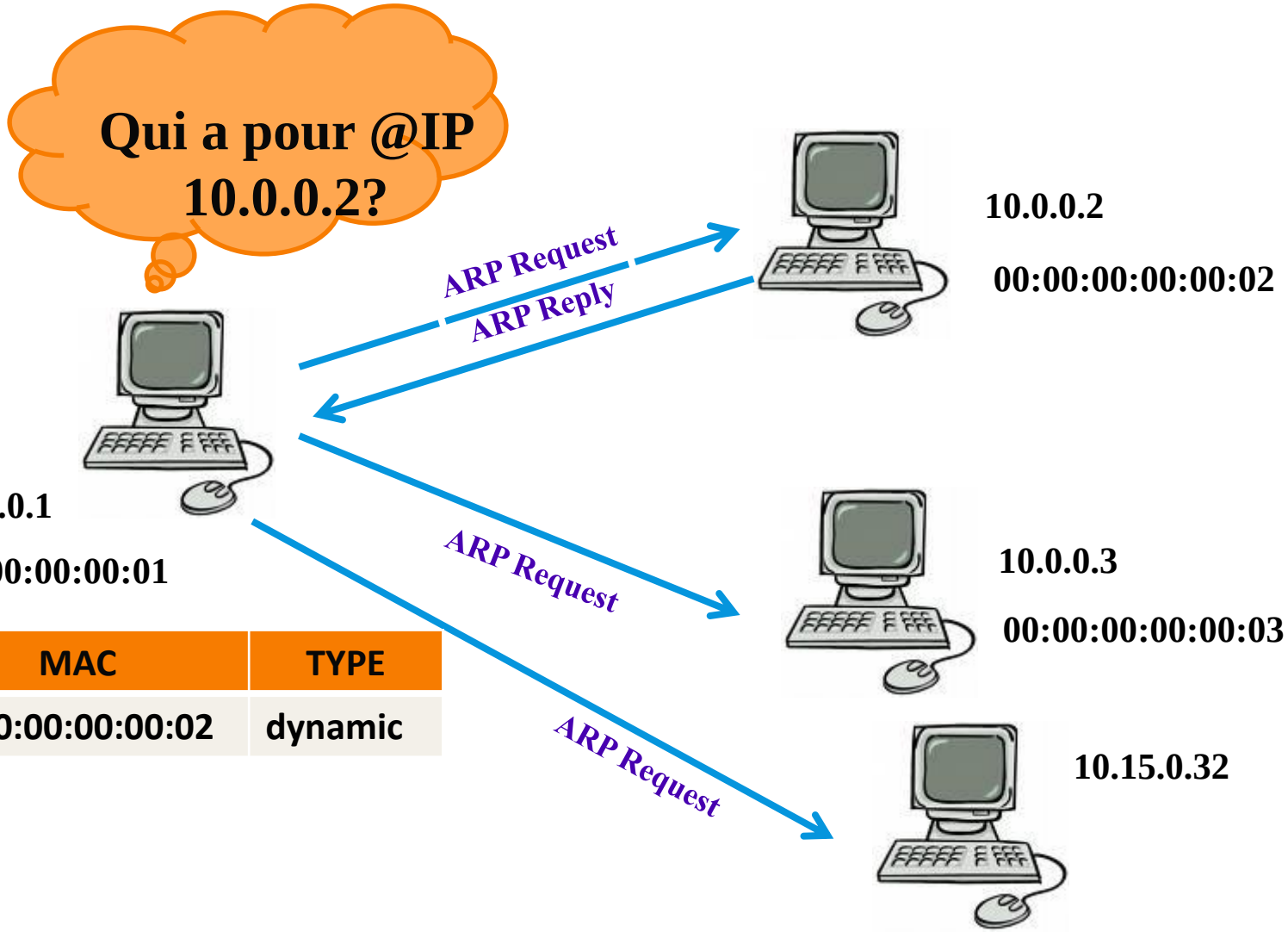
ARP - généralité

- ARP (Adresse Résolution Protocol)
  - RFC 826
  - Permet la correspondance @IP <-> @MAC
  - Utilisation :
    - Requête ARP (fonctionne en broadcast)
    - Réponse ARP (en unicast)
    - Mise en mémoire dans une table dynamique :

      arp –a
  - ARP est presque toujours utilisé avant d'envoyer un message en IP.
  - ARP gratuite (gratuitous ARP) : permet d'annoncer la correspondance à tous.

ARP (1)



IP	MAC	TYPE
10.0.0.2	00:00:00:00:00:02	dynamic

ARP - format

Hardware type : 01 ethernet Protocol type : 0x0800 IP

+	Bits 0 - 7	8 - 15	16 - 31
0	*Hardware type*		*Protocol type*
32	*Hardware Address Length*	*Protocol Address Length*	*Operation*
64	*Sender Hardware Address*		
?	*Sender Protocol Address*		
?	*Target Hardware Address*		
?	*Target Protocol Address*		

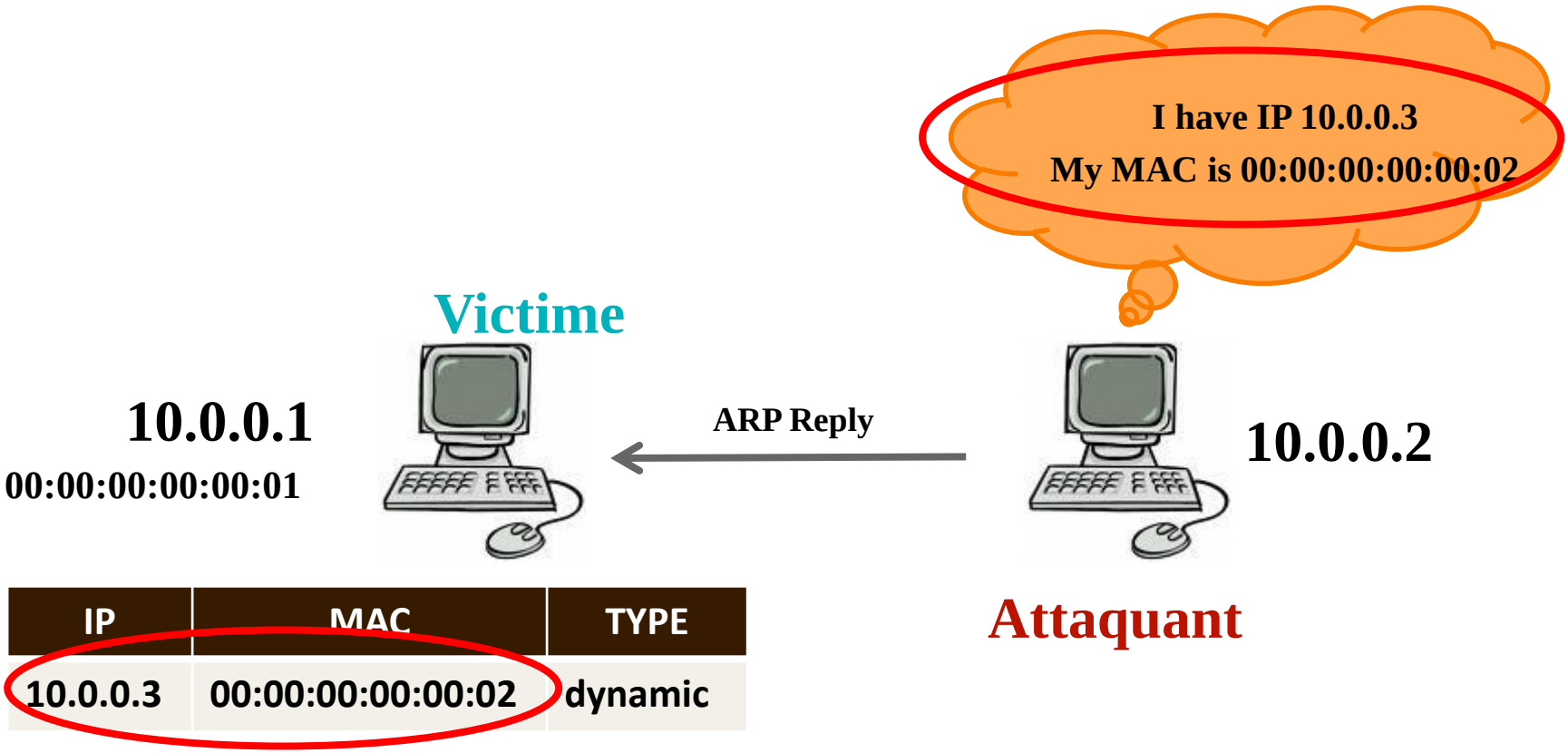
Hardware address length : 06 ethernet

Protocol Address length : 04 pour IPv4 , 16 pour Ipv6

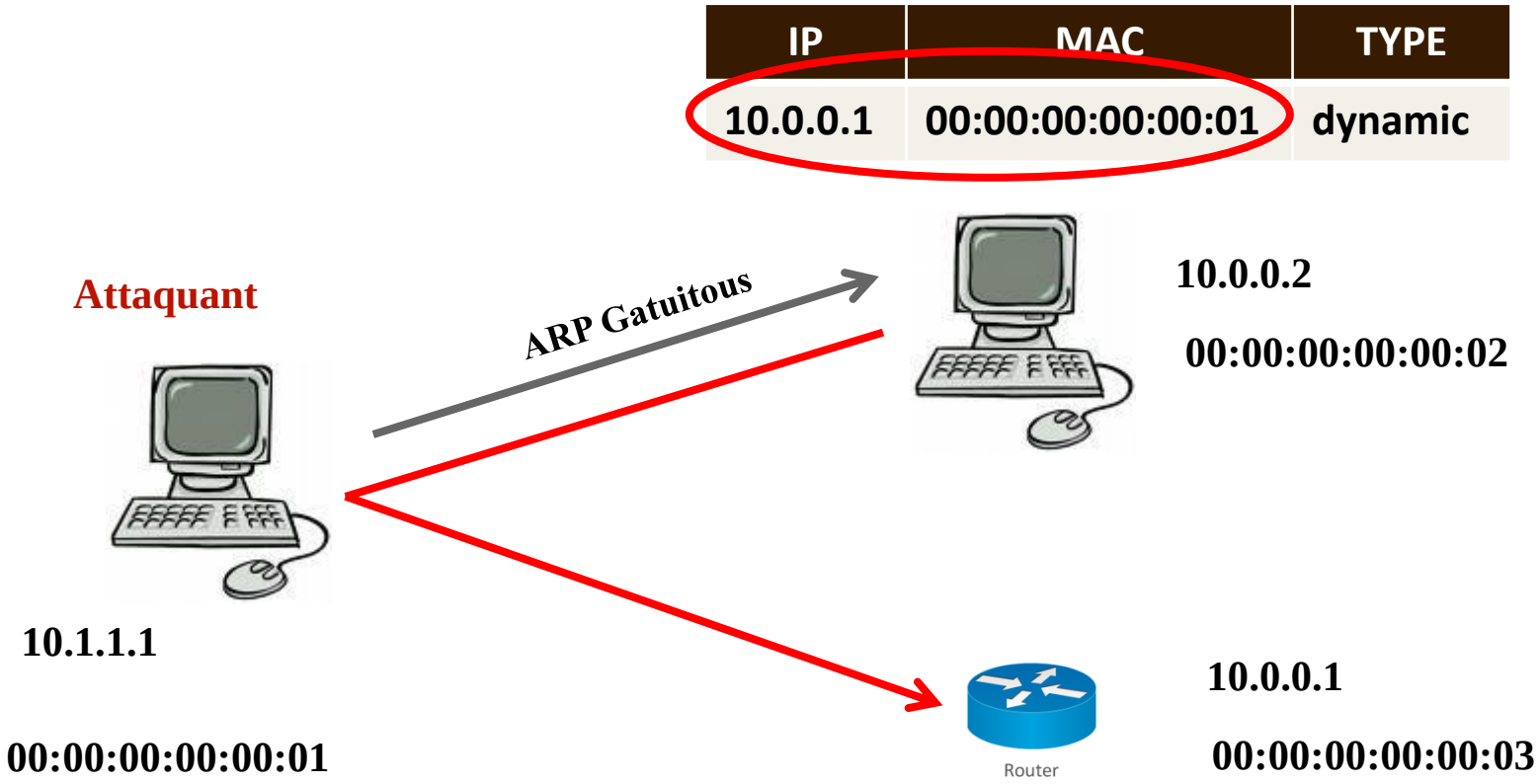
Opération : 1 requête

2 : réponse

ARP spoofing (1)



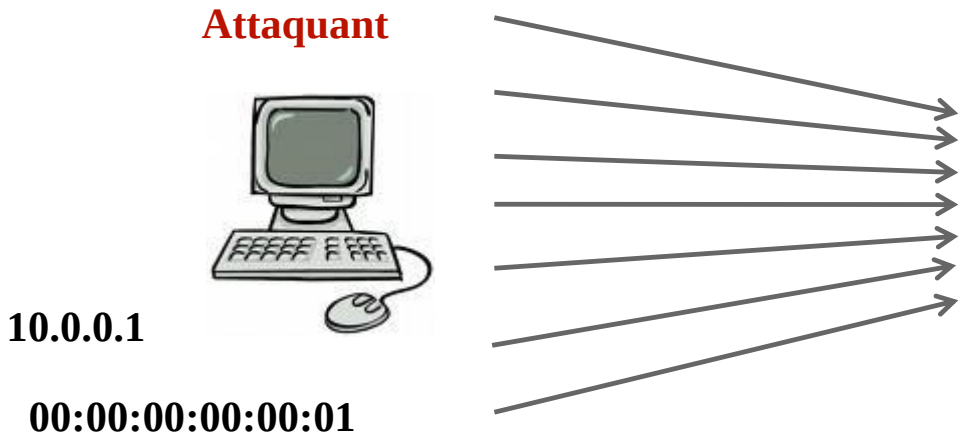
ARP spoofing (2)



Création de l'attaque Man in the Middle

Mac flooding

- Attaque du switch par l'intermédiaire de l'@MAC
- Objectif : Saturer la table CAM



PORT	MAC
1	00:00:01:01:01:01
1	00:00:02:02:02:02
….	……
…..	…….

- Obliger le switch à passer en mode HUB

Contre-mesure

- **ARP statique**
  - arp –s … : inscrit en statique une référence dans la table arp → prioritaire

- Utilisation d'équipement
  - Pare-feu pour boquer les ARP gratuitous

    (seul les réponses ARP qui suivent une requête sont autorisées)
  - IDS
  - DAI : Dynamic ARP Protection
    - En corrélation avec le DHCP (Création d'une BD des ports)
  - Configuration port des switches (Port-security)