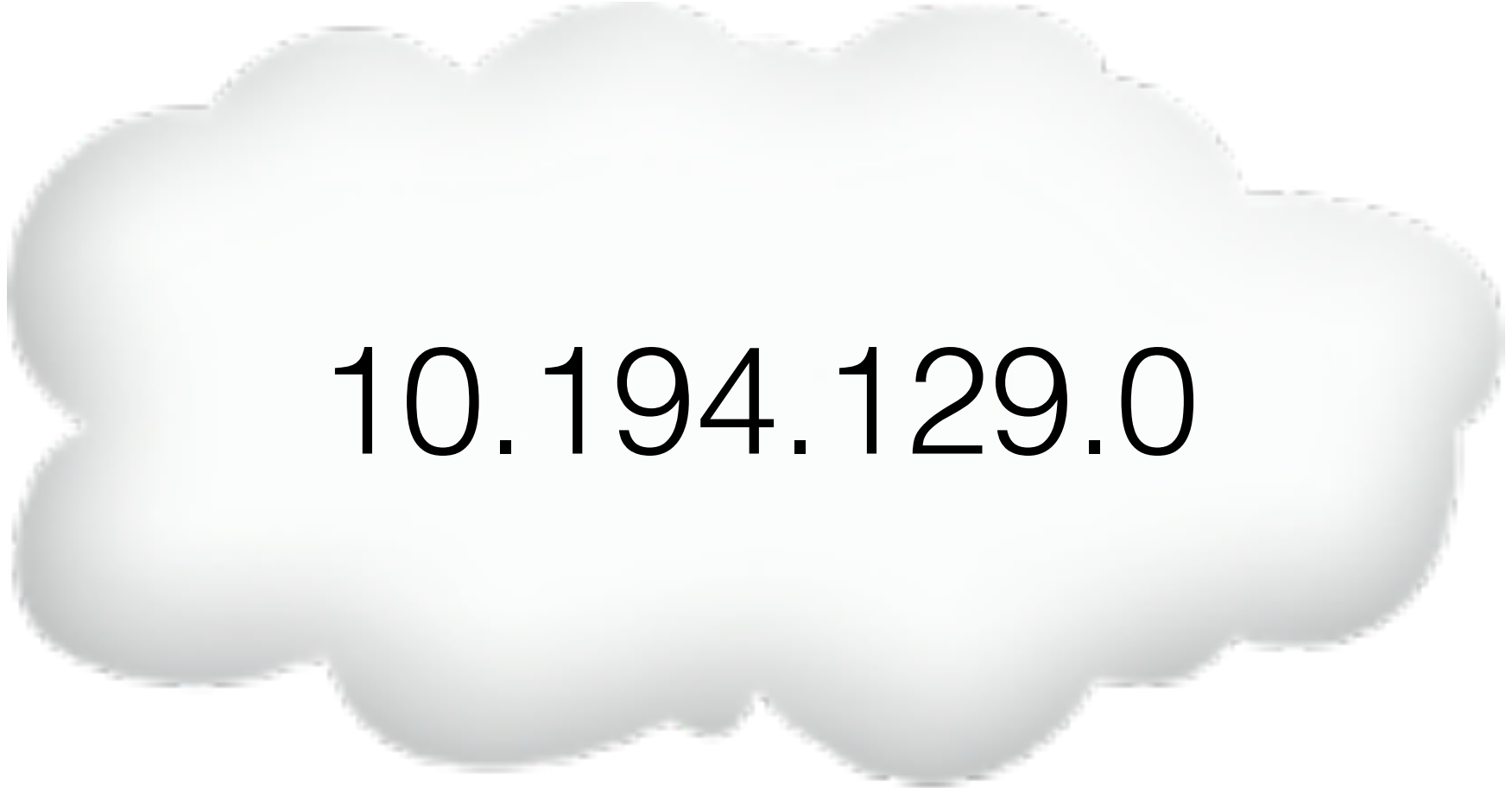
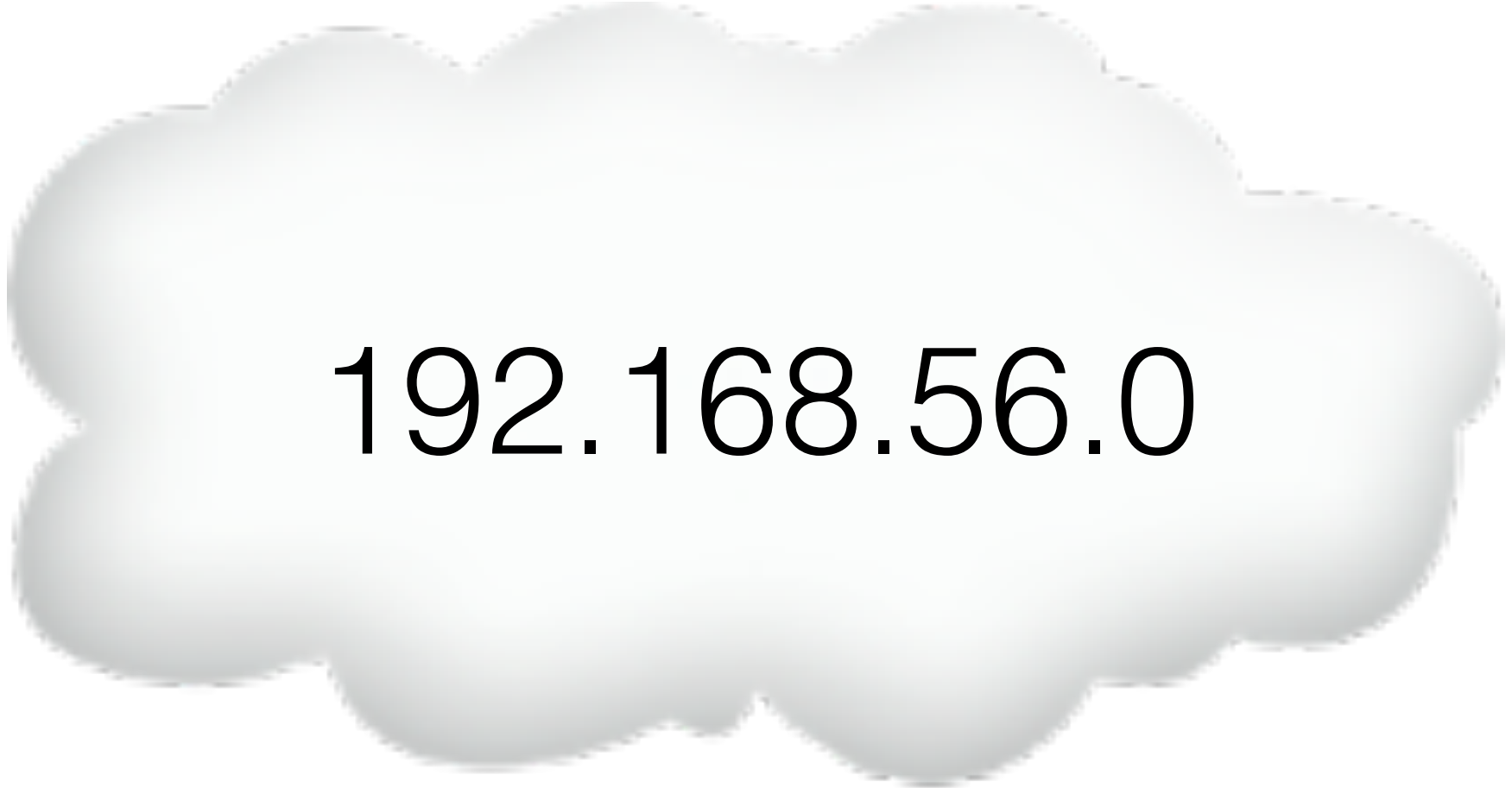
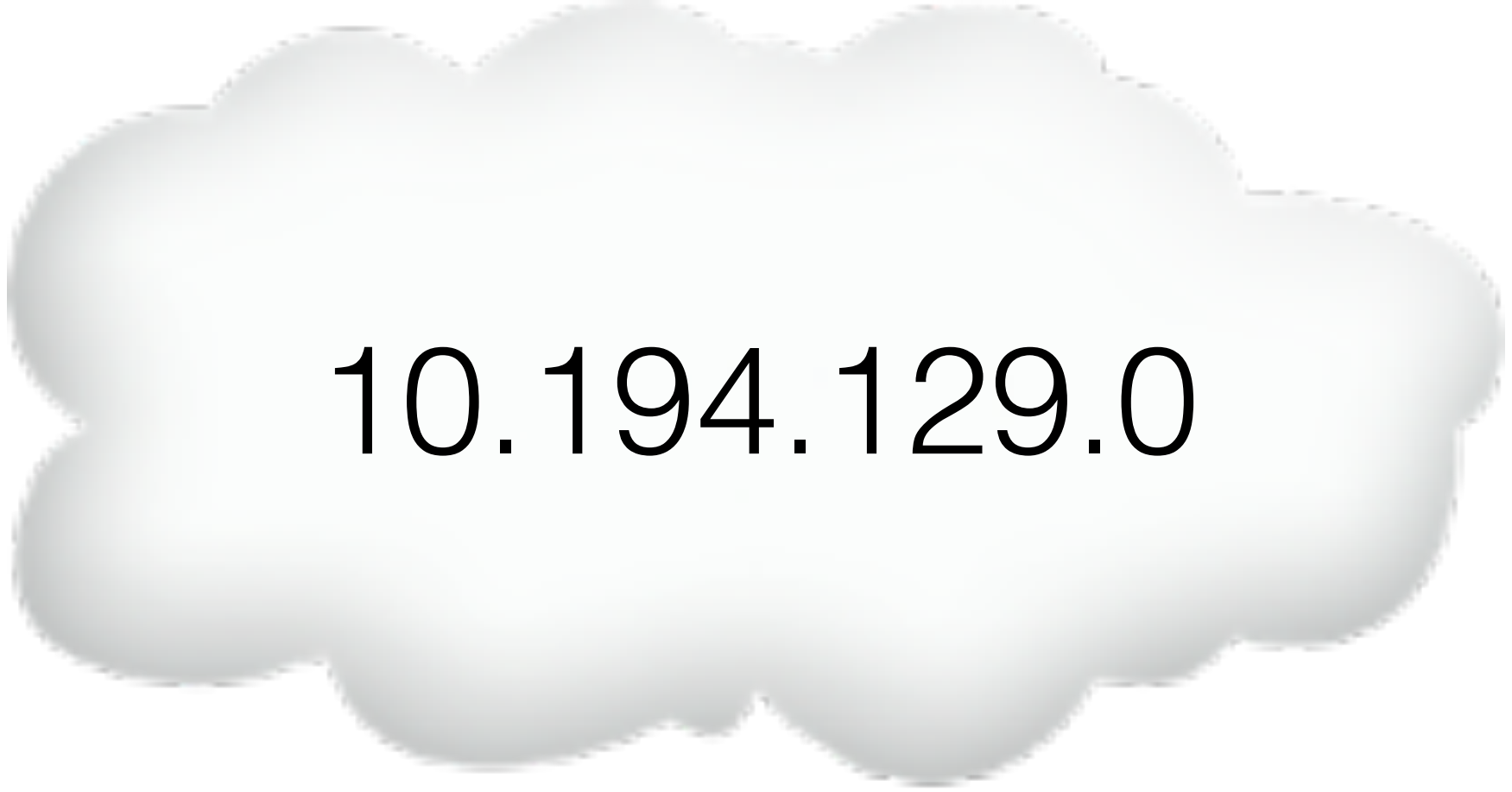
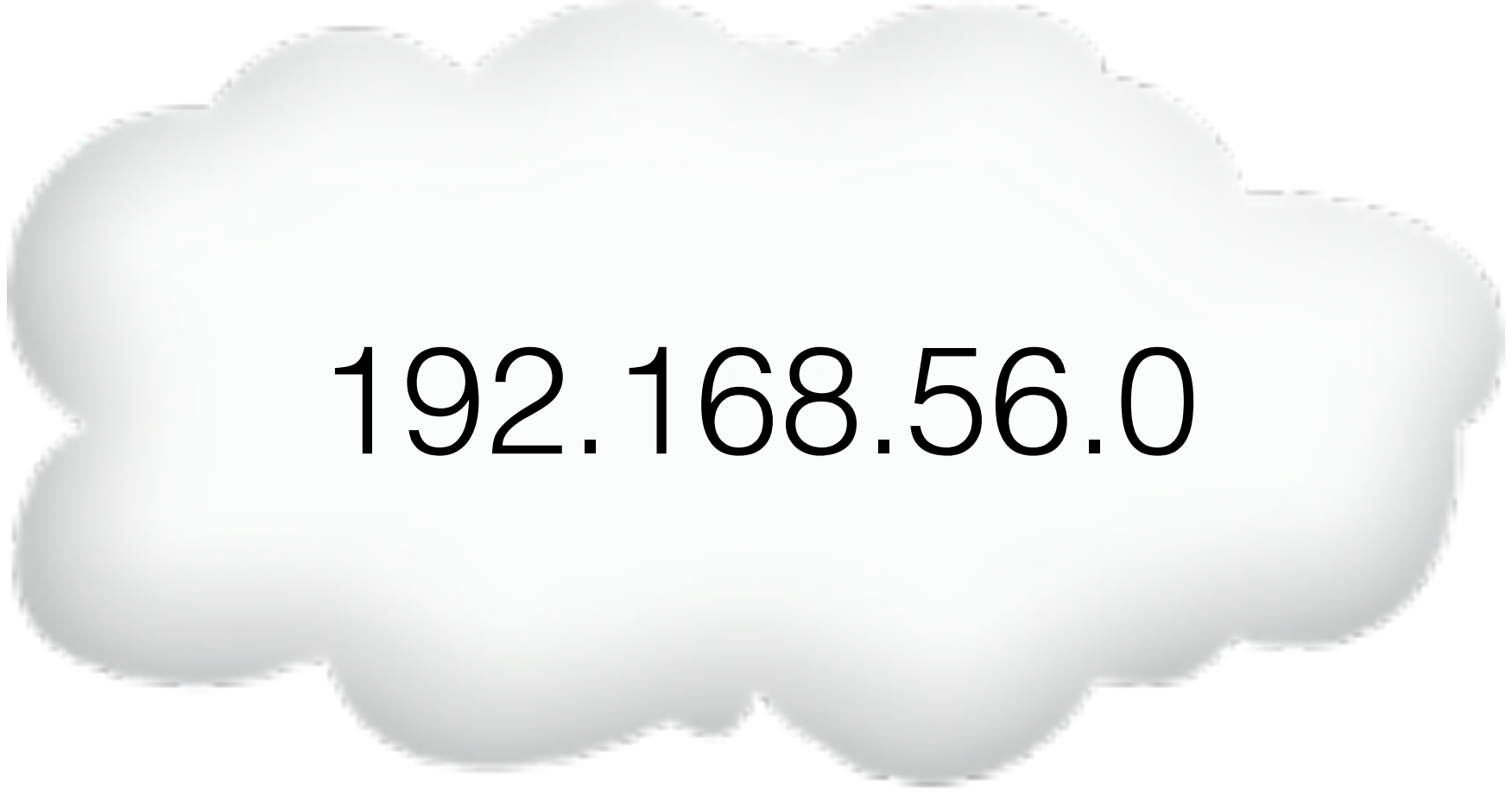

10.194.129.0

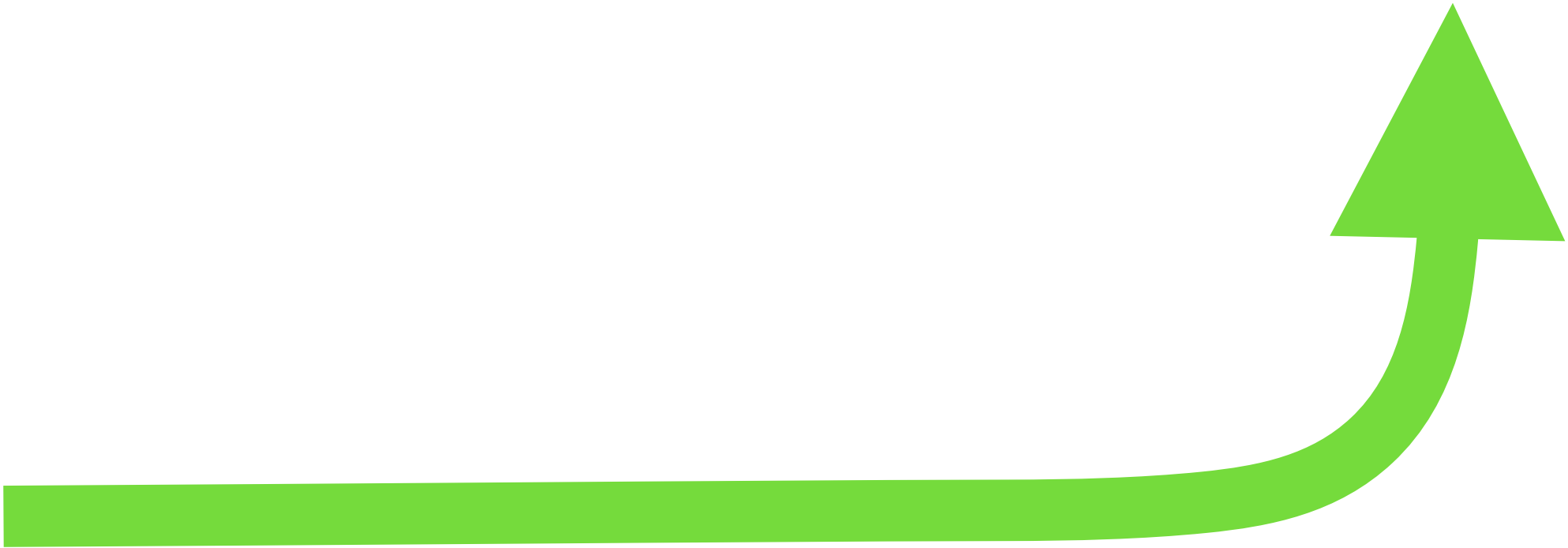

10.193.0.0

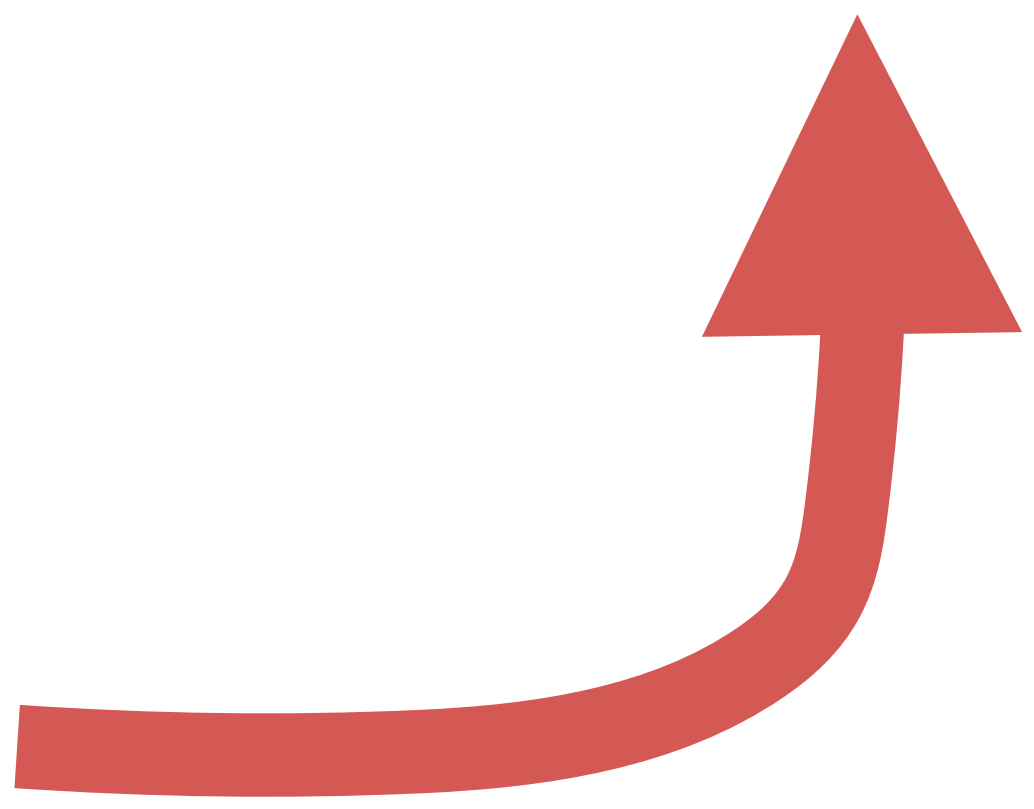

192.168.56.0


10.194.129.0


10.193.0.0


192.168.56.0





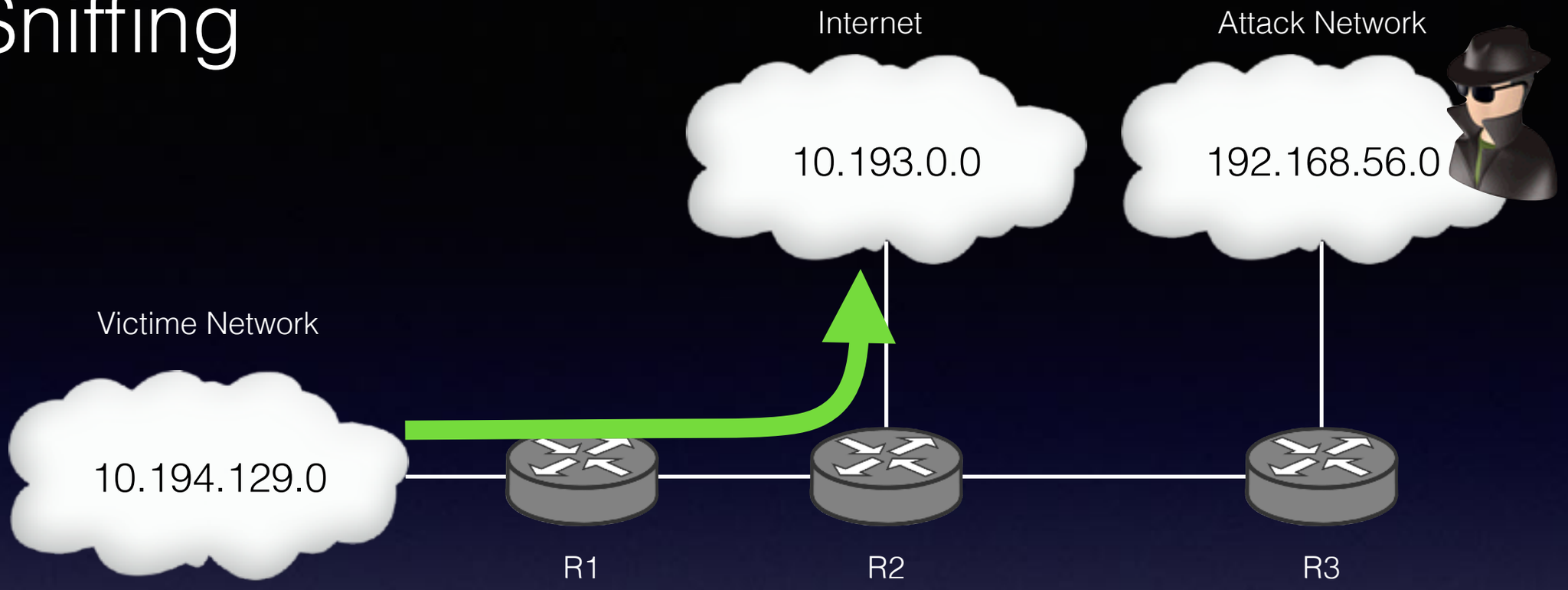
Tunnel GRE

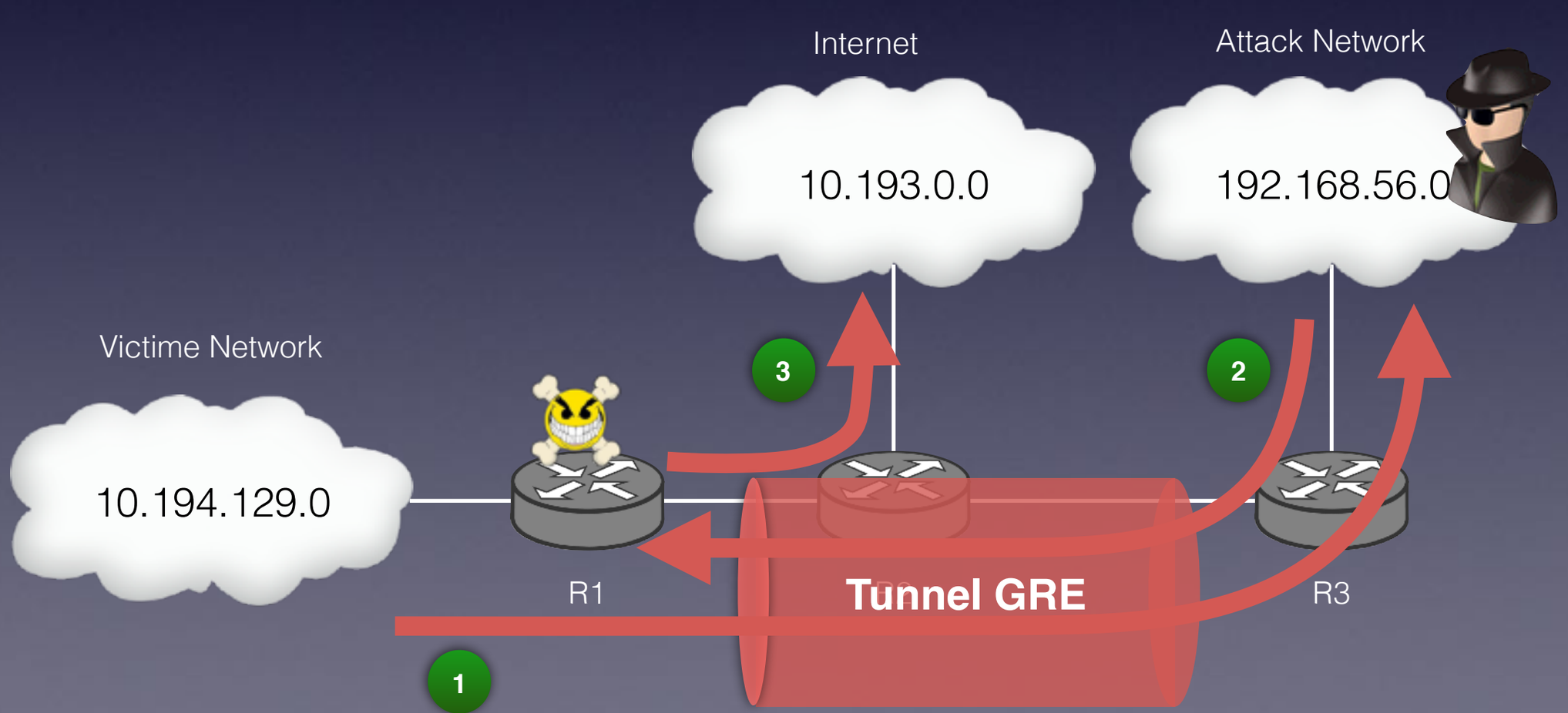

1


2


3

Gre Sniffing





Exploitation

Attaques sur les protocoles Cisco :
Attaques d'empreinte des mots de passe

- Plusieurs formes d'authentification possibles. Les commandes associées en mode d'exécution privilégié
  - `enable password`
  - `enable secret`
- `enable password <password>`
  - mot de passe stocké en clair dans le fichier de configuration !
  - Possibilité de le chiffrer en « type 7 »
  - Commande `service password-encryption`
- `enable secret <password>`
  - Mot de passe chiffré en « type 5 » dans le fichier de configuration.